

JP1 Version 13

JP1/Integrated Management 3 - Manager 運用ガイド

3021-3-L04-10

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 13-01

製品構成一覧および内訳形名

P-CC2A2C-9MDL JP1/Integrated Management 3 - Manager 13-01 (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 13-01 (適用 OS: Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-01 (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 13-00 (適用 OS: Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-00 (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 13-00 (適用 OS: AIX)

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

P-842C-8EDL JP1/Integrated Management 3 - Manager 13-01

製品構成一覧および内訳形名

P-CC842C-9MDL JP1/Integrated Management 3 - Manager 13-01 (適用 OS: Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, Amazon Linux 2023)

P-CC9W2C-9MDL JP1/Integrated Management 3 - Manager 13-01 (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 13-01 (適用 OS: Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-01 (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 13-00 (適用 OS: Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-00 (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 13-00 (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

HITACHI, AOMPLUS, AOMPLUSCIF, Cosminexus, HiRDB, JP1, uCosminexus は、株式会社日立製作所の商標または登録商標です。

Active Directory は、マイクロソフト 企業グループの商標です。

AIX は、世界の多くの国で登録された International Business Machines Corporation の商標です。

BSAFE は、Dell Inc. またはその子会社の商標です。

Docker および Docker ロゴは、Docker Inc. の米国およびその他の国における商標もしくは登録商標です。

Hyper-V は、マイクロソフト 企業グループの商標です。

Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標です。

Microsoft は、マイクロソフト 企業グループの商標です。

Oracle(R), Java 及び MySQL は、Oracle, その子会社及び関連会社の米国及びその他の国における登録商標です。

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries.

Red Hat は、米国およびその他の国における Red Hat, Inc.の登録商標です。

Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc. in the United States and other countries.

Red Hat Enterprise Linux は、米国およびその他の国における Red Hat, Inc.の登録商標です。

Ruby は、Advanced Micro Devices, Inc.の商標です。

SAP, および本文書に記載されたその他の SAP 製品, サービス, ならびにそれぞれのロゴは、ドイツおよびその他の国々における SAP SE の商標または登録商標です。

UNIX は、The Open Group の登録商標です。

Windows は、マイクロソフト 企業グループの商標です。

Windows Server は、マイクロソフト 企業グループの商標です。

その他記載の会社名、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。

本製品は、米国 Dell Inc.の Dell BSAFE(TM)ソフトウェアを搭載しています。

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/>).

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 64-bit
	Windows(R) 11 Home 64-bit
	Windows(R) 11 Pro 64-bit
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
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

2024年3月 3021-3-L04-10

■ 著作権

Copyright (C) 2023, 2024 Hitachi, Ltd.

Copyright (C) 2023, 2024 Hitachi Solutions, Ltd.

変更内容

変更内容(3021-3-L04-10) JP1/Integrated Management 3 - Manager 13-01

追加・変更内容	変更箇所
JP1/IM - Agent による性能監視機能に、Oracle Database 監視機能 (OracleDB exporter) を追加した。 これに伴い、OracleDB exporter の運用に関する説明を追加した。	1.1.2(1)(d), 1.1.2(2)(d), 10.4, 10.4.1, 12.4.2(1) (a), 12.4.2(2)(a)
JP1/IM - Agent による性能監視機能に、AIX 性能情報収集機能 (Node exporter for AIX) を追加した。 これに伴い、Node exporter for AIX の運用に関する説明を追加した。	1.1.2(1)(d), 1.1.2(2)(d), 10.4, 10.4.2, 12.4.2(1)(f), 12.4.2(2)(f)
「IM エクスポート」の章および用語を削除し、次の機能に関する説明を、JP1/IM - Agent または JP1/IM - Manager の説明個所に統合した。 <ul style="list-style-type: none">• Windows プロセス情報収集機能 (Windows exporter)• Linux プロセス情報収集機能 (Process exporter)• Azure monitor 性能情報収集機能 (Promitor)• UAP 監視機能 (Script exporter)• ログメトリクス機能 (Fluentd)• コンテナ監視機能	10.1, 12.5.1(5), 12.5.1(9), 12.5.1(10), 12.5.1(11)(a), 12.5.1(11) (b), 12.5.2(10), 12.5.2(11), 12.5.3(82), 12.5.3(83)
SAP システムのシステムログ情報および CCMS アラート情報を監視する機能を追加した。 これに伴い、SAP システム監視の運用に関する説明を追加した。	12.4.2(1)(a), 12.4.2(1)(b), 12.4.2(2)(a), 12.4.2(2)(b)
JP1/IM - Agent による性能監視機能に、Windows および Linux のサービス監視機能を追加した。 これに伴い、サービス監視機能を使用する場合の運用に関する説明を追加した。	12.4.2(1)(a), 12.4.2(1)(b), 12.4.2(2)(a), 12.4.2(2)(b), 12.5.1(4), 12.5.1(6)
統合オペレーション・ビューアーのツリーに監視対象の IM 管理ノードが表示されない場合の 主な要因と対処方法を追加した。	12.5.3(70)
エージェントとして AIX 版の JP1/Base を追加した。	—
次の適用 OS を追加した。 <ul style="list-style-type: none">• Amazon Linux 2023	—

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 の運用方法, 操作方法, トラブルシューティングなど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 を使って管理, 運用, 操作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したいシステム管理者
- システムを管理するインフラの状態をシステムで発生する事象と関連づけて一元監視したいシステム管理者
- 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, 次に示す編から構成されています。

第 1 編 運用編

JP1/Integrated Management のシステムを維持するために必要な作業, およびシステムの評価方法について説明しています。

第 2 編 操作編

JP1/Integrated Management を使った監視業務の操作方法について説明しています。

第 3 編 他製品との連携編

統合管理製品以外の他製品と連携した監視業務の概要, 連携機能, 監視環境の構築方法, 操作方法, 連携時の画面, および連携時に使用できるコマンドオプションについて説明しています。

第 4 編 トラブルシューティング編

JP1/Integrated Management でトラブルが発生した場合の対処方法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、システム的设计・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。
[] + []	キーを同時に押すことを示す。

記号	意味
	例 [Ctrl] + [C] キー 上記の例では、[Ctrl] キーと [C] キーを同時に押すことを示す。

■ 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。
…または…	この記号の直前に示された項目を繰り返して複数個、指定できる。 例 「A, B, …」は「A のあとに B を必要個数指定する」ことを示す。
— (下線)	括弧内のすべてを省略したときに、システムがとる標準値を示す。標準値がない場合は、指定した項目だけが有効である。 例 「 <u>A</u> B」はこの項目を指定しなかった場合に、A を選択したと見なすことを示す。
△	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。

●コンピュータ (端末) ●コンピュータ



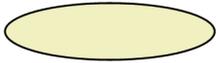
●ディスク装置,
ファイル



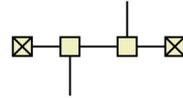
●画面



●WAN



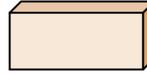
●ネットワーク



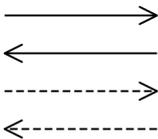
●通信回線



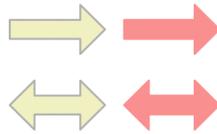
●プログラム



●制御の流れ



●データの流れ



●工程, 作業項目の
流れ



●障害



■ 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\jplima
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	7
はじめに	8

第1編 運用編

1	JP1/IM システムのメンテナンス	22
1.1	設定情報の管理	23
1.1.1	JP1/IM - Manager のバックアップとリカバリー	24
1.1.2	JP1/IM - Agent のバックアップとリカバリー	40
1.2	データベースの管理	52
1.2.1	データベースの再編成	52
1.2.2	データベースのバックアップおよびリカバリー	54
1.2.3	データベースの再作成および設定変更	65
1.3	ディスク容量の管理	79
1.3.1	データベース容量の管理	79
1.3.2	ログファイル容量の管理	82
1.3.3	ダンプファイルの管理	86
1.4	履歴レポートの活用	87
1.4.1	イベントの CSV 出力	87
1.4.2	関連イベントの発行履歴	87
1.4.3	共通除外条件の除外履歴および定義履歴	88
1.5	設定情報および DB の移行	89
1.5.1	移行の対象となる設定情報および DB	89
1.6	通信暗号化機能の証明書の管理	95
1.6.1	サーバ証明書の有効期限の管理	95
1.6.2	キーストアの管理	95
2	JP1/IM システムの構成変更	97
2.1	JP1/IM の設定情報の変更	98
2.1.1	統合エージェントホストの JP1/IM - Agent の設定変更	98
2.1.2	統合マネージャーホストの JP1/IM - Agent の設定変更	99
2.2	ホスト名を変更する場合に必要な作業	100
2.2.1	エージェントとして JP1/IM - Agent を使用している場合	100
2.2.2	エージェントとして JP1/Base を使用している場合	106

2.2.3	メールサーバのホスト名を変更した場合の作業	109
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	109
2.3	IP アドレスを変更する場合に必要な作業	111
2.3.1	エージェントとして JP1/IM - Agent を使用している場合	111
2.3.2	エージェントとして JP1/Base を使用している場合	113
2.3.3	メールサーバの IP アドレスを変更した場合の作業	114
2.4	マネージャーおよびエージェントの日時を変更した場合に必要な作業	116
2.4.1	マネージャーおよびエージェントの日時を過去に戻す	116
2.4.2	システムの時刻を進める	120
2.5	統合エージェントホストのシステム日時を変更する場合に必要な手順	121
2.5.1	統合エージェントホストのシステム日時を変更する	121
2.5.2	クラスタシステムでシステム日時を変更する	121
2.5.3	コンテナでシステム日時を変更する	122
2.6	リモート監視構成の監視対象ホストの日時を変更した場合に必要な作業	123
2.6.1	リモート監視構成の監視対象ホストの日時を過去に戻す	123
2.6.2	リモート監視構成の監視対象ホストの日時を進める	123
2.7	リモート監視構成の監視対象ホストのパスワードを変更した場合に必要な作業	124
2.8	リモート監視構成からエージェント構成に監視構成を変更する場合の注意事項	125
2.8.1	JP1/Base のログファイルトラップでの注意事項	125
2.8.2	JP1/Base のイベントログトラップでの注意事項	125
2.9	ポート番号を変更する場合に必要な手順	126
2.10	統合エージェントホストのロケールを変更する場合に必要な作業	127
2.10.1	統合エージェントホストのロケールを変更する	127
2.10.2	クラスタシステムでロケールを変更する	128
2.10.3	コンテナでロケールを変更する	128
2.11	統合エージェントホストの複製	129
2.11.1	物理ホストの複製	129
2.11.2	運用開始後の AWS/EC2 インスタンスの複製	129

第 2 編 操作編

3	JP1/IM - Manager の起動と終了	131
3.1	JP1/IM - Manager を起動する	132
3.1.1	Windows の場合	132
3.1.2	UNIX の場合	134
3.1.3	クラスタシステムで運用する場合	136
3.1.4	非クラスタシステムで論理ホストを運用する場合	136
3.2	JP1/IM - Manager を終了する	138
3.2.1	Windows の場合	138

- 3.2.2 UNIX の場合 138
- 3.2.3 クラスタシステムで運用する場合 140
- 3.2.4 非クラスタシステムで論理ホストを運用する場合 140
- 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 141
- 3.3.1 非クラスタシステムの論理ホスト運用で自動起動および自動停止を設定する (Windows の場合) 141
- 3.3.2 非クラスタシステムの論理ホスト運用で自動起動および自動停止を設定する (Linux の場合) 142
- 3.3.3 物理ホストおよび論理ホストの両方で自動起動および自動停止をする場合の設定 143
- 3.4 起動と終了に関する注意事項 145

- 4 JP1/IM - Manager へのログインとログアウト 148**
- 4.1 JP1/IM - Manager にログインする 149
 - 4.1.1 JP1/IM - Manager (インテリジェント統合管理基盤) に WWW ブラウザーでログインする 149
 - 4.1.2 JP1/IM - Manager に GUI でログインする 150
 - 4.1.3 JP1/IM - Manager にコマンドでログインする 151
- 4.2 JP1/IM - Manager からログアウトする 153

- 5 インテリジェント統合管理基盤によるシステムの監視 154**
- 5.1 システムの状態の見方 155
 - 5.1.1 インテリジェント統合管理基盤で監視できるもの 155
 - 5.1.2 サンバーストまたはツリーの表示項目 156
- 5.2 JP1 イベントの見方 ([イベント一覧] 画面) 158
 - 5.2.1 イベント一覧の表示項目 159
 - 5.2.2 [繰り返しイベント一覧] 画面を表示する 161
 - 5.2.3 JP1 イベントの詳細情報を表示する 162
- 5.3 トレンド表示とアラートで扱うメトリックの追加 164
- 5.4 ダッシュボードの見方 166
 - 5.4.1 ダッシュボードを表示する 166
 - 5.4.2 IM 管理ノード状態の監視 167
 - 5.4.3 アラート情報の監視 169
 - 5.4.4 各種 IT リソースの確認 170
 - 5.4.5 ダッシュボードを起点とした問題調査・対処の流れ 170
 - 5.4.6 注意事項 174
- 5.5 他製品との連携の見方 176
 - 5.5.1 予兆によって障害を回避する (JP1/AJS 連携) 176
 - 5.5.2 ジョブの運用中に発生した問題の影響範囲を把握し対処する (JP1/AJS 連携) 176
 - 5.5.3 ジョブの定義や内容を変更する場合に影響を受けるルートジョブネットを事前に把握する (JP1/AJS 連携) 177
 - 5.5.4 性能情報を確認して対処する (JP1/PFM 連携) 177
 - 5.5.5 提案を確認して対処する 177
 - 5.5.6 OIDC 認証している外部製品と連携してシングルサインオンする 179

5.5.7	ダイレクトアクセス URL で情報を共有する	180
5.6	インテリジェント統合管理基盤の運用上の注意事項	181
5.6.1	JP1/AJS と連携した場合の注意事項	181
5.6.2	ユーザーフィルターを使用する場合の注意事項	183
6	セントラルコンソールによるシステムの監視	185
6.1	JP1 イベントの見方	186
6.1.1	イベント一覧の表示項目	186
6.1.2	[イベントコンソール] 画面のイベント一覧に表示されるイベント	190
6.1.3	フィルターの適用	194
6.2	JP1 イベントの詳細情報を表示する	196
6.2.1	JP1 イベントのメモ情報を編集する	198
6.3	JP1 イベントの対処状況を設定する	200
6.3.1	JP1 イベントの対処状況の設定について	200
6.3.2	イベント一覧から JP1 イベントの対処状況を設定する	201
6.3.3	[重要イベント] ページから重要イベントを削除する	201
6.4	[関連イベント一覧] 画面から JP1 イベントを操作する	203
6.4.1	繰り返しイベントの詳細情報を確認し対処状況を変更する	203
6.4.2	関連イベントの詳細情報を確認し対処状況を変更する	204
6.5	JP1/IM のフィルターを適用する	208
6.5.1	表示フィルターを有効にして特定の JP1 イベントだけを表示する	208
6.5.2	重要イベントだけを表示する	208
6.5.3	適用するイベント取得フィルターを切り替える	209
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	214
6.6	表示開始位置を指定してイベントを表示する	216
6.7	表示する JP1 イベントの期間を指定して絞り込む	218
6.8	JP1 イベントを検索する	220
6.8.1	検索の方法	220
6.8.2	検索結果の表示	223
6.9	JP1 イベントの情報を運用に合わせてカスタマイズする	226
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)	226
6.9.2	JP1 イベントの固有の拡張属性を表示する (イベント情報のマッピング)	226
6.9.3	条件に一致する JP1 イベントにユーザー独自の固有の拡張属性を付加する	230
6.9.4	JP1 イベントの重大度を変更する	231
6.9.5	JP1 イベントの表示メッセージを変更する	234
6.10	イベントの大量発生に対処する	239
6.10.1	イベントの大量発生に対処する場合と備える場合の流れ	239
6.10.2	エージェントからのイベント転送を抑制するための準備をする	241
6.10.3	エージェントからのイベント転送を抑制してイベントの大量発生に対処する	244

- 6.10.4 イベントをマネージャーで集約してイベントの大量発生に対処する 248
- 6.10.5 イベント転送を自動で抑止するためのしきい値をエージェントに設定する 250
- 6.10.6 繰り返しイベント条件を設定する 250
- 6.10.7 イベントを大量に発行しているログファイルトラップをマネージャーから停止する 257
- 6.10.8 同じ属性のイベントが連続して発生した場合の集約表示について 258
- 6.11 他製品と連携して JP1 イベントに対処する 260
- 6.11.1 JP1 イベントをインシデントとして JP1/Service Support に登録する (JP1/Service Support 連携) 260
- 6.11.2 JP1 イベントに対応する運用手順を表示する (JP1/Navigation Platform 連携) 261
- 6.11.3 JP1 イベントを発行したアプリケーションをモニター起動する 261
- 6.11.4 JP1 イベントに対応する性能レポートを表示する (JP1/PFM 連携) 263
- 6.12 セントラルコンソールの注意事項 264
- 6.13 セントラルコンソール・ビューアーの運用上の注意事項 265

7 セントラルスコープによるシステムの監視 267

- 7.1 [監視ツリー] 画面で監視する 268
 - 7.1.1 監視ノードの状態を変更する 268
 - 7.1.2 監視ノードの監視状態を変更する 269
 - 7.1.3 監視ノードを検索する 270
 - 7.1.4 状態変更イベントを検索する 270
 - 7.1.5 監視ノードの属性を表示する 271
 - 7.1.6 ガイド情報を表示する 272
 - 7.1.7 [ビジュアル監視] 画面を表示する 272
 - 7.1.8 ログインユーザーの一覧を表示する 273
 - 7.1.9 [監視ツリー] 画面の情報をローカルホストに保存する 273
- 7.2 [ビジュアル監視] 画面で監視する 274
 - 7.2.1 [ビジュアル監視] 画面から [監視ツリー] 画面を呼び出す 274
 - 7.2.2 監視ノードの状態を変更する 275
 - 7.2.3 監視ノードの監視状態を変更する 275
 - 7.2.4 監視ノードを検索する 276
 - 7.2.5 状態変更イベントを検索する 276
 - 7.2.6 監視ノードの属性を表示する 277
 - 7.2.7 ガイド情報を表示する 277
- 7.3 セントラルスコープの注意事項 279

8 JP1/IM によるシステムの操作 284

- 8.1 コマンドを実行する 285
 - 8.1.1 [実行コマンド] でコマンドを実行する 285
 - 8.1.2 [コマンド] ボタンでコマンドを実行する 287
 - 8.1.3 コマンドを実行するユーザー 290

- 8.1.4 コマンドの実行状態を確認または削除する 290
- 8.2 自動アクションの状況を確認し、自動アクションの操作を行う 292
- 8.2.1 自動アクションの実行状況を確認する 292
- 8.2.2 自動アクションの実行結果を確認する 294
- 8.2.3 自動アクション機能の稼働状況を確認する 300
- 8.3 統合機能メニューで他アプリケーションの画面を表示する 301
- 8.3.1 [統合機能メニュー] 画面の操作 302
- 8.3.2 [統合機能メニュー] 画面から操作できる機能 302

9 IM 構成管理によるシステムの階層構成の管理 306

- 9.1 ホストを管理する 307
- 9.2 システムの階層構成を管理する 308
- 9.3 仮想化システム構成を管理する 310
- 9.3.1 仮想化システムのホストを登録する 310
- 9.3.2 仮想化システムのホスト情報を表示する 310
- 9.3.3 セントラルスコープの監視ツリーへ反映する 311
- 9.4 業務グループを管理する 312
- 9.5 プロファイルを管理する 313
- 9.6 サービスの稼働状況を管理する 315
- 9.6.1 サービスの稼働情報を収集する 315
- 9.6.2 サービスの稼働情報を表示する 316
- 9.7 IM 構成管理の管理情報をエクスポート・インポートする 318
- 9.7.1 IM 構成管理の管理情報をエクスポートする 318
- 9.7.2 IM 構成管理の管理情報をインポートする 322
- 9.7.3 インポートした IM 構成管理の管理情報をシステムに反映する 333
- 9.8 IM 構成管理の注意事項 336

10 JP1/IM - Agent の起動と終了 337

- 10.1 JP1/IM - Agent のサービス 338
- 10.2 サービスの起動 340
- 10.3 サービスの停止 341
- 10.4 JP1/IM - Agent のオプション機能 342
- 10.4.1 OracleDB exporter のサービス 342
- 10.4.2 Node exporter for AIX のサービス 343
- 10.5 クラスタシステムで運用する場合 351
- 10.5.1 サービスの起動 351
- 10.5.2 サービスの停止 351
- 10.5.3 自動起動の設定 351
- 10.5.4 OS シャットダウン時の自動停止 351

第3編 他製品との連携編

- 11 BJEX または JP1/AS との連携 352**
 - 11.1 BJEX または JP1/AS との連携の概要 353
 - 11.1.1 バッチジョブ実行システムと連携する場合のシステム構成 353
 - 11.2 BJEX または JP1/AS 連携用の JP1/IM の機能 356
 - 11.2.1 応答待ちイベントと JP1/IM の関係 356
 - 11.2.2 応答待ちイベントの監視 358
 - 11.2.3 応答待ちイベントの滞留 361
 - 11.2.4 応答待ちイベントへの応答 363
 - 11.2.5 応答待ちイベントのキャンセル 365
 - 11.3 BJEX または JP1/AS と連携するための設定 366
 - 11.3.1 JP1/IM - Manager の設定 366
 - 11.3.2 JP1/IM - View の設定 367
 - 11.3.3 JP1/Base の設定 368
 - 11.3.4 BJEX または JP1/AS と JP1/IM - Manager 間の通信に関する設定 368
 - 11.3.5 BJEX または JP1/AS の設定 370
 - 11.4 応答待ちイベントの操作 371
 - 11.4.1 応答待ちイベントに応答する操作の流れ 371
 - 11.4.2 応答待ちイベントに応答する 374
 - 11.4.3 応答待ちイベントの滞留を手動で解除する 375
 - 11.4.4 応答待ちイベントの滞留状態の監視を復帰させる 375
 - 11.5 BJEX または JP1/AS 連携時のコマンド 376
 - 11.5.1 jcoimdef 376
 - 11.5.2 jim_log.bat (Windows 限定) 376
 - 11.5.3 jim_log.sh (UNIX 限定) 377

第4編 トラブルシューティング編

- 12 トラブルシューティング 378**
 - 12.1 対処の手順 379
 - 12.2 ログ情報の種類 380
 - 12.2.1 JP1/IM - Manager のログ情報 380
 - 12.2.2 JP1/IM - Agent のログ情報 422
 - 12.3 トラブル発生時に採取が必要な資料 429
 - 12.3.1 JP1/IM - Manager に関する資料 429
 - 12.3.2 JP1/IM - Agent に関する資料 459
 - 12.4 資料の採取方法 461
 - 12.4.1 JP1/IM - Manager の資料採取方法 461
 - 12.4.2 JP1/IM - Agent の資料採取方法 474

- 12.5 トラブルシューティング 485
- 12.5.1 障害の切り分け方法 485
- 12.5.2 主な入力ミスに対して発生する現象と回復方法 517
- 12.5.3 主なトラブルと対処方法 520
- 12.5.4 JP1/IM - Agent が JP1/IM - Manager に接続できない場合の対処 609

索引 610

1

JP1/IM システムのメンテナンス

この章では、JP1/IM システムのメンテナンスについて説明します。

システム運用管理の基盤となる JP1/IM を安定して運用するために、定義ファイルのバックアップやデータベースの管理など、定期的にメンテナンス作業を計画してください。

1.1 設定情報の管理

ここでは、JP1 システムのバックアップおよびリカバリーについて説明します。

ディスク障害などが発生してシステムが動作しなくなった場合、JP1/IM で使用する各種のデータが回復できなくなることがあります。このような不測の事態に備えて、定期的に各種のファイルのバックアップを取得しておく必要があります。

ここでの説明を基に、システム全体のバックアップ計画の一環として、JP1 のバックアップ・リカバリーを検討してください。サーバ間での複製およびファイルの移行には使用できません。

バックアップ・リカバリーを実施する際には、バックアップ元とリカバリー先で次のすべてが一致している必要があります。

- ホスト名
- IP アドレス
- PP 形名
- PP バージョン (VVRRZZ の範囲で一致させてください)
- 製品の使用するディレクトリの構成 (権限などを含めて一致させてください)

また、OS、ハードウェアに関しては、同一の動作ができることが前提となります。

上記の条件に一致しない場合は、移行となります。

「[1.5 設定情報および DB の移行](#)」を参照して実施してください。

OS コマンドやバックアップソフトでシステム全体をフルバックアップすることもできますが、OS コマンドやバックアップソフトの動作に依存するため、JP1/IM - Manager では、JP1/IM - Manager の各機能で提供しているコマンドを使用したバックアップ・リカバリーをお勧めします。OS コマンドやバックアップソフトを使用する場合、次の前提条件となります。

- 事前に IM データベースを含む JP1/IM - Manager のすべてのサービスが停止された状態で取得されている。
- OS に登録している情報を含めて、ファイル、レジストリの情報がすべて整合性の取れた状態でバックアップされている。
- 取得されるバックアップ対象のファイルがスパースファイルとなっていない。

定義情報をバックアップ・リカバリーする場合は、データベースも合わせてバックアップ・リカバリーを実施してください。

バックアップ・リカバリー時は、JP1/IM - View を停止してください。

1.1.1 JP1/IM - Manager のバックアップとリカバリー

(1) バックアップ (Windows の場合)

JP1/IM の設定情報のバックアップについて説明します。

JP1/IM の設定を変更した場合に、バックアップを取得してください。JP1/IM のバックアップを取得する場合は、必ず JP1/Base のバックアップを同時に取得してください。JP1/Base のユーザーが設定する定義ファイルのバックアップ方法については、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 - Agent の製品プラグインのバックアップとリカバリーは、JP1/IM - Manager のバックアップとリカバリーに従います。

バックアップは、ファイルをコピーするなど、任意の方法で取得してください。バックアップは、できるだけ JP1/IM のサービスを停止した状態で取得してください。しかたなく実行中に取得する場合は、次の点に注意が必要です。

- 実行中に定義ファイルが書き換えられるケースがあります。ファイルの書き換え中にバックアップすると、ファイルが壊れた状態でバックアップされます。
バックアップ実行直後に、取得したバックアップとバックアップ元のファイルを比較して、内容が一致していることを確認してください。
- バックアップ時には対象ファイルに排他などのロックをしないでください。ロックする場合は、接続しているビューアーをすべてログアウトした状態で対象ファイルを別ファイルにコピーしてください。コピーしたあと、コピーしたファイルとコピー元ファイルを比較して、内容が一致していることを確認してから、コピーしたファイルをバックアップしてください。
- バックアップした設定情報をリストアした場合、リストアする内容で設定を変更するだけであり、JP1/IM - Manager に到着済みのイベントを再評価することはありません。

バックアップは、次の表に示す中で存在するすべてのファイルを一度にバックアップしてください。存在する中で一部のファイルしかバックアップしなかった場合、ほかの定義ファイルとの関連に矛盾が生じて正しく動作しないことがあります。

また、クラスタ運用している場合は、物理ホスト、論理ホストの順番で、各環境をバックアップしてください。

JP1/IM のバックアップ対象ファイルを次に示します。なお、論理ホストの場合は表中の「Console パス」を「共有フォルダ¥JP1Cons」、 「Scope パス」を「共有フォルダ¥JP1Scope」、 「Manager パス」を「共有フォルダ¥JP1IMM」に置き換えてください。

表 1-1 JP1/IM のバックアップ対象ファイル

製品名	ファイル名	内容
各製品共通	マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「7.3.4 JP1/IM - Manager	共通定義情報退避ファイル※ 1

製品名	ファイル名	内容
	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)」で作成した退避ファイル	
JP1/IM - Manager	ユーザー任意のファイル名	<p>通信暗号化機能で使用する秘密鍵 下記の共通定義情報に指定したファイル JP1_DEFAULT¥JP1BASE¥\$SL¥PRIVATEKEYFILE¥※2</p> <p>通信暗号化機能で使用するサーバ証明書 下記の共通定義情報に指定したファイル JP1_DEFAULT¥JP1BASE¥\$SL¥CERTIFICATEFILE¥※2</p> <p>通信暗号化機能で使用するルート証明書 下記の共通定義情報に指定したファイル JP1_DEFAULT¥JP1BASE¥\$SL¥CACERTIFICATEFILE¥※2</p>
JP1/IM - Manager	インテリジェント統合管理基盤	<p>Manager パス¥conf¥imdd¥imdd.properties インテリジェント統合管理基盤定義ファイル</p> <p>Manager パス¥conf¥imdd¥systemnode.conf システムノード定義ファイル</p> <p>Manager パス¥conf¥imdd¥category_name.conf IM 管理ノードカテゴリ名称定義ファイル</p> <p>Manager パス¥conf¥imdd¥target_host.conf 構成取得対象ホスト定義ファイル</p> <p>Manager パス¥conf¥imdd¥imdd_host_name.conf ホスト名定義ファイル</p> <p>Manager パス¥conf¥imdd¥imdd_nodeLink_def.conf IM 管理ノードリンク定義ファイル</p> <p>Manager パス ¥conf¥imdd¥imdd_sso_mapping.properties シングルサインオンマッピング定義ファイル</p> <p>Manager パス¥conf¥imdd¥plugin¥jp1ajs¥*.conf JP1/AJS のプラグイン定義ファイル</p> <p>Manager パス¥conf¥imdd¥plugin¥jp1pfm¥*.conf JP1/PFM のプラグイン定義ファイル</p> <p>Manager パス¥conf¥imdd¥ユーザー作成プラグイン ユーザー作成プラグイン</p> <p>Manager パス¥public¥customUI¥カスタム UI 用ユーザー作成フォルダ カスタム UI 用ファイル格納フォルダ</p>

製品名	ファイル名	内容	
	Manager パス ¥conf¥imdd¥suggestion¥template¥en¥imdd_suggestion_ajs_check_failed_agent_jobnet_en.conf	JP1/AJS の英語版提案テンプレートファイル	
	Manager パス ¥conf¥imdd¥suggestion¥template¥en¥imdd_suggestion_ajs_check_failed_agent_list_en.conf		
	Manager パス ¥conf¥imdd¥suggestion¥template¥en¥imdd_suggestion_pfm_cpu_event_en.conf	JP1/PFM の英語版提案テンプレートファイル	
	Manager パス ¥conf¥imdd¥suggestion¥template¥en¥imdd_suggestion_pfm_set_status_of_events_to_processed_en.conf		
	Manager パス ¥conf¥imdd¥suggestion¥template¥en¥imdd_suggestion_pfm_suspend_monitoring_en.conf		
	Manager パス ¥conf¥imdd¥suggestion¥template¥ja¥imdd_suggestion_ajs_check_failed_agent_jobnet_ja.conf	JP1/AJS の日本語版提案テンプレートファイル	
	Manager パス ¥conf¥imdd¥suggestion¥template¥ja¥imdd_suggestion_ajs_check_failed_agent_list_ja.conf		
	Manager パス ¥conf¥imdd¥suggestion¥template¥ja¥imdd_suggestion_pfm_cpu_event_ja.conf	JP1/PFM の日本語版提案テンプレートファイル	
	Manager パス ¥conf¥imdd¥suggestion¥template¥ja¥imdd_suggestion_pfm_set_status_of_events_to_processed_ja.conf		
	Manager パス ¥conf¥imdd¥suggestion¥template¥ja¥imdd_suggestion_pfm_suspend_monitoring_ja.conf		
	任意のパス¥提案定義ファイル	提案定義ファイル	
	Manager パス ¥conf¥imdd¥responseaction¥autoactconf.json	自動対処アクション定義ファイル	
	Manager パス ¥conf¥imdd¥responseaction¥responseactionnotice.conf	対処アクション状態監視定義ファイル	
	セントラルコンソール	Console パス¥conf¥jp1co_env.conf	IM 環境定義ファイル
		Console パス¥conf¥jp1co_param.conf	IM パラメーター定義ファイル

製品名	ファイル名	内容
	Console パス¥conf¥jp1co_param_V7.conf	IM パラメーター定義ファイル
	Console パス¥conf¥jp1co_service.conf	拡張起動プロセス定義ファイル
	Console パス¥conf¥jp1co_system.conf	IM サーバシステム環境設定ファイル
	Console パス¥conf¥action¥actdef.conf	自動アクション定義ファイル
	Console パス ¥conf¥console¥actprofile¥actprofile_JP1 ユーザー名	アクションプロファイル
	Console パス ¥conf¥console¥actprofile¥actprofile2_JP1 ユーザー名	
	Console パス ¥conf¥console¥actprofile¥actprofile_0950_JP1 ユーザー名	
	Console パス¥conf¥console¥attribute¥*.conf	イベント拡張属性定義ファイル
	Console パス ¥conf¥console¥attribute¥extend¥*.conf	イベント拡張属性定義ファイル (拡張ファイル)
	Console パス¥conf¥console¥filter¥*.conf	フィルター定義ファイル
	Console パス ¥conf¥console¥filter¥attr_list¥common_exclude_filter_attr_list.conf	共通除外条件表示項目定義ファイル
	Console パス ¥conf¥console¥filter¥auto_list¥common_exclude_filter_auto_list.conf	共通除外条件自動入力定義ファイル
	Console パス¥conf¥console¥mapping¥mapping.conf	イベント情報マッピング定義ファイル
	Console パス¥conf¥console¥monitor¥*.conf	モニター画面呼び出し定義ファイル
	Console パス¥conf¥console¥object_type¥*	オブジェクトタイプ定義ファイル
	Console パス¥conf¥console¥profile¥.system	システムプロファイル
	Console パス¥conf¥console¥profile¥defaultUser	JP1/IM - View のユーザープロファイル (デフォルト)
	Console パス¥conf¥console¥profile¥profile_JP1 ユーザー名	JP1/IM - View のユーザープロファイル

製品名	ファイル名	内容
	Console パス %conf%console%profile%systemColor.conf	システムカラー定義ファイル
	Console パス%default%console.conf※3	通信環境定義ファイル
	Console パス %conf%console%correlation%view_cor.conf	繰り返しイベントの集約設定ファイル
	Console パス %conf%console%correlation%view_cor_JP1 ユーザー名.conf	繰り返しイベントの集約設定ファイル
	Console パス%conf%console%rmtcmd%cmdbtn.conf	コマンドボタン定義ファイル
	Console パス%conf%health%jcohc.conf	ヘルスチェック定義ファイル
	Console パス%conf%hostmap%user_hostmap.conf	発生元ホストマッピング定義ファイル
	Console パス%conf%action%actnotice.conf	自動アクション通知定義ファイル
	Console パス %conf%processupdate%processupdate.conf	対処状況イベント定義ファイル
	Console パス%conf%guide%jco_guide.txt	イベントガイド情報ファイル
	Console パス%conf%system%event_storm%*.conf	繰り返しイベント条件定義ファイル
	Console パス %conf%console%event_storm%attr_list%event_storm_attr_list.conf	繰り返しイベント条件表示項目定義ファイル
	Console パス %conf%console%event_storm%auto_list%event_storm_auto_list.conf	繰り返しイベント条件自動入力定義ファイル
	Console パス%conf%console%incident%incident.conf	インシデント手動登録定義ファイル
	Console パス %conf%console%incident%incident_info.conf	インシデント引き継ぎ情報設定ファイル
	ユーザー任意のフォルダ%ユーザー任意のファイル名	イベントガイドメッセージファイル
	Console パス%conf%evgen%以下のすべてのファイル	関連イベント発行用定義ファイル
	ユーザー任意のフォルダ%ファイル名.conf	関連イベント発行定義ファイル
	Console パス %conf%action%attr_list%attr_list.conf	イベント条件表示項目定義ファイル
	Console パス%conf%chsev%jcochsev.conf	重大度変更定義ファイル

製品名	ファイル名	内容	
	Console パス ¥conf¥chsev¥attr_list¥chsev_attr_list.conf	重大度変更定義表示項目定義ファイル	
	Console パス ¥conf¥chsev¥auto_list¥chsev_auto_list.conf	重大度変更定義自動入力定義ファイル	
	Console パス¥conf¥mail¥jimmail.conf	メール環境定義ファイル	
	Console パス¥conf¥chattr¥jcochmsg.conf	表示メッセージ変更定義ファイル	
	Console パス ¥conf¥chattr¥attr_list¥chmsg_attr_list.conf	表示メッセージ変更定義表示項目定義ファイル	
	Console パス ¥conf¥chattr¥auto_list¥chmsg_auto_list.conf	表示メッセージ変更定義自動入力定義ファイル	
	Console パス ¥conf¥console¥performance¥performance.conf	性能レポート表示定義ファイル	
	セントラルス コープ	Scope パス¥conf¥jcs_guide*.txt	ガイド情報ファイル
		Scope パス¥conf¥jcs_hosts	ホスト情報ファイル
		Scope パス¥conf¥action_complete_on.conf	対処済み連動設定ファイル
		Scope パス¥conf¥action_complete_off.conf	
		ユーザー任意のフォルダ¥ユーザー任意のファイル名	状態変更イベント自動削除設定ファイル
		ユーザー任意のフォルダ¥ユーザー任意のファイル名	監視オブジェクト初期化設定ファイル
		Scope パス¥conf¥auto_dbbackup_on.conf	監視オブジェクトDBのバックアップ・リカバリー設定ファイル
		Scope パス¥conf¥auto_dbbackup_off.conf	
		Scope パス¥conf¥evhist_warn_event_on.conf	状態変更イベント件数の上限監視設定ファイル
		Scope パス¥conf¥evhist_warn_event_off.conf	
		ユーザー任意のフォルダ¥ユーザー任意のファイル名	ガイドメッセージファイル
		ユーザー任意のフォルダ¥ユーザー任意のファイル名	状態変更条件メモリー常駐機能の設定ファイル
		IM 構成管理	Manager パス¥conf¥imcf¥jp1cf_applyconfig.conf
	Manager パス ¥conf¥imcf¥jp1cf_treedefaultpolicy.csv		デフォルト監視ポリシー定義ファイル
Manager パス¥conf¥agtless¥targets¥wmi.ini	WMI 認証情報に関する定義ファイル		

製品名		ファイル名	内容
JP1/IM - Agent の製品プラグイン		Manager パス¥conf¥agless¥targets¥ssh.ini	SSH 認証情報に関する定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥aws_settings.conf	AWS 定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥property_labels.conf	プロパティ表示文字列定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_node_exporter.conf	Node exporter のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_windows_exporter.conf	Windows exporter のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_windows_exporter_process.conf	Windows exporter (プロセス監視) のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_blackbox_exporter.conf	Blackbox exporter のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_ya_cloudwatch_exporter.conf	Yet another cloudwatch exporter のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_kubernetes.conf	コンテナ監視のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_fluentd.conf	Fluentd のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_任意のPrometheusトレンド名.conf	ユーザー独自のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_process_exporter.conf	Process exporter のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_promitor.conf	Promitor のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥metrics_script_exporter.conf	Script exporter のメトリック定義ファイル
		Manager パス ¥conf¥imdd¥imagent¥jpc¥imbase.json	imbase 設定ファイル

製品名	ファイル名	内容
	Manager パス %conf%imdd%imagent%jpc_imbaseproxy.json	imbaseproxy 設定ファイル
	Manager パス%conf%imdd%imagent%サーバ証明書ファイル	統合エージェント管理基盤用のサーバ証明書ファイル
	Manager パス%conf%imdd%imagent%サーバ証明書キーファイル	統合エージェント管理基盤用のサーバ証明書キーファイル
JP1/IM - View	View パス%conf%webdata%ja%*.html View パス%conf%webdata%en%*.html View パス%conf%webdata%zh%*.html	WWW ページ呼び出し定義ファイル
	View パス%conf%tuning.conf	IM-View 設定ファイル
	View パス%conf%ssl%nosslhost.conf	非暗号化通信ホスト設定ファイル
	View パス%default%view.conf.update	通信環境定義ファイル
	View パス%default%tree_view.conf.update	
	View パス%conf%sovtool%exec%ja%!JP1_CS_APP0.conf View パス%conf%sovtool%exec%en%!JP1_CS_APP0.conf View パス%conf%sovtool%exec%zh%!JP1_CS_APP0.conf	起動プログラム定義ファイル
	View パス%conf%sovtool%item%ja%!JP1_CS_FT00L0.conf View パス%conf%sovtool%item%en%!JP1_CS_FT00L0.conf View パス%conf%sovtool%item%zh%!JP1_CS_FT00L0.conf	ツールバー定義ファイル
	View パス%conf%sovtool%item%ja%!JP1_CS_FTREE0.conf View パス%conf%sovtool%item%en%!JP1_CS_FTREE0.conf View パス%conf%sovtool%item%zh%!JP1_CS_FTREE0.conf	アイコン動作定義ファイル
	View パス%conf%appexecute%ja%*.conf View パス%conf%appexecute%en%*.conf View パス%conf%appexecute%zh%*.conf	アプリケーション実行定義ファイル
	View パス%conf%function%ja%*.conf View パス%conf%function%en%*.conf View パス%conf%function%zh%*.conf	統合機能メニュー定義ファイル
	ユーザー任意のフォルダ%ユーザー任意のファイル名	ツリー構成ファイル
	View パス%image%icon%以下のファイル	アイコンファイル

製品名	ファイル名	内容
	View パス¥image¥visual¥以下のファイル	ビジュアルアイコンファイル※4
	View パス¥image¥map¥以下のファイル	背景画像ファイル
	View パス¥conf¥jcfview¥jcfview.conf	IM 構成管理・ビューアー動作定義ファイル
	View パス¥conf¥sovsystem¥en¥system.conf	システムプロファイル (セントラルスコープ・ビューアー)
	View パス¥conf¥sovsystem¥ja¥system.conf	
	View パス¥conf¥sovsystem¥zh¥system.conf	

注※1 共通定義情報退避ファイルは、クラスタシステムの論理ホストの定義情報を退避したファイルです。この退避ファイルは、クラスタシステムのセットアップ時に作成します。この退避ファイルには、JP1/IM だけでなく、JP1/Base, JP1/AJS, および 06-02 以降の JP1/Power Monitor の定義情報も退避されます。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「7.1.3(5) 共通定義情報の設定」を参照してください。

注※2 論理ホストの場合は、「JP1_DEFAULT」は論理ホスト名となります。

注※3 物理ホストにだけ存在するファイルです。

注※4 ユーザーによって追加されたファイルが対象となります。

(2) リカバリー (Windows の場合)

JP1/IM の設定情報のリカバリーについて説明します。

JP1/IM のバックアップ情報をリカバリーする場合は、必ず JP1/Base を先にリカバリーしてください。次の前提条件を確認した上で、バックアップファイルを、元の位置にリカバリーしてください。

前提条件

- JP1/Base がインストール済みであること。
- JP1/IM - Manager がインストール済みであること。
- 論理ホスト環境をリカバリーする場合は、論理ホスト環境の JP1 がセットアップ済みであること。
- JP1/Base と JP1/IM - Manager が停止していること。

バックアップ情報のリカバリー先は、バックアップした環境のホストだけです。バックアップ情報をリカバリーする場合は、それぞれの環境でリカバリーしてください。

クラスタ運用している場合は、物理ホスト、論理ホストの順番で、各環境をリカバリーしてください。

(3) バックアップ (UNIX の場合)

JP1/IM の設定情報のバックアップについて説明します。

JP1/IM の設定を変更した場合に、バックアップを取得してください。JP1/IM のバックアップを取得する場合は、必ず JP1/Base のバックアップを同時に取得してください。JP1/Base のユーザーが設定する定義ファイルのバックアップ方法については、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 - Agent の製品プラグインのバックアップとリカバリーは、JP1/IM - Manager のバックアップとリカバリーに従います。

バックアップの手段にはtar やcpio などのコマンドがあります。また、JP1/OmniBack II などのバックアップツールを使用してバックアップを取得できます。任意の方法でバックアップを取得してください。バックアップは、できるだけJP1/IM のデーモンを停止した状態で取得してください。しかたなく実行中に取得する場合は、次の点に注意が必要です。

- 実行中に定義ファイルが書き換えられる場合があります。ファイルの書き換え中にバックアップすると、ファイルが壊れた状態でバックアップされます。
バックアップ実行直後に、取得したバックアップとバックアップ元のファイルを比較して、内容が一致していることを確認してください。
- バックアップ時には対象ファイルに排他などのロックをしないでください。ロックする場合は、接続しているビューアーをすべてログアウトした状態で対象ファイルを別ファイルにコピーしてください。コピーしたあと、コピーしたファイルとコピー元ファイルを比較して、内容が一致していることを確認してから、コピーしたファイルをバックアップしてください。
- バックアップした設定情報をリストアした場合、リストアする内容で設定を変更するだけであり、JP1/IM - Manager に到着済みのイベントを再評価することはありません。

バックアップは、次の表に示す中で存在するすべてのファイルを一度にバックアップしてください。存在する中で一部のファイルしかバックアップしなかった場合、ほかの定義ファイルとの関連に矛盾が生じて正しく動作しないことがあります。

また、クラスタ運用している場合は、物理ホスト、論理ホストの順番で、各環境をバックアップしてください。

JP1/IM のバックアップ対象ファイルを次に示します。なお、論理ホストの場合は表中の「/var/opt」および「/etc/opt」を「共有ディレクトリ」に置き換えてください。

表 1-2 JP1/IM のバックアップ対象ファイル

製品名	ファイル名	内容
各製品共通	マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」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）」で作成した退避ファイル	共通定義情報退避ファイル ※1
JP1/IM - Manager	ユーザー任意のファイル名	通信暗号化機能で使用する秘密鍵 下記の共通定義情報に指定したファイル JP1_DEFAULT¥JP1BASE¥SSL¥PRIVATEKEYFILE¥※2 通信暗号化機能で使用するサーバ証明書

製品名	ファイル名	内容	
		下記の共通定義情報に指定したファイル JP1_DEFAULT¥JP1BASE¥SSL¥CERTIFICATEFILE※2	
		通信暗号化機能で使用するルート証明書 下記の共通定義情報に指定したファイル JP1_DEFAULT¥JP1BASE¥SSL¥CACERTIFICATEFILE※2	
JP1/IM - Manager	インテリジェント統合管理基盤	/etc/opt/jp1imm/conf/imdd/imdd.properties	インテリジェント統合管理基盤定義ファイル
		/etc/opt/jp1imm/conf/imdd/imdd_systemnode.conf	システムノード定義ファイル
		/etc/opt/jp1imm/conf/imdd/imdd_category_name.conf	IM 管理ノードカテゴリ名称定義ファイル
		/etc/opt/jp1imm/conf/imdd/imdd_target_host.conf	構成取得対象ホスト定義ファイル
		/etc/opt/jp1imm/conf/imdd/imdd_host_name.conf	ホスト名定義ファイル
		/etc/opt/jp1imm/conf/imdd/imdd_nodeLink_def.conf	IM 管理ノードリンク定義ファイル
		/etc/opt/jp1imm/conf/imdd/imdd_sso_mapping.properties	シングルサインオンマッピング定義ファイル
		/etc/opt/jp1imm/conf/imdd/plugin/jp1ajs/*.conf	JP1/AJS のプラグイン定義ファイル
		/etc/opt/jp1imm/conf/imdd/plugin/jp1pfm/*.conf	JP1/PFM のプラグイン定義ファイル
		/etc/opt/jp1imm/plugin/imdd/ユーザー作成プラグイン	ユーザー作成プラグイン
		/opt/jp1imm/public/custumUI/カスタム UI 用ユーザー作成フォルダ	カスタム UI 用ファイル格納フォルダ
		/etc/opt/jp1imm/conf/imdd/suggestion/template/en/imdd_suggestion_ajs_check_failed_agent_jobnet_en.conf	JP1/AJS の英語版提案テンプレートファイル
		/etc/opt/jp1imm/conf/imdd/suggestion/template/en/imdd_suggestion_ajs_check_failed_agent_list_en.conf	
		/etc/opt/jp1imm/conf/imdd/suggestion/template/en/imdd_suggestion_pfm_cpu_event_en.conf	JP1/PFM の英語版提案テンプレートファイル

製品名	ファイル名	内容	
	/etc/opt/jp1imm/conf/imdd/suggestion/template/en/imdd_suggestion_pfm_set_status_of_events_to_processd_en.conf		
	/etc/opt/jp1imm/conf/imdd/suggestion/template/en/imdd_suggestion_pfm_suspend_monitoring_en.conf		
	/etc/opt/jp1imm/conf/imdd/suggestion/template/ja/imdd_suggestion_ajs_check_failed_agent_jobnet_ja.conf	JP1/AJS の日本語版提案テンプレートファイル	
	/etc/opt/jp1imm/conf/imdd/suggestion/template/ja/imdd_suggestion_ajs_check_failed_agent_list_ja.conf		
	/etc/opt/jp1imm/conf/imdd/suggestion/template/ja/imdd_suggestion_pfm_cpu_event_ja.conf	JP1/PFM の日本語版提案テンプレートファイル	
	/etc/opt/jp1imm/conf/imdd/suggestion/template/ja/imdd_suggestion_pfm_set_status_of_events_to_processd_ja.conf		
	/etc/opt/jp1imm/conf/imdd/suggestion/template/ja/imdd_suggestion_pfm_suspend_monitoring_ja.conf		
	任意のパス/提案定義ファイル	提案定義ファイル	
	/etc/opt/jp1imm/conf/imdd/responseaction/autoactconf.json	自動対処アクション定義ファイル	
	/etc/opt/jp1imm/conf/imdd/responseaction/responseactionnotice.conf	対処アクション状態監視定義ファイル	
	セントラルコンソール	/etc/opt/jp1cons/conf/jp1co_env.conf	IM 環境定義ファイル
		/etc/opt/jp1cons/conf/jp1co_param.conf	IM パラメーター定義ファイル
		/etc/opt/jp1cons/conf/jp1co_param_V7.conf	IM パラメーター定義ファイル
		/etc/opt/jp1cons/conf/jp1co_service.conf	拡張起動プロセス定義ファイル
		/etc/opt/jp1cons/conf/jp1co_system.conf	IM サーバシステム環境設定ファイル
		/etc/opt/jp1cons/conf/action/actdef.conf	自動アクション定義ファイル
		/etc/opt/jp1cons/conf/console/actprofile/actprofile_JP1 ユーザー名	アクションプロファイル
		/etc/opt/jp1cons/conf/console/actprofile/actprofile2_JP1 ユーザー名	

製品名	ファイル名	内容
	/etc/opt/jp1cons/conf/console/actprofile/ actprofile_0950_JP1 ユーザー名	
	/etc/opt/jp1cons/conf/console/attribute/*.conf	イベント拡張属性定義ファイル
	/etc/opt/jp1cons/conf/console/attribute/extend/ *.conf	イベント拡張属性定義ファイル (拡張ファイル)
	/etc/opt/jp1cons/conf/console/filter/*.conf	フィルター定義ファイル
	/etc/opt/jp1cons/conf/console/filter/attr_list/ common_exclude_filter_attr_list.conf	共通除外条件表示項目定義ファイル
	/etc/opt/jp1cons/conf/console/filter/auto_list/ common_exclude_filter_auto_list.conf	共通除外条件自動入力定義ファイル
	/etc/opt/jp1cons/conf/console/mapping/mapping.conf	イベント情報マッピング定義ファイル
	/etc/opt/jp1cons/conf/console/monitor/*.conf	モニター画面呼び出し定義ファイル
	/etc/opt/jp1cons/conf/console/object_type/*	オブジェクトタイプ定義ファイル
	/etc/opt/jp1cons/conf/console/profile/.system	システムプロファイル
	/etc/opt/jp1cons/conf/console/profile/defaultUser	JP1/IM - View のユーザープロファイル (デフォルト)
	/etc/opt/jp1cons/conf/console/profile/profile_JP1 ユーザー名	JP1/IM - View のユーザープロファイル
	/etc/opt/jp1cons/conf/console/profile/ systemColor.conf	システムカラー定義ファイル
	/etc/opt/jp1cons/default/console.conf※3	通信環境定義ファイル
	/etc/opt/jp1cons/conf/console/correlation/ view_cor.conf	繰り返しイベントの集約設定ファイル
	/etc/opt/jp1cons/conf/console/correlation/ view_cor_JP1 ユーザー名.conf	繰り返しイベントの集約設定ファイル
	/etc/opt/jp1cons/conf/console/rmtcmd/cmdbtn.conf	コマンドボタン定義ファイル
	/etc/opt/jp1cons/conf/health/jcohc.conf	ヘルスチェック定義ファイル
	/etc/opt/jp1cons/conf/hostmap/user_hostmap.conf	発生元ホストマッピング定義ファイル
	/etc/opt/jp1cons/conf/action/actnotice.conf	自動アクション通知定義ファイル

製品名	ファイル名	内容	
	/etc/opt/jp1cons/conf/processupdate/processupdate.conf	対処状況イベント定義ファイル	
	/etc/opt/jp1cons/conf/guide/jco_guide.txt	イベントガイド情報ファイル	
	/etc/opt/jp1cons/conf/console/incident/incident.conf	インシデント手動登録定義ファイル	
	/etc/opt/jp1cons/conf/console/incident/incident_info.conf	インシデント引き継ぎ情報設定ファイル	
	/etc/opt/jp1cons/conf/system/event_storm/*.conf	繰り返しイベント条件定義ファイル	
	/etc/opt/jp1cons/conf/console/event_storm/attr_list/event_storm_attr_list.conf	繰り返しイベント条件表示項目定義ファイル	
	/etc/opt/jp1cons/conf/console/event_storm/auto_list/event_storm_auto_list.conf	繰り返しイベント条件自動入力定義ファイル	
	ユーザー任意のディレクトリ/ユーザー任意のファイル名	イベントガイドメッセージファイル	
	/etc/opt/jp1cons/conf/evgen/以下のすべてのファイル	関連イベント発行用定義ファイル	
	ユーザー任意のディレクトリ/ファイル名.conf	関連イベント発行定義ファイル	
	/etc/opt/jp1cons/conf/chsev/jcochsev.conf	重大度変更定義ファイル	
	/etc/opt/jp1cons/conf/action/attr_list/attr_list.conf	イベント条件表示項目定義ファイル	
	/etc/opt/jp1cons/conf/chsev/attr_list/chsev_attr_list.conf	重大度変更定義表示項目定義ファイル	
	/etc/opt/jp1cons/conf/chsev/auto_list/chsev_auto_list.conf	重大度変更定義自動入力定義ファイル	
	/etc/opt/jp1cons/conf/chattr/jcochmsg.conf	表示メッセージ変更定義ファイル	
	/etc/opt/jp1cons/conf/chattr/attr_list/chmsg_attr_list.conf	表示メッセージ変更定義表示項目定義ファイル	
	/etc/opt/jp1cons/conf/chattr/auto_list/chmsg_auto_list.conf	表示メッセージ変更定義自動入力定義ファイル	
	/etc/opt/jp1cons/conf/console/performance/performance.conf	性能レポート表示定義ファイル	
	セントラルスコープ	/etc/opt/jp1scope/conf/jcs_guide*.txt	ガイド情報ファイル
		/etc/opt/jp1scope/conf/jcs_hosts	ホスト情報ファイル

製品名	ファイル名	内容	
	/etc/opt/jp1scope/conf/action_complete_on.conf	対処済み連動設定ファイル	
	/etc/opt/jp1scope/conf/action_complete_off.conf		
	ユーザー任意のディレクトリ/ユーザー任意のファイル名	状態変更イベント自動削除設定ファイル	
	ユーザー任意のディレクトリ/ユーザー任意のファイル名	監視オブジェクト初期化設定ファイル	
	/etc/opt/jp1scope/conf/auto_dbbackup_on.conf	監視オブジェクト DB の上限監視設定ファイル	
	/etc/opt/jp1scope/conf/auto_dbbackup_off.conf		
	/etc/opt/jp1scope/conf/evhist_warn_event_on.conf	状態変更イベント件数の上限監視設定ファイル	
	/etc/opt/jp1scope/conf/evhist_warn_event_off.conf		
	ユーザー任意のディレクトリ/ユーザー任意のファイル名	ガイドメッセージファイル	
	ユーザー任意のディレクトリ/ユーザー任意のファイル名	状態変更条件メモリー常駐機能の設定ファイル	
	IM 構成管理	/etc/opt/jp1imm/conf/imcf/jp1cf_applyconfig.conf	IM 構成反映方式設定ファイル
		/etc/opt/jp1imm/conf/imcf/jp1cf_treedefaultpolicy.csv	デフォルト監視ポリシー定義ファイル
		/var/opt/jp1imm/data/imcf/以下の全ファイル	システムの管理情報
		/etc/opt/jp1imm/conf/agtless/targets/ssh.ini	SSH 認証情報に関する定義ファイル
JP1/IM - Agent の製品プラグイン	/opt/jp1imm/conf/imdd/plugin/jp1pccs/aws_settings.conf	AWS 定義ファイル	
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/property_labels.conf	プロパティ表示文字列定義ファイル	
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_node_exporter.conf	Node exporter のメトリック定義ファイル	
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_windows_exporter.conf	Windows exporter のメトリック定義ファイル	
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_windows_exporter_process.conf	Windows exporter (プロセス監視) のメトリック定義ファイル	
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_blackbox_exporter.conf	Blackbox exporter のメトリック定義ファイル	
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_ya_cloudwatch_exporter.conf	Yet another cloudwatch exporter のメトリック定義ファイル	

製品名	ファイル名	内容
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_kubernetes.conf	コンテナ監視のメトリック定義ファイル
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_fluentd.conf	Fluentd のメトリック定義ファイル
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_任意のPrometheusトレンド名.conf	ユーザー独自のメトリック定義ファイル
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_process_exporter.conf	Process exporter のメトリック定義ファイル
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_promitor.conf	Promitor のメトリック定義ファイル
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/metrics_script_exporter.conf	Script exporter のメトリック定義ファイル
	/opt/jp1imm/conf/imdd/plugin/jp1pccs/user/metrics_任意のPrometheusトレンド名.conf	ユーザー独自のメトリック定義ファイル
	/opt/jp1imm/conf/imdd/imagent/jp1pccs/jpc_imbase.json	imbase 設定ファイル
	/opt/jp1imm/conf/imdd/imagent/jpc_imbaseproxy.json	imbaseproxy 設定ファイル
	/opt/jp1imm/conf/imdd/imagent/サーバ証明書ファイル	統合エージェント管理基盤用のサーバ証明書ファイル
	/opt/jp1imm/conf/imdd/imagent/サーバ証明書キーファイル	統合エージェント管理基盤用のサーバ証明書キーファイル

注※1 共通定義情報退避ファイルは、クラスタシステムの論理ホストの定義情報を退避したファイルです。この退避ファイルは、クラスタシステムのセットアップ時に作成します。この退避ファイルには、JP1/IM だけでなく、JP1/Base, JP1/AJS, および 06-02 以降の JP1/Power Monitor の定義情報も退避されます。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「7.1.3(5) 共通定義情報の設定」を参照してください。

注※2 論理ホストの場合は、「JP1_DEFAULT」は論理ホスト名となります。

注※3 物理ホストにだけ存在するファイルです。

(4) リカバリー (UNIX の場合)

JP1/IM の設定情報のリカバリーについて説明します。

JP1/IM のバックアップ情報をリカバリーする場合は、必ず JP1/Base を先にリカバリーしてください。次の前提条件を確認した上で、バックアップファイルを、元の位置にリカバリーしてください。

前提条件

- JP1/Base がインストールされ、セットアップコマンドが実行済みであること。
- JP1/IM - Manager がインストールされ、セットアップコマンドが実行済みであること。

- 論理ホスト環境をリカバリーする場合は、論理ホスト環境の JP1 がセットアップ済みであること。
- JP1/Base と JP1/IM - Manager が停止していること。

バックアップ情報のリカバリー先は、バックアップした環境のホストだけです。バックアップ情報をリカバリーする場合は、それぞれの環境でリカバリーしてください。

クラスタ運用している場合は、物理ホスト、論理ホストの順番で、各環境をリカバリーしてください。

1.1.2 JP1/IM - Agent のバックアップとリカバリー

(1) バックアップ

JP1/IM - Agent の設定を変更した場合に、バックアップを取得してください。稼働中でもバックアップを行えます。

(a) 通常ホスト

1. JP1/IM - Agent のバックアップ対象ファイルをバックアップする。

「1.1.2(3)バックアップ対象ファイル」の該当する OS の表で、バックアップ対象となっているファイルをバックアップしてください。

2. Alertmanager のサイレンスの設定を保存する場合は、REST API でサイレンスを取得してバックアップする。

サイレンスの取得に関する 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「Alertmanager のサイレンス取得」(5. API) を参照してください。

(b) クラスタ環境

「1.1.2(1)(a)通常ホスト」の手順と同じです。

ただし、次のことに注意してください。

- 実行系サーバと待機系サーバの両方でバックアップを取得してください。
- 共有ディレクトリもバックアップを取得する必要があります。

(c) コンテナ環境

Docker イメージ、Podman イメージのバックアップを取得してください。

(d) オプション機能のバックアップ

JP1/IM - Agent および JP1/IM - Manager のバックアップは、別途実施してください。

■ OracleDB exporter

次に示すファイルをバックアップしてください。

Windows の場合

- OracleDB exporter のサービス定義ファイル

OracleDB exporter の配置先

```
¥oracledb_exporter_windows¥jp1ima¥bin¥oracledb_exporter_*.service.xml
```

Linux の場合

- OracleDB exporter のユニット定義ファイル

```
/usr/lib/systemd/system/oracledb_exporter_*.service
```

■ Node exporter for AIX

バックアップするファイルはありません。

(2) リカバリー

(a) 通常ホスト

■ Windows の場合

1. バックアップした定義ファイルと同じホスト名、IP アドレスのマシンを用意する。
2. バックアップした定義ファイルと同じバージョンの JP1/IM - Agent をインストールする。
3. バックアップした定義ファイルをインストール先に上書きする。

通信暗号化で使用する証明書については、必要に応じて更新してください。

4. 使用するサービスが登録済みだった場合は Windows サービスへ登録しなおす。

サービスを登録しなおすには、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。

アドオンプログラムのサービスの有効化・無効化の方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

5. サービスを起動する。

6. Alertmanager のサイレンスの設定を登録する。

Alertmanager のサイレンス作成の API を使用します。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「5.21.4 Alertmanager のサイレンス作成」を参照してください。

なお、有効期間が過ぎているサイレンスは作成できないため、注意してください。

■ Linux の場合

1. バックアップした定義ファイルと同じホスト名, IP アドレスのマシンを用意する。
2. バックアップした定義ファイルと同じバージョンの JP1/IM - Agent をインストールする。
3. バックアップした定義ファイルをインストール先と「/usr/lib/systemd/system」に上書きする。
4. 次のコマンドを実行する。

```
# systemctl daemon-reload
```

5. サービスを起動する。
6. Alertmanager のサイレンスの設定を登録する。

Alertmanager のサイレンス作成の API を使用します。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「5.21.4 Alertmanager のサイレンス作成」を参照してください。

なお、有効期間が過ぎているサイレンスは作成できないため、注意してください。

(b) クラスタ環境

■ Windows の場合

1. バックアップした定義ファイルと同じホスト名, IP アドレスのマシンを用意する。
実行系サーバと待機系サーバの両方で用意します。
2. バックアップした定義ファイルと同じバージョンの JP1/IM - Agent をインストールする。
実行系サーバと待機系サーバの両方で実施します。
3. バックアップ時と同じ論理ホスト名で論理ホストを構築する。
4. バックアップした定義ファイルをインストール先と共有ディレクトリに上書きする。
実行系サーバと待機系サーバの両方で実施します。
5. 使用するサービスが登録済みだった場合は Windows サービスへ登録しなおす。
サービスを登録しなおすには、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。
実行系サーバと待機系サーバの両方で実施します。
6. クラスタソフトに JP1/IM - Agent の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、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。
7. クラスタソフトから JP1/IM - Agent を起動する。

8. Alertmanager のサイレンスの設定を登録する。

Alertmanager のサイレンス作成の API を使用します。

なお、有効期間が過ぎているサイレンスは作成できないため、注意してください。

■ Linux の場合

1. バックアップした定義ファイルと同じホスト名、IP アドレスのマシンを用意する。

実行系サーバと待機系サーバの両方で用意します。

2. バックアップした定義ファイルと同じバージョンの JP1/IM - Agent をインストールする。

実行系サーバと待機系サーバの両方で用意します。

3. バックアップした定義ファイルを、インストール先、[/usr/lib/systemd/system]、および共有ディレクトリに上書きする。

4. 次のコマンドを実行する。

```
# systemctl daemon-reload
```

5. サービスを起動する。

6. Alertmanager のサイレンスの設定を登録する。

Alertmanager のサイレンス作成の API を使用します。

なお、有効期間が過ぎているサイレンスは作成できないため、注意してください。

(c) コンテナ環境

バックアップした Docker イメージ、Podman イメージからリカバリーしてください。

(d) オプション機能のリカバリー

■ OracleDB exporter

Windows の場合

1. OracleDB exporter をインストールする。

2. OracleDB exporter の監視対象を追加する。

監視対象を追加する際、サービス定義ファイルを作成する手順で、バックアップしたサービス定義ファイルを使用します。

Linux の場合

1. OracleDB exporter をインストールする。

2. OracleDB exporter の監視対象を追加する。

監視対象を追加する際、ユニット定義ファイルを作成する手順で、バックアップしたサービス定義ファイルを使用します。

■ Node exporter for AIX

監視対象の AIX ホスト

1. Node exporter for AIX をインストールする。
Node exporter for AIX のインストールについては、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.23.2(2)Node exporter for AIX のインストール」を参照してください。
2. Node exporter for AIX のポート番号を変更する必要がある場合は、ポート番号を変更する。
Node exporter for AIX のポート番号の変更については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.23.2(4)(b)Node exporter のポートを変更する (オプション)」を参照してください。

(3) バックアップ対象ファイル

(a) Windows の場合

表 1-3 JP1/IM - Agent の物理ホストのバックアップ対象ファイル (Windows)

ファイル名	内容
Agent パス¥conf¥jpc_imagent.json	imagent 設定ファイル
Agent パス¥conf¥jpc_imagentproxy.json	imagentproxy 設定ファイル
Agent パス¥conf¥jpc_imagentaction.json	imagentaction 設定ファイル
Agent パス¥conf¥jpc_alertmanager.yml	Alertmanager 設定ファイル
Agent パス¥conf¥jpc_prometheus_server.yml	Prometheus 設定ファイル
Agent パス¥conf¥jpc_alerting_rules.yml	アラート設定ファイル
Agent パス¥conf¥jpc_file_sd_config_node.yml	Node exporter のディスカバリ設定ファイル
Agent パス¥conf¥jpc_file_sd_config_windows.yml	Windows exporter のディスカバリ設定ファイル
Agent パス¥conf¥jpc_file_sd_config_blackbox_http.yml	Blackbox exporter (HTTP/HTTPS 監視) のディスカバリ設定ファイル
Agent パス¥conf¥jpc_file_sd_config_blackbox_icmp.yml	Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル
Agent パス¥conf¥user¥file_sd_config_blackbox_任意の名前.yml	Blackbox exporter の監視対象 (ユーザー定義) のディスカバリ設定ファイル
Agent パス¥conf¥jpc_file_sd_config_cloudwatch.yml	Yet another cloudwatch exporter のディスカバリ設定ファイル
Agent パス¥conf¥user¥file_sd_config_任意の名前.yml	ユーザー独自のディスカバリ設定ファイル
Agent パス¥conf¥jpc_file_sd_config_process.yml	Process exporter のディスカバリ設定ファイル
Agent パス¥conf¥jpc_file_sd_config_promitor.yml	Promitor のディスカバリ設定ファイル

ファイル名	内容
Agent パス¥conf¥jpc_file_sd_config_script.yml	Script exporter のディスカバリ設定ファイル
Agent パス¥conf¥jpc_windows_exporter.yml	Windows exporter 設定ファイル
Agent パス¥conf¥jpc_blackbox_exporter.yml	Blackbox exporter 設定ファイル
Agent パス¥conf¥jpc_ya_cloudwatch_exporter.yml	Yet another cloudwatch exporter 設定ファイル
Agent パス¥conf¥jpc_script_exporter.yml	Script exporter 設定ファイル
Agent パス¥conf¥jpc_fluentd_common.conf	ログ監視共通定義ファイル
Agent パス¥conf¥jpc_fluentd_common_list.conf	ログ監視対象定義ファイル
Agent パス¥conf¥jpc_fluentd_common_wevt_rendered.conf	レンダリング情報取得定義ファイル
Agent パス¥conf¥fluentd_@@trapname@@_tail.conf.template	テキスト形式のログファイルの監視定義ファイルのテンプレート
Agent パス¥conf¥fluentd_@@trapname@@_wevt.conf.template	Windows イベントログの監視定義ファイルのテンプレート
Agent パス¥conf¥user¥fluentd_ログ監視名_tail.conf	テキスト形式のログファイルの監視定義ファイル
Agent パス¥conf¥user¥fluentd_ログ監視名_wevt.conf	Windows イベントログの監視定義ファイル
Agent パス¥conf¥user¥fluentd_任意の名前_logmetrics.conf	ログメトリクス定義ファイル
Agent パス¥conf¥jpc_user_deffile_list.json	ユーザー作成定義ファイルリスト定義ファイル
Agent パス¥conf¥promitor¥scraper¥metrics-declaration.yml	Promitor Scraper 設定ファイル
Agent パス¥conf¥promitor¥scraper¥runtime.yml	Promitor Scraper runtime 設定ファイル
Agent パス¥conf¥promitor¥resource-discovery¥resource-discovery-declaration.yml	Promitor Resource Discovery 設定ファイル
Agent パス¥conf¥promitor¥resource-discovery¥runtime.yml	Promitor Resource Discovery runtime 設定ファイル
Agent パス¥conf¥user¥cert¥CA 証明書ファイル	Black exporter 用の CA 証明書ファイル
Agent パス¥conf¥user¥cert¥クライアント証明書ファイル	Black exporter 用のクライアント証明書ファイル
Agent パス¥conf¥user¥secret¥クライアント証明書キーファイル	Black exporter 用のクライアント証明書キーファイル
Agent パス¥conf¥user¥secret¥パスワードファイル	Black exporter 用のパスワードファイル
Agent パス¥bin¥jpc_imagent_service.xml	imagent のサービス定義ファイル
Agent パス¥bin¥jpc_imagent_service_論理ホスト名.xml	論理ホスト用の imagent のサービス定義ファイル
Agent パス¥bin¥jpc_imagentproxy_service.xml	imagentproxy のサービス定義ファイル
Agent パス¥bin¥jpc_imagentproxy_service_論理ホスト名.xml	論理ホスト用の imagentproxy のサービス定義ファイル
Agent パス¥bin¥jpc_imagentaction_service.xml	imagentaction のサービス定義ファイル

ファイル名	内容
Agent パス¥bin¥jpc_imagentaction_service_論理ホスト名.xml	論理ホスト用の imagentaction のサービス定義ファイル
Agent パス¥bin¥jpc_alertmanager_service.xml	Alertmanager のサービス定義ファイル
Agent パス¥bin¥jpc_alertmanager_service_論理ホスト名.xml	論理ホスト用の Alertmanager のサービス定義ファイル
Agent パス¥bin¥jpc_prometheus_server_service.xml	Prometheus server のサービス定義ファイル
Agent パス¥bin¥jpc_prometheus_server_service_論理ホスト名.xml	論理ホスト用の Prometheus server のサービス定義ファイル
Agent パス¥bin¥jpc_windows_exporter_service.xml	Windows exporter のサービス定義ファイル
Agent パス¥bin¥jpc_windows_exporter_service_論理ホスト名.xml	論理ホスト用の Windows exporter のサービス定義ファイル
Agent パス¥bin¥jpc_blackbox_exporter_service.xml	Blackbox exporter のサービス定義ファイル
Agent パス¥bin¥jpc_blackbox _exporter_service_論理ホスト名.xml	論理ホスト用の Blackbox exporter のサービス定義ファイル
Agent パス¥bin¥jpc_ya_cloudwatch_exporter_service.xml	Yet another cloudwatch exporter のサービス定義ファイル
Agent パス¥bin¥jpc_ya_cloudwatch_exporter_service_論理ホスト名.xml	論理ホスト用の Yet another cloudwatch exporter のサービス定義ファイル
Agent パス¥bin¥jpc_promitor_scraper_service.xml	Promitor Scraper のサービス定義ファイル
Agent パス¥bin¥jpc_promitor_scraper_service_論理ホスト名.xml	論理ホスト用の Promitor Scraper のサービス定義ファイル
Agent パス¥bin¥jpc_promitor_resource_discovery_service.xml	Promitor Resource Discovery のサービス定義ファイル
Agent パス¥bin¥jpc_promitor_resource_discovery_service_論理ホスト名.xml	論理ホスト用の Promitor Resource Discovery のサービス定義ファイル
Agent パス¥bin¥jpc_script_exporter_service.xml	Script exporter のサービス定義ファイル
Agent パス¥bin¥jpc_script_exporter_service_論理ホスト名.xml	論理ホスト用の Script exporter のサービス定義ファイル
Agent パス¥bin¥jpc_fluentd_service.xml	Fluentd のサービス定義ファイル
Agent パス¥bin¥jpc_fluentd_service_論理ホスト名.xml	論理ホスト用の Fluentd のサービス定義ファイル

表 1-4 JP1/IM - Agent の論理ホストのバックアップ対象ファイル

ファイル名	内容
共有フォルダ¥jp1ima¥conf¥jpc_imagent.json	imagent 設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_imagentproxy.json	imagentproxy 設定ファイル

ファイル名	内容
共有フォルダ¥jp1ima¥conf¥jpc_imagentaction.json	imagentaction 設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_alertmanager.yml	Alertmanager 設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_prometheus_server.yml	Prometheus 設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_alerting_rules.yml	アラート設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_file_sd_config_node.yml	Node exporter のディスカバリ設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_file_sd_config_blackbox_http.yml	Blackbox exporter (HTTP/HTTPS 監視) のディスカバリ設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_file_sd_config_blackbox_icmp.yml	Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル
共有フォルダ¥jp1ima¥conf¥user¥file_sd_config_blackbox_任意の名前.yml	Blackbox exporter の監視対象 (ユーザー定義) のディスカバリ設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_file_sd_config_cloudwatch.yml	Yet another cloudwatch exporter のディスカバリ設定ファイル
共有フォルダ¥jp1ima¥conf¥user¥file_sd_config_任意の名前.yml	ユーザー独自のディスカバリ設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_file_sd_config_process.yml	Process exporter のディスカバリ設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_file_sd_config_promitor.yml	Promitor のディスカバリ設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_windows_exporter.yml	Windows exporter 設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_blackbox_exporter.yml	Blackbox exporter 設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_ya_cloudwatch_exporter.yml	Yet another cloudwatch exporter 設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_script_exporter.yml	Script exporter 設定ファイル
共有フォルダ¥jp1ima¥conf¥jpc_fluentd_common.conf	ログ監視共通定義ファイル
共有フォルダ¥jp1ima¥conf¥jpc_fluentd_common_list.conf	ログ監視対象定義ファイル
共有フォルダ¥jp1ima¥conf¥jpc_fluentd_common_wevt_rendered.conf	レンダリング情報取得定義ファイル
共有フォルダ¥jp1ima¥conf¥fluentd_@@trapname@@_tail.conf.template	テキスト形式のログファイルの監視定義ファイルのテンプレート
共有フォルダ¥jp1ima¥conf¥fluentd_@@trapname@@_wevt.conf.template	Windows イベントログの監視定義ファイルのテンプレート
共有フォルダ¥jp1ima¥conf¥jpc_user_deffile_list.json	ユーザー作成定義ファイルリスト定義ファイル
共有フォルダ¥jp1ima¥conf¥promitor¥scraper¥metrics-declaration.yml	Promitor Scraper 設定ファイル
共有フォルダ¥jp1ima¥conf¥promitor¥scraper¥runtime.yml	Promitor Scraper runtime 設定ファイル
共有フォルダ¥jp1ima¥conf¥promitor¥resource-discovery¥resource-discovery-declaration.yml	Promitor Resource Discovery 設定ファイル

ファイル名	内容
共有フォルダ¥jp1ima¥conf¥promitor¥resource-discovery¥runtime.yml	Promitor Resource Discovery runtime 設定ファイル
共有フォルダ¥jp1ima¥conf¥user¥cert¥CA 証明書ファイル	Black exporter 用の CA 証明書ファイル
共有フォルダ¥jp1ima¥conf¥user¥cert¥クライアント証明書ファイル	Black exporter 用のクライアント証明書ファイル
共有フォルダ¥jp1ima¥conf¥user¥secret¥クライアント証明書キーファイル	Black exporter 用のクライアント証明書キーファイル
共有フォルダ¥jp1ima¥conf¥user¥secret¥パスワードファイル	Black exporter 用のパスワードファイル

(b) UNIX の場合

表 1-5 JP1/IM - Agent の物理ホストのバックアップ対象ファイル (UNIX)

ファイル名	内容
/opt/jp1ima/conf/jpc_imagent.json	imagent 設定ファイル
/opt/jp1ima/conf/jpc_imagentproxy.json	imagentproxy 設定ファイル
/opt/jp1ima/conf/jpc_imagentaction.json	imagentaction 設定ファイル
/opt/jp1ima/conf/jpc_alertmanager.yml	Alertmanager 設定ファイル
/opt/jp1ima/conf/jpc_prometheus_server.yml	Prometheus 設定ファイル
/opt/jp1ima/conf/jpc_alerting_rules.yml	アラート設定ファイル
/opt/jp1ima/conf/jpc_file_sd_config_node.yml	Node exporter のディスカバリ設定ファイル
/opt/jp1ima/conf/jpc_file_sd_config_windows.yml	Windows exporter のディスカバリ設定ファイル
/opt/jp1ima/conf/jpc_file_sd_config_blackbox_http.yml	Blackbox exporter (HTTP/HTTPS 監視) のディスカバリ設定ファイル
/opt/jp1ima/conf/jpc_file_sd_config_blackbox_icmp.yml	Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル
/opt/jp1ima/conf/jpc_file_sd_config_cloudwatch.yml	Yet another cloudwatch exporter のディスカバリ設定ファイル
/opt/jp1ima/conf/user/file_sd_config_blackbox_任意の名前.yml	Blackbox exporter の監視対象 (ユーザー定義) のディスカバリ設定ファイル
/opt/jp1ima/conf/user/file_sd_config_任意の名前.yml	ユーザー独自のディスカバリ設定ファイル
/opt/jp1ima/conf/jpc_file_sd_config_process.yml	Process exporter のディスカバリ設定ファイル
/opt/jp1ima/conf/jpc_file_sd_config_promitor.yml	Promitor のディスカバリ設定ファイル
/opt/jp1ima/conf/jpc_file_sd_config_script.yml	Script exporter のディスカバリ設定ファイル
/opt/jp1ima/conf/jpc_blackbox_exporter.yml	Blackbox exporter 設定ファイル
/opt/jp1ima/conf/jpc_ya_cloudwatch_exporter.yml	Yet another cloudwatch exporter 設定ファイル

ファイル名	内容
/opt/jp1ima/conf/jpc_process_exporter.yml	Process exporter 設定ファイル
/opt/jp1ima/conf/jpc_script_exporter.yml	Script exporter 設定ファイル
/opt/jp1ima/conf/jpc_fluentd_common.conf	ログ監視共通定義ファイル
/opt/jp1ima/conf/jpc_fluentd_common_list.conf	ログ監視対象定義ファイル
/opt/jp1ima/conf/fluentd_@@trapname@@_tail.conf.template	テキスト形式のログファイルの監視定義ファイルのテンプレート
/opt/jp1ima/conf/user/fluentd_ログ監視名_tail.conf	テキスト形式のログファイルの監視定義ファイル
/opt/jp1ima/conf/user/fluentd_任意の名前_logmetrics.conf	ログメトリクス定義ファイル
/opt/jp1ima/conf/jpc_user_deffile_list.json	ユーザー作成定義ファイルリスト定義ファイル
/opt/jp1ima/conf/promitor/scrapper/metrics-declaration.yml	Promitor Scrapper 設定ファイル
/opt/jp1ima/conf/promitor/scrapper/runtime.yml	Promitor Scrapper runtime 設定ファイル
/opt/jp1ima/conf/promitor/resource-discovery/resource-discovery-declaration.yml	Promitor Resource Discovery 設定ファイル
/opt/jp1ima/conf/promitor/resource-discovery/runtime.yml	Promitor Resource Discovery runtime 設定ファイル
/opt/jp1ima/conf/user/cert/CA 証明書ファイル	Black exporter 用の CA 証明書ファイル
/opt/jp1ima/conf/user/cert/クライアント証明書ファイル	Black exporter 用のクライアント証明書ファイル
/opt/jp1ima/conf/user/secret/クライアント証明書キーファイル	Black exporter 用のクライアント証明書キーファイル
/opt/jp1ima/conf/user/secret/パスワードファイル	Black exporter 用のパスワードファイル
/usr/lib/systemd/system/jpc_imagentaction.service	imagentaction のユニット定義ファイル
/usr/lib/systemd/system/jpc_alertmanager.service	Alertmanager のユニット定義ファイル
/usr/lib/systemd/system/jpc_prometheus_server.service	Prometheus server のユニット定義ファイル
/usr/lib/systemd/system/jpc_node_exporter.service	Node exporter のユニット定義ファイル
/usr/lib/systemd/system/jpc_blackbox_exporter.service	Blackbox exporter のユニット定義ファイル
/usr/lib/systemd/system/jpc_ya_cloudwatch_exporter.service	Yet another cloudwatch exporter のユニット定義ファイル
/usr/lib/systemd/system/jpc_fluentd.service	Fluend のユニット定義ファイル
/usr/lib/systemd/system/jpc_imagent_論理ホスト名.service	論理ホスト用の imagent のユニット定義ファイル
/usr/lib/systemd/system/jpc_imagentproxy_論理ホスト名.service	論理ホスト用の imagentproxy のユニット定義ファイル
/usr/lib/systemd/system/jpc_imagentaction_論理ホスト名.service	論理ホスト用の imagentaction のユニット定義ファイル

ファイル名	内容
/usr/lib/systemd/system/jpc_alertmanager_論理ホスト名.service	論理ホスト用の Alertmanager のユニット定義ファイル
/usr/lib/systemd/system/jpc_prometheus_server_論理ホスト名.service	論理ホスト用の Prometheus server のユニット定義ファイル
/usr/lib/systemd/system/jpc_node_exporter_論理ホスト名.service	論理ホスト用の Node exporter のユニット定義ファイル
/usr/lib/systemd/system/jpc_blackbox_exporter_論理ホスト名.service	論理ホスト用の Blackbox exporter のユニット定義ファイル
/usr/lib/systemd/system/jpc_ya_cloudwatch_exporter_論理ホスト名.service	論理ホスト用の Yet another cloudwatch exporter のユニット定義ファイル
/usr/lib/systemd/system/jpc_process_exporter_論理ホスト名.service	論理ホスト用の Process exporter のユニット定義ファイル
/usr/lib/systemd/system/jpc_promitor_scraper_論理ホスト名.service	論理ホスト用の Promitor Scraper のユニット定義ファイル
/usr/lib/systemd/system/jpc_promitor_resource_discovery_論理ホスト名.service	論理ホスト用の Promitor Resource Discovery のユニット定義ファイル
/usr/lib/systemd/system/jpc_script_exporter_論理ホスト名.service	論理ホスト用の Script exporter のユニット定義ファイル
/usr/lib/systemd/system/jpc_fluentd_論理ホスト名.service	論理ホスト用の Fluentd のユニット定義ファイル

表 1-6 JP1/IM - Agent の論理ホストのバックアップ対象ファイル (UNIX)

ファイル名	内容
共有ディレクトリ/jp1ima/conf/jpc_imagent.json	imagent 設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_imagentproxy.json	imagentproxy 設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_imagentaction.json	imagentaction 設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_alertmanager.yml	Alertmanager 設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_prometheus_server.yml	Prometheus 設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_alerting_rules.yml	アラート設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_file_sd_config_node.yml	Node exporter のディスカバリ設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_file_sd_config_blackbox_http.yml	Blackbox exporter (HTTP/HTTPS 監視) のディスカバリ設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_file_sd_config_blackbox_icmp.yml	Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル
共有ディレクトリ/jp1ima/conf/user/file_sd_config_blackbox_任意の名前.yml	Blackbox exporter の監視対象 (ユーザー定義) のディスカバリ設定ファイル

ファイル名	内容
共有ディレクトリ/jp1ima/conf/jpc_file_sd_config_cloudwatch.yml	Yet another cloudwatch exporter のディスカバリ設定ファイル
共有ディレクトリ/jp1ima/conf/user/file_sd_config_任意の名前.yml	ユーザー独自のディスカバリ設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_file_sd_config_process.yml	Process exporter のディスカバリ設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_file_sd_config_promitor.yml	Promitor のディスカバリ設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_blackbox_exporter.yml	Blackbox exporter 設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_ya_cloudwatch_exporter.yml	Yet another cloudwatch exporter 設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_process_exporter.yml	Process exporter 設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_script_exporter.yml	Script exporter 設定ファイル
共有ディレクトリ/jp1ima/conf/jpc_fluentd_common.conf	ログ監視共通定義ファイル
共有ディレクトリ/jp1ima/conf/jpc_fluentd_common_list.conf	ログ監視対象定義ファイル
共有ディレクトリ/jp1ima/conf/jpc_fluentd_common_wevt_rendered.conf	レンダリング情報取得定義ファイル
共有ディレクトリ/jp1ima/conf/fluentd_@@trapname@@_tail.conf.template	テキスト形式のログファイルの監視定義ファイルのテンプレート
共有ディレクトリ/jp1ima/conf/fluentd_@@trapname@@_wevt.conf.template	Windows イベントログの監視定義ファイルのテンプレート
共有ディレクトリ/jp1ima/conf/jpc_user_deffile_list.json	ユーザー作成定義ファイルリスト定義ファイル
共有ディレクトリ/jp1ima/conf/promitor%scraper%metrics-declaration.yml	Promitor Scraper 設定ファイル
共有ディレクトリ/jp1ima/conf/promitor%scraper%runtime.yml	Promitor Scraper runtime 設定ファイル
共有ディレクトリ/jp1ima/conf/promitor%resource-discovery%resource-discovery-declaration.yml	Promitor Resource Discovery 設定ファイル
共有ディレクトリ/jp1ima/conf/promitor%resource-discovery%runtime.yml	Promitor Resource Discovery runtime 設定ファイル
共有ディレクトリ/jp1ima/conf/user/cert/CA 証明書ファイル	Black exporter 用の CA 証明書ファイル
共有ディレクトリ/jp1ima/conf/user/cert/クライアント証明書ファイル	Black exporter 用のクライアント証明書ファイル
共有ディレクトリ/jp1ima/conf/user/secret/クライアント証明書キーファイル	Black exporter 用のクライアント証明書キーファイル
共有ディレクトリ/jp1ima/conf/user/secret/パスワードファイル	Black exporter 用のパスワードファイル

1.2 データベースの管理

JP1/IM のシステムで使用するデータベースには次のものがあります。

- コマンド実行履歴
- 監視オブジェクト DB
- ホスト情報 DB
- イベント DB
- 応答待ちイベント滞留ファイル
- IM データベース
- インテリジェント統合管理データベース

監視オブジェクト DB およびホスト情報 DB は、セントラルスコープの機能を使用している場合に使われます。応答待ちイベント滞留ファイルは、応答待ちイベント管理機能を使用している場合に使われます。ここでは、これらのデータベースのバックアップ・リカバリー手順、およびデータベースの再作成手順について説明します。

1.2.1 データベースの再編成

(1) コマンド実行履歴の再編成

コマンド実行履歴は、再編成する必要はありません。

(2) 監視オブジェクト DB およびホスト情報 DB の再編成

監視オブジェクト DB、およびホスト情報 DB は、再編成する必要はありません。

(3) イベント DB の再編成

イベント DB は、再編成する必要はありません。

(4) 応答待ちイベント滞留ファイルの再編成

応答待ちイベント滞留ファイルは、再編成する必要はありません。

(5) IM データベースの再編成

ここでは、IM データベースの再編成手順について説明します。

IM データベースのうち、IM 構成管理 DB ではデータの追加、削除を繰り返すと、断片化された空き領域が発生して、ホストやプロファイルの数が上限値に達する前に新規登録ができなくなったり、登録、更新、削除の速度に遅れを感じたりすることがあります。

この現象を回避するために、次の契機で IM データベースを再編成します。

- 定期的なバックアップ作業のため、JP1/IM - Manager を停止したとき
- 年に 1 回程度の頻度で再編成実施計画を立てて実施するとき
- メッセージ「KFPH00212-I」または「KFPH00213-W」が Windows イベントログ (syslog) に出 forceされたとき

上記のような現象が起こった場合は、次の手順でデータベースの空き領域を解放してください。

1. Windows の場合、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. `jimdbreclaim` コマンドを使用して、データベースの空き領域を解放する。
3. IM データベースに登録されているホスト情報やプロファイルに不要なものがないかどうかを確認して、不要なものがあれば削除する。

この方法で、現象が解消されない場合は、IM データベースを再編成する必要があります。次に物理ホストでの IM データベースの再編成手順およびクラスタ環境での IM データベースの再編成手順について示します。

(a) 物理ホストでの IM データベースの再編成手順

1. サービスの状態を確認する。
 - Windows の場合、IM データベースサービス (JP1/IM3-Manager DB Server) が起動している。
 - JP1/IM3-Manager サービスが停止している。
 - JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスが停止している。
2. JP1/IM3-Manager サービスを停止する。

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。
3. `jimdbroorg` コマンドを使用して、対象データベースを再編成する。

`jimdbroorg` 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「`jimdbroorg`」(1. コマンド) を参照してください。
4. JP1/IM3-Manager サービスを起動する。

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 サービスも起動してください。

(b) クラスタ環境での IM データベースの再編成手順

クラスタ環境の場合、実行系ホスト上で実行します。また、共有ディレクトリにアクセスできる状態である必要があります。

1. サービスの状態を確認する。

- Windows の場合、IM データベースサービス (JP1/IM3-Manager DB Server_論理ホスト名) が起動している。
- JP1/IM3-Manager サービスおよび IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) が停止している。
- JP1/IM - MO を使用している場合、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスが停止している。

2. jimdbroorg コマンドを使用して、対象データベースを再編成する。

jimdbroorg 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「jimdbroorg」(1. コマンド) を参照してください。

3. JP1/IM3-Manager サービスと手順 1 で停止した IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を起動する。

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 サービスも起動してください。

(6) インテリジェント統合管理データベースの再編成

インテリジェント統合管理データベースの再編成を自動で行うため、ユーザーによる再編成の必要はありません。

1.2.2 データベースのバックアップおよびリカバリー

バックアップ・リカバリーを実施する際には、バックアップ元とリカバリー先で次のすべてが一致している必要があります。

- ホスト名
- IP アドレス
- PP 形名
- PP バージョン (VVRRZZ の範囲で一致させてください)
- 製品の使用するディレクトリの構成 (権限などを含めて一致させてください)

また、OS、ハードウェアに関しては、同一の動作ができることが前提となります。

上記の条件に一致しない場合は、移行となります。

「1.5 設定情報および DB の移行」を参照して実施してください。

OS コマンドやバックアップソフトでシステム全体をフルバックアップすることもできますが、OS コマンドやバックアップソフトの動作に依存するため、JP1/IM - Manager では、JP1/IM - Manager の各機能で提供しているコマンドを使用したバックアップ・リカバリーをお勧めします。OS コマンドやバックアップソフトを使用する場合、次の前提条件となります。

- 事前に IM データベースを含む JP1/IM - Manager のすべてのサービスが停止された状態で取得されている。
- OS に登録している情報を含めて、ファイル、レジストリの情報がすべて整合性の取れた状態でバックアップされている。
- 取得されるバックアップ対象のファイルがスパースファイルとなっていない。

一部のデータベースだけのバックアップ・リカバリーはできません。一部のデータベースだけをバックアップ・リカバリーをした場合、関連づけに矛盾が生じ、不正なデータを参照することがあります。

データベースをバックアップ・リカバリーする場合は、定義情報も合わせてバックアップ・リカバリーを実施してください。データベースだけをバックアップした場合、定義情報と矛盾が生じることがあります。

バックアップ・リカバリー時は、JP1/IM - View を停止してください。

(1) コマンド実行履歴のバックアップ・リカバリー手順

コマンド実行履歴のバックアップ・リカバリー手順について説明します。

(a) バックアップ手順

1. JP1/IM - Manager を停止する。
2. JP1/Base を停止する。
3. 対象ファイルのバックアップを取得する。
対象ファイルについては、「1.2.2(1)(c) バックアップ対象ファイル」を参照してください。
4. JP1/Base を起動する。
5. JP1/IM - Manager を起動する。

(b) リカバリー手順

1. JP1/IM - Manager を停止する。
2. JP1/Base を停止する。
3. バックアップしたファイルをそれぞれのディレクトリに配置する。
4. JP1/Base を起動する。

5. JP1/IM - Manager を起動する。

❗ 重要

リカバリーするとバックアップしてからリカバリーするまでに実行した自動アクション、および [コマンド実行] 画面から実行したコマンドの履歴が参照できなくなります。

(c) バックアップ対象ファイル

バックアップ対象のファイルを次に示します。

Windows の場合

表 1-7 バックアップ対象ファイル (Windows)

情報の種類	対象ファイル
コマンド実行履歴ファイル	Base パス¥log¥COMMAND¥以下の全ファイル
	共有フォルダ¥jp1base¥log¥COMMAND¥以下の全ファイル
アクション情報ファイル	Console パス¥log¥action¥actinf.log
	共有フォルダ¥jp1cons¥log¥action¥actinf.log
アクションホスト名格納ファイル	Console パス¥log¥action¥acttxt{1 2}.log
	共有フォルダ¥jp1cons¥log¥action¥acttxt{1 2}.log

UNIX の場合

表 1-8 バックアップ対象ファイル (UNIX)

情報の種類	対象ファイル
コマンド実行履歴ファイル	/var/opt/jp1base/log/COMMAND/以下の全ファイル
	共有ディレクトリ/jp1base/log/COMMAND/以下の全ファイル
アクション情報ファイル	/var/opt/jp1cons/log/action/actinf.log
	共有ディレクトリ/jp1cons/log/action/actinf.log
アクションホスト名格納ファイル	/var/opt/jp1cons/log/action/acttxt{1 2}.log
	共有ディレクトリ/jp1cons/log/action/acttxt{1 2}.log

コマンド実行履歴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) 監視オブジェクト DB のバックアップ・リカバリー手順

監視オブジェクト DB のバックアップ・リカバリー手順について説明します。監視オブジェクト DB は、セントラルスコープの機能を使用している場合に使われます。

(a) バックアップ手順

1. JP1/IM - Manager を停止する。
2. 対象ファイルのバックアップを取得する。

対象ファイルを次の表に示します。

表 1-9 バックアップ対象ファイル

OS	情報の種類	対象ファイル
Windows	監視オブジェクト DB	Scope パス¥database¥jcsdb¥以下の全ファイル
		共有フォルダ¥jp1scope¥database¥jcsdb¥以下の全ファイル
UNIX	監視オブジェクト DB	/var/opt/jp1scope/database/jcsdb/以下の全ファイル
		共有ディレクトリ/jp1scope/database/jcsdb/以下の全ファイル

3. JP1/IM - Manager を起動する。

(b) リカバリー手順

1. JP1/IM - Manager を停止する。
2. バックアップしたファイルをディレクトリに配置する。
3. JP1/IM - Manager を起動する。

(3) ホスト情報 DB のバックアップ・リカバリー手順

ホスト情報 DB のバックアップ・リカバリー手順について説明します。ホスト情報 DB は、セントラルスコープの機能を使用している場合に使われます。

(a) バックアップ手順

1. JP1/IM - Manager を停止する。
2. 対象ファイルのバックアップを取得する。

対象ファイルを次の表に示します。

表 1-10 バックアップ対象ファイル

OS	情報の種類	対象ファイル
Windows	ホスト情報 DB	Scope パス¥database¥jcshosts¥以下の全ファイル
		共有フォルダ¥jp1scope¥database¥jcshosts¥以下の全ファイル
UNIX	ホスト情報 DB	/var/opt/jp1scope/database/jcshosts/以下の全ファイル
		共有ディレクトリ/jp1scope/database/jcshosts/以下の全ファイル

3. JP1/IM - Manager を起動する。

(b) リカバリー手順

1. JP1/IM - Manager を停止する。
2. バックアップしたファイルをディレクトリに配置する。
3. JP1/IM - Manager を起動する。

(4) イベント DB のバックアップ・リカバリー手順

イベント DB のバックアップ・リカバリー手順については、マニュアル「JP1/Base 運用ガイド」のバックアップとリカバリーの説明を参照してください。

なお、JP1/IM - Manager ホストのイベント DB をバックアップ・リカバリーする場合、同時にコマンド実行履歴もバックアップ・リカバリーする必要があります。コマンド実行履歴のバックアップ・リカバリーの手順については、「1.2.2(1) コマンド実行履歴のバックアップ・リカバリー手順」を参照してください。

❗ 重要

イベント DB をバックアップ・リカバリーする場合は、必ずコマンド実行履歴も同時にバックアップ・リカバリーしてください。

イベント DB だけをバックアップ・リカバリーすると、イベント DB 内の JP1 イベントと自動アクションの実行結果の関連づけに矛盾が発生します。

イベント DB のリカバリーの前に実行された自動アクションの結果が、イベント DB のリカバリーのあとに登録された JP1 イベントに対する自動アクションの実行結果として表示されてしまうことがあります。

(5) 応答待ちイベント滞留ファイルのバックアップ・リカバリー手順

応答待ちイベント滞留ファイルのバックアップ・リカバリー手順について説明します。応答待ちイベント滞留ファイルは、応答待ちイベント管理機能を使用している場合に使われます。

(a) バックアップ手順

1. JP1/IM - Manager を停止する。
2. 対象ファイルのバックアップを取得する。
対象ファイルを次の表に示します。

表 1-11 バックアップ対象ファイル

OS	対象ファイル
Windows	Console パス¥log¥response¥resevent.dat
	共有フォルダ¥jp1cons¥log¥response¥resevent.dat
UNIX	/var/opt/jp1cons/log/response/resevent.dat
	共有ディレクトリ/jp1cons/log/response/resevent.dat

3. JP1/IM - Manager を起動する。

(b) リカバリー手順

1. JP1/IM - Manager を停止する。

2. バックアップしたファイルをディレクトリに配置する。

3. JP1/IM - Manager を起動する。

(6) IM データベースのバックアップ・リカバリー手順

ここでは、物理ホストでの IM データベースのバックアップ・リカバリー手順、およびクラスタ環境での IM データベースのバックアップ・リカバリー手順について説明します。

❗ 重要

IM データベースのバックアップ・リカバリーをする場合、同時にイベント DB のバックアップ・リカバリーをする必要があります。イベント DB のバックアップ・リカバリーの手順については、「1.2.2(4) イベント DB のバックアップ・リカバリー手順」を参照してください。

❗ 重要

イベント DB のリカバリー方法によってはイベント DB の再作成が必要になることがあり、イベント DB の再作成方法によっては IM データベースの再作成が必要になることがあります。この場合、IM データベースをリカバリーするとイベント DB の情報と不整合が発生し、対処状況変更時に意図しない JP1 イベントの対処状況が変更されるなどの影響があるため、IM データベースをリカバリーしないでください。

❗ 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。

(a) 物理ホストでの IM データベースのバックアップ・リカバリー手順

物理ホストでのバックアップ手順を次に示します。

1. Windows の場合、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
 - Windows の場合、IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service)
 - 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. jimdbbackup コマンドを使用して、対象データベースのバックアップを取得する。

jimdbbackup 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「jimdbbackup」(1. コマンド)を参照してください。
4. 対象ファイルのバックアップを取得する。

対象ファイルについては、「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。
5. インテリジェント統合管理基盤を使用している場合、次の表に示すファイルを削除する。
6. 手順 2 で停止したサービスを起動する。

物理ホストでのリカバリー手順を次に示します。

1. Windows の場合、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
 - Windows の場合、IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service)
 - 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. jimdbrecovery コマンドを使用して、対象データベースをリカバリーする。

jimdbrecovery 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「jimdbrecovery」(1. コマンド)を参照してください。

4. バックアップしたファイルを各ディレクトリに配置する。

IM 構成管理の機能を有効にしている場合、バックアップしたファイルを各ディレクトリに配置してください。

5. インテリジェント統合管理基盤を使用している場合、次の表に示すファイルを削除する。

OS	対象ファイル
Windows	Manager パス\data\imdd\actevent.ser
	Manager パス\data\imdd\imdd_nodeStatus.ser
	Manager パス\data\imdd\jddactseq.ser
UNIX	/var/opt/jplimm/data/imdd/actevent.ser
	/var/opt/jplimm/data/imdd/imdd_nodeStatus.ser
	/var/opt/jplimm/data/imdd/jddactseq.ser

6. 手順 2 で停止したサービスを起動する。

7. インテリジェント統合管理基盤を使用している場合、jddupdatetree コマンドを新規・再構築モードで実行する。

(b) クラスタ環境での IM データベースのバックアップ・リカバリー手順

クラスタ環境でのバックアップ手順を次に示します。クラスタ環境の場合、実行系ホスト上で実行します。また、共有ディレクトリにアクセスできる状態である必要があります。

1. JP1/IM3-Manager サービスおよび IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を停止する。

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. jimdbbackup コマンドを使用して、対象データベースのバックアップを取得する。

jimdbbackup 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「jimdbbackup」(1. コマンド) を参照してください。

3. 対象ファイルのバックアップを取得する。

対象ファイルについては、「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。

4. JP1/IM3-Manager サービスおよび手順 1 で停止した IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を起動する。

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 サービスも起動してください。

クラスタ環境でのリカバリー手順を次に示します。クラスタ環境の場合、実行系ホスト上で実行します。また、共有ディレクトリにアクセスできる状態である必要があります。

1. JP1/IM3-Manager サービスおよび IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を停止する。

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. jimdbrecovery コマンドを使用して、対象データベースをリカバリーする。

jimdbrecovery 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「jimdbrecovery」(1. コマンド) を参照してください。

3. バックアップしたファイルを各ディレクトリに配置する。

IM 構成管理の機能を有効にしている場合、バックアップしたファイルを各ディレクトリに配置してください。

4. インテリジェント統合管理基盤を使用している場合、次の表に示すファイルを削除する。

OS	対象ファイル
Windows	共有フォルダ¥data¥imdd¥actevent.ser
	共有フォルダ¥data¥imdd¥imdd_nodeStatus.ser
	共有フォルダ¥data¥imdd¥jddactseq.ser
UNIX	共有ディレクトリ/jp1imm/data/imdd/actevent.ser
	共有ディレクトリ/jp1imm/data/imdd/imdd_nodeStatus.ser
	共有ディレクトリ/jp1imm/data/imdd/jddactseq.ser

5. JP1/IM3-Manager サービスおよび手順 1 で停止した IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を起動する。

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 サービスも起動してください。

6. インテリジェント統合管理基盤を使用している場合、jddupdatetree コマンドを新規・再構築モードで実行する。

(7) インテリジェント統合管理データベースのバックアップ・リカバリー手順

インテリジェント統合管理データベースで障害が発生したときの復旧手段として、定期的にバックアップを行ってください。バックアップを取得する方法は、オフラインバックアップです。

計画停止などでインテリジェント統合管理データベースのサービスを停止できる場合に、インテリジェント統合管理データベースのサービスを停止した状態で行うオフラインバックアップおよびリカバリーの方法について説明します。

なお、ファイルおよびディレクトリをコピーするときは、Linux の場合はディレクトリおよびファイルの属性を保持したままコピーしてください。

(a) バックアップ手順

インテリジェント統合管理データベースのオフラインバックアップの手順を、次に示します。

1. JP1/IM - Manager のサービスを停止する。

停止方法については、「[3.2 JP1/IM - Manager を終了する](#)」を参照してください。

2. インテリジェント統合管理データベースのサービスを停止する。

■Windows の場合

インテリジェント統合管理データベースサービス、および、トレンドデータ管理サービスを停止する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、トレンドデータ管理サービス、インテリジェント統合管理データベースサービスの順番で停止してください。

■Linux の場合

JP1/IM - Manager の停止に合わせて、インテリジェント統合管理データベース、および、トレンドデータ管理サービスも停止します。詳細については、「[3.2.2 UNIX の場合](#)」を参照してください。

3. IM データベース（統合監視 DB）の障害復旧用バックアップを行う（インテリジェント統合管理データベースに合わせて統合監視 DB のバックアップを取得する場合）。

バックアップ方法については、「[1.2.2\(6\)\(a\) 物理ホストでの IM データベースのバックアップ・リカバリー手順](#)」および「[1.2.2\(6\)\(b\) クラスタ環境での IM データベースのバックアップ・リカバリー手順](#)」を参照してください。

4. jimgnbdbbackup コマンド（引数-m に MAINT を指定）を使用して、インテリジェント統合管理データベースの障害復旧用バックアップを行う。

jimgnbdbbackup コマンドの詳細や実行例については、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「jimgnbdbbackup」（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データベースのサービスを起動する。

■Windows の場合

インテリジェント統合管理データベースのサービスを起動する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、インテリジェント統合管理データベースサービス、トレンドデータ管理サービスを順番に起動してください（依存関係があるため、トレンドデータ管理サービスを起動すると、連動して。インテリジェント統合管理データベースサービスが自動で起動します）。

■Linux の場合

JP1/IM - Manager の起動に合わせて、インテリジェント統合管理データベース、および、トレンドデータ管理サービスも起動します。詳細については、「[3.1.2 UNIX の場合](#)」を参照してください。

6. JP1/IM - Manager のサービスを起動する。

起動方法については、「[3.1 JP1/IM - Manager を起動する](#)」を参照してください。

(b) リカバリー手順

オフラインバックアップで取得したインテリジェント統合管理データベースのバックアップをリカバリーする手順を、次に示します。

1. JP1/IM - Manager のサービスを停止する。

停止方法については、「[3.2 JP1/IM - Manager を終了する](#)」を参照してください。

2. JP/IM - Agent のサービスを停止する。

JP/IM - Agent の停止の詳細については、「[10.3 サービスの停止](#)」を参照してください。

3. インテリジェント統合管理データベースを削除する。

削除方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「[1.25.1 \(1\) インテリジェント統合管理データベースの削除の手順](#)」および「[2.23.1 \(1\) インテリジェント統合管理データベースの削除の手順](#)」を参照してください。

4. インテリジェント統合管理データベースを構築する。

構築方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「[1.5 インテリジェント統合管理データベースの構築 \(Windows の場合\)](#)」および「[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。

5. インテリジェント統合管理データベースのサービスを停止する。

■Windows の場合

インテリジェント統合管理データベースサービス、および、トレンドデータ管理サービスを停止する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、トレンドデータ管理サービス、インテリジェント統合管理データベースサービスの順番で停止してください。

■Linux の場合

JP1/IM - Manager の停止に合わせて、インテリジェント統合管理データベース、および、トレンドデータ管理サービスも停止します。詳細については、「[3.2.2 UNIX の場合](#)」を参照してください。

6. IM データベース (統合監視 DB) の障害復旧用リカバリーを行う

(インテリジェント統合管理データベースに合わせて統合監視 DB のリカバリーを取得する場合)。

リカバリー方法については、「[1.2.2\(6\)\(a\) 物理ホストでの IM データベースのバックアップ・リカバリー手順](#)」および「[1.2.2\(6\)\(b\) クラスタ環境での IM データベースのバックアップ・リカバリー手順](#)」を参照してください。

7. jimgnbrestore コマンド (引数-m に MAINT を指定) を使用して、インテリジェント統合管理データベースの障害復旧用リカバリーを行う。

jimgnbrestore コマンドの詳細や実行例については、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「[jimgnbrestore](#)」(1. コマンド)を参照してください。

8. インテリジェント統合管理データベースのサービスを起動する。

■Windows の場合

インテリジェント統合管理データベースのサービスを起動する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、インテリジェント統合管理データベースサービス、トレンドデータ管理サービスを順番に起動してください（依存関係があるため、トレンドデータ管理サービスを起動すると、連動して。インテリジェント統合管理データベースサービスが自動で起動します）。

■Linux の場合

JP1/IM - Manager の起動に合わせて、インテリジェント統合管理データベース、および、トレンドデータ管理サービスも起動します。詳細については、「[3.1.2 UNIX の場合](#)」を参照してください。

9. JP1/IM - Agent のサービスを起動する。

JP1/IM - Agent の起動の詳細については、「[10.2 サービスの起動](#)」を参照してください。

10. JP1/IM - Manager のサービスを起動する。

起動方法については、「[3.1 JP1/IM - Manager を起動する](#)」を参照してください。

11. jddupdatetree コマンドを新規・再構築モードで実行する。

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) を参照してください。

IM データベース（統合監視 DB）のリカバリーも合わせて行う場合は、IM データベース（統合監視 DB）のリカバリーの実施後に実行してください。

1.2.3 データベースの再作成および設定変更

(1) コマンド実行履歴の再作成手順

1. JP1/IM - Manager を停止する。

2. JP1/Base を停止する。

3. 次の表に示すコマンド実行履歴ファイル、アクション情報ファイル、アクションホスト名格納ファイルを削除する。

Windows の場合

表 1-12 削除対象ファイル (Windows)

情報の種類	対象ファイル
コマンド実行履歴ファイル	Base パス¥log¥COMMAND¥以下の全ファイル
	共有フォルダ¥jp1base¥log¥COMMAND¥以下の全ファイル
アクション情報ファイル	Console パス¥log¥action¥actinf.log
	共有フォルダ¥jp1cons¥log¥action¥actinf.log

情報の種類	対象ファイル
アクションホスト名格納ファイル	Console パス¥log¥action¥acttxt{1 2}.log
	共有フォルダ¥jp1cons¥log¥action¥acttxt{1 2}.log

UNIX の場合

表 1-13 削除対象ファイル (UNIX)

情報の種類	対象ファイル
コマンド実行履歴ファイル	/var/opt/jp1base/log/COMMAND/以下の全ファイル
	共有ディレクトリ/jp1base/log/COMMAND/以下の全ファイル
アクション情報ファイル	/var/opt/jp1cons/log/action/actinf.log
	共有ディレクトリ/jp1cons/log/action/actinf.log
アクションホスト名格納ファイル	/var/opt/jp1cons/log/action/acttxt{1 2}.log
	共有ディレクトリ/jp1cons/log/action/acttxt{1 2}.log

4. JP1/Base を起動する。

5. JP1/IM - Manager を起動する。

JP1/Base, JP1/IM - Manager を再起動し, JP1/IM - View や自動アクションからコマンド実行することでコマンド実行履歴が再作成されます。

(2) 監視オブジェクト DB およびホスト情報 DB の再作成手順

1. JP1/IM - Manager を停止する。

2. ファイルをバックアップする。

Scope パス¥database¥フォルダをバックアップしてください。

3. 監視オブジェクト DB を再作成する。

```
jcsdbsetup -f
```

コマンドを実行すると, 既存の監視オブジェクト DB を削除したあと, オブジェクト DB が再作成されます。

4. ホスト情報 DB を再作成する。

まず, Scope パス¥database¥jcshosts¥フォルダ以下のファイルを削除してから次のコマンドを実行してください。

```
jcshostsimport -r ホスト情報ファイル (jcs_hosts)
```

5. JP1/IM - Manager を起動する。

(3) イベント DB の再作成手順

イベント DB を再作成する対象ホストにインストールされている JP1/Base のバージョンによって、手順が異なります。

(a) マネージャー (JP1/Base 09-00 以降) の場合

統合監視 DB を使用しない場合と統合監視 DB を使用する場合で手順が異なります。

統合監視 DB を使用しない場合

JP1/Base の `jevdbinit` コマンドを実行してイベント DB を初期化します。

JP1/Base のイベント DB を初期化する手順については、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、イベント DB の初期化に関する説明を参照してください。

`jevdbinit` コマンドの `-s` オプションを指定してイベント DB 内通し番号を変更した場合は、コマンド実行履歴を再作成する必要があります。

コマンド実行履歴の再作成については、「[1.2.3\(1\) コマンド実行履歴の再作成手順](#)」を参照してください。

統合監視 DB を使用する場合

次の手順に従って、イベント DB を初期化します。

1. JP1/IM - Manager を停止する。
2. JP1/Base の `jevdbinit` コマンドを `-s` オプションを指定しないで実行する。
-s オプションを指定しないと、初期化する前のイベント DB 内通し番号を引き継ぎます。

`jevdbinit` コマンドの `-s` オプションを指定してイベント DB 内通し番号を変更した場合は、統合監視 DB の再セットアップ、およびコマンド実行履歴を再作成する必要があります。また、インテリジェント統合管理基盤を使用している場合、統合監視 DB の再セットアップ後の JP1/IM - Manager を起動する前に次の表に示すファイルを削除する必要があります。

OS	対象ファイル
Windows	Manager パス\data\imdd\actevent.ser
	Manager パス\data\imdd\imdd_nodeStatus.ser
	Manager パス\data\imdd\jddactseq.ser
	共有フォルダ\data\imdd\actevent.ser
	共有フォルダ\data\imdd\imdd_nodeStatus.ser
	共有フォルダ\data\imdd\jddactseq.ser
UNIX	/var/opt/jplimm/data/imdd/actevent.ser
	/var/opt/jplimm/data/imdd/imdd_nodeStatus.ser
	/var/opt/jplimm/data/imdd/jddactseq.ser
	共有ディレクトリ/jplimm/data/imdd/actevent.ser

OS	対象ファイル
	共有ディレクトリ/jp1imm/data/imdd/imdd_nodeStatus.ser
	共有ディレクトリ/jp1imm/data/imdd/jddactseq.ser

統合監視 DB の再セットアップは、最初に、jcodbunsetup コマンドを実行して統合監視 DB をアンセットアップしてください。

コマンド実行履歴の再作成については、「1.2.3(1) コマンド実行履歴の再作成手順」を参照してください。

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

なお、-s オプションを指定してjevdbinit コマンドを実行した場合、セントラルスコープでルート of 監視ノードを選択し、ステータスを変更して、状態変更イベント履歴を削除する必要があります。

(b) エージェント (JP1/Base 07-11 以降) の場合

JP1/Base のjevdbinit コマンドを実行してイベント DB を初期化します。イベント DB の削除および再作成は必要ありません。

JP1/Base のイベント DB を初期化する手順については、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、イベント DB の初期化に関する説明を参照してください。

❗ 重要

エージェント側でイベント DB を初期化した場合、JP1/Base はイベントをイベント DB に登録しないで破棄します。このため、手順どおりに実施しない場合、イベント DB を初期化したあとに一部のイベントが転送されなくなることがあります。

(c) エージェント (JP1/Base 07-10 以前) の場合

イベント DB を再作成すると、次の問題が発生します。

- JP1 イベントの転送先のホストで、JP1 イベントの転送受け付け、登録、および取得の処理性能が劣化する。

これは、再作成によって転送元のイベント DB が初期化され、転送先のイベント DB の管理情報と不整合が発生するためです。

❗ 重要

エージェント側でイベント DB を初期化した場合、JP1/Base はイベントをイベント DB に登録しないで破棄します。このため、手順どおりに実施しない場合、イベント DB を初期化したあとに一部のイベントが転送されなくなることがあります。

問題発生を防ぐため、次の手順に従ってイベント DB を再作成してください。

1. JP1/Base を停止する。

2. 手順 1 で停止した JP1/Base の転送設定ファイル (forward) に定義されているすべての転送先ホストの JP1/Base を停止する。

転送先ホストの JP1/Base から、さらにほかのホストへ転送している場合、その転送先も同様に停止します。なお、停止するホストに JP1/IM - Manager をインストールしている場合は、JP1/IM - Manager を事前に停止してください。

転送設定ファイル (forward) 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、JP1 イベントの転送設定の説明を参照してください。

3. 手順 1, 2 で停止した JP1/Base のイベント DB を削除する。

イベント DB の内容を参照する必要がある場合、JP1/Base の `jevexport` コマンドで CSV ファイルに出力しておいてください。なお、出力した CSV ファイルを使ってイベント DB を再作成することはできません。

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

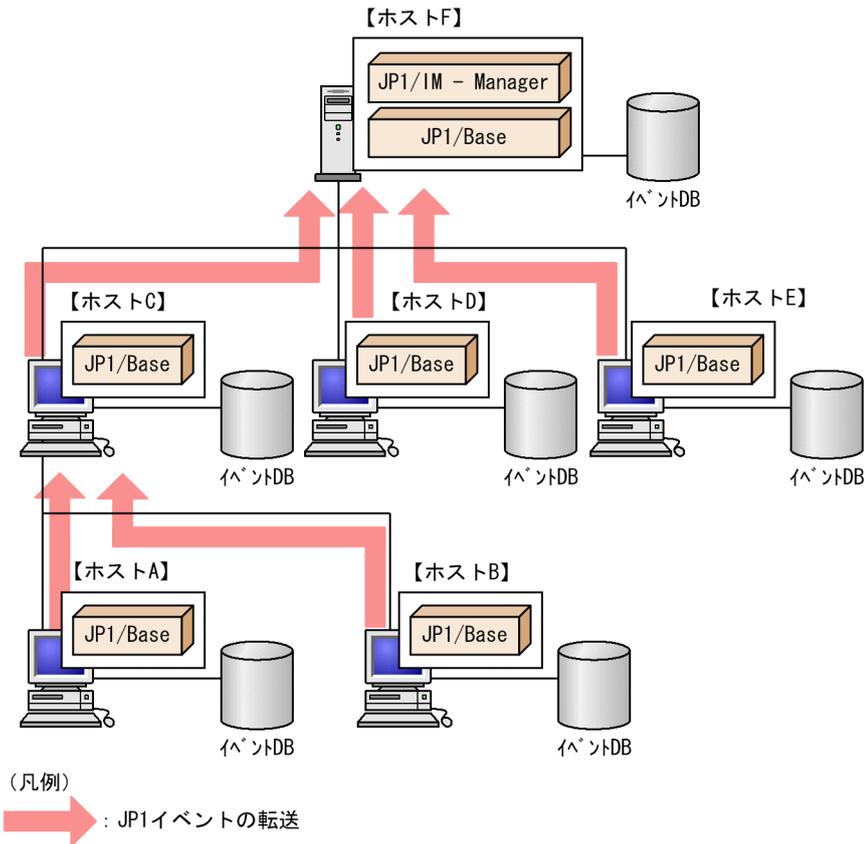
4. 手順 2 で停止した JP1/Base (および JP1/IM - Manager) を起動する。

5. 手順 1 で停止した JP1/Base を起動する。

手順 4, 5 で JP1/Base を起動することで、イベント DB が再作成されます。

例えば、次の図に示すようなシステム構成でイベント DB を再作成するとします。

図 1-1 イベント DB を再作成したいホストと転送先ホストの例



ホスト A のイベント DB を再作成（削除）する場合、JP1 イベントの転送先ホストであるホスト C およびホスト F のイベント DB を削除する必要があります。

(4) 応答待ちイベント滞留ファイルの再作成手順

1. JP1/IM - Manager を停止する。
2. 応答待ちイベント滞留ファイルを削除する。

表 1-14 削除対象ファイル

OS	対象ファイル
Windows	Console パス¥log¥response¥revent.dat
	共有フォルダ¥jp1cons¥log¥response¥revent.dat
UNIX	/var/opt/jp1cons/log/response/revent.dat
	共有ディレクトリ/jp1cons/log/response/revent.dat

3. JP1/IM - Manager を起動する。

(5) IM データベースのサイズ拡張手順

ここでは、物理ホストでの IM データベースのサイズ拡張手順、およびクラスタ環境での IM データベースのサイズ拡張手順について説明します。なお、セットアップ情報ファイル (jimdbsetupinfo.conf) でデータベースのサイズに L を指定して IM データベースを作成した場合、IM データベースのサイズは拡張できません。

(a) 物理ホストでの IM データベースのサイズ拡張手順

データベースのサイズ拡張時に IM データベースを使用しないでイベントを監視するかどうかで手順が異なります。それぞれの手順を次に示します。

- データベースのサイズ拡張時に IM データベースを使用しないでイベントを監視する場合の手順

1. 統合監視 DB および IM 構成管理 DB を切り離す。

統合監視 DB および IM 構成管理 DB を切り離し、セントラルコンソールが JP1/Base のイベント DB だけを使用するようにします。

次のコマンドを実行したあと、JP1/IM - Manager を再起動してください。

```
jcoimdef -db OFF
```

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。

また、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. データベースをバックアップする。

-m EXPAND オプションを指定して、jimdbbackup コマンドを実行します。

jimdbbackup 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「jimdbbackup」(1. コマンド) を参照してください。

3. 統合監視 DB と IM 構成管理 DB をアンセットアップする。

セットアップしているデータベースだけ、アンセットアップします。

4. セットアップ情報ファイルを編集する。

セットアップ情報ファイルのデータベースサイズ (IMDBSIZE) に指定したサイズを変更します。

5. JP1/IM - Manager を停止する。

6. JP1/Base を停止する。

7. OS を再起動する。

8. JP1/Base を起動する。

9. JP1/IM - Manager を起動する。

10. 統合監視 DB と IM 構成管理 DB をセットアップする。

手順 3 でアンセットアップしたデータベースだけ、セットアップします。

セットアップ時には、バックアップ時より大きなデータベースサイズと、バックアップ時と同じデータベース格納ディレクトリを指定する必要があります。

11. データベースをリカバリーする。

-m EXPAND オプションを指定して `jimdbrecovery` コマンドを実行します。

`jimdbrecovery` 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「`jimdbrecovery`」(1. コマンド)を参照してください。

12. JP1/IM3-Manager サービスを再起動する。

次のコマンドを実行したあと、JP1/IM - Manager を再起動してください。

```
jcoimdef -db ON
```

`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。

また、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 サービスも起動してください。

13. インテリジェント統合管理基盤を使用している場合、`jddupdatetree` コマンドを新規・再構築モードで実行する。

`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)を参照してください。

- データベースのサイズ拡張時にセントラルコンソールによるシステムの監視を停止する場合の手順

1. JP1/IM3-Manager サービスを停止する。

2. データベースをバックアップする。

-m EXPAND オプションを指定して、`jimdbbackup` コマンドを実行します。

`jimdbbackup` 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「`jimdbbackup`」(1. コマンド)を参照してください。

3. 統合監視 DB と IM 構成管理 DB をアンセットアップする。

セットアップしているデータベースだけ、アンセットアップします。

4. セットアップ情報ファイルを編集する。

セットアップ情報ファイルのデータベースサイズ (IMDBSIZE) に指定したサイズを変更します。

5. JP1/Base を停止する。

6. OS を再起動する。

7. JP1/Base を起動する。

8. 統合監視 DB と IM 構成管理 DB をセットアップする。

手順 3 でアンセットアップしたデータベースだけ、セットアップします。

セットアップ時には、バックアップ時より大きなデータベースサイズと、バックアップ時と同じデータベース格納ディレクトリを指定する必要があります。

9. データベースをリカバリーする。

-m EXPAND オプションを指定して `jimdbrecovery` コマンドを実行します。

`jimdbrecovery` 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「`jimdbrecovery`」(1. コマンド)を参照してください。

10. JP1/IM3-Manager サービスを起動する。

11. インテリジェント統合管理基盤を使用している場合、`jddupdatetree` コマンドを新規・再構築モードで実行する。

`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)を参照してください。

(b) クラスタ環境での IM データベースのサイズ拡張手順

データベースのサイズ拡張時にセントラルコンソールによるシステムの監視を継続するかどうかで手順が異なります。それぞれの手順を次に示します。

- データベースのサイズ拡張時にセントラルコンソールによるシステムの監視を継続（機能は一部縮退）する場合の手順

1. 統合監視 DB および IM 構成管理 DB を切り離す。

統合監視 DB および IM 構成管理 DB を切り離し、セントラルコンソールが JP1/Base のイベント DB だけを使用するようにします。

次のコマンドを実行したあと、JP1/IM - Manager を再起動してください。

```
jcoimdef -db OFF -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。

また、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. IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を停止する。

クラスタソフトに登録した IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を停止します。

3. データベースをバックアップする。

-m EXPAND オプションを指定して、`jimdbbackup` コマンドを実行します。

jimdbbackup 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「jimdbbackup」(1. コマンド)を参照してください。

4. 統合監視 DB と IM 構成管理 DB をアンセットアップする。

セットアップしているデータベースだけ、アンセットアップします。

5. クラスタセットアップ情報ファイルを編集する。

クラスタセットアップ情報ファイルのデータベースサイズ (IMDBSIZE) に指定したサイズを変更します。

6. JP1/IM - Manager を停止する。

7. JP1/Base を停止する。

8. OS を再起動する。

9. JP1/Base を起動する。

10. JP1/IM - Manager を起動する。

11. 統合監視 DB と IM 構成管理 DB をセットアップする。

手順 4 でアンセットアップしたデータベースだけ、セットアップします。

セットアップ時には、バックアップ時より大きなデータベースサイズと、バックアップ時と同じデータベース格納ディレクトリを指定する必要があります。

12. データベースをリカバリーする。

-m EXPAND オプションを指定して jimdbrecovery コマンドを実行します。

jimdbrecovery 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「jimdbrecovery」(1. コマンド)を参照してください。

13. IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を起動する。

手順 2 で停止した IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を起動します。

14. JP1/IM3-Manager サービスを再起動する。

次のコマンドを実行したあと、JP1/IM - Manager を再起動してください。

```
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。

また、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 サービスも起動してください。

15. インテリジェント統合管理基盤を使用している場合、jddupdatetree コマンドを新規・再構築モードで実行する。

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)を参照してください。

- データベースのサイズ拡張時にセントラルコンソールによるシステムの監視を停止する場合の手順

1. JP1/IM3-Manager サービスおよび IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を停止する。

JP1/IM3-Manager サービスおよびクラスタソフトに登録した IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を停止します。

2. データベースをバックアップする。

-m EXPAND オプションを指定して、jimdbbackup コマンドを実行します。

jimdbbackup 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「jimdbbackup」(1. コマンド)を参照してください。

3. 統合監視 DB と IM 構成管理 DB をアンセットアップする。

セットアップしているデータベースだけ、アンセットアップします。

4. クラスタセットアップ情報ファイルを編集する。

クラスタセットアップ情報ファイルのデータベースサイズ (IMDBSIZE) に指定したサイズを変更します。

5. JP1/Base を停止する。

6. OS を再起動する。

7. JP1/Base を起動する。

8. 統合監視 DB と IM 構成管理 DB をセットアップする。

手順 3 でアンセットアップしたデータベースだけ、セットアップします。

セットアップ時には、バックアップ時より大きなデータベースサイズと、バックアップ時と同じデータベース格納ディレクトリを指定する必要があります。

9. データベースをリカバリーする。

-m EXPAND オプションを指定して jimdbrecovery コマンドを実行します。

jimdbrecovery 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「jimdbrecovery」(1. コマンド)を参照してください。

10. JP1/IM3-Manager サービスおよび IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を起動する。

手順 1 で停止した JP1/IM3-Manager サービスおよび IM データベースのクラスタサービス (JP1/IM3-Manager DB Cluster Service_論理ホスト名) を起動します。

11. インテリジェント統合管理基盤を使用している場合、jddupdatetree コマンドを新規・再構築モードで実行する。

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)を参照してください。

(6) IM データベースのポート変更手順

1. JP1/IM3-Manager サービスを停止する。

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. データベースをバックアップする。

-m MAINT オプションを指定して、jimdbbackup コマンドを実行します。

jimdbbackup 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「jimdbbackup」(1. コマンド)を参照してください。

3. 統合監視 DB と IM 構成管理 DB をアンセットアップする。

セットアップしているデータベースだけ、アンセットアップします。

4. セットアップ情報ファイルを編集する。

セットアップ情報ファイルに記載されているポート番号を変更します。

5. JP1/Base を停止する。

6. OS を再起動する。

7. JP1/Base を起動する。

8. 統合監視 DB と IM 構成管理 DB をセットアップする。

手順 3 でアンセットアップしたデータベースだけ、セットアップします。

9. データベースをリカバリーする。

-m MAINT オプションを指定してjimdbrecovery コマンドを実行します。

jimdbrecovery 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「jimdbrecovery」(1. コマンド)を参照してください。

10. JP1/IM - Manager を起動する。

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 サービスも起動してください。

11. インテリジェント統合管理基盤を使用している場合、jddupdatetree コマンドを新規・再構築モードで実行する。

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)を参照してください。

(7) IM データベース再構築手順

ここでは、マネージャーのホスト名を変更した場合に必要な IM データベースの再構築手順について説明します。なお、物理ホストまたは論理ホストのホスト名を変更した場合も、IM データベースを再構築する必要があります。また、論理ホストのホスト名変更の場合は、クラスタソフトに登録する IM データベースのサービスも本手順で作成されたサービスを再登録する必要があります。再構築の手順を次に示します。

1. JP1/IM3-Manager サービスを停止する。

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 と IM 構成管理 DB をアンセットアップする。

セットアップしているデータベースだけ、アンセットアップします。

3. JP1/IM - Manager のインストールされているホストのホスト名を変更する。

ホスト名を変更しない場合、この手順は不要です。

4. JP1/Base を停止する。

5. OS を再起動する。

6. JP1/Base を起動する。

7. 統合監視 DB と IM 構成管理 DB をセットアップする。

手順 2 でアンセットアップしたデータベースだけ、セットアップします。

論理ホストのセットアップ時は、クラスタセットアップ情報ファイルの論理ホスト名の編集が必要です。

8. インテリジェント統合管理基盤を使用している場合、次の表に示すファイルを削除する。

OS	対象ファイル
Windows	Manager パス\data\imdd\actevent.ser
	Manager パス\data\imdd\imdd_nodeStatus.ser
	Manager パス\data\imdd\jddactseq.ser
	共有フォルダ\data\imdd\actevent.ser
	共有フォルダ\data\imdd\imdd_nodeStatus.ser
	共有フォルダ\data\imdd\jddactseq.ser
UNIX	/var/opt/jplimm/data/imdd/actevent.ser
	/var/opt/jplimm/data/imdd/imdd_nodeStatus.ser
	/var/opt/jplimm/data/imdd/jddactseq.ser
	共有ディレクトリ/jplimm/data/imdd/actevent.ser
	共有ディレクトリ/jplimm/data/imdd/imdd_nodeStatus.ser

OS	対象ファイル
	共有ディレクトリ/jp1imm/data/imdd/jddactseq.ser

9. JP1/IM - Manager を起動する。

変更対象ホストの JP1/IM - Manager を起動します。

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 サービスも起動してください。

10. インテリジェント統合管理基盤を使用している場合、jddupdatetree コマンドを新規・再構築モードで実行する。

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)を参照してください。

❗ 重要

ホスト名を変更して IM データベースを再構築する場合は、データベースをリカバリーできません。必要に応じて、jcoevreport コマンドを使って JP1 イベントの保存出力、および jcfexport コマンドを使って IM 構成管理情報の保存を実施してください。各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「1. コマンド」を参照してください。

なお、ホスト名を変更しない場合はデータベースをリカバリーできます。詳細については、「1.2.2 データベースのバックアップおよびリカバリー」を参照してください。

1.3 ディスク容量の管理

JP1/IM の運用を安定して継続するため、ディスクの空き容量を定期的に確認してください。

1.3.1 データベース容量の管理

(1) IM データベース容量の管理

JP1/IM が使用する統合監視 DB は、運用を継続しても無効領域が増加しないよう設計されています。必要な容量を確保していれば、運用中にデータベースを確認する必要はありません。

データ自体は、セットアップ時に作成されたデータベースに書き込むため、基本的にはセットアップ時に容量を見積もっておけば、容量の増加を考慮する必要はありません。

ログファイル容量の増加については、「[1.3.2 ログファイル容量の管理](#)」を参照してください。

統合監視 DB では、JP1 イベントの容量が格納可能な範囲を超えた場合、JP1 イベントが自動で削除されます。そのため、定期的に JP1 イベントの情報を保存出力し、データの消失を防ぐ必要があります。

次に、保存出力を用いてディスク容量を管理する手順を示します。

1. 保存出力に関する情報を確認する。

```
jcoevtreport -showsv
```

コマンドを実行すると、保存出力に関する情報を表示します。情報を参考に、保存出力する周期、保存出力に必要な空き容量を見積もってください。

表示する項目を次の表に示します。

表 1-15 表示する項目

表示項目	内容
未出力イベントの割合	統合監視 DB 内の保存出力していない JP1 イベントの割合（統合監視 DB の最大件数との比率）をパーセンテージで表示します。
未出力イベントのサイズ	統合監視 DB 内の保存出力していない JP1 イベントの統合監視 DB 内でのデータサイズを、メガバイト単位で表示します。 表示するサイズは、統合監視 DB 内でのデータサイズです。 CSV 出力には、表示された未出力イベントのサイズ×1.2 の容量が必要となります。
削除警告通知設定	削除警告通知位置の設定値を表示します。 削除警告通知が OFF の場合は「-」（半角ハイフン）を表示します。

2. 未出力イベントを保存出力する。

```
jcoevtreport -save
```

コマンドを実行すると、保存出力していない JP1 イベントをすべて CSV 形式で出力します。

jcoevtreport 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「jcoevtreport」(1. コマンド) を参照してください。

JP1 イベントが多く発生してしまい、定期的な保存出力では間に合わなかった場合は、削除警告通知イベントを発行できます。削除警告通知イベントは、保存出力していない JP1 イベントの割合が削除警告通知位置を超えたことを通知します。

次に、削除警告通知の設定手順を示します。

1. 削除警告通知イベントの発行を有効にする。

```
jcoimdef -dbntc ON
```

コマンドを実行すると、統合監視 DB 内の保存出力していない JP1 イベントの割合（統合監視 DB の最大件数との比率）が削除警告通知位置を超えたとき、削除警告通知イベントを発行する機能を有効にします。削除警告通知イベントのデフォルトはOFF です。

2. 削除警告通知位置を指定する。

```
jcoimdef -dbntcpos 70
```

コマンドを実行すると、削除警告通知イベントを発行する JP1 イベントの割合を、70%に指定します。

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。

IM 構成管理 DB を使用している場合については、「[1.2.1\(5\) IM データベースの再編成](#)」を参照してください。

(2) インテリジェント統合管理データベース容量の管理

インテリジェント統合管理データベースとして使用している PostgreSQL のディスク容量が不足すると、次のような問題が発生するおそれがあります。

- トレンドデータの書き込み、参照、削除の実行不可
- データベースの強制終了
- トレンドデータの破損※

注※

インテリジェント統合管理データベース (PostgreSQL) では、データベースの処理を高速に行えるように、トレンドデータが書き込まれる際のディスクアクセスをできる限り減らし、WAL (先行書き込みログ) と呼ばれるログにデータベースに対する更新操作 (トランザクション) の内容を書き出し、ある程度まとまった単位でディスクに書き出すようにしています。ディスクフルの状態となるタイミングによっては、この WAL への書き出しに失敗したり、WAL のファイル自体が破損したりすることが考えられます。

上記のような問題を未然に防止するには、ディスクの空き容量を監視する運用が必要です。

なお、データベース内で頻繁に登録が行われるデータに限り、データ件数が登録可能な上限に達した場合は、登録日時の古いデータが削除されて新しいデータが登録されます。

次の表に示す「JP1/IM - Manager での監視対象ディレクトリ」のディスクの空き容量を監視してください。

監視対象となる領域		JP1/IM - Manager での監視対象ディレクトリ
データベースクラスタ領域		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 ^{※1}
TABLESPACE 領域		
データベースの一時領域		
WAL の格納領域		
データベースのログの格納領域		
サーバーログの格納領域	運用コマンドの個別ログ	運用コマンドの個別ログの格納先 ^{※1}
	トレンドデータ管理サービスのログ	トレンドデータ管理サービスのログの格納先 ^{※1}
OS のログ	Windows イベントログ	システムドライブ:¥Windows¥System32¥winevt¥Logs
	syslog	/var/log ^{※2}
シスログ (syslog)		/var/log ^{※2}

注※1

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」を参照してください。

注※2

Linux 7 以降の場合、格納先は、「/etc/syslog.conf」または「/etc/rsyslog.conf」で変更できます。格納先を変更した場合は、変更先のディレクトリを監視対象としてください。

注意事項

データベースの再編成は自動で行うため、ユーザーによる再編成の必要はありません。

ユーザー単位のディスククォータを使用している場合は、トレンドデータ管理 DB を起動するユーザーに対して、ディスクの使用量と使用限度を監視してください。ディスクの容量不足に余裕をもって対処できるように、例えば、ディスクの空き容量が、全体の 20% を割り込む状態となったときに対処するなど、あらかじめ目安を設けておく運用を推奨します。

なお、インテリジェント統合管理データベースで管理するトレンドデータは、一定期間（デフォルトの保存期間は 32 日）が経過すると削除されますが、次のような場合に、トレンドデータが削除されるよりも前に、大量のトレンドデータがインテリジェント統合管理データベースに挿入されることで、ディスクが枯渇してしまうリスクが考えられます。

- トレンドデータの保存期間を長めに設定した場合
- 監視対象数やサンプル数が極端に多い場合

一定期間（1日、1週間など）の稼働後に、稼働前後のディスク使用量の増加量を元に、ディスクフルの状態となる時期を想定するなどして、事前に、ディスクの容量不足の対処に関する計画を立てておくことを検討してください。

(a) ディスクフル状態からの復旧

ディスクフルの状態となった場合に復旧する手順を、次に示します。

1. サービスが停止していることを確認する。

万が一、ディスクフルの状態となった場合、いったん監視エージェントからのリクエストを受け付けられない状態にして対処を行う必要があるため、インテリジェント統合管理データベースのサービス※が停止していることを確認してください。また、トレンドデータ管理サービスも停止させてください。

注※

ディスクフルの状態となった場合、サービスは強制終了していることが考えられますが、サービスが停止していなかったときは、停止させてください。

2. ディスクの空き領域を確保する。

不要なファイルの削除やディスク領域の追加（LVMなどOS機能）を行って、十分なディスクの空き領域を確保してください。

3. サービスを起動する。

インテリジェント統合管理データベースのサービス、およびトレンドデータ管理サービスを起動してください。

上記の手順で復旧できなかった場合は、インテリジェント統合管理データベースの削除および再構築を行ってください。定期的にバックアップを取得しているときは、バックアップからリカバリーすることで、前回バックアップを取得した時点の状態には復旧※できます。

注※

基本的には、ディスクフルの状態となった場合、それまでに収集したトレンドデータの復旧は保証できません。

1.3.2 ログファイル容量の管理

ディスク容量を圧迫する原因の一つとして、ログファイル容量の増加があります。

JP1/IM, JP1/Base の場合、ログファイルの容量を事前に見積もっておけば、ログファイル容量の増加を考慮する必要はありません。これは JP1/IM, JP1/Base が出力するログファイルは、複数のログファイルを切り替えて使用するなどの方式を採用しているためです。

OS や同ホストのほかの製品については、それぞれの仕様を確認してログファイルの容量が増加しないよう注意してください。

(1) インテリジェント統合管理データベースが出力するログの確認

PostgreSQL の設定に応じて、次に示すインテリジェント統合管理データベースのログを出力します。PostgreSQL の設定については、マニュアル「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の設定ファイル (postgresql.conf)」(2. 定義ファイル) を参照してください。

- 格納先

Windows の場合

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[※]¥log

UNIX の場合

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[※]/log

注※

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」を参照してください。

- ファイル名

postgresql-%a[※].log

注※

[%a] には、GMT タイムゾーンの曜日を表す英字 3 文字 (Mon, Tue, Wed, Thu, Fri, Sat, または Sun のどれか) が入ります。

- 出力内容

ログの出力行の形式を次に示します。

```
YYYY-MM-DD HH:MM:SS.FFF GMT [プロセスID] SQLステートメント ログ出力メッセージ
```

「YYYY-MM-DD HH:MM:SS.FFF GMT [プロセス ID] SQL ステートメント」の部分に、GMT タイムゾーンのタイムスタンプ、プロセス ID、SQL ステートメントを、プレフィックスとして出力します。

- ログファイルのサイズの見積もり

ログファイルのサイズに上限はありません。

通常の運用でのログの出力サイズの見積もり式を、次に示します。

通常の運用でのログの出力サイズ (1 週間分)

= 1 日分のログの出力サイズ × 7 (日)

1 日分のログの出力サイズ

= 1 サンプル当たりのログの出力サイズ^{※1} × 1 日のスクレイプ回数^{※2} × 1 回のスクレイプで各 Exporter から収集されるサンプル数^{※3}

注※1

トレンドデータの書き込みで出力されるログの出力サイズを示します。
JP1/IM - Agent の場合は、50 バイトを想定しています。

注※2

JP1/IM - Agent の場合は、Prometheus 設定ファイル (jpc_prometheus_server.yml) の scrape_interval で指定するスクレイプ間隔を元に算出します。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「Prometheus 設定ファイル (jpc_prometheus_server.yml)」(2. 定義ファイル) の scrape_interval について説明している個所を参照してください。
スクレイプ間隔の指定が 1m (1 分) の場合は、1440 回 (60 分×24 時間) となります。

注※3

監視エージェントがターゲットとする各 Exporter のメトリック定義ファイルで指定しているメトリック数の総和を示します。

JP1/IM - Agent がサポートする各 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」(2. 定義ファイル) の各 Exporter のメトリック定義ファイルについて説明している個所を参照してください。

なお、Linux の場合、次に示すようなスクリプト (一定期間のログを圧縮または削除する) ※を作成し、定期的 (1 回/日) に実行することで、ログファイルのディスク容量を削減できます。

注※ 「/etc/cron.daily」ディレクトリに配置します。

ログを 1 日単位で圧縮および 30 日単位で削除するシェルスクリプトの例

```
#!/usr/bin/bash
LOGDIR=/var/opt/jp1imm/database/imgndb/log
LOGSAVE=/var/opt/jp1imm/log/imgndb
COMPRESS_DAY=1
REMOVE_DAY=30
COMPRESS_CMD=gzip

COMPRESS_MTIME=`expr $COMPRESS_DAY - 1`
#Search for ".log" files whose modification date is "$COMPRESS_MTIME" or later
COMPRESS_FILE=`find $LOGDIR -name '*.log' -daystart -type f -mtime +$COMPRESS_MTIME`

#Add the date to the end of the file to be compressed and compress it.
if [ "$COMPRESS_FILE" != "" ]
then
  for i in $COMPRESS_FILE
  do
    if [ -f ${i} ]
    then
      mv ${i} ${i}.\`date +%Y%m%d`\`
      $COMPRESS_CMD ${i}.\`date +%Y%m%d`\`
    fi
  done
fi

#Search for ".gz" files
```

```

MV_FILE=`find $LOGDIR -name '*.gz'`

#Move compressed logfiles to "$LOGSAVE"
if [ "$MV_FILE" != "" ]
then
  for i in $MV_FILE
  do
    if [ -f ${i} ]
    then
      mv ${i} $LOGSAVE
    fi
  done
fi

REMOVEDTIME=`expr $REMOVE_DAY - 1`
#Search for ".gz" files whose modification date is "$REMOVEDTIME " or later
REMOVE_FILE=`find $LOGSAVE -name 'postgresl-*.gz' -daystart -type f -mtime +$REMOVEDTIME`

#Delete the file to be deleted
if [ "$REMOVE_FILE" != "" ]
then
  for i in $REMOVE_FILE
  do
    if [ -f ${i} ]
    then
      rm -f ${i}
    fi
  done
fi

```

上記のスクリプトを実行して運用する場合、監視対象数を 500 件としたときの、ログファイルのディスク容量の見積もりは、約 20GB※となります。

注※

次に示す各ログファイルのサイズの合計です。

- ・当日のログファイルのサイズ：約 4GB
- ・前日（圧縮前）のログファイルのサイズ：約 4GB
- ・圧縮後のログファイルのサイズ（400MB）×30 日分：約 12GB

インテリジェント統合管理データベースのログは、極めてサイズが大きいため、資料採取ツール※の採取対象外となります。「12.3.1(1)(b) JP1 の情報」および「12.3.1(2)(b) JP1 の情報」に記載しているケースに該当する場合は、手動で個別に採取する必要があります。

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」の「jim_log.bat (Windows 限定)」(1. コマンド) および「jim_log.sh (UNIX 限定)」(1. コマンド) を参照してください。

1.3.3 ダンプファイルの管理

JP1/IM, JP1/Base やユーザープログラムなどで問題が発生して異常終了した場合は、core ダンプ (UNIX の場合) などのダンプファイルが出力される場合があります。

これらのダンプファイルは容量が大きいことが多いため、トラブルが発生した場合は、必要なものを資料として採取してから、削除するようにしてください。

なお、Windows の場合は、プロセスがアプリケーションエラーになると、Windows エラー報告ダイアログボックスが表示されます。これらが表示されると入力待ちとなって再起動ができないため、画面表示によるエラーの通知を抑止する必要があります。

トラブル発生時の資料採取については、「[12. トラブルシューティング](#)」を参照してください。

1.4 履歴レポートの活用

JP1/IM は、運用中に発生した JP1 イベントの情報、JP1/IM の処理情報などの履歴を管理しています。履歴を活用して、JP1/IM のメンテナンスの検討材料としてください。

1.4.1 イベントの CSV 出力

JP1 イベントを CSV 出力する機能を、イベントレポート出力と呼びます。JP1 イベントを CSV 出力する方法には、次の三つがあります。

- イベント情報のスナップショットを CSV 出力する

スナップショットとは、特定のタイミングで情報を抽出することを意味します。JP1/IM - View に表示されるイベント情報のスナップショットは、運用に合わせてフィルタリングした JP1 イベントを出力できます。例えば、どのホストや製品で問題が発生しているのか、どのような対処をしているかなど、運用しているシステムの障害レポートとして利用できます。

[イベントコンソール] 画面に表示されているイベント一覧を CSV 出力する方法については、[「6.1 JP1 イベントの見方」](#)を参照してください。

- イベント DB の内容を CSV 出力する

JP1/Base が管理するイベント DB の内容を、`jevexport` コマンドを使用して CSV 出力します。マネージャーへ転送する必要のない JP1 イベント、例えば、JP1/AJS のジョブ正常終了などの JP1 イベントを運用の履歴や統計情報として利用したい場合は、エージェントのイベント DB の内容を `jevexport` コマンドを使用して CSV 出力できます。

`jevexport` コマンドについては、マニュアル「JP1/Base 運用ガイド」のコマンドに関する章を参照してください。

- 統合監視 DB の内容を CSV 出力する

統合監視 DB に登録されている JP1 イベントを、`jcoevtreport` コマンドを使用して CSV 出力します。統合監視 DB に登録されている JP1 イベント、例えば、先週発生した JP1 イベントの一覧を出力する場合、指定したイベントだけを出力する場合などに利用できます。

`jcoevtreport` 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「`jcoevtreport`」(1. コマンド)を参照してください。

1.4.2 関連イベントの発行履歴

関連イベント発行履歴ファイルには、関連イベント発行サービスの動作状況や関連イベントの発行処理の内容が出力されます。

関連イベント発行履歴ファイルを参照することで、定義した関連イベント発行条件どおりに関連イベントが発行されているかどうかを確認できます。例えば、特定の発行条件に対して、不成立の履歴が多く出力

されている場合、発行処理の対象としている JP1 イベントの組み合わせが適切でない、またはタイムアウト時間が短いおそれがあります。

定期的に発行条件を見直す際には、参考として関連イベント発行履歴ファイルを参照してください。

1.4.3 共通除外条件の除外履歴および定義履歴

共通除外条件に関する履歴情報は次のファイルに出力されます。

- 共通除外履歴ファイル

共通除外条件によって、取得対象外または自動アクションの実行対象外となった JP1 イベントの情報と、除外に使われた共通除外条件の情報が出力されます。さらに、共通除外条件定義の反映、変更の操作履歴が出力されます。除外に使われた共通除外条件定義の内容は、共通除外条件定義履歴ファイルで確認できます。

- 共通除外条件定義履歴ファイル

共通除外条件定義の反映、変更の操作履歴、および反映、変更後の共通除外条件定義の内容が出力されます。

共通除外履歴ファイルを参照することで、共通除外条件で意図したとおりに JP1 イベントが除外されているかどうかを確認できます。

例えば、イベントコンソールに JP1 イベントが表示されない、または自動アクションが実行されない場合は、共通除外条件によって意図せずに JP1 イベントが取得対象外または自動アクションの実行対象外になっている可能性があります。共通除外履歴ファイルを確認して、JP1 イベントが意図せず除外されていないか確認してください。

ファイルの詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.2.7(5) 共通除外履歴ファイルの内容」および「4.2.7(6) 共通除外条件定義履歴ファイルの内容」を参照してください。

1.5 設定情報および DB の移行

1.5.1 移行の対象となる設定情報および DB

次のうちどれかの設定が異なる別ホストに移行する場合、JP1/IM の設定情報を移行する必要があります。

- ホスト名
- IP アドレス
- PP バージョン
- 製品の使用するディレクトリの構成（権限なども含む）

この項では、JP1/IM の設定情報を移行する場合の対象について説明します。

(1) JP1/IM - Manager (インテリジェント統合管理基盤)

インテリジェント統合管理基盤を別ホストへ移行する場合、移行できるのは定義ファイルだけです。

移行先ホストで、インテリジェント統合管理基盤の定義ファイルを再定義する必要があります。

(2) JP1/IM - Manager (セントラルコンソール)

別ホストへ移行する場合、移行できる定義は「自動アクション定義ファイル」だけです。

その他の定義については、移行先ホストで再定義する必要があります。

(3) JP1/IM - Manager (セントラルスコープ)

jcsdbexport コマンド、jcsdbimport コマンドによって、監視オブジェクト DB の情報を移行できます。

その他の定義については、移行先ホストで再定義する必要があります。

なお、監視オブジェクト DB の情報を移行する際は、監視オブジェクトの状態変更条件および共通条件に設定している自ホストのホスト名および IP アドレスが合っているかを見直してください。

(4) JP1/IM - Manager (IM 構成管理)

jcfexport コマンド、jcfimport コマンドによって、IM 構成管理の管理情報を移行できます。

インポートした IM 構成管理の管理情報をシステムに反映するには、「[9.7.3 インポートした IM 構成管理の管理情報をシステムに反映する](#)」を参照してください。

なお、インポートした設定ファイルのプロファイル情報に、移行元のマネージャーホスト名を記載している場合は、プロファイルの設定を見直してください。

(5) JP1/IM - View

移行先ホストで JP1/IM - View の定義ファイルを再定義する必要があります。

(6) IM データベース

IM データベースの移行はできません。移行先ホストで IM データベースを再構築する必要があります。IM データベースの再構築については、「1.2.3(7) IM データベース再構築手順」を参照してください。

(7) イベント DB

イベント DB の移行はできません。移行先ホストでイベント DB を再構築する必要があります。イベント DB の構築については、マニュアル「JP1/Base 運用ガイド」を参照してください。

(8) インテリジェント統合管理データベース

インテリジェント統合管理データベースに格納されているトレンドデータおよび統合エージェントホストの情報だけを移行できます（移行対象となるのは、トレンドデータ管理 DB、統合エージェントホスト管理 DB です）。

移行元ホストでバックアップを取得し、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た移行先ホストでリストアを行う必要があります。移行手順について、次に示します。

1. JP1/IM - Manager を移行先ホストにインストールする。

2. 移行元のホスト上の定義ファイルをバックアップする。

次に示す定義ファイルをバックアップします。

- 物理ホストの場合

定義ファイル名	ファイルパス
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	<ul style="list-style-type: none">• Windows の場合 Manager パス¥imgndb¥setup¥jimgndbsetupinfo.conf• Linux の場合 /etc/opt/jp1imm/conf/imgndb/setup/jimgndbsetupinfo.conf
postgresql.conf	<ul style="list-style-type: none">• Windows の場合 Manager パス¥conf¥imgndb¥postgresql.conf• Linux の場合 /etc/opt/jp1imm/conf/imgndb/postgresql.conf

- 論理ホストの場合

定義ファイル名	ファイルパス
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	<ul style="list-style-type: none">• Windows の場合 Manager パス¥imgndb¥setup¥jimgndbclustersetupinfo.conf• Linux の場合

定義ファイル名	ファイルパス
	/etc/opt/jp1imm/conf/imgndb/setup/jimgndbclustersetupinfo.conf
postgresql.conf	<ul style="list-style-type: none"> Windows の場合 共有フォルダ¥jp1imm¥conf¥imgndb¥postgresql.conf Linux の場合 共有ディレクトリ/jp1imm/conf/imgndb/postgresql.conf

3. 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をバックアップする。

次に示す手順を実施します。

手順 1：JP1/IM - Manager のサービスを停止する。

停止方法については、「[3.2 JP1/IM - Manager を終了する](#)」を参照してください。

手順 2：インテリジェント統合管理データベースのサービスを停止する。

■Windows の場合

インテリジェント統合管理データベースサービス、および、トレンドデータ管理サービスを停止する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、トレンドデータ管理サービス、インテリジェント統合管理データベースサービスの順番で停止してください。

■Linux の場合

JP1/IM - Manager の停止に合わせて、インテリジェント統合管理データベース、および、トレンドデータ管理サービスも停止します。詳細については、「[3.2.2 UNIX の場合](#)」を参照してください。

手順 3：jimgndbbackup コマンド（引数-m に TRANSF を指定）を使用して、インテリジェント統合管理データベースのの移行用バックアップを行う。

jimgndbbackup コマンドの詳細や実行例については、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「jimgndbbackup」（1. コマンド）を参照してください。

手順 4：インテリジェント統合管理データベースのサービスを起動する。

■Windows の場合

インテリジェント統合管理データベースのサービスを起動する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、インテリジェント統合管理データベースサービス、トレンドデータ管理サービスを順番に起動してください（依存関係があるため、トレンドデータ管理サービスを起動すると、連動して、インテリジェント統合管理データベースサービスが自動で起動します）。

■Linux の場合

JP1/IM - Manager の起動に合わせて、インテリジェント統合管理データベース、および、トレンドデータ管理サービスも起動します。詳細については、「[3.1.2 UNIX の場合](#)」を参照してください。

手順 5：JP1/IM - Manager のサービスを起動する。

起動方法については、「[3.1 JP1/IM - Manager を起動する](#)」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移行を実施する。

インテリジェント統合管理基盤の移行については、「[1.5.1\(1\)JP1/IM - Manager \(インテリジェント統合管理基盤\)](#)」を参照してください。

5. 移行元からバックアップ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（論理ホストの場合は、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）を移行先ホストにコピーする。

6. 5.でコピー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（論理ホストの場合は、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）の内容に従い、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を実施する。

セットアップ手順の詳細については、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。

7. 移行元からバックアップした postgresql.conf ファイルからデフォルトから変更したパラメーターについて移行先の postgresql.conf ファイルに反映する。

8. 移行元でバックアップした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をリストアする。

次に示す手順を実施します。

手順 1：JP1/IM - Manager のサービスが停止していることを確認する。

停止状態でない場合の停止方法については、「[3.2 JP1/IM - Manager を終了する](#)」を参照してください。

手順 2：インテリジェント統合管理データベースのサービスが停止していることを確認する。

停止状態でない場合の停止方法について、次に示します。

■Windows の場合

インテリジェント統合管理データベースサービス、および、トレンドデータ管理サービスを停止する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、トレンドデータ管理サービス、インテリジェント統合管理データベースサービスの順番で停止してください。

■Linux の場合

JP1/IM - Manager の停止に合わせて、インテリジェント統合管理データベース、および、トレンドデータ管理サービスも停止します。詳細については、「[3.2.2 UNIX の場合](#)」を参照してください。

手順 3：jimgnbdbrestore コマンド（引数-m に TRANSF を指定）を使用して、インテリジェント統合管理データベースの移行用リストアを行う。

jimgnbdbrestore コマンドの詳細や実行例については、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「[jimgnbdbrestore](#)」（1. コマンド）を参照してください。

手順 4：インテリジェント統合管理データベースのサービスを起動する。

■Windows の場合

インテリジェント統合管理データベースのサービスを起動する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、インテリジェント統合管理データベースサービス、トレンドデータ管理サービスを順番に起動してください（依存関係があるため、トレンドデータ管理サービスを起動すると、連動して、インテリジェント統合管理データベースサービスが自動で起動します）。

■Linux の場合

JP1/IM - Manager の起動に合わせて、インテリジェント統合管理データベース、および、トレンドデータ管理サービスも起動します。詳細については、「[3.1.2 UNIX の場合](#)」を参照してください。

手順 5：JP1/IM - Manager のサービスを起動する。

起動方法については、「[3.1 JP1/IM - Manager を起動する](#)」を参照してください。

手順 6：jddupdatetree コマンドを新規・再構築モードで実行する。

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) を参照してください。

(9) 統合エージェントホストの JP1/IM - Agent の移行

(a) ホスト間のデータ移行

統合エージェントホストを同じホスト名のホストに移行できます。移行できる対象は、パフォーマンスデータ、JP1 イベントデータ、および定義情報です。

同じホスト名のホストに移行する場合は、「[1.1.2 JP1/IM - Agent のバックアップとリカバリー](#)」の手順と同じです。

異なるホスト名のホストに移行する場合は、「[1.1.2 JP1/IM - Agent のバックアップとリカバリー](#)」の手順で、同じホスト名のホストに移行したあと、「[2.2.1\(3\) エージェントのホスト名を変更した場合の作業](#)」の手順を実施します。

なお、異なるホスト名に変更すると、それまでに取得したパフォーマンスデータと JP1 イベントは参照できなくなりますので、注意してください。

(b) JP1 ユーザー間でのデータ参照について

JP1/IM - Agent で収集し、JP1/IM - Manager (インテリジェント統合管理基盤) に保存されているパフォーマンスデータは、そのパフォーマンスデータが紐付いている IM 管理ノードに対してアクセスできる JP1 ユーザーであれば、JP1/IM - Manager の統合オペレーション・ビューアーから誰でも参照できます。

JP1/IM - Agent では、JP1 ユーザーに依存するデータを保存することはないため、統合オペレーション・ビューアーにログインする JP1 ユーザー間でのデータの移行はありません。

(c) JP1/PFM の各製品からの移行について

JP1/IM - Agent は、JP1/PFM 製品とは異なるプロトコルによってパフォーマンスデータを収集します。そのため、JP1/PFM 製品からの移行手段はありません。

(10) 統合マネージャーホストの JP1/IM - Agent の移行

(a) ほかのホストへの移行

ほかのホストに移行する手順を次に示します。

1. 定義ファイルを移行する。

移行元ホストの定義ファイルの移行先にコピーします。

2. 「2.2.1(2)(i)JP1/IM - Agent で使用しているサーバ証明書に記載したホスト名」の「**■統合マネージャーホストのホスト名を変更する**」と「2.3.1(2)(d) JP1/IM - Agent で使用しているサーバ証明書に記載した IP アドレス」の「**■統合マネージャーホストの IP アドレスを変更する**」に従い、ホスト名と IP アドレスを変更する。

移行先ホスト固有の設定（ホスト名に関する設定など）を実施します。

3. マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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）」および「2.19.2(2)(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）」に従い、移行先のマネージャホストに変更する。

統合エージェントホスト側の接続情報（移行元ホストに接続していた情報）を移行先ホストの情報に更新します。

(b) クラスタシステムでのほかのホストへの移行

ほかのホストに移行する手順を次に示します。

移行元ホストの定義ファイルの移行先へのコピー、および、移行先ホスト固有の設定（ホスト名に関する設定など）を実施したあと、統合エージェントホスト側の接続情報（移行元ホストに接続していた情報）を移行先ホストの情報に更新します。

1. 定義ファイルを移行する。

移行元ホストの定義ファイルの移行先にコピーします。

2. 「2.2.1(2)(i)JP1/IM - Agent で使用しているサーバ証明書に記載したホスト名」の「**■クラスタシステムで統合マネージャーホストのホスト名を変更する**」と「2.3.1(2)(d) JP1/IM - Agent で使用しているサーバ証明書に記載した IP アドレス」の「**■クラスタシステムで統合マネージャーホストの IP アドレスを変更する**」に従い、ホスト名と IP アドレスを変更する。

移行先ホスト固有の設定（ホスト名に関する設定など）を実施します。

3. マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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）」および「2.19.2(2)(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）」に従い、移行先のマネージャホストに変更する。

統合エージェントホスト側の接続情報（移行元ホストに接続していた情報）を移行先ホストの情報に更新します。

1.6 通信暗号化機能の証明書の管理

通信暗号化機能を使用している場合は証明書および秘密鍵の管理が必要です。

JP1/IM の運用を安定して継続するためには、サーバ証明書の有効期限が有効期限外になる前に、サーバ証明書を更新する必要があります。

また、証明書と秘密鍵のアクセス権は正しく設定してください。

1.6.1 サーバ証明書の有効期限の管理

JP1/IM の通信暗号化機能は、マネージャーホストのサーバ証明書の有効期限が有効期限外の場合は、通信できないように設計されています。

JP1/IM の運用を安定して継続するためには、サーバ証明書の有効期限が有効期限外になる前に、サーバ証明書を更新する必要があります。

サーバ証明書を更新する手順は、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「9.4.2 設定済みの証明書を変更する」を参照してください。

サーバ証明書の有効期限は `openssl` コマンドで確認します。コマンドを実行すると、サーバ証明書の情報を表示します。情報を参考に、サーバ証明書を更新する時期を検討してください。

`openssl` のコマンドについては、OpenSSL の公式サイトを参照してください。

1.6.2 キーストアの管理

JP1/IM - Manager は通信暗号化機能が有効の場合に、起動時にキーストアの削除、および作成をし、停止時にキーストアの削除をします。通信暗号化機能が無効の場合は、起動時にキーストアの削除をします。

JP1/IM - Manager 用キーストアには次のファイルを格納します。

- 秘密鍵
- サーバ証明書
- 中間 CA 認証局証明書（使用する場合）

JP1/IM - Manager の起動時、または停止時にキーストアの削除ができなかった場合など、キーストアを手動で削除できます。不要なキーストアを手動で削除する場合は、次の手順に従って操作してください。

1. JP1/IM - Manager が停止していることを確認する。
2. 不要なキーストアを削除する。

キーストアの格納先については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「9.4.4(3) JP1/IM - Manager 用キーストア」を参照してください。

! **重要**

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。

2

JP1/IM システムの構成変更

この章では、JP1/IM システムの構成変更の際に必要な作業について説明します。

2.1 JP1/IM の設定情報の変更

JP1/IM で監視, 操作するホストを増加させる, JP1/IM の動作を変更して JP1/IM の業務 (システムの運用監視) の効率化を図るなど, JP1/IM の運用環境を変更する場合は, まず, どのような目的で変更するのかを明確にする必要があります。また, 運用環境の変更に伴い, 必要な設定作業が何かを洗い出す必要があります。

変更の目的と設定作業については, マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」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 構築ガイド」およびマニュアル「JP1/Base 運用ガイド」を参照してください。

2.1.1 統合エージェントホストの JP1/IM - Agent の設定変更

(1) IP バインド方式に変更する (オプション)

IP バインド方式に変更する場合は, 次の設定を変更します。

- 統合エージェント制御基盤の設定
- Prometheus server の設定
- Alertmanager の設定
- Node exporter の設定
- Windows exporter の設定
- Blackbox exporter の設定
- Yet another cloudwatch exporter の設定

設定の変更方法については, マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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)」および「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「IP バインド方式に変更する」の手順で, 物理ホストの設定を参照してください。

(2) コンテナシステムでの設定変更

設定変更が必要な場合は, Docker イメージや Podman イメージを作り直すことを推奨します。

コンテナを起動したあとで設定変更する場合, 次の注意事項があります。

- 定義ファイル操作機能を使用して更新や削除を行うことはできません。コンテナ環境に対して定義ファイル操作機能を使用して更新や削除を行うと KNBC00019-E エラーになります。
- コンテナ内のファイルを編集する場合は, コンテナを起動したあとで, 次に示すコマンドを実行してコンテナに接続する必要があります。

- Docker の場合

```
# docker exec -it コンテナ名 /bin/bash
```

- Podman の場合

```
# podman exec -it コンテナ名 /bin/bash
```

- ユニット定義ファイルを編集する手順は、コンテナでは、サービス管理プログラムの定義ファイルを編集します。例えば、supervisord の場合は、supervisord の定義ファイル (supervisord.conf) を編集します。

2.1.2 統合マネージャーホストの JP1/IM - Agent の設定変更

(1) 初期シークレットを更新する (オプション)

1. 統合オペレーション・ビューアーにログインする。

2. 初期シークレットの更新を実行する。

統合オペレーション・ビューアーの [オプション] メニューで [初期シークレットの発行] を選択し、[初期シークレットの表示] 画面を表示します。

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 オプションに関する画面」で、該当するメニューや画面の説明を参照してください。

3. 統合オペレーション・ビューアーに表示された新しい初期シークレットを入手する。

今後、統合エージェントを構築するときは、新しい初期シークレットを指定する必要があります。

2.2 ホスト名を変更する場合に必要な作業

マネージャーまたはエージェントのホスト名を変更した場合に必要な作業と、システム構成の再配布手順を説明します。JP1/IM - Manager は JP1/Base を前提としているため、マニュアル「JP1/Base 運用ガイド」の JP1/Base 運用中の設定変更の章を参照して、JP1/Base のホスト名の変更に必要な作業を行ってください。

また、メールサーバのホスト名やクラスタシステムで論理ホスト名を変更した場合、作業が必要になることもあります。ここで説明する内容を基に作業してください。

作業を開始する前にホスト名を変更するマネージャーまたはエージェントの JP1/Base を停止してください。

2.2.1 エージェントとして JP1/IM - Agent を使用している場合

(1) マネージャーのホスト名を変更した直後に必要な作業

マネージャーのホスト名を変更した直後に必要な作業について説明します。

(a) JP1/Base で必要な作業

ホスト名を変更したマネージャーの JP1/Base において、認証サーバのホスト名を変更してください。手順などの詳細については、マニュアル「JP1/Base 運用ガイド」の JP1/Base 運用中の設定変更の章、ホスト名の変更による影響および必要な作業の説明を参照してください。

その後、ホスト名を変更したマネージャーの JP1/Base をいったん終了してから、再起動する必要があります。

(b) IM データベースで必要な作業

マネージャーのホスト名を変更した場合、「1.2.3(7) IM データベース再構築手順」を参照して、IM データベースを再構築してください。

(2) マネージャーのホスト名を変更した場合の作業

(a) フィルター条件で設定したホスト名

[重要イベント定義] 画面、[表示フィルター設定] 画面、または [ユーザーフィルター詳細設定] 画面で定義してある登録ホスト名が変更対象であった場合は、それぞれの設定画面で登録ホスト名の設定を変更する必要があります。

(b) [アクション設定] 画面または自動アクション定義ファイルで設定したホスト名

[アクション設定] 画面または自動アクション定義ファイルで定義してある実行ホスト名が変更対象であった場合は、[アクション設定] 画面または自動アクション定義ファイルで実行ホスト名の設定を変更する必要があります。

ホスト名を設定したあとに次のどちらかの作業をします。

- JP1/IM - Manager の起動時、JP1/IM - View の [アクション設定] 画面の [適用] ボタンをクリックして定義を有効にする。
- jcachange コマンドを実行して定義を再読み込みする。

(c) 監視オブジェクトの状態変更条件で設定したホスト名

[状態変更条件設定] 画面または [共通条件詳細設定] 画面で設定したホスト名が変更対象であった場合は、それぞれの設定画面でホスト名の設定を変更する必要があります。

ホスト名を設定してからシステム構成の再配布を実施します。詳細については、「2.2.2(3) マネージャーまたは JP1/Base のホスト名を変更した場合のシステム構成の再配布手順」を参照してください。

(d) 関連イベント発行定義ファイルで設定したホスト名

関連イベント発行定義ファイルで、関連イベントの発行条件として定義してあるホスト名が変更対象であった場合は、関連イベント発行定義ファイルでホスト名の設定を変更する必要があります。

関連イベント発行定義ファイルでホスト名を設定してから、jcoegschange コマンドで関連イベント発行定義を有効にします。

(e) 重大度変更定義ファイルで設定したホスト名

重大度変更定義ファイルで、重大度変更条件として定義してあるホスト名が変更対象であった場合は、重大度変更定義ファイルでホスト名の設定を変更する必要があります。

イベントの重大度変更機能が有効な場合に、次のどれかの操作を実施してホスト名の変更を有効にします。

- jco_spmd_reload コマンドを実行する。
- JP1/IM - Manager を起動する。
- [追加重大度変更定義設定] 画面で [OK] ボタンをクリックする。
- [重大度変更定義一覧] 画面で [適用] ボタンをクリックする。

(f) 表示メッセージ変更定義ファイルで設定したホスト名

表示メッセージ変更定義ファイルで、表示メッセージ変更条件として定義してあるホスト名が変更対象であった場合は、表示メッセージ変更定義ファイルでホスト名の設定を変更する必要があります。

イベントの表示メッセージ変更機能が有効な場合に、次のどれかの操作を実施してホスト名の変更を有効にします。

- jco_spmd_reload コマンドを実行する。
- JP1/IM - Manager を起動する。
- [追加表示メッセージ変更定義設定] 画面で [OK] ボタンをクリックする。
- [表示メッセージ変更定義一覧] 画面で [適用] ボタンをクリックする。

(g) サーバ証明書の CN および SAN に記載したホスト名

通信暗号化機能が有効の場合に、サーバ証明書の CN および SAN に記載したホスト名が変更対象のときは、サーバ証明書を作成し直す必要があります。

サーバ証明書を作成し直す手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「9.4.2 設定済みの証明書を変更する」を参照してください。

(h) インテリジェント統合管理基盤が稼働するホストのホスト名

インテリジェント統合管理基盤が稼働するホストのホスト名を変更した場合は、JP1/IM - Manager の再起動が必要です。JP1/IM - Manager の起動手順については「3.1 JP1/IM - Manager を起動する」を参照してください。

また、通信暗号化機能が有効の場合に、サーバ証明書の CN および SAN に記載したホスト名が変更対象のときは、サーバ証明書を作成し直す必要があります。サーバ証明書を作成し直す手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「9.4.2 設定済みの証明書を変更する」を参照してください。

IM 管理ノードのホストのホスト名を変更する場合は、IM 管理ノードを再取得する必要があります。IM 管理ノードを再取得する手順については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.5.6 IM 管理ノードの変更」を参照してください。

(i) JP1/IM - Agent で使用しているサーバ証明書に記載したホスト名

■ 統合マネージャーホストのホスト名を変更する

1. JP1/IM - Manager を停止する。
2. ホスト名の変更を反映したサーバ証明書で更新する。
証明書の更新については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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「■証明書を設定する」を参照してください。
なお、証明書に変更前のホスト名を含んでいない場合は、この手順は不要です。
3. JP1/IM - Manager を起動する。

■ クラスタシステムで統合マネージャーホストのホスト名を変更する

1. 統合エージェント管理基盤を停止する。

2. 論理ホスト名の変更を反映したサーバ証明書で更新する。

証明書の更新については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「7.3.3(9)(a) 統合エージェント管理基盤の設定変更」および「8.3.3(9)(a) 統合エージェント管理基盤の設定変更」の「■証明書を設定する」を参照してください。

なお、証明書に変更前のホスト名を含んでいない場合は、この手順は不要です。

3. 統合エージェント管理基盤を起動する。

(3) エージェントのホスト名を変更した場合の作業

(a) エージェントのホスト名

1. 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. JP1/IM - Agent のすべての定義ファイルについて、旧ホスト名が記載されている個所を新ホスト名に変更する。

JP1/IM - Agent の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」(2. 定義ファイル) を参照してください。

4. JP1/IM - Agent のサービスを起動する。

5. IM 管理ノードのツリー情報を反映する。

マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.2(16) IM 管理ノードのツリー情報の作成と反映 (Windows の場合) (必須)」および「2.19.2(17) 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。

❗ 重要

定義ファイルを変更する作業について、次の注意事項があります。

一部の定義ファイルを編集せずに JP1/IM - Agent のサービスを起動、または、ホスト名を過去に使用されたホスト名 (トレンドデータ管理 DB にトレンドデータが残っているホスト名) に変更した場合、1 つのツリー SID に対して、複数の構成情報の SID がマッピングされます。その場合、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する必要があります。IM 管理ノードツリーファイルの編集については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

IM 管理ノードツリーファイルを編集せずにツリー情報を反映した場合、統合オペレーション・ビューアーの [トレンド] タブで、トレンドデータの表示に失敗する場合があります。

(b) Blackbox exporter の監視対象のホスト名

Blackbox exporter の監視対象の変更を実施します。

マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.2(6)(c) 監視対象を追加・変更・削除する (Windows の場合) (必須)」および「2.19.2(7)(c) 監視対象を追加・変更・削除する (Linux の場合) (必須)」を参照してください。

(c) インテリジェント統合管理基盤が稼働するホストのホスト名

インテリジェント統合管理基盤が稼働するホストのホスト名を変更した場合は、JP1/IM - Manager の再起動が必要です。JP1/IM - Manager の起動手順については「[3.1 JP1/IM - Manager を起動する](#)」を参照してください。

また、通信暗号化機能が有効の場合に、サーバ証明書の CN および SAN に記載したホスト名が変更対象のときは、サーバ証明書を作成し直す必要があります。サーバ証明書を作成し直す手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「9.4.2 設定済みの証明書を変更する」を参照してください。

IM 管理ノードのホストのホスト名を変更する場合は、IM 管理ノードを再取得する必要があります。IM 管理ノードを再取得する手順については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.5.6 IM 管理ノードの変更」を参照してください。

(d) クラスタシステムの論理ホスト名

■ Windows 環境の場合

1. 論理ホスト用の JP1/IM - Agent のサービスを停止する。

クラスタソフトからサービスを停止します

2. 論理ホストのサービスを Windows から解除する。

論理ホストで使用するサービスについて、実行系サーバと待機系サーバの両方で論理ホスト用のサービスを Windows から解除します。

次のコマンドを実行して、論理ホストのサービスを解除します。

```
Agentパス¥tools¥jpc_service -off サービスキー -h 論理ホスト名
```

Alertmanager のサービスを解除する場合の例を、次に示します。

```
Agentパス¥tools¥jpc_service -off jpc_alertmanager -h 論理ホスト名
```

3. 定義ファイルに記載されている論理ホスト名を更新する。

共有フォルダ¥jplima¥conf と Agent パス¥bin に存在するファイルに対して、変更前の論理ホスト名で検索し、該当する箇所をすべて新しい論理ホスト名に変更します。

Agent パス¥bin は、実行系サーバと待機系サーバの両方に存在するため、両方で実施します。

4. ファイル名に含まれている論理ホスト名を更新する。

Agent パス¥bin に存在するファイルに論理ホスト名が含まれているファイルがあるため、新しい論理ホスト名に変更します。

Agent パス¥bin は、実行系サーバと待機系サーバの両方に存在するため、両方で実施します。

5. 論理ホストのサービスを Windows に登録する。

論理ホストで使用するサービスについて、実行系サーバと待機系サーバの両方で論理ホスト用のサービスを Windows に登録します。

次のコマンドを実行して、論理ホストのサービスを登録します。

```
Agentパス¥tools¥jpc_service -on 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 -on jpc_alertmanager -h 論理ホスト名
```

6. 論理ホスト用の JP1/IM - Agent のサービスをすべて起動する。

クラスタソフトからサービスを起動します。

7. IM 管理ノードのツリー情報を反映する。

マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.2(16) IM 管理ノードのツリー情報の作成と反映（Windows の場合）（必須）」および「2.19.2(17) 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。

■ Linux 環境の場合

1. 論理ホスト用の JP1/IM - Agent のサービスを停止する。

クラスタソフトからサービスを停止します。

2. 論理ホストのサービスを systemd から解除する。

論理ホストで使用するサービスについて、実行系と待機系の両方で論理ホスト用のサービスを systemd から解除します。

次のコマンドを実行して、論理ホストのサービスを解除します。

```
/opt/jp1ima/tools/jpc_service -off サービスキー -h 論理ホスト名
```

Alertmanager のサービスを解除する場合の例を、次に示します。

```
/opt/jp1ima/tools/jpc_service -off jpc_alertmanager -h 論理ホスト名
```

3. 定義ファイルに記載されている論理ホスト名を更新する。

共有ディレクトリ/jp1ima/conf と /usr/lib/systemd/system に存在するファイルに対して、変更前の論理ホスト名で検索し、該当する箇所をすべて新しい論理ホスト名に変更します。

/usr/lib/systemd/system は、実行系サーバと待機系サーバの両方に存在するため、両方で実施します。

4. ファイル名に含まれている論理ホスト名を更新する。

/usr/lib/systemd/system に存在するファイルに論理ホスト名が含まれているファイルがあるため、新しい論理ホスト名に変更します。

/usr/lib/systemd/system は、実行系サーバと待機系サーバの両方に存在するため、両方で実施します。

5. 論理ホストのサービスを systemd に登録する。

論理ホストで使用するサービスについて、実行系と待機系の両方で論理ホスト用のサービスを systemd に登録します。

次のコマンドを実行して、論理ホストのサービスを登録します。

```
/opt/jp1ima/tools/jpc_service -on サービスキー -h 論理ホスト名
```

Alertmanager のサービスを登録する場合の例を、次に示します。

```
/opt/jp1ima/tools/jpc_service -on jpc_alertmanager -h 論理ホスト名
```

6. 論理ホスト用の JP1/IM - Agent のサービスをすべて起動する。

クラスタソフトからサービスを起動します。

7. IM 管理ノードのツリー情報を反映する。

マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.2(16) IM 管理ノードのツリー情報の作成と反映 (Windows の場合) (必須)」および「2.19.2(17) 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。

(e) コンテナのホスト名

コンテナのホスト名は変更できません。そのため、新しいコンテナを作成し、不要になったコンテナを削除してください。

コンテナの作成方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「2.20.1(3) Docker コンテナ, Podman コンテナの作成方法」、コンテナの削除方法については、「2.20.1(4) Docker コンテナ, Podman コンテナの削除方法」を参照してください。

2.2.2 エージェントとして JP1/Base を使用している場合

(1) マネージャーまたは JP1/Base のホスト名を変更した直後に必要な作業

マネージャーまたは JP1/Base のホスト名を変更した直後に必要な作業について説明します。

(a) JP1/Base で必要な作業

ホスト名を変更したマネージャーの JP1/Base において、認証サーバのホスト名を変更してください。手順などの詳細については、マニュアル「JP1/Base 運用ガイド」の JP1/Base 運用中の設定変更の章、ホスト名の変更による影響および必要な作業の説明を参照してください。

その後、ホスト名を変更したマネージャーまたはエージェントの JP1/Base をいったん終了してから、再起動する必要があります。

(b) IM データベースで必要な作業

マネージャーのホスト名を変更した場合、「1.2.3(7) IM データベース再構築手順」を参照して、IM データベースを再構築してください。

(2) マネージャーまたは JP1/Base のホスト名を変更した場合の作業

(a) フィルター条件で設定したホスト名

[重要イベント定義] 画面、[表示フィルター設定] 画面、または [ユーザーフィルター詳細設定] 画面で定義してある登録ホスト名が変更対象であった場合は、それぞれの設定画面で登録ホスト名の設定を変更する必要があります。

(b) [アクション設定] 画面または自動アクション定義ファイルで設定したホスト名

[アクション設定] 画面または自動アクション定義ファイルで定義してある実行ホスト名が変更対象であった場合は、[アクション設定] 画面または自動アクション定義ファイルで実行ホスト名の設定を変更する必要があります。

ホスト名を設定したあとに次のどちらかの作業をします。

- JP1/IM - Manager の起動時、JP1/IM - View の [アクション設定] 画面の [適用] ボタンをクリックして定義を有効にする。
- jchange コマンドを実行して定義を再読み込みする。

(c) 監視オブジェクトの状態変更条件で設定したホスト名

[状態変更条件設定] 画面または [共通条件詳細設定] 画面で設定したホスト名が変更対象であった場合は、それぞれの設定画面でホスト名の設定を変更する必要があります。

ホスト名を設定してからシステム構成の再配布を実施します。詳細については、「2.2.2(3) マネージャーまたは JP1/Base のホスト名を変更した場合のシステム構成の再配布手順」を参照してください。

(d) 関連イベント発行定義ファイルで設定したホスト名

関連イベント発行定義ファイルで、関連イベントの発行条件として定義してあるホスト名が変更対象であった場合は、関連イベント発行定義ファイルでホスト名の設定を変更する必要があります。

相関イベント発行定義ファイルでホスト名を設定してから、jcoegschange コマンドで相関イベント発行定義を有効にします。

(e) 重大度変更定義ファイルで設定したホスト名

重大度変更定義ファイルで、重大度変更条件として定義してあるホスト名が変更対象であった場合は、重大度変更定義ファイルでホスト名の設定を変更する必要があります。

イベントの重大度変更機能が有効な場合に、次のどれかの操作を実施してホスト名の変更を有効にします。

- jco_spmd_reload コマンドを実行する。
- JP1/IM - Manager を起動する。
- [追加重大度変更定義設定] 画面で [OK] ボタンをクリックする。
- [重大度変更定義一覧] 画面で [適用] ボタンをクリックする。

(f) 表示メッセージ変更定義ファイルで設定したホスト名

表示メッセージ変更定義ファイルで、表示メッセージ変更条件として定義してあるホスト名が変更対象であった場合は、表示メッセージ変更定義ファイルでホスト名の設定を変更する必要があります。

イベントの表示メッセージ変更機能が有効な場合に、次のどれかの操作を実施してホスト名の変更を有効にします。

- jco_spmd_reload コマンドを実行する。
- JP1/IM - Manager を起動する。
- [追加表示メッセージ変更定義設定] 画面で [OK] ボタンをクリックする。
- [表示メッセージ変更定義一覧] 画面で [適用] ボタンをクリックする。

(g) サーバ証明書の CN および SAN に記載したホスト名

通信暗号化機能が有効の場合に、サーバ証明書の CN および SAN に記載したホスト名が変更対象のときは、サーバ証明書を作成し直す必要があります。

サーバ証明書を作成し直す手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「9.4.2 設定済みの証明書を変更する」を参照してください。

(h) インテリジェント統合管理基盤が稼働するホストのホスト名

インテリジェント統合管理基盤が稼働するホストのホスト名を変更した場合は、JP1/IM - Manager の再起動が必要です。JP1/IM - Manager の起動手順については「[3.1 JP1/IM - Manager を起動する](#)」を参照してください。

また、通信暗号化機能が有効の場合に、サーバ証明書の CN および SAN に記載したホスト名が変更対象のときは、サーバ証明書を作成し直す必要があります。サーバ証明書を作成し直す手順については、マニユ

アル「JP1/Integrated Management 3 - Manager 構築ガイド」の「9.4.2 設定済みの証明書を変更する」を参照してください。

IM 管理ノードのホストのホスト名を変更する場合は、IM 管理ノードを再取得する必要があります。IM 管理ノードを再取得する手順については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.5.6 IM 管理ノードの変更」を参照してください。

(3) マネージャーまたは JP1/Base のホスト名を変更した場合のシステム構成の再配布手順

マネージャーまたは JP1/Base のホスト名を変更した場合、システム構成の再配布が必要になります。手順を次に示します。

1. JP1/IM - Manager に接続しているすべての JP1/IM - View を終了する。
2. JP1/IM - Manager を終了する。
3. jbsrt_distrib コマンドを実行し、システム構成の再配布をする。
4. JP1/IM - Manager を起動する。
5. JP1/IM - Manager に接続しているすべての JP1/IM - View を起動する。

システム構成の配布方法の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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)」、 「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)」または「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。

2.2.3 メールサーバのホスト名を変更した場合の作業

(1) メール環境定義ファイルで設定したホスト名

メール環境定義ファイルで、SMTP サーバおよび POP3 サーバとして定義してあるホスト名が変更対象であった場合は、メール環境定義ファイルでホスト名の設定を変更する必要があります。

メール環境定義ファイルでホスト名の設定を変更してから、jimmail コマンドを実行したときにホスト名は有効になります。

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

クラスタシステムを運用している環境で論理ホスト名を変更する場合は、変更前の論理ホスト環境を削除してください。そのあと、新たに論理ホストを再セットアップしてクラスタ運用ができるように設定してください。

Windows の場合

論理ホストの削除方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「7.7.1 論理ホストの削除 (Windows の場合)」を参照してください。セットアップ方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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)」, または「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)」を参照してください。

UNIX の場合

論理ホストの削除方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「8.7.1 論理ホストの削除 (UNIX の場合)」を参照してください。セットアップ方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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)」, または「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)」を参照してください。

❗ 重要

クラスタシステムの場合、旧ホスト名のときに発行された JP1 イベントについては、ホスト名が変更されたあとは、次のように処理されます。

- JP1/IM - View の「登録ホスト名」には、旧ホスト名が表示されます。
- イベント検索をする場合は、旧ホスト名でマッチされます。
- [イベント詳細] 画面を表示したときに、「指定した JP1 イベントが見つからない」などのエラーが発生することがあります。
- 旧ホスト名のときに発行された JP1 イベントからは、JP1/AJS - View のモニター表示はできません。
- [アクション結果] 画面, [アクション結果詳細] 画面, [アクション結果一覧] 画面の「ホスト名」には、旧ホスト名が表示されます。

2.3 IP アドレスを変更する場合に必要な作業

マネージャーまたはエージェントの IP アドレスを変更した場合に必要な作業と、システム構成の再配布手順を説明します。

また、メールサーバの IP アドレスを変更した場合、作業が必要になることもあります。ここで説明する内容を基に作業してください。

作業を開始する前にホスト名を変更するマネージャーまたはエージェントの JP1/Base を停止してください。

2.3.1 エージェントとして JP1/IM - Agent を使用している場合

(1) マネージャーの IP アドレスを変更した直後に必要な作業

マネージャーの IP アドレスを変更した直後に必要な作業について説明します。

(a) JP1/Base で必要な作業

IP アドレスを変更したマネージャーの JP1/Base をいったん終了してから、再起動する必要があります。

(b) IM データベースで必要な作業

マネージャーの IP アドレスを変更した場合、IM データベースをいったん終了してから、再起動する必要があります。

(2) マネージャーの IP アドレスを変更した場合の作業

(a) 監視オブジェクトの状態変更条件で設定した IP アドレス

[状態変更条件設定] 画面または [共通条件詳細設定] 画面で設定した IP アドレスが変更対象であった場合、それぞれの設定画面で IP アドレスの設定を変更する必要があります。

IP アドレスを設定してからシステムを再起動します。詳細については、「[2.3.2\(3\) マネージャーまたは JP1/Base の IP アドレスを変更した場合のシステムの再起動手順](#)」を参照してください。

(b) IM 構成管理を使用している場合

IM 構成管理機能を使用している場合、IM 構成管理・ビューアーを起動し、ホスト情報を収集してください。

(c) インテリジェント統合管理基盤が稼働するホストの IP アドレス

インテリジェント統合管理基盤が稼働するホストの IP アドレスを変更した場合は、JP1/IM - Manager の再起動が必要です。また、ユーザーによってカスタマイズされたプラグインを使用している場合は、プラグインの仕様に従って対処します。JP1/IM - Manager の起動手順については「[3.1 JP1/IM - Manager を起動する](#)」を参照してください。

なお、IM 管理ノードのホストの IP アドレスを変更した場合は、必要な作業はありません。

(d) JP1/IM - Agent で使用しているサーバ証明書に記載した IP アドレス

■ 統合マネージャーホストの IP アドレスを変更する

1. JP1/IM - Manager を停止する。

2. IP アドレスの変更を反映したサーバ証明書で更新する。

証明書の更新については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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「■証明書を設定する」を参照してください。

なお、証明書に変更前の IP アドレスを含んでいない場合は、この手順は不要です。

3. JP1/IM - Manager を起動する。

■ クラスタシステムで統合マネージャーホストの IP アドレスを変更する

1. 統合エージェント管理基盤を停止する。

2. 論理 IP アドレスの変更を反映したサーバ証明書で更新する。

証明書の更新については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「7.3.3(9)(a) 統合エージェント管理基盤の設定変更」および「8.3.3(9)(a) 統合エージェント管理基盤の設定変更」の「■証明書を設定する」を参照してください。

なお、証明書に変更前の IP アドレスを含んでいない場合は、この手順は不要です。

3. 統合エージェント管理基盤を起動する。

(3) エージェントの IP アドレスを変更した場合の作業

(a) エージェントの IP アドレス

次に示す条件に該当しない場合、設定変更は不要です。該当する場合、エージェントの IP アドレスの変更の影響を受けるため、設定変更が必要です。

- リッスンアドレスを IP アドレスで設定している場合

JP1/IM - Agent プロセスのリッスンアドレスを IP アドレスで指定している場合に影響があります。

各プロセスのポートの変更手順を確認し、リッスンアドレスを設定している場合は設定しなおしてください。

- 証明書に IP アドレス情報が含まれる場合

変更後の IP アドレスに、変更した証明書を配置しなおす必要があります。

(b) Blackbox exporter の監視対象の IP アドレス

Blackbox exporter の監視対象はホスト名で指定します。

IP アドレスを変更したとしても、エージェントの設定変更は不要です。

(c) インテリジェント統合管理基盤が稼働するホストの IP アドレス

インテリジェント統合管理基盤が稼働するホストの IP アドレスを変更した場合は、JP1/IM - Manager の再起動が必要です。また、ユーザーによってカスタマイズされたプラグインを使用している場合は、プラグインの仕様に従って対処します。JP1/IM - Manager の起動手順については「[3.1 JP1/IM - Manager を起動する](#)」を参照してください。

なお、IM 管理ノードのホストの IP アドレスを変更した場合は、必要な作業はありません。

(d) クラスタシステムの IP アドレス

「[2.3.1\(3\)\(a\) エージェントの IP アドレス](#)」と同じです。

ただし、次のことに注意してください。

- 統合エージェントのサービスを起動または停止するときは、クラスタソフトから行ってください。
- 変更作業は、実行系サーバと待機系サーバの両方で実施してください。
- IP アドレスを変更したあとに、統合エージェントのサービスの再起動が必要です。

(e) コンテナの IP アドレス

設定変更は不要です。

2.3.2 エージェントとして JP1/Base を使用している場合

(1) マネージャーまたは JP1/Base の IP アドレスを変更した直後に必要な作業

マネージャーまたは JP1/Base の IP アドレスを変更した直後に必要な作業について説明します。

(a) JP1/Base で必要な作業

IP アドレスを変更したマネージャーまたはエージェントの JP1/Base をいったん終了してから、再起動する必要があります。

(b) IM データベースで必要な作業

マネージャーの IP アドレスを変更した場合、IM データベースをいったん終了してから、再起動する必要があります。

(2) マネージャーまたは JP1/Base の IP アドレスを変更した場合の作業

(a) 監視オブジェクトの状態変更条件で設定した IP アドレス

[状態変更条件設定] 画面または [共通条件詳細設定] 画面で設定した IP アドレスが変更対象であった場合、それぞれの設定画面で IP アドレスの設定を変更する必要があります。

IP アドレスを設定してからシステムを再起動します。詳細については、「[2.3.2\(3\) マネージャーまたは JP1/Base の IP アドレスを変更した場合のシステムの再起動手順](#)」を参照してください。

(b) IM 構成管理を使用している場合

IM 構成管理機能を使用している場合、IM 構成管理・ビューアーを起動し、ホスト情報を収集してください。

(c) インテリジェント統合管理基盤が稼働するホストの IP アドレス

インテリジェント統合管理基盤が稼働するホストの IP アドレスを変更した場合は、JP1/IM - Manager の再起動が必要です。また、ユーザーによってカスタマイズされたプラグインを使用している場合は、プラグインの仕様に従って対処します。JP1/IM - Manager の起動手順については「[3.1 JP1/IM - Manager を起動する](#)」を参照してください。

なお、IM 管理ノードのホストの IP アドレスを変更した場合は、必要な作業はありません。

(3) マネージャーまたは JP1/Base の IP アドレスを変更した場合のシステムの再起動手順

マネージャーまたは JP1/Base の IP アドレスを変更した場合、JP1/IM - Manager および JP1/IM - View の再起動が必要になります。手順を次に示します。

1. JP1/IM - Manager に接続しているすべての JP1/IM - View を終了する。
2. JP1/IM - Manager を終了する。
3. JP1/IM - Manager を起動する。
4. JP1/IM - View を起動する。

2.3.3 メールサーバの IP アドレスを変更した場合の作業

(1) メール環境定義ファイルで設定した IP アドレス

メール環境定義ファイルで、SMTP サーバおよび POP3 サーバとして定義してある IP アドレスが変更対象であった場合は、メール環境定義ファイルで IP アドレスの設定を変更する必要があります。

メール環境定義ファイルで IP アドレスの設定を変更してから、jimmail コマンドを実行したときに IP アドレスは有効になります。

2.4 マネージャーおよびエージェントの日時を変更した場合に必要な作業

JP1/IM の運用中にマネージャーおよびエージェントの日時を変更する場合の注意事項および手順について説明します。リモート監視構成の監視対象ホストの日時を変更した場合は、「2.6 リモート監視構成の監視対象ホストの日時を変更した場合に必要な作業」を参照してください。

❗ 重要

通信暗号化機能を使用している場合、変更後の日時が使用中の証明書の有効期限内であることを確認してください。変更後の日時が使用中の証明書の有効期限外となる場合は、変更後の日時が有効期限内となる証明書を配置してください。

2.4.1 マネージャーおよびエージェントの日時を過去に戻す

マネージャーおよびエージェントの日時を変更する際、過去の日時に変更することは通常避けてください。JP1/IM が動作するホストの OS のシステム時刻を戻す場合は、データベースに大きな影響があり、JP1/IM の再インストールまたはデータベースの再セットアップを伴う作業が必要になります。

システム時刻の進みや遅れを補正する場合でも、システム時刻を過去に戻すと自動アクションの実行結果の表示順序や監視ツリーの状態更新日時などの表示が不正になることがあります。このような現象は、システム時刻を過去に戻したことで、JP1/IM - Manager, JP1/Base, JP1/IM - Agent の管理データに不整合が生じたときに発生します。JP1/IM - View には影響ありません。

また、システム時刻を過去に戻すと、到着時刻を指定してイベント検索したときに、正しくイベント検索ができないことがあります。

テストなどでシステム時刻を意図的に未来の日時へ変更したような場合に、システム時刻を元に戻すときは、次に示す手順で戻してください。

❗ 重要

サーバのシステム時刻を、NTP (Network Time Protocol) サーバなどを利用した時刻が過去に戻ることがない方式で合わせる場合には、次の手順に従わないで変更できます。その場合、JP1/Base を停止する必要はありません。

(1) マネージャーの日時を元に戻す

1. JP1/IM - Manager を終了する。
2. IM データベースを使用している場合は、IM データベースを終了する。
3. JP1/Base を終了する。

4. システム時刻を戻す。

5. システム時刻が時刻を戻す前の時刻に達したら JP1/Base, および JP1/IM - Manager を起動する。

例えば, 手順 4 で時刻を「02:00」から「01:00」に戻した場合, システム時刻が「02:00」になってから, JP1/Base および JP1/IM - Manager を起動します。

なお, IM データベースを使用している場合は, JP1/Base, IM データベース, JP1/IM - Manager の順で起動 Manager パス¥data¥imdd¥actevent.ser してください。

重要

システム時刻が, 時刻を戻す前の時刻に達する前 (手順 5 で「02:00」より前) にサービスを起動してしまった場合, 統合監視 DB が壊れるおそれがあります。統合監視 DB が壊れた場合はシステムを再構築する必要があります。

時刻を戻す前に設定情報, データベースをバックアップしておき, システム再構築後に, 設定情報, データベースをリカバリーしてください。

なお, リカバリーできるファイルは, リカバリー時点のシステム時刻より前のシステム時刻でバックアップしたファイルです。バックアップのシステム時刻がリカバリー時点のシステム時刻より前でない場合は, システム時刻がバックアップ時刻を過ぎてからリカバリーしてください。

また, 次の方法でも日時を元に戻せます。ただし, この方法では, アクション情報ファイルやアクションホスト名格納ファイルなどの手順 5 に示す情報, および IM データベースのイベント情報やホスト情報を削除するため注意してください。

1. JP1/IM - Manager を終了する。

2. JP1/Base を終了する。

3. IM データベースを使用している場合は, IM データベースをアンセットアップする。

Windows の場合は, 「JP1/IM3-Manager DB Server」サービスを起動しておく必要があります。

統合監視 DB および IM 構成管理 DB をセットアップしている場合には, 両方のアンセットアップが必要です。

4. システムの時刻を戻す。

5. アクション情報ファイル, アクションホスト名格納ファイル, コマンド実行履歴ファイル, イベント DB を削除する。

削除ファイルの格納場所は次の表のとおりです。

Windows の場合

表 2-1 削除対象ファイル (Windows)

ファイル名	格納場所
アクション情報ファイル	Console パス¥log¥action¥actinf.log
	共有フォルダ¥jp1cons¥log¥action¥actinf.log
アクションホスト名格納ファイル	Console パス¥log¥action¥acttxt{1 2}.log
	共有フォルダ¥jp1cons¥log¥action¥acttxt{1 2}.log
コマンド実行履歴ファイル	Base パス¥log¥COMMAND¥以下の全ファイル
	共有フォルダ¥jp1base¥log¥COMMAND¥以下の全ファイル
イベント DB	Base パス¥sys¥event¥servers¥default¥以下のIMEvent*. *ファイル※
	共有フォルダ¥jp1base¥event¥以下のIMEvent*. *ファイル※

注※ イベントサービインデックス (index) ファイルで別パスを指定した場合は、指定したパス以下のファイルが対象となります。

UNIX の場合

表 2-2 削除対象ファイル (UNIX)

ファイル名	格納場所
アクション情報ファイル	/var/opt/jp1cons/log/action/actinf.log
	共有ディレクトリ/jp1cons/log/action/actinf.log
アクションホスト名格納ファイル	/var/opt/jp1cons/log/action/acttxt{1 2}.log
	共有ディレクトリ/jp1cons/log/action/acttxt{1 2}.log
コマンド実行履歴ファイル	/var/opt/jp1base/log/COMMAND/以下の全ファイル
	共有ディレクトリ/jp1base/log/COMMAND/以下の全ファイル
イベント DB	/var/opt/jp1base/sys/event/servers/default/以下のIMEvent*. *ファイル※
	共有ディレクトリ/jp1base/event/以下のIMEvent*. *ファイル※

注※ イベントサービインデックス (index) ファイルで別パスを指定した場合は、指定したパス以下のファイルが対象となります。

6. IM データベースを使用している場合は、IM データベースをセットアップする。

7. インテリジェント統合管理基盤を使用している場合、次の表に示すファイルを削除する。

OS	対象ファイル
Windows	Manager パス¥data¥imdd¥actevent.ser
	Manager パス¥data¥imdd¥imdd_nodeStatus.ser

OS	対象ファイル
	Manager パス\data\imdd\jddactseq.ser
	共有フォルダ\data\imdd\actevent.ser
	共有フォルダ\data\imdd\imdd_nodeStatus.ser
	共有フォルダ\data\imdd\jddactseq.ser
UNIX	/var/opt/jp1imm/data/imdd/actevent.ser
	/var/opt/jp1imm/data/imdd/imdd_nodeStatus.ser
	/var/opt/jp1imm/data/imdd/jddactseq.ser
	共有ディレクトリ/jp1imm/data/imdd/actevent.ser
	共有ディレクトリ/jp1imm/data/imdd/imdd_nodeStatus.ser
	共有ディレクトリ/jp1imm/data/imdd/jddactseq.ser

8. JP1/Base を起動する。

9. JP1/IM - Manager を起動する。

以上で、マネージャーのシステム日時を元に戻す作業は完了です。なお、セントラルスコープの機能を使用する場合は、次の手順を続けて作業してください。

1. JP1/IM - View で JP1/IM - Manager (セントラルスコープ) にログインする。

2. [監視ツリー] 画面で最上位の監視グループを選択し、状態を「初期状態」にする。

監視ノードをすべて「初期状態」に戻すことで、セントラルスコープの管理するデータの不整合を解消します。

(2) エージェントの日時を元に戻す

(a) エージェントとして JP1/IM - Agent を使用している場合

エージェントの日時を元に戻す場合は、該当ホストの JP1/IM - Agent の設定変更を実施する必要があります。手順などの詳細については、「[2.5 統合エージェントホストのシステム日時を変更する場合に必要な手順](#)」の説明を参照してください。

(b) エージェントとして JP1/Base を使用している場合

エージェントの日時を元に戻す場合は、該当ホストの JP1/Base の設定変更を実施する必要があります。手順などの詳細については、マニュアル「[JP1/Base 運用ガイド](#)」の JP1/Base 運用中の設定変更の章、システムの日時変更時に必要な作業の説明を参照してください。

2.4.2 システムの時刻を進める

システムの時刻を進める場合には、過去に戻す場合と異なり、JP1/IM を停止したり、ファイルを削除したりする必要はありません。

ただし、IM データベースを使用している場合は、IM データベースの起動または停止処理中に時刻を変更しないでください。

2.5 統合エージェントホストのシステム日時を変更する場合に必要な手順

2.5.1 統合エージェントホストのシステム日時を変更する

数秒程度の時刻補正であれば、特に何もする必要はありません。

システム日時を変更する場合は、次の手順を実施します。

1. JP1/IM - Agent のサービスを停止する。
2. システム日時を変更する。
3. 下記のディレクトリを空にする。
 - Windows の場合
Agent パス\data>alertmanager
Agent パス\data#prometheus
Agent パス\data#fluentd
 - Linux の場合
/opt/jp1ima/data/alertmanager
/opt/jp1ima/data/prometheus
/opt/jp1ima/data/fluentd
4. JP1/IM - Agent のサービスを起動する。

2.5.2 クラスタシステムでシステム日時を変更する

数秒程度の時刻補正であれば、特に何もする必要はありません。

システム日時を変更する場合は、次の手順を実施します。

1. クラスタソフトから JP1/IM - Agent のサービスを停止する。
2. 物理ホストも運用している場合は、物理ホストの JP1/IM - Agent のサービスも停止する。
3. 実行系サーバと待機系サーバの両方でシステム日時を変更する。
4. 下記のディレクトリを空にする。
 - Windows の場合
Agent パス\data>alertmanager※
Agent パス\data#prometheus※

Agent パス¥data¥fluentd※

共有フォルダ¥jp1ima¥data¥alertmanager

共有フォルダ¥jp1ima¥data¥prometheus

共有フォルダ¥jp1ima¥data¥fluentd

注※ 実行系サーバと待機系サーバの両方に存在する点に注意してください。

- Linux の場合 (/opt/jp1ima は実行系と待機系の両方あるので注意が必要です。)

/opt/jp1ima/data/alertmanager※

/opt/jp1ima/data/prometheus※

/opt/jp1ima/data/fluentd※

共有ディレクトリ/jp1ima/data/alertmanager

共有ディレクトリ/jp1ima/data/prometheus

共有ディレクトリ/jp1ima/data/fluentd

注※

実行系サーバと待機系サーバの両方に存在する点に注意してください。

5. クラスタソフトから JP1/IM - Agent のサービスをすべて起動する。

6. 物理ホストも運用している場合は、物理ホストの JP1/IM - Agent のプロセスを起動する。

2.5.3 コンテナでシステム日時を変更する

数秒程度の時刻補正であれば、特に何もする必要はありません。

システム日時を変更する場合は、コンテナを削除し、システム日時を変更してからコンテナを作り直してください。

2.6 リモート監視構成の監視対象ホストの日時を変更した場合に必要な作業

リモート監視構成の監視対象ホストの日時を変更した場合の注意事項および手順について説明します。

2.6.1 リモート監視構成の監視対象ホストの日時を過去に戻す

テストなどでリモート監視構成の監視対象ホストの時刻を意図的に未来の日時へ変更したような場合に、リモート監視構成の監視対象ホストの日時を元に戻すときは、監視対象ホストで未来の日時のイベントログとリモート監視の収集状態を保存したファイルを削除する必要があります。

次に示す手順で戻してください。

1. 日時を戻すリモート監視構成の監視対象ホストで、稼働中のリモート監視イベントログトラップがある場合は、停止する。
2. リモート監視構成の監視対象ホストの日時を変更する。
3. リモート監視構成の監視対象ホストのイベントログに、リモート監視構成の監視対象ホストの現在日時より未来の日時のイベントログが存在しないか確認する。未来の日時のイベントログが存在する場合は、該当するイベントログを削除する。
4. 収集状態を保存している次のファイルをバックアップしたあと、次のファイルを削除する。
 - 物理ホストの場合
Manager パス¥log¥imcf¥profiles¥監視対象ホスト名¥al¥event_log_trap¥evt.wdef
 - 論理ホストの場合
共有フォルダ¥JP1IMM¥log¥imcf¥profiles¥監視対象ホスト名¥al¥event_log_trap¥evt.wdef誤ったファイルを削除した場合は、バックアップしたファイルをリストアします。
5. 停止したリモート監視イベントログトラップを再度起動する。

なお、JP1/IM - Manager が動作しているマシンと監視対象ホストの日時が異なっている場合、リモート監視イベントログトラップによる監視ができません。監視対象ホストの日時を変更する場合は、JP1/IM - Manager が動作しているマシンの日時も確認してください。

2.6.2 リモート監視構成の監視対象ホストの日時を進める

時刻が遅れているなどの理由で、リモート構成の監視対象ホストの日時を進める場合、手順は必要ありません。

2.7 リモート監視構成の監視対象ホストのパスワードを変更した場合に必要な作業

リモート監視構成の監視対象ホストを管理するマネージャーおよびリモートの監視対象ホストのパスワードを変更した場合には、[リモート監視設定] 画面または [システム共通設定] 画面の設定を見直す必要があります。

リモートの監視対象ホストのユーザー名およびドメイン名を変更した場合も、[リモート監視設定] 画面または [システム共通設定] 画面の設定を見直してください。

メモ

リモートの監視対象ホストを登録・変更する場合、OS 通信設定の情報をシステム共通設定として保存し、管理できます。この場合、[リモート監視設定] 画面ではなく、[システム共通設定] 画面で設定してください。

[リモート監視設定] 画面または [システム共通設定] 画面での設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

[リモート監視設定] 画面または [システム共通設定] 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」を参照してください。

- [5.7 [リモート監視設定] 画面]
- [5.20 [システム共通設定] 画面]

2.8 リモート監視構成からエージェント構成に監視構成を変更する場合の注意事項

リモート監視構成のログファイルトラップ（リモート監視ログファイルトラップ）およびイベントログトラップ（リモート監視イベントログトラップ）を、エージェント構成のログファイルトラップおよびイベントログトラップで監視するように構成を変更する場合の注意事項について説明します。

リモートの監視対象ホストの管理の概要については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.6 リモートの監視対象ホストの管理」を参照してください。

2.8.1 JP1/Base のログファイルトラップでの注意事項

ログファイルトラップの監視構成をリモート監視構成からエージェント監視構成に変更する場合は、次の点を注意してください。

- 共通定義情報で拡張正規表現を有効に設定する
- ファイル監視間隔（-t オプション）を指定していない場合、監視間隔が短くなる
- 論理ホストのリモート監視を移行する場合、登録先イベントサーバ名（-s オプション）を指定する

2.8.2 JP1/Base のイベントログトラップでの注意事項

イベントログトラップの監視構成をリモート監視構成からエージェント監視構成に変更する場合は、次の点を注意してください。

- 共通定義情報で拡張正規表現を有効に設定する
- 論理ホストのリモート監視を移行する場合、JP1/Base のイベントログトラップ動作定義ファイルのイベントサーバ名（server）を指定する

JP1/Base のイベントログトラップ動作定義ファイルについては、マニュアル「JP1/Base 運用ガイド」の定義ファイルの説明をしている章を参照してください。

- trap-interval に 181 以上を指定している場合、180 以下に変更する
JP1/Base のバージョンが、11-00 以降の場合は、trap-interval は設定不要です。
- trap-interval を指定していない場合、監視間隔が短くなる
JP1/Base のバージョンが、11-00 以降の場合は、trap-interval は設定不要です。
- リモート監視と同様に、イベントログの監視中にイベントログの取得に失敗した際に JP1 イベントを出力したい場合は、jp1event-send に 1（通知設定）を定義する

2.9 ポート番号を変更する場合に必要な手順

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する場合、次の手順を実行してください。

1. JP1/IM - Manager サービスを停止する。
2. 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` を変更する。
3. JP1/IM - Manager サービスを起動する。

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。

2.10 統合エージェントホストのロケールを変更する場合に必要な作業

2.10.1 統合エージェントホストのロケールを変更する

(1) Windows 環境の場合

次の手順で Windows の言語を変更します。

1. JP1/IM - Agent のサービスを停止する。
2. Windows の言語設定を変更する。

Windows の言語設定を、次のように統一する必要があります。

設定	設定箇所	確認方法
システムロケール※1	[コントロールパネル] - [地域] 画面 - [管理] タブ	[Unicode 対応でないプログラムの言語]
言語および地域の形式	[コントロールパネル] - [地域] 画面 - [形式] タブ	[形式]
	[コントロールパネル] - [地域] 画面 - [場所] タブ※2	[主な使用場所]
国または地域	[設定] - [時刻と言語] 画面 - [地域と言語] タブ※2	[国または地域]
	[設定] - [時刻と言語] 画面 - [地域] タブ※3	[国または地域] [地域設定]
言語	[設定] - [時刻と言語] 画面 - [地域と言語] タブ※2	[言語]
	[設定] - [時刻と言語] 画面 - [言語] タブ※3	[Windows の表示言語] [優先する言語]
システムアカウントおよびようこそ画面の地域と言語の設定	[コントロールパネル] - [地域] 画面 - [管理] タブ - [設定のコピー] ボタン - [ようこそ画面と新しいユーザーアカウントの設定] 画面	[現在のユーザー] [ようこそ画面]

注※1 「ベータ：ワールドワイド言語で Unicode UTF-8 を使用」はサポート対象外です。

注※2 Windows Server 2016 の場合が該当します。

注※3 Windows Server 2019 および Windows Server 2022 の場合が該当します。

3. 統合エージェントを起動する。

(2) Linux 環境の場合

Linux 環境でサポートする環境変数 LANG の設定については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.11(1) 統合エージェントの言語設定」を参照してください。

プロセス稼働時の環境変数 LANG の設定は、ユニット定義ファイルに、次のような形式で記載します。

```
Environment=LANG=ja_JP.UTF-8
```

ユニット定義ファイルの編集方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

2.10.2 クラスタシステムでロケールを変更する

「2.10.1 統合エージェントホストのロケールを変更する」の手順と同じです。

ただし、Windows 環境の場合は、次のことに注意してください。

- 統合エージェントのサービスを起動または停止するときは、クラスタソフトから行ってください。
- 変更作業は、実行系サーバと待機系サーバの両方で実施してください。

2.10.3 コンテナでロケールを変更する

「2.10.1 統合エージェントホストのロケールを変更する」の手順と同じです。

2.11 統合エージェントホストの複製

2.11.1 物理ホストの複製

1. すべての JP1/IM - Agent のサービスが自動起動しないように設定する。

自動起動の無効化の設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.1(2) 自動起動の有効化・無効化」および「2.19.1(2) 自動起動の有効化・無効化」を参照してください。

2. ホストを複製し、複製したホストを起動する。

3. 複製したホストに新しいホスト名を設定する。

4. 複製したホストに初期シークレットを再設定する。

統合マネージャーにアクセスするための初期シークレット（初回接続用のシークレット）を設定します。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を確認します。初期シークレットの表示については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.3 [初期シークレットの表示] 画面」を参照してください。シークレット管理コマンドで、初期シークレットを再設定します。

```
jimasecret -add -key immgr.initial_secret -s "初期シークレット"
```

5. 複製したホストに登録されている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
```

6. JP1/IM - Agent のホスト名の変更手順を実施する。

ホスト名の変更手順については、「2.2.1(3) エージェントのホスト名を変更した場合の作業」を参照してください。

7. 手順 1 で自動起動しないように設定変更した JP1/IM - Agent のサービスの自動起動の設定を元に戻す。

自動起動の有効化の設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.1(2) 自動起動の有効化・無効化」および「2.19.1(2) 自動起動の有効化・無効化」を参照してください。

2.11.2 運用開始後の AWS/EC2 インスタンスの複製

1. すべての JP1/IM - Agent のサービスが自動起動しないように設定する。

自動起動の無効化の設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.1(2) 自動起動の有効化・無効化」および「2.19.1(2) 自動起動の有効化・無効化」を参照してください。

2. AWS/EC2 インスタンスの AMI を作成する。

3. AMI から新しいホストを起動する。

4. 新しいホストに新しいホスト名を設定する。

5. 新しいホストに初回接続用のシークレットを再設定する。

統合マネージャーにアクセスするための初期シークレット（初回接続用のシークレット）を設定します。

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を確認します。初期シークレットの表示については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.2.3 [初期シークレットの表示] 画面」を参照してください。

シークレット管理コマンドで、初期シークレットを再設定します。

```
jimasecret -add -key immgr.initial_secret -s "初期シークレット"
```

6. 複製したホストに登録されている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. JP1/IM - Agent のホスト名の変更手順を実施する。

ホスト名の変更手順については、「2.2.1(3) エージェントのホスト名を変更した場合の作業」を参照してください。

8. 手順 1 で自動起動しないように設定変更したプロセスの自動起動の設定を元に戻す。

自動起動の有効化の設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.1(2) 自動起動の有効化・無効化」および「2.19.1(2) 自動起動の有効化・無効化」を参照してください。

3

JP1/IM - Manager の起動と終了

この章では、JP1/IM - Manager の起動および終了の手順について説明します。

3.1 JP1/IM - Manager を起動する

ここでは、JP1/IM - Manager の起動手順を説明します。

JP1/IM - Manager を起動する場合は、先に監視で必要な JP1/Base のサービスをすべて起動してください。JP1/Base のサービスを再起動する場合は、必ず JP1/IM - Manager を停止した状態にしてください。停止しなかった場合は、イベントが表示されないなどの現象が発生します。

JP1/Base のサービスの起動については、マニュアル「JP1/Base 運用ガイド」の起動と終了の章を参照してください。

また、JP1/Base のイベントサービスを再起動する場合は、必ず JP1/IM - Manager を停止した状態にしてください。再起動しなかった場合は、イベントが表示されないなどの現象が発生します。

起動方法は、OS によって異なります。詳細については、「3.1.1 Windows の場合」、「3.1.2 UNIX の場合」を参照してください。

3.1.1 Windows の場合

JP1/IM - Manager を起動するホストの OS が Windows であり、かつ物理ホストである場合の起動方法を説明します。

1. IM データベースを起動する (IM データベースを使用する場合)

JP1/IM3-Manager DB Server サービスを起動します。

2. インテリジェント統合管理データベースを起動する (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)

JP1/IM3-Manager Trend Data Management Service サービスを起動します。

JP1/IM3-Manager Intelligent Integrated DB Server サービスは、連動して自動的に起動されます。

3. JP1/IM - Manager を起動する。

JP1/IM3-Manager サービスを起動します。

IM データベース、インテリジェント統合管理データベース、および JP1/IM - Manager を起動するには、JP1/Base の起動管理機能を使用する方法と、起動管理機能を使わない方法があります。

起動管理機能は、あらかじめ設定した順序に従って、サービスを起動する機能です。起動管理機能が設定してあると、Windows の起動時に、まず、JP1/Base Control Service が起動し、そのあと JP1/Base、JP1/IM - Manager などの各サービスを順に起動します。

システムの起動時に自動で各サービスを起動したい場合は、JP1/Base の起動管理機能を使用してサービスの起動順序を制御してください。

なお、起動管理機能を使用してサービスを起動するには、Windowsの[コントロールパネル] - [管理ツール] - [サービス]を選択し、「サービス」ダイアログボックスで、次のサービスの起動方法を「手動」にしておく必要があります。

- JP1/IM3-Manager DB Server サービス (IM データベースを使用する場合)
- JP1/IM3-Manager Intelligent Integrated DB Server サービスおよび JP1/IM3-Manager Trend Data Management Service サービス (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)
- JP1/IM3-Manager サービス

起動管理機能の詳細については、マニュアル「JP1/Base 運用ガイド」のサービスの起動順序および終了順序の設定 (Windows 限定) の章を参照してください。

IM データベースの起動

IM データベースは、デフォルトでは、JP1/Base の起動管理機能で起動しないように設定されています。起動管理機能を使わないで起動する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、JP1/IM3-Manager DB Server サービスを起動してください。

起動管理機能を使って起動する場合は、JP1/Base の起動順序定義ファイルで、次の行から「#」を削除してください。また、StopCommand の<JP1/IM - Manager Path>の部分を Manager パスに置き換えてください。

```
#[Jp1IM-Manager DB]
#Name=JP1/IM-Manager DB Server
#ServiceName= HiRDBEmbeddedEdition_JM0
#StopCommand=Manager パス¥bin¥imdb¥jimdbstop.exe
```

インテリジェント統合管理データベースの起動

インテリジェント統合管理データベースは、デフォルトでは、JP1/Base の起動管理機能で起動しないように設定されています。

起動管理機能を使わないで起動する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、JP1/IM3-Manager Intelligent Integrated DB Server サービスおよび JP1/IM3-Manager Trend Data Management Service サービスを起動してください。

起動管理機能を使って起動する場合は、JP1/Base の起動順序定義ファイルで、次の行を[Jp1IM-Manager DB]と[Jp1IM-Manager]の間のセクションに追加してください。

```
[Jp1IM-GN DB]
Name= JP1/IM-Manager Intelligent Integrated DB Server
ServiceName= JP1_IMGNDDB_Service
StopCommand=Manager パス¥bin¥imgndb¥jimgnbdbstop.exe
[Jp1IM-Trend Data Management]
Name= JP1/IM-Manager Trend Data Management Service
ServiceName= promscale
```

JP1/IM - Manager の起動

JP1/IM - Manager は、デフォルトでは、JP1/Base の起動管理機能で起動するように設定されています。

起動管理機能を使わないで起動する場合は、[コントロールパネル] - [管理ツール] - [サービス] から、JP1/IM3-Manager サービスを起動してください。

! 重要

- JP1/Power Monitor を使用して JP1/IM - Manager を起動するホストの起動・停止をする場合は、JP1/Base の起動順序定義ファイルの `StopCommand` パラメーターに、「`net stop IM データベースサービス名`」を実行するバッチファイルなどのコマンドを指定してください。
- 統合監視 DB を使用する場合は統合監視 DB のセットアップ、IM 構成管理を使用する場合は IM 構成管理 DB のセットアップ、セントラルスコープを使用する場合は監視オブジェクト DB のセットアップをそれぞれ実施してから、JP1/IM - Manager を起動してください。

3.1.2 UNIX の場合

UNIX の場合は、OS の機能によって JP1/IM - Manager を起動します（自動起動スクリプトが設定されている場合）。

システム起動時に自動起動スクリプトが実行されて、次の順に起動します。

1. JP1/Base
2. JP1/IM - Manager
3. IM データベース（IM データベースを使用している場合）
4. インテリジェント統合管理データベース（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）
5. 統合エージェント管理基盤（JP1/IM - Agent を使用している場合）

なお、自動起動スクリプトの設定の有効・無効に関係なく、システム起動時に `pdprcd` プロセスが起動されます。

自動起動スクリプトの設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。また、自動起動スクリプ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「`jco_start`（UNIX 限定）」（1. コマンド）を参照してください。

自動起動スクリプトを設定しないで JP1/IM - Manager を起動する場合は、`/etc/opt/jp1cons/jco_start.model` スクリプト、またはこのスクリプトをコピーしたファイルを実行して起動してください。

なお、JP1/IM - Manager を起動する場合は、先に監視に必要な JP1/Base のサービスをすべて起動してください。また、JP1/IM - Manager の起動時に次のデータベースを起動してください。

- IM データベース (IM 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 (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)

JP1/Base のサービスを再起動する場合は、必ず JP1/IM - Manager を停止した状態にしてください。停止しなかった場合は、イベントが表示されないなどの現象が発生します。

JP1/Base のサービスの起動については、マニュアル「JP1/Base 運用ガイド」の起動と終了の章を参照してください。

❗ 重要

統合監視 DB を使用する場合は統合監視 DB のセットアップ、IM 構成管理を使用する場合は IM 構成管理 DB のセットアップ、セントラルスコープを使用する場合は監視オブジェクト DB のセットアップをそれぞれ実施してから、JP1/IM - Manager を起動してください。

(1) Linux 環境で JP1/IM - Manager の自動起動および自動終了を設定している場合の注意事項

自動起動・自動停止を有効にしたあと、JP1/IM - Manager を手動で起動する場合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。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の稼働状態は `jimgndbstatus` 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 の自動起動・自動停止が有効の場合、`systemctl` コマンド以外の、`jco_start/jco_start.cluster` コマンド、`jco_stop/jco_stop.cluster` コマンドで起動したり停止したりすると、JP1/IM - Manager の自動停止が行われません (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なままです)。

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` コマンドによる起動操作を行ってください。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
```

(2) JP1/IM - Agent を使用するための統合エージェント管理基盤の設定

統合マネージャーホストの JP1/IM - Agent サービスの起動方法（UNIX 環境）を、次に示します。

条件		操作
物理ホスト	統合エージェントを使用する場合	1. 「jco_start」コマンドを実行する。

3.1.3 クラスタシステムで運用する場合

プラットフォーム（OS およびクラスタソフトの種類）にかかわらず、クラスタシステムで論理ホストの JP1/IM - Manager を運用する場合は、クラスタソフトの制御によって JP1/IM - Manager を起動します。

クラスタシステムでは、実行系サーバでアプリケーションを実行し、システムダウンなどの障害発生時に待機系サーバへフェールオーバーするために、アプリケーションをクラスタソフトに登録して起動停止を制御しています。JP1/IM - Manager をクラスタ運用する場合も、クラスタソフトが JP1/IM - Manager を制御するように登録して運用します。

なお、クラスタ運用している JP1/IM - Manager は、クラスタソフトの操作によって起動・停止をしてください。コマンドを実行するなど手動で起動・停止した場合は、クラスタソフトの管理する JP1/IM - Manager の動作状態と実際の動作状態が異なってしまい、障害と判定される場合があります。

起動順序については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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）」、「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。

3.1.4 非クラスタシステムで論理ホストを運用する場合

非クラスタシステムの論理ホストでは、JP1/Base および JP1/IM - Manager を次の順に起動してください。

1. JP1/Base

2. IM データベース（IM データベースを使用する場合）

「JP1/IM3-Manager DB Cluster Service_論理ホスト名」を起動してください。

3. インテリジェント統合管理データベース（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）

3. JP1/IM - Manager の起動と終了

「JP1/IM3-Manager Intelligent Integrated DB Server_論理ホスト名」および「JP1/IM3-Manager Trend Data Management Service_論理ホスト名」を起動してください。

4. JP1/IM - Manager

「JP1/IM3-Manager サービス」を起動してください。

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については、[「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。

3.2 JP1/IM - Manager を終了する

ここでは、JP1/IM - Manager の終了手順を説明します。

JP1/IM - Manager は、JP1/Base より前に終了してください。また、JP1/IM - Manager の終了時に、次のデータベースを終了する必要があります。

- IM データベース (IM 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 (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)

終了方法は、OS によって異なります。

3.2.1 Windows の場合

次の順に終了してください。

1. JP1/IM3-Manager サービス
2. JP1/IM3-Manager Trend Data Management Service サービス (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)
3. JP1/IM3-Manager Intelligent Integrated DB Server サービス (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)
4. JP1/IM3-Manager DB Server サービス (IM データベースを使用している場合)
5. JP1/Base

JP1/Power Monitor をインストールしている場合は、JP1/Base の起動管理機能を使用してサービスを終了できます。起動管理機能の設定については、マニュアル「JP1/Base 運用ガイド」のサービスの起動順序および終了順序の設定 (Windows 限定) の章を参照してください。

起動管理機能を使わないで終了させる場合は、[コントロールパネル] - [管理ツール] - [サービス] から、JP1/IM3-Manager サービスを終了してください。

3.2.2 UNIX の場合

自動終了スクリプトが設定されているときは、システムを終了すると、次の順で続けて終了します。

1. JP1/IM - Manager
2. インテリジェント統合管理データベース (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)
3. IM データベース (IM データベースを使用している場合)
4. JP1/Base

なお、pdprcd プロセスは、JP1/IM - Manager、インテリジェント統合管理データベース、および IM データベースが終了しても起動したままとなりますが、停止する必要はありません。

自動終了スクリプトの設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。また、自動終了スクリプ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「jco_stop (UNIX 限定)」(1. コマンド) を参照してください。

自動終了スクリプトを設定しないで JP1/IM - Manager を終了させる場合は、`/etc/opt/jp1cons/jco_stop.model` スクリプト、またはこのスクリプトをコピーしたファイルを実行して終了してください。

(1) Linux 環境で JP1/IM - Manager の自動起動および自動終了を設定している場合の注意事項

自動起動・自動停止を有効にしたあと、JP1/IM - Manager を手動で停止する場合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。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の稼働状態は `jimgndbstatus` コマンドで確認できます。

- 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/jco_start.cluster` コマンド、`jco_stop/jco_stop.cluster` コマンドで起動したり停止したりすると、JP1/IM - Manager の自動停止が行われません (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なままです)。

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` コマンドによる起動操作を行ってください。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
```

3.2.3 クラスタシステムで運用する場合

プラットフォーム（OS およびクラスタソフトの種類）にかかわらず、クラスタシステムで論理ホストの JP1/IM - Manager を運用する場合は、クラスタソフトの制御によって JP1/IM - Manager を停止します。

クラスタシステムでは、実行系サーバでアプリケーションを実行し、システムダウンなどの障害発生時に待機系サーバへフェールオーバーするために、アプリケーションをクラスタソフトに登録して起動停止を制御しています。JP1/IM - Manager をクラスタ運用する場合も、クラスタソフトが JP1/IM - Manager を制御するように登録して運用します。

なお、クラスタ運用している JP1/IM - Manager は、クラスタソフトの操作によって起動・停止をしてください。コマンドを実行するなど手動で起動・停止した場合は、クラスタソフトの管理する JP1/IM - Manager の動作状態と実際の動作状態が異なってしまい、障害と判定される場合があります。

3.2.4 非クラスタシステムで論理ホストを運用する場合

非クラスタシステムの論理ホストでは、JP1/Base および JP1/IM - Manager を次の順に停止してください。

1. JP1/IM - Manager

「JP1/IM3-Manager_論理ホスト名」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（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）

「JP1/IM3-Manager Intelligent Integrated DB Server_論理ホスト名」および「JP1/IM3-Manager Trend Data Management Service_論理ホスト名」を停止してください。

3. IM データベース（IM データベースを使用する場合）

「JP1/IM3-Manager DB Cluster Service_論理ホスト名」を停止してください。

4. JP1/Base

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については、「[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。

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

システム開始時および停止時に、論理ホスト用の JP1 サービスを自動起動および自動停止する場合は、次の手順で設定する必要があります。設定方法は、JP1/IM - Manager がサポートする OS によって異なります。OS ごとの設定方法を次に示します。

3.3.1 非クラスタシステムの論理ホスト運用で自動起動および自動停止を設定する (Windows の場合)

1. 起動順序定義ファイル (JP1SVPRM.DAT) に、次の記述をテキストエディターで追記する。

格納先 : Base パス¥conf¥boot¥JP1SVPRM.DAT

```
[Jp1BaseEvent 論理ホスト名]
Name=JP1/BaseEvent 論理ホスト名
ServiceName=JP1_Base_Event 論理ホスト名

[Jp1Base 論理ホスト名]
Name=JP1/Base 論理ホスト名
ServiceName=JP1_Base 論理ホスト名
StopCommand=jbs_spm�_stop.exe -h 論理ホスト名

[JP1/IM-Manager DB Cluster Service 論理ホスト名]
Name=JP1/IM-Manager DB Cluster Service 論理ホスト名
ServiceName=HiRDBClusterService_JMn
StopCommand=Managerパス¥bin¥imdb¥jimdbstop.exe -h 論理ホスト名

[Jp1IM-Manager 論理ホスト名]
Name=JP1/IM-Manager 論理ホスト名
ServiceName=JP1_Console 論理ホスト名
StopCommand=jco_spm�_stop.exe -h 論理ホスト名
```

JMn : n はクラスタセットアップ情報ファイルの LOGICALHOSTNUMBER と同じものを指定してください。

StopCommand パラメーターで指定しているコマンドは、JP1/Power Monitor からのシャットダウン時に実行されます。

❗ 重要

JP1/Power Monitor を使用して JP1/IM - Manager を起動するホストの起動・停止をする場合は、JP1/Base の起動順序定義ファイルの StopCommand パラメーターに、「net stop IM データベースサービス」を実行するバッチファイルなどのコマンドを指定してください。

3.3.2 非クラスタシステムの論理HOST運用で自動起動および自動停止を設定する (Linux の場合)

1. 論理HOST用の自動起動および自動停止スクリプトを作成する。

格納先: /usr/lib/systemd/system/jp1_cons_論理HOST名.service

自動起動および自動停止スクリプト例

```
[Unit]
Description=JP1/Integrated Management - Manager 論理HOST名 Service
Requires=jp1_base_論理HOST名.service
After=jp1_base_論理HOST名.service
ConditionFileIsExecutable=/etc/opt/jp1cons/jco_start.cluster
ConditionFileIsExecutable=/etc/opt/jp1cons/jco_stop.cluster

[Service]
ExecStart=/etc/opt/jp1cons/jco_start.cluster 論理HOST名
ExecStop=/etc/opt/jp1cons/jco_stop.cluster 論理HOST名

Type=forking
KillMode=none
StandardOutput=null
StandardError=null

[Install]
WantedBy=multi-user.target graphical.target
```

論理HOST名は起動する論理HOST名とします。JP1/Base の論理HOSTの Unit ファイルの詳細については、JP1/Base の設定に従ってください。

論理HOST用の自動起動および自動停止スクリプトを作成したあとに、次のコマンドを実行してパーミッションを設定してください。

```
chmod 644 /usr/lib/systemd/system/jp1_cons_論理HOST名.service
chgrp root /usr/lib/systemd/system/jp1_cons_論理HOST名.service
chown root /usr/lib/systemd/system/jp1_cons_論理HOST名.service
```

2. 次のコマンドで作成した自動起動および自動停止スクリプトを登録する。

```
# systemctl --system enable jp1_cons_論理HOST名
```

3. 自動起動および自動停止スクリプトを編集した場合は、次のコマンドでその変更を systemd に反映させる。

```
# systemctl daemon-reload
```

❗ 重要

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_spm_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
```

3.3.3 物理ホストおよび論理ホストの両方で自動起動および自動停止をする場合の設定

物理ホストおよび論理ホストの両方で自動起動および自動停止をしたい場合は、論理ホストの自動起動および自動停止の設定に加えて、次に示す設定をする必要があります。

なお、設定方法は OS ごとに異なります。OS ごとの設定方法を次に示します。

Windows 環境の場合

起動管理機能では、起動順序定義ファイル（JP1SVPRM.DAT）に記載された順番どおりに上から起動・停止処理が実行されます。物理ホストおよび論理ホストの起動順序を変更したい場合は、起動順序定義

ファイル (JP1SVPRM.DAT) で、起動または停止したい順に、物理HOSTおよび論理HOSTの起動・停止順序を定義してください。

Linux 環境の場合

自動起動および自動停止の順序は、自動起動および自動停止スクリプトの数字部分 (S**およびK**の**部分) の値によって決定されます。数字部分の値が大きいほど、あとから実行されます。物理HOSTの自動起動および自動停止スクリプトへのシンボリックリンクは、インストール時に自動で作成されます。物理HOSTも含めた自動起動および自動停止をする場合は、論理HOST用に作成するシンボリックリンクの名称を変更して、物理HOSTおよび論理HOSTの起動および停止順序を調節してください。なお、物理HOST用の自動起動および自動停止スクリプトは、あらかじめ用意されています。物理HOSTの自動起動および自動停止スクリプトへのシンボリックリンク一覧を次の表に示します。

表 3-1 物理HOSTの自動起動および自動停止スクリプトへのシンボリックリンク一覧

起動スクリプト	停止スクリプト
/etc/rc.d/rc3.d/S99_JP1_20_CONS	/etc/rc.d/rc0.d/K01_JP1_80_CONS
/etc/rc.d/rc5.d/S99_JP1_20_CONS	/etc/rc.d/rc6.d/K01_JP1_80_CONS

シンボリックリンク一覧の S**および K**の** (数字) 部分の値と、論理HOSTの自動起動および自動停止スクリプトのシンボリックリンクの S**および K**の** (数字) 部分の値との大小関係によって、物理HOSTおよび論理HOSTの起動順序を調節してください。

例えば、論理HOSTを先に起動したい場合は、論理HOST用に作成する自動起動スクリプトへのシンボリックリンク名 S**の数字を、99 (Linux の場合) より小さい値にしてください。

3.4 起動と終了に関する注意事項

- JP1/IM - Manager のサービスの [ログオン] の設定は、初期設定の「システムアカウント」のまま変更しないでください。また、[デスクトップとの対話をサービスに許可] オプションにチェックを入れないでください。サービスが正常に動作しなくなるおそれがあります。

JP1/IM - Manager のサービスについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「2.8 JP1/IM - Manager のサービス」を参照してください。

- JP1/Base のイベントサービスを再起動した場合は、必ず JP1/IM - Manager を再起動してください。また、接続していた JP1/IM - View も再起動してください。再起動を行わない場合、イベントが表示されなくなるなどの現象が発生します。
- 論理ホスト対応の JP1/IM - Manager 全体のサービスを停止しても、プロセスが停止しない場合に、強制的にプロセスを停止したいときには、`jco_killall.cluster` コマンドを実行してください。このコマンドを使った停止は、正規の方法で JP1/IM - Manager のサービスを停止してもプロセスが停止しない場合にだけ使用してください。
- JP1/IM - Manager の起動時にイベントを大量^{※1} に取得する場合は、イベントの取得量に比例して起動時間^{※2} が長くなります。そのため、JP1/IM3-Manager サービス (Windows の場合) または `jco_start` コマンド (UNIX の場合) がタイムアウト^{※3} し、エラー値を返してることがあります。その場合は、JP1/IM - Manager が起動していないように見えますが、しばらくすると起動が完了します。

注※1

起動時のイベント取得フィルターの条件やイベント DB にたまっているイベントの量によって変わります。

注※2

マシン性能によって変わります。

注※3

JP1/IM3-Manager サービス (Windows の場合) のタイムアウトは 125 秒です。`jco_start` コマンド (UNIX の場合) のタイムアウトはデフォルトで 300 秒です。`jco_start` コマンドのタイムアウトの設定は、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド 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。

- IM データベースの起動が失敗した場合、IM データベースの状態が再起動中断状態であり、不安定な状態になることがあります (IM データベースの起動が失敗したあと、`jimdbstatus` コマンドを実行して、戻り値が 8 のとき)。

IM データベースの状態が再起動中断状態であり、不安定な状態になる要因は次のとおりです。

- ディスク容量不足 (IM データベースの容量不足ではない)
- メモリー容量不足

IM データベースの状態が再起動中断状態であり、不安定な状態の場合、サービスの停止、またはコマンドの実行による IM データベースの通常停止はできません。この状態を回避するためには、-f オプションを指定して jimdbstop コマンドを実行し、IM データベースを強制停止する必要があります。

- IM データベースを使用している場合、JP1/Base, IM データベースサービス, JP1/IM - Manager の順に起動してください。
- IM データベースを使用している場合、JP1/IM - Manager, IM データベースサービス, JP1/Base の順に終了してください。
- JP1/IM - MO を使用している場合は、JP1/IM - Manager の終了の前に、接続元の JP1/IM - MO の JP1/IM - Message Optimizer サービスを停止してください。
- JP1/Base の起動順序定義ファイル (jplsvprm.dat) の既定の記載例を用いて、JP1/Power Monitor からホストの終了処理を行う場合、IM データベースのサービスの停止処理において、イベントログに KAVA4516-E が出力されます。KAVA4516-E の出力を抑止するためには、起動順序定義ファイルを次に示す定義に変更してください。

- 物理ホストの場合

(1) 任意のファイル名で次の内容のバッチファイルを作成してください。

```
<Managerパス>%bin%imdb%jimdbstop.exe  
net stop HiRDBEmbeddedEdition_JM0
```

(2) 起動順序定義ファイルに以下のように記載してください。

以下は手順(1)で作成したバッチファイルの名称、及び格納先が"C:%jpl%jplimdbstopservice.bat" の場合の記載となります。

```
[Jp1IM-Manager DB]  
Name=JP1/IM-Manager DB Server  
ServiceName=HiRDBEmbeddedEdition_JM0  
StopCommand=C:%jpl%jplimdbstopservice.bat
```

- 論理ホストの場合

(1) 任意のファイル名で次の内容のバッチファイルを論理ホストごとに作成してください。

```
<Managerパス>%bin%imdb%jimdbstop.exe -h <論理ホスト名>  
net stop HiRDBCclusterService_JM<n>※
```

注※ <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 に指定した値を設定してください。

(2) 起動順序定義ファイルに以下のように記載してください。

以下は手順(1)で作成したバッチファイルの名称、及び格納先が"C:%jpl%jplimdbstopservice.bat" の場合の記載となります。

```
[Jp1IM-Manager DB]  
Name=JP1/IM-Manager DB Cluster Service_<論理ホスト名>  
ServiceName=HiRDBCclusterService_JM<n>※
```

StopCommand=C:¥jp1¥jp1imdbstopservice.bat

注※ <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 に指定した値を設定してください。

4

JP1/IM - Manager へのログインとログアウト

JP1/IM - View は、JP1/IM - Manager へログインして使用します。この章では、JP1/IM - Manager へのログイン・ログアウトの手順について説明します。

4.1 JP1/IM - Manager にログインする

JP1/IM - View および IM 構成管理・ビューアーを使用するには、ビューアーから JP1/IM - Manager へのログインが必要です。JP1/IM - Manager にログインする方法には、GUI でログインする方法と、`jcoview` コマンドまたは `jcfview` コマンドを使用してログインする方法があります。

なお、`jcoview` コマンドまたは `jcfview` コマンドのショートカットを Windows のスタートアップに登録すれば、Windows へのログオンと同時に JP1/IM - View および IM 構成管理・ビューアーを起動できます。また、`jcoview` コマンドまたは `jcfview` コマンドのショートカットを Windows の [スタート] ボタンの横に表示される「クイック起動バー (Quick Launch bar)」に登録したり、ホストまたはユーザーごとに `jcoview` コマンドまたは `jcfview` コマンドのショートカットを作成したりできます。

4.1.1 JP1/IM - Manager (インテリジェント統合管理基盤) に WWW ブラウザーでログインする

WWW ブラウザーを使用して JP1/IM - Manager (インテリジェント統合管理基盤) にログインする方法を次に示します。

1. WWW ブラウザーで接続先の JP1/IM - Manager (インテリジェント統合管理基盤) の URL を指定し、[ログイン] 画面を表示する。

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/login
```

注 SSL 通信を使用する場合は、`https` です。

URL の **ポート番号**には、インテリジェント統合管理基盤定義ファイル (`imdd.properties`) で設定したインテリジェント統合管理基盤のポート番号 (デフォルトは 20703) を指定します。

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「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。

2. ログイン画面で、ユーザー名、パスワードを入力する。

ユーザー名に指定できる文字数は、1~31 バイトです。半角英数字だけを使用できます。英字は大文字・小文字を区別しません。

パスワードは、大文字・小文字を区別します。

3. [ログイン] ボタンをクリックする。

統合オペレーション・ビューアーの画面が表示されます。

4.1.2 JP1/IM - Manager に GUI でログインする

(1) JP1/IM - View を使用する

JP1/IM - View を使用して JP1/IM - Manager に GUI でログインする方法を次に示します。

1. Windows のスタートメニューから、[すべてのプログラム] – [JP1_Integrated Management 3 - View] – [統合ビュー] を選択する。

[ログイン] 画面が表示されます。

2. ログイン画面で、ユーザー名、パスワード、および接続ホスト名を入力する。

ユーザー名に指定できる文字数は、1～31 バイトです。半角英数字だけを使用できます。英字は大文字・小文字を区別しません。

パスワードは、大文字・小文字を区別します。

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。

ログイン画面については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「1.2.2 セントラルコンソールおよびセントラルスコープの [ログイン] 画面」を参照してください。

セントラルスコープにログインする場合は、事前にセントラルスコープの機能を使用するための設定が必要です。

3. 使用したい機能に合わせてチェックボックスをチェックする。

片方または両方をチェックできます。

[セントラルコンソール] チェックボックスをチェックすると、JP1/IM - Manager (セントラルコンソール) に接続します。

[セントラルスコープ] チェックボックスをチェックすると、JP1/IM - Manager (セントラルスコープ) に接続します。

4. [OK] ボタンをクリックする。

JP1/IM - Manager (セントラルコンソール) に接続した場合は [イベントコンソール] 画面、JP1/IM - Manager (セントラルスコープ) に接続した場合は [監視ツリー] 画面が表示されます。

ログインするユーザー名は、事前に登録が必要です。ユーザーの登録については、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。

JP1/IM - Manager にログインする場合、一つのビューアーからは、最大三つの異なるマネージャーにログインできます。

(2) IM 構成管理・ビューアーを使用する

IM 構成管理・ビューアーを使用して JP1/IM - Manager に GUI でログインする方法を次に示します。

1. Windows のスタートメニューから、[すべてのプログラム] – [JP1_Integrated Management 3 - View] – [構成管理] を選択する。

[ログイン] 画面が表示されます。

Windows のスタートメニューから [構成管理] が削除されている場合には、jcovcfsetup コマンドを実行して、Windows のスタートメニューに [構成管理] を追加する必要があります。Windows のスタートメニューに [構成管理] を追加する方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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)」を参照してください。

2. ログイン画面で、ユーザー名、パスワード、および接続ホスト名を入力する。

ユーザー名には、小文字だけを使用できます。大文字を使用した場合も小文字として認証されます。

パスワードは、大文字・小文字を区別します。

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. [OK] ボタンをクリックする。

IM 構成管理に接続し、[IM 構成管理] 画面が表示されます。

ログインするユーザー名は、事前に登録が必要です。ユーザーの登録については、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。

JP1/IM - Manager にログインする場合、一つのビューアーからは、最大三つの異なるマネージャーにログインできます。

4.1.3 JP1/IM - Manager にコマンドでログインする

(1) JP1/IM - View を使用する

JP1/IM - Manager にjcoview コマンドでログインし、JP1/IM - View を使用する方法を次に示します。

次のコマンドを実行します。

- ログイン画面を起動する場合

```
jcoview [-c][-s][-h 接続ホスト名][-u ユーザー名]
```

引数を指定しなかった場合は、前回ログインしたときの情報が入力された状態でログイン画面が起動します。

引数を指定した場合は、指定した値が入力された状態で [ログイン] 画面が起動します。

- ログインする場合

```
jcoview [-c][-s][-h 接続ホスト名][-u ユーザー名][-p パスワード]
```

引数をすべて指定した場合は、JP1/IM - Manager のセントラルコンソール、セントラルスコープ両方にログインします。-c だけ指定した場合はセントラルコンソールに、-s だけ指定した場合はセントラルスコープにログインします。-c、-s 両方とも省略した場合はセントラルコンソールにログインします。ユーザーが認証されると、[ログイン] 画面は表示されません。指定した引数に従って [イベントコンソール] 画面、[監視ツリー] 画面が表示されます。

GUI でログインする方法については、「[4.1.2 JP1/IM - Manager に GUI でログインする](#)」を参照してください。また、jcoview 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「jcoview (Windows 限定)」(1. コマンド)を参照してください。

(2) IM 構成管理・ビューアーを使用する

JP1/IM - Manager に jcfview コマンドでログインし、IM 構成管理・ビューアーを使用する方法を次に示します。

次のコマンドを実行します。

- ログイン画面を起動する場合

```
jcfview [-h 接続ホスト名][-u ユーザー名]
```

引数を指定しなかった場合は、前回ログインしたときの情報が入力された状態でログイン画面が起動します。

引数を指定した場合は、指定した値が入力された状態で [ログイン] 画面が起動します。

- ログインする場合

```
jcfview [-h 接続ホスト名][-u ユーザー名][-p パスワード]
```

引数をすべて指定した場合は、JP1/IM - Manager の IM 構成管理にログインします。

ユーザーが認証されると、[ログイン] 画面は表示されません。指定した引数に従って [IM 構成管理] 画面が表示されます。

GUI でログインする方法については、「[4.1.2 JP1/IM - Manager に GUI でログインする](#)」を参照してください。また、jcfview 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「jcfview (Windows 限定)」(1. コマンド)を参照してください。

4.2 JP1/IM - Manager からログアウトする

JP1/IM - Manager からログアウトする場合は、次の方法でログアウトしてください。

JP1/IM - Manager (インテリジェント統合管理) からログアウトする場合

- [統合オペレーション・ビューアー] 画面で [ファイル] - [ログアウト] を選択する。

JP1/IM - Manager (セントラルコンソール) からログアウトする場合

- [イベントコンソール] 画面で [ファイル] - [終了 (ログアウト)] を選択する。
- [イベントコンソール] 画面の右上の×ボタンをクリックする。

JP1/IM - Manager (セントラルコンソール) からログアウトすると、ユーザープロファイルが更新されて、カラム幅や表示フィルターの有効・無効などイベントコンソールのユーザー環境が保存されます。

JP1/IM - Manager (セントラルスコープ) からログアウトする場合

- [監視ツリー] 画面で [ファイル] - [終了 (ログアウト)] を選択する。
- [監視ツリー] 画面の右上の×ボタンをクリックする。

JP1/IM - Manager (IM 構成管理) からログアウトする場合

- [IM 構成管理] 画面で [ファイル] - [終了 (ログアウト)] を選択する。
- [IM 構成管理] 画面の右上の×ボタンをクリックする。

上記方法で起動中の画面が終了します。ただし、統合機能メニューから起動した画面とモニター画面は終了しません。これらの画面は、個別に終了させてください。

ログアウトせずに終了した場合、マネージャー上にログイン情報が残った状態になり、最終的にマネージャーのリソース不足になることがあります。必ずログアウト操作で終了してください。

5

インテリジェント統合管理基盤によるシステムの監視

この章では、インテリジェント統合管理基盤を使用してシステムを監視する手順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でシステムを監視するためには、統合監視 DB および発生元ホストマッピングの定義が有効となっている必要があります。

5.1 システムの状態の見方

発生元ホストのマッピング機能を有効にすると、[統合オペレーション・ビューアー] 画面の [稼働状況] 領域に、ログインしているマネージャーの統合監視 DB に登録されたシステムの状態が表示されます。システムに変更が発生した場合は画面を自動更新し、常に最新の状況を表示します。

[統合オペレーション・ビューアー] 画面でシステムの状態を確認することで、次のような運用ができます。

- 管理しているシステム、およびそのシステムの状態を一目で確認できる
- ジョブの運用中の異常を検知し、重大な業務障害を回避できる
- システムの障害発生個所を特定し、重要な事象の発生を把握できる
- 管理しているどのシステムに影響があるか、障害の要因を把握できる
- サンバースト、ツリーまたはダッシュボードのノード状態パネルに表示された項目の色で、対処の優先度（緊急性）を把握できる
- 各種 IT リソースのアラート情報を把握できる
- 各種 IT リソースのトレンド情報を把握できる

5.1.1 インテリジェント統合管理基盤で監視できるもの

インテリジェント統合管理基盤では、「システムの状態」、「JP1 イベント」、「関連ノード」、「各種 IT リソースのアラート」、「各種 IT リソースのトレンド情報」を監視できます。

- システムの状態
サンバースト、ツリーでは、階層構造で監視できます。
ダッシュボードでは、見たいノードだけを選択して監視できます。
- JP1 イベント
イベント一覧画面では、ノード単位の絞り込みやエラー状態で絞り込んで表示できます。ダッシュボードでは、発生した重要イベント件数、対処状況ごとの件数をグラフで監視できます。
- 関連ノード
ノードの関係をグラフィカルに確認できます。
- 各種 IT リソースのアラート
ダッシュボードでは、選択したノード単位で発生件数をビジュアルに監視できます。
- 各種 IT リソースのトレンド情報
[トレンド] タブでは、選択したノードのトレンド情報をグラフで表示できます。ダッシュボードでは、選択したノードのトレンド情報をグラフ形式、ゲージ形式、数値形式、ランキング形式などで監視できます。

5.1.2 サンバーストまたはツリーの表示項目

[稼働状況] 領域のサンバースト，またはツリーには，次の項目が階層構造で表示されます。

表 5-1 サンバーストまたはツリーの表示項目

表示項目	説明
システム名	システムやサブシステムの名前が表示されます。
ホスト名	システムに所属するホストの名前が表示されます。
カテゴリ名	監視対象をグループ化した項目です。
スケジューラーサービス名/ジョブグループ名	JP1/AJS と連携した場合に，JP1/AJS のスケジューラーサービス名とその配下のジョブグループ名が一つの構成要素として表示されます。
ルートジョブネット名	JP1/AJS と連携した場合に，ジョブグループに存在するルートジョブネットの名前が表示されます。
JP1/PFM の監視エージェントのサービス名	JP1/PFM - Manager と連携した場合に，JP1/PFM - Manager から取得した監視エージェントのサービス名が表示されます。
インストール製品名	インストールされた JP1 製品名（JP1/Base, JP1/AJS, JP1/PFM, JP1/IM - Manager など）が表示されます。

[稼働状況] 領域の切り替え例を次に示します。

図 5-1 [稼働状況] 領域の切り替え例



各項目の色は、システムの運用状態の健全性を意味します。システムが健全な場合は、異常なし/対処済みとして「緑色」で表示されます。「黄色」は警告、「橙色」はエラー、「赤色」は緊急/警戒/致命的な障害が発生していることを表します。

項目をクリックすると、[詳細表示] 領域に選択した項目に関連する情報が表示されます。

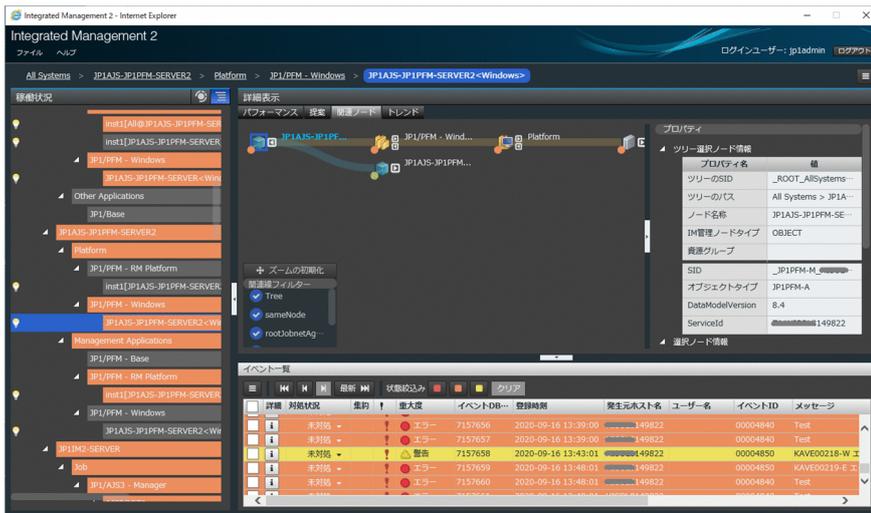
5.2 JP1 イベントの見方（[イベント一覧] 画面）

[イベント一覧] 画面でシステムの属性や対処状況を確認することで、次のような運用ができます。

[統合オペレーション・ビューアー] 画面の [稼働状況] 領域、および [詳細表示] 領域で項目を選択すると、選択した項目で発生している JP1 イベントの一覧が [イベント一覧] 領域に表示されます。

新しい JP1 イベントはイベント一覧の下に追加されます。到着日時が最も新しい JP1 イベントが、イベント一覧の最も下に表示されます。

図 5-2 [イベント一覧] 画面の表示例



イベント一覧に表示されるのは、次のイベントです。

- 統合監視 DB に登録されたイベント
- 選択した項目が発生元となるイベントおよび配下のすべての項目が発生元となるイベント
- 資源グループ・業務グループを設定している場合は、ログインしたユーザーに参照権限がある項目
- ユーザーフィルターを設定している場合は、ユーザーフィルターの設定に従ってフィルターを通過したイベント

[イベント一覧] 画面でシステムの属性や対処状況を確認することで、次のような運用ができます。

- システムに関連するイベントをすぐ絞り込みできるため、障害が発生したシステムの状態をすばやく確認できる
- イベントの詳細情報で、障害の原因や対処方法について詳細な調査ができる
- イベントの対処状況を簡単に変更できる
- 集約イベントの場合は、[繰り返しイベント一覧] 画面を表示することで、[繰り返しイベント一覧] 画面で集約された繰り返しイベントを確認できます。[繰り返しイベント一覧] 画面は、イベント一覧の [繰り返しイベント一覧] メニューをクリックすると表示されます。

- イベントがモニター起動対象のイベントの場合は、イベントに対応するアプリケーションの画面を起動し、イベントに関するより詳しい情報を確認できます。イベント一覧の [モニター起動] メニューからモニター起動できます。

5.2.1 イベント一覧の表示項目

イベント一覧には、各イベントの属性（基本属性、共通の拡張属性、または固有の拡張属性）が項目として表示されます。表示項目は変更できません。

イベント一覧に表示される項目（列）を次の表に示します。

表 5-2 イベント一覧の表示項目

表示項目 (列名)	説明
対処状況	JP1 イベントの対処状況を示す情報（対処済、処理中、保留、未処理）が表示されます。 集約イベントの場合は、集約開始イベントの対処状況が表示されます。集約開始イベントと集約している繰り返しイベントの対処状況が異なる場合は、集約開始イベントの対処状況欄に「!」が表示されます。
集約	集約開始イベントの場合に、  が表示されます。
! (重要イベント)	イベントが重要イベントの場合に、  が表示されます。集約イベントの場合は、集約開始イベントが重要イベントの場合に、  が表示されます。 重要イベントとして集約されている繰り返しイベントに、重要イベントと重要ではないイベントが混在している場合は、「!」が表示されます。
重大度	JP1 イベントの緊急性を示します。緊急性の高い順に、次の値があります。「緊急 (Emergency)」、「警戒 (Alert)」、「致命的 (Critical)」、「エラー (Error)」、「警告 (Warning)」、「通知 (Notice)」、「情報 (Information)」、「デバッグ (Debug)」 なお、統合監視 DB を使用する場合に、重大度変更機能で重大度を変更したときは、変更したあとの JP1 イベントの緊急性を表します。
イベント DB 内通し番号	発行元に関係なくこのイベントサーバに到達した順番です。
登録時刻	イベント発行元ホストのイベント DB に JP1 イベントが登録された時刻です。
発生元ホスト名	JP1 イベントを登録したエージェント名（発行元イベントサーバ名）です。
ユーザー名	JP1 イベント発行元のユーザー名です。
イベント ID	発行元のプログラムや、発生した事象を表す値です。
メッセージ	JP1 イベントの内容を表すメッセージテキストです。
オブジェクトタイプ	イベント発行の契機となる事象が発生したオブジェクトの種類を表す「JOB」、「JOBNET」などの文字列です。

表示項目 (列名)	説明
アクション	<p>自動アクションが設定されていて、イベントがアクション実行の対象となった場合に、アクションマーク  (抑止されなかったアクション)、 (抑止されたアクション)、または  (一部抑止されたアクション) が表示されます。</p> <p>また、繰り返しイベントの監視抑止でアクションの実行を抑止している場合にイベントが大量発生したとき、[イベント一覧] 画面に  が表示されます。</p> <p>共通除外条件によってアクションの実行対象外になった場合は  (アクション除外イベント) が表示されます。</p> <p>集約開始イベントと繰り返しイベントのアクション状況が異なる場合、アクション欄に「!」が表示されます。</p>

項目の列幅

表示される項目の列幅は、マウスでドラッグすると任意の幅に変更できます。また、列自体をドラッグして、列の順番を入れ替えることもできます。

重要イベントの背景色

重要イベントの場合、イベント一覧に表示される重大度によって次に示す背景色が付きます。

表 5-3 重要イベントの背景色

重大度	対処状況	背景色
警告／通知／情報／デバッグ	「対処済」以外	黄
エラー		橙
緊急／警戒／致命的		赤
上記以外	「対処済」	白 (背景色なし)

イベントの対処状況

JP1 イベントの対処状況を設定したイベントには、イベント一覧の左端の列に、対処状況とアイコンが表示されます。

対処状況の種類と、その対処状況を示す対処状況マークを次に示します。どのような場合にどの対処状況を設定するか、運用に合わせて決めてください。

表 5-4 対処状況の種類と対処状況マーク

対処状況	対処状況マーク
対処済	
処理中	
保留	
未対処	(無印)

設定した対処状況は、ログインしているマネージャーの統合監視 DB またはイベント DB に記録されます (ほかのホストから転送されてきた JP1 イベントの場合、転送元ホストの統合監視 DB またはイベ

ント DB の情報は変更されません)。そのため、同じマネージャーにログインしている JP1/IM - View の [イベント監視] ページおよび [重要イベント] ページにも反映されます。

画面に表示できるイベント数の上限

画面に表示できるイベント数の上限は 100 件です。JP1 イベントの数が、表示できる JP1 イベントの数の上限を超える場合、最新のイベントから 100 件ずつイベントを表示します。画面を切り替えると 201 件目以降のイベントを順次表示できます。

[イベント一覧] 画面の更新

[イベント一覧] 画面は、一定間隔で新しいイベントが到着していないかインテリジェント統合管理サーバをチェックし、画面を自動更新します。画面は、最新のイベントを表示している場合だけ自動更新されます。過去のイベント（101 件目以降）を表示している場合は自動更新されません。また、更新間隔の変更はできません。

なお、画面を手動で更新した場合は、最新のイベント一覧が表示されます。

状態の絞り込み

[イベント一覧] 画面に一覧表示するイベントを、 [状態絞り込み] ボタンで切り替えます。次に示す状態のイベントを、ボタンの色によって絞り込みできます。

表 5-5 ボタンの色と絞り込まれるイベント

ボタンの色	絞り込まれるイベント	
	重大度	対処状況
黄	警告／通知／情報／デバッグ	「対処済」以外
橙	エラー	
赤	緊急／警戒／致命的	

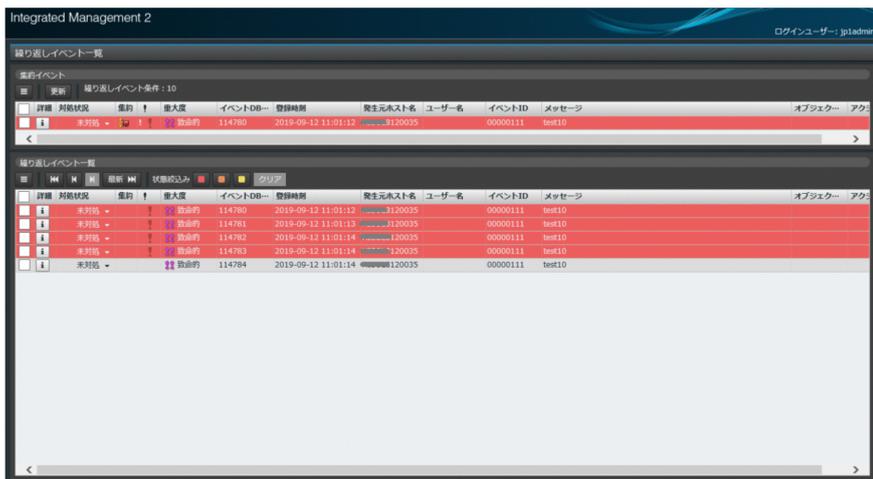
すべてのボタンを一度に選択することもできます。絞り込みを切り替えた場合は、変更後の設定で最新のイベント（100 件）を取得し直し、イベント一覧を更新します。

5.2.2 [繰り返しイベント一覧] 画面を表示する

[繰り返しイベント一覧] 画面は、集約イベントと集約された繰り返しイベントを一覧で表示する画面です。集約イベントの対処状況を、まとめて処理できます。

[繰り返しイベント一覧] 画面を表示するには、集約開始イベントを選択して  [操作メニュー] ボタンの [繰り返しイベント一覧] をクリックします。

図 5-3 「繰り返しイベント一覧」画面の例



「繰り返しイベント一覧」画面に表示される項目については、「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2. [統合オペレーション・ビューアー] 画面」を参照してください。

5.2.3 JP1 イベントの詳細情報を表示する

イベント一覧に表示されている JP1 イベントの詳細な属性情報を表示できます。

詳細情報を表示するには、「イベント一覧」画面のイベント一覧で、属性を表示したい JP1 イベントの ⓘ をクリックします。「イベント詳細」ダイアログが表示されます。

図 5-4 「イベント詳細」ダイアログの例



[イベント詳細] ダイアログには、その JP1 イベントに登録されているイベント属性名と属性値が表示されます。登録されている属性は、その JP1 イベントによって異なります。

選択した JP1 イベントがモニター起動対象のイベントの場合は、[モニター起動] ボタンが活性化します。クリックすると、JP1 イベントに対応するアプリケーションの画面が表示されます。

選択した JP1 イベントが 1 件の場合は、[対処アクション実行 (イベント情報引き継ぎ)] ボタンが活性化します。クリックすると、[対処アクション実行] 画面が表示されます。

詳細情報として表示される項目は、セントラルコンソールのイベント一覧の表示項目と同じです。詳細については「[6.1.1 イベント一覧の表示項目](#)」を参照してください。

5.3 トレンド表示とアラートで扱うメトリックの追加

JP1/IM - Agent のトレンド表示とアラートで扱うメトリックを追加できます。

トレンド表示で扱うメトリックについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.6(3)メトリック一覧の返却」および「3.15.6(4)トレンドデータの返却」、アラートで扱うメトリックについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.15.1(3)パフォーマンスデータの監視・通知機能」を参照してください。

メトリックを追加するための設定手順を、次に示します。

1. Exporter の設定

追加するメトリックを Exporter が収集していない場合、収集するための設定を行います。設定方法は Exporter ごとに異なります。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)(i)Blackbox exporter (外形監視機能)」、[「3.15.1\(1\)\(d\)Node exporter \(Linux 性能情報収集機能\)」](#)、[「3.15.1\(1\)\(c\)Windows exporter \(Windows 性能情報収集機能\)」](#)、および「3.15.1(1)(g)Yet another cloudwatch exporter (Amazon CloudWatch 性能情報収集機能)」で、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。

設定を行ったあと、Exporter を再起動します (Blackbox exporter の場合は、再起動の代わりにリロードを実行してもかまいません)。

2. Prometheus 設定ファイルの編集

Prometheus 設定ファイル (jpc_prometheus_server.yml) のスクレイプ定義で、metric_relabel_configs の設定を変更し、PromQL 文で使用する Exporter のメトリックが削除されないようにします。具体的には、metric_relabel_configs の regex で Exporter のメトリック名を羅列している個所に、Exporter で新たに使用するメトリック名を追加します。すでに追加されている場合は追加不要です。

Yet another cloudwatch exporter で「aws_ec2_network_in_average」メトリックを追加する場合の指定例を、次に示します (下線部分を追加します)。

```
- job_name: 'jpc_cloudwatch'
  . . .
  metric_relabel_configs:
  . . .
    - source_labels: ['__name__', 'jp1_pc_nodelabel']
      regex: '(aws_ec2_network_in_average|aws_ec2_cpuutilization_average|...);.+${'
      action: 'keep'
```

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。

3. アラート設定ファイルの編集 (アラートで扱うメトリックを追加する場合)

アラート設定ファイルのアラートの定義にメトリックを追加し、追加したメトリックを使用した PromQL 文をアラートの条件式に記述します。

アラート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「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。

4. Prometheus server のサービスの再起動またはリロード

Prometheus 設定ファイルおよびアラート設定ファイルを編集したホストの Prometheus server のサービスを再起動、または、リロードします。

5. メトリック定義ファイルの編集 (トレンド表示で扱うメトリックを追加する場合)

メトリック一覧の返却機能では、メトリック定義ファイルに定義されているメトリックを返却します。メトリック定義ファイルは、Exporter ごとに存在します。メトリックを追加したい IM 管理ノードの Exporter を確認し、該当する Exporter のメトリック定義ファイルに、メトリックの定義を追加します。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」の各 Exporter の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。

メトリック定義ファイルを編集したあと、次のどれかの操作を行ったときに、更新したメトリック定義ファイルの情報が反映されます。

- 統合オペレーション・ビューアーで [トレンド] タブを再表示
- 統合オペレーション・ビューアーで [ダッシュボード] を再表示
- JP1/IM - Manager のメトリック一覧取得 API を実行
- JP1/IM - Manager の時系列データ取得 API を実行

5.4 ダッシュボードの見方

ダッシュボードでは、「ノードの状態」、「各種 IT リソースのアラート」、「各種 IT リソースのトレンド情報」、「重要イベントの発生件数」を確認できます。「各種 IT リソースのアラート」、「各種 IT リソースのトレンド情報」、「重要イベントの発生件数」に対しては、ダッシュボードで指定した期間内の情報を表示できます。

ダッシュボードは、IM 管理ノードごとに作成できるため、システム全体を監視するダッシュボードだけでなく、サブシステムやサーバーごとに監視するダッシュボードも作成できます。なお、IM 管理ノードごとにデフォルトで表示される自動生成ダッシュボードをカスタマイズして、ユーザーごとにさまざまなダッシュボードを作成できます。ダッシュボードの作成手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」を参照してください。

図 5-5 ダッシュボードの画面例



1つの画面にノード状態、アラート情報、各種 IT リソースのトレンド情報などを並べて監視できます。

ダッシュボードの画面操作については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」を参照してください。

5.4.1 ダッシュボードを表示する

(1) [ダッシュボード] タブに表示する

[統合オペレーション・ビューアー] 画面を表示すると、[詳細表示] 領域に [ダッシュボード] タブが表示されます。このタブには、[稼働状況] 領域で選択している IM 管理ノードに応じたダッシュボードが表示されます。デフォルトでは、自動生成ダッシュボードが表示されます。

(2) [ダッシュボード一覧] 画面から表示する

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や、新規作成したダッシュボードは、[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] を選択すると、[ダッシュボード一覧] 画面が表示されます。一覧でタイトルをクリックすると、選択したダッシュボードが表示されます。

(3) フルスクリーンで表示する

タブや画面で表示したダッシュボードの操作メニューで、[フルスクリーン表示] をクリックすると、ダッシュボードをフルスクリーンで表示できます。フルスクリーンを解除する場合は、Esc キー、または、ディスプレイ上部へのマウスオーバーで表示される [×] ボタンをクリックします。

(4) Web ブラウザーの別ウィンドウで表示する

タブや画面で表示したダッシュボードの操作メニューで、[別ウィンドウで表示] をクリックすると、Web ブラウザーの別ウィンドウで [ダッシュボード] 画面を表示できます。

(5) Web ブラウザーの別タブやほかの端末の Web ブラウザーで表示する

Web ブラウザーの別タブやほかの端末の Web ブラウザーから、ダッシュボードの URL にアクセスして、[ダッシュボード] 画面を表示できます。

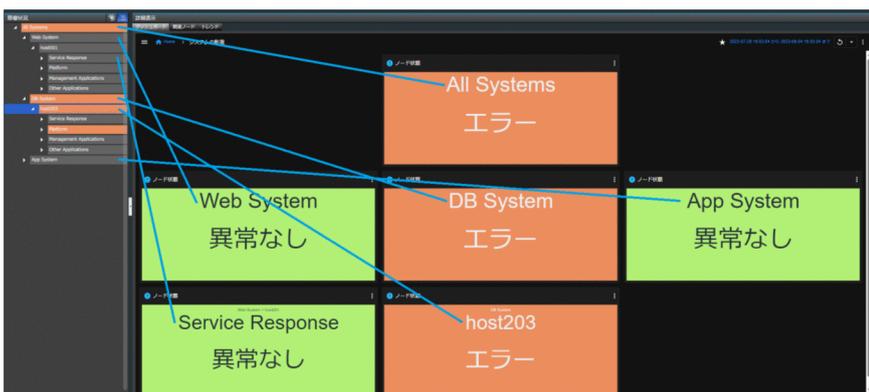
ダッシュボードの URL の取得方法を、次に示します。

1. 統合オペレーション・ビューアーで、対象のダッシュボードを表示する。
2. 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。
3. [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。

5.4.2 IM 管理ノード状態の監視

ダッシュボードでは、ツリーの中で監視したい IM 管理ノードだけを選択し、ダッシュボードに並べて監視できます。

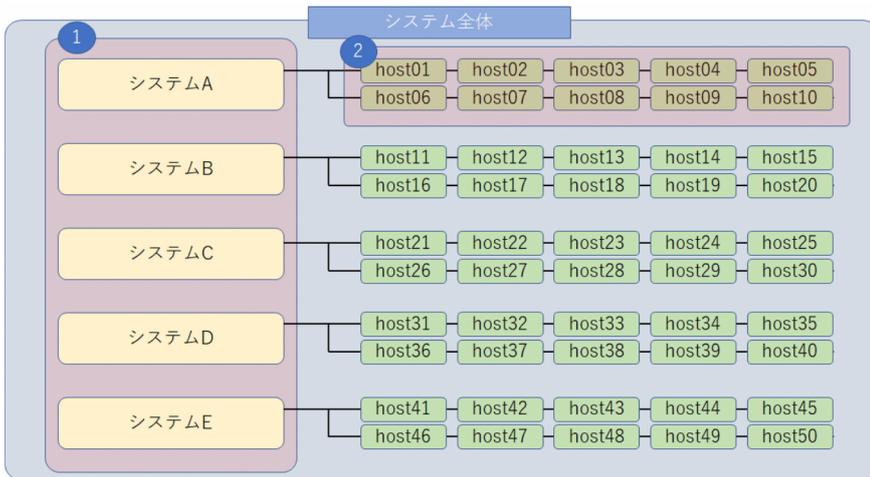
図 5-6 IM 管理ノード状態による監視例



(1) ノード状態パネルによる監視

次に示すシステムの構成の場合に、「①システム全体」を監視する例と、システムの一部の「②システム A」を監視する例を説明します。

図 5-7 システム構成例



システム全体を監視する

ダッシュボードにシステム単位のノード状態監視を指定し、「システム A」、「システム B」、「システム C」、「システム D」、「システム E」のノードを監視するパネルを定義するとシステム全体の状態を把握できます。



システム A を監視する

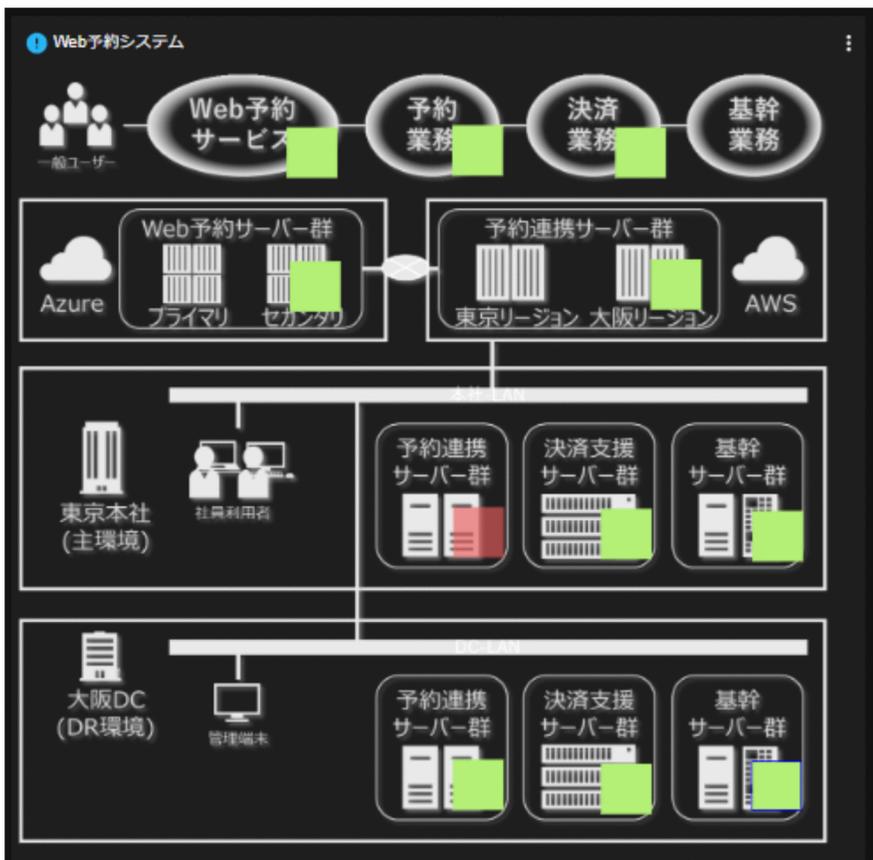
ダッシュボードにホスト単位のノード状態監視を指定し、「host01」から「host10」のノードを監視するパネルを定義すると、システム A の状態を把握できます。



(2) ノード状態マップによる監視

ノード状態マップによる監視では、背景画像を指定して背景画像上にノードの状態を表示できます。次の例では緑や赤の小さな四角のステータスアイコンでノードの状態を確認できます。

図 5-8 ノード状態マップによる監視例

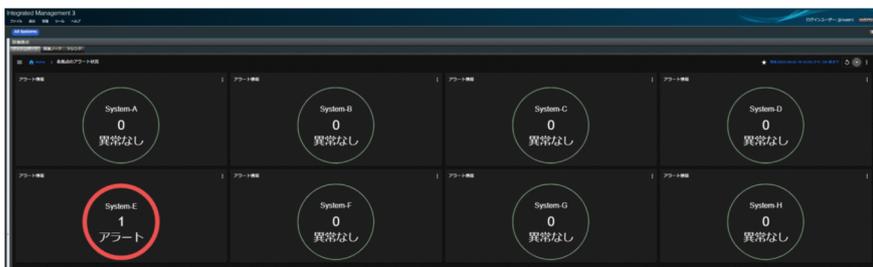


5.4.3 アラート情報の監視

JP1/IM - Agentでは、各種 IT リソースのパフォーマンスデータに対してしきい値監視ができます。ダッシュボードでは、しきい値を超過し、アラート通知が「firing」の状態の件数を、アラート情報として表示できます。複数のアラートが発生している場合は、数字が加算されて表示されます。

ダッシュボードの [アラート情報] パネルでは、任意の IM 管理ノードごとに、その配下で発生しているアラートの件数を確認できます。

図 5-9 アラート監視例

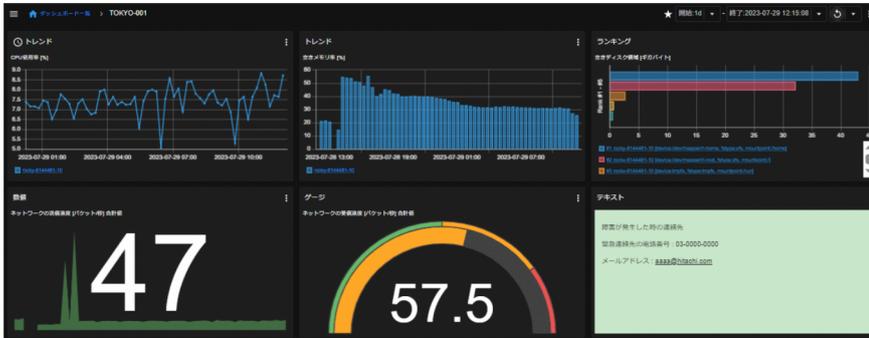


5.4.4 各種 IT リソースの確認

各種 IT リソースの情報をビジュアルに確認できます。

表示形式は、折れ線グラフ、棒グラフ、数値、ゲージ、ランキング形式から選択できます。

図 5-10 各種 IT リソースの表示例

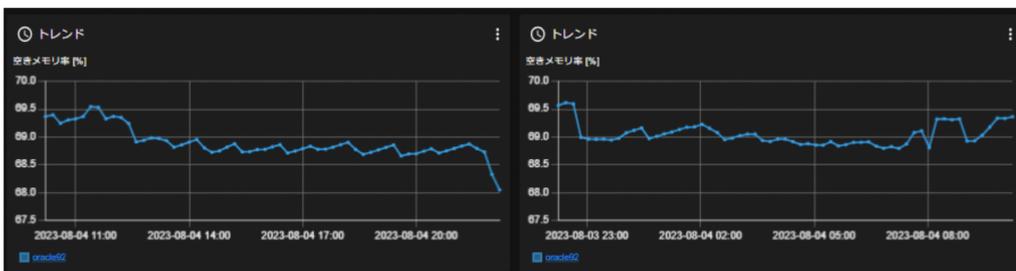


表示形式は、データの特徴や視認性を考慮して選択してください。対象メトリックは、OS のパフォーマンス情報、URL や ICMP での外形監視情報、クラウド監視情報、コンテナ監視情報など、JP1/IM - Agent の性能監視で収集されるメトリックと、JP1 イベントの件数（重要イベントの件数）です。

IT リソースで異常を検知した場合には、ダッシュボードで該当ホストの各種 IT リソース情報を確認すること、発生時刻前後の状況を把握することができます。

また、直近の状況だけでなく、過去の状況を並べて表示することができるので、今日だけ急に異常となったのか、前から徐々に異常に近づいたかの確認もできます。

図 5-11 右側に過去の状況のグラフを表示した例



5.4.5 ダッシュボードを起点とした問題調査・対処の流れ

ダッシュボードを使用した場合の監視から調査に至るまでの運用作業の流れについて、説明します。

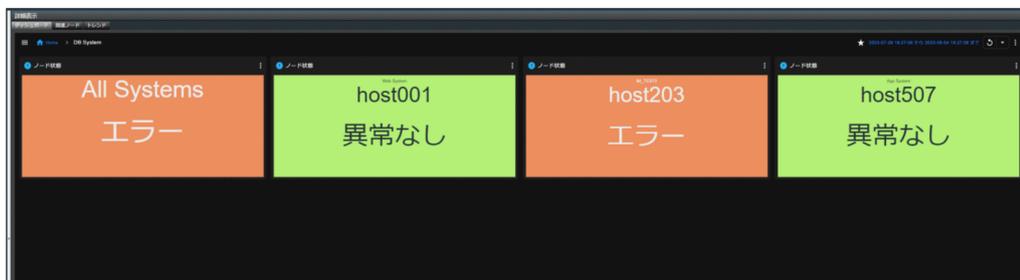
(1) IM 管理ノード状態監視からの一連の操作

[ノード状態] パネルは、IM 管理ノードの単位で監視できます。

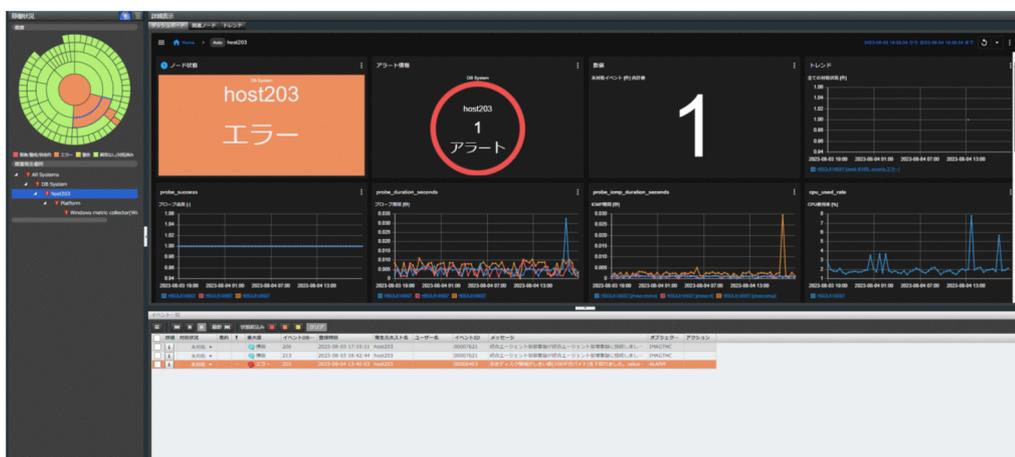
例えば、システム全体が8つのシステムから構成されるような場合、ダッシュボードでシステム単位にノード状態監視を8つ定義すると、システム全体を監視できます。

監視する際の手順を次に示します。

1. 監視を開始します。
2. 異常が発生すると、該当システムのパネルの色が変化します。



3. 色が変わった該当パネルをクリックすると、ツリー上のIM管理ノードが選択状態になります。



4. [イベント一覧] 画面には、該当するIM管理ノード配下のイベントだけにフィルタリングされます。
5. イベント一覧の中から、該当イベントの「イベント詳細」のメッセージを確認し、要因を特定して調査します。

属性名	属性値
イベントDB内通し番号	255
イベントID	00000403
発行元プロセスID	0
登録時刻	2023-08-04 13:40:03
到着時間	2023-08-04 13:40:03
発行元ユーザーID	-1
発行元グループID	-1
発行元ユーザー名	root
発行元グループ名	
発生元ホスト名	host203
発行元イベントサーバ名	host708
発行元IPアドレス	10.164.205.232
発行元イベントDB内通し番号	255
重大度	エラー
プロダクト名	/HITACHI/JP1/JPCS2
オブジェクトタイプ	ALARM
オブジェクト名	disk_unused(Windows exporter)
事象種別	NOTICE
アラートの発火日時	2023-08-04 13:39:58
監視エージェントのホスト名	host203
スクレイプジョブ	jpc_windows
jp1_pc_nodelabel	Windows metric collector(Windows exporter)
Exporter名	JPC Windows exporter
メトリック名	windows_logical_disk_free_bytes
コンポーネント名	/HITACHI/JP1/JPCS/CONFINFO
メッセージ	空きディスク領域がしきい値(100千バイト)を下回りました。 value=84.08203125千バイト, volume=C:

6. 要因が OS リソースやプロセスパフォーマンスに関係するものであれば、ダッシュボードで OS リソースなどをトレンド解析し、原因を調査します。



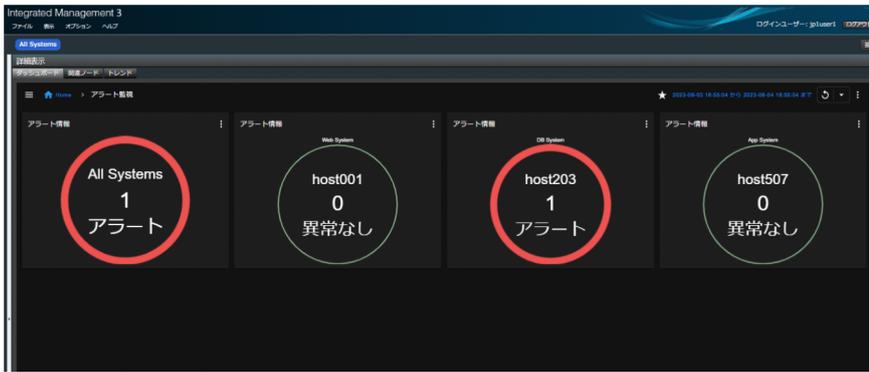
(2) アラート情報監視からの一連の操作

アラート情報は、IM 管理ノードの単位であるシステムやホスト単位などで監視できます。

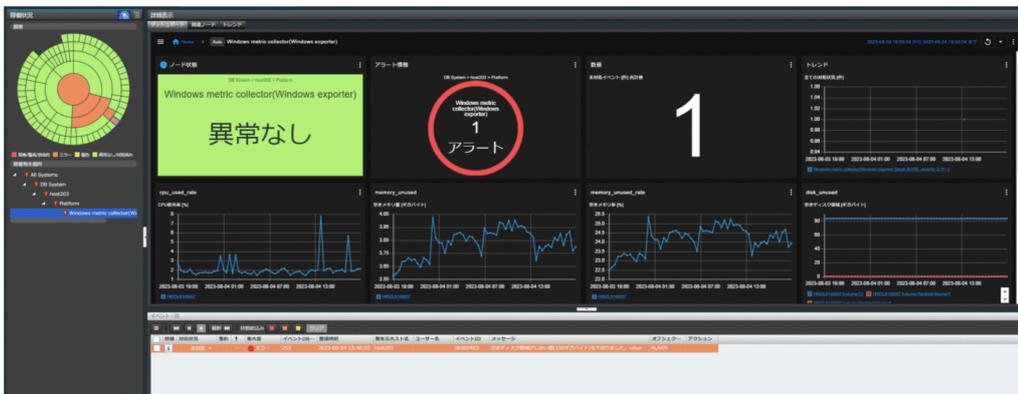
例えば、あるシステムが 16 個のホストから構成されるような場合、ダッシュボードでホスト単位にアラート情報監視を定義すると、システムのアラート情報を監視できます。

監視する際の手順を次に示します。

1. 監視を開始します。
2. アラートが発生すると、該当ホストのアラートパネルの色が変化し、発生しているアラートの数も表示されます。



3. 色が変わった該当パネルをクリックすると、IM 管理ノードと発生しているアラートの一覧が表示され、発生時刻も確認できます。表示された IM 管理ノードをクリックすると、ツリーの選択状態に変わります。



4. [イベント一覧] 画面には、該当する IM 管理ノード配下のイベントだけにフィルタリングされます。
5. イベント一覧の中から、アラート発生時刻を元に該当イベントの「イベント詳細」のメッセージを確認し、要因を特定して調査します。

属性名	属性値
イベントDB内通し番号	255
イベントID	00000403
発行元プロセスID	0
登録時刻	2023-08-04 13:40:03
到着時間	2023-08-04 13:40:03
発行元ユーザーID	-1
発行元グループID	-1
発行元ユーザー名	root
発行元グループ名	
発生元ホスト名	host203
発行元イベントサーバ名	host708
発行元IPアドレス	10.164.205.232
発行元イベントDB内通し番号	255
重大度	エラー
プロダクト名	/HITACHI/JP1/JPCS2
オブジェクトタイプ	ALARM
オブジェクト名	disk_unused(Windows exporter)
事象種別	NOTICE
アラートの発火日時	2023-08-04 13:39:58
監視エージェントのホスト名	host203
スクレイプジョブ	jpc_windows
jp1_pc_nodelabel	Windows metric collector(Windows exporter)
Exporter名	JPC Windows exporter
メトリック名	windows_logical_disk_free_bytes
コンポーネント名	/HITACHI/JP1/JPCS/CONFINFO
メッセージ	空きディスク領域がしきい値(100千バイト)を下回りました。 value=84.08203125千バイト, volume=C:

6. 要因が OS リソースやプロセスパフォーマンスに関係するものであれば、ダッシュボードで OS リソースなどをトレンド解析し、原因を調査します。

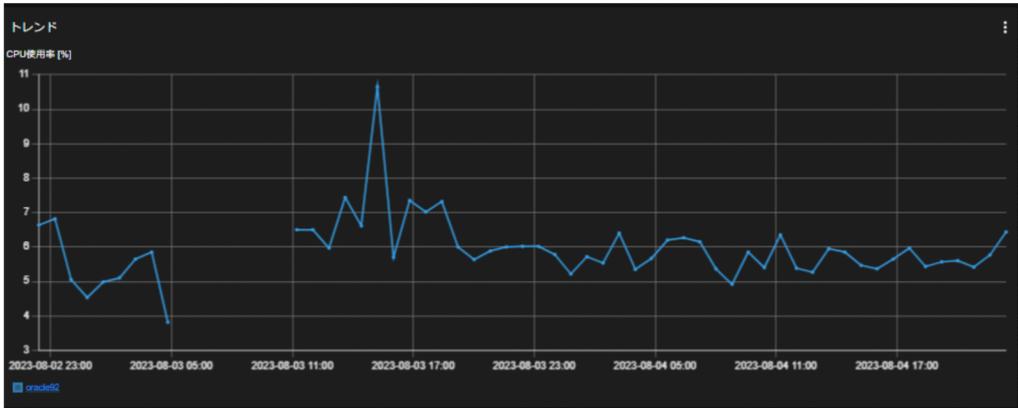


5.4.6 注意事項

- JP1 ユーザーを削除する場合は、その JP1 ユーザーで作成したダッシュボードを事前に削除してください。JP1 ユーザーを削除してもダッシュボードは自動的に削除されません。JP1 ユーザーがすでに存在しない場合は、再度 JP1 ユーザーを作成し、その JP1 ユーザーで作成したダッシュボードを削除してください。
- ダッシュボードのトレンドパネルのグラフの縦軸は、表示する範囲のデータの内容によって最小値と最大値が動的に変化します。連続して監視しているときでも縦軸の最小値と最大値が変わるため、注意してください。

最小値と最大値を固定したい場合は、パネルの設定時に「最小値」と「最大値」を設定してください。特に、過去との比較では 2 つのグラフの縦軸の最小値と最大値が異なるため、注意が必要です。同じスケールで比較したい場合は、両方に同じ最小値と最大値を指定してください

- ダッシュボードで表示できるメトリックデータの期間は、トレンドデータ管理DBで保存されている期間となります。
- メトリックのデータが一つも存在しない場合は、パネルに「NO DATA」と表示されます。
- 監視対象の停止などによって一時的にパフォーマンスデータを収集できなかった場合は、次のようにグラフの線が途切れた状態で表示されます。



5.5 他製品との連携の見方

インテリジェント統合管理基盤では、連携した他製品のデータを統合オペレーション・ビューアーで監視できます。

5.5.1 予兆によって障害を回避する (JP1/AJS 連携)

JP1/AJS の負荷の増大など業務障害の予兆をイベント通知で確認し、障害を回避する場合の手順を説明します。

1. [イベント一覧] で予兆を通知されたイベントの [詳細] ボタンをクリックする。
[イベント詳細] ダイアログが表示されます。
2. イベントガイド情報と [メッセージ] を確認する。
3. [トレンド] タブでスケジューラーサービスの稼働状況を確認する。
選択したイベントのトレンド情報のグラフが表示されます。
4. [[+] ノード追加] ボタンをクリックして、ジョブの実行先ホストの性能情報を持つノードを選択する。
ジョブの実行先ホストの性能情報のグラフが表示されます。
5. 手順 3. で表示したグラフと、手順 4. で表示したグラフを比較する。
トレンドの比較によって、影響範囲や障害の要因を切り分けます。
6. 障害の要因の切り分けの結果から、担当者に障害を回避する作業指示をする。

5.5.2 ジョブの運用中に発生した問題の影響範囲を把握し対処する (JP1/AJS 連携)

ジョブの運用中に発生した問題の原因と影響範囲を把握する場合の手順を示します。

1. [稼働状況] 領域で問題発生個所をクリックする。
問題発生個所は、サンバーストまたはツリー上に赤色、橙色、黄色で表示されます。
2. [業務フロー] タブに、クリックしたルートジョブネットの次の情報が表示される。
 - 先行ルートジョブネット、後続ルートジョブネットとの関連
 - 後続ルートジョブネットへの影響有無
 - 発生中のイベント一覧
3. ノードの前に表示されたアイコンをクリックして、[連携ユニット] ダイアログを表示する。
影響がある後続ユニットとその開始予定日時を確認します。

4. 後続ユニットのリンクをクリックして JP1/Web Console のモニター画面を起動する。
影響がある後続ユニットに対して、対処します。

5.5.3 ジョブの定義や内容を変更する場合に影響を受けるルートジョブネットワークを事前に把握する (JP1/AJS 連携)

ジョブの定義や内容を変更する場合に、影響を受けるルートジョブネットワークを事前に把握する手順を示します。

1. 変更予定のルートジョブネットワークをクリックする。
2. [ジョブフロー] タブ, [関連ノード] タブを確認する。
変更予定のルートジョブネットワークに関連するノードが表示されます。
3. 表示されたルートジョブネットワーク名, [プロパティ] の情報を参照し, 影響の有無や影響内容を把握する。

5.5.4 性能情報を確認して対処する (JP1/PFM 連携)

ジョブ異常終了の要因がインフラにあるか判断するため, 関連するインフラのステータスを確認する手順を示します。

1. [稼働状況] 領域で問題発生個所をクリックする。
問題発生個所は, サンバーストまたはツリー上に赤色, 橙色, 黄色で表示されます。
2. [関連ノード] タブで, ジョブの実行先エージェントを確認する。
関連ノードの階層を展開し, ジョブの実行先エージェントを確認します。
3. [トレンド] タブで実行先エージェントのノードを追加し, 性能情報のグラフを表示する。
実行先エージェントのイベントを確認します。
4. [パフォーマンス] タブを開く。
該当するメトリックに関連するレポートを選択し, リソースの使用率が高いプロセスを特定して対処します。
JP1/PFM の [カスタム UI] 画面については, JP1/PFM バージョン 12-10 以降のマニュアルの JP1/PFM - Web Console についての説明を参照してください。

5.5.5 提案を確認して対処する

提案機能でシステムの異常に対処する場合の手順を示します。

1. [稼働状況] 領域で問題発生個所を確認する。

問題発生個所は、サンバーストまたはツリー上に赤色、橙色、黄色で表示されます。

2.  アイコンが表示された IM 管理ノードをクリックする。

[提案] タブに提案の一覧が表示されます。

3. [提案] ボタンをクリックする。

問題に対して対処できる [提案バー] が、活性化します。

4. [提案バー] をクリックし、[提案詳細] 領域で提案の説明や前回実行履歴などを確認する。

条件の詳細を確認する場合は、[条件詳細表示] ボタンをクリックします。[条件詳細] 画面が表示され、提案の活性条件を確認できます。

5. [実行] ボタンをクリックする。

対処アクションが実行されます。ボタン名は [実行中] に変わります。

6. 対処アクションの完了を確認する。

ボタン名が [実行] に変わります。イベントの自動アクションのメールを通知によって、対処アクションの終了を確認することもできます。

- 対処アクションの実行が完了したあとに、もう一度 [提案] ボタンをクリックすると、対処アクションを実行したことによってシステム状況が変わっているため、活性化されていた提案一覧が非活性で表示されます。
- 提案定義ファイルで、システムが正常化した際にイベントを対処済みにする対処アクションを定義していた場合は、その提案が活性化します。
- イベントを対処済みにする対処アクションが定義された提案を実行した場合は、イベントが対処済みになることでノードのステータスが「異常なし」に変更されます。もう一度 [提案] ボタンをクリックすると、提案一覧がすべて非活性で表示されます。

 **重要**

- 同じ IM 管理ノードかつ同じ提案 ID の対処アクションを同時に実行することはできません。
- 対処アクションの実行中に `jddupdatesuggestion` コマンド、または `jddupdatetree` コマンドを実行した場合でも、対処アクションは途中で終了しません。このため、IM 管理ノードや提案定義を参照する対処アクションが失敗する場合があります。
- 対処アクションの実行中に JP1 ユーザーを削除、または JP1 ユーザー権限を変更・削除した場合、JP1 ユーザーの情報を使用するコマンド実行、プラグイン共通メソッド、REST API が失敗し、対処アクションが失敗する場合があります。
- 対処アクション実行中に JP1/IM - Manager サービスを停止すると、対処アクションが終了するまで JP1/IM - Manager サービスを停止しないため、サービスの停止に時間がかかる場合があります。対処アクションで時間のかかる REST API やコマンドを実行する場合は、非同期で処理する必要があります。

- 対処アクション実行開始直後に JP1/IM - Manager サービスを停止すると、次の種別の対処アクションは失敗するおそれがあります。
 - plugin (JP1 イベント関連の共通メソッドを使用している場合)
 - eventStatus

また、サービス停止中に JP1/IM の REST API を実行すると、ステータスコード「500」が返却されます。これによって、対処アクションが失敗する場合があります。

5.5.6 OIDC 認証している外部製品と連携してシングルサインオンする

OIDC 認証している外部製品と、シングルサインオン連携している場合の手順を示します。

(1) 他のサービスの Web コンソール画面を呼び出す

1. OpenID プロバイダによる認証で、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] 画面が表示されます。
2. [イベント一覧] 領域で、他のサービスが管理するイベントをクリックする。
3. OpenID プロバイダの認証画面を経由せずに、他のサービスの Web コンソール画面が表示される。

(2) 他のサービスから [統合オペレーション・ビューアー] 画面を呼び出す

1. OpenID プロバイダによる認証で、他のサービスにログインする。
2. 他のサービスから [統合オペレーション・ビューアー] 画面を起動する。
3. インテリジェント統合管理基盤のログイン画面を経由せずに、[統合オペレーション・ビューアー] 画面が表示される。

(3) 他のサービスから OpenID プロバイダによる認証済みの認証情報を付与して、JP1/IM の REST API を発行する

1. OpenID プロバイダによる認証で、他のサービスにログインする。
2. ログインする際の認証情報を付与した Rest API を発行する。

5.5.7 ダイレクトアクセス URL で情報を共有する

[統合オペレーション・ビューアー] 画面で [イベント詳細] ダイアログを確認するための URL を、自動アクションで担当者 (userA) にメール通知する場合を例に、特定のノードに対する情報を他のユーザーと共有する手順を説明します。

1. 自動アクションで送信するメールを定義する。※

メールは次のように定義します。

送信元 (From) : admin@xxxxx.com

送信先 (To) : userA@xxxxx.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](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)

2. システムで異常が発生し、自動アクションによって担当者 (userA) にメールが送信される。

3. 担当者 (userA) は、メール本文のダイレクトアクセス URL をクリックする。

イベント DB 内通し番号が指定されているメール内 URL で、[統合オペレーション・ビューアー] 画面にアクセスします。

4. [イベント詳細] ダイアログを開いた状態で [統合オペレーション・ビューアー] 画面が表示される。

注※

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、メール定義例の「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) は、http を https にしてください。

5.6 インテリジェント統合管理基盤の運用上の注意事項

インテリジェント統合管理基盤の運用上の注意事項を次に示します。

5.6.1 JP1/AJS と連携した場合の注意事項

- `jddcreatetree` コマンドは、JP1/AJS3 - Manager ホストでジョブを実行していない時間帯に実行してください。ジョブの実行中に `jddcreatetree` コマンドを実行した場合、両方の処理の負荷が同時にかかることにより、それぞれの処理が遅延する可能性があります。

ジョブを実行しない時間帯がない場合は、ジョブ実行量が少ない時間帯に `jddcreatetree` コマンドを実行し、業務に与える影響が少なくなるよう検討してください。また、事前に開発環境で十分に検証し、それぞれの処理に問題が発生しないことを確認してください。

- `jddcreatetree` コマンドで、各 JP1/AJS3 - Manager ホストから情報を取得できる時間は最大 60 分です。60 分を超えた場合、タイムアウトが発生し情報を取得することはできません。情報取得に 60 分以上かかりタイムアウトした場合、JP1/AJS3 - Manager ホストでは情報取得処理を行うアダプタコマンドのプロセス「`IMDDAdapter_HITACHI_JP1_AJS3`」が動作し続けている可能性があります。

アダプタコマンドは二重実行不可のため、再度情報を取得する場合は JP1/AJS3 - Manager ホスト上で次に示す方法によって「`IMDDAdapter_HITACHI_JP1_AJS3`」プロセスを強制終了する必要があります。

Windows の場合

タスクマネージャーを使用して強制終了する

UNIX の場合

`kill` コマンドを使用して強制終了する

その後、情報取得時間が 60 分以下になるようユニット構成や実行登録済みのジョブネット数を調整し、再度 `jddcreatetree` コマンドを実行してください。

- `jddcreatetree` コマンドで取得するユニット情報のうち、次のユニットは対象外です。
 - マネージャージョブグループ
 - マネージャージョブネット
 - リカバリーマネージャージョブネット
 - リモートジョブネットおよびその配下のユニット
 - リカバリーリモートジョブネットおよびその配下のユニット
 - 実行先サービスに「キューレス」を指定した JP1 イベント送信ジョブ、および待ち合わせ条件付きユニット
 - ルートジョブネットと同じ階層に定義された JP1 イベント受信監視ジョブおよび JP1 イベント送信ジョブ
 - 実行登録されていないルートジョブネットおよびその配下のユニット

- JP1/AJS3 - Manager ホストで実行中のアダプタコマンドは、JP1/IM - Manager ホストからは実行をキャンセルできません。キャンセルする場合は JP1/AJS3 - Manager ホスト上で次の方法を使って「IMDDAdapter_HITACHI_JP1_AJS3」プロセスを強制終了してください。

Windows の場合

タスクマネージャーを使用して強制終了する

UNIX の場合

kill コマンドを使用して強制終了する

- JP1/AJS3 - Manager ホストから情報を取得できるユニット数は、一つの JP1/AJS3 - Manager ホストあたり 40 万です。40 万ユニットを超えている場合、jddcreatetree コマンドはメッセージ KAJY04260-E を出力して失敗し、構成管理ツリーは更新されません。ユニット数は JP1/AJS3 - Manager ホスト上で次のコマンドを実行して見積もることができます。

Windows の場合

次に示すコマンドを実行して得られた行数の合計

```
ajsname -F スケジューラーサービス名 -R -E "/"
```

```
ajsname -F スケジューラーサービス名 -R -G "/"
```

UNIX の場合

次に示すコマンドを実行して得られた行数の合計

```
/opt/jp1ajs2/bin/ajsname -F スケジューラーサービス名 -R -E "/"
```

```
/opt/jp1ajs2/bin/ajsname -F スケジューラーサービス名 -R -G "/"
```

- JP1/AJS3 - Manager ホストで、環境設定パラメーター「ADMACLIMIT」を「yes」にしている場合、jddcreatetree コマンドによる情報取得が失敗する可能性があります。次の対処方法に従って情報を取得できるようにしてから運用してください。

Windows の場合

環境設定パラメーター「ADMACLIMIT」を「no」に設定するか、パラメーターを削除して機能を無効にしてください。または JP1/AJS3 - Manager ホストで、「system」という名前の JP1 ユーザーを登録し、次に示す JP1 権限レベルのどれかを設定してください。

- JP1_AJS_Admin 権限
- JP1_AJS_Manager 権限
- JP1_AJS_Editor 権限
- JP1_AJS_Operator 権限
- JP1_AJS_Guest 権限

UNIX の場合

環境設定パラメーター「ADMACLIMIT」を「no」に設定するか、パラメーターを削除して機能を無効にしてください。または JP1/AJS3 - Manager ホストで、スーパーユーザーを JP1 ユーザーとして登録し、次に示す JP1 権限レベルのどれかを設定してください。

- JP1_AJS_Admin 権限
- JP1_AJS_Manager 権限

- ・ JP1_AJS_Editor 権限
 - ・ JP1_AJS_Operator 権限
 - ・ JP1_AJS_Guest 権限
- `jddcreatetree` コマンドで取得する、ユニット名、ユニット定義内容、実行エージェント名、JP1 資源グループ名などの情報に制御文字が含まれている場合、情報取得が失敗する可能性があります。取得する情報には、制御文字を含めないようにして運用してください。
 - トレンド情報取得先の JP1/AJS3 マネージャーホストでシステム時刻が過去に戻された※場合、システム時刻の戻りによって稼働状況ログファイルに重複して記録された日時と、トレンド情報表示期間の開始または終了に指定した日時が重なると、稼働状況ログファイル内の重複したレコードが一部だけ表示されるときがあります。その場合、次のどちらかの方法で回避できるときがあります。
 - 時間を空けてから再度表示する
 - 期間を変更して再度表示する

上記の回避策を実施しても正しく出力されない場合は、次に示す方法を実施してください。

- トレンド情報取得先の JP1/AJS3 マネージャーホスト上で `ajsreport` コマンドを実行してください。トレンド情報のメトリックと `ajsreport` コマンドの稼働状況レポートに出力される項目の一覧は、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「2.7.1 JP1/AJS から取得できるメトリック」を参照してください。
- 稼働状況ログファイルの削除を検討してください。稼働状況ログファイルの削除には、トレンド情報取得先の JP1/AJS3 マネージャーホストのスケジューラーサービスを停止する必要があります。詳細は、JP1/Automatic Job Management System 3 のマニュアルを参照してください。

注※ トレンド情報表示機能の前提条件を満たしていない場合、またはトレンド情報取得先の JP1/AJS3 マネージャーホストで JP1/AJS3 サービス停止中にシステム時刻が過去に戻された場合が該当します。JP1/AJS3 サービス停止中にシステム時刻を過去に戻す場合は、マニュアル「JP1/Automatic Job Management System 3 運用ガイド」を参照し、稼働状況ログファイルを削除してください。

- `jddcreatetree` コマンドで情報を取得する対象の JP1/AJS3 - Manager ホストが 12-50 以降の場合、`jddcreatetree` コマンドを実行する前に、情報取得対象の JP1/AJS3 - Manager ホストで、ジョブ実行先のエージェントホスト名が正しく名前解決できるようにしておいてください。

5.6.2 ユーザーフィルターを使用する場合の注意事項

ユーザーフィルターを設定している際に、[統合オペレーション・ビューアー] 画面で次の操作を行った場合、イベント一覧を表示するためのイベント取得に時間が掛かることがあります。

- IM 管理ノードを選択したとき
- [イベント一覧] 領域のツールバーのボタンを使用して、イベント一覧を更新したとき

この場合、イベント取得を一定の検索回数で中断し、中断までに取得したイベントが [イベント一覧] 領域に表示されます。

イベント取得を中断するまでの検索回数の上限については、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.settings.eventSearchCount` プロパティで変更できます。イベント取得を中断するまでの時間を短縮する場合は、検索回数の上限值を小さくしてください。イベント取得を中断するまでの時間を長くする場合は、検索回数の上限值を大きくしてください。イベント検索を中断しない場合は、検索回数上限値に `0` を指定してください。

なお、インテリジェント統合管理基盤で参照・操作できるイベントの制限は、ユーザーフィルターではなく、システムノード定義ファイル (imdd_systemnode.conf) や業務グループを使用する運用を推奨します。

`jp1.imdd.gui.settings.eventSearchCount` 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、システムノード定義ファイル (imdd_systemnode.conf) の詳細については、「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。

6

セントラルコンソールによるシステムの監視

この章では、JP1/IM - View を使用して JP1 イベントを監視する手順について説明します。

6.1 JP1 イベントの見方

受信した JP1 イベントは、[イベントコンソール] 画面に表示されます。[イベントコンソール] 画面は、JP1/IM - Manager (セントラルコンソール) にログインすると表示されます。

[イベントコンソール] 画面の表示例を次に示します。

図 6-1 [イベントコンソール] 画面 ([イベント監視] ページ) の表示例

重大度	登録時刻	登録ホスト名	ユーザー名	イベントID	メッセージ	オブジェクト
情報	04/27 15:07:23	host		00000230	ノードが開始しました。	
エラー	04/27 15:07:23	host		00000130	Virus Detected!!	
情報	04/27 15:07:23	host		00000200	ジョブネット(統合業務)を開始します。	
情報	04/27 15:07:23	host		00000210	ジョブ(RWSジョブ)が正常終了しました。	
情報	04/27 15:07:23	host		00000220	ジョブ(ファイル転送ジョブ)が正常終了しました。	
通知	04/27 15:07:23	host		00000300	CPU負荷がしましV値を越えました。	
警告	04/27 15:07:23	host		00000400	不審行為検出。セキュリティホール4003がヒットしま...	
情報	04/27 15:07:23	host		00000240	ジョブ(R2ジョブ)が正常終了しました。	
情報	04/27 15:07:23	host		00000250	ジョブ(RP本店ジョブ)が正常終了しました。	
警告	04/27 15:07:23	host		00000410	ディスク容量が不足しています。	
エラー	04/27 15:07:23	host		00000140	ジョブ(UNIX本店ジョブ)が異常終了しました。	
情報	04/27 15:07:23	host		00000260	業務(商品発注件数3857/3857件)が完了しました。	
情報	04/27 15:07:23	host		00000270	バックアップ(本店売上データ)が正常終了しました。	
警告	04/27 15:07:23	host		00000420	自作のプログラムが実行されています。	
致命的	04/27 15:07:23	host		00000500	アプリケーションが異常終了しました。	
警告	04/27 15:07:23	host		00000600	SSD、PROCESSに異常が発生しています。	
緊急	04/27 15:07:23	host		00000700	サービスを停止しました。	
情報	04/27 15:07:23	host		00000200	ジョブネット(統合業務)を開始します。	
情報	04/27 15:07:23	host		00000210	ジョブ(RWSジョブ)が正常終了しました。	
情報	04/27 15:07:23	host		00000220	ジョブ(ファイル転送ジョブ)が正常終了しました。	

[イベントコンソール] 画面には、ログインしているマネージャーのイベント DBに登録されている JP1 イベントが表示されます。新しい JP1 イベントはイベント一覧の下に追加されます。到着日時が最も新しい JP1 イベントが、イベント一覧の最も下に表示されます。

メモ

[イベントコンソール] 画面に表示されるイベント一覧のスナップショットを CSV ファイルに保存できます。CSV ファイルに保存したい場合は、[イベントコンソール] 画面で [ファイル] - [表示イベントを保存] を選択して保存してください。

また、JP1 イベントの情報やアクションの実行結果などについて、選択した部分の情報を CSV 形式でクリップボードにコピーできます。CSV 形式でクリップボードにコピーできる情報や、機能を使用できる画面については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.15.3 JP1 イベントの情報やアクションの実行結果などをクリップボードにコピー」を参照してください。

6.1.1 イベント一覧の表示項目

イベント一覧には、JP1 イベントの属性、および対処状況が表示されます。イベントの属性として、基本属性、共通の拡張属性、および固有の拡張属性を表示できます。

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と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。

また、[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)』および「警告 (Warning)」のイベントです。

重大度変更機能を使用して重大度を変更した場合、変更後の重大度でイベントの背景色を設定します。

なお、重大度変更機能は、統合監視 DB を使用する場合に設定できます。

統合監視 DB を設定する方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.4.2 統合監視 DB の設定 (Windows の場合)」、[2.4.2 統合監視 DB の設定 (UNIX の場合)」を参照してください。

重大度変更機能を設定する方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「5.13 重大度変更機能の設定」を参照してください。

ログアウト時の各表示項目の列幅を保存するかどうか、および特定のイベントに背景色を付けるかどうかは、[ユーザー環境設定] 画面で設定できます。[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。

(1) JP1 イベントの基本属性、共通の拡張属性、および固有の拡張属性

イベント一覧には、各イベントの属性（基本属性、共通の拡張属性、または固有の拡張属性）が表示されます。デフォルトでは、重大度、登録時刻、登録ホスト名、ユーザー名、イベント ID、メッセージ、オブジェクトタイプ、およびアクションが表示されています。イベント一覧の表示項目は、[ユーザー環境設定] 画面で変更できます。表示項目の変更方法については、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。

イベント一覧に表示できる項目（列）は、イベント属性のうち、次のものです。

表 6-1 イベント一覧の表示項目

属性	説明
対処状況表示項目	JP1 イベントの対処状況を示す情報（対処済、処理中、保留、未処理）が表示されます。集約イベントの対処状況と、繰り返しイベントの対処状況が異なる場合には、「!」が表示されます。
集約状態	繰り返しイベントの監視抑止または繰り返しイベントの集約表示を使用している場合にだけ表示され、集約イベントの繰り返し回数が表示されます。 集約中イベントの場合は、集約中であることを示す「+」が、繰り返し回数後ろに表示されません。

属性	説明
重大度	JP1 イベントの緊急性を示します。緊急性の高い順に、次の値があります。「緊急 (Emergency)」, 「警戒 (Alert)」, 「致命的 (Critical)」, 「エラー (Error)」, 「警告 (Warning)」, 「通知 (Notice)」, 「情報 (Information)」, 「デバッグ (Debug)」 なお、統合監視 DB を使用する場合に、重大度変更機能で重大度を変更したときは、変更したあとの JP1 イベントの緊急性を表します。
登録時刻	イベント発行元ホストのイベント DB に JP1 イベントが登録された時刻です。
登録ホスト名	JP1 イベントを登録したエージェント名 (発行元イベントサーバ名) です。
ユーザー名	JP1 イベント発行元のユーザー名です。
イベント ID	発行元のプログラムや、発生した事象を表す値です。
メッセージ	JP1 イベントの内容を表すメッセージテキストです。
オブジェクトタイプ	イベント発行の契機となる事象が発生したオブジェクトの種類を表す「JOB」, 「JOBNET」などの文字列です。
アクション	自動アクションが設定されていて、イベントがアクション実行の対象となった場合に、アクションマーク  (抑止されなかったアクション),  (抑止されたアクション), または  (一部抑止されたアクション) が表示されます。 また、繰り返しイベントの監視抑止でアクションの実行を抑止している場合にイベントが大量発生したとき、[イベントコンソール] 画面に  が表示されます。 繰り返しイベントの監視抑止、または繰り返しイベントの集約表示でイベントを集約して表示している場合、集約イベントのアクション状況と、繰り返しイベントのアクション状況が異なるときには、「!」が表示されます。 共通除外条件によってアクションの実行対象外になった場合は  (アクション除外イベント) が表示されます。
プロダクト名	JP1 イベントを発行したプログラムの名称です。
オブジェクト名	イベント発行の契機となる事象が発生したオブジェクト (ジョブ, ジョブネットなど) の名称です。
登録名タイプ	オブジェクトの種別です。通常はオブジェクトタイプと同じですが、ジョブネットとジョブのように階層のある業務の場合は、最上層のオブジェクトの種別が表示されます。
登録名	オブジェクトの名称です。通常はオブジェクト名と同じですが、ジョブネットとジョブのように階層のある業務の場合は、最上層のオブジェクトの名称が表示されます。
到着時刻	接続しているマネージャーのイベント DB に JP1 イベントが到着した時刻です。 [イベント検索] ページの場合は、検索対象ホストのイベント DB に登録された時刻です。
開始時刻	実行を開始した時刻をビューアーのタイムゾーンで表示します。
終了時刻	実行を終了した時刻をビューアーのタイムゾーンで表示します。
事象種別	オブジェクトに対して起こった事象 (実行開始, 定義作成など) を表示します。
イベント DB 内通し番号	発行元に関係なくこのイベントサーバに到達した順番です。
発行元プロセス ID	発行元アプリケーションプログラムのプロセス ID です。
発行元ユーザー ID	発行元プロセスのユーザー ID です。Windows からのイベントの場合は-1 となります。

属性	説明
発行元グループ ID	発行元プロセスのグループ ID です。Windows からのイベントの場合は-1 となります。
発行元ユーザー名	発行元プロセスのユーザー名です。
発行元グループ名	発行元プロセスのグループ名です。Windows からのイベントの場合は空白となります。
発行元イベント DB 内通し番号	発行元ホストでのイベント DB 内通し番号です（転送によって値は変化しません）。
種別	JP1 イベントのイベント種別です。 相関成立のアイコン  および相関不成立のアイコン  が表示されます。 繰り返しイベントの監視抑止で、イベントを抑止している場合にイベントが大量発生したとき、 [イベントコンソール] 画面の各タブにイベントが大量発生したことを表す   が表示されます。
アクション種別	アクションの種別です。 アクション種別を示すアイコン  （コマンド）が表示されます。
重大度(変更前)	変更する前の重大度です。 統合監視 DB を使用し、重大度変更機能を有効にしたとき設定できます。
重大度変更	重大度を変更した場合に <input checked="" type="checkbox"/> を表示します。 統合監視 DB を使用し、重大度変更機能を有効にしたとき表示されます。
メッセージ(変更後)	変更後の表示メッセージです。 統合監視 DB を使用し、表示メッセージ変更機能を有効にしたとき表示されます。 10-50 以前からバージョンアップインストール後に jimbupdate コマンドで IM データベースを更新していない場合、使用できません。
表示メッセージ変更	表示メッセージを変更した場合に <input checked="" type="checkbox"/> を表示します。 統合監視 DB を使用し、表示メッセージ変更機能を有効にしたとき表示されます。 10-50 以前からバージョンアップインストール後に jimbupdate コマンドで IM データベースを更新していない場合、使用できません。
表示メッセージ変更定義名	表示メッセージ変更の定義の名称です。 統合監視 DB を使用し、表示メッセージ変更機能を有効にしたとき表示されます。 10-50 以前からバージョンアップインストール後に jimbupdate コマンドで IM データベースを更新していない場合、使用できません。
メモ	JP1 イベントにメモ情報がある場合に  を表示します。 統合監視 DB を使用し、メモ情報の設定機能を有効にしたとき設定できます。
発生元ホスト名	JP1 イベントの発行契機となった事象が発生したホストの名称です。 統合監視 DB を使用し、発生元ホストのマッピングを有効にしたときに表示されます。
発行元 IP アドレス	発行元イベントサーバに対応する IP アドレスです。
オブジェクト ID	アクションの契機となったイベントのイベント DB 内通し番号です。
終了コード	コマンドの実行結果です。
関連イベント DB 内通し番号	相関元イベントのイベント DB 内通し番号です。

属性	説明
関連イベント発行条件名	成立した関連イベント発行条件名です。
監視抑止 ID	発生件数がしきい値以上になった繰り返しイベントのイベント DB 内通し番号です。
繰り返しイベント条件名	繰り返しイベントと判断した繰り返しイベントの条件名です。
監視 ID	ログファイルトラップの ID 番号です。
監視名	ログファイルトラップの監視名です。
固有の拡張属性	固有の拡張属性の内容を表示します。 イベント拡張属性定義ファイル（拡張ファイル）に定義した固有の拡張属性が表示されます。

(2) JP1 イベントの固有の拡張属性（固有の拡張属性表示）

イベント拡張属性定義ファイル（拡張ファイル）を設定すると、イベント一覧の任意に指定した項目名の欄に、固有の拡張属性の内容を表示できます。例えば、固有の拡張属性「E.SYSTEM」に項目名として「システム名」と指定することで、イベント一覧にシステム名という項目で、固有の拡張属性「E.SYSTEM」の属性値を表示できます。

(3) JP1 イベントの固有の拡張属性（イベント情報マッピング）

イベント情報マッピングを設定すると、イベント一覧の表示項目（基本属性または共通の拡張属性）の欄に、固有の拡張属性の内容を表示できます。例えば、SNMP トラップが JP1 イベントに変換されてイベント一覧に表示される場合に、登録ホストの欄に SNMP トラップ発行元ホスト名を表示できます。

イベント情報マッピングによって表示される固有の拡張属性には、表示された属性値の先頭に「#」（シャープ記号と半角の空白）が表示されます。

イベント情報マッピングを使用して固有の拡張属性を表示するには、表示項目と固有の拡張属性とをマッピングしておく必要があります。イベント情報マッピングの詳細については、「[6.9.2 JP1 イベントの固有の拡張属性を表示する（イベント情報のマッピング）](#)」を参照してください。

(4) JP1 イベントの対処状況

イベント一覧に表示されているすべてのイベントの左端の列に、イベントへの対処状況（「対処済」、 「処理中」、 および「保留」）を示す対処状況マークを表示できます。対処状況マークを表示する方法については、「[6.3.1 JP1 イベントの対処状況の設定について](#)」を参照してください。

なお、繰り返しイベントの監視抑止機能または繰り返しイベントの集約表示機能を使用している場合で、集約イベントの対処状況と、繰り返しイベントの対処状況が異なる場合には、「!」が表示されます。

6.1.2 【イベントコンソール】画面のイベント一覧に表示されるイベント

画面に表示されるイベント

画面に表示されるイベントには、通常の JP1 イベント、集約イベント（集約中イベント、集約完了イベントを含む）および相関イベントがあります。

- 集約イベント

[集約状態] に繰り返し回数や、集約中であることを示す「+」が表示されます。

集約イベントの表示の詳細については、「[6.1.2\(1\) イベント一覧での集約イベントの表示について](#)」を参照してください。

- 相関イベント

[種別] にアイコン ,  が表示されます。

相関イベントの表示の詳細については、「[6.1.2\(2\) イベント一覧での相関イベントの表示について](#)」を参照してください。

画面に表示できるイベント数

画面に表示できるイベント数は、[ユーザー環境設定] 画面の [スクロールバッファ] に指定した値です。表示できる JP1 イベント数の上限は 2,000 件です。

統合監視 DB を使用すると、統合監視 DB に保存されているすべてのイベントを表示できます。[表示開始位置指定] 領域にあるスライダーでイベント表示位置を移動する、または時間を指定することで表示できます。統合監視 DB の設定方法については、マニュアル「[JP1/Integrated Management 3 - Manager 構築ガイド](#)」の「[1.4.2 統合監視 DB の設定 \(Windows の場合\)](#)」, 「[2.4.2 統合監視 DB の設定 \(UNIX の場合\)](#)」を参照してください。

JP1 イベントの数が、表示できる JP1 イベントの数の上限を超えると次の動作となります。

[イベント監視] ページ

対処状況の状態にかかわらず、最も到着時刻が古い JP1 イベントから消去されます。

[重要イベント] ページ

対処状況が対処済で、最も到着時刻の古い JP1 イベントから消去されます。

対処済の重要イベントがない場合は、対処状況の状態にかかわらず、到着時刻が古い JP1 イベントから消去されます。

画面から消去された JP1 イベントも、イベント DB には登録されています。画面から消去された JP1 イベントを参照する場合は、JP1 イベントを検索してください。JP1 イベントの検索方法については、「[6.8 JP1 イベントを検索する](#)」を参照してください。

画面起動時に表示される JP1 イベント

画面を起動したときに表示される JP1 イベントは、次のどちらかの条件に合う最新の JP1 イベントです。

- ログインしているマネージャーの起動後、画面を起動するまでに発生した JP1 イベント
- jcoimdef コマンドで設定した「イベント DB からのイベント取得開始位置」から、ログインしているマネージャーの起動時までに発生した JP1 イベント

画面を起動したときに表示される JP1 イベントの件数は、次の値のどちらか小さい方を上限とします。

- [システム環境設定] 画面の [イベントバッファ] に指定した値 (イベントバッファ数)
- [ユーザー環境設定] 画面の [スクロールバッファ] に指定した値 (スクロールバッファ数)

なお、JP1 イベントの件数には、内部的に使用する連絡用イベント※も含まれます。そのため、初期表示時には、表示される JP1 イベントの件数が上限値に達しない場合もあります。

注※ 連絡用イベント

重要イベントの対処状況を変更や削除したとき、および自動アクションを実行したときに内部的に発行されるイベントで、画面には表示されない。

イベント一覧の更新

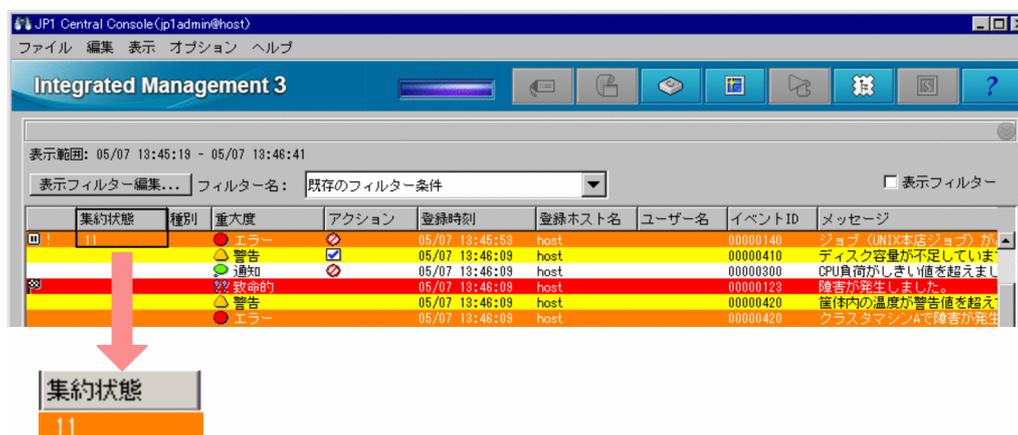
イベント一覧は、ユーザーが設定した更新間隔で更新され、最新の JP1 イベントが表示されます。ただし、自動更新をしない設定にしている場合は、画面を起動しても、最新の JP1 イベントが表示されません。この場合に、最新の JP1 イベントを表示するには、[表示] - [最新情報に更新] を選択します。

自動更新するかどうか、および自動更新の間隔は、[ユーザー環境設定] 画面で設定します。

(1) イベント一覧での集約イベントの表示について

繰り返しイベントの監視抑止機能、または繰り返しイベントの集約表示機能によって JP1 イベントが集約されていると、イベント一覧に集約イベントが表示されます。

図 6-2 集約イベントの集約表示例



[集約状態]

[集約状態] に繰り返し回数が表示されます。繰り返し回数とは、集約イベント数と繰り返しイベントの総数のことです。非集約イベントの場合は、何も表示されません。

- 集約完了イベントの場合
繰り返し回数が表示されます。
繰り返しイベントの監視抑止を設定している場合、表示される繰り返し回数は、1~1,000,000 です。

繰り返しイベントの集約表示を設定している場合、表示される繰り返し回数は、1～100 です。

集約状態	重大度
16	警告

- 集約中イベントの場合

繰り返し回数および集約中であることを示す「+」が表示されます。

繰り返し回数が1回（集約開始イベントだけ）の場合は「1+」、繰り返し回数が2回（集約開始イベントと繰り返しイベント1件）の場合は「2+」のように表示されます。なお、[重要イベント] ページでは、集約開始イベントが削除済み状態で、繰り返しイベントがない場合、「0+」と表示されます。

集約状態	重大度
12+	警告

また、集約イベントを削除すると次のように表示されます。

- 集約開始イベントを削除した場合

[イベントコンソール] 画面の [重要イベント] ページで、集約開始イベントを削除した場合、そのイベントは削除済み状態となり、繰り返し回数の右横に「削除」が表示されます。

集約状態	重大度
11+ 削除	緊急

そのあと、イベントの集約が完了して、削除済み状態の非集約イベントになった場合、[イベントコンソール] 画面の [重要イベント] ページに表示されなくなります。

- 繰り返しイベントを削除した場合

繰り返しイベントの集約表示機能を使用している場合は、[関連イベント一覧 (集約)] 画面の [関連イベント一覧] で、繰り返しイベントを削除したとき、集約イベントの繰り返し回数が、削除した数だけ減ります。

集約完了イベントの繰り返し回数が、繰り返しイベントを削除したことによって1回になった場合、そのイベントは非集約イベントとなります。また、その非集約イベントが削除済み状態であった場合、[イベントコンソール] 画面の [重要イベント] ページに表示されなくなります。

繰り返しイベントの監視抑止機能を使用している場合は、繰り返しイベントを削除しても集約イベントの繰り返し回数は減少しません。

対処状態表示

左端の列に JP1 イベントへの対処状況を示す対処状況マークが表示されます。

対処状況マークの種類および内容は、[イベントコンソール] 画面の [イベント監視] ページおよび [重要イベント] ページに表示される対処状況マークと同じです。

繰り返しイベントの監視抑止機能を使用している場合、1件目（集約開始イベント）から100件目までの繰り返しイベントの対処状況が異なるときに「!」が表示されます。101件以上集約している場合、1件目から100件目までの繰り返しイベントと、101件目以降の繰り返しイベントの対処状況が異なっても、「!」は表示されません。

集約状態	重大度
! 16	警告

【アクション】

自動アクションの抑止機能を使用している場合、[イベントコンソール] 画面にアクション抑止の状態を示すマークが表示されます。

表 6-2 アクション抑止の状態

アクション抑止の状態	説明
	抑止されなかったアクション
	抑止されたアクション
	一部抑止されたアクション

また、繰り返しイベントの監視抑止でアクションの実行を抑止している場合にイベントが大量発生したとき、[イベントコンソール] 画面に  が表示されます。

集約イベントと繰り返しイベントのアクション状況が異なる場合、アクション表示に「!」が表示されま

集約状態	重大度	アクション
 !	16  警告	 !

【種別】

繰り返しイベントの監視抑止でイベントを抑止している場合にイベントが大量発生したとき、[イベントコンソール] 画面にイベントが大量発生したことを表す  が表示されます。

【イベントコンソール】画面の各タブ

繰り返しイベントの監視抑止でイベントを抑止している場合にイベントが大量発生したとき、[イベントコンソール] 画面の各タブにイベントが大量発生したことを表す  が表示されます。

(2) イベント一覧での関連イベントの表示について

関連イベントは [イベントコンソール] 画面の [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] ページのイベント一覧に表示されます。

関連イベントは [種別] にアイコンが表示されます。

アイコンは、関連成立  と関連不成立  の 2 種類があります。

なお、[種別] はデフォルトで表示されている項目ではありません。表示するには [ユーザー環境設定] 画面で [種別] を表示項目に指定します。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「3.24 [ユーザー環境設定] 画面」を参照してください。

6.1.3 フィルターの適用

あらかじめ設定したフィルターを適用することで [イベントコンソール] 画面に表示される JP1 イベントを制限できます。適用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

フィルターの条件に一致する JP1 イベントだけをイベント一覧に表示します。

複数の表示フィルターを設定している場合に、適用する表示フィルターを切り替えるときの手順については「[6.5.1 表示フィルターを有効にして特定の JP1 イベントだけを表示する](#)」を参照してください。

なお、[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適用状態の保存を設定すると，JP1/IM - View のログアウト時に保存し，ログイン時に復元して表示されます。詳細についてはマニュアル「[JP1/Integrated Management 3 - Manager 構築ガイド](#)」の「[5.16 ログインユーザーごとの JP1/IM - View の設定](#)」を参照してください。

ユーザーフィルター

ログインしているユーザーによって，表示する JP1 イベントを制限します。

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] ページに重要イベントを表示します。[重要イベント] ページについては「[6.5.2 重要イベントだけを表示する](#)」を参照してください。

なお，JP1/IM - View が重要イベントを受信すると，画面上部のランプの色が赤に変わります。[重要イベント] ページで，すべての重要イベントを対処済にする，削除する，または重要イベントを解除すると，ランプの色が青に戻ります。

イベント取得フィルター

JP1/IM - Manager が JP1/Base から取得する JP1 イベントを制限します。

複数のイベント取得フィルターを設定している場合に，適用するイベント取得フィルターを切り替えるときの手順については「[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。

運用中に発生した JP1 イベントを基に共通除外条件を設定して適用する場合の手順については，「[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。

それぞれのフィルターをあらかじめ設定する手順については，マニュアル「[JP1/Integrated Management 3 - Manager 構築ガイド](#)」の「[5.2 JP1 イベントのフィルタリングの設定](#)」を参照してください。

6.2 JP1 イベントの詳細情報を表示する

イベント一覧に表示されている JP1 イベントの詳細な属性情報を表示できます。

詳細情報を表示するには、[イベントコンソール] 画面のイベント一覧で、属性を表示したい JP1 イベントをダブルクリックします。[イベント詳細] 画面が表示されます。

繰り返しイベントの監視抑止機能、または繰り返しイベントの集約表示機能によって表示される集約イベントをダブルクリックした場合、集約開始イベントの詳細情報が表示されます。集約イベントに集約されている繰り返しイベントの詳細情報を確認する場合には、「[6.4.1\(1\) 集約イベントに集約されている繰り返しイベントの詳細情報を確認する](#)」を参照してください。

[イベント詳細] 画面には、イベント属性、メッセージ、イベントガイド情報およびメモが表示されます。

[イベント属性] には、その JP1 イベントに登録されているイベント属性名と属性値が表示されます。登録されている属性は、その JP1 イベントによって異なります。

イベント一覧上で前後に並んでいる JP1 イベントの詳細情報を表示したい場合は、[前イベント] または [次イベント] のボタンをクリックします。

次のどれかの方法でも、JP1 イベントの詳細を表示できます。

- [イベントコンソール] 画面で JP1 イベントを選択し、[表示] - [イベント詳細表示] を選択する。
- [イベントコンソール] 画面で JP1 イベントを選択し、ポップアップメニューから [イベント詳細表示] を選択する。
- [イベントコンソール] 画面で JP1 イベントを選択し、ツールバーからイベント詳細表示ボタンをクリックする。

詳細情報として表示される項目を次に示します。

表 6-3 JP1 イベントの詳細情報

表示名※1	内容
イベント DB 内通し番号	発行元に関係なくこのイベントサーバに到達した順番。
イベント ID	発行アプリケーションプログラムや事象の内容を表す値。
発行元プロセス ID	発行元アプリケーションプログラムのプロセス ID。
登録時刻	発行元イベントサーバでの登録時刻。
到着時刻	自イベントサーバでの登録時刻。
発行元ユーザー ID	発行元プロセスのユーザー ID。Windows からのイベントの場合は-1 となる。
発行元グループ ID	発行元プロセスのグループ ID。Windows からのイベントの場合は-1 となる。
発行元ユーザー名	発行元プロセスのユーザー名。
発行元グループ名	発行元プロセスのグループ名。Windows からのイベントの場合は空白となる。

表示名※1	内容
発行元イベントサーバ名	発行元のイベントサーバ名（イベント一覧では、「登録ホスト名」と表示される）。イベントが、JP1/Base(エージェント)→JP1/IM - Manager(拠点マネージャー)→JP1/IM - Manager(統合マネージャー)のように転送された場合でも、最初の JP1/Base のイベントサーバ名が入る。
発行元 IP アドレス	発行元イベントサーバに対応する IP アドレス。
発行元イベント DB 内通し番号	発行元ホストでのイベント DB 内通し番号（転送によって値は変化しない）。
重大度	JP1 イベントの緊急性を表す。緊急性の高い順に、次の値がある。 「緊急 (Emergency)」、「警戒 (Alert)」、「致命的 (Critical)」、「エラー (Error)」、「警告 (Warning)」、「通知 (Notice)」、「情報 (Information)」、「デバッグ (Debug)」 なお、統合監視 DB を使用する場合に、重大度変更機能で重大度を変更したときは、変更したあとの JP1 イベントの緊急性を表す。
ユーザー名	業務を実行しているユーザー名。
プロダクト名	JP1 イベントを発行したプログラム名。
オブジェクトタイプ	イベント発行の契機となったオブジェクトの種類を表す名称。
オブジェクト名	イベント発行の契機となったオブジェクト（ジョブ、ジョブネットなど）の名称。
登録名タイプ	オブジェクトの種別。通常はオブジェクトタイプと同じだが、ジョブネットなど階層のあるオブジェクトの場合、最上層のオブジェクトの種別となる。値の範囲はオブジェクトタイプと同じ。
登録名	ユーザーの操作時に実行を指示する単位になる名称。通常はオブジェクト名と同じだが、ジョブネットなど階層のあるオブジェクトの場合、最上層のオブジェクトの名称になる。
オブジェクト ID	アクションの契機となったイベントのイベント DB 内通し番号。
事象種別	オブジェクト名に示したオブジェクトに対して起こった事象。
開始時刻	実行開始または再実行開始の時刻。
終了時刻	実行終了の時刻。
終了コード	コマンドの実行結果。
発生元ホスト名	JP1 イベントの発行契機となった事象が発生したホストの名称。 統合監視 DB を使用し、発生元ホストのマッピングを有効にしたときに表示される。
拡張属性の固有情報の項目名※2	イベント拡張属性定義ファイル（拡張ファイル）に定義した固有の拡張属性の属性値。
関連イベント DB 内通し番号	相関元イベントのイベント DB 内通し番号を半角スペースで区切ったもの。次の形式で表示される。 イベント DB 内通し番号△イベント DB 内通し番号△イベント DB 内通し番号・・・
相関イベント発行条件名	成立した相関イベント発行条件名。
重大度(変更前)	統合監視 DB を使用する場合に、重大度変更機能で重大度を変更したとき、変更する前の JP1 イベントの緊急性を表す。緊急性の高い順に、次の値がある。 「緊急 (Emergency)」、「警戒 (Alert)」、「致命的 (Critical)」、「エラー (Error)」、「警告 (Warning)」、「通知 (Notice)」、「情報 (Information)」、「デバッグ (Debug)」

表示名※1	内容
表示メッセージ変更定義名	表示メッセージ変更の定義の名称。統合監視 DB を使用している場合に、表示メッセージ変更機能でメッセージを変更した詳細情報を選択したときに表示される。
監視抑止 ID	発生件数がしきい値以上になった繰り返しイベントのイベント DB 内通し番号。繰り返しイベントの監視抑止機能を使用している場合に、文字列形式で表示される。
繰り返しイベント条件名	繰り返しイベントと判断した繰り返しイベントの条件名。繰り返しイベントの監視抑止機能を使用している場合に、文字列形式で表示される。
監視 ID	ログファイルトラップの ID 番号。
監視名	ログファイルトラップの監視名。
共通除外条件群 ID	除外をした共通除外条件群の ID。
共通除外条件群名	除外をした共通除外条件群の条件名。
共通除外条件群除外対象	共通除外条件の除外対象。自動アクションの実行対象から除外する場合に、「action」が表示される。
メッセージ	イベントの内容を表した文字列。統合監視 DB を使用している場合に、表示メッセージ変更機能でメッセージを変更した詳細情報を選択したときは、変更前と変更後の表示メッセージを表示できる。
ガイド	JP1 イベントに対応したイベントガイド情報。 イベントガイド表示を有効にしている場合に表示される。なお、JP1 イベントに対応するイベントガイド情報がない場合は「KAVB1588-I」のメッセージが表示される。
メモ	統合監視 DB を使用し、メモ情報の設定機能を有効にしたとき、メモ情報を表示する。

注※1 イベント拡張属性定義ファイルの定義に一致したイベントについては、イベント拡張属性定義ファイルに記載した項目名が表示されます。

注※2 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。

なお、重大度以降の項目は、イベントによって表示されない場合があります。

6.2.1 JP1 イベントのメモ情報を編集する

統合監視 DB を使用する場合、メモ情報の設定機能を有効にすると、統合監視 DB に保存されている JP1 イベントにメモ情報を追加できます。ここでは、メモ情報を編集し、統合監視 DB の JP1 イベントに反映する手順について説明します。

統合監視 DB の設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.4.2 統合監視 DB の設定 (Windows の場合)」、 「2.4.2 統合監視 DB の設定 (UNIX の場合)」を参照してください。

また、メモ情報の設定機能を有効にする方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「5.7 メモ情報の設定」を参照してください。

なお、これらの操作には、JP1_Console_Admin 権限または JP1_Console_Operator 権限が必要です。

1. [イベント詳細 (編集)] 画面を表示する。

[イベント詳細 (編集)] 画面は、[イベント詳細] 画面の [編集] ボタンをクリックするか、イベント一覧でイベントを1件選択し、[イベント詳細 (編集)] メニューを選択することで表示できます。

2. [イベント情報 (編集)] 画面にメモ情報を記述する。

3. [イベント詳細 (編集)] 画面の [適用] ボタンをクリックする。

イベント一覧の表示項目である「メモ」および [イベント詳細] 画面にメモが表示されます。また、メモ情報があるイベントにメモのアイコン  が表示されます。

6.3 JP1 イベントの対処状況を設定する

ここでは、JP1 イベントの対処状況の設定について概要および操作手順を説明します。また、併せて [重要イベント] ページに表示されている重要イベントを削除する手順についても説明します。

6.3.1 JP1 イベントの対処状況の設定について

[イベントコンソール] 画面の各ページのイベント一覧では、JP1 イベントの対処状況を設定できます。対処状況を設定したイベントには、イベント一覧の左端の列に対処状況マークが表示されます。

対処状況の種類と、その対処状況を示す対処状況マークを次に示します。どのような場合にどの対処状況を設定するか、運用に合わせて決めてください。

表 6-4 対処状況の種類と対処状況マーク

対処状況	対処状況マーク
対処済	
処理中	
保留	
未対処	(無印)
異なる対処状況※	!

注※

繰り返しイベントの監視抑止機能または繰り返しイベントの集約表示機能を使用している場合で、異なる対処状況が設定された JP1 イベントが一つの集約イベントに混在して集約されている状態です。

繰り返しイベントの監視抑止機能を使用している場合、1 件目（集約開始イベント）から 100 件目までの繰り返しイベントの対処状況が異なるときに「!」が表示されます。101 件以上集約している場合、1 件目から 100 件目までの繰り返しイベントと、101 件目以降の繰り返しイベントの対処状況が異なっても、「!」は表示されません。

設定した対処状況は、ログインしているマネージャーの統合監視 DB またはイベント DB に記録されます（ほかのホストから転送されてきた JP1 イベントの場合、転送元ホストの統合監視 DB またはイベント DB の情報は変更されません）。そのため、同じマネージャーにログインしている JP1/IM - View の [イベント監視] ページおよび [重要イベント] ページにも反映されます。

[イベント検索] ページでは、検索した時点の JP1 イベントの内容を表示しているため、ほかのページで対処状況を設定しても表示は変わりません。最新データを表示する場合は、再度検索を実行してください。

集約イベントに対する対処状況の設定

集約イベントに対して対処状況を設定すると、設定した時点までにその集約イベントに集約された繰り返しイベントもすべて同じ対処状況に変更されます。ただし、繰り返しイベントの監視抑止機能を使用している、かつ、101 件以上集約している場合は、101 件目以降の繰り返しイベントの対処状況は変更されません。

対処状況を変更したあとに集約された繰り返しイベントの対処状況は、設定されません。集約イベントの中に対処状況が異なる繰り返しイベントが混在することとなるため、対処状況表示に「!」が表示されます。

6.3.2 イベント一覧から JP1 イベントの対処状況を設定する

JP1 イベントに対処状況を設定する手順を示します。この操作の前提条件は次のとおりです。

- JP1/IM - Manager にログインする JP1 ユーザーに JP1_Console_Admin 権限または JP1_Console_Operator 権限があること。
- [イベント検索] ページから対処状況を設定する場合は、ログインしているマネージャーからの検索結果であること。

1. [イベントコンソール] 画面の各ページのイベント一覧から、対処状況を設定したい JP1 イベントを選択する。

2. 次のどれかに従って操作する（選択したイベントがどの対処状況であっても操作できる）。

- メニューバーから [表示] を選択し、サブメニューの中から設定したい対処状況を選ぶ。
- 右クリックして表示されるポップアップメニューから、設定したい対処状況を選ぶ。
- [重要イベント] ページ上のボタンから、設定したい対処状況のボタンをクリックする（[重要イベント] ページから対処状況を設定する場合）。

メモ

重要イベントの対処状況は、jcochstat コマンドを使用しても設定できます。jcochstat 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「jcochstat」(1. コマンド) を参照してください。

6.3.3 [重要イベント] ページから重要イベントを削除する

[重要イベント] ページから重要イベントを削除する手順を次に示します。この操作の前提条件は次のとおりです。

- JP1/IM - Manager にログインする JP1 ユーザーに JP1_Console_Admin 権限または JP1_Console_Operator 権限があること。

1. [イベントコンソール] 画面の [重要イベント] ページのイベント一覧から、削除したい JP1 イベントを選択する。

2. 次のどれかに従って操作する（選択したイベントがどの対処状況であっても操作できる）。

- メニューバーから [表示] - [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 [削除] を選択する。
- [重要イベント] ページ上のボタンから、削除のボタンをクリックする。

なお、ここでの「削除」は画面から削除するだけで、イベント DB または統合監視 DB からは削除されません。また、「削除」情報は [イベントコンソール] 画面のほかのページに反映されません。

6.4 [関連イベント一覧] 画面から JP1 イベントを操作する

ここでは、[関連イベント一覧] 画面から JP1 イベントを操作する手順について説明します。[関連イベント一覧] 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」の次の個所を参照してください。

- 3.8 [関連イベント一覧 (集約)] 画面
- 3.9 [関連イベント一覧 (相関)] 画面

6.4.1 繰り返しイベントの詳細情報を確認し対処状況を変更する

繰り返しイベントの監視抑止機能または繰り返しイベントの集約表示機能を使用している場合で、集約イベントに集約されている繰り返しイベントの詳細を確認したり、対処状況を設定したりするときは、[関連イベント一覧 (集約)] 画面から JP1 イベントを操作します。

(1) 集約イベントに集約されている繰り返しイベントの詳細情報を確認する

集約イベントに集約されている繰り返しイベントの詳細情報を確認する手順を次に示します。

1. [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] ページで集約イベントを一つ選択する。
2. [イベントコンソール] 画面のメニューから [表示] - [関連イベント一覧表示] を選択する。*
[関連イベント一覧 (集約)] 画面が表示されます。
3. [関連イベント一覧 (集約)] 画面の [関連イベント一覧] から詳細情報を確認したい繰り返しイベントをダブルクリックする。

[イベント詳細] 画面が表示されます。

繰り返しイベントの監視抑止機能が有効な場合、101 件目以降の繰り返しイベントは、[関連イベント一覧 (集約)] 画面に表示されません。その場合、[関連イベント一覧 (集約)] 画面の [表示できないイベント] に、101 件目の繰り返しイベントの到着時刻および最後に到着した繰り返しイベントの到着時刻が表示されます。101 件目以降の繰り返しイベントの詳細情報を参照したい場合は、[表示できないイベント] に表示されている繰り返しイベントの到着時刻を検索条件に指定して検索してください。

なお、[イベント検索条件設定] 画面で集約イベントごとに設定されている監視抑止 ID を検索条件に指定することで、一つの集約イベントに集約された繰り返しイベントを検索することもできます。

イベントの検索方法については、「6.8 JP1 イベントを検索する」を参照してください。

(2) 集約イベントに集約されている繰り返しイベントの対処状況を設定する

集約イベントに集約されている繰り返しイベントの対処状況を設定する手順を次に示します。

1. [イベントコンソール] 画面の [イベント監視] ページまたは [重要イベント] ページで集約イベントを一つ選択する。
2. [イベントコンソール] 画面のメニューから [表示] - [関連イベント一覧表示] を選択する。*
[関連イベント一覧 (集約)] 画面が表示されます。

注※

次の場合には、メニュー項目を選択できません。

- [イベント監視] ページまたは [重要イベント] ページで、イベントを複数選択している場合
 - 非集約イベントを選択している場合
3. [関連イベント一覧 (集約)] 画面の [関連イベント一覧] から対処状況を設定したい繰り返しイベントを選択する。
繰り返しイベントを複数選択することもできます。
 4. 選択した繰り返しイベント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設定したい対処状況を選択する。

繰り返しイベントの対処状況が設定されます。

繰り返しイベントが集約されている集約イベントの対処状況は変更されません。集約イベントの中に対処状況が異なる繰り返しイベントが存在することとなるため、対処状況表示に「!」が表示されます。

対処状況の種類と対処状況マークについては、「6.3.1 JP1 イベントの対処状況の設定について」を参照してください。

6.4.2 関連イベントの詳細情報を確認し対処状況を変更する

関連イベントは通常の JP1 イベントと同様の操作ができます。例えば、JP1 イベントの詳細表示や、対処状況の変更などができます。

関連成立イベントの場合、関連イベントからは発行の契機となった関連元イベントの表示ができます。関連イベントを発行したホストが、JP1/IM - View でログインしているホストと別ホストだった場合は、関連イベントを発行したホストから関連元イベントが取得されます。

関連不成立イベントの場合、関連不成立となった時までイベントの関連条件に従って関連づけられた関連元イベントを表示できます。

なお、繰り返しイベントの監視抑止機能または繰り返しイベントの集約表示機能を使用していた場合、関連イベントが次に示すように集約して表示されることがあります。

表 6-5 関連イベントが集約して表示される例

表示例	説明						
<table border="1"> <thead> <tr> <th>集約状態</th> <th>種別</th> <th>重大度</th> </tr> </thead> <tbody> <tr> <td>24</td> <td></td> <td>エラー</td> </tr> </tbody> </table>	集約状態	種別	重大度	24		エラー	関連イベントが集約完了した場合
集約状態	種別	重大度					
24		エラー					
<table border="1"> <thead> <tr> <th>集約状態</th> <th>種別</th> <th>重大度</th> </tr> </thead> <tbody> <tr> <td>18+</td> <td></td> <td>エラー</td> </tr> </tbody> </table>	集約状態	種別	重大度	18+		エラー	関連イベントが集約中の場合
集約状態	種別	重大度					
18+		エラー					
<table border="1"> <thead> <tr> <th>集約状態</th> <th>種別</th> <th>重大度</th> </tr> </thead> <tbody> <tr> <td>15 削除</td> <td></td> <td>警戒</td> </tr> </tbody> </table>	集約状態	種別	重大度	15 削除		警戒	集約が完了した関連イベントを削除した場合
集約状態	種別	重大度					
15 削除		警戒					
<table border="1"> <thead> <tr> <th>集約状態</th> <th>種別</th> <th>重大度</th> </tr> </thead> <tbody> <tr> <td> 24</td> <td></td> <td>エラー</td> </tr> </tbody> </table>	集約状態	種別	重大度	24		エラー	関連イベントの集約開始イベントと繰り返しイベントの対処状況が異なる場合
集約状態	種別	重大度					
24		エラー					

この場合、関連元イベントを表示するには、[関連イベント一覧 (集約)] 画面を表示してから [関連イベント一覧 (相関成立)] または [関連イベント一覧 (相関不成立)] 画面を表示します。

(1) 関連元イベントを表示する

関連元イベントを表示する手順を次に示します。なお、集約して表示されているイベントの見方の詳細については、「6.1.2(1) イベント一覧での集約イベントの表示について」を参照してください。

1. [イベントコンソール] 画面の各ページのイベント一覧から、関連イベントを一つ選択する。
2. [イベントコンソール] 画面のメニューから [表示] - [関連イベント一覧表示] を選択する。*
 - 前の手順で選択した関連イベントが非集約イベントの場合：
[関連イベント一覧 (相関成立)] または [関連イベント一覧 (相関不成立)] 画面が表示され、関連元イベントの一覧が表示されます。次の手順は不要です。
 - 前の手順で選択した関連イベントが集約イベントの場合：
[関連イベント一覧 (集約)] 画面が表示されます。次の手順に進んでください。

注※

イベント一覧から JP1 イベントを複数選択している場合は、メニュー項目を選択できません。

3. 前の手順で [関連イベント一覧 (集約)] 画面が表示された場合は、[関連イベント一覧] から関連イベントを一つ選択し、右クリックして表示されるポップアップメニューから [関連イベント一覧表示] を選択する。
[関連イベント一覧 (相関成立)] または [関連イベント一覧 (相関不成立)] 画面が表示され、関連元イベントの一覧が表示されます。

(2) [関連イベント一覧 (相関成立)] または [関連イベント一覧 (相関不成立)] 画面から相関元イベントの対処状況を設定する

[関連イベント一覧 (相関成立)] または [関連イベント一覧 (相関不成立)] 画面から相関元イベントの対処状況を設定する手順を次に示します。この操作の前提条件は次のとおりです。

- JP1/IM - Manager にログインする JP1 ユーザーに JP1_Console_Admin 権限または JP1_Console_Operator 権限があること。
- [イベント検索] ページから対処状況を設定する場合は、ログインしているマネージャーからの検索結果であること。

1. [6.4.2(1) 相関元イベントを表示する] の手順に従って、対処状況を設定したい相関元イベントを表示する。
2. [関連イベント一覧] から対処状況を設定したい相関元イベントを選択する。

メモ

[表示対象] から相関イベントを選択することで、相関イベントの対処状況を設定することもできます。

3. 選択した相関元イベント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設定したい対処状況を選択する。

相関元イベントの対処状況が設定されます。

メモ

[関連イベント一覧 (相関成立)] または [関連イベント一覧 (相関不成立)] 画面で、表示対象の相関イベントの対処状況を変更しても、一覧表示されている相関元イベントの対処状況は変更されません。同様に一覧表示されている相関元イベントの対処状況を変更しても、表示対象の相関イベントの対処状況は変更されません。これは、相関元イベントと相関イベントが別の事象を表すイベントであるためです。

(3) [関連イベント一覧 (相関成立)] または [関連イベント一覧 (相関不成立)] 画面から相関元イベントを削除する

[関連イベント一覧 (相関成立)] または [関連イベント一覧 (相関不成立)] 画面から相関元イベントを削除する手順を次に示します。この操作の前提条件は次のとおりです。

- JP1/IM - Manager にログインする JP1 ユーザーに JP1_Console_Admin 権限または JP1_Console_Operator 権限があること。
1. [6.4.2(1) 相関元イベントを表示する] の手順に従って、[重要イベント] ページを起点として削除したい相関元イベントを表示する。

2. [関連イベント一覧 (相関成立)] または [関連イベント一覧 (相関不成立)] 画面の [表示画面] の内容が、次のどちらかであることを確認する。

- 重要イベント
- 重要イベント - 関連イベント一覧 (集約)

3. [関連イベント一覧] から削除したい相関元イベントを選択する。

メモ

[表示対象] から相関イベントを選択することで、相関イベントを削除することもできます。

4. 選択した相関元イベント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 [削除] を選択する。
相関元イベントが削除されます。

なお、ここでの「削除」は画面から削除するだけで、イベント DB または統合監視 DB からは削除されません。また、「削除」情報は [イベントコンソール] 画面のほかのページに反映されません。

6.5 JP1/IM のフィルターを適用する

ここでは、JP1/IM - View から JP1/IM のフィルターを適用する手順について説明します。

6.5.1 表示フィルターを有効にして特定の JP1 イベントだけを表示する

[イベントコンソール] 画面の [イベント監視] ページおよび [重要イベント] に表示される JP1 イベントに対し、適用する表示フィルターを切り替えるには次の操作をします。なお、表示フィルターを切り替えるには、フィルター設定を済ませておく必要があります。

表示フィルターの設定について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「5.2.1 表示フィルターを設定する」

1. [フィルター名] リストボックスから、切り替えたい表示フィルターを選択する。
2. [表示フィルター] チェックボックスをチェックする、またはメニューから [表示] - [表示フィルターの適用] を選択する。
フィルターで設定した条件に一致する JP1 イベントが、[イベントコンソール] 画面の [イベント監視] ページおよび [重要イベント] に表示されます。

6.5.2 重要イベントだけを表示する

画面に重要イベントだけを表示するには、[イベントコンソール] 画面の [重要イベント] ページを選択します。[重要イベント] ページのイベント一覧には、[イベント監視] ページに表示されている JP1 イベントのうち、重要イベントだけが表示されます。

どの JP1 イベントを重要イベントとするかは、管理者が定義できます。デフォルトでは、重大度が「緊急 (Emergency)」、[警戒 (Alert)」、[致命的 (Critical)」、[エラー (Error)』の JP1 イベントが重要イベントとなっています。

[重要イベント] ページに表示されている重要イベントの数が、画面に表示できるイベント数の最大値を超えると、古い重要イベントから消去されます。このとき、最初に消去されるのは対処済の重要イベントです。対処済の重要イベントがない場合は、未対処、保留、処理中の重要イベントのうち最も古いイベントが削除されます。この場合は、状態にかかわらず、古い重要イベントから削除されます。JP1 イベントの対処状況の設定については、「6.3.2 イベント一覧から JP1 イベントの対処状況を設定する」を参照してください

なお、統合監視 DB を有効にすると、統合監視 DB に格納されているすべてのイベントを表示できます。イベントは、スライダーでイベント表示位置を移動して表示します。統合監視 DB の設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.4.2 統合監視 DB の設定 (Windows の場合)」、[2.4.2 統合監視 DB の設定 (UNIX の場合)』を参照してください。

また、繰り返しイベントの監視抑止機能を使用している場合、イベント一覧から集約イベントを削除すると、1件目（最も古い繰り返しイベント）から100件目までの繰り返しイベントのうち、削除されていない繰り返しイベントを削除します。101件目以降の繰り返しイベントは、削除されません。また、繰り返しイベントを削除しても、集約件数は減少しません。

表示フィルターが設定されている場合は、表示するJP1イベントをさらに絞り込むことができます。[フィルター名] リストボックスから適用するフィルターを選択し、[表示フィルター] チェックボックスをチェックします。それによって、設定されているフィルターの条件に一致するJP1イベントだけが表示されます。

[ユーザー環境設定] 画面の [カラーリング] で [有効] チェックボックスをチェックし、かつ [[重要イベント] ページを対象とする] ラジオボタンを選択している場合、イベントの重大度に基づいてイベントの行に背景色がつきます。

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。

6.5.3 適用するイベント取得フィルターを切り替える

JP1/IM が JP1/Base から JP1 イベントを取得するときのフィルター条件を、複数保存してあるイベント取得フィルターから一つ選択して、切り替えられます。

また、イベント取得フィルターで一時的に特定の JP1 イベントの取得を対象外にしたい場合に定義する共通除外条件の有効・無効を切り替えられます。

共通除外条件の切り替えは、メンテナンス作業を実施するホストを JP1/IM の監視対象外として、メンテナンス作業を実施するホストから発行される JP1 イベントを一時的に取得しないようフィルタリングする場合に実施します。

イベント取得フィルター、および共通除外条件の切り替え方法には、次の3種類があります。

- [システム環境設定] 画面から切り替える
切り替えるイベント取得フィルター名が明確な場合、[システム環境設定] 画面からイベント取得フィルターを選択して、切り替えを実施します。
- [イベント取得条件一覧] 画面から切り替える
[システム環境設定] 画面からでは切り替えるイベント取得フィルター名が特定できない場合、[イベント取得条件一覧] 画面でイベント取得フィルターの設定内容などを確認して、切り替えを実施します。
- jcochfilter コマンドを使用して切り替える
JP1/AJS のジョブスケジューラー機能を使用して、所定の時刻に jcochfilter コマンドを実行し、保守業務を開始するジョブネットを作成することで、保守業務と監視状態の変更を自動化できます。

ただし、イベント取得フィルターが互換用で動作している場合は、イベント取得フィルターの切り替えはできません。

[システム環境設定] 画面および [イベント取得条件一覧] 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。

イベント取得フィルターを切り替えた場合に発行されるイベントについては、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」を参照してください。

(1) [システム環境設定] 画面からイベント取得フィルターを切り替える

設定手順は、次のとおりです。

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. [適用中のフィルター] 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する。
3. [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) [システム環境設定] 画面から共通除外条件の有効・無効を切り替える

設定手順は、次のとおりです。

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. [共通除外条件群一覧] から、適用したい条件群をチェックする。
3. [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) [イベント取得条件一覧] 画面からイベント取得フィルターを切り替える

設定手順は、次のとおりです。

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. [フィルター一覧] から、イベント取得フィルターを選択する。

フィルター ID やフィルター名からイベント取得フィルターを特定します。内容を確認したい場合は、イベント取得フィルターを一つ選択し、[編集] ボタンをクリックすると、[イベント取得条件設定] 画面が表示され、選択したフィルターの内容が確認できます。

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。

なお、[イベント取得条件一覧] 画面では、フィルター条件の追加・編集・複製・削除ができます。詳細については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

(4) [イベント取得条件一覧] 画面から共通除外条件の有効・無効を切り替える

設定手順は、次のとおりです。

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. [共通除外条件群一覧] から、適用したい条件群をチェックする。

内容を確認したい場合は、共通除外条件を一つ選択し、[編集] ボタンをクリックすると、[共通除外条件設定] 画面が表示され、選択した共通除外条件の内容が確認できます。

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) jcochfilter コマンドを使用してイベント取得フィルターを切り替える

イベント取得フィルターには、固有のフィルター ID が設定されています。このフィルター ID を利用して、jcochfilter コマンドでイベント取得フィルターを切り替えます。

jcochfilter 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「jcochfilter」(1. コマンド) を参照してください。

設定手順は、次のとおりです。

1. jcochfilter コマンドを入力して、イベント取得条件一覧をリスト表示する。

物理ホストと論理ホストで、イベント取得条件一覧を表示する場合の例を次に示します。

- 物理ホスト上のイベント取得条件一覧を表示する場合

次のようにコマンドを入力します。

```
jcochfilter
```

- 論理ホスト hostA 上のイベント取得条件一覧を表示する場合

次のようにコマンドを入力します。

```
jcochfilter -h hostA
```

論理ホスト hostA 上のイベント取得条件一覧の表示例を次に示します。

図 6-3 jcochfilter コマンドによるイベント取得条件一覧の表示例

```
> jcochfilter
KAVB1005-I コマンド (jcochfilter) を開始しました
KAVB0856-I イベント取得フィルター一覧を表示します。ホスト名 : hostA
KAVB0857-I JP1/IM - Managerに接続しました
現在適用しているフィルターID : 3
      フィルター名 : 通常運用フィルター
現在適用している共通除外条件群ID : 0
      共通除外条件群名 : APサーバーメンテナンス
現在適用している共通除外条件群ID : 2
      共通除外条件群名 : DBサーバーメンテナンス

定義されているフィルター一覧 :
ID   フィルター名
0    既存のフィルター条件
3    通常運用フィルター
定義されている共通除外条件群一覧 :
ID   条件群名
0    APサーバーメンテナンス
1    Webサーバーメンテナンス
2    DBサーバーメンテナンス
KAVB1002-I コマンド (jcochfilter) が正常終了しました
```

指定したホスト上の JP1/IM - Manager が起動されていない場合、コマンドによるイベント取得フィルターの切り替えは実行できません。

2. フィルター ID やフィルター名からイベント取得フィルターを特定する。

3. jcochfilter -i コマンドを入力して、イベント取得フィルターを切り替える。

物理ホストと論理ホストで、イベント取得フィルターを切り替える場合の例を次に示します。

- 物理ホスト上のイベント取得フィルターをフィルター ID が 3 のフィルターに切り替える場合

次のようにコマンドを入力します。

```
jcochfilter -i 3
```

- 論理ホスト hostA 上のイベント取得フィルターをフィルター ID が 3 のフィルターに切り替える場合

次のようにコマンドを入力します。

```
jcochfilter -i 3 -h hostA
```

(6) jcochfilter コマンドを使用して共通除外条件の有効・無効を切り替える

共通除外条件には、固有の共通除外条件群 ID が設定されています。この共通除外条件群 ID を利用して、jcochfilter コマンドで共通除外条件の有効・無効を切り替えます。

jcochfilter 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「jcochfilter」(1. コマンド) を参照してください。

設定手順は、次のとおりです。

1. jcochfilter コマンドを入力して、イベント取得条件一覧をリスト表示する。

物理ホストと論理ホストで、イベント取得条件一覧を表示する場合の例を次に示します。

- 物理ホスト上のイベント取得条件一覧を表示する場合

次のようにコマンドを入力します。

```
jcochfilter
```

- 論理ホスト hostA 上のイベント取得条件一覧を表示する場合

次のようにコマンドを入力します。

```
jcochfilter -h hostA
```

指定したホスト上の JP1/IM - Manager が起動されていない場合、コマンドによるイベント取得フィルターの切り替えは実行できません。

2. 共通除外条件群 ID や共通除外条件群名から共通除外条件群を特定する。

3. 共通除外条件群の有効・無効を切り替える。

次のどちらかのオプションで共通除外条件群の有効・無効を切り替えます。

- -e オプション

有効にしたい共通除外条件群 ID を指定します。

指定しなかった共通除外条件群は無効となります。

- -on または -off オプション

有効にしたい共通除外条件群 ID を指定します。

指定しなかった共通除外条件群の有効・無効は変更されません。

共通除外条件の動作モードが拡張モードの場合に使用できます。

物理ホストと論理ホストで、共通除外条件の有効・無効を切り替える場合の例を次に示します。

- 物理ホスト上の共通除外条件群 ID が 3 の共通除外条件を有効にして、共通除外条件群 ID が 1, 2 の共通除外条件を無効にした場合（指定した共通除外条件群だけが変更されます。）

この指定は、共通除外条件の動作モードが拡張モードの場合に使用できます。

```
jcochfilter -on 3 -off 1,2
```

- 物理ホスト上の共通除外条件群 ID が 3 の共通除外条件を有効にして、それ以外を無効にする場合

```
jcochfilter -e 3
```

- 論理ホスト hostA 上の共通除外条件群 ID が 3 の共通除外条件を有効にして、それ以外を無効にする場合

```
jcochfilter -e 3 -h hostA
```

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

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、または監視はするがアクションは実行したくない 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。

(1) 発生した JP1 イベントを使って追加共通除外条件を設定する

1. 共通除外条件が基本モードの場合は、拡張モードに変更する。

変更する手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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」を参照してください。

2. [イベントコンソール] 画面のイベント一覧で、除外したい JP1 イベントを選択する。

3. [イベントコンソール] 画面の [表示] - [共通除外条件で除外] を選択するか、右クリックして表示されるメニューから [共通除外条件で除外] を選択して、[共通除外条件設定(拡張)] 画面を表示する。手順 2 で選択した JP1 イベントの属性がイベント条件に自動的に設定された状態で、[共通除外条件設定(拡張)] 画面が表示されます。

自動的に設定される項目は共通除外条件自動入力定義ファイル

(common_exclude_filter_auto_list.conf) で変更できます。共通除外条件自動入力定義ファイル

(common_exclude_filter_auto_list.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「共通除外条件自動入力定義ファイル (common_exclude_filter_auto_list.conf)」(2. 定義ファイル) を参照してください。

[共通除外条件設定(拡張)] 画面の [共通除外条件群 ID] には何も表示されません。また、設定もできません。追加共通除外条件群の共通除外条件群 ID は登録するときに割り当てられます。

4. 必要な項目を [共通除外条件設定(拡張)] 画面で編集する。

5. [OK] ボタンをクリックする。

6. 設定内容を反映してもよいかを確認するメッセージが表示されるため、問題なければ [はい] ボタンをクリックする。

[イベントコンソール] 画面に追加共通除外条件が設定されたことを表す JP1 イベントが表示され、イベント取得フィルターに適用されます。

(2) 追加共通除外条件を共通除外条件に変更する

追加共通除外条件は、追加共通除外条件から共通除外条件へ変更できます。

1. [システム環境設定] 画面で [一覧編集] ボタンをクリックして [イベント取得条件一覧] 画面を表示する。
2. [イベント取得条件一覧] 画面の [共通除外条件群] で共通除外条件に変更したい追加共通除外条件（種別に  アイコンが付いている条件）を選択する。
3. [種別変更] ボタンをクリックする。
4. 種別を変更してもよいかを確認するメッセージが表示されるため、問題なければ [OK] ボタンをクリックする。
5. [システム環境設定] 画面で [適用] ボタンをクリックする。

選択した追加共通除外条件が、共通除外条件に変更されます。

このとき、共通除外条件群 ID が変更されます。変更後の共通除外条件群 ID は、すでに定義されている共通除外条件群 ID の中で最も大きい ID の値に 1 を加えた値です。変更後の共通除外条件群 ID が最大値を超えた場合は、0 から順に使用していない ID を割り当てます。

重要

追加共通除外条件から共通除外条件へ誤って種別を変更してしまった場合は、[適用] ボタンをクリックする前に [システム環境設定] 画面で [閉じる] ボタンをクリックして変更内容をキャンセルしてください。

6.6 表示開始位置を指定してイベントを表示する

短時間に大量の JP1 イベントが発生し、[イベント監視] ページの最大表示件数を超えた場合、古いイベントが見えなくなってしまうことがあります。表示開始位置を指定することで、この見えなくなってしまったイベントを、[イベント監視] ページに表示できます。表示開始位置を指定する場合は、事前に統合監視 DB を有効にする必要があります。統合監視 DB の設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.4.2 統合監視 DB の設定 (Windows の場合)」, 「2.4.2 統合監視 DB の設定 (UNIX の場合)」を参照してください。表示開始位置を指定する場合の表示範囲については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.2 [イベント監視] ページ」を参照してください。

表示開始位置の指定が使用できる画面を次に示します。

- [イベント監視] ページ
- [重要イベント] ページ

ここでは、表示開始位置を指定して、見えなくなった JP1 イベントを表示する手順について説明します。

1. [イベントコンソール] 画面の [開閉] ボタンをクリックして、[表示開始位置指定] 領域を開く。

[表示開始位置指定] 領域は、ログインしたときは表示されません。

[表示開始位置指定] 領域の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.2 [イベント監視] ページ」の「図 3-4 [イベント監視] ページ ([表示開始位置指定] 領域を表示した場合)」を参照してください。

2. スライダーをイベントの表示を開始したい個所に移動する。

指定した表示開始位置より、現在適用しているユーザーフィルターと表示フィルターに一致するイベントを統合監視 DB から取得し、表示します。最大表示件数 (スクロールバッファ) のデフォルトは 500 件です。なお、表示開始位置からのイベント一覧の取得は、新たな表示開始位置を指定するか、[表示キャンセル] ボタンをクリックすることで中断できます。

また、表示開始位置を正確に指定したい場合、[表示開始位置] テキストボックスを用いて指定できます。なお、[表示開始位置] テキストボックスのデフォルトの値は、JP1/IM - Manager にログインする時刻によって異なります。JP1/IM - Manager にログインした時刻が基準時刻より遅かった場合、ログインした日の基準時刻がデフォルトで表示されます。

(例) 基準時刻が 09:00 の場合に、2008/07/08 10:00 にログインしたとき

[表示開始位置] テキストボックスに表示されるデフォルトの値は、2008/07/08 09:00 です。

JP1/IM - Manager にログインした時刻が基準時刻より早かった場合、ログインした前の日の基準時刻がデフォルトで表示されます。

(例) 基準時刻が 09:00 の場合に、2008/07/08 08:00 にログインしたとき

[表示開始位置] テキストボックスに表示されるデフォルトの値は、2008/07/07 09:00 です。

[最新イベント表示] ボタンをクリックすると、表示開始位置を設定する前の状態に戻ります。自動スクロール機能が有効な場合、新しいイベントを受信すると最新のイベントを表示します。新しいイベントを

受信しても [表示開始位置指定] 領域で指定した位置のイベントを表示するように設定したい場合は、自動スクロール機能を無効にしてください。

6.7 表示する JP1 イベントの期間を指定して絞り込む

指定期間のイベント表示を有効にすると、指定期間の JP1 イベントの一覧を表示できます。

指定期間のイベント表示が使用できる画面を次に示します。

- [イベント監視] ページ
- [重要イベント] ページ

指定期間のイベント表示は、すべてのフィルター（イベント取得フィルター、ユーザーフィルター、重要イベントフィルター、表示フィルター）を通過し、繰り返しイベントの集約処理をしたあとの JP1 イベントを対象とします。

ここでは、指定期間のイベント表示機能を有効にし、期間を指定する手順について説明します。

なお、指定期間内の JP1 イベントかどうかは、JP1/IM - Manager に JP1 イベントが到着した時刻と JP1/IM - View が稼働しているホストの現在時刻を比較して判定します。そのため、JP1/IM - Manager と JP1/IM - View の時刻が異なっていた場合、指定期間外の JP1 イベントが表示されることがあります。事前に JP1/IM - Manager と JP1/IM - View の時刻を合わせておくことをお勧めします。

1. [イベントコンソール] 画面のメニューから [オプション] - [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。

2. [イベント表示項目] - [指定期間のイベント表示] の [有効] をチェックする。

[基準時刻] および [表示期間] が活性となります。

3. [基準時刻] および [表示期間] 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。

基準時刻と現在時刻の大小関係により、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。

- JP1/IM - View が稼働しているホストの現在時刻が基準時刻より大きい場合
（表示期間-1）日前の基準時刻から、明日の基準時刻までの範囲。
- JP1/IM - View が稼働しているホストの現在時刻が基準時刻より小さい場合
表示期間前の基準時刻から、今日の基準時刻までの範囲。

終端の基準時刻は、範囲に含まれません。

例えば、現在時刻が「09:15」の時に表示期間を「2 日分」、基準時刻に「09:30」を指定した場合、「2 日前」の「09:30」から「今日」の「09:29」までの JP1 イベントの一覧を表示します。

[表示期間] 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。

4. [OK] をクリックする。

設定した内容（指定期間のイベント表示）が有効となり、[ユーザー環境設定] 画面が閉じます。[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。

指定期間のイベント表示機能が有効な場合、[イベントコンソール] 画面の [指定期間のイベント表示] チェックボックス、または [イベントコンソール] 画面のメニューから [表示] - [指定期間のイベント表示] を選択することで、指摘期間のイベント表示の適用と未適用を切り替えられます。

再ログインした場合に [ユーザー環境設定] 画面の指定期間のイベント表示機能が有効だったときは、[指定期間のイベント表示] チェックボックスと [指定期間のイベント表示] メニューのチェックを付け、指定期間のイベント表示を適用して各ページのイベント一覧を表示します。無効だった場合は、[指定期間のイベント表示] チェックボックスと [指定期間のイベント表示] メニューを非表示にし、指定期間のイベント表示を適用しないで各ページのイベント一覧を表示します。

指定期間のイベント表示の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.18 指定期間のイベント表示」を参照してください。

6.8 JP1 イベントを検索する

さまざまな条件で JP1 イベントを検索し、検索条件に合った JP1 イベントを画面に表示できます。

ここでは、検索方法および検索結果の表示について説明します。

検索の機能詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.6 イベント検索」を、イベント検索で使用する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「3.25 [イベント検索条件設定] 画面」を参照してください。

6.8.1 検索の方法

次に JP1 イベントの検索方法について説明します。

統合監視 DB を有効にすると、検索対象がイベント DB と統合監視 DB から選択できるようになります。統合監視 DB の設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.4.2 統合監視 DB の設定 (Windows の場合)」, 「2.4.2 統合監視 DB の設定 (UNIX の場合)」を参照してください。

(1) 検索手順

JP1 イベントを検索する手順は次のとおりです。

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検索条件として利用する場合は、[イベントコンソール] 画面のイベント一覧から JP1 イベントを選択する。
2. [イベントコンソール] 画面で [表示] - [イベント検索] を選択する。または [イベントコンソール] 画面の [イベント検索] ページで [イベント検索] ボタンをクリックする。
[イベント検索条件設定] 画面が表示されます。
3. [イベント検索条件設定] 画面で検索条件を設定する。
[イベント検索条件設定] 画面では次の項目を設定します。
 - 検索対象の設定
統合監視 DB を使用する場合、[イベント検索条件設定] 画面に [検索対象] が表示され、統合監視 DB またはイベント DB のどちらかを選択できます。統合監視 DB を使用しない場合、[検索対象] の項目は表示されません。イベント DB にある JP1 イベントを検索します。
 - 検索ホスト名の入力
[検索ホスト名] に検索対象のホスト名 (イベントサーバ名) を入力します。
接続しているホスト名がデフォルトで指定されます。
なお、統合監視 DB を使用する場合に [検索対象] で統合監視 DB を選択したときは、[検索ホスト名] の項目が非活性になります。

指定したホスト名は、マネージャーでアドレス解決します。マネージャー上で解決できるホスト名を指定してください。

特に、ファイアウォール環境で、ファイアウォールの外側のビューアーからイベントを検索する場合は、注意が必要です。ファイアウォール環境では、ファイアウォールの外側からと内側からでは、同じホストの IP アドレスが異なって見える場合があります。そのため、ファイアウォールの外側のビューアーから IP アドレスを指定してイベントを検索する場合は、マネージャー上で解決できる IP アドレスを指定してください。

また、複数の LAN に接続したエージェントに対して代表ホスト以外の NIC 経由で接続する場合も、IP アドレスを指定してください。

- 検索方向の指定

統合監視 DB または イベント DB を検索する方向を指定します。

イベントの検索方向が、[過去方向]、[未来方向] のどちらか指定します。なお、[過去方向] がデフォルトで指定されます。

詳細については、「[6.8.1\(2\) イベントの検索方向](#)」を参照してください。

- 条件群の設定

イベント検索の条件を区別するために、条件群に名前を付けます。

条件群は複数設定でき、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）

検索したい JP1 イベント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。

選択できる項目は、検索対象の設定によって異なります。

検索対象が イベント DB の場合に選択できる項目は、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、開始時刻、終了時刻、登録時刻、到着時刻、対処状況、アクション^{※2}、および固有の拡張属性です。

検索対象が 統合監視 DB の場合に選択できる項目は、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、開始時刻、終了時刻、登録時刻、到着時刻、対処状況、アクション

ン、固有の拡張属性、メモ^{※2}、重大度変更^{※3}、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}です。

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 表示メッセージ変更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。

なお、発生元ホスト名、登録ホスト名、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、事象種別、ユーザー名、メッセージ、プロダクト名、固有の拡張属性、メモ、監視抑止 ID、およびメッセージ(変更後)については、正規表現でも指定できます。正規表現での指定方法については、「6.8.1(3) 正規表現での指定方法」を参照してください。

4. [OK] ボタンをクリックする。

[イベント検索] ページが表示され、検索が開始するとページのタブに（検索中）が表示されます。検索結果は、[イベントコンソール] 画面の [イベント検索] ページに検索条件と一致したイベントが順次、表示されます。

イベント検索をキャンセルする場合は、[検索キャンセル] ボタンをクリックします。間違った検索条件でイベント検索を実行してしまった場合や、取得したいイベントを見つけた時点でイベント検索を中断できます。

(2) イベントの検索方向

条件の設定に従った範囲を、検索方向を指定して検索できます。1回の検索で取得できる件数は、[ユーザー環境設定] 画面で変更できます。1回の検索で取得できなかったイベントは [イベントコンソール] 画面の [イベント検索] ページで [次イベント検索] ボタンをクリックすることで取得、表示できます。

イベントの検索方向に [過去方向] を指定すると、統合監視 DB または イベント DB に登録された JP1 イベントの最後尾から（新しいイベントから古いイベント方向に）検索します。[過去方向] を指定してイベントを検索した場合、新しいイベントから順に取得、表示します。[次イベント検索] ボタンをクリックすると、表示しているイベントの上に [次イベント検索] ボタンで選択したイベントを表示します。なお、表示は、古い順（取得したイベントのうち、古いイベントが上に、新しいイベントが下に表示される）となるため、注意してください。

イベントの検索方向に [未来方向] を指定すると、統合監視 DB または イベント DB に登録された JP1 イベントの先頭から (古いイベントから新しいイベント方向に) 検索します。[未来方向] を指定してイベントを検索した場合、古いイベントから順に取得します。[次イベント検索] ボタンをクリックすると、表示しているイベントの下に [次イベント検索] ボタンで選択したイベントを表示します。

[6.8.2 検索結果の表示] の例を参考にして、イベント検索の動作を確認してください。

(3) 正規表現での指定方法

[イベント検索条件設定] 画面で設定する検索条件として、正規表現を指定できます。正規表現を指定できるのは、発生元ホスト名、登録ホスト名、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、事象種別、ユーザー名、メッセージ、プロダクト名、固有の拡張属性、メモ、監視抑止 ID、およびメッセージ(変更後)です。

[イベント検索条件設定] 画面で検索条件として正規表現を指定するには、[条件一覧] のテキストボックスに正規表現で検索条件を指定し、右側のリストボックスから「正規表現」を選択します。なお、固有の拡張属性に対して正規表現を指定するには、[固有の拡張属性条件詳細設定] 画面を使用します。

なお、使用できる正規表現の種類は検索先ホストの JP1/Base の設定に準じます。詳細については、マニュアル「JP1/Base 運用ガイド」のセットアップの章、正規表現の説明を参照してください。

6.8.2 検索結果の表示

イベントの検索結果は、[イベントコンソール] 画面の [イベント検索] ページに表示されます。

1 回のイベント検索で取得できるイベントの件数は、[ユーザー環境設定] 画面で設定できます。[ユーザー環境設定] 画面でイベント取得件数を設定する方法については、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。

イベント検索時に、1 回で取得されなかったイベントを表示するには、[次イベント検索] ボタンをクリックします。表示される内容は、検索方向、および各条件で設定した範囲によって異なります。

イベント検索結果の表示例を次に示します。

(前提条件)

- ・ 1 回のイベント検索で取得できるイベントは 20 件。
- ・ イベント DB には次に示すイベントだけが格納されている。

図 6-4 イベント DB に格納されているイベント

```
2000 07/01 00:01:00 イベント01
2000 07/01 00:02:00 イベント02
2000 07/01 00:03:00 イベント03
2000 07/01 00:04:00 イベント04
2000 07/01 00:05:00 イベント05
(中略)
2000 07/01 00:56:00 イベント56
2000 07/01 00:57:00 イベント57
2000 07/01 00:58:00 イベント58
2000 07/01 00:59:00 イベント59
2000 07/01 01:00:00 イベント60
```

(例 1)

[イベント検索条件設定] 画面の [検索方向] で [過去方向] を指定すると、イベント一覧には、イベント DB に登録された JP1 イベントの最後尾から 20 件までの JP1 イベントが表示されます。

図 6-5 イベントの最後尾から 20 件表示

```
2000 07/01 00:41:00 イベント41
2000 07/01 00:42:00 イベント42
(中略)
2000 07/01 00:59:00 イベント59
2000 07/01 01:00:00 イベント60
```

[次イベント検索] ボタンをクリックすると、次の 20 件のイベントがすでに表示されているイベントの上に追加して表示されます。

図 6-6 [次イベント検索] ボタンクリック後の表示

```
2000 07/01 00:21:00 イベント21
2000 07/01 00:22:00 イベント22
(中略)
2000 07/01 00:39:00 イベント39
2000 07/01 01:40:00 イベント40
2000 07/01 00:41:00 イベント41
2000 07/01 00:42:00 イベント42
(中略)
2000 07/01 00:59:00 イベント59
2000 07/01 01:00:00 イベント60
```

} 追加

(例 2)

[イベント検索条件設定] 画面の [検索方向] で [未来方向] を指定すると、イベント一覧には、イベント DB に登録された JP1 イベントの先頭から 20 件までの JP1 イベントが表示されます。

図 6-7 イベントの先頭から 20 件表示

```
2000 07/01 00:01:00 イベント01
2000 07/01 00:02:00 イベント02
(中略)
2000 07/01 00:19:00 イベント19
2000 07/01 00:20:00 イベント20
```

[次イベント検索] ボタンをクリックすると、次の 20 件のイベントがすでに表示されているイベントの下に追加して表示されます。

図 6-8 [次イベント検索] ボタンクリック後の表示

```
2000 07/01 00:01:00 イベント01
2000 07/01 00:02:00 イベント02
(中略)
2000 07/01 00:19:00 イベント19
2000 07/01 00:20:00 イベント20
2000 07/01 00:21:00 イベント21
2000 07/01 00:22:00 イベント22
(中略)
2000 07/01 00:39:00 イベント39
2000 07/01 00:40:00 イベント40
```

} 追加

6.9 JP1 イベントの情報を運用に合わせてカスタマイズする

JP1 イベントの情報は、運用に合わせてカスタマイズできます。

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）

イベント拡張属性定義ファイル（拡張ファイル）を設定すると、[イベントコンソール] 画面のイベント一覧に、固有の拡張属性を任意の項目名で表示できます。

イベント拡張属性定義ファイル（拡張ファイル）の設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「5.11 固有の拡張属性の表示および指定の設定」を参照してください。

ここでは、イベント拡張属性定義ファイル（拡張ファイル）に定義した固有の拡張属性を、[ユーザー環境設定] 画面で表示項目に追加して、[イベントコンソール] 画面のイベント一覧に表示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] - [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。
2. [イベント表示項目] - [表示項目] の [表示できる項目] ボックスから、イベント拡張属性定義ファイル（拡張ファイル）に定義した固有の拡張属性を選択する。
[表示できる項目] ボックスには、イベント拡張属性定義ファイル（拡張ファイル）に定義した固有の拡張属性が項目名で表示されます。
3. [→] ボタンをクリックして、選択した項目を [表示項目] ボックスに移動する。
[表示項目] ボックス内の項目の表示順序は、イベント一覧での表示順序を表します。表示順序を変更したい場合は、項目を選択して、[上へ移動] ボタンまたは [下へ移動] ボタンをクリックして、項目名を移動してください。
4. [OK] をクリックする。
[ユーザー環境設定] 画面が閉じます。[イベントコンソール] 画面のイベント一覧に固有の拡張属性が表示されます。

6.9.2 JP1 イベントの固有の拡張属性を表示する（イベント情報のマッピング）

基本属性または共通の拡張属性の項目にマッピングして、イベント一覧の表示項目（基本属性または共通の拡張属性）の欄に、固有の拡張属性の内容を表示できます。

例を次に示します。

マッピング定義の設定

次に示すマッピング定義が設定されています。

イベント情報マッピング定義 1

固有の拡張属性「LOGHOST」を「登録ホスト名」にマッピング
マッピング対象のイベント ID：12E0

イベント情報マッピング定義 2

固有の拡張属性「LOGTIME」を「到着時刻」にマッピング
マッピング対象のイベント ID：12E0

発行されたイベント

次の内容のイベントが発行されました。

表 6-6 イベント発行内容

項番	属性	内容
1	重大度	エラー
2	登録時刻	2001/10/30 17:47:31
3	到着時刻	2001/10/30 17:47:39
4	登録ホスト名	host_A
5	ユーザー名	jp1nps
6	イベント ID	000012E0
7	メッセージ	KAJC391-E ...
8	LOGHOST	loghost_1
9	LOGTIME	1003976997*

注※ 時刻形式では、2001/10/25 11:29:57 になります。

【イベントコンソール】画面での表示

通常、【イベントコンソール】画面のイベント一覧では、上記の表の項番 1～項番 7 の内容が表示されますが、項番 8 を項番 4 に、項番 9 を項番 3 にマッピングしているため、次のように表示されます。

表 6-7 【イベントコンソール】画面での表示

重大度	登録時刻	到着時刻	登録ホスト名	ユーザー名	イベント ID	メッセージ
エラー	10/25 17:47:31	# 10/25 11:29:57	# loghost_1	jp1nps	000012E0	KAJC391-E ...

固有の拡張属性を表示するには、【イベント情報マッピング定義】画面で表示項目と固有の拡張属性とをマッピングします。【イベント情報マッピング定義】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。

メモ

イベント情報マッピングと発生元ホストのマッピングの違いについて

イベント情報マッピングは、JP1 イベントの拡張属性の属性値をイベント一覧の表示項目の属性にマッピングして表示する機能です。イベント一覧の「登録ホスト名」に、別の属性値を表示できます。ただし、この機能は、イベント一覧上の表示の変更に限るため、アクションやイベント関連などのイベント条件には利用できません。

これに対し、発生元ホストのマッピングは、JP1/IM - Manager が取得した JP1 イベントのホスト名と発生元ホスト名を登録し、JP1 イベントを監視・管理するための機能です。イベント一覧の「発生元ホスト名」に表示でき、アクションやイベント関連などのイベント条件にも利用できます。ただし、統合監視 DB を使用し、発生元ホストのマッピングを有効にする必要があります。

固有の拡張属性をマッピングする手順は次のとおりです。

1. [イベントコンソール] 画面で [オプション] - [イベント情報マッピング定義] を選択する。
[イベント情報マッピング定義] 画面が表示されます。
[定義一覧] には、現在設定されているマッピング定義情報の一覧が表示されています。
最大で 16 個のマッピング定義ができます。
2. イベント情報マッピングを有効にするために、[マッピング] の [する] を選択する。
3. 新規にマッピングを定義するには、[追加] ボタンをクリックする。定義済みのマッピング情報を変更するには、[定義一覧] リストの項目を選択してから [編集] ボタンをクリックするか、[定義一覧] リストの項目をダブルクリックする。
[イベント情報マッピング詳細定義] 画面が表示されます。
4. [表示項目] から、イベント一覧のどの表示項目に固有の拡張属性をマッピングするかを選択する。
選択できる項目は、[ユーザー環境設定] 画面で選択できる次の項目です。
発行元プロセス ID, 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, 発行元イベント DB 内通し番号, 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, 事象種別, 開始時刻, 終了時刻
 - 指定例：登録ホスト名
5. [固有の拡張属性名] に、マッピングする固有の拡張属性の名前を指定する。
指定できる文字は、32 文字までの、半角英大文字、半角数字、および半角のアンダースコアです。拡張属性を表す「E」は不要です。
一つの表示項目には、一つだけの固有の拡張属性をマッピングできます。

到着時刻，開始時刻，および終了時刻に固有の拡張属性をマッピングするときは，属性値が数値（UTC 1970 年 1 月 1 日 00:00:00 からの秒数 0～4,102,444,799）である属性名を指定します。数値以外，または範囲外の数値を持つ属性を指定した場合は，元の属性が表示されます。

- 指定例：LOGHOST

6. [イベント ID] に，マッピングする JP1 イベントのイベント ID を指定する。

指定できる文字は，1,000 文字までの，A～F または a～f の半角英字，半角数字，および半角のコンマです。16 進数で指定します。指定できる範囲は，00000000～7FFFFFFF です。

複数のイベント ID を指定する場合は，コンマで区切って 100 個まで指定できます。

- 指定例 1：3FFF
- 指定例 2：12345B,7FFFFFFF

7. [OK] ボタンをクリックする。

[イベント情報マッピング詳細定義] 画面が閉じ，設定した内容が [イベント情報マッピング定義] 画面に反映されます。

8. [イベント情報マッピング定義] 画面で [適用] ボタンをクリックする。

[適用] ボタンをクリックされたあとに到着したイベントから，このマッピング定義に沿って固有の拡張属性が表示されます。

表示フィルター，重要イベントフィルター，ユーザーフィルターを使用するときは，マッピングした固有の拡張属性を指定して JP1 イベントをフィルタリングできます。

固有の拡張属性が表示されているときは，表示された属性値の先頭に「#」（シャープ記号と半角の空白）が表示されます。

表示されている固有の拡張属性をフィルター条件として指定する場合は，「#」を入力する必要はありません。

また，[ユーザー環境設定] 画面の [カラーリング] で [有効] チェックボックスをチェックしていた場合，イベントの重大度に基づいてイベントの行に背景色がつきます。

[イベント情報マッピング定義] 画面で設定内容を変更した場合は，その変更内容が，同じ JP1/IM - Manager に接続されているすべての JP1/IM - View のイベント一覧に反映されます。

マッピングされる前の情報を参照するには，マッピングされたイベントを選択してから [イベント詳細] 画面を表示します。[イベント詳細] 画面に，マッピングされる前の情報が表示されます。なお，イベント拡張属性定義ファイルを使用すれば，[イベント詳細] 画面に，固有の拡張属性を表示できます。詳細については，次の説明を参照してください。

イベント拡張属性定義ファイルを使った固有の拡張属性の表示について

参照先：マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.14 ユーザー独自のイベント属性の表示」

イベント拡張属性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「イベント拡張属性定義ファイル」(2. 定義ファイル)

なお、固有の拡張属性をマッピングする場合には、次の点に注意してください。

- イベント検索では、統合監視 DB またはイベントサービスのイベント DB に対して検索がかけられるため、マッピングされる前のイベントに対して検索が行われます。したがって、検索結果には、マッピング情報は反映されません。マッピング対象のイベントを検索する場合は、[イベント検索条件設定] 画面の [固有の拡張属性] 欄を使用して、マッピングする固有の拡張属性の情報を指定します。
- [関連イベント一覧] 画面に表示される関連イベントは、イベント検索の結果であるため、マッピング情報が反映されません。
- 固有の拡張属性がマッピングされたイベントを選択してから [イベント検索条件設定] 画面などで [選択イベント条件入力] ボタンをクリックした場合は、マッピング先の表示項目の属性および固有の拡張属性の値は、条件一覧に入力されません。

6.9.3 条件に一致する JP1 イベントにユーザー独自の固有の拡張属性を付加する

JP1/Base の属性付加設定ファイルから JP1 イベントにユーザー固有の情報を拡張属性として追加する手順を説明します。

機能については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.12 固有の属性付加」を参照してください。

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}
```

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。

6.9.4 JP1 イベントの重大度を変更する

統合監視 DB を使用する場合, 重大度変更機能を設定すると, イベントの重大度を変更できます。

統合監視 DB の設定方法については, マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.4.2 統合監視 DB の設定 (Windows の場合)」, 「2.4.2 統合監視 DB の設定 (UNIX の場合)」を参照してください。

また, 重大度変更機能を設定する方法は, マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「5.13 重大度変更機能の設定」を参照してください。

ここでは, イベントの重大度を変更する手順を次に示します。

(1) [重大度変更定義設定] 画面から重大度変更定義を設定する

[重大度変更定義設定] 画面から重大度変更定義を設定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. 設定する内容に合わせて, [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

[重大度変更定義設定] 画面が表示され, 新しい重大度変更定義を設定できます。

[編集] ボタンをクリックした場合

[重大度変更定義設定] 画面が表示され, 選択した重大度変更定義の設定を編集できます。

[複製] ボタンをクリックした場合

選択した重大度変更定義が複製され、[重大度変更定義一覧] 画面に追加されます。複製された重大度変更定義は、名称の先頭に「コピー」が追加されます。

[削除] ボタンをクリックした場合

選択した重大度変更定義が削除されます。
削除の場合、手順 4 は実施しません。

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. 設定を反映してもよいかを確認するメッセージが表示されるため、問題なければ [はい] ボタンをクリックする。

設定した重大度変更定義が有効になります。

(2) 重大度変更定義ファイルから重大度変更定義を設定する

重大度変更定義ファイルから重大度変更定義を設定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. 重大度変更定義ファイルに、イベントの重大度変更の定義を記述する。

重大度変更はシステム単位で定義します。重大度は、「緊急 (Emergency)」、「警戒 (Alert)」、「致命的 (Critical)」、「エラー (Error)」、「警告 (Warning)」、「通知 (Notice)」、「情報 (Information)」、「デバッグ (Debug)」の範囲で変更できます。

重大度変更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「重大度変更定義ファイル (jcochsev.conf)」(2. 定義ファイル) を参照してください。

重大度変更定義ファイルに設定する内容の例

```
DESC_VERSION=2
def 重大度変更1
cmt コメント
```

```
define enable
cnd
B.ID IN 100 200
E.SEVERITY IN Warning
B.SOURCESERVER IN hostA hostB hostC
end-cnd
sev Emergency
end-def
```

3. jco_spmd_reload コマンドを実行するか、JP1/IM - Manager を再起動する。

ただし、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。

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。

変更後の JP1 イベントの重大度は、イベント一覧の [重大度] に表示します。変更前の JP1 イベントの重大度は、イベント一覧の [重大度(変更前)] に表示します。また、重大度を変更した JP1 イベントは、イベント一覧の [重大度変更] にアイコンを表示します。

イベント基盤サービスは、マネージャー上のイベントサービスから受信した JP1 イベントの重大度を変更し、統合監視 DB に登録します。その際、イベントサービスのイベント DB の内容は変更されません。

また、マッピング定義を重大度の変更に使用することがあります。マッピング定義を使用すると、イベント一覧の [重大度] に、別の属性を表示できます。

(3) 運用中に発生したイベントを使って追加重大度変更定義を設定する

システム運用中に変更したいイベントを選択して [追加重大度変更定義設定] 画面から重大度変更定義の条件を追加できます。

イベントを選択して定義を追加した場合は、追加した定義を最優先にするために [重大度変更定義一覧] 画面に表示される定義の先頭に登録されます。

[追加重大度変更定義設定] 画面から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、重大度を変更したいイベントを選択し、右クリックして表示されるポップアップメニューから [重大度変更定義を設定] を選択する。

[追加重大度変更定義設定] 画面が表示されます。

2. [追加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て、[変更後の重大度] から、変更後の重大度を選択して、編集します。

3. [OK] ボタンをクリックする。

追加重大度変更定義が [重大度変更定義一覧] 画面に反映されます。運用中に追加した重大度変更定義には、種別にアイコンが表示されます。

(4) 追加重大度変更定義を重大度変更定義に変更する

システム運用中に追加した追加重大度変更定義は、重大度変更定義に変更できます。

1. [イベントコンソール] 画面のメニューから [オプション] - [重大度変更定義] を選択して [重大度変更定義一覧] 画面を表示する。
2. [重大度変更定義一覧] 画面の [重大度変更定義一覧] で重大度変更定義に変更したい追加重大度変更定義（種別にアイコンが付いている定義）を選択する。
3. [種別変更] ボタンをクリックする。
4. 種別を変更してもよいかを確認するメッセージが表示されるため、問題なければ [はい] ボタンをクリックする。
選択した追加重大度変更定義が、重大度変更定義に変更されます。
5. [重大度変更定義一覧] 画面の [適用] ボタンをクリックする。
6. 設定を反映してもよいかを確認するメッセージが表示されるため、問題なければ [はい] ボタンをクリックする。
追加した重大度変更定義が有効になります。

6.9.5 JP1 イベントの表示メッセージを変更する

統合監視 DB を使用する場合、表示メッセージ変更機能を設定すると、イベントの表示メッセージを変更できます。

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_spm�_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。

統合監視 DB の設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.4.2 統合監視 DB の設定 (Windows の場合)」, 「2.4.2 統合監視 DB の設定 (UNIX の場合)」を参照してください。

また、表示メッセージ変更機能を設定する方法は、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「5.14 表示メッセージ変更機能の設定」を参照してください。

ここでは、イベントの表示メッセージを変更する手順を次に示します。

(1) 【表示メッセージ変更定義設定】画面から表示メッセージ変更定義を設定する

【表示メッセージ変更定義設定】画面から表示メッセージ変更定義を設定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、jimbupdate 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。jimbupdate 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「jimbupdate」(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. 設定する内容に合わせて、【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
【表示メッセージ変更定義設定】画面が表示され、新しい表示メッセージ変更定義を設定できます。
- 【編集】ボタンをクリックした場合
【表示メッセージ変更定義設定】画面が表示され、選択した表示メッセージ変更定義の設定を編集できます。
- 【複製】ボタンをクリックした場合
選択した表示メッセージ変更定義が複製され、【表示メッセージ変更定義一覧】画面に追加されます。複製された表示メッセージ変更定義は、名称の先頭に「コピー」が追加されます。
- 【削除】ボタンをクリックした場合
選択した表示メッセージ変更定義が削除されます。
削除の場合、手順 4 は実施しません。

4. 【表示メッセージ変更定義設定】画面で、メッセージの設定をする。

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、メッセージの文字数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. 設定を反映してもよいかを確認するメッセージが表示されるため, 問題なければ [はい] ボタンをクリックする。

設定した表示メッセージ変更定義が有効になります。

(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

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. 表示メッセージ変更定義ファイルに, イベントの表示メッセージ変更の定義を記述する。

表示メッセージ変更定義はシステム単位で定義します。

表示メッセージ変更定義は, 表示メッセージを変更する JP1 イベントのイベント条件と, 変更後のメッセージ形式を指定します。

また, イベント引き継ぎ情報の変換機能を使うと, 文字列や数値の表示形式を統一して, イベント一覧に見やすく表示できます。

表示メッセージ変更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定義ファイル (jcochmsg.conf)」(2. 定義ファイル) を参照してください。

表示メッセージ変更定義ファイルに設定する内容の例

```
DESC_VERSION=1
def 表示メッセージ変更 1
cmt コメント 1
define enable
addflag false
end
```

```
B.ID IN 100 200
E.SEVERITY IN Warning
B.SOURCESERVER IN hostA hostB hostC
end-cnd
msg $EVDATE $EVTIME DB サーバで障害が発生しました
end-def
```

3. jco_spmd_reload コマンドを実行するか、JP1/IM - Manager を再起動する。

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。

変更後の JP1 イベントのメッセージは、イベント一覧の [メッセージ(変更後)] に表示します。変更前の JP1 イベントのメッセージは、イベント一覧の [メッセージ] に表示します。また、メッセージを変更した JP1 イベントは、イベント一覧の [表示メッセージ変更] にアイコン を表示します。

イベント基盤サービスは、マネージャー上のイベントサービスから受信した JP1 イベントのメッセージを変更し、「メッセージ(変更後)」に格納して統合監視 DB に登録します。オリジナルの「メッセージ」は変更しません。

(3) 運用中に発生したイベントを使って追加表示メッセージ変更定義を設定する

システム運用中に変更したいイベントを選択して [追加表示メッセージ変更定義設定] 画面から表示メッセージ変更定義の条件を追加できます。

イベントを選択して定義を追加した場合は、追加した定義を最優先にするために [表示メッセージ変更定義一覧] 画面に表示される定義の先頭に登録されます。

[追加表示メッセージ変更定義設定] 画面から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、表示メッセージを変更したいイベントを選択し、右クリックして表示されるポップアップメニューから [表示メッセージ変更定義を設定] を選択する。

[追加表示メッセージ変更定義設定] 画面が表示されます。

2. [追加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。

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、メッセージの文字数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。

3. [OK] ボタンをクリックする。

追加表示メッセージ変更定義が [表示メッセージ変更定義一覧] 画面に反映されます。運用中に追加した表示メッセージ変更定義には、種別にアイコンが表示されます。

(4) 追加表示メッセージ変更定義を表示メッセージ変更定義に変更する

システム運用中に追加した追加表示メッセージ変更定義は、表示メッセージ変更定義に変更できます。

1. [イベントコンソール] 画面のメニューから [オプション] - [表示メッセージ変更定義] を選択して [表示メッセージ変更定義一覧] 画面を表示する。
2. [表示メッセージ変更定義一覧] 画面の [表示メッセージ変更定義一覧] で表示メッセージ変更定義に変更したい追加表示メッセージ変更定義 (種別にアイコンが付いている定義) を選択する。
3. [種別変更] ボタンをクリックする。
4. 種別を変更してもよいかを確認するメッセージが表示されるため、問題なければ [はい] ボタンをクリックする。
選択した追加表示メッセージ変更定義が、表示メッセージ変更定義に変更されます。
5. [表示メッセージ変更定義一覧] 画面の [適用] ボタンをクリックする。
6. 設定を反映してもよいかを確認するメッセージが表示されるため、問題なければ [はい] ボタンをクリックする。
追加した表示メッセージ変更定義が有効になります。

6.10 イベントの大量発生に対処する

JP1 イベントが大量に発生した場合の対処方法には、次に示す二つの方法があります。

エージェントからのイベント転送を抑制する方法 (JP1/Base のイベント転送抑制機能)

JP1 イベントが大量に発生しているエージェントからのイベント転送を抑制して、該当のエージェントの監視を中止します。

イベントをマネージャーで集約する方法 (JP1/IM - Manager の繰り返しイベントの監視抑制機能)

繰り返しイベント条件を設定して、条件に一致する JP1 イベントをイベント一覧に集約して表示したり、自動アクションの実行を抑制したりします。

ここでは、それぞれの方法でイベントの大量発生に対処する手順を説明します。

JP1 イベントが大量に発生した場合の対処方法を、あらかじめ運用手順で決めておくことをお勧めします。

大量発生イベントの監視抑制の概要については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.5.1 大量発生イベントの監視抑制の仕組み」を参照してください。

また、JP1/Base からマネージャーへ転送する JP1 イベントの設定、およびマネージャーでの JP1 イベントのフィルタリングの設定についても、検討してください。JP1/Base が転送する JP1 イベントの設定については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「13.1.2 マネージャーに転送する JP1 イベントの検討」、マネージャーのフィルタリングの設定については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「13.1.3 JP1 イベントのフィルタリング設定の検討」を参照してください。

なお、イベントをマネージャーで集約する方法でイベントの大量発生に対処する場合は、事前に統合監視 DB を構築し、統合監視 DB および繰り返しイベントの監視抑制をマネージャーで有効に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 構築ガイド」の「5.3 繰り返しイベントの監視抑制の設定」を参照してください。

6.10.1 イベントの大量発生に対処する場合と備える場合の流れ

イベントの大量発生を検知した場合は、[イベントコンソール] 画面のイベント一覧に表示されるイベントを基に、該当するエージェントのイベント転送を抑制したり、繰り返しイベント条件を設定してイベントを集約したりします。過去にイベントが大量発生したことがある場合、または一時に大量発生することが予想される場合は、イベント転送を自動で抑制するためしきい値を設定したり、繰り返しイベント条件を事前に設定したりして、イベントの大量発生に備えます。

それぞれの流れを次の図に示します。

図 6-9 イベントが大量に発生したことを検知した場合の対処の流れ

6.10.2

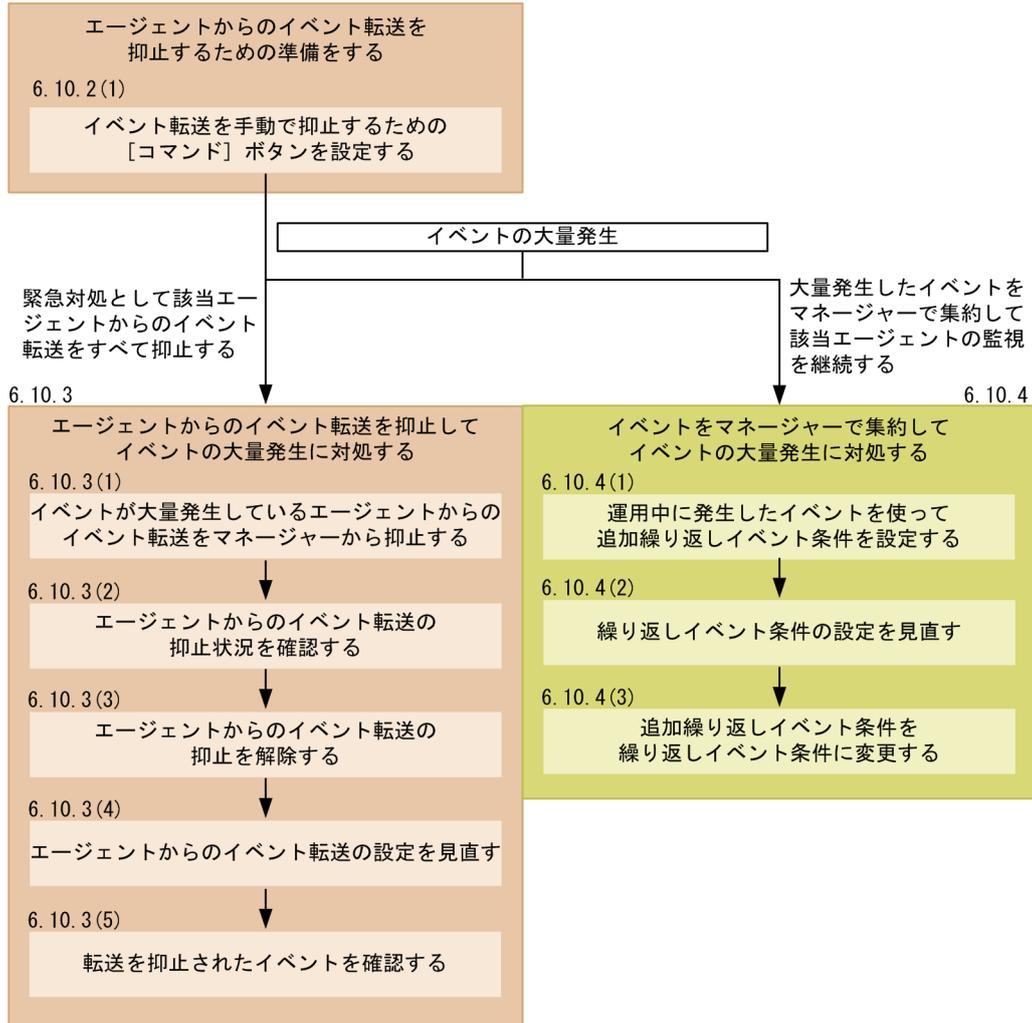
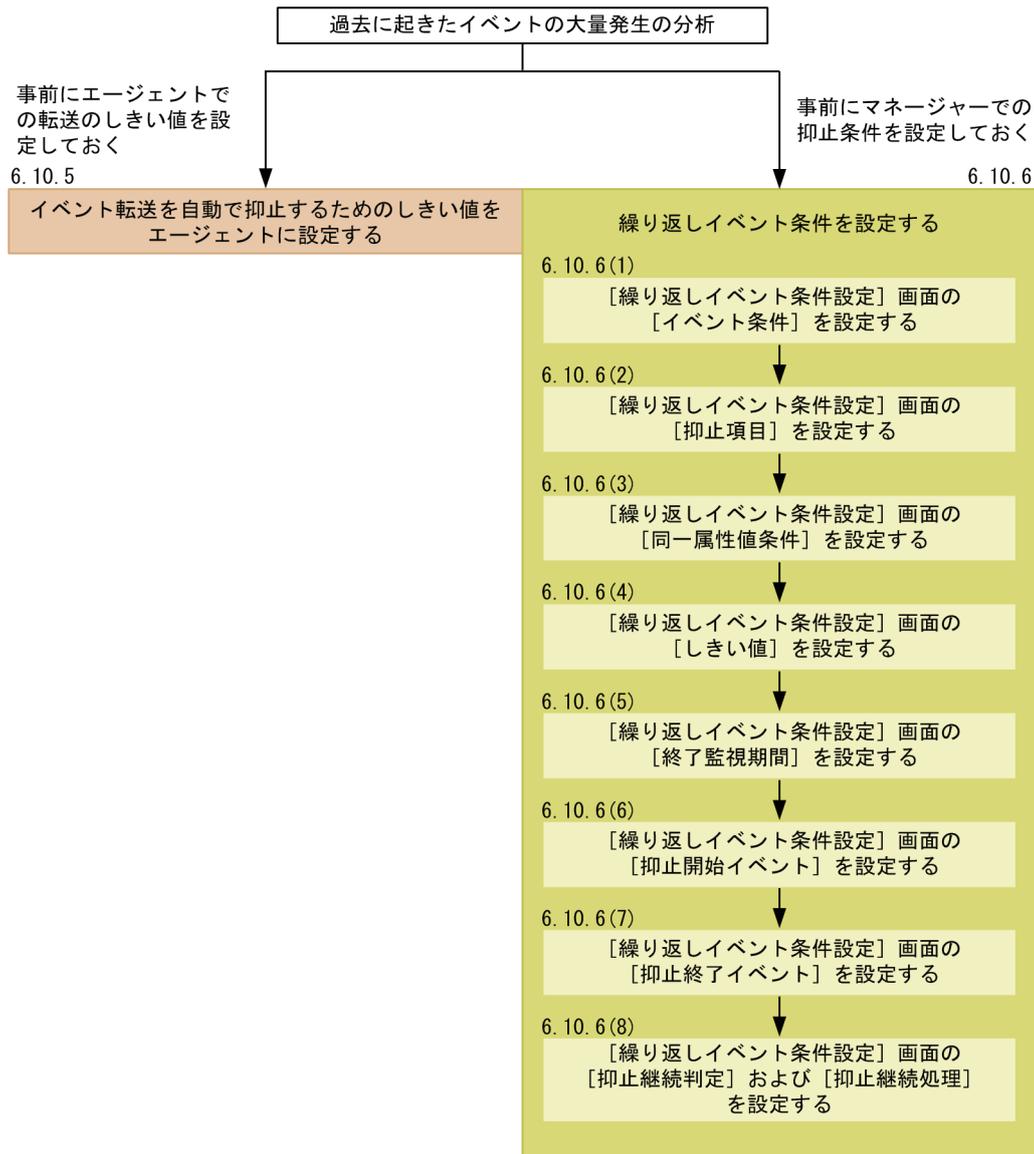


図 6-10 過去にイベントが大量発生したことがある場合、または一時に大量発生することが予想される場合の対処の流れ



6.10.2 エージェントからのイベント転送を抑止するための準備をする

エージェントからのイベント転送を抑止するための準備として、イベント転送を抑止したり、解除したりする [コマンド] ボタンを設定します。[コマンド] ボタンを設定することで、イベントの大量発生に対処する際に、管理者のコマンド入力を少なくし操作ミスを防止できます。

ここで設定する [コマンド] ボタンと各ボタンの動作内容を、次に示します。

「ALL 抑止」ボタン

- イベントが大量発生したエージェントに対して、そのエージェントからのすべてのイベント転送を抑止する。

- コマンド実行時は確認画面を表示し、管理者が確認し実行する。
- エージェントの選択は、管理者が JP1/IM - View のコンソール画面から選択した 1 つのイベントから自動でホスト名を抽出する。

「抑止解除」ボタン

- 障害対策の終了などを契機に該当エージェントのイベント監視（イベント転送）を再開する。
- コマンド実行時は確認画面を表示し、管理者が確認し実行する。
- エージェントの選択は、管理者が JP1/IM - View のコンソール画面から選択した 1 つのイベントから自動でホスト名を抽出する。

「抑止確認」ボタン

- 大量発生イベントの転送抑止の状況を表示して確認する。

コマンド実行に必要な条件を次に示します。

- JP1/IM - View からコマンドを実行する JP1 ユーザーが認証サーバに登録されている。
- JP1/IM - View からコマンドを実行する JP1 ユーザーに、次のどちらかの JP1 権限レベルが与えられている。
 - JP1_Console_Admin
 - JP1_Console_Operator
- JP1/Base の構成管理を使ったシステム構成の定義が済んでいる。
- マネージャーホストで JP1 ユーザーと OS ユーザーのマッピングが済んでいる。
- マネージャーホストで JP1 ユーザーとマッピングする OS ユーザーが、jevagtfw コマンドの実行権限を所有している。

jevagtfw コマンドの詳細については、マニュアル「JP1/Base 運用ガイド」のコマンドの章を参照してください。

コマンド実行環境の設定については、Windows の場合、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.16 コマンド実行環境の設定 (Windows の場合)」、UNIX の場合、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「2.15 コマンド実行環境の設定 (UNIX の場合)」を参照してください。

(1) イベント転送を手動で抑止するための [コマンド] ボタンを設定する

1. JP1/IM - Manager に接続しているすべての JP1/IM - View を終了する。
2. jcoimdef コマンドを実行して、[コマンド] ボタンを有効にする。

コマンド指定例

```
jcoimdef -i -cmdbtn ON
```

コマンド実行結果で、S_CMDBTN がONであることを確認します。-i オプションを指定しているため、コマンド実行後直ちに [コマンド] ボタンが有効になります。

3. [コマンド] ボタンとして使用するコマンドを設定する。

コマンドボタン定義ファイルを作成します。

定義例 (Windows の場合)

```
def
usr [コマンド] ボタンを使用するJP1ユーザー名

btn ALL抑止
cmt 該当のエージェントからのイベント転送をすべて抑止
cmdtype agent
inev true
hst マネージャーのホスト名
cmd "Baseパス¥bin¥jevagtfw.exe" -s -o all $EVHOST
qui false
preview true
end-btn

btn 抑止解除
cmt 該当のエージェントのイベント転送抑止をすべて解除
cmdtype agent
inev true
hst マネージャーのホスト名
cmd "Baseパス¥bin¥jevagtfw.exe" -r -f $EVHOST
qui false
preview true
end-btn

btn 抑止確認
cmt イベント転送抑止状態の確認
cmdtype agent
inev false
hst マネージャーのホスト名
cmd "Baseパス¥bin¥jevagtfw.exe" -l
qui false
preview true
end-btn

end-def
```

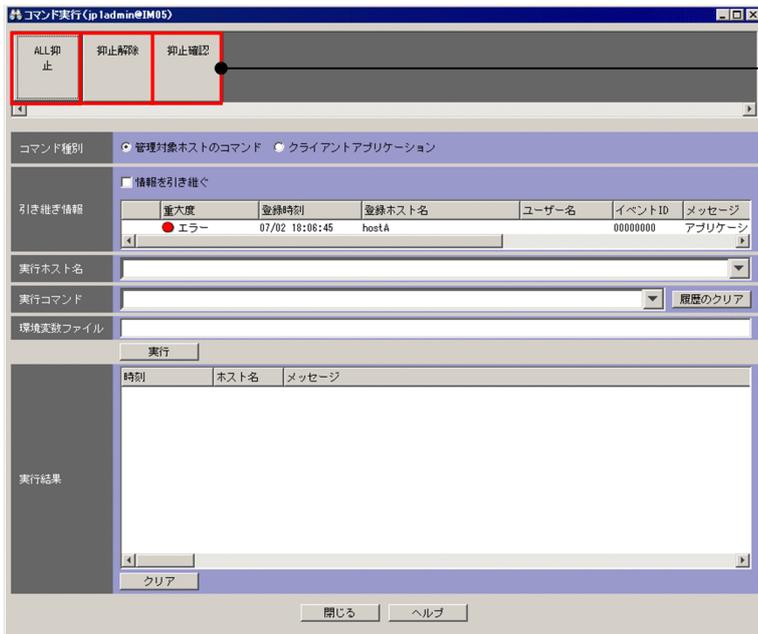
定義例中の\$EVHOSTは、JP1/IM - View のコンソール画面で選択したイベントのイベント発行元ホスト名が引き当てられます。

UNIX の場合、「Baseパス¥bin¥jevagtfw.exe」と表記している部分は、「/opt/jp1base/bin/jevagtfw」になります。

4. JP1/IM - View のコンソール画面を起動する。

5. [コマンド実行] 画面に設定した [コマンド] ボタンが表示されていることを確認する。

[コマンド実行] 画面は、[イベントコンソール] 画面の [コマンド実行] ボタンをクリックして表示します。



[コマンド] ボタンが表示されていることを確認する

6.10.3 エージェントからのイベント転送を抑制してイベントの大量発生に対処する

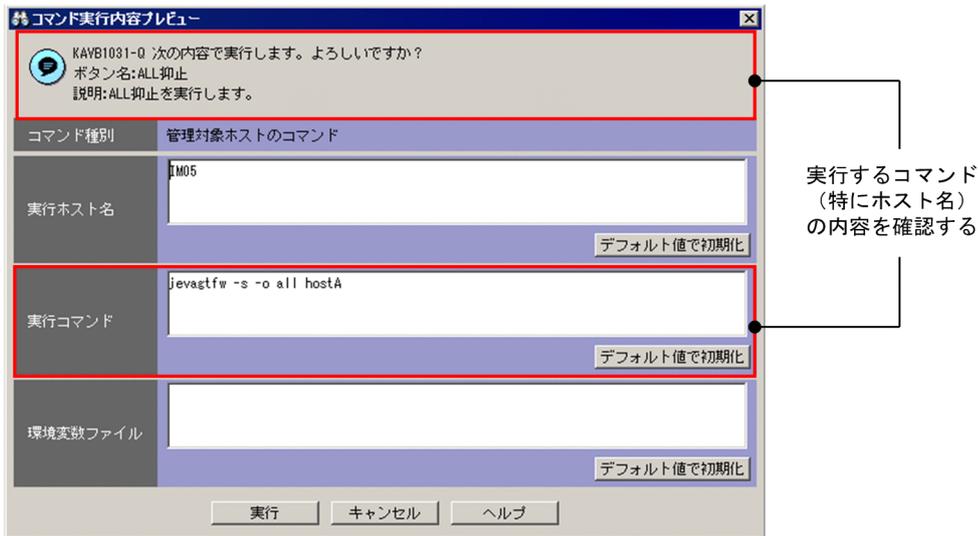
[6.10.2 エージェントからのイベント転送を抑制するための準備をする] で設定した [コマンド] ボタンを使用し、エージェントからのイベント転送を抑制して、イベントの大量発生に対処する場合の手順について説明します。

(1) イベントが大量発生しているエージェントからのイベント転送をマネージャーから抑止する

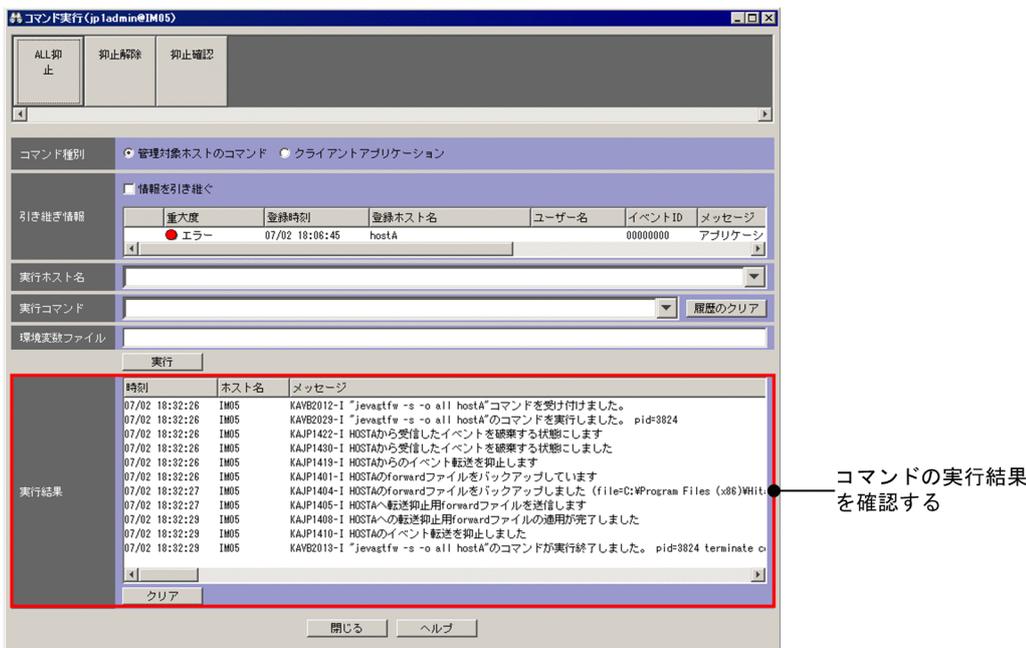
設定した [コマンド] ボタンを使用して、エージェントからのイベント転送をマネージャーから抑止します。

1. [イベントコンソール] 画面のイベント一覧で、特定のエージェントから JP1 イベントが大量に出力されているのを確認する。
2. イベントを抑止したいエージェントから転送されている JP1 イベントを選択する。
3. [コマンド実行] ボタンをクリックして、[コマンド実行] 画面を表示する。
4. [6.10.2 エージェントからのイベント転送を抑制するための準備をする] で設定した [コマンド] ボタンの「ALL 抑止」ボタンをクリックする。

[コマンド実行内容プレビュー] 画面が表示されます。実行されるコマンドの内容（特に抑止対象となるホスト名）を確認してください。



5. [コマンド実行内容プレビュー] 画面の [実行] ボタンをクリックして、jevagtfw コマンドを実行する。該当のエージェントからのイベント転送が抑止されます。コマンド実行結果は、[コマンド実行] 画面の [実行結果] で確認できます。



6. イベントが大量に発生している原因を特定して問題を解決する。

イベント転送を抑止している間に、イベント発生元のエージェントを調査して問題を解決してください。

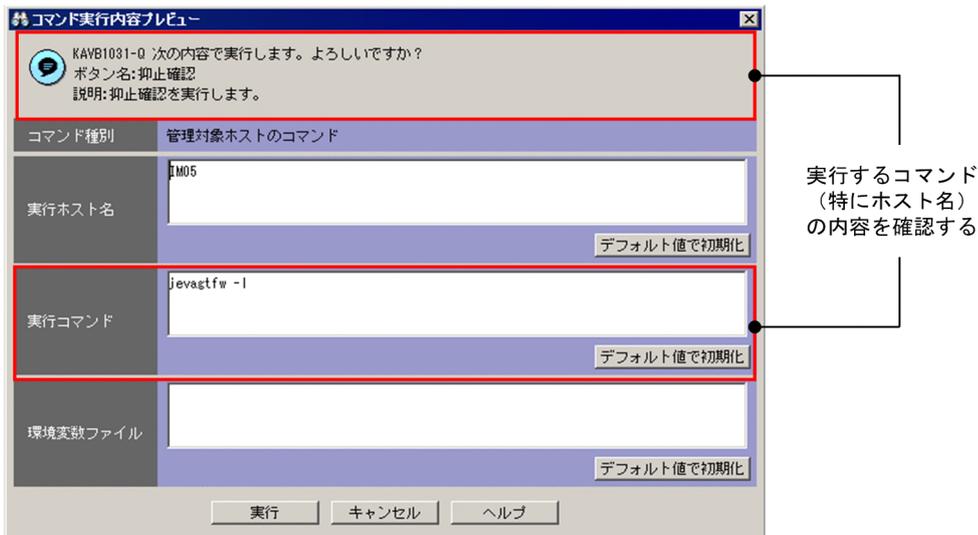
(2) エージェントからのイベント転送の抑止状況を確認する

設定した [コマンド] ボタンを使用して、エージェントからのイベント転送の抑止状況をマネージャーから確認します。

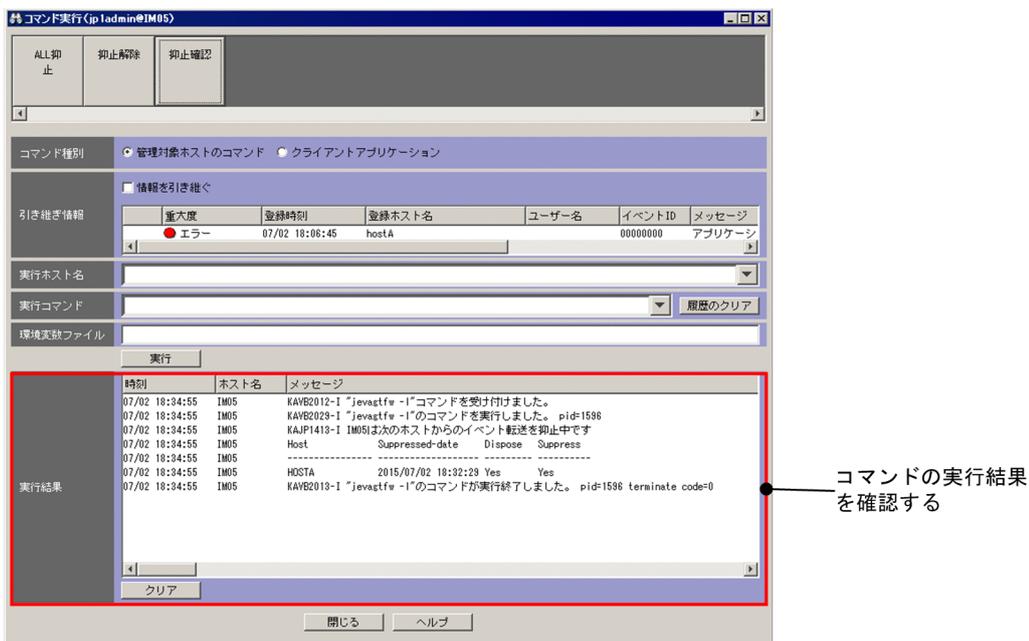
1. [イベントコンソール] 画面で、[コマンド] ボタンをクリックする。
[コマンド実行] 画面が表示されます。

2. [6.10.2 エージェントからのイベント転送を抑制するための準備をする] で設定した [コマンド] ボタンの [抑止確認] ボタンをクリックする。

[コマンド実行内容プレビュー] 画面が表示されます。実行されるコマンドの内容を確認してください。



3. [コマンド実行内容プレビュー] 画面の [実行] ボタンをクリックして、jevagtfw コマンドを実行する。
[コマンド実行] 画面の [実行結果] で抑止状態を確認します。
コマンド実行結果は、[コマンド実行] 画面の [実行結果] で確認できます。



(3) エージェントからのイベント転送の抑止を解除する

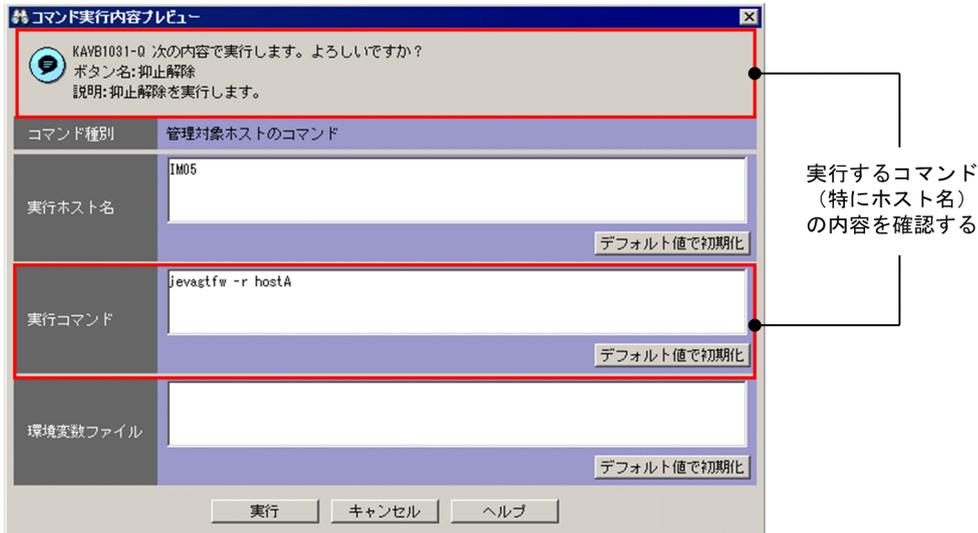
設定した [コマンド] ボタンを使用して、エージェントからのイベント転送の抑止をマネージャーから解除します。

1. [イベントコンソール] 画面で、イベントを抑止したいエージェントから転送されている JP1 イベントを選択する。

2. [コマンド実行] ボタンをクリックして、[コマンド実行] 画面を表示する。

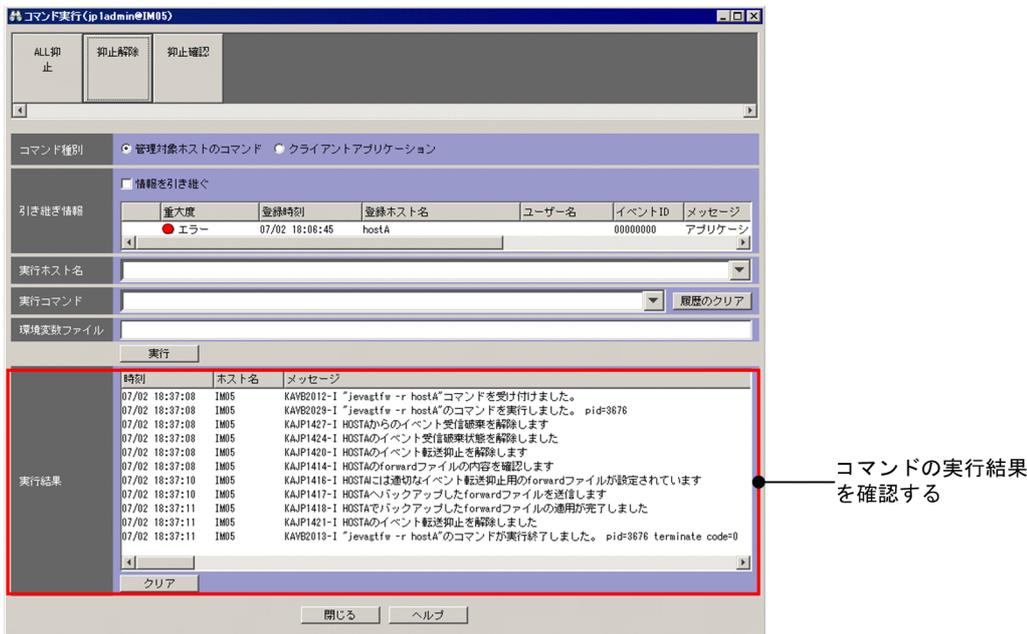
3. [6.10.2 エージェントからのイベント転送を抑制するための準備をする] で設定した [コマンド] ボタンの [抑止解除] ボタンをクリックする。

[コマンド実行内容プレビュー] 画面が表示されます。実行されるコマンドの内容 (特に抑止解除対象となるホスト名) を確認してください。

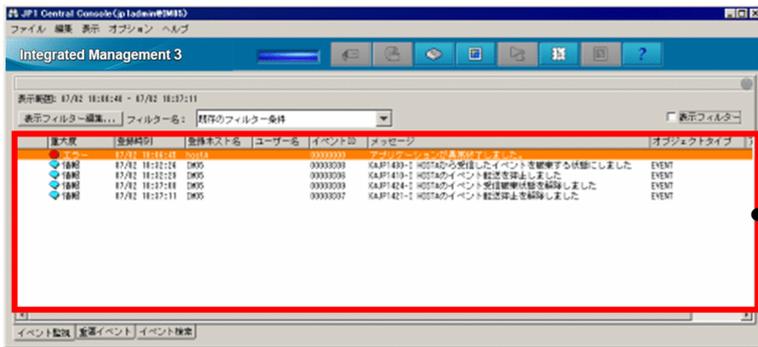


4. [コマンド実行内容プレビュー] 画面の [実行] ボタンをクリックして、jevagtfw コマンドを実行する。該当エージェントのイベント転送の抑止が解除されます。

コマンド実行結果は、[コマンド実行] 画面の [実行結果] で確認できます。



5. [イベントコンソール] 画面でも抑止解除の実行を確認し、該当のエージェントからのイベントが通知されることを確認する。



抑止の解除と
該当のエージェント
からのイベントの
通知を確認する

(4) エージェントからのイベント転送の設定を見直す

大量発生イベントの再発防止策として、今回大量発生したイベントの発生状況を分析して、イベント転送を自動で抑止するためのしきい値を設定します。

イベントの発生状況を分析する際の観点を中心に示します。

- 大量発生したイベントをフィルタリングするとしたら、どのようなフィルタリング条件が適切か。
- 一定期間内（例えば 60 秒間）に何件のイベントが発生したか。
- イベントの大量発生は継続的なものか。

このような観点で分析した結果を基に、大量発生イベントのしきい値に相当するイベント転送条件を、エージェントの JP1/Base の転送設定ファイルに設定します。設定手順については、「6.10.5 イベント転送を自動で抑止するためのしきい値をエージェントに設定する」を参照してください。

(5) 転送を抑止されたイベントを確認する

イベントが大量に発生しているエージェントのイベント転送を抑止すると、本来そのエージェントから転送されるはずだった重要なイベントがマネージャーに転送されていないおそれがあります。そのような場合は、転送を抑止したエージェントのイベント DB を JP1/IM - View から検索して、転送抑止中に発生したイベントを確認します。JP1 イベントの検索方法については、「6.8 JP1 イベントを検索する」を参照してください。

6.10.4 イベントをマネージャーで集約してイベントの大量発生に対処する

システム運用中に発生したイベントを基に繰り返しイベント条件を設定して、条件に一致する JP1 イベントをイベント一覧に集約して表示したり、自動アクションの実行を抑止したりして、イベントの大量発生に対処する場合の手順について説明します。

なお、対処状況を変更するには、JP1_Console_Admin 権限または JP1_Console_Operator 権限が必要です。

(1) 運用中に発生したイベントを使って追加繰り返しイベント条件を設定する

システム運用中に発生した繰り返しイベントを使って [繰り返しイベント条件設定] 画面で繰り返しイベントの監視を抑止します。このとき設定した条件を追加繰り返しイベント条件といいます。

1. [イベントコンソール] 画面のイベント一覧で、監視を抑止したい JP1 イベントを選択する。
2. [イベントコンソール] 画面のメニューから [表示] - [繰り返しイベント条件で抑止] を選択するか、右クリックして表示されるメニューから [繰り返しイベント条件で抑止] を選択して、[繰り返しイベント条件設定] 画面を表示する。

手順 1 で選択した JP1 イベントの属性が繰り返しイベント条件に自動的に設定された状態で、[繰り返しイベント条件設定] 画面が表示されます。

自動的に設定される項目は、繰り返しイベント条件自動入力定義ファイル (event_storm_auto_list.conf) で変更できます。繰り返しイベント条件自動入力定義ファイル (event_storm_auto_list.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「繰り返しイベント条件自動入力定義ファイル (event_storm_auto_list.conf)」(2. 定義ファイル) を参照してください。

3. 必要な項目を [繰り返しイベント条件設定] 画面で編集する。

4. [OK] ボタンをクリックする。

追加繰り返しイベント条件が [繰り返しイベント条件一覧] 画面に反映されます。運用中に追加した追加繰り返しイベント条件には、種別に  アイコンが表示されます。

設定した条件を満たしたイベントが、繰り返しイベントの監視抑止の対象となります。監視抑止の開始については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.5.4 大量発生イベントの監視抑止を開始する契機」を参照してください。

(2) 繰り返しイベント条件の設定を見直す

設定している繰り返しイベントの条件を見直します。詳細については、「[6.10.6 繰り返しイベント条件を設定する](#)」を参照してください。

(3) 追加繰り返しイベント条件を繰り返しイベント条件に変更する

システム運用中に追加した追加繰り返しイベント条件は、繰り返しイベント条件に変更できます。

1. [イベントコンソール] 画面のメニューから [オプション] - [繰り返しイベント条件設定] を選択して [繰り返しイベント条件一覧] 画面を表示する。
2. [繰り返しイベント条件一覧] 画面の [繰り返しイベント条件一覧] で繰り返しイベント条件に変更したい追加繰り返しイベント条件 (種別に  アイコンが付いている条件) を選択する。
3. [種別変更] ボタンをクリックする。

- 種別を変更してもよいかを確認するメッセージが表示されるため、問題なければ [はい] ボタンをクリックする。
選択した追加繰り返しイベント条件が、繰り返しイベント条件に変更されます。
- [繰り返しイベント条件一覧] 画面の [適用] ボタンをクリックする。
- 設定を反映してもよいかを確認するメッセージが表示されるため、問題なければ [はい] ボタンをクリックする。
追加した繰り返しイベント条件が有効になります。

6.10.5 イベント転送を自動で抑止するためのしきい値をエージェントに設定する

エージェントでイベントが大量に発生した場合に備えて、しきい値を設定してイベント転送を自動的に抑止する手順を次に示します。

- イベント転送を自動的に抑止したいエージェントの転送設定ファイルを編集する。
大量発生イベントのしきい値に相当するイベント転送抑止条件を、エージェントの JP1/Base の転送設定ファイルに設定します。

イベント転送抑止条件の形式

```
suppress 識別子 単位時間 しきい値 確認回数 [宛先 (省略可能) ]
イベントフィルター
end-suppress
```

イベント転送抑止条件の詳細については、マニュアル「JP1/Base 運用ガイド」の転送設定ファイル (forward) の説明を参照してください。

- 転送設定ファイルの変更内容を有効にする。
転送設定ファイルをリロードするか、イベントサービスを再起動すると、変更内容が有効になります。
イベントの発生状況が設定したイベント転送抑止条件に一致した場合、イベント転送が抑止されます。

イベント転送を抑止している間に、イベント発生元のエージェントを調査して、異常がある場合は問題を解決してください。

6.10.6 繰り返しイベント条件を設定する

繰り返しイベント条件を設定すると、条件に一致するイベント（繰り返しイベント）をマネージャーで集約して、イベント一覧への表示や自動アクションの実行を抑止できます。

繰り返しイベント条件は、[繰り返しイベント条件設定] 画面、および [繰り返しイベント条件一覧] 画面で設定します。各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「3.17 [繰り返しイベント条件設定] 画面」および「3.19 [繰り返しイベント条件一覧] 画面」を参照してください。

なお、繰り返しイベント条件を設定するには、JP1/IM - View から操作する JP1 ユーザーに JP1_Console_Admin 権限が与えられている必要があります。

繰り返しイベント条件を設定する手順を次に示します。

1. [イベントコンソール] 画面のメニューから [オプション] - [繰り返しイベント条件設定] を選択する。
[繰り返しイベント条件一覧] 画面が表示されます。

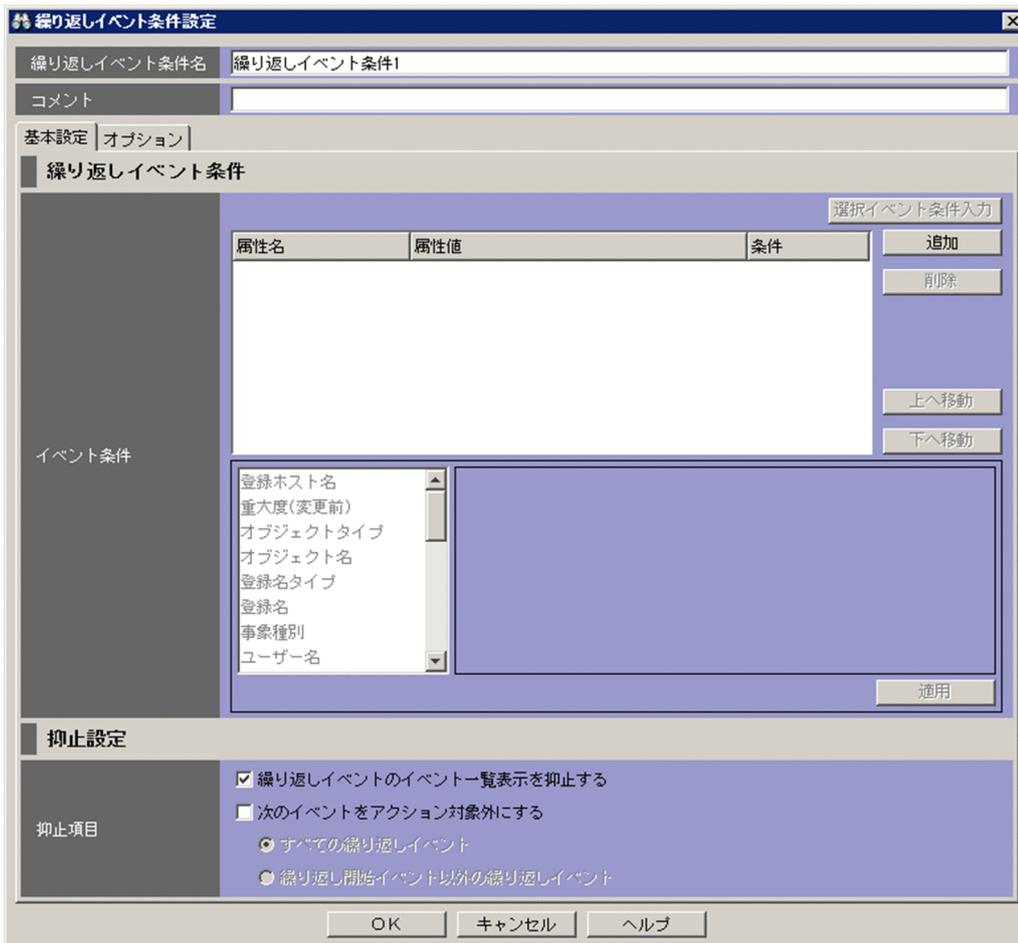
2. 次のどちらかの方法で [繰り返しイベント条件設定] 画面を表示する。

- 新規に繰り返しイベント条件を設定する場合は、[繰り返しイベント条件一覧] 画面の [追加] ボタンをクリックする。
- 既存の繰り返しイベント条件を編集する場合は、[繰り返しイベント条件一覧] 画面に表示されている繰り返しイベント条件を選択して [編集] ボタンをクリックする。



[繰り返しイベント条件設定] 画面が表示されます。

3. [繰り返しイベント条件設定] 画面の [基本設定] ページの [イベント条件] を設定する。(任意)
マネージャーが監視対象イベントを取得したときに、どの属性値を比較するかを設定します。



設定手順の詳細は、「6.10.6(1) [繰り返しイベント条件設定] 画面の [イベント条件] を設定する」を参照してください。

4. [繰り返しイベント条件設定] 画面の [基本設定] ページの [抑止項目] を設定する。(必須)

イベント条件に一致する JP1 イベントに対して、何を抑止するのかを設定します。

設定手順の詳細は、「6.10.6(2) [繰り返しイベント条件設定] 画面の [抑止項目] を設定する」を参照してください。

5. [繰り返しイベント条件設定] 画面の [オプション] ページの [同一属性値条件] を設定する。(任意)

「重大度が警告以下のイベントを、登録ホスト名 (B. SOURCESERVER) の属性値ごとに集約したい」など、繰り返しイベント条件に一致する繰り返しイベントを特定の属性ごとにまとめて抑止する場合に設定します。

設定手順の詳細は、「6.10.6(3) [繰り返しイベント条件設定] 画面の [同一属性値条件] を設定する」を参照してください。

6. [繰り返しイベント条件設定] 画面の [オプション] ページの [しきい値] を設定する。(任意)

繰り返しイベントの表示抑止および自動アクションの実行抑止を開始するしきい値を設定します。しきい値を設定しない場合、繰り返しイベント条件に一致するイベントを取得した時点で抑止を開始します。設定手順の詳細は、「6.10.6(4) [繰り返しイベント条件設定] 画面の [しきい値] を設定する」を参照してください。

7. [繰り返しイベント条件設定] 画面の [オプション] ページの [終了監視期間] を設定する。(必須)

イベントの大量発生が収束したと判断するための期間（終了監視期間）を設定します。設定手順の詳細は、「6.10.6(5) [繰り返しイベント条件設定] 画面の [終了監視期間] を設定する」を参照してください。

8. [繰り返しイベント条件設定] 画面の [オプション] ページの [抑止開始イベント] を設定する。(任意)

大量発生したイベントの抑止を開始したことを通知するイベントを発行する場合に設定します。設定手順の詳細は、「6.10.6(6) [繰り返しイベント条件設定] 画面の [抑止開始イベント] を設定する」を参照してください。

9. [繰り返しイベント条件設定] 画面の [オプション] ページの [抑止終了イベント] を設定する。(任意)

大量発生したイベントの抑止を終了したことを通知するイベントを発行する場合に発行します。

設定手順の詳細は、「6.10.6(7) [繰り返しイベント条件設定] 画面の [抑止終了イベント] を設定する」を参照してください。

10. [繰り返しイベント条件設定] 画面の [オプション] ページの [抑止継続判定] および [抑止継続処理] を設定する。(任意)

時間 (秒), または件数ごとに繰り返しイベントの監視抑止が継続されているかを判定して, 継続されている場合に JP1 イベントを発行して通知したり, 抑止を打ち切ったりする場合に設定します。

設定手順の詳細は、「6.10.6(8) [繰り返しイベント条件設定] 画面の [抑止継続判定] および [抑止継続処理] を設定する」を参照してください。

11. [繰り返しイベント条件設定] 画面の [OK] ボタンをクリックする。

繰り返しイベント条件が [繰り返しイベント条件一覧] 画面に反映されます。

12. 設定した繰り返しイベント条件について, [繰り返しイベント条件一覧] 画面の [適用] チェックボックスをチェックする。

13. [繰り返しイベント条件一覧] 画面の [適用] ボタンをクリックする。

14. 設定を反映してもよいかを確認するメッセージが表示されるため, 問題なければ [はい] ボタンをクリックする。

繰り返しイベント条件が有効になります。

(1) [繰り返しイベント条件設定] 画面の [イベント条件] を設定する

設定手順を次に示します。

1. [繰り返しイベント条件設定] 画面の [基本設定] ページを表示する。

2. 次のうち必要な操作を実施して, イベント条件を設定する。

- 新しくイベント条件を追加する場合は, [追加] ボタンをクリックする。
[属性名] [属性値] [条件] が空のイベント条件がイベント条件一覧に追加されます。
- イベント条件を編集する場合は, 編集したいイベント条件をイベント条件一覧から選択したあと, イベント条件の編集領域から属性名, 属性値, および条件を選択して, [適用] ボタンをクリックする。
- イベント条件を削除する場合は, 削除したいイベント条件をイベント条件一覧から選択したあと, [削除] ボタンをクリックする。
- [イベントコンソール] 画面で選択しているイベントと同じ属性値を条件に設定したい場合は, [選択イベント条件入力] ボタンをクリックする。
[選択イベント条件入力] ボタンをクリックする前に設定されていた条件は削除され, [イベントコンソール] 画面で選択しているイベントと同じ属性値に上書きされます。

(2) [繰り返しイベント条件設定] 画面の [抑止項目] を設定する

設定手順を次に示します。

1. [繰り返しイベント条件設定] 画面の [基本設定] ページを表示する。
2. 次のうちどちらか、または両方のチェックボックスをチェックする。
 - [繰り返しイベントのイベント一覧表示を抑止する]
 - [次のイベントをアクション対象外にする]
3. 前の手順で [次のイベントをアクション対象外にする] をチェックした場合は、アクション対象外にするイベントの範囲を指定する。

次のうちどちらかを選択してください。

- [すべての繰り返しイベント]
この繰り返しイベント条件に一致するすべての繰り返しイベントをアクション対象外にします。
- [繰り返し開始イベント以外の繰り返しイベント]
この繰り返しイベント条件に一致する繰り返しイベントのうち、抑止を開始する契機となったイベント（繰り返し開始イベント）以外をアクション対象外にします。

(3) [繰り返しイベント条件設定] 画面の [同一属性値条件] を設定する

設定手順を次に示します。

1. [繰り返しイベント条件設定] 画面の [オプション] ページを表示する。
2. 次のうち必要な操作を実施して、同一属性値条件を設定する。
 - 同一属性値条件を追加する場合は、[同一属性値条件] のドロップダウンリストから属性名を選択し、[追加] ボタンをクリックする。
 - 同一属性値条件を削除する場合は、[同一属性値条件] の [属性名] リストから属性名を選択し、[削除] ボタンをクリックする。

(4) [繰り返しイベント条件設定] 画面の [しきい値] を設定する

設定手順を次に示します。

1. [繰り返しイベント条件設定] 画面の [オプション] ページを表示する。
2. [しきい値] の [有効] チェックボックスをチェックする。
3. しきい値を設定する。
例えば、しきい値を「10 [件] /3 [秒]」と設定した場合、最後に JP1/IM - Manager が取得したイベントの到着時刻から、その3秒前までの間に、10件以上のイベントを取得した場合に抑止を開始します。

(5) 【繰り返しイベント条件設定】画面の【終了監視期間】を設定する

設定手順を次に示します。

1. 【繰り返しイベント条件設定】画面の【オプション】ページを表示する。

2. 終了監視期間を設定する。

「6.10.6(4) 【繰り返しイベント条件設定】画面の【しきい値】を設定する」でしきい値を設定しているかどうかで、終了監視期間の考え方は変わります。終了監視期間を 300 秒と設定した場合のそれぞれの違いを次に示します。

しきい値を設定している場合

最後に JP1/IM - Manager が取得したイベントの到着時刻から、その 300 秒前までの間に、設定したしきい値を下回り続けたときにイベントの大量発生が収束したと判断します。

しきい値を設定していない場合

最後に JP1/IM - Manager が取得したイベントの到着時刻から、その 300 秒前までの間に、繰り返しイベント条件に一致する繰り返しイベントを取得しなかったときにイベントの大量発生が収束したと判断します。

(6) 【繰り返しイベント条件設定】画面の【抑止開始イベント】を設定する

設定手順を次に示します。

1. 【繰り返しイベント条件設定】画面の【オプション】ページを表示する。

2. 【抑止開始イベント】の【発行する】チェックボックスをチェックする。

(7) 【繰り返しイベント条件設定】画面の【抑止終了イベント】を設定する

設定手順を次に示します。

1. 【繰り返しイベント条件設定】画面の【オプション】ページを表示する。

2. 【抑止終了イベント】の【発行する】チェックボックスをチェックする。

(8) 【繰り返しイベント条件設定】画面の【抑止継続判定】および【抑止継続処理】を設定する

【抑止継続判定】と【抑止継続処理】は、合わせて設定する必要があります。設定手順を次に示します。

1. 【繰り返しイベント条件設定】画面の【オプション】ページを表示する。

2. 【抑止継続判定】の【有効】チェックボックスをチェックする。

3. 【抑止継続判定】で抑止が継続されているかを判定する契機を指定する。

[時間] と [件数] のどちらかを選択します。それぞれの違いについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.4.7 繰り返しイベントの表示抑止が継続されている場合の通知」を参照してください。

4. [抑止継続処理] で抑止が継続されている場合の処理を選択する。

[抑止継続通知イベントを発行する] と [抑止を打ち切る] のどちらかを選択します。

[抑止を打ち切る] を選択した場合は、[抑止打ち切り通知イベントを発行する] をチェックすることで、抑止を打ち切ったことを通知する JP1 イベントを発行できます。

6.10.7 イベントを大量に発行しているログファイルトラップをマネージャーから停止する

ログファイルトラップでイベントが大量に発行された場合の対処として、IM 構成管理を使用して、マネージャーから特定のログファイルトラップを停止する手順を次に示します。IM 構成管理を使用しないで、特定のログファイルトラップを停止する方法については、マニュアル「JP1/Base 運用ガイド」の大量発生イベントの転送を抑止する説明をしている個所を参照してください。

なお、次に示す手順では、IM 構成管理を使用して、エージェントのプロファイル进行管理していることを前提とします。IM 構成管理のプロファイル管理の概要については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.5 プロファイルの管理」を参照してください。IM 構成管理のプロファイルの設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.5 プロファイルの設定」を参照してください。

また、発生元ホストのマッピングが有効に設定されていることを前提とします。発生元ホストのマッピングを有効にする手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「5.15 発生元ホストのマッピングの設定」を参照してください。

1. [イベントコンソール] 画面のイベント一覧で、ログファイルトラップが発行した JP1 イベントが大量に出力されているのを確認する。
2. 該当の JP1 イベントの [イベント詳細] 画面を表示する。
3. [イベント詳細] 画面のイベント属性に、発生元ホスト名および監視名※が表示されているのを確認する。

注※

[イベント詳細] 画面のイベント属性にログファイルトラップの監視名を表示するには、JP1/IM - Manager のバージョンが 10-50 以降、かつエージェントの JP1/Base のバージョンが 10-50 以降である必要があります。

4. IM 構成管理・ビューアー (IM 構成管理) にログインして、[IM 構成管理] 画面を表示する。
5. [IM 構成] タブをクリックして、[IM 構成] ページを表示する。

6. ツリー表示領域でログファイトラップの発生元ホスト名を選択して、[表示] メニューから [プロファイル表示] を選択する。
該当ホストの [プロファイル表示/編集] 画面が表示されます。
7. ツリー表示領域の [JP1/Base] を選択して、[編集] メニューから [排他編集設定] を選択する。
プロファイルの排他編集権を獲得します。
8. ツリー表示領域の [ログファイルトラップ情報] から抑止対象のログファイルトラップの監視名を選択して、[操作] 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ます。
9. [はい] ボタンをクリックする。
ログファイルトラップが停止します。
ログファイルトラップが停止している間に、ログの出力元のアプリケーションを調査して、異常がある場合は問題を解決してください。

6.10.8 同じ属性のイベントが連続して発生した場合の集約表示について

繰り返しイベントの集約表示機能を使用する場合、短時間に連続して発生する同一内容の JP1 イベントを一つに集約して、[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] ページに表示できます。繰り返しイベントの集約表示機能は、[ユーザー環境設定] 画面で設定できます。

繰り返しイベントの集約表示機能は、イベントの監視抑止機能と同時に使用できません。

繰り返しイベントおよび集約イベントは、詳細情報を確認できます。また、繰り返しイベントを監視していない場合と同様に対処状況を変更できます。なお、対処状況を変更するには、JP1_Console_Admin 権限または JP1_Console_Operator 権限が必要です。

繰り返しイベントの集約表示の概要については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.4.10 繰り返しイベントの集約表示機能で表示抑止する場合について」を参照してください。

連続して発生していない JP1 イベントを集約したい場合、イベント条件や集約して表示する契機を指定したい場合などは、繰り返しイベントの集約表示ではなく、繰り返しイベントの監視抑止を設定してください。繰り返しイベントの監視抑止の設定方法については、「6.10.4 イベントをマネージャーで集約してイベントの大量発生に対処する」を参照してください。

(1) 繰り返しイベントの集約表示機能を設定する

1. [イベントコンソール] 画面のメニューから [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。
2. [イベント表示項目] ページの [集約表示] の [有効] をチェックする。

[タイムアウト時間] が活性となります。

3. [タイムアウト時間] を指定する。

繰り返しイベントを集約する場合のタイムアウト時間を指定します。

集約開始イベントと受信イベントの到着時刻の差がタイムアウト時間を過ぎた場合、イベントの集約が完了します。

4. [OK] ボタンをクリックする。

設定した内容が反映されます。

一つに集約したイベントは集約イベントとして、[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] ページに表示されます。

備考

繰り返しイベントの集約表示は、設定が反映されたあと受信したイベントから適用されます。設定が反映される前に受信したイベントは、繰り返しイベントの集約表示の対象とはなりません。集約開始イベントと受信イベントの到着時刻の差が指定した時間を過ぎた場合、イベントの集約が完了します。また、1 件のイベントに集約できるイベントは最大 100 件です。

6.11 他製品と連携して JP1 イベントに対処する

ここでは、他製品と連携して JP1 イベントに対処する場合の、JP1/IM - View での操作手順について説明します。

6.11.1 JP1 イベントをインシデントとして JP1/Service Support に登録する (JP1/Service Support 連携)

JP1/Service Support 連携用の設定をしておくことで、JP1/IM - View に表示された JP1 イベントをインシデントとして JP1/Service Support に登録できます。設定手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「10.1.1 JP1/Service Support 画面呼び出し設定」を参照してください。

次の画面から、JP1/Service Support の [登録先プロセスワークボード選択] 画面を表示し、JP1/Service Support にインシデントを登録します。

- [イベントコンソール] 画面の各ページ
- [関連イベント一覧] 画面
- [イベント詳細] 画面

次に、各画面から JP1/Service Support の [登録先プロセスワークボード選択] 画面を表示するまでの手順を示します。JP1/Service Support の [登録先プロセスワークボード選択] 画面から JP1/Service Support にインシデントを登録する手順については、マニュアル「JP1/Service Support 操作ガイド」を参照してください。

なお、JP1 イベントをインシデントとして登録するには、JP1_Console_Admin 権限または JP1_Console_Operator 権限が必要です。

(1) [イベントコンソール] 画面の各ページから JP1/Service Support を表示する

手順を次に示します。

1. [イベントコンソール] 画面のイベント一覧に表示される JP1 イベントの中からインシデントとして登録する JP1 イベントを一つ選択する。

[イベント検索] ページには、マネージャー以外のイベント DB に登録された JP1 イベントを表示できますが、これらの JP1 イベントはインシデントとして登録できません。マネージャー上に登録された JP1 イベントだけ、インシデントとして登録できます。

2. 右クリックして [インシデント登録]、またはメニューから [表示] - [インシデント登録] を選択する。WWW ブラウザーが起動して、JP1/Service Support の [登録先プロセスワークボード選択] 画面が表示されます。

(2) [関連イベント一覧] 画面から JP1/Service Support を表示する

手順を次に示します。

1. [関連イベント一覧] 画面に表示される JP1 イベントの中からインシデントとして登録する JP1 イベントを一つ選択する。

2. 右クリックして [インシデント登録] を選択する。

WWW ブラウザーが起動して、JP1/Service Support の [登録先プロセスワークボード選択] 画面が表示されます。

(3) [イベント詳細] 画面から JP1/Service Support を表示する

手順を次に示します。

1. [イベント詳細] 画面の [インシデント登録] ボタンをクリックする。

WWW ブラウザーが起動して、JP1/Service Support の [登録先プロセスワークボード選択] 画面が表示されます。

6.11.2 JP1 イベントに対応する運用手順を表示する (JP1/Navigation Platform 連携)

JP1/Navigation Platform 連携用の設定をしておくことで、JP1/IM - View に表示された JP1 イベントから、JP1/Navigation Platform の業務コンテンツ (運用手順) にシングルサインオンでアクセスできます。設定手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「10.2 JP1/Navigation Platform と連携する」を参照してください。

[イベント詳細] 画面から、シングルサインオンで JP1/Navigation Platform の [業務実行] 画面を表示する手順を次に示します。

1. [イベント詳細] 画面の [ガイド] 表示領域のリンクをクリックする。

WWW ブラウザーが起動して、選択した JP1 イベントに対応する業務コンテンツ (運用手順) が、JP1/Navigation Platform の [業務実行] 画面に表示されます。

6.11.3 JP1 イベントを発行したアプリケーションをモニター起動する

受信した JP1 イベントに関連するプログラムのモニター画面を表示し、情報の参照や操作ができます。

[イベントコンソール] 画面からモニター画面を起動するには、次のように操作します。

1. [イベントコンソール] 画面のイベント一覧で JP1 イベントを選択し、[表示] - [モニター起動] を選択する。または、ツールバーの  をクリックするか、ポップアップメニューの [モニター起動] を選択する。

対応するプログラムのモニター画面（WWW ページまたはアプリケーションプログラム）が起動します。

また、[イベント詳細] 画面の [モニター起動] ボタンをクリックして、モニター画面を起動することもできます。

なお、選択した JP1 イベントに対応するプログラムがない、またはモニター画面を起動するための設定がされていない場合は、メニューおよびボタンは選択できません。モニター画面を起動するための設定方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

(1) モニター画面を起動できるアプリケーションの一覧

モニター画面を起動できるアプリケーションを次の表に示します。アプリケーションの対応 OS の詳細については、各アプリケーションのマニュアルを確認してください。

プログラム名	画面種別	モニター起動定義ファイル名
JP1/NETM/Asset Information Manager	WWW ページ	hitachi_jp1_aim_mon.conf
JP1/PFM	WWW ページ	hitachi_jp1_pfmmgr_mon.conf
JP1/IM - Event Gateway for Network Node Manager i	WWW ページ	hitachi_jp1_im_egn_mon.conf
JP1/Base (SNMP トラップ)	WWW ページ	hitachi_jp1_imevtgw_mon.conf
JP1/AJS2 - Scenario Operation	アプリケーションプログラム	hitachi_jp1_ajs2so_mon.conf
JP1/AJS3 (バージョン 9 以降) または JP1/AJS2 (バージョン 8 以前)	アプリケーションプログラム	hitachi_jp1_ajs2_mon.conf
JP1/AJS2 メインフレーム	アプリケーションプログラム	hitachi_jp1_ajs2_mainframe_mon.conf
Cosminexus Application Server	アプリケーションプログラム	hitachi_cosminexus_manager_mon.conf

6.11.4 JP1 イベントに対応する性能レポートを表示する (JP1/PFM 連携)

JP1/PFM 連携用の設定をしておくことで、JP1/IM - View に表示された JP1 イベントから、JP1/PFM - Web Console のレポート画面にシングルサインオンでアクセスできます。なお、JP1/PFM 連携用の設定については、JP1/PFM のマニュアルを参照してください。

(1) [イベントコンソール] 画面の各ページから JP1/PFM - Web Console のレポート画面を表示する

手順を次に示します。

1. [イベントコンソール] 画面のイベント一覧に表示される JP1 イベントの中から問題の事象を示す JP1 イベントを一つ選択する。
2. [イベントコンソール] 画面のメニューから [表示] - [性能表示] を選択する。または、ポップアップメニューの [性能表示] を選択する。
JP1/PFM - Web Console が起動し、レポート画面が表示されます。

(2) [イベント詳細] 画面から JP1/PFM - Web Console のレポート画面を表示する

手順を次に示します。

1. [イベント詳細] 画面の [性能表示] ボタンをクリックする。
JP1/PFM - Web Console が起動し、レポート画面が表示されます。

6.12 セントラルコンソールの注意事項

- 自動アクションの遅延監視は、一定間隔ごとに自動アクションの実行遅延を監視しています。そのため、[アクション詳細設定] 画面で設定した遅延監視の [監視時間] どおりに遅延を検知できないことがあります。また、[監視時間] 経過直後に自動アクションの終了などの遅延監視終了要因となった場合、遅延を検知できないことがあります。
- JP1/IM - Manager は WOW64 環境で動作します。このため、WOW64 環境の OS 上では、自動アクションで 64bit プログラムが実行できない場合があります。この場合は、自動アクションで次のコマンドを実行し、64bit の cmd.exe からプログラムを実行してください。

```
%WinDir%\%Sysnative%\cmd.exe 実行コマンド
```

- 次の場合に WWW ブラウザーに設定される URL の最大長が 2046 文字に制限されます。
 - HTML 形式のイベントガイドのハイパーリンクを押下したとき
 - JP1/IM - Service Support にインシデント登録するとき
 - 事象発生元ホストの性能レポート表示機能で性能レポートを表示するとき

次の共通定義情報を任意のファイルに記述し、jbssetcnf コマンドで適用することで、この制限を解除 (09-10 以前と同じ)、または制限値を変更することができます。なお、この制限を解除、または制限値を変更した場合は、URL が WWW ブラウザーで使用可能な長さである必要があります。

```
[論理ホスト名¥JP1CONSOLEMANAGER]  
"GUIDE_URLLIMIT"="値"  
"URLLIMIT_CHAR_NUM"=dword:値
```

論理ホスト名の部分を、物理ホストの場合は JP1_DEFAULT に、論理ホストの場合は論理ホスト名に設定します。

「[論理ホスト名¥JP1CONSOLEMANAGER]」をファイルの先頭に記述します。

GUIDE_URLLIMIT：HTML 形式のイベントガイドのハイパーリンクの URL 長を制限する、またはしないようにできます。

- URL 長を制限する場合：1 を指定する。
- URL 長を制限しない場合：0 を指定する。

URLLIMIT_CHAR_NUM：次の場合に WWW ブラウザーに設定される URL の最大長を指定できます。

- HTML 形式のイベントガイドのハイパーリンクを押下したとき
 - JP1/IM - Service Support にインシデント登録するとき
 - 事象発生元ホストの性能レポート表示機能で性能レポートを表示するとき
- 16 進数で記述します。単位は文字数です。

- 属性名が「E.JP1_」で始まる拡張属性を JP1 イベントに指定しないでください。

属性名が「E.JP1_」で始まる拡張属性を指定した JP1 イベントを JP1/IM - Manager が受信すると正しく動作しない場合があります。

6.13 セントラルコンソール・ビューアーの運用上の注意事項

- イベントの対処状況はそのときの状態を示すもので、対処状況遷移の妥当性のチェックは行いません。問題点管理システム等でトラブルチケットのクローズを契機に jcochstat コマンドで対処済みにした場合でも、画面からそのイベントの対処状況を未対処に変更できます。他のシステムと連携している場合に、画面からの対処状況を変更する場合は注意してください。
 - jcoview コマンドの引数に誤った値を指定し、JP1/IM - View を起動すると、「KAVB0104-E ユーザー認証に失敗しました」、または「KAVB1210-E 接続中に通信エラーが発生しました。ホスト名を IP アドレスに変換できません。ホスト名を確認してください ホスト名：ホスト名, ポート番号：ポート番号 詳細情報：詳細情報」メッセージを出力後に [ログイン] 画面が表示され、マウスでクリックしても、[ログイン] 画面の入力フィールドを選択して入力できなくなる場合があります。この場合は、いったん、タスクバーで JP1/IM - View 以外の画面をクリックした後、[ログイン] 画面をクリックすると入力できる状態になります。
 - イベント DB を検索対象とした場合、イベント検索の所要時間はイベント DB のサイズに比例します。イベント DB の容量が最大サイズに達した場合は、イベント検索の所要時間が 30 分以上になることもあります。イベント検索条件として [到着時刻] を指定することで、イベント検索の所要時間が短縮することがあります。
 - イベントコンソールサービスの起動がシステム負荷などの要因で時間がかかり、イベント基盤サービスとイベントコンソールサービスの接続でリトライ回数とリトライ間隔を超過した場合、JP1/IM - View を接続した際に過去のイベントが「イベント監視」ページ、「重要イベント」ページに表示されなくなります。イベントコンソールサービスを再起動し、統合トレースログに「KAVB4754-I イベントコンソールサービスに接続しました」が出力されていることを確認してから JP1/IM - View を再起動してください。
 - Windows の UAC (ユーザーアカウント制御) 機能が有効な場合、管理者ユーザーおよび標準ユーザーで起動した JP1/IM - View から表示イベント保存を実行すると、UAC の機能により、保存ファイルがユーザーごとの仮想フォルダにリダイレクトされ保存されます。保存先フォルダは以下の通りです。
 - %ProgramFiles% 以下の場合

```
%LocalAppData%\%VirtualStore%\Program Files
```

(デフォルトは、システムドライブ:¥Users¥<OS ユーザー名>¥AppData¥Local¥VirtualStore¥Program Files)

 - %WINDIR% 以下の場合

```
%LocalAppData%\%VirtualStore%\Windows
```

(デフォルトは、システムドライブ:¥Users¥<OS ユーザー名>¥AppData¥Local¥VirtualStore¥Windows)

また、表示イベント保存の際に応答メッセージ(KAVB0321-Q,KAVB0322-Q)中に含まれるファイル名のパスはリダイレクトされる前のパスが表示されます。
- Windows 10(x64), Windows Server 2016, Windows Server 2019, Windows Server 2022 および Windows 11 では、%WINDIR%\¥System32 フォルダ以下のファイルに対してアクセスおよび

コマンドの実行を行うと、WOW64のリダイレクト機能により%WINDIR%\SysWow64 フォルダ以下にリダイレクトされるため、アクセスやコマンドの実行に失敗することがあります。JP1/IM - Viewの [コマンド実行], アプリケーション実行定義ファイルの実行コマンドに, %WINDIR%\System32以下のコマンドを指定しないでください。

7

セントラルスコープによるシステムの監視

この章では、JP1/IM - View を使用して監視オブジェクトを監視する手順について説明します。

7.1 [監視ツリー] 画面で監視する

監視オブジェクトの状態は、[監視ツリー] 画面で監視できます。また、[監視ツリー] 画面に表示される監視ノード（監視グループ・監視オブジェクト）に対して、状態の変更や監視状態の変更など、各種操作ができます。

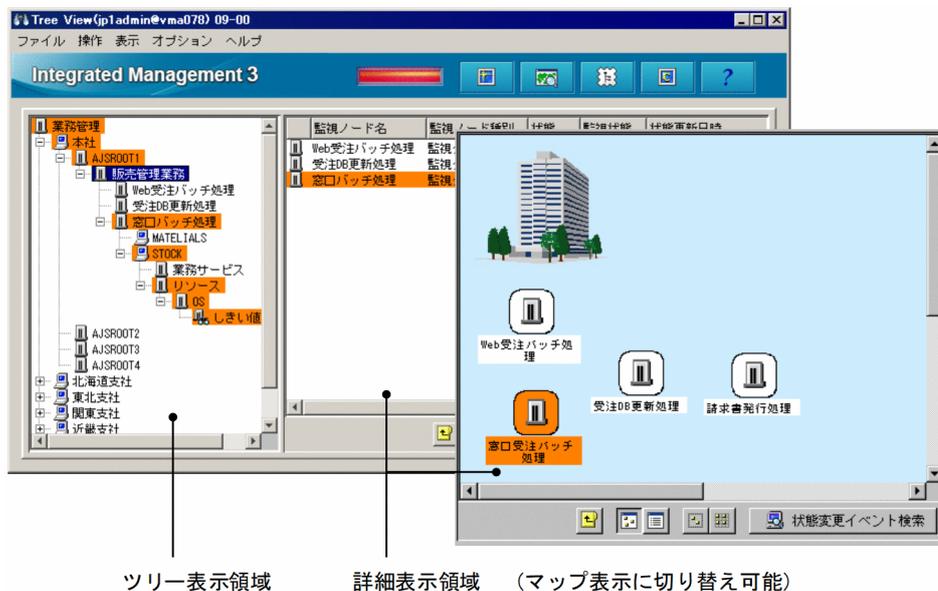
監視ツリーの監視範囲設定を有効にしている場合、監視ツリーには、ログインしている JP1 ユーザーと同じ JP1 資源グループが設定されている監視ノードだけが表示されます。このとき、仮想ルートノードが最上位ノードとして表示されます。表示できる監視ノードが一つもない場合は、仮想ルートノードだけが表示されます。ただし、JP1 資源グループが JP1_Console で、JP1_Console_Admin 権限を持つ JP1 ユーザーでログインしている場合は、すべての監視ノードが表示されます。

[監視ツリー] 画面は、次に示す三つのうち、どれかの方法で表示できます。

- JP1/IM - Manager（セントラルスコープ）にログインする。
- [イベントコンソール] 画面の [セントラルスコープ起動] ボタンをクリックする。
- [イベントコンソール] 画面のメニューバーから [ファイル] - [セントラルスコープ起動] を選択する。

[監視ツリー] 画面の表示例を次に示します。

図 7-1 [監視ツリー] 画面の表示例



7.1.1 監視ノードの状態を変更する

[監視ツリー] 画面に表示された監視ノードの状態を変更する手順について説明します。なお、変更できる状態、変更時の動作は、監視ノードの種別（監視グループ、監視オブジェクト）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 導入・設計ガイド」の「5.2.2 監視ノードの状態」を参照してください。

監視ノードの状態を変更するには、JP1_Console_Operator 以上の権限が必要です。監視ツリーの監視範囲設定が有効な場合は、表示されている監視ノードのうち、JP1_Console_Operator 以上の権限でアクセスできる監視ノードだけ状態を変更できます。

監視ノードの状態を変更する手順を次に示します。

1. ツリー表示領域または詳細表示領域に表示された監視ノードを選択する。
2. 次に示すどちらかの方法で監視ノードの状態を変更する。
 - メニューバーから [操作] - [状態変更] を選択し、ユーザーが意図する状態に変更する。
 - 右クリックして表示されるポップアップメニューから [状態変更] を選択し、ユーザーが意図する状態に変更する。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。

7.1.2 監視ノードの監視状態を変更する

監視ノードの監視状態を変更する手順について説明します。なお、変更時の動作は、監視ノードの種別（監視グループ、監視オブジェクト）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 導入・設計ガイド」の「5.2.2 監視ノードの状態」を参照してください。

監視ノードの監視状態を変更するには、JP1_Console_Operator 以上の権限が必要です。監視ツリーの監視範囲設定が有効な場合は、表示されている監視ノードのうち、JP1_Console_Operator 以上の権限でアクセスできる監視ノードだけ状態を変更できます。

監視ノードの監視状態を変更する手順を次に示します。

1. ツリー表示領域または詳細表示領域に表示された監視ノードを選択する。
2. 次に示すどれかの方法で監視ノードの状態を変更する。
 - メニューバーから [操作] - [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。
 - 右クリックして表示される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。
 - 右クリックして表示されるポップアップメニューから [プロパティ] を選択し、[全般] ページの「監視」「非監視」ボックスのどちらかを選択し、[OK] ボタンまたは [適用] ボタンをクリックする。
 - 選択した監視ノードをダブルクリックして、[プロパティ] 画面を表示し、[全般] ページの「監視」「非監視」ボックスのどちらかを選択し、[OK] ボタンまたは [適用] ボタンをクリックする（監視オブジェクト限定）。

❗ 重要

- 上位監視グループの監視状態が「非監視」の場合、下位監視ノードだけを「監視」にすることはできません。
- 監視ノードの監視状態を「非監視」にすると、状態は「初期状態」に戻ります。

7.1.3 監視ノードを検索する

監視ノードを検索する手順について説明します。監視ツリーの監視範囲設定が有効になっている場合、仮想ルートノードを基点に検索できません。また、仮想ルートノードは検索対象になりません。

監視ノードを検索する手順を次に示します。

1. ツリー表示領域または詳細表示領域に表示された監視グループを選択する。

検索できる監視ノードは、選択した監視グループおよびその監視グループ下の監視ノードに限定できません。

2. 次に示すどちらかの方法で [検索] 画面を表示する。

- メニューバーから [表示] - [検索] 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 [検索] を選択する。

3. [検索] 画面で条件を入力し、[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。

一覧表示された監視ノードに対して次の操作ができます。

- 監視ノードの状態、監視状態を変更する。
監視ノードの状態、監視状態を変更する場合は、右クリックしてポップアップメニューを表示してください。
- 目的とする監視ノードを選択した状態で [監視ツリー] 画面を表示する。
この場合は、ダブルクリックしてください。

7.1.4 状態変更イベントを検索する

状態変更イベントを検索する手順を次に示します。

1. 状態が変わった監視ノードを選択する。

2. 次に示すどれかの方法で状態変更イベント検索を実行する。

- メニューバーから [表示] - [状態変更イベント検索] 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 [状態変更イベント検索] を選択する。
- 詳細表示領域下にある [状態変更イベント検索] ボタンをクリックする。

監視オブジェクトに対し、状態変更イベント検索を実行した場合、その監視オブジェクトの、状態変更条件に合致した JP1 イベントが、発生 of 古い順に 100 件まで [イベントコンソール] 画面の [イベント検索] ページに表示されます (101 件以降は表示されません)。このため、検索結果として表示される JP1 イベントが増えてきたら、適宜、監視オブジェクトの状態を手動で変更することをお勧めします。

なお、監視オブジェクトの状態変更条件に合致した JP1 イベントが 100 件を超えた場合には、警告の JP1 イベント (イベント ID = 00003FB1) が発行されます。この JP1 イベントが発行された場合には、状態変更条件に合致した JP1 イベントへの対処を確認し、監視オブジェクトの状態を手動で変更してください。

監視グループに対し、状態変更イベント検索を実行した場合、その監視グループ配下の各監視オブジェクトの、状態変更条件に合致した JP1 イベントが、発生 of 古い順に 100 件まで [イベントコンソール] 画面の [イベント検索] ページに表示されます (101 件以降は表示されません)。ただし、監視グループの状態変更条件を定義している場合には、下位の監視ノードの状態を変更したイベントがあっても、対策の必要がある状態変更イベントだけ、発生 of 古い順に 100 件まで表示されます。

❗ 重要

- 監視ノードの状態を手動で変更すると、状態変更イベントの履歴がクリアされるため、それまでに発生していた状態変更イベントを検索 (表示) できなくなります。監視ノードの状態を手動で変更する前に、状態変更条件に合致した JP1 イベントへの対処を確認してください。
- 状態変更イベント検索で検索できる JP1 イベントは、ユーザーフィルターによって制限された JP1 イベントとなります (ユーザーフィルターによる制限の対象となるユーザーの場合)。
- 状態変更イベントの検索をする場合は、前もって [イベントコンソール] 画面を起動しておくことをお勧めします。
- 監視オブジェクトの状態変更条件に合致する JP1 イベントが 100 件を超えた場合には、対処済み連動機能は無効になります。このため、検索結果として表示される JP1 イベントが増えてきたら、適宜、監視オブジェクトの状態を手動で変更することをお勧めします。

7.1.5 監視ノードの属性を表示する

監視ノードの属性を表示する手順を次に示します。

1. 監視ノードを選択する。
2. 次に示すどれかの方法で [プロパティ] 画面を表示する。
 - メニューバーから [表示] - [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] を選択する。
 - メニューバーから [オプション] - [状態変更条件] を選択する。

- メニューバーから [オプション] - [イベント発行条件] 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 [プロパティ] を選択する。
- ダブルクリックする (監視オブジェクト限定)。

なお、[プロパティ] 画面に表示される属性のうち幾つかは、JP1_Console_Operator 以上の操作権限を持つ JP1 ユーザーであれば変更できます。監視ノードの属性を変更する場合は、JP1_Console_Operator 以上の操作権限を持つ JP1 ユーザーでログインしてください。

7.1.6 ガイド情報を表示する

ガイド情報を表示する手順を次に示します。

1. 監視オブジェクトを選択する。
2. 次に示すどちらかの方法で [ガイド] 画面を表示する。
 - メニューバーから [表示] - [ガイド] 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 [ガイド] を選択する。

なお、状況に応じたガイド情報を表示するための条件や、ガイド情報の内容は、あらかじめガイド情報ファイルに定義する必要があります。

ガイド情報の機能、設定、および定義ファイルについて

- 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編集について
参照先：マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「6.6 ガイド情報の編集」
- 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)

7.1.7 [ビジュアル監視] 画面を表示する

[ビジュアル監視] 画面を表示する手順を次に示します。

1. 次に示すどちらかの方法で [ビジュアル監視画面を開く] 画面を表示する。
 - メニューバーから [表示] - [ビジュアル監視] を選択する。

- ツールバーの  をクリックする。

2. [ビジュアル監視画面を開く] 画面で表示したい [ビジュアル監視] 画面名を選択し, [OK] ボタンをクリックする。

7.1.8 ログインユーザーの一覧を表示する

JP1/IM - Manager (セントラルスコープ) にログインしている JP1 ユーザーの一覧を表示する手順を次に示します。

1. メニューバーの [オプション] - [ログインユーザー一覧] を選択する。

7.1.9 [監視ツリー] 画面の情報をローカルホストに保存する

ローカルホストに保存する手順を次に示します。

1. メニューバーから [ファイル] - [監視ツリーの状態を保存] を選択する。
ファイル選択画面が開きます。

2. ローカルホストの任意のフォルダに任意の名称を付けて保存する。
監視ツリーの情報が CSV 形式のファイルで保存されます。

監視ツリーの監視範囲設定が有効になっている場合, [監視ツリー] 画面の情報はローカルホストに保存できません。保存したい場合は, [監視ツリー(編集中)] 画面からローカルホストに保存してください。

7.2 [ビジュアル監視] 画面で監視する

監視オブジェクトの状態は、[ビジュアル監視] 画面で監視できます。

監視ツリーの監視範囲設定を有効にしている場合、[ビジュアル監視] 画面には、ログインしている JP1 ユーザーと同じ JP1 資源グループが設定されている監視ノードだけが表示されます。ただし、JP1 資源グループが JP1_Console で、JP1_Console_Admin 権限の JP1 ユーザーでログインしている場合は、すべての監視ノードが表示されます。

[ビジュアル監視] 画面は、次に示す手順で表示できます。

1. 次に示すどちらかの方法で [ビジュアル監視画面を開く] 画面を表示する。

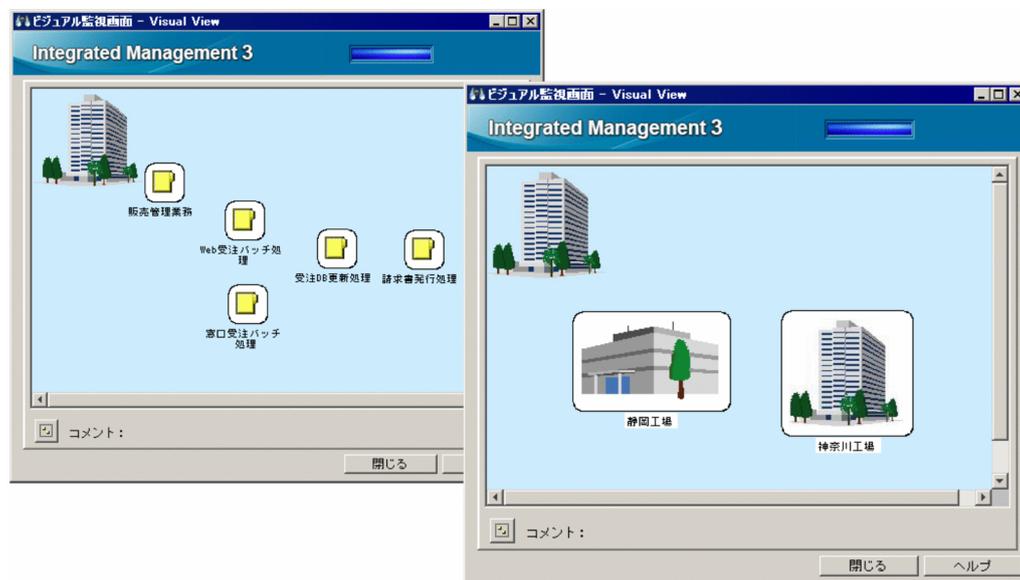
- [監視ツリー] 画面のメニューバーから [表示] - [ビジュアル監視] を選択する。
- [監視ツリー] 画面のツールバーの  をクリックする。

2. [ビジュアル監視画面を開く] 画面で表示したい [ビジュアル監視] 画面名を選択し、[OK] ボタンをクリックする。

監視ツリーの監視範囲設定が有効な場合、表示できる監視ノードが一つもないビジュアル監視画面は、[ビジュアル監視画面を開く] 画面の一覧に表示されません。

[ビジュアル監視] 画面の表示例を次に示します。

図 7-2 [ビジュアル監視] 画面の表示例



7.2.1 [ビジュアル監視] 画面から [監視ツリー] 画面を呼び出す

[ビジュアル監視] 画面から [監視ツリー] 画面を表示する手順を次に示します。

1. 監視ノードを選択し、ダブルクリックする。

[ビジュアル監視] 画面でダブルクリックした監視ノードを選択した状態で [監視ツリー] 画面が表示されます。

7.2.2 監視ノードの状態を変更する

[ビジュアル監視] 画面に表示された監視ノードの状態を変更する手順について説明します。なお、変更できる状態、変更時の動作は、監視ノードの種別（監視グループ、監視オブジェクト）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 導入・設計ガイド」の「5.2.2 監視ノードの状態」を参照してください。

監視ノードの状態を変更するには、JP1_Console_Operator 以上の権限が必要です。監視ツリーの監視範囲設定が有効な場合は、表示されている監視ノードのうち、JP1_Console_Operator 以上の権限でアクセスできる監視ノードだけ状態を変更できます。

監視ノードの状態を変更する手順を次に示します。

1. 監視ノードを選択する。

2. 右クリックして表示されるポップアップメニューから [状態変更] を選択し、ユーザーが意図する状態に変更する。

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。

7.2.3 監視ノードの監視状態を変更する

監視ノードの監視状態を変更する手順について説明します。なお、変更時の動作は、監視ノードの種別（監視グループ、監視オブジェクト）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 導入・設計ガイド」の「5.2.2 監視ノードの状態」を参照してください。

監視ノードの監視状態を変更するには、JP1_Console_Operator 以上の権限が必要です。監視ツリーの監視範囲設定が有効な場合は、表示されている監視ノードのうち、JP1_Console_Operator 以上の権限でアクセスできる監視ノードだけ状態を変更できます。

監視ノードの監視状態を変更する手順を次に示します。

1. 監視ノードを選択する。

2. 次に示すどれかの方法で監視ノードの状態を変更する。

- 右クリックして表示されるポップアップメニューから [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。

- 右クリックして表示されるポップアップメニューから [プロパティ] を選択し, [全般] ページの「監視」「非監視」ボックスのどちらかを選択し, [OK] ボタンまたは [適用] ボタンをクリックする。

❗ 重要

- 上位監視グループの監視状態が「非監視」の場合, 下位監視ノードだけを「監視」にすることはできません。上位監視グループの監視状態は, [監視ツリー] 画面で確認してください。
- 監視ノードの監視状態を「非監視」にすると, 状態は「初期状態」に戻ります。

7.2.4 監視ノードを検索する

監視ノードを検索する手順を次に示します。

1. 監視グループを選択する。

検索できる監視ノードは, 選択した監視グループおよびその監視グループ下の監視ノードに限定できません。

2. 右クリックして表示されるポップアップメニューから [検索] を選択する。

3. [検索] 画面で条件を入力し, [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。

一覧表示された監視ノードに対して次の操作ができます。

- 監視ノードの状態, 監視状態を変更する。
監視ノードの状態, 監視状態を変更する場合は, 右クリックしてポップアップメニューを表示してください。
- 目的とする監視ノードを選択した状態で [監視ツリー] 画面を表示する。
この場合は, ダブルクリックしてください。

7.2.5 状態変更イベントを検索する

状態変更イベントを検索する手順を次に示します。

1. 状態が変わった監視ノードを選択する。

2. 右クリックして表示されるポップアップメニューから [状態変更イベント検索] を選択する。

監視オブジェクトに対し, 状態変更イベント検索を実行した場合, その監視オブジェクトの, 状態変更条件に合致した JP1 イベントが, 発生 of 古い順に 100 件まで [イベントコンソール] 画面の [イベント検索] ページに表示されます (101 件以降は表示されません)。このため, 検索結果として表示される JP1 イベントが増えてきたら, 適宜, 監視オブジェクトの状態を手動で変更することをお勧めします。

なお、監視オブジェクトの状態変更条件に合致した JP1 イベントが 100 件を超えた場合には、警告の JP1 イベント（イベント ID = 00003FB1）が発行されます。この JP1 イベントが発行された場合には、状態変更条件に合致した JP1 イベントへの対処を確認し、監視オブジェクトの状態を手動で変更してください。

監視グループに対し、状態変更イベント検索を実行した場合、その監視グループ配下の各監視オブジェクトの、状態変更条件に合致した JP1 イベントが、発生 of 古い順に 100 件まで [イベントコンソール] 画面の [イベント検索] ページに表示されます（101 件以降は表示されません）。ただし、監視グループの状態変更条件を定義している場合には、下位の監視ノードの状態を変更したイベントがあっても、対策の必要がある状態変更イベントだけ、発生 of 古い順に 100 件まで表示されます。

❗ 重要

- 監視ノードの状態を手動で変更すると、状態変更イベントの履歴がクリアされるため、それまでに発生していた状態変更イベントを検索（表示）できなくなります。手動で変更する前に、状態変更条件に合致した JP1 イベントへの対処を確認してください。
- 状態変更イベント検索で検索できる JP1 イベントは、ユーザーフィルターによって制限された JP1 イベントとなります（ユーザーフィルターによる制限の対象となるユーザーの場合）。
- 状態変更イベントの検索をする場合は、前もって [イベントコンソール] 画面を起動しておくことをお勧めします。
- 監視オブジェクトの状態変更条件に合致する JP1 イベントが 100 件を超えた場合には、対処済み連動機能は無効になります。このため、検索結果として表示される JP1 イベントが増えてきたら、適宜、監視オブジェクトの状態を手動で変更することをお勧めします。

7.2.6 監視ノードの属性を表示する

監視ノードの属性を表示する手順を次に示します。

1. 監視ノードを選択する。
2. 右クリックして表示されるポップアップメニューから [プロパティ] を選択する。
[プロパティ] 画面が表示されます。

[プロパティ] 画面に表示される属性のうち幾つかは、JP1_Console_Operator 以上の操作権限を持つ JP1 ユーザーであれば変更できます。監視ノードの属性を変更する場合は、JP1_Console_Operator 以上の操作権限を持つ JP1 ユーザーでログインしてください。

7.2.7 ガイド情報を表示する

ガイド情報を表示する手順を次に示します。

1. 監視オブジェクトを選択する。

2. 右クリックして表示されるポップアップメニューから [ガイド] を選択する。

なお、状況に応じたガイド情報を表示するための条件や、ガイド情報の内容は、あらかじめガイド情報ファイルに定義する必要があります。

ガイド情報の機能, 設定, および定義ファイルについて

- 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編集について
参照先: マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「6.6 ガイド情報の編集」
- 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)

7.3 セントラルスコープの注意事項

- ツリー更新中にサービスを停止しないでください。監視オブジェクト DB の内容に不整合が発生することがあります。

監視オブジェクト DB に不整合が発生した場合、「KAVB7247-E JP1/IM - CS は JP1/IM - View からの操作要求が実行できませんでした (要因: データベースのレコード不正)」、 「KAVB7248-E JP1/IM - CS は JP1/IM - View からの操作要求が実行できませんでした (要因: データベースの操作不能)」などが出力されます。

その場合には、バックアップした監視オブジェクト DB をバックアップからリカバリーするか、`jcsdbsetup` コマンドで監視オブジェクト DB の再作成を行ってください。リカバリー手順については、「1.2.2(2) 監視オブジェクト DB のバックアップ・リカバリー手順」および「1.2.2(3) ホスト情報 DB のバックアップ・リカバリー手順」を参照してください。

- JP1/IM - Manager のセントラルスコープサービスが異常終了した場合や、強制終了された場合、セントラルスコープサービスで使用するデータベース (監視オブジェクト DB とホスト情報 DB) が壊れる可能性があります。このため、定期的にバックアップを行ってください。バックアップ・リカバリー手順については、「1.2.2(2) 監視オブジェクト DB のバックアップ・リカバリー手順」および「1.2.2(3) ホスト情報 DB のバックアップ・リカバリー手順」を参照してください。
- 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:

View パス¥log¥output

- JP1/Base のイベント DB を削除した場合、次の操作を行ってください。
 - JP1/IM - View の [監視ツリー] 画面を起動する。
 - 監視ツリーの最上位の監視ノードの状態が初期状態でない場合、初期状態に変更する。すでに初期状態の場合は、何もする必要はありません。

上記の操作を行わない場合、次のような現象が発生します。

- [監視ツリー] 画面の [状態変更イベント検索] で、間違ったイベントが表示される。
- ガイド機能で、別のガイドが表示される。
- JP1/IM - Manager のシステム構成定義で定義しているホスト名と、自動生成機能で収集した情報に含まれるホスト名が異なっていた場合、既存の監視ツリーに含まれる監視オブジェクトと同一の監視オブジェクトが差分として出力されます。例えば、JP1/IM のシステム構成定義で FQDN 形式で記述していたホスト名が、JP1/AJS2 のジョブ実行ホストでは、FQDN でない形式で定義されている場合、ジョブネット監視オブジェクトが差分として出力されます。不要であれば、差分として出力された監視オブジェクトは手動で削除してください。

- JP1/IM - Manager の起動直後、またはツリー更新中に JP1/IM - View の [監視ツリー] 画面を起動すると「KAVB7240-W JP1/IM - CS は JP1/IM - View からの操作要求 (監視ツリー取得) が一時的に実行できませんでした (要因: データベースが他の利用者により使用中)」が表示され、[監視ツリー] 画面が起動されません。その場合には、時間を置いてから [監視ツリー] 画面を再度起動してください。
- JP1/SES 形式のイベントを監視する場合、個別条件または共通条件に、基本属性のメッセージ・詳細情報を状態変更条件として設定する事はできません。
- JP1 イベントのメッセージ・詳細情報・拡張属性に関して、監視ノードの状態変更条件でサポートされる文字コードは、C (英語コード)、SJIS (シフト JIS コード)、EUCJIS (EUC コード)、UTF-8 です。
- 監視グループにおいて、監視グループの状態が初期状態以外で、かつ監視グループで表示されるガイド情報のガイド表示条件に、JP1 イベントの基本属性、または拡張属性が含まれている場合、この監視グループの状態が初期状態にならないと、表示されるガイド情報は変わりません。

例えば、監視グループの直下にエラー状態の監視オブジェクトと警告状態の監視オブジェクトが存在した場合で説明します。

監視グループはエラー状態になっており、また監視グループでは、エラー状態の監視オブジェクトの状態変更条件に合致した JP1 イベントをガイドの表示条件としたガイドが表示されているとします。

このとき、エラー状態の監視オブジェクトの状態を初期状態に変更し、その結果監視グループの状態が警告状態に変化しても、監視グループで表示されるガイド情報は変わりません。

警告状態の監視オブジェクトを初期状態に変更し、監視グループの状態が初期状態になると、表示されるガイド情報が変わるか、あるいは表示されなくなります。

監視グループで表示されるガイドの表示条件には、監視ノード ID だけを指定し、JP1 イベントの基本属性、または拡張属性を含めない定義を記述することを推奨します。

このように定義することにより、監視グループでガイドを表示させた場合に、監視グループの状態に関係なく常に同じガイドを表示させることができます。

また、このとき、監視ノード ID だけをガイドの表示条件に指定したガイドの定義は、JP1 イベントの基本属性、または拡張属性を含むガイドの表示条件のガイドの定義よりも前に記述してください。

- サーバの監視オブジェクト DB へのデータ更新の初期設定は、非同期書き込みです。
- クラスタ構成で次の設定を行うとサーバへのデータ更新時に同期書き込みをするようになります。
 - (a) 物理ホスト環境、論理ホスト環境すべての JP1/IM - Manager を停止する。
 - (b) 次の内容のテキストファイルを作成する (“ 論理ホスト名 ” の部分は、設定する論理ホストの論理ホスト名を記述する)。


```
[論理ホスト名]JP1SCOPE[BMS]
"DB_ACC_MODE_SYNC"=dword:00000000
```
 - (c) (b) で作成したテキストファイルを引数に指定して、実行系および待機系で次のコマンドを実行する。

jbssetcnf 作成したファイル

監視オブジェクト DB に同期書き込みを行う設定にすると、サーバへのデータ更新の性能が落ちますが、論理ホストのフェイルオーバー時に監視オブジェクト DB が破損しにくくなるため、クラスタ環境の場合は上記設定を行う事を推奨します。
- 同期書き込みの設定を非同期書き込みに戻す場合は、次の手順で行ってください。

(a) 物理ホスト環境, 論理ホスト環境すべての JP1/IM - Manager を停止する。

(b) 次の内容のテキストファイルを作成する(下記” 論理ホスト名” の部分は, 設定する論理ホストの論理ホスト名を記述する)。

[論理ホスト名¥JP1SCOPE¥BMS]

```
"DB_ACC_MODE_SYNC"=dword:00000001
```

(c) (b) で作成したテキストファイルを引数に指定して, 実行系および待機系で次のコマンドを実行する。
jbssetcnf 作成したファイル

- 監視オブジェクトの状態変更条件に指定するホスト名には, 次のどれかのホスト名を指定してください。下記ホスト名を指定しない場合, JP1 イベントが発生しても監視オブジェクトの状態が変化しないことがあります。

(a) hostname コマンドで返されるホスト名

(b) ホスト情報 DB に登録したホスト名

(b)の設定方法に関しては, マニュアル「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」にある, jcshostsimport コマンドを参照願います。

- JP1/IM - Manager の管理対象ホストおよびマネージャホストには, 次のホスト名を設定してください。下記ホスト名を設定しない場合, 監視ツリーの自動生成機能を使用したときに, 該当ホストの監視ノードが表示されないことがあります。

(a) hostname コマンドで返されるホスト名

JP1/IM - Manager の管理対象ホストおよびマネージャホストの設定方法については, マニュアル「JP1/Base 運用ガイド」の「構成定義ファイル (jbs_route.conf)」を説明している章を参照してください。

- 監視ツリーの自動生成機能で大量の監視ノードを自動生成する場合, 監視ツリーの自動生成がタイムアウトする事があります。その場合, JP1/IM - Manager の管理対象ホストで自動生成のセットアップコマンドを実行し自動生成の設定を解除して, 自動生成機能で生成される監視ノードの数を減らしてください。また, JP1/IM - Manager の管理対象ホストで JP1/Base の起動していないホストが複数ある場合, 監視ツリーの自動生成がタイムアウトする事があります。その場合, JP1/Base を起動するか, JP1/Base の起動していないホストを JP1/IM - Manager の管理対象ホストからはずしてください。

- 「業務指向ツリー」のテンプレートで監視ツリーを自動生成する場合, < AJS2 ホスト名>の監視グループ配下の JP1/PFM の監視オブジェクトは, < AJS2 ホスト名>のホストで JP1/PFM が監視するリソースまたはアプリケーションに対応して生成されます。< AJS2 ホスト名>が属する<ジョブネット名>の監視グループが表すジョブネットに関係しないリソースまたはアプリケーションの監視オブジェクトは, 手動で削除してください。

< Cosminexus 運用管理エージェントホスト名>の監視グループ配下の JP1/PFM の監視オブジェクトについても同様に, < Cosminexus 業務> の監視グループが表す J2EE アプリケーションに関係しないリソースまたはアプリケーションの監視オブジェクトは手動で削除してください。

- JP1/Cm2/NNM を監視するために, 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) を編集する場合は, サンプルファイル (snmpfilter_im_sample.conf) 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のみをフィルター定義ファイルに追加してください。なお, フィルター定義ファイルの定義内容を次の式で 900 バイト以内としてください。

$((a1+1)+(a2+1)+(a3+1)+(a4+1)\dots\dots(an+1))+34 < 900$ バイト

・ an: snmpfilter.conf で定義されている SNMP トラップの OID 長 (OID が 【.1.2.3.4.5】 の場合, an は 10 バイトになります)。

・ snmpfilter.conf に一般トラップが定義されている場合, フィルターサイズは [上記計算式の結果+(一般トラップ数×2)] になります。

・ フィルターはフィルターファイル (snmpfilter.conf) で定義されている内容を元に, 該当するオブジェクト ID (OID) を NNM の trapd.conf から取得したものです。

・ セントラルスコープの [共通条件設定] 画面の [共通条件設定] 一覧に, 次の共通条件が表示されますが, 使用しません。

- ・ System Alert Event (SSO), Application Alert Event (SSO) など JP1/Cm2/SSO 関連の共通条件
- ・ System Error Event (SCIM), System Warning Event (SCIM) など SCIM 関連の共通条件
- ・ Physical Host Emergency Event (System Manager) など System Manager 関連の共通条件

・ セントラルスコープの [新規監視ノード作成] 画面の [監視ノード種別] 一覧に, 以下の監視オブジェクトが表示されますが, 使用しません。

- ・ System Alert Event (SSO), Category Monitoring (SSO) など JP1/Cm2/SSO 関連の監視オブジェクト
- ・ System Error Event (SCIM), System Warning Event (SCIM) など SCIM と関連の監視オブジェクト
- ・ Physical Host Monitoring (System Manager) など System Manager 関連の監視オブジェクト

・ セントラルスコープの [自動生成-構成選択] 画面の [生成ツリー] 一覧に, 以下のツリー生成テンプレートが表示されますが, 使用しません。

- ・ システム構成ツリー

・ セントラルスコープの JP1 イベント受信性能向上に向けたチューニングポイントについて

JP1/IM - Manager の JP1 イベント受信時において, セントラルスコープでは受信した JP1 イベントと監視ツリー中の各監視オブジェクトの状態変更条件との比較処理を行うため, 監視オブジェクトの数が増大した場合, この比較回数が増大し, セントラルコンソール含めた JP1/IM - Manager 全体の JP1 イベント受信性能の性能劣化の要因となります。この性能劣化を防止し, セントラルスコープの JP1 イベント受信性能向上を行うためのチューニングポイントを次に示します。

(a)状態変更条件メモリー常駐機能を有効にすることにより, JP1 イベント受信時のセントラルスコープの処理でのディスクアクセス回数を削減でき, JP1 イベントの受信性能の向上が期待できます。

(b)セントラルスコープは, 比較対象の状態変更条件の削減のため, JP1 イベント受信時に状態変更条件中の以下の項目を用いてフィルター処理を行います。

- ・ 共通条件
- ・ 個別条件としてホスト名(比較方法として[ホスト名比較] を設定した個別条件)

そのため, 監視オブジェクトの状態変更条件には上記の項目を設定することにより, 比較対象の状態変更条件を減らすことができ, JP1 イベントの受信性能

の向上が期待できます。

- システム監視オブジェクト [NNMi 監視] または [ノード監視(NNMI)] を使用する場合は、JP1/IM-EG for NNMi が発行する、NNMi インシデントを変換した JP1 イベントに、拡張属性 NNMI_FAMILY_UK を設定してください（デフォルトでは設定されません）。

拡張属性 NNMI_FAMILY_UK を設定しない場合、システム監視オブジェクト [NNMi 監視] または [ノード監視(NNMI)] による監視を行うことができません。拡張属性 NNMI_FAMILY_UK の設定手順については、マニュアル「JP1/Integrated Management 2 - Event Gateway for Network Node Manager i」を参照してください。

8

JP1/IM によるシステムの操作

この章では、JP1/IM - View を使用したシステムの操作について説明します。この章で説明する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. [イベントコンソール] 画面」および「4. [監視ツリー] 画面」を参照してください。

8.1 コマンドを実行する

エージェントホストまたはマネージャーホストでコマンドを実行できます。また、クライアントホスト（ビューアーのホスト）のコマンド（クライアントアプリケーション）も実行できます。この機能は、JP1/IM - View から JP1/IM - Manager（セントラルコンソール）に接続している場合に使用できます。

なお、コマンド実行中のホストの JP1/Base を終了すると、Windows の場合は CMD.EXE と実行中のコマンド、UNIX の場合は shell と実行中のコマンドの状態が実行中のまま残る場合があります。その場合は、手動でコマンドを停止させるか、そのホストを再起動してください。

また、コマンド実行中にそのホストの JP1/Base を終了すると、キューイング中のコマンドは破棄されます。

8.1.1 【実行コマンド】でコマンドを実行する

次の操作には、JP1_Console_Admin 権限または JP1_Console_Operator 権限が必要です。

- エージェントホストでコマンドを実行する。
- マネージャーホストでコマンドを実行する。
- クライアントアプリケーションを実行する。

なお、イベント情報を引き継ぐコマンドを実行する場合は、JP1 イベントを選択してから実行してください。

操作方法を次に示します。

1. 【イベントコンソール】画面で、【オプション】 - 【コマンド実行】を選択する、またはツールバーから  をクリックする。

【コマンド実行】画面が表示されます。

2. 【コマンド種別】を選択する。

管理対象ホスト（エージェントホストまたはマネージャーホスト）上のコマンドを実行する場合は、【管理対象ホストのコマンド】ラジオボタンを選択します。

クライアントアプリケーションを実行する場合は、【クライアントアプリケーション】ラジオボタンを選択します。

3. 必要に応じて、【引き継ぎ情報】を指定する。

イベント情報を引き継ぐ場合は、【情報を引き継ぐ】チェックボックスをチェックします。

4. 【実行ホスト名】にコマンドを実行するホストを指定する。

実行ホスト名には、システム構成定義で管理対象ホストに設定したホスト名を指定します。

過去に指定したホスト名をリストボックスから選択できます。リストボックスには、過去に指定したホスト名が最大5個保存されます。

手順3で「情報を引き継ぐ」チェックボックスをチェックした場合は、イベント情報が引き継がれ、自動で入力されます。

コマンドの実行ホストには、ホストグループ名も指定できます。ホストグループ名を指定すると、ホストグループを構成するすべてのホストでコマンドが実行されます。指定できるホストグループ名は、ログインしているマネージャーで定義されているホストグループ名です。

ホストグループを定義する手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.16 コマンド実行環境の設定 (Windows の場合)」、 「2.15 コマンド実行環境の設定 (UNIX の場合)」を参照してください。

また、業務グループまたは監視グループを設定している場合、業務グループまたは監視グループを実行ホスト名に指定できます。実行ホスト名に次のように指定してください。

例：業務グループ「経営システム」を実行ホスト名に指定する場合

/経営システム

指定方法に関する詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「4.1.4(3) 業務グループの指定方法」を参照してください。

5. [実行コマンド] で実行するコマンドを指定する。必要に応じて、[環境変数ファイル] も指定する。

実行するコマンドラインを [実行コマンド] に入力します。

過去に指定したコマンドをリストボックスから選択することもできます。また、過去に指定したコマンドの履歴を消したい場合は、[履歴のクリア] ボタンをクリックします。

[環境変数ファイル] には、コマンド実行先ホストにある環境変数ファイルを絶対パスで指定します。

実行できるコマンドを次に示します。

コマンドを実行するホストが Windows の場合

- 実行形式ファイル(.com, .exe)
- バッチファイル(.bat)
- JP1/Script のスクリプトファイル(.spt) (ただし、.spt ファイルが実行できるよう関連づけが設定されていること)
- 自動アクションで実行できるアプリケーションに関連づけられているファイルタイプ (拡張子) を持つデータファイル(.vbs など)

コマンドを実行するホストが UNIX の場合

- UNIX のコマンド
- シェルスクリプト

ただし、次のようなコマンドは実行できません。

- 対話操作を必要とするコマンド
- 画面を表示するコマンド
- エスケープシーケンスや制御コードを伴うコマンド
- デーモンなどの、終了しないコマンド

- Windows メッセージ機構、DDE など、デスクトップとの対話が必要なコマンド（Windows の場合）
- shutdown や halt など、OS をシャットダウンするコマンド

6. [実行] ボタンをクリックする。

[引き継ぎ情報] で [情報を引き継ぐ] チェックボックスをチェックしない場合

[コマンド種別] で選択したコマンド種別のコマンドが、[実行ホスト] で指定したホストで実行されます。コマンドが実行されると、[実行結果] に、実行時刻、ホスト名、およびメッセージが表示されます。以降の手順は必要ありません。

[引き継ぎ情報] で [情報を引き継ぐ] チェックボックスをチェックした場合

[コマンド実行内容プレビュー] 画面が表示されます。次の手順に進んでください。

7. [コマンド実行内容プレビュー] 画面の内容を確認する。

変数を置き換えたあとの [実行ホスト名]、[実行コマンド]、および [環境変数ファイル] の内容を確認します。

❗ が表示されている項目は、設定に誤りがあります。設定を見直してください。

[コマンド実行内容プレビュー] 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「3.41 [コマンド実行内容プレビュー] 画面」を参照してください。

8. [実行] ボタンをクリックする。

[コマンド実行内容プレビュー] 画面に表示されている内容に問題がなければ、コマンドが実行され、[コマンド実行内容プレビュー] 画面が閉じられます。コマンドが実行されると、[コマンド実行] 画面の [実行結果] に、実行時刻、ホスト名、およびメッセージが表示されます。

8.1.2 [コマンド] ボタンでコマンドを実行する

[コマンド] ボタンにあらかじめ登録してあるコマンドを実行するには、コマンドを実行するホストに応じて次の 2 とおりがあります。

- エージェントホストまたはマネージャーホストでコマンドを実行する
- 選択したイベントの登録ホストに定義されたコマンドを実行する

コマンドを実行するには、JP1_Console_Admin 権限または JP1_Console_Operator 権限が必要です。カーソルを [コマンド] ボタンの上に合わせると、[コマンド実行] 画面に [コマンド] ボタンに設定した内容が表示されます。コマンドを実行する前に、必ずコマンドの内容を確認してください。

なお、イベント情報を引き継ぐコマンドを実行する場合は、JP1 イベントを選択してから実行してください。

[コマンド] ボタンの設定については、次の個所を参照してください。

- Windows の場合

マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.16 コマンド実行環境の設定 (Windows の場合)」

- UNIX の場合

マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「2.15 コマンド実行環境の設定 (UNIX の場合)」

(1) エージェントホストまたはマネージャーホストでコマンドを実行する

エージェントホストまたはマネージャーホストで、即時にコマンドを実行する場合の操作方法を次に示します。

(a) 即時にコマンドを実行する

[コマンド] ボタンをクリック後、即時にコマンドを実行できるように事前に次の内容を設定してください。

コマンド実行時に、イベント情報を引き継がない場合

コマンドボタン定義ファイルの`qui`パラメーターで`true`を指定してください。指定しておくと、[コマンド] ボタンをクリックしたあと、コマンドを実行してもよいかを確認するメッセージが表示されないので、エージェントホストまたはマネージャーホストですぐにコマンドが実行されます。

コマンド実行時に、イベント情報を引き継ぐ場合

コマンドボタン定義ファイルの`preview`パラメーターで`false`を指定してください。指定しておくと、[コマンド] ボタンをクリックしたあと、[コマンド実行内容プレビュー] 画面が表示されないので、すぐにコマンドが実行されます。

即時にコマンドを実行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] - [コマンド実行] を選択する、またはツールバーから  をクリックする。

[コマンド実行] 画面が表示されます。

2. 実行したいコマンドが登録されている [コマンド] ボタンをクリックする。

コマンドが実行されます。

(b) コマンドの登録内容を変更してからコマンドを実行する

コマンドの登録内容を変更してからコマンドを実行する場合の操作方法を次に示します。

イベント情報を引き継ぐ設定のコマンドを実行する場合は、コマンドの実行時に [コマンド実行内容プレビュー] 画面が表示され、コマンドの内容を変更できます。この操作は、イベントを引き継がない管理対象ホストのコマンドを実行する場合に有効です。

1. [イベントコンソール] 画面で、[オプション] - [コマンド実行] を選択する、またはツールバーから  をクリックする。

[コマンド実行] 画面が表示されます。

2. 実行したいコマンドが登録されている [コマンド] ボタンを右クリックしてポップアップメニューを表示する。

3. ポップアップメニューの [カスタム実行] をクリックする。

[コマンド実行] 画面の [コマンド種別], [引き継ぎ情報], [実行ホスト名], [実行コマンド], [環境変数ファイル] の項目に [コマンド] ボタンの設定内容が表示され、編集できる状態になります。

[実行ホスト名], [実行コマンド], [環境変数ファイル] の各項目を必要に応じて編集します。

4. [実行] ボタンをクリックする。

エージェントホストまたはマネージャーホストでコマンドが実行されます。

(2) 選択したイベントの登録ホストに定義されたコマンドを実行する

イベントの登録ホストが調査対象ホストや障害対策の対象ホストである場合、実行ホスト名に何も指定しないで [コマンド] ボタンを定義しておくとし、[コマンド] ボタンをクリックしたとき、選択したイベントの登録ホストに定義されたコマンドを実行できます。なお、登録ホストに対し、別の JP1 イベントの属性をマッピングしていても、[実行ホスト名] にはマッピング前の登録ホストが設定されます。

選択したイベントの登録ホストに定義されたコマンドを実行する手順を次に示します。

1. [イベント詳細] 画面で、[コマンド実行] ボタンを選択する。

[コマンド実行] 画面が表示されます。

2. 実行したいコマンドが登録されている [コマンド] ボタンをクリックする。

コマンド実行時に、イベント情報を引き継がない場合

コマンドを実行してもよいかを確認するメッセージが表示されるので、問題なければ [はい] ボタンをクリックします。

選択したイベントの登録ホストに定義されたコマンドが実行されます。なお、コマンドボタン定義ファイルの `qui` パラメーターで `true` を指定している場合、メッセージが表示されず、すぐにコマンドが実行されます。以降の手順は必要ありません。

コマンド実行時に、イベント情報を引き継ぐ場合

コマンドボタン定義ファイルの `preview` パラメーターで `false` を設定している場合、[コマンド実行内容プレビュー] 画面が表示されず、すぐにコマンドが実行されます。以降の手順は必要ありません。

`true` を設定している場合、[コマンド実行内容プレビュー] 画面が表示されます。次の手順に進んでください。

3. [コマンド実行内容プレビュー] 画面の内容を確認する。

変数を置き換えたあとの [実行ホスト名], [実行コマンド], および [環境変数ファイル] の内容を確認します。

⚠ が表示されている項目は、設定に誤りがあります。設定を見直してください。

[コマンド実行内容プレビュー] 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「3.41 [コマンド実行内容プレビュー] 画面」を参照してください。

4. [実行] ボタンをクリックする。

[コマンド実行内容プレビュー] 画面に表示されている内容に問題がなければ、コマンドが実行され、[コマンド実行内容プレビュー] 画面が閉じられます。コマンドが実行されると、[コマンド実行] 画面の [実行結果] に、実行時刻、ホスト名、およびメッセージが表示されます。

8.1.3 コマンドを実行するユーザー

コマンドは、コマンド実行先ホストのユーザーマッピング定義に従って、JP1/IM - Manager (セントラルコンソール) にログインした JP1 ユーザーを OS のユーザー名にマッピングして実行されます。ユーザーマッピング定義がされていない、またはログインした JP1 ユーザー名がユーザーマッピング定義に登録されていない場合は、コマンドを実行できません。

UNIX の場合、コマンドはマッピングされた OS ユーザーのシェル環境を使用して実行されます。2 バイト文字を使用したコマンドを実行する場合には、OS ユーザーのシェル環境を 2 バイト文字に対応した環境にしてください。

ユーザーマッピングの定義については、マニュアル「JP1/Base 運用ガイド」を参照してください。

8.1.4 コマンドの実行状態を確認または削除する

JP1/IM - View の [コマンド実行] 画面からコマンドを実行した際に、[実行結果] に実行終了を通知するメッセージ (KAVB2013-I) が表示されない場合、コマンド実行先ホストでトラブルが発生しているおそれがあります。

この場合は次の手順に従ってコマンドの実行状態を確認し、必要であればコマンドを削除してください。

❗ 重要

ここで示す手順は、コマンド実行先ホストの JP1/Base のバージョンが 07-10 以降の場合にだけ行えます。JP1/Base のバージョンが 07-00 以前の場合には行えません。

1. jcocmdshow コマンドでコマンドの状態を確認する。

コマンドを実行しているホストに対して、jcocmdshow コマンドを実行し、返される情報を基にトラブルが発生していないか調査します。調査の結果、コマンドを停止する必要があると判断した場合は次の手順に進んでください。

2. jcocmddel コマンドでコマンドを削除する。

コマンドを実行しているホストに対して、jcocmddel コマンドを実行し、コマンドを削除します。

3. jcocmdshow コマンドでコマンドの状態を確認する。

コマンドが正しく削除されたかどうかjcocmdshow コマンドを実行し、確認します。

コマンドの文法について

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

8.2 自動アクションの状況を確認し、自動アクションの操作を行う

特定の JP1 イベントを受信したときに、自動的にアクション（コマンド）を実行できます。この機能を自動アクションと呼びます。アクションは、自動アクションの定義を保存したホストだけでなく、エージェントホストまたはマネージャーホストでも実行できます。

自動アクションの定義方法については、下記参照先を参照してください。

- 自動アクションの設定（GUI で設定する場合）
参照先：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」
- 自動アクションの設定（定義ファイルで設定する場合）
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「自動アクション定義ファイル (actdef.conf)」(2. 定義ファイル)

自動アクションの状況確認には、次に示す 3 種類があります。

- 自動アクションの実行状況の確認
自動アクションの実行処理でトラブルが発生していないかどうかを確認します。
- 自動アクションの実行結果の確認と操作（自動アクションのキャンセル，再実行）
実行した自動アクションの実行結果を確認します。また、必要に応じて詳細情報の確認をしたり，手動による自動アクションの再操作をしたりします。
- 自動アクション機能の稼働状況の確認
自動アクション機能が稼働しているかどうかを確認します。稼働していない場合，自動アクションは実行されません。

ここでは、これらの確認方法，自動アクションの操作方法について説明します。

8.2.1 自動アクションの実行状況を確認する

自動アクションの実行監視（遅延監視，状態監視）機能を有効にしておくことで，下記トラブルが発生した場合でも早期に検知できます。

- 自動アクションが想定した時間内に終了しなかった。または，長時間掛かって終了した。
- 自動アクションの実行に失敗した（状態が「実行不可」「実行失敗」または「実行失敗（キャンセル失敗）」に遷移した）。

実行監視（遅延監視，状態監視）機能を有効にするかどうかは自動アクション定義時に前もって設定しておく必要があります。また，トラブル検知時に JP1 イベントを発行したり，通知コマンドを実行したりする設定が別途必要です。

設定の詳細については下記参照先を参照してください。

自動アクションの設定 (GUI で設定する場合)

参照先：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」

参照先：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」

自動アクションの設定 (定義ファイルで設定する場合)

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「自動アクション定義ファイル (actdef.conf)」(2. 定義ファイル)

JP1 イベントの発行設定, 通知コマンドの実行設定

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「自動アクション通知定義ファイル (actnotice.conf)」(2. 定義ファイル)

確認手順を次に示します。なお、異常検知後に実行監視機能（遅延監視，状態監視）を再度有効にするには、JP1_Console_Admin 権限または JP1_Console_Operator 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] 画面で自動アクションの実行状況を確認する。または、通知コマンドによって異常が発生したことが通知される。

JP1 イベントの発行設定をしていた場合は、イベント一覧にイベント ID 2010 または 2011 の JP1 イベントが表示されます。通知コマンドの実行設定をしていた場合は、通知コマンドによって異常が通知されます。

JP1 イベント，または通知コマンドによって異常が発生したことがわかった場合には次の手順に進んでください。

2. [アクション結果] 画面や [アクション結果一覧] 画面などを使用して、自動アクションの実行結果を確認し、必要に応じて対処する。

必要に応じて [アクション結果] 画面や [アクション結果一覧] 画面などを使用して、詳細確認やアクションのキャンセル，再実行をしてください。詳細については、「8.2.2 自動アクションの実行結果を確認する」を参照してください。

なお、遅延監視機能，状態監視機能による通知は，それぞれ一度実行されると，ユーザーが通知抑止を解除するまで通知が抑止されます。必要に応じて通知抑止を解除してください。抑止された機能を解除する場合には次の手順に進んでください。

3. [イベントコンソール] 画面のメニューから [オプション] - [機能状態通知復帰] - [アクション遅延監視] および [アクション状態監視] を表示し，活性している機能名を選択する。

抑止状態になっている機能は，表示（文字）が活性となります。活性している機能名を選択すると，通知抑止を解除するかどうか問い合わせるダイアログボックスが表示されます。

4. 問い合わせダイアログボックスで [はい] を選択する。

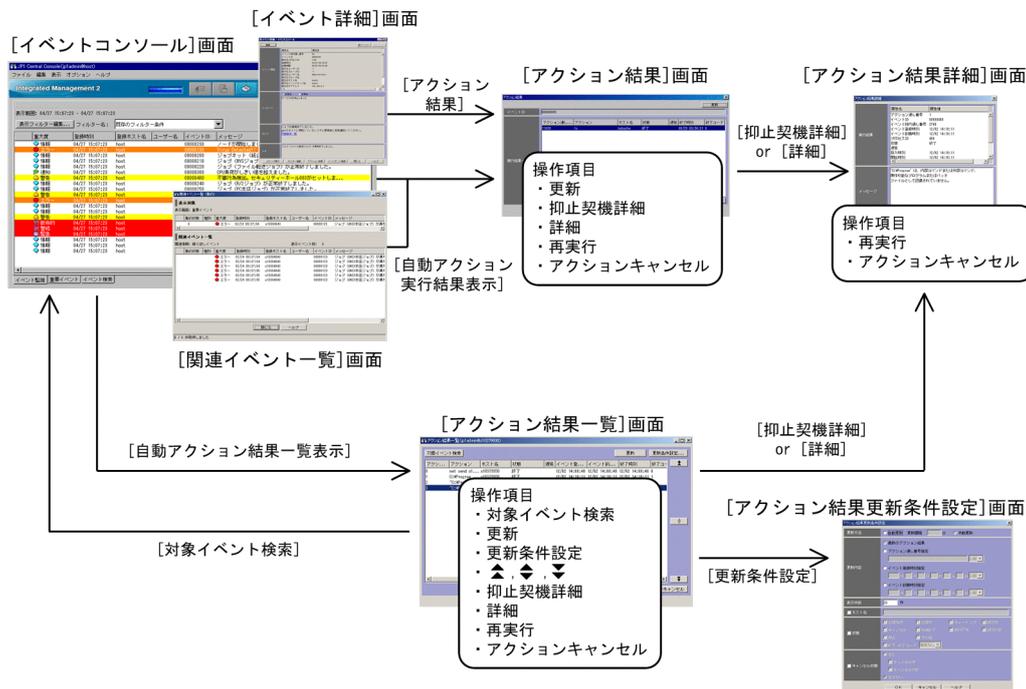
[はい] を選択すると、通知抑止が解除され、監視機能が再度有効になります。

8.2.2 自動アクションの実行結果を確認する

自動アクションの実行結果は、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] 画面で確認できます。また、jcashowa コマンドを使用して確認することもできます。

なお、[アクション結果] 画面や [アクション結果一覧] 画面からは、実行結果の確認だけでなく、アクションの詳細表示やアクションの再実行などの操作も行えます。自動アクションに関する画面遷移と操作項目を次の図に示します。

図 8-1 自動アクションに関する画面遷移と操作項目



操作項目は、アクションの実行結果に対し、詳細情報を表示するための項目と再操作（再実行，キャンセル）するための項目に分かれます。

ここでは、実行結果の確認方法、および再操作（再実行，キャンセル）方法について説明します。

(1) 自動アクションの実行結果を確認する

自動アクションの実行結果は、[アクション結果] 画面，[アクション結果一覧] 画面，またはjcashowa コマンドで確認できます。

(a) [アクション結果] 画面で実行結果を確認する

[アクション結果] 画面には、[イベントコンソール] 画面のイベント一覧で選択したイベントに設定されている自動アクションの実行結果を表示できます。

操作手順を次に示します。

1. [イベントコンソール] 画面のイベント一覧で、[アクション] の欄にアクションマークが表示されているイベントを 1 件選択する。

2. 次に示すどれかの方法で [アクション結果] 画面を表示する。

- メニューバーから [表示] - [自動アクション実行結果表示] を選択する。
- ポップアップメニューから [自動アクション実行結果表示] を選択する。
- [自動アクション実行結果表示] ボタンをクリックする。

[アクション結果] 画面が表示されます。

[アクション結果] 画面には、選択したイベント ID とそのイベント ID に設定されている自動アクションの実行結果が表示されます。

3. 各自動アクションの実行結果の詳細を知りたい場合、または状態が「抑止」となったアクションの抑止契機となった自動アクションの詳細を知りたい場合は、次に示す方法で [アクション結果詳細] 画面を表示する。

自動アクションの実行結果の詳細を知りたい場合

- [実行結果一覧] から自動アクションを選択し、[詳細] ボタンをクリックする。
- [実行結果一覧] に表示されている自動アクションをダブルクリックする。

抑止契機となった自動アクションを知りたい場合

- [実行結果一覧] から状態が「抑止」となった自動アクションを選択し、[抑止契機詳細] ボタンをクリックする。

[アクション結果詳細] 画面が表示されます。

実行結果と出力されたメッセージが表示されます。表示される実行結果の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.37 [アクション結果詳細] 画面」を参照してください。

[関連イベント一覧] 画面を表示している場合は、アクションマークの付いたイベント選択後、ポップアップメニューから [自動アクション実行結果表示] を選択して [アクション結果] 画面を表示できます。また、[イベント詳細] 画面を表示している場合は、[アクション結果] ボタンをクリックして、[アクション結果] 画面を表示できます。

(b) [アクション結果一覧] 画面で実行結果を確認する

[アクション結果一覧] 画面には、ログインしているマネージャーで設定した自動アクションの実行結果の一覧を表示できます。なお、表示する自動アクションの条件は、[アクション結果更新条件設定] 画面で設定します。

操作手順を次に示します。

1. [イベントコンソール] 画面で [表示] - [自動アクション結果一覧表示] を選択する。

[アクション結果一覧] 画面が表示されます。

ログインしているマネージャーで設定した自動アクションの中で、[アクション結果更新条件設定] 画面で設定された条件に合う自動アクションの実行結果の一覧が表示されます。

2. 自動アクションの実行結果を表示するための条件を変更したい場合は、[更新条件設定] ボタンをクリックする。

[アクション結果更新条件設定] 画面が表示されます。

更新方法（自動更新、手動更新）やアクション結果の取得範囲、更新時の表示件数や表示条件を指定できます。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「3.39 [アクション結果更新条件設定] 画面」を参照してください。

3. 自動アクションの実行結果の表示内容を更新条件に沿って更新したい場合は、[更新] ボタンをクリックする。

表示内容が、[アクション結果更新条件設定] 画面で設定された内容で更新されます。

4. リスト表示されている自動アクション以前に発生した自動アクションの実行結果を表示したい場合は

 を、以降に発生した自動アクションの実行結果を表示したい場合は  を、[アクション結果更新条件設定] 画面で設定した更新条件に従って再表示したい場合は  をクリックする。

5. 各自動アクションの実行結果の詳細を知りたい場合、または状態が「抑止」となったアクションの抑止契機となった自動アクションの詳細を知りたい場合は、次に示す方法で [アクション結果詳細] 画面を表示する。

自動アクションの実行結果の詳細を知りたい場合

- [実行結果一覧] から自動アクションを選択し、[詳細] ボタンをクリックする。
- [実行結果一覧] に表示されている自動アクションをダブルクリックする。

抑止契機となった自動アクションを知りたい場合

- [実行結果一覧] から状態が「抑止」となった自動アクションを選択し、[抑止契機詳細] ボタンをクリックする。

[アクション結果詳細] 画面が表示されます。

実行結果と出力されたメッセージが表示されます。表示される実行結果の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「3.37 [アクション結果詳細] 画面」を参照してください。

6. 自動アクションの実行契機となった JP1 イベントを表示したい場合は [実行結果一覧] から自動アクションを選択し、[対象イベント検索] ボタンをクリックする。

イベント検索が行われ [イベントコンソール] 画面の [イベント検索] ページに、自動アクションの実行契機となった JP1 イベントが表示されます。

(c) jcashowa コマンドで実行結果を確認する

自動アクションの実行結果を、jcashowa コマンドを使用して表示させることができます。jcashowa コマンドを実行するとアクション情報ファイルに格納されている、実行した自動アクションの結果を表示します。jcashowa コマンドは、JP1/IM - View のない環境や自動アクションの実行結果をファイル出力したいときなどに使用します。

コマンドの実行例を次に示します。7月1日の16時から17時の間に受信したJP1 イベントに対する自動アクションの実行結果を表示するには、マネージャーで次のように入力します。

```
jcashowa -d 07/01/16:00,07/01/17:00
```

jcashowa コマンドの文法、および実行結果の表示形式については、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「jcashowa」(1. コマンド)を参照してください。

(2) 自動アクションをキャンセルする

自動アクションの状態が次に示す状態のとき、その自動アクションをキャンセルできます。

- ・「送信待機」「キューイング」「実行中」
- ・「送信中 (キャンセル失敗)」「送信待機 (キャンセル失敗)」「キューイング (キャンセル失敗)」「実行中 (キャンセル失敗)」

キャンセルは、[アクション結果] 画面、[アクション結果一覧] 画面、[アクション結果詳細] 画面、またはjcacancel コマンドでできます。なお、画面を使ってキャンセルする場合にはJP1_Console_Admin 権限またはJP1_Console_Operator 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。

(a) [アクション結果] 画面、または [アクション結果一覧] 画面から自動アクションをキャンセルする

操作手順を次に示します。

1. [アクション結果] 画面、または [アクション結果一覧] 画面を表示する。
画面を表示する方法については、「8.2.2(1) 自動アクションの実行結果を確認する」を参照してください。
2. キャンセルしたい自動アクションを選択する。
3. [アクションキャンセル] ボタンをクリックする。
キャンセルするかどうかの確認ダイアログボックスが表示されます。
4. [OK] ボタンをクリックする。

選択した自動アクションのキャンセル要求の受け付けが完了します。

5. キャンセル後の状態を確認する場合は、[更新] ボタンをクリックする。

(b) [アクション結果詳細] 画面から自動アクションをキャンセルする

操作手順を次に示します。

1. [アクション結果詳細] 画面を表示する。

画面を表示する方法については、「8.2.2(1) 自動アクションの実行結果を確認する」を参照してください。

2. [アクションキャンセル] ボタンをクリックする。

キャンセルするかどうかの確認ダイアログボックスが表示されます。

3. [OK] ボタンをクリックする。

選択した自動アクションのキャンセル要求の受け付けが完了します。

4. キャンセル後の状態を確認する場合は、[閉じる] ボタンをクリックして [アクション結果] 画面または [アクション結果一覧] 画面に戻り、[更新] ボタンをクリックする。

(c) jcacancel コマンドから自動アクションをキャンセルする

自動アクションを、jcacancel コマンドを使用してキャンセルできます。jcacancel コマンドは、ホスト単位、システム単位で自動アクションの一括キャンセルしたいときなどに使用します。なお、このコマンドを使って自動アクションをキャンセルする場合には、どの自動アクションをキャンセルするのかを確認したあとに実行してください。確認方法については、「8.2.2(1) 自動アクションの実行結果を確認する」を参照してください。

コマンドの実行例を次に示します。host01 で状態がキューイング、実行中となっている自動アクションを一括キャンセルする場合には、マネージャーで次のように入力します。

```
jcacancel -s host01
```

jcacancel コマンドの文法、および実行結果の表示形式については、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「jcacancel」(1. コマンド)を参照してください。

(3) 自動アクションを再実行する

自動アクションの状態が次に示す状態のとき、その自動アクションを再実行できます。

- 「抑止」「終了」「実行失敗」「キャンセル」「強制終了」
- 「終了 (キャンセル失敗)」「実行失敗 (キャンセル失敗)」

再実行は、[アクション結果] 画面、[アクション結果一覧] 画面、または [アクション結果詳細] 画面から行えます。なお、これらの画面を使って再実行する場合には JP1_Console_Admin 権限または JP1_Console_Operator 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。

(a) [アクション結果] 画面、または [アクション結果一覧] 画面から自動アクションを再実行する

操作手順を次に示します。

1. [アクション結果] 画面、または [アクション結果一覧] 画面を表示する。
画面を表示する方法については、「8.2.2(1) 自動アクションの実行結果を確認する」を参照してください。
2. 再実行する自動アクションを選択する。
3. [再実行] ボタンをクリックする。
再実行要求をするかどうかの確認ダイアログボックスが表示されます。
4. [OK] ボタンをクリックする。
選択した自動アクションの再実行要求の受け付けが完了します。
5. 再実行後の状態を確認する場合は、[更新] ボタンをクリックして [アクション結果一覧] 画面を更新する。

(b) [アクション結果詳細] 画面から自動アクションを再実行する

操作手順を次に示します。

1. [アクション結果詳細] 画面を表示する。
画面を表示する方法については、「8.2.2(1) 自動アクションの実行結果を確認する」を参照してください。
2. [再実行] ボタンをクリックする。
再実行要求をするかどうかの確認ダイアログボックスが表示されます。
3. [OK] ボタンをクリックする。
自動アクションの再実行要求の受け付けが完了します。
4. 再実行後の状態を確認する場合は、[閉じる] ボタンをクリックして [アクション結果] 画面または [アクション結果一覧] 画面に戻り、[更新] ボタンをクリックする。

8.2.3 自動アクション機能の稼働状況を確認する

自動アクション機能が稼働していないと、自動アクションの実行契機となるイベントがマネージャー上のJP1/Baseに登録されても自動アクションが実行されません。自動アクション機能の稼働状況は、`jcastatus` コマンドを使用して確認できます。

`jcastatus` コマンドを実行すると、自動アクション機能の稼働状況（稼働、休止、または停止）に応じて、それぞれの状態を示す情報（`RUNNING`、`STANDBY`、または`STOP`）が標準出力に出力されます。稼働状況が「稼働（`RUNNING`）」であれば自動アクション機能は稼働しています。「休止（`STANDBY`）」の場合、自動アクション機能が稼働していないため、自動アクションが実行されません。稼働状態にするには`jcachange` コマンドを実行する必要があります。「停止（`STOP`）」の場合、JP1/IM - Manager が停止しているおそれがあります。この場合にはJP1/IM - Manager を再起動する必要があります。

詳細については、下記参照先を参照してください。

`jcastatus` コマンドの文法、表示形式について

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「`jcastatus`」(1. コマンド)

`jcachange` コマンドの文法、表示形式について

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「`jcachange`」(1. コマンド)

JP1/IM - Manager の起動・停止について

参照先：「[3. JP1/IM - Manager の起動と終了](#)」

8.3 統合機能メニューで他アプリケーションの画面を表示する

[統合機能メニュー] 画面には、JP1/IM と連携するプログラムの機能が一覧表示され、この画面からプログラムを起動できます。起動できるプログラムには次の 2 種類があります。

ビューアー上のアプリケーションプログラム

JP1/IM - View と同じホストにインストールされているアプリケーションプログラムのことです。統合機能メニューからプログラムを選択すると、実行ファイルが起動されます。

WWW ページ

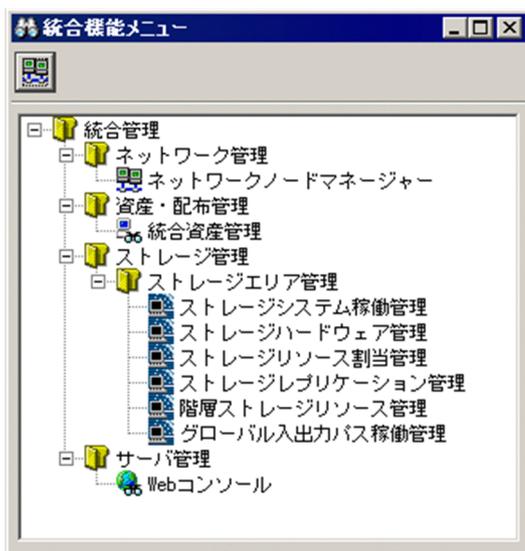
システム上のアプリケーションが WWW ページを提供している場合、その WWW ページを表示できます。統合機能メニューでプログラムを選択すると WWW ブラウザーが起動され、WWW ページが表示されます。

これらの機能を利用するには、WWW ページの URL を、あらかじめ設定しておく必要があります。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「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) を参照してください。

また、統合機能メニューを使用して、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 やブラウザなど) を事前に確認してください。

[統合機能メニュー] 画面の例を次に示します。

図 8-2 [統合機能メニュー] 画面の例



上図は、ビューアー上に JP1/IM と連携するアプリケーションプログラムを何もインストールしていない状態のときの [統合機能メニュー] 画面です。ビューアーにアプリケーションプログラムをインストールした場合は、そのインストールしたアプリケーションプログラムがツリーに追加された状態で表示されます。

連携するアプリケーションプログラムについては、「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。

8.3.1 [統合機能メニュー] 画面の操作

[統合機能メニュー] 画面には、JP1/IM と連携するプログラムの機能が、ツリー形式で表示されます。フォルダは機能の分類を表します。ツリーの末端をダブルクリックすると、WWW ページやアプリケーションプログラムの画面を表示できます。

操作方法を次に示します。

1. [イベントコンソール] 画面, [監視ツリー] 画面から [オプション] - [統合機能メニュー起動] を選択する。または、ツールバーから  をクリックする。

[統合機能メニュー] 画面が表示されます。

JP1/IM - View の `tuning.conf` ファイルで `[MENU_AUTO_START=ON]` が指定されている場合は、ログイン時に自動的に [統合機能メニュー] 画面が表示されます。JP1/IM - View の `tuning.conf` 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-View 設定ファイル (`tuning.conf`)」(2. 定義ファイル) を参照してください。

2. 統合機能メニューのツリーを展開して、表示したい項目をダブルクリックする。

選択した機能の画面が表示されます。

注意事項

統合機能メニューからアプリケーションプログラムを呼び出す場合、JP1/IM - View を起動した OS ユーザーに、呼び出すアプリケーションプログラムの実行権限がないとアプリケーションプログラムを起動できません。

呼び出すアプリケーションプログラムが実行できる権限で JP1/IM - View を起動する必要があります。

次の機能はツールバーのボタンからも呼び出せます。

表 8-1 ツールバーのボタンから呼び出せる機能

機能名	ボタン
ネットワークノードマネージャー	
Windows リモートコントロール	
資産・配布管理	 ※

注※ Windows では、JP1/NETM/DM Manager の WWW ページ版の動作条件を満たさないため、Windows 版の JP1/IM - View では、[資産・配布管理] ボタンは表示されません。JP1/NETM/DM は日本国内の製品名称です。

8.3.2 [統合機能メニュー] 画面から操作できる機能

[統合機能メニュー] 画面に表示される機能を次の表に示します。

なお、画面種別がアプリケーション画面で、該当するプログラムがビューアーにインストールされていない場合、機能名はメニューに表示されません。

連携製品の対応バージョン、および対応 OS の詳細については、各連携製品のマニュアルを確認してください。

表 8-2 [統合機能メニュー] 画面に表示される機能

メニュー項目			起動する機能の内容		
フォルダ名	サブフォルダ名	機能名	画面種別	プログラム名	インストール先
ネットワーク管理	-	ネットワークノードマネージャー	WWW ページ	JP1/Cm2/NNM	システム内のホスト
				HP NNM	
	-	インターネットゲートウェイ	アプリケーション画面	JP1/Cm2/Internet Gateway Server	JP1/IM - View がインストールされているホスト
ジョブ管理	-	ジョブスケジューラー	アプリケーション画面	JP1/AJS - View	JP1/IM - View がインストールされているホスト
	-	シナリオ運用	アプリケーション画面	JP1/AJS2 - Scenario Operation View	JP1/IM - View がインストールされているホスト
	-	プリントサービス	アプリケーション画面	JP1/NPS	JP1/IM - View がインストールされているホスト
	ファイル転送	-	伝送の登録／実行	アプリケーション画面	JP1/FTP
履歴情報の表示			アプリケーション画面		
自動プログラムの登録			アプリケーション画面		
資産・配布管理	-	統合資産管理	WWW ページ	JP1/NETM/Asset Information Manager	システム内のホスト
	-	資産・配布管理	WWW ページ	JP1/NETM/DM Manager	システム内のホスト
	-	設備資産管理	アプリケーション画面	JP1/NetInsight II - Facility Manager	JP1/IM - View がインストールされているホスト
	-	Windows リモートコントロール	アプリケーション画面	JP1/NETM/Remote Control Manager	JP1/IM - View がインストールされているホスト

メニュー項目			起動する機能の内容		
フォルダ名	サブフォルダ名	機能名	画面種別	プログラム名	インストール先
	—	配布／資産管理	アプリケーション画面	JP1/NETM/DM Manager	JP1/IM - View がインストールされているホスト
ストレージ管理	ストレージエリア管理	ストレージシステム稼働管理	WWW ページ	Hitachi Tuning Manager software	システム内のホスト
		ストレージハードウェア管理	WWW ページ	Hitachi Device Manager software	
		ストレージリソース割当管理	WWW ページ	Hitachi Provisioning Manager	
		ストレージレプリケーション管理	WWW ページ	Hitachi Replication Manager software	
		階層ストレージリソース管理	WWW ページ	Hitachi Tiered Storage Manager software	
		グローバル入出力パス稼働管理	WWW ページ	Hitachi Global Link Manager software	
サーバ管理	—	管理コンソール	アプリケーション画面	JP1/Server Conductor	JP1/IM - View がインストールされているホスト
	—	Web コンソール	WWW ページ		システム内のホスト
ハードウェア管理	—	SANRISE2000 Remote Console	アプリケーション画面	SANRISE	JP1/IM - View がインストールされているホスト
	—	SANRISE H512/H48 Remote Control XP	アプリケーション画面		
統合通報管理	—	通報ルール設定	アプリケーション画面	TELstaff または JP1/TELstaff	JP1/IM - View がインストールされているホスト

メニュー項目			起動する機能の内容		
フォルダ名	サブフォルダ名	機能名	画面種別	プログラム名	インストール先
メインフレーム連携	—	VOS3 コンソール操作	アプリケーション画面	VOS3 AOMPLUS(AOMPLUSCIF)	JP1/IM - View がインストールされているホスト
Cosminexus 運用管理	—	Cosminexus 運用管理ポータル	アプリケーション画面	Cosminexus Application Server	JP1/IM - View がインストールされているホスト

(凡例)

— : なし

9

IM 構成管理によるシステムの階層構成の管理

この章では、IM 構成管理を使用してシステムの階層構成（IM 構成）を管理する手順について説明します。この章で説明する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「5. IM 構成管理の画面」を参照してください。

9.1 ホストを管理する

JP1/IM システムの構成を変更する場合や、管理対象のホスト名や IP アドレスなどのホスト情報を変更する場合には、IM 構成管理 DB に登録されている管理対象ホストに関する情報を見直す必要があります。

IM 構成管理・ビューアーから次の作業を実施して、ホストの情報を管理してください。

ホストを登録する場合

IM 構成管理 DB に新しくホストを登録するには、[IM 構成管理] 画面から [ホスト登録] 画面を表示して設定します。

登録方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.1.1 ホストを登録する」を参照してください。

ホストを削除する場合

IM 構成管理 DB に登録されているホストは、[IM 構成管理] 画面の [ホスト一覧] ページで削除します。

削除方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.1.6 ホストを削除する」を参照してください。

ホストから情報を収集する場合

ホスト情報は、[IM 構成管理] 画面の [ホスト一覧] ページまたは [IM 構成] ページから収集します。

ホスト情報を収集するタイミングや収集方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.1.3 ホストから情報を収集する」を参照してください。

ホスト情報を変更する場合

IM 構成管理 DB に登録されているホスト情報は、[IM 構成管理] 画面から [ホスト属性編集] 画面を表示して変更します。

変更方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

なお、システムの階層構成 (IM 構成) に登録されているホスト名を編集した場合、システムの階層構成を反映し直す必要があります。反映方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

ホストの一覧を表示する場合

IM 構成管理 DB に登録したホストの一覧は、[IM 構成管理] 画面の [ホスト一覧] ページで表示します。

表示方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.1.4 ホスト情報を表示する」を参照してください。

9.2 システムの階層構成を管理する

システムの階層構成（IM 構成）を変更する場合に、IM 構成管理 DB に登録されているシステムの構成定義情報を見直す必要があります。

IM 構成管理・ビューアーから次の作業を実施して、システムの階層構成を管理してください。

システムの階層構成を取得する場合

システムの構成定義情報は、[IM 構成管理] 画面の [ホスト一覧] ページまたは [IM 構成] ページから取得します。システムを構成するすべてのホストから情報を取得できます。

取得方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

システムの階層構成を表示する場合

システムの階層構成は、[IM 構成管理] 画面の [IM 構成] ページで表示します。

表示方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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検証する場合

取得した構成定義情報と、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できます。構成定義情報は、[IM 構成管理] 画面の [ホスト一覧] ページまたは [IM 構成] ページで検証します。

検証方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.2.3 システムの階層構成を検証する」を参照してください。

システムの階層構成を編集する場合

構成定義情報を編集することで、ホストの追加、移動、削除ができます。構成定義情報は、[IM 構成管理] 画面から [エージェント構成編集] 画面または [リモート監視構成編集] 画面を表示して編集します。

編集方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

システムの階層構成を反映する場合

[エージェント構成編集] 画面、[リモート監視構成編集] 画面などで編集した構成定義情報を、システムを構成するすべてのホストに反映できます。構成定義情報は、[エージェント構成編集] 画面または [リモート監視構成編集] 画面で反映します。

反映方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

システムの階層構成の同期を取る場合

統合マネージャーと拠点マネージャーで、それぞれシステムの階層構成を定義した場合には、統合マネージャーと拠点マネージャーの間で、システムの階層構成の同期を取る必要があります。[IM 構成管理] 画面の [IM 構成] ページで実施します。

同期を取る方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

9.3 仮想化システム構成を管理する

IM 構成管理・ビューアーを操作、またはコマンドを実行して、仮想化ホストを含むシステムの階層構成（仮想化システム構成）を管理する方法について説明します。

なお、仮想化構成を管理するためには、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が必要です。使用できるソフトウェアについては、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。

9.3.1 仮想化システムのホストを登録する

IM 構成管理に仮想ホストを登録するには、[IM 構成管理] 画面から [ホスト登録] 画面を呼び出して登録します。

登録方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.3.1(2) 仮想化構成情報を設定する」を参照してください。

9.3.2 仮想化システムのホスト情報を表示する

システムの階層構成から、仮想ホストとして登録したホストの情報を表示する手順について説明します。ホストの情報を表示するには、[IM 構成管理] 画面から [ホスト一覧] ページを呼び出します。

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. ツリー表示領域から仮想ホストを選択する。

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。

ホストの情報を収集するには、仮想ホスト上で、JP1/Base が動作している必要があります。

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。

4. [基本情報] ボタン、[製品情報] ボタン、[サービス情報] ボタンのどれかを選択する。

選択したボタンによって、ノード情報表示領域にホスト情報が表示されます。[下位ホスト情報] ボタンは選択できません。

9.3.3 セントラルスコープの監視ツリーへ反映する

システムの階層構成に登録した仮想ホストをセントラルスコープで監視するには、IM 構成管理の管理情報をエクスポートし、セントラルスコープの監視ツリー情報へインポートする必要があります。ここでは、その手順について説明します。

1. jcfexport コマンドを実行する。

IM 構成管理の構成情報をエクスポートします。

2. jcldbexport コマンドを実行する。

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. jcfexport コマンドとjcldbexport コマンドの出力ファイルを引数にして、jcfmkcsdata コマンドを実行する。

IM 構成管理の構成情報と監視ツリー情報をマージします。

4. jcldbimport コマンドを実行する。

マージされた IM 構成管理の管理情報と監視ツリー情報をインポートします。

セントラルスコープ・ビューアーで、マージした仮想ホストが表示されていることを確認してください。

9.4 業務グループを管理する

監視対象を業務グループ単位で設定している場合、業務グループの構成を見直すタイミングで、業務グループを作成、編集、および削除する必要があります。

業務グループを新しく作成する

手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.4.1(1) (a) 業務グループの作成」を参照してください。

業務グループの登録内容を編集する

手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.4.1(1) (b) 業務グループのプロパティの編集」を参照してください。

不要となった業務グループを削除する

手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.4.1(1) (c) 業務グループの削除」を参照してください。

業務グループを作成、編集、および削除したあとは、監視ツリーに業務グループと監視グループの階層構成の反映が必要です。手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.4.4(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」を参照してください。

9.5 プロファイルを管理する

システムのアップデートやメンテナンスの際にプロファイルの内容を変更したり、プロファイルの内容をほかのホストのプロファイルに適用したりする場合に、IM 構成管理 DB に登録されているプロファイルを見直す必要があります。

IM 構成管理・ビューアーから次の作業を実施して、プロファイルを管理してください。

なお、プロファイルには、有効設定情報と設定ファイルの内容の 2 種類があります。

プロファイルを収集する場合

次のプロファイルを収集します。

- エージェントホストの JP1/Base の有効設定情報
- エージェントホストの JP1/Base の設定ファイル（イベントの転送設定ファイル、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実行定義ファイル）
- リモートの監視対象ホストの有効設定情報

プロファイルの収集方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.5.1(2) プロファイルを収集する」を参照してください。

プロファイルリストを収集する場合

エージェントホストの JP1/Base 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。

プロファイルリストの収集方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.5.1(1) プロファイルリストを収集する」を参照してください。

プロファイルを表示する場合

エージェントホストの JP1/Base、およびリモートの監視対象ホストのプロファイルを [プロファイル表示/編集] 画面に表示します。

表示方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.5.1(3) プロファイルを表示する」を参照してください。

設定ファイルを編集する場合

収集した設定ファイルを、[プロファイル表示/編集] 画面で編集します。なお、設定ファイルで編集できるプロファイル種別は、次のとおりです。

- 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
- 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

編集方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.5.1(5) 設定ファイルを編集する」を参照してください。

設定ファイルの編集内容を反映する場合

編集した設定ファイルの内容を反映します。

反映方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

9.6 サービスの稼働状況を管理する

IM 構成管理・ビューアーを操作して、各ホストでのサービスの稼働状況を管理する方法について説明します。

9.6.1 サービスの稼働情報を収集する

エージェント構成の場合に、システムの階層構成から、ホストごとに稼働しているサービスの稼働情報を収集できます。

なお、リモート監視構成の場合は、サービスの稼働情報は収集できません。

サービスの稼働情報は、[IM 構成管理] 画面の [ホスト一覧] ページまたは [IM 構成] ページから収集しますが、選択するページによって手順が異なります。

(1) [ホスト一覧] ページからサービスの稼働情報を収集する

[IM 構成管理] 画面の [ホスト一覧] ページからサービスの稼働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] タブをクリックする。

[ホスト一覧] ページが表示されます。

2. ツリー表示領域からホストを選択する。

[ホスト一覧] を選択して、サービスの稼働情報は収集できません。また、IM 構成管理が動作しているマネージャーにより、稼働情報を収集できるホストの範囲が異なります。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「8.7.2 サービスの稼働情報の収集」を参照してください。

3. [サービス情報] ボタンをクリックする。

収集されたサービスの稼働情報が、ノード情報表示領域に表示されます。

4. メニューバーから [表示] - [最新情報に更新] を選択する。

ホストから最新のサービスの稼働情報が収集されて、ノード情報表示領域の表示が更新されます。

(2) [IM 構成] ページからサービスの稼働情報を収集する

[IM 構成管理] 画面の [IM 構成] ページからサービスの稼働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 [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. ツリー表示領域からホストを選択する。

IM 構成管理が動作しているマネージャーにより、稼働情報を収集できるホストの範囲が異なります。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「8.7.2 サービスの稼働情報の収集」を参照してください。

3. 次に示すどちらかの方法でホスト情報を収集する。

- 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。

4. [サービス情報] ボタンをクリックする。

収集されたサービスの稼働情報が、ノード情報表示領域に表示されます。

5. メニューバーから [表示] - [最新情報に更新] を選択する。

ホストから最新のサービスの稼働情報が収集されて、ノード情報表示領域の表示が更新されます。

9.6.2 サービスの稼働情報を表示する

システムの階層構成 (IM 構成) から、ホストごとに稼働しているサービスの稼働情報を表示する手順については、「9.6.1 サービスの稼働情報を収集する」を参照してください。

[IM 構成管理] 画面のサービス情報には次の稼働情報が表示されます。

表 9-1 サービスごとに表示される稼働情報

製品名	サービス名	稼働状態
JP1/Base	JP1/Base	サービスの稼働状態が次のステータスで表示される <ul style="list-style-type: none"> • 稼働中 • 停止中 • 一部稼働中 • 収集失敗
	イベントサービス	
	ログファイルトラップ	
JP1/IM - Manager	JP1/IM-Manager	

[IM 構成管理] 画面の詳細情報には、次のとおり、各サービスの状態を収集するコマンドの実行結果が表示されます。

表 9-2 各サービスの状態を収集するコマンド

サービス名	収集コマンド
JP1/Base	jbs_spm�_status
イベントサービス	jevstat
ログファイルトラップ	jevlogstat ALL
JP1/IM-Manager	jco_spm�_status
ログファイルトラップ (リモート)	jcfallogstat*

サービス名	収集コマンド
イベントログトラップ (リモート)	jcfaletstat※

注※ 収集コマンド相当の情報が出力されます。

9.7 IM 構成管理の管理情報をエクスポート・インポートする

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・インポートする方法について説明します。

9.7.1 IM 構成管理の管理情報をエクスポートする

IM 構成管理の管理情報を出力（エクスポート）してから入力（インポート）することで、あるホストから別のホストへコピーできます。また、エクスポートされたシステムの構成情報を編集することで、簡単に変更できます。ここでは、`jcfexport` コマンドによってエクスポートされる管理情報について説明します。`jcfexport` 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「`jcfexport`」(1. コマンド) を参照してください。

(1) ホスト情報

IM 構成管理の管理対象ホストに関する情報がホスト入力情報ファイルとホスト収集情報ファイルにエクスポートされます。

ホスト入力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「ホスト入力情報ファイル (`host_input_data.csv`)」(2. 定義ファイル) を参照してください。

ホスト収集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「ホスト収集情報ファイル (`host_collect_data.csv`)」(2. 定義ファイル) を参照してください。

(2) システムの階層構成情報

システムの階層構成の情報がファイルにエクスポートされます。エクスポートされたファイルを編集してインポートできます。

出力される情報は、次に示すシステムの監視方法によって異なります。

- エージェント監視
- リモート監視

(a) エージェント監視の構成情報

エクスポートされるファイル名は、`system_tree_information.txt` です。

このファイルに出力されるエージェント監視の構成情報を次の表に示します。

表 9-3 エクスポートされるエージェント監視の構成情報

出力項目	出力値
[管理ホスト]	<ul style="list-style-type: none"> • JP1/Base のホストを管理する統合マネージャー、拠点マネージャー、または中継マネージャーのどれかを表す。 • 最初に定義された管理ホストが統合マネージャーで、以降に定義された管理ホストが拠点マネージャーまたは中継マネージャーである。 • 次に [] で括られたホストが出てくるまでを管理対象ホストとする。 • システムの階層構成を分割定義した場合、ホスト名の前にアスタリスクを付与する。
管理対象ホスト	<ul style="list-style-type: none"> • 管理ホストに管理される JP1/Base のホスト。 • 拠点マネージャーまたは中継マネージャーは、統合マネージャーの管理対象ホストとして定義されている。 • システムの階層構成を分割定義した場合、ホスト名の前にアスタリスクを付与する。

(b) リモート監視の構成情報

リモート監視の構成情報がファイルにエクスポートされます。エクスポートされるファイル名は、`system_remote_tree_information.txt` です。

このファイルに出力されるリモート監視の構成情報を次の表に示します。

表 9-4 エクスポートされるリモート監視の構成情報

出力項目	出力値
[管理ホスト]	<ul style="list-style-type: none"> • リモート監視構成を管理する統合マネージャーまたは拠点マネージャーのどちらかを表す。 • 拠点マネージャー場合は、管理ホスト名の前にアスタリスクを付与する。
管理対象ホスト	IM 構成管理のリモートで管理するホスト。

(3) プロファイル情報

ホストで動作するプロファイル情報がエクスポートされます。エクスポートの対象となるファイルは、次に示すシステムの監視方法によって異なります。

- エージェント監視
- リモート監視

(a) エージェント監視のプロファイル情報

ホストで動作する JP1/Base プロファイル情報がファイルにエクスポートされます。ファイルは「`definition_files`」ディレクトリ以下の 1 階層目のディレクトリ名の「ホスト名」、2 階層目のディレクトリ名の「JP1Base」以下にエクスポートされます。また、ログファイルトラップの動作定義ファイルは 3 階層目のディレクトリ名の「`cf_log_file_trap`」以下にエクスポートされます。エクスポートの対象となるプロファイル情報を次に示します。

表 9-5 エクスポートされるエージェント監視のプロファイル情報とエクスポートファイル名

プロファイル情報	エクスポートファイル名
イベントの転送設定ファイル	forward
ログファイルトラップ動作定義ファイル	ファイル名は任意
ログファイルトラップ起動定義ファイル	jevlog_start.conf
イベントログトラップ動作定義ファイル	ntevent.conf
ローカルアクション実行定義ファイル	jbslcact.conf

注 プロファイル設定ファイルを収集していないホストの場合、エクスポートするデータはありません（ディレクトリも作成されません）。

(b) リモート監視のプロファイル情報

JP1/IM - Manager プロファイル情報がファイルにエクスポートされます。リモート監視のプロファイル情報は編集できません。

ファイルは「definition_files」ディレクトリ以下の1階層目のディレクトリ名の「ホスト名」、2階層目のディレクトリ名の「al」以下にエクスポートされます。また、ログファイルトラップの動作定義ファイルは3階層目のディレクトリ名の「cf_log_file_trap」以下に、イベントログトラップの動作定義ファイルは3階層目のディレクトリ名の「cf_event_log_trap」以下にエクスポートされます。エクスポートの対象となるプロファイル情報を次に示します。

表 9-6 エクスポートされるリモート監視のプロファイル情報とエクスポートファイル名

プロファイル情報	エクスポートファイル名
リモート監視ログファイルトラップ動作定義ファイル	ファイル名は任意
リモート監視起動定義ファイル	jevlog_start.conf
リモート監視イベントログトラップ動作定義ファイル	ntevent.conf

(4) リモート認証情報

リモート監視をしている場合に、リモート認証情報がエクスポートされます。エクスポートされるファイル名は、wmi.ini、ssh.iniです。

(5) 業務グループ情報

業務グループを使用している場合に、業務グループの情報がファイルにエクスポートされます。エクスポートされるファイル名は、monitoring_system_data.csvです。monitoring_system_data.csvに出力される業務グループ情報を次の表に示します。

表 9-7 エクスポートされる業務グループ情報

行	出力項目	出力値
1 行目 (ヘッダー情報)	製品名	JP1/IM-CF
	ファイルフォーマットバージョン	ファイルフォーマットのバージョン 例えば、JP1/IM - Manager のバージョンが 09-50 の場合は、「095000」と出力されます。
	文字コード	文字コード マネージャーの環境変数 LANG の設定に依存します。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「ホスト入力情報ファイル (host_input_data.csv) (2. 定義ファイル) の「表 2-85 ファイルの文字コード」を参照してください。
2 行目 (ヘッダー情報)	業務グループ名	Monitoring_system_name
	割り当て JP1 資源グループ名	JP1_resource_group_name
	コメント	Comment
	ホスト名	Host_name_list
3 行目以降	業務グループ名	業務グループの名称
	割り当て JP1 資源グループ名	業務グループに割り当てた JP1 資源グループの名称
	コメント	コメント
	ホスト名	業務グループに登録されたホストのホスト名 (複数ある場合はコンマ (,) で区切り, 全体をダブルクォーテーション (") で囲む)

注 業務グループ情報は、業務グループ名で昇順にソートして出力されます。

業務グループ情報の出力例を次に示します。

```
JP1/IM-CF;095000;UTF-8,,,
```

```
Monitoring_system_name,JP1_resource_group_name,Comment,Host_name_list
```

```
System1,,This is the empty system,
```

```
System2,Resource_A,This is System2,"host21,host22,host23,host24"
```

```
System3,Resource_A,This is System3,"host31,host32"
```

(6) 監視グループ情報

業務グループを使用している場合に、IM 構成管理の監視グループ情報がファイルにエクスポートされます。エクスポートされるファイル名は、monitoring_group_data.csv です。monitoring_group_data.csv に出力される監視グループ情報を次の表に示します。

表 9-8 エクスポートされる監視グループ情報

行	出力項目	出力値
1 行目 (ヘッダー情報)	製品名	JP1/IM-CF
	ファイルフォーマットバージョン	ファイルフォーマットのバージョン 例えば, JP1/IM - Manager のバージョンが 10-50 の場合は, 「101000」と出力されます。
	文字コード	文字コード マネージャーの環境変数 LANG の設定に依存します。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「ホスト入力情報ファイル (host_input_data.csv)」(2. 定義ファイル) の「表 2-85 ファイルの文字コード」を参照してください。
2 行目 (ヘッダー情報)	監視グループパス	Monitoring_group_path
	コメント	Comment
	ホスト名	Host_name_list
3 行目以降	監視グループパス	監視グループのパス
	コメント	コメント
	ホスト名	監視グループに登録されたホストのホスト名 (複数ある場合はコンマ (,) で区切り, 全体をダブルクォーテーション (") で囲む)

注 監視グループ情報は, 監視グループパスで昇順にソートして出力されます。

監視グループ情報の出力例を次に示します。

```
JP1/IM-CF;101000;UTF-8,,
```

```
Monitoring_group_path,Comment,Host_name_list
```

```
/System1/Group1,This is the empty group,
```

```
/System1/Group2,This is Group2,host2
```

```
/System2/Group1,This is Group1,"host11,host12,host13,host14"
```

9.7.2 IM 構成管理の管理情報をインポートする

あるホストから出力 (エクスポート) された IM 構成管理の管理情報を, 必要があれば編集し, 別のホストへ入力 (インポート) します。インポートは, jcfimport コマンドで実行しますが, ホスト情報の収集情報はインポートできません。

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。

ここでは、`jcfimport` コマンドによってインポートされるシステム構成情報について説明します。インポートした IM 構成管理の管理情報をシステムに反映するには、「9.7.3 インポートした IM 構成管理の管理情報をシステムに反映する」を参照してください。

`jcfimport` 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「`jcfimport`」(1. コマンド)を参照してください。

(1) ホスト情報

手動入力情報の場合、エクスポートファイル (`host_input_data.csv`) の内容がインポートされます。

手動入力情報のエクスポートファイル (`host_input_data.csv`) からインポートされる項目と、各項目の入力範囲を次に示します。

表 9-9 インポートされるホスト情報 (手動入力情報)

項目	入力範囲	必須/任意	デフォルト
ホスト名	最大 255 バイトの文字列を入力できます。使用できる文字は、制御コードを除く半角英数字、半角ハイフン (-), ピリオド (.) です。	必須 ^{*1}	—
IP アドレス	IP アドレスを入力できます。使用できる文字は、制御コードを除く半角英数字、ピリオド (.), コロン (:) です。	任意	空欄
ホスト名一覧	ホスト名を入力できます。使用できる文字は、制御コードを除く半角英数字、半角ハイフン (-), ピリオド (.) です。	任意	空欄
コメント	最大 80 バイトの文字列を入力できます。	任意	空欄
ホスト種別	次のどれかを入力できます。 <ul style="list-style-type: none"> • physical • logical • virtual • unknown 	任意	physical
実行系ホスト	最大 255 バイトの文字列を入力できます。使用できる文字は、制御コードを除く半角英数字、半角ハイフン (-), ピリオド (.) です。	任意	空欄
待機系ホスト	ホスト名を入力できます。ホスト名は 1 個当たり最大 255 バイトの文字列を入力できます。使用できる文字は、制御コードを除く半角英数字、半角ハイフン (-), ピリオド (.) です。	任意	空欄
VMM ホスト	最大 255 バイトの文字列を入力できます。使用できる文字は、制御コードを除く半角英数字、半角ハイフン (-), ピリオド (.) です。	任意	空欄
仮想化管理種別	次のどれかを入力できます。大文字、小文字の区別はありません。	任意	空欄

項目	入力範囲	必須/任意	デフォルト
	仮想化システム管理ホストの場合 <ul style="list-style-type: none"> ・ vCenter ・ JP1/SC/CM ・ SCVMM ・ HCSM VMM ホストの場合 <ul style="list-style-type: none"> ・ ESX^{※2} ・ Hyper-V ・ KVM ・ Virtage^{※3} 		
ユーザー名	最大 255 バイトの文字列を入力できます。使用できる文字は、制御コードを除く半角英数字です。	任意	空欄
パスワード ^{※4}	最大 255 バイトの文字列を入力できます。使用できる文字は、制御コードを除く半角英数字です。	任意	空欄
ドメイン名 ^{※5}	最大 255 バイトの文字列を入力できます。使用できる文字は、制御コードを除く半角英数字です。	任意	空欄
通信種別 ^{※6}	http, https, ssh のどれかを入力できます。大文字、小文字の区別はありません。なお、仮想化管理種別の値によって、入力できる通信種別は異なります。 仮想化管理種別がvCenter の場合 <ul style="list-style-type: none"> https, http を入力できる。 仮想化管理種別がHCSM の場合 <ul style="list-style-type: none"> http を入力できる。 仮想化管理種別がKVM の場合 <ul style="list-style-type: none"> ssh を入力できる。 	任意	仮想化管理種別がvCenter の場合 <ul style="list-style-type: none"> https 仮想化管理種別がHCSM の場合 <ul style="list-style-type: none"> http 仮想化管理種別がKVM の場合 <ul style="list-style-type: none"> ssh
ポート番号 ^{※7}	半角数字で1~65535 までの値を入力できます。	任意	仮想化管理種別がHCSM の場合 <ul style="list-style-type: none"> 23015 仮想化管理種別がKVM の場合 <ul style="list-style-type: none"> 22
秘密鍵ファイル名 ^{※8}	最大 256 バイトの文字列を入力できます。大文字、小文字を区別します。使用できる文字は制御コードを除く半角英数字です。	任意	空欄
仮想化管理元ホスト名	最大 255 バイトの文字列を入力できます。使用できる文字は、制御コードを除く半角英数字、半角ハイフン (-), ピリオド (.) です。	任意	空欄

項目	入力範囲	必須/任意	デフォルト
リモート通信種別	リモート監視の場合に使用できる通信種別です。次のどれかを入力できます。 <ul style="list-style-type: none"> • disable • ssh • wmi 	任意	disable
認証情報の区分※9	リモート監視の場合に使用できる認証情報の区分です。次のどれかを入力できます。 <ul style="list-style-type: none"> • common • host • 空白 	任意	空白

(凡例)

－：デフォルト値がない

注 文字列のバイト長は UTF-8 換算です。

注※1 必須の項目が設定されていない場合は、エラーとなります。任意の項目が設定されていない場合は、デフォルトの値がインポートされます。

注※2 ESX は、VMware ESX を指します。

注※3 Virtage は、日立サーバ論理分割機構を指します。

注※4 仮想化管理種別がvCenter、SCVMM またはHCSM の場合に入力が必要です。

注※5 仮想化管理種別がSCVMM の場合に入力が必要です。

注※6 仮想化管理種別がvCenter、HCSM またはKVM の場合に入力が必要です。

注※7 仮想化管理種別がHCSM またはKVM の場合に入力が必要です。

注※8 仮想化管理種別がKVM の場合に入力が必要です。

注※9 認証情報の区分にhost が設定されているホストのホスト名を変更した場合、リモート監視に使用する認証情報が引き継がれません。インポート後に IM 構成管理画面でリモート通信設定を再設定してください。

ホスト情報に、文字コード間に互換性のない文字、および機種依存文字を使用していると、インポートしたときに文字化けが発生するおそれがあります。

手動入力情報のエクスポートファイル (host_input_data.csv) の内容が次のどれかの場合は、エラーとなり、インポートされません。

- ホスト名が重複している。
- ホスト名が 255 バイトより大きい。
- ホスト数がサポート数分 (IM データベースのサイズが、S または M の場合は 1,024 台、L の場合は 10,000 台) を超えている。
- 入力範囲外の値が設定されている。
- 入力データの列が少ない (コンマの数が少ない)。
- 実行系ホスト、待機系ホスト、および VMM ホストに記載されているホスト名が、ホスト情報ファイルに存在しない。
- 実行系ホストおよび待機系ホストのホストの種別に、physical、virtual 以外が設定されている。

- VMM ホストのホストの種別にphysical 以外が設定されている。
- ホスト種別にphysical, logical, virtual, unknown 以外が設定されている。
- 仮想化管理種別にESX, Hyper-V, KVM, Virtage, vCenter, JP1/SC/CM, SCVMM, HCSM 以外が設定されている。
- ホスト種別がlogical, unknown のホストに仮想化管理種別が設定されている。
- 仮想化管理元ホストに記載されているホストがホスト情報ファイルに存在しない。
- 仮想化管理元ホストに記載されているホストの種別がphysical, virtual 以外が設定されている。
- ドメイン名が設定されているホストの仮想化管理種別にSCVMM 以外が設定されている。
- 通信種別が指定されているホストの仮想化管理種別にvCenter, HCSM, KVM 以外が設定されている。
- 仮想化管理種別がvCenter であるホストの通信種別にhttps, http 以外が設定されている。
- 仮想化管理種別がHCSM であるホストの通信種別にhttp 以外が設定されている。
- 仮想化管理種別がKVM であるホストの通信種別にssh 以外が設定されている。
- 仮想化システム構成に関する情報が次の表の内容に該当しない。

ホスト種別	仮想化管理種別	入力する仮想化管理種別に関する情報	必須または任意	備考
物理ホスト	—	×	—	—
	vCenter	仮想化管理元ホスト名	任意	仮想化管理元ホスト名は、SCVMM を指定する
		ユーザー名	任意	
		パスワード	任意	
		通信種別	任意	
	JP1/SC/CM	×	—	—
	SCVMM	ユーザー名	任意	—
		パスワード	任意	
		ドメイン名	任意	
	HCSM	ユーザー名	任意	—
		パスワード	任意	
		ポート番号	任意	
		通信種別	任意	
	ESX	仮想化管理元ホスト名	任意	仮想化管理元ホスト名は、vCenter を指定する。
Hyper-V	仮想化管理元ホスト名	任意	仮想化管理元ホスト名は、SCVMM を指定する。	

ホスト種別	仮想化管理種別	入力する仮想化管理種別に関する情報	必須または任意	備考
	KVM	ユーザー名	任意	—
		ポート番号	任意	
		秘密鍵ファイル名	必須	
		通信種別	任意	
	Virtage	仮想化管理元ホスト名	任意	仮想化管理元ホスト名は、JP1/SC/CM またはHCSM を指定する。
仮想ホスト	—	VMM ホスト名	必須	VMM ホスト名は、vCenter, JP1/SC/CM, SCVMM, HCSM 以外を指定する。
	vCenter	VMM ホスト名	必須	VMM ホスト名は、vCenter, JP1/SC/CM, SCVMM, HCSM 以外を指定する。 仮想化管理元ホスト名は、SCVMM を指定する。
		仮想化管理元ホスト名	任意	
		ユーザー名	任意	
		パスワード	任意	
		通信種別	任意	
	JP1/SC/CM	VMM ホスト名	必須	VMM ホスト名は、vCenter, JP1/SC/CM, SCVMM, HCSM 以外を指定する。
	SCVMM	VMM ホスト名	必須	VMM ホスト名は、vCenter, JP1/SC/CM, SCVMM, HCSM 以外を指定する。
		ユーザー名	任意	
		パスワード	任意	
		ドメイン名	任意	
	HCSM	VMM ホスト名	必須	VMM ホスト名は、vCenter, JP1/SC/CM, SCVMM, HCSM 以外を指定する。
		ユーザー名	任意	
		パスワード	任意	
		ポート番号	任意	
		通信種別	任意	
	KVM	VMM ホスト名	必須	VMM ホスト名は、vCenter, JP1/SC/CM,
		ユーザー名	任意	

ホスト種別	仮想化管理種別	入力する仮想化管理種別に関する情報	必須または任意	備考
		ポート番号	任意	SCVMM, HCSM 以外を指定する。
		秘密鍵ファイル名	任意	
		通信種別	任意	
論理ホスト	—	×	—	—
不明	—	×	—	—

(凡例)

- ：該当なし
- ×：入力できない（入力した場合はエラーとなる）

- リモート通信種別がdisable, ssh, wmi 以外が設定されている。
- 認証情報の区分がcommon, host, 空白以外が設定されている。
- リモート通信種別にssh またはwmi が設定されているとき、認証情報の区分に空白が設定されている。

また、インポート先ホストとホスト名が同じホストは、手動入力情報のエクスポートファイル (host_input_data.csv) がインポートされたあと、IM 構成管理の管理対象ホストとして登録されません。

(2) システムの階層構成情報

システムの階層構成情報のエクスポートファイルの内容がインポートされます。エクスポートファイルは、次に示すシステムの監視方法によって異なります。

- エージェント監視
- リモート監視

(a) エージェント監視の構成情報

エージェント監視の構成情報のエクスポートファイル名は、system_tree_information.txt です。

エージェント監視の構成情報のエクスポートファイルの内容が次のどれかの場合は、エラーとなり、インポートされません。

- 同一ホストが複数行に存在する（管理対象ホストが複数の上位ホストを持つ）
- ホストの構成がループしている
- 管理ホストに設定される管理ホスト名が[]で囲まれていない（[] で閉じられていない）
- 管理ホストにホスト名が設定されていない
- ホスト数が 10,000 台より多く定義されている
- 管理対象ホストに自ホストが定義されている

ホスト情報（手動入力情報）のエクスポートファイル（host_input_data.csv）、またはエージェント監視の構成情報のエクスポートファイルを編集した結果、エージェント監視の構成情報のエクスポートファイルに設定されたホスト名が、ホスト情報（手動入力情報）のエクスポートファイルに設定されていない場合があります。この場合、エージェント監視の構成情報のエクスポートファイルがインポートされたあと、インポート警告メッセージが表示されて、未定義のホストが IM 構成管理の管理対象ホストとして自動的に登録されます。

エージェント監視の構成情報をインポートする場合、指定したディレクトリにエージェント監視の構成情報のエクスポートファイルが存在しないときは、エラーメッセージが表示されて、インポートが中止されます。

(b) リモート監視の構成情報

リモート監視の構成情報のエクスポートファイル名は、system_remote_tree_information.txt です。

リモート監視の構成情報のエクスポートファイルの内容が次のどれかの場合は、エラーとなり、インポートされません。

- 同一ホストが複数行に存在する（管理対象ホストが複数の上位ホストを持つ）
- ホストの構成がループしている
- 管理ホストに設定される管理ホスト名が [] で囲まれていない（[] で閉じられていない）
- 管理ホストにホスト名が設定されていない
- ホスト数が 1,024 台より多く定義されている
- 管理対象ホストに自ホストが定義されている

ホスト情報（手動入力情報）のエクスポートファイル（host_input_data.csv）、またはリモート監視の構成情報のエクスポートファイルを編集した結果、リモート監視の構成情報のエクスポートファイルに設定されたホスト名が、ホスト情報（手動入力情報）のエクスポートファイルに設定されていない場合があります。この場合、リモート監視の構成情報のエクスポートファイルがインポートされたあと、インポート警告メッセージが表示されて、未定義のホストが IM 構成管理の管理対象ホストとして自動的に登録されます。

リモート監視の構成情報をインポートする場合、指定したディレクトリにリモート監視の構成情報のエクスポートファイルが存在しないときは、エラーメッセージが表示されて、インポートが中止されます。

(3) プロファイル情報

プロファイル情報のエクスポートファイルの内容がインポートされます。インポートの対象となるファイルは、次に示すシステムの監視方法によって異なります。

- エージェント監視
- リモート監視

(a) エージェント監視のプロファイル情報

インポートの対象となるエージェント監視のプロファイル情報のエクスポートファイルを次に示します。

表 9-10 インポートされるエージェント監視のプロファイル情報のエクスポートファイル

プロファイル情報	エクスポートファイル名
イベントの転送設定ファイル	forward
ログファイルトラップ動作定義ファイル	ファイル名は任意
ログファイルトラップ起動定義ファイル	jevlog_start.conf
イベントログトラップ動作定義ファイル	ntevent.conf
ローカルアクション実行定義ファイル	jbslcact.conf

エージェント監視のプロファイル情報のインポートでは、「`definition_files`」ディレクトリ以下のディレクトリ名を使用してインポート先が決まります。「`definition_files`」ディレクトリ以下の1階層目のディレクトリ名は「ホスト名」、2階層目のディレクトリ名は「製品名」として読み込まれ、各ディレクトリに格納されたファイルが設定情報として該当するホストに登録されます。このため、ホスト情報（手動入力情報）のエクスポートファイル（`host_input_data.csv`）でホスト名を変更した場合は、同様にディレクトリ名も変更する必要があります。変更しないと、プロファイル情報はインポートされません。

プロファイル情報のファイルを、エクスポートデータ情報のエクスポートファイル（`data_information.txt`）の`encode`に記載されている文字コードとして読み込みます。この文字コードは、エクスポートを実行したサーバのOSの環境変数「`LANG`」が設定されます。プロファイル情報をインポートする場合には、エクスポートファイル（`data_information.txt`）に記述されている文字コードとプロファイル情報のファイルの文字コードが一致しているかどうかを確認してください。

ホスト情報に、文字コード間に互換性のない文字、および機種依存文字を使用していると、インポートしたときに文字化けが発生するおそれがあります。

ホスト数が10,000台より多く定義されている場合は、エラーとされて、インポートされません。

プロファイル（設定ファイル）のエクスポートファイルの内容に未対応製品や未対応のプロファイルなどがある場合には、その部分を無視して処理を続けます。

(b) リモート監視のプロファイル情報

リモート監視をしている場合に、リモート監視のプロファイル情報のエクスポートファイルの内容がインポートされます。リモート監視のプロファイル情報は編集できません。

インポートの対象となるリモート監視のプロファイル情報のエクスポートファイルを次に示します。

表 9-11 インポートされるリモート監視のプロファイル情報とエクスポートファイル名

プロファイル情報	エクスポートファイル名
リモート監視ログファイルトラップ動作定義ファイル	ファイル名は任意

プロファイル情報	エクスポートファイル名
リモート監視起動定義ファイル	jevlog_start.conf
リモート監視イベントログトラップ動作定義ファイル	nthevent.conf

リモート監視のプロファイル情報のインポートでは、「definition_files」ディレクトリ以下のディレクトリ名を使用してインポート先が決まります。

「definition_files」ディレクトリ以下の1階層目のディレクトリ名は「ホスト名」、2階層目のディレクトリ名は「製品名」として読み込まれ、各ディレクトリに格納されたファイルが設定情報として該当するホストに登録されます。このため、ホスト情報（手動入力情報）のエクスポートファイル（host_input_data.csv）でホスト名を変更した場合は、同様にディレクトリ名も変更する必要があります。変更しないと、プロファイル情報はインポートされません。

プロファイル情報のファイルを、エクスポートデータ情報のエクスポートファイル（data_information.txt）のencodeに記載されている文字コードとして読み込みます。この文字コードは、エクスポートを実行したサーバのOSの環境変数「LANG」が設定されます。プロファイル情報をインポートする場合には、エクスポートファイル（data_information.txt）に記述されている文字コードとプロファイル情報のファイルの文字コードが一致しているかどうかを確認してください。ホスト情報に、文字コード間に互換性のない文字、および機種依存文字を使用していると、インポートしたときに文字化けが発生するおそれがあります。

(4) リモート認証情報

リモート監視をしている場合に、リモート認証情報のエクスポートファイルの内容がインポートされます。インポートされるファイル名は、wmi.ini, ssh.ini です。

リモート監視をする場合は、インポート後にIM構成管理・ビューアーから [システム共通設定] 画面を開き、設定を確認後に [OK] ボタンをクリックしてください。

(5) 業務グループ情報

業務グループを使用している場合に、IM構成管理の監視グループ情報のエクスポートファイルの内容がインポートされます。業務グループ情報のエクスポートファイル（monitoring_system_data.csv）の内容が次のどれかの場合は、エラーとなり、インポートされません。

- 同じ階層に同じ名称の業務グループが存在する
- 入力範囲外
- 入力データの列が少ない（コンマの数が合わない）

業務グループ情報のエクスポートファイル（monitoring_system_data.csv）は、1行目（ヘッダー情報）に記載している文字コードで保存してください。また、UTF-8で保存する場合は、BOM (byte order mark) が付与されないように保存してください。

インポートの対象となる項目および各項目の入力範囲を次に示します。

表 9-12 インポートされる項目 (業務グループ情報)

項目	入力範囲	必須/任意	デフォルト
業務グループ名	UTF-8 換算で最大 255 バイトの文字を入力できます。使用できる文字は制御文字、スラッシュ (/), 半角コンマ (,) 以外の文字です。先頭および最後の文字に半角スペースは使用できません。大文字・小文字を区別します。ダブルクォーテーション (") を指定する場合は、ダブルクォーテーション (") を重ねて記述して、全体をダブルクォーテーション (") で囲みます。 なお、業務グループ名に環境依存文字などを使用すると定義に文字化けが発生することがあるため、使用しないでください。	必須	—
割り当て JP1 資源グループ名	最大 64 バイトの文字列を入力できます。使用できる文字は、"/ [] ; : , = + ? < > , タブ, スペースを除く ASCII コードです。	任意	空欄
コメント	UTF-8 換算で最大 80 バイトの文字列を入力できます。使用できる文字は、制御文字以外です。ダブルクォーテーション (") を指定する場合は、ダブルクォーテーション (") を重ねて記述して、全体をダブルクォーテーション (") で囲みます。コンマを指定する場合は、全体をダブルクォーテーション (") で囲みます。	任意	空欄
ホスト名	複数のホストをコンマで区切って最大 2,500 個まで指定できます。ホストを複数指定する場合は、全体をダブルクォーテーション (") で囲みます。1 個のホスト名の入力範囲は「表 9-9 インポートされるホスト情報 (手動入力情報)」を参照してください。	任意	空欄

(凡例)

— : デフォルト値がない

(6) 監視グループ情報

業務グループを使用している場合に、業務グループ情報のエクスポートファイルの内容がインポートされます。監視グループ情報のエクスポートファイル (monitoring_group_data.csv) の内容が次のどれかの場合は、エラーとなり、インポートされません。

- 同じ階層に同じ名称の監視グループまたはホストが存在する
- 入力範囲外
- 入力データの列が少ない (コンマの数が合わない)
- 上位の監視グループが、下位の監視グループよりも行番号の若い行に定義されていない

監視グループ情報のエクスポートファイル (monitoring_group_data.csv) は、1 行目 (ヘッダー情報) に記載している文字コードで保存してください。また、UTF-8 で保存する場合は、BOM (byte order mark) が付与されないように保存してください。

インポートの対象となる項目および各項目の入力範囲を次に示します。

表 9-13 インポートされる項目 (監視グループ情報)

項目	入力範囲	必須/任意	デフォルト
監視グループパス	UTF-8 換算で最大 2,048 バイトの文字列を入力できます。使用できる文字は、制御文字以外です。大文字・小文字を区別します。ダブルクォーテーション (") を指定する場合は、ダブルクォーテーション (") を重ねて記述して、全体をダブルクォーテーション (") で囲みます。 なお、監視グループ名に環境依存文字などを使用すると定義に文字化けが発生することがあるため、使用しないでください。	必須	—
コメント	UTF-8 換算で最大 80 バイトの文字列を入力できます。使用できる文字は、制御文字以外です。ダブルクォーテーション (") を指定する場合は、ダブルクォーテーション (") を重ねて記述して、全体をダブルクォーテーション (") で囲みます。コンマを指定する場合は、全体をダブルクォーテーション (") で囲みます。	任意	空欄
ホスト名	複数のホストをコンマで区切って最大 2,500 個まで指定できます。ホストを複数指定する場合は全体をダブルクォーテーション (") で囲みます。1 個のホスト名の入力範囲は「表 9-9 インポートされるホスト情報 (手動入力情報)」を参照してください。	任意	空欄

(凡例)

— : デフォルト値がない

9.7.3 インポートした IM 構成管理の管理情報をシステムに反映する

jcimport コマンドを実行して IM 構成管理の管理情報をインポートしたあとに、次の操作を実行してシステムに反映します。

(1) ホスト情報の収集

ホスト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. 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、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」を選択します。選択したホストの情報収集が実行されます。

(2) システムの階層構成情報の反映

システムの階層構成情報を反映する手順を次に示します。

(a) エージェント構成の場合

システムの階層構成情報を反映していない場合、[IM 構成管理] 画面の [IM 構成] タブでツリーがグレー表示されます。

次の手順でシステムの階層構成情報を反映してください。

1. [IM 構成管理] 画面のメニューバーから [編集] - [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。
2. [更新権取得] チェックボックスをチェックする。
JP1/IM システムの構成の編集ができるようになります。
3. ツリーの最上位ノード (統合マネージャー) を選択して、次のどちらかの方法で、統合マネージャーを変更する。
 - メニューバーから [操作] - [ホスト交換] 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 [ホスト交換] を選択する。なお、エクスポートしたホストとインポートしたホストが同じ場合には、この手順は不要です。
4. [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。
実システムにシステムの階層構成情報が反映されます。
5. [更新権取得] チェックボックスのチェックを外す。

なお、現在のシステムの階層構成を取得したい場合には、この操作は不要です。[IM 構成管理] 画面のメニューバーから [編集] - [IM 構成取得] を実行して、現在のシステムの階層構成を取得してください。

(b) リモート監視構成の場合

次の手順でシステムの階層構成情報を反映してください。

1. [IM 構成管理] 画面のメニューバーから [編集] - [リモート監視構成編集] を選択する。
[リモート監視構成編集] 画面が表示されます。
2. [更新権取得] チェックボックスをチェックする。
JP1/IM システムの構成の編集ができるようになります。
3. ツリーの最上位ノード (統合マネージャー) を選択して、次のどちらかの方法で、統合マネージャーを変更する。
 - メニューバーから [操作] - [ホスト交換] 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 [ホスト交換] を選択する。なお、エクスポートしたホストとインポートしたホストが同じ場合には、この手順は不要です。
4. [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。
実システムにシステムの階層構成情報が反映されます。
5. [更新権取得] チェックボックスのチェックを外す。

なお、現在のシステムの階層構成を取得したい場合には、この操作は不要です。[IM 構成管理] 画面のメニューバーから [編集] - [IM 構成取得] を実行して、現在のシステムの階層構成を取得してください。

(3) プロファイル情報の反映

IM 構成管理の管理情報をインポートしただけでは、システムに設定ファイルは反映されません。次の方法で設定ファイルの反映をしてください。

- 設定ファイルを一括で反映する方法
- ホストごとに設定ファイルを反映する方法

設定ファイルの反映方法は、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

なお、現在のシステムのプロファイル情報を取得したい場合には、プロファイル情報の反映は不要です。プロファイルを一括で収集してください。プロファイルの収集方法は、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「3.5.1(1) プロファイルリストを収集する」を参照してください。

9.8 IM 構成管理の注意事項

- IM 構成管理 DB を一度アンセットアップした後に、再セットアップを行った場合、IM 構成管理・ビューアーを接続すると [IM 構成] タブに表示されるシステムの階層構成にホストアイコンが表示されない場合があります。この場合、アンセットアップ前のシステムの階層構成が表示されているため、メニューバーから [操作] - [IM 構成取得] を選択してシステムの階層構成を更新してください。
- [ホスト一覧] ページの [製品情報] として表示される JP1/Integrated Management - Manager の情報のうち、次の項目のバージョンの内容が異なることがあります。
 - JP1/Integrated Management - Central Scope
 - JP1/Integrated Management - Central Console

JP1/Integrated Management - Manager のバージョンについては、JP1/Integrated Management - Manager の項目を参照してください。

- IM 構成管理で次の機能を使用する場合、JP1/Base 09-50-01 以降を使用してください。
 - 業務グループの参照/操作制限を使用する場合(jcoimdef で、-bizmonmode オプションを指定する場合)
 - IM 構成の反映において、システムの階層構成を削除しないで反映したい場合(IM 構成反映方式設定ファイル(jplcf_applyconfig.conf)に"APPLY_CONFIG_TYPE"=dword:00000001"を指定する場合)
- IM 構成管理の[仮想化管理設定] 画面の[仮想化管理種別]一覧に、[JP1/SC/CM]が表示されますが、使用しません。

10

JP1/IM - Agent の起動と終了

この章では、JP1/IM - Agent の起動および終了の手順について説明します。

10.1 JP1/IM - Agent のサービス

JP1/IM - Agent のサービスは、次に示すコマンドを使用して操作できます。

コマンド名	機能
jp1_service	Windows または Linux の systemd へのサービスの登録を、有効にするか無効にするかを設定します。
jp1_service_start	サービスを起動します。
jp1_service_stop	サービスを停止します。
jp1_service_autostart	OS 起動時に、サービスを自動的に起動させるかどうかを設定します。

上記のコマンドに指定するサービスキーを、次に示します。

表 10-1 Windows 環境での JP1/IM - Agent のサービスキー

表示名	サービスキー
JP1/IM3-Agent	jpc_imagent
JP1/IM3-Agent proxy	jpc_imagentproxy
JP1/IM3-Agent action	jpc_imagentaction
JP1/IM3-Agent Metric forwarder	jpc_prometheus_server
JP1/IM3-Agent Alert forwarder	jpc_alertmanager
JP1/IM3-Agent Windows metric collector	jpc_windows_exporter
JP1/IM3-Agent Synthetic metric collector	jpc_blackbox_exporter
JP1/IM3-Agent Log trapper	jpc_fluentd
JPC YA Cloudwatch exporter	jpc_ya_cloudwatch_exporter
JPC Promitor Scraper	jpc_promitor
JPC Promitor Resource Discovery	
JPC Script exporter	jpc_script_exporter

表 10-2 Linux 環境での JP1/IM - Agent のサービスキー

ユニット定義ファイル名	サービスキー
jpc_imagent.service	jpc_imagent
jpc_imagentproxy.service	jpc_imagentproxy
jpc_imagentaction.service	jpc_imagentaction
jpc_prometheus_server.service	jpc_prometheus_server

ユニット定義ファイル名	サービスキー
<code>jpc_alertmanager.service</code>	<code>jpc_alertmanager</code>
<code>jpc_node_exporter.service</code>	<code>jpc_node_exporter</code>
<code>jpc_blackbox_exporter.service</code>	<code>jpc_blackbox_exporter</code>
<code>jpc_ya_cloudwatch_exporter.service</code>	<code>jpc_ya_cloudwatch_exporter</code>
<code>jpc_fluentd.service</code>	<code>jpc_fluentd</code>
<code>jpc_process_exporter.service</code>	<code>jpc_process_exporter</code>
<code>jpc_promitor_scraper.service</code>	<code>jpc_promitor</code>
<code>jpc_promitor_resource_discovery.service</code>	
<code>jpc_script_exporter.service</code>	<code>jpc_script_exporter</code>

JP1/IM - Agent のアドオンプログラムの有効化・無効化については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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。

10.2 サービスの起動

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 サービスキー
```

サービスキーに「all」を指定した場合は、JP1/IM - Agent のすべてのサービスを起動します。

自動起動の設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.1(2)自動起動の有効化・無効化」を参照してください。

10.3 サービスの停止

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 サービスキー [-f]
```

サービスキーに「all」を指定した場合は、JP1/IM - Agent のすべてのサービスを停止します。

-f を指定した場合は、サービスを強制終了します。

OS シャットダウン時の自動停止については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.1(2)自動起動の有効化・無効化」を参照してください。

10.4 JP1/IM - Agent のオプション機能

10.4.1 OracleDB exporter のサービス

(1) Windows 環境

(a) サービス名と表示名

OracleDB exporter のサービス（Windows サービス）のサービス名と表示名を、次に示します。

サービスの動作環境	サービス名	表示名
物理ホスト	oracledb_exporter_インスタンス名	OracleDB Exporter インスタンス名
論理ホスト	oracledb_exporter_インスタンス名_論理ホスト名	OracleDB Exporter インスタンス名 論理ホスト名

(b) サービスの起動

次のどちらかの方法で、OracleDB exporter を起動します。

- Windows 管理ツールのサービス画面で起動する。
- sc コマンドや net コマンドで起動する。

(c) サービスの停止

次のどちらかの方法で、OracleDB exporter を停止します。

- Windows 管理ツールのサービス画面で停止する。
- sc コマンドや net コマンドで停止する。

(d) 自動起動の設定

Windows 管理ツールのサービス画面で、OracleDB exporter の「スタートアップの種類」に自動起動の設定をします。

(2) Linux 環境

(a) ユニット名と Description

Linux 環境での OracleDB exporter のサービスのユニット名と Description を、次に示します。

サービスの動作環境	ユニット名	Description
物理ホスト	oracledb_exporter_インスタンス名	OracleDB Exporter インスタンス名

サービスの動作環境	ユニット名	Description
論理ホスト	oracledb_exporter_インスタンス名_論理ホスト名	OracleDB Exporter インスタンス名 論理ホスト名

(b) サービスの起動

次のコマンドでサービスを起動します。

```
$ systemctl start ユニット名
```

(c) サービスの停止

次のコマンドでサービスを停止します。

```
$ systemctl stop ユニット名
```

(d) 自動起動の設定

- 自動起動の有効化

次のコマンドでサービスの自動起動を有効にします。

```
$ systemctl enable ユニット名
```

- 自動起動の無効化

次のコマンドでサービスの自動起動を無効にします。

```
$ systemctl disable ユニット名
```

(e) 死活監視

次のコマンドでサービスの稼働状況を確認します。

```
$ systemctl is-active ユニット名
```

10.4.2 Node exporter for AIX のサービス

Node exporter for AIX のサービスの操作は、監視対象の AIX ホストで実施します。

(1) サービスの登録の有効化

次のコマンドでサービスの登録を有効にします。

- 物理ホスト運用の場合

```
mkssys -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/jp1ima/bin/node_exporter_aix' -CcADmdiabf -p 20730 2>&1 | logger¥"
```

- 論理ホスト運用の場合

```
mkssys -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/jp1ima/bin/node_exporter_aix' -CcADmdiabf -p 20730 2>&1 | logger¥"
```

注※

論理ホスト名が8バイト以上の場合は、「jpc_node_exporter_aix_」の後ろに7文字以内の任意の文字列を付加して、-s オプションに指定します。また、-s オプションに指定する文字列は、lssrc -a コマンドのSubsystem 内で一意にしてください。

上記の node_exporer_aix コマンドのオプションの詳細を、次に示します。

- node_exporer_aix コマンドのオプション

項目名	説明	変更可否	JP1/IM - Agent でユーザーが設定する内容	JP1/IM - Agent のデフォルト値
-C※	linux node exporter に関するメトリックスの収集を行う場合に指定します。	○	—	—
-c※	CPU に関するメトリックスの収集を行う場合に指定します。	○	—	—
-A※	ディスクアダプタに関するメトリックスの収集を行う場合に指定します。	○	—	—
-D※	ディスクパスに関するメトリックスの収集を行う場合に指定します。	○	—	—
-m※	メモリに関するメトリックスの収集を行う場合に指定します。	○	—	—
-d※	ディスクに関するメトリックスの収集を行う場合に指定します。	○	—	—
-j※	ネットワークインターフェースに関するメトリックスの収集を行う場合に指定します。	○	—	—
-a※	ネットアダプタに関するメトリックスの収集を行う場合に指定します。	○	—	—
-b※	ネットバッファに関するメトリックスの収集を行う場合に指定します。	○	—	—
-f※	ファイルシステムに関するメトリックスの収集を行う場合に指定します。	○	—	—

項目名	説明	変更可否	JP1/IM - Agent でユーザーが設定する内容	JP1/IM - Agent のデフォルト値
-p	待ち受けポートを指定します。	○	ポートを変更したい場合に指定します。	-p 20730

(凡例)

○：変更可 －：該当なし

注※

-p 以外のオプションをすべて指定していない場合は有効になります。

(2) サービスの登録の無効化

次のコマンドでサービスの登録を無効にします。

- 物理ホスト運用の場合

```
rmssys -s jpc_node_exporter_aix
```

- 論理ホスト運用の場合

```
rmssys -s jpc_node_exporter_aix 論理ホスト名※
```

注※

論理ホスト名が 8 バイト以上の場合は、「10.4.2(1)サービスの登録の有効化」または「10.4.2(3)サービスの登録の変更」で指定した 7 文字以内の任意の文字列を、「jpc_node_exporter_aix_」の後ろに付加して、-s オプションに指定します。

(3) サービスの登録の変更

Node exporter for AIX のポート番号を変更する場合は、次のコマンドでサービス登録を変更します。

- 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/jp1ima/bin/node_exporter_aix' -CcADmdiabf -p 変更後のポート番号 2>&1 | logger¥"
```

- 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/jp1ima/bin/node_exporter_aix' -CcADmdiabf -p 変更後のポート番号 2>&1 | logger¥"
```

注※

論理ホスト名が8バイト以上の場合、[jpc_node_exporter_aix_]の後ろに7文字以内の任意の文字列を付加して、-s オプションに指定します。また、-s オプションに指定する文字列は、lssrc -a コマンドのSubsystem 内で一意にしてください。

(4) サービスの状態の確認

次のコマンドでサービスの状態を確認します。

- 物理ホスト運用の場合

```
lssrc -s jpc_node_exporter_aix
```

- 論理ホスト運用の場合

```
lssrc -s jpc_node_exporter_aix_論理ホスト名※
```

注※

論理ホスト名が8バイト以上の場合、[10.4.2(1)サービスの登録の有効化]または[10.4.2(3)サービスの登録の変更]で指定した7文字以内の任意の文字列を、[jpc_node_exporter_aix_]の後ろに付加して、-s オプションに指定します。

(5) サービスの登録内容の確認

次のコマンドでサービスの登録内容を確認します。

- 物理ホスト運用の場合

```
lssrc -S -s jpc_node_exporter_aix
```

- 論理ホスト運用の場合

```
lssrc -S -s jpc_node_exporter_aix_論理ホスト名※
```

注※

論理ホスト名が8バイト以上の場合、[10.4.2(1)サービスの登録の有効化]または[10.4.2(3)サービスの登録の変更]で指定した7文字以内の任意の文字列を、[jpc_node_exporter_aix_]の後ろに付加して、-s オプションに指定します。

(6) サービスの起動

1. サービスを起動する。

次のコマンドでサービスを起動します。

- 物理ホスト運用の場合

```
startsrc -s jpc_node_exporter_aix
```

- 論理ホスト運用の場合

```
startsrc -s jpc_node_exporter_aix_論理ホスト名※
```

注※

論理ホスト名が 8 バイト以上の場合は、「10.4.2(1)サービスの登録の有効化」または「10.4.2(3)サービスの登録の変更」で指定した 7 文字以内の任意の文字列を、「jpc_node_exporter_aix_」の後ろに付加して、-s オプションに指定します。

2. サービスの起動を確認する。

「10.4.2(4)サービスの状態の確認」を実施し、サービスが起動したことを確認してください。

(7) サービスの停止

1. サービスを停止する。

次のコマンドでサービスを停止します。

- 物理ホスト運用の場合

```
Node exporter for AIXの配置先/jp1ima/bin/jpc_stop_node_exporter_aix
```

- 論理ホスト運用の場合

```
Node exporter for AIXの配置先/jp1ima/bin/jpc_stop_node_exporter_aix -h 論理ホスト名※
```

注※

論理ホスト名が 8 バイト以上の場合は、「10.4.2(1)サービスの登録の有効化」または「10.4.2(3)サービスの登録の変更」で指定した 7 文字以内の任意の文字列を、「jpc_node_exporter_aix_」の後ろに付加して、-s オプションに指定します。

2. サービスの停止を確認する。

「10.4.2(4)サービスの状態の確認」を実施して、サービスが停止したことを確認します。

3. node_exporter_aix プロセスの停止を確認する。

ps コマンドを実行し、node_exporter_aix プロセスが停止したことを確認します。

(8) サービスの強制停止

1. サービスを強制停止する。

次のコマンドでサービスを強制停止します。

- 物理ホスト運用の場合

```
Node exporter for AIXの配置先/jp1ima/bin/jpc_stop_node_exporter_aix -f
```

- 論理ホスト運用の場合

```
Node exporter for AIXの配置先/jp1ima/bin/jpc_stop_node_exporter_aix -f -h 論理ホスト名※
```

注※

論理ホスト名が8バイト以上の場合は、「10.4.2(1)サービスの登録の有効化」または「10.4.2(3)サービスの登録の変更」で指定した7文字以内の任意の文字列を、「jpc_node_exporter_aix_」の後ろに付加して、-s オプションに指定します。

2. サービスの停止を確認する。

「10.4.2(4)サービスの状態の確認」を実施して、サービスが停止したことを確認します。

3. node_exporter_aix プロセスの停止を確認する。

ps コマンドを実行し、node_exporter_aix プロセスが停止したことを確認します。

(9) 自動起動の有効化

1. 自動起動を設定する。

次のコマンドで自動起動を有効にします。

- 物理ホスト運用の場合

```
mkitab "jpcaixexporter:2:wait:startsrc -s jpc_node_exporter_aix"
```

- 論理ホスト運用の場合

```
mkitab "jpcaixexporter:2:wait:startsrc -s jpc_node_exporter_aix_論理ホスト名※"
```

注※

論理ホスト名が8バイト以上の場合は、「10.4.2(1)サービスの登録の有効化」または「10.4.2(3)サービスの登録の変更」で指定した7文字以内の任意の文字列を、「jpc_node_exporter_aix_」の後ろに付加して、-s オプションに指定します。

2. 設定内容を確認する。

次のコマンドで設定内容を確認します。

```
lsitab -a
```

(実行結果の例)

```
init:2:initdefault:  
brc::sysinit:/sbin/rc.boot 3 >/dev/console 2>&1 # Phase 3 of system boot  
.  
.  
.  
jpcaixexporter:2:wait:startsrc -s jpc_node_exporter_aix
```

(10) 自動起動の無効化

1. 自動起動を設定する。

次のコマンドで自動起動を無効にします。

- 物理ホスト運用の場合

```
rmitab "jpcaixexporter"
```

- 論理ホスト運用の場合

```
rmitab "jpcaixexporter"
```

2. 設定内容を確認する。

次のコマンドで、手順 1 で指定した項目が削除されていることを確認します。

```
lsitab -a
```

(11) 自動停止の有効化

1. /etc/rc.shutdown ファイルをテキストエディターで開き、次に示す Node exporter for AIX の記述を追加する。

- 物理ホスト運用の場合

```
Node exporter for AIXの配置先/jp1ima/bin/jpc_stop_node_exporter_aix
```

- 論理ホスト運用の場合

```
Node exporter for AIXの配置先/jp1ima/bin/jpc_stop_node_exporter_aix -h 論理ホスト名※
```

注※

論理ホスト名が 8 バイト以上の場合は、「10.4.2(1)サービスの登録の有効化」または「10.4.2(3)サービスの登録の変更」で指定した 7 文字以内の任意の文字列を、「jpc_node_exporter_aix_」の後ろに付加して、-s オプションに指定します。

2. /etc/rc.shutdown ファイルの最後に、次に示す 1 行を追加する。

```
exit 0
```

/etc/rc.shutdown スクリプトは、最後に実行したコマンドの終了コードが「0」以外の場合、エラーと認識してシャットダウンの処理を中断します。

(12) 自動停止の無効化

1. /etc/rc.shutdown ファイルをテキストエディターで開き、次に示す Node exporter for AIX の記述を削除する。

- 物理ホスト運用の場合

```
Node exporter for AIXの配置先/jp1ima/bin/jpc_stop_node_exporter_aix
```

- 論理ホスト運用の場合

```
Node exporter for AIXの配置先/jp1ima/bin/jpc_stop_node_exporter_aix -h 論理ホスト名※
```

注※

論理ホスト名が 8 バイト以上の場合、[「10.4.2\(1\)サービスの登録の有効化」](#) または [「10.4.2\(3\)サービスの登録の変更」](#) で指定した 7 文字以内の任意の文字列を、「jpc_node_exporter_aix_」の後ろに付加して、-s オプションに指定します。

2. /etc/rc.shutdown ファイルの最後に、次に示す 1 行を追加する。

```
exit 0
```

/etc/rc.shutdown スクリプトは、最後に実行したコマンドの終了コードが「0」以外の場合、エラーと認識してシャットダウンの処理を中断します。

10.5 クラスタシステムで運用する場合

10.5.1 サービスの起動

クラスタソフトから起動します。

10.5.2 サービスの停止

クラスタソフトから停止します。

10.5.3 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。

10.5.4 OS シャットダウン時の自動停止

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自動停止の設定は行いません。

11

BJEX または JP1/AS との連携

JP1/IM は、BJEX または JP1/AS が発行する応答要求メッセージを JP1 イベントとして監視し、JP1/IM - View から応答入力する機能を提供しています。この章では、BJEX または JP1/AS と連携するために JP1/IM が提供する機能、BJEX または JP1/AS との連携方法、および BJEX または JP1/AS 連携時に使用するコマンドオプションについて説明します。

11.1 BJEX または JP1/AS との連携の概要

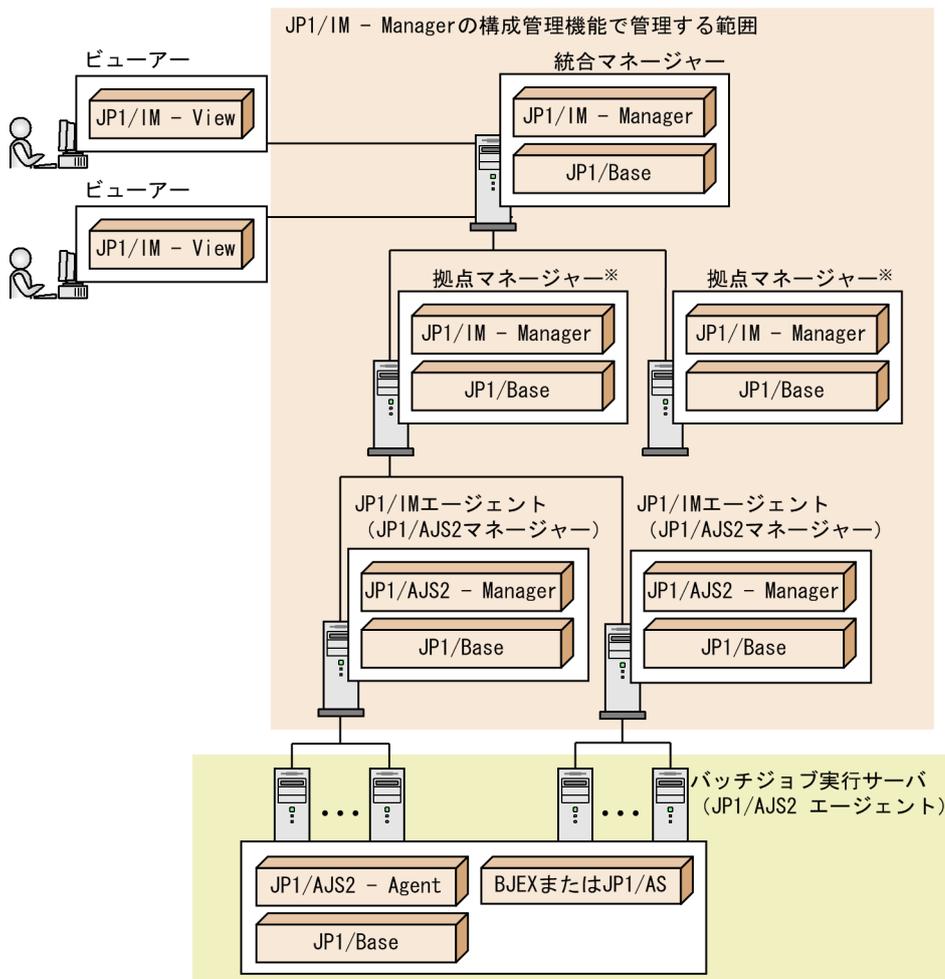
BJEX は、メインフレームと類似のジョブ管理システムを、オープンシステムで実現する製品です。JP1/AS は、バッチジョブのためのシェルスクリプトを作成・実行するための製品です。JP1/AJS と連携して、バッチジョブ（バッチ処理を実行するジョブ）を制御するジョブ管理システムを、**バッチジョブ実行システム**といいます。バッチジョブ実行システムに JP1/IM を導入することで、BJEX または JP1/AS が発行する JP1 イベントを基に、JP1/IM - View からバッチジョブの実行状況の監視、および実行結果の確認ができます。

BJEX または JP1/AS が出力するメッセージには、バッチジョブの実行中にオペレーターに応答入力を促す応答要求メッセージがあります。BJEX または JP1/AS は、応答要求メッセージを JP1 イベントとして発行します。JP1/IM では、この JP1 イベントを監視し、メッセージに対して応答入力できる機能を提供しています。応答要求メッセージに相当する JP1 イベントを**応答待ちイベント**と呼びます。応答待ちイベントを管理し、応答する機能を**応答待ちイベント管理機能**と呼びます。応答待ちイベント管理機能は、BJEX または JP1/AS と連携する場合に使用します。デフォルトでは無効となっているため、BJEX または JP1/AS と連携する場合は有効にしてください。

11.1.1 バッチジョブ実行システムと連携する場合のシステム構成

バッチジョブ実行システムと JP1/IM を連携する場合のシステム構成について説明します。

図 11-1 バッチジョブ実行システムと JP1/IM の構成例



注※ 拠点マネージャーまたは中継マネージャーを配置できます。

図の例では、拠点マネージャーがある階層型のシステムで、バッチジョブ実行システムを監視しています。

各サーバの役割、および前提製品について説明します。適用 OS については、各製品のマニュアルを参照してください。また、適用バージョンについては、JP1/IM - Manager のリリースノートを参照してください。

ビューアー

JP1/IM - View から JP1/IM - Manager に接続して、監視や操作をします。前提製品を次に示します。

- JP1/IM - View

統合マネージャー

システムを統合管理するサーバです。前提製品を次に示します。

- JP1/IM - Manager
- JP1/Base

拠点マネージャーまたは中継マネージャー

大規模なシステムを監視する場合などシステムを階層で管理したい場合に、統合マネージャーの下に配置するサーバです。前提製品を次に示します。

- JP1/IM - Manager
- JP1/Base

JP1/IM エージェント (JP1/AJS マネージャー)

JP1/IM の監視対象のサーバです。図の例では、JP1/AJS のマネージャーでもあります。前提製品を次に示します。

- JP1/AJS - Manager
- JP1/Base

バッチジョブ実行サーバ (JP1/AJS エージェント)

JP1/AJS - Manager から実行依頼を受けたバッチジョブなどの処理を実行するサーバです。バッチジョブ実行サーバは、JP1/IM の構成管理対象に含まれていなくても、JP1/IM と連携できます。JP1/IM - Manager とバッチジョブ実行サーバの BJEX または JP1/AS は 1 : n (n は 1 以上の整数) の構成で連携できます。連携する場合の設定方法については、「[11.3 BJEX または JP1/AS と連携するための設定](#)」を参照してください。

前提製品を次に示します。

- JP1/AJS - Agent
- JP1/Base
- BJEX または JP1/AS

11.2 BJEX または JP1/AS 連携用の JP1/IM の機能

BJEX または JP1/AS 連携用に JP1/IM が提供している機能について説明します。

11.2.1 応答待ちイベントと JP1/IM の関係

バッチジョブがオペレーターの応答入力待ちの状態になると発行される応答待ちイベントは、次のとおりです。

- BJEX の場合
イベント ID : 00005C21
- JP1/AS の場合
イベント ID : 00007121

応答待ちイベントを JP1/IM で監視するためには、BJEX または JP1/AS 側で、応答待ちイベントを JP1/IM - Manager のホスト（統合マネージャー）に直接発行する必要があります。また、JP1/IM - Manager では、応答待ちイベント管理機能を有効にする必要があります。

応答待ちイベント（イベント ID : 00005C21）の詳細については、マニュアル「uCosminexus Batch Job Execution Server 使用の手引」を参照してください。

応答待ちイベント（イベント ID : 00007121）の詳細については、マニュアル「JP1/Advanced Shell」を参照してください。

(1) 応答待ちイベントの発行経路

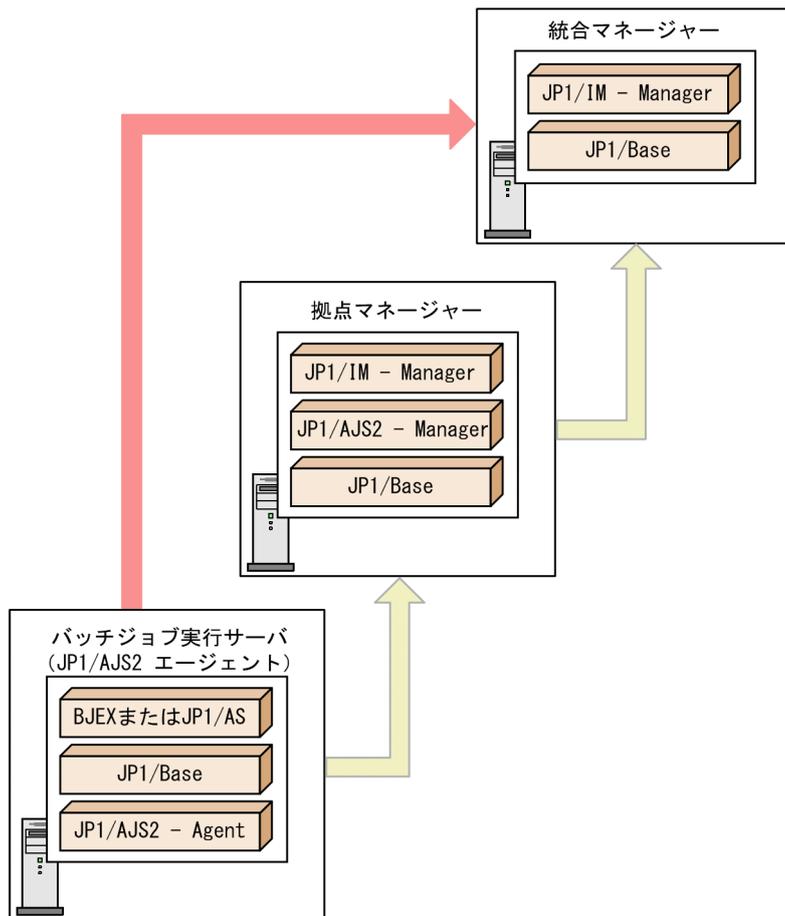
BJEX または JP1/AS が発行する応答待ちイベントは、JP1/Base のイベント転送経路を使わずに、統合マネージャーに対して直接発行します。BJEX が発行する応答待ちイベントを統合マネージャーに対して直接発行するには、BJEX の設定ファイル (bjex.conf) の JP1IM_MANAGER_HOST パラメーターで JP1/IM - Manager のホスト名を指定します。また、JP1/AS が連携する JP1/IM は、JP1/AS の環境ファイルの HOSTNAME_JP1IM_MANAGER パラメーターで指定します。

BJEX または JP1/AS が発行する応答待ちイベントと BJEX または JP1/AS 以外の製品が発行する JP1 イベントの到着順序

JP1/AJS や JP1/Base など、BJEX または JP1/AS ホスト上にある BJEX または JP1/AS 以外の製品が発行する JP1 イベントは、JP1/Base の転送経路を使って、拠点マネージャーを経由して統合マネージャーに転送します。そのため、BJEX または JP1/AS が発行する応答待ちイベントと BJEX または JP1/AS 以外の製品が発行した JP1 イベントが統合マネージャーに到着する順番が入れ替わる場合があります。この場合は、応答待ちイベントのメッセージテキスト中に含まれるジョブ ID を参照して、ジョブごとにメッセージを区別してください。

BJEX または JP1/AS ホストから発行される応答待ちイベントの発行経路を次の図に示します。

図 11-2 BJEX または JP1/AS ホストから発行される応答待ちイベントの発行経路



(凡例)



: BJEX または JP1/AS の応答待ちイベントの発行経路



: JP1/AJS2, JP1/Base の JP1 イベントの発行経路 (JP1/Base の転送経路を使用)

❗ 重要

BJEX または JP1/AS が指定したホスト以外の JP1/IM - Manager に応答待ちイベントを転送した場合、転送先のホストでは応答待ちイベントとして扱われません。そのため、転送先のホストでは応答入力できません。

(2) 応答待ちイベント管理機能

応答待ちイベント管理機能を有効にすると、応答待ちイベントに対して、JP1/IM - View から応答入力するための機能が有効になります。応答待ちイベント管理機能は BJEX または JP1/AS と連携する JP1/IM - Manager で設定します。

また、応答待ちイベント管理機能を有効にしたあとに、ユーザーごとに応答入力や操作を可能にするかどうかを、JP1/IM - View の [ユーザー環境設定] 画面で設定する必要があります。

設定方法については、「11.3 BJEX または JP1/AS と連携するための設定」を参照してください。

なお、応答待ちイベント管理機能、および応答待ちイベントの応答・操作を有効にしなくても、通常のJP1イベントとして応答待ちイベントを監視できます。

❗ 重要

応答待ちイベントとして扱われるJP1イベントは、応答待ちイベント管理機能を有効にしたあとにJP1/IM - Managerが受信した応答待ちイベントです。

11.2.2 応答待ちイベントの監視

応答待ちイベントは通常のJP1イベントと同様に扱われます。そのため自動アクションによる通知なども行えます。

ここでは、次の機能について、応答待ちイベントへの対応を説明します。このほかの機能については、通常のJP1イベントと同じ対応のため説明を省略します。

- [イベントコンソール] 画面での監視
- JP1 イベントのフィルタリング
- 繰り返しイベントの監視
- イベント検索
- JP1/IM - View での表示情報のCSV出力

(1) [イベントコンソール] 画面での監視

応答待ちイベントは、通常のJP1イベントと同様に、[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] ページのイベント一覧に表示されます。また、応答待ちイベント管理機能、および応答待ちイベントの応答・操作を有効にした場合だけ表示される [応答待ちイベント] ページには、応答待ちイベントだけが表示されます。

[イベントコンソール] 画面のイベント一覧では、通常のJP1イベントと同様に、応答待ちイベントに対して次の操作・設定ができます。

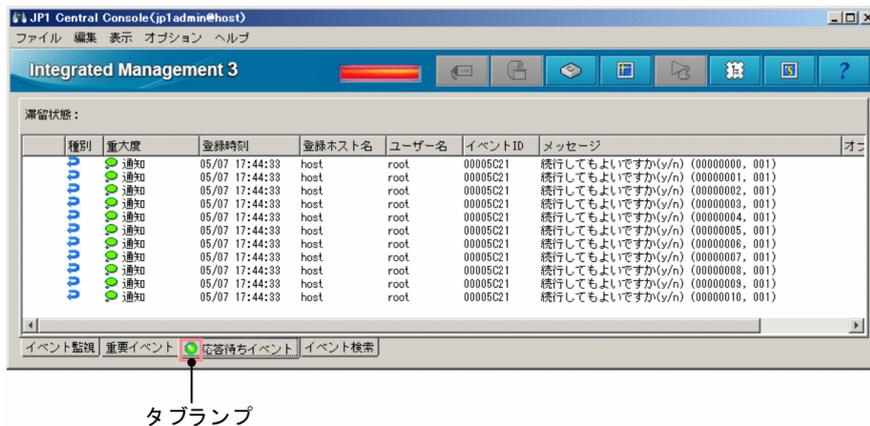
- 応答待ちイベントの詳細表示
- 連携製品のモニター起動
- 自動アクションの実行結果表示
- JP1 イベントの表示項目の変更
- JP1 イベントの背景色設定
- 応答待ちイベントへの対処状況設定
- 指定期間のイベント表示の設定

これらの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「4.1 JP1 イベントによる集中監視」を参照してください。

(a) [応答待ちイベント] ページでの監視

[応答待ちイベント] ページには、応答していない応答待ちイベントの一覧が表示されます。[応答待ちイベント] ページを次に示します。

図 11-3 [応答待ちイベント] ページ



応答していない応答待ちイベントがあるかどうかは、[応答待ちイベント] ページのタブランプで確認できます。[応答待ちイベント] ページに応答待ちイベントが表示されると、[応答待ちイベント] ページのタブランプが緑色に点灯します。

応答待ちイベントは、イベント DB とは別に、応答待ちイベント滞留ファイルと呼ばれるファイルに保持されます。これを**応答待ちイベントの滞留**といいます。[応答待ちイベント] ページには、応答待ちイベントファイルに滞留している応答待ちイベントの情報が表示されます。

応答待ちイベントは、次の契機で [応答待ちイベント] ページから削除されます。

- 応答待ちイベントに回答したとき
- 応答待ちイベントの滞留が解除されたとき
- 応答待ちイベントがキャンセルされたとき

応答待ちイベントの滞留が解除される契機については、「11.2.3 応答待ちイベントの滞留」を参照してください。

[応答待ちイベント] ページに表示されているすべての応答待ちイベントが [応答待ちイベント] ページから消えると、タブランプの点灯が消えます。

各ページのイベント一覧では、応答待ちイベントであることが判別できるように、[種別] に応答待ちイベントを示すマーク  が表示されます。

なお、[応答待ちイベント] ページでは、JP1 イベントの背景色を設定しても背景に色は付きません。

(2) 応答待ちイベントのフィルタリング

次のフィルターで応答待ちイベントをフィルタリングできます。

- ユーザーフィルター
- 重要イベントフィルター
- 表示フィルター

応答待ちイベント管理機能を有効にすると、ユーザーフィルター、および重要イベントフィルターの条件定義画面に、応答待ちイベントを表示対象とするかどうかを選択する項目が表示されます。表示フィルターで応答待ちイベントをフィルタリングする場合は、応答待ちイベント管理機能、および応答待ちイベントの応答・操作を有効にする必要があります。

各フィルターの条件定義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「3.44.8 フィルターの条件定義画面」を参照してください。

なお、イベント取得フィルターには、応答待ちイベントをフィルタリングする条件指定はありません。イベント取得フィルターは、応答待ちイベントを発行する製品単位で JP1 イベントをフィルタリングするよう設定してください。

(3) 応答待ちイベントの集約表示

ネットワーク障害などが原因で、一つのバッチジョブから同一の応答待ちイベントが連続して発行された場合、集約表示されます。集約表示されるのは、[イベント監視] ページ、および [重要イベント] ページだけです。

何らかの障害によって同一の応答待ちイベントが複数発行されても、すべてに回答する必要はありません。一つの応答待ちイベントに回答することで、ほかの同一の応答待ちイベントは回答不要となります。ただし、回答不要となった応答待ちイベントは [応答待ちイベント] ページに残ったままとなるため、応答待ちイベントの滞留を解除する必要があります。応答待ちイベントの滞留については、「11.2.3 応答待ちイベントの滞留」を参照してください。

(4) 応答待ちイベントの検索

JP1 イベントを検索する際、応答待ちイベントを検索条件として指定できます。応答待ちイベント管理機能、および応答待ちイベントの応答・操作を有効にした場合だけ、[イベント検索条件設定] 画面に応答待ちイベントの条件項目が表示されます。

[イベント検索条件設定] 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「3.44.7 [イベント検索条件設定] 画面」を参照してください。

なお、ログインしているマネージャーを検索対象にした場合だけ応答待ちイベントに対して回答できます。ログインしているマネージャー以外を検索対象とした場合は、応答待ちイベントであれば表示されますが回答できません。

(5) JP1/IM - View での表示情報の CSV 出力

イベント一覧に表示された応答待ちイベントの情報を CSV 出力できます。CSV 出力する機能には、次の二つがあります。

- イベント一覧情報をファイルに保存する。
JP1/IM - View に表示されるイベント情報のスナップショットを CSV 出力して保存できます。スナップショットとは、特定のタイミングで情報を抽出することを意味します。
- JP1 イベントの情報やアクションの実行結果などをクリップボードにコピーする。
クリップボードにコピーする機能を有効にしている場合、応答待ちイベントの情報やアクションの実行結果などについて、選択した部分の情報を CSV 形式でクリップボードにコピーできます。デフォルトでは有効となっています。

応答待ちイベントを CSV 出力して保存、またはクリップボードにコピーできるイベント一覧を次の表に示します。

表 11-1 CSV 出力, またはクリップボードにコピーできるイベント一覧

操作	[イベント監視] ページ	[重要イベント] ページ	[関連イベント一覧] 画面	[応答待ちイベント] ページ	[イベント検索] ページ
CSV 出力	○	○	×	○	○
クリップボードにコピー	○	○	○	○	○

(凡例)

- ：できる
- ×：できない

応答待ちイベントを CSV 出力して保存、またはクリップボードへコピーした場合、アイコンで表示されている「種別」は、「応答待ちイベント」の文字列に変わって出力されます。また、繰り返しイベントのアイコンと応答待ちイベントのアイコンが同時に表示されている場合は、「繰り返しイベント, 応答待ちイベント」の文字列に変わって出力されます。[応答待ちイベント] ページの情報を CSV 出力した場合、ヘッダー情報の出力対象画面名には、「応答待ちイベント」が出力されます。

クリップボードにコピーする機能を有効にする手順については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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)」を参照してください。

11.2.3 応答待ちイベントの滞留

応答待ちイベント管理機能を有効にすると、マネージャーのイベント DB に到着した応答待ちイベントは、イベント DB とは別に、応答待ちイベント滞留ファイルへ 2,000 件まで保持されます。これを**応答待ちイベントの滞留**といいます。

[応答待ちイベント] ページには、応答待ちイベント滞留ファイルに保持されている応答待ちイベントの情報が表示されます。

(1) 応答待ちイベントの滞留が解除される契機

応答待ちイベントは、次の契機で滞留が解除され、応答待ちイベント滞留ファイルから削除されます。

- 応答待ちイベントの応答に成功した場合
- BJEX または JP1/AS から応答待ちイベントをキャンセルした場合
- 応答待ちイベントの滞留を手動で解除した場合
- 応答待ちイベントが 2,000 件を超えて発生した場合
最も古い応答待ちイベントの滞留が解除されます。
- 応答待ちイベント管理機能を無効にして JP1/IM - Manager を再起動した場合

滞留の解除後、JP1/IM - View でイベント一覧の表示を更新すると、[応答待ちイベント] ページから滞留を解除した応答待ちイベントの表示が削除されます。なお、滞留が解除されて [応答待ちイベント] ページから表示が削除されても、応答待ちイベントがイベント DB に残っている場合は、[イベント検索] ページから検索できます。

(2) 応答待ちイベントが上限の 2,000 件を超えた場合の通知

JP1/IM - Manager は、応答待ちイベントの滞留数を監視し、滞留数が 2,000 件を超えると、上限を超えたことを通知する JP1 イベント（イベント ID：00003F41）を発行します。また、[応答待ちイベント] ページ上には KAVB0551-E のメッセージが表示されます。

図 11-4 応答待ちイベントが 2,000 件を超えた場合の [応答待ちイベント] ページ



滞留している応答待ちイベントの上限超過を通知する JP1 イベントは、一度しか発行されません。また、KAVB0551-E のメッセージは [応答待ちイベント] ページに表示されたままとなります。滞留数が上限を超えた場合は、メッセージに従って対処したあとに、滞留状態の監視を復帰させてください。滞留状態の監視を復帰させると、[応答待ちイベント] ページ上に表示されていた KAVB0551-E のメッセージが消え、再度 2,000 件を超えたときに JP1 イベントで通知します。

滞留状態の監視の復帰方法については、「11.4.4 応答待ちイベントの滞留状態の監視を復帰させる」を参照してください。

滞留解除された応答待ちイベントに応答したい場合

滞留数が上限を超えて、[応答待ちイベント] ページから削除された応答待ちイベントに対して応答したい場合は、[イベント検索] ページで応答待ちイベントを検索して応答してください。滞留解除された応答待ちイベントを特定するには、マネージャーの統合トレースログに出力される KAVB1801-E のメッセージで確認してください。

応答待ちイベントがイベント DB から削除された場合は、発行元のホスト上で、発行元が提供する応答コマンド (bjexchmsg または adshchmsg) を使用して応答できます。BJEX の応答コマンド (bjexchmsg) を使った応答方法については、マニュアル「uCosminexus Batch Job Execution Server 使用の手引」を参照してください。JP1/AS の応答コマンド (adshchmsg) を使った応答方法については、マニュアル「JP1/Advanced Shell」を参照してください。

11.2.4 応答待ちイベントへの応答

応答待ちイベントに対して、JP1/IM - View から応答入力できます。例えば、バッチ処理の続行をオペレーターに確認するメッセージに対して、続行するかどうかを「yes」などのテキスト形式で応答入力できます。応答入力、応答待ちイベントから表示する [応答入力] 画面で設定します。

[応答入力] 画面は、次に示すページのイベント一覧から応答したい応答待ちイベントを選択して起動します。

- [応答待ちイベント] ページ
- [イベント検索] ページ
検索先がログインしているマネージャーの場合だけ応答できます。
- [関連イベント一覧] 画面
[関連イベント一覧] 画面が、[応答待ちイベント] ページから派生した場合だけ応答できます。[イベント検索] ページから派生した場合は、検索先がログインしているマネージャーの場合だけ応答できません。

(1) 応答待ちイベントへの応答の仕組み

応答待ちイベントへの応答は、応答待ちイベントの発行元プロセスが存在し、応答できる状態の場合だけ可能です。発行元プロセスの状態は、[応答入力] 画面の [応答属性] に表示される [状態] で確認できます。発行元プロセスの状態は、[応答入力] 画面を表示するタイミングで、JP1/IM - Manager が発行元に対して確認します。発行元と JP1/IM - Manager 間の通信エラーなどで、発行元プロセスの状態が確認できなかった場合は、KAVB0555-E のメッセージが出力され [応答入力] 画面を表示できません。

図 11-5 [応答入力] 画面



[応答属性] の [状態] に表示される、応答待ちイベントの発行元プロセスの状態を次の表に示します。

表 11-2 応答待ちイベントの発行元プロセスの状態

発行元プロセスの状態	説明	応答入力の可否
READY TO RESPOND	発行元のジョブが応答を待っている状態。	○
NO LONGER MANAGED BY BJEX または NO LONGER MANAGED BY JP1/AS	次のどれかの状態を示す。 <ul style="list-style-type: none"> JP1/AJS から発行元のジョブがキャンセルされた状態。 発行元のジョブが KILL された状態。 応答した応答待ちイベントに対して [応答入力] 画面を表示・更新した場合に、対象の応答待ちイベントの状態を BJEX で保持していない。 	×
RESPONDED SUCCESSFULLY	[応答入力] 画面で応答し、応答に成功した状態 (応答した [応答入力] 画面にだけ表示される)。	×
ALREADY RESPONDED	すでに応答した状態 (応答した応答待ちイベントに対して [応答入力] 画面を表示・更新した場合に表示される)。	×

(凡例)

- ：応答入力できる
- ×：応答入力できない

発行元プロセスの状態が「READY TO RESPOND」の場合に、応答入力できます。それ以外の状態の応答待ちイベントは、すでに応答したか、発行元プロセスが存在しないため応答不要です。

応答待ちイベントに回答すると、回答入力した内容が発行元に送信されます。入力した内容が発行元に到達し、回答に成功すると、応答待ちイベントの状態が「対処済」になります。また、応答待ちイベントの滞留が解除され、[応答待ちイベント] ページから削除されます。

JP1/IM - Manager と発行元プロセス間で、応答待ちイベントの発行元プロセスの状態確認や回答入力通信の際、60 秒を超えて接続に失敗するとタイムアウトします。タイムアウト時間は変更できます。運用後に、応答待ちイベントの発行元サーバやネットワークの負荷が高いことが要因で、頻繁にエラーメッセージ (KAVB0554-E, KAVB0555-E) が出力される場合は、タイムアウト時間を長く設定してください。

い。タイムアウト時間の設定方法については、「11.3.4(1) 接続のタイムアウト時間の設定」を参照してください。

(2) 応答待ちイベントに応答するための条件

応答待ちイベントに応答できる条件を次に示します。

- 応答する JP1 ユーザーが JP1_Console_Operator 権限以上の操作権限を持っている。
- 応答していない応答待ちイベントである。
応答待ちイベントに応答できるのは一度だけです。イベント取得フィルターのイベント取得開始位置を変更して再取得しても、応答した応答待ちイベントには応答できません。
- 応答待ちイベント管理機能を有効にした状態で受信した応答待ちイベントである。
応答待ちイベント管理機能を無効にした状態で受信した応答待ちイベントは、応答入力できません。
- イベント検索をした場合、検索先がログインしているマネージャーである。

(3) BJEX または JP1/AS の応答コマンドによる応答

発行元プロセスと JP1/IM - Manager 間の通信エラーなどによって JP1/IM - View からの応答入力に失敗した場合や、応答待ちイベントの滞留が解除されてイベント DB から削除されてしまった場合など、JP1/IM - View 上から応答できなくなった場合は、発行元のホスト上で、発行元が提供する応答コマンド (bjexchmsg または adshchmsg) を使用して応答できます。BJEX の応答コマンド (bjexchmsg) を使った応答方法については、マニュアル「uCosminexus Batch Job Execution Server 使用の手引」を参照してください。JP1/AS の応答コマンド (adshchmsg) を使った応答方法については、マニュアル「JP1/Advanced Shell」を参照してください。

11.2.5 応答待ちイベントのキャンセル

JP1/AJS から BJEX または JP1/AS のジョブをキャンセルしたり、BJEX または JP1/AS でジョブを削除したりした場合など、発行した応答待ちイベントへの応答が不要になるケースがあります。このような場合、ジョブをキャンセルした時点で、BJEX は JP1/IM - Manager に対してキャンセルイベント (イベント ID : 00005C22, 00005C23, または 00005C24) を発行します。また、JP1/AS は JP1/IM - Manager に対してキャンセルイベント (イベント ID : 00007122, 00007123, または 00007124) を発行します。JP1/IM - Manager がキャンセルイベントを受信すると、キャンセル対象の応答待ちイベントの滞留が解除され、[応答待ちイベント] ページから削除されます。また、応答待ちイベントの対処状況が「対処済」となります。

BJEX のキャンセルイベントの詳細については、マニュアル「uCosminexus Batch Job Execution Server 使用の手引」を参照してください。JP1/AS のキャンセルイベントの詳細については、マニュアル「JP1/Advanced Shell」を参照してください。

また、JP1/IM - View 上から手動で応答待ちイベントをキャンセルすることもできます。不要となった応答待ちイベントをキャンセルするには、JP1/IM - View 上で応答待ちイベントの滞留を解除します。

11.3 BJEX または JP1/AS と連携するための設定

JP1/IM - Manager のセットアップが済んでいることを前提に、BJEX または JP1/AS と連携するための設定について説明します。

なお、JP1/Base と JP1/IM - Manager については次の構成および設定を推奨します。

- マネージャー上の JP1/Base, および JP1/IM - Manager をクラスタ構成にする。
- JP1/Base と JP1/IM - Manager のヘルスチェック機能を有効にする。

11.3.1 JP1/IM - Manager の設定

JP1/IM - Manager で必要な設定について説明します。

(1) 応答待ちイベント管理機能を有効にする

応答待ちイベント管理機能は JP1/IM - Manager で設定します。応答待ちイベント管理機能を有効にすると、次の機能が有効になります。

- 応答待ちイベントの滞留
- 応答待ちイベントのキャンセル
- 応答待ちイベントの応答・操作の設定
[ユーザー環境設定] 画面に応答待ちイベントの応答・操作を有効にするための設定項目が表示されます。
- 応答待ちイベントのフィルタリング
[ユーザーフィルター詳細設定] 画面, および [重要イベント定義設定] 画面に, 応答待ちイベントをフィルタリングするかどうかを選択する項目が表示されます。

応答待ちイベント管理機能を有効にする手順を次に示します。

1. jcoimdef コマンドを実行する。

`jcoimdef -resevent ON` を実行します。

2. JP1/IM - Manager を再起動する。

注 `jco_spm�_reload` コマンドによるリロードでは, 有効になりません。

`jcoimdef` コマンドの `-resevent` オプションについては, [11.5.1 `jcoimdef`] を参照してください。

(2) イベント取得フィルターの設定

イベント取得開始位置を, 前回停止したときの状態から処理を続行するように設定してください。

イベント取得フィルターの取得開始位置の設定手順を次に示します。

1. jcoimdef コマンドを実行する。

jcoimdef -b -1 を実行します。

2. jco_spm�_reload コマンドを実行するか、JP1/IM - Manager を再起動する。

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。

jco_spm�_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_spm�_reload」(1. コマンド)を参照してください。

11.3.2 JP1/IM - View の設定

JP1/IM - View で必要な設定について説明します。

(1) 応答待ちイベントの応答および操作を有効にする

応答待ちイベントの応答・操作は、ユーザーごとに JP1/IM - View の [ユーザー環境設定] 画面で有効に設定します。この設定を有効にすると、次の機能が有効となります。

- [応答待ちイベント] の監視
[イベントコンソール] 画面に [応答待ちイベント] ページが表示されます。
- 応答待ちイベントへの応答
[応答入力] 画面で応答できます。
- 応答待ちイベントの検索
[イベント検索条件設定] 画面に、検索条件として応答待ちイベントを指定する項目が表示されます。
- 応答待ちイベントのフィルタリング
[表示フィルター設定] 画面に、応答待ちイベントを表示対象にするかどうかを選択する項目が表示されます。

応答待ちイベントの応答・操作を有効にする手順を次に示します。

1. [ユーザー環境設定] 画面を表示する。
[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. [応答待ちイベント] の [有効] チェックボックスをチェックする。
3. [OK] ボタンをクリックする。

[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「3.44.6 [ユーザー環境設定] 画面」を参照してください。

(2) ユーザーフィルターの設定

ユーザーフィルターを使用して、ユーザーごとに監視できる JP1 イベントを制限できます。応答待ちイベントを表示させたくないユーザーには、ユーザーフィルターで応答待ちイベントを表示しないように設定してください。デフォルトでは応答待ちイベントを表示します。

ユーザーフィルターの作成方法、および変更方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「5.2.2 ユーザーフィルターを設定する」を参照してください。

[ユーザーフィルター詳細定義] 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「3.44.8 フィルターの条件定義画面」を参照してください。

11.3.3 JP1/Base の設定

認証サーバの JP1/Base で、応答待ちイベントを操作する JP1 ユーザーに対して操作権限を設定してください。

次の操作をする JP1 ユーザーには、JP1_Console_Operator 権限以上の操作権限が必要です。

- 応答待ちイベントへの応答入力
- 応答待ちイベントの滞留の手動解除

次の操作をする JP1 ユーザーには、JP1_Console_Admin 権限が必要です。

- 応答待ちイベントの滞留状態監視の復帰

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。

11.3.4 BJEX または JP1/AS と JP1/IM - Manager 間の通信に関する設定

BJEX または JP1/AS と JP1/IM - Manager 間の通信に関する設定について説明します。

(1) 接続のタイムアウト時間の設定

応答待ちイベントの発行元プロセスの状態確認や応答入力で通信する際の、接続のタイムアウト時間を変更できます。通常は設定を変更する必要はありません。運用後に、応答待ちイベントの発行元サーバやネットワークの負荷が高いことが要因で、頻繁にエラーメッセージ (KAVB0554-E, KAVB0555-E) が出力される場合は、タイムアウト時間を長く設定してください。タイムアウト時間は、JP1/IM - Manager で設定します。

接続のタイムアウト時間を変更する手順を次に示します。

1. マネージャーで任意のファイルを作成し、次のパラメーターを定義する。

[論理ホスト名¥JP1CONSOLEMANAGER]

”RESEV_TIMEOUT_MAX”=dword:16 進数値

論理ホスト名の部分を、物理ホストの場合はJP1_DEFAULT に、論理ホストの場合は論理ホスト名に設定します。

60~3,600 (秒) の 16 進数値で指定します。デフォルトは「dword:0000003c」(60 秒) です。

2. jbssetcnf コマンドを実行する。

作成した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、定義ファイルの設定が共通定義情報に反映されます。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_spm�_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_spm�_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_spm�_reload」(1. コマンド) を参照してください。

(2) ファイアウォール環境でのパケット・フィルタリングの設定

ファイアウォール環境で運用する場合は、BJEX または JP1/AS と JP1/IM - Manager 間の通信がファイアウォールを通過できるようにパケット・フィルタリングを設定してください。BJEX または JP1/AS と JP1/IM - Manager 間の通信で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）を次の表に示します。

表 11-3 BJEX または JP1/AS と JP1/IM - Manager 間の通信で使用するポート番号

サービス名	ポート	通過方向
jp1bsplugin	20306/tcp	JP1/IM - Manager → BJEX または JP1/AS
jp1imevt	20098/tcp	BJEX または JP1/AS → JP1/IM - Manager

(凡例)

→：コネクション確立時の接続方向を示す

このほかに、JP1/IM および JP1/Base が使用するポート番号について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」

11.3.5 BJEX または JP1/AS の設定

BJEX または JP1/AS で必要な設定について説明します。

(1) 連携する JP1/IM - Manager の指定

BJEX または JP1/AS が連携できる JP1/IM - Manager は 1 ホストであり、連携する JP1/IM - Manager を指定する必要があります。BJEX が連携する JP1/IM - Manager を指定するためには、BJEX の設定ファイル (bjex.conf) に、連携する JP1/IM - Manager のホスト名を指定します。JP1/AS が連携する JP1/IM - Manager を指定するためには、JP1/AS の環境ファイルに、連携する JP1/IM - Manager のホスト名を指定します。

BJEX の設定ファイル (bjex.conf) の詳細については、マニュアル「uCosminexus Batch Job Execution Server 使用の手引」を参照してください。JP1/AS の環境ファイルの詳細については、マニュアル「JP1/Advanced Shell」を参照してください。

(2) 応答待ちイベントの発行数の設定

BJEX または JP1/AS が発行する応答待ちイベントの発行数の上限を設定できます。滞留できる応答待ちイベントには 2,000 件の上限があるため、次の計算式の値が 2,000 以下になるように、応答待ちイベント数を見積もってください。

応答待ちイベントを出力する全ホストの USERREPLY_WAIT_MAXCOUNT パラメーター値の総和 + 他製品の最大応答待ちイベント出力数の総和

BJEX の応答待ちイベントの発行数の上限数は、BJEX の設定ファイル (bjex.conf) で設定します。JP1/AS の応答待ちイベントの発行数の上限数は、JP1/AS の環境ファイルで設定します。BJEX の応答待ちイベントの発行数の設定の詳細については、マニュアル「uCosminexus Batch Job Execution Server 使用の手引」を参照してください。JP1/AS の応答待ちイベントの発行数の設定の詳細については、マニュアル「JP1/Advanced Shell」を参照してください。

11.4 応答待ちイベントの操作

応答待ちイベントに対する操作手順について説明します。

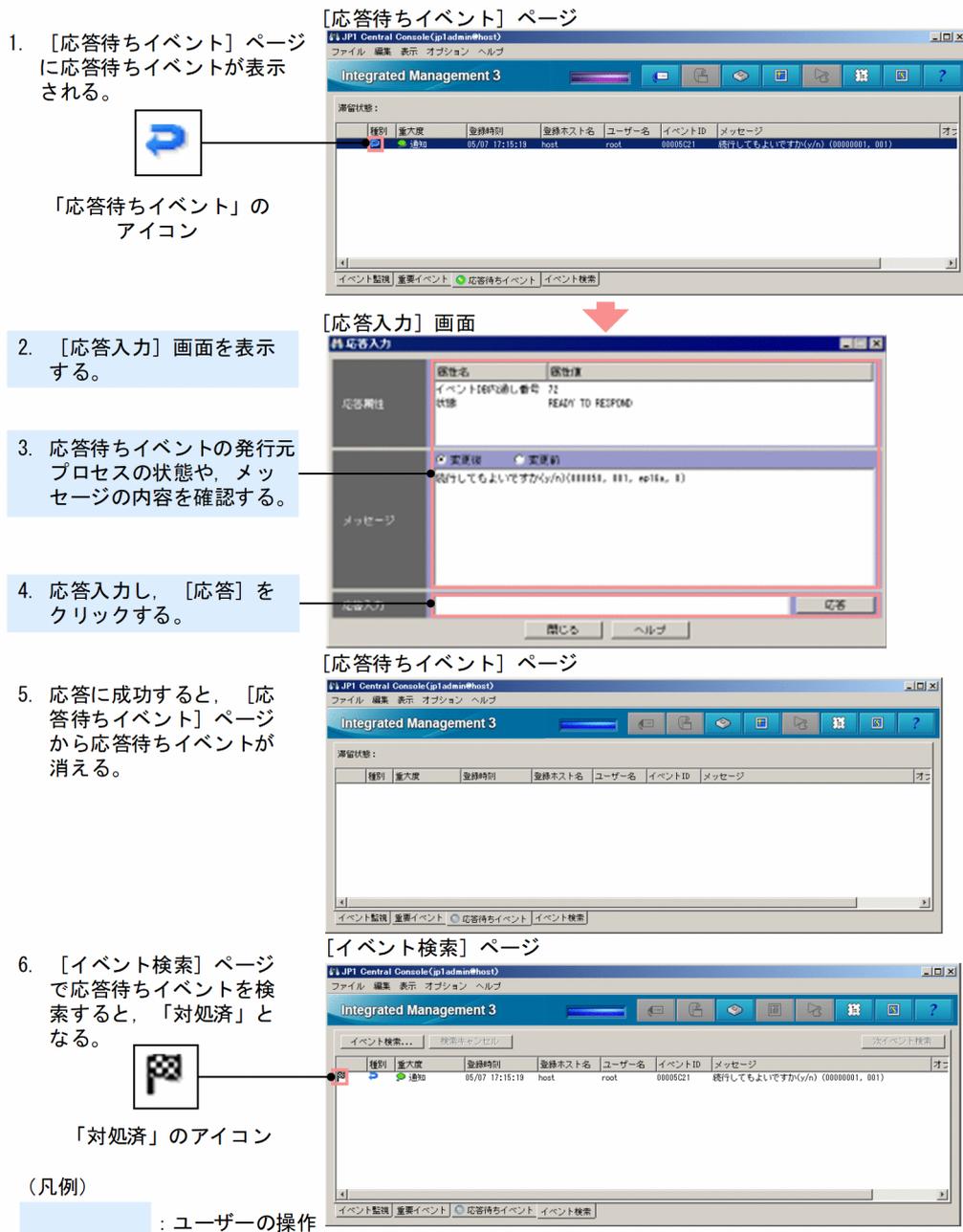
11.4.1 応答待ちイベントに回答する操作の流れ

セントラルコンソール、およびセントラルスコープで応答待ちイベントを監視して、応答する操作の流れについて説明します。

(1) セントラルコンソールで応答待ちイベントを監視する

セントラルコンソールで応答待ちイベントを監視し、応答する流れを次の図に示します。

図 11-6 セントラルコンソールで応答待ちイベントを監視して応答する流れ



図中の番号に従って説明します。

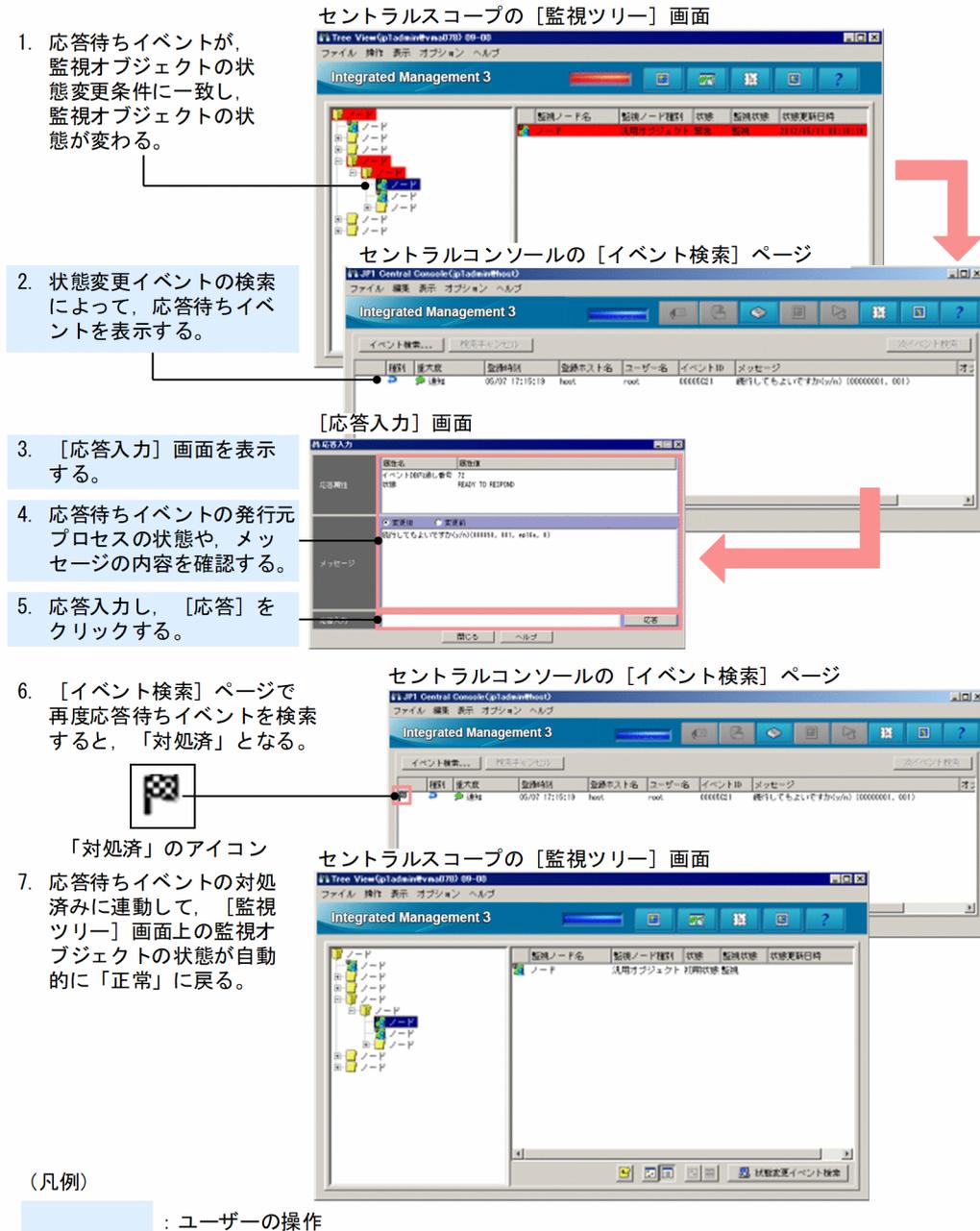
1. 応答待ちイベントを受信すると、[イベントコンソール] 画面の [応答待ちイベント] ページに
応答待ちイベントが表示されます。
2. 応答待ちイベントから [応答入力] 画面を表示します。
3. 応答待ちイベントの発行元プロセスの状態やメッセージの内容を確認します。
発行元プロセスの状態が「応答可能」になっていることを確認します。
4. [応答入力] 欄に
応答内容を入力し、[応答] ボタンをクリックします。
5. 応答に成功すると、[応答待ちイベント] ページから
応答待ちイベントが削除されます。

- [イベント検索] ページで応答待ちイベントを検索すると、応答待ちイベントの状態は「対処済」となります。

(2) セントラルスコープで応答待ちイベントを監視する

セントラルスコープで応答待ちイベントを監視して応答する流れを次の図に示します。

図 11-7 セントラルスコープで応答待ちイベントを監視して応答する流れ



図中の番号に従って説明します。

- 監視オブジェクトの状態変更条件に一致する応答待ちイベントを受信すると、監視オブジェクトの状態が変わります。

2. 監視オブジェクトから状態変更イベントを検索して、[イベント検索] ページに応答待ちイベントを表示します。
3. 応答待ちイベントから [応答入力] 画面を表示します。
4. 応答待ちイベントの発行元プロセスの状態やメッセージの内容を確認します。
発行元プロセスの状態が「応答可能」になっていることを確認します。
5. [応答入力] 欄に応答内容を入力し、[応答] ボタンをクリックします。
6. [イベント検索] ページで再度応答待ちイベントを検索すると、応答に成功した応答待ちイベントの状態は「対処済」となります。
7. 応答待ちイベントの対処済みに連動して、[監視ツリー] 画面上の監視オブジェクトの状態が正常に戻ります。

11.4.2 応答待ちイベントに応答する

応答待ちイベントに応答するための条件については、「[11.2.4\(2\) 応答待ちイベントに応答するための条件](#)」を参照してください。なお、この操作には JP1_Console_Operator 権限以上の操作権限が必要です。

応答待ちイベントに応答する手順を次に示します。

1. 次のどれかの方法で [応答入力] 画面を表示する。

- [応答待ちイベント] ページ、または [イベント検索] ページで応答待ちイベントを選択したあと、[メインメニュー] - [表示] - [応答入力] を選択する。
- [応答待ちイベント] ページ、[イベント検索] ページ、または [関連イベント一覧] 画面で応答待ちイベントを選択したあと、ポップアップメニューの [応答入力] を選択する。
- [イベント詳細] 画面の [応答入力] ボタンをクリックする。

2. [応答入力] 画面の [応答入力] 欄に、応答内容を入力する。

メッセージの内容を確認し、応答内容を入力します。

- 入力できるバイト数は 512 バイトまでです。
- 入力できる文字は、ASCII コード 0x20-0x7E の範囲の文字です。

3. [応答] ボタンをクリックする。

応答をしてよいかどうかを確認するダイアログボックスが表示されます。[はい] ボタンをクリックすると応答します。[いいえ] ボタンをクリックすると、応答しないで [応答入力] 画面に戻ります。

応答に成功すると、[応答待ちイベント] ページから応答待ちイベントが削除され、応答待ちイベントの対処状況が「対処済」に変わります。

11.4.3 応答待ちイベントの滞留を手動で解除する

応答が不要となった場合や、応答に成功したのに滞留の解除に失敗した場合に、応答待ちイベントの滞留を手動で解除してください。なお、この操作には JP1_Console_Operator 権限以上の操作権限が必要です。

応答待ちイベントの滞留を解除する手順を次に示します。

1. [イベントコンソール] 画面の [応答待ちイベント] ページを表示する。
2. 滞留を解除したい応答待ちイベントの発行元プロセスの状態を確認する。
滞留を解除したい応答待ちイベントを選択して、[応答入力] 画面を表示します。発行元プロセスの状態が「NO LONGER MANAGED BY BJEX」または「ALREADY RESPONDED」になっていることを確認します。
3. 応答待ちイベントの対処状況を「対処済」にする。
滞留を解除して問題なければ、応答待ちイベントの対処状況を「対処済」にします。応答待ちイベントを選択し、[表示] - [対処済] を選択します。
4. 滞留を解除したい応答待ちイベントを選択し、[表示] - [滞留解除] を選択する。または、ポップアップメニューの [滞留解除] を選択する。
複数の応答待ちイベントを選択できます。[滞留解除] を選択すると、滞留が解除されます。
イベント一覧の表示を更新すると、応答待ちイベントが [応答待ちイベント] ページから削除されます。

誤って滞留を解除した場合、再度滞留させることはできません。誤って滞留を解除した応答待ちイベントに応答したい場合は、[イベント検索] ページで応答待ちイベントを検索して応答してください。

11.4.4 応答待ちイベントの滞留状態の監視を復帰させる

応答待ちイベントの滞留数が 2,000 件を超えたあとに、滞留状態の監視を復帰させると、再び滞留数が 2,000 件を超えた場合に JP1 イベントで通知します。なお、この操作には JP1_Console_Admin 権限が必要です。

滞留状態の監視を復帰させる前に、マネージャーの統合トレースログであふれた応答待ちイベントを確認し、応答してください。滞留が解除された応答待ちイベントに応答する方法については、「[11.2.3\(2\) 応答待ちイベントが上限の 2,000 件を超えた場合の通知](#)」を参照してください。

応答待ちイベントの滞留状態の監視を復帰させ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] - [機能状態通知復帰] - [滞留状態監視] を選択する。
滞留状態の監視が復帰します。復帰したあとに [イベントコンソール] 画面を更新すると、[応答待ちイベント] ページの [滞留状態] に表示されている KAVB0551-E のメッセージが消えます。

11.5 BJEX または JP1/AS 連携時のコマンド

BJEX または JP1/AS と連携する場合に使用するコマンドのオプションについて説明します。そのほかのオプションや、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。なお、参照先のマニュアルでは、BJEX 連携用のオプションについては説明していません。

11.5.1 jcoimdef

jcoimdef コマンドは、JP1/IM - Manager のシステム環境を設定、または設定値を参照するためのコマンドです。このコマンドを実行すると設定内容が標準出力に出力されます。

BJEX または JP1/AS と連携する場合に指定するオプションを次に示します。

`-resevent {ON | OFF}`

`-resevent ON` を指定すると、応答待ちイベント管理機能が有効になります。`-resevent OFF` を指定すると、応答待ちイベント管理機能が無効になります。

JP1/IM - Manager を起動させたまま、jcoimdef コマンドの `-resevent` オプションで、応答待ちイベント管理機能を有効または無効に設定変更した場合は、JP1/IM - Manager の再起動が必要です。また、接続中の JP1/IM - View も再起動が必要です。

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。

11.5.2 jim_log.bat (Windows 限定)

jim_log.bat は、JP1/IM - Manager または JP1/IM - View で障害が発生したときに資料を採取するためのツールです。JP1/IM - Manager, JP1/IM - View, および JP1/Base の保守資料、OS のシステム情報、統合トレースログなどを採取します。

BJEX または JP1/AS と連携する場合に指定するオプションを次に示します。

`-a`

応答待ちイベント滞留ファイルを採取しない場合に指定します。

なお、jim_log.bat で採取した応答待ちイベント滞留ファイルは、次に示すフォルダに一次資料として格納されます。

物理ホストの一次資料の内部フォルダ

資料格納フォルダ¥jp1_default¥imm_1st¥cons¥log¥response

論理ホストの一次資料の内部フォルダ

資料格納フォルダ $\%論理ホスト名\%imm_1st\%cons\%log\%response$

jim_log.bat 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「jim_log.bat (Windows 限定)」(1. コマンド) を参照してください。

11.5.3 jim_log.sh (UNIX 限定)

jim_log.sh は、JP1/IM - Manager で障害が発生したときに資料を採取するためのツールです。JP1/IM - Manager および JP1/Base の保守資料、OS のシステム情報、統合トレースログなどを採取します。

BJEX または JP1/AS と連携する場合に指定するオプションを次に示します。

-a

応答待ちイベント滞留ファイルを採取しない場合に指定します。

なお、jim_log.sh で採取した応答待ちイベント滞留ファイルは、次に示すディレクトリに一次資料として格納されます。

物理ホストの一次資料の内部ディレクトリ

`./var/opt/jp1cons/log/response`

論理ホストの一次資料の内部ディレクトリ

`./共有ディスク/jp1cons/log/response`

jim_log.sh 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「jim_log.sh (UNIX 限定)」(1. コマンド) を参照してください。

12

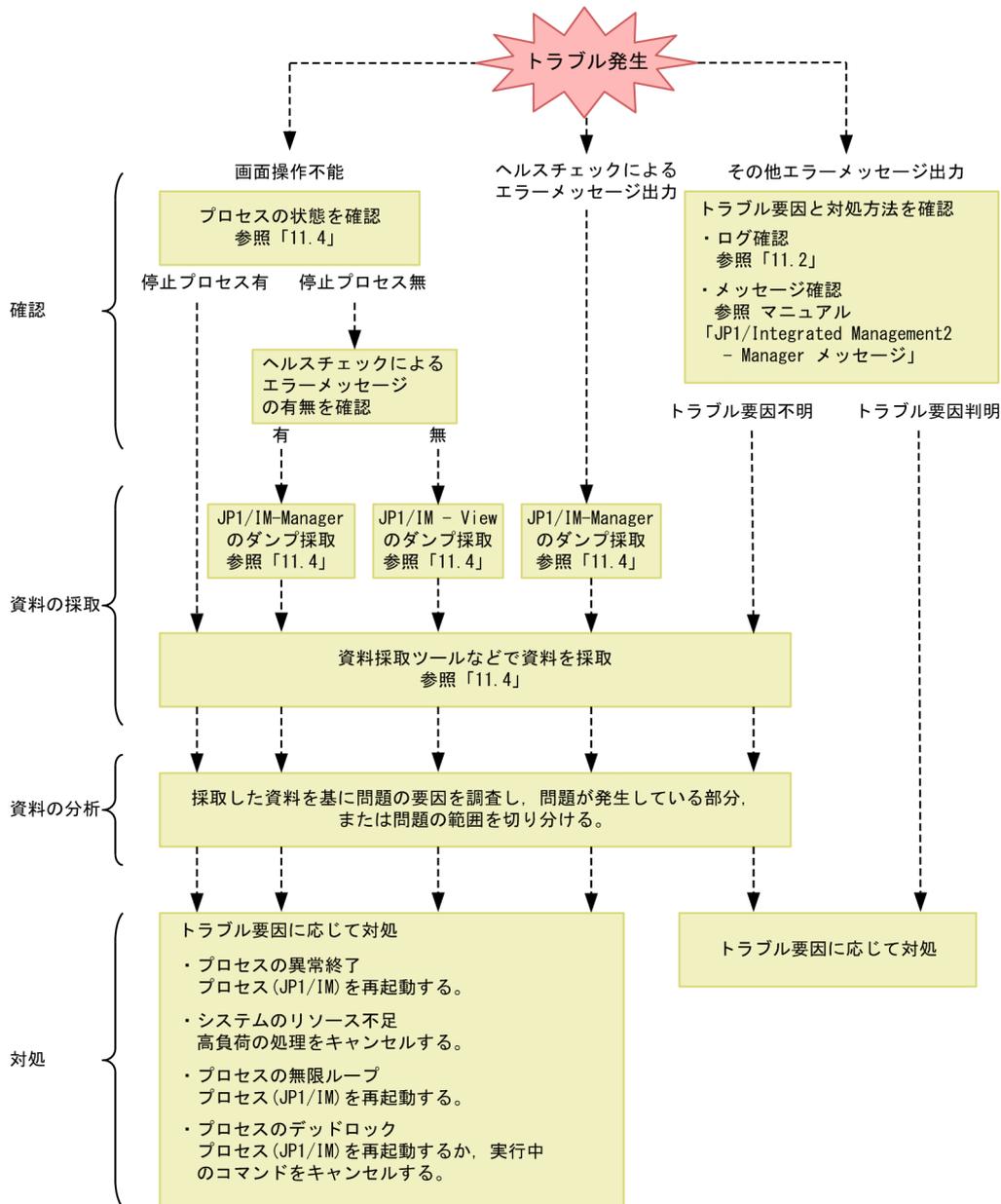
トラブルシューティング

この章では、JP1/IM でトラブルが発生した場合の対処方法や、トラブルの原因になりやすい項目について説明します。

12.1 対処の手順

JP1/IM でトラブルが起きた場合の対処の手順を次の図に示します。

図 12-1 トラブル発生時の対処手順



12.2 ログ情報の種類

この節では、JP1/IM を運用しているときに出力されるログ情報について説明します。

12.2.1 JP1/IM - Manager のログ情報

(1) 共通メッセージログ

共通メッセージログとは、システム側のトラブルを通知する、システム管理者向けのログ情報のことです。共通メッセージログは、必要最小限のトラブル情報を通知します。

共通メッセージログは、UNIX の場合は syslog ファイル、Windows の場合は Windows イベントログに出力されます。

なお、SUSE Linux 15 以降の場合、デフォルトでは syslog には出力されずに、ジャーナルと呼ばれるログファイルに出力されます。このマニュアルでのシスログ (syslog) をジャーナルに読み替えてください。

UNIX の場合は、次のファイルに出力されます。

- /var/log/messages (Linux の場合)

❗ 重要

UNIX の場合は、syslog ファイルにメッセージが出力されるときに、syslog ファイルの動作によってメッセージが出力されないことがあります。

(2) 統合トレースログ

統合トレースログとは、各プログラムが出力するトレース情報を、統合トレース機能 (HNTRLib2) を通じて、一つの出力先ファイルにまとめて採取するログ情報のことです。共通メッセージログより詳しい内容のメッセージが出力されます。

JP1/IM - Agent の製品プラグインのログは、JP1/IM - Manager の統合トレースログに出力されます。

統合トレースログのデフォルトの出力先は次のとおりです。

32bit 版の Windows の場合

システムドライブ¥Program Files¥Hitachi¥HNTRLib2¥spool¥hnr2{1|2|3|4}.log

64bit 版の Windows の場合

システムドライブ¥Program Files¥Hitachi¥HNTRLib2¥spool¥hnr2{1|2|3|4}.log

または

システムドライブ¥Program Files(x86)¥Hitachi¥HNTRLib2¥spool¥hnr2{1|2|3|4}.log

UNIX の場合

/var/opt/hitachi/HNTRLib2/spool/hntr2{1|2|3|4}.log

統合トレースログファイルは、任意のテキストエディターで参照できます。統合トレースログの出力例を次に示します。

図 12-2 統合トレースログファイルの出力例

The diagram shows a sample trace log output with labels pointing to specific fields:

- タイムゾーン** (Time Zone): Points to the TZ=(local)-9:00 line.
- OS情報** (OS Information): Points to the Microsoft WindowsNT5.2 (Build:3790) Service Pack 1 line.
- 統合トレースログ機能起動時刻** (Integrated Trace Log Function Start Time): Points to the 2007/02/05 20:58:50.875 timestamp.
- ホスト名** (Host Name): Points to the HOST line.
- 番号** (Number): Points to the message ID (e.g., 0000).
- 日付** (Date): Points to the date part of the timestamp (e.g., 2007/02/05).
- 時刻** (Time): Points to the time part of the timestamp (e.g., 21:07:17.890).
- AP名** (AP Name): Points to the application name (e.g., JP1/Console).
- pid**: Points to the process ID (e.g., 00000870).
- tid**: Points to the thread ID (e.g., JA83084D).
- メッセージID** (Message ID): Points to the message ID (e.g., KAVB1517-I).
- メッセージテキスト** (Message Text): Points to the message content (e.g., マネージャーを起動しました).

統合トレースログファイルに出力されるヘッダー情報と出力項目の説明を次に示します。

表 12-1 統合トレースログファイルのヘッダー情報

ヘッダー情報	説明
OS 情報	統合トレース機能が起動している OS の情報です。
ホスト名	統合トレース機能が起動しているホスト名です。
タイムゾーン	Windows の場合 OS のタイムゾーンです。 UNIX の場合 統合トレースプロセスの環境変数 TZ です。 環境変数 TZ が設定されていない場合は Unknown となります。
統合トレースログ機能起動時刻	統合トレース機能を起動した時刻です。

表 12-2 統合トレースログファイルの出力項目

出力項目	説明
番号 (4 桁)	トレースレコードの通番 番号はログを出力したプロセスごとに採番されます。
日付 (10 バイト)	トレースの取得日付 : yyyy/mm/dd (年/月/日)
時刻 (12 バイト)	トレースの取得時刻 (ローカル時刻) : hh:mm:ss.sss (時:分:秒.ミリ秒)
AP 名 (16 バイト以内)	アプリケーションを識別するための名称 (アプリケーション識別名)。 JP1/IM - Manager で出力される AP 名は次のとおりです。 <ul style="list-style-type: none"> JP1/IM-Manager サービス JP1/IM-Manager

出力項目	説明
	<ul style="list-style-type: none"> イベント基盤サービス evflow アクション実行サービス jcamain 関連イベント発行サービス evgen セントラルスコープサービス jcsmain IM 構成管理サービス jcfmain インテリジェント統合管理基盤サービス jddmain プロセス管理 JCO_SPMD jcochstat コマンド jcochngstat そのほかのコマンド コマンド名 <p>JP1/IM - View で出力される AP 名は次のとおりです。</p> <ul style="list-style-type: none"> セントラルコンソール・ビューアー JP1/IM-View セントラルスコープ・ビューアー JP1/IM-View IM 構成管理・ビューアー JP1/IM-View ツリー編集画面 JP1/IM-Edit
pid	プロセス ID。OS が付けるプロセス ID。
tid	スレッド ID。スレッドを識別するための ID。
メッセージ ID	メッセージの出力形式で説明したメッセージ ID。この製品で使用するメッセージ ID。
メッセージテキスト	統合トレースログに出力されるメッセージのテキスト。この製品から出力されるメッセージテキスト。

統合トレースログに出力されるログの時刻は、出力したプロセスのタイムゾーンでフォーマットされます。

このため、環境変数 TZ を変更したユーザーなどがサービスを起動したり、コマンドを実行したりすると、OS に設定されているタイムゾーンと異なる時刻が出力されることがあります。

(3) 操作ログ

JP1/IM - Manager の操作ログは、不正なアクセスなどセキュリティ上の問題発生時の原因究明や、システムを安全に運用するための情報収集を目的として、「いつ」「だれが」「どこから」「成功・不成功」など

のログイン・ログアウトの情報の履歴を出力するログ情報です。操作ログの詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 K 操作ログの出力」を参照してください。

(4) 個別ログ

初期シークレットおよび IM クライアントシークレットを使用した JP1/IM - Manager の REST API の認証結果について、認証の成功または失敗とその時刻を、次の形式でシークレット認証ログファイルに出力します。初期シークレット、IM クライアントシークレットについてはマニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「3.7 初期シークレットとクライアントシークレット」を参照してください。ファイルの文字コードは UTF-8 (BOM なし)、ファイルの最大サイズは 60MB です。

時刻 メッセージ種別 メッセージ

出力項目	説明
時刻	「yyyy/MM/dd hh:mm:ss.SSS」形式の時刻を出力します。
メッセージ種別	次のどれかのメッセージ種別を出力します。 <ul style="list-style-type: none">• INFO：通知• WARN：警告• ERROR：エラー
メッセージ	次のどれかのメッセージを出力します。 <ul style="list-style-type: none">• KAJY68010-I• KAJY68011-E• KAJY68019-E メッセージの詳細については、マニュアル「JP1/Integrated Management 3 - Manager メッセージ」の「2. メッセージ一覧」を参照してください。

1 行に出力できる文字数は 4,096 バイトまでです。4,096 バイトを超える場合は、折り返して出力します。4,096 バイト目がマルチバイト文字の途中だったときは、その文字から折り返します。

また、シークレット認証ログファイルの出力先は次のとおりです。

Windows の場合

物理ホストのとき：Manager パス¥log¥secretAuth¥jddSecretAuth. log{. 1|2|3}

論理ホストのとき：共有フォルダ¥jp1imm¥log¥secretAuth¥jddSecretAuth. log{. 1|2|3}

UNIX の場合

物理ホストのとき：/var/opt/jp1imm/log/secretAuth/jddSecretAuth. log{. 1|2|3}

論理ホストのとき：共有ディレクトリ/jp1imm/log/secretAuth/jddSecretAuth. log{. 1|2|3}

(5) ログファイルおよびディレクトリー一覧

JP1/IM が出力するログ情報の種類とデフォルトのファイル名およびディレクトリー名について説明します。

なお、ここで説明するファイルは、製品保守の必要上出力しているものです。これらのファイルについては、ユーザーが参照または変更する必要はありません。ただし、システム障害が発生したときなどには、資料採取のためにこれらのファイルをご利用元で一時保管していただくことがあります。

(a) Windows の場合

Windows 版の JP1/IM が出力するデフォルトのログファイルおよびフォルダを次の表に示します。

「ログの種類」には、JP1/IM が出力するログの種類を記載しています。

「デフォルトのファイル名・フォルダ名」には、JP1/IM - Manager, JP1/IM - View, または JP1/Base をデフォルトでインストールした場合のログファイル名を絶対パスで記載しています。また、クラスタ運用の場合の「デフォルトのファイル名・フォルダ名」には、共有フォルダのログファイル名を絶対パスで記載しています。

「最大ディスク使用量」には、ログファイルが最大でどの程度ディスクを使用するのかを記載しています。ログファイルが複数ある場合は、その合計量を記載しています。

「ファイルの切り替え時期」には、JP1/IM が出力先のログファイルを切り替えるタイミングを記載しています。ファイルがこの欄に示すサイズに達したとき、またはこの欄に示す事象が起きたときに、出力先が切り替わります。なお、ログファイルが複数あり、最大ディスク使用量に達した場合は、更新日付の古いファイルから上書きされます。

表 12-3 JP1/IM - Manager (コンポーネント共通) のログファイル・フォルダー一覧 (Windows)

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
操作ログ	Manager パス¥log¥operationlog¥imm_operation{なし 1 2... 16}.log ^{※1}	55 メガバイト ※1	5 メガバイト ^{※1} , ※2
jimnodecount コマンドのログ ^{※3}	Manager パス¥log¥nodecount¥jimnodecount_cmd{1 2}.log	20 メガバイト	10 メガバイト

注※1 マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「操作ログ定義ファイル (imm_operationlog.conf)」(2. 定義ファイル) によって、出力先、保存面数、ファイルサイズを変更できます。最大ディスク使用量とファイルの切り替え時期に記載しているバイト数は、保存面数およびファイルサイズが初期値の場合の値です。

注※2 操作ログのファイル切り替え時の動作については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 K.2 操作ログの保存形式」を参照してください。

注※3 プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

表 12-4 JP1/IM - Manager (セントラルコンソール) のログファイル・フォルダ一覧 (Windows)

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
プロセス管理ログ※9	Console パス¥log¥JCO_SPMD{1 2 3}. log	384 キロバイト	128 キロバイト
	Console パス¥log¥JCO_SPMD_COMMAND{1 2 3}. log	384 キロバイト	128 キロバイト
	共有フォルダ¥jp1cons¥log¥JCO_SPMD{1 2 3}. log	384 キロバイト	128 キロバイト
	共有フォルダ¥jp1cons¥log¥JCO_SPMD_COMMAND{1 2 3}. log	384 キロバイト	128 キロバイト
スタックトレースログ※9	Console パス¥log¥javaLog0{1 2 3 4}. log	1 メガバイト	起動時, または 256 キロバイト
	共有フォルダ¥jp1cons¥log¥javaLog0{1 2 3 4}. log	1 メガバイト	起動時, または 256 キロバイト
論理ホスト設定プログラムログ※9	Console パス¥log¥jp1hassetup. {log log. old}	2,000 キロバイト	1,000 キロバイト
セットアップ時のログ※9	Console パス¥log¥command¥comdef[_old]. log	512 キロバイト	256 キロバイト
イベントコンソールログ※9	Console パス¥log¥console¥EVCONS{1 2 3}. log	30,720 キロバイト	10,240 キロバイト
	Console パス¥log¥console¥jp1cons{1 2 3 4 5 6 7 8}. log	40,960 キロバイト	5,120 キロバイト ※1
	Console パス¥log¥console¥evtcon_exe{1 2 3}. log	256 キロバイト× 3	256 キロバイト
	Console パス¥log¥console¥JCOAPI{1 2 3}. log	96 キロバイト	32 キロバイト
	Console パス¥log¥console¥jp1consM{1 2 ... 60}. log	300 メガバイト	5 メガバイト※1
	Console パス¥log¥console¥jp1eventStormDef{1 2 3 4 5}. log	100 メガバイト	20 メガバイト
	Console パス¥log¥console¥jp1filterDef{1 2 3 4 5}. log	100 メガバイト	20 メガバイト
	Console パス¥log¥console¥jp1bizGroupDef{1 2}. log	10 メガバイト	5 メガバイト
	Console パス¥log¥console¥jp1cmdButtonDef{1 2 3 4 5}. log	25 メガバイト	5 メガバイト
	Console パス¥log¥console¥jp1exattrnameDef{1 2 3 4 5}. log	25 メガバイト	5 メガバイト
	共有フォルダ¥jp1cons¥log¥console¥EVCONS{1 2 3}. log	30,720 キロバイト	10,240 キロバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
	共有フォルダ¥jp1cons¥log¥console¥jp1cons{1 2 3 4 5 6 7 8}. log	40,960 キロバイト	5,120 キロバイト ※1
	共有フォルダ¥jp1cons¥log¥console¥evtcon_exe{1 2 3}. log	256 キロバイト×3	256 キロバイト
	共有フォルダ¥jp1cons¥log¥console¥JCOAPI{1 2 3}. log	96 キロバイト	32 キロバイト
	共有フォルダ¥jp1cons¥log¥console¥jp1consM{1 2 ... 60}. log	300 メガバイト	5 メガバイト ※1
	共有フォルダ ¥jp1cons¥log¥console¥jp1eventStormDef{1 2 3 4 5}. log	100 メガバイト	20 メガバイト
	共有フォルダ ¥jp1cons¥log¥console¥jp1filterDef{1 2 3 4 5}. log	100 メガバイト	20 メガバイト
	共有フォルダ ¥jp1cons¥log¥console¥jp1bizGroupDef{1 2}. log	10 メガバイト	5 メガバイト
	共有フォルダ ¥jp1cons¥log¥console¥jp1cmdButtonDef{1 2 3 4 5}. log	25 メガバイト	5 メガバイト
	共有フォルダ ¥jp1cons¥log¥console¥jp1exattrnameDef{1 2 3 4 5}. log	25 メガバイト	5 メガバイト
自動アクショントレースログ※9	Console パス¥log¥action¥JCAMAIN{1 2 3 4 5}. log	25,600 キロバイト ※2	5,120 キロバイト
	共有フォルダ ¥jp1cons¥log¥action¥JCAMAIN{1 2 3 4 5}. log	25,600 キロバイト ※2	5,120 キロバイト
製品情報のログ※9	Console パス¥log¥hliclib¥hliclibtrc{1 2 3 4 5}. log	5 メガバイト	1 メガバイト
	Console パス¥log¥hliclib¥hlicliberr{1 2 3 4 5}. log	5 メガバイト	1 メガバイト
	Console パス¥log¥hliclib¥hliclibmgrtrc{1 2 3 4 5}. log	5 メガバイト	1 メガバイト
	Console パス¥log¥hliclib¥hliclibmgrerr{1 2 3 4 5}. log	5 メガバイト	1 メガバイト
	共有フォルダ ¥jp1cons¥log¥hliclib¥hliclibtrc{1 2 3 4 5}. log	5 メガバイト	1 メガバイト
	共有フォルダ ¥jp1cons¥log¥hliclib¥hlicliberr{1 2 3 4 5}. log	5 メガバイト	1 メガバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
	共有フォルダ ¥jp1cons¥log¥hliclib¥hliclibmgrtrc{1 2 3 4 5}.log	5 メガバイト	1 メガバイト
	共有フォルダ ¥jp1cons¥log¥hliclib¥hliclibmgrerr{1 2 3 4 5}.log	5 メガバイト	1 メガバイト
アクション情報ファイル※9	Console パス¥log¥action¥actinf.log	626 キロバイト※3	切り替えなし
	共有フォルダ¥jp1cons¥log¥action¥actinf.log	626 キロバイト※3	切り替えなし
アクションホスト名格納ファイル※9	Console パス¥log¥action¥acttxt{1 2}.log	48.9 メガバイト※4	アクション情報ファイルのラップアラウンド時
	共有フォルダ¥jp1cons¥log¥action¥acttxt{1 2}.log	48.9 メガバイト※4	アクション情報ファイルのラップアラウンド時
アクション再実行用ファイル	Console パス¥log¥action¥actreaction	300 メガバイト	サービス起動時
	共有フォルダ¥jp1cons¥log¥action¥actreaction	300 メガバイト	サービス起動時
jcochstat, jcoevtreport コマンドトレースログ※5 ※9	Console パス¥log¥command¥CMD{1 2 3}.log	3,072 キロバイト	1,024 キロバイト
	Console パス¥log¥command¥jp1cons_cmd{1 2}.log	12,288 キロバイト	6,144 キロバイト
	Console パス¥log¥command¥jp1consM_cmd{1 2}.log	12,288 キロバイト	6,144 キロバイト
	Console パス ¥log¥command¥jp1exattrnameDef_cmd{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
プラグインのログ※9	Console パス¥log¥command¥jcoplugin{1 2 3}.log	3 メガバイト	1 メガバイト
通知状態格納ファイル※9	Console パス¥log¥notice¥notice_stat.dat	72 バイト	切り替えなし
	共有フォルダ¥jp1cons¥log¥notice¥notice_stat.dat	72 バイト	切り替えなし
アクション定義バックアップファイル※9	Console パス¥log¥action¥actdefbk.conf	2,048 キロバイト	切り替えなし
	共有フォルダ¥jp1cons¥log¥action¥actdefbk.conf	2,048 キロバイト	切り替えなし
イベント基盤トレースログ※9	Console パス¥log¥evflow¥EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 メガバイト	10 メガバイト
	Console パス¥log¥evflow¥jp1evflowM{1 2 ... 60}.log	300 メガバイト	5 メガバイト
	Console パス¥log¥evflow¥jp1actDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	Console パス¥log¥evflow¥jp1chsevDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
	Console パス¥log¥evflow¥jp1chmsgDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	Console パス¥log¥evflow¥jp1hostmapDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	Console パス¥log¥evflow¥evflow_exe{1 2 3}.log	256 キロバイト×3	256 キロバイト
	共有フォルダ¥jp1cons¥log¥evflow¥EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 メガバイト	10 メガバイト
	共有フォルダ¥jp1cons¥log¥evflow¥jp1evflowM{1 2 ... 60}.log	300 メガバイト	5 メガバイト
	共有フォルダ¥jp1cons¥log¥evflow¥jp1actDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	共有フォルダ¥jp1cons¥log¥evflow¥jp1chsevDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	共有フォルダ¥jp1cons¥log¥evflow¥jp1chmsgDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	共有フォルダ¥jp1cons¥log¥evflow¥jp1hostmapDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	共有フォルダ¥jp1cons¥log¥evflow¥evflow_exe{1 2 3}.log	256 キロバイト×3	256 キロバイト
マッチング情報ファイル※9	Console パス¥log¥evflow¥evflowinf.log	12 バイト	切り替えなし
	共有フォルダ¥jp1cons¥log¥evflow¥evflowinf.log	12 バイト	切り替えなし
イベント基盤エラーログ※9	Console パス¥log¥evflow¥jp1evflow{1 2 3 4 5 6 7 8}.log	40,960 キロバイト	5,120 キロバイト
	共有フォルダ¥jp1cons¥log¥evflow¥jp1evflow{1 2 3 4 5 6 7 8}.log	40,960 キロバイト	5,120 キロバイト
イベント基盤スタックトレース※9	Console パス¥log¥evflow¥javalog0{1 2 3 4}.log	1 メガバイト	起動時, または 256 キロバイト
	共有フォルダ¥jp1cons¥log¥evflow¥javalog0{1 2 3 4}.log	1 メガバイト	起動時, または 256 キロバイト
自動アクションエラーログ※9	Console パス¥log¥action¥jp1act{1 2 3}.log	15,360 キロバイト	5,120 キロバイト
	共有フォルダ¥jp1cons¥log¥action¥jp1act{1 2 3}.log	15,360 キロバイト	5,120 キロバイト
関連イベント発行履歴ファイル	Console パス¥operation¥evgen¥egs_discrim{1 2 3}.log※6	30 メガバイト※6	10 メガバイト※6

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
	共有フォルダ ¥jp1cons¥operation¥evgen¥egs_discrim{1 2 3}.log ※6	30 メガバイト※6	10 メガバイト※6
共通除外履歴ファイル	Console パス¥operation¥comexc lude¥comexc lude{1 2 3 4 5}.log	100 メガバイト	20 メガバイト
	共有フォルダ ¥jp1cons¥operati on¥comexc lude¥comexc lude{1 2 3 4 5}.log	100 メガバイト	20 メガバイト
共通除外条件定義履歴ファイル	Console パス ¥operati on¥comexc lude¥comexc ludeDef{1 2 3 4 5}.log	100 メガバイト	20 メガバイト
	共有フォルダ ¥jp1cons¥operati on¥comexc lude¥comexc ludeDef{1 2 3 4 5}.log	100 メガバイト	20 メガバイト
関連イベント発行トレースログ※9	Console パス¥log¥evgen¥EVGEN{1 2 3}.log	15 メガバイト	5 メガバイト
	Console パス¥log¥evgen¥evgen_exe{1 2 3}.log	256 キロバイト×3	256 キロバイト
	共有フォルダ¥jp1cons¥log¥evgen¥EVGEN{1 2 3}.log	15 メガバイト	5 メガバイト
	共有フォルダ¥jp1cons¥log¥evgen¥evgen_exe{1 2 3}.log	256 キロバイト×3	256 キロバイト
関連イベント発行個別ログ※9	Console パス¥log¥evgen¥jp1egs{1 2}.log	20 メガバイト	10 メガバイト
	Console パス¥log¥evgen¥jp1egsM{1 2}.log	20 メガバイト	10 メガバイト
	共有フォルダ¥jp1cons¥log¥evgen¥jp1egs{1 2}.log	20 メガバイト	10 メガバイト
	共有フォルダ¥jp1cons¥log¥evgen¥jp1egsM{1 2}.log	20 メガバイト	10 メガバイト
関連イベント発行個別ログ(コマンド用)※9	Console パス¥log¥evgen¥jp1egs_cmd{1 2 3 4}.log	20 メガバイト	5 メガバイト
	Console パス¥log¥evgen¥jp1egsM_cmd{1 2 3 4}.log	20 メガバイト	5 メガバイト
関連イベント発行スタックトレースログ※9	Console パス¥log¥evgen¥javalog0{1 2 3 4}.log	1 メガバイト	起動時, または 256 キロバイト
	共有フォルダ¥jp1cons¥log¥evgen¥javalog0{1 2 3 4}.log	1 メガバイト	起動時, または 256 キロバイト
関連イベントの発行処理引き継ぎ定義ファイル※9	Console パス¥log¥evgen¥egs_discrim_info{1 2 3 4}.dat	312 メガバイト※7	停止時
	共有フォルダ ¥jp1cons¥log¥evgen¥egs_discrim_info{1 2 3 4}.dat	312 メガバイト※8	停止時
関連イベント発行定義の適用ログ※9	Console パス¥log¥evgen¥jp1egsDefine{1 2}.log	10 メガバイト	5 メガバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
	共有フォルダ¥jp1cons¥log¥evgen¥jp1legsDefine{1 2}. log	10 メガバイト	5 メガバイト
応答待ちイベント滞留ファイル※8※9	Console パス¥log¥response¥resevent. dat	40 メガバイト	切り替えなし
	共有フォルダ¥jp1cons¥log¥response¥resevent. dat	40 メガバイト	切り替えなし
応答待ちイベント滞留バックアップファイル※9	Console パス¥log¥response¥resevent. dat. dump	40 メガバイト	切り替えなし
	共有フォルダ ¥jp1cons¥log¥response¥resevent. dat. dump	40 メガバイト	切り替えなし
コマンド実行履歴保存フォルダ※9	Base パス¥log¥COMMAND¥	マニュアル「JP1/Base 運用ガイド」を参照してください	
	共有フォルダ¥jp1base¥log¥COMMAND¥		
リモートコマンドログ※9	Base パス¥log¥JCOCMD¥joccmd_result{1 2 3}. log		
	Base パス¥log¥JCOCMD¥joccmdapi{1 2 3}. log		
	Base パス¥log¥JCOCMD¥joccmdapi_trace{1 2 3}. log		
	Base パス¥log¥JCOCMD¥joccmdcom{1 2 3}. log		
	Base パス¥log¥JCOCMD¥joccmdcom_trace{1 2 3}. log		
	Base パス¥log¥JCOCMD¥joccmdexe{1 2 3}. log		
	Base パス¥log¥JCOCMD¥joccmdexe_trace{1 2 3}. log		
	Base パス¥log¥JCOCMD¥joccmdrouter{1 2 3}. log		
	Base パス¥log¥JCOCMD¥joccmdrouter_trace{1 2 3}. log		
	Base パス¥log¥JCOCMD¥JCOCMDCMD{1 2 3}. log		
	共有フォルダ¥jp1base¥log¥JCOCMD¥joccmd_result{1 2 3}. log		
	共有フォルダ¥jp1base¥log¥JCOCMD¥joccmdapi{1 2 3}. log		
	共有フォルダ ¥jp1base¥log¥JCOCMD¥joccmdapi_trace{1 2 3}. log		
	共有フォルダ¥jp1base¥log¥JCOCMD¥joccmdcom{1 2 3}. log		
共有フォルダ ¥jp1base¥log¥JCOCMD¥joccmdcom_trace{1 2 3}. log			
共有フォルダ¥jp1base¥log¥JCOCMD¥joccmdexe{1 2 3}. log			
共有フォルダ ¥jp1base¥log¥JCOCMD¥joccmdexe_trace{1 2 3}. log			

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
	共有フォルダ¥jp1base¥log¥JCOCMD¥joccmdrouter{1 2 3}.log		
	共有フォルダ ¥jp1base¥log¥JCOCMD¥joccmdrouter_trace{1 2 3}.log		
	共有フォルダ¥jp1base¥log¥JCOCMD¥JCOCMDCMD{1 2 3}.log		
構成管理ログ※9	Base パス¥log¥route¥JBSRT{1 2 3}.log		
	共有フォルダ¥jp1base¥log¥route¥JBSRT{1 2 3}.log		
トレースログファイル※9	Base パス ¥sys¥tmp¥event¥logtrap¥jelallog¥jelallog{1 2 3 4 5}.log		
	Base パス ¥sys¥tmp¥event¥logtrap¥jelalelt¥jelalelt{1 2 3 4 5}.log		
統合監視 DB の API ログ ※9	Console パス¥log¥evflow¥EVFLOW_DBAPI{1 2 ... 16}.log	200 メガバイト	12.5 メガバイト
	Console パス¥log¥console¥EVCONS_DBAPI{1 2 3 4 5}.log	50 メガバイト	10 メガバイト
	Console パス¥log¥command¥CMD_DBAPI{1 2 3 4 5}.log	50 メガバイト	10 メガバイト
	共有フォルダ¥jp1cons¥log¥evflow¥EVFLOW_DBAPI{1 2 ... 16}.log	200 メガバイト	12.5 メガバイト
	共有フォルダ¥jp1cons¥log¥console¥EVCONS_DBAPI{1 2 3 4 5}.log	50 メガバイト	10 メガバイト
IM 構成管理 DB の API ログ※9	Console パス¥log¥evflow¥EVFLOW_CFBDBAPI{1 2 3}.log	30 メガバイト	10 メガバイト
	Console パス¥log¥console¥EVCONS_CFBDBAPI{1 2 3}.log	30 メガバイト	10 メガバイト
	Console パス¥log¥command¥CMD_CFBDBAPI{1 2 3}.log	30 メガバイト	10 メガバイト
	共有フォルダ ¥jp1cons¥log¥evflow¥EVFLOW_CFBDBAPI{1 2 3}.log	30 メガバイト	10 メガバイト
	共有フォルダ ¥jp1cons¥log¥console¥EVCONS_CFBDBAPI{1 2 3}.log	30 メガバイト	10 メガバイト
jcodbsetup コマンドの ログ※9	Console パス¥log¥imdb¥jcodbsetup{1 2}.log	512 キロバイト	256 キロバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
jcodbunsetup コマンドのログ※9	Console パス¥log¥imdb¥jcodbunsetup{1 2}.log	512 キロバイト	256 キロバイト
jimmail コマンドのログ※9	Console パス¥log¥mail¥jimmail_cmd{1 2 3}.log	15 メガバイト	5 メガバイト
	Console パス¥log¥mail¥jimmail_cmdM{1 2 3}.log	15 メガバイト	5 メガバイト
	Console パス¥log¥mail¥JIMMAIL{1 2 3}.log	15 メガバイト	5 メガバイト
	Console パス¥log¥mail¥jimmail_exe{1 2 3}.log	15 メガバイト	5 メガバイト
jimmailpasswd コマンドのログ※9	Console パス¥log¥mail¥jimmailpasswd_cmd{1 2 3}.log	768 キロバイト	256 キロバイト
	Console パス¥log¥mail¥jimmailpasswd_cmdM{1 2 3}.log	768 キロバイト	256 キロバイト
	Console パス¥log¥mail¥JIMMAILPASSWD{1 2 3}.log	768 キロバイト	256 キロバイト
	Console パス¥log¥mail¥jimmailpasswd_exe{1 2 3}.log	768 キロバイト	256 キロバイト

注※1 ファイルサイズが、この値より数十キロバイト程度大きくなる場合があります。

注※2 マニュアル「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) によって、65,536~104,857,600 バイト (64 キロバイト~100 メガバイト) の間で設定できます。

注※3 マニュアル「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) によって、1~4,096 キロバイトの間で設定できます。

注※4 アクション情報ファイルの容量がデフォルト (626 キロバイト) の場合の値です。このファイルの最大ディスク占有量は次の見積もり式で算出できます。また、アクションを再実行した場合、一回の再実行ごとに 5 キロバイトずつ増加します。

$((\text{アクション情報ファイルの容量}/64 \text{ バイト}) - 1) \times 5 \text{ キロバイト}$

注※5 クラスタ運用の場合も、物理ホスト上のjcochstat, jcoevtreport コマンドトレースログに出力されます。

注※6 マニュアル「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) によって、ファイル面数、ファイルサイズを変更できます。

注※7 このファイルは関連イベントの発行処理中のデータを引き継ぐときのメモリー情報を書き出したものであるため、関連イベント発行条件や関連元イベントの情報などによってファイルサイズが異なってきます。見積もりの詳細については、JP1/IM - Manager のリリースノートを参照してください。

注※8 応答待ちイベント管理機能を有効にして JP1/IM - Manager を起動した時点で作成されます。

注※9 プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

表 12-5 JP1/IM - Manager (セントラルスコープ) のログファイル・フォルダー一覧 (Windows)

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
セントラルスコープトレースログ	Scope パス¥log¥jcsmain{1 2 3}.log	6 メガバイト	2 メガバイト
	Scope パス¥log¥jcsmain_trace{1 2 3}.log	6 メガバイト	2 メガバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
	共有フォルダ¥JP1Scope¥log¥jcsmain{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ¥JP1Scope¥log¥jcsmain_trace{1 2 3}.log	6 メガバイト	2 メガバイト
通信用トレースログ	Scope パス¥log¥jcsmain_trace_com{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ ¥JP1Scope¥log¥jcsmain_trace_com{1 2 3}.log	6 メガバイト	2 メガバイト
	Scope パス¥log¥jcsmain_trace_ping{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ ¥JP1Scope¥log¥jcsmain_trace_ping{1 2 3}.log	6 メガバイト	2 メガバイト
論理ホスト設定プログラムログ	Scope パス¥log¥jp1hassetup. {log log.old}	2,000 キロバイト	1,000 キロバイト
DB 操作 API トレースログ	Scope パス¥log¥jcsmain_trace_db{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ¥JP1Scope¥log¥jcsmain_trace_db{1 2 3}.log	6 メガバイト	2 メガバイト
jcshostsexport コマンドログ	Scope パス¥log¥jcshostsexport{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ¥JP1Scope¥log¥jcshostsexport{1 2 3}.log	6 メガバイト	2 メガバイト
jcshostsimport コマンドログ	Scope パス¥log¥jcshostsimport{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ¥JP1Scope¥log¥jcshostsimport{1 2 3}.log	6 メガバイト	2 メガバイト
jcscdbsetup コマンドログ	Scope パス¥log¥jcscdbsetup{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ¥JP1Scope¥log¥jcscdbsetup{1 2 3}.log	6 メガバイト	2 メガバイト
jcscostat コマンドログ	Scope パス¥log¥jcscostat{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ¥JP1Scope¥log¥jcscostat{1 2 3}.log	6 メガバイト	2 メガバイト
jcscdbexport コマンドログ	Scope パス¥log¥jcscdbexport{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ¥JP1Scope¥log¥jcscdbexport{1 2 3}.log	6 メガバイト	2 メガバイト
jcscdbimport コマンドログ	Scope パス¥log¥jcscdbimport{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ¥JP1Scope¥log¥jcscdbimport{1 2 3}.log	6 メガバイト	2 メガバイト
jcscdbconvert コマンドログ	Scope パス¥log¥jcscdbconvert{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ¥JP1Scope¥log¥jcscdbconvert{1 2 3}.log	6 メガバイト	2 メガバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
jp1csverup コマンドログ	Scope パス¥log¥jp1csverup_front{1 2 3}.log	6 メガバイト	2 メガバイト
jp1cshaverup コマンドログ	共有フォルダ ¥JP1Scope¥log¥jp1cshaverup_front{1 2 3}.log	6 メガバイト	2 メガバイト

注 プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

表 12-6 JP1/IM - Manager (IM 構成管理) のログファイル・フォルダー一覧 (Windows)

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
IM 構成管理トレースログ	Manager パス¥log¥imcf¥jcfallogtrap{1 2 3 4 5 6 7 8 9 10}.log	200 メガバイト	10 メガバイト
	Manager パス ¥log¥imcf¥jcfallogtrap_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	Manager パス ¥log¥imcf¥jcfallogtrap_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	Manager パス¥log¥imcf¥jcfmain{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	Manager パス¥log¥imcf¥jcfmain_trace{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	Manager パス¥log¥imcf¥jcfmain_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfallogtrap{1 2 3 4 5 6 7 8 9 10}.log	200 メガバイト	10 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfallogtrap_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfallogtrap_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfmain{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfmain_trace{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfmain_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク 使用量	ファイルの切り替 え時期
通信用トレースログ	Manager パス¥log¥imcf¥jcfmain_trace_com{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	Manager パス¥log¥imcf¥jcfmain_ping{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfmain_trace_com{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfmain_ping{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
認証用トレースログ	Manager パス¥log¥imcf¥jcfmain_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfmain_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
論理ホスト設定プログラムログ	Manager パス¥log¥imcf¥jp1hassetup.{log log.old}	2,000 キロバ イト	1,000 キロバ イト
DB 操作 API トレースログ	Manager パス¥log¥imcf¥jcfmain_trace_db{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfmain_trace_db{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
コマンド共通ログ	Manager パス¥log¥imcf¥jcfcommand{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfcommand{1 2 3}.log	3 メガバイト	1 メガバイト
jcfallogstart コマンドログ	Manager パス¥log¥imcf¥jcfallogstart{1 2 3}.log	9 メガバイト	3 メガバイト
	Manager パス ¥log¥imcf¥jcfallogstart_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfallogstart{1 2 3}.log	9 メガバイト	3 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfallogstart_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfallogstat コマンドログ	Manager パス¥log¥imcf¥jcfallogstat{1 2 3}.log	9 メガバイト	3 メガバイト
	Manager パス ¥log¥imcf¥jcfallogstat_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク 使用量	ファイルの切り替 え時期
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfallogstat{1 2 3}.log	9 メガバイト	3 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfallogstat_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfallogstop コマンドログ	Manager パス¥log¥imcf¥jcfallogstop{1 2 3}.log	9 メガバイト	3 メガバイト
	Manager パス ¥log¥imcf¥jcfallogstop_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfallogstop{1 2 3}.log	9 メガバイト	3 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfallogstop_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfallogreload コマンドログ	Manager パス¥log¥imcf¥jcfallogreload{1 2 3}.log	9 メガバイト	3 メガバイト
	Manager パス ¥log¥imcf¥jcfallogreload_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfallogreload{1 2 3}.log	9 メガバイト	3 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfallogreload_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfallogdef コマンドログ	Manager パス¥log¥imcf¥jcfallogdef{1 2 3}.log	9 メガバイト	3 メガバイト
	Manager パス ¥log¥imcf¥jcfallogdef_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfallogdef{1 2 3}.log	9 メガバイト	3 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfallogdef_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfaleltstart コマンドログ	Manager パス¥log¥imcf¥jcfaleltstart{1 2 3}.log	6 メガバイト	2 メガバイト
	Manager パス ¥log¥imcf¥jcfaleltstart_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfaleltstart{1 2 3}.log	6 メガバイト	2 メガバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク 使用量	ファイルの切り替 え時期
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfaletstart_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfaletstat コマンドログ	Manager パス¥log¥imcf¥jcfaletstat{1 2 3}.log	6 メガバイト	2 メガバイト
	Manager パス ¥log¥imcf¥jcfaletstat_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfaletstat{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfaletstat_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfaletstop コマンドログ	Manager パス¥log¥imcf¥jcfaletstop{1 2 3}.log	6 メガバイト	2 メガバイト
	Manager パス ¥log¥imcf¥jcfaletstop_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfaletstop{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfaletstop_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfaletreload コマンドログ	Manager パス¥log¥imcf¥jcfaletreload{1 2 3}.log	6 メガバイト	2 メガバイト
	Manager パス ¥log¥imcf¥jcfaletreload_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfaletreload{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfaletreload_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfaletdef コマンドログ	Manager パス¥log¥imcf¥jcfaletdef{1 2 3}.log	6 メガバイト	2 メガバイト
	Manager パス ¥log¥imcf¥jcfaletdef_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ¥JP1IMM¥log¥imcf¥jcfaletdef{1 2 3}.log	6 メガバイト	2 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfaletdef_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク 使用量	ファイルの切り替 え時期
jcfcolvmesx コマンドログ	Manager パス¥log¥imcf¥jcfcolvmesx_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfcolvmscvmm コマンドログ	Manager パス¥log¥imcf¥jcfcolvmscvmm_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfcolvvirtage コマンドログ	Manager パス ¥log¥imcf¥jcfcolvvirtage_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfcolvsvc コマンドログ	Manager パス¥log¥imcf¥jcfcolvsvc_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfcolvkvm コマンドログ	Manager パス¥log¥imcf¥jcfcolvkvm_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfcolvhcsn コマンドログ	Manager パス¥log¥imcf¥jcfcolvhcsn_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfexport コマンドログ	Manager パス¥log¥imcf¥jcfexport_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfexport_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfimport コマンドログ	Manager パス¥log¥imcf¥jcfimport_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有フォルダ ¥JP1IMM¥log¥imcf¥jcfimport_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfmkhostsdata コマンドログ	Manager パス ¥log¥imcf¥jcfmkhostsdata_trace{1 2 3}.log	3 メガバイト	1 メガバイト
スタックトレースログ	Manager パス¥log¥imcf¥javalog{1 2 3 4}.log	1 メガバイト	起動時, または 256 キロバイト

注 プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

表 12-7 インテリジェント統合管理基盤のログファイル・フォルダ一覧

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク 使用量	ファイルの切り替 え時期
インテリジェント統合管理基盤サービス個別ログ	Manager パス¥log¥imdd¥jddmain¥jddmain.log{.1-7}	1 ギガバイト	128 メガバイト
	共有フォルダ¥jp1imm¥log¥imdd¥jddmain¥jddmain.log{.1-7}		
定義ファイル※1・ノード ファイル履歴ログ	Manager パス¥log¥imdd¥jddmain¥jimddDef.log{.1-10}	80 メガ バイト	8 メガバイト
	共有フォルダ¥jp1imm¥log¥imdd¥jddmain¥jimddDef.log{.1-10}		

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク 使用量	ファイルの切り 替え時期
	Manager パス¥log¥imdd¥jddmain¥jimddMaster. log{.1-30}	240 メガバ イト	8 メガバイト
	共有フォルダ ¥jplimm¥log¥imdd¥jddmain¥jimddMaster. log{.1-30}		
jddsetaccessuser コマ ンドトレースログ	Manager パス ¥log¥imdd¥jddsetaccessuser¥jddsetaccessuser. log{.1-6}	70 メガバ イト	10 メガバイト
	共有フォルダ ¥jplimm¥log¥imdd¥jddsetaccessuser¥jddsetaccessuser. log{ .1-6}		
	Manager パス ¥log¥imdd¥jddsetaccessuser¥jddsetaccessuser_exe{1 2 3}. log	768 キロバ イト	256 キロバイト
	共有フォルダ ¥jplimm¥log¥imdd¥jddsetaccessuser¥jddsetaccessuser_exe{ 1 2 3}. log		
	Manager パス¥log¥imdd¥jddsetaccessuser¥javalog0{1 2 3 4}. log	1,024 キロ バイト	起動時または 256 キロバイト
	共有フォルダ ¥jplimm¥log¥imdd¥jddsetaccessuser¥javalog0{1 2 3 4}. log		
jddcreatetree コマンド トレースログ	Manager パス ¥log¥imdd¥jddcreatetree¥jddcreatetree. log{.1-6}	70 メガバ イト	10 メガバイト
	共有フォルダ ¥jplimm¥log¥imdd¥jddcreatetree¥jddcreatetree. log{.1-6}		
	Manager パス ¥log¥imdd¥jddcreatetree¥jddcreatetree_exe{1 2 3}. log	768 キロバ イト	256 キロバイト
	共有フォルダ ¥jplimm¥log¥imdd¥jddcreatetree¥jddcreatetree_exe{1 2 3}. log		
	Manager パス¥imdd¥jddcreatetree¥javalog0{1 2 3 4}. log	1,024 キロ バイト	起動時または 256 キロバイト
	共有フォルダ¥jplimm¥log¥imdd¥jddcreatetree¥javalog0{1 2 3 4}. log		
jddupdatetree コマンド トレースログ	Manager パス ¥log¥imdd¥jddupdatetree¥jddupdatetree. log{.1-6}	70 メガバ イト	10 メガバイト
	共有フォルダ ¥jplimm¥log¥imdd¥jddupdatetree¥jddupdatetree. log{.1-6}		
	Manager パス ¥log¥imdd¥jddupdatetree¥jddupdatetree_exe{1 2 3}. log	768 キロバ イト	256 キロバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク 使用量	ファイルの切り 替え時期
	共有フォルダ ¥jplimm¥log¥imdd¥jddupdatetree¥jddupdatetree_exe{1 2 3}.log		
	Manager パス¥log¥imdd¥jddupdatetree¥javalog0{1 2 3 4}.log	1,024 キロ バイト	256 キロバイト
	共有フォルダ¥jplimm¥log¥imdd¥jddupdatetree¥javalog0{1 2 3 4}.log		
jddsetproxyuser コマンド トレースログ	Manager パス ¥log¥imdd¥jddsetproxyuser¥jddsetproxyuser.log{.1-6}	70 メガバ イト	10 メガバイト
	共有フォルダ ¥jplimm¥log¥imdd¥jddsetproxyuser¥jddsetproxyuser.log{.1-6}		
	Manager パス ¥log¥imdd¥jddsetproxyuser¥jddsetproxyuser_exe{1 2 3}.log	768 キロバ イト	256 キロバイト
	共有フォルダ ¥log¥imdd¥jddsetproxyuser¥jddsetproxyuser_exe{1 2 3}.log		
	Manager パス¥log¥imdd¥jddsetproxyuser¥javalog0{1 2 3 4}.log	1,024 キロ バイト	256 キロバイト
	共有フォルダ¥log¥imdd¥jddsetproxyuser¥javalog0{1 2 3 4}.log		
jddupdatesuggestion コ マンドトレースログ	Manager パス ¥log¥imdd¥jddupdatesuggestion¥jddupdatesuggestion.log{.1-6}	70 メガバ イト	10 メガバイト
	共有フォルダ ¥jplimm¥log¥jddupdatesuggestion¥jddupdatesuggestion.log{.1-6}		
	Manager パス ¥log¥imdd¥jddupdatesuggestion¥jddupdatesuggestion_exe{1 2 3}.log	768 キロバ イト	256 キロバイト
	共有フォルダ ¥log¥imdd¥jddupdatesuggestion¥jddupdatesuggestion_exe{1 2 3}.log		
	Manager パス¥log¥imdd¥jddupdatesuggestion¥javalog0{1 2 3 4}.log	1,024 キロ バイト	256 キロバイト
	共有フォルダ¥log¥imdd¥jddupdatesuggestion¥javalog0{1 2 3 4}.log		

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク 使用量	ファイルの切り 替え時期
jddsetopinfo コマンド トレースログ	Manager パス ¥log¥imdd¥jddsetopinfo¥jddsetopinfo.log{.1-6}	70 メガバ イト	10 メガバイト
	共有フォルダ ¥jplimm¥log¥jddsetopinfo¥jddsetopinfo.log{.1-6}		
	Manager パス¥log¥imdd¥jddsetopinfo¥jddsetopinfo_exe{1 2 3}.log	768 キロバ イト	256 キロバ イト
	共有フォルダ¥log¥imdd¥jddsetopinfo¥jddsetopinfo_exe{1 2 3}.log		
	Manager パス¥log¥imdd¥jddsetopinfo¥javalog0{1 2 3 4}.log	1,024 キロ バイト	256 キロバ イト
	共有フォルダ¥log¥imdd¥jddsetopinfo¥javalog0{1 2 3 4}.log		
jddupdatessomap コマン ドトレースログ	Manager パス ¥log¥imdd¥jddupdatessomap¥jddupdatessomap.log{.1-6}	70 メガバ イト	10 メガバイト
	共有フォルダ ¥jplimm¥log¥jddupdatessomap¥jddupdatessomap.log{.1-6}		
	Manager パス ¥log¥imdd¥jddupdatessomap¥jddupdatessomap_exe{1 2 3}.log	768 キロバ イト	256 キロバ イト
	共有フォルダ ¥log¥imdd¥jddupdatessomap¥jddupdatessomap_exe{1 2 3}.log		
	Manager パス¥log¥imdd¥jddupdatessomap¥javalog0{1 2 3 4}.log	1,024 キロ バイト	256 キロバ イト
	共有フォルダ¥log¥imdd¥jddupdatessomap¥javalog0{1 2 3 4}.log		
jimgndbsetup コマンド トレースログ	Manager パス¥log¥imgndb¥jimgndbsetup{1 2}.log	512 キロバ イト	256 キロバ イト
jimgndbunsetup コマン ドトレースログ	Manager パス¥log¥imgndb¥jimgndbunsetup{1 2}.log	512 キロバ イト	256 キロバ イト
jimgndbstop コマンド トレースログ	Manager パス¥log¥imgndb¥jimgndbstop{1-10}.log	51,200 キロ バイト	5,120 キロバ イト
	共有フォルダ¥jplimm¥log¥imgndb¥jimgndbstop{1-10}.log		
jimgndbstatus コマン ドトレースログ	Manager パス¥log¥imgndb¥jimgndbstatus{1-10}.log	51,200 キロ バイト	5,120 キロバ イト
	共有フォルダ¥jplimm¥log¥imgndb¥jimgndbstatus{1-10}.log		
対処アクション実行履歴 ファイルのログ※4	Manager パス ¥log¥suggestion¥jddSuggestionHistory.log{.1-3}	240 メガバ イト	60 メガバイト
	共有フォルダ ¥jplimm¥log¥suggestion¥jddSuggestionHistory.log{.1-3}		

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク 使用量	ファイルの切り 替え時期
シークレット認証ログ ファイル	Manager パス¥log¥secretAuth¥jddSecretAuth. log{.1-3}	240 メガバ イト	60 メガバイト
	共有フォルダ ¥jplimm¥log¥secretAuth¥jddSecretAuth. log{.1-3}		
ユーザー作成プラグイン	Manager パス¥log¥imdd¥ユーザー作成プラグイン名¥ユーザー 作成プラグイン. log{1-21}¥3	220 メガバ イト	10 メガバイト
	共有フォルダ¥JP1IMM¥log¥imdd¥ユーザー作成プラグイン名 ¥ユーザー作成プラグイン. log{1-21}¥3		
その他ログ	Manager パス¥log¥imdd¥jddmain¥jddmain_exe{1 2 3}. log	768 キロバ イト	256 キロバイト
	共有フォルダ¥jplimm¥log¥imdd¥jddmain¥jddmain_exe{1 2 3}. log		
	Manager パス¥log¥imdd¥jddmain¥javalog0{1 2 3 4}. log	1,024 キロ バイト	起動時または 256 キロバイト
	共有フォルダ¥jplimm¥log¥imdd¥jddmain¥javalog0{1 2 3 4}. log		
	Manager パス¥log¥imdd¥jcoapi{1-50}. log	500 メガバ イト	10 メガバイト
	共有フォルダ¥jplimm¥log¥imdd¥jddmain¥jcoapi{1-50}. log		
	Manager パス¥log¥imdd¥jcoapiM{1-50}. log	500 メガバ イト	10 メガバイト
	共有フォルダ¥jplimm¥log¥imdd¥jddmain¥jcoapiM{1-50}. log		
	Manager パス¥log¥imdd¥コンポーネント名¥コンポーネン ト名¥2{1-21}. log	220 メガバ イト	10 メガバイト
	共有フォルダ¥log¥imdd¥コンポーネント名¥コンポーネン ト名¥2{1-21}. log		

注 プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

注※1 インテリジェント統合管理基盤の定義ファイルログでは、次の定義ファイルのログを出力します。

システムノード定義ファイル、IM 管理ノードカテゴリ名称定義ファイル、ホスト名定義ファイル、構成取得対象ホスト定義ファイル、IM 管理ノードリンク定義ファイル、IM 管理ノードリンクファイル、IM 管理ノードツリーファイル、IM 管理ノードファイル

注※2 コンポーネント名には、次のどれかが表示されます。

- jplajs
- jplpfm
- jplim

注※3 {1-21}はファイルの面数です。ログファイルは任意のテキストエディターで参照できます。

注※4 対処アクションを実行した際のログです。失敗した場合の調査など、対処アクションのログをユーザー自身で確認できます。

表 12-8 JP1/IM - View のログファイル・フォルダー一覧

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
JP1/IM - View ログ※1	View パス¥log¥VIEW{1 2 3}. log	30,720 キロバイト	10,240 キロバイト
	View パス¥log¥jp1conv{1 2 3 4}. log	20,480 キロバイト	5,120 キロバイト※2
	View パス¥log¥jp1convM{1 2・・・ 60}. log	102,400 キロバイト	5,120 キロバイト※2
	View パス¥log¥jp1csov[_old]. log	6,144 キロバイト	3,072 キロバイト※2
	View パス¥log¥jp1csovM[_old]. log	6,144 キロバイト	3,072 キロバイト※2
スタックトレースログ※1	View パス¥log¥javalog0{1 2}. log	512 キロバイト	起動時, または 256 キロバイト
統合トレースログ	システムドライブ:¥Program Files¥Hi tachi¥HNTRLlib2¥spool¥hnr2{1 2 3 4}. log	1,024 キロバイト	256 キロバイト
製品情報のログ※1	View パス¥log¥hliclib¥hliclibtrc{1 2 3 4 5}. log	5 メガバイト	1 メガバイト
	View パス¥log¥hliclib¥hlicliberr{1 2 3 4 5}. log	5 メガバイト	1 メガバイト
	View パス¥log¥hliclib¥hliclibmgrtrc{1 2 3 4 5}. log	5 メガバイト	1 メガバイト
	View パス¥log¥hliclib¥hliclibmgrerr{1 2 3 4 5}. log	5 メガバイト	1 メガバイト

注 Windows の場合は「View パス¥log¥」を「システムドライブ:¥ProgramData¥Hi tachi¥jp1¥jp1_default¥JP1CoView¥log¥」に置き換えてください。

注※1 プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

注※2 ファイルサイズが、この値より数十キロバイト程度大きくなる場合があります。

表 12-9 JP1/IM - IM 構成管理・ビューアーのログファイル・フォルダー一覧

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
IM 構成管理トレースログ※	View パス¥log¥jcfview¥VIEW{1 2 3}. log	30 メガバイト	10 メガバイト
スタックトレースログ※	View パス¥log¥jcfjavalog{1 2}. log	512 キロバイト	起動時, または 256 キロバイト
統合トレースログ	システムドライブ:¥Program Files¥Hi tachi¥HNTRLlib2¥spool¥hnr2{1 2 3 4}. log	1,024 キロバイト	256 キロバイト

注 Windows の場合は「View パス¥log¥」を「システムドライブ:¥ProgramData¥Hi tachi¥jp1¥jp1_default¥JP1CoView¥log¥」に置き換えてください。

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※ プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

(b) UNIX の場合

UNIX 版の JP1/IM が出力するデフォルトのログファイルおよびディレクトリを次の表に示します。

「ログの種類」には、JP1/IM が出力するログの種類を記載しています。

「デフォルトのファイル名・ディレクトリ名」には、JP1/IM - Manager または JP1/Base をデフォルトでインストールした場合のログファイル名を絶対パスで記載しています。また、クラスタ運用の場合の「デフォルトのファイル名・ディレクトリ名」には、共有ディレクトリのログファイル名を絶対パスで記載しています。

「最大ディスク使用量」には、ログファイルが最大でどの程度ディスクを使用するのかを記載しています。ログファイルが複数ある場合は、その合計量を記載しています。

「ファイルの切り替え時期」には、JP1/IM が出力先のログファイルを切り替えるタイミングを記載しています。ファイルがこの欄に示すサイズに達したとき、またはこの欄に示す事象が起きたときに、出力先が切り替わります。なお、ログファイルが複数あり、最大ディスク使用量に達した場合は、更新日付の古いファイルから上書きされます。

表 12-10 JP1/IM - Manager (コンポーネント共通) のログファイル・フォルダー一覧 (UNIX)

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
操作ログ	/var/opt/jp1imm/log/operationlog/imm_operation{なし 1 2... 16}.log ^{※1}	55 メガバイト ※1	5 メガバイト ^{※1} , ※2
jimnodecount コマンドのログ ^{※3}	/var/opt/jp1imm/log/nodecount/jimnodecount_cmd{1 2}.log	20 メガバイト	10 メガバイト

注※1 マニュアル「JP1/Integrated Management 3 - Manager コマンド・定義ファイル・API リファレンス」の「操作ログ定義ファイル (imm_operationlog.conf)」(2. 定義ファイル) によって、出力先、保存面数、ファイルサイズを変更できます。最大ディスク使用量とファイルの切り替え時期に記載しているバイト数は、保存面数およびファイルサイズが初期値の場合の値です。

注※2 操作ログのファイル切り替え時の動作については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 K.2 操作ログの保存形式」を参照してください。

注※3 プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

表 12-11 JP1/IM - Manager (セントラルコンソール) のログファイル・ディレクトリ一覧 (UNIX)

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク使用量	ファイルの切り替え時期
プロセス管理ログ※1	/var/opt/jp1cons/log/JCO_SPMD{1 2 3}.log	384 キロバイト	128 キロバイト
	/var/opt/jp1cons/log/JCO_SPMD_COMMAND{1 2 3}.log	384 キロバイト	128 キロバイト
	共有ディレクトリ/jp1cons/log/JCO_SPMD{1 2 3}.log	384 キロバイト	128 キロバイト
	共有ディレクトリ/jp1cons/log/JCO_SPMD_COMMAND{1 2 3}.log	384 キロバイト	128 キロバイト
スタックトレースログ※1	/var/opt/jp1cons/log/javalog0{1 2 3 4}.log	1 メガバイト	起動時, または 256 キロバイト
	共有ディレクトリ/jp1cons/log/javalog0{1 2 3 4}.log	1 メガバイト	起動時, または 256 キロバイト
JP1/IM 起動時ログ※1	/var/opt/jp1cons/log/jco_start.log[.old]	1 キロバイト	起動時
	共有ディレクトリ/jp1cons/log/jco_start_論理ホスト名.log[.old]	1 キロバイト	起動時
JP1/IM 強制終了時のログ ※1, ※2	共有ディレクトリ/jp1cons/log/ jco_killall.cluster{なし 1 2 3 4}	2 キロバイト	jco_killall.cluster コマンド実行時
セットアップ時のログ※1	/var/opt/jp1cons/log/JCO_SETUP/jco_setup.log	100 キロバイト	インストール時
	/var/opt/jp1cons/log/JCO_SETUP/jco_inst.log	100 キロバイト	インストール時
	/var/opt/jp1cons/log/jco_setup/論理ホスト名/ jco_setup.log	100 キロバイト	インストール時
	/var/opt/jp1cons/log/jco_setup/論理ホスト名/ reg.txt	100 キロバイト	インストール時
	/var/opt/jp1cons/log/jco_setup/論理ホスト名/ reg_def.txt	100 キロバイト	インストール時
	/var/opt/jp1cons/log/command/comdef[_old].log	512 キロバイト	256 キロバイト
イベントコンソールログ※1	/var/opt/jp1cons/log/console/EVCONS{1 2 3}.log	30,720 キロバイト	10,240 キロバイト
	/var/opt/jp1cons/log/console/jp1cons{1 2 3 4 5 6 7 8}.log	40,960 キロバイト	5,120 キロバイト ※3
	/var/opt/jp1cons/log/console/JCOAPI{1 2 3}.log	96 キロバイト	32 キロバイト
	/var/opt/jp1cons/log/console/jp1consM{1 2 ... 60}.log	300 メガバイト	5 メガバイト※3
	/var/opt/jp1cons/log/console/jp1eventStormDef{1 2 3 4 5}.log	100 メガバイト	20 メガバイト

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク使用量	ファイルの切り替え時期
	/var/opt/jp1cons/log/console/jp1filterDef{1 2 3 4 5}.log	100 メガバイト	20 メガバイト
	/var/opt/jp1cons/log/console/jp1bizGroupDef{1 2}.log	10 メガバイト	5 メガバイト
	/var/opt/jp1cons/log/console/evtcon_exe{1 2 3}.log	256 キロバイト ×3	256 キロバイト
	/var/opt/jp1cons/log/console/jp1cmdButtonDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	/var/opt/jp1cons/log/console/jp1exattrnameDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	共有ディレクトリ/jp1cons/log/console/EVCONS{1 2 3}.log	30,720 キロバイト	10,240 キロバイト
	共有ディレクトリ/jp1cons/log/console/jp1cons{1 2 3 4 5 6 7 8}.log	40,960 キロバイト	5,120 キロバイト ※3
	共有ディレクトリ/jp1cons/log/console/JCOAPI{1 2 3}.log	96 キロバイト	32 キロバイト
	共有ディレクトリ/jp1cons/log/console/jp1consM{1 2 ... 60}.log	300 メガバイト	5 メガバイト※3
	共有ディレクトリ/jp1cons/log/console/jp1eventStormDef{1 2 3 4 5}.log	100 メガバイト	20 メガバイト
	共有ディレクトリ/jp1cons/log/console/jp1filterDef{1 2 3 4 5}.log	100 メガバイト	20 メガバイト
	共有ディレクトリ/jp1cons/log/console/jp1bizGroupDef{1 2}.log	10 メガバイト	5 メガバイト
	共有ディレクトリ/jp1cons/log/console/evtcon_exe{1 2 3}.log	256 キロバイト ×3	256 キロバイト
	共有ディレクトリ/jp1cons/log/console/jp1cmdButtonDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	共有ディレクトリ/jp1cons/log/console/jp1exattrnameDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
自動アクショントレース ログ※1	/var/opt/jp1cons/log/action/JCAMAIN{1 2 3 4 5}.log※4	25,600 キロバイト	5,120 キロバイト
	共有ディレクトリ/jp1cons/log/action/JCAMAIN{1 2 3 4 5}.log※4	25,600 キロバイト	5,120 キロバイト
アクション情報ファイル※1	/var/opt/jp1cons/log/action/actinf.log	626 キロバイト ※5	切り替えなし

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク使用量	ファイルの切り替え時期
	共有ディレクトリ/jp1cons/log/action/actinf.log	626 キロバイト ※5	切り替えなし
アクションホスト名格納ファイル※1	/var/opt/jp1cons/log/action/acttxt{1 2}.log	48.9 メガバイト ※6	アクション情報ファイルのラップアラウンド時
	共有ディレクトリ/jp1cons/log/action/acttxt{1 2}.log	48.9 メガバイト ※6	アクション情報ファイルのラップアラウンド時
アクション再実行用ファイル	/var/opt/jp1cons/log/action/actreaction	300 メガバイト	サービス起動時
	共有ディレクトリ/jp1cons/log/action/actreaction	300 メガバイト	サービス起動時
jcochafmode, jcochstat, jcoevtreport コマンドトレースログ※1, ※7	/var/opt/jp1cons/log/command/CMD{1 2 3}.log	3,072 キロバイト	1,024 キロバイト
	/var/opt/jp1cons/log/command/jp1cons_cmd{1 2}.log	12,288 キロバイト	6,144 キロバイト
	/var/opt/jp1cons/log/command/jp1consM_cmd{1 2}.log	12,288 キロバイト	6,144 キロバイト
	/var/opt/jp1cons/log/command/jp1exattrnameDef_cmd{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
プラグインのログ※1	/var/opt/jp1cons/log/command/jcoplugin{1 2 3}.log	3 メガバイト	1 メガバイト
通知状態格納ファイル※1	/var/opt/jp1cons/log/notice/notice_stat.dat	72 バイト	切り替えなし
	共有ディレクトリ/jp1cons/log/notice/notice_stat.dat	72 バイト	切り替えなし
アクション定義バックアップファイル※1	/var/opt/jp1cons/log/action/actdefbk.conf	2,048 キロバイト	切り替えなし
	共有ディレクトリ/jp1cons/log/action/actdefbk.conf	2,048 キロバイト	切り替えなし
イベント基盤トレースログ※1	/var/opt/jp1cons/log/evflow/EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 メガバイト	10 メガバイト
	/var/opt/jp1cons/log/evflow/jp1evflowM{1 2 ... 60}.log	300 メガバイト	5 メガバイト
	/var/opt/jp1cons/log/evflow/jp1actDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	/var/opt/jp1cons/log/evflow/jp1chsevDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	/var/opt/jp1cons/log/evflow/jp1chmsgDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク使用量	ファイルの切り替え時期
	/var/opt/jp1cons/log/evflow/jp1hostmapDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	/var/opt/jp1cons/log/evflow/evflow_exe{1 2 3}.log	256 キロバイト ×3	256 キロバイト
	共有ディレクトリ/jp1cons/log/evflow/EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 メガバイト	10 メガバイト
	共有ディレクトリ/jp1cons/log/evflow/jp1evflowM{1 2 ... 60}.log	300 メガバイト	5 メガバイト
	共有ディレクトリ/jp1cons/log/evflow/jp1actDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	共有ディレクトリ/jp1cons/log/evflow/jp1chsevDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	共有ディレクトリ/jp1cons/log/evflow/jp1chmsgDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	共有ディレクトリ/jp1cons/log/evflow/jp1hostmapDef{1 2 3 4 5}.log	25 メガバイト	5 メガバイト
	共有ディレクトリ/jp1cons/log/evflow/evflow_exe{1 2 3}.log	256 キロバイト ×3	256 キロバイト
マッチング情報ファイル※1	/var/opt/jp1cons/log/evflow/evflowinf.log	12 バイト	切り替えなし
	共有ディレクトリ/jp1cons/log/evflow/evflowinf.log	12 バイト	切り替えなし
イベント基盤エラーログ※1	/var/opt/jp1cons/log/evflow/jp1evflow{1 2 3 4 5 6 7 8}.log	40,960 キロバイト	5,120 キロバイト
	共有ディレクトリ/jp1cons/log/evflow/jp1evflow{1 2 3 4 5 6 7 8}.log	40,960 キロバイト	5,120 キロバイト
自動アクションエラーログ※1	/var/opt/jp1cons/log/action/jp1act{1 2 3}.log	15,360 キロバイト	5,120 キロバイト
	共有ディレクトリ/jp1cons/log/action/jp1act{1 2 3}.log	15,360 キロバイト	5,120 キロバイト
関連イベント発行履歴ファイル	/var/opt/jp1cons/operation/evgen/egs_discrim{1 2 3}.log※8	30 メガバイト※8	10 メガバイト※8
	共有ディレクトリ/jp1cons/operation/evgen/egs_discrim{1 2 3}.log※8	30 メガバイト※8	10 メガバイト※8
共通除外履歴ファイル	/var/opt/jp1cons/operation/comexclude/comexclude{1 2 3 4 5}.log	100 メガバイト	20 メガバイト
	共有ディレクトリ/jp1cons/operation/comexclude/comexclude{1 2 3 4 5}.log	100 メガバイト	20 メガバイト

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク使用量	ファイルの切り替え時期
共通除外条件定義履歴ファイル	/var/opt/jp1cons/operation%comexclude/comexcludeDef{1 2 3 4 5}.log	100 メガバイト	20 メガバイト
	共有ディレクトリ/jp1cons/operation/comexclude/comexcludeDef{1 2 3 4 5}.log	100 メガバイト	20 メガバイト
関連イベント発行トレースログ※1	/var/opt/jp1cons/log/evgen/EVGEN{1 2 3}.log	15 メガバイト	5 メガバイト
	/var/opt/jp1cons/log/evgen/evgen_exe{1 2 3}.log	256 キロバイト ×3	256 キロバイト
	共有ディレクトリ/jp1cons/log/evgen/EVGEN{1 2 3}.log	15 メガバイト	5 メガバイト
	共有ディレクトリ/jp1cons/log/evgen/evgen_exe{1 2 3}.log	256 キロバイト ×3	256 キロバイト
関連イベント発行個別ログ (関連イベント発行サービス用) ※1	/var/opt/jp1cons/log/evgen/jp1legs{1 2}.log	20 メガバイト	10 メガバイト
	/var/opt/jp1cons/log/evgen/jp1legsM{1 2}.log	20 メガバイト	10 メガバイト
	共有ディレクトリ/jp1cons/log/evgen/jp1legs{1 2}.log	20 メガバイト	10 メガバイト
	共有ディレクトリ/jp1cons/log/evgen/jp1legsM{1 2}.log	20 メガバイト	10 メガバイト
関連イベント発行個別ログ (コマンド用) ※1	/var/opt/jp1cons/log/evgen/jp1legs_cmd{1 2 3 4}.log	20 メガバイト	5 メガバイト
	/var/opt/jp1cons/log/evgen/jp1legsM_cmd{1 2 3 4}.log	20 メガバイト	5 メガバイト
関連イベント発行スタック トレースログ※1	/var/opt/jp1cons/log/evgen/javalog0{1 2 3 4}.log	1 メガバイト	起動時, または 256 キロバイト
	共有ディレクトリ/jp1cons/log/evgen/javalog0{1 2 3 4}.log	1 メガバイト	起動時, または 256 キロバイト
関連イベントの発行処理引き継ぎ定義ファイル※1	/var/opt/jp1cons/log/evgen/egs_discrim_info{1 2 3 4}.dat	312 メガバイト ※9	停止時
	共有ディレクトリ/jp1cons/log/evgen/egs_discrim_info{1 2 3 4}.dat	312 メガバイト ※9	停止時
関連イベント発行定義の適用ログ※1	/var/opt/jp1cons/log/evgen/jp1legsDefine{1 2}.log	10 メガバイト	5 メガバイト
	共有ディレクトリ/jp1cons/log/evgen/jp1legsDefine{1 2}.log	10 メガバイト	5 メガバイト
応答待ちイベント滞留ファイル※1, ※10	/var/opt/jp1cons/log/response/resevent.dat	40 メガバイト	切り替えなし
	共有ディレクトリ/jp1cons/log/response/resevent.dat	40 メガバイト	切り替えなし
応答待ちイベント滞留バックアップファイル※1, ※10	/var/opt/jp1cons/log/response/resevent.dat.dump	40 メガバイト	切り替えなし

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク使用量	ファイルの切り替え時期
	共有ディレクトリ/jp1cons/log/response/resevent.dat.dump	40 メガバイト	切り替えなし
統合監視 DB の API ログ※ 1	/var/opt/jp1cons/log/evflow/EVFLOW_DBAPI{1 2 3 4 5}.log	200 メガバイト	12.5 メガバイト
	/var/opt/jp1cons/log/console/EVCONS_DBAPI{1 2 3 4 5}.log	50 メガバイト	10 メガバイト
	/var/opt/jp1cons/log/command/CMD_DBAPI{1 2 3 4 5}.log	50 メガバイト	10 メガバイト
	共有ディレクトリ/jp1cons/log/evflow/EVFLOW_DBAPI{1 2 3 4 5}.log	200 メガバイト	12.5 メガバイト
	共有ディレクトリ/jp1cons/log/console/EVCONS_DBAPI{1 2 3 4 5}.log	50 メガバイト	10 メガバイト
IM 構成管理 DB の API ログ※1	/var/opt/jp1cons/log/evflow/EVFLOW_CFDBAPI{1 2 3 4 5}.log	30 メガバイト	10 メガバイト
	/var/opt/jp1cons/log/console/EVCONS_CFDBAPI{1 2 3}.log	30 メガバイト	10 メガバイト
	/var/opt/jp1cons/log/command/CMD_CFDBAPI{1 2 3}.log	30 メガバイト	10 メガバイト
	共有ディレクトリ/jp1cons/log/evflow/EVFLOW_CFDBAPI{1 2 3 4 5}.log	30 メガバイト	10 メガバイト
	共有ディレクトリ/jp1cons/log/console/EVCONS_CFDBAPI{1 2 3}.log	30 メガバイト	10 メガバイト
jcodbsetup コマンドの ログ※1	/var/opt/jp1cons/log/imdb/jcodbsetup{1 2}.log	512 キロバイト	256 キロバイト
jcodbunsetup コマンドの ログ※1	/var/opt/jp1cons/log/imdb/jcodbunsetup{1 2}.log	512 キロバイト	256 キロバイト
コマンド実行履歴保存ディ レクトリ※1	/var/opt/jp1base/log/COMMAND/	マニュアル「JP1/Base 運用ガイド」 を参照してください	
	共有ディレクトリ/jp1base/log/COMMAND		
リモートコマンドログ※1	/var/opt/jp1base/log/JCOCMD/jcocmd_result{1 2 3}.log		
	/var/opt/jp1base/log/JCOCMD/jcocmdapi{1 2 3}.log		
	/var/opt/jp1base/log/JCOCMD/jcocmdapi_trace{1 2 3}.log		
	/var/opt/jp1base/log/JCOCMD/jcocmdcmc{1 2 3}.log		
	/var/opt/jp1base/log/JCOCMD/jcocmdcmc_trace{1 2 3}.log		

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク使用量	ファイルの切り替え時期
	/var/opt/jp1base/log/JCOCMD/jcocmdcom{1 2 3}.log		
	/var/opt/jp1base/log/JCOCMD/jcocmdcom_trace{1 2 3}.log		
	/var/opt/jp1base/log/JCOCMD/jcocmdexe{1 2 3}.log		
	/var/opt/jp1base/log/JCOCMD/jcocmdexe_trace{1 2 3}.log		
	/var/opt/jp1base/log/JCOCMD/jcocmdrouter{1 2 3}.log		
	/var/opt/jp1base/log/JCOCMD/jcocmdrouter_trace{1 2 3}.log		
	/var/opt/jp1base/log/JCOCMD/JCOCMDCMD{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmd_result{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmdapi{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmdapi_trace{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmdcmc{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmdcmc_trace{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmdcom{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmdcom_trace{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmdexe{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmdexe_trace{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmdrouter{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/jcocmdrouter_trace{1 2 3}.log		
	共有ディレクトリ/jp1base/log/JCOCMD/JCOCMDCMD{1 2 3}.log		
構成管理ログ※1	/var/opt/jp1base/log/route/JBSRT{1 2 3}.log		

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク使用量	ファイルの切り替え時期
	共有ディレクトリ/jp1base/log/route/JBSRT{1 2 3}.log		
トレースログファイル※1	/var/opt/jp1base/sys/tmp/event/logtrap/jeallog/jeallog{1 2 3 4 5}.log		

注※1 プロセス別トレースログです。プロセス別トレースログとは、JP1/IMの各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

注※2 クラスタ環境でだけ作成されます。

注※3 ファイルサイズが、この値より数十キロバイト程度大きくなる場合があります。

注※4 マニュアル「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) によって、64 キロバイト～100 メガバイトの間で設定できます。

注※5 マニュアル「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) によって、1～4,096 キロバイトの間で設定できます。

注※6 アクション情報ファイルの容量がデフォルト (626 キロバイト) の場合の値です。このファイルの最大ディスク占有量は次の見積もり式で算出できます。また、アクションを再実行した場合、一回の再実行ごとに5 キロバイトずつ増加します。

$((\text{アクション情報ファイルの容量}/64 \text{ バイト}) - 1) \times 5 \text{ キロバイト}$

注※7 クラスタ運用の場合も、物理ホスト上のjcochstat, jcochafmode コマンドトレースログに出力されます。

注※8 マニュアル「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) によって、ファイル面数、ファイルサイズを変更できます。

注※9 このファイルは関連イベントの発行処理中のデータを引き継ぐときのメモリー情報を書き出したものであるため、関連イベント発行条件や関連元イベントの情報などによってファイルサイズが異なってきます。見積もりの詳細については、JP1/IM - Manager のリリースノートを参照してください。

注※10 応答待ちイベント管理機能を有効にして JP1/IM - Manager を起動した時点で作成されます。

表 12-12 JP1/IM - Manager (セントラルスコープ) のログファイル・ディレクトリ一覧 (UNIX)

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク使用量	ファイルの切り替え時期
セントラルスコープログ	/var/opt/jp1scope/log/jcsmain{1 2 3}.log	6 メガバイト	2 メガバイト
	/var/opt/jp1scope/log/jcsmain_trace{1 2 3}.log	6 メガバイト	2 メガバイト
	共有ディレクトリ/jp1scope/log/jcsmain{1 2 3}.log	6 メガバイト	2 メガバイト
	共有ディレクトリ/jp1scope/log/jcsmain_trace{1 2 3}.log	6 メガバイト	2 メガバイト
通信用トレースログ	/var/opt/jp1scope/log/jcsmain_trace_com{1 2 3}.log	6 メガバイト	2 メガバイト
	共有ディレクトリ/jp1scope/log/jcsmain_trace_com{1 2 3}.log	6 メガバイト	2 メガバイト
	/var/opt/jp1scope/log/jcsmain_trace_ping{1 2 3}.log	6 メガバイト	2 メガバイト

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク使用量	ファイルの切り替え時期
	共有ディレクトリ/jp1scope/log/jcsmain_trace_ping{1 2 3}.log	6 メガバイト	2 メガバイト
DB 操作 API トレースログ	/var/opt/jp1scope/log/jcsmain_trace_db{1 2 3}.log	6 メガバイト	2 メガバイト
	共有ディレクトリ/jp1scope/log/jcsmain_trace_db{1 2 3}.log	6 メガバイト	2 メガバイト
jcshostsexport コマンドログ	/var/opt/jp1scope/log/jcshostsexport{1 2 3}.log	6 メガバイト	2 メガバイト
	共有ディレクトリ/jp1scope/log/jcshostsexport{1 2 3}.log	6 メガバイト	2 メガバイト
jcshostsimport コマンドログ	/var/opt/jp1scope/log/jcshostsimport{1 2 3}.log	6 メガバイト	2 メガバイト
	共有ディレクトリ/jp1scope/log/jcshostsimport{1 2 3}.log	6 メガバイト	2 メガバイト
jcsdbsetup コマンドログ	/var/opt/jp1scope/log/jcsdbsetup{1 2 3}.log	6 メガバイト	2 メガバイト
	共有ディレクトリ/jp1scope/log/jcsdbsetup{1 2 3}.log	6 メガバイト	2 メガバイト
jcschstat コマンドログ	/var/opt/jp1scope/log/jcschstat{1 2 3}.log	6 メガバイト	2 メガバイト
	共有ディレクトリ/jp1scope/log/jcschstat{1 2 3}.log	6 メガバイト	2 メガバイト
jcsdbimport コマンドログ	/var/opt/jp1scope/log/jcsdbimport{1 2 3}.log	6 メガバイト	2 メガバイト
	共有ディレクトリ/jp1scope/log/jcsdbimport{1 2 3}.log	6 メガバイト	2 メガバイト
jcsdbexport コマンドログ	/var/opt/jp1scope/log/jcsdbexport{1 2 3}.log	6 メガバイト	2 メガバイト
	共有ディレクトリ/jp1scope/log/jcsdbexport{1 2 3}.log	6 メガバイト	2 メガバイト
セットアップ時のログ	/var/opt/jp1scope/log/JCS_SETUP/jcs_setup.log	100 キロバイト	インストール時
	/var/opt/jp1scope/log/jcs_setup/論理ホスト名/jcs_setup.log	100 キロバイト	インストール時
	/var/opt/jp1scope/log/jcs_setup/論理ホスト名/reg.txt	100 キロバイト	インストール時
	/var/opt/jp1scope/log/jcs_setup/論理ホスト名/reg_def.txt	100 キロバイト	インストール時

注 プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

表 12-13 JP1/IM - Manager (IM 構成管理) のログファイル・ディレクトリー一覧 (UNIX)

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク 使用量	ファイルの切り替 え時期
IM 構成管理トレースログ	/var/opt/jp1imm/log/imcf/jcfallogtrap{1 2 3 4 5 6 7 8 9 10}.log	200 メガバイト	10 メガバイト
	/var/opt/jp1imm/log/imcf/jcfallogtrap_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	/var/opt/jp1imm/log/imcf/jcfallogtrap_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	/var/opt/jp1imm/log/imcf/jcfmain{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	/var/opt/jp1imm/log/imcf/jcfmain_trace{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	/var/opt/jp1imm/log/imcf/jcfmain_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/jcfallogtrap{1 2 3 4 5 6 7 8 9 10}.log	200 メガバイト	10 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/jcfallogtrap_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/jcfallogtrap_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/jcfmain{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/jcfmain_trace{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/jcfmain_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
通信用トレースログ	/var/opt/jp1imm/log/imcf/jcfmain_trace_com{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	/var/opt/jp1imm/log/imcf/jcfmain_ping{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/jcfmain_trace_com{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/jcfmain_ping{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
認証用トレースログ	/var/opt/jp1imm/log/imcf/jcfmain_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク 使用量	ファイルの切り替 え時期
	共有ディレクトリ/jp1imm/log/imcf/ jcfmain_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
DB 操作 API トレースログ	/var/opt/jp1imm/log/imcf/jcfmain_trace_db{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfmain_trace_db{1 2 3 4 5 6 7 8 9 10}.log	20 メガバイト	2 メガバイト
コマンド共通ログ	/var/opt/jp1imm/log/imcf/jcfcommand{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/jcfcommand{1 2 3}.log	3 メガバイト	1 メガバイト
jcfallogstart コマンドログ	/var/opt/jp1imm/log/imcf/jcfallogstart{1 2 3}.log	9 メガバイト	3 メガバイト
	/var/opt/jp1imm/log/imcf/ jcfallogstart_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfallogstart{1 2 3}.log	9 メガバイト	3 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfallogstart_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfallogstat コマンドログ	/var/opt/jp1imm/log/imcf/jcfallogstat{1 2 3}.log	9 メガバイト	3 メガバイト
	/var/opt/jp1imm/log/imcf/ jcfallogstat_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfallogstat{1 2 3}.log	9 メガバイト	3 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfallogstat_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfallogstop コマンドログ	/var/opt/jp1imm/log/imcf/jcfallogstop{1 2 3}.log	9 メガバイト	3 メガバイト
	/var/opt/jp1imm/log/imcf/ jcfallogstop_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfallogstop{1 2 3}.log	9 メガバイト	3 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfallogstop_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfallogreload コマンドログ	/var/opt/jp1imm/log/imcf/jcfallogreload{1 2 3}.log	9 メガバイト	3 メガバイト
	/var/opt/jp1imm/log/imcf/ jcfallogreload_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク 使用量	ファイルの切り替 え時期
	共有ディレクトリ/jp1imm/log/imcf/ jcfallogreload{1 2 3}.log	9 メガバイト	3 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfallogreload_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfallogdef コマンドログ	/var/opt/jp1imm/log/imcf/jcfallogdef{1 2 3}.log	9 メガバイト	3 メガバイト
	/var/opt/jp1imm/log/imcf/ jcfallogdef_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/jcfallogdef{1 2 3}.log	9 メガバイト	3 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfallogdef_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfcolvmesx コマンドログ	/var/opt/jp1imm/log/imcf/jcfcolvmesx_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfcolvmesx_trace{1 2 3}.log		
jcfcolvmvirtage コマンドログ	/var/opt/jp1imm/log/imcf/ jcfcolvmvirtage_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfcolvmvirtage_trace{1 2 3}.log		
jcfcolvmvc コマンドログ	/var/opt/jp1imm/log/imcf/jcfcolvmvc_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfcolvmvc_trace{1 2 3}.log		
jcfcolvmkvm コマンドログ	/var/opt/jp1imm/log/imcf/jcfcolvmkvm_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfcolvmkvm_trace{1 2 3}.log		
jcfcolvmhcsn コマンドログ	/var/opt/jp1imm/log/imcf/jcfcolvmhcsn_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfcolvmhcsn_trace{1 2 3}.log		
jcfexport コマンドログ	/var/opt/jp1imm/log/imcf/jcfexport_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfexport_VM_trace{1 2 3}.log		

ログの種類	デフォルトのファイル名・ディレクトリ名	最大ディスク 使用量	ファイルの切り替 え時期
jcfimport コマンドログ	/var/opt/jp1imm/log/imcf/jcfimport_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
	共有ディレクトリ/jp1imm/log/imcf/ jcfimport_VM_trace{1 2 3}.log	3 メガバイト	1 メガバイト
jcfmkhostsdata コマンドログ	/var/opt/jp1imm/log/imcf/ jcfmkhostsdata_trace{1 2 3}.log	3 メガバイト	1 メガバイト
スタックトレースログ	/var/opt/jp1imm/log/imcf/javaLog0{1 2 3 4}.log	1 メガバイト	起動時, または 256 キロバイト
セットアップ時のログ	/var/opt/jp1imm/log/imcf/JCF_SETUP/ jcf_setup.log	100 キロバ イト	インストール時
	/var/opt/jp1imm/log/imcf/JCF_SETUP/論理ホスト 名/jcf_setup.log	100 キロバ イト	インストール時

注 プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

表 12-14 インテリジェント統合管理基盤のログファイル・フォルダー一覧

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使 用量	ファイルの切り 替え時期
インテリジェント統合管 理基盤サービス個別ログ	/var/opt/jp1imm/log/imdd/jddmain/jddmain.log{.1-7}	1 ギガバイト	128 メガバイト
	共有ディレクトリ/jp1imm/log/imdd/jddmain/ jddmain.log{.1-7}		
定義ファイル※1・ノー ドファイル履歴ログログ	/var/opt/jp1imm/log/imdd/jddmain/jimddDef.log{.1-10}	80 メガバイト	8 メガバイト
	共有ディレクトリ/jp1imm/log/imdd/jddmain/ jimddDef.log{.1-10}	240 メガバイト	8 メガバイト
	/var/opt/jp1imm/log/imdd/jddmain/jimddMaster.log{.1-30}		
	共有ディレクトリ/jp1imm/log/imdd/jddmain/ jimddMaster.log{.1-30}		
jddsetaccessuser コマ ンドトレースログ	/var/opt/jp1imm/log/imdd/jddsetaccessuser/ jddsetaccessuser.log{.1-6}	70 メガバイト	10 メガバイト
	共有ディレクトリ/jp1imm/log/imdd/jddsetaccessuser/ jddsetaccessuser.log{.1-6}	768 キロバイト	256 キロバイト
	/var/opt/jp1imm/log/imdd/jddsetaccessuser/ jddsetaccessuser_exe{1 2 3}.log		
	共有ディレクトリ/jp1imm/log/imdd/jddsetaccessuser/ jddsetaccessuser_exe{1 2 3}.log		

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
	/var/opt/jp1imm/log/imdd/jddsetaccessuser/javaLog0{1 2 3 4}.log	1024 キロバイト	起動時または256 キロバイト
	共有ディレクトリ/jp1imm/log/imdd/jddsetaccessuser/javaLog0{1 2 3 4}.log		
jddcreatetree コマンド トレースログ	/var/opt/jp1imm/log/imdd/jddcreatetree/jddcreatetree.log{.1-6}	70 メガバイト	10 メガバイト
	共有ディレクトリ/jp1imm/log/imdd/jddcreatetree/jddcreatetree.log{.1-6}		
	/var/opt/jp1imm/log/imdd/jddcreatetree/jddcreatetree_exe{1 2 3}.log	768 キロバイト	256 キロバイト
	共有ディレクトリ/jp1imm/log/imdd/jddcreatetree/jddcreatetree_exe{1 2 3}.log		
	/var/opt/jp1imm/log/imdd/jddcreatetree/javaLog0{1 2 3 4}.log	1,024 キロバイト	起動時または256 キロバイト
	共有ディレクトリ/jp1imm/log/imdd/jddcreatetree/javaLog0{1 2 3 4}.log		
jddupdatetree コマンド トレースログ	/var/opt/jp1imm/log/imdd/jddupdatetree/jddupdatetree.log{.1-6}	70 メガバイト	10 メガバイト
	共有ディレクトリ/jp1imm/log/imdd/jddupdatetree/jddupdatetree.log{.1-6}		
	/var/opt/jp1imm/log/imdd/jddupdatetree/jddupdatetree_exe{1 2 3}.log	768 キロバイト	256 キロバイト
	共有ディレクトリ/jp1imm/log/imdd/jddupdatetree/jddupdatetree_exe{1 2 3}.log		
	/var/opt/jp1imm/log/imdd/jddupdatetree/javaLog0{1 2 3 4}.log	1,024 キロバイト	256 キロバイト
	共有ディレクトリ/jp1imm/log/imdd/jddupdatetree/javaLog0{1 2 3 4}.log		
jddproxyuser コマンド トレースログ	/var/opt/jp1imm/log/imdd/jddproxyuser/jddproxyuser.log{.1-6}	70 メガバイト	10 メガバイト
	共有ディレクトリ/jp1imm/log/imdd/jddproxyuser/jddproxyuser.log{.1-6}		
	/var/opt/jp1imm/log/imdd/jddproxyuser/jddproxyuser_exe{1 2 3}.log	768 キロバイト	256 キロバイト
	共有ディレクトリ/jp1imm/log/imdd/jddproxyuser/jddproxyuser_exe{1 2 3}.log		

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
	/var/opt/jp1imm/log/imdd/jddproxyuser/javalog0{1 2 3 4}.log 共有ディレクトリ/jp1imm/log/imdd/jddproxyuser/javalog0{1 2 3 4}.log	1,024 キロバイト	256 キロバイト
jimgndbsetup コマンド トレースログ	/var/opt/jp1imm/log/imgndb/jimgndbsetup{1 2}.log	512 キロバイト	256 キロバイト
jimgndbunsetup コマンド トレースログ	/var/opt/jp1imm/log/imgndb/jimgndbunsetup{1 2}.log	512 キロバイト	256 キロバイト
jimgndbstop コマンド トレースログ	/var/opt/jp1imm/log/imgndb/jimgndbstop{1-10}.log 共有ディレクトリ/jp1imm/log/imgndb/jimgndbstop{1-10}.log	51,200 キロバイト	5,120 キロバイト
jimgndbstatus コマンド トレースログ	/var/opt/jp1imm/log/imgndb/jimgndbstatus{1-10}.log 共有ディレクトリ/jp1imm/log/imgndb/jimgndbstatus{1-10}.log	51,200 キロバイト	5,120 キロバイト
対処アクション実行履歴 ファイルのログ※4	/var/opt/jp1imm/log/suggestion/jddSuggestionHistory.log{.1-3} 共有ディレクトリ/jp1imm/log/suggestion/jddSuggestionHistory.log{.1-3}	240 メガバイト	60 メガバイト
シークレット認証ログ ファイル	/var/opt/jp1imm/log/secretAuth/jddSecretAuth.log{.1-3} 共有ディレクトリ/jp1imm/log/secretAuth/jddSecretAuth.log{.1-3}	240 メガバイト	60 メガバイト
ユーザー作成プラグイン	/var/opt/jp1imm/log/imdd/ユーザー作成プラグイン名/ユーザー作成プラグイン.log{1-21}※3 共有ディレクトリ/jp1imm/log/imdd/ユーザー作成プラグイン名/ユーザー作成プラグイン.log{1-21}※3	220 メガバイト	10 メガバイト
その他ログ	/var/opt/jp1imm/log/imdd/jddmain/jddmain_exe{1 2 3}.log 共有ディレクトリ/jp1imm/log/imdd/jddmain/jddmain_exe{1 2 3}.log	768 キロバイト	256 キロバイト
	/var/opt/jp1imm/log/imdd/jddmain/javalog0{1 2 3 4}.log 共有ディレクトリ/jp1imm/log/imdd/jddmain/javalog0{1 2 3 4}.log	1,024 キロバイト	起動時または 256 キロバイト
	/var/opt/jp1imm/log/imdd/jcoapi{1-50}.log 共有ディレクトリ/jp1imm/log/imdd/jddmain/jcoapi{1-50}.log	500 メガバイト	10 メガバイト
	/var/opt/jp1imm/log/imdd/jcoapiM{1-50}.log	500 メガバイト	10 メガバイト

ログの種類	デフォルトのファイル名・フォルダ名	最大ディスク使用量	ファイルの切り替え時期
	共有ディレクトリ/jp1imm/log/imdd/jddmain/jcoapiM{1-50}.log		
	/var/opt/jp1imm/log/imdd/<コンポーネント名>※2/<コンポーネント名>※2{1-21}.log	220 メガバイト	10 メガバイト
	共有ディレクトリ/jp1imm/log/imdd/<コンポーネント名>※2/<コンポーネント名>※2{1-21}.log		

注 プロセス別トレースログです。プロセス別トレースログとは、JP1/IM の各機能が出力するログ情報のことです。各機能によって異なるログファイルに出力されます。なお、プロセス別トレースログには製品情報が含まれているため、内容は公開していません。

注※1 インテリジェント統合管理基盤の定義ファイルログでは、次の定義ファイルのログを出力します。

システムノード定義ファイル、IM 管理ノードカテゴリ名称定義ファイル、ホスト名定義ファイル、構成取得対象ホスト定義ファイル、IM 管理ノードリンク定義ファイル、IM 管理ノードリンクファイル、IM 管理ノードツリーファイル、IM 管理ノードファイル

注※2 コンポーネント名には、次のどれかが表示されます。

- jplajs
- jplpfm
- jplim

注※3 {1-21}はファイルの面数です。ログファイルは任意のテキストエディターで参照できます。

注※4 対処アクションを実行した際のログです。失敗した場合の調査など、対処アクションのログをユーザー自身で確認できます。

(6) JP1/IM - Agent (統合エージェント管理基盤) のログ

(a) 公開ログ

統合エージェント管理基盤の公開用のログが出力されます。

ログサイズの上限と面数

統合エージェント管理基盤の定義ファイルで指定します。

出力先

- Windows の場合

Manager パス※¥log¥imdd¥imagent¥imbase¥

Manager パス※¥log¥imdd¥imagent¥imbaseproxy¥

注※ クラスタの場合は「共有フォルダ¥jp1imm」に読み替えてください。

- Linux の場合

/var/opt※/jp1imm/log/imdd/imagent/imbase/

/var/opt※/jp1imm/log/imdd/imagent/imbaseproxy/

注※ クラスタの場合は「共有ディレクトリ」に読み替えてください。

ファイル名

jima_message.log^{※1}

jima_message-YYYY-MM-DDThh-mm-ss.sss.log^{※2}

注※1

ログが規定のサイズに達すると、ログファイル名に「-YYYY-MM-DDThh-mm-ss.sss.log」付与して、ローテーションします。

注※2

出力先のログファイル名を新しい日付にリネームし、一番古いログファイルを削除します。

出力形式

日時 PID ジョブ識別子 メッセージ ID メッセージ

注意事項

対処アクションでコマンドを実行すると、実行したコマンドの標準出力や標準エラー出力の内容が imagent の公開ログに出力されます。このため、メッセージなどを出力するコマンドを対処アクションで実行することが想定される場合は、必要に応じて imagent の公開ログの面数とサイズを拡張してください。

imagent の公開ログの面数やサイズは、imagent 設定ファイルの log.message.num と log.message.size で指定できます。

(b) 起動時の設定値ログ

統合エージェント管理基盤が起動時に読み込んだ設定値が出力されます。

ログサイズの上限と面数

ログサイズと面数はシステムで固定です。ユーザーによる変更はできません。

出力先

- Windows の場合

Manager パス[※]¥log¥imdd¥imagent¥imbase¥

Manager パス[※]¥log¥imdd¥imagent¥imbaseproxy¥

注※ クラスタの場合は「共有フォルダ¥jp1imm」に読み替えてください。

- Linux の場合

/var/opt[※]/jp1imm/log/imdd/imagent/imbase/

/var/opt[※]/jp1imm/log/imdd/imagent/imbaseproxy/

注※ クラスタの場合は「共有ディレクトリ」に読み替えてください。

ファイル名

jima_setting.log^{※1}

jima_setting-YYYY-MM-DDThh-mm-ss.sss.log^{※2}

注※1

ログが規定のサイズに達すると、ログファイル名に「-YYYY-MM-DDThh-mm-ss.sss.log」付与して、ローテーションします。

注※2

出力先のログファイル名を新しい日付にリネームし、一番古いログファイルを削除します。

出力形式

日時と設定値がわかるログを出力します。

12.2.2 JP1/IM - Agent のログ情報

(1) Prometheus server のログ

Prometheus server のログが出力されます。

ログサイズの上限と面数

- Windows の場合
サービス定義ファイルで指定します。
- Linux の場合
ユニット定義ファイルで指定します。

指定方法については、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」(2. 定義ファイル) のサービス定義ファイルとユニット定義ファイルを参照してください。

出力先

- Windows の場合
Agent パス※`logs\prometheus_server\jpc_prometheus_server_service.(err|out).log`
注※ クラスタの場合は「共有フォルダ\jp1ima」に読み替えてください。
- Linux の場合
パス※`/opt/jp1ima/logs/prometheus_server/prometheus_service`
注※ クラスタの場合は「共有ディレクトリ」に読み替えてください。

出力形式

Prometheus server が、稼働中に標準出力または標準エラー出力に出力したテキストデータを出力します。

(2) Alertmanager のログ

Alertmanager のログが出力されます。

ログサイズの上限と面数

- Windows の場合
サービス定義ファイルで指定します。
- Linux の場合
ユニット定義ファイルで指定します。

指定方法については、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」(2. 定義ファイル) のサービス定義ファイルとユニット定義ファイルを参照してください。

出力先

- Windows の場合
Agent パス※`logs>alertmanager%jpc_alertmanager_service.(err|out).log`
注※ クラスタの場合は「共有フォルダ%jp1ima」に読み替えてください。
- Linux の場合
`/opt`※`/jp1ima/logs/alertmanager/alertmanager_service`
注※ クラスタの場合は「共有ディレクトリ」に読み替えてください。

出力形式

Alertmanager が、稼働中に標準出力または標準エラー出力に出力したテキストデータを出力します。

(3) Exporter のログ

Exporter のログが出力されます。

ログサイズの上限と面数

- Windows の場合
サービス定義ファイルで指定します。
- Linux の場合
ユニット定義ファイルで指定します。

指定方法については、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」(2. 定義ファイル) のサービス定義ファイルとユニット定義ファイルを参照してください。

出力先

- Windows の場合
Agent パス※`logs`Exporter 名`%jpc_Exporter 名_service.(err|out).log`
注※ クラスタの場合は「共有フォルダ%jp1ima」に読み替えてください。
- Linux の場合
`/opt`※`/jp1ima/logs/Exporter 名/Exporter 名_service`

注※ クラスタの場合は「共有ディレクトリ」に読み替えてください。

出力形式

Exporter が、稼働中に標準出力または標準エラー出力に出力したテキストデータを出力します。

(4) サービス制御のログ

- Windows の場合
サービスの起動と停止を行ったときのログが出力されます。
- Linux の場合
ログは出力されません。

ログサイズの上限と面数

ログが一定のサイズになったときにローテーションします。ログサイズの上限と面数は指定できません。

出力先

- Windows の場合
Agent パス※¥logs¥prometheus¥jpc_prometheus_server_service.wrapper.log
Agent パス※¥logs¥alertmanager¥jpc_alertmanager_service.wrapper.log
Agent パス※¥logs¥Exporter 名¥jpc_Exporter 名_service.wrapper.log
Agent パス※¥logs¥fluentd¥jpc_fluentd_service.wrapper.log
Agent パス※¥logs¥imagent¥jpc_imagent_service.wrapper.log
Agent パス※¥logs¥imagentproxy¥jpc_imagentproxy_service.wrapper.log
Agent パス※¥logs¥imagentaction¥jpc_imagentaction_service.wrapper.log
注※ クラスタの場合は「共有フォルダ¥jp1ima」に読み替えてください。

出力形式

Windows サービス化プログラムが出力したテキストデータを出力します。

出力する契機とサイズ

サービス制御のログに出力する契機とサイズの目安を、次に示します。

契機	サイズの目安 (バイト)	出力例
サービスの起動	750	2021-11-22 14:18:48,135 DEBUG - Starting WinSW in service mode 2021-11-22 14:18:48,394 INFO - Starting prometheus.exe -- config.file="jpc_prometheus_server.yml" --web.read-timeout=5m --web.max- connections=10 --web.enable-lifecycle --storage.tsdb.path="data/" -- storage.tsdb.retention.time=0d --storage.remote.flush-deadline=2m -- rules.alert.for-outage-tolerance=1h --rules.alert.for-grace-period=10m -- rules.alert.resend-delay=1m --alertmanager.notification-queue- capacity=10000 --log.level=info --log.format=logfmt 2021-11-22 14:18:50,805 INFO - Started process 17384

契機	サイズの目安 (バイト)	出力例
		2021-11-22 14:18:50,826 DEBUG - Forwarding logs of the process System.Diagnostics.Process (prometheus) to WinSW.SizeBasedRollingLogAppender
サービスの停止	300	2021-11-22 14:12:04,083 INFO - Stopping jpc_prometheus 2021-11-22 14:12:04,084 DEBUG - ProcessKill 16492 2021-11-22 14:12:04,108 DEBUG - Stopping process 16492... 2021-11-22 14:12:04,141 DEBUG - Process 16492 canceled with code 0. 2021-11-22 14:12:04,176 INFO - Finished jpc_prometheus

削除方法

ログファイルを、移動またはリネームして退避します。退避したあとは、ユーザーがログを出力する操作を行ったときに、プログラムがログファイルを作成します。ログファイルを退避するときに、サービスを停止させる必要はありません。

退避したファイルは、不要と判断したときに手動で削除します。

(5) Fluentd のログ

Fluentd のログが出力されます。

ログサイズの上限と面数

- Windows の場合
サービス定義ファイルで指定します。
- Linux の場合
ユニット定義ファイルで指定します。

指定方法については、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」(2. 定義ファイル) のサービス定義ファイルとユニット定義ファイルを参照してください。

出力先

- Windows の場合
Agent パス※¥logs¥fluentd¥jpc_fluentd_service.(err|out).log
注※ クラスタの場合は「共有フォルダ¥jp1ima」に読み替えてください。
- Linux の場合
/opt¥jp1ima/logs/fluentd/fluentd_server
注※ クラスタの場合は「共有ディレクトリ」に読み替えてください。

出力形式

Fluentd が、稼働中に標準出力または標準エラー出力に出力したテキストデータを出力します。

(6) コマンドのログ

コマンドのログが出力されます。

ログサイズの上限と面数

ログサイズの上限と面数はコマンドごとに決まっています。変更できません。

出力先

- Windows の場合

Agent パス※¥logs¥tools¥コマンド名.*

注※

クラスタの場合、物理ディスクに出力するコマンドと共有ディスクに出力するコマンドがあります。共有ディスクに出力するコマンドの場合は「共有フォルダ¥jp1ima」に読み替えてください。

- Linux の場合

/opt※/jp1ima/logs/tools/コマンド名.*

注※

クラスタの場合、物理ディスクに出力するコマンドと共有ディスクに出力するコマンドがあります。共有ディスクに出力するコマンドの場合は「共有ディレクトリ」に読み替えてください。

出力形式

日付 ログ内容

(7) 統合エージェント制御基盤のログ

(a) 公開ログ

統合エージェント制御基盤の公開用のログが出力されます。

ログサイズの上限と面数

統合エージェント制御基盤の定義ファイルで指定します。

出力先

- Windows の場合

Agent パス※¥logs¥imagent¥

Agent パス※¥logs¥imagentproxy¥

Agent パス※¥logs¥imagentaction¥

注※ クラスタの場合は「共有フォルダ¥jp1ima」に読み替えてください。

- Linux の場合

/opt※/jp1ima/logs/imagent/

/opt※/jp1ima/logs/imagentproxy/

/opt*/jp1ima/logs/imagentaction/

注※ クラスタの場合は「共有ディレクトリ」に読み替えてください。

ファイル名

jima_message.log^{※1}

jima_message-YYYY-MM-DDThh-mm-ss. sss. log^{※2}

注※1

ログが規定のサイズに達すると、ログファイル名に「-YYYY-MM-DDThh-mm-ss. sss. log」付与して、ローテーションします。

注※2

出力先のログファイル名を新しい日付にリネームし、一番古いログファイルを削除します。

出力形式

日時 PID ジョブ識別子 メッセージ ID メッセージ

(b) 起動時の設定値ログ

統合エージェント制御基盤が起動時に読み込んだ設定値が出力されます。

ログサイズの上限と面数

ログサイズと面数はシステムで固定です。ユーザーによる変更はできません。

出力先

- Windows の場合

Agent パス[※]¥logs¥imagent¥

Agent パス[※]¥logs¥imagentproxy¥

Agent パス[※]¥logs¥imagentaction¥

注※ クラスタの場合は「共有フォルダ¥jp1ima」に読み替えてください。

- Linux の場合

/opt*/jp1ima/logs/imagent/

/opt*/jp1ima/logs/imagentproxy/

/opt*/jp1ima/logs/imagentaction/

注※ クラスタの場合は「共有ディレクトリ」に読み替えてください。

ファイル名

jima_setting.log^{※1}

jima_setting-YYYY-MM-DDThh-mm-ss. sss. log^{※2}

注※1

ログが規定のサイズに達すると、ログファイル名に「-YYYY-MM-DDThh-mm-ss. sss. log」付与して、ローテーションします。

注※2

出力先のログファイル名を新しい日付にリネームし、一番古いログファイルを削除します。

出力形式

日時と設定値がわかるログを出力します。

12.3 トラブル発生時に採取が必要な資料

トラブルが発生したときに採取が必要な資料を示します。

なお、JP1 では採取が必要な資料を一括採取するための資料採取ツールを用意しています。資料採取ツールで採取できる資料は、OS のシステム情報や JP1 の情報です。次からは Windows, UNIX のそれぞれの場合について説明します。

12.3.1 JP1/IM - Manager に関する資料

(1) Windows の場合

(a) OS のシステム情報

OS に関する次の情報の採取が必要です。これらの情報は資料採取ツールで採取できます。

なお、資料採取ツール (jim_log.bat コマンド, jcoview_log.bat コマンド) では採取できる資料に違いがあります。次の表に示す資料は, jim_log.bat コマンドを実行するとすべて採取されます。jcoview_log.bat コマンドを実行するときに採取できる資料については右端の列に示します。

表 12-15 OS のシステム情報 (Windows)

情報の種類	採取資料	ファイル名※1	View
資料採取日時	<ul style="list-style-type: none">• date /t の実行結果• time /t の実行結果	date.log	○
日立総合インストーラのログファイル	Windows のインストール先フォルダ¥Temp¥HCDINST¥以下のファイル	左記ファイルのコピーファイル	○
JP1/IM - Manager のインストール/アンインストールログファイル	Windows のインストール先フォルダ ¥Temp¥HITACHI_JP1_INST_LOG¥jp1imm_inst{1 2 3 4 5}.log	jp1imm_inst{1 2 3 4 5}.log	△
JP1/IM - View インストール/アンインストールログファイル	Windows のインストール先フォルダ ¥Temp¥HITACHI_JP1_INST_LOG¥jp1coview_inst{1 2 3 4 5}.log	jp1coview_inst{1 2 3 4 5}.log	○
JP1/Base インストール/アンインストールログファイル	Windows のインストール先フォルダ ¥Temp¥HITACHI_JP1_INST_LOG¥jp1base_inst{1 2 3 4 5}.log	jp1base_inst{1 2 3 4 5}.log	△
製品情報ログファイル	Windows のインストール先フォルダ¥Temp¥jp1common¥以下のファイル	左記ファイルのコピー	○

情報の種類	採取資料	ファイル名※1	View
マシンに設定されているホスト名の設定	システムルートフォルダ ¥system32¥drivers¥etc¥hosts	hosts	○
マシンに設定されているサービスポートの設定	システムルートフォルダ ¥system32¥drivers¥etc¥services	services	○
NICの実装状況	ipconfig /allの実行結果	ipconfig.log	○
起動サービス一覧	net startの実行結果	netstart.log	○
ネットワーク統計情報	netstat -naoの実行結果	netstat.log	○
マシンの環境変数	setの実行結果	set.log	○
マシンのシステム情報	msinfo32 /report ファイル名の実行結果	msinfo32.log	○
レジストリ情報	レジストリ HKEY_LOCAL_MACHINE¥SOFTWARE¥HITACHI または レジストリ HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥HITACHI の値をregコマンドで採取した結果	hitachi_reg.txt	○
製品情報ファイル	システムドライブ:Program Files¥HITACHI¥jp1common¥以下のファイル	左記ファイルのコピーファイル	○
JP1/IM - Managerのインストール情報	システムドライブ:Program Files¥InstallShield Installation Information¥setup.ini	imm_setup.ini	△
JP1/IM - Managerのインストールログファイル	システムドライブ:Program Files¥InstallShield Installation Information¥setup.ilg	imm_setup.ilg	△
JP1/Baseのインストール情報	システムドライブ:Program Files¥InstallShield Installation Information¥setup.ini	base_setup.ini	△
JP1/Baseのインストールログファイル	システムドライブ:Program Files¥InstallShield Installation Information¥setup.ilg	base_setup.ilg	△
JP1/IM - Viewのインストール情報	システムドライブ:Program Files¥InstallShield Installation Information¥setup.ini	imv_setup.ini	○
JP1/IM - Viewのインストールログファイル	システムドライブ:Program Files¥InstallShield Installation Information¥setup.ilg	imv_setup.ilg	○

情報の種類	採取資料	ファイル名※1	View
JP1/Base のアクセス権限情報(インストールフォルダ)	cacls Base パス の実行結果	cacls_jp1base.log	△
	cacls 共有フォルダ¥JP1Base の実行結果※2	cacls_jp1base.log	—
JP1/Base のアクセス権限情報(ログフォルダ)	cacls Base パス¥log の実行結果	cacls_jp1base_log.log	△
	cacls 共有フォルダ¥JP1Base¥log の実行結果※2	cacls_jp1base_log.log	—
JP1/Base のアクセス権限情報(コマンド実行履歴フォルダ)	cacls Base パス¥log¥COMMAND の実行結果	cacls_jp1base_log_COMMAND.log	△
	cacls 共有フォルダ¥JP1Base¥log¥COMMAND の実行結果※2	cacls_jp1base_log_COMMAND.log	—
JP1/Base のアクセス権限情報(イベント DB フォルダ)	cacls Base パス¥sys の実行結果	cacls_jp1base_sys.log	△
JP1/Base のアクセス権限情報(イベント DB フォルダ)	cacls Base パス¥sys¥event の実行結果	cacls_jp1base_sys_event.log	△
	cacls 共有フォルダ¥JP1Base¥event の実行結果※2	cacls_jp1base_event.log	—
JP1/Base のアクセス権限情報(イベント DB フォルダ)	cacls Base パス¥sys¥event¥servers の実行結果	cacls_jp1base_sys_event_servers.log	△
JP1/Base のアクセス権限情報(イベント DB フォルダ)	cacls Base パス¥sys¥event¥servers¥default の実行結果	cacls_jp1base_sys_event_servers_default.log	△
JP1/IM - Manager(セントラルコンソール)のアクセス権限情報(インストールフォルダ)	cacls Console パス の実行結果	cacls_jp1cons.log	△
	cacls 共有フォルダ¥JP1Cons の実行結果※2	cacls_jp1cons.log	—
JP1/IM - Manager(セントラルコンソール)のアクセス権限情報(ログフォルダ)	cacls Console パス¥log の実行結果	cacls_jp1cons_log.log	△
	cacls 共有フォルダ¥JP1Cons¥log の実行結果※2	cacls_jp1cons_log.log	—
JP1/IM - Manager(セントラルコンソール)のアクセス権限情報(関連履歴フォルダ)	cacls Console パス¥operation の実行結果	cacls_jp1cons_operation.log	△
	cacls 共有フォルダ¥JP1Cons¥operation の実行結果※2	cacls_jp1cons_operation.log	—
JP1/IM - Manager(セントラルコンソール)のアクセス権限情報(関連履歴フォルダ)	cacls Console パス¥operation¥evgen の実行結果	cacls_jp1cons_operation_evgen.log	△

情報の種類	採取資料	ファイル名※1	View
イベント発行履歴フォルダ)	cacls 共有フォルダ ¥JP1Cons¥operation¥evgen の実行結果※2	cacls_jp1cons_operation_evgen.log	—
JP1/IM - Manager(セントラルコンソール)のアクセス権限情報(共通除外履歴フォルダ)	cacls Console パス ¥operation¥comexclude の実行結果	cacls_jp1cons_operation_comexclude.log	△
JP1/IM - View のアクセス権限情報(インストールフォルダ)	cacls View パス の実行結果	cacls_jp1coview.log	○
JP1/IM - View のアクセス権限情報(ログフォルダ)	cacls システムドライブ:¥ProgramData¥Hitech¥jp1¥jp1_default¥JP1CoView¥log の実行結果	cacls_programdata_jp1coview_log.log	○
JP1/IM - Manager のアクセス権限情報(インストールフォルダ)	cacls Manager パスの実行結果	cacls_jp1imm.log	△
JP1/IM - Manager のアクセス権限情報(ログフォルダ)	cacls Manager パス¥log の実行結果	cacls_jp1imm_log.log	△
JP1/IM - Manager(セントラルスコープ)のアクセス権限情報(インストールフォルダ)	cacls Scope パス の実行結果	cacls_jp1scope.log	△
	cacls 共有フォルダ¥JP1Scope の実行結果※2	cacls_jp1scope.log	—
JP1/IM - Manager(セントラルスコープ)のアクセス権限情報(ログフォルダ)	cacls Scope パス¥log の実行結果	cacls_jp1scope_log.log	△
	cacls 共有フォルダ¥JP1Scope¥log の実行結果※2	cacls_jp1scope_log.log	—
JP1/IM - Manager(セントラルスコープ)のアクセス権限情報(DB フォルダ)	cacls Scope パス¥database の実行結果	cacls_jp1scope_database.log	△
	cacls 共有フォルダ¥JP1Scope¥database の実行結果※2	cacls_jp1scope_database.log	—
JP1/IM - Manager(セントラルスコープ)のアクセス権限情報(DB フォルダ)	cacls Scope パス¥database¥event の実行結果	cacls_jp1scope_database_event.log	△
	cacls 共有フォルダ¥JP1Scope¥database¥event の実行結果※2	cacls_jp1scope_database_event.log	—
JP1/IM - Manager(セントラルスコープ)のアクセス権限情報(DB フォルダ)	cacls Scope パス¥database¥jcsdb の実行結果	cacls_jp1scope_database_jcsdb.log	△
	cacls 共有フォルダ¥JP1Scope¥database¥jcsdb の実行結果※2	cacls_jp1scope_database_jcsdb.log	—

情報の種類	採取資料	ファイル名※1	View
JP1/IM - Manager(セントラルスコープ)のアクセス権限情報(DB フォルダ)	cacls Scope パス ¥database¥jcsdb¥event の実行結果	cacls_jp1scope_database_jcsdb_event.log	△
	cacls 共有フォルダ ¥JP1Scope¥database¥jcsdb¥event の実行結果※2	cacls_jp1scope_database_jcsdb_event.log	—
JP1/IM - Manager(セントラルスコープ)のアクセス権限情報(DB フォルダ)	cacls Scope パス ¥database¥jcsdb¥pw の実行結果	cacls_jp1scope_database_jcsdb_pw.log	△
	cacls 共有フォルダ ¥JP1Scope¥database¥jcsdb¥pw の実行結果※2	cacls_jp1scope_database_jcsdb_pw.log	—
JP1/IM - Manager(セントラルスコープ)のアクセス権限情報(DB フォルダ)	cacls Scope パス ¥database¥jcsdb¥tree の実行結果	cacls_jp1scope_database_jcsdb_tree.log	△
	cacls 共有フォルダ ¥JP1Scope¥database¥jcsdb¥tree の実行結果※2	cacls_jp1scope_database_jcsdb_tree.log	—
JP1/IM - Manager(セントラルスコープ)のアクセス権限情報(DB フォルダ)	cacls Scope パス ¥database¥jcshosts の実行結果	cacls_jp1scope_database_jcshosts.log	△
	cacls 共有フォルダ ¥JP1Scope¥database¥jcshosts の実行結果※2	cacls_jp1scope_database_jcshosts.log	—
JP1/IM - Manager(インテリジェント統合管理基盤)のアクセス権限情報(ログフォルダ)	cacls Manager パス¥log¥imdd の実行結果	cacls_jp1imm_log_imdd.log	—
	cacls 共有フォルダ¥log¥imdd の実行結果※2	cacls_jp1imm_log_imdd.log	—
JP1/IM - Manager(インテリジェント統合管理基盤)のアクセス権限情報(対処アクション実行履歴フォルダ)	cacls Manager パス¥log¥suggestion の実行結果	cacls_jp1imm_log_suggestion.log	—
	cacls 共有フォルダ¥log¥suggestion の実行結果※2	cacls_jp1imm_log_suggestion.log	—
操作ログファイル出力先のアクセス権限情報	cacls 操作ログ出力先 の実行結果 操作ログ出力先は次に示す共通定義に指定されたフォルダ [JP1_DEFAULT¥JP1IMM¥OPERATION] "LOGFILEDIR"	cacls_jp1imm_operationlog.log	△
	cacls 操作ログ出力先 の実行結果 操作ログ出力先は次に示す共通定義に指定されたフォルダ [論理ホスト名¥JP1IMM¥OPERATION] "LOGFILEDIR"	cacls_jp1imm_operationlog.log	—

情報の種類	採取資料	ファイル名※1	View
JP1/Base のファイル一覧	dir Base パス /s の実行結果	dir_jp1base.log	△
	dir 共有フォルダ¥JP1Base /s の実行結果※2	dir_論理ホスト名_jp1base.log	—
JP1/IM - Manager(セントラルコンソール)のファイル一覧	dir Console パス /s の実行結果	dir_jp1cons.log	△
	dir 共有フォルダ¥JP1Cons /s の実行結果※2	dir_論理ホスト名_jp1cons.log	—
JP1/IM - View のファイル一覧	dir View パス /s の実行結果	dir_jp1coview.log	○
	Windows 限定 dir システムドライブ:¥ProgramData¥Hitachi¥jp1¥jp1_default¥JP1CoView /s の実行結果	dir_programdata_jp1coview.log	○
JP1/IM - Manager のファイル一覧	dir Manager パス /s の実行結果	dir_jp1imm.log	△
JP1/IM - Manager(セントラルスコープ)のファイル一覧	dir Scope パス /s の実行結果	dir_jp1scope.log	△
	dir 共有フォルダ¥JP1Scope /s の実行結果※2	dir_論理ホスト名_jp1scope.log	—
操作ログファイル出力先のファイル一覧	dir 操作ログ出力先 /s の実行結果 操作ログ出力先は次に示す共通定義に指定されたフォルダ [JP1_DEFAULT¥JP1IMM¥OPERATION] ”LOGFILEDIR”	dir_jp1imm_operationlog.log	△
	dir 操作ログ出力先 /s の実行結果 操作ログ出力先は次に示す共通定義に指定されたフォルダ [論理ホスト名¥JP1IMM¥OPERATION] ”LOGFILEDIR”	dir_jp1imm_operationlog.log	—
ネットワークアドレス解決のためのホスト名	jbsgethostbyname の実行結果	<ul style="list-style-type: none"> • jbsgethostbyname.log(標準出力) • jbsgethostbyname_err.log(標準エラー出力) 	△
	jbsgethostbyname 論理ホスト名 の実行結果※2	<ul style="list-style-type: none"> • jbsgethostbyname.log(標準出力) • jbsgethostbyname_err.log(標準エラー出力) 	—
ヘルスチェック	jbshcstatus -debug -a の実行結果	<ul style="list-style-type: none"> • jbshcstatus.log(標準出力) • jbshcstatus_err.log(標準エラー出力) 	△
	jbshcstatus -debug -a -h 論理ホスト名 の実行結果※2	<ul style="list-style-type: none"> • jbshcstatus.log(標準出力) • jbshcstatus_err.log(標準エラー出力) 	—
イベントサービスのプロセス稼働状態	• jevstat の実行結果	<ul style="list-style-type: none"> • jevstat.log(標準出力) • jevstat_err.log(標準エラー出力) 	△
	• jevstat 論理ホスト名の実行結果	<ul style="list-style-type: none"> • jevstat.log(標準出力) 	—

情報の種類	採取資料	ファイル名※1	View
		<ul style="list-style-type: none"> • jevstat_err.log(標準エラー出力) 	
イベントサービス以外のプロセス稼働状態	jbs_spmd_status の実行結果	<ul style="list-style-type: none"> • jbs_spmd_status.log(標準出力) • jbs_spmd_status_err.log(標準エラー出力) 	△
	jbs_spmd_status -h 論理ホスト名の の実行結果※2	<ul style="list-style-type: none"> • jbs_spmd_status.log(標準出力) • jbs_spmd_status_err.log(標準エラー出力) 	—
自動アクションの実行結果	jcashowa の実行結果※3	<ul style="list-style-type: none"> • jcashowa.log(標準出力) • jcashowa_err.log(標準エラー出力) 	△
	jcashowa -h 論理ホスト名 の実行 結果※2, ※3	<ul style="list-style-type: none"> • jcashowa.log(標準出力) • jcashowa_err.log(標準エラー出力) 	—
自動アクションの動作 状況	jcastatus の実行結果	<ul style="list-style-type: none"> • jcastatus.log(標準出力) • jcastatus_err.log(標準エラー出力) 	△
	jcastatus -h 論理ホスト名 の実行 結果※2	<ul style="list-style-type: none"> • jcastatus.log(標準出力) • jcastatus_err.log(標準エラー出力) 	—
自動アクション定義ファ イルの内容	jcastatus -d の実行結果	<ul style="list-style-type: none"> • jcastatus_d.log(標準出力) • jcastatus_d_err.log(標準エラー出力) 	△
	jcastatus -d -h 論理ホスト名 の実 行結果※2	<ul style="list-style-type: none"> • jcastatus_d.log(標準出力) • jcastatus_d_err.log(標準エラー出力) 	—
関連イベント発行サービ スの動作状況	jcoegsstatus の実行結果	<ul style="list-style-type: none"> • jcoegsstatus.log(標準出力) • jcoegsstatus_err.log(標準エラー出力) 	△
	jcoegsstatus -h 論理ホスト名 の実 行結果※2	<ul style="list-style-type: none"> • jcoegsstatus.log(標準出力) • jcoegsstatus_err.log(標準エラー出力) 	—
プロセス稼働状態	jco_spmd_status の実行結果	<ul style="list-style-type: none"> • jco_spmd_status.log(標準出力) • jco_spmd_status_err.log(標準エラー出力) 	△
	jco_spmd_status -h 論理ホスト名 の実行結果※2	<ul style="list-style-type: none"> • jco_spmd_status.log(標準出力) • jco_spmd_status_err.log(標準エラー出力) 	—
資料採取ツールの実行 結果	jim_log.bat コマンドの実行結果	jim_log_result.log	○
JP1/IM - Manager のライ センス情報	ライセンスライブラリ (HLICLIB) が インストール時に出力するトレース ログ, エラーログ	<ul style="list-style-type: none"> • hlicliberr{n}.log • hliclibmgrerr{n}.log • hliclibtrc{n}.log • hliclibmgrtrc{n}.log 	—
JP1/IM - View のライ センス情報	ライセンスライブラリ (HLICLIB) が インストール時に出力するトレース ログ, エラーログ	<ul style="list-style-type: none"> • hlicliberr{n}.log • hliclibmgrerr{n}.log • hliclibtrc{n}.log • hliclibmgrtrc{n}.log 	—

情報の種類	採取資料	ファイル名※1	View
Windows イベントログ	<ul style="list-style-type: none"> アプリケーション：システムルートフォルダ ¥system32¥config¥AppEvent.Evt システム：システムルートフォルダ ¥system32¥config¥SysEvent.Evt 	<ul style="list-style-type: none"> AppEvent(Backup).evt AppEvent(Backup).txt SysEvent(Backup).evt SysEvent(Backup).txt 	○
ホストに登録された jplhosts2 情報	<ul style="list-style-type: none"> jbshosts2export の実行結果 	<ul style="list-style-type: none"> jbshosts2export.log(標準出力) jbshosts2export_err.log(標準エラー出力) 	△
	<ul style="list-style-type: none"> jbshosts2export -h 論理ホスト名の実行結果 	<ul style="list-style-type: none"> jbshosts2export.log(標準出力) jbshosts2export_err.log(標準エラー出力) 	—
メディアセンス機能の ON/OFF 情報	レジストリ HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥Tcpip¥Parameters¥DisableDHCPMediaSense の値をreg コマンドで表示した結果	DisableDHCPMediaSense_reg.txt	—
サーバ証明書の情報 (CN と SAN の設定値、有効期限)	openssl x509 -noout -in サーバ証明書ファイル -subject -dates の実行結果	<ul style="list-style-type: none"> openssl_x509_server.log(標準出力) openssl_x509_server_err.log(標準エラー出力) 	—
サーバ証明書と秘密鍵の 整合性情報 (modulus)	<ul style="list-style-type: none"> openssl rsa -noout -in 秘密鍵ファイル -modulus の実行結果 openssl x509 -noout -in サーバ証明書ファイル -modulus の実行結果 	<ul style="list-style-type: none"> openssl_keymatching.log(標準出力) openssl_keymatching_err.log(標準エラー出力) 	—
インテリジェント統合管理データベースのファイル一覧	<ul style="list-style-type: none"> dir 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フォルダ※ /s の実行結果 dir インテリジェント統合管理データベースのデータ格納フォルダ※ /s の実行結果 	<ul style="list-style-type: none"> dir_jp1imgndb_env.log dir_jp1imgndb_data.log 	—

(凡例)

○：jcoview_log.bat コマンドで採取する

△：JP1/IM - View と同一ホストに JP1/Base, JP1/IM - Manager がインストールされている場合だけ、jcoview_log.bat コマンドで採取する

—：jcoview_log.bat コマンドで採取しない

注※1 資料採取ツールを実行したあとの格納先でのファイル名です。格納先については、次を参照してください。

- マニュアル「JP1/Integrated Management 3 - Manager 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)
- マニュアル「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)

注※2 論理ホスト (クラスター) 環境の資料を採取する際に採取できます。

注※3 <セントラルコンソールのインストールフォルダ>¥log¥action¥<アクション情報ファイル名>が存在する場合だけ採取します。

(b) JP1 の情報

JP1 に関する次の情報の採取が必要です。これらの情報は資料採取ツールで採取できます。また、ネットワーク接続でのトラブルの場合、接続先マシン上のファイルの採取も必要です。

なお、資料採取ツール (jim_log.bat コマンド, jcoview_log.bat コマンド) では採取できる資料に違いがあります。次の表に示す資料は, jim_log.bat コマンドを実行するとすべて採取されます。jcoview_log.bat コマンドを実行するとき採取できる資料については右端の列に示します。

表 12-16 JP1 の情報 (Windows)

情報の種類		採取資料	ファイル名※1	View
JP1/IM, JP1/ Base 共通	統合トレースログ	システムドライブ:Program Files¥Hitachi¥HNTRLib2¥spool	デフォルトで次のファイル hntr2[1 2 3 4].log	○
JP1/IM - Manager(コ ンポーネン ト 共通)	パッチ情報	Manager パス¥PATCHLOG.TXT	Patchlog_jp1imm.txt	—
	形名, バージョン 情報	Manager パス¥Version.txt	Version.txt	—
	ライセンス種別, 使用期限	Manager パス¥ProductInfo.txt	ProductInfo.txt	—
	設定および定義 ファイル	Manager パス¥conf¥以下のファイル	左記ファイルのコピーファ イル	—
	ログファイル	Manager パス¥log¥以下のファイル	左記ファイルのコピーファ イル	—
	操作ログファイル	次に示す共通定義に指定されたフォルダ以下 のファイル [JP1_DEFAULT¥JP1IMM¥OPERATION] "LOGFILEDIR"	左記ファイルのコピーファ イル	—
		次に示す共通定義に指定されたフォルダ以下 のファイル [論理ホスト¥JP1IMM¥OPERATION] "LOGFILEDIR"	左記ファイルのコピーファ イル	—
JP1/IM - Manager(セ ントラルコン ソール)	設定および定義 ファイル	Console パス¥conf¥以下のファイル	左記ファイルのコピーファ イル	—
		共有フォルダ¥JP1Cons¥conf¥以下のファイル ※2	左記ファイルのコピーファ イル	—
	共通定義情報	Console パス¥default¥以下のファイル	左記ファイルのコピーファ イル	—
	ログファイル	Console パス¥log¥以下のファイル	左記ファイルのコピーファ イル	—
		共有フォルダ¥JP1Cons¥log¥以下のファイル※ 2	左記ファイルのコピーファ イル	—

情報の種類		採取資料	ファイル名※1	View	
	応答待ちイベント 滞留ファイル※3	Console パス¥log¥response¥以下のファイル	左記ファイルのコピーファイル	—	
		共有フォルダ¥jp1cons¥log¥response¥以下のファイル	左記ファイルのコピーファイル	—	
	関連イベント発行 履歴ファイル	Console パス¥operation¥evgen¥以下のファイル	左記ファイルのコピーファイル	—	
		共有フォルダ¥JP1Cons¥operation¥evgen¥以下のファイル※2	左記ファイルのコピーファイル	—	
	共通除外履歴ファイルおよび共通除外条件定義履歴ファイル	Console パス¥operation¥comexcl¥以下のファイル	左記ファイルのコピーファイル	—	
		共有フォルダ ¥JP1Cons¥operation¥comexcl¥以下のファイル※2	左記ファイルのコピーファイル	—	
JP1/IM - Manager(セントラルス コープ)	設定および定義 ファイル	Scope パス¥conf¥以下のファイル	左記ファイルのコピーファイル	—	
		共有フォルダ¥JP1Scope¥conf¥以下のファイル※2	左記ファイルのコピーファイル	—	
	共通定義情報	Scope パス¥default¥以下のファイル	左記ファイルのコピーファイル	—	
	ログファイル	Scope パス¥log¥以下のファイル	左記ファイルのコピーファイル	—	
		共有フォルダ¥JP1Scope¥log¥以下のファイル※2	左記ファイルのコピーファイル	—	
	DB 情報	Scope パス¥database¥以下のファイル	左記ファイルのコピーファイル	—	
		共有フォルダ¥JP1Scope¥database¥以下のファイル※2	左記ファイルのコピーファイル	—	
	JP1/IM - Manager(インテリジェント 統合管理基 盤)	設定および定義 ファイル	Manager パス¥conf¥imdd¥以下のファイル	左記ファイルのコピーファイル	—
			共有フォルダ¥jp1imm¥conf¥imdd¥以下のファイル※2	左記ファイルのコピーファイル	—
		ログファイル	Manager パス¥log¥imdd¥以下のファイル	左記ファイルのコピーファイル	—
共有フォルダ¥jp1imm¥log¥imdd¥以下のファイル※2			左記ファイルのコピーファイル	—	
プラグインファイル		Manager パス¥plugin¥以下のファイル	左記ファイルのコピーファイル	—	

情報の種類		採取資料	ファイル名※1	View
	対処アクション実行履歴ファイル	共有フォルダ¥plugin¥以下のファイル※2	左記ファイルのコピーファイル	—
		Manager パス¥log¥suggestion¥以下のファイル	左記ファイルのコピーファイル	—
		共有フォルダ¥log¥suggestion¥以下のファイル※2	左記ファイルのコピーファイル	—
JP1/IM - Manager(IM 構成管理)	設定および定義ファイル	Manager パス¥conf¥imcf¥以下のファイル	左記ファイルのコピーファイル	—
		共有フォルダ¥jplimm¥conf¥imcf¥以下のファイル※2	左記ファイルのコピーファイル	—
	共通定義情報	Manager パス¥system¥default¥new¥imcf¥以下のファイル	左記ファイルのコピーファイル	—
	ログファイル	Manager パス¥log¥imcf¥以下のファイル	左記ファイルのコピーファイル	—
		共有フォルダ¥jplimm¥log¥imcf¥以下のファイル※2	左記ファイルのコピーファイル	—
JP1/IM - Manager(インテリジェント統合管理データベース) ※4	設定および定義ファイル	Manager パス¥conf¥imgndb¥以下のファイル	左記ファイルのコピーファイル	—
		共有フォルダ¥jplimm¥conf¥imgndb¥以下のファイル※2	左記ファイルのコピーファイル	—
		物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格納フォルダ¥imgndb¥以下の次のファイル <ul style="list-style-type: none"> • postgresql.conf • pg_hba.conf • pg_ident.conf • postmaster.pid • postmaster.opts • PG_VERSION 	左記ファイルのコピーファイル	—
		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格納フォルダ¥imgndb 論理ホスト番号¥以下の次のファイル <ul style="list-style-type: none"> • postgresql.conf • pg_hba.conf • pg_ident.conf • postmaster.pid • postmaster.opts • PG_VERSION 	左記ファイルのコピーファイル	—

情報の種類		採取資料	ファイル名※1	View
		物理ホストの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フォルダ ¥imgndbbin¥promscale¥以下の次のファイル	左記ファイルのコピーファイル	—
		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インストール先フォルダ ¥imgndbbin 論理ホスト番号¥promscale¥以下の次のファイル	左記ファイルのコピーファイル	—
	ログファイル	Manager パス¥log¥imgndb¥以下のファイル	左記ファイルのコピーファイル	—
		共有フォルダ¥jp1imm¥log¥imgndb¥以下のファイル	左記ファイルのコピーファイル	—
	データベースの状態	物理ホストの次のコマンドの実行結果 (jimgndb_status.txt)	左記ファイルのコピーファイル	—
		論理ホストの次のコマンドの実行結果 (jimgndb_status.txt)	左記ファイルのコピーファイル	—
JP1/IM - Agent(統合エージェント管理基盤)	定義ファイル	Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥以下の採取が必要なファイル	<ul style="list-style-type: none"> • AWS 定義ファイル (aws_settings.conf) • プロパティ表示名定義ファイル (property_labels.conf) • Node exporter のメトリック定義ファイル (metrics_node_exporter.conf) • Windows exporter のメトリック定義ファイル (metrics_windows_exporter.conf) • Windows exporter (プロセス監視) のメトリック定義ファイル (metrics_windows_e 	—

情報の種類		採取資料	ファイル名※1	View
			<ul style="list-style-type: none"> xporter_process.conf) Blackbox exporter のメトリック定義ファイル (metrics_blackbox_exporter.conf) Yet another cloudwatch exporter のメトリック定義ファイル (metrics_ya_cloudwatch_exporter.conf) コンテナ監視のメトリック定義ファイル (metrics_kubernetes.conf) Fluentd のメトリック定義ファイル (metrics_fluentd.conf) ユーザー独自の Exporter のメトリック定義ファイル (metrics_任意のPrometheus のトレンド名.conf) Process exporter のメトリック定義ファイル (metrics_process_exporter.conf) Promitor のメトリック定義ファイル (metrics_promitor.conf) Script exporter のメトリック定義ファイル (metrics_script_exporter.conf) 	
		Manager パス ¥conf¥imdd¥plugin¥jp1pccs¥user¥以下の採取が必要なファイル	ユーザー独自の Exporter のメトリック定義ファイル (metrics_任意のPrometheus のトレンド名.conf)	—
		Manager パス¥conf¥imdd¥imagent¥以下の採取が必要なファイル	<ul style="list-style-type: none"> imbase 設定ファイル (jpc_imbase.json) 	—

情報の種類		採取資料	ファイル名※1	View
			<ul style="list-style-type: none"> • imbaseproxy 設定ファイル (jpc_imbaseproxy.js on) • 統合エージェント管理基盤のサーバ証明書ファイル 	
	ログファイル	Manager パス ¥conf¥imdd¥imagent¥imbase¥以下の採取が必要なファイル	統合エージェント管理基盤 (imbase) のログ	—
		Manager パス ¥conf¥imdd¥imagent¥imbaseproxy¥以下の採取が必要なファイル	統合エージェント管理基盤 (imbaseproxy) のログ	—
		Manager パス¥conf¥imdd¥imagent¥tools¥以下の採取が必要なファイル	コマンドなどのログ	—
		Manager パス¥conf¥imdd¥jp1pccs¥以下の採取が必要なファイル	製品プラグインのログ	—
JP1/IM - View	パッチ情報	View パス¥Patchlog.txt	Patchlog_jp1coview.txt	○
	形名, バージョン情報	View パス¥Version.txt	Version.txt	—
	ライセンス種別, 使用期限	View パス¥ProductInfo.txt	ProductInfo.txt	—
	設定および定義ファイル	View パス¥conf¥以下のファイル	左記ファイルのコピーファイル	○
		システムドライブ:¥ProgramData¥Hitachi¥jp1¥jp1_default¥JP1CoView¥conf¥以下のファイル	左記ファイルのコピーファイル	○
	共通定義情報	View パス¥default¥以下のファイル	左記ファイルのコピーファイル	○
	ログファイル	システムドライブ:¥ProgramData¥Hitachi¥jp1¥jp1_default¥JP1CoView¥log¥以下のファイル	左記ファイルのコピーファイル	○
JP1/Base	パッチ情報	Base パス¥PatchLog.txt	Patchlog_jp1base.txt	—
	形名, バージョン情報	Base パス¥Version.txt	Version.txt	—
	ライセンス種別, 使用期限	Base パス¥ProductInfo.txt	ProductInfo.txt	—
	設定および定義ファイル	Base パス¥conf¥以下のファイル	左記ファイルのコピーファイル	—

情報の種類		採取資料	ファイル名 ^{※1}	View
		共有フォルダ $\%JP1Base\%conf\%$ 以下のファイル ^{※2}	左記ファイルのコピーファイル	—
	共通定義情報	Base パス $\%default\%$ 以下のファイル	左記ファイルのコピーファイル	—
	ログファイル	Base パス $\%log\%$ 以下のファイル	左記フォルダ配下のCOMMAND 以外の全ファイル	—
		共有フォルダ $\%JP1Base\%log\%$ 以下のファイル ^{※2}	左記フォルダ配下のCOMMAND 以外の全ファイル	—
	プラグインサービスの設定ファイル	Base パス $\%plugin\%conf\%$ 以下のファイル	左記ファイルのコピーファイル	—
	ログおよびテンポラリファイル	Base パス $\%sys\%tmp\%$ 以下のファイル	左記ファイルのコピーファイル	—
		共有フォルダ $\%JP1Base\%event\%$ ^{※2}	左記フォルダ配下のIMEvent*. * 以外の全ファイル	—
	コマンド実行履歴ファイル	Base パス $\%log\%COMMAND\%$ 以下のファイル	左記ファイルのコピーファイル	—
		共有フォルダ $\%JP1Base\%log\%COMMAND\%$ 以下のファイル ^{※2}	左記ファイルのコピーファイル	—
	イベント DB	Base パス $\%sys\%event\%servers\%default\%$ 以下のファイル	左記ファイルのコピーファイル	—
共有フォルダ $\%JP1Base\%event\%$ ^{※2}		IMEvent*. *	—	

(凡例)

○ : jcoview_log.bat コマンドで採取する

— : jcoview_log.bat コマンドで採取しない

注※1 資料採取ツールを実行したあとの格納先でのファイル名です。格納先については、次を参照してください。

- マニュアル「JP1/Integrated Management 3 - Manager 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)
- マニュアル「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)

注※2 論理ホスト (クラスタ) 環境の資料を採取する際に採取できます。

注※3 応答待ちイベント滞留ファイルは、応答待ちイベント管理機能を有効にすると作成されます。jim_log.bat コマンドのオプションによって採取しないこともできます。詳細については、「11.5.2 jim_log.bat (Windows 限定)」を参照してください。

注※4 インテリジェント統合管理データベースのログは、資料採取ツールの採取対象外です。インテリジェント統合管理データベースのログの詳細については、「1.3.2(1) インテリジェント統合管理データベースが出力するログの確認」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を使用している場合、次に示すケースに該当するときは、手動で個別に採取してください。

- インテリジェント統合管理データベースに関するエラーメッセージが出力され、そのメッセージのオペレーターの取る処置に、インテリジェント統合管理データベースのログを採取するように記載されているケース
- インテリジェント統合管理データベースに対するトレンドデータの格納または取得で、「KAJY6200」で始まるエラーメッセージが出力され、そのメッセージの対処方法で問題が解決できないケース

インテリジェント統合管理データベースのログファイルは、資料採取ツールでほかの資料を採取した直後に、合わせて採取してください（ログファイルを採取するまでの期間が1週間を経過するとログがラップします）。

なお、インテリジェント統合管理データベースのログファイルは、インテリジェント統合管理データベースのバックアップ対象に含まれるため、ディスク容量に余裕がある場合は、バックアップを取得して採取してもかまいません。バックアップの手順については、「1.2.2(7) インテリジェント統合管理データベースのバックアップ・リカバリー手順」を参照してください。

注※5 -ri および-rs オプション付きの実行結果は、データベースの稼働時だけ取得できます。

(c) オペレーション内容

トラブル発生時のオペレーション内容について次に示す情報が必要です。

- オペレーション内容の詳細
- 発生時刻
- マシン構成（各 OS のバージョン、ホスト名、セントラルコンソールの構成）
- 再現性
- JP1/IM - View からログインしている場合のログインユーザー名

(d) 画面上のエラー情報

次に示すハードコピーを採取してください。

- エラーダイアログボックスのハードコピー（および詳細ボタンがある場合はその内容）

(e) ユーザーダンプ (Windows 限定)

Windows で JP1/IM - View のプロセスがアプリケーションエラーで停止した場合は、ユーザーダンプを採取してください。

(f) リモート監視時の RAS 情報

リモート監視時にトラブルが発生した場合、ユーザー側で RAS 情報を採取する必要があります。RAS 情報の採取方法の詳細については、「12.4.1(1)(g)RAS 情報を採取する」を参照してください。

(g) IM 管理ノード関連ファイル

インテリジェント統合管理基盤を使用している場合は、次の情報を採取してください。

- jddcreatetree コマンドの-o オプションで指定したフォルダ以下のファイル
- jddupdatetree コマンドの-i オプションで指定したフォルダ以下のファイル

(2) UNIX の場合

(a) OS のシステム情報

OS に関する次の情報の採取が必要です。これらの情報は資料採取ツールで採取できます。

表 12-17 OS のシステム情報 (UNIX)

情報の種類	採取資料	ファイル名※1
インストール済み日立製品情報	/etc/.hitachi/pplistd/pplistd	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} pplistd
Hitachi PP Installer でインストールされた製品情報	/etc/.hitachi/bin/SHOWPP による出力結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} SHOWPP
Hitachi PP Installer のインストールログファイル	/etc/.hitachi/.install.log*	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} .install.log*
Hitachi PP Installer のアンインストールログファイル	/etc/.hitachi/.uninstall.log*	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} .uninstall.log*
共通定義情報	/opt/jp1/hcclibcfnf/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
JP1/IM - Manager(セントラルコンソール)の core の解析情報(バックトレース)※6	seraph による解析結果 /var/opt/jp1cons	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} core_モジュール名.log
	seraph による解析結果 共有ディレクトリ/jp1cons/log※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} core_モジュール名.log
JP1/IM - Manager(セントラルスコープ)の core の解析情報(バックトレース)※6	seraph による解析結果 /var/opt/jp1scope	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} core_モジュール名.log
	seraph による解析結果 共有ディレクトリ/jp1scope/log※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} core_モジュール名.log
JP1/IM - Manager(インテリジェント統合管理基盤)の core の解析情報(バックトレース)※6	seraph による解析結果 /var/opt/jp1imm/log	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} core_モジュール名.log
	seraph による解析結果 共有ディレクトリ/jp1imm/log※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} core_モジュール名.log
JP1/IM - Manager の ディストリビューション・リリースファイル	実行環境がどのディストリビューションか判別するための情報	<ul style="list-style-type: none"> Linux /etc/redhat-release Oracle Linux /etc/oracle-release SUSE Linux /etc/SuSE-release

情報の種類	採取資料	ファイル名※1
JP1/Base インストールログファイル	/tmp/HITACHI_JP1_INST_LOG/jp1base_inst{1 2 3 4 5}.log	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} jp1base_inst{1 2 3 4 5}.log
JP1/IM - Manager インストールログファイル	/tmp/HITACHI_JP1_INST_LOG/jp1imm_inst{1 2 3 4 5}.log	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} jp1imm_inst{1 2 3 4 5}.log
ファイル一覧	<ul style="list-style-type: none"> ls -lRa /opt/jp1imm の実行結果 ls -lRa /var/opt/jp1imm の実行結果 ls -lRa /opt/jp1cons の実行結果 ls -lRa /etc/opt/jp1cons の実行結果 ls -lRa /var/opt/jp1cons の実行結果 ls -lRa /opt/jp1scope の実行結果 ls -lRa /etc/opt/jp1scope の実行結果 ls -lRa /var/opt/jp1scope の実行結果 ls -lRa /opt/jp1base の実行結果 ls -lRa /etc/opt/jp1base の実行結果 ls -lRa /var/opt/jp1base の実行結果 ls -lRa ユーザが指定したセットアップ情報ファイル内のIMBENVDIR の値の実行結果 ls -lRa ユーザが指定したセットアップ情報ファイル内のIMBBDIR の値の実行結果 ls -lRa /etc/opt/jp1imm の実行結果 ls -lRa /tmp/HITACHI_JP1_INST_LOG の実行結果 ls -lRa /etc/.hitachi の実行結果 ls -lRa /etc/opt/.hlic の実行結果 ls -lRa 操作ログ出力先の実行結果※4 ls -lRa 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実行結果 ls -lRa インテリジェント統合管理データベースのデータ格納ディレクトリの実行結果 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} inst_dir.log
	<ul style="list-style-type: none"> ls -lRa 共有ディレクトリ/jp1cons の実行結果※2 ls -lRa 共有ディレクトリ/jp1scope の実行結果※2 ls -lRa 共有ディレクトリ/jp1base の実行結果※2 ls -lRa 共有ディレクトリ/event の実行結果※2 ls -lRa 操作ログ出力先の実行結果※5 ls -lRa 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実行結果 ls -lRa インテリジェント統合管理データベースのデータ格納ディレクトリの実行結果 	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} share_dir.log
ファイル一覧 (シンボリックリ)	<ul style="list-style-type: none"> ls -lRaL /opt/jp1imm の実行結果 ls -lRaL /var/opt/jp1imm の実行結果 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} inst_dir_lRaL.log

情報の種類	採取資料	ファイル名※1
リンク先のファイル・フォルダを参照する-L オプションを付与)	<ul style="list-style-type: none"> ls -lRaL /opt/jp1cons の実行結果 ls -lRaL /etc/opt/jp1cons の実行結果 ls -lRaL /var/opt/jp1cons の実行結果 ls -lRaL /opt/jp1scope の実行結果 ls -lRaL /etc/opt/jp1scope の実行結果 ls -lRaL /var/opt/jp1scope の実行結果 ls -lRaL /opt/jp1base の実行結果 ls -lRaL /etc/opt/jp1base の実行結果 ls -lRaL /var/opt/jp1base の実行結果 ls -lRaL ユーザが指定したセットアップ情報ファイル内のIMDBENVDIR の値の実行結果 ls -lRaL ユーザが指定したセットアップ情報ファイル内のIMDBDIR の値の実行結果 ls -lRaL /etc/opt/jp1imm の実行結果 ls -lRaL /tmp/HITACHI_JP1_INST_LOG の実行結果 ls -lRaL /etc/.hitachi の実行結果 ls -lRaL /etc/opt/.hlic の実行結果 ls -lRaL 操作ログ出力先の実行結果※4 ls -lRaL 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実行結果 ls -lRaL インテリジェント統合管理データベースのデータ格納ディレクトリの実行結果 	
	<ul style="list-style-type: none"> ls -lRaL 共有ディレクトリ/jp1cons の実行結果 ls -lRaL 共有ディレクトリ/jp1scope の実行結果 ls -lRaL 共有ディレクトリ/jp1base の実行結果 ls -lRaL 共有ディレクトリ/event の実行結果 ls -lRaL 操作ログ出力先の実行結果※5 ls -lRaL 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実行結果 ls -lRaL インテリジェント統合管理データベースのデータ格納ディレクトリの実行結果 	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} share_lRaL_dir.log
資料採取日時	date の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} jp1_default_imm_2nd.tar. {Z gz} 論理ホスト名_imm_1st.tar. {Z gz} 論理ホスト名_imm_2nd.tar. {Z gz} date.log
ディスク情報	df -k の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} df.log
btrfs ファイルシステム情報	Linux にbtrfs がインストールされている場合だけ <ul style="list-style-type: none"> btrfs filesystem show --all-device の結果 	<ul style="list-style-type: none"> Linux:jp1_default_imm_1st.tar.gz df.log

情報の種類	採取資料	ファイル名※1
自動起動サービス (systemd) によるプロセス稼働情報	Linux にsystemd がインストールされている場合だけ systemctl --all, systemctl list-unit-files, systemctl status jp1_base, systemctl status jp1_cons, systemctl status /usr/lib/systemd/system/2248- *start.service の結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz systemctl.log
マシンの環境変数	env の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} env.log
マシンに設定されているホスト名の設定	/etc/hosts (Linux)	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} hosts
プロセス間通信の共有メモリーステータス	ipcs -ma の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} ipcs.log
ネットワークアドレス解決のためのホスト名	jbsgethostbyname の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} jbsgethostbyname.log(標準出力) jbsgethostbyname_err.log(標準エラー出力)
	jbsgethostbyname 論理ホスト名の実行結果※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar.{Z gz} jbsgethostbyname_論理ホスト名.log
ヘルスチェック	jbshcstatus -debug -a の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} jbshcstatus.log(標準出力) jbshcstatus_err.log(標準エラー出力)
	jbshcstatus -debug -a -h 論理ホスト名 の実行結果※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar.{Z gz} jbshcstatus.log(標準出力) jbshcstatus_err.log(標準エラー出力)
イベントサービスのプロセス稼働状態	jevstat の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} jevstat.log(標準出力) jevstat_err.log(標準エラー出力)
	jevstat 論理ホスト名の実行結果	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar.{Z gz} jevstat.log(標準出力) jevstat_err.log(標準エラー出力)
イベントサービス以外のプロセス稼働状態	jbs_spmd_status の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} jbs_spmd_status.log(標準出力) jbs_spmd_status_err.log(標準エラー出力)
	jbs_spmd_status -h 論理ホスト名 の実行結果※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar.{Z gz} jbs_spmd_status.log(標準出力)

情報の種類	採取資料	ファイル名※1
		<ul style="list-style-type: none"> • jbs_spmd_status_err.log(標準エラー出力)
自動アクションの実行結果	jcashowa の実行結果※3	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jcashowa.log(標準出力) • jcashowa_err.log(標準エラー出力)
	jcashowa -h 論理ホスト名 の実行結果※2, ※3	<ul style="list-style-type: none"> • 論理ホスト名_imm_1st.tar.{Z gz} • jcashowa.log(標準出力) • jcashowa_err.log(標準エラー出力)
自動アクション機能の動作状態	jcastatus の実行結果	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jcastatus.log(標準出力) • jcastatus_err.log(標準エラー出力)
	jcastatus -h 論理ホスト名 の実行結果※2	<ul style="list-style-type: none"> • 論理ホスト名_imm_1st.tar.{Z gz} • jcastatus.log(標準出力) • jcastatus_err.log(標準エラー出力)
自動アクション定義ファイルの内容	jcastatus -d の実行結果	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jcastatus_d.log(標準出力) • jcastatus_d_err.log(標準エラー出力)
	jcastatus -d -h 論理ホスト名 の実行結果※2	<ul style="list-style-type: none"> • 論理ホスト名_imm_1st.tar.{Z gz} • jcastatus_d.log(標準出力) • jcastatus_d_err.log(標準エラー出力)
関連イベント発行サービスの動作状況	jcoegsstatus の実行結果	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jcoegsstatus.log(標準出力) • jcoegsstatus_err.log(標準エラー出力)
	jcoegsstatus -h 論理ホスト名 の実行結果※2	<ul style="list-style-type: none"> • 論理ホスト名_imm_1st.tar.{Z gz} • jcoegsstatus.log(標準出力) • jcoegsstatus_err.log(標準エラー出力)
プロセス稼働状態	jco_spmd_status の実行結果	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jco_spmd_status.log(標準出力) • jco_spmd_status_err.log(標準エラー出力)
	jco_spmd_status -h 論理ホスト名 の実行結果※2	<ul style="list-style-type: none"> • 論理ホスト名_imm_1st.tar.{Z gz} • jco_spmd_status.log(標準出力) • jco_spmd_status_err.log(標準エラー出力)
資料採取ツールの実行結果	jim_log.sh コマンドの実行結果	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jim_log_result.log
IP アドレスの取得	ifconfig -a	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • ifconfig.log

情報の種類	採取資料	ファイル名※1
	ip addr show	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz ip_addr_show.log
NIC の実装状況	netstat -ai の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} netstat_ai.log
	ip -s link	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz ip_s_link.log
ネットワーク統計情報	netstat -nap の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} netstat_na.log
	ss -nap	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz ss_na.log
マシンに設定されているユーザーの一覧	/etc/passwd	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} passwd
プロセス一覧	ps -elfa の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} ps.log
マシンに設定されているサービスの設定	/etc/services	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} services
メモリー情報	cat /proc/meminfo	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} swapinfo.log
システム診断情報	dmesg の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} sys_info.log
シスログ (syslog)	/var/log/messages	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} syslog.log
ジャーナル (journal)	journalctl -l --no-pager の実行結果 SUSE Linux 15 以降の場合に取得する	journal.log
jcogencore コマンドで出力した JP1/IM - Manager(セン トラルコンソール)の core の解析情報(バック トレース)※6	seraph による解析結果 /var/opt/jp1cons	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} trace_モジュール名.log
	seraph による解析結果 共有ディレクトリ/jp1cons/log (jcogencore で出力したcore)※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} trace_モジュール名.log
OS のバージョン情報	uname -a の実行結果	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} uname_a.log
カーネルパラメーター情報	<ul style="list-style-type: none"> sysctl -a の実行結果 ulimit -a の実行結果 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} sysctl.log

情報の種類	採取資料	ファイル名※1
		<ul style="list-style-type: none"> • ulimit.log
ページサイズ情報	採取しない	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • pagesize.log
OSのパッチ適用状況	rpm -qaの実行結果	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • rpm.log
ディストリビューション情報	/etc/*-release	*-release
JP1/IM - Managerのライセンス情報	ライセンスライブラリ (HLICLIB) がインストール時に出力するトレースログ, エラーログ	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • hlicliberr{n}.log • hliclibmgrerr{n}.log • hliclibtrc{n}.log • hliclibmgrtrc{n}.log
init デーモンが使用するプロセス起動情報	<ul style="list-style-type: none"> • /etc/init 配下のファイル Linux 6 だけで取得する。	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • 左のディレクトリ配下のファイル
ディスクマウント情報	/etc/fstab	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • fstab • filesystems
ホストに登録されたjp1hosts2情報	jbshosts2exportの実行結果	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jbshosts2export.log(標準出力) • jbshosts2export_err.log(標準エラー出力)
	jbshosts2export -h 論理ホスト名の実行結果	<ul style="list-style-type: none"> • 論理ホスト名_imm_1st.tar.{Z gz} • jbshosts2export.log(標準出力) • jbshosts2export_err.log(標準エラー出力)
サーバ証明書の情報 (CN と SAN の設定値, 有効期限)	openssl x509 -noout -in サーバ証明書ファイル -subject -datesの実行結果	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • openssl_x509_server.log(標準出力) • openssl_x509_server_err.log(標準エラー出力)
サーバ証明書と秘密鍵の整合性情報 (modulus)	<ul style="list-style-type: none"> • openssl rsa -noout -in 秘密鍵ファイル -modulusの実行結果 • openssl x509 -noout -in サーバ証明書ファイル -modulusの実行結果 	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • openssl_keymatching.log(標準出力) • openssl_keymatching_err.log(標準エラー出力)

注※1 資料採取ツールを実行したあとの圧縮ファイルおよび解凍後のファイル名です (圧縮ファイル, 解凍後のファイルの順に記載しています)。

圧縮ファイルは Windows の場合は, tar.Z 形式, Linux の場合は, tar.gz 形式で作成されます。

圧縮ファイルの内部ディレクトリ構成については, マニュアル「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) を参照してください。

注※2 論理ホスト（クラスタ）環境の資料を採取する際に採取できます。

注※3 /var/opt/jp1cons/log/action/<アクション情報ファイル名>が存在する場合だけ採取します。

注※4 操作ログ出力先は次に示す共通定義に指定されたディレクトリです。

```
[JP1_DEFAULT¥JP1IMM¥OPERATION]
"LOGFILEDIR"
```

注※5 操作ログ出力先は次に示す共通定義に指定されたディレクトリです。

```
[論理ホスト名¥JP1IMM¥OPERATION]
"LOGFILEDIR"
```

注※6 OS の設定などでコアダンプファイルの生成を制限している場合、コアダンプファイルが生成されないことがあります。コアダンプファイルに関する設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「2.18.10 JP1/IM - Manager の障害に備えた設定（UNIX の場合）」を参照してください。

(b) JP1 の情報

JP1 に関する次の情報の採取が必要です。これらの情報は資料採取ツールで採取できます。また、ネットワーク接続でのトラブルの場合、接続先マシン上のファイルの採取も必要です。

表 12-18 JP1 の情報（UNIX）

情報の種類		採取資料	ファイル名※1
JP1/IM, JP1/ Base 共通	統合トレースログ	/var/opt/hitachi/HNTRLib2/spool/以下の全ファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} デフォルトで以下のファイル hntr2[1 2 3 4].log
JP1/IM - Manager(コン ポーネント共通)	パッチ適用履歴	/opt/jp1imm/patch_history	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} patch_history
	パッチログ情報	/opt/jp1imm/update.log	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} update.log
	ライセンス種別, 使用 期限	/var/opt/jp1imm/log/ProductInfo	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} ProductInfo
	管理ノードカウントの ログファイル	/var/opt/jp1imm/log/nodecount	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} jimmnodecount_cmd{1 2}.log
	操作ログファイル	次に示す共通定義に指定されたディレクトリ以下のファイル [JP1_DEFAULT¥JP1IMM¥OPERATION] "LOGFILEDIR"	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピー
		次に示す共通定義に指定されたディレクトリ以下のファイル [論理ホスト名¥JP1IMM¥OPERATION] "LOGFILEDIR"	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} 左記ファイルのコピー
JP1/IM - Manager(セン トラルコンソ ール)※4	自動起動および自動終 了スクリプト	/etc/opt/jp1cons/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル

情報の種類		採取資料	ファイル名※1
	設定および定義ファイル	/etc/opt/jp1cons/conf/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1cons/conf/以下のファイル※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	共通定義情報	/etc/opt/jp1cons/default/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	ログファイル	/var/opt/jp1cons/log/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1cons/log/以下のファイル※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	応答待ちイベント滞留ファイル※3	/var/opt/jp1cons/log/response/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1cons/log/response/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	jcogencore コマンドで出力した core の解析情報(Car ファイル)	car コマンドの結果 /var/opt/jp1cons/log (jcogencore で出力したcore)	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar. {Z gz} car_モジュール名.tar[.Z]
		car コマンドの結果 共有ディレクトリ/jp1cons/log (jcogencore で出力したcore)※2	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar. {Z gz} car_モジュール名.tar[.Z]
	core の解析情報(Car ファイル)	car コマンドの結果 /var/opt/jp1cons/log	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar. {Z gz} core_モジュール名_car.tar[.Z]
		car コマンドの結果 共有ディレクトリ/jp1cons/log※2	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar. {Z gz} core_モジュール名_car.tar[.Z]
	関連イベント発行履歴ファイル	/var/opt/jp1cons/operation/evgen/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1cons/operation/evgen※2	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar. {Z gz} 左記ファイルのコピーファイル
	共通除外履歴ファイルおよび共通除外条件定義履歴ファイル	/var/opt/jp1cons/operation/comexclude/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1cons/operation/comexclude※2	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar. {Z gz} 左記ファイルのコピーファイル
JP1/IM - Manager(セン トラルスコープ) ※4	設定および定義ファイル	/etc/opt/jp1scope/conf/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1scope/conf/以下のファイル※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル

情報の種類		採取資料	ファイル名※1
	共通定義情報	/etc/opt/jp1scope/default/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} 左記ファイルのコピーファイル
	ログファイル	/var/opt/jp1scope/log/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1scope/log/以下のファイル※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar.{Z gz} 左記ファイルのコピーファイル
	coreの解析情報(Carファイル)	car コマンドの結果 /var/opt/jp1scope/log	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar.{Z gz} core_モジュール名_car.tar[.Z]
		car コマンドの結果 共有ディレクトリ/jp1scope/log※2	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar.{Z gz} core_モジュール名_car.tar[.Z]
	DB 情報	/var/opt/jp1scope/database/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar.{Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1scope/database/以下のファイル※2	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar.{Z gz} 左記ファイルのコピーファイル
	JP1/IM - Manager(インテリジェント統合管理基盤)※4	設定および定義ファイル	/etc/opt/jp1imm/conf/imdd 以下のファイル
共有ディレクトリ/jp1imm/conf/imdd 以下のファイル			<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar.{Z gz} 左記ファイルのコピーファイル
ログファイル		/var/opt/jp1imm/log/imdd 以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1imm/log/imdd 以下のファイル	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar.{Z gz} 左記ファイルのコピーファイル
プラグインファイル		/etc/opt/jp1imm/plugin 以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz 左記ファイルのコピーファイル
		共有ディレクトリ/jp1imm/plugin 以下のファイル	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar.gz 左記ファイルのコピーファイル
対処アクション実行履歴ファイル		/var/opt/jp1imm/log/suggestion 以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz 左記ファイルのコピーファイル
		共有ディレクトリ/jp1imm/log/suggestion 以下のファイル	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar.gz 左記ファイルのコピーファイル
coreの解析情報(Carファイル)		car コマンドの結果 /var/opt/jp1im/log/imdd	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar.{Z gz} core_モジュール名_car.tar[.Z]
		car コマンドの結果 共有ディレクトリ/jp1im/log/imdd※2	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar.{Z gz} core_モジュール名_car.tar[.Z]

情報の種類		採取資料	ファイル名※1
JP1/IM - Manager(IM 構成管理)※4	設定および定義ファイル	/etc/opt/jp1imm/conf/imcf/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1imm/conf/imcf/以下のファイル※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	共通定義情報	/etc/opt/jp1imm/default/imcf/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	ログファイル	/var/opt/jp1imm/log/imcf/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1imm/log/imcf/以下のファイル※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	core の解析情報(Car ファイル)	car コマンドの結果 /var/opt/jp1imm/log	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar. {Z gz} ./var/opt/jp1imm/log/_jp1_default/core/core_モジュール名_car.tar[.Z]
car コマンドの結果 共有ディレクトリ/jp1imm/log※2		<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar. {Z gz} ./var/opt/jp1imm/log/_論理ホスト名/core/core_モジュール名_car.tar[.Z] 	
JP1/IM - Manager(インテリジェント統合管理データベース)※5	設定および定義ファイル	/etc/opt/jp1imm/conf/imgndb/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz 左記ファイルのコピーファイル
		共有ディレクトリ/jp1imm/conf/imgndb/以下のファイル	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar.gz 左記ファイルのコピーファイル
		物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格納フォルダ/imgndb/以下の次のファイル <ul style="list-style-type: none"> postgresql.conf pg_hba.conf pg_ident.conf postmaster.pid postmaster.opts PG_VERSION 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz 左記ファイルのコピーファイル
		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格納フォルダ/imgndb/以下の次のファイル <ul style="list-style-type: none"> postgresql.conf pg_hba.conf pg_ident.conf postmaster.pid postmaster.opts PG_VERSION 	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar.gz 左記ファイルのコピーファイル

情報の種類		採取資料	ファイル名※1
	ログファイル	/var/opt/jp1imm/log/imgndb/以下のファイル	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.gz • 左記ファイルのコピーファイル
		共有ディレクトリ/jp1imm/log/imgndb/以下のファイル	<ul style="list-style-type: none"> • 論理ホスト名_imm_2nd.tar.gz • 左記ファイルのコピーファイル
	データベースの状態	物理ホストの次のコマンドの実行結果 (jimgndb_status.txt) <ul style="list-style-type: none"> • jimgndbstatus • jimgndbstauts -ri※6 • jimgndbstatus -rs※6 	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.gz • 左記ファイルのコピーファイル
		論理ホストの次のコマンドの実行結果 (jimgndb_status.txt) <ul style="list-style-type: none"> • jimgndbstatus • jimgndbstauts -ri※6 • jimgndbstatus -rs※6 	<ul style="list-style-type: none"> • 論理ホスト名_imm_2nd.tar.gz • 左記ファイルのコピーファイル
JP1/IM - Agent(統合エージェント管理基盤)	定義ファイル	/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/以下の採取が必要なファイル	<ul style="list-style-type: none"> • AWS 定義ファイル (aws_settings.conf) • プロパティ表示名定義ファイル (property_labels.conf) • Node exporter のメトリック定義ファイル (metrics_node_exporter.conf) • Windows exporter のメトリック定義ファイル (metrics_windows_exporter.conf) • 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) • Blackbox exporter のメトリック定義ファイル (metrics_blackbox_exporter.conf) • Yet another cloudwatch exporter のメトリック定義ファイル (metrics_ya_cloudwatch_exporter.conf) • コンテナ監視のメトリック定義ファイル (metrics_kubernetes.conf) • Fluentd のメトリック定義ファイル (metrics_fluentd.conf) • ユーザー独自の Exporter のメトリック定義ファイル (metrics_任意のPrometheusのトレンド名.conf)

情報の種類		採取資料	ファイル名※1
			<ul style="list-style-type: none"> Process exporter のメトリック定義ファイル (metrics_process_exporter.conf) Promitor のメトリック定義ファイル (metrics_promitor.conf) Script exporter のメトリック定義ファイル (metrics_script_exporter.conf)
		/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/user/以下の採取が必要なファイル	ユーザー独自の Exporter のメトリック定義ファイル (metrics_任意のPrometheus のトレンド名.conf)
		/etc/opt/jp1imm/conf/imdd/imagent/以下の採取が必要なファイル	<ul style="list-style-type: none"> imbase 設定ファイル (jpc_imbase.json) imbaseproxy 設定ファイル (jpc_imbaseproxy.json) 統合エージェント管理基盤のサーバ証明書ファイル
	ログファイル	/var/opt/jp1imm/conf/imdd/imagent/imbase/以下の採取が必要なファイル	統合エージェント管理基盤 (imbase) のログ
		/var/opt/jp1imm/conf/imdd/imagent/imbaseproxy/以下の採取が必要なファイル	統合エージェント管理基盤 (imbaseproxy) のログ
		/var/opt/jp1imm/conf/imdd/imagent/tools/以下の採取が必要なファイル	コマンドなどのログ
		/var/opt/jp1imm/conf/imdd/jp1pccs/以下の採取が必要なファイル	製品プラグインのログ
JP1/Base	自動起動および自動終了スクリプト	/etc/opt/jp1base/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	設定および定義ファイル	/etc/opt/jp1base/conf/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1base/conf/以下のファイル※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	共通定義情報	/etc/opt/jp1base/default/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	プラグインサービスの設定ファイル	/opt/jp1base/conf/plugin/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
	パッチ適用履歴	/opt/jp1base/PatchInfo	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} PatchInfo
	パッチログ情報	/opt/jp1base/PatchLog	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} PatchLog

情報の種類		採取資料	ファイル名※1
	ログファイル	/var/opt/jp1base/log	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ディレクトリ配下のCOMMAND 以外の全ファイル
		共有ディレクトリ/jp1base/log※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} 左記ディレクトリ配下のCOMMAND 以外の全ファイル
	ログおよびテンポラリファイル	/var/opt/jp1base/sys/tmp/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_1st.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/event※2	<ul style="list-style-type: none"> 論理ホスト名_imm_1st.tar. {Z gz} 左記ディレクトリ配下のIMEvent*以外の全ファイル
	SES 設定ファイル	<ul style="list-style-type: none"> /tmp/.JP1_SES* /usr/tmp/jp1_ses /usr/lib/jp1_ses/log /usr/lib/jp1_ses/sys /usr/bin/jp1_ses/jp* /var/opt/jp1_ses 	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar. {Z gz} 左記ファイルのコピーファイル
	コマンド実行履歴ファイル	/var/opt/jp1base/log/COMMAND/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/jp1base /log/COMMAND/以下のファイル※2	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar. {Z gz} 左記ファイルのコピーファイル
	イベント DB	/var/opt/jp1base/sys/event/servers/default/以下のファイル	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar. {Z gz} 左記ファイルのコピーファイル
		共有ディレクトリ/event※2	<ul style="list-style-type: none"> 論理ホスト名_imm_2nd.tar. {Z gz} IMEvent*.*

注※1 資料採取ツールを実行したあとの圧縮ファイルおよび解凍後のファイル名です（圧縮ファイル，解凍後のファイルの順に記載しています）。

圧縮ファイルは Linux の場合は .tar.gz 形式で作成されます。

圧縮ファイルの内部ディレクトリ構成については，マニュアル「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) を参照してください。

注※2 論理ホスト（クラスタ）環境の資料を採取する際に採取できます。

注※3 応答待ちイベント滞留ファイルは，応答待ちイベント管理機能を有効にすると作成されます。jim_log.sh コマンドのオプションによって採取しないこともできます。詳細については，「11.5.3 jim_log.sh (UNIX 限定)」を参照してください。

注※4 OS の設定などでコアダンプファイルの生成を制限している場合，コアダンプファイルが生成されないことがあります。

コアダンプファイルに関する設定については，マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「2.18.10 JP1/IM - Manager の障害に備えた設定 (UNIX の場合)」を参照してください。

注※5 インテリジェント統合管理データベースのログは，資料採取ツールの採取対象外です。インテリジェント統合管理データベースのログの詳細については，「1.3.2(1) インテリジェント統合管理データベースが出力するログの確認」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を使用している場合，次に示すケースに該当するときは，手動で個別に採取してください。

- インテリジェント統合管理データベースに関係するエラーメッセージが出力され、そのメッセージのオペレーターの取る処置に、インテリジェント統合管理データベースのログを採取するように記載されているケース
- インテリジェント統合管理データベースに対するトレンドデータの格納または取得で、「KAJY6200」で始まるエラーメッセージが出力され、そのメッセージの対処方法で問題が解決できないケース

インテリジェント統合管理データベースのログファイルは、資料採取ツールでほかの資料を採取した直後に、合わせて採取してください（ログファイルを採取するまでの期間が1週間を経過するとログがラップします）。

なお、インテリジェント統合管理データベースのログファイルは、インテリジェント統合管理データベースのバックアップ対象に含まれるため、ディスク容量に余裕がある場合は、バックアップを取得して採取してもかまいません。バックアップの手順については、「[1.2.2\(7\) インテリジェント統合管理データベースのバックアップ・リカバリー手順](#)」を参照してください。

注※6 -ri および-rs オプション付きの実行結果は、データベースの稼働時だけ取得できます。

(c) オペレーション内容

トラブル発生時のオペレーション内容について次に示す情報が必要です。

- オペレーション内容の詳細
- 発生時刻
- マシン構成（各 OS のバージョン、ホスト名、セントラルコンソールの構成）
- 再現性
- JP1/IM - View からログインしている場合のログインユーザー名

(d) 画面上のエラー情報

次に示すハードコピーを採取してください。

- エラーダイアログボックスのハードコピー

(e) リモート監視時の RAS 情報

リモート監視時にトラブルが発生した場合、ユーザー側で RAS 情報を採取する必要があります。RAS 情報の採取方法の詳細については、「[12.4.1\(2\)\(f\)RAS 情報を採取する](#)」を参照してください。

(f) IM 管理ノード関連ファイル

インテリジェント統合管理基盤を使用している場合は、次の情報を採取してください。

- `jddcreatetree` コマンドの `-o` オプションで指定したディレクトリ以下のファイル
- `jddupdatetree` コマンドの `-i` オプションで指定したディレクトリ以下のファイル

12.3.2 JP1/IM - Agent に関する資料

次の資料を手動で採取します。

- システムログ

- OS 情報
- 通信状態
- プロセス情報
- サイレンスの設定
- 製品情報
- 自動起動および自動停止の設定
- コンテナ情報
- ファイル一覧
- インストール時の資料
- シークレットのキー

各資料の採取方法について、次に説明します。

(1) Windows の場合

「12.4.2(1)(a)統合エージェントホスト」, 「12.4.2(1)(b)クラスタシステムでの統合エージェントホスト」, および 「12.4.2(1)(c)コンテナでの統合エージェントホスト」 を参照してください。

(2) UNIX の場合

「12.4.2(2)(a)統合エージェントホスト」, 「12.4.2(2)(b)クラスタシステムでの統合エージェントホスト」, および 「12.4.2(2)(c)コンテナでの統合エージェントホスト」 を参照してください。

12.4 資料の採取方法

トラブルが発生したときに資料を採取する方法を次に示します。

12.4.1 JP1/IM - Manager の資料採取方法

(1) Windows の場合

(a) プロセスの状態を確認する

Windows のタスクマネージャを使用して、プロセスの動作状態を確認してください。正常に動作している場合に表示されるプロセスを次に示します。

■ JP1/IM - Manager

JP1/IM - Manager のプロセスについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 B.1(1) JP1/IM - Manager」を参照してください。

■ JP1/IM - View

JP1/IM - View のプロセスについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 B.1(1) JP1/IM - Manager」を参照してください。

■ JP1/IM - IM 構成管理・ビューアー

JP1/IM - IM 構成管理・ビューアーのプロセスを次に示します。なお、表内の括弧（ ）内の数値は同時に実行するプロセス数です。

表 12-19 JP1/IM - IM 構成管理・ビューアーのプロセス

親プロセス名	機能	子プロセス名	機能
jcfview.exe (3)	JP1/IM - IM 構成管理・ ビューアーの画面制御	jcfview_evt.exe (3)	スレッドダンプ出力イベントの送信
		java.exe (3)	JP1/IM - IM 構成管理・ビューアー の画面制御

一つのマシンからログインして起動できる JP1/IM - IM 構成管理・ビューアーの数は三つまでです。JP1/IM - IM 構成管理・ビューアーを一つ起動するごとに、一つのプロセスが起動します。

(b) JP1/IM 用スレッドダンプを出力する

■ JP1/IM - View

次の手順に従いダンプファイルを出力してください。

1. タスク マネージャを開く。

2. [アプリケーション] ページ上で JP1/IM - View を選択し、ポップアップメニューから [手前に表示] を選択する。

これによって操作不能になった JP1/IM - View かどうかを特定します。操作不能な JP1/IM - View を特定できた場合、次に進みます。

3. ポップアップメニューから [プロセスを表示] を選択する。

[プロセス] ページに切り替わります。JP1/IM - View の java.exe が選択された状態で表示されるため、これによってプロセス ID (PID) ※を特定します。

注※ PID 項目がない場合はメニューの [表示] - [列の選択] を選択し、[列の選択] 画面で [PID(プロセス ID)] チェックボックスをチェックしてください。

4. 特定できたプロセス ID を引数にして、jcothreaddmp コマンドを実行する。

jcothreaddmp 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「jcothreaddmp (Windows 限定)」(1. コマンド) を参照してください。

■ JP1/IM - Manager

ヘルスチェック機能によって、JP1/IM - Manager のイベントコンソールサービス、イベント基盤サービス、または関連イベント発行サービスの異常を検知した場合に、JP1/IM - Manager 用のダンプファイルを出力してください。次のようにjcogencore コマンドを実行します。

```
jcogencore
```

jcogencore 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「jcogencore」(1. コマンド) を参照してください。

(c) 資料採取ツールを実行する

資料採取ツール (jim_log.bat またはjcoview_log.bat) を実行します。

JP1/IM - Manager で提供しているjim_log.bat を実行すれば、同ホスト上の JP1/IM - Manager, JP1/IM - View の障害調査に必要な資料を採取できます。

また、JP1/IM - View で提供しているjcoview_log.bat を実行すれば、JP1/IM - View の障害調査に必要な資料を採取できます。

運用に合わせて使い分けてください。

なお、資料採取ツールで採取する資料の総容量は膨大になるため、実行する前に容量を見積もり、ご使用のマシンの空き容量を確認する必要があります。jim_log.bat で採取する資料サイズについては、JP1/IM - Manager のリリースノートを参照してください。

jcoview_log.bat で採取する資料サイズについては、JP1/IM - View のリリースノートを参照してください。

次に、ツールの実行例を示します。

```
C:¥>"C:¥Program Files¥Hitachi¥JP1IMM¥tools¥jim_log.bat" -f 資料格納フォルダ
```

資料格納フォルダは絶対パスで指定してください。また、資料格納フォルダが空白を含むフォルダの場合、"で囲んで指定してください。

ツールを実行すると、資料格納フォルダに指定したフォルダ下にjp1_default フォルダができ、そこに採取した資料がコピーされます。なお、採取した資料は、圧縮ツールを使用して圧縮してください。

❗ 重要

- Microsoft(R) Office Outlook(R)をご使用の場合、資料採取ツールを実行すると、次のメッセージボックスが表示される場合があります。
「プログラムが、Outlook 内に保存されている電子メールアドレスにアクセスしようとしています。よろしいですか？」
これは、資料採取ツール内で実行するマシン構成情報採取プログラム(MSINFO32)の動作によるものです。資料採取ツールでは、電子メールアドレスの採取は行いませんので、メッセージボックスの [いいえ] ボタンを押下してください。なお、JP1/IM - Manager および JP1/IM - View の資料採取および、Microsoft(R) Outlook(R)の動作には問題はありません。
- 資料採取ツールは多重実行しないでください。
- 資料採取ツールの実行時の環境によって、資料採取に時間がかかる場合があります。
- JP1/IM - Manager の資料を採取する際、JP1/Base, JP1/IM - Manager のコマンドを実行して情報を収集する項目があり、実行するコマンドの中には、同一のコマンドまたは他のコマンドと同時に実行できないものが含まれます。資料採取中に JP1/Base や JP1/IM - Manager のコマンドは極力実行しないでください。
- 運用実績がない場合には、資料採取ツールの実行時に「KAVB4153-E アクション情報ファイル(アクション情報ファイル名)のオープンに失敗しました：指定されたファイルが見つかりません。」をイベントログおよび統合トレースログに出力します。これは、資料採取ツールの実行時にアクション情報ファイルが存在しないためですが、アクション情報ファイルは運用によって生成されるため、本メッセージが出力されても運用実績がない場合、資料採取には問題ありません。なお、論理ホストを指定した場合でも、物理ホストの資料を採取しますので、本メッセージが出力されても物理ホストでの運用実績がない場合、資料採取には問題ありません。
- Windows イベントログ中に、イベントログ発行元製品提供のメッセージフォーマットと埋め文字の数が一致していない Windows イベントが存在する場合、資料採取ツール実行中にアプリケーションエラーが発生することがあります。その場合も、資料は採取されていますので特に問題はありません。なお、本現象が発生した場合、ダイアログが表示され、資料採取ツールの実行が中断することがあります(ダイアログに応答することで、再開します)。ダイアログの表示を抑止したい場合は、次の手順を実行してください。

1. [スタート] メニューを開き、[プログラムとファイルの検索] または [ファイル名を指定して実行] で gpedit.msc を入力してください。
 2. [ローカルグループポリシーエディター] が開くので、左側のツリーで [ローカルコンピューターポリシー] - [コンピュータの構成] - [管理用テンプレート] - [Windows コンポーネント] - [Windows エラー報告] を選択してください。
 3. 右側の [設定] で [重大なエラーが発生したユーザー インターフェイスを表示しないようにする] で [有効] を選択し [OK] ボタンをクリックしてください。
- 資料採取ツールの実行が終了してもマシンのシステム情報が採取されていない場合があります。これは、資料採取ツールの実行が終了しても、内部的に OS の情報を採取するためのプロセスが終了していないためです。タスクマネージャを起動し、[プロセス] タブまたは [詳細] タブで「msinfo32.exe」が終了しているのを確認した後、採取した資料を圧縮ツールなどで圧縮したり、移動、削除などの操作を行ってください。

(d) オペレーション内容を確認する

トラブル発生時のオペレーション内容を確認し、記録しておいてください。確認が必要な情報を次に示します。

- オペレーション内容の詳細
- 発生時刻
- 再現性
- JP1/IM - View からログインしている場合は、ログインユーザー名
- マシン構成 (各 OS のバージョン、ホスト名、セントラルコンソールの構成)

(e) 画面上のエラー情報を採取する

画面にエラーが表示された場合は、その情報も採取します。次に示すハードコピーを採取してください。

- エラーダイアログボックスのハードコピー
詳細ボタンがある場合はその内容をコピーしてください。

(f) ユーザーダンプを採取する (Windows 限定)

Windows で JP1/IM - View のプロセスがアプリケーションエラーで停止した場合、エラーダイアログボックスが表示されている状態で、次の手順でユーザーダンプを採取してください。

1. タスクマネージャを起動する。

タスクマネージャは次のどちらかの手順で起動できます。

- タスクバーの空いている場所で右クリックをして「タスクマネージャ」を選択する。
- [Ctrl] + [Shift] + [Esc] キーを押してタスクマネージャを起動する。

2. [プロセス] タブをクリックする。
3. アプリケーションエラーで停止した JP1/IM - View のプロセス名を右クリックし、「ダンプファイルの生成」を選択する。
4. ユーザーダンプの出力先パスを示すダイアログボックスが表示されるので、そこから採取する。

❗ 重要

エラーダイアログボックスを消してしまうと正常なダンプは取得されないため、ユーザーダンプを採取できなくなってしまう可能性があります。誤って採取前にエラーダイアログボックスを（[OK] ボタンなどをクリックして）消してしまった場合は、現象を再現させてからユーザーダンプを採取してください。

(g) RAS 情報を採取する

リモート監視時にトラブルが発生した場合、RAS 情報を採取します。RAS 情報の資料は、マネージャーホストと監視対象ホストで採取します。

採取方法は、監視対象ホストとの接続方法によって異なります。リモート監視のホスト情報収集では、収集するログ情報、およびマネージャーホストの OS と監視対象ホストの OS によって、接続方法が異なります。リモート監視の接続方法の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.6.2 収集できるログ情報とリモート監視の接続方法」を参照してください。

ここでは、マネージャーホストの OS が Windows の場合の採取方法について説明します。

表 12-20 RAS 情報の資料の採取方法の参照先（マネージャーホストの OS が Windows の場合）

接続方法	資料を採取するホスト (OS)	採取方法の参照先
WMI 接続	マネージャーホスト (Windows)	表 12-21 マネージャーホスト (Windows) で資料を採取する方法 (WMI 接続の場合)
	監視対象ホスト (Windows)	表 12-22 監視対象ホスト (Windows) で資料を採取する方法 (WMI 接続の場合)
NetBIOS 接続	マネージャーホスト (Windows)	表 12-23 マネージャーホスト (Windows) で資料を採取する方法 (NetBIOS 接続の場合)
	監視対象ホスト (Windows)	表 12-24 監視対象ホスト (Windows) で資料を採取する方法 (NetBIOS 接続の場合)
SSH 接続	マネージャーホスト (Windows)	表 12-25 マネージャーホスト (Windows) で資料を採取する方法 (SSH 接続の場合)

接続方法	資料を採取するホスト (OS)	採取方法の参照先
	監視対象ホスト (UNIX)	表 12-28 監視対象ホスト (UNIX) で資料を採取する方法 (SSH 接続の場合)

注※ リモート監視のホスト情報収集では、監視対象ホストの OS が Windows の場合、WMI と NetBIOS (NetBIOS over TCP/IP)、UNIX の場合、SSH を使用します。リモート監視の接続方法の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.6.2 収集できるログ情報とリモート監視の接続方法」を参照してください。

Docker 環境上のコンテナの資料採取では、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.6.2 収集できるログ情報とリモート監視の接続方法」に記載の監視対象ホストで採取する資料に加えて、次の資料も採取してください。

Podman の場合

- `podman ps` コマンドの実行結果

Docker の場合

- `docker ps` コマンドの実行結果

■ WMI 接続の場合

WMI 接続でトラブルが発生した場合にマネージャーホスト (Windows) で資料を採取する方法について、次の表に示します。

表 12-21 マネージャーホスト (Windows) で資料を採取する方法 (WMI 接続の場合)

項番	採取方法
1	<p>コマンドプロンプトから次のコマンドを実行して結果を採取する。</p> <ul style="list-style-type: none"> • <code>whoami /all</code> • <code>nslookup</code> 監視対象ホスト名 • <code>netsh advfirewall firewall show rule name=all</code> • <code>netsh advfirewall show allprofiles</code> • <code>tasklist</code> • <code>systeminfo</code> • <code>wmic qfe</code> • <code>reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System 出力ファイル</code> • <code>reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\0le 出力ファイル</code> • <code>reg export HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System 出力ファイル</code> • <code>wmic /node:"監視対象ホスト名" /user:ユーザー名 /password:パスワード port</code> (任意の WMI コマンド) • マネージャーホストで実行するコマンド <ul style="list-style-type: none"> <code>date /t</code> <code>time /t</code> • 監視対象ホストに WMI 接続して実行するコマンド <ul style="list-style-type: none"> <code>wmic /node:"監視対象ホスト名" /user:ユーザー名 /password:パスワード path Win32_LocalTime</code>
2	<p>WMI 接続の認証情報を採取する。</p> <ul style="list-style-type: none"> • 物理ホストの場合

項番	採取方法
	Manager パス <code>%conf%agtless%targets%wmi.ini</code> <ul style="list-style-type: none"> 論理ホストの場合 共有フォルダ <code>%JP1IMM%conf%agtless%targets%wmi.ini</code>
3	WMI 接続のログを採取する。 <ul style="list-style-type: none"> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\Logging Directory に指定されたディレクトリ下のログファイル※
4	マネージャーホストから、コマンドプロンプトで「runas /user:ユーザー名 wbemtest」を実行していることがわかるスクリーンショットを採取する。 ユーザー名は [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する。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する。
5	wbemtest で [接続] ボタンをクリックしたときの、名前空間、資格証明のユーザー入力値がわかる状態のスクリーンショットを採取する。
6	wbemtest で [接続] ボタンをクリックしたあとの正しく接続できている状態、または [接続] ボタンをクリックしたあとに表示されるエラーメッセージのスクリーンショットを採取する。
7	wbemtest で [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。 <ul style="list-style-type: none"> Select * From Win32_NTLogEvent Where (Logfile='System' Or Logfile='Application') このクエリを実行したあとに、[クエリ結果] 画面に表示されるクエリの実行結果のスクリーンショットを採取する。

注※ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\Logging の値が既定値の0の場合、ログは出力されません。Logging の値が1の場合、エラー情報だけが出力されます。Logging の値が2の場合、詳細情報が出力されます。

WMI 接続でトラブルが発生した場合に監視対象ホスト (Windows) で資料を採取する方法について、次の表に示します。

表 12-22 監視対象ホスト (Windows) で資料を採取する方法 (WMI 接続の場合)

項番	採取方法
1	監視対象ユーザーが監視対象ホストにログインし、コマンドプロンプトから次のコマンドを実行して結果を採取する。 <ul style="list-style-type: none"> hostname whoami /all nslookup マネージャーホスト名 ipconfig /all netstat -na netsh advfirewall firewall show rule name=all netsh advfirewall show allprofiles tasklist 監視対象ホスト名 systeminfo %ProgramFiles%\Common Files\Microsoft Shared\MSInfo\msinfo32.exe /report 出力ファイル wmic qfe tasklist 監視対象ホスト名 reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System 出力ファイル

項番	採取方法
	<ul style="list-style-type: none"> reg export HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥0le 出力ファイル
2	<p>WMI 接続のログを採取する。</p> <ul style="list-style-type: none"> HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥WBEM¥CIMOM¥Logging Directory に指定されたディレクトリ下のログファイル※
3	<ul style="list-style-type: none"> ファイアウォールが無効の場合 Windows のファイアウォールが有効になっていないことがわかる資料を採取する。 ファイアウォールが有効の場合 コマンドプロンプトで次のコマンドを実行して結果を採取する。 reg export HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥WindowsFirewall¥StandardProfile¥RemoteAdminSettings 出力ファイル
4	<p>監視対象ホストで正しくイベントログが生成されていることを確認する資料を採取する。</p> <ul style="list-style-type: none"> [管理ツール] の [イベントビューアー] からアプリケーション、システム、セキュリティのイベントログのバイナリ形式とテキスト形式の両方を保存したもの

注※ HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥WBEM¥CIMOM¥Logging の値が既定値の0の場合、ログは出力されません。Logging の値が1の場合、エラー情報だけが出力されます。Logging の値が2の場合、詳細情報が出力されます。

■ NetBIOS 接続の場合

NetBIOS 接続でトラブルが発生した場合にマネージャーホスト (Windows) で資料を採取する方法について、次の表に示します。

表 12-23 マネージャーホスト (Windows) で資料を採取する方法 (NetBIOS 接続の場合)

項番	採取方法
1	<p>コマンドプロンプトから次のコマンドを実行して結果を採取する。</p> <ul style="list-style-type: none"> whoami nslookup 監視対象ホスト名 nbtstat -s netsh advfirewall firewall show rule name=all netsh advfirewall show allprofiles net use systeminfo wmic qfe date /t※ time /t※
2	<p>[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] を右クリックし、表示されたメニューから [プロパティ] を選択し、設定されたユーザー名がわかるスクリーンショットを採取する。</p>
3	<p>[IM ホストアカウント] に設定したユーザー名でログインし、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] を入力して接続し、監視対象ファイルを参照できたことがわかる資料を採取する。</p>

注※ マネージャーホストと監視対象ホストの時刻差を確認するため、監視対象ホストでも同じコマンドを、間隔を大きく空けずに実行してください。

NetBIOS 接続でトラブルが発生した場合に監視対象ホスト（Windows）で資料を採取する方法について、次の表に示します。

表 12-24 監視対象ホスト（Windows）で資料を採取する方法（NetBIOS 接続の場合）

項番	採取方法
1	<p>監視対象ユーザーが監視対象ホストにログインし、コマンドプロンプトから次のコマンドを実行して結果を採取する。</p> <ul style="list-style-type: none"> • hostname • nslookup マネージャーホスト名 • ipconfig /all • netsh advfirewall firewall show rule name=all • netsh advfirewall show allprofiles • net session • systeminfo • %ProgramFiles%\Common Files\Microsoft Shared\MSInfo\msinfo32.exe /report 出力ファイル • wmic qfe • cacls 監視対象ファイル • dir /A 監視対象ファイルが配置されているディレクトリ • net share 共有フォルダ名 • reg export HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters 出力ファイル • date /t※ • time /t※
2	<p>[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] を右クリックし、表示されたメニューから [プロパティ] を選択し、設定されたユーザー名がわかるスクリーンショットを採取する。</p>
3	<p>監視対象ファイルを採取する。</p>

注※ マネージャーホストと監視対象ホストの時刻差を確認するため、マネージャーホストでも同じコマンドを、間隔を大きく空けないで実行してください。

■ SSH 接続の場合

SSH 接続でトラブルが発生した場合にマネージャーホスト（Windows）で資料を採取する方法について、次の表に示します。

表 12-25 マネージャーホスト（Windows）で資料を採取する方法（SSH 接続の場合）

項番	採取方法
1	<p>コマンドプロンプトから次のコマンドを実行して結果を採取する。</p> <ul style="list-style-type: none"> • whoami • nslookup 監視対象ホスト名 • netsh advfirewall firewall show rule name=all • netsh advfirewall show allprofiles

項番	採取方法
	<ul style="list-style-type: none"> • systeminfo • wmic qfe • マネージャーホストで実行 date /t time /t • 監視対象ホストに SSH 接続して実行 date • dir /A 秘密鍵を配置したディレクトリ
2	SSH 接続の認証情報を採取する。 <ul style="list-style-type: none"> • 物理ホストの場合 Manager パス¥conf¥agt less¥targets¥ssh. ini • 論理ホストの場合 共有フォルダ¥JP1IMM¥conf¥agt less¥targets¥ssh. ini
3	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 接続できたことがわかる資料を採取する。

SSH 接続でトラブルが発生した場合に監視対象ホスト（UNIX）で資料を採取する方法については、「表 12-28 監視対象ホスト（UNIX）で資料を採取する方法（SSH 接続の場合）」を参照してください。

(2) UNIX の場合

(a) プロセスの状態を確認する

ps コマンドを使用したときに表示されるプロセス名を次に示します。なお、UNIX の場合、資料採取ツール (jim_log.sh) を実行することでほかの資料とともに ps コマンドの実行結果を採取できます。

■ JP1/IM - Manager

JP1/IM - Manager のプロセスについては、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 B.2(1) JP1/IM - Manager」を参照してください。

(b) JP1/IM 用ダンプファイルを出力する

■ JP1/IM - Manager

ヘルスチェック機能によって、JP1/IM - Manager の異常を検知した場合にだけ JP1/IM - Manager 用のダンプファイルを出力してください。次のように jcogencore コマンドを実行します。

```
jcogencore
```

jcogencore コマンドを実行すると、どのプロセスのダンプファイルを出力するかの問い合わせメッセージが表示されます。この場合、ヘルスチェック機能によって通知されたメッセージ情報に含まれるプロセスのダンプファイルを出力するよう選択してください。なお、すでにダンプファイルが存在する場合、上書きするかの問い合わせメッセージが表示されます。ダンプファイルを上書きしない場合は、n を選択し、

コマンドを終了してください。そのあと、ダンプファイルを退避し、再度jcogencore コマンドを実行してください。

jcogencore 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「jcogencore」(1. コマンド)を参照してください。

(c) 資料採取ツールを実行する

資料採取ツール (jim_log.sh) を実行します。

JP1/IM - Manager で提供している jim_log.sh を実行すれば、同ホスト上の JP1/IM - Manager, JP1/Base の障害調査に必要な資料を採取できます。

なお、資料採取ツールで採取する資料の総容量は膨大になるため、実行する前に容量を見積もり、ご使用のマシンの空き容量を確認する必要があります。資料サイズ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。

次に、ツールの実行例を示します。

```
# /opt/jp1imm/tools/jim_log.sh -f 資料格納ディレクトリ
```

ツールを実行すると、採取資料が tar 形式でまとめられ、圧縮した形で出力されます。

(d) オペレーション内容を確認する

トラブル発生時のオペレーション内容を確認し、記録しておいてください。確認が必要な情報を次に示します。

- オペレーション内容の詳細
- 発生時刻
- 再現性
- JP1/IM - View からログインしている場合は、ログインユーザー名
- マシン構成 (各 OS のバージョン, ホスト名, セントラルコンソールの構成)

(e) 画面上のエラー情報を採取する

画面にエラーが表示された場合は、その情報も採取します。次に示すハードコピーを採取してください。

- エラーダイアログボックスのハードコピー
詳細ボタンがある場合はその内容をコピーしてください。

(f) RAS 情報を採取する

リモート監視時にトラブルが発生した場合、RAS 情報を採取します。RAS 情報の資料は、マネージャーホストと監視対象ホストで採取します。

採取方法は、監視対象ホストとの接続方法によって異なります。リモート監視のホスト情報収集では、収集するログ情報、およびマネージャーホストの OS と監視対象ホストの OS によって、接続方法が異なります。リモート監視の接続方法の詳細については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「8.6.2 収集できるログ情報とリモート監視の接続方法」を参照してください。

ここでは、マネージャーホストの OS が UNIX の場合の採取方法について説明します。

表 12-26 RAS 情報の資料の採取方法の参照先（マネージャーホストの OS が UNIX の場合）

接続方法	資料を採取するホスト (OS)	採取方法の参照先
SSH 接続	マネージャーホスト (UNIX)	表 12-27 マネージャーホスト (UNIX) で資料を採取する方法 (SSH 接続の場合)
	監視対象ホスト (UNIX)	表 12-28 監視対象ホスト (UNIX) で資料を採取する方法 (SSH 接続の場合)

■ SSH 接続の場合

SSH 接続でトラブルが発生した場合にマネージャーホスト (UNIX) で資料を採取する方法について、次の表に示します。

表 12-27 マネージャーホスト (UNIX) で資料を採取する方法 (SSH 接続の場合)

項番	採取方法
1	<p>コンソールから次のコマンドを実行して結果を採取する。</p> <ul style="list-style-type: none"> • whoami • nslookup 監視対象ホスト名 • マネージャーホストで実行 date • 監視対象ホストに SSH 接続して実行 Date • ls -al 秘密鍵を配置したディレクトリ
2	<p>SSH 接続の認証情報を採取する。</p> <ul style="list-style-type: none"> • 物理ホストの場合 Manager パス%conf%agtless%targets%ssh. ini • 論理ホストの場合 共有フォルダ%JP1IMM%conf%agtless%targets%ssh. ini
3	<p>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 接続できたことがわかる資料を採取する。</p>

SSH 接続でトラブルが発生した場合に監視対象ホスト (UNIX) で資料を採取する方法について、次の表に示します。

表 12-28 監視対象ホスト (UNIX) で資料を採取する方法 (SSH 接続の場合)

項番	採取方法
1	<p>監視対象ユーザーが監視対象ホストにログインし、コンソールから次のコマンドを実行して結果を採取する。</p> <ul style="list-style-type: none"> • <code>uname -a</code> • <code>nslookup</code> マネージャーホスト名 • <code>ifconfig -a</code> • <code>netstat -i</code> • <code>netstat -na</code> • <code>iptables --list</code> • <code>env</code> • <code>which</code> コマンド名 (コマンド名に次のコマンド名を指定する) <ul style="list-style-type: none"> <code>uname</code> <code>ls</code> <code>wc</code> <code>tail</code> <code>head</code> <code>grep</code> <code>find</code> • <code>ls -ail</code> 監視対象ファイルが配置されているディレクトリ • <code>ls -al sshd_config</code> ファイルの AuthorizedKeysFile に指定されたディレクトリの上位ディレクトリ • <code>ls -al sshd_config</code> ファイルの AuthorizedKeysFile に指定されたディレクトリ • Linux の場合 <ul style="list-style-type: none"> <code>dmesg</code> <code>rpm -qa</code>
2	<p>次のファイルを採取する。</p> <ul style="list-style-type: none"> • <code>/etc/hosts.allow</code> • <code>/etc/hosts.deny</code> • 監視対象ファイル • Linux の場合 <ul style="list-style-type: none"> <code>/etc/nsswitch.conf</code> <code>/etc/issue</code> <code>/etc/ssh/sshd_config</code> <code>/var/log/messages</code> <code>/var/log/secure</code>

12.4.2 JP1/IM - Agent の資料採取方法

(1) Windows の場合

(a) 統合エージェントホスト

1. 統合エージェントホストにログインする。
2. コマンドを実行して生成されたファイルを採取する。

- シークレットのキー

```
jimasecret -list > secretkeys.txt
```

- システムログ

```
wevtutil el 2> nul 1> event_list.txt  
for /f "delims=" %i in ( event_list.txt ) do echo %i 2> nul 1>> event_info.txt& wevtutil  
gli "%i" 2> nul 1>> event_info.txt& echo ----- 2> nul 1>> event_info.txt  
wevtutil qe System /rd:true /f:text 2> nul 1> System.txt  
wevtutil qe Application /rd:true /f:text 2> nul 1> Application.txt  
wevtutil qe Security /rd:true /f:text 2> nul 1> Security.txt  
for /f "delims=" %i in ( event_list.txt ) do echo %i 2> nul 1>> event_config_info.txt& we  
vtutil gl "%i" 2> nul 1>> event_config_info.txt& echo ----- 2> nul 1>> event_config_info.  
txt
```

- OS 情報

```
hostname 1> hostname.txt 2>nul  
"%CommonProgramFiles%\Microsoft Shared\MSInfo\msinfo32" /report os_system.txt /categories  
SystemSummary 2>nul 1>nul  
set > getenv.log
```

- 通信状態

```
echo --Command netsh interface ip show address -- 1>> netstat.txt 2>nul  
netsh interface ip show address 1>> netstat.txt 2>nul  
echo --Command netsh interface ipv6 show address -- 1>> netstat.txt 2>nul  
netsh interface ipv6 show address 1>> netstat.txt 2>nul  
echo -- netsh advfirewall show currentprofile -- 1> firewall.txt 2>nul  
netsh advfirewall show currentprofile 1>> firewall.txt 2>nul  
echo -- netsh advfirewall firewall show rule -- 1>> firewall.txt 2>nul  
netsh advfirewall firewall show rule name=all verbose 1>> firewall.txt 2>nul
```

- プロセス情報

```
tasklist /svc > proc_svc.list 2>&1  
tasklist /v > proc_v.list 2>&1
```

- サービス情報

```
sc query > service.list 2>&1
```

- サイレンスの設定

Alertmanager のサービスが稼働している状態で、Alertmanager のサイレンス一覧取得 API を実行し、サイレンスの設定を採取します。API 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「5.21.3 Alertmanager のサイレンス一覧取得」を参照してください。

OSS の curl コマンドを使用する場合は、次に示すとおり実行し、生成されたファイルを採取します。

```
curl --request GET http://localhost:Alertmanagerのポート番号/api/v2/silences -o silence.txt
```

サイレンスの設定にパスワードなどの機密情報が含まれる場合は、採取したあとの定義ファイルから該当する定義を削除してください。

- ファイル一覧

```
dir /S JP1/IM - Agentのインストール先フォルダ 1>jp1ima_list.txt 2>nul
```

3. 手動で必要なファイルを採取する。

次の表に示すファイルを手動で採取します。

採取する資料	採取対象
OS 情報	<ul style="list-style-type: none"> • %systemroot%\system32\drivers\etc\hosts • %systemroot%\system32\drivers\etc\services
インストール時の資料	<ul style="list-style-type: none"> • 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) <p>注※ %TEMP%は、環境変数 TEMP に指定されているパスを示します。</p>
製品情報	<p>■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)」に記載されているトラブル発生時の資料採取対象のファイル ただし、次のファイルを除きます。</p> <ul style="list-style-type: none"> • 論理ホスト用の共有フォルダ以下のファイル • /usr/lib/systemd/system/以下のファイル <p>■OracleDB exporter を配置した場合、次のファイルを手動で採取します。</p> <ul style="list-style-type: none"> • OracleDB exporter の配置先%oracledb_exporter_windows%jp1ima%logs フォルダ • OracleDB exporter のサービス定義ファイル <p>■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、次のファイルを手動で採取します。</p> <ul style="list-style-type: none"> • 環境パラメーター設定ファイル (任意の名前.ini) • SAP システムのログ抽出コマンドの構築時に配置した RFC ライブラリ • SAP システムのログ抽出コマンドの構築時に配置した CRT ライブラリ

採取する資料	採取対象
	<ul style="list-style-type: none"> • 環境パラメーター設定ファイルの WORKDIR に設定しているパスに格納されている次のファイル • SAP システムのログ抽出コマンドのログファイル (任意の名前) • SAP システムのログ抽出コマンドのトレースファイル (コマンド名.log, コマンド名.dat) • RFC ライブラリが出力するトレースファイル (dev_rfc*) <p>環境パラメーター設定ファイル, または, SAP システムのログ抽出コマンド実行時の引数で, 上記ファイルの格納先ディレクトリを変更した場合は, 変更後のディレクトリも採取する必要があります。</p>

(b) クラスタシステムでの統合エージェントホスト

1. 実行系の統合エージェントホストにログインする。

2. コマンドを実行して生成されたファイルを採取する。

- シークレットのキー

```
jimasecret -list -l 共有フォルダ > secretkeys.txt
```

- サイレンスの設定

Alertmanager のサービスが稼働している状態で, Alertmanager のサイレンス一覧取得 API を実行し, サイレンスの設定を採取します。API 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「5.21.3 Alertmanager のサイレンス一覧取得」を参照してください。

OSS の curl コマンドを使用する場合は, 次に示すとおり実行し, 生成されたファイルを採取します。

```
curl --request GET http://論理ホスト名:論理ホストのAlertmanagerのポート番号/api/v2/silences -o scilence_論理ホスト名.txt
```

実行系の物理ホストで Alertmanager を運用している場合は, 次に示すとおり実行し, 生成されたファイルを採取します。

```
curl --request GET http://localhost:物理ホストのAlertmanagerのポート番号/api/v2/silences -o scilence.txt
```

サイレンスの設定にパスワードなどの機密情報が含まれる場合は, 採取したあとの定義ファイルから該当する定義を削除してください。

- ファイル一覧

```
dir /S JP1/IM - Agentのインストール先ディレクトリ 1>jp1ima_list.txt 2>nul
dir /S 共有ディレクトリ 1>jp1ima_list_論理ホスト名.txt 2>nul
```

- システムログ, OS 情報, 通信状態, プロセス情報, サービス情報

「12.4.2(1)(a)統合エージェントホスト」の手順 2 の「システムログ」, 「OS 情報」, 「通信状態」, 「プロセス情報」, および「サービス情報」を参照してください。

3. 手動で必要なファイルを採取する。

次の表に示すファイルを手動で採取します。

採取する資料	採取対象
OS 情報	「12.4.2(1)(a)統合エージェントホスト」の手順3の「OS 情報」および「インストール時の資料」を参照してください。
インストール時の資料	
製品情報	<p>■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)」に記載されているトラブル発生時の資料採取対象のファイル</p> <p>ただし、次のファイルを除きます。</p> <ul style="list-style-type: none">• /usr/lib/systemd/system/以下のファイル <p>■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、次のファイルを手動で採取します。</p> <ul style="list-style-type: none">• 環境パラメーター設定ファイル (任意の名前.ini)• SAP システムのログ抽出コマンドの構築時に配置した RFC ライブラリ• SAP システムのログ抽出コマンドの構築時に配置した CRT ライブラリ• 環境パラメーター設定ファイルの WORKDIR に設定しているパスに格納されている次のファイル<ul style="list-style-type: none">• SAP システムのログ抽出コマンドのログファイル (任意の名前)• SAP システムのログ抽出コマンドのトレースファイル (コマンド名.log, コマンド名.dat)• RFC ライブラリが出力するトレースファイル (dev_rfc*) <p>環境パラメーター設定ファイル、または、SAP システムのログ抽出コマンド実行時の引数で、上記ファイルの格納先ディレクトリを変更した場合は、変更後のディレクトリも採取する必要があります。</p>

4. 待機系の統合エージェントホストにログインする。

5. コマンドを実行して生成されたファイルを採取する。

- サイレンスの設定

Alertmanager のサービスが稼働している状態で、Alertmanager のサイレンス一覧取得 API を実行し、サイレンスの設定を採取します。API 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「5.21.3 Alertmanager のサイレンス一覧取得」を参照してください。

待機系の物理ホストで Alertmanager を運用している場合は、OSS の curl コマンドを使用するときは、次に示すとおり実行し、生成されたファイルを採取します。

```
curl --request GET http://localhost:物理ホストのAlertmanagerのポート番号/api/v2/silences -o silence.txt
```

サイレンスの設定にパスワードなどの機密情報が含まれる場合は、採取したあとの定義ファイルから該当する定義を削除してください。

- システムログ、OS 情報、通信状態、プロセス情報、サービス情報、ファイル一覧

「12.4.2(1)(a)統合エージェントホスト」の手順2の「システムログ」, 「OS情報」, 「通信状態」, 「プロセス情報」, 「サービス情報」, および「ファイル一覧」を参照してください。

6. 手動で必要なファイルを採取する。

次の表に示すファイルを手動で採取します。

採取する資料	採取対象
OS情報	「12.4.2(1)(a)統合エージェントホスト」の手順3の「OS情報」および「インストール時の資料」を参照してください。
インストール時の資料	
製品情報	<p>■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)」に記載されているトラブル発生時の資料採取対象のファイル</p> <p>ただし、次のファイルを除きます。</p> <ul style="list-style-type: none"> • /usr/lib/systemd/system/以下のファイル <p>■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、次のファイルを手動で採取します。</p> <ul style="list-style-type: none"> • 環境パラメーター設定ファイル (任意の名前.ini) • SAPシステムのログ抽出コマンドの構築時に配置したRFCライブラリ • SAPシステムのログ抽出コマンドの構築時に配置したCRTライブラリ • 環境パラメーター設定ファイルのWORKDIRに設定しているパスに格納されている次のファイル <ul style="list-style-type: none"> • SAPシステムのログ抽出コマンドのログファイル (任意の名前) • SAPシステムのログ抽出コマンドのトレースファイル (コマンド名.log, コマンド名.dat) • RFCライブラリが出力するトレースファイル (dev_rfc*) <p>環境パラメーター設定ファイル, または, SAPシステムのログ抽出コマンド実行時の引数で, 上記ファイルの格納先ディレクトリを変更した場合は, 変更後のディレクトリも採取する必要があります。</p>

(c) コンテナでの統合エージェントホスト

「12.4.2(1)(a) 統合エージェントホスト」と同じです。

(d) 統合マネージャーホスト

統合エージェント管理基盤 (imbase, imbaseproxy) に関する情報を, 資料採取ツール (jim_log.bat) で採取します。

採取対象の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「付録 A.4(1)統合マネージャーホスト (Windows)」のファイル・フォルダー一覧を参照してください。

(e) クラスタシステムでの統合マネージャーホスト

「12.4.2(1)(d) 統合マネージャーホスト」と同じです。

(f) 監視対象の AIX ホスト (Node exporter for AIX を配置した場合)

1. 監視対象の AIX ホストにログインする。
2. コマンドを実行して生成されたファイルを採取する。

- OS 情報

```
echo "-- lslpp -l -a --" > os_inst_pp.list 2> /dev/null
lslpp -l -a >> os_inst_pp.list 2> /dev/null
echo "-- /usr/sbin/instfix -a -icv --" >> os_inst_pp.list 2> /dev/null
/usr/sbin/instfix -a -icv >> os_inst_pp.list 2> /dev/null
lsattr -E -l sys0 > kernel_param.list 2> /dev/null
hostname >> hostname.txt 2> /dev/null
echo "-- uname --" > os_system.txt 2> /dev/null
uname -a >> os_system.txt 2> /dev/null
echo "-- date --" >> os_system.txt 2>&1
date >> os_system.txt 2>&1
env > getenv.log 2> /dev/null
```

- 通信状態

```
echo "--Command netstat -an --" > netstat.txt 2> /dev/null
netstat -an >> netstat.txt 2> /dev/null
echo "--Command netstat -rn --" >> netstat.txt 2> /dev/null
netstat -rn >> netstat.txt 2> /dev/null
echo "--Command ifconfig -a --" >> netstat.txt 2> /dev/null
ifconfig -a >> netstat.txt 2> /dev/null
echo "-- lsfilt --" >> firewall.txt 2>&1
lsfilt >> firewall.txt 2>&1
```

- プロセス情報

```
ps -elfa > proc.list 2> /dev/null
```

- 自動起動設定

```
lsitab -a > lsitab.txt 2> /dev/null
```

- ファイル一覧

```
ls -lR Node exporter for AIXの配置先*/jp1ima > jp1ima_list.txt 2>&1
```

注※ 論理ホスト運用の場合は、論理ホストの共有フォルダの配置先となります。

3. 手動で必要なファイルを採取する。

次の表に示すファイルを手動で採取します。

採取する資料	採取対象
システムログ	/var/adm/syslog/syslog.log※ 注※ システムログの出力先は「/etc/syslog.conf」の設定を参照して取得します。

採取する資料	採取対象
OS 情報	<ul style="list-style-type: none"> • /etc/hosts • /etc/services
自動停止設定	/etc/rc.shutdown

(2) UNIX の場合

(a) 統合エージェントホスト

1. 統合エージェントホストにログインする。
2. コマンドを実行して生成されたファイルを採取する。

- シークレットのキー

```
jimasecret -list > secretkeys.txt
```

- OS 情報

```
/bin/rpm -qa > os_inst_pp.list 2> /dev/null
/sbin/sysctl -a > kernel_param.list 2> /dev/null
hostname >> hostname.txt 2> /dev/null
echo "-- uname --" > os_system.txt 2> /dev/null
uname -a >> os_system.txt 2> /dev/null
echo "-- ls -l /boot --" >> os_system.txt 2> /dev/null
ls -l /boot >> os_system.txt 2> /dev/null
echo "-- cat /etc/os-release --" >> os_system.txt 2> /dev/null
cat /etc/os-release >> os_system.txt 2> /dev/null
echo "-- timedatectl --" >> os_system.txt 2>&1
timedatectl >> os_system.txt 2>&1
env > getenv.log 2> /dev/null
```

- 通信状態

```
echo "--Command ss -a --" > netstat.txt 2> /dev/null
ss -a >> netstat.txt 2> /dev/null
echo "--Command ip route --" >> netstat.txt 2> /dev/null
ip route >> netstat.txt 2> /dev/null
echo "--Command ip addr --" >> netstat.txt 2> /dev/null
ip addr >> netstat.txt 2> /dev/null
echo "-- iptables -v -n -L --line-numbers --" >> firewall.txt 2>&1
iptables -v -n -L --line-numbers >> firewall.txt 2>&1
echo "-- firewall-cmd --list-all-zones --" >> firewall.txt 2>&1
firewall-cmd --list-all-zones >> firewall.txt 2>&1
```

- プロセス情報

```
ps -elfa > proc.list 2> /dev/null
```

- サービス情報

```
systemctl list-unit-files -t service > service.list 2> /dev/null
```

- サイレンスの設定

「12.4.2(1)(a)統合エージェントホスト」の手順2の「サイレンスの設定」を参照してください。

- 起動停止設定

JP1/IM - Agentのユニット定義ファイルごとに、次のコマンドを実行します。

```
systemctl is-enabled ユニット定義ファイル名 > ユニット定義ファイル名.txt 2> /dev/null
```

- コンテナ情報

< Docker の場合 >

```
docker version > ./Docker_Verison 2>&1
docker ps -a --no-trunc > ./Docker_Process_Container_List 2>&1
docker_container_list=`docker ps -a --no-trunc -q`;for loop in $docker_container_list;do
echo $loop >> Docker_Top 2>&1;docker top $loop >> Docker_Top 2>&1;echo $loop >> Docker_In
spect 2>&1;docker inspect $loop >> Docker_Inspect 2>&1;done
/bin/cat /etc/docker/daemon.json > docker_daemon.json 2>&1
/bin/cat /etc/sysconfig/docker > sysconfig_docker 2>&1
```

< Podman の場合 >

```
podman version > Podman_Verison 2>&1
podman ps --all --no-trunc --format={{.ID}} > Podman_Process_Container_List 2>&1
podman_container_list=`podman ps --all --no-trunc --format={{.ID}}`;for loop in $podman_c
ontainer_list;do echo $loop >> Podman_Top 2>&1;podman top $loop hpid args >> Podman_Top 2
>&1;echo $loop >> Podman_Inspect 2>&1;podman inspect $loop >> Podman_Inspect 2>&1;done
```

- ファイル一覧

```
ls -lR /opt/jplima > jplima_list.txt 2>&1
ls -l /usr/lib/systemd/system/jpc* > systemd_jpc_list.txt 2>&1
getfacl -R /opt/jplima > jplima_acl_list.txt 2>&1
getfacl /usr/lib/systemd/system/jpc* > systemd_jpc_acl_list.txt 2>&1
```

3. 手動で必要なファイルを採取する。

次の表に示すファイルを手動で採取します。

採取する資料	採取対象
システムログ	/var/log/messages*
OS 情報	<ul style="list-style-type: none"> • /etc/hosts • /etc/services
インストール時の資料	<ul style="list-style-type: none"> • /etc/.hitachi/pplistd/pplistd • /etc/.hitachi/.install.log* • /etc/.hitachi/.uninstall.log* • /tmp/HITACHI_JP1_INST_LOG/以下のファイル
製品情報	<p>■マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 A.4(4)統合エージェントホスト (Linux)」に記載されているトラブル発生時の資料採取対象のファイル</p> <p>ただし、次のファイルを除きます。</p>

採取する資料	採取対象
	<ul style="list-style-type: none"> • 論理ホスト用の共有ディレクトリ以下のファイル • /usr/lib/systemd/system/以下の論理ホスト用のファイル ■OracleDB exporter を配置した場合、次のファイルを手動で採取します。 • OracleDB exporter の配置先/oracledb_exporter_linux/jp1ima/logsディレクトリ • ユニット定義ファイル ■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、次のファイルを手動で採取します。 • 環境パラメーター設定ファイル (任意の名前.ini) • SAP システムのログ抽出コマンドの構築時に配置した RFC ライブラリ • SAP システムのログ抽出コマンドの構築時に配置した CRT ライブラリ • 環境パラメーター設定ファイルの WORKDIR に設定しているパスに格納されている次のファイル <ul style="list-style-type: none"> • SAP システムのログ抽出コマンドのログファイル (任意の名前) • SAP システムのログ抽出コマンドのトレースファイル (コマンド名.log, コマンド名.dat) • RFC ライブラリが出力するトレースファイル (dev_rfc*) <p>環境パラメーター設定ファイル, または, SAP システムのログ抽出コマンド実行時の引数で, 上記ファイルの格納先ディレクトリを変更した場合は, 変更後のディレクトリも採取する必要があります。</p>

(b) クラスタシステムでの統合エージェントホスト

1. 実行系の統合エージェントホストにログインする。

2. コマンドを実行して生成されたファイルを採取する。

- シークレットのキー

```
jimasecret -list -l 共有ディレクトリ > secretkeys.txt
```

- サイレンスの設定

「12.4.2(1)(b)クラスタシステムでの統合エージェントホスト」の手順2の「サイレンスの設定」を参照してください。

- ファイル一覧

```
ls -lR /opt/jp1ima > jp1ima_list.txt 2>&1
ls -l /usr/lib/systemd/system/jpc* > systemd_jpc_list.txt 2>&1
ls -lR 共有ディレクトリ > jp1ima_list_論理ホスト名.txt 2>&1
getfacl -R /opt/jp1ima > jp1ima_acl_list.txt 2>&1
getfacl /usr/lib/systemd/system/jpc* > systemd_jpc_acl_list.txt 2>&1
getfacl -R 共有ディレクトリ > jp1ima_acl_list_論理ホスト名.txt 2>&1
```

- OS 情報, 通信状態, プロセス情報, サービス情報, 起動停止設定, コンテナ情報

「12.4.2(2)(a)統合エージェントホスト」の手順2の「OS 情報」, 「通信状態」, 「プロセス情報」, 「サービス情報」, 「起動停止設定」, および「コンテナ情報」を参照してください。

3. 手動で必要なファイルを採取する。

次の表に示すファイルを手動で採取します。

採取する資料	採取対象
システムログ	「12.4.2(2)(a)統合エージェントホスト」の手順3の「システムログ」, 「OS 情報」, および「インストール時の資料」を参照してください。
OS 情報	
インストール時の資料	
製品情報	<p>■マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 A.4(4)統合エージェントホスト (Linux)」に記載されているトラブル発生時の資料採取対象のファイル</p> <p>■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、次のファイルを手動で採取します。</p> <ul style="list-style-type: none">• 環境パラメーター設定ファイル (任意の名前.ini)• SAP システムのログ抽出コマンドの構築時に配置した RFC ライブラリ• SAP システムのログ抽出コマンドの構築時に配置した CRT ライブラリ• 環境パラメーター設定ファイルの WORKDIR に設定しているパスに格納されている次のファイル<ul style="list-style-type: none">• SAP システムのログ抽出コマンドのログファイル (任意の名前)• SAP システムのログ抽出コマンドのトレースファイル (コマンド名.log, コマンド名.dat)• RFC ライブラリが出力するトレースファイル (dev_rfc*) <p>環境パラメーター設定ファイル, または, SAP システムのログ抽出コマンド実行時の引数で, 上記ファイルの格納先ディレクトリを変更した場合は, 変更後のディレクトリも採取する必要があります。</p>

4. 待機系の統合エージェントホストにログインする。

5. コマンドを実行して生成されたファイルを採取する。

- サイレンスの設定

「12.4.2(1)(b)クラスタシステムでの統合エージェントホスト」の手順4の「サイレンス設定」を参照してください。

- OS 情報, 通信状態, プロセス情報, サービス情報, 起動停止設定, コンテナ情報, ファイル一覧

「12.4.2(1)(a)統合エージェントホスト」の手順2の「OS 情報」, 「通信状態」, 「プロセス情報」, 「サービス情報」, 「起動停止設定」, 「コンテナ情報」, および「ファイル一覧」を参照してください。

6. 手動で必要なファイルを採取する。

次の表に示すファイルを手動で採取します。

採取する資料	採取対象
システムログ	「12.4.2(2)(a)統合エージェントホスト」の手順3の「システムログ」, 「OS 情報」, および「インストール時の資料」を参照してください。
OS 情報	
インストール時の資料	

採取する資料	採取対象
製品情報	<p>■マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「付録 A.4(4)統合エージェントホスト (Linux)」に記載されているトラブル発生時の資料採取対象のファイル</p> <p>ただし、次のファイルを除きます。</p> <ul style="list-style-type: none"> • 論理ホスト用の共有ディレクトリ以下のファイル <p>■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、次のファイルを手動で採取します。</p> <ul style="list-style-type: none"> • 環境パラメーター設定ファイル (任意の名前.ini) • SAP システムのログ抽出コマンドの構築時に配置した RFC ライブラリ • SAP システムのログ抽出コマンドの構築時に配置した CRT ライブラリ • 環境パラメーター設定ファイルの WORKDIR に設定しているパスに格納されている次のファイル <ul style="list-style-type: none"> • SAP システムのログ抽出コマンドのログファイル (任意の名前) • SAP システムのログ抽出コマンドのトレースファイル (コマンド名.log, コマンド名.dat) • RFC ライブラリが出力するトレースファイル (dev_rfc*) <p>環境パラメーター設定ファイル、または、SAP システムのログ抽出コマンド実行時の引数で、上記ファイルの格納先ディレクトリを変更した場合は、変更後のディレクトリも採取する必要があります。</p>

(c) コンテナでの統合エージェントホスト

「12.4.2(2)(a) 統合エージェントホスト」と同じです。

(d) 統合マネージャーホスト

統合エージェント管理基盤 (imbase, imbaseproxy) に関する情報を、資料採取ツール (jim_log.sh) で採取します。

採取対象の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「付録 A.4(2)統合マネージャーホスト (Linux)」のファイル・ディレクトリ一覧を参照してください。

(e) クラスタシステムでの統合マネージャーホスト

「12.4.2(2)(d) 統合マネージャーホスト」と同じです。

(f) 監視対象の AIX ホスト (Node exporter for AIX を配置した場合)

「12.4.2(1)(f)監視対象の AIX ホスト (Node exporter for AIX を配置した場合)」と同じです。

12.5 トラブルシューティング

12.5.1 障害の切り分け方法

各アドオンプログラムのログに出力するメッセージに対する原因と対処を、次に示します。

各ログの格納先については、「[12.2.2 JP1/IM - Agent のログ情報](#)」を参照してください。なお、Node exporter for AIX のログは、システムログに出力します。

(1) Prometheus server のログ

メッセージ	原因	対処
msg="Error on ingesting samples that are too old or are too far into the future"	システム時刻を過去に変更した。	変更前の時刻になるまで待ってください。
msg="Append failed" err="out of bounds"		
msg="Appending scrape report failed" err="out of bounds"		
component=remote msg="Failed to send batch, retrying"	JP1/IM - Manager ホストが高負荷などで、Prometheus から性能情報を送信できなかった。	JP1/IM - Manager ホストの負荷状況を確認してください。
	JP1/IM - Manager ホストとの接続が確立されていないか、または不安定な状況だった。	JP1/IM - Manager ホストとの接続状況を確認してください。
	JP1/IM - Manager のサービスが起動していなかった。	JP1/IM - Manager のサービスの起動状態を確認してください。
	JP1/IM - Manager のサービスからエラーを示す HTTP レスポンスが返却された。	JP1/IM - Manager のサービス側でエラーが発生していないか確認してください。
	Prometheus 設定ファイル (jpc_prometheus_server.yml) に指定したリモートライト先が誤っていた。	Prometheus 設定ファイル (jpc_prometheus_server.yml) の指定内容を見直してください。
msg="Skipping resharding, last successful send was beyond threshold"	JP1/IM - Manager ホストの負荷状況、接続状況などの理由で、Prometheus から性能情報の送信に失敗のときに、しきい値に達しているため、再度の負荷分散を省略した。	JP1/IM - Manager ホストの負荷状況、接続状況を確認してください。
msg="Error sending alert"	Alertmanager が停止していた。	Alertmanager を起動してください。

メッセージ	原因	対処
	Alertmanager からエラーを示す HTTP レスポンスが返却された。	Alertmanager 側でエラーが発生していないか確認してください。
	Prometheus 設定ファイル (jpc_prometheus_server.yml) に指定したアラート通知先が誤っていた。	Prometheus 設定ファイル (jpc_prometheus_server.yml) の指定内容を見直してください。
msg="Scrape failed"	Exporter が停止しているため、スクレイプに失敗した。	Exporter を起動してください。
	ディスカバリ設定ファイル (file_sd_config_*.yaml) に存在しないホスト名を指定したため、スクレイプに失敗した。	ディスカバリ設定ファイル (file_sd_config_*.yaml) の指定内容を見直してください。
	スクレイプ先からエラーを示す HTTP レスポンスが返却された。	スクレイプ先でエラーが発生していないか確認してください。
msg="Unable to start web listener"	コマンドラインオプション--web.listen-address に、不正なホスト名を指定した。	正しいホスト名を指定してください。
	コマンドラインオプション--web.listen-address に、すでに使用されているポートを指定した。	使用されていないポートを指定してください。
msg="Error loading config (--config.file=jpc_prometheus_server.yml)" msg="Error reading file"	Prometheus 設定ファイル (jpc_prometheus_server.yml) の期間を指定する項目に不正な値を指定した。	err に表示されている不正な行番号または項目名を確認して、Prometheus 設定ファイル (jpc_prometheus_server.yml) の指定内容を見直してください。
	Prometheus 設定ファイル (jpc_prometheus_server.yml) の書式に従っていなかった。	
	Prometheus 設定ファイル (jpc_prometheus_server.yml) の job_name に値を指定していなかった。	

(2) Alertmanager のログ

メッセージ	原因	対処
<ul style="list-style-type: none"> msg="Notify for alerts failed" msg="Notify attempt failed, will retry later" 	JP1/IM - Manager ホストが高負荷などで、Alertmanager からアラートを送信できなかった。	JP1/IM - Manager ホストの負荷状況を確認してください。
	JP1/IM - Manager ホストとの接続が確立されていないか、または不安定な状況だった。	JP1/IM - Manager ホストとの接続状況を確認してください。
	JP1/IM - Manager のサービスが起動していなかった。	JP1/IM - Manager のサービスの起動状態を確認してください。

メッセージ	原因	対処
	JPI/IM - Manager のサービスからエラーを示す HTTP レスポンスが返却された。	JPI/IM - Manager のサービス側でエラーが発生していないか確認してください。
	Alertmanager 設定ファイル (alertmanager.yml) に指定したアラート送信先が誤っていた。	Alertmanager 設定ファイル (alertmanager.yml) の指定内容を見直してください。
msg="Loading configuration file failed"	Alertmanager 設定ファイル (alertmanager.yml) の指定内容が不正であった。	err に記載されている内容を確認して、Alertmanager 設定ファイル (alertmanager.yml) の指定内容を見直してください。
msg="Listen error"	コマンドラインオプション--web.listen-address に、不正なホスト名を指定した。	正しいホスト名を指定してください。
	コマンドラインオプション--web.listen-address に、すでに使用されているポートを指定した。	使用されていないポートを指定してください。

(3) blackbox_exporter のログ

blackbox_exporter で、次のようなログを採取するには、ログレベルを「debug」にする必要があります。

メッセージ	原因	対処
msg=" Unable to do unprivileged listen on socket, will attempt privileged " err=" socket: permission denied"	カーネルパラメーター「net.ipv4.ping_group_range」で、ping ソケットを生成するための権限がない状態で、ソケットを生成するときに発生します。これは特権ユーザー (root) でも発生します。	メッセージの出力後、特権ユーザー (root) の権限で ICMP のソケットを生成して継続するため、このメッセージは無視して問題ありません。 また、このメッセージを抑止するためだけに、カーネルパラメーター「net.ipv4.ping_group_range」を設定して、権限を付与することは推奨しません。
module=icmp msg="Timeout reading from socket"	Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル (file_sd_config_blackbox_icmp.yml) に指定した監視対象のホストが停止しているため、ICMP プローブが失敗した。	Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル (file_sd_config_blackbox_icmp.yml) の指定内容を見直してください。
module=icmp msg="Resolution with IP protocol failed"	Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル (file_sd_config_blackbox_icmp.yml) に、存在しないホスト名を指定したため、ICMP プローブが失敗した。	Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル (file_sd_config_blackbox_icmp.yml) の指定内容を見直してください。
module=http msg="Error for HTTP request"	Blackbox exporter (HTTP/HTTPS 監視) のディスカバリ設定ファイル (file_sd_config_blackbox_http.yml) に指定した監視対象のホストが停止していた。	Blackbox exporter (HTTP/HTTPS 監視) のディスカバリ設定ファイル (file_sd_config_blackbox_http.yml) の指定内容を見直してください。

メッセージ	原因	対処
	Blackbox exporter (HTTP/HTTPS 監視) のディスクバリ設定ファイル (file_sd_config_blackbox_http.yml) に指定した監視対象のサービスが停止していた。	
	Blackbox exporter (HTTP/HTTPS 監視) のディスクバリ設定ファイル (file_sd_config_blackbox_http.yml) の modules.モジュール名.http.basic_auth.password_file に、存在しないパスを指定した。	
module=http msg="Error resolving address"	Blackbox exporter (HTTP/HTTPS 監視) のディスクバリ設定ファイル (file_sd_config_blackbox_http.yml) に、存在しないホスト名を指定した。	Blackbox exporter (HTTP/HTTPS 監視) のディスクバリ設定ファイル (file_sd_config_blackbox_http.yml) の指定内容を見直してください。
module=http msg="Failed to get decompressor for HTTP response body"	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の modules.モジュール名.http.basic_auth.username に指定したユーザー名が不正なため、HTTP プローブに失敗した。	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の指定内容を見直してください。
	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の modules.モジュール名.http.basic_auth.password に指定したパスワードが不正なため、HTTP プローブに失敗した。	
	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の modules.モジュール名.http.basic_auth.bearer_token が不正なため、HTTP プローブに失敗した。	
module=icmp msg="Error listening to socket"	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の modules.モジュール名.icmp.source_ip_address に、不正な IP アドレスを指定した。	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の指定内容を見直してください。
module=http msg="Error generating HTTP client"	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の modules.モジュール名.http.tls_config.ca_file に指定したパスが存在しないため、HTTP プローブに失敗した。	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の指定内容を見直してください。
	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の	

メッセージ	原因	対処
	modules.モジュール名.http.tls_config.cert_file に指定したパスが存在しないため、HTTP プローブに失敗した。	
	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の modules.モジュール名.http.tls_config.key_file に指定したパスが存在しないため、HTTP プローブに失敗した。	
msg="Error loading config"	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の数値を指定する項目に、不正な値を指定した。	err に表示されている不正な行番号または項目名を確認して、Blackbox exporter 設定ファイル (blackbox_exporter.yml) の指定内容を見直してください。
	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の正規表現を指定する項目に、不正な値を指定した。	
	Blackbox exporter 設定ファイル (blackbox_exporter.yml) の boolean 型の値を指定する項目に、不正な文字列を指定した。	
module=icmp msg="Failed to set Control Message for retrieving TTL" err=" not implemented on windows/amd64 " (省略) module=icmp msg=" Cannot get TTL from the received packet. 'probe_icmp_reply_hop_limit' will be missing. "	Windows 環境で、Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル (file_sd_config_blackbox_icmp.yml) を設定して ICMP 監視を行っている。	対処不要です。

(4) node_exporter のログ

メッセージ	原因	対処
err="listen tcp: lookup ホスト名 on DNS: no such host"	コマンドラインオプション--web.listen-address に、不正なホスト名を指定した。	正しいホスト名を指定してください。
err="listen tcp :ポート: bind: address already in use"	コマンドラインオプション--web.listen-address に、すでに使用されているポートを指定した。	使用されていないポートを指定してください。

メッセージ	原因	対処
msg="Parsed flag -- collector.filesystem.オプション名" flag=[aaa panic: regexp: Compile(`[aaa`): error parsing regexp: missing closing]: `[aaa`	コマンドラインオプションに、不正な正規表現を指定した。	コマンドラインオプションを見直してください。
msg="Parsed flag -- collector.systemd.unit-include" flag=(panic: regexp: Compile(`^(?:() \$`): error parsing regexp: missing closing): `^(?:() \$`	--collector.systemd.unit-include に不正な正規表現を指定した。	指定している正規表現を見直してください。

(5) process_exporter のログ

メッセージ	原因	対処
flag needs an argument: コマンドラインオプション	コマンドラインオプションに値が指定されていない。	コマンドラインオプションの指定内容を見直してください。
Failed to start the server: listen tcp: address ポート: missing port in address	コマンドラインオプションの--web.listen-address に不正なポートを指定した。	コマンドラインオプションの--web.listen-address の指定内容を見直してください。
Failed to start the server: listen tcp: lookup ホスト名 on DNS: エラー詳細	コマンドラインオプションの--web.listen-address に存在しないアドレスを指定した。	コマンドラインオプションの--web.listen-address の指定内容を見直してください。
Failed to start the server: listen tcp :ポート: bind: address already in use	コマンドラインオプションの--web.listen-address にすでに使用されているポートを指定した。	使用されていないポートを指定してください。
-config.path cannot be used with -namemapping or -procnames	コマンドラインオプションの--procnames と--config.path の両方が指定されている。	コマンドラインオプションの指定内容を見直してください。
	コマンドラインオプションの--namemapping と--config.path の両方が指定されている。	
Error parsing -namemapping argument '指定した文字列': bad namemapper: odd number of tokens	コマンドラインオプションの--namemapping に奇数個の値が指定されている。	コマンドラインオプションの--namemapping の指定内容を見直してください。

メッセージ	原因	対処
Error parsing -namemapping argument '指定した文字列': error compiling regexp '不正な正規表現': error parsing regexp: エラー詳細	コマンドラインオプションの--namemapping に不正な正規表現が指定された。	コマンドラインオプションの--namemapping の指定内容を見直してください。
error reading config file "指定したパス": error reading config file "指定したパス": open 指定したパス: no such file or directory	コマンドラインオプションの--config.path に存在しないパスが指定された。	コマンドラインオプションの--config.path の指定内容を見直してください。
error reading config file "指定したパス": エラー詳細	コマンドラインオプションの--config.path に指定したファイルの書式が不正。	<ul style="list-style-type: none"> コマンドラインオプションの--config.path の指定内容を見直してください。 Process exporter 設定ファイル (jpc_process_exporter.yml) の書式を見直してください。
error reading config file "指定したパス": エラー詳細	設定ファイルに不正な書式が存在する。	Process exporter 設定ファイル (jpc_process_exporter.yml) の書式を見直してください。
Error initializing: open /proc/stat: permission denied	/proc ディレクトリにアクセスできない権限で Process exporter を実行した、または、実行中に/proc ディレクトリのアクセス権限がなくなった。	Process exporter の実行ユーザーに、/proc ディレクトリ配下の読み込み権限を付与してください。Exporter が停止している場合は、統合エージェントを再起動してください。
error reading procs: Error reading procs: Error reading procs: open /proc: permission denied		

(6) windows_exporter のログ

メッセージ	原因	対処
msg="cannot start windows_exporter: listen tcp: lookup ホスト名: no such host"	コマンドラインオプション--telemetry.addr に、不正なホスト名を指定した。	コマンドラインオプションを見直してください。
msg="cannot start windows_exporter: listen tcp :ポート: bind: Only one usage of each socket address (protocol/network address/port) is normally permitted."	コマンドラインオプション--telemetry.addr に、すでに使用されているポートを指定した。	コマンドラインオプションを見直してください。

メッセージ	原因	対処
msg="Loading configuration file: windows_exporter.yml"	Windows exporter 設定ファイル (windows_exporter.yml) の正規表現を指定する項目に、不正な正規表現を指定した。	Windows exporter 設定ファイル (windows_exporter.yml) の指定内容を見直してください。
	Windows exporter 設定ファイル (windows_exporter.yml) の数値を指定する項目に、不正な値を指定した。	
level=error msg="failed collecting service metrics:<nil> 例外が発生しました。(無効なクエリです)" source="service.go:77"	services-where に不正な WQL の where 句を指定した。	windows_exporter.yml の services-where の指定を見直してください。

(7) node_exporter_aix のログ

メッセージ	原因	対処
Error starting HTTP server: bind: Address already in use	サービスに登録している node_exporter_aix の起動時のコマンドラインオプションに使用済みのポート番号を指定して起動した。	サービスに登録している node_exporter_aix の起動時のコマンドラインオプションを見直してください。
~/node_exporter_aix: illegal option -- ~	サービスに登録している node_exporter_aix の起動時のコマンドラインオプションに使用できないオプションを指定して起動した。	サービスに登録している node_exporter_aix の起動時のコマンドラインオプションを見直してください。
Error calling perfstat_fcstat: Invalid argument	FC 情報を取得できない環境で以下のどちらかで起動した状態で、スクレイプされた。 <ul style="list-style-type: none"> コマンドラインオプションの-F を指定 コマンドラインオプションの-p 以外を指定していない 	サービスに登録している node_exporter_aix の起動時のコマンドラインオプションを見直してください。

(8) ya_cloudwatch_exporter のログ

メッセージ	原因	対処
"msg": "Couldn't get account Id for role : NoCredentialProviders:~"	~/aws/credentials が存在しないため、CloudWatch からのデータ取得に失敗した。	credentials ファイルを配置してください。
"msg": "Couldn't get account Id for role : InvalidClientTokenId:~"	~/aws/credentials に記載されている Access Key ID が不正なため、CloudWatch からのデータ取得に失敗した。	credentials ファイルの記載内容を見直してください。

メッセージ	原因	対処
"msg": "Couldn't get account Id for role : SignatureDoesNotMatch: ~"	~/aws/credentials に記載されている Secret Access Key が不正なため、CloudWatch からのデータ取得に失敗した。	credentials ファイルの記載内容を見直してください。
"msg": "Couldn't describe resources for region リージョン名: ~"	Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) の discovery.jobs.regions に、存在しない AWS リージョンを指定した。	Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) の指定内容を見直してください。
"msg": "Couldn't read config.yml: Discovery job [0]: Service is not in known list!: AWS サービス名"	Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) の discovery.jobs.type に、存在しない AWS サービスを指定した。	Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) の指定内容を見直してください。
"msg": "Couldn't read config.yml: yaml: unmarshal errors: ~"	Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) の数値を指定する項目に、不正な値を指定した。	msg に表示されている不正な行番号または項目名を確認して、Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) の指定内容を見直してください。
	Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) の書式に従っていない。	
	Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) の boolean 型の値を指定する項目に、不正な文字列を指定した。	
"msg": "Couldn't read config.yml: Metric [/0] in Discovery job [ジョブ名]: Name should not be empty"	Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) の discovery.jobs.metrics.name に、値を指定していない。	Yet another cloudwatch exporter 設定ファイル (ya_cloudwatch_exporter.yml) の指定内容を見直してください。

(9) Promitor のログ

(a) Scraper のログ

メッセージ	原因	対処
Failed to scrape resource collection ディスカバリーグループ名: Connection refused	Resource Discovery のサービスが停止している状態で、Scraper のサービスを起動した。	Resource Discovery Agent を起動してください。

メッセージ	原因	対処
(promitor.agents.resourcediscovery:ポート)	Promitor Scraper runtime 設定ファイル (runtime.yaml) の resourceDiscovery.port に誤ったポート番号を指定した。	Promitor Scraper runtime 設定ファイル (runtime.yaml) の resourceDiscovery.port の指定内容を見直してください。
AuthorizationFailed: The client 'オブジェクト ID' with object id 'オブジェクト ID' does not have authorization to perform action 'microsoft.insights/metricDefinitions/read' over scope '/subscriptions/サブスクリプション ID/resourceGroups/リソースグループ名 / providers/リソース種別/リソース名/providers/microsoft.insights' or the scope is invalid. If access was recently granted, please refresh your credentials.	Monitoring Reader ロール未満の権限の identity を指定した。	Monitoring Reader ロール以上の権限を付与してください。
Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. System.Security.Authentication.AuthenticationException: No identity secret was configured for service principle authentication	Promitor Scraper runtime 設定ファイル (runtime.yaml) の authentication.mode が ServicePrincipal の場合に、Azure Monitor に接続するためのシークレットに誤った値を登録して、Scraper を起動した。	環境変数 AUTH_APPKEY の指定内容を見直してください。
The following problems were found with the metric configuration: <エラー詳細> Validation failed: Errors were found while deserializing the metric configuration. Promitor is not configured correctly. Please fix validation issues and re-run.	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の書式に従っていない。 Promitor Scraper 設定ファイル (metrics-declaration.yaml) で、metrics.resources を指定したメトリックがない場合に、同ファイルの azureMetadata.cloud に範囲外の値を指定した。 Promitor Scraper 設定ファイル (metrics-declaration.yaml) で、metrics.resources を指定したメトリックがない場合に、	エラー詳細に不正な行番号と項目名が表示されるので、Promitor Scraper 設定ファイル (metrics-declaration.yaml) の指定内容を見直してください。

メッセージ	原因	対処
	<p><code>metricDefault.aggregation.interval</code> に形式不正な値を指定した。</p> <p>Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) で、<code>metrics.resources</code> を指定したメトリックがない場合に、<code>metricDefault.scraping.schedule</code> に不正な値を指定した。</p> <p>Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metrics.resourceType</code> に範囲外の値を指定した。</p> <p>Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metrics.scraping.schedule</code> に形式不正な値を指定した。</p> <p>Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) で、<code>metrics.resources</code> を指定したメトリックがない場合に、<code>metrics.azureMetricConfiguration.aggregation.type</code> に範囲外の値を指定した。</p> <p>Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) で、<code>metrics.resources</code> を指定したメトリックがない場合に、<code>metrics.azureMetricConfiguration.aggregation.interval</code> に形式不正な値を指定した。</p>	
<p>Validation failed: Errors were found while deserializing the metric configuration. Promitor is not configured correctly. Please fix validation issues and re-run.</p>	<p>Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の書式に従っていない。</p> <p>Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) で、<code>metrics.resources</code> を指定したメトリックがある場合に、<code>metricDefault.aggregation.interval</code> に不正な値を指定した。</p> <p>Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) で、<code>metrics.resources</code> を指定したメトリックがある場合に、<code>metricDefault.scraping.schedule</code> に不正な値を指定した。</p> <p>Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) で、<code>metrics.resources</code> を指定したメトリックがある場合に、<code>metrics.azureMetricConfiguration.aggregation.type</code> に不正な値を指定した。</p>	<p>Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) を見直してください。</p>

メッセージ	原因	対処
	Promitor Scraper 設定ファイル (metrics-declaration.yaml) で 、 <code>metrics.resources</code> を指定したメトリックがある場合に、 <code>metrics.azureMetricConfiguration.aggregation.interval</code> に不正な値を指定した。	
Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. Unable to deserialize the configured metrics declaration. Please verify that it is a well-formed YAML specification.	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の書式に従っていない。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の指定内容を見直してください。
Failed to scrape resource for metric 'メトリック名' AADSTS900023: Specified tenant identifier '指定した文字列' is neither a valid DNS name, nor a valid external domain.	Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>authentication.mode</code> が <code>ServicePrincipal</code> の場合に、Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.tenantId</code> に形式不正な値を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.tenantId</code> の指定内容を見直してください。
Validation failed: No tenant id is configured. Promitor is not configured correctly. Please fix validation issues and re-run.	Promitor Scraper 設定ファイル (metrics-declaration.yaml) で、 <code>metrics</code> に <code>resources</code> を指定したメトリックがない場合に、 <code>authentication.tenantId</code> に値が指定されていない。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>authentication.tenantId</code> の指定内容を見直してください。
	Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>metrics</code> に <code>resources</code> を指定したメトリックがある場合に、Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>authentication.tenantId</code> に値が指定されていない。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>authentication.tenantId</code> の指定内容を見直してください。
Failed to scrape resource for metric 'メトリック名' AADSTS90002: Tenant 'テナント ID' not found. Check to make sure you have the correct tenant ID and are signing into the correct cloud. Check with your subscription	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.tenantId</code> に存在しないテナント ID を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.tenantId</code> の指定内容を見直してください。

メッセージ	原因	対処
administrator, this may happen if there are no active subscriptions for the tenant.		
InvalidSubscriptionId: The provided subscription identifier '指定した文字列' is malformed or invalid.	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.subscriptionId</code> に形式不正な値を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.subscriptionId</code> の指定内容を見直してください。
	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.resources.subscriptionId</code> に形式不正な値を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.resources.subscriptionId</code> の指定内容を見直してください。
Validation failed: - No subscription id is configured Promitor is not configured correctly. Please fix validation issues and re-run.	Promitor Scraper 設定ファイル (metrics-declaration.yaml) で、 <code>metrics.resources</code> を指定したメトリックがない場合に、 <code>azureMetadata.subscriptionId</code> に値が指定されていない。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.subscriptionId</code> の指定内容を見直してください。
	Promitor Scraper 設定ファイル (metrics-declaration.yaml) で、 <code>metrics.resources</code> を指定したメトリックがある場合に、 <code>azureMetadata.subscriptionId</code> に値が指定されていない。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.subscriptionId</code> の指定内容を見直してください。
SubscriptionNotFound: The subscription 'サブスクリプション ID' could not be found.	Promitor Scraper 設定ファイル (metrics-declaration.yaml) で、 <code>metrics.resources</code> を指定したメトリックがある場合に、 <code>azureMetadata.subscriptionId</code> に存在しないサブスクリプション ID を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.subscriptionId</code> の指定内容を見直してください。
	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.resources.subscriptionId</code> に存在しないサブスクリプション ID を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.resources.subscriptionId</code> の指定内容を見直してください。
AuthorizationFailed: The client 'オブジェクト ID' with object id 'オブジェクト ID' does not have authorization to perform action microsoft.insights/metricDefinitions/read' over scope '/subscriptions/サブスクリプション ID/resourceGroups/指定した文字列/providers/リソース種別/リソース名/providers/microsoft.insights' or the	Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>authentication.mode</code> が <code>SystemAssignedManagedIdentity</code> の場合、かつ、Promitor Scraper 設定ファイル (metrics-declaration.yaml) で、 <code>metrics.resources</code> を指定したメトリックがある場合に、 <code>azureMetadata.resourceGroupName</code> に不正な値を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.resourceGroupName</code> の指定内容を見直してください。
	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.resources.resourceGroupName</code> に不正な値を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.resources.resourceGroupName</code> の指定内容を見直してください。

メッセージ	原因	対処
scope is invalid. If access was recently granted, please refresh your credentials.		
Validation failed: - No resource group name is not configured Promitor is not configured correctly. Please fix validation issues and re-run.	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.resourceGroupName</code> に値が指定されていない。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.resourceGroupName</code> の指定内容を見直してください。
Microsoft.IdentityModel.Clients.ActiveDirectory.AdalServiceException: AADSTS90038: Tenant 'テナント ID' request is being redirected to the National Cloud 'MicrosoftOnline.COM'.	Promitor Scraper 設定ファイル (metrics-declaration.yaml) で、 <code>metrics.resources</code> を指定したメトリックがある場合に、 <code>azureMetadata.cloud</code> に範囲外の値を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.cloud</code> の指定内容を見直してください。
Failed to scrape metric 'メトリック名' for resource 'リソース名'. System.NotSupportedException: Environment 'クラウド名' is not supported for scraping Azure Log Analytics resource(s)	Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>authentication.mode</code> が <code>ServicePrincipal</code> の場合に、 <code>metrics-declaration.yaml</code> の <code>azureMetadata.cloud</code> に誤ったクラウド名を指定した。	<code>metrics-declaration.yaml</code> の <code>azureMetadata.cloud</code> の指定内容を見直してください。
Failed to scrape resource for metric 'メトリック名' AADSTS500011: The resource principal named https://management.core.cloudapi.de/ was not found in the tenant named テナント ID. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You might have sent your authentication request to the wrong tenant.	Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>authentication.mode</code> が <code>SystemAssignedManagedIdentity</code> または <code>UserAssignedManagedIdentity</code> の場合に、Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.cloud</code> に誤ったクラウド名を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>azureMetadata.cloud</code> の指定内容を見直してください。
Failed to scrape: Value cannot be null. (Parameter 'key')	Promitor Scraper 設定ファイル (metrics-declaration.yaml) で、 <code>metrics.resources</code> を指定したメトリックがある場合に、	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metricDefault.aggregation</code> または

メッセージ	原因	対処
	<code>metricDefault.aggregation</code> と <code>metrics.azureMetricConfiguration.aggregation</code> のどちらにも <code>interval</code> と <code>type</code> を指定しなかった。	<code>metrics.azureMetricConfiguration.aggregation</code> の <code>interval</code> と <code>type</code> の指定内容を見直してください。
Failed to scrape resource collection リソース名: Value cannot be null. (Parameter 'key')	Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) で, <code>metrics.resources</code> を指定したメトリックがない場合に, <code>metricDefault.aggregation</code> と <code>metrics.azureMetricConfiguration.aggregation</code> のどちらにも <code>interval</code> と <code>type</code> を指定しなかった。	Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metricDefault.aggregation</code> または <code>metrics.azureMetricConfiguration.aggregation</code> の <code>interval</code> と <code>type</code> の指定内容を見直してください。
Validation failed: - Limit has to be at least 1 Promitor is not configured correctly. Please fix validation issues and re-run.	Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metricDefault.limit</code> に 1 未満の値が指定された。 Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metrics.azureMetricConfiguration.limit</code> に 1 未満の値が指定された。	Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metricDefault.limit</code> の指定内容を見直してください。
Validation failed: - No default metric scraping schedule is defined. - No metrics scraping schedule is configured Promitor is not configured correctly. Please fix validation issues and re-run.	Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metricDefault.scraping.schedule</code> に値が指定されていない。	Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metricDefault.scraping.schedule</code> の指定内容を見直してください。
Validation failed: - No metric name is configured Promitor is not configured correctly. Please fix validation issues and re-run.	Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metrics.name</code> に値が指定されていない。	Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metrics.name</code> の指定内容を見直してください。
Validation failed: - Metric name 'メトリック名' is declared multiple times Promitor is not configured correctly. Please fix validation issues and re-run.	Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metrics.name</code> に, ほかのメトリックと同じ値を指定した。	Promitor Scraper 設定ファイル (<code>metrics-declaration.yaml</code>) の <code>metrics.name</code> の指定内容を見直してください。

メッセージ	原因	対処
Validation failed: - No metric name for Azure is configured Promitor is not configured correctly. Please fix validation issues and re-run.	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.azureMetricConfiguration.Name</code> に値が指定されていない。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.azureMetricConfiguration.Name</code> の指定内容を見直してください。
Failed to scrape resource for metric 'メトリック名' Promitor.Integrations.AzureMonitor.Exceptions.MetricNotFoundExpection: The metric '指定した文字列' was not found	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.azureMetricConfiguration.Name</code> に不正な値を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.azureMetricConfiguration.Name</code> の指定内容を見直してください。
Validation failed: - Limit cannot be higher than <code>metricDefault.limit</code> の値	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.azureMetricConfiguration.limit</code> に 10000 より大きい値を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.azureMetricConfiguration.limit</code> の指定内容を見直してください。
BadRequest: Metric: Available Memory Bytes does not support requested dimension combination: 指定した文字列, supported ones are: , TraceId: {トレース ID }	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.azureMetricConfiguration.dimension.name</code> に不正な値を指定した。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.azureMetricConfiguration.dimension.name</code> の指定内容を見直してください。
Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. [resourceDiscoveryGroupName] cannot be Null, empty or white-space. (Parameter 'resourceDiscoveryGroupName')	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.resourceDiscoveryGroups.name</code> に値が指定されていない。	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.resourceDiscoveryGroups.name</code> の指定内容を見直してください。
Failed to scrape resource collection 指定した文字列: Response status code does not indicate success: 404 (Not Found).	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.resourceDiscoveryGroups.name</code> に不正な値を指定した。 Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の	Promitor Scraper 設定ファイル (metrics-declaration.yaml) の <code>metrics.resourceDiscoveryGroups.name</code> の指定内容を見直してください。 Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の <code>resourceDiscoveryGroups.name</code> の指定内容を見直してください。

メッセージ	原因	対処
	<p>resourceDiscoveryGroups.name に不正な値を指定した。</p> <p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の resourceDiscoveryGroups.type に不正な値を指定した。</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の resourceDiscoveryGroups.type の指定内容を見直してください。</p>
<p>Validation failed: - No プロパティ名 is configured Promitor is not configured correctly. Please fix validation issues and re-run.</p>	<p>Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.resources.property に値が指定されていない。</p>	<p>Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.resources.property の指定内容を見直してください。</p>
<p>ResourceNotFound: The Resource 'リソース種別/指定した文字列' under resource group 'リソースグループ名' was not found. For more details please go to https://aka.ms/ARMResourceNotFoundFix</p>	<p>Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.resources.property に不正な値を指定した。</p>	<p>Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.resources.property の指定内容を見直してください。</p>
<p>Validation failed: - Queue & topic name are both configured while we only support one or the other. Promitor is not configured correctly. Please fix validation issues and re-run.</p>	<p>Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.resourceType が ServiceBusNamespace のとき、metrics.resources に queueName と topicName をどちらも指定した。</p>	<p>Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.resources の指定内容を見直してください。</p>
<p>BadRequest: Metric: Azure メトリック名 does not accept zero dimension case</p>	<p>Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.resourceType が SqlServer のとき、metrics.azureMetricConfiguration.dimension.name に値が指定されていない。</p>	<p>Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.azureMetricConfiguration.dimension.name の指定内容を見直してください。</p>
<p>BadRequest: Metric: Azure メトリック名 does not support requested dimension combination: 指定した値, supported ones are: DatabaseResourceId, TraceId: {トレース ID}</p>	<p>Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.resourceType が SqlServer のとき、metrics.azureMetricConfiguration.dimension.name に不正な値を指定した。</p>	<p>Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.azureMetricConfiguration.dimension.name の指定内容を見直してください。</p>
<p>Failed to scrape resource collection ディスカバリー</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の</p>

メッセージ	原因	対処
ループ名: Response status code does not indicate success: 501 (Not Implemented).	declaration.yaml) の resourceDiscoveryGroups.type に値が指定されていない。	resourceDiscoveryGroups.type の指定内容を見直してください。
Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. Failed to convert configuration value at 'authentication:Mode' to type 'Promitor.Integrations.Azure.Authentication.AuthenticationMode'.	Promitor Scraper runtime 設定ファイル (runtime.yaml) の authentication.mode に不正な値を指定した。	Promitor Scraper runtime 設定ファイル (runtime.yaml) の authentication.mode の指定内容を見直してください。
Validation failed: Azure authentication is not configured correctly - No identity was configured for service principle authentication Promitor is not configured correctly. Please fix validation issues and re-run.	Azure Monitor に接続するためのシークレットが登録されていない場合、かつ、Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.resources を指定したメトリックがない場合に、Promitor Scraper runtime 設定ファイル (runtime.yaml) の authentication.mode に値が指定されていない。	Promitor Scraper runtime 設定ファイル (runtime.yaml) の authentication.mode の指定内容を見直してください。
	Promitor Scraper runtime 設定ファイル (runtime.yaml) の authentication.mode に Serviceprincipal を指定した場合、かつ、Promitor Scraper 設定ファイル (metrics-declaration.yaml) の metrics.resources を指定したメトリックがない場合に、Promitor Scraper runtime 設定ファイル (runtime.yaml) の authentication.identityId に値が指定されていない。	Promitor Scraper runtime 設定ファイル (runtime.yaml) の authentication.identityId の指定内容を見直してください。
Failed to scrape resource for metric 'メトリック名' AADSTS700016: Application with identifier '指定した文字列' was not found in the directory 'ディレクトリ名'. This can happen if the application has not been installed by the administrator of the tenant or consented to by	Promitor Scraper runtime 設定ファイル (runtime.yaml) で、 authentication.mode が ServicePrincipal の場合に、 authentication.identityId に不正な値を指定した。	Promitor Scraper runtime 設定ファイル (runtime.yaml) の authentication.identityId の指定内容を見直してください。
	Promitor Scraper runtime 設定ファイル (runtime.yaml) の server.httpPort にすでに使用されているポートを指定した。	Promitor Scraper runtime 設定ファイル (runtime.yaml) の server.httpPort に使用されていないポートを指定してください。

メッセージ	原因	対処
<p>any user in the tenant. You may have sent your authentication request to the wrong tenant.</p> <p>Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Failed to bind to address <code>http://[::]:ポート: address already in use.</code></p>		
<p>Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Failed to convert configuration value at <code>'server:HttpPort'</code> to type <code>'System.Int32'</code>.</p>	<p>Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>server.httpPort</code> に不正な値を指定した。</p>	<p>Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>server.httpPort</code> の指定内容を見直してください。</p>
<p>Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Could not find file <code>'パス'</code>.</p>	<p>Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>metricsConfiguration.absolutePath</code> に不正な値を指定した。</p>	<p>Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>metricsConfiguration.absolutePath</code> の指定内容を見直してください。</p>
<p>Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Could not find a part of the path <code>'/config/metrics-declaration.yaml'</code>.</p>	<p>Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>metricsConfiguration.absolutePath</code> に値が指定されていない。</p>	<p>Promitor Scraper runtime 設定ファイル (runtime.yaml) の <code>metricsConfiguration.absolutePath</code> の指定内容を見直してください。</p>

メッセージ	原因	対処
Promitor Scaper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. Failed to convert configuration value at 'resourceDiscovery:Port' to type 'System.Int32'.	Promitor Scaper runtime 設定ファイル (runtime.yaml) の resourceDiscovery.port に不正な値を指定した。	Promitor Scaper runtime 設定ファイル (runtime.yaml) の resourceDiscovery.port の指定内容を見直してください。
AuthorizationFailed: The client 'クライアント ID' with object id 'オブジェクト ID' does not have authorization to perform action 'microsoft.insights/metricDefinitions/read' over scope 'リソース uri' or the scope is invalid. If access was recently granted, please refresh your credentials	Promitor Scaper runtime 設定ファイル (runtime.yaml) の authentication.mode が ServicePrincipal の場合、かつ、Promitor 設定ファイル (metrics-declaration.yaml) の metrics.resources を指定した場合に、Promitor 設定ファイル (metrics-declaration.yaml) の azureMetadata.resourceGroupName に不正な値を指定した。	Promitor 設定ファイル (metrics-declaration.yaml) の azureMetadata.resourceGroupName の指定内容を見直してください。
Failed to scrape resource for metric 'メトリック名' System.Net.Http.HttpRequestException: Resource temporarily unavailable (ホスト:ポート)	Scaper がネットワークから遮断された。	ネットワークを接続してください。
Failed to discover resources for group リソースグループ名. System.Threading.Tasks.TaskCanceledException: The request was canceled due to the configured HttpClient.Timeout of 100 seconds elapsing.	Scaper がネットワークから遮断された Resource Discovery から情報を取得しようとした。	ネットワークを接続してください。
Failed to scrape resource for metric 'メトリック名' System.Net.Http.HttpRequestException: Name or service not known (ホスト:ポート)	不正なプロキシを設定して Scaper を実行した。	プロキシ設定を見直してください。

メッセージ	原因	対処
Failed to discover resources for group kubernetes-service-group. System.Net.Http.HttpRequestException: Response status code does not indicate success: 500 (Internal Server Error).	Scrapers が不正なプロキシが設定された Resource Discovery から情報を取得しようとした。	プロキシ設定を見直してください。

(b) Resource Discovery のログ

メッセージ	原因	対処
Unhandled exception in job Azure Subscription Discovery One or more errors occurred. ([subscriptions] cannot be Null. (Parameter 'subscriptions'))	Reader ロール未満の権限の identity を指定した。	Reader ロール以上の権限を付与してください。
ClientSecretCredential authentication failed: AADSTS700016: Application with identifier 'identityId に指定した値' was not found in the directory 'Azure ディレクトリ名'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant.	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) の authentication.mode が ServicePrincipal の場合に、Azure Resource Graph に接続するためのシークレットに誤った値を登録して、Resource Discovery を起動した。	Azure Resource Graph に接続するためのシークレットを見直す。
	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) で、 authentication.mode が ServicePrincipal の場合に、 authentication.identityId に不正な値を指定した。	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) の authentication.identityId の指定内容を見直す。
Unhandled exception in job Azure Subscription Discovery One or more errors occurred. (ClientSecretCredential authentication failed: AADSTS900023: Specified tenant identifier '指定した文字列' is neither a valid DNS name, nor a valid external domain.	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) の authentication.mode が ServicePrincipal のとき Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.tenantId に形式不正な値を指定した。	Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.tenantId の指定内容を見直してください。

メッセージ	原因	対処
<p>Unhandled exception in job Azure Subscription Discovery</p> <p>One or more errors occurred.</p> <p>(ClientSecretCredential authentication failed: AADSTS90002: Tenant '指定した文字列' not found. Check to make sure you have the correct tenant ID and are signing into the correct cloud. Check with your subscription administrator, this may happen if there are no active subscriptions for the tenant.</p>	<p>Promitor Resource Discovery 設定ファイル (runtime.yaml) の authentication.mode がServicePrincipal の場合に、Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.tenantId に存在しないテナント ID を指定した。</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.tenantId の指定内容を見直してください。</p>
<p>Validation failed:</p> <p>- No tenant id was configured</p> <p>Promitor is not configured correctly. Please fix validation issues and re-run.</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.tenantId に値が指定されていない。</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.tenantId の指定内容を見直してください。</p>
<p>Operation returned an invalid status code 'BadRequest'</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.subscriptions.subscriptionId に形式不正な値が指定された。</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.subscriptions.subscriptionId の指定内容を見直してください。</p>
<p>[queriedSubscriptions] cannot be Null. (Parameter 'queriedSubscriptions')</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.subscriptions.subscriptionId に存在しないサブスクリプション ID が指定された。</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.subscriptions.subscriptionId の指定内容を見直してください。</p>
<p>Validation failed:</p> <p>- No subscription id(s) were configured to query</p> <p>Promitor is not configured correctly. Please fix validation issues and re-run.</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.subscriptions.subscriptionId に値が指定されていない。</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の azureLandscape.subscriptions.subscriptionId の指定内容を見直してください。</p>
<p>Promitor Discovery Agent has encountered an unexpected error. Please</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の</p>	<p>Promitor Resource Discovery 設定ファイル (resource-discovery-declaration.yaml) の</p>

メッセージ	原因	対処
open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. Value cannot be null. (Parameter 'text')	resourceDiscoveryGroups.name に値が指定されていない。	resourceDiscoveryGroups.name の指定内容を見直してください。
Promitor Discovery Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. Failed to convert configuration value at 'authentication:Mode' to type 'Promitor.Integrations.Azure.Authentication.AuthenticationMode'.	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) の authentication.mode に不正な値を指定した。	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) の authentication.mode の指定内容を見直してください。
Validation failed: Azure authentication is not configured correctly - No identity was configured for service principle authentication Promitor is not configured correctly. Please fix validation issues and re-run.	Azure Resource Graph に接続するためのシークレットが登録されていない、かつ、Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) の authentication.mode に値が指定されていない。	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) の authentication.mode の指定内容を見直してください。
	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) で、 authentication.mode がServicePrincipal の場合に、 authentication.identityId に値が指定されていない。	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) の authentication.identityId の指定内容を見直してください。
Promitor Discovery Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. Failed to bind to address http://[::]:ポート: address already in use.	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) の server.httpPort にすでに使用されているポートを指定した。	Promitor Resource Discovery runtime 設定ファイル (runtime.yaml) の server.httpPort の指定内容を見直してください。
ClientSecretCredential authentication failed: Retry failed after 2 tries. Retry settings can be adjusted in	Resource Discovery と Scraper がネットワークから遮断された状態で起動した。	ネットワークを接続してください。

メッセージ	原因	対処
<p>ClientOptions.Retry. (Resource temporarily unavailable (ホスト:ポート)) (The operation was canceled.)</p>		
<p>Unhandled exception in job Azure Subscription Discovery System.AggregateException: One or more errors occurred. (ClientSecretCredential authentication failed: Retry failed after 4 tries. Retry settings can be adjusted in ClientOptions.Retry. (Resource temporarily unavailable (ホスト:ポート)) (Resource temporarily unavailable (ホスト:ポート)) (Resource temporarily unavailable (ホスト:ポート)) (Resource temporarily unavailable (ホスト:ポート)))</p>	<p>Resource Discovery がネットワークから遮断された状態で起動した。</p>	<p>ネットワークを接続してください。</p>
<p>Unhandled exception in job Azure Subscription Discovery System.AggregateException: One or more errors occurred. (Resource temporarily unavailable (ホスト:ポート))</p>	<p>Resource Discover の実行中にネットワークから遮断された。</p>	<p>ネットワークを接続してください。</p>
<p>ClientSecretCredential authentication failed: Retry failed after 4 tries. Retry settings can be adjusted in ClientOptions.Retry. (Name or service not known (ホスト:ポート)) (Name or service not known (ホスト:ポート)) (Name or service not known (ホスト:ポート)) (Name or service not known (ホスト:ポート))</p>	<p>不正なプロキシを設定して Resource Discovery を実行した。</p>	<p>プロキシ設定を見直してください。</p>

(10) script_exporter のログ

メッセージ	原因	対処
flag needs an argument: コマンドラインオプション	コマンドラインオプションに値が指定されていない。	コマンドラインオプションを見直してください。
open パス: no such file or directory	コマンドラインオプションの--config.file に存在しないパスが指定された。	コマンドラインオプションの--config.file の指定内容を見直してください。
listen tcp: address 指定した文字列: missing port in address	コマンドラインオプションの--web.listen-address に不正な値を指定した。	コマンドラインオプションの--web.listen-address の指定内容を見直してください。
<ul style="list-style-type: none"> Windows の場合 listen tcp: lookup ホスト名 : no such host <ul style="list-style-type: none"> Linux の場合 listen tcp: lookup ホスト名 on 10.0.0.1:53: read udp 10.1.0.1:46736->10.0.0.1:53: i/o timeout	コマンドラインオプションの--web.listen-address に存在しないアドレスを指定した。	正しいホスト名を指定してください。
<ul style="list-style-type: none"> Windows の場合 listen tcp : ポート: bind: Only one usage of each socket address (protocol/network address/port) is normally permitted. <ul style="list-style-type: none"> Linux の場合 listen tcp :ポート: bind: address already in use	コマンドラインオプションの--web.listen-address にすでに使用されているポートを指定した。	使用されていないポートを指定してください。
invalid value "指定した文字列" for flag -timeout-offset: parse error	コマンドラインオプションの--timeout-offset に不正な値を指定した。	コマンドラインオプションの--timeout-offset の指定内容を見直してください。
invalid value "指定した値" for flag -timeout-offset: value out of range	コマンドラインオプションの--timeout-offset に float64 の範囲外の値を指定した。	コマンドラインオプションの--timeout-offset の指定内容を見直してください。
<ul style="list-style-type: none"> Windows の場合 open 指定したパス: The system cannot find the file specified. <ul style="list-style-type: none"> Linux の場合 open 指定したパス: no such file or directory	コマンドラインオプションの--config.file に誤ったパスが指定された。	コマンドラインオプションの--config.file の指定内容を見直してください。
mapping values are not allowed in this context	コマンドラインオプションの--config.file に指定したファイルの項目に型が不正な値を指定した。	設定ファイルの指定内容を見直してください。

メッセージ	原因	対処
Script parameter is missing	Script exporter 設定ファイル (jpc_script_exporter.yml) のscripts の name に誤った値を指定した。	Script exporter 設定ファイル (jpc_script_exporter.yml) のscript.name の指定内容を見直してください。
Script not found	Prometheus 設定ファイル (jpc_prometheus_server.yml) のparams のscript に誤った値を指定した。	Prometheus 設定ファイル (jpc_prometheus_server.yml) のparams.script の指定内容を見直してください。
Script config "script名" has neither 'script' nor 'command'	Script exporter 設定ファイル (jpc_script_exporter.yml) のscripts のcommand が指定されていない。	Script exporter 設定ファイル (jpc_script_exporter.yml) のscripts.command の指定内容を見直してください。
Script failed: exit status 1	Script exporter 設定ファイル (jpc_script_exporter.yml) のscripts のcommand に指定したスクリプトの実行に失敗した。	指定したスクリプトを見直してください。
Script 'script名' execution failed <ul style="list-style-type: none"> Windows の場合 exec: 指定した文字列: file does not exist <ul style="list-style-type: none"> Linux の場合 fork/exec 指定した文字列: exec format error	Script exporter 設定ファイル (jpc_script_exporter.yml) のscripts のcommand に実行可能ファイルではないものを指定した。	Script exporter 設定ファイル (jpc_script_exporter.yml) の指定内容を見直してください。
Script 'script名' execution failed <ul style="list-style-type: none"> Windows の場合 exec: 指定した文字列: Access is denied <ul style="list-style-type: none"> Linux の場合 fork/exec 指定した文字列: permission denied	Script exporter 設定ファイル (jpc_script_exporter.yml) のscripts のcommand に実行権限のないものを指定した。	指定したスクリプトが実行できるように権限を変更してください。
Script 'script名' execution failed <ul style="list-style-type: none"> Windows の場合 exec: "指定した文字列": file does not exist <ul style="list-style-type: none"> Linux の場合 fork/exec: "指定した文字列": no such file or directory	Script exporter 設定ファイル (jpc_script_exporter.yml) のscripts のcommand に存在しないスクリプトを指定した。	Script exporter 設定ファイル (jpc_script_exporter.yml) のscripts.command の指定内容を見直してください。
Script 'script名' execution failed <ul style="list-style-type: none"> Windows の場合 	Script の実行がタイムアウトした。	Script exporter 設定ファイル (jpc_script_exporter.yml) の

メッセージ	原因	対処
exit status 1 • Linux の場合 signal: killed		scripts.timeout の指定内容を見直してください。

(11) Fluentd のログ

メッセージ	原因	対処
error="tail: 'path' parameter is required on tail input"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの path を指定しなかった。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="Unsupported timezone~"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの timezone に不正な値を指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="specifying timezone requires time format"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの time_format を指定せずに、timezone に値を指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="valid options are string, unixtime, float, mixed but got ~"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの time_type に不正な値を指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="unknown encoding name~"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの from_encoding に不正な値を指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="No named captures in 'expression' parameter. The regexp must have at least one named capture"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの expression に名前付きキャプチャ (?<NAME> PATTERN) が含まれない正規表現を指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="format should be Regexp, need //, ~"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションのログを解析する正規表現に正規表現をデリミタ (/) で挟まずに指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="valid options are rfc3164, rfc5424, auto but got ~"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの message_format に不正な値を指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。

メッセージ	原因	対処
error="with_priority' parameter is required but ~ is specified"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの with_priority に不正な値を指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
"valid options are regexp, string but got~"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの parser_type に不正な値を指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="support_colonless_ident' parameter is required but ~ is specified"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの support_colonless_ident に不正な値を指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
got incomplete JSON array configuration at ~ (Fluent::ConfigParseError)	テキスト形式のログファイルの監視定義ファイルで、[Inclusion Settings]セクションまたは、[Exclusion Settings]セクションの pattern に正規表現をデリミタ (/) で挟まずに指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="Plugin 'tail' does not support multi workers configuration (Fluent::Plugin::TailInput)"	テキスト形式のログファイルの監視定義ファイルで、workers パラメータを 2 以上の数に指定した場合で、worker の id を複数指定した。または、workers パラメータを 2 以上の数に指定した場合で、<worker>ディレクティブを指定しなかった。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="Unknown parser plugin ~. Run 'gem search -rd fluent-plugin' to find plugins"	テキスト形式のログファイルの監視定義ファイルで、[Input Settings]セクションの<parse>ディレクティブの @type に不正な値を指定した。	テキスト形式のログファイルの監視定義ファイルを見直してください。
error="Invalid Bookmark XML is loaded.~"	Windows イベントログの監視定義ファイルで、[Input Settings]セクションの channels に不正な値を指定した。	Windows イベントログの監視定義ファイルを見直してください。
error="Plugin 'windows_eventlog2' does not support multi workers configuration (Fluent::Plugin::WindowsEventLog2Input)"	Windows イベントログの監視定義ファイルで、workers パラメータを 2 以上の数に指定した場合で、worker の id を複数指定した。または、workers パラメータを 2 以上の数に指定した場合で、<worker>ディレクティブを指定しなかった。	Windows イベントログの監視定義ファイルを見直してください。
error="valid options are throw_exception, block, drop_oldest_chunk but got~"	ログ監視共通定義ファイルで、[Output Settings]セクションの overflow_action に不正な値を指定した。	ログ監視共通定義ファイルを見直してください。

メッセージ	原因	対処
valid options are trace, debug, info, warn, error, fatal but got ~ (Fluent::ConfigParseError)	ログ監視共通定義ファイルで, [System Settings]セクションの log_level に不正な値を指定した。	ログ監視共通定義ファイルを見直してください。
invalid number of workers (must be > 0):0 (Fluent::ConfigError)	ログ監視共通定義ファイルで, [System Settings]セクションの workers パラメータに不正な値を指定した。	ログ監視共通定義ファイルを見直してください。
error="greater first_worker_id<1> than last_worker_id<0> specified by <worker> directive is not allowed. Available multi worker assign syntax is <smaller_worker_id>-<greater_worker_id>"	ログ監視共通定義ファイル, ログメトリクス定義ファイルのいずれかで, <worker N-M>ディレクティブにおいて N > M となる数値を指定した。	ログ監視共通定義ファイル, ログメトリクス定義ファイルを見直してください。
error="worker id ~ specified by <worker> directive is not allowed. Available worker id is between ~"	ログ監視共通定義ファイル, テキスト形式のログファイルの監視定義ファイル, Windows イベントログの監視定義ファイル, ログメトリクス定義ファイルのいずれかで, workers パラメータの値を超える範囲で, <worker>ディレクティブの引数を指定した。または, workers パラメータを指定せずに, <worker N-M>ディレクティブまたは <worker>ディレクティブの引数に 0 以外の id を指定した。	ログ監視共通定義ファイル, テキスト形式のログファイルの監視定義ファイル, Windows イベントログの監視定義ファイル, ログメトリクス定義ファイルを見直してください。
error="Missing worker id on <worker> directive"	ログ監視共通定義ファイル, テキスト形式のログファイルの監視定義ファイル, Windows イベントログの監視定義ファイル, ログメトリクス定義ファイルのいずれかで, <worker>ディレクティブの引数に worker の id を指定しなかった。	ログ監視共通定義ファイル, テキスト形式のログファイルの監視定義ファイル, Windows イベントログの監視定義ファイル, ログメトリクス定義ファイルを見直してください。
[error]: failed to read data from plugin storage file path=~	storage ファイルが破損している。	storage ファイルを削除してから起動してください。
Not a directory @ dir_s_mkdir - ~ (Errno::ENOTDIR)	不正な監視名を設定した。	監視名を見直してください。

(a) prometheus-client のログ

メッセージ	原因	対処
metric name must match <code>/[a-zA-Z_][a-zA-Z0-9_]*/</code> (ArgumentError)	ログメトリクス定義ファイルで、 <code><metric></code> の name が空である。	ログメトリクス定義ファイルで、 <code><metric></code> の name を指定してください。
docstring must be given (ArgumentError)	ログメトリクス定義ファイルで、 <code><metric></code> の desc が空である。	ログメトリクス定義ファイルで、 <code><metric></code> の desc を指定してください。
label ラベルのキー must not start with <code>_</code> (Prometheus::Client::LabelSetValidator::ReservedLabelError)	ログメトリクス定義ファイルの <code><labels></code> で、ラベルのキーを <code>_</code> (半角アンダースコア 2 つ) で開始している。	ログメトリクス定義ファイルの <code><labels></code> で、ラベルのキーを <code>_</code> (半角アンダースコア 2 つ) で開始しないように指定してください。
label name must match <code>/(?-mix:%%A[a-zA-Z_][a-zA-Z0-9_]*%%Z)/</code> (Prometheus::Client::LabelSetValidator::InvalidLabelError)	ログメトリクス定義ファイルの <code><labels></code> で、ラベルのキーが正規表現 <code>/(?-mix:%%A[a-zA-Z_][a-zA-Z0-9_]*%%Z)/</code> に合致しない。	ログメトリクス定義ファイルの <code><labels></code> で、ラベルのキーを正規表現 <code>/(?-mix:%%A[a-zA-Z_][a-zA-Z0-9_]*%%Z)/</code> に合致するように指定してください。

(b) fluent-plugin-prometheus プラグインのログ

メッセージ	原因	対処
config error file="物理インストール先ディレクトリ/jplima/conf/ログ監視共通定義ファイル名" error_class=Fluent::ConfigError error="Missing '@type' parameter on <source> directive"	ログメトリクス定義ファイルの <code><source></code> で、 <code>@type prometheus</code> という設定が存在しない。	ログメトリクス定義ファイルの <code><source></code> で、 <code>@type prometheus</code> を設定してください。
config error file="物理インストール先ディレクトリ/jplima/conf/ログ監視共通定義ファイル名" error_class=Fluent::NotFoundPluginError error="Unknown input plugin '@type' で指定した値". Run 'gem search -rd fluent-plugin' to find plugins"	ログメトリクス定義ファイルの <code><source></code> で、 <code>@type</code> が空である、または、 <code>@type</code> に指定した値が「prometheus」ではない。	ログメトリクス機能を利用する場合は、ログメトリクス定義ファイルの <code><source></code> で、 <code>@type</code> には「prometheus」を設定してください。
#0 unexpected error error_class=SocketError error="getaddrinfo: Name or service not known"	ログメトリクス定義ファイルの <code><source></code> で、 <code>bind</code> が不正な値である。	ログメトリクス定義ファイルの <code><source></code> で、 <code>bind</code> に正しいホスト名を指定してください。

メッセージ	原因	対処
#0 unexpected error error_class=Errno::EADDRNO TAVAIL error="Cannot assign requested address - bind(2) for bind で指定し た値: port で指定した値"	ログメトリクス定義ファイルの<source>で、 bind が不正なフォーマットである。	ログメトリクス定義ファイルの<source>で、 bind に正しい IP アドレスのフォーマットを指 定してください。
config error file="物理イン ストール先ディレクトリ/ jp1ima/conf/ログ監視共通定 義ファイル名" error_class=Fluent::Config Error error="Missing '@type' parameter on <match> directive"	ログメトリクス定義ファイルの<match>にお いて、@type prometheus という設定が存在 しない。	ログメトリクス定義ファイルの<match>におい て、@type prometheus を設定してください。
config error file="物理イン ストール先ディレクトリ/ jp1ima/conf/ログ監視共通定 義ファイル名" error_class=Fluent::NotFou ndPluginError error="Unknown output plugin '@type で指定した 値'. Run 'gem search -rd fluent-plugin' to find plugins"	ログメトリクス定義ファイルの<match>で、 @type が空である、または @type で指定し た値が「prometheus」ではない。	ログメトリクス機能を利用する場合は、ログメ トリクス定義ファイルの<match>で、@type に は「prometheus」を設定してください。
section <セクション名> is not used in <match> of prometheus plugin	ログメトリクス定義ファイルの<match>で、 指定したセクション名が、次のどちらでもな かった。 <ul style="list-style-type: none">metriclabels	ログメトリクス定義ファイルの<match>で、セ クション名には、次のどちらかを指定してくだ さい。 <ul style="list-style-type: none">metriclabels
unmatched end tag at fluentd_任意の名前 _logmetrics.conf 定義ファイル の内容 (Fluent::ConfigparseError)	ログメトリクス定義ファイルで、セクション の開始と終了のどちらかが指定されていない。	ログメトリクス定義ファイルの次に示すセク ションで、開始と終了が定義されているかを見 直してください。 <ul style="list-style-type: none"><source><parse><match><metric><labels>
parameter 'パラメーター名' in セクション	ログメトリクス定義ファイルのセクション で、利用できないパラメーター (パラメー ター名) を指定している。	ログメトリクス定義ファイルのセクションで、 パラメーター (パラメーター名) の指定内容 を見直してください。
#0 unknown placeholder `ブ レースホルダー` found	ログメトリクス定義ファイルのラベルセク ションで、設定したプレースホルダーが、ブ レースホルダーとして不正である。	ログメトリクス定義ファイルのラベルセクショ ンで、設定したプレースホルダーの設定内容 を見直してください。

メッセージ	原因	対処
config error file="物理インストール先ディレクトリ/jp1ima/conf/ログ監視共通定義ファイル名" error_class=Fluent::ConfigError error="labels section must have at most 1"	ログメトリクス定義ファイルで、1つのセクション内に、<labels>が並列して複数存在する。	ログメトリクス定義ファイルで、1つのセクション内に存在する<labels>が1つとなるように修正してください。
config error file="物理インストール先ディレクトリ/jp1ima/conf/ログ監視共通定義ファイル名" error_class=Fluent::ConfigError error="type option must be 'counter', 'gauge', 'summary' or 'histogram'"	ログメトリクス定義ファイルで、<metric>のtypeに、次に示す文字列以外が指定されている、または、何も指定されていない。 <ul style="list-style-type: none"> • counter • gauge 	ログメトリクス定義ファイルで、<metric>のtypeに、次に示す文字列のどれかを指定してください。 <ul style="list-style-type: none"> • counter • gauge
	ログメトリクス定義ファイルで、<metric>のtypeが存在しない。	
#0 prometheus: failed to instrument a metric. error_class=ArgumentError error=#<ArgumentError: comparison of String with 0 failed> tag="任意のタグ" name="任意のログメトリクス名"	ログメトリクス定義ファイルにおいて定義した、ログメトリクスタイプcounterのログメトリクスの値が、RubyのIntegerまたはFloatでない。	ログメトリクス定義ファイルの<parse>で、ログメッセージの期待した値を抽出できているか、または、<metric>のkeyで期待している項目が指定できているか、を見直してください。
#0 prometheus: failed to instrument a metric. error_class=ArgumentError error=#<ArgumentError: value must be a number> tag="任意のタグ" name="任意のログメトリクス名"	ログメトリクス定義ファイルで定義した、ログメトリクスタイプgaugeのログメトリクスの値が、RubyのIntegerまたはFloatでない。	ログメトリクス定義ファイルの<parse>で、ログメッセージの期待した値を抽出できているか、または、<metric>のkeyで期待している項目が指定できているか、を見直してください。
#0 prometheus: failed to instrument a metric. error_class=Prometheus::Client::LabelSetValidator::InvalidLabelSetError error=#<Prometheus::Client::LabelSetValidator::InvalidLabelSetError: labels must have the same signature (keys given: [:ラベルのキー] vs. keys expected: [:ラベルのキー]> tag="任意のタグ" name="任意のログメトリクス名"	ログメトリクス定義ファイルで、同じnameかつ同じtypeかつ同じdescを持つログメトリクス（任意のログメトリクス名）が定義されており、それらのログメトリクスの<labels>の定義が異なる。	ログメトリクス定義ファイルで、すべてのログメトリクス（任意のログメトリクス名）の<labels>の定義内容を見直してください。

メッセージ	原因	対処
config error file="物理インストール先ディレクトリ/jplima/conf/ログ監視共通定義ファイル名" error_class=Fluent::Config Error error="metric requires 'name' option"	ログメトリクス定義ファイルにおいて、<metric>に設定項目nameが存在しない。	ログメトリクス定義ファイルで、<metric>に設定項目nameを指定してください。
config error file="物理インストール先ディレクトリ/jplima/conf/ログ監視共通定義ファイル名" error_class=Fluent::Config Error error="metric requires 'desc' option"	ログメトリクス定義ファイルで、<metric>に設定項目descが存在しない。	ログメトリクス定義ファイルで、<metric>に設定項目descを指定してください。
config error file="物理インストール先ディレクトリ/jplima/conf/ログ監視共通定義ファイル名" error_class=Fluent::Config Error error="gauge metric requires 'key' option"	ログメトリクス定義ファイルで、<metric>のtypeにgaugeを指定しているが、設定項目keyが存在しない。	ログメトリクス定義ファイルで、<metric>の設定項目keyを指定してください。
任意のログメトリクス名 has already been registered as ログメトリクスタイプ type (Fluent::Plugin::Prometheus::AlreadyRegisteredError)	ログメトリクス定義ファイルで、同じnameかつ同じdescを持つログメトリクス(任意のログメトリクス名)が定義されており、それらのtypeの指定が異なる。	ログメトリクス定義ファイルで、すべてのログメトリクス(任意のログメトリクス名)のtypeの指定内容を見直してください。
任意のログメトリクス名 has already been registered with different docstring	ログメトリクス定義ファイルで、同じnameかつ同じtypeを持つログメトリクス(任意のログメトリクス名)が定義されており、それらのdescの指定が異なる。	ログメトリクス定義ファイルで、すべてのログメトリクス(任意のログメトリクス名)のdescの指定内容を見直してください。

12.5.2 主な入力ミスに対して発生する現象と回復方法

(1) Prometheus server のスクレイプ先に不正なホストやポートを指定した

現象

スクレイプが失敗し、up メトリックが0として収集される。

スクレイプ先の設定を誤った Prometheus server 経由で取得するデータに関して、統合オペレーション・ビューアーのトレンド情報に、最新の情報が表示されない。

回復方法

スクレイプの定義を修正して、Prometheus server をリロードまたは再起動してください。

(2) Prometheus server のリモートライト先に不正なホストやポートを指定した

現象

リモートライト先の設定を誤った Prometheus server 経由で取得するデータに関して、統合オペレーション・ビューアーのトレンド情報に、最新の情報が表示されない。

回復方法

リモートライトの定義を修正して、Prometheus server をリロードまたは再起動してください。

(3) Prometheus server のアラート通知先に不正なホストやポートを指定した

現象

アラート通知先の設定を誤った Prometheus server から発生するアラートに関して、統合オペレーション・ビューアーの JP1 イベント一覧に、最新の情報が表示されない。

回復方法

通知先の定義を修正して、Prometheus server をリロードまたは再起動してください。

(4) Alertmanager の通知先に不正なホストやポートを指定した

現象

通知先の設定を誤った Alertmanager から送信するアラートに関して、統合オペレーション・ビューアーの JP1 イベント一覧に、最新の情報が表示されない。

回復方法

通知先の定義を修正して、Alertmanager をリロードまたは再起動してください。

(5) Blackbox exporter の監視先に不正なホストやポートを指定した

現象

監視先の情報取得に失敗し、probe_success メトリックが 0 として収集される。

回復方法

監視先のホストやポートの定義を修正して、Prometheus server をリロードまたは再起動してください。

(6) Prometheus server の定義ファイルの書式が不正

現象

Prometheus server のリロードの API を実行したとき、ステータスコード 500 が返却され、次のようなメッセージが表示される。

```
failed to reload config: couldn't load configuration (--config.file="ファイルのパス"): parsing YAML file ファイルのパス: yaml: unmarshal errors: line 行数: field test not found in type config.plain
```

回復方法

メッセージに出力されているファイルのパスと行数を確認し、定義を修正して、Prometheus server をリロードまたは再起動してください。

(7) ディスカバリ設定ファイルの書式が不正

現象

jddcreatetree コマンドおよび jddupdatetree コマンドの実行に成功したにも関わらず、ディスカバリ設定ファイルに記述した情報の IM 管理ノードが統合オペレーション・ビューアーに表示されない。

回復方法

コロンの指定や半角スペースの数が合っているかなど、ディスカバリ設定ファイルの書式が誤っていないかを確認してください。誤りを訂正したあと、再度 jddcreatetree コマンドおよび jddupdatetree コマンド（構成変更モード（-c オプション）を指定）を実行してください。

(8) ログ監視共通定義ファイルの書式が不正

現象

ログ監視共通定義ファイル（jpc_fluentd_common.conf）の、<buffer>ディレクティブ内のpathパラメーターに対して、256バイトを超えるパス名が指定されている場合、または、Windows環境で、: ; * ? " < > | とタブ・スペースを含むパスが指定されている場合に、fluentdのログに、次のようなエラーが繰り返して出力され続ける。

```
unexpected error error_class=Errno::ENOENT error="No such file or directory @ dir_s_mkdir - ディレクトリ名 "
```

回復方法

ログ監視共通定義ファイル（jpc_fluentd_common.conf）の、<buffer>ディレクティブ内のpathパラメーターの値について、書式と設定内容が誤っていないかを確認してください。

(9) テキスト形式のログファイルの監視定義ファイルの書式が不正

現象

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）の、[Input Settings]セクション内のpos_fileパラメーターに対して、空白、または、OSのファイル名の上限值を超える文字列が指定されている場合に、fluentdのログに、次のようなエラーが繰り返して出力され続ける。

```
unexpected error error_class=Errno::ENOENT error="No such file or directory @ rb_sysopen - ディレクトリ名 "
```

回復方法

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) の, [Input Settings]セクション内のpos_fileパラメーターについて, 書式と設定内容が誤っていないかを確認してください。

(10) Script exporter が存在しないスクリプトを実行した

現象

script_success メトリックが 0 として収集される。また, script_exit_code メトリックが-1 として収集される。

回復方法

定義を修正して Script exporter をリロードまたは再起動してください。

(11) Promitor の Scraper の Resource Discovery に不正なホストやポートを指定した

現象

リソースディスカバリーから取得するメトリックが取得されない。

回復方法

定義を修正して Promitor の Scraper をリロードまたは再起動してください。

12.5.3 主なトラブルと対処方法

一般的に想定されるトラブルについて, 対処方法を説明します。

(1) JP1/IM - View からログインできない場合の対処方法

メッセージの種類によって対処方法が異なります。

「KAVB1200-E 接続中に通信エラーが発生しました」メッセージが出力される。

要因

次の要因が考えられます。

- JP1/IM - Manager が起動されていません。
- 接続先ホスト名が誤っています。

対処

要因に従って対処してください。

- JP1/IM - Manager を起動してください。
- 接続先ホスト名が正しいかどうかを確認してください。

「KAVB0104-E ユーザー認証に失敗しました」メッセージが出力される。

要因

接続先に対するユーザー名またはパスワードが誤っています。

対処

接続先に対するユーザー名またはパスワードが正しいかどうかを確認してください。

「KAVB0109-E 接続ホストと認証サーバの間で、通信エラーが発生しました」または「KAVB0111-E 認証サーバに接続できません」メッセージが出力される。

要因

接続先ホスト上で設定されている認証サーバが起動されていません。

対処

次のことを確認し、問題点を対処してください。

- 認証サーバが起動しているか。
- 接続ホストと認証サーバ間の通信ができるか。
- 認証サーバの設定が間違っていないか。

「KNAN20100-E 指定された接続先ホスト名のアドレスの解決に失敗しました」メッセージが出力される。

要因

次の要因が考えられます。

- 接続先ホスト名が誤っています。
- 接続先ホストが起動されていません。
- 接続先ホストとの通信で障害が発生しています。

対処

要因に従って対処してください。

- 接続先ホスト名が正しいかどうかを確認してください。
- 接続先ホストが起動しているかどうかを確認してください。
- 接続先ホストとの通信に問題はないかどうかを確認してください。

「KNAN20101-E 接続中に通信エラーが発生しました」メッセージが出力される。

要因

次の要因が考えられます。

- 接続先ホスト名が誤っています。
- 接続先ホストが起動されていません。
- 接続先ホストとの通信で障害が発生しています。

対処

要因に従って対処してください。

- 接続先ホスト名が正しいかどうかを確認してください。
- 接続先ホストが起動しているかどうかを確認してください。
- 接続先ホストとの通信に問題はないかどうかを確認してください。

「KNAN20102-E 接続中に通信エラーが発生しました」メッセージが出力される。

要因

次の要因が考えられます。

- 接続先ホスト名が誤っています。
- ポート番号が誤っています。
- 接続先ホストが起動されていません。
- 接続先ホストとの通信で障害が発生しています。

対処

要因に従って対処してください。

- 接続先ホスト名が正しいかどうかを確認してください。
- ポート番号は使用できる番号かどうかを確認してください。
- 接続先ホストが起動しているかどうかを確認してください。
- 接続先ホストとの通信に問題はないかどうかを確認してください。

「KNAN20103-E データ送信中に、通信エラーが発生しました」メッセージが出力される。

要因

接続ホストと認証サーバの間で、通信エラーが発生しました。

対処

次の内容を確認してから、再実行してください。

- 接続ホスト名が正しいかどうかを確認してください。
- 接続ホストが起動しているかどうかを確認してください。
- 接続ホストとの通信に問題はないかどうかを確認してください。

「KNAN20104-E データ受信中に、通信エラーが発生しました」メッセージが出力される。

要因

ホスト接続中に、通信エラーが発生しました。

対処

次を確認してから、再実行してください。

- 接続先ホスト名が正しいかどうかを確認してください。
- ポート番号が正しいかどうかを確認してください。
- 接続先ホストが起動しているかどうかを確認してください。
- 接続先ホストとの通信に問題はないかどうかを確認してください。

(2) イベントサービスへの接続に失敗する場合の対処方法

要因 1

マネージャー上のイベントサービスが起動していないおそれがあります。

対処 1

`jbs_spmd_status` コマンドでマネージャー上のイベントサービスが起動しているかどうかを確認してください。

起動していない場合は、イベントサービスを起動してください。

要因 2

API 設定ファイル (`api`) の `server` パラメーターの設定に誤りがあるおそれがあります。

対処 2

API 設定ファイル (`api`) の `server` パラメーターの設定は、イベントサーバ設定ファイル (`conf`) の `ports` パラメーターの設定と一致させてください。

なお、API 設定ファイル (`api`) の `server` パラメーターのアドレスやイベント設定ファイル (`conf`) の `ports` パラメーターのアドレスにホスト名を指定している場合、IP アドレスの解決は OS の処理に依存するため、意図する IP アドレスで動作しないおそれがあります。

API 設定ファイル (`api`)、およびイベントサーバ設定ファイル (`conf`) については、マニュアル「JP1/Base 運用ガイド」の API 設定ファイル (`api`)、およびイベントサーバ設定ファイル (`conf`) の説明をしている章を参照してください。

要因 3

IPv6 ホストで JP1/IM - Manager を起動しているおそれがあります。

対処 3

JP1/IM - Manager は、IPv6 ホストをサポートしていません。監視対象ホストが IPv6 ホストの場合は、JP1/IM - Manager を IPv4・IPv6 ホストにインストールしてください。また、各エラーメッセージに従って対処してください。

(3) [イベントコンソール] 画面で定義メニューが表示されない場合の対処方法

[イベントコンソール] 画面の「オプション」のメニューで定義関連が非活性となる。

要因

JP1 資源グループの設定が誤っています。

対処

JP1 資源グループの設定で、ログインする JP1 ユーザーの JP1 資源グループにグループ名「JP1_Console」、権限レベルに「JP1_Console_Admin」または「JP1_Console_Operator」が設定されているか確認してください。

(4) トラップした JP1 イベントのメッセージが文字化けしてしまう場合の対処方法

次の要因が考えられます。

- ・ 監視するログファイルの文字コードと、[設定ファイル] ページで設定した文字コードが一致していない。
- ・ 設定した文字コードがエージェントホストでサポートされていない。

それぞれの対処を次に示します。

監視するログファイルの文字コードと、[設定ファイル] ページで設定した文字コードが一致していない。

監視するログファイルの文字コードを設定し直し、再度実行してください。

なお、このトラブルは、リモート監視の場合も同様です。

設定した文字コードがエージェントホストでサポートされていない。

JP1/IM - Manager がサポートしている文字コードでも、エージェントホストにインストールされている JP1/Base のバージョンによっては、設定できない文字コードがあります。エージェントホストにインストールされている JP1/Base のバージョンを確認し、サポートされている文字コードを設定してください。そのあと、再度実行してください。

(5) コマンド実行ができない場合の対処方法

[コマンド実行] 画面で「KAVB0415-E 実行ホスト名に指定された業務グループ、または監視グループが定義されていないため、コマンドが実行できません。(実行ホスト名:実行ホスト名)」メッセージが出力される。

要因

実行ホスト名に指定した業務グループ、または監視グループが定義されていません。

対処

業務グループまたは監視グループを見直してから、コマンドを再実行してください。なお、このメッセージは JP1/Base の `jcocmdshow` コマンドでは確認できません。

それでも実行できない場合は、システム管理者に連絡し、業務グループの設定を確認してください。

[コマンド実行] 画面で「KAVB0416-E 実行ホスト名に指定されたホストが管理対象でないため、コマンドが実行できません。(実行ホスト名:実行ホスト名)」メッセージが出力される。

要因

実行ホスト名に指定したホストは管理対象ではありません。

対処

ホストを見直してから、コマンドを再実行してください。なお、このメッセージは JP1/Base の `jcocmdshow` コマンドでは確認できません。

それでも実行できない場合は、システム管理者に連絡し、業務グループの設定を確認してください。

[コマンド実行] 画面で [KAVB0417-E 実行ホスト名に指定された業務グループに対してコマンドを実行する権限がないため、コマンドが実行できません。(実行ホスト名:実行ホスト名)] メッセージが出力される。

要因

実行ホスト名に指定した業務グループに対してコマンドを実行する権限がありません。

対処

業務グループ、または監視グループを見直してから、コマンドを再実行してください。なお、このメッセージは JP1/Base の jcocmdshow コマンドでは確認できません。

それでも実行できない場合は、システム管理者に連絡し、業務グループの設定を確認してください。

[コマンド実行] 画面で [KAVB0418-E 実行ホスト名に指定されたホストに対してコマンドを実行する権限がないため、コマンドが実行できません。(実行ホスト名:実行ホスト名)] メッセージが出力される。

要因

実行ホスト名に指定したホストに対してコマンドを実行する権限がありません。

対処

ホストを見直してから、コマンドを再実行してください。なお、このメッセージは JP1/Base の jcocmdshow コマンドでは確認できません。

それでも実行できない場合は、システム管理者に連絡し、業務グループの設定を確認してください。

[コマンド実行] 画面で [KAVB0419-E 実行ホスト名に指定されたホスト名と同じ名称のホストグループが定義されているため、コマンドが実行できません。(実行ホスト名:実行ホスト名)] メッセージが出力される。

要因

実行先ホスト名に実行ホストと同じ名称のホストグループ名が指定されています。

対処

実行ホスト名に指定したホスト名と同じ名称のホストグループがないか確認してください。ある場合は、ホスト名かホストグループのどちらかの名称を変更してください。

[コマンド実行] 画面で [KAVB0422-E 業務グループ、または監視グループにホストが定義されていません。(グループ名:グループ名)] メッセージが出力される。

要因

実行ホスト名に指定した業務グループ、または監視グループには、ホストが一つも定義されていません。

対処

指定した業務グループ、または監視グループにホストを定義してください。また、業務グループ、または監視グループのパスの表記を見直してください。

[コマンド実行] 画面で「KAVB0423-E 業務グループ、または監視グループが定義されていません。(グループ名:グループ名)」メッセージが出力される。

要因

実行ホスト名に、定義されていない業務グループ、または監視グループが指定されています。

対処

指定した業務グループ、または監視グループを定義してください。また、業務グループ、または監視グループのパスの表記を見直してください。

[コマンド実行] 画面で「KAVB2027-E ユーザー名のユーザ偽装に失敗したため、コマンド実行できません」メッセージが出力される。

要因

ユーザーマッピングの設定が誤っています。

対処

ユーザーマッピングの設定を確認してください。設定されていない場合はユーザーマッピングを設定してください。この設定は Windows の場合必須です。

なお、マッピング元のサーバ名として指定するホストが DNS を使用している場合、ドメイン名を含めて記述する必要があります。ホスト名が正しくて、偽装に失敗する場合は DNS を使用していないか確認してください。

ユーザーマッピングの設定については、マニュアル「JP1/Base 運用ガイド」のユーザーマッピングに関する章を参照してください。

[コマンド実行] 画面で「KAVB2031-E ホスト (ホスト名) が管理対象でないため、コマンドが実行できません」メッセージが出力される。

要因

構成定義ファイルの定義に誤りがあります。または、実行ホスト名が解決できません。

対処

- 構成定義ファイルの定義で構成情報が定義されているか確認してください。
- 実行ホスト名を解決できるようにしてください。
- Windows で物理ホストと論理ホストの両方を起動する環境でこのメッセージが出力される場合は、ネットワークの設定が不足しています。詳細については、マニュアル「JP1/Base 運用ガイド」のクラスタ運用に関する注意事項 (Windows 限定の注意事項) の中の、同一ホスト上で物理ホスト環境と論理ホスト環境を構築する場合の項を参照してください。

[コマンド実行] 画面で「KAVB8452-E ログイン中に業務グループによる参照・操作制限機能が有効から無効に変更されたため、実行できません」メッセージが出力される。

要因

JP1/IM - View が接続している状態で、業務グループによる参照・操作制限を有効から無効に変更しています。

対処

JP1/IM - View を再起動したあと、再ログインしてからコマンドを再実行してください。

DOS プロンプトでの実行結果と [コマンド実行] 画面や自動アクションでの実行結果が異なる。

要因

実行する OS ユーザーの環境が不正です。

対処

jccomddef コマンドの `-loaduserprofile` オプションを有効にしてください。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「9.4.4(3)(c) コマンドを実行するときの環境」、およびマニュアル「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。

[コマンド実行内容プレビュー] 画面からコマンドを実行すると、KAVB0002-E のメッセージが表示され、コマンドが中断される。

要因

実行ホスト名または実行コマンドが指定されていません。

対処

実行ホスト名または実行コマンドを指定し、再度コマンドを実行してください。

[コマンド実行内容プレビュー] 画面からコマンドを実行すると、KAVB1037-E のメッセージが表示され、コマンドが中断される。

要因

実行ホスト名、実行コマンド、または環境変数ファイルに指定した値が上限値を超えています。

対処

上限値を超えている項目の値を見直し、再度コマンドを実行してください。

[コマンド実行] 画面が起動できなく、KAVB1046-E のメッセージが表示される。

要因

イベント引き継ぎ情報変換設定ファイルの読み込み時に、I/O エラーが発生しました。

対処

必要な権限がイベント引き継ぎ情報変換設定ファイルに設定されているか確認し、再度コマンドを実行してください。

それでも実行できない場合は、システム管理者に連絡してください。

(6) イベント情報を引き継げない場合の対処方法

属性値が引き継がれない。また、[コマンド実行内容プレビュー] 画面に警告情報が表示される。

要因

変数に対応する属性が、イベントに存在しません。

または、変数に対応する属性値がありません。

対処

指定したイベントおよび変数を指定したコマンドの実行内容を確認し、再度コマンドを実行してください。

[コマンド実行] 画面に引き継ぎ対象のイベントが表示されない。

要因

引き継ぎできないメニューまたはボタンをクリックしました。

対処

引き継げるイベントを一つ選択し、引き継ぎできるメニューまたはボタンをクリックしてください。

イベント引き継ぎ情報の特殊文字が変換されない。また、KAVB1040-W, KAVB1041-W, KAVB1042-W, KAVB1043-W, または KAVB1044-W のメッセージが表示される。

要因

イベント引き継ぎ情報変換設定ファイルが不正です。

対処

イベント引き継ぎ情報変換設定ファイルを見直し、[コマンド実行] 画面を再起動してください。

[コマンド実行内容プレビュー] 画面で、切り捨て前の文字がすべて表示されない。また、KAVB1036-W のメッセージが表示される。

要因

変数を置き換えたあとの切り捨て前の値の文字数が、[コマンド実行内容プレビュー] 画面のテキストエリアに表示できる上限値を超えています。

対処

変数を指定しているコマンド実行内容を見直し、再度実行してください。

(7) [コマンド] ボタンからコマンドを実行できない場合の対処方法

KAVB1035-E のメッセージが表示され、コマンドが中断される。

要因

実行するコマンドはイベントを引き継ぐ設定になっていますが、引き継ぎ対象のイベントが指定されていません。

対処

引き継ぐイベントを指定し、再度実行してください。

KAVB0002-E のメッセージが表示され、コマンドが中断される。

要因

イベント情報を引き継いだあとに、実行ホスト名または実行コマンドの値が空文字になっています。

対処

実行するコマンドに設定している項目の変数名、および引き継ぐイベントが正しいか確認し、再度実行してください。

KAVB1037-E のメッセージが表示され、コマンドが中断される。

要因

イベント情報を引き継いだあとに、実行ホスト名、実行コマンド、または環境変数ファイルに指定した値が上限値を超えています。

対処

上限値を超えた項目の値を見直し、再度実行してください。

(8) クライアントアプリケーションを起動できない場合の対処方法

KAVB1034-E のメッセージが [コマンド実行] 画面に表示され、コマンドが中断される。

次の要因が考えられます。

- コマンドの実行ファイルパスが見つからない。
- コマンドの実行権限がない。
- コマンドプロセスの起動時に、入出力エラーが発生した。

それぞれの対処を次に示します。

コマンドの実行ファイルパスが見つからない。

コマンドラインを見直し、コマンドプロンプトで実行できることを確認してください。そのあと、再度実行してください。

コマンドの実行権限がない。

実行するコマンドに実行権限があるか確認し、コマンドプロンプトで実行できることを確認してください。そのあと、再度実行してください。

コマンドプロセスの起動時に、入出力エラーが発生した。

実行するコマンドがコマンドプロンプトで実行できることを確認し、再度実行してください。

(9) コマンド実行履歴ファイルが壊れている場合の対処方法

電源断によるマシン停止などによってコマンド実行履歴ファイルへの書き込みが中断された場合、自動アクションまたはコマンド実行のコマンド実行履歴ファイルが壊れる場合があります。

その場合、次に示すメッセージが出力されます。

- JP1/IM - View の [アクション結果詳細] 画面、またはjcashowa コマンドで自動アクションの実行結果を表示したときに、実行結果に「KAVB5151-W コマンド実行履歴からデータの取得に失敗しました」が表示される。
自動アクションのコマンド実行履歴ファイルが壊れているおそれがあります。
- jcocmdlog コマンドを実行したときに、「KAVB2523-E コマンド実行のコマンド実行履歴ファイルがオープンできません」が出力される。

コマンド実行のコマンド実行履歴ファイルが壊れているおそれがあります。

- `jcocmdlog` コマンドを実行したときに、「KAVB2525-E 自動アクションのコマンド実行履歴ファイルがオープンできません」が出力される。

自動アクションのコマンド実行履歴ファイルが壊れているおそれがあります。

- `jcocmdlog` コマンドを実行したときに、「KAVB2527-E コマンド実行履歴ファイルの読込に失敗しました」が出力される。
 - オプションに`-act` を指定している場合、自動アクションのコマンド実行履歴ファイルが壊れているおそれがあります。
 - オプションに`-window` を指定している場合、コマンド実行のコマンド実行履歴ファイルが壊れているおそれがあります。
 - `-act` と`-window` のオプションを指定していない場合、自動アクションまたはコマンド実行のコマンド実行履歴ファイルが壊れているおそれがあります。
- 統合トレースログに「KAVB2064-E コマンド実行履歴ファイルの書き込みに失敗しました」が出力される。

自動アクションまたはコマンド実行のコマンド実行履歴ファイルが壊れているおそれがあります。

これらのメッセージが出力される場合、次の手順でコマンド実行履歴ファイルの状態を確認してください。

1. 壊れたおそれのあるファイルを(a)に示す手順で確認する。
2. 確認の結果、壊れていない場合には各メッセージの対処方法に従って、対処する。
3. 壊れている場合は、(b)の手順で回復する。
4. (b)の手順でも回復しない場合は、(c)の手順に従ってコマンド実行履歴ファイルを削除する。

(a) コマンド実行履歴ファイルの確認手順

自動アクションのコマンド実行履歴ファイルを確認する場合

- Windows の場合

コマンドプロンプトから次のコマンドを実行してください。

```
cd Base パス¥log¥COMMAND
```

```
(論理ホストの場合 : cd 共有フォルダ¥jp1base¥log¥COMMAND)
```

```
Jischk -l3 Base パス¥log¥COMMAND¥ACTISAMLOGV8
```

- UNIX の場合

次のコマンドを実行してください。

```
cd /var/opt/jp1base/log/COMMAND
```

```
(論理ホストの場合 : cd 共有ディレクトリ/jp1base/log/COMMAND)
```

```
/opt/jp1base/bin/Jischk -l3 actisamlogv8
```

コマンド実行のコマンド実行履歴ファイルを確認する場合

- Windows の場合
コマンドプロンプトから次のコマンドを実行してください。
cd Base パス¥log¥COMMAND
(論理ホストの場合 : cd 共有フォルダ¥jp1base¥log¥COMMAND)
Jischk -l3 Base パス¥log¥COMMAND¥CMDISAMLOGV8

- UNIX の場合
次のコマンドを実行してください。
cd /var/opt/jp1base/log/COMMAND
(論理ホストの場合 : cd 共有ディレクトリ/jp1base/log/COMMAND)
/opt/jp1base/bin/Jischk -l3 cmdisamlogv8

Jischk コマンドでファイルの不正が検出されない場合、コマンド実行履歴ファイルは壊れていません。Jischk コマンドでファイルの不正が検出された場合には、(b)に示す手順でコマンド実行履歴ファイルを回復してください。

Jischk 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。

(b) コマンド実行履歴ファイルの回復手順

自動アクションのコマンド実行履歴ファイルを回復する場合

- Windows の場合
次の操作は Administrators 権限で実行してください。また、回復する際には、ACTISAMLOGV8.DRF の約 3 倍の空き容量が必要です。
 1. JP1/IM - Manager を停止する。
 2. JP1/Base を停止する。
 3. コマンドプロンプトから次のコマンドを実行し、コマンド実行履歴ファイルを回復する。
なお、Jiscond 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。
cd Base パス¥Log¥COMMAND
(論理ホストの場合 : cd 共有フォルダ¥jp1base¥Log¥COMMAND)
Jiscond ACTISAMLOGV8
 4. コマンドプロンプトから次のコマンドを実行して、コマンド実行履歴ファイルが正常に回復したことを確認する。
Jischk -l3 ACTISAMLOGV8
Jischk コマンドでファイルの不正が検出された場合、コマンド実行履歴ファイルは回復できない状態です。正常に回復できなかった場合、(c)に示す手順で自動アクションのコマンド実行履歴ファイルを削除してください。
 5. JP1/Base を起動する。

6. JP1/IM - Manager を起動する。

- UNIX の場合

次の操作はスーパーユーザー権限で実行してください。また、回復する際には、actisamlogv8.DAT の約 3 倍の空き容量が必要です。

1. JP1/IM - Manager を停止する。

2. JP1/Base を停止する。

3. 次のコマンドを実行し、コマンド実行履歴ファイルを回復する。

なお、Jiscond 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。

```
cd /var/opt/jp1base/log/COMMAND
```

(論理ホストの場合：cd 共有ディレクトリ/jp1base/log/COMMAND)

```
/opt/jp1base/bin/Jiscond actisamlogv8
```

4. コマンドプロンプトから次のコマンドを実行して、コマンド実行履歴ファイルが正常に回復したことを確認する。

```
/opt/jp1base/bin/Jischk -l3 actisamlogv8
```

Jischk コマンドでファイルの不正が検出された場合、コマンド実行履歴ファイルは回復できない状態です。正常に回復できなかった場合、(c)に示す手順で自動アクションのコマンド実行履歴ファイルを削除してください。

5. JP1/Base を起動する。

6. JP1/IM - Manager を起動する。

コマンド実行のコマンド実行履歴ファイルを回復する場合

- Windows の場合

次の操作は Administrators 権限で実行してください。また、回復する際には、CMDISAMLOGV8.DRF の約 3 倍の空き容量が必要です。

1. JP1/IM - Manager を停止する。

2. JP1/Base を停止する。

3. コマンドプロンプトから次のコマンドを実行し、コマンド実行履歴ファイルを回復する。

Jiscond 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。

```
cd Base パス¥log¥COMMAND
```

(論理ホストの場合：cd 共有フォルダ¥jp1base¥log¥COMMAND)

```
Jiscond CMDISAMLOGV8
```

4. コマンドプロンプトから次のコマンドを実行して、コマンド実行履歴ファイルが正常に回復したことを確認する。

```
Jischk -l3 CMDISAMLOGV8
```

Jischk コマンドでファイルの不正が検出された場合、コマンド実行履歴ファイルは回復できない状態です。正常に回復できなかった場合、(c)に示す手順でコマンド実行のコマンド実行履歴ファイルを削除してください。

5.JP1/Base を起動する。

6.JP1/IM - Manager を起動する。

- UNIX の場合

次の操作はスーパーユーザー権限で実行してください。また、回復する際には、cmdisamlogv8.DAT の約 3 倍の空き容量が必要です。

1.JP1/IM - Manager を停止する。

2.JP1/Base を停止する。

3. 次のコマンドを実行する。

```
cd /var/opt/jp1base/log/COMMAND
```

(論理ホストの場合：cd 共有ディレクトリ/jp1base/log/COMMAND)

```
/opt/jp1base/bin/Jiscond cmdisamlogv8
```

4. コマンドプロンプトから次のコマンドを実行して、コマンド実行履歴ファイルが正常に回復したことを確認する。

```
/opt/jp1base/bin/Jischk -l3 cmdisamlogv8
```

Jischk コマンドでファイルの不正が検出された場合、コマンド実行履歴ファイルは回復できない状態です。正常に回復できなかった場合、(c)に示す手順でコマンド実行のコマンド実行履歴ファイルを削除してください。

5.JP1/Base を起動する。

6.JP1/IM - Manager を起動する。

(c) コマンド実行履歴ファイルの削除手順

自動アクションのコマンド実行履歴ファイルを削除する場合

自動アクションのコマンド実行履歴ファイルを削除すると、過去の自動アクションによる履歴はすべて失われます。削除することに問題がある場合は、ファイルをバックアップしてください。詳細については、「[1.2.2 データベースのバックアップおよびリカバリー](#)」を参照してください。

1. JP1/IM - Manager を停止する。

2. JP1/Base を停止する。

3. コマンド実行履歴ファイルを削除する。

正常に回復できなかった次のファイルを削除してください。なお、コマンド実行履歴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。

Windows の場合

表 12-29 削除対象ファイル格納場所 (Windows)

ファイル名	ファイル名
自動アクションのコマンド実行履歴ファイル	<ul style="list-style-type: none"> Base パス¥log¥COMMAND¥ACTISAMLOGV8.DRF Base パス¥log¥COMMAND¥ACTISAMLOGV8.K01 Base パス¥log¥COMMAND¥ACTISAMLOGV8.KDF
	<ul style="list-style-type: none"> 共有フォルダ¥jp1base¥log¥COMMAND¥ACTISAMLOGV8.DRF 共有フォルダ¥jp1base¥log¥COMMAND¥ACTISAMLOGV8.K01 共有フォルダ¥jp1base¥log¥COMMAND¥ACTISAMLOGV8.KDF
アクション情報ファイル	Console パス¥log¥action¥actinf.log
	共有フォルダ¥jp1cons¥log¥action¥actinf.log
アクションホスト名格納ファイル	Console パス¥log¥action¥acttxt{1 2}.log
	共有フォルダ¥jp1cons¥log¥action¥acttxt{1 2}.log

UNIX の場合

表 12-30 削除対象ファイル格納場所 (UNIX)

ファイル名	ファイル名
自動アクションのコマンド実行履歴ファイル	<ul style="list-style-type: none"> /var/opt/jp1base/log/COMMAND/actisamlogv8.DAT /var/opt/jp1base/log/COMMAND/actisamlogv8.K01 /var/opt/jp1base/log/COMMAND/actisamlogv8.DEF
	<ul style="list-style-type: none"> 共有ディレクトリ/jp1base/log/COMMAND/actisamlogv8.DAT 共有ディレクトリ/jp1base/log/COMMAND/actisamlogv8.K01 共有ディレクトリ/jp1base/log/COMMAND/actisamlogv8.DEF
アクション情報ファイル	/var/opt/jp1cons/log/action/actinf.log
	共有ディレクトリ/jp1cons/log/action/actinf.log
アクションホスト名格納ファイル	/var/opt/jp1cons/log/action/acttxt{1 2}.log
	共有ディレクトリ/jp1cons/log/action/acttxt{1 2}.log

4. JP1/Base を起動する。

5. JP1/IM - Manager を起動する。

コマンド実行のコマンド実行履歴ファイルを削除する場合

コマンド実行のコマンド実行履歴ファイルを削除すると、過去のコマンド実行による履歴はすべて失われます。削除することに問題がある場合は、ファイルをバックアップしてください。詳細については、「1.2.2 データベースのバックアップおよびリカバリー」を参照してください。

1. JP1/IM - Manager を停止する。

2. JP1/Base を停止する。

3. コマンド実行履歴ファイルを削除する。

正常に回復できなかった次のファイルを削除してください。なお、コマンド実行履歴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。

Windows の場合

表 12-31 削除対象ファイル格納場所 (Windows)

ファイル名	ファイル名
コマンド実行のコマンド実行履歴ファイル	<ul style="list-style-type: none">• Base パス¥log¥COMMAND¥CMDISAMLOGV8.DRF• Base パス¥log¥COMMAND¥CMDISAMLOGV8.K01• Base パス¥log¥COMMAND¥CMDISAMLOGV8.KDF
	<ul style="list-style-type: none">• 共有フォルダ¥jp1base¥log¥COMMAND¥CMDISAMLOGV8.DRF• 共有フォルダ¥jp1base¥log¥COMMAND¥CMDISAMLOGV8.K01• 共有フォルダ¥jp1base¥log¥COMMAND¥CMDISAMLOGV8.KDF

UNIX の場合

表 12-32 削除対象ファイル格納場所 (UNIX)

ファイル名	ファイル名
コマンド実行のコマンド実行履歴ファイル	<ul style="list-style-type: none">• /var/opt/jp1base/log/COMMAND/cmdisamlogv8.DAT• /var/opt/jp1base/log/COMMAND/cmdisamlogv8.K01• /var/opt/jp1base/log/COMMAND/cmdisamlogv8.DEF
	<ul style="list-style-type: none">• 共有ディレクトリ/jp1base/log/COMMAND/cmdisamlogv8.DAT• 共有ディレクトリ/jp1base/log/COMMAND/cmdisamlogv8.K01• 共有ディレクトリ/jp1base/log/COMMAND/cmdisamlogv8.DEF

4. JP1/Base を起動する。

5. JP1/IM - Manager を起動する。

(10) 自動アクションの実行状態が「状態不明」と表示される場合の対処方法

自動アクションの実行結果を保存したファイル（アクション情報ファイル、アクションホスト名格納ファイル、コマンド実行履歴ファイル）に不整合が発生しているおそれがあります。

この場合、実行結果を保存したファイルを削除する必要があります。なお、ファイルを削除すると、過去の自動アクションの実行結果は参照できなくなります。削除することに問題がある場合は、ファイルをバックアップしてください。詳細については、「1.2.2 データベースのバックアップおよびリカバリー」を参照してください。

削除手順を次に示します。

1. JP1/IM - Manager を停止し、JP1/Base を停止する。

クラスタ構成の場合は、クラスタソフトの操作で論理ホストを停止してください。また、停止確認後に共有ディスクを共有ディレクトリにマウントしてください。

2. アクション情報ファイル、アクションホスト名格納ファイル、およびコマンド実行履歴ファイルを削除する。

削除ファイルの格納場所は次の表のとおりです。

Windows の場合

表 12-33 削除対象ファイル格納場所 (Windows)

ファイル名	格納場所
アクション情報ファイル	Console パス¥log¥action¥actinf. log
	共有フォルダ¥jp1cons¥log¥action¥actinf. log
アクションホスト名格納ファイル	Console パス¥log¥action¥acttxt{1 2}. log
	共有フォルダ¥jp1cons¥log¥action¥acttxt{1 2}. log
コマンド実行履歴ファイル	Base パス¥Log¥COMMAND¥以下の全ファイル
	共有フォルダ¥jp1base¥log¥COMMAND¥以下の全ファイル

UNIX の場合

表 12-34 削除対象ファイル格納場所 (UNIX)

ファイル名	格納場所
アクション情報ファイル	/var/opt/jp1cons/log/action/actinf. log
	共有ディレクトリ/jp1cons/log/action/actinf. log
アクションホスト名格納ファイル	/var/opt/jp1cons/log/action/acttxt{1 2}. log
	共有ディレクトリ/jp1cons/log/action/acttxt{1 2}. log
コマンド実行履歴ファイル	/var/opt/jp1base/log/COMMAND/以下の全ファイル
	共有ディレクトリ/jp1base/log/COMMAND/以下の全ファイル

3. JP1/Base を起動し、JP1/IM - Manager を起動する。

クラスタ構成の場合は、共有ディスクをアンマウントしてから、クラスタソフトの操作で論理ホストを起動してください。

(11) 自動アクションが遅延する場合の対処方法

自動アクションの状態が「実行中」のままになっている。

まず、jccomdshow コマンド※で、コマンドの状態を確認してください。その結果によって、対処方法が異なります。確認して得られた結果ごとに、考えられる要因とその対処方法について次に説明します。

「コマンド実行経過時間 (ETIME)」が長いコマンドがある場合。

要因

終了しないコマンドまたは時間がかかるコマンドが実行されています。

対処

jcocmdel コマンド※で、終了しないコマンドを削除してください。詳細については、「8.1.4 コマンドの実行状態を確認または削除する」およびマニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「9.4.4(6) トラブルシューティング用コマンド」を参照してください。

「KAVB2239-E 接続先ホストへのネットワーク接続を確立できませんでした」メッセージが表示される場合。

要因

実行先ホストの JP1/Base がコマンド実行中に停止しました。

対処

実行先ホストの JP1/Base を再起動してください。

なお、JP1/Base を監視する方法として、JP1/Base のヘルスチェック機能があります。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「9.4.8 JP1/Base のヘルスチェック機能」を参照してください。

「コマンド実行状態 (STATUS)」が「Q」となっているコマンドが大量にある場合。

要因

自動アクション実行数が多過ぎます。

対処

実行中の自動アクションを確認して、次を見直してください。

- 不要な自動アクションが設定されていないか
- 自動アクションを設定する JP1 イベントを絞り込めないか

不要な自動アクションがない場合は、jcocmddef コマンド※で、コマンド同時実行数を増やしてください。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「14.7.6 コマンド実行環境の検討」を参照してください。

注※

jcocmdshow コマンド、jcocmdel コマンドおよび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」のコマンドを説明している章を参照してください。

(12) 監視オブジェクト DB が破損している場合の対処方法

「KAVB7247-E JP1/IM - CS は JP1/IM - View からの操作要求が実行できませんでした(要因:データベースのレコード不正)」、 「KAVB7248-E JP1/IM - CS は JP1/IM - View からの操作要求が実行できませんでした(要因:データベースの操作不能)」などのメッセージが出力される。

要因

次の要因が考えられます。

- JP1/IM - Manager の監視オブジェクト DB に論理矛盾が発生している。

対処

次の処置を実行してください。

1. JP1/IM - Manager を停止する。
2. 障害調査用に、Scope パス¥database フォルダのバックアップをとる。
3. `jcsdbsetup -f` コマンドを実行する。
4. Scope パス¥database¥jcshosts フォルダ内のすべてのファイルを削除する。
5. `jcshostsimport -r jcshosts` コマンドを実行する。
6. JP1/IM - Manager を起動する。

(13) 監視オブジェクト DB のロックが解除されない場合の対処方法

監視オブジェクト DB がロックされたままになっている。

要因

次の要因が考えられます。

- JP1/IM - Manager の監視オブジェクト DB でロック取得に失敗している。

対処

次の処置を実行してください。

1. `jcsmain` プロセスが起動していないことを、`jco_spm_status` コマンドで確認する。
2. `Jismlcktr` コマンドを実行する。
3. Scope パス¥database 以下のファイルをロックしているプロセスを確認する。
4. 手順 3 で確認したプロセス ID に対して、`Jislckfree -p PID` コマンドを実行する。

`Jismlcktr`, `Jislckfree` コマンドは JP1/Base が提供しています。詳細については、マニュアル「JP1/Base 運用ガイド」のコマンドの章を参照してください。

(14) アクション結果の詳細情報（メッセージ）に KAVB5150-W が表示される場合の対処方法

[アクション結果詳細] 画面を表示すると、メッセージ欄に「KAVB5150-W コマンド実行履歴に該当データがありません」と表示される。

要因

コマンド実行履歴ファイル (ISAM) がラップしたおそれがあります。コマンド実行履歴ファイルがラップすると、自動アクションの実行結果が表示されません。

対処

この現象が頻繁に起こる場合には、コマンド実行履歴ファイルのレコード数の上限値を大きくすることを検討してください。レコード数の上限値を大きくすると、ディスク容量も圧迫しますので、その点も考慮に入れてください。

次に手順を示します。

レコード数の上限値を変更する

レコード数の上限値を変更した場合、設定を有効にするためにコマンド実行履歴ファイルを削除する必要があります。コマンド実行履歴ファイルを削除すると、過去の自動アクション、コマンド実行による履歴はすべて失われます。削除することに問題がある場合は、ファイルをバックアップしてください。詳細については、「1.2.2 データベースのバックアップおよびリカバリー」を参照してください。

1. `jcocmdef` コマンドで、コマンド実行履歴ファイルのレコード数を変更する。

2. JP1/IM - Manager, JP1/Base を停止する。

クラスタ構成の場合は、クラスタソフトの操作で論理ホストを停止してください。

また、停止確認後に共有ディスクを共有ディレクトリにマウントしてください。

3. コマンド実行履歴ファイルを削除する。

コマンド実行履歴保存ディレクトリ以下の全ファイルが該当します。コマンド実行履歴保存ディレクトリは、デフォルトでは下記のとおりです。

Windows の場合

表 12-35 コマンド実行履歴ファイル格納場所 (Windows)

ファイル名	格納場所
コマンド実行履歴ファイル	Base パス¥log¥COMMAND¥以下の全ファイル
	共有フォルダ¥jp1base¥log¥COMMAND¥以下の全ファイル

UNIX の場合

表 12-36 コマンド実行履歴ファイル格納場所 (UNIX)

ファイル名	格納場所
コマンド実行履歴ファイル	/var/opt/jp1base/log/COMMAND/以下の全ファイル
	共有ディレクトリ/jp1base/log/COMMAND/以下の全ファイル

なお、コマンド実行履歴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。

4. JP1/Base, JP1/IM - Manager を起動する。

クラスタ構成の場合は、共有ディスクをアンマウントしてから、クラスタソフトの操作で論理ホストを起動してください。

`jcocmdef` コマンドについては、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。

(15) JP1/IM - Manager, JP1/IM - View のどちらかのバージョンが古い場合の対処方法

メッセージの種類によって対処方法が異なります。

「KAVB6060-E 接続先サーバには対応していません」が表示される。

要因

JP1/IM - View よりも JP1/IM - Manager が古いバージョン、または監視オブジェクト DB が古いバージョンです。

対処

JP1/IM - View よりも JP1/IM - Manager が古いバージョンの場合

次の手順に従って、JP1/IM - Manager をバージョンアップしてください。

1. [監視ツリー(編集中)] 画面で [ファイル] - [ツリーを保存] の操作をし、編集した監視ツリーを csv ファイルに保存する。
2. JP1/IM - Manager を JP1/IM - View と同じバージョンにバージョンアップする。
3. [監視ツリー(編集中)] 画面で [ファイル] - [ツリーを開く] の操作をし、保存しておいた csv ファイルを読み込む。
4. [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] の操作をし、サーバのツリーを更新する。

JP1/IM - View と JP1/IM - Manager が同じバージョンで、監視オブジェクト DB が古いバージョンの場合

次の手順に従って、監視オブジェクト DB をバージョンアップしてください。

1. [監視ツリー(編集中)] 画面で [ファイル] - [ツリーの保存] の操作をし、編集した監視ツリーを csv ファイルに保存する。
2. 監視オブジェクト DB をバージョンアップする。
3. [監視ツリー(編集中)] 画面で [ファイル] - [サーバのツリーを開く] の操作をし、保存しておいた csv ファイルを読み込む。
4. [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] の操作をし、サーバのツリーを更新する。

監視オブジェクト DB のバージョンアップについては次を参照してください。

- 物理ホストの場合
Windows：マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.19.7(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」
UNIX：マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「2.18.11(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」
- 論理ホストの場合

Windows：マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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)」

UNIX：マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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 - View よりも JP1/IM - Manager が新しいバージョンで、監視オブジェクト DB が古いバージョンの場合

次の手順に従って、JP1/IM - View をバージョンアップしてください。

1. [監視ツリー(編集中)] 画面で [ファイル] - [ツリーの保存] の操作をし、編集した監視ツリーを csv ファイルに保存する。
2. JP1/IM - Manager をアンインストールする。
3. JP1/IM - Manager のインストールディレクトリを削除する。
4. JP1/IM - View と同じバージョンの JP1/IM - Manager をインストールする。
5. [監視ツリー(編集中)] 画面で [ファイル] - [サーバのツリーを開く] の操作をし、保存しておいた csv ファイルを読み込む。
6. [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] の操作をし、サーバのツリーを更新する。
7. 新しいバージョンの JP1/IM - Manager にバージョンアップする。
8. JP1/IM - View を JP1/IM - Manager と同じバージョンにバージョンアップする。

「KAVB6046-E ユーザー(ユーザー)には操作に必要な管理者権限がありません」のメッセージが表示される。

要因

JP1/IM - Manager よりも JP1/IM - View が古いバージョン、または JP1/IM - View の編集データが古いバージョンです。

対処

次の手順に従って、JP1/IM - View をバージョンアップしてください。

1. [監視ツリー(編集中)] 画面で [ファイル] - [ツリーを保存] の操作をし、編集した監視ツリーを csv ファイルに保存する。
2. JP1/IM - Manager をアンインストールする。
3. JP1/IM - Manager のインストールディレクトリを削除する。
4. JP1/IM - View と同じバージョンの JP1/IM - Manager をインストールする。
5. [監視ツリー(編集中)] 画面で [ファイル] - [ツリーを開く] の操作をし、保存しておいた csv ファイルを読み込む。
6. [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] の操作をし、サーバのツリーを更新する。
7. 新しいバージョンの JP1/IM - Manager にバージョンアップする。

8.JP1/IM - View を JP1/IM - Manager と同じバージョンにバージョンアップする。

(16) 関連イベントの発行処理の対象となる JP1 イベントが多発した場合の対処方法

システムのメンテナンスなどで、関連イベントの発行処理の対象となる JP1 イベントが多発した場合、関連イベントの発行処理が過負荷状態になるおそれがあります。

回避方法は次の二つがあります。

- 関連イベントの発行処理を休止する。
- JP1/IM - Manager を停止する。

なお、関連イベントの発行処理を休止しても状況回避できない場合だけ、JP1/IM - Manager を停止してください。

関連イベントの発行処理を休止する。

関連イベントの発行処理をいったん休止して、状況が回復したあとで関連イベントの発行処理を再開してください。

手順を次に示します。

1. `jcoegsstop` コマンドを実行して、関連イベントの発行処理を休止する。
`jcoegsstop` コマンドを実行すると、関連イベント発行サービスが機能停止状態になります。この間に発生した JP1 イベントは処理の対象外になります。
サービスを停止させずに処理だけを停止するため、クラスタ運用している場合にフェールオーバーさせないで運用を継続できます。
2. 関連イベント発行処理を再開したい場合、`jcoegsstart` コマンドを実行する。

JP1/IM - Manager を停止する。

JP1/IM - Manager を停止する場合、起動オプションが `cold` であれば次に説明する手順を実施する必要はありません。 `warm` の場合だけ実施してください。

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`) を編集して、起動オプションを `cold` に変更する。
2. JP1/IM - Manager を再起動する。
3. 関連イベント発行システムプロファイル (`egs_system.conf`) を編集して、起動オプションを `warm` に戻す。
4. `jco_spmd_reload` コマンドを実行して、起動オプションの設定を有効にする。

(17) JP1/IM - View に関連イベントが表示されない場合の対処方法

次の要因が考えられます。

- 関連イベントの発行が有効になっていない。
- 関連イベント発行定義が定義されていない。
- 関連イベントがフィルタリングされている。
- 反映した関連イベント発行定義が破損している。

それぞれの対処を次に示します。

関連イベントの発行が有効になっていない。

関連イベント発行サービスはオプション機能であり、デフォルトでは起動しません。関連イベント発行サービスの起動設定をしていない場合、`jcoimdef` コマンドで起動設定をしたあと、JP1/IM - Manager を再起動すると関連イベント発行サービスが起動するようになります。

関連イベントの発行処理が稼働していることを確認するには、JP1/IM - Manager を再起動したあと、`jcoegsstatus` コマンドを実行して、関連イベント発行サービスが関連稼働状態 (RUNNING) になっていることを確認してください。

関連イベント発行定義が定義されていない。

関連イベント発行サービスは、関連イベント発行定義に従って関連イベントを発行します。関連イベント発行定義はデフォルトでは定義されていないため、関連イベントは発行されません。

関連イベント発行定義ファイルを作成したあと、`jcoegschange` コマンドを実行して、関連イベント発行サービスに関連イベント発行定義を反映してください。反映した関連イベント発行定義は `jcoegsstatus` コマンドで確認できます。

関連イベントがフィルタリングされている。

関連イベントがイベント取得フィルター、ユーザーフィルター、重要イベントフィルターおよび表示フィルターのフィルタリング対象になっていないかどうか確認してください。

関連イベントは通常の JP1 イベントと同様に、イベント取得フィルター、ユーザーフィルター、重要イベントフィルターおよび表示フィルターの対象になります。また、重大度が定義されていないイベントは、イベント取得フィルターによってフィルタリングされます (デフォルト設定の場合)。

反映した関連イベント発行定義が破損している。

統合トレースログに次のメッセージが出力される場合、`jcoegschange` コマンドで関連イベント発行サービスに反映した関連イベント発行定義が壊れたおそれがあります。

- 「KAJV2246-E 関連イベント発行定義保存ファイルが壊れているため定義不正が検出されました。
行番号:行番号 不正内容:不正内容」

このメッセージが出力された場合、`jcoegschange` コマンドを実行して、再度関連イベント発行定義を反映してください。

(18) JP1/IM - View でログインしたあと、JP1/IM - View の画面が表示されない場合の対処方法

JP1/IM - View でログインしたあと、JP1/IM - View の画面が表示されない。なお、タスクバーには、JP1/IM - View のタスクバーボタンが表示されている。

要因

次の操作をすると、JP1/IM - View でログインしたあとに画面が表示されません。

- 仮想画面構成※によって、JP1/IM - View が表示されていない画面領域を表示した状態で、JP1/IM - View を終了する。

注※

メモリー上にディスプレイ画面以上のデスクトップを持ち、分割したそれぞれの領域を仮想的に一つのデスクトップとして表示することで複数のデスクトップを画面を切り替えて使用できる構成のことをいいます。

仮想デスクトップともいいます。

対処

次のどれかの方法で対処してください。

対処 1

1. [Alt] + [Tab] キーを押して JP1/IM - View を選択する。
2. タスクバーから「重ねて表示」を選択し、すべての画面を重ねて表示する。
3. JP1/IM - View やそのほかの画面の表示位置およびサイズを変更する。

対処 2

1. [Alt] + [Tab] キーを押して JP1/IM - View を選択する。
2. タスクバーから「上下に並べて表示」を選択し、すべての画面を上下に並べて表示する。
3. JP1/IM - View やそのほかの画面の表示位置およびサイズを変更する。

対処 3

1. [Alt] + [Tab] キーを押して JP1/IM - View を選択する。
2. タスクバーから「左右に並べて表示」を選択し、すべての画面を左右に並べて表示する。
3. JP1/IM - View やそのほかの画面の表示位置およびサイズを変更する。

対処 4

1. [Alt] + [Tab] キーを押して JP1/IM - View を選択する。
2. JP1/IM - View のコンテキストメニューから「移動」を選択し、カーソルキーで位置を調整する。
3. 表示された画面またはその画面の枠の位置を決定したら、リターンキーを押す。

対処 5

1. [Alt] + [Tab] キーを押して JP1/IM - View を選択する。
2. JP1/IM - View のコンテキストメニューから「最大化」を選択し、画面を最大化した状態でいったんログアウトする。
3. 再ログインしたあと、画面の表示位置およびサイズを変更する。

(19) コマンド実行, 自動アクションで実行したバッチファイルが正常終了しない場合(Windows 限定)の対処方法

要因

次の条件を満たす場合, バッチファイルの処理が中断され, バッチファイルが正常に処理されません。

- コマンド実行先に指定したホストの OS が Windows2000 である。
- バッチファイルで FOR /F コマンドを使用している。
- FOR /F コマンドの実行後, 標準エラー出力への出力をしている。

対処

次のどちらかの方法で対処してください。

- FOR /F コマンドを使用しない。
- FOR /F コマンド実行後に標準エラー出力への出力をしない。

(20) 追加共通除外条件を設定できない場合の対処方法

KAVB1155-E のメッセージが表示され, 追加共通除外条件を登録できない。

要因

[共通除外条件で除外] メニューから [共通除外条件設定(拡張)] 画面を表示しようとしたとき, または追加共通除外条件を登録しようとしたとき, すでに共通除外条件の定義件数が上限に達しています。

対処

不要な共通除外条件群を削除してください。

KAVB1163-E のメッセージが表示され, 追加共通除外条件を登録できない。

要因

次の要因が考えられます。

- イベント取得フィルターが互換モードで動作している, または共通除外条件の動作モードが基本モードで動作しています。
- 定義ファイルに誤りがあります。
- イベント取得フィルターの切り替えに失敗しました。

対処

要因に従って対処してください

- JP1/IM - Manager の共通除外条件の動作モードが拡張になっていない場合は, JP1/IM - Manager の共通除外条件の動作モードを確認し, 拡張モードにしてください。そのあと, JP1/IM - View を再起動してから, 再度実行してください。
- JP1/IM - Manager を停止し, 共通除外条件の動作モードをいったん基本モードに変更してから, 再度拡張モードに変更して共通除外条件 (拡張) 定義を初期化してください。

- マネージャーの統合トレースログに KAVB4003-I のメッセージが出力されていることを確認してから、再度実行してください。KAVB4003-I のメッセージが出力されていなく統合監視 DB を使用している場合は、`jimdbstatus` コマンドを実行し、IM データベースサービスの状態を確認してください。IM データベースサービスが稼働中になったことを確認し、統合トレースログに KAVB4003-I のメッセージが出力されてから、再度実行してください。

なお、その他の要因の場合は、ファイルディスクリプタなどの OS のリソース不足がほかに発生していないかを確認してください。

- Windows の場合：Windows イベントログ
- UNIX の場合：シスログ (syslog)

発生していない場合は、資料採取ツールで資料を採取し、システム管理者に連絡してください。

KAVB1157-E のメッセージが表示され、追加共通除外条件を登録できない。

要因

[共通除外条件で除外] メニューから [共通除外条件設定(拡張)] 画面を表示しようとした、または追加共通除外条件を登録しようとしたとき、すでに共通除外条件のフィルターサイズが上限に達しています。

対処

不要な共通除外条件群を削除、またはフィルターの上限サイズに収まるように条件群を定義してください。

KAVB0256-E のメッセージが表示され、追加共通除外条件を登録できない。

要因

追加共通除外条件を登録しようとしたとき、指定した共通除外条件群名がすでに存在しています。

対処

重複しない共通除外条件群名を指定し、再度実行してください。

KAVB1153-E のメッセージがログに出力され、[共通除外条件で除外] メニューから [共通除外条件設定(拡張)] 画面を表示したときの [イベント条件] に共通除外条件自動入力定義ファイルで設定した属性の条件が自動的に表示されない。

要因

共通除外条件自動入力定義ファイルが存在しません。

対処

次を確認してください。

- 共通除外条件自動入力定義ファイルが存在するかどうか。
- 共通除外条件自動入力定義ファイルにアクセス権があるかどうか。

そのあと、`jco_spm�_reload` コマンドを実行するか、JP1/IM - Manager を再起動し、共通除外条件自動入力定義ファイルを再度読み込んでください。

KAVB1154-W のメッセージがログに出力され、[共通除外条件で除外] メニューから [共通除外条件設定(拡張)] 画面を表示したときの [イベント条件] に自動設定した条件が表示されない。

要因

共通除外条件自動入力定義ファイルの読み込みに失敗しています。

対処

OS のリソース不足が発生していないかどうかを確認してください。

- Windows の場合：Windows イベントログ
- UNIX の場合：syslog

OS のリソース不足が発生していない場合は、資料採取ツールで資料を採取し、システム管理者に連絡してください。

KAVB1158-W のメッセージがログに出力され、[共通除外条件で除外] メニューから [共通除外条件設定(拡張)] 画面を表示したときの [イベント条件] に自動設定した条件が表示されない。

要因

共通除外条件自動入力定義ファイルに、定義が入力されていません。

対処

共通除外条件自動入力定義ファイルに属性名を指定し、jco_spmc_reload コマンドを実行するか、JP1/IM - Manager を再起動し、共通除外条件自動入力定義ファイルを再度読み込んでください。

KAVB1159-W または KAVB1160-W のメッセージがログに出力され、[共通除外条件で除外] メニューから [共通除外条件設定(拡張)] 画面を表示したときの [イベント条件] に自動設定した条件が表示されない。

要因

次の要因が考えられます。

- 共通除外条件自動入力定義ファイルに、無効な属性名が定義されています。
- 共通除外条件自動入力定義ファイルに、属性名が重複して定義されています。

対処

共通除外条件自動入力定義ファイルに正しい属性名を定義し、jco_spmc_reload コマンドを実行するか、JP1/IM - Manager を再起動し、共通除外条件自動入力定義ファイルを再度読み込んでください。

KAVB1161-W のメッセージがログに出力され、[共通除外条件設定 (拡張)] 画面の [共通除外条件群名] がすべて表示されない。

要因

共通除外条件自動入力定義ファイルで定義した共通除外条件群名が 40 バイトを超えています。

対処

共通除外条件自動入力定義ファイルの共通除外条件群名を 40 バイト以下で定義し、jco_spmc_reload コマンドを実行するか、JP1/IM - Manager を再起動し、共通除外条件自動入力定義ファイルを再度読み込んでください。

KAVB1162-W のメッセージがログに出力され、[共通除外条件設定(拡張)] 画面の [共通除外条件群名] が正しく表示されない。

要因

共通除外条件自動入力定義ファイルの共通除外条件群名に指定できない文字が使用されています。

対処

共通除外条件自動入力定義ファイルの共通除外条件群名を見直し、jco_spmc_reload コマンドを実行するか、JP1/IM - Manager を再起動し、共通除外条件自動入力定義ファイルを再度読み込んでください。

(21) JP1/IM - Manager (セントラルスコープ) が受信した JP1 イベントの処理が遅延する場合の対処方法

要因

状態変更条件設定の個別条件設定で、属性値に指定した文字列（ホスト名または IP アドレス）の名前解決ができていないおそれがあります。

対処

名前解決に失敗したホスト名は、次のログファイルに出力されます。

Windows の場合

Scope パス¥log¥jcsmain_trace{1|2|3}.log※

UNIX の場合

/var/opt/jp1scope/log/jcsmain_trace{1|2|3}.log※

注※

JP1/Base のログファイルトラップ機能の監視対象にはしないでください。

名前解決に失敗した場合、上記ログファイル内に、次のメッセージが出力されます。

・・・ fs_jcsHostsAccessPtr->getHostByName() is failed. (host = 名前解決に失敗したホスト名, jp1error = 2001)・・・

または、

・・・ fs_jcsHostsAccessPtr->getHostByAddr() is failed. (host = 名前解決に失敗した IP アドレス, jp1error = 2001)・・・

これを確認の上、個別条件の条件として [ホスト名比較] を設定し、次に示すどれかの方法で属性値に指定したホスト名または IP アドレスの名前解決ができるようにしてください。

- 個別条件の属性値に指定したホスト名または IP アドレスをホスト情報 DB に登録する。
- 個別条件の属性値に指定したホスト名または IP アドレスを JP1/Base の jp1hosts 情報または jp1hosts2 情報に登録する。
- 個別条件の属性値に指定したホスト名または IP アドレスを hosts や DNS などに登録する。

(22) 応答待ちイベントが JP1/IM - View に表示されない場合の対処方法

要因

次の要因が考えられます。

- 応答待ちイベント管理機能が無効となっている。
jcoimdef コマンドの `-resevent` オプションの指定が OFF となっているおそれがあります。
- 応答待ちイベントが発行されていない。
- 応答待ちイベントは発行されているが、JP1/IM - Manager でフィルタリングされている。

対処

応答待ちイベント管理機能を有効が無効となっている場合は、jcoimdef コマンドの `-resevent` オプションの指定を ON にしてください。

また、次の手順で要因を切り分けて対処してください。

1. JP1/IM - Manager ホストのイベント DB に応答待ちイベントが登録されていることを確認する。
管理者ユーザーなど、ユーザーフィルターが設定されていない JP1 ユーザーでイベント検索し、応答待ちイベントがイベント DB に登録されていることを確認します。
登録されていない場合は、手順 2 の方法で調査します。
登録されている場合は、JP1/IM - Manager のフィルター（イベント取得フィルター、またはユーザーフィルター）でフィルタリングされているため、フィルター条件を見直してください。
2. BJEX または JP1/AS ホストのログを確認し、BJEX のエラー、JP1/AS のエラー、または通信エラーが発生していないことを確認する。
エラーメッセージが出力されている場合は、そのメッセージの対処方法に従って対処してください。
BJEX または JP1/AS のセットアップ時の誤りや通信エラーが考えられます。

(23) 応答待ちイベントが JP1/IM - View に表示されるが、応答待ちイベントとして表示されない（種別の矢印アイコンが表示されない、応答入力できない）場合の対処方法

要因

次の要因が考えられます。

- 応答待ちイベント管理機能が無効となっている。
jcoimdef コマンドの `-resevent` オプションの指定が OFF となっているおそれがあります。
- BJEX または JP1/AS の設定で、JP1/IM - Manager のホスト名の指定が間違っている。
ホスト名ではなく IP アドレスが指定されているおそれがあります。
- BJEX または JP1/AS で設定した JP1/IM - Manager のホスト以外のホストに転送している応答待ちイベントである。

対処

要因に従って対処してください。

- 応答待ちイベント管理機能を有効にする。
jcoimdef コマンドの `-resevent` オプションの指定を ON にしてください。
- BJEX または JP1/AS の設定で、正しい JP1/IM - Manager のホスト名を指定する。
- 応答待ちイベントに応答する場合は、BJEX または JP1/AS で設定した JP1/IM - Manager ホストに対してログインする。

(24) 【イベントコンソール】画面に JP1 イベントが表示されない場合の対処方法

要因

フィルターの除外条件、有効な共通除外条件に、条件が何も設定されていない条件群があるため、すべての JP1 イベントが除外されています。

対処

拡張モードの共通除外条件を使用している場合、共通除外履歴ファイルを参照し、共通除外条件によって JP1 イベントが取得対象外にされていないかを確認してください。JP1 イベントが除外されている場合は、共通除外条件を見直してください。

拡張モードの共通除外条件を使用していない場合、または拡張モードの共通除外条件を見直しても回復しない場合は、次のフィルターの除外条件、および基本モードの有効な共通除外条件を見直してください。

- イベント取得フィルター
- ユーザーフィルター
- 重要イベントフィルター
- 表示フィルター

(25) 【イベントコンソール】画面に JP1 イベントが遅延して表示される場合の対処方法

要因

次の要因が考えられます。

- イベント条件（フィルター条件※、自動アクションの実行条件、相関イベント発行条件のイベント属性条件、重大度変更機能のイベント条件、事象発生元ホストのマッピング機能のイベント条件）で正規表現を使用している場合、JP1 イベント受信時のマッチング処理に時間が掛かっていることが考えられます。

注※

次のフィルターの通過条件、除外条件、または、有効な共通除外条件を指します。

- ・ イベント取得フィルター
 - ・ ユーザーフィルター
 - ・ 重要イベントフィルター
- 自動アクション環境定義でイベント発行元ホスト名の取得方法を「local」に設定している場合、自動アクションのマッチング処理で、イベント属性中の「発行元 IP アドレス」からホスト名の逆引きに時間が掛かっていることが考えられます。
 - セントラルスコープを使用している場合、[イベントコンソール] 画面に JP1 イベントが遅延して表示される要因として、状態変更条件設定の個別条件設定で、属性値に指定した文字列（ホスト名または IP アドレス）の名前解決ができていない、または監視ノードの状態変更条件で、マッチング処理に時間が掛かっていることが考えられます。
 - API 設定ファイル (api) の server パラメーターの設定に誤りがあり、ポートの不足によって JP1/IM - Manager のイベント受信で通信エラーが多発していることが考えられます。

対処

要因に従って対処してください。

- イベント条件（フィルター条件※、自動アクションの実行条件、相関イベント発行条件のイベント属性条件、重大度変更機能のイベント条件、または事象発生元ホストのマッピング機能のイベント条件）で正規表現を使用している場合は、正規表現を見直したあと、JP1/IM - Manager を再起動してください。また、セントラルスコープを使用している場合、監視ノードの状態変更条件をイベント条件として使用しているときも、正規表現を見直したあと、JP1/IM - Manager を再起動してください。

注※

次のフィルターの通過条件、除外条件、または、有効な共通除外条件を指します。

- ・ イベント取得フィルター
- ・ ユーザーフィルター
- ・ 重要イベントフィルター

すべての文字にマッチする「.*」など、再帰的にマッチングされる正規表現を多用している場合、マッチング処理に時間が掛かることがあります。詳細はマニュアル「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。

- 自動アクション環境定義でイベント発行元ホスト名の取得方法を「local」に設定している場合、イベント属性中の「発行元 IP アドレス」からホスト名への解決をします。このホスト名の逆引きに時間が掛からないようにするために、OS の hosts ファイルの設定を見直す、またはイベント発行元ホスト名の取得方法を「remote」に設定してから、JP1/IM - Manager を再起動してください。イベント発行元ホスト名の取得方法の詳細は、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「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。OS の hosts の設定については、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「14.4.1 ホスト名と IP アドレス」を参照してください。

- セントラルスコープを使用している場合は、今まで述べた対処のほかに、状態変更条件設定の個別条件設定で、属性値に指定した文字列（ホスト名または IP アドレス）が遅延なく名前解決できるかを確認してください。詳細は「12.5.3(21) JP1/IM - Manager（セントラルスコープ）が受信した JP1 イベントの処理が遅延する場合の対処方法」を参照してください。

また、監視オブジェクトの状態変更条件をメモリーに常駐させる機能を使用すると、監視オブジェクトの状態変更のマッチング処理が短縮されます。メモリー所要量を見積もった上、十分なメモリーが確保できる場合は、この機能の設定をお勧めします。監視オブジェクトの状態変更条件をメモリーに常駐させる機能の詳細は、マニュアル「JP1/Integrated Management 3 - Manager 導入・設計ガイド」の「5.2.3 状態変更条件」を参照してください。

- API 設定ファイル (api) の server パラメーターの通信タイプが close になっている場合、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し、通信エラーやイベント受信の遅延が発生するおそれがあります。JP1/IM - Manager が接続するイベントサーバについて、API 設定ファイル (api) の server パラメーターの通信タイプを必ず keep-alive にしてください。

(26) 対処状況が変更できない場合の対処方法

次の要因が考えられます。

- イベントコンソールとセントラルコンソール・ビューアーの接続が確立しない。または、イベントコンソールと jcochstat コマンドの接続が確立しない。
- 指定した JP1 イベントが変更できないイベントだった。
- イベントコンソールサービスとイベントサービスの接続が確立しない。
- イベントコンソールサービスとイベント基盤サービスの接続が確立しない。
- イベント基盤サービスと IM データベースサービスの接続が確立しない。

それぞれの対処を次に示します。

イベントコンソールとセントラルコンソール・ビューアーの接続が確立しない。または、イベントコンソールと jcochstat コマンドの接続が確立しない。

マネージャー上のイベントコンソールが起動していない、システム（ホスト、ネットワーク）が高負荷状態である、ネットワークの設定に誤りがあるというおそれがあります。

- 対処

jco_spm�_status コマンドを実行してマネージャー上のイベントコンソールサービスが起動しているか確認し、再度対処状況を変更します。

または、ping コマンドなどを使用してログインしているホストが正常に稼働しているか確認し、再度対処状況を変更します。

指定したイベントが変更できないイベントだった。

- 対処

イベント DB 内通し番号の指定を見直し、再度対処状況を変更します。

イベントコンソールサービスとイベントサービスの接続が確立しない。

- 対処

イベントサービスが起動しているか確認し、再度対処状況を変更します。

イベントコンソールサービスとイベント基盤サービスの接続が確立しない。

イベント基盤サービスが起動していない、システム（ホスト、ネットワーク）が高負荷状態になっているというおそれがあります。

- 対処

`jco_spmc_status` コマンドを実行してマネージャー上のイベント基盤サービスが起動しているか確認し、再度対処状況を変更します。

イベント基盤サービスと IM データベースサービスの接続が確立しない。

IM データベースサービスが起動していない、システム（ホスト、ネットワーク）が高負荷状態になっているというおそれがあります。

- 対処

IM データベースサービスを起動後、再度対処状況を変更します。

(27) イベント検索が実行できない場合の対処方法

次の要因が考えられます。

- イベントコンソールとビューアーの接続が確立しない。
- イベント基盤サービスとイベントコンソールサービスの接続が確立しない。
- イベント基盤サービスと統合監視 DB の接続が確立しない。
- イベントコンソールサービスとイベントサービスの接続が確立しない。
- サポートしていない条件で JP1 イベントを検索した。
- イベント検索実行時、指定した正規表現が間違っている。
- 除外条件を指定してイベント検索を実行した時、検索ホストの JP1/Base のバージョンが 08-11 以前だった。

それぞれの対処を次に示します。

イベントコンソールとビューアーの接続が確立しない。

マネージャー上のイベントコンソールが起動していない、システム(ホスト、ネットワーク)が高負荷状態になっている、ネットワークの設定に誤りがあるというおそれがあります。

- 対処

`jco_spmc_status` コマンドを実行してマネージャー上のイベントコンソールサービスが起動しているか確認し、イベント検索を再実行します。

または、`ping` コマンドを使用してログインしているホストが正常に稼働しているか確認し、イベント検索を再実行します。

イベント基盤サービスとイベントコンソールサービスの接続が確立しない。

イベント基盤サービスが起動していない、システム(ホスト、ネットワーク)が高負荷状態になっているというおそれがあります。

- 対処

jco_spmc_status コマンドを実行してマネージャー上のイベント基盤サービスが起動しているか確認し、イベント検索を再実行します。

イベント基盤サービスと統合監視 DB の接続が確立しない。

統合監視 DB が起動していない、システム (ホスト、ネットワーク) が高負荷状態になっているというおそれがあります。

- 対処

統合監視 DB を起動後、イベント検索を再実行します。

イベントコンソールサービスとイベントサービスの接続が確立しない。

検索先ホストのイベントサービスが起動していない、システム (ホスト、ネットワーク) が高負荷状態になっている、ネットワークの設定に誤りがあるというおそれがあります。

- 対処

jevstat コマンドを実行して検索先ホスト上のイベントサービスが起動しているか確認し、再度検索します。jevstat 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。

または、マネージャーホスト上でping コマンドなどを使用して検索先ホストが正常に稼働しているか確認し、再度検索します。

サポートしていない条件で JP1 イベントを検索した。

バージョン 06-00 以前の JP1/Base のイベントサービスに対して、サポートしていない条件（「を含む」、「を含まない」、「正規表現」の指定、または対処状況の複数指定）で JP1 イベントを検索しました。または、バージョン 06-51 以前の JP1/Base のイベントサービスに対して、サポートしていない条件（「正規表現」の指定）で JP1 イベントを検索しました。

- 対処

「を含む」、「を含まない」、「正規表現」を選択していないか、対処状況を複数選択していないかを確認後、再度検索します。

イベント検索実行時、指定した正規表現が間違っている。

- 対処

指定した正規表現を確認後、再度検索します。

除外条件を指定してイベント検索を実行した時、検索ホストの JP1/Base のバージョンが 08-11 以前だった。

- 対処

イベント検索の実行先に指定したホストの、JP1/Base のバージョンを確認し、08-11 以前の場合は除外条件を使用しないでイベント検索をします。

(28) メモ情報が設定できない場合の対処方法

次の要因が考えられます。

- イベントコンソールとセントラルコンソール・ビューアーの接続が確立しない。
- イベントコンソールサービスとイベント基盤サービスの接続が確立しない。
- イベント基盤サービスと統合監視 DB の接続が確立しない。

それぞれの対処を次に示します。

イベントコンソールとセントラルコンソール・ビューアーの接続が確立しない。

マネージャー上のイベントコンソールが起動していない、システム（ホスト、ネットワーク）が高負荷状態である、ネットワークの設定が誤っているというおそれがあります。

- 対処

イベントコンソールサービス、またはホストが正常に稼働しているか確認し、メモ情報を設定します。

`jco_spmc_status` コマンドを実行してマネージャー上のイベントコンソールサービスが起動しているか確認し、再度メモ情報を設定します。

または、`ping` コマンドなどを使用してログインしているホストが正常に稼働しているか確認し、再度メモ情報を設定します。

イベントコンソールサービスとイベント基盤サービスの接続が確立しない。

イベント基盤サービスが起動していない、システム（ホスト、ネットワーク）が高負荷状態になっているというおそれがあります。

- 対処

`jco_spmc_status` コマンドを実行してマネージャー上のイベント基盤サービスが起動しているか確認し、再度メモ情報を設定します。

イベント基盤サービスと統合監視 DB の接続が確立しない。

統合監視 DB が起動していない、システム（ホスト、ネットワーク）が高負荷状態になっているというおそれがあります。

- 対処

統合監視 DB を起動後、再度メモ情報を設定します。

(29) IM データベースが終了できない場合の対処方法

要因

接続中の JP1/IM - Manager プロセスが存在します。

対処

JP1/IM - Manager が起動しているかどうか確認します。起動している場合、JP1/IM - Manager を終了してから IM データベースを終了します。

(30) IM データベースに接続できない場合の対処方法

次の要因が考えられます。

- IM データベースを使用する設定になっていない。
- IM データベースが起動していない。
- ポート番号が正しく設定されていない。
- 非クラスタシステムの論理ホストをセットアップしたときに、`jcfdbsetup` または `jcodbsetup` コマンドの `-c` オプションに「standby」を指定している。

それぞれの対処を次に示します。

IM データベースを使用する設定になっていない。

- 対処

`jcoimdef` コマンドのオプションを指定せずに使用して、「S_DB」の設定値がON になっているか確認してください。`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。

IM データベースが起動していない。

- 対処

IM データベースが起動していることを確認してください。

ポート番号が正しく設定されていない。

- 対処

指定したポート番号が次のポート番号と重複していないかどうか確認してください。

- ほかの論理ホストのセットアップで指定したポート番号
- `services` ファイルに記載されているポート番号
- ほかの製品の組み込み HiRDB で使用しているポート番号
- ほかの製品、OS などが使用する一時ポート番号

非クラスタシステムの論理ホストをセットアップしたときに、オプション `-c` に「standby」を指定している。

- 対処

非クラスタシステムの論理ホストをセットアップする場合、`jcfdbsetup` または `jcodbsetup` コマンドの `-c` オプションに「online」を指定してください。

(31) JP1/IM - Manager がアンインストールできない場合の対処方法

「KAVB9940-E 物理ホストの IM データベースサービスがアンセットアップされていません」メッセージまたは「KAVB9941-E 論理ホストの IM データベースサービスがアンセットアップされていません」メッセージが出力される。

要因

IM データベースがアンセットアップされていません。

対処

統合監視 DB と IM 構成管理 DB がアンセットアップされていることを確認してください。

(32) IM データベースをセットアップしたときに、ポート番号不正のエラーメッセージが出力される場合の対処方法

「KNAN11044-E ポート番号が重複しています」メッセージが出力される。

要因

指定したポート番号が、ほかで使用しているポート番号と重複しています。

対処

指定したポート番号が次のポート番号と重複していないかどうか確認してください。

- ほかの論理ホストのセットアップで指定したポート番号
- services ファイルに記載されているポート番号
- ほかの製品の組み込み HiRDB で使用しているポート番号
- ほかの製品、OS などが使用する一時ポート番号

(33) IM データベースのセットアップに失敗する場合の対処方法

「KNAN11084-E DB ファイルシステム領域の作成に失敗しました」メッセージが出力される。

次の要因が考えられます。

- IMDBDIR, SHAREDDBDIR に指定したパスのファイルシステムがラージファイルに対応していない。
- カーネルパラメーターが適切に設定されていない。
- LOGICALHOSTNAME や ONLINEHOSTNAME に正しいホスト名を指定していない。

それぞれの対処を次に示します。

IMDBDIR, SHAREDDBDIR に指定したパスのファイルシステムがラージファイルに対応していない。

- 対処
対象の OS でラージファイル設定を有効にしてください。

カーネルパラメーターが適切に設定されていない。

- 対処
カーネルパラメーターが正しく設定されているか確認してください。カーネルパラメーターの詳細は、JP1/IM - Manager のリリースノートを参照してください。

LOGICALHOSTNAME や ONLINEHOSTNAME に正しいホスト名を指定していない。

- 対処

次の項目を確認してください。

- LOGICALHOSTNAME や ONLINEHOSTNAME に指定したホスト名が適切かどうか
- データベース関連のコマンドの-h オプションに指定したホスト名が適切かどうか
- hosts ファイルに指定したホスト名が記載されているかどうか、およびホスト名の重複がないかどうか
- 指定したホスト名に対応する IP アドレスが適切かどうか、および IP アドレスの重複がないかどうか

(34) IM データベースのセットアップでセットアップ情報ファイルが不正と出力される場合の対処方法

次のメッセージが出力される。

- [KNAN11030-E セットアップ情報ファイルに必須項目が指定されていません。(項目名:項目名)]
- [KNAN11038-E セットアップ情報ファイルに指定した項目が不正です。(項目名:項目名)]
- [KNAN11047-E セットアップ情報ファイルに指定した項目名が不正です。(項目名:項目名)]
- [KNAN11048-E セットアップ情報ファイルに指定した項目名が重複しています。(項目名:項目名)]

次の要因が考えられます。

- 指定されていない必須項目と値がある。
- 項目名に正しい文字列が指定されていない。
- 値に正しい値が指定されていない。
- ” =” の前後に不要な空白文字が入っている。

それぞれの対処を次に示します。

指定されていない必須項目と値がある。

- 対処

セットアップ情報ファイルおよびクラスタ情報ファイルを確認し、必須項目をすべて指定してください。

項目名に正しい文字列が指定されていない。

- 対処

セットアップ情報ファイルおよびクラスタ情報ファイルを確認し、必須項目をすべて指定してください。

値に正しい値が指定されていない。

- 対処

指定できる値であるかどうかを確認し、修正してください。

”=”の前後に不要な空白文字が入っている。

- 対処

”=”の前後などに不要な空白文字がないかどうか確認し、ある場合それを削除してください。

(35) IM データベースを起動できない、またはデータベース関連のコマンドが実行できない場合の対処方法

データベース関連のコマンドを実行するときに、「KNAN11037-E IM データベースサービスのデータ格納ディレクトリにアクセスできません」メッセージまたは「KNAN11143-E IM データベースサービスの構成が不正です」メッセージが出力される。

次の要因が考えられます。

- UNIX の場合、IM データベースのインストールディレクトリやデータ格納ディレクトリがアンマウントされている。
- ホスト名が変更されている。
- IM データベースが、ほかの製品で使用しているポート番号と重複したものを使用している。

それぞれの対処を次に示します。

UNIX の場合、IM データベースのインストールディレクトリやデータ格納ディレクトリがアンマウントされている。

- 対処

ディレクトリにアクセスできるかどうか確認し、アクセスできない場合はマウントしてください。

ホスト名が変更されている。

- 対処

ホスト名を一度以前のホスト名に戻してから、IM データベースのホスト名を変更する手順に従って、ホスト名を変更してください。

IM データベースが、他製品で使用しているポート番号と重複したものを使用している。

- 対処

指定したポート番号が次のポート番号と重複していないかどうか確認してください。

- ほかの論理ホストのセットアップで指定したポート番号
- services ファイルに記載されているポート番号
- ほかの製品の組み込み HiRDB で使用しているポート番号
- ほかの製品、OS などが使用する一時ポート番号

(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

要因

次の要因が考えられます。

- システムの階層構成を反映する次のホストの JP1/Base が起動していません。
 - 一括配布方式の場合
システムの階層構成に含まれているすべてのホスト
 - 差分配布方式の場合
システムの階層構成の変更対象のホストとその上位のマネージャーホスト
- システムの階層構成を反映するホストが、すでに別のシステムの階層構成に含まれています。
- 統合マネージャー，中継マネージャー，エージェント間で名前解決ができません。

対処

要因に従って対処してください。

- システムの階層構成の反映が失敗した次のホストの JP1/Base が起動しているか確認したあと，再実行してください。
 - 一括配布方式の場合
システムの階層構成に含まれているすべてのホスト
 - 差分配布方式の場合
システムの階層構成の変更対象のホストとその上位のマネージャーホスト
- システムの階層構成の反映が失敗したホスト上で，`jbsrt_get` コマンドを実行し，別のシステムの階層構成に含まれていないか確認してください。別のシステムの階層構成に含まれていた場合，そのシステムの階層構成から削除および反映したあとに，再実行してください。
- 各ホスト間で，ホスト名の名前解決ができていないかどうか確認してください。名前解決されていない場合は，名前解決されるように設定を変更したあとに，再実行してください。

(37) IM 構成管理でログファイルトラップ動作定義ファイルの取得に失敗した場合の対処方法

要因

ログファイルトラップ動作定義ファイルは，エージェント内でユニークにする必要があります。同一の設定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，または異なるディレクトリであっても，同一の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おそれがあります。

対処

次の手順で対処してください。

1. エージェント上で，ログファイルトラップを停止する。
2. ログファイルトラップ動作定義ファイル名をエージェント内でユニークな名称になるように設定し，再度ログファイルトラップ機能を起動する。

3. IM 構成管理・ビューアーの [プロフィール表示/編集] 画面で, [操作] メニューから [プロフィールツリー再構築] を選択して, プロファイルツリーを再構築する。

(38) JP1/IM - View から起動中のログファイルトラップがすべて表示されない場合の対処方法

要因

次の要因が考えられます。

- ログファイルトラップ機能を起動したあとに, プロファイルツリーの再構築を実行していません。
[プロフィール表示/編集] 画面の起動後, プロファイルツリーの再構築後, またはプロフィールの一括収集後に, ログファイルトラップが起動または再起動されたおそれがあります。
- ログファイルトラップを起動するときに指定した動作定義ファイルが, JP1Base パス¥conf 配下がありません。

対処

要因に従って対処してください。

- 最新のプロフィールリストを収集する必要があります。IM 構成管理・ビューアーの [プロフィール表示/編集] 画面で, [操作] メニューから [プロフィールツリー再構築] を選択して, プロファイルツリーを再構築してください。
- ログファイルトラップ動作定義ファイルを JP1Base パス¥conf 配下に配置して, ログファイルトラップ機能を再起動してください。

ログファイルトラップを起動したあと, IM 構成管理・ビューアーの [プロフィール表示/編集] 画面で, [操作] メニューから [プロフィールツリー再構築] を選択して, プロファイルツリーを再構築してください。

(39) プロファイルの設定ファイルと有効設定情報の内容が異なる場合の対処方法

要因

次の要因が考えられます。

- 設定ファイルを編集したあと, 編集内容を反映していない, または反映に失敗しています。
- 設定ファイルの記述が一部間違っています。

設定ファイルの記述が一部間違っていると, エージェントでは記述誤りの個所を読み飛ばして反映する場合があります。この場合, IM 構成管理・ビューアーから反映を実行したときにエラーダイアログが表示されます。

対処

要因に従って対処してください。

- IM 構成管理・ビューアーの [プロフィール表示/編集] 画面から, 設定ファイルの内容を確認したあと, プロファイルの反映を実行し, 正常に反映が終了したことを確認してください。

- 設定ファイルの反映に失敗した場合、設定ファイルの記述どおりにサービスが稼働していないおそれがあります。記述誤りを修正し、反映を再実行してください。

(40) IM 構成管理・ビューアーで、[ホスト登録]、[エージェント構成編集]などのメニュー項目が非活性になっている場合の対処方法

要因

IM 構成管理・ビューアーにログインした JP1 ユーザーに IM 構成管理の権限（JP1_CF_Admin, JP1_CF_Manager, JP1_CF_User のどれか）が割り当てられていないため、実行できる操作が参照だけになっています。次の場合が考えられます。

- 認証サーバに設定されている JP1/Base がバージョン 8 以前です。
- 認証サーバに設定されている JP1/Base をバージョン 8 以前から上書きインストールしたあと、JP1 ユーザーに IM 構成管理の権限（JP1_CF_Admin, JP1_CF_Manager, JP1_CF_User のどれか）を割り当てていません。
- JP1 ユーザーに IM 構成管理の権限（JP1_CF_Admin, JP1_CF_Manager, JP1_CF_User のどれか）を割り当てていません。

対処

要因に従って対処してください。

- 認証サーバに設定されている JP1/Base をバージョン 9 以降にしてください。
- ログインする JP1 ユーザーの JP1 資源グループにグループ名「JP1_Console」、権限レベルに IM 構成管理の権限（JP1_CF_Admin, JP1_CF_Manager, JP1_CF_User のどれか）を割り当ててから、再度ログインしてください。

なお、IM 構成管理の権限レベルによって、各メニューの操作できる範囲が異なります。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「付録 E.4 IM 構成管理で必要な操作権限」を参照してください。

(41) IM 構成管理で仮想化システム構成の収集に失敗した場合の対処方法

「KNAN22062-E ホスト(ホスト名)の通信種別はサポートしていないため、仮想化構成の収集に失敗しました」メッセージが出力される。

要因

次の要因が考えられます。

- 収集先ホスト名が異なります。
- 収集先ホストの名前解決ができていません。
- 収集先ホストが起動されていません。
- 収集先ホストの vCenter, JP1/SC/CM, SCVMM, HCSM, KVM が起動されていない、またはセットアップされていません。

- 収集先ホストとの通信で障害が発生しています。

対処

要因に従って対処してください。

- 収集先ホスト名が正しいかどうか確認してください。
- 収集先ホストが起動しているかどうか確認してください。
- 収集先ホストの vCenter, JP1/SC/CM, SCVMM, HCSM, KVM が起動しているかどうか、およびセットアップが完了しているかどうか確認してください。
- 収集先ホストとの通信に問題はないかどうか確認してください。また、収集先ホストの VMM ホストが KVM の場合、SSH 接続が正しく設定されているか確認してください。

(42) IM 構成管理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の有効設定情報が参照できない場合の対処方法

「KNAN22422-E ログファイルトラップ情報の有効設定上の収集が出来ませんでした。(詳細情報: 該当するサービスもしくはプロセスが稼働していません)」または、「KNAN22422-E イベントログトラップ情報の有効設定上の収集が出来ませんでした。(詳細情報: 該当するサービスもしくはプロセスが稼働していません)」メッセージが出力される。

要因

次の要因が考えられます。

- リモート監視ログファイルトラップの稼働中にエラーが発生したため、リモート監視ログファイルトラップが停止した。
- リモート監視イベントログトラップの稼働中にエラーが発生したため、リモート監視イベントログトラップが停止した。

対処

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の稼働中に発生したエラーの内容は、統合ログに出力されます。統合ログに出力されているエラーメッセージの対処を参照して、エラーの原因を取り除いてください。そのあと、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を停止したあと、再度起動してください。

(43) IM 構成管理でリモート監視ログファイルトラップが稼働しているにもかかわらず JP1 イベントが受信されない場合の対処方法

要因

次の要因が考えられます。

- リモート監視ログファイルトラップ動作定義ファイルのフィルター (filter~end-filter) の指定に誤りがあります。

- リモート監視ログファイルトラップの監視間隔が長く、ログファイルの差分がまだ監視されていません。
- リモートの監視対象ホストまたは監視対象ログファイルが不正な状態ですが、[プロファイル表示/編集] 画面の [有効設定情報] ページで [ログファイルトラップ情報] - [起動オプション動作] の [open リトライ指定[-r]] を有効に指定している、または `jcfallogstart` コマンドに `-r` オプションを指定しているためエラーが発生していません。
- リモート監視ログファイルトラップの起動オプションでフィルターの指定が誤っているため、監視対象のログファイルデータが監視対象ホストから転送されていません。

対処

- リモート監視ログファイルトラップ動作定義ファイルのフィルター (`filter~end-filter`) の指定が正しいかどうか確認してください。
- `jcfallogstart` コマンドの `-t` オプションで指定しているファイル監視間隔以上の時間が経過しても JP1 イベントが受信されないかどうか確認してください。
- リモートの監視対象ホストが Windows の場合、リモートの監視対象ホストでログ監視をするための NetBIOS (NetBIOS over TCP/IP) の設定が正しいかどうかを確認してください。NetBIOS (NetBIOS over TCP/IP) の設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.18.2 NetBIOS (NetBIOS over TCP/IP) の設定 (Windows の場合)」を参照してください。
- リモートの監視対象ホストが UNIX の場合、リモートの監視対象ホストでログ監視をするための SSH の設定が正しいかどうかを確認してください。SSH の設定については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「2.17.1 SSH の設定 (UNIX の場合)」を参照してください。
- 監視対象ログファイルが読み取りできる状態であることを確認してください。
- 対話操作が必要となる、`stty`, `tty`, `tset`, `script` コマンドなどが SSH 接続ユーザーのログインスクリプトに記載されている場合、ログファイルの読み込みに失敗することがあります。この場合、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。
- リモート監視ログファイルトラップの起動オプションでフィルターの指定に誤りがないか確認してください。フィルターの指定に誤りがない場合、リモートの監視対象ホストで SSH 接続を使用しているユーザーが、次のコマンドを実行できるかどうかを確認してください。

Linux の場合

```
/bin/grep -E 'フィルターに指定した正規表現文字列' 監視対象ログファイルパス
```

Solaris の場合

```
/usr/xpg4/bin/grep -E 'フィルターに指定した正規表現文字列' 監視対象ログファイルパス
```

Linux, Solaris 以外の場合

```
/usr/bin/grep -E 'フィルターに指定した正規表現文字列' 監視対象ログファイルパス
```

また、監視対象ログファイルのデータが、フィルターの指定によって除外されていないかどうかを確認してください。

- 追加オプションに-rを指定している場合、次の点も確認してください。
 「12.5.3(50) リモート監視の監視対象ログファイル名が誤っている場合の対処方法」を参照してパスが正しく指定されているか確認してください。
 - ファイルのアクセス権が正しく設定されているか確認してください。
 - rを指定しないでログファイルトラップを稼働させエラーが発生するか確認することも有効です。
- 以上の対処をしても現象が解決しない場合、JP1/IM - Manager ホストおよび監視対象ホストで資料採取ツールを使って資料を採取してください。監視対象ホストで採取する資料を次に示します。

監視対象ホストの OS	採取する資料	方法
Windows	システム情報	1. 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. テキストボックスに「msinfo32」と入力し、[OK] ボタンをクリックする。 3. [システム情報] 画面で [ファイル] - [エクスポート] を選択して、システム情報をテキストファイルに保存する。
	監視対象ログファイル	複数ある場合は、すべてのログファイルを採取する。
	Windows イベントログのアプリケーションおよびシステム	1. イベントビューアーで対象のイベントログを選択する。 2. [ログファイルの名前を付けて保存] を選択する。 3. 出力形式は、「evt」を指定する。
UNIX	監視対象ログファイル	複数ある場合は、すべてのログファイルを採取する。
	シスログ (syslog)	シスログを採取する。詳細については、「12.3.1(2)UNIX の場合」を参照してください。

(44) IM 構成管理でリモート監視イベントログトラップが稼働しているにもかかわらず JP1 イベントが受信されない場合の対処方法

要因

- リモートの監視対象ホストと JP1/IM - Manager ホストで時刻設定に差異があります。
- リモートの監視対象ホストに、監視対象ホストの現在時刻より未来の時刻のイベントログが存在します。
- フィルターの指定が正しくありません。

対処

- リモートの監視対象ホスト、および JP1/IM - Manager の時刻を正しく現在の時刻に合わせてください。

- リモートの監視対象ホストに、監視対象ホストの現在時刻より未来の時刻のイベントログが存在しないか確認してください。
- 有効設定情報に表示されるフィルター情報の条件文に示す内容が取得できるフィルター設定にしてください。
- 以上の対処をしても現象が解決しない場合、JP1/IM - Manager ホストおよび監視対象ホストで資料採取ツールを使って資料を採取してください。監視対象ホストで採取する資料を次に示します。

採取する資料	方法
システム情報	<ol style="list-style-type: none"> 1. 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. テキストボックスに「msinfo32」と入力し、[OK] ボタンをクリックする。 3. [システム情報] 画面で [ファイル] - [エクスポート] を選択して、システム情報をテキストファイルに保存する。
Windows イベントログのアプリケーションおよびシステム	<ol style="list-style-type: none"> 1. イベントビューアーで対象のイベントログを選択する。 2. [ログファイルの名前を付けて保存] を選択する。 3. 出力形式は、「evt」を指定する。

(45) IM 構成管理・ビューアーで処理中ダイアログが表示され続ける場合の対処方法

要因

JP1/IM - Manager ホスト、または操作対象のエージェントが停止しています。

対処

JP1/IM - Manager ホスト、または操作対象のエージェントが停止していないかどうか確認してください。

停止している場合は、[処理中] ダイアログボックスの [×] (閉じる) ボタンをクリックし、IM 構成管理・ビューアーを強制終了してください。

停止していない場合は、IM 構成管理が処理中のため、処理が完了するまで待ってください。

(46) IM 構成管理・ビューアーで、[IM 構成] ページのツリー表示領域がグレー表示される場合の対処方法

IM 構成管理・ビューアーで、[IM 構成の取得] を実行した場合にツリー表示領域がグレー表示される。

要因

次の要因が考えられます。

- マネージャーホストでjbsrt_del コマンドが実行され、JP1/Base で保持している構成定義情報が存在しない。

対処

IM 構成管理・ビューアーで、[エージェント構成の反映] を実行してください。

IM 構成管理・ビューアーで、ログインまたは [IM 構成の検証] を実行した場合にツリー表示領域がグレー表示される。

要因

IM 構成管理 DB が保持する構成定義情報と、JP1/Base で保持している構成定義情報が不一致となっています。次の要因が考えられます。

- jcfimport コマンドでインポートした直後でエージェント構成が反映されていない。
- マネージャーホストで jbsrt_del コマンドが実行され、JP1/Base で保持している構成定義情報が存在しない。
- jbsrt_distrib コマンドが実行され、JP1/Base で保持している構成定義情報が変更されている。
- エージェント構成が反映されていない。
- 拠点マネージャーで拠点ごとに管理する場合に、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「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」の手順が実行されていない。

対処

要因に従って対処してください。

- エージェント構成が反映されていない場合は IM 構成管理・ビューアーで、[エージェント構成の反映] を実行してください。
- IM 構成管理・ビューアーで、[IM 構成の取得] を実行してください。実行した結果、意図した構成になっていない場合には、[エージェント構成の反映] を実行してください。

(47) IM 構成管理のリモート監視ログファイルトラップで同じ JP1 イベントが重複して受信される場合の対処方法

要因

- ログ収集処理中にログが出力された場合、同一のログが 2 回トラップされる場合があります。

対処

- 対処の必要はありません。重複した JP1 イベントは無視してください。

(48) IM 構成管理でリモート監視ログファイルトラップのプロファイルの起動に失敗した場合の対処方法

「KNAN26039-E 起動対象のリモートログファイルトラップの開始に失敗しました。(監視対象ホスト名: 監視対象ホスト名, 監視名: 監視名, 詳細情報: 詳細メッセージ)」メッセージが出力され、プロファイルの起動に失敗する。

マニュアル「JP1/Integrated Management 3 - Manager メッセージ」の「2.13 IM 構成管理に関するメッセージ (KNAN22000~KNAN26999)」の「KNAN26039-E」の対処を参照してください。

それでも解決できない場合は次の対処方法を確認してください。

詳細情報の種類によって対処方法が異なります。

監視対象ホストに接続できません。

要因

- 監視対象ホストに接続できていません。

対処

- 「12.5.3(51) リモート監視の監視対象ホストと接続できない場合の対処方法」を参照してリモート監視対象との接続を確認してください。

監視対象のログファイルにアクセスできません。

要因

- ログファイルのパスが正しく指定されていません。

対処

- 「12.5.3(50) リモート監視の監視対象ログファイル名が誤っている場合の対処方法」を参照してパスが正しく指定されているか確認してください。

(49) IM 構成管理でリモート監視ログファイルトラップを始める前の注意事項

注意点

- ログファイルのファイルタイプが合っているか確認してください。
- ログファイルサイズが大き過ぎないか確認してください。
- ログファイルのヘッダーサイズが大き過ぎないか確認してください。
- JP1/Base LogTrap サービスが停止していないか確認してください。

(50) リモート監視の監視対象ログファイル名が誤っている場合の対処方法

次の項目が正しく設定できているか確認してください。

マニュアル「JP1/Integrated Management 3 - Manager 画面リファレンス」の「5.9.2 [設定ファイル] ページ」の「表 5-31 設定ファイルに追加して表示される項目 (ログファイルトラップ情報を選択した場合)」の項目

間違いやすい例を次に示します。

- リモートの監視対象ホストが Windows の場合でパスが「¥共有フォルダ名¥ファイル名」になっていない。

- リモートの監視対象ホストが UNIX の場合でパスがフルパスになっていない。
- パスがフォルダを指定している。

(51) リモート監視の監視対象ホストと接続できない場合の対処方法

次の項目が正しく設定できているか確認してください。

JP1/IM - Manager ホストが Windows の場合

マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の次に示す個所を参照してください。

- 「1.18.1 WMI の設定 (Windows の場合)」
- 「1.18.2 NetBIOS (NetBIOS over TCP/IP) の設定 (Windows の場合)」
- 「1.18.3 SSH の設定 (Windows の場合)」

JP1/IM - Manager ホストが UNIX の場合

マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「2.17.1 SSH の設定 (UNIX の場合)」

次の項目を確認してください。

- 監視対象ホストが起動していない。
- JP1/IM - Manager ホストから監視対象ホストが名前解決できない。

(52) IM 構成管理でホスト情報の収集に失敗した場合の対処方法

メッセージの種類によって対処方法が異なります。

「KNAN22017-E ホスト(ホスト名)と通信できなかったため、ホスト情報の収集に失敗しました」メッセージが出力され、ホスト情報の収集に失敗する。

要因

次の要因が考えられます。

- 収集先ホスト名が異なります。
- 収集先ホストの名前解決ができていません。
- 収集先ホストが起動されていません。
- 収集先ホストの JP1/Base が起動されていません。
- 収集先ホストとの通信で障害が発生しています。
- 収集先ホストの JP1/Base のバージョンが 07-00 より古いです。

対処

要因に従って対処してください。

- JP1/IM - Manager のホストで次のコマンドを実行し、IM 構成管理に登録したホストの名前解決ができるか、および IM 構成管理に登録したホストに通信できるか確認してください。なお、IPv6 環境で運用する場合、IPv6 アドレスがプライマリー IP アドレスとなっているか（次のコマンドの結果の一つとして表示される「Resolved Host List」に、最初に表示されているか）、IPv6 アドレスで通信できるか確認してください。

- `jp1ping` IM 構成管理に登録したホスト名

JP1/IM - Manager のホストで次のコマンドを実行し、IM 構成管理に登録したホストに対して、指定したポート番号で通信できるか確認してください。

- `telnet` エージェントホスト名または IP アドレス 20306

なお、IPv6 環境で運用する場合、`telnet` のコマンドの接続先に IPv6 アドレスを指定してください。ホスト情報を収集するときに使用するポート番号は、デフォルトの場合、20306/tcp です。接続できない場合は、接続できないことを表すメッセージが表示されます。接続できた場合は、黒い画面が表示されます。

Windows Server 2008 R2 以降の Windows ホストの場合、Telnet クライアントは既定ではインストールされていません。Telnet クライアントは Windows の機能の追加と削除からインストールできます。

- 収集先ホストの JP1/Base のバージョンが 07-00 以降であるか確認してください。IPv6 環境で運用する場合、収集先ホストの JP1/Base がバージョン 10 以降か確認してください。

- 次のコマンドで収集先ホストの JP1/Base が起動しているか確認してください。

- `jbs_spmd_status` (論理ホストの場合：`jbs_spmd_status -h` 論理ホスト名)

- `jevstat` (論理ホストの場合：`jevstat` 論理ホスト名)

- 収集先ホストで次のコマンドを実行し、JP1/IM - Manager のホストの名前解決ができるか、および JP1/IM - Manager のホストに通信できるか確認してください。なお、IPv6 環境で運用する場合、IPv6 アドレスがプライマリー IP アドレスとなっているか（次のコマンドの結果の一つとして表示される「Resolved Host List」に、最初に表示されているか）、IPv6 アドレスで通信できるか確認してください。

- `jp1ping` JP1/IM - Manager のホスト名

- IPv6 環境で運用する場合、JP1/IM - Manager のホストで通信方式が ANY バインドアドレスを指定しているときは、バインドする IP アドレスのバージョンの設定が正しいか、次の手順で確認してください。

1.jbsgetcnf コマンドを実行する。

```
jbsgetcnf > config.txt
```

2.config.txt をテキストエディターで開く。

3.[JP1_DEFAULT¥JP1BASE¥JP1_ANY_BIND]の値が「ALL」になっているかを確認する。

- IPv6 環境で運用する場合、収集先ホストで通信方式が ANY バインドアドレスを指定しているときは、バインドする IP アドレスのバージョンの設定が正しいか、次の手順で確認してください。

1.jbsgetcnf コマンドを実行する。

```
jbsgetcnf > config.txt
```

2.config.txt をテキストエディターで開く。

3.[JP1_DEFAULT¥JP1BASE¥JP1_ANY_BIND]の値が「ALL」または「IPv6」になっているかを確認する。

- 収集先ホストのショート名と FQDN から解決される IP アドレスが同一であることを確認してください。

次のメッセージが出力され、ホスト情報の収集に失敗する。

- KNAN21400-W ホスト(ホスト名)のホスト情報の収集に一部成功しました
JP1/Base からのホスト情報の収集に成功しました
リモートによるホスト情報の収集に失敗しました
詳細情報: [詳細情報](#)
- KNAN21402-E ホスト(ホスト名)のホスト情報の収集に失敗しました
JP1/Base からホスト情報収集に失敗しました
詳細情報: [詳細情報](#)
リモートによるホスト情報の収集に失敗しました
詳細情報: [詳細情報](#)
- KNAN21403-E ホスト(ホスト名)のリモートによるホスト情報の収集に失敗しました
詳細情報: [詳細情報](#)

要因

リモートによるホスト情報の収集に失敗した場合、次の要因が考えられます。

- リモート通信設定が設定されていません。
- 監視対象ホストと接続できません。
- ログファイルの収集がタイムアウトしました。
- 認証に失敗しました。
- 秘密鍵が存在しません。
- リモート監視プロセスの作成に失敗しました。

対処

要因に従って対処してください。

- 監視対象ホストのリモート通信を設定してから再実行してください。
- リモート監視対象との接続を確認してください。確認方法については、「[12.5.3\(51\) リモート監視の監視対象ホストと接続できない場合の対処方法](#)」を参照してください。
- 次の項目を確認してください。

監視対象ホスト名のホストの OS が Windows の場合

- 監視対象ホスト名のホストに通信できるか
- 監視対象ホストにログインするユーザーのパスワードの有効期限が切れていないか
- 監視対象ホスト名のリモート通信種別が正しく設定されているか

- ・ WMI サービスが起動しているか

確認して異常がない場合は、WMI 接続が正常に設定できているか確認してください。

監視対象ホスト名のホストの OS が UNIX の場合

- ・ 監視対象ホスト名のホストに通信できるか
- ・ 監視対象ホスト名のリモート通信種別が正しく設定されているか
- ・ 監視対象ホスト名のホストで SSH サーバが起動しているか

確認して異常がない場合は、SSH 接続が正常に設定できているか確認してください。

- ・ 次の項目を確認してください。

監視対象ホスト名のホストの OS が Windows の場合

- ・ [システム共通設定] 画面または [リモート監視設定] 画面のユーザー名、パスワード、およびドメイン名が正しく設定されているか
- ・ 監視対象ホスト名のホストで DCOM が正しく設定されているか
- ・ JP1/IM - Manager のホストで DCOM が正しく設定されているか

確認して異常がない場合は、WMI 接続が正常に設定できているか確認してください。

監視対象ホスト名のホストの OS が UNIX の場合

- ・ SSH 認証の設定が正しいか

確認して異常がない場合は、SSH 接続が正常に設定できているか確認してください。

- ・ 秘密鍵があるか確認してください。
- ・ [システム共通設定] 画面の [IM ホストアカウント] ページの設定を確認してください。

(53) IM 構成管理に登録するホスト名と発生元ホスト名が異なってしまう場合の対処方法

対処

バージョンによって対処をしてください。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「14.3.10(2)(b) JP1 イベントの属性を変更する (JP1/IM - Manager の設定)」を参照してください。

- ・ JP1/IM - Manager を新規インストールまたは上書きインストールした場合、次の手順を実行してください。
 1. 共通定義設定用ファイル (JP1 イベントの属性変更) の内容を確認する。
 2. jbssetcnf コマンドを実行する。
 3. JP1/IM - Manager を再起動する。
- ・ JP1/IM - Manager のバージョンが 10-00 より前の場合、IM 構成管理にショートネームと FQDN 形式の両方のホスト名を登録してください。

(54) 監視対象ホスト名と発生元ホスト名が異なっていてフィルターが正常に動作しない場合の対処方法

対処

対処方法については、「12.5.3(53) IM 構成管理に登録するホスト名と発生元ホスト名が異なってしまふ場合の対処方法」を参照してください。

(55) Windows で OS 起動後またはネットワーク設定変更後、JP1/IM - Manager が起動しない、または、JP1/IM - View の操作ができなくなった場合の対処方法

要因

次の要因が考えられます。

- OS 起動後、ネットワークが使用できる前に、JP1/IM - Manager の起動処理が開始されました。OS 起動後、ネットワークが使用できるまでの時間は環境に依存します。チーミングを設定している環境では、ネットワークが使用できるまでに（2～3分程度）時間が掛かる現象が確認されています。チーミングを設定している環境では、JP1/Base の起動管理機能で JP1/IM - Manager が自動的に起動されるなど、ネットワークが使用できるようになる前に、JP1/IM - Manager の起動処理が開始されることがあります。
- JP1/IM - Manager の起動中にネットワークの設定（チーミングの設定など）を変更しました。

対処

物理ホスト、すべての論理ホストの JP1/IM - Manager, JP1/IM - View, JP1/Base, および JP1/Base が前提のプログラムを終了します。「jplping 自ホスト名」を実行し、想定する IP アドレスで自ホスト名が解決できることを確認してから、JP1/Base, JP1/IM - Manager, JP1/IM - View, および JP1/Base が前提のプログラムを起動してください。

また、それぞれの回避方法を次に示します。

- OS 起動後、ネットワークが使用できるようになる前に、JP1/IM - Manager の起動処理が開始された場合
OS 起動時に JP1/IM - Manager を自動的に起動する場合、JP1/Base の起動管理機能を使用してください。その場合は、JP1/IM - Manager のサービスが起動するタイミングを遅らせる設定にすることで、ネットワークが使用できるようになってから JP1/IM - Manager を起動するようにしてください。設定の詳細については、マニュアル「JP1/Base 運用ガイド」のサービスが起動するタイミングを設定する説明に関する章を参照してください。
- JP1/IM - Manager の起動中にネットワークの設定（チーミングの設定など）を変更した場合
ネットワークの設定（チーミングの設定など）を変更する場合は、物理ホスト、およびすべての論理ホストの JP1/IM - Manager, JP1/IM - View, JP1/Base, および JP1/Base が前提のプログラムを終了してください。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。

(56) JP1/SES 形式のイベントを受信して文字化けが発生した場合の対処方法

要因

JP1/SES 形式のイベント（バージョンが古い JP1 製品が出力したイベント、または JP1/Open Job Entry など JP1 イベント出力に対応していない製品が出力したイベント）は、文字コード情報を保持しません。

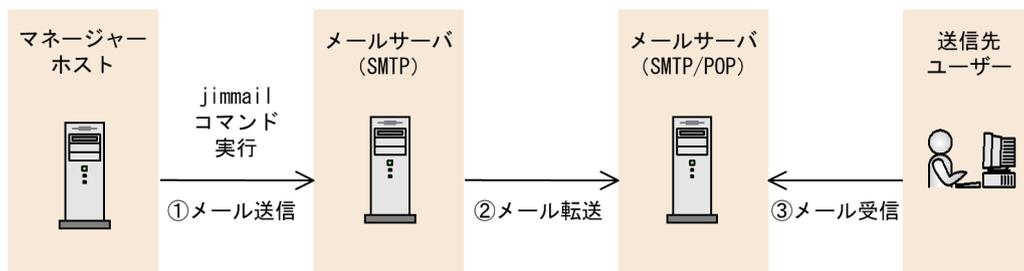
JP1/IM - Manager は、JP1/IM - Manager が動作する文字コードで JP1/SES 形式のイベントを解釈します。そのため、JP1/SES 形式のイベントの文字コードと JP1/IM - Manager が動作する文字コードが異なる場合、JP1/SES 形式のイベントが文字化けして表示されたり、異なる文字として扱われたりします。

対処

次のどちらかの方法で対処してください。

- JP1/SES 形式のイベントの文字コードと JP1/IM - Manager が動作している文字コードを統一してください。
- JP1/SES 形式のイベントと同じ文字コードで動作する JP1/Base でローカルアクションを使用して、JP1/SES 形式のイベント受信時に JP1 イベントを発行し、JP1/IM - Manager 側のホストで JP1 イベントを受信するようにしてください。ローカルアクションの詳細は、マニュアル「JP1/Base 運用ガイド」のローカルアクションの説明に関する章を参照してください。

(57) JP1/IM - Manager のメール通知機能でメールが送信先に届かない場合の対処方法



JP1/IM - Manager

`jimmail` コマンドは正常終了したが、メールが送信先に届かない場合

要因 1

メールの送信先アドレスが誤っています。

対処 1

メールの送信先アドレスが誤っているおそれがあるため、`jimmail` コマンドの `-to` オプション、またはメール環境定義ファイルの `DefaultTo` の送信先メールアドレスが正しいか確認してください。

`jimmail` コマンドの `-to` オプションと、メール環境定義ファイルの `DefaultTo` の両方に送信先メールアドレスが指定されている場合、`jimmail` コマンドの `-to` オプションに指定した送信先メールアドレスが優先されます。

要因 2

メールサーバ (SMTP) とメールサーバ (SMTP/POP3) 間でエラーが発生し、メールの転送に失敗しています。

対処 2

次の項目を確認して、再度 jimmail コマンドを実行してください。

- メールサーバ (SMTP/POP3) が起動しているか。
- メールサーバ (SMTP) のログを見て、エラーが発生していないか。
- ファイアウォールで使用するポート番号の通過が可能か。
- メールサーバのホスト名解決が可能か。

要因 3

メールサーバ (SMTP/POP3) とメールクライアント間でメールの受信に失敗しました。

対処 3

メールサーバとメールクライアントの通信のため、JP1/IM - Manager ではエラーを確認できません。メールサーバとメールクライアントのメッセージ、およびログを確認してください。

また、メールクライアントの設定 (POP3 サーバ名、POP3 アカウント名、パスワード、ポート番号) が正しいか確認してください。

jimmail コマンドが異常終了した場合

要因

メールサーバ (SMTP) に接続できません。

対処

エラー内容によって、jimmail コマンドがエラーメッセージを出力します。出力されたメッセージの対処、および次の項目を確認して、再度 jimmail コマンドを実行してください。

メッセージの詳細については、マニュアル「JP1/Integrated Management 3 - Manager メッセージ」の「2. メッセージ一覧」を参照してください。

- メールサーバ (SMTP) が起動しているか。
- メールサーバ (SMTP) のログを見て、エラーが発生していないか。
- ファイアウォールで使用するポート番号の通過が可能か。
- メールサーバ (SMTP) のホスト名解決が可能か。
- メール環境定義ファイルの認証アカウントおよびパスワードが正しいか。

(58) 通信暗号化機能が有効の JP1/IM - Manager で、エラーが表示される場合の対処方法

メッセージの種類によって対処方法が異なります。

JP1/IM - Manager が起動しない場合

- 「KAVB8817-E JP1/IM - Manager の通信暗号化機能のパラメーターで指定したファイルが読み込めません。(パラメーター名:パラメーター名, パラメーター値:パラメーター値)」メッセージが出力される。
- 「KAVB8818-E JP1/IM - Manager の通信暗号化機能のパラメーターで指定した秘密鍵が読み込めません。(秘密鍵パラメーター名:パラメーター名, 秘密鍵パラメーター値:パラメーター値, サーバ証明書パラメーター名:パラメーター名, サーバ証明書パラメーター値:パラメーター値)」メッセージが出力される。

要因

次の要因が考えられます。

- JP1/IM - Manager の通信暗号化機能のパラメーターで指定したファイルが読み込めません。
- JP1/IM - Manager の通信暗号化機能のパラメーターで指定した秘密鍵が読み込めない、またはサーバ証明書と対になっていません。

対処

要因に従って対処してください。

- サーバ証明書と秘密鍵が対になっていることを確認してください。対になっていない場合は、対になっているサーバ証明書と秘密鍵を配置してください。
- 秘密鍵のファイルのフォーマットに問題ないことを確認してください。
- 秘密鍵にパスワードが設定されている場合は、パスワードを解除してください。
- 次の OS のログを確認し、ファイルディスクリプタなどの OS のリソース不足がほかに発生していないかを確認してください。
 - ・ Windows の場合：Windows イベントログ
 - ・ UNIX の場合：シスログ (syslog)

jcochfilter コマンド、jcochstat コマンドが実行時に失敗する場合

- 「KAVB1956-E コマンド(コマンド名)の通信暗号化機能の初期化処理でエラーが発生しました。(要因:要因, ディレクトリ名:ディレクトリ名)」メッセージが出力される。
- 「KAVB1957-E コマンド(コマンド名)の通信暗号化機能で暗号化通信に失敗しました。(接続先ホスト名:接続先ホスト名, 要因:要因)」メッセージが出力される。

要因

次の要因が考えられます。

- ルート証明書ファイルが見つかりません。
- ルート証明書ファイルが読み込めません。
- サーバ証明書の CN または SAN と接続先のホスト名が異なります。
- 通信エラーが発生しました。
- システムエラーが発生しました。

対処

要因に従って対処してください。

- ルート証明書がある場合は、ルート証明書に読み込み権限があるか確認してください。読み込み権限がない場合は、ルート証明書に読み込み権限を設定してください。
- ルート証明書がない場合はルート証明書を配置してください。
- ルート証明書のファイルに問題がないことを確認してください。
- 次の OS のログを確認し、ファイルディスクリプタなどの OS のリソース不足がほかに発生していないかを確認してください。
 - Windows の場合：Windows イベントログ
 - UNIX の場合：シスログ (syslog)
- 接続先のマネージャーホストのサーバ証明書の CN または SAN と、jcochstat コマンドの-h オプションで指定したマネージャーホスト名が同じであることを確認して、コマンドを再実行してください。
- 次の確認をしてからコマンドを再実行してください。
 - jcochstat コマンドの場合は-h オプションで指定したマネージャーホストのサーバ証明書に対応するルート証明書が、コマンドを実行したホストに配置されているか確認してください。配置されていない場合は、配置してください。
 - jcochstat コマンドの場合は-h オプションで指定したマネージャーホストの通信暗号化機能が有効であることを確認してください。有効でない場合は、有効にしてください。
 - jcochstat コマンドの場合は-h オプションで指定したマネージャーホストのサーバ証明書が有効期限内かどうか確認してください。有効期間外の場合は、サーバ証明書を更新してください。
 - JP1/IM - Manager 起動後に通信暗号化機能の設定を変更した可能性があります。JP1/Base および JP1/IM - Manager を再起動し、通信暗号化機能の設定を反映してください。
- 「システムエラーが発生しました。」の場合は、資料採取ツールで資料を採取し、システム管理者に連絡してください。

jcochfilter コマンド、jcochstat コマンドの実行時に警告メッセージが出力される場合

「KAVB1972-W コマンド(コマンド名)の通信暗号化機能で使用するルート証明書が有効期間外です。(ファイル名:ファイル名)」

要因

次の要因が考えられます。

- 通信暗号化機能で使用するルート証明書が有効期間外です。

対処

要因に従って対処してください。

- ルート証明書が有効期間外の状態で運用することに問題があるか確認してください。問題がある場合は、システム管理者に連絡し、ルート証明書を更新してください。

コマンド (jcschstat, jcsdbexport, jcsdbimport) 実行時に失敗する場合

- 「KAVB7602-E メモリ不足のためコマンドの実行を中断します」メッセージが出力される。
- 「KAVB7810-E コマンド(コマンド名)の通信暗号化機能の初期化処理でエラーが発生しました。(要因:要因)」メッセージが出力される。
- 「KAVB7818-E コマンド(コマンド名)に必要なライブラリがありません。」メッセージが出力される。
- 「KAVB7812-E コマンド(コマンド名)の通信暗号化機能で暗号化通信に失敗しました。(接続先ホスト名:接続先ホスト名, 要因:要因)」メッセージが出力される。

要因

次の要因が考えられます。

- コマンドの実行に必要なメモリーが不足しています。
- コマンドに必要なライブラリがありません。
- 通信エラーが発生しました。
- システムエラーが発生しました。

対処

JP1/IM - Manager 起動後に通信暗号化機能の設定を変更した可能性があります。JP1/Base および JP1/IM - Manager を再起動し、通信暗号化機能の設定を反映してから、コマンドを再実行してください。解決されない場合は、資料採取ツールで資料を採取し、システム管理者に連絡してください。

次のコマンド実行時に失敗する場合

jcfvirtualchstat, jcfexport, jcfimport, jcfaleltdef, jcfaleltreload, jcfaleltstart, jcfaleltstat, jcfaleltstop, jcfallogdef, jcfallogreload, jcfallogstart, jcfallogstat, jcfallogstop

- 「KNAN24155-E コマンド(コマンド名)の通信暗号化機能で暗号化通信に失敗しました。(接続先ホスト名:接続先ホスト名, 要因:要因)」メッセージが出力される。

要因

次の要因が考えられます。

- 通信エラーが発生しました。
- システムエラーが発生しました。

対処

要因に従って対処してください。

- JP1/IM - Manager 起動後に通信暗号化機能の設定を変更した可能性があります。JP1/Base および JP1/IM - Manager を再起動し、通信暗号化機能の設定を反映してから、コマンドを再実行してください。解決されない場合は、資料採取ツールで資料を採取し、システム管理者に連絡してください。

IM 構成同期実行時に失敗する場合

- 「KNAN29095-E IM 構成管理サービスの通信暗号化機能の初期化処理でエラーが発生しました。(要因:要因, ファイル名:ファイル名)」メッセージが出力される。
- 「KNAN29098-E IM 構成管理サービスの通信暗号化機能で暗号化通信に失敗しました。(接続先ホスト名:接続先ホスト名, 要因:要因)」メッセージが出力される。

要因

次の要因が考えられます。

- ルート証明書ファイルが見つかりません。
- ルート証明書ファイルが読み込めません。
- サーバ証明書の CN または SAN と接続先のホスト名が異なります。
- 通信エラーが発生しました。
- システムエラーが発生しました。

対処

要因に従って対処してください。

- ルート証明書に読み込み権限があるか確認してください。読み込み権限がない場合は、ルート証明書に読み込み権限を設定してください。
- ルート証明書がない場合はルート証明書を配置してください。
- ルート証明書のファイルに問題がないことを確認してください。
- 次の OS のログを確認し、ファイルディスクリプタなどの OS のリソース不足がほかに発生していないかを確認してください。
 - Windows の場合：Windows イベントログ
 - UNIX の場合：シスログ (syslog)
- 接続先のマネージャーホストのサーバ証明書の CN または SAN と、接続先ホスト名が同じであることを確認し、再実行してください。
- 統合トレースログに「一部のルート証明書の読み込みに失敗しました」が出力されているか確認してください。出力されている場合は、メッセージの対処方法に従って対処してください。
- 接続先ホストのサーバ証明書に対応するルート証明書がマネージャーホストに配置されているか確認してください。配置されていない場合は、配置してください。
- 接続先ホストのサーバ証明書が有効期間内かどうか確認してください。有効期間外の場合は、サーバ証明書を更新してください。
- 要因が「システムエラーが発生しました。」の場合は、資料採取ツールで資料を採取し、システム管理者に連絡してください。

IM 構成同期実行時に警告メッセージが出力される場合

- 「KNAN29097-W IM 構成管理サービスの通信暗号化機能で使用するルート証明書が有効期間外です。(ファイル名:ファイル名)」メッセージが出力される。

要因

次の要因が考えられます。

- 通信暗号化機能で使用するルート証明書が有効期間外です。

対処

要因に従って対処してください。

- ルート証明書が有効期間外の状態で運用することに問題があるか確認してください。問題がある場合は、システム管理者に連絡し、ルート証明書を更新してください。

(59) 通信暗号化機能が有効の JP1/IM - View で、エラーが表示される場合の対処方法

メッセージの種類によって対処方法が異なります。

ログインできない場合

- 「KAVB1958-E JP1/IM - View の通信暗号化機能の初期化処理でエラーが発生しました。(要因: 要因, ディレクトリ名:ディレクトリ名)」メッセージが出力される。
- 「KAVB6601-E JP1/IM - View の通信暗号化機能の初期化処理でエラーが発生しました。(要因: 要因, ディレクトリ名:ディレクトリ名)」メッセージが出力される。
- 「KNAN20121-E IM 構成管理・ビューアーの通信暗号化機能の初期化処理でエラーが発生しました。(要因:要因, ディレクトリ名:ディレクトリ名)」メッセージが出力される。
- 「KNAN20141-E 拠点マネージャーの IM 構成管理・ビューアーの通信暗号化機能の初期化処理でエラーが発生しました。(要因:要因, ディレクトリ名:ディレクトリ名)」メッセージが出力される。

要因

次の要因が考えられます。

- ルート証明書ファイルが 1 個も見つかりません。
- すべてのルート証明書ファイルが読み込めません。
- ルート証明書の配置先ディレクトリがありません。

対処

要因に従って対処してください。

- 要因が「ルート証明書が 1 個も見つかりません。」の場合は、次の確認をしてから再ログインしてください。

ルート証明書があるか確認してください。ルート証明書がある場合は読み込み権限があるか確認してください。読み込み権限がない場合は、ルート証明書に読み込み権限を設定してください。ルート証明書がない場合はルート証明書を配置してください。

- 要因が「すべてのルート証明書が読み込めません。」の場合は、次の確認をしてから再ログインしてください。

- ・ルート証明書があるか確認してください。ルート証明書がある場合は読み込み権限があるか確認してください。読み込み権限がない場合は、ルート証明書に読み込み権限を設定してください。
- ・ルート証明書のファイルに問題がないことを確認してください。
- ・Windows イベントログを確認し、ファイルディスクリプタなどの OS のリソース不足がほかに発生していないかを確認してください。
- ・要因が「ルート証明書の配置先ディレクトリがありません。」の場合は、ルート証明書の配置先ディレクトリを作成してルート証明書を配置してください。

マネージャーへの接続が失敗する場合

- ・「KAVB1959-E JP1/IM - View の通信暗号化機能で暗号化通信に失敗しました。(接続先ホスト名:接続先ホスト名, 要因:要因)」メッセージが出力される。
- ・「KAVB6602-E JP1/IM - View の通信暗号化機能で暗号化通信に失敗しました。(接続先ホスト名:接続先ホスト名, 要因:要因)」メッセージが出力される。
- ・「KNAN20122-E IM 構成管理・ビューアーの通信暗号化機能で暗号化通信に失敗しました。(接続先ホスト名:接続先ホスト名, 要因:要因)」メッセージが出力される。
- ・「KNAN20142-E 拠点マネージャーの IM 構成管理・ビューアーの通信暗号化機能で暗号化通信に失敗しました。(接続先ホスト名:接続先ホスト名, 要因:要因)」メッセージが出力される。

要因

次の要因が考えられます。

- ・サーバ証明書の CN または SAN と接続先のホスト名が異なります。
- ・通信エラーが発生しました。
- ・システムエラーが発生しました。

対処

要因に従って対処してください。

- ・接続先のマネージャーホストのサーバ証明書の CN, または SAN とビューアーの接続先のホスト名が同じであることを確認し、再ログインしてください。
- ・接続先のマネージャーホストの通信暗号化機能が有効であることを確認してください。有効である場合は、非暗号化通信ホスト設定ファイルに接続先のマネージャーホスト名が記載されていないことを確認してください。
- ・統合トレースログに「一部のルート証明書の読み込みに失敗しました」が出力されているか確認してください。出力されている場合は、メッセージの対処方法に従って対処してください。
- ・接続先のマネージャーホストのサーバ証明書に対応するルート証明書が JP1/IM - View に配置されているか確認してください。配置されていない場合は配置してください。
- ・接続先のマネージャーホストのサーバ証明書が有効期間内かどうか確認してください。有効期間外の場合は、サーバ証明書を更新してください。
- ・要因が「システムエラーが発生しました。」の場合は、資料採取ツールで資料を採取し、システム管理者に連絡してください。

警告メッセージが出力される場合

- 「KAVB1969-W JP1/IM - View の通信暗号化機能で使用する一部のルート証明書の読み込みに失敗しました。(ディレクトリ名:ディレクトリ名, ファイル名:ファイル名, ファイル名, …)」メッセージが出力される。
- 「KAVB1971-W JP1/IM - View の通信暗号化機能で使用するルート証明書が有効期間外です。(ディレクトリ名:ディレクトリ名, ファイル名:ファイル名, ファイル名, …)」メッセージが出力される。
- 「KAVB6603-W JP1/IM - View の通信暗号化機能で使用する一部のルート証明書の読み込みに失敗しました。(ディレクトリ名:ディレクトリ名, ファイル名:ファイル名)」メッセージが出力される。
- 「KNAN20123-W IM 構成管理・ビューアーの通信暗号化機能で使用する一部のルート証明書の読み込みに失敗しました。(ディレクトリ名:ディレクトリ名, ファイル名:ファイル名, ファイル名, …)」メッセージが出力される。
- 「KNAN20124-W IM 構成管理・ビューアーの通信暗号化機能で使用するルート証明書が有効期間外です。(ディレクトリ名:ディレクトリ名, ファイル名:ファイル名, ファイル名, …)」メッセージが出力される。
- 「KNAN20143-W 拠点マネージャーの IM 構成管理・ビューアーの通信暗号化機能で使用する一部のルート証明書の読み込みに失敗しました。(ディレクトリ名:ディレクトリ名, ファイル名:ファイル名, ファイル名, …)」メッセージが出力される。
- 「KNAN20144-W 拠点マネージャーの IM 構成管理・ビューアーの通信暗号化機能で使用するルート証明書が有効期間外です。(ディレクトリ名:ディレクトリ名, ファイル名:ファイル名, ファイル名, …)」メッセージが出力される。

要因

次の要因が考えられます。

- JP1/IM - View の通信暗号化機能で使用する一部のルート証明書の読み込みに失敗しました。
- JP1/IM - View の通信暗号化機能で使用するルート証明書が有効期間外です。

対処

要因に従って対処してください。

- ルート証明書に読み込み権限があるか確認してください。読み込み権限がない場合は、ルート証明書に読み込み権限を設定してください。
- Windows イベントログを確認し、ファイルディスクリプタなどの OS のリソース不足が発生していないかを確認してください。
- ルート証明書のファイルに問題がないことを確認してください。
- ルート証明書を有効期間外の状態で運用することに問題があるか確認してください。問題がある場合は、ルート証明書を更新してください。

IM 構成の同期でリモート監視構成の取得に失敗する場合

次のメッセージが出力された時の通信暗号化機能に関する要因と対処方法を示します。

- 「KNAN21404-E IM 構成の同期に失敗したホストがあります。マニュアルに従って対処を実行したあと、IM 構成の同期を再度実行して下さい」メッセージが出力される。

要因

次の要因が考えられます。

- 接続先のマネージャーにてルート証明書ファイルが見つかりません。
- 接続先のマネージャーにてルート証明書ファイルが読み込めません。
- 拠点マネージャーのサーバ証明書の CN または SAN と拠点マネージャーのホスト名が異なります。
- 拠点マネージャーのサーバ証明書が有効期間外です。

対処

要因に従って対処してください。

- ルート証明書がない場合はルート証明書を配置して、JP1/Base にルート証明書の配置場所を設定してください。
- ルート証明書に読み込み権限があるか確認してください。読み込み権限がない場合は、ルート証明書に読み込み権限を設定してください。
- ルート証明書のファイルに問題がないことを確認してください。
- 次の OS のログを確認し、ファイルディスクリプタなどの OS のリソース不足がほかに発生していないかを確認してください。
 - ・ Windows の場合：Windows イベントログ
 - ・ UNIX の場合：シスログ (syslog)
- 拠点マネージャーのサーバ証明書の CN または SAN と、拠点マネージャーのホスト名が同じであることを確認してください。
- 接続先マネージャーの統合トレースログに「一部のルート証明書の読み込みに失敗しました」が出力されているか確認してください。出力されている場合は、メッセージの対処方法に従って対処してください。
- 拠点マネージャーのサーバ証明書に対応するルート証明書が接続先のマネージャーに配置されているか確認してください。配置されていない場合は、配置して、JP1/Base にルート証明書の配置場所を設定してください。
- 拠点マネージャーのサーバ証明書が有効期間内かどうか確認してください。有効期間外の場合は、サーバ証明書を更新してください。

(60) 拡張リカバリーに失敗した場合の対処手順

IM データベースのログを確認し、KFPL15308-E メッセージが出力されているかどうか確認してください。

IM データベースのログは次の手順で確認してください。

- Windows の場合

1. 次のコマンドを実行して環境変数を設定する。

```
set PDDIR=<IM データベースサービスのインストールディレクトリ>%JM< n>
set PDUXPLDIR=%PDDIR%\UXPLDIR
```

2. 次のコマンドを実行して IM データベースのログを表示する。

```
<IM データベースサービスのインストールディレクトリ>%JM< n>%bin%pdcat
```

• Linux の場合

1. 次のコマンドを実行して環境変数を設定する。

```
export PDDIR=<IM データベースサービスのインストールディレクトリ>/JM< n>
export LD_LIBRARY_PATH=$PDDIR/lib/:$LD_LIBRARY_PATH
```

2. 次のコマンドを実行して IM データベースのログを表示する。

```
$PDDIR/bin/pdcat
```

<IM データベースサービスのインストールディレクトリ>:

セットアップ情報ファイルの項目「IMBENVDIR」に指定したパス

<n>:

物理ホストの場合「0」、論理ホストの場合、クラスタセットアップ情報ファイルでLOGICALHOSTNUMBERに指定した値

IM データベースのログに KFPL15308-E メッセージが出力されている場合、バックアップファイル取得時のテーブルスキーマと、IM データベースサービスのテーブルスキーマを同一にする必要があります。

jimdbupdate コマンドを実行して、IM データベースをアップデートする必要があるか確認し、次の手順でリカバリーしてください。

IM データベースが最新であることを示す KNAN11201-I が表示された場合:

1. 統合監視 DB をアンセットアップする。
2. Windows の場合、OS を再起動する。
3. [-v] オプションを指定して、jicodbsetup コマンドを実行する。
4. 拡張リカバリーに失敗したバックアップファイルと [-m EXPAND] オプションを指定して、jimdbrecovery コマンドを実行する。
5. データベースのテーブルスキーマをアップデートする。
[-i] オプションを指定して、jimdbupdate コマンドを実行します。

IM データベースが最新であることを示す KNAN11201-I が表示されなかった場合:

1. データベースのテーブルスキーマをアップデートする。
[-i] オプションを指定して、jimdbupdate コマンドを実行します。
2. 拡張リカバリーに失敗したバックアップファイルと [-m EXPAND] オプションを指定して、jimdbrecovery コマンドを実行する。

KFPL15308-E メッセージが出力されていない場合、次の内容を確認し、jimbrecovey コマンドを再実行してください。

- 同じ OS で取得したバックアップファイルを指定しているか。
- バックアップ取得時と同じ DB 構成か。
- 現在の IM データベースがバックアップ取得時より小さいサイズでないか。
- IM データベースを再セットアップしたあとにリカバリーしているか。
- IM データベースのインストールディレクトリに十分な空き容量があるか。DB サイズが S のときに 1 ギガバイト、M のときに 1 ギガバイト、L のときに 4 ギガバイト程度必要です。

(61) セントラルコンソール・ビューアーまたはセントラルスコープ・ビューアーのログがラップして現象発生時のログが採取できなかった場合のログの拡張手段

JP1/IM - View がインストールされているマシン上で、次の共通定義情報を任意のファイルに記述し、jbssetcnf コマンドで適用することで、セントラルコンソール・ビューアーまたはセントラルスコープ・ビューアーのプロセス別トレースログを拡張できます。

形式

```
[JP1_DEFAULT¥JP1CONSOLEVIEW¥LOG_CONTROL¥VIEW]
"LOGFILENUM"=dword:16進数値
"LOGSIZE"=dword:16進数値
"JP1COVIEW_LOGNUM"= dword:16進数値
"JP1COVIEW_LOGSIZE"= dword:16進数値
"JP1COVIEW_APILOGNUM"= dword:16進数値
"JP1COVIEW_APILOGSIZE"= dword:16進数値
[JP1_DEFAULT¥JP1CONSOLEVIEW]
"JP1COVIEW_LOGSIZE"=dword:16進数値
"JP1COVIEW_APILOGSIZE"=dword:16進数値
```

設定値は、同時接続する JP1/IM - View の台数に合わせて、各プロセス別トレースログの最大ディスク占有量（最大サイズ数×面数）がデフォルト値×同時接続台数となるように見積もってください。

このとき、追加したサイズ分のディスク空き容量が必要となります。

記述内容

次の値を記述します。

```
[JP1_DEFAULT¥JP1CONSOLEVIEW¥LOG_CONTROL¥VIEW]
```

JP1/IM - View の環境設定のキー名称であり、固定です。

```
"LOGFILENUM"=dword:16 進数値
```

プロセス別トレースログのうちVIEWn. log の面数を指定します。

1~16 の 16 進数で指定します。デフォルト値は「dword:00000003」（3 面）です。

"LOGSIZE"=dword:16 進数値

プロセス別トレースログのうちVIEWn.log (1 ファイル) の最大サイズ値を指定します。
4,096~2,147,483,647 バイトの 16 進数で指定します。単位はバイトです。デフォルト値は「dword:00A00000」(10,485,760 バイト (10MB)) です。

"JP1COVIEW_LOGNUM"= dword:16 進数値

プロセス別トレースログのうちjp1convn.log の面数を指定します。
2~100 の 16 進数で指定します。デフォルト値は「dword:00000008」(8 面) です。

"JP1COVIEW_LOGSIZE"= dword:16 進数値

プロセス別トレースログのうちjp1convn.log (1 ファイル) の最大サイズ値を指定します。
4,096~104,857,600 バイトの 16 進数で指定します。単位はバイトです。デフォルト値は「dword:00500000」(5,242,880 バイト (5MB)) です。

"JP1COVIEW_APILOGNUM"= dword:16 進数値

プロセス別トレースログのうちjp1convMn.log の面数を指定します。
2~100 の 16 進数で指定します。デフォルト値は「dword:0000003C」(60 面) です。

"JP1COVIEW_APILOGSIZE"= dword:16 進数値

プロセス別トレースログのうちjp1convMn.log (1 ファイル) の最大サイズ値を指定します。
4,096~104,857,600 バイトの 16 進数で指定します。単位はバイトです。
デフォルト値は「dword:00500000」(5,242,880 バイト (5MB)) です。

[JP1_DEFAULT¥JP1CONSOLEVIEW]

JP1/IM - View の環境設定のキー名称であり、固定です。

"JP1COVIEW_LOGSIZE"=dword:16 進数値

プロセス別トレースログのうちjp1csov[_old].log の最大サイズ値を設定します。
512~2,097,152KB の 16 進数で指定します。デフォルト値は「dword:00300000」(3,145,728 バイト (3MB)) です。

"JP1COVIEW_APILOGSIZE"=dword:16 進数値

プロセス別トレースログのうちjp1csovM[_old].log の最大サイズ値を設定します。
512~2,097,152KB の 16 進数で指定します。デフォルト値は「dword:00600000」(6,291,456 バイト (6MB)) です。

拡張手順

プロセス別トレースログの拡張手順を次に示します。

1. リモートデスクトップ接続を含めて、ログの拡張を実施するホスト上で起動している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、および監視ツリー編集ビューアーをすべて終了する。
2. 「システムドライブ:¥ProgramData¥Hitachi¥jp1¥jp1_default¥JP1CoView¥log¥mmap」フォルダ以下を確認し、VIEW.mm ファイルがある場合は、手動でファイルを削除する。
3. 共通定義情報を設定した任意のファイルをjbssetcnf コマンドで適用する。

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。

(62) IM 構成管理・ビューアーのログがラップして現象発生時のログが採取できなかった場合のログの拡張手段

JP1/IM - View がインストールされているマシン上で、次のファイルを設定して JP1/IM - View を再起動すると、IM 構成管理・ビューアーのプロセス別トレースログを拡張できます。

- IM 構成管理・ビューアーのプロセス別ログ設定定義ファイル (jcfview_reg.conf)

ファイル名

jcfview_reg.conf (IM 構成管理・ビューアーのプロセス別ログ設定定義ファイル)

格納先ディレクトリ

View パス¥conf¥jcfview¥

形式

```
"TRACELEVEL"=dword:00000028
"SHMTHRESHOLD"=dword:0000001E
"FILETHRESHOLD"=dword:00000000
"LOGFILENUM"=dword:16進数値
"LOGSIZE"=dword:16進数値
```

設定値は、同時接続する JP1/IM - View の台数に合わせて、各プロセス別トレースログの最大ディスク占有量（最大サイズ数×面数）がデフォルト値×同時接続台数となるように見積もってください。

このとき、追加したサイズ分のディスク空き容量が必要となります。

記述内容

次の値を記述します。

"TRACELEVEL"=dword:00000028

このパラメーターは固定です。変更しないでください。

"SHMTHRESHOLD"=dword:0000001E

このパラメーターは固定です。変更しないでください。

"FILETHRESHOLD"=dword:00000000

このパラメーターは固定です。変更しないでください。

"LOGFILENUM"=dword:16 進数値

プロセス別トレースログのうちVIEWn. log の最大面数の値を設定します。

1~64 の 16 進数で指定します。デフォルト値は「dword:00000003」（3 面）です。

"LOGSIZE"=dword:16 進数値

プロセス別トレースログのうちVIEWn. log の最大サイズの値を設定します。

4,096~16,777,216 の 16 進数で指定します。デフォルト値は「dword:00A00000」（10,485,760 バイト（10MB））です。

拡張手順

- プロセス別トレースログの拡張手順を次に示します。
1. リモートデスクトップ接続を含めて、ログの拡張を実施するホスト上で起動している IM 構成管理・ビューアーをすべて終了する。
 2. 「システムドライブ:¥ProgramData¥Hitachi¥jp1¥jp1_default¥JP1CoView¥log¥jcfview¥mmap」フォルダ以下を確認し、VIEW.mm ファイルがある場合は、手動でファイルを削除する。
 3. IM 構成管理・ビューアーのプロセス別ログ設定定義ファイル（jcfview_reg.conf）のログ拡張に必要なパラメーターの値を設定する。

(63) 自動アクションが実行されない場合の対処方法

要因

次の要因が考えられます。

- 共通除外条件によって、取得した JP1 イベントが自動アクションの実行対象外になっている。
- 自動アクション定義が無効になっている。
- 自動アクション定義のアクションを実行する条件が取得した JP1 イベントに一致していない。

対処

要因に従って対処してください。

- 拡張モードの共通除外条件を使用している場合、共通除外履歴ファイルを参照し、共通除外条件によって JP1 イベントが自動アクションの実行対象外にされていないかを確認してください。JP1 イベントが除外されている場合は、共通除外条件を見直してください。
- 自動アクション定義が無効になっていないかを確認してください。
- 自動アクション定義のアクションを実行する条件を見直してください。

(64) JP1/IM - View が起動しない場合の対処方法

JP1/IM - View では起動時に Java ヒープ領域として連続したメモリー領域を確保します。上記領域を確保するには連続した領域が必要ですが、ご使用の環境のメモリーの状態により、Java ヒープ領域の確保に失敗し、JP1/IM - View が起動しない場合があります。

JP1/IM - View が起動を試みても [ログイン] 画面が表示されない場合は、以下の対処を実施してください。

対処

1. JP1/IM - View インストールフォルダ¥conf¥jcoview.conf をワークフォルダにコピーし、バックアップを取得してください。

2. JP1/IM - View インストールフォルダ¥conf¥jcoview.conf をテキストエディターで開き, "-Xmx"オプションを現在設定されている値から 100 減算した値へ変更してください。

変更前

[JavaVM]

```
Options=-Xms32m -Xmx768m -Dsun.java2d.noddraw=true
```

変更後

[JavaVM]

```
Options=-Xms32m -Xmx668m -Dsun.java2d.noddraw=true
```

3. JP1/IM - View を起動してください。

4. JP1/IM - View が起動できた場合は, 手順 5.に進んでください。

JP1/IM - View が起動できなかった場合は, 手順 2.により"-Xmx"オプションの指定値を更に 100 減算し, 手順 3.を実施してください。

JP1/IM - View が起動できるまで, 手順 2., 3.を繰り返し実施してください。

5. JP1/IM - View を終了してください。

6. JP1/IM - View インストールフォルダ¥conf¥jcoview.conf をテキストエディターで開き, "-Xmx"オプションに指定されている値に 12 加算した値を"-Xmx"オプションに指定してください。

7. JP1/IM - View を起動してください。

8. JP1/IM - View が起動できた場合は, 手順 5.~6.により"-Xmx"オプションの指定値を更に 12 加算し, 手順 7.を実施してください。

JP1/IM - View が起動できなくなるまで, 手順 5.~7.を繰り返し実施してください。

JP1/IM - View が起動できなかった場合は, 前回起動できた"-Xmx"オプションの値に戻してください。

前回起動できた"-Xmx"オプションの値が, ご使用の環境で JP1/IM - View が確保可能な Java ヒープ領域の最大値となります。

(65) IM 構成管理でホスト情報の収集に成功したが, プロファイルの収集で失敗した場合の対処方法

「KNAN22403-E プロファイル一覧の取得に失敗しました。(詳細情報: 通信エラーが発生しました)」のメッセージが出力される。

要因 1

ファイアウォールによりプロファイル収集のための通信が遮断されています。

対処 1

jp1bscom サービスが通信できる設定になっているかを確認し, jp1bscom サービスが通信できる設定をしてください。

詳細については, マニュアル「JP1/Base 運用ガイド」の JP1/Base のポート番号, ファイアウォールの通過方向についての記載を参照してください。

要因 2

次に示す運用の場合に、エージェントホストからマネージャーホストへの通信（張り返し通信）に失敗します。

- ネットワークを分離した環境で、JP1/Base を IP バインド方式で運用する場合（`physical_ipany.conf` または `logical_ipany.conf` を適用する場合）
- マネージャーとエージェントのホスト間でアドレス変換（NAT）をする場合

対処 2

IM 構成管理での張り返し通信で名前解決をする方式に設定していない場合

名前解決をする方式に設定してください。

詳細については、マニュアル「JP1/Base 運用ガイド」の IM 構成管理での張り返し通信方式の設定についての記載を参照してください。

IM 構成管理での張り返し通信で名前解決をする方式に設定している場合

エージェントホストでマネージャーホスト名の名前解決ができるか確認し、名前解決ができるように設定してください。また、エージェントホストで名前解決されたマネージャーホストの IP アドレスが、マネージャーホストの JP1/Base がバインドしている IP アドレスに一致しているか確認し、一致するように設定してください。

詳細については、マニュアル「JP1/Base 運用ガイド」の IM 構成管理での張り返し通信方式の設定についての記載を参照してください。

(66) 連携した JP1/AJS の構成が統合オペレーション・ビューアーに表示されない場合の対処方法

JP1/IM - Manager（インテリジェント統合管理基盤）と連携した JP1/AJS の構成が統合オペレーション・ビューアーに表示されない場合は、次の対処を実施してください。

要因

アダプタコマンド設定ファイルの `cmdpath` 属性に、存在しないファイルを指定している。

対処

アダプタコマンド設定ファイルの `cmdpath` 属性の設定を見直してください。

`cmdpath` 属性の詳細については、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。

(67) jimdbupdate コマンドを実行すると KNAN11199-E メッセージが出力される、または jimdbupdate コマンド実行後に IM データベースを起動できない場合の対処方法

`jimdbupdate` コマンドを実行すると「KNAN11199-E IM データベースサービスのアップデートに失敗しました」メッセージが出力される、または `jimdbupdate` コマンド実行後に IM データベースを起動できない場合は、次の対処を実施してください。

要因

テキストエディターで次のファイルを開き、14行目の記載を確認してください。

Windows の場合

- 物理ホスト
セットアップ情報ファイルの IMDBENVDIR の値¥JM0¥CONF¥pdsys
- 論理ホスト
クラスタセットアップ情報ファイルの IMDBENVDIR の値¥JM<n>※¥CONF¥pdsysn: クラスタ情報セットアップファイルの LOGICALHOSTNUMBER の値

注※ <n>はクラスタ情報セットアップファイルのLOGICALHOSTNUMBER の値

UNIX の場合

- 物理ホスト
セットアップ情報ファイルの IMDBENVDIR の値/JM0/conf/pdsys
- 論理ホスト
クラスタセットアップ情報ファイルの IMDBENVDIR の値/JM<n>※/conf/pdsys

注※ <n>はクラスタ情報セットアップファイルのLOGICALHOSTNUMBER の値

14行目の記載が「set pd_max_users = 96」である場合、次の要因が考えられます。

- jimdbupdate コマンドが下記メッセージを出力し終了した後に、jimdbupdate コマンドを再実行した、または IM データベースを起動した。
KNAN11034-E IM データベースサービスの停止に失敗しました
KNAN11199-E IM データベースサービスのアップデートに失敗しました
- マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」に記載の IM データベースの更新手順と異なる手順を実施した。

対処

Windows の場合

物理ホストで発生した場合、次の対処を実施してください。実施後の jimdbupdate コマンドの再実行は不要です。

1. jimdbstop コマンドを実行し、IM データベースを停止します。

```
jimdbstop -f
```

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
```

```
KNAN11046-E 「JP1/IM3-Manager DB Server」 サービスが起動していません
```

2. テキストエディターで次のファイルを開きます。

セットアップ情報ファイルの IMDBENVDIR の値¥JM0¥CONF¥pdsys

3. 手順 2 で開いたファイルの 14 行目 (set pd_max_users) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 96
```

(変更後)

```
set pd_max_users = 32
```

4. JP1/IM3-Manager DB Server サービスを起動します。

5. 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します。

```
jimdbstatus
```

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。

6. JP1/IM3-Manager DB Server サービスを停止します。

7. テキストエディターで、手順 2 で開いたファイルを再び開きます。

8. 手順 7 で開いたファイルの 14 行目 (set pd_max_users) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 32
```

(変更後)

```
set pd_max_users = 96
```

9. JP1/IM3-Manager DB Server サービスを起動します。

10. JP1/IM3-Manager サービスを起動します。

クラスタ環境で発生した場合、次の対処を実施してください。実施後の jimdbupdate コマンドの再実行は不要です。

1. クラスタソフトで次のサービスをオフラインにし、実行系、待機系ともに次のサービスが停止した状態であることを確認します。起動している場合は停止します。

- ・ 論理ホストの JP1/IM3-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/IM3-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)

2. 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します。

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. 実行系ホストで jimdbstop コマンドを実行し、IM データベースを停止します。

```
jimdbstop -f -h 論理ホスト名
```

次のどちら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
```

4. 実行系ホストで、テキストエディターで次のファイルを開きます。

```
クラスタセットアップ情報ファイルの IMDBENVDIR の値¥JM<n>※¥CONF¥pdsys
```

注※ <n>はクラスタ情報セットアップファイルのLOGICALHOSTNUMBER の値

5. 手順 4 で開いたファイルの 14 行目 (set pd_max_users) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 96
```

(変更後)

```
set pd_max_users = 32
```

6. 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します。

論理ホストの JP1/IM3-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)

7. 実行系ホストで 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します。

```
jimdbstatus -h 論理ホスト名
```

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。

8. 実行系ホストで jimdbstop コマンドを実行し、IM データベースを停止します。

```
jimdbstop -h 論理ホスト名
```

KNAN11186-I 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
```

9. 実行系ホストで OS のサービス画面から次の順でサービスを停止します。

- ・ 論理ホストの JP1/IM3-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)

10. 実行系ホストで、手順 4 で開いたファイルをテキストエディターで再び開きます。

11. 手順 10 で開いたファイルの 14 行目 (set pd_max_users) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 32
```

(変更後)

```
set pd_max_users = 96
```

12. 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します。

13. 待機系ホストで OS のサービス画面から次のサービスを起動します。

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)

14. 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します。

```
jimdbstop -h 論理ホスト名
```

次のどちら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
```

15. 待機系ホストで OS のサービス画面から次のサービスを起動します。

論理ホストの JP1/IM3-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)

サービスの起動に成功した場合は、OS のサービス画面から次の順でサービスを停止した後、手順 24 以降を実施してください。

- ・ 論理ホストの JP1/IM3-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)

サービスの起動に失敗した場合は、手順 16 以降を実施してください。

16. 待機系ホストで、テキストエディターで次のファイルを開きます。

クラスタセットアップ情報ファイルの `IMDBENVDIR` の値 `¥JM<n>*` `¥CONF¥pdsys`

注※ `<n>` はクラスタ情報セットアップファイルの `LOGICALHOSTNUMBER` の値

17. 手順 16 で開いたファイルの 14 行目 (`set pd_max_users`) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 96
```

(変更後)

```
set pd_max_users = 32
```

18. 待機系ホストで OS のサービス画面から次のサービスを起動します。

論理ホストの JP1/IM3-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)

19. 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します。

```
jimdbstatus -h 論理ホスト名
```

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。

20. 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します。

```
jimdbstop -h 論理ホスト名
```

KNAN11186-I 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

21. 待機系ホストで OS のサービス画面から次の順でサービスを停止します。

- ・ 論理ホストの JP1/IM3-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)

22. 待機系ホストで、手順 16 で開いたファイルをテキストエディターで再び開きます。

23. 手順 22 で開いたファイルの 14 行目 (`set pd_max_users`) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 32
```

(変更後)

```
set pd_max_users = 96
```

24. 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します。

25. 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します。

- ・ 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/IM3-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/IM3-Manager サービス (サービス表示名: JP1/IM3-Manager_論理ホスト名)

UNIX の場合

物理ホストで発生した場合、次の対処を実施してください。実施後の `jimdbupdate` コマンドの再実行は不要です。

1. `jimdbstop` コマンドを実行し、IM データベースを停止します。

```
jimdbstop -f
```

次のどちら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

2. テキストエディターで次のファイルを開きます。

セットアップ情報ファイルの `IMDBENVDIR` の値/`JM0/conf/pdsys`

3. 手順 2 で開いたファイルの 14 行目 (`set pd_max_users`) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 96
```

(変更後)

```
set pd_max_users = 32
```

4. `/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します。

```
jimdbstart
```

5. `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します。

```
jimdbstatus
```

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。

6. `jimdbstop` コマンドを実行し、IM データベースを停止します。

```
jimdbstop
```

KNAN11186-I 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

7. テキストエディターで、手順 2 で開いたファイルを再び開きます。

8. 手順 7 で開いたファイルの 14 行目 (`set pd_max_users`) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 32
```

(変更後)

```
set pd_max_users = 96
```

9. JP1/IM - Manager を起動します。

クラスタ環境で発生した場合、次の対処を実施してください。実施後の `jimdbupdate` コマンドの再実行は不要です。

1. 実行系ホストで論理ホストの JP1/IM - Manager が停止した状態であることを確認します。起動している場合は停止します。
2. 実行系ホストで `jimdbstop` コマンドを実行し、IM データベースを停止します。

```
jimdbstop -f -h 論理ホスト名
```

次のどちら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
```

3. 実行系ホストで、テキストエディターで次のファイルを開きます。

```
クラスタセットアップ情報ファイルの IMDBENVDIR の値/JM<n>*/conf/pdsys
```

注※ <n>はクラスタ情報セットアップファイルのLOGICALHOSTNUMBER の値

4. 手順 3 で開いたファイルの 14 行目 (set pd_max_users) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 96
```

(変更後)

```
set pd_max_users = 32
```

5. 実行系ホストで/opt/jp1imm/bin/imdb にあるjimdbstart コマンドを実行し、IM データベースを起動します。

```
jimdbstart -h 論理ホスト名
```

6. 実行系ホストで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します。

```
jimdbstatus -h 論理ホスト名
```

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。

7. 実行系ホストでjimdbstop コマンドを実行し、IM データベースを停止します。

```
jimdbstop -f -h 論理ホスト名
```

KNAN11186-I 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
```

8. 実行系ホストで、手順 3 で開いたファイルをテキストエディターで再び開きます。

9. 手順 8 で開いたファイルの 14 行目 (set pd_max_users) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 32
```

(変更後)

```
set pd_max_users = 96
```

10. 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します。

11. 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します。

```
jimdbstop -f -h 論理ホスト名
```

次のどちら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
```

12. 待機系ホストで `/opt/jp1imm/bin/imdb` にある `jimdbstart` コマンドを実行します。

```
jimdbstart -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 を再度実施し IM データベースを停止した後、手順 20 以降を実行してください。

```
KNAN11180-I IM データベースサービスの起動処理は正常に終了しました
```

・次のメッセージが出力された場合は、手順 13 以降を実行してください。

```
KNAN11035-E IM データベースサービスの起動に失敗しました
```

13. 待機系ホストで、テキストエディターで次のファイルを開きます。

クラスタセットアップ情報ファイルの `IMDBENVDIR` の値 `/JM<n>*/conf/pdsys`

注※ <n>はクラスタ情報セットアップファイルの `LOGICALHOSTNUMBER` の値

14. 手順 13 で開いたファイルの 14 行目 (`set pd_max_users`) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 96
```

(変更後)

```
set pd_max_users = 32
```

15. 待機系ホストで `/opt/jp1imm/bin/imdb` にある `jimdbstart` コマンドを実行し、IM データベースを起動します。

```
jimdbstart -h 論理ホスト名
```

16. 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します。

```
jimdbstatus -h 論理ホスト名
```

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。

17. 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します。

```
jimdbstop -f -h 論理ホスト名
```

`KNAN11186-I` 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
```

18. 待機系ホストで、手順 13 で開いたファイルをテキストエディターで再び開きます。

19. 手順 18 で開いたファイルの 14 行目 (set pd_max_users) の値を以下のように変更して、保存します。

(変更前)

```
set pd_max_users = 32
```

(変更後)

```
set pd_max_users = 96
```

20. 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します。

21. 実行系ホストでクラスタソフトから論理ホストの JP1/IM - Manager を起動します。

(68) ユーザー作成プラグインで__configurationGet メソッドが実行されない場合の対象方法

ユーザー作成プラグインで__configurationGet メソッドが実行されない場合は、アダプタコマンド設定ファイルの文字コードが ASCII で保存されているかどうか確認してください。

アダプタコマンド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「7.3.2 アダプタコマンド設定ファイル」を参照してください。

(69) jimdbupdate コマンドによる IM データベースの更新に失敗し、KNAN11215-E メッセージが出力された場合の対処方法

「KNAN11215-E IM データベースサービスのアップデートに失敗しました。バージョンアップからやり直してください」のメッセージが出力される。

要因

次の要因が考えられます。

- IM データベースの更新の際に、メモリ不足やファイルロックなどの要因でエラーが発生し、IM データベースの更新が失敗したまま不正な状態になっています。

対処

要因に従って対処してください。

- KNAN11215-E メッセージより前にエラーメッセージが出力されている場合、そのメッセージの対処をしてください。対処したあと、次の手順を参考に、JP1/Base, JP1/IM - Manager をバージョンアップ前の状態に復元し、バージョンアップからやり直してください。バージョンアップ前の状態への復元には、バージョンアップインストールをする前に取得した JP1/Base, JP1/IM - Manager のバックアップを使用します。

バージョン 12 からバージョン 13 にバージョンアップする場合の手順の例を、次に示します。

手順		説明
1	JP1/IM - Manager (バージョン 13) のアンインストール	IM データベースを手動アンインストールします。*1
2		JP1/IM - Manager をアンインストールします。
3	JP1/Base (バージョン 13) のアンインストール	JP1/Base のバージョン 13 へのバージョンアップ後に設定変更を行っている場合は、バックアップを取得します。
4		JP1/Base をアンインストールします。*1
5	JP1/Base (バージョン 12) のインストールと復元	バージョンアップ前のバージョンの JP1/Base をインストールします。*1*2
6		JP1/Base の設定情報およびイベント DB を復元します。*2
7	JP1/IM - Manager (バージョン 12) のインストールと復元	バージョンアップ前のバージョンの JP1/IM - Manager をインストールします。
8		バージョンアップ前に取得したバックアップファイルを使用して、JP1/IM - Manager の設定情報をリカバリーします。
9		IM データベースをセットアップします。
10		バージョンアップ前に取得したバックアップファイルを使用して、IM データベースをリカバリーします。
11	JP1/Base のバージョンアップ (バージョン 12 からバージョン 13 へ) と復元	JP1/Base のバージョンアップを実施します。*2
12		手順 3 でバックアップを取得している場合は、それを使用してリカバリーします。
13	JP1/IM - Manager のバージョンアップ (バージョン 12 からバージョン 13 へ)	JP1/IM - Manager のバージョンアップを実施します。
14		jimdbupdate コマンドを実行し IM データベースを更新します。

注※1

OS 再起動を含みます。

注※2

JP1/AJS など、JP1/Base を前提とする製品がインストールされている場合は、それらの製品についても同様の対応が必要です。

また、アンインストールは上位製品から先に実施し、インストールやバージョンアップは JP1/Base から先に実施します。

(70) 統合オペレーション・ビューアーのツリーに監視対象の IM 管理ノードが表示されない、トレンド表示でパフォーマンスデータが表示されない、または一部が欠落している

項番	主な要因	対処方法
1	Prometheus server が停止しているため、スクレイプが行われない。	Prometheus server を起動してください。
2	Exporter が停止しているため、スクレイプが失敗している。	Exporter を起動してください。

項番	主な要因	対処方法
3	Prometheus server と JP1/IM - Manager (インテリジェント統合管理基盤) のホスト間で通信障害が発生しているため、パフォーマンスデータを送信できない。	通信障害を解決してください。
4	監視対象ホストのシステム時刻を過去に戻した。	監視対象ホストのシステム時刻が変更前の時刻に戻るまで待ってください。
5	Prometheus server のスクレイプ間隔をデフォルトの 1m から変更したあと、メトリック定義ファイルの PromQL 文の値を変更していない。	Prometheus server のスクレイプ間隔を初期値 (1m) から変更した場合、メトリック定義ファイルの PromQL 文に range Vector 型で指定している「さかのぼる時刻」の値 (大括弧 [] で指定する値) を見直す必要があります。スクレイプ間隔の 2 倍以上の値を指定してください。
6	IM 管理ノードのラベル名 (jp1_pc_nodelabel の値) に設定される文字列の長さが上限を超えている。上限は、URL エンコードしたときの文字列が 234 バイト (すべてマルチバイト文字の場合、26 文字) である。	マニュアル「JP1/Integrated Management - Manager 構築ガイド」の「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)」に記載する設定手順 (Linux の場合も同じです) で、jp1_pc_nodelabel の値が上限を超えないように設定してください。

(71) 統合オペレーション・ビューアーに JP1 イベントが通知されない

項番	主な要因	対処方法
1	Prometheus server が停止しているため、スクレイプが行われない。	Prometheus server を起動してください。
2	Exporter が停止しているため、スクレイプが失敗している。	Exporter を起動してください。
3	Alertmanager が停止しているため、通知が行われない。	Alertmanager を起動してください。
4	Alertmanager と JP1/IM - Manager (インテリジェント統合管理基盤) のホスト間で通信障害が発生しているため、JP1 イベントを通知できない。	通信障害を解決してください。

(72) JP1/IM - Agent の停止が通知された (JP1/IM - Agent のプロセスを監視している場合)

項番	主な要因	対処方法
1	監視している JP1/IM - Agent のプロセスが停止した。	JP1/IM - Agent のプロセスを起動してください。

(73) Yet another cloudwatch exporter の IM 管理ノードが作成されない

項番	主な要因	対処方法
1	CloudWatch でメトリックが表示されていない。	インスタンスを起動させるなど (EC2 の場合), CloudWatch で, メトリックが確認できるようにする操作を行ってください。
2	リソースに jpl_pc_nodelabel タグを設定していない。	AWS のリソースごとに jpl_pc_nodelabel タグを設定してください。
3	Yet another cloudwatch exporter の設定が誤っている。	<ul style="list-style-type: none">CloudWatch への接続設定が誤っていないか確認してください。type, metrics などの設定項目に指定している値が誤っていないかを確認してください。
4	Yet another cloudwatch exporter をスクレイプしている Prometheus のスクレイプ間隔に 10 分を超える値を設定している。	スクレイプ間隔を 10 分以内に設定してください。
5	JP1/IM - Manager のホストと Yet another cloudwatch exporter のホストのシステム時刻に 10 分以上のずれがある。	システム時刻のずれを是正してください。

(74) Windows 環境で, 統合エージェントのサービスを起動すると, 実行中のステータスになるが, すぐに停止状態のステータスに変化してしまう

項番	主な要因	対処方法
1	統合エージェントのプロセスは, Windows サービス化プロセスとサービスプロセスで構成される。 Windows サービス化プロセスだけが停止し, サービスプロセスが停止していない状態で, 統合エージェントのサービスを起動した場合に, この現象が発生する。	タスクマネージャーで, 次に示す各サービスのプロセスが起動しているか確認してください。片方のプロセスだけが起動している場合は, タスクマネージャーの [タスクの終了] を実行して, プロセスを停止してからサービスを起動してください。 <ul style="list-style-type: none">JP1/IM3-Agent imagent.exe, jpc_imagent_service.exeJP1/IM3-Agent proxy imagentproxy.exe, jpc_imagentproxy_service.exeJP1/IM3-Agent action imagentaction.exe, jpc_imagentaction_service.exeJP1/IM3-Agent Alert forwarder alertmanager.exe, jpc_alertmanager_service.exeJP1/IM3-Agent metric forwarder prometheus.exe, jpc_prometheus_server_service.exeJP1/IM3-Agent Synthetic metric collector

項番	主な要因	対処方法
		blackbox_exporter.exe, jpc_blackbox_exporter_service.exe • JP1/IM3-Agent Windows metric collector windows_exporter.exe, jpc_windows_exporter_service.exe • JP1/IM3-Agent AWS metric collector ya_cloudwatch_exporter.exe jpc_ya_cloudwatch_exporter_service.exe • JP1/IM3-Agent Azure metric collector promitor_scraper.exe jpc_promitor_scraper_service.exe • JP1/IM3-Agent Azure resource discovery promitor_resource_discovery.exe, jpc_promitor_resource_discovery_service.exe • JP1/IM3-Agent Script metric collector script_exporter.exe, jpc_script_exporter_service.exe • JP1/IM3-Agent Log trapper ruby.exe (1 + worker の数), jpc_fluentd_service.exe

(75) Windows 環境で、統合エージェントのサービスを起動または停止したときに、サービス画面のダイアログや net コマンドの標準エラー出力に Error 1067 が通知され、サービスの起動または停止に失敗する

項番	主な要因	対処方法
1	統合エージェントのプロセスは、Windows サービス化プロセスとサービスプロセスで構成される。 Windows サービス化プロセスだけが停止し、サービスプロセスが停止していない状態で、統合エージェントのサービスを起動または停止した場合に、この現象が発生する。	「(74)」と同じです。

(76) サービスが起動しない

項番	主な要因	対処方法
1	定義ファイルが誤っている。	次に示す定義ファイルの書式、設定内容、文字コード、改行コードなどに誤りがないか確認してください。各ファイルの書式については、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」の該当する定義ファイルについて説明している個所を参照してください。

項番	主な要因	対処方法
		<ul style="list-style-type: none"> • Alertmanager <ul style="list-style-type: none"> - Alertmanager 設定ファイル - サービス定義ファイル (Windows の場合) - ユニット定義ファイル (Linux の場合) • Prometheus server <ul style="list-style-type: none"> - Prometheus 設定ファイル* - アラート設定ファイル* - Node exporter のディスカバリ設定ファイル* - Windows exporter のディスカバリ設定ファイル* - Blackbox exporter (HTTP/HTTPS 監視) のディスカバリ設定ファイル* - Blackbox exporter (ICMP 監視) のディスカバリ設定ファイル* - Yet another cloudwatch exporter のディスカバリ設定ファイル* - ユーザー独自のディスカバリ設定ファイル* - サービス定義ファイル (Windows の場合) - ユニット定義ファイル (Linux の場合) • Node exporter <ul style="list-style-type: none"> - ユニット定義ファイル • Windows exporter <ul style="list-style-type: none"> - Windows exporter 設定ファイル - サービス定義ファイル • Blackbox exporter <ul style="list-style-type: none"> - Blackbox exporter 設定ファイル - サービス定義ファイル (Windows の場合) - ユニット定義ファイル (Linux の場合) • Yet another cloudwatch exporter <ul style="list-style-type: none"> - Yet another cloudwatch exporter 設定ファイル - ユニット定義ファイル <p>注※</p> <p>Prometheus server の定義ファイルは、promtool check config コマンドで定義ファイルの検証が行えます。</p>
2	ほかのプロセスが使用しているポートと、JP1/IM - Agent のプロセスが使用するポートが重複している。	<p>JP1/IM - Agent が使用するポートは、ユニット定義ファイル、または、サービス定義ファイルに記載されている次に示すコマンドラインオプションで確認できます。</p> <ul style="list-style-type: none"> • Prometheus server, Alertmanager, Node exporter, Blackbox exporter の場合 <ul style="list-style-type: none"> --web.listen-address=IP アドレス:ポート番号 • Windows exporter の場合

項番	主な要因	対処方法
		<pre>--telemetry.addr=IP アドレス:ポート番号</pre> <ul style="list-style-type: none"> • Yet another cloudwatch exporter <pre>-listen-address=IP アドレス:ポート番号</pre> <p>JP1/IM - Agent のプロセスを停止してから、次に示すコマンドを実行し、上記のコマンドラインオプションに指定されているポートが使用中になっていないか確認します。</p> <ul style="list-style-type: none"> • Windows 環境の場合 netstat -ane • Linux 環境の場合 ss -ant <p>使用中になっている場合は、重複しないようにポートの設定を変更します。ポート番号の設定の変更方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」の「1.21.2 JP1/IM - Agent の設定変更」(Windows の場合) および「2.19.2 JP1/IM - Agent の設定変更」(UNIX の場合) の該当する説明を参照してください。</p>

(77) JP1/IM - Agent のプロセスは稼働しているが、正常に動作しない

項番	主な要因	対処方法
1	ほかのプロセスが使用しているポートと、JP1/IM - Agent のプロセスが使用するポートが重複している。	<p>JP1/IM - Agent が使用するポートは、ユニット定義ファイル、または、サービス定義ファイルに記載されている次に示すコマンドラインオプションで確認できます。</p> <ul style="list-style-type: none"> • Prometheus server, Alertmanager, Node exporter, Blackbox exporter の場合 --web.listen-address=IP アドレス:ポート番号 • Windows exporter の場合 --telemetry.addr=IP アドレス:ポート番号 • Yet another cloudwatch exporter -listen-address=IP アドレス:ポート番号 <p>JP1/IM - Agent のプロセスを停止してから、次に示すコマンドを実行し、上記のコマンドラインオプションに指定されているポートが使用中になっていないか確認します。</p> <ul style="list-style-type: none"> • Windows 環境の場合 netstat -ane • Linux 環境の場合 ss -ant <p>使用中になっている場合は、重複しないようにポートの設定を変更します。ポート番号の設定の変更方法については、マニュアル「JP1/Integrated Management</p>

項番	主な要因	対処方法
		3 - Manager 構築ガイド」(Windows の場合) の「1.21.2 JP1/IM - Agent の設定変更」および「2.19.2 JP1/IM - Agent の設定変更」(UNIX の場合) の該当する説明を参照してください。

(78) JP1/IM - Agent のプロセスの稼働中に、JP1/IM - Agent が提供している REST API を実行すると、レスポンスがなかったり、エラーが返却されたりする

項番	主な要因	対処方法
1	ほかのプロセスが使用しているポートと、JP1/IM - Agent のプロセスが使用するポートが重複している。	<p>JP1/IM - Agent が使用するポートは、ユニット定義ファイル、または、サービス定義ファイルに記載されている次に示すコマンドラインオプションで確認できます。</p> <ul style="list-style-type: none"> Prometheus server, Alertmanager, Node exporter, Blackbox exporter の場合 --web.listen-address=IP アドレス:ポート番号 Windows exporter の場合 --telemetry.addr=IP アドレス:ポート番号 Yet another cloudwatch exporter -listen-address=IP アドレス:ポート番号 <p>JP1/IM - Agent のプロセスを停止してから、次に示すコマンドを実行し、上記のコマンドラインオプションに指定されているポートが使用中になっていないか確認します。</p> <ul style="list-style-type: none"> Windows 環境の場合 netstat -ane Linux 環境の場合 ss -ant <p>使用中になっている場合は、重複しないようにポートの設定を変更します。ポート番号の設定の変更方法については、マニュアル「JP1/Integrated Management 3 - Manager 構築ガイド」(Windows の場合) の「1.21.2 JP1/IM - Agent の設定変更」および「2.19.2 JP1/IM - Agent の設定変更」(UNIX の場合) の該当する説明を参照してください。</p>

(79) blackbox_exporter で正しく監視ができない

項番	主な要因	対処方法
1	次の原因が考えられます。	<p>次のことを確認してください。</p> <ul style="list-style-type: none"> 監視対象が正常に稼働していること

項番	主な要因	対処方法
	<ul style="list-style-type: none"> • ディスカバリ設定ファイル (file_sd_config_blackbox_モジュール名.yml) に存在しないホスト名を指定している。 • ディスカバリ設定ファイル (file_sd_config_blackbox_モジュール名.yml) に指定した監視対象のホストが停止している。 • ディスカバリ設定ファイル (file_sd_config_blackbox_http.yml) に指定した監視対象のサービスが停止している。 • ディスカバリ設定ファイル (file_sd_config_blackbox_http.yml) に誤った URL を指定している。 • Blackbox exporter 設定ファイル (blackbox_exporter.yml) の compression に不正な値を指定している。 • Blackbox exporter 設定ファイル (blackbox_exporter.yml) に指定した認証情報が誤っている。 • Blackbox exporter 設定ファイル (blackbox_exporter.yml) の source_ip_address が誤っている。 • Blackbox exporter 設定ファイル (blackbox_exporter.yml) に指定した証明書が存在しない。 • Blackbox exporter 設定ファイル (blackbox_exporter.yml) に指定した証明書が誤っている。 	<ul style="list-style-type: none"> • file_sd_config_blackbox_モジュール名.yml の記述内容が正しいこと • blackbox_exporter.yml の記述内容が正しいこと <p>上記に問題がない場合は、原因を特定するため、blackbox_exporter の詳細なログを出力して調査する必要があります。次の手順を実施してください。</p> <ol style="list-style-type: none"> 1. blackbox_exporter のログのレベルの設定値を「info」（デフォルト）から「debug」に変更する。ユニット定義ファイル、または、サービス定義ファイルに記述している--log.level を「info」から「debug」に書き換えます。 2. サービスを再起動する。 サービスを再起動すると、ログのレベルの設定変更が有効になります。 3. blackbox_exporter で監視を行い、現象を再現させたあと、blackbox_exporter のログを採取してシステム管理者に問い合わせる。 <p>なお、ログのレベルを「debug」に変更すると、大量にログが出力されるため、ログを採取したあと、ログのレベルを「info」に戻しておく必要があります。</p>

(80) ユーザー独自の Exporter で正しく監視ができない

項番	主な要因	対処方法
1	<p>次の原因が考えられます。</p> <ul style="list-style-type: none"> • ユーザー独自の Exporter に起因する原因 • Prometheus 設定ファイル (jpc_prometheus_server.yml) にユーザー独自の Exporter に関するスクレイプジョブの設定を追加していない、または、設定が誤っている。 • ユーザー独自のディスカバリ設定ファイル (file_sd_config_任意の名前.yml) を作成していない、または、設定が誤っている。 	<p>次のことを確認してください。</p> <ul style="list-style-type: none"> • ユーザー独自の Exporter が正常に動作しているか確認する。curl やブラウザを使用してユーザー独自の Exporter をスクレイプし、正常に情報が取得できることを確認する。正常に情報が取得できない場合は、ユーザー独自の Exporter に問題があると考えられるため、ユーザー独自の Exporter の原因を調査してください。 • ユーザー独自の Exporter の動作に問題がない場合は、Prometheus server からスクレイプができていないことが考えられるため、Prometheus 設定ファイル (jpc_prometheus_server.yml) にスクレイプジョブが定義されているか、ユーザー独自のディスカバリ設定ファイル (file_sd_config_任

項番	主な要因	対処方法
		意の名前.yml) が作成されているかを見直してください。

(81) ログ監視機能で監視したログまたはイベントログが JP1 イベントとして発行されない

項番	主な要因	対処方法
1	次の原因が考えられます。 <ul style="list-style-type: none"> Fluentd の監視定義ファイルが誤っている。 	次に示すファイルについて、書式、設定内容、文字コード、改行コードなどに誤りがないかを確認してください。 <ul style="list-style-type: none"> ログ監視共通定義ファイル (jpc_fluentd_common.conf) ログ監視対象定義ファイル (jpc_fluentd_common_list.conf) 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) Windows イベントログの監視定義ファイル (fluentd_@@trapname@@_wevt.conf.template)

(82) Script exporter のメトリックが取得できない

項番	主な要因	対処方法
1	実行したスクリプトが異常終了した。	Script exporter で実行するスクリプトを修正し、Script exporter を再起動してください。
2	実行権限のないファイルを実行しようとした。	実行するファイルの権限を変更してください。

(83) Promitor のメトリックが取得できない

項番	主な要因	対処方法
1	Resource Discovery が停止している。	Resource Discovery を起動してください。
2	Resource Discovery の設定が誤っている。	type などの指定値が誤っていないか確認してください。
3	Scraper の設定が誤っている。	<ul style="list-style-type: none"> Resource Discovery への接続設定が誤っていないか確認してください。 resourceType や metricName などの指定値が誤っていないか確認してください。

12.5.4 JP1/IM - Agent が JP1/IM - Manager に接続できない場合の対処

(1) JP1/IM - Manager が TLS 有効なのに JP1/IM - Agent が TLS 無効になっている

KNBC20057-W が出力されます。詳細として「received an error response status」が出力されます。

JP1/IM - Agent を TLS 有効にしてください。

(2) JP1/IM - Manager が TLS 無効なのに JP1/IM - Agent が TLS 有効になっている

KNBC20057-W が出力されます。詳細として「http: server gave HTTP response to HTTPS client」が出力されます。

JP1/IM - Agent を TLS 無効にしてください。

(3) 証明書が不正

KNBC20057-W が出力されます。詳細として「x509: certificate signed by unknown authority」が出力されます。

JP1/IM - Agent に正しい証明書を設定してください。

(4) 証明書が有効期限切れ

KNBC20057-W が出力されます。詳細として「x509: certificate has expired or is not yet valid」が出力されます。

JP1/IM - Agent に正しい証明書を設定してください。

(5) 初期シークレットが登録されていない、または、初期シークレットが不正

KNBC20057-W が出力されます。詳細として「認証エラーが発生しました。

(URL のパス:/ima/api/v1/-/healthy)」が出力されます。

JP1/IM - Agent に正しい初期シークレットを設定してください。

索引

B

- BJEX との連携の概要 353
- BJEX と連携するための設定 366
- BJEX の設定 370
- BJEX または JP1/AS と JP1/IM - Manager 間の通信に関する設定 368
- BJEX または JP1/AS との連携 352
- BJEX または JP1/AS との連携の概要 353
- BJEX または JP1/AS と連携するための設定 366
- BJEX または JP1/AS の設定 370
- BJEX または JP1/AS 連携時のコマンド 376
- BJEX または JP1/AS 連携用の JP1/IM の機能 356
- BJEX 連携時のコマンド 376
 - jcoimdef 376
 - jim_log.bat (Windows 限定) 376
 - jim_log.sh (UNIX 限定) 377
- BJEX 連携用の JP1/IM の機能 356

D

- DB の管理 52
 - 再作成 65
 - 再作成 (イベント DB) 67
 - 再作成 (応答待ちイベント滞留ファイル) 70
 - 再作成 (監視オブジェクト DB・ホスト情報 DB) 66
 - 再作成 (コマンド実行履歴) 65
 - サイズ拡張 (IM データベース) 71
 - 再編成 52
 - 再編成 (IM データベース) 52
 - 再編成 (イベント DB) 52
 - 再編成 (インテリジェント統合管理データベース) 54
 - 再編成 (応答待ちイベント滞留ファイル) 52
 - 再編成 (監視オブジェクト DB・ホスト情報 DB) 52
 - 再編成 (コマンド実行履歴) 52
 - バックアップ 54
 - バックアップ (IM データベース) 59

- バックアップ (イベント DB) 58
- バックアップ (インテリジェント統合管理データベース) 62
- バックアップ (応答待ちイベント滞留ファイル) 58
- バックアップ (監視オブジェクト DB) 56
- バックアップ (コマンド実行履歴) 55
- バックアップ (ホスト情報 DB) 57
- ポート変更 (IM データベース) 76
- リカバリー 54
- リカバリー (IM データベース) 59
- リカバリー (イベント DB) 58
- リカバリー (インテリジェント統合管理データベース) 62
- リカバリー (応答待ちイベント滞留ファイル) 58
- リカバリー (監視オブジェクト DB) 56
- リカバリー (コマンド実行履歴) 55
- リカバリー (ホスト情報 DB) 57
- DB の再作成および設定変更 65
- DB のバックアップおよびリカバリー 54

I

- IM 管理ノード状態の監視 167
- IM 構成管理
 - IM 構成管理の管理情報をエクスポート・インポートする 318
 - 仮想化システム構成を管理する 310
 - 業務グループを管理する 312
 - サービスの稼働状況を管理する 315
 - システムの階層構成の管理 306
 - セントラルスコープの監視ツリーへ反映する 311
 - プロファイルを管理する 313
 - ホストを管理する 307
- IM 構成管理で仮想化システム構成の収集に失敗した場合の対処方法 562
- 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 560

IM 構成管理でリモート監視イベントログトラップが稼働しているにもかかわらず JP1 イベントが受信されない場合の対処方法 565

IM 構成管理でリモート監視ログファイルトラップが稼働しているにもかかわらず JP1 イベントが受信されない場合の対処方法 563

IM 構成管理でリモート監視ログファイルトラップのプロファイルの起動に失敗した場合の対処方法 567

IM 構成管理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の有効設定情報が参照できない場合の対処方法 563

IM 構成管理でリモート監視ログファイルトラップを始める前の注意事項 568

IM 構成管理でログファイルトラップ動作定義ファイルの取得に失敗した場合の対処方法 560

IM 構成管理に登録するホスト名と発生元ホスト名が異なってしまう場合の対処方法 572

IM 構成管理の管理情報

 インポートする 322

 エクスポートする 318

IM 構成管理のリモート監視ログファイルトラップで同じ JP1 イベントが重複して受信される場合の対処方法 567

IM 構成管理・ビューアーで、[IM 構成] ページのツリー表示領域がグレー表示される場合の対処方法 566

IM 構成管理・ビューアーで、[ホスト登録]、[エージェント構成編集]などのメニュー項目が非活性になっている場合の対処方法 562

IM 構成管理・ビューアーで処理中ダイアログが表示され続ける場合の対処方法 566

IM 構成管理・ビューアーのログがラップして現象発生時のログが採取できなかった場合のログの拡張手段 587

IM データベース

 サイズ拡張 71

 バックアップ・リカバリー手順 59

 ポート変更 76

IM データベースが終了できない場合の対処方法 555

IM データベースに接続できない場合の対処方法 556

IM データベースの再編成 52

IM データベースのセットアップでセットアップ情報ファイルが不正と出力される場合の対処方法 558

IM データベースのセットアップに失敗する場合の対処方法 557

IM データベース容量の管理 79

IM データベースを起動できない、またはデータベース関連のコマンドが実行できない場合の対処方法 559

IM データベースをセットアップしたときに、ポート番号不正のエラーメッセージが出力される場合の対処方法 557

IP アドレス

 変更 111

 メールサーバの IP アドレス 114

IP アドレスの変更 111

J

JP1/AS との連携 352

JP1/AS との連携の概要 353

JP1/AS と連携するための設定 366

JP1/AS の設定 370

JP1/AS 連携時のコマンド 376

 jcoimdef 376

 jim_log.bat (Windows 限定) 376

 jim_log.sh (UNIX 限定) 377

JP1/AS 連携用の JP1/IM の機能 356

JP1/IM

 BJEX との連携 352

 JP1/IM - Agent の起動と終了 337

 JP1/IM - Manager からログアウトする 153

 JP1/IM - Manager にログインする 149

 JP1/IM - Manager の起動と終了 131

 JP1/IM - Manager へのログインとログアウト 148

 JP1/IM - Manager を起動する 132

 JP1/IM - Manager を終了する 138

 JP1/IM システムの構成変更 97

 JP1/IM システムのメンテナンス 22

 JP1/IM によるシステムの操作 284

 JP1/IM の設定情報の変更 98

 JP1 イベントの重大度を変更する 231

 JP1 イベントのメモ情報を編集する 198

 JP1 イベントを検索する 220

- JP1 イベントを発行したアプリケーションをモニター起動する 261
- [監視ツリー] 画面で監視する 268
- 起動する 132
- 起動と終了に関する注意事項 145
- 自動アクションの状況を確認し、自動アクションの操作を行う 292
- 終了する 138
- 資料の採取方法 461
- スレッドダンプを出力する (Windows) 461
- 設定情報の管理 23
- セントラルコンソールによるシステムの監視 185
- セントラルスコープによるシステムの監視 267
- 対処の手順 379
- ダンプファイルを出力する (UNIX) 470
- ディスク容量の管理 79
- データベースの管理 52
- 適用するイベント取得フィルターを切り替える 209
- 統合機能メニューで他アプリケーションの画面を表示する 301
- トラブルシューティング 378
- トラブル発生時に採取が必要な資料 429
- トラブルへの対処方法 485
- [ビジュアル監視] 画面で監視する 274
- 履歴レポートの活用 87
- ログアウトする 153
- ログインする 149
- ログ情報の種類 380
- JP1/IM - Manager
 - GUI でログインする 150
 - 起動する 132
 - 起動と終了に関する注意事項 145
 - コマンドでログインする 151
 - 終了する 138
 - ログアウトする 153
 - ログインする 149
 - ログファイル一覧 (IM 構成管理) (UNIX) 414
 - ログファイル一覧 (IM 構成管理) (Windows) 394
 - ログファイル一覧 (セントラルコンソール) (UNIX) 405
 - ログファイル一覧 (セントラルコンソール) (Windows) 385
 - ログファイル一覧 (セントラルスコープ) (UNIX) 412
 - ログファイル一覧 (セントラルスコープ) (Windows) 392
 - JP1/IM - Manager, JP1/IM - View のどちらかのバージョンが古い場合の対処方法 540
 - JP1/IM - Manager がアンインストールできない場合の対処方法 556
 - JP1/IM - View
 - JP1 イベントを発行したアプリケーションをモニター起動する 261
 - [イベント取得条件一覧] 画面からイベント取得フィルターを切り替える 210
 - [イベント取得条件一覧] 画面から共通除外条件を切り替える 211
 - [コマンド] ボタンでコマンドを実行する 287
 - コマンドを実行するユーザー 290
 - [システム環境設定] 画面からイベント取得フィルターを切り替える 210
 - [システム環境設定] 画面から共通除外条件を切り替える 210
 - システムを操作する 284
 - [実行コマンド] でコマンドを実行する 285
 - 自動アクションの結果確認と再実行をする 292
 - 統合機能メニューで他アプリケーションの画面を表示する 301
 - ログインしたあと画面が表示されない 543
 - ログインできない場合の対処方法 520
 - ログファイル一覧 403
 - JP1/IM - View から起動中のログファイルトラップがすべて表示されない場合の対処方法 561
 - JP1/IM システム
 - 構成の管理 306
 - 構成の同期を取る 308
 - 構成を管理する 308
 - 構成を検証する 308
 - 構成を取得する 308

- 構成を反映する 308
- 構成を表示する 308
- 構成を編集する 308
- JP1/IM のフィルターを適用する 208
- JP1/IM - Agent のサービス 338
- JP1/IM - Agent のバックアップ 40
- JP1/IM - Agent のバックアップ対象ファイル 44
- JP1/IM - Agent のバックアップとリカバリー 40
- JP1/IM - Agent のリカバリー 41
- JP1/IM - Manager (インテリジェント統合管理基盤)
 - WWW ブラウザーでログインする 149
- JP1/IM - Manager のバックアップ
 - 設定情報 (UNIX) 32
 - 設定情報 (Windows) 24
- JP1/IM - Manager のバックアップとリカバリー 24
- JP1/IM - Manager のリカバリー
 - 設定情報 (UNIX) 39
- JP1/IM - Manager のリカバリー
 - 設定情報 (Windows) 32
- JP1/Navigation Platform
 - JP1 イベントに対応する運用手順を表示する (JP1/Navigation Platform 連携) 261
- JP1/Navigation Platform 連携
 - 操作する 261
- JP1/PFM
 - JP1 イベントに対応する性能レポートを表示する (JP1/PFM 連携) 263
 - 操作する 263
- JP1/Service Support
 - JP1 イベントをインシデントとして JP1/Service Support に登録する (JP1/Service Support 連携) 260
 - 操作する 260
- JP1/SES 形式のイベントを受信して文字化けが発生した場合の対処方法 574
- JP1 イベント
 - JP1 イベントの重大度を変更する 231
 - JP1 イベントの対処状況を設定する 200
 - 一覧に表示できる項目 187
 - 検索結果の表示 223
 - 検索する 220
 - 検索手順 220
 - 検索の方法 220
 - 固有の拡張属性を表示する (イベント情報のマッピング) 226
 - 固有の拡張属性を表示する (固有の拡張属性表示) 226
 - 重要イベントだけを表示する 208
 - 詳細情報を表示する 196
 - 発行したアプリケーションをモニター起動する 261
 - 表示する 186
 - 見方 186
- JP1 イベント検索
 - 検索手順 220
 - 操作する 220
- JP1 イベントに対応する運用手順を表示する (JP1/Navigation Platform 連携) 261
- JP1 イベントに対応する性能レポートを表示する (JP1/PFM 連携) 263
- JP1 イベントのグルーピング 230
- JP1 イベントの固有の拡張属性 (イベント情報マッピング) 190
- JP1 イベントの固有の拡張属性 (固有の拡張属性表示) 190
- JP1 イベントの固有の拡張属性を表示する (イベント情報のマッピング) 226
- 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) 226
- JP1 イベントの詳細情報を表示する 196
- JP1 イベントの情報を運用に合わせてカスタマイズする 226
- JP1 イベントの対処状況 190
- JP1 イベントの対処状況の設定について 200
- JP1 イベントの対処状況を設定する 200
- JP1 イベントの表示メッセージを変更する 234
- JP1 イベントの見方 186
- JP1 イベントの見方 ([イベント一覧] 画面) 158
- JP1 イベントをインシデントとして JP1/Service Support に登録する (JP1/Service Support 連携) 260

K

KAVB0002-E	527	KAVB2027-E	526
KAVB0104-E	521	KAVB2031-E	526
KAVB0109-E	521	KAVB2239-E	537
KAVB0256-E	546	KAVB6601-E	580
KAVB0415-E	524	KAVB6602-E	581
KAVB0416-E	524	KAVB6603-W	582
KAVB0417-E	525	KAVB7247-E	537
KAVB0418-E	525	KAVB7248-E	537
KAVB0419-E	525	KAVB7602-E	578
KAVB0422-E	525	KAVB7810-E	578
KAVB0423-E	526	KAVB7812-E	578
KAVB1034-E	529	KAVB7818-E	578
KAVB1036-W	528	KAVB8452-E	526
KAVB1037-E	527, 529	KAVB8817-E	576
KAVB1040-W	528	KAVB8818-E	576
KAVB1041-W	528	KNAN22403-E	599
KAVB1042-W	528	KNAN20100-E	521
KAVB1043-W	528	KNAN20101-E	521
KAVB1044-W	528	KNAN20102-E	522
KAVB1046-E	527	KNAN20103-E	522
KAVB1153-E	546	KNAN20104-E	522
KAVB1154-W	547	KNAN20121-E	580
KAVB1155-E	545	KNAN20122-E	581
KAVB1157-E	546	KNAN20123-W	582
KAVB1158-W	547	KNAN20124-W	582
KAVB1159-W	547	KNAN20141-E	580
KAVB1160-W	547	KNAN20142-E	581
KAVB1161-W	547	KNAN20143-W	582
KAVB1162-W	548	KNAN20144-W	582
KAVB1163-E	545	KNAN21400-W	571
KAVB1200-E	520	KNAN21402-E	571
KAVB1956-E	576	KNAN21403-E	571
KAVB1957-E	576	KNAN21404-E	583
KAVB1958-E	580	KNAN22017-E	569
KAVB1959-E	581	KNAN22403-E	589
KAVB1969-W	582	KNAN24155-E	578
KAVB1971-W	582	KNAN26039-E	568
KAVB1972-W	577	KNAN29095-E	579
		KNAN29097-W	579

P

Promitor のメトリックが取得できない 608

R

RAS 情報を採取する (UNIX) 471

RAS 情報を採取する (Windows) 465

S

Script exporter のメトリックが取得できない 608

U

UNIX の場合 (JP1/IM - Manager を起動する) 134

UNIX の場合 (JP1/IM - Manager を終了する) 138

W

Windows で OS 起動後またはネットワーク設定変更後、JP1/IM - Manager が起動しない、または、JP1/IM - View の操作ができなくなった場合の対処方法 573

Windows の場合 (JP1/IM - Manager を起動する) 132

Windows の場合 (JP1/IM - Manager を終了する) 138

あ

アクション結果の詳細情報 (メッセージ) に KAVB5150-W が表示される場合の対処方法 538

アプリケーションをモニター起動する 261

アラート情報の監視 169

い

イベント

重大度を変更する 231

イベント DB の再作成手順 67

イベント DB の再編成 52

イベント DB のバックアップ・リカバリー手順 58

イベント一覧から JP1 イベントの対処状況を設定する 201

イベント一覧での集約イベントの表示について 192

イベント一覧での関連イベントの表示について 194

イベント一覧の表示項目 186

イベント検索が実行できない場合の対処方法 553

[イベントコンソール] 画面

トラブルシューティング (定義メニューが表示されない) 523

[イベントコンソール] 画面に JP1 イベントが遅延して表示される場合の対処方法 550

[イベントコンソール] 画面に JP1 イベントが表示されない場合の対処方法 550

[イベントコンソール] 画面のイベント一覧に表示されるイベント 190

[イベントコンソール] 画面の各ページから JP1/Service Support を表示する 260

イベントサービス

トラブルシューティング (接続に失敗する) 523

イベントサービスへの接続に失敗する場合の対処方法 523

イベント取得フィルター

jcochfilter コマンドを使用して切り替える 211

切り替える 209

フィルターの適用 194

[イベント詳細] 画面から JP1/Service Support を表示する 261

イベント情報

トラブルシューティング (イベント情報を引き継がない) 527

イベント情報を引き継がない場合の対処方法 527

イベント転送

エージェントからのイベント転送を抑制してイベントの大量発生に対処する 244

イベント転送を自動で抑止するためのしきい値をエージェントに設定する 250

イベントの CSV 出力 87

イベントの検索方向 222

イベントの大量発生に対処する 239

イベント表示

表示開始位置を指定してイベントを表示する 216

イベントを大量に発行しているログファイルトラップをマネージャーから停止する 257

インシデント

[イベントコンソール] 画面の各ページから JP1/Service Support を表示する 260

[イベント詳細] 画面から JP1/Service Support を表示する 261

[関連イベント一覧] 画面から JP1/Service Support を表示する 261

インテリジェント統合管理基盤

JP1 イベント 158

OIDC 認証している外部製品と連携してシングルサインオンする 179

運用上の注意事項 181

システムの状態の見方 155

システムを監視する 154

性能情報を確認して対処する (JP1/PFM 連携) 177

ダイレクトアクセス URL で情報を共有する 180

他製品との連携 176

提案を確認して対処する 177

ポート番号を変更する 126

予兆によって障害を回避する (JP1/AJS 連携) 176

インテリジェント統合管理基盤によるシステムの監視 154

インテリジェント統合管理データベース

バックアップ・リカバリー手順 62

インテリジェント統合管理データベースが出力するログの確認 83

インテリジェント統合管理データベースの再編成 54

インテリジェント統合管理データベース容量の管理 80

インポートした IM 構成管理の管理情報をシステムに反映する 333

え

エージェントからのイベント転送を抑制してイベントの大量発生に対処する 244

エージェントからのイベント転送を抑制するための準備をする 241

エージェントホストまたはマネージャーホストでコマンドを実行する 288

お

応答待ちイベント 353

応答 363

応答する 374

応答待ちイベントと JP1/IM の関係 356

応答待ちイベントとして表示されない 549

監視 358

キャンセル 365

セントラルコンソールで応答待ちイベントを監視する 371

セントラルスコープで応答待ちイベントを監視する 373

滞留 361

滞留状態の監視を復帰させる 375

滞留を手動で解除する 375

発行経路 356

応答待ちイベントが JP1/IM - View に表示されない場合の対処方法 549

応答待ちイベント管理機能 353, 357

応答待ちイベント滞留ファイル 361

再作成 70

再編成 52

バックアップ・リカバリー手順 58

同じ属性のイベントが連続して発生した場合の集約表示について 258

オペレーション内容を確認する (UNIX) 471

オペレーション内容を確認する (Windows) 464

か

ガイド情報

表示する (監視ツリー) 272

表示する (ビジュアル監視) 277

拡張リカバリーに失敗した場合の対処手順 583

仮想化システム構成の管理 310

ホスト情報を表示する 310

ホストを登録する 310

画面上のエラー情報を採取する (UNIX) 471

画面上のエラー情報を採取する (Windows) 464

監視オブジェクト DB およびホスト情報 DB の再作成手順 66

監視オブジェクト DB およびホスト情報 DB の再編成 52

監視オブジェクト DB が破損している場合の対処方法
537

監視オブジェクト DB のバックアップ・リカバリー
手順 56

監視オブジェクト DB のロックが解除されない場合の
対処方法 538

監視構成の変更 125

監視対象ホスト名と発生元ホスト名が異なっていて
フィルターが正常に動作しない場合の対処方法 573

監視ツリー

- ガイド情報を表示する 272
- 画面で監視する 268
- 監視ノードの監視状態を変更する 269
- 監視ノードの状態を変更する 268
- 監視ノードの属性を表示する 271
- 監視ノードを検索する 270
- 状態変更イベントを検索する 270
- 情報をローカルホストに保存する 273
- [ビジュアル監視] 画面から呼び出す 274
- [ビジュアル監視] 画面を表示する 272
- ログインユーザーの一覧を表示する 273

[監視ツリー] 画面の情報をローカルホストに保存する
273

監視ノード

- 監視ツリーから監視状態を変更する 269
- 監視ツリーから検索する 270
- 監視ツリーから状態を変更する 268
- 監視ツリーから属性を表示する 271
- [ビジュアル監視] 画面から監視状態を変更する 275
- [ビジュアル監視] 画面から検索する 276
- [ビジュアル監視] 画面から状態を変更する 275
- [ビジュアル監視] 画面から属性を表示する 277

管理する

- ホスト 307

関連イベント一覧 (相関成立)] または [関連イベン
ト一覧 (相関不成立)] 画面から相関元イベントを削
除する 206

[関連イベント一覧 (相関成立)] または [関連イベン
ト一覧 (相関不成立)] 画面から相関元イベントの対
処状況を設定する 206

[関連イベント一覧] 画面から JP1/Service Support
を表示する 261

[関連イベント一覧] 画面から JP1 イベントを操作する
203

き

起動する 132

- 注意事項 145

起動と終了に関する注意事項 145

共通除外条件

- コマンドを使用して切り替える 213

共通除外条件の除外履歴 88

共通除外条件の定義履歴 88

共通メッセージログ 380

業務グループ

- 管理する 312

業務グループを管理する 312

<

クライアントアプリケーションを起動できない場合の
対処方法 529

クラスタシステム

- JP1/IM を運用する (起動) 136
- JP1/IM を運用する (終了) 140

繰り返しイベント

- 集約イベント 203

繰り返しイベントの詳細情報を確認し対処状況を変更
する 203

グルーピング

- JP1 イベント 230

け

検索結果の表示 (JP1 イベント) 223

検索する

- JP1 イベント 220
- 監視ノード (監視ツリーから) 270
- 監視ノード (ビジュアル監視から) 276

検索の方法 (JP1 イベント) 220

こ

- 個別ログ 383
- コマンド実行
 - コマンドの実行状態を確認する 290
 - [コマンド] ボタンでコマンドを実行する 287
 - コマンドを削除する 290
 - コマンドを実行する 285
 - [実行コマンド] でコマンドを実行する 285
 - トラブルシューティング (コマンド実行ができない) 524
 - トラブルシューティング (バッチファイルが正常終了しない(Windows 限定)) 545
 - トラブルシューティング (履歴ファイルが壊れている) 529
- コマンド実行ができない場合の対処方法 524
- コマンド実行履歴の再作成手順 65
- コマンド実行履歴の再編成 52
- コマンド実行履歴のバックアップ・リカバリー手順 55
- コマンド実行履歴ファイルが壊れている場合の対処方法 529
- [コマンド] ボタンからコマンドを実行できない場合の対処方法 528
- コマンドを実行する 285
- コマンドを実行するユーザー 290

さ

- サービスの稼働状況の管理 315
 - 稼働情報を収集する 315
 - 稼働情報を表示する 316

し

- しきい値
 - イベント転送を自動で抑止するためのしきい値をエージェントに設定する 250
- システム構成情報
 - エクスポート・インポートする 318
- システムの日時変更 116
 - 時刻を進める 120
- 自動アクション
 - 稼働状況を確認する 300

- キャンセルする 297
- 再実行する 298
- 実行結果を確認する 294
- 実行状況を確認する 292
- 状況を確認し、操作を行う 292
- トラブルシューティング (KAVB5150-W が表示される) 538
- トラブルシューティング (実行状態が「状態不明」と表示される) 535
- トラブルシューティング (遅延する) 536
- トラブルシューティング (バッチファイルが正常終了しない(Windows 限定)) 545
- 自動アクションが実行されない場合の対処方法 588
- 自動起動および自動停止の設定例 141
- 集約
 - 同じ属性のイベントが連続して発生した場合の集約表示について 258
- 集約イベント
 - 繰り返しイベントの対処状況を設定する 204
- 集約イベントに集約されている繰り返しイベントの詳細情報を確認する 203
- 集約イベントに集約されている繰り返しイベントの対処状況を設定する 204
- 集約表示
 - 同じ属性のイベントが連続して発生した場合の集約表示について 258
- 重要イベント
 - 表示する 208
 - フィルターの適用 194
- [重要イベント] ページから重要イベントを削除する 201
- 終了する 138
 - 注意事項 145
- 準備する
 - エージェントからのイベント転送を抑止するための準備をする 241
- 条件に一致する JP1 イベントにユーザー独自の固有の拡張属性を付加する 230
- 状態変更イベント
 - 検索する (監視ツリー) 270
 - 検索する (ビジュアル監視) 276

しよふのうんようちゆうにはつせいしたもんたいのえいきようはんいはあくしたいしよする (jp1/ajs れんけい)

ジョブの運用中に発生した問題の影響範囲を把握し対処する (JP1/AJS 連携) 176

しよふのていきやないようをへんこうするはあいへえいきようをうけるうとしよふねつとをしせんにはあくする (jp1/ajs れんけい)

ジョブの定義や内容を変更する場合に影響を受けるルートジョブネットを事前に把握する (JP1/AJS 連携) 177

資料採取ツール

実行する (UNIX) 471

実行する (Windows) 462

資料の採取方法 461

せ

正規表現

指定方法 (イベント検索) 223

設定情報および DB の移行 89

設定情報の管理 23

設定情報の変更 98

設定する

JP1/IM の設定情報の変更 98

イベント転送を自動で抑止するためのしきい値をエージェントに設定する 250

繰り返しイベント条件を設定する 250

発生した JP1 イベントを使って追加共通除外条件を設定する 214

設定ファイルの編集内容を反映する 314

選択したイベントの登録ホストに定義されたコマンドを実行する 289

セントラルコンソール

JP1 イベントのグループピング 230

システムを監視する 185

セントラルコンソール・ビューアーまたはセントラルスコープ・ビューアーのログがラップして現象発生時のログが採取できなかった場合のログの拡張手段 585

セントラルスコープ

[監視ツリー] 画面で監視する 268

システムを監視する 267

[ビジュアル監視] 画面で監視する 274

セントラルスコープの監視ツリーへ反映する 311

そ

関連イベントの詳細情報を確認し対処状況を変更する 204

関連イベントの発行

トラブルシューティング (JP1/IM - View に関連イベントが表示されない) 542

トラブルシューティング (発行処理の対象となる JP1 イベントが多発した) 542

発行履歴 87

関連元イベントを表示する 205

操作する 131, 337

GUI でログイン 150

JP1 イベント検索結果を表示 223

JP1 イベントに対応する運用手順を表示する (JP1/Navigation Platform 連携) 261

JP1 イベントに対応する性能レポートを表示する (JP1/PFM 連携) 263

JP1 イベントの重大度を変更 231

JP1 イベントの詳細情報を表示 196

JP1 イベントをインシデントとして JP1/Service Support に登録する (JP1/Service Support 連携) 260

JP1 イベントを検索 220

WWW ブラウザーでログインする 149

イベント一覧から JP1 イベントの対処状況を設定する 201

イベント取得フィルターの切り替え 209

[監視ツリー] 画面からガイド情報を表示 272

[監視ツリー] 画面から監視ノードの監視状態を変更 269

[監視ツリー] 画面から監視ノードの状態を変更 268

[監視ツリー] 画面から監視ノードの属性を表示 271

[監視ツリー] 画面から監視ノードを検索 270

[監視ツリー] 画面から状態変更イベントを検索 270

[監視ツリー] 画面で監視 268

[監視ツリー] 画面の情報をローカルホストに保存 273

起動 132

コマンドでログイン 151
コマンドの実行状態を確認 290
[コマンド] ボタンでコマンドを実行 287
コマンドを削除 290
[実行コマンド] でコマンドを実行 285
自動アクション機能の稼働状況を確認 300
自動アクションの実行結果を確認 294
自動アクションの実行状況を確認 292
自動アクションをキャンセル 297
自動アクションを再実行 298
重要イベントだけを表示 208
重要イベントを削除 201
終了 138
[統合機能メニュー] 画面 302
[ビジュアル監視] 画面からガイド情報を表示 277
[ビジュアル監視] 画面から [監視ツリー] 画面の呼び出し 274
[ビジュアル監視] 画面から監視ノードの監視状態を変更 275
[ビジュアル監視] 画面から監視ノードの状態を変更 275
[ビジュアル監視] 画面から監視ノードの属性を表示 277
[ビジュアル監視] 画面から監視ノードを検索 276
[ビジュアル監視] 画面から状態変更イベントを検索 276
[ビジュアル監視] 画面で監視 274
[ビジュアル監視] 画面を表示 272
メモ情報を編集 198
モニター起動 261
ログアウト 153
ログイン 149
ログインユーザーの一覧を表示 273
操作ログ 382
備える
イベントの大量発生に対処する場合と備える場合の流れ 239

た

他アプリケーションの画面を表示する 301

対処状況が変更できない場合の対処方法 552
対処状況の変更
変更する 201
対処する
イベントの大量発生に対処する 239
イベントの大量発生に対処する場合と備える場合の流れ 239
対処の手順 (トラブルシューティング) 379
他製品と連携して JP1 イベントに対処する 260
ダッシュボードの見方 166
ダッシュボードを表示する 166
ダンプファイルの管理 86

ち

注意事項

JP1/IM の起動と終了 145

つ

追加共通除外条件

追加共通除外条件を共通除外条件に変更する 215

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 214

追加共通除外条件を設定できない場合の対処方法 545

発生した JP1 イベントを使って追加共通除外条件を設定する 214

追加共通除外条件を共通除外条件に変更する 215

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 214

追加共通除外条件を設定できない場合の対処方法 545

通信暗号化機能が有効の JP1/IM - Manager で、エラーが表示される場合の対処方法 575

通信暗号化機能が有効の JP1/IM - View で、エラーが表示される場合の対処方法 580

て

停止

イベントを大量に発行しているログファイルトラップをマネージャーから停止する 257

ディスク容量の管理 79

データベースの管理 52

再作成 65
再作成 (イベント DB) 67
再作成 (応答待ちイベント滞留ファイル) 70
再作成 (監視オブジェクト DB・ホスト情報 DB) 66
再作成 (コマンド実行履歴) 65
サイズ拡張 (IM データベース) 71
再編成 52
再編成 (IM データベース) 52
再編成 (イベント DB) 52
再編成 (インテリジェント統合管理データベース) 54
再編成 (応答待ちイベント滞留ファイル) 52
再編成 (監視オブジェクト DB・ホスト情報 DB) 52
再編成 (コマンド実行履歴) 52
バックアップ 54
バックアップ (IM データベース) 59
バックアップ (イベント DB) 58
バックアップ (インテリジェント統合管理データベース) 62
バックアップ (応答待ちイベント滞留ファイル) 58
バックアップ (監視オブジェクト DB) 56
バックアップ (コマンド実行履歴) 55
バックアップ (ホスト情報 DB) 57
ポート変更 (IM データベース) 76
リカバリー 54
リカバリー (IM データベース) 59
リカバリー (イベント DB) 58
リカバリー (インテリジェント統合管理データベース) 62
リカバリー (応答待ちイベント滞留ファイル) 58
リカバリー (監視オブジェクト DB) 56
リカバリー (コマンド実行履歴) 55
リカバリー (ホスト情報 DB) 57
データベースの再編成 52
データベース容量の管理 79

と

統合エージェントホストの JP1/IM - Agent の設定変更 98

統合エージェントホストのシステム日時を変更する場合に必要な手順 121
統合エージェントホストの複製 129
統合エージェントホストのロケールを変更する場合に必要な作業 127
統合機能メニュー
画面から操作できる機能 302
画面の操作 302
他アプリケーションの画面を表示する 301
統合トレースログ 380
統合マネージャーホストの JP1/IM - Agent の設定変更 99
トラップした JP1 イベントのメッセージが文字化けしてしまう場合の対処方法 524
トラブルシューティング 378, 485
採取が必要な資料 429
資料の採取方法 461
対処の手順 379
対処方法 485
ログ情報の種類 380
トラブルシューティング (IM 構成管理に登録するホスト名と発生元ホスト名が異なってしまう) 572
トラブルシューティング (JP1/IM - Manager のメール通知機能でメールが送信先に届かない場合の対処方法)
JP1/IM - Manager のメール通知機能でメールが送信先に届かない場合の対処方法 574
トラブルシューティング (監視対象ホスト名と発生元ホスト名が異なっていてフィルターが正常に動作しない) 573
トラブルシューティング (クライアントアプリケーションを起動できない) 529
トラブルシューティング ([コマンド] ボタンからコマンドを実行できない) 528
トラブルシューティング (追加共通除外条件を設定できない) 545
トラブルシューティング (トラップした JP1 イベントのメッセージが文字化けしてしまう) 524
トレンド表示とアラートで扱うメトリックの追加 164

は

バックアップ

- IM データベース 59
- イベント DB 58
- インテリジェント統合管理データベース 62
- 応答待ちイベント滞留ファイル 58
- 監視オブジェクト DB 56
- コマンド実行履歴 55
- データベース (DB) 54
- バックアップ対象ファイル (UNIX) 33
- バックアップ対象ファイル (Windows) 24
- ホスト情報 DB 57

発生した JP1 イベントを使って追加共通除外条件を設定する 214

バッチジョブ実行システム 353

- バッチジョブ実行システムと連携する場合のシステム構成 353

ひ

非クラスタシステム

- 論理ホストを運用する (起動) 136
- 論理ホストを運用する (停止) 140

ビジュアル監視

- ガイド情報を表示する 277
- 画面から [監視ツリー] 画面を呼び出す 274
- 画面で監視する 274
- 監視ツリーから [ビジュアル監視] 画面を表示する 272
- 監視ノードの監視状態を変更する 275
- 監視ノードの状態を変更する 275
- 監視ノードの属性を表示する 277
- 監視ノードを検索する 276
- 状態変更イベントを検索する 276
- [ビジュアル監視] 画面で監視する 274
- 表示開始位置を指定してイベントを表示する 216
- 表示する
 - 集約イベント 258
- 表示する JP1 イベントの期間を指定して絞り込む 218
- 表示フィルター

フィルターの適用 194

ふ

- フィルター 208
- フィルターの適用 194
- プロセスの状態を確認する
 - UNIX 470
 - Windows 461
- プロファイル
 - 管理する 313
- プロファイルの管理 313
 - 収集する 313
 - 設定ファイルを編集する 313
 - 表示する 313
- プロファイルの設定ファイルと有効設定情報の内容が異なる場合の対処方法 561
- プロファイルリストを収集する 313

へ

変更

- JP1 イベントの表示メッセージを変更する 234
- 変更する
 - 追加共通除外条件を共通除外条件に変更する 215
- 編集する
 - メモ情報 198

ほ

ホスト情報

- DB のバックアップ・リカバリー手順 57
- 収集する 307
- ホスト情報を変更する 307
- ホストの管理 307
 - 一覧を表示する 307
 - 削除する ([IM 構成管理] 画面) 307
 - 情報を収集する 307
 - 登録する 307
- ホスト名
 - クラスタシステムの論理ホスト名 109
 - 変更 100

メールサーバのホスト名 109

ホスト名の変更 100

ま

マネージャーおよびエージェントの日時変更

過去に戻す 116

マネージャーおよびエージェントの日時を変更した場合に必要な作業 116

マネージャーの IP アドレス

変更した直後に必要な作業 111

変更した場合の作業 111

マネージャーのホスト名

変更した直後に必要な作業 100

変更した場合の作業 100

マネージャーまたは JP1/Base の IP アドレス

変更した直後に必要な作業 113

変更した場合の作業 114

マネージャーまたは JP1/Base の IP アドレスを変更した場合のシステムの再起動手順 114

マネージャーまたは JP1/Base のホスト名

変更した直後に必要な作業 106

変更した場合の作業 107

マネージャーまたは JP1/Base のホスト名を変更した場合のシステム構成の再配布手順 109

め

メッセージ

JP1 イベントの表示メッセージを変更する 234

メモ情報が設定できない場合の対処方法 555

メンテナンス 22

設定情報の管理 23

ディスク容量の管理 79

データベースの管理 52

履歴レポートの活用 87

も

モニター画面 261

モニター起動

JP1 イベントを発行したアプリケーションを起動する 261

ゆ

ユーザーダンプを採取する (Windows 限定) 464

よ

抑止する

エージェントからのイベント転送を抑止してイベントの大量発生に対処する 244

エージェントからのイベント転送を抑止するための準備をする 241

り

リカバリー

IM データベース 59

イベント DB 58

インテリジェント統合管理データベース 62

応答待ちイベント滞留ファイル 58

監視オブジェクト DB 56

コマンド実行履歴 55

データベース (DB) 54

ホスト情報 DB 57

リモート監視構成からエージェント構成に監視構成を変更する場合の注意事項 125

リモート監視構成の監視対象ホストの日時を変更した場合に必要な作業 123

リモート監視構成の監視対象ホストのパスワードを変更した場合に必要な作業 124

リモート監視の監視対象ホストと接続できない場合の対処方法 569

リモート監視の監視対象ログファイル名が誤っている場合の対処方法 568

履歴レポートの活用 87

れ

連携する

他製品と連携して JP1 イベントに対処する 260

連携製品

BJEX 352

JP1/AS との連携 352

ろ

ログアウトする 153

ログインする 149

GUI から 150

WWW ブラウザーで 149

ログインユーザーの一覧を表示する 273

ログ情報の種類 380

ログファイル一覧 384

ログファイルトラップ

イベントを大量に発行しているログファイルトラップをマネージャーから停止する 257

ログファイル容量の管理 82

 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
