

JP1 Version 13

JP1/Integrated Management 3 - Manager 構築ガイド

3021-3-L03-30

前書き

■ 対象製品

適用 OS のバージョン, JP1/Integrated Management 3 - Manager, JP1/Integrated Management 3 - View, および JP1/Integrated Management 3 - Agent が前提とするサービスパックやパッチなどの詳細については各製品のリリースノートで確認してください。

●JP1/Integrated Management 3 - Manager (適用 OS : Windows)

P-2A2C-8EDL JP1/Integrated Management 3 - Manager 13-11

製品構成一覧および内訳形名

P-CC2A2C-9MDL JP1/Integrated Management 3 - Manager 13-11 (適用 OS: Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC2A2C-6HDL JP1/Integrated Management 3 - View 13-00 (適用 OS: Windows 11, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10)

P-CC2A2C-9GDL JP1/Integrated Management 3 - Agent 13-11 (適用 OS: Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-11 (適用 OS: Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC2A2C-6LDL JP1/Base 13-10 (適用 OS: Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-10 (適用 OS: Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC1M2C-6LDL JP1/Base 13-10 (適用 OS: AIX)

●JP1/Integrated Management 3 - Manager (適用 OS : Linux)

P-842C-8EDL JP1/Integrated Management 3 - Manager 13-11

製品構成一覧および内訳形名

P-CC842C-9MDL JP1/Integrated Management 3 - Manager 13-11 (適用 OS: Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7)

P-CC9W2C-9MDL JP1/Integrated Management 3 - Manager 13-11 (適用 OS: SUSE Linux 15, SUSE Linux 12)

P-CC2A2C-6HDL JP1/Integrated Management 3 - View 13-00 (適用 OS: Windows 11, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10)

P-CC2A2C-9GDL JP1/Integrated Management 3 - Agent 13-11 (適用 OS: Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-11 (適用 OS: Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC2A2C-6LDL JP1/Base 13-10 (適用 OS: Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-10 (適用 OS: Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC1M2C-6LDL JP1/Base 13-10 (適用 OS: AIX)

■ 輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。

なお、不明な場合は、弊社担当営業にお問い合わせください。

■ 商標類

記載の会社名、製品名などは、それぞれの会社の商標もしくは登録商標です。

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from <ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/>

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)
2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)

4. 本製品には OpenSSL Toolkit ソフトウェアを OpenSSL License および Original SSLeay License に従い使用しています。OpenSSL License および Original SSLeay License は以下のとおりです。

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*

=====

* Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:

*

* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.

*

* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.

*

* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

*

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without


```

* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
=====
=====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License
-----

```

```

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to. The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * "This product includes cryptographic software written by
 * Eric Young (eay@cryptsoft.com)"
 * The word 'cryptographic' can be left out if the rouines from the library
 * being used are not cryptographic related :-).

```

- * 4. If you include any Windows specific code (or a derivative thereof) from
- * the apps directory (application code) you must include an acknowledgement:
- * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
- *
- * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND
- * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
- * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
- * PURPOSE
- * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
- * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
- * CONSEQUENTIAL
- * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
- * GOODS
- * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
- * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
- * STRICT
- * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
- * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
- * SUCH DAMAGE.
- *
- * The licence and distribution terms for any publically available version or
- * derivative of this code cannot be changed. i.e. this code cannot simply be
- * copied and put under another distribution licence
- * [including the GNU Public Licence.]
- */

This product includes software developed by Andy Clark.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (<http://relaxngcc.sf.net/>).

This product includes software developed by IAIK of Graz University of Technology.

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (<http://java.apache.org/>).

Java is a registered trademark of Oracle and/or its affiliates.



■ マイクロソフト製品の表記について

このマニュアルでは、マイクロソフト製品の名称を次のように表記しています。

表記	製品名
Hyper-V	Microsoft(R) Windows Server(R) 2012 Hyper-V(R)
SCVMM	Microsoft(R) System Center Virtual Machine Manager 2012
Windows 10	Windows(R) 10 Enterprise 64-bit
	Windows(R) 10 Home 64-bit
	Windows(R) 10 Pro 64-bit
Windows 11	Windows(R) 11 Enterprise
	Windows(R) 11 Home
	Windows(R) 11 Pro
Windows Server 2016	Microsoft(R) Windows Server(R) 2016 Datacenter
	Microsoft(R) Windows Server(R) 2016 Standard
Windows Server 2019	Microsoft(R) Windows Server(R) 2019 Datacenter
	Microsoft(R) Windows Server(R) 2019 Standard

表記	製品名
Windows Server 2022	Microsoft(R) Windows Server(R) 2022 Datacenter
	Microsoft(R) Windows Server(R) 2022 Standard

Windows 11, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10 を総称して Windows と表記することがあります。

■ 発行

2025 年 3 月 3021-3-L03-30

■ 著作権

Copyright (C) 2023, 2025 Hitachi, Ltd.

Copyright (C) 2023, 2025 Hitachi Solutions, Ltd.

変更内容

変更内容(3021-3-L03-30) JP1/Integrated Management 3 - Manager 13-11

追加・変更内容	変更箇所
複数マネージャーホストへのデータ配信機能を追加した。 これに伴い、複数マネージャーホストへのデータ配信機能の設定および解除に関する説明を追加した。 また、統合エージェント制御基盤のセカンダリーの設定に関する説明を追加した。	1.3.1(3)(b), 1.21.2(2)(a), 1.21.2(2)(b), 1.21.2(2)(c), 1.21.2(2)(i), 1.21.2(2)(j), 1.25.1(5), 2.19.2(2)(h), 2.19.2(2)(i), 2.23.1(4), 7.3.6, 7.3.7(2), 7.6.2, 7.7.3, 8.3.7(2), 8.6.2, 8.7.3
JP1/IM - Agent による性能監視機能に、Hyper-V 監視機能 (Windows exporter (Hyper-V 監視)) を追加した。 これに伴い、Windows exporter (Hyper-V 監視) の構築に関する説明を追加した。 また、JP1/IM - Agent のインストーラーで使用する初期設定用環境変数 JP1IMAGENT_ADDON_WINDOWS_EXPORTER_HYPERV_ACTIVE (Hyper-V 監視機能の有効/無効の設定) を追加した。	1.3.1(3)(c), 1.21.2(3)(k), 1.21.2(15), 7.5, 7.6.2
JP1/IM - Agent をバージョン 13-00~13-10 からバージョンアップした場合の注意事項を追加した。	1.3.1(4), 1.3.3(15), 2.3.1(3), 2.3.4(10)
次に示す仮想化プラットフォームで、JP1/IM - Agent をイメージ作成モードでインストールした統合エージェントホスト環境の仮想マシンのクローンを作成できるようにした。 • VMware ESX • Hyper-V • SCVMM また、統合エージェントホストの複製ができる仮想化プラットフォームの説明を追加した。	1.3.6, 1.26, 2.3.7, 2.24
JP1/IM - Manager をバージョン 13-10 以前からバージョンアップした場合に実施するインテリジェント統合管理データベースの設定を追加した。	1.19.7(8), 2.18.11(10), 7.6.1, 8.6.1
作成済みのコンテナ上の JP1/IM - Agent をバージョンアップする手順を追加した。	1.22.2
JP1/IM - Agent のオプション機能の構築での、IM マネージャー更新可能定義ファイルリスト定義ファイルおよび IM エージェント更新可能定義ファイルの更新に関する説明を追加した。	1.23.1(1)(b), 1.23.1(1)(c)
JP1/IM - Agent による性能監視機能に、Microsoft SQL Server 監視機能 (SQL exporter) を追加した。 これに伴い、SQL exporter の構築に関する説明を追加した。	1.23.4
JP1/IM - Agent の論理ホストをセットアップするコマンドと設定ファイルを追加した。 これに伴い、JP1/IM - Agent の論理ホストの新規インストールおよびバージョンアップインストールするときの手順を追加した。	7.3.6, 7.6.2, 8.3.6, 8.6.2

単なる誤字・脱字などはお断りなく訂正しました。

はじめに

このマニュアルは、JP1/Integrated Management 3 - Manager, JP1/Integrated Management 3 - View, および JP1/Integrated Management 3 - Agent のシステム構築方法について説明したものです。なお、このマニュアルでは、JP1/Integrated Management 3 - Manager, JP1/Integrated Management 3 - View, および JP1/Integrated Management 3 - Agent を総称して、JP1/Integrated Management または JP1/IM と表記します。また、このマニュアルでの JP1/Integrated Management - Manager, JP1/Integrated Management - View, および JP1/Integrated Management - Agent は、それぞれ JP1/Integrated Management 3 - Manager, JP1/Integrated Management 3 - View, および JP1/Integrated Management 3 - Agent と読み替えてください。

■ 対象読者

オープンプラットフォームのシステムを管理するインフラを、JP1/IM で構築される方を対象としています。具体的には次の方を対象としています。

- ・ システムで発生する事象を一元監視するシステムを JP1/IM を使って構築されるシステム管理者
- ・ OS およびアプリケーションについて知識がある方

■ マニュアルの構成

このマニュアルは、次に示す章から構成されています。

第 1 章 インストールとセットアップ (Windows の場合)

Windows 環境で JP1/IM をインストールおよびセットアップする手順について説明しています。

第 2 章 インストールとセットアップ (UNIX の場合)

UNIX 環境で JP1/IM をインストールおよびセットアップする手順について説明しています。

第 3 章 IM 構成管理によるシステムの階層構成の設定

IM 構成管理を使用する場合にシステムの階層構成 (IM 構成) を設定する方法について説明しています。

第 4 章 インテリジェント統合管理基盤の設定

インテリジェント統合管理基盤を使用するための環境を設定する方法について説明しています。

第 5 章 セントラルコンソールの設定

セントラルコンソールを使用するための環境を設定する方法について説明しています。

第6章 セントラルスコープの設定

セントラルスコープを使用するための環境を設定する方法について説明しています。

第7章 クラスタシステムでの運用と環境構築 (Windows の場合)

Windows の場合の JP1/IM - Manager のクラスタシステムでの運用と環境構築について説明しています。

第8章 クラスタシステムでの運用と環境構築 (UNIX の場合)

UNIX の場合の JP1/IM - Manager のクラスタシステムでの運用と環境構築について説明しています。

第9章 ネットワーク構成に応じた運用と環境構築

ネットワーク構成 (JP1/IM - Manager のホストが複数のネットワークに接続された構成, およびファイアウォールを経由した構成) に応じた運用と環境構築について説明しています。

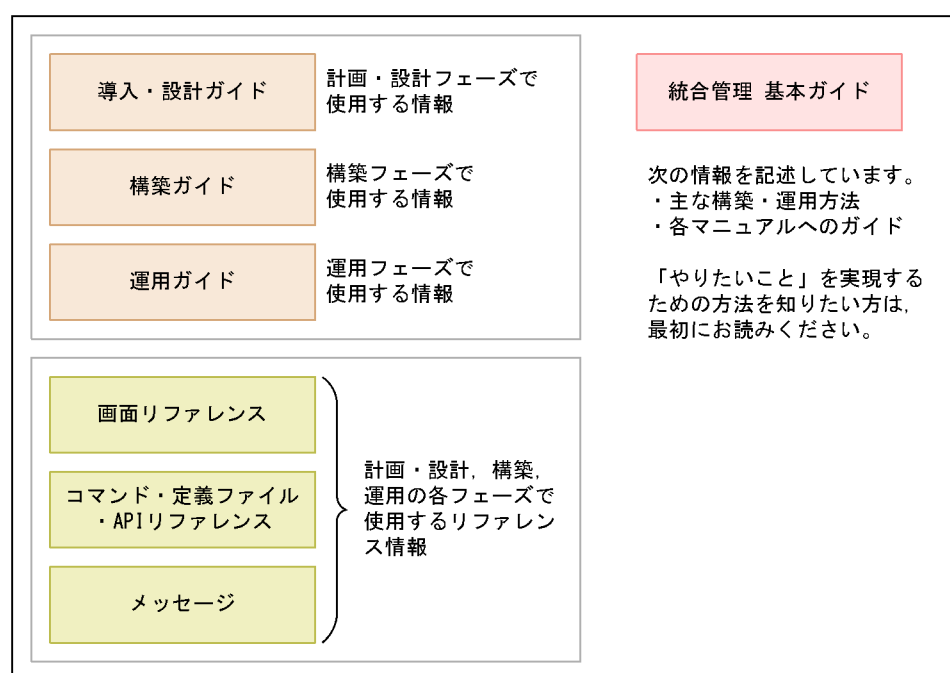
第10章 ほかの JP1 製品と連携するための設定

JP1/IM とほかの JP1 製品 (JP1/Service Support, JP1/Navigation Platform, JP1/AJS, および JP1/PFM) を連携する場合の環境設定について説明しています。

■ マニュアルの体系

JP1/IM のマニュアルでは, システムの設計・構築・運用などのシステムのライフサイクルでの段階ごとに必要な情報を説明しています。目的に合わせて必要なマニュアルをお読みください。

JP1/IM のマニュアルとシステムのライフサイクルの関係を次の図に示します。



■ このマニュアルで使用する記号

このマニュアルで使用する記号を次に示します。

記号	意味
[]	メニュー項目、画面名、ボタン名、およびキーボードのキーなどを示す。 例 メニュー項目：[新規作成] 画面名：[ログイン] 画面 ボタン名：[OK] ボタン キーボードのキー：[Ctrl] キー
[] - []	画面のメニューから項目を選択する操作を示す。 例 [ファイル] - [新規作成] を選択する。 上記の例では、メニューバーの [ファイル] を選んで、プルダウンメニューの [新規作成] を選択することを示す。

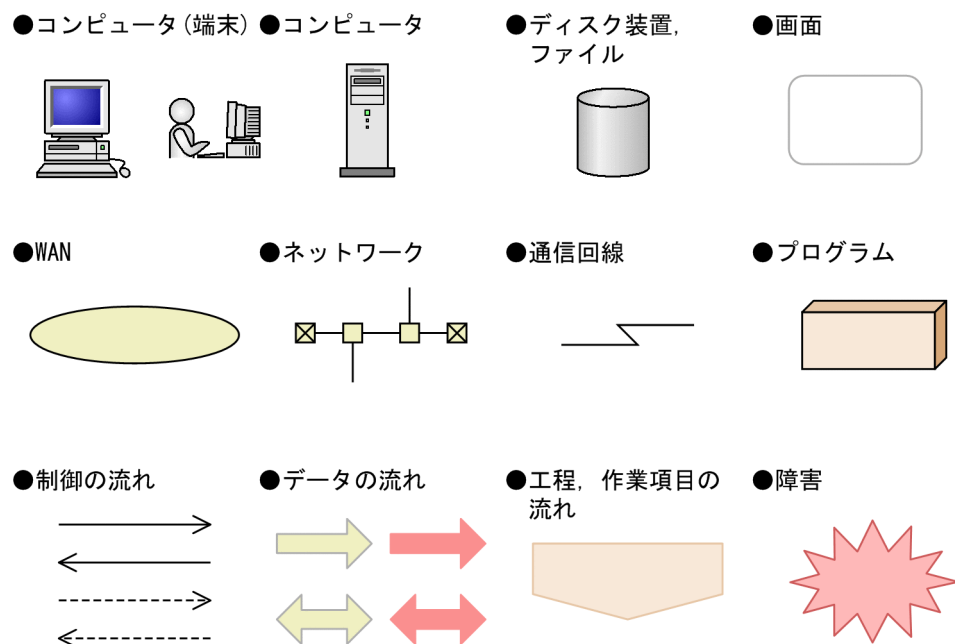
■ コマンドの文法で使用する記号

コマンドとパラメーターの説明で使用する記号を、次のように定義します。

記号	意味
 (ストローク)	複数の項目に対し、項目間の区切りを示し、「または」の意味を示す。 例 「A B C」は、「A, B または C」を示す。
{ }	この記号で囲まれている複数の項目の中から、必ず一つの項目を選択する。項目の区切りは で示す。 例 {A B C} は「A, B または C のどれかを指定する」ことを示す。
[]	この記号で囲まれている項目は任意に指定できる（省略してもよい）。 複数の項目が記述されている場合には、すべてを省略するか、どれか一つを選択する。 例 [A]は「何も指定しない」か「A を指定する」ことを示す。 [B C]は「何も指定しない」か「B または C を指定する」ことを示す。
△	空白を表す。 △ ₀ ：0 個以上の空白（空白を省略できる） △ ₁ ：1 個以上の空白（空白を省略できない）
▲	タブを表す。 例 ▲A とした場合に、A の前にタブがあることを示す。

■ 図中で使用する記号

このマニュアルの図中で使用する記号を、次のように定義します。



■ Windows 版 JP1/IM, JP1/Base のインストール先フォルダの表記

このマニュアルでは、Windows 版 JP1/IM, JP1/Base のインストール先フォルダを次のように表記しています。

製品名	インストール先フォルダの表記	デフォルトインストール先フォルダ※
JP1/IM - View	View パス	システムドライブ:¥Program Files¥Hitachi¥JP1CoView
JP1/IM - Manager	Manager パス	システムドライブ:¥Program Files¥Hitachi¥JP1IMM
	Console パス	システムドライブ:¥Program Files¥Hitachi¥JP1Cons
	Scope パス	システムドライブ:¥Program Files¥Hitachi¥JP1Scope
JP1/IM - Agent	Agent パス	システムドライブ:¥Program Files¥Hitachi¥jp1ima
JP1/Base	Base パス	システムドライブ:¥Program Files¥Hitachi¥JP1Base

注※ 各製品をデフォルトのままインストールした場合のインストール先フォルダを表しています。「システムドライブ:¥Program Files」と表記している部分は、インストール時の OS 環境変数によって決定されるため、環境によって異なる場合があります。

■ このマニュアルで使用する「Administrators 権限」について

このマニュアルで表記している「Administrators 権限」とは、ローカル PC に対する Administrators 権限です。ローカル PC に対して Administrators 権限を持つユーザーであれば、ローカルユーザー、ドメインユーザーおよび、Active Directory 環境で動作に違いはありません。

■ オンラインマニュアルについて

JP1/IM では、Web ブラウザーで参照できる HTML マニュアルを提供しています。

オンラインマニュアルの内容は、このマニュアルと同様です。

オンラインマニュアルは、次の操作で目次が表示されます。

- JP1/IM - View：[ヘルプ]－[目次]を選択する。
- 統合オペレーション・ビューアー：[ヘルプ]－[オンラインマニュアル]を選択する。

注意事項

- スタートメニューからオンラインマニュアルを表示させると、OS の設定によってすでに表示されているブラウザの画面上に HTML マニュアルが表示されることがあります。

■ 統合トレースログの出力先について

JP1/IM 12-10 から、JP1/IM - Manager の 32 ビット Java プロセスを、すべて 64 ビット Java プロセスに変更しました。このため、JP1/IM の各機能の Java プロセス機能が出力する統合トレースログの出力先が変更となります。

バージョン 12-10 以降の JP1/IM の各機能の統合トレースログの出力先を次に示します。ログファイルトラップ機能を使用している場合、出力先の変更に応じて設定変更が必要です。

統合トレースログの出力先（32 ビット）：システムドライブ¥Program
Files(x86)¥Hitachi¥HNTRLib2¥spool

- IM データベース
- セントラルスコープサービス
- プロセス管理
- コマンド実行
- 自動アクション
- インストールおよびセットアップ

統合トレースログの出力先（64 ビット）：システムドライブ¥Program Files¥Hitachi¥HNTRLib2¥spool

- イベント基盤サービス
- セントラルコンソール・ビューアー
- セントラルスコープ・ビューアー
- 相関イベント発行サービス
- IM 構成管理
- IM 構成管理・ビューアー
- インテリジェント統合管理基盤

目次

前書き	2
変更内容	10
はじめに	11

1	インストールとセットアップ (Windows の場合)	29
1.1	インストールとセットアップの流れ (Windows の場合)	30
1.2	インストール前に必要な作業 (Windows の場合)	33
1.2.1	JP1/IM のセットアップ内容の設計 (Windows の場合)	33
1.2.2	システム環境の構築 (Windows の場合)	33
1.2.3	前提プログラムのインストール (Windows の場合)	34
1.3	インストール (Windows の場合)	35
1.3.1	インストール手順 (Windows の場合)	35
1.3.2	インストール直後に必要な設定 (Windows の場合)	48
1.3.3	インストール時の注意事項 (Windows の場合)	49
1.3.4	インストール時の資料採取方法 (Windows の場合)	55
1.3.5	オートスケール機能と連携する方法 (Windows の場合)	56
1.3.6	仮想マシンのクローン作成 (Windows の場合)	57
1.4	IM データベースの構築 (Windows の場合)	59
1.4.1	IM データベースを構築するための準備 (Windows の場合)	59
1.4.2	統合監視 DB の設定 (Windows の場合)	60
1.4.3	IM 構成管理 DB の設定 (Windows の場合)	62
1.4.4	IM 構成管理の機能を使用するための設定 (Windows の場合)	64
1.4.5	IM データベースの更新 (Windows の場合)	64
1.5	インテリジェント統合管理データベースの構築 (Windows の場合)	66
1.5.1	インテリジェント統合管理データベースを構築するための準備 (Windows の場合)	66
1.5.2	インテリジェント統合管理データベースの設定 (Windows の場合)	66
1.5.3	セキュリティ製品の除外設定 (Windows の場合)	67
1.6	サービスの起動順序の設定 (Windows の場合)	68
1.7	ユーザー認証の設定およびユーザーマッピングの設定 (Windows の場合)	69
1.7.1	認証サーバの指定 (Windows の場合)	70
1.7.2	JP1 ユーザーの登録 (Windows の場合)	70
1.7.3	JP1 ユーザーの操作権限の設定 (Windows の場合)	70
1.7.4	プライマリー認証サーバの設定情報のコピー (Windows の場合)	70
1.7.5	ユーザーマッピングの設定 (Windows の場合)	71
1.8	JP1/Base の障害に備えた設定 (Windows の場合)	72

1.9	IM 構成管理を使用する場合のシステムの階層構成の設定 (Windows の場合)	73
1.9.1	IM 構成管理・ビューアーによる設定 (Windows の場合)	73
1.9.2	エクスポート・インポート機能による設定 (Windows の場合)	76
1.9.3	仮想化システム構成の管理および監視のための設定 (Windows の場合)	76
1.10	IM 構成管理を使用しない場合のシステムの階層構成の設定 (Windows の場合)	77
1.10.1	構成定義情報の設定 (Windows の場合)	77
1.10.2	構成定義情報の削除 (Windows の場合)	78
1.10.3	構成定義情報の変更 (Windows の場合)	78
1.10.4	構成定義情報の設定での注意事項 (Windows の場合)	78
1.11	イベントサービス機能の設定 (Windows の場合)	80
1.12	IM 構成管理を使用する場合の JP1 イベントの転送設定 (Windows の場合)	81
1.13	IM 構成管理を使用しない場合の JP1 イベントの転送設定 (Windows の場合)	82
1.14	IM 構成管理を使用する場合のイベントサービスの定義情報の収集と配布 (Windows の場合)	83
1.15	IM 構成管理を使用しない場合のイベントサービスの定義情報の収集と配布 (Windows の場合)	84
1.16	コマンド実行環境の設定 (Windows の場合)	85
1.16.1	管理対象ホストのコマンド実行機能の設定 (Windows の場合)	85
1.16.2	クライアントアプリケーションの実行環境の設定 (Windows の場合)	86
1.17	イベントサービスの登録ホスト名を FQDN 形式で利用する場合の設定 (Windows の場合)	87
1.17.1	前提条件 (Windows の場合)	87
1.17.2	設定方法 (Windows の場合)	87
1.17.3	起動方法 (Windows の場合)	88
1.18	リモートの監視対象ホストでログ監視をするための設定 (Windows の場合)	89
1.18.1	WMI の設定 (Windows の場合)	89
1.18.2	NetBIOS (NetBIOS over TCP/IP) の設定 (Windows の場合)	96
1.18.3	SSH の設定 (Windows の場合)	98
1.18.4	1 回の監視間隔で収集できるログのサイズの設定 (Windows の場合)	105
1.19	JP1/IM - Manager のセットアップ (Windows の場合)	106
1.19.1	JP1/IM - Manager の設定ファイルの編集について (Windows の場合)	106
1.19.2	インテリジェント統合管理基盤の機能を使用するための設定 (Windows の場合)	107
1.19.3	エージェントとして JP1/IM - Agent を使用する場合の設定	108
1.19.4	JP1/IM - Agent パッケージの登録 (Windows の場合)	121
1.19.5	セントラルスコープの機能を使用するための設定 (Windows の場合)	122
1.19.6	JP1/IM - Manager の障害に備えた設定 (Windows の場合)	123
1.19.7	バージョンアップ時の設定 (Windows の場合)	127
1.20	JP1/IM - View のセットアップ (Windows の場合)	132
1.20.1	JP1/IM - View の障害に備えた設定 (Windows の場合)	132
1.20.2	JP1/IM - View (セントラルコンソール・ビューアーおよびセントラルスコープ・ビューアー) の動作カスタマイズ (Windows の場合)	132
1.20.3	IM 構成管理・ビューアーのセットアップおよび動作カスタマイズ (Windows の場合)	133

1.21	JP1/IM - Agent のセットアップ (Windows の場合)	136
1.21.1	JP1/IM - Agent のサービスの設定	136
1.21.2	JP1/IM - Agent の設定	140
1.22	JP1/IM - Agent のコンテナ環境の構築 (Windows の場合)	230
1.22.1	コンテナイメージの作成	230
1.22.2	JP1/IM - Agent のバージョンアップ	237
1.23	JP1/IM - Agent のオプション機能の構築 (Windows の場合)	239
1.23.1	OracleDB exporter の設定	239
1.23.2	Node exporter for AIX の設定	255
1.23.3	SAP システム監視の設定	269
1.23.4	SQL exporter の設定	274
1.24	マニュアルの組み込み手順 (Windows の場合)	286
1.25	アンインストール (Windows の場合)	288
1.25.1	アンインストール手順 (Windows の場合)	288
1.25.2	アンインストール時の注意事項 (Windows の場合)	292
1.26	インストールとセットアップの注意事項 (Windows の場合)	297
2	インストールとセットアップ (UNIX の場合)	299
2.1	インストールとセットアップの流れ (UNIX の場合)	300
2.2	インストール前に必要な作業 (UNIX の場合)	302
2.2.1	JP1/IM のセットアップ内容の設計 (UNIX の場合)	302
2.2.2	システム環境の構築 (UNIX の場合)	302
2.2.3	前提プログラムのインストール (UNIX の場合)	302
2.3	インストール (UNIX の場合)	304
2.3.1	インストール手順 (UNIX の場合)	304
2.3.2	Hitachi PP Installer の使用方法 (UNIX の場合)	308
2.3.3	インストール直後に必要な設定 (UNIX の場合)	310
2.3.4	インストール時の注意事項 (UNIX の場合)	313
2.3.5	インストール時の資料採取方法 (UNIX の場合)	316
2.3.6	オートスケール機能と連携する方法 (UNIX の場合)	316
2.3.7	仮想マシンのクローン作成 (UNIX の場合)	317
2.4	IM データベースの構築 (UNIX の場合)	320
2.4.1	IM データベースを構築するための準備 (UNIX の場合)	320
2.4.2	統合監視 DB の設定 (UNIX の場合)	321
2.4.3	IM 構成管理 DB の設定 (UNIX の場合)	323
2.4.4	IM 構成管理の機能を使用するための設定 (UNIX の場合)	324
2.4.5	IM データベースの更新 (UNIX の場合)	325
2.5	インテリジェント統合管理データベースの構築 (UNIX の場合)	327
2.5.1	インテリジェント統合管理データベースを構築するための準備 (UNIX の場合)	327

2.5.2	インテリジェント統合管理データベースの設定 (UNIX の場合)	327
2.5.3	セキュリティ製品の除外設定 (UNIX の場合)	328
2.6	ユーザー認証の設定およびユーザーマッピングの設定 (UNIX の場合)	329
2.6.1	認証サーバの指定 (UNIX の場合)	330
2.6.2	JP1 ユーザーの登録 (UNIX の場合)	330
2.6.3	JP1 ユーザーの操作権限の設定 (UNIX の場合)	330
2.6.4	プライマリー認証サーバの設定情報のコピー (UNIX の場合)	331
2.6.5	ユーザーマッピングの設定 (UNIX の場合)	331
2.7	JP1/Base の障害に備えた設定 (UNIX の場合)	332
2.8	IM 構成管理を使用する場合のシステムの階層構成の設定 (UNIX の場合)	333
2.8.1	IM 構成管理・ビューアーによるシステム構成の設定 (UNIX の場合)	333
2.8.2	エクスポート・インポート機能によるシステム構成の設定 (UNIX の場合)	335
2.8.3	仮想化システム構成の管理および監視のための設定 (UNIX の場合)	336
2.9	IM 構成管理を使用しない場合のシステムの階層構成の設定 (UNIX の場合)	337
2.9.1	構成定義情報の設定 (UNIX の場合)	337
2.9.2	構成定義情報の削除 (UNIX の場合)	338
2.9.3	構成定義情報の変更 (UNIX の場合)	338
2.9.4	構成定義情報の設定での注意事項 (UNIX の場合)	338
2.10	イベントサービス機能の設定 (UNIX の場合)	340
2.11	IM 構成管理を使用する場合の JP1 イベントの転送設定 (UNIX の場合)	341
2.12	IM 構成管理を使用しない場合の JP1 イベントの転送設定 (UNIX の場合)	342
2.13	IM 構成管理を使用する場合のイベントサービスの定義情報の収集と配布 (UNIX の場合)	343
2.14	IM 構成管理を使用しない場合のイベントサービスの定義情報の収集と配布 (UNIX の場合)	344
2.15	コマンド実行環境の設定 (UNIX の場合)	345
2.15.1	管理対象ホストのコマンド実行機能の設定 (UNIX の場合)	345
2.15.2	クライアントアプリケーションの実行環境の設定 (UNIX の場合)	346
2.16	イベントサービスの登録ホスト名を FQDN 形式で利用する場合の設定 (UNIX の場合)	347
2.16.1	前提条件 (UNIX の場合)	347
2.16.2	設定方法 (UNIX の場合)	347
2.16.3	起動方法 (UNIX の場合)	348
2.17	リモートの監視対象ホストでログ監視をするための設定 (UNIX の場合)	349
2.17.1	SSH の設定 (UNIX の場合)	349
2.17.2	1 回の監視間隔で収集できるログのサイズの設定 (UNIX の場合)	356
2.18	JP1/IM - Manager のセットアップ (UNIX の場合)	357
2.18.1	セットアッププログラムの実行 (UNIX の場合)	357
2.18.2	自動起動および自動終了の設定 (UNIX の場合)	357
2.18.3	JP1/IM - Manager の設定ファイルの編集について (UNIX の場合)	359
2.18.4	インテリジェント統合管理基盤の機能を使用するための設定 (UNIX の場合)	359
2.18.5	エージェントとして JP1/IM - Agent を使用する場合の設定	360

2.18.6	JP1/IM - Agent パッケージの登録 (UNIX の場合)	361
2.18.7	セントラルスコープの機能を使用するための設定 (UNIX の場合)	363
2.18.8	SELinux に関する設定 (UNIX の場合)	363
2.18.9	システムログ (syslog) に出力するメッセージの抑止	367
2.18.10	JP1/IM - Manager の障害に備えた設定 (UNIX の場合)	368
2.18.11	バージョンアップ時の設定 (UNIX の場合)	374
2.19	JP1/IM - Agent のセットアップ (UNIX の場合)	380
2.19.1	JP1/IM - Agent のサービスの設定	380
2.19.2	JP1/IM - Agent の設定	384
2.20	JP1/IM - Agent のコンテナ環境の構築 (UNIX の場合)	403
2.21	JP1/IM - Agent のオプション機能の構築 (UNIX の場合)	404
2.21.1	OracleDB exporter の設定	404
2.21.2	Node exporter for AIX の設定	409
2.21.3	SAP システム監視の設定	409
2.22	マニュアルの組み込み手順 (UNIX の場合)	410
2.23	アンインストール (UNIX の場合)	411
2.23.1	アンインストール手順 (UNIX の場合)	411
2.23.2	アンインストール時の注意事項 (UNIX の場合)	415
2.24	インストールとセットアップの注意事項 (UNIX の場合)	421

3 IM 構成管理によるシステムの階層構成の設定 423

3.1	ホストの登録	424
3.1.1	ホストを登録する	424
3.1.2	リモートの監視対象ホストを登録する	425
3.1.3	ホストから情報を収集する	427
3.1.4	ホスト情報を表示する	428
3.1.5	ホスト情報の属性を変更する	428
3.1.6	ホストを削除する	429
3.2	システムの階層構成の設定	431
3.2.1	システムの階層構成を取得する	431
3.2.2	システムの階層構成を表示する	432
3.2.3	システムの階層構成を検証する	432
3.2.4	システムの階層構成を編集する	433
3.2.5	システムの階層構成の同期を取る	440
3.3	仮想化システム構成の設定	441
3.3.1	IM 構成管理で仮想化構成を管理する	441
3.3.2	仮想化システムの構成情報を収集する	457
3.3.3	セントラルスコープで仮想化構成を監視するために監視ツリーを設定する	459
3.3.4	仮想化構成収集を行う場合の注意事項	461

3.4	業務グループの設定	463
3.4.1	業務グループを新規に構築する	464
3.4.2	業務グループにホストを追加する	471
3.4.3	業務グループからホストを削除する	471
3.4.4	セントラルスコープで業務グループを監視する	471
3.5	プロファイルの設定	474
3.5.1	エージェント構成のホストにプロファイルを設定する	474
3.5.2	リモート監視構成のホストにプロファイルを設定する	489
3.6	IM 構成管理の管理情報のインポート・エクスポート	500
4	インテリジェント統合管理基盤の設定	501
4.1	インテリジェント統合管理基盤の環境設定の概要	502
4.1.1	インテリジェント統合管理基盤の環境設定を始める前に	502
4.2	システム構成情報を設定する	503
4.3	インテリジェント統合管理基盤で暗号化機能を使用する場合の設定	506
4.4	インテリジェント統合管理基盤のクラスタ環境を構築する	507
4.5	カスタム UI 表示機能を使用する場合の設定	508
4.6	繰り返しイベントの表示抑止機能の互換設定	510
4.7	関連性の定義の設定	511
4.8	業務影響アイコンの設定	512
4.9	連携製品のモニター起動の設定	514
4.10	システムの状況に応じた対処アクションの提案機能の設定	515
4.11	OpenID プロバイダとシングルサインオン連携するための設定（外部製品との連携）	516
4.11.1	OpenID プロバイダとシングルサインオン連携する	516
4.11.2	シングルサインオンマッピング定義ファイル（imdd_sso_mapping.properties）のリロード手順	518
4.11.3	OpenID プロバイダとの連携解除手順	518
4.12	ダイレクトアクセス URL の設定	520
4.12.1	ダイレクトアクセス URL	520
4.12.2	ノード選択のダイレクトアクセス URL 取得	522
4.12.3	OpenID 認証ダイレクトアクセス URL	523
4.12.4	ダイレクトアクセス URL の指定例	524
4.13	システム構成情報反映方式の設定	528
4.14	IM 管理ノードリンク定義ファイルの移行手順	529
4.15	統合オペレーション・ビューアーを使用するための Web ブラウザーの設定手順	530
4.16	ダッシュボードの設定	531
4.16.1	自動生成ダッシュボードをカスタマイズする	531
4.16.2	ダッシュボードを新規に作成する	531
4.16.3	ダッシュボードを編集する	532
4.16.4	[ダッシュボード] 画面を共有する	532

4.16.5 ダッシュボードを削除する 532

5 セントラルコンソールの設定 534

- 5.1 JP1/IM のイベント取得時の動作設定 535
 - 5.1.1 ログイン時のイベント取得範囲を指定してイベントを表示する 536
- 5.2 JP1 イベントのフィルタリングの設定 538
 - 5.2.1 表示フィルターを設定する 538
 - 5.2.2 ユーザーフィルターを設定する 541
 - 5.2.3 重要イベントフィルターを設定する 543
 - 5.2.4 イベント取得フィルターを設定する 545
- 5.3 繰り返しイベントの監視抑止の設定 553
- 5.4 JP1 イベントの表示色の設定 554
- 5.5 自動アクションの設定 555
 - 5.5.1 自動アクション機能の実行環境の設定 555
 - 5.5.2 自動アクションの実行条件および実行内容の設定 556
 - 5.5.3 自動アクションの実行状況監視の設定 557
 - 5.5.4 自動アクションの実行抑止の設定 558
 - 5.5.5 メール送信の設定 559
- 5.6 関連イベント発行の設定 563
 - 5.6.1 関連イベント発行機能の起動設定 563
 - 5.6.2 関連イベント発行履歴ファイルのサイズおよび面数の設定 563
 - 5.6.3 関連イベント発行機能の起動オプションの設定 564
 - 5.6.4 関連イベント発行定義の作成および反映 565
- 5.7 メモ情報の設定 567
- 5.8 イベントガイド情報の編集 568
 - 5.8.1 イベントガイド情報の編集の手順 568
- 5.9 対処状況変更時の JP1 イベント発行の設定 571
- 5.10 固有の属性付加の設定 572
- 5.11 固有の拡張属性の表示および指定の設定 573
- 5.12 ユーザー独自のイベント属性（拡張属性の固有情報）を表示する手順 575
 - 5.12.1 定義ファイルを作成する 577
 - 5.12.2 定義ファイルを有効にする 580
- 5.13 重大度変更機能の設定 581
 - 5.13.1 [重大度変更定義設定] 画面から設定する手順 581
 - 5.13.2 重大度変更定義ファイルから設定する手順 583
- 5.14 表示メッセージ変更機能の設定 584
 - 5.14.1 [表示メッセージ変更定義設定] 画面から設定する手順 584
 - 5.14.2 表示メッセージ変更定義ファイルから設定する手順 586
 - 5.14.3 表示メッセージ変更後のイベントを発行する手順 587

- 5.15 発生元ホストのマッピングの設定 588
- 5.16 ログインユーザーごとの JP1/IM - View の設定 592
 - 5.16.1 JP1/IM - View の設定項目 592
 - 5.16.2 JP1/IM - View の設定手順 593
- 5.17 連携製品のモニター起動の設定 595
 - 5.17.1 モニター画面を呼び出す手順 595
 - 5.17.2 モニター画面呼び出しをするための画面の決定 596
 - 5.17.3 定義ファイルの作成 596
- 5.18 統合機能メニューの設定 598
 - 5.18.1 統合機能メニューから連携製品の GUI を起動するための設定 598
 - 5.18.2 新規メニューを追加する手順 599
 - 5.18.3 [統合機能メニュー] 画面から起動する画面の決定 599
 - 5.18.4 定義ファイルの作成 600
 - 5.18.5 統合機能メニューから連携製品の WWW ページを起動するための設定 603
- 5.19 業務グループの参照・操作制限の設定 604

6 セントラルスコープの設定 606

- 6.1 セントラルスコープの環境設定の概要 607
 - 6.1.1 セントラルスコープの環境設定を始める前に 607
- 6.2 ホスト情報の登録 608
- 6.3 監視ツリーを GUI で作成する 609
 - 6.3.1 監視ツリーの編集画面の起動 609
 - 6.3.2 既存の監視ツリーの取得 611
 - 6.3.3 監視ツリーの自動生成 612
 - 6.3.4 監視ツリーのカスタマイズ 614
 - 6.3.5 カスタマイズした監視ツリーのローカルホストへの保存 624
 - 6.3.6 カスタマイズした監視ツリーのマネージャーへの反映 624
- 6.4 [ビジュアル監視] 画面を GUI で作成する 626
 - 6.4.1 [ビジュアル監視] 画面の編集画面の起動 626
 - 6.4.2 既存の [ビジュアル監視] 画面の取得 627
 - 6.4.3 [ビジュアル監視] 画面のカスタマイズ 627
 - 6.4.4 カスタマイズした [ビジュアル監視] 画面のローカルホストへの保存 631
 - 6.4.5 カスタマイズした [ビジュアル監視] 画面のマネージャーへの反映 632
 - 6.4.6 [ビジュアル監視] 画面の一覧の編集および削除 633
- 6.5 保存した CSV ファイルを編集して [監視ツリー] 画面を作成 634
- 6.6 ガイド情報の編集 635
 - 6.6.1 ガイド情報の編集の手順 635
- 6.7 セントラルスコープの動作環境の設定 638
 - 6.7.1 状態変更イベント件数の上限監視の設定 638

6.7.2	対処済み連動機能の設定	638
6.7.3	JP1 イベントの対処済み時に状態変更イベントを自動で削除するための設定	639
6.7.4	JP1 イベント受信時に監視オブジェクトを初期化するための設定	640
6.7.5	状態変更条件メモリー常駐機能の設定	640
6.7.6	【監視ツリー】画面のツールバーのカスタマイズ	641
6.7.7	監視ノード名および監視ノードアイコン余白の表示を抑止するための設定	641
6.7.8	監視ノード名の状態色および監視ノードの状態色の設定	643
6.7.9	監視ノードのアイコンの移動を抑止するための設定	644
6.8	連携製品のセットアップ	646
6.8.1	JP1/AJS との連携でのセットアップ	646
6.8.2	JP1/Cm2/SSO との連携でのセットアップ	647
6.8.3	JP1/PFM との連携でのセットアップ	650
6.8.4	JP1/Cm2/NNM との連携でのセットアップ	651
6.8.5	JP1/NETM/DM との連携でのセットアップ	653
6.8.6	JP1/PAM との連携でのセットアップ	653
6.8.7	Cosminexus との連携でのセットアップ	654
6.8.8	HiRDB との連携でのセットアップ	655
6.8.9	JP1/ServerConductor との連携でのセットアップ	655
6.9	監視オブジェクト作成例	656
6.9.1	システム監視オブジェクトの作成例 (JP1/AJS のジョブネット監視)	656
6.9.2	汎用監視オブジェクトの作成例 (JP1/Cm2/SSO による CPU 監視)	657
6.9.3	汎用監視オブジェクトの作成例 (HiRDB の監視)	662
6.9.4	汎用監視オブジェクトの作成例 (JP1/Cm2/SSO による Cosminexus 業務のリソース監視)	668

7 クラスタシステムでの運用と環境構築 (Windows の場合) 674

7.1	クラスタ運用の概要 (Windows の場合)	675
7.1.1	クラスタシステムの概要 (Windows の場合)	676
7.1.2	クラスタ運用の前提条件 (Windows の場合)	677
7.1.3	クラスタシステムでの JP1/IM の構成 (Windows の場合)	680
7.2	クラスタ運用の環境設定の流れ (Windows の場合)	684
7.3	論理ホストの新規インストール・セットアップ (Windows の場合)	686
7.3.1	JP1/Base および JP1/IM - Manager の新規インストール (Windows の場合)	686
7.3.2	JP1/IM - Manager の新規インストール時の物理ホスト環境のセットアップ (Windows の場合)	687
7.3.3	JP1/IM - Manager の新規インストール時の論理ホスト環境 (実行系) のセットアップ (Windows の場合)	687
7.3.4	JP1/IM - Manager の新規インストール時の共通定義情報のコピー (Windows の場合)	695
7.3.5	JP1/IM - Manager の新規インストール時の論理ホスト環境 (待機系) のセットアップ (Windows の場合)	696
7.3.6	統合エージェントホストでの JP1/IM - Agent の新規インストール (Windows の場合)	701

7.3.7	統合エージェントホストでの JP1/IM - Agent の新規インストール時のセットアップ (Windows の場合)	702
7.4	インテリジェント統合管理基盤のクラスタ環境を構築する (Windows の場合)	708
7.4.1	クラスタ環境を新規構築する (Windows の場合)	708
7.4.2	修正版を適用したクラスタ環境を構築する (Windows の場合)	710
7.4.3	バージョンアップしてクラスタ環境を構築する (Windows の場合)	711
7.5	新規インストール・セットアップでのクラスタソフトへの登録 (Windows の場合)	714
7.5.1	クラスタソフトへの登録 (Windows の場合)	716
7.5.2	リソースの起動停止順序の設定 (Windows の場合)	717
7.5.3	クラスタソフトのパラメーターの設定 (Windows の場合)	717
7.6	論理ホストのバージョンアップインストール・セットアップ (Windows の場合)	718
7.6.1	JP1/Base および JP1/IM - Manager のバージョンアップインストール (Windows の場合)	718
7.6.2	JP1/IM - Agent のバージョンアップインストール (Windows の場合)	719
7.6.3	バージョンアップインストール時の物理ホスト環境のセットアップ (Windows の場合)	721
7.6.4	バージョンアップインストール時の論理ホスト環境 (実行系) のセットアップ (Windows の場合)	721
7.6.5	バージョンアップインストール時の共通定義情報のコピー (Windows の場合)	722
7.7	論理ホストのアンインストール (Windows の場合)	723
7.7.1	論理ホストの削除 (Windows の場合)	723
7.7.2	JP1/IM - Manager および JP1/Base のアンインストール (Windows の場合)	726
7.7.3	JP1/IM - Agent のアンインストール (Windows の場合)	726
7.8	設定変更時の作業 (Windows の場合)	728
7.8.1	ファイルでの設定変更 (Windows の場合)	728
7.8.2	コマンドでの設定変更 (Windows の場合)	729
7.8.3	クラスタ環境での IM データベースの更新 (Windows の場合)	729
7.9	クラスタ運用時の注意事項 (Windows の場合)	733
7.10	非クラスタシステムでの論理ホストの運用と環境構築 (Windows の場合)	735
7.10.1	非クラスタシステムで論理ホストを運用する場合の構成の検討 (Windows の場合)	735
7.10.2	非クラスタシステムで論理ホストを運用する場合の環境設定 (Windows の場合)	735
7.10.3	非クラスタシステムで論理ホストを運用する場合の注意事項 (Windows の場合)	736
8	クラスタシステムでの運用と環境構築 (UNIX の場合)	737
8.1	クラスタ運用の概要 (UNIX の場合)	738
8.1.1	クラスタシステムの概要 (UNIX の場合)	738
8.1.2	クラスタ運用の前提条件 (UNIX の場合)	738
8.1.3	クラスタシステムでの JP1/IM の構成 (UNIX の場合)	738
8.2	クラスタ運用の環境設定の流れ (UNIX の場合)	742
8.3	論理ホストの新規インストール・セットアップ (UNIX の場合)	744
8.3.1	JP1/Base および JP1/IM - Manager の新規インストール (UNIX の場合)	744
8.3.2	JP1/IM - Manager の新規インストール時の物理ホスト環境のセットアップ (UNIX の場合)	745

8.3.3	JP1/IM - Manager の新規インストール時の論理ホスト環境（実行系）のセットアップ（UNIX の場合）	745
8.3.4	JP1/IM - Manager の新規インストール時の共通定義情報のコピー（UNIX の場合）	752
8.3.5	JP1/IM - Manager の新規インストール時の論理ホスト環境（待機系）のセットアップ（UNIX の場合）	752
8.3.6	統合エージェントホストでの JP1/IM - Agent の新規インストール（UNIX の場合）	756
8.3.7	統合エージェントホストでの JP1/IM - Agent の新規インストール時のセットアップ（UNIX の場合）	758
8.4	インテリジェント統合管理基盤のクラスタ環境を構築する（UNIX の場合）	763
8.4.1	クラスタ環境を新規構築する（UNIX の場合）	763
8.4.2	修正版を適用したクラスタ環境を構築する（UNIX の場合）	765
8.4.3	バージョンアップしてクラスタ環境を構築する（UNIX の場合）	765
8.5	新規インストール・セットアップでのクラスタソフトへの登録（UNIX の場合）	768
8.5.1	クラスタソフトに登録するスクリプトの作成（UNIX の場合）	769
8.5.2	リソースの起動停止順序の設定（UNIX の場合）	772
8.5.3	クラスタソフトのパラメーターの設定（Linux の場合）	772
8.6	論理ホストのバージョンアップインストール・セットアップ（UNIX の場合）	773
8.6.1	JP1/Base および JP1/IM - Manager のバージョンアップインストール（UNIX の場合）	773
8.6.2	JP1/IM - Agent のバージョンアップインストール（UNIX の場合）	774
8.6.3	バージョンアップインストール時の物理ホスト環境のセットアップ（UNIX の場合）	776
8.6.4	バージョンアップインストール時の論理ホスト環境（実行系）のセットアップ（UNIX の場合）	776
8.6.5	バージョンアップインストール時の共通定義情報のコピー（UNIX の場合）	777
8.7	論理ホストのアンインストール（UNIX の場合）	778
8.7.1	論理ホストの削除（UNIX の場合）	778
8.7.2	JP1/IM - Manager および JP1/Base のアンインストール（UNIX の場合）	780
8.7.3	JP1/IM - Agent のアンインストール（UNIX の場合）	781
8.8	設定変更時の作業（UNIX の場合）	782
8.8.1	ファイルでの設定変更（UNIX の場合）	782
8.8.2	コマンドでの設定変更（UNIX の場合）	783
8.8.3	クラスタ環境での IM データベースの更新（UNIX の場合）	783
8.9	クラスタ運用時の注意事項（UNIX の場合）	786
8.10	非クラスタシステムでの論理ホストの運用と環境構築（UNIX の場合）	788
8.10.1	非クラスタシステムで論理ホストを運用する場合の構成の検討（UNIX の場合）	788
8.10.2	非クラスタシステムで論理ホストを運用する場合の環境設定（UNIX の場合）	788
8.10.3	非クラスタシステムで論理ホストを運用する場合の注意事項（UNIX の場合）	789
9	ネットワーク構成に応じた運用と環境構築	790
9.1	JP1/Base による通信の制御	791
9.2	複数ネットワークでの運用	792
9.2.1	構成例 1（クラスタ運用なし、JP1/IM - View 接続）	792

9.2.2	構成例 2 (クラスタ運用なし, コマンド実行)	793
9.2.3	構成例 3 (クラスタ運用, JP1/IM - View 接続)	794
9.2.4	構成例 4 (クラスタ運用, コマンド実行)	795
9.3	ファイアウォール環境での運用	797
9.3.1	ファイアウォールの基礎知識	797
9.3.2	JP1/IM の通信	803
9.3.3	Windows ファイアウォールの注意事項	809
9.4	暗号化通信の構築	811
9.4.1	新規に通信暗号化機能を使用する	811
9.4.2	設定済みの証明書を変更する	816
9.4.3	通信暗号化機能の使用を中止する	818
9.4.4	JP1/IM - Manager の設定	820
9.4.5	JP1/IM - Agent (統合エージェント制御基盤) の設定	821
9.4.6	通信暗号化機能が正しく設定できているか確認する	822

10 **ほかの JP1 製品と連携するための設定 824**

10.1	JP1/Service Support と連携する	825
10.1.1	JP1/Service Support 画面呼び出し設定	825
10.2	JP1/Navigation Platform と連携する	826
10.3	JP1/AJS と連携する	827
10.3.1	モニター起動で JP1/AJS の画面を起動するための設定	827
10.3.2	[統合機能メニュー] 画面から JP1/AJS の画面を起動するための設定	827
10.3.3	イベントガイド情報からモニター画面を表示するための設定	827
10.3.4	自動アクションの送信メールからモニター画面を表示するための設定	827
10.3.5	インテリジェント統合管理基盤でルートジョブネットの関連や構成情報を確認するための設定	827
10.4	JP1/PFM と連携する	829
10.4.1	モニター起動で JP1/PFM の画面を起動するための設定	829
10.4.2	[統合機能メニュー] 画面から JP1/PFM の画面を起動するための設定	829
10.4.3	事象発生元ホストの性能レポートを表示する場合の設定	829
10.4.4	インテリジェント統合管理基盤で稼働情報を確認するための設定	829

索引 | 831

1

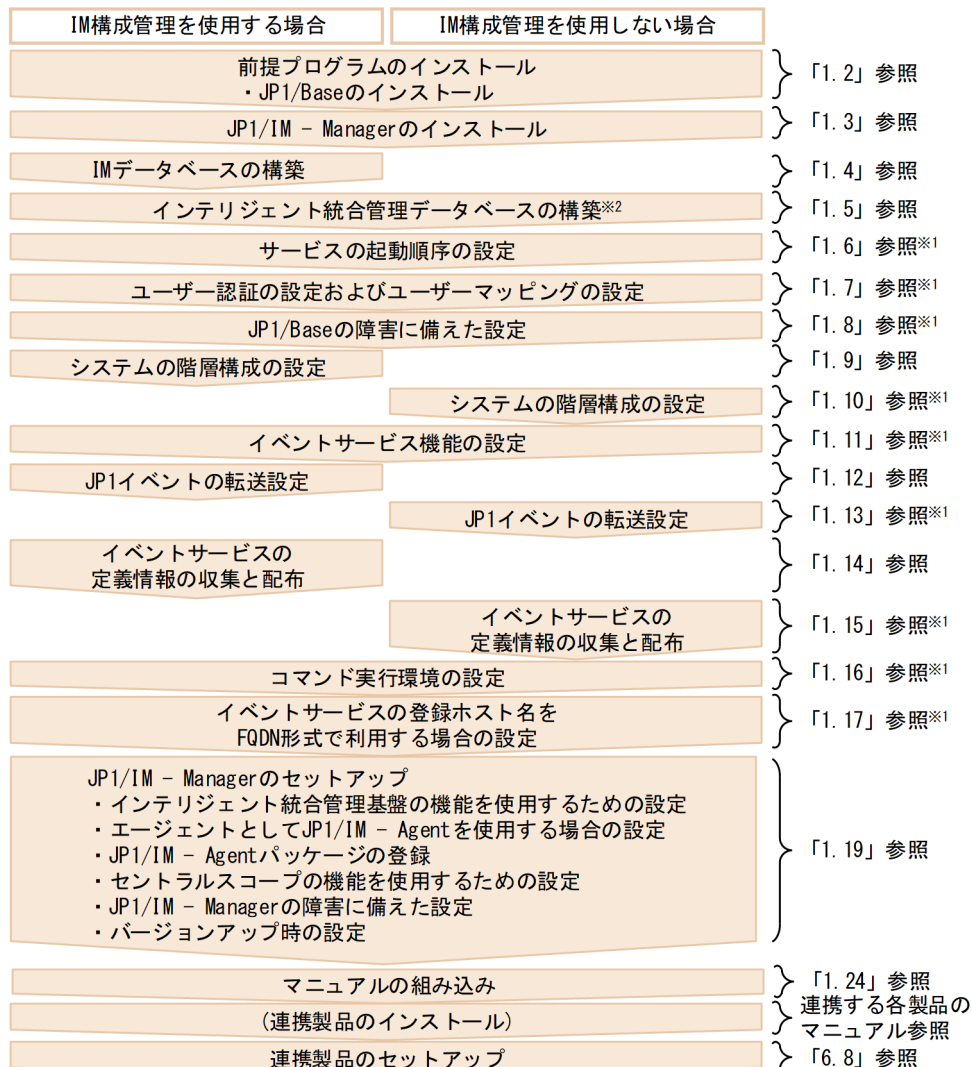
インストールとセットアップ（Windows の場合）

この章では、Windows 環境で JP1/IM をインストール、およびセットアップする手順について説明します。

1.1 インストールとセットアップの流れ (Windows の場合)

インストールの開始からセットアップの終了までの作業の流れを、マネージャーの場合、エージェントの場合、リモートの監視対象ホストの場合およびビューアーの場合に分けて示します。なお、アンインストール手順の詳細については、「1.25.1 アンインストール手順 (Windows の場合)」を参照してください。

図 1-1 インストールとセットアップの作業の流れ (マネージャー)



注※1 詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

注※2 インテリジェント統合管理データベースを使用する場合に実施します。

図 1-2 インストールとセットアップの作業の流れ（エージェント（JP1/IM - Agent））

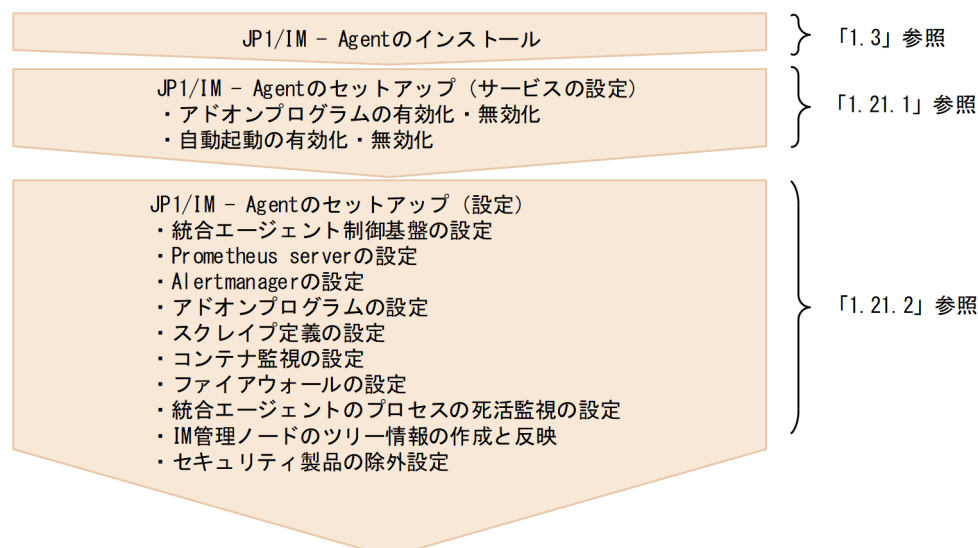
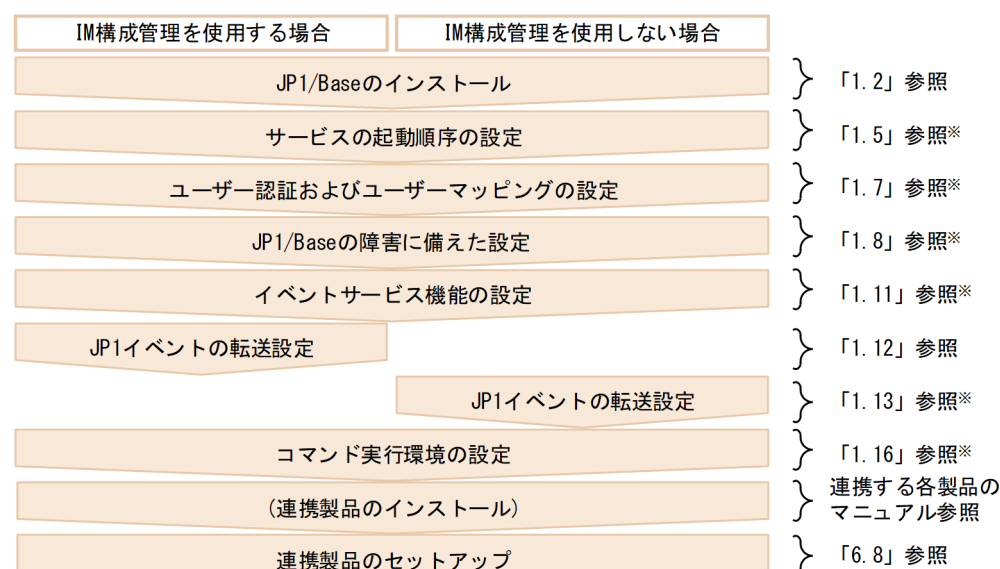


図 1-3 インストールとセットアップの作業の流れ（エージェント（JP1/Base））



注※ 詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

図 1-4 インストールとセットアップの作業の流れ（ビューアー）



リモートの監視対象ホストでログ監視をするための設定については、「[1.18 リモートの監視対象ホストでログ監視をするための設定 \(Windows の場合\)](#)」を参照してください。

通信データを暗号化する通信暗号化機能を使用するための設定については、「[9.4 暗号化通信の構築](#)」を参照してください。

1.2 インストール前に必要な作業（Windows の場合）

1.2.1 JP1/IM のセットアップ内容の設計（Windows の場合）

インストール作業に入る前に、JP1/IM のセットアップ内容について検討し、設定する内容をまとめておいてください。

セットアップ内容の設計については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「第3編 設計編」を参照してください。

1.2.2 システム環境の構築（Windows の場合）

(1) OS の環境構築

JP1/IM のインストール前に、次を満たす OS の環境を構築してください。

- JP1/IM の前提バージョンの OS であること
- JP1/IM の前提とするサービスパックやパッチが適用されていること
- ホスト名解決、IP アドレス解決が一意に行えること
- IM データベースを使用する場合、ホスト名が、半角英数字、-, .（ピリオド）で構成される 32 文字以内の文字列であること

JP1/IM - Manager および JP1/IM - View のリリースノートを参照して、JP1/IM が前提とするサービスパックやパッチを確認し、OS に適用してください。

OS のパッチを適用する際は、JP1/IM を停止した状態で適用してください。

❗ 重要

- インストール、セットアップおよびアンインストールの操作を行うには、管理者権限が必要です。Windows の UAC（ユーザーアカウント制御）が有効な環境で管理者（Administrator）以外のユーザーからこれらの操作を行う場合は、管理者への昇格を行ってください。なお、UAC が無効な環境である場合は、Administrators グループに所属するユーザーでこれらの操作を行ってください。
- JP1/IM - Manager および JP1/IM - View がインストールされている OS をアップグレードする場合、OS をアップグレードする前に JP1/IM - Manager および JP1/IM - View を必ずアンインストールしてください。

1.2.3 前提プログラムのインストール (Windows の場合)

(1) JP1/Base のインストール

JP1/IM のマネージャーおよびエージェントには、JP1/IM の前提製品である JP1/Base をインストールする必要があります。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「1.5 JP1/IM - Manager の構成」を参照し、システム構成を確認してください。また、JP1/Base のインストール方法については、マニュアル「JP1/Base 運用ガイド」を参照してください。

1.3 インストール (Windows の場合)

ここでは、JP1/IM - Manager, JP1/IM - View, および JP1/IM - Agent をインストールする手順について説明します。なお、インストール作業を行うユーザーは、Administrators 権限が必要です。

1.3.1 インストール手順 (Windows の場合)

JP1/IM - Manager, JP1/IM - View, および JP1/IM - Agent をインストールする手順について説明します。

なお、JP1/IM - Manager をインストールすると、JP1/IM - Agent を利用するための統合エージェント管理基盤もインストールされます。

(1) JP1/IM - Manager のインストールの手順

次の手順でインストールします。

1. すべてのプログラムを終了する。

インストールする前に、すべてのプログラムを終了してください。

「JP1/Base」のサービスを停止してください。

バージョンアップインストールをする場合、「JP1/IM3-Manager」サービスを停止してください。また、バージョンアップインストールをする JP1/IM - Manager に接続中の JP1/IM - View がある場合は、ログアウトしてください。

2. 提供媒体を該当するドライブに入れ、インストールする。

自動的に起動するインストーラーの指示に従ってインストールします。

インストールするソフトウェアを選択したあと、次の項目を入力します。

• ユーザー情報

新規インストールの場合だけ入力します。

旧バージョンの JP1/IM - Manager からバージョンアップした場合は、旧バージョンで設定した情報を引き継ぎます。

• インストール先フォルダ

x64 環境の場合、システムドライブ¥Program Files¥配下 (x86 が付いていない Program Files フォルダ) にはインストールしないでください。64 ビットモジュールと混在することによって、動作上問題が発生することがあります。

JP1/IM - Manager をインストールすると、次に示すインストール先フォルダが作成されます。

表 1-1 インストール時に作成されるフォルダ

製品	作成されるフォルダ※1	説明
JP1/IM - Manager	インストール先フォルダ¥JP1IMM¥※2	JP1/IM - Manager 情報が格納される。

製品	作成されるフォルダ※1	説明
	インストール先フォルダ¥JP1Cons¥※2	セントラルコンソール情報が格納される。
	インストール先フォルダ¥JP1Scope¥※2	セントラルスコープ情報が格納される。

注※1 インストール先フォルダのデフォルト値は"システムドライブ:¥Program Files¥Hitachi"です。Windows の場合, 「システムドライブ:¥Program Files」と表記している部分は, インストール時の OS 環境変数によって決定されるため, 環境によって異なる場合があります。

注※2 異なるフォルダに旧バージョンの JP1/IM - Manager をインストールしていた場合は, 旧バージョンのインストール先フォルダを引き継ぎます。その場合, 上に示すフォルダは作成されません。

なお, JP1/IM - Manager のインストール先フォルダに指定できるドライブは固定ディスクだけです。

3. 再起動を要求された場合は, Windows を再起動する。

統合トレース機能 (HNTRLlib2) がインストールされる時に再起動が必要です。詳細については, 「[1.3.3 インストール時の注意事項 \(Windows の場合\)](#)」を参照してください。

❗ 重要

- IM データベースをセットアップ済みの環境で, JP1/IM - Manager をバージョンアップした場合, jimdbupdate コマンドを実行して IM データベースを更新してください。IM データベースを更新していない場合は, JP1/IM - Manager を起動したときに警告メッセージが表示されます。
- JP1/IM - Manager のインストール先フォルダに指定できるドライブは固定ディスクだけです。リムーバブルディスク, ネットワークドライブ, UNC パスにはインストールできません。
- JP1/IM - Manager のインストール先フォルダに次に示すフォルダを指定しないでください。インストールした場合, 正常に動作しません。
 - 記号 (; # ' % など) を含むフォルダ
 - SJIS の文字コード範囲外の文字コード (JIS 第 3 水準, 第 4 水準) を含むフォルダ
- JP1/IM - Manager のインストール先フォルダ (JP1IMM, JP1Cons, および JP1Scope) は, ほかの製品のインストール先フォルダと同じにしないでください。
- JP1/IM - Manager によって作成される最上位フォルダ (JP1IMM, JP1Cons, および JP1Scope), 下位フォルダ, およびファイルは, インストール先フォルダの権限を継承します。そのため, インストール先フォルダには, 管理者権限のない OS ユーザーに対して次に示す権限を付与しないことを推奨します。
 - フルコントロール
 - 変更
 - 書き込み
 - 特殊なアクセス許可

- JP1/IM - Manager をインストールするボリューム、および、JP1/IM - Manager のデータを格納するボリュームでは、ショートネーム（8.3 形式の名前）が作成されている必要があります。OS によっては、デフォルトでショートネームの作成が無効の場合があるため、JP1/IM - Manager をインストールする前に OS の設定を確認し、ショートネームの作成が有効となっていること、およびショートネームが削除されていないことを確認してください。
- Windows Server 2016, Windows Server 2019, Windows Server 2022 の記憶域プールで作成した仮想ディスクへのインストールはサポートしていません。
- インストール中にキャンセルした場合、タイミングによってファイルが残る場合があります。

JP1/IM - Agent との暗号化通信を行う場合は、統合エージェント管理基盤に関する次の手順を実施します。

1. サーバ証明書とサーバ証明書のキーファイルを設定する。

統合エージェントホストと暗号通信を行う場合は、imbase 共通設定ファイル (jpc_imbasecommon.json) の tls_config.cert_file にサーバ証明書ファイルのフルパス、tls_config.key_file にサーバ証明書のキーファイルのフルパスを指定してください。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「imbase 共通設定ファイル (jpc_imbasecommon.json)」(2. 定義ファイル) を参照してください。

(2) JP1/IM - View のインストールの手順

次の手順でインストールします。

1. すべてのプログラムを終了する。

インストールする前に、すべてのプログラムを終了してください。

2. 提供媒体を該当するドライブに入れ、インストールする。

自動的に起動するインストーラーの指示に従ってインストールします。

インストールするソフトウェアを選択したあと、次の項目を入力します。

- ユーザー情報

新規インストールの場合だけ入力します。

- インストール先フォルダ

x64 環境の場合、システムドライブ¥Program Files¥配下 (x86 が付いていないProgram Files フォルダ) にはインストールしないでください。64 ビットモジュールと混在することによって、動作上問題が発生することがあります。

JP1/IM - View をインストールすると、次に示すインストール先フォルダが作成されます。

表 1-2 インストール時に作成されるフォルダ

製品	作成されるフォルダ※1	説明
JP1/IM - View	インストール先フォルダ¥JP1CoView¥※2	JP1/IM - View 情報が格納される。

1. インストールとセットアップ (Windows の場合)

注※1 インストール先フォルダのデフォルト値は"システムドライブ:¥Program Files¥Hitachi"です。Windows の場合、「システムドライブ:¥Program Files」と表記している部分は、インストール時の OS 環境変数によって決定されるため、環境によって異なる場合があります。

注※2 異なるフォルダに旧バージョンの JP1/IM - View をインストールしていた場合は、旧バージョンのインストール先フォルダを引き継ぎます。その場合、上に示すフォルダは作成されません。
なお、JP1/IM - View のインストール先フォルダに指定できるドライブは固定ディスクだけです。

3. 再起動を要求された場合は、Windows を再起動する。

統合トレース機能 (HNTRLlib2) がインストールされるときに再起動が必要です。詳細については、「[1.3.3 インストール時の注意事項 \(Windows の場合\)](#)」を参照してください。

❗ 重要

- JP1/IM - View のインストール先フォルダに指定できるドライブは固定ディスクだけです。リムーバブルディスク、ネットワークドライブ、UNC パスにはインストールできません。
- JP1/IM - View のインストール先フォルダに次に示すフォルダを指定しないでください。インストールした場合、正常に動作しません。
 - ・記号 (; # ' % など) を含むフォルダ
 - ・SJIS の文字コード範囲外の文字コード (JIS 第 3 水準, 第 4 水準) を含むフォルダ
- 旧バージョンからバージョンアップする場合、JP1/IM - View が固定ディスク以外にインストールされているときはバージョンアップできません。
- JP1/IM - View のインストール先フォルダ (JP1CoView) は、ほかの製品のインストール先フォルダと同じにしないでください。
- JP1/IM - View によって作成される最上位フォルダ (JP1CoView)、下位フォルダ、およびファイルは、インストール先フォルダの権限を継承します。そのため、インストール先フォルダには、管理者権限のない OS ユーザーに対して次に示す権限を付与しないことを推奨します。
 - ・フルコントロール
 - ・変更
 - ・書き込み
 - ・特殊なアクセス許可
- Windows 10, および Windows 11 にインストールする場合、インストール先としてシステムドライブ:¥Program Files¥WindowsApps 配下を指定しないでください。上記のフォルダは管理者ユーザーであっても書き込みができないため、インストールが失敗します。

(3) JP1/IM - Agent のインストールの手順

(a) インストール前に必要な情報

JP1/IM - Agent を新規インストールする場合は、次の情報が必要です。インストール前に準備してください。

表 1-3 新規インストールに必要な情報

項目	指定要否	説明
インストール先フォルダ	任意	インストール先フォルダを指定します。 次に示す条件に従ったフォルダを指定してください。それ以外のフォルダにインストールした場合、正常に動作しません。 指定できる文字は、半角英数字、半角スペース、半角ハイフン (-)、半角アンダースコア (_)、半角円記号 (¥) ※ ¹ 、半角コロン (:) ※ ² です。 注※1 フォルダ間の区切りに使用する文字を示します。フォルダ名には使用できません。 注※2 ドライブとフォルダの区切りに使用する文字を示します。フォルダ名には使用できません。
接続先 JP1/IM - Manager のホスト名	必須	インストールする統合エージェントを管理する接続先のマネージャーホストのホスト名を指定します。IP アドレスに名前解決する必要があります。
imbase プロセスの待ち受けポート	任意	接続先のマネージャーホストで稼働している imbase プロセスの待ち受けポートを 5001～65535 の範囲で指定します。 省略時は imbase のデフォルトのポート (20724) が使用されます。
imbaseproxy プロセスの待ち受けポート	任意	接続先のマネージャーホストで稼働している imbaseproxy プロセスの待ち受けポートを 5001～65535 の範囲で指定します。 省略時は imbaseproxy のデフォルトのポート (20725) が使用されます。
imbase に初回接続するための初期シークレット	必須	接続先のマネージャーホストで稼働している imbase プロセスに初回接続するための初期シークレットを指定します。 初期シークレットは、統合オペレーション・ビューアーから発行します。すでに発行済みで値を保存している場合は、その値を準備します。
プロキシの URL	任意	マネージャーホストに接続する際にプロキシサーバを経由する場合、プロキシの URL を「http://host:port」形式で指定します。省略時のデフォルトは空文字列となります。
プロキシ認証のユーザー ID	任意	マネージャーホストに接続する場合に、プロキシサーバを経由するときはプロキシサーバの認証用のユーザー ID を指定します。 指定できる文字は ASCII コード 0x20～0x7E の範囲の文字です。 指定できる最大長は 1007 文字です。 省略時のデフォルトは空文字列となります。
プロキシ認証のパスワード	任意	マネージャーホストに接続する際にプロキシサーバを経由する場合、プロキシサーバの認証用のパスワードを指定します。 指定できる文字は ASCII コード 0x20～0x7E の範囲の文字です。 指定できる最大長は 1024 文字です。

項目	指定要否	説明
		省略時のデフォルトは空文字列となります。
使用する機能	任意	JP1/IM - Agent で使用する機能を選択できます。新規インストールを行うと、使用する機能に関するサービスが自動起動するように設定されます。

(b) インストール手順

次の手順でインストールします。

1. エージェントホストに管理者権限でログインする。

インストール作業を行うユーザーには、Administrators 権限が必要です。

2. JP1/IM - Agent をインストールする。

JP1/IM - Agent をインストールするには、次の二つの方法があります。

- 提供媒体をドライブにセットしてインストールする方法
- マネージャーホストに登録されている JP1/IM - Agent パッケージを統合オペレーション・ビューアーからダウンロードで取得してインストールする方法※

注※

JP1/IM - Agent パッケージをダウンロードで取得する手順については、「[1.19.4\(3\) JP1/IM - Agent パッケージのダウンロードの手順](#)」を参照してください。

3. インストールするホストに対し、初期設定用環境変数を設定する。

■サイレントインストールおよびリモートインストールの場合（必須）

インストール時に必要となるパラメーターはあらかじめ環境変数※で設定しておく必要があります。

■通常のインストールの場合（任意）

インストーラーの画面上で設定する各パラメーターは、ユーザー名、所属、およびインストール先フォルダを除いて、あらかじめ環境変数※で値を設定しておくことができます。

インストーラーの画面上で手動で入力する場合は、環境変数を設定する必要はありません。

注※

環境変数の詳細については、「[1.3.1\(3\)\(c\)インストーラーで使用する初期設定用環境変数](#)」を参照してください。

4. すべてのプログラムを終了する。

インストールする前に、すべてのプログラムを終了してください。

バージョンアップインストールをする場合、JP1/IM - Agent のサービスを停止してください。

5. 取得した JP1/IM - Agent のインストーラーを実行し、JP1/IM - Agent をインストールする。

起動したインストーラーの指示に従ってインストールします。

インストールするソフトウェアを選択したあと、次の項目を入力します。インストールモードは「通常インストールモード」を選択します。

- ユーザー情報

新規インストールの場合だけ入力します。

旧バージョンの JP1/IM - Agent からバージョンアップした場合は、旧バージョンで設定した情報を引き継ぎます。

- インストール先フォルダ

システムドライブ¥Program Files (x86)¥配下 (x86 が付いているProgram Files フォルダ) にはインストールしないでください。32 ビットモジュールと混在することによって、動作上問題が発生することがあります。

JP1/IM - Agent をインストールすると、次に示すインストール先フォルダが作成されます。

表 1-4 インストール時に作成されるフォルダ

製品	作成されるフォルダ※1	説明
JP1/IM - Agent	インストール先フォルダ¥jp1ima※2	JP1/IM - Agent 情報が格納されます。

注※1 インストール先フォルダのデフォルト値は”システムドライブ:¥Program Files¥Hitachi”です。Windows の場合、「システムドライブ:¥Program Files」と表記している部分は、インストール時の OS 環境変数によって決定されるため、環境によって異なる場合があります。

注※2 異なるフォルダに旧バージョンの JP1/IM - Agent をインストールしていた場合は、旧バージョンのインストール先フォルダを引き継ぎます。その場合、上に示すフォルダは作成されません。なお、JP1/IM - Agent のインストール先フォルダに指定できるドライブは固定ディスクだけです。

■バージョンアップインストールを実行した場合

複数マネージャーホストへのデータ配信機能を使用している場合、JP1/IM - Agent のサービスを起動する前に、「1.21.2(2)(i) 複数マネージャーホストへのデータ配信機能を設定する (Windows の場合) (オプション)」の「バージョンアップ時の設定」を実施します。

6. 再起動を要求された場合は、Windows を再起動します。

7. インストール完了後、必要な設定変更を行う。

「1.21.2 JP1/IM - Agent の設定」に記載されている必要な設定変更を行います。必須の設定については、漏れなく実施してください。

❗ 重要

- JP1/IM - Agent のインストール先フォルダに指定できるドライブは固定ディスクだけです。リムーバブルディスク、ネットワークドライブ、UNC パスにはインストールできません。
- JP1/IM - Agent のインストール先フォルダは、次に示す条件に従ったフォルダを指定してください。それ以外のフォルダにインストールした場合、正常に動作しません。
 - ・指定できる文字は、半角英数字、半角スペース、半角ハイフン (-)、半角アンダースコア (_)、半角円記号 (¥) ※1、半角コロン (:) ※2 です。

注※1 フォルダ間の区切りに使用する文字を示します。フォルダ名には使用できません。

注※2 ドライブとフォルダの区切りに使用する文字を示します。フォルダ名には使用できません。

- JP1/IM - Agent のインストール先フォルダ (jplima) は、ほかの製品のインストール先フォルダと同じにしないでください。
- JP1/IM - Agent によって作成される最上位フォルダ (jplima)、下位フォルダ、およびファイルは、インストール先フォルダの権限を継承します。そのため、インストール先フォルダには、管理者権限のない OS ユーザーに対して次に示す権限を付与しないことを推奨します。
 - ・フルコントロール
 - ・変更
 - ・書き込み
 - ・特殊なアクセス許可
- Windows Server 2016, Windows Server 2019, Windows Server 2022 の記憶域プールで作成した仮想ディスクへのインストールはサポートしていません。
- インストール中にキャンセルした場合、タイミングによってファイルが残る場合があります。
- 統合エージェントホストで、統合エージェント制御基盤をインストールしたあと、統合エージェント制御基盤の初回起動までの間に、初期シークレットを変更した場合は、統合エージェントに登録された初期シークレットを更新するか、統合エージェントをアンインストールして再度インストールする必要があります。統合エージェントに登録された初期シークレットを更新する方法については、「[1.21.2\(2\)\(a\) 接続先の統合マネージャーを変更する \(Windows の場合\) \(オプション\)](#)」の手順 4 を参照してください。

(c) インストーラーで使用する初期設定用環境変数

JP1/IM - Agent のインストーラーで使用する初期設定用環境変数を、次に示します。

表 1-5 JP1/IM - Agent のインストーラーで使用する初期設定用環境変数の一覧

項目	環境変数	省略可否	値の説明	デフォルト値
JP1/IM - Agent のインストールモード	JP1IMAGENT_INSTALL_MODE	不可	• normal 通常インストールモード インストールした環境で運用する場合に選択します。 • image イメージ作成モード 次の場合に選択します。 ・インストールした環境を仮想マシンイメージにし、仮想マシンイメージから新しいインスタンスで運用する場合 ・ベースとなるコンテナイメージを作成する場合	なし

項目	環境変数	省略可否	値の説明	デフォルト値
			注意事項 運用開始前に <code>jimasetup</code> コマンドを使用して初期設定を完了させる必要があります。 詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasetup」(1. コマンド)を参照してください。	
接続先のマネージャーホストのホスト名	JP1IMAGENT_IMMGR_HOST	不可	新規インストールする統合エージェントを管理する接続先のマネージャーホストのホスト名を指定します。	なし
imbase の待ち受けポート番号	JP1IMAGENT_IMMGR_IMBASE_PORT	可	接続先のマネージャーホストで稼働している <code>imbase</code> プロセスの待ち受けポート番号を、5001～65535 の範囲で指定します。 この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	20724
imbaseproxy の待ち受けポート番号	JP1IMAGENT_IMMGR_IMBASEPROXY_PORT	可	接続先のマネージャーホストで稼働している <code>imbaseproxy</code> プロセスの待ち受けポート番号を、5001～65535 の範囲で指定します。 この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	20725
初期シークレット	JP1IMAGENT_IMMGR_INITIAL_SECRET	不可	接続先のマネージャーホストで稼働している <code>imbase</code> プロセスに初回接続するための初期シークレットを指定します。 初期シークレットは、統合オペレーション・ビューアーから確認します。	なし
接続先のプロキシ URL	JP1IMAGENT_IMMGR_PROXY_URL	可	マネージャーホストに接続するときにプロキシサーバを経由する場合、プロキシURL を「<code>http://host:port</code>」形式で指定します。 この環境変数を省略した場合、プロキシは経由しないと仮定して初期設定を行います。	なし
プロキシ認証のユーザー ID	JP1IMAGENT_IMMGR_PROXY_USER	可	マネージャーホストに接続するときにプロキシサーバを経由する場合、プロキシサーバの認証用のユーザー ID を指定します。 環境変数 <code>JP1IMAGENT_IMMGR_PROXY_URL</code> を省略した場合、この環境変数を設定しても無視します。	なし
プロキシ認証パスワード	JP1IMAGENT_IMMGR_PROXY_PASSWORD	可	マネージャーホストに接続するときにプロキシサーバを経由する場合、プロキシサーバの認証用のパスワードを指定します。 環境変数 <code>JP1IMAGENT_IMMGR_PROXY_URL</code> または環境変数 <code>JP1IMAGENT_IMMGR_PROXY_USER</code> を	なし

項目	環境変数	省略可否	値の説明	デフォルト値
			省略した場合、この環境変数を設定しても無視します。	
Prometheus server, Alertmanager の有効／無効の設定	JP1IMAGENT_ADDON_PROMETHEUS_AND_ALERTMANAGER_ACTIVE	可	Prometheus server, Alertmanager の有効／無効を指定します。 • yes Prometheus server と Alertmanager を有効にする • no Prometheus server と Alertmanager を無効にする この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	yes
Node exporter の有効／無効の設定	JP1IMAGENT_ADDON_NODE_EXPORTER_ACTIVE	可	Node exporter の有効／無効を指定します。 • yes Node exporter を有効にする • no Node exporter を無効にする Linux の場合にだけ設定する環境変数です。Windows の場合に設定したときは無視されます。 この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	yes
Windows exporter の有効／無効の設定	JP1IMAGENT_ADDON_WINDOWS_EXPORTER_ACTIVE	可	Windows exporter の有効／無効を指定します。 • yes Windows exporter を有効にする • no Windows exporter を無効にする Windows の場合にだけ設定する環境変数です。Linux の場合に設定したときは無視されます。 この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	yes
Blackbox exporter の有効／無効の設定	JP1IMAGENT_ADDON_BLACKBOX_EXPORTER_ACTIVE	可	Blackbox exporter の有効／無効を指定します。 • yes Blackbox exporter を有効にする • no Blackbox exporter を無効にする この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	no

項目	環境変数	省略可否	値の説明	デフォルト値
Yet another cloudwatch exporter の有効／無効の設定	JP1IMAGENT_ADDON_YA_CLOUDWATCH_EXPORTER_ACTIVE	可	Yet another CloudWatch exporter の有効／無効を指定します。 • yes Yet another cloudwatch exporter を有効にする • no Yet another cloudwatch exporter を無効にする この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	no
Fluentd の有効／無効の設定	JP1IMAGENT_ADDON_FLUENTD_ACTIVE	可	Fluentd の有効／無効を指定します。 • yes Fluentd を有効にする • no Fluentd を無効にする この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	yes
Promitor の有効／無効の設定	JP1IMAGENT_ADDON_PROMITOR_ACTIVE※	可	Promitor の有効／無効を指定します。 • yes Promitor を有効にする • no Promitor を無効にする	no
Process exporter の有効／無効の設定	JP1IMAGENT_ADDON_PROCESS_EXPORTER_ACTIVE※	可	Process exporter の有効／無効を指定します。 • yes Process exporter を有効にする • no Process exporter を無効にする Linux の場合にだけ設定する環境変数です。Windows の場合に設定したときは無視されます。	yes
Script exporter の有効／無効の設定	JP1IMAGENT_ADDON_SCRIPT_EXPORTER_ACTIVE※	可	Script exporter の有効／無効を指定します。 • yes Script exporter を有効にする • no Script exporter を無効にする	no
Web シナリオ監視機能の有効／無効の設定	JP1IMAGENT_ADDON_WEB_EXPORTER_ACTIVE	可	Web シナリオ監視機能の有効／無効を指定します。 • yes Web シナリオ監視機能を有効にする • no	no

項目	環境変数	省略可否	値の説明	デフォルト値
			Web シナリオ監視機能を無効にする この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	
VMware exporter の有効／無効の設定	JP1IMAGENT_ADDON_VMWARE_EXPORTER_ACTIVE	可	VMware exporter の有効／無効を指定します。 • yes VMware exporter を有効にする • no VMware exporter を無効にする この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	no
Hyper-V 監視機能の有効／無効の設定	JP1IMAGENT_ADDON_WINDOWS_EXPORTER_HYPERV_ACTIVE	可	Hyper-V 監視機能の有効／無効を指定します。 • yes Hyper-V 監視機能を有効にする • no Hyper-V 監視機能を無効にする この環境変数を省略した場合、デフォルト値を仮定して初期設定を行います。	no

注※

指定を省略した場合、デフォルト値が仮定されます。

(4) 各種インストールについて

バージョンアップインストールについて

旧バージョンからバージョンアップする場合は、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.2 旧バージョンの JP1/IM からのバージョンアップについて」を参照してバージョンアップ時の注意について事前に知っておってください。

また、JP1/IM - Agent をバージョンアップした場合の注意事項については、「[1.3.3\(14\) JP1/IM - Agent をバージョン 13-00 または 13-01 からバージョンアップした場合の注意事項](#)」および「[1.3.3\(15\) JP1/IM - Agent をバージョン 13-00～13-10 からバージョンアップした場合の注意事項](#)」を参照してください。

スタートメニューのプログラムフォルダの注意事項

- バージョンアップインストール中の「プログラムフォルダの選択」画面に示されるデフォルトのプログラムフォルダ名称は、バージョンアップ前の製品で使用していたプログラムフォルダの名称となります。バージョンアップ前の製品で使用していたプログラムフォルダ名称から変更する場合は、「プログラムフォルダの選択」画面で新しいプログラムフォルダ名称を入力してください。

- JP1/NETM/DM を使用してバージョンアップインストールした場合は、バージョンアップ前製品で使用していたプログラムフォルダが引き継がれます。プログラムフォルダ名称を変更する場合は、バージョンアップインストールが完了してから手動で行ってください。
- バージョンアップ前の製品で、スタートメニューのプログラムフォルダを手動で変更した場合は、JP1/IM - Manager, JP1/IM - View, および JP1/IM - Agent をバージョンアップインストールしてもプログラムフォルダは削除されません。不要な場合は、バージョンアップインストール完了後に手動で削除してください。

バージョンアップする前の製品でプログラムフォルダにショートカットが設定されている場合

- プログラムフォルダ名称を変更した場合は、バージョンアップ前製品で設定されたショートカットは引き継がれません。バージョンアップ前製品のショートカットを使用したい場合は、ショートカットを変更後のプログラムフォルダに設定してください。また、バージョンアップ前製品で使用していたプログラムフォルダにはショートカットが残ったままとなりますので、不要な場合は削除してください。

バージョンアップインストールする前に次の内容を実施してください。

■JP1/IM - Manager の場合

- JP1/IM - Manager のサービス（サービス名：JP1_Console）を停止してください。
- 論理ホストを設定している場合は、論理ホストの JP1/IM - Manager のサービス（サービス名：JP1_Console_論理ホスト名）を停止してください。
- [サービス] 画面および [コンピュータの管理] 画面のサービスを表示している場合は画面を閉じてください。

■JP1/IM - Agent の場合

- 論理ホストのサービスが起動している場合は、サービスを停止してからバージョンアップインストールを実行してください。論理ホストのサービス起動中にバージョンアップインストールを実行すると、論理ホストのサービスで使用するファイルが削除され、サービスが異常終了するおそれがあります。

インストール後は、コンピュータを再起動してください。

JP1/NETM/DM, JP1/IT Desktop Management 2 および Job Management Partner 1/Software Distribution を使ったリモートインストールについて

JP1/IM は、JP1/NETM/DM, JP1/IT Desktop Management 2 および Job Management Partner 1/Software Distribution を使ったリモートインストール（ソフトウェア配布）に対応しており、JP1/IM の新規インストールおよびバージョンアップができます。次のリモートインストール方法が利用できます。

・更新インストール

■JP1/IM - Manager の場合

インストール済みの JP1/IM - Manager と同じフォルダにインストールします。インストール済みの JP1/IM - Manager の設定情報は引き継がれます。JP1/IM - Manager がインストールされていない場合、更新インストールはできません。

■JP1/IM - Agent の場合

インストール済みの JP1/IM - Agent と同じフォルダにインストールします。インストール済みの JP1/IM - Agent の設定情報は引き継がれます。JP1/IM - Agent がインストールされていない場合、更新インストールはできません。

■JP1/IM - View の場合

インストール済みの JP1/IM - View と同じフォルダにインストールします。インストール済みの JP1/IM - View の設定情報は引き継がれます。JP1/IM - View がインストールされていない場合、更新インストールはできません。

・新規インストール

ドライブ・フォルダともデフォルト値を使用した場合、次のフォルダを作成してインストールします。

■JP1/IM - Manager の場合

- "システムドライブ:¥Program Files¥HITACHI¥JP1IMM"フォルダ
- "システムドライブ:¥Program Files¥HITACHI¥JP1Cons"フォルダ
- "システムドライブ:¥Program Files¥HITACHI¥JP1Scope"フォルダ

■JP1/IM - Agent の場合

- "システムドライブ:¥Program Files¥HITACHI¥jp1ima"フォルダ

■JP1/IM - View の場合

- "システムドライブ:¥Program Files¥HITACHI¥JP1CoView"フォルダ

ドライブのみ指定した場合、指定したドライブ直下にインストールします。

フォルダを指定した場合、指定したフォルダにインストールします。

実際の操作・運用方法については、JP1/NETM/DM, JP1/IT Desktop Management 2 または Job Management Partner 1/Software Distribution のマニュアルを参照してください。JP1/IM をパッケージングする際は、必ず JP1/NETM/DM 09 -00 以降, Job Management Partner 1/Software Distribution 09 -00 以降, または JP1/IT Desktop Management 2 のパッケージを使用してください。なお、JP1/NETM/DM は日本でだけ販売している製品です。

1.3.2 インストール直後に必要な設定 (Windows の場合)

インストール後にロケール (システムロケール) を変更する場合は、次の表に示す文字コードの設定が必要になります。JP1/Base で設定します。

表 1-6 Windows の文字コード

OS	言語種別	文字コード
Windows	日本語	SJIS
	中国語	GB18030
	英語	C

❗ 重要

JP1/IM - View を使用中にシステムのロケールを変更した場合の動作は保証しません。システムのロケールを変更する場合は、JP1/IM をアンインストールしてからロケールを変更した後に、本製品をインストールし直してください。

(1) 文字コードの設定手順

1. jp1bs_param.conf を編集する。

Base パス¥conf¥jp1bs_param.conf ファイルをエディターで開き、"LANG"="文字コード"の文字コードの部分に、上の表で示した文字コードの値を設定してください。

2. ファイルを保存したあと、Administrators 権限で次に示すコマンドを実行する。

```
Base/パス¥bin¥jbssetcnf Base/パス¥conf¥jp1bs_param.conf
```

3. JP1/Base および JP1/IM - Manager を起動または再起動する。

設定は JP1/Base および JP1/IM - Manager の起動時に有効になります。JP1/Base および JP1/IM - Manager が起動済みの場合は、再起動してください。

📄 メモ

文字コードを設定して運用を開始した後でも、この手順で文字コードの変更ができます。

1.3.3 インストール時の注意事項 (Windows の場合)

(1) 製品間の関連について

JP1/IM - Manager は JP1/Base を前提製品としています。製品のインストール時には、次の点に注意してください。

- 前提製品がある場合は、前提の製品から順にインストールしてください。
- JP1/Base, JP1/IM - Manager の順序にインストールしてください。
- JP1/Base を停止してから、JP1/IM - Manager をインストールしてください。JP1/Base の停止を忘れた場合は、必ず JP1/Base を再起動してください。再起動しなかった場合は、システム構成情報を正しく管理できません。

(2) 統合トレース機能 (HNTRLib2) について

- JP1/IM - View, JP1/IM - Agent, または JP1/Base のインストール時に, 統合トレース機能 (HNTRLib2) がインストールされます。このとき, Windows のシステム環境変数 Path に HNTRLib2 のパス (システムドライブ:¥Program Files¥Common Files¥Hitachi※) が追加されます。
- JP1/IM - View または JP1/IM - Agent のインストール時に, Hitachi Network Objectplaza Trace Monitor 2 サービス (統合トレース) に「自動」が設定され, システムの起動時に自動起動するように初期設定されます。

注※ Windows の場合, 「システムドライブ:¥Program Files」と表記している部分は, インストール時の OS 環境変数によって決定されるため, 環境によって異なる場合があります。

(3) Windows 環境への設定について

インストール時に次の情報を Windows に設定します。

- システム環境変数に, 次の JP1/IM のbin フォルダのパスと HNTRLib2 のパスを設定します。

Console パス¥bin

JP1/IM - Manager のインストール時に追加されます。

View パス¥bin

JP1/IM - View のインストール時に追加されます。

システムドライブ:¥Program Files¥Common Files¥Hitachi※

JP1/IM - View または JP1/Base のどちらかのインストール時に追加されます。

services ファイルに, マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 C ポート番号」のポート番号を設定します。なお, アンインストール時に, ポート番号は削除されます。

注※ Windows の場合, 「システムドライブ:¥Program Files」と表記している部分は, インストール時の OS 環境変数によって決定されるため, 環境によって異なる場合があります。

(4) インストールパスの変更について

- インストールパスを変更する場合は, 一度アンインストールしてから再インストールしてください。
- JP1/Base と同じホストに JP1/IM - View を再インストールする場合は, アンインストールしたあと, インストール先のconf フォルダおよびbin フォルダの下位のファイルを削除してから再インストールしてください。
- JP1/IM - Manager, JP1/IM - View, または JP1/Base のインストールパスを変更する際に, バックアップから定義をリカバリーできません。再インストール後, 定義を個別に設定し直してください。

(5) ファイル・レジストリについて

- JP1/IM - Manager および JP1/IM - View は、プログラム情報、設定情報、保守情報などをファイル、およびレジストリで管理しているため、次の操作を行わないでください。次の操作を行った場合、JP1/IM - Manager および JP1/IM - View の動作を保証できません。
 - エクスプローラなどを使用して、JP1/IM - Manager のファイル、およびフォルダの削除や変更を行う。または、アクセス権限を変更する。
 - レジストリエディターで、JP1/IM - Manager の情報の削除や変更、およびアクセス権限の変更を行う。
- "システムドライブ:\Program"という名前のファイルまたはフォルダを作成しないでください。上記ファイルまたはフォルダが存在する場合、jcodbsetup コマンド、またはjcfdbsetup コマンドが次のメッセージを出力して異常終了するなどの問題が発生します。

KNAN11053-E ファイルの読み込みに失敗しました。（ファイル名:instdb.log）

なお、上記ファイルまたはフォルダが存在する場合、JP1/IM - Manager に限らず、各種プログラムが正しく動かない可能性があります。

(6) 再インストールについて

JP1/IM - Manager, JP1/IM - View, および JP1/IM - Agent のアンインストールでは、インストール後に作成された定義ファイルやログファイル、ユーザーが修正する可能性のあるファイルは削除されません。これらのファイルが残っている状態で再インストールすると、プログラムの動作が不正になる場合があります。したがって、再インストールする場合は、OS を必ず再起動し、JP1/IM - Manager, JP1/IM - View, および JP1/IM - Agent をインストールしていたフォルダをエクスプローラにより削除してから、再インストールしてください。

(7) バージョンダウンインストールについて

JP1/IM - Manager, JP1/IM - View, および JP1/IM - Agent は、バージョンダウンインストールに対応していません。インストールされている製品をバージョンダウンしたい場合は、製品をアンインストールしてから再インストールしてください。

(8) ウィルス対策ソフトについて

- JP1/IM - Manager のインストールを実施した際に、ウィルス対策ソフトが JP1/IM - Manager のインストール先のウィルススキャンを行った場合、インストーラーとウィルス対策ソフトとの競合によりアプリケーションエラーが発生し、インストールに失敗する可能性があります。ウィルス対策ソフトを停止してインストールを実施してください。
- JP1/IM - View をインストールする前に、ウィルス対策ソフトなど JP1/IM - View のファイルをロックするようなアプリケーションを終了してください。終了しなかった場合、インストールに失敗することがあります。

- JP1/IM - View をバージョンアップインストールする前に、ウィルス対策ソフトなど JP1/IM - View のファイルをロックするようなアプリケーションを終了してください。終了しなかった場合、インストールに失敗し、JP1/IM - View が起動しなかったり、JP1/IM - View 起動時にエラーが発生したりすることがあります。
- JP1/IM - View バージョンアップ後、イベントログ（アプリケーション）に次のようなメッセージが出力されており、かつ JP1/IM - View が起動しない場合は、OS 再起動後、JP1/IM - View を再インストールしてください。

再起動が必要です。製品名: JP1/Integrated Management - View,
製品バージョン: <バージョンアップ前のJP1/IM - Viewのバージョン>,
製品の言語: 1041, 製造元: Hitachi, Ltd.,
システム再起動の種類: <XX>, 再起動の理由: <XX>

(9) サイレントインストールについて

JP1/IM - Manager では、サイレントインストール機能によるインストール方法が利用できます。

実行コマンド

提供媒体¥_OWNEXE¥HPPSINST.BAT△/提供媒体¥_PPDIR¥PCC2A2C9MDL¥DISK1△/"インストール先のフルパス"

△: 1 個以上の半角スペース

JP1/IM - View では、サイレントインストール機能によるインストール方法が利用できます。

実行コマンド

提供媒体¥_OWNEXE¥HPPSINST.BAT△/提供媒体¥_PPDIR¥PCC2A2C6HDL¥DISK1△/"インストール先のフルパス"

△: 1 個以上の半角スペース

JP1/IM - Agent では、サイレントインストール機能によるインストール方法が利用できます。

実行コマンド

- 提供媒体の場合

提供媒体¥_OWNEXE¥HPPSINST.BAT△/提供媒体¥_PPDIR¥PCC2A2C9GDL¥DISK1△/"インストール先のフルパス"

- 統合オペレーション・ビューアーからダウンロードして取得した JP1/IM - Agent パッケージの場合

msiexec△/i△JP1/IM - Agentパッケージ¥DISK1¥JP1IMAgent.msi△/qn△STARTFROM=NETM

△: 1 個以上の半角スペース

- 提供媒体を HDD 上にコピーして実行する場合は、スペースを含まないディレクトリパス上に媒体の内容をすべてコピーしてください。また、コピーしたファイル群は、コンペアなどによって、バイナリレベルで一致することを確認してください。
- インストールが正常終了したかどうかは、実行結果の戻り値を参照してください。戻り値については、JP1 の Web サイトに公開しているドキュメントの「サイレントインストール機能」を参照してください。
- JP1/IM - Manager, JP1/IM - View, および JP1/IM - Agent をサイレントインストール機能でインストールする場合は、ユーザー情報を指定することができません。ユーザー情報を指定する場合は、「[1.3.1 インストール手順 \(Windows の場合\)](#)」に記載のインストール手順でインストールしてください。
- JP1/IM - Agent はサイレントインストール機能でインストールする前に setx コマンドでユーザー環境変数を設定する必要があります。
また、サイレントインストール後は再度 setx コマンドを実行してユーザー環境変数をクリアしてください。

(10) Windows Defender について

Windows Defender が有効になっている場合に、JP1/IM - Manager および JP1/IM - View をインストールすると Windows Defender の履歴およびイベントビューアの Windows ログ（システムログ）に Windows Defender の警告イベントが出力される場合がありますが問題ありません。

(11) 上書きインストール後の再起動について

JP1/NETM/DM を使用せずにインストールをする場合は、次の手順を適用することで、上書きインストール後にコンピュータの再起動を行わずに JP1/IM - Manager および JP1/IM - View を動作させることができます。

1. 上書きインストール前に次のプログラムを終了してください。
 - JP1/IM - Manager および JP1/IM - View
 - JP1/IM - Manager および JP1/IM - View のインストール先フォルダ以下のファイルをロックするアプリケーション（ウイルス対策ソフト製品など）
 - JP1/Base の全てのサービス
 - JP1/Base を前提とする製品のすべてのサービス
 - 統合トレース機能(HNTRLib2)のサービス
2. JP1/IM - Manager および JP1/IM - View のインストール後に、コンピュータの再起動を要求された場合は「いいえ」を選択してください。

(12) ReFS を使用する場合

Windows Server 2016, Windows Server 2019, Windows Server 2022 の ReFS 上に JP1/IM - Manager をインストールした場合、NTFS 上にインストールした場合に比べて、処理性能が低下する可能性があります。そのため、ReFS を使用する場合は運用を想定したテストを十分に実施し、性能に問題がないことを検証してください。性能要件を満たせない場合は、ReFS ではなく NTFS を使用することを検討してください。

(13) JP1/IM - View について

- JP1/IM - View をインストールしているボリュームには、Windows Server 2016, Windows Server 2019, Windows Server 2022 のデータ重複除去を適用しないでください。
- JP1/IM - View を使用中に上書きインストールした場合、ダイアログが表示されます。この場合は [キャンセル] ボタンをクリックし、いったん上書きインストールを中断したあと、起動中の JP1/IM - View をすべて停止してから、再度 JP1/IM - View を上書きインストールしてください。

(14) JP1/IM - Agent をバージョン 13-00 または 13-01 からバージョンアップした場合の注意事項

- 統合エージェント管理基盤と統合エージェント制御基盤の間の通信を暗号化している場合に必要となる証明書に関して、脆弱性がある次の暗号スイートはサポート対象外となります。
 - "TLS_RSA_WITH_AES_128_CBC_SHA" (TLS1.2 まで)
 - "TLS_RSA_WITH_AES_256_CBC_SHA" (TLS1.2 まで)
 - "TLS_RSA_WITH_AES_128_GCM_SHA256" (TLS1.2 だけ)
 - "TLS_RSA_WITH_AES_256_GCM_SHA384" (TLS1.2 だけ)

上記の暗号スイートを使用している場合は、サポートする暗号スイートを使用するように、証明書を変更してください。サポートする暗号スイートについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(1)(c) 暗号通信」の「サポートする暗号スイート」を説明している個所を参照してください。

- Yet another cloudwatch exporter を使用している場合、Yet another cloudwatch exporter 設定ファイル (jpc_ya_cloudwatch_exporter.yml) の exportedTagsOnMetrics パラメーターに指定しているサービス名が、jobs パラメーターの type にも指定されていることを確認してください。指定されていない場合、JP1/IM - Agent 13-10 以降の Yet another cloudwatch exporter のサービス起動に失敗することがあります。

(15) JP1/IM - Agent をバージョン 13-00～13-10 からバージョンアップした場合の注意事項

JP1/IM - Agent をバージョンアップすると、アドオン管理機能に対応している OSS に OSS ラッパーを適用させるために、次の表に示すサービス定義ファイルに対して、executable 行の更新および arguments

行の 1 行目の追加が行われます。JP1/IM - Agent のインストーラーのログで、各サービス定義ファイルに対して KAVB9447-I のメッセージが出力されていることを確認してください。JP1/IM - Agent のインストーラーのログについては、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「12.2.2(8) インストーラーのログ」を参照してください。

アドオンプログラム	サービス定義ファイル名	バックアップファイル名
Prometheus server	jpc_prometheus_server_service.xml	jpc_prometheus_server_service.xml.bk
Alertmanager	jpc_alertmanager_service.xml	jpc_alertmanager_service.xml.bk
Windows exporter	jpc_windows_exporter_service.xml	jpc_windows_exporter_service.xml.bk
Blackbox exporter	jpc_blackbox_exporter_service.xml	jpc_blackbox_exporter_service.xml.bk
Yet another cloudwatch exporter	jpc_ya_cloudwatch_exporter_service.xml	jpc_ya_cloudwatch_exporter_service.xml.bk
Promitor	jpc_promitor_resource_discovery_service.xml	jpc_promitor_resource_discovery_service.xml.bk
	jpc_promitor_scraper_service.xml	jpc_promitor_scraper_service.xml.bk
Script exporter	jpc_script_exporter_service.xml	jpc_script_exporter_service.xml.bk
Fluentd	jpc_fluentd_service.xml	jpc_fluentd_service.xml.bk
Web exporter	jpc_web_exporter_service.xml	jpc_web_exporter_service.xml.bk
VMware exporter	jpc_vmware_exporter_service.xml	jpc_vmware_exporter_service.xml.bk

KAVB9448-W および KAVB9450-W のメッセージが出力されている場合は、該当するサービス定義ファイルを手動で編集して、executable 行の更新および arguments 行の 1 行目の追加を行ってください。executable 行および arguments 行の記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「サービス定義ファイル (jpc_プログラム名_service.xml)」(2. 定義ファイル)を参照してください。

1.3.4 インストール時の資料採取方法 (Windows の場合)

(1) JP1/IM - Manager のインストール時の資料採取方法

インストール時に障害が発生した場合の資料採取方法を、次に示します。

1. マネージャーホストにログインする。

2. 次のファイルを手動で採取する。

- システムドライブ¥Windows¥Temp¥HCDINST¥以下のファイル

(2) JP1/IM - Agent のインストール時の資料採取方法

インストール時に障害が発生した場合の資料採取方法を、次に示します。

1. 統合エージェントホストにログインする。

2. 次のファイルを手動で採取する。

- 提供媒体でインストールした場合
システムドライブ¥Windows¥Temp¥HCDINST¥以下のファイル
- 統合オペレーション・ビューアーからダウンロードした JP1/IM - Agent パッケージでインストールした場合
%TEMP%¥以下のインストール実行時に出力されたログファイル (MSI*.LOG)

注※ %TEMP%は、環境変数 TEMP に指定されているパスを示します。

1.3.5 オートスケール機能と連携する方法 (Windows の場合)

(1) JP1/IM - Agent でオートスケール機能と連携する方法

(a) 前提サービスと前提条件

オートスケール機能と連携して運用する場合の前提サービスと前提条件を、次に示します。

前提サービス

- Amazon EC2
- Amazon EC2 Auto Scaling

前提条件

オートスケール機能と連携して運用する場合の前提条件を次に示します。

- クラスタ環境の論理ホストを対象とすることはできません。
- システムの構成はマネージャーホストを含めて 2,500 台以内にしてください。
- スケールアウトやスケールインが行われた後でシステム構成情報の作成と反映を行う必要があります。詳細については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください

(b) 仮想マシンイメージ (AMI) の作成

仮想マシンイメージ (AMI) を作成する手順を次に示します。

1. JP1/IM - Agent をインストールします。

このとき、インストールモード [イメージ作成モード] を選択します。詳細については、[「1.3.1\(3\)\(c\) インストーラーで使用する初期設定用環境変数」](#) を参照してください。

2. 仮想マシンイメージ (AMI) を作成します。

仮想マシンイメージ (AMI) の作成方法については、Amazon Web Services の公式サイトを参照してください。

(c) Auto Scaling の起動設定の作成

Auto Scaling の起動設定を作成する手順を次に示します。

1. [AWS マネジメントコンソール] から [Amazon EC2] コンソールを開きます。
2. 左側ナビゲーションペインの [Auto Scaling] で [起動設定] をクリックします。
3. [起動設定の作成] をクリックします。
4. [AMI の選択] 画面から、手順 1 で作成した仮想マシンイメージ (AMI) を選択します。
5. [詳細設定] 画面の [高度な詳細] - [ユーザーデータ] で [テキストで] を選択して、テキストボックスに次の内容を記述します。

Windows の場合

```
<script>
インストール先¥jp1ima¥tools¥jimasetup phost
インストール先¥jp1ima¥tools¥jpc_service_start -s all
</script>
```

1.3.6 仮想マシンのクローン作成 (Windows の場合)

次に示す仮想化プラットフォームでは、JP1/IM - Agent をイメージ作成モードでインストールした統合エージェントホスト環境の仮想マシンテンプレートから、仮想マシンのクローンを作成できます。

- VMware ESX
- Hyper-V
- SCVMM

(1) 前提条件

エージェントを複製する場合の前提条件となる注意事項を次に示します。

- 仮想マシンのクローンを作成できる対象はエージェントホストだけです。また、クラスタ環境の論理ホストを対象とすることはできません。
- エージェント構成上のホスト数の最大値は、マネージャーホストを含めて 2,500 台です。

- ・ 仮想マシンテンプレートを作成するとき、JP1/IM - Agent のインストールモードには [イメージ作成モード] を選択してください。

(2) 仮想マシンのテンプレートの作成方法

仮想マシンのテンプレートの作成方法を、次に示します。

1. 仮想マシンに JP1/IM - Agent をインストールする。

インストール時のインストールモードは [イメージ作成モード] を選択します。

インストール方法については、「[1.3.1\(3\)JP1/IM - Agent のインストールの手順](#)」を参照してください。

! 重要

JP1/IM - Agent の初期設定は行いません。

(3) 仮想マシンのクローンの作成方法

仮想マシンのクローンの作成方法を、次に示します。

1. 仮想マシンテンプレートから、新しい仮想マシンを複製する。

仮想化プラットフォームが提供する複製機能については、仮想化ソフトウェアのマニュアルを参照してください。

複製に関して OS で必要な作業については、OS の仕様を確認してください。

2. 新しい仮想マシンを起動する。

3. 新しい仮想マシンのホスト名を変更する。

必要に応じて、仮想マシンのホスト名を変更してください。

4. 新しい仮想マシンの IP アドレスを変更する。

必要に応じて、仮想マシンの IP アドレスを変更してください。

IP アドレスを変更した場合の作業については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「[2.3.1\(3\)エージェントの IP アドレスを変更した場合の作業](#)」を参照してください。

5. JP1/IM - Agent の初期設定を行う。

JP1/IM - Agent の初期設定コマンドを実行します。

```
JP1/IM - Agentのインストール先¥jplima¥tools¥jimasetup phost
```

6. JP1/IM - Agent の接続先の JP1/IM - Manager で、IM 管理ノードのツリー情報を更新する。

詳細については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください。

1.4 IM データベースの構築 (Windows の場合)

IM データベースを使用して、システムで発生したイベントを監視します。IM データベースには、統合監視 DB と IM 構成管理 DB とがあります。統合監視 DB は、インテリジェント統合管理基盤、またはセン
トラルコンソールを利用する場合に使用します。IM 構成管理 DB は、IM 構成管理を使用してシステムの
階層構成を管理します。統合監視 DB と IM 構成管理 DB を使用した場合に利用できる機能の詳細につい
ては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.6 IM データ
ベースが提供する機能」を参照してください。

システム構築時および運用開始後に、統合監視 DB、IM 構成管理 DB のどちらかまたは両方が必要になっ
たときは、その時点で IM データベースを構築できます。

IM データベースは、JP1/IM3-Manager サービスより先に、起動する必要があります。マニュアル「JP1/
Integrated Management 3 - Manager 運用ガイド」の「3.1.1 Windows の場合」を参照し、JP1/Base
の起動管理機能を使って設定してください。

統合監視 DB には、JP1/IM3-Manager サービスが起動したあとにイベント DB から取得した JP1 イベント
が格納されます。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設
計ガイド」の「4.1.3(2) 統合監視 DB を使用する場合の JP1 イベント制御の仕組み」を参照してください。

ここでは、IM データベースを構築する手順について説明します。

❗ 重要

Amazon EC2 インスタンス環境での運用では、ホスト名が 32 文字を超えることがあります
(例：ip-xx-xx-xx-xx.ap-northeast-1.compute.internal (xx-xx-xx-xx の部分は IP アドレ
ス))。IM データベースをセットアップする場合、IM データベースのホスト名が上限 (32 文
字) を超えると、KNAN11141-E のエラーメッセージを出力して、セットアップが失敗しま
す。そのため、AWS が公開する Amazon EC2 インスタンスに静的ホスト名を永続的に割り
当てる方法に従って、上限 (32 文字) を超えないホスト名に変更してください。

1.4.1 IM データベースを構築するための準備 (Windows の場合)

IM データベースを構築するために必要なデータベース領域のサイズやデータベース格納ディレクトリの情
報を記述したセットアップ情報ファイルを準備します。

1. セットアップ情報ファイルを編集する。

設定例を次に示します。

#IM DATABASE SERVICE - DB Size

IMDBSIZE=S

#IM DATABASE SERVICE - Data Storage Directory

IMDBDIR=Manager パス¥database

```
#IM DATABASE SERVICE - Port Number
IMDBPORT=20700

#IM DATABASE SERVICE - DB Install Directory
IMDBENVDIR=Manager パス¥dbms
```

JP1/IM - MO を使用する場合で、JP1/IM - Manager と JP1/IM - MO が異なるホストで動作するときは、セットアップ情報ファイルに記載する項目に「IMDBHOSTNAME」を追加する必要があります。セットアップ情報ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「セットアップ情報ファイル (jimdbsetupinfo.conf)」(2. 定義ファイル) を参照してください。

2. セットアップ情報ファイルの設定値を確認する。

次の項目を確認してください。

- IMDBENVDIR およびIMBDDIR に、ネットワークドライブや Windows の予約デバイスファイルを指定していないか。また、シンボリックリンクを含むパスを指定していないか。

3. Application Experience サービスが存在する場合は、Application Experience サービスのスタートアップの種類が無効になっていないことを確認する。

無効の場合、jcodbsetup コマンド、またはjcfdbsetup コマンドを実行した際に、次のメッセージを出力して IM データベースのセットアップに失敗する可能性があります。

KNAN11141-E システム DB 領域の作成中にエラーが発生しました。(エラーコード:-1073741811)。

❗ 重要

- システム環境変数 TEMP に 200 バイト以上のパスを指定しないでください。200 バイト以上のパスを指定している場合、IM データベースのセットアップ、アンセットアップに失敗することがあります。セットアップに失敗した場合は、システム環境変数 TEMP の値を修正した後、一度、統合監視 DB、IM 構成管理 DB の両方をアンセットアップし、再セットアップを行ってください。アンセットアップに失敗した場合は、システム環境変数 TEMP の値を修正した後、統合監視 DB、IM 構成管理 DB の両方をアンセットアップしてください。
- jcodbsetup コマンド、またはjcfdbsetup コマンドを実行する際は、Manager パスのディスク容量が不足していないか確認してください。ディスク容量が不足している場合、次のメッセージを出力して異常終了する問題が発生します。

KNAN11053-E ファイルの読み込みに失敗しました。(ファイル名:instdb.log)

1.4.2 統合監視 DB の設定 (Windows の場合)

統合監視 DB を作成し、インテリジェント統合管理基盤、またはセントラルコンソール機能で統合監視 DB を使用できるように設定します。統合監視 DB を使用しない場合、この手順は不要です。

すでに IM 構成管理 DB をセットアップしているかどうかで、設定の手順が異なります。それぞれの設定手順を次に示します。

(1) すでに IM 構成管理 DB をセットアップしている場合の手順

JP1/IM3-Manager サービスを停止するかどうかで、設定の手順が異なります。それぞれの設定手順を次に示します。

- JP1/IM3-Manager サービスを停止して統合監視 DB を作成する場合の手順

1. IM データベースサービス (JP1/IM3-Manager DB Server) が起動しているか確認する。

2. 次のサービスを停止する。

- JP1/IM3-Manager サービス
- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス

3. jcodbsetup コマンドを実行し、統合監視 DB を作成する。

```
jcodbsetup -s [-q]
```

4. jcoimdef コマンドを実行して、統合監視 DB を有効にする。

```
jcoimdef -db ON
```

5. JP1/IM3-Manager サービスを起動する。

- JP1/IM3-Manager サービスを停止しないで統合監視 DB を作成する場合の手順

1. jcoimdef コマンドを実行して、IM 構成管理サービス (jcfmain) を無効にする。

```
jcoimdef -cf OFF
```

2. JP1/IM3-Manager サービスを再起動する。

3. IM データベースサービス (JP1/IM3-Manager DB Server) が起動しているか確認する。

4. 次のサービスを停止する。

- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス

5. jcodbsetup コマンドを実行し、統合監視 DB を作成する。

```
jcodbsetup -s [-q]
```

6. jcoimdef コマンドを実行して、統合監視 DB を有効にする。

```
jcoimdef -db ON
```

7. jcoimdef コマンドを実行して、IM 構成管理サービス (jcfmain) を有効にする。

```
jcoimdef -cf ON
```

8. JP1/IM3-Manager サービスを再起動する。

jcodbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcodbsetup」(1. コマンド) を参照してください。

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

(2) IM 構成管理 DB をセットアップしていない場合の手順

1. 次のサービスを停止する。

- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス

2. jcodbsetup コマンドを実行し、統合監視 DB を作成する。

```
jcodbsetup -f セットアップ情報ファイル名 [-q]
```

3. jcoimdef コマンドを実行して、統合監視 DB を有効にする。

```
jcoimdef -db ON
```

4. JP1/IM3-Manager サービスを再起動する。

jcodbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcodbsetup」(1. コマンド) を参照してください。

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

1.4.3 IM 構成管理 DB の設定 (Windows の場合)

IM 構成管理 DB を作成し、IM 構成管理サービスをプロセス管理から起動できるように設定します。IM 構成管理の機能を使用しない場合、この手順は不要です。

すでに統合監視 DB をセットアップしているかどうかで、設定の手順が異なります。それぞれの設定手順を次に示します。

(1) すでに統合監視 DB をセットアップしている場合の手順

JP1/IM3-Manager サービスを停止するかどうかで、設定の手順が異なります。それぞれの設定手順を次に示します。

- JP1/IM3-Manager サービスを停止して IM 構成管理 DB を作成する場合の手順

1. IM データベースサービス (JP1/IM3-Manager DB Server) が起動しているか確認する。

2. 次のサービスを停止する。

- JP1/IM3-Manager サービス
- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス

3. jcfdbsetup コマンドを実行して、IM 構成管理 DB を作成する。

```
jcfdbsetup -s [-q]
```

• JP1/IM3-Manager サービスを停止しないで IM 構成管理 DB を作成する場合の手順

1. jcoimdef コマンドを実行して、統合監視 DB を無効にする。

```
jcoimdef -db OFF
```

2. JP1/IM3-Manager サービスを再起動する。

3. IM データベースサービス (JP1/IM3-Manager DB Server) が起動しているか確認する。

4. 次のサービスを停止する。

- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス

5. jcfdbsetup コマンドを実行して、IM 構成管理 DB を作成する。

```
jcfdbsetup -s [-q]
```

6. jcoimdef コマンドを実行して、統合監視 DB を有効にする。

```
jcoimdef -db ON
```

jcfdbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcfdbsetup」(1. コマンド) を参照してください。

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

(2) 統合監視 DB をセットアップしていない場合の手順

1. jcfdbsetup コマンドを実行して、IM 構成管理 DB を作成する。

```
jcfdbsetup -f セットアップ情報ファイル名 [-q]
```

jcfdbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcfdbsetup」(1. コマンド) を参照してください。

1.4.4 IM 構成管理の機能を使用するための設定 (Windows の場合)

JP1/IM - Manager を新規にインストールした場合、IM 構成管理の機能はデフォルトで無効になっています。システム構築時またはシステム運用時に IM 構成管理を使用する場合は、「1.4.3 IM 構成管理 DB の設定 (Windows の場合)」の手順で IM 構成管理 DB を構築したあと、IM 構成管理の機能を有効にする必要があります。

ここでは、IM 構成管理の機能を有効にする手順について説明します。

1. jcoimdef コマンドを実行して、IM 構成管理サービス (jcfmain) を有効にする。

```
jcoimdef -cf ON
```

2. JP1/IM - Manager を再起動する。

3. jco_spmd_status コマンドを実行して、IM 構成管理サービス (jcfmain) が稼働プロセスに表示されていることを確認する。

jcoimdef コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

jco_spmd_status コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jco_spmd_status」(1. コマンド) を参照してください。

1.4.5 IM データベースの更新 (Windows の場合)

JP1/IM - Manager をバージョンアップまたは JP1/IM - Manager の修正版を適用した場合に IM データベースを使用しているときは、IM データベースの更新処理が必要になります。次に示す手順に従い、IM データベースを更新してください。

1. サービスの状態を確認する。

次の状態と異なる場合は、サービスを起動または停止し次の状態にしてください。

- JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスが停止している。
- JP1/OA で JP1/IM3 - Manager から JP1 イベントを取得している場合は、接続元の JP1/OA が停止している。
- JP1/IM3-Manager DB Server サービスが起動している。
- JP1/IM3-Manager サービスが停止している。

2. jimdbupdate コマンドを実行して IM データベースの更新を確認する。

- 次のメッセージが出力された場合は、手順 7 を実行してください。
KNAN11201-I IM データベースサービスは最新の状態です
- 次のどれかのメッセージが出力された場合は、手順 3 以降を実行してください。

KNAN11202-I IM データベースサービスの上書きインストールが必要です
KNAN11207-I IM データベースサービスのテーブルスキーマの更新が必要です
KNAN11211-I IM データベースサービスの設定ファイルの更新が必要です

3. `jimdbbackup` コマンドを実行し、IM データベースをバックアップする。

`jimdbbackup -o バックアップファイル名 -m MAINT`

4. `jimdbupdate` コマンドを実行し、IM データベースを更新する。

`jimdbupdate -i`

5. 次のサービスを停止する。

- JP1/IM3-Manager DB Server サービス

6. 次のサービスを開始する。

- JP1/IM3-Manager DB Server サービス

7. 次のサービスを開始する。

- JP1/IM3-Manager サービス

8. 手順 1 で次のサービスを停止した場合、開始する。

- 接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス
(JP1/IM - MO を使用している場合)
- 接続元の JP1/OA
(JP1/OA で JP1/IM3 - Manager から JP1 イベントを取得している場合)

❗ 重要

`jimdbupdate` コマンドを実行する前に取得した IM データベースの更新前のバックアップデータは、`jimdbupdate` コマンド実行後の IM データベースにリカバリーしないでください。

`jimdbupdate` コマンドを実行したあとは、再度 `jimdbbackup` コマンドでバックアップを取得してください。

1.5 インテリジェント統合管理データベースの構築 (Windows の場合)

インテリジェント統合管理データベースを使用する場合は、JP1/IM - Manager のインストール後、セットアップコマンド (jimgnbdbsetup コマンド) を手動で実行してください。

インテリジェント統合管理データベースを構築することで、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.7.1(1)(a)データベースの構成」に示す各種情報の管理 DB を構築して、各種機能で使用するデータを管理できるようになります。

インテリジェント統合管理データベースを構築する手順について、次に説明します。

1.5.1 インテリジェント統合管理データベースを構築するための準備 (Windows の場合)

インテリジェント統合管理データベースを構築するために必要な定義を記述したインテリジェント統合管理データベースセットアップ情報ファイルを準備します。

マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インテリジェント統合管理データベースセットアップ情報ファイル (jimgnbdbsetupinfo.conf)」(2. 定義ファイル) を参照して、インテリジェント統合管理データベースセットアップ情報ファイルを編集してください。

1.5.2 インテリジェント統合管理データベースの設定 (Windows の場合)

インテリジェント統合管理データベースを作成し、インテリジェント統合管理基盤でインテリジェント統合管理データベースを使用できるように設定します。インテリジェント統合管理データベースを使用しない場合、この手順は不要です。

設定手順を次に示します。

1. jimgnbdbsetup コマンドを実行し、インテリジェント統合管理データベースを作成する。

```
jimgnbdbsetup -f インテリジェント統合管理データベースセットアップ情報ファイル
```

jimgnbdbsetup コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimgnbdbsetup」(1. コマンド) を参照してください。

1.5.3 セキュリティ製品の除外設定 (Windows の場合)

JP1/IM - Manager の起動中にウイルスチェックを実施する場合は、次のファイルおよびフォルダをスキャンの対象から除外してください。また、JP1/IM - Manager の停止中にウイルスチェックを実施して JP1/IM - Manager を再起動する場合は、次のファイルおよびフォルダに対してウイルスチェックが完了したことを確認してください。

JP1/IM - Manager のファイルおよびフォルダ (Windows の場合)

- インテリジェント統合管理データベースの実行ファイルの格納先¥以下すべて※
- インテリジェント統合管理データベースのデータファイルの格納先¥以下すべて※
- インテリジェント統合管理データベースの関連ライブラリの格納先¥以下すべて※
- インテリジェント統合管理データベースの設定ファイルの格納先¥以下すべて※
- インテリジェント統合管理データベースの運用コマンドの格納先¥以下すべて※
- インテリジェント統合管理データベースの運用コマンドの個別ログの格納先¥以下すべて※
- トレンドデータ管理サービスのログの格納先¥以下すべて※

上記の各格納先の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の、「2.7.1 インテリジェント統合管理データベース」の「(1)(d)関連ファイルの格納先」を参照してください。

論理ホスト環境の場合は、共有フォルダ以下もスキャンの対象から除外してください。

- 共有フォルダ¥jp1imm¥以下すべて
- 論理ホストのインテリジェント統合管理データベースのデータファイルの格納先¥以下すべて

注※

インテリジェント統合管理データベースをセットアップしている場合は除外してください。

1.6 サービスの起動順序の設定 (Windows の場合)

JP1/Base の起動管理機能により、各 JP1 のサービスの起動順序を設定します。

1. 起動順序制御の設定をする。

通常はデフォルトのまま運用できますが、例えば、次のような場合は設定をカスタマイズしてください。

- JP1/Power Monitor により起動停止を管理する
- IM データベースを使用する

設定内容の詳細については、マニュアル「JP1/Base 運用ガイド」のサービス起動終了順序の設定の章を参照してください。また、IM データベースの起動については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3.1 JP1/IM - Manager を起動する」を参照してください。

1.7 ユーザー認証の設定およびユーザーマッピングの設定（Windows の場合）

JP1 ユーザー管理に必要な、認証サーバの指定、JP1 ユーザーの登録、ユーザーマッピングの設定をします。
ホストの役割に合わせて、次のように設定します。

表 1-7 ホストの役割ごとの設定項目

設定項目	認証サーバとして使用する		認証サーバとして使用しない	
	プライマリー 認証サーバ	セカンダリー 認証サーバ	マネージャー ホスト	エージェント ホスト
認証サーバ指定	○	○	○	—
JP1 ユーザーの設定	○	—	—	—
操作権限の設定	○	—	—	—
認証サーバ設定のコピー	—	○	—	—
ユーザーマッピング※	○	○	○	○

（凡例）

- ：設定が必要
- ：設定が不要

注※ 自動アクションしない場合、および JP1/IM - View から管理対象ホストにコマンド実行しない場合は不要です。

設定は、GUI の [JP1/Base 環境設定] ダイアログボックスまたは JP1/Base のコマンドにより行います。

また、ユーザーマッピングは、自動アクションまたは JP1/IM - View の操作によってコマンドを実行するすべてのホストで、次のように設定します。

表 1-8 自動アクションや JP1/IM - View によってコマンドを実行する場合のユーザーマッピング

操作	JP1 ユーザー名	サーバホスト名	OS ユーザー名
JP1/IM - View からコマンドを実行する場合	マネージャーにログインするユーザー	JP1/IM - View が接続するマネージャー※	コマンド実行先ホストの OS に登録されたユーザー
自動アクションを実行する場合	アクション定義で指定したユーザー名	自動アクションを定義したマネージャー※	アクション実行先ホストの OS に登録されたユーザー

注※ サーバホスト名には「*」も指定できます。この場合は、すべてのホストでユーザーマッピングが許可されます。

なお、「jpladmin」という JP1 ユーザーがデフォルトで登録されています。「jpladmin」には、JP1 資源グループが「*」で、JP1 権限レベルが JP1_Console_Admin である操作権限が設定されています（JP1 資源グループが「*」の場合、すべての JP1 資源グループにアクセスできます）。

1.7.1 認証サーバの指定 (Windows の場合)

認証サーバのホスト名を指定します。この設定は、認証サーバのホストおよび JP1/IM のマネージャーが必要です。エージェントでは必要ありません。

1. 認証サーバを指定する。

〔認証サーバ〕 タブの 〔認証サーバの検索順序〕 で指定します。

認証サーバはプライマリー、セカンダリーの 2 台まで設定できます。

設定方法の詳細については、マニュアル「JP1/Base 運用ガイド」のユーザー管理機能の設定の章を参照してください。

1.7.2 JP1 ユーザーの登録 (Windows の場合)

JP1/IM を使用する JP1 ユーザーを登録します。この設定は、プライマリー認証サーバのホストが必要です。

1. JP1 ユーザーを登録する。

〔認証サーバ〕 タブの 〔JP1 ユーザー〕 で、JP1 ユーザーとパスワードを登録します。

1.7.3 JP1 ユーザーの操作権限の設定 (Windows の場合)

JP1/IM を使用する JP1 ユーザーに操作権限を登録します。この設定は、プライマリー認証サーバのホストが必要です。

1. JP1 ユーザーに操作権限を設定する。

〔認証サーバ〕 タブの 〔JP1 資源グループ別権限レベル〕 で、JP1 ユーザーの操作権限を設定します。

JP1/IM の操作権限としては、JP1 資源グループに JP1_Console、権限レベルに JP1_Console_Adminなどを指定します。

なお、IM 構成管理の操作権限としては、JP1 資源グループに JP1_Console、権限レベルに JP1/IM の権限レベルと IM 構成管理の権限レベルを設定する必要があります。IM 構成管理の権限レベルを設定していない場合、実行できる操作は、IM 構成管理の JP1 権限レベル「JP1_CF_User」の範囲に限定されます。

JP1/IM の操作権限については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「9.4.1 JP1 ユーザーの管理」および「付録 E 操作権限一覧」を参照してください。

1.7.4 プライマリー認証サーバの設定情報のコピー (Windows の場合)

プライマリー認証サーバから認証サーバの設定ファイルをコピーします。この設定は、セカンダリー認証サーバのホストが必要です。

1. 認証サーバの設定ファイルをコピーする。

Base パス¥conf¥user_acl¥フォルダに格納されている設定ファイルJP1_Group, JP1_Passwd, JP1_UserLevel をコピーします。テキストファイルのため、FTP で ASCII 転送するなどコピーします。

1.7.5 ユーザーマッピングの設定 (Windows の場合)

自動アクションや JP1/IM - View の操作によって、コマンドを実行するホストで、JP1 ユーザー名と OS ユーザー名とのユーザーマッピングを設定します。この設定は、JP1/IM からコマンドを実行するすべてのホストが必要です。

1. OS ユーザー名とパスワードを登録する。

[ユーザーマッピング] タブの [パスワード管理] で登録します。

2. JP1 ユーザー名とホスト名を設定する。

[ユーザーマッピング] タブの [JP1 ユーザー] で設定します。

3. JP1 ユーザーと OS ユーザーをマッピングする。

[JP1 ユーザー] ダイアログボックスで [OK] ボタンをクリックして、[マッピング OS ユーザー詳細] ダイアログボックスを表示し、ユーザーマッピングを設定します。

なお、ユーザーが複数いる場合は、すべてのユーザーに対してユーザーマッピングの設定が必要です。JP1 ユーザー名と OS ユーザー名が同じ場合でも、ユーザーマッピングの設定が必要です。

また、自動アクションや JP1/IM - View の操作によって実行されるコマンドは、JP1 ユーザーにマッピングされているプライマリーユーザーで実行されます。特定の OS ユーザーでコマンドを実行したい場合には、その OS ユーザーをプライマリーユーザーとして登録してください。

ユーザーマッピングの詳細については、マニュアル「JP1/Base 運用ガイド」のユーザー管理機能の設定の説明を参照してください。

1.8 JP1/Base の障害に備えた設定 (Windows の場合)

JP1/Base は、JP1/Base 自身の障害がシステム運用に影響を及ぼすのをできるだけ防ぐために、次の機能を提供しています。

- プロセスの異常を検知する機能（ヘルスチェック機能）
- プロセスが異常終了した場合に自動で再起動する機能
- プロセスや認証サーバの異常を検知した場合に JP1 イベントを発行する機能
- JP1/Base の障害発生時に調査資料を採取するツール

デフォルトではプロセスの異常検知や再起動、JP1 イベントの発行もしない設定になっています。設定を変更する場合は、マニュアル「JP1/Base 運用ガイド」のインストールとセットアップの章の説明を参照してください。

また、JP1/Base では、トラブルシュート資料を迅速に採取できるよう、資料採取ツールを提供しています。

JP1/Base の資料採取ツールで採取できる資料については、マニュアル「JP1/Base 運用ガイド」を参照してください。なお、JP1/Base の資料採取ツールで採取できる資料にはメモリーダンプ、クラッシュダンプがあります。これらのダンプは、あらかじめ出力されるよう、設定しておく必要があります。詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

1.9 IM 構成管理を使用する場合のシステムの階層構成の設定 (Windows の場合)

ここでは、IM 構成管理を使用する場合のシステムの階層構成 (IM 構成) の設定について説明します。IM 構成管理を使用しない場合のシステムの階層構成の設定については、「[1.10 IM 構成管理を使用しない場合のシステムの階層構成の設定 \(Windows の場合\)](#)」を参照してください。

IM 構成管理を使用する場合は、IM 構成管理・ビューアーを操作して、JP1/IM が運用管理するシステムのマネージャーおよびエージェントの階層関係を設定します。

また、IM 構成管理のエクスポート・インポート機能を使用して、テスト環境のシステム構成を運用環境に移行したり、変更前の環境のシステム構成を変更後の環境に移行したりできます。

IM 構成管理のエクスポート・インポート機能を使用すると、仮想ホストを含むシステムの階層構成 (仮想化システム構成) を IM 構成管理で管理するための設定や、セントラルスコープで監視するための設定ができます。

IM 構成管理を使用してシステムの階層構成を管理している場合、次の処理を実行すると、IM 構成管理が保持する構成定義情報と JP1/Base が保持する構成定義情報が不一致となります。

- JP1/Base の構成定義ファイルを編集する
- `jbsrt_distrib` コマンドを実行する

そのため、IM 構成管理を使用してシステムの階層構成を管理している場合は、IM 構成管理を使用して構成を一元管理することを推奨します。

JP1/Base が提供する機能を使用してシステムの階層構成の定義の配布をした場合は、IM 構成管理と JP1/Base で保持する構成定義情報を一致させるために、システムの階層構成を取得する必要があります。システムの階層構成の取得がされていない場合、構成定義情報が不一致のため、動作が不正になります。

1.9.1 IM 構成管理・ビューアーによる設定 (Windows の場合)

ここでは、IM 構成管理・ビューアーを操作して、システムの階層構成を設定する方法について説明します。

IM 構成管理を使用していない既存の JP1/IM システムに IM 構成管理を追加した場合、IM 構成管理・ビューアーを使用すると、既存の JP1/IM のシステムから収集した構成定義情報を編集して、システムの階層構成を設定できます。

ここでは、新規にシステムの階層構成を設定する場合、および既存のシステムの階層構成を編集する場合の手順について説明します。

(1) 新規にシステムの階層構成を設定する場合

システムの階層構成は、最上位のマネージャーで一括して定義する方法と、各マネージャーが管理する複数の部分に分割して定義する方法があります。

システムの階層構成の管理および構成定義情報の定義例については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.2.1 IM 構成管理で管理対象となるシステムの階層構成」を参照してください。

新規にシステムの階層構成を設定する手順を次に示します。

1. システムの階層構成に追加するホストを、IM 構成管理の管理対象として登録する。

- ホストを登録する方法、およびホストに関する情報を設定する方法については、「[3.1.1 ホストを登録する](#)」を参照してください。
- 登録したホストに関する情報を参照する方法については、「[3.1.4 ホスト情報を表示する](#)」を参照してください。
- ホストを削除する方法については、「[3.1.6 ホストを削除する](#)」を参照してください。
- 登録したホストに関する情報を変更する方法については、「[3.1.5 ホスト情報の属性を変更する](#)」を参照してください。

2. IM 構成管理に登録したホストをシステムの階層構成に追加して、マネージャーとエージェントの階層関係を設定する。

- JP1/IM のシステムにホストを追加する方法については、「[3.2.4\(1\)\(a\) ホストを追加する](#)」を参照してください。
- マネージャーとエージェントの階層関係を設定する方法については、「[3.2.4\(1\)\(b\) ホストを移動する](#)」を参照してください。
- JP1/IM のシステムからホストを削除する方法については、「[3.2.4\(1\)\(c\) ホストを削除する](#)」を参照してください。

3. 設定したシステムの階層構成をシステムに反映する。

IM 構成管理・ビューアーで設定したシステムの階層構成を、JP1/IM が運用管理するシステムに反映します。

- 設定したシステムの階層構成をシステムに反映する方法については、「[3.2.4\(3\) システムの階層構成を IM 構成管理が管理するシステムに反映する](#)」を参照してください。
- 設定したシステムの階層構成を確認する方法については、「[3.2.2 システムの階層構成を表示する](#)」を参照してください。

システムの階層構成を統合マネージャーと拠点マネージャーに分割して定義する場合は、マネージャーごとに上記の手順を行ってください。そのあとに、統合マネージャーに接続した IM 構成管理ビューアーで次の手順を実施して、システム全体の定義を作成します。

1. システムの階層構成の同期を取る。

統合マネージャーと拠点マネージャーの間で、構成定義情報の同期を取ります。

システムの階層構成の同期を取る方法については、「[3.2.5 システムの階層構成の同期を取る](#)」を参照してください。

(2) 既存のシステムの階層構成を編集する場合

構成管理情報の設定方法を JP1/Base が提供する構成管理機能から IM 構成管理に切り替える場合の手順を次に示します。

1. IM 構成管理・ビューアーの [IM 構成管理] 画面から既存の JP1/IM の構成定義情報を読み込んで、システムの階層構成を取得する。

取得した構成定義情報が IM 構成管理 DB に保存され、自動的にホストの登録が実施されます。

詳細は、「[3.2.1 システムの階層構成を取得する](#)」を参照してください。

2. [ホスト属性編集] 画面から登録されたホスト属性を確認し、必要に応じてホスト名やホスト種別を編集する。

詳細は、「[3.1.5 ホスト情報の属性を変更する](#)」を参照してください。

3. [IM 構成管理] 画面からホスト情報を収集する。

詳細は、「[3.1.3 ホストから情報を収集する](#)」を参照してください。

4. [IM 構成管理] 画面から収集したホスト情報を確認する。

ホスト情報として下位ホスト情報、基本情報、製品情報、およびサービス情報を確認できます。

詳細は、「[3.1.4 ホスト情報を表示する](#)」を参照してください。

5. [IM 構成管理] 画面からシステムの階層構成を確認し、必要に応じて編集する。

システムの階層構成を編集した場合は、必ずシステムの階層構成を反映してください。

詳細は、「[3.2.2 システムの階層構成を表示する](#)」, 「[3.2.4 システムの階層構成を編集する](#)」, および「[3.2.4\(3\) システムの階層構成を IM 構成管理が管理するシステムに反映する](#)」を参照してください。

6. [IM 構成管理] 画面からプロファイル情報を収集する。

エージェントの各サービスで現在使用されている設定情報とエージェントに保存されている設定ファイルが収集されます。

詳細は、「[3.5.1\(2\) プロファイルを収集する](#)」を参照してください。

7. [IM 構成管理] 画面からプロファイル情報を確認し、必要に応じて設定ファイルを編集する。

設定ファイルを編集した場合は、必ず設定ファイルの編集内容を反映してください。また、反映後に手順 6 を実施し、プロファイル情報を確認してください。

詳細は、「[3.5.1\(3\) プロファイルを表示する](#)」, 「[3.5.1\(5\) 設定ファイルを編集する](#)」, および「[3.5.1\(6\) 設定ファイルの編集内容を反映する](#)」を参照してください。

1.9.2 エクスポート・インポート機能による設定 (Windows の場合)

IM 構成管理のエクスポート・インポート機能を使用すると、テスト環境のシステム構成を運用環境に移行したり、環境を変更する前のシステムの階層構成 (IM 構成) を変更後の環境に移行したりできます。エクスポート・インポート機能によってシステムの階層構成を設定する方法については、「[3.6 IM 構成管理の管理情報のインポート・エクスポート](#)」を参照してください。

1.9.3 仮想化システム構成の管理および監視のための設定 (Windows の場合)

IM 構成管理のエクスポート・インポート機能を使用すると、仮想化システム構成の構成定義情報を IM 構成管理で管理したり、仮想化システム構成をセントラルスコープで監視したりできます。仮想化システム構成を管理および監視するための環境を設定する方法については、「[3.3 仮想化システム構成の設定](#)」を参照してください。

1.10 IM 構成管理を使用しない場合のシステムの階層構成の設定 (Windows の場合)

ここでは、IM 構成管理を使用しない場合のシステムの階層構成 (IM 構成) の設定について説明します。IM 構成管理を使用する場合のシステムの階層構成の設定については、「[1.9 IM 構成管理を使用する場合のシステムの階層構成の設定 \(Windows の場合\)](#)」を参照してください。

IM 構成管理を使用しない場合は、JP1/Base が提供する構成管理機能を使用して、JP1/IM が運用管理するシステムのマネージャーおよびエージェントの階層関係を設定します。

システムの階層構成は、最上位のマネージャーで一括して定義する方法と、各マネージャーが管理する複数の部分に分割して定義する方法があります。

IM 構成管理を使用してシステムの階層構成を管理している場合は、JP1/Base が提供する構成管理機能の定義ファイルを編集したり、コマンドを実行したりしないでください。

システムの階層構成の管理および構成定義情報の定義例については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「[9.4.3 システムの階層構成の管理](#)」を参照してください。

1.10.1 構成定義情報の設定 (Windows の場合)

構成定義情報は、次の手順で設定します。

1. マネージャーで、構成定義ファイル (jbs_route.conf) を作成する。

システムを一括して定義する場合はシステム階層構成全体を、分割して定義する場合はそのマネージャーから下位に当たる管理対象ホストおよびマネージャーを、定義ファイルに記述します。

2. マネージャーで、設定コマンド (jbsrt_distrib) を実行する。

コマンドを実行すると、定義情報が更新されます。

システム階層構成を複数の部分に分割して定義する場合は、マネージャーごとに上記の手順を行ってください。そのあとに、最上位のマネージャーで次の手順を実施してシステム全体の定義を作成します。

1. 最上位のマネージャーで、構成定義ファイル (jbs_route.conf) を作成する。

最上位のマネージャーから次の階層のマネージャーまでのシステム階層構成を、定義ファイルに記述します。

2. 最上位のマネージャーで、設定コマンド (jbsrt_sync) を実行する。

なお、構成定義情報の内容を確認するには、各ホスト上で jbsrt_get コマンドを実行してください。

構成定義ファイル、jbsrt_distrib コマンドおよび jbsrt_sync コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

IM 構成管理を使用している場合は、[IM 構成管理] 画面から [IM 構成取得] を実行してください。

1.10.2 構成定義情報の削除 (Windows の場合)

構成定義情報を一度クリアするなど、定義を削除できます。

1. マネージャーで、構成定義ファイル (jbs_route.conf) を用意する。

構成定義ファイルがない場合は、自ホスト名だけを記述したファイルを作成してください。

既存のファイルがある場合は、そのまま使用します。

2. マネージャーで、設定コマンド (jbsrt_distrib) を実行する。

なお、JP1/Base が停止していて構成定義情報が削除されなかったホストがある場合は、そのホストで jbsrt_del コマンドを実行して構成定義情報を削除します。そのあと、最上位のマネージャーで jbsrt_distrib コマンドを実行してください。

jbsrt_del コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

1.10.3 構成定義情報の変更 (Windows の場合)

構成定義情報を変更する場合は、「[1.10.1 構成定義情報の設定 \(Windows の場合\)](#)」と同じ手順で設定してください。これによって、変更後の構成定義情報が配布されます。

最上位のマネージャーを変更する場合

システムの最上位のマネージャーを変更する場合は、次の手順で変更してください。

1. 変更前の最上位のマネージャーで、構成定義情報を削除する。

変更前の最上位のマネージャーで、「[1. 10.2 構成定義情報の削除 \(Windows の場合\)](#)」の削除手順により構成定義情報を削除します。

2. 変更後の最上位のマネージャーで、構成定義情報を設定する。

変更後の最上位のマネージャーで、「[1. 10.1 構成定義情報の設定 \(Windows の場合\)](#)」の設定手順により、構成定義情報を設定します。

1.10.4 構成定義情報の設定での注意事項 (Windows の場合)

構成定義情報を配布するときは、各ホストで JP1/Base が動作している必要があります。JP1/Base が停止していた場合の影響と対処方法を説明します。

• JP1/Base が停止していた場合の影響

構成定義情報は、JP1/Base により管理されています。このため、構成定義情報で定義したホストの JP1/Base が停止していると、構成定義情報の配布に失敗します。この場合、次のように対処してください。

1. `jbsrt_distrib` コマンド実行時に KAVB3107-E のメッセージが表示されても、そのまま処理を続行する。

JP1/Base が起動しているホストには構成定義情報が配布されます。

2. 定義を配布できなかったホストの JP1/Base を起動してから、再度 `jbsrt_distrib` コマンドを実行する。

- JP1/Base イベントサービスが停止していた場合の影響

構成定義情報は JP1 イベント転送に関連するため、`jbsrt_distrib` コマンドや `jbsrt_del` コマンドを実行した時に、`jevreload` コマンドが自動的に実行され、イベントサービスの転送設定が更新（リロード）されます。このリロードのとき、イベントサービスが停止していると、構成定義情報が配布されても JP1 イベントの転送先は更新されません。この場合は、イベントサービスを再起動してください。

なお、構成定義情報については、マニュアル「JP1/Base 運用ガイド」を参照してください。

1.11 イベントサービス機能の設定 (Windows の場合)

JP1/IM で JP1 イベントにより事象を管理するために、各ホストを設定します。

1. イベントサービス環境の設定をする。

通常はデフォルトの設定のまま運用できますが、例えば、次のような場合は設定をカスタマイズしてください。

- イベント DB の容量を大きくする
- JP1/SES 形式のイベントを JP1/IM で管理する

また、JP1/IM - Manager は、JP1/Base (イベントサービス) からユーザー名 **SYSTEM** および **root** で JP1 イベントを取得します。同一ホスト上で動作する JP1/Base (イベントサービス) のイベントサーバ設定ファイル (conf) で **users** パラメーターを指定する場合には、**SYSTEM** および **root** を含める設定としてください。含めなかった場合、JP1/IM - Manager が正常に起動できなくなります。

2. イベント変換機能の設定をする。

ログファイル、SNMP トラップ、Windows イベントログを JP1 イベントにより管理する場合は、イベント変換機能の設定をしてください。

設定内容の詳細については、マニュアル「JP1/Base 運用ガイド」イベントサービス環境の設定の章、およびイベント変換機能の章を参照してください。

❗ 重要

JP1/IM - Manager が動作するホストの API 設定ファイルでは、通信タイプに必ず **keep-alive** を指定してください。通信タイプに **close** を指定すると、JP1/IM - Manager がイベントを 1 件受信するたびに一時ポートを一つ使用するため、一時ポートの不足が発生する場合があります。

1.12 IM 構成管理を使用する場合の JP1 イベントの転送設定 (Windows の場合)

ここでは、IM 構成管理を使用する場合の JP1 イベントの転送設定について説明します。

IM 構成管理を使用する場合は、IM 構成管理・ビューアーを操作して、JP1 イベントの転送設定を実行します。

JP1 イベントの転送設定では、JP1/IM で管理する JP1 イベントを、上位の JP1/IM マネージャーに転送するように、各ホストを設定します。

通常はデフォルトのまま運用できますが、例えば、次のような場合は設定をカスタマイズしてください。

- JP1 イベントの重大度の通知や情報のイベントを JP1/IM で管理する
- JP1/SES 形式のイベントを JP1/IM で管理する

なお、デフォルトの設定では、「[1.9 IM 構成管理を使用する場合のシステムの階層構成の設定 \(Windows の場合\)](#)」で設定する階層定義に従ってイベントが転送されます。

IM 構成管理を使用する場合、[プロファイル表示/編集] 画面の [設定ファイル] ページで、イベント転送情報の設定ファイルを編集して、イベント転送設定を変更できます。設定ファイルを編集する方法については、「[3.5.1\(5\) 設定ファイルを編集する](#)」を参照してください。

1.13 IM 構成管理を使用しない場合の JP1 イベントの転送設定 (Windows の場合)

ここでは、IM 構成管理を使用しない場合の JP1 イベントの転送設定について説明します。

IM 構成管理を使用しない場合は、JP1/Base が提供する構成管理機能を使用して、JP1 イベントの転送設定を実行します。

JP1 イベントの転送設定では、JP1/IM で管理する JP1 イベントを、上位の JP1/IM マネージャーに転送するように、各ホストを設定します。

通常はデフォルトのまま運用できますが、例えば、次のような場合は設定をカスタマイズしてください。

- JP1 イベントの重大度の通知や情報のイベントを JP1/IM で管理する
- JP1/SES 形式のイベントを JP1/IM で管理する

なお、デフォルトの設定では、「[1.10 IM 構成管理を使用しない場合のシステムの階層構成の設定 \(Windows の場合\)](#)」で設定する階層定義に従ってイベントが転送されます。

設定内容の詳細については、マニュアル「JP1/Base 運用ガイド」の転送設定ファイルの詳細の章を参照してください。

1.14 IM 構成管理を使用する場合のイベントサービスの定義情報の収集と配布 (Windows の場合)

ここでは、IM 構成管理を使用する場合のイベントサービスの定義情報の収集と配布について説明します。

IM 構成管理を使用する場合は、IM 構成管理・ビューアーを操作して、イベントサービスの定義情報の収集と配布を実行します。

JP1/Base と JP1/IM で構成されたシステムでは、バージョン 9 以降の JP1/Base が動作するホストとの間で、マネージャーから複数のホストのイベントサービスの定義情報を一括して収集したり、複数のホストへイベントサービスの定義情報を配布したりできます。そのため、イベントサービスの定義情報を各ホストで確認したり、定義したりすることなく、マネージャー上で各ホストの定義情報を集中的に管理できます。

IM 構成管理を使用する場合に収集、配布できるのは、次の定義情報です。

- 転送設定ファイル
- ログファイルトラップ動作定義ファイル
- ログファイルトラップ起動定義ファイル
- イベントログトラップ動作定義ファイル
- ローカルアクションの定義ファイル

IM 構成管理を使用する場合、[IM 構成管理] 画面の [ホスト一覧] ページまたは [IM 構成] ページで、プロファイル (有効設定情報および設定ファイル) の収集を実行して、イベントサービスの定義情報を収集できます。プロファイルを収集する方法については、[\[3.5.1\(2\) プロファイルを収集する\]](#) を参照してください。

また、IM 構成管理を使用する場合、[IM 構成管理] 画面の [ホスト一覧] ページまたは [IM 構成] ページで、設定ファイルの編集内容の反映を実行して、イベントサービスの定義情報を、JP1/Base が動作するホストに配布できます。設定ファイルの編集内容を反映する方法については、[\[3.5.1\(6\) 設定ファイルの編集内容を反映する\]](#) を参照してください。

1.15 IM 構成管理を使用しない場合のイベントサービスの定義情報の収集と配布 (Windows の場合)

ここでは、IM 構成管理を使用しない場合のイベントサービスの定義情報の収集と配布について説明します。

IM 構成管理を使用しない場合は、JP1/Base が提供する定義収集・配布機能を使用して、イベントサービスの定義情報の収集と配布を実行します。

JP1/Base と JP1/IM で構成されたシステムでは、マネージャーから複数のホストのイベントサービスの定義情報を一括して収集したり、複数のホストへイベントサービスの定義情報を配布したりできます。そのため、イベントサービスの定義情報を各ホストで確認したり、定義したりすることなく、マネージャー上で各ホストの定義情報を集中的に管理できます。

IM 構成管理を使用しない場合の収集方法、配布方法の詳細については、マニュアル「JP1/Base 運用ガイド」のイベントサービスの定義情報の収集と配布の章を参照してください。

1.16 コマンド実行環境の設定 (Windows の場合)

コマンド実行環境の設定について、管理対象ホストのコマンド実行環境の設定と、クライアントアプリケーションの実行環境の設定に分けて説明します。

1.16.1 管理対象ホストのコマンド実行機能の設定 (Windows の場合)

自動アクション機能および JP1/IM - View の [コマンド実行] 画面から管理対象ホストのコマンドを実行するときの、コマンド実行環境を設定します。

1. コマンド実行環境の設定

`jcocmddef` コマンドを実行して、コマンド実行環境を設定します。

コマンド同時実行数の調整をすることを推奨します。この場合は、次のようにコマンドを実行します。

(例) コマンド同時実行数を 3 にする場合

```
jcocmddef -execnum 3
```

2. 環境変数ファイルの作成

コマンド実行時に環境変数ファイルを使用する場合は、ファイルを作成します。

3. ホストグループの定義

必要に応じて、ホストグループ（同時に複数のホストにコマンド実行を指示するためのグループ）を定義します。

4. コマンドボタン定義ファイルの作成

コマンドを [コマンド] ボタンから実行する場合は、コマンドボタン定義ファイルを作成します。

イベント情報を引き継ぐ場合は、`inev` パラメーターに `true` を設定してください。

5. イベント引き継ぎ情報変換設定ファイルの作成

自動アクションおよびコマンド実行でイベント情報を引き継ぐ場合、引き継がれるイベント情報に含まれる特定の ASCII 文字を別の文字列に変換するときは、イベント引き継ぎ情報変換設定ファイルを作成します。

なお、コマンド実行環境設定が有効になる契機や、定義ファイルの作成方法などについては、次の説明を参照してください。

コマンド実行環境について

- `jcocmddef` コマンドについて
参照先：マニュアル「JP1/Base 運用ガイド」のコマンドを説明している章
- 環境変数ファイルの作成について
参照先：マニュアル「JP1/Base 運用ガイド」の環境変数ファイルを説明している章

- ホストグループの定義について
参照先：マニュアル「JP1/Base 運用ガイド」のホストグループの定義ファイルを説明している章
- コマンドボタン定義ファイルの作成について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「コマンドボタン定義ファイル (cmdbtn.conf)」(2. 定義ファイル)
- イベント引き継ぎ情報変換設定ファイルの作成について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベント引き継ぎ情報変換設定ファイル (event_info_replace.conf)」(2. 定義ファイル)

1.16.2 クライアントアプリケーションの実行環境の設定 (Windows の場合)

JP1/IM - View の「コマンド実行」画面からクライアントアプリケーションを実行するときの、コマンド実行環境を設定します。

1. コマンドボタン定義ファイルの作成

クライアントアプリケーションを「コマンド」ボタンから実行する場合は、コマンドボタン定義ファイルを作成します。

イベント情報を引き継ぐ場合は、inev パラメーターにtrue を設定してください。また、cmdtype パラメーターにclient を設定してください。

2. イベント引き継ぎ情報変換設定ファイルの作成

自動アクションおよびコマンド実行でイベント情報を引き継ぐ場合、引き継がれるイベント情報に含まれる特定の ASCII 文字を別の文字列に変換するときは、イベント引き継ぎ情報変換設定ファイルを作成します。

なお、コマンド実行環境設定が有効になる契機や、定義ファイルの作成方法などについては、次の説明を参照してください。

コマンド実行環境について

- コマンドボタン定義ファイルの作成について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「コマンドボタン定義ファイル (cmdbtn.conf)」(2. 定義ファイル)
- イベント引き継ぎ情報変換設定ファイルの作成について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベント引き継ぎ情報変換設定ファイル (event_info_replace.conf)」(2. 定義ファイル)

1.17 イベントサービスの登録ホスト名を FQDN 形式で利用する場合の設定 (Windows の場合)

JP1/IM - Manager はイベントサービスの登録ホスト名を FQDN 形式で利用する運用に対応しています。イベントサービスの登録ホスト名を FQDN 形式で利用することで、複数のドメインで構成されたシステムで JP1 イベントを監視できます。

ここでは、マネージャー上のイベントサービスの登録ホスト名を FQDN 形式で利用する場合の前提条件、設定方法、および起動方法について説明します。エージェント上のイベントサービスの登録ホスト名を FQDN 形式で利用する場合、ここで説明する設定は不要です。

1.17.1 前提条件 (Windows の場合)

JP1/IM ホスト上の JP1/Base イベントサービスの登録ホスト名を FQDN 形式で利用する場合は、次の前提条件を満たす必要があります。

- 物理ホストの環境であること。
- JP1/IM - Manager ホスト上で `hostname` コマンドを実行して、ショートネーム形式のホスト名が返されること。

1.17.2 設定方法 (Windows の場合)

JP1/IM3-Manager サービスと JP1/Base Event サービスの依存関係を解除する必要があります。JP1/Base で FQDN 形式のイベントサーバを設定後、次の手順でサービスの依存関係を解除してください。

1. コマンドプロンプトから次のコマンドを実行して、JP1/IM3-Manager サービスと JP1/Base Event サービスの依存関係を解除する。

```
SpmSetSvcCon -setdepend no
```

FQDN 形式のイベントサーバの設定については、マニュアル「JP1/Base 運用ガイド」の次に示す説明を参照してください。

- DNS を使ったシステムでのイベントサーバの設定
- イベントサービスの注意事項

`SpmSetSvcCon` コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`SpmSetSvcCon` (Windows 限定)」(1. コマンド)を参照してください。

1.17.3 起動方法 (Windows の場合)

JP1/IM3-Manager サービスは FQDN 形式の JP1/Base Event サービスと依存関係を設定していないため、JP1/IM3-Manager サービスを起動する前に FQDN 形式の JP1/Base Event サービス、JP1/Base サービスを起動しておく必要があります。

次の順序でサービスを起動してください。

1. JP1/Base Event_FQDN ホスト名 サービスを起動する。
2. JP1/Base サービスを起動する。
3. JP1/IM3-Manager サービスを起動する。

1.18 リモートの監視対象ホストでログ監視をするための設定 (Windows の場合)

ここでは、リモートの監視対象ホストでログ監視をするための WMI, NetBIOS (NetBIOS over TCP/IP), および SSH の設定について説明します。

なお、リモートの監視対象ホストから収集できるログの種別とリモート通信の接続方法については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「13.5.2 リモート監視構成の管理」を参照してください。

また、リモートの監視対象ホストを IM 構成管理に登録する手順については、「3.1 ホストの登録」を参照してください。

メモ

リモート監視が停止している間にリモート監視対象ホストで出力されたログ情報を収集できません。リモート監視が停止中に出力されたログ情報を収集するかどうかは、リモートログトラップ環境定義ファイル (jp1cf_remote_logtrap.conf) の START_OPTION パラメーターで指定します。なお、新規にインストールした場合は、有効です。11-01 以前からバージョンアップした場合は無効です。必要に応じて、リモートログトラップ環境定義ファイルを設定してください。

リモートログトラップ環境定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「リモートログトラップ環境定義ファイル (jp1cf_remote_logtrap.conf)」(2. 定義ファイル) を参照してください。

1.18.1 WMI の設定 (Windows の場合)

ここでは、WMI の設定について説明します。

WMI の接続には次の設定が必要となります。

- DCOM の設定

JP1/IM - Manager ホストとリモートの監視対象ホストの両方で設定が必要です。

なお、JP1/IM - Manager ホストをクラスタシステムで運用する場合は、実行系ノードと待機系ノードの両方で設定してください。

- ファイアウォールの設定

リモートの監視対象ホストで設定します。必要に応じて設定してください。

設定が完了したら、JP1/IM - Manager ホストからリモートの監視対象ホストに接続できることを確認してください。

注意事項

- リモートの監視対象ホストの OS のシステム管理情報を提供する Windows Management Instrumentation サービス（サービス名：WinMgmt）のスタートアップの種類が「無効」に設定されている場合は収集できません。
- リモートの監視対象ホストに接続するユーザーは、リモートの監視対象ホストの Administrators グループのメンバーに設定されている必要があります。

(1) DCOM を設定する

JP1/IM - Manager ホストとリモートの監視対象ホストで DCOM を設定する方法について説明します。

(a) JP1/IM - Manager ホストでの設定をする

JP1/IM - Manager ホストで、DCOM を設定します。

DCOM の設定手順について次に示します。

なお、リモートの監視対象ホストの OS の環境によっては、一部の実施手順が異なることがあります。

例えば、リモートの監視対象ホストの OS が Windows Server 2008 の場合、Windows の [スタート] メニューに [ファイル名を指定して実行] が表示されない場合があります。その場合は、[Windows] + [r] キーを押して呼び出すなどして表示してください。

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択する。
2. [dcomcnfg.exe] を入力し、[OK] ボタンをクリックする。
[コンポーネントサービス] 画面が表示されます。
3. [コンポーネントサービス] 画面の [コンポーネントサービス] と [コンピュータ] をクリックし、ツリーを展開する。
4. [マイコンピュータ] を右クリックし、表示されたメニューから [プロパティ] を選択する。
[マイコンピュータのプロパティ] 画面が表示されます。
5. [既定のプロパティ] タブを選択して、[このコンピュータ上で分散 COM を有効にする] チェックボックスをチェックする。
6. [OK] ボタンをクリックする。
[マイコンピュータのプロパティ] 画面が閉じます。
7. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択する。
8. [gpedit.msc] を入力し、[OK] ボタンをクリックする。
[グループポリシー] 画面が表示されます。

9. [グループポリシー] 画面の [コンピュータの構成] - [管理用テンプレート] - [システム] - [ユーザープロファイル] をクリックし、ツリーを展開する。
10. 「ユーザーのログオフ時に強制的にユーザーレジストリをアンロードしない」を有効にする。
11. マシンを再起動する。

(b) リモートの監視対象ホストでの設定をする

リモートの監視対象ホストで、DCOM を設定します。

DCOM の設定手順を次に示します。

なお、リモートの監視対象ホストの OS の環境によって、次のように一部の実施手順が異なることがあります。

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択する。
2. [dcomcnfg.exe] を入力し、[OK] ボタンをクリックする。
[コンポーネントサービス] 画面が表示されます。
3. [コンポーネントサービス] 画面の [コンポーネントサービス] と [コンピュータ] をクリックし、ツリーを展開する。
4. [マイコンピュータ] を右クリックし、表示されたメニューから [プロパティ] を選択する。
[マイコンピュータのプロパティ] 画面が表示されます。
5. [既定のプロパティ] タブを選択し、[このコンピュータ上で分散 COM を有効にする] チェックボックスをチェックする。
6. [COM セキュリティ] タブを選択して、[アクセス許可] の [制限の編集] ボタンをクリックする。
[アクセス許可] 画面が表示されます。
[アクセス許可] 画面の [グループ名またはユーザー名] に、リモートの監視対象ホストに接続するユーザー、またはユーザーが属するグループが表示されているかどうかを確認してください。
表示されていない場合は、[追加] ボタンをクリックして、ユーザーまたはユーザーが属するグループを追加してください。
7. [ユーザーまたはグループの選択] のリモートの監視対象ホストに接続するユーザーまたはユーザーが属するグループを選択する。
「リモートアクセス」の [許可] がチェックされているかどうか確認してください。チェックが外されている場合は、チェックしてください。
8. [OK] ボタンをクリックする。
[アクセス許可] 画面が閉じます。

9. [COM セキュリティ] タブを選択し、[起動とアクティブ化のアクセス許可] の [制限の編集] ボタンをクリックする。
[起動とアクティブ化のアクセス許可] 画面が表示されます。
[グループ名またはユーザー名] に、リモートの監視対象ホストに接続するユーザー、またはユーザーが属するグループが表示されているかどうかを確認してください。
表示されていない場合は、[追加] ボタンをクリックし、ユーザーまたはユーザーが属するグループを追加してください。
10. [起動とアクティブ化のアクセス許可] 画面の [ユーザーまたはグループの選択] のリモートの監視対象ホストに接続するユーザーまたはユーザーが属するグループを選択する。
[リモートからの起動] と [リモートからのアクティブ化] の [許可] がチェックされているかどうか確認してください。チェックが外されている場合は、チェックしてください。
11. [OK] ボタンをクリックする。
[マイコンピュータのプロパティ] 画面に戻ります。
12. [OK] ボタンをクリックする。
[マイコンピュータのプロパティ] 画面が閉じます。
13. マシンを再起動する。
[このコンピュータ上で分散 COM を有効にする] の設定を変更していない場合、この作業は不要です。

(2) ファイアウォールを設定する

この設定は、Windows のファイアウォールが有効になっている場合に必要です。

Windows の [スタート] メニューから、[コントロールパネル] - [Windows ファイアウォール] を選択し、Windows のファイアウォールが有効になっているかどうかを確認してください。

有効になっている場合の設定手順を次に示します。

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択する。
2. [gpedit.msc] を入力し、[OK] ボタンをクリックする。
[グループポリシーオブジェクトエディタ] 画面が表示されます。
3. [グループポリシーオブジェクトエディタ] 画面の [コンピュータの構成]、[管理用テンプレート]、[ネットワーク]、[ネットワーク接続] および [Windows ファイアウォール] をクリックし、ツリーを展開させる。
4. [標準プロファイル] ※をクリックして、右ペインにある [Windows ファイアウォール：着信リモート管理の例外を許可する] を右クリックし、表示されたメニューから [編集] を選択する。
[Windows ファイアウォール：リモート管理の例外を許可するのプロパティ] 画面が表示されます。
注※ ホストマシンがドメイン環境の場合は、[ドメインプロファイル] となります。

5. [Windows ファイアウォール：リモート管理の例外を許可するのプロパティ] 画面のラジオボタンから [有効] を選択する。
6. [OK] ボタンをクリックする。
[Windows ファイアウォール：リモート管理の例外を許可するのプロパティ] 画面が閉じます。

(3) WMI の名前空間を設定する

WMI の名前空間の設定手順を次に示します。

監視対象ホストで UAC のセキュリティ機能が有効の場合は、ユーザー自身に対して設定するか、Users グループと Administrators グループ以外のユーザーが属するグループに対して設定してください。

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択する。
2. [wmimgmt.msc] を入力し、[OK] ボタンをクリックする。
[Windows Management Infrastructure (WMI)] ダイアログが表示されます。
3. [WMI コントロール (ローカル)] を選択して、右クリックメニューから [プロパティ] を選択する。
[WMI コントロール (ローカル)のプロパティ] ダイアログが表示されます。
4. [セキュリティ] タブを選択して、[Root] と [CIMV2] をクリックし、ツリーを展開させる。
5. [セキュリティ] ボタンをクリックする。
[セキュリティ ROOT¥CIMV2] ダイアログが表示されます。
[グループ名またはユーザー名] に、監視対象ホストに接続するユーザー、またはユーザーが属するグループが表示されているかどうかを確認してください。表示されていない場合は、[追加] ボタンをクリックして、ユーザーまたはユーザーが属するグループを追加してください。
6. [グループ名またはユーザー名] の監視対象ホストに接続するユーザーまたはユーザーが属するグループを選択する。
[アカウントの有効化] と [リモートの有効化] の [許可] がチェックされているかどうか確認してください。チェックが外されている場合は、チェックしてください。
7. [OK] ボタンをクリックする。
[セキュリティ ROOT¥CIMV2] ダイアログが閉じ、[WMI コントロール (ローカル)のプロパティ] ダイアログに戻ります。
8. [OK] ボタンをクリックする。
[WMI コントロール (ローカル)のプロパティ] ダイアログが閉じます。
9. [Windows Management Infrastructure (WMI)] ダイアログの [ファイル] - [終了] を選択して、[Windows Management Infrastructure (WMI)] ダイアログを終了する。

(4) UAC を設定する

監視対象の設定で User にビルトイン Administrator 以外の管理者権限を持つユーザーを指定したとき、UAC によって権限が制限され、一般ユーザーの権限で接続されます。これによって、アクセス拒否が発生し、性能情報を取得できないことがあります。この場合、次のどちらかの設定を実施してください。

(a) LocalAccountTokenFilterPolicy を設定する

監視対象ホストが自ホストではない場合だけ設定できます。

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

元に戻す場合は次のコマンドを実行してください。

```
reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /f
```

(b) UAC を無効化する

JP1/IM - Manager ホストおよび監視対象ホストで次の設定を実施してください。

- UAC の設定スライダーを「通知しない」に設定
 1. [コントロールパネル] - [ユーザー アカウント] - [ユーザーアカウント制御設定の変更] を選択する。
 2. [ユーザーアカウント制御の設定] ウィンドウの左にあるスライダーを「通知しない」に設定する。
- ローカルセキュリティポリシーを設定
 1. [コントロールパネル] - [管理ツール] - [ローカルセキュリティポリシー] を選択する。
 2. [セキュリティの設定] - [ローカルポリシー] - [セキュリティオプション] を選択する。
 3. 「ユーザーアカウント制御：管理者承認モードですべての管理者を実行する」を無効にする。

(5) WMI の接続確認をする

Windows のツール「wbemtest.exe」を使用して JP1/IM - Manager ホストとリモートの監視対象ホストが接続されているかどうかを確認します。

WMI の接続確認手順を次に示します。なお、この手順は JP1/IM - Manager ホストで実施してください。

1. コマンドプロンプトで次のコマンドを実行する。

```
runas /user:ユーザー名 wbemtest
```

[Windows Management Instrumentation テスト] 画面が表示されます。

なお、ユーザー名には [システム共通設定] 画面の [IM ホストアカウント] ページの [ユーザー名] に設定する値を指定します。また、コマンドの実行後にパスワード入力を要求された場合は、[IM ホストアカウント] ページの [パスワード] に設定する値を指定します。

2. [Windows Management Instrumentation テスト] 画面の [接続] ボタンをクリックする。

[接続] 画面が表示されます。

3. [接続] 画面の [名前空間], [ユーザー], [パスワード] および [機関] に必要な情報を入力する。

入力内容を説明します。

- 名前空間

「¥¥監視対象ホスト名¥root¥cimv2」を入力します。

監視対象ホスト名は、実際に監視するホスト名に置き換えてください。

- ユーザー

リモートの監視対象ホストにログオンするユーザー名を入力します。

- パスワード

ユーザーのパスワードを入力します。

- 機関

「ntlmdomain:監視対象ホストのドメイン名」を入力します。リモートの監視対象ホストがワークグループの場合は、未入力のままにしてください。

4. [接続] ボタンをクリックする。

接続に成功すると [接続] 画面が閉じ、[Windows Management Instrumentation テスト] 画面のボタンがすべて活性化されます。

エラーが表示される場合は、エラー番号に応じて設定を確認してください。エラー番号とその要因を次に示します。

なお、ツール「wbemtest.exe」を起動したまま設定を変更し、接続を再度実施してもエラーになることがあります。その場合は、ツールを再起動してから接続を確認してください。

- 0x8001011c

JP1/IM - Manager ホストで DCOM が設定されていません。

- 0x80070005

次のどれかがエラー要因として考えられます。

- ・ JP1/IM - Manager ホストで DCOM が設定されていない
- ・ リモートの監視対象ホストで DCOM が設定されていない
- ・ リモートの監視対象ホストに接続するユーザー名、パスワードまたはドメイン名に誤りがある

- 0x80041003

リモートの監視対象ホストで WMI の「名前空間」が設定されていません。

- 0x80041008

「機関」に指定している値が「ntlmdomain:」で始まっていません。

- 0x800706XX

次のどれかがエラー要因として考えられます。

- リモートの監視対象ホスト名に誤りがある
- リモートの監視対象ホストが起動していない
- リモートの監視対象ホストでファイアウォールが設定されていない
- リモートの監視対象ホストにログインするユーザーのパスワードが有効期限を過ぎている

5. リモートの監視対象ホストで、ログの種別が” System” または” Application” のイベントログがあることを確認したあと、[クエリ] ボタンをクリックし、次のクエリを入力して、[適用] ボタンをクリックする。

```
Select * From Win32_NTLogEvent Where ( Logfile='System' Or Logfile='Application' )
```

実行後に、[クエリ結果] 画面にクエリの実行結果が表示されることを確認してください。

1.18.2 NetBIOS (NetBIOS over TCP/IP) の設定 (Windows の場合)

ここでは、NetBIOS (NetBIOS over TCP/IP) の設定について説明します。設定後、JP1/IM - Manager ホストから監視対象ホストのログファイルが読み取り可能になっていることを確認してください。監視対象ホストのログファイルが SEQ2 形式の場合は、監視対象のログファイルの退避ファイルも読み取り可能になっていることを確認してください。

(1) ファイル共有を設定する

リモートの監視対象ホストで、監視対象のログファイルが配置されているフォルダの共有設定を有効にします。監視対象ホストのホスト情報のリモート通信設定にユーザー名を追加し、そのユーザーに読み取り可能な権限を付与します。なお、ファイル共有を許可するユーザー数を少なく設定すると、ログファイルトラップの開始時に、ファイル共有の接続を許可するユーザー数の上限を超え、エラーとなるおそれがあります。

(2) JP1/IM - Manager ホストでローカルセキュリティを設定する

JP1/IM - Manager ホストで [管理ツール] - [ローカルセキュリティポリシー] - [セキュリティの設定] - [ローカルポリシー] - [ユーザー権利の割り当て] - [ネットワーク経由でのアクセス] に、システム共通設定の IM ホストアカウントに設定するユーザー名を追加します。

(3) 監視対象ホストでローカルセキュリティを設定する

リモートの監視対象ホストで [管理ツール] - [ローカルセキュリティポリシー] - [セキュリティの設定] - [ローカルポリシー] - [ユーザー権利の割り当て] - [ネットワーク経由でのアクセス] に、監視対象ホストのホスト情報のリモート通信設定に設定するユーザー名を追加します。

(4) レジストリを設定する

監視対象ホストが論理ホストの場合、一つの監視対象ホストに対して複数の IP アドレスやホスト名を使用してリモート監視するときは、対象の監視対象ホストでレジストリを設定してください。手順を次に示します。

1. 監視対象ホストに管理者権限でログインする。
2. レジストリエディターを起動する。
3. [レジストリエディタ] で対応するキーを選択する。
 - キー名
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters
4. レジストリ値を追加する。
 - 名前：DisableStrictNameChecking
 - データ型：REG_DWORD
 - 基数：10 進数
 - 値：1
5. レジストリエディターを終了する。
6. 監視対象ホストを再起動する。

(5) NetBIOS (NetBIOS over TCP/IP) の接続確認をする

1. エクスプローラの [アドレス] に「¥リモートの監視対象ホスト名」を入力する。
リモートの監視対象ホスト名には、実際に設定した内容を入力してください。
2. 接続ウィンドウが表示されたら、リモートの監視対象ホストにログオンするユーザー名とパスワードを入力する。
3. リモートの監視対象ホストに NetBIOS 接続ができることを確認する。
4. エクスプローラの [アドレス] に「¥リモートの監視対象ホスト名¥(1)で共有したフォルダのパス」を入力する。
リモートの監視対象ホスト名および(1)で共有したフォルダのパスには、実際に設定した内容を入力してください。
5. (1)で共有したフォルダのパスにアクセスできることを確認する。

アクセスに失敗する場合は、手順が正しく実施できているかどうか見直してください。

1.18.3 SSH の設定 (Windows の場合)

ここでは、JP1/IM - Manager ホストが Windows 環境である場合の、SSH の設定について説明します。なお、SSH の認証には、公開鍵認証方式を使用します。

SSH で接続するには次の設定が必要となります。

- SSH サーバを設定する
リモートの監視対象ホストで設定します。
- 鍵を作成する
UNIX 環境の監視対象ホストで設定します。
- 秘密鍵を JP1/IM - Manager ホストに配置する
UNIX 環境の監視対象ホストから JP1/IM - Manager ホストに配置します。
- 公開鍵を監視対象ホストに配置する
リモートの監視対象ホストに配置します。
- 監視対象のログファイルへのアクセス権を設定する
監視対象ホストが UNIX の場合は、マネージャーホストから監視対象ホストに SSH 接続するユーザーにアクセス権を設定します。

❗ 重要

対話環境が前提である `stty`, `tty`, `tset`, `script` コマンドなどは、SSH 接続ユーザーのログインスクリプトに記載しないでください。記載されている場合は、リモート監視用に SSH 接続ユーザーを新たに作成するか、これらのコマンドを実行しないように SSH 接続ユーザーのログインスクリプトを変更してください。

(1) SSH サーバを設定する

SSH サーバを設定するための手順を次に示します。なお、OS の設定やコマンドは、OS のバージョンによって異なる可能性があります。詳細は、各 OS のマニュアルおよび JP1/IM - Manager のリリースノートを参照してください。

1. リモートの監視対象ホストに root 権限のユーザーでログインする。
2. `sshd_config` を開く。
Linux, AIX の場合：`/etc/ssh/sshd_config`
3. `PubkeyAuthentication` の値を `yes` に設定する※1。
4. `UseDNS` を `no` に設定する※1, ※2。
5. `PermitRootLogin` を `yes` に設定する※1。

1. インストールとセットアップ (Windows の場合)

root 権限のユーザーでログインして情報収集する場合だけ、この手順を実行してください。

6. 次のコマンドを実行し、sshd サービスを再起動する。

実行するコマンドの例を、OS ごとに次に示します。

- Linux の場合（Linux 9 の例）
`systemctl restart sshd.service`
- AIX の場合（AIX 7.3 の例）
`stopsrc -s sshd`
`startsrc -s sshd`

注※1

sshd_config の設定項目および設定方法については、使用する SSH サーバのマニュアルを参照してください。

注※2

設定しない場合は、監視対象ホストで次の名前解決ができるように設定してください。

- マネージャーホストの IP アドレスからマネージャーホスト名を解決できる
 - マネージャーホストのホスト名の解決先 IP アドレスが、マネージャーホストの IP アドレスと一致する
- 名前解決に DNS を使用していて DNS サーバに接続できない場合、リモート監視ログファイルトラップの起動、またはログファイルの収集が遅延することがあります。また、遅延によってタイムアウトしてしまい、起動や収集が失敗することがあります。そのため、UseDNS をno に設定することを推奨します。

(2) 鍵を作成する（初めて鍵を作成する場合）

UNIX 環境の監視対象ホストにリモート監視で使用するユーザーでログインし、ssh-keygen コマンドを実行して鍵を作成します。なお、この手順は、初めて鍵を作成する場合だけに必要な作業です。

鍵の種類は RSA 暗号と DSA 暗号のどちらかを選択できます。

作業を始める前に、ssh ディレクトリの上位ディレクトリのパーミッションに所有者以外の書き込み権限が設定されていないことを確認してください。所有者以外の書き込み権限が設定されていると SSH の接続に失敗します。

1. UNIX 環境の監視対象ホストにリモート監視で使用するユーザーでログインする。

2. ssh-keygen コマンドを実行する。

次のように入力してコマンドを実行してください。

- RSA 鍵を作成する場合：ssh-keygen -t rsa
- DSA 鍵を作成する場合：ssh-keygen -t dsa

3. 秘密鍵の出力先と名前を決める。

マルチバイト文字を含まないパスとファイル名を指定してください。デフォルトは「`~/.ssh/id_rsa`」が設定されます。

4. リターンキーを 2 回押す。

秘密鍵のパスフレーズの入力を求められるため、何も入力しないでリターンキーを押します。再入力を求められるので、何も入力しないで再度リターンキーを押します。

`ssh-keygen -t rsa` コマンドの実行例を次に示します。

```
[root@HOST]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ssh-user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ssh-user/.ssh/id_rsa.
Your public key has been saved in /home/ssh-user/.ssh/id_rsa.pub.
The key fingerprint is:
ax:xx:xx:xx:xx:bx:xx:xc:xx:xx:xx:xd:xd:xa:ed:xx root@HOST
```

5. `cat` コマンドを実行し、公開鍵ファイルの内容を認証鍵ファイルに追加する。

6. `chmod` コマンドを実行し、認証鍵ファイルの属性を 600 に変更する。

`cat` コマンドおよび `chmod` コマンドの実行例を次に示します。

```
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

7. `/etc/ssh/sshd_config` の `AuthorizedKeysFile` を設定する。

デフォルトでは「`~/.ssh/authorized_keys`」または「`.ssh/authorized_keys`」が設定されています。手順 6 で作成した認証鍵のパスを変更した場合は、`AuthorizedKeysFile` の値を見直してください。なお、`sshd_config` の設定を変更した場合は、スーパーユーザーで `sshd` サービスを再起動してください。

注意事項

- 秘密鍵の情報は厳重に管理してください。
- 鍵（公開鍵と秘密鍵のペア）の作成は環境やツールには依存しないため、どのような環境やツールでも問題ありません。ただし、鍵の作成後は、秘密鍵と公開鍵を適切に配置する必要があります。

(3) 秘密鍵を JP1/IM - Manager ホストに配置する（初めて鍵を作成する場合）

JP1/IM - Manager ホストが Windows の場合は、「[1.18.3\(2\) 鍵を作成する（初めて鍵を作成する場合）](#)」で作成した秘密鍵を Windows の JP1/IM - Manager ホストに配置します。秘密鍵を配置するパスには、マルチバイト文字を含まないようにしてください。配置した秘密鍵ファイルが管理者権限の無い OS ユー

ザーにアクセスされないよう、適切なアクセス権限を付与してください。なお、この手順は、初めて鍵を作成する場合だけに必要な作業です。

(4) 秘密鍵が配置された場所を登録する

次のように秘密鍵が JP1/IM - Manager ホストに配置された場所を [システム共通設定] 画面で登録してください。

1. [IM 構成管理] 画面のメニューバーから [編集] - [システム共通設定] を選択する。

[システム共通設定] 画面が表示されます。

2. [システム共通設定] 画面で SSH の秘密鍵ファイルパスを設定する。

[システム共通設定] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.20 [システム共通設定] 画面」を参照してください。

(5) 公開鍵をリモートの監視対象ホストに配置する（すでに鍵を作成している場合）

「1.18.3(2) 鍵を作成する（初めて鍵を作成する場合）」で作成した公開鍵をリモートの監視対象ホストに配置します。配置する手順を次に示します。なお、この手順は、すでに別のリモートの監視対象ホストで鍵を作成している場合だけに必要な作業です。

作業を始める前に、`.ssh` ディレクトリの上位ディレクトリのパーミッションに所有者以外の書き込み権限が設定されていないことを確認してください。所有者以外の書き込み権限が設定されていると SSH の接続に失敗します。

1. リモートの監視対象ホストにリモート監視で使用するユーザーでログインする。

2. `.ssh` ディレクトリに移動する。

リモート監視で使用するユーザーのホームディレクトリ配下に `.ssh` ディレクトリがない場合は作成してください。ディレクトリの属性は 700 を設定してください。

3. `scp` コマンドを実行し、公開鍵ファイルをリモートの監視対象ホストにコピーする。

「1.18.3(2) 鍵を作成する（初めて鍵を作成する場合）」で作成済みの公開鍵ファイルを監視対象ホストにコピーします。公開鍵のコピー先は、リモート監視で使用するユーザーのホームディレクトリの `.ssh` ディレクトリです。

4. `cat` コマンドを実行し、公開鍵ファイルの内容を認証鍵ファイルに追加する。

5. コピーした公開鍵ファイルを削除する。

6. `chmod` コマンドを実行し、認証鍵ファイルの属性を 600 に変更する。

7. `[/etc/ssh/sshd_config]` の `[AuthorizedKeysFile]` を設定する。

デフォルトでは「~/ssh/authorized_keys」または「.ssh/authorized_keys」が設定されています。手順 6 で作成した認証鍵のパスを変更した場合は、AuthorizedKeysFile の値を見直してください。なお、sshd_config の設定を変更した場合は、スーパーユーザーでsshd サービスを再起動してください。

scp コマンド、cat コマンド、およびchmod コマンドの実行例を次に示します。ここでは、「[1. 18.3\(2\) 鍵を作成する（初めて鍵を作成する場合）](#)」で鍵を作成したホストのホスト名を IMHost としています。

- コマンドの実行例

```
[ClientUser@TargetHost]$ cd .ssh
[ClientUser@TargetHost .ssh]$ scp
root@IMHost:/home/ssh-user/.ssh/id_rsa.pub ./
root@IMHost's password: <パスワードを入力>
id_rsa 100% 233 0.2KB/s 00:00
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ rm id_rsa.pub
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

(6) 監視対象のログファイルへのアクセス権を設定する

監視対象ホストが UNIX の場合は、マネージャーホストから監視対象ホストに SSH 接続するユーザーは、次に示すアクセス権が必要です。

- 監視対象のログファイル

読み込み権限が必要です。監視対象のログファイルが SEQ2 形式の場合は、監視対象のログファイルの退避ファイルにも読み込み権限が必要です。

- 監視対象のログファイルがあるディレクトリおよびその上位のすべてのディレクトリ

読み込み権限と実行権限が必要です。監視対象のログファイルが SEQ2 形式の場合は、監視対象のログファイルの退避ファイルがあるディレクトリおよびその上位のすべてのディレクトリに読み込み権限と書き込み権限が必要です。

(7) 接続を確認する

Windows 環境の JP1/IM - Manager ホストに SSH クライアントソフトがインストールされている場合は、配置した秘密鍵を使って、リモートの監視対象ホストに SSH 接続ができることを確認してください。また、SSH 接続するときに、パスワードおよびパスフレーズの入力が必要であることを確認してください。

エラーが発生した場合や、パスワードおよびパスフレーズの入力を要求された場合は、手順どおり正しく設定できているかどうかを見直してください。また、OS の設定を見直し、SSH 接続ができる環境であるか確認してください。

また、リモート監視では、リモートの監視対象ホストで次のコマンドを実行します。リモート監視で使用するユーザーで次のコマンドが実行できることを確認してください。

- `uname`
- `ls`
- `wc`
- `tail`
- `find`
- `grep`
- `head`

コマンドを実行できるか確認する際の手順を、次に示します。

(a) ホスト情報を収集する場合に使用するコマンドの確認

1. [システム共通設定] 画面の [SSH] ページで設定したユーザーで監視対象ホストにログインする。
2. 次のコマンドを実行し、戻り値が0であることを確認する。

```
uname -s
```

(b) ログファイルを収集する場合に使用するコマンドの確認

1. [システム共通設定] 画面の [SSH] ページで設定したユーザーで監視対象ホストにログインする。
2. 次のコマンドを実行し、戻り値が0であることを確認する。

- `ls -ild` 監視対象のログファイルパス

コマンドの例：

```
ls -ild /var/log/messages
```

実行結果の例：

```
12345 -rw-r--r-- 1 root root 100 4月 12 13:00 2013 messages
```

- `ls` 監視対象のログファイルが存在するディレクトリパス

コマンドの例：

```
ls /var/log
```

実行結果の例：

```
messages
```

- (監視対象ホストの OS が AIX の場合) `LC_CTYPE=C wc -l` 監視対象のログファイルパス

コマンドの例：

```
LC_CTYPE=C wc -l /var/log/messages
```

実行結果の例：

```
20 /var/log/messages
```

- (監視対象ホストの OS が Linux の場合) `wc -l` 監視対象のログファイルパス

コマンドの例：

```
wc -l /var/log/messages
```

実行結果の例：

```
20 /var/log/messages
```

- `tail -n +監視対象のファイルの任意の行番号 監視対象のログファイルパス | tail -c 収集するサイズの上限值`

コマンドの例：

```
tail -n +19 /var/log/messages | tail -c 10241
```

実行結果の例：

```
line num = 19
```

```
line num = 20
```

3. ログファイルの出力形式が SEQ2 の場合、手順 2 のコマンドに加えて、次のコマンドを実行し、標準出力の結果を確認する。

- `find 監視対象のログファイルが存在するディレクトリパス -xdev -inum 監視対象のログファイルの退避ファイルのinode`

コマンドの例：

```
find /var/log/ -xdev -inum 12345
```

標準出力の例：

```
/var/log/messages.1
```

標準出力の結果として、監視対象のログファイルの退避ファイルのパスが出力されることを確認してください。

標準出力を確認する場合に、標準出力を `stdout.txt` に出力して標準エラー出力を `stderr.txt` に出力するときは、次のように実行してください。

コマンドの例：

```
find /var/log/ -xdev -inum 12345 1> stdout.txt 2> stderr.txt
```

(c) 事前フィルターを適用する場合に使用するコマンドの確認

1. [システム共通設定] 画面の [SSH] ページで設定したユーザーで監視対象ホストにログインする。

2. 次のコマンドを実行し、戻り値が 0 であることを確認する。

- (監視対象ホストの OS が Linux の場合) `/bin/grep -E '事前フィルター'`

コマンドの例：

```
tail -n +19 /var/log/messages | /bin/grep -E 'filter' | tail -c 10241
```

実行結果の例：

```
line num = 19
```

```
line num = 20
```

- (監視対象ホストの OS が AIX の場合) `/usr/bin/grep -E '事前フィルター'`

コマンドの例：

```
tail -n +19 /var/log/messages | /usr/bin/grep -E 'filter' | tail -c 10241
```

実行結果の例：

```
line num = 19
```

```
line num = 20
```

- head -n 監視対象ファイルの任意の行番号

コマンドの例：

```
tail -n +19 /var/log/messages | head -n 20
```

実行結果の例：

```
line num = 19
```

```
line num = 20
```

1.18.4 1 回の監視間隔で収集できるログのサイズの設定 (Windows の場合)

事前フィルターを適用しても、1 回の監視間隔で収集できるログのサイズの上限が超えてしまう環境では、1 回の監視間隔で収集できるログのサイズの上限の初期値を変更することができます。

変更する場合は、次の手順で設定します。

1. リモート監視ログファイルトラップ機能とリモート監視イベントログトラップ機能の実行環境を設定する。

リモートログトラップ環境定義ファイル (jp1cf_remote_logtrap.conf) を編集します。

Manager パス¥conf¥imcf

2. jbssetcnf コマンドを実行して、定義内容を反映する。

jbssetcnf Manager パス¥conf¥imcf¥jp1cf_remote_logtrap.conf

3. JP1/IM - Manager を再起動する。

再起動後に設定内容が反映されます。

1 回の監視間隔で収集できるログのサイズの設定について

- リモートログトラップ環境定義ファイル (jp1cf_remote_logtrap.conf)

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「リモートログトラップ環境定義ファイル (jp1cf_remote_logtrap.conf)」(2. 定義ファイル)

1.19 JP1/IM - Manager のセットアップ (Windows の場合)

ここでは、JP1/IM - Manager のセットアップ項目について説明します。

なお、セットアップ作業を行うユーザーは、Administrators 権限が必要です。

1.19.1 JP1/IM - Manager の設定ファイルの編集について (Windows の場合)

設定ファイルを変更するには、次の 2 つの方法があります。

- 統合オペレーション・ビューアーを使用する方法
- ホストにログインして設定する方法

統合オペレーション・ビューアーを使用する場合に、編集できる設定ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「定義ファイル一覧」(2. 定義ファイル) で、JP1/IM - Manager に関する定義ファイルの注記を参照してください。ホストにログインして設定する方法の場合は、すべての設定ファイルを編集できます。

各設定方法の手順を次に示します。

■統合オペレーション・ビューアーを使用する方法

1. 統合オペレーション・ビューアーから設定ファイルをダウンロードする。
ファイルを追加する場合は、ダウンロードする必要はありません。
2. ダウンロードしたファイルを編集する。
3. 統合オペレーション・ビューアーを使用して、編集したファイルをアップロードする。
アップロードすると自動的に設定が反映されます。

■ホストにログインして設定する方法

1. マネージャーホストにログインする。
2. JP1/IM - Manager のサービスを停止する。
3. 設定ファイルを編集する。
4. サービスを起動する。

1.19.2 インテリジェント統合管理基盤の機能を使用するための設定 (Windows の場合)

JP1/IM - Manager を新規インストールした場合、インテリジェント統合管理基盤の機能はデフォルトで無効になっています。

インテリジェント統合管理基盤の機能を使用する場合は、次の手順に従ってください。

1. 統合監視 DB を設定する。

2. インテリジェント統合管理データベースを設定する。

3. 発生元ホストのマッピングを有効にする。

`jcoimdef -hostmap ON` を実行します。

4. インテリジェント統合管理基盤サービス (jddmain) を有効にする。

`jcoimdef -dd ON` を実行します。

5. JP1/IM - Manager を起動する。

6. インテリジェント統合管理基盤サービスの稼働を確認する。

`jco_spmd_status` コマンドを実行します。稼働中のプロセスに `jddmain` が表示されていることを確認してください。

統合監視 DB については、「[1.4.2 統合監視 DB の設定 \(Windows の場合\)](#)」を参照してください。

インテリジェント統合管理データベースについては、「[1.5.2 インテリジェント統合管理データベースの設定 \(Windows の場合\)](#)」を参照してください。

`jcoimdef` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jcoimdef`」(1. コマンド)を参照してください。

❗ 重要

インテリジェント統合管理基盤の設定を行うと、JP1/IM3-Manager サービスの起動時間が延びます。クラスタソフトで JP1/IM3-Manager サービスの起動時間を監視している場合や JP1/Base の起動管理機能で JP1/IM3-Manager サービスを起動している場合は、クラスタソフトのタイムアウト値を見直す必要があります。インテリジェント統合管理基盤を設定したあとでサービスの起動時間を確認し、タイムアウト値を調整してください。

1.19.3 エージェントとして JP1/IM - Agent を使用する場合の設定

(1) 統合エージェント管理基盤の設定変更

(a) 共通の設定方法

■ 設定ファイルを編集する (Windows の場合)

設定ファイルは、次のディレクトリに格納されています。

OS	格納先
Windows	Manager パス¥conf¥imdd¥plugin¥jp1pccs¥ Manager パス¥conf¥imdd¥imagent¥
Linux	/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/ /etc/opt/jp1imm/conf/imdd/imagent/

設定ファイルを変更するには、次の 2 つの方法があります。

- 統合オペレーション・ビューアーを使用する方法
- ホストにログインして設定する方法

統合オペレーション・ビューアーを使用する場合に、編集できる設定ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「定義ファイル一覧」(2. 定義ファイル)で、JP1/IM - Agent (統合エージェント管理基盤)に関する定義ファイルの注記を参照してください。ホストにログインして設定する方法の場合は、すべての設定ファイルを編集できます。

各設定方法の手順を次に示します。

■統合オペレーション・ビューアーを使用する方法

1. 統合オペレーション・ビューアーから設定ファイルをダウンロードする。
ファイルを追加する場合は、ダウンロードする必要はありません。
2. ダウンロードしたファイルを編集する。
3. 統合オペレーション・ビューアーを使用して、編集したファイルをアップロードする。
アップロードすると自動的に設定が反映されます。

■ホストにログインして設定する方法

1. 統合マネージャーホストにログインする。
2. JP1/IM - Manager のサービスを停止する。

サービスの停止方法については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3.2 JP1/IM - Manager を終了する」を参照してください。

3. 設定ファイルを編集する。

4. サービスを起動する。

サービスの起動方法については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3.1 JP1/IM - Manager を起動する」を参照してください。

(b) 統合エージェント管理基盤の設定変更 (Windows の場合)

統合エージェント管理基盤 (imbase, imbaseproxy) の設定変更の手順を、次に示します。

■ 統合エージェント管理基盤の設定ファイルを変更する

統合エージェント管理基盤の設定ファイルは、imbase 設定ファイル (jpc_imbase.json) と imbaseproxy 設定ファイル (jpc_imbaseproxy.json) です。

設定ファイルの編集方法については、「[1.19.3\(1\)\(a\) 共通の設定方法](#)」の「設定ファイルを編集する (Windows の場合)」を参照してください。

■ 統合エージェント管理基盤のポートを変更する

次の手順を実施します。

1. JP1/IM - Manager を停止する。

2. 統合エージェント管理基盤のリッスンポート番号を変更する。

待ち受けポート番号は、統合エージェント管理基盤の imbase 設定ファイル (jpc_imbase.json) と imbaseproxy 設定ファイル (jpc_imbaseproxy.json) の port メンバーに設定されています。これを新しいポート番号に変更します。

imbase 設定ファイルと imbaseproxy 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の該当するファイル (2. 定義ファイル) を参照してください。

3. JP1/IM - Manager を開始する。

すでに運用中の環境において統合エージェント管理基盤のリッスンポート番号を変更した場合、統合エージェント制御基盤側の接続先ポートも変更する必要があります。

■ 証明書を設定する

JP1/IM3 - Manager と JP1/IM3 - Agent 間の通信を暗号化する場合、次の手順を実施します。

1. JP1/IM - Manager を停止する。

2. 統合エージェント管理基盤のサーバ証明書およびキーファイルを変更する。

リッスンポート番号は、imbase 共通設定ファイル (jjpc_imbasecommon.json) の cert_file や key_file のメンバーに設定されています。

cert_file や key_file の設定値、または、設定しているファイル自体を更新します。

imbase 共通設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「2. 定義ファイル」の、該当するファイルの説明を参照してください。

3. JP1/IM - Manager を開始する。

■ イベント転送中継機能を設定する（オプション）

イベント転送中継機能を使用する場合、JP1/IM - Manager を 13-01 以降にする必要があります。

イベント転送中継機能を有効する場合の JP1/IM - Manager の設定手順を、次に示します。

1. JP1/IM - Manager のサービスを停止する。

クラスタ構成の場合は、クラスタソフトからサービスを停止します。

2. imbase 設定ファイル (jpc_imbase.json) を開き、jp1base_forward_send の項目を設定する。

- JP1/IM - Manager 13-10 以降を新規インストールした場合
imbase 設定ファイルに jp1base_forward_send の項目が記載されていますが、「//jp1base_forward_send」のようにコメント化されているため、先頭の「//」を削除します。
- JP1/IM - Manager 13-10 より前のバージョンからバージョンアップした場合
imbase 設定ファイルに jp1base_forward_send の項目が記載されていないため、imbase 設定ファイルのモデルファイルを参考にして、imbase 設定ファイルに記載します。記載する際、先頭の「//」を削除します。

3. imbase 設定ファイルの jp1base_forward_send の項目の下にある port を設定する。

同居する JP1/Base のイベント転送用のポートを指定します。

サービス名で指定する場合は、services ファイルにサービス名と TCP ポートを設定してください。

4. JP1/IM - Manager のサービスを起動する。

クラスタ構成の場合は、クラスタソフトからサービスを起動します。

イベント転送機能を無効にする場合は、上記と同じ手順を実施し、手順 2 で、jp1base_forward_send の項目を「//jp1base_forward_send」のようにコメント化するか、または jp1base_forward_send の項目を削除してください。

(c) IM 管理ノードのツリー情報の作成と反映（Windows の場合）（必須）

次に示す手順で、IM 管理ノードのツリー情報の作成と反映を行います。

1. 統合エージェントホストで行う手順を実施する。

「1.21.2(19) IM 管理ノードのツリー情報の作成と反映（Windows の場合）（必須）」の手順 1～4 を実施します。

2. JP1/IM - Manager の `jddcreatetree` コマンドまたは IM 管理ノード関連情報の生成 API を実行する。
実行に失敗した場合は、メッセージの内容に従って対処を行い、再度実行します。

3. アドオンプログラム、または、ユーザー独自の Prometheus もしくは Fluentd の構成変更や削除を行った場合、構成変更前にトレンドデータ管理 DB に保存したトレンドデータが不要なときは、トレンドデータを削除したあと、JP1/IM - Manager の `jddcreatetree` コマンドまたは IM 管理ノード関連情報の生成 API を実行する。

トレンドデータの削除は、指定したホスト上の Prometheus および Fluentd（ユーザー独自の Prometheus およびユーザー独自の Fluentd を含む）が保存したトレンドデータをすべて削除するため、構成変更をしていないアドオンプログラムのトレンドデータを残す場合は、トレンドデータを削除せずに、JP1/IM - Manager の `jddcreatetree` コマンドまたは IM 管理ノード関連情報の生成 API を実行します。

実行に失敗した場合は、メッセージの内容に従って対処を行い、再度実行します。

トレンドデータの削除方法については、次の個所の説明を参照してください。

- ・ マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンスの「2.2.1 [統合エージェント一覧] 画面」
- ・ マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.11.4トレンドデータ削除」および「5.18.2 統合エージェント情報削除」

4. アドオンプログラム、または、ユーザー独自の Prometheus もしくは Fluentd の構成変更や削除を行った場合に、下記の「**■IM 管理ノード関連ファイルの編集**」に記載する IM 管理ノード関連ファイルの編集を行う（新規構築時には実施不要です）。

5. JP1/IM - Manager の `jddupdatetree` コマンド（構成変更モード）または IM 管理ノード関連情報の反映 API を実行する。

実行に失敗した場合は、メッセージの内容に従って対処を行い、再度実行します。

6. 統合オペレーション・ビューアーを表示し、正しく IM 管理ノードが作成されているか確認する。

正しく作成されていない場合、作成されていない統合エージェント、アドオンプログラム、ユーザー独自の Prometheus または Fluentd の設定内容を見直し、再度、手順 2 以降を実施します。

■IM 管理ノード関連ファイルの編集

アドオンプログラム、または、ユーザー独自の Prometheus もしくは Fluentd の構成変更（設定変更、または、削除）を行った場合、トレンドデータ管理 DB からそれらのサンプルが削除されるまで、構成変更前の IM 管理ノードが作成されます。トレンドデータが削除される契機については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.7.2トレンドデータ管理 DB」を参照してください。

構成変更前の IM 管理ノードを作成したくない場合、`jddcreatetree` コマンドにより出力された IM 管理ノードファイル、および、IM 管理ノードツリーファイルを編集します。IM 管理ノードツリーファイ

ルについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.5.3 IM 管理ノード関連ファイル」を参照してください。ファイルをコピーしてバックアップを作成してから編集を行ってください。

■IM 管理ノードファイルの編集

jddcreatetree コマンドにより出力された IM 管理ノードファイル（ファイル名：imdd_node_HITACHI_JP1_JPCCS_CONFINFO_JP1/IM - Manager のホスト名.json）には、構成変更前の IM 管理ノードの情報も出力されます。設定変更の場合、変更前と変更後で構成情報の SID が同一となり、2 つ目以降の構成情報の SID は、末尾に「-xx」（xx は 01～99 までの数字）を付与して出力されます。

構成変更前の IM 管理ノードが不要である場合、jddcreatetree コマンドにより出力された IM 管理ノードファイルを編集して、構成変更前の IM 管理ノードのオブジェクトの情報を削除します。IM 管理ノードファイルの形式を次に示します。

```
{
  "meta":{
    . . .
  },
  "simtData": [
    IM管理ノードのオブジェクト,
    . . .
  ]
}
```

IM 管理ノードのオブジェクトは、simtData の配列の要素で、次の形式です。

- IM 管理ノードのオブジェクトの形式

```
{
  "sid": "構成情報のSID",
  "value": {
    . . .
    "property": {
      IM管理ノードのプロパティに表示する値
    },
    "jp1im_TrendData_labels": {
     トレンドデータを特定するための値
    },
    . . .
  }
}
```

IM 管理ノードのプロパティに表示する値、および、トレンドデータを特定するための値を確認し、構成変更前の IM 管理ノードのオブジェクトを削除します。IM 管理ノードのプロパティに表示する値については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.6(1) (f) プロパティ表示」を参照してください。トレンドデータを特定するための値として、次に表に示す値が設定されています。

キー	値の説明
jp1_pc_prome_hostname	Prometheus server のホスト名

キー	値の説明
	Prometheus 設定ファイルの jpl_pc_prome_hostname に設定されている値です。 ログ監視対象の SID の場合、このキーと値は出力されません。
job	スクレイプジョブ名 Prometheus 設定ファイルの job_name に設定されている値です。ログ監視対象の SID、または、kubernetes の SID の場合、このキーと値は出力されません。
instance	インスタンス名 ディスカバリ設定ファイルの targets に指定した値です。
jpl_pc_nodelabel	IM 管理ノードのラベル名 Prometheus 設定ファイルの scrape_configs もしくは metrics_scrape_configs、または、AWS リソースの jpl_pc_nodelabel タグで設定した値です。

構成情報の SID の末尾に「-xx」が付与されていない IM 管理ノードのオブジェクトを削除し、末尾に「-xx」が付与されている IM 管理ノードのオブジェクトを残す場合、残す構成情報の SID の末尾の「-xx」を削除して保存してください。

Node exporter のポート番号を変更した場合の編集例を、次に示します。

この例では、変更前のポート番号が 20716、変更後のポート番号が 29999 とします。

- 編集前の IM 管理ノードファイルの例

```
{
  "meta":{
    . . .
  },
  "simtData": [
    . . .
    {
      "sid": "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29",
      "value": {
        "component": "/HITACHI/JP1/JPCS/CONFINFO",
        "category": "platform",
        "visible": true,
        "label": "Linux metric collector(Node exporter)",
        "property": {
          "jpl_pc_prome_hostname": "ahost",
          "job": "jpc_node",
          "jpl_pc_exporter": "JPC Node exporter",
          "jpl_pc_trendname": "node_exporter"
        },
        "jplim_TrendData_labels": {
          "jpl_pc_prome_hostname": "ahost",
          "job": "jpc_node",
          "instance": "ahost:20716",
          "jpl_pc_nodelabel": "Linux metric collector(Node exporter)"
        },
        "methods": [
          "_metricListGet",
          "_timeSeriesDataGet"
        ]
      }
    }
  ]
}
```



```

    },
    {
      "sid": "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29-01",
      "value": {
        "component": "/HITACHI/JP1/JPCS/CONFINFO",
        "category": "platform",
        "visible": true,
        "label": "Linux metric collector(Node exporter)",
        "property": {
          "jp1_pc_prome_hostname": "ahost",
          "job": "jpc_node",
          "jp1_pc_exporter": "JPC Node exporter",
          "jp1_pc_trendname": "node_exporter"
        },
        "jp1im_TrendData_labels": {
          "jp1_pc_prome_hostname": "ahost",
          "job": "jpc_node",
          "instance": "ahost:29999",
          "jp1_pc_nodelabel": "Linux metric collector(Node exporter)"
        },
        "methods": [
          "_metricListGet",
          "_timeSeriesDataGet"
        ]
      }
    },
    . . .
  ]
}

```

instance のキーに「ahost:20716」が設定されている IM 管理ノードのオブジェクトを削除し、残す構成情報の SID の末尾の「-xx」を削除します。編集後の IM 管理ノードファイルを、次に示します。

- 編集後の IM 管理ノードファイルの例

```

{
  "meta":{
    . . .
  },
  "simtData": [
    . . .
    {
      "sid": "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29",
      "value": {
        "component": "/HITACHI/JP1/JPCS/CONFINFO",
        "category": "platform",
        "visible": true,
        "label": "Linux metric collector(Node exporter)",
        "property": {
          "jp1_pc_prome_hostname": "ahost",
          "job": "jpc_node",
          "jp1_pc_exporter": "JPC Node exporter",
          "jp1_pc_trendname": "node_exporter"
        },
        "jp1im_TrendData_labels": {
          "jp1_pc_prome_hostname": "ahost",

```

```

        "job": "jpc_node",
        "instance": "ahost:29999",
        "jp1_pc_nodelabel": "Linux metric collector(Node exporter)"
    },
    "methods": [
        "_metricListGet",
        "_timeSeriesDataGet"
    ]
}
},
...
]
}

```

■IM 管理ノードツリーファイルの編集

jddcreatetree コマンドにより出力された IM 管理ノードツリーファイルを編集します。

構成の削除を行った場合、削除した IM 管理ノードのツリーオブジェクトの記述を削除します。

設定変更を行った場合、構成情報の SID の末尾に「-xx」が付与されている構成情報の SID の記述を、target の配列から削除します。

Node exporter の設定を変更した場合の編集例を、次に示します。

- 編集前の IM 管理ノードツリーファイルの例

```

{
  "meta":{
    ...
  },
  "simtData": [
    ...
    {
      "sid": "_ROOT_AllSystems/_HOST_AHOST/_CATEGORY_platform/_OBJECT_JP1PC-ALinux%20metric%20collector%28Node%20exporter%29",
      "value": {
        "target": [
          "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29"
        ],
        "label": "Linux metric collector(Node exporter)"
      }
    },
    {
      "sid": "_ROOT_AllSystems/_HOST_AHOST/_CATEGORY_platform/_OBJECT_JP1PC-ALinux%20metric%20collector%28Node%20exporter%29-01",
      "value": {
        "target": [
          "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29-01"
        ],
        "label": "Linux metric collector(Node exporter)"
      }
    }
  ],
  ...
}

```

- 編集後の IM 管理ノードツリーファイルの例

```
{
  "meta":{
    . . .
  },
  "simtData": [
    . . .
    {
      "sid": "_ROOT_AllSystems/_HOST_AHOST/_CATEGORY_platform/_OBJECT_JP1PC-ALinux%20metric%20collector%28Node%20exporter%29",
      "value": {
        "target": [
          "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29"
        ],
        "label": "Linux metric collector(Node exporter)"
      }
    },
    . . .
  ]
}
```

■ IM 管理ノード関連ファイルの編集しない場合の動作

IM 管理ノード関連ファイルを編集しない場合、トレンドデータ管理 DB から構成変更前のサンプルが削除されるまで、それらの IM 管理ノードが作成されます。設定変更の場合、アドオンプログラム、または、ユーザー独自の Prometheus および Fluentd が発行する JP1 イベントは、構成情報の SID の末尾に「-xx」が付与されていない IM 管理ノードにマッピングされます。

(d) 製品プラグインの設定 (Windows の場合)

製品プラグインの設定方法について説明します。

■ トレンド表示するメトリックを定義する (オプション)

統合オペレーション・ビューアーの「トレンド」タブで表示するメトリックを、メトリック定義ファイルに定義します。主要なメトリックは、初期設定されています。メトリック定義ファイルについては、「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の各メトリック定義ファイル (2. 定義ファイル) を参照してください。

■ AWS 定義ファイルを設定する (オプション)

Yet another cloudwatch exporter で監視を行う場合、AWS 定義ファイルを編集し、Yet another cloudwatch exporter で監視するときに使用する AWS のアカウント ID と、SID や IM 管理ノードのプロパティに設定するアカウント文字列のマッピングを指定します。

AWS 定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「AWS 定義ファイル (aws_settings.conf)」(2. 定義ファイル) を参照してください。

■ システムノード定義ファイル (imdd_systemnode.conf) を編集する (Yet another cloudwatch exporter を使用する場合だけ必須)

アドオンプログラムの Yet another cloudwatch exporter を使用して監視を行い、システムノードを作成する場合、JP1/IM - Manager のシステムノード定義ファイル (imdd_systemnode.conf) を設定します。

この設定は、アドオンプログラムの Yet another cloudwatch exporter を使用して監視する場合は、必須の設定となります。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.6(1)(i)ツリーの形式」に示すシステムノードを作成するときは、システムノード定義ファイル (imdd_systemnode.conf) を編集して、次の設定項目を指定します。ここに記載のない設定項目については、任意の値を指定します。

項目名	説明
displayName	Amazon CloudWatch のメトリクスを発行するサービスの名前※を指定します。
type	AWS 名前空間名※を指定します。 スラッシュ (/) は、ハイフン (-) に変更して指定してください。
name	次の文字列を指定します。 [{".*":"regex"}]

注※

Amazon CloudWatch の Web ページに記載されている内容を示します。

Yet another cloudwatch exporter のメトリック定義ファイル (metrics_ya_cloudwatch_exporter.conf) の初期設定で監視する AWS 名前空間に対して、システム管理ノードの設定する場合に、システムノード定義ファイルの各項目に設定する値の例を、次に示します。

displayName	type	name
Amazon Simple Storage Service	JP1PC-AWS-S3	[{".*":"regex"}]
AWS Lambda	JP1PC-AWS-LAMBDA	
Amazon DynamoDB	JP1PC-AWS-DYNAMODB	
AWS Step Functions	JP1PC-AWS-STATES	
Amazon Simple Queue Service	JP1PC-AWS-SQS	
Amazon Elastic Container Service	JP1PC-AWS-ECS	
Amazon Elastic Block Store	JP1PC-AWS-EBS	
Amazon Elastic File System	JP1PC-AWS-EFS	
FSx File System	JP1PC-AWS-FSX	
Simple Notification Service	JP1PC-AWS-SNS	

displayName	type	name
Relational Database Service	JP1PC-AWS-RDS	

上記の内容をシステムノード定義ファイルに設定した場合、次のとおりになります。

```
{
  "meta":{
    "version":"2"
  },
  "allSystem":[
    {
      "id":"strageSystem",
      "displayName":"Amazon Simple Storage Service",
      "objectRoot":[
        {
          "type":"JP1PC-AWS-S3",
          "name":[".*":"regexp"]
        }
      ]
    },
    {
      "id":"lambda",
      "displayName":"AWS Lambda",
      "objectRoot":[
        {
          "type":"JP1PC-AWS-LAMBDA",
          "name":[".*":"regexp"]
        }
      ]
    },
    {
      "id":"dynamodb",
      "displayName":"Amazon DynamoDB",
      "objectRoot":[
        {
          "type":"JP1PC-AWS-DYNAMODB",
          "name":[".*":"regexp"]
        }
      ]
    },
    {
      "id":"states",
      "displayName":"AWS Step Functions",
      "objectRoot":[
        {
          "type":"JP1PC-AWS-STATES",
          "name":[".*":"regexp"]
        }
      ]
    },
    {
      "id":"sqs",
      "displayName":"Amazon Simple Queue Service",
      "objectRoot":[
        {
          "type":"JP1PC-AWS-SQS",

```

```

        "name":[".*":"regex"]
    }
],
{
    "id":"ecs",
    "displayName":"Amazon Elastic Container Service",
    "objectRoot":[
        {
            "type":"JP1PC-AWS-ECS",
            "name":[".*":"regex"]
        }
    ]
},
{
    "id":"ebs",
    "displayName":"Amazon Elastic Block Store",
    "objectRoot":[
        {
            "type":"JP1PC-AWS-EBS",
            "name":[".*":"regex"]
        }
    ]
},
{
    "id":"efs",
    "displayName":"Amazon Elastic File System",
    "objectRoot":[
        {
            "type":"JP1PC-AWS-EFS",
            "name":[".*":"regex"]
        }
    ]
},
{
    "id":"fsx",
    "displayName":"FSx File System",
    "objectRoot":[
        {
            "type":"JP1PC-AWS-FSX",
            "name":[".*":"regex"]
        }
    ]
},
{
    "id":"sns",
    "displayName":"Simple Notification Service",
    "objectRoot":[
        {
            "type":"JP1PC-AWS-SNS",
            "name":[".*":"regex"]
        }
    ]
},
{
    "id":"rds",
    "displayName":"Relational Database Service",
    "objectRoot":[]
}

```

```

    {
      "type": "JP1PC-AWS-RDS",
      "name": [{"*": "regex"}]
    }
  ]
}
]
}

```

システムノード定義ファイルの設定を行ったあと、JP1/IM - Manager の `jddcreatetree` コマンドを実行して、EC2 以外の CloudWatch を作成すると、JP1/IM - Manager の統合オペレーション・ビューアの「稼働状況」領域で、AWS 名前空間名に応じたシステムノードの配下に、IM 管理ノードが表示されます。

システムノード定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「システムノード定義ファイル (imdd_systemnode.conf)」(2. 定義ファイル) を参照してください。

■ credentials ファイルの配置について

アドオンプログラムの Yet another cloudwatch exporter で監視を行う場合、「[1.21.2\(7\) Yet another cloudwatch exporter の設定](#)」の「(b) CloudWatch に接続するための設定を変更する (Windows の場合) (必須)」に記載している credentials ファイルは、
 「C:\Windows\System32\config\systemprofile\aws\」に配置してください。

■ IM 管理ノードカテゴリ名称定義ファイル (imdd_category_name.conf) の編集 (オプション)

サービス監視機能を使用する場合、次の設定を行います。ただし、JP1/IM - Manager 13-01 以降を新規インストールしたときは、インストール時に設定されているため、この設定は不要です。

IM 管理ノードカテゴリ名称定義ファイル (imdd_category_name.conf) に、次の表に示す定義を追加します。サービス監視機能によって作成するエージェント SID の IM 管理ノードは、この表で示した表示カテゴリ名称の値で表示されます。なお、定義を追加しない場合は、IM 管理ノードのカテゴリは「service」(指定カテゴリ ID の値) となります。すでに指定カテゴリ ID に「service」を設定しているときは、この設定は不要です。

表 1-9 サービス監視機能のカテゴリ

表示カテゴリ名称	指定カテゴリ ID
Service	service

この定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「IM 管理ノードカテゴリ名称定義ファイル (imdd_category_name.conf)」(2. 定義ファイル) を参照してください。

1.19.4 JP1/IM - Agent パッケージの登録 (Windows の場合)

JP1/IM のマネージャーホストに、JP1/IM - Agent のパッケージ（以降、JP1/IM - Agent パッケージと呼びます）を登録できます。複数のバージョンの JP1/IM - Agent パッケージを登録することもできます。

JP1/IM - Agent の提供媒体を使用せずに、JP1/IM のマネージャーホストに登録された JP1/IM - Agent パッケージをダウンロードして、エージェントホストに JP1/IM - Agent をインストールできます。

なお、JP1/IM - Agent パッケージの登録は任意です。

(1) JP1/IM - Agent パッケージの登録方法

JP1/IM のマネージャーホストに JP1/IM - Manager をインストールすると、同梱されている JP1/IM - Agent パッケージが自動的に登録されます。

❗ 重要

マネージャーホストに登録された JP1/IM - Agent パッケージをダウンロードできるようにするには、インテリジェント統合管理基盤のセットアップが必要です。

マネージャーホストに JP1/IM - Manager をバージョンアップインストールした場合、すでにインストールされている旧バージョンの JP1/IM - Agent パッケージは、削除されます。

(2) JP1/IM - Agent パッケージの削除方法

マネージャーホストに登録された JP1/IM - Agent パッケージを削除したい場合は、次に示す JP1/IM - Agent パッケージの登録場所のファイルを削除します。

表 1-10 JP1/IM - Agent パッケージの登録場所 (統合マネージャーホスト (Windows の場合))

OS	JP1/IM - Agent パッケージ		
	登録場所	ファイル名	製品名
Windows	Manager パス ¥public¥download¥imagent¥	jp1_pc_agent_windows_JP1/IM - Agent のバージョン番号 (VVRSS 形式) .zip	JP1/IM - Agent (Windows 版)
		jp1_pc_agent_linux_JP1/IM - Agent のバージョン番号 (VVRSS 形式) .tar.gz	JP1/IM - Agent (Linux 版)

(3) JP1/IM - Agent パッケージのダウンロードの手順

JP1/IM - Agent パッケージをダウンロードする手順を、次に示します。

■前提条件

- マネージャーホストに JP1/IM - Agent パッケージが登録されている
- インテリジェント統合管理基盤のセットアップが完了している

- ログインに使用する JP1 ユーザーに必要な権限が割り当てられている

■手順

1. ファイルダウンロードの REST API を実行して、JP1/IM - Agent パッケージをダウンロードする。

<記述例>

```
GET http://JP1/IM - Manager (インテリジェント管理基盤) のホスト名:20703/download/imagent/  
JP1/IM - Agentパッケージのファイル名
```

JP1/IM - Manager から配布物を取得（ファイルダウンロード）するには、JP1 ユーザーの認証が必要です。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.2.8 REST API の認証方法」を参照してください。

2. ダウンロードした JP1/IM - Agent パッケージを解凍する。

- Windows 版の場合

PowerShell を使用して、次のコマンドを実行します。

```
Expand-Archive -Path jpl_pc_agent_windows_JP1/IM - Agentのバージョン番号 (VRRSS形式).zip
```

- Linux 版の場合

シェルを使用して、次のコマンドを実行します。

```
tar -zxvf jpl_pc_agent_linux_JP1/IM - Agentのバージョン番号 (VRRSS形式).tar.gz
```

1.19.5 セントラルスコープの機能を使用するための設定 (Windows の場合)

JP1/IM - Manager を新規インストールした場合、セントラルスコープの機能はデフォルトで無効になっています。

セントラルスコープの機能を使用する場合は、次の手順に従ってください。

1. セントラルスコープのデータベースを作成する。

Scope パス¥bin¥jcldbsetup を実行します。必要に応じてオプションを指定してください。

2. セントラルスコープサービス (jcsmain) を有効にする。

jcoimdef -s ON を実行します。

3. JP1/IM - Manager を起動する。

4. セントラルスコープサービスの稼働を確認する。

jco_spmd_status コマンドを実行します。稼働中のプロセスに jcsmain が表示されていることを確認してください。

jcsdbsetup コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcsdbsetup」(1. コマンド)を参照してください。

jcoimdef コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド)を参照してください。

❗ 重要

セントラルスコープのデータベースの再構成について

JP1/IM - Manager アンインストール後の再インストールまたは jcsdbsetup コマンド実行後に、JP1/IM - View を接続すると[監視ツリー]画面に JP1/IM - Manager 再インストール前または jcsdbsetup コマンド実行前の監視ツリーが表示される場合があります。この場合は、起動中の JP1/IM - View を停止し、次のフォルダを削除後、JP1/IM - View を起動してください。

削除フォルダ：

システムドライブ:\ProgramData\HITACHI\JP1\JP1_DEFAULT\JP1CoView\log\output

1.19.6 JP1/IM - Manager の障害に備えた設定 (Windows の場合)

JP1/IM - Manager は JP1/IM - Manager 自身に障害が発生した場合に備えて、トラブル解決の調査資料を採取するツールや、プロセスの異常終了時に自動で再起動する機能などを提供しています。

ここでは、JP1/IM - Manager の障害に備えた設定項目について説明します。

(1) 障害発生時の資料採取の準備

JP1/IM - Manager ではトラブル発生時に資料を採取するためのツールをバッチファイル (jim_log.bat) として提供しています。このツールは、トラブルの解決の調査資料となる情報を一括して採取するツールです。

JP1/IM - Manager の資料採取ツールで採取できるのは、JP1/IM - Manager, JP1/Base および JP1/IM - View (同一ホストにある場合) のトラブルシュート資料です。採取できる資料の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「12.3 トラブル発生時に採取が必要な資料」を参照してください。

資料採取ツールについて

- jim_log.batについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jim_log.bat (Windows 限定)」(1. コマンド)

なお、トラブルが発生した場合にメモリーダンプおよびクラッシュダンプが必要となることがあります (資料採取ツールでこれらのダンプも採取できます)。

❗ 重要

- メモリーダンプのサイズは、実メモリーのサイズによって異なります。搭載している物理メモリーが大きいと、メモリーダンプのサイズも大きくなります。メモリーダンプを採取できるだけのディスク領域を確保してください。詳細は、Windows のヘルプの「STOP エラー」の項目を参照してください。
- クラッシュダンプに出力される情報は JP1 だけでなく、ほかのアプリケーションプログラムのトラブル情報も出力されます。また、クラッシュダンプが出力されると、その分ディスク容量が圧迫されます。クラッシュダンプが出力されるように設定する場合は、十分なディスク領域を確保しておいてください。
- 起動前に以下のレジストリを設定することで、JavaVM 異常終了時に即座に調査資料のユーザーモードプロセスダンプを取得できます。なお、レジストリの設定はシステム全体に対して影響を与えますので、設定にあたりましては十分ご注意願います。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥Windows Error Reporting¥LocalDumps

上記のレジストリキーに次のレジストリ値を設定する。

DumpFolder : REG_EXPAND_SZ <ダンプ出力先のフォルダ名>

(出力先フォルダにはアクセス権が必要です)

DumpCount : REG_DWORD <保存するダンプの数>

DumpType : REG_DWORD 2

(2) プロセス異常終了時の再起動の設定

1. プロセス再起動を定義する。

プロセス再起動が有効になるよう、次の拡張起動プロセス定義ファイル (jp1co_service.conf) を編集します。

Console パス¥conf¥jp1co_service.conf

「再起動可否」パラメーターは「|」で区切られた 3 番目の値で、0 (再起動しない：デフォルト) または 1 (再起動する) を設定します。なお、「|」で区切られた 1 番目の値は変更しないでください。

2. 定義内容を反映する。

JP1/IM - Manager が稼働している場合は、プロセス再起動の設定が有効になるよう、JP1/IM - Manager のリロードコマンドを実行します。

jco_spmd_reload

プロセス再起動の定義について

- 拡張起動プロセス定義ファイル (jp1co_service.conf) について

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「拡張起動プロセス定義ファイル (jp1co_service.conf)」(2. 定義ファイル)

注意事項

異常終了時の再起動設定は、クラスタ運用時には設定しないでください。JP1/IM - Manager の障害時にはプロセス再起動の機能も障害の影響を受けるおそれがあります。クラスタ運用時に再起動をしたい場合は、JP1/IM - Manager 外部のクラスタソフトから再起動を制御してください。

(3) プロセス異常検知時の JP1 イベントの発行の設定

1. JP1 イベント発行を設定する。

次の IM パラメーター定義ファイル (jp1co_param_V7.conf) を編集します。

Console パス¥conf¥jp1co_param_V7.conf

このファイルの「SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT」と「SEND_PROCESS_RESTART_EVENT」が JP1 イベント発行の設定パラメーターです。JP1 イベントを発行するには、値を「dword:1」に変更します。

2. jbssetcnf コマンドを実行して、定義内容を反映する。

jbssetcnf Console パス¥conf¥jp1co_param_V7.conf

3. JP1/Base および JP1/Base を前提とする製品を再起動する。

再起動後に設定内容が反映されます。

JP1 イベント発行の設定について

- IM パラメーター定義ファイル (jp1co_param_V7.conf) について

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「IM パラメーター定義ファイル (jp1co_param_V7.conf)」(2. 定義ファイル)

(4) ヘルスチェック機能の設定

ヘルスチェック機能を使って JP1/IM - Manager プロセスのハングアップを検知したい場合に設定します。

1. ヘルスチェック定義ファイル (jcohc.conf) を開き、パラメーターを設定する。

ヘルスチェック機能を有効にするため、ENABLE=true にします。

また、ハングアップ検知時に JP1 イベントを発行する場合にはEVENT=true を、通知コマンドを実行する場合にはCOMMAND=実行するコマンドを指定します。

2. jco_spmd_reload コマンドで JP1/IM - Manager をリロードする。または、JP1/IM - Manager を再起動する。

3. 通知コマンドを設定した場合は、jcohctest コマンドを実行して動作確認する。

jcohctest コマンドを実行して、正しくCOMMAND で指定したコマンドが実行されるか確認します。正しく動作しなかった場合は指定を見直してください。

❗ 重要

Windows (x64)では、%WINDIR%\System32 フォルダ以下に配置されているコマンドを実行すると、WOW64のリダイレクト機能によって、%WINDIR%\SysWow64 フォルダ以下に配置されているコマンドにリダイレクトされます。リダイレクト先のコマンドがない場合、コマンドの実行に失敗することがあります。%WINDIR%\System32 フォルダ以下に配置されているコマンドを実行コマンドに指定する場合は注意してください。

ヘルスチェック機能の設定について

- ヘルスチェック定義ファイル (jcohc.conf) について

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ヘルスチェック定義ファイル (jcohc.conf)」(2. 定義ファイル)

- jcohctest コマンドについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcohctest」(1. コマンド)

(5) 監視オブジェクト DB の自動バックアップ・リカバリー設定

セントラルスコープの機能を使用する場合に設定します。

監視ツリーの更新中に、OS がシャットダウンしたり、クラスタ運用時にフェールオーバーしたりすると、監視オブジェクト DB が破損するおそれがあります。このため、監視ツリーの更新時に監視オブジェクト DB を自動でバックアップ・リカバリーするよう設定します。

なお、新規インストールの場合は有効、旧バージョンの JP1/IM - Manager で設定を無効にしていた場合は無効となっています。運用に合わせて、設定を変更してください。

1. JP1/IM - Manager を停止する。

2. 次のファイルを引数にして jbssetcnf コマンドを実行する。

監視オブジェクト DB の自動バックアップ・リカバリー機能を有効にする：auto_dbbackup_on.conf

監視オブジェクト DB の自動バックアップ・リカバリー機能を無効にする：auto_dbbackup_off.conf

jbssetcnf コマンドを実行すると、JP1 共通定義情報に設定内容が反映されます。

jbssetcnf コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「監視オブジェクト DB の自動バックアップ・リカバリー設定ファイル (auto_dbbackup_xxx.conf)」(2. 定義ファイル) を参照してください。

3. JP1/IM - Manager を起動する。

1.19.7 バージョンアップ時の設定 (Windows の場合)

ここでは、JP1/IM - Manager のバージョンアップインストール時のセットアップ項目について説明します。

IM データベースを使用している場合は、「[1.4.5 IM データベースの更新 \(Windows の場合\)](#)」を参照して、IM データベースを更新する必要があります。

(1) セントラルスコープのバージョンアップコマンドの実行

バージョン 8 以前の JP1/IM - Central Scope からバージョンアップした場合は、次の手順に従い、バージョンアップコマンドを実行してください。バージョンアップコマンドを実行するまでは、旧バージョンの JP1/IM - Central Scope と互換モードで動作します（旧バージョンから追加された機能は使用できません）。

1. JP1/IM - Manager を停止する。

2. ディスクの空き容量を確認する。

次の手順に示す `jp1csverup.bat` コマンドを実行するには、監視オブジェクト DB 分の空き容量が必要です。監視オブジェクト DB は、次に示すフォルダ内のすべてのデータです。

Scope パス¥database¥jcsdb¥

3. `jp1csverup.bat` コマンドを実行する。

4. `jbssetcnf` コマンドを実行する。

次に示す機能の有効、無効は旧バージョンの JP1/IM - Central Scope の設定に依存します。

- 対処済み連動機能
- 状態変更イベントの上限監視

機能を無効から有効にしたい場合、次の表に示すファイルを引数に `jbssetcnf` コマンドを実行してください。

表 1-11 機能を有効にするための設定ファイル

ファイル名	説明
action_complete_on.conf	対処済み連動機能を有効にするためのファイルです。
evhist_warn_event_on.conf	監視オブジェクトの状態変更イベント件数が上限値（100 件）を超えた際に、JP1 イベントを発行する機能を有効にするためのファイルです。

5. JP1/IM - Manager を起動する。

6. JP1/IM - View で JP1/IM - Manager（JP1/IM - Central Scope）に接続し、問題がないか動作を確認する。

- `jp1csverup.bat` コマンドについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jp1csverup.bat (Windows 限定)」(1. コマンド)

(2) 自動アクション定義ファイルの更新

11-10 以前の JP1/IM - Manager からバージョンアップした場合は、次の手順に従い、自動アクション定義ファイルを更新してください。

ただし、11-10 以前の自動アクション定義ファイルをそのまま使用したい場合は必要ありません。

1. JP1/IM - Manager を停止する。

2. jcadefconv コマンドを実行して自動アクション定義ファイルを更新する。

jcadefconv -i 変換するアクション定義ファイル名 -o 変換後のアクション定義ファイル名

3. jcadefconv コマンドの-o オプションに指定したファイルをactdef.conf にリネームして格納先に配置する。

格納先およびファイル名を次に示します。なお、次に示す格納先およびファイル名を-o オプションに直接指定している場合は、この手順は不要です。

物理ホストの場合：Console パス¥conf¥action¥actdef.conf

論理ホストの場合：共有フォルダ¥jp1cons¥conf¥action¥actdef.conf

4. JP1/IM - Manager を起動する。

- 自動アクションの機能について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「6. 自動アクションによるコマンド実行 (JP1/Base 連携)」

- jcadefconv コマンドについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcadefconv」(1. コマンド)

(3) イベントレポート出力の出力形式の指定

10-50 以前の JP1/IM - Manager からバージョンアップした場合、イベントレポート出力で CSV 出力する際に、1 件の固有の拡張属性に一つの列を割り当てて出力する機能が無効になっています。この機能を有効にするかどうかは、イベントレポート出力環境定義ファイル (evtreport.conf) の PROGRAM_SPECIFIC_EX_ATTR_COLUMN パラメーターで指定します。なお、新規にインストールした場合は有効です。必要に応じて、イベントレポート出力環境定義ファイルを設定してください。

イベントレポート出力環境定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベントレポート出力環境定義ファイル (evtreport.conf)」(2. 定義ファイル) を参照してください。

(4) [ログファイルトラップサービスが起動したときに自動でプロセス起動する] チェックボックスの表示

11-01 以前の JP1/IM - Manager からバージョンアップした場合、[ログファイルトラップサービスが起動したときに自動でプロセス起動する] チェックボックスが無効（非表示）になっています。

[ログファイルトラップサービスが起動したときに自動でプロセス起動する] チェックボックスの有効・無効は、プロファイル管理環境定義ファイル (jplcf_profile_manager.conf) の LOGFILETRAP_AUTO_START_CONTROL パラメーターで指定します。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「プロファイル管理環境定義ファイル (jplcf_profile_manager.conf)」(2. 定義ファイル) を参照してください。

(5) エージェントのプロファイル更新通知機能

11-01 以前の JP1/IM - Manager からバージョンアップした場合、エージェントのプロファイル更新通知機能が無効になっています。

エージェントのプロファイル更新通知機能の有効・無効は、プロファイル管理環境定義ファイル (jplcf_profile_manager.conf) の AGENT_PROFILE_UPDATE_NOTICE はパラメーターで指定します。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「プロファイル管理環境定義ファイル (jplcf_profile_manager.conf)」(2. 定義ファイル) を参照してください。

(6) リモート監視が停止中のログの監視設定

11-01 以前の JP1/IM - Manager からバージョンアップした場合、リモート監視が停止中に出力されたログ情報を収集しない設定になっています。

リモート監視が停止中に出力されたログ情報を収集するかどうかは、リモートログトラップ環境定義ファイル (jplcf_remote_logtrap.conf) の START_OPTION パラメーターで指定します。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「リモートログトラップ環境定義ファイル (jplcf_remote_logtrap.conf)」(2. 定義ファイル) を参照してください。

(7) インテリジェント統合管理基盤のバージョンアップ (Windows の場合)

インテリジェント統合管理基盤を利用している場合のバージョンアップ時の設定について説明します。

なお、連携製品のバージョンアップも同時に実施する場合は、手順 5 を実行する前に連携製品のバージョンアップを実施してください。

1. JP1/IM - Manager を停止する。
2. 12-50 以前の JP1/IM - Manager からバージョンアップした場合、インテリジェント統合管理データベースを構築する。

インテリジェント統合管理データベースの構築の詳細については、「[1.5 インテリジェント統合管理データベースの構築 \(Windows の場合\)](#)」を参照してください。

3. 新しい設定値を追加する。

利用する機能に合わせて、新しく追加された設定値を追加します。※

注※

JP1/IM - Manager を 13-00 または 13-01 から 13-10 以降にバージョンアップした場合、テキストエディターなどで、次のファイルの末尾に「web-enable-admin-api: true」の行を追加します。なお、インテリジェント統合管理データベースを再構築したときは、自動で追加されるため、この手順は不要です。

- ・物理ホストの場合：Manager パス¥conf¥imgndb¥config.yml
- ・論理ホストの場合：共有フォルダ¥jp1imm¥conf¥imgndb¥config.yml

上記の手順を実施しなかった場合、トレンドデータの削除と統合エージェント情報の削除が失敗します。

トレンドデータの削除と統合エージェント情報については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.1 [統合エージェント一覧] 画面」、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.11.4トレンドデータ削除」および「5.18.2 統合エージェント情報削除」を参照してください。

4. JP1/IM - Manager を起動する。

5. jddcreatetree コマンドを実行する。

6. jddupdatetree コマンドを新規・再構築モードで実行する。

- ・ jddcreatetree コマンドについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddcreatetree」(1. コマンド)

- ・ jddupdatetree コマンドについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddupdatetree」(1. コマンド)

バージョンアップを実行しない場合、インテリジェント統合管理基盤 13-00 の機能は利用できません。

(8) インテリジェント統合管理データベースのバージョンアップ (Windows の場合)

インテリジェント統合管理データベースを利用している場合のバージョンアップ時の設定について説明します。

JP1/IM - Manager をバージョン 13-10 以前からバージョンアップした場合に、インテリジェント統合管理データベースを利用しているときは、jimgnbupdate コマンドを実行する必要があります。jimgnbupdate

コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimgndbupdate」(1. コマンド)を参照してください。

(9) 拡張起動プロセス定義ファイルの更新

バージョン 11 以前の JP1/IM - Manager からバージョンアップした場合は、拡張起動プロセス定義ファイル (jplco_service.conf) に jddmain, imbase, imbaseproxy プロセスの定義を追加してください。

バージョン 12 からバージョンアップした場合は、imbase, imbaseproxy プロセスの定義を追加してください。

拡張起動プロセス定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「拡張起動プロセス定義ファイル (jplco_service.conf)」(2. 定義ファイル)を参照してください。

1.20 JP1/IM - View のセットアップ (Windows の場合)

ここでは、JP1/IM - View のセットアップ項目について説明します。

なお、セットアップ作業を行うユーザーは、Administrators 権限が必要です。

1.20.1 JP1/IM - View の障害に備えた設定 (Windows の場合)

JP1/IM - View は、障害が発生した場合に備えて、トラブル解決の調査資料を採取するツールを提供しています。JP1/IM - View に障害が発生した場合に備え、ツールの実行時に Windows のクラッシュダンプおよびメモリーダンプを採取できるよう、ダンプの出力設定をしておくことをお勧めします。

JP1/IM - View では、トラブル発生時に資料を採取するためのツールをバッチファイル (jcoview_log.bat) として提供しています。JP1/IM - View の資料採取ツールで採取できるのは、JP1/IM - View のトラブルシュート資料です。採取できる資料の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「12.3 トラブル発生時に採取が必要な資料」を参照してください。

資料採取ツールについて

- jcoview_log.batについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoview_log.bat (Windows 限定)」(1. コマンド)

メモリーダンプおよびクラッシュダンプを出力する設定を「[1.19.6\(1\) 障害発生時の資料採取の準備](#)」の説明を参照して、設定してください。

また、IM 構成管理では、IM 構成管理・ビューアーで障害が発生した場合、スレッドダンプを採取するためのコマンド (jcftreaddmp) を提供しています。jcftreaddmp コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcftreaddmp (Windows 限定)」(1. コマンド) を参照してください。

1.20.2 JP1/IM - View (セントラルコンソール・ビューアーおよびセントラルスコープ・ビューアー) の動作カスタマイズ (Windows の場合)

JP1/IM - View (セントラルコンソール・ビューアーおよびセントラルスコープ・ビューアー) の動作を設定します。設定を変更したい場合は、IM-View 設定ファイル (tuning.conf) を編集します。JP1/IM - View (セントラルコンソール・ビューアーおよびセントラルスコープ・ビューアー) の動作について、設定できる項目を次に示します。

- [ログイン] 画面の接続先ホスト入力履歴数
- 次の項目で、前回ログインした JP1 ユーザー名の表示を抑止

- [ログイン] 画面の [ユーザー名]
- [イベントコンソール] 画面起動時の [統合機能メニュー] 画面起動可否
- [イベントコンソール] 画面起動時の [アクション結果一覧] 画面起動可否
- 統合機能メニューおよびモニター画面呼び出しで使用する WWW ブラウザーの起動パス
- クリップボードへのコピー可否
- [監視ツリー] 画面, [監視ツリー (編集)] 画面, [ビジュアル監視 (編集)] 画面, [イベントコンソール] 画面, [アクション結果一覧] 画面, および [コマンド実行] 画面のログイン中の JP1 ユーザー名の表示を抑止

ここで設定した内容は、IM-View 設定ファイルを編集したビューアーでだけ有効になります。手順を次に示します。

1. 次の IM-View 設定ファイル (tuning.conf) をテキストエディターなどで編集する。

View パス¥conf¥tuning.conf

2. JP1/IM - View を再起動する。

IM-View 設定ファイルの動作カスタマイズについて

- IM-View 設定ファイルについて

参照先: マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「IM-View 設定ファイル (tuning.conf)」(2. 定義ファイル)

1.20.3 IM 構成管理・ビューアーのセットアップおよび動作カスタマイズ (Windows の場合)

IM 構成管理・ビューアーを起動するには、次の 2 種類の方法があります。

- Windows のスタートメニューから起動する方法
- IM 構成管理・ビューアーを起動するコマンド (jcfview) を実行して起動する方法

(1) IM 構成管理・ビューアーのセットアップ

ここでは、IM 構成管理・ビューアーを Windows のスタートメニューから起動する場合のセットアップについて説明します。なお、jcfview コマンドを実行して起動する場合には、このセットアップは不要です。

JP1/IM - View のインストール時に、スタートメニューに IM 構成管理・ビューアーのショートカットが作成されます。

IM 構成管理・ビューアーのショートカットを削除したあとに再度作成する場合には、次の手順を実施してください。

1. JP1/IM - View を停止する。

2. 次のコマンドを実行する。

```
jcovcfsetup -i      (-i オプションは省略できます)
```

Windows のスタートメニューの [すべてのプログラム] - [JP1_Integrated Management 3 - View] の下に、IM 構成管理・ビューアーのショートカットが追加されます。名称は [構成管理] です。

jcovcfsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcovcfsetup (Windows 限定)」(1. コマンド) を参照してください。

注意事項

スタートメニューに登録されている [JP1_Integrated Management 3 - View] (ショートカット) の位置、または名称を変更した場合には、ショートカットは追加されません。

(2) IM 構成管理・ビューアーの動作カスタマイズ

IM 構成管理・ビューアーの動作を設定します。設定を変更したい場合は、IM 構成管理・ビューアー動作定義ファイル (jcfview.conf) を編集します。IM 構成管理・ビューアーの動作について、設定できる項目を次に示します。

- IM 構成管理の [ログイン] 画面の接続先ホスト入力履歴数
- IM 構成管理の [ログイン] 画面の接続ユーザー入力履歴数
- [IM 構成管理] 画面、[エージェント構成編集] 画面、[リモート監視構成編集] 画面、および [プロファイル表示/編集] 画面起動時の画面表示設定履歴機能の使用可否
- サーバ応答待ちのタイムアウト時間
- システムの階層構成の反映応答待ちタイムアウト時間
- [IM 構成管理] 画面、[エージェント構成編集] 画面、[リモート監視構成編集] 画面、および [プロファイル表示/編集] 画面のログイン中の JP1 ユーザー名の表示を抑止

ここで設定した内容は、IM 構成管理・ビューアー動作定義ファイルを編集したビューアーでだけ有効になります。手順を次に示します。

1. 次の IM 構成管理・ビューアー動作定義ファイル (jcfview.conf) をテキストエディターなどで編集する。

```
View パス¥conf¥jcfview.conf
```

2. JP1/IM - View を再起動する。

IM 構成管理・ビューアー動作定義ファイルの動作カスタマイズについて

- IM 構成管理・ビューアー動作定義ファイルについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API
リファレンス」の「IM 構成管理・ビューアー動作定義ファイル (jcfview.conf)」(2. 定義ファイル)

1.21 JP1/IM - Agent のセットアップ (Windows の場合)

1.21.1 JP1/IM - Agent のサービスの設定

(1) アドオンプログラムの有効化・無効化

アドオンプログラムの有効化・無効化について説明します。JP1/IM - Agent は、複数のアドオンプログラムを含んでおり、有効化したサービスだけを起動できます。

なお、ログメトリクス機能は、Fluentd のプラグインであるため、ログメトリクス機能そのものを起動・停止する方法はありません。ログメトリクス機能の起動・停止は、Fluentd の起動・停止に準じます。

(a) アドオンプログラムの有効化

■インストール時に設定する場合

インストール時に使用する初期設定コマンドで、有効化したいアドオンプログラムを選択します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.9 初期設定コマンド」の説明を参照してください。

なお、バージョンアップインストール時は、既存の設定を引き継ぎます。ただし、新バージョンで新たに追加されたアドオンプログラムは無効化された状態となります。

■インストール後に設定する場合

JP1/IM - Agent のアドオンプログラムのサービスを有効化する手順を、次に示します。

1. サービスが起動中の場合は、次のコマンドを実行して停止する。

```
Agentパス¥tools¥jpc_service_stop -s all
```

2. 次のコマンドを実行して、サービスを有効化する。

```
Agentパス¥tools¥jpc_service -on [JP1/IM - Agentのサービスキー]
```

3. サービスに対応するディスカバリ設定ファイルを移動する。

次に示すサービスに対応するディスカバリ設定ファイルを、Agentパス¥conf¥jpc_file_sd_config_off フォルダから Agentパス¥conf フォルダに移動します。

サービス	ディスカバリ設定ファイル
prometheus_server	なし
alertmanager	なし
windows_exporter	jpc_file_sd_config_windows.yml

サービス	ディスカバリ設定ファイル
blackbox_exporter	- jpc_file_sd_config_blackbox_http.yml - jpc_file_sd_config_blackbox_icmp.yml
ya_cloudwatch_exporter	jpc_file_sd_config_cloudwatch.yml
fluentd	なし
promitor	jpc_file_sd_config_promitor.yml
script_exporter	なし
web_exporter	jpc_file_sd_config_web.yml
vmware_exporter	jpc_file_sd_config_vmware.yml

4. サービスが有効化されたことを確認する。

コマンドプロンプトで「services.msc」を実行すると、管理コンソールでサービスを確認できます。該当するサービスが存在する場合、そのサービスは有効です。

5. 「1.21.2(19) IM 管理ノードのツリー情報の作成と反映 (Windows の場合) (必須)」を実施する。

(b) アドオンプログラムの無効化

JP1/IM - Agent のアドオンプログラムのサービスを無効化する手順を、次に示します。

1. サービスが起動中の場合は、次のコマンドを実行して停止する。

```
Agentパス¥tools¥jpc_service_stop -s all
```

2. 次のコマンドを実行して、サービスを無効化する。

```
Agentパス¥tools¥jpc_service -off [JP1/IM - Agentのサービスキー]
```

3. サービスに対応するディスカバリ設定ファイルを移動する。

次に示すサービスに対応するディスカバリ設定ファイルを、Agent パス¥conf フォルダから Agent パス¥conf¥jpc_file_sd_config_off フォルダに移動します。

サービス	ディスカバリ設定ファイル
prometheus_server	なし
alertmanager	なし
windows_exporter	jpc_file_sd_config_windows.yml
blackbox_exporter	- jpc_file_sd_config_blackbox_http.yml - jpc_file_sd_config_blackbox_icmp.yml
ya_cloudwatch_exporter	jpc_file_sd_config_cloudwatch.yml
fluentd	なし
promitor	jpc_file_sd_config_promitor.yml

サービス	ディスカバリ設定ファイル
script_exporter	なし
web_exporter	jpc_file_sd_config_web.yml
vmware_exporter	jpc_file_sd_config_vmware.yml

4. サービスが無効化されたことを確認する。

コマンドプロンプトで「services.msc」を実行すると、管理コンソールでサービスを確認できます。該当するサービスが存在しない場合、そのサービスは無効です。

(2) 自動起動の有効化・無効化

(a) 自動起動の有効化

OS 起動時のサービス自動起動を有効にする手順を、次に示します。

1. 次のコマンドを実行して、JP1/IM - Agent のすべてのサービスの自動起動を有効にする。

```
jpc_service_autostart -on
```

(b) 自動起動の無効化

OS 起動時のサービス自動起動を無効にする手順を、次に示します。

1. 次のコマンドを実行して、JP1/IM - Agent のすべてのサービスの自動起動を無効にする。

```
jpc_service_autostart -off
```

(c) 自動起動および自動停止の確認方法

コマンドプロンプトで「services.msc」を実行すると、管理コンソールでサービスを確認できます。

該当するサービスのプロパティを開き、「スタートアップの種類」が「自動」または「自動（遅延）」であれば有効です。それ以外であれば無効です。サービス名については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.9 JP1/IM - Agent のサービス」を参照してください。

(d) OS シャットダウン時の自動停止についての注意事項

Windows をシャットダウンする前に、統合エージェントのすべてのサービスを手動で停止してください。Windows のシャットダウンは、サービスの停止完了を待たないため、サービスが稼動中に Windows をシャットダウンするとサービスが正常に停止できない場合があります。この場合、イベントログにエラーや警告が出力され、OS シャットダウンした前後の統合エージェントのログの内容が不正になることがあります。また、次のサービスの起動に時間がかかることがあります。

(3) 手動で起動・停止する方法

JP1/IM - Agent を手動で起動・停止する場合は、次のコマンドを使用します。

表 1-12 起動停止コマンド

コマンド	説明
jpc_service_start	エージェントサービスを起動します。
jpc_service_stop	エージェントサービスを停止します

コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「1. コマンド」を参照してください。

(4) サービスの起動状態の確認方法

コマンドプロンプトで「services.msc」を実行すると、管理コンソールでサービスを確認できます。対象のサービスの状態を確認します。

(5) 設定ファイルの配置場所

インストール時に、imagent, imagentproxy, imagentaction, および各アドオンプログラムのサービス定義ファイルを、次の場所に配置します。

サービス定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「サービス定義ファイル (jpc_プログラム名_service.xml)」(2. 定義ファイル) を参照してください。

表 1-13 アドオンプログラムのサービス定義ファイルの配置場所

配置場所 (パス)	用途	配置方法
Agent パス¥conf¥ (物理ホストの場合)	モデルファイル (サービス定義ファイルの雛型) モデルファイルは編集しないでください。	インストーラーで配置します。
共有ディスク¥jp1ima¥conf¥ (論理ホストの場合)	モデルファイル (サービス定義ファイルの雛型) モデルファイルは編集しないでください。	手動で配置します。
Agent パス¥bin¥	サービス定義ファイル本体 このファイルを編集してください。	物理ホスト用は初期設定コマンドで、論理ホスト用は手動で配置します。

(6) 設定ファイルの編集

サービスの設定を変更したい場合は、サービス定義ファイルを編集します。サービス定義ファイルを編集した場合、定義の反映方法は、変更したパラメーターに応じて異なり、次のどれかになります。

- サービスをアンインストール (`jpc_service disable` コマンドを実行) して再インストール (`jpc_service enable` コマンドを実行) する
- サービスを再起動する
- サービス定義ファイルを保存する

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「サービス定義ファイル (`jpc_プログラム名_service.xml`)」(2. 定義ファイル)の「定義の反映時期」を参照してください。

(7) サービス自動起動の設定変更に関する注意事項

サービス定義ファイルの`<startmode>`で、サービス自動起動の設定を行うことができます。ただし、`jpc_service_autostart` コマンドや Windows サービスの設定を直接変更することで、サービス自動起動の設定を変更できるため、必ずしもサービス定義ファイルに指定した`<startmode>`の設定と現在のサービス自動起動の設定が一致しているとは限りません。

(8) サービスの無効化に関する注意事項

`jpc_service disable` コマンドを実行してサービスを無効化する場合、サービス定義ファイルが存在しない、または、サービス定義ファイルの内容が不正だったときは、無効化に失敗することがあります。その場合は、次のコマンドを管理者権限で実行してください。

```
SC Delete サービス名
```

1.21.2 JP1/IM - Agent の設定

(1) 共通の設定方法

(a) 設定ファイルを編集する (Windows の場合)

設定ファイルは、`conf` ディレクトリに格納されています。設定ファイルの内容を変更する方法には、次の2つの方法があります。

- 統合オペレーション・ビューアーを使用する方法
- ホストにログインして設定する方法

統合オペレーション・ビューアーを使用する場合に、編集できる設定ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「定義ファイル一覧」(2. 定義ファイル)で、JP1/IM - Agent (統合エージェント制御基盤)に関する定義ファイルの注記を参照してください。ホストにログインして設定する方法の場合は、すべての設定ファイルを編集できます。

■ 統合オペレーション・ビューアーを使用する方法

1. 統合オペレーション・ビューアーから設定ファイルをダウンロードする。

統合オペレーション・ビューアーから編集したい定義ファイルを選択してダウンロードします。

ユーザーが任意で作成できる定義ファイルを追加する場合は、次の手順を実施します。

1. ユーザー作成定義ファイルリスト定義ファイルをダウンロードします。
2. ユーザー作成定義ファイルリスト定義ファイルに追加したい定義ファイルの情報を記載します。
3. ユーザー作成定義ファイルリスト定義ファイルをアップロードします。
4. 追加したい定義ファイルをアップロードします。

2. ダウンロードしたファイルを編集する。

メモ

Prometheus server の定義ファイルは、`promtool` コマンドで書式チェックができるため、この時点でチェックすることを推奨します。

`promtool` コマンドは、Prometheus server に付属しています。Prometheus server は、GitHub のサイトからダウンロードできます。JP1/IM - Agent に同梱されている Prometheus server と同じバージョンを使用してください。

JP1/IM - Agent のアドオンプログラムのバージョンは、統合オペレーション・ビューアーの「統合エージェント一覧」画面のアドオン機能一覧、または、**Agent パス** `¥addon_management¥アドオン名¥フォルダ`に格納されている `addon_info.txt` ファイルで確認できます。

3. 統合オペレーション・ビューアーを使用して、編集したファイルをアップロードする。

アップロードすると自動的に設定が反映されます。

■ ホストにログインして設定する方法

1. 統合エージェントホストにログインする。

2. JP1/IM - Agent のサービスを停止する。

3. 設定ファイルを編集する。

メモ

Prometheus server の定義ファイルは、`promtool` コマンドで書式チェックができるため、この時点でチェックすることを推奨します。

4. JP1/IM - Agent のサービスを起動する。

(b) サービス定義ファイルを変更する (Windows の場合)

サービス定義ファイルの格納先とファイル名を、次に示します。

- 格納先：インストール先フォルダ¥jplima¥bin¥
- ファイル名：jpc_サービス名_service.xml

❗ 重要

- サービス定義ファイルの項目を変更した場合、変更を反映するために、サービスの再起動またはサービスの再インストール※が必要となります。各項目の反映に必要な操作については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「サービス定義ファイル (jpc_プログラム名_service.xml)」(2. 定義ファイル) の「定義の反映時期」を参照してください。
- サービスの再インストール※が必要な項目を変更した場合は、サービスの登録を一度無効化し、有効化しなおす必要があります。サービスの登録の有効化・無効化の方法については、「[1.21.1\(1\)アドオンプログラムの有効化・無効化](#)」を参照してください。

注※

サービスの再インストールとは、いったんサービスを削除してから、再度サービスを作成する (jpc_service コマンドを使用) ことを意味しています。

サービス定義ファイルを変更する手順を、次に示します。

1. 統合エージェントホストにログインする。
2. JP1/IM - Agent のサービスを停止する。
3. サービス定義ファイルを編集する。
4. JP1/IM - Agent のサービスを起動する。

(c) コマンドラインオプションを変更する (Windows の場合)

サービス定義ファイルの<arguments>タグで、コマンドラインオプションを変更します。

編集方法については、「[1.21.2\(1\)\(b\)サービス定義ファイルを変更する \(Windows の場合\)](#)」を参照してください。

(2) 統合エージェント制御基盤の設定

(a) 接続先の統合マネージャーを変更する (Windows の場合) (オプション)

1. JP1/IM - Agent のサービスを停止する。

2. 接続先の統合マネージャーを変更する。

imagent 共通設定ファイル (jpc_imagentcommon.json) に定義されている接続先の統合マネージャーを、新しい接続先に変更します。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

複数マネージャーホストへのデータ配信機能で、セカンダリーの統合エージェント制御基盤からの接続先の統合マネージャーを変更する場合、immgr ではなく immgr_add.secondery 配下の定義を変更します。

3. 統合エージェントホストを削除する。

統合オペレーション・ビューアーの「統合エージェント一覧」画面で接続先を変更する統合エージェントホストにチェックをつけて、「削除」ボタンを選択します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.1 「統合エージェント一覧」画面」を参照してください。

4. 初期シークレットを確認する。

統合マネージャーホストの統合オペレーション・ビューアーで初期シークレット（初回接続用のシークレット）を確認します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.3 「初期シークレット表示」画面」を参照してください。

5. 初期シークレットを難読化して登録する。

シークレット管理コマンドで、初期シークレットを難読化して登録します。※

```
jimasecret -add -key immgr.initial_secret -s "初期シークレット"
```

6. 個別シークレットを削除する。

シークレット管理コマンドで、個別シークレットを削除します。※

```
jimasecret -rm -key immgr.client_secret
```

7. 証明書を変更する。

CA 証明書の変更方法については、「[1.21.2\(2\)\(c\) CA 証明書を配置する \(Windows の場合\) \(オプション\)](#)」を参照してください。

変更前の接続先の統合マネージャーと新しい接続先の imbase のサーバー証明書を発行した認証局が同じである場合は、この手順は不要です。

8. JP1/IM - Agent を起動する。

注※

複数マネージャーホストへのデータ配信機能で、セカンダリーの統合エージェント制御基盤からの接続先の統合マネージャーを変更する場合、-key オプションに指定する文字列については、マニュアル

「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(e) 初期シークレット、クライアントシークレット、および HTTP プロキシパスワードのキー」を参照してください。

(b) ポートを変更する (Windows の場合) (オプション)

統合エージェント制御基盤が使用するリスンポートは、imagent 設定ファイル (jpc_imagent.json) と imagentproxy 設定ファイル (jpc_imagent_proxy.json) に指定します。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

デフォルトのポート番号については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 C.1(2)JP1/IM - Agent が使用するポート番号」を参照してください。

❗ 重要

- ・ イベント転送中継機能の待ち受けポートを変更した場合は、「[1.21.2\(2\)\(g\) イベント転送中継機能を設定する \(Windows の場合\) \(オプション\)](#)」を参照して、イベント転送中継元の JP1/Base のイベント転送設定を見直してください。
- ・ imagentproxy プロセスのポートを変更した場合は、Prometheus のリモートライト先、Alertmanager のアラート通知先、および Fluentd のアラート通知先を変更する必要があります。それぞれの変更の詳細については、下記を参照してください。
 - ・ Prometheus のリモートライト先：[1.21.2\(3\)\(e\) リモートライト先を変更する \(Windows の場合\) \(オプション\)](#)
 - ・ Alertmanager のアラート通知先：[1.21.2\(4\)\(b\) アラート通知先を変更する \(Windows の場合\) \(オプション\)](#)
 - ・ Fluentd のアラート通知先：[1.21.2\(9\)\(a\) ログ監視の共通定義の設定を変更する \(Windows の場合\) \(オプション\)](#)
- ・ 複数マネージャーホストへのデータ配信機能で、統合エージェント制御基盤のセカンダリーの設定を行う場合、imagent 設定ファイル (jpc_imagent.json) と imagentproxy 設定ファイル (jpc_imagent_proxy.json) の最上位の port や jplbase_forward_receive.port ではなく、listen_add.secondary 配下の同名のメンバーを設定します。

❗ 重要

ポート番号を変更した場合は、ファイアウォールの設定についても見直す必要があります。詳細については、「[1.21.2\(17\) ファイアウォールの設定 \(Windows の場合\) \(必須\)](#)」を参照してください。

(c) CA 証明書を配置する (Windows の場合) (オプション)

統合エージェント管理基盤と統合エージェント制御基盤の間の通信を暗号化する場合、imagent 共通設定ファイル (jpc_imagentcommon.json) の tls_config を指定した上で、下記の設定が必要となります。複

数マネージャーホストへのデータ配信機能で、統合エージェント制御基盤のセカンダリーの設定を行うときは、最上位の `tls_config` ではなく、`immgr_add.secondary.tls_config` を設定します。

暗号化を行わない場合は、下記の設定は不要です。

CA 証明書を配置する手順については、「[9.4.5 JP1/IM - Agent（統合エージェント制御基盤）の設定](#)」を参照してください。

■ 統合エージェント管理基盤のサーバー証明書を検証する場合

1. CA 証明書を配置する。

接続先の imbase のサーバー証明書を発行した認証局の CA 証明書を、次のディレクトリに配置します。

- Windows の場合
Agent パス¥conf¥user¥cert¥
- Linux の場合
/opt/jp1ima/conf/user/cert/

2. imagent 共通設定ファイル (`jpc_imagentcommon.json`) に CA 証明書のパスを記載する。

3. imagent と imagentproxy を再起動する。

■ 統合エージェント管理基盤のサーバー証明書を検証しない場合

1. imagent 共通設定ファイル (`jpc_imagentcommon.json`) の `tls_config.insecure_skip_verify` に「true」を設定する。

(d) アクション実行に関する設定を変更する (Windows の場合) (オプション)

アクション実行に関する設定は、`imagent` 設定ファイル (`jpc_imagent.json`) に定義します。

設定方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

(e) プロキシ認証の認証 ID とパスワードを設定する (Windows の場合) (オプション)

エージェントホストとマネージャーホストの間に Basic 認証が必要なプロキシサーバが存在する場合、認証 ID とパスワードを設定する必要があります。

認証 ID は、`imagent` 共通設定ファイル (`jpc_imagentcommon.json`) の `immgr.proxy_user` に設定します。各定義ファイルの設定方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

パスワードは、次の手段で設定します。詳細については、それぞれの説明箇所を参照してください。

- シークレット管理コマンド
詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jimasecret`」(1. コマンド) を参照してください。

- 統合オペレーション・ビューアーの「シークレット一覧」ダイアログ
詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.2(4)「シークレット一覧」ダイアログ」を参照してください。
- 統合オペレーション・ビューアーのシークレット管理の REST API
詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.4.3 初期シークレット発行」を参照してください。

(f) アクションの実行ユーザーを変更する (Windows の場合) (必須)

imagent 設定ファイル (jpc_imagent.json) の action.username, action.domainname を変更します。設定方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。また、指定したユーザーのパスワードを jimasecret コマンドで登録する必要があります。

(g) イベント転送中継機能を設定する (Windows の場合) (オプション)

イベント転送中継機能を使用する場合、JP1/IM - Agent を 13-01 以降にする必要があります。

イベント転送中継機能の設定は、JP1/IM - Agent の設定を行う前に、JP1/IM - Manager の設定を実施してください。JP1/IM - Manager の設定が完了したあと、JP1/IM - Agent の設定を行い、次に JP1/Base の設定を行います。最後に JP1/IM - Manager でツリーの更新を実施してください。

JP1/IM - Manager の設定については、「[1.19.3\(1\)\(b\) 統合エージェント管理基盤の設定変更 \(Windows の場合\)](#)」の「イベント転送中継機能を設定する (オプション)」を参照してください。

JP1/IM - Agent と JP1/Base の設定手順を、次に示します。

■ JP1/IM - Agent の設定

1. JP1/IM - Agent のサービスを停止する。

クラスタ構成の場合は、クラスタソフトからサービスを停止します。

2. imagent 設定ファイル (jpc_imagent.json) を開き、jp1base_forward_recieve の項目を設定する。

- JP1/IM - Agent 13-10 以降を新規インストールした場合
imagent 設定ファイルに jp1base_forward_recieve の項目が記載されていますが、「// jp1base_forward_recieve」のようにコメント化されているため、先頭の「//」を削除します。
- JP1/IM - Agent 13-10 より前のバージョンからバージョンアップした場合
imagent 設定ファイルに jp1base_forward_recieve の項目が記載されていないため、imagent 設定ファイルのモデルファイルを参考にして、imagent 設定ファイルに記載します。記載する際、先頭の「//」を削除します。

3. imagent 設定ファイルの jp1base_forward_recieve の項目の下にある port を設定する。

4. JP1/IM - Agent のサービスを起動する。

クラスタ構成の場合は、クラスタソフトからサービスを起動します。

■ JP1/IM - Base の設定

1. JP1/Base を停止する。

クラスタ構成の場合は、クラスタソフトから停止します。

2. イベントサーバ設定ファイル (conf) の remote-server に imagent を登録する。

次のように設定します。

```
remote-server イベントサーバ名 通信タイプ アドレス ポート指定
```

イベントサーバ名

固定値「imagent」を指定します。

通信タイプ

固定値「keep-alive」を指定します。

アドレス

自ホストのホスト名（物理ホスト名または論理ホスト名）または IP アドレスを指定します。

ホスト名が jplhosts や jplhosts2 で名前解決できない場合は、IP アドレスを指定してください。

ポート指定

「JP1/IM - Agent の設定」で設定したポート番号を指定します。

3. 転送設定ファイル (forward) を設定する。

次のように設定します。

```
to imagent  
イベントフィルター  
end-to
```

4. JP1/Base を起動する。

クラスタ構成の場合は、クラスタソフトから起動します。

■ ツリーの更新

1. JP1/IM - Manager でインテリジェント統合管理基盤のツリーの更新を実行する。

ツリーの更新を実行してもイベント転送中継元の IM 管理ノードが表示されない場合は、イベント中継元の imagent の jima_message.log にエラーが出力されていないか確認してください。

(h) イベント転送中継機能を解除する (Windows の場合)

JP1/Base の設定を行い、次に JP1/IM - Agent の設定を行います。最後に JP1/IM - Manager でツリーの更新を実施してください。

■ JP1/IM - Base の設定

1. JP1/Base を停止する。

クラスタ構成の場合は、クラスタソフトから停止します。

2. 転送設定ファイル (forward) を編集し, imagent へのイベント転送を解除する。

3. JP1/Base を起動する。

クラスタ構成の場合は, クラスタソフトから起動します。

■ JP1/IM - Agent の設定

1. JP1/IM - Agent のサービスを停止する。

クラスタ構成の場合は, クラスタソフトからサービスを停止します。

2. imagent 設定ファイル (jpc_imagent.json) を開き, jp1base_forward_recieve の項目をコメント化または削除する。

3. JP1/IM - Agent のサービスを起動する。

クラスタ構成の場合は, クラスタソフトからサービスを起動します。

■ ツリーの更新

1. JP1/IM - Manager でインテリジェント統合管理基盤のツリーの更新を実行する。

ツリーの更新を実行してもイベント転送中継元の IM 管理ノードが表示されない場合は, イベント中継元の imagent の jima_message.log にエラーが出力されていないか確認してください。

(i) 複数マネージャーホストへのデータ配信機能を設定する (Windows の場合) (オプション)

■ 新規設定

1. JP1/IM - Agent のサービスを停止する。

停止するサービスのサービスキーを次に示します。

- jpc_imagent
- jpc_imagentaction
- jpc_imagentproxy
- jpc_alertmanager
- jpc_prometheus_server
- jpc_fluentd

2. 統合エージェント管理基盤のセカンダリー用のフォルダを作成する。

統合エージェント管理基盤のセカンダリー用のフォルダとして, 次のフォルダを作成します。

- Agent パス¥tmp¥download-imagent グループ識別子
- Agent パス¥tmp¥upload-imagent グループ識別子
- Agent パス¥tmp¥jbsfwd-imagent グループ識別子

- Agent パス¥logs¥imagent-imagent グループ識別子
- Agent パス¥logs¥imagentproxy-imagent グループ識別子
- Agent パス¥logs¥imagentaction-imagent グループ識別子

上記のフォルダの作成には、次のコマンドを使用します。

```
mkdir フォルダ
```

3. 統合エージェント管理基盤のセカンダリー用のファイルを作成する。

Agent パス¥bin 下にあるコピー元のファイルをコピーし、コピー先のファイル名にリネームします。

コピー元のファイル名	コピー先のファイル名
jpc_imagent_service.exe	jpc_imagent-imagent グループ識別子_service.exe
jpc_imagent_service.xml	jpc_imagent-imagent グループ識別子_service.xml
jpc_imagentproxy_service.exe	jpc_imagentproxy-imagent グループ識別子_service.exe
jpc_imagentproxy_service.xml	jpc_imagentproxy-imagent グループ識別子_service.xml
jpc_imagentaction_service.exe	jpc_imagentaction-imagent グループ識別子_service.exe
jpc_imagentaction_service.xml	jpc_imagentaction-imagent グループ識別子_service.xml

4. 統合エージェント制御基盤のセカンダリー用の設定を行う。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(d) 統合エージェント制御基盤の設定ファイル」を参照してください。

5. 統合エージェント制御基盤のセカンダリー用のシークレットを登録する。

セカンダリーの統合エージェント制御基盤が接続する JP1/IM - Manager の初期シークレットを取得して登録します。

パスワードによる HTTP 認証 (Basic 認証) が必要な HTTP プロキシサーバを介して JP1/IM - Manager に接続する場合は、HTTP プロキシパスワードをシークレットとして登録してください。

登録する初期シークレットのキー、および HTTP プロキシパスワードのキーについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(e) 初期シークレット、クライアントシークレット、および HTTP プロキシパスワードのキー」を参照してください。

6. 統合エージェント制御基盤以外の設定を行う。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(f) 統合エージェント制御基盤以外の各プログラムの送信設定」を参照してください。

7. サービスの起動設定を行う。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(c) セカンダリーのサービス起動の設定」を参照してください。

8. 次のコマンドを実行して、サービスを有効化する。

Agentパス¥tools¥jpc_service -on サービスキー

サービスキーについては、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10.1 JP1/IM - Agent のサービス」に記載している Windows 環境での JP1/IM - Agent のサービスキーのうち、「-imagent グループ識別子」が付いているものを使用します。

9. JP1/IM - Agent のサービスを起動する。

起動するサービスのサービスキーを次に示します。

- jpc_imagent
- jpc_imagentaction
- jpc_imagentproxy
- jpc_imagent-imagent グループ識別子
- jpc_imagentaction-imagent グループ識別子
- jpc_imagentproxy-imagent グループ識別子
- jpc_alertmanager
- jpc_prometheus_server
- jpc_fluentd

10. OS 起動時の自動起動設定を行う。

自動起動の有効化の設定については、「[1.21.1\(2\)\(a\) 自動起動の有効化](#)」を参照してください。

■ バージョンアップ時の設定

複数マネージャーホストへのデータ配信機能を有効にしているバージョンからのバージョンアップの場合は、下記の手順を実施してください。

下記の手順は、バージョンアップインストール時の「[1.3.1\(3\)\(b\) インストール手順](#)」の手順5のあと（手順6の前）に実施します。

1. 統合エージェント管理基盤のセカンダリー用のファイルを作成する。

Agent パス¥bin 下にあるコピー元のファイルをコピーし、コピー先のファイル名にリネームします。

コピー元のファイル名	コピー先のファイル名
jpc_imagent_service.exe	jpc_imagent-imagent グループ識別子_service.exe
jpc_imagentproxy_service.exe	jpc_imagentproxy-imagent グループ識別子_service.exe
jpc_imagentaction_service.exe	jpc_imagentaction-imagent グループ識別子_service.exe

(j) 複数マネージャーホストへのデータ配信機能を解除する（Windows の場合）（オプション）

複数マネージャーホストへのデータ配信機能を使用しなくなった場合の設定手順を次に示します。

ご使用の運用環境に合わせて、次のどちらかを実施します。

- JP1/IM - Agent のアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する
- JP1/IM - Agent 自体のアンインストールを行う

■ JP1/IM - Agent のアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合

1. JP1/IM - Agent のすべてのサービスを停止する。

サービスが起動中の場合は、次のコマンドを実行して停止する。

```
Agentパス¥tools¥jpc_service_stop -s all
```

2. セカンダリーのサービスを無効化する。

次のコマンドを実行して、統合エージェント制御基盤のセカンダリーのサービスを無効化します。

```
Agentパス¥tools¥jpc_service -off サービスキー
```

サービスを無効化する方法については、「[1.21.1\(1\)\(b\)アドオンプログラムの無効化](#)」の手順 2 と手順 4 を参照してください。

サービスキーについては、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10.1 JP1/IM - Agent のサービス」に記載している Windows 環境での JP1/IM - Agent のサービスキーのうち、「-imagent グループ識別子」が付いているものが該当します。

3. 複数マネージャーホストへのデータ配信機能を使用するために作成したシークレットを削除する。

「[1.21.2\(2\)\(i\) 複数マネージャーホストへのデータ配信機能を設定する \(Windows の場合\) \(オプション\)](#)」の手順 5 で登録した統合エージェント制御基盤のセカンダリー用のシークレットを削除します。

削除するシークレットのキーについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「[3.15.7\(5\)\(e\) 初期シークレット, クライアントシークレット, および HTTP プロキシパスワードのキー](#)」を参照してください。

すでに消えているシークレットについては、この手順は不要です。

4. 複数マネージャーホストへのデータ配信機能を使用するために設定した内容を元に戻す。

「[1.21.2\(2\)\(i\) 複数マネージャーホストへのデータ配信機能を設定する \(Windows の場合\) \(オプション\)](#)」の手順 4 で設定した統合エージェント制御基盤のセカンダリー用の設定を元に戻します。

5. 複数マネージャーホストへのデータ配信機能を使用するためにコピーしたファイルを削除する。

「[1.21.2\(2\)\(i\) 複数マネージャーホストへのデータ配信機能を設定する \(Windows の場合\) \(オプション\)](#)」の手順 3 でコピーした統合エージェント管理基盤のセカンダリー用のファイルを削除します。

6. 複数マネージャーホストへのデータ配信機能を使用するために作成したフォルダを削除する。

ログなどの必要なファイルを退避したあと、「[1.21.2\(2\)\(i\) 複数マネージャーホストへのデータ配信機能を設定する \(Windows の場合\) \(オプション\)](#)」の手順 2 で作成した統合エージェント管理基盤のセカンダリー用のフォルダを削除します。

7. 無効化したセカンダリーのサービスが接続している JP1/IM - Manager 側で登録している統合エージェント情報を削除する。

統合エージェント情報の削除手順については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.1 [統合エージェント一覧] 画面」を参照してください。

■ JP1/IM - Agent 自体のアンインストールを行う場合

「1.25.1(5) JP1/IM - Agent のアンインストールの手順」の手順 1 と手順 2 の間に、上記の「JP1/IM - Agent のアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合」の手順 3 から手順 6 を実施します。

実施後に、上記の「JP1/IM - Agent のアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合」の手順 7 を実施します。

(3) Prometheus server の設定

(a) ポートを変更する (Windows の場合) (オプション)

Prometheus server が使用するリスンポートは、prometheus コマンドの--web.listen-address オプションに指定します。

prometheus コマンドのオプションの変更方法については、「1.21.2(1)(c) コマンドラインオプションを変更する (Windows の場合)」を参照してください。また、--web.listen-address オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「サービス定義ファイル (jpc_プログラム名_service.xml)」(2. 定義ファイル) の「prometheus コマンドのオプション」を参照してください。

なお、デフォルトのポートは「20713」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。ただし、他ホストの Blackbox exporter による外形監視で Prometheus server を監視する場合は、アクセスを許可します。この場合、必要に応じて送信元 IP アドレスを制限するなどセキュリティ対策を検討してください。

(b) アラート定義を追加する (Windows の場合) (オプション)

アラート定義は、アラート設定ファイル (jpc_alerting_rules.yml) に定義します。

アラート設定ファイルの編集方法については、「1.21.2(1)(a) 設定ファイルを編集する (Windows の場合)」を参照してください。

アラート定義で設定が必要な項目については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の、「3.15.1(3)(a)アラート評価機能」の「JP1 イベントに変換するためのアラートルール定義」を参照してください。また、各項目の詳細およびアラート定義のサンプルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「アラート設定ファイル (jpc_alerting_rules.yml)」(2. 定義ファイル) を参照してください。

メモ

アラート定義を作成するときのポイントを次に示します。

- JP1/IM - Agent の性能監視機能では、期間 (for) を指定できます。指定した期間に継続してアラート条件に該当した場合、発火と判定されます。
- メトリックが存在することを検知したい場合は、アラート条件で `absent()` 関数を使用して実現します。

`absent(メトリック{ラベル})`

- 特定期間だけアラートを有効にしたい場合は、アラート条件に PromQL を使用して設定します。

(例) 日本時刻で 8 時から 12 時まで監視する場合

アラート条件 `and ON() (23 <= hour() or 0 <= hour() < 3)`

「`hour()`」は UTC の時刻を返却するため、UTC を考慮する必要がある点に注意してください。

- JP1/IM - Agent の性能監視機能では発火と回復が通知されます。警告と異常の 2 段階で通知させたい場合は、警告用のアラートと異常用のアラートを作成してください。
- アラート発生時に表示するメッセージには、次の内容を指定できます。
 - ・発火時のメッセージ
 - ・回復時のメッセージ
- アラートのメッセージに埋め込むことができる変数については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(3)(a)アラート評価機能」を参照してください。

重要

アラート定義は、各アラート定義で評価される時系列データ数の合計が 150 未満となるように設定してください。

たとえば、Windows のネットワークインターフェースに関するアラートを 3 つ作成したとして、Windows ホストにネットワークインターフェースが 4 つある場合、Windows exporter が収集するネットワークインターフェースの時系列データは 4 つ生成されます。

このため、4 つの時系列データが 3 つのアラートで評価されることになるので、合計で時系列データは $4 * 3 = 12$ 個となります。

(c) Blackbox exporter のスクレイプジョブを追加する (Windows の場合) (オプション)

Blackbox exporter のスクレイプジョブを追加する前に、Blackbox exporter の設定ファイルにモジュールを追加する必要があります。詳細については、「[1.21.2\(6\)\(b\) モジュールを追加・変更・削除する \(Windows の場合\) \(オプション\)](#)」を参照してください。

モジュールを追加したあとに、次の手順を実施して、新しく作成したモジュールをスクレイプするスクレイプジョブを設定します。

1. Blackbox exporter のディスカバリ設定ファイルを作成する。

次に示すコピー元のモデルファイルをコピーし、コピー先の定義ファイル名にリネームすることで、Blackbox exporter のディスカバリ設定ファイルを作成します。

■HTTP/HTTPS 監視を行う場合

- Windows の場合

コピー元：Agent パス¥conf¥jpc_file_sd_config_blackbox_http.yml.model

コピー先：Agent パス¥conf¥file_sd_config_blackbox_http で始まるモジュール

- Linux の場合

コピー元：/opt/jp1ima/conf/jpc_file_sd_config_blackbox_http.yml.model

コピー先：/opt/jp1ima/conf/file_sd_config_blackbox_http で始まるモジュール名.yml

■ICMP 監視を行う場合

- Windows の場合

コピー元：Agent パス¥conf¥jpc_file_sd_config_blackbox_icmp.yml.model

コピー先：Agent パス¥conf¥file_sd_config_blackbox_icmp で始まるモジュール名.yml

- Linux の場合

コピー元：/opt/jp1ima/conf/jpc_file_sd_config_blackbox_icmp.yml.model

コピー先：/opt/jp1ima/conf/file_sd_config_blackbox_icmp で始まるモジュール名.yml

モジュール名は、「[1.21.2\(6\)\(b\) モジュールを追加・変更・削除する \(Windows の場合\) \(オプション\)](#)」で追加したモジュールを示します。

2. Blackbox exporter のディスカバリ設定ファイルを編集する。

- HTTP/HTTPS 監視のディスカバリ設定ファイルの場合

記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Blackbox exporter (HTTP/HTTPS 監視) のディスカバリ設定ファイル (jpc_file_sd_config_blackbox_http.yml)」(2. 定義ファイル)を参照してください。

- ICMP 監視のディスカバリ設定ファイルの場合

記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル (jpc_file_sd_config_blackbox_icmp.yml)」(2. 定義ファイル)を参照してください。

3. 統合オペレーション・ビューアーを使用して定義ファイルを追加する。

定義ファイルを追加する手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

4. Prometheus 設定ファイルにスクレイプジョブを追加する。

- HTTP/HTTPS 監視を行う場合

Prometheus 設定ファイル (jpc_prometheus_server.yml) で、ジョブ名が「jpc_blackbox_http」のスクレイプジョブの定義をコピーして、新しいスクレイプジョブを追加します。

- ICMP 監視を行う場合

Prometheus 設定ファイル (jpc_prometheus_server.yml) で、ジョブ名「jpc_blackbox_icmp」のスクレイプジョブの定義をコピーして、新しいスクレイプジョブを追加します。

<設定例>

```
scrape_configs:
- job_name: 任意のスクレイプジョブ名
  metrics_path: /probe
  params:
    module: [モジュール名]
  file_sd_configs:
    - files:
        - 'ディスカバリ設定ファイル名'
  relabel_configs:
    (省略)
  metric_relabel_configs:
    (省略)
```

任意のスクレイプジョブ名

ほかのスクレイプジョブ名と重複しない任意の名前を、1～255 文字の範囲で、制御文字以外の文字で指定します。

モジュール名

「[1.21.2\(6\)\(b\) モジュールを追加・変更・削除する \(Windows の場合\) \(オプション\)](#)」で追加したモジュール名を指定します。

ディスカバリ設定ファイル名

手順 1 で作成したファイル名を指定します。

Prometheus 設定ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Prometheus 設定ファイル (jpc_prometheus_server.yml)」(2. 定義ファイル) の<scrape_config>を参照してください。

Prometheus 設定ファイルを編集する手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

(d) ユーザー独自の Exporter のスクレイプジョブを追加する (Windows の場合) (オプション)

ユーザー独自の Exporter をスクレイプするには、次の設定が必要です。

- ユーザー独自のディスカバリ設定ファイルの追加
- Prometheus 設定ファイル (jpc_prometheus_server.yml) の編集

各定義ファイルを追加・編集する手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

1. ユーザー独自のディスカバリ設定ファイルを追加する。

スクレイプしたいユーザー独自の Exporter を、ユーザー独自のディスカバリ設定ファイルに指定します。

記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユーザー独自のディスカバリ設定ファイル (user_file_sd_config_任意の名前.yml)」(2. 定義ファイル) を参照してください。

2. Prometheus 設定ファイルにスクレイプジョブを追加する。

Prometheus 設定ファイル (jpc_prometheus_server.yml) に、ユーザー独自の Exporter をスクレイプするためのスクレイプジョブを追加します。

スクレイプジョブは scrape_configs の中に記載します。

<設定例>

```
scrape_configs:
- job_name: スクレイプジョブ名

  file_sd_configs:
  - files:
    - ディスカバリ設定ファイル名

  relabel_configs:
  - target_label: jpl_pc_nodelabel
    replacement: IM管理ノードのラベルに表示する文字列

  metric_relabel_configs:
  - source_labels: ['__name__']
    regex: 'メトリック1|メトリック2|メトリック3'
    action: 'keep'
```

スクレイプジョブ名

任意の文字列を指定します。この値がメトリックの job ラベルに設定されます。

ディスカバリ設定ファイル名

上記の手順 1 で作成したユーザー独自のディスカバリ設定ファイルのファイル名を指定します。

メトリック 1, メトリック 2, メトリック 3

収集したいメトリックを指定します。収集したいメトリックが複数存在する場合は、「|」で区切って指定します。

すべてのメトリックを収集したい場合は、「metric_relabel_configs」の記載は不要です。ただし、メトリックが大量に存在した場合に、データ量が増加するため、「metric_relabel_configs」を記載し、監視するメトリックだけに絞ることを推奨します。

IM 管理ノードのラベルに表示する文字列

統合オペレーション・ビューアーで IM 管理ノードのラベルに表示する文字列を制御文字以外の文字で指定します。

値は、URL エンコードしたときの文字列が、234 バイト以内（すべてマルチバイト文字の場合の上限は 26 文字）となるようにしてください。JP1/IM - Agent が作成する IM 管理ノードのラベルと同じ値を指定することはできません。同一ホスト内で重複しない文字列を指定してください。重複する文字列を指定した場合、構成情報の SID が同一となり、正しく IM 管理ノードが作成されません。

3. メトリック定義ファイルを追加する。

ユーザー独自の Exporter 用のメトリック定義ファイルを追加します。

記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユーザー独自のメトリック定義ファイル（metrics_任意の Prometheus トレンド名.conf）」（2. 定義ファイル）を参照してください。

(e) リモートライト先を変更する（Windows の場合）（オプション）

リモートライト先は、Prometheus 設定ファイル（jpc_prometheus_server.yml）の remote_write.url に、同じホスト上で稼働する imagentproxy プロセスの URL とポートを指定します。imagentproxy プロセスのポートを変更する場合にだけ、変更が必要です。

<設定例>

```
remote_write:
- url: http://localhost:20727/ima/api/v1/proxy/service/promscale/write
```

設定ファイルを変更する手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する（Windows の場合）](#)」を参照してください。

(f) サービス監視の設定をする（Windows の場合）（オプション）

JP1/IM - Agent 13-00 から 13-01 以降にバージョンアップインストールした環境で、サービス監視機能を使用する場合、次の設定を行います。JP1/IM - Agent 13-01 以降を新規インストールした場合は、この設定は不要です。

■ Prometheus 設定ファイル（jpc_prometheus_server.yml）の編集

jpc_windows スクレイプジョブの metric_relabel_configs の設定で、メトリックを保持する設定に「windows_service_state」が設定されていない場合、設定を追加します。また、同じ metric_relabel_configs の設定で、「windows_service_.*」メトリックに対する relabel config が設定されていない場合、設定を追加します。下記のとおり到下線部分の設定を追加します。

```
(省略)
scrape_configs:
(省略)
- job_name: 'jpc_windows'
(省略)
  metric_relabel_configs:
```

```

- source_labels: ['__name__']
  regex: 'windows_cs_physical_memory_bytes|windows_cache_copy_read_hits_total| (省略)
|windows_process_working_set_peak_bytes|windows_process_working_set_bytes|windows_service_st
ate'
  action: 'keep'
- source_labels: ['__name__']
  regex: 'windows_process.*'
  target_label: 'jp1_pc_trendname'
  replacement: 'windows_exporter_process'
- source_labels: ['__name__', 'process']
  regex: 'windows_process.*;(.)'
  target_label: 'jp1_pc_nodelabel'
  replacement: '${1}'
- source_labels: ['__name__']
  regex: 'windows_service.*'
  target_label: 'jp1_pc_trendname'
  replacement: 'windows_exporter_service'
- source_labels: ['__name__']
  regex: 'windows_service.*'
  target_label: 'jp1_pc_category'
  replacement: 'service'
- source_labels: ['__name__', 'name']
  regex: 'windows_service.*;(.)'
  target_label: 'jp1_pc_nodelabel'
  replacement: '${1}'
- regex: jp1_pc_multiple_node
  action: labeldrop

```

■ Windows exporter のディスカバリ設定ファイル (jpc_file_sd_config_windows.yml) の編集

jp1_pc_multiple_node の設定に、「windows_service_state」が設定されていない場合、下記のとおり
下線部分の設定を追加します。

```

- targets:
  - ホスト名:20717
  labels:
    jp1_pc_exporter: JPC Windows exporter
    jp1_pc_category: platform
    jp1_pc_trendname: windows_exporter
    jp1_pc_multiple_node: "{__name__=~'windows_process.*|windows_service.*'}"

```

(g) IM 管理ノードのラベル名 (jp1_pc_nodelabel の値) が上限を超える場合の設定を する (Windows の場合) (オプション)

IM 管理ノードのラベル名 (jp1_pc_nodelabel の値) の長さの上限は、URL エンコードしたときの文字
列で 234 バイトです (すべてマルチバイト文字の場合の上限は 26 文字です)。上限を超える場合、
Prometheus 設定ファイル (jpc_prometheus_server.yml) の metric_relabel_configs で、
jp1_pc_nodelabel の値を変更する必要があります。値を変更しなかった場合、IM 管理ノードを作成する
操作を行ったときに、その値をもつ IM 管理ノードは作成されません。

値を変更する場合、Prometheus 設定ファイル (jpc_prometheus_server.yml) のスクレイプジョブの、metric_relabel_configs の設定に、次の下線部分の設定を追加します。複数の監視対象で値を変更するときは、監視対象の数だけ設定を追加します。

■ Prometheus 設定ファイル (jpc_prometheus_server.yml) の編集

```
(省略)
scrape_configs:
  (省略)
  - job_name: 'スクレイプジョブ名'
  (省略)
    metric_relabel_configs:
  (省略)
    - source_labels: ['jp1_pc_nodelabel']
      regex: 'jp1_pc_nodelabelの変更前の値にマッチする正規表現'
      target_label: 'jp1_pc_nodelabel'
      replacement: 'jp1_pc_nodelabelの変更後の値'
```

(h) SAP システムのログ抽出コマンドを Script exporter を使用して実行する場合の設定 (Windows の場合) (オプション)

次の手順を実施します。

1. Prometheus 設定ファイルのスクレイプ定義を編集する。

SAP システムのログ抽出コマンドを、Script exporter の http_sd_config 方式を使用して実行する場合は、Script exporter のスクレイプ定義を、下記の下線部分のように変更します。

- Prometheus 設定ファイル (jpc_prometheus_server.yml) の編集

```
(省略)
scrape_configs:
  (省略)

  - job_name: 'jpc_script'

    http_sd_configs:
      - url: 'http://インストールホスト名:ポート/discovery'
  (省略)

    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'script_success|script_duration_seconds|script_exit_code'
        action: 'keep'
      - source_labels: [jp1_pc_script]
        target_label: jp1_pc_nodelabel
      - source_labels: [jp1_pc_script]
        regex: '.*jr3slget.*|.*jr3alget.*'
        target_label: 'jp1_pc_category'
        replacement: 'enterprise'
      - regex: (jp1_pc_script|jp1_pc_multiple_node|jp1_pc_agent_create_flag)
        action: labeldrop
```

(i) Web exporter のスクレイプジョブを追加する (Windows の場合) (オプション)

1. Prometheus 設定ファイルにデフォルトのスクレイプジョブを追加する。

JP1/IM - Agent 13-10 以降を新規にインストールした場合は、実施不要です。

JP1/IM - Agent を 13-10 より前のバージョンから 13-10 以降にバージョンアップした場合、JP1/IM - Agent のインストール先¥jplima¥conf フォルダに格納されている Prometheus 設定ファイルのモデルファイルが更新されます。Prometheus 設定ファイルのモデルファイル (jpc_prometheus_server.yml.model) の次の内容を Prometheus 設定ファイル (jpc_prometheus_server.yml) の scrape_configs 配下に追記します。

論理ホスト運用の場合は、共有フォルダ¥jplima¥conf¥jpc_prometheus_server.yml を更新します。

<追記する内容>

```
scrape_configs:
  - job_name: 'jpc_web_probe'
    scrape_interval: 6m
    scrape_timeout: 5m
    metrics_path: /probe
    file_sd_configs:
      - files:
        - 'jpc_file_sd_config_web.yml'
    relabel_configs:
      (省略)
    metric_relabel_configs:
      (省略)
```

2. Web exporter のディスカバリ設定ファイルを追加する (オプション)。

Web シナリオ監視を行う場合、新しいスクレイプジョブを追加するときは、新しくディスカバリ設定ファイルを作成します。

次に示す Web exporter のディスカバリ設定ファイルのモデルファイルをひな形としてコピーし、コピー先の定義ファイル名にリネームしてディスカバリ設定ファイルを作成します。

コピー元：Agent パス¥conf¥jpc_file_sd_config_web.yml.model

コピー先：Agent パス¥conf¥user¥file_sd_config_web_任意の名前.yml

Web exporter のディスカバリ設定ファイルの形式については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Web exporter のディスカバリ設定ファイル (jpc_file_sd_config_web.yml)」(2. 定義ファイル) を参照してください。

Web exporter のディスカバリ設定ファイルを編集する手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

3. Prometheus 設定ファイルに新しいスクレイプジョブを追加する (オプション)。

Web シナリオ監視を行う場合、新しいスクレイプジョブを追加するときは、Prometheus 設定ファイル (jpc_prometheus_server.yml) で、値が「jpc_web_probe」であるスクレイプジョブの定義をコピーして、新しいスクレイプジョブを追加します。

<設定例>

```

scrape_configs:
- job_name: 任意のスクレイプジョブ名
  scrape_interval: スクレイプ要求の間隔
  scrape_timeout: スクレイプ要求のタイムアウト時間
  metrics_path: /probe
  file_sd_configs:
    - files:
        - 'user/ディスカバリ設定ファイル名'
  relabel_configs:
    (省略)
  metric_relabel_configs:
    (省略)

```

任意のスクレイプジョブ名

ほかのスクレイプジョブ名と重複しない任意の名前を、1～255 文字の範囲で、制御文字以外の文字で指定します。

Prometheus 設定ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Prometheus 設定ファイル (jpc_prometheus_server.yml)」(2. 定義ファイル) の<scrape_config>を参照してください。

Prometheus 設定ファイルを編集する手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

(j) VMware exporter のスクレイプジョブを追加する (Windows の場合だけ) (オプション)

1. Prometheus 設定ファイルにデフォルトのスクレイプジョブを追加する。

JP1/IM - Agent 13-10 以降を新規にインストールした場合は、実施不要です。

JP1/IM - Agent を 13-10 より前のバージョンから 13-10 以降にバージョンアップした場合、JP1/IM - Agent のインストール先¥jp1ima¥conf フォルダに格納されている Prometheus 設定ファイルのモデルファイルが更新されます。Prometheus 設定ファイルのモデルファイル (jpc_prometheus_server.yml.model) の次の内容を Prometheus 設定ファイル (jpc_prometheus_server.yml) の scrape_configs 配下に追記します。

論理ホスト運用の場合は、共有フォルダ¥jp1ima¥conf¥jpc_prometheus_server.yml を更新します。

<追記する内容>

```

scrape_configs:
- job_name: 'jpc_vmware'
  params:
    section: ['section']
  file_sd_configs:
    - files:
        - 'jpc_file_sd_config_vmware.yml'
  relabel_configs:
    (省略)
  metric_relabel_configs:
    - source_labels: [vm_name]
      regex: '(.*)'
      target_label: instance
      action: replace

```



```

- source_labels: ['ds_name']
  regex: '(.*)'
  target_label: instance
  replacement: ${1}
- source_labels: ['ds_name']
  regex: '(.*)_(.*)'
  target_label: instance
  replacement: ${1}
- source_labels: ['vm_name', '__name__']
  regex: '(.*)vmware_vm_.*'
  target_label: instance
  replacement: ${1}
  action: replace
- source_labels: ['host_name', '__name__']
  regex: '(.*)vmware_host_.*'
  target_label: instance
  replacement: ${1}
  action: replace
- source_labels: ['__name__']
  regex: 'vmware_host_.*|vmware_datastore_.*'
  target_label: jpl_pc_trendname
  replacement: vmware_exporter_host
- source_labels: ['__name__']
  regex: 'vmware_vm_.*'
  target_label: jpl_pc_trendname
  replacement: vmware_exporter_vm
(省略)

```

2. Prometheus 設定ファイルにスクレイプジョブを追加する。

VMware exporter のスクレイプジョブを追加する前に、VMware exporter の設定ファイルにセクションを追加する必要があります。詳細については、「[1.21.2\(14\)\(b\) セクションを追加・変更・削除する \(Windows の場合\) \(必須\)](#)」を参照してください。

セクションを追加したあと、次の手順を実施して、新しく作成したセクションをスクレイプするスクレイプジョブを設定します。

VMware ESXi の監視を行う場合、Prometheus 設定ファイル (jpc_prometheus_server.yml) で、ジョブ名が「jpc_vmware」であるスクレイプジョブの定義をコピーして、新しいスクレイプジョブを追加します。

また、新しいセクションを追加で監視を行う場合も、Prometheus 設定ファイル (jpc_prometheus_server.yml) で、ジョブ名が「jpc_vmware」であるスクレイプジョブの定義をコピーして、新しいスクレイプジョブを追加します。この場合、params のセクション名には、VMware exporter 設定ファイル (jpc_vmware_exporter.yml) で設定したセクション名を記載します。

<設定例>

```

scrape_configs:
- job_name: 任意のスクレイプジョブ名
  params:
    section: ['セクション名']
  file_sd_configs:
    - files:
        - 'jpc_file_sd_config_vmware.yml'
  relabel_configs:
(省略)

```



```
metric_relabel_configs:
- source_labels: [vm_name]
  regex: '(.*)'
  target_label: instance
  action: replace
- source_labels: ['ds_name']
  regex: '(.*)'
  target_label: instance
  replacement: ${1}
- source_labels: ['ds_name']
  regex: '(.*)_(.*)'
  target_label: instance
  replacement: ${1}
- source_labels: ['vm_name', '__name__']
  regex: '(.*);vmware_vm_.*'
  target_label: instance
  replacement: ${1}
  action: replace
- source_labels: ['host_name', '__name__']
  regex: '(.*);vmware_host_.*'
  target_label: instance
  replacement: ${1}
  action: replace
- source_labels: ['__name__']
  regex: 'vmware_host_.*|vmware_datastore_.*'
  target_label: jp1_pc_trendname
  replacement: vmware_exporter_host
- source_labels: ['__name__']
  regex: 'vmware_vm_.*'
  target_label: jp1_pc_trendname
  replacement: vmware_exporter_vm
(省略)
```

任意のスクレイプジョブ名

先頭の「jpc_vmware」は変更せずにアンダースコア（_）を付与し、その後ろにほかのスクレイプジョブ名と重複しない任意の名前を、1～255文字の範囲で、制御文字以外の文字で指定します。

セクション名

「[1.21.2\(14\)\(b\) セクションを追加・変更・削除する（Windows の場合）（必須）](#)」で追加したセクション名を指定します。

セクション名は、シングルクォーテーション「'」またはダブルクォーテーション「"」で囲みます。

Prometheus 設定ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Prometheus 設定ファイル (jpc_prometheus_server.yml)」(2. 定義ファイル) の<scrape_config>を参照してください。

Prometheus 設定ファイルを編集する手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する（Windows の場合）](#)」を参照してください。

(k) Windows exporter (Hyper-V 監視) のスクレイプジョブを追加する (Windows の場合だけ) (オプション)

1. Prometheus 設定ファイルにデフォルトのスクレイプジョブを追加する。

JP1/IM - Agent 13-11 以降を新規にインストールした場合は、実施不要です。

JP1/IM - Agent を 13-11 より前のバージョンから 13-11 以降にバージョンアップした場合、JP1/IM - Agent のインストール先¥jplima¥conf フォルダに格納されている Prometheus 設定ファイルのモデルファイルが更新されます。Prometheus 設定ファイルのモデルファイル (jpc_prometheus_server.yml.model) の次の内容を Prometheus 設定ファイル (jpc_prometheus_server.yml) の scrape_configs 配下に追記します。

論理ホストの場合は、共有フォルダ¥jplima¥conf¥jpc_prometheus_server.yml を更新します。

<追記する内容>

```
scrape_configs:
  - job_name: 'jpc_hyperv'

    file_sd_configs:
      - files:
        - 'jpc_file_sd_config_windows_hyperv.yml'

    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'windows_hyperv_vm_cpu_total_run_time|windows_hyperv_vm_device_bytes_writ
en|windows_hyperv_vm_device_bytes_read|windows_hyperv_host_cpu_total_run_time|windows_hyp
erv_vswitch_bytes_received_total|windows_hyperv_vswitch_bytes_sent_total|windows_cs_logic
al_processors|windows_hyperv_vm_cpu_hypervisor_run_time'
        action: 'keep'
      - source_labels: ['__name__']
        regex: 'windows_hyperv_host_.*|windows_hyperv_vswitch_.*|windows_hyperv_vm_cpu_.*
|windows_cs_.*'
        target_label: jp1_pc_nodelabel
        replacement: Hyperv metric collector(Hypervisor)
      - source_labels: ['__name__', 'instance']
        regex: 'windows_hyperv_vm_device_.*;([^:]+):?.*'
        target_label: jp1_pc_nodelabel
        replacement: 'Hyperv metric collector(VM) Hypervisor:${1}'
      - source_labels: ['__name__', 'instance']
        regex: 'windows_hyperv_vm_cpu_total_run_time;([^:]+):?.*'
        target_label: jp1_pc_nodelabel
        replacement: 'Hyperv metric collector(VM) Hypervisor:${1}'
      - source_labels: ['vm', '__name__']
        regex: '(.*)windows_hyperv_vm_cpu_total_run_time'
        target_label: instance
        replacement: ${1}
        action: replace
      - source_labels: ['vm_device']
        regex: '^(.*)-([^-]*)?(?:_[^.]*)?¥.[^.]*$'
        target_label: instance
        replacement: ${2}
        action: replace
      - source_labels: ['__name__']
        regex: 'windows_hyperv_host_.*|windows_hyperv_vswitch_.*|windows_hyperv_vm_cpu_hy
pervisor_.*|windows_cs_.*'
        target_label: jp1_pc_trendname
        replacement: windows_exporter_hyperv_host
      - source_labels: ['__name__']
        regex: 'windows_hyperv_host_.*|windows_hyperv_vswitch_.*|windows_hyperv_vm_cpu_hy
pervisor_.*|windows_cs_.*'
        target_label: jp1_pc_category
```

```

replacement: VirtualMachine Host
- source_labels: ['__name__']
  regex: 'windows_hyperv_vm_device_.*|windows_hyperv_vm_cpu_total_run_time'
  target_label: jp1_pc_trendname
  replacement: windows_exporter_hyperv_vm
- source_labels: ['__name__']
  regex: 'windows_hyperv_vm_device_.*|windows_hyperv_vm_cpu_total_run_time'
  target_label: 'jp1_pc_remote_monitor_instance'
  replacement: 'JP1/IM - Agentのインストールホスト名:Hyperv metric collector(VM)'
  action: 'replace'

```

(4) Alertmanager の設定

(a) ポートを変更する (Windows の場合) (オプション)

Alertmanager が使用するリスンポートは、alertmanager コマンドの--web.listen-address オプションに指定します。

alertmanager コマンドのオプションの変更方法については、「[1.21.2\(1\)\(c\) コマンドラインオプションを変更する \(Windows の場合\)](#)」を参照してください。また、--web.listen-address オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「サービス定義ファイル (jpc_プログラム名_service.xml)」(2. 定義ファイル) の「alertmanager コマンドのオプション」を参照してください。

なお、デフォルトのポートは「20714」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。ただし、他ホストの Blackbox exporter による外形監視で Alertmanager を監視する場合は、アクセスを許可します。この場合、必要に応じて送信元 IP アドレスを制限するなどセキュリティ対策を検討してください。

(b) アラート通知先を変更する (Windows の場合) (オプション)

アラート通知先は、Alertmanager 設定ファイル (jpc_alertmanager.yml) の receivers.webhook_configs.url に、アラート通知先は同じホスト上で稼働する imagentproxy プロセスの URL とポートを指定します。imagentproxy プロセスのポートを変更する場合にだけ、変更が必要です。

設定ファイルを変更する手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

(c) サイレンスを設定する (Windows の場合) (オプション)

サイレンスを設定したい Alertmanager が稼働しているホストに対して、JP1/IM - Manager からコマンドを実行します。curl コマンドを使用して、サイレンスの設定を行う REST API を呼び出します。

サイレンスを設定する REST API については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.22.4 Alertmanager のサイレンス作成」を参照してください。

リクエストのメッセージボディーに指定するサイレンスの設定内容は、curl コマンドの引数で渡します。

(5) Windows exporter の設定

(a) ポートを変更する (オプション)

Windows exporter が使用するリスンポートは、windows_exporter コマンドの--telemetry.addr オプションに指定します。

windows_exporter コマンドのオプションの変更方法については、「[1.21.2\(1\)\(c\) コマンドラインオプションを変更する \(Windows の場合\)](#)」を参照してください。また、--telemetry.addr オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「サービス定義ファイル (jpc_プログラム名_service.xml)」(2. 定義ファイル) の「windows_exporter コマンドのオプション」を参照してください。

なお、デフォルトのポートは「20717」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

(b) 収集するメトリックを変更する (オプション)

1. Prometheus 設定ファイルにメトリックを追加する。

Prometheus 設定ファイル (jpc_prometheus_server.yml) の metric_relabel_configs に、収集するメトリックが「[]」で区切って定義されています。収集する必要がないメトリックを削除し、収集するメトリックを追加します。

設定ファイルを更新する手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

<設定例>

```
- job_name: 'jpc_windows'
  :
  metric_relabel_configs:
    - source_labels: ['__name__']
      regex: 'windows_cache_copy_read_hits_total|windows_cache_copy_reads_total|windows_cpu_time_total|windows_logical_disk_free_bytes|windows_logical_disk_idle_seconds_total|windows_logical_disk_read_bytes_total| . . . |windows_net_packets_sent_total|windows_net_packets_received_total|windows_system_context_switches_total|windows_system_processor_queue_length|windows_system_system_calls_total【ここにメトリクスを追加します】'
      action: 'keep'
```

2. 必要に応じて、メトリック定義ファイルにトレンド表示の定義を行う。

Windows exporter および Windows exporter (プロセス監視) のメトリック定義ファイルに、トレンド表示の定義を行います。

記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Windows exporter のメトリック定義ファイル (metrics_windows_exporter.conf)」(2. 定義ファイル) および「Windows exporter (プロセス監視) のメトリック定義ファイル (metrics_windows_exporter_process.conf)」(2. 定義ファイル) を参照してください。

3. サービス監視の設定を行う。

■Windows exporter 設定ファイル (jpc_windows_exporter.yml) の編集
サービス監視を行う場合、下記の下線部分のとおり、Windows exporter 設定ファイル (jpc_windows_exporter.yml) の編集を行います。

```
collectors:
  enabled: cache,cpu,logical_disk,memory,net,system,cs,process,service
collector:
  logical_disk:
    volume-whitelist: ".+"
    volume-blacklist: ""
  net:
    nic-whitelist: ".+"
    nic-blacklist: ""
  process:
    whitelist: ""
    blacklist: ""
  service:
    services-where: "WQLのWhere句"
scrape:
  timeout-margin: 0.5
```

「collectors」の「enabled」に「service」が設定されていない場合、「service」の設定を追加します。
「collector」の「service」が設定されていない場合、「service」と「services-where」の行を追加します。「services-where」の値は、WQLのWhere句で、監視したいサービスのサービス名を「Name='サービス名」の形式で設定します。サービス名は完全一致で設定し、複数のサービスを監視する場合は、OR でつなげて、「Name=' サービス名' OR Name=' サービス名' OR …」の形式で設定します。

■Windows exporter 設定ファイル (jpc_windows_exporter.yml) の定義例
jpc_imagent と jpc_imagentproxy のサービスを監視する場合の定義例を、次に示します。

```
collectors:
  enabled: cache,cpu,logical_disk,memory,net,system,cs,process,service
collector:
  logical_disk:
    volume-whitelist: ".+"
    volume-blacklist: ""
  net:
    nic-whitelist: ".+"
    nic-blacklist: ""
  process:
    whitelist: ""
    blacklist: ""
  service:
    services-where: "Name=' jpc_imagent' OR Name=' jpc_imagentproxy'"
scrape:
  timeout-margin: 0.5
```

(c) 監視対象プロセスの指定 (必須)

■Windows exporter 設定ファイル (jpc_windows_exporter.yml) の編集

Windows exporter 設定ファイル (jpc_windows_exporter.yml) を編集し、監視対象プロセスを定義します。

デフォルトでは、すべてのプロセスが監視対象外となるため、監視したいプロセスの指定を Windows exporter 設定ファイルで行います。

Windows exporter 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Windows exporter 設定ファイル (jpc_windows_exporter.yml)」(2. 定義ファイル) を参照してください。

(6) Blackbox exporter の設定

(a) ポートを変更する (Windows の場合) (オプション)

Blackbox exporter が使用するリッスンポートは、blackbox_exporter コマンドの--web.listen-address オプションに指定します。

blackbox_exporter コマンドのオプションの変更方法については、「[1.21.2\(1\)\(c\) コマンドラインオプションを変更する \(Windows の場合\)](#)」を参照してください。また、--web.listen-address オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「サービス定義ファイル (jpc_プログラム名_service.xml)」(2. 定義ファイル) の「blackbox_exporter コマンドのオプション」を参照してください。

なお、デフォルトのポートは「20715」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

(b) モジュールを追加・変更・削除する (Windows の場合) (オプション)

Blackbox exporter では、監視対象 (ホストや URL) ごとに、プロトコル、認証情報などの監視方法を定義する必要があります。

初期設定で定義されているモジュールは、次のとおりです。

表 1-14 初期設定で定義されているモジュール

モジュール名	特徴
http	• http/https を監視します。 • メソッドは「GET」で、ヘッダは設定しません。 • クライアント認証、サーバ認証、HTTP 認証 (Basic 認証) は行いません。 • http/https の URL に対してアクセスし、200 番台のステータスコードが返却された場合、probe_success メトリックに 1 を設定します。 • URL に対して通信できない、または、ステータスコードが 200 番台でない場合、probe_success メトリックに 0 を設定します。 • 監視対象がリダイレクトする場合は、リダイレクト先のステータスコードに依存します。

1. インストールとセットアップ (Windows の場合)

モジュール名	特徴
icmp	- icmp を監視します。 - 認証は行いません。 - 監視対象のホストまたは IP アドレスに対して、icmp で通信できた場合、probe_success メトリックに 1 を設定します。通信できない場合、0 を設定します。

初期設定のモジュールで監視できる場合は、新たに定義する必要はありません。次に示すように、初期設定のモジュールでは監視できない要件がある場合は、モジュール定義を追加する必要があります。

- 認証が必要な場合
- レスポンスの内容によって判定を変更したい場合

モジュールは、Blackbox exporter 設定ファイルに定義します。記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Blackbox exporter 設定ファイル (jpc_blackbox_exporter.yml)」(2. 定義ファイル) を参照してください。

記述規則を次に示します。

- 新しいモジュール名は、次のように設定してください。
 - HTTP/HTTPS 監視を行う場合
http で始まる名称を設定します。
 - ICMP 監視の場合
icmp で始まる名称を設定します。
- クライアント認証、サーバ認証、HTTP 認証 (Basic 認証) を行うモジュールを作成する場合、証明書やパスワードの設定が必要となります。

証明書の配置先については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 A.4 JP1/IM - Agent」のファイルおよびディレクトリ一覧を参照してください。

HTTP 認証 (Basic 認証) のパスワードの設定方法については、「[1.21.2\(6\)\(e\) プロキシ認証の認証 ID とパスワードを設定する \(Windows の場合\) \(オプション\)](#)」と「[1.21.2\(6\)\(f\) 監視対象の Web サーバにアクセスするための認証 ID, パスワード, Bearer トークンを設定する \(Windows の場合\) \(オプション\)](#)」を参照してください。

表 1-15 監視条件と必要な設定

監視条件	必要なファイル	必要な設定
サーバー認証する	監視対象が持つサーバー証明書を発行した認証局の CA 証明書を Agent パス/conf/user/cert に配置します。	Blackbox exporter 設定ファイルの <code>tls_config</code> に下記を設定します。 • <code>ca_file</code> に CA 証明書のパスを設定 • <code>insecure_skip_verify</code> に <code>false</code> を設定
サーバー認証しない	なし。	Blackbox exporter 設定ファイルの <code>tls_config</code> に下記を設定します。 • <code>insecure_skip_verify</code> に <code>true</code> を設定

監視条件	必要なファイル	必要な設定
クライアント認証する	- クライアント証明書を Agent パス/conf/user/cert に配置します。 - クライアント証明書キーファイルを Agent パス/conf/user/secret に配置します。	Blackbox exporter 設定ファイルの <code>tls_config</code> に下記を設定します。 <code>cert_file</code> にクライアント証明書パスを設定 <code>key_file</code> にクライアント証明書キーファイルを設定
クライアント認証しない	なし。	なし。
Basic 認証する	なし。	Blackbox exporter 設定ファイルの <code>basic_auth</code> に下記を設定します。 <code>username</code> に Basic 認証に使用するユーザー名を設定 Basic 認証のパスワードの設定については、「 1.21.2(6)(f) 監視対象の Web サーバにアクセスするための認証 ID、パスワード、Bearer トークンを設定する (Windows の場合) (オプション) 」を参照してください。

Blackbox exporter 設定ファイルの更新、証明書ファイルの配置の手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

Blackbox exporter から監視対象 Web サーバにアクセスする際にプロキシサーバを経由する必要がある場合は、プロキシサーバの設定が必要です。「[1.21.2\(6\)\(d\) プロキシ経由で HTTP 監視をする \(Windows の場合\) \(オプション\)](#)」を参照してください。

モジュール定義を追加した場合は、Prometheus server から新しく作成したモジュールを使ってスクレイプするためのスクレイプジョブの定義が必要になります。Prometheus server 側の設定については、「[1.21.2\(3\)\(c\) Blackbox exporter のスクレイプジョブを追加する \(Windows の場合\) \(オプション\)](#)」を参照してください。

(c) 監視対象を追加・変更・削除する (Windows の場合) (必須)

Blackbox exporter の監視対象を、次の表に示す定義ファイルに記載します。

監視対象を追加したあとで、IM 管理ノードのツリー情報を更新する必要があります。詳細については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください。

- Blackbox exporter (HTTP/HTTPS 監視) のディスカバリ設定ファイル

項目	説明
ファイル名	<code>jpc_file_sd_config_blackbox_http.yml</code> <code>file_sd_config_blackbox_http</code> で始まるモジュール名.yml
設定対象	HTTP/HTTPS の監視対象を定義します。

項目	説明
書式	マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Blackbox exporter (HTTP/HTTPS 監視) のディスカバリ設定ファイル (jpc_file_sd_config_blackbox_http.yml)」(2. 定義ファイル) を参照してください。
更新手順	「1.21.2(1)(a) 設定ファイルを編集する (Windows の場合)」を参照してください。

- Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル

項目	説明
ファイル名	• jpc_file_sd_config_blackbox_icmp.yml • file_sd_config_blackbox_icmp で始まるモジュール名.yml
設定対象	ICMP の監視対象を定義します。
書式	マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル (jpc_file_sd_config_blackbox_icmp.yml)」(2. 定義ファイル) を参照してください。
更新手順	「1.21.2(1)(a) 設定ファイルを編集する (Windows の場合)」を参照してください。

(d) プロキシ経由で HTTP 監視をする (Windows の場合) (オプション)

Blackbox exporter 設定ファイル (jpc_blackbox_exporter.yml) に「proxy_url」を設定します。

Blackbox exporter 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Blackbox exporter 設定ファイル (jpc_blackbox_exporter.yml)」(2. 定義ファイル) を参照してください。

Blackbox exporter 設定ファイルの更新手順については、「1.21.2(1)(a) 設定ファイルを編集する (Windows の場合)」を参照してください。

なお、認証が必要なプロキシを経由する場合は、認証 ID とパスワードを設定する必要があります。認証 ID とパスワードの設定方法については、「1.21.2(6)(e) プロキシ認証の認証 ID とパスワードを設定する (Windows の場合) (オプション)」を参照してください。

Blackbox exporter が実施する DNS 解決と URL の変更をスキップする場合は、Blackbox exporter 設定ファイルの skip_resolve_phase_with_proxy に true を設定する必要があります。

skip_resolve_phase_with_proxy の設定が必要な場合の例と詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Blackbox exporter 設定ファイル (jpc_blackbox_exporter.yml)」(2. 定義ファイル) を参照してください。

(e) プロキシ認証の認証 ID とパスワードを設定する (Windows の場合) (オプション)

HTTP/HTTPS 監視を行う際に、Blackbox exporter と監視対象の Web サーバの間に Basic 認証が必要なプロキシサーバが存在する場合、認証 ID とパスワードを設定する必要があります。

認証 ID は、Blackbox exporter 設定ファイル (jpc_blackbox_exporter.yml) の「modules. モジュール名.http.proxy_user」に指定します。Blackbox exporter 設定ファイルの設定方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

パスワードは、次の手段で設定します。詳細については、それぞれの説明箇所を参照してください。

- シークレット管理コマンド
- 統合オペレーション・ビューアーの「シークレット一覧」ダイアログ
- 統合オペレーション・ビューアーのシークレット管理の REST API

(f) 監視対象の Web サーバにアクセスするための認証 ID、パスワード、Bearer トークンを設定する (Windows の場合) (オプション)

HTTP/HTTPS 監視を行う際に、監視対象の Web サーバにアクセスするために Basic 認証が必要な場合、認証 ID、パスワード、および Bearer トークンを設定する必要があります。

認証 ID は、Blackbox exporter 設定ファイル (jpc_blackbox_exporter.yml) の「modules. モジュール名.http.basic_auth.username」に指定します。Blackbox exporter 設定ファイルの設定方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

パスワードおよび Bearer トークンは、次の手段で設定します。詳細については、それぞれの説明箇所を参照してください。

- シークレット管理コマンド
- 統合オペレーション・ビューアーの「シークレット一覧」ダイアログ
- 統合オペレーション・ビューアーのシークレット管理の REST API

(7) Yet another cloudwatch exporter の設定

(a) ポートを変更する (Windows の場合) (オプション)

Yet another cloudwatch exporter が使用するリスンポートは、yet-another-cloudwatch-exporter コマンドの -listen-address オプションに指定します。

yet-another-cloudwatch-exporter コマンドのオプションの変更方法については、「[1.21.2\(1\)\(c\) コマンドラインオプションを変更する \(Windows の場合\)](#)」を参照してください。また、-listen-address オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユニット定義ファイル (jpc_プログラム名.service)」の「yet-another-cloudwatch-exporter コマンドのオプション」を参照してください。

なお、デフォルトのポートは「20718」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

(b) CloudWatch に接続するための設定を変更する (Windows の場合) (必須)

Yet another cloudwatch exporter から CloudWatch に接続する方式には、アクセスキーを使用する方式（以降、アクセスキー方式と呼びます）と IAM ロールを使用する方式（以降、IAM ロール方式と呼びます）があります。Yet another cloudwatch exporter を AWS/EC2 以外のホスト上にインストールする場合は、アクセスキー方式だけが使用できます。Yet another cloudwatch exporter を AWS/EC2 上にインストールする場合は、アクセスキー方式または IAM ロール方式を使用できます。

CloudWatch に接続する手順について、次に示す 4 つのパターンで説明します。

- アクセスキー方式（その 1）
AWS アカウントの IAM ユーザーで CloudWatch に接続する
- アクセスキー方式（その 2）
同じロールを設定した AWS アカウントの複数の IAM ユーザーを作成し、このロール内の IAM ユーザーで CloudWatch に接続する
- IAM ロール方式（その 1）
IAM ロールを設定した AWS アカウントで CloudWatch に接続する
- IAM ロール方式（その 2）
同じ IAM ロールを設定した複数の AWS アカウントで CloudWatch に接続する

■アクセス方式（その 1）で CloudWatch に接続する場合

1. AWS アカウント①に、IAM ポリシー「yace_policy」を作成し、次に示す JSON 形式の情報を設定する。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudWatchExporterPolicy",
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "cloudwatch:ListTagsForResource",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource": "*"
    }
  ]
}
```

2. AWS アカウント①に、IAM グループ「yace_group」を作成し、手順 1 で作成した IAM ポリシー「yace_policy」を割り当てる。
3. AWS アカウント①に、IAM ユーザー「yace_user」を作成し、手順 2 で作成した IAM グループ「yace_group」に所属させる。

- 監視モジュールのホストで、[/root/.aws/] ディレクトリに credentials ファイルを作成し、credentials ファイルの [default] セクションに、手順 3 で作成した IAM ユーザー「yace_user」のアクセスキーとシークレットアクセスキーを設定する。

■アクセス方式（その 2）で CloudWatch に接続する場合

- AWS アカウント②に、IAM ポリシー「yace_policy」を作成し、「■アクセス方式（その 1）」の手順 1 と同じ JSON 形式の情報を設定する。
- AWS アカウント②に、IAM ロール「cross_access_role」を作成し、[信頼されたエンティティの種類を選択] に「別の AWS アカウント」を選択したあと、アカウント ID に AWS アカウント①のアカウント ID を指定する。
- 手順 2 で作成した IAM ロール「cross_access_role」に、手順 1 で作成した IAM ポリシー「yace_policy」を割り当てる。
- AWS アカウント①に、IAM ポリシー「yace_policy」を作成し、「■アクセス方式（その 1）」の手順 1 と同じ JSON 形式の情報を設定する。
- AWS アカウント①に、IAM ポリシー「account2_yace_policy」を作成し、次に示す JSON 形式の情報を設定する。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::AWSアカウント②:role/cross_access_role"
    }
  ]
}
```

下線部の「cross_access_role」は、手順 2 で作成した IAM ロールの名称です。

- AWS アカウント①に、IAM グループ「yace_group」を作成し、手順 1 で作成した IAM ポリシー「yace_policy」と手順 5 で作成した IAM ポリシー「account2_yace_policy」を割り当てる。
- AWS アカウント①に、IAM ユーザー「yace_user」を作成し、手順 6 で作成した IAM グループ「yace_group」に所属させる。
- 監視モジュールのホストで、[/root/.aws/] ディレクトリに credentials ファイルを作成し、credentials ファイルの [default] セクションに、手順 7 で作成した IAM ユーザー「yace_user」のアクセスキーとシークレットアクセスキーを設定する。
- Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) に、次に示す AWS アカウント②の定義※を追加する。

```
discovery:
  exportedTagsOnMetrics:
```

```

    AWS/S3:
      - jp1_pc_nodelabel
  jobs:
  - type: AWS/S3
    regions:
      - us-east-2
    metrics:
      - name: BucketSizeBytes
        statistics:
          - Sum
        period: 300000
        length: 400000
        nilToZero: true

  - type: AWS/S3
    regions:
      - us-east-2
    roles:
      - roleArn: "arn:aws:iam::AWSアカウント②:role/cross_access_role"
    metrics:
      - name: BucketSizeBytes
        statistics:
          - Sum
        period: 300000
        length: 400000
        nilToZero: true

```

注※

1～15 行目は AWS アカウント①の収集設定, 17 行目以降は AWS アカウント②の収集設定を示します。

AWS アカウント②の収集設定には, 「roles.roleArn」を指定する必要があります。「roles.roleArn」には, AWS アカウントを 2 つまで指定できますが, 2 つ以上のアカウントを指定する場合は, 日立営業までお問い合わせください。

■IAM ロール方式 (その 1) で CloudWatch に接続する場合

1. AWS アカウント①に, IAM ポリシー「yace_policy」を作成し, 「■アクセス方式 (その 1)」の手順 1 と同じ JSON 形式の情報を設定する。
2. AWS アカウント①に, IAM ロール「yace_role」を作成し, 「信頼されたエンティティの種類を選択」には AWS サービス, 「ユースケースの選択」には EC2 を選択する。
3. 手順 2 で作成した IAM ロール「yace_role」に, 手順 1 で作成した IAM ポリシー「yace_policy」を割り当てる。
4. AWS アカウント①の監視モジュールをインストールした EC2 インスタンスに, 手順 2～3 で作成した IAM ロール「yace_role」を割り当てる。※

注※

AWS コンソールの EC 画面を開き, 「アクション」－「セキュリティ」－「IAM ロールを変更」のメニューで実施します。

■IAM ロール方式（その 2）で CloudWatch に接続する場合

1. AWS アカウント②に、IAM ポリシー「yace_policy」を作成し、「■アクセス方式（その 1）」の手順 1 と同じ JSON 形式の情報を設定する。
2. AWS アカウント②に、IAM ロール「cross_access_role」を作成し、[信頼されたエンティティの種類を選択] に「別の AWS アカウント」を選択したあと、アカウント ID に AWS アカウント①のアカウント ID を指定する。また、必要に応じて外部 ID を指定する。
3. AWS アカウント①に、IAM ポリシー「account2_yace_policy」を作成し、次に示す JSON 形式の情報を設定する。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::AWSアカウント②:role/cross_access_role"
    }
  ]
}
```

下線部の「cross_access_role」は、手順 2 で作成した IAM ロールの名称です。

4. AWS アカウント①に、IAM ロール「yace_role」を作成し、[信頼されたエンティティの種類を選択] には AWS サービス、[ユースケースの選択] には EC2 を選択する。
5. 手順 4 で作成した IAM ロール「yace_role」に、手順 3 で作成した IAM ポリシー「account2_yace_policy」を割り当てる。
6. AWS アカウント①の監視モジュールをインストールした EC2 インスタンスに、手順 4 で作成した IAM ロール「yace_role」を割り当てる。※

注※

AWS コンソールの EC 画面を開き、[アクション] - [セキュリティ] - [IAM ロールを変更] のメニューで実施します。

7. Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) に、次に示す AWS アカウント②の定義※を追加する。

```
discovery:
  exportedTagsOnMetrics:
    AWS/S3:
      - jp1_pc_nodelabel
jobs:
- type: AWS/S3
  regions:
    - us-east-2
  roles:
    - roleArn: "arn:aws:iam::AWSアカウント②:role/cross_access_role"
      externalId: "外部ID"
```



```
metrics:
  - name: BucketSizeBytes
    statistics:
      - Sum
    period: 300000
    length: 400000
    nilToZero: true
```

注※

9～11 行目が AWS アカウント②の収集設定を示します。

AWS アカウント②の収集設定には、「roles.roleArn」を指定する必要があります。「roles.roleArn」には、AWS アカウントを 2 つまで指定できますが、2 つ以上のアカウントを指定する場合は、日立営業までお問い合わせください。

AWS アカウント②の収集設定の「externalId」は、手順 2 で外部 ID を指定した場合にだけ指定します。

(c) CloudWatch にプロキシ経由で接続する (Windows の場合) (オプション)

CloudWatch にプロキシ経由で接続する必要がある場合は、環境変数 HTTPS_PROXY を使用します (環境変数 HTTP_PROXY は使用できません)。

環境変数 HTTPS_PROXY に指定する値の書式を次に示します。

```
http://プロキシのユーザー名:パスワード@プロキシサーバのホスト名:ポート番号
```

❗ 重要

環境変数名の HTTPS_PROXY に対して、値の先頭が「http://」となる点に注意してください。

■ Windows の場合

1. Yet another cloudwatch exporter を停止する。
2. [設定] - [システム] - [詳細情報] - [関連設定] - [システムの詳細設定] からシステムのプロパティダイアログを表示する。
3. [環境変数] ボタンをクリックし、環境変数ダイアログを表示する。
4. システム環境変数に、次のように設定する。

変数名	変数値
HTTPS_PROXY	http://プロキシのユーザー名:パスワード@プロキシサーバのホスト名:ポート番号

5. Yet another cloudwatch exporter を起動する。

❗ 重要

- 環境変数 HTTPS_PROXY をシステム環境変数に設定するため、そのホストで稼働するすべてのプロセスに反映されます。
- システム環境変数は、ログイン可能なユーザーであれば内容を表示できてしまう点に注意が必要です。環境変数 HTTPS_PROXY にパスワードを指定して運用する場合は、ログインできるユーザーを限定するなどの対策が必要です。

■ Linux の場合

1. Yet another cloudwatch exporter を停止する。

2. 任意のファイルを作成して、次のように記載する。

```
HTTPS_PROXY=http://プロキシのユーザー名:パスワード@プロキシサーバのホスト名:ポート番号
```

記載する内容の詳細については、man systemd.exec を実行して、「EnvironmentFile=」に設定されている値を確認してください。

3. ユニット定義ファイルに EnvironmentFile を追加し、手順 2 で作成したファイルのパスを記載する。

```
:  
[Service]  
EnvironmentFile = "手順2で作成したファイルのパス"  
WorkingDirectory = ....  
ExecStart = ....  
:
```

4. systemd を更新する。

次のコマンドを実行します。

```
systemctl daemon-reload
```

5. Yet another cloudwatch exporter を起動する。

(d) 監視する AWS サービスを追加する（オプション）

デフォルトで監視対象となっている AWS サービスは、次の通りです。それ以外の AWS サービスを監視する場合、ここでの手順を実施してください。

- AWS/EC2
- AWS/Lambda
- AWS/S3
- AWS/DynamoDB
- AWS/States
- AWS/SQS

- AWS/EBS
- AWS/ECS
- AWS/EFS
- AWS/FSx
- AWS/RDS
- AWS/SNS
- ECS/ContainerInsights

1. Yet another cloudwatch exporter 設定ファイルに AWS サービスの定義を追加する。

編集方法については、「[1.21.2\(1\)\(a\)設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

下記の下線部の個所に AWS サービスの定義を追加します。

- discovery.exportedTagsOnMetrics

■記載内容

```
discovery:
  exportedTagsOnMetrics:
    AWSサービス名:
    - jp1_pc_nodelabel
```

■設定例

```
discovery:
  exportedTagsOnMetrics:
    AWS/EC2:
      - jp1_pc_nodelabel
```

- discovery.jobs

■記載内容

```
discovery:
  :
  jobs:
    - type: AWSサービス名
      regions:
        - AWSリージョン
      period: 0
      length: 600
      delay: 120
      metrics:
```

■設定例

```
discovery:
  :
  jobs:
    - type: AWS/EC2
      regions:
        - ap-northeast-1
      period: 0
```

```
length: 600
delay: 120
metrics:
```

2. 収集するメトリックを追加する。

「[1.21.2\(7\)\(f\) 収集するメトリックを変更する（オプション）](#)」を参照してください。

(e) AWS リソースを監視対象にする（必須）

AWS リソースを Yet another cloudwatch exporter で監視するためには、監視対象としたい AWS リソースに、`jp1_pc_nodelabel` タグを設定する必要があります。AWS リソースに対するタグの設定方法については、AWS のドキュメントを参照してください。

`jp1_pc_nodelabel` タグには、次の値を設定します。1～255 文字の範囲で、英数字またはハイフンで指定してください。

- EC2 の場合
ホスト名を指定します。
- EC2 以外の場合
IM 管理ノードのラベルに表示する文字列を指定します。

❗ 重要

- AWS のサービス内でユニークな文字列を設定します。EC2 と Lambda など、別のサービスであれば同一の文字列でも設定できます。
- Yet another cloudwatch exporter の監視先が異なるアカウントは異なる文字列にしてください。異なるリージョンであっても、同一のサービスであれば異なる文字列としてください。
- 文字列が重複した場合、IM 管理ノードが 1 つしか作成されません。

`jp1_pc_nodelabel` タグに設定した値は、Yet another cloudwatch exporter が収集するサンプルの、`jp1_pc_nodelabel` ラベルの値として追加されます。

(f) 収集するメトリックを変更する（オプション）

1. CloudWatch で収集されているメトリックを確認する。

収集したいメトリックが CloudWatch で収集されていることを確認します。

また、以降の手順での設定に備えて、CloudWatch メトリック名、CloudWatch 統計タイプの設定を確認しておく必要があります。

CloudWatch メトリック名および CloudWatch 統計タイプについては、AWS のドキュメントの「[Amazon CloudWatch User Guide](#)」を参照してください。

2. Yet another cloudwatch exporter 設定ファイルに CloudWatch メトリックの定義を追加する。

下記の discovery.jobs.metrics の下線部の個所に、CloudWatch メトリックの定義を記載します。

```
discovery:
  :
  jobs:
  - type: AWSサービス名
    regions:
    - AWSリージョン
    period: 0
    length: 600
    delay: 120
    metrics:
      - name: CloudWatchメトリック名1※1
        statistics:
        - CloudWatch統計タイプ※2
      - name: CloudWatchメトリック名2※3
        statistics:
        - CloudWatch統計タイプ※4
      - name: CloudWatchメトリック名3※5
        statistics:
        - CloudWatch統計タイプ※6
      :
```

注※1 CloudWatch メトリック名 1 の例：CPUUtilization

注※2 CloudWatch 統計タイプの例：Average

注※3 CloudWatch メトリック名 2 の例：DiskReadBytes

注※4 CloudWatch 統計タイプの例：Sum

注※5 CloudWatch メトリック名 3 の例：DiskWriteBytes

注※6 CloudWatch 統計タイプの例：Sum

3. Prometheus 設定ファイルにメトリックを追加する。

metric_relabel_configs の値に、収集するメトリックが「|」で区切って記載されています。収集が必要なメトリックを追加します。また、収集が不要なメトリックを削除します。メトリック名の名称規則については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の、「3.15.1(1)(g) Yet another cloudwatch exporter (Amazon CloudWatch 性能情報収集機能)」の「■Exporter のメトリックの名称規則」の説明を参照してください。

Prometheus 設定ファイルの編集方法については、「[1.21.2\(1\)\(a\)設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

<設定例>

```
- job_name: 'jpc_cloudwatch'
  :
  metric_relabel_configs:
  - regex: 'tag_(jp1_pc_*)'
    replacement: ${1}
    action: labelmap
  - regex: 'tag_(jp1_pc_*)'
    action: 'labeldrop'
  - source_labels: ['__name__', 'jp1_pc_nodelabel']
    regex: '(aws_ec2_cpuutilization_average|aws_ec2_disk_read_bytes_sum|aws_ec2_disk_
```

```
write_bytes_sum|aws_lambda_errors_sum|aws_lambda_duration_average|aws_s3_bucket_size_byte
s_sum|aws_s3_5xx_errors_sum|aws_dynamodb_consumed_read_capacity_units_sum|aws_dynamodb_co
nsumed_write_capacity_units_sum|aws_states_execution_time_average|aws_states_executions_fa
iled_sum|aws_sqs_approximate_number_of_messages_delayed_sum|aws_sqs_number_of_messages_d
eleted_sum【ここに追加するメトリックを「|」で区切って記載します】);.+${
    action: 'keep'
```

4. 必要に応じて、メトリック定義ファイルにトレンド表示の定義を行う。

記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Yet another cloudwatch exporter のメトリック定義ファイル (metrics_ya_cloudwatch_exporter.conf)」(2. 定義ファイル) を参照してください。

(8) Promitor の設定

Promitor で監視を行う場合は、次の設定を行います。

(a) Azure に接続するための設定 (必須)

■サービス定義ファイル (Windows の場合) またはユニット定義ファイル (Linux の場合) の変更

Promitor の設定ファイルの格納先は、環境変数 PROMITOR_CONFIG_FOLDER に絶対パスで指定します。この環境変数はサービス定義ファイル (Windows の場合) またはユニット定義ファイル (Linux の場合) に定義されているため、該当箇所を変更します。サービス定義ファイル (Windows の場合) およびユニット定義ファイル (Linux の場合) については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「2. 定義ファイル」の、該当するファイルを説明している箇所を参照してください。

■Promitor Scraper runtime 設定ファイル (runtime.yaml) の変更

Promitor Scraper の runtime 設定ファイル (runtime.yaml) では、Promitor Scraper の設定ファイル (metrics-declaration.yaml) のパスを metricsConfiguration.absolutePath に指定します。Promitor Scraper の runtime 設定ファイル (runtime.yaml) については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「2. 定義ファイル」の、該当するファイルを説明している箇所を参照してください。

■Azure への接続情報の設定

Promitor から Azure に接続するための認証情報を設定します。設定方法については、「[1.21.2\(8\)\(b\) Azure に接続するための認証情報の設定](#)」を参照してください。

(b) Azure に接続するための認証情報の設定

Promitor から Azure に接続する方式には、サービスプリンシパル方式とマネージド ID 方式があります。Promitor を Azure VirtualMachine 以外のホスト上にインストールする場合は、サービスプリンシパル方式だけが使用できます。Promitor を Azure VirtualMachine 上にインストールする場合は、サービスプリンシパル方式またはマネージド ID 方式が使用できます。

Azure に接続する手順について、次に示す 3 つのパターンで説明します。

- サービスプリンシパル方式

クライアントシークレットを使用して、Azure に接続する

- マネージド ID 方式（システム割り当て）
システム割り当てマネージド ID を使用して、Azure に接続する
- マネージド ID 方式（ユーザー割り当て）
ユーザー割り当てマネージド ID を使用して、Azure に接続する

■サービスプリンシパル方式で Azure に接続する場合

Azure Portal で手順 1～3、Promitor がインストールされたホストで手順 4～6 を実施します。

1. アプリケーションを作成し、クライアントシークレットを発行する。
2. アプリケーションの [概要] からアプリケーション（クライアント）ID を取得する。
3. 監視対象のリソースグループ（またはサブスクリプション）を選択し、[アクセス制御(IAM)] – [ロールの割り当ての追加] を実行し、「監視閲覧者」を指定する。
4. 手順 1 で取得したクライアントシークレットの「値」を、JP1/IM - Agent に登録する。
シークレットを登録するためのキーには、次に示す値を指定します。

シークレットを登録するためのキー	指定する値
Promitor Resource Discovery のキー	Promitor.resource_discovery.env.AUTH_APPKEY
Promitor Scraper のキー	Promitor.scrapper.env.AUTH_APPKEY

シークレットの登録方法については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の JP1/IM - Agent の「3.15.10(2)シークレットの追加・変更・削除」の説明を参照してください。

❗ 重要

コンテナ環境で構築する場合、コンテナイメージの作成前にこの手順を実施できません。コンテナの作成後に実施してください。

5. Promitor Scraper runtime 設定ファイル (runtime.yaml) と Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) で、authentication.mode にServicePrincipal を指定します。
6. Promitor Scraper 設定ファイル (metrics-declaration.yaml) と Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) に、接続先の Azure の情報を指定する。
 - Promitor Scraper 設定ファイル (metrics-declaration.yaml)
azureMetadata に接続先の Azure の情報を指定します。
 - Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml)
azureLandScape に接続先の Azure の情報を指定します。

■マネージド ID 方式（システム割り当て）で Azure に接続する場合

1. インストールとセットアップ (Windows の場合)

Azure Portal で手順 1～3, Promitor がインストールされたホストで手順 4～6 を実施します。

1. [Virtual Machines] で, Promitor がインストールされている Azure VirtualMachine を選択する。
2. [ID] – [システム割り当て済み] で [状態] を「オン」に変更する。
3. [ID] – [システム割り当て済み] の [アクセス許可] で「Azure ロールの割り当て」を選択し, 「監視閲覧者」を指定する。
4. Promitor Scraper runtime 設定ファイル (runtime.yaml) と Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) で, authentication.mode にSystemAssignedManagedIdentity を指定する。
5. Promitor Scraper 設定ファイル (metrics-declaration.yaml) と Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) に, 接続先の Azure の情報を指定する。
 - Promitor Scraper 設定ファイル (metrics-declaration.yaml)
azureMetadata に接続先の Azure の情報を指定します。
 - Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml)
azureLandScape に接続先の Azure の情報を指定します。

■マネージド ID 方式 (ユーザー割り当て) で Azure に接続する場合

Azure Portal で手順 1～5, Promitor がインストールされたホストで手順 6～7 を実施します。

1. サービス検索で, [マネージド ID] – [マネージド ID の作成] を選択する。
2. リソースグループ, 名前などを指定して, マネージド ID を作成する。
3. [Azure ロールの割り当て] で「監視閲覧者」を割り当てる。
4. [Virtual Machines] で, Promitor がインストールされている Azure VirtualMachine を選択する。
5. [ID] – [ユーザー割り当て済み] – [追加] を選択し, 手順 2 で作成したマネージド ID を追加する。
6. Promitor Scraper runtime 設定ファイル (runtime.yaml) と Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) で, authentication.mode にUserAssignedManagedIdentity を指定します。
7. Promitor Scraper 設定ファイル (metrics-declaration.yaml) と Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) に, 接続先の Azure の情報を指定する。
 - Promitor Scraper 設定ファイル (metrics-declaration.yaml)
azureMetadata に接続先の Azure の情報を指定します。
 - Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml)
azureLandScape に接続先の Azure の情報を指定します。

(c) Azure にプロキシ経由で接続する設定 (オプション)

Azure にプロキシ経由で接続する必要がある場合は、環境変数 `HTTPS_PROXY` と `NO_PROXY` を使用します。設定方法の詳細については、「[2.19 JP1/IM - Agent のセットアップ \(UNIX の場合\)](#)」の「[2.19.2\(8\)\(c\)CloudWatch にプロキシ経由で接続する \(Linux の場合\) \(オプション\)](#)」を参照してください。`NO_PROXY` には、Promitor Scraper runtime 設定ファイル (`runtime.yaml`) の `resourceDiscovery.host` の値を指定してください。

(d) 取得対象の設定 (必須)

■個別に指定が必要な監視対象の設定 (必須)

監視対象は、デフォルトでは自動検出する設定となっていますが、次に示す一部のサービスは自動検出に対応していません。これらのサービスについては、Promitor Scraper 設定ファイル (`metrics-declaration.yaml`) を編集し、監視対象を個別に指定してください。

- 監視対象を個別に指定する必要があるサービス

マニュアル「[JP1/Integrated Management 3 - Manager 導入・設計ガイド](#)」の「[3.15.1\(1\)\(h\)Promitor \(Azure Monitor 性能情報収集機能\)](#)」の Promitor が監視対象としてサポートするサービスについて説明している表で、オートディスカバリの対象外となっているサービスが該当します。

- 監視対象を個別に指定する方法

Promitor Scraper 設定ファイル (`metrics-declaration.yaml`) のコメントアウトを解除し、`resources` セクションで監視対象を指定します。

■監視対象の変更 (オプション)

Promitor で監視対象を指定する方法には、次に示す 2 種類の方法があります。

- 監視対象を個別に指定する方法

監視する Azure リソースを個別に指定する場合は、Promitor Scraper 設定ファイル (`metrics-declaration.yaml`) に指定します。

- 監視対象を自動検出する方法

テナント内のリソースを自動的に検出し、Azure リソースを監視する場合は、Promitor Scraper 設定ファイル (`metrics-declaration.yaml`) および Promitor Resource Discovery 設定ファイル (`resource-discovery-declaration.yaml`) に指定します。

■監視メトリクスの変更 (オプション)

取得するメトリクスや表示するメトリクスを変更する場合は、次の設定を行います。

1. Azure Monitor で収集されていることを確認する。

収集したいメトリックが Azure Monitor で収集されていることを確認します。

次の手順での設定に備えて、メトリック名、統計タイプを確認しておきます。

メトリック名については、Azure Monitor Documentation の [Reference - Supported metrics - Resource metrics](#) の [Metric](#) を参照してください。統計タイプについては、Azure Monitor Documentation の [Reference - Supported metrics - Resource metrics](#) の [Aggregation Type](#) を参照してください。

2. Prometheus 設定ファイル (jpc_prometheus_server.yml) の設定内容を変更する。

収集対象のメトリクスを変更する場合は、Prometheus 設定ファイル (jpc_prometheus_server.yml) の metric_relabel_configs の設定を変更します。

Prometheus 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」(2. 定義ファイル) の JP1/IM - Agent の「Prometheus 設定ファイル (jpc_prometheus_server.yml)」を参照してください。

3. Promitor のメトリック定義ファイル (metrics_promitor.conf) の設定内容を変更する。

統合オペレーション・ビューアーの「トレンド」タブに表示するメトリックを変更する場合は、Promitor のメトリック定義ファイル (metrics_promitor.conf) の設定を変更します。

Promitor のメトリック定義ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Promitor のメトリック定義ファイル (metrics_promitor.conf)」(2. 定義ファイル) を参照してください。

(e) テナント情報の表示文字列の設定 (オプション)

プロパティ表示文字列定義ファイル (property_labels.conf) に、監視対象のテナント ID とサブスクリプション ID の表示文字列を設定します。この設定を行わない場合、IM 管理ノードのプロパティや JP1 イベントの拡張属性には、テナントとサブスクリプションは「default」と表示されます。

プロパティ表示文字列定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「プロパティ表示文字列定義ファイル (property_labels.conf)」(2. 定義ファイル) を参照してください。

(f) システムノード定義ファイル (imdd_systemnode.conf) の設定 (必須)

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.6(1)(i)ツリーの形式」に示すシステムノードを作成するときは、システムノード定義ファイル (imdd_systemnode.conf) を編集して、次の設定項目を指定します。ここに記載のない設定項目については、任意の値を指定します。

表 1-16 システムノード定義ファイル (imdd_systemnode.conf) の設定項目

設定項目	設定値
displayname	Azure Monitor のメトリクスを発行するサービスの名前を指定します。
type	次の文字列を大文字表記で指定します。 Azure-Azure サービス名 「Azure サービス名」は、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(1)(h)Promitor (Azure Monitor 性能情報収集機能)」で、Promitor が監視対象としてサポートするサービスについて説明している個所の「Promitor の resourceType 名」が該当します。
name	次の文字列を指定します。 [{"*":"regex"}]

Promitor のメトリック定義ファイル (metrics_promitor.conf) の初期設定で監視する Azure サービスに対して、システム管理ノードを設定する場合の、システムノード定義ファイルの設定例を、次に示します。

表 1-17 システムノード定義ファイル (imdd_systemnode.conf) の設定例

設定項目		
displayName	type	name
Azure Function App	JP1PC-AZURE-FUNCTIONAPP	[{"*":"regex"}]
Azure Container Instances	JP1PC-AZURE-CONTAINERINSTANCE	[{"*":"regex"}]
Azure Kubernetes Service	JP1PC-AZURE-KUBERNETESSERVICE	[{"*":"regex"}]
Azure File Storage	JP1PC-AZURE-FILESTORAGE	[{"*":"regex"}]
Azure Blob Storage	JP1PC-AZURE-BLOBSTORAGE	[{"*":"regex"}]
Azure Service Bus Namespace	JP1PC-AZURE-SERVICEBUSNAMESPACE	[{"*":"regex"}]
Azure Cosmos DB	JP1PC-AZURE-COSMOSDB	[{"*":"regex"}]
Azure SQL Database	JP1PC-AZURE-SQLDATABASE	[{"*":"regex"}]
Azure SQL Server	JP1PC-AZURE-SQLSERVER	[{"*":"regex"}]
Azure SQL Managed Instance	JP1PC-AZURE-SQLMANAGEDINSTANCE	[{"*":"regex"}]
Azure SQL Elastic Pool	JP1PC-AZURE-SQLELASTICPOOL	[{"*":"regex"}]
Azure Logic Apps	JP1PC-AZURE-LOGICAPP	[{"*":"regex"}]

上記の内容をシステムノード定義ファイルに設定した場合、次のようになります。

```
{
  "meta":{
    "version":"2"
  },
  "allSystem":[
    {
      "id":"functionApp",
      "displayName":"Azure Function App",
      "objectRoot":[
        {
          "type":"JP1PC-AZURE-FUNCTIONAPP",
          "name":["*":"regex"]
        }
      ]
    },
    {
      "id":"containerInstance",
      "displayName":"Azure Container Instances",
      "objectRoot":[
        {
          "type":"JP1PC-AZURE-CONTAINERINSTANCE",
          "name":["*":"regex"]
        }
      ]
    },
    {
      "id":"kubernetesService",
```

```

    "displayName": "Azure Kubernetes Service",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-KUBERNETESSERVICE",
        "name": [{".*": "regex"}]
      }
    ]
  },
  {
    "id": "fileStorage",
    "displayName": "Azure File Storage",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-FILESTORAGE",
        "name": [{".*": "regex"}]
      }
    ]
  },
  {
    "id": "blobStorage",
    "displayName": "Azure Blob Storage",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-BLOBSTORAGE",
        "name": [{".*": "regex"}]
      }
    ]
  },
  {
    "id": "serviceBusNamespace",
    "displayName": "Azure Service Bus Namespace",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-SERVICEBUSNAMESPACE",
        "name": [{".*": "regex"}]
      }
    ]
  },
  {
    "id": "cosmosDb",
    "displayName": "Azure Cosmos DB",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-COSMOSDB",
        "name": [{".*": "regex"}]
      }
    ]
  },
  {
    "id": "sqlDatabase",
    "displayName": "Azure SQL Database",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-SQLDATABASE",
        "name": [{".*": "regex"}]
      }
    ]
  }
],

```

```

{
  "id": "sqlServer",
  "displayName": "Azure SQL Server",
  "objectRoot": [
    {
      "type": "JP1PC-AZURE-SQLSERVER",
      "name": [ { ".*" : "regex" } ]
    }
  ]
},
{
  "id": "sqlManagedInstance",
  "displayName": "Azure SQL Managed Instance",
  "objectRoot": [
    {
      "type": "JP1PC-AZURE-SQLMANAGEDINSTANCE",
      "name": [ { ".*" : "regex" } ]
    }
  ]
},
{
  "id": "sqlElasticPool",
  "displayName": "Azure SQL Elastic Pool",
  "objectRoot": [
    {
      "type": "JP1PC-AZURE-SQLELASTICPOOL",
      "name": [ { ".*" : "regex" } ]
    }
  ]
},
{
  "id": "logicApp",
  "displayName": "Azure Logic Apps",
  "objectRoot": [
    {
      "type": "JP1PC-AZURE-LOGICAPP",
      "name": [ { ".*" : "regex" } ]
    }
  ]
}
]
}

```

システムノード定義ファイルを設定しておくことで、jddcreatetree コマンドが実行されて、VirtualMachine 以外の PromitorSID が作成されたときに、Azure サービス名に応じたシステムノードの配下に IM 管理ノードが表示されます。VirtualMachine の PromitorSID については、システムノード定義ファイルに記載不要で、ホストを表すノードの配下に IM 管理ノードが表示されます。

システムノード定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」(2. 定義ファイル) の JP1/IM - Manager の「システムノード定義ファイル (imdd_systemnode.conf)」を参照してください。

(g) ポートを変更する (オプション)

■ Promitor Scraper が使用するスクレイプのポート番号の指定

Promitor Scraper が使用するリッスンポートは、Promitor Scraper runtime 設定ファイル (runtime.yml) に指定します。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

なお、デフォルトのポートは「20719」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

注意事項

コマンドラインオプションではなく、Promitor Scraper runtime 設定ファイル (runtime.yml) で変更します。この設定ファイルを変更した場合、Promitor のディスカバリ設定ファイル (jpc_file_sd_config_promitor.yml) も変更する必要があります。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Promitor Scraper runtime 設定ファイル (runtime.yml)」(2. 定義ファイル) を参照してください。

■ Promitor Resource Discovery が使用するスクレイプのポート番号の指定

Promitor Resource Discovery が使用するリッスンポートは、Promitor Resource Discovery runtime 設定ファイル (runtime.yml) に指定します。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

なお、デフォルトのポートは「20720」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

注意事項

コマンドラインオプションではなく、Promitor Resource Discovery runtime 設定ファイル (runtime.yml) で変更します。この設定ファイルを変更した場合、Promitor Scraper runtime 設定ファイル (runtime.yml) も変更する必要があります。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Promitor Resource Discovery runtime 設定ファイル (runtime.yml)」(2. 定義ファイル) を参照してください。

(9) Fluentd の設定

(a) ログ監視の共通定義の設定を変更する (Windows の場合) (オプション)

次の設定を変更する場合は、ログ監視共通定義ファイルの設定を変更します。

- 統合エージェントの制御基盤のポート番号
- buffer プラグインの設定

ログ監視共通定義ファイルについての詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ログ監視共通定義ファイル (jpc_fluentd_common.conf)」(2. 定義ファイル) を参照してください。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

(b) テキスト形式のログファイルを監視する (Windows の場合) (必須)

テキスト形式のログファイルを新たに監視する場合、次の手順を実施します。

1. テキスト形式のログファイルの監視定義ファイルを作成する。

次に示すコピー元のテンプレートをコピーし、コピー先の定義ファイルにリネームすることで、テキスト形式のログファイルの監視定義ファイルを作成します。

コピー元: Agent パス¥conf¥fluentd_@@trapname@@_tail.conf.template

コピー先: Agent パス¥conf¥user¥fluentd_ログ監視名_tail.conf

テンプレート (fluentd_@@trapname@@_tail.conf.template) をコピーして、テキスト形式のログファイルの監視定義ファイルを作成します。コピー先のファイル名は「fluentd_ログ監視名_tail.conf」に変更します。

テキスト形式のログファイルの監視定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「テキスト形式のログファイルの監視定義ファイル (fluentd_@@trapname@@_tail.conf.template)」(2. 定義ファイル) を参照してください。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

2. ログ監視対象定義ファイル (jpc_fluentd_common_list.conf) を編集する。

一時的に一部の監視定義ファイルのログ監視を止める運用を行いたい場合、ログ監視対象定義ファイルに、監視定義ファイルのファイル名を列挙して定義します。

ログ監視対象定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ログ監視対象定義ファイル (jpc_fluentd_common_list.conf)」(2. 定義ファイル) を参照してください。ログ監視対象定義ファイルを編集する運用を行っていない場合は編集不要です。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

3. 統合オペレーション・ビューアーのツリーに反映する。

反映方法については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください。

メモ

監視定義ファイルのログ監視名を変更した場合などで、テキスト形式のログファイルの監視設定を変更するときは、上記の手順 2 と 3 を実施してください。

(c) テキスト形式のログファイルの監視設定を変更する (Windows の場合) (オプション)

テキスト形式のログファイルの監視設定を変更する場合、次の手順を実施します。

1. テキスト形式のログファイルの監視定義ファイルを変更する。

作成済みの監視定義ファイル (fluentd_ログ監視名_tail.conf) を変更します。

テキスト形式のログファイルの監視定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「テキスト形式のログファイルの監視定義ファイル (fluentd_@@trapname@@_tail.conf.template)」(2. 定義ファイル) を参照してください。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

2. ログ監視対象定義ファイル (jpc_fluentd_common_list.conf) を編集する。

次の場合、ログ監視対象定義ファイルに、監視定義ファイルのファイル名を列挙して定義します。

- 監視定義ファイルのログ監視名を変更した場合
- 一時的に一部の監視定義ファイルのログ監視を止める運用を行うユーザーの場合

ログ監視対象定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ログ監視対象定義ファイル (jpc_fluentd_common_list.conf)」(2. 定義ファイル) を参照してください。ログ監視対象定義ファイルを編集する運用を行っていない場合は編集不要です。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

3. 統合オペレーション・ビューアーのツリーに反映します。

[Metric Settings] セクションの値を変更した場合、変更内容を統合オペレーション・ビューアーのツリーに反映します。反映方法については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください。

(d) テキスト形式のログファイルの監視設定を削除する (Windows の場合) (オプション)

テキスト形式のログファイルの監視設定を削除する場合、次の手順を実施します。

1. テキスト形式のログファイルの監視定義ファイルを削除する。

作成済みの監視定義ファイル (fluentd_ログ監視名_tail.conf) を削除します。

設定ファイルの削除方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

2. ログ監視対象定義ファイル (jpc_fluentd_common_list.conf) を編集する。

一時的に一部の監視定義ファイルのログ監視を止める運用を行う場合、ログ監視対象定義ファイルに定義されている監視定義ファイルのファイル名を削除します。

3. 統合オペレーション・ビューアーのツリーに反映する。

反映方法については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください。

(e) Windows イベントログを監視する (必須)

Windows イベントログを新たに監視する場合、次の手順を実施します。

1. Windows イベントログの監視定義ファイルを作成する。

次に示すコピー元のテンプレートをコピーし、コピー先の定義ファイルにリネームすることで、Windows イベントログの監視定義ファイルを作成します。

コピー元：Agent パス¥conf¥fluentd_@@trapname@@_wevt.conf.template

コピー先：Agent パス¥conf¥user¥fluentd_ログ監視名_wevt.conf

テンプレート (fluentd_@@trapname@@_wevt.conf.template) をコピーして、Windows イベントログの監視定義ファイルを作成します。コピー先のファイル名は「fluentd_ログ監視名_wevt.conf」に変更します。

Windows イベントログの監視定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Windows イベントログの監視定義ファイル (fluentd_@@trapname@@_wevt.conf.template)」(2. 定義ファイル) を参照してください。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

2. Windows イベントログの監視定義ファイルを編集する。

一時的に一部の監視定義ファイルのログ監視を止める運用を行いたい場合、Windows イベントログの監視定義ファイルに、監視定義ファイルのファイル名を列挙して定義します。

ログ監視対象定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ログ監視対象定義ファイル (jpc_fluentd_common_list.conf)」(2. 定義ファイル) を参照してください。ログ監視対象定義ファイルを編集する運用を行っていない場合は編集不要です。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

3. 統合オペレーション・ビューアーのツリーに反映する。

反映方法については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください。

メモ

監視定義ファイルのログ監視名を変更した場合などで、テキスト形式のログファイルの監視設定を変更するときは、上記の手順 2 と 3 を実施してください。

(f) Windows イベントログの監視設定を変更する（オプション）

Windows イベントログの監視設定を変更する場合、次の手順を実施します。

1. Windows イベントログの監視定義ファイルを変更する。

作成済みの監視定義ファイル（`fluentd_ログ監視名_wevt.conf`）を変更します。

Windows イベントログの監視定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Windows イベントログの監視定義ファイル（`fluentd_@@trapname@@_wevt.conf.template`）」（2. 定義ファイル）を参照してください。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する（Windows の場合）](#)」を参照してください。

2. ログ監視対象定義ファイル（`jpc_fluentd_common_list.conf`）を編集する。

次の場合、ログ監視対象定義ファイルに、監視定義ファイルのファイル名を列挙して定義します。

- 監視定義ファイルのログ監視名を変更した場合
- 一時的に一部の監視定義ファイルのログ監視を止める運用を行うユーザーの場合

ログ監視対象定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ログ監視対象定義ファイル（`jpc_fluentd_common_list.conf`）」（2. 定義ファイル）を参照してください。ログ監視対象定義ファイルを編集する運用を行っていない場合は編集不要です。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する（Windows の場合）](#)」を参照してください。

3. 統合オペレーション・ビューアーのツリーに反映する。

[Metric Settings] セクションの値を変更した場合、変更内容を統合オペレーション・ビューアーのツリーに反映します。反映方法については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映（Windows の場合）（必須）](#)」を参照してください。

(g) Windows イベントログの監視設定を削除する（オプション）

Windows イベントログの監視設定を削除する場合、次の手順を実施します。

1. Windows イベントログの監視定義ファイルを削除する。

作成済みの監視定義ファイル（`fluentd_ログ監視名_wevt.conf`）を削除します。

Windows イベントログの監視定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Windows イベントロ

グの監視定義ファイル (fluentd_@@trapname@@_wevt.conf.template)」(2. 定義ファイル) を参照してください。

設定ファイルの削除方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

2. ログ監視対象定義ファイル (jpc_fluentd_common_list.conf) を編集する。

一時的に一部の監視定義ファイルのログ監視を止める運用を行う場合、ログ監視対象定義ファイルに定義されている監視定義ファイルのファイル名を削除します。

3. 統合オペレーション・ビューアーのツリーに反映する。

反映方法については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください。

(h) ログメトリクス定義の設定 (必須)

ログメトリクス機能を使用する場合、アドオンプログラムの有効化手順で JP1/IM - Agent の Fluentd の設定を実施したあと、次の設定を行います。

■ ログメトリクス定義ファイルの編集 (ログメトリクスの定義)

ログメトリクス定義ファイル (fluentd_任意の名前_logmetrics.conf) を作成し、インプットプラグイン機能とアウトプットプラグイン機能の定義を行います。

また、監視対象のログメトリクスは、ログメトリクス定義ファイルのアウトプットプラグイン機能定義で指定します。

- 監視対象のログメトリクスを追加する場合
既存の<metric>の定義に並列して、新たな<metric>の定義を追加します。
- 監視対象のログメトリクスを変更する場合
該当する<metric>の定義内容を変更します。
- 監視対象のログメトリクスを削除する場合
ログメトリクス定義ファイル内の関連する定義を、すべて削除またはコメントアウトします。

ログメトリクス定義ファイルのサンプルファイルについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「[3.15.1\(1\)\(l\) Fluentd \(ログメトリクス機能\)](#)」で、該当するファイルを説明している個所を参照してください。

■ ログ監視対象定義ファイルの編集 (include の追加)

ログメトリクス定義ファイルによるログ監視を有効にするため、ログ監視対象定義ファイル (jpc_fluentd_common_list.conf) に「@include」の行を追加して、「ログメトリクス定義ファイルの編集 (ログメトリクスの定義)」で定義したログメトリクス定義ファイルを追加します。

ログ監視対象定義ファイルのサンプルファイルについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(1)(l) Fluentd (ログメトリクス機能)」で、該当するファイルを説明している個所を参照してください。

■ Fluentd の再起動

「ログメトリクス定義ファイルの編集 (ログメトリクスの定義)」および「ログ監視対象定義ファイルの編集 (include の追加)」の定義内容を反映するため、Fluentd の再起動を行います。

再起動する場合のサービスの起動と停止の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10. JP1/IM - Agent の起動と終了」を参照してください。

■ JP1/IM - Manager でのログメトリクス定義のセットアップ

ログメトリクス機能を利用して、JP1/IM - Manager の統合オペレーション・ビューアーの [トレンド] タブで、ノードのトレンド情報を表示したときに、ログメトリクスの時系列データを表示したい場合は、JP1/IM - Manager で表示するログメトリクスの定義を行います。

ここでのログメトリクス定義には、ユーザー独自のメトリック定義を利用します。

記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユーザー独自のメトリック定義ファイル (metrics_任意の Prometheus トレンド名.conf)」(2. 定義ファイル) を参照してください。

(i) ポートを変更する (オプション)

■ Fluentd が使用するスクレイプのポート番号の指定

ログメトリクス定義ファイルに、fluent-plugin-prometheus プラグインが使用するスクレイプのポート番号を指定します。

次の変更例に示す<source>内のport にリッスンポート番号^{*}を指定します。

(変更例)

```
## Input
<worker ログメトリクス機能で使用するworkerのid>
  <source>
    @type prometheus
    bind 0.0.0.0
    port リッスンポート番号
    metrics_path /metrics
  </source>
</worker>

<worker workerのid>
  <source>
    (省略)
  </source>

(以降, 省略)
```

注※

Fluentd（ログメトリクス機能）で実際に使用する Listen ポートは、ログメトリクス機能で使用する worker の worker_id（ログメトリクス定義ファイル（fluentd_任意の名前_logmetrics.conf）の「worker の id」で指定する値）に依存し、次に示す式のとおりのポート番号になります。

$24820 + \text{worker\_id}$

なお、ログメトリクス機能で 129 個の worker を利用する場合、デフォルトのポート番号は 24820 から 24948 までの連番となります。

■ Prometheus がスクレイプで使用するポート番号の変更

Prometheus のディスカバリ設定ファイルに定義したスクレイプのポート番号を、「Fluentd が使用するスクレイプのポート番号の指定」で指定したリスンポート番号+worker の id に変更します。

次の変更例に示す targets のリスンポート番号を変更します。

```
- targets:
  - 監視対象ホスト名: リスンポート番号+workerのid
  (省略)
  labels:
  (省略)
```

(j) SAP システムのログ情報を監視する（オプション）

SAP システムのシステムログ情報を新たに監視する場合、次に記載する Fluentd の設定手順と、「[1.21.2\(12\)\(d\)SAP システムのログ抽出コマンドを実行する場合の設定（オプション）](#)」に記載する Script exporter の設定手順を併せて実施します。

1. SAP システムのシステムログ情報監視定義ファイルを作成する。

サンプルファイル（fluentd_sap_syslog_tail.conf）をコピーして、テキスト形式のログファイルの監視定義ファイルを作成します。配置先については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 A.4 JP1/IM - Agent」のファイルおよびディレクトリ一覧を参照してください。コピー先のファイル名は「fluentd_ログ監視名_tail.conf」に変更します。

テキスト形式のログファイルの監視定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「テキスト形式のログファイルの監視定義ファイル（fluentd_@@trapname@@_tail.conf.template）」（2. 定義ファイル）を参照してください。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する（Windows の場合）](#)」を参照してください。

2. ログ監視対象定義ファイル（jpc_fluentd_common_list.conf）を編集する。

一時的に一部の監視定義ファイルのログ監視を止める運用を行いたい場合、ログ監視対象定義ファイルに、監視定義ファイルのファイル名を列挙して定義します。

ログ監視対象定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ログ監視対象定義ファイル

(jpc_fluentd_common_list.conf)」(2. 定義ファイル)を参照してください。ログ監視対象定義ファイルを編集する運用を行っていない場合は編集不要です。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\)設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

3. 統合オペレーション・ビューアーのツリーに反映する。

反映方法については、「[1.21.2\(19\)IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください。

(k) SAP システムのログ情報の監視設定を変更する (オプション)

SAP システムのシステムログ情報の監視設定を変更する場合の手順については、「[1.21.2\(9\)\(c\)テキスト形式のログファイルの監視設定を変更する \(Windows の場合\) \(オプション\)](#)」を参照してください。

(l) SAP システムのログ情報の監視設定を削除する (オプション)

SAP システムのシステムログ情報の監視設定を削除する場合の手順については、「[1.21.2\(9\)\(d\)テキスト形式のログファイルの監視設定を削除する \(Windows の場合\) \(オプション\)](#)」を参照してください。

(m) SAP システムの CCMS アラート情報を監視する (オプション)

SAP システムの CCMS アラート情報を新たに監視する場合、次の手順を実施します。

1. SAP システムの CCMS アラート情報監視定義ファイルを作成する。

サンプルファイル (fluentd_sap_alertlog_tail.conf) をコピーして、テキスト形式のログファイルの監視定義ファイルを作成します。配置先については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 A.4 JP1/IM - Agent」のファイルおよびディレクトリ一覧を参照してください。コピー先のファイル名は「fluentd_ログ監視名_tail.conf」に変更します。

テキスト形式のログファイルの監視定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「テキスト形式のログファイルの監視定義ファイル (fluentd_@@trapname@@_tail.conf.template)」(2. 定義ファイル)を参照してください。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

2. ログ監視対象定義ファイル (jpc_fluentd_common_list.conf) を編集する。

一時的に一部の監視定義ファイルのログ監視を止める運用を行いたい場合、ログ監視対象定義ファイルに、監視定義ファイルのファイル名を列挙して定義します。

ログ監視対象定義ファイルの記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ログ監視対象定義ファイル (jpc_fluentd_common_list.conf)」(2. 定義ファイル)を参照してください。ログ監視対象定義ファイルを編集する運用を行っていない場合は編集不要です。

設定ファイルの変更方法については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

3. 統合オペレーション・ビューアーのツリーに反映する。

反映方法については、「[1.21.2\(19\)IM 管理ノードのツリー情報の作成と反映（Windows の場合）（必須）](#)」を参照してください。

(n) SAP システムの CCMS アラート情報の監視設定を変更する（オプション）

SAP システムの CCMS アラート情報の監視設定を変更する場合の手順については、「[1.21.2\(9\)\(c\)テキスト形式のログファイルの監視設定を変更する（Windows の場合）（オプション）](#)」を参照してください。

(o) SAP システムの CCMS アラート情報の監視設定を削除する（オプション）

SAP システムの CCMS アラート情報の監視設定を削除する場合の手順については、「[1.21.2\(9\)\(d\)テキスト形式のログファイルの監視設定を削除する（Windows の場合）（オプション）](#)」を参照してください。

(10) スクレイプ定義の設定

アドオンプログラムが提供する機能をスクレイプ対象に設定する場合は、次に示すスクレイプ定義を追加します。

表 1-18 アドオンプログラムが提供する機能のスクレイプ定義

アドオンプログラムの提供機能	対応 OS	スクレイプする Exporter または対象	スクレイプ定義
Windows 性能情報収集機能	Windows	Windows exporter	設定不要です。
Linux プロセス情報収集機能	Linux	Process exporter	
AWS CloudWatch 性能情報収集機能	Windows および Linux	Yet another cloudwatch exporter	
Azure Monitor 性能情報収集機能		Promitor	
ログメトリクス機能		Fluentd	ログメトリクス機能を使用する場合、設定が必要です。 必要な設定については、「 1.21.2(10)(a)ログメトリクス機能のスクレイプ定義 」を参照してください。
UAP 監視機能		Script exporter	監視対象スクリプトの設定が必要です。 必要な設定については、「 1.21.2(10)(b)Script exporter のスクレイプ定義 」を参照してください。

(a) ログメトリクス機能のスクレイプ定義

ログメトリクス機能のスクレイプ機能では、ユーザー独自の Exporter のスクレイプ機能を利用します。

- ユーザー独自のディスカバリ設定ファイルの作成（必須）

ユーザー独自のディスカバリ設定ファイル（`user_file_sd_config_任意の名前.yml`）を作成し、監視対象を定義します。

ユーザー独自のディスカバリ設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」(2. 定義ファイル) の該当するファイルを説明している個所を参照してください。

また、ログメトリクス機能に関する記述内容については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(1)(l) Fluentd (ログメトリクス機能)」で、該当するファイルのサンプルファイルを説明している個所を参照してください。

- Prometheus 設定ファイルでの `scrape_configs` の設定（必須）

Prometheus 設定ファイル（`jpc_prometheus_server.yml`）で、`scrape_configs` の設定を追加します。Prometheus 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」(2. 定義ファイル) の該当するファイルを説明している個所を参照してください。

また、ログメトリクス機能に関する記述内容については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(1)(l) Fluentd (ログメトリクス機能)」で、該当するファイルのサンプルファイルを説明している個所を参照してください。

(b) Script exporter のスクレイプ定義

スクレイプ定義を指定する方法には、Script exporter 設定ファイル（`jpc_script_exporter.yml`）に定義したスクリプトをすべて実行する「`http_sd_config` 方式」と、Script exporter 設定ファイル（`jpc_script_exporter.yml`）に定義したスクリプトの 1 つを Prometheus 設定ファイル（`jpc_prometheus_server.yml`）の `scrape_configs` の `params` に指定する「`file_sd_config` 方式」があります。デフォルトは「`http_sd_config` 方式」です。

Script exporter 設定ファイルおよび Prometheus 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」(2. 定義ファイル) の該当するファイルを説明している個所を参照してください。

スクレイプ定義の例を、次に示します。

- `http_sd_config` 方式によるスクレイプ定義の例

```
scrape_configs:
- job_name: jpc_script_exporter
  http_sd_configs:
  - url: http://インストールホスト名:ポート/discovery
  relabel_configs:
  - source_labels: [__param_script]
    target_label: jp1_pc_script
  - target_label: jp1_pc_exporter
    replacement: JPC Script Exporter
  - target_label: jp1_pc_category
    replacement: 任意のカテゴリ名
  - target_label: jp1_pc_trendname
```

```

replacement: script_exporter
- target_label: jp1_pc_multiple_node
  replacement: jp1_pc_exporter="{job='jpc_script.*',jp1_pc_multiple_node=''}"
- target_label: jp1_pc_nodelabel
  replacement: Script metric collector(Script exporter)
- target_label: jp1_pc_agent_create_flag
  replacement: false
metric_relabel_configs:
- source_labels: [jp1_pc_script]
  target_label: jp1_pc_nodelabel
- regex: (jp1_pc_multiple_node|jp1_pc_script|jp1_pc_agent_create_flag)
  action: labeldrop

```

インストールホスト名

Script exporter をインストールしたホスト名を、1～255 文字の制御文字以外の文字で指定します。

ポート

Script exporter のポート番号を指定します。

任意のカテゴリ名

エージェント SID の IM 管理ノードのカテゴリ ID を、1～255 文字の制御文字以外の文字で指定します。

- file_sd_config 方式によるスクレイプ定義の例

```

scrape_configs:
# 設定ファイルのスクリプトを実行する例
- job_name: 任意のスクレイプジョブ名1
  file_sd_configs:
    - files:
        - 'Script Exporterのディスカバリ設定ファイルのパス'
  metrics_path: /probe
  params:
    script: [Script Exporter設定ファイルのscripts.name]
  relabel_configs:
    - source_labels: [__param_script]
      target_label: jp1_pc_script
    - target_label: jp1_pc_category
      replacement: 任意のカテゴリ名
    - target_label: jp1_pc_nodelabel
      replacement: Script metric collector(Script exporter)
  metric_relabel_configs:
    - source_labels: [jp1_pc_script]
      target_label: jp1_pc_script
    - regex: (jp1_pc_multiple_node|jp1_pc_script|jp1_pc_agent_create_flag)
      action: labeldrop
# 設定ファイルのスクリプトに、追加で引数1,2を指定し実行する例
- job_name: 任意のスクレイプジョブ名2
  file_sd_configs:
    - files:
        - 'Script Exporterのディスカバリ設定ファイルのパス'
  metrics_path: /probe
  params:
    script: [Script Exporter設定ファイルのscripts.name]
    引数名1: [引数名1の値]
    引数名2: [引数名2の値]

```

```

relabel_configs:
- source_labels: [_param_script]
  target_label: jp1_pc_nodelabel
- target_label: jp1_pc_category
  replacement: 任意のカテゴリ名
- target_label: jp1_pc_nodelabel
  replacement: Script metric collector(Script exporter)
metric_relabel_configs:
- source_labels: [jp1_pc_script]
  target_label: jp1_pc_nodelabel
- regex: (jp1_pc_multiple_node|jp1_pc_script|jp1_pc_agent_create_flag)
  action: labeldrop

```

任意のスクレイプジョブ名

同一ホストのほかのスクレイプジョブ名と重複しない任意の名前を、1～255 文字の制御文字以外の文字で指定します。

Script exporter のディスカバリ設定ファイルのパス

Script exporter のディスカバリ設定ファイル (jpc_file_sd_config_script.yml) のパスを指定します。

任意のカテゴリ名

エージェント SID の IM 管理ノードのカテゴリ ID を、1～255 文字の制御文字以外の文字で指定します。

(11) コンテナ監視の設定

監視対象によって、利用する機能とセットアップの方法が異なります。監視対象ごとの利用する機能とセットアップ方法の参照先を、次に示します。

監視対象	利用する機能	セットアップ方法の参照先
Red Hat OpenShift	ユーザー独自の Prometheus	この表以降の説明を参照してください。
Kubernetes		
Amazon Elastic Kubernetes Service (EKS)		
Azure Kubernetes Service (AKS)	Azure 監視機能 (Promitor) デフォルトで AKS の監視も有効です。	「 1.21.2(8) Promitor の設定 」の説明を参照してください。

(a) ユーザー独自の Prometheus でのスクレイプの設定 (必須)

- Red Hat OpenShift の場合

設定不要です。

インストール時に openshift-monitoring プロジェクトのインストールとスクレイピングの設定が行われます。

- Kubernetes および Amazon Kubernetes Service (EKS) の場合

Prometheus が未導入の場合、または、Prometheus が導入済みで次の表に示すスクレイプ対象が未設定の場合に、スクレイピングの設定を行います。

スクレイプ対象	取得できる情報	収集できるメトリック
kube-stat-metrics	ノード, Pod, ワークロードのステータス情報	マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の、「3.15.4(2)(a)Red Hat OpenShift」の「主な取得項目」について説明している個所を参照してください。
node_exporter	ノードの性能情報	
kubelet	Pod の性能情報	

以降の手順は、Red Hat OpenShift, Kubernetes, および Amazon Kubernetes Service (EKS) で共通となります。

(b) 接続のための設定 (必須)

ユーザー独自の Prometheus から情報を収集するための、リモートライトの設定を行います。

監視対象ごとの設定変更の方法については、「[1.21.2\(11\)\(c\) Prometheus の設定変更 \(Red Hat OpenShift\)](#)」および「[1.21.2\(11\)\(d\) Prometheus の設定変更 \(Amazon Elastic Kubernetes Service \(EKS\)\)](#)」を参照してください。

■global.external_labels セクション

- `jp1_pc_prome_hostname` (必須)
Prometheus のホスト名を指定します。
- `jp1_pc_prome_clustername` (オプション)
クラスタ名を指定します。
このラベルを指定しない場合、クラスタの IM 管理ノードは作成されません。

(指定例)

```
global:
external_labels:
  jp1_pc_prome_hostname: promHost
  jp1_pc_prome_clustername: myCluster
```

■remote_write セクション

- 接続先の設定
リモートライト先として、JP1/IM - Manager (インテリジェント統合管理基盤) のエンドポイントを指定します。エンドポイントを 2 つ指定し、「コンテナ監視に必要なラベルの設定」の 1.と 2.をそれぞれのセクションに記載します。クラスタのノードを作成する場合は、エンドポイントをもう 1 つ指定し、3.を記載してください。
- コンテナ監視に必要なラベルの設定
コンテナ監視に必要なラベルを付与するため、次に示す内容を `write_relabel_configs` セクションに記述します。リモートライト時にリラベルされるため、ユーザー独自の Prometheus のローカルストレージには影響しません。

Red Hat OpenShift を監視する場合は、「1. 基本の設定」「2. Pod のノードを作成するための設定」の先頭に、次の内容を追加で設定してください。

```
- source_labels: ['__name__']
  regex: 'kube_.*'
  target_label: instance
  replacement: クラスタ内で一意となる任意の値※
```

注※ ここで指定した値は、Kubernetes state metric collector (Kube state metrics) が稼働するホストとしてツリーに表示されます。

1. 基本の設定

```
- source_labels: ['__name__']
  regex: 'kube_job_status_failed|kube_job_owner|kube_pod_status_phase|kube_daemonset_status_desired_number_scheduled|kube_daemonset_status_current_number_scheduled|kube_deployment_spec_replicas|kube_deployment_status_replicas_available|kube_replicaset_spec_replicas|kube_replicaset_status_ready_replicas|kube_replicaset_owner|kube_statefulset_replicas|kube_statefulset_status_replicas_ready|kube_node_status_condition|container_cpu_usage_seconds_total|container_fs_reads_bytes_total|container_fs_writes_bytes_total|container_memory_working_set_bytes|container_spec_memory_limit_bytes|node_boot_time_seconds|node_context_switches_total|node_cpu_seconds_total|node_disk_io_now|node_disk_io_time_seconds_total|node_disk_read_bytes_total|node_disk_read_time_seconds_total|node_disk_reads_completed_total|node_disk_write_time_seconds_total|node_disk_writes_completed_total|node_disk_written_bytes_total|node_filesystem_avail_bytes|node_filesystem_files|node_filesystem_files_free|node_filesystem_free_bytes|node_filesystem_size_bytes|node_intr_total|node_load1|node_load15|node_load5|node_memory_Active_file_bytes|node_memory_Buffers_bytes|node_memory_Cached_bytes|node_memory_Inactive_file_bytes|node_memory_MemAvailable_bytes|node_memory_MemFree_bytes|node_memory_MemTotal_bytes|node_memory_SReclaimable_bytes|node_memory_SwapFree_bytes|node_memory_SwapTotal_bytes|node_netstat_Icmp6_InMsgs|node_netstat_Icmp_InMsgs|node_netstat_Icmp6_OutMsgs|node_netstat_Icmp_OutMsgs|node_netstat_Tcp_InSegs|node_netstat_Tcp_OutSegs|node_netstat_Udp_InDatagrams|node_netstat_Udp_OutDatagrams|node_network_flags|node_network_iface_link|node_network_mtu_bytes|node_network_receive_errs_total|node_network_receive_packets_total|node_network_transmit_colls_total|node_network_transmit_errs_total|node_network_transmit_packets_total|node_time_seconds|node_uname_info|node_vmstat_pswpin|node_vmstat_pswpout'
  action: 'keep'
- source_labels: ['__name__', 'namespace']
  regex: '(kube_pod|kube_job|container).*(.*)'
  target_label: jp1_pc_nodelabel
  replacement: ${2}
- source_labels: ['__name__', 'node']
  regex: 'kube_node.*(.*)'
  target_label: jp1_pc_nodelabel
- source_labels: ['__name__', 'daemonset']
  regex: 'kube_daemonset.*(.*)'
  target_label: jp1_pc_nodelabel
- source_labels: ['__name__', 'deployment']
  regex: 'kube_deployment.*(.*)'
  target_label: jp1_pc_nodelabel
- source_labels: ['__name__', 'replicaset']
  regex: 'kube_replicaset.*(.*)'
  target_label: jp1_pc_nodelabel
- source_labels: ['__name__', 'statefulset']
  regex: 'kube_statefulset.*(.*)'
  target_label: jp1_pc_nodelabel
- source_labels: ['__name__', 'owner_kind', 'owner_name']
```



```

    regex: 'kube_job_owner;CronJob;(.*)'
    target_label: jp1_pc_nodelabel
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: jp1_pc_nodelabel
  replacement: Linux metric collector(Node exporter)
- source_labels: ['__name__']
  regex: '(kube_pod_|kube_job_|container_).*'
  target_label: jp1_pc_module
  replacement: kubernetes/Namespace
- source_labels: ['__name__']
  regex: 'kube_node_.*'
  target_label: jp1_pc_module
  replacement: kubernetes/Node
- source_labels: ['__name__']
  regex: 'kube_daemonset_.*'
  target_label: jp1_pc_module
  replacement: kubernetes/DaemonSet
- source_labels: ['__name__']
  regex: 'kube_deployment_.*'
  target_label: jp1_pc_module
  replacement: kubernetes/Deployment
- source_labels: ['__name__']
  regex: 'kube_replicaset_.*'
  target_label: jp1_pc_module
  replacement: kubernetes/ReplicaSet
- source_labels: ['__name__']
  regex: 'kube_statefulset_.*'
  target_label: jp1_pc_module
  replacement: kubernetes/StatefulSet
- source_labels: ['__name__', 'owner_kind']
  regex: 'kube_job_owner;CronJob'
  target_label: jp1_pc_module
  replacement: kubernetes/CronJob
- source_labels: ['__name__']
  regex: 'kube_.*|container_.*'
  target_label: jp1_pc_trendname
  replacement: kubernetes
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: jp1_pc_trendname
  replacement: node_exporter
- source_labels: ['__name__']
  regex: 'kube_.*'
  target_label: jp1_pc_exporter
  replacement: JPC Kube state metrics
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: jp1_pc_exporter
  replacement: JPC Node exporter
- source_labels: ['__name__']
  regex: 'container_.*'
  target_label: jp1_pc_exporter
  replacement: JPC Kubelet
- source_labels: ['__name__']
  regex: 'kube_.*'
  target_label: job
  replacement: jpc_kube_state

```

```

- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: job
  replacement: jpc_kube_node
- source_labels: ['__name__']
  regex: 'container_.*'
  target_label: job
  replacement: jpc_kubelet
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: jp1_pc_category
  replacement: platform
- source_labels: ['job', 'instance']
  regex: 'jpc_kube_state;([^.:]+):?(.*)'
  target_label: jp1_pc_remote_monitor_instance
  replacement: ${1}:Kubernetes state metric collector(Kube state metrics)
- source_labels: ['job', 'instance']
  regex: 'jpc_kubelet;([^.:]+):?(.*)'
  target_label: jp1_pc_remote_monitor_instance
  replacement: ${1}:Kubernetes resource metric collector(Kubelet)
- regex: '.__.+_|jp1_pc_prome_hostname|jp1_pc_prome_clustername|jp1_pc_nodelabel|jp1_pc_trendname|jp1_pc_module|jp1_pc_exporter|jp1_pc_remote_monitor_instance|instance|job|cron|job|namespace|schedule|concurrency_policy|daemonset|deployment|condition|status|job_name|owner_kind|owner_name|owner_is_controller|reason|replicaset|statefulset|revision|phase|node|kernel_version|os_image|container_runtime_version|kubelet_version|kubeproxy_version|pod_cidr|provider_id|system_uuid|internal_ip|key|value|effect|resource|unit|pod|host_ip|pod_ip|created_by_kind|created_by_name|uid|priority_class|host_network|ip|ip_family|image_image_id|image_spec|container_id|container|type|persistentvolumeclaim|label_.+_LABEL|id|name|device|major|minor|operation|cpu|mode|failure_type|scope'
  action: 'labelkeep'

```

2. Pod のノードを作成するための設定

```

- source_labels: ['__name__']
  regex: 'kube_pod_owner|kube_pod_status_phase|container_cpu_usage_seconds_total|container_fs_reads_bytes_total|container_fs_writes_bytes_total|container_memory_working_set_bytes|container_spec_memory_limit_bytes'
  action: 'keep'
- source_labels: ['pod']
  target_label: jp1_pc_nodelabel
- target_label: jp1_pc_module
  replacement: kubernetes/Pod
- target_label: jp1_pc_trendname
  replacement: kubernetes
- target_label: jp1_pc_exporter
  replacement: JPC Kube state metrics
- target_label: job
  replacement: jpc_kube_state
- source_labels: ['instance']
  regex: '([^.:]+):?(.*)'
  target_label: jp1_pc_remote_monitor_instance
  replacement: ${1}:Kubernetes state metric collector(Kube state metrics)
- regex: '.__.+_|jp1_pc_prome_hostname|jp1_pc_prome_clustername|jp1_pc_nodelabel|jp1_pc_trendname|jp1_pc_module|jp1_pc_exporter|jp1_pc_remote_monitor_instance|instance|job|cron|job|namespace|schedule|concurrency_policy|daemonset|deployment|condition|status|job_name|owner_kind|owner_name|owner_is_controller|reason|replicaset|statefulset|revision|phase|node|kernel_version|os_image|container_runtime_version|kubelet_version|kubeproxy_version|pod_cidr|provider_id|system_uuid|internal_ip|key|value|effect|resource|unit|pod|host_ip|pod

```

```
_ip|created_by_kind|created_by_name|uid|priority_class|host_network|ip|ip_family|image_image_id|image_spec|container_id|container|type|persistentvolumeclaim|label_+_LABEL|id|name|device|major|minor|operation|cpu|mode|failure_type|scope'
  action: labelkeep
```

3. クラスターのノードを作成するための設定

```
- source_labels: ['__name__', 'jp1_pc_prome_clustername']
  regex: '(container_cpu_usage_seconds_total|container_fs_reads_bytes_total|container_fs_writes_bytes_total|container_memory_working_set_bytes|container_spec_memory_limit_bytes);(.+)'
  action: 'keep'
- source_labels: ['jp1_pc_prome_clustername']
  target_label: jp1_pc_nodelabel
- target_label: jp1_pc_module
  replacement: kubernetes/Cluster
- target_label: jp1_pc_trendname
  replacement: kubernetes
- target_label: jp1_pc_exporter
  replacement: JPC Kubelet
- target_label: job
  replacement: jpc_kubelet
- source_labels: ['instance']
  regex: '([^:]+):?(.*)'
  target_label: jp1_pc_remote_monitor_instance
  replacement: ${1}:Kubernetes resource state metric collector(Kubelet)
- regex: '.__+_|jp1_pc_prome_hostname|jp1_pc_prome_clustername|jp1_pc_nodelabel|jp1_pc_trendname|jp1_pc_module|jp1_pc_exporter|jp1_pc_remote_monitor_instance|instance|job|cronjob|namespace|schedule|concurrency_policy|daemonset|deployment|condition|status|job_name|owner_kind|owner_name|owner_is_controller|reason|replicaset|statefulset|revision|phase|node|kernel_version|os_image|container_runtime_version|kubelet_version|kubeproxy_version|pod_cidr|provider_id|system_uuid|internal_ip|key|value|effect|resource|unit|pod|host_ip|pod_ip|created_by_kind|created_by_name|uid|priority_class|host_network|ip|ip_family|image_image_id|image_spec|container_id|container|type|persistentvolumeclaim|label_+_LABEL|id|name|device|major|minor|operation|cpu|mode|failure_type|scope'
  action: labelkeep
```

(c) Prometheus の設定変更 (Red Hat OpenShift)

■前提条件

- cluster-admin ロールを持つユーザーとしてクラスターにアクセスできる
- OpenShift CLI (oc) がインストールされている

■手順

1. ConfigMap オブジェクトが作成されているか確認する。

```
$ oc -n openshift-monitoring get configmap cluster-monitoring-config
```

2. ConfigMap オブジェクトが作成されていない場合、新規にファイルを作成する。

```
$ vi cluster-monitoring-config.yaml
```

3. ConfigMap オブジェクトが作成されている場合、openshift-monitoring プロジェクトで cluster-monitoring-config オブジェクトを編集する。

```
$ oc -n openshift-monitoring edit configmap cluster-monitoring-config
```

4. data/config.yaml/prometheusK8s に設定内容をキャメルケースで記載する。

(記載例)

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-monitoring-config
  namespace: openshift-monitoring
data:
  config.yaml: |
    prometheusK8s:
      externalLabels:
        jp1_pc_prome_hostname: promHost
        jp1_pc_prome_clustername: myCluster
      remoteWrite:
        - url: http://JP1/IM - Manager (インテリジェント統合管理基盤) のホスト名:20703/im/api/v1/trendData/write
      writeRelabelConfigs:
        - sourceLabels: ['__name__']
          regex: 'kube_job_status_failed|kube_job_owner|kube_pod_status_phase|kube_daemonset_status_desired_number_scheduled|kube_daemonset_status_current_number_scheduled|kube_deployment_spec_replicas|kube_deployment_status_replicas_available|kube_replicaset_spec_replicas|kube_replicaset_status_ready_replicas|kube_replicaset_owner|kube_statefulset_replicas|kube_statefulset_status_replicas_ready|kube_node_status_condition|container_cpu_usage_seconds_total|container_fs_reads_bytes_total|container_fs_writes_bytes_total|container_memory_working_set_bytes|container_spec_memory_limit_bytes|node_boot_time_seconds|node_context_switches_total|node_cpu_seconds_total|node_disk_io_now|node_disk_io_time_seconds_total|node_disk_read_bytes_total|node_disk_reads_completed_total|node_disk_writes_completed_total|node_disk_written_bytes_total|node_filesystem_avail_bytes|node_filesystem_files|node_filesystem_files_free|node_filesystem_free_bytes|node_filesystem_size_bytes|node_intra_node_load1|node_load1|node_load15|node_load5|node_memory_Active_file_bytes|node_memory_Buffers_bytes|node_memory_Cached_bytes|node_memory_Inactive_file_bytes|node_memory_MemAvailable_bytes|node_memory_MemFree_bytes|node_memory_MemTotal_bytes|node_memory_SReclaimable_bytes|node_memory_SwapFree_bytes|node_memory_SwapTotal_bytes|node_netstat_Icmp6_InMsgs|node_netstat_Icmp_InMsgs|node_netstat_Icmp6_OutMsgs|node_netstat_Icmp_OutMsgs|node_netstat_Tcp_InSegs|node_netstat_Tcp_OutSegs|node_netstat_Udp_InDatagrams|node_netstat_Udp_OutDatagrams|node_network_flags|node_network_iface_link|node_network_mtu_bytes|node_network_receive_errors_total|node_network_receive_packets_total|node_network_transmit_colls_total|node_network_transmit_errors_total|node_network_transmit_packets_total|node_time_seconds|node_uname_info|node_vmstat_pswpin|node_vmstat_pswpout'
          action: keep
        - sourceLabels: ['__name__', 'namespace']
          regex: '(kube_pod_|kube_job_|container_.*)';(.*)'
          target_label: jp1_pc_node_label
          replacement: $2
        - sourceLabels: ['__name__', 'node']
          regex: 'kube_node_.*;(.*)'
          target_label: jp1_pc_node_label
        - sourceLabels: ['__name__', 'daemonset']
          regex: 'kube_daemonset_.*;(.*)'
          target_label: jp1_pc_node_label
```

```

- sourceLabels: ['__name__', 'deployment']
  regex: 'kube_deployment_.*;(.)'
  target_label: jp1_pc_nodelabel
- sourceLabels: ['__name__', 'replicaset']
  regex: 'kube_replicaset_.*;(.)'
  target_label: jp1_pc_nodelabel
- sourceLabels: ['__name__', 'statefulset']
  regex: 'kube_statefulset_.*;(.)'
  target_label: jp1_pc_nodelabel
- sourceLabels: ['__name__', 'owner_name']
  regex: 'kube_job_owner;(.)'
  target_label: jp1_pc_nodelabel
- sourceLabels: ['__name__', 'instance']
  regex: 'node_.*;(.)'
  target_label: jp1_pc_nodelabel
- sourceLabels: ['__name__']
  regex: 'kube_.*'
  target_label: jp1_pc_trendname
  replacement: kube_state_metrics
- sourceLabels: ['__name__']
  regex: 'node_.*'
  target_label: jp1_pc_trendname
  replacement: node_exporter
- sourceLabels: ['__name__']
  regex: 'container_.*'
  target_label: jp1_pc_trendname
  replacement: kubelet
- sourceLabels: ['__name__']
  regex: 'kube_.*'
  target_label: jp1_pc_exporter
  replacement: JPC Kube state metrics
- sourceLabels: ['__name__']
  regex: 'node_.*'
  target_label: jp1_pc_exporter
  replacement: JPC Node exporter
- sourceLabels: ['__name__']
  regex: 'container_.*'
  target_label: jp1_pc_exporter
  replacement: JPC Kubelet
- sourceLabels: ['__name__']
  regex: 'kube_.*'
  target_label: job
  replacement: jpc_kube_state
- sourceLabels: ['__name__']
  regex: 'node_.*'
  target_label: job
  replacement: jpc_node
- sourceLabels: ['__name__']
  regex: 'container_.*'
  target_label: job
  replacement: jp1_kubelet

```

5. ファイルを保存して、変更内容を ConfigMap オブジェクトに適用する。

```
$ oc apply -f cluster-monitoring-config.yaml
```

(d) Prometheus の設定変更 (Amazon Elastic Kubernetes Service (EKS))

■手順

1. 任意の名前の yml ファイル (例: my_prometheus_values.yml) を作成し, server セクションに設定内容を記載する。

- external_labels の設定内容
global.external_labels セクションに記載します。
- remote_write の設定内容
remoteWrite セクションに記載します。

(記載例)

```
server:
  global:
    external_labels:
      jp1_pc_prome_hostname: promHost
      jp1_pc_prome_clustername: myCluster
  remoteWrite:
    - url: http://JP1/IM - Manager (インテリジェント統合管理基盤) のホスト名:20703/im/api/v1/trendData/write
      write_relabel_configs:
        - sourceLabels: ['__name__']
          regex: 'kube_job_status_failed|kube_job_owner|kube_pod_status_phase|kube_daemonset_status_desired_number_scheduled|kube_daemonset_status_current_number_scheduled|kube_deployment_spec_replicas|kube_deployment_status_replicas_available|kube_replicaset_spec_replicas|kube_replicaset_status_ready_replicas|kube_replicaset_owner|kube_statefulset_replicas|kube_statefulset_status_replicas_ready|kube_node_status_condition|container_cpu_usage_seconds_total|container_fs_reads_bytes_total|container_fs_writes_bytes_total|container_memory_working_set_bytes|container_spec_memory_limit_bytes|node_boot_time_seconds|node_context_switches_total|node_cpu_seconds_total|node_disk_io_now|node_disk_io_time_seconds_total|node_disk_read_bytes_total|node_disk_reads_completed_total|node_disk_writes_completed_total|node_disk_written_bytes_total|node_filesystem_avail_bytes|node_filesystem_files|node_filesystem_files_free|node_filesystem_free_bytes|node_filesystem_size_bytes|node_intra_node_load1|node_load15|node_load5|node_memory_Active_file_bytes|node_memory_Buffers_bytes|node_memory_Cached_bytes|node_memory_Inactive_file_bytes|node_memory_MemAvailable_bytes|node_memory_MemFree_bytes|node_memory_MemTotal_bytes|node_memory_SReclaimable_bytes|node_memory_SwapFree_bytes|node_memory_SwapTotal_bytes|node_netstat_Icmp6_InMsgs|node_netstat_Icmp_InMsgs|node_netstat_Icmp6_OutMsgs|node_netstat_Icmp_OutMsgs|node_netstat_Tcp_InSegs|node_netstat_Tcp_OutSegs|node_netstat_Udp_InDatagrams|node_netstat_Udp_OutDatagrams|node_network_flags|node_network_iface_link|node_network_mtu_bytes|node_network_receive_errs_total|node_network_receive_packets_total|node_network_transmit_colls_total|node_network_transmit_errs_total|node_network_transmit_packets_total|node_time_seconds|node_uname_info|node_vmstat_pswpin|node_vmstat_pswpout'
          action: keep
        - source_labels: ['__name__', 'namespace']
          regex: '(kube_pod|kube_job|container).*(.*)'
          target_label: jp1_pc_node_label
          replacement: $2
        - source_labels: ['__name__', 'node']
          regex: 'kube_node.*(.*)'
          target_label: jp1_pc_node_label
        - source_labels: ['__name__', 'daemonset']
          regex: 'kube_daemonset.*(.*)'
```

```

target_label: jp1_pc_nodelabel
- source_labels: ['__name__', 'deployment']
  regex: 'kube_deployment_.*;(.)'
  target_label: jp1_pc_nodelabel
- source_labels: ['__name__', 'replicaset']
  regex: 'kube_replicaset_.*;(.)'
  target_label: jp1_pc_nodelabel
- source_labels: ['__name__', 'statefulset']
  regex: 'kube_statefulset_.*;(.)'
  target_label: jp1_pc_nodelabel
- source_labels: ['__name__', 'owner_name']
  regex: 'kube_job_owner;(.)'
  target_label: jp1_pc_nodelabel
- source_labels: ['__name__', 'instance']
  regex: 'node_.*;(.)'
  target_label: jp1_pc_nodelabel
- source_labels: ['__name__']
  regex: 'kube_.*'
  target_label: jp1_pc_trendname
  replacement: kube_state_metrics
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: jp1_pc_trendname
  replacement: node_exporter
- source_labels: ['__name__']
  regex: 'container_.*'
  target_label: jp1_pc_trendname
  replacement: kubelet
- source_labels: ['__name__']
  regex: 'kube_.*'
  target_label: jp1_pc_exporter
  replacement: JPC Kube state metrics
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: jp1_pc_exporter
  replacement: JPC Node exporter
- source_labels: ['__name__']
  regex: 'container_.*'
  target_label: jp1_pc_exporter
  replacement: JPC Kubelet
- source_labels: ['__name__']
  regex: 'kube_.*'
  target_label: job
  replacement: jpc_kube_state
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: job
  replacement: jpc_node
- source_labels: ['__name__']
  regex: 'container_.*'
  target_label: job
  replacement: jp1_kubelet

```

2. 変更内容を適用する。

```

helm upgrade prometheus-chart-name prometheus-community/prometheus -n prometheus-namespac
e -f my_prometheus_values.yaml

```


(e) 取得対象の設定（オプション）

■監視対象の変更

ユーザー環境の監視対象の一部だけを JP1/IM で監視したい場合は、write_relabel_configs セクションに指定します。下記に指定例を示します。

(指定例 1) 特定のリソースのホワイトリストを指定

```
- source_labels: ['__name__', 'pod']
  regex: '(kube_pod_|container_).*;coredns-.*|prometheus'
  action: 'keep'
```

(指定例 2) すべてのリソースのブラックリストを指定

```
- source_labels: ['jp1_pc_nodelabel']
  regex: 'coredns-.*|prometheus'
  action: 'drop'
```

また、すでに収集対象としているメトリックについて、異なる単位でも集約して監視を行いたい場合は、remote_writeセクションを追加し、監視したい単位での定義を行います。

■監視メトリクスの変更

統合オペレーション・ビューアーの [トレンド] タブに表示するメトリックを変更する場合は、メトリック定義ファイルを編集します。

対象となるメトリック定義ファイルを、次に示します。

- Node exporter のメトリック定義ファイル (metrics_node_exporter.conf)
- コンテナ監視のメトリック定義ファイル (metrics_kubernetes.conf)

各メトリック定義ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の該当するファイルを説明している個所を参照してください。

(f) システムノード定義ファイル (imdd_systemnode.conf) の設定（必須）

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.6(1)(i)ツリーの形式」に示すシステムノードを作成するときは、システムノード定義ファイル (imdd_systemnode.conf) を編集して、次の設定項目を指定します。ここに記載のない設定項目については、任意の値を指定します。

表 1-19 システムノード定義ファイル (imdd_systemnode.conf) の設定項目

設定項目	設定値
displayname	Kubernetes コンポーネントの名前を指定します。
type	次の文字列を大文字表記で指定します。 Kubernetes-Kubernetes コンポーネント名 「Kubernetes コンポーネント名」は、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.4(2)(b)Kubernetes」で、Kubernetes の監視対象のコンポーネント名について説明している個所の「コンポーネント名」が該当します。
name	次の文字列を指定します。

設定項目	設定値
	[{"*":"regex"}]

コンテナ監視のメトリック定義ファイルの初期設定で監視する Kubernetes コンポーネントに対して、システム管理ノードを設定する場合の、システムノード定義ファイルの設定例を、次に示します。

表 1-20 システムノード定義ファイル (imdd_systemnode.conf) の設定例

設定項目		
displayName	type	name
Clusters	JP1PC-KUBERNETES-CLUSTER	[{"*":"regex"}]
Nodes	JP1PC-KUBERNETES-NODE	[{"*":"regex"}]
Namespaces	JP1PC-KUBERNETES-NAMESPACE	[{"*":"regex"}]
Deployments	JP1PC-KUBERNETES-DEPLOYMENT	[{"*":"regex"}]
DaemonSets	JP1PC-KUBERNETES-DAEMONSET	[{"*":"regex"}]
ReplicaSets	JP1PC-KUBERNETES-REPLICASET	[{"*":"regex"}]
StatefulSets	JP1PC-KUBERNETES-STATEFULSET	[{"*":"regex"}]
CronJobs	JP1PC-KUBERNETES-CRONJOB	[{"*":"regex"}]
Pods	JP1PC-KUBERNETES-POD	[{"*":"regex"}]

上記の内容と上位の Kubernetes をシステムノード定義ファイルに設定した場合、次のようになります。

<pre> { "meta":{ "version":"2" }, "allSystem":[{ "id":"kubernetes", "displayName":"Kubernetes", "children":[{ "id":"cluster", "displayName":"Clusters", "objectRoot":[{ "type":"JP1PC-KUBERNETES-CLUSTER", "name":["*":"regex"] }] }] }, { "id":"namespace", "displayName":"Namespaces", "objectRoot":[{ </pre>

```

        "type": "JP1PC-KUBERNETES-NAMESPACE",
        "name": [{".*": "regexp"}]
    }
]
},
{
    "id": "node",
    "displayName": "Nodes",
    "objectRoot": [
        {
            "type": "JP1PC-KUBERNETES-NODE",
            "name": [{".*": "regexp"}]
        }
    ]
},
{
    "id": "deployment",
    "displayName": "Deployments",
    "objectRoot": [
        {
            "type": "JP1PC-KUBERNETES-DEPLOYMENT",
            "name": [{".*": "regexp"}]
        }
    ]
},
{
    "id": "daemonset",
    "displayName": "DaemonSets",
    "objectRoot": [
        {
            "type": "JP1PC-KUBERNETES-DAEMONSET",
            "name": [{".*": "regexp"}]
        }
    ]
},
{
    "id": "replicaset",
    "displayName": "ReplicaSets",
    "objectRoot": [
        {
            "type": "JP1PC-KUBERNETES-REPLICASET",
            "name": [{".*": "regexp"}]
        }
    ]
},
{
    "id": "statefulset",
    "displayName": "StatefulSets",
    "objectRoot": [
        {
            "type": "JP1PC-KUBERNETES-STATEFULSET",
            "name": [{".*": "regexp"}]
        }
    ]
},
{
    "id": "cronjob",
    "displayName": "CronJobs",

```

```

    "objectRoot":[
      {
        "type":"JP1PC-KUBERNETES-CRONJOB",
        "name":[".*":"regex"]
      }
    ],
    {
      "id":"pod",
      "displayName":"Pods",
      "objectRoot":[
        {
          "type":"JP1PC-KUBERNETES-POD",
          "name":[".*":"regex"]
        }
      ]
    }
  ]
}
}
}
}

```

システムノード定義ファイルを指定しておくと、jddcreatetree コマンドが実行されたときに、Kubernetes コンポーネント名に応じたシステムノードの配下に IM 管理ノードが表示されます。

システムノード定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」(2. 定義ファイル) の JP1/IM - Manager の「システムノード定義ファイル (imdd_systemnode.conf)」を参照してください。

(12) Script exporter の定義ファイルの編集

(a) 監視対象スクリプトの指定 (必須)

■Script exporter 設定ファイル (jpc_script_exporter.yml) の編集

Script exporter 設定ファイル (jpc_script_exporter.yml) を編集して、監視対象スクリプトを定義します。

Script exporter 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Script exporter 設定ファイル (jpc_script_exporter.yml)」(2. 定義ファイル) を参照してください。

(b) 監視メトリックの変更 (オプション)

■Prometheus 設定ファイル (jpc_prometheus_server.yml) の編集

スクリプトから収集したメトリクスを追加する場合は、Prometheus 設定ファイル (jpc_prometheus_server.yml) の metric_relabel_config セクションに追加します。

Prometheus 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Prometheus 設定ファイル (jpc_prometheus_server.yml)」(2. 定義ファイル) を参照してください。

```
scrape_configs:
  - job_name: jpc_script_exporter
    :
    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'script_success|script_duration_seconds|script_exit_code【ここにメトリクスを追加します】'
```

■Script exporter のメトリック定義ファイル (metrics_script_exporter.conf) の編集

統合オペレーション・ビューアーの [トレンド] タブに表示するメトリックを変更する場合は、Script exporter のメトリック定義ファイル (metrics_script_exporter.conf) の設定を変更します。

Script exporter のメトリック定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Script exporter のメトリック定義ファイル (metrics_script_exporter.conf)」(2. 定義ファイル) を参照してください。

(c) ポートを変更する (オプション)

Script exporter が使用するリッスンポートは、script_exporter コマンドの--web.listen-address オプションに指定します。

script_exporter コマンドのオプションの変更方法については、「[1.21.2\(1\)\(c\)コマンドラインオプションを変更する \(Windows の場合\)](#)」、および「[2.19.2\(1\)\(c\)コマンドラインオプションを変更する \(Linux の場合\)](#)」を参照してください。また、--web.listen-address オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「サービス定義ファイル (jpc_プログラム名.service.xml)」(2. 定義ファイル) の「script_exporter コマンドのオプション」、および「ユニット定義ファイル (jpc_プログラム名.service)」(2. 定義ファイル) の「コマンドラインのオプションを変更したい場合」を参照してください。

なお、デフォルトのポートは「20722」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

注意事項

- このオプションにホスト名を指定する場合、同じホスト上の Script exporter のディスカバリ設定ファイル (jpc_file_sd_config_script.yml) の targets に、同じホスト名を設定する必要があります。http_sd_config で指定する場合は、url も変更します。
- このオプションに IP アドレスを指定する場合、同じホスト上の Script exporter のディスカバリ設定ファイル (jpc_file_sd_config_script.yml) の targets に、オプションで指定した IP アドレスに解決されるホスト名を設定する必要があります。http_sd_config で指定する場合は、url も変更します。

(d) SAP システムのログ抽出コマンドを実行する場合の設定 (オプション)

Script exporter を使用して、SAP システムのログ抽出コマンドを実行する場合は、SAP システム監視の Script exporter 設定ファイルのサンプルファイル (jpc_script_exporter_sap.yml) を使用して、Script exporter の設定を行います。

SAP システム監視の Script exporter 設定ファイルのサンプルファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「SAP システム監視の Script exporter 設定ファイルのサンプルファイル (jpc_script_exporter_sap.yml)」(2. 定義ファイル) を参照してください。

設定方法については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「SAP システム監視の Script exporter 設定ファイルのサンプルファイル (jpc_script_exporter_sap.yml)」(2. 定義ファイル), および「[1.21.2\(12\)Script exporter の定義ファイルの編集](#)」を参照してください。

(13) Web シナリオ監視機能の設定

Web シナリオ監視機能を使用する場合の Web exporter の設定手順について説明します。

(a) JP1/IM - Agent のセットアップ

JP1/IM - Agent が Web シナリオ監視機能を使用できるようにするためのセットアップを行います。

■ エージェントホスト上のブラウザの設定

- ブラウザーのインストール
Playwright による Web シナリオファイルの実行, および, Web シナリオ作成機能で起動するブラウザをインストールします。
ブラウザが既にインストール済みの場合は, インストール不要です。
- ブラウザーの言語の設定
ブラウザを表示する場合に使用する言語を, ブラウザーでできるようにしておく必要があります。
使用するブラウザの設定画面で, 使用する言語が追加されているかを確認し, 追加されていない場合は, Codegen の実行, および, Playwright による監視が正常に動作しないことがあるため, 使用する言語を追加します。

■ 認証の設定

Playwright が監視先の Web アプリケーションにアクセスする際に, クライアント認証または HTTP 認証 (Basic 認証) を行う場合, 証明書やパスワードなどの設定が必要となります。

表 1-21 監視条件と必要な設定

監視条件	必要なファイル	必要な設定
クライアント認証する	PKCS#12 形式のクライアント証明書ファイルを, クライアントホストの任意のフォルダに配置します。	• クライアントホストのブラウザに証明書ファイルをインポートします。 • 次のコマンドを実行して, 使用するレジストリキーを登録します。 ■Google Chrome を使用する場合 reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\AutoSelectCertificateForUrls" /v 1 以

監視条件	必要なファイル	必要な設定
		上の整数 /t "REG_SZ" /d "{¥"pattern¥":¥"クライアント認証が必要な Web サイトの URL¥",¥"filter¥":{¥"ISSUER¥":{¥"CN¥":¥"CA 証明書の発行者の CN¥"}}}" ■Microsoft Edge を使用する場合 <pre>reg add "HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Edge¥AutoSelectCertificateForUrls" /v 1 以上の整数 /t "REG_SZ" /d "{¥"pattern¥":¥"クライアント認証が必要な Web サイトの URL¥",¥"filter¥":{¥"ISSUER¥":{¥"CN¥":¥"CA 証明書の発行者の CN¥"}}}"</pre> Playwright 設定ファイルで次のオプションを変更します。 <変更前> <pre>headless true</pre> <変更後> <pre>headless false</pre>
Basic 認証する	なし。	Web シナリオファイルに、ユーザー名とパスワードを定義します。 Web シナリオ作成機能で、URL を指定してログインする Web サイトに遷移する際に、ユーザー名とパスワードを次のように入力します。 <pre>http://ユーザー名:パスワード@ドメイン名:ポート/パス...</pre>

■ 環境変数の設定

JP1/IM - Agent のホストが、Web exporter から npx playwright test コマンドを実行できるように、環境変数を設定します。次の手順を実施します。

1. [設定] - [システム] - [詳細情報] - [関連設定] - [システムの詳細設定] からシステムのプロパティダイアログを表示する。
2. [環境変数] ボタンをクリックし、環境変数ダイアログを表示する。
3. システム環境変数に、次のように設定する。

変数名	変数値
Path	JP1/IM - Agent のインストール先¥jp1ima¥lib¥nodejs

■ Web exporter の設定

Web exporter 設定ファイル (jpc_web_exporter.yml) に指定した Web シナリオを実行するユーザーに対して、パスワードを登録する必要があります。パスワードの登録については、マニュアル「JP1/Integrated

Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」(1. コマンド) の引数を参照してください。

Web exporter 設定ファイル (jpc_web_exporter.yml) およびシークレットキーは、Web exporter の起動時にだけ反映されます。Web exporter の起動後に変更した Web exporter 設定ファイル (jpc_web_exporter.yml) またはシークレットキーを反映するためには、Web exporter の再起動が必要です。

■ Web シナリオファイルの新規作成

Web シナリオファイルを新たに作成する場合は、次の手順を実施します。

1. Web exporter を停止する。

Web exporter がすでに起動している場合は、停止します。

2. Web シナリオファイルを作成する。

ユーザーは、Web シナリオ作成支援機能を使用して、Web シナリオファイルを作成します。Web シナリオ作成支援機能の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(1)(m) Web シナリオ監視機能」の「Web シナリオ作成支援機能」を説明している個所を参照してください。

Web シナリオ作成支援機能で生成したコードを Web シナリオファイルに出力します。操作記録中に、誤って操作した結果が記録され、誤ったコードが生成された場合は、codegen を終了し、再度操作を記録します。

作成した Web シナリオファイルは、次のフォルダに配置します。

- 物理ホストの場合

JP1/IM - Agent のインストール先フォルダ¥jplima¥lib¥playwright¥tests¥

- 論理ホストの場合

共有フォルダ¥jplima¥lib¥playwright¥tests¥

Codegen の操作によって記録されるコードのうち、動作を確認したコードについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(1)(m) Web シナリオ監視機能」の「Web シナリオ作成機能 (playwright codegen)」に記載している「Web シナリオとして記録し計測できるブラウザの操作や動作」を参照してください。

Web シナリオファイルの形式については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Web シナリオファイル (任意の名前.spec.ts)」(2. 定義ファイル) を参照してください。

設定ファイルの編集方法については、「1.19.3(1)(a) 共通の設定方法」の「設定ファイルを編集する (Windows の場合)」を参照してください。

■ Playwright 設定ファイルの設定

作成した Web シナリオファイルを実行する定義を、Playwright 設定ファイル (jpc_playwright.config.ts) に追加します。なお、インストール時に格納されているファイル以外を Playwright 設定ファイルとして

使用する場合（モデルファイルやオリジナルの設定ファイルをコピーして作成した場合も含む）、ファイルのアクセス権限を Administrators だけに設定してください。

Playwright 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Playwright 設定ファイル (jpc_playwright.config.ts)」(2. 定義ファイル) を参照してください。

設定ファイルの編集方法については、「[1.19.3\(1\)\(a\) 共通の設定方法](#)」の「設定ファイルを編集する (Windows の場合)」を参照してください。

■ Web exporter のディスカバリ設定ファイルの設定

1. Web exporter のディスカバリ設定ファイルを編集する。

Web exporter のディスカバリ設定ファイル (jpc_file_sd_config_web.yml) を編集し、実行する Web シナリオファイル名を定義します。

設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Web exporter のディスカバリ設定ファイル (jpc_file_sd_config_web.yml)」(2. 定義ファイル) を参照してください。

2. Web exporter のディスカバリ設定ファイルを新規作成する（オプション）。

異なるタイムアウトを設定して複数の Web exporter のスクレイプを実行したい場合など、Prometheus 設定ファイルにデフォルトで定義されているスクレイプジョブを追加で設定したいときは、新しくディスカバリ設定ファイルを作成します。

作成方法については、「[1.21.2\(3\)\(i\) Web exporter のスクレイプジョブを追加する \(Windows の場合\) \(オプション\)](#)」の手順「Web exporter のディスカバリ設定ファイルを追加する (オプション)」を参照してください。

■ Web exporter のスクレイプジョブの設定

「[1.21.2\(3\)\(i\) Web exporter のスクレイプジョブを追加する \(Windows の場合\) \(オプション\)](#)」を参照してください。

■ Web exporter の起動

Web exporter を起動します。

(14) VMware exporter の設定

(a) ポートを変更する (Windows の場合) (オプション)

VMware exporter が使用するリッスンポートは、vmware_exporter コマンドの--port オプションに指定します。変更したポートは、VMware exporter のサービスを再起動したタイミングで反映されます。

vmware_exporter コマンドのオプションの変更方法については、「[1.21.2\(1\)\(c\) コマンドラインオプションを変更する \(Windows の場合\)](#)」を参照してください。また、--port オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の

「サービス定義ファイル (jpc_プログラム名_service.xml)」(2. 定義ファイル) の「vmware_exporter コマンドのオプション」を参照してください。

なお、デフォルトのポートは「20732」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

(b) セクションを追加・変更・削除する (Windows の場合) (必須)

VMware exporter では、監視対象 (VMware ESXi) ごとに、接続情報を VMware exporter 設定ファイル (jpc_vmware_exporter.yml) に定義する必要があります。この定義を「セクション」と呼びます。

初期設定で定義されているサンプル用のセクションは、次のとおりです。

表 1-22 初期設定で定義されているセクション

セクション名	特徴
default	1 件目の監視対象を設定するセクションです。 - 値を書き換えて使用します (ホスト名とポートの設定は必須)。 - セクション名「default」は、存在チェックの対象となるため、削除または変更をしないでください。

監視対象を追加する場合、default セクションをコピーし、監視対象の台数分のセクション定義を設定する必要があります。

設定を変更した場合、VMware exporter および Prometheus server のサービスの再起動が必要です。

セクションは、VMware exporter 設定ファイル (jpc_vmware_exporter.yml) に定義します。VMware exporter 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「VMware exporter 設定ファイル (jpc_vmware_exporter.yml)」(2. 定義ファイル) を参照してください。

新しいセクションのセクション名は、Prometheus 設定ファイル (jpc_prometheus_server.yml) に設定するパラメーターのセクション名と同一の名称を設定してください。詳細については、「[1.21.2\(3\)\(j\) VMware exporter のスクレイプジョブを追加する \(Windows の場合だけ\) \(オプション\)](#)」を参照してください。

新しいセクションを追加する際は、セクション別で VM 名が重複しないように設定してから、セクションを追加してください。

VMware ESXi への接続に使用するユーザーについては、「アクセスなし」または「非暗号化管理者」以外のロールを付与したものを使用します。

VMware ESXi への接続に使用するパスワードの登録については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」(1. コマンド) の引数を参照してください。シークレット登録時のパスワードの長さについては、シークレット管理コマンド (jimasecret) に従います。VMware ESXi 側でパスワードの長さの上限を変更している場合、1024 文字以内でパスワードを設定します。

VMware exporter 設定ファイルの更新、証明書ファイルの配置の手順については、「[1.21.2\(1\)\(a\) 設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

セクション定義を追加した場合は、Prometheus server から新しく作成したセクションを使用してスクレイプするためのスクレイプジョブの定義が必要になります。Prometheus server 側の設定については、「[1.21.2\(3\)\(j\) VMware exporter のスクレイプジョブを追加する \(Windows の場合だけ\) \(オプション\)](#)」を参照してください。

VMware exporter 設定ファイル (jpc_vmware_exporter.yml) およびシークレットキーは、VMware exporter の起動時にだけ反映されます。VMware exporter の起動後に変更した VMware exporter 設定ファイル (jpc_vmware_exporter.yml) またはシークレットキーを反映するためには、VMware exporter の再起動が必要です。

(c) シークレットの登録 (必須)

監視対象 (VMware ESXi) の default セクションおよびユーザーが追加するセクションの接続に使用するシークレットの登録を行います。

また、任意のセクションを追加した場合、対応するシークレットの登録を行う必要があります。

監視対象のシークレットの登録方法については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」(1. コマンド) の引数を参照してください。

■ シークレットの登録時の注意事項

シークレット管理コマンド (jimasecret) で VMware ESXi のパスワードを難読化する場合の注意事項については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」(1. コマンド) の注意事項を参照してください。

(d) 証明書の設定 (必須)

VMware exporter で SSL 認証を行う場合、物理ホスト・論理ホストに関わらず、同じ手順でマシン上に証明書の設定が必要です。

次のどれかの証明書が必要です。

- デフォルト証明書
VMware の構築時に作成される証明書です。
- vCenter Server の証明書 (証明局の証明書)
vCenter Server から発行された証明書です。
- 独自の証明書 (自己署名サーバ証明書)
使用者が自ら発行した証明書を指します。

証明書ごとの手順を、次に示します。

- デフォルト証明書の場合

1. VMware exporter 設定ファイル (jpc_vmware_exporter.yml) の項目「ignore_ssl」を True に設定する。

この設定を行っても運用上問題ないことを事前に確認してから、設定を行ってください。

- vCenter Server の証明書または独自の証明書※の場合

次の手順を実施して、証明書をインポートします。

注※ 「独自の証明書」で認証不備が発生した場合は、作成した証明書の見直しを行ってください。見直しをしても接続ができないときは、運用上問題ないことを事前に確認した上で、「デフォルトの証明書」の手順を参照してください。

■Windows の場合

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択する。
2. [ファイル名を指定して実行] ダイアログで「mmc」と入力し、[OK] ボタンをクリックする。
3. [コンソール 1] で [ファイル] - [スナップインの追加と削除] を選択する。
4. 証明書を選択し、[追加] ボタンをクリックする。
5. [コンピューターアカウント] を選択し、[次へ] ボタンをクリックする。
6. [ローカルコンピューター] を選択し、[完了] ボタンをクリックする。
7. [選択されたスナップイン] に [証明書 (ローカルコンピューター)] が追加されたことを確認し、[OK] ボタンをクリックする。
8. [証明書 (ローカルコンピューター)] - [信頼されたルート証明機関] - [証明書] を右クリックし、表示された [すべてのタスク] - [インポート] メニューを選択する。
9. [次へ] ボタンをクリックする。
10. [ファイル名] テキストボックスに、証明書の保存ファイル名を入力し、[次へ] ボタンをクリックする。
11. [証明書をすべて次のストアに配置する] を選択し、[次へ] ボタンをクリックする。
12. [完了] ボタンをクリックし、[OK] ボタンをクリックする。

■Linux の場合

- Linux 7 または Linux 8 の場合※

注※ ca-certificate パッケージが OS にインストールされていることが前提となります。

1. 次のコマンドを実行し、証明書ファイルをコピーする。
`# cp 証明書ファイルパス/etc/pki/ca-trust/source/anchors`

2. トラストストアの設定を更新する。

＜システム全体のトラストストアの設定を更新する場合の例＞

`# update-ca-trust`

- Linux 9 の場合

1. 証明書ファイルをサーバー上に配置し、次のコマンドを実行する。


```
# PKICertImport -d . -n 証明書ファイルパス -t "CT,C,C" -a -i ca_root.crt -u L
```

- Oracle Linux 7, Oracle Linux 8, または Oracle Linux 9 の場合
Linux 7 の手順を参照してください。
- SUSE Linux 12 または SUSE Linux 15 の場合

1. SSL 環境変数に証明書ファイルの場所を指定する。

```
export CA_CERT=証明書ファイルパス
export SERVER_KEY=キーファイルパス
export SERVER_CERT=サーバ証明書パス
```

2. SUSE Manager のセットアップコマンドを実行する。

```
# yast susemanager_setup
```

- Amazon Linux 2023 の場合
Linux 7 の手順を参照してください。

(15) Windows exporter (Hyper-V 監視機能) の設定

(a) ポートを変更する (オプション)

Windows exporter (Hyper-V 監視) が使用するリッスンポートは、windows_exporter コマンドの--telemetry.addr オプションに指定します。

windows_exporter コマンドのオプションの変更方法については、「[1.21.2\(1\)\(c\) コマンドラインオプションを変更する \(Windows の場合\)](#)」を参照してください。また、--telemetry.addr オプションの詳細については、マニュアル「[JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス](#)」の「サービス定義ファイル (jpc_プログラム名_service.xml)」(2. 定義ファイル) の「windows_exporter コマンドのオプション (Hyper-V 監視)」を参照してください。

なお、デフォルトのポートは「20734」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

(16) リッスンポート番号とリッスンアドレスの設定 (オプション)

デフォルトのポート番号から変更しない、かつ、リッスンする IP アドレスを限定しない場合は、この手順の実施は不要です。

リッスンするポート番号や IP アドレスを変更する場合の変更箇所などについては、「[1.21.2 JP1/IM - Agent の設定](#)」(Windows の場合) および「[2.19.2 JP1/IM - Agent の設定](#)」(Linux の場合) で、JP1/IM - Agent のモジュールやアドオンプログラムのポートを変更する手順について説明している箇所を参照してください。

(17) ファイアウォールの設定 (Windows の場合) (必須)

次に示すとおりファイアウォールを設定し、外部からのアクセスを制限する必要があります。

表 1-23 ファイアウォールの設定

ポート	ファイアウォールの設定
imagent のポート	外部からのアクセスを禁止します。
imagentproxy のポート	外部からのアクセスを禁止します。
imagentaction のポート	外部からのアクセスを禁止します。
alertmanager のポート	外部からのアクセスを禁止します。 ただし、他ホストの Blackbox exporter による外形監視で Alertmanager を監視する場合は、アクセスを許可します。この場合、必要に応じて送信元 IP アドレスを制限するなどセキュリティ対策を検討します。
prometheus_server のポート	外部からのアクセスを禁止します。 ただし、他ホストの Blackbox exporter による外形監視で Prometheus server を監視する場合は、アクセスを許可します。この場合、必要に応じて送信元 IP アドレスを制限するなどセキュリティ対策を検討します。
windows_exporter のポート	外部からのアクセスを禁止します。
node_exporter のポート	
process_exporter のポート	
ya_cloudwatch_exporter のポート	
promitor_scraper のポート	
promitor_resource_discovery のポート	
blackbox_exporter のポート	
script_exporter のポート	
fluentd のポート	

(18) 統合エージェントのプロセスの死活監視の設定（Windows の場合）（オプション）

統合エージェントのプロセスは、次の種類の方法で監視します。

- 他ホストの Blackbox exporter による外形監視
- Windows exporter によるプロセスの死活監視
- Prometheus server の up メトリックによる監視

(a) 他ホストの Blackbox exporter による外形監視

Prometheus server サービスと Alertmanager サービスは、他ホスト上で稼働している統合エージェントの Blackbox exporter から監視します。監視する URL は、次の表のとおりです。

Blackbox exporter の HTTP 監視を追加する方法については、「[1.21.2\(6\)\(c\) 監視対象を追加・変更・削除する（Windows の場合）（必須）](#)」を参照してください。アラート定義の設定方法については、「[1.21.2\(3\)\(b\) アラート定義を追加する（Windows の場合）（オプション）](#)」を参照してください。

表 1-24 Blackbox exporter の HTTP 監視で監視する URL

サービス	監視する URL
Prometheus server	http://統合エージェントのホスト名:Prometheus server のポート番号/-/healthy
Alertmanager	http://統合エージェントのホスト名:Alertmanager のポート番号/-/healthy

Blackbox exporter の HTTP 監視で監視するアラート定義の例を、次に示します。

```
groups:
- name: service_healthcheck
  rules:
- alert: jp1_pc_prometheus_healthcheck
  expr: probe_success{instance=~".*:20713/-/healthy"} == 0
  for: 3m
  labels:
    jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
    jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
    jp1_pc_severity: "Error"
    jp1_pc_metricname: "probe_success"
  annotations:
    jp1_pc_firing_description: "Prometheus serverへの通信に失敗しました。"
    jp1_pc_resolved_description: "Prometheus serverへの通信に成功しました。"
- alert: jp1_pc_alertmanager_healthcheck
  expr: probe_success{instance=~".*:20714/-/healthy"} == 0
  for: 3m
  labels:
    jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
    jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
    jp1_pc_severity: "Error"
    jp1_pc_metricname: "probe_success"
  annotations:
    jp1_pc_firing_description: "Alertmanagerへの通信に失敗しました。"
    jp1_pc_resolved_description: "Alertmanagerへの通信に成功しました。"
```

(b) Windows exporter によるプロセスの死活監視

imagentproxy サービス、imagentaction サービス、Fluentd サービス、および Windows サービス化プログラムは、Windows exporter のプロセス監視の稼動情報で監視します。監視するプロセスは次の表に記載されています。

アラート定義の設定方法については、「[1.21.2\(3\)\(b\) アラート定義を追加する（Windows の場合）（オプション）](#)」を参照してください。

表 1-25 Windows exporter で監視するプロセス

サービス	監視するプロセス	監視対象名
jpc_imagent_service※	Agent パス ¥bin¥jpc_imagent_service.exe	監視対象名 1 : imagent 監視対象名 2 : imagent
jpc_imagentproxy_service※	Agent パス ¥bin¥jpc_imagentproxy_service.exe	監視対象名 1 : imagentproxy 監視対象名 2 : imagentproxy
jpc_imagentaction_service※	Agent パス ¥bin¥jpc_imagentaction_service.exe	監視対象名 1 : imagentaction 監視対象名 2 : imagentaction
jpc_prometheus_server_service※	Agent パス ¥bin¥jpc_prometheus_server_service.exe	監視対象名 1 : prometheus 監視対象名 2 : prometheus_server
jpc_alertmanager_service※	Agent パス ¥bin¥jpc_alertmanager_service.exe	監視対象名 1 : alertmanager 監視対象名 2 : alertmanager
jpc_windows_exporter_service※	Agent パス ¥bin¥jpc_windows_exporter_service.exe	監視対象名 1 : Windows metric collector(Windows exporter) 監視対象名 2 : windows_exporter
jpc_blackbox_exporter_service※	Agent パス ¥bin¥jpc_blackbox_exporter_service.exe	監視対象名 1 : RM Synthetic metric collector(Blackbox exporter) 監視対象名 2 : blackbox_exporter
jpc_ya_cloudwatch_exporter_service※	Agent パス ¥bin¥jpc_ya_cloudwatch_exporter_service.exe	監視対象名 1 : RM AWS metric collector(Yet another cloudwatch exporter) 監視対象名 2 : ya_cloudwatch_exporter
jpc_fluentd_service※	Agent パス¥bin¥jpc_fluentd_service.exe	- ログ監視機能を使用する場合 監視対象名 1 : fluentd_win Log trapper(Fluentd) 監視対象名 2 : fluentd - ログメトリクス機能だけを使用する場合 監視対象名 1 : fluentd_prome_win Log trapper(Fluentd) 監視対象名 2 : fluentd
jpc_script_exporter_service※	Agent パス ¥bin¥jpc_script_exporter_service.exe	監視対象名 1 : Script exporter 監視対象名 2 : script_exporter
jpc_promitor_scraper_service※	Agent パス ¥bin¥jpc_promitor_scraper_service.exe	監視対象名 1 : RM Promitor 監視対象名 2 : promitor_scraper
jpc_promitor_resource_discovery_service※	Agent パス ¥bin¥jpc_promitor_resource_discovery_service.exe	監視対象名 1 : RM Promitor 監視対象名 2 : promitor_resource_discovery

注※

Windows サービス化プログラムを示します。

Windows exporter で監視するアラート定義の例を、次に示します。

```
groups:
- name: windows_exporter
  rules:
  - alert: jp1_pc_procmon 監視対象名1
    expr: expr: absent(windows_process_start_time{instance="imahost:20717", job="jpc_windows", jp1_pc_exporter="JPC Windows exporter", jp1_pc_nodelabel="jpc 監視対象名2_service", process="jpc 監視対象名2_service"}) == 1
    for: 3m
    labels:
      jp1_pc_product_name: "/HITACHI/JP1/JPCS2"
      jp1_pc_component: "/HITACHI/JP1/JPCS/CONFINFO"
      jp1_pc_severity: "Error"
      jp1_pc_metricname: "windows_process_start_time"
    annotations:
      jp1_pc_firing_description: "プロセス数がしきい値(1個)を下回りました。"
      jp1_pc_resolved_description: "プロセス数がしきい値(1個)を上回りました。"
```

- imahost の部分には、統合エージェントホスト名を指定します。20717 の部分には、Windows exporter のポート番号を指定します。
- 監視対象名 1 と監視対象名 2 には、「表 1-25 Windows exporter で監視するプロセス」の監視対象名を指定します。
- アラート定義を複数指定する場合は、「 - alert:」から始まる行以降を複数回繰り返して設定します。

(c) Prometheus server の up メトリックによる監視

Windows exporter サービス、Blackbox exporter サービス、Yet another cloudwatch exporter サービスは、Prometheus server のアラート監視で監視します。アラート定義の設定方法については、「1.21.2(3)(b) アラート定義を追加する (Windows の場合) (オプション)」を参照してください。

up メトリックを監視するアラート定義の例を、次に示します。

```
groups:
- name: exporter_healthcheck
  rules:
  - alert: jp1_pc_exporter_healthcheck
    expr: up{jp1_pc_remote_monitor_instance=""} == 0 or label_replace(sum by (jp1_pc_remote_monitor_instance, jp1_pc_exporter) (up{jp1_pc_remote_monitor_instance!=""}), "jp1_pc_nodelabel", "${1}", "jp1_pc_remote_monitor_instance", "^[^:]*:([^:]*)$") == 0
    for: 3m
    labels:
      jp1_pc_product_name: "/HITACHI/JP1/JPCS2"
      jp1_pc_component: "/HITACHI/JP1/JPCS/CONFINFO"
      jp1_pc_severity: "Error"
      jp1_pc_metricname: "up"
    annotations:
```

```
jp1_pc_firing_description: "Exporterへの通信に失敗しました。"  
jp1_pc_resolved_description: "Exporterへの通信に成功しました。"
```

(19) IM 管理ノードのツリー情報の作成と反映 (Windows の場合) (必須)

次に示す手順で、IM 管理ノードのツリー情報の作成と反映を行います。

1. 統合エージェントホストを新しく追加、または、統合エージェントホストのホスト名を変更した場合、そのホストの統合エージェント制御基盤のサービスを起動する。
2. アドオンプログラムを新しく追加、または、アドオンプログラムの設定を変更し構成が変更となる場合、そのアドオンプログラム、および、同居する統合エージェント制御基盤のサービスを起動する。
3. すべての統合エージェントホストで手順 1～2 に該当するサービスを起動したら、サービス起動後 1 分※経過するのを待つ。

注※ Prometheus 設定ファイル (jpc_prometheus_server.yml) の scrape_interval の値を変更している場合、その値の時間だけ待ちます。

4. 統合マネージャーホストで行う手順を実施する。

手順については、「[1.19.3\(1\)\(c\)IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」の手順 2～5 を参照してください。

(20) セキュリティ製品の除外設定 (Windows の場合) (オプション)

アンチウイルスソフトやセキュリティ製品を導入している場合は、次のディレクトリを除外するように設定してください。

- Windows の場合
Agent パス¥
- Linux の場合
/opt/jp1ima/

(21) 定義ファイル更新時の注意事項 (Windows の場合)

定義ファイルの更新内容を反映するために、JP1/IM - Agent のサービスを再起動した場合、サービスの再起動中は監視が停止します。

1.22 JP1/IM - Agent のコンテナ環境の構築 (Windows の場合)

コンテナ環境の作成は、次の手順で行います。

1. コンテナイメージを作成する
2. コンテナを起動する

1.22.1 コンテナイメージの作成

(1) ベースとするコンテナイメージの条件

Docker イメージ、Podman イメージのベースとするコンテナイメージの条件については、それぞれマニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.3.12(4)(c)コンテナイメージの前提条件」, 「14.3.12(5)(b)コンテナイメージの前提条件」を参照してください。

(2) Docker イメージ、Podman イメージの作成方法

1. イメージを作成する Docker ホスト上または Podman ホスト上に作業ディレクトリを作成する。
2. 作業ディレクトリ下に、次のものを用意する。

- Dockerfile ファイル
- JP1/IM - Agent のインストールパッケージ
- supervisord 定義ファイル (Supervisor を使用する場合を例として記載しています)
- 起動スクリプト
- credentials ファイル (Yet another cloudwatch exporter を使用する場合)
- conf ディレクトリに配置するファイル

ここでは、次のディレクトリ構成とします。

JP1/IM - Agent の定義ファイルのうち、更新したいファイルを conf ディレクトリに配置します。

```
作業ディレクトリ/※1
├─ Dockerfile※2
├─ JP1IMA/※3
│   └─ X64LIN/
│       ├── h_inst
│       ├── ppmanage
│       ├── setup
│       └─ PCC842C/
│           └─ 9GDL/
│               └─ . . .
├─ supervisord.conf※4
├─ start.sh※5
└─ credentials※6
```

1. インストールとセットアップ (Windows の場合)

```

└─ conf/
  └─ jpc_imagentcommon.json.model※7
  └─ jpc_alerting_rules.yml.model※8
  └─ jpc_ya_cloudwatch_exporter.yml.model※9
  └─ jpc_blackbox_exporter.yml.model※10
  └─ jpc_file_sd_config_blackbox_http.yml.model※11
  └─ jpc_file_sd_config_blackbox_icmp.yml.model※12
  └─ jpc_process_exporter.yml※13
  └─ jpc_script_exporter.yml※14
  └─ promitor/※15
    └─ scraper/※16
      └─ runtime.yml※17
      └─ metrics-declaration.yml※18
      └─ resource-discovery/※19
        └─ runtime.yml※20
        └─ resource-discovery-declaration.yml※21
  └─ user/
    └─ cert/
      └─ XXXX.crt※22

```

注※1 手順 1 で作成した作業ディレクトリ

注※2 Dockerfile ファイル

注※3 JPI/IM - Agent のインストールパッケージを展開したディレクトリおよびファイル

注※4 supervisord 定義ファイル

注※5 起動スクリプト

注※6 AWS クレデンシャルファイル (Yet another cloudwatch exporter を使用する場合)

注※7 imagent 共通設定ファイル

注※8 アラート設定ファイル (アラート定義を行う場合)

注※9 Yet another cloudwatch exporter 設定ファイル

注※10 Blackbox exporter 設定ファイル

注※11 Blackbox (HTTP/HTTPS 監視) のディスカバリ設定ファイル

注※12 Blackbox (ICMP 監視) のディスカバリ設定ファイル

注※13 Process exporter 設定ファイル (設定を変更する場合)

注※14 Script exporter 設定ファイル (設定を変更する場合)

注※15 Promitor 定義ファイル格納ディレクトリ (設定を変更する場合)

注※16 Promitor Scraper 定義ファイル格納ディレクトリ (設定を変更する場合)

注※17 Promitor Scraper 設定ファイル (設定を変更する場合)

注※18 Promitor Scraper runtime 設定ファイル (設定を変更する場合)

注※19 Promitor Resource Discovery 定義ファイル格納ディレクトリ (設定を変更する場合)

注※20 Promitor Resource Discovery 設定ファイル (設定を変更する場合)

注※21 PromitorResource Discovery runtime 設定ファイル (設定を変更する場合)

注※22 統合マネージャーホストに接続するための CA 証明書

なお、サービスプリンシパル方式で Azure に接続する場合の構築手順は、次のとおりです。

1. 「JP1/IM - Agent のコンテナ環境の構築」の構築手順のうち、「[1.21.2\(8\) Promitor の設定](#)」の「(b) Azure に接続するための認証情報の設定」の手順 4 以外を実施し、作業ディレクトリ下にファイルを作成します。
2. コンテナを起動後、「[1.21.2\(8\) Promitor の設定](#)」の「(b) Azure に接続するための認証情報の設定」の手順 4 を実施します。
3. Promitor のサービスを起動します。サービス管理については、「JP1/IM - Agent のコンテナ環境の構築」の説明を参照してください。

■定義ファイルに関する注意事項

定義ファイルに IP アドレスを指定しないでください。また、証明書ファイルに IP アドレス情報を含めしないでください。IP アドレス情報を含めた場合、動的に IP アドレスが変わるコンテナに対応できません。

■Dockerfile ファイルの例

下記の例にある ENV の行のように必要に応じてインストーラの環境変数を設定してください。

```
FROM oraclelinux:8

RUN mkdir /root/.aws
COPY credentials /root/.aws/credentials
COPY JP1IMA/X64LIN /tmp/X64LIN
COPY start.sh /opt/start.sh
COPY supervisord.conf /opt/supervisord.conf
RUN dnf install -y python3
RUN pip3 install supervisor
RUN dnf install -y cpio
RUN chmod a+x /opt/start.sh

ENV JP1IMAGENT_INSTALL_MODE "image"
ENV JP1IMAGENT_IMMGR_HOST "接続先マネージャのホスト名を設定する"
ENV JP1IMAGENT_IMMGR_INITIAL_SECRET "初期シークレットを設定する"
ENV JP1IMAGENT_ADDON_BLACKBOX_EXPORTER_ACTIVE "yes"
ENV JP1IMAGENT_ADDON_YA_CLOUDWATCH_EXPORTER_ACTIVE "yes"
ENV JP1IMAGENT_ADDON_PROMITOR_ACTIVE "no"※
ENV JP1IMAGENT_ADDON_PROCESS_EXPORTER_ACTIVE "yes"
ENV JP1IMAGENT_ADDON_SCRIPT_EXPORTER_ACTIVE "no"

RUN /tmp/X64LIN/setup -f -k P-CC842C-9GDL /tmp/
COPY conf /opt/jp1ima/conf

CMD [ "/bin/bash", "-c", "/opt/start.sh" ]
```

注※

"yes"の場合、コンテナ起動後に次のログが出力され、サービス起動に失敗した状態となります。認証情報を設定して再起動すると、正常に起動します。

Validation failed: Azure authentication is not configured correctly - No identity secret was configured for service principle authentication

■supervisord のサービス定義ファイルの作成例


```

[unix_http_server]
file=/tmp/supervisord.sock ; the path to the socket file

[supervisord]
logfile=/tmp/supervisord.log
logfile_maxbytes=5MB
logfile_backups=10
loglevel=info
pidfile=/tmp/supervisord.pid
nodaemon=true

[program:imagent]
command=/opt/jp1ima/bin/imagent
directory=/opt/jp1ima/bin/
stopasgroup=true
autostart=true
stopwaitsecs=180

[program:imagentaction]
command=/opt/jp1ima/bin/imagentaction
directory=/opt/jp1ima/bin/
stopasgroup=true
autostart=true
stopwaitsecs=180

[program:imagentproxy]
command=/opt/jp1ima/bin/imagentproxy
directory=/opt/jp1ima/bin/
stopasgroup=true
autostart=true
stopwaitsecs=180

[program:prometheus]
command=コマンドライン ※1
directory=/opt/jp1ima/bin ※2
autostart=true ※3
stopasgroup=true
stopwaitsecs=180

[program:alertmanager]
command=コマンドライン ※1
directory=/opt/jp1ima/bin ※2
autostart=true ※3
stopasgroup=true
stopwaitsecs=180

[program:node_exporter]
command=コマンドライン ※1
directory=/opt/jp1ima/bin ※2
autostart=true ※3
stopasgroup=true
stopwaitsecs=180

[program:process_exporter]
command=コマンドライン ※1
directory=/opt/jp1ima/bin

```

```

autostart=true
stopwaitsecs=180

[program:プログラム名]
command=コマンドライン ※1
directory=/opt/jplima/bin ※2
autostart=true ※3
stopasgroup=true ※4
stopwaitsecs=180

```

注 使用しないサービスについては記述不要です。

注※1 コマンドラインには、物理ホストの/usr/lib/systemd/system ディレクトリに格納されている jpc_XXXXXXX.service に記載されている ExecStart の値を使用します。このとき、「@@installdir1@@」と「@@installdir2@@」を「/opt」に置換する必要があります。

また、jpc_XXXXXXX.service に記載されている ExecStart の値が「/bin/sh -c 'XXXXXXX」で始まる場合は、「/bin/sh -c 'trap "" 15; XXXXXXXX」のように修正してください。

Alertmanager の場合の例

```
/bin/sh -c 'trap "" 15; /opt/jplima/bin/osswrapper "/opt/jplima/bin/alertmanager" ...
```

注※2 サービス管理プログラムから JP1/IM - Agent プログラムを動かす際のカレントディレクトリは「/opt/jplima/bin」にします。

注※3 自動起動を有効にします。

注※4 stopasgroup を true にします。

■起動スクリプトの例

```

#!/bin/bash
/opt/jplima/tools/jimasetup container※1
mv -f /opt/jplima/conf/jpc_file_sd_config_blackbox_http.yml ¥
/opt/jplima/conf/jpc_file_sd_config_off※2
mv -f /opt/jplima/conf/jpc_file_sd_config_blackbox_icmp.yml ¥
/opt/jplima/conf/jpc_file_sd_config_off※2
mv -f /opt/jplima/conf/jpc_file_sd_config_cloudwatch.yml ¥
/opt/jplima/conf/jpc_file_sd_config_off※2
mv -f /opt/jplima/conf/jpc_file_sd_config_process.yml ¥
/opt/jplima/conf/jpc_file_sd_config_off※2
mv -f /opt/jplima/conf/jpc_file_sd_config_promitor.yml ¥
/opt/jplima/conf/jpc_file_sd_config_off※2
exec /usr/local/bin/supervisord -c /opt/supervisord.conf※3

```

注※1 JP1/IM - Agent の初期設定コマンドを container オプション指定で実行します。

注※2 次に示すサービスについて、使用しないサービスに対応するディスカバリ設定ファイルを、/opt/jplima/conf ディレクトリから/opt/jplima/conf/jpc_file_sd_config_off ディレクトリに移動します。

サービス	ディスカバリ設定ファイル
prometheus_server	なし
alertmanager	なし
windows_exporter	jpc_file_sd_config_windows.yml

サービス	ディスカバリ設定ファイル
blackbox_exporter	- jpc_file_sd_config_blackbox_http.yml - jpc_file_sd_config_blackbox_icmp.yml
ya_cloudwatch_exporter	jpc_file_sd_config_cloudwatch.yml
fluentd	なし
promitor	jpc_file_sd_config_promitor.yml
script_exporter	なし

注※3 サービス管理ツールを実行します。

■imagent 共通設定ファイルの例

imagent 共通定義ファイルのモデルファイル (jpc_imagentcommon.json.model) の例は次のとおりです。

TLS を使用する場合は ca_file に CA 証明書のパスを設定します。TLS を使用しない場合は tls_config の項目を削除します。

```
{
  "JP1_BIND_ADDR": "ANY",
  "COM_LISTEN_ALL_ADDR": 0,
  "COM_MAX_LISTEN_NUM": 4,
  "JP1_CLIENT_BIND_ADDR": "ANY",
  "http": {
    "max_content_length": 10,
    "client_timeout": 30
  },
  "immgr": {
    "host": "@@immgr.host@",
    "proxy_url": "@@immgr.proxy_url@",
    "proxy_user": "@@immgr.proxy_user@",
    "tls_config": {
      "ca_file": "/opt/jplima/conf/user/cert/XXXX.crt",
      "insecure_skip_verify": false,
      "min_version": "TLSv1_2"
    },
    "ibase": {
      "port": @@immgr.imbase_port@@
    },
    "ibaseproxy": {
      "port": @@immgr.imbaseproxy_port@@
    }
  }
}
```

3. Dockerfile の存在するディレクトリに移動し、Docker ビルドまたは Podman ビルドを起動する。

- Docker の場合

```
# docker build -t Dockerイメージ名:タグ .
```

- Podman の場合

```
# podman build -t Podmanイメージ名:タグ .
```

(3) Docker コンテナ, Podman コンテナの作成方法

1. Docker コンテナまたは Podman コンテナを起動する。

- Docker の場合

```
# docker container run --ulimit nofile=65536:65536 --add-host=マネージャホスト名:IPアドレス -d -h コンテナにつけるホスト名 Dockerイメージ名:タグ
```

- Podman の場合

```
# podman container run --ulimit nofile=65536:65536 --add-host=マネージャホスト名:IPアドレス -d -h コンテナにつけるホスト名 Podmanイメージ名:タグ
```

❗ 重要

コンテナのホスト名は、統合オペレーション・ビューアーのツリーに表示されます。-h オプションを省略すると、Docker や Podman が自動的にホスト名を設定し、そのホスト名が統合オペレーション・ビューアーのツリーに表示されることになるため、ホスト名を指定することを推奨します。

2. サービス管理ツールのログ, JP1/IM - Agent のログを確認し、正常に稼働していることを確認する。

エラーが出力されている場合や稼働させたいプロセスが起動していない場合は、原因を特定して、Docker イメージまたは Podman イメージを作り直します。

3. IM 管理ノードのツリー情報を更新する。

詳細については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映（Windows の場合）（必須）](#)」を参照してください。

(4) Docker コンテナ, Podman コンテナの削除方法

1. Docker コンテナまたは Podman コンテナを停止する。

- Docker の場合

```
# docker container stop コンテナ名
```

- Podman の場合

```
# podman container stop コンテナ名
```

2. Docker コンテナまたは Podman コンテナを削除する。

- Docker の場合

```
# docker container rm コンテナ名
```

- Podman の場合

```
# podman container rm コンテナ名
```

3. IM 管理ノードのツリー情報を更新する。

詳細については、「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください。

(5) カーネルパラメーターへの影響について

ファイルディスクリプタ数の上限については、コンテナ起動時の`--ulimit` オプションに「65536」を指定します。

詳細については、「[1.22.1\(3\) Docker コンテナ, Podman コンテナの作成方法](#)」を参照してください。

1.22.2 JP1/IM - Agent のバージョンアップ

作成済みのコンテナ上の JP1/IM - Agent をバージョンアップすることはできますが、新しいバージョンの JP1/IM - Agent を使用して Docker イメージや Podman イメージを作成し、新しいコンテナイメージからコンテナを作り直すことを推奨します。

作成済みのコンテナ上の JP1/IM - Agent をバージョンアップする手順は、下記のとおりです。

(1) 作成済みのコンテナ上の JP1/IM - Agent を 13-11 より前のバージョンからバージョンアップする場合の手順

■JP1/IM - Agent の停止

作成済みのコンテナ上の JP1/IM - Agent をバージョンアップするときは、事前にサービス管理ツールで JP1/IM - Agent のサービスを停止します。

■サービス定義ファイルの更新

コンテナ上の JP1/IM - Agent を、13-11 より前のバージョンから 13-11 以降にバージョンアップインストールすると、`/opt/jp1ima/conf` フォルダに存在するユニット定義ファイルのモデルファイルが更新されます。このモデルファイルの `ExecStart` 行に記載されているコマンドラインを、サービス管理ツールで実行するコマンドラインとして、手動で設定しなおします。また、「`@@installdir1@@`」と「`@@installdir2@@`」を「`/opt`」に置換します。

また、コマンドラインが「`/bin/sh -c 'xxxxxxxxx`」で始まる場合は、「`/bin/sh -c 'trap "" 15; xxxxxxxxx`」のように修正します。

このマニュアルでは、サービス管理ツールとして supervisord を使用した例を記載しています。supervisord のサービス定義ファイルに記載されている Prometheus server のコマンドラインを変更する場合の例を、次に示します。下線部分の記載を追加します。

- 変更前

```
[program:prometheus]
command=/bin/sh -c '"/opt/jplima/bin/prometheus" --config.file="/opt/jplima/conf/jpc_prometheus_server.yml" --web.listen-address="0.0.0.0:20713" --web.read-timeout=5m --web.max-connections=10 --web.enable-lifecycle --storage.tsdb.path="/opt/jplima/data/prometheus_server/" --storage.tsdb.retention.time=1h --storage.tsdb.min-block-duration=1h --storage.tsdb.max-block-chunk-segment-size=32MB --storage.remote.flush-deadline=5s --rules.alert.for-outage-tolerance=1h --rules.alert.for-grace-period=10m --rules.alert.resend-delay=1m --alertmanager.notification-queue-capacity=10000 --log.level=debug --log.format=logfmt |& ( trap "" 15 && exec "/opt/jplima/bin/rotatelogs" -n 8 "/opt/jplima/logs/prometheus_server/prometheus_service" 10240K)'
directory=/opt/jplima/bin
autostart=true
stopasgroup=true
stopwaitsecs=180
```

- 変更後

```
[program:prometheus]
command=/bin/sh -c '"/opt/jplima/bin/osswrapper" "/opt/jplima/bin/prometheus" --config.file="/opt/jplima/conf/jpc_prometheus_server.yml" --web.listen-address="0.0.0.0:20713" --web.read-timeout=5m --web.max-connections=10 --web.enable-lifecycle --storage.tsdb.path="/opt/jplima/data/prometheus_server/" --storage.tsdb.retention.time=1h --storage.tsdb.min-block-duration=1h --storage.tsdb.max-block-chunk-segment-size=32MB --storage.remote.flush-deadline=5s --rules.alert.for-outage-tolerance=1h --rules.alert.for-grace-period=10m --rules.alert.resend-delay=1m --alertmanager.notification-queue-capacity=10000 --log.level=debug --log.format=logfmt |& ( trap "" 15 && exec "/opt/jplima/bin/rotatelogs" -n 8 "/opt/jplima/logs/prometheus_server/prometheus_service" 10240K)'
directory=/opt/jplima/bin
autostart=true
stopasgroup=true
stopwaitsecs=180
```

1.23 JP1/IM - Agent のオプション機能の構築 (Windows の場合)

1.23.1 OracleDB exporter の設定

ここでは、統合エージェントホストのオプション機能である OracleDB exporter の設定手順について説明します。

(1) OracleDB exporter の設定の前準備

OracleDB exporter の設定をする前準備について説明します。

(a) セットアップアーカイブファイルの入手

OracleDB exporter を使用するためのセットアップアーカイブファイルを取得します。セットアップアーカイブファイルは JP1/IM - Agent のインストール先フォルダに格納されています。

セットアップアーカイブファイルのファイル名は、次のとおりです。

JP1/IM - Agent のインストール先/jp1ima/options/

- oracledb_exporter_windows_VVRRSS.zip (Windows 版)
- oracledb_exporter_linux_VVRRSS.tar.gz (Linux 版)

(b) JP1/IM - Manager のセットアップ

JP1/IM - Manager 13-01 以降を新規にインストールした場合は、実施不要です。

JP1/IM - Manager 13-01 より前のバージョンからバージョンアップした場合、次の手順を実施します。

■ メトリック定義ファイルの配置

論理ホスト運用で、JP1/IM - Manager 13-01 より前のバージョンからバージョンアップした場合、次の手順を実施します。

1. 次を示す OracleDB exporter のメトリック定義ファイルをコピーし、コピー先の定義ファイル名にリネームする。

- Windows の場合
コピー元のファイル名：JP1/IM - Manager のインストール先
¥jp1imm¥conf¥imdd¥plugin¥jp1pccs¥metrics_oracledb_exporter.conf.model
コピー先のファイル名：JP1/IM - Manager のインストール先
¥jp1imm¥conf¥imdd¥plugin¥jp1pccs¥metrics_oracledb_exporter.conf
- Linux の場合
コピー元のファイル名：JP1/IM - Manager のインストール先/jp1imm/conf/imdd/plugin/jp1pccs/
metrics_oracledb_exporter.conf.model

コピー先のファイル名：JP1/IM - Manager のインストール先/jp1imm/conf/imdd/plugin/jp1pccs/metrics_oracledb_exporter.conf

Linux の場合は、パーミッションを「600」に設定します。

また、論理ホスト運用の場合、このファイルを次の場所に配置します。

- Windows の場合
共有フォルダ¥jp1imm¥conf¥imdd¥plugin¥jp1pccs¥
- Linux の場合
共有ディレクトリ/jp1imm/conf/imdd/plugin/jp1pccs/

■ IM マネージャー更新可能定義ファイルリスト定義ファイルの更新

論理ホスト運用で、JP1/IM - Manager 13-01 より前のバージョンからバージョンアップした場合、次の手順を実施します。

別のオプション機能のインストール手順で、最新のアーカイブファイルから取得した「imdd_product_deffile_list.json.update」で上書きしている場合、下記の手順は実施不要です。

1. 次を示す IM マネージャー更新可能定義ファイルリスト定義ファイルをコピーし、コピー先の定義ファイル名にリネームする。

- Windows の場合
コピー元のファイル名：JP1/IM - Manager のインストール先
¥jp1imm¥conf¥imdd¥system¥fileoperation¥imdd_product_deffile_list.json.update
コピー先のファイル名：JP1/IM - Manager のインストール先
¥jp1imm¥conf¥imdd¥system¥fileoperation¥imdd_product_deffile_list.json
- Linux の場合
コピー元のファイル名：JP1/IM - Manager のインストール先/jp1imm/conf/imdd/system/fileoperation/imdd_product_deffile_list.json.update
コピー先のファイル名：JP1/IM - Manager のインストール先/jp1imm/conf/imdd/system/fileoperation/imdd_product_deffile_list.json

また、論理ホスト運用の場合、このファイルを次の場所に配置します。

- Windows の場合
共有フォルダ¥jp1imm¥conf¥imdd¥system¥fileoperation¥
- Linux の場合
共有ディレクトリ/jp1imm/conf/imdd/system/fileoperation/

(c) JP1/IM - Agent のセットアップ

JP1/IM - Agent 13-01 以降を新規にインストールする場合は、実施不要です。

JP1/IM - Agent 13-01 より前のバージョンからバージョンアップした場合、次の手順を実施します。

■ JP1/IM - Agent の停止

JP1/IM - Agent のサービスを停止します。

- 物理ホストの場合

次のコマンドを実行して、JP1/IM - Agent のサービスを停止します。

```
jpc_service_stop -s all
```

- 論理ホストの場合

クラスタソフトから停止します。

■ OracleDB exporter のスクレイプジョブの設定

バージョンアップ時に Prometheus の設定ファイルのモデルファイルが更新されます。Prometheus 設定ファイルのモデルファイル (jpc_prometheus_server.yml.model) の次の内容を Prometheus 設定ファイル (jpc_prometheus_server.yml) の scrape_configs 配下に記載してください。

論理ホスト運用の場合は、次のファイルを更新します。

- Windows の場合

共有フォルダ¥jp1ima¥conf¥jpc_prometheus_server.yml

- Linux の場合

共有ディレクトリ/jp1ima/conf/jpc_prometheus_server.yml

```
(略)
:
scrape_configs:
  :
  - job_name: 'jpc_oracledb'
    scrape_interval: 60s
    scrape_timeout: 30s
    metrics_path: /metrics
    file_sd_configs:
      - files:
        - 'jpc_file_sd_config_oracledb.yml'
    relabel_configs:
      - source_labels: [__address__]
        target_label: instance
        regex: ([^:]+):([^.]+):(.*)
        replacement: ${1}:${2}
      - source_labels: [__address__]
        target_label: jp1_pc_node_label
        regex: ([^:]+):([^.]+):(.*)
        replacement: ${2}
      - source_labels: [__address__]
        target_label: __address__
        regex: ([^:]+):([^.]+):(.*)
        replacement: @@hostname@@※:${3}
    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'oracledb_sessions_value|oracledb_resource_current_utilization|oracledb_resou
```

```
rce_limit_value|oracledb_asm_diskgroup_total|oracledb_asm_diskgroup_free|oracledb_activity_e
xecute_count|oracledb_activity_parse_count_total|oracledb_activity_user_commits|oracledb_act
ivity_user_rollbacks|oracledb_activity_physical_reads_cache|oracledb_activity_consistent_get
s_from_cache|oracledb_activity_db_block_gets_from_cache|oracledb_process_count|oracledb_wait
_time_administrative|oracledb_wait_time_application|oracledb_wait_time_commit|oracledb_wait_t
ime_concurrency|oracledb_wait_time_configuration|oracledb_wait_time_network|oracledb_wait_t
ime_other|oracledb_wait_time_scheduler|oracledb_wait_time_system_io|oracledb_wait_time_user
_io|oracledb_tablespace_bytes|oracledb_tablespace_max_bytes|oracledb_tablespace_free|oracledb
_tablespace_used_percent|oracledb_exporter_last_scrape_duration_seconds|oracledb_exporter_la
st_scrape_error|oracledb_exporter_scrapes_total|oracledb_up'
action: 'keep'
```

注※

JP1/IM - Agent のホスト名（論理ホスト運用の場合は、論理ホスト名）を指定します。

■ OracleDB exporter のディスカバリ設定ファイルの配置

別のオプション機能のインストール手順で、最新のアーカイブファイルから取得した「jpc_product_deffile_list.json.update」で上書きしている場合、下記の手順は実施不要です。

1. 次を示す OracleDB exporter の監視対象を定義する定義ファイルのモデルファイルをコピーし、コピー先の定義ファイル名にリネームする。

- Windows の場合

コピー元のファイル名：JP1/IM - Agent のインストール先

¥jp1ima¥conf¥jpc_file_sd_config_oracledb.yml.model

コピー先のファイル名：JP1/IM - Agent のインストール先

¥jp1ima¥conf¥jpc_file_sd_config_oracledb.yml

- Linux の場合

コピー元のファイル名：JP1/IM - Agent のインストール先/jp1ima/conf/

jpc_file_sd_config_oracledb.yml.model

コピー先のファイル名：JP1/IM - Agent のインストール先/jp1ima/conf/

jpc_file_sd_config_oracledb.yml

Linux の場合は、パーミッションを「600」に設定します。

また、論理ホスト運用の場合、このファイルを次の場所に配置します。

- Windows の場合

共有フォルダ¥jp1ima¥conf¥

- Linux の場合

共有ディレクトリ/jp1ima/conf/

2. 手順 1. で作成した jpc_file_sd_config_oracledb.yml ファイルをテキストエディターで開き、次のように編集して上書き保存する。

```
- targets:
# - Oracleデータベースのホスト名:任意の名前:OracleDB exporterのポート番号
labels:
```

```
jp1_pc_exporter: JPC OracleDB exporter
jp1_pc_category: database
jp1_pc_trendname: oracledb_exporter
jp1_pc_remote_monitor_instance: @@hostname@@*:OracleDB collector(OracleDB exporter)
```

注※

JP1/IM - Agent のホスト名（論理ホスト運用の場合は、論理ホスト名）を指定します。

■ IM エージェント更新可能定義ファイルリスト定義ファイルの更新

IM エージェント更新可能定義ファイルリスト定義ファイルを更新する手順を次に示します。

別のオプション機能のインストール手順で、最新のアーカイブファイルから取得した「jpc_product_deffile_list.json.update」で上書きしている場合、下記の手順は実施不要です。

1. 次に示す IM エージェント更新可能定義ファイルリスト定義ファイルをコピーし、コピー先の定義ファイル名にリネームする。

- Windows の場合

コピー元のファイル名：JP1/IM - Agent のインストール先

¥jp1ima¥conf¥jpc_product_deffile_list.json.update

コピー先のファイル名：JP1/IM - Agent のインストール先

¥jp1ima¥conf¥jpc_product_deffile_list.json

- Linux の場合

コピー元のファイル名：JP1/IM - Agent のインストール先/jp1ima/conf/

jpc_product_deffile_list.json.update

コピー先のファイル名：JP1/IM - Agent のインストール先/jp1ima/conf/

jpc_product_deffile_list.json

また、論理ホスト運用の場合、このファイルを次の場所に配置します。

- Windows の場合

共有フォルダ¥jp1ima¥conf¥

- Linux の場合

共有ディレクトリ/jp1ima/conf/

■ 設定内容のチェック

Prometheus server の定義ファイルは、promtool コマンドで書式チェックができるため、チェックします。

promtool コマンドは、JP1/IM - Agent のインストール先/jp1ima/tools に格納されています。

```
promtool check config jpc_prometheus_server.yml
```

エラーが表示された場合は見直しを実施してください。

なお、次のような警告は表示されても問題はありません。

WARNING: file "../conf/jpc_file_sd_config_windows.yml" for file_sd in scrape job "jpc_windows" does not exist

■ JP1/IM - Agent の起動

JP1/IM - Agent のサービスを起動します。

- 物理ホストの場合

次のコマンドを実行して、JP1/IM - Agent のサービスを起動します。

```
jpc_service_start -s all
```

- 論理ホストの場合

クラスタソフトから起動します。

(2) OracleDB exporter のインストール

OracleDB exporter をインストールする手順について説明します。

(a) OracleDB exporter の配置

「1.23.1(1)(a) セットアップアーカイブファイルの入手」で入手したセットアップアーカイブファイル※を任意のフォルダに展開します。展開先フォルダに、JP1/IM - Manager や JP1/IM - Agent のインストール先フォルダを指定しないでください。

注※

- Windows の場合
oracledb_exporter_windows_VVRRSS.zip
- Linux の場合
oracledb_exporter_linux_VVRRSS.tar.gz

OracleDB exporter を論理ホストで運用する場合は、共有フォルダに配置してください。

(b) デフォルトのメトリック定義ファイルの作成

1. 次を示すデフォルトのメトリック定義ファイルのモデルファイルをコピーし、コピー先の定義ファイル名にリネームする。

- Windows の場合
コピー元のファイル名：OracleDB exporter の配置先
¥oracledb_exporter_windows¥jp1ima¥conf¥default-metrics.toml.model
コピー先のファイル名：OracleDB exporter の配置先
¥oracledb_exporter_windows¥jp1ima¥conf¥default-metrics.toml
- Linux の場合

コピー元のファイル名：OracleDB exporter の配置先/oracledb_exporter_linux/jp1ima/conf/default-metrics.toml.model

コピー先のファイル名：OracleDB exporter の配置先/oracledb_exporter_linux/jp1ima/conf/default-metrics.toml

(c) 監視対象の追加

監視対象追加の詳細については、「[1.23.1\(4\)\(a\) 監視対象を追加する（必須）](#)」を参照してください。

(3) OracleDB exporter のアンインストール

OracleDB exporter をアンインストールする手順について説明します。

(a) 監視対象の削除

OracleDB exporter をアンインストールする場合、監視対象をすべて削除したあと、OracleDB exporter を削除してください。監視対象削除の詳細については、「[1.23.1\(4\)\(d\) 監視対象を削除する（オプション）](#)」を参照してください。

(b) OracleDB exporter の削除

OracleDB exporter の削除は、「[1.23.1\(2\)\(a\) OracleDB exporter の配置](#)」で配置したフォルダを削除してください。

(4) OracleDB exporter の設定

OracleDB exporter の設定方法について説明します。

(a) 監視対象を追加する（必須）

■ 監視対象を追加するための準備

1. OracleDB exporter のインスタンス名を決める。

OracleDB exporter は監視対象ごとに起動する必要があります。複数の監視対象がある場合、複数の OracleDB exporter サービスを作成する必要があります。OracleDB exporter サービスを区別するための識別子を「インスタンス名」と呼びます。

- インスタンス名に使用できる文字は英数字だけです。
- インスタンス名の長さは 32 バイト以内です。

2. OracleDB exporter のリッスンポートを決める。

OracleDB exporter サービスがリッスンするポート番号を決めます。ほかのサービスやほかの OracleDB exporter サービスで使用していないポート番号にしてください。

3. 環境変数 JP1IMADIR に設定する値を確認する。

OracleDB exporter のサービス定義ファイル, または, ユニット定義ファイルに環境変数 JP1IMADIR を設定する必要があります。JP1/IM - Agent のホストの種類によって次の値となります。

- Windows の場合

ホスト種別	環境変数 JP1IMADIR
物理ホスト運用の場合	JP1/IM - Agent のインストール先¥jp1ima
論理ホスト運用の場合	共有フォルダ¥jp1ima

- Linux の場合

ホスト種別	環境変数 JP1IMADIR
物理ホスト運用の場合	/opt/jp1ima
論理ホスト運用の場合	共有ディレクトリ/jp1ima

4. 環境変数 DATA_SOURCE_NAME に設定する値を確認する。

OracleDB exporter のサービス定義ファイルに設定する環境変数 DATA_SOURCE_NAME には, 接続用ユーザーや接続先情報を設定する必要があります。

環境変数 DATA_SOURCE_NAME は, 次の書式で指定します。

- Windows の場合

```
oracle://ユーザー名@ホスト名:ポート/サービス名?connection timeout=10[&instance name=インスタンス名]
```

- Linux の場合

```
oracle://ユーザー名@ホスト名:ポート/サービス名?connection timeout=10 [&instance name=インスタンス名]
```

ユーザー名

Oracle Database への接続に使用するユーザーのユーザー名を指定します。

指定できる文字は, 英大文字, 数字, アンダースコア, ドル記号, シャープ記号, ピリオド, アットマークです。30 字以内で指定してください。

ホスト名

監視対象の OracleDB ホストのホスト名を指定します。

指定できる文字は, 英大文字, 英小文字, 数字, - (ハイフン), . (ピリオド) です。253 文字以内で指定してください。

ポート

Oracle リスナーに接続するためのポート番号を指定します。

サービス名

Oracle リスナーのサービス名を指定します。

使用できる文字, 英大文字, 英小文字, 数字, _ (アンダースコア), - (ハイフン), . (ピリオド) です。64 文字以内で指定してください。

オプション

接続オプションを指定します。複数のオプションがある場合は、Windows では「&」, Linux では「&」 でつなげて指定します。

- connection timeout=秒数

コネクションタイムアウトを秒数で指定します。このオプションの指定は必須です。

必ず 10 を指定してください。

10 以外の値を指定、およびこのオプションを指定しなかった場合は、Prometheus server のスクレイプがタイムアウトとなり、OracleDB exporter が稼働している場合でも up メトリックが 0 になる場合があります。

- instance name=インスタンス名

接続するインスタンス名を指定します。このオプションの指定は任意です。

ホスト名、ポート、サービス名は Oracle Database の `lsnrctl service` コマンドで確認できます。下記の例では、ホスト名は「ORAHOST」、ポートは「1521」、サービス名は「orcl.local」、インスタンス名は「orcl」となります。

```
$ lsnrctl service

LSNRCTL for 64-bit Windows: Version 19.0.0.0.0 - Production on 13-12月-2023 09:09:34

Copyright (c) 1991, 2019, Oracle. All rights reserved.

(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=ORAHOST)(PORT=1521)))に接続中
サービスのサマリー...
:
:
サービス"orcl.local"には、1件のインスタンスがあります。
  インスタンス"orcl"、状態READYには、このサービスに対する1件のハンドラがあります...
  ハンドラ:
    "DEDICATED" 確立:10674 拒否:1 状態:ready
    LOCAL SERVER
:
:
```

この場合、環境変数 `DATA_SOURCE_NAME` は、次のようになります。

- Windows の場合

```
oracle://ユーザー名@ORAHOST:1521/orcl.local?connection timeout=10&instance name=orcl
```

- Linux の場合

```
oracle://ユーザー名@ORAHOST:1521/orcl.local?connection timeout=10&instance name=orcl
```

5. インテリジェント統合管理基盤のツリーに表示される監視対象名を決める。

OracleDB exporter の監視対象はインテリジェント統合管理基盤のツリーに次のように表示されます。監視対象名には任意の名称を指定できるので適切な監視対象名を決めておいてください。

```
All Systems
+ Oracle Databaseホスト名
```

```
+ Database
+ 監視対象名 1
+ 監視対象名 2
```

使用できる文字および文字列の長さについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「OracleDB exporter のディスカバリ設定ファイル (jpc_file_sd_config_oracledb.yml)」(2. 定義ファイル) を参照してください。

6. 物理ホストで運用するか論理ホストで運用するか確認する。

新しく追加する OracleDB exporter をスクレイプする JP1/IM - Agent が物理ホスト運用の場合は、OracleDB exporter も物理ホスト運用となります。

新しく追加する OracleDB exporter をスクレイプする JP1/IM - Agent が論理ホスト運用の場合は、OracleDB exporter も論理ホスト運用となります。

7. 監視したいメトリックが取得できることを確認する。

データ取得用の SQL 文を接続に使用するユーザーで直接実行し、必要なメトリックが取得できるか確認することを推奨します。

監視したいメトリックが取得できない場合は、Oracle Database のサポートに問い合わせるようしてください。

■ OracleDB exporter の設定

1. Windows サービス化プログラムをコピーし、コピー先のプログラム名にリネームする。

コピー元のファイル名：OracleDB exporter の配置先

¥oracledb_exporter_windows¥jp1ima¥bin¥oracledb_exporter_@@instance@@_service.exe

コピー先のファイル名：

- 物理ホスト運用の場合

OracleDB exporter の配置先¥oracledb_exporter_windows¥jp1ima¥bin¥oracledb_exporter_インスタンス名*_service.exe

- 論理ホスト運用の場合

OracleDB exporter の配置先¥oracledb_exporter_windows¥jp1ima¥bin¥oracledb_exporter_インスタンス名*_論理ホスト名_service.exe

注※

インスタンス名は、「1.23.1(4)(a) 監視対象を追加する (必須)」の「■監視対象を追加するための準備」で決めた名称を指定します。

2. サービス定義ファイルを作成する。

コピー元のサービス定義ファイルをコピーし、コピー先のプログラム名にリネームします。

コピー元のファイル名：OracleDB exporter の配置先

¥oracledb_exporter_windows¥jp1ima¥bin¥oracledb_exporter_@@instance@@_service.xml.model

コピー先のファイル名：

- 物理ホスト運用の場合

OracleDB exporter の配置先¥oracledb_exporter_windows¥jp1ima¥bin¥oracledb_exporter_インスタンス名*_service.xml

- 論理ホスト運用の場合

OracleDB exporter の配置先¥oracledb_exporter_windows¥jp1ima¥bin¥oracledb_exporter_インスタンス名*_論理ホスト名_service.xml

注※

インスタンス名は、「1.23.1(4)(a) 監視対象を追加する（必須）」の「■監視対象を追加するための準備」で決めた名称を指定します。

3. サービス定義ファイルを更新する。

手順 2.で作成したサービス定義ファイルの次の値を変更します。

変更する値	指定する値
@@instance@@	• 物理ホスト運用の場合 「1.23.1(4)(a) 監視対象を追加する（必須）」の「■監視対象を追加するための準備」の手順 1.で決めた名称に置換する。 • 論理ホスト運用する場合 「1.23.1(4)(a) 監視対象を追加する（必須）」の「■監視対象を追加するための準備」の手順 1.で決めた名称「_論理ホスト名」を付与した値に置換する。
@@oracledb_exporter_installdir@@	OracleDB exporter の配置先に置換する。
@@autostart@@	• OS 起動時に自動起動させたい場合 "Automatic" • 自動起動させない場合 "Manual" 論理ホストの場合は"Manual"に置換する。
@@port@@	「1.23.1(4)(a) 監視対象を追加する（必須）」の「■監視対象を追加するための準備」の手順 2.で決めたポート番号に置換する。 論理ホストの場合は論理ホスト名も指定し、--web.listen-address="論理ホスト名:ポート番号"となるように置換する。
@@installdir2@@	「1.23.1(4)(a) 監視対象を追加する（必須）」の「■監視対象を追加するための準備」の手順 3.で確認したディレクトリに置換する。
@@data_source_name@@	「1.23.1(4)(a) 監視対象を追加する（必須）」の「■監視対象を追加するための準備」の手順 4.で確認した内容に置換する。

4. サービスを登録する。

手順 1.で作成したコマンドを次のように実行します。

- 物理ホスト運用の場合

oracledb_exporter_インスタンス名*_service.exe install

- 論理ホスト運用の場合

```
oracledb_exporter_インスタンス名*_論理ホスト名_service.exe install
```

論理ホスト運用の場合はクラスタを構成する両ノードで実行してください。

注※

インスタンス名は、「1.23.1(4)(a) 監視対象を追加する (必須)」の「■監視対象を追加するための準備」で決めた名称を指定します。

5. Oracle Database への接続に使用するユーザーのパスワードを登録する。

Oracle Database への接続に使用するユーザーのパスワードを jimasecret コマンドで登録します。

- 物理ホスト運用の場合

```
jimasecret -add -key OracleDB.user.ユーザー名 -s パスワード
```

- 論理ホスト運用の場合

```
jimasecret -add -key OracleDB.user.ユーザー名 -s パスワード -l 共有フォルダ
```

同一ユーザー名でパスワードが異なるユーザーを登録したい場合は、ホスト名とサービス名を含むキーを使用することができます。

jimasecret コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」(1. コマンド)を参照してください。

6. クラスタソフトにサービスを登録する。

クラスタ構成の場合は、クラスタソフトにサービスを登録します。

7. OracleDB exporter サービスを起動する。

コマンドラインまたは Windows サービスコントロールマネージャーから OracleDB exporter のサービスを起動します。

クラスタ構成の場合はクラスタソフトからサービスを起動します。

8. OracleDB exporter で性能情報が取得できることを確認する。

curl コマンドやブラウザで次の URL にアクセスし、性能情報が取得できているか確認してください。

```
http://ホスト名:ポート/metrics
```

ホスト名には OracleDB exporter を起動しているホスト、ポートには OracleDB exporter のリスポートを指定します。

■ Prometheus の設定

1. OracleDB exporter のディスカバリ設定ファイルに監視対象を追加する。

OracleDB exporter のディスカバリ設定ファイル (jpc_file_sd_config_oracledb.yml) の targets の下に新しいエントリーを追加します。

```
- targets:
# - Oracleデータベースのホスト名:任意の名前:OracleDB exporterのポート番号
- Oracle Databaseホスト名:監視対象名1:ポート番号1
- Oracle Databaseホスト名:監視対象名2:ポート番号2
- Oracle Databaseホスト名:監視対象名3:ポート番号3
```

- **Oracle Database**ホスト名:監視対象名4:ポート番号4

←ここに追加

labels:

jp1_pc_exporter: JPC OracleDB exporter

jp1_pc_category: database

jp1_pc_trendname: oracledb_exporter

jp1_pc_remote_monitor_instance: **インストール先のホスト名**:OracleDB metric collector(OracleDB exporter)

項目	指定する値
Oracle Database ホスト名	「1.23.1(4)(a) 監視対象を追加する (必須)」の「■監視対象を追加するための準備」の手順 4.で確認したホスト名を指定する。
監視対象名	「1.23.1(4)(a) 監視対象を追加する (必須)」の「■監視対象を追加するための準備」の手順 5.で決めた監視対象名を指定する。
ポート番号	「1.23.1(4)(a) 監視対象を追加する (必須)」の「■監視対象を追加するための準備」の手順 2.で決めたポート番号を指定する。

2. promtool コマンドで設定内容をチェックする。

設定内容が正しいことを確認します。

promtool コマンドは JP1/IM - Agent のインストール先/jp1ima/tools フォルダにあります。

```
promtool check config jpc_prometheus_server.yml
```

エラーが表示された場合は見直しを実施してください。

3. Prometheus を再起動する。

変更した内容を反映するために Prometheus を再起動します。

■ インテリジェント統合管理基盤の設定

1. すべてのサービスの起動が完了してから数分後にインテリジェント統合管理基盤のツリーの更新を実行する。

統合オペレーション・ビューアーからのツリー情報の生成もしくは反映、または、jddcreatetree コマンドもしくはjddupdatetree コマンドを実行してツリーを更新し、次の表示を確認します。

- ・ インテリジェント統合管理基盤のツリーに Oracle Database の監視対象が表示されていること
- ・ 監視対象を選択し、トレンド表示できること

(b) OracleDB exporter のポートを変更する (オプション)

OracleDB exporter のリッスンポートと Prometheus がスクレイプするポート番号を、変更する必要があります。

変更する手順を、次に示します。

1. Prometheus サービスを停止する。

2. OracleDB exporter サービスを停止する。

3. 次の表に示す定義ファイルの OracleDB exporter のリッスンポートを変更します。

- Windows の場合

ホスト種別	変更対象ファイル
物理ホスト運用の場合	OracleDB exporter の配置先 ¥oracledb_exporter_windows¥jp1ima¥bin¥oracledb_exporter_インスタンス名.xml
論理ホスト運用の場合	OracleDB exporter の配置先 ¥oracledb_exporter_windows¥jp1ima¥bin¥oracledb_exporter_インスタンス名_論理ホスト名.xml

- Linux の場合

ホスト種別	変更対象ファイル
物理ホスト運用の場合	/usr/lib/systemd/system/oracledb_exporter_インスタンス名.service
論理ホスト運用の場合	/usr/lib/systemd/system/oracledb_exporter_インスタンス名_論理ホスト名.service

4. Linux の場合、systemctl daemon-reload コマンドを実行する。

5. 次の表に示す定義ファイルの Prometheus がスクレイプする OracleDB exporter のポート番号を変更する。

- Windows の場合

ホスト種別	変更対象ファイル
物理ホスト運用の場合	JP1/IM - Manager のインストール先¥JP1IMM¥conf¥jpc_file_sd_config_oracledb.yml
論理ホスト運用の場合	共有フォルダ¥jp1imm¥conf¥jpc_file_sd_config_oracledb.yml

- Linux の場合

ホスト種別	変更対象ファイル
物理ホスト運用の場合	/opt/jp1ima/conf/jpc_file_sd_config_oracledb.yml
論理ホスト運用の場合	共有ディレクトリ/jp1ima/conf/jpc_file_sd_config_oracledb.yml

6. OracleDB exporter サービスを起動する。

7. Prometheus サービスを起動する。

(c) 接続のためのパスワードを変更する（オプション）

Oracle Database のパスワードを変更した場合、OracleDB exporter が接続に使用するパスワードを更新する必要があります。

1. OracleDB exporter を停止する。

2. パスワードを更新する。

Oracle Database への接続に使用するユーザーのパスワードを jimasecret コマンドで更新する。

- 物理ホスト運用の場合

```
jimasecret -add -key OracleDB.user.ユーザー名 -s パスワード
```

- 論理ホスト運用の場合

```
jimasecret -add -key OracleDB.user.ユーザー名 -s パスワード -l 共有フォルダ
```

同一ユーザー名でパスワードが異なるユーザーを登録したい場合は、ホスト名とサービス名を含むキーを使用することができます。

3. OracleDB exporter を起動する。

(d) 監視対象を削除する（オプション）

■ Prometheus の設定

1. OracleDB exporter のディスカバリ設定ファイル（jpc_file_sd_config_oracledb.yml）から監視対象を削除する。

OracleDB exporter のディスカバリ設定ファイル（jpc_file_sd_config_oracledb.yml）の targets に記載されている監視対象を削除します。

2. Prometheus を再起動する。

変更した内容を反映するために Prometheus を再起動します。

■ クラスタソフトから OracleDB exporter の削除

論理ホスト運用の場合、クラスタソフトから OracleDB exporter を削除します。必要に応じてサービスの停止なども実施してください。

■ OracleDB exporter の設定

1. 削除する監視対象の OracleDB exporter サービスを停止する。

コマンドラインまたは Windows サービスコントロールマネージャーから OracleDB exporter のサービスを停止します。

2. サービスの登録を解除する。

次のコマンドを実行してサービスの登録を解除してください。

- 物理ホスト運用の場合

```
oracledb_exporter_インスタンス名_service.exe uninstall
```

- 論理ホスト運用の場合

```
oracledb_exporter_インスタンス名_論理ホスト名_service.exe uninstall
```

論理ホスト運用の場合はクラスタを構成する両ノードで実行してください。

3. Oracle Database への接続に使用するユーザーのパスワードを削除する。

ほかの OracleDB exporter で同じユーザーを使用していない場合は、登録済みのパスワードを jimasecret コマンドで削除します。

- 物理ホスト運用の場合

```
jimasecret -rm -key OracleDB.user.ユーザー名
```

- 論理ホスト運用の場合

```
jimasecret -rm -key OracleDB.user.ユーザー名 -s パスワード -l 共有フォルダ
```

ホスト名やリスナー名を含むキーを指定して登録した場合は、そのキーを指定してください。

4. サービス定義ファイルと Windows サービス化プログラムを削除する。

OracleDB exporter の配置先¥oracledb_exporter_windows¥jp1ima¥bin フォルダに存在する次のファイルを削除してください。

- 物理ホスト運用の場合

```
oracledb_exporter_インスタンス名_service.xml
```

```
oracledb_exporter_インスタンス名_service.exe
```

- 論理ホスト運用の場合

```
oracledb_exporter_インスタンス名_論理ホスト名_service.xml
```

```
oracledb_exporter_インスタンス名_論理ホスト名_service.exe
```

(e) OracleDB exporter の死活監視を設定する（オプション）

OracleDB exporter サービスの死活監視は Prometheus server の up メトリックで監視できます。アラート定義で OracleDB exporter も監視する場合の例を次に示します。

```
groups:
- name: exporter_healthcheck
  rules:
  - alert: jp1_pc_exporter_healthcheck
    expr: up{jp1_pc_remote_monitor_instance=""} == 0 or label_replace(up{jp1_pc_exporter="JPC OracleDB exporter"}, "jp1_pc_nodelabel", "${1}", "jp1_pc_remote_monitor_instance", "^[:]*(:[:])*$") == 0 or label_replace(up{jp1_pc_remote_monitor_instance!="", jp1_pc_exporter!="JPC OracleDB exporter"}, "jp1_pc_nodelabel", "${1}", "jp1_pc_remote_monitor_instance", "^[:]*(:[:])*$") == 0
    for: 3m
    labels:
      jp1_pc_product_name: "/HITACHI/JP1/JPCS2"
      jp1_pc_component: "/HITACHI/JP1/JPCS/CONFINFO"
      jp1_pc_severity: "Error"
      jp1_pc_metricname: "up"
    annotations:
      jp1_pc_firing_description: "Exporterへの通信に失敗しました。instance={{ $labels.instance }}"
      jp1_pc_resolved_description: "Exporterへの通信に成功しました。instance={{ $labels.instance }}"
```

(f) 接続のためのユーザーを変更する（オプション）

1. Oracle Database に新しいユーザーを追加する。

2. OracleDB exporter を停止する。

3. 変更前のユーザーのパスワードを削除する。

Oracle Database への接続に使用するユーザーのパスワードを jimasecret コマンドで削除する。

- 物理ホスト運用の場合

```
jimasecret -rm -key OracleDB.user.旧ユーザー名
```

- 論理ホスト運用の場合

```
jimasecret -rm -key OracleDB.user.旧ユーザー名 -l 共有フォルダ
```

同一ユーザー名でパスワードが異なるユーザーを登録したい場合は、ホスト名とサービス名を含むキーを使用してください。

4. 変更後のユーザーのパスワードを登録する。

Oracle Database への接続に使用するユーザーのパスワードを jimasecret コマンドで登録します。

- 物理ホスト運用の場合

```
jimasecret -add -key OracleDB.user.新ユーザー名 -s パスワード
```

- 論理ホスト運用の場合

```
jimasecret -add -key OracleDB.user.新ユーザー名 -s パスワード -l 共有フォルダ
```

同一ユーザー名でパスワードが異なるユーザーを登録したい場合は、ホスト名とサービス名を含むキーを使用することができます。

5. 環境変数 DATA_SOURCE_NAME を修正する。

サービス定義ファイルをテキストエディターで開き、環境変数 DATA_SOURCE_NAME に記載されているユーザー名を新しいユーザー名に変更して保存します。

6. OracleDB exporter を起動する。

7. Oracle Database から変更前のユーザーを削除する。

変更前のユーザーが不要な場合、Oracle Database から変更前のユーザーを削除してください。

(5) クラスタ環境

OracleDB exporter をスケレイプする JP1/IM - Agent が論理ホスト運用の場合は、OracleDB exporter も論理ホスト運用とする必要があります。

1.23.2 Node exporter for AIX の設定

ここでは、統合エージェントホストのオプション機能である Node exporter for AIX の設定手順について説明します。

(1) Node exporter for AIX の設定の前準備

Node exporter for AIX の設定をする前準備について説明します。

(a) セットアップアーカイブファイルの入手

Node exporter for AIX を使用するためのセットアップアーカイブファイルを取得します。セットアップアーカイブファイルは JP1/IM - Agent のインストール先フォルダに格納されています。

セットアップアーカイブファイルのファイル名は、次のとおりです。

JP1/IM - Agent のインストール先/jp1ima/options/

- node_exporter_aix_VVRRSS.tar.Z (AIX 版)

(b) JP1/IM - Manager のセットアップ

JP1/IM - Manager 13-01 以降を新規にインストールした場合は、実施不要です。

JP1/IM - Manager 13-01 より前のバージョンからバージョンアップした場合、次の手順を実施します。

■ メトリック定義ファイルの配置

論理ホスト運用で、JP1/IM - Manager 13-01 より前のバージョンから 13-01 以降にバージョンアップした場合、次の手順を実施します。

1. 次を示す Node exporter for AIX のメトリック定義ファイルをコピーし、コピー先の定義ファイル名にリネームする。

バージョンアップ時に、メトリック定義ファイルのモデルファイルが生成されます。

- Windows の場合

コピー元のファイル名：JP1/IM - Manager のインストール先

¥jp1imm¥conf¥imdd¥plugin¥jp1pccs¥metrics_node_exporter_aix.conf.model

コピー先のファイル名：共有フォルダ

¥jp1imm¥conf¥imdd¥plugin¥jp1pccs¥metrics_node_exporter_aix.conf

- Linux の場合

コピー元のファイル名：JP1/IM - Manager のインストール先/jp1imm/conf/imdd/plugin/jp1pccs/metrics_node_exporter_aix.conf.model

コピー先のファイル名：共有ディレクトリ/jp1imm/conf/imdd/plugin/jp1pccs/metrics_node_exporter_aix.conf

Linux の場合は、パーミッションを「600」に設定します。

■ IM マネージャー更新可能定義ファイルリスト定義ファイルの更新

IM マネージャー更新可能定義ファイルリスト定義ファイルを更新する手順については、「[1.23.1\(1\)\(b\) JP1/IM - Manager のセットアップ](#)」の「**■IM マネージャー更新可能定義ファイルリスト定義ファイルの更新**」を参照してください。

(c) JP1/IM - Agent のセットアップ

JP1/IM - Manager 13-01 以降を新規にインストールした場合は、実施不要です。

JP1/IM - Manager 13-01 より前のバージョンからバージョンアップした場合、次の手順を実施します。

■ JP1/IM - Agent の停止

JP1/IM - Agent のサービスを停止します。

- 物理ホストの場合

次のコマンドを実行して、JP1/IM - Agent のサービスを停止します。

```
jpc_service_stop -s all
```

- 論理ホストの場合

クラスタソフトから停止します。

■ Node exporter for AIX のスクレイプジョブの設定

バージョンアップ時に Prometheus の設定ファイルのモデルファイルが更新されます。Prometheus 設定ファイルのモデルファイル (jpc_prometheus_server.yml.model) の次の内容を Prometheus 設定ファイル (jpc_prometheus_server.yml) の scrape_configs 配下に記載してください。

論理ホスト運用の場合は、次のファイルを更新します。

- Windows の場合

共有フォルダ¥jp1ima¥conf¥jpc_prometheus_server.yml

- Linux の場合

共有ディレクトリ/jp1ima/conf/jpc_prometheus_server.yml

```
(略)
:
scrape_configs:
:
- job_name: 'jpc_node_aix'

  file_sd_configs:
  - files:
    - 'jpc_file_sd_config_node_aix.yml'

  relabel_configs:
  - target_label: jp1_pc_nodelabel
    replacement: AIX metric collector(Node exporter for AIX)

  metric_relabel_configs:
  - source_labels: ['__name__']
    regex: 'node_context_switches|node_cpu|aix_diskpath_wblks|aix_diskpath_rblks|aix_disk_rserv|aix_disk_rblks|aix_disk_wserv|aix_disk_wblks|aix_disk_time|aix_disk_xrate|aix_disk_xfers|node_filesystem_avail_bytes|node_filesystem_files|node_filesystem_files_free|node_filesystem_free_bytes|node_filesystem_size_bytes|node_intr|node_load1|node_load5|node_load15|aix_memory_real_avail|aix_memory_real_free|aix_memory_real_inuse|aix_memory_real_total|aix_netin
```

```
terface_mtu|aix_netinterface_ibytes|aix_netinterface_ierrors|aix_netinterface_ipackets|aix_n  
etinterface_obytes|aix_netinterface_collisions|aix_netinterface_oerrors|aix_netinterface_opa  
ckets|aix_memory_pgspins|aix_memory_pgspouts'  
    action: 'keep'
```

■ Node exporter for AIX のディスカバリ設定ファイルの配置

1. 次を示す Node exporter for AIX のディスカバリ設定ファイルのモデルファイルをコピーし、コピー先の定義ファイル名にリネームする。

バージョンアップ時にディスカバリ設定ファイルのモデルファイルが生成されます。

- Windows の場合

コピー元のファイル名 : JP1/IM - Agent のインストール先

¥jp1ima¥conf¥jpc_file_sd_config_node_aix.yml.model

コピー先のファイル名 : JP1/IM - Agent のインストール先

¥jp1ima¥conf¥jpc_file_sd_config_node_aix.yml

- Linux の場合

コピー元のファイル名 : JP1/IM - Agent のインストール先/jp1ima/conf/

jpc_file_sd_config_node_aix.yml.model

コピー先のファイル名 : JP1/IM - Agent のインストール先/jp1ima/conf/

jpc_file_sd_config_node_aix.yml

Linux の場合は、パーミッションを「600」に設定します。

また、論理ホスト運用の場合、このファイルを次の場所に配置します。

- Windows の場合

共有フォルダ¥jp1ima¥conf¥

- Linux の場合

共有ディレクトリ/jp1ima/conf/

監視対象の設定を追加する場合は、「[1.23.2\(4\)\(a\) 監視対象を追加する \(必須\)](#)」を参照してください。

■ IM エージェント更新可能定義ファイルリスト定義ファイルの更新

IM エージェント更新可能定義ファイルリスト定義ファイルの更新については、「[1.23.1\(1\)\(c\) JP1/IM - Agent のセットアップ](#)」の「**■IM エージェント更新可能定義ファイルリスト定義ファイルの更新**」を参照してください。

■ 設定内容のチェック

設定内容のチェック手順については、「[1.23.1\(1\)\(c\) JP1/IM - Agent のセットアップ](#)」の「**■設定内容のチェック**」を参照してください。

■ JP1/IM - Agent の起動

JP1/IM - Agent の起動手順については、「[1.23.1\(1\)\(c\) JP1/IM - Agent のセットアップ](#)」の「**■JP1/IM - Agent の起動**」を参照してください。

(2) Node exporter for AIX のインストール

Node exporter for AIX をインストールする手順について説明します。

(a) Node exporter for AIX の配置

「[1.23.2\(1\)\(a\) セットアップアーカイブファイルの入手](#)」で入手したnode_exporter_aix_VVRRSS.tar.Zを監視対象ホスト（AIX）の任意のディレクトリに展開します。展開先ディレクトリに、JP1/IM - ManagerやJP1/IM - Agentのインストール先と同じディレクトリ構成を指定しないでください。

Node exporter for AIX を論理ホストで運用する場合は、共有ディレクトリに配置してください。

(b) システムログの出力設定

システムログを出力していない場合は設定します。

Node exporter for AIX のログは、OS のシステムログに出力されます。そのため、Node exporter for AIX のログ出力の設定は、OS のシステムログの設定に従います。OS のシステムログを出力する設定にしていない場合は、/etc/syslog.conf に設定を追加します。

追加する設定例を次に示します。

```
user.info /var/log/syslog.log rotate size 10m files 8
```

上記の設定を追加したあと、syslogd を再起動して設定を有効にします。

なお、ほかの製品などでuser を使用してシステムログに出力している場合は、そのログも出力されます。

(c) Node exporter for AIX のサービスの登録有効化

Node exporter for AIX のサービスの登録の有効化については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「[10.4.2\(1\) サービスの登録の有効化](#)」を参照してください。

(d) Node exporter for AIX のサービスの登録有効化確認

Node exporter for AIX のサービスの登録有効化確認については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「[10.4.2\(4\) サービスの状態の確認](#)」を参照してください。

(e) Node exporter for AIX の起動

Node exporter for AIX のサービスの起動については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「[10.4.2\(6\) サービスの起動](#)」を参照してください。

(f) 監視対象の追加

監視対象追加の詳細については、「[1.23.2\(4\)\(a\) 監視対象を追加する（必須）](#)」を参照してください。

(3) Node exporter for AIX のアンインストール

Node exporter for AIX をアンインストールする手順について説明します。

(a) 監視対象ホスト (AIX) の削除

1. 監視対象ホスト (AIX) を削除する。

Node exporter for AIX のディスカバリ設定ファイル (jpc_file_sd_config_node_aix.yml) の targets に記載されている監視対象ホスト (AIX) を削除します。

Node exporter for AIX のディスカバリ設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Node exporter for AIX のディスカバリ設定ファイル (jpc_file_sd_config_node_aix.yml)」(2. 定義ファイル) を参照してください。

監視対象ホスト (AIX) を複数削除する場合は、targets に記載されている監視対象ホスト (AIX) を複数削除し、Prometheus を再起動したあと、「[1.23.2\(3\)\(b\) Node exporter for AIX の停止](#)」以降を、削除した監視対象ホスト (AIX) に対してそれぞれ実施してください。

2. Prometheus を再起動する。

変更した内容を反映するために Prometheus を再起動します。

(b) Node exporter for AIX の停止

Node exporter for AIX のサービスの停止については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10.4.2(7) サービスの停止」を参照してください。

(c) Node exporter for AIX の自動起動の無効化

Node exporter for AIX の自動起動を有効化している場合、無効化する必要があります。

Node exporter for AIX の自動起動無効化については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10.4.2(10) 自動起動の無効化」を参照してください。

(d) Node exporter for AIX の自動停止の無効化

Node exporter for AIX の自動停止を有効化している場合、無効化する必要があります。

Node exporter for AIX の自動停止無効化については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10.4.2(12) 自動停止の無効化」を参照してください。

(e) Node exporter for AIX のサービスの登録の無効化

Node exporter for AIX のサービスの登録を有効化している場合、無効化する必要があります。

Node exporter for AIX のサービスの登録の無効化については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10.4.2(2) サービスの登録の無効化」を参照してください。

実施後に Node exporter for AIX のサービスの登録が無効化されたことを確認してください。

(f) Node exporter for AIX の削除

Node exporter for AIX の削除は、「1.23.2(2)(a) Node exporter for AIX の配置」で配置したディレクトリを削除してください。

(4) Node exporter for AIX の設定

(a) 監視対象を追加する（必須）

監視対象を追加する手順を次に示します。

■ Prometheus の設定

1. Node exporter for AIX のディスカバリ設定ファイルに監視対象を追加する。

Node exporter for AIX のディスカバリ設定ファイル (jpc_file_sd_config_node_aix.yml) の targets の下に新しいエントリーを追加します。

```
- targets:
- 監視対象ホスト名1:ポート番号1
- 監視対象ホスト名2:ポート番号2
- 監視対象ホスト名3:ポート番号3    ←ここに追加
  labels:
    jp1_pc_exporter: JPC Node exporter for AIX
    jp1_pc_category: platform
    jp1_pc_trendname: node_exporter_aix
```

項目	指定する値
監視対象ホスト名	監視対象ホスト（AIX）のホスト名を指定する。
ポート番号	Node exporter for AIX ポート番号を指定する。

2. promtool コマンドで設定内容をチェックする。

設定内容が正しいことを確認します。

promtool コマンドは JP1/IM - Agent のインストール先/jp1ima/tools フォルダにあります。

```
promtool check config jpc_prometheus_server.yml
```

エラーが表示された場合は見直しを実施してください。

3. Prometheus を再起動する。

変更した内容を反映するために Prometheus を再起動します。

■ インテリジェント統合管理基盤の設定

1. すべてのサービスの起動が完了してから数分後にインテリジェント統合管理基盤のツリーの更新を実行する。

統合オペレーション・ビューアーからのツリー情報の生成もしくは反映、または、jddcreatetree コマンドもしくはjddupdatetree コマンドを実行してツリーを更新し、次の表示を確認します。

- ・インテリジェント統合管理基盤のツリーに Node exporter for AIX のノードが表示されていること
- ・Node exporter for AIX のノードを選択し、トレンド表示できること

(b) Node exporter for AIX のポートを変更する（オプション）

Node exporter for AIX のリッスンポートと Prometheus がスクレイプするポート番号を、変更する必要があります。

変更する手順を、次に示します。

1. Prometheus サービスを停止する。
2. Node exporter for AIX サービスを停止する。
3. 次の表に示すサービスに登録している Node exporter for AIX のリッスンポートを変更します。

OS	ホスト種別	変更対象ファイル
AIX	物理ホスト運用の場合	サブシステム名が「jpc_node_exporter_aix」のサービス
	論理ホスト運用の場合	サブシステム名が「jpc_node_exporter_aix_論理ホスト名」のサービス

サービスの登録の変更については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10.4.2(3) サービスの登録の変更」を参照してください。

4. 次の表に示す定義ファイルの Prometheus がスクレイプする Node exporter for AIX のポート番号を変更する。

OS	ホスト種別	変更対象ファイル
Windows	物理ホスト運用の場合	JP1/IM - Agent のインストール先 ¥jp1ima¥conf¥jpc_file_sd_config_node_aix.yml
	論理ホスト運用の場合	JP1/IM - Agent の共有フォルダ ¥jp1ima¥conf¥jpc_file_sd_config_node_aix.yml
Linux	物理ホスト運用の場合	/opt/jp1ima/conf/jpc_file_sd_config_node_aix.yml
	論理ホスト運用の場合	JP1/IM - Agent の共有ディレクトリ/jp1ima/conf/ jpc_file_sd_config_node_aix.yml

5. Node exporter for AIX を起動する。
6. Prometheus サービスを起動する。
7. 手順 1～6 の設定を実施して、すべてのサービスの起動が完了してから数分待つ。
8. IM 管理ノードのツリーを更新する。

「1.19.3(1)(c)IM 管理ノードのツリー情報の作成と反映（Windows の場合）（必須）」の手順 2～5 を実施します。

(c) 収集するメトリックを変更する（オプション）

1. Prometheus 設定ファイル（jpc_prometheus_server.yml）にメトリックを追加する。

Prometheus 設定ファイル（jpc_prometheus_server.yml）の metric_relabel_configs に記載されているメトリックを変更します。

Prometheus 設定ファイルの編集方法については、「1.21.2(1)(a)設定ファイルを編集する（Windows の場合）」を参照してください。

なお、サポートしているメトリックは初期設定で収集する設定になっています。

```
- job_name: 'jpc_node_aix'
  :
  metric_relabel_configs:
    - source_labels: ['__name__']
      regex: 'node_context_switches|node_cpu|aix_diskpath_wblks|aix_diskpath_rblks|aix_
disk_rserv|aix_disk_rblks|aix_disk_wserv|aix_disk_wblks| . . . . . |aix_netinterface_o
packets|aix_memory_pgspins|aix_memory_pgspouts  【ここに追加】'
      action: 'keep'
```

2. メトリック定義ファイルにトレンド表示の定義

必要に応じて統合オペレーション・ビューアーのトレンド表示で表示するメトリックをメトリック定義ファイルに定義します。主要なメトリックは初期設定されています。

(d) Node exporter for AIX の死活監視を設定する（オプション）

Node exporter for AIX のプロセスは、Prometheus server の up メトリックで監視します。

Prometheus server の up メトリックによる監視の設定方法は、「1.21.2(18)(c) Prometheus server の up メトリックによる監視」を参照してください。

(e) 監視対象ホスト（AIX）上のプロセス監視（オプション）

Script exporter で次のスクリプトの結果を使って、監視対象ホスト(AIX)上のプロセスを監視します。

- ・ 監視対象ホスト（AIX）に SSH 接続し、監視対象ホスト（AIX）上で ps コマンドを実行するスクリプト

設定手順と具体的なスクリプトや定義ファイルの例を、次に示します。

次の例の場合、統合オペレーション・ビューアーのツリー形式で、AIX のホストノードの Platform カテゴリノード配下に、プロセス名のノードが作成され、「プロセスの状態」のメトリックだけがグラフ表示されます。「プロセスの状態」以外の Script exporter のメトリックは、Script exporter をインストールしているエージェントホストノードの Other Applications カテゴリノード配下の「監視対象ホスト名（AIX）：aix_process」ノードで、グラフ表示され、「プロセスの状態」のメトリックはグラフ表示されません。

1. Script exporter で実行するスクリプトを作成する。

監視対象ホスト（AIX）に SSH 接続し、監視対象ホスト（AIX）上でps コマンドを実行するスクリプトを作成します。

注

あらかじめ統合エージェントホストから監視対象ホスト（AIX）に SSH 接続できるように設定しておく必要があります。

また、次に示すスクリプトを実行するユーザーで SSH 接続できる必要があります。

Script exporter が動作する環境	スクリプトを実行するユーザー
Windows	Script exporter サービスを実行するユーザー（ローカルシステムアカウント）
Linux	root

- Windows 環境で Script exporter が動作する場合

次のバッチファイルとテキストファイルを作成します。

なお、SSH 接続には、PuTTY の Plink コマンドを使用しています。

■バッチファイル

```
@echo off
setlocal

rem 監視対象ホスト(AIX)上の監視するプロセス名（複数指定する場合は空白文字区切りで指定）
set PROCESS=node_exporter_aix logger

rem 監視対象ホスト(AIX)にssh接続するユーザー
set USER=user1

rem 監視対象ホスト(AIX)にssh接続する際に使用するPuTTY形式の秘密鍵ファイルパス
set PUTTY_ID_RSA="C:\tmp\ScriptExporter\id_rsa.ppk"

rem 監視対象ホスト(AIX)のホスト名
set AIX_HOST=aixhost1

rem psコマンドの結果出力先ファイル(任意の場所を指定)
set FILE1="C:\tmp\ScriptExporter\ps.txt"

rem Script exporterに読み込ませる内容を入力するファイル(任意の場所を指定)
set FILE2="C:\tmp\ScriptExporter\ps_for_exporter.txt"

rem plink.exeのファイルパスを指定
set PLINK_EXE="C:\Program Files\PuTTY\plink.exe"

rem (b)のテキストファイルパスを指定
set CMD_LIST="C:\tmp\ScriptExporter\command.txt"

rem plink.exeの標準エラー出力の出力先ファイル(任意の場所を指定)
set LOG_FILE="C:\tmp\ScriptExporter\ssh_log.txt"

echo enter | %PLINK_EXE% %USER%@%AIX_HOST% -i %PUTTY_ID_RSA% -m %CMD_LIST% > %FILE1% 2>%LOG_FILE%

rem Output metrics
(echo # HELP script_aix_process AIX process status.&echo # TYPE script_aix_process gauge
```

```

)> %FILE2%

for %%i in (%PROCESS%) do call:findpsinfo %%i

type %FILE2%
endlocal
exit /b

:findpsinfo
for /f "tokens=1-3* usebackq" %%i in (`findstr %1 %FILE1%`) do (
    set PNAME=%%1
    set STATE=%%2
    call:putinfo
    exit /b
)
set PNAME=%%1
set STATE=
call:putinfo
exit /b

:putinfo
if "%STATE%"=="A" (
    echo script_aix_process{host="%AIX_HOST%",process="%PNAME%",state="A"} 1 >> %FILE2%
) else (
    echo script_aix_process{host="%AIX_HOST%",process="%PNAME%",state="A"} 0 >> %FILE2%
)
exit /b

```

■ テキストファイル

```
/usr/bin/ps -A -X -o comm,st,etime
```

- Linux 環境で Script exporter が動作する場合

次のシェルスクリプトを作成します。

```

#!/bin/sh

# 監視対象ホスト(AIX)上の監視するプロセス名（複数指定する場合は空白文字区切りで指定）
PROCESS="node_exporter_aix" "logger")

# 監視対象ホスト(AIX)にssh接続する際に使用する秘密鍵ファイル
ID_RSA=/temp/script_exporter/id_rsa

# 監視対象ホスト(AIX)にssh接続するユーザー
USER=guest

# 監視対象ホスト(AIX)のホスト名
AIX_HOST=aixhsot1

# psコマンドの結果出力先ファイル(任意の場所を指定)
FILE1=/temp/script_exporter/ps.txt

#Script exporterに読み込ませる内容を出力するファイル(任意の場所を指定)
FILE2=/temp/script_exporter/ps_for_exporter.txt

# sshの標準エラー出力の出力先ファイル(任意の場所を指定)
LOG_FILE=/temp/script_exporter/ssh_log.txt

```

```

/usr/bin/ssh -i $ID_RSA $USER@$AIX_HOST /usr/bin/ps -A -X -o comm,st,etime >$FILE1 2>$LOG
_FILE

echo '# HELP script_aix_process AIX process status.'>$FILE2
echo '# TYPE script_aix_process gauge'>>$FILE2

for target in "${PROCESS[@]}"; do
    psinfo=`grep -m1 "$target" $FILE1`
    find_flag=$?
    if [ $find_flag = 0 ]; then
        psinfo=($psinfo)
        if [ "${psinfo[1]}" = "A" ]; then
            echo "script_aix_process{host=\"$AIX_HOST\",process=\"$target\",state=\"$A\"} 1">>$F
FILE2
        else
            echo "script_aix_process{host=\"$AIX_HOST\",process=\"$target\",state=\"$A\"} 0">>$F
FILE2
        fi
    else
        echo "script_aix_process{host=\"$AIX_HOST\",process=\"$target\",state=\"$A\"} 0">>$FIL
E2
    fi
done

cat $FILE2

```

2. Script exporter 設定ファイルと Prometheus 設定ファイルを編集する。

Script exporter 設定ファイルと Prometheus 設定ファイルを次のように編集します。設定ファイルの編集方法については、「[1.21.2\(1\)\(a\)設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

- Script exporter 設定ファイルの編集

次のように変更します。

```

scripts:
- name: 監視対象ホスト名 (AIX) : aix process
  command: 手順1で作成したスクリプトのファイルパス
  timeout:
    max timeout: 30
    enforced: true

```

- Prometheus 設定ファイルの編集

Script exporter の metric_relabel_configs を次のように変更します。

```

- job_name: 'jpc_script_exporter'
  :
  metric_relabel_configs:
    - source_labels: ['__name__']
      regex: 'script_success|script_duration_seconds|script_exit_code|script aix proces
s'
      action: 'keep'
    - source_labels: [jp1_pc_script]
      target_label: jp1_pc_nodelabel
    - source_labels: ['__name__']
      target_label: jp1_pc_category

```

```

    regex: 'script aix process'
    replacement: platform
  - source labels: [' name ', 'process']
    regex: 'script aix process.*;(.)'
    target label: jp1_pc_nodelabel
    replacement: ${1}
  - source labels: [' name ', 'host']
    regex: 'script aix process.*;(.)'
    target label: instance
    replacement: ${1}
  - regex: (jp1_pc_script|jp1_pc_multiple_node|jp1_pc_agent_create_flag)
    action: labeldrop

```

3. アラート設定ファイルを編集する。

監視対象プロセスが停止したときにアラートを発行するアラート定義の場合は、アラート設定ファイルを次のように編集します。

アラート設定ファイルの編集方法については、「[1.21.2\(1\)\(a\)設定ファイルを編集する（Windows の場合）](#)」を参照してください。

```

groups:
  - name: script_exporter
    rules:
      - alert: process_state(Script exporter)
        expr: script aix process{state="A"} == 0
        for: 3m
        labels:
          jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
          jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
          jp1_pc_severity: "Error"
          jp1_pc_eventid: "1404"
          jp1_pc_metricname: "script aix process"
        annotations:
          jp1_pc_firing_description: "プロセスの状態が実行中ではありません。"
          jp1_pc_resolved_description: "プロセスの状態が実行中になりました。"

```

4. IM 管理ノードのツリー情報の作成と反映を行う。

手順 1～3 の設定を実施して、すべてのサービスの起動が完了してから数分後に、「[1.19.3\(1\)\(c\)IM 管理ノードのツリー情報の作成と反映（Windows の場合）（必須）](#)」の手順 2～5 を実施します。

5. Script exporter のメトリック定義ファイルを編集する。

Script exporter のメトリック定義ファイルを次のように編集します。

Script exporter のメトリック定義ファイルの編集方法については、「[1.19.3\(1\)\(a\)共通の設定方法](#)」の「設定ファイルを編集する（Windows の場合）」を参照してください。

```

[
  :
  {
    "name": "script_exit_code",
    :
  }
  {
    "name": "script aix process",

```



```

    "default": true,
    "promql": "script aix process{state=~\"A~\"} and $jplim TrendData labels",
    "resource en": {
      "category": "script aix process",
      "label": "Process status",
      "description": "Status of processes on AIX hosts.",
      "unit": "-"
    },
    "resource ja": {
      "category": "script aix process",
      "label": "プロセスの状態",
      "description": "AIXホストのプロセスの状態。",
      "unit": "-"
    }
  }
}
]

```

上記の監視対象ホスト（AIX）は、次の OS とパッケージを適用している環境で動作確認しています。

- OS
AIX7.2 TL3 SP2
- パッケージ
openssh.base.client 7.5.102.1500
openssh.base.server 7.5.102.1500
openssh.man.en_US 7.5.102.1500
openssh.msg.en_US 7.5.102.1500

(f) Node exporter for AIX のログ出力先の変更（オプション）

Node exporter for AIX のログは、OS のシステムログに出力されます。Node exporter for AIX のログ出力先を変更する場合は、syslogd の設定と logger コマンドを使用します。

logger コマンドの -p に local1.info を指定して、システムログのログ出力先を /var/log/jpc_node_exporter_aix/jpc_node_exporter_aix.log に、ログサイズを 10MB、ログ面数を 8 面に変更する例を次に示します。※

注※

ほかの製品などで local1 を使用してシステムログに出力している場合は、そのログの出力先も変更されます。なお、jpc_stop_node_exporter_aix コマンドのログ出力先は変更されません。

1. /etc/syslog.conf に次を追加する。

```
local1.info /var/log/jpc_node_exporter_aix/jpc_node_exporter_aix.log rotate size 10m file
s 8
```

2. ログ出力先のディレクトリおよびファイルを作成する。

3. syslogd を再起動する。

4. Node exporter for AIX を停止する。

5. サービスの登録を変更する。

次のコマンドを実行してください。

- 物理ホスト運用の場合
`chssys -p /bin/sh -s jpc_node_exporter_aix -u root -S -f 9 -n 15 -a "-c ¥" "Node exporter for AIX の配置先/jplima/bin/node_exporter_aix" -CcADmdiabf -p 20730 2>&1 | logger -p local1.info¥"`
- 論理ホスト運用の場合
`chssys -p /bin/sh -s jpc_node_exporter_aix_論理ホスト名 -u root -S -f 9 -n 15 -a "-c ¥" "Node exporter for AIX の配置先/jplima/bin/node_exporter_aix" -CcADmdiabf -p 20730 2>&1 | logger -p local1.info¥"`

6. Node exporter for AIX を起動する。

1.23.3 SAP システム監視の設定

ここでは、統合エージェントホストのオプション機能である SAP システム監視機能のうち、SAP システムのログ抽出コマンドの設定手順について説明します。

SAP システムのログ抽出コマンド以外の、SAP システム監視機能の設定手順については、次のとおりです。

機能		設定手順
スクリプト実行機能（Script exporter）		この機能を使用する場合は、SAP システムのログ抽出コマンドのセットアップが完了したあとに、次の個所に記載している設定手順を実施します。 「1.21.2(3)(h) SAP システムのログ抽出コマンドを Script exporter を使用して実行する場合の設定（Windows の場合）（オプション）」 「1.21.2(12)(d) SAP システムのログ抽出コマンドを実行する場合の設定（オプション）」
SAP システムのログ抽出コマンド（jr3slget, jr3alget）		この項に記載している設定手順を実施します。
スクリプト実行結果監視機能		
	スクリプト実行結果監視機能（Fluentd）	この機能を使用する場合は、SAP システムのログ抽出コマンドのセットアップが完了したあとに、次の個所に記載している設定手順を実施します。 「1.21.2(9) Fluentd の設定」の「(j) SAP システムのログ情報を監視する（オプション）」～「(o) SAP システムの CCMS アラート情報の監視設定を削除する（オプション）」
	スクリプト実行結果監視機能（JP1/Base）	この機能を使用する場合は、マニュアル「JP1/Base 運用ガイド」の、JP1/Base のログファイルトラップに関する記載を参照してください。
メトリック送信機能		

機能	設定手順
メトリック送信機能 (Script exporter)	スクリプト実行機能 (Script exporter) の設定手順を実施することで使用できます。
メトリック送信機能 (Fluentd)	スクリプト実行機能 (Fluentd) の設定手順を実施することで使用できます。

(1) SAP システム監視の設定の前準備

SAP システム監視の設定をする前準備について説明します。

(a) セットアップアーカイブファイルの入手

SAP システム監視を使用するためのアーカイブファイルを取得します。アーカイブファイルは JP1/IM - Agent のインストール先フォルダに格納されています。

アーカイブファイルのファイル名は、次のとおりです。

JP1/IM - Agent のインストール先/jp1ima/options/

- sap_windows_VVRRSS.zip (Windows 版)
- sap_linux_VVRRSS.tar.gz (Linux 版)

(b) SAP システムのログ抽出コマンドのセットアップ

同梱する SAP のログ抽出コマンドは、JP1/PFM - Agent for EAP と JP1/IM - Agent が同居していない場合にだけ使用できます。JP1/PFM - Agent for EAP と JP1/IM - Agent が同居する環境での手順については、「[1.23.3\(1\)\(d\) JP1/IM - Agent と JP1/PFM - Agent for EAP が同居する環境での構築手順](#)」を参照してください。

■ SAP システムのログ抽出コマンドのインストール

- Windows の場合

1. コマンドが使用するレジストリを登録する。

コマンドプロンプトで次のコマンドを実行してください。

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hitachi\JP1PC\InstalledProduct" /v "JP1PCAGTM" /t "REG_SZ" /d "1200"
```

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hitachi\JP1PCAGTM\1200\PathName" /v "Path00※" /t "REG_SZ" /d "C:\Program Files (x86)\Hitachi\jp1pc"
```

注※

コマンドの配置先です。

2. 解凍後のagtm フォルダを配置する。

sap_windows_VVRRSS.zip を JP1/IM - Agent のインストール先フォルダ\jp1ima\options に展開すると、sap_windows フォルダが生成されます。

sap_windows¥command 配下にあるagtm フォルダをPath00 に設定したパスのフォルダ（コマンドの配置先）直下に配置します。手順 1 のコマンドを実行した場合は、次のパスに配置します。

C:¥Program Files (x86)¥Hitachi¥jp1pc

agtmフォルダの配置先パスが存在しない場合は、新しく配置先フォルダを作成してください。

- Linux の場合

1. 解凍後のagtm ディレクトリを配置する。

sap_linux_VVRRSS.tar.gz を JP1/IM - Agent のインストール先ディレクトリ/jp1ima/options/に展開すると、sap_linux ディレクトリが生成されます。

sap_linux/command 配下にあるagtm ディレクトリを、次のディレクトリ直下に配置します。

/opt/jp1pc/

agtm ディレクトリの配置先パスが存在しない場合は、次に示すオーナーと権限で、新しく配置先ディレクトリを作成してください。

オーナー：root

権限：755

■ RFC ライブラリの入手

RFC ライブラリの入手および配置手順については、JP1/IM - Agent のリリースノートもあわせて参照してください。

1. SAP NW RFC SDK 7.50 を SAP Software Download Center から入手する。

- Windows の場合

SAP NW RFC SDK 7.50（Windows on x64 64bit）（パッチレベル 0 以上）

- Linux の場合

SAP NW RFC SDK 7.50（Linux on 64bit）（パッチレベル 0 以上）

2. 入手した圧縮ファイルを SAP の手順に従って解凍する。

解凍したフォルダの構造は、次のとおりです。

```
nwrfcsdk
├─bin          : 実行可能なサンプルプログラム
├─demo         : サンプルプログラムのCソースファイル
├─include      : Cヘッダファイル
└─lib          : 共有ライブラリ
```

SAP のログ抽出コマンドの動作に必要なファイルはlib フォルダに格納されています。

3. 解凍した「lib」フォルダ配下の全てのファイルを、次のフォルダに格納する。

- Windows の場合

コマンドの配置先¥¥agtm¥lib¥rfc

注※：「■SAP システムの情報を取得するコマンドのインストール」で設定したコマンドの配置先

- Linux の場合

/opt/jp1pc/agtm/lib/rfc/

上記のパスにインストール先フォルダと同じ権限がない場合は、権限を付与してください。

■ CRT ライブラリの入手 (Windows の場合だけ)

RFC ライブラリの動作に必要な CRT ライブラリを入手し、適用します。必要な CRT ライブラリのバージョンについては、SAP ノート 2573790 で確認できます。

■ 環境パラメーター設定ファイルのセットアップ (オプション)

1. 環境パラメーター設定ファイルを作成する。

環境設定パラメーター設定ファイルのサンプルファイル (jr3slget.ini.sample, jr3alget.ini.sample) をコピーし、コピー先のファイル名を「任意の名前.ini」に変更して使用します。

環境設定パラメーター設定ファイルの配置先については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 A.4(3)統合エージェントホスト (Windows)」および「付録 A.4(4)統合エージェントホスト (Linux)」を参照してください。

環境設定パラメーター設定ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」(2. 定義ファイル) の「jr3slget コマンドの環境パラメーター設定ファイル (jr3slget.ini)」および「jr3alget コマンドの環境パラメーター設定ファイル (jr3alget.ini)」を参照してください。

環境設定パラメーター設定ファイルのサンプルファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」(2. 定義ファイル) の「jr3slget コマンドの環境パラメーター設定ファイルのサンプルファイル (jr3slget.ini.sample)」および「jr3alget コマンドの環境パラメーター設定ファイルのサンプルファイル (jr3alget.ini.sample)」を参照してください。

2. SAP システムのログ抽出コマンドの作業ディレクトリを作成する。

環境パラメーター設定ファイルを編集したあと、SAP システムのログ抽出コマンドの作業ディレクトリを作成します。環境パラメーター設定ファイルの WORKDIR ラベルに設定しているパスのディレクトリを作成してください。

なお、Linux の場合は、次に示すオーナーと権限で作成してください。

オーナー：root

権限：777

(c) SAP システムのログ抽出コマンドのアンインストール

1. スクリプト実行結果監視を停止する。

SAP システムのログ抽出コマンドのログデータを、スクリプト実行結果監視機能 (Fluentd または JP1/Base) を使用して監視している場合は、監視を停止します。

2. スクリプト実行を停止する。

SAP システム監視のスクリプト実行機能 (Script exporter) や cron を使用して、SAP システムのログ抽出コマンドを実行している場合は、コマンドの実行を停止します。

3. コマンドが使用していたレジストリを削除する (Windows の場合だけ)。

コマンドプロンプトで次のコマンドを実行します。

```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hitachi\JP1PC\InstalledProduct" /v "JP1PCAGTM"  
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hitachi\JP1PCAGTM\1200\PathName" /v "Path00"
```

4. SAP システムのログ抽出コマンドの作業ディレクトリを削除する。

「[1.23.3\(1\)\(b\)SAP システムのログ抽出コマンドのセットアップ](#)」の「環境パラメーター設定ファイルのセットアップ (オプション)」で、環境パラメーター設定ファイルの WORKDIR ラベルに設定しているパスのディレクトリを作成した場合は、作成したディレクトリを削除します。

5. SAP システムのログ抽出コマンドの配置先ディレクトリを削除する。

次のフォルダおよび配下のファイルを削除します。

- Windows の場合

コマンドの配置先※¥agtm

注※:「[1.23.3\(1\)\(b\)SAP システムのログ抽出コマンドのセットアップ](#)」の「SAP システムのログ抽出コマンドのインストール」で設定したコマンドの配置先

- Linux の場合

/opt/jp1pc/agtm

(d) JP1/IM - Agent と JP1/PFM - Agent for EAP が同居する環境での構築手順

■ JP1/PFM - Agent for EAP が導入済みの環境で JP1/IM - Agent を新規インストールする

JP1/IM - Agent と JP1/PFM - Agent for EAP が同居する環境では、JP1/IM - Agent に同梱する SAP のログ抽出コマンドは使用できません。

■ JP1/IM - Agent が導入済みの環境で JP1/PFM - Agent for EAP を新規インストールする

SAP システムのログ抽出コマンドがセットアップ済みの場合

JP1/IM - Agent に同梱する SAP のログ抽出コマンドは使用できないため、削除する必要があります。

1. JP1/IM - Agent に同梱する SAP システムのログ抽出コマンドと定義ファイルをバックアップする。

SAP システムの情報を取得するコマンドのインストールで指定した配置先フォルダおよび配下にあるファイルをコピーして、任意のフォルダにバックアップしてください。

2. SAP システムのログ抽出コマンドのアンインストールを実施する。

手順については、「[1.23.3\(1\)\(c\) SAP システムのログ抽出コマンドのアンインストール](#)」を参照してください。

3. JP1/PFM - Agent for EAP のインストールとセットアップを実施する。

SAP システムのログ抽出コマンドが未セットアップの場合

事前にしておくことはありません。

■ JP1/IM - Agent と JP1/PFM - Agent for EAP が同居する環境で JP1/PFM - Agent for EAP をバージョンアップインストールする

この環境では、JP1/IM - Agent に同梱する SAP のログ抽出コマンドは使用できないため、必要な手順はありません。

■ JP1/IM - Agent と JP1/PFM - Agent for EAP が同居する環境で JP1/IM - Agent をバージョンアップインストールする

この環境では、JP1/IM - Agent に同梱する SAP のログ抽出コマンドは使用できないため、必要な手順はありません。

■ JP1/IM - Agent と JP1/PFM - Agent for EAP が同居する環境から JP1/PFM - Agent for EAP をアンインストールする

JP1/PFM - Agent for EAP を運用中に作成した、jr3slget および jr3alget コマンドを使用するための環境パラメーター設定ファイルをバックアップしてください。

JP1/IM - Agent に同梱する SAP のログ抽出コマンドは使用する場合に、バックアップした JP1/PFM - Agent for EAP の環境パラメーター設定ファイルのパラメーターを参考値として参照できます。

■ JP1/IM - Agent と JP1/PFM - Agent for EAP が同居する環境から JP1/IM - Agent をアンインストールする

この環境では、JP1/IM - Agent に同梱する SAP のログ抽出コマンドは使用できないため、必要な手順はありません。

1.23.4 SQL exporter の設定

ここでは、統合エージェントホストのオプション機能である SQL exporter の設定手順について説明します。

(1) SQL exporter の設定の前準備

SQL exporter の設定をする前準備について説明します。

(a) JP1/IM - Manager のセットアップ

JP1/IM - Manager 13-11 以降を新規にインストールした場合は、実施不要です。

JP1/IM - Manager 13-11 より前のバージョンからバージョンアップした場合、次の手順を実施します。

(b) セットアップアーカイブファイルの入手

SQL exporter を使用するためのセットアップアーカイブファイルを取得します。セットアップアーカイブファイルは JP1/IM - Agent のインストール先フォルダに格納されています。

セットアップアーカイブファイルのファイル名は、次のとおりです。

JP1/IM - Agent のインストール先/jp1ima/options/

- sql_exporter_windows_VVRRSS.zip

■ メトリック定義ファイルの配置

論理ホスト運用で、JP1/IM - Manager 13-11 より前のバージョンからバージョンアップした場合、次の手順を実施します。

1. 次を示す SQL exporter のメトリック定義ファイルのモデルファイルをコピーし、コピー先の定義ファイル名にリネームする。

コピー元のファイル名：JP1/IM - Manager のインストール先

¥jp1imm¥conf¥imdd¥plugin¥jp1pccs¥metrics_sql_exporter.conf.model

コピー先のファイル名：JP1/IM - Manager のインストール先

¥jp1imm¥conf¥imdd¥plugin¥jp1pccs¥metrics_sql_exporter.conf

また、論理ホスト運用の場合、このファイルを次の場所に配置します。

共有フォルダ¥jp1imm¥conf¥imdd¥plugin¥jp1pccs¥

(c) JP1/IM - Agent のセットアップ

JP1/IM - Agent 13-11 以降を新規にインストールする場合は、実施不要です。

JP1/IM - Agent 13-11 より前のバージョンからバージョンアップした場合、次の手順を実施します。

なお、JP1/IM - Agent のホストに Microsoft SQL Server のモジュールをインストールする必要はありません。

■ JP1/IM - Agent の停止

JP1/IM - Agent のサービスを停止します。

- 物理ホストの場合

次のコマンドを実行して、JP1/IM - Agent のサービスを停止します。

```
jpc_service_stop -s all
```

- 論理ホストの場合

クラスタソフトから停止します。

■ SQL exporter のスクレイプジョブの設定

バージョンアップ時に Prometheus の設定ファイルのモデルファイルが更新されます。Prometheus 設定ファイルのモデルファイル (jpc_prometheus_server.yml.model) の次の内容を Prometheus 設定ファイル (jpc_prometheus_server.yml) の scrape_configs 配下に記載してください。

論理ホスト運用の場合は、次のファイルを更新します。

```

(略)
:
scrape_configs:
  :
  - job_name: 'jpc_sql'
    scrape_interval: 60s
    scrape_timeout: 30s

    metrics_path: /metrics

    file_sd_configs:
      - files:
        - 'jpc_file_sd_config_mssql.yml'

    relabel_configs:
      - target_label: jp1_pc_nodelabel
        replacement: MSSQL metric collector(SQL exporter)

    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'mssql_local_time_seconds|mssql_connections|mssql_deadlocks|mssql_user_errors|mssql_kill_connection_errors|mssql_page_life_expectancy_seconds|mssql_batch_requests|mssql_log_growths|mssql_buffer_cache_hit_ratio|mssql_checkpoint_pages_sec|mssql_io_stall_seconds|mssql_io_stall_total_seconds|mssql_resident_memory_bytes|mssql_virtual_memory_bytes|mssql_memory_utilization_percentage|mssql_page_fault_count|mssql_os_memory|mssql_os_page_file|mssql_database_detail_process_count|mssql_global_server_summary_perc_busy|mssql_global_server_summary_packet_errors|mssql_server_detail_blocked_processes|mssql_server_overview_cache_hit|mssql_transaction_log_overview_log_space_used'
        action: 'keep'
      - source_labels: [exported_job]
        target_label: instance
        replacement: ${1}
      - source_labels: [target]
        target_label: jp1_pc_nodelabel
        replacement: ${1}

```

■ SQL exporter のディスカバリ設定ファイルの配置

1. 次に示す SQL exporter の監視対象を定義する定義ファイルのモデルファイルをコピーし、コピー先の定義ファイル名にリネームする。

コピー元のファイル名：JP1/IM - Agent のインストール先

¥jp1ima¥conf¥jpc_file_sd_config_mssql.yml.model

コピー先のファイル名：JP1/IM - Agent のインストール先

¥jp1ima¥conf¥jpc_file_sd_config_mssql.yml

また、論理ホスト運用の場合、このファイルを次の場所に配置します。

共有フォルダ¥jp1ima¥conf¥

2. 手順 1. で作成した jpc_file_sd_config_mssql.yml ファイルをテキストエディターで開き、次のように編集して上書き保存する。

```
- targets:
# - @@hostname@@※:SQL exporterのポート番号
labels:
  jp1_pc_exporter: JPC SQL exporter
  jp1_pc_category: database
  jp1_pc_trendname: sql_exporter
  jp1_pc_remote_monitor_instance: @@hostname@@:MSSQL metric collector(SQL exporter)
  jp1_pc_multiple_node: "{__name__=~'mssql_.*'}"
```

注※

JP1/IM - Agent のホスト名（論理ホスト運用の場合は、論理ホスト名）を指定します。

■ 設定内容のチェック

Prometheus server の定義ファイルは、promtool コマンドで書式チェックができるため、チェックします。

promtool コマンドは、JP1/IM - Agent のインストール先¥jplima¥tools に格納されています。

```
promtool check config jpc_prometheus_server.yml
```

エラーが表示された場合は見直しを実施してください。

なお、次のような警告は表示されても問題はありません。

```
WARNING: file "../conf/jpc_file_sd_config_windows.yml" for file_sd in scrape job "jpc_windows" does not exist
```

■ JP1/IM - Agent の起動

JP1/IM - Agent のサービスを起動します。

- 物理ホストの場合

次のコマンドを実行して、JP1/IM - Agent のサービスを起動します。

```
jpc_service_start -s all
```

- 論理ホストの場合

クラスタソフトから起動します。

(2) SQL exporter のインストール

SQL exporter をインストールする手順について説明します。

(a) インストールの前準備

1. 環境変数 JP1IMADIR に設定する値を確認する。

SQL exporter のサービス定義ファイルに環境変数 JP1IMADIR を設定する必要があります。JP1/IM - Agent のホストの種類によって次の値となります。

ホスト種別	環境変数 JP1IMADIR
物理ホスト運用の場合	JP1/IM - Agent のインストール先¥jp1ima
論理ホスト運用の場合	共有フォルダ¥jp1ima

2. 物理ホストで運用するか論理ホストで運用するか確認する。

新しく追加する SQL exporter をスクレイプする JP1/IM - Agent が物理ホスト運用の場合は、SQL exporter も物理ホスト運用となります。

新しく追加する SQL exporter をスクレイプする JP1/IM - Agent が論理ホスト運用の場合は、SQL exporter も論理ホスト運用となります。

(b) SQL exporter のインストール

1. SQL exporter を配置する。

「[1.23.4\(1\)\(b\) セットアップアーカイブファイルの入手](#)」で入手したセットアップアーカイブファイル※を任意のフォルダに展開します。展開先フォルダに、JP1/IM - Manager や JP1/IM - Agent のインストール先フォルダを指定しないでください。

注※

sql_exporter_windows_VVRRSS.zip

SQL exporter を論理ホストで運用する場合は、共有フォルダに配置してください。

2. デフォルトのメトリック定義ファイルを作成する。

次に示すデフォルトのメトリック定義ファイルのモデルファイルをコピーし、コピー先の定義ファイル名にリネームする。

コピー元のファイル名：SQL exporter の配置先

¥sql_exporter_windows¥jp1ima¥conf¥mssql_standard.collector.yml.model

コピー先のファイル名：SQL exporter の配置先

¥sql_exporter_windows¥jp1ima¥conf¥mssql_standard.collector.yml

3. サービス定義ファイルを更新する。

次のファイルが存在することを確認する。

SQL exporter の配置先¥sql_exporter_windows¥jp1ima¥bin¥sql_exporter_service.exe

SQL exporter の配置先¥sql_exporter_windows¥jp1ima¥bin¥sql_exporter_service.xml.model

サービス定義ファイルの次の値を変更します。

変更する値	指定する値
@@sql_exporter_installdir@@	SQL exporter の配置先に置換する。
@@autostart@@	- OS 起動時に自動起動させたい場合 "Automatic"に置換する。 - 自動起動させない場合 "Manual"に置換する。

変更する値	指定する値
	論理ホストの場合は"Manual"に置換する。

4. サービスを登録する。

次のコマンドを実行して、SQL exporter サービスを Windows に登録します。

- 物理ホスト運用の場合

```
sql_exporter_service.exe install
```

- 論理ホスト運用の場合

```
sql_exporter_論理ホスト名_service.exe install
```

論理ホスト運用の場合はクラスタを構成する両ノードで実行してください。

5. SQL exporter 設定ファイルに監視対象を設定する。

SQL exporter の監視対象を、SQL exporter 設定ファイル (jpc_sql_exporter.yml) に記載します。

SQL exporter 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「SQL exporter 設定ファイル (jpc_sql_exporter.yml)」(2. 定義ファイル) を参照してください。

6. 監視対象を追加する。

監視対象の追加の詳細については、「[1.23.4\(4\)\(a\) 監視対象を追加する \(必須\)](#)」を参照してください。

7. クラスタソフトにサービスを登録する。

クラスタ構成の場合は、クラスタソフトにサービスを登録します。

(c) Prometheus の設定

1. SQL exporter のディスカバリ設定ファイルに監視対象を設定する。

SQL exporter の監視対象を SQL exporter のディスカバリ設定ファイル (jpc_file_sd_config_mssql.yml) の targets に記載します。

SQL exporter のディスカバリ設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「SQL exporter のディスカバリ設定ファイル (jpc_file_sd_config_mssql.yml)」(2. 定義ファイル) を参照してください。

2. promtool コマンドで設定内容をチェックする。

設定内容が正しいことを確認します。

promtool コマンドは JP1/IM - Agent のインストール先¥jplima¥tools フォルダにあります。

```
promtool check config jpc_prometheus_server.yml
```

エラーが表示された場合は見直しを実施してください。

なお、次のような警告は表示されても問題はありません。

```
WARNING: file "../conf/jpc_file_sd_config_windows.yml" for file_sd in scrape job "jpc_windows" does not exist
```

3. Prometheus を再起動する。

変更した内容を反映するために Prometheus を再起動します。

(3) SQL exporter のアンインストール

1. SQL exporter を削除する。

SQL exporter の削除は、「1.23.4(2)(b) SQL exporter のインストール」で配置したフォルダを削除してください。

(4) SQL exporter の設定

SQL exporter の設定方法について説明します。

(a) 監視対象を追加する (必須)

■ 監視対象を追加するための準備

1. SQL exporter 設定ファイルに監視対象を設定する。

SQL exporter の監視対象を、SQL exporter 設定ファイル (jpc_sql_exporter.yml) に記載します。

SQL exporter 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「SQL exporter 設定ファイル (jpc_sql_exporter.yml)」(2. 定義ファイル) を参照してください。

2. 監視に使用する Microsoft SQL Server のユーザーに必要な権限が割り当てられているか確認する。

必要な権限については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(1)(q)SQL exporter (Microsoft SQL Server 監視機能)」に記載している「Microsoft SQL Server を監視するための前提条件」を参照してください。

■ SQL exporter の設定

1. SQL exporter のサービスを停止する。

2. Microsoft SQL Server への接続に使用するユーザーのパスワードを登録する。

Microsoft SQL Server への接続に使用するユーザーのパスワードを jimasecret コマンドで登録します。

- 物理ホスト運用の場合

```
jimasecret -add -key MSSQL.ホスト名.インスタンス名.ユーザー名 -s パスワード
```

- 論理ホスト運用の場合

```
jimasecret -add -key MSSQL.ホスト名.インスタンス名.ユーザー名 -s パスワード -l 共有フォルダ
```

jimasecret コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」(1. コマンド) を参照してください。

3. SQL exporter サービスを起動する。

Windows 管理ツールのサービス画面などから、SQL exporter のサービスを起動します。
クラスタ構成の場合はクラスタソフトからサービスを起動します。

4. SQL exporter で性能情報が取得できることを確認する。

curl コマンドやブラウザで次の URL にアクセスし、性能情報が取得できているか確認してください。

```
http://ホスト名:20735/metrics
```

ホスト名には SQL exporter を起動しているホストを指定します。

■ インテリジェント統合管理基盤の設定

1. すべてのサービスの起動が完了してから数分後にインテリジェント統合管理基盤のツリーの更新を実行する。

統合オペレーション・ビューアーからのツリー情報の生成もしくは反映、または、jddcreatetree コマンドもしくはjddupdatetree コマンドを実行してツリーを更新し、次の表示を確認します。

- インテリジェント統合管理基盤のツリーに Microsoft SQL Server の監視対象が表示されていること
- 監視対象を選択し、トレンド表示できること

(b) 接続のためのパスワードを変更する（オプション）

運用中に Microsoft SQL Server のパスワードを変更した場合、SQL exporter が接続に使用するパスワードを更新する必要があります。

1. SQL exporter を停止する。

2. パスワードを更新する。

Microsoft SQL Server への接続に使用するユーザーのパスワードを jimasecret コマンドで更新します。

- 物理ホスト運用の場合
`jimasecret -add -key MSSQL.ホスト名.インスタンス名.ユーザー名 -s パスワード`
- 論理ホスト運用の場合
`jimasecret -add -key MSSQL.ホスト名.インスタンス名.ユーザー名 -s パスワード -l 共有フォルダ`

jimasecret コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」(1. コマンド)を参照してください。

3. SQL exporter を起動する。

(c) 監視対象を削除する（オプション）

■ SQL exporter の設定

<一部の監視対象を削除する場合>

1. SQL exporter を停止する。

2. パスワードを削除する。

Microsoft SQL Server への接続に使用するユーザーのパスワードを jimasecret コマンドで削除する。

- 物理ホスト運用の場合

```
jimasecret -rm -key MSSQL.ホスト名.インスタンス名.ユーザー名
```

- 論理ホスト運用の場合

```
jimasecret -rm -key MSSQL.ホスト名.インスタンス名.ユーザー名 -l 共有フォルダ
```

jimasecret コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」(1. コマンド) を参照してください。

3. SQL exporter 設定ファイルから監視対象の接続情報を削除する。

SQL exporter の監視対象の接続情報を、SQL exporter 設定ファイル (jpc_sql_exporter.yml) から削除します。

SQL exporter 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「SQL exporter 設定ファイル (jpc_sql_exporter.yml)」(2. 定義ファイル) を参照してください。

4. SQL exporter を起動する。

<すべての監視対象を削除する場合>

1. SQL exporter を停止する。

2. サービスの登録を解除する。

次のコマンドを実行してサービスの登録を解除してください。

- 物理ホスト運用の場合

```
sql_exporter_service.exe uninstall
```

- 論理ホスト運用の場合

```
sql_exporter_論理ホスト名_service.exe uninstall
```

論理ホスト運用の場合はクラスタを構成する両ノードで実行する必要がある。

3. Microsoft SQL Server への接続に使用するユーザーのパスワードを削除する。

- 物理ホスト運用の場合

```
jimasecret -rm -key MSSQL.ホスト名.インスタンス名.ユーザー名
```

- 論理ホスト運用の場合

```
jimasecret -rm -key MSSQL.ホスト名.インスタンス名.ユーザー名 -l 共有フォルダ
```

jimasecret コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」(1. コマンド) を参照してください。

複数の Microsoft SQL Server ユーザーのパスワードを登録している場合は、すべてのユーザーに対し同様の操作を行ってください。

(d) SQL exporter の死活監視を設定する (オプション)

SQL exporter サービスの死活監視は Prometheus server の up メトリックで監視できます。アラート定義で SQL exporter も監視する場合の例を次に示します。

```
groups:
- name: exporter_healthcheck
  rules:
- alert: jp1_pc_exporter_healthcheck
  expr: up{jp1_pc_remote_monitor_instance=""} == 0 or label_replace(up{jp1_pc_exporter="JPC SQL exporter"}, "jp1_pc_nodelabel", "${1}", "jp1_pc_remote_monitor_instance", "~^[^:]*:(~^[^:]*)$") == 0 or label_replace(up{jp1_pc_remote_monitor_instance!="", jp1_pc_exporter!="JPC SQL exporter"}, "jp1_pc_nodelabel", "${1}", "jp1_pc_remote_monitor_instance", "~^[^:]*:(~^[^:]*)$") == 0
  for: 3m
  labels:
    jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
    jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
    jp1_pc_severity: "Error"
    jp1_pc_metricname: "up"
  annotations:
    jp1_pc_firing_description: "Exporterへの通信に失敗しました。instance={{ $labels.instance }}"
    jp1_pc_resolved_description: "Exporterへの通信に成功しました。instance={{ $labels.instance }}"
```

(e) 接続のためのユーザーを変更する (オプション)

1. Microsoft SQL Server に新しいユーザーを追加する。

新しい監視用ユーザーが必要かつ未登録の場合だけ、この手順を実行してください。

2. SQL exporter を停止する。

3. 変更前のユーザーのパスワードを削除する。

Microsoft SQL Server への接続に使用していたユーザーのパスワードを jimasecret コマンドで削除します。

- 物理ホスト運用の場合

```
jimasecret -rm -key MSSQL,ホスト名,インスタンス名,旧ユーザー名
```

- 論理ホスト運用の場合

```
jimasecret -rm -key MSSQL.ホスト名.インスタンス名.旧ユーザー名 -l 共有フォルダ
```

jimasecret コマンドの詳細については、マニュアル「JPI/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」（1. コマンド）を参照してください。

4. 変更後のユーザーのパスワードを登録する。

Microsoft SQL Server への接続に使用するユーザーのパスワードを jimasecret コマンドで登録します。

- 物理ホスト運用の場合

```
jimasecret -add -key MSSQL.ホスト名,インスタンス名,新ユーザー名 -s パスワード
```

- 論理ホスト運用の場合

```
jimasecret -add -key MSSQL.ホスト名.インスタンス名.新ユーザー名 -s パスワード -l 共有フォルダ
```

jimasecret コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimasecret」(1. コマンド)を参照してください。

5. SQL exporter 設定ファイルに記載している接続情報のユーザー名を変更する。

SQL exporter の接続情報のユーザー名を、SQL exporter 設定ファイル (jpc_sql_exporter.yml) から削除します。

SQL exporter 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「SQL exporter 設定ファイル (jpc_sql_exporter.yml)」(2. 定義ファイル)を参照してください。

6. SQL exporter を起動する。

7. Microsoft SQL Server から変更前のユーザーを削除する。

変更前のユーザーが不要な場合、Microsoft SQL Server から変更前のユーザーを削除してください。

(5) SQL exporter の構築に関するトラブルシューティング

■SQL exporter の設定が完了したあと、メトリクスの値が取得できない場合

「1.23.4(4)(a) 監視対象を追加する (必須)」の手順を実施したあと、メトリクスの値が取得できない場合の確認内容と対象方法を、次に示します。

確認内容	対処方法	参照先
監視対象の Microsoft SQL Server のサービスとインスタンスが起動しているか。	監視対象の Microsoft SQL Server サービスとインスタンスを起動する。	なし
監視対象の Microsoft SQL Server への接続に使用するユーザーの権限は正しく設定されているか。	接続に使用するユーザーに正しい権限を付与する。	マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(1)(q)SQL exporter (Microsoft SQL Server 監視機能)」の「Microsoft SQL Server を監視するための前提条件」
監視対象の Microsoft SQL Server への接続に使用するユーザーのパスワードが登録済みか。	接続に使用するユーザーのパスワードを登録する。	なし
SQL exporter の配置先 ¥sql_exporter_windows¥jplima¥logs フォルダにエラーログが出力されていないか。エラーログが出力されている場合は、参照先の説明に対処方法が記載されていないか。	参照先に記載されている対処方法を実施する。	マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「12.5.1(14) sql_exporter のログ」

(6) クラスタ環境

SQL exporter をスクレイプする JP1/IM - Agent が論理ホスト運用の場合は、SQL exporter も論理ホスト運用とする必要があります。

1.24 マニュアルの組み込み手順 (Windows の場合)

所定のフォルダに HTML マニュアルを格納することで、各画面の [ヘルプ] ボタンからマニュアルを参照できます。

HTML マニュアルの組み込み手順を次に示します。

1. プログラムプロダクトに標準添付されているマニュアル提供媒体を用意する。
2. マニュアル提供媒体に格納されている対象データを JP1/IM - Manager および JP1/IM - View に格納する。

マニュアル提供媒体の格納先フォルダ配下に格納されているすべての対象データを、マニュアルごとに JP1/IM - Manager および JP1/IM - View の格納先フォルダに格納してください。

すべてのマニュアルを正しく配置することで、マニュアルの目次ページを表示できるようになります。データを誤って配置している状態や一部のデータだけを配置している状態で [ヘルプ] - [目次] を選択すると、エラーダイアログボックス (KAVB8550-E) が表示されます。

- 格納されている対象データ (HTML マニュアル)
CSS ファイル, HTM ファイル, GRAPHICS フォルダ
- マニュアル提供媒体側の格納先 (Windows マシンのドライブにマニュアル提供媒体をセットした場合)
「該当するドライブ¥MAN¥3021」配下に資料番号フォルダ単位でマニュアルが格納されています。ここに格納されているマニュアルがどの製品に対応するかを確認する場合は、資料番号フォルダ配下の INDEX.HTM を参照してください。
- JP1/IM - Manager 側の格納先
「インストール先フォルダ¥JP1Cons¥www¥manual¥ja」配下
「インストール先フォルダ¥JP1IMM¥public¥manual¥ja」配下
各資料番号のフォルダに、マニュアル提供媒体の資料番号フォルダ配下に格納されているすべての対象データを格納してください。
- JP1/IM - View 側の格納先
統合管理 基本ガイド (マニュアル提供媒体側の格納先¥ja¥03L0100D)
インストール先フォルダ¥JP1CoView¥manual¥ja¥03L0100D
JP1/IM3 - Manager 導入・設計ガイド (マニュアル提供媒体側の格納先¥ja¥03L0200D)
インストール先フォルダ¥JP1CoView¥manual¥ja¥03L0200D
JP1/IM3 - Manager 構築ガイド (マニュアル提供媒体側の格納先¥ja¥03L0300D)
インストール先フォルダ¥JP1CoView¥manual¥ja¥03L0300D
JP1/IM3 - Manager 運用ガイド (マニュアル提供媒体側の格納先¥ja¥03L0400D)
インストール先フォルダ¥JP1CoView¥manual¥ja¥03L0400D
JP1/IM3 - Manager 画面リファレンス (マニュアル提供媒体側の格納先¥ja¥03L0500D)
インストール先フォルダ¥JP1CoView¥manual¥ja¥03L0500D

JP1/IM3 - Manager コマンド・定義ファイル・API リファレンス（マニュアル提供媒体側の格納先¥ja¥03L0600D）

インストール先フォルダ¥JP1CoView¥manual¥ja¥03L0600D

JP1/IM3 - Manager メッセージ（マニュアル提供媒体側の格納先¥ja¥03L0700D）

インストール先フォルダ¥JP1CoView¥manual¥ja¥03L0700D

マニュアル提供媒体の資料番号フォルダ名と、格納先の資料番号フォルダ名の一部が異なる場合は、マニュアル提供媒体の資料番号フォルダを配置したあと、格納先の資料番号フォルダ名にリネームしてください。

すでに HTML マニュアルが JP1/IM - Manager および JP1/IM - View の格納先フォルダに格納されている場合は、格納されている HTML マニュアルを削除してから格納してください。

1.25 アンインストール (Windows の場合)

ここでは、JP1/IM - Manager, JP1/IM - View, および JP1/IM - Agent をアンインストールする手順について説明します。なお、アンインストール作業を行うユーザーは、Administrators 権限が必要です。

1.25.1 アンインストール手順 (Windows の場合)

JP1/IM - Manager, JP1/IM - View, および JP1/IM - Agent をアンインストールする手順について説明します。なお、IM データベース (統合監視 DB および IM 構成管理 DB) およびインテリジェント統合管理データベースを使用している場合は、JP1/IM - Manager をアンインストールする前に IM データベースおよびインテリジェント統合管理データベースを削除する必要があります。

(1) インテリジェント統合管理データベースの削除の手順

環境を再構築するためにインテリジェント統合管理データベースを削除する場合は、事前にバックアップを取得してください。バックアップの方法については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「1.2 データベースの管理」を参照してください。

次の手順でインテリジェント統合管理データベースを削除します。

1. JP1/IM - Manager を停止する。

JP1/IM - Manager を停止してください。

2. インテリジェント統合管理データベースを削除する。

次のコマンドを実行してください。

- 物理ホスト運用の場合

```
jimgndbunsetup [-q]
```

- 論理ホスト運用で実行系ホストの場合

```
jimgndbunsetup -h 論理ホスト名 -c online [-q]
```

- 論理ホスト運用で待機系ホストの場合

```
jimgndbunsetup -h 論理ホスト名 -c standby [-q]
```

3. マシンを再起動する。

(2) IM データベースの削除の手順

環境を再構築するために IM データベースを削除する場合は、事前にバックアップを取得してください。バックアップの方法については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「1.2 データベースの管理」を参照してください。

各コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「1. コマンド」を参照してください。

次の手順で IM データベースを削除します。

1. JP1/IM - Manager を停止する。

JP1/IM - Manager を停止してください。JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスも停止してください。

2. 統合監視 DB または IM 構成管理 DB を削除する場合、次のサービスの状態を確認する。

- 物理ホストの場合
IM データベースサービス (JP1/IM3-Manager DB Server) が開始している。
- 物理ホストの場合に、統合監視 DB または IM 構成管理 DB がセットアップ済み、かつ IM データベースを使用しているとき
JP1/IM - Manager のサービス (JP1/IM3-Manager) が停止している。
- 論理ホストの場合
論理ホストの IM データベースサービス (JP1/IM3-Manager DB Server_論理ホスト名) が開始している。
- 論理ホストの場合に、統合監視 DB または IM 構成管理 DB がセットアップ済み、かつ IM データベースを使用しているとき
JP1/IM - Manager のサービス (JP1/IM3-Manager_論理ホスト名) が停止している。

3. 統合監視 DB を削除する場合、jcoimdef コマンドを実行する。

```
jcoimdef -db OFF
```

統合監視 DB が無効になります。

4. 統合監視 DB を削除する場合、jcodbunsetup コマンドを実行する。

```
jcodbunsetup
```

統合監視 DB が削除されます。

5. IM 構成管理 DB を削除する場合、jcoimdef コマンドを実行する。

```
jcoimdef -cf OFF
```

IM 構成管理サービス (jcfmain) が無効になります。

6. IM 構成管理 DB を削除する場合、jcfdbunsetup コマンドを実行する。

```
jcfdbunsetup
```

IM 構成管理 DB が削除されます。

7. 次の物理ホストのファイルおよびフォルダを削除する。

Manager パス¥data¥imcf¥imconfig 以下のファイル

Manager パス¥data¥imcf¥profiles 以下のファイルおよびフォルダ

8. マシンを再起動する。

(3) JP1/IM - Manager のアンインストールの手順

次の手順でアンインストールします。

なお、JP1/IM - Manager をアンインストールすると、JP1/IM - Agent を利用するための統合エージェント管理基盤もアンインストールされます。

1. プログラムを終了する。

アンインストールする前に、すべてのプログラムを終了してください。

「JP1/IM3-Manager サービス」のサービスを停止してください。また、アンインストールする JP1/IM - Manager に接続中の JP1/IM - View がある場合はログアウトしてください。

2. Windows の [サービス] ダイアログボックスを閉じる。

Windows の [サービス] ダイアログボックスを表示している場合は、製品のアンインストール前に閉じてください。

3. Windows の [コントロールパネル] - [プログラム] - [プログラムのアンインストール] ※から、アンインストールしたい製品を選択する。

起動したインストーラの指示に従ってアンインストールを進めてください。

アンインストール時には、入力項目はありません。

注※ コントロールパネルをクラシック表示にしている場合は、[コントロールパネル] - [プログラムと機能] となります。

4. 再起動を要求された場合は、Windows を再起動する。

5. ユーザーファイルを削除する。

アンインストールでは、インストール後に作成された定義ファイルやログファイル、ユーザーが修正する可能性のあるファイルは削除されません。これらのファイルを削除する場合は、JP1/IM - Manager をインストールしていたフォルダを、エクスプローラにより削除してください。

(4) JP1/IM - View のアンインストールの手順

次の手順でアンインストールします。

1. プログラムを終了する。

アンインストールする前に、すべてのプログラムを終了してください。

2. Windows の [サービス] ダイアログボックスを閉じる。

Windows の [サービス] ダイアログボックスを表示している場合は、製品のアンインストール前に閉じてください。

3. Windows の [コントロールパネル] - [プログラム] - [プログラムのアンインストール] ※から、アンインストールしたい製品を選択する。
- 起動したインストーラーの指示に従ってアンインストールを進めてください。
- アンインストール時には、入力項目はありません。
- 注※ コントロールパネルをクラシック表示にしている場合は、[コントロールパネル] - [プログラムと機能] となります。

4. 再起動を要求された場合は、Windows を再起動する。

5. ユーザーファイルを削除する。

アンインストールでは、インストール後に作成された定義ファイルやログファイル、ユーザーが修正する可能性のあるファイルは削除されません。これらのファイルを削除する場合は、JP1/IM - View をインストールしていたフォルダを、エクスプローラにより削除してください。

(5) JP1/IM - Agent のアンインストールの手順

次の手順でアンインストールします。

1. JP1/IM - Agent のサービスを停止する。

2. 複数マネージャーホストへのデータ配信機能を使用している場合は、サービス削除の前に次の手順を実施する。

「[1.21.2\(2\)\(j\) 複数マネージャーホストへのデータ配信機能を解除する \(Windows の場合\) \(オプション\)](#)」に記載している「JP1/IM - Agent 自体のアンインストールを行う場合」を実施します。

3. JP1/IM - Agent のサービス削除を実行する。

サービスの削除方法については、「[1.21.1\(1\)\(b\) アドオンプログラムの無効化](#)」を参照してください。

4. Windows のコントロールパネルの [プログラムと機能] 画面を表示し、JP1/IM - Agent を削除する。

5. 削除が完了したら、統合マネージャーの統合オペレーション・ビューアーにログインし、削除したホストの統合エージェント情報を手動で削除する。

統合エージェント情報の削除手順については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「[2.2.1 \[統合エージェント一覧\] 画面](#)」を参照してください。

6. ユーザーファイルを削除する。

アンインストールでは、インストール後に作成された定義ファイルやログファイル、ユーザーが修正する可能性のあるファイルは削除されません。これらのファイルを削除する場合は、JP1/IM - Agent をインストールしていたフォルダを、エクスプローラにより削除してください。

❗ 重要

論理ホストのサービスを起動している場合は、サービスを停止したのち論理ホストのサービスを削除してから実行してください。論理ホストのサービス起動中にアンインストールを実行す

ると、論理ホストのサービスで使用するファイルが削除され、サービスが異常終了する可能性があります。論理ホストのサービスを削除せずアンインストールを実行した場合は、アンインストール後に論理ホストのサービスを削除してください。

1.25.2 アンインストール時の注意事項（Windows の場合）

(1) 統合トレース機能（HNTRLib2）について

JP1/IM - View のアンインストール時に、統合トレース機能（HNTRLib2）はほかの製品が使用していないければ削除されます。

(2) Windows 環境への設定

インストール時に追加したシステム環境変数 Path の値は、アンインストール時に削除されます。ただし、統合トレース機能（HNTRLib2）を使用している製品がほかにある場合、HNTRLib2 のパス（システムドライブ:¥Program Files¥Common Files¥Hitachi※）は削除されません。

注※ Windows の場合、「システムドライブ:¥Program Files」と表記している部分は、インストール時の OS 環境変数によって決定されるため、環境によって異なる場合があります。

(3) JP1/IM - Manager, JP1/IM - View, および JP1/IM - Agent のアンインストールについて

- JP1/IM - Manager および JP1/IM - View をアンインストールした場合、スタートメニューにプログラムフォルダが残るときがあります。不要な場合はスタートメニューで Windows のヘルプを参照して削除方法を確認の上、削除してください。
- JP1/IM - Manager をアンインストールすると、監視オブジェクト DB およびホスト情報 DB は削除されます。
- JP1/IM - Manager および JP1/IM - View をアンインストールした後に再インストールする場合、アンインストール後に必ず OS を再起動してください。OS を再起動したあと、JP1/IM - Manager および JP1/IM - View をインストールしていたフォルダをエクスプローラから削除してから、再インストールしてください。
- JP1/IM - View を使用中にアンインストールした場合、ダイアログが表示されます。この場合は [キャンセル] ボタンをクリックし、いったんアンインストールを中断したあと、起動中の JP1/IM - View をすべて停止してから、再度 JP1/IM - View をアンインストールしてください。

(4) JP1/Base のアンインストールについて

JP1/Base をアンインストールすると、JP1/IM - Manager および JP1/IM - View の定義情報も削除されます。JP1/Base を再インストールしても、JP1/IM - Manager および JP1/IM - View は動作しません。

このような場合は、JP1/IM - Manager および JP1/IM - View をアンインストールしてから、JP1/IM - Manager および JP1/IM - View を再インストールする必要があります。

(5) 物理ホストで IM データベースを手動アンインストールする手順について

物理ホストで IM データベースを手動でアンインストールする場合、次の手順で行なってください。

1. Administrators 権限のあるユーザーでログオンする。
2. JP1/IM - Manager のサービス (JP1/IM3-Manager) が稼働している場合、停止する。
3. IM データベースのサービス (JP1/IM3-Manager DB Server) が稼働している場合、停止する。
4. 次のフォルダが存在する場合は削除する。

セットアップ情報ファイルの IMDBENVDIR の値¥JM0

セットアップ情報ファイルの IMDBDIR の値¥imdb

5. レジストリエディターで次のレジストリを選択し、[InstallGuid]※2 の値を確認する。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Hitachi¥HiRDBEmbeddedEdition_JM0¥{英数字列}※1
```

注※1 {英数字列}の例 08042Y

注※2 [InstallGuid]の値の例 BAB5F425-3C8F-4CD5-9117-DA371EAD50DF

6. 次のレジストリが存在する場合は、レジストリエディターを使用して削除する。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Hitachi¥HiRDBEmbeddedEdition_JM0※1
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥{英数字列}※1※2
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥HiRDBEmbeddedEdition_JM0
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥HiRDBCusterService_JM0
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥Application¥JP1/IM-M_DB_Server
```

注※1 Windows が 32bit 環境の場合は、HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥HITACHI¥を HKEY_LOCAL_MACHINE¥SOFTWARE¥HITACHI¥に読み替えてください。

注※2 {英数字列}が手順 5 で確認した[InstallGuid]の値と等しいことを確認して削除してください。

7. 次を示すフォルダ (隠しフォルダ) が存在する場合は削除する。

```
OSドライブ:¥Program Files(x86)¥
InstallShield Installation Information¥{英数字列}※1
```

注※1 {英数字列}が手順 5 で確認した[InstallGuid]の値と等しいことを確認して削除してください。

8. 次の手順で IM データベースの設定ファイルを更新する。

- Manager パス¥conf¥imdb¥system¥dbconf¥JM0 を削除する。
- Manager パス¥conf¥imdb¥system¥dbconf¥jimdbsetuplist.conf をテキストエディターで開き、次のように編集してJP1_DEFAULT を削除し、上書き保存する。
(編集前) _JM0=JP1_DEFAULT

(編集後) _JM0=

9. OS を再起動してください。レジストリエディターの値とメモリ上の値の同期を取るため、必ず実施してください。

(6) クラスタシステムで IM データベースを手動アンインストールする手順について

クラスタシステムで IM データベースを手動でアンインストールする場合、次に示す手順で行なってください。

1. 実行系ホストに Administrators 権限のあるユーザーでログオンする。
2. 実行系ホストで JP1/IM - Manager のサービス (JP1/IM3-Manager_論理ホスト) が稼働している場合、停止する。
3. 実行系ホストで次の IM データベースのサービスが稼働している場合、停止する。

JP1/IM3-Manager DB Server_論理ホスト名

JP1/IM3-Manager DB Cluster Service_論理ホスト名

4. 実行系ホストに次のフォルダが存在する場合、削除する。

クラスタセットアップ情報ファイルの IMDBENVDIR の値¥JMn※1

クラスタセットアップ情報ファイルの IMDBDIR の値¥imdb

クラスタセットアップ情報ファイルの SHAREDDBDIR の値¥imdb

注※1 n はクラスタセットアップ情報ファイルの LOGICALHOSTNUMBER の値

5. レジストリエディターを使用して次のレジストリを選択し、[InstallGuid]※2 の値を確認する。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Hitachi¥HiRDBEmbeddedEdition_JMn¥{英数字列}※1※2

注※1 {英数字列}の例 08042Y

注※2 [InstallGuid]の値の例 BAB5F425-3C8F-4CD5-9117-DA371EAD50DF

6. 実行系ホストに次のレジストリが存在する場合は、レジストリエディターを使用して削除する。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Hitachi¥HiRDBEmbeddedEdition_JMn※1
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥{英数字列}※1※2
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥HiRDBEmbeddedEdition_JMn
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥HiRDBClusterService_JMn
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥Application¥HiRDBEmbeddedEdition_JMn
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥Application¥JP1/IM-M_DB_Server_論理ホスト名

注※1 Windows が 32bit 環境の場合は、HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥HITACHI¥を HKEY_LOCAL_MACHINE¥SOFTWARE¥HITACHI¥に読み替えてください。

注※2 {英数字列}が手順 5 で確認した[InstallGuid]の値と等しいこと確認して削除してください。

7. 実行系ホストに次のフォルダ (隠しフォルダ) が存在する場合は、削除する。

OSドライブ:¥Program Files(x86)¥InstallShield Installation Information¥{英数字列}※1

注※1 {英数字列}が手順 5 で確認した[InstallGuid]の値と等しいことを確認して削除してください。

8. 実行系ホストで IM データベースの設定ファイルを、次の手順で更新する。

- Manager パス¥conf¥imdb¥system¥dbconf¥JMn※を削除する。
- Manager パス¥conf¥imdb¥system¥dbconf¥jimdbsetuplist.conf をテキストエディターで開き、n+1 行目を次のように編集して論理ホスト名を削除し、上書き保存する。

注※ n はクラスタセットアップ情報ファイルのLOGICALHOSTNUMBER の値

(編集前) jimdbsetuplist.conf n+1 行目

_JMn=論理ホスト名

(編集後) jimdbsetuplist.conf n+1 行目

_JMn=

9. 実行系ホストで OS を再起動する。

レジストリエディターの値とメモリ上の値の同期を取るため、必ず実施してください。

10. 待機系ホストに Administrators 権限のあるユーザーでログオンする。

11. 待機系ホストで JP1/IM - Manager のサービス (JP1_IM3-Manager_論理ホスト名) が稼働している場合、停止する。

12. 待機系ホストで IM データベースのサービスが稼働している場合、停止する。

- JP1/IM3-Manager DB Server_論理ホスト名
- JP1/IM3-Manager DB Cluster Service_論理ホスト名

13. 待機系ホストに次のフォルダが存在する場合、削除する。

クラスタセットアップ情報ファイルの IMDBENVDIR の値¥_JMn※

クラスタセットアップ情報ファイルの IMDBDIR の値¥imdb

クラスタセットアップ情報ファイルの SHAREDDBDIR の値¥imdb

注※1 n はクラスタセットアップ情報ファイルのLOGICALHOSTNUMBER の値

14. 待機系ホストに次のレジストリが存在する場合は、レジストリエディターを使用して削除する。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Hitachi¥HiRDBEmbeddedEdition_JMn※1
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥{英数字列}※1※2
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥HiRDBEmbeddedEdition_JMn
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥HiRDBClusterService_JMn
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥Application¥HiRDBEmbeddedEdition_JMn
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥Application¥JP1/IM-M_DB_Server_論理ホスト名
```

注※1 Windows が 32bit 環境の場合は、HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥HITACHI¥を HKEY_LOCAL_MACHINE¥SOFTWARE¥HITACHI¥に読み替えてください。

注※2 {英数字列}が手順 5 で確認した[InstallGuid]の値と等しいことを確認して削除してください。

15. 待機系ホストに次のフォルダ（隠しフォルダ）が存在する場合は、削除する。

OS ドライブ：¥Program Files(x86)¥InstallShield Installation Information¥{英数字列}※

注※ {英数字列}が手順 5 で確認した[InstallGuid]の値と等しいことを確認して削除してください。

16. 待機系ホストで次の手順で IM データベースの設定ファイルを更新する。

- Manager パス¥conf¥imdb¥system¥dbconf¥JM<n>※¹ を削除する。
- Manager パス¥conf¥imdb¥system¥dbconf¥jimdbsetuplist.conf をテキストエディターで開き、n+1 行目を次のように編集して論理ホスト名を削除し、上書き保存する。

注※ n はクラスタセットアップ情報ファイルのLOGICALHOSTNUMBER の値

（編集前） jimdbsetuplist.conf n+1 行目

_JMn=論理ホスト名

（編集後） jimdbsetuplist.conf n+1 行目

_JMn=

17. 待機系ホストで OS を再起動する。

レジストリエディタの値とメモリ上の値の同期を取るため、必ず実施してください。

1.26 インストールとセットアップの注意事項 (Windows の場合)

❗ 重要

Linux 8 以降でコンテナ環境を作成する場合は Docker を Podman に読み替えてください。

- JP1/IM は、ServerConductor/DeploymentManager および JP1/ServerConductor/Deployment Manager のディスク複製インストール、仮想化プラットフォームが提供するイメージファイル化を使用することで、統合エージェントホストの複製ができます。次の仮想化プラットフォームに対応しています。

- VMware ESX
- Hyper-V
- SCVMM
- Amazon EC2

上記以外の未対応の仮想プラットフォームでは、複製を実施する前に、JP1/IM をアンインストールし、ディスク複製インストールまたは仮想化プラットフォームによる複製後に、改めて JP1/IM をインストールし直してください。

ディスク複製インストールの操作・運用方法については、ServerConductor/DeploymentManager および JP1/ServerConductor/Deployment Manager のマニュアルを参照してください。仮想化プラットフォームの複製機能については、仮想化ソフトウェアのマニュアルを参照してください。

- Docker 環境上のコンテナをエージェントホストとして監視する場合の注意事項
 - コンテナ上に JP1/Base がインストールされている必要があります。JP1/Base がサポートする Docker 環境については JP1/Base のリリースノートを参照してください。
 - コンテナ上の JP1/Base が使用するポート番号に対して、JP1/IM - Manager ホストから TCP/IP 通信できるようにしてください。
 - コンテナから外部への通信に NAT（ネットワークアドレス変換）が使用されているため、通常と同様に、コンテナ上の JP1/Base から発行されたイベントの「発行元 IP アドレス」には正確な値が表示されません。JP1/IM - Manager の各機能の条件に、「発行元 IP アドレス」に表示される IP アドレスを使用しないでください。
- Docker 環境上のコンテナをリモート監視ホストとして監視する場合の注意事項
 - リモート監視機能がサポートしている Docker 環境は次のとおりです。
Docker ホストの OS
リモート監視機能がサポートしている OS のうち、以下の OS をサポートします。
 - Red Hat Enterprise Linux Server 7.1 以降Docker バージョン
Docker ホストの OS がサポートするバージョン
 - コンテナ上に SSH がインストールされている必要があります。

- コンテナに対して JP1/IM - Manager ホストから SSH 接続できるようにしてください。

2

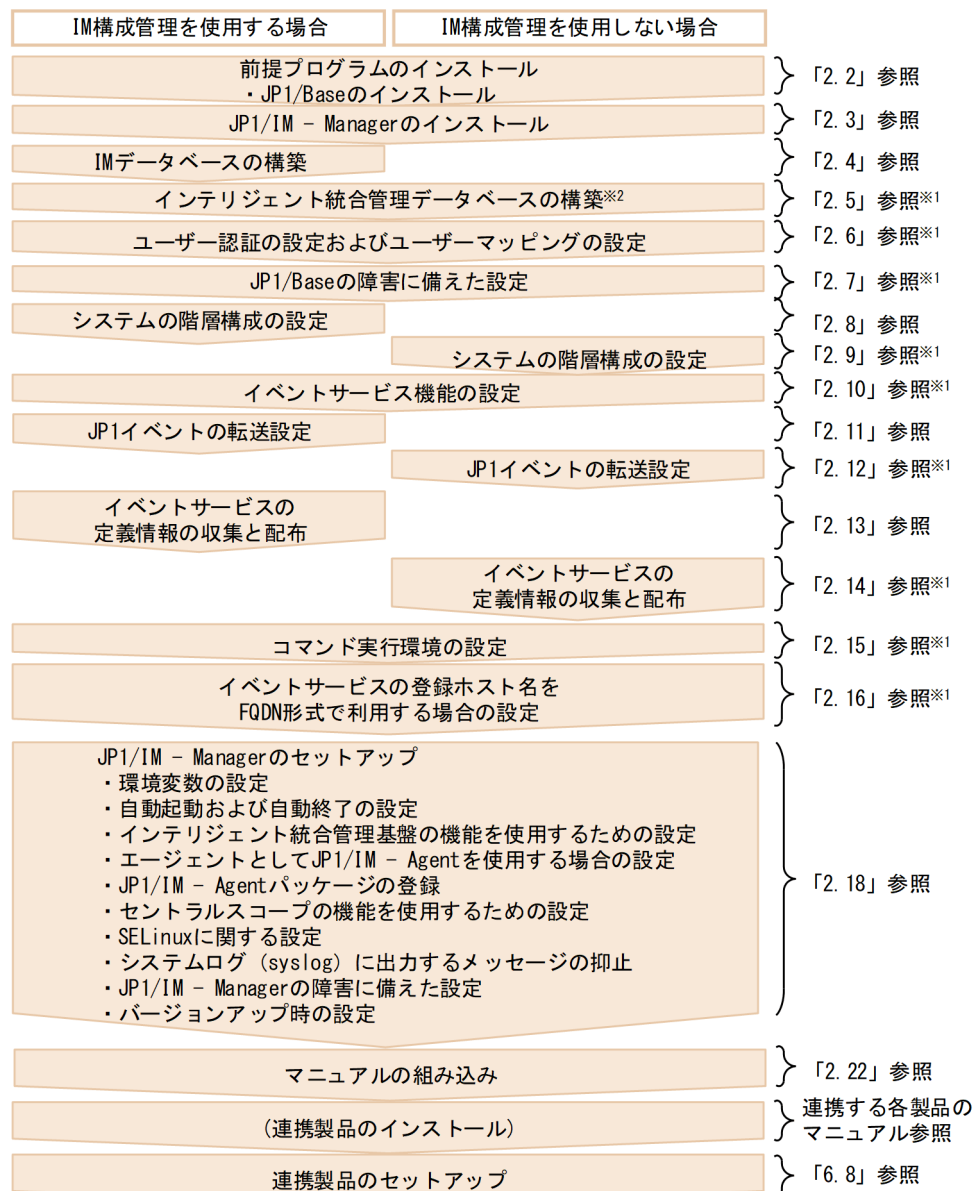
インストールとセットアップ (UNIX の場合)

この章では、UNIX 環境で JP1/IM をインストール、およびセットアップする手順について説明します。

2.1 インストールとセットアップの流れ (UNIX の場合)

インストールの開始からセットアップの終了までの作業の流れを、マネージャーの場合、エージェントの場合、およびリモートの監視対象ホストの場合に分けて示します。なお、アンインストール手順の詳細については、「2.23.1 アンインストール手順 (UNIX の場合)」を参照してください。

図 2-1 インストールとセットアップの作業の流れ (マネージャー)



注※1 詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

注※2 インテリジェント統合管理データベースを使用する場合に実施します。

図 2-2 インストールとセットアップの作業の流れ（エージェント（JP1/IM - Agent））

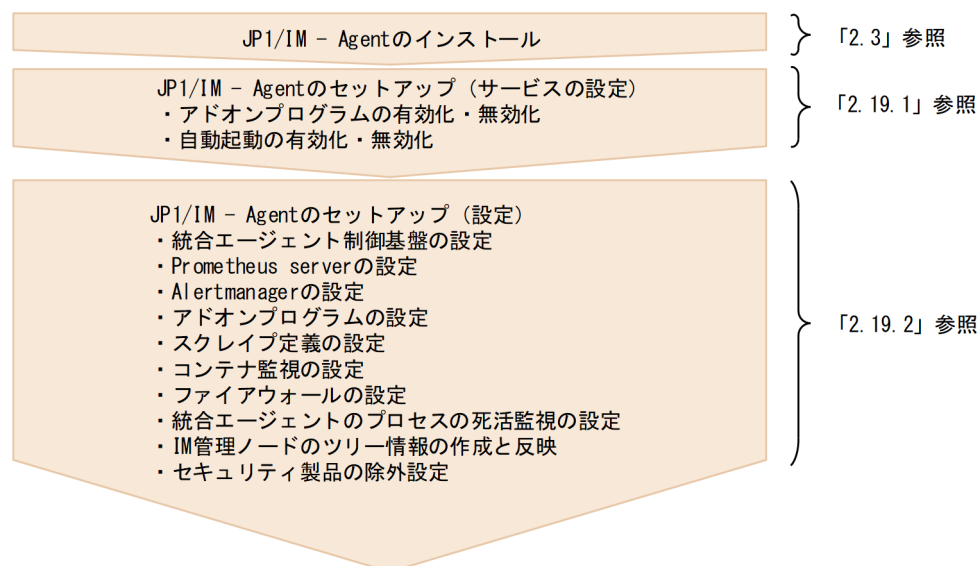
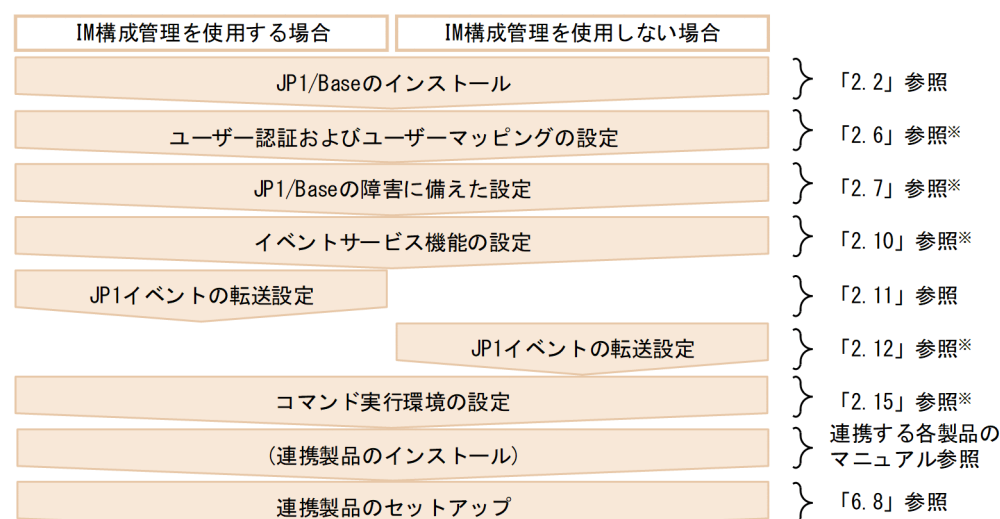


図 2-3 インストールとセットアップの作業の流れ（エージェント（JP1/Base））



注※ 詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

リモートの監視対象ホストでログ監視をするための設定については、「[2.17 リモートの監視対象ホストでログ監視をするための設定（UNIX の場合）](#)」を参照してください。

通信データを暗号化する通信暗号化機能を使用するための設定については、「[9.4 暗号化通信の構築](#)」を参照してください。

2.2 インストール前に必要な作業（UNIX の場合）

2.2.1 JP1/IM のセットアップ内容の設計（UNIX の場合）

インストール作業に入る前に、JP1/IM のセットアップ内容について検討し、設定する内容をまとめておいてください。

セットアップ内容の設計については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「第3編 設計編」を参照してください。

2.2.2 システム環境の構築（UNIX の場合）

(1) OS の環境構築

JP1/IM のインストール前に、次を満たす OS の環境を構築してください。

- JP1/IM の前提バージョンの OS であること
- JP1/IM の前提とするサービスパックやパッチが適用されていること
- JP1/IM の構成に合わせてカーネルパラメーターを調整していること
- 自ホストのホスト名を、接続している LAN 環境の IP アドレス（ループバックアドレス以外の IP アドレス）で名前解決できること
- IM データベースを使用する場合、ホスト名が、半角英数字、-, .（ピリオド）で構成される 32 文字以内の文字列であること

JP1/IM - Manager および JP1/IM - View のリリースノートを参照して、次を実施してください。

- JP1/IM が前提とするパッチを確認し、OS に適用する
- JP1/IM の構成に合わせてカーネルパラメーターを調整する

OS のパッチを適用する際は、JP1/IM を停止した状態で適用してください。

2.2.3 前提プログラムのインストール（UNIX の場合）

(1) JP1/Base のインストール

JP1/IM のマネージャーおよびエージェントには、JP1/IM - Manager の前提製品である JP1/Base をインストールする必要があります。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「1.5 JP1/IM - Manager の構成」を参照し、システム構成を確認してください。また、JP1/Base のインストール方法については、マニュアル「JP1/Base 運用ガイド」を参照してください。

2.3 インストール (UNIX の場合)

ここでは、JP1/IM - Manager および JP1/IM - Agent をインストールおよびアンインストールする手順について説明します。

なお、インストール作業を行うユーザーは、root 権限が必要です。

2.3.1 インストール手順 (UNIX の場合)

JP1/IM - Manager および JP1/IM - Agent をインストールする手順について説明します。

(1) JP1/IM - Manager のインストールの手順

次の手順で JP1/IM - Manager および JP1/IM - Agent をインストールします。この作業には、root 権限が必要です。

なお、JP1/IM - Manager をインストールすると、JP1/IM - Agent を利用するための統合エージェント管理基盤もインストールされます。

1. すべてのプログラムを終了する。

インストールする前に、JP1/Base および JP1/Base を前提とするプログラムを停止してください。

バージョンアップインストールをする場合、JP1/IM - Manager を停止してください。また、接続中の JP1/IM - View がある場合はログアウトしてください。

2. Hitachi PP Installer を実行する。

Hitachi PP Installer の指示に従ってインストールしてください。操作手順については、「[2.3.2 Hitachi PP Installer の使用方法 \(UNIX の場合\)](#)」を参照してください。

なお、JP1/IM - Manager のインストール時にインストーラーのログとして次のファイルが作成されます。これはインストールが異常終了した場合の保守資料です。インストールが正常終了したあと、JP1/IM - Manager を起動して問題がなければ削除してください。

/tmp/HITACHI_JP1_INST_LOG/jplimm_inst{1|2|3|4|5}.log

❗ 重要

IM データベースをセットアップ済みの環境で、JP1/IM - Manager をバージョンアップした場合、jimdbupdate コマンドを実行して IM データベースを更新してください。IM データベースを更新していない場合は、JP1/IM - Manager を起動したときに警告メッセージが表示されます。

JP1/IM - Agent との暗号化通信を行う場合は、統合エージェント管理基盤に関する次の手順を実施します。

1. サーバ証明書とサーバ証明書のキーファイルを設定する。

2. インストールとセットアップ (UNIX の場合)

統合エージェントホストと暗号通信を行う場合は、imbase 共通設定ファイル (jpc_imbasecommon.json) の tls_config.cert_file にサーバ証明書ファイルのフルパス、tls_config.key_file にサーバ証明書のキーファイルのフルパスを指定してください。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「imbase 共通設定ファイル (jpc_imbasecommon.json)」(2. 定義ファイル)を参照してください。

(2) JP1/IM - Agent のインストールの手順

(a) インストール前に必要な情報

JP1/IM - Agent を新規インストールする場合は、次の情報が必要です。インストール前に準備してください。

表 2-1 新規インストールに必要な情報

項目	指定要否	説明
接続先 JP1/IM - Manager のホスト名	必須	インストールする統合エージェントを管理する接続先のマネージャーホストのホスト名を指定します。IP アドレスに名前解決する必要があります。
imbase プロセスの待ち受けポート	任意	接続先のマネージャーホストで稼働している imbase プロセスの待ち受けポートを 5001～65535 の範囲で指定します。 省略時は imbase のデフォルトのポート (20724) が使用されます。
imbaseproxy プロセスの待ち受けポート	任意	接続先のマネージャーホストで稼働している imbaseproxy プロセスの待ち受けポートを 5001～65535 の範囲で指定します。 省略時は imbaseproxy のデフォルトのポート (20725) が使用されます。
imbase に初回接続するための初期シークレット	必須	接続先のマネージャーホストで稼働している imbase プロセスに初回接続するための初期シークレットを指定します。 統合オペレーション・ビューアーから確認します。
プロキシの URL	任意	マネージャーホストに接続する際にプロキシサーバを経由する場合、プロキシの URL を「http://host:port」形式で指定します。省略時のデフォルトは空文字列となります。
プロキシ認証のユーザー ID	任意	マネージャーホストに接続する場合に、プロキシサーバを経由するときはプロキシサーバの認証用のユーザー ID を指定します。 指定できる文字は ASCII コード 0x20～0x7E の範囲の文字です。 指定できる最大長は 1007 文字です。 省略時のデフォルトは空文字列となります。
プロキシ認証のパスワード	任意	マネージャーホストに接続する際にプロキシサーバを経由する場合、プロキシサーバの認証用のパスワードを指定します。 指定できる文字は ASCII コード 0x20～0x7E の範囲の文字です。 指定できる最大長は 1024 文字です。 省略時のデフォルトは空文字列となります。
使用する機能	任意	JP1/IM - Agent で使用する機能を選択できます。新規インストールを行うと、使用する機能に関するサービスが自動起動するように設定されます。

(b) インストール手順

次の手順でインストールします。

1. エージェントホストに管理者権限でログインする。

インストール作業を行うユーザーには、root 権限が必要です。

2. JP1/IM - Agent をインストールする。

JP1/IM - Agent をインストールするには、次の二つの方法があります。

- 提供媒体をドライブにセットしてインストールする方法
- マネージャーホストに登録されている JP1/IM - Agent パッケージをダウンロードで取得してインストールする方法※

注※

JP1/IM - Agent パッケージをダウンロードで取得する手順については、「[2.18.6\(3\) JP1/IM - Agent パッケージのダウンロードの手順](#)」を参照してください。

3. インストールするホストに対し、初期設定用環境変数を設定する。

■通常のインストール、サイレントインストール、およびリモートインストールの場合（必須）

インストール時に必要となるパラメーターはあらかじめ環境変数※で設定しておく必要があります。

注※

環境変数の詳細については、「[1.3.1\(3\)\(c\)インストーラーで使用する初期設定用環境変数](#)」を参照してください。

4. すべてのプログラムを終了する。

インストールする前に、すべてのプログラムを終了してください。

バージョンアップインストールをする場合、JP1/IM - Agent のサービスを停止してください。

5. 取得した JP1/IM - Agent のインストーラーを実行し、JP1/IM - Agent をインストールする。

Hitachi PP Installer※の指示に従ってインストールします。

注※ 操作手順については、「[2.3.2 Hitachi PP Installer の使用方法 \(UNIX の場合\)](#)」を参照してください。

インストールするソフトウェアを選択します。

6. インストール完了後、必要な設定変更を行う。

「[2.19.2 JP1/IM - Agent の設定](#)」に記載されている必要な設定変更を行います。必須の設定については、漏れなく実施してください。

JP1/IM - Agent の新規インストール後、/tmp/HITACHI_JP1_INST_LOG/jp1imagent_inst1.log に、jimasetup コマンドまたはjimasecret コマンドの実行に失敗したことを示すエラーメッセージが出力されていないか確認してください。エラーメッセージが出力されている場合は、jimasetup コマンドまたはjimasecret コマンドのログファイルを確認し、出力されているエラーメッセージの内容に従って対処してください。

❗ 重要

統合エージェントホストで、JP1/IM - Agent をインストールしたあと、統合エージェント制御基盤の初回起動までの間に、初期シークレットを変更した場合は、統合エージェントに登録された初期シークレットを更新するか、JP1/IM - Agent をアンインストールして再度インストールする必要があります。統合エージェントに登録された初期シークレットを更新する方法については、「[1.21.2\(2\)\(a\) 接続先の統合マネージャーを変更する（Windows の場合）（オプション）](#)」の手順 4 を参照してください。

(3) 各種インストールについて

バージョンアップインストールについて

バージョンアップインストールする前に次の内容を実施してください。

■JP1/IM - Agent の場合

論理ホストのサービスが起動している場合は、サービスを停止してからバージョンアップインストールを実行してください。論理ホストのサービス起動中にバージョンアップインストールを実行すると、論理ホストのサービスで使用するファイルが削除され、サービスが異常終了するおそれがあります。

旧バージョンの JP1/IM - Manager からバージョンアップする場合は、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「[14.2 旧バージョンの JP1/IM からのバージョンアップについて](#)」を参照してバージョンアップ時の注意について事前に知っておいてください。

また、JP1/IM - Agent をバージョンアップした場合の注意事項については、「[2.3.4\(9\) JP1/IM - Agent をバージョン 13-00 または 13-01 からバージョンアップした場合の注意事項](#)」および「[2.3.4\(10\) JP1/IM - Agent をバージョン 13-00～13-10 からバージョンアップした場合の注意事項](#)」を参照してください。

❗ 重要

論理ホストの設定を行っているコンピュータでバージョンアップインストールする場合は、バージョンアップインストールを行う前に論理ホストの JP1/IM - Manager のデーモンを停止してください。

JP1/NETM/DM, JP1/IT Desktop Management 2 および Job Management Partner 1/Software Distribution を使ったリモートインストールについて

JP1/IM は、JP1/NETM/DM, JP1/IT Desktop Management 2 および Job Management Partner 1/Software Distribution を使ったリモートインストール（ソフトウェア配布）に対応しており、JP1/IM の新規インストールおよびバージョンアップができます。次のリモートインストール方法が利用できます。

・更新インストール

■JP1/IM - Manager の場合

インストール済みの JP1/IM - Manager の設定情報は引き継がれます。JP1/IM - Manager がインストールされていない場合、更新インストールはできません。

■JP1/IM - Agent の場合

インストール済みの JP1/IM - Agent の設定情報は引き継がれます。JP1/IM - Agent がインストールされていない場合、更新インストールはできません。

新規インストール

新規インストールします。

実際の操作・運用方法については、JP1/NETM/DM, JP1/IT Desktop Management 2 または Job Management Partner 1/Software Distribution のマニュアルを参照してください。JP1/IM をパッケージングする際は、必ず JP1/NETM/DM 09 -00 以降, Job Management Partner 1/Software Distribution 09 -00 以降, または JP1/IT Desktop Management 2 のパッケージを使用してください。なお、JP1/NETM/DM は日本でだけ販売している製品です。

2.3.2 Hitachi PP Installer の使用方法 (UNIX の場合)

Hitachi PP Installer は、JP1/IM の提供媒体に格納されています。ここでは、次の操作について説明します。

- Hitachi PP Installer の起動方法
- Hitachi PP Installer を使用して JP1/IM - Manager または JP1/IM - Agent をインストールする方法
- Hitachi PP Installer を使用して JP1/IM - Manager または JP1/IM - Agent を削除する方法
- Hitachi PP Installer を使用して現在インストールされている日立製品のバージョンを確認する方法

Hitachi PP Installer 実行時のユーザー権限

- Hitachi PP Installer を使用するときは、root 権限が必要です。root でログインするか、または su コマンドでユーザーを root に変更してください。

(1) Hitachi PP Installer の起動

Hitachi PP Installer の起動手順を次に示します。

1. ドライブに JP1/IM - Manager または JP1/IM - Agent の提供媒体をセットする。

2. 提供媒体をマウントする。

マウント方法は、ご使用の OS, ハードウェアおよび環境によって異なります。マウント方法の詳細は OS のマニュアルを参照してください。

- Linux の場合

```
/bin/mount -r -o mode=0544 /dev/cdrom /mnt/cdrom
```

下線部の提供媒体ファイルシステムのマウントディレクトリ名は、環境によって異なりますので注意してください。

3.Hitachi PP Installer を起動する。

提供媒体のディレクトリ名やファイル名は、マシン環境によっては記載されている内容と見え方が異なる場合があります。ls コマンドで確認の上、表示されたファイル名を入力してください。

- Linux の場合

```
/mnt/cdrom/linux/setup /mnt/cdrom
```

下線部にはご使用になる提供媒体のマウントディレクトリ名を指定してください。

❗ 重要

インストール時は/etc/hitachi_x64setup を実行して Hitachi PP Installer を起動しないでください。

1. 提供媒体をアンマウントする。

インストール完了後、アンマウントします。アンマウント方法の詳細は OS のマニュアルを参照してください。

- Linux の場合

```
/bin/umount /mnt/cdrom
```

下線部にはご使用になる提供媒体のマウントディレクトリ名を指定してください。

(2) JP1/IM - Manager および JP1/IM - Agent のインストール

Hitachi PP Installer を使用して JP1/IM - Manager または JP1/IM - Agent をインストールする方法を説明します。Hitachi PP Installer を起動すると、初期画面が表示されます。

図 2-4 Hitachi PP Installer の初期画面例

```
L) List Installed Software.
I) Install Software.
D) Delete Software.
Q) Quit.

Select Procedure ==>

+-----+
| CAUTION!                                     |
| YOU SHALL INSTALL AND USE THE SOFTWARE PRODUCT LISTED IN THE |
| "List Installed Software." UNDER THE TERMS AND CONDITION OF  |
| THE SOFTWARE LICENSE AGREEMENT ATTACHED TO SUCH SOFTWARE PRODUCT. |
+-----+
```

初期画面で「I」を入力すると、インストールできるソフトウェアの一覧が表示されます。インストールしたいソフトウェアにカーソルを移動し、スペースバーで選択します。さらに「I」を入力すると、JP1/IM - Manager または JP1/IM - Agent がインストールされます。インストール完了後、「Q」を入力すると初期画面に戻ります。

(3) JP1/IM - Manager および JP1/IM - Agent の削除

次のコマンドを実行して、Hitachi PP Installer を起動します。

```
/etc/hitachi_x64setup
```

Hitachi PP Installer の初期画面が表示されます。初期画面については、「[図 2-4 Hitachi PP Installer の初期画面例](#)」を参照してください。

初期画面で「D」を入力すると、削除できるソフトウェアの一覧が表示されます。削除したいソフトウェアにカーソルを移動し、スペースバーで選択します。さらに「D」を入力すると、ソフトウェアが削除されます。削除完了後、「Q」を入力すると初期画面に戻ります。

(4) バージョン情報の表示

次のコマンドを実行して、Hitachi PP Installer を起動します。

```
/etc/hitachi_x64setup
```

Hitachi PP Installer の初期画面が表示されます。初期画面については、「[図 2-4 Hitachi PP Installer の初期画面例](#)」を参照してください。

初期画面で「L」を入力すると、インストール済みの日立製品の一覧が表示されます。

2.3.3 インストール直後に必要な設定（UNIX の場合）

JP1/Base の環境変数に JP1/IM - Manager の動作する言語コードを設定してください。言語コードの設定は環境変数ファイルと共通定義の両方に設定してください。なお、11-00 から JP1/IM の環境変数（jp1co_env.conf ファイル）は、なくなります。

それぞれの設定は、ローカルホスト内で統一して運用してください。また、JP1/SES 形式イベントを監視するシステムでは、システム内の言語環境を JP1/SES 形式のイベントの文字コードで統一してください。設定方法を次に示します。

(1) 環境変数ファイルの設定

/etc/opt/jp1base/conf/jp1bs_env.conf ファイルを vi などを開き、先頭行の「LANG=」の後ろに、次の表に従って環境変数 LANG の値を設定します。

表 2-2 jp1bs_env.conf ファイルの LANG に指定できる値

OS	言語種別	文字コード	環境変数 LANG の値※3
Linux	日本語	SJIS※1	ja_JP.SJIS または ja_JP.sjis
		UTF-8※2	ja_JP.UTF-8 または ja_JP.utf8

OS	言語種別	文字コード	環境変数 LANG の値※3
	英語	C	C
		UTF-8※2	en_US.UTF-8 または en_US.utf8
	中国語	GB18030	zh_CN.gb18030

注※1

SUSE Linux の場合だけ有効です。

注※2

UTF-8 コードでは、次に示す記号を二つの文字コードで表現します。

円記号(¥)：0x5C または 0xC2A5

チルダ(~)：0x7E または 0xE280BE

これらの記号について、JP1/IM - Manager では¥：0x5C, ~：0x7E の文字コードを使用します。

注※3

記載されている LANG の値以外を指定しないでください。また、LANG の値は大文字・小文字を区別します。

この定義は、次に JP1/IM - Manager を起動したときから有効になります。

❗ 重要

言語種別を英語に設定した場合、JP1/IM - Manager の設定にマルチバイト文字を使用しないでください。使用した場合、ASCII 文字で記述されたものとして扱われます。このため、JP1/IM - Manager の動作が不正になることがあります。

(2) JP1/Base の言語環境設定の確認

1. /etc/opt/jp1base/conf/jp1bs_env.conf ファイルの設定値を確認する。

jp1bs_env.conf ファイルの「LANG=」の後ろに設定されている値が、「[2.3.3\(1\) 環境変数ファイルの設定](#)」で設定した値と一致していることを確認してください。

jp1bs_env.conf ファイルについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

2. /etc/opt/jp1base/jbs_start ファイルの設定値を確認する。

jbs_start ファイルの「LANG=」の後ろに設定されている値が、「[2.3.3\(1\) 環境変数ファイルの設定](#)」で設定した値と一致していることを確認してください。

jbs_start ファイルについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

📄 メモ

文字コードを設定して運用を開始した後でも、この手順で文字コードの変更ができます。

JP1/Base の言語環境設定については、マニュアル「JP1/Base 運用ガイド」の言語種別の設定の説明を参照してください。

(3) 共通定義への言語環境設定

- 1.jp1bs_param.conf ファイルを編集する。
/etc/opt/jp1base/conf/jp1bs_param.conf ファイルをテキストエディターで開き、「LANG=」の後ろに、次の表に従って共通定義への設定値を指定します。

表 2-3 jp1bs_param.conf ファイルの LANG に指定できる値

言語種別	コード	LANG の値
日本語	シフト JIS コード	SJIS
	EUC コード	EUCJIS
	UTF-8 コード	UTF-8
英語		C
		UTF-8
中国語		GB18030

- 2.JP1/IM - Manager を停止する。
- 3.JP1/Base を停止する。
- 4.次のコマンドを実行する。

```
/opt/jp1base/bin/jbssetcnf /etc/opt/jp1base/conf/jp1bs_param.conf
```

セントラルスコープを使用している場合、稼働中に JP1/IM - Manager の環境変数を変更するときは、次の操作をしてください。

- 1.jcsdbexport コマンドで監視オブジェクト DB の保管情報をローカルファイルに出力する。
- 2.JP1/IM - Manager を停止する。
- 3.JP1/IM - Manager で動作する言語コードを変更して、JP1/IM - Manager を起動する。
- 4.jcsdbimport コマンドでローカルファイルに出力した監視オブジェクト DB を、セントラルスコープの監視オブジェクト DB に反映する。

上記の操作をしない場合は、[監視ツリー] 画面、[ビジュアル監視] 画面の表示が不正になります。

(4) JP1/Base および JP1/IM - Manager の起動

- 1.JP1/Base を起動する。
- 2.JP1/IM - Manager を起動する。

2.3.4 インストール時の注意事項（UNIX の場合）

(1) 製品間の関連について

JP1/IM - Manager は JP1/Base を前提製品としています。製品のインストール時には、次の点に注意してください。

- 前提製品がある場合は、前提の製品から順にインストールしてください。
- JP1/Base, JP1/IM - Manager の順序にインストールしてください。
- JP1/Base を停止してから、JP1/IM - Manager をインストールしてください。JP1/Base の停止を忘れた場合は、必ず JP1/Base を再起動してください。再起動しなかった場合は、システム構成情報を正しく管理できません。

(2) 統合トレース機能（HNTRLib2）について

JP1/Base のインストール時に、統合トレース機能（HNTRLib2）がインストールされます。

(3) OS 環境への設定

インストール時に次の情報を OS に設定します。

`services` ファイルに、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 C ポート番号」のポート番号を設定します。

JP1/IM - Manager のアンインストール時に、`services` ファイルに設定された、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 C ポート番号」のポート番号が削除されます。

(4) バージョンダウングレードインストールについて

JP1/IM - Manager および JP1/IM - Agent は、バージョンダウングレードインストールに対応していません。インストールされている製品をバージョンダウングレードしたい場合は、製品をアンインストールしてから再インストールしてください。

(5) JP1/IM - Manager の管理する情報について

JP1/IM - Manager は、プログラム情報、設定情報、保守情報などをファイルで管理しているため、次の操作を行わないでください。次の操作を行った場合、JP1/IM - Manager の動作を保証できません。

- JP1/IM - Manager のファイル、およびディレクトリの削除や変更を行う。
- JP1/IM - Manager のファイル、およびディレクトリのアクセス権限を変更する。

(6) インストール実行について

一時ディレクトリ (/tmp) に、5MB の空きがあることを確認してからインストールを実行してください。

(7) ウィルス対策ソフトについて

JP1/IM - Manager のインストールを実施した際に、ウィルス対策ソフトが JP1/IM - Manager のインストール先のウィルススキャンを行った場合、インストーラーとウィルス対策ソフトとの競合によりアプリケーションエラーが発生し、インストールに失敗する可能性があります。ウィルス対策ソフトを停止してインストールを実施してください。

(8) サイレントインストールについて

(a) JP1/IM - Manager の場合

JP1/IM - Manager では、サイレントインストール機能によるインストール方法が利用できます。

実行コマンド

Linux の場合：DVD-R 媒体/X64LIN/setup△-f△-k△P-CC842C-9MDL△DVD-R 媒体のパス

SUSE Linux の場合：DVD-R 媒体/SLES/setup△-f△-k△P-CC9W2C-9MDL△DVD-R 媒体のパス

△：1 個以上の半角スペース

- DVD-R 媒体を HDD 上にコピーして実行する場合は、スペースを含まないディレクトリパス上に媒体の内容をすべてコピーしてください。また、コピーしたファイル群は、コンペアなどによって、バイナリレベルで一致することを確認してください。
- インストールが正常終了したかどうかは、実行結果の戻り値を参照してください。戻り値については、JP1 の Web サイトに公開しているドキュメントの「サイレントインストール機能」を参照してください。
- JP1/IM - Manager および JP1/IM - View をサイレントインストール機能でインストールする場合は、ユーザー情報を指定することができません。ユーザー情報を指定する場合は、「[2.3.1 インストール手順 \(UNIX の場合\)](#)」に記載のインストール手順でインストールしてください。

(b) JP1/IM - Agent の場合

JP1/IM - Agent では、サイレントインストール機能によるインストール方法が利用できます。

実行コマンド

Linux の場合：DVD-R 媒体/X64LIN/setup△-f△-k△P-CC842C-9GDL△DVD-R 媒体のパス

△：1 個以上の半角スペース

(9) JP1/IM - Agent をバージョン 13-00 または 13-01 からバージョンアップした場合の注意事項

「1.3.3(14) JP1/IM - Agent をバージョン 13-00 または 13-01 からバージョンアップした場合の注意事項」を参照してください。

(10) JP1/IM - Agent をバージョン 13-00～13-10 からバージョンアップした場合の注意事項

JP1/IM - Agent をバージョンアップすると、アドオン管理機能に対応している OSS に OSS ラッパーを適用させるために、次の表に示すユニット定義ファイルに対して、ExecStart 行の更新が行われます。JP1/IM - Agent のインストーラーのログで、各ユニット定義ファイルに対して KAVB9447-I のメッセージが出力されていることを確認してください。JP1/IM - Agent のインストーラーのログについては、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「12.2.2(8) インストーラーのログ」を参照してください。

アドオンプログラム	ユニット定義ファイル名	バックアップファイル名
Prometheus server	jpc_prometheus_server.service	jpc_prometheus_server.service.bk
Alertmanager	jpc_alertmanager.service	jpc_alertmanager.service.bk
Blackbox exporter	jpc_blackbox_exporter.service	jpc_blackbox_exporter.service.bk
Yet another cloudwatch exporter	jpc_ya_cloudwatch_exporter.service	jpc_ya_cloudwatch_exporter.service.bk
process_exporter	jpc_process_exporter.service	jpc_process_exporter.service.bk
Promitor	jpc_promitor_resource_discovery.service	jpc_promitor_resource_discovery.service.bk
	jpc_promitor_scraper.service	jpc_promitor_scraper.service.bk
Script exporter	jpc_script_exporter.service	jpc_script_exporter.service.bk
Fluentd	jpc_fluentd.service	jpc_fluentd.service.bk
VMware exporter	jpc_vmware_exporter.service	jpc_vmware_exporter.service.bk
node exporter	jpc_node_exporter.service	jpc_node_exporter.service.bk

KAVB9448-W および KAVB9450-W のメッセージが出力されている場合は、該当するユニット定義ファイルを手動で編集して、ExecStart 行の更新を行ってください。ExecStart 行の記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユニット定義ファイル (jpc_プログラム名.service)」(2. 定義ファイル) を参照してください。

2.3.5 インストール時の資料採取方法（UNIX の場合）

(1) JP1/IM - Manager のインストール時の資料採取方法

インストール時に障害が発生した場合の資料採取方法を、次に示します。

1. マネージャーホストにログインします。
2. 次のファイルを手動で採取します。
 - /etc/.hitachi/.hitachi.log
 - /etc/.hitachi/.install.log
 - /etc/.hitachi/.uninstall.log
 - /tmp/HITACHI_JP1_INST_LOG/以下のファイル

(2) JP1/IM - Agent のインストール時の資料採取方法

インストール時に障害が発生した場合の資料採取方法を、次に示します。

1. 統合エージェントホストにログインする。
2. 次のファイルを手動で採取する。
 - /etc/.hitachi/pplistd/pplistd
 - /etc/.hitachi/.install.log*
 - /etc/.hitachi/.uninstall.log*
 - /tmp/HITACHI_JP1_INST_LOG/以下のファイル

2.3.6 オートスケール機能と連携する方法（UNIX の場合）

(1) JP1/IM - Agent でオートスケール機能と連携する方法

(a) 前提サービスと前提条件

オートスケール機能と連携して運用する場合の前提サービスと前提条件を、次に示します。

前提サービス

- Amazon EC2
- Amazon EC2 Auto Scaling

前提条件

オートスケール機能と連携して運用する場合の前提条件を次に示します。

- クラスタ環境の論理ホストを対象とすることはできません。
- システムの構成はマネージャーホストを含めて 2,500 台以内にしてください。
- スケールアウトやスケールインが行われた後でシステム構成情報の作成と反映を行う必要があります。詳細については、「[2.19.2\(18\) IM 管理ノードのツリー情報の作成と反映 \(Linux の場合\) \(必須\)](#)」を参照してください

(b) 仮想マシンイメージ (AMI) の作成

仮想マシンイメージ (AMI) を作成する手順を次に示します。

1. JP1/IM - Agent をインストールします。

このとき、インストールモード [イメージ作成モード] を選択します。詳細については、「[1.3.1\(3\)\(c\) インストーラーで使用する初期設定用環境変数](#)」を参照してください。

2. 仮想マシンイメージ (AMI) を作成します。

仮想マシンイメージ (AMI) の作成方法については、Amazon Web Services の公式サイトを参照してください。

(c) Auto Scaling の起動設定の作成

Auto Scaling の起動設定を作成する手順を次に示します。

1. [AWS マネジメントコンソール] から [Amazon EC2] コンソールを開きます。
2. 左側ナビゲーションペインの [Auto Scaling] で [起動設定] をクリックします。
3. [起動設定の作成] をクリックします。
4. [AMI の選択] 画面から、手順 1 で作成した仮想マシンイメージ (AMI) を選択します。
5. [詳細設定] 画面の [高度な詳細] - [ユーザーデータ] で [テキストで] を選択して、テキストボックスに次の内容を記述します。

```
#!/bin/sh
/opt/jp1ima/tools/jimasetup phost
/opt/jp1ima/tools/jpc_service_start -s all
```

2.3.7 仮想マシンのクローン作成 (UNIX の場合)

次に示す仮想化プラットフォームでは、JP1/IM - Agent をイメージ作成モードでインストールした統合エージェントホスト環境の仮想マシンテンプレートから、仮想マシンのクローンを作成できます。

- VMware ESX
- Hyper-V
- SCVMM

(1) 前提条件

エージェントを複製する場合の前提条件となる注意事項を次に示します。

- 仮想マシンのクローンを作成できる対象はエージェントホストだけです。また、クラスタ環境の論理ホストを対象とすることはできません。
- エージェント構成上のホスト数の最大値は、マネージャーホストを含めて 2,500 台です。
- 仮想マシンテンプレートを作成するとき、JP1/IM - Agent のインストールモードには [イメージ作成モード] を選択してください。

(2) 仮想マシンのテンプレートの作成方法

仮想マシンのテンプレートの作成方法を、次に示します。

1. 仮想マシンに JP1/IM - Agent をインストールする。
インストール時のインストールモードは [イメージ作成モード] を選択します。
インストール方法については、[2.3.1(2)JP1/IM - Agent のインストールの手順] を参照してください。

❗ 重要

JP1/IM - Agent の初期設定は行いません。

(3) 仮想マシンのクローンの作成方法

仮想マシンのクローンの作成方法を、次に示します。

1. 仮想マシンテンプレートから、新しい仮想マシンを複製する。
仮想化プラットフォームが提供する複製機能については、仮想化ソフトウェアのマニュアルを参照してください。
複製に関して OS で必要な作業については、OS の仕様を確認してください。
2. 新しい仮想マシンを起動する。
3. 新しい仮想マシンのホスト名を変更する。
必要に応じて、仮想マシンのホスト名を変更してください。
4. 新しい仮想マシンの IP アドレスを変更する。
必要に応じて、仮想マシンの IP アドレスを変更してください。
IP アドレスを変更した場合の作業については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「2.3.1(3)エージェントの IP アドレスを変更した場合の作業」を参照してください。
5. JP1/IM - Agent の初期設定を行う。
JP1/IM - Agent の初期設定コマンドを実行します。

```
JP1/IM - Agentのインストール先/jp1ima/tools/jimasetup phost
```

6. JP1/IM - Agent の接続先の JP1/IM - Manager で、IM 管理ノードのツリー情報を更新する。

詳細については、「[2.19.2\(18\)IM 管理ノードのツリー情報の作成と反映（Linux の場合）（必須）](#)」を参照してください。

2.4 IM データベースの構築 (UNIX の場合)

IM データベースを使用して、システムで発生したイベントを監視します。IM データベースには、統合監視 DB と IM 構成管理 DB とがあります。統合監視 DB は、インテリジェント統合管理基盤、またはセン
トラルコンソールを利用する場合に使用します。IM 構成管理 DB は、IM 構成管理を使用してシステムの
階層構成を管理します。統合監視 DB と IM 構成管理 DB を使用した場合に利用できる機能の詳細につい
ては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.6 IM データ
ベースが提供する機能」を参照してください。

システム構築時および運用開始後に、統合監視 DB、IM 構成管理 DB のどちらかまたは両方が必要になっ
たときは、その時点で IM データベースを構築できます。

統合監視 DB には、JP1/IM3-Manager サービスが起動したあとにイベント DB から取得した JP1 イベント
が格納されます。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設
計ガイド」の「4.1.3(2) 統合監視 DB を使用する場合は JP1 イベント制御の仕組み」を参照してください。

ここでは、IM データベースを構築する手順について説明します。

❗ 重要

Amazon EC2 インスタンス環境での運用では、ホスト名が 32 文字を超えることがあります
(例: ip-xx-xx-xx-xx.ap-northeast-1.compute.internal (xx-xx-xx-xx の部分は IP アドレ
ス))。IM データベースをセットアップする場合、IM データベースのホスト名が上限 (32 文
字) を超えると、KNAN11141-E のエラーメッセージを出力して、セットアップが失敗しま
す。そのため、AWS が公開する Amazon EC2 インスタンスに静的ホスト名を永続的に割り
当てる方法に従って、上限 (32 文字) を超えないホスト名に変更してください。

2.4.1 IM データベースを構築するための準備 (UNIX の場合)

IM データベースを構築するために必要なデータベース領域のサイズやデータベース格納ディレクトリの情
報を記述したセットアップ情報ファイルを準備します。

1. セットアップ情報ファイルを編集する。

設定例を次に示します。

```
#IM DATABASE SERVICE - DB Size
IMDBSIZE=S
#IM DATABASE SERVICE - Data Storage Directory
IMDBDIR=/var/opt/jp1imm/database
#IM DATABASE SERVICE - Port Number
IMDBPORT=20700
#IM DATABASE SERVICE - DB Install Directory
IMBENVDIR=/var/opt/jp1imm/dbms
```

2. インストールとセットアップ (UNIX の場合)

JP1/IM - MO を使用する場合は、JP1/IM - Manager と JP1/IM - MO が異なるホストで動作するときは、セットアップ情報ファイルに記載する項目に「IMDBHOSTNAME」を追加する必要があります。セットアップ情報ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「セットアップ情報ファイル (jimbdbsetupinfo.conf)」(2. 定義ファイル) を参照してください。

2. セットアップ情報ファイルの設定値を確認する。

次の項目を確認してください。

- IMDBENVDIR およびIMDBDIR に、常にマウント状態にあるディレクトリを指定しているか。アンマウントされやすいディレクトリを指定していないか。また、シンボリックリンクを含むパスを指定していないか。

❗ 重要

jicodbsetup コマンド、またはjcfdbsetup コマンドを実行する際は、/etc/opt/jp1imm/のディスク容量が不足していないか確認してください。ディスク容量が不足している場合、以下のメッセージを出力して異常終了する問題が発生します。

KNAN11053-E ファイルの読み込みに失敗しました。(ファイル名:instdb.log)

2.4.2 統合監視 DB の設定 (UNIX の場合)

統合監視 DB を作成し、インテリジェント統合管理基盤、またはセントラルコンソール機能で統合監視 DB を使用できるように設定します。統合監視 DB を使用しない場合、この手順は不要です。

すでに IM 構成管理 DB をセットアップしているかどうかで、設定の手順が異なります。それぞれの設定手順を次に示します。

(1) すでに IM 構成管理 DB をセットアップしている場合の手順

JP1/IM3-Manager サービスを停止するかどうかで、設定の手順が異なります。それぞれの設定手順を次に示します。

- JP1/IM3-Manager サービスを停止して統合監視 DB を作成する場合の手順

1. IM データベースサービス (JP1/IM3-Manager DB Server) が起動しているか確認する。

2. 次のサービスを停止する。

- JP1/IM3-Manager サービス
- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス

3. jicodbsetup コマンドを実行し、統合監視 DB を作成する。

```
jcodbsetup -s [-q]
```

4. jcoimdef コマンドを実行して、統合監視 DB を有効にする。

```
jcoimdef -db ON
```

5. JP1/IM3-Manager サービスを起動する。

- JP1/IM3-Manager サービスを停止しないで統合監視 DB を作成する場合の手順

1. jcoimdef コマンドを実行して、IM 構成管理サービス (jcfmain) を無効にする。

```
jcoimdef -cf OFF
```

2. JP1/IM3-Manager サービスを再起動する。

3. IM データベースサービス (JP1/IM3-Manager DB Server) が起動しているか確認する。

4. 次のサービスを停止する。

- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス

5. jcodbsetup コマンドを実行し、統合監視 DB を作成する。

```
jcodbsetup -s [-q]
```

6. jcoimdef コマンドを実行して、統合監視 DB を有効にする。

```
jcoimdef -db ON
```

7. jcoimdef コマンドを実行して、IM 構成管理サービス (jcfmain) を有効にする。

```
jcoimdef -cf ON
```

8. JP1/IM3-Manager サービスを再起動する。

jcodbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcodbsetup」(1. コマンド) を参照してください。

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

(2) IM 構成管理 DB をセットアップしていない場合の手順

1. 次のサービスを停止する。

- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス

2. jcodbsetup コマンドを実行し、統合監視 DB を作成する。

```
jcodbsetup -f セットアップ情報ファイル名 [-q]
```

3. jcoimdef コマンドを実行して、統合監視 DB を有効にする。

```
jcoimdef -db ON
```

4. JP1/IM3-Manager サービスを再起動する。

jcodbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcodbsetup」(1. コマンド) を参照してください。

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

2.4.3 IM 構成管理 DB の設定 (UNIX の場合)

IM 構成管理 DB を作成し、IM 構成管理サービスをプロセス管理から起動できるように設定します。IM 構成管理の機能を使用しない場合、この手順は不要です。

すでに統合監視 DB をセットアップしているかどうかで、設定の手順が異なります。それぞれの設定手順を次に示します。

(1) すでに統合監視 DB をセットアップしている場合の手順

JP1/IM3-Manager サービスを停止するかどうかで、設定の手順が異なります。それぞれの設定手順を次に示します。

- JP1/IM3-Manager サービスを停止して IM 構成管理 DB を作成する場合の手順

1. IM データベースサービス (JP1/IM3-Manager DB Server) が起動しているか確認する。

2. 次のサービスを停止する。

- JP1/IM3-Manager サービス
- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス

3. jcfdbsetup コマンドを実行して、IM 構成管理 DB を作成する。

```
jcfdbsetup -s [-q]
```

- JP1/IM3-Manager サービスを停止しないで IM 構成管理 DB を作成する場合の手順

1. jcoimdef コマンドを実行して、統合監視 DB を無効にする。

```
jcoimdef -db OFF
```

2. JP1/IM3-Manager サービスを再起動する。

3. IM データベースサービス (JP1/IM3-Manager DB Server) が起動しているか確認する。

4. 次のサービスを停止する。

- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス

5. jcfdbsetup コマンドを実行して、IM 構成管理 DB を作成する。

```
jcfdbsetup -s [-q]
```

6. jcoimdef コマンドを実行して、統合監視 DB を有効にする。

```
jcoimdef -db ON
```

jcfdbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcfdbsetup」(1. コマンド) を参照してください。

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

(2) 統合監視 DB をセットアップしていない場合の手順

1. jcfdbsetup コマンドを実行して、IM 構成管理 DB を作成する。

```
jcfdbsetup -f セットアップ情報ファイル名 [-q]
```

jcfdbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcfdbsetup」(1. コマンド) を参照してください。

2.4.4 IM 構成管理の機能を使用するための設定 (UNIX の場合)

JP1/IM - Manager を新規にインストールした場合、IM 構成管理の機能はデフォルトで無効になっています。システム構築時またはシステム運用時に IM 構成管理を使用する場合は、「[2.4.3 IM 構成管理 DB の設定 \(UNIX の場合\)](#)」の手順で IM 構成管理 DB を構築したあと、IM 構成管理の機能を有効にする必要があります。

ここでは、IM 構成管理の機能を有効にする手順について説明します。

1. jcoimdef コマンドを実行して、IM 構成管理サービス (jcfmain) を有効にする。

```
jcoimdef -cf ON
```

2. JP1/IM - Manager を再起動する。

3. jco_spmc_status コマンドを実行して、IM 構成管理サービス (jcfmain) が稼働プロセスに表示されていることを確認する。

jcoimdef コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

jco_spmd_status コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jco_spmd_status」(1. コマンド) を参照してください。

2.4.5 IM データベースの更新 (UNIX の場合)

JP1/IM - Manager をバージョンアップまたは JP1/IM - Manager の修正版を適用した場合に IM データベースを使用しているときは、IM データベースの更新処理が必要になります。次に示す手順に従い、IM データベースを更新してください。

1. サービスの状態を確認する。

次の状態と異なる場合は、サービスを停止し次の状態にしてください。

- JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスが停止している。
- JP1/OA で JP1/IM - Manager から JP1 イベントを取得している場合は、接続元の JP1/OA が停止している。
- JP1/IM - Manager が停止している。

2. jimdbupdate コマンドを実行して IM データベースの更新を確認する。

- 次のメッセージが出力された場合は、手順 6 を実行してください。
KNAN11201-I IM データベースサービスは最新の状態です
- 次のどれかのメッセージが出力された場合は、手順 3 以降を実行してください。
KNAN11202-I IM データベースサービスの上書きインストールが必要です
KNAN11207-I IM データベースサービスのテーブルスキーマの更新が必要です
KNAN11211-I IM データベースサービスの設定ファイルの更新が必要です

3. jimdbbackup コマンドを実行し、IM データベースをバックアップする。

jimdbbackup -o バックアップファイル名 -m MAINT

4. jimdbupdate コマンドを実行し、IM データベースを更新する。

jimdbupdate -i

5. jimdbstop コマンドを実行し、IM データベースを停止する。

jimdbstop

次のどれかのメッセージが出力されることを確認します。

KNAN11186-I IM データベースサービスの停止処理は正常に終了しました

KNAN11183-I IM データベースサービスは停止中です

6. JP1/IM - Manager を起動する。

7. 手順 1 で次のサービスを停止した場合、開始する。

- 接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービス
(JP1/IM - MO を使用している場合)
- 接続元の JP1/OA
(JP1/OA で JP1/IM - Manager から JP1 イベントを取得している場合)

❗ 重要

`jimdbupdate` コマンドを実行する前に取得した IM データベースの更新前のバックアップデータは、`jimdbupdate` コマンド実行後の IM データベースにリカバリーしないでください。

`jimdbupdate` コマンドを実行したあとは、再度 `jimdbbackup` コマンドでバックアップを取得してください。

2.5 インテリジェント統合管理データベースの構築（UNIX の場合）

インテリジェント統合管理データベースを使用する場合は、JP1/IM - Manager のインストール後、セットアップコマンド（jimgndbsetup コマンド）を手動で実行してください。

インテリジェント統合管理データベースを構築することで、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.7.1(1)(a)データベースの構成」に示す各種情報の管理 DB を構築して、各種機能で使用するデータを管理できるようになります。

インテリジェント統合管理データベースを構築する手順について、次に説明します。

2.5.1 インテリジェント統合管理データベースを構築するための準備（UNIX の場合）

インテリジェント統合管理データベースを構築するために必要な定義を記述したインテリジェント統合管理データベースセットアップ情報ファイルを準備します。

マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インテリジェント統合管理データベースセットアップ情報ファイル（jimgndbsetupinfo.conf）」（2. 定義ファイル）を参照して、インテリジェント統合管理データベースセットアップ情報ファイルを編集してください。

2.5.2 インテリジェント統合管理データベースの設定（UNIX の場合）

インテリジェント統合管理データベースを作成し、インテリジェント統合管理基盤でインテリジェント統合管理データベースを使用できるように設定します。インテリジェント統合管理データベースを使用しない場合、この手順は不要です。

設定手順を次に示します。

1. root 以外の OS ユーザーを作成する。

インテリジェント統合管理データベースを起動する root 以外の OS ユーザー（ログインが可能なユーザー）が必要です。

必要に応じて、OS の useradd コマンドで、インテリジェント統合管理データベースを起動するユーザーを作成してください。すでに作成済みの場合は、次の手順に進んでください。

ユーザー「imdbuser」を作成する場合の useradd コマンドの実行例を次に示します。

```
useradd imdbuser
```

2. jimgndbsetup コマンドを実行し、インテリジェント統合管理データベースを作成する。

```
jimgndbsetup -f インテリジェント統合管理データベースセットアップ情報ファイル
```

jimgndbsetup コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimgndbsetup」(1. コマンド)を参照してください。

2.5.3 セキュリティ製品の除外設定 (UNIX の場合)

JP1/IM - Manager の起動中にウイルスチェックを実施する場合は、次のファイルおよびディレクトリをスキャンの対象から除外してください。また、JP1/IM - Manager の停止中にウイルスチェックを実施して JP1/IM - Manager を再起動する場合は、次のファイルおよびディレクトリに対してウイルスチェックが完了したことを確認してください。

JP1/IM - Manager のファイルおよびディレクトリ (UNIX の場合)

- ・ インテリジェント統合管理データベースの実行ファイルの格納先/以下すべて※
- ・ インテリジェント統合管理データベースのデータファイルの格納先/以下すべて※
- ・ インテリジェント統合管理データベースの関連ライブラリの格納先/以下すべて※
- ・ インテリジェント統合管理データベースの設定ファイルの格納先/以下すべて※
- ・ インテリジェント統合管理データベースの運用コマンドの格納先/以下すべて※
- ・ インテリジェント統合管理データベースの運用コマンドの個別ログの格納先/以下すべて※
- ・ トレンドデータ管理サービスのログの格納先/以下すべて※

上記の各格納先の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の、「2.7.1 インテリジェント統合管理データベース」の「(1)(d)関連ファイルの格納先」を参照してください。

論理ホスト環境の場合は、共有ディレクトリ以下もスキャンの対象から除外してください。

- ・ 共有ディレクトリ/jp1imm/以下すべて
- ・ 論理ホストのインテリジェント統合管理データベースのデータファイルの格納先/以下すべて

注※

インテリジェント統合管理データベースをセットアップしている場合は除外してください。

2.6 ユーザー認証の設定およびユーザーマッピングの設定（UNIX の場合）

JP1 ユーザー管理に必要な、認証サーバの指定、JP1 ユーザーの登録、ユーザーマッピングの設定をします。
ホストの役割に合わせて、次のように設定します。

表 2-4 ホストの役割ごとの設定項目

設定項目	認証サーバとして使用する		認証サーバとして使用しない	
	プライマリー 認証サーバ	セカンダリー 認証サーバ	マネージャー ホスト	エージェント ホスト
認証サーバ指定	○	○	○	—
JP1 ユーザーの設定	○	—	—	—
操作権限の設定	○	—	—	—
認証サーバ設定のコピー	—	○	—	—
ユーザーマッピング※	○	○	○	○

(凡例)

- ：設定が必要
- ：設定が不要

注※ 自動アクションしない場合、および JP1/IM - View から管理対象ホストにコマンド実行しない場合は不要です。

設定は、JP1/Base のコマンドによって行います。

なお、ユーザーマッピングは、自動アクションまたは JP1/IM - View の操作によってコマンドを実行するすべてのホストで、次のように設定します。

表 2-5 自動アクションや JP1/IM - View によってコマンドを実行する場合のユーザーマッピング

操作	JP1 ユーザー名	サーバホスト名	OS ユーザー名
JP1/IM - View からコマンド を実行する場合	マネージャーにログインする ユーザー	JP1/IM - View が接続するマ ネージャー※	コマンド実行先ホストの OS に登録されたユーザー
自動アクションを実行する 場合	アクション定義で指定した ユーザー名	自動アクションを定義したマ ネージャー※	アクション実行先ホストの OS に登録されたユーザー

注※ サーバホスト名には「*」も指定できます。この場合は、すべてのホストでユーザーマッピングが許可されます。

なお、「jpladmin」という JP1 ユーザーがデフォルトで登録されています。「jpladmin」には、JP1 資源グループが「*」で、JP1 権限レベルが JP1_Console_Admin である操作権限が設定されています（JP1 資源グループが「*」の場合、すべての JP1 資源グループにアクセスできます）。

2.6.1 認証サーバの指定 (UNIX の場合)

認証サーバのホスト名を指定します。この設定は、認証サーバのホストおよび JP1/IM のマネージャーが必要です。エージェントでは必要ありません。

1. 認証サーバを指定する。

```
/opt/jp1base/bin/jbssetusrsrv ホスト名 1 [ホスト名 2]
```

認証サーバはプライマリー、セカンダリーの 2 台まで設定できます。ホスト名 1 がプライマリー認証サーバ、ホスト名 2 がセカンダリー認証サーバです。

設定方法の詳細については、マニュアル「JP1/Base 運用ガイド」のユーザー管理機能の設定の章を参照してください。

2.6.2 JP1 ユーザーの登録 (UNIX の場合)

JP1/IM を使用する JP1 ユーザーを登録します。この設定は、プライマリー認証サーバのホストが必要です。

1. JP1 ユーザーを登録する。

```
/opt/jp1base/bin/jbsadduser JP1 ユーザー名
```

2.6.3 JP1 ユーザーの操作権限の設定 (UNIX の場合)

JP1/IM を使用する JP1 ユーザーに操作権限を登録します。この設定は、プライマリー認証サーバのホストが必要です。

1. JP1 ユーザーに操作権限を設定する。

認証サーバのホストで、ユーザー権限レベルファイル (JP1_UserLevel) を編集し、JP1 ユーザーに操作権限を設定します。

設定内容については、マニュアル「JP1/Base 運用ガイド」の JP1 ユーザーの操作権限の設定に関する説明を参照してください。

JP1/IM の操作権限としては、JP1 資源グループに JP1_Console、権限レベルに JP1_Console_Adminなどを指定します。

なお、IM 構成管理の操作権限としては、JP1 資源グループに JP1_Console、権限レベルに JP1/IM の権限レベルと IM 構成管理の権限レベルを設定する必要があります。IM 構成管理の権限レベルを設定していない場合、実行できる操作は、IM 構成管理の JP1 権限レベル「JP1_CF_User」の範囲に限定されます。

JP1/IM の操作権限については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「9.4.1 JP1 ユーザーの管理」および「付録 E 操作権限一覧」を参照してください。

2. インストールとセットアップ (UNIX の場合)

2.6.4 プライマリー認証サーバの設定情報のコピー (UNIX の場合)

プライマリー認証サーバから認証サーバの設定ファイルをコピーします。この設定は、セカンダリー認証サーバのホストで必要です。

1. 認証サーバの設定ファイルをコピーする。

/etc/opt/jp1base/conf/user_acl ディレクトリに格納されている設定ファイルJP1_Group, JP1_Passwd, JP1_UserLevel をコピーします。テキストファイルのため、FTP で ASCII 転送するなどでコピーします。

2.6.5 ユーザーマッピングの設定 (UNIX の場合)

自動アクションや JP1/IM - View の操作によって、コマンドを実行するホストで、JP1 ユーザー名と OS ユーザー名とのユーザーマッピングを設定します。この設定は、JP1/IM からコマンドを実行するすべてのホストで必要です。

1. ユーザーマッピング定義を設定する。

コマンド実行をする各ホストで、ユーザーマッピング定義ファイル (jp1BsUmap.conf) を編集し、JP1 ユーザーと OS ユーザーのユーザーマッピングを設定します。

2. 次のユーザーマッピング定義コマンドを実行する。

/opt/jp1base/bin/jbsmkumap

なお、ユーザーが複数いる場合は、すべてのユーザーに対してユーザーマッピングの設定が必要です。JP1 ユーザー名と OS ユーザー名が同じ場合でも、ユーザーマッピングの設定が必要です。

また、自動アクションや JP1/IM - View の操作によって実行されるコマンドは、JP1 ユーザーにマッピングされているプライマリーユーザーで実行されます。特定の OS ユーザーでコマンドを実行したい場合には、その OS ユーザーをプライマリーユーザーとして登録してください。

ユーザーマッピング定義ファイル (jp1BsUmap.conf)、および jbsmkumap コマンドについては、マニュアル「JP1/Base 運用ガイド」のユーザー管理機能の設定の説明を参照してください。

2.7 JP1/Base の障害に備えた設定 (UNIX の場合)

JP1/Base は、JP1/Base 自身の障害がシステム運用に影響を及ぼすのをできるだけ防ぐために、次の機能を提供しています。

- プロセスの異常を検知する機能 (ヘルスチェック機能)
- プロセスが異常終了した場合に自動で再起動する機能
- プロセスや認証サーバの異常を検知した場合に JP1 イベントを発行する機能
- JP1/Base の障害発生時に調査資料を採取するツール

デフォルトでは、プロセスの異常検知や再起動、JP1 イベントの発行もしない設定になっています。設定を変更する場合は、マニュアル「JP1/Base 運用ガイド」のインストールとセットアップの章の説明を参照してください。

2.8 IM 構成管理を使用する場合のシステムの階層構成の設定 (UNIX の場合)

ここでは、IM 構成管理を使用する場合のシステムの階層構成 (IM 構成) の設定について説明します。IM 構成管理を使用しない場合のシステムの階層構成の設定については、「[2.9 IM 構成管理を使用しない場合のシステムの階層構成の設定 \(UNIX の場合\)](#)」を参照してください。

IM 構成管理を使用する場合は、IM 構成管理・ビューアーを操作して、JP1/IM が運用管理するシステムのマネージャーおよびエージェントの階層関係を設定します。

また、IM 構成管理のエクスポート・インポート機能を使用して、テスト環境のシステム構成を運用環境に移行したり、変更前の環境のシステム構成を変更後の環境に移行したりできます。

IM 構成管理のエクスポート・インポート機能を使用すると、仮想ホストを含むシステムの階層構成 (仮想化システム構成) を IM 構成管理で管理するための設定や、セントラルスコープで監視するための設定ができます。

IM 構成管理を使用してシステムの階層構成を管理している場合、次の処理を実行すると、IM 構成管理が保持する構成定義情報と JP1/Base が保持する構成定義情報が不一致となります。

- JP1/Base の構成定義ファイルを編集する
- `jbsrt_distrib` コマンドを実行する

そのため、IM 構成管理を使用してシステムの階層構成を管理している場合は、IM 構成管理を使用して構成を一元管理することを推奨します。

JP1/Base が提供する機能を使用してシステムの階層構成の定義の配布をした場合は、IM 構成管理と JP1/Base で保持する構成定義情報を一致させるために、システムの階層構成を取得する必要があります。システムの階層構成の取得がされていない場合、構成定義情報が不一致のため、動作が不正になります。

2.8.1 IM 構成管理・ビューアーによるシステム構成の設定 (UNIX の場合)

ここでは、IM 構成管理・ビューアーを操作して、システムの階層構成を設定する方法について説明します。

IM 構成管理を使用していない既存の JP1/IM システムに IM 構成管理を追加した場合、IM 構成管理・ビューアーを使用すると、既存の JP1/IM のシステムから収集した構成定義情報を編集して、システムの階層構成を設定できます。

新規にシステムの階層構成を設定する場合、および既存のシステムの階層構成を編集する場合の手順について説明します。

(1) 新規にシステムの階層構成を設定する場合

システムの階層構成は、最上位のマネージャーで一括して定義する方法と、各マネージャーが管理する複数の部分に分割して定義する方法があります。

システムの階層構成の管理および構成定義情報の定義例については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.2.1 IM 構成管理で管理対象となるシステムの階層構成」を参照してください。

新規にシステムの階層構成を設定する手順の概要を次に示します。

1. システムの階層構成に追加するホストを、IM 構成管理の管理対象として登録する。

- ホストを登録する方法、およびホストに関する情報を設定する方法については、「[3.1.1 ホストを登録する](#)」を参照してください。
- 登録したホストに関する情報を参照する方法については、「[3.1.4 ホスト情報を表示する](#)」を参照してください。
- ホストを削除する方法については、「[3.1.6 ホストを削除する](#)」を参照してください。
- 登録したホストに関する情報を変更する方法については、「[3.1.5 ホスト情報の属性を変更する](#)」を参照してください。

2. IM 構成管理に登録したホストをシステムの階層構成に追加して、マネージャーとエージェントの階層関係を設定する。

- JP1/IM のシステムにホストを追加する方法については、「[3.2.4\(1\)\(a\) ホストを追加する](#)」を参照してください。
- JP1/IM のシステムからホストを削除する方法については、「[3.2.4\(1\)\(c\) ホストを削除する](#)」を参照してください。
- マネージャーとエージェントの階層関係を設定する方法については、「[3.2.4\(1\)\(b\) ホストを移動する](#)」を参照してください。

3. 設定したシステムの階層構成をシステムに反映する。

IM 構成管理・ビューアーで設定したシステムの階層構成を、JP1/IM が運用管理するシステムに反映します。

- 設定したシステムの階層構成をシステムに反映する方法については、「[3.2.4\(3\) システムの階層構成を IM 構成管理が管理するシステムに反映する](#)」を参照してください。
- 設定したシステムの階層構成を確認する方法については、「[3.2.2 システムの階層構成を表示する](#)」を参照してください。

システムの階層構成を統合マネージャーと拠点マネージャーに分割して定義する場合は、マネージャーごとに上記の手順を行ってください。そのあとに、統合マネージャーに接続した IM 構成管理ビューアーで次の手順を実施して、システム全体の定義を作成します。

1. システムの階層構成の同期を取る。

統合マネージャーと拠点マネージャーの間で、構成定義情報の同期を取ります。

システムの階層構成の同期を取る方法については、「[3.2.5 システムの階層構成の同期を取る](#)」を参照してください。

(2) 既存のシステムの階層構成を編集する場合

構成管理情報の設定方法を JP1/Base が提供する構成管理機能から IM 構成管理に切り替える場合の手順を次に示します。

1. IM 構成管理・ビューアーの [IM 構成管理] 画面から既存の JP1/IM の構成定義情報を読み込んで、システムの階層構成を取得する。
取得した構成定義情報が IM 構成管理 DB に保存され、自動的にホストの登録が実施されます。
詳細は、「[3.2.1 システムの階層構成を取得する](#)」を参照してください。
2. [ホスト属性編集] 画面から登録されたホスト属性を確認し、必要に応じてホスト名やホスト種別を編集する。
詳細は、「[3.1.5 ホスト情報の属性を変更する](#)」を参照してください。
3. [IM 構成管理] 画面からホスト情報を収集する。
詳細は、「[3.1.3 ホストから情報を収集する](#)」を参照してください。
4. [IM 構成管理] 画面から収集したホスト情報を確認する。
ホスト情報として下位ホスト情報、基本情報、製品情報、およびサービス情報を確認できます。
詳細は、「[3.1.4 ホスト情報を表示する](#)」を参照してください。
5. [IM 構成管理] 画面からシステムの階層構成を確認し、必要に応じて編集する。
システムの階層構成を編集した場合は、必ずシステムの階層構成を反映してください。
詳細は、「[3.2.2 システムの階層構成を表示する](#)」, 「[3.2.4 システムの階層構成を編集する](#)」, および「[3.2.4\(3\) システムの階層構成を IM 構成管理が管理するシステムに反映する](#)」を参照してください。
6. [IM 構成管理] 画面からプロファイル情報を収集する。
エージェントの各サービスで現在使用されている設定情報とエージェントに保存されている設定ファイルが収集されます。
詳細は、「[3.5.1\(2\) プロファイルを収集する](#)」を参照してください。
7. [IM 構成管理] 画面からプロファイル情報を確認し、必要に応じて設定ファイルを編集する。
設定ファイルを編集した場合は、必ず設定ファイルの編集内容を反映してください。また、反映後に手順 6 を実施し、プロファイル情報を確認してください。
詳細は、「[3.5.1\(3\) プロファイルを表示する](#)」, 「[3.5.1\(5\) 設定ファイルを編集する](#)」, および「[3.5.1\(6\) 設定ファイルの編集内容を反映する](#)」を参照してください。

2.8.2 エクスポート・インポート機能によるシステム構成の設定 (UNIX の場合)

IM 構成管理のエクスポート・インポート機能を使用すると、テスト環境のシステム構成を運用環境に移行したり、変更前の環境のシステムの階層構成 (IM 構成) を変更後の環境に移行したりできます。エクス

ポート・インポート機能によってシステムの階層構成を設定する方法については、「[3.6 IM 構成管理の管理情報のインポート・エクスポート](#)」を参照してください。

2.8.3 仮想化システム構成の管理および監視のための設定（UNIX の場合）

IM 構成管理のエクスポート・インポート機能を使用すると、仮想化システム構成の構成定義情報を IM 構成管理で管理したり、仮想化システム構成をセントラルスコープで監視したりできます。仮想化システム構成を管理および監視するための環境を設定する方法については、「[3.3 仮想化システム構成の設定](#)」を参照してください。

2.9 IM 構成管理を使用しない場合のシステムの階層構成の設定 (UNIX の場合)

ここでは、IM 構成管理を使用しない場合のシステムの階層構成 (IM 構成) の設定について説明します。IM 構成管理を使用する場合のシステムの階層構成の設定については、「[2.8 IM 構成管理を使用する場合のシステムの階層構成の設定 \(UNIX の場合\)](#)」を参照してください。

IM 構成管理を使用しない場合は、コマンドを操作して、JP1/IM が運用管理するシステムのマネージャーおよびエージェントの階層関係を設定します。

システムの階層構成は、最上位のマネージャーで一括して定義する方法と、各マネージャーが管理する複数の部分に分割して定義する方法があります。

IM 構成管理を使用してシステムの階層関係を管理している場合は、JP1/Base が提供する構成管理機能の定義ファイルを編集したり、コマンドを実行したりしないでください。

システムの階層構成の管理および構成定義情報の定義例については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「[9.4.3 システムの階層構成の管理](#)」を参照してください。

ここでは、構成定義情報の設定、削除、および変更の手順について説明します。

2.9.1 構成定義情報の設定 (UNIX の場合)

構成定義情報は、次の手順で設定します。

1. マネージャーで、構成定義ファイル (jbs_route.conf) を作成する。

システムを一括して定義する場合はシステム階層構成全体を、分割して定義する場合はそのマネージャーから下位に当たる管理対象ホストおよびマネージャーを、定義ファイルに記述します。

2. マネージャーで、設定コマンド (jbsrt_distrib) を実行する。

コマンドを実行すると、定義情報が更新されます。

システム階層構成を複数の部分に分割して定義する場合は、マネージャーごとに上記の手順を行ってください。そのあとに、最上位のマネージャーで次の手順を実施してシステム全体の定義を作成します。

1. 最上位のマネージャーで、構成定義ファイル (jbs_route.conf) を作成する。

最上位のマネージャーから次の階層のマネージャーまでのシステム階層構成を、定義ファイルに記述します。

2. 最上位のマネージャーで、設定コマンド (jbsrt_sync) を実行する。

なお、構成定義情報の内容を確認するには、各ホスト上で jbsrt_get コマンドを実行してください。

構成定義ファイル、jbsrt_distrib コマンドおよびjbsrt_sync コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

2.9.2 構成定義情報の削除（UNIX の場合）

構成定義情報を一度クリアするなど、定義を削除できます。

1. マネージャーで、構成定義ファイル（jbs_route.conf）を用意する。

構成定義ファイルがない場合は、自ホスト名だけを記述したファイルを作成してください。

既存のファイルがある場合は、そのまま使用します。

2. マネージャーで、設定コマンド（jbsrt_distrib）を実行する。

なお、JP1/Base が停止していて構成定義情報が削除されなかったホストがある場合は、そのホストで jbsrt_del コマンドを実行して構成定義情報を削除します。そのあと、最上位のマネージャーで jbsrt_distrib コマンドを実行してください。

jbsrt_del コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

2.9.3 構成定義情報の変更（UNIX の場合）

構成定義情報を変更する場合は、「[2.9.1 構成定義情報の設定（UNIX の場合）](#)」と同じ手順で設定してください。これにより、変更後の構成定義情報が配布されます。

最上位のマネージャーを変更する場合

システムの最上位のマネージャーを変更する場合は、次の手順で変更してください。

1. 変更前の最上位のマネージャーで、構成定義情報を削除する。

変更前の最上位のマネージャーで、「[2.9.2 構成定義情報の削除（UNIX の場合）](#)」の手順により、構成定義情報を削除します。

2. 変更後の最上位のマネージャーで、構成定義情報を設定する。

変更後の最上位のマネージャーで、「[2.9.1 構成定義情報の設定（UNIX の場合）](#)」の手順により、構成定義情報を設定します。

2.9.4 構成定義情報の設定での注意事項（UNIX の場合）

構成定義情報を配布するときは、各ホストで JP1/Base が動作している必要があります。JP1/Base が停止していた場合の影響と対処方法を説明します。

- JP1/Base が停止していた場合の影響

構成定義情報は、JP1/Base により管理されています。このため、構成定義情報で定義したホストの JP1/Base が停止していると、構成定義情報の配布に失敗します。この場合、次のように対処してください。

1. `jbsrt_distrib` コマンド実行時に KAVB3107-E のメッセージが表示されても、そのまま処理を続行する。

JP1/Base が起動しているホストには構成定義情報が配布されます。

2. 定義を配布できなかったホストの JP1/Base を起動してから、再度 `jbsrt_distrib` コマンドを実行する。

- JP1/Base イベントサービスが停止していた場合の影響

構成定義情報は JP1 イベント転送に関連するため、`jbsrt_distrib` コマンドや `jbsrt_del` コマンドを実行した時に、`jevreload` コマンドが自動的に実行され、イベントサービスの転送設定が更新（リロード）されます。このリロードのとき、イベントサービスが停止していると、構成定義情報が配布されても JP1 イベントの転送先は更新されません。イベントサービスを再起動してください。

なお、構成定義情報については、マニュアル「JP1/Base 運用ガイド」を参照してください。

2.10 イベントサービス機能の設定 (UNIX の場合)

JP1/IM で JP1 イベントにより事象を管理するために、各ホストを設定します。

1. イベントサービス環境の設定をする。

通常はデフォルトの設定のまま運用できますが、例えば、次のような場合は設定をカスタマイズしてください。

- イベント DB の容量を大きくする
- JP1/SES 形式のイベントを JP1/IM で管理する

また、JP1/IM - Manager は、JP1/Base (イベントサービス) からユーザー名 root で JP1 イベントを取得します。同一ホスト上で動作する JP1/Base (イベントサービス) のイベントサーバ設定ファイル (conf) で `users` パラメーターを指定する場合には、root を含める設定としてください。含めなかった場合、JP1/IM - Manager が正常に起動できなくなります。

2. イベント変換機能の設定をする。

ログファイルや SNMP トラップなどを JP1 イベントにより管理する場合は、イベント変換機能の設定をしてください。

設定内容の詳細については、マニュアル「JP1/Base 運用ガイド」のイベントサービス環境の設定の章、およびイベント変換機能の章を参照してください。

❗ 重要

JP1/IM - Manager が動作するホストの API 設定ファイルでは、通信タイプに必ず `keep-alive` を指定してください。通信タイプに `close` を指定すると、JP1/IM - Manager がイベントを 1 件受信するたびに一時ポートを一つ使用するため、一時ポートの不足が発生する場合があります。

❗ 重要

JP1/IM - Manager は、JP1/Base (イベントデーモン) から、ユーザー名 root で JP1 イベントを取得します。同一ホスト上で動作する JP1/Base (イベントデーモン) のイベントサーバ設定ファイルで `users` パラメーターを指定する場合は、root を含める設定としてください。含めなかった場合、JP1/IM - Manager が正常に起動できません。

2.11 IM 構成管理を使用する場合の JP1 イベントの転送設定 (UNIX の場合)

ここでは、IM 構成管理を使用する場合の JP1 イベントの転送設定について説明します。

IM 構成管理を使用する場合は、IM 構成管理・ビューアーを操作して、JP1 イベントの転送設定を実行します。

JP1 イベントの転送設定では、JP1/IM で管理する JP1 イベントを、上位の JP1/IM マネージャーに転送するように、各ホストを設定します。

通常はデフォルトのまま運用できますが、例えば、次のような場合は設定をカスタマイズしてください。

- JP1 イベントの重大度の通知や情報のイベントを JP1/IM で管理する
- JP1/SES 形式のイベントを JP1/IM で管理する

なお、デフォルトの設定では、「[2.8 IM 構成管理を使用する場合のシステムの階層構成の設定 \(UNIX の場合\)](#)」で設定する階層定義に従ってイベントが転送されます。

IM 構成管理を使用する場合、[プロファイル表示/編集] 画面の [設定ファイル] ページで、イベント転送情報の設定ファイルを編集して、イベント転送設定を変更できます。設定ファイルを編集する方法については、「[3.5.1\(5\) 設定ファイルを編集する](#)」を参照してください。

2.12 IM 構成管理を使用しない場合の JP1 イベントの転送設定 (UNIX の場合)

ここでは、IM 構成管理を使用しない場合の JP1 イベントの転送設定について説明します。

IM 構成管理を使用しない場合は、JP1/Base が提供する構成管理機能を使用して、JP1 イベントの転送設定を実行します。

JP1 イベントの転送設定では、JP1/IM で管理する JP1 イベントを、上位の JP1/IM マネージャーに転送するように、各ホストを設定します。

通常はデフォルトのまま運用できますが、例えば、次のような場合は設定をカスタマイズしてください。

- JP1 イベントの重大度の通知や情報のイベントを JP1/IM で管理する
- JP1/SES 形式のイベントを JP1/IM で管理する

なお、デフォルトの設定では、「[2.9 IM 構成管理を使用しない場合のシステムの階層構成の設定 \(UNIX の場合\)](#)」で設定する階層定義に従ってイベントが転送されます。

設定内容の詳細については、マニュアル「JP1/Base 運用ガイド」の転送設定ファイルの詳細の章を参照してください。

2.13 IM 構成管理を使用する場合のイベントサービスの定義情報の収集と配布 (UNIX の場合)

ここでは、IM 構成管理を使用する場合のイベントサービスの定義情報の収集と配布について説明します。

IM 構成管理を使用する場合は、IM 構成管理・ビューアーを操作して、イベントサービスの定義情報の収集と配布を実行します。

JP1/Base と JP1/IM で構成されたシステムでは、バージョン 9 以降の JP1/Base が動作するホストとの間で、マネージャーから複数のホストのイベントサービスの定義情報を一括して収集したり、複数のホストへイベントサービスの定義情報を配布したりできます。そのため、イベントサービスの定義情報を各ホストで確認したり、定義したりすることなく、マネージャー上で各ホストの定義情報を集中的に管理できます。

IM 構成管理を使用する場合に収集、配布できるのは、次の定義情報です。

- 転送設定ファイル
- ログファイルトラップ動作定義ファイル
- ログファイルトラップ起動定義ファイル
- ローカルアクション定義ファイル

IM 構成管理を使用する場合、[IM 構成管理] 画面の [ホスト一覧] ページまたは [IM 構成] ページで、プロファイル（有効設定情報および設定ファイル）の収集を実行して、イベントサービスの定義情報を収集できます。プロファイルを収集する方法については、[「3.5.1\(2\) プロファイルを収集する」](#)を参照してください。

また、IM 構成管理を使用する場合、[IM 構成管理] 画面の [ホスト一覧] ページまたは [IM 構成] ページで、設定ファイルの編集内容の反映を実行して、イベントサービスの定義情報を、JP1/Base が動作するホストに配布できます。設定ファイルの編集内容を反映する方法については、[「3.5.1\(6\) 設定ファイルの編集内容を反映する」](#)を参照してください。

2.14 IM 構成管理を使用しない場合のイベントサービスの定義情報の収集と配布 (UNIX の場合)

ここでは、IM 構成管理を使用しない場合に実行するイベントサービスの定義情報の収集と配布について説明します。この操作は、JP1/IM のシステムの構築で IM 構成管理 DB を使用しない場合に実行します。

IM 構成管理を使用しない場合は、JP1/Base が提供するコマンドを操作して、イベントサービスの定義情報の収集と配布を実行します。

JP1/Base と JP1/IM で構成されたシステムでは、マネージャーから複数のホストの、イベントサービスの定義情報を一括して収集したり、複数のホストへイベントサービスの定義情報を配布したりできます。そのため、イベントサービスの定義情報を各ホストで確認したり、定義したりすることなく、マネージャー上で各ホストの定義情報を集中的に管理できます。

収集方法、配布方法の詳細については、マニュアル「JP1/Base 運用ガイド」のイベントサービスの定義情報の収集と配布の章を参照してください。

2.15 コマンド実行環境の設定 (UNIX の場合)

コマンド実行環境の設定について、管理対象ホストのコマンド実行環境の設定と、クライアントアプリケーションの実行環境の設定に分けて説明します。

2.15.1 管理対象ホストのコマンド実行機能の設定 (UNIX の場合)

自動アクション機能および JP1/IM - View の [コマンド実行] 画面から管理対象ホストのコマンドを実行するときの、コマンド実行環境を設定します。

1. コマンド実行環境の設定

jcocmddef コマンドを実行して、コマンド実行環境を設定します。

コマンド同時実行数の調整をすることを推奨します。この場合は、次のようにコマンドを実行します。

(例) コマンド同時実行数を 3 にする場合

```
/opt/jp1base/bin/jcocmddef -execnum 3
```

2. 環境変数ファイルの作成

コマンド実行の時に環境変数ファイルを使用する場合は、ファイルを作成します。

3. ホストグループの定義

必要に応じて、ホストグループ（同時に複数のホストにコマンド実行を指示するためのグループ）を定義します。

4. コマンドボタン定義ファイルの作成

コマンドを [コマンド] ボタンから実行する場合は、コマンドボタン定義ファイルを作成します。

イベント情報を引き継ぐ場合は、inev パラメーターにtrueを設定してください。

5. イベント引き継ぎ情報変換設定ファイルの作成

自動アクションおよびコマンド実行でイベント情報を引き継ぐ場合、引き継がれるイベント情報に含まれる特定の ASCII 文字を別の文字列に変換するときは、イベント引き継ぎ情報変換設定ファイルを作成します。

なお、コマンド実行環境設定が有効になる契機や、定義ファイルの作成方法などについては、次の説明を参照してください。

コマンド実行環境について

- jcocmddef コマンドについて

参照先：マニュアル「JP1/Base 運用ガイド」のコマンドを説明している章

- 環境変数ファイルの作成について

参照先：マニュアル「JP1/Base 運用ガイド」の環境変数ファイルを説明している章

- ホストグループの定義について
参照先：マニュアル「JP1/Base 運用ガイド」のホストグループの定義ファイルを説明している章
- コマンドボタン定義ファイルの作成について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「コマンドボタン定義ファイル (cmdbtn.conf)」(2. 定義ファイル)
- イベント引き継ぎ情報変換設定ファイルの作成について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベント引き継ぎ情報変換設定ファイル (event_info_replace.conf)」(2. 定義ファイル)

2.15.2 クライアントアプリケーションの実行環境の設定 (UNIX の場合)

JP1/IM - View の「コマンド実行」画面からクライアントアプリケーションを実行するときの、コマンド実行環境を設定します。

1. コマンドボタン定義ファイルの作成

クライアントアプリケーションを「コマンド」ボタンから実行する場合は、コマンドボタン定義ファイルを作成します。

イベント情報を引き継ぐ場合は、`inev` パラメーターに `true` を設定してください。また、`cmdtype` パラメーターに `client` を設定してください。

2. イベント引き継ぎ情報変換設定ファイルの作成

自動アクションおよびコマンド実行でイベント情報を引き継ぐ場合、引き継がれるイベント情報に含まれる特定の ASCII 文字を別の文字列に変換するときは、イベント引き継ぎ情報変換設定ファイルを作成します。

なお、コマンド実行環境設定が有効になる契機や、定義ファイルの作成方法などについては、次の説明を参照してください。

コマンド実行環境について

- コマンドボタン定義ファイルの作成について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「コマンドボタン定義ファイル (cmdbtn.conf)」(2. 定義ファイル)
- イベント引き継ぎ情報変換設定ファイルの作成について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベント引き継ぎ情報変換設定ファイル (event_info_replace.conf)」(2. 定義ファイル)

2.16 イベントサービスの登録ホスト名を FQDN 形式で利用する場合の設定 (UNIX の場合)

JP1/IM - Manager はイベントサービスの登録ホスト名を FQDN 形式で利用する運用に対応しています。イベントサービスの登録ホスト名を FQDN 形式で利用することで、複数のドメインで構成されたシステムで JP1 イベントを監視できます。

ここでは、マネージャー上のイベントサービスの登録ホスト名を FQDN 形式で利用する場合の前提条件、設定方法、および起動方法について説明します。エージェント上のイベントサービスの登録ホスト名を FQDN 形式で利用する場合、ここで説明する設定は不要です。

2.16.1 前提条件 (UNIX の場合)

JP1/IM ホスト上の JP1/Base イベントサービスの登録ホスト名を FQDN 形式で利用する場合は、次の前提条件を満たす必要があります。

- 物理ホストの環境であること。
- JP1/IM - Manager ホスト上で `hostname` コマンドを実行して、ショートネーム形式のホスト名が返されること。

2.16.2 設定方法 (UNIX の場合)

JP1/IM - Manager を自動的に起動するためのコマンドである `jco_start` を編集します。`jco_start` コマンドは、JP1/IM - Manager を起動する前に JP1/Base の起動確認をしています。FQDN 形式のイベントサーバを利用する場合、FQDN 形式のイベントサーバの起動確認を行う必要があります。JP1/Base で FQDN 形式のイベントサーバを設定後、次の手順で `jco_start` コマンドを編集してください。

1. `jco_start.model` を任意の名称でコピーする。

```
cd /etc/opt/jp1cons
cp -p jco_start.model 任意の名称
```

2. 1.でコピーしたスクリプトをテキストエディターで開き、次のように編集する。

変更前：`EVS_HOST=`hostname``

変更後：`EVS_HOST=FQDN 形式ホスト名`

FQDN 形式のイベントサーバの設定については、マニュアル「JP1/Base 運用ガイド」の次の説明を参照してください。

- DNS を使ったシステムでのイベントサーバの設定
- イベントサービスの注意事項

2.16.3 起動方法 (UNIX の場合)

通常の起動方法と同じです。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3.1.2 UNIX の場合」を参照してください。

2.17 リモートの監視対象ホストでログ監視をするための設定 (UNIX の場合)

ここでは、リモートの監視対象ホストでログ監視をするための SSH の設定について説明します。

なお、リモートの監視対象ホストから収集できるログの種別とリモート通信の接続方法については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「13.5.2 リモート監視構成の管理」を参照してください。

また、リモートの監視対象ホストを IM 構成管理に登録する手順については、「[3.1 ホストの登録](#)」を参照してください。

メモ

リモート監視が停止している間にリモート監視対象ホストで出力されたログ情報を収集できません。リモート監視が停止中に出力されたログ情報を収集するかどうかは、リモートログトラップ環境定義ファイル (`jp1cf_remote_logtrap.conf`) の `START_OPTION` パラメーターで指定します。なお、新規にインストールした場合は、有効です。11-01 以前からバージョンアップした場合は無効です。必要に応じて、リモートログトラップ環境定義ファイルを設定してください。

リモートログトラップ環境定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「リモートログトラップ環境定義ファイル (`jp1cf_remote_logtrap.conf`)」(2. 定義ファイル)を参照してください。

2.17.1 SSH の設定 (UNIX の場合)

ここでは、JP1/IM - Manager ホストが UNIX 環境である場合の、SSH の設定について説明します。なお、SSH の認証には、公開鍵認証方式を使用します。

SSH で接続するには次の設定が必要となります。

- SSH サーバを設定する
リモートの監視対象ホストで設定します。
- 鍵を作成する
UNIX 環境の JP1/IM - Manager ホストで設定します。
- 公開鍵を監視対象ホストに配置する
リモートの監視対象ホストで設定します。
- 監視対象のログファイルへのアクセス権を設定する
監視対象ホストが UNIX の場合は、マネージャーストから監視対象ホストに SSH 接続するユーザーにアクセス権を設定します。

❗ 重要

対話環境が前提である `stty`, `tty`, `tset`, `script` コマンドなどは、SSH 接続ユーザーのログインスクリプトに記載しないでください。記載されている場合は、リモート監視用に SSH 接続ユーザーを新たに作成するか、これらのコマンドを実行しないように SSH 接続ユーザーのログインスクリプトを変更してください。

(1) SSH サーバを設定する

SSH サーバを設定するための手順を次に示します。なお、OS の設定やコマンドは、OS のバージョンによって異なる可能性があります。詳細は、各 OS のマニュアルおよび JP1/IM - Manager のリリースノートを参照してください。

1. リモートの監視対象ホストに root 権限のユーザーでログインする。

2. `sshd_config` を開く。

Linux, AIX の場合：`/etc/ssh/sshd_config`

3. `PubkeyAuthentication` の値を `yes` に設定する※1。

4. `UseDNS` を `no` に設定する※1, ※2。

5. `PermitRootLogin` を `yes` に設定する※1。

root 権限のユーザーでログインして情報収集する場合だけ、この手順を実行してください。

6. 次のコマンドを実行し、`sshd` サービスを再起動する。

実行するコマンドの例を、OS ごとに次に示します。

- Linux の場合 (Linux 9 の例)
`systemctl restart sshd.service`
- AIX の場合 (AIX 7.3 の例)
`stopsrc -s sshd`
`startsrc -s sshd`

注※1

`sshd_config` の設定項目および設定方法については、使用する SSH サーバのマニュアルを参照してください。

注※2

設定しない場合は、監視対象ホストで次の名前解決ができるように設定してください。

- マネージャーホストの IP アドレスからマネージャーホスト名を解決できる
- マネージャーホストのホスト名の解決先 IP アドレスが、マネージャーホストの IP アドレスと一致する

名前解決に DNS を使用していて DNS サーバに接続できない場合、リモート監視ログファイルトラップの起動、またはログファイルの収集が遅延することがあります。また、遅延によってタイムアウトしてしまい、起動や収集が失敗することがあります。そのため、UseDNS をno に設定することを推奨します。

(2) 鍵を作成する（初めて鍵を作成する場合）

UNIX 環境の JP1/IM - Manager ホストに root 権限のユーザーでログインし、ssh-keygen コマンドを実行して鍵を作成します。なお、この手順は、初めて鍵を作成する場合だけに必要な作業です。

鍵の種類は RSA 暗号と DSA 暗号のどちらかを選択できます。

1.root 権限のユーザーでログインする。

2. ssh-keygen コマンドを実行する。

次のように入力してコマンドを実行してください。

- RSA 鍵を作成する場合：ssh-keygen -t rsa
- DSA 鍵を作成する場合：ssh-keygen -t dsa

3. 秘密鍵の出力先と名前を決める。

マルチバイト文字を含まないパスとファイル名を指定してください。デフォルトは「`~/.ssh/id_rsa`」が設定されます。

4. リターンキーを 2 回押す。

秘密鍵のパスフレーズの入力を求められるため、何も入力しないでリターンキーを押します。再入力を求められるので、何も入力しないで再度リターンキーを押します。

ssh-keygen -t rsa コマンドの実行例を次に示します。

```
[root@HOST]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ssh-user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ssh-user/.ssh/id_rsa.
Your public key has been saved in /home/ssh-user/.ssh/id_rsa.pub.
The key fingerprint is:
ax:xx:xx:xx:xx:bx:xx:xc:xx:xx:xx:xd:xd:xa:ed:xx root@HOST
```

注意事項

- 秘密鍵の情報は厳重に管理してください。また、秘密鍵ファイルが管理者権限の無い OS ユーザーにアクセスされないよう、適切なアクセス権限を付与してください。
- 鍵（公開鍵と秘密鍵のペア）の作成は環境やツールには依存しないため、どのような環境やツールでも問題ありません。ただし、鍵の作成後は、秘密鍵と公開鍵を適切に配置する必要があります。

(3) 公開鍵をリモートの監視対象ホストに配置する

「2.17.1(2) 鍵を作成する (初めて鍵を作成する場合)」で作成した公開鍵をリモートの監視対象ホストに配置します。配置する手順を次に示します。

なお、作業を始める前に、ssh ディレクトリの上位ディレクトリのパーミッションに所有者以外の書き込み権限が設定されていないことを確認してください。所有者以外の書き込み権限が設定されていると SSH の接続に失敗します。

1. リモートの監視対象ホストにリモート監視で使用するユーザーでログインする。

2. .ssh ディレクトリに移動する。

リモート監視で使用するユーザーのホームディレクトリ配下に .ssh ディレクトリがない場合は作成してください。ディレクトリの属性は 700 を設定してください。

3. scp コマンドを実行し、公開鍵ファイルをリモートの監視対象ホストにコピーする。

「2.17.1(2) 鍵を作成する (初めて鍵を作成する場合)」で作成済みの公開鍵ファイルを監視対象ホストにコピーします。公開鍵のコピー先は、リモート監視で使用するユーザーのホームディレクトリの .ssh ディレクトリです。

4. cat コマンドを実行し、公開鍵ファイルの内容を認証鍵ファイルに追加する。

5. コピーした公開鍵ファイルを削除する。

6. chmod コマンドを実行し、認証鍵ファイルの属性を 600 に変更する。

7. [/etc/ssh/sshd_config] の [AuthorizedKeysFile] を設定する。

デフォルトでは「~/ssh/authorized_keys」または「.ssh/authorized_keys」が設定されています。手順 6 で作成した認証鍵のパスを変更した場合は、AuthorizedKeysFile の値を見直してください。なお、sshd_config の設定を変更した場合は、スーパーユーザーで sshd サービスを再起動してください。

scp コマンド、cat コマンドおよび chmod コマンドの実行例を次に示します。ここでは、「2.17.1(2) 鍵を作成する (初めて鍵を作成する場合)」で鍵を作成した JP1/IM - Manager ホストのホスト名を IMHost としています。

- コマンドの実行例

```
[ClientUser@TargetHost]$ cd .ssh
[ClientUser@TargetHost .ssh]$ scp root@IMHost:/home/ssh-user/.ssh/id_rsa.pub ./
root@IMHost's password: <パスワードを入力>
id_rsa.pub 100% 233 0.2KB/s 00:00
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ rm id_rsa.pub
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

(4) 監視対象のログファイルへのアクセス権を設定する

監視対象ホストが UNIX の場合は、マネージャーホストから監視対象ホストに SSH 接続するユーザーは、次に示すアクセス権が必要です。

- 監視対象のログファイル
読み込み権限が必要です。監視対象のログファイルが SEQ2 形式の場合は、監視対象のログファイルの退避ファイルにも読み込み権限が必要です。
- 監視対象のログファイルがあるディレクトリおよびその上位のすべてのディレクトリ
読み込み権限と実行権限が必要です。監視対象のログファイルが SEQ2 形式の場合は、監視対象のログファイルの退避ファイルがあるディレクトリおよびその上位のすべてのディレクトリに読み込み権限と書き込み権限が必要です。

(5) 接続を確認する

JP1/IM - Manager ホストとリモートの監視対象ホストが接続できるかどうかを確認する手順について説明します。

1. JP1/IM - Manager ホストに root 権限のユーザーでログインする。
2. 作成した秘密鍵を利用し、リモートの監視対象ホストに対して ssh コマンドを実行する。

何も入力しないで接続に成功したら、SSH の設定は完了です。

エラーが発生した場合や、パスワードおよびパスフレーズの入力を要求された場合は、手順どおり正しく設定できているかどうかを見直してください。また、OS の設定を見直し、SSH 接続ができる環境であるか確認してください。

接続を確認するときの ssh コマンドの実行例を次に示します。

ここでは、JP1/IM - Manager ホストのホスト名を IMHost としています。また、監視対象ホストのホスト名を TargetHost、リモート監視で使用するユーザー名を ssh-user としています。

- コマンドの実行例

```
[root@IMHost]$ /usr/bin/ssh -i /home/ssh-user/.ssh/id_rsa -p 22 ssh-user@TargetHost
The authenticity of host 'TargetHost (xxx.xxx.xxx.xxx)' can't be established.
RSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'TargetHost,xxx.xxx.xxx.xxx' (RSA) to the list of known hosts.
Last login: Mon Mar 23 17:17:52 2011 from xxx.xxx.xxx.xxx
[ssh-user@TargetHost ~]$ exit
logout
Connection to TargetHost closed.
```

```
[root@IMHost]$
```

また、リモート監視では、リモートの監視対象ホストで次のコマンドを実行します。リモート監視で使用するユーザーで次のコマンドが実行できることを確認してください。

- `uname`
- `ls`
- `wc`
- `tail`
- `find`
- `grep`
- `head`

コマンドを実行できるか確認する際の手順を、次に示します。

(a) ホスト情報を収集する場合に使用するコマンドの確認

1. [システム共通設定] 画面の [SSH] ページで設定したユーザーで監視対象ホストにログインする。
2. 次のコマンドを実行し、戻り値が0であることを確認する。

```
uname -s
```

(b) ログファイルを収集する場合に使用するコマンドの確認

1. [システム共通設定] 画面の [SSH] ページで設定したユーザーで監視対象ホストにログインする。
2. 次のコマンドを実行し、戻り値が0であることを確認する。

- `ls -ild` 監視対象のログファイルパス

コマンドの例：

```
ls -ild /var/log/messages
```

実行結果の例：

```
12345 -rw-r--r-- 1 root root 100 4月 12 13:00 2013 messages
```

- `ls` 監視対象のログファイルが存在するディレクトリパス

コマンドの例：

```
ls /var/log
```

実行結果の例：

```
messages
```

- (監視対象ホストの OS が AIX の場合) `LC_CTYPE=C wc -l` 監視対象のログファイルパス

コマンドの例：

```
LC_CTYPE=C wc -l /var/log/messages
```

実行結果の例：

```
20 /var/log/messages
```

- (監視対象ホストの OS が Linux の場合) `wc -l` 監視対象のログファイルパス

コマンドの例：

```
wc -l /var/log/messages
```

実行結果の例：

```
20 /var/log/messages
```

- `tail -n +監視対象のファイルの任意の行番号 監視対象のログファイルパス | tail -c 収集するサイズの上限值`

コマンドの例：

```
tail -n +19 /var/log/messages | tail -c 10241
```

実行結果の例：

```
line num = 19
```

```
line num = 20
```

3. ログファイルの出力形式が SEQ2 の場合、手順 2 のコマンドに加えて、次のコマンドを実行し、標準出力の結果を確認する。

- `find 監視対象のログファイルが存在するディレクトリパス -xdev -inum 監視対象のログファイルの退避ファイルのinode`

コマンドの例：

```
find /var/log/ -xdev -inum 12345
```

標準出力の例：

```
/var/log/messages.1
```

標準出力の結果として、監視対象のログファイルの退避ファイルのパスが出力されることを確認してください。

標準出力を確認する場合に、標準出力を `stdout.txt` にリダイレクトして標準エラー出力を `stderr.txt` にリダイレクトするときは、次のように実行してください。

コマンドの例：

```
find /var/log/ -xdev -inum 12345 1> stdout.txt 2> stderr.txt
```

(c) 事前フィルターを適用する場合に使用するコマンドの確認

1. [システム共通設定] 画面の [SSH] ページで設定したユーザーで監視対象ホストにログインする。

2. 次のコマンドを実行し、戻り値が 0 であることを確認する。

- (監視対象ホストの OS が Linux の場合) `/bin/grep -E '事前フィルター'`

コマンドの例：

```
tail -n +19 /var/log/messages | /bin/grep -E 'filter' | tail -c 10241
```

実行結果の例：

line num = 19

line num = 20

- (監視対象ホストの OS が AIX の場合) /usr/bin/grep -E '事前フィルター'

コマンドの例：

```
tail -n +19 /var/log/messages | /usr/bin/grep -E 'filter' | tail -c 10241
```

実行結果の例：

line num = 19

line num = 20

- head -n 監視対象ファイルの任意の行番号

コマンドの例：

```
tail -n +19 /var/log/messages | head -n 20
```

実行結果の例：

line num = 19

line num = 20

2.17.2 1 回の監視間隔で収集できるログのサイズの設定 (UNIX の場合)

事前フィルターを適用しても、1 回の監視間隔で収集できるログのサイズの上限が超えてしまう環境では、1 回の監視間隔で収集できるログのサイズの上限の初期値を変更することができます。

変更する場合は、次の手順で設定します。

1. リモート監視ログファイルトラップ機能とリモート監視のイベントログトラップ機能の実行環境を設定する。

リモートログトラップ環境定義ファイル (jp1cf_remote_logtrap.conf) を編集します。

```
/etc/opt/jp1imm/conf/imcf/jp1cf_remote_logtrap.conf
```

2. jbssetcnf コマンドを実行して、定義内容を反映する。

```
/opt/jp1base/bin/jbssetcnf /etc/opt/jp1imm/conf/imcf/jp1cf_remote_logtrap.conf
```

3. JP1/IM - Manager を再起動する。

再起動後に設定内容が反映されます。

1 回の監視間隔で収集できるログのサイズの設定について

- リモートログトラップ環境定義ファイル (jp1cf_remote_logtrap.conf)

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「リモートログトラップ環境定義ファイル (jp1cf_remote_logtrap.conf)」(2. 定義ファイル)

2.18 JP1/IM - Manager のセットアップ (UNIX の場合)

ここでは、JP1/IM - Manager のセットアップ項目について説明します。

なお、セットアップ作業を行うユーザーは、root 権限が必要です。

2.18.1 セットアッププログラムの実行 (UNIX の場合)

JP1/IM - Manager をインストールしたあと、セットアッププログラムを実行します。

1. セットアッププログラムを実行する。

- /opt/jp1cons/bin/jp1cc_setup
- /opt/jp1scope/bin/jp1cs_setup
- /opt/jp1imm/bin/imcf/jp1cf_setup

なお、セットアッププログラムは、実行が必要な場合と、不要な場合があります。

- セットアッププログラムの実行が必要な場合
JP1/Base をアンインストールして、再インストールした場合
- セットアッププログラムの実行が不要な場合
JP1/IM - Manager を新規インストールした場合
同バージョンの JP1/IM - Manager を上書きインストールした場合

2.18.2 自動起動および自動終了の設定 (UNIX の場合)

ホストの起動・終了時に JP1/IM - Manager を自動的に起動・終了するためには、次の操作をします。

なお、自動起動・終了スクリプトでは、デフォルトでは環境変数 LANG に C が設定されています。スクリプト実行時の出力メッセージの言語を変更したい場合は、スクリプト内の環境変数 LANG を設定している行を編集してください。

(1) Linux の場合

1. 自動起動、自動終了のスクリプトをコピーする。

```
# cd /etc/opt/jp1cons
# cp -p jco_start.model jco_start
# cp -p jco_stop.model jco_stop
```

2. インストールとセットアップ (UNIX の場合)

(a) サービスの自動起動での注意事項

Linux 環境で JP1/IM - Manager の自動起動および自動終了を設定し有効にしている場合に、JP1/IM - Manager を手動で起動したり停止したりするときは、次のコマンドを実行してください。JP1/IM - Manager のプロセス群の起動状態は、`jco_spmc_status` コマンドで確認できます。IM データベースを使用している場合、IM データベースの稼働状態は `jimdbstatus` コマンドで確認できます。

- JP1/IM - Manager の起動

物理ホストの場合

```
systemctl start jp1_cons.service
```

論理ホストの場合

```
systemctl start jp1_cons_論理ホスト名.service
```

- JP1/IM - Manager の停止

物理ホストの場合

```
systemctl stop jp1_cons.service
```

論理ホストの場合

```
systemctl stop jp1_cons_論理ホスト名.service
```

JP1/IM - Manager の自動起動・自動停止が有効の場合、`systemctl` コマンド以外の、`jco_start` コマンド、`jco_start.cluster` コマンドで起動したり、`jco_stop` コマンド、`jco_stop.cluster` コマンドで停止したりすると、JP1/IM - Manager の自動停止が実行されません（システムの停止時に停止スクリプトは起動されませんが、自動起動・自動停止の設定は有効のままです）。

システム停止時に JP1/IM - Manager を自動停止させる場合は、再度 `systemctl` コマンドで起動操作をしてください。JP1/IM - Manager が自動停止するかどうかは、次のコマンドを実行して、「active」が表示されることを確認してください。

物理ホストの場合

```
systemctl is-active jp1_cons.service
```

論理ホストの場合

```
systemctl is-active jp1_cons_論理ホスト名.service
```

(b) syslog での注意事項

`systemd` パッケージがインストールされている Linux の場合、自動起動および自動終了の設定を行っていない状態※1 で、システムの起動、およびシステムの終了が行われると、`syslog` に次のメッセージが出力されます。

次のメッセージは出力されるが、設定が行われていないため、自動起動および自動終了は行われません。JP1/IM - Manager サービスのステータスは `jco_spmc_status` コマンドで確認する必要があります。

- `syslog` に出力されるメッセージ※2

起動時：systemd: Started JP1/Integrated Management - Manager Service.

注※1

自動起動および自動終了の設定を行っていない状態とは、次のファイルが存在しない場合を指します。

/etc/opt/jp1cons/jco_start

/etc/opt/jp1cons/jco_stop

注※2

非クラスタシステムでの論理ホストの自動起動および自動終了する場合は、論理ホスト用に作成した自動起動および自動終了スクリプトのDescription に指定したサービス名がメッセージに表示されます。

例

起動時：systemd: Started JP1/Integrated Management - Manager 論理ホスト名 Service.

(c) 自動終了の注意事項

JP1/IM - Manager を自動終了させるように設定した場合は、次の点に注意してください。

- JP1/IM - Manager の自動終了はランレベルが 0 または 6 に変更されたときにのみ実行されるため、ランレベルをシングルユーザモードに変更した場合などは自動的に停止しません。
- JP1/IM - Manager 起動中にランレベルを変更する場合は、必要に応じて JP1/IM -Manager を停止するか、以下のコマンドを実行して JP1/IM - Manager の自動停止スクリプトを設定してください。

```
ln -s /etc/rc.d/init.d/jp1_cons /etc/rc.d/rc<ランレベル>.d/K01_JP1_80_CONS
```

2.18.3 JP1/IM - Manager の設定ファイルの編集について（UNIX の場合）

Windows の場合と同じです。「[1.19.1 JP1/IM - Manager の設定ファイルの編集について（Windows の場合）](#)」を参照してください。

2.18.4 インテリジェント統合管理基盤の機能を使用するための設定（UNIX の場合）

JP1/IM - Manager を新規インストールした場合、インテリジェント統合管理基盤の機能はデフォルトで無効になっています。

インテリジェント統合管理基盤の機能を使用する場合は、次の手順に従ってください。

1. 統合監視 DB を設定する。
2. インテリジェント統合管理データベースを設定する。
3. 発生元ホストのマッピングを有効にする。

jcoimdef -hostmap ON を実行します。

4. インテリジェント統合管理基盤サービス (jddmain) を有効にする。

jcoimdef -dd ON を実行します。

5. JP1/IM - Manager を起動する。

6. インテリジェント統合管理基盤サービスの稼働を確認する。

jco_spmd_status コマンドを実行します。稼働中のプロセスに jddmain が表示されていることを確認してください。

統合監視 DB については、「[2.4.2 統合監視 DB の設定 \(UNIX の場合\)](#)」を参照してください。

インテリジェント統合管理データベースについては、「[2.5.2 インテリジェント統合管理データベースの設定 \(UNIX の場合\)](#)」を参照してください。

jcoimdef コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

❗ 重要

インテリジェント統合管理基盤の設定を行うと、JP1/IM3-Manager サービスの起動時間が延びます。クラスタソフトで JP1/IM3-Manager サービスの起動時間を監視している場合や JP1/Base の起動管理機能で JP1/IM3-Manager サービスを起動している場合は、クラスタソフトのタイムアウト値を見直す必要があります。インテリジェント統合管理基盤を設定したあとでサービスの起動時間を確認し、タイムアウト値を調整してください。

2.18.5 エージェントとして JP1/IM - Agent を使用する場合の設定

(1) 統合エージェント管理基盤のサービスの設定

(a) 自動起動の設定

JP1/IM - Manager の自動起動の設定に準じます。JP1/IM - Manager の自動起動の設定については、「[2.18.2 自動起動および自動終了の設定 \(UNIX の場合\)](#)」を参照してください。

(2) 統合エージェント管理基盤の設定変更

(a) 共通の設定方法

■ 設定ファイルを編集する

「[1.19.3\(1\)\(a\) 共通の設定方法](#)」の「設定ファイルを編集する (Windows の場合)」を参照してください。

(b) 統合エージェント管理基盤の設定変更

「1.19.3(1)(b) 統合エージェント管理基盤の設定変更 (Windows の場合)」を参照してください。

(c) IM 管理ノードのツリー情報の作成と反映 (必須)

「1.19.3(1)(c) IM 管理ノードのツリー情報の作成と反映 (Windows の場合) (必須)」を参照してください。

(d) 製品プラグインの設定

「1.19.3(1)(d) 製品プラグインの設定 (Windows の場合)」を参照してください。

2.18.6 JP1/IM - Agent パッケージの登録 (UNIX の場合)

JP1/IM のマネージャーホストに、JP1/IM - Agent のパッケージ (以降、JP1/IM - Agent パッケージと呼びます) を登録できます。複数のバージョンの JP1/IM - Agent パッケージを登録することもできます。

JP1/IM - Agent の提供媒体を使用せずに、JP1/IM のマネージャーホストに登録された JP1/IM - Agent パッケージをダウンロードして、エージェントホストに JP1/IM - Agent をインストールできます。

なお、JP1/IM - Agent パッケージの登録は任意です。

(1) JP1/IM - Agent パッケージの登録方法

JP1/IM のマネージャーホストに JP1/IM - Manager をインストールすると、同梱されている JP1/IM - Agent パッケージが自動的に登録されます。

❗ 重要

マネージャーホストに登録された JP1/IM - Agent パッケージをダウンロードできるようにするには、インテリジェント統合管理基盤のセットアップが必要です。

マネージャーホストに JP1/IM - Manager をバージョンアップインストールした場合、すでにインストールされている旧バージョンの JP1/IM - Agent パッケージは、削除されます。

(2) JP1/IM - Agent パッケージの削除方法

マネージャーホストに登録された JP1/IM - Agent パッケージを削除したい場合は、次に示す JP1/IM - Agent パッケージの登録場所のファイルを削除します。

表 2-6 JP1/IM - Agent パッケージの登録場所（統合マネージャーホスト（Linux の場合））

OS	JP1/IM - Agent パッケージ		
	登録場所	ファイル名	製品名
Linux	/opt/jplimm/public/download/ imagent/	jp1_pc_agent_windows_JP1/IM - Agent のバージョン番号（VVRSS 形式）.zip	JP1/IM - Agent（Windows 版）
		jp1_pc_agent_linux_JP1/IM - Agent のバージョン番号（VVRSS 形式）.tar.gz	JP1/IM - Agent（Linux 版）

(3) JP1/IM - Agent パッケージのダウンロードの手順

JP1/IM - Agent パッケージをダウンロードする手順を、次に示します。

■前提条件

- マネージャーホストに JP1/IM - Agent パッケージが登録されている
- インテリジェント統合管理基盤のセットアップが完了している
- ログインに使用する JP1 ユーザーに必要な権限が割り当てられている

■手順

1. ファイルダウンロードの REST API を実行して、JP1/IM - Agent パッケージをダウンロードする。

JP1/IM - Manager から配布物を取得（ファイルダウンロード）するには、JP1 ユーザーの認証が必要です。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.2.8 REST API の認証方法」を参照してください。

OSS の curl コマンドを利用して、ファイルダウンロードの REST API でファイルを取得する場合の使用例を、次に示します。

```
curl -OL -H "Authorization: Bearer トークン" -H "Cookie: JSESSIONID=セッションID" -v http://JP1/IM - Managerホスト名:20703/download/imagent/ファイル名
```

トークンおよびセッション ID は、ログインの REST API を発行して取得します。

```
curl -X POST -H "Content-Type: application/json" -d '{"user": "ユーザー名", "password": "パスワード"}' -v http://JP1/IM - Managerホスト名:20703/im/api/v1/login
```

なお、ファイルの取得完了後は、速やかにログアウトの REST API を発行することを推奨します。

```
curl -X POST -H "Content-Type: application/json" -H "Cookie: JSESSIONID=セッションID" -v http://JP1/IM - Managerホスト名:20703/im/api/v1/logout
```

2. ダウンロードした JP1/IM - Agent パッケージを解凍する。

- Windows 版の場合

PowerShell を使用して、次のコマンドを実行します。

```
Expand-Archive -Path jpl_pc_agent_windows_JP1/IM - Agentのバージョン番号 (VRRSS形式).zip
```

- Linux 版の場合

シェルを使用して、次のコマンドを実行します。

```
tar -zxvf jpl_pc_agent_linux_JP1/IM - Agentのバージョン番号 (VRRSS形式).tar.gz
```

2.18.7 セントラルスコープの機能を使用するための設定（UNIX の場合）

JP1/IM - Manager を新規インストールした場合、セントラルスコープの機能はデフォルトで無効になっています。

セントラルスコープの機能を使用する場合は、次の手順に従ってください。

1. セントラルスコープのデータベースを作成する。

jcsdbsetup コマンドを実行します。

2. セントラルスコープサービス（jcsmain）を有効にする。

jcoimdef -s ON を実行します。

3. JP1/IM - Manager を再起動する。

4. セントラルスコープサービスの稼働を確認する。

jco_spmd_status コマンドを実行します。稼働中のプロセスにjcsmainが表示されていることを確認してください。

jcsdbsetup コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcsdbsetup」（1. コマンド）を参照してください。

jcoimdef コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」（1. コマンド）を参照してください。

2.18.8 SELinux に関する設定（UNIX の場合）

ここでは、Linux 8 以降の SELinux が有効な環境で、JP1/IM - Manager を動作させるための手順について説明します。

なお、SELinux セキュリティコンテキストの設定・解除では、semanage fcontext コマンドとrestorecon コマンドを使用します。

(1) 自動起動および自動停止の設定

SELinux を有効にしている場合は、jco_start およびjco_stop の SELinux セキュリティコンテキストのコンテキストタイプをbin_t に設定する必要があります。

設定手順は次のとおりです。

```
# semanage fcontext -a -t bin_t '/etc/opt/jplcons/jco_start'
# semanage fcontext -a -t bin_t '/etc/opt/jplcons/jco_stop'
# restorecon -F /etc/opt/jplcons/jco_start
# restorecon -F /etc/opt/jplcons/jco_stop
```

(2) IM データベースの設定

SELinux を有効にしている場合は、IM データベースのインストール先ディレクトリ配下のファイルに対し、SELinux セキュリティコンテキストを設定する必要がありますが、IM データベースの構築、更新、削除で使用する各コマンドの内部処理で自動的に行います。ユーザーの手動による個別の設定は不要です。

また、SELinux セキュリティコンテキストの設定や解除は、SELinux の有効無効の状態に関わらず行われますが、IM データベースの構築後の運用中に、SELinux の有効無効の状態を変更した場合も同様に、ユーザーによる設定・解除の操作は不要です。

なお、SELinux セキュリティコンテキストの設定に失敗した場合、SELinux が無効状態でも以降の動作に問題がないため、エラーで中断せずに続行します。そのあと、SELinux を有効状態に変更した場合、IM データベースの起動時（IM データベースに関する各コマンド内部での起動を含む）にエラーとなります。この場合は、エラーメッセージの対処に従って、SELinux セキュリティコンテキストの再設定 (jimdbupdate コマンドの実行) を行ってください。

- SELinux セキュリティコンテキストの設定・解除の契機
IM データベースの SELinux セキュリティコンテキストの設定・解除の契機を、次に示します。

表 2-7 IM データベースに対する設定・解除の契機

契機	対応コマンド	区分	説明
新規構築	- jcodbsetup - jcfdbsetup	設定	SELinux の有効無効の状態に関わらず、コマンド実行時に自動的に SELinux セキュリティコンテキストの設定を行います。 コマンド実行時点で、組み込み HiRDB が未インストールの場合に設定を行います（統合監視 DB または IM 構成管理 DB のどちらかがセットアップ済みの場合はスキップします）。 SELinux が無効状態の場合、SELinux セキュリティコンテキストの設定に失敗しても以降の動作に問題がないため、エラーにせず続行します。そのあと、SELinux を有効状態に変更した場合、IM データベースの起動時（各コマンド内部での起動を含む）でエラーとなります。この場合は、エラー

契機	対応コマンド	区分	説明
			メッセージの対処に従って、SELinux セキュリティコンテキストの再設定 (jimdbupdate コマンドの実行) を行ってください。
更新	jimdbupdate	設定または再設定	SELinux の有効無効の状態に関わらず、コマンド実行時に自動的に SELinux セキュリティコンテキストの設定または再設定を行います。 HiRDB のバージョンアップやスキーマの変更がない場合も、SELinux セキュリティコンテキストの設定を行います。
削除	• jcodbunsetup • jcfdbunsetup	解除	SELinux の有効無効の状態に関わらず、コマンド実行時に自動的に SELinux セキュリティコンテキストの解除を行います。 コマンド実行時点で、組み込み HiRDB がインストール済み、かつ、IM 構成管理 DB が未セットアップの場合に解除を行います (統合監視 DB または IM 構成管理 DB のどちらかが未セットアップの場合はスキップします)。

- JP1/IM - Manager を 13-00 より前のバージョンから 13-00 以降にバージョンアップする場合の注意事項

IM データベースがセットアップされた状態で、JP1/IM - Manager を 13-00 より前のバージョンから 13-00 以降へバージョンアップする場合は、SELinux を有効状態にする前に、必ず jimdbupdate コマンドを実行し、IM データベースをアップデートする必要があります。

JP1/IM - Manager の 13-00 より前のバージョンでは、IM データベースに SELinux セキュリティコンテキストが設定されないため、jimdbupdate コマンドを実行するまでは、SELinux セキュリティコンテキストが設定されていない状態のままとなります。そのため、この状態で SELinux を有効状態にすると、IM データベースの起動に失敗し、jimdbupdate コマンドの実行を促すエラーメッセージが表示されます。

- SELinux セキュリティコンテキストの設定対象ディレクトリ

IM データベースのインストール先ディレクトリを「/var/opt/jp1imm/dbms/JM0」（物理ホスト用の IM データベースのデフォルトのパス※）に仮定した場合の、SELinux セキュリティコンテキストが設定される対象ディレクトリと配下のファイルに設定する SELinux セキュリティコンテキストのタイプ、次に示します。

注※ パスは必要に応じて読み替えてください。

対象ディレクトリ	配下のファイルに設定する SELinux セキュリティコンテキストのタイプ
/var/opt/jp1imm/dbms/JM0 配下	user_t
/var/opt/jp1imm/dbms/JM0/bin 配下	bin_t
/var/opt/jp1imm/dbms/JM0/lib 配下	lib_t
/var/opt/jp1imm/dbms/JM0/bin/servers 配下	bin_t

なお、IM データベースのインストール先ディレクトリのパスは、物理ホスト用と論理ホスト用で、次のように異なります。

- 物理ホストの場合

物理ホスト用の IM データベースのセットアップに使用するセットアップ情報ファイル (jimdbsetupinfo.conf) の定義に従います。パスは「IMDBENVDIR の値/JM0」となります。

- 論理ホストの場合

論理ホスト用の IM データベースのセットアップに使用するクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) の定義に従います。パスは「IMDBENVDIR の値/JMLOGICALHOSTNUMBER の値」となります。

(3) インテリジェント統合管理データベースの設定

SELinux を有効にしている場合は、インテリジェント統合管理データベースのインストール先ディレクトリ配下のファイルに対し、SELinux セキュリティコンテキストを設定する必要がありますが、インテリジェント統合管理データベースの構築、更新、削除で使用する各コマンドの内部処理で自動的に行います。ユーザーの手動による個別の設定は不要です。

また、SELinux セキュリティコンテキストの設定や解除は、SELinux の有効無効の状態に関わらず行われますが、インテリジェント統合管理データベースの構築後の運用中に、SELinux の有効無効の状態を変更した場合も同様に、ユーザーによる設定・解除の操作は不要です。

なお、SELinux セキュリティコンテキストの設定に失敗した場合、SELinux が無効状態でも以降の動作に問題がないため、エラーで中断せずに続行します。また、SELinux を有効状態に変更してもエラーとなりません。

- SELinux セキュリティコンテキストの設定・解除の契機

インテリジェント統合管理データベースの SELinux セキュリティコンテキストの設定・解除の契機を、次に示します。

表 2-8 インテリジェント統合管理データベースに対する設定・解除の契機

契機	対応コマンド	区分	説明
新規構築	jimgndbsetup	設定	SELinux の有効無効の状態に関わらず、コマンド実行時に自動的に SELinux セキュリティコンテキストの設定を行います。
削除	jimgndbunsetup	解除	SELinux の有効無効の状態に関わらず、コマンド実行時に自動的に SELinux セキュリティコンテキストの解除を行います。

- SELinux セキュリティコンテキストの設定対象ディレクトリ

インテリジェント統合管理データベースのインストール先ディレクトリを「/var/opt/jplimm/dbms/jimgndbbin/pgsql」（物理ホスト用のインテリジェント統合管理データベースのデフォルトのパス※）に仮定した場合の、SELinux セキュリティコンテキストが設定される対象ディレクトリと配下のファイルに設定する SELinux セキュリティコンテキストのタイプ、次に示します。

注※ パスは必要に応じて読み替えてください。

対象ディレクトリ	配下のファイルに設定する SELinux セキュリティコンテキストのタイプ
/var/opt/jp1imm/dbms/imgndbbin/pgsql 配下	postgresql_db_t

なお、インテリジェント統合管理データベースのインストール先ディレクトリのパスは、物理ホスト用と論理ホスト用で、次のように異なります。

- 物理ホストの場合

物理ホスト用のインテリジェント統合管理データベースのセットアップに使用するインテリジェント統合管理データベースセットアップ情報ファイル (jimgndbsetupinfo.conf) の定義に従います。パスは「**IMGNDDBENVDIR の値**/imgndbbin/pgsql」となります。

- 論理ホストの場合

論理ホスト用のインテリジェント統合管理データベースのセットアップに使用するクラスタ環境インテリジェント統合管理データベースセットアップ情報ファイル (jimgndbclustersetupinfo.conf) の定義に従います。パスは「**IMGNDDBENVDIR の値**/imgndbbin**LOGICALHOSTNUMBER の値**/pgsql」となります。

2.18.9 システムログ (syslog) に出力するメッセージの抑止

Linux 版の JP1/IM - Manager の稼働中は、OS (Linux) のシステムログ (syslog) に、メッセージが繰り返し出力されます。このため、システムログの容量、および、ログのローテーション (切り替え) の間隔には十分に注意し、必要に応じて、ディスク容量を増やす、または、ログのローテーションの間隔を短くするなどに対処してください。

例えば、Linux 8 の場合は、次のようなメッセージがシステムログに出力されます。

- 「/var/log/messages」ファイル

```
Feb  8 13:11:17 RHEL-8 su[17358]: (to imdbuser) root on pts/4
```

- 「/var/log/secure」ファイル

```
Feb  8 13:12:38 RHEL-8 su[17462]: pam_systemd(su-l:session): Cannot create session: Already running in a session or user slice
Feb  8 13:12:38 RHEL-8 su[17462]: pam_unix(su-l:session): session opened for user imdbuser by root(uid=0)
Feb  8 13:12:38 RHEL-8 su[17462]: pam_unix(su-l:session): session closed for user imdbuser
```

これらのメッセージの監視が不要な場合は、システムログに出力しないようにすることができます。なお、システムログの設定変更は、システム全体 (Linux 環境) に影響するため、十分に注意してください。また、システムログへの出力抑止の詳細については、OS に関連する資料などを参照してください。

2.18.10 JP1/IM - Manager の障害に備えた設定 (UNIX の場合)

JP1/IM - Manager は JP1/IM - Manager 自身に障害が発生した場合に備えて、トラブル解決の調査資料を採取するツールや、プロセスの異常終了時に自動で再起動する機能などを提供しています。

ここでは、JP1/IM - Manager の障害に備えた設定項目について説明します。

(1) 障害発生時の資料採取の準備

JP1/IM - Manager ではトラブル発生時に資料を採取するためのツールをシェルスクリプト (`jim_log.sh`) として提供しています。このツールは、トラブルの解決の調査資料となる情報を一括して採取するツールです。

JP1/IM - Manager の資料採取ツールで採取できるのは、JP1/IM - Manager および JP1/Base のトラブルシュート資料です。採取できる資料の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「12.3 トラブル発生時に採取が必要な資料」を参照してください。

資料採取ツールについて

- `jim_log.sh`について

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jim_log.sh` (UNIX 限定)」(1. コマンド)

なお、トラブルが発生した場合に調査資料として、コアダンプファイルが必要になることがあります。コアダンプファイルの出力はユーザーの環境設定に依存するため、次に示す設定を確認しておいてください。

(a) コアダンプファイルのサイズ設定

コアダンプファイルの最大サイズは、root ユーザーのコアダンプファイルのサイズ設定 (`ulimit -c`) によって制限されます。JP1/IM - Manager ではコアダンプファイルがユーザーの環境設定に依存しないで出力されるよう、`jco_start` および `jco_start.cluster` スクリプト内で次の設定をしています。

```
ulimit -c unlimited
```

この設定が、ご使用のマシンのセキュリティポリシーに反する場合は、これらのスクリプトの設定を次のように許容できる値に変更してください。

- 例 8388608 ブロックに制限する場合

```
ulimit -c 8388608
```

❗ 重要

コメント行にした場合や `unlimited` 以外を設定した場合は、JP1/IM - Manager のプロセスで発生したセグメンテーション障害、バス障害や `jcogencore` コマンド実行時などのコアダンプ

ファイルの出力契機に、調査に十分なサイズのコアダンプファイルが出力されないため、調査が行えないおそれがあります。

(b) コアダンプに関連するカーネルパラメーターの設定 (Linux 限定)

Linux のカーネルパラメーター (`kernel.core_pattern`) の設定で、コアダンプファイルの出力先が採取対象のログファイルディレクトリ以外に設定されている場合や、ファイル名をデフォルトの設定から変更している場合、資料採取ツールの実行時にコアダンプファイルを採取できません。

資料採取ツールは、次に示す採取対象のログファイルディレクトリにあるファイル名が `core` から始まるファイルを採取します。

物理ホストの場合

- `/var/opt/jp1cons/log/`
- `/var/opt/jp1scope/log`
- `/var/opt/jp1imm/log/imcf`
- `/var/opt/jp1imm/log/imdb`
- `/var/opt/jp1imm/log/imdd`

論理ホストの場合

- 共有ディレクトリ/`jp1cons/log/`
- 共有ディレクトリ/`jp1socpe/log`
- 共有ディレクトリ/`jp1imm/log/imcf`
- 共有ディレクトリ/`jp1imm/log/imdb`
- 共有ディレクトリ/`jp1imm/log/imdd`

`kernel.core_pattern` の設定によって、資料採取ツールの実行前に次のことを確認および対処を実施しておく必要があります。デフォルトの設定内容は OS のバージョンによって異なるので、必ず設定内容を確認してください。

- コアダンプファイルの出力先ディレクトリが採取対象のログファイルディレクトリ以外の場合
コアダンプファイルをデフォルトの出力先ディレクトリにコピーしておく。
- コアダンプファイルのファイル名を変更している場合
コアダンプファイルのファイル名を `core` から始まるファイル名にリネームしておく。
- コアダンプファイルを圧縮している場合
コアダンプファイルを解凍しておく。

(c) コアダンプファイルに関連する ABRT の設定 (Linux 限定)

自動バグレポートツール (ABRT) をインストールしている Linux で、ABRT の設定でプロセスや OS アカウントのユーザーまたはユーザーのグループに対してコアダンプファイルの生成を制限している場合、JP1/IM - Manager のプロセスで発生したセグメンテーション障害、バス障害やjcogencore コマンド実行時などのコアダンプファイルの出力契機に、コアダンプファイルが出力されないため、調査が行えません。

ご使用の運用に合わせて、JP1/IM - Manager を実行する OS アカウントのユーザーまたはユーザーのグループやプロセスに対して、コアダンプファイルの生成を制限しないように ABRT の設定を見直してください。詳しくは、ご使用の Linux のドキュメントを参照してください。

(d) コアダンプファイルに関連する systemd の設定 (Linux 限定)

コアダンプファイル名の設定ファイル (/proc/sys/kernel/core_pattern) が「|/usr/lib/systemd/systemd-coredump」から始まる文字列で設定されている Linux が対象です。

コアダンプファイルの動作設定ファイル (/etc/systemd/coredump.conf) でコアダンプファイルを生成しない設定をしている場合、JP1/IM - Manager のプロセスで発生したセグメンテーション障害、バス障害やjcogencore コマンド実行時などのコアダンプファイルの出力契機に、コアダンプが出力されないため、調査が行えません。

ご使用の運用に合わせて、コアダンプファイルを生成するようにコアダンプファイルの動作設定ファイル (/etc/systemd/coredump.conf) の設定を見直してください。詳しくは、ご使用の Linux のドキュメントを参照してください。

(e) SUSE Linux での注意事項

SUSE Linux Enterprise Server 12 SP2 以降で、jcogencore コマンドでダンプを出力するときに、コマンドを格納するディレクトリにコアダンプファイルが出力されず、次のどちらかのメッセージが出力された場合は、次の手順を実行してください。

- ・KAVB8428-W コアダンプファイルが見つかりません
- ・KAVB8408-E 指定したプロセスは起動していません

なお、コアダンプファイルが/var/lib/systemd/coredump/ に出力する設定であるものとして示します。

1. /var/lib/systemd/coredump/にある、jcogencore コマンドを実行した頃のタイムスタンプの JP1/IM - Manager の実行ファイル名を含むファイルを次に示すコピー先ディレクトリにコピーしてください。

No	JP1/IM - Manager の実行ファイル名	実行ファイル名ごとのコピー先ディレクトリ	
		物理ホスト	論理ホスト
1	evflow	/var/opt/jplcons/log/	<共有ディスク>/jplcons/log/
2	jcamain		

No	JP1/IM - Manager の実行ファイル名	実行ファイル名ごとのコピー先ディレクトリ	
		物理ホスト	論理ホスト
3	evtcon		
4	evgen		
5	jcdmain		
6	jcfmain	/var/opt/jplimm/log/imcf/	<共有ディスク>/jplimm/log/imcf/
7	jcfallogtrap		

2. 圧縮されたファイルの場合は、展開する(非圧縮ファイルの場合は 3.へ)。コピーしたファイルの拡張子が xz の場合は、次のコマンドで展開する。

unxz < 1.でコピーしたファイルパス>

3. 次のファイル名に変更する。

No	変更前のファイル名 (デフォルトの場合)	変更後のファイル名
1	接頭辞"core.evflow."のファイル名	core.evflow
2	接頭辞"core.jcamain."のファイル名	core.jcamain
3	接頭辞"core.evtcon"のファイル名	core.java
4	接頭辞"core.evgen"のファイル名	core.evgen
5	接頭辞"core.jcdmain "のファイル名	core.jcdmain
6	接頭辞"core.jcfmain"のファイル名	core.jcfmain
7	接頭辞"core.jcfallogtrap"のファイル名	core.<PID>.jcfallogtrap※

注※ <PID>は変更前のファイルにある<PID>を指定してください。変更前のファイル名は次の命名規則になっています（圧縮されてない場合は拡張子 xz はありません）。

core.<実行ファイル名>.<実 UID>.<Boot ID>.<PID>.<通算秒>.xz

次のファイル名の場合は、1378 が<PID>になります。

core.jcfallogtrap.0.71abdba3becd450a8ac5c4469dfcd648.1378.1493089252000000.xz

(2) プロセス異常終了時の再起動の設定

1. プロセス再起動を定義する。

プロセス再起動が有効になるよう、次の拡張起動プロセス定義ファイル (jp1co_service.conf) を編集します。

/etc/opt/jp1cons/conf/jp1co_service.conf

「再起動可否」パラメーターは「|」で区切られた 4 番目の値で、0（再起動しない：デフォルト）または 1（再起動する）を設定します。

2. 定義内容を反映する。

JP1/IM - Manager が稼働している場合は、プロセス再起動の設定が有効になるよう、JP1/IM - Manager のリロードコマンドを実行します。

```
/opt/jp1cons/bin/jco_spmc_reload
```

プロセス再起動の定義について

- 拡張起動プロセス定義ファイル (jp1co_service.conf) について

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「拡張起動プロセス定義ファイル (jp1co_service.conf)」(2. 定義ファイル)

注意事項

異常終了時の再起動設定は、クラスタ運用時には設定しないでください。JP1/IM - Manager の障害時にはプロセス再起動の機能も障害の影響を受けるおそれがあります。クラスタ運用時に再起動をしたい場合は、JP1/IM - Manager 外部のクラスタソフトから再起動を制御してください。

(3) プロセス異常検知時の JP1 イベントの発行の設定

1. JP1 イベント発行の設定をする。

次の IM パラメーター定義ファイル (jp1co_param_V7.conf) を編集します。

```
/etc/opt/jp1cons/conf/jp1co_param_V7.conf
```

このファイルの「SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT」と「SEND_PROCESS_RESTART_EVENT」が JP1 イベント発行の設定パラメーターです。JP1 イベントを発行するには、値を「dword:1」に変更します。

2. jbssetcnf コマンドを実行して、定義内容を反映する。

```
/opt/jp1base/bin/jbssetcnf /etc/opt/jp1cons/conf/jp1co_param_V7.conf
```

3. JP1/Base および JP1/Base を前提とする製品を再起動する。

再起動後に設定内容が反映されます。

JP1 イベント発行の設定について

- IM パラメーター定義ファイル (jp1co_param_V7.conf) について

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「IM パラメーター定義ファイル (jp1co_param_V7.conf)」(2. 定義ファイル)

(4) ヘルスチェック機能の設定

ヘルスチェック機能を使って JP1/IM - Manager プロセスのハングアップを検知したい場合に設定します。

1. ヘルスチェック定義ファイル (jcohc.conf) を開き、パラメーターを設定する。

ヘルスチェック機能を有効にするため、ENABLE=true にします。

また、ハングアップ検知時に JP1 イベントを発行する場合にはEVENT=true を、通知コマンドを実行する場合にはCOMMAND=実行するコマンドを指定します。

2. インストールとセットアップ (UNIX の場合)

2. `jco_spmd_reload` コマンドで JP1/IM - Manager をリロードする。または、JP1/IM - Manager を再起動する。
3. 通知コマンドを設定した場合は、`jcohctest` コマンドを実行して動作確認する。
`jcohctest` コマンドを実行して、正しく `COMMAND` で指定したコマンドが実行されるか確認します。正しく動作しなかった場合は指定を見直してください。

ヘルスチェック機能の設定について

- ヘルスチェック定義ファイル (`jcohc.conf`) について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ヘルスチェック定義ファイル (`jcohc.conf`)」(2. 定義ファイル)
- `jcohctest` コマンドについて
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jcohctest`」(1. コマンド)

(5) 監視オブジェクト DB の自動バックアップ・リカバリー設定

セントラルスコープの機能を使用する場合に設定します。

監視ツリーの更新中に、OS がシャットダウンしたり、クラスタ運用時にフェールオーバーしたりすると、監視オブジェクト DB が破損するおそれがあります。このため、監視ツリーの更新時に監視オブジェクト DB を自動でバックアップ・リカバリーするよう設定します。

新規インストールの場合は有効、旧バージョンの JP1/IM - Manager で設定を無効にしていた場合は無効となっています。運用に合わせて、設定を変更してください。

1. JP1/IM - Manager を停止する。
2. 次のファイルを引数に `jbssetcnf` コマンドを実行する。

監視オブジェクト DB の自動バックアップ・リカバリー機能を有効にする：`auto_dbbackup_on.conf`

監視オブジェクト DB の自動バックアップ・リカバリー機能を無効にする：`auto_dbbackup_off.conf`

`jbssetcnf` コマンドを実行すると、JP1 共通定義情報に設定内容が反映されます。

`jbssetcnf` コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「監視オブジェクト DB の自動バックアップ・リカバリー設定ファイル (`auto_dbbackup_xxx.conf`)」(2. 定義ファイル)を参照してください。

3. JP1/IM - Manager を起動する。

2.18.11 バージョンアップ時の設定 (UNIX の場合)

ここでは、JP1/IM - Manager のバージョンアップインストール時のセットアップ項目について説明しています。

IM データベースを使用している場合は、「[2.4.5 IM データベースの更新 \(UNIX の場合\)](#)」を参照して、IM データベースを更新する必要があります。

(1) イベント取得フィルターの位置の変更

旧バージョンの JP1/IM - Manager で、イベント取得フィルター（互換用）を使用していた場合は、`jcochafmode` コマンドを実行して、イベント取得フィルターの位置をイベントコンソールサービスからイベント基盤サービスに変更できます。イベント取得フィルターの位置をイベント基盤サービスに変更すると、JP1 イベントの監視に加えて、自動アクションや監視オブジェクトの状態監視にも有効なフィルターとして動作させることができます。また、フィルター条件を詳細に定義できるようになります。ただし、バージョンアップ前のイベント取得フィルターで運用したい場合は、フィルター位置の変更は不要です。

❗ 重要

一度イベント取得フィルターの位置を変更すると、以前のイベント取得フィルターには戻せません。`jcochafmode` コマンドを実行する前に、イベント取得フィルターの位置の変更について、十分に検討してください。

1. JP1/IM - Manager を停止する。

2. `jcochafmode` コマンドを実行してフィルター位置を変更する。

3. JP1/IM - Manager を起動する。

- イベント取得フィルターの機能について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.2.2 イベント取得フィルター」

- `jcochafmode` コマンドについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jcochafmode` (UNIX 限定)」(1. コマンド)

(2) セントラルスコープのバージョンアップコマンドの実行

バージョン 8 以前の JP1/IM - Central Scope からバージョンアップした場合は、次の手順に従い、バージョンアップコマンドを実行してください。バージョンアップコマンドを実行するまでは、旧バージョンの JP1/IM - Central Scope と互換モードで動作します（旧バージョンから追加された機能は使用できません）。

1. JP1/IM - Manager を停止する。

2. インストールとセットアップ (UNIX の場合)

2. ディスクの空き容量を確認する。

次の手順に示す `jp1csverup` コマンドを実行するには、監視オブジェクト DB 分の空き容量が必要です。
監視オブジェクト DB は、次に示すディレクトリ内のすべてのデータです。

`/var/opt/jp1scope/database/jcsdb/`

3. `jp1csverup` コマンドを実行する。

4. `jbssetcnf` コマンドを実行する。

次に示す機能の有効、無効は旧バージョンの JP1/IM - Central Scope の設定に依存します。

- 対処済み連動機能
- 状態変更イベントの上限監視

機能を無効から有効にしたい場合、次の表に示すファイルを引数に `jbssetcnf` コマンドを実行してください。

表 2-9 機能を有効にするための設定ファイル

ファイル名	説明
<code>action_complete_on.conf</code>	対処済み連動機能を有効にするためのファイルです。
<code>evhist_warn_event_on.conf</code>	監視オブジェクトの状態変更イベント件数が上限値（100 件）を超えた際に、JP1 イベントを発行する機能を有効にするためのファイルです。

5. JP1/IM - Manager を起動する。

6. JP1/IM - View で JP1/IM - Manager（JP1/IM - Central Scope）に接続し、問題がないか動作を確認する。

- `jp1csverup` コマンドについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jp1csverup` (UNIX 限定)」(1. コマンド)

(3) 自動アクション定義ファイルの更新

11-10 以前の JP1/IM - Manager からバージョンアップした場合は、次の手順に従い、自動アクション定義ファイルを更新してください。

ただし、11-10 以前の自動アクション定義ファイルをそのまま使用したい場合は必要ありません。

1. JP1/IM - Manager を停止する。

2. `jcadefconv` コマンドを実行して自動アクション定義ファイルを更新する。

`jcadefconv -i` 変換するアクション定義ファイル名 `-o` 変換後のアクション定義ファイル名

3. `jcadefconv` コマンドの `-o` オプションに指定したファイルを `actdef.conf` にリネームして格納先に配置する。

格納先およびファイル名を次に示します。なお、次に示す格納先およびファイル名を-o オプションに直接指定している場合は、この手順は不要です。

物理ホスト：/etc/opt/jp1cons/conf/action/actdef.conf

論理ホスト：共有ディレクトリ/jp1cons/conf/action/actdef.conf

4. JP1/IM - Manager を起動する。

- 自動アクションの機能について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「6. 自動アクションによるコマンド実行 (JP1/Base 連携)」

- jcadefconv コマンドについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcadefconv」(1. コマンド)

(4) 発生元ホストの項目の表示

JP1/IM - Manager 09-00～09-10 からバージョンアップした場合、イベント条件表示項目定義ファイルに発生元ホストが設定されていません。そのため、発生元ホストのマッピング機能を有効にしても、[アクション詳細設定] 画面のイベント条件に発生元ホストの項目が表示されません。[アクション詳細設定] 画面のイベント条件に発生元ホストの項目を表示する場合、イベント条件表示項目定義ファイルに「E. JP1_SOURCEHOST」を追加する必要があります。

[アクション詳細設定] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.33.1 [アクション詳細設定] 画面」を参照してください。

イベント条件表示項目定義ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベント条件表示項目定義ファイル (attr_list.conf)」(2. 定義ファイル) を参照してください。

(5) イベントレポート出力の出力形式の指定

10-50 以前の JP1/IM - Manager からバージョンアップした場合、イベントレポート出力で CSV 出力する際に、1 件の固有の拡張属性に一つの列を割り当てて出力する機能が無効になっています。この機能を有効にするかどうかは、イベントレポート出力環境定義ファイル (evtreport.conf) の PROGRAM_SPECIFIC_EX_ATTR_COLUMN パラメーターで指定します。なお、新規にインストールした場合は有効です。必要に応じて、イベントレポート出力環境定義ファイルを設定してください。

イベントレポート出力環境定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベントレポート出力環境定義ファイル (evtreport.conf)」(2. 定義ファイル) を参照してください。

(6) [ログファイルトラップサービスが起動したときに自動でプロセス起動する] チェックボックスの表示

11-01 以前の JP1/IM - Manager からバージョンアップした場合、[ログファイルトラップサービスが起動したときに自動でプロセス起動する] チェックボックスが無効（非表示）になっています。

[ログファイルトラップサービスが起動したときに自動でプロセス起動する] チェックボックスの有効・無効は、プロファイル管理環境定義ファイル (jplcf_profile_manager.conf) の LOGFILETRAP_AUTO_START_CONTROL パラメーターで指定します。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「プロファイル管理環境定義ファイル (jplcf_profile_manager.conf)」(2. 定義ファイル) を参照してください。

(7) エージェントのプロファイル更新通知機能

11-01 以前の JP1/IM - Manager からバージョンアップした場合、エージェントのプロファイル更新通知機能が無効になっています。

エージェントのプロファイル更新通知機能の有効・無効は、プロファイル管理環境定義ファイル (jplcf_profile_manager.conf) の AGENT_PROFILE_UPDATE_NOTICE はパラメーターで指定します。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「プロファイル管理環境定義ファイル (jplcf_profile_manager.conf)」(2. 定義ファイル) を参照してください。

(8) リモート監視が停止中のログの監視設定

11-01 以前の JP1/IM - Manager からバージョンアップした場合、リモート監視が停止中に出力されたログ情報を収集しない設定になっています。

リモート監視が停止中に出力されたログ情報を収集するかどうかは、リモートログトラップ環境定義ファイル (jplcf_remote_logtrap.conf) の START_OPTION パラメーターで指定します。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「リモートログトラップ環境定義ファイル (jplcf_remote_logtrap.conf)」(2. 定義ファイル) を参照してください。

(9) インテリジェント統合管理基盤のバージョンアップ (UNIX の場合)

インテリジェント統合管理基盤を利用している場合のバージョンアップ時の設定について説明します。

なお、連携製品のバージョンアップも同時に実施する場合は、手順 5 を実行する前に連携製品のバージョンアップを実施してください。

1. JP1/IM - Manager を停止する。
2. 12-50 以前の JP1/IM - Manager からバージョンアップした場合、インテリジェント統合管理データベースを構築する。

インテリジェント統合管理データベースの構築の詳細については、「[2.5 インテリジェント統合管理データベースの構築 \(UNIX の場合\)](#)」を参照してください。

3. 新しい設定値を追加する。

利用する機能に合わせて、新しく追加された設定値を追加します。※

注※

JP1/IM - Manager を 13-00 または 13-01 から 13-10 以降にバージョンアップした場合、テキストエディターなどで、次のファイルの末尾に「web-enable-admin-api: true」の行を追加します。なお、インテリジェント統合管理データベースを再構築したときは、自動で追加されるため、この手順は不要です。

- ・物理ホストの場合：/etc/opt/jp1imm/conf/imgndb/config.yml
- ・論理ホストの場合：共有ディレクトリ/jp1imm/conf/imgndb/config.yml

上記の手順を実施しなかった場合、トレンドデータの削除と統合エージェント情報の削除が失敗します。

トレンドデータの削除と統合エージェント情報については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.1 [統合エージェント一覧] 画面」、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.11.4 トレンドデータ削除」および「5.18.2 統合エージェント情報削除」を参照してください。

4. JP1/IM - Manager を起動する。

5. jddcreatetree コマンドを実行する。

6. jddupdatetree コマンドを新規・再構築モードで実行する。

- ・ jddcreatetree コマンドについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddcreatetree」(1. コマンド)

- ・ jddupdatetree コマンドについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddupdatetree」(1. コマンド)

バージョンアップを実行しない場合、インテリジェント統合管理基盤 13-00 の機能は利用できません。

(10) インテリジェント統合管理データベースのバージョンアップ (UNIX の場合)

インテリジェント統合管理データベースを利用している場合のバージョンアップ時の設定について説明します。

JP1/IM - Manager をバージョン 13-10 以前からバージョンアップした場合に、インテリジェント統合管理データベースを利用しているときは、jimgnbupdate コマンドを実行する必要があります。jimgnbupdate

コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimgndbupdate」(1. コマンド) を参照してください。

(11) 拡張起動プロセス定義ファイルの更新

バージョン 11 以前の JP1/IM - Manager からバージョンアップした場合は、拡張起動プロセス定義ファイル (jplco_service.conf) に jddmain, imbase, imbaseproxy プロセスの定義を追加してください。

バージョン 12 からバージョンアップした場合は、imbase, imbaseproxy プロセスの定義を追加してください。

拡張起動プロセス定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「拡張起動プロセス定義ファイル (jplco_service.conf)」(2. 定義ファイル) を参照してください。

2.19 JP1/IM - Agent のセットアップ (UNIX の場合)

2.19.1 JP1/IM - Agent のサービスの設定

(1) アドオンプログラムの有効化・無効化

アドオンプログラムの有効化・無効化について説明します。JP1/IM - Agent は、複数のアドオンプログラムを含んでおり、有効化したサービスだけを起動できます。

(a) アドオンプログラムの有効化

■インストール時に設定する場合

インストール時に使用する初期設定コマンドで、有効化したいアドオンプログラムを選択します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.9 初期設定コマンド」の説明を参照してください。

なお、バージョンアップインストール時は、既存の設定を引き継ぎます。ただし、新バージョンで新たに追加されたアドオンプログラムは無効化された状態となります。

■インストール後に設定する場合

JP1/IM - Agent のアドオンプログラムのサービスを有効化する手順を、次に示します。

1. サービスが起動中の場合は、次のコマンドを実行して停止する。

```
/opt/jp1ima/tools/jpc_service_stop -s all
```

2. 次のコマンドを実行して、サービスを有効化する。

```
/opt/jp1ima/tools/jpc_service -on [JP1/IM - Agentのサービスキー]
```

3. サービスに対応するディスカバリ設定ファイルを移動する。

次に示すサービスに対応するディスカバリ設定ファイルを、/opt/jp1ima/conf/jpc_file_sd_config_off ディレクトリから/opt/jp1ima/conf ディレクトリに移動します。

サービス	ディスカバリ設定ファイル
prometheus_server	なし
alertmanager	なし
node_exporter	jpc_file_sd_config_node.yml
blackbox_exporter	• jpc_file_sd_config_blackbox_http.yml • jpc_file_sd_config_blackbox_icmp.yml

サービス	ディスカバリ設定ファイル
ya_cloudwatch_exporter	jpc_file_sd_config_cloudwatch.yml
fluentd	なし
process_exporter	jpc_file_sd_config_process.yml
promitor	jpc_file_sd_config_promitor.yml
script_exporter	なし

4. サービスが有効化されたことを確認する。

systemctl list-unit-files コマンドを実行します。該当するサービスの STATE の値が「masked」以外であれば有効です。

5. 「2.19.2(18) IM 管理ノードのツリー情報の作成と反映 (Linux の場合) (必須)」を実施する。

(b) アドオンプログラムの無効化

JP1/IM - Agent のアドオンプログラムのサービスを無効化する手順を、次に示します。

1. サービスが起動中の場合は、次のコマンドを実行して停止する。

```
/opt/jplima/tools/jpc_service_stop -s all
```

2. 次のコマンドを実行して、サービスを無効化する。

```
/opt/jplima/tools/jpc_service -off [JP1/IM - Agentのサービスキー]
```

3. サービスに対応するディスカバリ設定ファイルを移動する。

次に示すサービスに対応するディスカバリ設定ファイルを、/opt/jplima/conf ディレクトリから/opt/jplima/conf/jpc_file_sd_config_off ディレクトリに移動します。

サービス	ディスカバリ設定ファイル
prometheus_server	なし
alertmanager	なし
node_exporter	jpc_file_sd_config_node.yml
blackbox_exporter	- jpc_file_sd_config_blackbox_http.yml - jpc_file_sd_config_blackbox_icmp.yml
ya_cloudwatch_exporter	jpc_file_sd_config_cloudwatch.yml
fluentd	なし
process_exporter	jpc_file_sd_config_process.yml
promitor	jpc_file_sd_config_promitor.yml
script_exporter	なし

4. サービスが無効化されたことを確認する。

systemctl list-unit-files コマンドを実行します。該当するサービスの STATE の値が「masked」であれば無効です。

(2) 自動起動の有効化・無効化

(a) 自動起動の有効化

OS 起動時のサービス自動起動を有効にする手順を、次に示します。

1. 次のコマンドを実行して、JP1/IM - Agent のすべてのサービスの自動起動を有効にする。

```
jpc_service_autostart -on
```

(b) 自動起動の無効化

OS 起動時のサービス自動起動を無効にする手順を、次に示します。

1. 次のコマンドを実行して、JP1/IM - Agent のすべてのサービスの自動起動を無効にする。

```
jpc_service_autostart -off
```

(c) 自動起動および自動停止の確認方法

次のコマンドで確認します。

```
systemctl list-unit-files
```

該当するサービスの STATE の値が「enabled」であれば有効です。「disabled」であれば無効です。サービス名については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.9 JP1/IM - Agent のサービス」を参照してください。

(d) OS シャットダウン時の自動停止についての注意事項

統合エージェントのサービスが稼働している状態で Linux をシャットダウンした場合、統合エージェントのサービスは停止しますが、/var/log/messages ファイルに統合エージェントのサービスが停止したことを通知するメッセージが出力されないことがあります。

(3) 手動で起動・停止する方法

JP1/IM - Agent を手動で起動・停止する場合は、次のコマンドを使用します。

表 2-10 起動停止コマンド

コマンド	説明
jpc_service_start	エージェントサービスを起動します。

コマンド	説明
<code>jpc_service_stop</code>	エージェントサービスを停止します

コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「1. コマンド」を参照してください。

(4) サービスの起動状態の確認方法

次のコマンドで確認します。

```
systemctl list-units --all --type=service
```

ACTIVE 列が「active」なら起動中です。それ以外なら停止中です。

(5) 設定ファイルの配置場所

systemd のユニット定義ファイルを、次の場所に配置します。

ユニット定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユニット定義ファイル (jpc_プログラム名.service)」(2. 定義ファイル) を参照してください。

表 2-11 systemd のユニット定義ファイルの配置場所

配置場所 (パス)	用途	配置方法
/opt/jp1ima/conf/ (物理ホストの場合)	モデルファイル (ユニット定義ファイルの雛型) モデルファイルは編集しないでください。	インストーラーで配置します。
共有ディスク/jp1ima/conf/ (論理ホストの場合)	モデルファイル (ユニット定義ファイルの雛型) モデルファイルは編集しないでください。	手動で配置で配置します。
/usr/lib/systemd/system/	ユニット定義ファイル本体 このファイルを編集してください。 systemd はこのファイルを使用します。	物理ホスト用は初期設定コマンドで、論理ホスト用は手動で配置します。

(6) 設定ファイルの編集

サービスの設定を変更したい場合は、ユニット定義ファイルを編集します。ユニット定義ファイルを編集した場合、定義を反映するには、root 権限を持つユーザーで次のコマンドを実行する必要があります (マシンを再起動した場合も反映されます)。

```
systemctl daemon-reload
```

2.19.2 JP1/IM - Agent の設定

(1) 共通の設定方法

(a) 設定ファイルを編集する (Linux の場合)

「[1.21.2\(1\)\(a\)設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

(b) ユニット定義ファイルを変更する (Linux の場合だけ)

ユニット定義ファイルの格納先とファイル名を、次に示します。

- 格納先: /usr/lib/systemd/system/
- ファイル名: jpc_サービス名.service

ユニット定義ファイルを変更する手順を、次に示します。

1. 統合エージェントホストにログインする。
2. JP1/IM - Agent のサービスを停止する。
3. ユニット定義ファイルを編集する。
4. 次のコマンドを実行し、ユニット定義を反映する。

```
# systemctl daemon-reload
```

5. JP1/IM - Agent のサービスを起動する。

(c) コマンドラインオプションを変更する (Linux の場合)

ユニット定義ファイルのExecStart 行で、コマンドラインオプションを変更します。

編集方法については、「[2.19.2\(1\)\(b\)ユニット定義ファイルを変更する \(Linux の場合だけ\)](#)」を参照してください。

(2) 統合エージェント制御基盤の設定

(a) 接続先の統合マネージャーを変更する (Linux の場合) (オプション)

「[1.21.2\(2\)\(a\)接続先の統合マネージャーを変更する \(Windows の場合\) \(オプション\)](#)」を参照してください。

(b) ポートを変更する (Linux の場合) (オプション)

「[1.21.2\(2\)\(b\)ポートを変更する \(Windows の場合\) \(オプション\)](#)」を参照してください。

(c) CA 証明書を配置する (Linux の場合) (オプション)

「1.21.2(2)(c)CA 証明書を配置する (Windows の場合) (オプション)」を参照してください。

(d) アクション実行に関する設定を変更する (Linux の場合) (オプション)

「1.21.2(2)(d)アクション実行に関する設定を変更する (Windows の場合) (オプション)」を参照してください。

(e) プロキシ認証の認証 ID とパスワードを設定する (Linux の場合) (オプション)

「1.21.2(2)(e)プロキシ認証の認証 ID とパスワードを設定する (Windows の場合) (オプション)」を参照してください。

(f) アクションの実行ユーザーを変更する (Linux の場合) (必須)

imagent 設定ファイル (jpc_imagent.json) の action.username を変更します。

設定方法については、「2.19.2(1)(a) 設定ファイルを編集する (Linux の場合)」を参照してください。

(g) イベント転送中継機能を設定する (Linux の場合) (オプション)

「1.21.2(2)(g)イベント転送中継機能を設定する (Windows の場合) (オプション)」を参照してください。

(h) 複数マネージャーホストへのデータ配信機能を設定する (Linux の場合) (オプション)

■ 新規設定

1. JP1/IM - Agent のサービスを停止する。

停止するサービスのサービスキーを次に示します。

- jpc_imagent
- jpc_imagentaction
- jpc_imagentproxy
- jpc_alertmanager
- jpc_prometheus_server
- jpc_fluentd

2. 統合エージェント管理基盤のセカンダリー用のディレクトリを作成する。

統合エージェント管理基盤のセカンダリー用のディレクトリとして、次のディレクトリを作成します。

- /opt/jp1ima/tmp/download-imagent グループ識別子
- /opt/jp1ima/tmp/upload-imagent グループ識別子
- /opt/jp1ima/tmp/jbsfwd-imagent グループ識別子
- /opt/jp1ima/logs/imagent-imagent グループ識別子

2. インストールとセットアップ (UNIX の場合)

- /opt/jp1ima/logs/imagentproxy-imagent グループ識別子
- /opt/jp1ima/logs/imagentaction-imagent グループ識別子

上記のディレクトリの作成には、次のコマンドを使用します。

```
mkdir -m 700 ディレクトリ
chown -R root:root ディレクトリ
```

3. 統合エージェント管理基盤のセカンダリー用のユニット定義ファイルを作成する。

/usr/lib/systemd/system 下にあるコピー元のユニット定義ファイルをコピーし、コピー先のファイル名にリネームします。

作成したユニット定義ファイルのオーナーおよびオーナーグループは、root、アクセス権は 644 にします。

コピー元のファイル名	コピー先のファイル名
jpc_imagent.service	jpc_imagent-imagent グループ識別子.service
jpc_imagentproxy.service	jpc_imagentproxy-imagent グループ識別子.service
jpc_imagentaction.service	jpc_imagentaction-imagent グループ識別子.service

4. 統合エージェント制御基盤のセカンダリー用の設定を行う。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(d) 統合エージェント制御基盤の設定ファイル」を参照してください。

5. 統合エージェント制御基盤のセカンダリー用のシークレットを登録する。

セカンダリーの統合エージェント制御基盤が接続する JP1/IM - Manager の初期シークレットを取得して登録します。

パスワードによる HTTP 認証 (Basic 認証) が必要な HTTP プロキシサーバを介して JP1/IM - Manager に接続する場合は、HTTP プロキシパスワードをシークレットとして登録してください。

登録する初期シークレットのキー、および HTTP プロキシパスワードのキーについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(e) 初期シークレット、クライアントシークレット、および HTTP プロキシパスワードのキー」を参照してください。

6. 統合エージェント制御基盤以外の設定を行う。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(f) 統合エージェント制御基盤以外の各プログラムの送信設定」を参照してください。

7. サービスの起動設定を行う。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(c) セカンダリーのサービス起動の設定」を参照してください。

8. systemd を更新する。

次のコマンドを実行します。

```
systemctl daemon-reload
```


9. [systemctl list-unit-files] を実行し、サービスの状態がmasked になっているセカンダリーサービスに対して、次のコマンドを実行して、サービスを有効化する。

```
/opt/jp1ima/tools/jpc_service -on サービスキー
```

サービスキーについては、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10.1 JP1/IM - Agent のサービス」に記載している Linux 環境での JP1/IM - Agent のサービスキーのうち、「-imagent グループ識別子」が付いているものを使用します。

10. JP1/IM - Agent のサービスを起動する。

停止するサービスのサービスキーを次に示します。

- jpc_imagent
- jpc_imagentaction
- jpc_imagentproxy
- jpc_imagent-imagent グループ識別子
- jpc_imagentaction-imagent グループ識別子
- jpc_imagentproxy-imagent グループ識別子
- jpc_alertmanager
- jpc_prometheus_server
- jpc_fluentd

11. OS 起動時の自動起動設定を行う。

自動起動の有効化の設定については、「[2.19.1\(2\)\(a\) 自動起動の有効化](#)」を参照してください。

(i) 複数マネージャーホストへのデータ配信機能を解除する (Linux の場合) (オプション)

複数マネージャーホストへのデータ配信機能を使用しなくなった場合の設定手順を次に示します。

ご使用の運用環境に合わせて、次のどちらかを実施します。

- JP1/IM - Agent のアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する
- JP1/IM - Agent 自体のアンインストールを行う

■ JP1/IM - Agent のアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合

1. JP1/IM - Agent のすべてのサービスを停止する。

サービスが起動中の場合は、次のコマンドを実行して停止する。

```
/opt/jp1ima/tools/jpc_service_stop -s all
```

2. セカンダリーのサービスを有効化する。

次のコマンドを実行して、統合エージェント制御基盤のセカンダリーのサービスを有効化します。

```
/opt/jp1ima/tools/jpc_service -on サービスキー
```

サービスを有効化する方法については、「[2.19.1\(1\)\(a\)アドオンプログラムの有効化](#)」の手順 2 と手順 4 を参照してください。

サービスキーについては、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10.1 JP1/IM - Agent のサービス」に記載している Linux 環境での JP1/IM - Agent のサービスキーのうち、「-imagent グループ識別子」が付いているものが該当します。

3. 複数マネージャーホストへのデータ配信機能を使用するために作成したシークレットを削除する。

「[2.19.2\(2\)\(h\) 複数マネージャーホストへのデータ配信機能を設定する \(Linux の場合\) \(オプション\)](#)」の手順 5 で登録した統合エージェント制御基盤のセカンダリー用のシークレットを削除します。

削除するシークレットのキーについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(e) 初期シークレット、クライアントシークレット、および HTTP プロキシパスワードのキー」を参照してください。

すでに消えているシークレットについては、この手順は不要です。

4. 複数マネージャーホストへのデータ配信機能を使用するために設定した内容を元に戻す。

「[2.19.2\(2\)\(h\) 複数マネージャーホストへのデータ配信機能を設定する \(Linux の場合\) \(オプション\)](#)」の手順 4 で設定した統合エージェント制御基盤のセカンダリー用の設定を元に戻します。

5. 複数マネージャーホストへのデータ配信機能を使用するためにコピーしたファイルを削除する。

「[2.19.2\(2\)\(h\) 複数マネージャーホストへのデータ配信機能を設定する \(Linux の場合\) \(オプション\)](#)」の手順 3 でコピーした統合エージェント管理基盤のセカンダリー用のユニット定義ファイルを削除します。

6. 複数マネージャーホストへのデータ配信機能を使用するために作成したディレクトリを削除する。

ログなどの必要なファイルを退避したあと、「[2.19.2\(2\)\(h\) 複数マネージャーホストへのデータ配信機能を設定する \(Linux の場合\) \(オプション\)](#)」の手順 2 で作成した統合エージェント管理基盤のセカンダリー用のディレクトリを削除します。

7. systemd を更新する。

次のコマンドを実行します。

```
systemctl daemon-reload
```

8. 無効化したセカンダリーのサービスが接続している JP1/IM - Manager 側で登録している統合エージェント情報を削除する。

統合エージェント情報の削除手順については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.1 [統合エージェント一覧] 画面」を参照してください。

■ JP1/IM - Agent 自体のアンインストールを行う場合

「[2.23.1\(4\) JP1/IM - Agent のアンインストールの手順](#)」の手順 1 と手順 2 の間に、上記の「JP1/IM - Agent のアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合」の手順 3 から手順 6 を実施します。

実施後に、上記の「JP1/IM - Agent のアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合」の手順 8 を実施します。

(3) Prometheus server の設定

(a) ポートを変更する (Linux の場合) (オプション)

Prometheus server が使用するリスンポートは、prometheus コマンドの`--web.listen-address` オプションに指定します。

prometheus コマンドのオプションの変更方法については、「[2.19.2\(1\)\(c\) コマンドラインオプションを変更する \(Linux の場合\)](#)」を参照してください。また、`--web.listen-address` オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユニット定義ファイル (jpc_プログラム名.service)」(2. 定義ファイル) の「コマンドラインのオプションを変更したい場合」を参照してください。

なお、デフォルトのポートは「20713」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。ただし、他ホストの Blackbox exporter による外形監視で Prometheus server を監視する場合は、アクセスを許可します。この場合、必要に応じて送信元 IP アドレスを制限するなどセキュリティ対策を検討してください。

(b) アラート定義を追加する (Linux の場合) (オプション)

「[1.21.2\(3\)\(b\) アラート定義を追加する \(Windows の場合\) \(オプション\)](#)」を参照してください。

(c) Blackbox exporter のスクレイプジョブを追加する (Linux の場合) (オプション)

「[1.21.2\(3\)\(c\) Blackbox exporter のスクレイプジョブを追加する \(Windows の場合\) \(オプション\)](#)」を参照してください。

(d) ユーザー独自の Exporter のスクレイプジョブを追加する (Linux の場合) (オプション)

「[1.21.2\(3\)\(d\) ユーザー独自の Exporter のスクレイプジョブを追加する \(Windows の場合\) \(オプション\)](#)」を参照してください。

(e) リモートライト先を変更する (Linux の場合) (オプション)

「[1.21.2\(3\)\(e\) リモートライト先を変更する \(Windows の場合\) \(オプション\)](#)」を参照してください。

(f) サービス監視の設定をする (Linux の場合) (オプション)

JP1/IM - Agent 13-00 から 13-01 以降にバージョンアップインストールした環境で、サービス監視機能を使用する場合、次の設定を行います。JP1/IM - Agent 13-01 以降を新規インストールした場合は、この設定は不要です。

■ Prometheus 設定ファイル (jpc_prometheus_server.yml) の編集

jpc_node スクレイプジョブの metric_relabel_configs の設定で、メトリックを保持する設定に「node_systemd_unit_state」が設定されていない場合、設定を追加します。また、同じ metric_relabel_configs の設定で、「node_systemd_unit_state」メトリックに対する relabel config が設定されていない場合、設定を追加します。下記のとおり到下線部分の設定を追加します。

```
(省略)
scrape_configs:
  (省略)
  - job_name: 'jpc_node'
    (省略)
    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'node_network_receive_bytes_total|node_network_transmit_bytes_total|～省略～|
node_vmstat_pswpin|node_vmstat_pswpout|node_systemd_unit_state'
        action: 'keep'
      - source_labels: ['__name__']
        regex: 'node_systemd_unit_.*'
        target_label: 'jp1_pc_trendname'
        replacement: 'node_exporter_service'
      - source_labels: ['__name__']
        regex: 'node_systemd_unit_.*'
        target_label: 'jp1_pc_category'
        replacement: 'service'
      - source_labels: ['__name__', 'name']
        regex: 'node_systemd_unit_.*;(.*?)'
        target_label: 'jp1_pc_nodelabel'
        replacement: '${1}'
      - regex: jp1_pc_multiple_node
        action: labeldrop
```

■ Node exporter のディスカバリ設定ファイル (jpc_file_sd_config_node.yml) の編集

jp1_pc_multiple_node が設定されていない場合、下記のとおり到下線部分の設定を追加します。

```
- targets:
  - ホスト名:20716
  labels:
    jp1_pc_exporter: JPC Node exporter
    jp1_pc_category: platform
    jp1_pc_trendname: node_exporter
    jp1_pc_multiple_node: "{ name =~'node_systemd_unit_.*'}"
```

(g) IM 管理ノードのラベル名 (jp1_pc_nodelabel の値) が上限を超える場合の設定をする (Linux の場合) (オプション)

「1.21.2(3)(g)IM 管理ノードのラベル名 (jp1_pc_nodelabel の値) が上限を超える場合の設定をする (Windows の場合) (オプション)」を参照してください。

(h) SAP システムのログ抽出コマンドを Script exporter を使用して実行する場合の設定 (Linux の場合) (オプション)

「1.21.2(3)(h)SAP システムのログ抽出コマンドを Script exporter を使用して実行する場合の設定 (Windows の場合) (オプション)」を参照してください。

(i) VMware exporter のスクレイプジョブを追加する (Linux の場合) (オプション)

「1.21.2(3)(j)VMware exporter のスクレイプジョブを追加する (Windows の場合だけ) (オプション)」を参照してください。

(4) Alertmanager の設定

(a) ポートを変更する (Linux の場合) (オプション)

Alertmanager が使用するリスンポートは、alertmanager コマンドの--web.listen-address オプションに指定します。

alertmanager コマンドのオプションの変更方法については、「[2.19.2\(1\)\(c\)コマンドラインオプションを変更する \(Linux の場合\)](#)」を参照してください。また、--web.listen-address オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユニット定義ファイル (jpc_プログラム名.service)」(2. 定義ファイル) の「コマンドラインのオプションを変更したい場合」を参照してください。

なお、デフォルトのポートは「20714」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。ただし、他ホストの Blackbox exporter による外形監視で Alertmanager を監視する場合は、アクセスを許可します。この場合、必要に応じて送信元 IP アドレスを制限するなどセキュリティ対策を検討してください。

(b) アラート通知先を変更する (Linux の場合) (オプション)

「1.21.2(4)(b)アラート通知先を変更する (Windows の場合) (オプション)」を参照してください。

(c) サイレンスを設定する (Linux の場合) (オプション)

「1.21.2(4)(c)サイレンスを設定する (Windows の場合) (オプション)」を参照してください。

(5) Node exporter の設定

(a) ポートを変更する (オプション)

Node exporter が使用するリスンポートは、node_exporter コマンドの--web.listen-address オプションに指定します。

node_exporter コマンドのオプションの変更方法については、「[2.19.2\(1\)\(c\)コマンドラインオプションを変更する \(Linux の場合\)](#)」を参照してください。また、--web.listen-address オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユニット定義ファイル (jpc_プログラム名.service)」(2. 定義ファイル) の「コマンドラインのオプションを変更したい場合」を参照してください。

なお、デフォルトのポートは「20716」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

(b) 収集するメトリックを変更する (オプション)

1. Prometheus 設定ファイルにメトリックを追加する。

Prometheus 設定ファイル (jpc_prometheus_server.yml) の metric_relabel_configs に、収集するメトリックが「|」で区切って定義されています。収集する必要がないメトリックを削除し、収集するメトリックを追加します。

設定ファイルを更新する手順については、「[1.21.2\(1\)\(a\)設定ファイルを編集する \(Windows の場合\)](#)」を参照してください。

<設定例>

```
- job_name: 'jpc_node'
  :
  metric_relabel_configs:
    - source_labels: ['__name__']
      regex: 'node_boot_time_seconds|node_context_switches_total|node_cpu_seconds_total|node_disk_io_now|node_disk_io_time_seconds_total|node_disk_read_bytes_total|node_disk_reads_completed_total|...|node_time_seconds|node_uname_info|node_vmstat_pswpin|node_vmstat_pswpout【ここにメトリクスを追加します】'
      action: 'keep'
```

2. 必要に応じて、メトリック定義ファイルにトレンド表示の定義を行う。

Node exporter のメトリック定義ファイルに、トレンド表示の定義を行います。

記述内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Node exporter のメトリック定義ファイル (metrics_node_exporter.conf)」(2. 定義ファイル) を参照してください。

3. サービス監視の設定を行う。

■Node exporter のユニット定義ファイル (jpc_node_exporter.service) の編集

サービス監視を行う場合、下記の下線部分のとおり、Node exporter のユニット定義ファイル (jpc_node_exporter.service) の編集を行います。


```
[Unit]
Description = JP1/IM3-Agent Linux metric collector
After=local-fs.target remote-fs.target rsyslog.service network.target
[Service]
WorkingDirectory = @@installdir2@@/jp1ima/bin
ExecStart = /bin/sh -c "'@@installdir1@@/jp1ima/bin/node_exporter" ¥
--collector.cpu.info ¥
(省略)
--no-collector.supervisord ¥
--collector.systemd ¥
--collector.systemd.unit-include="ユニットファイル名にマッチする正規表現" ¥
--no-collector.tcpstat ¥
--no-collector.textfile ¥
--no-collector.thermal_zone ¥
(省略)
```

ExecStart 行に設定する引数の値として、「--no-collector.systemd」が設定されている場合、「--collector.systemd」に変更します。「--collector.systemd.unit-include」が設定されていない場合は、行を追加し、値には監視したいユニットのユニットファイル名にマッチする正規表現を設定します。正規表現の指定の仕方によって、性能情報の収集に時間がかかることがあります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 G.4 正規表現を使用する際のヒント」を参照してください。

■Node exporter のユニット定義ファイル (jpc_node_exporter.service) の定義例

jpc_imagent.service と jpc_imagentproxy.service のユニットを監視する場合の定義例を、次に示します。

```
[Unit]
Description = JP1/IM3-Agent Linux metric collector
After=local-fs.target remote-fs.target rsyslog.service network.target
[Service]
WorkingDirectory = @@installdir2@@/jp1ima/bin
ExecStart = /bin/sh -c "'@@installdir1@@/jp1ima/bin/node_exporter" ¥
--collector.cpu.info ¥
(省略)
--no-collector.supervisord ¥
--collector.systemd ¥
--collector.systemd.unit-include="^(jpc_imagent|jpc_imagentproxy)¥.service$" ¥
--no-collector.tcpstat ¥
--no-collector.textfile ¥
--no-collector.thermal_zone ¥
(省略)
```

上記の指定に該当するユニットのうち、自動起動が有効、または、状態が実行中であるユニットが監視対象となります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(1)(d)Node exporter (Linux 性能情報収集機能)」の「監視対象サービスの指定」を参照してください。

(6) Process exporter の設定

(a) 監視対象プロセスの指定 (必須)

■Process exporter 設定ファイル (jpc_process_exporter.yml) の編集

Process exporter 設定ファイル (jpc_process_exporter.yml) を編集し、監視対象プロセスを定義します。

デフォルトでは、コメントアウトによりすべてのプロセスが監視対象外となるため、初期設定のコメントアウトを解除した上で、監視したいプロセスを指定します。

Process exporter 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Process exporter 設定ファイル (jpc_process_exporter.yml)」(2. 定義ファイル) を参照してください。

(b) 監視メトリックの変更 (オプション)

■Prometheus 設定ファイル (jpc_prometheus_server.yml) の編集

収集対象のメトリクスを変更する場合は、Prometheus 設定ファイル (jpc_prometheus_server.yml) の metric_relabel_configs の設定を変更します。

Prometheus 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Prometheus 設定ファイル (jpc_prometheus_server.yml)」(2. 定義ファイル) を参照してください。

■Process exporter のメトリック定義ファイル (metrics_process_exporter.conf) の編集

統合オペレーション・ビューアーの「トレンド」タブに表示するメトリックを変更する場合は、Process exporter のメトリック定義ファイル (metrics_process_exporter.conf) の設定を変更します。

Process exporter のメトリック定義ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Process exporter のメトリック定義ファイル (metrics_process_exporter.conf)」(2. 定義ファイル) を参照してください。

(c) ポートを変更する (オプション)

Process exporter が使用するリッスンポートは、process_exporter コマンドの--web.listen-address オプションに指定します。

process_exporter コマンドのオプションの変更方法については、「[2.19.2\(1\)\(c\)コマンドラインオプションを変更する \(Linux の場合\)](#)」を参照してください。また、--web.listen-address オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユニット定義ファイル (jpc_プログラム名.service)」(2. 定義ファイル) の「コマンドラインのオプションを変更したい場合」を参照してください。

なお、デフォルトのポートは「20721」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

注意事項

- このオプションにホスト名を指定する場合、同じホスト上の Process exporter のディスカバリ設定ファイル (jpc_file_sd_config_process.yml) の targets に、同じホスト名を設定する必要があります。
- このオプションに IP アドレスを指定する場合、同じホスト上の Process exporter のディスカバリ設定ファイル (jpc_file_sd_config_process.yml) の targets に、オプションで指定した IP アドレスに解決されるホスト名を設定する必要があります。

(d) 子プロセスを監視対象から外す設定 (オプション)

Process exporter は、デフォルトでは監視対象プロセスの監視を行う際に、その子プロセスを含めて監視して、子プロセスを含めた稼働情報を取得します。

Process exporter で子プロセスを含めずに稼働情報を取得したい場合は、Process exporter のユニット定義ファイルを次のように編集してください。

編集対象ファイル

- 物理ホストの場合
/usr/lib/systemd/system/jpc_process_exporter.service
- 論理ホストの場合
/usr/lib/systemd/system/jpc_process_exporter_論理ホスト名.service

編集内容

ExecStart に記載する process_exporter の起動オプションで、-children=false を設定してください。

設定例

```
ExecStart = /bin/sh -c '"/opt/jp1ima/bin/process_exporter" ¥  
-children=false ¥  
-debug=true ¥  
--config.path="/opt/jp1ima/conf/jpc_process_exporter.yml" ¥
```

(7) Blackbox exporter の設定

(a) ポートを変更する (Linux の場合) (オプション)

Blackbox exporter が使用するリッスンポートは、blackbox_exporter コマンドの--web.listen-address オプションに指定します。

blackbox_exporter コマンドのオプションの変更方法については、[「2.19.2\(1\)\(c\) コマンドラインオプションを変更する \(Linux の場合\)」](#)を参照してください。また、--web.listen-address オプションの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユニット定義ファイル (jpc_プログラム名.service)」(2. 定義ファイル) の「コマンドラインのオプションを変更したい場合」を参照してください。

なお、デフォルトのポートは「20715」です。ポート番号を変更した場合は、ファイアウォールの設定を見直して、外部からのアクセスを禁止してください。

(b) モジュールを追加・変更・削除する (Linux の場合) (オプション)

「1.21.2(6)(b)モジュールを追加・変更・削除する (Windows の場合) (オプション)」を参照してください。

(c) 監視対象を追加・変更・削除する (Linux の場合) (必須)

「1.21.2(6)(c)監視対象を追加・変更・削除する (Windows の場合) (必須)」を参照してください。

(d) プロキシ経由で HTTP 監視をする (Linux の場合) (オプション)

「1.21.2(6)(d)プロキシ経由で HTTP 監視をする (Windows の場合) (オプション)」を参照してください。

(e) プロキシ認証の認証 ID とパスワードを設定する (Linux の場合) (オプション)

「1.21.2(6)(e)プロキシ認証の認証 ID とパスワードを設定する (Windows の場合) (オプション)」を参照してください。

(f) 監視対象の Web サーバにアクセスするための認証 ID, パスワード, Bearer トークンを設定する (Linux の場合) (オプション)

「1.21.2(6)(f)監視対象の Web サーバにアクセスするための認証 ID, パスワード, Bearer トークンを設定する (Windows の場合) (オプション)」を参照してください。

(8) Yet another cloudwatch exporter の設定

(a) ポートを変更する (Linux の場合) (オプション)

「1.21.2(7)(a)ポートを変更する (Windows の場合) (オプション)」を参照してください。

(b) CloudWatch に接続するための設定を変更する (Linux の場合) (必須)

「1.21.2(7)(b)CloudWatch に接続するための設定を変更する (Windows の場合) (必須)」を参照してください。

(c) CloudWatch にプロキシ経由で接続する (Linux の場合) (オプション)

「1.21.2(7)(c)CloudWatch にプロキシ経由で接続する (Windows の場合) (オプション)」を参照してください。

(d) 監視する AWS サービスを追加する (オプション)

「1.21.2(7)(d)監視する AWS サービスを追加する (オプション)」を参照してください。

(e) AWS リソースを監視対象にする (必須)

「1.21.2(7)(e)AWS リソースを監視対象にする (必須)」を参照してください。

(f) 収集するメトリックを変更する (オプション)

「1.21.2(7)(f)収集するメトリックを変更する (オプション)」を参照してください。

(9) Promitor の設定

「1.21.2(8)Promitor の設定」を参照してください。

(10) Fluentd の設定

(a) ログ監視の共通定義の設定を変更する (オプション)

「1.21.2(9)(a)ログ監視の共通定義の設定を変更する (Windows の場合) (オプション)」を参照してください。

(b) テキスト形式のログファイルを監視する (必須)

「1.21.2(9)(b)テキスト形式のログファイルを監視する (Windows の場合) (必須)」を参照してください。

(c) テキスト形式のログファイルの監視設定を変更する (オプション)

「1.21.2(9)(c)テキスト形式のログファイルの監視設定を変更する (Windows の場合) (オプション)」を参照してください。

(d) テキスト形式のログファイルの監視設定を削除する (オプション)

「1.21.2(9)(d)テキスト形式のログファイルの監視設定を削除する (Windows の場合) (オプション)」を参照してください。

(e) ログメトリクス定義の設定 (必須)

「1.21.2(9)(h)ログメトリクス定義の設定 (必須)」を参照してください。

(f) ポートを変更する (オプション)

「1.21.2(9)(i)ポートを変更する (オプション)」を参照してください。

(g) SAP システムのログ情報を監視する (オプション)

「1.21.2(9)(j)SAP システムのログ情報を監視する (オプション)」を参照してください。

(h) SAP システムのログ情報の監視設定を変更する (オプション)

「1.21.2(9)(k)SAP システムのログ情報の監視設定を変更する (オプション)」を参照してください。

(i) SAP システムのログ情報の監視設定を削除する (オプション)

「1.21.2(9)(l)SAP システムのログ情報の監視設定を削除する (オプション)」を参照してください。

(j) SAP システムの CCMS アラート情報を監視する (オプション)

「1.21.2(9)(m)SAP システムの CCMS アラート情報を監視する (オプション)」を参照してください。

(k) SAP システムの CCMS アラート情報の監視設定を変更する (オプション)

「1.21.2(9)(n)SAP システムの CCMS アラート情報の監視設定を変更する (オプション)」を参照してください。

(l) SAP システムの CCMS アラート情報の監視設定を削除する (オプション)

「1.21.2(9)(o)SAP システムの CCMS アラート情報の監視設定を削除する (オプション)」を参照してください。

(11) スクレイプ定義の設定

「1.21.2(10)スクレイプ定義の設定」を参照してください。

(12) コンテナ監視の設定

「1.21.2(11)コンテナ監視の設定」を参照してください。

(13) Script exporter の定義ファイルの編集

「1.21.2(12)Script exporter の定義ファイルの編集」を参照してください。

(14) VMware exporter の設定

「1.21.2(14)VMware exporter の設定」を参照してください。

(15) リッスンポート番号とリッスンアドレスの設定 (オプション)

「1.21.2(16)リッスンポート番号とリッスンアドレスの設定 (オプション)」を参照してください。

(16) ファイアウォールの設定 (Linux の場合) (必須)

「1.21.2(17)ファイアウォールの設定 (Windows の場合) (必須)」を参照してください。

(17) 統合エージェントのプロセスの死活監視の設定 (Linux の場合) (オプション)

統合エージェントのプロセスは、次の種類の方法で監視します。

- 他ホストの Blackbox exporter による外形監視
- Process exporter によるプロセスの死活監視
- Prometheus server の up メトリックによる監視

(a) 他ホストの Blackbox exporter による外形監視

Prometheus server サービスと Alertmanager サービスは、他ホスト上で稼働している統合エージェントの Blackbox exporter から監視します。監視する URL は、次の表のとおりです。

Blackbox exporter の HTTP 監視を追加する方法については、「[1.21.2\(6\)\(c\)監視対象を追加・変更・削除する（Windows の場合）（必須）](#)」を参照してください。アラート定義の設定方法については、「[1.21.2\(3\)\(b\)アラート定義を追加する（Windows の場合）（オプション）](#)」を参照してください。

Blackbox exporter の HTTP 監視で監視するアラート定義の例については、「[1.21.2\(18\)統合エージェントのプロセスの死活監視の設定（Windows の場合）（オプション）](#)」を参照してください。

表 2-12 Blackbox exporter の HTTP 監視で監視する URL

サービス	監視する URL
Prometheus server	http://統合エージェントのホスト名:Prometheus server のポート番号/-/healthy
Alertmanager	http://統合エージェントのホスト名:Alertmanager のポート番号/-/healthy

(b) Process exporter によるプロセスの死活監視

imagentproxy サービス、imagentaction サービス、Fluentd サービスは、Process exporter のプロセス監視の稼動情報で監視します。監視するプロセスは次の表に記載されています。

設定方法の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「Process exporter 設定ファイル (jpc_process_exporter.yml)」(2. 定義ファイル) を参照してください。

アラート定義の設定方法については、「[1.21.2\(3\)\(b\)アラート定義を追加する（Windows の場合）（オプション）](#)」を参照してください。

表 2-13 Process exporter で監視するプロセス

サービス	監視するプロセス	備考
imagent	Agent パス/bin/imagent	マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.8(2)統合エージェント制御基盤のポーリング監視」の注意事項に記載している imagent が異常停止してから短時間で起動するケースを検知したい場合に設定します。

サービス	監視するプロセス	備考
imagentproxy	Agent パス/bin/imagentproxy	該当なし。
imagentaction	Agent パス/bin/imagentaction	該当なし。
Fluentd	Agent パス/lib/ruby/bin/ruby	コマンドラインに「jpc_fluentd_common.conf」の文字列があるため、Fluentd 以外の ruby と区別できます。
rotatelog (Fluentd の場合だけ)	Agent パス/bin/rotatelog	コマンドラインに「Agent パス/logs/fluentd」の文字列があるため、Fluentd 以外の rotatelog と区別できます。

Process exporter で監視する Process exporter 設定ファイルの例を、次に示します。

```
process_names:
- name: "{{.ExeBase}};{{.Username}};{{.Matches.cmdline}}"
  exe:
    - /opt/jplima/bin/imagent
    - /opt/jplima/bin/imagentproxy
    - /opt/jplima/bin/imagentaction

- name: "{{.ExeBase}};{{.Username}};{{.Matches.cmdline}}"
  exe:
    - /opt/jplima/bin/rotatelog
  cmdline:
    - (?P<cmdline>.*\/opt\/jplima\/logs\/fluentd¥.*)

- name: "{{.ExeBase}};{{.Username}};{{.Matches.cmdline}}"
  exe:
    - /opt/jplima/lib/ruby/bin/ruby
  cmdline:
    - (?P<cmdline>.*jpc_fluentd_common¥.conf.*)
```

Process exporter で監視するアラート定義の例を、次に示します。

```
groups:
- name: process_exporter
  rules:
    - alert: jp1_pc_procmon_imagent
      expr: 1 > sum by (program, instance, job, jp1_pc_nodelabel, jp1_pc_exporter) (namedprocess_namegroup_num_procs{program="imagent"})
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1303"
        jp1_pc_metricname: "namedprocess_namegroup_num_procs"
      annotations:
        jp1_pc_firing_description: "プロセス数がしきい値(1個)を下回りました。value={{ $value }}"
    }
```



```

    jp1_pc_resolved_description: "プロセス数がしきい値(1個)を上回りました。"

- alert: jp1_pc_procmon_imagentproxy
  expr: 1 > sum by (program, instance, job, jp1_pc_nodelabel, jp1_pc_exporter) (namedprocess_namegroup_num_procs{program="imagentproxy"})
  for: 3m
  labels:
    jp1_pc_product_name: "/HITACHI/JP1/JPCS2"
    jp1_pc_component: "/HITACHI/JP1/JPCS/CONFINFO"
    jp1_pc_severity: "Error"
    jp1_pc_eventid: "1303"
    jp1_pc_metricname: "namedprocess_namegroup_num_procs"
  annotations:
    jp1_pc_firing_description: "プロセス数がしきい値(1個)を下回りました。value={{ $value }}"
    jp1_pc_resolved_description: "プロセス数がしきい値(1個)を上回りました。"

- alert: jp1_pc_procmon_imagentactoin
  expr: 1 > sum by (program, instance, job, jp1_pc_nodelabel, jp1_pc_exporter) (namedprocess_namegroup_num_procs{program="imagentaction"})
  for: 3m
  labels:
    jp1_pc_product_name: "/HITACHI/JP1/JPCS2"
    jp1_pc_component: "/HITACHI/JP1/JPCS/CONFINFO"
    jp1_pc_severity: "Error"
    jp1_pc_eventid: "1303"
    jp1_pc_metricname: "namedprocess_namegroup_num_procs"
  annotations:
    jp1_pc_firing_description: "プロセス数がしきい値(1個)を下回りました。value={{ $value }}"
    jp1_pc_resolved_description: "プロセス数がしきい値(1個)を上回りました。"

- alert: jp1_pc_procmon_fluentd_rotatelog Log trapper(Fluentd) ※1
  expr: 1 > sum by (program, instance, job, jp1_pc_nodelabel, jp1_pc_exporter) (namedprocess_namegroup_num_procs{program="rotatelog"})
  for: 3m
  labels:
    jp1_pc_product_name: "/HITACHI/JP1/JPCS2"
    jp1_pc_component: "/HITACHI/JP1/JPCS/CONFINFO"
    jp1_pc_severity: "Error"
    jp1_pc_eventid: "1303"
    jp1_pc_metricname: "namedprocess_namegroup_num_procs"
  annotations:
    jp1_pc_firing_description: "プロセス数がしきい値(1個)を下回りました。value={{ $value }}"
    jp1_pc_resolved_description: "プロセス数がしきい値(1個)を上回りました。"

- alert: jp1_pc_procmon_fluentd_ruby Log trapper(Fluentd) ※2
  expr: 2 > sum by (program, instance, job, jp1_pc_nodelabel, jp1_pc_exporter) (namedprocess_namegroup_num_procs{program="ruby"}) ※3
  for: 3m
  labels:
    jp1_pc_product_name: "/HITACHI/JP1/JPCS2"
    jp1_pc_component: "/HITACHI/JP1/JPCS/CONFINFO"
    jp1_pc_severity: "Error"
    jp1_pc_eventid: "1303"
    jp1_pc_metricname: "namedprocess_namegroup_num_procs"
  annotations:

```

```
    jp1_pc_firing_description: "プロセス数がしきい値(2個)を下回りました。value={{ $value  
  }}"  
    jp1_pc_resolved_description: "プロセス数がしきい値(2個)を上回りました。"
```

注※1

ログメトリクス機能のみ使う場合、「jp1_pc_procmon_fluentd_prome_rotatelogs Log trapper(Fluentd)」を指定します。

注※2

ログメトリクス機能のみ使う場合、「jp1_pc_procmon_fluentd_prome_ruby Log trapper(Fluentd)」を指定します。

注※3

ruby のプロセスは worker の数+1 起動します。しきい値は worker の数+1 を指定してください。
worker の数については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ログ監視共通定義ファイル (jpc_fluentd_common.conf)」(2. 定義ファイル) を参照してください。

(c) Prometheus server の up メトリックによる監視

Node exporter サービス、Process exporter サービス、Blackbox exporter サービス、Yet another cloudwatch exporter サービスは、Prometheus server のアラート監視で監視します。アラート定義の設定方法については、「[1.21.2\(3\)\(b\)アラート定義を追加する \(Windows の場合\) \(オプション\)](#)」を参照してください。

up メトリックを監視するアラート定義の例については、「[1.21.2\(18\)統合エージェントのプロセスの死活監視の設定 \(Windows の場合\) \(オプション\)](#)」を参照してください。

(18) IM 管理ノードのツリー情報の作成と反映 (Linux の場合) (必須)

「[1.21.2\(19\) IM 管理ノードのツリー情報の作成と反映 \(Windows の場合\) \(必須\)](#)」を参照してください。

(19) セキュリティ製品の除外設定 (Linux の場合) (オプション)

「[1.21.2\(20\)セキュリティ製品の除外設定 \(Windows の場合\) \(オプション\)](#)」を参照してください。

(20) 定義ファイル更新時の注意事項 (Linux の場合)

「[1.21.2\(21\)定義ファイル更新時の注意事項 \(Windows の場合\)](#)」を参照してください。

2.20 JP1/IM - Agent のコンテナ環境の構築 (UNIX の場合)

JP1/IM - Agent のコンテナ環境の構築手順については、「[1.22 JP1/IM - Agent のコンテナ環境の構築 \(Windows の場合\)](#)」を参照してください。

2.21 JP1/IM - Agent のオプション機能の構築 (UNIX の場合)

2.21.1 OracleDB exporter の設定

ここでは、統合エージェントホストのオプション機能である OracleDB exporter の設定手順について説明します。

(1) OracleDB exporter の設定の前準備

Windows の場合と共通です。「[1.23.1\(1\)OracleDB exporter の設定の前準備](#)」を参照してください。

(2) OracleDB exporter のインストール

Windows の場合と共通です。「[1.23.1\(2\)OracleDB exporter のインストール](#)」を参照してください。

(3) OracleDB exporter のアンインストール

Windows の場合と共通です。「[1.23.1\(3\)OracleDB exporter のアンインストール](#)」を参照してください。

(4) OracleDB exporter の設定

OracleDB exporter の設定方法について説明します。

(a) 監視対象を追加する (必須)

■ 監視対象を追加するための準備

Windows の場合と共通です。「[1.23.1\(4\)\(a\)監視対象を追加する \(必須\)](#)」の「**■監視対象を追加するための準備**」を参照してください。

■ OracleDB exporter の設定

1. ユニット定義ファイルを作成する。

コピー元のユニット定義ファイルをコピーし、コピー先のファイル名にリネームします。

作成したユニット定義ファイルのオーナーおよびオーナーグループは root、アクセス権は 644 にします。

コピー元のファイル名：OracleDB exporter の配置先/oracledb_exporter_linux/jp1ima/conf/oracledb_exporter_@@instance@@.service.model

コピー先のファイル名：

- 物理ホスト運用の場合
OracleDB exporter の配置先/oracledb_exporter_linux/jp1ima/conf/oracledb_exporter_インスタンス名[※].service
- 論理ホスト運用の場合

2. インストールとセットアップ (UNIX の場合)

OracleDB exporter の配置先/oracledb_exporter_linux/jp1ima/conf/oracledb_exporter_インスタンス名*_論理ホスト名.service

注※

インスタンス名は、「1.23.1(4)(a)監視対象を追加する（必須）」の「■監視対象を追加するための準備」で決めた名称を指定します。

2. ユニット定義ファイルを更新する。

手順 1. で作成したユニット定義ファイルの次の値を表のとおりに変更します。

変更する値	指定する値
@@instance@@	- 物理ホスト運用の場合 「1.23.1(4)(a)監視対象を追加する（必須）」の「■監視対象を追加するための準備」の手順 1. で決めた名称に置換する。 - 論理ホスト運用する場合 「1.23.1(4)(a)監視対象を追加する（必須）」の「■監視対象を追加するための準備」の手順 1. で決めた名称「_論理ホスト名」を付与した値に置換する。
@@oracledb_exporter_installdir@@	OracleDB exporter の配置先に置換する。
@@port@@	「1.23.1(4)(a)監視対象を追加する（必須）」の「■監視対象を追加するための準備」の手順 2. で決めたポート番号に置換する。 論理ホストの場合は論理ホスト名も指定し、 <code>--web.listen-address="論理ホスト名:ポート番号"</code> となるように置換する。
@@installdir2@@	「1.23.1(4)(a)監視対象を追加する（必須）」の「■監視対象を追加するための準備」の手順 3. で確認したディレクトリに置換する。
@@data_source_name@@	「1.23.1(4)(a)監視対象を追加する（必須）」の「■監視対象を追加するための準備」の手順 4. で確認した内容に置換する。

3. ユニット定義ファイルを systemd に登録する。

手順 2. で更新したユニット定義ファイルを次のディレクトリ配下にコピー※します。論理ホスト運用の場合は、クラスタを構成する両ノードでコピーします。

コピー先のディレクトリ：`/usr/lib/systemd/system`

注※

移動ではなくコピーしてください。移動した場合、SELinux のパーミッションが正しく設定されず、サービスが正しく起動されない場合があります。

ユニット定義ファイルをコピー先のディレクトリにコピーした後、次のコマンドを実行し、systemd をリロードします。論理ホスト運用の場合は、クラスタを構成する両ノードでコマンドを実行します。

```
systemctl daemon-reload
```

物理ホスト運用で OS 起動時に自動起動させたい場合は、次のコマンドを実行します。論理ホスト運用の場合は、自動起動させません。

```
systemctl enable サービス名
```

4. ログディレクトリを作成する。

OracleDB exporter の配置先にログディレクトリを作成します。

作成したディレクトリのオーナーおよびオーナーグループは root、アクセス権は 700 にします。

- 物理ホスト運用の場合

OracleDB exporter の配置先/`oracledb_exporter_linux/jp1ima/logs/oracledb_exporter/インスタンス名※`

- 論理ホスト運用の場合

OracleDB exporter の配置先/`oracledb_exporter_linux/jp1ima/logs/oracledb_exporter/インスタンス名※_論理ホスト名`

注※

インスタンス名は、「1.23.1(4)(a)監視対象を追加する (必須)」の「■監視対象を追加するための準備」で決めた名称を指定します。

5. Oracle Database への接続に使用するユーザーのパスワードを登録する。

Oracle Database への接続に使用するユーザーのパスワードを `jimasecret` コマンドで登録します。

- 物理ホスト運用の場合

```
jimasecret -add -key OracleDB.user.ユーザー名 -s パスワード
```

- 論理ホスト運用の場合

```
jimasecret -add -key OracleDB.user.ユーザー名 -s パスワード -l 共有ディレクトリ
```

同一ユーザー名でパスワードが異なるユーザーを登録したい場合は、ホスト名とサービス名を含むキーを使用することができます。

`jimasecret` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jimasecret`」(1. コマンド)を参照してください。

6. クラスタソフトにサービスを登録する。

クラスタ構成の場合は、クラスタソフトにサービスを登録します。

7. OracleDB exporter サービスを起動する。

`systemctl start` コマンドで OracleDB exporter のサービスを起動します。

クラスタ構成の場合はクラスタソフトからサービスを起動します。

8. OracleDB exporter で性能情報が取得できることを確認する。

`curl` コマンドやブラウザで次の URL にアクセスし、性能情報が取得できているか確認してください。

```
http://ホスト名:ポート/metrics
```

ホスト名には OracleDB exporter を起動しているホスト、ポートには OracleDB exporter のリスニングポートを指定します。

■ Prometheus の設定

Windows の場合と共通です。「[1.23.1\(4\)\(a\)監視対象を追加する（必須）](#)」の「**■Prometheus の設定**」を参照してください。

■ インテリジェント統合管理基盤の設定

Windows の場合と共通です。「[1.23.1\(4\)\(a\)監視対象を追加する（必須）](#)」の「**■インテリジェント統合管理基盤の設定**」を参照してください。

(b) OracleDB exporter のポートを変更する（オプション）

Windows の場合と共通です。「[1.23.1\(4\)\(b\)OracleDB exporter のポートを変更する（オプション）](#)」を参照してください。

(c) 接続のためのパスワードを変更する（オプション）

Windows の場合と共通です。「[1.23.1\(4\)\(c\)接続のためのパスワードを変更する（オプション）](#)」を参照してください。

(d) 監視対象を削除する（オプション）

■ Prometheus の設定

Windows の場合と共通です。「[1.23.1\(4\)\(d\)監視対象を削除する（オプション）](#)」の「**■Prometheus の設定**」を参照してください。

■ Prometheus の設定

Windows の場合と共通です。「[1.23.1\(4\)\(d\)監視対象を削除する（オプション）](#)」の「**■クラスタソフトから OracleDB exporter を削除**」を参照してください。

■ OracleDB exporter の設定

1. 削除する監視対象の OracleDB exporter サービスを停止する。

systemctl start コマンドで OracleDB exporter のサービスを停止します。

2. ユニット定義ファイルを削除する。

次に示すユニット定義ファイルを削除します。

- 物理ホスト運用の場合
oracledb_exporter_インスタンス名_service
- 論理ホスト運用の場合
oracledb_exporter_インスタンス名_論理ホスト名_service

論理ホスト運用の場合はクラスタを構成する両ノードで削除してください。

3. systemctl を更新する。

次のコマンドを実行し、systemctl を更新します。

systemctl daemon-reload

論理ホスト運用の場合はクラスタを構成する両ノードで削除してください

4. Oracle Database への接続に使用するユーザーのパスワードを削除する。

ほかの OracleDB exporter で同じユーザーを使用していない場合は、登録済みのパスワードを `jimasecret` コマンドで削除します。

- 物理ホスト運用の場合

```
jimasecret -rm -key OracleDB.user.ユーザー名
```

- 論理ホスト運用の場合

```
jimasecret -rm -key OracleDB.user.ユーザー名 -s パスワード -l 共有ディレクトリ
```

ホスト名やリスナー名を含むキーを指定して登録した場合は、そのキーを指定してください。

(e) OracleDB exporter の死活監視を設定する（オプション）

Windows の場合と共通です。「[1.23.1\(4\)\(e\)OracleDB exporter の死活監視を設定する（オプション）](#)」を参照してください。

(f) 接続のためのユーザーを変更する（オプション）

1. Oracle Database に新しいユーザーを追加する。

2. OracleDB exporter を停止する。

3. 変更前のユーザーのパスワードを削除する。

Oracle Database への接続に使用するユーザーのパスワードを `jimasecret` コマンドで削除する。

- 物理ホスト運用の場合

```
jimasecret -rm -key OracleDB.user.旧ユーザー名
```

- 論理ホスト運用の場合

```
jimasecret -rm -key OracleDB.user.旧ユーザー名 -l 共有ディレクトリ
```

同一ユーザー名でパスワードが異なるユーザーを登録したい場合は、ホスト名とサービス名を含むキーを使用してください。

4. 変更後のユーザーのパスワードを登録する。

Oracle Database への接続に使用するユーザーのパスワードを `jimasecret` コマンドで登録します。

- 物理ホスト運用の場合

```
jimasecret -add -key OracleDB.user.新ユーザー名 -s パスワード
```

- 論理ホスト運用の場合

```
jimasecret -add -key OracleDB.user.新ユーザー名 -s パスワード -l 共有ディレクトリ
```

同一ユーザー名でパスワードが異なるユーザーを登録したい場合は、ホスト名とサービス名を含むキーを使用することができます。

5. 環境変数 DATA_SOURCE_NAME を修正する。

ユニット定義ファイルをテキストエディターで開き、環境変数 DATA_SOURCE_NAME に記載されているユーザー名を新しいユーザー名に変更して保存します。

6. OracleDB exporter を起動する。

7. Oracle Database から変更前のユーザーを削除する。

変更前のユーザーが不要な場合、Oracle Database から変更前のユーザーを削除してください。

(5) クラスタ環境

Windows の場合と共通です。「[1.23.1\(5\)クラスタ環境](#)」を参照してください。

2.21.2 Node exporter for AIX の設定

Windows の場合と同じです。「[1.23.2 Node exporter for AIX の設定](#)」を参照してください。

2.21.3 SAP システム監視の設定

Windows の場合と同じです。「[1.23.3 SAP システム監視の設定](#)」を参照してください。

2.22 マニュアルの組み込み手順 (UNIX の場合)

所定のディレクトリに HTML マニュアルを格納することで、各画面の [ヘルプ] ボタンからマニュアルを参照できます。

HTML マニュアルの組み込み手順を次に示します。

1. プログラムプロダクトに標準添付されているマニュアル提供媒体を用意する。

2. マニュアル提供媒体に格納されている対象データを JP1/IM - Manager に格納する。

マニュアル提供媒体の格納先ディレクトリ配下に格納されているすべての対象データを、マニュアルごとに JP1/IM - Manager の格納先ディレクトリに格納してください。

すべてのマニュアルを正しく配置することで、マニュアルの目次ページを表示できるようになります。

データを誤って配置している状態や一部のデータだけを配置している状態で [ヘルプ] - [目次] を選択すると、エラーダイアログボックス (KAVB8550-E) が表示されます。

- 格納されている対象データ (HTML マニュアル)
CSS ファイル, HTM ファイル, GRAPHICS フォルダ
- マニュアル提供媒体側の格納先 (UNIX マシンのドライブにマニュアル提供媒体をセットした場合)
「マニュアル提供媒体のマウントポイント/MAN/3021/」配下に資料番号フォルダ単位でマニュアルが格納されています。ここに格納されているマニュアルがどの製品に対応するかを確認する場合は、資料番号フォルダ配下の INDEX.HTM を参照してください。
- JP1/IM - Manager 側の格納先
「/opt/jp1cons/www/manual/ja/」配下
「/opt/jp1imm/public/manual/ja」配下
各資料番号のフォルダに、マニュアル提供媒体の資料番号フォルダ配下に格納されているすべての対象データを格納してください。

ファイルを FTP で転送する場合は、バイナリ転送してください。

すでに HTML マニュアルが JP1/IM - Manager の格納先ディレクトリに格納されている場合は、格納されている HTML マニュアルを削除してから格納してください。

2.23 アンインストール (UNIX の場合)

ここでは、JP1/IM - Manager および JP1/IM - Agent をアンインストールする手順について説明します。
なお、アンインストール作業を行うユーザーは、root 権限が必要です。

2.23.1 アンインストール手順 (UNIX の場合)

JP1/IM - Manager および JP1/IM - Agent をアンインストールする手順について説明します。

なお、IM データベース（統合監視 DB および IM 構成管理 DB）およびインテリジェント統合管理データベースを使用している場合は、JP1/IM - Manager をアンインストールする前に IM データベースおよびインテリジェント統合管理データベースを削除する必要があります。

また、インテリジェント統合管理データベースサービスがセットアップされている場合、Hitachi PP Installer の端末上に「Deletion failed.」と表示され、アンインストールに失敗します。その場合、最新の更新日時の JP1/IM - Manager のインストーラーのログ（/tmp/HITACHI_JP1_INST_LOG/jp1imm_inst{1|2|3|4|5}.log）に、KAVB9944-E メッセージ（物理ホストのとき）または KAVB9945-E メッセージ（論理ホストのとき）が出力されていることを確認してください。

KAVB9944-E メッセージまたは KAVB9945-E メッセージが出力されている場合は、アンセットアップコマンド（jimgndbunsetup コマンド）で、インテリジェント統合管理データベースサービスをアンセットアップしたあと、再度 JP1/IM - Manager をアンインストールしてください。KAVB9946-E メッセージが出力されている場合は、KAVB9946-E メッセージの対処に従ってください。

(1) インテリジェント統合管理データベースの削除の手順

環境を再構築するためにインテリジェント統合管理データベースを削除する場合は、事前にバックアップを取得してください。バックアップの方法については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「1.2 データベースの管理」を参照してください。

次の手順でインテリジェント統合管理データベースを削除します。

1. JP1/IM - Manager を停止する。

JP1/IM - Manager を停止してください。

2. インテリジェント統合管理データベースを削除する。

次のコマンドを実行してください。

- 物理ホスト運用の場合

```
jimgndbunsetup [-q]
```

- 論理ホスト運用で実行系ホストの場合

```
jimgndbunsetup -h 論理ホスト名 -c online [-q]
```

- 論理ホスト運用で待機系ホストの場合

```
jimgndbunsetup -h 論理ホスト名 -c standby [-q]
```

3. マシンを再起動する。

(2) IM データベースの削除の手順

環境を再構築するために IM データベースを削除する場合は、事前にバックアップを取得してください。バックアップの方法については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「1.2 データベースの管理」を参照してください。

各コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「1. コマンド」を参照してください。

次の手順で IM データベースを削除します。

1. JP1/IM - Manager を停止する。

JP1/IM - Manager を停止してください。JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスも停止してください。

2. 統合監視 DB または IM 構成管理 DB を削除する場合、次のサービスの状態を確認する。

- 物理ホストの場合

IM データベースサービス (JP1/IM3-Manager DB Server) が開始している。

- 物理ホストの場合に、統合監視 DB または IM 構成管理 DB がセットアップ済み、かつ IM データベースを使用しているとき

JP1/IM - Manager のサービス (JP1/IM3-Manager) が停止している。

- 論理ホストの場合

論理ホストの IM データベースサービス (JP1/IM3-Manager DB Server_論理ホスト名) が開始している。

- 論理ホストの場合に、統合監視 DB または IM 構成管理 DB がセットアップ済み、かつ IM データベースを使用しているとき

JP1/IM - Manager のサービス (JP1/IM3-Manager_論理ホスト名) が停止している。

3. 統合監視 DB を削除する場合、jcoimdef コマンドを実行する。

```
jcoimdef -db OFF
```

統合監視 DB が無効になります。

4. 統合監視 DB を削除する場合、jcodbunsetup コマンドを実行する。

```
jcodbunsetup
```

統合監視 DB が削除されます。

5. IM 構成管理 DB を削除する場合、jcoimdef コマンドを実行する。

```
jcoimdef -cf OFF
```

IM 構成管理サービス (jcfmain) が無効になります。

6. IM 構成管理 DB を削除する場合、jcfdbunsetup コマンドを実行する。

```
jcfdbunsetup
```

IM 構成管理 DB が削除されます。

7. 次の物理ホストのファイルおよびディレクトリを削除する。

/var/opt/jp1imm/data/imcf/imconfig 以下のファイル

/var/opt/jp1imm/data/imcf/profiles 以下のファイルおよびディレクトリ

8. マシンを再起動する。

(3) JP1/IM - Manager のアンインストールの手順

次の手順でアンインストールします。この作業には、root 権限が必要です。

なお、JP1/IM - Manager をアンインストールすると、JP1/IM - Agent を利用するための統合エージェント管理基盤もアンインストールされます。

1. プログラムを終了する。

アンインストールする前に、JP1/IM - Manager を前提とするプログラムを停止してください。また、接続中の JP1/IM - View がある場合は停止してください。

2. ユーザーファイルをバックアップする。

JP1/IM - Manager のアンインストールでは、定義ファイルやログファイルなども含めて、フォルダごと削除されますので、必要に応じてバックアップしてください。

3. Hitachi PP Installer を実行する。

Hitachi PP Installer の指示に従ってアンインストールしてください。

4. ユーザーファイルを削除する。

ファイルを使用中のプロセスがあった場合などには、ファイルが残ることがあります。次のディレクトリを確認して手動で削除してください。

- /opt/jp1imm/
- /var/opt/jp1imm/
- /etc/opt/jp1cons/
- /opt/jp1cons/
- /var/opt/jp1cons/
- /etc/opt/jp1scope/
- /opt/jp1scope/

- /var/opt/jp1scope/

なお、JP1/IM - Manager のアンインストール時にインストーラーのログとして次のファイルが作成されます。これはアンインストールが異常終了した場合の保守資料です。アンインストールが正常終了したあとに削除してください。

- /tmp/HITACHI_JP1_INST_LOG/jp1imm_inst{1|2|3|4|5}.log

(4) JP1/IM - Agent のアンインストールの手順

次の手順でアンインストールします。この作業には、root 権限が必要です。

JP1/IM - Agent のアンインストールでは、定義ファイルやログファイルなども含めて、フォルダごと削除されますので、必要に応じてバックアップしてください。

1. JP1/IM - Agent のサービスを停止する。

2. 複数マネージャーホストへのデータ配信機能を使用している場合は、サービス削除の前に次の手順を実施する。

「[2.19.2\(2\)\(i\) 複数マネージャーホストへのデータ配信機能を解除する \(Linux の場合\) \(オプション\)](#)」に記載している「JP1/IM - Agent 自体のアンインストールを行う場合」を実施します。

3. JP1/IM - Agent サービス削除を実行する。

サービスの削除方法については、「[2.19.1\(1\)\(b\) アドオンプログラムの無効化](#)」を参照してください。

4. Hitachi PP Installer を起動し、JP1/IM - Agent を削除します。

5. 削除が完了したら、統合マネージャーの統合オペレーション・ビューアーにログインし、削除したホストの統合エージェント情報が削除されていることを確認します。削除されていない場合は、手動で削除します。

統合エージェント情報の削除手順については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「[2.2.1 \[統合エージェント一覧\] 画面](#)」を参照してください。

❗ 重要

論理ホストのサービスを起動している場合は、サービスを停止したのち論理ホストのサービスを削除してから実行してください。論理ホストのサービス起動中にアンインストールを実行すると、論理ホストのサービスで使用するファイルが削除され、サービスが異常終了する可能性があります。論理ホストのサービスを削除せずアンインストールを実行した場合は、アンインストール後に論理ホストのサービスを削除してください。

2.23.2 アンインストール時の注意事項（UNIX の場合）

(1) OS 環境への設定

JP1/IM - Manager のアンインストール時に、`services` ファイルに設定された、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 C ポート番号」のポート番号が削除されます。

(2) JP1/Base のアンインストールについて

JP1/Base をアンインストールすると、JP1/IM - Manager の定義情報も削除されます。JP1/Base を再インストールしても、JP1/IM - Manager は動作しません。このような場合、`jp1cc_setup` コマンド、`jp1cs_setup` コマンド、および `jp1cf_setup` コマンドを実行して環境設定を行う必要があります。

(3) アンインストール後の確認について

JP1/IM - Manager のアンインストール後、次のディレクトリが残っていないか確認し、残っている場合は削除してください。

- `/etc/opt/jp1cons`
- `/opt/jp1cons`
- `/var/opt/jp1cons`
- `/etc/opt/jp1scope`
- `/opt/jp1scope`
- `/var/opt/jp1scope`

JP1/IM - Manager をアンインストールすると、監視オブジェクト DB およびホスト情報 DB は削除されます。

(4) 物理ホストで IM データベースを手動アンインストールする場合の手順

物理ホストで、IM データベースを手動でアンインストールする場合、次に示す手順を実施してください。

1. スーパーユーザーでログインします。
2. JP1/IM - Manager が起動している場合は停止します。
3. 下記のファイルを削除します。
 - `/usr/lib/systemd/system/2248-PDxx-start.service`
 - `/usr/lib/systemd/system/2248-PDxx-stop.service`
 - `/usr/lib/systemd/system/2248-PDxx.service`
 - `/usr/lib/systemd/system/2248-pexx.service`

ファイル名の`xx` 部分は 01 からの通番となります。上記ファイルに以下の内容が記載されていることを確認してから削除してください。誤ったファイルを削除すると例えば論理ホストの IM データベースが正常に動作しなくなる、などの影響がありますので、十分に注意してください。

確認内容

<IMDBENVDIR>/JM0

<IMDBENVDIR>：削除対象の物理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したセットアップ情報ファイル（`jimdbsetupinfo.conf`）のIMDBENVDIR パラメーターに指定したパスです。

4. 下記のシンボリックリンクファイルを削除します。

- `/etc/systemd/system/multi-user.target.wants/2248-PDxx-start.service`
- `/etc/systemd/system/multi-user.target.wants/2248-PDxx-stop.service`
- `/etc/systemd/system/multi-user.target.wants/2248-PDxx.service`
- `/etc/systemd/system/multi-user.target.wants/2248-pexx.service`

ファイル名の`xx` 部分は 01 からの通番となります。上記ファイルに以下の内容が記載されていることを確認してから削除してください。誤ったファイルを削除すると例えば論理ホストの IM データベースが正常に動作しなくなる、などの影響がありますので、十分に注意してください。

確認内容

<IMDBENVDIR>/JM0

<IMDBENVDIR>：削除対象の物理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したセットアップ情報ファイル（`jimdbsetupinfo.conf`）のIMDBENVDIR パラメーターに指定したパスです。

5. 以下の手順で IM データベースの設定ファイルを更新してください。

- `/etc/opt/jp1imm/conf/imdb/system/dbconf/JM0` を削除する。
- `/etc/opt/jp1imm/conf/imdb/system/dbconf/jimdbsetuplist.conf` をテキストエディタで開き、以下のように編集してJP1_DEFAULT を削除して、上書き保存する。

編集前

`_JM0=JP1_DEFAULT`

編集後

`_JM0=`

6. OS を再起動してください。

7. 次を示すディレクトリが存在する場合は削除してください。

- <IMDBDIR>/imdb
- <IMDBENVDIR>/JM0

<IMDBDIR>：削除対象の物理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したセットアップ情報ファイル（`jimdbsetupinfo.conf`）のIMDBDIR パラメーターに指定したパスです。

<IMDBENVDIR>：削除対象の物理ホストの統合監視 DB、IM 構成管理 DB 構築時に指定したセットアップ情報ファイル (jimdbsetupinfo.conf) のIMDBENVDIR パラメーターに指定したパスです。

(5) クラスタシステムで IM データベースを手動アンインストールする場合の手順

1. 実行系ホストにスーパーユーザーでログインします。
2. 実行系ホストにおいて、JP1/IM - Manager が起動している場合は停止します。
3. 実行系ホストにおいて、下記のファイルを削除します。

- /usr/lib/systemd/system/2248-PDxx-start.service
- /usr/lib/systemd/system/2248-PDxx-stop.service
- /usr/lib/systemd/system/2248-PDxx.service
- /usr/lib/systemd/system/2248-pexx.service

ファイル名のxx 部分は 01 からの通番となります。上記ファイルに下記が記載されていることを確認してから削除してください。誤ったファイルを削除すると例えば物理ホストの IM データベースが正常に動作しなくなるなどの影響がありますので、十分ご注意ください。

確認内容

<IMDBENVDIR>/JM<n>

<IMDBENVDIR>：削除対象の論理ホストの統合監視 DB、IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のIMDBENVDIR パラメーターに指定したパスです。

<n>：削除対象の論理ホストの統合監視 DB、IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のLOGICALHOSTNUMBER パラメーターに指定した値です。

4. 実行系ホストにおいて、下記のシンボリックリンクファイルを削除します。

- /etc/systemd/system/multi-user.target.wants/2248-PDxx-start.service
- /etc/systemd/system/multi-user.target.wants/2248-PDxx-stop.service
- /etc/systemd/system/multi-user.target.wants/2248-PDxx.service
- /etc/systemd/system/multi-user.target.wants/2248-pexx.service

ファイル名のxx 部分は 01 からの通番となります。上記ファイルに下記が記載されていることを確認してから削除してください。誤ったファイルを削除すると例えば物理ホストの IM データベースが正常に動作しなくなるなどの影響がありますので、十分ご注意ください。

確認内容

<IMDBENVDIR>/JM<n>

<IMDBENVDIR>：削除対象の物理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したセットアップ情報ファイル (imdbsetupinfo.conf) のIMDBENVDIR パラメーターに指定したパスです。

<n>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のLOGICALHOSTNUMBER パラメーターに指定した値です。

5. 実行系ホストにおいて、以下の手順で IM データベースの設定ファイルを更新してください。

- /etc/opt/jp1imm/conf/imdb/system/dbconf/JM<n>を削除する。
- /etc/opt/jp1imm/conf/imdb/system/dbconf/jimdbsetuplist.conf をテキストエディタで開き、n+1 行目を以下のように編集して論理ホスト名を削除して、上書き保存する。

編集前 jimdbsetuplist.conf n+1行目

_JM<n>=論理ホスト名

編集後 jimdbsetuplist.conf n+1行目

_JM<n>=

<n>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のLOGICALHOSTNUMBER パラメーターに指定した値です。

6. 実行系ホストにおいて、OS を再起動してください。

7. 実行系ホストにおいて、次に示すディレクトリが存在する場合は削除してください。

- <IMDBDIR>/imdb
- <SHAREDDBDIR>/imdb
- <IMDBENVDIR>/JM<n>

<IMDBDIR>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のIMDBDIR パラメーターに指定したパスです。

<SHAREDDBDIR>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のSHAREDDBDIR パラメーターに指定したパスです。

<IMDBENVDIR>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のIMDBENVDIR パラメーターに指定したパスです。

<n>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のLOGICALHOSTNUMBER パラメーターに指定した値です。

8. 待機系ホストにスーパーユーザーでログインします。

9. 待機系ホストにおいて、JP1/IM - Manager が起動している場合は停止します。

10. 待機系ホストにおいて、下記のファイルを削除します。

- /usr/lib/systemd/system/2248-PDxx-start.service
- /usr/lib/systemd/system/2248-PDxx-stop.service

- /usr/lib/systemd/system/2248-PDxx.service
- /usr/lib/systemd/system/2248-pexx.service

ファイル名のxx 部分は 01 からの通番となります。上記ファイルに下記が記載されていることを確認してから削除してください。誤ったファイルを削除すると例えば物理ホストの IM データベースが正常に動作しなくなるなどの影響がありますので、十分にご注意ください。

確認内容

<IMDBENVDIR>/JM<n>

<IMDBENVDIR>：削除対象の論理ホストの統合監視 DB、IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のIMDBENVDIR パラメーターに指定したパスです。

<n>：削除対象の論理ホストの統合監視 DB、IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のLOGICALHOSTNUMBER パラメーターに指定した値です。

11. 待機系ホストにおいて、下記のシンボリックリンクファイルを削除します。

- /etc/systemd/system/multi-user.target.wants/2248-PDxx-start.service
- /etc/systemd/system/multi-user.target.wants/2248-PDxx-stop.service
- /etc/systemd/system/multi-user.target.wants/2248-PDxx.service
- /etc/systemd/system/multi-user.target.wants/2248-pexx.service

ファイル名のxx 部分は 01 からの通番となります。上記ファイルに下記が記載されていることを確認してから削除してください。誤ったファイルを削除すると例えば論理ホストの IM データベースが正常に動作しなくなるなどの影響がありますので、十分にご注意ください。

確認内容

<IMDBENVDIR>/JM<n>

<IMDBENVDIR>：削除対象の物理ホストの統合監視 DB、IM 構成管理 DB 構築時に指定したセットアップ情報ファイル (jimdbsetupinfo.conf) のIMDBENVDIR パラメーターに指定したパスです。

<n>：削除対象の論理ホストの統合監視 DB、IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のLOGICALHOSTNUMBER パラメーターに指定した値です。

12. 待機系ホストにおいて、以下の手順で IM データベースの設定ファイルを更新してください。

- /etc/opt/jp1imm/conf/imdb/system/dbconf/JM<n>を削除する。
- /etc/opt/jp1imm/conf/imdb/system/dbconf/jimdbsetuplist.conf をテキストエディタで開き、n+1 行目を以下のように編集して論理ホスト名を削除して、上書き保存する。

編集前 jimdbsetuplist.conf n+1行目

_JM<n>=論理ホスト名

編集後 `jimdbsetuplist.conf` n+1行目

`_JM<n>=`

<n>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (`jimdbclustersetupinfo.conf`) の `LOGICALHOSTNUMBER` パラメーターに指定した値です。

13. 待機系ホストにおいて，OS を再起動してください。

14. 待機系ホストにおいて，次に示すディレクトリが存在する場合は削除してください。

- `<IMDBDIR>/imdb`
- `<SHAREDDBDIR>/imdb`
- `<IMDBENVDIR>/JM<n>`

<IMDBDIR>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (`jimdbclustersetupinfo.conf`) の `IMDBDIR` パラメーターに指定したパスです。

<SHAREDDBDIR>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (`jimdbclustersetupinfo.conf`) の `SHAREDDBDIR` パラメーターに指定したパスです。

<IMDBENVDIR>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (`jimdbclustersetupinfo.conf`) の `IMDBENVDIR` パラメーターに指定したパスです。

<n>：削除対象の論理ホストの統合監視 DB，IM 構成管理 DB 構築時に指定したクラスタセットアップ情報ファイル (`jimdbclustersetupinfo.conf`) の `LOGICALHOSTNUMBER` パラメーターに指定した値です。

2.24 インストールとセットアップの注意事項（UNIX の場合）

❗ 重要

CentOS 8 以降、Linux 8 以降でコンテナ環境を作成する場合は Docker を Podman に読み替えてください。

- JP1/IM は、ServerConductor/DeploymentManager および JP1/ServerConductor/Deployment Manager のディスク複製インストール、仮想化プラットフォームが提供するイメージファイル化を使用して、統合エージェントホストの複製ができます。次の仮想化プラットフォームに対応しています。

- VMware ESX
- Hyper-V
- SCVMM
- Amazon EC2

上記以外の未対応の仮想プラットフォームでは、複製を実施する前に、JP1/IM をアンインストールし、ディスク複製インストールまたは仮想化プラットフォームによる複製後に、改めて JP1/IM をインストールし直してください。

ディスク複製インストールの操作・運用方法については、ServerConductor/DeploymentManager および JP1/ServerConductor/Deployment Manager のマニュアルを参照してください。仮想化プラットフォームの複製機能については、仮想化ソフトウェアのマニュアルを参照してください。

- Docker 環境上のコンテナをエージェントホストとして監視する場合の注意事項
 - コンテナ上に JP1/Base がインストールされている必要があります。JP1/Base がサポートする Docker 環境については JP1/Base のリリースノートを参照してください。
 - コンテナ上の JP1/Base が使用するポート番号に対して、JP1/IM - Manager ホストから TCP/IP 通信できるようにしてください。
 - コンテナから外部への通信に NAT（ネットワークアドレス変換）が使用されているため、通常と同様に、コンテナ上の JP1/Base から発行されたイベントの「発行元 IP アドレス」には正確な値が表示されません。JP1/IM - Manager の各機能の条件に、「発行元 IP アドレス」に表示される IP アドレスを使用しないでください。

- Docker 環境上のコンテナをリモート監視ホストとして監視する場合の注意事項

コンテナ上に SSH がインストールされている必要があります。

コンテナに対して JP1/IM - Manager ホストから SSH 接続できるようにしてください。

リモート監視機能がサポートしている Docker 環境は次のとおりです。

Docker ホストの OS

リモート監視機能がサポートしている OS のうち、以下の OS をサポートします。

- Red Hat Enterprise Linux Server 7.1 以降
- Cent OS 7.1 以降

Docker バージョン

- Docker ホストの OS がサポートするバージョン

3

IM 構成管理によるシステムの階層構成の設定

この章では、IM 構成管理を使用する場合のシステムの階層構成（IM 構成）の設定について説明します。

3.1 ホストの登録

IM 構成管理にホストを登録するためには、IM 構成管理・ビューアーを操作します。ここでは、ホストを登録したりホスト情報に含まれる属性を変更したりする場合の注意事項を示します。IM 構成管理にホストを登録する手順については、「[3.1.1 ホストを登録する](#)」を参照してください。

- マネージャーによって管理される管理対象ホストのホスト名を指定します。
- ホスト名は、半角英数字および記号 ("-", ".", ".") で指定します。
- リモートの監視対象ホストでは、JP1/IM - Manager にリモートの監視対象ホストでログ監視をするための設定が完了している必要があります。
- ホスト名には、hosts ファイルや DNS に登録してあるホスト名、jp1hosts または jp1hosts2 に定義しているホスト名を指定してください。リモート監視構成では、jp1hosts または jp1hosts2 の設定は参照されません。hosts ファイルや DNS に登録してあるホスト名を指定してください。
- ホスト名は、JP1/IM - Manager のインストールパス長との合計が 235 文字以下となるようにしてください。235 文字を超える場合、その監視対象ホストからプロファイルを収集できません。
- ホストをエイリアス名で定義する場合、同一ホストのエイリアス名を複数設定しないでください。同一ホストであっても、それぞれ別ホストとして扱われます。
- システムの階層構成に登録するホスト名には、IP アドレス、およびエイリアス名を入力しないでください。
- エージェント監視の場合は、IM 構成管理に登録するホスト名と、登録するホストの JP1/Base のイベントサーバ名を同じにする必要があります。同様に、ホスト名の形式（ショートネーム形式、または FQDN 形式）も同じにする必要があります。FQDN 形式のホストを登録する場合については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.3.10 FQDN 形式のホスト名の監視対象ホストを管理する場合のシステム構成」を参照してください。イベントサーバ名の変更手順については、マニュアル「JP1/Base 運用ガイド」の DNS を使ったシステムでのイベントサーバの設定について記述されている個所を参照してください。

3.1.1 ホストを登録する

IM 構成管理 DB に、新しくホストを登録する手順を次に示します。

1. [IM 構成管理] 画面の [ホスト一覧] タブをクリックする。

[ホスト一覧] ページが表示されます。

2. 次に示すどちらかの方法で [ホスト登録] 画面を表示する。

- [ホスト一覧] ページのツリー表示領域の [ホスト一覧] を選択し、メニューバーから [編集] - [ホスト登録] を選択する。
- [ホスト一覧] ページのツリー表示領域の [ホスト一覧] を選択し、右クリックして表示されるポップアップメニューから [ホスト登録] を選択する。

3. [ホスト登録] 画面に表示される項目を指定して、新しいホストを登録する。

[ホスト登録] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.2 [ホスト登録] 画面」を参照してください。

4. [OK] ボタンをクリックする。

3.1.2 リモートの監視対象ホストを登録する

リモートの監視対象ホストを登録する場合、リモート接続用の通信設定をする必要があります。マネージャーホストと監視対象ホストの OS に応じて、必要となる通信設定が異なります。

また、通信設定はシステム共通で設定する方法と、監視対象ホストごとに設定する方法の両方を使用できます。通信設定をシステム共通で設定する場合、システムで共通の設定項目を[システム共通設定]画面で別途設定することで、[リモート監視設定]画面で監視対象ホストごとに設定する項目が削減されます。

1. [IM 構成管理] 画面の [ホスト一覧] タブをクリックする。

[ホスト一覧] ページが表示されます。

2. 次に示すどちらかの方法で [ホスト登録] 画面を表示する。

- [ホスト一覧] ページのツリー表示領域の [ホスト一覧] を選択し、メニューバーから [編集] - [ホスト登録] を選択する。
- [ホスト一覧] ページのツリー表示領域の [ホスト一覧] を選択し、右クリックして表示されるポップアップメニューから [ホスト登録] を選択する。

3. [ホスト登録] 画面に表示される項目を指定して、新しいホストを登録する。

[ホスト登録] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.2 [ホスト登録] 画面」を参照してください。

4. マネージャーホストが Windows の場合、[システム共通設定] 画面の [IM ホストアカウント] ページで IM ホストアカウントを設定する。

[IM 構成管理] 画面のメニューバーから [編集] - [システム共通設定] を選択すると、[システム共通設定] 画面が表示されます。

[システム共通設定] 画面の [IM ホストアカウント] ページで、IM ホストアカウントを設定してください。

[システム共通設定] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.20 [システム共通設定] 画面」を参照してください。

5. 監視対象ホストが Windows の場合、WMI/NetBIOS の設定をする。

通信の設定をシステム共通で設定する場合、次の(a)(b)の両方を、監視対象ホストごとに設定する場合、次の(b)を設定してください。

(a) システムで共通の設定項目

[IM 構成管理] 画面のメニューバーから [編集] - [システム共通設定] を選択すると、[システム共通設定] 画面が表示されます。[システム共通設定] 画面の [WMI/NetBIOS] ページで、WMI/NetBIOS の設定をしてください。

[システム共通設定] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.20 [システム共通設定] 画面」を参照してください。

(b) 監視対象ホストごとの設定項目

[ホスト登録] 画面の [リモート通信設定] の [設定] ボタンをクリックすると、[リモート監視設定] 画面が表示されます。[リモート監視設定] 画面の [リモート通信種別] に WMI/NetBIOS を指定してください。

監視対象ホストごとに通信の設定をする場合、[リモート監視設定] 画面の [設定方法] に個別を指定してください。

システム共通で通信の設定をする場合、[リモート監視設定] 画面の [設定方法] に共通を指定してください。

[リモート監視設定] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.7 [リモート監視設定] 画面」を参照してください。

6. 監視対象ホストが UNIX の場合、SSH の設定をする。

通信の設定をシステム共通で設定する場合、次の(a)(b)の両方を、監視対象ホストごとに設定する場合、次の(b)を設定してください。

(a) システムで共通の設定項目

[IM 構成管理] 画面のメニューバーから [編集] - [システム共通設定] を選択すると、[システム共通設定] 画面が表示されます。[システム共通設定] 画面の [SSH] ページで、SSH の設定をしてください。

[システム共通設定] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.20 [システム共通設定] 画面」を参照してください。

(b) 監視対象ホストごとの設定項目

[リモート通信設定] の [設定] ボタンをクリックすると、[リモート監視設定] 画面が表示されます。[リモート監視設定] 画面の [リモート通信種別] に SSH を指定してください。

監視対象ホストごとに通信の設定をする場合、[リモート監視設定] 画面の [設定方法] に個別を指定してください。

システム共通で通信の設定をする場合、[リモート監視設定] 画面の [設定方法] に共通を指定してください。

[リモート監視設定] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.7 [リモート監視設定] 画面」を参照してください。

7. [OK] ボタンをクリックする。

3.1.3 ホストから情報を収集する

ホスト情報の収集では、指定したホストからホスト情報を収集します。ホストを登録した直後、または次に示すように、ホスト自身の情報やインストールされているソフト情報が更新された場合にだけ実行してください。

- OS の入れ替え
- IP アドレスの変更
- ソフトウェアの入れ替え
 - ソフトウェアのインストールやアンインストール
 - ソフトウェアのバージョンアップ

なお、ホスト情報の収集を実行すると、プロファイルリストはクリアされます。ホスト情報を収集したあとは、[プロファイル表示/編集] 画面を起動した際に、最新のプロファイルリストを取得し直します。そのため、サーバで保存している JP1/Base の未反映のプロファイルはすべて削除されます。

IM 構成管理 DB からホストの情報を収集する手順を次に示します。

1. [IM 構成管理] 画面の [ホスト一覧] タブまたは [IM 構成] タブをクリックする。

[ホスト一覧] ページまたは [IM 構成] ページが表示されます。

2. [ホスト一覧] ページまたは [IM 構成] ページのツリー表示領域からホストを選択する。

選択したホストに下位のホストがある場合、[下位ホスト情報] ボタンをクリックして表示される [下位ホスト情報] のリストからも、ホストを選択できます。この場合は、複数のホストを同時に選択できません。

3. 次に示すどちらかの方法でホストの情報を収集する。

- メニューバーから [操作] - [ホスト情報収集] を選択する。
- 右クリックして表示されるポップアップメニューから [ホスト情報収集] を選択する。

選択したホストの情報を収集するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。選択したホストの情報収集が実行されます。選択したホストでリモート監視ログファイルトラップまたはリモート監視イベントログトラップが稼働している場合にホスト情報を収集すると、確認メッセージの回答に従ってホスト情報を収集します。ホスト情報の収集時に、監視対象ホストから情報を取得できない場合、および前回までに収集されていた OS 名が異なる場合は、リモート監視は停止します。

複数のホストを選択した場合は、実行結果を [実行結果] 画面で確認できます。

なお、VMware ESX および日立サーバ論理分割機構には JP1/Base をインストールできないので、[ホスト情報収集] を実行するとエラーになります。また、ホスト情報にリモート通信種別が設定されているホストでは、システムの階層構成 (IM 構成) にホスト情報が登録されるまで、JP1/Base からのホスト情報の収集とリモートによるホスト情報の収集の両方をします。そのため、システムの階層構成 (IM 構成) に登録されていないホストで、かつ JP1/Base がインストールされていないホストに対して [ホスト情報収集] を実行すると、JP1/Base に接続できないために警告が出力されます。

ホスト情報の収集を実行したあとのホストの状態は、[ホスト一覧] ページで確認できます。収集に失敗した場合、[ホスト一覧] ページではツリー表示領域のホストアイコンがグレー表示されます。詳細は、[ホスト一覧] ページのノード情報表示領域で [基本情報] ボタンをクリックすると参照できます。

3.1.4 ホスト情報を表示する

IM 構成管理 DB に登録したホストの情報を表示する手順を次に示します。基本情報以外のホスト情報を表示する場合は、事前にホスト情報を収集している必要があります。ホスト情報を収集する手順については、[\[3.1.3 ホストから情報を収集する\]](#) を参照してください。

1. [IM 構成管理] 画面の [ホスト一覧] タブをクリックする。

[ホスト一覧] ページが表示されます。

[ホスト一覧] ページについては、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.1.1 [ホスト一覧] ページ」を参照してください。

2. ホスト一覧を選択する。

ツリー表示領域から [ホスト一覧] を選択すると、ノード情報表示領域に下位ホスト情報としてホスト一覧が表示されます。

ホストの情報を参照する場合は、次の操作を行ってください。

基本情報を表示する場合

ツリー表示領域またはノード情報表示領域からホストを選択し、[基本情報] ボタンをクリックすると、ノード情報表示領域に基本情報と詳細情報が表示されます。

製品情報を表示する場合

ツリー表示領域またはノード情報表示領域からホストを選択し、[製品情報] ボタンをクリックすると、ノード情報表示領域に製品情報と詳細情報が表示されます。

サービス情報を表示する場合

ツリー表示領域またはノード情報表示領域からホストを選択し、[サービス情報] ボタンをクリックすると、ノード情報表示領域にサービス情報と詳細情報が表示されます。

3.1.5 ホスト情報の属性を変更する

IM 構成管理 DB に登録されているホスト情報の属性を変更する手順を次に示します。

1. [IM 構成管理] 画面の [ホスト一覧] タブをクリックする。

[ホスト一覧] ページが表示されます。

2. [ホスト一覧] ページのツリー表示領域からホストを選択する。

選択したホストに下位のホストがある場合、[下位ホスト情報] ボタンをクリックして表示される [下位ホスト情報] のリストからも、ホストを選択できます。

3. 次に示すどちらかの方法で [ホスト属性編集] 画面を表示する。

- メニューバーから [編集] - [ホスト属性編集] を選択する。
- 右クリックして表示されるポップアップメニューから [ホスト属性編集] を選択する。

4. [ホスト属性編集] 画面に表示される項目の指定を変更して、ホスト情報を変更する。

[ホスト属性編集] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.4 [ホスト属性編集] 画面」を参照してください。

5. リモートの監視対象ホストのホスト情報の属性を変更する場合、次のどちらかの方法でリモート接続用の通信設定を変更する。

- OS 通信設定の情報を個別に設定する場合
[リモート通信設定] の [設定] ボタンをクリックすると、[リモート監視設定] 画面が表示されます。
[ホスト登録] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.7 [リモート監視設定] 画面」を参照してください。
- OS 通信設定の情報をシステム共通設定として保存・管理する場合
[IM 構成管理] 画面のメニューバーから [編集] - [システム共通設定] を選択すると、[システム共通設定] 画面が表示されます。
[システム共通設定] 画面に表示される項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.20 [システム共通設定] 画面」を参照してください。

なお、リモート接続用の通信には、Windows の場合は WMI/NetBIOS (NetBIOS over TCP/IP) 接続、UNIX の場合は SSH 接続が使用されます。

6. [OK] ボタンをクリックする。

なお、エージェント構成に含まれるホストのホスト名を変更すると、システムの階層構成のホスト名も変更されます。このとき、[IM 構成] ページのツリー表示領域で、システムの階層構成がグレー表示されます。

ホスト名の変更は実ホストでホスト名を変更した場合に実行してください。

ホスト名を変更した場合は、再度ホスト情報の収集を実行してください。ホスト情報を収集する方法については、「[3.1.3 ホストから情報を収集する](#)」を参照してください。

エージェント構成に含まれるホストのホスト名を変更した場合は、エージェント構成を反映してください。反映する方法については、「[3.2.4\(3\) システムの階層構成を IM 構成管理が管理するシステムに反映する](#)」を参照してください。

3.1.6 ホストを削除する

IM 構成管理 DB からホストを削除する手順を次に示します。

1. [IM 構成管理] 画面の [ホスト一覧] タブをクリックする。

[ホスト一覧] ページが表示されます。

2. [ホスト一覧] ページのツリー表示領域からホストを選択する。

選択したホストに下位のホストがある場合, [下位ホスト情報] ボタンをクリックして表示される [下位ホスト情報] のリストからも, ホストを選択できます。この場合は, 複数のホストを同時に選択できます。

3. 次に示すどちらかの方法でホストを削除する。

- メニューバーから [編集] - [ホスト削除] を選択する。
- 右クリックして表示されるポップアップメニューから [ホスト削除] を選択する。

選択したホストを削除するかどうかを確認するメッセージが出力されるので, [はい] ボタンをクリックします。

選択したホストが IM 構成管理 DB から削除されます。削除に失敗した場合は, エラーメッセージが出力されます。

3.2 システムの階層構成の設定

ここでは、JP1/IM のシステム構築時に、IM 構成管理でシステムの階層構成（IM 構成）を設定する手順について説明します。

3.2.1 システムの階層構成を取得する

システムの階層構成（IM 構成）を取得する手順を次に示します。

1. [IM 構成管理] 画面の [ホスト一覧] タブまたは [IM 構成] タブをクリックする。

[ホスト一覧] ページまたは [IM 構成] ページが表示されます。

2. [ホスト一覧] ページまたは [IM 構成] ページのメニューバーから [操作] - [IM 構成取得] を選択する。

構成定義情報を取得するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。取得した構成定義情報が、IM 構成管理が動作するマネージャーに保存されます。

- 取得した構成定義情報に、IM 構成管理に登録されていないホストが含まれている場合は、自動的に IM 構成管理 DB に登録されます。ただし、ホスト情報は取得されません。ホスト情報の取得は、[IM 構成管理] 画面の [ホスト一覧] ページまたは [IM 構成] ページで実行します。
- 取得した構成定義情報に、同一のホスト名が複数存在する場合は、エラーメッセージが表示されて、IM 構成管理 DB が保持する構成定義情報には反映されません。
- 取得した構成定義情報に同一ホスト名が複数存在する場合は、取得した構成定義情報が破棄されて、[IM 構成] ページで、IM 構成ツリーがグレー表示されます。
- 取得した構成定義情報（エージェント構成）が、IM 構成管理 DB が保持する構成定義情報と不一致の場合は、[IM 構成] ページのツリー表示領域で、システムの階層構成がグレー表示されます。
- IM 構成管理が動作するマネージャーの JP1/Base が保持する構成定義情報が削除されていた場合は、メッセージ「KNAN20230-Q」が表示されます。

[はい] ボタンをクリックすると、IM 構成管理 DB が保持する構成定義情報が削除され、エージェント構成が未定義となります。そのため、[IM 構成] ページのツリー表示領域で、システムの階層構成がグレー表示されます。[いいえ] ボタンをクリックすると、IM 構成管理 DB が保持する構成定義情報は削除されないで、[IM 構成] ページのツリー表示領域で、システムの階層構成がグレー表示されます。

- エージェント構成の場合に、[IM 構成] ページのツリー表示領域でシステムの階層構成がグレー表示となったとき、構成定義情報（エージェント構成）を見直してからエージェント構成を反映してください。反映する方法については、[「3.2.4\(3\) システムの階層構成を IM 構成管理が管理するシステムに反映する」](#)を参照してください。

3.2.2 システムの階層構成を表示する

システムの階層構成（IM 構成）は、[IM 構成管理] 画面の [IM 構成] ページで参照します。[IM 構成管理] 画面の [ホスト一覧] ページを表示する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

[IM 構成] ページについては、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.1.2 [IM 構成] ページ」を参照してください。

2. [下位ホスト情報] ボタンを選択する。

ツリー表示領域からホストを選択し、[下位ホスト情報] ボタンをクリックすると、ノード情報表示領域に下位ホスト情報が表示されます。

3.2.3 システムの階層構成を検証する

システムを構成するすべてのホストから取得できる構成定義情報と、IM 構成管理が保持している構成定義情報の内容が一致しているかどうかを検証する手順を次に示します。

1. [IM 構成管理] 画面の [ホスト一覧] タブまたは [IM 構成] タブをクリックする。

[ホスト一覧] ページまたは [IM 構成] ページが表示されます。

2. [ホスト一覧] ページまたは [IM 構成] ページのメニューバーから [操作] - [IM 構成検証] を選択する。

構成定義情報を検証するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。

構成定義情報の検証を実行すると、選択したホストの構成定義情報が取得され、IM 構成管理が保持している構成定義情報と内容が一致しているかどうかの検証が実行されます。

IM 構成管理が動作するマネージャーの JP1/Base が保持する構成定義情報（エージェント構成）と、IM 構成管理 DB が保持する構成定義情報の内容が不一致の場合は、[IM 構成管理] 画面の [IM 構成] ページで、ツリー表示領域のホストアイコンに、エラーの状態を示すアイコンが表示されます。

検証に失敗した場合は、[IM 構成管理] 画面の [IM 構成] ページで、ツリー表示領域のホストアイコンに、エラーの状態を示すアイコンが表示されます。

ホストで動作する JP1/Base のバージョンがバージョン 9 より前の場合は、システムの階層構成（IM 構成）の検証に対応していません。そのため、[IM 構成管理] 画面の [IM 構成] ページで、ツリー表示領域のホストアイコンに、構成状態が不明なことを示すアイコンが表示されます。

なお、マネージャーの構成定義情報が存在しない場合、または構成定義情報が不一致になっている場合には、マネージャーの検証がエラーとなり、処理が中断され [IM 構成] ページのツリー表示領域で、システムの階層構成がグレー表示されます。

3.2.4 システムの階層構成を編集する

システムの階層構成（IM 構成）は、次の手順で設定・変更します。

1. IM 構成管理・ビューアーでエージェント構成およびリモート監視構成を編集する。
2. 更新権を取得する。
3. システムの階層構成を反映する。
4. 更新権を解除する。

それぞれの手順について説明します。

(1) IM 構成管理・ビューアーでエージェント構成およびリモート監視構成を編集する

エージェント構成およびリモート監視構成を編集する手順について説明します。

エージェント構成は、ホストを追加、移動、削除することで構成を変更します。リモート監視構成は、ホストを追加、削除することで構成を変更します。

エージェント構成およびリモート監視構成は、次の画面で編集します。

エージェント構成を編集する場合

[エージェント構成編集] 画面で編集します。[エージェント構成編集] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.6 [エージェント構成編集] 画面」を参照してください。

リモート監視構成を編集する場合

[リモート監視構成編集] 画面で編集します。[リモート監視構成編集] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.8 [リモート監視構成編集] 画面」を参照してください。

(a) ホストを追加する

ホストを追加する手順を次に示します。

1. [IM 構成管理] 画面の [ホスト一覧] タブまたは [IM 構成] タブをクリックする。
[ホスト一覧] ページまたは [IM 構成] ページが表示されます。

2. 編集画面を表示する。

エージェント構成を編集する場合

[IM 構成管理] 画面のメニューバーから [編集] - [エージェント構成編集] を選択して [エージェント構成編集] 画面を表示します。

リモート監視構成を編集する場合

[IM 構成管理] 画面のメニューバーから [編集] - [リモート監視構成編集] を選択して [リモート監視構成編集] 画面を表示します。

3. ツリー表示領域で、追加するホストの上位ホストを選択する。

[下位ホスト情報] には、選択したホストの下位にあるホストの情報が表示されます。[ホスト一覧] には、選択したホストへ追加できるホストの情報が表示されます。

4. 次のどれかの方法でホストを登録する。

- 編集画面の [ホスト一覧] から追加するホストを選択し、ツリー表示領域へドラッグ&ドロップする。
- 編集画面のメニューバーから [編集] - [ホスト追加] を選択する。
[ホスト選択] 画面が表示されます。[選択候補ホスト] に表示されるホスト一覧から追加するホストを選択し、[選択済みホスト] の一覧へ追加してください。選択が終わったら、[OK] ボタンをクリックしてください。
- 編集画面の追加したいホスト (アイコン) 上で右クリックして表示されるポップアップメニューから [ホスト追加] を選択する。
[ホスト選択] 画面が表示されます。[選択候補ホスト] に表示されるホスト一覧から追加するホストを選択し、[選択済みホスト] の一覧へ追加してください。選択が終わったら、[OK] ボタンをクリックしてください。

[ホスト選択] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.5 [ホスト選択] 画面」を参照してください。

(b) ホストを移動する

マネージャーとエージェントの階層構成を設定するために、エージェント構成のホストを移動する手順を次に示します。リモート監視構成の場合、ホストの移動はできません。

1. [IM 構成管理] 画面で [ホスト一覧] タブまたは [IM 構成] タブをクリックする。

[ホスト一覧] ページまたは [IM 構成] ページが表示されます。

2. エージェントのホストを移動する場合は、メニューバーから [編集] - [エージェント構成編集] を選択する。

[エージェント構成編集] 画面が表示されます。

3. [エージェント構成編集] 画面のツリー表示領域で、移動するホストを選択し、次のどれかの方法でホストを移動する。

- ドラッグ&ドロップでツリー表示領域の別な階層に移動する。
- メニューバーから [編集] - [切り取り] を選択したあと、ツリー表示領域で移動先の上位ホストを選択し、[編集] - [貼り付け] を選択する。

- ・ ツリー表示領域で右クリックして表示されるポップアップメニューから「切り取り」を選択したあと、ツリー表示領域で移動先の上位ホストを選択し、右クリックして表示されるポップアップメニューから「貼り付け」を選択する。

上位のホストを移動すると、下位のホストも同時に移動します。

選択したホストの種類によって移動先のホストが限定されます。選択できるホストの範囲については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.2.5 システムの階層構成の編集」を参照してください。

(c) ホストを削除する

ホストを削除する手順を次に示します。

1. [IM 構成管理] 画面で「ホスト一覧」タブまたは「IM 構成」タブをクリックする。

「ホスト一覧」ページまたは「IM 構成」ページが表示されます。

2. 編集画面を表示する。

エージェント構成を編集する場合

メニューバーから「編集」－「エージェント構成編集」を選択して「エージェント構成編集」画面を表示します。

リモート監視構成を編集する場合

メニューバーから「編集」－「リモート監視構成編集」を選択して「リモート監視構成編集」画面を表示します。

3. 編集画面のツリー表示領域で、削除するホストを選択し、次のどれかの方法でホストを削除する。

- ・ ツリー表示領域から削除するホストを選択し、「ホスト一覧」ヘドラッグ&ドロップする。
- ・ メニューバーから「編集」－「ホスト削除」を選択する。
- ・ ツリー表示領域で右クリックして表示されるポップアップメニューから、「ホスト削除」を選択する。

JP1/IM の構成定義情報から選択したホストが削除されます。

上位のホストを削除すると、下位のホストも同時に削除されます。

なお、エージェント構成からホストを削除して反映すると、サーバで保存している JP1/Base のプロファイルリストをクリアし、エージェントで稼働しているプロファイルツリーを再取得します。そのため、サーバで保存している未反映のプロファイルはすべて削除されます。また、リモート監視構成からホストを削除して反映すると、リモート監視のプロファイルはすべて削除されます。

システムの階層構成から対象ホストを削除する場合は、システムの階層構成を反映する前に、プロファイルから対象ホストのイベント転送情報の設定を変更し、JP1 イベントが転送されない設定に変更してください。この設定を変更しないと、システムの階層構成の反映後にもエージェントが保持する構成情報が残っているため、エージェントで発生する JP1 イベントが上位ホストに転送され続けます。

JP1 イベントが転送されない設定に変更する方法を次に示します。

1. システムの階層構成を反映する前に、IM 構成管理のプロファイルからイベント転送情報の設定ファイルについて、JP1 イベントが転送されないようにコメントを挿入する方法で変更する。
2. システムの階層構成を変更する前、または反映したあとにエージェントでjbsrt_del コマンドを実行する。

なお、システムの階層構成の反映方式が一括配布方式（構成削除あり）の場合は、システムの階層構成をいったん削除してから、システムの階層構成を反映します。システムの階層構成の反映方式については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.2.6 システムの階層構成の反映」を参照してください。

(d) ホストを交換する

ホストを交換する手順を次に示します。

1. [IM 構成管理] 画面で [ホスト一覧] タブまたは [IM 構成] タブをクリックする。

[ホスト一覧] ページまたは [IM 構成] ページが表示されます。

2. 編集画面を表示する。

エージェント構成を編集する場合

メニューバーから [編集] - [エージェント構成編集] を選択して [エージェント構成編集] 画面を表示します。

リモート監視構成を編集する場合

メニューバーから [編集] - [リモート監視構成編集] を選択して [リモート監視構成編集] 画面を表示します。

3. 編集画面のツリー表示領域で、交換するホストを選択し、次のどちらかの方法で [ホスト交換] ダイアログを表示する。

- ・ メニューバーから [編集] - [ホスト交換] を選択する。
- ・ ツリー表示領域で右クリックして表示されるポップアップメニューから、[ホスト交換] を選択する。

選択したホストは [ホスト交換] ダイアログに [交換前ホスト] として表示されます。

4. [ホスト交換] ダイアログで、[交換後ホスト] を入力する。

3. で選択した [交換前ホスト] と [交換後ホスト] が交換されます。

(e) 拠点マネージャーを設定する

ホストを拠点マネージャーとして設定する手順を次に示します。

■ 統合マネージャーホストでの設定

1. [IM 構成管理] 画面で [ホスト一覧] タブまたは [IM 構成] タブをクリックする。

[ホスト一覧] ページまたは [IM 構成] ページが表示されます。

2. メニューバーから [編集] - [エージェント構成編集] を選択する。

[エージェント構成編集] 画面が表示されます。

3. ツリー表示領域で、拠点マネージャーとして設定するホストを選択する。

4. 次のどちらかの方法でホストを拠点マネージャーとして設定する。

- 編集画面のメニューバーから [編集] - [拠点マネージャー設定] を選択する。
- 編集画面のツリー表示領域で右クリックして表示されるポップアップメニューから [拠点マネージャー設定] を選択する。

■ 拠点マネージャーホストでの設定

1. [IM 構成管理] 画面で [ホスト一覧] タブまたは [IM 構成] タブをクリックする。

[ホスト一覧] ページまたは [IM 構成] ページが表示されます。

2. メニューバーから [編集] - [エージェント構成編集] を選択する。

[エージェント構成編集] 画面が表示されます。

3. [エージェント構成編集] 画面のツリー表示領域で、接続先ホストを選択する。

4. 次のどちらかの方法でホストを拠点マネージャーとして設定する。

- 編集画面のメニューバーから [編集] - [拠点マネージャー設定] を選択する。
- 編集画面のツリー表示領域で右クリックして表示されるポップアップメニューから [拠点マネージャー設定] を選択する。

(f) 拠点マネージャーを解除する

ホストの拠点マネージャーの設定を解除する手順を次に示します。

■ 統合マネージャーホストでの設定

1. [IM 構成管理] 画面で [ホスト一覧] タブまたは [IM 構成] タブをクリックする。

[ホスト一覧] ページまたは [IM 構成] ページが表示されます。

2. メニューバーから [編集] - [エージェント構成編集] を選択する。

[エージェント構成編集] 画面が表示されます。

3. ツリー表示領域で、拠点マネージャーとして設定するホストを選択する。

4. 次のどちらかの方法でホストの拠点マネージャーの設定を解除する。

- 編集画面のメニューバーから [編集] - [拠点マネージャー解除] を選択する。
- 編集画面のツリー表示領域で右クリックして表示されるポップアップメニューから [拠点マネージャー解除] を選択する。

■ 拠点マネージャーホストでの設定

1. [IM 構成管理] 画面で [ホスト一覧] タブまたは [IM 構成] タブをクリックする。
[ホスト一覧] ページまたは [IM 構成] ページが表示されます。
2. メニューバーから [編集] - [エージェント構成編集] を選択する。
[エージェント構成編集] 画面が表示されます。
3. [エージェント構成編集] 画面のツリー表示領域で、接続先ホストを選択する。
4. 次のどちらかの方法でホストの拠点マネージャーの設定を解除する。
 - 編集画面のメニューバーから [編集] - [拠点マネージャー解除] を選択する。
 - 編集画面のツリー表示領域で右クリックして表示されるポップアップメニューから [拠点マネージャー解除] を選択する。

(2) 更新権を取得する

更新権を取得する手順を次に示します。

エージェント構成を編集した場合

[エージェント構成編集] 画面で [更新権取得] チェックボックスをチェックする。

リモート監視構成を編集した場合

[リモート監視構成編集] 画面で [更新権取得] チェックボックスをチェックする。

システムの階層構成 (IM 構成) を反映できるようになります。なお、更新権を取得して編集している間、ほかのユーザーはシステムの階層構成を反映できません。

(3) システムの階層構成を IM 構成管理が管理するシステムに反映する

システムの階層構成を IM 構成管理が管理するシステムに反映する手順を次に示します。エージェント構成を反映する場合は、反映するエージェントおよび削除するエージェントの JP1/Base がすべて起動している必要があります。

エージェント構成を編集した場合

[エージェント構成編集] 画面のメニューバーから [操作] - [エージェント構成の反映] を選択する。

[エージェント構成編集] 画面で編集した構成定義情報がマネージャーとエージェントに配布されます。

リモート監視構成を編集した場合

[リモート監視構成編集] 画面のメニューバーから [操作] - [リモート監視構成の反映] を選択する。

[リモート監視構成編集] 画面で編集した構成定義情報で構成を更新します。

リモート監視構成は統合マネージャーまたは拠点マネージャーで構成を管理しているため、各ホストにはアクセスしません。

システムの階層構成の反映結果は、ダイアログに表示されます。また、反映を実行したあとのシステムの階層構成は、[IM 構成管理] 画面の [IM 構成] ページで確認できます。反映に失敗した場合は、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「12.5.3(36) IM 構成管理でシステムの階層構成の反映に失敗した場合の対処方法」を参照して再度反映してください。再度反映した結果、反映に失敗した場合、[IM 構成] ページで、ツリー表示領域のホストアイコンに、エラーの状態を示すアイコンが表示されます。詳細は、[IM 構成] ページのノード情報表示領域で [基本情報] ボタンをクリックすると参照できます。

リモート監視構成を反映しても、エージェント構成が反映されていない場合は、[IM 構成] ページのツリー表示領域で、システムの階層構成がグレー表示されます。リモート監視構成を使用する場合は、エージェント構成を反映してください。

なお、拠点マネージャーで拠点ごとに管理する場合は次の手順で設定・変更します。

1. 拠点マネージャーで、[エージェント構成の反映]、[リモート監視構成の反映] を実行する。
2. 統合マネージャーで、[エージェント構成の反映]、[リモート監視構成の反映] を実行する。
3. 統合マネージャーで、[IM 構成の同期] を実行する。
4. 拠点マネージャーで、[IM 構成の取得] を実行する。

また、拠点マネージャー配下のエージェント構成およびリモート監視構成を変更する場合は、次の手順で設定・変更します。

1. 拠点マネージャーで、[エージェント構成の反映]、[リモート監視構成の反映] を実行する。
2. 統合マネージャーで、[IM 構成の同期] を実行する。
3. 拠点マネージャーで、[IM 構成の取得] を実行する。

ただし、手順 1 で [エージェント構成の反映] を実行していない場合は必要ありません。

上記の手順を実行しない場合、拠点マネージャー上のホストで JP1/Base が保持する構成定義情報と不一致になるため、[IM 構成検証] または JP1/IM - Manager のサービス再起動でツリーがグレー表示されます。

また、システムの階層構成の反映方式が一括配布方式（構成削除あり）の場合は、拠点マネージャーで [エージェント構成の反映] を実行すると、拠点マネージャーが保持しているシステムの階層構成を削除してから反映するため、イベント転送されなくなります。

統合マネージャーで IM 構成の反映を実行したあとに、拠点マネージャーで IM 構成の反映を実行する場合、次の手順で実行してください。

1. 統合マネージャーから、IM 構成の同期を実行する。
2. 拠点マネージャーで、jevreload コマンドを実行する。
3. 拠点マネージャーから、IM 構成の収集を実行する。

エージェント構成の反映には、差分配布方式、一括配布方式（構成削除あり）、および一括配布方式（構成削除なし）があります。システムの階層構成の反映方式については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.2.6 システムの階層構成の反映」を参照してください。

(4) 更新権を解除する

更新権を解除する手順を次に示します。

エージェント構成を編集した場合

「エージェント構成編集」画面で「更新権取得」チェックボックスのチェックを外す。

リモート監視構成を編集した場合

「リモート監視構成編集」画面で「更新権取得」チェックボックスのチェックを外す。

ほかのユーザーがシステムの階層構成を反映できるようになります。

3.2.5 システムの階層構成の同期を取る

システムの階層構成（IM 構成）の同期を取る手順を次に示します。

1. 「IM 構成管理」画面の「ホスト一覧」タブまたは「IM 構成」タブをクリックする。

「ホスト一覧」ページまたは「IM 構成」ページが表示されます。

2. メニューバーから「操作」－「IM 構成同期」を選択する。

統合マネージャーと拠点マネージャー間で、構成定義情報の同期が実行されます。

統合マネージャーの下位に拠点マネージャーが定義されていない場合は、システム構成定義情報の同期は実行されません。

3.3 仮想化システム構成の設定

ここでは、JP1/IM のシステム構築時に、IM 構成管理で仮想化システム構成を設定する手順について説明します。

3.3.1 IM 構成管理で仮想化構成を管理する

ここでは、IM 構成管理で仮想化構成を管理するための設定について説明します。

(1) 仮想化構成を管理するための前提条件

仮想化構成を管理するために必要な前提条件を次に示します。

(a) 管理できる仮想化構成の条件

KVM を管理する場合は、仮想化環境管理ソフトウェアがなくても仮想化システム構成を管理できます。KVM 以外の仮想化ソフトウェアを管理する場合は、次に示す仮想化環境管理ソフトウェアのうちのどれかが、仮想化システム管理ホストにインストールされている必要があります。

- vCenter
- JP1/SC/CM
- SCVMM
- HCSM

それぞれの仮想化環境管理ソフトウェアおよび KVM を利用するために必要な条件を次に示します。

表 3-1 仮想化環境管理ソフトウェアに必要な条件

仮想化環境管理ソフトウェア	マネージャー上で必要な条件	仮想化システム管理ホストに必要な条件	ゲスト OS の VMM ホストに必要な条件	ゲスト OS で必要な条件
vCenter	接続先 vCenter のアカウントのユーザー ID とパスワードが IM 構成管理に登録されていること。	vCenter が稼働するホストとマネージャーが通信できる環境になっていること。	VMware ESX がインストールされていること。	VMware ESX で稼働するゲスト OS に VMware Tools がインストールされ、IP アドレスとホスト名が設定されていること。
JP1/SC/CM	なし	JP1/SC/CM が稼働するホストの JP1/Base とマネージャーが通信できる環境になっていること。	日立サーバ論理分割機構がインストールされていること。	日立サーバ論理分割機構で管理するゲスト OS に、IP アドレスとホスト名が設定されていること。
SCVMM	• 接続先 SCVMM のドメイン名、そのドメイ	• SCVMM が稼働するホストの OS が	Hyper-V または vCenter がインス	Hyper-V で稼働するゲスト OS に Hyper-

仮想化環境管理ソフトウェア	マネージャー上で必要な条件	仮想化システム管理ホストに必要な条件	ゲスト OS の VMM ホストに必要な条件	ゲスト OS で必要な条件
	ンで管理者権限を持つユーザー名、およびパスワードが IM 構成管理に登録されていること。 - マネージャーに SCVMM 管理コンソールがインストールされていること※1※2。 - SCVMM 管理コンソールのバージョンが、収集対象となる仮想化システム管理ホストの SCVMM のバージョンと統一されていること。	Windows Server 2012 であること。 - マネージャーにインストールされている SCVMM 管理コンソールが、仮想化システム管理ホストにインストールされている SCVMM と通信できる環境になっていること。 - 同一のマネージャーから収集対象に指定されている仮想化システム管理ホスト同士で、SCVMM のバージョンが統一されていること。	トールされていること。	V Integrated Services がインストールされ、IP アドレスとホスト名が設定されていること。
HCSM	- 接続先 HCSM のユーザー名、パスワード、ポート番号が IM 構成管理に登録されていること。 - 接続先 HCSM がインストールされているホストに上記ユーザー名、パスワード、ポート番号を用いて HTTP 通信ができる環境になっていること。	なし	- 日立サーバ論理分割機構が稼働するシャーシおよびブレードが HCSM によって管理されていること。 - 仮想化システム構成を収集したいホストが HCSM によって管理されていること。	日立サーバ論理分割機構で管理するゲスト OS に、IP アドレスとホスト名が設定されていること。

注※1 異なるバージョンの SCVMM 管理コンソールを、同一のマネージャーにインストールしないでください。

注※2 事前に SCVMM 管理コンソールをインストールするための前提 OS を確認してください。

表 3-2 KVM に必要な条件

マネージャー上で必要な条件	仮想ホストの VMM ホストに必要な条件	ゲスト OS で必要な条件
- KVM がインストールされている接続先ホストの OS ユーザー名、秘密鍵のパス、ポート番号が IM 構成管理に登録されていること。 - IM 構成管理に登録されている情報を基に、KVM がインストールされている接続先ホストと SSH 接続できること。 - IM 構成管理に登録されている OS ユーザーに root 権限があること。	マネージャーと SSH 接続するために必要な公開鍵が配布されていること。	- KVM で管理するゲスト OS に、IP アドレスとホスト名が設定されていること。 - KVM で管理するゲスト OS が、自ホストの IP アドレスとホスト名を名前解決できること。 - KVM で管理するゲスト OS のホスト名が、KVM で定義されたホ

マネージャー上で必要な条件	仮想ホストの VMM ホストで必要な条件	ゲスト OS で必要な条件
		ストの識別名と同一の名前であること。※ • ゲスト OS のホスト名が変更された場合に、KVM で定義されたホストの識別名も同一の名前に再定義されていること。

注※ KVM の仮想化構成情報を収集する場合、仮想ホストのホスト名として、KVM で定義されたホストの識別名（KVM ではドメイン名と呼ばれる、`virsh list` コマンドを実行したとき `Id Name` に表示される名前）を収集します。

詳細は、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.3 仮想化システム構成の管理」を参照してください。

(b) 仮想化構成を管理するための JP1/Base の条件

次に示す JP1/Base の設定が、仮想化構成を管理するために必要な前提条件を満たしているか確認してください。

- JP1 権限レベル

IM 構成管理で仮想化構成を管理するには、次のどちらかの JP1 権限レベルで操作してください。

- JP1_CF_Admin
- JP1_CF_Manager

なお、IM 構成管理・ビューアーから仮想化システム構成をセントラルスコープへ反映する場合、IM 構成管理・ビューアーにログインしている JP1 ユーザーに次の権限が必要です。

- JP1 資源グループ：JP1_Console
- JP1 権限レベル：JP1_Console_Admin

- ホストを登録するときの条件

- 仮想化構成情報で取得したホストをそのまま IM 構成管理に登録する場合は、登録するホストの JP1/Base のイベントサーバ名の設定を次のとおり確認する。
 - ・ショートネーム形式のホスト名を登録するとき、登録するホストの JP1/Base のイベントサーバ名がショートネームかどうか
 - ・FQDN 形式のホスト名を登録するとき、登録するホストの JP1/Base のイベントサーバ名が FQDN 形式かどうか
- 仮想化構成情報で取得したホスト名と IM 構成に登録したいホスト名が異なる場合は、IM 構成に登録したいホスト名のホストをホスト管理に新たに登録する。

(2) 仮想化構成情報を設定する

次のどちらかの方法で、JP1/IM のシステムに追加する仮想ホストに関する情報を設定します。

(a) [ホスト登録] 画面から登録する

[IM 構成管理] 画面から [ホスト登録] 画面を呼び出して、新しい仮想ホストを登録します。

1. [IM 構成管理] 画面の [ホスト一覧] タブをクリックして、[ホスト一覧] ページを表示する。

2. 次のどちらかの方法で [ホスト登録] 画面を表示する。

- ツリー表示領域の [ホスト一覧] を選択し、メニューバーから [編集] - [ホスト登録] を選択する。
- ツリー表示領域内の [ホスト一覧] を右クリックして表示されるポップアップメニューから [ホスト登録] を選択する。

3. [ホスト登録] 画面に表示される項目を指定して、新しいホストを登録する。

[ホスト種別] に「物理ホスト」または「仮想ホスト」を選択する。

[ホスト種別] に「物理ホスト」を選択した場合

[仮想化管理設定] 画面で該当ホストの仮想化管理種別を指定する。

[ホスト種別] に「仮想ホスト」を選択した場合

[VMM ホスト] に仮想マシンモニターが動作しているホストのホスト名を指定する。

[仮想化管理種別] に該当ホストの仮想化管理種別を指定する。

(b) 仮想化システム管理ホストから仮想化構成情報を収集する

仮想化システム管理ホストから仮想化構成情報を収集して、管理下のホストの仮想化構成情報を IM 構成管理に設定します。

仮想化システム管理ホストから仮想化構成情報を収集する方法については、「[3.3.2 仮想化システムの構成情報を収集する](#)」を参照してください。

(3) 仮想ホストをシステムの階層構成に追加する

IM 構成管理・ビューアーを操作して、「[3.3.1\(2\) 仮想化構成情報を設定する](#)」で登録した仮想ホストを、システムの階層構成 (IM 構成) に追加します。JP1/IM のシステム構成にホストを追加する方法については、「[3.2.4 システムの階層構成を編集する](#)」を参照してください。

(4) システムの階層構成をシステムに反映する

IM 構成管理・ビューアーを操作して、「[3.3.1\(3\) 仮想ホストをシステムの階層構成に追加する](#)」で設定したシステムの階層構成 (IM 構成) を、システムに反映します。システムの階層構成をシステムに反映する方法については、「[3.2.4\(3\) システムの階層構成を IM 構成管理が管理するシステムに反映する](#)」を参照してください。

反映後、[IM 構成管理] 画面の [IM 構成] ページで、物理ホストと仮想ホストの階層関係を表示できるようになります。

(5) 証明書を組み込む

vCenter および VMware ESX の仮想化構成情報を取得する場合に使用する通信方法には、SSL を使う方法 (https) と SSL を使わない方法 (http) の 2 種類があります。

❗ 重要

仮想化構成情報を取得する場合の通信種別は vCenter, VMware ESX の仕様によりバージョン 5.5 および 6 では https のみのサポートとなります。

また、他のバージョンにつきましても、vCenter, VMware ESX の仕様により http 接続を利用できない場合があります。http 接続を利用できない場合は、JP1/IM - Manager と vCenter, VMware ESX との接続プロトコルは https をご使用ください。vCenter, VMware ESX の接続プロトコルのサポート状況については、ご購入元にご確認ください。

vCenter または VMware ESX との通信に SSL を使用する場合は、通信先の vCenter ホストまたは VMware ESX ホストの証明書を JP1/IM - Manager が動作するマネージャーに組み込む必要があります。証明書の組み込みは、通信する vCenter または VMware ESX の件数分だけ実施してください。

ここでは、vCenter ホストまたは VMware ESX ホストの証明書を組み込む手順の概要を説明します。詳細については、vCenter または VMware ESX が提供するドキュメントを参照してください。

(a) 証明書を入手する

VMware ESX から SSL 証明書を入手するには、Microsoft Edge を使用する方法と、証明書ファイルを直接入手する方法があります。vCenter から SSL 証明書を入手するには、Microsoft Edge を使用します。それぞれの手順を次に示します。

❗ 重要

入手した証明書ファイルが管理者権限の無い OS ユーザーにアクセスされないよう、適切なアクセス権限を付与してください。

■ Microsoft Edge を使用する場合

Microsoft Edge を使用して VMware ESX または vCenter から SSL 証明書を入手する場合は、Microsoft Edge のヘルプを参照してください。

■ 証明書ファイルを直接入手する場合

VMware ESX 3.5 の場合は、VMware ESX ホストの `/etc/vmware/ssl/rui.crt` に証明書のファイルが格納されています。

(b) 証明書を IM 構成管理に組み込む

入手した証明書を次の手順で、IM 構成管理に組み込みます。

■ Windows の場合

この作業は、Administrators 権限を持つユーザーで実施してください。

1. コマンドプロンプトを開き、Manager パス¥bin¥jdk¥bin に移動する。

2. Keytool コマンドを実行して、証明書を IM 構成管理に組み込む。

```
keytool -import -file 証明書ファイル名 -alias ホスト名 -  
keystore ..¥..¥data¥imcf¥vmware.keystore
```

注：論理ホストに証明書を組み込む場合は、"..¥..¥.."を"共有ディレクトリ¥JP1IMM"に読み替えてください。

証明書ファイル名には、「3.3.1(5)(a) 証明書を入手する」で取得した証明書ファイルをパスを含めて指定します。

ホスト名には、証明書取得先の vCenter または VMware ESX のホスト名を指定します。

3. キーストアのパスワード（ユーザー任意）を入力する。

証明書を複数組み込む場合は、同じパスワードを入力してください。

4. 証明書を信頼するかどうかを確認するメッセージが表示されるので、「yes」を入力する。

証明書が IM 構成管理に組み込まれます。

5. 手順 1 から手順 4 の作業を vCenter または VMware ESX のホストの件数分だけ繰り返す。

■ UNIX の場合

この作業は、スーパーユーザー権限を持つユーザーで実施してください。

1. コンソールまたはターミナルを開き、cd /opt/jp1imm/bin/jdk/bin を実行する。

2. Keytool コマンドを実行して、証明書を IM 構成管理に組み込む。

```
./keytool -import -file 証明書ファイル名 -alias ホスト名 -keystore /var/opt/jp1imm/data/  
imcf/vmware.keystore
```

注：論理ホストに証明書を組み込む場合は、"/var/opt/jp1imm"を"共有ディレクトリ/jp1imm"に読み替えてください。

証明書ファイル名には、「3.3.1(5)(a) 証明書を入手する」で取得した証明書ファイルをパスを含めて指定します。

ホスト名には、証明書取得先の vCenter または VMware ESX のホスト名を指定します。

3. キーストアのパスワード（ユーザー任意）を入力する。

証明書を複数組み込む場合は、同じパスワードを入力してください。

4. 証明書を信頼するかどうかを確認するメッセージが表示されるので、「yes」を入力する。

証明書が IM 構成管理に組み込まれます。

5. 手順 1 から手順 4 の作業を vCenter または VMware ESX のホストの件数分だけ繰り返す。

(c) 証明書を IM 構成管理から削除する

証明書を IM 構成管理から削除する場合の手順を次に示します。

■ Windows の場合

1. コマンドプロンプトを開き、Manager パス¥bin¥jdk¥bin に移動する。

2. Keytool コマンドを実行して、証明書を IM 構成管理から削除する。

```
keytool -delete -alias ホスト名 -keystore ..¥..¥..¥data¥imcf¥vmware.keystore
```

注：論理ホストの証明書を削除する場合は、"..¥..¥.."を"共有ディレクトリ¥JP1IMM"に読み替えてください。

ホスト名には、削除する証明書に該当する vCenter または VMware ESX のホスト名を指定します。

3. [3.3.1(5)(b) 証明書を IM 構成管理に組み込む] で設定したパスワードを入力する。

指定した vCenter または VMware ESX のホストの証明書が IM 構成管理から削除されます。

■ UNIX の場合

1. コンソールまたはターミナルを開き、cd /opt/jp1imm/bin/jdk/bin を実行する。

2. Keytool コマンドを実行して、証明書を IM 構成管理から削除する。

```
./keytool -delete -alias ホスト名 -keystore /var/opt/jp1imm/data/imcf/vmware.keystore
```

注：論理ホストの証明書を削除する場合は、"/var/opt/jp1imm"を"共有ディレクトリ/jp1imm"に読み替えてください。

ホスト名には、削除する証明書に該当する vCenter または VMware ESX のホスト名を指定します。

3. [3.3.1(5)(b) 証明書を IM 構成管理に組み込む] で設定したパスワードを入力する。

指定した vCenter または VMware ESX のホストの証明書が IM 構成管理から削除されます。

(6) VMware ESX の通信種別を変更する

jcfcvmesx コマンドは、VMware Infrastructure SDK のインターフェースを使って VMware ESX と通信し、仮想化構成情報を取得できます。

デフォルトでは、SSL を使う通信 (https) だけを許可する設定になっています。

ここでは、VMware Infrastructure SDK が許可する通信種別を変更する手順の概要を説明します。ただし、VMware ESX のバージョンによっては、次に示す手順と異なる場合があります。詳細については、VMware ESX が提供するドキュメントを参照してください。

1. VMware ESX のサービスコンソールに、スーパーユーザー権限でログインする。

2. /etc/vmware/hostd に移動する。

3. proxy.xml ファイルをテキストエディターで開く。

4. proxy.xml ファイルの<EndpointList>タグにある, VMware Infrastructure SDK の項目を変更して, ファイルを保存する。

次の定義例の太字部分を, 使用する通信種別に合わせて変更します。

```
...
<e id="1">
  <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
  <accessMode>httpsWithRedirect</accessMode>
  <pipeName>/var/run/vmware/proxy-sdk</pipeName>
  <serverNamespace>/sdk</serverNamespace>
</e>
...
```

- SSL を使用する方法 (https) だけを許可する場合は, **httpsWithRedirect** を指定します。
- SSL を使用しない方法 (http) だけを許可する場合は, **httpOnly** を指定します。
- SSL を使用する方法 (https) と SSL を使用しない方法 (http) の両方を許可する場合は, **httpAndHttps** を指定します。

5. 次のコマンドを実行し, vmware-hostd プロセスを再起動する。

```
service mgmt-vmware restart
```

(7) vCenter の通信種別を変更する

jcfcolvmvc コマンド, または IM 構成管理画面上の vCenter ホストに対する仮想化構成収集機能は, VMware Infrastructure SDK のインターフェースを使って vCenter と通信し, 仮想化構成情報を取得できます。

デフォルトでは, SSL を使う通信 (https) だけを許可する設定になっています。

ここでは, VMware Infrastructure SDK が許可する通信種別を変更する手順の概要を説明します。ただし, vCenter のバージョンによっては, 次に示す手順と異なる場合があります。詳細については, vCenter が提供するドキュメントを参照してください。

1. vCenter ホストに, Administrator 権限でログインする。

2. C:¥Documents and Settings¥All Users¥Application Data¥VMware¥VMware VirtualCenterに移動する。

3. proxy.xml ファイルをテキストエディターで開く。

4. proxy.xml ファイルの<EndpointList>タグにある, VMware Infrastructure SDK の項目を変更して, ファイルを保存する。

次の定義例の太字部分を, 使用する通信種別に合わせて変更します。

```
...
<e id="5">
  <_type>vim.ProxyService.LocalServiceSpec</_type>
  <accessMode>httpsWithRedirect</accessMode>
  <port>8085</port>
</e>
```



```
<serverNamespace>/sdk</serverNamespace>
</e>
...
```

- SSL を使用する方法 (https) だけを許可する場合は、httpsWithRedirect を指定します。
- SSL を使用しない方法 (http) だけを許可する場合は、httpOnly を指定します。
- SSL を使用する方法 (https) と SSL を使用しない方法 (http) の両方を許可する場合は、httpAndHttps を指定します。

5. コマンドラインまたは Windows サービス コントロール パネルから vCenter Service を再起動します。

(8) KVM が起動するホストとの SSH 接続を設定する (Windows 環境の場合)

ここでは、JP1/IM - Manager ホストが Windows 環境である場合の、SSH の設定について説明します。
なお、SSH の認証には、公開鍵認証方式を使用します。

SSH で接続するには次の設定が必要となります。

- SSH サーバを設定する
KVM がインストールされているホストで設定します。
- 鍵を作成する
KVM がインストールされているホストで設定します。
- 秘密鍵を JP1/IM - Manager ホストに配置する
KVM がインストールされているホストから JP1/IM - Manager ホストに配置します。
- 公開鍵を監視対象ホストに配置する
KVM がインストールされているホストに配置します。

❗ 重要

対話環境が前提である stty, tty, tset, script コマンドなどは、SSH 接続ユーザーのログインスクリプトに記載しないでください。記載されている場合は、KVM がインストールされているホスト用に SSH 接続ユーザーを新たに作成するか、これらのコマンドを実行しないように SSH 接続ユーザーのログインスクリプトを変更してください。

(a) SSH サーバを設定する

SSH サーバを設定するための手順を次に示します。

1. KVM がインストールされているホストに root 権限のユーザーでログインする。
2. /etc/ssh/sshd_config を開く。

3. PubkeyAuthentication の値を yes に設定する※1。

4. UseDNS を no に設定する※1, ※2。

5. PermitRootLogin を yes に設定する※1。

6. 次のコマンドを実行し、sshd サービスを再起動する。

```
/etc/rc.d/init.d/sshd restart
```

なお、このコマンドは、OS のバージョンによって異なる可能性があります。詳細は、各 OS のマニュアルを参照してください。

注※1

sshd_config の設定項目および設定方法については、使用する SSH サーバのマニュアルを参照してください。

注※2

設定しない場合は、KVM がインストールされているホストで次の名前解決ができるように設定してください。

- マネージャーホストの IP アドレスからマネージャーホスト名を解決できる
- マネージャーホストのホスト名の解決先 IP アドレスが、マネージャーホストの IP アドレスと一致する

名前解決に DNS を使用していて DNS サーバに接続できない場合、KVM からの仮想化構成情報の収集が遅延することがあります。また、遅延によってタイムアウトしてしまい、起動や収集が失敗することがあります。そのため、UseDNS やLookupClientHostnames をno に設定することを推奨します。

(b) 鍵を作成する（初めて鍵を作成する場合）

KVM がインストールされているホストに KVM からの仮想化構成情報の収集で使用するユーザーでログインし、ssh-keygen コマンドを実行して鍵を作成します。なお、この手順は、初めて鍵を作成する場合だけに必要な作業です。

鍵の種類は RSA 暗号と DSA 暗号のどちらかを選択できます。

作業を始める前に、ssh ディレクトリの上位ディレクトリのパーミッションに所有者以外の書き込み権限が設定されていないことを確認してください。所有者以外の書き込み権限が設定されていると SSH の接続に失敗します。

1. KVM がインストールされているホストに KVM からの仮想化構成情報の収集で使用するユーザーでログインする。

2. ssh-keygen コマンドを実行する。

次のように入力してコマンドを実行してください。

- RSA 鍵を作成する場合：ssh-keygen -t rsa
- DSA 鍵を作成する場合：ssh-keygen -t dsa

3. 秘密鍵の出力先と名前を決める。

マルチバイト文字を含まないパスとファイル名を指定してください。デフォルトは「`~/ssh/id_rsa`」が設定されます。

4. リターンキーを 2 回押す。

秘密鍵のパスフレーズの入力を求められるため、何も入力しないでリターンキーを押します。再入力を求められるので、何も入力しないで再度リターンキーを押します。

ssh-keygen -t rsa コマンドの実行例を次に示します。

```
[root@HOST]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ssh-user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ssh-user/.ssh/id_rsa.
Your public key has been saved in /home/ssh-user/.ssh/id_rsa.pub.
The key fingerprint is:
ax:xx:xx:xx:xx:bx:xx:xc:xx:xx:xx:xd:xd:xa:ed:xx root@HOST
```

5. cat コマンドを実行し、公開鍵ファイルの内容を認証鍵ファイルに追加する。

6. chmod コマンドを実行し、認証鍵ファイルの属性を 600 に変更する。

cat コマンドおよびchmod コマンドの実行例を次に示します。

```
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

7. [/etc/ssh/sshd_config] の [AuthorizedKeysFile] を設定する。

デフォルトでは「`~/ssh/authorized_keys`」または「`./ssh/authorized_keys`」が設定されています。手順 6 で作成した認証鍵のパスを変更した場合は、AuthorizedKeysFile の値を見直してください。なお、sshd_config の設定を変更した場合は、スーパーユーザーでsshdサービスを再起動してください。

注意事項

- 秘密鍵の情報は厳重に管理してください。
- 鍵（公開鍵と秘密鍵のペア）の作成は環境やツールには依存しないため、どのような環境やツールでも問題ありません。ただし、鍵の作成後は、秘密鍵と公開鍵を適切に配置する必要があります。

(c) 秘密鍵を JP1/IM - Manager ホストに配置する（初めて鍵を作成する場合）

JP1/IM - Manager ホストが Windows の場合は、「[3.3.1\(8\)\(b\) 鍵を作成する（初めて鍵を作成する場合）](#)」で作成した秘密鍵を Windows の JP1/IM - Manager ホストに配置します。秘密鍵を配置するパスには、マルチバイト文字を含まないようにしてください。配置した秘密鍵ファイルが管理者権限の無い OS

ユーザーにアクセスされないよう、適切なアクセス権限を付与してください。なお、この手順は、初めて鍵を作成する場合だけに必要な作業です。

(d) 公開鍵を KVM がインストールされたホストに配置する（すでに鍵を作成している場合）

「3.3.1(8)(b) 鍵を作成する（初めて鍵を作成する場合）」で作成した公開鍵を KVM がインストールされているホストに配置します。配置する手順を次に示します。なお、この手順は、すでに別のホストで鍵を作成している場合だけに必要な作業です。

作業を始める前に、`.ssh` ディレクトリの上位ディレクトリのパーミッションに所有者以外の書き込み権限が設定されていないことを確認してください。所有者以外の書き込み権限が設定されていると SSH の接続に失敗します。

1. KVM がインストールされているホストに KVM からの仮想化構成情報の収集で使用するユーザーでログインする。

2. `.ssh` ディレクトリに移動する。

KVM からの仮想化構成情報の収集で使用するユーザーのホームディレクトリ配下に `.ssh` ディレクトリがない場合は作成してください。ディレクトリの属性は 700 を設定してください。

3. `scp` コマンドを実行し、公開鍵ファイルを KVM がインストールされているホストにコピーする。

「3.3.1(8)(b) 鍵を作成する（初めて鍵を作成する場合）」で作成済みの公開鍵ファイルを監視対象ホストにコピーします。公開鍵のコピー先は、KVM からの仮想化構成情報の収集で使用するユーザーのホームディレクトリの `.ssh` ディレクトリです。

4. `cat` コマンドを実行し、公開鍵ファイルの内容を認証鍵ファイルに追加する。

5. コピーした公開鍵ファイルを削除する。

6. `chmod` コマンドを実行し、認証鍵ファイルの属性を 600 に変更する。

7. `[/etc/ssh/sshd_config]` の `[AuthorizedKeysFile]` を設定する。

デフォルトでは `[/home/ssh-user/.ssh/authorized_keys]` または `[.ssh/authorized_keys]` が設定されています。手順 6 で作成した認証鍵のパスを変更した場合は、`AuthorizedKeysFile` の値を見直してください。なお、`sshd_config` の設定を変更した場合は、スーパーユーザーで `sshd` サービスを再起動してください。

`scp` コマンド、`cat` コマンド、および `chmod` コマンドの実行例を次に示します。ここでは、「3.3.1(8)(b) 鍵を作成する（初めて鍵を作成する場合）」で鍵を作成したホストのホスト名を `IMHost` としています。

- コマンドの実行例

```
[ClientUser@TargetHost]$ cd .ssh
[ClientUser@TargetHost .ssh]$ scp
root@IMHost:/home/ssh-user/.ssh/id_rsa.pub ./
root@IMHost's password: <パスワードを入力>
```

```
id_rsa 100% 233 0.2KB/s 00:00
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ rm id_rsa.pub
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

(e) 接続を確認する

Windows 環境の JP1/IM - Manager ホストに SSH クライアントソフトがインストールされている場合は、「[3.3.1\(8\)\(c\) 秘密鍵を JP1/IM - Manager ホストに配置する（初めて鍵を作成する場合）](#)」で配置した秘密鍵を用いて、KVM がインストールされているホストに SSH 接続ができることを確認してください。また、SSH 接続するときに、パスワードおよびパスフレーズの入力が必要であることを確認してください。

エラーが発生した場合や、パスワードおよびパスフレーズの入力を要求された場合は、手順どおり正しく設定できているかどうかを見直してください。また、OS の設定を見直し、SSH 接続ができる環境であるか確認してください。

KVM からの仮想化構成情報の収集では、KVM がインストールされているホストで次のコマンドを実行します。KVM からの仮想化構成情報の収集で使用するユーザーで次のコマンドが実行できることを確認してください。実行できない場合は、KVM が正常にインストールされているか、コマンドのパスが設定されているか確認してください。

- `virsh version`
- `virsh list --all`

(9) KVM が起動するホストとの SSH 接続を設定する（UNIX の場合）

ここでは、JP1/IM - Manager ホストが UNIX 環境である場合の、SSH の設定について説明します。なお、SSH の認証には、公開鍵認証方式を使用します。

SSH で接続するには次の設定が必要となります。

- SSH サーバを設定する
KVM がインストールされているホストで設定します。
- 鍵を作成する
UNIX 環境の JP1/IM - Manager ホストで設定します。
- 公開鍵を監視対象ホストに配置する
KVM がインストールされているホストで設定します。

❗ 重要

対話環境が前提である `stty`, `tty`, `tset`, `script` コマンドなどは、SSH 接続ユーザーのログインスクリプトに記載しないでください。記載されている場合は、KVM からの仮想化構成情報

の収集用に SSH 接続ユーザーを新たに作成するか、これらのコマンドを実行しないように SSH 接続ユーザーのログインスクリプトを変更してください。

(a) SSH サーバを設定する

SSH サーバを設定するための手順を次に示します。

1. KVM がインストールされているホストに root 権限のユーザーでログインする。
2. `/etc/ssh/sshd_config` を開く。
3. `PubkeyAuthentication` の値を `yes` に設定する※1。
4. `UseDNS` を `no` に設定する※1, ※2。
5. `PermitRootLogin` を `yes` に設定する※1。
6. 次のコマンドを実行し、`sshd` サービスを再起動する。

```
/etc/rc.d/init.d/sshd restart
```

なお、このコマンドは、OS のバージョンによって異なる可能性があります。詳細は、各 OS のマニュアルを参照してください。

注※1

`sshd_config` の設定項目および設定方法については、使用する SSH サーバのマニュアルを参照してください。

注※2

設定しない場合は、KVM がインストールされているホストで次の名前解決ができるように設定してください。

- マネージャーホストの IP アドレスからマネージャーホスト名を解決できる
 - マネージャーホストのホスト名の解決先 IP アドレスが、マネージャーホストの IP アドレスと一致する
- 名前解決に DNS を使用していて DNS サーバに接続できない場合、KVM からの仮想化構成情報の収集が遅延することがあります。また、遅延によってタイムアウトしてしまい、起動や収集が失敗することがあります。そのため、`UseDNS` や `LookupClientHostnames` を `no` に設定することを推奨します。

(b) 鍵を作成する（初めて鍵を作成する場合）

UNIX 環境の JP1/IM - Manager ホストに root 権限のユーザーでログインし、`ssh-keygen` コマンドを実行して鍵を作成します。なお、この手順は、初めて鍵を作成する場合だけに必要な作業です。

鍵の種類は RSA 暗号と DSA 暗号のどちらかを選択できます。

1. root 権限のユーザーでログインする。
2. `ssh-keygen` コマンドを実行する。

次のように入力してコマンドを実行してください。

- RSA 鍵を作成する場合：ssh-keygen -t rsa
- DSA 鍵を作成する場合：ssh-keygen -t dsa

3. 秘密鍵の出力先と名前を決める。

マルチバイト文字を含まないパスとファイル名を指定してください。デフォルトは「`~/.ssh/id_rsa`」が設定されます。

4. リターンキーを 2 回押す。

秘密鍵のパスフレーズの入力を求められるため、何も入力しないでリターンキーを押します。再入力を求められるので、何も入力しないで再度リターンキーを押します。

ssh-keygen -t rsa コマンドの実行例を次に示します。

```
[root@HOST]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ssh-user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ssh-user/.ssh/id_rsa.
Your public key has been saved in /home/ssh-user/.ssh/id_rsa.pub.
The key fingerprint is:
ax:xx:xx:xx:xx:bx:xx:xc:xx:xx:xx:xd:xd:xa:ed:xx root@HOST
```

注意事項

- 秘密鍵の情報は厳重に管理してください。また、秘密鍵ファイルが管理者権限の無い OS ユーザーにアクセスされないよう、適切なアクセス権限を付与してください。
- 鍵（公開鍵と秘密鍵のペア）の作成は環境やツールには依存しないため、どのような環境やツールでも問題ありません。ただし、鍵の作成後は、秘密鍵と公開鍵を適切に配置する必要があります。

(c) 公開鍵を KVM がインストールされたホストに配置する

「3.3.1(9)(b) 鍵を作成する（初めて鍵を作成する場合）」で作成した公開鍵を KVM がインストールされているホストに配置します。配置する手順を次に示します。

なお、作業を始める前に、ssh ディレクトリの上位ディレクトリのパーミッションに所有者以外の書き込み権限が設定されていないことを確認してください。所有者以外の書き込み権限が設定されていると SSH の接続に失敗します。

1. KVM がインストールされたホストに KVM からの仮想化構成情報の収集で使用するユーザーでログインする。
2. `.ssh` ディレクトリに移動する。

KVM からの仮想化構成情報の収集で使用するユーザーのホームディレクトリ配下に、ssh ディレクトリがない場合は作成してください。ディレクトリの属性は 700 を設定してください。

3. scp コマンドを実行し、公開鍵ファイルを KVM がインストールされたホストにコピーする。

「3.3.1(9)(b) 鍵を作成する (初めて鍵を作成する場合)」で作成済みの公開鍵ファイルを KVM がインストールされたホストにコピーします。公開鍵のコピー先は、KVM からの仮想化構成情報の収集で使用するユーザーのホームディレクトリの .ssh ディレクトリです。

4. cat コマンドを実行し、公開鍵ファイルの内容を認証鍵ファイルに追加する。

5. コピーした公開鍵ファイルを削除する。

6. chmod コマンドを実行し、認証鍵ファイルの属性を 600 に変更する。

7. [/etc/ssh/sshd_config] の [AuthorizedKeysFile] を設定する。

デフォルトでは「~/ .ssh/authorized_keys」または「.ssh/authorized_keys」が設定されています。手順 6 で作成した認証鍵のパスを変更した場合は、AuthorizedKeysFile の値を見直してください。なお、sshd_config の設定を変更した場合は、スーパーユーザーで sshd サービスを再起動してください。

scp コマンド、cat コマンドおよび chmod コマンドの実行例を次に示します。ここでは、「3.3.1(9)(b) 鍵を作成する (初めて鍵を作成する場合)」で鍵を作成した JP1/IM - Manager ホストのホスト名を IMHost としています。

- コマンドの実行例

```
[ClientUser@TargetHost]$ cd .ssh
[ClientUser@TargetHost .ssh]$ scp root@IMHost:/home/ssh-user/.ssh/id_rsa.pub ./
root@IMHost's password: <パスワードを入力>
id_rsa.pub 100% 233 0.2KB/s 00:00
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ rm id_rsa.pub
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

(d) 接続を確認する

JP1/IM - Manager ホストと KVM がインストールされたホストが接続できるかどうかを確認する手順について説明します。

1. JP1/IM - Manager ホストに root 権限のユーザーでログインする。

2. 作成した秘密鍵を利用し、KVM がインストールされたホストに対して ssh コマンドを実行する。

何も入力しないで接続に成功したら、SSH の設定は完了です。

エラーが発生した場合や、パスワードおよびパスフレーズの入力を要求された場合は、手順どおり正しく設定できているかどうかを見直してください。また、OS の設定を見直し、SSH 接続ができる環境であるか確認してください。

接続を確認するときのssh コマンドの実行例を次に示します。

ここでは、JP1/IM - Manager ホストのホスト名を IMHost としています。また、監視対象ホストのホスト名を TargetHost、KVM からの仮想化構成情報の収集で使用するユーザー名を ssh-user としています。

- コマンドの実行例

```
[root@IMHost]$ /usr/bin/ssh -i /home/ssh-user/.ssh/id_rsa -p 22 ssh-user@TargetHost
The authenticity of host 'TargetHost (xxx.xxx.xxx.xxx)' can't be established.
RSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'TargetHost,xxx.xxx.xxx.xxx' (RSA) to the list of known hosts.
Last login: Mon Mar 23 17:17:52 2011 from xxx.xxx.xxx.xxx
[ssh-user@TargetHost ~]$ exit
logout
Connection to TargetHost closed.
[root@IMHost]$
```

KVM からの仮想化構成情報の収集では、KVM がインストールされているホストで次のコマンドを実行します。KVM からの仮想化構成情報の収集で使用するユーザーで次のコマンドが実行できることを確認してください。実行できない場合は、KVM が正常にインストールされているか、コマンドのパスが設定されているか確認してください。

- virsh version
- virsh list --all

3.3.2 仮想化システムの構成情報を収集する

仮想化システムの構成情報を収集する（インポート）手順には、画面を使った方法と、コマンドを使った方法があります。それぞれについて説明します。

(1) 画面を使って仮想化システムの構成情報を収集する

1. [IM 構成管理] 画面から仮想化システム管理ホストが登録されていることを確認する。
仮想化システム管理ホストが登録されていない場合は、登録してください。登録手順は、「[3.3.1\(2\) \(a\) \[ホスト登録\] 画面から登録する](#)」を参照してください。
2. 次のどちらかの方法で仮想化システムの構成情報を収集する。

- 情報を一括収集する場合は、[IM 構成管理] 画面のメニューから「仮想化構成一括収集」を選択する。
- 特定のホストの情報を収集する場合は、[IM 構成管理] 画面で情報を収集するホストを選択して、メニューから「仮想化構成収集」を選択する。

収集が完了すると、[IM 構成管理] 画面のホスト一覧にホスト名が追加されます。

なお、仮想ホストはマネージャーに登録された順番で表示されます。参照したい仮想ホストを探す場合の手順を次に示します。

1. [ホスト一覧] ページを開き、[下位ホスト情報] ボタンをクリックする。
2. 下位ホスト情報の中で参照したいホストを特定できる項目名（ホスト名、IP アドレス、ホスト種別など）をクリックしてソートする。

指定したホストの管理する仮想化構成が変更された場合は、手順 2 を再実施してください。

(2) コマンドを使って仮想化システムの構成情報を収集する（仮想化構成情報をインポートする）

仮想化ソフトウェアおよび仮想化環境管理ソフトウェアから取得した仮想化構成情報を IM 構成管理が動作するマネージャーにインポートして、新しい仮想ホストを登録します。

1. jcsdbexport コマンドを実行して、セントラルスコープの監視ツリー情報をエクスポートする。
エクスポートした情報は、ツリー構成ファイルに出力されます。
2. jcfcolvmesx コマンドを実行して、VMware ESX から仮想化構成情報を取得する。
jcfcolvmesx コマンドには、次のオプションを指定してください。

オプション	指定する値
-m	VMware ESX との通信に SSL を使用する場合は、https を指定してください。 VMware ESX との通信に SSL を使用する場合は、通信先の VMware ESX ホストの証明書入手し、あらかじめ IM 構成管理に組み込んでおく必要があります。 証明書の入手方法および組み込み方法については、 [3.3.1(5) 証明書を組み込む] を参照してください。
-u	VMware ESX のユーザー名を指定してください。
-p	VMware ESX のパスワードを指定してください。
-c	仮想化構成情報取得する VMware ESX を指定してください。
-o	仮想化構成情報を格納する仮想化構成情報ファイルの名称を指定してください。

このコマンドを実行すると、KNAN24030-I、KNAN24031-I のメッセージが表示され、仮想化構成情報が取得されます。

3. jcfexport コマンドを実行して、IM 構成管理の管理情報をエクスポートする。
IM 構成管理が動作するマネージャーで、jcfexport コマンドを実行します。

IM 構成管理 DB に登録された IM 構成管理の管理情報（ホスト入力情報ファイル（host_input_data.csv））をエクスポートします。

エクスポートできる IM 構成管理の管理情報については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.8.1 IM 構成管理でエクスポート・インポートの対象となる情報」を参照してください。

4. IM 構成管理が動作するマネージャーでjcfmkhostsdata コマンドを実行して、仮想化構成情報を反映したホスト入力情報ファイルを作成する。

jcfmkhostsdata コマンドのオプションは、次のとおり指定してください。

オプション	指定する値
-imcf	手順 3 でエクスポートしたホスト入力情報ファイル（host_input_data.csv）の名称を指定してください。
-vm	手順 2 で作成した仮想化構成情報ファイルの名称を指定してください。
-o	仮想化構成情報を反映したホスト入力情報ファイル（host_input_data.csv）の出力先を指定してください。

5. 手順 3 でエクスポートしたホスト入力情報ファイルを手順 4 で作成したホスト入力情報ファイルで上書きする。

6. jcfimport コマンドを実行して、手順 5 で作成したホスト入力情報ファイルを IM 構成管理にインポートする。

jcfimport コマンドを実行すると、IM 構成管理が持つホスト、システムの階層構成（IM 構成）、およびプロファイルの 3 種類の情報は削除されます。プロファイルを管理するには、インポート後にこの 3 種類の情報を収集する必要があります。3 種類の情報を収集する手順を次に示します。

1. [IM 構成管理] 画面の [ホスト一覧] ページを表示する。
 2. ツリー表示領域の [ホスト一覧] を選択し、[下位ホスト情報] に表示されるホストをすべて選択する。
 3. メニューバーから [操作] - [ホスト情報収集] を選択する。
 4. メニューバーから [操作] - [IM 構成取得] を選択する。
 5. メニューバーから [操作] - [プロファイル一括収集] を選択する。
- プロファイルの一括収集が実行されます。

3.3.3 セントラルスコープで仮想化構成を監視するために監視ツリーを設定する

ここでは、セントラルスコープで仮想化構成を監視するために監視ツリーを設定する手順について説明します。

(1) 前提となるセントラルスコープの監視ツリーの条件

仮想化構成を監視する場合、セントラルスコープの監視ツリーに表示されている監視対象のホストのツリー部分を、仮想化構成でグルーピングします。その結果、仮想化構成の監視ツリーが生成されます。そのため、仮想化構成の監視ツリーを生成するためには、生成元のセントラルスコープの監視ツリーは、監視オブジェクトがサーバ単位でグルーピングされているサーバ指向の監視ツリーである必要があります。

サーバ指向ではない監視ツリーを基に仮想化構成の監視ツリーを生成する場合、生成した仮想化構成の監視ツリーを修正する必要があります。

(2) セントラルスコープの監視ツリーに仮想化構成情報を反映する

次のどちらかの方法で、セントラルスコープの監視ツリーに仮想化構成情報を反映します。

(a) [IM 構成管理] 画面から反映する

1. [IM 構成管理] 画面のメニューバーから [操作] - [仮想化構成] - [セントラルスコープ監視ツリー反映] を選択する。

セントラルスコープの監視ツリーに仮想化構成情報が反映されます。

(b) 仮想化構成情報をインポートする

仮想化システムの構成情報を収集したあと、次の手順を実施して仮想化構成情報をインポートしてください。仮想化システムの構成情報を収集する手順については、「[3.3.2 仮想化システムの構成情報を収集する](#)」を参照してください。

ここで説明するコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の次に示す各コマンドを参照してください。

- jcfexport コマンド：「jcfexport」(1. コマンド)
- jcfmkcsdata コマンド：「jcfmkcsdata」(1. コマンド)
- jcsdbimport コマンド：「jcsdbimport」(1. コマンド)
- jcsdbexport コマンド：「jcsdbexport」(1. コマンド)

1. jcfexport コマンドを実行して、IM 構成管理の管理情報をエクスポートする。

エクスポートした情報は、ホスト入力情報ファイル (host_input_data.csv) に出力されます。

エクスポートできる IM 構成管理の管理情報については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「[8.8.1 IM 構成管理でエクスポート・インポートの対象となる情報](#)」を参照してください。

2. jcfmkcsdata コマンドを実行して、IM 構成管理の管理情報を反映したツリー構成ファイルを作成する。

jcfmkcsdata コマンドのオプションは、次のとおりに指定してください。

オプション	指定する値
-f	手順 1 でエクスポートしたホスト入力情報ファイル (host_input_data.csv), および事前に jcsdbexport コマンドで作成したツリー構成ファイルの名称を指定してください。
-o	IM 構成管理の管理情報を反映したツリー構成ファイルの出力先を指定してください。

3. jcsdbimport コマンドを実行して、手順 2 で作成したツリー構成ファイルをセントラルスコープにインポートする。

jcsdbimport コマンドを実行すると、監視ツリーの状態がすべて削除されます。

3.3.4 仮想化構成収集を行う場合の注意事項

- 仮想化構成収集を行う場合は、収集したホストの IP アドレスは設定されません。
- JP1/IM - Manager がサポートしていないバージョンの仮想化環境管理ソフトウェアに対し仮想化構成収集を行う場合、次のメッセージが出力されて収集に失敗することがあります。
KNAN22066-E ホスト(ホスト名)と通信できなかったため、仮想化構成の収集に失敗しました
サポートしている仮想化環境管理ソフトウェアについては、リリースノートを参照してください。
- JP1/SC/CM から仮想化構成を収集する場合、VMM ホスト名には HVM IP アドレスが設定されます。
- SCVMM, vCenter から仮想化構成収集を行う場合、SCVMM の VMM サーバが管理コンソールとの通信に使用するポート、vCenter Server が使用するポートは、デフォルトのポート(SCVMM VMM Server:8100, vCenter Server HTTP:80, vCenter Server HTTPS:443)以外を指定しないでください。
 - SCVMM の場合
デフォルト以外のポートを指定した場合、仮想化構成収集はできません。
 - vCenter の場合
HTTP, HTTPS のいずれかのポートを変更し、他方のポートがデフォルトのままの場合、JP1/IM - Manager からは、デフォルトのままになっているポート(通信種別)を指定して通信を行ってください。両方のポートをデフォルト以外のものに変更した場合、仮想化構成収集はできません。
- 同一ホストに複数の仮想化環境管理ソフトウェア(SCVMM, vCenter, JP1/SC/CM)を稼働させ、JP1/IM - Manager から仮想化構成を収集する場合は、以下の手順に従って設定を行ってください。
 - JP1/IM - Manager が稼働するホストに、複数の仮想化環境管理ソフトウェアが稼働するホストのエイリアスを、仮想化環境管理ソフトウェアの数分設定する。
 - JP1/IM - Manager に(1)で設定したホストのエイリアスをすべて登録し、それぞれのホストに各仮想化環境管理ソフトウェアの情報を設定する。
 仮想化構成収集は通常と同様に、ホストごとの収集、または一括収集を実行してください。
注 IM 構成には(1)で定義したエイリアスを使用しないでください。
- 同一ホストに Hyper-V と仮想化環境管理ソフトウェア(SCVMM, vCenter, JP1/SC/CM のいずれか)を稼働させる構成は、JP1/IM - Manager のサポート対象外です。JP1/IM - Manager から仮想化構成収集を行う場合は、Hyper-V と仮想化環境管理ソフトウェアを別ホストで稼働させてください。

- SCVMM(Hyper-V)と vCenter(VMWare ESX)がサポートしていないゲスト OS を使用した場合、ゲスト OS の情報は JP1/IM - Manager で収集できません。

3.4 業務グループの設定

業務グループを設定するには、次の前提条件を満たす必要があります。

- IM データベース（統合監視 DB および IM 構成管理 DB）が有効である
IM データベースを有効にする方法については、Windows の場合、「[1.4 IM データベースの構築 \(Windows の場合\)](#)」、UNIX の場合、「[2.4 IM データベースの構築 \(UNIX の場合\)](#)」を参照してください。
- 業務グループを管理するための JP1 ユーザーが準備されている
業務グループの JP1 ユーザーについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「[13.5.4 業務グループの検討](#)」を参照してください。

❗ 重要

業務グループを使用する場合はインストール後に次の設定を実施してください。

Windows の場合

- 発生元ホストのマッピングを使用しない場合
コマンドプロンプトから次のコマンドを実行して `jp1cf_treedefaultpolicy_default.csv` を `jp1cf_treedefaultpolicy.csv` に上書きコピーによるファイルの置き換えを実施してください。
`copy Managerパス¥conf¥imcf¥jp1cf_treedefaultpolicy_default.csv Managerパス¥conf¥imcf¥jp1cf_treedefaultpolicy.csv`
- 発生元ホストのマッピングを使用する場合
コマンドプロンプトから次のコマンドを実行して `jp1cf_treedefaultpolicy_hostmapping.csv` を `jp1cf_treedefaultpolicy.csv` に上書きコピーによるファイルの置き換えを実施してください。
`copy Managerパス¥conf¥imcf¥jp1cf_treedefaultpolicy_hostmapping.csv Managerパス¥conf¥imcf¥jp1cf_treedefaultpolicy.csv`

Unix の場合

- 発生元ホストのマッピングを使用しない場合
シェルのプロンプトから次のコマンドを実行して `jp1cf_treedefaultpolicy_default.csv` を `jp1cf_treedefaultpolicy.csv` に上書きコピーによるファイルの置き換えを実施してください。
`# cp /etc/opt/jp1imm/conf/imcf/jp1cf_treedefaultpolicy_default.csv /etc/opt/jp1imm/conf/imcf/jp1cf_treedefaultpolicy.csv`
- 発生元ホストのマッピングを使用する場合
シェルのプロンプトから次のコマンドを実行して `jp1cf_treedefaultpolicy_hostmapping.csv` を `jp1cf_treedefaultpolicy.csv` に上書きコピーによるファイルの置き換えを実施してください。


```
# cp /etc/opt/jp1imm/conf/imcf/jp1cf_treedefaultpolicy_hostmapping.csv  
/etc/opt/jp1imm/conf/imcf/jp1cf_treedefaultpolicy.csv
```

この節では、次の設定について説明します。

- 業務グループを新規に構築する
- 業務グループにホストを追加する
- 業務グループからホストを削除する
- セントラルスコープで業務グループを監視する

3.4.1 業務グループを新規に構築する

業務グループを新規に構築する手順を説明します。

(1) 業務グループを設定する

業務グループを作成し、作成した業務グループにホストを割り当てます。業務グループの設定は、次の作業を組み合わせる実施します。

- 業務グループの作成
- 業務グループのプロパティの編集
- 業務グループの削除
- 業務グループに所属するホストの登録または登録解除
- 業務グループに所属するホストの一覧表示

(a) 業務グループの作成

業務グループを新規に作成する手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページで [更新権取得] チェックボックスをチェックする。
3. [業務グループ] ページのツリー表示領域に表示されているルートノードを選択し、右クリックして表示されるポップアップメニューから [新規作成] を選択する。
[業務グループの新規作成] 画面が表示されます。
4. [業務グループの新規作成] 画面の [業務グループ名], [割り当て JP1 資源グループ名], [コメント] を入力する。

5. [OK] ボタンをクリックする。

業務グループが新規に作成されます。

[業務グループの新規作成] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.14 [業務グループの新規作成] 画面」を参照してください。

(b) 業務グループのプロパティの編集

業務グループのプロパティを編集する手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。

[業務グループ] ページが表示されます。

2. [業務グループ] ページで [更新権取得] チェックボックスをチェックする。

3. [業務グループ] ページのツリー表示領域に表示されているノードを選択し、右クリックして表示されるポップアップメニューから [基本情報編集] を選択する。

[業務グループ基本情報編集] 画面が表示されます。

4. [業務グループ基本情報編集] 画面の [業務グループ名], [割り当て JP1 資源グループ名], [コメント] を編集する。

5. [OK] ボタンをクリックする。

業務グループの編集内容が登録されます。

[業務グループ基本情報編集] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.15 [業務グループ基本情報編集] 画面」を参照してください。

(c) 業務グループの削除

業務グループを削除する手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。

[業務グループ] ページが表示されます。

2. [業務グループ] ページで [更新権取得] チェックボックスをチェックする。

3. [業務グループ] ページのツリー表示領域に表示されているノードを選択し、右クリックして表示されるポップアップメニューから [削除] を選択する。

業務グループとその下の階層の監視グループがすべて削除されます。

[IM 構成管理] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.1 [IM 構成管理] 画面」を参照してください。

(d) 業務グループに所属するホストの登録または登録解除

業務グループに所属するホストを登録または登録解除する手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページで [更新権取得] チェックボックスをチェックする。
3. [業務グループ] ページのツリー表示領域に表示されている、ホストを登録または登録解除したい業務グループのノードを選択し、右クリックして表示されるポップアップメニューから [所属ホストの登録/解除] を選択する。
[所属ホストの登録/登録解除] 画面が表示されます。
4. [所属ホストの登録/登録解除] 画面の [登録候補ホスト] リストから登録したいホストを選択し、[登録] ボタンをクリックする。登録解除したいときは [登録済みホスト] リストから登録解除したいホストを選択し、[解除] ボタンをクリックする。
選択したホストが登録または登録解除されます。

[所属ホストの登録/登録解除] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.18 [所属ホストの登録/登録解除] 画面」を参照してください。

(e) 業務グループに所属するホストの一覧表示

業務グループに所属するホストを一覧表示する手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページのツリー表示領域に表示されているノードの中から所属ホストの一覧を表示したい業務グループのノードを選択する。
3. [業務グループ] ページのノード情報表示領域の [所属ホスト一覧] ボタンをクリックする。
選択した業務グループに所属しているホストの一覧が表示されます。基本情報を表示したいときは [基本情報] ボタンをクリックします。

[IM 構成管理] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.1 [IM 構成管理] 画面」を参照してください。

(2) 監視グループを設定する

システム全体を監視する管理者は、業務システムを監視する管理者にヒアリングして業務グループ内のホストをグルーピングします。グルーピングした内容を監視グループとして登録します。監視グループは、次に示す手順で設定します。

- 監視グループの作成
- 監視グループのプロパティの編集
- 監視グループの削除

- 監視グループのコピー
- 監視グループの切り取り
- 監視グループの貼り付け
- 監視グループに所属するホストの登録または登録解除
- 監視グループに所属するホストの一覧表示

(a) 監視グループの作成

監視グループを新規に作成する手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページで [更新権取得] チェックボックスをチェックする。
3. [業務グループ] ページのツリー表示領域に表示されている業務グループのノードを選択し、右クリックして表示されるポップアップメニューから [新規作成] を選択する。
[監視グループの新規作成] 画面が表示されます。
4. [監視グループの新規作成] 画面の [監視グループ名], [コメント] を入力する。
5. [OK] ボタンをクリックする。
選択した業務グループの下の階層に新規に監視グループが作成されます。監視グループを選択した場合は、選択した監視グループの下の階層に新規に監視グループが作成されます。

[監視グループの新規作成] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.16 [監視グループの新規作成] 画面」を参照してください。

(b) 監視グループのプロパティの編集

監視グループのプロパティを編集する手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページで [更新権取得] チェックボックスをチェックする。
3. [業務グループ] ページのツリー表示領域に表示されているノードを選択し、右クリックして表示されるポップアップメニューから [基本情報編集] を選択する。
[監視グループ基本情報編集] 画面が表示されます。
4. [監視グループ基本情報編集] 画面の [監視グループ名], [コメント] を編集する。
5. [OK] ボタンをクリックする。
監視グループの編集内容が登録されます。

「監視グループ基本情報編集」画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.17 「監視グループ基本情報編集」画面」を参照してください。

(c) 監視グループの削除

監視グループを削除する手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページで [更新権取得] チェックボックスをチェックする。
3. [業務グループ] ページのツリー表示領域に表示されているノードを選択し、右クリックして表示されるポップアップメニューから [削除] を選択する。
監視グループとその下の階層の監視グループがすべて削除されます。

(d) 監視グループのコピー

監視グループをコピーする手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページのツリー表示領域に表示されているノードを選択し、右クリックして表示されるポップアップメニューから [コピー] を選択する。
監視グループとその下の階層の監視グループがすべてコピーされます。

(e) 監視グループの切り取り

監視グループを切り取る手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページのツリー表示領域に表示されているノードを選択し、右クリックして表示されるポップアップメニューから [切り取り] を選択する。
監視グループとその下の階層の監視グループがすべて切り取られます。

(f) 監視グループの貼り付け

「3.4.1(2)(d) 監視グループのコピー」または「3.4.1(2)(e) 監視グループの切り取り」で操作をした内容を貼り付けます。貼り付け先に指定できるのは、同じ業務グループのノードだけです。

監視グループを貼り付ける手順を次に示します。

1. [業務グループ] ページのツリー表示領域に表示されているノードを選択し、右クリックして表示されるポップアップメニューから [貼り付け] を選択する。

右クリックで選択したノードの下にコピーまたは切り取りをした監視グループが貼り付けられます。貼り付け先に同じ名前の監視グループまたはホストが見つかった場合、[監視グループ名の変更] 画面が表示されるので、名称を変更してください。

(g) 監視グループに所属するホストの登録または登録解除

監視グループに所属するホストを登録または登録解除する手順を次に示します。なお、監視グループに所属させるホストは、業務グループにあらかじめ登録しておいてください。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページで [更新権取得] チェックボックスをチェックする。
3. [業務グループ] ページのツリー表示領域に表示されているノードの中からホストを登録または登録解除したい監視グループのノードを選択し、右クリックして表示されるポップアップメニューから [所属ホストの登録/解除] を選択する。
[所属ホストの登録/登録解除] 画面が表示されます。
4. [所属ホストの登録/登録解除] 画面の [登録候補ホスト] リストから登録したいホストを選択し、[登録] ボタンをクリックする。登録解除したいときは [登録済みホスト] リストから登録解除したいホストを選択し、[解除] ボタンをクリックする。
選択したホストが登録または登録解除されます。

[所属ホストの登録/登録解除] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.18 [所属ホストの登録/登録解除] 画面」を参照してください。

(h) 監視グループに所属するホストの一覧表示

監視グループに所属するホストを一覧表示する手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページのツリー表示領域に表示されているノードの中から所属ホストの一覧を表示したい監視グループのノードを選択する。
3. [業務グループ] ページのノード情報表示領域の [所属ホスト一覧] ボタンをクリックする。
選択した監視グループに所属しているホストの一覧が表示されます。基本情報を表示したいときは [基本情報] ボタンをクリックします。

(3) 業務グループを反映する

編集した業務グループと監視グループを、次の手順で IM 構成管理 DB およびセントラルコンソールに反映します。

業務グループや監視グループを反映すると、セントラルコンソールの次の定義に指定された業務グループ・監視グループの名称が最新の名称に変更されます。なお、業務グループや監視グループを削除した場合、セントラルコンソールで指定していた業務グループ・監視グループの名称が"/"となり、無効になります。

- 重要イベント定義
- イベント検索条件
- イベント取得フィルター（拡張モードの共通除外条件）
- ユーザーフィルター
- 表示フィルター
- 関連イベント発行定義
- 自動アクション定義
- アクション結果更新条件
- コマンドボタン定義
- 重大度変更定義
- 表示メッセージ変更定義
- 発生元ホストマッピング定義

反映する手順を次に示します。

1. [IM 構成管理] 画面の [業務グループ] タブをクリックする。
[業務グループ] ページが表示されます。
2. [業務グループ] ページで [更新権取得] チェックボックスをチェックする。
3. メニューバーから [操作] - [業務グループ] - [業務グループ反映] を選択する。
[業務グループ] 画面の表示内容でホスト情報が更新され、構成定義情報が最新の状態になります。
4. [業務グループ] ページで [更新権取得] チェックボックスのチェックを外す。

(4) 業務グループの参照・操作制限を設定する

システム管理者は、業務システムを監視する管理者に業務グループの参照・操作制限を設定できます。参照・操作制限を設定する方法については「[5.19 業務グループの参照・操作制限の設定](#)」を参照してください。

以上の作業で業務システムを監視する管理者は、自分の業務システムについてだけ参照・操作ができるようになります。

3.4.2 業務グループにホストを追加する

業務グループにホストを追加する手順を説明します。

(1) 業務グループに監視対象のホストを追加する

システム全体を監視する管理者は、業務システムを監視する管理者からの依頼に基づき業務グループに監視対象のホストを追加します。業務グループに監視対象のホストを追加する手順については、「[3.4.1\(1\)\(d\) 業務グループに所属するホストの登録または登録解除](#)」を参照してください。

(2) 監視グループに監視対象のホストを追加する

業務システムを監視する管理者からの依頼内容が「監視グループに監視対象のホストを追加する」であった場合、システム全体を監視する管理者は、監視グループに監視対象のホストを追加します。監視グループに監視対象のホストを追加する手順については、「[3.4.1\(2\)\(g\) 監視グループに所属するホストの登録または登録解除](#)」を参照してください。

3.4.3 業務グループからホストを削除する

(1) 業務グループから監視対象のホストの割り当てを登録解除する

システム全体を監視する管理者は、業務システムを監視する管理者から監視対象のホストの割り当てを登録解除する依頼があった場合、業務グループから監視対象のホストの割り当てを登録解除します。業務グループから監視対象のホストの割り当てを登録解除する手順については、「[3.4.1\(1\)\(d\) 業務グループに所属するホストの登録または登録解除](#)」を参照してください。

3.4.4 セントラルスコープで業務グループを監視する

ここでは、セントラルスコープで業務グループを監視するための設定について説明します。業務グループをセントラルスコープに反映する場合は、サーバ指向ツリーにだけ反映できます。

(1) 前提条件

業務グループ情報および監視グループ情報を、セントラルスコープの監視ツリーに反映するための前提条件を次に示します。

- セントラルスコープが有効であり、かつセントラルスコープの監視オブジェクト DB のデータバージョンが 081000 以降であること
- 業務グループが反映済みであること
- IM 構成管理のログインユーザーに、JP1_Console 資源グループの JP1_CF_Admin 権限と JP1_Console_Admin 権限の両方が設定されていること

(2) セントラルスコープの監視ツリーに業務グループ情報および監視グループ情報を反映する

次のどちらかの方法で、セントラルスコープの監視ツリーに業務グループ情報および監視グループ情報を反映します。

なお、業務グループと監視グループの階層構成をセントラルスコープの監視ツリーに反映する場合、ホストの表示順が変更になる場合があります。

❗ 重要

業務グループ定義のセントラルスコープへの反映（View 及び jcfmkcsdata コマンド）で一度反映後に、ホストマッピング機能の有効無効を変更して、デフォルト監視定義を変更して、再度、セントラルスコープに反映する場合、監視定義は最初に反映した際に作成された監視定義が引き継がれます。新しいデフォルト監視定義でご使用になりたい場合は、反映の前にセントラルスコープの業務ツリーを削除してから反映操作を実施してください。

(a) [IM 構成管理] 画面から反映する

1. [IM 構成管理] 画面メニューバーから [操作] - [業務グループ] - [セントラルスコープ監視ツリー反映] を選択する。

業務グループ情報および監視グループ情報がセントラルスコープの監視ツリーに反映されます。

(b) 業務グループ情報および監視グループ情報をインポートする

1. 業務グループ情報および監視グループ情報をエクスポートする。

IM 構成管理が動作するマネージャーで、jcfexport コマンドを実行し、IM 構成管理 DB に登録された業務グループ情報および監視グループ情報をエクスポートします。

- 業務グループ情報および監視グループ情報だけをエクスポートする場合
jcfexport コマンドを -g オプションを指定して実行してください。
- IM 構成管理の管理情報のすべての情報をエクスポートする場合
jcfexport コマンドを -a オプションを指定して実行してください。

エクスポートできる IM 構成管理の管理情報については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.8.1 IM 構成管理でエクスポート・インポートの対象となる情報」を参照してください。

2. セントラルスコープの監視ツリー情報をエクスポートする。

同じマネージャーで、jcsdbexport コマンドを実行して、セントラルスコープの監視ツリー情報をエクスポートします。

3. エクスポートした業務グループ情報および監視グループ情報とセントラルスコープの監視ツリー情報をマージする。

同じマネージャーで、`jcfmkcsdata` コマンドを `-g` オプションを指定して実行して、エクスポートした業務グループ情報および監視グループ情報とセントラルスコープの監視ツリー情報をマージします。

4. 手順 3 でマージした情報をセントラルスコープにインポートする。

同じマネージャーで、`jcsdbimport` コマンドを実行して、エクスポートされた業務グループ情報および監視グループ情報をインポートします。セントラルスコープの監視ツリーに、業務グループおよび監視グループの監視ツリーが追加されます。

3.5 プロファイルの設定

ここでは、JP1/IM のシステム構築時に、監視対象のホストで動作するプロファイルを設定する方法について説明します。新規に監視対象のホストを追加したときにプロファイルを設定して監視できるようにします。

監視対象がエージェント構成のホストか、リモート監視構成のホストかでプロファイルの設定の流れが異なります。構成ごとにプロファイル設定作業を説明します。

3.5.1 エージェント構成のホストにプロファイルを設定する

設定できるプロファイルには、設定ファイルがあります。設定ファイルの内容を次に示します。

- プロファイル（設定ファイル）
エージェントに保存されている設定ファイルです。各サービスは、この設定ファイルに記述されている設定情報を使用していません。定義ファイルの情報を編集したあとにサービスに反映していない場合、有効設定情報と設定ファイルの情報が異なります。

作業ごとに処理できるプロファイル種別と設定ファイルを次に示します。

表 3-3 プロファイル種別と設定ファイル

作業内容	プロファイル種別	設定ファイル
プロファイルの追加，削除	ログファイルトラップ情報	- ログファイルトラップ動作定義ファイル - ログファイルトラップ起動定義ファイル
プロファイルの編集・保存，一括反映，リロードによる反映，再起動による反映	- イベント転送設定情報 - ログファイルトラップ情報 - イベントログトラップ情報 - ローカルアクション情報	- ログファイルトラップ動作定義ファイル - ログファイルトラップ起動定義ファイル

なお，起動・停止できるトラップの種類は，ログファイルトラップだけです。

エージェント構成のホストにプロファイルを設定する場合の前提条件については，「[3.5.1\(8\) エージェントにプロファイルを設定するときの前提条件](#)」を参照してください。

(1) プロファイルリストを収集する

エージェントから IM 構成管理で管理するプロファイルリストを収集します。収集した情報が，[プロファイル表示/編集] 画面のツリー表示領域に表示されます。

次の操作を実行した場合に，プロファイルリストが登録されていない状態になります。

- IM 構成管理の初期起動
- ホスト情報の収集
- システムの階層構成の反映
- jcfimport コマンドの実行

プロファイルリストを収集する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域でプロファイルリストを収集したいエージェントを選択する。

3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。

- メニューバーから [表示] - [プロファイル表示] を選択する。
- 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。

4. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次に示すどちらかの方法で排他編集権を取得する。

- メニューバーから [編集] - [排他編集設定] を選択する。
- 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次に示すどちらかの方法でプロファイルリストを更新する。

- メニューバーから [操作] - [プロファイルツリー再構築] を選択する。
- 右クリックして表示されるポップアップメニューから [プロファイルツリー再構築] を選択する。

プロファイルツリーが再構築され、プロファイルリストが更新されます。エージェントまたはエージェントの JP1/Base を再起動した場合は、プロファイルの編集または反映を行う前に、プロファイルツリーを再構築してください。

注意事項

- プロファイルツリーの再構築に失敗した場合には、エラーメッセージが表示され、再構築を実行する前のプロファイルツリーが表示されます。再構築を実行する前のプロファイル、およびエージェントと情報が同じプロファイルに関しては操作できますが、その後の操作に影響が出るおそれがあります。このため、エラー要因を取り除いたあとに、再度、プロファイルツリーの再構築を実行してください。
- 同一の動作定義ファイルで複数のログファイルトラップを起動している場合、または異なるディレクトリであっても、同じ名称の動作定義ファイルでログファイルトラップを起動している場合は、プロファイルリストの収集に失敗します。なお、JP1/IM - Manager の OS が Windows の場合は、エージェントで使用する設定ファイル名の大文字小文字は区別しません。

- ・ プロファイルツリー再構築を実行すると、マネージャーで保存しているプロファイルをすべて削除し、エージェントのプロファイルリストを再取得します。プロファイルが未反映の場合、プロファイルをエージェントに反映してからプロファイルツリーを再構築してください。

(2) プロファイルを収集する

エージェントから JP1/Base のプロファイルを収集するには、収集対象の範囲の違いによって二つの方法があります。この二つの方法の手順について説明します。

(a) プロファイルを一括で収集する

システムの階層構成（IM 構成）で定義しているすべてのエージェントから、JP1/Base のプロファイルを一括で収集する手順について説明します。

なお、次の場合には、プロファイルを一括収集できません。

- ・ ほかのユーザーが排他編集権を取得している設定ファイルがある場合
- ・ ほかのユーザーがプロファイルの一括収集を行っている場合
- ・ ほかのユーザーが設定ファイルの編集内容の一括反映を行っている場合

プロファイルを一括で収集する手順を次に示します。

1. [IM 構成管理] 画面の [ホスト一覧] タブまたは [IM 構成] タブをクリックする。

[ホスト一覧] ページまたは [IM 構成] ページが表示されます。

2. メニューバーから [操作] - [プロファイル一括収集] を選択する。

プロファイルを一括収集するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。プロファイルの一括収集が実行されて、IM 構成管理が動作するマネージャーに保存されます。実行の結果は、[実行結果] 画面に出力されます。

一括収集を実行したあとのプロファイルの状態は、[プロファイル表示/編集] 画面で確認できます。収集に失敗したプロファイルがある場合、ノード情報表示領域の [設定内容] が非活性表示され、[状態] にプロファイルの状態が表示されます。

プロファイルの一括収集を実行したあとのエージェントの状態は、[IM 構成管理] 画面の [IM 構成] ページで確認できます。収集に失敗したプロファイルがある場合、[IM 構成] ページのツリー表示領域のホストアイコンに、エラーの状態を示すアイコンが表示されます。詳細は、[IM 構成] ページのノード情報表示領域で [基本情報] ボタンをクリックすると参照できます。

(b) エージェントごとにプロファイルを収集する

エージェントごとにプロファイルを収集する手順について説明します。

エージェントごとのプロファイルは、[プロファイル表示/編集] 画面から収集します。

なお、ほかのユーザーが排他編集権を取得している設定ファイルがある場合、エージェントごとのプロフィールは収集できません。

エージェントごとのプロフィールを収集する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域でプロフィールを収集したいエージェントを選択する。

3. 次に示すどちらかの方法で [プロフィール表示/編集] 画面を表示する。

- メニューバーから [表示] - [プロフィール表示] を選択する。
- 右クリックして表示されるポップアップメニューから [プロフィール表示] を選択する。

4. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次に示すどちらかの方法で排他編集権を取得する。

- メニューバーから [編集] - [排他編集設定] を選択する。
- 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. [設定ファイル] ボタンをクリックする。

[設定ファイル] ページが表示されます。

なお、一度も設定ファイルを収集していない場合、[設定ファイル] ボタンをクリックすると、自動的に設定ファイルが収集されます。

6. [設定ファイル] ページのツリー表示領域から収集対象のプロファイルを選択し、次に示すどちらかの方法でプロフィールを収集する。

- メニューバーから [操作] - [プロフィール収集] を選択する。
- 右クリックして表示されるポップアップメニューから [プロフィール収集] を選択する。

エージェントから対象のプロファイルを収集するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。プロフィールが収集されて、IM 構成管理が動作するマネージャーに保存されます。

(3) プロファイルを表示する

IM 構成管理が動作するマネージャーに格納されているプロフィールを表示するには、表示する情報の違いによって二つの方法があります。この二つの方法の手順について説明します。

(a) 有効設定情報を表示する

エージェントごとに有効設定情報を表示する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域で有効設定情報を表示したいエージェントを選択する。
3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。
 - メニューバーから [表示] - [プロファイル表示] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。
4. [プロファイル表示/編集] 画面のツリー表示領域から有効設定情報を表示したい表示項目を選択する。
5. [有効設定情報] ボタンをクリックする。

表示される有効設定情報の内容は、[プロファイル表示/編集] 画面のツリー表示領域で選択した表示項目によって異なります。選択する項目と表示される情報の関係については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.9.1 [有効設定情報] ページ」を参照してください。

(b) 設定ファイルを表示する

エージェントごとに設定ファイルを表示する手順について説明します。エージェントごとの設定ファイルは、[プロファイル表示/編集] 画面に表示されます。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。
[IM 構成] ページが表示されます。
2. [IM 構成] ページのツリー表示領域で設定ファイルを表示したいエージェントを選択する。
3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。
 - メニューバーから [表示] - [プロファイル表示] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。
4. [プロファイル表示/編集] 画面のツリー表示領域から設定ファイルを表示したい表示項目を選択する。
5. [設定ファイル] ボタンをクリックする。

表示される設定ファイルの内容は、[プロファイル表示/編集] 画面のツリー表示領域で選択した表示項目によって異なります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.9.2 [設定ファイル] ページ」を参照してください。

設定ファイルに表示される情報は、項目によって編集できるものと、編集できないものがあります。設定ファイルを編集する方法については、「[3.5.1\(5\) 設定ファイルを編集する](#)」を参照してください。

(4) プロファイルを追加または削除する

IM 構成管理が動作するマネージャーに収集したプロファイルの情報を追加したり、削除したりできます。

(a) プロファイルを追加する

プロファイルを追加する手順について説明します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。
[IM 構成] ページが表示されます。
2. [IM 構成] ページのツリー表示領域でプロファイルを追加したいエージェントを選択する。
3. 次を示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。
 - メニューバーから [表示] - [プロファイル表示] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。
4. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次を示すどちらかの方法で排他編集権を取得する。
 - メニューバーから [編集] - [排他編集設定] を選択する。
 - 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。すでに排他編集権を取得している場合、この操作は不要です。
5. [設定ファイル] ボタンをクリックする。
[設定ファイル] ページが表示されます。
6. [設定ファイル] ページのツリー表示領域からログファイルトラップ情報を選択する。
7. 次を示すどちらかの方法で [プロファイル追加] 画面を表示する。
 - メニューバーから [編集] - [プロファイル追加] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロファイル追加] を選択する。
8. 次を示す項目を設定する。
 - 監視名
すでに指定している監視名やログファイルトラップ動作定義ファイルと同じ名称の監視名は、指定できません。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.10 [プロファイル追加] 画面」を参照してください。
クラスタ用のログファイルトラップを設定する場合、待機系サーバの物理ホストに、実行系サーバの物理ホストで指定した監視名と同じ名称の監視名を指定してください。この項目は必ず指定してください。
 - クラスタ ID
クラスタ用のログファイルトラップを設定する場合、実行系サーバの物理ホストでクラスタ ID を有効に設定し、クラスタ ID を入力してください。
また、待機系サーバの物理ホストに、実行系サーバの物理ホストで指定したクラスタ ID と同じクラスタ ID を入力してください。この項目の指定は省略できます。

9. [OK] ボタンをクリックする。

追加したログファイルトラップの監視名が、ツリー表示領域に表示されます。

ログファイルトラップの設定ファイルを編集する手順については、「[3.5.1\(5\) 設定ファイルを編集する](#)」を参照してください。

ログファイルトラップのプロファイルを新規で追加した場合、ログファイルトラップは起動していません。そのため、ツリー表示領域では、監視名がグレーで表示されます。ログファイルトラップを起動する手順については、「[3.5.1\(7\)\(a\) ログファイルトラップを起動する](#)」を参照してください。

(b) プロファイルを削除する

プロファイルを削除する手順について説明します。

なお、次の場合には、プロファイルが削除できません。

- 選択したプロファイルに対応するログファイルトラップが起動している場合
ログファイルトラップが起動している場合は、ログファイルトラップを停止してください。ログファイルトラップを停止する手順については、「[3.5.1\(7\)\(b\) ログファイルトラップを停止する](#)」を参照してください。

プロファイルを削除する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域でプロファイルを削除したいエージェントを選択する。

3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。

- メニューバーから [表示] - [プロファイル表示] を選択する。
- 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。

4. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次に示すどちらかの方法で排他編集権を取得する。

- メニューバーから [編集] - [排他編集設定] を選択する。
- 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. [設定ファイル] ボタンをクリックする。

[設定ファイル] ページが表示されます。

6. [設定ファイル] ページのツリー表示領域からログファイルトラップの監視名を選択する。

ツリー表示領域のログファイルトラップ情報の下位に、ログファイルトラップの監視名が一覧表示されます。削除したいログファイルトラップの監視名を選択してください。

7. 次に示すどちらかの方法でプロファイルの監視名を削除する。

- ・ メニューバーから [編集] - [プロファイル削除] を選択する。
- ・ 右クリックして表示されるポップアップメニューから [プロファイル削除] を選択する。

削除してよいかを確認するメッセージが表示されるので、[はい] ボタンをクリックします。

ログファイルトラップの監視名が削除されます。

(5) 設定ファイルを編集する

「3.5.1(2) プロファイルを収集する」の操作で収集した設定ファイルを編集して、保存する手順について説明します。設定ファイルは、[プロファイル表示/編集] 画面で編集・保存できます。

設定ファイルを編集・保存する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域で設定ファイルを編集したいエージェントを選択する。

3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。

- ・ メニューバーから [表示] - [プロファイル表示] を選択する。
- ・ 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。

4. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次に示すどちらかの方法で排他編集権を取得する。

設定ファイルの文字列を切り取りまたは貼り付けする場合は、必ず排他編集権を取得してください。

- ・ メニューバーから [編集] - [排他編集設定] を選択する。
- ・ 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、および設定ファイルの文字列をコピーする場合、この操作は不要です。

5. [プロファイル表示/編集] 画面のツリー表示領域で編集したい設定ファイルを選択する。

6. [プロファイル表示/編集] 画面のノード情報表示領域で [設定ファイル] ボタンをクリックする。

IM 構成管理が動作するマネージャーに保存されている編集・保存対象のプロファイルの設定ファイルの内容が表示されます。編集項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.9.2 [設定ファイル] ページ」を参照してください。

7. 編集が終了したら、メニューバーから [操作] - [プロファイル保存/反映] - [サーバに保存] を選択する。

編集した設定ファイルの内容が、IM 構成管理が動作するマネージャーに保存されます。

ただし、IM 構成管理が動作するマネージャーに保存された設定ファイルの内容は、エージェントには転送されません。エージェントへ転送し、反映する方法については、「[3.5.1\(6\) 設定ファイルの編集内容を反映する](#)」を参照してください。

IM 構成管理が動作するマネージャーに設定ファイルの内容を保存したあと、エージェントからプロファイルを集集すると、集集した内容で上書き保存されてしまいます。設定ファイルをエージェントへ反映したい場合は、プロファイルの集集前にエージェントへの反映を済ませてください。

(6) 設定ファイルの編集内容を反映する

設定ファイルの編集内容は、反映対象の範囲の違いによって、一括反映またはエージェントごとに反映できます。

反映を実行したあとの設定ファイルの状態は、[プロファイル表示/編集] 画面の [設定ファイル] ページで確認できます。反映に成功すると「反映済み」、失敗すると「反映失敗」の状態となります。サーバで保存している設定ファイルを使用していない場合、「空白」(未反映) となります。また、サーバに設定ファイルがあり、対象となるホストで使用していない場合、「サーバ保存済み」の状態となります。

設定ファイルの状態が「反映失敗」または「サーバ保存済み」の場合、[設定ファイル] ページのツリー表示領域に、編集中の状態を示すアイコンが表示されます。

なお、JP1/Base がバージョン 9 の場合、設定ファイルの反映に失敗すると、エージェントの設定ファイルは元の設定ファイルにロールバックされます。

反映を実行したあとのホストの状態は、[IM 構成管理] 画面の [IM 構成] ページで確認できます。「反映失敗」や「サーバ保存済み」の設定ファイルがある場合、ツリー表示領域のホストアイコンに、エラーの状態を示すアイコンが表示されます。詳細は、[IM 構成] ページのノード情報表示領域で [基本情報] ボタンをクリックすると参照できます。

(a) 設定ファイルの編集内容を一括で反映する

設定ファイルの編集内容を、システムの階層構成 (IM 構成) に登録されているすべてのエージェントへ一括で反映する手順について説明します。

なお、次の場合には、設定ファイルの編集内容を一括反映できません。

- ほかのユーザーが排他編集権を取得している設定ファイルがある場合
- ほかのユーザーがプロファイルの一括集集を行っている場合
- ほかのユーザーが設定ファイルの編集内容の一括反映を行っている場合

設定ファイルの編集内容を一括で反映する手順を次に示します。

1. [IM 構成管理] 画面の [ホスト一覧] タブまたは [IM 構成] タブをクリックする。
[ホスト一覧] ページまたは [IM 構成] ページが表示されます。
2. メニューバーから [操作] - [プロファイル一括反映] を選択する。

プロファイルの一括反映が実行されます。実行の結果は、[実行結果] 画面に出力されます。

設定ファイルを一括反映するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。IM 構成管理が動作するマネージャーに保存されていた設定ファイルの内容が、すべてのエージェントに反映されます。なお、サーバに設定ファイルが存在しないときは、KNAN22497-I のメッセージが表示されて、反映されません。

(b) エージェントごとに設定ファイルの編集内容を反映する

エージェントごとに設定ファイルの編集内容を反映する手順を 3 種類説明します。

■ リロードして反映する

設定ファイルの編集内容を、リロードして反映する手順について説明します。

なお、次の場合には、リロードして反映できません。

- ログファイルトラップのプロファイルを反映時に、選択したログファイルトラップが停止している場合

設定ファイルの編集内容をリロードして反映する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。
[IM 構成] ページが表示されます。
2. [IM 構成] ページのツリー表示領域で設定ファイルをリロードして反映したいエージェントを選択する。
3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。
 - メニューバーから [表示] - [プロファイル表示] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。
4. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次に示すどちらかの方法で排他編集権を取得する。
 - メニューバーから [編集] - [排他編集設定] を選択する。
 - 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。すでに排他編集権を取得している場合、この操作は不要です。
5. ツリー表示領域から反映するプロファイルを選択し、[設定ファイル] ボタンをクリックする。
[設定ファイル] ページが表示されます。
反映したいプロファイルの設定ファイルに対して編集している場合、この操作は必要ありません。
6. [設定ファイル] ページのノード情報表示領域の [設定内容の保存/反映] で次の二つの項目をチェックし、[実行] ボタンをクリックする。
 - 反映する
 - リロード

プロファイルの反映が実行されます。

設定ファイルの内容を反映するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。

■ 再起動して反映する

設定ファイルの編集内容を、ログファイルトラップを再起動して反映する手順について説明します。

なお、次の場合には、再起動での反映はできません。

- 選択したログファイルトラップが停止している場合
- 選択したログファイルトラップがログファイルトラップ起動定義ファイルに指定されていない場合
- クラスタ ID が指定されている場合

再起動して反映する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域で設定ファイルを再起動して反映したいエージェントを選択する。

3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。

- メニューバーから [表示] - [プロファイル表示] を選択する。
- 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。

4. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次に示すどちらかの方法で排他編集権を取得する。

- メニューバーから [編集] - [排他編集設定] を選択する。
- 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. ツリー表示領域で反映するログファイルトラップの監視名を選択し、[設定ファイル] ボタンをクリックする。

[設定ファイル] ページが表示されます。

反映したいプロファイルの設定ファイルに対して編集している場合、この操作は必要ありません。

6. [設定ファイル] ページのノード情報表示領域の [設定内容の保存/反映] で次の二つの項目をチェックする。

- 反映する
- 再起動

設定ファイルの内容を反映するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。プロファイルの反映が実行されます。

■ ファイルを送付して反映する

設定ファイルを送付して反映する手順について説明します。

ファイルの送付による反映先は、次のパターンがあります。

- エージェントから収集した設定ファイルをファイルの送付で反映する。
- IM 構成管理から追加した設定ファイルをファイルの送付で反映する。

IM 構成管理は次に示すエージェントのフォルダから設定ファイルを収集できます。収集した設定ファイルを対象にファイルの送付を実行すると、収集時と同じフォルダに設定ファイルが反映されます。

表 3-4 設定ファイルの送付先（エージェントから収集した設定ファイルをファイルの送付で反映する場合）

設定ファイル	エージェントの OS 種別	反映先
ログファイルトラップ 動作定義ファイル	Windows	Base パス¥conf
		Base パス¥conf¥任意のフォルダ
		Base パス¥conf¥cf_log_file_trap
	UNIX	/etc/opt/jp1base/conf
		/etc/opt/jp1base/conf/任意のディレクトリ
		/etc/opt/jp1base/conf/cf_log_file_trap
ログファイルトラップ 起動定義ファイル	Windows	Base パス¥conf¥event¥
	UNIX	/etc/opt/jp1base/conf/event/

IM 構成管理から追加した設定ファイルをファイルの送付で反映する場合、設定ファイルは次に示すフォルダに送付されます。

表 3-5 設定ファイルの送付先（IM 構成管理から追加した設定ファイルをファイルの送付で反映する場合）

設定ファイル	エージェントの OS 種別	反映先
ログファイルトラップ 動作定義ファイル	Windows	Base パス¥conf¥cf_log_file_trap¥
	UNIX	/etc/opt/jp1base/conf/cf_log_file_trap/
ログファイルトラップ 起動定義ファイル	Windows	Base パス¥conf¥event¥
	UNIX	/etc/opt/jp1base/conf/event/

次の場合には、設定ファイルを送付して反映できません。

- エージェントの JP1/Base のバージョンが 09-10 より前の場合
- 選択したログファイルトラップがエージェントで起動している場合

• エージェントの JP1/Base のバージョンが 11-10 より前で、クラスタ ID が指定されていない場合
設定ファイルを送付して反映する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域で設定ファイルを反映したいエージェントを選択する。

3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。

- メニューバーから [表示] - [プロファイル表示] を選択する。
- 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。

4. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次に示すどちらかの方法で排他編集権を取得する。

- メニューバーから [編集] - [排他編集設定] を選択する。
- 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. ツリー表示領域でログファイルトラップの監視名を選択し、[設定ファイル] ボタンをクリックする。

[設定ファイル] ページが表示されます。

反映したいプロファイルの設定ファイルに対して編集している場合、この操作は必要ありません。

6. [設定ファイル] ページのノード情報表示領域の [設定内容の保存/反映] で次の二つの項目をチェックし、[実行] ボタンをクリックする。

- 反映する
- ファイルの送付

プロファイルの反映が実行されます。

設定ファイルの内容を反映するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。フォルダにファイルが送付されます。

(7) ログファイルトラップを起動または停止する

エージェントのログファイルトラップを起動したり停止したりできます。

(a) ログファイルトラップを起動する

ログファイルトラップを起動する手順について説明します。

なお、次の場合には、ログファイルトラップを起動できません。

- 選択したログファイルトラップが起動している場合
- JP1/Base のバージョンが 09-10 より前のとき

- クラスタ ID が指定されているとき

ログファイルトラップを起動する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域でログファイルトラップを起動したいエージェントを選択する。

3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。

- メニューバーから [表示] - [プロファイル表示] を選択する。
- 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。

4. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次に示すどちらかの方法で排他編集権を取得する。

- メニューバーから [編集] - [排他編集設定] を選択する。
- 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. ツリー表示領域でログファイルトラップの監視名を選択する。

6. 次に示すどちらかの方法でログファイルトラップを起動する。

- メニューバーから [操作] - [プロセス起動] を選択する。
- 右クリックして表示されるポップアップメニューから [プロセス起動] を選択する。

ログファイルトラップを起動するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。ログファイルトラップが起動します。

(b) ログファイルトラップを停止する

ログファイルトラップを停止する手順について説明します。

なお、次の場合には、ログファイルトラップを停止できません。

- エージェントの JP1/Base のバージョンが 09-10 より前のとき
- 選択したログファイルトラップが停止している場合
- クラスタ ID が指定されているとき

ログファイルトラップを停止する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域でログファイルトラップを停止したいエージェントを選択する。

3. 次に示すどちらかの方法で「プロファイル表示/編集」画面を表示する。

- メニューバーから「表示」－「プロファイル表示」を選択する。
- 右クリックして表示されるポップアップメニューから「プロファイル表示」を選択する。

4. ツリー表示領域から JP1 製品名 (JP1/Base) を選択し、次に示すどちらかの方法で排他編集権を取得する。

- メニューバーから「編集」－「排他編集設定」を選択する。
- 右クリックして表示されるポップアップメニューから「排他編集設定」を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. ツリー表示領域でログファイルトラップの監視名を選択する。

6. 次に示すどちらかの方法でプロセスを停止する。

- メニューバーから「操作」－「プロセス停止」を選択する。
- 右クリックして表示されるポップアップメニューから「プロセス停止」を選択する。

ログファイルトラップを停止するかどうかを確認するメッセージが出力されるので、「はい」ボタンをクリックします。ログファイルトラップが停止します。

(c) クラスタ用のログファイルトラップの設定

クラスタ用のログファイルトラップを起動したり停止したりするときに、クラスタソフトに次のコマンドを登録してください。

- jevlogstart (クラスタ運用限定) コマンド
- jevlogstop (クラスタ運用限定) コマンド

各コマンドの詳細については、マニュアル「JP1/Base 運用ガイド」のコマンドを説明している章を参照してください。

(8) エージェントにプロファイルを設定するときの前提条件

- IM 構成管理のプロファイル管理と JP1/Base のプロファイル管理を併用する場合
エージェントの JP1/Base のバージョンが 11-10 以降である必要があります。

- ログファイルトラップの操作をする場合

次の操作をする場合、エージェントの JP1/Base のバージョンが 09-10 以降である必要があります。

- 3.5.1(4) プロファイルを追加または削除する
- 3.5.1(6)(b) エージェントごとに設定ファイルの編集内容を反映する
 - 再起動して反映する
 - ファイルを送付して反映する
- 3.5.1(7) ログファイルトラップを起動または停止する

エージェントの JP1/Base のバージョンが 09-10 より前の場合は、09-10 以降に上書きインストールしてください。上書きインストールの詳細については、マニュアル「JP1/Base 運用ガイド」のインストールとセットアップの章の説明を参照してください。また、JP1/Base のバージョンを 09-10 より前のバージョンから 09-10 以降に上書きインストールした場合、次の操作を実行してください。

- 起動順序定義ファイルまたは `jbs_start` コマンドでログファイルトラップを起動するように定義しているときは、ログファイルトラップの定義をログファイルトラップ起動定義ファイルに移行する。

参照先：マニュアル「JP1/Base 運用ガイド」のインストール・アンインストール時の注意事項

- IM 構成管理でエージェントから情報を収集する。

参照先：「[3.1.3 ホストから情報を収集する](#)」

- プロファイルリストおよびプロファイルの操作をする場合

次の操作をする場合、エージェントの JP1/Base のバージョンがバージョン 9 以降である必要があります。

- プロファイルリストを収集する
- プロファイルを収集する
- プロファイルを表示する

また、JP1/Base のバージョンがバージョン 9 の場合、設定ファイルの反映に失敗すると、エージェントの設定ファイルは元の設定ファイルにロールバックされます。

- ログファイルトラップの定義をしている場合

エージェントの JP1/Base のバージョンを 09-10 より前のバージョンから 09-10 以降にした場合、起動順序定義ファイルまたは `jbs_start` コマンドでログファイルトラップを起動するように定義しているときは、ログファイルトラップの定義をログファイルトラップ起動定義ファイルに移行する必要があります。移行する方法については、マニュアル「JP1/Base 運用ガイド」のインストール・アンインストール時の注意事項の説明を参照してください。

- クラスタ用のログファイルトラップを設定する場合

- 待機系サーバの設定ファイルを実行系サーバと同じ内容に編集してください。
- 実行系サーバおよび待機系サーバの設定ファイルをエージェントの JP1/Base に送付して反映する必要があります。設定ファイルを送付して反映する方法については、「[3.5.1\(6\)\(b\) エージェントごとに設定ファイルの編集内容を反映する](#)」の「ファイルを送付して反映する」を参照してください。
- クラスタソフトでコマンドを実行してログファイルトラップを起動したり停止したりします。詳細については、「[3.5.1\(7\)\(c\) クラスタ用のログファイルトラップの設定](#)」を参照してください。

3.5.2 リモート監視構成のホストにプロファイルを設定する

プロファイルには、有効設定情報と設定ファイルの二つがあります。それぞれの内容を次に示します。

- プロファイル（有効設定情報）

リモート監視の各サービスで、現在使用されている設定情報です。各サービスが正常に起動した際に、リモート監視構成のホスト（リモートの監視対象ホスト）から収集されます。収集した情報を有効設定情報として表示できます。

- プロファイル（設定ファイル）

IM 構成管理が動作するマネージャーに保存されている設定ファイルです。IM 構成管理がリモートの監視対象ホストに対して収集するための設定情報は、この設定ファイルに記述されている設定情報を必ずしも使用して稼働しているわけではありません。定義ファイルの情報を編集した際に、IM 構成管理へのリロードや再起動による反映が行われていない場合、有効設定情報と設定ファイルの情報が異なります。

作業ごとに処理できるプロファイル種別と設定ファイルを次に示します。

表 3-6 プロファイル種別と設定ファイル

作業内容	プロファイル種別	設定ファイル
プロファイルの追加・削除	リモート監視ログファイルトラップ情報	リモート監視ログファイルトラップ動作定義ファイル
• プロファイルの編集・保存 • 一括反映 • リロードによる反映 • 再起動による反映	• リモート監視ログファイルトラップ情報 • リモート監視イベントログトラップ情報	• リモート監視ログファイルトラップ動作定義ファイル • リモート監視イベントログトラップ動作定義ファイル

リモートの監視対象ホストで起動・停止できるトラップの種類は、リモート監視ログファイルトラップとリモート監視イベントログトラップです。

「リロードによる反映」は、リモート監視が監視対象ホストに接続してログを収集している場合、即時に適用されません。次の収集時に適用されます。ログを収集している間は、「リロードによる反映」をしないで待機するため、ログの収集に時間が掛かる場合、「リロードによる反映」に時間が掛かることがあります。プロファイルを早急に反映したい場合は、「再起動」で反映してください。リモートの監視対象ホストにプロファイルを設定する場合の前提条件については、「[3.5.2\(6\) リモートの監視対象ホストにプロファイルを設定する場合の前提条件](#)」を参照してください。

(1) プロファイルを追加または削除する

IM 構成管理が動作するマネージャーに収集したプロファイルの情報を追加したり削除したりできます。

(a) プロファイルを追加する

プロファイルを追加する手順について説明します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。
[IM 構成] ページが表示されます。
2. [IM 構成] ページのツリー表示領域でプロファイルを追加したいリモートの監視対象ホストを選択する。

3. 次に示すどちらかの方法で「プロファイル表示/編集」画面を表示する。

- メニューバーから「表示」－「プロファイル表示」を選択する。
- 右クリックして表示されるポップアップメニューから「プロファイル表示」を選択する。

4. ツリー表示領域からリモート監視のプロファイル（リモート監視）を選択し、次に示すどちらかの方法で排他編集権を取得する。

- メニューバーから「編集」－「排他編集設定」を選択する。
- 右クリックして表示されるポップアップメニューから「排他編集設定」を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. ツリー表示領域からログファイルトラップ情報を選択する。

6. 次に示すどちらかの方法で「プロファイル追加」画面を表示する。

- メニューバーから「編集」－「プロファイル追加」を選択する。
- 右クリックして表示されるポップアップメニューから「プロファイル追加」を選択する。

7. 次に示す項目を設定する。

- 監視名

すでに指定している監視名やリモート監視ログファイルトラップ動作定義ファイルと同じ名称の監視名は、指定できません。この項目は必ず指定してください。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.10 「プロファイル追加」画面」を参照してください。

8. [OK] ボタンをクリックする。

追加したリモート監視ログファイルトラップのプロファイルの監視名が、ツリー表示領域に表示されません。

リモート監視ログファイルトラップの設定ファイルを編集する手順については、「[3.5.1\(5\) 設定ファイルを編集する](#)」を参照してください。

リモート監視ログファイルトラップのプロファイルを新規で追加した場合、リモート監視ログファイルトラップは起動していません。そのため、ツリー表示領域では、監視名がグレーで表示されます。リモート監視ログファイルトラップを起動する手順については、「[3.5.2\(3\) 設定ファイルを編集する](#)」を参照してください。

(b) プロファイルを削除する

プロファイルを削除する手順について説明します。

なお、次の場合には、プロファイルが削除できません。

- 選択したプロファイルに対応するリモート監視ログファイルトラップが起動している場合

リモート監視ログファイルトラップが起動している場合は、リモート監視ログファイルトラップを停止してください。リモート監視ログファイルトラップを停止する手順については、「[3.5.2\(5\)\(b\) リモート監視ログファイルトラップを停止する](#)」を参照してください。

プロファイルを削除する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域でプロファイルを削除したいリモートの監視対象ホストを選択する。

3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。

- ・ メニューバーから [表示] - [プロファイル表示] を選択する。
- ・ 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。

4. ツリー表示領域からリモート監視のプロファイル（リモート監視）を選択し、次に示すどちらかの方法で排他編集権を取得する。

- ・ メニューバーから [編集] - [排他編集設定] を選択する。
- ・ 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. ツリー表示領域からログファイルトラップの監視名を選択する。

ツリー表示領域のログファイルトラップ情報の下位に、リモート監視ログファイルトラップの監視名が一覧表示されます。削除したいリモート監視ログファイルトラップの監視名を選択してください。

6. 次に示すどちらかの方法でプロファイルの監視名を削除する。

- ・ メニューバーから [編集] - [プロファイル削除] を選択する。
- ・ 右クリックして表示されるポップアップメニューから [プロファイル削除] を選択する。

削除してよいかを確認するメッセージが表示されるので、[はい] ボタンをクリックします。

リモート監視ログファイルトラップのプロファイルの監視名が削除されます。

(2) プロファイルを表示する

IM 構成管理が動作するマネージャーに格納されているプロファイルを表示するには、表示する情報の種類によって表示方法が異なります。これらの手順について説明します。

(a) 有効設定情報を表示する

リモートの監視対象ホストごとに有効設定情報を表示する手順について説明します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域で有効設定情報を表示したいリモートの監視対象ホストを選択する。
3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。
 - メニューバーから [表示] – [プロファイル表示] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。
4. [プロファイル表示/編集] 画面のツリー表示領域から有効設定情報に表示したい表示項目を選択する。
5. [有効設定情報] ボタンをクリックする。

表示される有効設定情報の内容は、[プロファイル表示/編集] 画面のツリー表示領域で選択した表示項目によって異なります。選択する項目と表示される情報の関係については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.9.1 [有効設定情報] ページ」を参照してください。

(b) 設定ファイルを表示する

リモートの監視対象ホストごとに設定ファイルを表示する手順について説明します。リモートの監視対象ホストごとの設定ファイルは、[プロファイル表示/編集] 画面に表示されます。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。
[IM 構成] ページが表示されます。
2. [IM 構成] ページのツリー表示領域で設定ファイルを表示したいリモートの監視対象ホストを選択する。
3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。
 - メニューバーから [表示] – [プロファイル表示] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。
4. [プロファイル表示/編集] 画面のツリー表示領域から設定ファイルに表示したい表示項目を選択する。
5. [設定ファイル] ボタンをクリックする。

表示される設定ファイルの内容は、[プロファイル表示/編集] 画面のツリー表示領域で選択した表示項目によって異なります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.9.2 [設定ファイル] ページ」を参照してください。

設定ファイルに表示される情報は、項目によって編集できるものと、編集できないものがあります。

(3) 設定ファイルを編集する

IM 構成管理が動作しているマネージャーが収集した設定ファイルを編集して、保存する手順について説明します。設定ファイルは、[プロファイル表示/編集] 画面で編集・保存できます。

設定ファイルを編集・保存する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域で設定ファイルを編集したいリモートの監視対象ホストを選択する。

3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。

- メニューバーから [表示] - [プロファイル表示] を選択する。
- 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。

4. ツリー表示領域からリモート監視のプロファイル (リモート監視) を選択し、次に示すどちらかの方法で排他編集権を取得する。

設定ファイルの文字列を切り取るまたは貼り付ける場合は、必ず排他編集権を取得してください。

- メニューバーから [編集] - [排他編集設定] を選択する。
- 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、および設定ファイルの文字列をコピーする場合、この操作は不要です。

5. [プロファイル表示/編集] 画面のツリー表示領域で編集したい設定ファイルを選択する。

6. [プロファイル表示/編集] 画面のノード情報表示領域で [設定ファイル] ボタンをクリックする。

IM 構成管理が動作するマネージャーに保存されている編集・保存対象のプロファイルの設定ファイルの内容が表示されます。編集項目の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.9.2 [設定ファイル] ページ」、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「リモート監視ログファイルトラップ動作定義ファイル」(2. 定義ファイル)、および「リモート監視イベントログトラップ動作定義ファイル」(2. 定義ファイル) を参照してください。

7. 編集が終了したら、メニューバーから [操作] - [プロファイル保存/反映] - [サーバに保存] を選択する。

編集した設定ファイルの内容が、IM 構成管理が動作するマネージャーに保存されます。

(4) 設定ファイルの編集内容を反映する

設定ファイルの編集内容は、反映対象の範囲の違いによって二つの方法で反映できます。

反映を実行したあとの設定ファイルの状態は、[プロファイル表示/編集] 画面の [設定ファイル] ページで確認できます。反映に成功すると「反映済み」、失敗すると「反映失敗」の状態となります。サーバで保存している設定ファイルを使用していない場合、「空白」(未反映) となります。また、サーバに設定ファイルがあり、対象となるホストで使用していない場合、「サーバ保存済み」の状態となります。

設定ファイルの状態が「反映失敗」または「サーバ保存済み」の場合、[設定ファイル] ページのツリー表示領域に、編集中の状態を示すアイコンが表示されます。

反映を実行したあとのリモートの監視対象ホストの状態は、[IM 構成管理] 画面の [IM 構成] ページで確認できます。「反映失敗」や「サーバ保存済み」の設定ファイルがある場合、ツリー表示領域のホストアイコンに、エラーの状態を示すアイコンが表示されます。詳細は、[IM 構成] ページのノード情報表示領域で [基本情報] ボタンをクリックすると参照できます。

(a) 設定ファイルの編集内容を一括で反映する

設定ファイルの編集内容を、システムの階層構成に登録されているすべてのリモートの監視対象ホストへ一括で反映する手順について説明します。

なお、次の場合には、設定ファイルの編集内容を一括反映できません。

- ほかのユーザーが排他編集権を取得している設定ファイルがある場合
- ほかのユーザーがプロファイルの一括収集を行っている場合
- ほかのユーザーが設定ファイルの編集内容の一括反映を行っている場合
- JP1/IM - Manager が起動していない場合
- リモート監視構成下に監視対象のホストが存在しない場合
- リモートの監視対象ホストのホスト情報が収集済みでない場合
- JP1/IM - Manager とリモートの監視対象ホストの OS がともに Windows であり、WMI でイベントログを監視している場合、DCOM の設定がされていないとき
- イベントログトラップが起動していない場合

設定ファイルの編集内容を一括で反映する手順を次に示します。

■ リモート監視ログファイルトラップの設定ファイル

1. jcfallogdef コマンドを実行して複数の稼働中のリモート監視ログファイルトラップの設定ファイルを上書きする。
稼働中のリモート監視ログファイルトラップの設定ファイルが上書きされます。
2. jcfallogreload コマンドを実行して複数の設定ファイルを一括でリロードする。
複数のリモート監視ログファイルトラップの設定ファイルが一括でリロードされます。

■ リモート監視イベントログトラップの設定ファイル

1. jcfaleltdef コマンドを実行して複数の稼働中のリモート監視イベントログトラップの設定ファイルを上書きする。
このコマンドは JP1/IM - Manager の OS が Windows の場合に実行できます。
稼働中のリモート監視イベントログトラップの設定ファイルが上書きされます。
2. jcfaleltreload コマンドを実行して複数の設定ファイルを一括でリロードする。
このコマンドは JP1/IM - Manager の OS が Windows の場合に実行できます。
複数のリモート監視イベントログトラップの設定ファイルが一括でリロードされます。

(b) リモートの監視対象ホストごとに設定ファイルの編集内容を反映する

リモートの監視対象ホストごとに設定ファイルの編集内容を反映する手順を2種類説明します。

■ リロードして反映する

設定ファイルの編集内容を、リロードして反映する手順について説明します。

なお、次の場合には、リロードして反映できません。

- ・ リモート監視ログファイルトラップのプロファイル反映時に、選択したリモート監視ログファイルトラップが停止している場合

設定ファイルの編集内容をリロードして反映する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域で設定ファイルをリロードして反映したいリモートの監視対象ホストを選択する。

3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。

- ・ メニューバーから [表示] - [プロファイル表示] を選択する。
- ・ 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。

4. ツリー表示領域からリモート監視のプロファイル（リモート監視）を選択し、次に示すどちらかの方法で排他編集権を取得する。

- ・ メニューバーから [編集] - [排他編集設定] を選択する。
- ・ 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. ツリー表示領域から反映するプロファイルを選択し、[設定ファイル] ボタンをクリックする。

[設定ファイル] ページが表示されます。

反映したいプロファイルの設定ファイルに対して編集している場合、この操作は必要ありません。

6. [設定ファイル] ページのノード情報表示領域の [設定内容の保存/反映] で次の二つの項目をチェックし、[実行] ボタンをクリックする。

- ・ 反映する
- ・ リロード

設定ファイルの内容を反映するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。プロファイルの反映が実行されます。

■ 再起動して反映する

設定ファイルの編集内容を、リモート監視ログファイルトラップを再起動して反映する手順について説明します。

なお、次の場合には、再起動での反映はできません。

- 選択したリモート監視ログファイルトラップが停止している場合
- 選択したリモート監視ログファイルトラップがリモート監視ログファイルトラップ起動定義ファイルに指定されていない場合

設定ファイルの編集内容を再起動して反映する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。

[IM 構成] ページが表示されます。

2. [IM 構成] ページのツリー表示領域で設定ファイルを再起動して反映したいリモートの監視対象ホストを選択する。

3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。

- メニューバーから [表示] - [プロファイル表示] を選択する。
- 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。

4. ツリー表示領域からリモート監視のプロファイル（リモート監視）を選択し、次に示すどちらかの方法で排他編集権を取得する。

- メニューバーから [編集] - [排他編集設定] を選択する。
- 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。

すでに排他編集権を取得している場合、この操作は不要です。

5. ツリー表示領域で反映するリモート監視ログファイルトラップの監視名を選択し、[設定ファイル] ボタンをクリックする。

[設定ファイル] ページが表示されます。

反映したいプロファイルの設定ファイルに対して編集している場合、この操作は必要ありません。

6. [設定ファイル] ページのノード情報表示領域の [設定内容の保存/反映] で次の二つの項目をチェックし、[実行] ボタンをクリックする。

- 反映する
- 再起動

設定ファイルの内容を反映するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。プロファイルの反映が実行されます。

(5) リモート監視ログファイルトラップを起動または停止する

リモートの監視対象ホストのリモート監視ログファイルトラップを起動したり停止したりできます。

(a) リモート監視ログファイルトラップを起動する

リモート監視ログファイルトラップを起動する手順について説明します。

なお、ログファイルトラップ起動定義ファイルは初期設定では提供されません。また、単独で作成・配布できません。次の場合に、ほかの設定ファイルと同時に作成・更新されます。

- 設定ファイルの編集内容を、ログファイルトラップを再起動して反映した場合
- 設定ファイルを送付して反映した場合
- ログファイルトラップを起動した場合
- ログファイルトラップを停止した場合

なお、次の場合には、リモート監視ログファイルトラップを起動できません。

- 選択したリモート監視ログファイルトラップが起動している場合

リモート監視ログファイルトラップを起動する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。
[IM 構成] ページが表示されます。
2. [IM 構成] ページのツリー表示領域でリモート監視ログファイルトラップを起動したいリモートの監視対象ホストを選択する。
3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。
 - メニューバーから [表示] - [プロファイル表示] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。
4. ツリー表示領域からリモート監視のプロファイル（リモート監視）を選択し、次に示すどちらかの方法で排他編集権を取得する。
 - メニューバーから [編集] - [排他編集設定] を選択する。
 - 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。すでに排他編集権を取得している場合、この操作は不要です。
5. ツリー表示領域でリモート監視ログファイルトラップの監視名を選択する。
6. 次に示すどちらかの方法でリモート監視ログファイルトラップを起動する。
 - メニューバーから [操作] - [プロセス起動] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロセス起動] を選択する。

リモート監視ログファイルトラップを起動するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。リモート監視ログファイルトラップが起動します。

(b) リモート監視ログファイルトラップを停止する

リモート監視ログファイルトラップを停止する手順について説明します。

なお、次の場合には、リモート監視ログファイルトラップを停止できません。

- 選択したリモート監視ログファイルトラップが停止している場合

リモート監視ログファイルトラップを停止する手順を次に示します。

1. [IM 構成管理] 画面の [IM 構成] タブをクリックする。
[IM 構成] ページが表示されます。
2. [IM 構成] ページのツリー表示領域でリモート監視ログファイルトラップを停止したいリモートの監視対象ホストを選択する。
3. 次に示すどちらかの方法で [プロファイル表示/編集] 画面を表示する。
 - メニューバーから [表示] - [プロファイル表示] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロファイル表示] を選択する。
4. ツリー表示領域からリモート監視のプロファイル（リモート監視）を選択し、次に示すどちらかの方法で排他編集権を取得する。
 - メニューバーから [編集] - [排他編集設定] を選択する。
 - 右クリックして表示されるポップアップメニューから [排他編集設定] を選択する。すでに排他編集権を取得している場合、この操作は不要です。
5. ツリー表示領域でリモート監視ログファイルトラップの監視名を選択する。
6. 次に示すどちらかの方法でプロセスを停止する。
 - メニューバーから [操作] - [プロセス停止] を選択する。
 - 右クリックして表示されるポップアップメニューから [プロセス停止] を選択する。リモート監視ログファイルトラップを停止するかどうかを確認するメッセージが出力されるので、[はい] ボタンをクリックします。リモート監視ログファイルトラップが停止します。

(6) リモートの監視対象ホストにプロファイルを設定する場合の前提条件

リモートの監視対象ホストのプロファイルを設定する場合は、IM 構成管理が動作するマネージャーの JP1/Base のバージョンが 09-50 以降である必要があります。

3.6 IM 構成管理の管理情報のインポート・エクスポート

ここでは、JP1/IM のシステム構築時に、IM 構成管理の管理情報をエクスポート・インポートして、システムの階層構成（IM 構成）を設定する手順について説明します。

インポートを実行すると IM 構成管理が保持するデータが変更されるため、インポート前にバックアップすることをお勧めします。インポート時にエラーが発生した場合は、インポート前のデータにロールバックされます。

1. IM 構成管理の管理情報をエクスポートする。

移行元の IM 構成管理が動作するマネージャーで、`jcfexport` コマンドを実行し、IM 構成管理 DB に登録された IM 構成管理の管理情報をエクスポートします。

エクスポート機能の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.8 IM 構成管理の管理情報のエクスポート・インポート」を参照してください。

エクスポート手順の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「9.7.1 IM 構成管理の管理情報をエクスポートする」を参照してください。

2. エクスポートした IM 構成管理の管理情報を編集する。

ホスト名を変更したい場合は、エクスポートした IM 構成管理の管理情報を編集して変更できます。

3. エクスポートした IM 構成管理の管理情報をインポートする。

エクスポートされた IM 構成管理の管理情報を、移行先の IM 構成管理が動作するマネージャーで、`jcfimport` コマンドを実行してインポートします。

インポート機能の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.8 IM 構成管理の管理情報のエクスポート・インポート」を参照してください。

インポート手順の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「9.7.2 IM 構成管理の管理情報をインポートする」を参照してください。

4. システムの階層構成を JP1/IM が運用管理するシステムに反映する。

インポートされたシステムの階層構成を、IM 構成管理・ビューアーを操作して、JP1/IM が運用管理するシステムに反映します。システムの階層構成を反映する方法については、[「3.2.4\(3\) システムの階層構成を IM 構成管理が管理するシステムに反映する」](#)を参照してください。

4

インテリジェント統合管理基盤の設定

この章では、インテリジェント統合管理基盤の構成と環境構築について説明します。

4.1 インテリジェント統合管理基盤の環境設定の概要

インテリジェント統合管理基盤の環境設定は、連携する製品から取得したシステム構成情報を一元監視するための管理グループの定義やホストの定義を作成する作業です。

なお、この章での説明は、インテリジェント統合管理基盤がセットアップ済みで動作していることを前提にしています。

インテリジェント統合管理基盤のセットアップについて

参照先：「[1.19.2 インテリジェント統合管理基盤の機能を使用するための設定（Windows の場合）](#)」
または「[2.18.4 インテリジェント統合管理基盤の機能を使用するための設定（UNIX の場合）](#)」

4.1.1 インテリジェント統合管理基盤の環境設定を始める前に

インテリジェント統合管理基盤の環境設定を始める前に、次の準備をしてください。

JP1/IM 全般とインテリジェント統合管理基盤について知っておく

- インテリジェント統合管理基盤の使い方の概要
参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「1. JP1/Integrated Management の概要」
参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2. 機能の概要」
- インテリジェント統合管理基盤の機能について
参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3. インテリジェント統合管理基盤による IT 運用の最適化」

JP1/IM の動作環境を構築する

参照先：「[1. インストールとセットアップ（Windows の場合）](#)」
参照先：「[2. インストールとセットアップ（UNIX の場合）](#)」

監視対象製品をセットアップする

インテリジェント統合管理基盤と連携する監視対象製品を事前にセットアップします。セットアップ手順については、各製品のマニュアルを参照してください。

4.2 システム構成情報を設定する

連携製品のシステム構成情報を取得し、インテリジェント統合管理基盤に設定する流れを、次の図に示します。

図 4-1 システム構成情報取得の流れ



注※ 詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・APIリファレンス」を参照してください。

(凡例)  : 必須
 : 任意

図中の番号に従って説明します。

1. システムノード定義ファイル (imdd_systemnode.conf) で、システムの階層構造を定義する。(任意)
システムノード定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「システムノード定義ファイル (imdd_systemnode.conf)」(2. 定義ファイル) を参照してください。

2. IM 管理ノードカテゴリ名称定義ファイル (`imdd_category_name.conf`) で、収集したデータをサンバーストまたはツリー形式で表示する際の、管理グループの IM 管理ノード名を定義する。(任意)
IM 管理ノードカテゴリ名称定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「IM 管理ノードカテゴリ名称定義ファイル (`imdd_category_name.conf`)」(2. 定義ファイル) を参照してください。
3. ホスト名定義ファイル (`imdd_host_name.conf`) で、エイリアス名と実ホスト名のマッピングを定義する。(任意)
ホスト名にエイリアス名を付けることができる製品を IM 管理ノードの構成に加える場合に必要な定義です。
ホスト名定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ホスト名定義ファイル (`imdd_host_name.conf`)」(2. 定義ファイル) を参照してください。
4. JP1/IM - Manager および JP1/IM データベースを起動する。
JP1/IM - Manager および JP1/IM データベースを起動して、システム構成管理情報を取得します。
IM データベースの起動については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3.1 JP1/IM - Manager を起動する」を参照してください。
5. `jddsetaccessuser` コマンドを実行して、システム構成情報を取得する際に、監視対象製品にアクセスするユーザーを設定する。
`jddsetaccessuser` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jddsetaccessuser`」(1. コマンド) を参照してください。
6. 構成取得対象ホスト定義ファイル (`imdd_target_host.conf`) で、連携製品、および連携製品の監視オブジェクトの構成情報を取得するホスト名を定義する。(任意)
構成取得対象ホスト定義ファイル (`imdd_target_host.conf`) の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「構成取得対象ホスト定義ファイル (`imdd_target_host.conf`)」(2. 定義ファイル) を参照してください。
7. `jddcreatetree` コマンドを実行して、IM 管理ノード関連ファイルを生成する。
`jddcreatetree` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jddcreatetree`」(1. コマンド) を参照してください。
作成した IM 管理ノード関連ファイルを開き、内容を確認します。IM 管理ノード関連ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の IM 管理ノード関連ファイルについて説明している章を参照してください。
8. IM 管理ノードリンク定義ファイル (`imdd_nodeLink_def.conf`) で、IM 管理ノード間の関連を定義する。(任意)

IM 管理ノードリンク定義ファイル (imdd_nodeLink_def.conf) の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「IM 管理ノードリンク定義ファイル (imdd_nodeLink_def.conf)」(2. 定義ファイル) を参照してください。

9. jddupdatetree コマンドを実行して、定義内容をインテリジェント統合管理サーバに反映する。

jddupdatetree コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddupdatetree」(1. コマンド) を参照してください。

メモ

IM 管理ノードの構成を変更した場合は、5 以降の手順を再度実行してください。

4.3 インテリジェント統合管理基盤で暗号化機能を使用する場合の設定

インテリジェント統合管理基盤の暗号化通信機能では、インテリジェント統合管理基盤のビューアー（統合オペレーション・ビューアー）と JP1/IM - Manager の間の通信を暗号化します。

暗号化通信は、インテリジェント統合管理基盤定義ファイル (`imdd.properties`) の `server.port` プロパティに指定したポートを使用して行います。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インテリジェント統合管理基盤定義ファイル (`imdd.properties`)」(2. 定義ファイル) を参照してください。

暗号化通信の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の暗号化通信について説明している章を参照してください。

4.4 インテリジェント統合管理基盤のクラスタ環境を構築する

クラスタシステムで運用されている JP1/IM - Manager ホストに対応する場合に、インテリジェント統合管理基盤で行うクラスタ環境の構築については、「[7.4 インテリジェント統合管理基盤のクラスタ環境を構築する（Windows の場合）](#)」および「[8.4 インテリジェント統合管理基盤のクラスタ環境を構築する（UNIX の場合）](#)」を参照してください。

4.5 カスタム UI 表示機能を使用する場合の設定

カスタム UI 表示機能は、ユーザーが特定の IM 管理ノードを選択した際に、あらかじめ定義した IM 管理ノードに対応する任意の画面を「詳細表示」領域に表示する機能です。

カスタム UI 表示機能を使用する場合の設定手順を次に示します。

1. 統合オペレーション・ビューアーに表示する画面の定義ファイルを、html 形式で配置する。

配置場所は物理ホスト、論理ホストとも同じです。クラスタ構成の場合は、物理ホスト、論理ホストの両方に同じファイルを配置してください。

次の場所にサブフォルダ、またはサブディレクトリを作成して配置します。なお、「hitachi」から始まるサブフォルダ名、またはサブディレクトリ名は使用できません。

Windows の場合

Manager パス¥public¥customUI¥

UNIX の場合

/opt/jp1imm/public/customUI/

画面の定義ファイルの作成方法および記述例については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「6. 「統合オペレーション・ビューアー」画面のカスタマイズ」を参照してください。

2. インテリジェント統合管理基盤定義ファイル (imdd.properties) を編集する。

次のプロパティを指定します。指定は省略できません。

jp1.imdd.gui.settings.contentViews.<custom UI Id>.title

jp1.imdd.gui.settings.contentViews.<custom UI Id>.url

jp1.imdd.gui.settings.contentViews.<custom UI Id>.sid

jp1.imdd.gui.settings.contentViews.<custom UI Id>.target

各プロパティの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インテリジェント統合管理基盤定義ファイル (imdd.properties)」(2. 定義ファイル) を参照してください。

3. 統合オペレーション・ビューアーで、インテリジェント統合管理基盤定義ファイル (imdd.properties) に定義した IM 管理ノードを選択し、画面が表示されるか確認する。

定義情報が不正な場合は、ダイアログにメッセージが表示されます。メッセージに従って対処してください。

html の配置場所は物理ホストと論理ホストで共通ですが、どの html を表示させるかはそれぞれのインテリジェント統合管理基盤定義ファイル (imdd.properties) に定義します。このため、同じホスト上で物理ホストと論理ホストの JP1/IM - Manager を同時に立ち上げても、それぞれ別々の html を用いたカスタム UI 表示を統合オペレーション・ビューアーに表示できます。作成した html で使用できるメソッドとオブジェクトの詳細についてはマニュアル「JP1/Integrated Management 3 - Manager コマンド・定義

ファイル・API リファレンス」の「6.3 ユーザー定義画面で利用できるメソッドとオブジェクト」を参照してください。

インテリジェント統合管理基盤定義ファイル (`imdd.properties`) の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インテリジェント統合管理基盤定義ファイル (`imdd.properties`)」(2. 定義ファイル) を参照してください。

4.6 繰り返しイベントの表示抑止機能の互換設定

JP1/IM - Manager（インテリジェント統合管理基盤）のバージョン 12-00 では、`jcoimdef` コマンドの繰り返しイベントの監視抑止設定（`-storm` オプション）の設定が ON の場合でも、繰り返しイベントの表示が抑止されません。このため、JP1/IM - Manager（インテリジェント統合管理基盤）のバージョン 12-00 からバージョンアップした場合、繰り返しイベントの表示抑止機能を使用するには、繰り返しイベントの表示抑止機能の互換設定を無効（`false`）にする必要があります。

なお、バージョン 12-10 以降を新規インストールした場合、繰り返しイベントの表示抑止機能の互換設定はあらかじめ無効（`false`）に設定されています。

繰り返しイベントの互換表示の設定は、インテリジェント統合管理基盤定義ファイル（`imdd.properties`）の `jp1.imdd.event.stormCompatible` プロパティで設定します。

インテリジェント統合管理基盤の繰り返しイベントの表示抑止機能が有効となる条件を、次の表に示します。

表 4-1 繰り返しイベントの表示抑止機能が有効となる条件

- storm の設定値	jp1.imdd.event.stormCompatible の設定値	繰り返しイベントの表示抑止機能
on（有効）	true（バージョン 12-00 互換設定）	無効
	false（無効）	有効
off（無効）	true（バージョン 12-00 互換設定）	無効
	false（無効）	無効

`jcoimdef` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jcoimdef`」（1. コマンド）を参照してください。

インテリジェント統合管理基盤定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インテリジェント統合管理基盤定義ファイル（`imdd.properties`）」（2. 定義ファイル）を参照してください。

4.7 関連性の定義の設定

JP1/IM が製品標準で定義している関連性に対して、新たに関連性を定義したい場合は、IM 管理ノードリンク定義ファイル (`imdd_nodeLink_def.conf`) で IM 管理ノード間の関連の定義が必要です。

IM 管理ノードリンク定義ファイル (`imdd_nodeLink_def.conf`) の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「IM 管理ノードリンク定義ファイル (`imdd_nodeLink_def.conf`)」(2. 定義ファイル) を参照してください。

4.8 業務影響アイコンの設定

統合オペレーション・ビューアーの「業務フロー」タブでは、ルートジョブネット間のつながりを確認することによって、先行ルートジョブネットに問題が発生した際の後続ルートジョブネットへの影響範囲を把握できます。ただし、先行ルートジョブネットで実行に失敗したジョブによっては、後続のルートジョブネットに影響しない場合もあります。このため、ルートジョブネット間のつながりに、先行ルートジョブネットの障害が後続のルートジョブネットに影響するかどうかを、アイコン（業務影響アイコン）で表示します。

後続ルートジョブネットへ影響があるかどうかは、先行ルートジョブネットの連携ユニットのステータスの取得によって判定されます。業務影響アイコンは、ツリーで選択した IM 管理ノードが先行ルートジョブネット、または後続ルートジョブネットに当たる関連情報に対して表示されます。影響がない場合は、アイコンは表示されません。

表示される業務影響アイコンの種類と表示条件を次の表に示します。

表 4-2 業務影響アイコンの種類と表示条件

業務影響アイコン	表示条件
 (影響あり)	先行ルートジョブネットの連携ユニットのステータスがエラーで終了している場合、または未実行終了の場合
 (影響の確認時にエラーが発生した)	次のどれかの条件に合致した場合 - JP1/AJS - Manager からの情報取得に失敗した - 先行ユニットに指定されたユニットが JP1/AJS - Manager 上に存在しない、またはユニットが実行登録されていない - 影響情報を取得するルートジョブネット間の関連数が最大数を超えた 最大数の設定については、JP1/AJS のマニュアルを参照してください。
 (影響の有無が不明)	次のどれかの条件に合致した場合 - 先行または後続のルートジョブネットが 12-10 より前のバージョンの JP1/AJS - Manager 配下のルートジョブネットである - IM 管理ノードリンク定義ファイル (imdd_nodeLink_def.conf) に定義した関連に、連携ユニット情報が指定されていない - 先行ルートジョブネットが UNKNOWN ノードである

一つのルートジョブネット間のつながりに対して複数のユニット情報が存在し、それぞれへの影響が異なる場合は、（影響あり）、（影響の確認時にエラーが発生した）、（影響の有無が不明）、表示なしの順位で表示されます。

 アイコンを表示するかどうかは、インテリジェント統合管理基盤定義ファイル (imdd.properties) の `jp1.imdd.gui.linkedUnit.impact.unknownDisplay` プロパティで設定します。デフォルトは表示する設定です。表示しない設定とした場合は、空欄が表示されます。

連携ユニットの情報は、IM 管理ノードリンク定義ファイル (imdd_nodeLink_def.conf) の `value` パラメータの `unit` で設定します。JP1/IM - Manager（インテリジェント統合管理基盤）を 12-00 からバージョン

ンアップした場合は、`type` パラメーターの種別が`rootJobnetExecutionOrder`（ルートジョブネット実行順序）のリンク定義に、`value` パラメーターの`unit` の定義の追加が必要です。定義が追加されていない場合は、 アイコンまたは空欄が表示されます。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「IM 管理ノードリンク定義ファイル (`imdd_nodeLink_def.conf`)」(2. 定義ファイル) および「インテリジェント統合管理基盤定義ファイル (`imdd.properties`)」(2. 定義ファイル) を参照してください。

4.9 連携製品のモニター起動の設定

インテリジェント統合管理基盤のモニター起動の設定については、「[5.17 連携製品のモニター起動の設定](#)」を参照してください。

4.10 システムの状況に応じた対処アクションの提案機能の設定

システムの状況に応じた対処アクションの提案機能は、システム管理者が運用手順書に基づいて設定します。

提案機能の設定手順を説明します。

1. 最初に、提案定義ファイルを作成する。

作成時に定義する内容を次に示します。

- 対処アクションを表示する条件
どの IM 管理ノードに対処アクションを表示するかを定義します。
- 対処アクションを表示するユーザーの条件
どのユーザーに対して対処アクションを表示するかを紐づけします。
- 対処アクションを提案する条件
JP1 イベントの条件や時系列データの個数の条件、コマンドの実行結果の条件など、対処アクションをどんな時に提案するかを定義します。
- 対処アクションの内容
REST API の実行や製品プラグイン関数の実行、イベントの対処状況の変更など、何をするかを定義します。

2. 作成した提案定義ファイルを `jddupdatesuggestion` コマンドで、JP1/IM - Manager（インテリジェント統合管理基盤）に反映する。

[統合オペレーション・ビューアー] 画面のツリーに、定義した IM 管理ノードに提案があることを示す提案アイコンが表示されるようになります。定義した対処アクションの表示条件と一致した場合は、[統合オペレーション・ビューアー] 画面の [提案] タブに、対処アクションの内容や前回実行時の情報が表示されます。

提案定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「提案定義ファイル」(2. 定義ファイル) を参照してください。

4.11 OpenID プロバイダとシングルサインオン連携するための設定（外部製品との連携）

OpenID プロバイダで認証を行う JP1 製品以外の外部製品と、シングルサインオン連携するための設定について説明します。

4.11.1 OpenID プロバイダとシングルサインオン連携する

OpenID プロバイダとシングルサインオン連携する手順について説明します。

なお、OpenID 認証の設定は JP1/IM - Manager を再起動したあとに反映されます。JP1/IM - Manager を起動した状態で設定した場合、手順 6.まで実施した時点では設定は反映されません。

また、OpenID プロバイダと JP1/IM - Manager ホストの時刻に差異がある場合、OpenID 認証に失敗することがあります。

そのような場合には、OpenID プロバイダと JP1/IM - Manager ホストの時刻を秒単位の精度で合わせてください。許容される時刻の差異は、OpenID プロバイダの仕様や設定に依存します。

1. 連携先の OpenID プロバイダにインテリジェント統合管理基盤を登録し、インテリジェント統合管理基盤クライアント情報のクライアント ID、クライアントシークレットを取得する。

クライアントの登録方法については、連携する OpenID プロバイダの仕様を確認してください。

- インテリジェント統合管理基盤の REST API の認証方法に OpenID 認証を使用する場合は、JP1 ユーザー名と OpenID プロバイダに登録されているユーザー名をマッピングする際のアクセストークンに、ログインユーザー名が必要です。このため、OpenID 認証を使用する場合は、アクセストークンの `preferred_username` クレームに OpenID プロバイダのログインユーザー名を含めるよう、連携先の OpenID プロバイダの設定をしてください。OpenID 認証については、「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.2.8 REST API の認証方法」を参照してください。
- OpenID プロバイダのログインまたはログアウトが成功したあと、Web ブラウザーはインテリジェント統合管理基盤にリダイレクトします。このため、インテリジェント統合管理基盤の `jp1.imdd.oidc.<OpenID プロバイダのキー名>.redirect-uri` に設定するリダイレクト URL の URI と、インテリジェント統合管理基盤ログイン URI のリダイレクトを、許可に設定してください。

2. インテリジェント統合管理基盤定義ファイル（`imdd.properties`）に連携先の OpenID プロバイダの情報を定義する。

定義するプロパティの詳細についてはマニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インテリジェント統合管理基盤定義ファイル（`imdd.properties`）」（2. 定義ファイル）を参照してください。

なお、プロパティに設定する OpenID プロバイダの設定値は、OpenID プロバイダの構成情報を取得して設定してください。OpenID プロバイダは OpenID Connect の仕様に基づき、次に示す URI のパスで OpenID プロバイダの構成情報を提供します。

```
/.well-known/openid-configuration
```

詳細は、連携する OpenID プロバイダの仕様を確認してください。

3. インテリジェント統合管理基盤で使用する JP1 ユーザーを、`jddsetaccessuser` コマンドで設定する。
すでに設定済みの場合は、この操作は不要です。

`jddsetaccessuser` コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jddsetaccessuser`」(1. コマンド)を参照してください。

4. 手順 1. で取得した OpenID プロバイダに登録したクライアント ID とクライアントシークレットを、`jddsetopinfo` コマンドで設定する。

`jddsetopinfo` コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jddsetopinfo`」(1. コマンド)を参照してください。

5. インテリジェント統合管理基盤から OpenID プロバイダに接続する際に、プロキシサーバを通して接続する場合は、インテリジェント統合管理基盤定義ファイル (`imdd.properties`) にプロキシ情報を定義する。

プロキシサーバがない環境では設定する必要はありません。プロキシサーバのユーザー認証が必要な場合は、手順 6. の設定をしてください。

6. プロキシサーバのユーザー認証が必要な場合、インテリジェント統合管理基盤定義ファイル (`imdd.properties`) でユーザー情報を、`jddsetproxyuser` コマンドで認証情報を設定する。

プロキシサーバのユーザー認証が不要な場合は設定する必要はありません。

`jddsetproxyuser` コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jddsetproxyuser`」(1. コマンド)を参照してください。

7. JP1/IM - Manager サービスを起動する。

すでに起動中の場合は、再起動してください。

8. シングルサインオンマッピング定義ファイルに OpenID プロバイダに登録されているユーザー名と JP1/Base に登録されている JP1 ユーザー名のマッピングを定義する。

シングルサインオンマッピング定義ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「シングルサインオンマッピング定義ファイル (`imdd_sso_mapping.properties`)」(2. 定義ファイル)を参照してください。

9. `jddupdatessomap` コマンドまたはシングルサインオンマッピング定義反映 API (`im_api_v1_updateSsoMap`) で定義を反映する。

jddupdatessomap コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddupdatessomap」(1. コマンド)を参照してください。

シングルサインオンマッピング定義反映 API (im_api_v1_updateSsoMap) については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.14.1 シングルサインオンマッピング定義反映」を参照してください。

4.11.2 シングルサインオンマッピング定義ファイル (imdd_sso_mapping.properties) のリロード手順

シングルサインオンマッピング定義ファイル (imdd_sso_mapping.properties) のリロード手順について説明します。

シングルサインオンマッピング定義ファイル (imdd_sso_mapping.properties) については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「シングルサインオンマッピング定義ファイル (imdd_sso_mapping.properties)」(2. 定義ファイル)を参照してください。

1. シングルサインオンマッピング定義ファイル (imdd_sso_mapping.properties) で、OpenID プロバイダに登録されているユーザー名と JP1/Base に登録されている JP1 ユーザー名のマッピングを編集する。
2. jddupdatessomap コマンドまたはシングルサインオンマッピング定義反映 API (im_api_v1_updateSsoMap) で定義を反映する。

jddupdatessomap コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddupdatessomap」(1. コマンド)を参照してください。

シングルサインオンマッピング定義反映 API (im_api_v1_updateSsoMap) については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.14.1 シングルサインオンマッピング定義反映」を参照してください。

4.11.3 OpenID プロバイダとの連携解除手順

OpenID プロバイダとの連携を解除する手順について説明します。

1. JP1/IM - Manager サービスを停止する。
2. 連携先の OpenID プロバイダに登録済みのインテリジェント統合管理基盤情報を削除する。
3. jddsetopinfo コマンドで OpenID プロバイダに登録したクライアント ID とクライアントシークレットを削除する。

jddsetopinfo コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddsetopinfo」(1. コマンド)を参照してください。

4. jddsetproxyuser コマンドでインテリジェント統合管理基盤に設定されているプロキシサーバ認証情報を削除する。

インテリジェント統合管理基盤の OpenID 認証以外の通信でプロキシサーバを使用している場合、この手順は不要です。

jddsetproxyuser コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddsetproxyuser」(1. コマンド)を参照してください。

5. インテリジェント統合管理基盤定義ファイル (imdd.properties) を編集し、登録済みの連携先の OpenID プロバイダのプロパティを削除する。プロキシ情報を定義している場合もプロパティを削除する。

インテリジェント統合管理基盤定義ファイル (imdd.properties) については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インテリジェント統合管理基盤定義ファイル (imdd.properties)」(2. 定義ファイル)を参照してください。

6. インテリジェント統合管理基盤シングルサインオンマッピング定義ファイルを編集し、マッピング定義をすべて削除する。

7. JP1/IM - Manager サービスを起動する。

8. jddupdatessomap コマンドまたはシングルサインオンマッピング定義反映 API (im_api_v1_updateSsoMap) で定義を反映する。

シングルサインオンマッピング定義をクリアすることが目的のため、KAJY52031-W メッセージが出力されます。

jddupdatessomap コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddupdatessomap」(1. コマンド)を参照してください。

シングルサインオンマッピング定義反映 API (im_api_v1_updateSsoMap) については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.14.1 シングルサインオンマッピング定義反映」を参照してください。

4.12 ダイレクトアクセス URL の設定

ダイレクトアクセスするための URL には、目的の画面を表示するための情報をクエリパラメーターとして含めます。各機能のクエリパラメーターは、[統合オペレーション・ビューアー] 画面の index の後ろに指定します。

URL の形式を次に示します。

```
http://インテリジェント統合管理サーバのホスト名:ポート番号/index?<query parameters>=<value>&<query parameters>=<value>&eou=1
```

注 SSL 通信の場合はhttps を使用します。

4.12.1 ダイレクトアクセス URL

ダイレクトアクセス URL で指定するクエリパラメーターを次に示します。なお、各クエリパラメーターには URL エンコードした値を指定してください。

表 4-3 ダイレクトアクセス URL のクエリパラメーター

項番	クエリパラメーター	指定規則	説明
1	seqno	任意	イベント DB 内通し番号を指定します。
2	sid	任意	選択状態で表示するノードのツリー SID を指定します。 指定が省略された場合は、ツリーの先頭の [All Systems] のツリー SID が仮定されます。 seqno が指定されている場合は、sid が指定済みかどうかに関わらず、イベント DB 内通し番号に対応するsid を取得して、値を上書きします。
3	dialog	任意	detail が指定されている場合 [イベント詳細] 画面を表示します。 指定が省略された場合、不正な値が指定されている場合は、JP1 イベントの SID は取得されません。
4	tab	任意	ダイレクトアクセスで表示するタブを指定します。次の値を指定できます。 • <code>_HITACHIJP1PFMWC</code> [パフォーマンス] タブを表示します。 • <code>custom UI Id*</code> [カスタム UI] タブを表示します。Id にはカスタム UI 表示機能のプロパティ <code>jp1.imdd.gui.settings.contentView.<custom UI Id></code> に指定した値を指定してください。 • <code>suggestion</code> [提案] タブを表示します。 • <code>job</code> [業務フロー] タブを表示します。 • <code>relation</code>

項番	クエリパラメーター	指定規則	説明
			【関連ノード】 タブを表示します。 • trend 【トレンド】 タブを表示します。 指定が省略された場合は、表示するタブの優先度に従います。詳細は表 4-4 を参照してください。
5	view	任意	表示する【統合オペレーション・ビューアー】画面の、【稼働状況】領域の形式を指定します。指定できる形式を次に示します。 • sunburst：サンバースト形式 • tree：ツリー形式 指定が省略された場合は、sunburst が仮定されます。
6	eou	必須	URL の終端フラグです。URL の末尾に「1」を指定します。

注※

カスタム UI 表示機能のプロパティ `jp1.imdd.gui.settings.contentViews.<custom UI Id>` については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「6.2 【統合オペレーション・ビューアー】画面のカスタマイズの定義情報」を参照してください。

表 4-4 表示するタブの優先度

タブ名	優先度
パフォーマンス	1
カスタム UI※	2
提案	3
業務フロー	4
関連ノード	5
トレンド	6

注※

ユーザーが定義した【カスタム UI】タブは、定義した数に応じた個数が表示されます。なお、【カスタム UI】タブの表示順は、インテリジェント統合管理基盤定義ファイル (`imdd.properties`) に定義された順序で表示されます。詳細は、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インテリジェント統合管理基盤定義ファイル (`imdd.properties`)」(2. 定義ファイル) を参照してください。

! 重要

- サーバリプレースやディスク障害などでイベント DB 内通し番号が変更された場合は、JP1/IM - Manager の統合監視 DB でイベント DB の通し番号が重複する可能性があります。イベント DB 内通し番号が重複した場合は、`seqno` パラメーターで引き当てるイベント情報は最新のイベントとなります。このため、古いインシデントの情報からイベント DB 内通し番号を `seqno` パラメーターに指定した場合などは、目的と異なるイベントを引き当てる

おそれがあります。イベント DB 内通し番号が変更された場合は、パラメーターを指定する際に、インシデントの内容とイベントの内容が合致しているかを確認してください。

- seqno パラメーターに指定したイベント DB 内通し番号は、イベント DB 内通し番号に対応するsid を引き当てたあとにリダイレクトされるため、Web ブラウザーのアドレスバーには残りません。そのため、呼び出し元でイベント DB 内通し番号を保持しておき、イベント情報を確認できるようにしてください。

4.12.2 ノード選択のダイレクトアクセス URL 取得

ノード選択のダイレクトアクセスの URL は、[統合オペレーション・ビューアー] 画面の [操作メニュー] - [ツリーの URL をコピー] で取得します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.1 [統合オペレーション・ビューアー] 画面の概要」を参照してください。

[ツリーの URL をコピー] で生成されるダイレクトアクセス URL の形式を次に示します。

```
http://サーバのホスト名:ポート番号/index?sid=<sid>&view=<view>&eou=1
```

クエリパラメーターに設定されている値の意味は、次のとおりです。

表 4-5 ノード選択のダイレクトアクセス URL 取得のクエリパラメーター

クエリパラメーター	意味
sid	[ツリーの URL をコピー] ボタンをクリックした際に選択しているノードに対応するツリー SID です。
view	[ツリーの URL をコピー] ボタンをクリックした際に表示している [稼働状況] 領域の形式です。 • sunburst : サンバースト形式 • tree : ツリー形式
eou	常に1が表示されます。

サンバースト形式を表示している際に、システム「SYSTEM01」の所属ホスト「HOSTB」のノードを選択している状態の場合に、[ツリーの URL をコピー] ボタンで取得されるダイレクトアクセス URL の例を、次に示します。

```
http://HOSTA:20703/index?sid=%5FR00T%5FAllSystems%2F%5FSYSTEM%5FSYSTEM01%2F%5FHOST%5FHOSTB&view=sunburst&eou=1
```

4.12.3 OpenID 認証ダイレクトアクセス URL

OpenID 認証ダイレクトアクセス URL は、ダイレクトアクセス URL 機能を OpenID 認証でのシングルサインオンで利用できるようにする機能です。ダイレクトアクセス URL のクエリパラメーターと同時に指定できます。

クエリパラメーターに指定するパラメーターを次に示します。なお、各パラメーターには URL エンコードした値を指定してください。

表 4-6 OpenID 認証のダイレクトアクセス URL のクエリパラメーター

項番	クエリパラメーター	指定規則	説明
1	op	任意	OpenID プロバイダ名を指定します。OpenID プロバイダ名には、インテリジェント統合管理基盤定義ファイル (imdd.properties) で定義した<OpenID プロバイダのキー名>と同じ値を指定する必要があります。 このパラメーターを指定した場合、インテリジェント統合管理基盤のログイン画面を経由しないで、指定された OpenID プロバイダの認証 URL に認証リクエストを実行します。 存在しない OpenID プロバイダのキー名を指定した場合は、OP パラメーターが指定されていないものと仮定して動作します。

op パラメーターの指定有無と、インテリジェント統合管理基盤定義ファイル (imdd.properties) の jp1.imdd.jp1LoginForm パラメーター、および OpenID プロバイダ定義機能に定義した OpenID プロバイダ定義数による OpenID 認証ダイレクトアクセス URL 機能の動作を次の表に示します。

表 4-7 op パラメーター、OP 定義数、jp1.imdd.jp1LoginForm パラメーターの関係

op パラメーター	OP 定義数	jp1.imdd.jp1LoginForm の指定値	
		true	false
指定なし	なし	ログイン画面を表示	ログイン画面を表示 (JP1/Base 認証ログインフォームが表示されます)
	1		OpenID プロバイダの認証 URL に認証リクエストを送信
	2 以上		ログイン画面を表示
指定あり	なし	ログイン画面を表示 (op パラメーターの指定は無視されます)	
	1	OpenID プロバイダの認証 URL に認証リクエストを送信	
	2 以上		

なお、jp1.imdd.jp1LoginForm パラメーターに false を指定し、かつ OpenID プロバイダの定義が一つだけの場合は、op パラメーターを省略したときでも、定義した OpenID プロバイダに直接認証します。

❗ 重要

「統合オペレーション・ビューアー」画面の「操作メニュー」－「ツリーの URL をコピー」で取得した URL には、op パラメーターは付与されません。

次の条件の場合のダイレクトアクセス URL の指定例を示します。

- システム「SYSTEM01」の所属ホスト「HOSTB」のノードを選択している状態の「統合オペレーション・ビューアー」画面を表示する
- okta 認証
- 表示形式：サンバースト

```
http://インテリジェント統合管理サーバのホスト名:ポート番号/index?op=okta&sid=%5FR00T%5FALLSystems%2F%5FSYSTEM%5FSYSTEM01%2F%5FHOST%5FHOSTB&view=sunburst&eou=1
```

4.12.4 ダイレクトアクセス URL の指定例

ダイレクトアクセス URL の指定例について説明します。

なお、インテリジェント統合管理基盤サービスで、HTTP 通信を受け付けるポート番号を変更している場合は、定義例のポート番号「20703」を変更後のポート番号に変更してください。また、JP1/IM - Manager の通信暗号化機能を使用して、Web ブラウザーとインテリジェント統合管理基盤の間の通信を https で暗号化する場合は、http を https にしてください。

(1) 「イベント詳細」画面を指定してアクセスする場合

URL

```
http://サーバのホスト名:ポート番号/index?seqno=3611&dialog=detail&eou=1
```

表示される画面

seqno（イベント DB 内通し番号）に対応する IM 管理ノードが選択された状態で、「イベント詳細」画面が表示されます。



(2) タブを指定してアクセスする場合

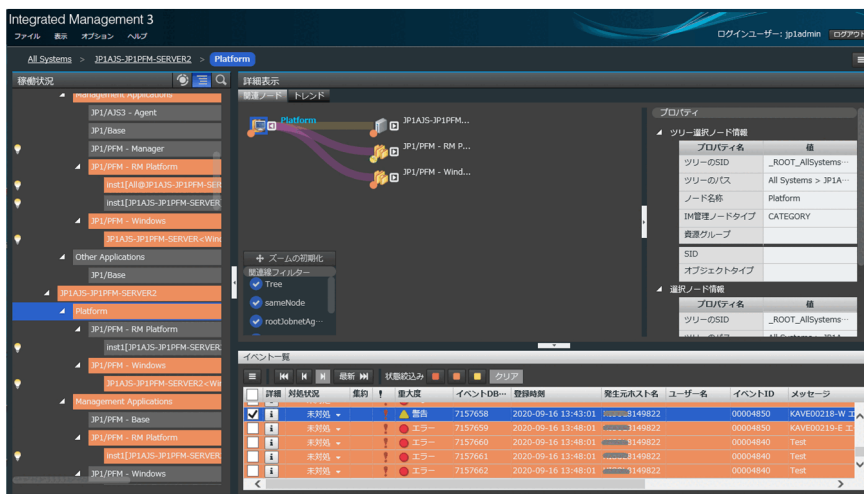
URL

<http://サーバのホスト名:ポート番号/index?seqno=3611&tab=relation&eou=1>

表示される画面

seqno（イベント DB 内通し番号）に対応する IM 管理ノードが選択された状態で、指定したタブが表示されます。

上記の URL は「関連ノード」タブを指定しています。



(3) タブと「イベント詳細」画面を指定してアクセスする場合

URL

<http://サーバのホスト名:ポート番号/index?seqno=3611&dialog=detail&tab=trend&eou=1>

表示される画面

seqno（イベント DB 内通し番号）に対応する IM 管理ノードが選択された状態で指定したタブを表示し、さらに「イベント詳細」画面が表示されます。

上記の URL は [トレンド] タブを指定しています。



(4) 自動アクションの定義例

自動アクション機能でダイレクトアクセス URL を使用する場合の例を、説明します。

例 1

[統合オペレーション・ビューアー] 画面で、特定の IM 管理ノードの業務インパクトを確認するための URL を、自動アクションで担当者 (userA) にメール通知する。

メール受信者がメール本文の URL をクリックすると、ダイレクトアクセス URL 機能によって、[業務フロー] タブを開いた状態で [統合オペレーション・ビューアー] 画面が表示される。

メールの定義

送信元 (From) : admin@xxxxxx.com

送信先 (To) : userA@xxxxxx.com

メールの主題 : 業務インパクト確認

メールの本文 : http://インテリジェント統合管理サーバのホスト名:20703/index?

seqno=73&tab=job&eou=1

コマンドの定義例

```
jimmail.exe -to userA@xxxxxx.com -s "業務インパクト確認" -b "http://$ACTHOST:20703/index?seqno=$EVSEQNO&tab=job&eou=1"
```

例 2

自動アクションで、障害発生時にインテリジェント統合管理の [統合オペレーション・ビューアー] 画面で、該当ノードの [イベント詳細] 画面を確認するための URL を、担当者 (userA) にメール通知する。

メール受信者がメール本文の URL をクリックすると、ダイレクトアクセス URL 機能によって、[イベント詳細] 画面を開いた状態で [統合オペレーション・ビューアー] 画面を表示する。

メールの定義

送信元 (From) : admin@xxxxxx.com

送信先 (To) : userA@xxxxx.com

メールの主題 : [重大度:Error] 障害発生通知

メールの本文 : http://インテリジェント統合管理サーバのホスト名:20703/index?
seqno=74&detail=1&eou=1

コマンドの定義例

```
jimmail.exe -to userA@xxxxx.com -s "[重大度:$EVSEV] 障害発生通知" -b "http://$ACTHOST:  
20703/index?seqno=$EVSEQNO&dialog=detail&eou=1"
```

4.13 システム構成情報反映方式の設定

システム構成情報は、統合オペレーション・ビューアー（WebGUI）から参照、管理できます。また、統合オペレーション・ビューアーから、マネージャーおよびエージェントの定義ファイルをダウンロード／アップロードして設定を変更できる機能や、IM 管理ノードのツリー情報を生成、反映できる機能も提供しています。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.6 WebGUI（統合オペレーション・ビューアー）を使用した運用」を参照してください。

ここでは、システム構成情報反映方式の設定について説明します。

システムの構成情報の反映方式を、`jddupdatetree` コマンドのオプションで指定します。なお、`jddupdatetree` コマンドで反映方式のオプションを指定しなかった場合は、インテリジェント統合管理基盤定義ファイル（`imdd.properties`）の `jp1.imdd.simt.updateMode` プロパティの定義に従います。

次の場合は「新規・再構築モード」を指定します。

- 新規構築する場合
- 構築ミスを修正する場合
- IM データベースをバックアップ（`jimdbbackup` コマンド）し、リカバリー（`jimdbrecover` コマンド）した場合
- 統合監視 DB をアンセットアップ（`jcodbunsetup` コマンド）し、再セットアップ（`jcodbsetup` コマンド）した場合
- インテリジェント統合管理基盤を利用している環境で、JP1/IM - Manager をバージョンアップした場合

次の場合は「構成変更モード」を指定します。

- 構築ミスの修正以外に、インテリジェント統合管理基盤の管理対象の追加・削除・変更を反映する場合

なお、`jddupdatetree` コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jddupdatetree`」(1. コマンド)、インテリジェント統合管理基盤定義ファイル（`imdd.properties`）については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インテリジェント統合管理基盤定義ファイル（`imdd.properties`）」(2. 定義ファイル)を参照してください。

4.14 IM 管理ノードリンク定義ファイルの移行手順

JP1/IM と JP1/AJS をバージョン 12-50 以降にアップデートする際に、[連携ユニット] ダイアログの [連携予定日時] に表示される情報を、ルートジョブネットの関連付けで自動的に関連付けした場合の情報に統一したいときの手順について説明します。移行手順の対象となるのは、IM 管理ノードリンク定義ファイル (imdd_nodeLink_def.conf) で、待ち合わせ条件やジョブネットコネクタを定義している環境の場合だけです。

IM 管理ノードリンク定義ファイル (imdd_nodeLink_def.conf) については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「IM 管理ノードリンク定義ファイル (imdd_nodeLink_def.conf)」(2. 定義ファイル) を参照してください。[連携ユニット] ダイアログについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.14.2 業務インパクトの判断支援」を参照してください。

1. IM 管理ノードリンク定義ファイル (imdd_nodeLink_def.conf) が存在するか確認する。
2. IM 管理ノードリンク定義ファイルの「type」(処理対象種別) に「rootJobnetExecutionOrder」(ルートジョブネット実行順序の関連) を指定しているか確認する。
3. 「rootJobnetExecutionOrder」の定義内容が、次に示す項目と一致しているか確認する。
該当しない場合は、手順 4.以降は不要です。
 - 次の待ち合わせ条件を使用したユニットの関連を定義している。
from: 待ち合わせ対象ユニット
to: 待ち合わせ条件付きユニット
 - 次のジョブネットコネクタを使用した関連を定義している。
from: 接続先ルートジョブネット, またはジョブネットコネクタ
to: ジョブネットコネクタ, または接続先ルートジョブネット
4. IM管理ノードリンク定義ファイルから設定内容を削除する。
手順 3.で該当した定義を削除します。
5. jddcreatetree コマンドを実行する。
jddcreatetree コマンドを実行し、構成情報を取得します。jddcreatetree コマンドについては、「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddcreatetree」(1. コマンド) を参照してください。
6. jddupdatetree コマンドを実行する。
jddupdatetree コマンドを実行し、IM 管理ノードのツリー情報とリンク情報を作成します。
jddupdatetree コマンドについては、「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddupdatetree」(1. コマンド) を参照してください。

4.15 統合オペレーション・ビューアーを使用するための Web ブラウザーの設定手順

統合オペレーション・ビューアーを使用する場合は、次の手順に従ってください。インテリジェント統合管理基盤を使用するために、次に示す Web ブラウザーの設定が必要です。設定方法の詳細については、使用する Web ブラウザーのドキュメントを参照してください。

- JavaScript を有効にする
- Cookie を有効にする
- 画像（GIF データ）の表示を有効にする
- ポップアップブロックの設定

ポップアップブロックの設定が有効になっているとダイアログボックスの表示がブロックされる場合がありますので、許可するサイトに統合オペレーション・ビューアーのアドレスを追加してください。

JP1/IM - Manager の通信暗号化機能を使用する場合（Web ブラウザーとインテリジェント統合管理基盤の間の通信を https で暗号化する場合）、Web ブラウザーの SSL/TLS の設定を有効にする必要があります。

また、ルート証明書（サーバ証明書を発行した認証局のもの）がインポートされていない場合、ルート証明書をインポートしてください。

4.16 ダッシュボードの設定

統合オペレーション・ビューアーの [ダッシュボード] 画面、および [ダッシュボード] タブに表示する内容を、運用に合わせて設定できます。

監視対象システムに適したダッシュボードを設定することで、IT システムの健全性の可視化ができます。

4.16.1 自動生成ダッシュボードをカスタマイズする

統合オペレーション・ビューアーは、[稼働状況] 領域で選択した IM 管理ノードごとに、自動生成ダッシュボードを [ダッシュボード] タブにデフォルトで表示します。

この自動生成ダッシュボードをカスタマイズする手順を、次に示します。

1. [ダッシュボード] タブの操作メニューから [ダッシュボード複製] メニューを選択する。
2. [ダッシュボード] タブの編集画面で、任意のダッシュボード名を入力する。
3. パネルの追加や編集を実施したあと、[保存] ボタンをクリックし、[編集終了] ボタンをクリックして終了する。

カスタマイズしたダッシュボードを編集したい場合は、[編集] メニューから編集できます。

4.16.2 ダッシュボードを新規に作成する

統合オペレーション・ビューアーでは、特定の IM 管理ノードには依存しない任意のダッシュボードを新規に作成できます。作成したダッシュボードは、ダッシュボードの URL をコピーして、独立した [ダッシュボード] 画面として利用できます。

さらに、作成したダッシュボードをお気に入りに登録しておくことで、どの IM 管理ノードを選択しても [ダッシュボード] タブのサイドメニューから表示できるようになります。

ダッシュボードを新規に作成する手順を、次に示します。

1. [統合オペレーション・ビューアー] 画面のメニューから [表示] - [ダッシュボード一覧] を選択する。
2. [ダッシュボード一覧] ダイアログで、[新規追加] ボタンをクリックする。
3. 編集画面で任意のダッシュボード名を入力する。
4. パネルの追加を実施したあと、[保存] ボタンをクリックし、[編集終了] ボタンをクリックして終了する。

4.16.3 ダッシュボードを編集する

[ダッシュボード一覧] ダイアログで、新規に作成したダッシュボードや、自動生成ダッシュボードをカスタマイズしたダッシュボードを編集できます。

ダッシュボードを編集する手順を、次に示します。

1. [ダッシュボード一覧] ダイアログで、編集対象のダッシュボードを確認し、[編集] ボタンをクリックする。
2. 編集画面で、ダッシュボード名やパネルの編集を実施したあと、[保存] ボタンをクリックし、[編集終了] ボタンをクリックして終了する。

4.16.4 [ダッシュボード] 画面を共有する

自動生成ダッシュボードや新規作成したダッシュボードは、[ダッシュボード] 画面として独立した画面で表示できます。

この画面の URL を取得するための手順を、次に示します。URL を共有することで、複数のユーザーやシステムで [ダッシュボード] 画面を共有できます。

1. 新規作成したダッシュボードを共有する場合は、[ダッシュボード一覧] ダイアログで、対象のダッシュボードを確認し、公開範囲列で [共有] に変更する。
2. ダッシュボード一覧で対象のタイトルを選択してダッシュボードを表示する、または、統合オペレーション・ビューアーで IM 管理ノードを選択し、[ダッシュボード] タブに対象のダッシュボードを表示する。
3. 表示されたダッシュボードの操作メニューから [ダッシュボードの URL をコピー] メニューを選択する。
4. [ダッシュボード URL コピー] ダイアログで、[クリップボードにコピー] ボタンをクリックする。

4.16.5 ダッシュボードを削除する

自動生成ダッシュボードからカスタマイズしたダッシュボードや、新規作成したダッシュボードを削除できます。

ダッシュボードを削除する手順を、次に示します。なお、ダッシュボードを削除して、IM 管理ノードに関連付いているダッシュボードが無くなった場合は、自動生成ダッシュボードが再度表示されるようになります。

1. [ダッシュボード一覧] ダイアログで、削除対象のダッシュボードを確認し、[削除] ボタンをクリックする。

2. [ダッシュボード削除] ダイアログで、削除内容を確認し、[OK] ボタンをクリックする。

5

セントラルコンソールの設定

この章では、セントラルコンソールの機能である JP1 イベントのフィルタリング、自動アクションなどの設定手順について説明します。

5.1 JP1/IM のイベント取得時の動作設定

JP1/IM - Manager がイベントサービスに登録された JP1 イベントを取得するときのイベント取得フィルターの条件や、マネージャーのメモリー上に JP1 イベントをバッファリングするバッファサイズ、ログイン時に統合監視 DB から取得するイベントの範囲などを設定します。

通常は、デフォルトの設定で運用できますが、必要に応じて設定をカスタマイズしてください。設定する項目を次に示します。

- イベント取得フィルターの設定
- JP1 イベントを抽出して、マネージャー上にバッファリングするときのイベント件数の上限（イベントバッファ）
- イベントサービスと再接続するときのリトライ回数およびリトライ間隔
- jcochstat コマンドの使用許可
- ログイン時のイベント取得範囲の設定

設定は、JP1/IM - View の [システム環境設定] 画面を使用します。なお、ここで設定した内容はマネージャーの JP1/IM - Manager に保存されます。このため、同じ JP1/IM - Manager に接続しているすべての JP1/IM - View で見え方が同じになります。

イベント取得時の動作を設定する手順を次に示します。

1. [システム環境設定] 画面を起動する。

[イベントコンソール] 画面で [オプション] - [システム環境設定] を選択します。

2. パラメーターを調整する。

必要に応じて、イベントバッファの件数やイベントサービスとの接続リトライ数などのパラメーターを調整してください。

[システム環境設定] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.11 [システム環境設定] 画面」を参照してください。

❗ 重要

システムプロファイル（.system）にも上記の設定についての定義内容が記述されていますが、直接編集することは推奨しません。設定を誤ると JP1/IM - Manager の動作が不正になることがあります。

5.1.1 ログイン時のイベント取得範囲を指定してイベントを表示する

ログイン時のイベント取得範囲に、重要イベントの対処までに必要な日数を設定すると、JP1/IM にログインするだけで、対処済み以外の重要イベント、および最新のイベントを表示できます。指定方法は、日数指定または時間指定のどちらかです。

日数指定または時間指定によって、イベント取得開始位置の指定方法が異なります。設定した日数とログイン時のセントラルコンソールが稼働するホストの時刻、および基準時刻を使用して指定します。

指定する手順を次に示します。

1. [イベントコンソール] 画面のメニューから [オプション] - [システム環境設定] を選択する。
[システム環境設定] 画面が表示されます。
2. [表示] - [[イベント監視] ページで有効にする], または [[重要イベント] ページで有効にする] のチェックボックスをチェックする。
[イベント取得の範囲] が活性となります。
3. [基準時刻] および [日分], または [時間分] を指定する。
[基準時刻] は、1 日の区切りとする時刻を 00:00~23:59 の範囲で指定できます。デフォルトは、09:00 です。

メモ

ログイン時にセントラルコンソールが稼働しているホストの基準時刻と現在時刻の大小関係によって、イベントの表示範囲が変わります。それぞれの場合の JP1 イベントの表示範囲について次に示します。

- ログイン時にセントラルコンソールが稼働しているホストの現在時刻が現在日の基準時刻より大きい場合
(現在日 - (設定した日数 - 1)) の日付の基準時刻を、イベント取得開始位置とする。
- ログイン時にセントラルコンソールが稼働しているホストの現在時刻が現在日の基準時刻より小さい場合
(現在日 - 設定した日数) の基準時刻をイベント取得開始位置とする。

ログイン時に、イベント取得開始位置から最新のイベントが表示されます。その後は、イベントが発生するごとに表示されます。

例えば、取得範囲を「2 日分」、基準時刻に「09:30」を指定した場合、6 月 23 日「09:15」にログインすると 6 月 21 日の「09:30」から最新までの JP1 イベントの一覧を表示されます。

[日分] は、過去何日分の JP1 イベントを表示するか 1~31 日の範囲で指定できます。デフォルトは、1 日です。

[時間分] は、ログイン時に最新のイベントから何時間分のイベントを取得するか 1~744 の範囲で指定できます。デフォルトは 1 です。

4. [OK] をクリックする。

設定した内容（ログイン時のイベント取得範囲）が有効となり，[システム環境設定] 画面が閉じます。
次回ログイン時から [イベントコンソール] 画面に，指定した期間の JP1 イベントが表示されます。

ログイン時にセントラルコンソールが稼働しているホストの現在時刻が現在日の基準時刻より大きい場合など，1 日分で指定した範囲が，24 時間分とならない場合があります。基準時刻をまたいで引き継ぎを行う場合，前任者の監視範囲も引き継ぎ対象とするには，監視範囲を+1 日するか，スライダーを使用してイベントを表示してください。

ログイン時のイベント取得範囲の詳細については，マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.17 ログイン時のイベント取得範囲」を参照してください。

5.2 JP1 イベントのフィルタリングの設定

[イベントコンソール] 画面に表示する JP1 イベントの種類を制限するためにフィルターを設定できます。これによって、監視の目的に合った JP1 イベントだけを表示することができます。[イベントコンソール] 画面から設定できるフィルターには、次の 4 種類があります。

- 表示フィルター

[イベントコンソール] 画面の [イベント監視] ページ、または [重要イベント] ページに表示する JP1 イベントの条件をユーザーが設定します。各 JP1 ユーザーにつき、50 個まで定義できます。

- ユーザーフィルター

ユーザーが監視できる JP1 イベントの種類をシステム管理者が設定します。ユーザーフィルターは 128 個まで定義できます。

- 重要イベントフィルター

[イベントコンソール] 画面の [重要イベント] ページに表示する重要イベントを定義します。

- イベント取得フィルター※

JP1/IM - Manager (イベント基盤サービス) が JP1/Base (イベントサービス) からイベントを取得するときのフィルター条件を設定します。マネージャーごとに、50 個まで定義できます。

注※

イベント取得フィルター (互換用) の場合、JP1/IM - Manager の一制御 (イベントコンソールサービス) が JP1/IM - Manager の一制御 (イベント基盤サービス) からイベントを取得するときのフィルター条件となります。

次に各フィルターの設定手順について説明します。

5.2.1 表示フィルターを設定する

[イベントコンソール] 画面の [イベント監視] ページ、または [重要イベント] ページに表示する JP1 イベントの条件を設定します。

(1) 表示フィルターを新規に作成する

表示フィルターを新規に作成する手順を次に示します。

1. イベント一覧に表示されている JP1 イベントの属性値を表示条件として利用する場合は、イベント一覧から JP1 イベントを選択する。
2. [イベントコンソール] 画面から [表示] - [表示フィルター一覧] を選択する。
[表示フィルター一覧] 画面が表示されます。この画面にはフィルター名が表示されます。
3. 新規に作成する場合は [追加] ボタンをクリック、既存フィルターを流用する場合は [複製] ボタンをクリックしたあと [編集] ボタンをクリックする。

[追加] ボタンをクリックすると、[表示フィルター設定] 画面が表示されます。

[複製] ボタンをクリックすると、「コピー 表示フィルター名」がフィルターに追加されます。この場合は「コピー 表示フィルター名」を選択し、[編集] ボタンをクリックして [表示フィルター設定] 画面を表示します。

4. [表示フィルター設定] 画面でフィルターの設定をする。

[表示フィルター設定] 画面では次の設定を行います。

- フィルター名の入力

設定条件を区別するために、フィルターに名前を付けます。

- 条件群の設定

フィルターの通過条件、および除外条件を区別するために、条件群に名前を付けます。

条件群は、通過条件群、除外条件群それぞれ最大 5 件設定でき、条件群同士の関係は OR 条件となります。

なお、条件群の設定は [一覧表示] ボタンをクリックして [一覧] を表示状態にしておく必要があります。

条件群の追加：[追加] ボタンをクリックすると、定義していない名称「条件群 n」（n は数字）が追加されます。

条件群の複製：条件群を選択し、[複製] ボタンをクリックすると、「コピー 選択した条件群名」が追加されます。

条件群の削除：条件群を選択し、[削除] ボタンをクリックすると、選択した条件群が削除されます。

条件群のリネーム：条件群を選択すると、選択した条件群の名前が [条件群名] に表示されます。これを編集し、フォーカスを移動すると、条件群の名前が変更されます。

- 条件の設定（各条件群の詳細設定）

フィルターの通過条件、または除外条件を設定します。

条件は、複数の条件を組み合わせで設定でき、条件同士の関係は AND 条件となります。

設定できる項目は、発生元ホスト名※¹、登録ホスト名、重大度、オブジェクトタイプ、オブジェクト名、登録名タイプ、登録名、事象種別、ユーザー名、メッセージ、プロダクト名、イベント ID、対処状況、アクション、および固有の拡張属性です。

統合監視 DB を使用する場合は、設定できる項目に、メモ※²、重大度変更※⁴、重大度(変更前)※³、表示メッセージ変更※⁴、メッセージ(変更後)※⁴、繰り返しイベント※⁵、および監視抑止 ID※⁵ が追加されます。

注※¹ 発生元ホストのマッピングを有効にした場合に設定できる項目です。

注※² メモ機能を有効にした場合に設定できる項目です。

注※³ 重大度変更機能を有効にした場合に設定できる項目です。

注※⁴ 表示メッセージ機能を有効にした場合に設定できる項目です。

注※⁵ 繰り返しイベントの監視抑止機能を有効にした場合に設定できる項目です。

[イベントコンソール] 画面で選択した JP1 イベントの属性値を条件一覧に反映させたいときは、[選択イベント条件入力] ボタンをクリックします。

繰り返しイベントの監視抑止機能を有効にした場合、[選択イベントの監視抑止 ID 入力] ボタンが表示されます。[イベントコンソール] 画面で選択した繰り返しイベントの監視抑止 ID を条件一覧の [監視抑止 ID] に反映させたいときは、[選択イベントの監視抑止 ID 入力] ボタンをクリックします。一つの集約イベントに集約されている繰り返しイベントには同じ監視抑止 ID が設定されているため、一つの集約イベントに集約されている繰り返しイベント（選択した繰り返しイベントと同じ監視抑止 ID の繰り返しイベント）をフィルタリングする際に使用します。

5. [OK] ボタンをクリックする。

[表示フィルター設定] 画面が閉じ、[表示フィルター一覧] 画面に戻ります。

6. [OK] ボタンをクリックする。

設定した内容（フィルターの追加）が有効になり、[表示フィルター一覧] 画面が閉じます。

(2) 表示フィルターを変更する

既存の表示フィルターの内容を変更する手順を次に示します。

1. イベント一覧に表示されている JP1 イベントの属性値を表示条件として利用する場合は、イベント一覧から JP1 イベントを選択する。

2. [表示フィルター設定] 画面を表示する。

次に示すどちらかの方法で [表示フィルター設定] 画面を表示します。

- [イベントコンソール] 画面から [表示] - [表示フィルター一覧] を選択し、[表示フィルター一覧] 画面を表示する。

次に、[表示フィルター一覧] 画面で変更したい表示フィルターを選択し、[編集] ボタンをクリックする。

- [イベントコンソール] 画面の [イベント監視] ページ、または [重要イベント] ページの [フィルター名] リストボックスから変更したい表示フィルターを選択し、[表示フィルター編集] ボタンをクリックまたはメニューバーから [表示] - [表示フィルター編集] を選択する。

3. [表示フィルター設定] 画面でフィルターの設定内容を編集する。

[イベントコンソール] 画面で選択した JP1 イベントの属性値を条件一覧に反映させたいときは、[選択イベント条件入力] ボタンをクリックします。

[イベントコンソール] 画面で選択した繰り返しイベントの監視抑止 ID を条件一覧の [監視抑止 ID] に反映させたいときは、[選択イベントの監視抑止 ID 入力] ボタンをクリックします。一つの集約イベントに集約されている繰り返しイベントには同じ監視抑止 ID が設定されているため、選択した繰り返しイベントと関連する繰り返しイベントをフィルタリングする際に使用します。

4. [OK] ボタンをクリックする。

[表示フィルター設定] 画面が閉じ、[表示フィルター設定] 画面を呼び出した画面に戻ります。[表示フィルター一覧] 画面に戻った場合は [OK] ボタンをクリックして設定した内容（フィルターの変更）を有効にしてください。

(3) 表示フィルターを削除する

既存の表示フィルターを削除する手順を次に示します。

1. [イベントコンソール] 画面から [表示] - [表示フィルター一覧] を選択する。
[表示フィルター一覧] 画面が表示されます。この画面にはフィルター名が表示されます。
2. 削除したい表示フィルターを選択して、[削除] ボタンをクリックする。
選択した表示フィルターが削除されます。
3. [OK] ボタンをクリックする。
設定した内容（フィルターの削除）が有効になり、[表示フィルター一覧] 画面が閉じます。

5.2.2 ユーザーフィルターを設定する

[イベントコンソール] 画面でユーザーが監視できる JP1 イベントを制限します。設定内容は、[ユーザーフィルター設定] 画面で [適用] ボタンをクリックしたあとに JP1/IM - View に配信するイベントが対象となります。ユーザーフィルターが設定されていないユーザーは、すべての JP1 イベントを監視できます。

ユーザーフィルターを設定するには、JP1_Console_Admin 権限が必要です。また、業務グループの参照・操作制限を設定している場合、JP1 資源グループと JP1 権限レベルの組み合わせによっては操作できないことがあります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.1.4(2) JP1 ユーザーに対する JP1 資源グループと JP1 権限レベルの割り当て」を参照してください。

(1) ユーザーフィルターを新規に作成する

ユーザーフィルターを新規に作成する手順を次に示します。

1. イベント一覧に表示されている JP1 イベントの属性値を条件として利用する場合は、イベント一覧から JP1 イベントを選択する。
2. [イベントコンソール] 画面から [オプション] - [ユーザーフィルター設定] を選択する。
[ユーザーフィルター設定] 画面が表示されます。
この画面には、フィルター名と対象ユーザー名が表示されます。
3. [追加] ボタンをクリックする。
[ユーザーフィルター詳細設定] 画面が表示されます。
4. [ユーザーフィルター詳細設定] 画面でフィルターの設定をする。
[ユーザーフィルター詳細設定] 画面では次の設定を行います。
 - フィルター名の入力
設定条件を区別するために、フィルターに名前を付けます。

- フィルターの対象ユーザー名の入力

フィルターによって制限を受けるユーザー名を入力します。複数のユーザー名を入力する場合は、ユーザー名をコンマで区切って入力します。

一人のユーザーを複数のフィルターの対象ユーザーにすることはできません。

- 条件群の設定

フィルターの通過条件、および除外条件を区別するために、条件群に名前を付けます。

条件群は、通過条件群、除外条件群それぞれ最大 30 件設定でき、条件群同士の関係は OR 条件となります。

なお、条件群の設定は [一覧表示] ボタンをクリックして [一覧] を表示状態にしておく必要があります。

条件群の追加：[追加] ボタンをクリックすると、定義していない名称「条件群 n」（n は数字）が追加されます。

条件群の複製：条件群を選択し、[複製] ボタンをクリックすると、「コピー 選択した条件群名」が追加されます。

条件群の削除：条件群を選択し、[削除] ボタンをクリックすると、選択した条件群が削除されます。

条件群のリネーム：条件群を選択すると、選択した条件群の名前が [条件群名] に表示されます。これを編集し、フォーカスを移動すると、条件群の名前が変更されます。

- 条件の設定（各条件群の詳細設定）

フィルターの通過条件、または除外条件を設定します。

条件は、複数の条件を組み合わせて設定でき、条件同士の関係は AND 条件となります。

設定できる項目は、登録ホスト名、重大度、オブジェクトタイプ、オブジェクト名、登録名タイプ、登録名、事象種別、ユーザー名、メッセージ、プロダクト名、イベント ID、対処状況の状態、アクションの状態、および固有の拡張属性です。発生元ホストのマッピングを有効にした場合は、設定できる項目に発生元ホスト名が追加されます。

[イベントコンソール] 画面で選択した JP1 イベントの属性値を条件一覧に反映させたいときは、[選択イベント条件入力] ボタンをクリックします。

5. [OK] ボタンをクリックする。

[ユーザーフィルター詳細設定] 画面が閉じ、[ユーザーフィルター設定] 画面に戻ります。

6. [適用] ボタンをクリックする。

設定した内容が適用されます。

(2) ユーザーフィルターを変更する

ユーザーフィルターの内容を変更する手順を次に示します。

1. イベント一覧に表示されている JP1 イベントの属性値を条件として利用する場合は、イベント一覧から JP1 イベントを選択する。
2. [イベントコンソール] 画面から [オプション] - [ユーザーフィルター設定] を選択する。

[ユーザーフィルター設定] 画面が表示されます。

3. [ユーザーフィルター設定] 画面で変更したいユーザーフィルターを選択して、[編集] ボタンをクリックする。

[ユーザーフィルター詳細設定] 画面が表示されます。

4. [ユーザーフィルター詳細設定] 画面でフィルターの設定内容を編集する。

[イベントコンソール] 画面で選択した JP1 イベントの属性値を条件一覧に反映させたいときは、[選択イベント条件入力] ボタンをクリックします。

5. [OK] ボタンをクリックする。

[ユーザーフィルター詳細設定] 画面が閉じ、[ユーザーフィルター設定] 画面に戻ります。

6. [適用] ボタンをクリックする。

設定した内容が適用されます。

(3) ユーザーフィルターを削除する

ユーザーフィルターを削除する手順を次に示します。

1. [イベントコンソール] 画面から [オプション] - [ユーザーフィルター設定] を選択する。

[ユーザーフィルター設定] 画面が表示されます。

2. [ユーザーフィルター設定] 画面で変更したいユーザーフィルターを選択して、[削除] ボタンをクリックする。

選択したユーザーフィルターが削除されます。

3. [適用] ボタンをクリックする。

設定した内容が適用されます。

5.2.3 重要イベントフィルターを設定する

[イベントコンソール] 画面の [重要イベント] ページに表示する重要イベントの条件を設定します。重要イベントフィルターを設定することで、どの JP1 イベントを重要イベントとするかを定義できます。

設定した内容はマネージャーの JP1/IM - Manager に保存されます。このため、同じ JP1/IM - Manager に接続しているすべての JP1/IM - View で見え方が同じになります。

重要イベントフィルターを設定するには、JP1_Console_Admin 権限が必要です。また、業務グループの参照・操作制限を設定している場合、JP1 資源グループと JP1 権限レベルの組み合わせによっては操作できないことがあります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.1.4(2) JP1 ユーザーに対する JP1 資源グループと JP1 権限レベルの割り当て」を参照してください。

重要イベントフィルターを設定する手順を次に示します。

1. イベント一覧に表示されている JP1 イベントの属性値を重要イベントの定義条件とする場合は、イベント一覧から JP1 イベントを選択する。

2. [イベントコンソール] 画面で、[オプション] – [重要イベント定義] を選択する。

[重要イベント定義] 画面が表示されます。

3. [重要イベント定義] 画面で重要イベントの定義を設定する。

[重要イベント定義] 画面では次の設定を行います。

- 条件群の設定

フィルターの通過条件、および除外条件を区別するために、条件群に名前を付けます。

条件群は、通過条件群、除外条件群それぞれ最大 30 件設定でき、条件群同士の関係は OR 条件となります。

なお、条件群の設定は [一覧表示] ボタンをクリックして [一覧] を表示状態にしておく必要があります。

条件群の追加：[追加] ボタンをクリックすると、定義していない名称「条件群 n」（n は数字）が追加されます。

条件群の複製：条件群を選択し、[複製] ボタンをクリックすると、「コピー 選択した条件群名」が追加されます。

条件群の削除：条件群を選択し、[削除] ボタンをクリックすると、選択した条件群が削除されます。

条件群のリネーム：条件群を選択すると、選択した条件群の名前が [条件群名] に表示されます。これを編集し、フォーカスを移動すると、条件群の名前が変更されます。

- 条件の設定（各条件群の詳細設定）

フィルターの通過条件、または除外条件を設定します。

条件は、複数の条件を組み合わせて設定でき、条件同士の関係は AND 条件となります。

設定できる項目は、登録ホスト名、重大度、オブジェクトタイプ、オブジェクト名、登録名タイプ、登録名、事象種別、ユーザー名、メッセージ、プロダクト名、イベント ID、アクションの状態、および固有の拡張属性です。発生元ホストのマッピングを有効にした場合は、設定できる項目に発生元ホスト名が追加されます。

[イベントコンソール] 画面で選択した JP1 イベントの属性値を条件一覧に反映させるには、[選択イベント条件入力] ボタンをクリックします。

4. [OK] ボタンをクリックする。

設定した定義が有効になり、[重要イベント定義] 画面が閉じます。

❗ 重要

重要イベントの定義は、マネージャーごとに一つだけ定義できます。同じマネージャーの JP1/IM - Manager に接続しているすべての JP1/IM - View で同じ見え方になります。設定内容を十分検討してから設定してください。

5.2.4 イベント取得フィルターを設定する

イベント取得フィルターの設定方法を、一つだけ設定する場合、切り替えて設定する場合に分けてそれぞれ説明します。イベント取得フィルターは、統合監視 DB を使用する場合または使用しない場合に関係なく設定されます。

ここで設定するイベント取得フィルターは、JP1/IM - Manager のすべてのサービスに配信する JP1 イベントを制限するフィルターです。

なお、イベント取得フィルター（互換用）の設定については、「[5.2.4\(4\) イベント取得フィルター（互換用）を設定する](#)」を参照してください。

(1) イベント取得フィルターを一つだけ設定する

JP1/IM - Manager が JP1/Base のイベント DB からイベントを取得するときのフィルター条件を一つだけ設定する場合の方法を示します。設定手順は、次のとおりです。なお、[システム環境設定] 画面を起動するには、JP1_Console_Admin 権限が必要です。また、業務グループの参照・操作制限を設定している場合、JP1 資源グループと JP1 権限レベルの組み合わせによっては操作できないことがあります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.1.4(2) JP1 ユーザーに対する JP1 資源グループと JP1 権限レベルの割り当て」を参照してください。

1. イベント一覧に表示されている JP1 イベントの属性値を条件として利用する場合は、イベント一覧から JP1 イベントを選択する。
2. [イベントコンソール] 画面で [オプション] - [システム環境設定] を選択する。
[システム環境設定] 画面が表示されます。
3. [システム環境設定] 画面の [適用中のフィルター] の [設定] ボタンをクリックする。
[イベント取得条件設定] 画面が表示されます。
設定済みのイベント取得フィルターを編集する場合は、[イベント取得条件] のドロップダウンリストからイベント取得フィルターを選択したあと、[設定] ボタンをクリックします。[イベント取得条件設定] 画面に選択したイベント取得フィルターの内容が表示され、設定内容を編集できます。
4. [イベント取得条件設定] 画面でフィルターの設定をする。
[イベント取得条件設定] 画面では次の設定を行います。
 - フィルター名とフィルター ID
新規でイベント取得フィルターを作成する場合、フィルター名を入力します。フィルター ID は、イベント取得条件一覧の中で、未使用のフィルター ID が数値の小さい順に自動的に割り振られます。イベント取得フィルターを編集する場合、編集するイベント取得フィルターのフィルター名およびフィルター ID が表示されます。フィルター名やフィルター ID を編集すると、フィルター名やフィルター ID が編集した内容に変更されます。新しいイベント取得フィルターが作成されるわけではありませんので、注意してください。また、すでに指定されているフィルター名やフィルター ID を重複して指定できません。

- 条件群の設定

フィルターの通過条件、および除外条件を区別するために、条件群に名前を付けます。なお、通過条件群と除外条件群に同じ名前は付けられません。

条件群は、通過条件群、除外条件群それぞれ最大 30 件設定でき、条件群同士の関係は OR 条件となります。

なお、条件群の設定は [一覧表示] ボタンをクリックして [一覧] を表示状態にしておく必要があります。

条件群の追加：[追加] ボタンをクリックすると、定義していない名称「条件群 n」（n は数字）が追加されます。

条件群の複製：条件群を選択し、[複製] ボタンをクリックすると、「コピー 選択した条件群名」が追加されます。

条件群の削除：条件群を選択し、[削除] ボタンをクリックすると、選択した条件群が削除されます。

条件群のリネーム：条件群を選択すると、選択した条件群の名前が [条件群名] に表示されます。これを編集し、フォーカスを移動すると、条件群の名前が変更されます。

- 条件の設定（各条件群の詳細設定）

フィルターの通過条件、または除外条件を設定します。

条件は、複数の条件を組み合わせて設定でき、条件同士の関係は AND 条件となります。

設定できる項目は、登録ホスト名、重大度（または JP1/SES イベント）、オブジェクトタイプ、オブジェクト名、登録名タイプ、登録名、事象種別、ユーザー名、メッセージ、プロダクト名、アクション、およびイベント ID です。

[イベントコンソール] 画面で選択した JP1 イベントの属性値を条件一覧に反映させるには、[選択イベント条件入力] ボタンをクリックします。

5. [OK] ボタンをクリックする。

[イベント取得条件設定] 画面が閉じ、[システム環境設定] 画面に戻ります。

6. [適用] ボタンをクリックする。

設定した内容が有効になります。

(2) イベント取得フィルターを切り替えて設定する

JP1/IM - Manager が JP1/Base のイベント DB からイベントを取得するときのフィルター条件を切り替えて設定する場合の方法を示します。

イベント取得フィルターを切り替えて設定する場合、[システム環境設定] 画面から [イベント取得条件一覧] 画面を表示して、イベント取得フィルターを設定します。この方法では、新規のイベント取得フィルターの作成や設定済みのイベント取得フィルターの編集、複製、および削除ができます。

設定手順は、次のとおりです。なお、[システム環境設定] 画面を起動するには、JP1_Console_Admin 権限が必要です。また、業務グループの参照・操作制限を設定している場合、JP1 資源グループと JP1 権限レベルの組み合わせによっては操作できないことがあります。詳細については、マニュアル「JP1/Integrated

Management 3 - Manager 導入・設計ガイド」の「4.1.4(2) JP1 ユーザーに対する JP1 資源グループと JP1 権限レベルの割り当て」を参照してください。

1. [イベントコンソール] 画面で [オプション] - [システム環境設定] を選択する。
[システム環境設定] 画面が表示されます。
2. [イベント取得条件] の [一覧編集] ボタンをクリックする。
[イベント取得条件一覧] 画面が表示されます。
3. イベント取得フィルターを編集・複製・削除する場合は、[イベント取得条件一覧] 画面の [フィルター一覧] から編集したいイベント取得フィルターを選択する。
4. 設定する内容にあわせて、[追加] ボタン・[編集] ボタン・[複製] ボタン・[削除] ボタンをクリックする。

[追加] ボタンをクリックした場合

[イベント取得条件設定] 画面が表示され、新しいイベント取得フィルターを設定できます。

[編集] ボタンをクリックした場合

[イベント取得条件設定] 画面が表示され、手順 3 で選択したイベント取得フィルターの設定を編集できます。[イベント取得条件設定] 画面で設定する内容の概要については、「[5.2.4\(1\) イベント取得フィルターを一つだけ設定する](#)」を参照してください。

[複製] ボタンをクリックした場合

選択したイベント取得フィルターが複製され、[フィルター一覧] に追加されます。複製されたイベント取得フィルターは、名称の文頭に「コピー」が追加されます。ここでは、複製されたイベント取得フィルターの名称は変更できません。

イベント取得フィルターの名称を変更したい場合は、[編集] ボタンをクリックして表示される [イベント取得条件設定] 画面で編集してください。

[削除] ボタンをクリックした場合

選択したイベント取得フィルターが削除されます。

5. [OK] ボタンをクリックする。
[イベント取得条件一覧] 画面が閉じ、[システム環境設定] 画面に戻ります。

6. [適用] ボタンをクリックする。
設定した内容が有効になります。

(3) 共通除外条件を設定する

一時的にメンテナンス対象ホストの発行する JP1 イベントを取得対象外または自動アクションの実行対象外とするための、共通除外条件を設定する方法を示します。共通除外条件の動作モードには、基本モードと拡張モードの 2 種類があります。jcochcefmode コマンドで共通除外条件の動作モードを基本モードと拡張モードに切り替えて使用します。JP1 イベントを自動アクションの実行対象外とする共通除外条件を使用する場合は、拡張モードにする必要があります。

共通除外条件を設定するには、基本モードの場合は「共通除外条件設定」画面、拡張モードの場合は「共通除外条件設定(拡張)」画面を使用します。拡張モードの場合には、共通除外条件拡張定義ファイルと `jcochfilter` コマンドの `-ef` オプションを使用して設定することもできます。共通除外条件の有効・無効を切り替える方法については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「6.5.3 適用するイベント取得フィルターを切り替える」を参照してください。

また、共通除外条件が拡張モードの場合、[イベントコンソール] 画面で監視したくない JP1 イベントを選択し、右クリックして表示されるポップアップメニューから「共通除外条件で除外」を選択すると、共通除外条件として登録できます。

登録した共通除外条件は、追加共通除外条件として、[システム環境設定] 画面に表示されます。共通除外条件が基本モードの場合は、「5.2.4(3)(a) 共通除外条件の基本モードと拡張モードの切り替え」を参照して拡張モードに切り替えてください。そのあと、追加共通除外条件を設定してください。追加共通除外条件の設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「6.5.4 追加共通除外条件を設定して JP1 イベントを監視またはアクション実行の対象外にする」を参照してください。

追加共通除外条件の編集方法は、共通除外条件の編集方法と同じです。「5.2.4(3)(b) 共通除外条件の設定 ([共通除外条件設定] 画面または [共通除外条件設定(拡張)] 画面を使用する場合)」を参考に編集してください。

(a) 共通除外条件の基本モードと拡張モードの切り替え

共通除外条件の動作モードを切り替える方法を次に示します。

1. JP1/IM - Manager を停止する。

2. 共通除外条件の動作モードを基本モードから拡張モードに変更する場合は、JP1/Base の正規表現を拡張正規表現に変更する。

拡張正規表現については、マニュアル「JP1/Base 運用ガイド」の使用する正規表現を拡張する説明をしている個所を参照してください。

共通除外条件の動作モードを拡張モードから基本モードに変更する場合は、手順 3 に進んでください。

3. 次のコマンドを実行する。

- 基本モードから拡張モードに変更する場合

```
jcochcefmode -m extended
```

- 拡張モードから基本モードに変更する場合

```
jcochcefmode -m normal
```

共通除外条件の動作モードが切り替わります。

4. JP1/IM - Manager を起動する。

なお、`jcochcefmode` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jcochcefmode`」(1. コマンド) を参照してください。

(b) 共通除外条件の設定（[共通除外条件設定] 画面または [共通除外条件設定(拡張)] 画面を使用する場合）

[共通除外条件設定] 画面（基本モードの場合）、[共通除外条件設定(拡張)] 画面（拡張モードの場合）を使用して、共通除外条件を設定する方法を次に示します。

なお、[システム環境設定] 画面を起動するには、JP1_Console_Admin 権限が必要です。また、業務グループの参照・操作制限を設定している場合、JP1 資源グループと JP1 権限レベルの組み合わせによっては操作できないことがあります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.1.4(2) JP1 ユーザーに対する JP1 資源グループと JP1 権限レベルの割り当て」を参照してください。

1. [イベントコンソール] 画面で [オプション] - [システム環境設定] を選択する。

[システム環境設定] 画面が表示されます。

2. 設定済みの共通除外条件を編集する場合は、[システム環境設定] 画面の対象の共通除外条件群名を選択して、[共通除外条件群一覧] の [設定] ボタンをクリックする。

[共通除外条件設定] 画面が表示されます。手順 4 に進みます。

3. 新たに共通除外条件を定義する場合は、[システム環境設定] 画面の [一覧編集] ボタンをクリックする。

[イベント取得条件一覧] 画面が表示されます。

[イベント取得条件一覧] 画面では、共通除外条件を追加、編集、複製、削除できます。基本モードの場合、共通除外条件群は最大 30 件設定できます。拡張モードの場合、共通除外条件群は最大 2,500 件設定できます。条件群同士の関係は OR 条件となります。

- 条件群の追加：[追加] ボタンをクリックすると、共通除外条件設定の画面が表示され、新規の共通除外条件群を設定できます。
- 条件群の編集：共通除外条件群を選択し、[編集] ボタンをクリックすると、共通除外条件設定の画面が表示され、選択した共通除外条件群を編集できます。
- 条件群の複製：共通除外条件群を選択し、[複製] ボタンをクリックすると、「コピー 選択した条件群名」が追加されます。
- 条件群の削除：共通除外条件群を選択し、[削除] ボタンをクリックすると、選択した条件群が削除されます。

4. 共通除外条件設定の画面で条件を設定する。

- 共通除外条件群 ID

共通除外条件群 ID をドロップダウンリストから選択します。

共通除外条件を追加する場合、共通除外条件群一覧の中で未使用の共通除外条件群 ID が、数値の小さい順に自動的に割り振られます。

共通除外条件を編集する場合、共通除外条件群一覧から選択した共通除外条件群 ID が表示されます。すでに指定されている共通除外条件群 ID を重複して指定できません。

追加共通除外条件を編集する場合は、共通除外条件 ID を指定できません。

- 共通除外条件群名

共通除外条件群の名称を入力します。

既存の共通除外条件群を選択した状態で名称を変更した場合は、新しく指定した名称で上書きされます。

- 除外対象（[共通除外条件設定(拡張)] 画面の場合だけ）

共通除外条件群（拡張）の除外対象を指定します。

共通除外条件に一致する JP1 イベントを取得対象外にする場合は、[イベントを取得対象外にする]を選択します。共通除外条件に一致する JP1 イベントを自動アクションの実行対象外にする場合は、[イベントを取得しアクションの実行対象外にする]を選択します。

- 条件の設定（各条件群の詳細設定）

取得対象外としたい JP1 イベントの条件を設定します。

条件は、複数の条件を組み合わせて設定でき、条件同士の関係は AND 条件となります。設定できる項目は、次のとおりです。

基本モードの場合

登録ホスト名、重大度（または JP1/SES イベント）、オブジェクトタイプ、オブジェクト名、登録名タイプ、登録名、事象種別、ユーザー名、メッセージ、プロダクト名、およびイベント ID です。

拡張モードの場合

イベント ID、登録要因、発行元プロセス ID、登録時刻、到着時刻、発行元ユーザー ID、発行元グループ ID、発行元ユーザー名、発行元グループ名、登録ホスト名、発行元 IP アドレス、メッセージ、重大度、ユーザー名、プロダクト名、オブジェクトタイプ、オブジェクト名、登録名タイプ、登録名、オブジェクト ID、事象種別、開始時刻、終了時刻、終了コード、発生元ホスト名、および固有の拡張属性です。

なお、重大度変更機能を有効にした場合、[重大度]は[重大度(変更前)]と表示されます。

[イベントコンソール] 画面で選択した JP1 イベントの属性値を条件一覧に反映させるには、[選択イベント条件入力] ボタンをクリックします。

5. [OK] ボタンをクリックする。

共通除外条件設定の画面が閉じ、[システム環境設定] 画面に戻ります。

6. 設定した共通除外条件を有効にしたい場合は、[適用] の各チェックボックスをチェックする。

7. [適用] ボタンをクリックする。

設定した内容が有効になります。

なお、[システム環境設定] 画面、[共通除外条件設定] 画面、[共通除外条件設定(拡張)] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の次の個所を参照してください。

- [システム環境設定] 画面

参照先：3.11 [システム環境設定] 画面

- [共通除外条件設定] 画面

参照先：3.15 [共通除外条件設定] 画面

- [共通除外条件設定(拡張)] 画面

参照先：3.16 [共通除外条件設定(拡張)] 画面

(c) 共通除外条件の設定（共通除外条件拡張定義ファイルおよび jcochfilter コマンドを使用する場合）

拡張モードの場合、共通除外条件を共通除外条件拡張定義ファイルおよび jcochfilter コマンドの -ef オプションを使用して設定できます。設定する方法を次に示します。

1. 共通除外条件拡張定義ファイルで、条件群を定義する。
2. jcochfilter コマンドを実行し、定義した条件群を一括で反映する。

次のようにコマンドを入力します。

jcochfilter -ef 共通除外条件拡張定義ファイル名

共通除外条件拡張定義ファイルについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「共通除外条件拡張定義ファイル」(2. 定義ファイル)を参照してください。

jcochfilter コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcochfilter」(1. コマンド)を参照してください。

(4) イベント取得フィルター（互換用）を設定する

イベントコンソールサービスがイベント基盤サービスからイベントを取得するときのフィルター条件を設定します。なお、ここで示す設定はイベント取得フィルター（互換用）を使用している場合だけ実施できません。

なお、イベント取得フィルター（互換用）を設定すると、統合監視 DB を使用してもイベント取得フィルター（互換用）が使用されます。

設定手順は、次のとおりです。なお、[システム環境設定] 画面を起動するには、JP1_Console_Admin 権限が必要です。また、業務グループの参照・操作制限を設定している場合、JP1 資源グループと JP1 権限レベルの組み合わせによっては操作できないことがあります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.1.4(2) JP1 ユーザーに対する JP1 資源グループと JP1 権限レベルの割り当て」を参照してください。

1. [イベントコンソール] 画面で [オプション] - [システム環境設定] を選択する。
[システム環境設定] 画面が表示されます。
2. [システム環境設定] 画面の [イベント取得条件] の [設定] ボタンをクリックする。
[イベント取得条件設定] 画面（互換用）が表示されます。

3. イベントサービスからイベントを取得するときのフィルター条件を設定する。

JP1/SES のイベントを [イベントコンソール] 画面に表示する場合は、[イベント取得条件設定] 画面（互換用）の [JP1/SES イベント] の [取得する] チェックボックスをチェックします。

JP1 イベントの重大度を指定する場合は、[イベント取得条件設定] 画面（互換用）の [重大度] チェックボックスをチェックしたあと、緊急、警戒、致命的、エラー、警告、通知、情報、デバッグの中から必要な項目をチェックします。[重大度] チェックボックスにチェックがない場合は、重大度が定義されているすべてのイベントが対象になります。

イベント ID を指定したい場合は、[イベント取得条件設定] 画面（互換用）の [イベント ID] チェックボックスをチェックしたあと、JP1 イベントの ID を指定します。複数のイベント ID を指定したい場合は、コンマで区切って指定します。

ここで設定した各条件は、「JP1/SES イベントとイベント ID の AND 条件」、または「重大度とイベント ID の AND 条件」としてイベントサービスに渡されます。

4. [OK] ボタンをクリックする。

[システム環境設定] 画面に戻ります。

5. [適用] ボタンをクリックする。

設定した内容が有効になります。

5.3 繰り返しイベントの監視抑止の設定

繰り返しイベントの監視抑止を使用するための手順を説明します。繰り返しイベントの監視抑止は、統合監視 DB を使用している場合に利用できます。統合監視 DB の設定方法については、次の個所を参照してください。

- Windows の場合
「[1.4.2 統合監視 DB の設定 \(Windows の場合\)](#)」
- UNIX の場合
「[2.4.2 統合監視 DB の設定 \(UNIX の場合\)](#)」

なお、繰り返しイベントの監視抑止を有効にすると、繰り返しイベントの集約表示が無効になります。

1. 繰り返しイベントの監視抑止を有効にする。

`jcoimdef -storm ON` を実行します。

`jcoimdef` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jcoimdef`」(1. コマンド) を参照してください。

2. JP1/IM - Manager を再起動する。

3. JP1/IM - View を再起動する。

繰り返しイベントの監視抑止が有効になります。

5.4 JP1 イベントの表示色の設定

イベント一覧に表示されるイベントの表示色を重大度ごとに設定できます。この設定は、システムカラー定義ファイルで定義したあと、[ユーザー環境設定] 画面からユーザーごとに有効にします。なお、イベントの表示色の設定は、システム単位です。ユーザー単位では設定できません。

JP1 イベントの表示色を設定する手順を次に示します。

1. システムカラー定義ファイル (systemColor.conf) を編集する。

システムカラー定義ファイルの定義内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「システムカラー定義ファイル (systemColor.conf)」(2. 定義ファイル) を参照してください。

2. [イベントコンソール] 画面で [オプション] - [ユーザー環境設定] を選択する。

[ユーザー環境設定] 画面が表示されます。

[ユーザー環境設定] 画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.24 [ユーザー環境設定] 画面」を参照してください。

3. カラーリング項目の [有効] チェックボックスをチェックする。[重要イベント] ページに表示色を設定したい場合は、[[重要イベント] ページを対象とする] ラジオボタンを選択する。

4. [OK] ボタンをクリックする。

設定した内容が有効になります。

5.5 自動アクションの設定

自動アクション機能を使用するための設定について説明します。

5.5.1 自動アクション機能の実行環境の設定

自動アクションの実行環境は、自動アクション環境定義ファイル (action.conf.update) を編集して設定します。自動アクション環境定義ファイルには、自動アクションを実行する標準ユーザーや、自動アクション機能で使用する正規表現などを記述します。

自動アクションの実行環境を設定する手順を次に示します。

1. モデルファイルをコピーして、定義ファイル名 (action.conf) にリネームしたあと、定義内容を編集する。

自動アクション実行環境の定義ファイルのモデルファイルをコピーして、リネームしたあと、定義ファイル (action.conf) を編集します。次を実施してください。

Windows の場合

```
cd Console パス
copy default¥action.conf.update conf¥action.conf
notepad conf¥action.conf
```

UNIX の場合

```
cd /etc/opt/jp1cons
cp -p default/action.conf.update conf/action.conf
vi conf/action.conf
```

自動アクション環境定義ファイルの定義内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「自動アクション環境定義ファイル (action.conf.update)」(2. 定義ファイル) を参照してください。

2. JP1/IM - Manager を停止する。
3. jbssetcnf コマンドを実行して定義を反映する。

Windows の場合

```
jbssetcnf Console パス¥conf¥action.conf
```

UNIX の場合

```
/opt/jp1base/bin/jbssetcnf /etc/opt/jp1cons/conf/action.conf
```

jbssetcnf コマンドを実行すると、JP1 共通定義情報へ自動アクション機能の実行環境の設定が反映されます。jbssetcnf コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

4. JP1/IM - Manager を起動する。

5.5.2 自動アクションの実行条件および実行内容の設定

自動アクションの実行条件および実行内容は、JP1/IM - View の GUI または定義ファイルで設定できます。それぞれの手順について説明します。

注意事項

11-10 以前のバージョンからセントラルコンソールをバージョンアップした場合、定義ファイルを更新する必要があります。

更新の手順については、「[1.19.7\(2\) 自動アクション定義ファイルの更新](#)」(Windows) または、「[2.18.11\(3\) 自動アクション定義ファイルの更新](#)」(UNIX) を参照してください。なお、11-10 以前のバージョンの定義ファイルを使用したい場合は、更新する必要はありません。

(1) JP1/IM - View の GUI を使って設定する

手順を次に示します。

1. [イベントコンソール] 画面で [オプション] – [自動アクション設定] を選択する。

[アクション設定] 画面が表示されます。

2. 設定する内容にあわせて [追加], [編集] または [削除] のボタンをクリックする。

新規に自動アクションを設定したい場合

[追加] ボタンをクリックします。[アクション詳細設定] 画面で、自動アクションの実行条件や実行内容を設定します。

[OK] ボタンをクリックすると、[アクション設定] 画面に戻ります。

既存の自動アクションの条件を変更したい場合

一覧から変更したい自動アクションを選択して [編集] ボタンをクリックします。[アクション詳細設定] 画面で、既存の自動アクションの実行条件や実行内容を変更します。

[OK] ボタンをクリックすると、[アクション設定] 画面に戻ります。

既存の自動アクションの条件を削除したい場合

一覧から削除したい自動アクションを選択して [削除] ボタンをクリックします。

3. 設定した自動アクションの条件を無効にしたい場合は、[適用] の各チェックボックスのチェックを外す。

4. [適用] ボタンをクリックする。

設定した内容が有効になります。

[アクション設定] 画面の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「[3.32 \[アクション設定\] 画面](#)」を参照してください。

[アクション詳細設定] 画面の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「[3.33.1 \[アクション詳細設定\] 画面](#)」を参照してください。

(2) 定義ファイルを編集して設定する

手順を次に示します。

1. 自動アクション定義ファイル (actdef.conf) を編集する。

自動アクション定義ファイルの格納先を次に示します。

表 5-1 自動アクション定義ファイルの格納先

OS	格納先
Windows	物理ホストのとき Console パス¥conf¥action¥
	論理ホストのとき 共有フォルダ¥jp1cons¥conf¥action¥
UNIX	物理ホストのとき /etc/opt/jp1cons/conf/action/
	論理ホストのとき 共有ディレクトリ/jp1cons/conf/action/

自動アクション定義ファイルの内容に不正がないか確認したい場合は、jcamakea コマンドを実行してください。

2. 編集した内容を有効にする。

自動アクション定義ファイルの編集内容を有効にするため、次のどれかを実施します。

- JP1/IM - Manager を再起動する。
- jcachange コマンドを実行する。
- JP1/IM - View の [アクション設定] 画面で [適用] ボタンをクリックする。

自動アクション定義ファイル (actdef.conf) の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「自動アクション定義ファイル (actdef.conf)」(2. 定義ファイル) を参照してください。

5.5.3 自動アクションの実行状況監視の設定

自動アクションの実行状況の監視には、状態監視および遅延監視があります。また、状態監視および遅延監視で異常を検知したときに JP1 イベントを発行したり、通知コマンドを実行したりして自動アクションの異常を通知できます。

それぞれの設定について説明します。

(1) 自動アクションの状態監視および遅延監視の設定

自動アクションの実行状況監視は、JP1/IM - View の GUI または定義ファイルで設定できます。

JP1/IM - View の GUI を使って設定する

状態監視は [アクション設定] 画面、遅延監視は [アクション詳細設定] 画面で設定します。なお、[アクション設定] 画面、[アクション詳細設定] 画面の詳細については、次を参照してください。

- マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.32 [アクション設定] 画面」を参照してください。
- マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.33.1 [アクション詳細設定] 画面」を参照してください。

定義ファイルを編集して設定する

状態監視、遅延監視のどちらも自動アクション定義ファイル (actdef.conf) を編集して設定します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「自動アクション定義ファイル (actdef.conf)」(2. 定義ファイル) を参照してください。

(2) 状態監視および遅延監視で異常を検知した場合の通知の設定

状態監視および遅延監視で異常を検知した場合の通知は、自動アクション通知定義ファイル (actnotice.conf) を編集して設定します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「自動アクション通知定義ファイル (actnotice.conf)」(2. 定義ファイル) を参照してください。

5.5.4 自動アクションの実行抑止の設定

自動アクションの実行抑止は、自動アクション一つ一つに対して設定します。実行抑止は、JP1/IM - View の GUI または定義ファイルで設定できます。

(1) JP1/IM - View の GUI を使って設定する

自動アクションの実行抑止は [アクション詳細設定] 画面で設定します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.33.1 [アクション詳細設定] 画面」を参照してください。

(2) 定義ファイルを編集して設定する

自動アクションの実行抑止は、自動アクション定義ファイル (actdef.conf) を編集して設定します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「自動アクション定義ファイル (actdef.conf)」(2. 定義ファイル) を参照してください。

5.5.5 メール送信の設定

JP1/IM - Manager のメール通知機能を使用するための設定の手順を示します。

1. 通信環境を設定する。

- メールサーバホストの名前解決

SMTP サーバ名および POP3 サーバ名のホスト名解決ができるように、次のどれかのファイルを設定します。

ファイルは、次の順序で参照されます。

- マネージャースト上の JP1/Base の jp1hosts ファイル
- マネージャースト上の JP1/Base の jp1hosts2 ファイル
- hosts ファイルまたは DNS

メールサーバの IP アドレスは、IPv4 アドレスだけを指定できます。

- ファイアウォールの設定

jimmail コマンドとメールサーバが SMTP/POP3 通信できるようにするため、ファイアウォールの通過方向を設定します。

ファイアウォールの設定の詳細については、「[9.3.1 ファイアウォールの基礎知識](#)」を参照してください。

2. 通知メールを定義する。

通知するメールを作成するために、jimmail コマンドのコマンドラインを定義します。

自動アクションに通知メールを定義する場合の例を次に示します。

```
jimmail.exe -to user@hitachi.com -s "[重大度:$EVSEV] 障害発生通知" -b "業務サーバで障害が発生しました。¥n---¥nイベントDB内通し番号=$EVSEQNO¥nイベント発生日時=$EVDATE $EVTIME¥nイベントID=$EVIDBASE¥n重大度=$EVSEV¥nプロダクト名=$EV"PRODUCT_NAME"¥nメッセージ=$EVMSG¥n---¥nFrom:IM-Mホスト($ACTHOST)"
```

jimmail コマンドの詳細については、「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimmail (Windows 限定)」(1. コマンド) を参照してください。

3. メール環境定義ファイルをテキストエディターで開く。

- 物理ホストのとき

Console パス¥conf¥mail¥jimmail.conf

- 論理ホストのとき

共有フォルダ¥JP1Cons¥conf¥mail¥jimmail.conf

4. メール環境定義ファイルに次の表に示す項目を設定する。

パラメーター名	設定項目	設定要否	説明
Charset	メールの文字コード	△	指定できる文字コードの例は次のとおりです。 • iso-2022-jp • shift_jis • euc-jp • utf-8 • iso-8859-1 • us-ascii • GB18030 初期値はiso-8859-1 です。
From	送信元メールアドレス	○	1～256 バイトの範囲で 1 件だけ指定します。 使用できる文字は次のとおりです。 • 0-9, a-z (半角英数字) • @ (アットマーク) • . (ピリオド) • - (ハイフン) • _ (アンダースコア)
DefaultTo	デフォルトの送信先メールアドレス	△	デフォルトで送信するメールアドレスを指定します。jimmial コマンドで -to オプションが指定された場合、-to オプションが優先されます。
SmtServer	SMTP サーバのホスト名	○	メール送信時に接続する SMTP サーバのホスト名または IP アドレスを指定します。IPv4 だけに対応します。SMTP サーバは複数指定できません。
SmtPort	SMTP ポート番号	△	SMTP サーバの通信ポートのポート番号を指定します。 AuthMethod で「NONE」または、「POP」を指定した場合だけ、この項目は有効になります。 初期値は 25 です。
AuthMethod	メール送信時の認証方式	○	メール送信時の認証方式を指定します。 • NONE：認証なし • POP：POP before SMTP 認証 • SMTP：SMTP-AUTH 認証 (LOGIN/PLAIN) 初期値は「NONE」です。
SmtAuthPort	SMTP-AUTH 認証のサブミッションポート番号	△	SMTP-AUTH 認証用の通信ポートのサブミッションポート番号を指定します。 AuthMethod で「SMTP」を指定した場合だけ、この項目は有効になります。

5. セントラルコンソールの設定

パラメーター名	設定項目	設定要否	説明
			1～65535 の範囲で指定します。初期値は 587 です。
Pop3Server	POP3 サーバのホスト名	△	POP before SMTP 認証の場合、必須です。 POP before SMTP 認証で使用する POP3 サーバのホスト名または IP アドレスを指定します。IPv4 だけに対応します。複数指定できません。
Pop3Port	POP3 ポート番号	△	POP before SMTP 認証で使用する POP3 サーバの通信ポートのポート番号を指定します。 1～65535 の範囲で指定します。初期値は 110 です。
AuthUser	認証アカウント名	△	POP before SMTP 認証または SMTP-AUTH 認証で使用する認証アカウント名を指定します。1～255 バイトの半角文字で指定します。
AuthPassword	認証パスワード	△	手順 5 の jimmailpasswd コマンドで設定した値が暗号化されて入ります。
ConnectTimeout	ネットワーク接続タイムアウト時間	△	SMTP と POP3 サーバとの接続完了を待つタイムアウト時間を 1,000～3,600,000（ミリ秒）の範囲で指定します。初期値は 10,000（ミリ秒）（10 秒）です。
SoTimeout	通信タイムアウト時間	△	SMTP と POP3 サーバからの応答を受信するまでのタイムアウト時間を 1,000～3,600,000（ミリ秒）の範囲で指定します。初期値は 10,000（ミリ秒）（10 秒）です。
MailSubjectCutting	メール主題の切り捨て設定	△	メール送信時にメール主題が最大長を超えていた場合にメールの主題を切り捨てて強制的に送信するかを指定します。 • OFF：主題を切り捨てないで、異常終了 • ON：主題を 512 バイトで切り捨てて、メール送信 初期値は「OFF」です。
MailNewLine	メールの改行コード	△	メール本文で使用する改行コードを定義します。 • CRLF：CR（0x0d）+LF（0x0A） • LF：LF（0x0A） • CR：CR（0x0d） 初期値は「CRLF」です。

（凡例）

- ：必須
- △：任意

メール環境定義ファイルの詳細については、「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「メール環境定義ファイル (jimmail.conf)」(2. 定義ファイル) を参照してください。

5. jimmailpasswd コマンドで認証パスワードを設定する。

メール環境定義ファイルのメール送信時の認証方式が「POP before SMTP 認証」、または「SMTP-AUTH 認証」の場合、jimmailpasswd コマンドで POP3 認証パスワード、または SMTP 認証パスワードをメール環境定義ファイルに設定します。

jimmailpasswd コマンドの詳細については、「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimmailpasswd (Windows 限定)」(1. コマンド) を参照してください。

6. メール送信のテストをする。

メール送信の環境が正しく設定されたか、jimmail コマンドを実行してメール送信のテストをします。コマンドプロンプト上で、テストメールを送信して、jimmail コマンドが正常終了すること、および送信先ユーザーがメールを受信できることを確認してください。

user@hitachi.com にメール送信する例を次に示します。

```
$ jimmail -to user@hitachi.com -s IMTestMail -b IMTestMail
```

5.6 関連イベント発行の設定

関連イベントを発行するために必要な設定項目を次に示します。

- 関連イベント発行機能の起動設定
- 関連イベント発行履歴ファイルのサイズおよび面数の設定
- 起動オプションの設定
- 関連イベント発行定義の作成および反映

5.6.1 関連イベント発行機能の起動設定

関連イベント発行機能を起動するための設定手順を次に示します。

1. 関連イベント発行機能の起動コマンドを実行する。

```
jcoimdef -egs ON
```

統合監視 DB を使用しない場合

JP1/IM - Manager の起動時に、関連イベント発行サービスが自動で起動するようになります。

統合監視 DB を使用する場合

JP1/IM - Manager の起動時に、イベント基盤サービスの関連イベント発行機能が自動で起動するようになります。

jcoimdef コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

5.6.2 関連イベント発行履歴ファイルのサイズおよび面数の設定

関連イベント発行履歴ファイルのサイズ、および面数を設定する手順について説明します。なお、デフォルトの設定で問題ない場合、ここで説明する手順を実施する必要はありません。

関連イベント発行履歴ファイルのサイズ、および面数のデフォルト値を次に示します。

表 5-2 関連イベント発行履歴ファイルのデフォルト値

項目	デフォルト値
サイズ	10 メガバイト
面数	3 面

サイズおよび面数を設定する手順を次に示します。

1. 関連イベント発行環境定義ファイルを作成する。

関連イベント発行環境定義ファイルは、任意のファイルで作成します。

関連イベント発行環境定義ファイルに記述するパラメーターや、設定できる値の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「関連イベント発行環境定義ファイル」(2. 定義ファイル)を参照してください。

なお、作成した関連イベント発行環境定義ファイルは、次に示すディレクトリに格納しておくことをお勧めします。

表 5-3 関連イベント発行環境定義ファイルを格納するディレクトリ

OS	格納先※
Windows	物理ホストのとき Console パス¥default¥
	論理ホストのとき 共有フォルダ¥jp1cons¥default¥
UNIX	物理ホストのとき /etc/opt/jp1cons/default/
	論理ホストのとき 共有ディレクトリ/jp1cons/default/

注※

関連イベント発行環境定義ファイルを上記のディレクトリに格納しておくことで、ほかの定義ファイルと同様に資料採取ツールで自動採取できます。

2. jbssetcnf コマンドを実行する。

作成した関連イベント発行環境定義ファイルを引数にして、jbssetcnf コマンドを実行します。

jbssetcnf コマンドを実行すると、JP1 共通定義情報へ関連イベント発行環境定義ファイルの設定が反映されます。jbssetcnf コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

3. jco_spmdd_reload コマンドを実行するか、JP1/IM - Manager を再起動する。

定義した内容が有効になります。jco_spmdd_reload コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jco_spmdd_reload」(1. コマンド)を参照してください。

5.6.3 関連イベント発行機能の起動オプションの設定

関連イベント発行機能の起動オプションを設定する手順を次に示します。

1. 関連イベント発行システムプロファイル (egs_system.conf) を編集する。

関連イベント発行システムプロファイル (egs_system.conf) については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「関連イベント発行システムプロファイル (egs_system.conf)」(2. 定義ファイル)を参照してください。

2. jco_spmd_reload コマンドを実行するか、JP1/IM - Manager を再起動する。
- 定義した内容が有効になります。
- jco_spmd_reload コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jco_spmd_reload」(1. コマンド) を参照してください。

5.6.4 関連イベント発行定義の作成および反映

関連イベント発行定義の作成および反映する手順を次に示します。

1. 関連イベント発行定義ファイルを作成する。
- 関連イベント発行定義ファイルは、任意のファイルで作成します。ただし、ファイル名、拡張子は次に従ってください。

表 5-4 関連イベント発行定義ファイルの命名規則

項目	規則
ファイル名	ファイル名に使用できる文字は、半角英数字とアンダースコア「_」だけです。
拡張子	拡張子は.conf としてください。

関連イベント発行定義ファイルに記述する定義内容の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「関連イベント発行定義ファイル」(2. 定義ファイル) を参照してください。

なお、作成した関連イベント発行定義ファイルは、次に示すディレクトリに格納しておくことをお勧めします。

表 5-5 関連イベント発行定義ファイルを格納するディレクトリ

OS	格納先※
Windows	物理ホストのとき Console パス¥conf¥evgen¥define¥
	論理ホストのとき 共有フォルダ¥jp1cons¥conf¥evgen¥define¥
UNIX	物理ホストのとき /etc/opt/jp1cons/conf/evgen/define/
	論理ホストのとき 共有ディレクトリ/jp1cons/conf/evgen/define/

注※

関連イベント発行定義ファイルを上記のディレクトリに格納しておくことで、ほかの定義ファイルと同様に資料採取ツールで自動採取できます。また、クラスタ運用時は実行系、待機系の動作を同じにするため、関連イベント発行定義ファイルを共有ディスク上に格納してください。

2. jcoegscheck コマンドを実行して、相関イベント発行定義に定義不正がないかどうか確認する。

jcoegscheck コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoegscheck」(1. コマンド)を参照してください。

3. jcoegschange コマンドを実行する。

定義した内容が有効になります。

なお、JP1/IM - Manager が停止中の場合、次回の起動時にjcoegschange コマンドで反映した定義内容が有効になります。

jcoegschange コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoegschange」(1. コマンド)を参照してください。

5.7 メモ情報の設定

ここでは、メモ情報の設定機能を有効にする手順について説明します。メモ情報を編集するには、JP1_Console_Admin 権限または JP1_Console_Operator 権限が必要です。

メモ情報は、すべてのユーザーが参照できます。

1. メモ情報の設定機能を有効にする。

`jcoimdef -memo ON` を実行します。

2. JP1/IM - Manager を再起動する。

`jcoimdef` コマンドに `-i` オプションを指定して実行すると、JP1/IM - Manager を再起動する必要はありません。

3. JP1/IM - View を再起動する。

メモ情報の設定が反映されます。

4. [ユーザー環境設定] 画面で「メモ」を表示項目に指定する。

[ユーザー環境設定] 画面の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.24 [ユーザー環境設定] 画面」を参照してください。

メモ情報の編集方法は、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「6.2.1 JP1 イベントのメモ情報を編集する」を参照してください。

5.8 イベントガイド情報の編集

イベントガイド情報は、システム監視中に問題が発生したときに、JP1 イベントの「イベント詳細」画面に表示する情報です。イベントガイド情報として、問題の調査事例、対策事例などを表示することで、システム管理者の負担を軽減できます。また、問題対策での実績や対処記録などを、運用ノウハウとして蓄積できます。

イベントガイド情報として表示する内容は、JP1/IM - Manager のホストにあるイベントガイド情報ファイルに設定します。

ここでは、イベントガイド情報の編集手順について説明します。

イベントガイド情報として設定する内容や、考え方、またイベントガイド機能については、下記を参照してください。

イベントガイド情報の編集、設定について

- イベントガイド機能について
参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.10 イベントガイド機能」
- イベントガイドの考え方について
参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「13.1.10 イベントガイドの検討」
- イベントガイド情報ファイルの書式について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベントガイド情報ファイル（jco_guide.txt）」（2. 定義ファイル）

5.8.1 イベントガイド情報の編集の手順

編集手順を次に示します。なお、イベントガイド情報ファイルを編集した場合は、「イベント詳細」画面を表示し直すことで、編集内容が更新されます。

- イベントガイド情報ファイルのサンプルファイル（sample_jco_guide_ja.txt または sample_jco_guide_en.txt）をコピーして、ファイル名を jco_guide.txt に変更する。
なお、イベントガイド情報ファイル（jco_guide.txt）は、次に示すイベントガイド情報ファイルのサンプルファイルと、同じディレクトリに格納してください。

表 5-6 イベントガイド情報ファイルのサンプルファイルのディレクトリ

OS	環境	サンプルファイルのディレクトリ
Windows	日本語	Console パス%conf%guide%sample_jco_guide_ja.txt
		共有フォルダ%conf%guide%sample_jco_guide_ja.txt

OS	環境	サンプルファイルのディレクトリ
UNIX	英語	Console パス¥conf¥guide¥sample_jco_guide_en.txt
		共有フォルダ¥conf¥guide¥sample_jco_guide_en.txt
	日本語	/etc/opt/jp1cons/conf/guide/sample_jco_guide_ja.txt
		共有ディレクトリ/jp1cons/conf/guide/sample_jco_guide_ja.txt
	英語	/etc/opt/jp1cons/conf/guide/sample_jco_guide_en.txt
		共有ディレクトリ/jp1cons/conf/guide/sample_jco_guide_en.txt

2. イベントガイド情報ファイル (jco_guide.txt) を編集する。

イベントガイド情報ファイルは、TXT 形式のファイルです。テキストエディターで開き、編集してください。なお、イベントガイド情報ファイルは JP1/IM - Manager の動作する言語コードで記述してください。

イベントガイドメッセージファイルを利用する場合は、テキストエディターなどを使ってイベントガイドメッセージファイルを作成してください。

3. イベントガイド情報の設定内容を有効にする。

イベントガイド情報ファイルは、JP1/IM - Manager をリロードまたは再起動したときに読み込まれます。

次のどちらかをしてください。

- jco_spmd_reload コマンドを実行して、JP1/IM をリロードする。
- JP1/IM - Manager を再起動する。

また、JP1/IM - View を再起動してください。

4. イベントガイド情報の読み込みが成功したことを確認する。

JP1/IM - Manager がイベントガイド情報ファイルを読み込むときに、イベントガイド情報ファイルに記述誤りがあるとエラーが発生します。統合トレースログを確認して、イベントガイド情報ファイルの読み込みが成功したことを確認してください。

表 5-7 統合トレースログのディレクトリ

OS	統合トレースログ
Windows	システムドライブ:¥Program Files¥Hitachi¥HNTRLib2¥spool¥※
UNIX	/var/opt/hitachi/HNTRLib2/spool/

注※ Windows の場合、「システムドライブ:¥Program Files」と表記している部分は、インストール時の OS 環境変数によって決定されるため、環境によって異なる場合があります。

- イベントガイド情報ファイルの読み込みが成功した場合
「KAVB1585-I」のメッセージが統合トレースログに出力されます。このメッセージが出力されていることを確認してください。
- イベントガイド情報ファイルの読み込みでエラーがあった場合

「KAVB1586-W」「KAVB1587-E」のメッセージが統合トレースログに出力されます。エラーが発生している場合は、メッセージの示すエラー要因を見直して修正してください。そのあと、再度 JP1/IM - Manager をリロードまたは再起動してください。

5.9 対処状況変更時の JP1 イベント発行の設定

JP1 イベントの対処状況変更による JP1 イベント（3F11）の発行は、対処状況イベント定義ファイル（`processupdate.conf`）で設定します。

1. 対処状況イベント定義ファイル（`processupdate.conf`）をテキストエディターなどで編集する。

2. JP1/IM - Manager を起動する。

起動後に設定内容が反映されます。

JP1 イベント発行の設定について

- 対処状況イベント定義ファイル（`processupdate.conf`）について

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「対処状況イベント定義ファイル（`processupdate.conf`）」（2. 定義ファイル）

5.10 固有の属性付加の設定

JP1 イベントに固有の属性を付加するための手順を説明します。

1. JP1/Base の属性付加設定ファイルにイベントの属性付加の定義を記述する。

属性付加設定ファイルには、属性を付加するための条件と条件成立時に付加する拡張属性を定義します。

属性付加条件の指定形式は、JP1/Base のイベントフィルターで指定します。

拡張属性名の先頭 7 バイトは「JP1ADD_」から始まる名称を指定します。

属性付加設定ファイルの詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

属性付加設定ファイルに設定する内容の例

```
# Event : Extended attribute adding setting
add
filter
# input Event-filter
B.ID IN 111
end-filter
# input Extended-attribute
E.JP1ADD_SYSTEMNAME SystemA
end-add
```

2. JP1/Base を起動, またはjevextreload コマンドを実行する。

```
jevextreload [-h イベントサーバ名] {-recv | -send}
```

属性付加設定ファイルが有効になります。

3. 拡張属性のE. JP1ADD_SYSTEMNAME を自動アクションや各種フィルターなどの条件にする。

なお、属性付加設定ファイル、およびjevextreload コマンドの詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

5.11 固有の拡張属性の表示および指定の設定

[イベントコンソール] 画面のイベント一覧や [イベント詳細] 画面に固有の拡張属性を任意の項目名で表示したり、イベント条件に固有の拡張属性を任意の項目名で指定したりするための設定手順を説明します。

1. イベント拡張属性定義ファイル（拡張ファイル）のファイル名を変更する。

JP1/IM - Manager をインストールすると、イベント拡張属性定義ファイル（拡張ファイル）のテンプレートとなるファイルが格納されます。イベント拡張属性定義ファイル（拡張ファイル）は、JP1/IM - Manager の動作言語ごとに定義します。該当する言語のファイル名から先頭の「template_」を削除して、ファイル名を変更します。

イベント拡張属性定義ファイル（拡張ファイル）の格納先を次に示します。

表 5-8 イベント拡張属性定義ファイル（拡張ファイル）の格納先

OS	格納先	
Windows	物理ホスト	Console パス¥conf¥console¥attribute¥extend
	論理ホスト	共有フォルダ¥JP1Cons¥conf¥console¥attribute¥extend
UNIX	物理ホスト	/etc/opt/jp1cons/conf/console/attribute/extend
	論理ホスト	共有ディレクトリ/jp1cons/conf/console/attribute/extend

動作言語ごとのファイル名と変更後のファイル名を次に示します。

表 5-9 イベント拡張属性定義ファイル（拡張ファイル）のファイル名

言語	格納されているファイル名	変更後のファイル名
日本語	template_extend_attr_ja.conf	extend_attr_ja.conf
英語	template_extend_attr_en.conf	extend_attr_en.conf
中国語	template_extend_attr_zh.conf	extend_attr_zh.conf

2. 拡張属性定義ファイル（拡張ファイル）を編集する。

JP1/IM - Manager のイベント拡張属性定義ファイル（拡張ファイル）に、固有の拡張属性の項目名を定義します。編集が必要なパラメーターを次に示します。

```
attr name="E.属性名", title="項目名";
```

定義例を次に示します。

```
@encode UTF-8
@file type="extended-attributes-definition", version="0300";
@define-block type="event-attr-def";
attr name="E.SYSTEM", title="システム名";
attr name="E.ROLE ", title="サーバ用途";
@define-block-end;
```

イベント拡張属性定義ファイル（拡張ファイル）の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベント拡張属性定義ファイル（拡張ファイル）」（2. 定義ファイル）を参照してください。

なお、JP1/IM には、イベント拡張属性定義ファイル（拡張ファイル）の記述内容をチェックするためのコマンド「jcoattrfcheck」が用意されています。このコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoattrfcheck」（1. コマンド）を参照してください。

3. jco_spmc_reload コマンドを実行して、イベント拡張属性定義ファイル（拡張ファイル）を JP1/IM - Manager に反映する。

JP1/IM - Manager が起動している場合は、jco_spmc_reload コマンドを実行して、イベント拡張属性定義ファイル（拡張ファイル）を JP1/IM - Manager に反映してください。JP1/IM - Manager が起動していない場合は、JP1/IM - Manager が起動するタイミングで反映されます。

jco_spmc_reload コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jco_spmc_reload」（1. コマンド）を参照してください。

4. JP1/IM - View から JP1/IM - Manager（セントラルコンソール）にログインする。

JP1/IM - View から JP1/IM - Manager（セントラルコンソール）にログインすると、JP1/IM - Manager に定義したイベント拡張属性定義ファイル（拡張ファイル）の内容が JP1/IM - View の画面に反映されます。JP1/IM - Manager にイベント拡張属性定義ファイル（拡張ファイル）を反映したタイミングで、JP1/IM - View を接続している場合は、JP1/IM - View の再起動が必要です。

なお、ここで設定した固有の拡張属性の項目名をイベント一覧に表示するには、[ユーザー環境設定] 画面で表示項目に追加する必要があります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「6.9.1 JP1 イベントの固有の拡張属性を表示する（固有の拡張属性表示）」を参照してください。

メモ

イベント拡張属性定義ファイル（拡張ファイル）に固有の拡張属性を定義した場合、イベントレポート出力で CSV 出力する際に、基本属性、共通の拡張属性、および IM 属性と同じように 1 件の固有の拡張属性に一つの列を割り当てて出力できます。1 件の固有の拡張属性に一つの列を割り当てて出力する機能を有効にするかどうかは、イベントレポート出力環境定義ファイル（evtreport.conf）のPROGRAM_SPECIFIC_EX_ATTR_COLUMN パラメーターで指定します。なお、新規にインストールした場合は有効です。10-50 以前からバージョンアップした場合は無効です。必要に応じて、イベントレポート出力環境定義ファイルを設定してください。

イベントレポート出力環境定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベントレポート出力環境定義ファイル（evtreport.conf）」（2. 定義ファイル）を参照してください。

5.12 ユーザー独自のイベント属性（拡張属性の固有情報）を表示する手順

ユーザー独自のイベント属性（拡張属性の固有情報）を表示するための作業手順を示します。

なお、JP1/IM で作業に入る前に、JP1/Base で独自イベントを発行できるようにするための作業が必要です。JP1/Base での独自イベントを発行できるようにする方法については、マニュアル「JP1/Base 関数リファレンス」を参照してください。

また、独自イベントは、JP1/Base で `jevsend` および `jevsendd` コマンドを使用して発行することもできます。その場合にも、イベント拡張属性定義ファイルの設定などが必要になることがあります。JP1/Base で `jevsend` および `jevsendd` コマンドを使用して独自イベントを発行できるようにする方法については、マニュアル「JP1/Base 運用ガイド」を参照してください。

JP1/IM での作業の流れは次のとおりです。

1. 定義ファイルを作成する。

JP1/IM - Manager がインストールされたマシン上に、次の定義ファイルを作成します。

- イベント拡張属性定義ファイル
表示したいユーザー独自のイベント属性を定義します。
- オブジェクトタイプ定義ファイル
ユーザー独自のイベント属性を JP1/IM - View の画面のどの表示項目に表示するかを定義します。

2. 定義ファイルを有効にする。

それぞれの作業の詳細を次項から説明します。例として次に示す JP1 イベントを仮定し、そのイベント属性を表示するための定義ファイルの作成方法を説明します。

例として取り上げる JP1 イベント

Windows 上で動作する「SAMPLE」という名称のアプリケーションが、起動・停止時に発行する開始イベントと異常終了イベントを例として取り上げます。

それぞれのイベントの詳細を次に示します。

表示する JP1 イベントの種類

- SAMPLE アプリケーションの開始時に発行される JP1 イベント（開始イベント）
イベント ID：0x00000001
メッセージ：「SAMPLE アプリケーションを開始します。」
- SAMPLE アプリケーションの異常終了時に発行される JP1 イベント（異常終了イベント）
イベント ID：0x00000002
メッセージ：「SAMPLE アプリケーションが異常終了しました。」

開始イベントのイベント属性定義（拡張属性(extattrs)）

SAMPLE アプリケーションの開始イベントには、次の属性が定義されています。

表 5-10 開始イベントの属性

属性の種別	項目	属性名	内容
基本属性	イベント ID	—	0x00000001
	メッセージ	—	「SAMPLE アプリケーションを開始します。」
拡張属性 (共通報)	重大度	SEVERITY	Notice
	ユーザー名	USER_NAME	SAMPLE_USER
	プロダクト名	PRODUCT_NAME	/COMPANY/APP1/ SAMPLE_PRODUCT (プロダクトの名称)
	オブジェクトタイプ	OBJECT_TYPE	SAMPLE
	オブジェクト名	OBJECT_NAME	SAMPLE_NAME
	登録名タイプ	ROOT_OBJECT_TYPE	ROOT_SAMPLE
	登録名	ROOT_OBJECT_NAME	ROOT_SAMPLE_NAME
	オブジェクト ID	OBJECT_ID	SAMPLE_ID
	事象種別	OCCURRENCE	START
	開始時刻	START_TIME	SAMPLE アプリケーションの開始時刻。UTC 1970 年 1 月 1 日 00:00:00 からの秒数。
	プラットフォーム種別	PLATFORM	NT
	バージョン情報	ACTION_VERSION	0600
拡張属性 (固有情報)	SAMPLE 共通属性 1	COMMON_ATTR1	NATIVE
	SAMPLE 共通属性 2	COMMON_ATTR2	TRUE
	SAMPLE 開始属性 1	START_ATTR1	SAMPLE1
	SAMPLE 開始属性 2	START_ATTR2	SAMPLE2

(凡例)

—：なし

異常終了イベントのイベント属性定義 (拡張属性(extattrs))

SAMPLE アプリケーションの異常終了イベントには、次の属性が定義されています。

表 5-11 異常終了イベントの属性

属性の種別	項目	属性名	内容
基本属性	イベント ID	—	0x00000002
	メッセージ	—	「SAMPLE アプリケーションが異常終了しました。」

属性の種別	項目	属性名	内容
拡張属性 (共通情報)	重大度	SEVERITY	Error
	ユーザー名	USER_NAME	SAMPLE_USER
	プロダクト名	PRODUCT_NAME	/COMPANY/APP1/ SAMPLE_PRODUCT (プロダクトの名称)
	オブジェクトタイプ	OBJECT_TYPE	SAMPLE
	オブジェクト名	OBJECT_NAME	SAMPLE_NAME
	登録名タイプ	ROOT_OBJECT_TYPE	ROOT_SAMPLE
	登録名	ROOT_OBJECT_NAME	ROOT_SAMPLE_NAME
	オブジェクト ID	OBJECT_ID	SAMPLE_ID
	事象種別	OCCURRENCE	END
	終了時刻	END_TIME	SAMPLE アプリケーションの終了時刻。UTC 1970 年 1 月 1 日 00:00:00 からの秒数。
	終了コード	RESULT_CODE	SAMPLE アプリケーション終了時の終了コード
	プラットフォーム種別	PLATFORM	NT
	バージョン情報	ACTION_VERSION	0600
拡張属性 (固有情報)	SAMPLE 共通属性 1	COMMON_ATTR1	NATIVE
	SAMPLE 共通属性 2	COMMON_ATTR2	TRUE
	SAMPLE 終了属性 1	END_ATTR1	SAMPLE1
	SAMPLE 終了属性 2	END_ATTR2	SAMPLE2

(凡例)

ー：なし

5.12.1 定義ファイルを作成する

ユーザー独自のイベント属性を表示する際、イベント拡張属性定義ファイルおよびオブジェクトタイプ定義ファイルを作成する必要があります。ここでは、それぞれのファイルについて説明します。

(1) イベント拡張属性定義ファイル

イベント拡張属性定義ファイルでは、表示したい独自イベントに設定されているイベント属性のうち、詳細情報として表示したいイベント属性だけを定義します。基本属性、および拡張属性の共通情報部分は自

動的に設定されるため、定義の必要はありません。固有情報部分だけを定義します。イベント拡張属性定義ファイルの格納先を次に示します。

Windows の場合

Console パス¥conf¥console¥attribute¥

クラスタ運用の場合は、**共有フォルダ¥jp1cons¥conf¥console¥attribute¥**となります。

UNIX の場合

/etc/opt/jp1cons/conf/console/attribute/

クラスタ運用の場合は、**共有ディレクトリ/jp1cons/conf/console/attribute/**となります。

定義の反映時期

JP1/IM - Manager を再起動したあとに有効になります。

イベント拡張属性定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベント拡張属性定義ファイル」(2. 定義ファイル) を参照してください。

なお、JP1/IM には、イベント拡張属性定義ファイルの記述内容をチェックするためのコマンド「jcoattrfcheck」が用意されています。このコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoattrfcheck」(1. コマンド) を参照してください。

定義例

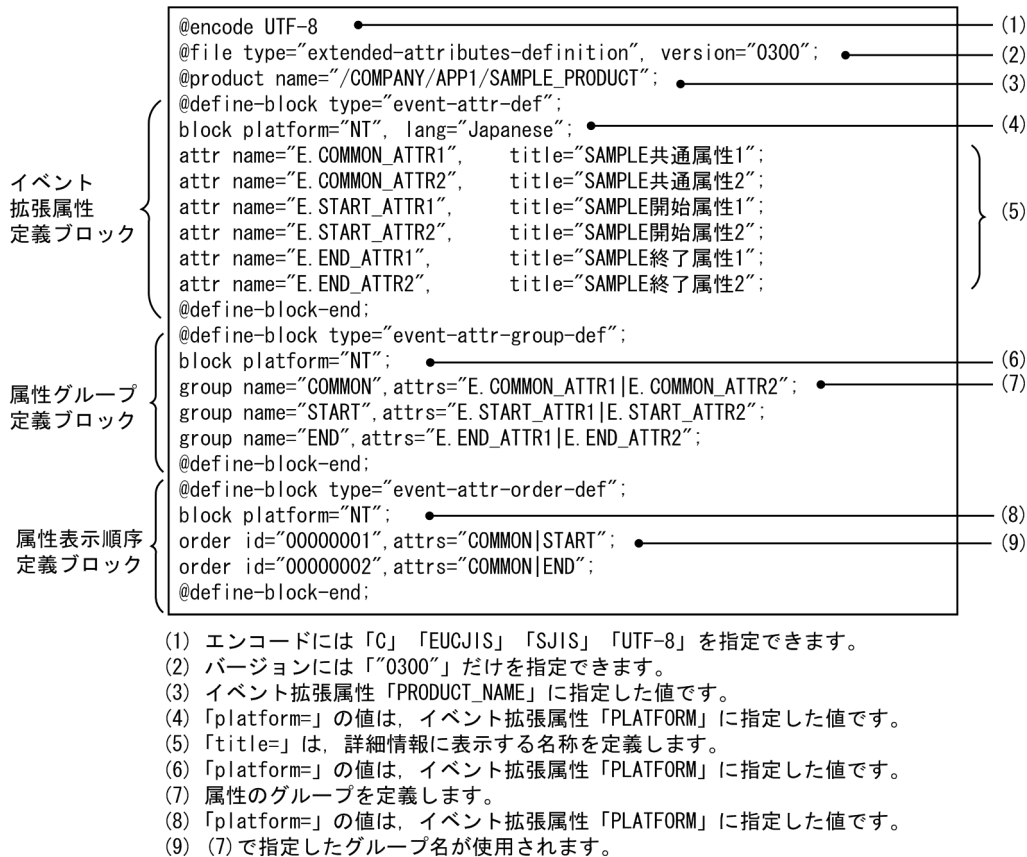
前述の「SAMPLE」というアプリケーションが発行する独自イベントについてイベント拡張属性定義ファイルに定義をする例を示します。この定義ファイルでは、一つのアプリケーションが発行するすべての JP1 イベントの属性をまとめて定義します。この例では、SAMPLE アプリケーションが発行するイベント ID 00000001 および 00000002 の JP1 イベントの属性をまとめて記述してあります。

この例では次のファイル名を使用します。

company_sample_attr_ja.conf

このファイル名は、「company」という会社の SAMPLE アプリケーションであることを表します。イベント拡張属性定義ファイルの定義例を次に示します。

図 5-1 イベント拡張属性定義ファイルの定義例



(2) オブジェクトタイプ定義ファイルの作成

オブジェクトタイプ定義ファイルには、表示したい独自イベントの拡張属性値、および JP1/IM - View の画面（[重要イベント定義] 画面，[イベント取得条件設定] 画面など）の [オブジェクトタイプ] および [登録名タイプ] に表示される項目を定義します。この定義ファイルは、JP1 イベントの詳細情報を表示するために必要です。オブジェクトタイプ定義ファイルの格納先を次に示します。

Windows の場合

Console パス¥conf¥console¥object_type¥

クラスタ運用の場合は、共有フォルダ¥jp1cons¥conf¥console¥object_type¥となります。

UNIX の場合

/etc/opt/jp1cons/conf/console/object_type/

クラスタ運用の場合は、共有ディレクトリ/jp1cons/conf/console/object_type/となります。

反映時期

JP1/IM - View を再起動したあとに有効になります。

オブジェクトタイプ定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「オブジェクトタイプ定義ファイル」(2. 定義ファイル) を参照してください。

定義例

前述の「SAMPLE」というアプリケーションが発行する独自イベントについてオブジェクトタイプ定義ファイルに定義をする例を示します。この例では、ROOT_OBJECT_TYPE と OBJECT_TYPE に新しい定義を追加しているので、オブジェクト定義ファイルに定義する必要があります。

この例では次のファイル名を使用します。

company_sample_obj. ja

このファイル名は、「company」という会社の SAMPLE アプリケーションであることを表します。オブジェクトタイプ定義ファイルの定義例を次に示します。

```
[ObjectType]
# 拡張属性値, リスト表示文字列, コメント
ROOT_SAMPLE, ROOT_SAMPLE //サンプルのルートオブジェクト名
SAMPLE, SAMPLE //サンプルのオブジェクト名
[End]
```

5.12.2 定義ファイルを有効にする

定義ファイルが有効になる契機は、ファイルによって異なります。有効になる契機を次に示します。

表 5-12 定義ファイルが有効になる契機

定義ファイル名	有効になる契機
イベント拡張属性定義ファイル	jco_spmd_reload コマンドの実行時，または JP1/IM - Manager の再起動時
オブジェクトタイプ定義ファイル	JP1/IM - View の再起動時

5.13 重大度変更機能の設定

重大度変更機能を設定するための手順を説明します。なお、重大度変更機能は、統合監視 DB を使用する
場合の機能です。手順を次に示します。

5.13.1 [重大度変更定義設定] 画面から設定する手順

(1) 重大度変更定義を新規に作成する

重大度変更定義を新規に作成する手順を次に示します。

1. イベントの重大度変更機能が有効になっていることを確認する。

jcoimdef コマンドを実行し、-chsev オプションを確認してください。無効になっている場合は、
jcoimdef コマンドを使用し、イベントの重大度変更機能を有効にしてください。デフォルトは無効で
す。重大度変更機能を有効にした場合は、JP1/IM - Manager を再起動してください。jcoimdef コマ
ンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・
API リファレンス」の「jcoimdef」(1. コマンド)を参照してください。

2. [イベントコンソール] 画面から [オプション] - [重大度変更定義] を選択する。

[重大度変更定義一覧] 画面が表示されます。

3. 新規に作成する場合は [追加] ボタンをクリック、既存の重大度変更定義を流用する場合は [複製] ボ
タンをクリックしたあと [編集] ボタンをクリックする。

[追加] ボタンをクリックすると、[重大度変更定義設定] 画面が表示されます。

[複製] ボタンをクリックすると、「コピー 重大度変更定義名」がフィルターに追加されます。この場
合は「コピー 重大度変更定義名」を選択し、[編集] ボタンをクリックして [重大度変更定義設定] 画
面を表示します。

4. [重大度変更定義設定] 画面で、重大度の設定をする。

重大度を変更するイベント条件の設定をします。そのあと、[変更後の重大度] から変更後の重大度を
選択して、[OK] ボタンをクリックします。

5. [重大度変更定義一覧] 画面で、[適用] ボタンをクリックして有効にする。

[重大度変更定義設定] 画面で設定した重大度変更定義を、[重大度変更定義一覧] 画面から選択して、
[適用] チェックボックスをチェックして有効にします。複数の重大度変更定義を設定したい場合は、
手順 3~5 を繰り返します。

6. 確認のダイアログボックスで [はい] ボタンをクリックする。

(2) 重大度変更定義を変更する

既存の重大度変更定義の内容を変更する手順を次に示します。

1. イベントの重大度変更機能が有効になっていることを確認する。

jcoimdef コマンドを実行し、-chsev オプションを確認してください。無効になっている場合は、jcoimdef コマンドを使用し、イベントの重大度変更機能を有効にしてください。デフォルトは無効です。重大度変更機能を有効にした場合は、JP1/IM - Manager を再起動してください。jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド)を参照してください。

2. [イベントコンソール] 画面の [オプション] - [重大度変更定義] を選択する。

[重大度変更定義一覧] 画面が表示されます。

3. [重大度変更定義一覧] 画面で変更したい重大度変更定義を選択して、[編集] ボタンをクリックする。

[重大度変更定義設定] 画面が表示されます。

4. [重大度変更定義設定] 画面で、重大度を変更する。

重大度を変更するイベント条件の設定をします。そのあと、[変更後の重大度] から変更後の重大度を選択して、[OK] ボタンをクリックします。

5. [重大度変更定義一覧] 画面で、[適用] チェックボックスをチェックして有効にする。

[重大度変更定義設定] 画面で、設定した重大度変更定義を [重大度変更定義一覧] 画面から選択して、[適用] チェックボックスをチェックして有効にします。

複数のイベントを設定したい場合は、手順 3~5 を繰り返します。

6. 確認のダイアログボックスで [はい] ボタンをクリックする。

(3) 重大度変更定義を削除する

既存の重大度変更定義を削除する手順を次に示します。

1. イベントの重大度変更機能が有効になっていることを確認する。

jcoimdef コマンドを実行し、-chsev オプションを確認してください。無効になっている場合は、jcoimdef コマンドを使用し、イベントの重大度変更機能を有効にしてください。デフォルトは無効です。重大度変更機能を有効にした場合は、JP1/IM - Manager を再起動してください。jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド)を参照してください。

2. [イベントコンソール] 画面の [オプション] - [重大度変更定義] を選択する。

[重大度変更定義一覧] 画面が表示されます。

3. [重大度変更定義一覧] 画面で削除したい重大度変更定義を選択して、[削除] ボタンをクリックする。

選択した重大度変更定義が削除されます。

4. 確認のダイアログボックスで [はい] ボタンをクリックする。

5.13.2 重大度変更定義ファイルから設定する手順

1. イベントの重大度変更機能が有効になっていることを確認する。

jcoimdef コマンドを実行し、-chsev オプションを確認してください。無効になっている場合は、jcoimdef コマンドを使用し、イベントの重大度変更機能を有効にしてください。デフォルトは無効です。重大度変更機能を有効にした場合は、JP1/IM - Manager を再起動してください。jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド)を参照してください。

2. 重大度変更定義ファイルを編集する。

編集する内容については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「6.9.4 JP1 イベントの重大度を変更する」を参照してください。

3. jco_spmd_reload コマンドを実行するか、JP1/IM - Manager を再起動する。

手順 1 で重大度変更機能を無効から有効に変更した場合は、JP1/IM - Manager を再起動する必要があります。

重大度変更機能が有効になっている状態で、重大度変更定義ファイルを編集した場合は、jco_spmd_reload コマンドを実行することで定義を反映できます。jco_spmd_reload コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jco_spmd_reload」(1. コマンド)を参照してください。

5.14 表示メッセージ変更機能の設定

表示メッセージ変更機能を設定するための手順を説明します。なお、表示メッセージ変更機能は、統合監視 DB を使用する場合の機能です。

表示メッセージ変更機能を設定する方法には、GUI で設定する方法と、表示メッセージ変更定義ファイルで定義し、jco_spmd_reload コマンドを実行して設定を反映する方法があります。

❗ 重要

ただし、GUI からの設定と定義ファイルからの設定を同時にしないでください。GUI からの定義を更新中にユーザーがテキストエディターなどでファイルを更新した場合に、定義ファイルとメモリーに持っているデータが不一致になることがあります。

それぞれの手順を次に示します。

5.14.1 [表示メッセージ変更定義設定] 画面から設定する手順

(1) 表示メッセージ変更定義を新規に作成する

表示メッセージ変更定義を新規に作成する手順を次に示します。

1. イベントの表示メッセージ変更機能が有効になっていることを確認する。

[イベントコンソール] 画面で [オプション] - [表示メッセージ変更定義] が表示されるかどうかを確認してください。表示されない場合、統合監視 DB を有効にすると表示メッセージ変更機能が有効になります。表示メッセージ変更機能を有効にした場合は、JP1/IM - Manager を再起動してください。また、10-50 以前からバージョンアップインストール後に、jimdbupdate コマンドで IM データベースを更新していない場合は、IM データベースを更新してください。jimdbupdate コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimdbupdate」(1. コマンド) を参照してください。

2. [イベントコンソール] 画面から [オプション] - [表示メッセージ変更定義] を選択する。

[表示メッセージ変更定義一覧] 画面が表示されます。

3. 新規に作成する場合は [追加] ボタンをクリック、既存の表示メッセージ変更定義を流用する場合は [複製] ボタンをクリックしたあと [編集] ボタンをクリックする。

[追加] ボタンをクリックすると、[表示メッセージ変更定義設定] 画面が表示されます。

[複製] ボタンをクリックすると、「コピー 複製元の表示メッセージ変更定義名」がフィルターに追加されます。この場合は「コピー 複製元の表示メッセージ変更定義名」を選択し、[編集] ボタンをクリックして [表示メッセージ変更定義設定] 画面を表示します。

4. [表示メッセージ変更定義設定] 画面で、表示メッセージ変更の設定をする。

表示メッセージを変更するイベント条件の設定をします。そのあと、[表示変更後のメッセージ] で変更後のメッセージの形式を設定します。イベント引き継ぎ情報の変換機能を指定すると、メッセージの文字や数値の表示形式を見やすく統一できます。イベント引き継ぎ情報の変換機能の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「表示メッセージ変更定義ファイル (jcochmsg.conf)」(2. 定義ファイル) を参照してください。設定後に [OK] ボタンをクリックします。

5. [表示メッセージ変更定義一覧] 画面で、[適用] ボタンをクリックして有効にする。

[表示メッセージ変更定義設定] 画面で設定した表示メッセージ変更定義を、[表示メッセージ変更定義一覧] 画面から選択して、[適用] チェックボックスをチェックして有効にします。複数の表示メッセージ変更定義を設定したい場合は、手順 3～5 を繰り返します。

6. 確認のダイアログボックスで [はい] ボタンをクリックする。

(2) 表示メッセージ変更定義を変更する

既存の表示メッセージ変更定義の内容を変更する手順を次に示します。

1. イベントの表示メッセージ変更機能が有効になっていることを確認する。

[イベントコンソール] 画面で [オプション] - [表示メッセージ変更定義] が表示されるかどうかを確認してください。表示されない場合、統合監視 DB を有効にすると表示メッセージ変更機能が有効になります。表示メッセージ変更機能を有効にした場合は、JP1/IM - Manager を再起動してください。

2. [イベントコンソール] 画面の [オプション] - [表示メッセージ変更定義] を選択する。

[表示メッセージ変更定義一覧] 画面が表示されます。

3. [表示メッセージ変更定義一覧] 画面で変更したい表示メッセージ変更定義を選択して、[編集] ボタンをクリックする。

[表示メッセージ変更定義設定] 画面が表示されます。

4. [表示メッセージ変更定義設定] 画面で、表示メッセージを変更する。

表示メッセージを変更するイベント条件の設定をします。そのあと、[表示変更後のメッセージ] で変更後のメッセージの形式を設定します。イベント引き継ぎ情報の変換機能を指定すると、メッセージの文字や数値の表示形式を見やすく統一できます。イベント引き継ぎ情報の変換機能の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「表示メッセージ変更定義ファイル (jcochmsg.conf)」(2. 定義ファイル) を参照してください。設定後に [OK] ボタンをクリックします。

5. [表示メッセージ変更定義一覧] 画面で、[適用] チェックボックスをチェックして有効にする。

[表示メッセージ変更定義設定] 画面で設定した表示メッセージ変更定義を、[表示メッセージ変更定義一覧] 画面から選択して、[適用] チェックボックスをチェックして有効にします。複数のイベントを設定したい場合は、手順 3～5 を繰り返します。

6. 確認のダイアログボックスで [はい] ボタンをクリックする。

(3) 表示メッセージ変更定義を削除する

既存の表示メッセージ変更定義を削除する手順を次に示します。

1. イベントの表示メッセージ変更機能が有効になっていることを確認する。

「イベントコンソール」画面で「オプション」－「表示メッセージ変更定義」が表示されるかどうかを確認してください。表示されない場合、統合監視 DB を有効にすると表示メッセージ変更機能が有効になります。表示メッセージ変更機能を有効にした場合は、JP1/IM - Manager を再起動してください。

2. 「イベントコンソール」画面の「オプション」－「表示メッセージ変更定義」を選択する。

「表示メッセージ変更定義一覧」画面が表示されます。

3. 「表示メッセージ変更定義一覧」画面で削除したい表示メッセージ変更定義を選択して、「削除」ボタンをクリックする。

選択した表示メッセージ変更定義が削除されます。

4. 確認のダイアログボックスで「はい」ボタンをクリックする。

5.14.2 表示メッセージ変更定義ファイルから設定する手順

1. イベントの表示メッセージ変更機能が有効になっていることを確認する。

「イベントコンソール」画面で「オプション」－「表示メッセージ変更定義」が表示されるかどうかを確認してください。表示されない場合、統合監視 DB を有効にすると表示メッセージ変更機能が有効になります。表示メッセージ変更機能を有効にした場合は、JP1/IM - Manager を再起動してください。また、10-50 以前からバージョンアップインストール後に、jimdbupdate コマンドで IM データベースを更新していない場合は、IM データベースを更新してください。jimdbupdate コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimdbupdate」(1. コマンド)を参照してください。

2. 表示メッセージ変更定義ファイルを編集する。

編集する内容については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「6.9.5(2) 表示メッセージ変更定義ファイルから表示メッセージ変更定義を設定する」を参照してください。

3. jco_spmc_reload コマンドを実行するか、JP1/IM - Manager を再起動する。

表示メッセージ変更機能が有効になっている状態で、表示メッセージ変更定義ファイルを編集した場合は、jco_spmc_reload コマンドを実行することで定義を反映できます。jco_spmc_reload コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jco_spmc_reload」(1. コマンド)を参照してください。

4. JP1/IM - View から JP1/IM - Manager (セントラルコンソール) にログインする。

JP1/IM - View から JP1/IM - Manager（セントラルコンソール）にログインすると、JP1/IM - Manager に定義した表示メッセージ変更定義ファイルの内容が JP1/IM - View の画面に反映されます。JP1/IM - View を接続して、[表示メッセージ変更定義設定] 画面、または [表示メッセージ変更定義一覧] 画面を表示中に、表示メッセージ変更定義ファイルを反映した場合は、[表示メッセージ変更定義設定] 画面では [キャンセル] ボタン、[表示メッセージ変更定義一覧] 画面では [閉じる] ボタンで閉じて、再度画面を開いてください。

5.14.3 表示メッセージ変更後のイベントを発行する手順

表示メッセージ変更後イベントを発行するための設定手順を次に示します。

1. 表示メッセージ変更後イベント環境定義ファイルを編集する。

"SEND_CHANGE_MESSAGE_EVENT"=dword:に「00000001」を指定します。

表示メッセージ変更後イベント環境定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「表示メッセージ変更後イベント環境定義ファイル (chmsgevent.conf)」(2. 定義ファイル) を参照してください。

2. jbssetcnf コマンドを実行する。

JP1/Base の jbssetcnf コマンドで、表示メッセージ変更後イベント環境定義ファイルの内容を JP1 共通定義情報に反映します。jbssetcnf コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

3. JP1/IM - Manager を再起動する。

表示メッセージ変更後にイベントが発行されるようになります。なお、表示メッセージ変更後にイベントを発行する場合は、イベントを再取得しないように、イベント取得フィルターでイベント ID が 00006400 のイベントを除外条件に設定してください。イベント取得フィルターの詳細については、[「5.2.4 イベント取得フィルターを設定する」](#)を参照してください。

5.15 発生元ホストのマッピングの設定

発生元ホストをマッピングするための手順を説明します。発生元ホストのマッピングは、統合監視 DB を使用している場合に利用できます。

発生元ホストのマッピングを設定する手順を次に示します。

1. 発生元ホストのマッピングを有効にする。

```
jcoimdef -hostmap ON
```

jcoimdef コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド)を参照してください。

2. 発生元ホストマッピング定義ファイルを編集する。※

発生元ホストマッピング定義ファイルを編集します。この定義ファイルには、1,000 個まで定義を指定できます。

なお、発生元ホストのマッピングを有効にすると次の表の JP1 イベントが自動的にマッピングされます。次の表以外の JP1 イベントについては個別に設定する必要があります。また、発生元ホストマッピング定義ファイルに次の表に該当するイベントを定義しても、次の表のマッピングが優先されます。

表 5-13 マッピングされる JP1 イベント

項番	製品名	マッピングされる JP1 イベント	マッピング元の属性名	備考
1	JP1/Base	イベント ID が 3A71、拡張属性「E.PPNAME」が「/HITACHI/JP1/NTEVENT_LOGTRAP」と一致する JP1 イベント	B.SOURCESERVER	共通定義設定用ファイル (JP1 イベントの属性変更) で JP1 イベントの属性変更が設定されている場合に、マッピングされます。
2		イベント ID が次の JP1 イベント • 3A71	E.A1	共通定義設定用ファイル (JP1 イベントの属性変更) で JP1 イベントの属性変更が設定されていない場合に、マッピングされます。
3		イベント ID が次の JP1 イベント • 3A80	E.SNMP_SOURCE	—
4	JP1/AJS2 および JP1/AJS3	イベント ID が次の JP1 イベント • 4105 • 4106 • 4107 • 4109 • 410A • 4125	E.C0	—

項番	製品名	マッピングされる JP1 イベント	マッピング元の属性名	備考
		• 4126 • 4127		
5	JP1/PFM	プロダクト名が次の JP1 イベント • /PFM/ALARM_EVENT • /HITACHI/JP1/PFM/ALARM_EVENT • /HITACHI/JP1/PFM/STATE_EVENT	E. JPC_AGENT	—
6		プロダクト名が次の JP1 イベント • /HITACHI/JP1/PFM	E. JPC_MGR	—
7	JP1/Cm2/SSO JP1/Cm2/NNM JP1/PFM/SSO - Agent for Process	イベント ID が次の JP1 イベント • 3A80	ホスト名が入っている次の属性のどれかがマッピングされます。 • E. SNMP_VARBIND1 • E. SNMP_VARBIND2 • E. SNMP_VARBIND3 • E. SNMP_VARBIND6 • E. SNMP_VARBIND12	—
8	JP1/PAM	プロダクト名が次の JP1 イベント • /HITACHI/JP1/PAM	E. PAM_HOSTNAME	—
9	JP1/SCIM	イベント ID が次の JP1 イベント • 432B • 432C	E. SCIM_AGENT_ADDR	—
10	Cosminexus	イベント ID が次の JP1 イベント • 12000 • 12080	E. HOST_NAME	—
11	JP1/ServerConductor	プロダクト名が次の JP1 イベント • /HITACHI/SYSTEM_MANAGER	E. HSM_SERVER	—
12	JP1/IM - EG for NNMi	イベント ID が次の JP1 イベント • 6100	E. NNMI_SRC_NODE_NAME	—
13	JP1/Console Agent for VOS3	• イベント ID が次の JP1 イベント	E. CIF_PNAM	—

項番	製品名	マッピングされる JP1 イベント	マッピング元の属性名	備考
		・ 11503 ・ 11504 ・ 11505 ・ 11506 ・ 11516 ・ 11520 ・ 11521 ・ 11522 ・ 11523 ・ 1159F ・ イベント ID が 11502, または 1150A で, オブジェクトタイプが「CPN」と一致する JP1 イベント		
14	JP1/NETM/DM	イベント ID が次の JP1 イベント ・ 10110 ・ 10112 ・ 10111 ・ 10410 ・ 10411 ・ 10412	E. A2	—
15		イベント ID が次の JP1 イベント ・ 10420 ・ 10421 ・ 10422	E. 03	—
16	JP1/IM - MO	イベント ID が次の JP1 イベント ・ 6400	E. EVTSRC_INFO	—
17	JP1/IM - Manager	イベント ID が次の JP1 イベント ・ 3A71	E. A1	—
18		イベント ID が次の JP1 イベント ・ 6400	E. EVTSRC_INFO	表示メッセージ変更後のイベントを発行する機能が有効の場合に発行される表示メッセージ変更後のイベントです。

(凡例)

— : なし

編集する内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「発生元ホストマッピング定義ファイル (user_hostmap.conf)」(2. 定義ファイル) を参照してください。

注※

リモート監視ログファイルトラップの場合は設定に関係なく、発生元ホスト名 (E. JP1_SOURCEHOST) が設定されます。このため、発生元ホストマッピング定義ファイルを編集する必要はありません。

3. JP1/IM - Manager を再起動する。

手順 1 で発生元ホストのマッピングを無効から有効に変更した場合は、JP1/IM - Manager を再起動する必要があります。

発生元ホストのマッピングを有効にしている状態で、発生元ホストマッピング定義ファイルを編集した場合は、jco_spmd_reload コマンドを実行することで定義を反映できます。

jco_spmd_reload コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jco_spmd_reload」(1. コマンド) を参照してください。

5.16 ログインユーザーごとの JP1/IM - View の設定

JP1/IM - Manager にログインする JP1 ユーザーごとに、JP1/IM - View の GUI 環境を設定します。ビューアーのメモリー上に JP1 イベントをバッファリングするバッファサイズや、イベントの表示項目などを設定できます。

5.16.1 JP1/IM - View の設定項目

必要に応じて設定をカスタマイズしてください。設定する項目を次に示します。

- 表示内容を自動更新するかどうか、および自動更新をする場合の更新間隔
表示できない JP1 イベントがある場合は、間隔を短くします。
- [イベントコンソール] 画面に表示できる JP1 イベントの数（スクロールバッファ）
表示できない JP1 イベントがある場合は、数を増やします。
使用するメモリー量を減らしたい場合は、数を減らします。
- [イベントコンソール] 画面の更新時のイベント取得件数
- 検索時のイベント取得件数
- イベント一覧の表示項目
イベント一覧の列に表示する項目を、追加・削除できます。

設定できる項目は、重大度、登録時刻、登録ホスト名、ユーザー名、メッセージ、オブジェクトタイプ、イベント ID、開始時刻、終了時刻、プロダクト名、オブジェクト名、登録名タイプ、登録名、到着時刻、アクション、事象種別、イベント DB 内通し番号、発行元プロセス ID、発行元ユーザー ID、発行元グループ ID、発行元ユーザー名、発行元グループ名、発行元イベント DB 内通し番号、種別、アクション種別、重大度(変更前)、重大度変更、メッセージ(変更後)、表示メッセージ変更、表示メッセージ変更定義名、発生元ホスト名、メモ、固有の拡張属性です。重大度変更機能が無効な場合、重大度(変更前)、重大度変更は表示できません。表示メッセージ変更機能が無効な場合、メッセージ(変更後)、表示メッセージ変更、表示メッセージ変更定義名は表示できません。またメモ情報の設定が無効な場合、メモは表示できません。発生元ホストのマッピングを有効にしていない場合は、発生元ホスト名が表示できません。固有の拡張属性は、イベント拡張属性定義ファイル（拡張ファイル）に定義した項目名が表示されます。

- [イベントコンソール] 画面で表示しているページの状態を保存するかどうか
[イベントコンソール] 画面で選択中のページ（[イベント監視] ページ、[重要イベント] ページ）の表示フィルター、および表示フィルターチェックボックスの状態を JP1/IM - View のログアウト時に保存し、ログイン時に復元するかどうかを設定できます。
- [イベントコンソール] 画面のイベント一覧に表示される項目の列幅を保存するかどうか
イベント一覧に表示される項目の列幅は、マウスでドラッグすることによって任意の幅に変更できます。一つのページ（例：[イベント監視] ページ）で列幅を変更すると、ほかの二つのページ（例：[重

要イベント] ページおよび [イベント検索] ページ) の列幅も変更されます。ログアウト時にそのときの列幅の大きさを保存するかどうかを設定できます。

- [イベントコンソール] 画面のイベント一覧の文字のフォントサイズ

イベント一覧に表示される文字のフォントサイズを 12~72 ポイントの範囲で変更できます。フォントサイズを大きくすると、大画面モニターを離れて見るような運用でも文字が見やすくなります。フォントサイズを変更できるのは、イベント一覧の [イベント監視] ページ, [重要イベント] ページおよび [イベント検索] ページに表示されるイベント一覧の文字です。

- [イベントコンソール] 画面のイベント一覧に表示される特定のイベントに背景色を付けるかどうか
[イベント監視] ページ, [重要イベント] ページおよび [イベント検索] ページに表示される特定のイベントに背景色が付くように設定できます。

背景色が付く対象となるイベントは、重大度が「緊急 (Emergency)」, 「警戒 (Alert)」, 「致命的 (Critical)」, 「エラー (Error)」, 「警告 (Warning)」, 「通知 (Notice)」, 「情報 (Information)」および「デバッグ (Debug)」のイベントです。

なお、イベントの文字色と背景色は、システムカラー定義ファイル (systemColor.conf) で変更できます。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「システムカラー定義ファイル (systemColor.conf)」(2. 定義ファイル) を参照してください。

- 繰り返しイベントを集約して表示するかどうか

繰り返しイベントの集約表示機能を使用して、短時間に大量に発生した同一内容のイベントを集約して [イベントコンソール] 画面に表示するかどうかを設定できます。

[集約表示] の [有効] チェックボックスをチェックして、集約中イベントのタイムアウト時間を設定してください。

[集約表示] の設定を変更する場合、設定が有効になったあと受信したイベントから新しい設定でイベント集約が開始されます。また、設定を変更したあと再ログインすると、新しい設定でイベント集約が開始されます。

なお、繰り返しイベントの監視抑止機能を有効にした場合、繰り返しイベントの集約表示機能は使用できません。

- [コマンド実行] 画面での実行結果表示行数
- 指定期間のイベント表示

5.16.2 JP1/IM - View の設定手順

設定は JP1/IM - View の [ユーザー環境設定] 画面を使用します。なお、ここで設定した内容は JP1/IM - Manager にログインする JP1 ユーザーごとに保持されます。手順を次に示します。

1. [ユーザー環境設定] 画面を起動する。

[イベントコンソール] 画面で [オプション] - [ユーザー環境設定] を選択します。

2. パラメーターを調整する。

必要に応じて、各パラメーターを調整してください。

設定できるパラメーターについては、次の説明を参照してください。

JP1 ユーザー環境の設定について

- [ユーザー環境設定] 画面について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.24 [ユーザー環境設定] 画面」

❗ 重要

ユーザープロファイルにも上記の設定についての定義内容が記述されていますが、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ユーザープロファイル (defaultUser | profile_ユーザー名)」の「記述内容」に記載がない属性および属性値についてはユーザープロファイルから直接変更しないでください。変更した場合、JP1/IM - View は正しく動作しないことがあります。

5.17 連携製品のモニター起動の設定

モニター起動とは、[イベントコンソール] 画面および[統合オペレーション・ビューアー] 画面に表示されている JP1 イベントから、その JP1 イベントに関連するアプリケーションの画面を起動する機能です。モニター起動によってほかの製品と連携する場合には、その製品の稼働環境（サポート OS やブラウザーなど）を事前に確認してください。

❗ 重要

連携製品によっては、連携製品側で定義ファイルを用意していることがあります。各製品がモニター起動に対応しているかどうかや設定手順の詳細については、各製品のマニュアルを参照して確認してください。

なお、連携製品側で提供している定義ファイルについても、配置先の JP1/IM - Manager が動作する文字コードを使用してください。

5.17.1 モニター画面を呼び出す手順

モニター画面呼び出しをするための作業手順を示します。作業の流れは次のとおりです。

1. モニター画面呼び出しをするための画面を決める。

2. 定義ファイルを作成する。

次の定義ファイルを作成します。

- モニター画面呼び出し定義ファイル

この定義ファイルでは、どの JP1 イベントが発行されたときにどの画面を呼び出すかを定義します。この定義ファイルは、JP1/IM - Manager がインストールされたマシン上に作成します。

この定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「モニター画面呼び出し定義ファイル」（2. 定義ファイル）を参照してください。

- アプリケーション実行定義ファイル

この定義ファイルでは、モニター画面呼び出し定義ファイルで定義されたアプリケーション実行定義識別子とパスの関連づけを定義します。この定義ファイルは、JP1/IM - View がインストールされたマシン上に作成します。

この定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「アプリケーション実行定義ファイル」（2. 定義ファイル）を参照してください。

3. `jco_spmd_reload` コマンドを実行して、モニター画面呼び出し定義ファイルを JP1/IM - Manager に反映する。

JP1/IM - Manager が起動している場合は、`jco_spmd_reload` コマンドを実行して、モニター画面呼び出し定義ファイルを JP1/IM - Manager に反映してください。JP1/IM - Manager が起動していない場合は、JP1/IM - Manager が起動するタイミングで反映されます。`jco_spmd_reload` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jco_spmd_reload`」(1. コマンド) を参照してください。

4. JP1/IM - View から JP1/IM - Manager (セントラルコンソール) にログインする。([イベントコンソール] 画面からモニター起動する場合)

JP1/IM - View を起動したタイミングで、アプリケーション実行定義ファイルの内容が JP1/IM - View に反映されます。また、JP1/IM - Manager にモニター画面呼び出し定義ファイルを反映したタイミングで、JP1/IM - View を接続している場合は、JP1/IM - View の再起動が必要です。

5. Web ブラウザーから JP1/IM - Manager (インテリジェント統合管理基盤) にログインする。([統合オペレーション・ビューアー] 画面からモニター起動する場合)

Web ブラウザーのアドレスバーに (URL 入力エリア) に、ログイン画面の URL を入力して、[統合オペレーション・ビューアー] 画面を表示します。すでにログインしている場合は、いったんログアウトしてからログインし直してください。なお、JP1/IM - Manager (インテリジェント統合管理基盤) を再起動する必要はありません。

それぞれの作業の詳細を次項から説明します。

5.17.2 モニター画面呼び出しをするための画面の決定

モニター画面呼び出しをするためには、どの JP1 イベントが発行されたときにどの画面を呼び出すか、およびその画面を起動するときにどんな引数を指定するかを決める必要があります。モニター画面呼び出しは、ある JP1 イベントを発行したジョブやアプリケーションの詳細画面を呼び出したり、その詳細画面から直接、該当するジョブやアプリケーションを操作したりできるようにすることを目的としています。この目的に適した画面を選んでください。

また、画面起動時に必要な情報はすべて JP1 イベントの属性値から引き継ぐことになるので、JP1 イベントの属性もあわせて考慮する必要があります。

なお、モニター画面呼び出しによって起動されたアプリケーションのログイン認証などは共通化できないため、必要であればログインを省略するなどの方法 (画面起動コマンドのオプション化) をアプリケーションごとにとる必要があります。

5.17.3 定義ファイルの作成

ここでは、モニター画面呼び出し定義ファイルおよびアプリケーション実行定義ファイルに定義する内容、格納場所および定義例を説明します。

(1) モニター画面呼び出し定義ファイルの作成

モニター画面呼び出し定義ファイルでは、モニター画面呼び出しをする JP1 イベントの ID や属性などを定義します。

JP1 イベントの属性は、イベント拡張属性定義ファイルの定義と対応させる必要があります。

イベント拡張属性定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベント拡張属性定義ファイル」(2. 定義ファイル) を参照してください。

また、この定義ファイルでは、呼び出す画面、および画面を呼び出すときの引数を定義します。呼び出す画面を定義するために、アプリケーション実行定義識別子を指定します。アプリケーション実行定義識別子は、モニター画面呼び出し定義ファイルで定義した画面を JP1/IM - View 側で識別するためのものです。したがって、モニター画面呼び出し定義ファイルで指定するアプリケーション実行定義識別子を、アプリケーション実行定義ファイルに定義する必要があります。指定したアプリケーション実行定義識別子は、アプリケーション実行定義ファイルによってパスが解決されます。また、実行ファイルの起動時には、モニター画面呼び出し定義ファイルで指定した引数が渡されます。モニター画面呼び出し定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「モニター画面呼び出し定義ファイル」(2. 定義ファイル) を参照してください。

なお、JP1/IM には、モニター画面呼び出し定義ファイルの記述内容をチェックするためのコマンド「jcomonitorfcheck」が用意されています。このコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcomonitorfcheck」(1. コマンド) を参照してください。

(2) アプリケーション実行定義ファイルの作成

アプリケーション実行定義ファイルには、モニター画面呼び出し定義ファイルで定義されたアプリケーション実行定義識別子とパスの関連づけを定義します。

アプリケーション実行定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「アプリケーション実行定義ファイル」(2. 定義ファイル) を参照してください。

なお、JP1/IM には、アプリケーション実行定義ファイルの記述内容をチェックするために jcoappexecfcheck (Windows 限定) コマンドが用意されています。このコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoappexecfcheck (Windows 限定)」(1. コマンド) を参照してください。

5.18 統合機能メニューの設定

〔統合機能メニュー〕画面から連携製品の GUI（アプリケーション画面）や、WWW ページを起動する設定をします。

5.18.1 統合機能メニューから連携製品の GUI を起動するための設定

JP1/IM - Manager と連携する製品の幾つかは、デフォルトで〔統合機能メニュー〕画面に表示されています。この場合、JP1/IM - View と同ホストに連携製品をインストールすると〔統合機能メニュー〕画面から連携製品の GUI（アプリケーション画面）を起動できます。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「8.3.2 〔統合機能メニュー〕画面から操作できる機能」を参照してください。

表示されていない製品を新規に登録したい場合に、次からの説明を参照してください。

〔統合機能メニュー〕画面から連携製品の GUI（アプリケーション画面）を起動するための設定手順を次に示します。

1. 〔統合機能メニュー〕画面から起動するアプリケーションを決める。

2. 定義ファイルを作成する。

JP1/IM - View がインストールされたホストに次の定義ファイルを作成します。

- 統合機能メニュー定義ファイル
- アプリケーション実行定義ファイル

統合機能メニュー定義ファイルおよびアプリケーション実行定義ファイルは、次のフォルダに作成します。

View パス¥conf¥function¥ja¥

3. JP1/IM - View を再起動する。

なお、上記の手順の詳細については、「[5.18.4 定義ファイルの作成](#)」を参照してください。設定のための前提条件、設定例などについて説明しています。

❗ 重要

連携製品によっては、上記と異なった手順が必要になる場合があります。設定手順の詳細については、各製品のマニュアルも参照してください。

5.18.2 新規メニューを追加する手順

〔統合機能メニュー〕画面に新規メニューを追加するための作業手順を示します。作業の流れは次のとおりです。

1. 〔統合機能メニュー〕画面から起動する画面を決める。

2. 定義ファイルを作成する。

JP1/IM - View がインストールされたマシン上に、次の定義ファイルを作成します。

- 統合機能メニュー定義ファイル

この定義ファイルでは、追加する新規メニューの情報、新規メニューから起動する画面などを定義します。

- アプリケーション実行定義ファイル

この定義ファイルでは、統合機能メニュー定義ファイルで定義されたアプリケーションのパスを JP1/IM - View で解決するための定義をします。

3. 定義ファイルを有効にする。

それぞれの作業の詳細を次項から説明します。

5.18.3 〔統合機能メニュー〕画面から起動する画面の決定

〔統合機能メニュー〕画面から起動する画面は、システムやアプリケーションを管理するための画面です。この目的に適した画面を選んでください。

なお、ログイン認証などは共通化できないため、必要であればログインを省略するなどの方法（画面起動コマンドのオプション化）をアプリケーションごとにとる必要があります。

〔統合機能メニュー〕画面から起動する画面を決める手順を次に示します。

1. 〔統合機能メニュー〕画面に表示する名称と使用する ID を決める。

ID はメニュー識別子です。「会社名_製品名」の形式で指定します。ID は、メニュー全体でユニークにしてください。

2. 〔統合機能メニュー〕画面に表示するときのフォルダを決める。

既存のフォルダに適切なものがない場合は、フォルダの名称と使用する ID を決めます。ID は、「会社名_製品名」の形式で指定します。ID は、メニュー全体でユニークにしてください。

3. 〔統合機能メニュー〕画面に表示するアイコンを準備する。

アイコンは、16×16 ピクセルの GIF ファイルとして作成します。アイコンを指定しない場合は、デフォルトのアイコンが使用されます。

5.18.4 定義ファイルの作成

ここでは、統合機能メニュー定義ファイルおよびアプリケーション実行定義ファイルに定義する内容、格納場所および定義例を説明します。

(1) 統合機能メニュー定義ファイルの作成

統合機能メニュー定義ファイルには、メニューから起動する画面、メニューツリーの上位ノード、メニューに表示するときの名称などを定義します。

(a) 定義する内容

メニューから起動する画面を定義するために、アプリケーション実行定義識別子を指定します。アプリケーション実行定義識別子は、統合機能メニュー定義ファイルで定義した画面を JP1/IM - View で識別するためのものです。したがって、統合機能メニュー定義ファイルで指定するアプリケーション実行定義識別子を、アプリケーション実行定義ファイルに定義する必要があります。指定したアプリケーション実行定義識別子は、アプリケーション実行定義ファイルによってパスが解決され、それによってメニューから画面を起動できるようになります。統合機能メニュー定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「統合機能メニュー定義ファイル」(2. 定義ファイル)を参照してください。アプリケーション実行定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「アプリケーション実行定義ファイル」(2. 定義ファイル)を参照してください。

なお、JP1/IM には、統合機能メニュー定義ファイルの記述内容をチェックするためのコマンド「jcofuncfcheck (Windows 限定)」が用意されています。このコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcofuncfcheck (Windows 限定)」(1. コマンド)を参照してください。

(b) 格納場所

この定義ファイルは、ビューア上の次のディレクトリに格納します。定義は、JP1/IM - View を再起動したあとに有効になります。

View パス¥conf¥function¥ja¥

(c) 定義例

ここでは、次の例を示します。

アプリケーション

COMPANY 社の SAMPLE という名称の製品

フォルダの名称と ID

「SAMPLE 管理」, ID ="company_sample_management"

メニューの名称と ID

「SAMPLE 管理画面 (アプリケーション)」, ID ="company_sample_naitive"

「SAMPLE 管理画面（WWW）」, ID="company_sample_web"

アイコンファイル

sample_icon.gif

実行ファイル

sample.exe

URL

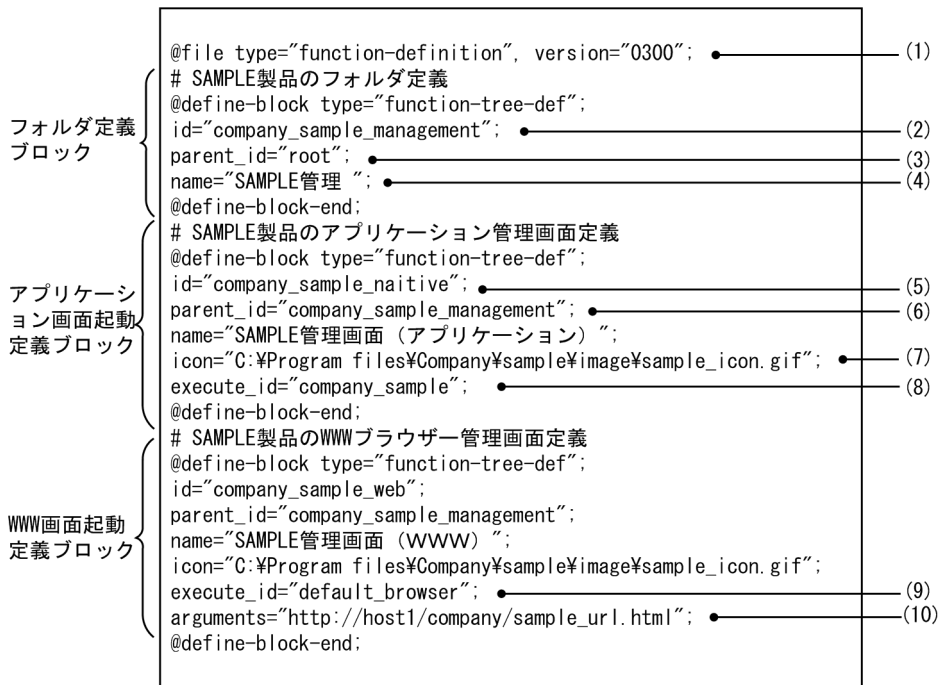
http://host1/company/sample_url.html

この例では、次のファイル名を使用します。

company_sample_tree.conf

統合機能メニュー定義ファイルの定義例を次に示します。

図 5-2 統合機能メニュー定義ファイルの定義例



- (1) バージョンは「0300」だけを指定できます。
- (2) フォルダのIDを指定します。
- (3) 親フォルダを指定します。「root」は最上位のフォルダです。
- (4) フォルダの名称を指定します。
- (5) メニューのIDを指定します。
- (6) 親フォルダを指定します。
- (7) アイコンファイルを指定します。
- (8) アプリケーション実行定義識別子を指定します。
- (9) デフォルトのWWWブラウザを使用することを指定します。
- (10) 起動するWWWページのURLを指定します。

この定義によって、[統合機能メニュー] 画面のツリー上では、「SAMPLE 管理」という名称のフォルダの下に「SAMPLE 管理画面（アプリケーション）」および「SAMPLE 管理画面（WWW）」という名称のメニューが定義した順序で表示されるようになります。

(2) アプリケーション実行定義ファイルの作成

アプリケーション実行定義ファイルには、統合機能メニュー定義ファイルで定義されたアプリケーション実行定義識別子とパスの関連づけを定義します。

(a) 定義する内容

アプリケーション実行定義ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「アプリケーション実行定義ファイル」(2. 定義ファイル)を参照してください。

なお、JP1/IM には、アプリケーション実行定義ファイルの記述内容をチェックするためのコマンド「jcoappexecfcheck (Windows 限定)」が用意されています。このコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoappexecfcheck (Windows 限定)」(1. コマンド)を参照してください。

(b) 格納場所

この定義ファイルは、ビューアー上の次のディレクトリに格納します。定義は、JP1/IM - View を再起動したあとに有効になります。

View パス¥conf¥appexecute¥ja¥

(c) 定義例

ここでは、モニター画面呼び出しをする場合と同じ例を使用します。この例では、次のファイル名を使用します。

company_sample_app.conf

アプリケーション実行定義ファイルの定義例を次に示します。

図 5-3 アプリケーション実行定義ファイルの定義例

```
@file type="application-execution-definition", version="0300"; (1)
# アプリケーションプログラム画面起動sample.exeコマンドの定義
@define-block type="application-execution-def";
id="company_sample";
path="[¥HKEY_LOCAL_MACHINE¥SOFTWARE¥COMPANY¥SAMPLE¥PathName¥Path00]¥bin¥sample.exe"; (2)
@define-block-end;
# WWWページでデフォルトのWWWブラウザ以外を使用する場合
@define-block type="application-execution-def";
id="company_sample_web";
path="C:¥Program files¥Netscape¥bin¥netscape.exe"; (3)
@define-block-end;
```

- (1) バージョンは「"0300"」だけを指定できます。
- (2) []で囲まれた部分をレジストリーキーから解決します。
- (3) レジストリー情報にパスがない場合は、フルパスを指定します。

5.18.5 統合機能メニューから連携製品の WWW ページを起動するための設定

JP1/IM - View の統合機能メニューから連携製品の WWW ページを表示させる場合、WWW ページ呼び出し定義ファイル (hitachi_jp1_製品名.html) を編集して表示させる WWW ページの URL を設定する必要があります。手順を次に示します。

1. WWW ページ呼び出し定義ファイル (hitachi_jp1_製品名.html) を編集する。

WWW ページ呼び出し定義ファイルの格納フォルダは次のとおりです。

View パス¥conf¥webdata¥ja¥

WWW ページ呼び出し定義ファイルをテキストエディターなどで開きます。ファイル内の<META>タグを検索し、CONTENT 属性の URL に、起動する WWW ページの URL を指定します。

2. 編集した WWW ページ呼び出し定義ファイルを上書き保存する。

3. JP1/IM - View を再起動する。

なお、統合機能メニュー定義ファイルを作成することで、WWW ページ呼び出し定義ファイルが提供されていない製品についても WWW ページを起動できます。

WWW ページの URL の設定について

- WWW ページ呼び出し定義ファイルについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「WWW ページ呼び出し定義ファイル (hitachi_jp1_製品名.html)」(2. 定義ファイル)

上記の URL の設定をしないで、WWW ページを表示しようとした場合、設定手順を記述した画面を表示します。画面の記述に従って設定してください。この画面は WWW ページを表示しようとした製品名 (画面名) ごとに内容が異なります。

5.19 業務グループの参照・操作制限の設定

業務グループの参照・操作制限を設定する方法を説明します。JP1 ユーザーに割り当てる JP1 資源グループおよび JP1 権限レベルの設定を検討してから設定してください。

なお、業務グループの参照・操作制限を有効にする場合、統合監視 DB、IM 構成管理 DB および発生元ホストのマッピングが有効となっている必要があります。

業務グループの参照・操作制限を設定する手順を次に示します。

1. 業務グループの参照・操作制限を有効にする。

```
jcoimdef -bizmonmode ON
```

jcoimdef コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド)を参照してください。

2. JP1/IM - Manager を再起動する。

3. JP1/IM - View を再起動する。

JP1/IM - View を再起動するまで、設定前の状態が保持されます。業務グループの参照・操作制限を有効から無効または無効から有効に変更した場合は、必ず JP1/IM - View を再起動してください。

4. 業務グループの内容をセントラルコンソールに反映する。

IM 構成管理ビューアーから反映します。業務グループの内容をセントラルコンソールに反映する手順については、「[3.4.1\(3\) 業務グループを反映する](#)」を参照してください。

JP1 資源グループおよび JP1 権限レベル、業務グループ、統合監視 DB、IM 構成管理 DB および発生元ホストのマッピングについては、各項目を参照してください。

JP1 資源グループおよび JP1 権限レベルについて

- 業務グループの JP1 資源グループおよび JP1 権限レベルの組み合わせについて
参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.1.4 業務グループの参照・操作制限の仕組み」
- JP1 資源グループおよび JP1 権限レベルの設定方法について
参照先：マニュアル「JP1/Base 運用ガイド」のユーザー管理の設定の章

業務グループについて

- 業務グループの概要について
参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.4 業務グループの管理」
- 業務グループの設定方法について
参照先：「[3.4 業務グループの設定](#)」

統合監視 DB について

- 統合監視 DB の設定方法について

参照先：

Windows の場合「[1.4.2 統合監視 DB の設定 \(Windows の場合\)](#)」

UNIX の場合「[2.4.2 統合監視 DB の設定 \(UNIX の場合\)](#)」

IM 構成管理 DB について

- IM 構成管理 DB の設定方法について

参照先：

Windows の場合「[1.4.3 IM 構成管理 DB の設定 \(Windows の場合\)](#)」

UNIX の場合「[2.4.3 IM 構成管理 DB の設定 \(UNIX の場合\)](#)」

発生元ホストのマッピングについて

- 発生元ホストのマッピングの概要について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「[4.9 発生元ホストのマッピング](#)」

- 発生元ホストのマッピングの設定方法について

参照先：「[5.15 発生元ホストのマッピングの設定](#)」

6

セントラルスコープの設定

セントラルスコープでは、[監視ツリー] 画面と [ビジュアル監視] 画面によってシステムを管理者の目的に合わせた視点で監視できます。

この章では、これらの監視画面の環境を設定する手順について説明します。

6.1 セントラルスコープの環境設定の概要

セントラルスコープの環境設定は、管理者の目的に合わせた視点でシステムを監視するために、稼働しているシステムの構成とその監視目的に合わせて、セントラルスコープの監視画面を作成する作業です。

まず、実際のシステム構成を、監視目的に合わせたツリー形式で「監視ツリー」画面に設定します。そのあとで、重点的に監視が必要なポイントをマップ形式で「ビジュアル監視」にまとめます。

なお、この章での説明は、セントラルスコープがセットアップ済みで動作していることを前提にしています。

6.1.1 セントラルスコープの環境設定を始める前に

セントラルスコープの環境設定を始める前に、次の準備をしてください。

JP1/IM 全般とセントラルスコープについて知っておく

- セントラルスコープの使い方の概要

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「1. JP1/Integrated Management の概要」

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2. 機能の概要」

- セントラルスコープの機能について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5. セントラルスコープによる目的指向型のシステム監視」

JP1/IM の動作環境を構築する

- JP1/IM のインストールとセットアップをする

参照先：「1. インストールとセットアップ（Windows の場合）」

参照先：「2. インストールとセットアップ（UNIX の場合）」

6.2 ホスト情報の登録

セントラルスコープ用のホスト情報をホスト情報 DB に登録します。

1. ホスト情報ファイル (jcs_hosts) を作成, 編集する。
2. jcshostsimport コマンドを実行する。
3. ホスト情報ファイルの内容を有効にする。

次の場合にホスト情報ファイルの内容が有効になります。

- jco_spmd_reload コマンドを実行する。
- JP1/IM - Manager を再起動する。

ホスト情報の設定については, 次の説明を参照してください。

ホスト情報の設定について

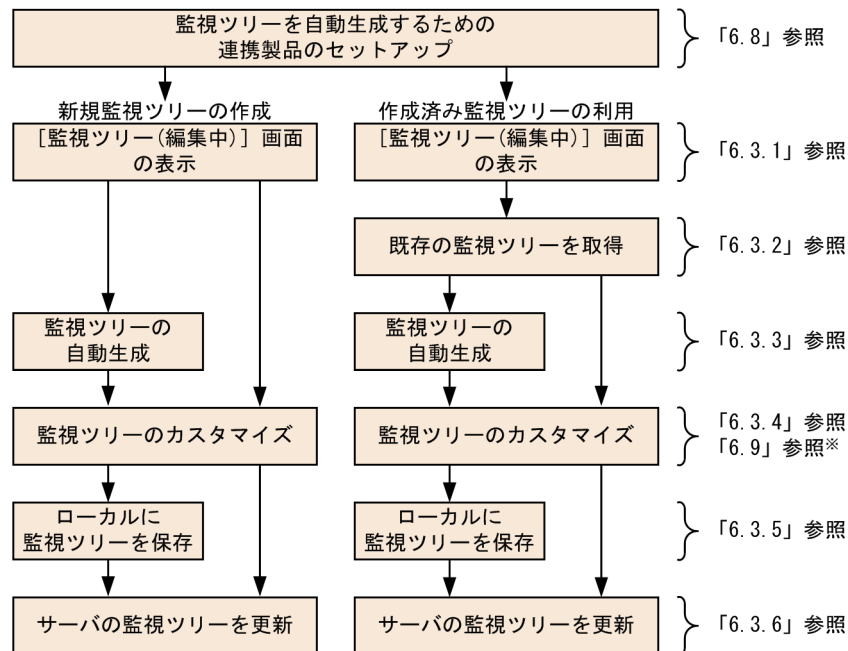
- ホスト情報について
参照先: マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5.11.2 ホスト情報」
- ホスト情報ファイルの書式について
参照先: マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ホスト情報ファイル (jcs_hosts)」(2. 定義ファイル)
- jcshostsimport コマンドについて
参照先: マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcshostsimport」(1. コマンド)

6.3 監視ツリーを GUI で作成する

ここでは、監視オブジェクトを監視するための監視ツリーを GUI で作成する手順について説明します。

作業の流れを次に示します。

図 6-1 監視ツリーを GUI で作成する作業の流れ



注※ 監視オブジェクトの作成例について説明しています。

6.3.1 監視ツリーの編集画面の起動

監視ツリーは、[監視ツリー(編集)] 画面から編集します。

1. [監視ツリー(編集)] 画面を起動する。

次のどれかの手順で起動します。

- スタートメニューから [すべてのプログラム] – [JP1_Integrated Management 3 - View] – [監視ツリー編集] を選択する。
- jcoview コマンドを実行する。
jcoview -e
- システムを監視中の [監視ツリー] 画面のメニューバーから、[オプション] – [ツリー編集] を選択する。

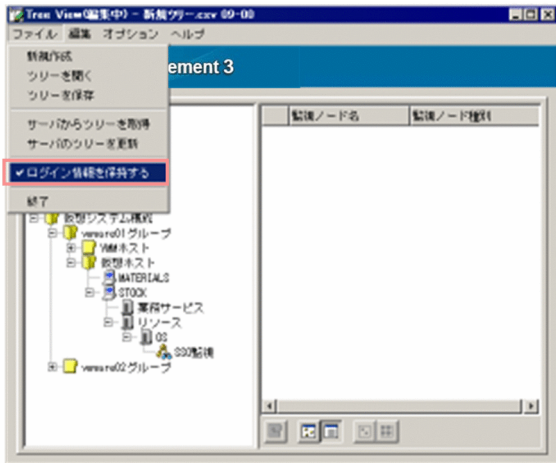
なお、[監視ツリー(編集)] 画面を起動した直後は、なにも表示されていない（監視ツリーの情報が無い）状態です。

ログイン情報の保持

[監視ツリー(編集)] 画面で、[ログイン情報を保持する] 機能の設定ができます。この設定は、[監視ツリー(編集)] 画面からログインが必要な操作をする際、一度目のログイン時にユーザー名・パスワード・接続ホスト名を保持します。このため、二度目以降のログイン操作が不要になります。

- [監視ツリー(編集)] 画面から、[ファイル] – [ログイン情報を保持する] をチェックする。

図 6-2 [ログイン情報を保持する] メニュー



ログインが必要な操作を次に示します。

表 6-1 ログインを必要とする操作一覧

画面名	操作	説明
監視ツリー(編集 中)	[ファイル] – [サーバからツリーを取得] を選択	監視ツリーの既存の設定をマネージャーから取得する。
	[ファイル] – [サーバのツリーを更新] を選択	監視ツリーの編集内容をマネージャーに反映する。
	[オプション] – [ツリーの自動生成] を選択	監視ツリーを自動生成する。
	[オプション] – [最新定義取得] を選択	マネージャー上の共通条件定義の最新情報を取得する。
	[編集] – [ビジュアル監視画面一覧編集] を選択	[ビジュアル監視画面一覧編集] 画面を表示する。
ビジュアル監視 (編集)	[サーバからのビジュアル監視データを取得] ボタンをクリック	マネージャー上のビジュアル監視データを読み込む。
	[サーバのビジュアル監視データを更新] ボタンをクリック	編集したビジュアル監視データをマネージャーに反映する。

[ログイン情報を保持する] へのチェック状態は、[監視ツリー(編集)] 画面の終了時に保存されま
す。次回、[監視ツリー(編集)] 画面の起動時に、その状態が反映されます。

6.3.2 既存の監視ツリーの取得

すでに監視ツリーを作成して運用している場合は、まず、マネージャーに接続して、既存の設定を取得します。

[監視ツリー(編集)] 画面でサーバから、またはローカルホストの CSV ファイルから監視ツリーを取得します。[監視ツリー(編集)] 画面のタイトルバーには、サーバの JP1/IM - Manager (セントラルスコープ) のバージョン、または取得したファイルのバージョンが表示されます。

❗ 重要

ローカルホストの CSV ファイルから監視ツリーを取得した場合、[監視ツリー(編集)] 画面のタイトルバーに表示されるファイルバージョンが古い場合、[監視ツリー(編集)] 画面で編集した情報をマネージャーに反映できません。

(1) サーバからの監視ツリーの取得

1. [サーバからツリーを取得] を選択する。

[監視ツリー(編集)] 画面から、[ファイル] - [サーバからツリーを取得] を選択します。

2. サーバにログインする。

JP1/IM - Manager (セントラルスコープ) にログインするための [ログイン] 画面が表示されます。JP1 ユーザー名とパスワードを入力します。JP1 ユーザーは、JP1 資源グループが JP1_Console で、JP1_Console_Admin 権限を持っている必要があります。接続先ホスト名には、監視ツリーを取得する JP1/IM - Manager のホスト名を入力します。

ログインが成功すると、監視ツリーのデータを取得し、[監視ツリー(編集)] 画面に表示します。

または、ローカルに保存している監視ツリーの設定 (CSV ファイル) がある場合は、それを使用することもできます。

(2) ローカルに保存した監視ツリー (CSV ファイル) の取得

1. [ツリーを開く] を選択する。

[監視ツリー(編集)] 画面から、[ファイル] - [ツリーを開く] を選択します。

ファイルを選択する [ツリーを開く] 画面が表示されます。

2. 監視ツリー (CSV ファイル) を指定する。

[ツリーを開く] 画面で、利用する監視ツリー (CSV ファイル) を選択し、[開く] ボタンをクリックします。

確認ダイアログボックスが表示されるので、[はい] ボタンをクリックしてください。

6.3.3 監視ツリーの自動生成

監視ツリーを自動生成します。

なお、他製品と連携して監視ツリーを自動生成する場合、連携製品のセットアップ（JP1 イベントを発行する設定や、アダプタコマンドの実行など）を事前にしておく必要があります。「[6.8 連携製品のセットアップ](#)」を参照して自動生成前にセットアップを終えておいてください。

運用上の理由で jpladmin ユーザーを削除している場合は、連携製品の定義情報にアクセスできる権限レベルを持つ JP1 ユーザーでログインし、自動生成を行ってください。例えば、JP1/AJS のジョブネット情報を取得するには、ジョブネットにアクセスできる権限レベルが必要です。

また、監視ツリーの自動生成機能の詳細は、次の説明を参照してください。

監視ツリーの自動生成について

- 監視ツリーの自動生成機能について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5.2 監視ツリー」

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5.3 監視ツリーの自動生成」

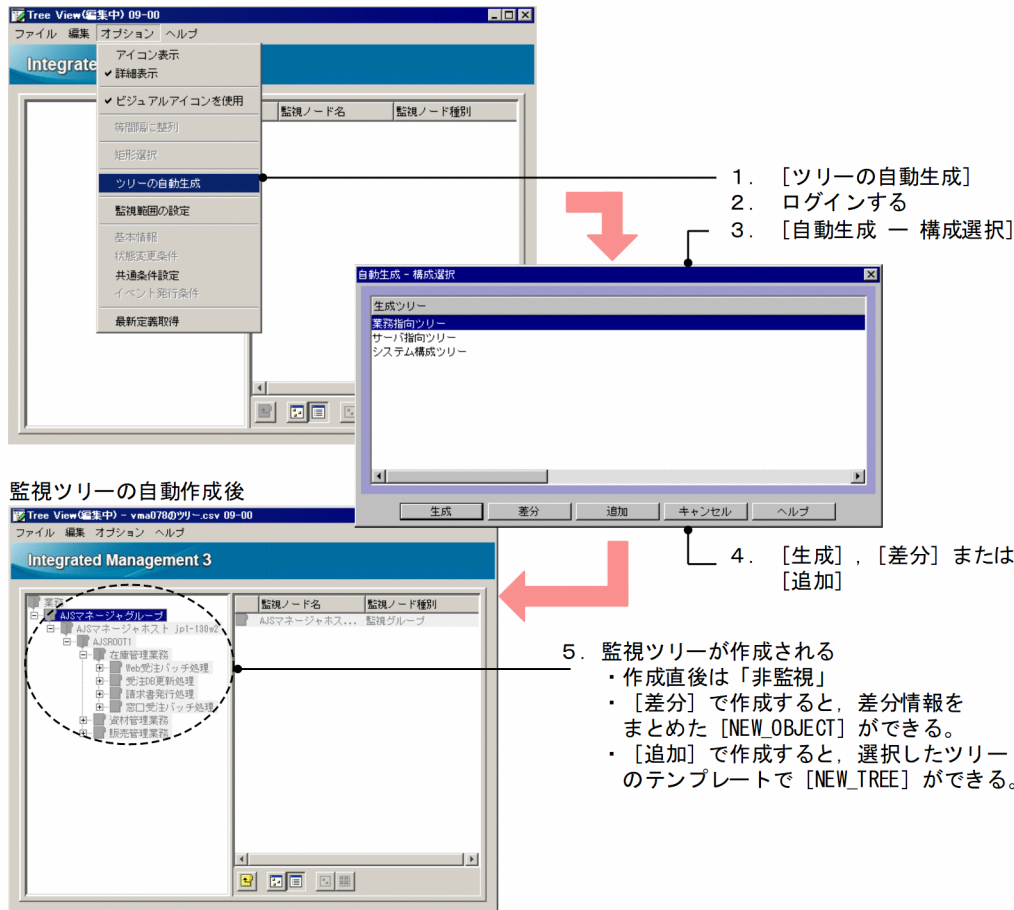
- 自動生成で作成される監視ツリーのモデルについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「9. 監視ツリーモデル（セントラルスコープ用）」

次に監視ツリー自動生成の手順を示します。

図 6-3 監視ツリーの自動生成の手順

監視ツリーの自動作成前



1. [ツリーの自動生成] を選択する。

[監視ツリー(編集集中)] 画面から、[オプション] - [ツリーの自動生成] を選択します。

なお、すでに監視ツリーを編集集中だった場合は、「編集集中のツリー構成情報を置き換えますか？」のように確認されます。ここで [はい] を選択すると、編集集中の情報は、自動生成した情報で置き換えられます。

2. サーバにログインする。

JP1/IM - Manager (セントラルスコープ) にログインするための [ログイン] 画面が表示されます。jpladmin ユーザーでログインしてください。

接続ホスト名には、ログインする JP1/IM - Manager があるホストの名称を指定します。ビューアーで定義されているホスト名か、IP アドレスを指定してください。

3. [自動生成-構成選択] 画面で、監視ツリーのモデルを選択する。

自動生成する監視ツリーのモデルを選択します。

- ・ 業務指向ツリー
- ・ サーバ指向ツリー

4. [生成], [差分] または [追加] のボタンをクリックする。

6. セントラルスコープの設定

- [生成] …新しい監視ツリーを、収集した定義情報から作成します。
- [差分] …編集画面の監視ツリーと収集した定義情報との差分情報（監視オブジェクトと監視グループを含む）から新規の監視ツリーを作成します。なお、新規の監視ツリーは [NEW_OBJECT] という監視グループに作成されます。
- [追加] …編集画面の監視ツリーから新規の監視ツリーを作成します。なお、新規の監視ツリーは [NEW_TREE] という監視グループに作成されます。

5. 監視ツリーが自動的に生成される。

JP1/IM が管理する各ホストから定義情報を収集し、監視ツリーを自動生成します。しばらくお待ちください。

なお、生成される監視ノードの状態は、最初は非監視の状態になっています。

自動生成した監視ツリーは、監視方法に合わせてカスタマイズしてから運用を始めてください。

6.3.4 監視ツリーのカスタマイズ

[監視ツリー(編集)] 画面では、監視ツリーを新規作成したり、既存の監視ツリーをカスタマイズしたりできます。監視ツリーに関してできる操作を次に示します。

- 監視ノードの追加
- 監視ノードの属性設定
- 監視ノードの削除
- 監視ノードの移動
- 監視範囲の設定
- マップ表示設定

ここでは、監視ツリーに関してできる操作、および作成済み監視ノードの検索について説明します。

なお、監視ツリーをカスタマイズするには、監視ツリーの機能や設定内容を知っておく必要があります。次の説明を参照してください。

監視ツリーの機能や設定内容について

- 監視ツリーの機能について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5.2 監視ツリー」

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5.3 監視ツリーの自動生成」

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5.4 監視ツリーの編集」

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5.11 セントラルスコープの仕組み」

- 監視ツリーの設定項目について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5.2 監視ツリー」

- 基本的な設定が定義済みのシステム監視オブジェクトについて

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「8. システム監視オブジェクト一覧（セントラルスコープ用）」

なお、監視ノードの属性設定で「共通条件」を設定する、かつ、設定済みの共通条件を利用する場合は、次の操作によって、共通条件を取得しておいてください。

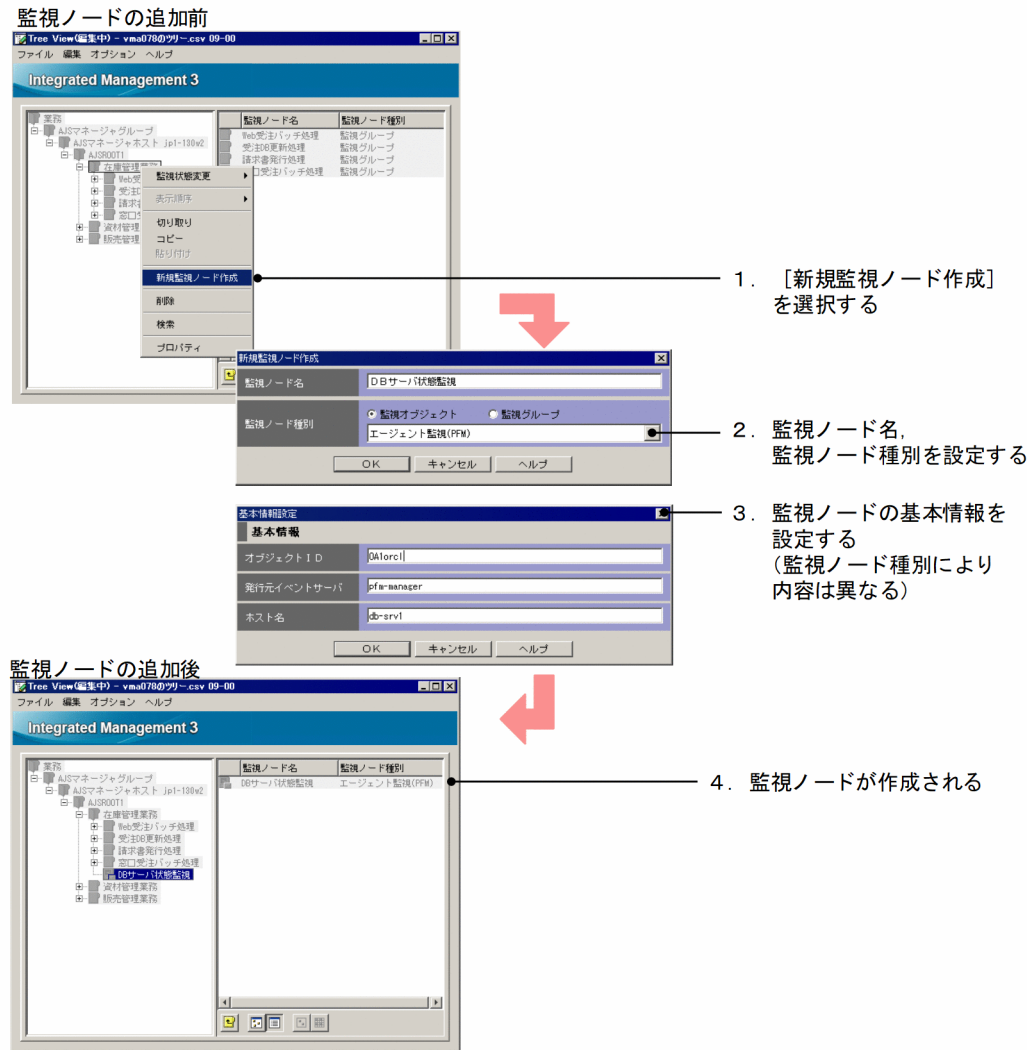
ツリー構成ファイル（CSV ファイル）使用時にはツリー構成ファイルが保持する共通条件、新規監視ツリー作成時には JP1/IM - View が保持する共通条件を利用できます。

1. [監視ツリー(編集)] 画面のメニューバーの [オプション] - [最新定義取得] を選択する。

(1) 監視ノードの追加

監視ノードを追加する手順を説明します。

図 6-4 監視ノードの追加の手順



1. [新規監視ノード作成] 画面を開く。

次のどれかの操作により画面を開いてください。

- 監視グループを選択し、右クリックしてポップアップメニューから [新規監視ノード作成] を選択する。
- 監視グループを選択し、メニューバーから [編集] - [新規監視ノード作成] を選択する。
- 詳細表示領域から画面を開く場合は、監視ノード非選択状態で右クリックし、ポップアップメニューから [新規監視ノード作成] を選択する。

なお、監視ノードが一つもない場合は、メニューバー、または監視ツリー領域の右クリックで表示されるポップアップメニューから操作をしてください。

2. 監視ノード名, 監視ノード種別を設定する。

[新規監視ノード作成] 画面で、次の項目を設定します。

- 監視ノード名
任意の名称を指定します。

- 監視ノード種別

監視ノードの種別を選択します。

「監視グループ」、または「監視オブジェクト」とその種類を選択します。

監視オブジェクトの種類を選択する場合は、システム監視オブジェクトから選ぶことができます。これは、JP1/IM のシステムが標準で用意している監視オブジェクトで、JP1/IM と連携する JP1 シリーズ製品ごとに基本的な項目があらかじめ設定されています。

監視オブジェクトの種類で「汎用オブジェクト」を選ぶと、汎用監視オブジェクトが作成されますので、後述する監視ノードの「プロパティ」画面で属性を設定してください。

なお、ここで「監視グループ」または「監視オブジェクト」の「汎用オブジェクト」を選択した場合は、次の基本情報の設定は必要なく、監視ノードが作成されます。

3. 監視ノードの基本情報を設定する。

「基本情報設定」画面で、監視ノードの種類に合わせた基本情報を設定します。

基本情報は、監視オブジェクトが監視している対象を特定するための情報を設定します。監視ノード種別で指定したシステム監視オブジェクトの種類によって、設定する値は異なります。詳しくは次の説明を参照してください。

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「8. システム監視オブジェクト一覧（セントラルスコープ用）」

4. 監視ノードが作成される。

設定した内容で、監視ノードが作成されます。

なお、既存の監視オブジェクトをコピー&ペーストすることもできます。

既存の監視オブジェクトをコピー&ペーストする

次の手順でコピー&ペーストしてください。

1. 監視ノードを選択し、コピーする。

- 右クリックしてポップアップメニューから「コピー」を選択する。
- メニューバーの「編集」－「コピー」を選択する。

2. 貼り付け先の監視グループを選択する。

3. 監視ノードをペーストする。

- 右クリックしてポップアップメニューから「貼り付け」を選択する。
- メニューバーの「編集」－「貼り付け」を選択する。

(2) 監視ノードの属性設定

監視ノードの属性を設定する手順を説明します。

なお、監視ノードの属性を設定するには、それぞれの設定項目の意味を知る必要があります。ここでは、設定手順と簡単な例だけを説明します。設定内容の詳細は、この項のはじめに説明している参照先で確認してください。

1. 監視ノードの [プロパティ] 画面を開く。

監視ノードを選択して、次のどれかの方法で [プロパティ] 画面を開きます。

- ダブルクリックする（監視オブジェクトの場合だけ有効）。
- 右クリックしてポップアップメニューから [プロパティ] を選択する。
- メニューバーから [編集] - [プロパティ] を選択する。
- メニューバーから [オプション] - [基本情報], [状態変更条件], または [イベント発行条件] を選択する。

2. [全般] ページを設定する。

監視ノード名、使用するアイコン、使用するビジュアルアイコン※¹、背景画像設定（監視グループ限定）、監視状態、および JP1 資源グループ※² を設定します。

3. [基本情報] ページを設定する。

監視ノードの基本情報を設定します。

4. [状態変更条件] ページを設定する。

- 監視オブジェクト選択時

JP1/IM - Manager がどのような JP1 イベントを受信したときに、監視ノードの状態を変更するかを設定します。

監視オブジェクトの状態変更条件に設定する内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「8. システム監視オブジェクト一覧（セントラルスコープ用）」を参考にしてください。

- 監視グループ選択時

監視グループの下位の監視ノードがどのような状態になったときに、監視グループの状態を変更するかを設定します。

5. [イベント発行条件] ページを設定する。

監視ノードがどのような状態になったときに、JP1 イベントを発行するかを設定します。

なお、監視ノードの状態により自動アクションをする場合は、この [イベント発行条件] を設定して、イベント ID が 00003FB0 の JP1 イベントに対して自動アクションをするよう設定してください。

6. [OK] ボタンまたは [適用] ボタンをクリックする。

注※¹ ビジュアルアイコンを使用するためには、フォルダ作成やファイルの格納など準備が必要です。詳細については、「6.3.4(7) ビジュアルアイコンを使用するための設定」を参照してください。

次に、プロパティの設定の例について説明します。

Tree View(編集中) - v-ma078のファイル.csv 09:00
ファイル 編集 オプション ヘルプ

Integrated Management 3

業務
 AJSマネージャグループ
 AJSマネージャネスト jpl-180v2
 AJSROOT1
 在庫管理業務
 Web受入バッチ処理
 Web jpl-180v2
 JP1ジョブサービス
 ジョブ
 Web
 ジョブ
 受託品更新処理
 請求書発行処理
 窓口受入バッチ処理
 DBサーバ状態監視
 運料管理業務
 販売管理業務

監視ノード名
 JP1ジョブサービス

監視ノード種別
 監視グループ

1. 監視したい監視ノードの
「プロパティ」を選択する

業務サービスのプロパティ

全般 基本情報 状態変更条件 イベント実行条件

監視サービス

監視ノードID: 00000000

場所: /業務/AJSマネージャグループ/AJSマネージャ

監視ノード種別: 監視グループ

アイコン(通常時): jos_g_folder02.gif 変更

アイコン(懸断時): jos_g_folder01.gif 変更

ビジュアルアイコン: 変更

警告音設定: 警告音設定

計画更新日時: ----/---/--- :--:--

状態:
☒ 監視
☐ 非監視

2. 状態を「監視」に設定する

運用方法に合わせて、
監視する、または監視しないを設定する

OK 適用 キャンセル ヘルプ

監視ノード属性名:

監視ノード属性値:

監視ノード属性名	監視ノード属性値
ジョブ実行ホスト	jp1-130w2

発行元イベントサーバ登録名: jp1-130w2

AJSROOT1:/在庫管理業務...

図 6-7 「状態変更条件」 ページにより、監視ノードの状態変更条件を設定する例

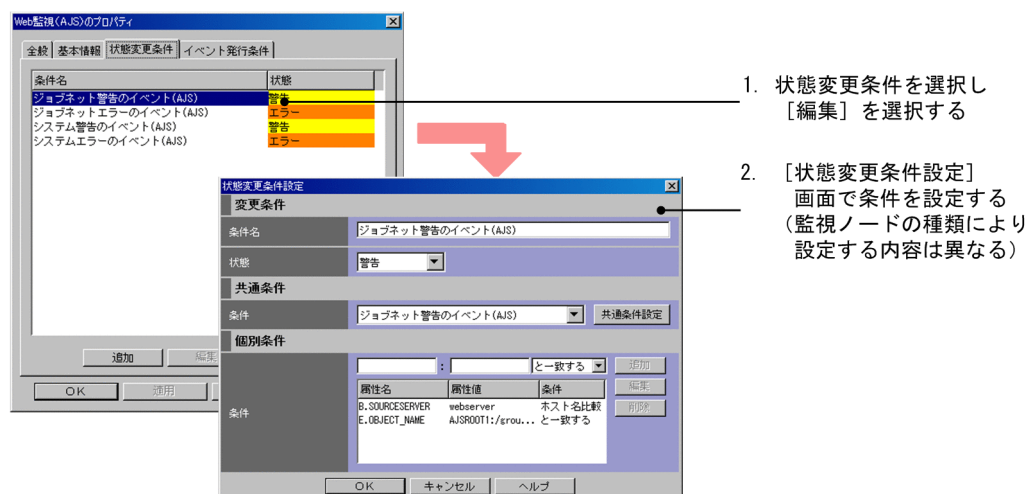
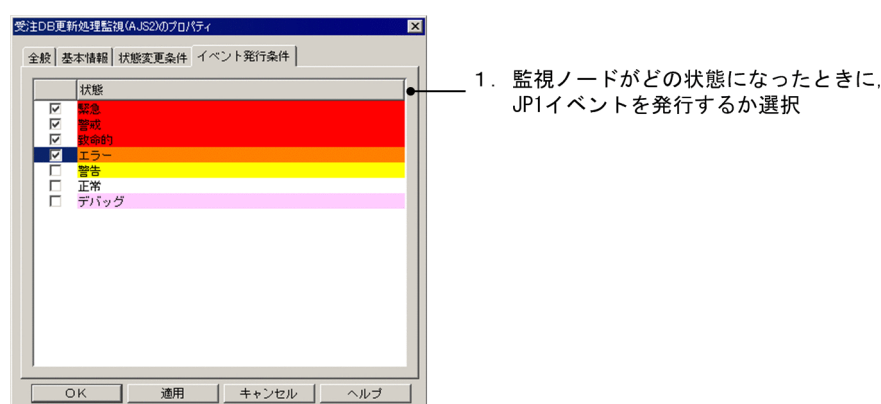


図 6-8 「イベント発行条件」 ページにより、JP1 イベント発行の設定をする例



(3) 監視ノードの削除

監視ノードを削除する手順について説明します。

監視グループを削除する場合、配下の監視ノードも削除されるため注意してください。

1. 監視ノードを選択する。

2. 監視ノードを削除する。

- メニューバーから [編集] - [削除] を選択する。
- 右クリックしてポップアップメニューから [削除] を選択する。

[削除確認] ダイアログボックスが表示されます。削除してよろしければ、[はい] ボタンをクリックします。

なお、すべての監視ノードを、次の手順で削除することもできます。

1. メニューバーの [編集] - [すべて削除] を選択する。

確認ダイアログボックスが表示されます。削除してよければ [はい] ボタンをクリックします。

(4) 監視ノードの移動

監視ノードは、監視ツリー上の別の位置に移動することができます。

移動は、ドラッグ&ドロップ、またはカット&ペーストで行います。

(a) ドラッグ&ドロップで移動する

1. 監視ノードをドラッグ（左クリック）して、監視グループにドロップする。

ドラッグ（左クリック）はツリー表示領域、詳細表示領域どちらでもできます。ドロップはツリー表示領域で行ってください。

(b) カット&ペーストで移動する

1. 監視ノードを選択する。
2. 監視ノードをカット（切り取り）する。
 - 右クリックしてポップアップメニューから「切り取り」を選択する。
 - メニューバーの「編集」－「切り取り」を選択する。
3. 貼り付け先の監視グループを選択する。
4. ペースト（貼り付け）する。
 - 右クリックしてポップアップメニューから「貼り付け」を選択する。
 - メニューバーの「編集」－「貼り付け」を選択する。

(5) マップ表示設定

マップ表示設定は、[監視ツリー] 画面の詳細表示領域に表示される監視ノードをマップ形式で表示したい場合に設定します。

設定手順を次に示します。

1. メニューバーから「表示」－「アイコン表示」を選択する、または  をクリックする。

詳細表示領域がマップ表示設定できる状態に変わります。

2. [背景画像設定] を開く。

次に示すどちらかの操作で「背景画像設定」画面を表示します。

- 詳細表示領域上の何もないところ（監視ノード非選択状態）で右クリックし、ポップアップメニューから「背景画像設定」を選択して「背景画像設定」画面を表示する。
- 監視グループの「プロパティ」画面を開き、[全般] ページの「背景画像設定」ボタンをクリックする。

3. 背景画像を選択する。

「背景画像設定」画面で、背景にする画像ファイル名を選択して、[OK] ボタンをクリックします。背景画像には、次のフォルダにある、次のフォーマットのファイルが使用できます。

- 画像ファイルのフォルダ：View パス¥image¥map¥
- 使用できる画像ファイルのフォーマット：JPEG, GIF, PNG

なお、背景を無地（白色）のまま使うこともできます。

この場合は、ファイル選択で「背景画像なし」を選んでください。

選択すると、確認ダイアログボックスが表示されるので [はい] ボタンをクリックします。

4. 監視ノードを、ドラッグ&ドロップする。

背景画像の設定が済んだ詳細表示領域上で監視ノードをドラッグ&ドロップし、任意の場所に配置します。配置をリセットしたいときは、 をクリックするか、メニューバーから [表示] – [等間隔に整列] を選択してください。確認ダイアログボックスが表示されるので [はい] ボタンをクリックします。

(6) 監視範囲の設定

JP1 資源グループで監視範囲を設定する方法について、手順を次に示します。

1. メニューから [オプション] – [監視範囲の設定] をチェックする。

監視ツリーの監視範囲設定が有効になります。

2. 監視ノードの [プロパティ] 画面を開く。

監視ノードを選択して、次のどれかの方法で [プロパティ] 画面を開きます。

- ダブルクリックする（監視オブジェクトの場合だけ有効）。
- 右クリックしてポップアップメニューから [プロパティ] を選択する。
- メニューバーから [編集] – [プロパティ] を選択する。

3. [全般] ページの JP1 資源グループを設定する。

監視範囲にあわせて、JP1 資源グループを指定してください。

4. [OK] ボタンまたは [適用] ボタンをクリックする。

(7) ビジュアルアイコンを使用するための設定

監視ノードのアイコンにビジュアルアイコンを使用するための設定について、手順を次に示します。なお、ビジュアルアイコンは標準提供されていません。事前にビジュアルアイコンとして使用するファイルを作成しておいてください。

1. メニューバーから [オプション] – [ビジュアルアイコンを使用] を選択し、チェックする。

ビジュアルアイコンを表示できるようにします。

2. ビジュアルアイコンの格納フォルダを作成する。

次に示すように、View パス¥image¥フォルダの下にvisual フォルダを作成します。

View パス¥image¥visual

3. ビジュアルアイコンとして使用したい画像ファイルを、手順 2 で作成したフォルダに格納する。

使用できる画像の形式、サイズは次のとおりです。

- 画像の形式：JPEG, GIF, PNG
- 画像のサイズ：最小 24×24 ピクセル、最大 2,048×2,048 ピクセル

なお、ビジュアルアイコンとする画像ファイルは、監視ノードの状態によって背景の色が変わることを考慮した上で、選択または作成してください。

インストール時点での、監視ノードの状態と色（状態色）の対応を次の表に示します。

表 6-2 監視ノードの状態と状態色の対応

監視ノードの状態	状態色 (RGB 値)
緊急	赤 (255, 0, 0)
警戒	
致命的	
エラー	橙 (255, 200, 0)
警告	黄色 (255, 255, 0)
デバッグ	薄い紫 (255, 175, 175)

画像ファイルに状態色と同じ色を使わないようにすることをお勧めします。

4. 監視ノードの【プロパティ】画面を開く。

監視ノードを選択して、次のどれかの方法で【プロパティ】画面を開きます。

- ダブルクリックする（監視オブジェクトの場合だけ有効）。
- 右クリックしてポップアップメニューから【プロパティ】を選択する。
- メニューバーから【編集】－【プロパティ】を選択する。

5. [全般] ページで「ビジュアルアイコン」の【変更】ボタンをクリックする。

【ビジュアルアイコン選択】画面が表示されます。

6. ビジュアルアイコンを選択する。

【ビジュアルアイコン選択】画面で、使用する画像ファイル名を選択して、【OK】ボタンをクリックします。

7. [全般] ページで【OK】ボタンまたは【適用】ボタンをクリックする。

(8) 監視ノードの検索

監視ノードの検索は、階層の深い監視ツリーから目的の監視ノードを探すときに利用できます。手順を次に示します。

1. 監視ノードを選択する。

検索対象となる監視ノードは、選択した監視ノードおよびその下層の監視ノードとなります。

2. [検索] 画面を表示する。

- 右クリックしてポップアップメニューから [検索] を選択する。
- または、メニューバーから [編集] - [検索] を選択する。

3. 検索条件を入力し、[検索] ボタンをクリックする。

検索条件に一致する監視ノードが一覧表示されます。

4. 表示したい監視ノードをダブルクリックする。

検索結果に一覧表示された監視ノードをダブルクリックすると、その監視ノードを選択した状態で [監視ツリー(編集)] 画面が表示されます。

6.3.5 カスタマイズした監視ツリーのローカルホストへの保存

[監視ツリー(編集)] 画面でカスタマイズした監視ツリーは、CSV ファイルとして、ローカルホストに保存できます。監視ツリーの作成を中断したいときや、バックアップ用データとして保管しておきたいときにローカルホストに保存してください。

1. [ツリーを保存] を選択する。

[監視ツリー(編集)] 画面のメニューバーから [ファイル] - [ツリーを保存] を選択します。

2. 任意のフォルダに任意のファイル名で保存する。

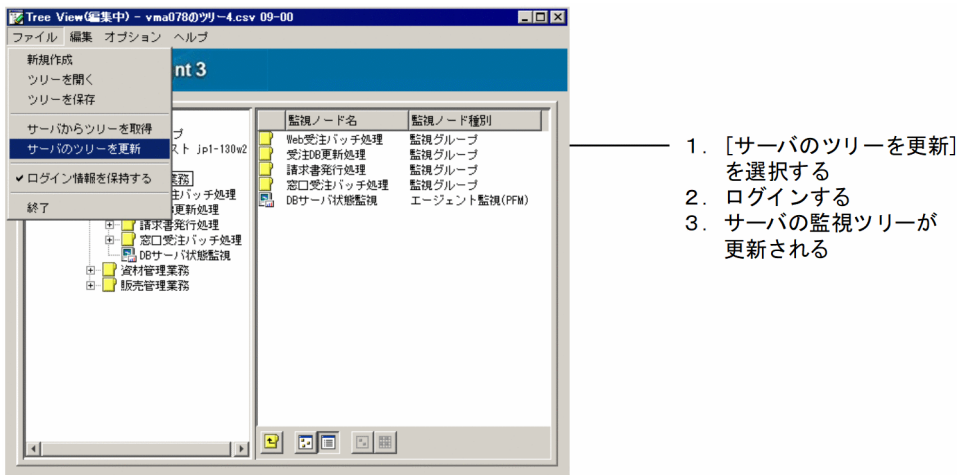
[ツリーを保存] 画面が表示されるので、任意のフォルダ名、任意のファイル名を指定して、保存してください。

6.3.6 カスタマイズした監視ツリーのマネージャーへの反映

[監視ツリー(編集)] 画面でカスタマイズした監視ツリーは、マネージャーに反映すると、システムの運用監視で使用できるようになります。なお、マネージャーへの反映の際に、[監視ツリー(編集)] 画面で監視ツリーの監視範囲設定を有効にしていると、マネージャーでも監視範囲設定が有効になります。

マネージャーへの反映手順を次に示します。

図 6-9 サーバのツリーを更新



1. [サーバのツリーを更新] を選択する。

「監視ツリー(編集集中)」画面のメニューバーから「ファイル」－「サーバのツリーを更新」を選択します。
確認ダイアログボックスが表示されるので、更新してよければ「はい」ボタンをクリックします。

2. サーバにログインする。

JP1/IM - Manager (セントラルスコープ) にログインするための「ログイン」画面が表示されます。
JP1 ユーザー名とパスワードを入力します。JP1 ユーザーは、JP1 資源グループが JP1_Console で、JP1_Console_Admin 権限を持っている必要があります。

接続先ホスト名には、監視ツリーを更新する JP1/IM - Manager のホスト名を入力します。

3. カスタマイズした監視ツリーがサーバに反映される。

反映中にはダイアログボックスが表示され、反映が完了するとダイアログボックスが閉じます。

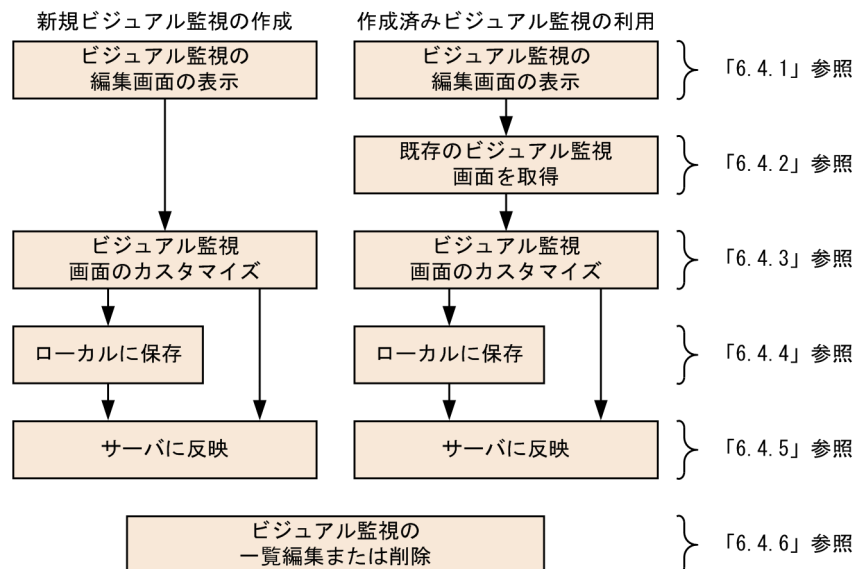
なお、反映した監視ツリーを確認するには、JP1/IM - Manager (セントラルスコープ) にログインして「監視ツリー」画面により確認してください。

6.4 [ビジュアル監視] 画面を GUI で作成する

ここでは、[ビジュアル監視] 画面を GUI で作成する手順について説明します。

作業の流れを次に示します。

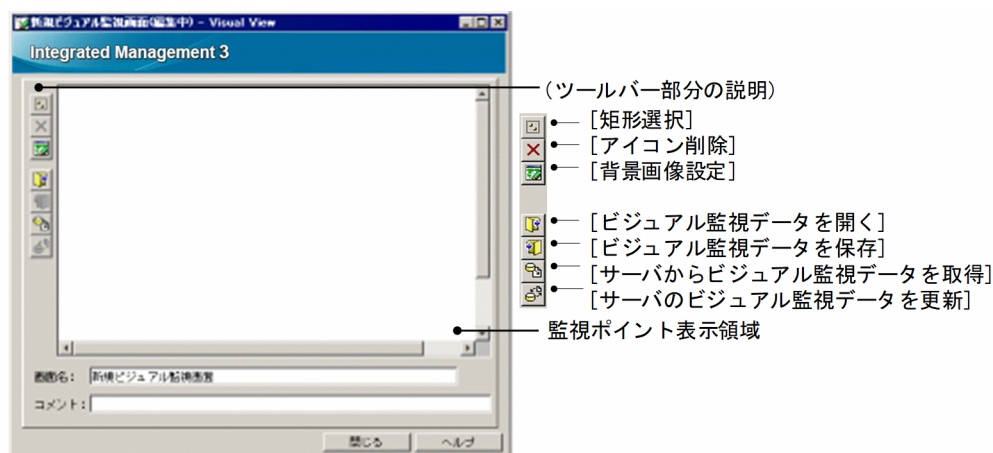
図 6-10 [ビジュアル監視] 画面を GUI で作成する作業の流れ



6.4.1 [ビジュアル監視] 画面の編集画面の起動

[ビジュアル監視] 画面は、[ビジュアル監視(編集)] 画面により編集します。この画面は、[監視ツリー(編集)] 画面から起動します。

図 6-11 [ビジュアル監視(編集)] 画面



1. [監視ツリー(編集)] 画面のメニューバーから [編集] - [新規ビジュアル監視画面作成] を選択する。
[ビジュアル監視(編集)] 画面が起動されます。

6.4.2 既存の【ビジュアル監視】画面の取得

すでに【ビジュアル監視】画面を作成して運用している場合は、まず、マネージャーに接続して、既存の設定を取得します。または、ローカルに保存している【ビジュアル監視】画面の設定（CSV ファイル）がある場合は、それを使用することもできます。

(1) サーバからの【ビジュアル監視】画面の取得

1. 【サーバからビジュアル監視データを取得】を選択する。

【ビジュアル監視(編集集中)】画面のツールバーにある、 をクリックします。

2. サーバにログインする。

JP1/IM - Manager（セントラルスコープ）にログインするための【ログイン】画面が表示されます。

JP1 ユーザー名とパスワードを入力します。JP1 ユーザーは、JP1 資源グループが JP1_Console で、JP1_Console_Admin 権限を持っている必要があります。

接続先ホスト名には、ビジュアル監視データを取得する JP1/IM - Manager のホスト名を入力します。

3. 取得する【ビジュアル監視】画面を選択する。

ログインが成功すると、【ビジュアル監視画面を開く】画面が表示されます。データを取得する【ビジュアル監視】画面を選択して、【OK】ボタンをクリックしてください。

(2) ローカルに保存した【ビジュアル監視】画面（CSV ファイル）の取得

1. 【ビジュアル監視データを開く】画面を開く。

【ビジュアル監視(編集集中)】画面のツールバーにある、 をクリックします。

【ビジュアル監視データを開く】画面が表示されます。

2. 【ビジュアル監視】画面の設定（CSV ファイル）を指定する。

【ビジュアル監視データを開く】画面で、利用する【ビジュアル監視】画面の設定（CSV ファイル）を選択し、【開く】ボタンをクリックします。

確認ダイアログボックスが表示されるので、【はい】ボタンをクリックしてください。

6.4.3 【ビジュアル監視】画面のカスタマイズ

【ビジュアル監視(編集集中)】画面では、【ビジュアル監視】画面を新規作成したり、既存の【ビジュアル監視】画面をカスタマイズしたりできます。【ビジュアル監視】画面に関してできる操作を次に示します。

- 背景画像の設定
- 監視ノードの追加
- 監視ノードの削除

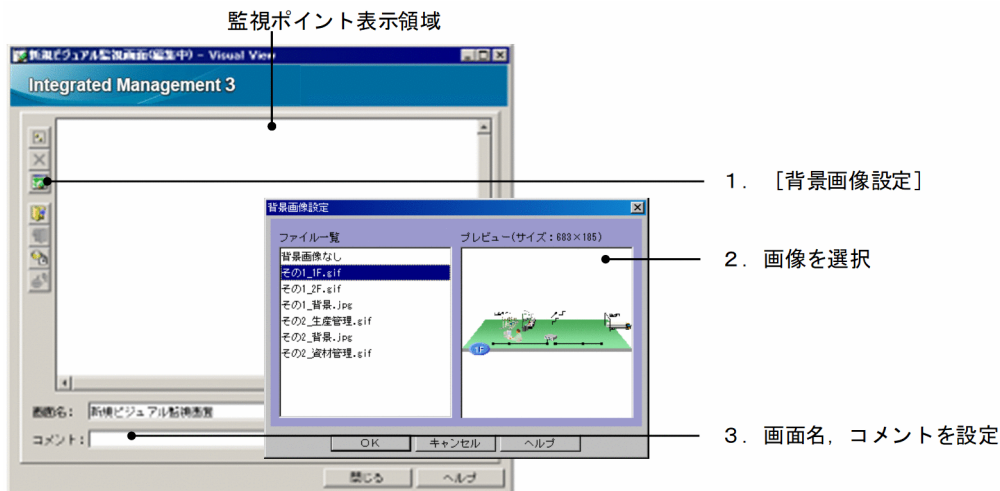
- ・ 監視ノードの属性設定
- ・ 監視ノードの監視状態変更
- ・ 監視ノードの検索

(1) 【ビジュアル監視】 画面の背景画像の設定

【ビジュアル監視】画面の背景に表示される画像を設定します。なお、背景画像には、次のフォルダにある、次のフォーマットのファイルが使用できます。

- ・ 画像ファイルのフォルダ：View パス¥image¥map¥
- ・ 使用できる画像ファイルのフォーマット：JPEG, GIF, PNG

図 6-12 背景画像設定



1. 【背景画像設定】を開く。

次のどちらかの操作をして【背景画像設定】画面を表示します。

- ・ 【ビジュアル監視(編集)】画面のツールバーにある、 をクリックする。
- ・ 監視ポイント表示領域上の何もないところ（監視ノード非選択状態）で右クリックし、ポップアップメニューから【背景画像設定】を選択する。

2. 背景画像を選択する。

【背景画像設定】画面で、背景にする画像ファイル名を選択して、[OK] ボタンをクリックします。

なお、背景を無地（白色）のまま【ビジュアル監視】画面を使うこともできます。この場合は、ファイル選択で【背景画像なし】を選んでください。

選択すると、確認ダイアログボックスが表示されるので [はい] ボタンをクリックします。

3. 【ビジュアル監視】画面に名前を付ける。

背景画像が決まったら、【ビジュアル監視】画面に名前を付けます。

【画面名】と【コメント】の欄に、監視目的や画像にあわせて名前とコメントを入力します。

画面名は「[ビジュアル監視]」画面のタイトルバー部分に、コメントは背景画像の下の部分に表示されます。

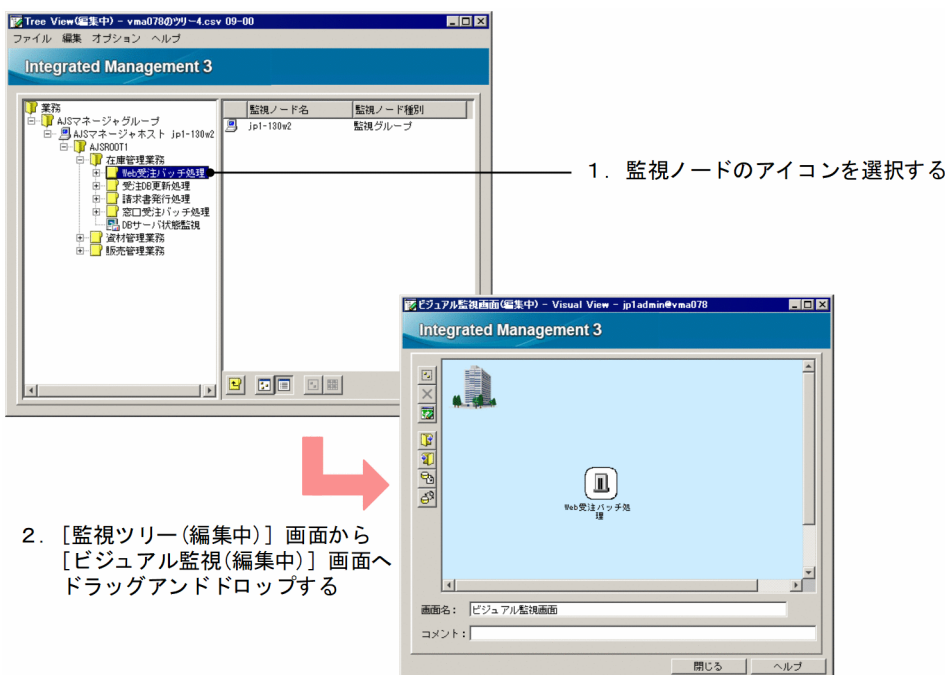
「[ビジュアル監視]」画面の操作のヒント

監視ポイント表示領域で背景画像を選択した状態でドラッグすると、背景画像がマウスの動きにあわせてスクロールします。

(2) 「[ビジュアル監視]」画面への監視ノードの追加

「[ビジュアル監視]」画面の背景画像の上に、監視ノードのアイコンを追加します。監視ノードの追加は、「[監視ツリー]」画面から「[ビジュアル監視]」画面へ、監視ノードのアイコンをドラッグ&ドロップすることで行います。

図 6-13 「[ビジュアル監視]」画面への監視ノードの追加



1. 監視ツリー上の監視ノードを選択する。

「[監視ツリー (編集)]」画面で、「[ビジュアル監視]」画面により監視したい監視ノードを表示し、選択します。

2. 監視ノードを、「[ビジュアル監視]」画面へドラッグ&ドロップする。

監視ノードのアイコンを、「[監視ツリー (編集)]」画面でドラッグ（左クリック）して、「[ビジュアル監視 (編集)]」画面へドロップします。

上記の手順で追加した監視ノードのアイコンは、監視ツリー上の監視ノードの状態と連動して、状態色（障害のときは赤色など）が表示されるようになります。

なお、「[監視ツリー]」画面の表示は、少し経ってから「[ビジュアル監視]」画面に反映されます。

(3) 【ビジュアル監視】 画面からの監視ノードの削除

【ビジュアル監視】 画面から監視ノードを削除するには、次のようにします。

1. 監視ノードのアイコンを選択し、削除する。

次のどちらかの操作をします。なお、複数のアイコンを一括削除する場合は、 を利用して複数選択してください。

- アイコンを選択して、【ビジュアル監視(編集)】画面のツールバーにある  をクリックする。
- アイコンを選択して右クリックして、ポップアップメニューから【アイコン削除】を選択する。

確認ダイアログボックスが表示されるので【はい】 ボタンをクリックします。

(4) 監視ノードの属性設定

【ビジュアル監視(編集)】画面に配置した監視ノードに対し、属性を設定する手順を説明します。

なお、【ビジュアル監視(編集)】画面で監視ノードの属性を設定した場合、その設定内容は【監視ツリー(編集)】画面の該当する監視ノードに反映されます。

1. 監視ノードの【プロパティ】画面を開く。

監視ノードを選択して、次の方法で【プロパティ】画面を開きます。

- 右クリックしてポップアップメニューから【プロパティ】を選択する。

2. 【全般】 ページを設定する。

監視ノード名、使用するアイコン、使用するビジュアルアイコン※¹、背景画像設定（監視グループ限定）、監視状態、JP1 資源グループ※²を設定します。

3. 【基本情報】 ページを設定する。

監視ノードの基本情報について設定します。

4. 【状態変更条件】 ページを設定する。

JP1/IM - Manager がどのような JP1 イベントを受信したときに、監視ノードの状態を変更するかを設定します。

状態変更条件に設定する内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「8. システム監視オブジェクト一覧（セントラルスコープ用）」を参考にしてください。

5. 【イベント発行条件】 ページを設定する。

監視ノードがどの状態になったときに、JP1 イベントを発行するかを設定します。

なお、監視ノードの状態により自動アクションをする場合は、この【イベント発行条件】を設定して、イベント ID が 00003FB0 の JP1 イベントに対して自動アクションをするよう設定してください。

6. 【OK】 ボタンまたは【適用】 ボタンをクリックする。

注※1 ビジュアルアイコンを使用する場合、準備が必要です。手順については、「[6.3.4\(7\) ビジュアルアイコンを使用するための設定](#)」を参照してください。

注※2 監視ツリーの監視範囲設定が有効な場合、設定できる項目です。

プロパティの設定例については、「[6.3.4\(2\) 監視ノードの属性設定](#)」を参照してください。

(5) 監視ノードの監視状態変更

[ビジュアル監視(編集)] 画面に配置した監視ノードに対し、監視状態を変更する手順を説明します。

なお、[ビジュアル監視(編集)] 画面で監視ノードの監視状態を変更した場合、その変更は[監視ツリー(編集)] 画面の該当する監視ノードに反映されます。

1. 監視ノードを選択する。
2. 右クリックしてポップアップメニューから [監視状態変更] を選択し、ユーザーが意図する監視状態に変更する。
確認ダイアログボックスが表示されます。
3. 確認ダイアログボックスで [はい] ボタンをクリックする。

(6) 監視ノードの検索

監視ノードの検索は、階層の深い監視ツリーから目的の監視ノードを探すときに利用できます。手順を次に示します。

1. 監視ノードを選択する。
検索対象となる監視ノードは、選択した監視ノードおよびその下層の監視ノードとなります。
2. [検索] 画面を表示する。
右クリックしてポップアップメニューから [検索] を選択します。
3. 検索条件を入力し、[検索] ボタンをクリックする。
検索条件に一致する監視ノードが一覧表示されます。
4. 一覧表示された監視ノードから [ビジュアル監視] 画面で監視したい監視ノードを選択し、[ビジュアル監視(編集)] 画面にドラッグ&ドロップする。

6.4.4 カスタマイズした [ビジュアル監視] 画面のローカルホストへの保存

[ビジュアル監視(編集)] 画面でカスタマイズした [ビジュアル監視] 画面は、CSV ファイルとして、ローカルホストに保存できます。[ビジュアル監視] 画面の作成を中断したいときや、バックアップ用データとして保管しておきたいときにローカルホストに保存してください。

1. [ビジュアル監視データを保存] を選択する。

[ビジュアル監視(編集集中)] 画面のツールバーにある、 をクリックします。

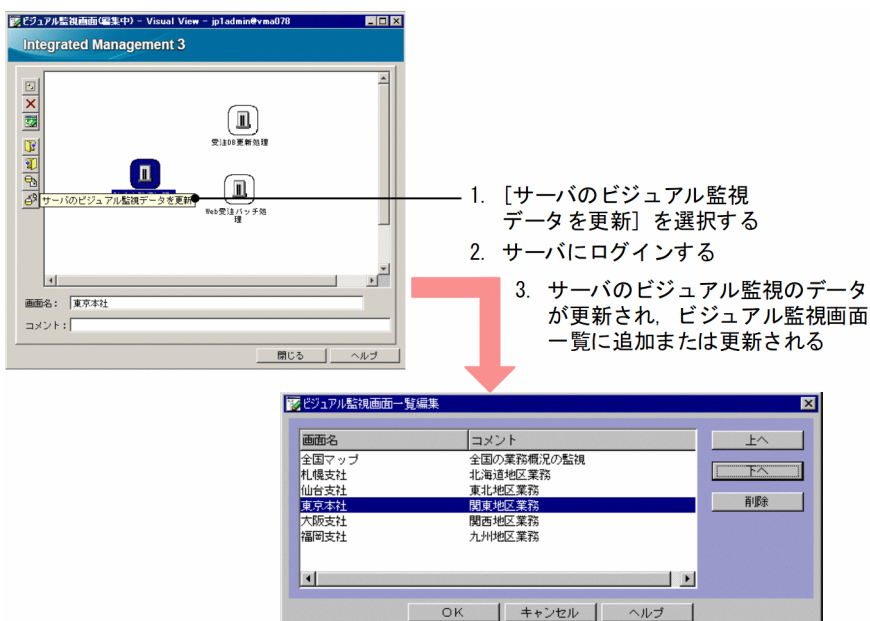
2. 任意のフォルダに任意のファイル名で保存する。

[ビジュアル監視データを保存] 画面が表示されるので、任意のフォルダ名、任意のファイル名を指定して、保存してください。

6.4.5 カスタマイズした [ビジュアル監視] 画面のマネージャーへの反映

[ビジュアル監視(編集集中)] 画面でカスタマイズした [ビジュアル監視] 画面は、マネージャーに反映すると、システムの運用監視で使用できるようになります。マネージャーへの反映手順を次に示します。

図 6-14 サーバのビジュアル監視データを更新



1. [サーバのビジュアル監視データを更新] を選択する。

[ビジュアル監視(編集集中)] 画面のツールバーにある、 をクリックします。

確認ダイアログボックスが表示されるので [はい] ボタンをクリックします。

2. サーバにログインする。

JP1/IM - Manager (セントラルスコープ) にログインするための [ログイン] 画面が表示されます。

JP1 ユーザー名とパスワードを入力します。JP1 ユーザーは、JP1 資源グループが JP1_Console で、JP1_Console_Admin 権限を持っている必要があります。

接続先ホスト名には、JP1/IM - Manager のホスト名を入力します。

3. カスタマイズした [ビジュアル監視] 画面がサーバに反映される。

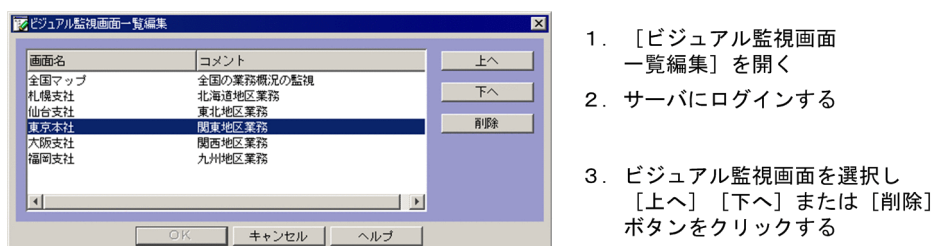
反映中にはダイアログボックスが表示され、反映が完了するとダイアログボックスが閉じます。反映が終わると、[ビジュアル監視] 画面は、ビジュアル画面一覧に追加または更新されます。

なお、反映した [ビジュアル監視] 画面を確認するには、JP1/IM - Manager (セントラルスコープ) にログインして [ビジュアル監視] 画面により確認してください。

6.4.6 [ビジュアル監視] 画面の一覧の編集および削除

[ビジュアル監視画面一覧編集] 画面により、[ビジュアル監視] 画面の一覧を編集する手順、および [ビジュアル監視] 画面を削除する手順を説明します。

図 6-15 [ビジュアル監視] 画面の一覧の編集および削除



1. [ビジュアル監視画面一覧編集] を開く
2. サーバにログインする
3. ビジュアル監視画面を選択し [上へ] [下へ] または [削除] ボタンをクリックする

1. [ビジュアル監視画面一覧編集] を開く。

[監視ツリー(編集)] 画面のメニューバーから [編集] - [ビジュアル監視画面一覧編集] を選択します。

2. サーバにログインする。

JP1/IM - Manager (セントラルスコープ) にログインするための [ログイン] 画面が表示されます。JP1 ユーザー名とパスワードを入力します。JP1 ユーザーは、JP1 資源グループが JP1_Console で、JP1_Console_Admin 権限を持っている必要があります。

接続先ホスト名には、JP1/IM - Manager のホスト名を入力します。

3. [ビジュアル監視] 画面を選択し、表示位置の移動または削除する。

[ビジュアル監視画面一覧編集] 画面で、[ビジュアル監視] 画面の画面名を選択して、[上へ] や [下へ]、または [削除] ボタンをクリックします。この時点では、まだ編集画面の表示が変更されただけで、サーバ上のデータは変更されていません。変更をやめるには [キャンセル] をクリックします。

[OK] ボタンが、非活性状態から活性状態になっているので、クリックします。この時点で、一覧画面の表示が更新され、[削除] ボタンをクリックした場合は [ビジュアル監視] 画面のデータがサーバ上から消えます。

6.5 保存した CSV ファイルを編集して [監視ツリー] 画面を作成

ローカルに保存した CSV ファイルを編集することで、多くの監視ノードの環境設定をまとめて変更できます。

設定手順については、次の説明を参照してください。

CSV ファイルによる監視画面（[監視ツリー] 画面）の作成

- CSV ファイルとして監視画面の設定の保存

参照先：「[6.3.5 カスタマイズした監視ツリーのローカルホストへの保存](#)」

- CSV ファイルからの監視画面の作成

参照先：「[6.3.4 監視ツリーのカスタマイズ](#)」

- ツリー構成ファイルの詳細

参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ツリー構成ファイル」（2. 定義ファイル）

6.6 ガイド情報の編集

ガイド情報は、システム監視中に問題が発生したときに「ガイド」画面に表示する情報です。ガイド情報として、問題の対処方法のアドバイスなどを表示することで、問題が発生したときの初動対応でのシステム管理者の負担を軽減することができます。また、その監視ノードが、どの業務の何を監視しているものを説明するためのガイドとしても利用できます。

ガイド情報として表示する内容は、JP1/IM - Manager のホストにあるガイド情報ファイルに設定します。

ここでは、ガイド情報の編集方法について説明します。

ガイド情報として設定する内容や、ガイド機能については、下記を参照してください。

ガイド情報の機能、設定について

- ガイド情報について設定する内容、ガイド機能について
参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5.8 ガイド機能」
- ガイド情報ファイルの書式について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ガイド情報ファイル (jcs_guide_XXX.txt)」(2. 定義ファイル)

6.6.1 ガイド情報の編集の手順

編集手順を次に示します。

1. ガイド情報ファイルを編集する。

ガイド情報ファイルは、TXT 形式のファイルです。次のファイルをテキストエディターで開き、編集してください。

表 6-3 JP1/IM - Manager の動作する言語コードとガイド情報ファイルの対応

OS	言語種別	JP1/IM - Manager の 動作する言語コード	編集するガイド情報ファイル
Windows ※1	日本語※2		Scope パス¥conf¥jcs_guide_sjis.txt
			共有フォルダ¥jp1scope¥conf¥jcs_guide_sjis.txt
	英語※3		Scope パス¥conf¥jcs_guide.txt
			共有フォルダ¥jp1scope¥conf¥jcs_guide.txt
	中国語※4		Scope パス¥conf¥jcs_guide_GB18030.txt※5
			共有フォルダ¥jp1scope¥conf¥jcs_guide_GB18030.txt※5
UNIX※1	日本語	シフト JIS コード	/etc/opt/jp1scope/conf/jcs_guide_sjis.txt

OS	言語種別	JP1/IM - Manager の 動作する言語コード	編集するガイド情報ファイル
			共有ディレクトリ/jp1scope/conf/jcs_guide_sjis.txt
		EUC コード	/etc/opt/jp1scope/conf/jcs_guide_euc.txt
			共有ディレクトリ/jp1scope/conf/jcs_guide_euc.txt
		UTF-8 コード	/etc/opt/jp1scope/conf/jcs_guide_UTF-8.txt
			共有ディレクトリ/jp1scope/conf/jcs_guide_UTF-8.txt
	英語		/etc/opt/jp1scope/conf/jcs_guide.txt
			共有ディレクトリ/jp1scope/conf/jcs_guide.txt
	中国語		/etc/opt/jp1scope/conf/jcs_guide_GB18030.txt※5
			共有ディレクトリ/jp1scope/conf/jcs_guide_GB18030.txt※5

注※1

JP1/IM - Manager の動作する言語コードによって、編集するガイド情報ファイルが異なります。言語コードに対応したガイド情報ファイルを編集してください。なお、非サポートの言語コードに対応するガイド情報ファイルは同梱されていません。

また、ガイドメッセージファイルを利用する場合は、テキストエディターなどを使ってガイドメッセージファイルを作成してください。

注※2

日本語 OS では、この言語コードで動作します。

注※3

英語 OS では、この言語コードで動作します。

注※4

中国語 OS では、この言語コードで動作します。

注※5

ユーザー自身で作成するファイルです。インストール時に作成されません。

2. JP1/IM - Manager をリロードまたは再起動して、ガイド情報の設定内容を有効にする。

ガイド情報ファイルは、JP1/IM - Manager をリロードまたは起動したときに読み込まれます。次のどちらかをしてください。

- jco_spmd_reload コマンドを実行して、JP1/IM - Manager をリロードする。
- JP1/IM - Manager を停止して、起動する。

3. ガイド情報の読み込みが成功したことを確認する。

JP1/IM - Manager がガイド情報ファイルを読み込むときに、ガイド情報ファイルに記述誤りがあるとエラーが発生します。統合トレースログを参照して、ガイド情報ファイルの読み込みが成功したことを確認してください。

表 6-4 統合トレースログのディレクトリ

OS	統合トレースログ
Windows	システムドライブ:¥Program Files¥Hitachi¥HNTRLib2¥spool¥※
UNIX	/var/opt/hitachi/HNTRLib2/spool/

注※ Windows の場合、「システムドライブ:¥Program Files」と表記している部分は、インストール時の OS 環境変数によって決定されるため、環境によって異なる場合があります。

ガイド情報ファイルの読み込みが成功した場合は、次のメッセージが統合トレースに記録されます。このメッセージが記録されていることを確認してください。

- KAVB7393-I（再起動した場合）
- KAVB7394-I（リロードした場合）

ガイド情報ファイルにエラーがあった場合は、KAVB7377-W から KAVB7392-W のメッセージが統合トレースに記録されます。エラーが発生している場合は、メッセージの示すエラーを見直して修正してください。そのあと、再度 JP1/IM - Manager をリロードまたは再起動してください。

6.7 セントラルスコープの動作環境の設定

ここでは、セントラルスコープの動作環境の設定手順について説明します。

6.7.1 状態変更イベント件数の上限監視の設定

監視オブジェクトの状態変更イベントが上限（100 件）を超えると、警告の JP1 イベントが発行されます。

JP1/IM - Manager を新規インストールした場合は、有効（JP1 イベントを発行する）になっています。バージョンアップ時は、バージョンアップ前に設定を無効にしていた場合は、無効（JP1 イベントを発行しない）になっています。運用にあわせて、設定を変更してください。

1. JP1/IM - Manager を停止する。

2. 次のファイルを引数に `jbssetcnf` コマンドを実行する。

状態変更イベントの件数が上限を超えた場合に、JP1 イベントを発行する：`evhist_warn_event_on.conf`

状態変更イベントの件数が上限を超えた場合に、JP1 イベントを発行しない：

`evhist_warn_event_off.conf`

`jbssetcnf` コマンドを実行すると、JP1 共通定義情報に設定内容が反映されます。

`jbssetcnf` コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「状態変更イベント件数の上限監視設定ファイル（`evhist_warn_event_XXX.conf`）」（2. 定義ファイル）を参照してください。

3. JP1/IM - Manager を起動する。

6.7.2 対処済み連動機能の設定

対処済み連動機能は、JP1 イベントの対処状況に応じて、監視オブジェクトの状態を自動的に変更する機能です。

JP1 イベントの対処状況に連動して、監視オブジェクトの状態が変わるため、監視オブジェクト、監視グループの状態を手動で変更する手間が省け、セントラルスコープでの操作がより簡易になります。

JP1/IM - Manager を新規インストールした場合は、有効になっています。バージョンアップ時は、バージョンアップ前に設定を無効にしていた場合は、無効になっています。運用にあわせて、設定を変更してください。

1. JP1/IM - Manager を停止する。

2. 次のファイルを引数に `jbssetcnf` コマンドを実行する。

対処済み連動機能を有効にする：action_complete_on.conf

対処済み連動機能を無効にする：action_complete_off.conf

jbssetcnf コマンドを実行すると、JP1 共通定義情報に設定内容が反映されます。

jbssetcnf コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「対処済み連動設定ファイル (action_complete_XXX.conf)」(2. 定義ファイル) を参照してください。

3. JP1/IM - Manager を起動する。

6.7.3 JP1 イベントの対処済み時に状態変更イベントを自動で削除するための設定

JP1 イベントの対処済み時に、監視オブジェクトの状態変更イベントを自動で削除するための設定です。

JP1/IM - Manager を新規インストールした場合は、無効になっています。バージョンアップ時は、バージョンアップ前に設定を有効にしていた場合は、有効になっています。運用にあわせて、設定を変更してください。

1. 次のどれかの方法で監視ツリー中のすべての状態変更イベントを削除する。

- [監視ツリー] 画面からの操作またはjcshstat コマンドで、監視ツリー中のすべての監視ノードを初期状態にする。
- [監視ツリー(編集中)] 画面から [ファイル] - [サーバのツリーを更新] を実行し、監視ツリーを更新する。
- jcsdbimport コマンドで、監視ツリーを更新する。

2. JP1/IM - Manager を停止する。

3. 状態変更イベント自動削除設定ファイルを作成する。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「状態変更イベント自動削除設定ファイル」(2. 定義ファイル) を参照してください。

4. 手順 3 で設定したファイルを引数に jbssetcnf コマンドを実行する。

jbssetcnf コマンドを実行すると、JP1 共通定義情報に設定内容が反映されます。

jbssetcnf コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

5. JP1/IM - Manager を起動する。

6.7.4 JP1 イベント受信時に監視オブジェクトを初期化するための設定

JP1 イベント受信時に監視オブジェクトを初期化するための設定です。

JP1/IM - Manager を新規インストールした場合は、無効になっています。バージョンアップ時は、バージョンアップ前に設定を有効にしていた場合は、有効になっています。運用にあわせて、設定を変更してください。

1. JP1/IM - Manager を停止する。
2. 監視オブジェクト初期化設定ファイルを作成する。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「監視オブジェクト初期化設定ファイル」(2. 定義ファイル) を参照してください。

3. 2 で設定したファイルを引数に `jbssetcnf` コマンドを実行する。

`jbssetcnf` コマンドを実行すると、JP1 共通定義情報に設定内容が反映されます。

`jbssetcnf` コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

4. JP1/IM - Manager を起動する。

6.7.5 状態変更条件メモリー常駐機能の設定

状態変更条件をメモリーに常駐させる機能の設定です。

JP1/IM - Manager を新規インストールした場合は、有効になっています。バージョンアップ時は、バージョンアップ前に設定を無効にしていた場合は、無効になっています。運用にあわせて、設定を変更してください。

1. JP1/IM - Manager を停止する。
2. 状態変更条件メモリー常駐機能の設定ファイルを作成する。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「状態変更条件メモリー常駐機能の設定ファイル」(2. 定義ファイル) を参照してください。

3. 2 で設定したファイルを引数に `jbssetcnf` コマンドを実行する。

`jbssetcnf` コマンドを実行すると、JP1 共通定義情報に設定内容が反映されます。

`jbssetcnf` コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

4. JP1/IM - Manager を起動する。

6.7.6 【監視ツリー】画面のツールバーのカスタマイズ

【監視ツリー】画面をカスタマイズして、ツールバーにプログラム（アイコン）を追加する手順を次に示します。

なお、カスタマイズ内容は、次に JP1/IM - Manager（セントラルスコープ）にログインしたときから有効になります。

1. アイコンを次のフォルダに格納する。

View パス¥image¥sovtool

2. アイコンから起動するプログラムを任意のフォルダに格納する。

3. 起動プログラム定義ファイル（!JP1_CS_APP0.conf）を編集する。

起動プログラム定義ファイル（!JP1_CS_APP0.conf）は次のフォルダに格納されています。

View パス¥conf¥sovtool¥exec¥ja¥

4. ツールバー定義ファイル（!JP1_CS_FT00L0.conf）を編集する。

ツールバー定義ファイル（!JP1_CS_FT00L0.conf）は次のフォルダに格納されています。

View パス¥conf¥sovtool¥item¥ja¥

5. アイコン動作定義ファイル（!JP1_CS_FTREE0.conf）を編集する。

アイコン動作定義ファイル（!JP1_CS_FTREE0.conf）は次のフォルダに格納されています。

View パス¥conf¥sovtool¥item¥ja¥

【監視ツリー】画面のカスタマイズについて

- 起動プログラム定義ファイル（!JP1_CS_APP0.conf）について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「起動プログラム定義ファイル（!JP1_CS_APP0.conf）」（2. 定義ファイル）
- ツールバー定義ファイル（!JP1_CS_FT00L0.conf）について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「ツールバー定義ファイル（!JP1_CS_FT00L0.conf）」（2. 定義ファイル）
- アイコン動作定義ファイル（!JP1_CS_FTREE0.conf）について
参照先：マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「アイコン動作定義ファイル（!JP1_CS_FTREE0.conf）」（2. 定義ファイル）

6.7.7 監視ノード名および監視ノードアイコン余白の表示を抑止するための設定

監視ノードのアイコンの監視ノード名、およびアイコン余白の表示を抑止する手順を、反映したい画面ごとに示します。

(1) 監視ノード名および監視ノードアイコン余白の表示を抑止する（[監視ツリー] 画面のマップ表示および [ビジュアル監視] 画面の場合）

[監視ツリー] 画面のマップ表示, および [ビジュアル監視] 画面で, 監視ノード名, およびアイコン余白の表示を抑止する手順を示します。この設定は, JP1/IM - Manager (セントラルスコープ) にログインしたときから有効になります。

1. システムプロファイル (セントラルスコープ) (`jcs_sysprofile_xxx.def`) をテキストエディターで開く。
システムプロファイル (セントラルスコープ) (`jcs_sysprofile_xxx.def`) は次のフォルダに格納されています。

- Windows の場合 (物理ホストのとき)
Scope パス¥conf
- Windows の場合 (論理ホストのとき)
共有フォルダ¥jp1scope¥conf
- UNIX の場合 (物理ホストのとき)
/etc/opt/jp1scope/conf
- UNIX の場合 (論理ホストのとき)
共有ディレクトリ/jp1scope/conf

2. FrameVisible パラメーターの内容を編集する。

ファイルの設定内容について

ファイルの設定内容については, マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「システムプロファイル (セントラルスコープ) (`jcs_sysprofile_xxx.def`)」(2. 定義ファイル) を参照してください。

(2) 監視ノード名および監視ノードアイコン余白の表示を抑止する（[監視ツリー(編集)] 画面のマップ表示および [ビジュアル監視(編集)] 画面の場合）

[監視ツリー(編集)] 画面のマップ表示, および [ビジュアル監視(編集)] 画面で監視ノード名, およびアイコン余白の表示を抑止する手順を示します。この設定は, [監視ツリー(編集)] 画面, または [ビジュアル監視(編集)] 画面を表示したときから有効になります。

1. システムプロファイル (セントラルスコープ・ビューアー) (`system.conf`) をテキストエディターで開く。

システムプロファイル (セントラルスコープ・ビューアー) (`system.conf`) は次のフォルダに格納されています。

- 日本語 OS の場合
View パス¥conf¥sovsystem¥ja

- 英語 OS の場合

View パス¥conf¥sovsystem¥en

- 中国語 OS の場合

View パス¥conf¥sovsystem¥zh

2. FrameVisible パラメーターの内容を編集する。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「システムプロファイル（セントラルスコープ・ビューアー）（system.conf）」（2. 定義ファイル）を参照してください。

6.7.8 監視ノード名の状態色および監視ノードの状態色の設定

監視ノード名の状態色および監視ノードの状態色を設定する手順を、反映したい画面ごとに示します。

(1) 監視ノード名の状態色および監視ノードの状態色を設定する（[監視ツリー] 画面および [ビジュアル監視] 画面の場合）

[監視ツリー] 画面、および [ビジュアル監視] 画面で、監視ノード名の状態色および監視ノードの状態色を設定する手順を説明します。この設定は、JP1/IM - Manager（セントラルスコープ）にログインしたときから有効になります。

1. システムプロファイル（セントラルスコープ）（jcs_sysprofile_XXX.def）をテキストエディターで開く。
システムプロファイル（セントラルスコープ）（jcs_sysprofile_XXX.def）は次のフォルダに格納されています。

- Windows の場合（物理ホストのとき）
Scope パス¥conf
- Windows の場合（論理ホストのとき）
共有フォルダ¥jp1scope¥conf
- UNIX の場合（物理ホストのとき）
/etc/opt/jp1scope/conf
- UNIX の場合（論理ホストのとき）
共有ディレクトリ/jp1scope/conf

2. 状態色を変更したい状態について定義された[ColorItem]～[End]の内容を編集する。

監視ノード名の状態色を設定したい場合は、[TEXT]～[End]の RGB 値を編集します。

監視ノードの状態色を設定したい場合は、[Label]～[End]の RGBA 値を編集します。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「システムプロファイル（セントラルスコープ）（jcs_sysprofile_XXX.def）」（2. 定義ファイル）を参照してください。

(2) 監視ノード名の状態色および監視ノードの状態色を設定する（[監視ツリー(編集)中] 画面および [ビジュアル監視(編集)中] 画面の場合）

[監視ツリー(編集)中] 画面、および [ビジュアル監視(編集)中] 画面で監視ノード名の状態色、および監視ノードの状態色を設定する手順を示します。この設定は、[監視ツリー(編集)中] 画面、または [ビジュアル監視(編集)中] 画面を表示したときから有効になります。なお、初期状態に対する状態色の設定だけが画面に反映されます。

1. システムプロファイル（セントラルスコープ・ビューアー）（system.conf）をテキストエディターで開く。

システムプロファイル（セントラルスコープ・ビューアー）（system.conf）は次のフォルダに格納されています。

- 日本語 OS の場合
View パス¥conf¥sovsystem¥ja
- 英語 OS の場合
View パス¥conf¥sovsystem¥en
- 中国語 OS の場合
View パス¥conf¥sovsystem¥zh

2. 初期状態について定義された[ColorItem]～[End]の内容を編集する。

監視ノード名の状態色を設定したい場合は、[TEXT]～[End]の RGB 値を編集します。

監視ノードの状態色を設定したい場合は、[Label]～[End]の RGBA 値を編集します。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「システムプロファイル（セントラルスコープ・ビューアー）（system.conf）」（2. 定義ファイル）を参照してください。

6.7.9 監視ノードのアイコンの移動を抑止するための設定

[監視ツリー] 画面のマップ表示、および [ビジュアル監視] 画面で、監視ノードのアイコンの移動を抑止する手順を説明します。この設定は、JP1/IM - Manager（セントラルスコープ）にログインしたときから有効になります。

1. システムプロファイル（セントラルスコープ）（jcs_sysprofile_XXX.def）をテキストエディターで開く。

システムプロファイル（セントラルスコープ）（jcs_sysprofile_xxx.def）は次のフォルダに格納されています。

- Windows の場合（物理ホストのとき）
Scope パス¥conf
- Windows の場合（論理ホストのとき）
共有フォルダ¥jp1scope¥conf
- UNIX の場合（物理ホストのとき）
/etc/opt/jp1scope/conf
- UNIX の場合（論理ホストのとき）
共有ディレクトリ/jp1scope/conf

2. Movable パラメーターの内容を編集する。

ファイルの設定内容について

ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「システムプロファイル（セントラルスコープ）（jcs_sysprofile_xxx.def）」（2. 定義ファイル）を参照してください。

6.8 連携製品のセットアップ

ここでは、セントラルスコープと連携するための連携製品のセットアップについて説明します。

セントラルスコープでは、各製品との連携を容易にするため、システム監視オブジェクト（監視に必要な基本的な定義をあらかじめ設定している監視オブジェクト）および監視ツリーの自動生成機能を提供しています。

このシステム監視オブジェクトを使って、各製品を監視する場合、および監視ツリーを自動生成により作成する場合には、ここで説明するセットアップをしてください。

なお、連携製品は、すでにインストールされているものとして説明します。

各製品と連携セットアップの概要

各製品と連携するためのセットアップ作業について、概要を説明します。

- システムの階層構成（IM 構成）を定義する

IM 構成管理を使用している場合は、IM 構成管理・ビューアーを操作して、連携製品を実行するホストを JP1/IM の管理対象として登録します。

IM 構成管理を使用していない場合は、コマンドを実行して、連携製品を実行するホストを JP1/IM の管理対象として登録します。

- 連携製品で、JP1 イベント発行を有効にする（連携製品の設定）

JP1/IM では JP1 イベントによりシステムを監視するため、各連携製品が JP1 イベントを発行するように、連携製品で設定します。

- SNMP トラップ変換を設定する（JP1/Base の設定）

連携する製品がバージョン 8 以前の JP1/Cm2/SSO やバージョン 8 以前の JP1/Cm2/NNM の場合、JP1 イベントは発行せずに SNMP トラップを発行します。JP1/IM で監視できるように、SNMP トラップを JP1 イベントに変換するように、JP1/Base で設定します。

- 連携用プログラムをセットアップする（連携製品の設定）

監視ツリーの自動生成に対応している製品では、自動生成のときに定義情報を収集する機能（連携用プログラム）を、連携製品でセットアップします。

6.8.1 JP1/AJS との連携でのセットアップ

(1) システム監視オブジェクトで監視するためのセットアップ

JP1/AJS のシステム監視オブジェクトを使用するためには、JP1/AJS が JP1 イベントを発行するようにセットアップする必要があります。

連携のセットアップについては、次のマニュアルを参照してください。

- JP1/AJS の説明

参照先：マニュアル「JP1/Automatic Job Management System 3 連携ガイド」の JP1/IM を使った監視の章

(2) 監視ツリーを自動生成するためのセットアップ

JP1/AJS は、監視ツリーの自動生成に対応しています。自動生成の連携を有効にするには、連携用プログラムをセットアップします。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- JP1/AJS の説明

参照先：マニュアル「JP1/Automatic Job Management System 3 連携ガイド」の JP1/IM を使った監視の章

(a) JP1/AJS - Manager のホストの場合

1. JP1/AJS の連携用プログラムをセットアップする。

監視ツリーの自動生成をするときに、JP1/AJS から定義情報を収集できるようにするため、次のコマンドを実行します。

```
ajs_adapter_setup -i （自動生成の連携を有効にする場合）
```

上記のセットアップをしていない場合は、監視ツリーの自動生成をしても JP1/AJS の監視オブジェクトは生成されません。

また、次のコマンドを実行すると連携を解除することができます。

```
ajs_adapter_setup -u （自動生成の連携を解除する場合）
```

(b) JP1/AJS - Agent のホストの場合

JP1/AJS - Agent のホストでは、連携用プログラムのセットアップは不要です。JP1/AJS - Manager でセットアップをしておけば、セントラルスコープで監視ツリーの自動生成をしたときに収集するジョブネットの定義により、ジョブ実行ホストを抽出して自動的に監視ツリーにします。

6.8.2 JP1/Cm2/SSO との連携でのセットアップ

ここでは、バージョン 8 以前の JP1/Cm2/SSO と連携する場合のセットアップについて説明します。

(1) システム監視オブジェクトで監視するためのセットアップ

バージョン 8 以前の JP1/Cm2/SSO と連携するには、JP1/Cm2/SSO がバージョン 8 以前の JP1/Cm2/NNM 経由で発行する SNMP トラップを JP1 イベントに変換して、それをセントラルスコープで監視できるように設定します。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- バージョン 8 以前の JP1/Cm2/SSO の説明
参照先：マニュアル「JP1/Cm2/SNMP System Observer」
- バージョン 8 以前の JP1/Cm2/NNM の説明
参照先：マニュアル「JP1/Cm2/Network Node Manager ネットワーク管理ガイド」
- SNMP トラップの JP1 イベントへの変換の説明
参照先：マニュアル「JP1/Base 運用ガイド」のイベント変換機能の設定の説明

(a) JP1/Cm2/SSO のホストの場合

バージョン 8 以前の JP1/Cm2/SSO（およびバージョン 8 以前の JP1/Cm2/NNM）がインストールされているマネージャーでは、次のようにセットアップします。

1. JP1/Base の SNMP トラップ変換機能を設定する。

SNMP トラップを JP1 イベントに変換するため、JP1/Base の SNMP トラップ変換機能の設定をします。JP1/Base の SNMP トラップ変換機能の設定は、バージョン 8 以前の JP1/Cm2/NNM と連携する場合と同じです。

SNMP トラップ変換機能の設定手順については、マニュアル「JP1/Base 運用ガイド」のイベント変換機能の設定の章を参照してください。

設定手順の概要を次に示します。

- NNM と JP1/Base の連携を設定（imevtgw_setup を実行）する
- NNM の URL を設定する
- JP1 イベントの送信先を設定する
- フィルター定義ファイル（snmpfilter.conf）を設定する

2. JP1/Base の SNMP トラップ変換機能のフィルター定義ファイルを編集する。

JP1/Base の SNMP トラップ変換機能のフィルター定義ファイル（snmpfilter.conf）に、セントラルスコープで扱う SNMP トラップを変換するための設定を記述したサンプルファイル（snmpfilter_im_sample.conf）の内容を追加します。

ファイル名は次のとおりです。

- SNMP トラップ変換機能のフィルター定義ファイル

Windows の場合：

Base パス¥conf¥evtgw¥snmpfilter.conf

UNIX の場合：

/etc/opt/jp1base/conf/evtgw/snmpfilter.conf

- セントラルスコープのサンプルファイル

Windows の場合：

Scope パス¥conf¥snmpfilter_im_sample.conf

UNIX の場合：

❗ 重要

- サンプルファイルの行頭にある[+]は SNMP トラップのバリアブルバインディングを JP1 イベントに取り込む設定です。外さないでください。
- フィルター定義ファイルのサイズには制限があります。そのため、サンプルファイルの定義のうち、お客様の環境で監視対象とする SNMP トラップに関する定義だけをフィルター定義ファイルに追加してください。
フィルター定義ファイルのサイズの制限については、マニュアル「JP1/Base 運用ガイド」を参照してください。

1. JP1/Cm2/SSO のデーモン動作定義ファイルを設定する。

バージョン 8 以前の JP1/Cm2/SSO のデーモン動作定義ファイル（ssoapmon.def および ssocolmng.def）の設定を編集し、SNMP トラップにセントラルスコープが必要とする情報を含まれるように設定します。

次の二つのファイルを設定してください。

- 設定するファイル

JP1/Cm2/SSO のインストール先フォルダ%conf%ssoapmon.def

- 設定内容

プロセス状態変更イベント発行（threshold-event）の設定、およびバリアブルバインディングにソース名を取り込む（source-name）設定をします。

threshold-event: on

source-name: on

- 設定するファイル

JP1/Cm2/SSO のインストール先フォルダ%conf%ssocolmng.def

- 設定内容

リソースしきい値監視状態変更イベント発行の設定をします。

threshold-event: on

(2) 監視ツリーを自動生成するためのセットアップ

バージョン 8 以前の JP1/Cm2/SSO は、監視ツリーの自動生成に対応しています。自動生成の連携を有効にするには、連携用プログラムをセットアップします。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- バージョン 8 以前の JP1/Cm2/SSO の説明

参照先：マニュアル「JP1/Cm2/SNMP System Observer」

- バージョン 8 以前の JP1/Cm2/NNM の説明

参照先：マニュアル「JP1/Cm2/Network Node Manager ネットワーク管理ガイド」

- SNMP トラップの JP1 イベントへの変換の説明

参照先：マニュアル「JP1/Base 運用ガイド」のイベント変換機能の設定の説明

(a) JP1/Cm2/SSO のホストの場合

1. JP1/Cm2/SSO の連携用プログラムをセットアップする。

監視ツリーの自動生成をするときに、バージョン 8 以前の JP1/Cm2/SSO から定義情報を収集できるようにするため、次のコマンドを実行します。

```
ssoimsetup -install （自動生成の連携を有効にする場合）
```

上記のセットアップをしていない場合は、監視ツリーの自動生成をしてもバージョン 8 以前の JP1/Cm2/SSO の監視オブジェクトは生成されません。

また、次のコマンドを実行すると連携を解除することができます。

```
ssoimsetup -uninstall （自動生成の連携を解除する場合）
```

なお、監視ツリーの自動生成で、バージョン 8 以前の JP1/Cm2/SSO の監視オブジェクトを自動生成するには、次の条件があります。

- バージョン 8 以前の JP1/Cm2/SSO の自動生成を行う場合には、SSO の [リソース収集条件設定] 画面および [プロセス監視条件設定] 画面を閉じておく必要があります。画面を開いていると、SSO の定義情報取得に失敗します。
- バージョン 8 以前の JP1/Cm2/SSO の自動生成で取得する定義情報は、収集状態が「収集中」となっているリソース情報です。

6.8.3 JP1/PFM との連携でのセットアップ

(1) システム監視オブジェクトで監視するためのセットアップ

JP1/PFM のシステム監視オブジェクトを使用するには、JP1/PFM が JP1 イベントを発行するように、次の設定をしてください。また、JP1/PFM は、監視ツリーの自動生成に対応しています。自動生成の連携を有効にするには、連携用プログラムをセットアップしてください。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- JP1/PFM の説明

参照先：マニュアル「JP1/Performance Management 運用ガイド」の JP1/IM との連携の説明

(a) JP1/PFM - Manager のホストの場合

JP1/PFM - Manager がインストールされているマネージャーでは、次のようにセットアップします。

1. JP1/PFM の JP1 イベント発行を有効にする。

アラームの定義の、コマンド実行のアクションで JP1 イベントを発行するように設定してください。

- JP1 イベントを発行する `jpcimevt` コマンドの引数で、設定している属性を外したり、属性値にデフォルトとは異なる値を入れたりすると、システム監視オブジェクトの状態を監視できなくなります。
- [アラームレベルを重大度に設定する] チェックボックスのチェックを外した場合、システム監視オブジェクトの状態を監視できなくなります。

(2) 監視ツリーを自動生成するためのセットアップ

JP1/PFM は、監視ツリーの自動生成に対応しています。自動生成の連携を有効にするには、連携用プログラムをセットアップします。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- JP1/PFM の説明

参照先：マニュアル「JP1/Performance Management 運用ガイド」の JP1/IM との連携の説明

(a) JP1/PFM - Manager のホストの場合

JP1/PFM - Manager がインストールされているマネージャーでは、次のようにセットアップします。

1. JP1/PFM の連携用プログラムをセットアップする。

監視ツリーの自動生成をするときに、JP1/PFM から定義情報を収集できるようにするため、次のコマンドを実行します。

```
jpcimsetup -i （自動生成の連携を有効にする場合）
```

上記のセットアップをしていない場合は、監視ツリーの自動生成をしても JP1/PFM の監視オブジェクトは生成されません。

また、次のコマンドを実行すると連携を解除することができます。

```
jpcimsetup -u （自動生成の連携を解除する場合）
```

6.8.4 JP1/Cm2/NNM との連携でのセットアップ

ここでは、バージョン 8 以前の JP1/Cm2/NNM と連携する場合のセットアップについて説明します。JP1/IM - EG for NNMi を使用して JP1/NNMi と連携する場合のセットアップについては、マニュアル「JP1/Integrated Management - Event Gateway for Network Node Manager i」を参照してください。

(1) システム監視オブジェクトで監視するためのセットアップ

バージョン 8 以前の JP1/Cm2/NNM と連携するには、JP1/Cm2/NNM が発行する SNMP トラップを JP1 イベントに変換して、それをセントラルスコープで監視できるように設定します。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- バージョン 8 以前の JP1/Cm2/NNM の説明

参照先：マニュアル「JP1/Cm2/Network Node Manager ネットワーク管理ガイド」

- SNMP トラップの JP1 イベントへの変換の説明

参照先：マニュアル「JP1/Base 運用ガイド」のイベント変換機能の設定の説明

(a) JP1/Cm2/NNM のホストの場合

バージョン 8 以前の JP1/Cm2/NNM がインストールされているマネージャーでは、次のようにセットアップします。

1. JP1/Base の SNMP トラップ変換機能を設定する。

SNMP トラップを JP1 イベントに変換するため、JP1/Base の SNMP トラップ変換機能の設定をします。JP1/Base の SNMP トラップ変換機能の設定は、バージョン 8 以前の JP1/Cm2/SSO と連携する場合と同じです。

SNMP トラップ変換機能の設定手順については、マニュアル「JP1/Base 運用ガイド」のイベント変換機能の設定の章を参照してください。

設定手順の概要を次に示します。

- NNM と JP1/Base の連携を設定（imevtgw_setup を実行）する
- NNM の URL を設定する
- JP1 イベントの送信先を設定する
- フィルター定義ファイル（snmpfilter.conf）を設定する

2. JP1/Base の SNMP トラップ変換機能のフィルター定義ファイルを編集する。

JP1/Base の SNMP トラップ変換機能のフィルター定義ファイル（snmpfilter.conf）に、セントラルスコープで扱う SNMP トラップを変換するための設定を記述したサンプルファイル（snmpfilter_im_sample.conf）の内容を追加します。

ファイル名は次のとおりです。

- SNMP トラップ変換機能のフィルター定義ファイル

Windows の場合：

Base パス¥conf¥evtgw¥snmpfilter.conf

UNIX の場合：

/etc/opt/jp1base/conf/evtgw/snmpfilter.conf

- セントラルスコープのサンプルファイル

Windows の場合：

Scope パス¥conf¥snmpfilter_im_sample.conf

UNIX の場合：

/etc/opt/jp1scope/conf/snmpfilter_im_sample.conf

❗ 重要

- サンプルファイルの行頭にある[+]は SNMP トラップのバリアブルバインディングを JP1 イベントに取り込む設定です。外さないでください。
- フィルター定義ファイルのサイズには制限があります。そのため、サンプルファイルの定義のうち、お客様の環境で監視対象とする SNMP トラップに関する定義だけをフィルター定義ファイルに追加してください。
フィルター定義ファイルのサイズの制限については、マニュアル「JP1/Base 運用ガイド」を参照してください。

6.8.5 JP1/NETM/DM との連携でのセットアップ

(1) システム監視オブジェクトで監視するためのセットアップ

JP1/NETM/DM のシステム監視オブジェクトを使用するには、JP1/NETM/DM が JP1 イベントを発行するように設定をしてください。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- JP1/NETM/DM の説明

参照先：マニュアル「JP1/NETM/DM 構築ガイド(Windows(R)用)」

(a) JP1/NETM/DM Manager のホストの場合

JP1/NETM/DM Manager がインストールされているマネージャーでは、次のようにセットアップします。

1. JP1/NETM/DM で JP1 イベント発行を有効にする。

JP1/NETM/DM セットアップ画面を起動し、イベントサービスパネルを選択して「イベントサービス機能を使用する」チェックボックスをチェックしてください。

セントラルスコープと連携を行う場合は「サーバダウンイベント」チェックボックスと「指令エラー終了」チェックボックスをチェックしてください。

6.8.6 JP1/PAM との連携でのセットアップ

(1) システム監視オブジェクトで監視するためのセットアップ

JP1/PAM のシステム監視オブジェクトを使用するには、JP1/PAM が JP1 イベントを発行するように設定をしてください。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- JP1/PAM の説明

参照先：マニュアル「JP1/Performance Management - Analysis」

(a) JP1/PA - Manager のホストの場合

JP1/PA - Manager がインストールされているマネージャーでは、次のようにセットアップします。

1. JP1/PAM の JP1 イベント発行を有効にする。

JP1/PAM の JP1 イベント発行定義ファイル (pamjp1ev.conf) を次のように設定してください。

- 設定するファイル

pamjp1ev.conf

- 設定内容

JP1 イベント発行の有無 (jp1evt_flag), およびイベントごとの JP1 イベント発行の有無 (metricNW など) に Y を設定します。イベントごとの JP1 イベント発行の有無については、すべて Y を設定してください。

jp1evt_flag=Y

metricNW=Y

:

6.8.7 Cosminexus との連携でのセットアップ

(1) システム監視オブジェクトで監視するためのセットアップ

Cosminexus のシステム監視オブジェクトを使用するには、Cosminexus 側で次の設定してください。

- JP1 イベントの発行設定

JP1/IM で Cosminexus のシステム環境を監視するには、Cosminexus で JP1 イベントを発行するよう、設定する必要があります。

また、JP1/IM - View から Cosminexus の運用管理ポータル画面を表示するには、Cosminexus が提供する Cosminexus モニター起動コマンドおよび設定ファイルを使って、モニター起動の設定をする必要があります。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- Cosminexus の説明

参照先：マニュアル「Cosminexus アプリケーションサーバ V8 システム構築・運用ガイド」

(2) 監視ツリーを自動生成するためのセットアップ

監視ツリーの自動生成により Cosminexus と連携する場合は、Cosminexus 側で次の設定してください。

- アダプタコマンドのセットアップ

JP1/IM で Cosminexus のシステム環境の情報を収集するには、Cosminexus が提供する Cosminexus アダプタコマンド (mngsvr_adapter_setup) によってセットアップを行う必要があります。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- Cosminexus の説明

参照先：マニュアル「Cosminexus アプリケーションサーバ V8 システム構築・運用ガイド」

注意事項

JP1/IM で Cosminexus のシステム環境の情報を収集し、監視するには、次のことに注意してください。

- 自動生成でサーバ指向ツリーを作成する場合、運用管理サーバと業務サーバすべてを JP1/IM のシステム構成に含める必要があります。

6.8.8 HiRDB との連携でのセットアップ

HiRDB のシステム監視オブジェクトを使用するには、HiRDB が出力するイベントを、JP1 イベントとして JP1/IM に通知するように設定をしてください。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- HiRDB の説明

JP1/IM へのイベント通知

参照先：マニュアル「HiRDB Version 8 システム導入・設計ガイド (Windows(R)用)」

参照先：マニュアル「HiRDB Version 8 システム導入・設計ガイド (UNIX(R)用)」

JP1/IM へのイベント通知の設定詳細

参照先：マニュアル「HiRDB Version 8 システム定義 (Windows(R)用)」

参照先：マニュアル「HiRDB Version 8 システム定義 (UNIX(R)用)」

6.8.9 JP1/ServerConductor との連携でのセットアップ

JP1/ServerConductor のシステム監視オブジェクトを使用するには、JP1/ServerConductor が検知したアラートを、JP1 イベントとして JP1/IM に通知するように設定してください。

連携のセットアップについては、次のマニュアルもあわせて参照してください。

- JP1/ServerConductor の説明

参照先：マニュアル「JP1/Server Conductor/Blade Server Manager 系 設計・構築ガイド」

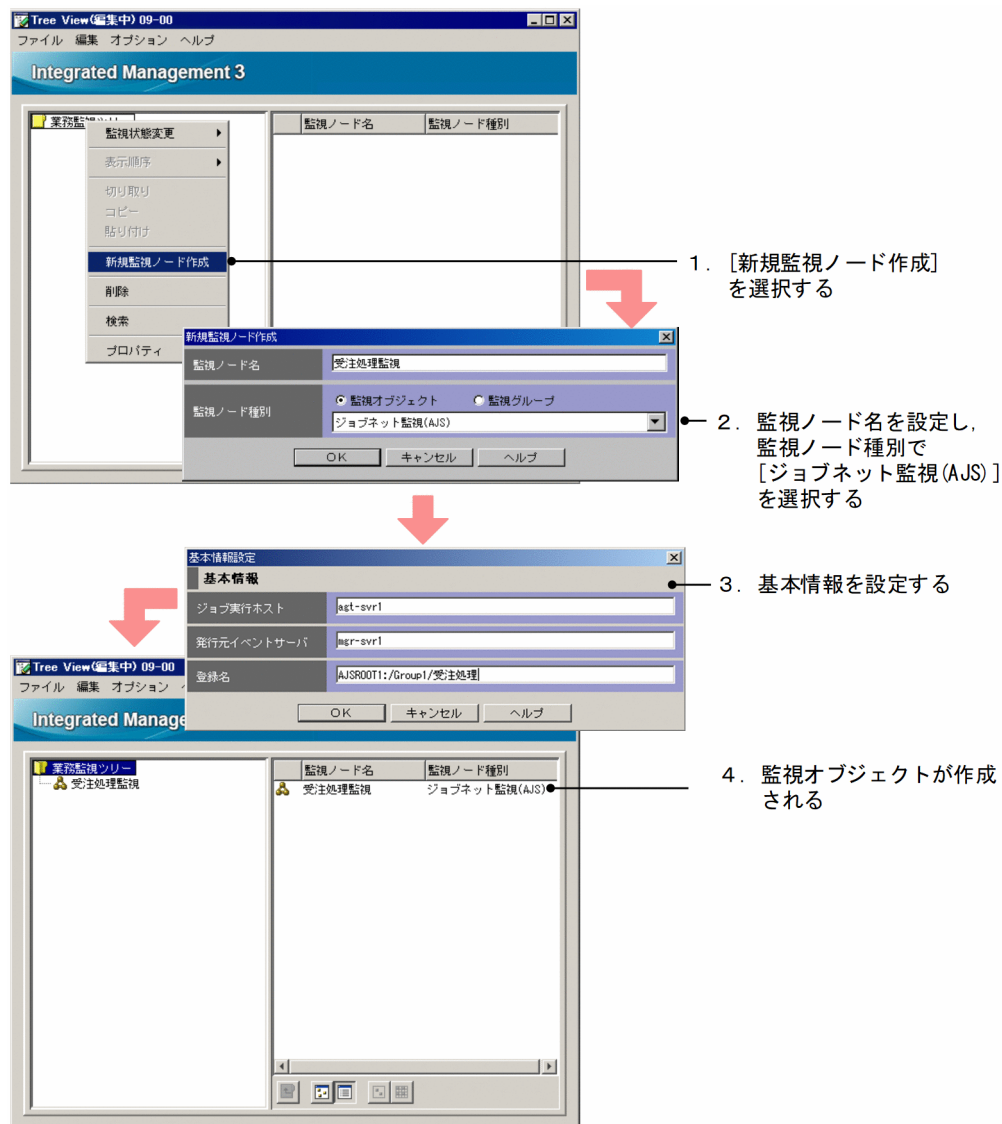
6.9 監視オブジェクト作成例

監視オブジェクトを手動で作成する例について説明します。

6.9.1 システム監視オブジェクトの作成例（JP1/AJS のジョブネット監視）

JP1/AJS のジョブネット「AJSROOT:/Group1/受注処理」の実行状態を監視するシステム監視オブジェクトを作成する例を示します。

図 6-16 システム監視オブジェクトの作成例



1. [新規監視ノード作成] 画面を開く。

次のどれかの操作により画面を開いてください。

- 監視グループを選択し、右クリックしてポップアップメニューから [新規監視ノード作成] を選択する。

6. セントラルスコープの設定

- 監視グループを選択し、メニューバーから [編集] - [新規監視ノード作成] を選択する。
- 詳細表示領域から画面を開く場合は、監視ノード非選択状態で右クリックし、ポップアップメニューから [新規監視ノード作成] を選択する。

なお、監視ノードが一つもない場合は、メニューバー、または監視ツリー領域の右クリックで表示されるポップアップメニューから操作をしてください。

2. 監視ノード名を入力し、監視ノード種別で [ジョブネット監視(AJS)] を選択する。

[新規監視ノード作成] 画面で次の項目を設定します。

- 監視ノード名
任意の名称を指定します。
- 監視ノード種別
[ジョブネット監視(AJS)] を選択します。

3. 監視ノードの基本情報を設定する。

[基本情報設定] 画面で次のように設定します。

表 6-5 監視ノードの基本情報の設定例

監視ノード属性名	入力する属性値 (例)	説明
ジョブ実行ホスト	agt-svr1	ジョブ実行先のホストです。ジョブを実行する JP1/AJS エージェント名を入力します。
発行元イベントサーバ	mgr-svr1	JP1 イベントを発行するホストです。JP1/AJS の場合、JP1/AJS マネージャ名を入力します。
登録名	AJSROOT:/Group/受注処理	登録名は完全名を入力します。完全名は次の形式で記述します。ジョブグループ名は省略できます。 スケジューラサービス名:/ジョブグループ名 1/ジョブグループ名 2/・・・/ジョブネット名

4. 監視オブジェクトが作成される。

JP1/AJS のジョブネット「AJSROOT:/Group/受注処理」の実行状態を監視する監視オブジェクトが作成されます。

6.9.2 汎用監視オブジェクトの作成例 (JP1/Cm2/SSO による CPU 監視)

バージョン 8 以前の JP1/Cm2/SSO の CPU 監視など、監視ツリーの自動生成でサポートしていない対象を監視したい場合には、監視オブジェクトを手動で作成する必要があります。

(1) 前提知識

バージョン 8 以前の JP1/Cm2/SSO のように SNMP トラップを出力する製品を JP1/IM で監視する場合、まず、SNMP トラップを JP1 イベントに変換する必要があります。これは、セントラルスコープが JP1 イベントの属性名と属性値をキーにして、監視オブジェクトを監視しているためです。

JP1/Base の SNMP トラップ変換機能を使うことで、SNMP トラップを JP1 イベントに変換できます。SNMP トラップ変換機能を使えば、SNMP の各フィールドを JP1 イベントの属性にマッピングすることができます。

変換後の JP1 イベントの属性と、SNMP トラップの各フィールドの対応を次の表に示します。

表 6-6 JP1 イベントの属性と SNMP トラップの各フィールドの対応

変換後の JP1 イベント		変換対象の SNMP トラップ	
基本属性		メッセージ	PDU Type
拡張属性	共通情報	SEVERITY	specific trap
		—	—
	固有情報	SNMP_OID	Enter prise
		SNMP_DATE	timestamp
		SNMP_SOURCE	agent address
		SNMP_SEVERITY	specific trap
		SNMP_URL	—
		SNMP_VARBIND_RESULT	—
		SNMP_VARBIND_NUM	—
		SNMP_VARBIND1	バリアブルバインディングの Data1 の値
		SNMP_VARBIND2	バリアブルバインディングの Data2 の値
		(省略)	(省略)
		SNMP_VARBIND28	バリアブルバインディングの Data28 の値

(凡例)

—：メッセージの固有情報に該当する情報がない

なお、SNMP トラップ変換機能の詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

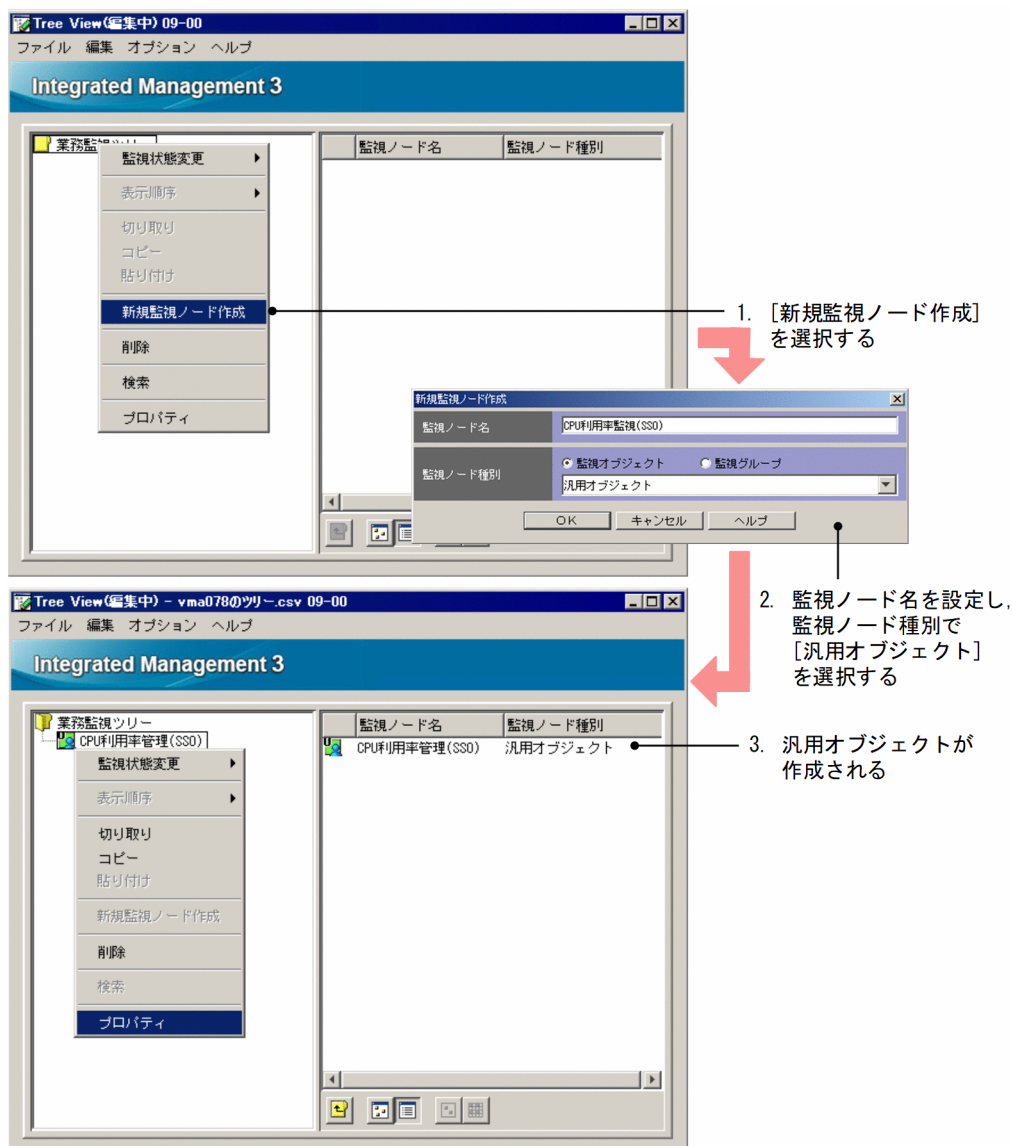
(2) 監視オブジェクト作成前の確認

CPU 監視をする監視オブジェクトを作成する前に、次の 2 点を確認してください。

- エージェントでバージョン 8 以前の JP1/Cm2/SSO の設定が完了していて、マネージャーに JP1 イベントが送信されている。
セントラルコンソールの [イベントコンソール] 画面で、バージョン 8 以前の JP1/Cm2/SSO の CPU 監視のイベントが表示されていることを確認してください。
- バージョン 8 以前の JP1/Cm2/SSO の CPU 監視をするエージェントで、セントラルスコープとの連携の設定が完了している。
セントラルスコープの監視ツリーの自動生成で、「SSO 監視」の監視オブジェクトが生成され、JP1 イベントの受信によって状態が変わることを確認してください。

(3) 監視オブジェクトの作成 (CPU の監視)

図 6-17 汎用監視オブジェクトの作成



作成手順を次に示します。

1. [監視ツリー(編集)] 画面で、[編集] - [新規監視ノード作成] を選択する。

[新規監視ノード作成] 画面が表示されます。

2. 次の内容を入力して、[OK] ボタンをクリックする。

表 6-7 監視ノード名と監視ノード種別の設定内容

設定項目	設定内容
監視ノード名	任意の名称を入力します。 管理しやすい名称にすることをお勧めします。この例では、「CPU 利用率監視 (SSO)」と入力します。
監視ノード種別	「監視オブジェクト」をラジオボタンで選択し、「汎用オブジェクト」をリストボックスから選択します。

監視ツリーに、監視オブジェクト「CPU 利用率監視 (SSO)」が追加されます。

(4) 監視オブジェクトの設定 (CPU の監視)

図 6-18 汎用監視オブジェクトの設定 (状態変更条件の追加 その 1)

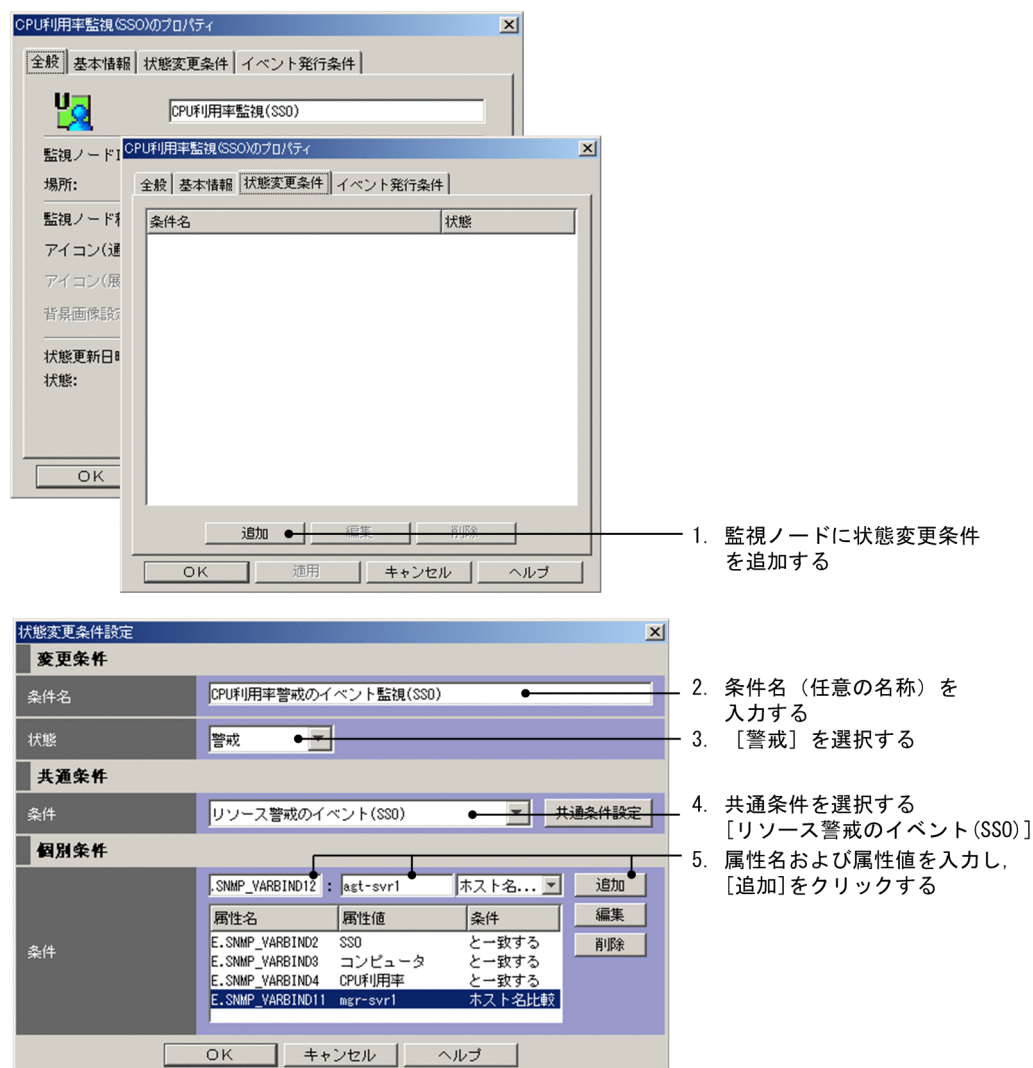
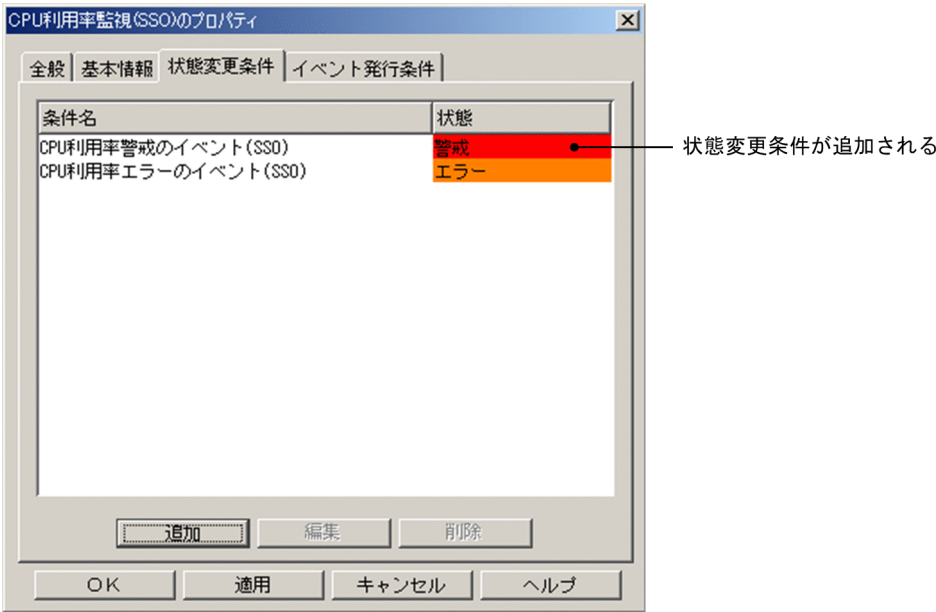


図 6-19 汎用監視オブジェクトの設定（状態変更条件の追加 その 2）



設定手順を次に示します。

- 1. 作成した監視オブジェクト（「CPU 利用率監視（SSO）」）を選択し，[編集]－[プロパティ]を選択する。
[プロパティ] 画面が表示されます。
- 2. [プロパティ] 画面で [状態変更条件] ページを選択し，[追加] ボタンをクリックする。
[状態変更条件設定] 画面が表示されます。
- 3. [状態変更条件設定] 画面で条件設定する。

JP1/IM - Manager が，どのような JP1 イベントを受信したときに，監視ノードの状態を変更するかを設定します。

状態変更条件を入力後，[OK] ボタンをクリックします（[OK] ボタンをクリックすると [状態変更条件] ページへ戻ります）。続けて状態変更条件を入力する場合は，再度 [追加] ボタンをクリックし，[状態変更条件設定] 画面で条件を入力します。

状態変更条件は，次のように設定します。

表 6-8 状態変更条件の設定例

条件名 (任意の名称)	状態	共通条件
CPU 利用率警戒のイベント(SSO)	警戒	リソース警戒のイベント(SSO)
CPU 利用率エラーのイベント(SSO)	エラー	リソースエラーのイベント(SSO)

それぞれの条件での個別条件は次のように設定します。個別条件を追加するときは，一つの個別条件を入力するごとに [追加] を選択してください。

表 6-9 状態変更条件（個別条件）の設定例

監視ノード属性名	属性名	属性値（例）	条件
カテゴリ名	E.SNMP_VARBIND2	SSO	と一致する
グループ名	E.SNMP_VARBIND3	コンピュータ	と一致する
リソース名	E.SNMP_VARBIND4	CPU 利用率※1	と一致する
イベント発行元ホスト	E.SNMP_VARBIND11	mgr-svr1※2	ホスト名比較
ホスト名	E.SNMP_VARBIND12	agt-srv1※3	ホスト名比較

注※1 バージョン 8 以前の JP1/Cm2/SSO で監視対象となっているリソース名を設定します。

- CPU 監視の場合：CPU 利用率
- メモリー監視の場合：メモリー使用率

注※2 イベント発行ホスト名を設定します。gethostname で取得したホスト名です。hostname コマンドで表示されるホスト名の形式で指定してください。

注※3 監視先ホスト名を設定します。gethostbyaddr で取得したホスト名です。DNS が設定されている場合は、ホスト名に DNS のsuffix が付加された名称を指定してください。DNS が設定されていない場合は、hosts ファイルに書かれているホスト名の形式で指定してください。

4. [状態変更条件] ページでの設定が完了したら，[OK] ボタンをクリックする。

サーバのツリーを更新して，監視ツリーに作成した監視ノードが追加されているか確認してください。

バージョン 8 以前の JP1/Cm2/SSO のリソース名「CPU 利用率」の状態を監視する監視オブジェクトは，システム監視オブジェクト「カテゴリ監視(SSO)」を利用して作ることもできます。カテゴリ監視(SSO)のシステム監視オブジェクト作成後，不足している個別条件をすべての状態変更条件に追加してください。

❗ 重要

バージョン 8 以前の JP1/Cm2/SSO を監視するには，エージェントの JP1/Cm2/SSO および JP1/Base をバージョン 7 またはバージョン 8 にする必要があります。

エージェントの JP1/Cm2/SSO，JP1/Base がバージョン 6 の場合は，監視することはできませんが，自動での情報収集ができないため，これまでの手順に加えて多くの手作業が発生します。このため，推奨しません。

なお，JP1/Cm2/SSO の製品名称は，バージョン 7 は JP1/PFM/SSO，バージョン 6 は JP1/SSO です。

6.9.3 汎用監視オブジェクトの作成例（HiRDB の監視）

ここでは，バージョン 6 の HiRDB を監視するための監視オブジェクトの作成および設定手順について説明します。なお，監視オブジェクトの状態変更条件には，HiRDB が出力するメッセージログイベント（JP1/SES イベント：0x00010C03）を利用すると仮定します。

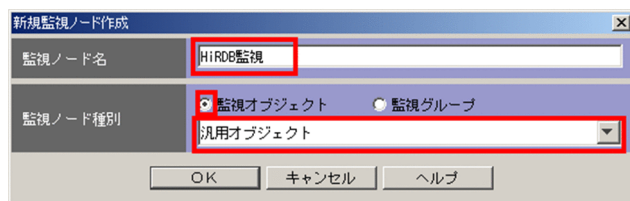
メモ

HiRDB のバージョンが 07-02 以降の場合は、JP1/SES イベントでなく JP1 イベントを出力できます（HiRDB 側で出力設定が別途必要）。この場合は、セントラルスコープが提供するシステム監視オブジェクトを使って HiRDB 用の監視オブジェクトを作成してください。

(1) 監視オブジェクト（HiRDB 監視）の作成

1. [監視ツリー] 画面から [オプション] - [ツリー編集] を選択する。
[監視ツリー(編集)] 画面が表示されます。
2. [監視ツリー(編集)] 画面で [ファイル] - [ツリーを開く] を選択する。
HiRDB の監視オブジェクトを追加する監視ツリーを開きます。
3. [ツリー表示領域] で HiRDB の監視オブジェクトを追加したい場所を選択する。
4. [編集] - [新規ノード作成] を選択する。
[新規監視ノード作成] 画面が表示されます。

図 6-20 [新規監視ノード作成] 画面



[新規監視ノード作成] 画面の設定内容は次のとおりです。

表 6-10 [新規監視ノード作成] 画面の設定内容

設定項目	設定内容
監視ノード名	任意の名称を入力します。 管理しやすい名称にすることをお勧めします。この例では、「HiRDB 監視」と入力しています。
監視ノード種別	「監視オブジェクト」をラジオボタンで選択し、「汎用オブジェクト」をリストボックスから選択します。

5. [OK] ボタンをクリックする。
監視ツリーに、監視オブジェクト「HiRDB 監視」が追加されます。

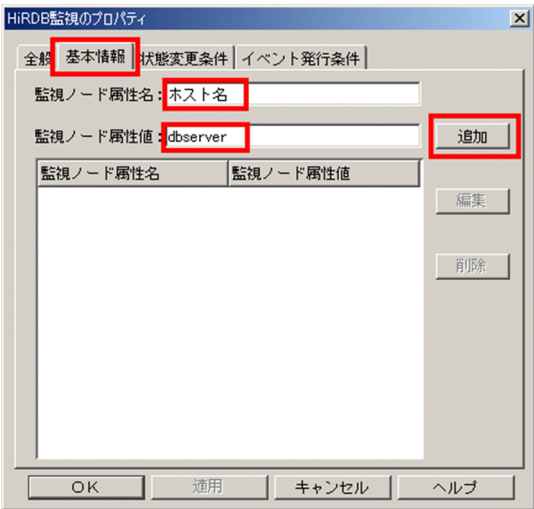
(2) 監視オブジェクト（HiRDB 監視）の設定

(a) 監視オブジェクトの基本情報を設定する

1. 新規作成した監視オブジェクトを選択する。

- 2. [編集] – [プロパティ] を選択する。
[プロパティ] 画面が表示されます。
- 3. [プロパティ] 画面で [基本情報] ページを選択する。

図 6-21 [基本情報] ページ



[基本情報] ページの設定内容は次のとおりです。

表 6-11 [基本情報] ページの設定内容

設定項目	設定内容
監視ノード属性名	任意の名称を入力します。 「ホスト名」など、イメージしやすい名称を入力しておくことをお勧めします。
監視ノード属性値	任意の値を入力します。監視ノード属性名として入力した名称に対応する値を入力します。 監視ノード属性名として「ホスト名」と入力した場合、それに対応する値としてhostname コマンドで表示されるホスト名、または製品を連想しやすい値を入力します。ここでは HiRDB を連想しやすい値として、「dbserver」と入力しています。

注 ここで指定した監視ノードの基本情報は、監視ノードを検索する際の検索条件に指定することができます。なお、基本情報は監視オブジェクトの状態遷移には影響しません。

- 4. [追加] ボタンをクリックする。
監視オブジェクトに、基本情報が設定されます。

(b) 監視オブジェクトの状態変更条件を設定する

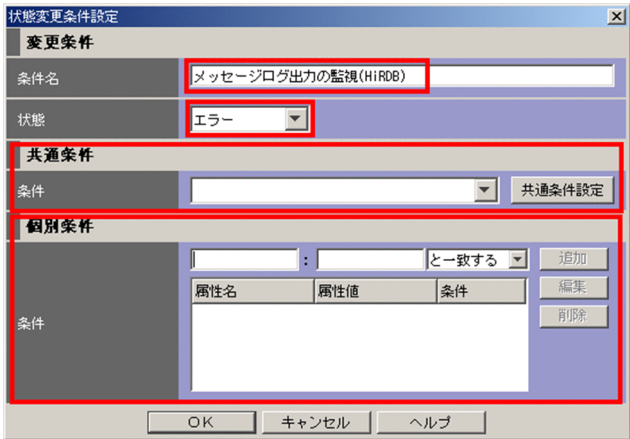
- 1. 新規作成した監視オブジェクトを選択する。
- 2. [編集] – [プロパティ] を選択する。
[プロパティ] 画面が表示されます。
- 3. [プロパティ] 画面で [状態変更条件] ページを選択する。

図 6-22 「状態変更条件」 ページ



4. [追加] ボタンをクリックする。
[状態変更条件設定] 画面が表示されます。

図 6-23 「状態変更条件設定」 画面



[状態変更条件設定] 画面の設定内容は次のとおりです。

表 6-12 「状態変更条件設定」 画面の設定内容

設定項目	設定内容
条件名	条件名を設定します。
状態	イベントを受信した場合に、監視オブジェクトが遷移する状態をリストボックスから選択します。
共通条件	発生元製品、発生事象を特定するための情報を設定します。 詳細は、以降で説明します。
個別条件	発生場所を特定するための情報を設定します。 詳細は、以降で説明します。

5. 条件名、状態、共通条件および個別条件を入力したら、[OK] ボタンをクリックする。

共通条件の設定

共通条件には、発生元製品、発生事象を特定するための情報を設定します。

- 1. [共通条件設定] ボタンをクリックする。
[共通条件設定] 画面が表示されます。
- 2. [共通条件設定] 画面の [追加] ボタンをクリックする。
[共通条件詳細設定] 画面が表示されます。

図 6-24 [共通条件詳細設定] 画面

[共通条件詳細設定] 画面の設定内容は次のとおりです。

表 6-13 [共通条件詳細設定] 画面の設定内容

設定項目	設定内容
共通条件名	共通条件の名称を指定します。
メッセージ	JP1 イベント（ここでは JP1/SES イベント）のメッセージを指定します。 特定のメッセージだけを監視対象としたい場合に指定します。HiRDB の場合、HiRDB が出力する JP1/SES イベントのメッセージ情報を指定します。 例えば、「KFPS01222-I」と入力し、右側のリストボックスで「から始まる」を選択することにより、HiRDB のログスワップメッセージだけを監視対象にできます。
イベント ID	監視をする JP1 イベント（ここでは JP1/SES イベント）のイベント ID を指定します。 HiRDB のように JP1/SES イベントを発行する製品の場合は、監視したい JP1/SES イベントの基本コード（00010C03）を指定します。

- 3. [OK] ボタンをクリックする。

6. セントラルスコープの設定

[共通条件設定] 画面に戻ります。

4. [閉じる] ボタンをクリックする。

[共通変更条件設定] 画面に戻ります。

5. 作成した共通条件を選択する。

作成した共通条件がリストボックスに追加されています。作成した共通条件を選択してください。

個別条件の設定

個別条件には、障害発生ホスト名など、事象の発生個所を特定するための条件を設定します。

1. 属性名および属性値を入力し、[追加] ボタンをクリックする。

個別条件が追加されます。個別条件を追加する回数、上記手順を繰り返してください。

個別条件の設定内容は次のとおりです。

表 6-14 個別条件の設定内容

属性名	属性値	説明
B. SOURCESERVER	dbserver	属性名には、イベントを通知する事象の発生元（ホスト）を絞り込むため、B. SOURCESERVER を入力します。 属性値には、HiRDB のシステムマネージャーが稼働するホスト名を指定します。
B. MESSAGE	HiRDB のサーバ名	イベント情報として製品個別のメッセージ情報が出力される場合は、そのメッセージ情報を基に絞り込みます。 メッセージに事象の発生個所を特定する情報が含まれることがあるためです（HiRDB が出力するメッセージログイベントなどが該当）。 メッセージの情報を基に、事象の発生個所を特定したい場合には、属性名として B. MESSAGE を入力し、属性値として絞り込みができるキーワードを入力します。 例えば、HiRDB のログスワップのメッセージには、HiRDB のサーバ名が含まれるため、属性名に B. MESSAGE、属性値に HiRDB のサーバ名を入力し、リストボックスで「正規表現」を選択することにより、特定の HiRDB のサーバで発生したログスワップだけを監視対象とすることができます。 なお、B. MESSAGE を設定する場合には、監視対象外のメッセージが条件に一致しないように注意してください。

なお、状態変更条件に JP1/SES イベントの詳細情報を指定することはできません。

(c) 編集した監視ツリーの更新

編集した監視ツリーを更新して、監視に使えるようにします。

1. [監視ツリー(編集中)] 画面で、[ファイル] - [サーバのツリーを更新] を選択する。

HiRDB の監視ノードがセントラルスコープの監視オブジェクト DB に追加されます。

6.9.4 汎用監視オブジェクトの作成例（JP1/Cm2/SSO による Cosminexus 業務のリソース監視）

Cosminexus で定義した J2EE アプリケーションおよび一部の論理サーバは、バージョン 8 以前の JP1/Cm2/SSO を使って稼働性能を監視することができます。

セントラルスコープでは、Cosminexus およびバージョン 8 以前の JP1/Cm2/SSO とともにセットアップコマンドによる連携（監視ツリーの自動生成）ができるため、次の条件を満たす場合は、JP1/Cm2/SSO で監視している J2EE アプリケーションおよび論理サーバのリソース状態変化により発行される JP1 イベントを監視する監視オブジェクト（汎用オブジェクト）を自動生成できます（Cosminexus + JP1/Cm2/SSO 連携）。

自動生成の条件

- Cosminexus のバージョンが 06-00 以降、JP1/Cm2/SSO のバージョンがバージョン 7 またはバージョン 8（バージョン 7 の JP1/Cm2/SSO の製品名称は JP1/PM/SSO）
- 連携製品がセットアップ済みである（Cosminexus, JP1/Cm2/SSO）
- JP1/IM 連携用セットアップコマンドが実行済みである（Cosminexus, JP1/Cm2/SSO）
- バージョン 8 以前の JP1/Cm2/SSO で、Cosminexus で定義した J2EE アプリケーションまたは論理サーバを監視している
- 監視ツリーの自動生成で「業務指向ツリー」を生成（サーバ指向ツリーでは生成されない）

Cosminexus + JP1/Cm2/SSO 連携で自動生成できる監視オブジェクトを次の表に示します。

表 6-15 Cosminexus + SSO 連携で自動生成できる監視オブジェクト

監視オブジェクト名	説明	監視単位
J2EE サーバリソース監視 (SSO)	Cosminexus の J2EE サーバのリソース状況を監視する監視オブジェクト※。J2EE サーバリソースに関するイベント発行を契機に状態が変化する。	J2EE サーバ
CTM リソース監視(SSO)	Cosminexus の CTM のリソース状況を監視する監視オブジェクト※。CTM に関するイベント発行を契機に状態が変化する。	CTM
SFO リソース監視(SSO)	Cosminexus の SFO のリソース状況を監視する監視オブジェクト※。SFO に関するイベント発行を契機に状態が変化する。	SFO
J2EE アプリケーションリソース監視(SSO)	Cosminexus の J2EE アプリケーションのリソース状況を監視する監視オブジェクト※。J2EE アプリケーションに関するイベント発行を契機に状態が変化する。	J2EE アプリケーションサーバ

注※ 重要度が「Warning」以上の SNMP トラップが監視オブジェクトの監視対象イベントになります。

自動生成の条件に一致しない Cosminexus 環境のリソース状況を監視したい場合には、ユーザーは手動で監視オブジェクトを作成する必要があります。

以降、手動で監視オブジェクトを作成する方法について説明します。なお、以降の説明では、次表に示す Cosminexus の J2EE サーバ、CTM、SFO、および J2EE アプリケーションのリソース状況を監視すると仮定して説明します。

表 6-16 監視対象となる Cosminexus のサーバ、アプリケーション情報

監視対象種別	監視オブジェクト名	設定項目	設定値
J2EE サーバ	J2EE サーバリソース監視 (SSO)	ドメイン名	DefaultDomain
		論理サーバ名	J2EE_SV1
		バージョン 8 以前の JP1/Cm2/SSO マネージャ名(イベント発行元ホスト名)	HostA
		論理サーバが稼働するホスト名(ホスト名)	HostB
CTM	CTM リソース監視(SSO)	ドメイン名	DefaultDomain
		論理サーバ名	CTM_SV1
		バージョン 8 以前の JP1/Cm2/SSO マネージャ名(イベント発行元ホスト名)	HostA
		論理サーバが稼働するホスト名(ホスト名)	HostB
SFO	SFO リソース監視(SSO)	ドメイン名	DefaultDomain
		論理サーバ名	SFO_SV1
		バージョン 8 以前の JP1/Cm2/SSO マネージャ名(イベント発行元ホスト名)	HostA
		論理サーバが稼働するホスト名(ホスト名)	HostB
J2EE アプリケーション	J2EE アプリケーションリソース監視(SSO)	ドメイン名	DefaultDomain
		論理サーバ名	J2EE_SV1
		バージョン 8 以前の JP1/Cm2/SSO マネージャ名(イベント発行元ホスト名)	HostA
		論理サーバが稼働するホスト名(ホスト名)	HostB

上記表に示したサーバ、アプリケーションのリソース状態を監視する監視オブジェクトを作成する場合、幾つかの項目はユーザーが入力する必要があります。ユーザーが監視条件として入力する項目、値を次の表に示します。なお、ユーザーが入力する必要があるのは、次表の下線を引いた個所です。

表 6-17 監視条件として入力する必要がある項目、値

監視オブジェクト種別	入力画面	監視ノード属性名	属性名	監視ノード属性値	条件
J2EE サーバリソース監視(SSO)	[基本情報設定]画面	カテゴリ名	E. SNMP_VARBIND2	<u>COSMINEXUS</u>	と一致する
		イベント発行元ホスト	E. SNMP_VARBIND11	<u>HostA</u> ※1	ホスト名比較

監視オブジェクト種別	入力画面	監視ノード属性名	属性名	監視ノード属性値	条件
	[状態変更条件設定]画面	ホスト名	E. SNMP_VARBIND12	<u>HostB</u> ※1	ホスト名比較
		リソースグループ名	<u>E. SNMP_VARBIND3</u>	<u>サーバ</u>	と一致する
		インスタンス名	<u>E. SNMP_VARBIND6</u>	<u>^DefaultDomain:J2EE_SV1(:. * \$)</u> ※2	正規表現
CTM リソース監視 (SSO)	[基本情報設定]画面	カテゴリ名	E. SNMP_VARBIND2	<u>COSMINEXUS</u>	と一致する
		イベント発行元ホスト	E. SNMP_VARBIND11	<u>HostA</u> ※1	ホスト名比較
		ホスト名	E. SNMP_VARBIND12	<u>HostB</u> ※1	ホスト名比較
	[状態変更条件設定]画面	リソースグループ名	<u>E. SNMP_VARBIND3</u>	<u>スケジューラ (CTM)</u>	と一致する
		インスタンス名	<u>E. SNMP_VARBIND6</u>	<u>^DefaultDomain:CTM_SV1(:. * \$)</u> ※2	正規表現
SFO リソース監視 (SSO)	[基本情報設定]画面	カテゴリ名	E. SNMP_VARBIND2	<u>COSMINEXUS</u>	と一致する
		イベント発行元ホスト	E. SNMP_VARBIND11	<u>HostA</u> ※1	ホスト名比較
		ホスト名	E. SNMP_VARBIND12	<u>HostB</u> ※1	ホスト名比較
	[状態変更条件設定]画面	インスタンス名	<u>E. SNMP_VARBIND6</u>	<u>^DefaultDomain:SFO_SV1(:. * \$)</u> ※2	正規表現
J2EE アプリケーションリソース監視(SSO)	[基本情報設定]画面	カテゴリ名	E. SNMP_VARBIND2	<u>COSMINEXUS</u>	と一致する
		イベント発行元ホスト	E. SNMP_VARBIND11	<u>HostA</u> ※1	ホスト名比較
		ホスト名	E. SNMP_VARBIND12	<u>HostB</u> ※1	ホスト名比較
	[状態変更条件設定]画面	インスタンス名	<u>E. SNMP_VARBIND6</u>	<u>^DefaultDomain:J2EE_SV1:API(:. * \$)</u> ※2	正規表現

注※1 ホスト名については、Cosminexusで使用しているホスト名とバージョン 8 以前の JP1/Cm2/SSO で使用しているホスト名の対応付けができるようあらかじめ設定しておく必要があります。

注※2 インスタンス名(サブリソース名)については、マニュアル「JP1/Cm2/SNMP System Observer」のリソースの取得対象と収集する MIB オブジェクトの説明を参照してください。

J2EE サーバリソース監視(SSO)の設定手順を次に示します。なお、ほかの CTM リソース監視(SSO)、SFO リソース監視(SSO)および J2EE アプリケーションリソース監視(SSO)については、手順 7 で入力する値が異なるだけであるため、省略します（手順 7 で入力する値を、「表 6-16 監視対象となる Cosminexus のサーバ、アプリケーション情報」を参考に読み替えてください）。

図 6-25 J2EE サーバリソース監視(SSO)の監視オブジェクト作成手順 (手順 1～4)

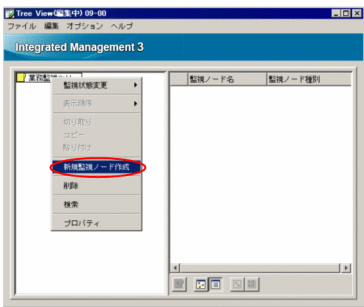
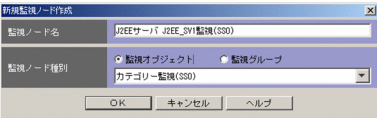
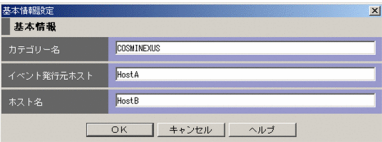
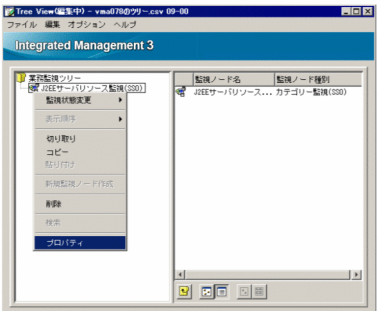
JP1/IM - Viewの画面	手順
	手順1: [監視ツリー (編集集中)] 画面での操作 上位ノードとなる監視グループを選択し、右クリックしてポップアップメニューから[新規監視ノード作成]を選択する。
	手順2: [新規監視ノード作成] 画面での操作 - 監視ノード名を入力する。 監視ノード名には、どの論理サーバを監視しているかわかるように、「<種別><論理サーバ名>監視(SSO)」と入力します。 例: J2EEサーバ J2EE_SV1監視(SSO) - 監視ノード種別は「カテゴリ監視(SSO)」を選択する。
	手順3: [基本情報設定] 画面での操作 - カテゴリ名に「COSMINEXUS」を入力する。 - イベント発行元ホストにJP1/Cm2/SSOのマネージャーホスト名を入力する。 例: HostA - ホスト名に論理サーバが稼働するホスト名を入力する 例: HostB
	手順4 [OK] ボタンをクリックし、[監視ツリー (編集集中)] 画面に戻る。

図 6-26 J2EE サーバリソース監視(SSO)の監視オブジェクト作成手順 (手順 5～8)

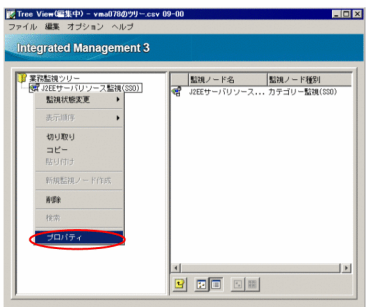
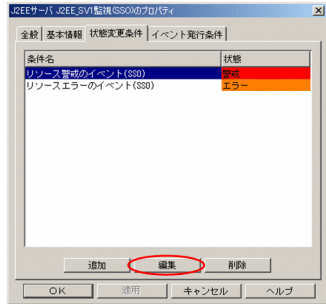
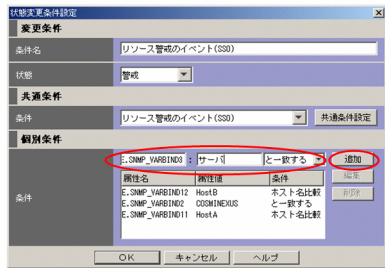
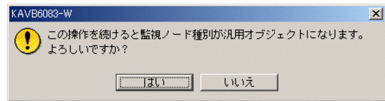
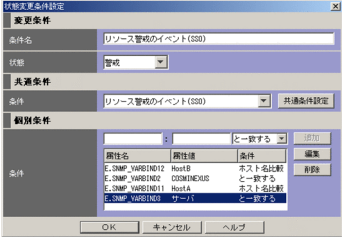
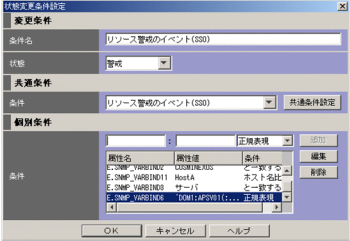
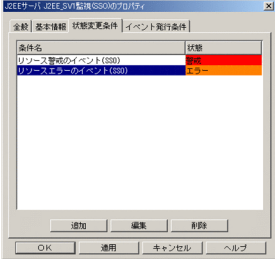
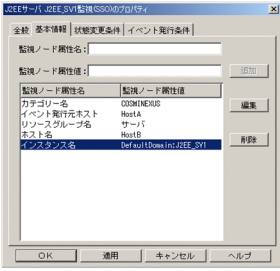
JP1/IM - Viewの画面	手順
	手順5: [監視ツリー (編集)] 画面での操作 手順1～手順4で作成した監視オブジェクトを選択し、右クリックしてポップアップメニューから[プロパティ]を選択する。
	手順6: [プロパティ] 画面での操作 [状態変更条件] タブを選択し、「リソース警戒のイベント(SSO)」を選択する。次に[編集] ボタンをクリックする。
	手順7: [状態変更条件設定] 画面での操作 表6-17を参考にして、不足している監視条件を追加する。※ 注※ 種別ごとに追加する監視条件が異なります。 例: J2EEサーバリソース監視(SSO)の場合 - E SNMP_VARS IND3 サーバ - E SNMP_VARS IND6 ^DefaultDomain:J2EE_SV1 (:.* \$)
	手順8 [追加] ボタンをクリックしたときに「KAVB6083-W」のメッセージが表示されるので、[はい]をクリックする。

図 6-27 J2EE サーバリソース監視(SSO)の監視オブジェクト作成手順 (手順 9～12)

JP1/IM - Viewの画面	手順
	手順9 : [状態変更条件設定]画面での操作 続けてほかの条件を追加する(以降, 手順8のダイアログは表示されない)。
	手順10 [OK]ボタンをクリックし, [状態変更条件設定]画面を終了する。
	手順11 : [プロパティ]画面での操作 手順7, 手順9および手順10の操作を「リソースエラーのイベント (SS0)」についても繰り返し行い, 監視条件を追加する。
	手順12 : [プロパティ]画面での操作 (任意設定) [基本情報]タブを選択し, 監視ノードの属性名と属性値を入力する※。 注※入力した内容は状態遷移条件には影響しませんが, 監視ノードを検索する場合の条件として利用できます。例では検索しやすいようにインスタンス名は「<ドメイン名>:<論理サーバ名>」としています(自動生成の場合に設定される値と同じ形式)。また, J2EEアプリケーションの場合は, 「<ドメイン名>:<論理サーバ名>:<J2EEアプリケーション名>」となります。 [適用]ボタンまたは[OK]ボタンをクリックし, 設定を終了する。

設定終了後, 監視ツリーに反映([サーバのツリーを更新]を実行)

7

クラスタシステムでの運用と環境構築（Windows の場合）

JP1/IM - Manager は、クラスタシステムでの運用に対応しています。JP1/IM - Manager をクラスタ運用することによって、サーバ障害などが発生しても実行系から待機系に処理を引き継ぎ、システム統合管理を継続できます。

この章では、Windows の場合の JP1/IM - Manager のクラスタ運用およびセットアップ方法について説明します。セットアップ後に JP1/IM - Manager を起動する手順については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3. JP1/IM - Manager の起動と終了」を参照してください。

なお、この機能については、ご使用になるクラスタソフトに JP1/IM - Manager が対応していることをご確認の上、ご使用ください。

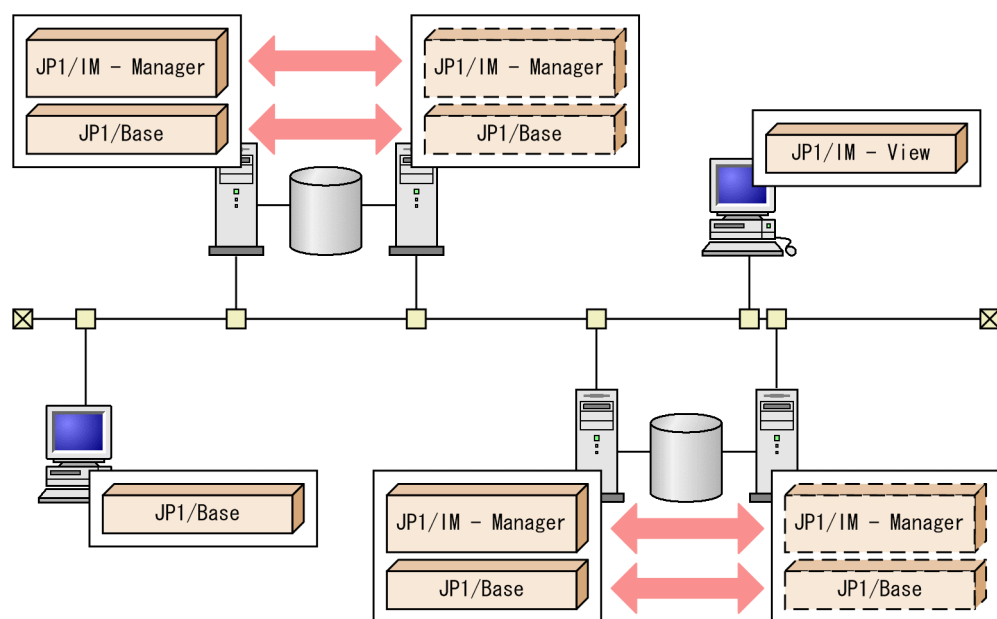
7.1 クラスタ運用の概要 (Windows の場合)

JP1/IM - Manager は、クラスタシステムでの運用に対応しています。JP1/IM - Manager をクラスタ運用することによって、サーバ障害などが発生した場合でも実行系から待機系に処理を引き継いで、システム運用管理を継続できます。

なお、クラスタシステムとは、これまで JP1 のマニュアルで「系切り替えシステム」と呼ばれていたものと同じです。

クラスタシステムで JP1/IM - Manager を運用する場合は、次のような構成で運用します。

図 7-1 クラスタシステムでの JP1/IM の構成例



ここでは、JP1/IM - Manager のクラスタシステムでの運用について、クラスタシステムの概要から JP1/IM - Manager の機能について順に説明します。

JP1/IM - Manager をクラスタ運用する場合、JP1/IM - Manager と JP1/Base を同じ論理ホスト環境で実行する必要があります。

JP1/Base のクラスタ運用については、マニュアル「JP1/Base 運用ガイド」のクラスタシステムで運用する場合の設定に関する説明を参照してください。

なお、この節では高可用性（HA：High Availability）の実現を目的としたクラスタシステムについて説明します。負荷分散などを目的としたクラスタシステムについては説明しません。

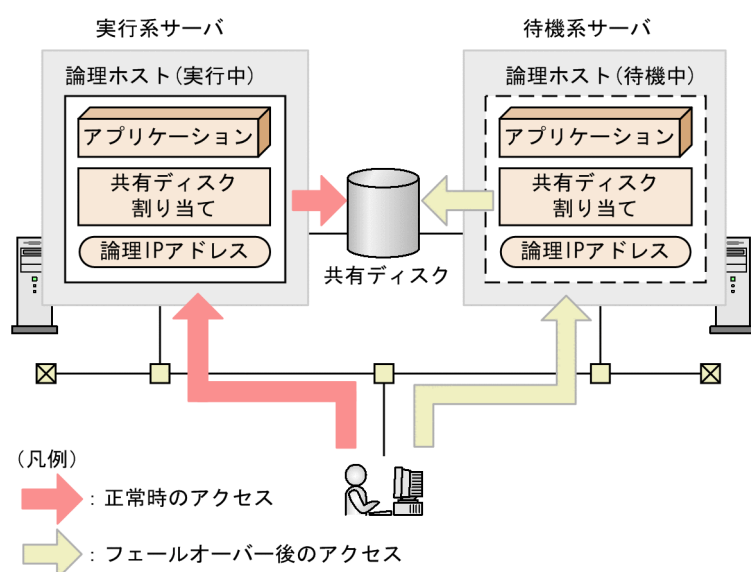
JP1/IM - Agent をクラスタ運用する場合、マネージャーで動作するモジュールについては、JP1/IM - Manager での対応と同じです。また、エージェントとして動作する JP1/IM - Agent がサポートするクラスタ構成については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.3.7(2) JP1/IM - Agent をクラスタシステムで運用する場合の構成」を参照してください。

7.1.1 クラスタシステムの概要 (Windows の場合)

クラスタシステムは処理を実行する実行系サーバと、障害が発生したときに処理を引き継げるように待機している待機系サーバで構成します。障害発生時は、実行系から待機系に処理を引き継いで業務の停止を防ぎ、可用性を向上させることができます。この障害時に処理を引き継ぐことを「フェールオーバー」といいます。

クラスタシステム全体を制御するソフトウェアを「クラスタソフト」といいます。クラスタソフトは、システムが正常に動作しているかを監視し、異常を検知した場合にはフェールオーバーを行って業務が止まることを防ぎます。

図 7-2 正常時、フェールオーバー後のアクセス



JP1/IM - Manager のようなアプリケーションがフェールオーバーできるようにするには「論理ホスト」で運用します。論理ホストは、クラスタソフトに制御された、フェールオーバーする際の単位となる論理的なサーバのことです。論理ホストは、ホスト名として「論理ホスト名」を使い、実行系から待機系に引き継ぎができる「共有ディスク」と「論理 IP アドレス」を持ちます。論理ホストで実行するアプリケーションは、共有ディスクにデータを格納し、論理 IP アドレスで通信することによって、物理的なサーバに依存しないで、フェールオーバーして実行することができます。

JP1/IM - Manager を、クラスタシステムの論理ホスト環境で運用することを「クラスタ運用」といいます。

メモ

「論理ホスト」という用語

このマニュアルではフェールオーバーの単位を意味する用語として「論理ホスト」を使いますが、クラスタソフトやアプリケーションによっては「グループ」や「パッケージ」などの用語が使われています。クラスタソフトのマニュアルなどを参照し、対応する用語を確認してください。

なお、フェールオーバーの単位となる論理的なサーバを論理ホストというのに対して、物理的なサーバを「物理ホスト」といいます。物理ホストが使うホスト名（hostname コマンドを実行したときに表示されるホスト名）を「物理ホスト名」、物理ホスト名に対応した IP アドレスを「物理 IP アドレス」といいます。また、ディスクは「ローカルディスク」を使います。これらはサーバ固有のものであり、ほかのサーバに引き継ぐことはできません。

7.1.2 クラスタ運用の前提条件（Windows の場合）

JP1/IM - Manager は、クラスタシステムでは論理ホスト環境で動作し、フェールオーバーに対応します。論理ホスト環境で実行する場合の JP1/IM - Manager の前提条件は、共有ディスクや論理 IP アドレスの割り当て・削除・動作監視がクラスタソフトによって正常に制御されていることです。

❗ 重要

JP1/IM - Manager がサポートしているクラスタソフトであっても、システム構成や環境設定によってはここで説明する前提条件を満たさない場合があります。前提条件を満たすよう、システム構成や環境設定を検討してください。

(1) 論理ホスト環境の前提条件

JP1/IM - Manager を論理ホスト環境で実行する場合、論理 IP アドレスと共有ディスクについて、次に示す前提条件があります。

表 7-1 論理ホスト環境の前提条件

論理ホストの構成要素	前提条件
共有ディスク	- 実行系から待機系へ引き継ぎ可能な共有ディスクが使用できること。 - JP1 を起動する前に、共有ディスクが割り当てられること。 - JP1 を実行中に、共有ディスクの割り当てが解除されないこと。 - JP1 を停止したあとに、共有ディスクの割り当てが解除されること。 - 共有ディスクが、不当に複数のノードから使用されないよう制御されていること。 - システムダウンなどでファイルが消えないよう、ジャーナル機能を持つファイルシステムなどでファイルを保護すること。 - フェールオーバーしてもファイルに書き込んだ内容が保証されて引き継がれること。 - フェールオーバー時に共有ディスクを使用中のプロセスがあっても、強制的にフェールオーバーができること。 - 共有ディスクの障害を検知した場合の回復処置はクラスタソフトなどが制御し、回復処置を JP1 が意識する必要がないこと。回復処置の延長で JP1 の起動や停止が必要な場合は、クラスタソフトから JP1 に起動や停止の実行要求をすること。
論理 IP アドレス	- 引き継ぎ可能な論理 IP アドレスを使って通信できること。 - 論理ホスト名から論理 IP アドレスが一意に求められること。 - JP1 を起動する前に、論理 IP アドレスが割り当てられること。

論理ホストの構成要素	前提条件
	- JP1 を実行中に、論理 IP アドレスが削除されないこと。 - JP1 を実行中に、論理ホスト名と論理 IP アドレスの対応が変更されないこと。 - JP1 を停止したあとに、論理 IP アドレスが削除されること。 - ネットワーク障害を検知した場合の回復処置はクラスタソフトなどが制御し、JP1 が回復処理を意識する必要がないこと。また、回復処置の延長で JP1 の起動や停止が必要な場合は、クラスタソフトから JP1 に起動や停止の実行要求をすること。

上記の条件が満たされていない場合は、JP1 の動作に問題が発生することがあります。例えば、次のような問題が発生します。

- 実行系で書き込んだデータが、フェールオーバーした時に壊れてしまう場合
JP1 でエラー・データ消失・起動失敗などの問題が発生し、正常に動作できません。
- LAN ボード障害が発生しても回復処理がされない場合
クラスタソフトなどの制御によって LAN ボードが切り替えられるか、または他サーバへフェールオーバーするまで、通信エラーが発生し JP1 は正常に動作できません。

(2) 物理ホスト環境の前提条件

JP1/IM - Manager を論理ホストで運用するクラスタシステムでは、各サーバの物理ホスト環境が次に示す前提条件を満たしている必要があります。

表 7-2 物理ホスト環境の前提条件

物理ホストの構成要素	前提条件
サーバ本体	2 台以上のサーバ機によるクラスタ構成になっていること。 - 実行する処理に応じた CPU 性能があること。 (例えば、論理ホストを多重起動する場合などに、対応できる CPU 性能があること) - 実行する処理に応じた実メモリー容量があること。 (例えば、論理ホストを多重起動する場合などに、対応できる実メモリー容量があること)
ディスク	システムダウンなどでファイルが消えないよう、ジャーナル機能を持つファイルシステムなどでファイルを保護すること。
ネットワーク	- 物理ホスト名 (hostname コマンドを実行したときに表示されるホスト名) に対応する IP アドレスで通信が可能なこと。 (クラスタソフトなどにより通信ができない状態に変更されないこと) ※ - JP1 の動作中に、ホスト名と IP アドレスの対応が変更されないこと。 (クラスタソフトやネームサーバなどによって変更がされないこと) - Windows の場合、ホスト名に対応した LAN ボードがネットワークのバインド設定で最優先になっていること。 (ハートビート用などほかの LAN ボードが優先になっていないこと)

物理ホストの構成要素	前提条件
OS, クラスタソフト	- JP1 がサポートするクラスタソフトおよびバージョンであること。 - JP1 およびクラスタソフトが前提とするパッチやサービスパックが適用済みであること。 - フェールオーバーしても同じ処理ができるよう、各サーバの環境が適切に設定されていること。
サービス	リモート監視構成の場合、JP1/Base のログファイルトラップサービスが起動していること。

注※

クラスタソフトによっては、物理ホスト名（hostname コマンドを実行したときに表示されるホスト名）に対応する IP アドレスで通信ができなくなる構成場合があります。この場合、物理ホスト環境の JP1 は動作できません。論理ホスト環境の JP1 だけを使用してください。

(3) JP1 がサポートする範囲

クラスタシステムで論理ホストの JP1 を運用する場合、JP1 が制御する範囲は、JP1 自身の動作だけです。論理ホスト環境（共有ディスクおよび論理 IP アドレス）の制御、および JP1 の起動や停止の契機はクラスタソフトの制御に依存します。

前述の論理ホスト環境および物理ホスト環境の前提条件が満たされていない、または論理ホスト環境の制御に問題がある場合は、JP1 の動作に発生した問題もサポートの対象外となります。この場合は、論理ホスト環境を制御しているクラスタソフトや OS で問題に対処してください。

(4) 物理ホスト名

物理ホスト名は、IM データベースを使用する場合、半角英数字、-、および.（ピリオド）で構成される 32 文字以内の文字列で指定してください。

(5) 論理ホスト名

JP1/IM - Manager で論理ホスト名を指定する場合、次の点について確認してください。

- hosts ファイルやネームサーバに設定されていて、TCP/IP 通信ができること。
- 前提である JP1/Base で扱える論理ホスト名であること。詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。
- IM データベースを使用するときは、半角英数字、および半角ハイフン（-）で構成される 32 文字以内の文字列であること。

JP1/IM - Agent で論理ホスト名を指定する場合、次の点について確認してください。

- hosts ファイルやネームサーバに設定されていて、TCP/IP 通信ができること。
- 論理ホスト名は、半角英数字、および半角ハイフン（-）で構成される 63 文字以内の文字列であること。

(6) その他の条件

JP1/IM - Agent を使用する場合は、次の点に注意してください。

- Windows 環境の場合、実行系サーバと待機系サーバに JP1/IM - Agent をインストールするときは、インストール先を同一フォルダにすること。
- 実行系サーバと待機系サーバに JP1/IM - Agent をインストールするときは、バージョンを同じにすること。
- SAP システムのログ抽出コマンドをインストールする場合、実行系サーバと待機系サーバで同様のセットアップを実施すること。SAP システムのログ抽出コマンドの入出力ファイル※は共有ディスク上に配置すること。

注※

コマンドの入出力ファイルは次のとおりです。

- 環境パラメーター設定ファイル
 - SAP システムのログ抽出コマンドのログファイル
 - SAP システムのログ抽出コマンドのトレースファイル
 - RFC ライブラリが出力するトレースファイル
- Web シナリオ監視機能を使用する場合、実行系と待機系に同一の Web シナリオファイルを配置すること。
 - クラスタ環境のホスト間で Web シナリオファイルをコピーするときは、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「1.5.1(9)(c)Web シナリオファイルの別ホストへの移行」に記載している手順を実施して、コピー先ホストの Web exporter で問題なくシナリオ実行できるようにすること。

7.1.3 クラスタシステムでの JP1/IM の構成 (Windows の場合)

クラスタシステムで JP1/IM - Manager を運用するには、クラスタソフトの制御により論理ホストの JP1/IM - Manager および JP1/Base を実行し、フェールオーバーに対応します。このときの JP1/IM の構成は次のようになります。

(1) クラスタ運用での JP1/IM の構成の概要

表 7-3 クラスタシステムでの JP1/IM の構成

製品名	クラスタシステムでの JP1/IM の構成
JP1/IM - View	• JP1/IM - View から JP1/IM - Manager に接続するときは、論理 IP アドレスあてに接続します。 • JP1/IM - View 自身は物理ホスト環境で動作します。
JP1/IM - Manager	• 論理ホスト環境で動作することができます。 • クラスタソフトに登録することで、フェールオーバーに対応します。

製品名	クラスタシステムでの JP1/IM の構成
	- クラスタソフトに登録するときは、前提リソースとして論理 IP アドレスと共有ディスクが必要です。 - 共有ディスクに定義情報を格納し、フェールオーバー時に引き継ぎます。 - 一つのサーバで複数の論理ホストを実行できます。このため、アクティブ・スタンバイ構成だけでなく、アクティブ・アクティブ構成のクラスタシステムでも運用できます。 - JP1/IM - Manager は前提製品 JP1/Base と同じ論理ホストで実行します。

(2) 共有ディスク上のファイル構成

論理ホスト環境の JP1/IM - Manager をセットアップすると、共有ディスク上に次のファイルが作成されます。これらは、論理ホストで JP1/IM - Manager を実行するために必要なファイルです。

表 7-4 共有ディスク上のファイル構成 (Windows)

機能	共有ファイルの種別	フォルダ名
セントラルコンソール	定義ファイル	共有フォルダ¥jp1cons¥conf¥
	ログファイル	共有フォルダ¥jp1cons¥log¥
	一時ファイル	共有フォルダ¥jp1cons¥tmp¥
	履歴ファイル※	共有フォルダ¥jp1cons¥operation¥
セントラルスコープ	定義ファイル	共有フォルダ¥jp1scope¥conf¥
	ログファイル	共有フォルダ¥jp1scope¥log¥
	一時ファイル	共有フォルダ¥jp1scope¥tmp¥
	データベース	共有フォルダ¥jp1scope¥database¥
IM 構成管理	定義ファイル	共有フォルダ¥JP1IMM¥conf¥imcf¥
	ログファイル	共有フォルダ¥JP1IMM¥log¥imcf¥
	一時ファイル	共有フォルダ¥JP1IMM¥tmp¥
	IM 構成のデータおよびプロファイルのデータ	共有フォルダ¥JP1IMM¥data¥imcf¥
IM データベース	データベース	共有ディスク上のユーザーが指定したフォルダ¥imdb
インテリジェント統合管理データベース	実行ファイル	マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.7.1(1)(d) 関連ファイルの格納先」の「 ■ インテリジェント統合管理データベースの実行ファイルの格納先」を参照してください。
	ログファイル	マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.7.1(1)(d) 関連ファイルの格納先」の「 ■ 運用コマンドの個別ログの格納先」および「 ■ トレンドデータ管理サービスのログの格納先」を参照してください。

機能	共有ファイルの種別	フォルダ名
	データファイル	マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.7.1(1)(d) 関連ファイルの格納先」の「 ■ インテリジェント統合管理データベースのデータファイルの格納先」を参照してください。

注※ 関連イベント発行サービスの処理、共通除外条件による除外処理、および共通除外条件定義の更新処理が履歴として出力されます。

(3) JP1/IM - Manager のサービスおよびプロセス

クラスタ運用での JP1/IM - Manager は、論理ホストのサービスまたはプロセスを実行します。

論理ホスト環境の JP1/IM - Manager をセットアップすると、次のサービスが Windows に登録されます。このサービスをクラスタソフトに登録して実行します。

表 7-5 JP1/IM - Manager のサービス (Windows)

表示名称	サービス名
JP1/IM3-Manager_論理ホスト名	JP1_Console_論理ホスト名
JP1/IM3-Manager DB Server_論理ホスト名 ^{※1}	HiRDBEmbeddedEdition_JMn ^{※2}
JP1/IM3-Manager DB Cluster Service_論理ホスト名 ^{※1}	HiRDBClusterService_JMn ^{※2}

注※1

IM データベースを使用する場合に登録されます。

注※2

n は 1~9 の数字です。この数字は、クラスタセットアップ情報ファイルで LOGICALHOSTNUMBER に指定した値と一致します。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。

表示名称の欄は、[コントロールパネル] - [管理ツール] - [サービス] で表示される名前です。また、クラスタソフトからサービスを net コマンド (net start や net stop) で制御する場合は、この名前を net コマンドに指定します。

サービス名の欄は、クラスタソフトに登録する場合の名前です。これを WSFC (Windows Server(R) Failover Cluster) の「サービス名」の設定項目に指定します。

(4) 通信方式

論理ホストの JP1/IM - Manager をセットアップすると、JP1/IM - Manager の通信方式を IP バインド方式と呼ぶ方式に設定します。IP バインド方式に変更するのは、論理ホストと物理ホストの両方の環境が対象です。

通信方式には、IP バインド方式と ANY バインド方式の 2 種類があります。これは、通信するときに使用する IP アドレスを、内部処理で割り当て (バインド) をする方法をきめます。

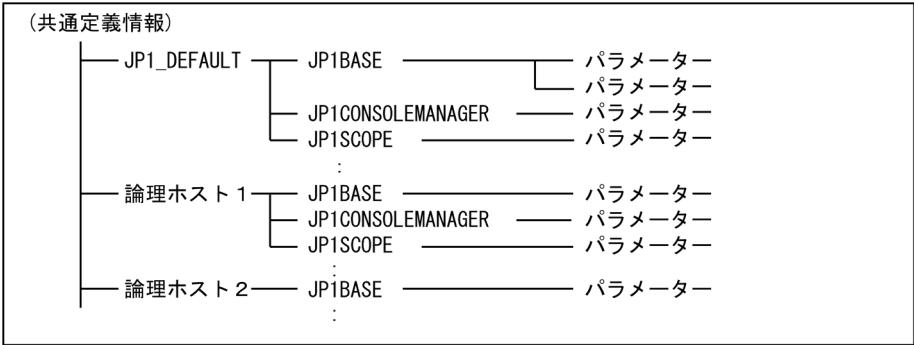
通信方式については、マニュアル「JP1/Base 運用ガイド」の JP1/Base の通信方式に関する説明を参照してください。JP1/IM - Manager は、JP1/Base と同じ通信方式で通信をします。

(5) 共通定義情報の設定

論理ホストの JP1/IM - Manager をセットアップすると、共通定義情報に、論理ホスト用の設定情報が設定されます。

共通定義情報とは、JP1 の設定情報を格納するデータベースで、JP1/Base が管理しています。設定情報のデータは、各サーバのローカルディスク上に、次のような形式で格納されています。

図 7-3 共通定義情報



共通定義情報は、物理ホスト（JP1_DEFAULT）および論理ホストごとに分かれて格納されています。物理ホストおよび論理ホスト単位に、jbssetcnf コマンドで設定し、jbsgetcnf コマンドで読み出します。

論理ホストの共通定義情報は、各サーバで同じ内容になるようにします。セットアップ時および設定変更時は、設定をした実行系サーバの共通定義情報を、待機系サーバへコピーして設定します。

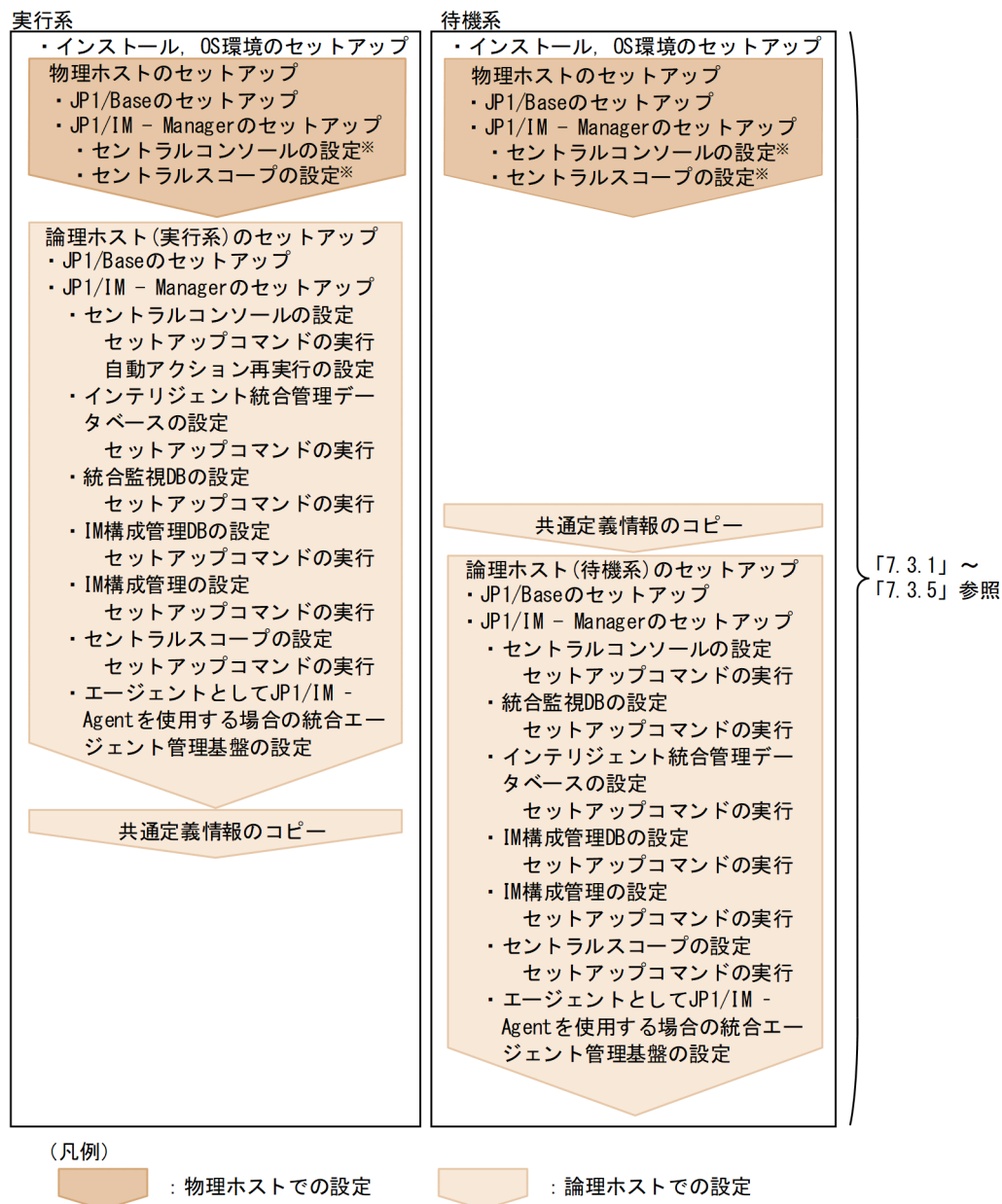
なお、共通定義情報は、JP1/IM - Manager、JP1/Base、JP1/AJS、および JP1/Power Monitor（06-02 以降）が設定情報を格納するために使用しています。

7.2 クラスタ運用の環境設定の流れ（Windows の場合）

クラスタ運用に対応するための JP1/IM - Manager および JP1/IM - Agent の環境設定について説明します。セットアップの作業の流れを示します。

なお、インテリジェント統合管理基盤のクラスタシステムの設定については「7.4 インテリジェント統合管理基盤のクラスタ環境を構築する（Windows の場合）」を参照してください。

図 7-4 セットアップ作業の流れ（新規に環境設定する場合（JP1/IM - Manager））



注※ 物理ホストでJP1/IM - Managerを起動する場合に設定します。

図 7-5 セットアップ作業の流れ（新規に環境設定する場合（JP1/IM - Agent））

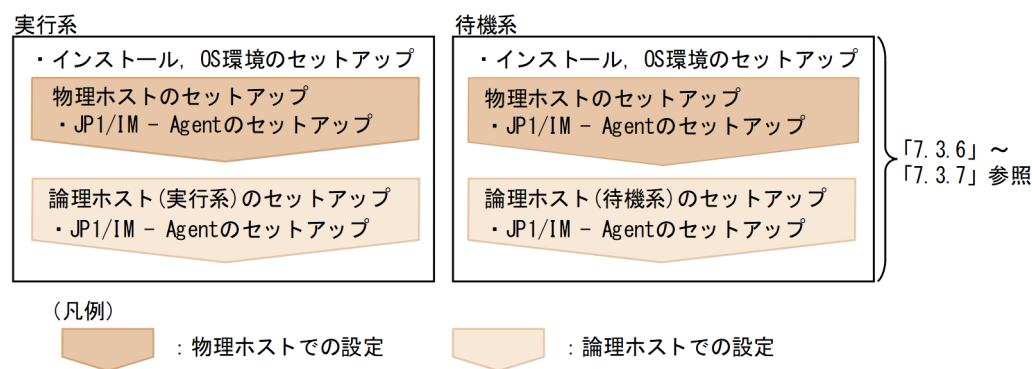
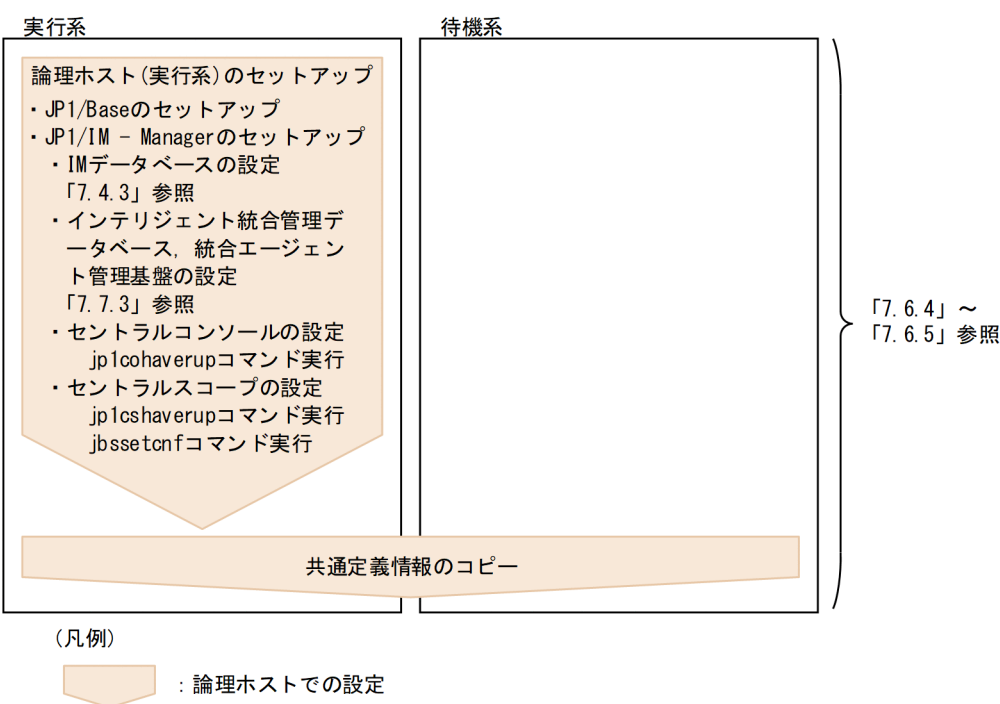


図 7-6 セットアップ作業の流れ（既存の論理ホスト環境をバージョンアップする場合（JP1/IM - Manager））



7.3 論理ホストの新規インストール・セットアップ (Windows の場合)

JP1/IM - Manager および JP1/IM - Agent の論理ホストの新規インストールおよびセットアップについて説明します。なお、JP1/IM - Manager と同じ論理ホストに JP1/Base をセットアップする必要があるため、あわせて説明します。

作業を始める前に、クラスタシステムについて次の情報を確認してください。

表 7-6 論理ホストのインストール・セットアップ前の確認 (Windows)

確認項目	説明
論理ホスト名	JP1 を実行する論理ホストのホスト名
論理 IP アドレス	論理ホスト名に対応する IP アドレス
共有フォルダ	論理ホストの JP1 の実行環境ファイル一式を格納する共有ディスク上のフォルダ

また、これらが「[7.1.2 クラスタ運用の前提条件 \(Windows の場合\)](#)」を満たしていることを確認してください。

確認ができれば、インストール・セットアップを始めます。

なお、論理ホスト名は、英大文字・英小文字を区別します。論理ホスト名には、JP1/Base で設定した論理ホスト名を英大文字・英小文字を含めて正確に指定してください。誤った論理ホスト名を指定し、論理ホストのインストール・セットアップを行ってしまった場合は、IM データベースと論理ホストを削除してから、再度、論理ホストのインストール・セットアップを行ってください。IM データベースと論理ホストの削除については、「[7.7.1 論理ホストの削除 \(Windows の場合\)](#)」を参照してください。

7.3.1 JP1/Base および JP1/IM - Manager の新規インストール (Windows の場合)

実行系サーバ、待機系サーバそれぞれのローカルディスク上に JP1/IM - Manager および JP1/Base をインストールしてください。

なお、JP1/IM - Manager をインストールすると、JP1/IM - Agent を利用するための統合エージェント管理基盤もインストールされます。

1. JP1/Base をインストールする。
2. JP1/IM - Manager をインストールする。

実行系サーバ・待機系サーバとも、同じ名称のドライブおよびフォルダにインストールしてください。

また、共有ディスク上には、インストールしないでください。

統合エージェント管理基盤と統合エージェント制御基盤で暗号化通信を行う場合は、統合エージェント管理基盤に関する次の手順を実施します。

1. サーバ証明書とサーバ証明書のキーファイルを配置する。

暗号通信（HTTPS）を有効にする場合は、クラスタ環境のサーバ証明書とキーファイル（秘密鍵ファイル）を共有ディレクトリに配置する。

7.3.2 JP1/IM - Manager の新規インストール時の物理ホスト環境のセットアップ（Windows の場合）

実行系サーバ、待機系サーバそれぞれで、JP1/Base および JP1/IM - Manager をインストール後、JP1/Base および JP1/IM - Manager の物理ホスト環境のセットアップをしてください。

なお、JP1/IM - Manager をインストールすると、JP1/IM - Agent を利用するための統合エージェント管理基盤もインストールされます。

1. JP1/Base の物理ホスト環境をセットアップする。

2. JP1/IM - Manager の物理ホスト環境をセットアップする。

JP1/Base のセットアップ手順については、マニュアル「JP1/Base 運用ガイド」を参照してください。

JP1/IM - Manager のセットアップ手順は、クラスタ運用ではない場合と同じ手順です。手順については、「[1. インストールとセットアップ（Windows の場合）](#)」を参照してください。なお、物理ホストの JP1/IM - Manager を使わない場合は、セットアップの必要はありません。

7.3.3 JP1/IM - Manager の新規インストール時の論理ホスト環境（実行系）のセットアップ（Windows の場合）

(1) セットアップの前準備

1. JP1/IM と JP1/Base のサービスが停止していることを確認する。

物理ホストおよびすべての論理ホストの、JP1/IM と JP1/Base のサービスが停止していることを確認してください。JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスも停止してください。

2. 共有ディスクが使用可能なことを確認する。

(2) JP1/Base のセットアップ

1. JP1/Base の論理ホスト（実行系）をセットアップする。

手順の詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

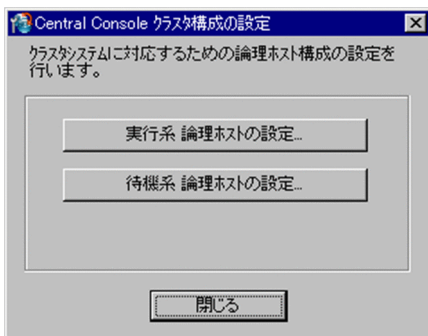
2. JP1/Base のコマンド実行環境を設定する。

jcocmddef コマンドを実行して、JP1/Base のコマンド実行環境を設定します。jcocmddef コマンドの詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

(3) JP1/IM - Manager (セントラルコンソール) の設定

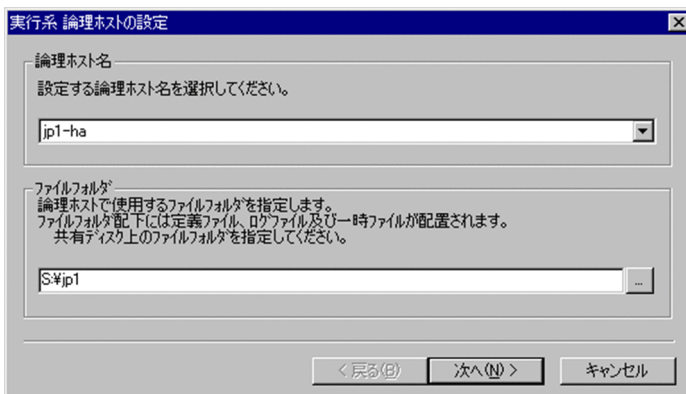
1. JP1/IM - Manager (セントラルコンソール) の論理ホストの設定画面を起動する。

Console パス¥bin¥jp1cohasetup.exe を実行すると、クラスタ構成の設定画面 (実行系) が表示されます。



2. [実行系論理ホストの設定] ボタンをクリックする。

論理ホストの設定画面が表示されます。



論理ホスト名と、ファイルフォルダを指定します。

- 論理ホスト名

JP1/Base で作成した論理ホスト名が表示されますので、選択します。

- ファイルフォルダ

共有ディスク上のフォルダを指定してください。「指定したフォルダ名¥jp1cons¥」フォルダ下に、論理ホストの JP1/IM - Manager のファイル一式が作成されます。

設定したら [次へ] ボタンをクリックします。

3. 設定内容を確認する。

次の画面が表示されます。



設定内容を確認してください。設定内容が正しければ、[完了] ボタンをクリックしてください。

なお、論理ホストの JP1/IM - Manager の環境設定は、物理ホストの設定値を引き継ぎます。必要に応じて、jcoimdef コマンド (-h オプション) で論理ホストの環境設定をカスタマイズしてください。

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

続けて、フェールオーバー時に自動アクションの再実行が適切に動作するように論理ホストの JP1/IM - Manager (セントラルコンソール) の環境設定をカスタマイズします。

4. 自動アクションの再実行の設定をする。

次のコマンドを実行して、フェールオーバー時の自動アクションの再実行について設定をします。コマンドに指定するシステム環境の設定情報は、物理ホストの定義情報を引き継ぎます。物理ホストのシステム環境の設定情報を確認し、必要に応じて論理ホストのシステム環境を設定してください。

`jcoimdef -r { EXE | OUTPUT | OFF } -h 論理ホスト名`

フェールオーバー時に次の状態となっているアクションに対する動作を設定できます。

- 送信待機
- 送信待機 (キャンセル中)
- 送信待機 (キャンセル失敗)
- 送信中
- 送信中 (キャンセル中)
- 送信中 (キャンセル失敗)
- キューイング
- キューイング (キャンセル中)
- キューイング (キャンセル失敗)
- 実行中
- 実行中 (キャンセル中)
- 実行中 (キャンセル失敗)

EXE を指定するとアクションを再実行し、OUTPUT を指定するとアクションの一覧をファイルに出力し、OFF を指定すると処理を行いません。システム設計時の検討内容に従って設定してください。この設定は任意です。

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

(4) JP1/IM - Manager (統合監視 DB) の設定

JP1/IM - Manager (統合監視 DB) を使用する場合は、必要です。統合監視 DB を使用して JP1 イベントを管理するためには、統合監視 DB を構築する必要があります。

1. クラスタセットアップ情報ファイルを編集する。

統合監視 DB を構築するために必要なデータベース領域のサイズやデータベース格納ディレクトリの情報を記述したクラスタセットアップ情報ファイルを準備します。

クラスタセットアップ情報ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。

2. jcodbsetup コマンドを実行し、統合監視 DB を作成する。

```
jcodbsetup -f クラスタセットアップ情報ファイル名 -h 論理ホスト名 -c online [-q]
```

引数により、クラスタセットアップ情報ファイル名、論理ホスト名、セットアップ種別を指定します。

- クラスタセットアップ情報ファイル名 (-f オプション)

手順 1. で作成したクラスタセットアップ情報ファイル名を指定します。

- 論理ホスト名 (-h オプション)

実行系サーバでセットアップした論理ホスト名を指定します。

論理ホスト名には、JP1/Base で設定した論理ホスト名を、大文字・小文字を含めて正確に指定してください。JP1/Base のセットアップについては、「[7.3.3\(2\) JP1/Base のセットアップ](#)」を参照してください。

- セットアップ種別 (-c オプション)

実行系ホストのセットアップ種別 (online) を指定します。

「online」を指定する場合は、共有ディスクをマウントし、論理ホストと通信できる状態にしてください。

jcodbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcodbsetup」(1. コマンド) を参照してください。

3. jcoimdef コマンドを実行して、統合監視 DB を有効にする。

```
jcoimdef -db ON -h 論理ホスト名
```

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

(5) JP1/IM - Manager（インテリジェント統合管理データベース）の設定

インテリジェント統合管理データベースを使用している場合の、インテリジェント統合管理データベース（トレンドデータ管理 DB）の論理ホスト環境の構築手順を、次に示します。

1. JP1/IM - Manager の論理ホスト環境を構築する。

インテリジェント統合管理データベースの論理ホスト環境の構築では、作成済みの JP1/IM - Manager の論理ホスト環境を参照する必要があるため、インテリジェント統合管理データベースの論理ホスト環境を構築する前に、JP1/IM - Manager（セントラルコンソール）の論理ホスト環境を構築します。また、統合オペレーション・ビューアーの前提機能であるインテリジェント統合管理基盤の構築、統合監視 DB の設定も行う必要があります。すでに構築済みの場合は、次の手順に進みます。

JP1/IM - Manager（セントラルコンソール）の論理ホスト環境の構築手順については、[「7.3.3\(3\) JP1/IM - Manager（セントラルコンソール）の設定」](#)を参照してください。また、インテリジェント統合管理基盤の構築については、[「4.4 インテリジェント統合管理基盤のクラスタ環境を構築する」](#)、統合監視 DB の設定については、[「7.3.3\(4\) JP1/IM - Manager（統合監視 DB）の設定」](#)を参照してください。

2. クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイルを準備する。

クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイルに、データディレクトリ、ポート番号などの必要な定義を記述します。

マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイル (jimgnbdbclustersetupinfo.conf)」(2. 定義ファイル)を参照して、インテリジェント統合管理データベースセットアップ情報ファイルを編集してください。

3. jimgnbdbsetup コマンドを実行する。

次のコマンドを実行します。

```
jimgnbdbsetup -f クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイル
-h 論理ホスト名 -c online
```

4. サービスの依存関係を設定する。

JP1/IM - Manager をクラスタ運用するには、論理ホストの JP1/IM - Manager および JP1/Base をクラスタソフトに登録して、クラスタソフトからの制御で起動・停止するように設定します。

JP1/IM - Manager をクラスタに登録する設定内容は、次のとおりです。

表 7-7 クラスタソフトに登録する設定内容（Windows）

項番	名前	サービス名	依存関係
1	JP1/Base Event 論理ホスト名	JP1_Base_Event 論理ホスト名	IP アドレスリソース 物理ディスクリソース
2	JP1/Base_論理ホスト名	JP1_Base_論理ホスト名	項番 1 のクラスタリソース

項番	名前	サービス名	依存関係
3	JP1/IM3-Manager DB Server_論理ホスト名※1	HiRDBEmbeddedEdition_JMn※2	項番 1 および項番 2 のクラスタリソース
4	JP1/IM3-Manager DB Cluster Service_論理ホスト名※1	HiRDBClusterService_JMn※2	項番 1, 項番 2 および項番 3 のクラスタリソース
5	JP1/IM3-Manager_論理ホスト名	JP1_Console_論理ホスト名	項番 1, 項番 2, 項番 3, 項番 4, 項番 6, および項番 7 のクラスタリソース※3※4
6	JP1/IM3-Manager Intelligent Integrated DB Server_論理ホスト名	JP1_IMGNDDB_Service_論理ホスト名	項番 1, 項番 2 および項番 3 のクラスタリソース
7	JP1/IM3-Manager Trend Data Management Service_論理ホスト名	promscale_論理ホスト名	項番 1, 項番 2, 項番 3 および項番 6 のクラスタリソース

注※1

IM データベースを使用する場合だけ、クラスタソフトに登録してください。

注※2

n は 1～9 の数字です。この数字は、クラスタセットアップ情報ファイルで LOGICALHOSTNUMBER に指定した値と一致します。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。

5. クラスタソフトから JP1/IM - Manager のサービスを起動する

クラスタソフトから次のサービスを起動します。

JP1/IM3-Manager Intelligent Integrated DB Server_論理ホスト名

JP1/IM3-Manager Trend Data Management Service_論理ホスト名

(6) JP1/IM - Manager (IM 構成管理 DB) の設定 (任意)

JP1/IM - Manager (IM 構成管理 DB) を使用する場合に設定します。IM 構成管理 DB を使用してシステムの階層構成 (IM 構成) を管理するためには、IM 構成管理 DB を構築する必要があります。

1. クラスタセットアップ情報ファイルを編集する。

IM 構成管理 DB を構築するために必要なデータベース領域のサイズやデータベース格納ディレクトリの情報を記述したクラスタセットアップ情報ファイルを準備します。

クラスタセットアップ情報ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。

2. jcfdbssetup コマンドを実行して、IM 構成管理 DB を作成する。

```
jcfdbssetup -f クラスタセットアップ情報ファイル名 -h 論理ホスト名 -c online [-q]
```

引数により、クラスタセットアップ情報ファイル名、論理ホスト名、セットアップ種別を指定します。

- クラスタセットアップ情報ファイル名 (-f オプション)

手順 1 で作成したクラスタセットアップ情報ファイル名を指定します。

- 論理ホスト名 (-h オプション)

実行系サーバでセットアップした論理ホスト名を指定します。

論理ホスト名には、JP1/Base で設定した論理ホスト名を、大文字・小文字を含めて正確に指定してください。JP1/Base のセットアップについては、「[7.3.3\(2\) JP1/Base のセットアップ](#)」を参照してください。

- セットアップ種別 (-c オプション)

実行系ホストのセットアップ種別 (online) を指定します。

「online」を指定する場合は、共有ディスクをマウントし、論理ホストと通信できる状態にしてください。

jcfdbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcfdbsetup」(1. コマンド) を参照してください。

3. jcoimdef コマンドを実行して、IM 構成管理 DB を有効にする。

jcoimdef -cf ON -h 論理ホスト名

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

(7) JP1/IM - Manager (IM 構成管理) の設定 (任意)

JP1/IM - Manager (IM 構成管理) を使用する場合に設定します。なお、表示される設定画面は、タイトルバーに Configuration Management と表示される以外は、JP1/IM - Manager (セントラルコンソール) の場合と同じです。

1. JP1/IM - Manager (IM 構成管理) の論理ホストの設定画面を起動する。

Manager パス¥bin¥imcf¥jp1cfhassetup.exe コマンドを実行します。

2. [実行系論理ホストの設定] ボタンをクリックする。

[実行系論理ホストの設定] 画面で、論理ホスト名と、ファイルフォルダを指定します。

- 論理ホスト名

JP1/Base で作成した論理ホスト名が表示されますので、選択します。

- ファイルフォルダ

共有ディスク上のフォルダを指定してください。「指定したフォルダ名¥jp1imm¥」フォルダ下に、論理ホストの JP1/IM - Manager のファイル一式が作成されます。

設定したら [次へ] ボタンをクリックします。

3. 設定内容を確認する。

確認画面が表示されますので、設定内容を確認してください。設定内容が正しければ、[完了] ボタンをクリックしてください。

(8) JP1/IM - Manager (セントラルスコープ) の設定 (任意)

JP1/IM - Manager (セントラルスコープ) を使用する場合に設定します。なお、表示される設定画面は、タイトルバーに Central Scope と表示される以外は、JP1/IM - Manager (セントラルコンソール) の場合と同じです。

1. JP1/IM - Manager (セントラルスコープ) の論理ホストの設定画面を起動する。

Scope パス¥bin¥jp1cshasetup.exe を実行する。

2. [実行系論理ホストの設定] ボタンをクリックする。

[実行系論理ホストの設定] 画面で、論理ホスト名と、ファイルフォルダを指定します。

- 論理ホスト名

JP1/Base で作成した論理ホスト名が表示されますので、選択します。

- ファイルフォルダ

共有ディスク上のフォルダを指定してください。「指定したフォルダ名¥jp1scope¥」フォルダ下に、論理ホストの JP1/IM - Manager のファイル一式が作成されます。

設定したら [次へ] ボタンをクリックします。

3. 設定内容を確認する。

確認画面が表示されますので、設定内容を確認してください。設定内容が正しければ、[完了] ボタンをクリックしてください。

(9) エージェントとして JP1/IM - Agent を使用する場合の設定

(a) 統合エージェント管理基盤の設定変更

統合エージェント管理基盤 (imbase, imbaseproxy) の設定変更の手順を、次に示します。

■ 統合エージェント管理基盤のポートを変更する

次の手順を実施します。

1. 統合エージェント管理基盤を停止する。

2. 統合エージェント管理基盤のリッスンポート番号を変更する。

待ち受けポート番号の設定は、統合エージェント管理基盤の imbase 設定ファイル (jpc_imbase.json) と imbaseproxy 設定ファイル (jpc_imbaseproxy.json) の port メンバーに設定されています。これを新しいポート番号に変更します。

imbase 設定ファイルと imbaseproxy 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の該当するファイル (2. 定義ファイル) を参照してください。

3. 統合エージェント管理基盤を開始する。

■ 証明書を設定する

次の手順を実施します。

1. 統合エージェント管理基盤を停止する。

2. 統合エージェント管理基盤のサーバ証明書およびキーファイルを変更する。

リスポート番号は、imbase 設定ファイル (jpc_imbase.json) や imbaseproxy 設定ファイル (jpc_imbaseproxy.json) の cert_file や key_file のメンバーに設定されています。

cert_file や key_file の設定値、または、設定しているファイル自体を更新します。

imbase 設定ファイルと imbaseproxy 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「2. 定義ファイル」の、該当するファイルの説明を参照してください。

3. 統合エージェント管理基盤を開始する。

7.3.4 JP1/IM - Manager の新規インストール時の共通定義情報のコピー (Windows の場合)

実行系サーバの共通定義情報を、待機系サーバにコピーします。

共通定義情報には、論理ホストの JP1/IM - Manager および JP1/Base を実行するための設定情報が記録されています。次の手順でコピーしてください。

1. 実行系サーバで、共通定義情報を退避する。

実行系で jbsgetcnf コマンドを実行し、共通定義情報を退避します。

jbsgetcnf -h 論理ホスト名 > 共通定義情報退避ファイル名

なお、論理ホスト名は、大文字・小文字を区別します。論理ホスト名には、JP1/Base で設定した論理ホスト名を、大文字・小文字を含めて正確に指定してください。

2. 退避ファイルを、実行系サーバから待機系サーバにコピーする。

FTP など任意の方法でコピーしてください。

3. 待機系サーバで、共通定義情報を設定する。

待機系サーバに、実行系サーバからコピーした退避ファイルを使って、共通定義情報を設定します。

jbssetcnf 共通定義情報退避ファイル名

7.3.5 JP1/IM - Manager の新規インストール時の論理ホスト環境（待機系）のセットアップ（Windows の場合）

(1) セットアップの前準備

1. JP1/IM と JP1/Base のサービスが停止していることを確認する。

物理ホストおよびすべての論理ホストの、JP1/IM と JP1/Base のサービスが停止していることを確認してください。JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスも停止してください。

2. 実行系サーバで IM データベースをセットアップした場合は、実行系サーバで使したクラスタセットアップ情報ファイルを待機系サーバにコピーする（実行系サーバで IM データベースをセットアップしていない場合は不要）。

コピーしたファイルは、Manager パス¥conf¥imdb¥setup に格納してください。

なお、待機系サーバでは、共有ディスクが使用可能である必要はありません。

(2) JP1/Base のセットアップ

1. JP1/Base の論理ホスト（待機系）をセットアップする。

手順の詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

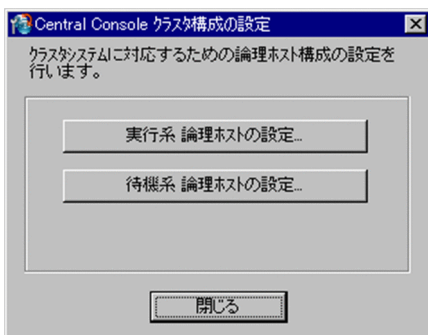
2. JP1/Base のコマンド実行環境を設定する。

jcocmddef コマンドを実行して、JP1/Base のコマンド実行環境を設定します。jcocmddef コマンドの詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

(3) JP1/IM - Manager（セントラルコンソール）の設定

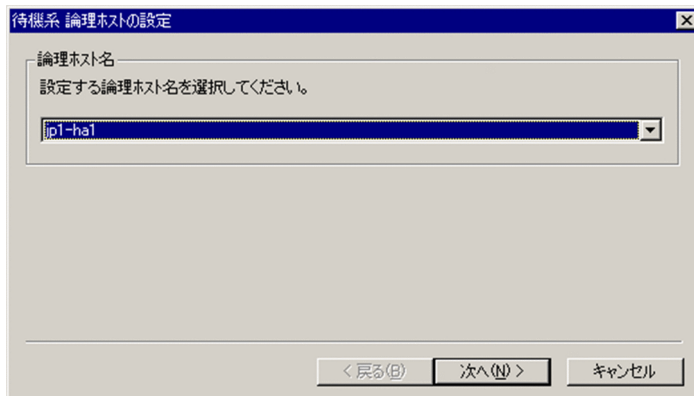
1. JP1/IM - Manager（セントラルコンソール）論理ホストの設定画面を起動する。

Console パス¥bin¥jp1cohasetup.exe コマンドを実行すると、クラスタ構成の設定画面（待機系）が表示されます。



2. [待機系論理ホストの設定] ボタンをクリックする。

論理ホストの設定画面が表示されます。



論理ホスト名を指定します。

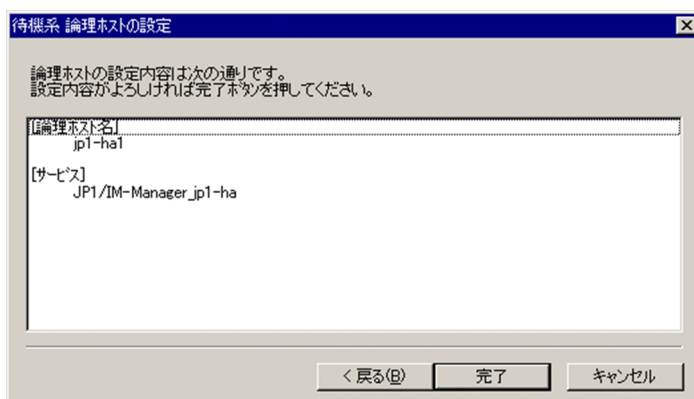
- 論理ホスト名

実行系サーバでセットアップした論理ホストを選択します。

設定したら [次へ] ボタンをクリックします。

3. 設定内容を確認する。

次の画面が表示されます。



設定内容を確認してください。設定内容が正しければ、[完了] ボタンをクリックしてください。

(4) JP1/IM - Manager（統合監視 DB）の設定

JP1/IM - Manager（統合監視 DB）を使用する場合は、必要です。統合監視 DB を使用して JP1 イベントを管理するためには、統合監視 DB を構築する必要があります。

1. クラスタセットアップ情報ファイルを確認する。

統合監視 DB を構築するために必要なデータベース領域のサイズやデータベース格納ディレクトリの情報を記述したクラスタセットアップ情報ファイルを準備します。「[7.3.5\(1\) セットアップの前準備](#)」で実行系のホストからコピーしたクラスタセットアップ情報ファイルの内容を確認してください。クラスタセットアップ情報ファイルは、実行系で指定した設定内容と同一である必要があります。

クラスタセットアップ情報ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。

2. jcodbsetup コマンドを実行し、統合監視 DB を作成する。

jcodbsetup -f クラスタセットアップ情報ファイル名 -h 論理ホスト名 -c standby [-q]

引数により、クラスタセットアップ情報ファイル名、論理ホスト名、セットアップ種別を指定します。

- クラスタセットアップ情報ファイル名 (-f オプション)
手順 1 で作成したクラスタセットアップ情報ファイル名を指定します。
- 論理ホスト名 (-h オプション)
実行系サーバでセットアップした論理ホスト名を指定します。
- セットアップ種別 (-c オプション)
待機系ホストのセットアップ種別 (standby) を指定します。

jcodbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcodbsetup」(1. コマンド) を参照してください。

(5) JP1/IM - Manager (インテリジェント統合管理データベース) の設定

インテリジェント統合管理データベースを使用している場合の、インテリジェント統合管理データベース (トレンドデータ管理 DB) の論理ホスト環境の構築手順を、次に示します。

1. JP1/IM - Manager の論理ホスト環境を構築する。

インテリジェント統合管理データベースの論理ホスト環境の構築では、作成済みの JP1/IM - Manager の論理ホスト環境を参照する必要があるため、インテリジェント統合管理データベースの論理ホスト環境を構築する前に、JP1/IM - Manager (セントラルコンソール) の論理ホスト環境を構築します。また、統合オペレーション・ビューアーの前提機能であるインテリジェント統合管理基盤の構築、統合監視 DB の設定も行う必要があります。すでに構築済みの場合は、次の手順に進みます。

JP1/IM - Manager (セントラルコンソール) の論理ホスト環境の構築手順については、[「7.3.5\(3\) JP1/IM - Manager \(セントラルコンソール\) の設定」](#)を参照してください。また、インテリジェント統合管理基盤の構築については、[「4.4 インテリジェント統合管理基盤のクラスタ環境を構築する」](#)、統合監視 DB の設定については、[「7.3.5\(4\) JP1/IM - Manager \(統合監視 DB\) の設定」](#)を参照してください。

2. クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイルを準備する。

クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイルに、データディレクトリ、ポート番号などの必要な定義を記述します。

マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイル (jimgnbdbclustersetupinfo.conf)」(2. 定義ファイル) を参照して、インテリジェント統合管理データベースセットアップ情報ファイルを編集してください。

3. jimgnbdbsetup コマンドを実行する。

次のコマンドを実行します。

```
jimgndbsetup -f クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイル  
-h 論理ホスト名 -c standby
```

4. サービスの依存関係を設定する。

JP1/IM - Manager をクラスタ運用するには、論理ホストの JP1/IM - Manager および JP1/Base をクラスタソフトに登録して、クラスタソフトからの制御で起動・停止するように設定します。

JP1/IM - Manager をクラスタに登録する設定内容については、「[7.5 新規インストール・セットアップでのクラスタソフトへの登録 \(Windows の場合\)](#)」を参照してください。

5. クラスタソフトから JP1/IM - Manager のサービスを起動する

クラスタソフトから次のサービスを起動します。

JP1/IM3-Manager Intelligent Integrated DB Server_論理ホスト名

JP1/IM3-Manager Trend Data Management Service_論理ホスト名

(6) JP1/IM - Manager (IM 構成管理 DB) の設定 (任意)

JP1/IM - Manager (IM 構成管理 DB) を使用する場合に設定します。IM 構成管理 DB を使用してシステムの階層構成 (IM 構成) を管理するためには、IM 構成管理 DB を構築する必要があります。

1. クラスタセットアップ情報ファイルを確認する。

IM 構成管理 DB を構築するために必要なデータベース領域のサイズやデータベース格納ディレクトリの情報を記述したクラスタセットアップ情報ファイルを準備します。「[7.3.5\(1\) セットアップの前準備](#)」で実行系のホストからコピーしたクラスタセットアップ情報ファイルの内容を確認してください。クラスタセットアップ情報ファイルは、実行系で指定した設定内容と同一である必要があります。

クラスタセットアップ情報ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。

2. jcfdbsetup コマンドを実行して、IM 構成管理 DB を作成する。

```
jcfdbsetup - f セットアップ情報ファイル名 - h 論理ホスト名 -c standby [-q]
```

引数により、クラスタセットアップ情報ファイル名、論理ホスト名、セットアップ種別を指定します。

- クラスタセットアップ情報ファイル名 (-f オプション)
手順 1 で作成したクラスタセットアップ情報ファイル名を指定します。
- 論理ホスト名 (-h オプション)
実行系サーバでセットアップした論理ホスト名を指定します。
- セットアップ種別 (-c オプション)
待機系ホストのセットアップ種別 (standby) を指定します。

jcfdbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcfdbsetup」(1. コマンド) を参照してください。

(7) JP1/IM - Manager (IM 構成管理) の設定 (任意)

JP1/IM - Manager (IM 構成管理) を使用する場合に設定します。なお、表示される設定画面は、タイトルバーに Configuration Management と表示される以外は、JP1/IM - Manager (セントラルコンソール) の場合と同じです。

1. JP1/IM - Manager (IM 構成管理) の論理ホストの設定画面を起動する。

Manager パス¥bin¥imcf¥jp1cfhasetup.exe コマンドを実行します。

2. [待機系論理ホストの設定] ボタンをクリックする。

[待機系論理ホストの設定] 画面で、論理ホスト名を指定します。

- 論理ホスト名

実行系サーバでセットアップした論理ホストを選択します。

設定したら [次へ] ボタンをクリックします。

3. 設定内容を確認する。

確認画面が表示されますので、設定内容を確認してください。設定内容が正しければ、[完了] ボタンをクリックしてください。

(8) JP1/IM - Manager (セントラルスコープ) の設定 (任意)

JP1/IM - Manager (セントラルスコープ) を使用する場合に設定します。なお、表示される設定画面は、タイトルバーに Central Scope と表示される以外は、JP1/IM - Manager (セントラルコンソール) の場合と同じです。

1. JP1/IM - Manager (セントラルスコープ) の論理ホストの設定画面を起動する。

Scope パス¥bin¥jp1cshasetup.exe コマンドを実行します。

2. [待機系論理ホストの設定] ボタンをクリックする。

[待機系論理ホストの設定] 画面で、論理ホスト名を指定します。

- 論理ホスト名

実行系サーバでセットアップした論理ホストを選択します。

設定したら [次へ] ボタンをクリックします。

3. 設定内容を確認する。

確認画面が表示されますので、設定内容を確認してください。設定内容が正しければ、[完了] ボタンをクリックしてください。

(9) エージェントとして JP1/IM - Agent を使用する場合の設定

実行系サーバで実施する手順と同じです。手順については、「[7.3.3\(9\)エージェントとして JP1/IM - Agent を使用する場合の設定](#)」を参照してください。

7.3.6 統合エージェントホストでの JP1/IM - Agent の新規インストール (Windows の場合)

実行系サーバ、待機系サーバそれぞれのローカルディスク上に JP1/IM - Agent をインストールしてください。

1. JP1/IM - Agent を新規インストールする。

インストール方法については、「[1.3.1\(3\)JP1/IM - Agent のインストールの手順](#)」を参照してください。
インストール時のインストールモードは「通常インストールモード」を選択します。

実行系サーバと待機系サーバの両方で実施します。

Windows の場合は、実行系サーバと待機系サーバでインストール先フォルダを同じパスにする必要があります。

物理ホストの JP1/IM - Agent のサービスは起動しないでください。起動している場合はすべて停止してください。

2. 論理ホスト用の新規セットアップコマンドの設定ファイルを作成する。

設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「論理ホスト新規セットアップの設定ファイル（任意のファイル名）」（2. 定義ファイル）を参照してください。

また、設定ファイルのサンプルファイルが、次のパスに格納されています。コピーして作成できます。

```
JP1/IM - Agentのインストール先フォルダ¥jplima¥conf¥sample¥jpc_lhsetup.properties
```

3. 論理ホスト用の新規セットアップコマンドを実行する。

```
jimalhsetup -h 論理ホスト名 -d 共有フォルダ -c {online|standby} -f セットアップ設定ファイル [-q]
```

論理ホスト用の新規セットアップコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimalhsetup」（1. コマンド）を参照してください。

実行系サーバと待機系サーバの両方で実施します。

4. Windows サービスが登録されたことを確認する。

実行系サーバと待機系サーバの両方で、Windows サービスを表示して、論理ホスト用のサービスが登録されたことを確認します。

論理ホスト用のサービスの名称は、「_論理ホスト名」が付加された名称となります。

5. TLS の設定を行う。

TLS を有効にして運用する場合は、共有フォルダ¥jplima¥conf¥user¥cert に CA 証明書ファイルを配置してください。

また、共有フォルダ¥jplima¥conf¥jpc_imagentcommon.json の immgr.tls_config.ca_file に CA 証明書のフルパスを記入してください。

6. 必要な設定を行う。

「7.3.7 統合エージェントホストでの JP1/IM - Agent の新規インストール時のセットアップ (Windows の場合)」, 「1.21.2 JP1/IM - Agent の設定」を参照して必要な設定変更を行います。

7. クラスタソフトに論理ホスト用のサービスを登録する。

JP1/IM - Agent のサービスのクラスタソフトへの登録については, 「7.5 新規インストール・セットアップでのクラスタソフトへの登録 (Windows の場合)」を参照してください。

8. クラスタの設定で JP1/IM - Agent のサービスが停止したと判定する期間を 1 分に設定する。

統合オペレーション・ビューアーに定義ファイルをアップロードすると, 定義ファイルを配置した後にサービスの再起動が行われることがあります。また, アップロードした定義ファイルの内容が不正でサービスの起動に失敗した場合, 定義ファイルを元に戻してサービスを起動します。

上記のように, 一時的にサービスが停止することがあるため, クラスタが一時的なサービス停止を検知しないように設定する必要があります。

9. 複数マネージャーホストへのデータ配信機能を使用する場合は, 動作確認の前に次の手順を実施する。

「7.3.7(2)(a) 複数マネージャーホストへのデータ配信機能を設定する (Windows の場合) (オプション)」の「新規設定」を実施します。

10. 動作に問題がないか確認する。

- クラスタソフトからサービスを起動します。
- フェールオーバーさせます。

7.3.7 統合エージェントホストでの JP1/IM - Agent の新規インストール時のセットアップ (Windows の場合)

クラスタ構成では, 次の点に注意してください。

- JP1/IM - Agent のファイルやフォルダについて, 共有ディスク上のファイルやフォルダが対象になる場合があります。
- 統合エージェントホストでの JP1/IM - Agent のサービスの起動と停止は, クラスタソフトから行います。
- サービス定義ファイルの設定変更を行う場合は, 実行系サーバと待機系サーバの両方で行う必要があります。また, 設定する値も同じ値を設定する必要があります。
- セキュリティ製品の除外設定では, 共有フォルダ¥jp1ima も除外対象にする必要があります。

(1) 自動起動の設定

クラスタソフトで制御するため, OS 起動時のサービス自動起動の設定は行いません。

(2) 統合エージェント制御基盤の設定

(a) 複数マネージャーホストへのデータ配信機能を設定する（Windows の場合）（オプション）

■ 新規設定

1. クラスタソフトから JP1/IM - Agent サービスを停止する。

停止するサービスのサービスキーを次に示します。

- jpc_imagent
- jpc_imagentaction
- jpc_imagentproxy
- jpc_alertmanager
- jpc_prometheus_server
- jpc_fluentd

2. 統合エージェント管理基盤のセカンダリー用のフォルダを作成する。

統合エージェント管理基盤のセカンダリー用のフォルダとして、次のフォルダを作成します。

- 共有フォルダ¥jp1ima¥tmp¥download-imagent グループ識別子
- 共有フォルダ¥jp1ima¥tmp¥upload-imagent グループ識別子
- 共有フォルダ¥jp1ima¥tmp¥jbsfwd-imagent グループ識別子
- 共有フォルダ¥jp1ima¥logs¥imagent-imagent グループ識別子
- 共有フォルダ¥jp1ima¥logs¥imagentproxy-imagent グループ識別子
- 共有フォルダ¥jp1ima¥logs¥imagentaction-imagent グループ識別子

上記のフォルダの作成には、次のコマンドを使用します。

```
mkdir フォルダ
```

3. 統合エージェント管理基盤のセカンダリー用のファイルを作成する。

実行系サーバと待機系サーバの両方で実施します。

Agent パス¥bin 下にあるコピー元のファイルをコピーし、コピー先のファイル名にリネームします。

コピー元のファイル名	コピー先のファイル名
jpc_imagent_service.exe	jpc_imagent-imagent グループ識別子_service_論理ホスト名.exe
jpc_imagent_service_論理ホスト名.xml	jpc_imagent-imagent グループ識別子_service_論理ホスト名.xml
jpc_imagentproxy_service.exe	jpc_imagentproxy-imagent グループ識別子_service_論理ホスト名.exe
jpc_imagentproxy_service_論理ホスト名.xml	jpc_imagentproxy-imagent グループ識別子_service_論理ホスト名.xml

コピー元のファイル名	コピー先のファイル名
jpc_imagentaction_service.exe	jpc_imagentaction-imagent グループ識別子_service_論理ホスト名.exe
jpc_imagentaction_service_論理ホスト名.xml	jpc_imagentaction-imagent グループ識別子_service_論理ホスト名.xml

4. サービスの起動設定を行う。

実行系サーバと待機系サーバの両方で実施します。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(c) セカンダリーのサービス起動の設定」を参照してください。

5. 統合エージェント制御基盤のセカンダリー用の設定を行う。

実行系サーバで実施します。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(d) 統合エージェント制御基盤の設定ファイル」を参照してください。

6. 統合エージェント制御基盤のセカンダリー用のシークレットを登録する。

実行系サーバで実施します。

セカンダリーの統合エージェント制御基盤が接続する JP1/IM - Manager の初期シークレットを取得して登録します。

登録する初期シークレットのキーについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(e) 初期シークレット、クライアントシークレット、および HTTP プロキシパスワードのキー」を参照してください。

7. 統合エージェント制御基盤以外の設定を行う。

実行系サーバで実施します。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(f) 統合エージェント制御基盤以外の各プログラムの送信設定」を参照してください。

8. 次のコマンドを実行して、サービス定義ファイルで定義したサービスを有効化する。

実行系サーバと待機系サーバの両方で実施します。

```
Agentパス¥tools¥jpc_service -on サービスキー -h 論理ホスト名
```

サービスキーについては、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「10.1 JP1/IM - Agent のサービス」に記載している Windows 環境での JP1/IM - Agent のサービスキーのうち、「-imagent グループ識別子」が付いているものを使用します。

9. クラスタソフトに論理ホスト用のサービスを登録する。

クラスタソフトに登録するサービスは、次のとおりです。

サービス	依存関係
jpc_imagent-imagent グループ識別子_service_論理ホスト名	- IP アドレスリソース - 物理ディスクリソース

サービス	依存関係
jpc_imagentproxy-imagent グループ識別子_service_論理ホスト名	jpc_imagent-imagent グループ識別子_service_論理ホスト名
jpc_imagentaction-imagent グループ識別子_service_論理ホスト名	jpc_imagentproxy-imagent グループ識別子_service_論理ホスト名

クラスタソフトに登録するコマンドについては、「[7.3.6 統合エージェントホストでの JP1/IM - Agent の新規インストール（Windows の場合）](#)」の手順 7「クラスタソフトに論理ホスト用のサービスを登録する。」を参照してください。

■ バージョンアップ時の設定

複数マネージャーホストへのデータ配信機能を有効にしているバージョンからのバージョンアップの場合は、下記の手順を実施してください。

下記の手順は、バージョンアップインストール時の「[1.3.1\(3\)\(b\) インストール手順](#)」の手順 5 のあと（手順 6 の前）に実施します。

1. 統合エージェント管理基盤のセカンダリー用のファイルを作成する。

Agent パス¥bin 下にあるコピー元のファイルをコピーし、コピー先のファイル名にリネームします。

コピー元のファイル名	コピー先のファイル名
jpc_imagent_service.exe	jpc_imagent-imagent グループ識別子_service_論理ホスト名.exe
jpc_imagentproxy_service.exe	jpc_imagentproxy-imagent グループ識別子_service_論理ホスト名.exe
jpc_imagentaction_service.exe	jpc_imagentaction-imagent グループ識別子_service_論理ホスト名.exe

(b) 複数マネージャーホストへのデータ配信機能を解除する（Windows の場合）（オプション）

複数マネージャーホストへのデータ配信機能を使用しなくなった場合の設定手順を次に示します。

ご使用の運用環境に合わせて、次のどちらかを実施します。

- ・ 論理ホストのアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する
- ・ 論理ホストのアンインストールを行う

■ 論理ホストのアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合

1. 論理ホストで稼働している JP1/IM - Agent のサービスを停止する。

実行系サーバだけで実施します。

クラスタソフトから論理ホストで稼働しているサービスを停止します。

2. クラスタソフトに登録されたサービスを解除する。

実行系サーバだけで実施します。

「7.3.7(2)(a) 複数マネージャーホストへのデータ配信機能を設定する (Windows の場合) (オプション)」の手順 8 で登録したサービスを解除します。

サービスを解除する方法については、クラスタソフトのドキュメントを確認してください。

3. Windows に登録されたセカンダリーのサービスを解除する。

実行系サーバと待機系サーバの両方で実施します。

解除方法については、「7.7.3 JP1/IM - Agent のアンインストール (Windows の場合)」の手順 3 を参照してください。

4. 複数マネージャーホストへのデータ配信機能を使用するために作成したシークレットを削除する。

実行系サーバで実施します。

削除するシークレットのキーについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(e) 初期シークレット, クライアントシークレット, および HTTP プロキシパスワードのキー」を参照してください。

すでに消えているシークレットについては、この手順は不要です。

5. 複数マネージャーホストへのデータ配信機能を使用するために設定した内容を元に戻す。

「7.3.7(2)(a) 複数マネージャーホストへのデータ配信機能を設定する (Windows の場合) (オプション)」の「新規設定」の手順 4 と手順 7 で設定した統合エージェント制御基盤のセカンダリー用の設定を元に戻します。

6. 複数マネージャーホストへのデータ配信機能を使用するためにコピーしたファイルを削除する。

「7.3.7(2)(a) 複数マネージャーホストへのデータ配信機能を設定する (Windows の場合) (オプション)」の「新規設定」の手順 2 でコピーした統合エージェント管理基盤のセカンダリー用のファイルを削除します

7. 複数マネージャーホストへのデータ配信機能を使用するために作成したフォルダを削除する。

ログなどの必要なファイルを退避したあと、「7.3.7(2)(a) 複数マネージャーホストへのデータ配信機能を設定する (Windows の場合) (オプション)」の「新規設定」の手順 1 で作成した統合エージェント管理基盤のセカンダリー用のフォルダを削除します。

8. 無効化したセカンダリーのサービスが接続している JP1/IM - Manager 側で登録している統合エージェント情報を削除する。

JP1/IM - Manager の実行系サーバと待機系サーバの両方で実施します。JP1/IM - Agent の実行系サーバと待機系サーバでは実施しません。

統合エージェント情報の削除手順については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.1 [統合エージェント一覧] 画面」を参照してください。

■ 論理ホストのアンインストールを行う場合

「7.7.3 JP1/IM - Agent のアンインストール (Windows の場合)」の手順 1 と手順 2 の間に、上記の「論理ホストのアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合」の手順 4 から手順 8 を実施します。

実施後に、上記の「論理ホストのアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合」の手順 9 を実施します。

(3) OS シャットダウン時の自動停止の設定

クラスタソフトで制御するため、OS シャットダウン時のサービス停止の設定は行いません。

(4) その他の設定

クラスタ構成での設定変更の手順については、通常ホストの設定変更と基本的に同じです。通常ホストの設定変更については、「1.21 JP1/IM - Agent のセットアップ (Windows の場合)」を参照してください。

7.4 インテリジェント統合管理基盤のクラスタ環境を構築する（Windows の場合）

クラスタシステムで運用されている JP1/IM - Manager ホストに対応する場合に、インテリジェント統合管理基盤で行うクラスタ環境の構築について説明します。

なお、インテリジェント統合管理基盤のクラスタ環境を構築すると、JP1/IM - Manager サービスの起動時間が延びます。クラスタソフトで JP1/IM - Manager サービスの起動時間を監視している場合や JP1/Base の起動管理機能で JP1/IM - Manager サービスを起動している場合は、クラスタソフトのタイムアウト値を見直す必要があります。インテリジェント統合管理基盤を設定したあとでサービスの起動時間を確認し、タイムアウト値を調整してください。

インテリジェント統合管理基盤の共有ディスク上のファイル構成を、次の表に示します。

表 7-8 共有ディスク上のファイル構成

OS	共有ファイル種別	フォルダ名
Windows	定義ファイル	共有フォルダ¥jp1imm¥conf¥imdd¥ 共有フォルダ¥jp1imm¥conf¥ssl¥※
	ログファイル	共有フォルダ¥jp1imm¥log¥imdd¥
	プラグイン	共有フォルダ¥jp1imm¥plugin¥imdd¥
	データファイル	共有フォルダ¥jp1imm¥data¥imdd¥
	対処アクション実行履歴	共有フォルダ¥jp1imm¥log¥suggestion

注※ ssl フォルダは、通信暗号化機能を有効にして JP1/IM3-Manager サービスを起動すると作成されます。

7.4.1 クラスタ環境を新規構築する（Windows の場合）

インテリジェント統合管理基盤のクラスタ環境の新規構築手順を次に示します。

セットアップ後に JP1/IM - Manager を起動する手順については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3. JP1/IM - Manager の起動と終了」を参照してください。

なお、次の手順を行う前に、セントラルコンソールと統合監視 DB のクラスタ環境の構築が完了していることを確認してください。

1. JP1/IM - Manager を停止する。

物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止してください。

2. 定義ファイルのフォルダをコピーする。

物理ホストの定義ファイルの imdd フォルダを、共有フォルダにコピーします。次のコマンドを実行します。


```
xcopy Managerパス¥conf¥imdd 共有フォルダ¥jp1imm¥conf¥imdd /s/e/i
```

3. プラグインのフォルダをコピーする。

物理ホストのプラグインのplugin フォルダを、共有フォルダにコピーします。次のコマンドを実行します。

```
xcopy Managerパス¥plugin 共有フォルダ¥jp1imm¥plugin /s/e/i
```

4. データファイル出力先フォルダを作成する。

データファイル出力先フォルダとして「共有フォルダ¥jp1imm¥data¥imdd¥」を作成します。次のコマンドを実行します。

```
mkdir 共有フォルダ¥jp1imm¥data¥imdd¥
```

5. イベント転送中継情報フォルダを作成する。

イベント転送中継情報フォルダとして「共有フォルダ¥jp1imm¥data¥imdd¥eventForward¥」を作成します。次のコマンドを実行します。

```
mkdir 共有フォルダ¥jp1imm¥data¥imdd¥eventForward¥
```

6. インテリジェント統合管理基盤定義ファイル (imdd.properties) を編集します。

論理ホストの統合監視 DB のセットアップ時に使用したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) の LOGICALHOSTNUMBER パラメーターと IMDBPORT パラメーターに指定した値をインテリジェント統合管理基盤定義ファイルに指定します。

```
jp1.im.db.DEFAULT.logicalHostNum=LOGICALHOSTNUMBERの設定値  
jp1.im.db.DEFAULT.portNo=IMDBPORTの設定値
```

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。また、トレンドデータ削除を実行するときのインターバルとして、インテリジェント統合管理基盤定義ファイル (imdd.properties) の設定項目「jp1.imdd.trenddata.deleteInterval」に、「[7.5.3 クラスタソフトのパラメーターの設定 \(Windows の場合\)](#)」で「監視する間隔」に指定した値の 2 倍の値を設定します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」で、「2.7.2(3)(g)トレンドデータの手動削除 (統合エージェント, ユーザー独自の Prometheus, ユーザー独自の Fluentd のホスト名を指定して削除)」の「[トレンドデータの削除時の注意事項](#)」の 1. を参照してください。

7. 次のjcoimdef コマンドを実行して、インテリジェント統合管理基盤を有効にします。

```
Consoleパス¥bin¥jcoimdef -dd ON -hostmap ON -h 論理ホスト名
```

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

8. 操作履歴出力先フォルダを作成する。

操作履歴出力先フォルダとして「共有フォルダ¥jp1imm¥operation¥imdd¥suggestion¥」を作成します。
次のコマンドを実行します。

```
mkdir 共有フォルダ¥jp1imm¥operation¥imdd¥suggestion¥
```

9. インテリジェント統合管理データベースをセットアップする。

インテリジェント統合管理データベースの論理ホスト環境を構築します。

- 実行系ホストの場合
構築手順については、「[7.3.3\(5\) JP1/IM - Manager \(インテリジェント統合管理データベース\) の設定](#)」を参照してください。
- 待機系ホストの場合
構築手順については、「[7.3.5\(5\) JP1/IM - Manager \(インテリジェント統合管理データベース\) の設定](#)」を参照してください。

10. サービスを起動する。

クラスタソフトから次のサービスを起動します。

- JP1/IM3-Manager_論理ホスト名
- JP1/IM3-Manager DB Server_論理ホスト名
- JP1/IM3-Manager DB Cluster Service_論理ホスト名
- JP1/IM3-Manager Intelligent Integrated DB Server_論理ホスト名
- JP1/IM3-Manager Trend Data Management Service_論理ホスト名

7.4.2 修正版を適用したクラスタ環境を構築する (Windows の場合)

修正版を適用したクラスタ環境の構築手順について説明します。クラスタ環境に修正版を適用した場合は、プラグインの再配置が必要です。

1. JP1/IM - Manager を停止する。

物理ホスト環境，論理ホスト環境すべての JP1/IM - Manager を停止してください。

2. プラグインのフォルダをコピーする。

物理ホストのプラグインの plugin フォルダを，共有フォルダにコピーします。次のコマンドを実行します。

```
xcopy Managerパス¥plugin 共有フォルダ¥jp1imm¥plugin /s/e/i
```

3. サービスを起動する。

クラスタソフトから JP1/IM-Manager_論理ホスト名のサービスを起動します。

7.4.3 バージョンアップしてクラスタ環境を構築する (Windows の場合)

インテリジェント統合管理基盤をクラスタ環境で使用している場合に、バージョンアップする手順について説明します。なお、手順を実行しない場合、旧バージョンから追加された機能は使用できません。

また、連携製品のバージョンアップも同時に実施する場合は、手順 9 を実行する前に連携製品のバージョンアップを実施してください。

1. JP1/IM - Manager を停止する。

物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止してください。

2. プラグインのフォルダをコピーする。

物理ホストのプラグインの plugin フォルダを、共有フォルダにコピーします。次のコマンドを実行します。

```
xcopy Managerパス¥plugin 共有フォルダ¥jp1imm¥plugin /s/e/i
```

3. 定義ファイルをコピーする。

物理ホストの定義ファイルを、共有フォルダにコピーします。次のコマンドを実行します。

```
robocopy Managerパス¥conf¥imdd 共有フォルダ¥jp1imm¥conf¥imdd /e /xn /xo /xc
xcopy Managerパス¥conf¥imdd¥*.model 共有フォルダ¥jp1imm¥conf¥imdd /y
xcopy Managerパス¥conf¥imdd¥system¥*.model 共有フォルダ¥jp1imm¥conf¥imdd¥system /y
xcopy Managerパス¥conf¥imdd¥system¥*.update 共有フォルダ¥jp1imm¥conf¥imdd¥system /y
xcopy Managerパス¥conf¥imdd¥system¥fileoperation¥*.update 共有フォルダ¥jp1imm¥conf¥imdd¥system¥fileoperation /y
xcopy Managerパス¥conf¥imdd¥responseaction¥*.model 共有フォルダ¥jp1imm¥conf¥imdd¥responseaction /y
xcopy Managerパス¥conf¥imdd¥fileoperation¥*.model 共有フォルダ¥jp1imm¥conf¥imdd¥fileoperation /y
xcopy Managerパス¥conf¥imdd¥suggestion¥*.model 共有フォルダ¥jp1imm¥conf¥imdd¥suggestion /y
xcopy Managerパス¥conf¥imdd¥plugin 共有フォルダ¥jp1imm¥conf¥imdd¥plugin /s/e/i/y
echo f | xcopy 共有フォルダ¥jp1imm¥conf¥imdd¥system¥imdd_system.properties.update 共有フォルダ¥jp1imm¥conf¥imdd¥system¥imdd_system.properties /y
echo f | xcopy 共有フォルダ¥jp1imm¥conf¥imdd¥system¥fileoperation¥imdd_product_deffile_list.json.update 共有フォルダ¥jp1imm¥conf¥imdd¥system¥fileoperation¥imdd_product_deffile_list.json /y
```

4. イベント転送中継情報フォルダを作成する。

イベント転送中継情報フォルダとして「共有フォルダ¥jp1imm¥data¥imdd¥eventForward¥」を作成します。次のコマンドを実行します。

```
mkdir 共有フォルダ¥jp1imm¥data¥imdd¥eventForward¥
```

5. インテリジェント統合管理データベースをセットアップする。

V12 の JP1/IM - Manager からバージョンアップした場合は、インテリジェント統合データベースの論理ホスト環境を構築します。

- 実行系ホストの場合

構築手順については、「[7.3.3\(5\) JP1/IM - Manager \(インテリジェント統合管理データベース\) の設定](#)」を参照してください。

- 待機系ホストの場合

構築手順については、「[7.3.5\(5\) JP1/IM - Manager \(インテリジェント統合管理データベース\) の設定](#)」を参照してください。

6. 新しい設定値を追加する。

利用する機能に合わせて、新しく追加された設定値を追加します。※

注※

JP1/IM - Manager を 13-00 または 13-01 から 13-10 以降にバージョンアップした場合、テキストエディターなどで、次のファイルの末尾に「web-enable-admin-api: true」の行を追加します。なお、インテリジェント統合管理データベースを再構築したときは、自動で追加されるため、この手順は不要です。

共有フォルダ¥jplimm¥conf¥imgndb¥config.yml

上記の手順を実施しなかった場合、トレンドデータの削除と統合エージェント情報の削除が失敗します。

トレンドデータの削除と統合エージェント情報については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.1 [統合エージェント一覧] 画面」、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.11.4 トレンドデータ削除」および「5.18.2 統合エージェント情報削除」を参照してください。

7. サービスの依存関係を設定する。

統合エージェント管理基盤とインテリジェント統合管理データベースのサービスをクラスタソフトに登録して、クラスタソフトからの制御で起動・停止するように設定します。

依存関係の設定内容については、「[7.3.5\(5\) JP1/IM - Manager \(インテリジェント統合管理データベース\) の設定](#)」を参照してください。

8. サービスを起動する。

クラスタソフトから次のサービスを起動します。

- JP1/IM3-Manager_論理ホスト名
- JP1/IM3-Manager Intelligent Integrated DB Server_論理ホスト名
- JP1/IM3-Manager Trend Data Management Service_論理ホスト名
- JP1/IM3-Agent Base Server_論理ホスト名
- JP1/IM3-Agent Base Proxy Server_論理ホスト名

9. jddcreatetree コマンドを実行して、IM 管理ノード関連ファイルを生成する。

jddcreatetree コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jddcreatetree」(1. コマンド)を参照してください。

10. `jddupdatetree` コマンドを新規・再構築モードで実行して、定義内容をインテリジェント統合管理サーバに反映する。

`jddupdatetree` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jddupdatetree`」(1. コマンド)を参照してください。

7.5 新規インストール・セットアップでのクラスタソフトへの登録 (Windows の場合)

新規にインストール・セットアップする場合、JP1/IM - Manager をクラスタ運用するには、論理ホストの JP1/IM - Manager, JP1/Base, および JP1/IM - Agent をクラスタソフトに登録して、クラスタソフトからの制御で起動・停止するように設定します。

起動については、リソース, JP1/Base, JP1/IM - Manager, JP1/IM - Agent の順番でサービスを起動してください。

JP1/IM - Manager をクラスタソフトに登録する設定内容は、次のとおりです。

次の表の項番 1～4 の順番でサービスを起動してください (JP1/Base, JP1/IM - Manager の順番で起動する)。

表 7-9 JP1/IM - Manager をクラスタソフトに登録する設定内容 (Windows)

項番	名前	サービス名	依存関係
1	JP1/Base Event 論理ホスト名	JP1_Base_Event 論理ホスト名	IP アドレスリソース 物理ディスクリソース
2	JP1/Base_論理ホスト名	JP1_Base_論理ホスト名	項番 1 のクラスタリソース
3	JP1/IM3-Manager DB Server_論理ホスト名※1	HiRDBEmbeddedEdition_JMn※2	項番 1 および項番 2 のクラスタリソース
4	JP1/IM3-Manager DB Cluster Service_論理ホスト名※1	HiRDBClusterService_JMn※2	項番 1, 項番 2 および項番 3 のクラスタリソース
5	JP1/IM3-Manager_論理ホスト名	JP1_Console_論理ホスト名	項番 1, 項番 2, 項番 3, 項番 4, 項番 6 および項番 7 のクラスタリソース※3※5
6	JP1/IM3-Manager Intelligent Integrated DB Server_論理ホスト名※4	JP1_IMGNDDB_Service_論理ホスト名	項番 1, 項番 2 および項番 3 のクラスタリソース
7	JP1/IM3-Manager Trend Data Management Service_論理ホスト名※4	promscale_論理ホスト名	項番 1, 項番 2, 項番 3 および項番 6 のクラスタリソース

注※1

IM データベースを使用する場合だけ、クラスタソフトに登録してください。

注※2

n は 1～9 の数字です。この数字は、クラスタセットアップ情報ファイルで LOGICALHOSTNUMBER に指定した値と一致します。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。

注※3

IM データベースを使用しない場合は、項番 3 および項番 4 のクラスタリソースを依存関係から除いてください。

注※4

インテリジェント統合管理データベースを使用する場合だけ、クラスタソフトに登録してください。

注※5

インテリジェント統合管理データベースを使用しない場合は、項番 6 および項番 7 のクラスタリソースを依存関係から除いてください。

JP1/IM - Agent をクラスタソフトに登録する設定内容は、次のとおりです。

クラスタソフトに登録するときは、次の依存関係となるように設定します。使用するサービスだけをクラスタソフトに登録します。

表 7-10 JP1/IM - Agent をクラスタソフトに登録する設定内容（Windows）

サービス	依存関係
jpc_windows_exporter_service_論理ホスト名	- IP アドレスリソース - 物理ディスクリソース
jpc_blackbox_exporter_service_論理ホスト名	- IP アドレスリソース - 物理ディスクリソース
jpc_ya_cloudwatch_exporter_service_論理ホスト名	- IP アドレスリソース - 物理ディスクリソース
jpc_imagent_service_論理ホスト名	- IP アドレスリソース - 物理ディスクリソース
jpc_imagentproxy_service_論理ホスト名	jpc_imagent_service_論理ホスト名
jpc_imagentaction_service_論理ホスト名	jpc_imagentproxy_service_論理ホスト名
jpc_alertmanager_service_論理ホスト名	- jpc_windows_exporter_service_論理ホスト名 - jpc_blackbox_exporter_service_論理ホスト名 - jpc_ya_cloudwatch_exporter_service_論理ホスト名 - jpc_script_exporter_service_論理ホスト名 - jpc_promitor_resource_discovery_service_論理ホスト名 - jpc_promitor_scraper_service_論理ホスト名 - jpc_imagentaction_service_論理ホスト名
jpc_prometheus_server_service_論理ホスト名	jpc_alertmanager_service_論理ホスト名
jpc_fluentd_service_論理ホスト名	jpc_imagentaction_service_論理ホスト名
jpc_web_exporter_論理ホスト名	- IP アドレスリソース - 物理ディスクリソース
jpc_vmware_exporter_service_論理ホスト名	- IP アドレスリソース - 物理ディスクリソース
jpc_windows_exporter_hyperv_service_論理ホスト名	- IP アドレスリソース - 物理ディスクリソース

7.5.1 クラスタソフトへの登録 (Windows の場合)

(1) MSCS (Microsoft Cluster Service) または WSFC (Windows Server Failover Cluster) の場合

JP1/IM - Manager および JP1/Base のサービスを、MSCS または WSFC のリソースとして登録します。各リソースの設定は次のようにします。次の [] は、MSCS の設定項目です。WSFC の設定方法については、WSFC のマニュアルを参照してください。

- [リソースの種類] は「汎用サービス」として登録する。
- [名前] [依存関係] [サービス名] を表のとおりを設定する。
なお、名前はサービスを表示するときの名称で、サービス名は MSCS から制御するサービスを指定するときの名称です。
- [起動パラメータ] および [レジストリ複製] は、設定しない。
- プロパティの [詳細設定] ページを、JP1/IM - Manager の障害時にフェールオーバーするかどうかの運用に合わせて設定する。
例えば、JP1/IM - Manager の障害時に、フェールオーバーするように設定するには、[再開する] チェックボックスと [グループに適用する] チェックボックスをチェックし、3 回を目安に再起動試行回数の [しきい値] を設定してください。

(2) サービスの起動停止コマンドを登録する場合

JP1/IM - Manager および JP1/Base のサービスを、起動・停止するようクラスタソフトに登録してください。例えば、表の「名前」の項目で示すサービスを、net コマンドで起動停止するように設定してください。

なお、JP1/IM - Manager および JP1/Base の動作確認する場合は、次のコマンドを使ってください。

- jco_spmd_status
JP1/IM - Manager (IM データベースを除く) の動作確認をする場合
- jimdbstatus
IM データベースを使用時に IM データベースの動作確認をする場合
- jbs_spmd_status
JP1/Base の動作確認をする場合
- jevstat
JP1/Base イベントサービスの動作確認をする場合

これらのコマンドの使い方については、各コマンドのリファレンスを参照してください。また「[8.5 新規インストール・セットアップでのクラスタソフトへの登録 \(UNIX の場合\)](#)」の説明を参考にしてください。

7.5.2 リソースの起動停止順序の設定 (Windows の場合)

論理ホストの JP1/IM - Manager および JP1/Base を実行するには、共有ディスクおよび論理 IP アドレスが使用可能になっている必要があります。

クラスタソフトの制御によって次のように起動停止の順序または依存関係を設定してください。

- 論理ホストの起動時
 1. 共有ディスクおよび論理 IP アドレスを割り当てて使用可能にする。
 2. JP1/Base, JP1/IM - Manager の順に起動する。
- 論理ホストの停止時
 1. JP1/IM - Manager, JP1/Base の順に停止する。
 2. 共有ディスクおよび論理 IP アドレスの割り当てを解除する。

7.5.3 クラスタソフトのパラメーターの設定 (Windows の場合)

「7.5 新規インストール・セットアップでのクラスタソフトへの登録 (Windows の場合)」の「表 7-9 JP1/IM - Manager をクラスタソフトに登録する設定内容 (Windows)」に記載している「JP1/IM3-Manager Trend Data Management Service_論理ホスト名」のサービスに対して、次の設定をします。設定する値の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」で、「2.7.2(3)(g) トレンドデータの手動削除 (統合エージェント, ユーザー独自の Prometheus, ユーザー独自の Fluentd のホスト名を指定して削除)」の「**■**トレンドデータの削除時の注意事項」の 1.を参照してください。

- 監視する間隔：14 秒以上
- 停止したと判断する回数：連続で 2 回以上

7.6 論理ホストのバージョンアップインストール・セットアップ (Windows の場合)

JP1/IM - Manager および JP1/IM - Agent の論理ホストのバージョンアップインストールおよびセットアップについて説明します。なお、JP1/IM - Manager と同じ論理ホストに JP1/Base をセットアップする必要がありますので、あわせて説明します。

作業を始める前に、クラスタシステムについて次の情報を確認してください。

表 7-11 論理ホストのインストール・セットアップ前の確認 (Windows)

確認項目	説明
論理ホスト名	JP1 を実行する論理ホストのホスト名
論理 IP アドレス	論理ホスト名に対応する IP アドレス
共有フォルダ	論理ホストの JP1 の実行環境ファイル一式を格納する共有ディスク上のフォルダ

また、これらが「[7.1.2 クラスタ運用の前提条件 \(Windows の場合\)](#)」を満たしていることを確認してください。

確認ができれば、インストール・セットアップを始めます。

なお、論理ホスト名は、英大文字・英小文字を区別します。論理ホスト名には、JP1/Base で設定した論理ホスト名を英大文字・英小文字を含めて正確に指定してください。誤った論理ホスト名を指定し、論理ホストのインストール・セットアップを行ってしまった場合は、IM データベースと論理ホストを削除してから、再度、論理ホストのインストール・セットアップを行ってください。IM データベースと論理ホストの削除については、「[7.7.1 論理ホストの削除 \(Windows の場合\)](#)」を参照してください。

7.6.1 JP1/Base および JP1/IM - Manager のバージョンアップインストール (Windows の場合)

実行系サーバ、待機系サーバそれぞれのローカルディスク上に JP1/IM - Manager および JP1/Base をインストールしてください。

1. 設定情報とデータベースをバックアップする。

バックアップの方法は、過去のバージョンのマニュアルを参照してください。

2. JP1/Base をインストールする。

3. JP1/IM - Manager をインストールする。

❗ 重要

IM データベースをセットアップ済みの環境で、JP1/IM - Manager をバージョンアップした場合、jimdbupdate コマンドを実行して IM データベースを更新してください。IM データベースを更新していない場合は、JP1/IM - Manager を起動したときに警告メッセージが表示されます。

❗ 重要

インテリジェント統合管理データベースをセットアップ済みの環境で、JP1/IM - Manager をバージョン 13-10 以前から 13-11 以降にバージョンアップした場合、jimgndbupdate コマンドを実行してインテリジェント統合管理データベースを更新してください。インテリジェント統合管理データベースを更新していない場合、JP1/IM - Manager のサービス起動に失敗することがあります。

7.6.2 JP1/IM - Agent のバージョンアップインストール (Windows の場合)

JP1/IM - Agent をバージョン 13-00 または 13-01 からバージョンアップする場合、「[1.3.3\(14\) JP1/IM - Agent をバージョン 13-00 または 13-01 からバージョンアップした場合の注意事項](#)」も参照してください。

1. JP1/IM - Agent のサービスを停止する。

クラスタソフトから論理ホストの JP1/IM - Agent のサービスを停止します。

物理ホストでも運用している場合は、物理ホストの JP1/IM - Agent のサービスを停止します。

2. JP1/IM - Agent をバージョンアップインストールする。

インストール方法については、「[1.3.1\(3\) JP1/IM - Agent のインストールの手順](#)」を参照してください。

実行系サーバと待機系サーバの両方で実施します。

3. 論理ホスト用のバージョンアップセットアップコマンドの設定ファイルを作成する。

設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「論理ホストバージョンアップセットアップの設定ファイル（任意のファイル名）」（2. 定義ファイル）を参照してください。

また、設定ファイルのサンプルファイルが、次のパスに格納されています。コピーして作成できます。

```
JP1/IM - Agentのインストール先フォルダ¥jplima¥conf¥sample¥jpc_lhupdate.properties
```

4. 論理ホスト用のバージョンアップセットアップコマンドを実行する。

```
jimalhupdate -h 論理ホスト名 -d 共有フォルダ -c {online|standby} -f セットアップ設定ファイル [-q]
```

論理ホスト用のバージョンアップセットアップコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimalhupdate」(1. コマンド) を参照してください。

実行系サーバと待機系サーバの両方で実施します。

5. Windows サービスが登録されたことを確認する。

実行系サーバと待機系サーバの両方で、Windows サービスを表示して、論理ホスト用のサービスが登録されたことを確認します。

論理ホスト用のサービスの名称は、「_論理ホスト名」が付加された名称となります。

6. 追加されたアドオンプログラムに必要な設定を行う。

追加されたアドオンプログラムを使用する場合、「1.21.2(13) Web シナリオ監視機能の設定」, 「1.21.2(14) VMware exporter の設定」, 「1.21.2(3)(i) Web exporter のスクレイプジョブを追加する (Windows の場合) (オプション)」, および「1.21.2(3)(j) VMware exporter のスクレイプジョブを追加する (Windows の場合だけ) (オプション)」を参照して必要な設定を行います。

7. クラスタソフトに論理ホスト用のサービスを登録する。

クラスタソフトに登録するときは、次の依存関係となるように設定します。使用するサービスだけをクラスタソフトに登録します。

サービス	依存関係
jpc_web_exporter_service_論理ホスト名	• IP アドレスリソース • 物理ディスクリソース
jpc_vmware_exporter_service_論理ホスト名	• IP アドレスリソース • 物理ディスクリソース
jpc_windows_exporter_hyperv_service_論理ホスト名	• IP アドレスリソース • 物理ディスクリソース

8. 複数マネージャーホストへのデータ配信機能を使用している場合は、サービス起動の前に次の手順を実施する。

「7.3.7(2)(a) 複数マネージャーホストへのデータ配信機能を設定する (Windows の場合) (オプション)」の「バージョンアップ時の設定」を実施します。

9. JP1/IM - Agent のサービスを起動する。

クラスタソフトから論理ホストの JP1/IM - Agent のサービスを起動します。

物理ホストでも運用している場合は、物理ホストの JP1/IM - Agent のサービスを起動します。

7.6.3 バージョンアップインストール時の物理ホスト環境のセットアップ (Windows の場合)

物理ホストの JP1/IM - Manager を使う場合は、「[1.19.7 バージョンアップ時の設定 \(Windows の場合\)](#)」の手順に従ってセットアップを行ってください。

7.6.4 バージョンアップインストール時の論理ホスト環境 (実行系) のセットアップ (Windows の場合)

セントラルスコープの機能を使用する場合は、手順 5 から手順 7 が必要になります。セントラルスコープの機能を使用しない場合は、手順 5 から手順 7 を飛ばしてください。

1. JP1/IM - Manager を停止する。

物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止してください。

2. JP1/Base の論理ホスト環境をセットアップする。

JP1/Base をバージョンアップした場合には、マニュアル「JP1/Base 運用ガイド」のインストール・アンインストール時の注意事項の説明を参照し、セットアップをしてください。JP1/Base をバージョンアップしなかった場合にはセットアップの必要はありません。

3. 共有ディスクが使用可能なことを確認する。

4. jp1cohaverup コマンドを実行する。

jp1cohaverup -h 論理ホスト名

5. ディスクの空き容量を確認する。

JP1/IM - Manager をバージョンアップするには、共有フォルダ¥JP1Scope¥database¥下のディスク容量分の空き容量が、ハードディスクに必要です。

6. jp1cshaverup.bat コマンドを実行する。

jp1cshaverup.bat -h 論理ホスト名 -w 作業フォルダ

7. jbssetcnf コマンドを実行する。

次に示す機能の有効、無効は旧バージョンの JP1/IM - Manager またはセントラルスコープの設定に依存します。

- 状態変更イベントの上限監視
- 対処済み連動機能
- 状態変更イベントの自動削除
- 監視オブジェクトの初期化
- 状態変更条件メモリー常駐機能

機能の有効、無効を設定したい場合、次の表に示すファイルを引数にjbssetcnf コマンドを実行してください。

表 7-12 機能の有効、無効を設定するためのファイル

ファイル名	説明
状態変更イベント件数の上限監視設定ファイル (evhist_warn_event_on.conf, evhist_warn_event_off.conf)	監視オブジェクトの状態変更イベント件数が上限値（100 件）を超えた際に、JP1 イベントを発行する機能を有効または無効にするためのファイルです。
対処済み連動設定ファイル (action_complete_on.conf, action_complete_off.conf)	対処済み連動機能を有効または無効にするためのファイルです。
状態変更イベント自動削除設定ファイル	JP1 イベントの対処状況を「対処済」にしたときに、状態変更イベントを自動で削除する機能を有効または無効にするためのファイルです。
監視オブジェクト初期化設定ファイル	特定の JP1 イベントを受信したときに、監視オブジェクトを自動で初期化する機能を有効または無効にするためのファイルです。
状態変更条件メモリー常駐機能の設定ファイル	状態変更条件メモリー常駐機能を有効または無効にするためのファイルです。

8. 共通定義情報を退避する。

jbsgetcnf -h 論理ホスト名 > 共通定義情報退避ファイル名

7.6.5 バージョンアップインストール時の共通定義情報のコピー（Windows の場合）

1. JP1/IM - Manager を停止する。

物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止してください。

2. 実行系で退避した共通定義情報退避ファイルを待機系にコピーする。

FTP など任意の方法でコピーしてください。

3. 共通定義情報を設定する。

jbssetcnf 共通定義情報退避ファイル名

7.7 論理ホストのアンインストール (Windows の場合)

JP1/IM - Manager および JP1/IM - Agent の論理ホストのアンインストールについて説明します。まず、論理ホストを削除する手順について説明します。次に、実行系サーバ、待機系サーバそれぞれのローカルディスク上の JP1/IM - Manager, JP1/Base, および JP1/IM - Agent のアンインストール手順について説明します。

7.7.1 論理ホストの削除 (Windows の場合)

論理ホストを削除するための手順を次に示します。実行系サーバおよび待機系サーバで削除を行ってください。

IM データベース（統合監視 DB および IM 構成管理 DB）を使用している場合は、論理ホストを削除する前、または削除したあとに IM データベースを削除する必要があります。

(1) IM データベースの削除

IM データベース（統合監視 DB および IM 構成管理 DB）を使用している場合の手順です。

環境を再構築するために IM データベースを削除する場合は、事前にバックアップを取得してください。バックアップの方法については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「1.2 データベースの管理」を参照してください。

1. サービスを起動、停止する。

物理ホスト環境、論理ホスト環境の JP1/IM - Manager が起動している場合はすべての JP1/IM - Manager のサービス（JP1/IM3-Manager および JP1/IM3-Manager_論理ホスト名）を停止してください。論理ホスト環境の場合はクラスタソフトの操作で停止してください。

接続中の JP1/IM - View はログアウトして切断してください。

JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスも停止してください。

2. 論理ホストの IM データベースのサービスの状態を変更する。

次のとおり変更してください。

- 論理ホストの JP1/IM - Manager DB Cluster Service サービス（JP1/IM3-Manager DB Cluster Service_論理ホスト名）
停止にしてください。
- 論理ホストの IM データベースサービス（JP1/IM3-Manager DB Server_論理ホスト名）
開始にしてください。

3. jcodbunsetup コマンドを実行し、統合監視 DB を削除する。

jcodbunsetup -h 論理ホスト名 -c {online|standby} [-q]

引数により、論理ホスト名、アンセットアップ種別を指定します。

- 論理ホスト名 (-h オプション)

実行系サーバでセットアップした論理ホスト名を指定します。

- アンセットアップ種別 (-c オプション)

実行系ホストでの統合監視 DB を削除する場合は「online」、待機系ホストでの統合監視 DB を削除する場合は「standby」を指定します。

jcodbunsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcodbunsetup」(1. コマンド)を参照してください。

4. jcfdbunsetup コマンドを実行し、IM 構成管理 DB を削除する。

jcfdbunsetup -h 論理ホスト名 -c {online|standby} [-q]

引数により、論理ホスト名、アンセットアップ種別を指定します。

- 論理ホスト名 (-h オプション)

実行系サーバでセットアップした論理ホスト名を指定します。

- アンセットアップ種別 (-c オプション)

実行系ホストでの IM 構成管理 DB を削除する場合は「online」、待機系ホストでの IM 構成管理 DB を削除する場合は「standby」を指定します。

jcfdbunsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcfdbunsetup」(1. コマンド)を参照してください。

5. 次のファイルおよびフォルダを削除する。

共有フォルダ¥data¥imcf¥imconfig 以下のファイル

共有フォルダ¥data¥imcf¥profiles 以下のファイルおよびフォルダ

(2) インテリジェント統合管理データベースの削除

インテリジェント統合管理データベースを使用している場合、jimgnadbunsetup コマンドを実行して、論理ホストのインテリジェント統合管理データベース（トレンドデータ管理 DB）を削除します。

jimgnadbunsetup コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimgnadbunsetup」(1. コマンド)を参照してください。

また、論理ホスト全体の削除については、「[7.7.1\(3\) 論理ホストの削除](#)」を参照してください。

なお、クラスタソフトを利用して、インテリジェント統合管理データベースだけを削除する場合は、インテリジェント統合管理データベースが停止してもフェールオーバーが発生しないように、クラスタソフトの設定を見直してください。

(3) 論理ホストの削除

Windows で論理ホストを削除する場合は、JP1/Base の `jp1bshasetup.exe` コマンドを使用します。

1. `jp1bshasetup.exe` コマンドを実行する。
2. [Base クラスタ構成の設定] 画面の [論理ホストの削除] ボタンをクリックする。
3. 削除したい論理ホスト名を選択する。
4. [次へ] ボタンをクリックする。
5. 削除内容を確認し、[完了] ボタンをクリックする。

これによって、論理ホストが削除されます。なお、論理ホストを削除すると、JP1/Base, JP1/IM - Manager, JP1/AJS, JP1/Power Monitor (06-02 以降) が一括して削除されます。

共有ディスク上の共有ファイル、共有フォルダは削除されません。手作業で削除してください。

(4) 論理ホストから JP1/IM - Manager および IM データベースだけを削除する手順

JP1/Base, JP1/IM - Manager, JP1/AJS, JP1/Power Monitor (06-02 以降) をインストールしている論理ホストから JP1/IM - Manager および IM データベースだけを削除する手順を次に示します。

1. 停止前に、接続中の JP1/IM - View はログアウトして切断する。
2. JP1/IM - Manager, JP1/Base を順にクラスタソフトの操作で停止する。
3. IM データベースを使用している場合は、[\[7.7.1\(1\) IM データベースの削除\]](#) の手順で IM データベースを削除する。
4. 実行系/待機系のマシンで次のコマンドを実行して共通定義を削除する。
 - [論理ホスト名¥JP1CONSOLEMANAGER¥] キー
`jbsunsetcnf -h 論理ホスト名 -c JP1CONSOLEMANAGER`
 - [論理ホスト名¥JP1SCOPE¥] キー
`jbsunsetcnf -h 論理ホスト名 -c JP1SCOPE`
 - [論理ホスト名¥JP1CONFIG¥] キー
`jbsunsetcnf -h 論理ホスト名 -c JP1CONFIG`
5. JP1/IM - Manager の共有ファイル、共有フォルダを削除する。
6. クラスタソフトから、論理ホストの JP1/IM - Manager の設定を削除する。
7. 実行系/待機系のマシンで次のコマンドを実行して論理ホストの JP1/IM - Manager のサービスを削除する。

7.7.2 JP1/IM - Manager および JP1/Base のアンインストール (Windows の場合)

実行系サーバ、待機系サーバそれぞれのローカルディスク上の JP1/IM - Manager および JP1/Base をアンインストールしてください。

なお、JP1/IM - Manager をアンインストールすると、JP1/IM - Agent を利用するための統合エージェント管理基盤もアンインストールされます。

1. JP1/IM - Manager をアンインストールする。
2. JP1/Base をアンインストールする。

7.7.3 JP1/IM - Agent のアンインストール (Windows の場合)

実行系サーバ、待機系サーバそれぞれのローカルディスク上の JP1/IM - Agent をアンインストールしてください。

1. 論理ホストで稼働している JP1/IM - Agent のサービスを停止する。
クラスタソフトから論理ホストで稼働しているサービスを停止します。
2. 複数マネージャホストへのデータ配信機能を使用している場合は、サービス停止後に次の手順を実施する。
「7.3.7(2)(b) 複数マネージャホストへのデータ配信機能を解除する (Windows の場合) (オプション)」に記載している「論理ホストのアンインストールを行う場合」を実施します。
3. クラスタソフトに登録されたサービスを解除する。
サービスを解除する方法については、クラスタソフトのドキュメントを確認してください。
4. Windows に登録されたサービスを解除する。
論理ホストで使用するサービスについて、稼働系と待機系の両方で論理ホスト用のサービスを Windows から解除します。
論理ホストのサービスの解除には、次のコマンドを使用します。

Agentパス¥tools¥jpc_service -off **サービスキー** -h **論理ホスト名**

Alertmanager のサービスを登録する場合の例を次に示します。

Agentパス¥tools¥jpc_service -off jpc_alertmanager -h **論理ホスト名**
5. 論理ホスト用のサービス定義ファイルを削除する。

Agent パス¥bin 下にある論理ホスト用のサービス定義ファイルを削除します。

削除するファイル名：jpc_サービス名_service_論理ホスト名.xml

Alertmanager の場合の例を次に示します。

削除するファイル名
jpc_alertmanager_service_論理ホスト名.xml

6. 論理ホスト用の Windows サービス化プログラムを削除する。

Agent パス¥bin 下にある論理ホスト用の Windows サービス化プログラムを削除します。

削除するファイル名：jpc_サービス名_service_論理ホスト名.exe

Alertmanager の場合の例を次に示します。

削除するファイル名
jpc_alertmanager_service_論理ホスト名.exe

7. 共有フォルダを削除する。

7.8 設定変更時の作業 (Windows の場合)

クラスタシステムでの運用開始後に実行系サーバの設定を変更した場合には、その内容を待機系サーバにも反映して同期をとる必要があります。同期をとらないと、フェールオーバーしたときに実行系サーバの動作と待機系サーバの動作が変わってしまうことがあります。

次に示す場合には、実行系サーバおよび待機系サーバの両サーバでの設定変更をしてください。

7.8.1 ファイルでの設定変更 (Windows の場合)

次のファイルを編集し、`jbssetcnf` コマンドで設定を有効にした場合には、実行系サーバから待機系サーバに共通定義情報をコピーする必要があります。

- 自動アクション環境定義ファイル (`action.conf.update`)
- 通信環境定義ファイル (`console.conf.update`)
- 状態変更イベント件数の上限監視設定ファイル (`evhist_warn_event_XXX.conf`)
- 対処済み連動設定ファイル (`action_complete_XXX.conf`)
- 状態変更イベント自動削除設定ファイル
- 監視オブジェクト初期化設定ファイル
- 監視オブジェクト DB の自動バックアップ・リカバリー設定ファイル (`auto_dbbackup_XXX.conf`)
- 相関イベント発行環境定義ファイル
- 状態変更条件メモリ常駐機能の設定ファイル
- IM 構成反映方式設定ファイル (`jp1cf_applyconfig.conf`)
- リモートログトラップ環境定義ファイル (`jp1cf_remote_logtrap.conf`)
- 表示メッセージ変更後イベント環境定義ファイル (`chmsgevent.conf`)
- イベントレポート出力環境定義ファイル (`evtreport.conf`)
- 操作ログ定義ファイル (`imm_operationlog.conf`)
- プロファイル管理環境定義ファイル (`jp1cf_profile_manager.conf`)

セットアップ手順の「[7.3.4 JP1/IM - Manager の新規インストール時の共通定義情報のコピー \(Windows の場合\)](#)」で説明した手順で、共通定義情報をコピーするようにしてください。

なお、共通定義情報には JP1/Base, JP1/IM - Manager, JP1/AJS, および JP1/Power Monitor (06-02 以降) の設定情報が格納されています。論理ホストにこれらの製品がセットアップされている場合は、設定情報が一緒にコピーされます。

7.8.2 コマンドでの設定変更 (Windows の場合)

jcochafmode コマンド、jcochcefmode コマンド、およびjcocmddef コマンドを実行して、設定を変更した場合には、実行系サーバおよび待機系サーバの両サーバで同様の設定をする必要があります。

- jcochafmode コマンドを実行した場合
-h オプションを指定して、イベント取得フィルターの位置を変更した場合には、実行系サーバから待機系サーバに共通定義情報をコピーする必要があります。
セットアップ手順の「[7.3.4 JP1/IM - Manager の新規インストール時の共通定義情報のコピー \(Windows の場合\)](#)」で説明した手順で、共通定義情報をコピーするようにしてください。
- jcochcefmode コマンドを実行した場合
-h オプションを指定して、共通除外条件の動作モードを変更した場合には、実行系サーバから待機系サーバに共通定義情報をコピーする必要があります。
セットアップ手順の「[7.3.4 JP1/IM - Manager の新規インストール時の共通定義情報のコピー \(Windows の場合\)](#)」で説明した手順で、共通定義情報をコピーするようにしてください。
- jcocmddef コマンドを実行した場合
-host オプションを指定して、実行系サーバの設定を変更した場合には、待機系サーバでも同様の設定をしてください。なお、jcocmddef コマンドは共有ディスクがマウントされていなくても実行できます。

7.8.3 クラスタ環境での IM データベースの更新 (Windows の場合)

クラスタ環境で JP1/IM - Manager をバージョンアップまたは JP1/IM - Manager の修正版を適用した場合に IM データベースを使用しているときは、クラスタ環境の IM データベースの更新処理が必要になります。次に示す手順に従い、IM データベースを更新してください。

ここでは、論理ホストの JP1/IM - Manager が動作しているホストを実行系ホストとし、動作していないホストを待機系ホストとします。

1. サービスの状態を確認する。

次の状態と異なる場合は、サービスを停止してください。

- JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスが停止している。
- JP1/OA で JP1/IM - Manager から JP1 イベントを取得している場合は、接続元の JP1/OA が停止している。

2. 実行系ホストで、クラスタソフトの操作で次のサービスをオフラインにし、次の順でサービスを停止する。

- 論理ホストの JP1/IM - Manager サービス (サービス表示名: JP1/IM3-Manager_論理ホスト名)
- 論理ホストの JP1/IM - Manager DB Cluster Service サービス (サービス表示名: JP1/IM3-Manager DB Cluster Service_論理ホスト名)

- 論理ホストの IM データベースサービス（サービス表示名：JP1/IM3-Manager DB Server_論理ホスト名）
3. 実行系ホストに割り当てられた共有ディスクおよび論理 IP アドレスを待機系ホストに引き継ぎ、論理ホストで共有ディスクおよび論理 IP アドレスを使用できる状態にする。
4. 待機系ホストで OS のサービス画面から、次の順で次のサービスを起動する。
- 論理ホストの IM データベースサービス（サービス表示名：JP1/IM3-Manager DB Server_論理ホスト名）
 - 論理ホストの JP1/IM - Manager DB Cluster Service サービス（サービス表示名：JP1/IM3-Manager DB Cluster Service_論理ホスト名）
5. 待機系ホストでjimdbstatus コマンドを実行し、IM データベースサービスが稼働中であることを確認する。
- IM データベースサービスが稼働中の場合、KNAN11182-I メッセージが出力されます。
KNAN11182-I IM データベースサービスは稼働中です
 - IM データベースサービスが稼働中でない場合は、10 秒ごと程度でjimdbstatus コマンドを実行し、稼働中になるまで待ちます。
jimdbstatus -h 論理ホスト名
6. 待機系ホストでjimdbstop コマンドを実行し、IM データベースを停止する。
jimdbstop -h 論理ホスト名
7. 待機系ホストで OS のサービス画面から、次のサービスを停止する。
論理ホストの JP1/IM - Manager DB Cluster Service サービス（サービス表示名：JP1/IM3-Manager DB Cluster Service_論理ホスト名）
8. 待機系ホストに割り当てられた共有ディスクおよび論理 IP アドレスを実行系ホストに引き継ぎ、論理ホストで共有ディスクおよび論理 IP アドレスを使用できる状態にする。
9. 待機系ホストでjimdbupdate コマンドを実行する。
jimdbupdate -h 論理ホスト名
- 次のメッセージが出力された場合は、手順 11 以降を実行してください。
KNAN11201-I IM データベースサービスは最新の状態です
 - 次のどれかのメッセージが出力された場合は、手順 10 以降の手順を実行してください。
KNAN11202-I IM データベースサービスの上書きインストールが必要です
KNAN11211-I IM データベースサービスの設定ファイルの更新が必要です
- なお、待機系ホストでは次のメッセージが出力されますが、問題はありません。
KNAN11210-W 共有ディスクにアクセスできないため、テーブルスキーマを確認できませんでした
10. 待機系ホストでjimdbupdate コマンドを実行し、IM データベースを更新する。

jimdbupdate -h 論理ホスト名 -i

なお、待機系ホストでは次のメッセージが出力されますが、問題はありません。

KNAN11210-W 共有ディスクにアクセスできないため、テーブルスキーマを確認できませんでした

11. 待機系ホストで OS のサービス画面から、次のサービスを停止する。

論理ホストの IM データベースサービス (サービス表示名: JP1/IM3-Manager DB Server_論理ホスト名)

12. 実行系ホストで OS のサービス画面から、次のサービスを起動する。

論理ホストの IM データベースサービス (サービス表示名: JP1/IM3-Manager DB Server_論理ホスト名)

13. 実行系ホストで jimdbupdate コマンドを実行する。

jimdbupdate -h 論理ホスト名

- 次のメッセージが出力された場合は、手順 16 を実行してください。

KNAN11201-I IM データベースサービスは最新の状態で

- 次のどれかのメッセージが出力された場合は、手順 14 以降を実行してください。

KNAN11202-I IM データベースサービスの上書きインストールが必要です

KNAN11207-I IM データベースサービスのテーブルスキーマの更新が必要です

KNAN11211-I IM データベースサービスの設定ファイルの更新が必要です

14. 実行系ホストで jimdbbackup コマンドを実行し、IM データベースをバックアップする。

jimdbbackup -h 論理ホスト名 -o バックアップファイル名 -m MAINT

15. 実行系ホストで jimdbupdate コマンドを実行し、IM データベースを更新する。

jimdbupdate -h 論理ホスト名 -i

16. 実行系ホストで OS のサービス画面から、次のサービスを停止する。

論理ホストの IM データベースサービス (サービス表示名: JP1/IM3-Manager DB Server_論理ホスト名)

17. 実行系ホストでクラスタソフトの操作で次のサービスをオンラインにし、次の順でサービスを起動する。

- 論理ホストの IM データベースサービス (サービス表示名: JP1/IM3-Manager DB Server_論理ホスト名)
- 論理ホストの JP1/IM - Manager DB Cluster Service サービス (サービス表示名: JP1/IM3-Manager DB Cluster Service_論理ホスト名)
- 論理ホストの JP1/IM - Manager サービス (サービス表示名: JP1/IM3-Manager_論理ホスト名)

18. 手順 1 で停止したサービスを開始する。

❗ 重要

jimdbupdate コマンドを実行する前に取得した IM データベースの更新前のバックアップデータは、jimdbupdate コマンド実行後の IM データベースにリカバリーしないでください。

jimdbupdate コマンドを実行したあとは、再度jimdbbackup コマンドでバックアップを取得してください。

7.9 クラスタ運用時の注意事項 (Windows の場合)

- クラスタシステムで多重起動を行う場合、多重起動する論理ホストの数だけ、システムのリソースが必要となります。
- クラスタシステムで JP1/IM - Manager の設定を行う場合は、物理ホストで動作している JP1/IM - Manager を必ず停止してください。物理ホストの JP1/IM - Manager を停止しないまま、クラスタシステムの設定を行った場合、論理ホストのサービスが正常に動作しなくなります。サーバを再起動して、回復してください。
- クラスタシステムで起動する場合、論理ホストで使用する認証サーバを必ず設定してから JP1/IM - Manager を起動してください。認証サーバの設定方法については、マニュアル「JP1/Base 運用ガイド」を参照してください。また、JP1/IM - Manager を起動する際は、設定した認証サーバが起動していることを確認してから、JP1/IM - Manager を起動してください。
- 論理ホストの認証サーバの設定およびユーザー登録を行う場合、必ず実行系のホストで操作をしてください。また、ユーザー登録を行う場合は、必ず論理ホストのサービスを起動してから行ってください。
- ログイン中に系切り替えで認証サーバが切り替わった場合、JP1/IM - Manager では、通信障害が発生し、系切り替え後に回復します。

JP1/IM - Manager の動作に問題がある場合は、認証サーバをクラスタシステム以外の場所に設置しておくことで、回避できます。

- 実行系の定義を退避するときに `jbsgetcnf` コマンドに指定する論理ホスト名には、論理ホストを定義したときに指定した名称と、大文字・小文字が同じになるように指定してください。
誤って異なる指定を行った場合は、論理ホストを削除してから再度設定を行ってください。
- IM 構成管理を使用していない場合、クラスタシステムで構成定義情報を配布する場合は、構成定義ファイルを次の名称で作成してください。

共有フォルダ¥`jp1base¥conf¥route¥jbs_route.conf`

- JP1/IM - Manager の起動中に、クラスタソフトの機能などでホスト名を変更しないでください。
ホスト名を変更した場合は、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「2.2.4 クラスタシステムで論理ホスト名を変更する場合の作業」を参照し、必要な作業を行ってください。
- クラスタシステムで論理ホストを作成する場合、またはバインド方式を変える場合は、物理ホストで動作している「JP1/IM3-Manager」サービスを必ず停止してください。物理ホストのサービスを停止せずに、論理ホストの作成、またはバインド方式を変える設定を行った場合、論理ホストのサービスが正常に動作しなくなります。この場合、設定内容を確認した後、サーバマシンのリブートを行って回復してください。
- 物理ホストの JP1/Base を使用し、物理ホストの JP1/IM - Manager の起動をしないのであれば、JP1/Base の起動順序定義ファイル (Base パス¥`JP1Base¥conf¥boot¥JP1SVPRM.DAT`) から JP1/IM - Manager の定義を削除 (コメントアウト) してください。

- クラスタ運用の待機系ホストで"jbsrt_get -h 論理ホスト"を実行すると、共有ディレクトリがオフラインのため、「KAVB3113-I 定義情報が存在しませんでした」メッセージを出力します。この場合、実行系ホストで、"jbsrt_get -h 論理ホスト"を実行してください。
- クラスタソフトの対応状況および注意事項につきましては、以下のページをご参照ください。

<http://www.hitachi.co.jp/Prod/comp/soft1/jp1/products/environments/cluster/index.html>

7.10 非クラスタシステムでの論理ホストの運用と環境構築 (Windows の場合)

フェールオーバーしない論理ホストの構築および運用についての概要を説明します。

JP1/IM - Manager の操作、バックアップやリカバリーなど、フェールオーバーしない論理ホストの運用方法は、クラスタシステムで運用する論理ホストと同じです。ただし、クラスタソフトと連動してフェールオーバーすることを除きます。

7.10.1 非クラスタシステムで論理ホストを運用する場合の構成の検討 (Windows の場合)

複数の論理ホストで JP1/IM - Manager を起動すると、それぞれの JP1/IM - Manager がシステムリソース（メモリー・ディスク・プロセス・セマフォなど）を使用します。同時に起動する JP1/IM - Manager の数に合わせて、リソース量も見積もってください。

または、システムの性能に合わせて、同時に起動する JP1/IM - Manager の数を調整してください。複数の JP1/IM - Manager を同時に実行してリソースが不足すると、システムが正常に動作しません。同時に起動する論理ホストの数は 2～3 を目安にしてください。

なお、メモリー所要量およびディスク占有量の見積もりについては、JP1/IM - Manager のリリースノートを参照してください。

7.10.2 非クラスタシステムで論理ホストを運用する場合の環境設定 (Windows の場合)

フェールオーバーしない論理ホスト環境で、JP1/IM - Manager を運用する手順を次に示します。

(1) 論理ホスト環境の準備

論理ホスト環境を作成するために、論理ホスト用のディスク領域および IP アドレスを用意してください。

- 論理ホスト用のディスク領域

物理ホストやほかの論理ホストの JP1 が使用しているものとは別に、論理ホストの JP1/IM - Manager が専用で使用するファイルの格納先ディレクトリを、ローカルディスクに作成してください。

- 論理ホスト用の IP アドレス

論理ホストの JP1/IM - Manager が使用する IP アドレスを、OS で割り当ててください。

IP アドレスの割り当ては、実 IP でもエイリアス IP でもかまいません。ただし、論理ホスト名から一意に特定できる IP アドレスにしてください。

これらに対する前提条件は、クラスタシステムでの運用の場合と同じです。ただし、フェールオーバーしない運用方法のため「サーバ間で引き継がれる」などの条件は除きます。

なお、「7. クラスタシステムでの運用と環境構築 (Windows の場合)」で、共有ディスク・論理 IP アドレスと説明している部分は、上記で割り当てた論理ホスト用のディスク領域・IP アドレスに読み替えてください。

- 性能の見積もり

次のような観点でシステムとして動作できるか見積もってください。

- システム内で複数の JP1/IM - Manager が起動できるリソースを割り当てられるかどうかを見積もってください。リソースが十分に割り当てられないと、正しく動作しなかったり、十分な性能が確保できなかったりします。

(2) 論理ホスト環境の JP1 のセットアップ

クラスタシステムの実行系サーバと同じ手順で、論理ホスト環境の JP1 をセットアップしてください。なお、クラスタシステムではフェールオーバーする両側のサーバに対してセットアップする必要がありますが、フェールオーバーしない論理ホストでは、動作するサーバだけセットアップしてください。

(3) 論理ホスト環境の自動起動および自動停止の設定

論理ホスト環境の JP1 のセットアップ時に、自動起動および自動停止の設定はされません。論理ホスト環境の自動起動および自動停止をする場合は、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3.3 非クラスタシステムの論理ホスト運用での自動起動および自動停止の設定例」を参照してください。

7.10.3 非クラスタシステムで論理ホストを運用する場合の注意事項 (Windows の場合)

(1) 論理ホストの JP1 に対する操作

論理ホストに作成した JP1 に対してコマンドを実行する場合は、クラスタシステムで動作する論理ホストと同様に論理ホスト名を明示して実行してください。

(2) 論理ホストの引き継ぎ

非クラスタシステム環境の論理ホストでは共有ディスク上の管理情報が引き継がれないため、フェールオーバーに対応していません。複数のホストで論理ホスト IP を引き継ぐ運用はしないでください。

8

クラスタシステムでの運用と環境構築（UNIX の場合）

JP1/IM - Manager は、クラスタシステムでの運用に対応しています。JP1/IM - Manager をクラスタ運用することによって、サーバ障害などが発生しても実行系から待機系に処理を引き継ぎ、システム統合管理を継続できます。

この章では、UNIX の場合の JP1/IM - Manager のクラスタ運用およびセットアップ方法について説明します。セットアップ後に JP1/IM - Manager を起動する手順については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3. JP1/IM - Manager の起動と終了」を参照してください。

なお、この機能については、ご使用になるクラスタソフトに JP1/IM - Manager が対応していることをご確認の上、ご使用ください。

8.1 クラスタ運用の概要（UNIX の場合）

クラスタ運用の概要は、Windows の場合と同じです。詳細については、「7.1 クラスタ運用の概要（Windows の場合）」を参照してください。

8.1.1 クラスタシステムの概要（UNIX の場合）

クラスタシステムの概要は、Windows の場合と同じです。詳細については、「7.1.1 クラスタシステムの概要（Windows の場合）」を参照してください。

8.1.2 クラスタ運用の前提条件（UNIX の場合）

クラスタ運用の前提条件は、Windows の場合と同じです。詳細については、「7.1.2 クラスタ運用の前提条件（Windows の場合）」を参照してください。

8.1.3 クラスタシステムでの JP1/IM の構成（UNIX の場合）

クラスタシステムで JP1/IM - Manager を運用するには、クラスタソフトの制御により論理ホストの JP1/IM - Manager および JP1/Base を実行し、フェールオーバーに対応します。このときの JP1/IM の構成は次のようになります。

(1) クラスタ運用での JP1/IM の構成の概要

表 8-1 クラスタシステムでの JP1/IM の構成

製品名	クラスタシステムでの JP1/IM の構成
JP1/IM - View	- JP1/IM - View から JP1/IM - Manager に接続するときは、論理 IP アドレスあてに接続します。 - JP1/IM - View 自身は物理ホスト環境で動作します。
JP1/IM - Manager	- 論理ホスト環境で動作することができます。 - クラスタソフトに登録することで、フェールオーバーに対応します。 - クラスタソフトに登録するときは、前提リソースとして論理 IP アドレスと共有ディスクが必要です。 - 共有ディスクに定義情報を格納し、フェールオーバー時に引き継ぎます。 - 一つのサーバで複数の論理ホストを実行できます。このため、アクティブ・スタンバイ構成だけでなく、アクティブ・アクティブ構成のクラスタシステムでも運用できます。 - JP1/IM - Manager は前提製品 JP1/Base と同じ論理ホストで実行します。

(2) 共有ディスク上のファイル構成

論理ホスト環境の JP1/IM - Manager をセットアップすると、共有ディスク上に次のファイルが作成されます。これらは、論理ホストで JP1/IM - Manager を実行するために必要なファイルです。

表 8-2 共有ディスク上のファイル構成 (UNIX)

機能	共有ファイルの種別	ディレクトリ名
セントラルコンソール	定義ファイル	共有ディレクトリ/jp1cons/conf/
	ログファイル	共有ディレクトリ/jp1cons/log/
	一時ファイル	共有ディレクトリ/jp1cons/tmp/
	履歴ファイル※	共有ディレクトリ/jp1cons/operation/
セントラルスコープ	定義ファイル	共有ディレクトリ/jp1scope/conf/
	ログファイル	共有ディレクトリ/jp1scope/log/
	一時ファイル	共有ディレクトリ/jp1scope/tmp/
	データベース	共有ディレクトリ/jp1scope/database/
IM 構成管理	定義ファイル	共有ディレクトリ/jp1imm/conf/imcf/
	ログファイル	共有ディレクトリ/jp1imm/log/imcf/
	一時ファイル	共有ディレクトリ/jp1imm/tmp/
	IM 構成のデータおよびプロファイルのデータ	共有ディレクトリ/jp1imm/data/imcf/
IM データベース	データベース	共有ディスク上のユーザーが指定したディレクトリ/imdb
インテリジェント統合管理データベース	実行ファイル	マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.7.1(1)(d) 関連ファイルの格納先」の「■インテリジェント統合管理データベースの実行ファイルの格納先」を参照してください。
	ログファイル	マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.7.1(1)(d) 関連ファイルの格納先」の「■運用コマンドの個別ログの格納先」および「■トレンドデータ管理サービスのログの格納先」を参照してください。
	データファイル	マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.7.1(1)(d) 関連ファイルの格納先」の「■インテリジェント統合管理データベースのデータファイルの格納先」を参照してください。

注※ 相関イベント発行サービスの処理、共通除外条件による除外処理、および共通除外条件定義の更新処理が履歴として出力されます。

(3) JP1/IM - Manager のサービスおよびプロセス

クラスタ運用での JP1/IM - Manager は、論理ホストのサービスまたはプロセスを実行します。

論理ホストの JP1/IM - Manager を実行すると、論理ホストに対応したプロセスが動作します。

プロセス名は、引数に論理ホスト名が付加された名称になります。プロセス名については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 B プロセス一覧」を参照してください。

(4) 通信方式

論理ホストの JP1/IM - Manager をセットアップすると、JP1/IM - Manager の通信方式を IP バインド方式と呼ぶ方式に設定します。IP バインド方式に変更するのは、論理ホストと物理ホストの両方の環境が対象です。

通信方式には、IP バインド方式と ANY バインド方式の 2 種類があります。これは、通信するときに使用する IP アドレスを、内部処理で割り当て（バインド）をする方法をきめます。

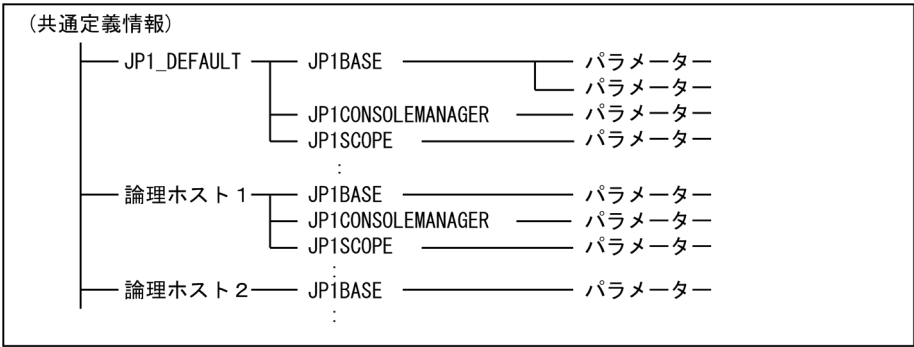
通信方式については、マニュアル「JP1/Base 運用ガイド」の JP1/Base の通信方式に関する説明を参照してください。JP1/IM - Manager は、JP1/Base と同じ通信方式で通信をします。

(5) 共通定義情報の設定

論理ホストの JP1/IM - Manager をセットアップすると、共通定義情報に、論理ホスト用の設定情報が設定されます。

共通定義情報とは、JP1 の設定情報を格納するデータベースで、JP1/Base が管理しています。設定情報のデータは、各サーバのローカルディスク上に、次のような形式で格納されています。

図 8-1 共通定義情報



共通定義情報は、物理ホスト（JP1_DEFAULT）および論理ホストごとに分かれて格納されています。物理ホストおよび論理ホスト単位に、jbssetcnf コマンドで設定し、jbsgetcnf コマンドで読み出します。

論理ホストの共通定義情報は、各サーバで同じ内容になるようにします。セットアップ時および設定変更時は、設定をした実行系サーバの共通定義情報を、待機系サーバへコピーして設定します。

なお、共通定義情報は、JP1/IM - Manager, JP1/Base, JP1/AJS, および JP1/Power Monitor (06-02 以降) が設定情報を格納するために使用しています。

8.2 クラスタ運用の環境設定の流れ（UNIX の場合）

クラスタ運用に対応するための JP1/IM - Manager および JP1/IM - Agent の環境設定について説明します。セットアップの作業の流れを示します。

なお、インテリジェント統合管理基盤のクラスタシステムの設定については「8.4 インテリジェント統合管理基盤のクラスタ環境を構築する（UNIX の場合）」を参照してください。

図 8-2 セットアップ作業の流れ（新規に環境設定する場合（JP1/IM - Manager））

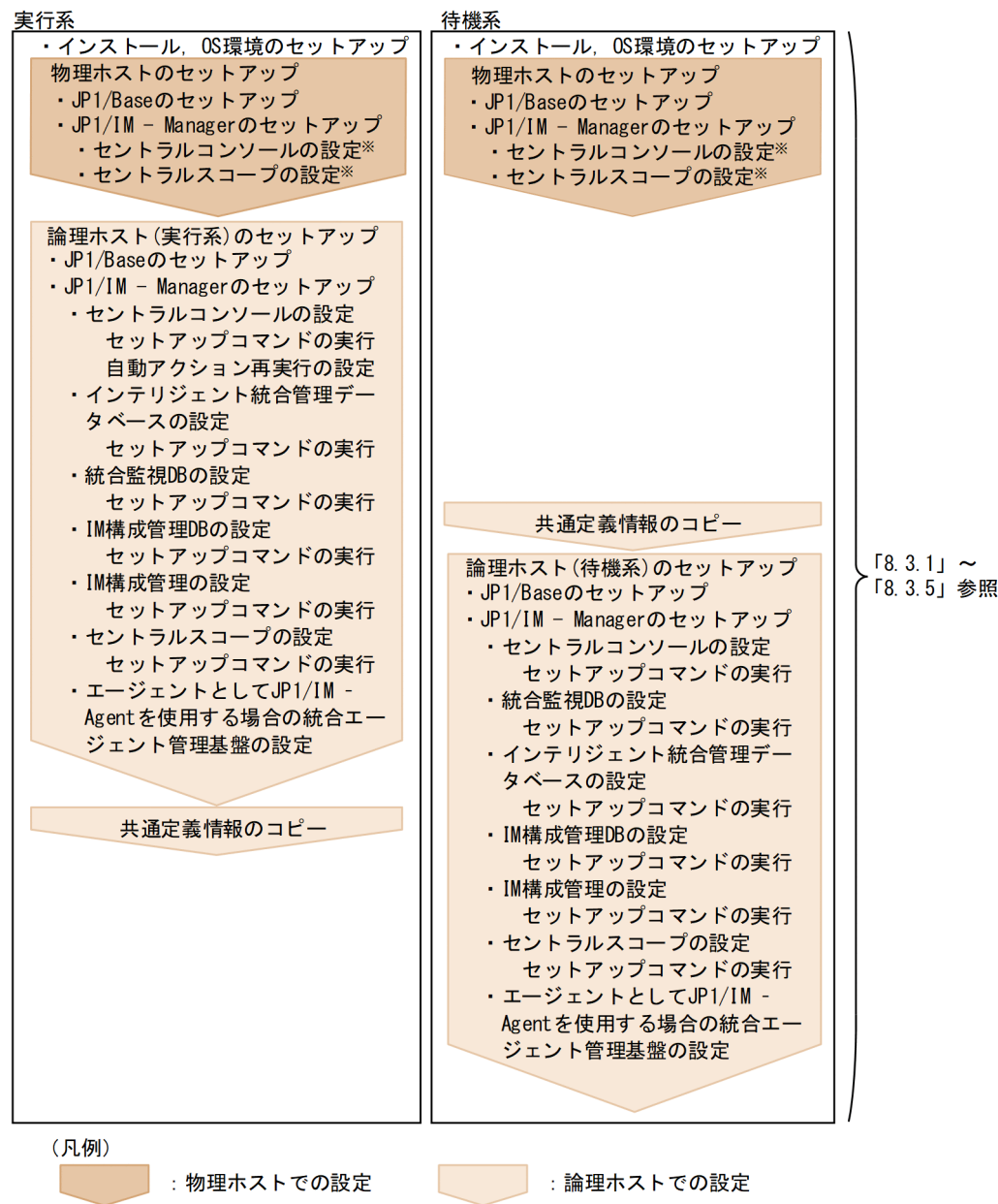


図 8-3 セットアップ作業の流れ（新規に環境設定する場合（JP1/IM - Agent））

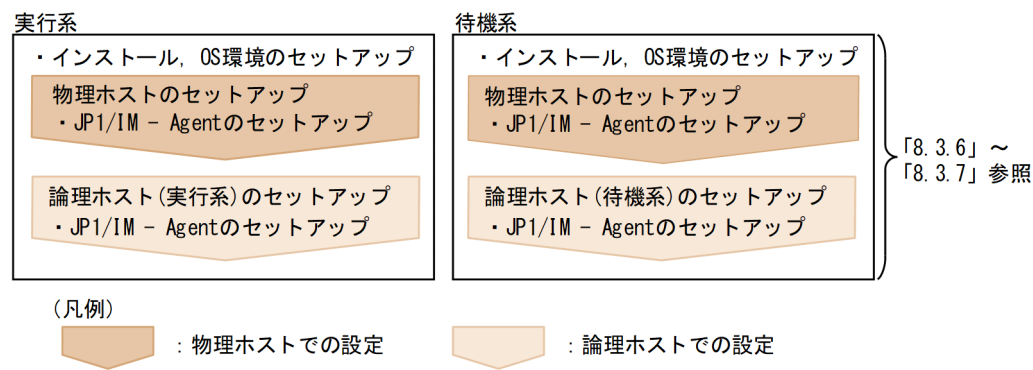
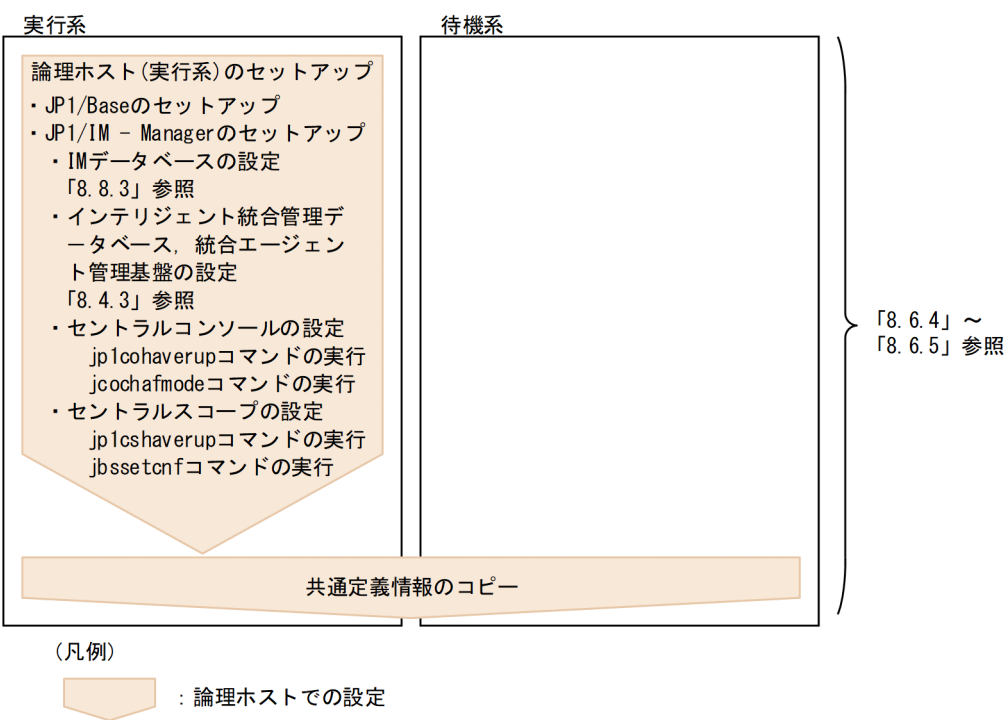


図 8-4 セットアップ作業の流れ（既存の論理ホスト環境をバージョンアップする場合（JP1/IM - Manager））



8.3 論理ホストの新規インストール・セットアップ (UNIX の場合)

JP1/IM - Manager および JP1/IM - Agent の論理ホストの新規インストールおよびセットアップについて説明します。なお、JP1/IM - Manager と同じ論理ホストに JP1/Base をセットアップする必要があるため、あわせて説明します。

作業を始める前に、クラスタシステムについて次の情報を確認してください。

表 8-3 論理ホストのインストール・セットアップ前の確認 (UNIX)

確認項目	説明
論理ホスト名	JP1 を実行する論理ホストのホスト名
論理 IP アドレス	論理ホスト名に対応する IP アドレス
共有ディレクトリ	論理ホストの JP1 の実行環境ファイル一式を格納する共有ディスク上のフォルダ

また、これらが「[7.1.2 クラスタ運用の前提条件 \(Windows の場合\)](#)」を満たしていることを確認してください。

確認ができれば、インストール・セットアップを始めます。

なお、論理ホスト名は、英大文字・英小文字を区別します。論理ホスト名には、JP1/Base で設定した論理ホスト名を英大文字・英小文字を含めて正確に指定してください。誤った論理ホスト名を指定し、論理ホストのインストール・セットアップを行ってしまった場合は、IM データベースと論理ホストを削除してから、再度、論理ホストのインストール・セットアップを行ってください。IM データベースと論理ホストの削除については、「[8.7.1 論理ホストの削除 \(UNIX の場合\)](#)」を参照してください。

8.3.1 JP1/Base および JP1/IM - Manager の新規インストール (UNIX の場合)

実行系サーバ、待機系サーバそれぞれのローカルディスク上に JP1/IM - Manager および JP1/Base をインストールしてください。

なお、JP1/IM - Manager をインストールすると、JP1/IM - Agent を利用するための統合エージェント管理基盤もインストールされます。

バージョンアップする場合は、インストールする前に設定情報とデータベースのバックアップをしてください。バックアップの方法は、過去のバージョンのマニュアルを参照してください。

1. JP1/Base をインストールする。
2. JP1/IM - Manager をインストールする。

なお、共有ディスク上には、インストールしないでください。

統合エージェント管理基盤と統合エージェント制御基盤で暗号化通信を行う場合は、統合エージェント管理基盤に関する次の手順を実施します。

1. サーバ証明書とサーバ証明書のキーファイルを配置する。

暗号通信（HTTPS）を有効にする場合は、クラスタ環境のサーバ証明書とキーファイル（秘密鍵ファイル）を共有ディレクトリに配置する。

8.3.2 JP1/IM - Manager の新規インストール時の物理ホスト環境のセットアップ（UNIX の場合）

実行系サーバ、待機系サーバそれぞれで、JP1/Base および JP1/IM - Manager をインストール後、JP1/Base および JP1/IM - Manager の物理ホスト環境のセットアップをしてください。

なお、JP1/IM - Manager をインストールすると、JP1/IM - Agent を利用するための統合エージェント管理基盤もインストールされます。

1. JP1/Base の物理ホスト環境をセットアップする。

2. JP1/IM - Manager の物理ホスト環境をセットアップする。

JP1/Base のセットアップ手順については、マニュアル「JP1/Base 運用ガイド」を参照してください。

JP1/IM - Manager のセットアップ手順は、クラスタ運用ではない場合と同じ手順です。手順については、「[2. インストールとセットアップ（UNIX の場合）](#)」を参照してください。なお、物理ホストの JP1/IM - Manager を使わない場合は、セットアップの必要はありません。

8.3.3 JP1/IM - Manager の新規インストール時の論理ホスト環境（実行系）のセットアップ（UNIX の場合）

(1) セットアップの前準備

1. JP1/IM と JP1/Base のサービスが停止していることを確認する。

物理ホストおよびすべての論理ホストの、JP1/IM と JP1/Base のプロセスが停止していることを確認してください。JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスも停止してください。

2. 共有ディスクが使用可能なことを確認する。

共有ディスクがマウントされていることをmount コマンドを実行して確認してください。

(2) JP1/Base のセットアップ

1. JP1/Base の論理ホスト（実行系）をセットアップする。

手順の詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

2. JP1/Base のコマンド実行環境を設定する。

jcocmddef コマンドを実行して、JP1/Base のコマンド実行環境を設定します。jcocmddef コマンドの詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

(3) JP1/IM - Manager（セントラルコンソール）の設定

1. JP1/IM - Manager（セントラルコンソール）の論理ホストのセットアップコマンドを実行する。

```
/opt/jp1cons/bin/jp1cc_setup_cluster -h 論理ホスト名 -d 共有ディレクトリ名
```

引数により、論理ホスト名と共有ディレクトリ名を指定します。

- 論理ホスト名（-h オプション）

JP1/Base で設定した論理ホスト名を指定します。

- 共有ディレクトリ名（-d オプション）

共有ディスク上のディレクトリを指定してください。

「指定したディレクトリ名/jp1cons/」ディレクトリが作成され、論理ホストの JP1/IM - Manager（セントラルコンソール）のファイル一式が作成されます。

なお、論理ホストの JP1/IM - Manager の環境設定は、物理ホストの設定値を引き継ぎます。必要に応じて、jcoimdef コマンド（-h オプション）で論理ホストの環境設定をカスタマイズしてください。コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jp1cc_setup_cluster（UNIX 限定）」（1. コマンド）および「jcoimdef」（1. コマンド）を参照してください。

続けて、フェールオーバー時に適切に動作するよう、論理ホストの JP1/IM - Manager の環境設定をカスタマイズします。

2. 自動アクションの再実行の設定をする。

次のコマンドを実行して、フェールオーバー時の自動アクション再実行について設定をします。コマンドに指定するシステム環境の設定情報は、物理ホストの定義情報を引き継ぎます。物理ホストのシステム環境の設定情報を確認し、必要に応じて論理ホストのシステム環境を設定してください。

```
/opt/jp1cons/bin/jcoimdef -r { EXE | OUTPUT | OFF } -h 論理ホスト名
```

フェールオーバー時に次の状態となっているアクションに対する動作を設定できます。

- 送信待機
- 送信待機（キャンセル中）
- 送信待機（キャンセル失敗）
- 送信中

- 送信中 (キャンセル中)
- 送信中 (キャンセル失敗)
- キューイング
- キューイング (キャンセル中)
- キューイング (キャンセル失敗)
- 実行中
- 実行中 (キャンセル中)
- 実行中 (キャンセル失敗)

EXE を指定するとアクションを再実行し、OUTPUT を指定するとアクションの一覧をファイルに出力し、OFF を指定すると処理を行いません。システム設計時の検討内容に従って設定してください。この設定は任意です。

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

(4) JP1/IM - Manager (統合監視 DB) の設定

JP1/IM - Manager (統合監視 DB) を使用する場合は、必要です。統合監視 DB を使用して JP1 イベントを管理するためには、統合監視 DB を構築する必要があります。

1. クラスタセットアップ情報ファイルを編集する。

統合監視 DB を構築するために必要なデータベース領域のサイズやデータベース格納ディレクトリの情報を記述したクラスタセットアップ情報ファイルを準備します。

クラスタセットアップ情報ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。

2. jcodbsetup コマンドを実行し、統合監視 DB を作成する。

```
jcodbsetup -f クラスタセットアップ情報ファイル名 -h 論理ホスト名 -c online [-q]
```

引数により、クラスタセットアップ情報ファイル名、論理ホスト名、セットアップ種別を指定します。

- クラスタセットアップ情報ファイル名 (-f オプション)

手順 1 で作成したクラスタセットアップ情報ファイル名を指定します。

- 論理ホスト名 (-h オプション)

実行系サーバでセットアップした論理ホスト名を指定します。

論理ホスト名には、JP1/Base で設定した論理ホスト名を、大文字・小文字を含めて正確に指定してください。JP1/Base のセットアップについては、「[8.3.3\(2\) JP1/Base のセットアップ](#)」を参照してください。

- セットアップ種別 (-c オプション)

実行系ホストのセットアップ種別 (online) を指定します。

「online」を指定する場合は、共有ディスクをマウントし、論理ホストと通信できる状態にしてください。

jcodbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcodbsetup」(1. コマンド)を参照してください。

3. jcoimdef コマンドを実行して、統合監視 DB を有効にする。

jcoimdef -db ON -h 論理ホスト名

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド)を参照してください。

以上で、実行系サーバでの論理ホストのセットアップは完了です。

共有ディスクに論理ホストの JP1/IM - Manager のファイルが作成されていることを確認し、必要に応じて共有ディスクをアンマウントしてください。

(5) JP1/IM - Manager (インテリジェント統合管理データベース) の設定

インテリジェント統合管理データベースを使用している場合の、インテリジェント統合管理データベース (トレンドデータ管理 DB) の論理ホスト環境の構築手順を、次に示します。

1. JP1/IM - Manager の論理ホスト環境を構築する。

インテリジェント統合管理データベースの論理ホスト環境の構築では、作成済みの JP1/IM - Manager の論理ホスト環境を参照する必要があるため、インテリジェント統合管理データベースの論理ホスト環境を構築する前に、JP1/IM - Manager (セントラルコンソール) の論理ホスト環境を構築します。また、統合オペレーション・ビューアーの前提機能であるインテリジェント統合管理基盤の構築、統合監視 DB の設定も行う必要があります。すでに構築済みの場合は、次の手順に進みます。

JP1/IM - Manager (セントラルコンソール) の論理ホスト環境の構築手順については、「[8.3.3\(3\) JP1/IM - Manager \(セントラルコンソール\) の設定](#)」を参照してください。また、インテリジェント統合管理基盤の構築については、「[4.4 インテリジェント統合管理基盤のクラスタ環境を構築する](#)」、統合監視 DB の設定については、「[8.3.3\(4\) JP1/IM - Manager \(統合監視 DB\) の設定](#)」を参照してください。

2. root 以外の OS ユーザーを作成する。

インテリジェント統合管理基盤データベース (PostgreSQL) を起動する root 以外の OS ユーザー (root 以外のログイン可能なユーザー) が必要です。

必要に応じて、OS の useradd コマンドでユーザーを作成してください。すでに作成済みの場合は、次の手順に進んでください。

ユーザー「imsrvuser」を作成する場合の useradd コマンドの実行例を次に示します。

```
useradd imsrvuser
```

すでに作成済みの場合は、次の手順に進みます。

3. クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイルを準備する。

クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイルに、データディレクトリ、ポート番号などの必要な定義を記述します。

マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイル (jimgnbdbclustersetupinfo.conf)」(2. 定義ファイル) を参照して、インテリジェント統合管理データベースセットアップ情報ファイルを編集してください。

4. jimgnbdbsetup コマンドを実行する。

次のコマンドを実行します。

```
jimgnbdbsetup -f クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイル  
-h 論理ホスト名 -c online
```

5. クラスタソフトから JP1/IM - Manager のサービスを起動する

クラスタソフトから次のサービスを起動します。

```
jp1_cons_論理ホスト名.service
```

(6) JP1/IM - Manager (IM 構成管理 DB) の設定 (任意)

JP1/IM - Manager (IM 構成管理 DB) を使用する場合に設定します。IM 構成管理 DB を使用してシステムの階層構成 (IM 構成) を管理するためには、IM 構成管理 DB を構築する必要があります。

1. クラスタセットアップ情報ファイルを編集する。

IM 構成管理 DB を構築するために必要なデータベース領域のサイズやデータベース格納ディレクトリの情報を記述したクラスタセットアップ情報ファイルを準備します。

クラスタセットアップ情報ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。

2. jcfdbsetup コマンドを実行して、IM 構成管理 DB を作成する。

```
jcfdbsetup -f クラスタセットアップ情報ファイル名 -h 論理ホスト名 -c online [-q]
```

引数により、クラスタセットアップ情報ファイル名、論理ホスト名、セットアップ種別を指定します。

- クラスタセットアップ情報ファイル名 (-f オプション)

手順 1 で作成したクラスタセットアップ情報ファイル名を指定します。

- 論理ホスト名 (-h オプション)

実行系サーバでセットアップした論理ホスト名を指定します。

論理ホスト名には、JP1/Base で設定した論理ホスト名を、大文字・小文字を含めて正確に指定してください。JP1/Base のセットアップについては、「[8.3.3\(2\) JP1/Base のセットアップ](#)」を参照してください。

- セットアップ種別 (-c オプション)

実行系ホストのセットアップ種別 (online) を指定します。

「online」を指定する場合は、共有ディスクをマウントし、論理ホストと通信できる状態にしてください。

jcfdbssetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcfdbssetup」(1. コマンド)を参照してください。

3. jcoimdef コマンドを実行して、IM 構成管理 DB を有効にする。

jcoimdef -cf ON -h 論理ホスト名

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド)を参照してください。

以上で、実行系サーバでの論理ホストのセットアップは完了です。

共有ディスクに論理ホストの JP1/IM - Manager のファイルが作成されていることを確認し、必要に応じて共有ディスクをアンマウントしてください。

(7) JP1/IM - Manager (IM 構成管理) の設定 (任意)

JP1/IM - Manager (IM 構成管理) を使用する場合に設定します。

1. JP1/IM - Manager (IM 構成管理) の論理ホストのセットアップコマンドを実行する。

/opt/jp1imm/bin/imcf/jp1cf_setup_cluster -h 論理ホスト名 -d 共有ディレクトリ名

引数により、論理ホスト名と共有ディレクトリ名を指定します。

- 論理ホスト名 (-h オプション)
JP1/Base で設定した論理ホスト名を指定します。
- 共有ディレクトリ名 (-d オプション)
共有ディスク上のディレクトリを指定してください。

jp1cf_setup_cluster を実行すると、次のディレクトリが作成されます。

- 共有ディレクトリ/jp1imm/conf/imcf
- 共有ディレクトリ/jp1imm/tmp
- 共有ディレクトリ/jp1imm/log/imcf
- 共有ディレクトリ/jp1imm/data/imcf

なお、コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jp1cf_setup_cluster (UNIX 限定)」(1. コマンド)を参照してください。

(8) JP1/IM - Manager (セントラルスコープ) の設定 (任意)

JP1/IM - Manager (セントラルスコープ) を使用する場合に設定します。

1. JP1/IM - Manager (セントラルスコープ) の論理ホストのセットアップコマンドを実行する。

`/opt/jp1scope/bin/jp1cs_setup_cluster -h 論理ホスト名 -d 共有ディレクトリ名`
引数により、論理ホスト名と共有ディレクトリ名を指定します。

- 論理ホスト名 (-h オプション)
JP1/Base で設定した論理ホスト名を指定します。
- 共有ディレクトリ名 (-d オプション)
共有ディスク上のディレクトリを指定してください。
「指定したディレクトリ名/jp1scope/」ディレクトリが作成され、論理ホストの JP1/IM - Manager (セントラルスコープ) のファイル一式が作成されます。

なお、コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jp1cs_setup_cluster (UNIX 限定)」(1. コマンド) を参照してください。

(9) エージェントとして JP1/IM - Agent を使用する場合の設定

(a) 統合エージェント管理基盤の設定変更

統合エージェント管理基盤 (imbase, imbaseproxy) の設定変更の手順を、次に示します。

■ 統合エージェント管理基盤のポートを変更する

次の手順を実施します。

1. 統合エージェント管理基盤を停止する。
2. 統合エージェント管理基盤のリッスンポート番号を変更する。

待ち受けポート番号の設定は、統合エージェント管理基盤の imbase 設定ファイル (jpc_imbase.json) と imbaseproxy 設定ファイル (jpc_imbaseproxy.json) の port メンバーに設定されています。これを新しいポート番号に変更します。

imbase 設定ファイルと imbaseproxy 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の該当するファイル (2. 定義ファイル) を参照してください。

3. 統合エージェント管理基盤を開始する。

■ 証明書を設定する

次の手順を実施します。

1. 統合エージェント管理基盤を停止する。
2. 統合エージェント管理基盤のサーバ証明書およびキーファイルを変更する。

リッスンポート番号は、imbase 設定ファイル (jpc_imbase.json) や imbaseproxy 設定ファイル (jpc_imbaseproxy.json) の cert_file や key_file のメンバーに設定されています。
cert_file や key_file の設定値、または、設定しているファイル自体を更新します。

imbase 設定ファイルと imbaseproxy 設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「2. 定義ファイル」の、該当するファイルの説明を参照してください。

3. 統合エージェント管理基盤を開始する。

8.3.4 JP1/IM - Manager の新規インストール時の共通定義情報のコピー (UNIX の場合)

実行系サーバの共通定義情報を、待機系サーバにコピーします。

共通定義情報には、論理ホストの JP1/IM - Manager および JP1/Base を実行するための設定情報が記録されています。次の手順でコピーしてください。

1. 実行系サーバで、共通定義情報を退避する。

実行系で `jbsgetcnf` コマンドを実行し、共通定義情報を退避します。

`/opt/jp1base/bin/jbsgetcnf -h 論理ホスト名 > 共通定義情報退避ファイル名`

なお、論理ホスト名は、大文字・小文字を区別します。論理ホスト名には、JP1/Base で設定した論理ホスト名を、大文字・小文字を含めて正確に指定してください。

2. 退避ファイルを、実行系サーバから待機系サーバにコピーする。

FTP など任意の方法でコピーしてください。

3. 待機系サーバで、共通定義情報を設定する。

待機系サーバに、実行系サーバからコピーした退避ファイルを使って、共通定義情報を設定します。

`/opt/jp1base/bin/jbssetcnf 共通定義情報退避ファイル名`

8.3.5 JP1/IM - Manager の新規インストール時の論理ホスト環境 (待機系) のセットアップ (UNIX の場合)

(1) セットアップの前準備

1. JP1/IM と JP1/Base のサービスが停止していることを確認する。

物理ホストおよびすべての論理ホストの、JP1/IM と JP1/Base のプロセスが停止していることを確認してください。JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスも停止してください。

2. 実行系サーバで IM データベースをセットアップした場合は、実行系サーバで使用したクラスタセットアップ情報ファイルを待機系サーバにコピーする (実行系サーバで IM データベースをセットアップしていない場合は不要)。

コピーしたファイルは、`/etc/opt/jp1imm/conf/imdb/setup/`に格納してください。

なお、待機系サーバでは、共有ディスクが使用可能である必要はありません。

(2) JP1/Base のセットアップ

1. JP1/Base の論理ホスト（待機系）をセットアップする。

手順の詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

2. JP1/Base のコマンド実行環境を設定する。

`jcocmddef` コマンドを実行して、JP1/Base のコマンド実行環境を設定します。`jcocmddef` コマンドの詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

(3) JP1/IM - Manager（セントラルコンソール）の設定

1. JP1/IM - Manager（セントラルコンソール）の論理ホストのセットアップコマンドを実行する。

`/opt/jp1cons/bin/jp1cc_setup_cluster -h 論理ホスト名`

引数により、論理ホスト名を指定します。

- 論理ホスト名（`-h` オプション）

実行系サーバでセットアップした論理ホスト名を指定します。

なお、コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jp1cc_setup_cluster`（UNIX 限定）」（1. コマンド）を参照してください。

(4) JP1/IM - Manager（統合監視 DB）の設定

JP1/IM - Manager（統合監視 DB）を使用する場合は、必要です。統合監視 DB を使用して JP1 イベントを管理するためには、統合監視 DB を構築する必要があります。

1. クラスタセットアップ情報ファイルを編集する。

統合監視 DB を構築するために必要なデータベース領域のサイズやデータベース格納ディレクトリの情報を記述したクラスタセットアップ情報ファイルを準備します。「8.3.5(1) セットアップの前準備」で実行系のホストからコピーしたクラスタセットアップ情報ファイルの内容を確認してください。クラスタセットアップ情報ファイルは、実行系で指定した設定内容と同一である必要があります。

クラスタセットアップ情報ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル（`jimdbclustersetupinfo.conf`）」（2. 定義ファイル）を参照してください。

2. `jcodbsetup` コマンドを実行し、統合監視 DB を作成する。

`jcodbsetup -f クラスタセットアップ情報ファイル名 -h 論理ホスト名 -c standby [-q]`

引数により、クラスタセットアップ情報ファイル名、論理ホスト名、セットアップ種別を指定します。

- クラスタセットアップ情報ファイル名（`-f` オプション）

手順 1 で作成したクラスタセットアップ情報ファイル名を指定します。

- 論理ホスト名 (-h オプション)

実行系サーバでセットアップした論理ホスト名を指定します。

- セットアップ種別 (-c オプション)

待機系ホストのセットアップ種別 (standby) を指定します。

jcodbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcodbsetup」(1. コマンド) を参照してください。

(5) JP1/IM - Manager (インテリジェント統合管理データベース) の設定

インテリジェント統合管理データベースを使用している場合の、インテリジェント統合管理データベース (トレンドデータ管理 DB) の論理ホスト環境の構築手順を、次に示します。

1. JP1/IM - Manager の論理ホスト環境を構築する。

インテリジェント統合管理データベースの論理ホスト環境の構築では、作成済みの JP1/IM - Manager の論理ホスト環境を参照する必要があるため、インテリジェント統合管理データベースの論理ホスト環境を構築する前に、JP1/IM - Manager (セントラルコンソール) の論理ホスト環境を構築します。また、統合オペレーション・ビューアーの前提機能であるインテリジェント統合管理基盤の構築、統合監視 DB の設定も行う必要があります。すでに構築済みの場合は、次の手順に進みます。

JP1/IM - Manager (セントラルコンソール) の論理ホスト環境の構築手順については、「[8.3.3\(3\) JP1/IM - Manager \(セントラルコンソール\) の設定](#)」を参照してください。また、インテリジェント統合管理基盤の構築については、「[4.4 インテリジェント統合管理基盤のクラスタ環境を構築する](#)」、統合監視 DB の設定については、「[8.3.3\(4\) JP1/IM - Manager \(統合監視 DB\) の設定](#)」を参照してください。

2. root 以外の OS ユーザーを作成する。

インテリジェント統合管理基盤データベース (PostgreSQL) を起動する root 以外の OS ユーザー (root 以外のログイン可能なユーザー) が必要です。

必要に応じて、OS の useradd コマンドでユーザーを作成してください。すでに作成済みの場合は、次の手順に進んでください。

ユーザー「imsrvuser」を作成する場合の useradd コマンドの実行例を次に示します。

```
useradd imsrvuser
```

すでに作成済みの場合は、次の手順に進みます。

3. クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイルを準備する。

クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイルに、データディレクトリ、ポート番号などの必要な定義を記述します。

マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイル

(jimgnbdbclustersetupinfo.conf)」(2. 定義ファイル)を参照して、インテリジェント統合管理データベースセットアップ情報ファイルを編集してください。

4. jimgnbdbsetup コマンドを実行する。

次のコマンドを実行します。

```
jimgnbdbsetup -f クラスタ環境インテリジェント統合管理データベースセットアップ情報ファイル  
-h 論理ホスト名 -c standby
```

5. クラスタソフトから JP1/IM - Manager のサービスを起動する

クラスタソフトから次のサービスを起動します。

```
jp1_cons_論理ホスト名.service
```

(6) JP1/IM - Manager (IM 構成管理 DB) の設定 (任意)

JP1/IM - Manager (IM 構成管理 DB) を使用する場合に設定します。IM 構成管理 DB を使用してシステムの階層構成 (IM 構成) を管理するためには、IM データベースを構築する必要があります。

1. クラスタセットアップ情報ファイルを編集する。

IM 構成管理 DB を構築するために必要なデータベース領域のサイズやデータベース格納ディレクトリの情報を記述したクラスタセットアップ情報ファイルを準備します。「[8.3.5\(1\) セットアップの前準備](#)」で実行系のホストからコピーしたクラスタセットアップ情報ファイルの内容を確認してください。クラスタセットアップ情報ファイルは、実行系で指定した設定内容と同一である必要があります。

クラスタセットアップ情報ファイルの設定内容については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル)を参照してください。

2. jcfdbsetup コマンドを実行して、IM 構成管理 DB を作成する。

```
jcfdbsetup -f クラスタセットアップ情報ファイル名 -h 論理ホスト名 -c standby [-q]
```

引数により、クラスタセットアップ情報ファイル名、論理ホスト名、セットアップ種別を指定します。

- クラスタセットアップ情報ファイル名 (-f オプション)
手順 1 で作成したクラスタセットアップ情報ファイル名を指定します。
- 論理ホスト名 (-h オプション)
実行系サーバでセットアップした論理ホスト名を指定します。
- セットアップ種別 (-c オプション)
待機系ホストのセットアップ種別 (standby) を指定します。

jcfdbsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcfdbsetup」(1. コマンド)を参照してください。

(7) JP1/IM - Manager (IM 構成管理) の設定 (任意)

JP1/IM - Manager (IM 構成管理) を使用する場合に設定します。

1. JP1/IM - Manager (IM 構成管理) の論理ホストのセットアップコマンドを実行する。

```
/opt/jp1imm/bin/imcf/jp1cf_setup_cluster -h 論理ホスト名
```

引数により、論理ホスト名を指定します。

- 論理ホスト名 (-h オプション)

JP1/Base で設定した論理ホスト名を指定します。

なお、コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jp1cf_setup_cluster (UNIX 限定)」(1. コマンド) を参照してください。

(8) JP1/IM - Manager (セントラルスコープ) の設定 (任意)

JP1/IM - Manager (セントラルスコープ) を使用する場合に設定します。

1. JP1/IM - Manager (セントラルスコープ) の論理ホストのセットアップコマンドを実行する。

```
/opt/jp1scope/bin/jp1cs_setup_cluster -h 論理ホスト名
```

引数により、論理ホスト名を指定します。

- 論理ホスト名 (-h オプション)

実行系サーバでセットアップした論理ホスト名を指定します。

なお、コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jp1cs_setup_cluster (UNIX 限定)」(1. コマンド) を参照してください。

(9) エージェントとして JP1/IM - Agent を使用する場合の設定

実行系サーバで実施する手順と同じです。手順については、「[8.3.3\(9\)エージェントとして JP1/IM - Agent を使用する場合の設定](#)」を参照してください。

8.3.6 統合エージェントホストでの JP1/IM - Agent の新規インストール (UNIX の場合)

実行系サーバ、待機系サーバそれぞれのローカルディスク上に JP1/IM - Agent をインストールしてください。

1. JP1/IM - Agent を新規インストールする。

インストール方法については、「[2.3.1\(2\)JP1/IM - Agent のインストールの手順](#)」参照してください。

インストール時のインストールモードは「通常インストールモード」を選択します。

実行系サーバと待機系サーバの両方で実施します。

物理ホストの JP1/IM - Agent のサービスは起動しないでください。起動している場合はすべて停止してください。

2. 論理ホスト用の新規セットアップコマンドの設定ファイルを作成する。

設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「論理ホスト新規セットアップの設定ファイル（任意のファイル名）」（2. 定義ファイル）を参照してください。

また、設定ファイルのサンプルファイルが、次のパスに格納されています。コピーして作成できます。

JP1/IM - Agent のインストール先ディレクトリ/jp1ima/conf/sample/jpc_lhsetup.properties

3. 論理ホスト用の新規セットアップコマンドを実行する。

```
jimalhsetup -h 論理ホスト名 -d 共有ディレクトリ -c {online|standby} -f セットアップ設定ファイル [-q]
```

論理ホスト用の新規セットアップコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimalhsetup」（1. コマンド）を参照してください。

実行系サーバと待機系サーバの両方で実施します。

4. systemd にサービスが登録されたことを確認する。

実行系サーバと待機系サーバの両方で、systemd のサービス一覧を表示して、論理ホスト用のサービスが登録されたことを確認します。

論理ホスト用のサービスの名称は、ユニット定義ファイルのファイル名となります。

5. TLS の設定を行う。

TLS を有効にして運用する場合は、共有ディレクトリ/jp1ima/conf/user/cert に CA 証明書ファイルを配置してください。

また、共有ディレクトリ/jp1ima/conf/jpc_imagentcommon.json のimmgr.tls_config.ca_file に CA 証明書のフルパスを記入してください。

6. 必要な設定を行う。

「[8.3.7 統合エージェントホストでの JP1/IM - Agent の新規インストール時のセットアップ（UNIX の場合）](#)」, 「[2.19.2 JP1/IM - Agent の設定](#)」を参照して必要な設定変更を行います。

7. クラスタソフトに論理ホスト用のサービスを登録する。

JP1/IM - Agent のサービスのクラスタソフトへの登録については、「[8.5 新規インストール・セットアップでのクラスタソフトへの登録（UNIX の場合）](#)」を参照してください。

8. クラスタの設定で JP1/IM - Agent のサービスが停止したと判定する期間を 1 分に設定する。

統合オペレーション・ビューアーに定義ファイルをアップロードすると、定義ファイルを配置した後にサービスの再起動が行われることがあります。

また、アップロードした定義ファイルの内容が不正でサービスの起動に失敗した場合、定義ファイルを元に戻してサービスを起動します。

上記のように、一時的にサービスが停止することがあるため、クラスタが一時的なサービス停止を検知しないように設定する必要があります。

9. 複数マネージャーホストへのデータ配信機能を使用する場合は、動作確認の前に次の手順を実施する。
「8.3.7(2)(a) 複数マネージャーホストへのデータ配信機能を設定する (Linux の場合) (オプション)」
の「新規設定」を実施します。

10. 動作に問題がないか確認する。

- クラスタソフトからサービスを起動します。
- フェールオーバーさせます。

8.3.7 統合エージェントホストでの JP1/IM - Agent の新規インストール時のセットアップ (UNIX の場合)

クラスタ構成では、次の点に注意してください。

- JP1/IM - Agent のファイルやディレクトリについて、共有ディスク上のファイルやディレクトリが対象になる場合があります。
- 統合エージェントホストでの JP1/IM - Agent のサービスの起動と停止は、クラスタソフトから行います。
- ユニット定義ファイルの設定変更を行う場合は、実行系サーバと待機系サーバの両方で行う必要があります。また、設定する値も同じ値を設定する必要があります。
- セキュリティ製品の除外設定では、共有ディレクトリ/jp1ima も除外対象にする必要があります。

(1) 自動起動の設定

クラスタソフトで制御するため、OS 起動時のサービス自動起動の設定は行いません。

(2) 統合エージェント制御基盤の設定

(a) 複数マネージャーホストへのデータ配信機能を設定する (Linux の場合) (オプション)

■ 新規設定

1. クラスタソフトから JP1/IM - Agent サービスを停止する。

停止するサービスのサービスキーを次に示します。

- jpc_imagent
- jpc_imagentaction
- jpc_imagentproxy
- jpc_alertmanager
- jpc_prometheus_server

- jpc_fluentd

2. 統合エージェント管理基盤のセカンダリー用のディレクトリを作成する。

統合エージェント管理基盤のセカンダリー用のディレクトリとして、次のディレクトリを作成します。

- 共有ディレクトリ/jp1ima/tmp/download-imagent グループ識別子
- 共有ディレクトリ/jp1ima/tmp/upload-imagent グループ識別子
- 共有ディレクトリ/jp1ima/tmp/jbsfwd-imagent グループ識別子
- 共有ディレクトリ/jp1ima/logs/imagent-imagent グループ識別子
- 共有ディレクトリ/jp1ima/logs/imagentproxy-imagent グループ識別子
- 共有ディレクトリ/jp1ima/logs/imagentaction-imagent グループ識別子

上記のディレクトリの作成には、次のコマンドを使用します。

```
mkdir -m 700 ディレクトリ
```

3. 統合エージェント管理基盤のセカンダリー用のユニット定義ファイルを作成する。

/usr/lib/systemd/system 下にあるコピー元のユニット定義ファイルをコピーし、コピー先のファイル名にリネームします。

作成したユニット定義ファイルのオーナーおよびオーナーグループは、root、アクセス権は 644 にします。

コピー元のファイル名	コピー先のファイル名
jpc_imagent_論理ホスト名.service	jpc_imagent-imagent グループ識別子_論理ホスト名.service
jpc_imagentproxy_論理ホスト名.service	jpc_imagentproxy-imagent グループ識別子_論理ホスト名.service
jpc_imagentaction_論理ホスト名.service	jpc_imagentaction-imagent グループ識別子_論理ホスト名.service

4. サービスの起動設定を行う。

実行系サーバと待機系サーバの両方で実施します。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(c) セカンダリーのサービス起動の設定」を参照してください。

5. 統合エージェント制御基盤のセカンダリー用の設定を行う。

実行系サーバで実施します。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(d) 統合エージェント制御基盤の設定ファイル」を参照してください。

6. 統合エージェント制御基盤のセカンダリー用のシークレットを登録する。

実行系サーバで実施します。

セカンダリーの統合エージェント制御基盤が接続する JP1/IM - Manager の初期シークレットを取得して登録します。

登録する初期シークレットのキーについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(e) 初期シークレット，クライアントシークレット，および HTTP プロキシパスワードのキー」を参照してください。

7. 統合エージェント制御基盤以外の設定を行う。

実行系サーバで実施します。

マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.7(5)(f) 統合エージェント制御基盤以外の各プログラムの送信設定」を参照してください。

8. 次のコマンドを実行して，ユニット定義ファイルで定義したサービスを有効化する。

実行系サーバと待機系サーバの両方で実施します。

```
systemctl daemon-reload
```

9. クラスタソフトに論理ホスト用のサービスを登録する。

クラスタソフトに登録するサービスは，次のとおりです。

サービス
jpc_imagent-imaget グループ識別子
jpc_imagentproxy-imaget グループ識別子
jpc_imagentaction-imaget グループ識別子

クラスタソフトに登録するコマンドについては、「[8.3.6 統合エージェントホストでの JP1/IM - Agent の新規インストール \(UNIX の場合\)](#)」の手順 7「クラスタソフトに論理ホスト用のサービスを登録する。」を参照してください。

(b) 複数マネージャーホストへのデータ配信機能を解除する (Linux の場合) (オプション)

複数マネージャーホストへのデータ配信機能を使用しなくなった場合の設定手順を次に示します。

ご使用の運用環境に合わせて，次のどちらかを実施します。

- 論理ホストのアンインストールを行わずに，複数マネージャーホストへのデータ配信機能だけを削除する
- 論理ホストのアンインストールを行う

■ 論理ホストのアンインストールを行わずに，複数マネージャーホストへのデータ配信機能だけを削除する場合

1. 論理ホストで稼働している JP1/IM - Agent のサービスを停止する。

実行系サーバだけで実施します。

クラスタソフトから論理ホストで稼働しているサービスを停止します。

2. クラスタソフトに登録されたサービスを解除する。

実行系サーバだけで実施します。

「[8.3.7\(2\)\(a\) 複数マネージャーホストへのデータ配信機能を設定する \(Linux の場合\) \(オプション\)](#)」の手順 8 で登録したサービスを解除します。

サービスを解除する方法については、クラスタソフトのドキュメントを確認してください。

3. systemd に登録されたセカンダリーのサービスを解除するために有効化する。

実行系サーバと待機系サーバの両方で実施します。

有効化する方法については、「[8.7.3 JP1/IM - Agent のアンインストール \(UNIX の場合\)](#)」の手順 3 を参照してください。

4. 複数マネージャーホストへのデータ配信機能を使用するために作成したシークレットを削除する。

実行系サーバで実施します。

削除するシークレットのキーについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「[3.15.7\(5\)\(e\) 初期シークレット, クライアントシークレット, および HTTP プロキシパスワードのキー](#)」を参照してください。

すでに消えているシークレットについては、この手順は不要です。

5. 複数マネージャーホストへのデータ配信機能を使用するために設定した内容を元に戻す。

実行系サーバと待機系サーバの両方で実施します。

「[8.3.7\(2\)\(a\) 複数マネージャーホストへのデータ配信機能を設定する \(Linux の場合\) \(オプション\)](#)」の「新規設定」の手順 4 と手順 7 で設定した統合エージェント制御基盤のセカンダリー用の設定を元に戻します。

6. 複数マネージャーホストへのデータ配信機能を使用するためにコピーしたファイルを削除する。

実行系サーバと待機系サーバの両方で実施します。

「[8.3.7\(2\)\(a\) 複数マネージャーホストへのデータ配信機能を設定する \(Linux の場合\) \(オプション\)](#)」の「新規設定」の手順 2 でコピーした統合エージェント管理基盤のセカンダリー用のファイルを削除します。

7. 複数マネージャーホストへのデータ配信機能を使用するために作成したディレクトリを削除する。

実行系サーバと待機系サーバの両方で実施します。

ログなどの必要なファイルを退避したあと、「[8.3.7\(2\)\(a\) 複数マネージャーホストへのデータ配信機能を設定する \(Linux の場合\) \(オプション\)](#)」の「新規設定」の手順 1 で作成した統合エージェント管理基盤のセカンダリー用のディレクトリを削除します。

8. systemd を更新する。

実行系サーバと待機系サーバの両方で実施します。

更新方法については、「[8.7.3 JP1/IM - Agent のアンインストール \(UNIX の場合\)](#)」の手順 5 を参照してください。

9. 無効化したセカンダリーのサービスが接続している JP1/IM - Manager 側で登録している統合エージェント情報を削除する。

JP1/IM - Manager の実行系サーバと待機系サーバの両方で実施します。JP1/IM - Agent の実行系サーバと待機系サーバでは実施しません。

統合エージェント情報の削除手順については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.1 [統合エージェント一覧] 画面」を参照してください。

■ 論理ホストのアンインストールを行う場合

「8.7.3 JP1/IM - Agent のアンインストール (UNIX の場合)」の手順 1 と手順 2 の間に、上記の「論理ホストのアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合」の手順 4 から手順 8 を実施します。

実施後に、上記の「論理ホストのアンインストールを行わずに、複数マネージャーホストへのデータ配信機能だけを削除する場合」の手順 10 を実施します。

(3) OS シャットダウン時の自動停止の設定

クラスタソフトで制御するため、OS シャットダウン時のサービス停止の設定は行いません。

(4) その他の設定

クラスタ構成での設定変更の手順については、通常ホストの設定変更と基本的に同じです。通常ホストの設定変更については、「2.19 JP1/IM - Agent のセットアップ (UNIX の場合)」を参照してください。

8.4 インテリジェント統合管理基盤のクラスタ環境を構築する（UNIX の場合）

クラスタシステムで運用されている JP1/IM - Manager ホストに対応する場合に、インテリジェント統合管理基盤で行うクラスタ環境の構築について説明します。

なお、インテリジェント統合管理基盤のクラスタ環境を構築すると、JP1/IM - Manager サービスの起動時間が延びます。クラスタソフトで JP1/IM - Manager サービスの起動時間を監視している場合や JP1/Base の起動管理機能で JP1/IM - Manager サービスを起動している場合は、クラスタソフトのタイムアウト値を見直す必要があります。インテリジェント統合管理基盤を設定したあとでサービスの起動時間を確認し、タイムアウト値を調整してください。

インテリジェント統合管理基盤の共有ディスク上のファイル構成を、次の表に示します。

表 8-4 共有ディスク上のファイル構成

OS	共有ファイル種別	フォルダ名
UNIX	定義ファイル	共有ディレクトリ/jp1imm/conf/imdd/ 共有ディレクトリ/jp1imm/conf/ssl/※
	ログファイル	共有ディレクトリ/jp1imm/log/imdd/
	プラグイン	共有ディレクトリ/jp1imm/plugin/imdd/
	データファイル	共有ディレクトリ/jp1imm/data/imdd/
	対処アクション実行履歴	共有ディレクトリ/jp1imm/log/suggestion

注※ ssl フォルダは、通信暗号化機能を有効にして JP1/IM3 - Manager サービスを起動すると作成されます。

8.4.1 クラスタ環境を新規構築する（UNIX の場合）

インテリジェント統合管理基盤のクラスタ環境の新規構築手順を次に示します。

セットアップ後に JP1/IM - Manager を起動する手順については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3. JP1/IM - Manager の起動と終了」を参照してください。

なお、次の手順を行う前に、セントラルコンソールと統合監視 DB のクラスタ環境の構築が完了していることを確認してください。

1. JP1/IM - Manager を停止する。

物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止してください。

2. 定義ファイルのディレクトリをコピーする。

物理ホストの定義ファイルの imdd ディレクトリを、共有ディレクトリにコピーします。次のコマンドを実行します。

```
cp -a /etc/opt/jp1imm/conf/imdd 共有ディレクトリ/jp1imm/conf/
```


3. プラグインのディレクトリをコピーする。

物理ホストのプラグインのplugin ディレクトリを、共有ディレクトリにコピーします。次のコマンドを実行します。

```
cp -a /etc/opt/jp1imm/plugin 共有ディレクトリ/jp1imm/
```

4. データファイル出力先ディレクトリを作成する。

データファイル出力先ディレクトリとして「共有ディレクトリ/jp1imm/data/imdd/」を作成します。次のコマンドを実行します。

```
mkdir -p 共有ディレクトリ/jp1imm/data/imdd/
```

5. イベント転送中継情報ディレクトリを作成する。

イベント転送中継情報ディレクトリとして「共有ディレクトリ/jp1imm/data/imdd/eventForward/」を作成します。次のコマンドを実行します。

```
mkdir -p 共有ディレクトリ/jp1imm/data/imdd/eventForward/
```

6. インテリジェント統合管理基盤定義ファイル (imdd.properties) を編集します。

論理ホストの統合監視 DB のセットアップ時に使用したクラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf) のLOGICALHOSTNUMBER パラメーターとIMDBPORT パラメーターに指定した値をインテリジェント統合管理基盤定義ファイルに指定します。

```
jp1.im.db.DEFAULT.logicalHostNum=LOGICALHOSTNUMBERの設定値  
jp1.im.db.DEFAULT.portNo=IMDBPORTの設定値
```

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「クラスタセットアップ情報ファイル (jimdbclustersetupinfo.conf)」(2. 定義ファイル) を参照してください。

また、トレンドデータ削除を実行するときのインターバルとして、インテリジェント統合管理基盤定義ファイル (imdd.properties) の設定項目「jp1.imdd.trenddata.deleteInterval」に、「[8.5.3 クラスタソフトのパラメーターの設定 \(Linux の場合\)](#)」で「監視する間隔」に指定した値の2倍の値を設定します。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」で、「2.7.2(3)(g)トレンドデータの手動削除 (統合エージェント, ユーザー独自の Prometheus, ユーザー独自の Fluentd のホスト名を指定して削除)」の「[トレンドデータの削除時の注意事項](#)」の1.を参照してください。

7. 次のjcoimdef コマンドを実行して、インテリジェント統合管理基盤を有効にします。

```
/opt/jp1cons/bin/jcoimdef -dd ON -hostmap ON -h 論理ホスト名
```

jcoimdef コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcoimdef」(1. コマンド) を参照してください。

8. 操作履歴出力先ディレクトリを作成する。

操作履歴出力先ディレクトリとして「共有ディレクトリ/jp1imm/operation/imdd/suggestion/」を作成します。次のコマンドを実行します。

```
mkdir -p 共有ディレクトリ/jp1imm/operation/imdd/suggestion/
```

9. インテリジェント統合管理データベースをセットアップする。

インテリジェント統合データベースの論理ホスト環境を構築します。

- 実行系ホストの場合
構築手順については、「[8.3.3\(5\) JP1/IM - Manager \(インテリジェント統合管理データベース\) の設定](#)」を参照してください。
- 待機系ホストの場合
構築手順については、「[8.3.5\(5\) JP1/IM - Manager \(インテリジェント統合管理データベース\) の設定](#)」を参照してください。

10. サービスを起動する。

クラスタソフトから次のサービスを起動します。

- JP1/IM3-Manager_論理ホスト名

8.4.2 修正版を適用したクラスタ環境を構築する (UNIX の場合)

修正版を適用したクラスタ環境の構築手順について説明します。クラスタ環境に修正版を適用した場合は、プラグインの再配置が必要です。

1. JP1/IM - Manager を停止する。

物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止してください。

2. プラグインのディレクトリをコピーする。

物理ホストのプラグインのplugin ディレクトリを、共有ディレクトリにコピーします。次のコマンドを実行します。

```
cp -a /etc/opt/jp1imm/plugin 共有ディレクトリ/jp1imm/
```

3. サービスを起動する。

クラスタソフトから JP1/IM3-Manager を起動します。

8.4.3 バージョンアップしてクラスタ環境を構築する (UNIX の場合)

インテリジェント統合管理基盤をクラスタ環境で使用している場合に、バージョンアップする手順について説明します。なお、手順を実行しない場合、旧バージョンから追加された機能は使用できません。

また、連携製品のバージョンアップも同時に実施する場合は、手順 8 を実行する前に連携製品のバージョンアップを実施してください。

1. JP1/IM - Manager を停止する。

物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止してください。

2. プラグインのディレクトリをコピーする。

物理ホストのプラグインの plugin ディレクトリを、共有ディレクトリにコピーします。次のコマンドを実行します。

```
cp -a /etc/opt/jp1imm/plugin 共有ディレクトリ/jp1imm/
```

3. 定義ファイルをコピーする。

物理ホストの定義ファイルを、共有ディレクトリにコピーします。次のコマンドを実行します。

```
cp -a -n /etc/opt/jp1imm/conf/imdd/ 共有ディレクトリ/jp1imm/conf/imdd/  
cp -a /etc/opt/jp1imm/conf/imdd/*.model 共有ディレクトリ/jp1imm/conf/imdd/  
cp -a /etc/opt/jp1imm/conf/imdd/system/*.model 共有ディレクトリ/jp1imm/conf/imdd/system/  
cp -a /etc/opt/jp1imm/conf/imdd/system/*.update 共有ディレクトリ/jp1imm/conf/imdd/system/  
cp -a /etc/opt/jp1imm/conf/imdd/system/fileoperation/*.update 共有ディレクトリ/jp1imm/conf/imdd/system/fileoperation  
cp -a /etc/opt/jp1imm/conf/imdd/responseaction/*.model 共有ディレクトリ/jp1imm/conf/imdd/responseaction  
cp -a /etc/opt/jp1imm/conf/imdd/fileoperation/*.model 共有ディレクトリ/jp1imm/conf/imdd/fileoperation  
cp -a /etc/opt/jp1imm/conf/imdd/suggestion/*.model 共有ディレクトリ/jp1imm/conf/imdd/suggestion  
cp -a /etc/opt/jp1imm/conf/imdd/plugin 共有ディレクトリ/jp1imm/conf/imdd/  
cp 共有ディレクトリ/jp1imm/conf/imdd/system/imdd_system.properties.update 共有ディレクトリ/jp1imm/conf/imdd/system/imdd_system.properties  
cp 共有ディレクトリ/jp1imm/conf/imdd/system/fileoperation/imdd_product_deffile_list.json.update 共有ディレクトリ/jp1imm/conf/imdd/system/fileoperation/imdd_product_deffile_list.json
```

4. イベント転送中継情報ディレクトリを作成する。

イベント転送中継情報ディレクトリとして「共有ディレクトリ/jp1imm/data/imdd/eventForward/」を作成します。次のコマンドを実行します。

```
mkdir -p 共有ディレクトリ/jp1imm/data/imdd/eventForward/
```

5. インテリジェント統合管理データベースをセットアップする。

V12 の JP1/IM - Manager からバージョンアップした場合は、インテリジェント統合管理データベースの論理ホスト環境を構築します。

- 実行系ホストの場合
構築手順については、「[8.3.3\(5\) JP1/IM - Manager \(インテリジェント統合管理データベース\) の設定](#)」を参照してください。
- 待機系ホストの場合

構築手順については、「[8.3.5\(5\) JP1/IM - Manager \(インテリジェント統合管理データベース\) の設定](#)」を参照してください。

6. 新しい設定値を追加する。

利用する機能に合わせて、新しく追加された設定値を追加します。※

注※

JP1/IM - Manager を 13-00 または 13-01 から 13-10 以降にバージョンアップした場合、テキストエディターなどで、次のファイルの末尾に「`web-enable-admin-api: true`」の行を追加します。なお、インテリジェント統合管理データベースを再構築したときは、自動で追加されるため、この手順は不要です。

共有ディレクトリ/`jp1imm/conf/imgndb/config.yml`

上記の手順を実施しなかった場合、トレンドデータの削除と統合エージェント情報の削除が失敗します。

トレンドデータの削除と統合エージェント情報については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.1 [統合エージェント一覧] 画面」、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「5.11.4 トレンドデータ削除」および「5.18.2 統合エージェント情報削除」を参照してください。

7. サービスを起動する。

クラスタソフトから次のサービスを起動します。

- JP1/IM3-Manager_論理ホスト名
- JP1/IM3-Manager Intelligent Integrated DB Server_論理ホスト名
- JP1/IM3-Manager Trend Data Management Service_論理ホスト名
- JP1/IM-Agent Base Server_論理ホスト名
- JP1/IM-Agent Base Proxy Server_論理ホスト名

8. `jddcreatetree` コマンドを実行して、IM 管理ノード関連ファイルを生成する。

`jddcreatetree` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jddcreatetree`」(1. コマンド)を参照してください。

9. `jddupdatetree` コマンドを新規・再構築モードで実行して、定義内容をインテリジェント統合管理サーバに反映する。

`jddupdatetree` コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「`jddupdatetree`」(1. コマンド)を参照してください。

8.5 新規インストール・セットアップでのクラスタソフトへの登録（UNIXの場合）

新規にインストール・セットアップする場合、JP1/IM - Manager をクラスタ運用するには、論理ホストの JP1/IM - Manager, JP1/Base, および JP1/IM - Agent をクラスタソフトに登録して、クラスタソフトからの制御で起動・停止するように設定します。

起動については、リソース、JP1/Base, JP1/IM - Manager, JP1/IM - Agent の順番でサービスを起動してください。

なお、JP1/IM - Agent のサービスは複数存在します。これらのサービスの起動処理や停止処理が同時に行われないように、依存関係などを設定してください。サービスの起動や停止の順番は、任意で問題ありません。

また、JP1/IM - Agent のサービスは、論理 IP アドレスリソースと共有ディレクトリの準備ができたあとで起動するように、依存関係を設定してください。

JP1/IM - Agent の対象のサービスは次のとおりです。使用するサービスのみクラスタに登録します。

- jpc_node_exporter
- jpc_blackbox_exporter
- jpc_ya_cloudwatch_exporter
- jpc_imagent
- jpc_imagentproxy
- jpc_imagentaction
- jpc_alertmanager
- jpc_prometheus_server
- jpc_fluentd
- jpc_vmware_exporter

クラスタに登録したあとの操作については次のとおりです。

- 起動

次のコマンドでサービスを起動します。

```
/opt/jp1ima/tools/jpc_service_start -s サービスキー -h 論理ホスト名
```

- 停止

次のコマンドでサービスを停止します。

```
/opt/jp1ima/tools/jpc_service_stop -s サービスキー -h 論理ホスト名
```

- 強制停止

次のコマンドでサービスを強制停止します。

```
/opt/jp1ima/tools/jpc_service_stop -s サービスキー -h 論理ホスト名 -f
```

- 動作監視

次のコマンドでサービスのステータスをチェックします。

```
systemctl is-active サービスキー 論理ホスト名
```

8.5.1 クラスタソフトに登録するスクリプトの作成 (UNIX の場合)

UNIX のクラスタソフトでは、通常、スクリプトなどによりアプリケーションを制御するツールを作成して、クラスタソフトに登録します。このときのスクリプトには一般的に、起動、停止、動作監視、強制停止の機能が必要です。

ここでは、スクリプト設計に必要な JP1/IM - Manager の情報を次に説明します。この情報を基に、クラスタソフトの仕様に合わせて、JP1/IM - Manager を制御するスクリプトを作成し、クラスタソフトに登録してください。

表 8-5 クラスタ登録でのスクリプト設計のための詳細情報

登録する機能	説明
起動	JP1/IM - Manager を起動します。 • 使用するコマンド 「jco_start.cluster 論理ホスト名」 • 起動コマンドの終了タイミング 起動コマンドは、JP1/IM - Manager が起動するのを待って終了します。ただし、何らかの問題によって、タイムアウト時間（デフォルト 300 秒）を過ぎても起動処理が完了しない場合は、起動処理の途中でコマンドが終了します。この場合、起動処理は中断せず、起動処理を続けている状態のままコマンドが終了します。 タイムアウト時間の設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.7.11 JP1/IM - Manager の起動・停止のタイムアウト時間の検討 (UNIX の場合)」を参照してください。 • 起動コマンドの結果判定 JP1/IM - Manager を起動した結果は、後述する動作監視の方法によって判定してください。通常は、クラスタソフトの動作監視によって判定します。なお、起動コマンドの戻り値は、0（正常終了）と 1（引数異常）のため、戻り値での結果判定はできません。
停止	JP1/IM - Manager を停止します。 • 使用するコマンド 「jco_stop.cluster 論理ホスト名」 • 停止コマンドの終了タイミング 停止コマンドは、JP1/IM - Manager が停止するのを待って終了します。ただし、何らかの問題によって、タイムアウト時間（デフォルト 300 秒）を過ぎても停止処理が完了しない場合は、停止処理の途中でコマンドが終了します。この場合、停止処理は中断せず、停止処理を続けている状態のままコマンドが終了します。

登録する機能	説明
	タイムアウト時間の設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.7.11 JP1/IM - Manager の起動・停止のタイムアウト時間の検討 (UNIX の場合)」を参照してください。 停止コマンドの結果判定 JP1/IM - Manager を停止した結果は、後述する動作監視の方法によって判定してください。なお、停止コマンドの戻り値は、0 (正常終了) と 1 (引数異常) のため、戻り値での結果判定はできません。 なお、停止コマンドが終了したあと、後述する強制停止コマンドを実行することをお勧めします。これは、何らかの問題がある場合でも確実にプロセスを終了させ、フェールオーバーが失敗することを防ぐためです。
JP1/IM - Manager の動作監視※1	JP1/IM - Manager が正常に動作していることを監視します。 - 使用するコマンド 「jco_spmc_status -h 論理ホスト名」 正常動作していることは、jco_spmc_status コマンドの戻り値によって判定します。このコマンドでは、各プロセスが動作しているか、動作していないかで動作状態を判定しています。 動作監視の機能を提供していないクラスタソフトもあります。また、JP1/IM - Manager の障害時にフェールオーバーする必要がある場合、この機能は登録しません。 - 動作監視の結果判定 各戻り値の判定方法を次に示します。 戻り値=0 (すべて動作) JP1/IM - Manager は正常に動作しています。 戻り値=1 (エラー) 回復不能なエラーが発生しました。異常と判定してください。 注意 共有ディスクがオフラインの待機系サーバでjco_spmc_status コマンドを実行すると、共有ディスクがないため戻り値が 1 になります。 戻り値=4 (一部停止) JP1/IM - Manager の一部のプロセスが、何らかの問題によって停止しています。異常と判定してください。 戻り値=8 (すべて停止) JP1/IM - Manager のプロセスが何らかの問題によって停止しています。異常と判定してください。 戻り値=12 (リトライ可能エラー) jco_spmc_status コマンドによる動作状態の確認中に、リトライによって復旧可能なエラーが発生しました。一定回数を限度に、動作状態の確認をリトライしてください。
IM データベースの稼働状態の確認※2	IM データベースが正常に稼働しているかどうかを確認します。 - 使用するコマンド 「jimdbstatus -h 論理ホスト名」 稼働状態は、jimdbstatus コマンドの戻り値によって判定します。 - 稼働状態の結果判定 各戻り値の判定方法を次に示します。 戻り値=0：稼働中 戻り値=1：jimdbstatus コマンドが異常終了 戻り値=4：起動・停止処理中

登録する機能	説明
	戻り値=8：停止中（IM データベースが再起動中断状態であり、不安定な状態） 戻り値=12：停止中（正常に停止された状態） 戻り値=20：組み込み HiRDB が未セットアップの状態 戻り値 1, 4 がリトライ対象の値となります。また、戻り値 8 以降はエラーで、フェールオーバー対象となります。
インテリジェント統合管理データベースの稼働状態の確認※3	インテリジェント統合管理データベースを使用している場合、インテリジェント統合管理データベースが正常に稼働しているかどうかを確認します。 - 使用するコマンド 「jimgndbstatus -h 論理ホスト名」 - 稼働状態の結果判定 各戻り値の判定方法を次に示します。 戻り値=0：稼働中 戻り値=1：jimgndbstatus コマンドが異常終了 戻り値=12：停止中 戻り値=16：インテリジェント統合管理データベースが起動状態、かつ、トレンドデータ管理サービスが停止状態 戻り値=17：インテリジェント統合管理データベースが停止状態、かつ、トレンドデータ管理サービスが起動状態 戻り値=20：インテリジェント統合管理データベースが未セットアップの状態
強制停止	JP1/IM - Manager を強制的に停止し、使用中のリソースを解放します。 使用するコマンド 「jco_killall.cluster 論理ホスト名」 jco_killall.cluster コマンドを実行すると、JP1/IM - Manager の終了処理を一切行わずに、各プロセスを強制的に停止します。 IM データベースサービスを使用している場合、IM データベースサービスも強制終了します。 インテリジェント統合管理データベース（トレンドデータ管理 DB）を使用している場合、インテリジェント統合管理データベースサービスも強制終了します。 注意 強制停止をする前に、停止コマンドによって JP1/IM - Manager を停止してください。

注※1

動作確認に関する JP1 の動作について、ここで説明している UNIX の場合と、Windows の場合は、使用するコマンドは同じですが動作は異なりますので注意してください。

Windows の場合は、Windows のサービス制御との関連によって、UNIX の場合とは動作が異なります。Windows では、プロセスの一部が停止すると、JP1 のプロセス管理が自動的にすべての各プロセスを停止して、サービスを停止状態にします。サービスの停止によって異常と判定するか、jco_spmc_status コマンドなどの戻り値が 8 になるのを待ってから異常と判定してください。

注※2

IM データベースを使用している場合に実行します。

注※3

インテリジェント統合管理データベースを使用している場合に実行します。

メモ

JP1 の再起動について

クラスタ運用の JP1 の障害を検知した場合に、待機系サーバにフェールオーバーする前に、同じサーバで JP1 を再起動して回復を試みる場合があります。

この場合は、JP1 のプロセス管理による再起動を使用しないでください。

クラスタソフトは JP1 の障害検知後に再起動を試みるため、障害の内容によっては JP1 の再起動機能が影響を受け、正常に動作できない可能性があります。より確実に再起動を行うために、クラスタソフトからの制御で JP1 を再起動してください。

8.5.2 リソースの起動停止順序の設定（UNIX の場合）

論理ホストの JP1/IM - Manager および JP1/Base を実行するには、共有ディスクおよび論理 IP アドレスが使用可能になっている必要があります。

クラスタソフトの制御により、次のように動作するように起動停止の順序またはリソースの依存関係を設定してください。

- 論理ホストの起動時
 1. 共有ディスクおよび論理 IP アドレスを割り当てて使用可能にする。
 2. JP1/Base, JP1/IM - Manager の順に起動する。
- 論理ホストの停止時
 1. JP1/IM - Manager, JP1/Base の順に停止する。
 2. 共有ディスクおよび論理 IP アドレスの割り当てを解除する。

8.5.3 クラスタソフトのパラメーターの設定（Linux の場合）

「8.5.1 クラスタソフトに登録するスクリプトの作成（UNIX の場合）」の「表 8-5 クラスタ登録でのスクリプト設計のための詳細情報」に記載している「インテリジェント統合管理データベースの稼働状態の確認（`jimgndbstatus` コマンド）」に対して、次の設定をします。設定する値の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」で、「2.7.2(3)(g) トレンドデータの手動削除（統合エージェント、ユーザー独自の Prometheus、ユーザー独自の Fluentd のホスト名を指定して削除）」の「トレンドデータの削除時の注意事項」の 1.を参照してください。

- 監視する間隔：14 秒以上
- 停止したと判断する回数：連続で 2 回以上

8.6 論理ホストのバージョンアップインストール・セットアップ (UNIX の場合)

JP1/IM - Manager および JP1/IM - Agent の論理ホストのバージョンアップインストールおよびセットアップについて説明します。なお、JP1/IM - Manager と同じ論理ホストに JP1/Base をセットアップする必要がありますので、あわせて説明します。

作業を始める前に、クラスタシステムについて次の情報を確認してください。

表 8-6 論理ホストのインストール・セットアップ前の確認 (UNIX)

確認項目	説明
論理ホスト名	JP1 を実行する論理ホストのホスト名
論理 IP アドレス	論理ホスト名に対応する IP アドレス
共有ディレクトリ	論理ホストの JP1 の実行環境ファイル一式を格納する共有ディスク上のフォルダ

また、これらが「[7.1.2 クラスタ運用の前提条件 \(Windows の場合\)](#)」を満たしていることを確認してください。

確認ができれば、インストール・セットアップを始めます。

なお、論理ホスト名は、英大文字・英小文字を区別します。論理ホスト名には、JP1/Base で設定した論理ホスト名を英大文字・英小文字を含めて正確に指定してください。誤った論理ホスト名を指定し、論理ホストのインストール・セットアップを行ってしまった場合は、IM データベースと論理ホストを削除してから、再度、論理ホストのインストール・セットアップを行ってください。IM データベースと論理ホストの削除については、「[8.7.1 論理ホストの削除 \(UNIX の場合\)](#)」を参照してください。

8.6.1 JP1/Base および JP1/IM - Manager のバージョンアップインストール (UNIX の場合)

実行系サーバ、待機系サーバそれぞれのローカルディスク上に JP1/IM - Manager および JP1/Base をインストールしてください。

1. 設定情報とデータベースをバックアップする。

バックアップの方法は、過去のバージョンのマニュアルを参照してください。

2. JP1/Base をインストールする。

3. JP1/IM - Manager をインストールする。

❗ 重要

IM データベースをセットアップ済みの環境で、JP1/IM - Manager をバージョンアップした場合、`jimdbupdate` コマンドを実行して IM データベースを更新してください。IM データベースを更新していない場合は、JP1/IM - Manager を起動したときに警告メッセージが表示されます。

❗ 重要

インテリジェント統合管理データベースをセットアップ済みの環境で、JP1/IM - Manager をバージョン 13-10 以前から 13-11 以降にバージョンアップした場合、`jimgndbupdate` コマンドを実行してインテリジェント統合管理データベースを更新してください。インテリジェント統合管理データベースを更新していない場合、JP1/IM - Manager のサービス起動に失敗することがあります。

8.6.2 JP1/IM - Agent のバージョンアップインストール (UNIX の場合)

JP1/IM - Agent をバージョン 13-00 または 13-01 からバージョンアップする場合、「[2.3.4\(9\) JP1/IM - Agent をバージョン 13-00 または 13-01 からバージョンアップした場合の注意事項](#)」も参照してください。

1. JP1/IM - Agent のサービスを停止する。

クラスタソフトから論理ホストの JP1/IM - Agent のサービスを停止します。物理ホストでも運用している場合は、物理ホストの JP1/IM - Agent のサービスを停止します。

2. JP1/IM - Agent をバージョンアップインストールする。

インストール方法については、「[2.3.1\(2\) JP1/IM - Agent のインストールの手順](#)」を参照してください。実行系サーバと待機系サーバの両方で実施します。

3. 論理ホスト用のバージョンアップセットアップコマンドの設定ファイルを作成する。

設定ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「論理ホストバージョンアップセットアップの設定ファイル (任意のファイル名)」(2. 定義ファイル) を参照してください。

また、設定ファイルのサンプルファイルが、次のパスに格納されています。コピーして作成できます。

JP1/IM - Agentのインストール先ディレクトリ/jp1ima/conf/sample/jpc_lhupdate.properties

4. 論理ホスト用のバージョンアップセットアップコマンドを実行する。

```
jimalhupdate -h 論理ホスト名 -d 共有ディレクトリ -c {online | standby} -f セットアップ設定ファイル [-q]
```

論理ホスト用のバージョンアップセットアップコマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimalhupdate」(1. コマンド) を参照してください。

実行系サーバと待機系サーバの両方で実施します。

5. systemd に追加されたサービスが登録されたことを確認する。

実行系サーバと待機系サーバの両方で、systemd のサービス一覧を表示して、論理ホスト用のサービスが登録されたことを確認します。

論理ホスト用のサービスの名称は、ユニット定義ファイルのファイル名となります。

コマンドプロンプトで次のコマンドを実行します。

```
systemctl list-unit-files -t service
```

6. 追加されたアドオンプログラムで必要な設定を行う。

追加されたアドオンプログラムを使用する場合、「[2.19.2 \(14\) VMware exporter の設定](#)」および「[2.19.2\(3\)\(i\) VMware exporter のスケイプジョブを追加する \(Linux の場合\) \(オプション\)](#)」を参照して必要な設定を行います。

7. クラスタソフトに論理ホスト用のサービスを登録する。

クラスタソフトに論理ホスト用のサービスを登録します。

対象のサービス名は次のとおりです。使用するサービスだけをクラスタソフトに登録します。

```
jpc_vmware_exporter
```

- 起動

次のコマンドでサービスを起動します。

```
/opt/jp1ima/tools/jpc_service_start -s jpc_vmware_exporter -h 論理ホスト名
```

- 停止

次のコマンドでサービスを停止します。

```
/opt/jp1ima/tools/jpc_service_stop -s jpc_vmware_exporter -h 論理ホスト名
```

- 強制停止

次のコマンドでサービスを強制停止します。

```
/opt/jp1ima/tools/jpc_service_stop -s jpc_vmware_exporter -h 論理ホスト名 -f
```

- 動作監視

次のコマンドでサービスのステータスをチェックします。

```
systemctl is-active jpc_vmware_exporter_論理ホスト名
```

8. 動作に問題がないか確認する。

- クラスタソフトからサービスを起動します。
- フェールオーバーさせます。

9. JP1/IM - Agent のサービスを起動する。

クラスタソフトから論理ホストの JP1/IM - Agent のサービスを起動します。

物理ホストでも運用している場合は、物理ホストの JP1/IM - Agent のサービスを起動します。

8.6.3 バージョンアップインストール時の物理ホスト環境のセットアップ (UNIX の場合)

物理ホストの JP1/IM - Manager を使う場合は、「2.18.11 バージョンアップ時の設定 (UNIX の場合)」の手順に従ってセットアップを行ってください。

8.6.4 バージョンアップインストール時の論理ホスト環境 (実行系) のセットアップ (UNIX の場合)

セントラルスコープの機能を使用する場合は、手順 6 から手順 8 が必要になります。セントラルスコープの機能を使用しない場合は、手順 6 から手順 8 を飛ばしてください。

1. JP1/IM - Manager を停止する。

物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止してください。

2. JP1/Base の論理ホスト環境をセットアップする。

JP1/Base をバージョンアップした場合には、マニュアル「JP1/Base 運用ガイド」のインストール・アンインストール時の注意事項の説明を参照し、セットアップをしてください。JP1/Base をバージョンアップしなかった場合にはセットアップの必要はありません。

3. 共有ディスクが使用可能なことを確認する。

4. jp1cohaverup コマンドを実行する。

/opt/jp1cons/bin/jp1cohaverup -h 論理ホスト名

5. イベント取得フィルターの位置をイベント基盤サービスに変更する場合は jcochafmode コマンドを実行する。

/opt/jp1cons/bin/jcochafmode -h 論理ホスト名

6. ディスクの空き容量を確認する。

JP1/IM - Manager をバージョンアップするには、/var/opt/jp1scope/database/下のディスク容量分の空き容量が、ハードディスクに必要です。

7. jp1cshaverup コマンドを実行する。

/opt/jp1scope/bin/jp1cshaverup -h 論理ホスト名 -w 作業フォルダ

8. jbssetcnf コマンドを実行する。

次に示す機能の有効、無効は旧バージョンの JP1/IM - Manager またはセントラルスコープの設定に依存します。

- 状態変更イベントの上限監視
- 対処済み連動機能
- 状態変更イベントの自動削除
- 監視オブジェクトの初期化
- 状態変更条件メモリー常駐機能

機能の有効、無効を設定したい場合、次の表に示すファイルを引数に `jbssetcnf` コマンドを実行してください。

表 8-7 機能の有効、無効を設定するためのファイル

ファイル名	説明
状態変更イベント件数の上限監視設定ファイル (<code>evhist_warn_event_on.conf</code> , <code>evhist_warn_event_off.conf</code>)	監視オブジェクトの状態変更イベント件数が上限値（100 件）を超えた際に、JP1 イベントを発行する機能を有効または無効にするためのファイルです。
対処済み連動設定ファイル (<code>action_complete_on.conf</code> , <code>action_complete_off.conf</code>)	対処済み連動機能を有効または無効にするためのファイルです。
状態変更イベント自動削除設定ファイル	JP1 イベントの対処状況を「対処済」にしたときに、状態変更イベントを自動で削除する機能を有効または無効にするためのファイルです。
監視オブジェクト初期化設定ファイル	特定の JP1 イベントを受信したときに、監視オブジェクトを自動で初期化する機能を有効または無効にするためのファイルです。
状態変更条件メモリー常駐機能の設定ファイル	状態変更条件メモリー常駐機能を有効または無効にするためのファイルです。

9. 共通定義情報を退避する。

`/opt/jp1base/bin/jbsgetcnf -h 論理ホスト名 > 共通定義情報退避ファイル名`

8.6.5 バージョンアップインストール時の共通定義情報のコピー（UNIX の場合）

1. JP1/IM - Manager を停止する。

物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止してください。

2. 実行系で退避した共通定義情報退避ファイルを待機系にコピーする。

FTP など任意の方法でコピーしてください。

3. 共通定義情報を設定する。

`/opt/jp1base/bin/jbssetcnf 共通定義情報退避ファイル名`

8.7 論理ホストのアンインストール (UNIX の場合)

JP1/IM - Manager および JP1/IM - Agent の論理ホストのアンインストールについて説明します。まず、論理ホストを削除する手順について説明します。次に、実行系サーバ、待機系サーバそれぞれのローカルディスク上の JP1/IM - Manager, JP1/Base, および JP1/IM - Agent のアンインストール手順について説明します。

8.7.1 論理ホストの削除 (UNIX の場合)

論理ホストを削除するための手順を次に示します。実行系サーバおよび待機系サーバで削除を行ってください。

IM データベース (統合監視 DB および IM 構成管理 DB) を使用している場合は、論理ホストを削除する前、または削除したあとに IM データベースを削除する必要があります。

(1) IM データベースの削除

IM データベース (統合監視 DB および IM 構成管理 DB) を使用している場合の設定手順です。

環境を再構築するために IM データベースを削除する場合は、事前にバックアップを取得してください。バックアップの方法については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「1.2 データベースの管理」を参照してください。

1. JP1/IM - Manager を停止する。

物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止してください。論理ホスト環境の場合はクラスタソフトの操作で停止してください。

接続中の JP1/IM - View はログアウトして切断してください。

JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスも停止してください。

2. jcodbunsetup コマンドを実行し、統合監視 DB を削除する。

jcodbunsetup -h 論理ホスト名 -c {online|standby} [-q]

引数により、論理ホスト名、アンセットアップ種別を指定します。

- 論理ホスト名 (-h オプション)

実行系サーバでセットアップした論理ホスト名を指定します。

- アンセットアップ種別 (-c オプション)

実行系ホストでの統合監視 DB を削除する場合は「online」、待機系ホストでの統合監視 DB を削除する場合は「standby」を指定します。

jcodbunsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcodbunsetup」(1. コマンド) を参照してください。

3. jcfdbunsetup コマンドを実行し、IM 構成管理 DB を削除する。

```
jcfdbunsetup -h 論理ホスト名 -c {online|standby} [-q]
```

引数により、論理ホスト名、アンセットアップ種別を指定します。

- 論理ホスト名 (-h オプション)

実行系サーバでセットアップした論理ホスト名を指定します。

- アンセットアップ種別 (-c オプション)

実行系ホストでの IM 構成管理 DB を削除する場合は「online」、待機系ホストでの IM 構成管理 DB を削除する場合は「standby」を指定します。

jcfdbunsetup コマンドについては、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jcfdbunsetup」(1. コマンド)を参照してください。

4. 次のファイルおよびディレクトリを削除する。

共有ディレクトリ/data/imcf/imconfig 以下のファイル

共有ディレクトリ/data/imcf/profiles 以下のファイルおよびディレクトリ

(2) インテリジェント統合管理データベースの削除

インテリジェント統合管理データベースを使用している場合、jimgnadbunsetup コマンドを実行して、論理ホストのインテリジェント統合管理データベース（トレンドデータ管理 DB）を削除します。

jimgnadbunsetup コマンドの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「jimgnadbunsetup」(1. コマンド)を参照してください。

また、論理ホスト全体の削除については、「[8.7.1\(3\) 論理ホストの削除](#)」を参照してください。

なお、クラスタソフトを利用して、インテリジェント統合管理データベースだけを削除する場合は、インテリジェント統合管理データベースが停止してもフェールオーバーが発生しないように、クラスタソフトの設定を見直してください。

(3) 論理ホストの削除

UNIX で論理ホストを削除する場合は、JP1/Base のjbsunsetcnf コマンドを使用します。次のコマンドを実行してください。

```
/opt/jp1base/bin/jbsunsetcnf -i -h 論理ホスト名
```

jbsunsetcnf コマンドの詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

これによって、論理ホストが削除されます。なお、論理ホストを削除すると、JP1/Base, JP1/IM - Manager, JP1/AJS, JP1/Power Monitor (06-02 以降) が一括して削除されます。

共有ディスク上の共有ファイル、共有ディレクトリは削除されません。手作業で削除してください。

(4) 論理ホストから JP1/IM - Manager および IM データベースだけを削除する手順

JP1/Base, JP1/IM - Manager, JP1/AJS, JP1/Power Monitor (06-02 以降) をインストールしている論理ホストから JP1/IM - Manager および IM データベースだけを削除する手順を次に示します。

1. 停止前に、接続中の JP1/IM - View はログアウトして切断する。
2. JP1/IM - Manager, JP1/Base を順にクラスタソフトの操作で停止する
3. IM データベースを使用している場合は、[\[8.7.1\(1\) IM データベースの削除\]](#) の手順で IM データベースを削除する。
4. 実行系/待機系のマシンで次のコマンドを実行して共通定義を削除する。
 - [論理ホスト名¥JP1CONSOLEMANAGER¥]キー
/opt/jp1base/bin/jbsunsetcnf -h 論理ホスト名 -c JP1CONSOLEMANAGER
 - [論理ホスト名¥JP1SCOPE¥]キー
/opt/jp1base/bin/jbsunsetcnf -h 論理ホスト名 -c JP1SCOPE
 - [論理ホスト名¥JP1CONFIG¥]キー
/opt/jp1base/bin/jbsunsetcnf -h 論理ホスト名 -c JP1CONFIG
5. JP1/IM - Manager の共有ファイル、共有ディレクトリを削除する。
6. クラスタソフトで、起動スクリプト (jco_start.cluster) を実行しないように設定を確認する。

8.7.2 JP1/IM - Manager および JP1/Base のアンインストール (UNIX の場合)

実行系サーバ、待機系サーバそれぞれのローカルディスク上の JP1/IM - Manager および JP1/Base をアンインストールしてください。

なお、JP1/IM - Manager をアンインストールすると、JP1/IM - Agent を利用するための統合エージェント管理基盤もアンインストールされます。

1. JP1/IM - Manager をアンインストールする。
2. JP1/Base をアンインストールする。

8.7.3 JP1/IM - Agent のアンインストール (UNIX の場合)

実行系サーバ、待機系サーバそれぞれのローカルディスク上の JP1/IM - Agent をアンインストールしてください。

1. 論理ホストで稼働している JP1/IM - Agent のサービスを停止する。

クラスタソフトから論理ホストで稼働しているサービスを停止します。

2. 複数マネージャホストへのデータ配信機能を使用している場合は、サービス停止後に次の手順を実施する。

「8.3.7(2)(b) 複数マネージャホストへのデータ配信機能を解除する (Linux の場合) (オプション)」に記載している「論理ホストのアンインストールを行う場合」を実施します。

3. クラスタソフトに登録されたサービスを解除する。

サービスを解除する方法については、クラスタソフトのドキュメントを確認してください。

4. systemd に登録されたサービスを解除するために有効化する。

論理ホストで使用するサービスについて、稼働系と待機系の両方で論理ホスト用のサービスを systemd から解除するために有効化します。

論理ホストのサービスの有効化には、次のコマンドを使用します。

```
/opt/jp1ima/tools/jpc_service -on サービスキー -h 論理ホスト名
```

Alertmanager のサービスを有効化する場合の例を次に示します。

```
/opt/jp1ima/tools/jpc_service -on jpc_alertmanager -h 論理ホスト名
```

5. 論理ホスト用のユニット定義ファイルを削除します。

/usr/lib/systemd/system 下にあるユニット定義ファイルを削除します。

削除するファイル名: jpc_サービス名_論理ホスト名.service

Alertmanager の場合の例を以下に示します。

削除するファイル名
jpc_alertmanager_論理ホスト名.service

6. systemd を更新する。

次のコマンドを実行して systemd を更新します。

```
# systemctl daemon-reload
```

7. 共有ディレクトリを削除する。

8.8 設定変更時の作業 (UNIX の場合)

クラスタシステムでの運用開始後に実行系サーバの設定を変更した場合には、その内容を待機系サーバにも反映して同期をとる必要があります。同期をとらないと、フェールオーバーしたときに実行系サーバの動作と待機系サーバの動作が変わってしまうことがあります。

次に示す場合には、実行系サーバおよび待機系サーバの両サーバでの設定変更をしてください。

8.8.1 ファイルでの設定変更 (UNIX の場合)

次のファイルを編集し、`jbssetcnf` コマンドで設定を有効にした場合には、実行系サーバから待機系サーバに共通定義情報をコピーする必要があります。

- 自動アクション環境定義ファイル (`action.conf.update`)
- 通信環境定義ファイル (`console.conf.update`)
- 状態変更イベント件数の上限監視設定ファイル (`evhist_warn_event_XXX.conf`)
- 対処済み連動設定ファイル (`action_complete_XXX.conf`)
- 状態変更イベント自動削除設定ファイル
- 監視オブジェクト初期化設定ファイル
- 監視オブジェクト DB の自動バックアップ・リカバリー設定ファイル (`auto_dbbackup_XXX.conf`)
- 相関イベント発行環境定義ファイル
- 状態変更条件メモリ常駐機能の設定ファイル
- IM 構成反映方式設定ファイル (`jp1cf_applyconfig.conf`)
- リモートログトラップ環境定義ファイル (`jp1cf_remote_logtrap.conf`)
- 表示メッセージ変更後イベント環境定義ファイル (`chmsgevent.conf`)
- イベントレポート出力環境定義ファイル (`evtreport.conf`)
- 操作ログ定義ファイル (`imm_operationlog.conf`)
- プロファイル管理環境定義ファイル (`jp1cf_profile_manager.conf`)

セットアップ手順の「[8.3.4 JP1/IM - Manager の新規インストール時の共通定義情報のコピー \(UNIX の場合\)](#)」で説明した手順で、共通定義情報をコピーするようにしてください。

なお、共通定義情報には JP1/Base, JP1/IM - Manager, JP1/AJS, および JP1/Power Monitor (06-02 以降) の設定情報が格納されています。論理ホストにこれらの製品がセットアップされている場合は、設定情報が一緒にコピーされます。

8.8.2 コマンドでの設定変更 (UNIX の場合)

jcochafmode コマンド、jcochcefmode コマンド、およびjcocmddef コマンドを実行して、設定を変更した場合には、実行系サーバおよび待機系サーバの両サーバで同様の設定をする必要があります。

- jcochafmode コマンドを実行した場合
 - h オプションを指定して、イベント取得フィルターの位置を変更した場合には、実行系サーバから待機系サーバに共通定義情報をコピーする必要があります。
 - セットアップ手順の「[8.3.4 JP1/IM - Manager の新規インストール時の共通定義情報のコピー \(UNIX の場合\)](#)」で説明した手順で、共通定義情報をコピーするようにしてください。
- jcochcefmode コマンドを実行した場合
 - h オプションを指定して、共通除外条件の動作モードを変更した場合には、実行系サーバから待機系サーバに共通定義情報をコピーする必要があります。
 - セットアップ手順の「[8.3.4 JP1/IM - Manager の新規インストール時の共通定義情報のコピー \(UNIX の場合\)](#)」で説明した手順で、共通定義情報をコピーするようにしてください。
- jcocmddef コマンドを実行した場合
 - host オプションを指定して、実行系サーバの設定を変更した場合には、待機系サーバでも同様の設定をしてください。なお、jcocmddef コマンドは共有ディスクがマウントされていなくても実行できます。

8.8.3 クラスタ環境での IM データベースの更新 (UNIX の場合)

クラスタ環境で JP1/IM - Manager をバージョンアップまたは JP1/IM - Manager の修正版を適用した場合に IM データベースを使用しているときは、クラスタ環境の IM データベースの更新処理が必要になります。次に示す手順に従い、IM データベースを更新してください。

ここでは、論理ホストの JP1/IM - Manager が動作しているホストを実行系ホストとし、動作していないホストを待機系ホストとします。

1. サービスの状態を確認する。

次の状態と異なる場合は、サービスを停止してください。

- JP1/IM - MO を使用している場合は、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスが停止している。
- JP1/OA で JP1/IM - Manager から JP1 イベントを取得している場合は、接続元の JP1/OA が停止している。

2. 実行系ホストで、クラスタソフトの操作で論理ホストの JP1/IM - Manager を停止する。

3. 実行系ホストに割り当てられた共有ディスクおよび論理 IP アドレスを待機系ホストに引き継ぎ、論理ホストで共有ディスクおよび論理 IP アドレスを使用できる状態にする。

4. 待機系ホストで/opt/jplimm/bin/imdbにあるjimdbstart コマンドを実行し、IM データベースを起動する。

```
jimdbstart -h 論理ホスト
```

5. 待機系ホストでjimdbstatus コマンドを実行し、IM データベースサービスが稼働中であることを確認する。

- IM データベースサービスが稼働中の場合、KNAN11182-I メッセージが出力されます。

KNAN11182-I IM データベースサービスは稼働中です

- IM データベースサービスが稼働中でない場合は、10 秒ごと程度でjimdbstatus コマンドを実行し、稼働中になるまで待ちます。

```
jimdbstatus -h 論理ホスト名
```

6. 待機系ホストでjimdbstop コマンドを実行し、IM データベースを停止する。

```
jimdbstop -h 論理ホスト名
```

7. 待機系ホストに割り当てられた共有ディスクおよび論理 IP アドレスを実行系ホストに引き継ぎ、論理ホストで共有ディスクおよび論理 IP アドレスを使用できる状態にする。

8. 待機系ホストでjimdbupdate コマンドを実行する。

```
jimdbupdate -h 論理ホスト名
```

- 次のメッセージが出力された場合は、手順 10 以降を実行してください。

KNAN11201-I IM データベースサービスは最新の状態です

- 次のどれかのメッセージが出力された場合は、手順 9 以降の手順を実行してください。

KNAN11202-I IM データベースサービスの上書きインストールが必要です

KNAN11211-I IM データベースサービスの設定ファイルの更新が必要です

なお、待機系ホストでは次のメッセージが出力されますが、問題はありません。

KNAN11210-W 共有ディスクにアクセスできないため、テーブルスキーマを確認できませんでした

9. 待機系ホストでjimdbupdate コマンドを実行し、IM データベースを更新する。

```
jimdbupdate -h 論理ホスト名 -i
```

なお、待機系ホストでは次のメッセージが出力されますが、問題はありません。

KNAN11210-W 共有ディスクにアクセスできないため、テーブルスキーマを確認できませんでした

10. 実行系ホストでjimdbupdate コマンドを実行する。

```
jimdbupdate -h 論理ホスト名
```

- 次のメッセージが出力された場合は、手順 13 を実行してください。

KNAN11201-I IM データベースサービスは最新の状態です

- 次のどれかのメッセージが出力された場合は、手順 11 以降を実行してください。

KNAN11202-I IM データベースサービスの上書きインストールが必要です

KNAN11207-I IM データベースサービスのテーブルスキーマの更新が必要です

KNAN11211-I IM データベースサービスの設定ファイルの更新が必要です

11. 実行系ホストでjimdbbackup コマンドを実行し、IM データベースをバックアップする。

```
jimdbbackup -h 論理ホスト名 -o バックアップファイル名 -m MAINT
```

12. 実行系ホストでjimdbupdate コマンドを実行し、IM データベースを更新する。

```
jimdbupdate -h 論理ホスト名 -i
```

13. 実行系ホストでクラスタソフトの操作で論理ホストの JP1/IM - Manager を起動する。

14. 手順 1 で停止したサービスを開始する。

❗ 重要

jimdbupdate コマンドを実行する前に取得した IM データベースの更新前のバックアップデータは、jimdbupdate コマンド実行後の IM データベースにリカバリーしないでください。

jimdbupdate コマンドを実行したあとは、再度jimdbbackup コマンドでバックアップを取得してください。

8.9 クラスタ運用時の注意事項 (UNIX の場合)

- クラスタシステムで多重起動を行う場合、多重起動する論理ホストの数だけ、システムのリソースが必要となります。
- クラスタシステムで JP1/IM - Manager の設定を行う場合は、物理ホストで動作している JP1/IM - Manager を必ず停止してください。物理ホストの JP1/IM - Manager を停止しないまま、クラスタシステムの設定を行った場合、論理ホストのサービスが正常に動作しなくなります。サーバを再起動して、回復してください。
- クラスタシステムで起動する場合、論理ホストで使用する認証サーバを必ず設定してから JP1/IM - Manager を起動してください。認証サーバの設定方法については、マニュアル「JP1/Base 運用ガイド」を参照してください。また、JP1/IM - Manager を起動する際は、設定した認証サーバが起動していることを確認してから、JP1/IM - Manager を起動してください。
- 論理ホストの認証サーバの設定およびユーザー登録を行う場合、必ず実行系のホストで操作をしてください。また、ユーザー登録を行う場合は、必ず論理ホストのサービスを起動してから行ってください。
- ログイン中に系切り替えで認証サーバが切り替わった場合、JP1/IM - Manager では、通信障害が発生し、系切り替え後に回復します。

JP1/IM - Manager の動作に問題がある場合は、認証サーバをクラスタシステム以外の場所に設置しておくことで、回避できます。

- 実行系の定義を退避するときに `jbsgetcnf` コマンドに指定する論理ホスト名には、論理ホストを定義したときに指定した名称と、大文字・小文字が同じになるように指定してください。
誤って異なる指定を行った場合は、論理ホストを削除してから再度設定を行ってください。
- IM 構成管理を使用していない場合、クラスタシステムで構成定義情報を配布する場合は、構成定義ファイルを次の名称で作成してください。

共有ディレクトリ/`jp1base/conf/route/jbs_route.conf`

- JP1/IM - Manager の起動中に、クラスタソフトの機能などでホスト名を変更しないでください。
ホスト名を変更した場合は、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「2.2.4 クラスタシステムで論理ホスト名を変更する場合の作業」を参照し、必要な作業を行ってください。
- クラスタシステムで論理ホストを作成する場合、またはバインド方式を変える場合は、物理ホストで動作している JP1/IM - Manager のデーモンを必ず停止してください。物理ホストのデーモンを停止せずに、論理ホストの作成、またはバインド方式を変える設定を行った場合、論理ホストのデーモンが正常に動作しなくなります。この場合、サーバマシンのリブートを行って回復してください。
- 物理ホストで JP1/IM - Manager を使用しない場合、必ず自動起動・停止スクリプトの設定をはずしておいてください。
- クラスタ運用の待機系ホストで `"jbsrt_get -h 論理ホスト"` を実行すると、共有ディレクトリがオフラインのため、「KAVB3113-I 定義情報が存在しませんでした」メッセージを出力します。この場合、実行系ホストで、`"jbsrt_get -h 論理ホスト"` を実行してください。
- クラスタソフトの対応状況および注意事項につきましては、以下のページをご参照ください。

<http://www.hitachi.co.jp/Prod/comp/soft1/jp1/products/environments/cluster/index.html>

8.10 非クラスタシステムでの論理ホストの運用と環境構築（UNIX の場合）

フェールオーバーしない論理ホストの構築および運用についての概要を説明します。

JP1/IM - Manager の操作、バックアップやリカバリーなど、フェールオーバーしない論理ホストの運用方法は、クラスタシステムで運用する論理ホストと同じです。ただし、クラスタソフトと連動してフェールオーバーすることを除きます。

8.10.1 非クラスタシステムで論理ホストを運用する場合の構成の検討（UNIX の場合）

複数の論理ホストで JP1/IM - Manager を起動すると、それぞれの JP1/IM - Manager がシステムリソース（メモリー・ディスク・プロセス・セマフォなど）を使用します。同時に起動する JP1/IM - Manager の数に合わせて、リソース量も見積もってください。

または、システムの性能に合わせて、同時に起動する JP1/IM - Manager の数を調整してください。複数の JP1/IM - Manager を同時に実行してリソースが不足すると、システムが正常に動作しません。同時に起動する論理ホストの数は 2～3 を目安にしてください。

なお、メモリー所要量およびディスク占有量の見積もりについては、JP1/IM - Manager のリリースノートを参照してください。

8.10.2 非クラスタシステムで論理ホストを運用する場合の環境設定（UNIX の場合）

フェールオーバーしない論理ホスト環境で、JP1/IM - Manager を運用する手順を次に示します。

(1) 論理ホスト環境の準備

論理ホスト環境を作成するために、論理ホスト用のディスク領域および IP アドレスを用意してください。

- 論理ホスト用のディスク領域

物理ホストやほかの論理ホストの JP1 が使用しているものとは別に、論理ホストの JP1/IM - Manager が専用で使用するファイルの格納先ディレクトリを、ローカルディスクに作成してください。

- 論理ホスト用の IP アドレス

論理ホストの JP1/IM - Manager が使用する IP アドレスを、OS で割り当ててください。

IP アドレスの割り当ては、実 IP でもエイリアス IP でもかまいません。ただし、論理ホスト名から一意に特定できる IP アドレスにしてください。

これらに対する前提条件は、クラスタシステムでの運用の場合と同じです。ただし、フェールオーバーしない運用方法のため「サーバ間で引き継がれる」などの条件は除きます。

なお、「8. クラスタシステムでの運用と環境構築 (UNIX の場合)」で、共有ディスク・論理 IP アドレスと説明している部分は、上記で割り当てた論理ホスト用のディスク領域・IP アドレスに読み替えてください。

- 性能の見積もり

次のような観点でシステムとして動作できるか見積もってください。

- システム内で複数の JP1/IM - Manager が起動できるリソースを割り当てられるかどうかを見積もってください。リソースが十分に割り当てられないと、正しく動作しなかったり、十分な性能が確保できなかったりします。

(2) 論理ホスト環境の JP1 のセットアップ

クラスタシステムの実行系サーバと同じ手順で、論理ホスト環境の JP1 をセットアップしてください。なお、クラスタシステムではフェールオーバーする両側のサーバに対してセットアップする必要がありますが、フェールオーバーしない論理ホストでは、動作するサーバだけセットアップしてください。

(3) 論理ホスト環境の自動起動および自動停止の設定

論理ホスト環境の JP1 のセットアップ時に、自動起動および自動停止の設定はされません。論理ホスト環境の自動起動および自動停止をする場合は、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「3.3 非クラスタシステムの論理ホスト運用での自動起動および自動停止の設定例」を参照してください。

8.10.3 非クラスタシステムで論理ホストを運用する場合の注意事項 (UNIX の場合)

(1) 論理ホストの JP1 に対する操作

論理ホストに作成した JP1 に対してコマンドを実行する場合は、クラスタシステムで動作する論理ホストと同様に論理ホスト名を明示して実行してください。

(2) 論理ホストの引き継ぎ

非クラスタシステム環境の論理ホストでは共有ディスク上の管理情報が引き継がれないため、フェールオーバーに対応していません。複数のホストで論理ホスト IP を引き継ぐ運用はしないでください。

9

ネットワーク構成に応じた運用と環境構築

この章では、ネットワーク構成に応じた運用と環境構築について説明します。

JP1/IM - Manager のホストが複数のネットワークに接続された構成や、ファイアウォールを経由した構成などの場合は、ネットワークの構成に応じた JP1/IM - Manager および JP1/Base の設定や運用検討が必要です。

9.1 JP1/Base による通信の制御

JP1/IM - Manager は、前提製品である JP1/Base の通信設定に依存して動作します。

例えば、複数 LAN（複数のネットワークに接続された構成）での通信の設定や、クラスタシステムで運用する場合の IP バインド方式などの通信方式は、JP1/Base の通信制御の機能を使って動作しています。

通信方式および設定内容については、マニュアル「JP1/Base 運用ガイド」の次の説明を参照してください。

- 「JP1/Base の機能詳細」の章の JP1/Base の通信方式
- 「ネットワーク構成に応じた JP1/Base の通信設定」の章

9.2 複数ネットワークでの運用

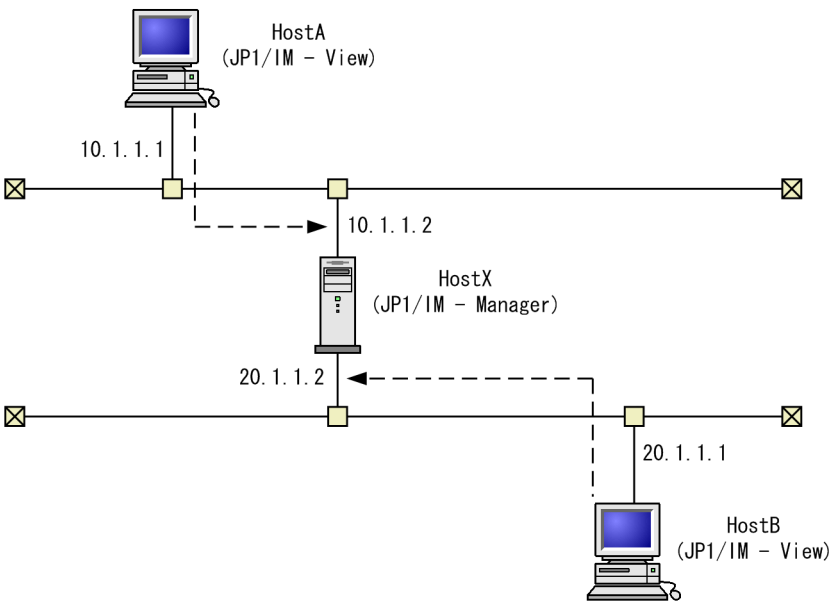
ここでは、複数 LAN（複数のネットワークに接続された構成）でのシステム構成例とその構成例を基に必要な通信設定について説明します。

なお、複数 LAN に関する設定は、JP1/Base と共通です。JP1/Base で設定すると、その設定にあわせて JP1/IM - Manager が動作します。

9.2.1 構成例 1（クラスタ運用なし、JP1/IM - View 接続）

クラスタ運用していない状態で、マネージャーが互いにルーティングできない二つの LAN に接続されており、それぞれの LAN から JP1/IM - View を接続する場合の例を次に示します。

図 9-1 複数 LAN 環境での JP1/IM - View 接続（クラスタ運用なし）



この場合の各ホストの設定を次の表に示します。

表 9-1 HostX の設定（JP1/IM - Manager）

ホスト名	バインド方式※	jp1host 設定※
HostX	送信 ANY, 受信 ANY	—
	送信 ANY, 受信 IP	10.1.1.2, 20.1.1.2

（凡例）

—：設定不要

注※ どちらの設定でも接続できます。

JP1/Base の通信設定を変更しなくても問題なく動作します（クラスタ運用しない場合、送受信ともに ANY バインド方式で動作します）。

表 9-2 HostA, HostB の設定 (JP1/IM - View)

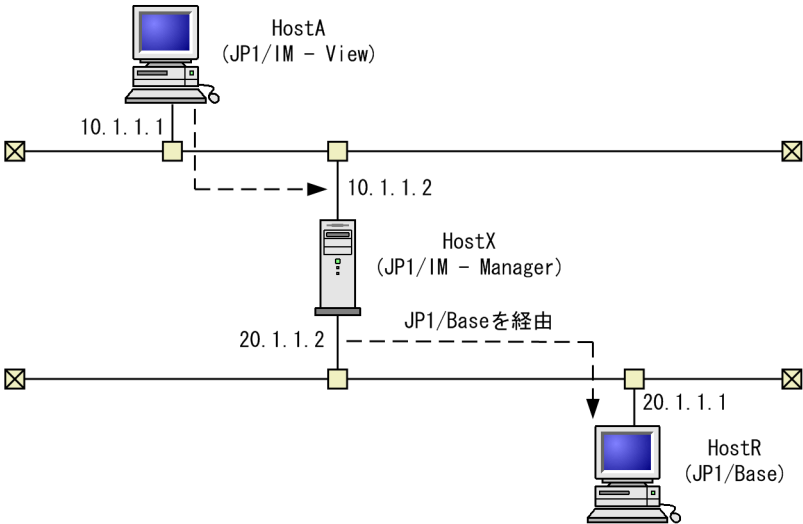
ホスト名	接続ホスト	その他条件※
HostA	HostX	ホスト名 HostX→10.1.1.2 の変換ができること
HostB	HostX	ホスト名 HostX→20.1.1.2 の変換ができること

注※ JP1/IM - View はjp1hosts ファイルおよびjp1hosts2 ファイルの設定を参照しないため、ホスト名の名前解決はhosts ファイルや DNS で設定してください。

9.2.2 構成例 2 (クラスタ運用なし, コマンド実行)

クラスタ運用していない状態で、マネージャーが互いにルーティングできない二つの LAN に接続されており、一方の LAN から JP1/IM - View でマネージャーに接続し、もう一方にあるホスト上でコマンドを実行する場合の例を次に示します。

図 9-2 複数 LAN 環境でのコマンド実行 (クラスタ運用なし)



この場合の各ホストの設定を次の表に示します。

表 9-3 HostX の設定 (JP1/IM - Manager)

ホスト名	バインド方式※	jp1host 設定※
HostX	送信 ANY, 受信 ANY	—
	送信 ANY, 受信 IP	10.1.1.2, 20.1.1.2

(凡例)

—：設定不要

注※ どちらの設定でも接続できます。

JP1/Base の通信設定を変更しなくても問題なく動作します (クラスタ運用しない場合、送受信ともに ANY バインド方式で動作します)。

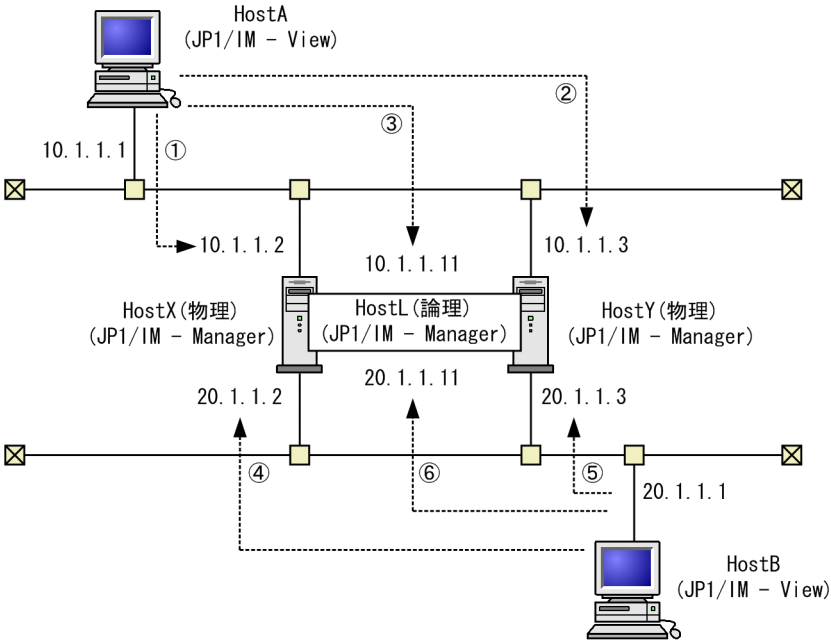
表 9-4 HostA の設定 (JP1/IM - View)

ホスト名	接続ホスト	その他条件
HostA	HostX	ホスト名 HostX→10.1.1.2 の変換ができること

9.2.3 構成例 3 (クラスタ運用, JP1/IM - View 接続)

マネージャーが互いにルーティングできない二つの LAN に接続され、クラスタ運用されているとき、それぞれの LAN から JP1/IM - View を接続する場合の例を示します。

図 9-3 複数 LAN 環境での JP1/IM - View 接続 (クラスタ運用)



この場合の各ホストの設定を次の表に示します。

表 9-5 HostX, HostY, HostL の設定 (JP1/IM - Manager)

ホスト名	バインド方式	jp1host 設定
HostX(物理ホスト)	送信 ANY, 受信 IP	10.1.1.2, 20.1.1.2
HostY(物理ホスト)	送信 ANY, 受信 IP	10.1.1.3, 20.1.1.3
HostL(論理ホスト)	送信 ANY, 受信 IP	10.1.1.11, 20.1.1.11

なお、JP1/Base の通信設定が必要になります。設定の詳細については、マニュアル「JP1/Base 運用ガイド」のネットワーク構成に応じた JP1/Base の通信設定の章を参照してください。

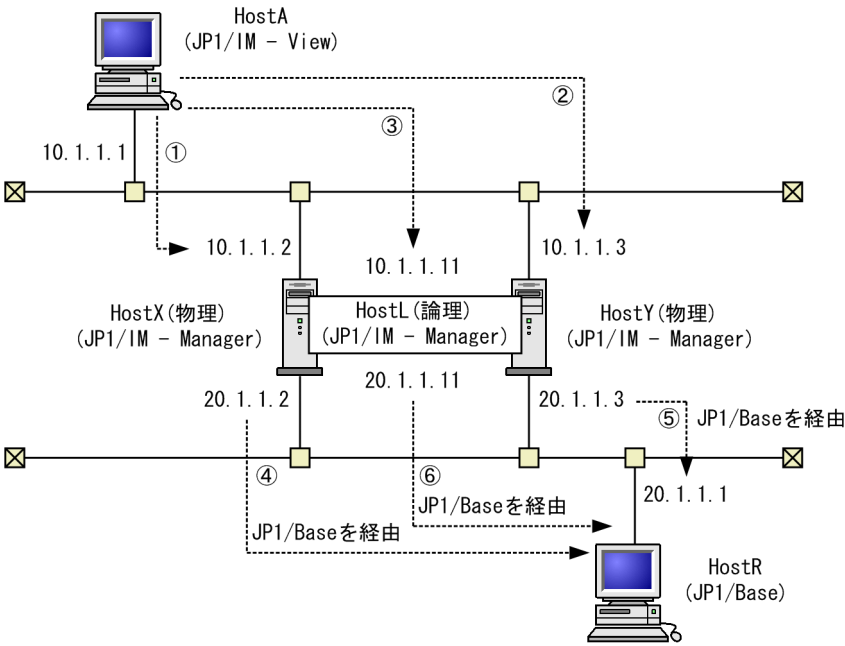
表 9-6 HostA の設定 (JP1/IM - View)

ホスト名	接続 ホスト	その他条件	図中の丸付き 数字との対応
HostA	HostX	ホスト名 HostX→10.1.1.2 の変換ができること	1
	HostY	ホスト名 HostY→10.1.1.3 の変換ができること	2
	HostL	ホスト名 HostL→10.1.1.11 の変換ができること	3
HostB	HostX	ホスト名 HostX→20.1.1.1 の変換ができること	4
	HostY	ホスト名 HostY→20.1.1.2 の変換ができること	5
	HostL	ホスト名 HostL→20.1.1.11 の変換ができること	6

9.2.4 構成例 4 (クラスタ運用, コマンド実行)

マネージャーが互いにルーティングできない二つの LAN に接続され、クラスタ運用されているとき、一方の LAN から JP1/IM - View でマネージャーに接続し、もう一方にあるホスト上でコマンドを実行する場合の例を次に示します。

図 9-4 複数 LAN 環境でのコマンド実行 (クラスタ運用)



この場合の各ホストの設定を次の表に示します。

表 9-7 HostX, HostY, HostL の設定 (JP1/IM - Manager)

ホスト名	バインド方式	jp1host 設定
HostX(物理ホスト)	送信 ANY, 受信 IP	10.1.1.2, 20.1.1.2

ホスト名	バインド方式	jp1host 設定
HostY(物理ホスト)	送信 ANY, 受信 IP	10.1.1.3, 20.1.1.3
HostL(論理ホスト)	送信 ANY, 受信 IP	10.1.1.11, 20.1.1.11

なお、JP1/Base の通信設定が必要になります。設定の詳細については、マニュアル「JP1/Base 運用ガイド」のネットワーク構成に応じた JP1/Base の通信設定の章を参照してください。

表 9-8 HostA の設定 (JP1/IM - View)

ホスト名	接続 ホスト	その他条件	図中の丸付き 数字との対応
HostA	HostX	ホスト名 HostX→10.1.1.2 の変換ができること	1, 4
	HostY	ホスト名 HostY→10.1.1.3 の変換ができること	2, 5
	HostL	ホスト名 HostL→10.1.1.11 の変換ができること	3, 6

9.3 ファイアウォール環境での運用

ここでは、ファイアウォールを含むネットワーク環境で JP1/IM を運用する場合について説明します。JP1/IM ではファイアウォールを介したシステム構成に対応しています。

9.3.1 ファイアウォールの基礎知識

ファイアウォール環境での運用について説明する前に、まず、ファイアウォールの基礎知識について説明します。

ファイアウォールを含むネットワーク環境で JP1 を運用する場合、ファイアウォールの機能のうち、次の二つについて対応を検討する必要があります。

- パケット・フィルタリング（アクセスの制限）
必要な通信だけを許可し、許可していない不正な通信を防ぐ。
- NAT（アドレスの変換）
IP アドレスを変換し、直接接続できない異なるアドレスのネットワークと接続する。また、IP アドレスを変換するマシンの存在を外部から隠す。

これらを検討し環境を設定するためには、ファイアウォールが通信を制御する方法を理解する必要があります。

❗ 重要

ここで説明する内容は、ファイアウォールの基礎を理解していただくための概要であり、実際にファイアウォールの検討や設定をするためには十分ではありません。実際にファイアウォールを設置する場合は、必ずファイアウォールのマニュアルやセキュリティの専門書を参照し十分に理解した上で、検討や環境設定をしてください。

(1) パケット・フィルタリング

パケット・フィルタリングは、ファイアウォール経由で利用できるアプリケーションを、特定のアプリケーションだけに制限するための機能です。ファイアウォールを通過する通信パケットを一つずつ確認し、あらかじめ指定した通過条件に一致しないパケットを破棄することで、不正な通信がファイアウォールを通過することを防ぎます。これによって、通過条件に指定されたアプリケーションだけがファイアウォール経由で使用できます。

JP1/IM は、パケット・フィルタリングに対応しています。

(a) パケット・フィルタリングを設定するには

パケット・フィルタリングを設定するには、次の作業が必要です。

1. アプリケーションが使用するポート番号など通信の方式を調べる。

ファイアウォールの通過条件として設定するポート番号や IP アドレスおよび通過方向を確認します。
JP1/IM の場合、この章の説明とマニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 C ポート番号」の説明を参照して、通信方式を確認してください。

2. ファイアウォールに通過条件を設定する。

まず、すべての通過を禁止してから、特定のアプリケーションの通信だけがファイアウォールを通過できるように通過条件を設定します。

JP1/IM の場合、先の手順で確認した JP1/IM の通信がファイアウォールを通過できるように設定してください。

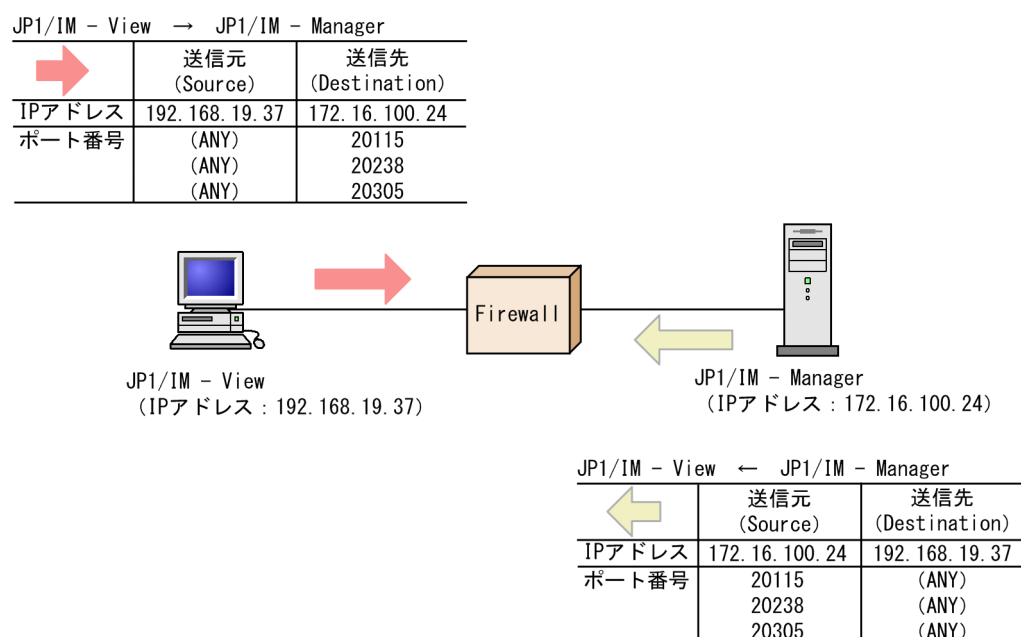
(b) JP1/IM の場合の設定例

ここでは、JP1/IM - View と JP1/IM - Manager の間にファイアウォールがある環境を例に、パケット・フィルタリングの設定について説明します。

例：JP1/IM - View をファイアウォール経由で JP1/IM - Manager に接続します。

- JP1/IM - View のマシンの IP アドレスは 192.168.19.37 とする。
- JP1/IM - Manager のマシンの IP アドレスは 172.16.100.24 とする。
- ポート番号は、JP1 の標準のポート番号を使う。

図 9-5 パケット・フィルタリングの設定例



1. JP1 の通信の方法を調べる。

まず、パケット・フィルタリング設定に必要な情報である、JP1 の通信の方法を調べます。マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 C.2 ファイアウォールの

通過方向」の説明を参照すると、JP1/IM が使用するポート番号について次のような表で説明されています。

表 9-9 ファイアウォールの通過方向

サービス名	ポート番号	ファイアウォールの通過方向
jplimevtcon	20115/tcp	JP1/IM - View → JP1/IM - Manager (セントラルコンソール)
jplimcmda	20238/tcp	JP1/IM - View → JP1/Base ^{※1} JP1/IM - Manager (セントラルコンソール) → JP1/Base ^{※1}
jplimcss	20305/tcp	JP1/IM - View → JP1/IM - Manager (セントラルスコープ)
jplimegs	20383/tcp	JP1/IM - Manager がインストールされたマシン内だけの通信となるため、ファイアウォールの設定は不要
jddmain	20703/tcp	WWW ブラウザー → JP1/IM - Manager (インテリジェント統合管理基盤)
なし ^{※2}	IM データベースのポート番号 ^{※3}	JP1/IM - Manager (物理ホスト) → JP1/IM - Manager (IM データベース (物理ホスト))
	IM データベースのポート*番号 ^{※4}	JP1/IM - Manager (論理ホスト) → JP1/IM - Manager (IM データベース (論理ホスト))
jplimcf	20702/tcp	JP1/IM - View → JP1/IM - Manager (IM 構成管理)
jplimfcs	20701/tcp	JP1/IM - Manager がインストールされたマシン内だけの通信となるため、ファイアウォールの設定は不要
jimmail	25/tcp ^{※2}	JP1/IM - Manager → メールサーバ (SMTP) (認証なしの場合)
	587/tcp ^{※2}	JP1/IM - Manager → メールサーバ (SMTP) (SMTP-AUTH 認証の場合)
	110/tcp ^{※2}	JP1/IM - Manager → メールサーバ (POP3) (POP before SMTP 認証の場合)

(凡例)

→ : コネクション確立時の接続方向を示す

注※1 マネージャーの JP1/Base が対象です。

注※2 services ファイルには登録しません。

注※3 物理ホストの IM データベースのセットアップ時にセットアップ情報ファイルで設定した IM データベース (物理ホスト) のポート番号です。

注※4 論理ホストの IM データベースのセットアップ時にクラスタセットアップ情報ファイルで設定した IM データベース (論理ホスト) のポート番号です。

注※5 接続先ポート番号は、接続先サーバの使用するポートによって変わる場合があります。

注※6 HTTP サーバの設定によっては異なる場合があります。

この表は、次のような通信の方法を意味しています。

- サービス名とポート番号の欄

JP1 が通信で使用するサービス名とポート番号です。JP1/IM - View と JP1/IM - Manager の通信は、ポート番号 20115 (サービス名 jplimevtcon)、ポート番号 20238 (サービス名 jplimcmda)、

およびポート番号 20305（サービス名 jplimcss）を使い、通信のプロトコルは TCP であることがわかります。

- ファイアウォールの通過方向の欄

この欄は、接続開始時（コネクション確立時）の通信方向を意味しており、表中の矢印に接続します。接続開始時の方向は、ファイアウォール通過を許可する方向を制限したいときに必要な情報です。例えば、この表の項番 1 からは、JP1/IM - View から JP1/IM - Manager（セントラルコンソール）への方向で接続することがわかります。

- その他

表には直接書かれていませんが、表の情報と TCP の通信の仕様から考えると次のことがわかります。TCP は双方向の通信であるため、行き（JP1/IM - View→JP1/IM - Manager）と帰り（JP1/IM - View←JP1/IM - Manager）の通信があります。通信での行きと帰りのパケットでは、送信元 IP アドレス（Source IP アドレス）と送信先 IP アドレス（Destination IP アドレス）が入れ替わります。

2. パケット・フィルタリングを設定する。

確認した JP1/IM - View と JP1/IM - Manager の通信の方法を基に、この通信だけがファイアウォールを通過できるように設定します。

パケット・フィルタリングの通過条件は次のようになります。

（例）フィルタリング条件：JP1/IM - View と JP1/IM - Manager の場合

表 9-10 パケット・フィルタリングの通過条件

項番	送信元 IP アドレス	送信先 IP アドレス	プロトコル	送信元ポート	送信先ポート	制御
1	192.168.19.37	172.16.100.24	TCP	(ANY)	20115	accept
2	192.168.19.37	172.16.100.24	TCP	(ANY)	20238	accept
3	192.168.19.37	172.16.100.24	TCP	(ANY)	20305	accept
4	172.16.100.24	192.168.19.37	TCP	20115	(ANY)	accept
5	172.16.100.24	192.168.19.37	TCP	20238	(ANY)	accept
6	172.16.100.24	192.168.19.37	TCP	20305	(ANY)	accept
7	(ANY)	(ANY)	(ANY)	(ANY)	(ANY)	reject

この表は、パケットを確認する条件と条件に一致した場合の制御を示しています。

制御の列は、ファイアウォールがパケットの通過を許可（accept）するか、拒否（reject）するかの指定です。（ANY）は、OS によって割り当てられる任意の空きポート番号を使用するという意味です。この表のフィルタリング条件に合わせて、ファイアウォールのパケット・フィルタリングを設定します。なお、具体的な設定方法はファイアウォールによって異なります。ご使用のファイアウォールのマニュアルを参照してください。

(2) NAT (アドレス変換)

NAT (Network Address Translator: アドレス変換) は、プライベートな IP アドレスと、グローバルな IP アドレスとを相互に変換する機能です。アドレス変換をすることで、プライベート側のアドレスが外部から隠され、内部のマシンのセキュリティを高めることができます。なお、NAT は、ファイアウォールだけではなく、ルーターの機能として提供されている場合もあります。

JP1 は、スタティック・モード (あらかじめ決められたルールに従ってアドレスを変換する方法) の NAT にだけ対応しています。

(a) NAT を設定するには

NAT を設定するには、次の作業が必要です。

1. 使用する IP アドレスを確認する。

まず、アプリケーションが使用する IP アドレスを確認します。IP アドレスを一つしか使っていないマシンの場合は単純ですが、複数のネットワークアダプターがある (つまり複数の IP アドレスがある) 場合や、クラスタシステムで論理 IP アドレスを使う場合などは、アプリケーションによってどの IP アドレスを使用するかが異なります。

JP1/IM の場合、JP1/Base で通信の設定をしている場合や、クラスタ運用で論理 IP アドレスを使用する場合など、設定によって使用する IP アドレスが異なります。

2. アドレスの変換ルールを検討し設定する。

アプリケーションが使用する IP アドレスが確認できたら、変換後の IP アドレスを決めます。

アドレスの変換ルールが決まったら、NAT に設定します。

(b) JP1/IM の場合の設定例

ここでは、JP1/IM - View と JP1/IM - Manager の間にファイアウォールがある環境を例に、NAT の設定について説明します。

例: JP1/IM - View からアドレス変換した JP1/IM - Manager に接続します。

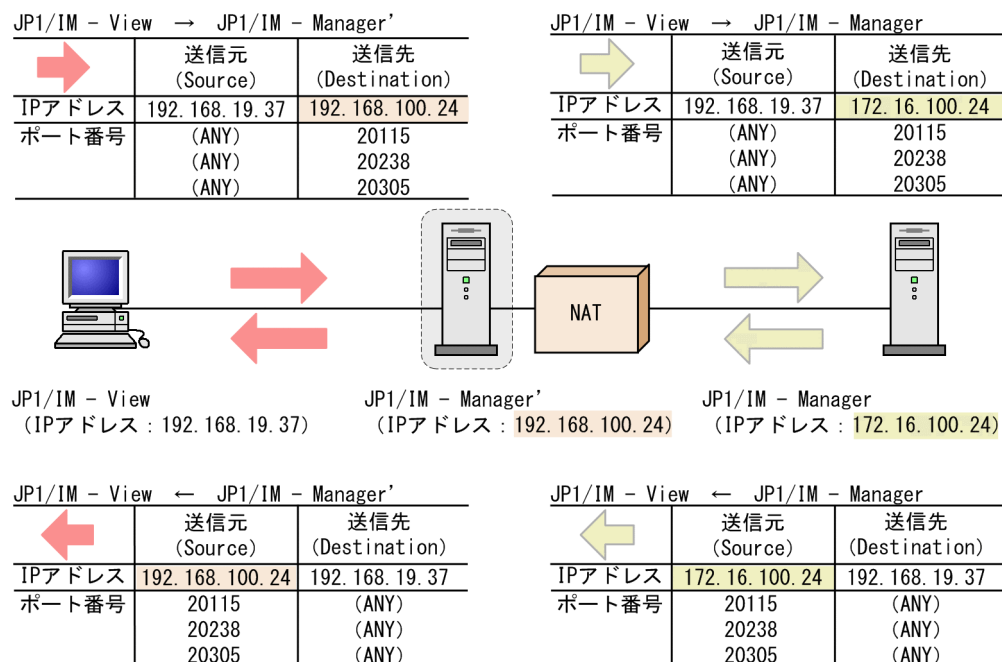
- JP1/IM - View のマシンの IP アドレスは 192.168.19.37 とする。

- JP1/IM - Manager のマシンの IP アドレスは 172.16.100.24 とする。

この JP1/IM - Manager の IP アドレスを、JP1/IM - Manager' の IP アドレス 192.168.100.24 に変換する。

JP1/IM - View からは変換後の 192.168.100.24 に接続する。

図 9-6 NAT の設定例



注意：これは NAT でのアドレス変換の例であり、ほかの変換方法の場合もあります。

1. 使用する IP アドレスを確認する。

まず、NAT の設定に必要な情報である、JP1 が使用する IP アドレスを調べます。

今回の例では、ホスト名 (hostname コマンドを実行したときに表示されるホスト名) に対応する IP アドレスを使って通信します。

2. アドレス変換ルールを検討し設定する。

JP1/IM - Manager のマシンの IP アドレスを NAT によって 172.16.100.24 から 192.168.100.24 へアドレス変換するよう変換ルールを決めます。

(例) アドレス変換ルール：172.16.100.24 を 192.168.100.24 に変換

表 9-11 アドレス変換ルール

項番	送信元 IP アドレス	送信先 IP アドレス	送信元 IP アドレス (アドレス変換後)	送信先 IP アドレス (アドレス変換後)
1	(ANY)	192.168.100.24	(ANY)	172.16.100.24
2	172.16.100.24	(ANY)	192.168.100.24	(ANY)

この表は、元のパケットと、アドレス変換したパケット (アドレス変換後) との対応を示しています。このアドレス変換ルールをファイアウォールの NAT 設定に定義します。

なお、具体的な設定方法はファイアウォールやルーターによって異なりますので、ご使用の製品のマニュアルを参照してください。

JP1/IM - View がアクセスするのは、実際の JP1/IM - Manager のマシンのアドレス (172.16.100.24) ではなく、アドレス変換したあとのアドレス (192.168.100.24) となります。

このため、JP1/IM - View からは、あたかもアドレス（192.168.100.24）のホスト JP1/IM - Manager' にアクセスしているように見えます。

(3) ファイアウォール環境での運用する JP1 の通信設定

ファイアウォールを経由するネットワーク環境で JP1 を運用する場合は、JP1 の通信方式を IP バインド方式に設定することと、複数 LAN 接続の設定による影響を考慮してください。

ファイアウォール環境で JP1 を運用するには、これまで説明したようにパケット・フィルタリングや NAT に、IP アドレスとポート番号による条件を設定する必要があります。

このため、JP1 が使用する IP アドレスを明確にする必要があり、JP1 の使用する IP アドレスが JP1 の設定によって決められる IP バインド方式が適しています。

例えば、JP1 を実行するサーバが、複数の LAN に接続されている構成やクラスタシステム構成では、使用する IP アドレスが OS によって決められる場合があります、意図しない IP アドレスが使われることがあります。この場合は、JP1 の通信方式を IP バインド方式に設定し、JP1 の環境設定で指定した IP アドレスを使って通信することで対処できます。

9.3.2 JP1/IM の通信

JP1/IM の通信について、ポート番号、IP アドレス、アドレス変換(NAT)の対応を説明します。

なお、JP1/IM の機能には、前提製品 JP1/Base の機能を使用しているため、JP1/IM と JP1/Base の通信をまとめて説明します。

(1) ポート番号

(a) ポート番号

JP1/IM および JP1/Base が使用するポート番号と、ファイアウォールの通過方向（コネクション確立の方向）は、次の説明を参照してください。

- JP1/Base のポート番号：マニュアル「JP1/Base 運用ガイド」のポート番号の説明
- JP1/IM のポート番号：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 C ポート番号」

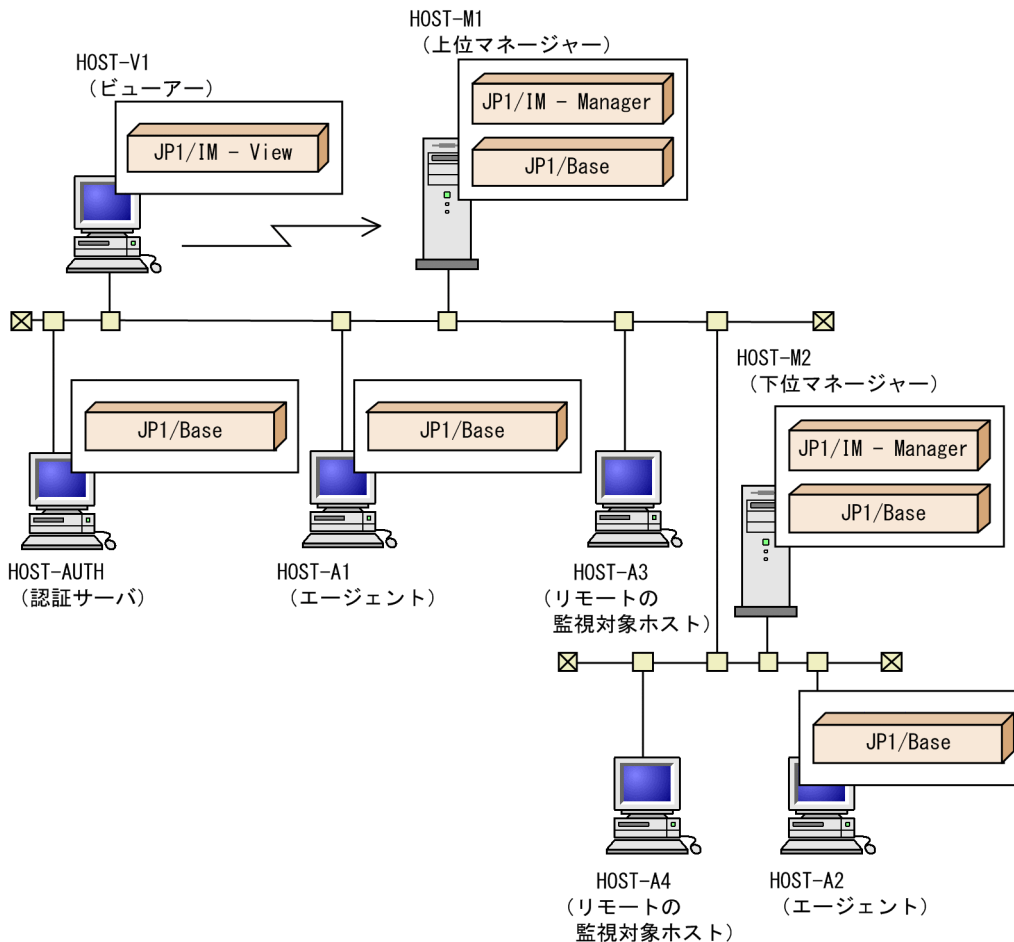
(b) システム構成例と通信

システム構成の例によって、使用するポート番号とファイアウォール通過方向（コネクション確立の方向）を説明します。

重要

ファイアウォールのホストで JP1 を使用する場合、自ホスト内の通信については、JP1 が使うすべてのポートを通過できるように設定してください。これは、JP1 のプロセス同士の通信にポートを使用するためです。

図 9-7 システム構成 (例)



1. HOST-M1 に、HOST-V1 の JP1/IM - View で接続する。
2. HOST-M1 の下位に HOST-M2 を設置する。
3. HOST-M1 の下に HOST-A1、HOST-M2 の下に HOST-A2 をエージェントとして設置する。
4. HOST-M1 の下に HOST-A3、HOST-M2 の下に HOST-A4 をリモートの監視対象ホストとして設置する。
5. HOST-M1 の認証サーバを、HOST-AUTH に設定する。

- 認証サーバと、マネージャーおよびエージェントの通信

マネージャーまたはエージェント (JP1/Base)	通過方向	認証サーバ (JP1/Base)
(ANY)	→	20240/tcp (jp1bsuser)

この表はシステム構成例の、各ホストと HOST-AUTH の通信に相当します。

- マネージャーとリモートの監視対象ホストの通信

マネージャー (JP1/IM)	通過方向	リモートの監視対象ホスト
(ANY)	→	135/tcp (WMI) 445/tcp (WMI) 1024 以上の動的ポート/tcp (WMI) 137/udp (NetBIOS) 138/udp (NetBIOS) 139/tcp (NetBIOS) 22/tcp (SSH) ※

注※ SSH サーバの設定によっては異なる場合があります。

- ビューアーとマネージャーの通信

JP1/IM - View	通過方向	マネージャー (JP1/IM および JP1/Base)
(ANY)	→	20115/tcp (jplimevtcon) 20238/tcp (jplimcmda) 20305/tcp (jplimcss) ※ ¹ 20702/tcp (jplimcf) ※ ²

注※¹ jplimcss のポートは、JP1/IM - Manager (セントラルスコープ) を使用する場合だけ使用します。

注※² jplimcf のポートは、JP1/IM - Manager (IM 構成管理) を使用する場合だけ使用します。

統合オペレーション・ビューアー	通過方向	マネージャー (JP1/IM および JP1/Base)
(ANY)	→	20703/tcp (jddmain) ※

注※ jddmain のポートは、JP1/IM - Manager (インテリジェント統合管理基盤) を使用する場合だけ使用します。

この表はシステム構成例の、HOST-V1 と HOST-M1 の通信に相当します。

- JP1/IM - View とエージェントの通信

JP1/IM - View とエージェント (JP1/Base) の通信はありません。

- 上位マネージャーと下位マネージャーの通信

上位マネージャー (JP1/IM および JP1/Base)	通過方向	下位マネージャー (JP1/IM および JP1/Base)
(ANY)	→	20099/tcp (jplimevtapi) 20237/tcp (jplimrt) 20239/tcp (jplimcmdc) 20306/tcp (jplbsplugin) 20600/tcp (jplbscom) 20702/tcp (jplimcf) ※

上位マネージャー (JP1/IM および JP1/Base)	通過方向	下位マネージャー (JP1/IM および JP1/Base)
20098/tcp (jplimevt) 20239/tcp (jplimcmdc)	←	(ANY)
20600/tcp (jplbscom)	←	(ANY)

注※ jplimcf のポートは、JP1/IM - Manager (IM 構成管理) を使用する場合だけ使用します。

この表はシステム構成例の、HOST-M1 と HOST-M2 の通信に相当します。

なお、イベント転送は下位から上位だけ、コマンド実行は上位から下位だけであることを前提にしています。

- マネージャーとエージェントの通信

マネージャー (JP1/Base)	通過方向	エージェント (JP1/Base)
(ANY)	→	20099/tcp (jplimevtapi) 20237/tcp (jplimrt) 20239/tcp (jplimcmdc) 20306/tcp (jplbsplugin) 20600/tcp (jplbscom)
20098/tcp (jplimevt) 20239/tcp (jplimcmdc)	←	(ANY)
20600/tcp (jplbscom)	←	(ANY)

この表はシステム構成例の、HOST-M1 と HOST-A1 や HOST-A2、および HOST-M2 と HOST-A2 の通信に相当します。

- マネージャー (インテリジェント統合管理基盤) と連携製品ホストの通信

マネージャー (JP1/IM)	通過方向	連携製品ホスト (JP1/Base, JP1/AJS, JP1/PFM およびその 他の連携製品※2)
(ANY)	→	20306/tcp (jplbsplugin) 20358/tcp (PFM - Web Console※1)

注※1 JP1/PFM - Manager と連携する場合に使用します。

注※2 その他の連携製品ホストと連携するためのポート番号の設定については、各連携製品のマニュアルの JP1/IM との連携方法について書かれた個所を参照してください。その際、JP1/PFM は、バージョン 12-10 以降のマニュアルを参照してください。

JP1/SES イベントを使用する場合

なお、JP1/SES 形式の JP1 イベントを扱う場合は、これまでの説明に加えて、次の設定が必要です。

- サービス名 JP1AutoJob (Windows の場合) または jesrd (UNIX の場合) で任意のポート番号を定義する。
- 定義したポート番号で、JP1/SES イベントを扱う製品と JP1/Base の間が、双方向で通過できるように、ファイアウォールに設定する。

詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

(2) IP アドレス

JP1/IM および JP1/Base が使う IP アドレスについて説明します。

IP アドレスは、JP1/IM - View と JP1/IM - Manager との間では IPv4 アドレス形式のアドレスを使用できます。JP1/Base と JP1/IM - Manager との間では、IPv4 アドレス形式または IPv6 アドレス形式のアドレスを使用できます。

IP アドレスでフィルタリングする場合や、アドレス変換(NAT)をする場合は、ここで説明する IP アドレスを指定してください。

なお、JP1/IM は、前提製品 JP1/Base の機能を使って通信方式を制御しています。

設定の詳細については、マニュアル「JP1/Base 運用ガイド」のネットワーク構成に応じた JP1/Base の通信設定の章を参照してください。

(a) 通常のシステムの場合

クラスタではない通常のシステムで、論理ホストのセットアップをしていない場合に使用する IP アドレスを説明します。

- 受信側 IP アドレス (受信側が ANY バインドの場合)

JP1 のサービスが接続を受け付ける IP アドレスです。

ホスト名 (hostname コマンドを実行したときに表示されるホスト名) に対応する IP アドレスを使います。

- 送信側 IP アドレス (送信側が ANY バインドの場合)

JP1 のサービスへ接続する側が使う IP アドレスです。

JP1 では自 IP アドレスを指定せずにコネクション要求 (connect 関数を実行) します。この場合、OS の仕様に依存し、接続先に対応した IP アドレスが OS によって割り当てられます。一般に、接続先 IP アドレスへパケットを送るときに使われる NIC に対応した IP アドレスが割り当てられますが、詳細については OS の TCP/IP 制御の仕様を確認してください。

(b) クラスタシステムの場合

クラスタシステムで論理ホスト環境のセットアップをしている場合、通常のシステムと異なり、次の IP アドレスを使用します。

- 受信側 IP アドレス (受信側が IP バインドの場合)

JP1 のサービスが接続を受け付ける IP アドレスです。

物理ホスト環境は、物理ホスト名 (hostname コマンドを実行したときに表示されるホスト名) に対応した IP アドレスを使います。論理ホスト環境は、論理ホスト名に対応した論理 IP アドレスを使います。

- **送信側 IP アドレス (送信側が IP バインドの場合)**

JP1 のサービスへ接続する側が使う IP アドレスです。

物理ホスト環境は、物理ホスト名 (hostname コマンドを実行したときに表示されるホスト名) に対応した IP アドレスを使います。論理ホスト環境は、論理ホスト名に対応した論理 IP アドレスを使います。

(c) 通信設定をカスタマイズしている場合の注意

「9.3.2(2)(a) 通常のシステムの場合」および「9.3.2(2)(b) クラスタシステムの場合」の説明は、JP1 をセットアップしたままの標準的な通信設定の場合の動作です。JP1/Base でjp1hosts 情報またはjp1hosts2 情報を定義するなど複数 LAN 接続の設定をカスタマイズしている場合は、受信側・送信側の通信方式 (ANY バインド, IP バインド) の組み合わせによって動作が決まりますので注意してください。

受信側：IP バインド, 送信側：ANY バインドになるようにカスタマイズしている場合は、受信側は「9.3.2(2)(b) クラスタシステムの場合」の説明の動作, 送信側は「9.3.2(2)(a) 通常のシステムの場合」の説明の動作になります。

また、jp1hosts 情報またはjp1hosts2 情報を設定している場合、jp1hosts 情報またはjp1hosts2 情報に定義されたホスト名および IP アドレスに関しては、hosts ファイルの定義は参照されませんので注意してください。

例えば、jp1hosts 情報に次のように定義されていると仮定します。

```
hostA 100.0.0.10 200.0.0.10
```

また、hosts ファイルに次のように定義されていると仮定します。

```
100.0.0.10 hostA hostB
```

```
200.0.0.10 hostC
```

この場合、hostA、IP アドレス 100.0.0.10、および IP アドレス 200.0.0.10 に関しては、hosts ファイルは参照されません。このため、jp1hosts 情報に定義されていない hostB および hostC を構成定義ファイルに指定しても、システム構成を定義することはできません。

(d) JP1/IM - Manager メール通知機能を使用する場合の注意

JP1/IM - Manager メール通知機能は、IPv4 形式の IP アドレスでメールサーバと通信します。そのため、IPv4 形式の IP アドレスを持ったメールサーバを用意してください。IPv6 形式の IP アドレスを使った通信はできません。

(3) アドレス変換(NAT)の対応

JP1/IM は、スタティック・モードでのアドレス変換(NAT)に対応しています。

JP1/IM が使用する IP アドレスを、適切に変換できるように、NAT に設定してください。

9.3.3 Windows ファイアウォールの注意事項

(1) Windows ファイアウォールの設定

- Windows ファイアウォールを「有効」に設定した環境で JP1/IM - View から統合管理を行う場合には、プログラムまたはポート番号を必要に応じて Windows ファイアウォール経由の通信を許可するように登録する必要があります。設定については、JP1 の Web サイトに公開しているドキュメントの「JP1/Integrated Management - Manager ファイアウォール設定ガイド」を参照してください。
- Windows ファイアウォールを「有効」に設定した環境でセントラルスコープをご使用になる場合には、上記の設定に加えて、統合スコープのプログラムあるいはポート番号を必要に応じて、Windows ファイアウォール経由の通信を許可するように登録する必要があります。設定については、JP1 の Web サイトに公開しているドキュメントの「JP1/Integrated Management - Manager ファイアウォール設定ガイド」を参照してください。
- Windows ファイアウォールを「有効」に設定した環境で IM 構成管理をご使用になる場合には、上記の設定に加えて、IM 構成管理のプログラムあるいはポート番号を必要に応じて Windows ファイアウォール経由の通信を許可するように登録する必要があります。設定については、JP1 の Web サイトに公開しているドキュメントの「JP1/Integrated Management - Manager ファイアウォール設定ガイド」を参照してください。
- セキュリティの強化された Windows ファイアウォールで、規則に一致しない送信接続を許可している環境（OS のデフォルト）で、JP1/IM - View または統合オペレーション・ビューアーを使用する場合
 - 次のポート番号の送信をブロックしないでください。
 - 20115/tcp
 - 20238/tcp
 - 20305/tcp
 - 20702/tcp
 - 20703/tcp
 - 22301/tcp
 - 22302/tcp
 - 22303/tcp
 - 22304/tcp
 - 次のプログラムの送信をブロックしないでください。
 - View パス¥bin¥jdk¥bin¥java.exe
 - 接続先の JP1/IM - Manager の IP アドレスに対する送信をブロックしないでください。
- セキュリティの強化された Windows ファイアウォールで、規則に一致しない送信接続をブロックしている環境で、JP1/IM - View を使用する場合

[コントロールパネル] - [管理ツール] - [セキュリティが強化された Windows ファイアウォール] を選択し、[送信の規則] の [新規の送信の規則ウィザード] から、以下のプログラムの接続を許可してください。

ファイル名：View パス¥bin¥jdk¥bin¥java.exe

(2) Windows ファイアウォールからの削除

本製品をアンインストールする場合には、Windows ファイアウォールから登録情報を削除する必要があります。削除方法については、JP1 の Web サイトに公開しているドキュメントの「JP1/Integrated Management - Manager ファイアウォール設定ガイド」を参照してください。

(3) Windows ファイアウォールの一時無効化

Windows ファイアウォールから登録情報を一時無効化したい場合は、Windows ファイアウォールの [プログラムおよびサービス(P)] に表示されている項目のチェックをオフにしてください。

9.4 暗号化通信の構築

ここでは、通信暗号化機能を新規、変更、中止で使用する場合の設定、通信暗号化機能の JP1/IM - Manager での設定、および通信暗号化機能の設定確認について説明します。

❗ 重要

- 通信暗号化機能を使用する場合、以前の構成では接続できないことがあります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.10.7 通信暗号化機能の有効・無効と製品バージョン間の接続性」、「付録 H 下位バージョンとの接続性」を参照してください。
- 秘密鍵、サーバ証明書、およびルート証明書は復旧できるように、管理者がバックアップを取得してください。バックアップ対象については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「1.1.1(1)バックアップ (Windows の場合)」、「1.1.1(3)バックアップ (UNIX の場合)」を参照してください。

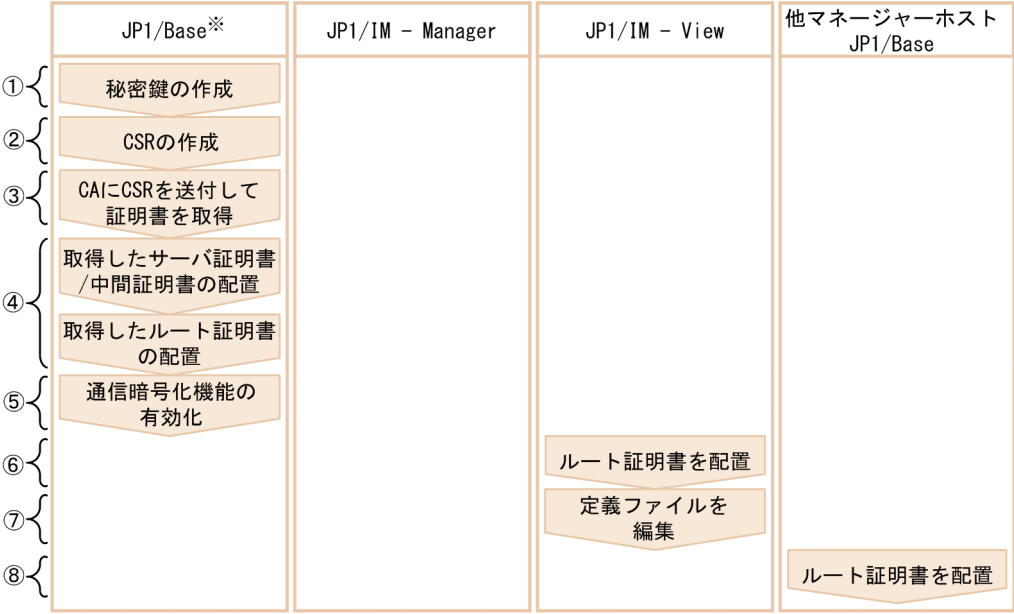
9.4.1 新規に通信暗号化機能を使用する

通信暗号化機能を初めて使用するユーザーが、マネージャーホストとビューアーホストで設定する手順を説明します。JP1/IM - Manager で設定する手順はありません。なお、マネージャーホストが複数ある場合はそれぞれで実施してください。システム構成については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.10.6 システム構成」を参照してください。

マネージャーホストで使用する秘密鍵、CSR、各証明書、および SSL 通信定義ファイル (jp1bs_ssl.conf) を基に設定する共通定義情報は、JP1/IM - Manager, JP1/AJS3, および JP1/Base の通信暗号化機能で使します。

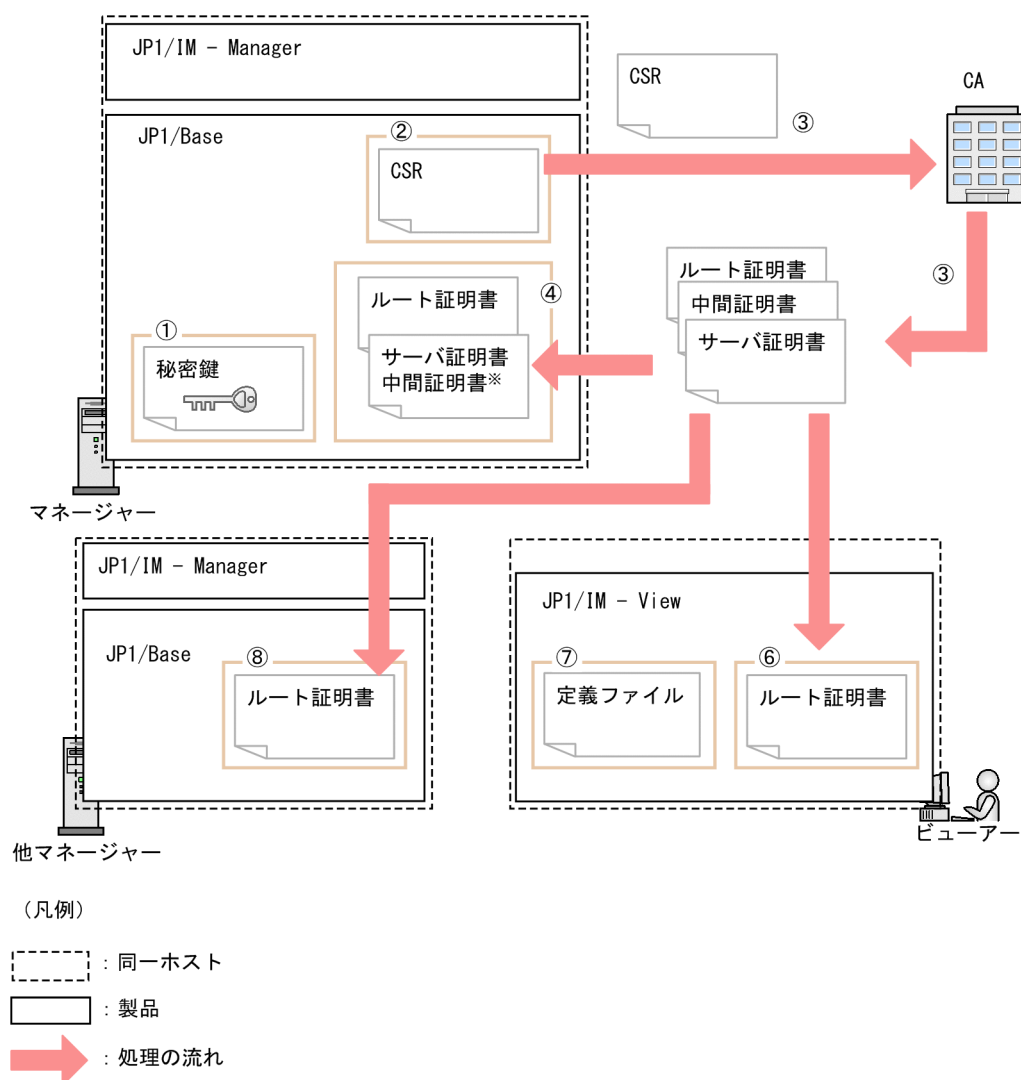
新規に通信暗号化機能を使用する場合の手順を図に示すと、次のようになります。

図 9-8 新規に通信暗号化機能を使用する場合の手順



注※ 詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

図 9-9 ユーザーが操作するファイルの概要



注※ 中間証明書を使用する場合は、サーバ証明書と結合します。

図中の番号に従って説明します（図中の丸付き番号は、次に示す番号にそれぞれ対応しています）。

1. JP1/Base で秘密鍵を作成する。※1

秘密鍵にパスフレーズを設定しないでください。パスフレーズ付きの秘密鍵は使用できません。

2. JP1/Base で CSR（証明書署名要求）を作成する。※1

手順 1 で作成した秘密鍵を指定し、CSR を作成します。CN（Common Name）にマネージャーホスト名を設定してください。CN のマネージャーホスト名は、サーバ証明書のホスト名の検証（CN および SAN の検証）で使用します。

サーバ証明書のホスト名の検証（CN および SAN の検証）については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.10.4(2) サーバ証明書のホスト名の検証（CN および SAN の検証）」を参照してください。

3. CA（認証局）に手順 2 で作成した CSR を送付し、各証明書を発行してもらう。※1

手順 2 で作成した CSR を CA に送付し、サーバ証明書とルート証明書を発行してもらいます。

中間 CA 証明書がある場合は、中間 CA 証明書を取得します。

なお、CA から署名を受けた証明書ではなく、自己署名証明書を使用する場合は CSR を CA に送付しません。

4. JP1/Base に秘密鍵、各証明書を配置する。※1※2

手順 1 で作成した秘密鍵、手順 3 で発行されたサーバ証明書およびルート証明書をサーバ側の任意のフォルダに配置します。

中間 CA 証明書がある場合は、サーバ証明書に証明書の階層構造に従って中間 CA 証明書をテキストエディターなどで結合します。

結合後のサーバ証明書は次のようになります。

```
-----BEGIN CERTIFICATE-----
```

サーバ証明書の内容

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

中間 CA 証明書の内容

```
-----END CERTIFICATE-----
```

5. JP1/Base で通信暗号化機能を有効にする。※1

通信暗号化機能の設定手順を次に示します。

1. SSL 通信定義ファイル (jp1bs_ssl.conf) を定義する。

SSL 通信定義ファイルに、SSL 通信を有効にするかどうか、およびサーバ証明書のファイル名やルート証明書の格納先など、SSL 通信の設定情報を定義します。

SSL 通信定義ファイルの詳細については、マニュアル「JP1/Base 運用ガイド」の SSL 通信定義ファイルについて説明している章を参照してください。

2. SSL 通信定義ファイルを引数に jbssetcnf コマンドを実行する。

jbssetcnf コマンドを実行すると、共通定義情報に設定内容が反映されます。反映される設定内容は、JP1/IM - Manager, JP1/AJS3, および JP1/Base で通信暗号化機能を実行するための設定情報です。

jbssetcnf コマンドについては、マニュアル「JP1/Base 運用ガイド」を参照してください。

6. JP1/IM - View に手順 3 で発行されたルート証明書を配置する。※2

- ルート証明書の格納場所

View パス¥conf¥ssl¥rootcer

JP1/IM - View はルート証明書のファイルを複数配置できます。

JP1/IM - View へのルート証明書の配置については、ユーザーは配置するルート証明書が、どのマネージャーホストに対応するルート証明書か区別する必要があります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.10.3(1) マネージャーホストとビューアーホスト間の暗号化」を参照してください。

7. 非暗号化通信するホストを設定するファイルを編集する。

非暗号化通信ホスト設定ファイルは、非暗号化通信をするホストを設定するファイルです。初期設定では、すべてのホストで非暗号化通信となる設定がされています。詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「非暗号化通信ホスト設定ファイル (nosslhost.conf)」(2. 定義ファイル) を参照してください。

8. 次の場合、他マネージャーホストにルート証明書を配置する。※2

- 他マネージャーホストから jcochstat コマンドの -h オプションで対処状況を変更する場合
他マネージャーホストで通信暗号化機能を使用していない場合は、通信暗号化機能を有効にし、他マネージャーホストのルート証明書ファイルに手順 3 で発行されたルート証明書を追加してください。
- 上位マネージャーで IM 構成管理機能を使用する場合
上位マネージャーとなる他マネージャーホストの JP1/Base に、手順 3 で発行されたルート証明書を配置します。他マネージャーホストの JP1/Base に、ルート証明書の格納場所（共通定義情報の CACERTIFICATEFILE）を設定する作業は必要ですが、通信暗号化機能を有効にする必要はありません。

他マネージャーホストで通信暗号化機能を使用している場合は、他マネージャーホストのルート証明書ファイルに手順 3 で発行されたルート証明書を追加してください。

他マネージャーホストにルート証明書を追加する場合は、追加するルート証明書をテキストエディターなどで結合します。

結合後のルート証明書ファイルは次のようになります。

-----BEGIN CERTIFICATE-----

ルート証明書の内容

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

ルート証明書の内容

-----END CERTIFICATE-----

注※1 詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

注※2 複数の証明書を結合する場合は、テキストエディターで証明書を開き、証明書を結合してください。

❗ 重要

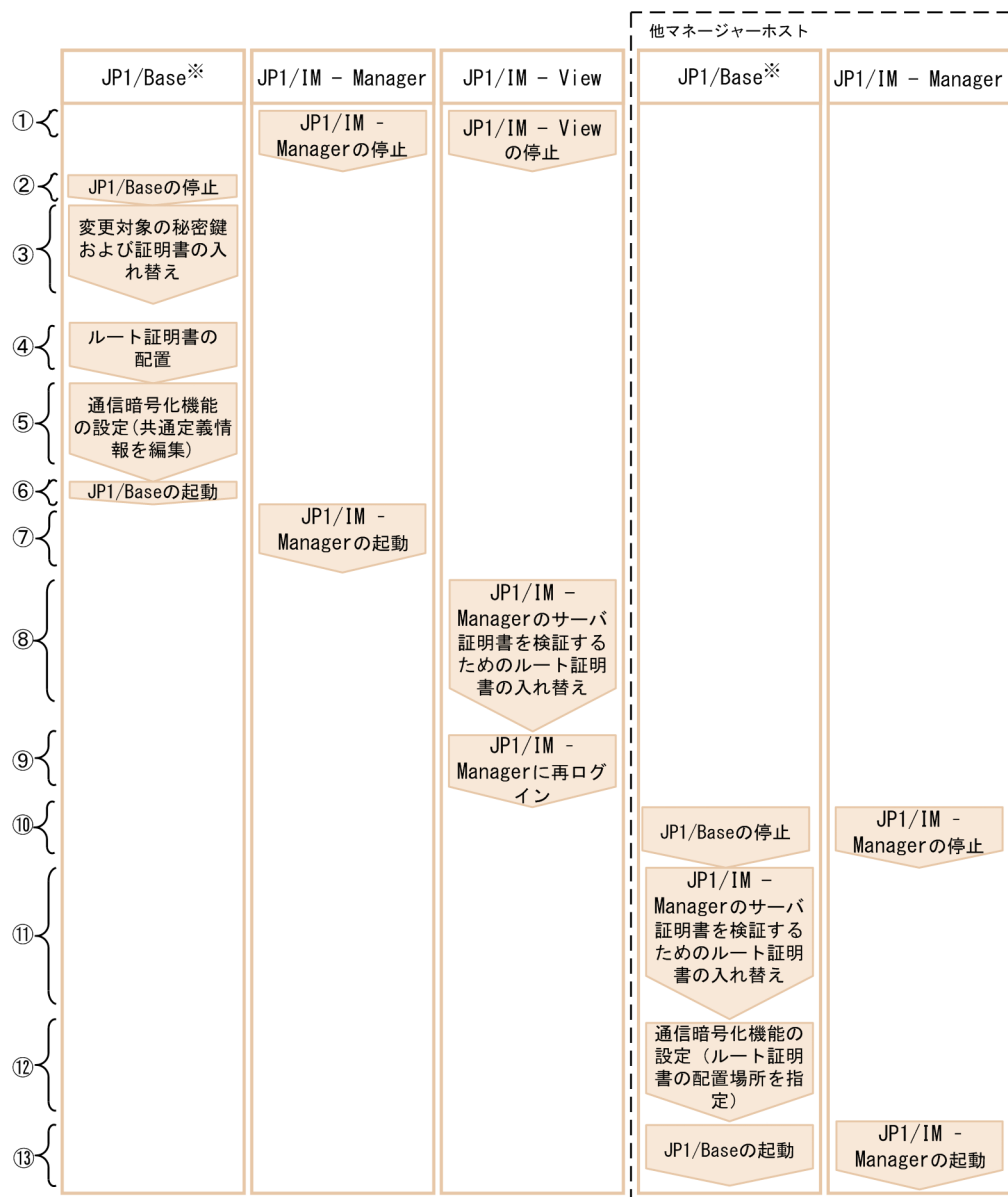
JP1/IM - Manager および JP1/Base の起動中は、通信暗号化機能の設定は変更できません。有効期限切れに伴うサーバ証明書やルート証明書の入れ替えなどで、通信暗号化機能の設定を変更する場合は、JP1/IM - Manager および JP1/Base を停止してから変更してください。

設定後、通信暗号化機能が正しく設定できているかどうかを確認してください。確認手順については、[「9.4.6 通信暗号化機能が正しく設定できているか確認する」](#)を参照してください。

9.4.2 設定済みの証明書を変更する

設定済みの証明書を変更する場合、ユーザーがマネージャーホストとビューアーホストで変更する手順は次のとおりです。なお、マネージャーホストが複数ある場合はそれぞれで実施してください。

図 9-10 証明書を変更する場合の手順



(凡例) : 同一ホスト

注※ 詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

図中の番号に従って説明します（図中の丸付き番号は、次に示す番号にそれぞれ対応しています）。

1. JP1/IM - View, JP1/IM - Manager を停止する。
2. JP1/Base を停止する。
3. 変更対象の秘密鍵, およびサーバ証明書を入れ替える。

4. 手順3 で入れ替えたサーバ証明書に対応するルート証明書に変更がある場合は、JP1/Base のルート証明書を入れ替える。
5. 秘密鍵、証明書のファイル名、または格納場所を変更した場合は、JP1/Base で通信暗号化機能の設定をする（共通定義情報を編集する）。※1
6. JP1/Base を起動する。
7. JP1/IM - Manager を起動する。
8. JP1/IM - View のルート証明書に変更がある場合は、JP1/IM - Manager のサーバ証明書を検証するためのルート証明書を入れ替える。※2※3
 - ルート証明書の格納場所
View パス¥conf¥ssl¥rootcer
9. JP1/IM - View から JP1/IM - Manager に再ログインする。
10. 次の場合、他マネージャーホストの JP1/IM - Manager、および JP1/Base を停止する。
 - 他マネージャーホストから jcochstat コマンドの -h オプションで対処状況を変更する場合
 - 上位マネージャーで IM 構成管理機能を使用する場合
11. 次の場合、他マネージャーホストのルート証明書を入れ替える。※3
 - 他マネージャーホストから jcochstat コマンドの -h オプションで対処状況を変更する場合
 - 上位マネージャーで IM 構成管理機能を使用する場合

ルート証明書に変更がある場合は、JP1/IM - Manager のサーバ証明書を検証するためのルート証明書を入れ替えます。なお、ルート証明書が結合されている場合は、対応するルート証明書だけ入れ替えます。
12. 次の場合、ルート証明書のファイル名、または格納場所を変更するときは、他マネージャーホストの JP1/Base で通信暗号化機能を設定する（共通定義情報を編集する）。※1
 - 他マネージャーホストから jcochstat コマンドの -h オプションで対処状況を変更する場合
 - 上位マネージャーで IM 構成管理機能を使用する場合
13. 次の場合、他マネージャーホストの JP1/IM - Manager、および JP1/Base を起動する。
 - 他マネージャーホストから jcochstat コマンドの -h オプションで対処状況を変更する場合
 - 上位マネージャーで IM 構成管理機能を使用する場合

注※1 詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

注※2 詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.10.3(1) マネージャーホストとビューアーホスト間の暗号化」を参照してください。

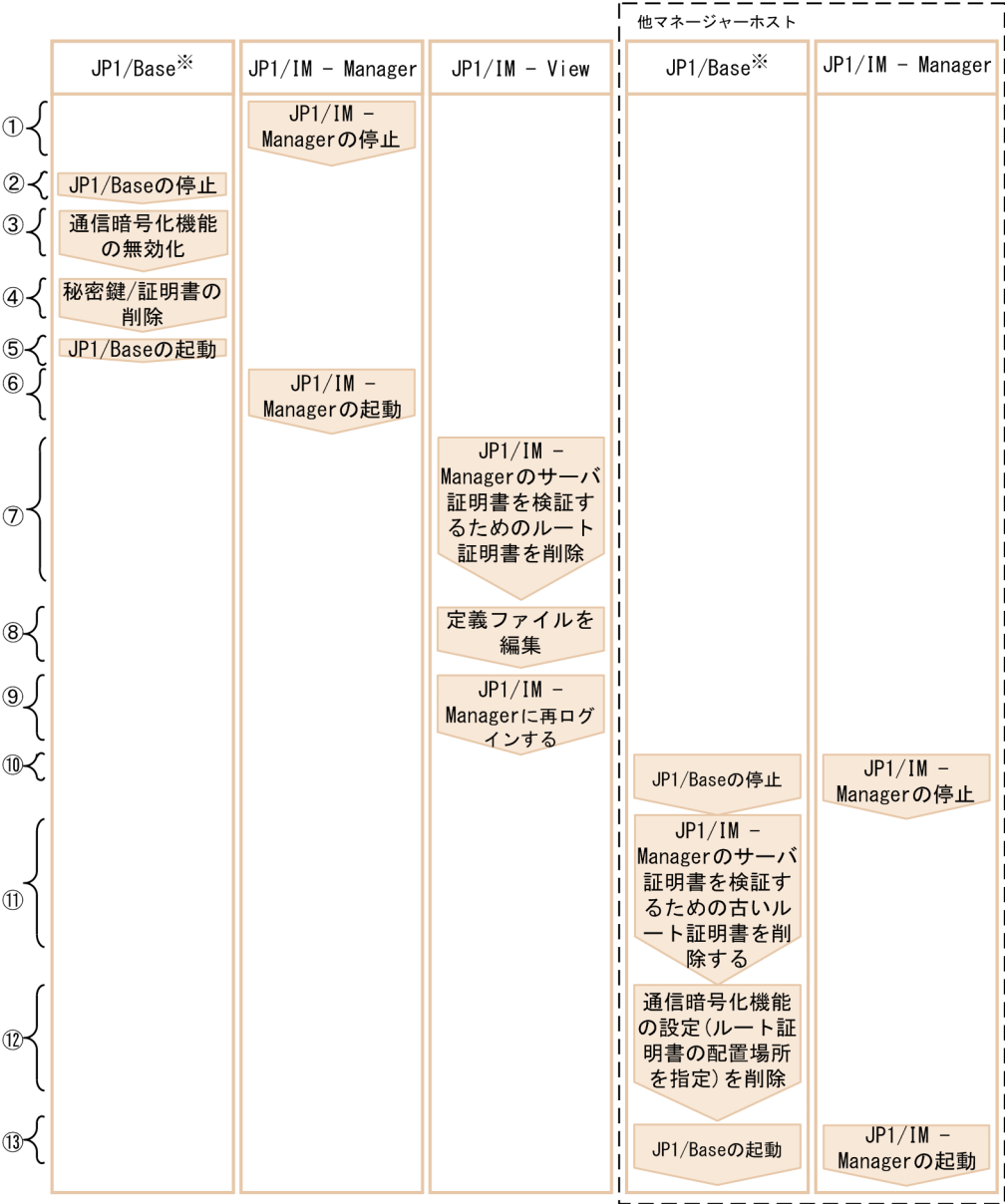
注※3 証明書を編集する場合は、テキストエディターで証明書を開き、編集してください。

設定後、通信暗号化機能が正しく設定できているかどうかを確認してください。確認手順については、[「9.4.6 通信暗号化機能が正しく設定できているか確認する」](#)を参照してください。

9.4.3 通信暗号化機能の使用を中止する

通信暗号化機能の使用を中止する場合、ユーザーがマネージャーホストとビューアーホストで変更する手順は次のとおりです。機能の使用を一時的にやめる場合は、手順 4、手順 7、および手順 11 は不要です。なお、マネージャーホストが複数ある場合はそれぞれで実施してください。

図 9-11 通信暗号化機能の使用を中止する場合の手順



(凡例) □ □ □ : 同一ホスト
注※ 詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

図中の番号に従って説明します（図中の丸付き番号は、次に示す番号にそれぞれ対応しています）。

1. JP1/IM - Manager を停止する。
2. JP1/Base を停止する。
3. JP1/Base で通信暗号化機能を無効にする。※1
4. JP1/Base で秘密鍵、および証明書を削除する。
5. JP1/Base を起動する。
6. JP1/IM - Manager を起動する。
7. JP1/IM - View で、通信暗号化機能の使用を中止する JP1/IM - Manager のサーバ証明書を検証するためのルート証明書を削除する。※2

JP1/IM - View のルート証明書の削除については、ユーザーは削除するルート証明書が、どのマネージャーホストに対応するルート証明書か区別する必要があります。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.10.3(1) マネージャーホストとビューアーホスト間の暗号化」を参照してください。

- ルート証明書の格納場所
View パス¥conf¥ssl¥rootcer

8. 機能の使用を中止するマネージャーホストに非暗号化通信する場合は、JP1/IM - View の定義ファイルに非暗号化通信するマネージャーホストのホスト名を記載する。

詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「非暗号化通信ホスト設定ファイル (nossllhost.conf)」(2. 定義ファイル) を参照してください。

9. JP1/IM - View から JP1/IM - Manager に再ログインする。

10. 次の場合、他マネージャーホストの JP1/IM - Manager、および JP1/Base を停止する。

- 他マネージャーホストから jcochstat コマンドの -h オプションで対処状況を変更する場合
- 上位マネージャーで IM 構成管理機能を使用する場合

11. 次の場合、他マネージャーホストのルート証明書を削除する。※2

- 他マネージャーホストから jcochstat コマンドの -h オプションで対処状況を変更する場合
- 上位マネージャーで IM 構成管理機能を使用する場合

通信暗号化機能の使用を中止する JP1/IM - Manager のサーバ証明書を検証するためのルート証明書を削除します。なお、ルート証明書が結合されている場合は、対応するルート証明書だけ削除します。

12. 次の場合、配置してあるルート証明書をすべて削除したときは、JP1/Base で通信暗号化機能の設定を削除する。（共通定義情報を編集する）※1

- 他マネージャーホストからjcochstat コマンドの-h オプションで対処状況を変更する場合
- 上位マネージャーで IM 構成管理機能を使用する場合

13. 次の場合、他マネージャーホストの JP1/IM - Manager と JP1/Base を起動する。

- 他マネージャーホストからjcochstat コマンドの-h オプションで対処状況を変更する場合
- 上位マネージャーで IM 構成管理機能を使用する場合

注※1 詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

注※2 証明書を編集する場合は、テキストエディターで証明書を開き、編集してください。

設定後、通信暗号化機能が正しく設定できているかどうかを確認してください。確認手順については、[「9.4.6 通信暗号化機能が正しく設定できているか確認する」](#)を参照してください。

9.4.4 JP1/IM - Manager の設定

JP1/IM - Manager での通信暗号化機能の有効・無効の設定、および証明書の配置の設定について説明します。

(1) 通信暗号化機能の有効・無効

通信暗号化機能の有効・無効は、JP1/Base で設定する共通定義情報を参照します。

JP1/IM - Manager は起動時に、JP1/Base で設定した共通定義情報を参照し起動します。JP1/Base で設定する共通定義情報については、マニュアル「JP1/Base 運用ガイド」の SSL 通信定義ファイルについて説明している章を参照してください。

また、JP1/IM - Manager の起動時に JP1/Base（マネージャーホスト）と通信暗号化機能の有効・無効が同じことを確認するためのメッセージを出力します。機能が有効の場合は、統合トレースログに「KAVB8810-I」のメッセージが出力され、機能が無効の場合は、統合トレースログに「KAVB8811-I」のメッセージが出力されます。通信暗号化機能の有効・無効の確認手順の詳細については、[「9.4.6 通信暗号化機能が正しく設定できているか確認する」](#)を参照してください。

(2) SSL のバージョンや証明書の配置先の設定

SSL のバージョン、および証明書の配置先は JP1/Base で設定する共通定義情報を参照します。JP1/Base で設定する共通定義情報については、マニュアル「JP1/Base 運用ガイド」の SSL 通信定義ファイルについて説明している章を参照してください。

(3) JP1/IM - Manager 用キーストア

秘密鍵または JP1/IM - Manager 用のキーストアを入手した場合、通信データを暗号化しても解読されるおそれがあるため、秘密鍵と JP1/IM - Manager 用のキーストアは、JP1/IM - Manager の管理者が厳重

に管理してください。秘密鍵または JP1/IM - Manager 用のキーストアを格納しているフォルダは、一般ユーザーは参照できないように設定してください。

JP1/IM - Manager 用のキーストアは、JP1/IM - Manager が暗号化通信のために使用し、次のデータを格納しているファイルです。

- 秘密鍵
- サーバ証明書
- 中間 CA 認証局証明書（使用する場合）

格納先は、マネージャーホストで次のとおりに設定されています。

- 物理ホストの場合
Windows の場合：Manager パス¥conf¥ssl¥server.keystore
UNIX の場合：/etc/opt/jp1imm/conf/ssl/server.keystore
- 論理ホストの場合
Windows の場合：共有フォルダ¥JP1IMM¥conf¥ssl¥server.keystore
UNIX の場合：共有ディレクトリ/jp1imm/conf/ssl/server.keystore

9.4.5 JP1/IM - Agent（統合エージェント制御基盤）の設定

統合エージェント管理基盤と統合エージェント制御基盤間の通信を暗号化する場合に、次の設定が必要です。

(1) 統合エージェント管理基盤のサーバー証明書を検証する場合

1. CA 証明書を配置する。

接続先の imbase のサーバー証明書を発行した認証局の CA 証明書を、次のディレクトリに配置します。

- Windows の場合
Agent パス¥conf¥cert¥
- Linux の場合
/opt/jp1ima/conf/cert/

2. imagent 共通設定ファイル (jpc_imagentcommon.json) に CA 証明書のパスを記載する。

3. imagent と imagentproxy を再起動する。

(2) 統合エージェント管理基盤のサーバー証明書を検証しない場合

1. imagent 共通設定ファイル (jpc_imagentcommon.json) の tls_config.insecure_skip_verify に [true] を設定する。

2. imagent と imagentproxy を再起動する。

9.4.6 通信暗号化機能が正しく設定できているか確認する

通信暗号化機能が有効になっていること、または無効になっていることは次の手順で確認してください。
なお、マネージャーホストが複数ある場合はそれぞれで実施してください。

1. マネージャーホストの統合トレースログを確認する。

- 通信暗号化機能が有効になっていることを確認する場合は、統合トレースログに「KAVB8810-I」のメッセージが出力されていることを確認してください。
- 通信暗号化機能が無効になっていることを確認する場合は、統合トレースログに「KAVB8811-I」のメッセージが出力されていることを確認してください。

2. WWW ブラウザーから JP1/IM - Manager に接続できることを確認する。

インテリジェント統合管理基盤を使用する場合は、インテリジェント統合管理基盤にログインできることを確認してください。

ログインする手順はマニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「4. JP1/IM - Manager へのログインとログアウト」を参照してください。

3. JP1/IM - View から JP1/IM - Manager に接続できることを確認する。

セントラルコンソールにログインできることを確認してください。

セントラルスコープを使用する場合は、セントラルスコープにログインできることを確認してください。

IM 構成管理を使用する場合は、IM 構成管理にログインできることを確認してください。

ログインする手順はマニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「4. JP1/IM - Manager へのログインとログアウト」を参照してください。

4. コマンド実行および自動アクションによるコマンド実行ができることを確認する。

マネージャーホストに対して JP1/IM - View の「コマンド実行」画面からコマンドを実行し、【実行結果】に実行終了を通知するメッセージ「KAVB2013-I」が表示されることを確認してください。

マネージャーホストに対して自動アクションによるコマンド実行をし、JP1/IM - View の「アクション結果」画面、または「アクション結果一覧」画面で、実行したアクションの状態が終了であることを確認してください。

コマンド実行の手順については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「8.1 コマンドを実行する」を参照してください。

自動アクションによるコマンド実行をする手順については、「5.5 自動アクションの設定」を参照してください。

5. IM 構成同期ができることを確認する。

IM 構成管理を使用して拠点マネージャーを管理する場合は、【IM 構成管理】画面から IM 構成同期を実行し、リモート監視構成の情報を収集できることを確認してください。

IM 構成同期を実行する手順については「[3.2.5 システムの階層構成の同期を取る](#)」を参照してください。

10

ほかの JP1 製品と連携するための設定

この章では、JP1/IM とほかの JP1 製品を連携する場合の環境設定について説明します。

10.1 JP1/Service Support と連携する

JP1/Service Support と連携する場合には、JP1/Service Support 画面呼び出しを設定する必要があります。

10.1.1 JP1/Service Support 画面呼び出し設定

JP1/IM - View から JP1/Service Support の [登録先プロセスワークボード選択] 画面を呼び出す場合、JP1/IM - View のログイン先の JP1/IM - Manager (セントラルコンソール) が管理するインシデント手動登録定義ファイル (`incident.conf`) を編集する必要があります。また、インシデントの登録モードを 3 に設定した場合、任意の JP1 イベントの属性や文字列をインシデントとして引き継ぐために、インシデント引き継ぎ情報設定ファイル (`incident_info.conf`) を編集する必要があります。

JP1/Service Support 画面の呼び出し設定をする手順を次に示します。

1. インシデント手動登録定義ファイル (`incident.conf`) をテキストエディターなどで編集する。
2. インシデントの登録モードを 3 に設定した場合、インシデント引き継ぎ情報設定ファイル (`incident_info.conf`) をテキストエディターなどで編集する。
3. インシデント手動登録定義ファイル (`incident.conf`) の `SS_URL=` に指定したポート番号について、ファイアウォールを通過できるように設定する。
JP1/IM - View のマシンから、JP1/Service Support のマシンに対して、ファイアウォールを通過できるようにします。
4. `jco_spmd_reload` コマンドを実行するか、JP1/IM - Manager を再起動する。
5. JP1/IM - View から JP1/IM - Manager (セントラルコンソール) に再ログインする。
定義した内容が有効になります。

JP1/Service Support を呼び出す際の URL の最大長は 2,046 文字です。インシデントの登録モードを 2 に設定した場合イベント ID を引き継ぐため、登録モードを 1 に設定した場合より、引き継げるメッセージが短くなります。メッセージが途中で切れている場合は、[イベント詳細] 画面に表示されているメッセージを JP1/Service Support にコピー&ペーストしてください。

インシデント手動登録定義ファイル (`incident.conf`) の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インシデント手動登録定義ファイル (`incident.conf`)」(2. 定義ファイル) を参照してください。

インシデント引き継ぎ情報設定ファイル (`incident_info.conf`) の詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「インシデント引き継ぎ情報設定ファイル (`incident_info.conf`)」(2. 定義ファイル) を参照してください。

10.2 JP1/Navigation Platform と連携する

JP1/Navigation Platform と連携する場合には、イベントガイド情報ファイルの、イベントガイドメッセージファイルの URL を設定する必要があります。

イベントガイド情報ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「イベントガイド情報ファイル (jco_guide.txt)」(2. 定義ファイル) を参照してください。URL の設定の詳細については、JP1/Navigation Platform のマニュアルの JP1 製品からナビゲーションプラットフォームを呼び出すための URL について説明されている箇所を参照してください。

シングルサインオンで業務コンテンツ（運用手順）を参照するためには、JP1/IM - Manager と JP1/Navigation Platform の認証サーバを同一にしてください。また、認証サーバの JP1/Base のバージョンは、10-10 以降を指定してください。

シングルサインオンで業務コンテンツ（運用手順）を参照できる場合の組み合わせを次の表に示します。

表 10-1 シングルサインオンで業務コンテンツ（運用手順）を参照できる場合の組み合わせ

バージョン	JP1/IM - View が 10-00 以前			JP1/IM - View が 10-10 以降		
	JP1/IM - NP が 10-00 (uCNP09-50)	JP1/IM - NP が 10-10 (uCNP09-60)	JP1/IM - NP が 10-50 以降 ※1 (HNP10-00 以降)	JP1/IM - NP が 10-00 (uCNP09-50)	JP1/IM - NP が 10-10 (uCNP09-60)	JP1/IM - NP が 10-50 以降 ※1 (HNP10-00 以降)
JP1/IM - Manager が 10-00 以前	×			×		
JP1/IM - Manager が 10-10 以降	×			×	○※2	

(凡例)

- ：シングルサインオンで業務コンテンツ（運用手順）を表示できる
- ×：シングルサインオンで業務コンテンツ（運用手順）を表示できない（JP1/IM - Navigation Platform のログイン画面が表示される）

注※1
JP1/IM - NP の製品名称は、11-00 以降、JP1/Navigation Platform に変更になります。

注※2
セントラルコンソールのイベントガイドメッセージファイルに、シングルサインオン対応 URL を記述しておく必要があります。

10.3 JP1/AJS と連携する

JP1/AJS と連携する場合の設定について説明します。

10.3.1 モニター起動で JP1/AJS の画面を起動するための設定

モニター起動の設定については、「[5.17 連携製品のモニター起動の設定](#)」および JP1/AJS のマニュアルを参照してください。

10.3.2 [統合機能メニュー] 画面から JP1/AJS の画面を起動するための設定

JP1/AJS - View は、デフォルトで [統合機能メニュー] 画面に表示されています。JP1/IM - View と同ホストに JP1/AJS - View をインストールすると [統合機能メニュー] 画面から JP1/AJS - View を起動できます。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 運用ガイド」の「[8.3.2 \[統合機能メニュー\] 画面から操作できる機能](#)」を参照してください。また、統合機能メニューの設定については、「[5.18 統合機能メニューの設定](#)」を参照してください。

10.3.3 イベントガイド情報からモニター画面を表示するための設定

イベントガイド情報の URL から JP1/AJS - Web Console のモニター画面を表示する場合は、JP1/AJS - Web Console 連携用の URL をイベントガイドメッセージファイルに記載する必要があります。

設定の詳細については、JP1/AJS のマニュアルを参照してください。

10.3.4 自動アクションの送信メールからモニター画面を表示するための設定

自動アクションの送信メールからモニター画面を表示する場合は、JP1/AJS - Web Console のモニター画面の URL をメール本文に記載する必要があります。

設定の詳細については、JP1/AJS のマニュアルを参照してください。

10.3.5 インテリジェント統合管理基盤でルートジョブネットの関連や構成情報を確認するための設定

インテリジェント統合管理基盤を使用して JP1/AJS のルートジョブネットを監視する場合は、JP1/AJS のシステム構成管理情報を取得する必要があります。JP1/AJS と連携する場合の設定の詳細については、JP1/AJS のマニュアルを参照してください。

JP1/AJS からは、次の情報を取得します。

- JP1/AJS - Manager がインストールされているホスト名
- ホストの中の JP1/AJS - Manager
- スケジューラーサービス名
- ジョブグループ名
- ルートジョブネット名
- JP1/AJS - Manager 配下の JP1/AJS - Agent がインストールされているホスト名
- ホストの中の JP1/AJS - Manager 配下の JP1/AJS - Agent

なお、JP1/AJS3 - Manager ホストからは、実行登録済みのルートジョブネットだけを取得します。

10.4 JP1/PFM と連携する

JP1/PFM と連携する場合の設定について説明します。

10.4.1 モニター起動で JP1/PFM の画面を起動するための設定

モニター起動の設定については、「[5.17 連携製品のモニター起動の設定](#)」および JP1/PFM のマニュアルを参照してください。

10.4.2 [統合機能メニュー] 画面から JP1/PFM の画面を起動するための設定

統合機能メニューの設定については、「[5.18 統合機能メニューの設定](#)」および JP1/PFM のマニュアルを参照してください。

10.4.3 事象発生元ホストの性能レポートを表示する場合の設定

事象発生元ホストの性能レポート表示機能を使用するには、性能レポート表示定義ファイルに接続先の JP1/PFM - Web Console の URL を定義する必要があります。

設定の詳細については、JP1/PFM のマニュアルを参照してください。

10.4.4 インテリジェント統合管理基盤で稼働情報を確認するための設定

インテリジェント統合管理基盤を使用して JP1/PFM の稼働情報を監視する場合は、JP1/PFM のシステム構成管理情報を構成取得アダプタコマンド、および他製品連携用のプラグインを利用して取得する必要があります。JP1/PFM と連携する場合の設定の詳細については、JP1/PFM のマニュアルを参照してください。

JP1/PFM のシステム構成管理情報を取得する場合の前提条件を次に示します。

- JP1/IM - Manager, JP1/PFM - Manager, および JP1/PFM - Web Console のバージョンが 12-00 以降であること
- JP1/IM - Manager と連携先の JP1/PFM - Web Console の認証サーバが同一であること
- 連携先の JP1/PFM の認証モードが、JP1/Base で一元管理する JP1 認証モードであること
- JP1/IM - Manager のホストから連携先の JP1/PFM - Web Console にログインできること
- JP1/IM - Manager にログインしている JP1 ユーザーが、JP1/PFM の操作権限を持っていること

JP1/PFM からは、次の情報を取得します。

- JP1/PFM - Manager がインストールされているホスト名
- ホストの中の JP1/PFM - Manager
- JP1/PFM - Manager 配下の JP1/PFM - Agent または JP1/PFM - RM がインストールされているホスト名、および JP1/PFM - RM の監視対象ホスト名
- JP1/PFM - Manager 配下の JP1/PFM - Agent または JP1/PFM - RM がインストールされているホストにインストールされている JP1/PFM - Base
- JP1/PFM - Manager 配下の JP1/PFM - Agent または JP1/PFM - RM のサービス ID
- JP1/PFM - Manager 配下の JP1/PFM - Agent または JP1/PFM - RM のサービス

構成取得アダプタコマンド、および他製品連携用のプラグインの詳細については、マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「4. ユーザー作成プラグイン」を参照してください。

統合オペレーション・ビューアーを使用する場合は、マニュアル「JP1/Performance Management 設計・構築ガイド」の、監視コンソールを使用するための Web ブラウザーの設定手順について説明している個所を参照してください。

索引

数字

- 1 回の監視間隔で収集できるログのサイズの設定 (UNIX の場合) 356
- 1 回の監視間隔で収集できるログのサイズの設定 (Windows の場合) 105

C

Cosminexus

連携用のセットアップ 654

CSV ファイルを編集して [監視ツリー] 画面を作成 634

H

HiRDB

汎用監視オブジェクトの作成例 662

連携用のセットアップ 655

Hitachi PP Installer (UNIX の場合) 308

Hitachi PP Installer の起動 308

Hitachi PP Installer の使用方法 (UNIX の場合) 308

I

IM 管理ノードリンク定義ファイルの移行手順 529

IM 構成管理

仮想化システム構成の設定 441

管理情報のインポート・エクスポート 500

機能を使用するための設定 (UNIX の場合) 324

機能を使用するための設定 (Windows の場合) 64

システムの階層構成の設定 423

ホストの登録 424

IM 構成管理 DB の設定 (UNIX の場合) 323

IM 構成管理 DB の設定 (Windows の場合) 62

[IM 構成管理] 画面, [IM 構成編集] 画面, および [プロファイル表示/編集] 画面起動時の画面表示設定履歴機能の使用可否 134

IM 構成管理で仮想化構成を管理する 441

IM 構成管理の [ログイン] 画面の接続先ホスト入力履歴数 134

IM 構成管理の [ログイン] 画面の接続ユーザー入力履歴数 134

IM 構成管理を使用しない場合の JP1 イベントの転送設定 (UNIX の場合) 342

IM 構成管理を使用しない場合の JP1 イベントの転送設定 (Windows の場合) 82

IM 構成管理を使用しない場合のイベントサービスの定義情報の収集と配布 (UNIX の場合) 344

IM 構成管理を使用しない場合のイベントサービスの定義情報の収集と配布 (Windows の場合) 84

IM 構成管理を使用しない場合のシステムの階層構成の設定 (UNIX の場合) 337

IM 構成管理を使用しない場合のシステムの階層構成の設定 (Windows の場合) 77

IM 構成管理を使用する場合の JP1 イベントの転送設定 (UNIX の場合) 341

IM 構成管理を使用する場合の JP1 イベントの転送設定 (Windows の場合) 81

IM 構成管理を使用する場合のイベントサービスの定義情報の収集と配布 (UNIX の場合) 343

IM 構成管理を使用する場合のイベントサービスの定義情報の収集と配布 (Windows の場合) 83

IM 構成管理を使用する場合のシステムの階層構成の設定 (UNIX の場合) 333

IM 構成管理を使用する場合のシステムの階層構成の設定 (Windows の場合) 73

IM 構成管理・ビューアーのセットアップ 133

IM 構成管理・ビューアーのセットアップ (Windows の場合) 133

IM 構成管理・ビューアーの動作カスタマイズ 134

IM データベースの更新 (UNIX の場合) 325

IM データベースの更新 (Windows の場合) 64

IM データベースの構築 (UNIX の場合) 320

IM データベースの構築 (Windows の場合) 59

IM データベースを構築するための準備 (UNIX の場合) 320

IM データベースを構築するための準備 (Windows の場合) 59

IP アドレス 807

J

jcfview.conf 134

JP1/AJS

システム監視オブジェクトの作成例 656

連携用のセットアップ 646

JP1/AJS と連携する 827

JP1/Base

JP1 ユーザーの操作権限の設定 (UNIX の場合) 330

JP1 ユーザーの操作権限の設定 (Windows の場合) 70

JP1 ユーザーの登録 (UNIX の場合) 330

JP1 ユーザーの登録 (Windows の場合) 70

イベントサービス機能の設定 (UNIX の場合) 340

イベントサービス機能の設定 (Windows の場合) 80

イベントサービスの登録ホスト名を FQDN 形式で利用する場合の設定 (UNIX の場合) 347

イベントサービスの登録ホスト名を FQDN 形式で利用する場合の設定 (Windows の場合) 87

インストール 34, 302

言語環境設定の確認 311

コマンド実行環境の設定 (UNIX の場合) 345

コマンド実行環境の設定 (Windows の場合) 85

サービスの起動順序の設定 (Windows の場合) 68

障害に備えた設定 (UNIX の場合) 332

障害に備えた設定 (Windows の場合) 72

通信の制御 791

認証サーバの指定 (UNIX の場合) 330

認証サーバの指定 (Windows の場合) 70

プライマリー認証サーバの設定情報のコピー (UNIX の場合) 331

プライマリー認証サーバの設定情報のコピー (Windows の場合) 70

ユーザー認証の設定 (UNIX の場合) 329

ユーザー認証の設定 (Windows の場合) 69

ユーザーマッピングの設定 (UNIX の場合) 329

ユーザーマッピングの設定 (Windows の場合) 69

JP1/Base および JP1/IM - Manager の起動 312

JP1/Base および JP1/IM - Manager の新規インストール (UNIX の場合) 744

JP1/Base および JP1/IM - Manager の新規インストール (Windows の場合) 686

JP1/Base および JP1/IM - Manager のバージョンアップインストール (UNIX の場合) 773

JP1/Base および JP1/IM - Manager のバージョンアップインストール (Windows の場合) 718

JP1/Cm2/NNM

連携用のセットアップ 651

JP1/Cm2/SSO

汎用監視オブジェクトの作成例 657

汎用監視オブジェクトの作成例 (Cosminexus 業務のリソース監視) 668

連携用のセットアップ 647

JP1/IM

IM 構成管理・ビューアーのセットアップ (Windows の場合) 133

IM データベースの構築 (UNIX の場合) 320

IM データベースの構築 (Windows の場合) 59

JP1/Base による通信の制御 791

JP1/IM - Agent のセットアップ (UNIX の場合) 380

JP1/IM - Agent のセットアップ (Windows の場合) 136

JP1/IM - Manager のセットアップ (UNIX の場合) 357

JP1/IM - Manager のセットアップ (Windows の場合) 106

JP1/IM - View のセットアップ (Windows の場合) 132

JP1/IM のイベント取得時の動作設定 535

JP1 イベントのフィルタリングの設定 538

アンインストール (UNIX の場合) 411

アンインストール (Windows の場合) 288

イベントガイド情報の編集 568

インストール (UNIX の場合) 304

インストール (Windows の場合) 35

インストールとセットアップ (UNIX の場合) 299

インストールとセットアップ (Windows の場合) 29

インストールとセットアップの流れ (UNIX の場合) 300

インストールとセットアップの流れ (Windows の場合) 30

インストール前に必要な作業 (UNIX の場合) 302

インストール前に必要な作業 (Windows の場合) 33

インテリジェント統合管理データベースの構築 (UNIX の場合) 327

インテリジェント統合管理データベースの構築 (Windows の場合) 66

ガイド情報の編集 635

監視ツリーを GUI で作成する 609

クラスタ運用時の注意事項 (UNIX の場合) 786

クラスタ運用時の注意事項 (Windows の場合) 733

クラスタ運用の概要 (UNIX の場合) 738

クラスタ運用の概要 (Windows の場合) 675

クラスタ運用の環境設定の流れ (UNIX の場合) 742

クラスタ運用の環境設定の流れ (Windows の場合) 684

クラスタシステムでの運用と環境構築 (UNIX の場合) 737

クラスタシステムでの運用と環境構築 (Windows の場合) 674

システムの階層構成の設定 423

自動アクションの設定 555

セットアップ内容の設計 (UNIX の場合) 302

セットアップ内容の設計 (Windows の場合) 33

セントラルコンソールの設定 534

セントラルスコープの環境設定の概要 607

セントラルスコープの設定 606

セントラルスコープの動作環境の設定 638

関連イベント発行の設定 563

対処状況変更時の JP1 イベント発行の設定 571

通信 803

統合機能メニューの設定 598

ネットワーク構成に応じた運用と環境構築 790

[ビジュアル監視] 画面を GUI で作成する 626

ファイアウォール環境での運用 797

複数ネットワークでの運用 792

ほかの JP1 製品と連携するための設定 824

ホスト情報の登録 608

保存した CSV ファイルを編集して [監視ツリー] 画面を作成 634

連携製品のモニター起動の設定 595

ログインユーザーごとの JP1/IM - View の設定 592

JP1/IM - Agent

アンインストール (UNIX の場合) 411

アンインストール (Windows の場合) 288

インストール (UNIX の場合) 304

インストール (Windows の場合) 35

セットアップ (UNIX の場合) 380

セットアップ (Windows の場合) 136

JP1/IM - Manager

SELinux に関する設定 (UNIX の場合) 363

アンインストール (UNIX の場合) 411

アンインストール (Windows の場合) 288

インストール (UNIX の場合) 304

インストール (Windows の場合) 35

サービスおよびプロセス (クラスタシステム) 682, 740

自動起動 (UNIX の場合) 357

自動終了 (UNIX の場合) 357

障害に備えた設定 (UNIX の場合) 368

障害に備えた設定 (Windows の場合) 123

セットアップ (UNIX の場合) 357

セットアップ (Windows の場合) 106

セットアッププログラムの実行 (UNIX の場合) 357

JP1/IM - Manager の設定 820

JP1/IM - View

JP1/IM - View の動作カスタマイズ (Windows の場合) 132

アンインストール (Windows の場合) 288

インストール (Windows の場合) 35

障害に備えた設定 (Windows の場合) 132

セットアップ (Windows の場合) 132

JP1/IM - View の動作カスタマイズ (Windows の場合) 132

JP1/IM - Agent (統合エージェント制御基盤) の設定
821

JP1/IM - Agent のアンインストール (UNIX の場合)
781

JP1/IM - Agent のアンインストール (Windows の場合)
726

JP1/IM - Agent のコンテナ環境の構築 (UNIX の場合)
403

JP1/IM - Agent のコンテナ環境の構築 (Windows の場合)
230

JP1/IM - Agent のサービスの設定 136, 380

JP1/IM - Agent の設定 140, 384

JP1/IM - Agent のバージョンアップインストール (UNIX の場合)
774

JP1/IM - Agent のバージョンアップインストール (Windows の場合)
719

JP1/IM - Agent のパッケージの登録 (UNIX の場合)
361

JP1/IM - Agent のパッケージの登録 (Windows の場合)
121

JP1/IM - Manager および JP1/Base のアンインストール (UNIX の場合)
780

JP1/IM - Manager および JP1/Base のアンインストール (Windows の場合)
726

JP1/Manager の新規インストール時の共通定義情報のコピー (UNIX の場合)
752

JP1/Manager の新規インストール時の共通定義情報のコピー (Windows の場合)
695

JP1/Manager の新規インストール時の物理ホスト環境のセットアップ (UNIX の場合)
745

JP1/Manager の新規インストール時の物理ホスト環境のセットアップ (Windows の場合)
687

JP1/Manager の新規インストール時の論理ホスト環境 (実行系) のセットアップ (UNIX の場合)
745

JP1/Manager の新規インストール時の論理ホスト環境 (実行系) のセットアップ (Windows の場合)
687

JP1/Manager の新規インストール時の論理ホスト環境 (待機系) のセットアップ (UNIX の場合)
752

JP1/Manager の新規インストール時の論理ホスト環境 (待機系) のセットアップ (Windows の場合)
696

JP1/IM - Manager の設定ファイルの編集について (UNIX の場合)
359

JP1/IM - Manager の設定ファイルの編集について (Windows の場合)
106

JP1/IM - View の設定項目 592

JP1/IM - View の設定手順 593

JP1/Navigation Platform と連携する 826

JP1/NETM/DM

- リモートインストール (UNIX)
307
- リモートインストール (Windows)
47
- 連携用のセットアップ
653

JP1/PAM

- 連携用のセットアップ
653

JP1/PFM

- 連携用のセットアップ
650

JP1/PFM と連携する 829

JP1/ServerConductor

- 連携用のセットアップ
655

JP1/Service Support と連携する 825

jp1cohasetup.exe 688

jp1cshasetup.exe 694

JP1 イベント

- 表示手順 575

JP1 イベントの表示色の設定 554

JP1 イベントのフィルタリングの設定 538

JP1 がサポートする範囲 (クラスタ運用) 679

JP1 ユーザー

- 操作権限の設定 (UNIX の場合)
330
- 操作権限の設定 (Windows の場合)
70
- 登録 (UNIX の場合)
330
- 登録 (Windows の場合)
70

K

KVM が起動するホストとの SSH 接続を設定する (UNIX の場合)
453

KVM が起動するホストとの SSH 接続を設定する (Windows 環境の場合)
449

N

NAT 801

NetBIOS (NetBIOS over TCP/IP) の設定
(Windows の場合) 96

O

OpenID プロバイダとシングルサインオン連携する
(外部製品との連携) 516

OS の環境構築 33, 302

S

SSH の設定 (UNIX の場合) 349

SSH の設定 (Windows の場合) 98

T

tuning.conf 133

V

vCenter の通信種別を変更する 448

VMware ESX の通信種別を変更する 447

W

WMI の設定 (Windows の場合) 89

WWW ブラウザーの起動パスの設定 133

あ

[アクション結果一覧] 画面起動可否の設定 133

アドレス変換(NAT)の対応 808

アンインストール

UNIX 411

Windows 288

アンインストール (Windows の場合)

Windows 288

アンインストール時の注意事項 (UNIX の場合) 415

アンインストール時の注意事項 (Windows の場合)
292

アンインストール手順 (UNIX の場合) 411

アンインストール手順 (Windows の場合) 288

暗号化機能を使用する場合の設定 506

暗号化通信の構築 811

い

イベントガイド情報

編集 568

イベントガイド情報からモニター画面を表示するための設定 827

イベントガイド情報の編集の手順 568

[イベントコンソール] 画面起動時の [アクション結果一覧] 画面起動可否の設定 133

[イベントコンソール] 画面起動時の [統合機能メニュー] 画面起動可否の設定 133

イベントサービス

設定 (UNIX の場合) 340

設定 (Windows の場合) 80

イベントサービスの登録ホスト名を FQDN 形式で利用する場合の設定 (UNIX の場合) 347

イベントサービスの登録ホスト名を FQDN 形式で利用する場合の設定 (Windows の場合) 87

イベント取得フィルター

共通除外条件を設定する 547

切り替えて設定する 546

設定する 545

バージョンアップ時の設定をする 374

一つだけ設定する 545

イベント取得フィルター (互換用) を設定する 551

イベント取得フィルターの位置の変更 374

イベントレポート出力の出力形式の指定 128, 376

インストーラーで使用する初期設定用環境変数 42

インストール

UNIX 304

作業の流れ (UNIX の場合) 300

作業の流れ (Windows の場合) 30

前提作業 (UNIX の場合) 302

前提作業 (Windows の場合) 33

前提プログラム (UNIX の場合) 302

前提プログラム (Windows の場合) 34

手順 (UNIX の場合) 304

手順 (Windows の場合) 35

インストール (Windows の場合)

Windows 35

インストール時の注意事項 (UNIX の場合) 313

インストール時の注意事項 (Windows の場合) 49
インストール直後に必要な設定 (UNIX の場合) 310
インストール直後に必要な設定 (Windows の場合) 48
インストール時の資料採取方法 (Windows の場合) 55
インストールとセットアップの流れ (UNIX の場合) 300
インストールとセットアップの流れ (Windows の場合) 30
インテリジェント統合管理基盤
IM 管理ノードリンク定義ファイルの移行手順 529
OpenID プロバイダとシングルサインオン連携するための設定 (外部製品との連携) 516
暗号化機能を使用する場合の設定 506
カスタム UI 表示機能の設定 508
環境設定の概要 502
環境設定を始める前に 502
関連性の定義の設定 511
機能を使用するための設定 (Windows の場合) 107
業務影響アイコンの設定 512
クラスタ環境の構築 507
クラスタ環境の構築 (UNIX の場合) 763
クラスタ環境の構築 (Windows の場合) 708
クラスタ環境の構築 (新規) (UNIX の場合) 763
クラスタ環境の構築 (新規) (Windows の場合) 708
クラスタ環境の構築 (バージョンアップ) (UNIX の場合) 765
クラスタ環境の構築 (バージョンアップ) (Windows の場合) 711
繰り返しイベントの表示抑止機能の互換設定 510
システム構成情報の設定 503
システム構成情報反映方式の設定 528
システムの状況に応じた対処アクションの提案機能の設定 515
修正版を適用したクラスタ環境の構築 (UNIX の場合) 765
修正版を適用したクラスタ環境の構築 (Windows の場合) 710

ダイレクトアクセス URL の設定 520
インテリジェント統合管理基盤で稼働情報を確認するための設定 829
インテリジェント統合管理基盤でルートジョブネットの関連や構成情報を確認するための設定 827
インテリジェント統合管理基盤の環境設定の概要 502
インテリジェント統合管理基盤の環境設定を始める前に 502
インテリジェント統合管理基盤の機能を使用するための設定 (UNIX の場合) 359
インテリジェント統合管理基盤の設定 501
インテリジェント統合管理データベースの構築 (UNIX の場合) 327
インテリジェント統合管理データベースの構築 (Windows の場合) 66
インテリジェント統合管理データベースの設定 (UNIX の場合) 327
インテリジェント統合管理データベースの設定 (Windows の場合) 66
インテリジェント統合管理データベースを構築するための準備 (UNIX の場合) 327
インテリジェント統合管理データベースを構築するための準備 (Windows の場合) 66

え

エージェントとして JP1/IM - Agent を使用する場合の設定 108, 360
エージェントのプロファイル更新通知機能 129, 377
エクスポート・インポート機能によるシステム構成の設定 (UNIX の場合) 335

お

オートスケール機能と連携する方法 (Windows の場合) 56

か

ガイド情報
編集 635
編集の手順 635
各種インストールについて (Windows の場合) 46
確認する

- JP1/Base の言語環境設定の確認 311
- カスタマイズした監視ツリーのマネージャーへの反映 624
- カスタマイズした監視ツリーのローカルホストへの保存 624
- 仮想化システム構成の管理および監視のための設定 (UNIX の場合) 336
- 仮想化システムの構成情報を収集する 457
- 仮想マシンのクローン作成 (UNIX の場合) 317
- 仮想マシンのクローン作成 (Windows の場合) 57
- 環境変数ファイルの設定 310
- 監視オブジェクト
 - 作成例 656
- 監視オブジェクト DB
 - 自動バックアップ・リカバリー設定 126, 373
- 監視ツリー
 - CSV ファイルを編集して [監視ツリー] 画面を作成 634
 - GUI で作成する 609
 - カスタマイズしたツリーをマネージャーへ反映する 624
 - カスタマイズしたツリーをローカルホストへ保存する 624
 - カスタマイズする 614
 - 監視範囲の設定をする 622
 - 既存の設定を取得する 611
 - サーバからの取得 611
 - 自動生成する 612
 - ビジュアルアイコンを使用するための設定 622
 - 編集画面の起動 609
 - 連携製品のセットアップ 646
 - ローカルに保存した (CSV ファイル) の取得 611
 - [監視ツリー] 画面のツールバーのカスタマイズ 641
- 監視ノード
 - 監視ツリーから削除 620
 - 監視ツリーでの移動 621
 - 監視ツリーでの検索 624
 - 監視ツリーでの属性設定 617
 - 監視ツリーへ追加 615
 - [ビジュアル監視] 画面から削除 630

- [ビジュアル監視] 画面での監視状態変更 631
- [ビジュアル監視] 画面での検索 631
- [ビジュアル監視] 画面での属性設定 630
- [ビジュアル監視] 画面へ追加 629
- 監視ノードのアイコンの移動を抑止するための設定 644
- 監視ノード名および監視ノードアイコン余白の表示を抑止するための設定 641
- 監視ノード名の状態色および監視ノードの状態色の設定 643
- 監視範囲の設定 622
- 管理対象ホストのコマンド実行機能の設定 (UNIX の場合) 345
- 管理対象ホストのコマンド実行機能の設定 (Windows の場合) 85

き

- 既存の監視ツリーの取得 611
- 共通除外条件の基本モードと拡張モードの切り替え 548
- 共通除外条件の設定 (共通除外条件拡張定義ファイルおよび jcochfilter コマンドを使用する場合) 551
- 共通除外条件の設定 ([共通除外条件設定] 画面または [共通除外条件設定(拡張)] 画面を使用する場合) 549
- 共通除外条件を設定する 547
- 共通定義情報 683, 740
- 共通定義情報の設定 (クラスタシステム) 683, 740
- 共通定義への言語環境設定 312
- 業務影響アイコン 512
- 業務グループ
 - 参照・操作制限の設定 604
- 業務グループからホストを削除する 471
- 業務グループにホストを追加する 471
- 業務グループの参照・操作制限の設定 604
- 業務グループの設定 463
- 共有ディスク 676
 - 共有ディスク上のファイル構成 681, 739
 - 前提条件 677

く

クライアントアプリケーションの実行環境の設定 (UNIX の場合) 346

クライアントアプリケーションの実行環境の設定 (Windows の場合) 86

クラスタ運用時の注意事項 (UNIX の場合) 786

クラスタ運用時の注意事項 (Windows の場合) 733

クラスタ運用での JP1/IM の構成の概要 680, 738

クラスタ環境での IM データベースの更新 (UNIX の場合) 783

クラスタ環境での IM データベースの更新 (Windows の場合) 729

クラスタ環境を構築する 507

クラスタ環境を構築する (UNIX の場合) 763

クラスタ環境を構築する (Windows の場合) 708

クラスタシステム

- JP1/IM の構成 (UNIX の場合) 738
- JP1/IM の構成 (Windows の場合) 680
- 概要 (UNIX の場合) 738
- 概要 (Windows の場合) 676
- クラスタ運用 676
- クラスタ運用時の注意事項 (UNIX の場合) 786
- クラスタ運用時の注意事項 (Windows の場合) 733
- クラスタ運用の概要 (UNIX の場合) 738
- クラスタ運用の概要 (Windows の場合) 675
- クラスタ運用の環境設定の流れ (UNIX の場合) 742
- クラスタ運用の環境設定の流れ (Windows の場合) 684
- クラスタ運用の前提条件 (UNIX の場合) 738
- クラスタ運用の前提条件 (Windows の場合) 677
- クラスタシステムでの運用と環境構築 (UNIX の場合) 737
- クラスタシステムでの運用と環境構築 (Windows の場合) 674
- クラスタソフト 676
- クラスタソフトへの登録 (新規インストール・セットアップ) (Windows の場合) 714
- 新規インストール・セットアップでのクラスタソフトへの登録 (UNIX の場合) 768

論理ホスト 676

論理ホストの新規インストール・セットアップ (UNIX の場合) 744

論理ホストの新規インストール・セットアップ (Windows の場合) 686

論理ホストのバージョンアップインストール・セットアップ (UNIX の場合) 773

論理ホストのバージョンアップインストール・セットアップ (Windows の場合) 718

クラスタソフトに登録するスクリプトの作成 (UNIX の場合) 769

繰り返しイベントの監視抑止の設定 553

繰り返しイベントの集約

設定 593

クリップボードへのコピー可否の設定 133

け

言語コード 310

検索時のイベント取得件数 592

こ

更新間隔 592

更新時のイベント取得件数 592

構成定義

情報の削除 (UNIX の場合) 338

情報の削除 (Windows の場合) 78

情報の設定での注意事項 (UNIX の場合) 338

情報の設定での注意事項 (Windows の場合) 78

情報の変更 (UNIX の場合) 338

情報の変更 (Windows の場合) 78

構成定義情報の設定での注意事項 (UNIX の場合) 338

構成定義情報の設定での注意事項 (Windows の場合) 78

構成例 1 (クラスタ運用なし, JP1/IM - View 接続) 792

構成例 2 (クラスタ運用なし, コマンド実行) 793

構成例 3 (クラスタ運用, JP1/IM - View 接続) 794

構成例 4 (クラスタ運用, コマンド実行) 795

コマンド実行

実行環境の設定をする (UNIX の場合) 345
実行環境の設定をする (Windows の場合) 85
コマンドでの設定変更 (UNIX の場合) 783
コマンドでの設定変更 (Windows の場合) 729
固有の拡張属性の表示および指定の設定 573
固有の属性付加の設定 572

さ

サーバ応答待ちのタイムアウト時間 134
サーバからの監視ツリーの取得 611
サーバからの [ビジュアル監視] 画面の取得 627
サービスの起動順序の設定 (Windows の場合) 68
作業の流れ
インストールとセットアップ (UNIX の場合) 300
インストールとセットアップ (Windows の場合) 30
参照・操作制限の設定 604

し

事象発生元ホストの性能レポートを表示する場合の設定 829
システム環境
構築 (UNIX の場合) 302
構築 (Windows の場合) 33
システム監視オブジェクト
作成例 (JP1/AJS のジョブネット監視) 656
システム構成情報反映方式の設定 528
システム構成定義情報の削除 (UNIX の場合) 338
システム構成定義情報の削除 (Windows の場合) 78
システム構成定義情報の設定 (UNIX の場合) 337
システム構成定義情報の設定 (Windows の場合) 77
システム構成定義情報の変更 (UNIX の場合) 338
システム構成定義情報の変更 (Windows の場合) 78
システム構成の設定 (IM 構成管理を使用する場合)
仮想化システム構成の管理および監視のための設定 (Windows の場合) 76
システム構成の設定 (IM 構成管理を使用する場合) (UNIX の場合)
IM 構成管理・ビューアーによるシステム構成の設定 (UNIX の場合) 333

システム構成の設定 (IM 構成管理を使用する場合) (Windows の場合)

IM 構成管理・ビューアーによる設定 (Windows の場合) 73
エクスポート・インポート機能による設定 (Windows の場合) 76

システムの階層構成の反映応答待ちタイムアウト時間 134

システムの状態に応じた対処アクションの提案機能 515

システムログ (syslog) に出力するメッセージの抑止 367

自動アクション

実行環境の設定をする 555
実行状況監視の設定をする 557
実行条件の設定をする 556
実行内容の設定をする 556
実行抑止の設定をする 558
設定する 555

自動アクション定義ファイルの更新 128, 375

自動アクションの送信メールからモニター画面を表示するための設定 827

自動起動 (UNIX の場合) 357

自動終了 (UNIX の場合) 357

自動生成ダッシュボードをカスタマイズする 531

重大度変更機能の設定 581

集約

繰り返しイベントの集約設定 593

重要イベントフィルター

設定する 543

障害発生時の資料採取の準備 123, 368

状態変更イベント

状態変更イベント件数の上限監視の設定 638

証明書を組み込む 445

新規に通信暗号化機能を使用する 811

せ

正規表現

選択 (設定) 555

セキュリティ製品の除外設定 (UNIX の場合) 328

セキュリティ製品の除外設定 (Windows の場合) 67

設定済みの証明書を変更する 816

設定する

JP1/Base の障害に備えた設定 (UNIX の場合)
332

JP1/Base の障害に備えた設定 (Windows の場合) 72

JP1/IM - Manager の障害に備えた設定 (UNIX の場合) 368

JP1/IM - Manager の障害に備えた設定
(Windows の場合) 123

JP1/IM - View の障害に備えた設定 (Windows の場合) 132

JP1/IM - View の動作 (Windows の場合) 132

JP1/IM のイベント取得時の動作設定 535

JP1/IM の各プログラムのアンインストール (UNIX の場合) 411

JP1/IM の各プログラムのアンインストール
(Windows の場合) 288

JP1/IM の各プログラムのインストール (UNIX の場合) 304

JP1/IM の各プログラムのインストール (Windows の場合) 35

JP1 イベント受信時に監視オブジェクトを初期化するための設定 640

JP1 イベントの対処済み時に状態変更イベントを自動で削除する 639

JP1 イベントのフィルタリング 538

SELinux に関する設定 (UNIX の場合) 363

WWW ブラウザーの起動パス 133

イベントガイド機能 568

[イベントコンソール] 画面起動時の [アクション
結果一覧] 画面起動可否 133

[イベントコンソール] 画面起動時の [統合機能メ
ニュー] 画面起動可否 133

イベントサービス機能 (JP1/Base) (UNIX の場合) 340

イベントサービス機能 (JP1/Base) (Windows の場合) 80

イベント取得フィルター 545

イベント取得フィルターの位置の変更 374

インテリジェント統合管理基盤の機能を使用するための設定 (UNIX の場合) 359

インテリジェント統合管理基盤の機能を使用するための設定 (Windows の場合) 107

ガイド情報の編集 635

カスタマイズした監視ツリーをマネージャーへ反映
624

カスタマイズした監視ツリーをローカルホストへ
保存 624

カスタマイズした [ビジュアル監視] 画面をマネー
ジャーへ反映 632

カスタマイズした [ビジュアル監視] 画面をローカ
ルホストへ保存 631

監視オブジェクト DB の自動バックアップ・リカバ
リー 126, 373

[監視ツリー] 画面のツールバーのカスタマイズ 641

監視ツリーから監視ノードの削除 620

監視ツリーでの監視ノードの検索 624

監視ツリーでの監視ノードの属性 617

監視ツリーのカスタマイズ 614

監視ツリーの監視ノードの移動 621

監視ツリーの自動生成 612

監視ツリーの編集画面の起動 609

監視ツリーへの監視ノードの追加 615

監視ノードのアイコンの移動を抑止するための設定
644

監視ノード名および監視ノードアイコン余白の表示
を抑止するための設定 641

監視ノード名の状態色および監視ノードの状態色の
設定 643

監視範囲 622

既存の監視ツリーの取得 611

既存の [ビジュアル監視] 画面の取得 627

クラスタ運用環境 (UNIX の場合) 742

クラスタ運用環境 (Windows の場合) 684

クラスタ運用環境の設定変更 (UNIX の場合) 782

クラスタ運用環境の設定変更 (Windows の場合)
728

クリップボードへのコピー可否 133

コマンド実行環境 (JP1/Base) (UNIX の場合)
345

- コマンド実行環境 (JP1/Base) (Windows の場合) 85
- サービスの起動順序 (JP1/Base) (Windows の場合) 68
- 自動アクション 555
- 自動アクション機能の実行環境 555
- 自動アクションの実行条件および実行内容 556
- 自動起動 (UNIX の場合) 357
- 自動終了 (UNIX の場合) 357
- 重要イベントフィルター 543
- 状態変更イベント件数の上限監視 638
- 状態変更条件メモリー常駐機能 640
- 資料採取の準備 123, 368
- セントラルコンソール 534
- セントラルスコープ 606
- セントラルスコープの機能を使用するための設定 (UNIX の場合) 363
- セントラルスコープの機能を使用するための設定 (Windows の場合) 122
- セントラルスコープの動作環境 638
- 関連イベント発行の設定 563
- 対処状況変更時の JP1 イベントの発行 571
- 対処済み連動機能 638
- 統合機能メニュー 598
- バージョンアップ時 (UNIX の場合) 374
- バージョンアップ時 (Windows の場合) 127
- ビジュアルアイコン 622
- [ビジュアル監視] 画面からの監視ノードの削除 630
- [ビジュアル監視] 画面の一覧の編集および削除 633
- [ビジュアル監視] 画面のカスタマイズ 627
- [ビジュアル監視] 画面の編集画面の起動 626
- [ビジュアル監視] 画面への監視ノードの追加 629
- 表示フィルター 538
- プライマリー認証サーバの設定情報のコピー (JP1/Base) (UNIX の場合) 331
- プライマリー認証サーバの設定情報のコピー (JP1/Base) (Windows の場合) 70
- プロセス異常検知時の JP1 イベントの発行 125, 372
- プロセス異常終了時の再起動 124, 371
- ヘルスチェック機能 125, 372
- ホスト情報 608
- メモ情報の設定 567
- モニター起動 595
- ユーザー認証 (JP1/Base) (UNIX の場合) 329
- ユーザー認証 (JP1/Base) (Windows の場合) 69
- ユーザーフィルター 541
- ユーザーマッピング (JP1/Base) (UNIX の場合) 329
- ユーザーマッピング (JP1/Base) (Windows の場合) 69
- 連携製品のセットアップ (セントラルスコープ用) 646
- [ログイン] 画面の接続先ホスト入力履歴数 132
- ログインユーザーごとの JP1/IM - View の設定 592
- 設定ファイルの編集内容を反映する (エージェント構成) 482
- 設定ファイルの編集内容を反映する (リモート監視構成) 494
- セットアップ
 - JP1/IM - Agent (UNIX の場合) 380
 - JP1/IM - Agent (Windows の場合) 136
 - JP1/IM - Manager (UNIX の場合) 357
 - JP1/IM - Manager (Windows の場合) 106
 - 作業の流れ (UNIX の場合) 300
 - 作業の流れ (Windows の場合) 30
- セットアップ
 - JP1/IM - View 132
- セットアッププログラムの実行
 - JP1/IM - Manager (UNIX の場合) 357
- 前提プログラム
 - インストール (UNIX の場合) 302
 - インストール (Windows の場合) 34
- セントラルコンソール
 - 設定 534
- セントラルコンソール・ビューアーおよびセントラルスコープ・ビューアーの動作カスタマイズ (Windows の場合) 132
- セントラルスコープ

環境設定の概要 607
環境設定を始める前に 607
機能を使用するための設定 (UNIX の場合) 363
機能を使用するための設定 (Windows の場合) 122
設定 606
動作環境の設定 638
バージョンアップコマンドの実行 127, 374
ホスト情報の登録 608
連携製品のセットアップ 646
セントラルスコープで業務グループを監視する 471
セントラルスコープの監視ツリーに業務グループ情報および監視グループ情報を反映する 472

そ

関連イベントの発行
サービスの起動設定 563
設定する 563
発行定義の作成および反映 565
発行履歴ファイルのサイズおよび面数の設定 563
関連イベント発行機能の起動オプションの設定 564

た

対処状況の変更
対処状況変更時の JP1 イベント発行の設定 571
対処済み連動
設定する 638
ダイレクトアクセス URL の設定 520
[ダッシュボード] 画面を共有する 532
ダッシュボードの設定 531
ダッシュボードを削除する 532
ダッシュボードを新規に作成する 531
ダッシュボードを編集する 532

ち

注意事項
クラスタ運用時 (UNIX の場合) 786
クラスタ運用時 (Windows の場合) 733
構成定義情報の設定 (UNIX の場合) 338
構成定義情報の設定 (Windows の場合) 78

注意事項 (UNIX の場合)
アンインストール 415
インストール 313
注意事項 (Windows の場合)
アンインストール 292
インストール 49

つ

通信
JP1/Base による通信の制御 791
ポート番号, IP アドレス, アドレス変換 (NAT) の対応 803
通信暗号化機能が正しく設定できているか確認する 822
通信暗号化機能の使用を中止する 818
通信方式の設定 (クラスタシステム) 682, 740

と

統合エージェントホストでの JP1/Agent の新規インストール (Windows の場合) 701
統合エージェントホストでの JP1/Agent の新規インストール (UNIX の場合) 756
統合エージェントホストでの JP1/IM - Agent の新規インストール時のセットアップ (UNIX の場合) 758
統合エージェントホストでの JP1/IM - Agent の新規インストール時のセットアップ (Windows の場合) 702
[統合オペレーション・ビューアー] 画面
Web ブラウザーの設定手順 530
統合監視 DB の設定 (UNIX の場合) 321
統合監視 DB の設定 (Windows の場合) 60
統合機能メニュー
設定する 598
連携製品の GUI を起動するための設定 598
連携製品の WWW ページを起動するための設定 603
[統合機能メニュー] 画面
起動する画面の決定 599
新規メニューの追加手順 599
定義ファイルを作成する 600

[統合機能メニュー] 画面から JP1/AJS の画面を起動するための設定 827

[統合機能メニュー] 画面から JP1/PFM の画面を起動するための設定 829

[統合機能メニュー] 画面起動可否の設定 133

に

認証サーバの指定 (UNIX の場合) 330

認証サーバの指定 (Windows の場合) 70

ね

ネットワーク

ネットワーク構成に応じた運用と環境構築 790

ファイアウォール環境での運用 797

複数ネットワークでの運用 792

は

バージョンアップインストール時の共通定義情報のコピー (UNIX の場合) 777

バージョンアップインストール時の共通定義情報のコピー (Windows の場合) 722

バージョンアップインストール時の論理ホスト環境 (実行系) のセットアップ (UNIX の場合) 776

バージョンアップインストール時の論理ホスト環境 (実行系) のセットアップ (Windows の場合) 721

バージョンアップ時の設定 (UNIX の場合) 374

バージョンアップ時の設定 (Windows の場合) 127

バージョン情報の表示 310

パケット・フィルタリング 797

発生元ホストのマッピングの設定 588

バリアブルバインディング

JP1 イベントに取り込む 649

汎用監視オブジェクト

作成例 (HiRDB の監視) 662

作成例 (JP1/Cm2/SSO による Cosminexus 業務のリソース監視) 668

作成例 (JP1/Cm2/SSO による CPU 監視) 657

ひ

非クラスタシステム

論理ホスト運用の注意事項 (UNIX の場合) 789

論理ホスト運用の注意事項 (Windows の場合) 736

論理ホストの運用と環境構築 (UNIX の場合) 788

論理ホストの運用と環境構築 (Windows の場合) 735

論理ホストを運用する場合の環境設定 (UNIX の場合) 788

論理ホストを運用する場合の環境設定 (Windows の場合) 735

論理ホストを運用する場合の構成の検討 (UNIX の場合) 788

論理ホストを運用する場合の構成の検討 (Windows の場合) 735

ビジュアル監視

GUI で作成する 626

一覧の編集および削除 633

カスタマイズ 627

カスタマイズした画面をマネージャーへ反映 632

カスタマイズした画面をローカルホストへ保存 631

既存の設定を取得する 627

編集画面の起動 626

[ビジュアル監視] 画面からの監視ノードの削除 630

[ビジュアル監視] 画面の背景画像の設定 628

[ビジュアル監視] 画面への監視ノードの追加 629

表示フィルター

削除する 541

新規に作成する 538

設定する 538

変更する 540

表示メッセージ変更機能の設定 584

[表示メッセージ変更定義設定] 画面から設定する手順 584

表示メッセージ変更定義ファイルから設定する手順 586

ふ

ファイアウォール

JP1/IM の通信 803

JP1 の通信設定 803

NAT 801

基礎知識 797

パケット・フィルタリング 797

ファイアウォール環境での運用 797

ファイルでの設定変更 (UNIX の場合) 782

ファイルでの設定変更 (Windows の場合) 728

フィルター

設定する 538

フェールオーバー 676

複数 LAN 対応

通信設定 792

複数ネットワークでの運用 792

物理ホスト 677

物理ホスト環境の前提条件 (クラスタシステム)
678

プライマリー認証サーバ

設定情報のコピー (UNIX の場合) 331

設定情報のコピー (Windows の場合) 70

プロセス異常検知時の JP1 イベントの発行の設定
125, 372

プロセス異常終了時の再起動の設定 124, 371

プロファイルの管理

収集する 476

設定ファイルを編集する (エージェント構成) 481

設定ファイルを編集する (リモート監視構成) 493

表示する (エージェント構成) 477

表示する (リモート監視構成) 492

プロファイルリストを収集する (エージェント構成)
474

プロファイルを削除する (エージェント構成) 480

プロファイルを削除する (リモート監視構成) 491

プロファイルを追加する (エージェント構成) 479

プロファイルを追加する (リモート監視構成) 490

プロファイルを追加または削除する (エージェント構成)
478

プロファイルを追加または削除する (リモート監視構成)
490

へ

ヘルスチェック機能

設定 125, 372

ほ

ポート番号 (JP1/IM の通信) 803

ほかの JP1 製品と連携するための設定 824

ホスト情報

登録 608

保存した CSV ファイルを編集して [監視ツリー] 画面
を作成 634

ま

マッピング

発生元ホスト 588

マップ表示設定 621

マニュアルの組み込み手順 (UNIX の場合) 410

マニュアルの組み込み手順 (Windows の場合) 286

め

メモ情報の設定 567

も

モニター画面

定義ファイルの作成 596

呼び出しをするための画面の決定 596

呼び出すための設定手順 595

モニター起動

設定する 595

モニター起動で JP1/AJS の画面を起動するための設定
827

モニター起動で JP1/PPM の画面を起動するための
設定 829

ゆ

ユーザー独自のイベント属性

定義ファイルを作成する 577

定義ファイルを有効にする 580

表示する手順 575

ユーザー独自のイベント属性 (拡張属性の固有情報)
を表示する手順 575

ユーザー認証

設定 (UNIX の場合) 329

設定 (Windows の場合) 69

ユーザーフィルター

削除する 543

新規に作成する 541

設定する 541

変更する 542

ユーザーマッピング

設定 (UNIX の場合) 329

設定 (Windows の場合) 69

ユーザーマッピングの設定 (UNIX の場合) 331

ユーザーマッピングの設定 (Windows の場合) 71

り

リモートインストール (UNIX) 307

リモートインストール (Windows) 47

リモート監視が停止中のログの監視設定 129, 377

リモート監視構成のホストにプロファイルを設定する 489

リモートの監視対象ホストでログ監視をするための設定 (UNIX の場合) 349

リモートの監視対象ホストでログ監視をするための設定 (Windows の場合) 89

れ

連携製品

モニター起動の設定 595

連携製品のセットアップ (セントラルスコープ用) 646

ろ

ローカルに保存した監視ツリー (CSV ファイル) の取得 611

ローカルに保存した [ビジュアル監視] 画面 (CSV ファイル) の取得 627

ログイン JP1 ユーザー名の表示を抑止 133

ログイン JP1 ユーザー名の表示を抑止する 132, 134

[ログイン] 画面の接続先ホスト入力履歴数の設定 132

ログイン情報の保持 610

ログイン時のイベント取得範囲を指定してイベントを表示する 536

ログインユーザーごとの JP1/IM - View の設定 592

[ログファイルトラップサービスが起動したときに自動でプロセス起動する] チェックボックスの表示 129, 377

ログファイルトラップを起動する 486

ログファイルトラップを起動または停止する 486

ログファイルトラップを停止する 487

論理 IP アドレス 676

前提条件 677

論理ホスト 676

クラスタソフトに登録するスクリプトの作成 (UNIX の場合) 769

クラスタソフトへの登録 (Windows の場合) 716

削除 (UNIX の場合) 778

削除 (Windows の場合) 723

新規インストール・セットアップ (UNIX の場合) 744

新規インストール・セットアップ (Windows の場合) 686

バージョンアップインストール・セットアップ (UNIX の場合) 773

バージョンアップインストール・セットアップ (Windows の場合) 718

リソースの起動停止順序の設定 (UNIX の場合) 772

リソースの起動停止順序の設定 (Windows の場合) 717

論理ホスト環境の前提条件 677

論理ホストのアンインストール (UNIX の場合) 778

論理ホストのアンインストール (Windows の場合) 723

 株式会社 日立製作所

〒100-8280 東京都千代田区丸の内一丁目6番6号
