HITACHI
Inspire the Next

JP1 Version 13

JP1/IT Desktop Management 2 構築ガイド

3021-3-L73-40

前書き

■ 対象製品

適用 OS のバージョン、JP1/IT Desktop Management 2 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リリースノートで確認してください。

●P-2A42-78DL　JP1/IT Desktop Management 2 - Manager　13-50

製品構成一覧および内訳形名

・P-CC2A42-7ADL　JP1/IT Desktop Management 2 - Manager（適用 OS：Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016）

・P-CC2A42-7BDL　JP1/IT Desktop Management 2 - Agent（適用 OS：Windows Server 2025、Windows Server 2022、Windows 11、Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、Windows Server 2008 R2）

・P-CC2A42-7CDL　JP1/IT Desktop Management 2 - Network Monitor（適用 OS：Windows Server 2025、Windows Server 2022、Windows 11、Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1 Enterprise、Windows 8.1 Pro、Windows 8 Enterprise、Windows 8 Pro、Windows Server 2012、Windows 7 Enterprise、Windows 7 Professional、Windows 7 Ultimate）

・P-CC2A42-7DDL　JP1/IT Desktop Management 2 - Asset Console（適用 OS：Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016）

・P-CC2A42-7PDL　JP1/IT Desktop Management 2 - Internet Gateway（適用 OS：Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016）

●P-2A42-7KDL　JP1/IT Desktop Management 2 - Operations Director　13-50

製品構成一覧および内訳形名

・P-CC2A42-7ADL　JP1/IT Desktop Management 2 - Manager（適用 OS：Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016）

・P-CC2A42-7BDL　JP1/IT Desktop Management 2 - Agent（適用 OS：Windows Server 2025、Windows Server 2022、Windows 11、Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、Windows Server 2008 R2）

・P-CC2A42-7CDL　JP1/IT Desktop Management 2 - Network Monitor（適用 OS：Windows Server 2025、Windows Server 2022、Windows 11、Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1 Enterprise、Windows 8.1 Pro、Windows 8 Enterprise、Windows 8 Pro、Windows Server 2012、Windows 7 Enterprise、Windows 7 Professional、Windows 7 Ultimate）

・P-CC2A42-7PDL　JP1/IT Desktop Management 2 - Internet Gateway（適用 OS：Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016）

■ 輸出時の注意

本製品を輸出される場合には、外国為替および外国貿易法の規制なら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

BSAFE は、Dell Inc.の米国およびその他の国における商標または登録商標です。

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。

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。

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 IAIK of Graz University of Technology.

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

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

This product includes software developed by Andy Clark.

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。

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

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

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)
2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)
4. 本製品には OpenSSL Toolkit ソフトウェアを OpenSSL License および Original SSLeay License に従い使用しています。OpenSSL License および Original SSLeay License は以下のとおりです。

```
LICENSE ISSUES
==============
The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSD-style
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.
OpenSSL License
---------------
/* ====================================================================
* Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
```

```
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
```

```
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License
-----------------------
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
```

```
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the rouines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
```

*/

■ マイクロソフト製品のスクリーンショットの使用について

マイクロソフトの許可を得て使用しています。

■ 発行

2025 年 9 月　3021-3-L73-40

■ 著作権

変更内容

変更内容（3021-3-L73-40） JP1/IT Desktop Management 2 13-50

追加・変更内容	変更個所
Windows Server 2025 を次の製品の適用 OS に追加した。 • JP1/IT Desktop Management 2 - Manager • JP1/IT Desktop Management 2 - Agent • JP1/IT Desktop Management 2 - Network Monitor • JP1/IT Desktop Management 2 - Asset Console • JP1/IT Desktop Management 2 - Internet Gateway	－
JP1/IT Desktop Management 2 の認証を認証プロバイダーで実行できる IDaaS 連携機能を追加した。	1.4.1、2.7.1、2.12

（凡例） －：該当なし

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/IT Desktop Management 2 - Manager および JP1/IT Desktop Management 2 - Operations Director の構築方法を説明したものです。以降、JP1/IT Desktop Management 2 - Manager および JP1/IT Desktop Management 2 - Operations Director を、JP1/IT Desktop Management 2 と略します。

また、JP1/IT Desktop Management 2 - Manager と比較して、JP1/IT Desktop Management 2 - Operations Director では一部の機能が制限されます。機能制限については、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」の、JP1/IT Desktop Management 2 - Operations Director での機能制限の説明を参照してください。

最新の注意事項については、リリースノートを参照してください。

■ 対象読者

このマニュアルは、次の方にお読みいただくことを前提に説明しています。

- JP1/IT Desktop Management 2 のシステムの構築をしている方
- JP1/IT Desktop Management 2 の構築方法、上書きインストール方法、アンインストール方法、または環境の移行方法について知りたい方

■ マニュアルの構成

このマニュアルは、次に示す章と付録から構成されています。

第 1 章　管理用サーバとエージェントの構築

管理用サーバとエージェントの構築方法について説明しています。

第 2 章　各システム構成の構築

システム構成ごとの構築方法について説明しています。

第 3 章　セットアップ内容の変更

管理用サーバでセットアップ時に設定した内容の変更について説明しています。

第 4 章　構築時の設定のカスタマイズ

構築時の設定で、カスタマイズできる項目について説明しています。

第５章　製品の上書きインストールおよびコンポーネントのアップデート

JP1/IT Desktop Management 2 - Manager の上書きインストール、およびコンポーネント（エージェント、中継システムおよびネットワークモニタエージェント）のアップデートについて説明しています。

第６章　製品のアンインストール

JP1/IT Desktop Management 2 の各種プログラムをアンインストールする方法について説明しています。

第７章　環境の移行

JP1/IT Desktop Management 2 で環境を移行する方法について説明しています。

第８章　構築関連で使用するコマンド

システムの構築、設定変更、リプレースなどで使用する、JP1/IT Desktop Management 2 のコマンドについて説明しています。

第９章　トラブルシューティング

JP1/IT Desktop Management 2 の構築時に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。

付録 A　参考情報

JP1/IT Desktop Management 2 を使用する上での参考情報について説明しています。

このマニュアルをお読みになる場合の参考情報は、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」を参照してください。

目次

1 管理用サーバとエージェントの構築

ここでは、管理用サーバとエージェントの構築方法について説明します。管理用サーバとエージェントを構築して、基盤となる構成システムを準備します。基盤となる構成システムには、最小構成システム、基本構成システム、および複数サーバ構成システムがあります。

基盤となる構成システムを構築したあとは、設定を変更したり、ほかのシステム構成要素を導入したりして、管理の目的に応じたシステム構成を構築してください。基盤となる構成システム以外のシステムを構築する場合は、先に「2.　各システム構成の構築」を参照してください。

1.1　基盤となる構成システムの構築

1.1.1　最小構成システムを構築する流れ

最小構成システムを構築するには、管理用サーバを構築したあとで、管理対象とするコンピュータにエージェントを導入します。

1. 管理用サーバを構築します。
2. JP1/IT Desktop Management 2 の製品ライセンスを登録します。
3. 操作画面にログインしてユーザーアカウントの情報を設定します。
4. 事前に組織内の機器を把握して、どのコンピュータにどの方法でエージェントを導入するかを計画します。
5. JP1/IT Desktop Management 2 の管理対象とするコンピュータに、エージェントを導入します。

最小構成システムの構築が完了します。

関連リンク

- 1.2　管理用サーバの環境構築
- 1.3　製品ライセンスを登録する
- 1.4　操作画面にログインする
- 1.5　組織内の機器を把握する
- 1.6　エージェントを手動でインストールする
- 1.7　エージェントを自動でインストールする

1.1.2　基本構成システムを構築する流れ

基本構成システムを構築するには、まず管理用サーバの環境を構築し、そのあとで中継システムの構築を実施します。

1. 管理用サーバの環境を構築します。
2. JP1/IT Desktop Management 2 の製品ライセンスを登録します。
3. 操作画面にログインしてユーザーアカウントの情報を設定します。
4. 中継システム用のコンピュータに中継システムのプログラムをインストールし、セットアップします。

5. 事前に組織内の機器を把握して、どのコンピュータにどの方法でエージェントを導入するかを計画します。

6. JP1/IT Desktop Management 2 の管理対象とするコンピュータに、エージェントを導入します。

基本構成システムの構築が完了します。

> **ヒント**
>
> 管理用サーバとは別のコンピュータに、リモートインストールマネージャだけをインストールすることもできます。

関連リンク

- 1.2　管理用サーバの環境構築
- 1.8　中継システムの環境構築
- 1.3　製品ライセンスを登録する
- 1.4　操作画面にログインする
- 1.6　エージェントを手動でインストールする
- 1.7　エージェントを自動でインストールする
- 1.9.1　リモートインストールマネージャだけをインストールする手順

1.1.3　複数サーバ構成システムを構築する流れ

複数サーバ構成システムを構築するには、まず統括管理用サーバを構築します。そのあとで、管理用中継サーバを構築します。

1. 統括管理用サーバの環境を構築します。

2. 管理用中継サーバの環境を構築します。

3. 統括管理用サーバに、JP1/IT Desktop Management 2 の製品ライセンスを登録します。

4. 各管理用サーバで JP1/IT Desktop Management 2 の製品ライセンスの保有数や残数を管理したい場合は、`distributelicense` コマンドを実行して管理用中継サーバにライセンスの登録許可または JP1/IT Desktop Management 2 の製品ライセンスの分配をします。
   ライセンスの登録を許可した管理用中継サーバには、製品ライセンスを登録します。

5. 各管理用サーバの操作画面にログインしてユーザーアカウントの情報を設定します。

6. 事前に組織内の機器を把握して、どのコンピュータにどの方法でエージェントを導入するかを計画します。

7. JP1/IT Desktop Management 2 の管理対象とするコンピュータに、エージェントを導入します。

複数サーバ構成システムの構築が完了します。

関連リンク

- 1.2　管理用サーバの環境構築
- 1.3　製品ライセンスを登録する
- 1.4　操作画面にログインする
- 1.6　エージェントを手動でインストールする
- 1.7　エージェントを自動でインストールする
- 8.11　distributelicense（ライセンスの分配）

1.2　管理用サーバの環境構築

管理用サーバは、JP1/IT Desktop Management 2 - Manager をインストールおよびセットアップして構築します。

インストールタイプを決めたら、単数サーバ構成または複数サーバ構成で、それぞれ次の個所を参照してインストールしてください。

単数サーバ構成の環境構築

- 1.2.2　JP1/IT Desktop Management 2 - Manager をインストールする手順（単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバの場合）
- 1.2.4　単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順

複数サーバ構成の環境構築

- 1.2.2　JP1/IT Desktop Management 2 - Manager をインストールする手順（単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバの場合）
- 1.2.4　単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順
- 1.2.3　JP1/IT Desktop Management 2 - Manager をインストールする手順（管理用中継サーバの場合）
- 1.2.5　管理用中継サーバをセットアップする手順

1.2.1　JP1/IT Desktop Management 2 - Manager のインストールタイプ

JP1/IT Desktop Management 2 - Manager のインストールタイプには、次の 2 種類があります。インストール時に、目的に応じて選択してください。

簡単インストール

最小限の操作でインストールとセットアップを完了できます。インストールおよびセットアップには、デフォルトの値が設定されます。特別な設定をする必要がない場合は、この方法をお勧めします。

カスタムインストール

各種設定をしながらインストールを進めます。インストール終了後にセットアップを実行してデータベースを作成する必要があります。インストールおよびセットアップで任意の値を設定したい場合は、この方法をお勧めします。複数サーバ構成の場合または大規模管理用のオプションを有効にしてサーバを導入する場合は、カスタムインストールを選択してください。

1.2.2 JP1/IT Desktop Management 2 - Manager をインストールする手順（単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバの場合）

JP1/IT Desktop Management 2 - Manager のインストールを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

重要

コンピュータが Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016 または Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- *システムドライブ*:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

重要

インストール前は、すべての Windows アプリケーションを終了させてください。誤って JP1/IT Desktop Management 2 - Manager のプログラムを起動したままインストールを実行した場合は、インストールの実行結果に関係なく OS を再起動してください。OS を再起動しても、サービスが起動しない場合や、JP1/IT Desktop Management 2 - Manager のプログラムが動作しない場合は、次に示す手順でインストールを再実行してください。

1. すべての Windows アプリケーションを終了させてください。
2. サービス（JP1_ITDM2_Service）を停止してください。
3. 上書きインストールを再実行してください。サービスが開始されます。

重要

インストール先のドライブは、ローカルディスクを使用してください。ネットワーク接続のディスク（NFS、NAS など）をマウントしインストールしないでください。

JP1/IT Desktop Management 2 - Manager をインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Manager］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。
4. ［使用許諾契約］ダイアログで、内容を確認してから［使用許諾契約の条項に同意します］を選択し、［次へ］ボタンをクリックします。
5. ［インストールタイプ］ダイアログで、インストールタイプを選択して［次へ］ボタンをクリックします。
   簡単インストールを選択した場合は、手順 7.へ進んでください。
   複数サーバ構成の統括管理用サーバをインストールする場合は、カスタムインストールを選択してください。
6. ［ユーザー登録］ダイアログで、ユーザー名と会社名を入力して［次へ］ボタンをクリックします。
7. ［インストール先のフォルダ］ダイアログで、インストール先のフォルダを指定して［次へ］ボタンをクリックします。
   簡単インストールの場合は、ここでデータベースの作成先フォルダも指定してください。
8. ［データベースの設定］ダイアログで、データベースを使用するためのユーザー ID とパスワードを指定して［次へ］ボタンをクリックします。
   簡単インストールを選択した場合に必要な手順です。カスタムインストールを選択した場合は、セットアップ時にデータベースの設定をします。

ヒント

ユーザー ID は、8 文字以内の半角英数字（先頭の文字は英字）で指定します。デフォルトは「itdm2m」です。パスワードは、任意の 28 文字以内の半角英数字（先頭の文字は英字）です。ここで設定したユーザー ID とパスワードは、JP1/IT Desktop Management 2 - Asset Console を使用する場合に必要になります。忘れないようにしてください。

重要

ユーザー ID に「root」、「ALL」、「MASTER」、「netmdm」、および「PUBLIC」は指定しないでください。（大文字小文字は区別しません。）

9. コンポーネントを選択するダイアログで、インストールするコンポーネントとして Manager を選択し、そのインストール方法を指定して［次へ］ボタンをクリックします。

   カスタムインストールを選択した場合に必要な手順です。

   ヒント

   Manager をインストールする場合、Remote Install Manager もインストールする必要があります。Remote Install Manager のプルダウンメニューで［この機能を使用できないようにします。］を選択していると、インストールできません。

   インストール方法は、文字列の左にあるアイコンをクリックして、プルダウンメニューから選択します。

10. ［インストールする Manager の種別］ダイアログで、［単数サーバ構成の管理用サーバ、または複数サーバ構成の統括管理用サーバ］を選択して［次へ］ボタンをクリックします。

    機器の台数が 50,000 台以上の大規模で運用する場合は、［大規模管理用］にチェックをしてください。

    カスタムインストールを選択した場合に必要な手順です。

11. インストール内容を確認するダイアログで、インストール内容に問題がないことを確認し、［インストール］ボタンをクリックします。

    インストールが実行されます。インストール内容に問題がある場合は、［戻る］ボタンをクリックして設定を修正してください。

12. インストールが完了したら、［完了］ボタンをクリックします。

JP1/IT Desktop Management 2 - Manager のインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

簡単インストールの場合は、インストール時にセットアップも自動で実行されるので、インストール完了後すぐに JP1/IT Desktop Management 2 にログインして操作を開始できます。

カスタムインストールの場合は、データベースを作成するために、インストール完了後にセットアップを実行する必要があります。インストール完了時に、［セットアップ］をチェックした場合、インストールが完了するとセットアップが自動で起動します。

ヒント

インストールが完了すると、デスクトップに操作画面へログインするためのショートカットが作成されます。ただし、カスタムインストールの場合、ショートカットはセットアップが完了するまで使用できません。

重要

JP1/IT Desktop Management 2 - Manager をインストールした後、イベントログ（システム）に次のメッセージが出力される場合がありますが、動作上、問題はありません。

- JP1_ITDM2_Agent Remote Control サービスは、対話型サービスとしてマークされています。
  しかし、システムは対話型サービスを許可しないように構成されています。
  このサービスは正常に機能しない可能性があります。
- JP1_ITDM2_Agent Service サービスは、対話型サービスとしてマークされています。
  しかし、システムは対話型サービスを許可しないように構成されています。
  このサービスは正常に機能しない可能性があります。
- JP1_ITDM2_Agent Monitor Control サービスは、対話型サービスとしてマークされています。
  しかし、システムは対話型サービスを許可しないように構成されています。
  このサービスは正常に機能しない可能性があります。

1.2.3 JP1/IT Desktop Management 2 - Manager をインストールする手順（管理用中継サーバの場合）

JP1/IT Desktop Management 2 - Manager のインストールを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

重要

JP1/IT Desktop Management 2 - Agent をインストールしているコンピュータには、管理用中継サーバをインストールできません。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

重要

コンピュータが Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016 または Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- *システムドライブ*:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

重要

インストール前は、すべての Windows アプリケーションを終了させてください。誤って JP1/IT Desktop Management 2 - Manager のプログラムを起動したままインストールを実行した場合は、インストールの実行結果に関係なく OS を再起動してください。OS を再起動しても、サービスが起動しない場合や、JP1/IT Desktop Management 2 - Manager のプログラムが動作しない場合は、次に示す手順でインストールを再実行してください。

1. すべての Windows アプリケーションを終了させてください。
2. サービス（JP1_ITDM2_Service）を停止してください。
3. 上書きインストールを再実行してください。サービスが開始されます。

重要

インストール先のドライブは、ローカルディスクを使用してください。ネットワーク接続のディスク（NFS、NAS など）をマウントしインストールしないでください。

管理用中継サーバ用のコンピュータに JP1/IT Desktop Management 2 - Manager をインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Manager］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。
4. ［使用許諾契約］ダイアログで、内容を確認してから［使用許諾契約の条項に同意します］を選択し、［次へ］ボタンをクリックします。
5. ［インストールタイプ］ダイアログで、［カスタムインストール］を選択して［次へ］ボタンをクリックします。
6. ［ユーザー登録］ダイアログで、ユーザー名と会社名を入力して［次へ］ボタンをクリックします。

7. [インストール先のフォルダ] ダイアログで、インストール先のフォルダを指定して［次へ］ボタンをクリックします。

8. コンポーネントを選択するダイアログで、インストールするコンポーネントとして Manager を選択し、そのインストール方法を指定して［次へ］ボタンをクリックします。

> **ヒント**
>
> Manager をインストールする場合、Remote Install Manager もインストールする必要があります。Remote Install Manager のプルダウンメニューで［この機能を使用できないようにします。］を選択していると、インストールできません。
>
> インストール方法は、文字列の左にあるアイコンをクリックして、プルダウンメニューから選択します。

9. [インストールする Manager の種別] ダイアログで、[管理用中継サーバ] を選択して［次へ］ボタンをクリックします。

10. [エージェントのコンポーネント設定] ダイアログで、管理用中継サーバに含めるエージェントのコンポーネントを選択して［次へ］ボタンをクリックします。

11. インストール内容を確認するダイアログで、インストール内容に問題がないことを確認し、[インストール] ボタンをクリックします。

    インストールが実行されます。インストール内容に問題がある場合は、[戻る] ボタンをクリックして設定を修正してください。

12. インストールが完了したら、[完了] ボタンをクリックします。

管理用中継サーバとしての JP1/IT Desktop Management 2 - Manager のインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

データベースを作成するために、インストール完了後にセットアップを実行する必要があります。インストール完了時に、[セットアップ] をチェックした場合、インストールが完了するとセットアップが自動で起動します。

> **ヒント**
>
> インストールが完了すると、デスクトップに操作画面へログインするためのショートカットが作成されます。ただし、セットアップが完了するまで使用できません。

> **重要**
>
> JP1/IT Desktop Management 2 - Manager をインストールした後、イベントログ（システム）に次のメッセージが出力される場合がありますが、動作上、問題はありません。

- JP1_ITDM2_Agent Remote Control サービスは、対話型サービスとしてマークされています。
  しかし、システムは対話型サービスを許可しないように構成されています。
  このサービスは正常に機能しない可能性があります。
- JP1_ITDM2_Agent Service サービスは、対話型サービスとしてマークされています。
  しかし、システムは対話型サービスを許可しないように構成されています。
  このサービスは正常に機能しない可能性があります。
- JP1_ITDM2_Agent Monitor Control サービスは、対話型サービスとしてマークされています。
  しかし、システムは対話型サービスを許可しないように構成されています。
  このサービスは正常に機能しない可能性があります。

1.2.4 単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順

JP1/IT Desktop Management 2 - Manager をカスタムインストールでインストールした場合、データベースの作成や各種環境設定のために、インストール直後にセットアップを実行する必要があります。

管理用サーバをセットアップするには：

1. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
2. セットアップ画面で、［次へ］ボタンをクリックします。
3. ［セットアップの選択］画面で、セットアップの種類を選択して［次へ］ボタンをクリックします。
   インストール後の初回セットアップ時には、この画面は表示されません。
4. ［データベースの設定］画面で、データベースにアクセスするためのパスワードを変更するかどうかを選択して［次へ］ボタンをクリックします。
   パスワードを変更する場合は、現在のパスワードと新しいパスワードを入力し、手順 18.へ進んでください。
   インストール後の初回セットアップ時には、この画面は表示されません。非クラスタ環境かクラスタ環境の現用系の 2 回目以降のセットアップ時に、手順 3.の［セットアップの選択］画面で［設定変更］を選択した場合に、この画面が表示されます。

ヒント

ユーザー ID は、簡単インストール時または初回セットアップ時に設定したものが表示されます。パスワードは、任意の 28 文字以内の半角英数字（先頭の文字は英字）で指定しま

す。ここで変更したパスワードは、JP1/IT Desktop Management 2 - Asset Console を使用する場合に必要になります。忘れないようにしてください。

5. [クラスタ環境] 画面で、クラスタシステムを運用するための設定をして、[次へ] ボタンをクリックします。

クラスタ環境を使用する場合に［待機系］を選択したときは、手順 6.～手順 8.、および手順 10.～手順 18.は不要です。

6. [サーバ構成の選択] 画面で、サーバ構成を選択して［次へ］ボタンをクリックします。

7. [データベースの設定] 画面で、データベースにアクセスするためのユーザー ID とパスワードを設定して［次へ］ボタンをクリックします。

非クラスタ環境かクラスタ環境の現用系の 2 回目以降のセットアップ時には、この画面は表示されません。

ヒント

ユーザー ID は、8 文字以内の半角英数字（先頭の文字は英字）で指定します。デフォルトは「itdm2m」です。パスワードは、任意の 28 文字以内の半角英数字（先頭の文字は英字）です。ここで設定したユーザー ID とパスワードは、JP1/IT Desktop Management 2 - Asset Console を使用する場合に必要になります。忘れないようにしてください。

重要

ユーザー ID に「root」、「ALL」、「MASTER」、「netmdm」、および「PUBLIC」は指定しないでください。（大文字小文字は区別しません。）

8. 表示された画面で、データベースにアクセスするための管理用サーバの IP アドレスとデータベースへのアクセス時のキャッシュ容量を設定して［次へ］ボタンをクリックします。

ヒント

データベースへのアクセス時のキャッシュ容量には、目安として管理対象のコンピュータが 10,000 台までの場合は 1 ギガバイトを、10,000～50,000 台の場合は 16 ギガバイトを指定してください。

インストール時に［大規模管理用］にチェックをした場合は、管理する機器の台数に合わせて、データベースへのアクセス時のキャッシュ容量を選択してください。

9. [フォルダの設定] 画面で、JP1/IT Desktop Management 2 - Manager が使用する各種フォルダを指定して［次へ］ボタンをクリックします。

10. [操作ログの設定] 画面で、操作ログを取得するかどうかを設定して［次へ］ボタンをクリックします。

操作ログを取得しない場合は、手順 14.へ進んでください。

11. 表示された画面で、操作ログを保管するかどうかを設定して、［次へ］ボタンをクリックします。

12. 表示された画面で、管理対象の機器の台数、操作ログのデータベース格納最大日数、および操作ログのデータベースフォルダを設定して、［次へ］ボタンをクリックします。

13. 操作ログの検索性能を向上させたい場合、データベースのキャッシュを追加できます。必要に応じて、表示された画面で追加するキャッシュ容量を設定して、［次へ］ボタンをクリックします。

14. ［保存用の変更履歴の出力設定］画面で、保存用の変更履歴を定期的に出力するかどうかを設定して［次へ］ボタンをクリックします。

15. ［ポート番号の設定］画面で、JP1/IT Desktop Management 2 - Manager が使用するポート番号を設定して［次へ］ボタンをクリックします。

16. ［アドレス解決の設定］画面で、ホスト間で通信するときに通信相手のコンピュータを決定する情報の種類（ホスト名または IP アドレス）を選択します。ホスト名を選択した場合は、アドレス解決の方法およびアドレス解決ができなかったときの処理を設定します。

    ここで設定する通信相手のコンピュータを決定する情報の種類を運用キーと呼びます。

17. ［ユーザー管理の設定］画面で、JP1/Base を使用してユーザー管理するかどうかを選択します。選択した場合は、JP1/IT Desktop Management 2 で使用する JP1 ユーザーが関連づけられている JP1 資源グループ名を指定します。

    > **ヒント**
    >
    > JP1/Base を使用してユーザー管理する場合は、セットアップ開始前に JP1 ユーザー、JP1 資源グループ、および JP1 権限レベルを JP1/Base の認証サーバで設定しておく必要があります。JP1/Base を使用してユーザー管理する構成システムを構築する流れについては、「2.7.1　JP1 認証を使用した構成システムを構築する流れ」を、認証サーバでの設定手順についてはマニュアル「JP1/Base 運用ガイド」を参照してください。

18. ［その他の設定］画面で、操作画面に表示される通貨単位、および ITDM 互換配布の機能を使用するときに流量制御するかどうかを設定して［次へ］ボタンをクリックします。

19. 表示された画面で、アカウントをロックする連続入力失敗の回数、ユーザパスワードの有効日数、および操作画面での資産情報の操作を抑止するかどうかを設定して［次へ］ボタンをクリックします。

20. ［セットアップの確認］画面で、セットアップ内容に問題がないことを確認し、［次へ］ボタンをクリックします。

    セットアップ内容に問題がある場合は、［戻る］ボタンをクリックして設定を修正してください。

21. ［リモートインストールマネージャを使用した配布のセットアップ］画面で、リモートインストールマネージャを使用した配布に関する各種の情報を設定して［OK］ボタンをクリックします。

    デフォルトの設定を変更したい場合は、それぞれのタブを選択して、情報を入力してください。それぞれのタブで指定する内容、および指定できる値については、マニュアル「JP1/IT Desktop Management

2 導入・設計ガイド」の、セットアップ時のパラメーターの説明を参照してください。ここでは、各タブで設定する概要を示します。

通信関連

リモートインストールマネージャを使用した配布で使用するポート番号、エージェントおよび中継システムへのファイル転送のインターバルなどについて設定します。

サーバカスタマイズオプション

管理用サーバに同時に接続する下位システム数、ジョブを同時実行する下位システム数、下位システム数の起動監視、ファイル転送エラーの監視などについて設定します。

マルチキャスト配布

ジョブのマルチキャスト配布で使用するポート番号、マルチキャストアドレス、ジョブを配布するときのパケットのサイズなどについて設定します。

結果記録オプション

ジョブの実行結果を記録するかどうか、ID を指定したジョブのクライアントごとの実行結果を記録するかどうか、記録するジョブの実行状態などについて設定します。

システム構成関連

JP1/IT Desktop Management 2 のシステム構成情報が変更になった場合にその変更を自動的に下位システムのシステム構成情報に反映させるかどうか、JP1/IT Desktop Management 2 のシステム構成情報からホストを削除したときの履歴を保管するかどうかなどを設定します。複数サーバ構成の場合、[システム構成変更時の同期] が常に有効になります。

イベントサービス

実行したジョブの結果や JP1/IT Desktop Management 2 に異常が発生したことを JP1 イベントとして JP1/IM に通知するかどうか、ジョブや指令の正常終了、エラー発生を通知するかどうかなどについて設定します。

障害関連

ログの世代管理数、ログエントリの出力行数、Windows NT のイベントビューアに出力するメッセージの種別などについて設定します。

監査ログ

出力する監査ログの粒度を設定します。

22. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

[セットアップを終了します] 画面に、[コンポーネントを登録する]、[コンポーネントを自動的にアップデートする]、および [コンポーネントをパッケージとして登録する] が表示され、チェックできる場合があります。これらは、セットアップの実行タイミングやセットアップの種類で表示される項目が変わります。

[コンポーネントを登録する] が表示された場合

インストールセットを作成する場合、または管理用サーバから ITDM 互換配布でコンポーネントを配布する場合にチェックします。チェックすると、[セットアップを終了します] 画面が閉じたあとに [コンポーネントの登録] 画面が表示されます。[コンポーネントの登録] 画面でフォルダに登録

するコンポーネントを指定してください。インストーラーからセットアップを実行した場合は、［コンポーネントを登録する］は表示されず、コンポーネントは自動的に登録されます。

［コンポーネントを自動的にアップデートする］が表示された場合

管理用サーバへエージェントが接続した際に、［コンポーネントを登録する］で登録したコンポーネントをエージェントへ自動的に送信してアップデートする場合にチェックします。

［コンポーネントをパッケージとして登録する］が表示された場合

コンポーネントをパッケージとして登録する場合にチェックします。自動的にアップデートしない場合でも、コンポーネントをパッケージとして登録して ITDM 互換配布で配布することでアップデートできます。

これらの設定は、セットアップ終了後でも設定できます。セットアップ終了後に設定したい場合は、［スタート］メニューから［コンポーネントの登録］を起動してください。

コンポーネントのアップデートについては、「5.8　コンポーネントのアップデート方法」を参照してください。

セットアップが完了し、設定した内容で管理用サーバが動作するようになります。

ヒント

カスタムインストール後に初めてセットアップする場合、セットアップ時にデータベースが新規作成されます。

1.2.5　管理用中継サーバをセットアップする手順

JP1/IT Desktop Management 2 - Manager を管理用中継サーバとしてインストールした場合、データベースの作成や各種環境設定のために、インストール直後にセットアップを実行する必要があります。

管理用中継サーバをセットアップするには：

1. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
2. セットアップ開始画面で、［次へ］ボタンをクリックします。
3. ［セットアップの選択］画面で、セットアップの種類を選択して［次へ］ボタンをクリックします。
   インストール後の初回セットアップ時には、この画面は表示されません。
4. ［データベースの設定］画面で、データベースにアクセスするためのパスワードを変更するかどうかを選択して［次へ］ボタンをクリックします。
   パスワードを変更する場合は、現在のパスワードと新しいパスワードを入力し、手順 22.へ進んでください。
   手順 3.でセットアップの種類に「設定変更」を選択したときに表示されます。

インストール後の初回セットアップ時には、この画面は表示されません。

> **ヒント**
>
> ユーザー ID は、初回セットアップ時に設定したものが表示されます。パスワードは、任意の 28 文字以内の半角英数字（先頭の文字は英字）で指定します。ここで変更したパスワードは、JP1/IT Desktop Management 2 - Asset Console を使用する場合に必要になります。忘れないようにしてください。

5. [データベースの設定] 画面で、データベースにアクセスするためのユーザー ID とパスワードを設定して［次へ］ボタンをクリックします。

インストール後の初回セットアップ時、または手順 3.でセットアップの種類に「サーバの再構築」を選択したときに表示されます。

2 回目以降のセットアップ時には、この画面は表示されません。

> **ヒント**
>
> ユーザー ID は、8 文字以内の半角英数字（先頭の文字は英字）で指定します。デフォルトは「itdm2m」です。パスワードは、任意の 28 文字以内の半角英数字（先頭の文字は英字）です。ここで設定したユーザー ID とパスワードは、JP1/IT Desktop Management 2 - Asset Console を使用する場合に必要になります。忘れないようにしてください。

> **重要**
>
> ユーザー ID に「root」、「ALL」、「MASTER」、「netmdm」、および「PUBLIC」は指定しないでください。（大文字小文字は区別しません。）

6. [データベースの設定] 画面で、データベースにアクセスするための管理用サーバの IP アドレスとデータベースへのアクセス時のキャッシュ容量を設定して［次へ］ボタンをクリックします。

データベースへのアクセス時のキャッシュ容量は、インストール後の初回セットアップ時だけ選択できます。2 回目以降のセットアップ時は、初回セットアップ時に選択したキャッシュ容量が選択された状態となり、再設定できません。

> **ヒント**
>
> データベースへのアクセス時のキャッシュ容量には、目安として管理対象のコンピュータが 10,000 台までの場合は 1 ギガバイトを、10,000～30,000 台の場合は 16 ギガバイトを指定してください。

7. [フォルダの設定] 画面で、JP1/IT Desktop Management 2 - Manager が使用する各種フォルダを指定して［次へ］ボタンをクリックします。

8. [操作ログの設定] 画面で、操作ログを取得するかどうかを設定して［次へ］ボタンをクリックします。

操作ログを取得しない場合は、手順 12.へ進んでください。

9. [操作ログの設定] 画面で、操作ログを保管するかどうかを設定して、[次へ] ボタンをクリックします。

10. [操作ログの設定] 画面で、管理対象の機器の台数、操作ログのデータベース格納最大日数、および操作ログのデータベースフォルダを設定して、[次へ] ボタンをクリックします。

11. 操作ログの検索性能を向上させたい場合、データベースのキャッシュを追加できます。必要に応じて、[操作ログの設定] 画面で追加するキャッシュ容量を設定して、[次へ] ボタンをクリックします。

12. [保存用の変更履歴の出力設定] 画面で、保存用の変更履歴を定期的に出力するかどうかを設定して [次へ] ボタンをクリックします。

13. [ポート番号の設定] 画面で、JP1/IT Desktop Management 2 - Manager が使用するポート番号を設定して [次へ] ボタンをクリックします。

    設定した各ポート番号は、自サーバ、上位の管理用サーバ、および下位の管理用中継サーバにも同じポート番号を設定してください。

14. [アドレス解決の設定] 画面で、ホスト間で通信するときに通信相手のコンピュータを決定する情報の種類（ホスト名または IP アドレス）を選択します。ホスト名を選択した場合は、アドレス解決の方法およびアドレス解決ができなかったときの処理を設定します。

    ここで設定する通信相手のコンピュータを決定する情報の種類を運用キーと呼びます。

15. [管理用中継サーバの設定] 画面で、接続先の上位の管理用サーバを指定します。また、管理対象のコンピュータから収集した操作ログ情報と USB デバイスの登録情報を、上位の管理用サーバに通知するかどうかを選択します。

    [ホスト名または IP アドレス] は、上位の管理用サーバの [アドレス解決の設定] 画面で選択した運用キーで指定してください。

16. [管理用中継サーバの通信設定] 画面で、上位サーバへの通知間隔、ポーリングの間隔、無通信の監視、および通信エラー時のリトライをするかどうかを設定して [次へ] ボタンをクリックします。

    JP1/IT Desktop Management 2 - Manager のインストール時の [エージェントのコンポーネント設定] ダイアログで [リモコンエージェント] を選択していない場合は、手順 19.へ進んでください。

17. [管理用中継サーバのリモートコントロール設定] 画面で、管理用中継サーバのリモートコントロールの開始時の処理、接続設定、および接続モードの設定をして [次へ] ボタンをクリックします。

18. リモートコントロールに関する詳細を設定したい場合は、[管理用中継サーバのリモートコントロール設定] 画面でそれぞれ設定をして [次へ] ボタンをクリックします。

    リモートコントロールを許可するコントローラを制限したい場合は、[コントロール許可の設定] の [追加] ボタンをクリックし、許可するコントローラのホスト名または IP アドレスを入力して追加してください。

    コントローラとの接続時にユーザー認証をしたい場合は、[ユーザー設定] の [追加] ボタンをクリックし、許可ユーザーの追加をしてください。

19. [ユーザー管理の設定] 画面で、JP1/Base を使用してユーザー管理するかどうかを選択します。選択した場合は、JP1/IT Desktop Management 2 で使用する JP1 ユーザーが関連づけられている JP1 資源グループ名を指定します。

> **ヒント**
>
> JP1/Base を使用してユーザー管理する場合は、セットアップ開始前に JP1 ユーザー、JP1 資源グループ、および JP1 権限レベルを JP1/Base の認証サーバで設定しておく必要があります。JP1/Base を使用してユーザー管理する構成システムを構築する流れについては、「2.7.1　JP1 認証を使用した構成システムを構築する流れ」を、認証サーバでの設定手順についてはマニュアル「JP1/Base 運用ガイド」を参照してください。

20. [その他の設定] 画面で、操作画面に表示される通貨単位、および ITDM 互換配布の機能を使用するときに流量制御するかどうかを設定して［次へ］ボタンをクリックします。

21. [その他の設定] 画面で、アカウントをロックする連続入力失敗の回数、ユーザパスワードの有効日数、および操作画面での資産情報の操作を抑止するかどうかを設定して［次へ］ボタンをクリックします。

22. [セットアップの確認] 画面で、セットアップ内容に問題がないことを確認し、［次へ］ボタンをクリックします。

    セットアップ内容に問題がある場合は、［戻る］ボタンをクリックして設定を修正してください。

23. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、リモートインストールマネージャを使用した配布に関する各種の情報を設定して［次へ］ボタンをクリックします。

    ［次へ］ボタンをクリックすると、セットアップが実行されます。［キャンセル］ボタンをクリックすると、セットアップが中止され、画面が閉じられます。

    デフォルトの設定を変更したい場合は、それぞれのタブを選択して、情報を入力してください。それぞれのタブで指定する内容、および指定できる値については、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」の、セットアップ時のパラメーターの説明を参照してください。ここでは、各タブで設定する概要を示します。

    通信関連

    リモートインストールマネージャを使用した配布で使用するポート番号、エージェントおよび中継システムへのファイル転送のインターバルなどについて設定します。

    サーバカスタマイズオプション

    管理用サーバに同時に接続する下位システム数、ジョブを同時実行する下位システム数、下位システム数の起動監視、ファイル転送エラーの監視などについて設定します。

    マルチキャスト配布

    ジョブのマルチキャスト配布で使用するポート番号、マルチキャストアドレス、ジョブを配布するときのパケットのサイズなどについて設定します。

    結果記録オプション

    ジョブの実行結果を記録するかどうか、ID を指定したジョブのクライアントごとの実行結果を記録するかどうか、記録するジョブの実行状態などについて設定します。

システム構成関連

JP1/IT Desktop Management 2 のシステム構成情報からホストを削除したときの履歴を保管するかどうかなどを設定します。

イベントサービス

実行したジョブの結果や JP1/IT Desktop Management 2 に異常が発生したことを JP1 イベントとして JP1/IM に通知するかどうか、ジョブや指令の正常終了、エラー発生を通知するかどうかなどについて設定します。

障害関連

ログの世代管理数、ログエントリの出力行数、Windows NT のイベントビューアに出力するメッセージの種別などについて設定します。

監査ログ

出力する監査ログの粒度を設定します。

24. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

[セットアップを終了します] 画面に、[コンポーネントを登録する]、[コンポーネントを自動的にアップデートする]、および [コンポーネントをパッケージとして登録する] が表示され、チェックできる場合があります。これらは、セットアップの実行タイミングやセットアップの種類で表示される項目が変わります。

[コンポーネントを登録する] が表示された場合

インストールセットを作成する場合、または管理用サーバから ITDM 互換配布でコンポーネントを配布する場合にチェックします。チェックすると、[セットアップを終了します] 画面が閉じたあとに [コンポーネントの登録] 画面が表示されます。[コンポーネントの登録] 画面でフォルダに登録するコンポーネントを指定してください。インストーラーからセットアップを実行した場合は、[コンポーネントを登録する] は表示されず、コンポーネントは自動的に登録されます。

[コンポーネントを自動的にアップデートする] が表示された場合

管理用サーバへエージェントが接続した際に、[コンポーネントを登録する] で登録したコンポーネントをエージェントへ自動的に送信してアップデートする場合にチェックします。

[コンポーネントをパッケージとして登録する] が表示された場合

コンポーネントをパッケージとして登録する場合にチェックします。自動的にアップデートしない場合でも、コンポーネントをパッケージとして登録して ITDM 互換配布で配布することでアップデートできます。

これらの設定は、セットアップ終了後でも設定できます。セットアップ終了後に設定したい場合は、[スタート] メニューから [コンポーネントの登録] を起動してください。

コンポーネントのアップデートについては、「5.8　コンポーネントのアップデート方法」を参照してください。

セットアップが完了し、設定した内容で管理用中継サーバが動作するようになります。

ヒント

初めてセットアップする場合、セットアップ時にデータベースが新規作成されます。

1.3　製品ライセンスを登録する

ここでは、製品ライセンスを登録する方法について説明します。また、製品ライセンスを削除する手順についても説明します。

1.3.1　製品ライセンスを登録する手順

製品ライセンスを JP1/IT Desktop Management 2 に登録することで、登録したライセンス数分だけ機器を管理できるようになります。

なお、複数サーバ構成では、統括管理用サーバおよびライセンスの登録を許可されている管理用中継サーバだけに、製品ライセンスを登録できます。

製品ライセンスを登録するには：

1. ログイン画面を表示します。
2. ログイン画面の［ライセンス］ボタンをクリックします。
3. 表示された［製品ライセンス情報］ダイアログで［ライセンスを登録］ボタンをクリックします。
4. 表示された［ファイルアップロード］画面でライセンスキーファイルを選択して、［開く］ボタンをクリックします。
5. ライセンス登録が完了すると［ライセンス登録完了］ダイアログが表示するので、［OK］ボタンをクリックします。

ライセンス登録が完了します。

ヒント

ライセンスキーファイルは、管理用サーバをリプレースする際にも必要となります。ライセンスキーファイルを紛失された場合、再発行できませんので、必ず保管しておいてください。リプレースの詳細については、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の「管理用サーバをリプレースする」の説明を参照してください。

ヒント

初回登録時以外は、設定画面の［製品ライセンス］－［製品ライセンスの設定］画面でもライセンスを登録できます。［ライセンスを登録］ボタンをクリックしてください。表示されたダイアログでライセンスキーファイルを選択して、［開く］ボタンをクリックすると、ライセンス登録が完了します。

ヒント

初回登録時以外は、画面左上の［ヘルプ］－［製品ライセンス情報］から表示される［製品ライセンス情報］ダイアログでもライセンスを登録できます。［ライセンスを登録］ボタンをクリックしてください。表示されたダイアログでライセンスキーファイルを選択して、［開く］ボタンをクリックすると、ライセンス登録が完了します。

関連リンク

- 1.3.2　製品ライセンスを追加する手順

1.3.2　製品ライセンスを追加する手順

組織内の機器を JP1/IT Desktop Management 2 で管理するためには、製品ライセンスが必要です。

製品ライセンスが不足した場合は、製品ライセンスを追加購入してください。購入した製品ライセンスを登録することで、ライセンスを追加できます。

1.3.3　管理用中継サーバに製品ライセンスの情報を設定する手順

製品ライセンスの情報を設定した管理用中継サーバでは、自サーバが共有元であるライセンスの共有範囲について、製品ライセンスを管理できるようになります。管理用中継サーバに製品ライセンスの情報を設定するには、統括管理用サーバでdistributelicense コマンドを実行します。distributelicense コマンドの詳細については、関連リンクを参照してください。

ヒント

distributelicense コマンドでライセンスの登録を許可した管理用中継サーバには、コマンド実行後に製品ライセンスを登録する必要があります。

ヒント

すべての管理用中継サーバへの設定が完了したかどうかは、統括管理用サーバのイベント画面で確認できます。また、特定の管理用中継サーバへの設定が完了したかどうかは、各管理用中継サーバの操作画面のイベント画面で確認できます。設定に失敗した場合は、イベントの詳細情報を確認して、distributelicense コマンドを再実行してください。

関連リンク

- 1.3.1　製品ライセンスを登録する手順
- 8.11　distributelicense（ライセンスの分配）

1.4　操作画面にログインする

ここでは、JP1/IT Desktop Management 2 の操作画面にログインする方法について説明します。

1.4.1　ログインする手順

ログイン画面ではユーザーの認証をします。認証に成功すると JP1/IT Desktop Management 2 にログインできます。

初めてログインする場合は、JP1/IT Desktop Management 2 のライセンスを登録する必要があります。ライセンスを登録するには、[ライセンス] ボタンをクリックしてください。

ログインするには：

1. Web ブラウザのアドレスバーに次の URL を入力します。

   http※1*://管理用サーバの IP アドレスまたはホスト名:管理者のコンピュータからの接続受付ポート番号※2*※/jp1itdm/jp1itdm.jsp

   注※1　Microsoft Entra ID を使用する場合、ITDM2 の管理画面を https 化する必要があります。管理画面を HTTPS 化する手順については、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の操作画面に HTTPS で接続する手順の説明を参照してください。

   なお、リモートインストールマネージャ、パッケージャ、およびネットワーク制御コマンドは、JP1/IT Desktop Management 2 - Manager と HTTP 通信を使用しています。そのため、管理用サーバの HTTP 通信用のポート番号（デフォルト 31080）はブロックしないでください。

   注※2　セットアップの［ポート番号の設定］画面で設定したポート番号です。簡単インストール時にはデフォルトの「31080」が設定されています。管理画面を https する場合のポート番号は注※1 に記載のマニュアルを参照してください。

2. ユーザー ID とパスワードを入力します。

3. [ログイン] ボタンをクリックします。

ユーザーアカウントの認証に成功するとホーム画面が表示されます。

ITDM2 認証の場合、デフォルトのユーザー ID は「system」、パスワードは「manager」です。デフォルトのユーザー ID とパスワードでログインすると［パスワードの変更］ダイアログが表示されるので、パスワードを変更してください。なお、新しく追加したユーザーアカウントで初めてログインする場合も、[パスワードの変更] ダイアログが表示されます。

JP1 認証でログインする場合は、あらかじめ JP1/Base の認証サーバに登録した JP1 ユーザーでログインしてください。

ヒント

ITDM2 認証の場合、パスワードの有効期限は、セットアップ時に［その他の設定］画面で、ユーザーパスワードの有効日数として指定した日数です。有効期限の 7 日前からログイン時にパスワードの変更が要求されるので、新しいパスワードに変更してください。パスワードの有効期限を過ぎると、ログイン時に［パスワードの変更］ダイアログが表示されます。

重要

ITDM2 認証の場合、セットアップ時に［その他の設定］画面で、アカウントをロックする連続入力失敗の回数が指定されている場合に、指定された回数続けてログインに失敗するとユーザーアカウントがロックされます。ユーザーアカウントがロックされると、ロックが解除されるまでそのユーザーアカウントではログインできません。

関連リンク

- 1.4.4　ユーザーアカウントのロックを解除する手順

1.4.2　デフォルトパスワードを変更する手順

JP1/IT Desktop Management 2 にビルトインアカウントで初めてログインするとき、または新規に作成したユーザーアカウントで初めてログインするときは、パスワードの変更が要求されます。また、ユーザーアカウント管理権限を持つ管理者によって、ユーザーアカウントのパスワードが変更された場合、次回ログイン時にパスワードの変更が要求されます。セキュリティ確保のため、デフォルトパスワードは必ず変更してください。パスワードを変更すると、次回のログイン時から変更後のパスワードを使う必要があります。

ヒント

パスワードの有効期限は、セットアップ時に［その他の設定］画面で、ユーザーパスワードの有効日数として指定した日数です。有効期限の 7 日前からログイン時にパスワードの変更が要求されるので、新しいパスワードに変更してください。パスワードの有効期限を過ぎると、ログイン時に［パスワードの変更］ダイアログが表示されます。

ヒント

脆弱なパスワードを設定すると、自分のユーザーアカウントが不正に使われるおそれがあります。例えば、次のような設定方針で強固なパスワードを利用することをお勧めします。

- 大文字、小文字、数字、記号の組み合わせである
- 連続した文字列（12345 など）ではない

- 自分や親しい人の名前または誕生日、辞書に掲載されている単語ではない

ログイン中のユーザーアカウントのパスワードを変更したい場合は、［ログアウト］ボタンの左側にあるユーザー ID のリンクをクリックして表示されるダイアログからパスワードを変更できます。

ユーザーアカウント管理権限を持つ管理者の場合は、設定画面の［ユーザー管理］－［ユーザーアカウントの管理］画面から、各ユーザーアカウントのパスワードを変更できます。

1.4.3 ユーザーアカウントの情報を設定する手順

JP1/IT Desktop Management 2 にログインしたあとは、ユーザーアカウントの情報を設定してください。

［ログアウト］ボタンの左側にあるユーザー ID のリンクをクリックすると、表示されるダイアログでユーザーアカウントの情報を編集できます。

ユーザーアカウントには、次の情報を設定します。

- ユーザーアカウントを使用する利用者名
- 利用者のメールアドレス

ユーザーアカウントにメールアドレスを設定しておくと、そのメールアドレスに対してダイジェストレポートを送付したり、探索完了、イベントの発生を通知したりできます。操作画面を頻繁にチェックすることなく運用状況を把握できるようになるので、メールアドレスを設定しておくことをお勧めします。なお、これらの通知を受け取るには、メールアドレスの設定のほかに、ダイジェストレポートの送付先の設定、探索条件の設定、およびイベント通知の設定が必要です。

ヒント

ユーザーアカウントの情報は、設定画面の［ユーザー管理］－［ユーザーアカウントの管理］画面からも設定できます。［ユーザーアカウントの管理］画面では、ユーザーアカウントを新規に追加することもできます。

1.4.4 ユーザーアカウントのロックを解除する手順

アカウントをロックする連続入力失敗の回数が指定されている場合に、指定された回数続けてログインに失敗するとユーザーアカウントがロックされます。ロックされたユーザーアカウントを使用するためには、ロックを解除する必要があります。

ユーザーアカウントのロックを解除するには：

1. ユーザーアカウント管理権限を持つユーザーでログインします。

2. 設定画面の［ユーザー管理］－［ユーザーアカウントの管理］画面を表示します。

3. ロックされたユーザーアカウントの［編集］ボタンをクリックします。

4. 表示されたダイアログで、［アカウントロック状態］の［解除］を選択します。

> **ヒント**
>
> ［アカウントロック状態］が表示され［解除］を選択できるのは、ロックされたユーザアカウントだけです。

ユーザーアカウントのロックが解除されます。

> **ヒント**
>
> ユーザーアカウント管理権限を持つ別のユーザーアカウントがない場合は、管理用サーバを再起動してください。ユーザーアカウントのロックが解除されます。

1.5　組織内の機器を把握する

エージェントを導入するコンピュータを決定するために、組織内の機器の現状を把握する必要があります。

管理台帳がメンテナンスできていない、管理台帳が手もとにないなど、機器の現状を把握できていない場合は、JP1/IT Desktop Management 2 を利用して機器を探索してください。探索によって組織内の機器の情報を収集できます。組織内の機器を把握したら、エージェントの導入計画を立案します。なお、探索と同時にエージェントを自動配信することもできます。

管理台帳などで組織内の機器の現状を把握できている場合は、機器を探索する必要はありません。エージェントの導入計画を立案します。

関連リンク

- 1.5.2　エージェントの導入計画を立案する

1.5.1　ネットワークに接続されている機器を探索する手順

機器を探索する方法の一つです。ネットワークに接続されている機器を探索できます。

設定画面の［機器の探索］－［探索条件の設定］－［ネットワークの探索］画面で、探索する IP アドレスの範囲や探索時に使用する認証情報などを設定します。［探索を開始］ボタンをクリックすると、設定したスケジュールに従って探索が開始されます。

ネットワークに接続されている機器を探索するには：

1. 設定画面の［機器の探索］－［探索条件の設定］－［ネットワークの探索］画面を表示します。
2. ［探索範囲の設定内容］で、探索したい IP アドレスの範囲を設定します。

   デフォルトで、「管理用サーバセグメント」という名称の探索範囲が設定されています。管理用サーバセグメントとは、管理用サーバが含まれるネットワークセグメントのことです。

> **重要**
>
> 期間を指定して集中的に探索する場合は、探索範囲に含まれる IP アドレスの数が 50,000 件以下になるように設定してください。IP アドレスの数が 50,000 件よりも多いと、ネットワーク探索が停止することがあります。
>
> 50,000 件より多い IP アドレスを探索する場合は、「期間を指定して集中的に探索する」を設定しないでネットワーク探索を実施してください。

重要

複数サーバ構成の場合、異なる管理用サーバに同じ探索範囲を設定しないでください。それぞれの管理用サーバが機器を発見したタイミングで、機器情報の管理元が意図しないで変更されるため、機器情報を正常に管理できなくなるおそれがあります。

3. [認証情報] で、探索時に使用する認証情報を設定します。

4. [探索範囲の設定内容] で、各探索範囲に使用する認証情報を設定します。

重要

探索範囲の機器に、ログオンを一定回数失敗し、アカウントをロックするような設定がされている場合は、探索範囲ごとに特定の認証情報を割り当ててください。[すべて] を選択すると、機器に対してすべての認証情報を試します。そのため、利用者が知らないうちにアカウントがロックされてしまうおそれがあります。

重要

[すべて] を選択すると、認証情報を 1 つずつ使用して機器にアクセスを試みます。そのため、通信回数が増えネットワークの負荷が高くなります。ネットワークの負荷を考慮した上で選択してください。

5. [探索スケジュール] で探索スケジュールを設定します。

6. [発見した機器への操作] で、発見した機器を自動的に管理対象にするか、エージェントを自動配信するかを設定します。

7. 探索の完了を管理者にメールで通知したい場合は、[完了通知] で通知先を設定します。

8. 画面右上の [探索を開始] ボタンをクリックします。

9. 表示されるダイアログで探索の範囲を確認して、[OK] ボタンをクリックします。

[期間を指定して集中的に探索する] をチェックすると、指定した期間は探索が終了したらすぐに次の探索が開始され、絶え間なくネットワークが探索されるようになります。このため、運用の初期段階で、できるだけ多くの機器を発見したい場合にチェックすることをお勧めします。例えば、1 回目の探索時に電源が OFF のため発見できなかった機器があっても、探索を繰り返すことで、2 回目以降の探索で発見できる可能性が高くなります。

重要

[期間を指定して集中的に探索する] をチェックすると、探索が終了したらすぐに次の探索を繰り返します。そのため、設定した期間中はネットワークの負荷が高くなります。ネットワークの負荷を考慮した上で選択してください。

［機器の探索］－［探索履歴の確認］－［ネットワークの探索］画面に移動し、設定したスケジュールに従って探索が実行されます。

ヒント

冗長構成のネットワーク機器に対してネットワーク探索を実施した場合、機器が二重登録される場合があります。どちらかの機器を管理したくない場合は、それを除外対象機器として設定してください。

関連リンク

- 4.1.1　探索条件を設定する手順（ネットワークの探索）
- 1.7.3　機器の探索状況の確認

1.5.2　エージェントの導入計画を立案する

組織内の機器を把握したら、どのコンピュータにエージェントを導入するか、どのような方法でエージェントを導入するかを検討します。

エージェントを導入するコンピュータ

組織内で利用されているコンピュータのうち、JP1/IT Desktop Management 2 によるセキュリティ管理やソフトウェア配布の対象としたいコンピュータにエージェントを導入します。

エージェントを導入したコンピュータは、自動的に JP1/IT Desktop Management 2 の管理対象になります。コンピュータを管理対象にすると JP1/IT Desktop Management 2 のライセンスが消費されるため、ライセンス数を考慮して、エージェントを導入するコンピュータを決定してください。

ヒント

管理用サーバをセキュリティ管理の対象にする場合、利用者のコンピュータと同様にエージェントをインストールします。

ヒント

JP1/IT Desktop Management 2 では、ライセンス保有数は OS ごと（Windows 用、Linux 用、UNIX 用の 3 種類）に管理されますが、ライセンス使用数は OS の種類に関係なくまとめて管理されます。なお、Mac OS は Windows 用のライセンスを共用できます（Windows 用として購入したライセンスを Mac OS のコンピュータに割り当てられます）。ただ、Mac OS のコンピュータに割り当てた分、Windows のコンピュータに割り当てられるライセンスは減少します。

例えば、次のとおり合計 520 のライセンスを登録したとします。

- Windows 用エージェントのライセンス：500
- Linux 用エージェントのライセンス：10
- UNIX 用エージェントのライセンス：10

このとき、Windows のコンピュータ 510 台を管理対象にすると、合計のライセンス保有数（520）は超過しませんが、Windows 用エージェントのライセンス保有数（500）を超過してしまいます。このような場合は、次のどちらかの方法で対処する必要があります。

- Windows 用エージェントのライセンスを追加で 10 以上登録する
- 超過している Windows の機器（10 台以上）を除外対象にする

OS ごとのライセンス使用数が超過しているかどうかは、設定画面の［製品ライセンス］－［製品ライセンスの設定］に表示される［ライセンス保有数］と、機器画面の［機器一覧（機器種別）］に表示される OS ごとの管理対象機器の台数で確認してください。

エージェントの導入方法

エージェントの導入方法には、手動でインストールする方法と自動でインストールする方法があります。

どのインストール方法を選択するかは、インストールする際に重視するポイントによって異なります。各方法を確認して、ご使用の環境に合ったインストール方法を決定してください。

エージェントを手動でインストールする

まずインストールセットを作成します。その後、インストールセットを利用してコンピュータにエージェントをインストールします。手動でインストールするには、次の 7 種類の方法があります。

- Web サーバでエージェントを公開する
- ファイルサーバでエージェントを公開する
- エージェントインストール用の媒体（CD-R や USB メモリ）を配布する
- メールの添付ファイルでエージェントを配布する
- ログオンスクリプトを利用してエージェントをインストールする
- ディスクコピーでエージェントをインストールする
- エージェントを提供媒体からインストールする

エージェントを自動でインストールする

管理用サーバから各コンピュータに対して、エージェントを自動で配信します。自動でインストールするには、次の 2 種類の方法があります。

- 探索と同時にエージェントを自動配信する
- エージェント未導入のコンピュータに個別配信する

関連リンク

- 1.6　エージェントを手動でインストールする
- 1.7　エージェントを自動でインストールする

1.6　エージェントを手動でインストールする

エージェントを手動でインストールするためには、まずエージェントのインストールセットを作成します。その後、インストールセットを利用してコンピュータにエージェントをインストールします。

インストールセットの作成方法については、「1.6.1　インストールセットを作成する手順」を参照してください。

インストールセットを利用したエージェントのインストール方法は複数あります。インストール方法は、インストールする際に重視するポイントによって異なります。各方法を確認して、ご使用の環境に合ったインストール方法を決定してください。

利用者にインストールの作業だけをさせる場合

インストールセットを利用者が起動するように環境を準備しておくことで、利用者にセットアップの作業をさせることなく、エージェントをインストールします。利用者にインストールの作業だけをさせる方法を次に示します。

- 1.6.3　Web サーバでエージェントを公開する
- 1.6.4　ファイルサーバでエージェントを公開する
- 1.6.5　エージェントインストール用の媒体（CD-R や USB メモリ）を配布する
- 1.6.6　メールの添付ファイルでエージェントを配布する

利用者にインストールの作業自体をさせたくない場合

インストールセットをファイルサーバに格納します。その後、ドメインコントローラにログオンスクリプトを登録しておくことで、利用者が Windows にログオンしたときに、自動的にエージェントがインストールされます。利用者にインストールの作業自体をさせない方法を次に示します。

- 1.6.7　ログオンスクリプトを利用してエージェントをインストールする

利用者にコンピュータを配布する前にインストールしたい場合

利用者にコンピュータを配布する前に、配布するコンピュータのモデルとなるコンピュータに、インストールセットを使ってエージェントをインストールします。次に、モデルとなるコンピュータのディスク全体を、専用のツールやソフトウェアを使用して配布前のコンピュータにディスクコピーします。利用者にコンピュータを配布する前にインストールする方法を次に示します。

- 1.6.8　ディスクコピーでエージェントをインストールする

これらのほかに、提供媒体を使用してエージェントを手動でインストールする方法もあります。この場合、セットアップの作業も必要です。

なお、Citrix XenApp、Microsoft RDS サーバにエージェントをインストールする場合は、インストールセットを使ってインストールする必要があります。

1.6.1　インストールセットを作成する手順

組織内のコンピュータにエージェントをインストールして管理する場合、インストールセットを作成します。インストールセットは Web ポータルに公開して利用者にダウンロードしてもらったり、CD/DVD に記録して配布したりします。利用者はインストールセットを自分のコンピュータで実行することで、簡単にエージェントをインストールできます。

インストールセットを作成する手順を次に示します。

インストールセットを作成するには：

1. 画面上部の［実行］メニュー－［機器の管理を始めましょう］を選択します。
2. 表示されたウィザードで［次へ］ボタンをクリックします。
3. コンピュータに適用したいインストールセットを作成するために、ウィザードに沿って設定します。

   次に示す項目を設定します。項目を設定するごとに［次へ］ボタンをクリックしてください。

   エージェント設定を選択する

   ［エージェント設定名］からコンピュータに適用したいエージェント設定を選択します。

   エージェント設定とは、各エージェントの動作を設定したものです。エージェント設定は、設定画面の［エージェント］－［Windows エージェント設定とインストールセットの作成］画面で追加できます。

   エージェント設定を選択すると、エージェントのインストール先を変更できます。

   インストール先を変更したい場合は、［インストールフォルダ］にエージェントのインストール先を入力してください。

   また、共有型 VDI 方式の仮想コンピュータへエージェントをインストールする場合は、［ホスト識別子生成時の設定］を設定してください。

   アカウントの設定

   エージェントをインストールするために、Administrator 権限を持つアカウント情報を設定するかどうかを選択できます。この設定は、OS が Windows XP、および Windows Server 2003 のコンピュータにエージェントをインストールする場合に限り有効になります。

   エージェントをインストールするためには、対象コンピュータの Administrator 権限が必要です。

   ここで、Administrator 権限を持つアカウントを設定すると、Administrator 権限を持たない利用者がエージェントをインストールするとき、設定したアカウントでインストールが実行されます。Administrator 権限は、エージェントをインストールするときだけ使用されるため、権限を制限したい利用者のコンピュータにエージェントをインストールする場合に便利です。

   インストールするコンポーネントの設定

   インストールするコンポーネントの種別（エージェントとしてインストールするか、中継システムとしてインストールするかの選択）とサブコンポーネントのリモコンエージェントをインストールするかどうかを指定します。

登録先の ID の設定

エージェントを登録する ID（配布管理システムからのジョブを受け取るためのグループ）を指定します。

展開するファイルの設定

エージェントのインストールと同時に展開するファイルと展開先のフォルダを指定します。

自動実行するファイルの設定

エージェントのインストール後に自動実行するファイル、自動実行に必要なファイル、および引数を指定します。

> **ヒント**
>
> 秘文などの連携製品を自動実行でエージェントにインストールする場合は、前準備として、管理者のコンピュータの`C:¥DATA`下などに秘文（秘文 DC または秘文 DE）などの連携製品のインストール媒体を作成して、フォルダごとまたはフォルダ配下の全ファイルを ZIP 化しておきます。その ZIP ファイルを自動実行するファイルとして設定することで、エージェントのインストール後に自動実行で秘文などの連携製品をエージェントにインストールできます。秘文のインストール媒体の作成方法の詳細については、マニュアル「JP1/秘文 セットアップガイド（管理者用）」を参照してください。

上書きインストールの設定

エージェントがすでにインストールされている場合、上書きインストールするかどうかを設定します。

4. **設定内容を確認して、［作成］ボタンをクリックします。**

［インストールセットの作成］ダイアログが表示されます。

5. **［インストールセットの作成］ダイアログで［保存］ボタンをクリックします。**

保存するインストールセットのデフォルトのファイル名は「ITDM2Agt.exe」です。

6. **［完了］画面が表示されたら、［閉じる］ボタンをクリックしてウィザードを終了します。**

インストールセットが作成され、ダウンロードが開始されます。

> **ヒント**
>
> 設定画面の［エージェント］－［Windows エージェント設定とインストールセットの作成］画面でも、インストールセットを作成できます。コンピュータに適用したいエージェント設定の［インストールセットを作成］ボタンをクリックしてください。表示されるダイアログで情報を入力して［作成］ボタンをクリックすると、インストールセットが作成され、ダウンロードが開始されます。

ヒント

接続先設定ファイル（itdmhost.conf）または上位接続先情報ファイル（dmhost.txt）を作成して、JP1/IT Desktop Management 2 - Manager のデータフォルダに格納しておくと、インストールセットの作成時にインストールセットに取り込まれます。接続先設定ファイル（itdmhost.conf）については、マニュアル「JP1/IT Desktop Management 2 構築ガイド」のエージェントの接続先を自動設定する手順の説明を参照してください。上位接続先情報ファイルの詳細については、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、エージェントの接続先の自動変更についての説明を参照してください。

ヒント

インターネットゲートウェイ接続先設定ファイル（itdmigw.conf）をインストールセットに取り込む場合は、手順 3 の「展開するファイルの設定」で指定してください。[展開するファイル] には作成したインターネットゲートウェイ接続先設定ファイルを、[展開先フォルダ] には「%ITDM2AGT%¥MASTER¥DB」をそれぞれ指定します。インターネットゲートウェイ接続先設定ファイル（itdmigw.conf）の詳細については、「1.6.12　エージェントのインターネットゲートウェイ経由の接続先を自動設定する手順」を参照してください。

重要

OS が UNIX、Mac のコンピュータにはインストールセットを使ってエージェントをインストールできません。

関連リンク

- 4.1.3　エージェント設定を追加する手順
- 1.6.2　エージェントをコンピュータに導入する方法

1.6.2　エージェントをコンピュータに導入する方法

インストールセットを作成したら、インストールセットを利用してエージェントをコンピュータに導入します。

インストールセットを利用してエージェントを導入できるのは、インストールセットを作成した管理用サーバの直下のコンピュータだけです。

インストールセットの利用例を次に示します。

Web サーバでエージェントを公開する

Web サーバにインストールセットを格納して、組織内のサイトからダウンロードできるようにします。コンピュータの利用者は、組織内のサイトからインストールセットをダウンロードしてエージェントをインストールします。

ファイルサーバでエージェントを公開する

ファイルサーバにインストールセットを格納して、ファイルサーバにアクセスしてダウンロードできるようにします。コンピュータの利用者は、ファイルサーバからインストールセットをダウンロードしてエージェントをインストールします。

エージェントインストール用の媒体を配布する

インストールセットを格納した媒体（CD-R や USB メモリ）を作成して、この媒体をコンピュータの利用者に配布します。コンピュータの利用者は、受け取った媒体からエージェントをインストールします。

メールの添付ファイルでエージェントを配布する

インストールセットをメールに添付して、コンピュータの利用者に送信します。メールを受け取ったコンピュータの利用者は、添付されたファイルを実行してエージェントをインストールします。

ログオンスクリプトを利用してエージェントをインストールする

インストールセットを作成して、ドメインコントローラにインストールセットを実行するログオンスクリプト用のバッチファイルを格納します。コンピュータの利用者が OS にログオンしたときに、自動的にエージェントがインストールされます。

ディスクコピーでエージェントをインストールする

モデルとなるコンピュータにエージェントをインストールします。このコンピュータのディスク全体をバックアップします。エージェントを導入するコンピュータにバックアップデータをリストアすることでエージェントがインストールされます。

関連リンク

- 1.6.3　Web サーバでエージェントを公開する
- 1.6.4　ファイルサーバでエージェントを公開する
- 1.6.5　エージェントインストール用の媒体（CD-R や USB メモリ）を配布する
- 1.6.6　メールの添付ファイルでエージェントを配布する
- 1.6.7　ログオンスクリプトを利用してエージェントをインストールする
- 1.6.8　ディスクコピーでエージェントをインストールする

1.6.3　Web サーバでエージェントを公開する

管理者は、作成したインストールセットを組織内の Web サーバに格納したあと、組織内のサイトからダウンロードできるようにして、利用者に公開します。

利用者はそのページにアクセスしてエージェントをインストールします。

> **ヒント**
>
> Web サーバに格納したファイルを直接ダウンロードできる URL を公開する方法もあります。

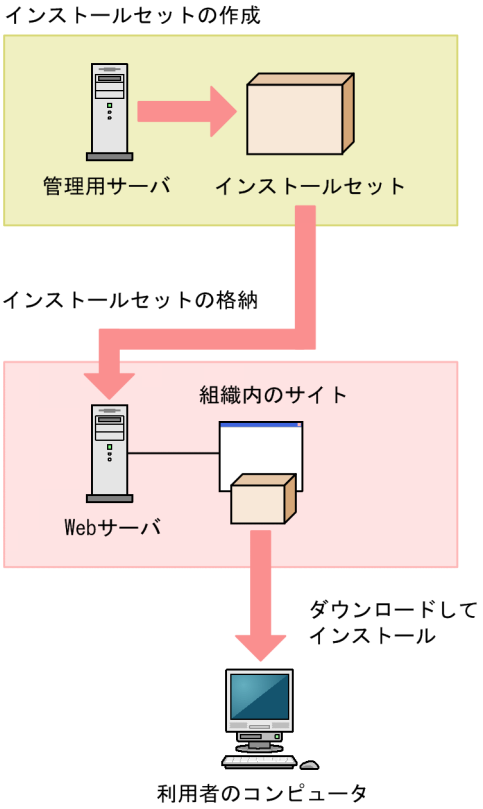
メリット

利用者にサイトの URL を一斉展開することで、多くのコンピュータに素早くエージェントをインストールできます。また、Web システムを利用するので、アクセス制御しなくてもサーバ側にセキュリティ上の問題が発生しません。

デメリット

組織内に Web サーバを構築できる環境、および Web サーバにアクセスできる環境が必要です。

Web サーバからエージェントをインストールするイメージを、次の図に示します。



関連リンク

- 1.6.1　インストールセットを作成する手順
- 1.7.1　エージェントのインストール状況を確認する流れ

1.6.4　ファイルサーバでエージェントを公開する

管理者は、ファイル共有できるファイルサーバにインストールセットを格納します。利用者は、ファイルサーバにアクセスしてエージェントをインストールします。

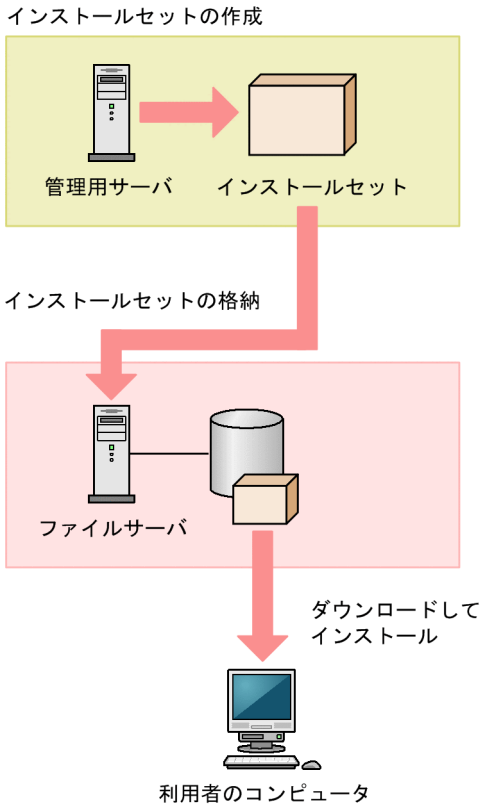
メリット

利用者にインストールセットの格納先を一斉展開することで、多くのコンピュータに素早くエージェントをインストールできます。

デメリット

ファイル共有できる環境が必要です。また、ファイル共有の参照先を公開するため、公開の範囲や権限などサーバ側で確実にアクセス制御をしておく必要があります。

ファイル共有でエージェントをインストールするイメージを、次の図に示します。



ヒント

ネットワークドライブ上にあるオフラインインストール用媒体を実行する場合、管理者権限が必要です。

関連リンク

- 1.6.1　インストールセットを作成する手順
- 1.7.1　エージェントのインストール状況を確認する流れ

1.6.5　エージェントインストール用の媒体（CD-R や USB メモリ）を配布する

管理者は、インストールセットのデータを媒体（CD-R や USB メモリ）に書き込みます。そして、その媒体を利用者に配布します。利用者は、配布された媒体を使用してエージェントをインストールします。

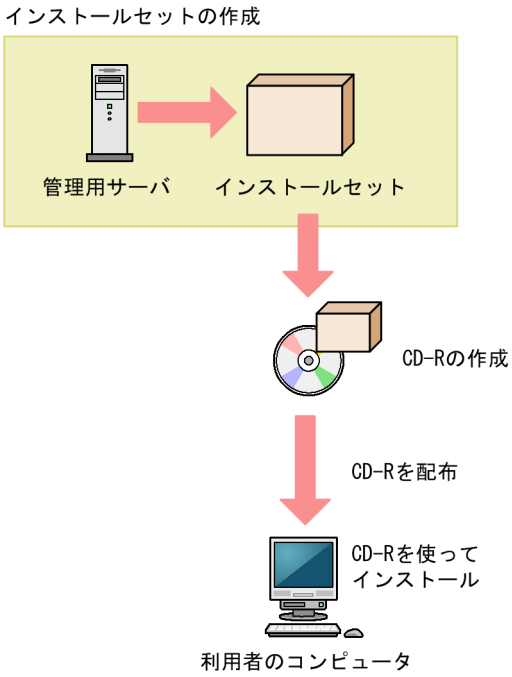
メリット

Web ページにセキュリティ管理用のページを作成したり、共有フォルダの環境を作成したりする必要がありません。この方法は、エージェントをインストールするコンピュータの台数が少ない場合に有効です。また、ネットワークの通信速度が遅い場合に、ネットワークに負荷をかけないでエージェントをインストールできます。利用者のコンピュータを構築するユーザー専用に、エージェントのプログラムを保持できることにもなります。

デメリット

必要な枚数分だけデータを媒体に書き込んで利用者に配布する必要があるため、展開に時間が掛かります。

CD-R の場合を例に、媒体を配布してエージェントをインストールするイメージを、次の図に示します。



ヒント

Autorun.inf を作成してインストールセットと一緒に CD-R に格納しておくと、媒体をコンピュータに接続した際に、自動でインストールが開始されます。インストールセットのファイル名が「ITDM2Agt.exe」の場合の Autorun.inf の作成例は次のとおりです。

```
[Autorun]
```

```
open=ITDM2Agt.exe
```

関連リンク

- 1.6.1　インストールセットを作成する手順
- 1.7.1　エージェントのインストール状況を確認する流れ

1.6.6　メールの添付ファイルでエージェントを配布する

管理者は、インストールセットをメールに添付して利用者に送信します。利用者は、添付ファイルをダブルクリックしてエージェントをインストールします。

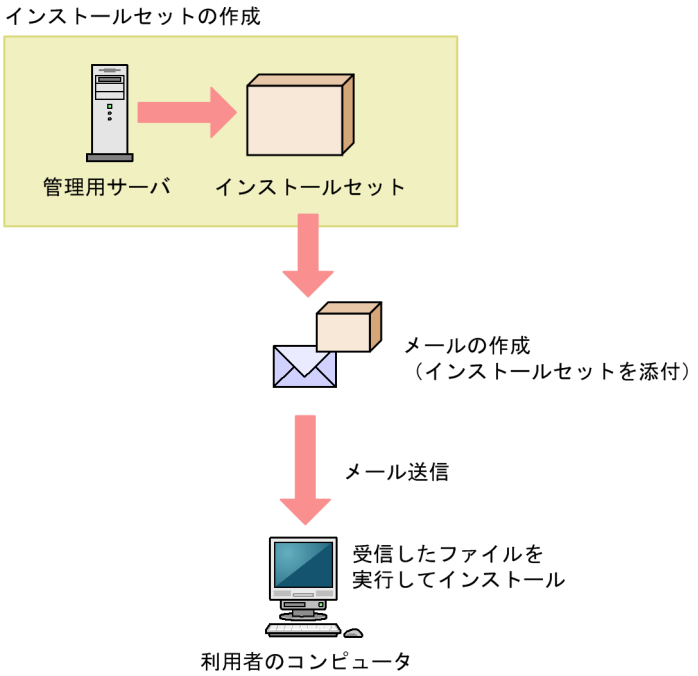
メリット

利用者にメールを一斉送信することで、多くのコンピュータに素早くエージェントをインストールできます。

デメリット

インストールセットの容量は、最小約 80 メガバイトで、設定に応じて増減します。そのため、インストールセットを添付して一斉に多数の宛先にメールを送信すると、メールサーバに負担が掛かったり、添付ファイルの容量に制限があるとメールを送信できなかったりします。

メールの添付ファイルでエージェントをインストールするイメージを、次の図に示します。



関連リンク

- 1.6.1　インストールセットを作成する手順
- 1.7.1　エージェントのインストール状況を確認する流れ

1.6.7　ログオンスクリプトを利用してエージェントをインストールする

管理者は、インストールセットをファイルサーバに格納します。そのあと、インストールセットを実行するログオンスクリプト用のバッチファイルを作成し、Active Directory サーバに格納しておきます。利用者が Windows にログオンしたときに、自動的にエージェントがインストールされます。なお、すでにエージェントがインストールされている場合はインストールされません。

ログオンスクリプト用のバッチファイルの作成例を次に示します。

```
if %PROCESSOR_ARCHITECTURE%==AMD64 (
if not exist "%ProgramFiles(x86)%¥Hitachi¥jp1itdma¥bin¥jdnglogon.exe" (
start /w ¥¥サーバ名¥共有フォルダ名¥ITDM2Agt.exe
)
) else (
if not exist "%ProgramFiles%¥Hitachi¥jp1itdma¥bin¥jdnglogon.exe" (
start /w ¥¥サーバ名¥共有フォルダ名¥ITDM2Agt.exe
)
)
```

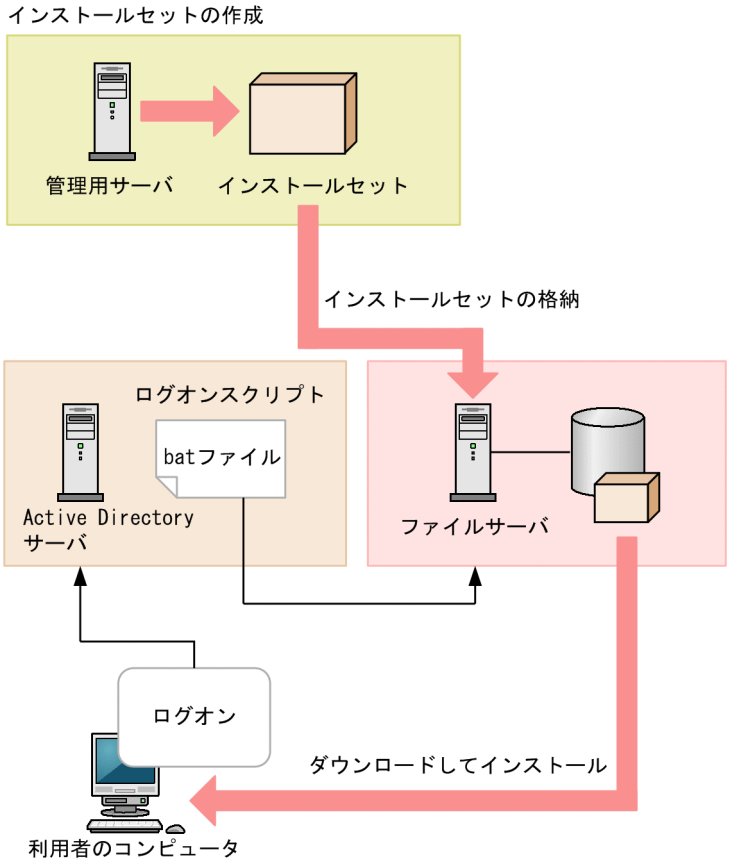
メリット

ログオンスクリプトを利用することで、利用者に作業してもらうことなくエージェントを自動的にインストールできます。そのため、利用者の操作ミスによるトラブルを避けられます。

デメリット

ファイルサーバおよびファイルサーバにアクセスできる環境が必要です。また、利用者のコンピュータはドメインで管理されていて、ログオンスクリプトを実行できる環境が必要です。

ログオンスクリプトを利用してエージェントを自動インストールするイメージを、次の図に示します。



関連リンク

- 1.6.1　インストールセットを作成する手順
- 1.7.1　エージェントのインストール状況を確認する流れ

1.6.8　ディスクコピーでエージェントをインストールする

利用者にコンピュータを配布する前に、配布するコンピュータのモデルとなるコンピュータに、インストールセットを使ってエージェントをインストールします。また、インストールが完了したら、モデルとなるコンピュータでresetnid.vbs コマンドを実行し、機器を識別するための ID（ホスト識別子）をリセットしておきます。次に、モデルとなるコンピュータのディスク全体を、専用のツールやソフトウェアを使用して配布前のコンピュータにディスクコピーします。そのあと、利用者にコンピュータを配布します。

重要

ディスクコピーを開始する前に、必ずモデルとなるコンピュータ（ディスクコピー元のコンピュータ）でresetnid.vbs コマンドを実行してください。このコマンドを実行しない場合、ディスクコピー先のコンピュータが、ディスクコピー元のコンピュータと同一の機器として識別されてしまいます。

VMWare などの仮想環境を複製して使用する場合も、resetnid.vbs コマンドを実行してください。

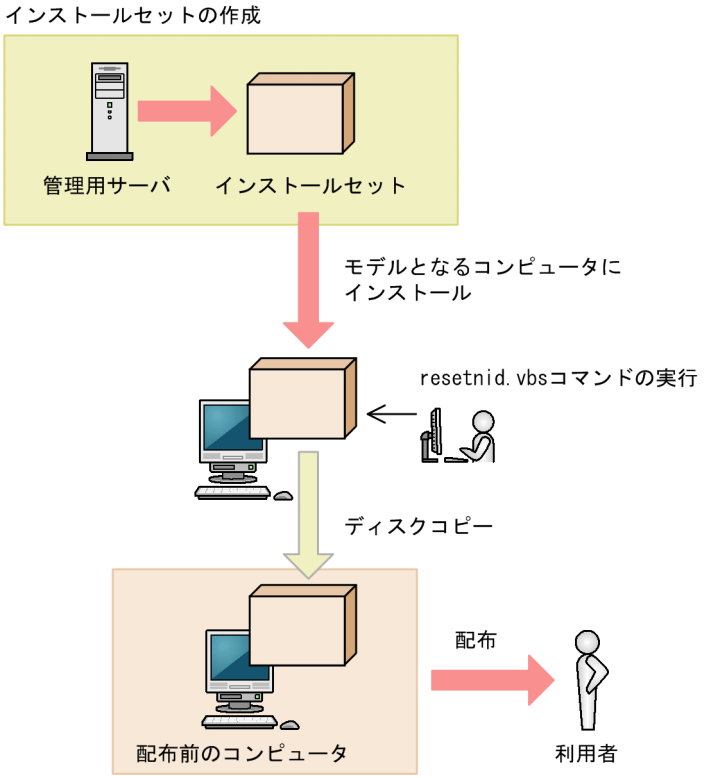
メリット

配布する時点でエージェントのインストールおよびセットアップがすでに完了しているため、利用者がエージェントをインストールする必要がありません。そのため、利用者の操作ミスによるトラブルを避けられます。

デメリット

配布前のコンピュータだけが対象です。すでに配布されているコンピュータには、この方法でエージェントをインストールできません。

ディスクコピーでエージェントをインストールするイメージを、次の図に示します。



関連リンク

- 1.6.1　インストールセットを作成する手順
- 1.7.1　エージェントのインストール状況を確認する流れ
- 8.10　resetnid.vbs（ホスト識別子のリセット）

1.6.9　エージェントを提供媒体からインストールする手順

エージェントのインストールを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

重要

コンピュータが Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8 および Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- *システムドライブ*:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

重要

エージェント環境を作成する場合、ユーザ環境変数およびシステム環境変数の TEMP および TMP で定義するディレクトリが存在することを確認してください。

OS が 64 ビット版の Windows の場合、ユーザ環境変数およびシステム環境変数の TEMP および TMP で定義するディレクトリに、環境変数%windir%¥system32 以下のディレクトリを定義しないでください。

重要

インストール先のドライブは、ローカルディスクを使用してください。ネットワーク接続のディスク（NFS、NAS など）をマウントしインストールしないでください。

エージェントをインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。

2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Agent］を選択して、［インストール実行］ボタンをクリックします。

3. インストール開始のダイアログで［次へ］ボタンをクリックします。

4. ［インストールタイプ］ダイアログで、インストールタイプを選択して［次へ］ボタンをクリックします。

   インストール先フォルダを指定したい場合はカスタムインストールを選択してください。簡単インストールの場合、インストール先フォルダにはデフォルト値が設定されます。

   簡単インストールを選択した場合は、手順 9.へ進んでください。

   ヒント

   エージェントのインストール先フォルダのデフォルト値は、「C:¥Program Files¥HITACHI¥jp1itdma」です。ただし、OS が 64 ビット版の Windows の場合は、環境変数%ProgramFiles(x86)%で定義されたフォルダ配下（OS が C ドライブにインストールされているときは、「C:¥Program Files (x86)¥Hitachi¥jp1itdma¥」）になります。

   重要

   OS が 64 ビット版の Windows の場合、環境変数%windir%¥system32 以下のフォルダにインストールしないでください。

   重要

   インストール先フォルダには、SYSTEM および Administrators グループのフルコントロール権限が必要です。また、適用先として「このフォルダ、サブフォルダおよびファイル」が設定されている必要があります。

5. ［インストール先のフォルダ］ダイアログで、インストール先のフォルダを指定して［次へ］ボタンをクリックします。

6. ［インストールするコンポーネントの種別］ダイアログで、［エージェント］を選択して［次へ］ボタンをクリックします。

7. ［インストールするコンポーネント］ダイアログで、インストールするほかのコンポーネント、サブコンポーネント、およびそのインストール方法を指定して［次へ］ボタンをクリックします。

   ヒント

   リモコンエージェントは、エージェントのサブコンポーネントとしてインストールされます。

   インストール方法は、文字列の左にあるアイコンをクリックして、プルダウンメニューから選択します。

8. インストールの開始準備の完了を示すダイアログで、［インストール］ボタンをクリックします。

インストールが実行されます。

9. インストールが完了したら、[完了] ボタンをクリックします。

エージェントのインストールが完了し、セットアップのダイアログが表示されます。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

ヒント

JP1/IT Desktop Management 2 - Agent をインストールすると、同時にリモコンエージェントもインストールされます。リモコンエージェントとは、リモートコントロール時に、接続される側のコンピュータに必要なプログラムです。

重要

JP1/IT Desktop Management 2 - Agent をインストールした後、イベントログ（システム）に次のメッセージが出力される場合がありますが、動作上、問題はありません。

- JP1_ITDM2_Agent Remote Control サービスは、対話型サービスとしてマークされています。
  しかし、システムは対話型サービスを許可しないように構成されています。
  このサービスは正常に機能しない可能性があります。
- JP1_ITDM2_Agent Service サービスは、対話型サービスとしてマークされています。
  しかし、システムは対話型サービスを許可しないように構成されています。
  このサービスは正常に機能しない可能性があります。
- JP1_ITDM2_Agent Monitor Control サービスは、対話型サービスとしてマークされています。
  しかし、システムは対話型サービスを許可しないように構成されています。
  このサービスは正常に機能しない可能性があります。

重要

インストールの多重実行はできません。エージェントまたはネットワークモニタエージェントの自動アップデートと、ユーザー操作によるバージョンアップインストールが重なった場合も同様です。この場合、次のメッセージのダイアログが表示されることがあります。

「JP1/IT Desktop Management 2 - Agent のインストールでエラーが発生しました。システム管理者に連絡してください。」

1.6.10　エージェントをセットアップする手順

提供媒体からエージェントをインストールした場合、管理用サーバと接続するためにセットアップを実行する必要があります。

なお、エージェントのセットアップを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

管理用中継サーバ用のエージェントのセットアップは、管理用中継サーバのセットアップに含まれます。管理用中継サーバをセットアップする手順については、「1.2.5　管理用中継サーバをセットアップする手順」を参照してください。

ヒント

インストールセットの配布や管理用サーバからの配信でエージェントを導入した場合は、自動で接続先が設定されるため、接続先を設定するためのセットアップは不要です。

なお、接続先設定ファイル（itdmhost.conf）または上位接続先情報ファイル（dmhost.txt）を使用して接続先を設定することもできます。接続先設定ファイル（itdmhost.conf）または上位接続先情報ファイル（dmhost.txt）を JP1/IT Desktop Management 2 - Manager のデータフォルダに格納しておくと、インストールセットの作成時にインストールセットに取り込まれて、各エージェントに配布されます。ただし、エージェントに接続先設定ファイルまたは上位接続先情報ファイルが存在する場合は、エージェント設定の［基本設定］で指定する接続先よりも接続先設定ファイル、上位接続先情報ファイルに指定した接続先の方が優先されます。接続先設定ファイルと上位接続先情報ファイルの両方がエージェントに存在する場合は、上位接続先情報ファイルは無視されます。接続先設定ファイル（itdmhost.conf）については、「1.6.11　エージェントの接続先を自動設定する手順」を参照してください。上位接続先情報ファイルの詳細については、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、エージェントの接続先の自動変更についての説明を参照してください。

また、インターネットゲートウェイ接続先設定ファイル（itdmigw.conf）を使用してインターネット接続設定を設定することもできます。インターネットゲートウェイ接続先設定ファイル（itdmigw.conf）を作成して、インストールセットの作成時に「展開するファイルの設定」で指定すると、インストールセットに取り込まれて、各エージェントに配布されます。なお、インターネット接続オプションが有効な場合、インターネットゲートウェイを経由する上位接続が有効になります。また、接続先設定ファイル（itdmhost.conf）または上位接続先情報ファイル（dmhost.txt）を使用した接続先の自動設定よりも優先されます。インターネットゲートウェイ接続先設定ファイル（itdmigw.conf）の詳細については、「1.6.12　エージェントのインターネットゲートウェイ経由の接続先を自動設定する手順」を参照してください。インストールセットの作成手順については、「1.6.1　インストールセットを作成する手順」を参照してください。

エージェントをセットアップするには：

1. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Agent］－［管理者ツール］－［セットアップ］を選択します。
   エージェントにパスワード保護が設定されている場合、パスワードの入力画面が表示されます。該当するエージェント設定に設定したパスワードを入力してください。パスワードのデフォルトは「manager」です。

2. ［セットアップ（エージェント）］ダイアログの［接続先設定］タブで、接続先の管理用サーバのホスト名または IP アドレスと、ポート番号を指定します。
   接続先設定ファイル（itdmhost.conf）を使用した運用の場合、接続先設定ファイルを優先するため、セットアップで接続先を変更することはできません。

3. 使用するネットワークアダプタが複数存在する（複数 LAN 接続）環境で、JP1/IT Desktop Management 2 で使う通信回線に優先順位を付けたい場合、［セットアップ（エージェント）］ダイアログの［通信設定］タブで、［ネットワークアダプタの設定］ボタンクリックし、表示されるダイアログで優先順位と自動更新に関する情報を指定して［OK］ボタンをクリックします。

4. 表示される確認ダイアログで［はい］ボタンをクリックします。

セットアップが完了し、設定した内容でエージェントが動作するようになります。

> **ヒント**
>
> エージェントが管理用サーバと接続できている場合、操作画面からエージェントのセットアップを実行できます。操作画面からエージェントをセットアップするには、エージェント設定を利用します。

1.6.11　エージェントの接続先を自動設定する手順

接続先を決定するための情報をエージェントに配布しておくと、管理対象のコンピュータの IP アドレスから適切な接続先の上位システムを判断して、自動的に設定できます。コンピュータの IP アドレスが変更されると接続先も自動的に変更されるため、コンピュータが移動した場合に便利です。また、管理する機器に割り当てる IP アドレスの範囲ごとに複数の管理用サーバを用意して、1 台の管理用サーバで管理する機器の台数が上限を超えないように分散して管理することもできます。ここでは、エージェントの接続先を自動設定する手順について説明します。

この機能は、JP1/IT Desktop Management 2 - Agent で使用できます。なお、中継システム、UNIX エージェントおよび Mac エージェントでは使用できません。

メモ

この機能を使用する場合、マルチポーリングの設定（エージェント設定の［通信設定］－［複数の上位システムへのポーリングの設定］）はしないでください。ただし、配布用の上位システムを切り替える機能を使用する場合は、マルチポーリングの設定をしてください。

メモ

パッケージセットアップマネージャの起動中にエージェントの接続先変更が動作した場合、パッケージセットアップマネージャの画面の更新を促すダイアログが表示され、新しい接続先に切り替わります。

メモ

この機能は、Citrix XenApp、Microsoft RDS サーバでは、サポートしていません。

(1) 接続する上位システムを自動的に設定・変更する

接続先の上位システムを自動的に設定・変更するには、あらかじめ接続先設定ファイル（itdmhost.conf）を作成し、管理対象のコンピュータに配布します。配布後の特定のタイミングで、接続先が自動的に再設定されます。

接続先設定ファイルを作成する

接続先設定ファイルは、接続する上位システムを決定するためのファイルです。このファイルは、管理対象のコンピュータの IP アドレスの範囲と対応する接続先の上位システムの組み合わせを定義しています。例えば、IP アドレスが「172.16.22.1～172.16.22.255」のコンピュータの接続先は東京支部の管理用サーバ、IP アドレスが「172.17.22.1～172.17.22.255」のコンピュータの接続先は名古屋支部の管理用サーバというように定義します。接続先設定ファイルの作成方法の詳細については、「(2) 接続先設定ファイル（itdmhost.conf）の作成」を参照してください。

作成した接続先設定ファイルを JP1/IT Desktop Management 2 - Manager のデータフォルダに格納しておくと、インストールセットの作成時にインストールセットに取り込まれます。

接続先設定ファイルを管理対象のコンピュータに配布する

接続先設定ファイルが取り込まれたインストールセットを使用して JP1/IT Desktop Management 2 - Agent をインストールすると、管理対象のコンピュータの次のフォルダに接続先設定ファイルが格納されます。

JP1/IT Desktop Management 2 - Agentのインストール先フォルダ¥MASTER¥DB

パッケージとして接続先設定ファイルを登録し、そのパッケージを配布するジョブを作成すれば、対象のコンピュータに配布することもできます。その場合の配布先は上記になるように設定してください。

管理対象になる前のコンピュータの場合は、手動で格納してもかまいません。

接続先が決定されるタイミング

接続先設定ファイルを管理対象のコンピュータに格納したあと、ポーリング（エージェントからのジョブの問い合わせ）が実行されるのを待つか、または管理対象のコンピュータの OS を再起動してください。接続先設定ファイルの内容に従って、エージェントが接続する上位システムが設定されます。

エージェントの接続先が決定されるポーリングは次の 3 種類です。

- システム起動を基準としたポーリング

  エージェント設定の［基本設定］で、［システム起動を基準としたポーリングをする］のチェックボックスをオンにしている場合
- 定期ポーリング（デフォルトは 30 分ごと）
- 時刻指定によるポーリング

  エージェント設定の［基本設定］で、［時刻を指定してポーリングする］のチェックボックスをオンにしている場合

一度設定したあとでも、次の操作をしたあとにポーリングが実行されるのを待つか、または OS を再起動すると接続先が再設定されます。

- 管理対象のコンピュータの IP アドレス変更
- 接続先設定ファイルの編集または上書き

  接続先情報を変更した接続先設定ファイルをエージェントに再配布するか、各エージェントの*インストール先フォルダ*¥MASTER¥DB に格納されている接続先設定ファイルを直接編集して上書きし、コンピュータを再起動すると接続先が変更されます。

管理対象のコンピュータを移動して IP アドレスを変更した場合、ポーリングが実行されるのを待つか、または OS を再起動するだけで適切な上位システムに接続先が変更されます。エンドユーザは接続先の変更を意識する必要がありません。

接続先設定ファイルによってエージェントの接続先の自動設定・変更が起きると、ログがエージェントごとに*インストール先フォルダ*¥LOG¥USER.LOG ファイルに取得されます。接続先の自動変更に関するログについては、「JP1/IT Desktop Management 2 配布機能 運用ガイド」の接続先の自動変更関連のログの説明を参照してください。

> **ヒント**
>
> エージェントに複数の IP アドレスが設定されている場合、OS が決めた優先度が一番高い IP アドレスを取得して、接続する上位システムを決定します。その上位システムへの接続に成功した場合に、エージェントの接続先として設定されます。

接続先の自動変更と他機能との関係

接続先設定ファイルを使用した接続先の自動変更は、JP1/IT Desktop Management 2 の他機能と併用できない場合があります。次の点に注意してください。

- 管理対象のコンピュータの起動時に*JP1/IT Desktop Management 2 - Agentのインストール先フォルダ*￥MASTER￥DB￥下に接続先設定ファイルが存在する場合は、エージェント設定で設定した管理用サーバや配布用の上位システムではなく、接続先設定ファイルに指定された接続先情報に基づいて上位システム（管理用サーバや中継システム）に接続されます。
- 管理対象のコンピュータの*JP1/IT Desktop Management 2 - Agentのインストール先フォルダ*￥MASTER￥DB￥下に接続先設定ファイル（itdmhost.conf）と上位接続先情報ファイル（dmhost.txt）の両方が存在する場合は、上位接続先情報ファイル（dmhost.txt）は無視されます。
- 配布用の上位システムを切り替える機能によって上位システムの接続先が切り替えられた場合、接続先設定ファイル（itdmhost.conf）および上位接続先情報ファイル（dmhost.txt）の内容や、エージェント設定の［通信設定］－［複数の上位システムへのポーリングの設定］で指定する［ポーリング対象とする上位システム］の設定内容は変更されません。

接続先設定ファイルによる接続先の設定を無効にするには、次のどれかの対処をしてください。どの場合でも、エージェントに上位接続先情報ファイルが存在しなければエージェント設定で指定した接続先に接続されるようになり、上位接続先情報ファイルが存在する場合は上位接続先情報ファイルに指定された接続先に接続されるようになります。

- 中身が空の接続先設定ファイルをエージェントに配布する
- 各エージェントの*インストール先フォルダ*￥MASTER￥DB￥下の接続先設定ファイルを削除する
- 各エージェントの*インストール先フォルダ*￥MASTER￥DB￥下の接続先設定ファイルの名前をitdmhost.conf 以外に変更する

上位接続先情報ファイルによる接続先の設定も無効にする場合は、上記の接続先設定ファイルを上位接続先情報ファイルに読み替えてどれかの対処をしてください。

接続先設定ファイル（itdmhost.conf）の有無と［一定時間ポーリングに失敗する場合は配布用の上位システムを切り替え］の設定の組み合わせによる、切り替えの有無と切り替え先は次のようになります。

接続先設定ファイルの有無	［一定時間ポーリングに失敗する場合は配布用の上位システムを切り替える］の設定	
	無効	有効
接続先設定ファイルが存在しない	ポーリングの切り替え： 　実施しない 配布用の上位システムの切り替え： 　実施しない	ポーリングの切り替え： 　実施しない 配布用の上位システムの切り替え： 　実施する（エージェント設定に従う）
接続先設定ファイルが存在する	ポーリングの切り替え： 　実施する（itdmhost.conf に従う）	ポーリングの切り替え： 　実施する（itdmhost.conf に従う）

接続先設定ファイルの有無	［一定時間ポーリングに失敗する場合は配布用の上位システムを切り替える］の設定	
	無効	有効
接続先設定ファイルが存在する	配布用の上位システムの切り替え： 実施しない	配布用の上位システムの切り替え： 実施する（itdmhost.conf に従う）

(2) 接続先設定ファイル（itdmhost.conf）の作成

接続先設定ファイルは、itdmhost.conf という名称のテキストファイルです。作成方法を次に説明します。

接続先設定ファイルの形式

接続先設定ファイルには、管理対象のコンピュータの IP アドレスの範囲と対応する接続先の組み合わせを、1 行につき 1 件定義します。各項目間は「,」（コンマ）で区切ってください。行の先頭に「;」（セミコロン）を付けると、その行はコメントと見なされます。なお、最終行の改行はしないでください。また、ファイルの文字コードには UTF-8 を使用してください。

接続先設定ファイルの形式を次に示します。

```
[ITDM]
最小のIPアドレス,最大のIPアドレス,接続先
最小のIPアドレス,最大のIPアドレス,接続先
      :
[DM]
最小のIPアドレス,最大のIPアドレス,接続先,接続種別 [,マルチキャスト
配布用アドレス]
最小のIPアドレス,最大のIPアドレス,接続先,接続種別 [,マルチキャスト
配布用アドレス]
      :
```

接続先設定ファイルの設定項目を次の表に示します。

セクション	項目	説明	入力できる値	省略可否
ITDM	エージェントが接続する管理用サーバを設定します。			必須
	最小の IP アドレス	管理対象のコンピュータの IP アドレスの範囲で最小の IP アドレスを指定します。	半角数字で「xxx.xxx.xxx.xxx」の形式	必須
	最大の IP アドレス	管理対象のコンピュータの IP アドレスの範囲で最大の IP アドレスを指定します。	半角数字で「xxx.xxx.xxx.xxx」の形式	必須
	接続先	接続先の管理用サーバのホスト名または IP アドレス※1 を指定します。	ホスト名の場合は半角英数字 255 文字以下 IP アドレスの場合は半角数字で「xxx.xxx.xxx.xxx」の形式	必須

セクション	項目	説明	入力できる値	省略可否
DM	リモートインストールマネージャを使用した配布用の上位システムを設定します。			必須
	最小の IP アドレス	管理対象のコンピュータの IP アドレスの範囲で最小の IP アドレスを指定します。	半角数字で「xxx.xxx.xxx.xxx」の形式	必須
	最大の IP アドレス	管理対象のコンピュータの IP アドレスの範囲で最大の IP アドレスを指定します。	半角数字で「xxx.xxx.xxx.xxx」の形式	必須
	接続先※2	リモートインストールマネージャを使用した配布用の接続先となる上位システムのホスト名または IP アドレス※1 を指定します。	ホスト名の場合は半角英数字 64 文字以下 IP アドレスの場合は半角数字で「xxx.xxx.xxx.xxx」の形式	必須
	接続種別※2	接続先が管理用サーバであれば「netmdm」を、中継システムであれば「netmdmw」を指定します。		必須
	マルチキャスト配布用アドレス	管理対象のコンピュータにジョブをマルチキャスト配布したい場合、接続先に設定しているマルチキャストアドレスを指定します。	半角数字で「xxx.xxx.xxx.xxx」の形式（範囲は 224.0.1.0～239.255.255.255）	省略可

注※1　ホスト名または IP アドレスのどちらで指定するかは、管理用サーバのセットアップ時に［アドレス解決の設定］で指定した運用キーの内容に一致させてください。

注※2　1 行に接続先と接続種別のセットを最大 8 個まで指定できます。複数の接続先と接続種別を指定した場合、先に指定した接続先の方が優先順位が上位となります。

接続先設定ファイルについての注意事項を次に示します。

- 管理対象のコンピュータの IP アドレスが定義した範囲に含まれない場合、接続先の設定は変更されません。
- 管理対象のコンピュータの IP アドレスの範囲が重複する複数の定義をした場合は、先に定義した行が有効となります。
- セクションが重複する場合、先に定義したセクションが有効となります。
- セクションがない場合、定義した行は無効になります。
- 次の場合は、指定行の定義が無効になります。
  - 必須項目を省略した場合
  - IP アドレスに無効な値を指定した場合
  - 「接続先」として入力できる文字数以上の値を指定した場合
  - 「接続種別」として「netmdm」、「netmdmw」以外を指定した場合
  - 改行だけの行の場合

- 「マルチキャスト配布用アドレス」の指定を省略した場合、または無効な値を指定した場合、マルチキャストアドレスの設定はできません。ただし、「マルチキャスト配布用アドレス」以外の項目で定義した、IP アドレスの範囲と対応する接続先の組み合わせは有効になります。
- 1 行に指定できる項目以外の項目を指定した場合、その項目は無視されます。
- セミコロンに続く記述はコメントとして扱われ、無視されます。
- 各項目の先頭や末尾に含まれる半角スペースは無視されます。

接続先設定ファイルの作成例

接続先設定ファイルの作成例を次に示します。

```
;接続先設定
[ITDM]
172.17.12.1,172.17.12.250,manager01
172.17.13.1,172.17.13.250,manager02
0.0.0.0,255.255.255.254,manager04
[DM]
172.17.12.1,172.17.12.250,dmsub01,netmdmw,dmsub02,netmdmw,dmman01,netmdm
172.17.13.1,172.17.13.250,dmman01,netmdm,dmman02,netmdm
0.0.0.0,255.255.255.254,dmman02,netmdm
```

この例では、管理対象のコンピュータの IP アドレスが「172.17.13.6」の場合、接続先の管理用サーバは「manager02」という名前のホストで、リモートインストールマネージャを使用した配布用の上位システムは「dmman01」または「dmman02」という名前の管理用サーバになります。

なお、接続先設定ファイルの各セクションの最終行に、すべての IP アドレスを範囲とする「0.0.0.0～255.255.255.254」を定義しておくと、該当する IP アドレスがなかった場合の接続先となります。この例では 172.17.12.1～172.17.12.250、172.17.13.1～172.17.13.250 以外のコンピュータの接続先は、管理用サーバが「manager04」で、リモートインストールマネージャを使用した配布用の上位システムが「dmman02」になります。また、複数の接続先を指定した場合、先に指定した接続先の優先順位が上位となります。この例では、「dmsub01」や「dmman01」が優先順位 1 位となります。

> **ヒント**
>
> 接続先設定ファイルを作成したあと、ファイルフォーマットを満たしているかどうかを checkitdmhost コマンドでチェックできます。checkitdmhost コマンドについては、「8.13 checkitdmhost（接続先設定ファイルのフォーマットチェック）」を参照してください。

接続先設定ファイルを配布したあとの注意事項

接続先設定ファイルを管理対象のコンピュータに配布して接続先が設定されたあと、接続先ホストの IP アドレスを変更するときは、それまで適用していた接続先設定ファイルを該当する管理対象のコンピュータから削除しておいてください。削除しないと、接続先ホストの IP アドレス変更を契機に接続先の自動変更が動作し、想定した上位システムとは別の接続先が設定されることがあります。

1.6.12　エージェントのインターネットゲートウェイ経由の接続先を自動設定する手順

インターネットゲートウェイを経由してエージェントが管理用サーバと接続する環境の場合、接続先のインターネットゲートウェイを決定するための情報をエージェントに配布しておくと、管理対象のコンピュータの IP アドレスから適切な接続先のインターネットゲートウェイを判断して、自動的に設定できます。ここでは、エージェントの接続先インターネットゲートウェイを自動設定する手順について説明します。

この機能は、JP1/IT Desktop Management 2 - Agent で使用できます。なお、中継システム、UNIX エージェントおよび Mac エージェントでは使用できません。

(1)　インターネットゲートウェイ経由で接続する上位システムを自動的に設定・変更する

接続先のインターネットゲートウェイを自動的に設定・変更するには、あらかじめインターネットゲートウェイ接続先設定ファイル（itdmigw.conf）を作成し、管理対象のコンピュータに配布します。配布後の特定のタイミングで、接続先インターネットゲートウェイが自動的に再設定されます。

インターネットゲートウェイ接続先設定ファイルを作成する

インターネットゲートウェイ接続先設定ファイルは、接続するインターネットゲートウェイを決定するためのファイルです。このファイルは、管理対象のコンピュータの IP アドレスの範囲と対応する接続先のインターネットゲートウェイの組み合わせを定義しています。インターネットゲートウェイ接続先設定ファイルの作成方法の詳細については、「(2)　インターネットゲートウェイ接続先設定ファイル（itdmigw.conf）の作成」を参照してください。

インターネットゲートウェイ接続先設定ファイルを管理対象のコンピュータに配布する

インターネットゲートウェイ接続先設定ファイルが取り込まれたインストールセットを使用して JP1/IT Desktop Management 2 - Agent をインストールすると、管理対象のコンピュータの次のフォルダに接続先設定ファイルが格納されます。

JP1/IT Desktop Management 2 - Agentのインストール先フォルダ¥MASTER¥DB

パッケージとしてインターネットゲートウェイ接続先設定ファイルを登録し、そのパッケージを配布するジョブを作成すれば、対象のコンピュータに配布することもできます。その場合の配布先は上記になるように設定してください。

管理対象になる前のコンピュータの場合は、手動で格納してもかまいません。

接続先が決定されるタイミング

インターネットゲートウェイ接続先設定ファイルを管理対象のコンピュータに格納したあと、ポーリング（エージェントからのジョブの問い合わせ）が実行されるのを待つか、または管理対象のコンピュータの OS を再起動してください。インターネットゲートウェイ接続先設定ファイルの内容に従って、エージェントが接続するインターネットゲートウェイが設定されます。

エージェントの接続先インターネットゲートウェイが決定されるポーリングは次の 3 種類です。

- システム起動を基準としたポーリング
  エージェント設定の［基本設定］で、［システム起動を基準としたポーリングをする］のチェックボックスをオンにしている場合
- 定期ポーリング（デフォルトは 30 分ごと）
- 時刻指定によるポーリング
  エージェント設定の［基本設定］で、［時刻を指定してポーリングする］のチェックボックスをオンにしている場合

一度設定したあとでも、次の操作をしたあとにポーリングが実行されるのを待つか、または OS を再起動すると接続先インターネットゲートウェイが再設定されます。

- 管理対象のコンピュータの IP アドレス変更
- インターネットゲートウェイ接続先設定ファイルの編集または上書き
  接続先インターネットゲートウェイ情報を変更したインターネットゲートウェイ接続先設定ファイルをエージェントに再配布するか、各エージェントの*インストール先フォルダ*¥MASTER¥DB に格納されているインターネットゲートウェイ接続先設定ファイルを直接編集して上書きし、コンピュータを再起動すると接続先インターネットゲートウェイが変更されます。

管理対象のコンピュータを移動して IP アドレスを変更した場合、ポーリングが実行されるのを待つか、または OS を再起動するだけで適切なインターネットゲートウェイに接続先が変更されます。エンドユーザは接続先インターネットゲートウェイの変更を意識する必要がありません。

インターネットゲートウェイ接続先設定ファイルによってエージェントの接続先インターネットゲートウェイの自動設定・変更が起きると、ログがエージェントごとに*インストール先フォルダ*¥LOG¥USER.LOG ファイルに取得されます。接続先インターネットゲートウェイの自動変更に関するログについては、「JP1/IT Desktop Management 2 配布機能 運用ガイド」の接続先の自動変更関連のログの説明を参照してください。

ヒント

エージェントに複数の IP アドレスが設定されている場合、OS が決めた優先度が一番高い IP アドレスを取得して、接続するインターネットゲートウェイを決定します。そのインターネットゲートウェイサーバへの接続に成功した場合に、エージェントの接続先インターネットゲートウェイとして設定されます。

接続先の自動変更と他機能との関係

インターネットゲートウェイ接続先設定ファイルを使用した接続先インターネットゲートウェイの自動変更は、JP1/IT Desktop Management 2 の他機能と併用できない場合があります。次の点に注意してください。

- 管理対象のコンピュータの起動時に*JP1/IT Desktop Management 2 - Agentのインストール先フォルダ*￥MASTER￥DB￥下にインターネットゲートウェイ接続先設定ファイルが存在する場合は、エージェント設定で設定したインターネットゲートウェイサーバではなく、インターネットゲートウェイ接続先設定ファイルに指定されたインターネットゲートウェイサーバに接続されます。
- 管理対象のコンピュータのエージェント設定でインターネット接続オプションが有効で、かつ起動時に*JP1/IT Desktop Management 2 - Agentのインストール先フォルダ*￥MASTER￥DB￥下にインターネットゲートウェイ接続先設定ファイル（itdmigw.conf）に加えて接続先設定ファイル（itdmhost.conf）または上位接続先情報ファイル（dmhost.txt）が存在する場合、接続先設定ファイルに指定された接続先情報に基づいた上位システム（管理用サーバや中継システム）でなく、インターネットゲートウェイ接続先設定ファイルに指定されたインターネットゲートウェイサーバに接続されます。
- 次の条件をすべて満たす場合は、接続先設定ファイル（itdmhost.conf）または上位接続先情報ファイル（dmhost.txt）の接続先情報に基づいて上位システム（管理用サーバや中継システム）に接続されます。接続先設定ファイルが存在しない場合は、エージェント設定で設定した管理用サーバや配布用の上位システムに接続されます。
  - インターネットゲートウェイ接続先設定ファイルに指定されたインターネットゲートウェイサーバに接続できない
  - インターネットゲートウェイ接続先設定ファイルの［インターネットゲートウェイと通信できない場合に、上位システムと直接通信する］の設定が「1」（通信する）である

インターネットゲートウェイ接続先設定ファイルによる接続先の設定を無効にするには、次のどれかの対処をしてください。

- 中身が空のインターネットゲートウェイ接続先設定ファイルをエージェントに配布する
- 各エージェントの*インストール先フォルダ*￥MASTER￥DB￥下のインターネットゲートウェイ接続先設定ファイルを削除する
- 各エージェントの*インストール先フォルダ*￥MASTER￥DB￥下のインターネットゲートウェイ接続先設定ファイルの名前を itdmigw.conf 以外に変更する

(2) インターネットゲートウェイ接続先設定ファイル（itdmigw.conf）の作成

インターネットゲートウェイ接続先設定ファイルは、itdmigw.conf という名称のテキストファイルです。作成方法を次に説明します。

インターネットゲートウェイ接続先設定ファイルの形式

インターネットゲートウェイ接続先設定ファイルには、管理対象のコンピュータの IP アドレスの範囲と対応する接続先インターネットゲートウェイサーバの組み合わせを、1 行につき 1 件定義します。各項目間は「,」（コンマ）で区切ってください。行の先頭に「;」（セミコロン）を付けると、その行はコメントと見なされます。なお、最終行の改行はしないでください。また、ファイルの文字コードには UTF-8 を使用してください。

インターネットゲートウェイ接続先設定ファイルの形式を次に示します。

```
[IGW]
最小のIPアドレス,最大のIPアドレス,インターネットゲートウェイのホスト名またはIPアドレス,インターネットゲートウェイのポート番号,エージェントで使用するポート番号1,エージェントで使用するポート番号2,インターネットゲートウェイと通信できない場合に、上位システムと直接通信する,ユーザー認証する,インターネットゲートウェイサーバのユーザーID,インターネットゲートウェイサーバのパスワード,プロキシサーバを使用する,プロキシサーバのホスト名またはIPアドレス,プロキシサーバのポート番号,プロキシサーバのユーザーID,プロキシサーバのパスワード,証明書のエラーを無視する,ファイルの分割サイズ
最小のIPアドレス,最大のIPアドレス,インターネットゲートウェイのホスト名またはIPアドレス,インターネットゲートウェイのポート番号,エージェントで使用するポート番号1,エージェントで使用するポート番号2,インターネットゲートウェイと通信できない場合に、上位システムと直接通信する,ユーザー認証する,インターネットゲートウェイサーバのユーザーID,インターネットゲートウェイサーバのパスワード,プロキシサーバを使用する,プロキシサーバのホスト名またはIPアドレス,プロキシサーバのポート番号,プロキシサーバのユーザーID,プロキシサーバのパスワード,証明書のエラーを無視する,ファイルの分割サイズ
      :
```

インターネットゲートウェイ接続先設定ファイルの設定項目を次の表に示します。

セクション	項目	説明	入力できる値	省略可否
IGW	エージェントが接続するインターネットゲートウェイサーバを設定します。			必須
	最小の IP アドレス	管理対象のコンピュータの IP アドレスの範囲で最小の IP アドレスを指定します。	半角数字で「xxx.xxx.xxx.xxx」の形式	必須
	最大の IP アドレス	管理対象のコンピュータの IP アドレスの範囲で最大の IP アドレスを指定します。	半角数字で「xxx.xxx.xxx.xxx」の形式	必須
	インターネットゲートウェイのホスト名または IP アドレス	インターネットゲートウェイのホスト名または IP アドレスを指定します。	ホスト名の場合は半角英数字 255 文字以下 IP アドレスの場合は半角数字で「xxx.xxx.xxx.xxx」の形式	必須
	インターネットゲートウェイのポート番号	インターネットゲートウェイのポート番号を指定します。	半角数字で 1～65535 の範囲の数値	必須
	エージェントで使用するポート番号 1※	エージェントで使用するポート番号 2 個中 1 個目を指定します。	半角数字で 1～65535 の範囲の数値	必須
	エージェントで使用するポート番号 2※	エージェントで使用するポート番号 2 個中 2 個目を指定します。	半角数字で 1～65535 の範囲の数値	必須
	インターネットゲートウェイと通信できない場合に、上位システムと直接通信する	インターネットゲートウェイと通信できない場合に、上位システムと直接通信するかを指定します。	半角数字で次のどちらかを指定します。 1：通信する 0：通信しない	必須

セクション	項目	説明	入力できる値	省略可否
IGW	ユーザー認証する	インターネットゲートウェイへの接続時にユーザー認証するかを指定します。	半角数字で次のどちらかを指定します。 1：認証する 0：認証しない	必須
	インターネットゲートウェイサーバのユーザー ID	インターネットゲートウェイの認証時のユーザー ID を指定します。	ASCII 制御文字以外の ASCII 文字 276 文字以内	「ユーザー認証する」が 1 の場合必須。0 の場合、値は無視されます。
	インターネットゲートウェイサーバのパスワード	インターネットゲートウェイの認証時のパスワードを指定します。	ASCII 制御文字以外の ASCII 文字 48 文字以内	「ユーザー認証する」が 1 の場合必須。0 の場合、値は無視されます。
	プロキシサーバを使用する	プロキシサーバを使用するかどうかを指定します。	半角数字で次のどちらかを指定します。 1：使用する 0：使用しない	必須
	プロキシサーバのホスト名または IP アドレス	プロキシサーバを使用してインターネットゲートウェイと通信する場合に、プロキシサーバのホスト名または IP アドレスを指定します。	ホスト名の場合は半角英数字 249 文字以下 IP アドレスの場合は半角数字で「xxx.xxx.xxx.xxx」の形式	「プロキシサーバを使用する」が 1 の場合必須。0 の場合、値は無視されます。
	プロキシサーバのポート番号	プロキシサーバのポート番号を指定します。	半角数字で 5001～49151 の範囲の数値	「プロキシサーバを使用する」が 1 の場合必須。0 の場合、値は無視されます。
	プロキシサーバのユーザー ID	プロキシサーバへの接続時にユーザー認証する場合のユーザー ID を指定します。	ASCII 制御文字以外の ASCII 文字 276 文字以内	任意 「プロキシサーバを使用する」が 0 の場合、値は無視されます。
	プロキシサーバのパスワード	プロキシサーバへの接続時にユーザー認証する場合のパスワードを指定します。	ASCII 制御文字以外の ASCII 文字 48 文字以内	任意 「プロキシサーバを使用する」が 0 の場合、値は無視されます。
	証明書のエラーを無視する	サーバ証明書の有効期限が切れた場合に、インターネットゲートウェイとの接続をエラーとするかどうかを指定します。	半角数字で次のどちらかを指定します。 1：エラーとする 0：エラーとしない	必須
	ファイルの分割サイズ	アップロードファイルの分割サイズを KB で指定します。	半角数字で 10～102400 の範囲の数値	必須

注※　エージェントで使用するポート番号を変更した場合、エージェント機器を再起動してください。

重要

インターネットゲートウェイ接続先設定ファイルの作成後は、checkitdmigw コマンドでファイルフォーマットを満たしているかチェックし、ファイルを難読化してから、インストールセットに取り込んだり各エージェントに配布したりすることを強く推奨します。checkitdmigw コマンドの詳細は、「8.14　checkitdmigw（インターネットゲートウェイ接続先設定ファイルのフォーマットチェック）」を参照してください。

インターネットゲートウェイ接続先設定ファイルについての注意事項を次に示します。

- 管理対象のコンピュータの IP アドレスが定義した範囲に含まれない場合、接続先の設定は変更されません。
- 管理対象のコンピュータの IP アドレスの範囲が重複する複数の定義をした場合は、先に定義した行が有効となります。
- セクションが重複する場合、先に定義したセクションが有効となります。
- セクションがない場合、定義した行は無効になります。
- 次の場合は、指定行の定義が無効になります。
  - 必須項目を省略した場合
  - IP アドレスに無効な値を指定した場合
  - 入力できる文字数以上の値を指定した場合
  - 改行だけの行の場合
- 1 行に指定できる項目以外の項目を指定した場合、その項目は無視されます。
- セミコロンに続く記述はコメントとして扱われ、無視されます。
- 各項目の先頭や末尾に含まれる半角スペースは無視されます。

インターネットゲートウェイ接続先設定ファイルの作成例

インターネットゲートウェイ接続先設定ファイルの作成例を次に示します。

```
[IGW]
172.17.12.1, 172.17.12.250, igwserver01, 443, 31024, 31025,0, 1, igwuser01, igwpwd01,  1, pr
oxyserver01, 8080, proxyuser01, proxypwd01, 0, 1024
172.17.13.1, 172.17.13.250, igwserver02, 443, 31024, 31025,1, 1, igwuser02, igwpwd02,  1, pr
oxyserver02, 8080, proxyuser02, proxypwd02, 0, 1024
0.0.0.0, 255.255.255.254, igwserver03, 443 , 31024, 31025 ,0, 1, igwuser03, igwpwd03,  1, pr
oxyserver03, 8080, proxyuser03, proxypwd03, 0, 1024
```

この例では、管理対象のコンピュータの IP アドレスが「172.17.13.6」の場合、接続先のインターネットゲートウェイは「igwserver02」という名前のホストで、インターネットゲートウェイの認証時にユーザー ID「igwuser02」、パスワード「igwpwd02」を使用します。またインターネットゲートウェイの接続時にプロキシサーバ「proxyserver02」を使用し、プロキシサーバの認証時にユーザー ID「proxyuser02」、

パスワード「proxypwd02」を使用します。また、インターネットゲートウェイと通信できない場合に、上位システムと直接通信しません。

なお、接続先設定ファイルの各セクションの最終行に、すべての IP アドレスを範囲とする「0.0.0.0～255.255.255.254」を定義しておくと、該当する IP アドレスがなかった場合の接続先となります。この例では 172.17.12.1～172.17.12.250、172.17.13.1～172.17.13.250 以外のコンピュータの接続先インターネットゲートウェイは「igwserver03」になります。

インターネットゲートウェイ接続先設定ファイルを配布したあとの注意事項

インターネットゲートウェイ接続先設定ファイルを管理対象のコンピュータに配布して接続先インターネットゲートウェイが設定されたあと、接続先インターネットゲートウェイの IP アドレスを変更するときは、新しい IP アドレスを設定したインターネットゲートウェイ接続先設定ファイルを管理対象のコンピュータに再配布してください。

1.7　エージェントを自動でインストールする

管理用サーバから各コンピュータに対して、エージェントを自動で配信できます。エージェントを配信するには、次の 2 つの方法があります。

探索と同時にエージェントを自動配信する

探索で発見した OS が Windows のコンピュータに対して、エージェントを自動的に配信できます。発見したコンピュータに順次エージェントが配信されるので、組織内のすべてのコンピュータにエージェントを自動配信したい場合は、この方法を選択してください。

エージェント未導入のコンピュータに個別配信する

管理対象のコンピュータ、および発見したコンピュータに対して、エージェントを個別に配信できます。エージェントを配信するコンピュータを選択できるので、組織内にエージェントをインストールしたくないコンピュータがある場合は、この方法を選択してください。

重要

OS が UNIX、Mac のコンピュータにエージェントの配信はできません（Windows と UNIX や Mac のコンピュータを複数、同時に選択して配信した場合、UNIX や Mac のコンピュータへの配信結果は「配信失敗」になります）。

ヒント

エージェントの OS の表示言語が日本語、英語、中国語以外の場合、そのエージェント自身をリモートインストールした際に、エージェント上で OS から対話型サービスダイアログの検出が表示されることがありますが、インストールは正常に終了するため無視してください。

OS の表示言語は、［コントロールパネル］－［地域と言語］－［キーボードと言語］タブを確認してください。Windows 8、Windows Server 2012 以降の場合は、［コントロールパネル］－［言語］を確認してください。

1.7.1　エージェントのインストール状況を確認する流れ

組織内のコンピュータにエージェントがインストールされているかどうかは、機器画面の［機器情報］画面で確認します。

［機器情報］画面には、管理対象の機器が表示されます。管理対象のコンピュータにエージェントがインストールされているかどうかは、一覧の項目の［管理種別］のアイコンで確認できます。

エージェントをインストールする前後で、［管理種別］欄に表示されるアイコンを次に示します。

-  ：コンピュータにエージェントがインストールされています。

-  ：コンピュータにエージェントはインストールされていません。ただし、エージェントレスのコンピュータとして管理されています。
-  ：コンピュータにエージェントはインストールされていません。

すべてのコンピュータにエージェントがインストールされたかどうかは、手持ちの機器の管理台帳と機器画面の［機器情報］画面に表示されているコンピュータを比較して確認します。

> **ヒント**
>
> 手持ちの管理台帳がない場合は、探索機能を利用して組織内の機器を発見してください。発見した機器を管理対象にすることで、管理台帳を作成できます。

1.エージェント導入済みのコンピュータだけを表示する

フィルタを利用して、［管理種別］が［エージェント管理］のコンピュータだけを表示します。

2.機器情報をエクスポートする

［操作メニュー］から［機器一覧をエクスポートする］または［機器一覧（詳細）をエクスポートする］を選択します。表示されるダイアログでエクスポートする項目を選択して、［OK］ボタンをクリックしてください。エクスポートする項目には、手持ちの管理台帳と突き合わせて確認できる項目を選択します。

3.エージェントのインストール状況を確認する

手持ちの管理台帳とエクスポートしたコンピュータの一覧を比較します。このとき、エクスポートした一覧にないコンピュータが、エージェントをインストールしていないコンピュータになります。

エージェントが未導入のコンピュータがあった場合は、早急にインストールするよう指示してください。なお、エージェントを自動配信している場合は、配信に失敗しているおそれがあります。設定画面の［Windows エージェントの配信］画面で配信状況を確認して再度配信するか、配信に失敗したコンピュータに対してエージェントを手動でインストールしてください。

1.7.2　探索と同時にエージェントを自動配信する手順（ネットワークの探索）

発見したコンピュータに対して自動的にエージェントを配信する方法の一つです。ネットワークの探索と同時にエージェントを配信します。

> **ヒント**
>
> エージェントを配信する際は、各コンピュータに約 80 メガバイトのデータ（インストールセット）が送信されます。インストールセットの容量は、設定に応じて増減します。

探索と同時にエージェントを自動配信するには（ネットワークの探索）：

1. 設定画面の［機器の探索］－［探索条件の設定］－［ネットワークの探索］画面を表示します。

2. [発見した機器への操作]の[編集]ボタンをクリックします。

3. 表示されるダイアログで[エージェントを自動配信する]をチェックします。

4. [OK]ボタンをクリックしてダイアログを閉じます。
   配信するエージェントにリモコンエージェントを含める場合は、手順 5.へ進んでください。リモコンエージェントを含めない場合は、手順 10.へ進んでください。

5. 設定画面の[エージェント]－[Windows エージェントの配信]画面を表示します。

6. [配信するエージェントのコンポーネントの設定]の[編集]ボタンをクリックします。

7. 表示されるダイアログで[リモコンエージェントを含める]をチェックします。

8. [OK]ボタンをクリックしてダイアログを閉じます。

9. 設定画面の[機器の探索]－[探索条件の設定]－[ネットワークの探索]画面を表示します。

10. [探索を開始]ボタンをクリックします。

11. 表示されるダイアログで[OK]ボタンをクリックします。

探索が開始され、発見したコンピュータにエージェントが配信されます。エージェントの配信状況は、設定画面の[エージェント]－[Windows エージェントの配信]画面に表示されます。

1.7.3 機器の探索状況の確認

JP1/IT Desktop Management 2 では、組織内の機器を探索したあと、設定画面の[機器の探索]画面で、探索履歴や発見した機器の状況などを確認できます。探索状況を確認して、組織内の機器の現状を把握します。

機器の探索履歴には、次の 2 つがあります。探索で利用した方法に応じた探索履歴を確認してください。

- Active Directory の探索履歴
- ネットワークの探索履歴

また、機器の管理状態には、次の 3 つがあります。必要に応じて、発見した機器を管理対象にしたり、除外対象にしたりしてください。

発見
: 探索によって発見された機器は、この管理状態になり、設定画面の[機器の探索]－[発見した機器]画面に表示されます。発見した機器は管理対象にしたり、除外対象にしたりできます。

管理対象

JP1/IT Desktop Management 2 で管理したい機器は、この管理状態にします。管理対象の機器は、設定画面の［機器の探索］－［管理対象機器］画面に表示されます。管理対象の機器は除外対象にできます。なお、機器を管理対象にすると、製品ライセンスを消費します。

除外対象

JP1/IT Desktop Management 2 で管理する必要がない機器は、この管理状態に設定します。除外対象の機器は、設定画面の［機器の探索］－［除外対象機器］画面に表示されます。除外対象の機器は管理対象にしたり、削除したりできます。除外対象に設定すると、もう一度機器の探索を行っても、［発見した機器］画面には表示されません。

関連リンク

- 1.7.4　最新の探索状況を確認する手順
- 1.7.5　発見した機器を確認する手順
- 1.7.6　管理対象の機器を確認する手順
- 1.7.7　除外対象の機器を確認する手順

1.7.4　最新の探索状況を確認する手順

最新の探索の実行状況および実行結果を一覧で確認できます。

最新の探索状況を確認するには：

1. 設定画面を表示します。
2. メニューエリアで［機器の探索］－［探索履歴の確認］を選択します。
3. インフォメーションエリアで［Active Directory の探索］または［ネットワークの探索］を選択します。

［Active Directory の探索］画面または［ネットワークの探索］画面が表示されます。探索の進捗に伴って、探索履歴が更新されます。

ヒント

［Active Directory の探索］画面または［ネットワークの探索］画面では、探索を中止したり、実行したりすることもできます。探索エラーが多い場合は、探索を中止して探索条件の設定を見直すことをお勧めします。設定を見直したら、もう一度探索を実行してください。

1.7.5　発見した機器を確認する手順

Active Directory またはネットワークの探索で発見した機器を一覧で確認できます。また、発見した機器は管理対象や除外対象に変更したり、削除したりできます。

発見した機器を確認するには：

1. 設定画面を表示します。
2. メニューエリアで［機器の探索］－［発見した機器］を選択します。

［発見した機器］画面が表示されます。発見した機器の台数や管理できる機器の台数、および管理対象とした機器の台数を確認できます。

インフォメーションエリアで機器を選択して［管理対象にする］ボタンをクリックすると、機器を管理対象にできます。［除外対象にする］ボタンをクリックすると、機器を除外対象にできます。また、［操作メニュー］の［削除する］を選択すると、一覧から機器を削除できます。複数の機器を選択して一括で管理対象や除外対象に変更したり、削除したりすることもできます。

なお、除外対象に設定した機器は、この画面に表示されません。再び機器を管理したい場合は、［除外対象機器］画面で機器の状態を管理対象に変更してください。また、削除した機器を管理したい場合は、再度探索を実行してください。

関連リンク

- 1.7.6　管理対象の機器を確認する手順
- 1.7.7　除外対象の機器を確認する手順

1.7.6　管理対象の機器を確認する手順

JP1/IT Desktop Management 2 で管理している機器を一覧で確認できます。また、管理対象の機器は除外対象に変更したり、削除したりできます。

管理対象の機器を確認するには：

1. 設定画面を表示します。
2. メニューエリアで［機器の探索］－［管理対象機器］を選択します。

［管理対象機器］画面が表示されます。管理対象の機器の台数および管理対象に変更できる機器の台数を確認できます。

インフォメーションエリアで機器を選択して［除外対象にする］ボタンをクリックすると、機器を除外対象にできます。また、［操作メニュー］の［削除する］を選択すると、一覧から機器を削除できます。複数の機器を選択して一括で除外対象に変更したり、削除したりすることもできます。

なお、除外対象に設定した機器は、この画面に表示されません。再び機器を管理したい場合は、[除外対象機器]画面で機器の状態を管理対象に変更してください。

> **ヒント**
>
> 機器を削除すると、もう一度探索したとき、設定画面の［機器の探索］－［発見した機器］画面に表示されるようになります。

関連リンク

- 1.7.7　除外対象の機器を確認する手順

1.7.7　除外対象の機器を確認する手順

JP1/IT Desktop Management 2 で管理しないと設定した機器を一覧で確認できます。また、除外対象の機器は管理対象に変更できます。

除外対象の機器を確認するには：

1. 設定画面を表示します。
2. メニューエリアで［機器の探索］－［除外対象機器］を選択します。

[除外対象機器]画面が表示されます。除外対象の機器の台数および管理対象にできる機器の台数を確認できます。

インフォメーションエリアで機器を選択して［管理対象にする］ボタンをクリックすると、機器を管理対象にできます。また、[操作メニュー]の［削除する］を選択すると、一覧から機器を削除できます。複数の機器を選択して一括で管理対象にしたり、削除したりすることもできます。

> **ヒント**
>
> 機器を削除すると、もう一度探索したとき、設定画面の［機器の探索］－［発見した機器］画面に表示されるようになります。

関連リンク

- 1.7.6　管理対象の機器を確認する手順

1.7.8　エージェント未導入のコンピュータに個別配信する手順

管理対象のコンピュータに対して、エージェントを個別に配信できます。

> **ヒント**
>
> エージェントを配信する際は、各コンピュータに約 80 メガバイトのデータが送信されます。

エージェントを個別配信するには：

1. 設定画面の［エージェント］－［Windows エージェントの配信］画面を表示します。
2. ［配信するエージェントのコンポーネントの設定］の［編集］ボタンをクリックします。
   配信するエージェントにリモコンエージェントを含める場合は、表示されるダイアログで［リモコンエージェントを含める］をチェックします。リモコンエージェントを含めない場合は、チェックを外します。
3. ［OK］ボタンをクリックしてダイアログを閉じます。
4. エージェントを配信したいコンピュータを選択します。
5. ［配信を実行］ボタンをクリックします。
6. 表示されるダイアログで適用するエージェント設定を選択します。
   エージェント設定には、設定画面の［エージェント］－［Windows エージェント設定とインストールセットの作成］画面で作成したエージェント設定が表示されます。エージェント設定の作成については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のエージェント設定の管理について説明している個所を参照してください。
7. ［OK］ボタンをクリックします。

選択したコンピュータにエージェントが配信されます。エージェントの配信状況は、設定画面の［エージェント］－［Windows エージェントの配信］画面に表示されます。

> **ヒント**
>
> エージェントのインストールフォルダは、デフォルトエージェント設定で指定しているフォルダです。インストールフォルダを変更している場合は、ドライブおよび書き込みできるフォルダが指定されている必要があります。なお、指定したエージェント設定はインストール完了後に適用されます。

1.8　中継システムの環境構築

1.8.1　中継システムのインストール方法

中継システムのインストール方法は次の 2 種類があります。 目的に応じて選択してください。

提供媒体からインストールする方法

対象のコンピュータ上で、各種設定をしながらインストールを進めます。インストール終了後にセットアップを実行する必要があります。中継システムごとにインストールおよびセットアップで任意の値を設定したい場合は、この方法をお勧めします。

インストールセットを利用してインストールする方法

まず、中継システム用のインストールセットを作成します。作成したインストールセットを Web サーバやファイルサーバに格納したり、媒体（CD-R や USB メモリ）に書き込んだり、メールに添付したりして配布し、対象のコンピュータ上で中継システムをインストールします。インストールおよびセットアップには、エージェント設定で指定した値が設定されます。

特別な設定をする必要がない場合は、インストールセットを利用してインストールする方法をお勧めします。

ヒント

中継システムがインストールされているかどうかは、機器画面の［機器情報］画面で確認します。

関連リンク

- 1.8.2　中継システムを提供媒体からインストールする手順
- 1.6.1　インストールセットを作成する手順
- 1.6.3　Web サーバでエージェントを公開する
- 1.6.4　ファイルサーバでエージェントを公開する
- 1.6.5　エージェントインストール用の媒体（CD-R や USB メモリ）を配布する
- 1.6.6　メールの添付ファイルでエージェントを配布する

1.8.2　中継システムを提供媒体からインストールする手順

中継システムのインストールを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

重要

コンピュータが Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8 および Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- *システムドライブ*:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

重要

エージェント環境を作成する場合、ユーザ環境変数およびシステム環境変数の TEMP および TMP で定義するディレクトリが存在することを確認してください。

重要

インストール先のドライブは、ローカルディスクを使用してください。ネットワーク接続のディスク（NFS、NAS など）をマウントしインストールしないでください。

ヒント

中継システムは、管理用サーバにはインストールできません。

中継システムを提供媒体からインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Agent］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。

4. [インストールタイプ] ダイアログで、[カスタムインストール] を選択して [次へ] ボタンをクリックします。

5. [インストール先のフォルダ] ダイアログで、インストール先のフォルダを指定して [次へ] ボタンをクリックします。

> **ヒント**
>
> 中継システムのインストール先フォルダのデフォルト値は、「C:¥Program Files¥HITACHI¥jp1itdma」です。ただし、OS が 64 ビット版の Windows の場合は、環境変数%ProgramFiles(x86)%で定義されたフォルダ配下（OS が C ドライブにインストールされているときは、「C:¥Program Files (x86)¥Hitachi¥jp1itdma¥」）になります。

> **重要**
>
> OS が 64 ビット版の Windows の場合、%windir%¥system32 以下のフォルダにインストールしないでください。

> **重要**
>
> インストール先フォルダには、SYSTEM および Administrators グループのフルコントロール権限が必要です。また、適用先として「このフォルダ、サブフォルダおよびファイル」が設定されている必要があります。

6. [インストールするコンポーネントの種別] ダイアログで、[中継システム] を選択して [次へ] ボタンをクリックします。

7. [インストールするコンポーネント] ダイアログで、インストールするほかのコンポーネント、サブコンポーネント、およびそのインストール方法を指定して [次へ] ボタンをクリックします。

> **ヒント**
>
> リモコンエージェントは、中継システムのサブコンポーネントとしてインストールされます。
>
> インストール方法は、文字列の左にあるアイコンをクリックして、プルダウンメニューから選択します。

8. インストールの開始準備の完了を示すダイアログで、[インストール] ボタンをクリックします。

   インストールが実行されます。インストール内容に問題がある場合は、[戻る] ボタンをクリックして設定を修正してください。

9. インストールが完了したら、[完了] ボタンをクリックします。

中継システムのインストールが完了し、セットアップのダイアログが表示されます。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

ヒント

JP1/IT Desktop Management 2 - Agent をインストールすると、同時にデフォルトでリモコンエージェントもインストールされます。リモコンエージェントとは、リモートコントロール時に、接続される側のコンピュータに必要なプログラムです。

1.8.3 中継システムをセットアップする手順

中継システムを提供媒体からインストールした場合、管理用サーバと接続するためにセットアップを実行する必要があります。

なお、セットアップを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

ヒント

インストールセットの配布や管理用サーバからの配信でエージェントを導入した場合は、自動で接続先が設定されるため、接続先を設定するためのセットアップは不要です。

なお、上位接続先情報ファイル（dmhost.txt）を使用して接続先を設定することもできます。上位接続先情報ファイル（dmhost.txt）を JP1/IT Desktop Management 2 - Manager のデータフォルダに格納しておくと、インストールセットの作成時にインストールセットに取り込まれて、各エージェントに配布されます。ただし、エージェントに上位接続先情報ファイルが存在する場合は、エージェント設定の［基本設定］で指定する接続先よりも上位接続先情報ファイルに指定した接続先の方が優先されます。上位接続先情報ファイルの詳細については、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、エージェントの接続先の自動変更についての説明を参照してください。

中継システムをセットアップするには：

1. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Agent］－［管理者ツール］－［セットアップ］を選択します。
   パスワード保護が設定されている場合、パスワードの入力画面が表示されます。該当するエージェント設定に設定したパスワードを入力してください。パスワードのデフォルトは「manager」です。

2. ［セットアップ（中継システム）］ダイアログの［接続先設定］タブで、接続先の管理用サーバのホスト名または IP アドレス、およびポート番号を指定して［OK］ボタンをクリックします。

3. 使用するネットワークアダプタが複数存在する（複数 LAN 接続）環境で、JP1/IT Desktop Management 2 で使う通信回線に優先順位を付けたい場合、［セットアップ（中継システム）］ダイアログの［通信設定］タブで、［ネットワークアダプタの設定］ボタンクリックし、表示されるダイアログで優先順位と自動更新に関する情報を指定して［OK］ボタンをクリックします。

4. 表示される確認ダイアログで［OK］ボタンをクリックします。

セットアップが完了し、設定した内容で中継システムが動作するようになります。

ヒント

中継システムが管理用サーバと接続できている場合、操作画面から中継システムのセットアップを実行できます。操作画面から中継システムをセットアップするには、エージェント設定を利用します。

重要

中継システムは、同一キー名称で登録しないでください。中継システムを同一キー名称で登録すると、中継システムのキー名称変更が、システム構成の経路情報に正しく反映されないことがあります。この場合、変更前後のキー名称を持つ中継するシステムに「システム構成情報の取得」ジョブを実行し、システム構成情報を更新してください。

1.9 リモートインストールマネージャだけをインストールする

1.9.1 リモートインストールマネージャだけをインストールする手順

リモートインストールマネージャのインストールを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

重要

コンピュータが Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8 および Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- *システムドライブ*:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

重要

インストール前は、すべての Windows アプリケーションを終了させてください。誤ってリモートインストールマネージャを起動したままインストールを実行した場合は、インストールの実行結果に関係なく OS を再起動してください。OS を再起動しても、サービスが起動しない場合や、リモートインストールマネージャが動作しない場合は、次に示す手順でインストールを再実行してください。

1. すべての Windows アプリケーションを終了させてください。
2. 上書きインストールを再実行してください。

重要

インストール先のドライブは、ローカルディスクを使用してください。ネットワーク接続のディスク（NFS、NAS など）をマウントしインストールしないでください。

リモートインストールマネージャをインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Manager］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。
4. ［使用許諾契約］ダイアログで、内容を確認してから［使用許諾契約の条項に同意します］を選択し、［次へ］ボタンをクリックします。
5. ［インストールタイプ］ダイアログで、［カスタムインストール］を選択して［次へ］ボタンをクリックします。
6. ［ユーザー登録］ダイアログで、ユーザー名と会社名を入力して［次へ］ボタンをクリックします。
7. ［インストール先のフォルダ］ダイアログで、インストール先のフォルダを指定して［次へ］ボタンをクリックします。
8. ［カスタムインストール］ダイアログで、次のとおりに設定して［次へ］ボタンをクリックします。
   - Manager のプルダウンメニュー：［この機能を使用できないようにします。］
   - Remote Install Manager のプルダウンメニュー：［この機能、およびすべてのサブ機能をローカルのハードディスク ドライブにインストールします。］
9. インストール内容を確認するダイアログで、インストール内容に問題がないことを確認し、［インストール］ボタンをクリックします。

   インストールが実行されます。インストール内容に問題がある場合は、［戻る］ボタンをクリックして設定を修正してください。
10. インストールが完了したら、［完了］ボタンをクリックします。

リモートインストールマネージャのインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

リモートインストールマネージャだけをインストールした場合は、インストール完了後すぐにリモートインストールマネージャを起動し、管理用サーバにアクセスするためのホスト名または IP アドレスと、JP1/IT Desktop Management 2 のユーザーアカウント情報を指定してログオンすれば、操作を開始できます。

2 各システム構成の構築

ここでは、システム構成ごとの構築方法について説明します。

なお、Asset Console を使用した資産管理システムを構築する場合は、別途 JP1/IT Desktop Management 2 - Asset Console をインストールする必要があります。JP1/IT Desktop Management 2 - Asset Console のインストールおよびセットアップ手順については、マニュアル「JP1/IT Desktop Management 2 - Asset Console 構築・運用ガイド」を参照してください。

2.1　オフライン管理構成システムの構築

2.1.1　オフライン管理構成システムを構築する流れ

オフライン管理構成システムを構築するには、まず最小構成システムを構築します。そのあとで、コンピュータにオフライン管理用のエージェントをインストールします。

1. 最小構成システムを構築します。
2. オフライン管理用のエージェントを作成します。
3. オフライン管理したいコンピュータに、オフライン管理用のエージェントを導入します。

オフライン管理構成システムの構築が完了します。

関連リンク

- 1.　管理用サーバとエージェントの構築

2.2　エージェントレス構成システムの構築

2.2.1　エージェントレス構成システムを構築する流れ

エージェントレス構成システムを構築するには、まず管理用サーバを構築します。そのあとで、探索を実行して、発見した機器を管理対象にします。

1. 管理用サーバを構築します。
2. 操作画面から、ネットワークの探索を実行して機器を発見します。
   すべての機器を管理対象にする場合は、探索の設定で、発見した機器を自動的に管理対象にすることもできます。この場合、手順 4.に進んでください。
3. 発見された機器を管理対象にします。
4. 機器の情報を定期的に更新するための設定をします。

エージェントレス構成システムの構築が完了します。

> **ヒント**
>
> エージェント導入済みのコンピュータと、エージェントレスのコンピュータが混在するシステムを構築する場合、最小構成システムを構築したあとで、上記の手順 2.から始めてください。

関連リンク

- 4.1.1　探索条件を設定する手順（ネットワークの探索）
- 1.7.5　発見した機器を確認する手順
- 4.2.1　エージェントレスの機器の情報を定期的に更新する手順

2.3　サポートサービス連携構成システムの構築

2.3.1　サポートサービス連携構成システムを構築する流れ

サポートサービス連携構成システムを構築するには、まず最小構成システムを構築し、そのあとでサポートサービスサイトに接続するための情報を設定します。

1. 最小構成システムを構築します。
2. 操作画面で、サポートサービスサイトに接続するための情報を設定します。

> **ヒント**
>
> 管理対象のコンピュータの更新プログラムの状況を判定したり、判定結果に応じて自動対策したりするには、セキュリティポリシーの設定が必要です。セキュリティポリシーで更新プログラムを管理する方法については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」を参照してください。

サポートサービス連携構成システムの構築が完了します。

関連リンク

- 4.3.1　サポートサービスと接続するための情報を設定する手順

2.4 Active Directory 連携構成システムの構築

2.4.1 Active Directory 連携構成システムを構築する流れ

Active Directory 連携構成システムを構築するには、Active Directory と接続して、Active Directory に登録されているコンピュータを管理対象にします。

1. Active Directory が導入されているシステム内に、管理用サーバを構築します。
2. JP1/IT Desktop Management 2 が Active Directory と接続するための情報を設定します。
3. 必要に応じて、Active Directory で管理されている情報を追加管理項目として取得するように設定します。
4. Active Directory に登録されているコンピュータを探索します。
   すべての機器を管理対象にする場合は、探索の設定で、発見した機器を自動的に管理対象にすることもできます。同様に、探索と同時にエージェントを自動配信することもできます。手順 5.および手順 6.は必要に応じて実施してください。
5. 発見されたコンピュータを管理対象にします。
6. 管理対象のコンピュータに、エージェントを導入します。

Active Directory 連携構成システムの構築が完了します。

関連リンク

- 1.2 管理用サーバの環境構築
- 4.4.1 Active Directory と接続するための情報を設定する手順
- 4.4.2 追加管理項目として Active Directory から取得する情報を設定する手順
- 4.4.3 Active Directory に登録されている機器を探索する手順

2.5 MDM 連携構成システムの構築

2.5.1 MDM 連携構成システムを構築する流れ

MDM 連携構成システムを構築するには、まず最小構成システムを構築し、そのあとで MDM システムからスマートデバイスの情報を取得します。

1. 最小構成システムを構築します。
2. JP1/IT Desktop Management 2 が MDM システムと連携するための情報を設定します。
3. MDM システム に登録されているスマートデバイスの情報を取得します。
   すべてのスマートデバイスを管理対象にする場合は、MDM 連携の設定で、発見したスマートデバイスを自動的に管理対象にすることもできます。手順 4.は必要に応じて実施してください。
4. 発見されたスマートデバイスを管理対象にします。

MDM 連携構成システムの構築が完了します。

関連リンク

- 4.5.1 MDM システムと連携するための情報を設定する手順

2.6　ネットワーク監視構成システムの構築

2.6.1　ネットワーク監視構成システムを構築する流れ

ネットワーク監視構成システムを構築するには、まず最小構成システムを構築します。そのあとでネットワーク制御リストの設定を確認し、ネットワークセグメントごとにネットワークモニタを有効にします。

1. 最小構成システムを構築します。
2. 操作画面からネットワークの探索を実行し、組織内のすべての機器を発見します。
3. ネットワーク制御リストで、ネットワーク接続を許可するかどうかの設定が正しいかを確認します。

> **ヒント**
>
> ネットワーク接続を許可しない機器があった場合は、その機器のネットワーク接続を許可しない設定にしてください。

4. 操作画面から、各ネットワークセグメントのネットワークモニタ機能を有効にします。

   表示されるダイアログで、ネットワークへの接続を許可するネットワークモニタ設定を選択してください。

ネットワーク監視構成システムの構築が完了します。

なお、この手順で構築したシステムでは、新規にネットワーク接続した機器を検知することはできますが、自動的に遮断することはできません。新規にネットワーク接続した機器を自動的に遮断したい場合は、システム構築完了後に、次の設定をしてください。

新規にネットワーク接続した機器を自動的に遮断する

ネットワークモニタ設定で、発見した機器のネットワークへの接続を許可しないように設定し、反映したいネットワークセグメントに割り当ててください。詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の、未登録の機器のネットワーク接続を禁止する流れの説明を参照してください。

> **ヒント**
>
> セキュリティに問題がある機器のネットワーク接続を自動的に遮断することもできます。この場合は、セキュリティポリシーのアクション項目にあるネットワーク接続制御の設定で、セキュリティ状況の判定結果に応じたネットワーク接続の制御を設定してください。

重要

UNIX エージェント、Mac エージェントに対しては、ネットワークモニタを有効にできません。なお、UNIX エージェントの場合、セキュリティポリシーによるネットワーク接続の自動制御もできませんが、手動による接続の許可または遮断はできます。Mac エージェントの場合、セキュリティ状況の判定結果に応じて接続/遮断を自動的に制御できます。

関連リンク

- 4.1.1　探索条件を設定する手順（ネットワークの探索）
- 4.6.1　ネットワーク制御リストの機器を編集する手順
- 2.6.2　ネットワークモニタを有効にする手順
- 4.6.3　ネットワークモニタ設定を追加する手順
- 4.6.4　ネットワークモニタ設定の割り当てを変更する手順

2.6.2　ネットワークモニタを有効にする手順

オンライン管理のコンピュータのネットワークモニタを有効にすると、そのコンピュータが所属するネットワークセグメントに対して、ネットワークに接続された機器を自動的に発見したり、機器のネットワーク接続を制御したりできるようになります。

ネットワークモニタを有効にするには：

1. 機器画面を表示します。
2. メニューエリアの［機器情報］で、［機器一覧（ネットワーク）］から該当するネットワークセグメントを選択します。
3. インフォメーションエリアでエージェント導入済みのコンピュータを選択します。
4. ［操作メニュー］の［ネットワークモニタを有効にする］を選択します。

選択したコンピュータのネットワークモニタが有効になり、ネットワークセグメントのネットワークが監視されます。

ネットワークモニタが有効になっているコンピュータには、管理種別に  、  または  が表示されます。また、メニューエリアのグループに が表示されます。

重要

メニューエリアに表示されるネットワークモニタの動作状態が「ネットワークモニタが有効です」または「ネットワークモニタを有効化しています」の場合、次の操作が制限されます。

- 該当するネットワークのグループを削除できません。
- ネットワークモニタが有効になっているコンピュータは除外対象にできません。また、削除もできません。

重要

ネットワークモニタを有効にする場合、あらかじめ管理用サーバにコンポーネント（ネットワークモニタエージェント）が登録されている必要があります。

重要

UNIX エージェント、Mac エージェントはネットワークモニタを有効にできません。

重要

複数サーバ構成の場合、ネットワークモニタを有効化できるのは、自サーバ直下のコンピュータだけです。

重要

同一の機器に対してネットワークモニタの有効化と無効化を短時間に繰り返し行うと、ネットワークモニタの有効化に失敗する場合があります。失敗した場合は、しばらくしてからネットワークモニタの有効化を再度実行してください。

ヒント

設定画面の［ネットワーク制御］－［ネットワークモニタ設定の割り当て］画面でもネットワークモニタを有効にできます。

ヒント

エージェント導入済みのコンピュータに、提供媒体から「JP1/IT Desktop Management 2 - Network Monitor」をインストールする方法でも、ネットワークモニタを有効にできます。

ヒント

ネットワークモニタを有効にしたコンピュータが複数のネットワークセグメントに所属している場合、所属しているすべてのネットワークセグメントでネットワークモニタが有効になります。

2.7 JP1 認証を使用した構成システムの構築

2.7.1 JP1 認証を使用した構成システムを構築する流れ

JP1 認証を使用した構成システムを構築するには、まず JP1/Base の認証サーバで JP1 ユーザーを登録し、各 JP1 ユーザーに JP1 資源グループおよび JP1 権限レベルを設定します。それから、JP1/IT Desktop Management 2 をインストールし、セットアップの［ユーザー管理の設定］画面で JP1/Base を使用してユーザー管理する設定にします。

重要

JP1 認証を使用した構成システムを構築した場合、IDaaS 連携は使用できません。コンフィグレーションファイル（jdn_manager_config.conf）で IDaaS 連携を使用する設定とした場合でも JP1 認証が使用されます。

構築の流れを次に示します。なお、認証サーバでの設定手順の詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

1. Windows ファイアウォールが有効な環境の場合、管理用サーバから JP1/Base の認証サーバに接続できるよう設定します。

   認証サーバで、ポート番号（20240）を通過できるように設定してください。

2. JP1/Base のバージョンが 11-10 の場合は、 JP1/Base のアクセス権限レベルファイルを更新します。

   JP1/IT Desktop Management 2 のインストールフォルダからファイルをコピーして、JP1/Base のアクセス権限レベルファイルを上書きしてください。その後、JP1/Base の認証サーバで`jbsaclreload`コマンドを実行して、更新内容を適用してください。

   コピー元ファイル

   認証サーバが Windows の場合：

   JP1/IT Desktop Management 2 - Manager のインストールフォルダ¥mgr¥conf¥JP1_AccessLevel.1110Windows

   認証サーバが UNIX の場合：

   JP1/IT Desktop Management 2 - Manager のインストールフォルダ¥mgr¥conf¥JP1_AccessLevel.1110UNIX

   コピー先ファイル

   認証サーバが Windows の場合：

   JP1/Base のインストールフォルダ¥conf¥user_acl¥JP1_AccessLevel

   認証サーバが UNIX の場合：

   共有フォルダ¥jp1base¥conf¥user_acl¥JP1_AccessLevel

3. JP1/IT Desktop Management 2 で使用するユーザーアカウントと、各ユーザーアカウントのユーザー ID、パスワード、権限、業務分掌を検討します。

> **重要**
>
> JP1 認証を使用する場合、管轄範囲を設定することはできません。

ユーザー ID およびパスワードで使用できる文字については、マニュアル「JP1/Base 運用ガイド」を参照してください。

検討結果の例を次の表に示します。

役割	ユーザー ID	パスワード	権限	業務分掌
統括システム管理者	Account01	********	• システム管理権限 • ユーザーアカウント権限	全体
開発部のシステム管理者 A	Account02	********	システム管理権限	• セキュリティ管理 • 資産管理 • 機器管理
開発部のシステム管理者 B	Account03	********	システム管理権限	機器管理

4. JP1/IT Desktop Management 2 で使用する JP1 ユーザーに設定する JP1 資源グループ名を検討します。

JP1 資源グループ名は、1～64 バイトで指定できます。使用できる文字は、半角英数字、および次に示す記号です。

「!」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「-」、「.」、「@」、「¥」、「^」、「_」、「`」、「{」、「}」、および「~」

> **ヒント**
>
> 1 台の管理用サーバにつき、1 つの資源グループを設定できます。複数サーバ構成の場合、管理用サーバごとに異なる JP1 資源グループを設定することで、異なる JP1 権限レベルを設定できます。

5. 認証サーバで JP1 ユーザーを登録し、ユーザー ID とパスワードを指定します。

6. 認証サーバで、各 JP1 ユーザーに JP1 資源グループおよび JP1 権限レベルを設定します。

JP1 権限レベルには、検討した権限と業務分掌を指定します。JP1 権限レベルと JP1/IT Desktop Management 2 の権限・業務分掌との対応については、「2.7.4　JP1 権限レベルと JP1/IT Desktop Management 2 の権限・業務分掌との対応」を参照してください。

7. JP1/IT Desktop Management 2 - Manager をインストールします。

8. JP1/IT Desktop Management 2 - Manager をセットアップします。［ユーザー管理の設定］画面で［JP1/Base を使用してユーザー管理する］を選択して、JP1 資源グループを指定します。

重要

クラスタシステムで JP1/IT Desktop Management 2 を運用する場合は、JP1/Base のクラスタ環境用セットアップで指定する論理ホスト名と、JP1/IT Desktop Management 2 - Manager のセットアップで指定する論理ホスト名とを、同じ名前に設定する必要があります。

2.7.2 ITDM2 認証から JP1 認証に切り替える流れ

ITDM2 認証を使用した構成システムから JP1 認証を使用した構成システムに切り替えるには、まずこれまで使用していた ITDM2 ユーザーの情報を、JP1 ユーザーとして JP1/Base の認証サーバに登録し、各 JP1 ユーザーに JP1 資源グループおよび JP1 権限レベルを設定します。それから、JP1/IT Desktop Management 2 のセットアップ内容を変更し、JP1/Base を使用してユーザー管理する設定にします。最後に、必要に応じて設定画面の［ユーザーアカウントの管理］画面でメールの通知先を追加します。

認証方法を切り替える流れを次に示します。なお、認証サーバでの設定手順の詳細については、マニュアル「JP1/Base 運用ガイド」を参照してください。

重要

JP1 認証を使用する場合、管轄範囲を設定することはできません。管轄範囲を設定したい場合は、ITDM2 認証で運用してください。

1. **Windows ファイアウォールが有効な環境の場合、管理用サーバから JP1/Base の認証サーバに接続できるよう設定します。**

   認証サーバで、ポート番号（20240）を通過できるように設定してください。

2. **JP1/Base のバージョンが 11-10 の場合は、 JP1/Base のアクセス権限レベルファイルを更新します。**

   JP1/IT Desktop Management 2 のインストールフォルダからファイルをコピーして、JP1/Base のアクセス権限レベルファイルを上書きしてください。その後、JP1/Base の認証サーバで`jbsaclreload`コマンドを実行して、更新内容を適用してください。

   コピー元ファイル

   認証サーバが Windows の場合：

   JP1/IT Desktop Management 2 - Manager のインストールフォルダ¥mgr¥conf¥JP1_AccessLevel.1110Windows

   認証サーバが UNIX の場合：

   JP1/IT Desktop Management 2 - Manager のインストールフォルダ¥mgr¥conf¥JP1_AccessLevel.1110UNIX

   コピー先ファイル

   認証サーバが Windows の場合：

   JP1/Base のインストールフォルダ¥conf¥user_acl¥JP1_AccessLevel

認証サーバが UNIX の場合：

共有フォルダ¥jp1base¥conf¥user_acl¥JP1_AccessLevel

3. JP1/IT Desktop Management 2 で使用する JP1 ユーザーに設定する JP1 資源グループ名を検討します。

JP1 資源グループ名は、1～64 バイトで指定できます。使用できる文字は、半角英数字、および次に示す記号です。

「!」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「-」、「.」、「@」、「¥」、「^」、「_」、「`」、「{」、「}」、および「~」

ヒント

1 台の管理用サーバにつき、1 つの資源グループを設定できます。複数サーバ構成の場合、管理用サーバごとに異なる JP1 資源グループを設定することで、異なる JP1 権限レベルを設定できます。

4. これまで使用していた ITDM2 ユーザーを、JP1 ユーザーとして JP1/Base の認証サーバに登録します。

重要

これまで使用していたユーザー ID およびパスワードが JP1/Base に対応していない場合は、ユーザー ID およびパスワードを変更する必要があります。JP1/Base で使用できる文字については、JP1/Base のマニュアル「JP1/Base 運用ガイド」を参照してください。

5. 認証サーバで、各 JP1 ユーザーに JP1 資源グループおよび JP1 権限レベルを設定します。

JP1 権限レベルには、JP1/IT Desktop Management 2 で使用していた権限と業務分掌を指定します。JP1 権限レベルと JP1/IT Desktop Management 2 の権限・業務分掌との対応については、「2.7.4 JP1 権限レベルと JP1/IT Desktop Management 2 の権限・業務分掌との対応」を参照してください。

6. JP1/IT Desktop Management 2 - Manager のセットアップ内容を変更します。［ユーザー管理の設定］画面で［JP1/Base を使用してユーザー管理する］を選択して、JP1 資源グループを指定します。

重要

クラスタシステムで JP1/IT Desktop Management 2 を運用する場合は、JP1/Base のクラスタ環境用セットアップで指定する論理ホスト名と、JP1/IT Desktop Management 2 - Manager のセットアップで指定する論理ホスト名とを、同じ名前に設定する必要があります。

7. イベントやレポートなどの通知先として JP1 ユーザーのメールアドレスを指定したい場合は、設定画面の［ユーザーアカウントの管理］画面でメールの通知先を追加します。

2.7.3 JP1 認証から ITDM2 認証に切り替える流れ

JP1 認証を使用した構成システムから ITDM2 認証を使用した構成システムに切り替えるには、まず設定画面の［ユーザーアカウントの管理］画面で、これまで使用していた JP1 ユーザーの情報を ITDM2 ユーザーとして登録します。それから、JP1/IT Desktop Management 2 のセットアップ内容を変更し、JP1/Base を使用してユーザー管理する設定を解除します。

認証方法を切り替える流れを次に示します。

1. 設定画面の［ユーザーアカウントの管理］画面で、これまで使用していた JP1 ユーザーの情報を ITDM2 ユーザーとして追加します。
2. JP1/IT Desktop Management 2 - Manager のセットアップ内容を変更します。［ユーザー管理の設定］画面で［JP1/Base を使用してユーザー管理する］のチェックを解除してください。

2.7.4 JP1 権限レベルと JP1/IT Desktop Management 2 の権限・業務分掌との対応

JP1 権限レベルと JP1/IT Desktop Management 2 の権限・業務分掌との対応を、次に示します。

項番	種別	権限名または業務分掌名	JP1 権限レベルの操作権限名
1	共通	システム管理権限、ユーザーアカウント権限、およびすべての業務分掌を持つ権限レベル。JP1/IT Desktop Management 2 のビルトインアカウントと同じ権限を持つ。	JP1_ITDM_Admin
2	権限※1	システム管理権限	JP1_ITDM_SystemAdmin
3		ユーザーアカウント管理権限	JP1_ITDM_UserManage
4		参照権限	JP1_ITDM_Reference
5		API 権限	JP1_ITDM_API_Admin
6	業務分掌※2	セキュリティ管理および配布管理	JP1_ITDM_Security
7		資産管理	JP1_ITDM_Assets
8		機器管理	JP1_ITDM_Inventory
9		配布管理	JP1_ITDM_Distribution
10		システム設定管理※3	JP1_ITDM_Settings

注※1

同じ JP1 資源グループに参照権限を含む複数の権限を指定した場合、参照権限および API 権限以外の権限が優先されます。

また、同じ JP1 資源グループに API 権限を含む複数の権限を指定した場合、API 権限は無視されます。

注※2

業務分掌の操作権限を指定した場合、参照権限を指定していなくても、該当する業務分掌の参照権限が自動で付与されます。

注※3

システム設定管理を指定する場合は、システム管理権限も指定する必要があります。システム設定管理だけを指定しても、システム設定の操作はできません。

なお、指定する権限と業務分掌の組み合わせによっては、操作が制限されます。詳細については、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」の、ユーザーアカウントの権限ごとの操作範囲の説明およびユーザーアカウントの業務分掌ごとの操作範囲の説明を参照してください。

2.8 JP1/NETM/NM - Manager 連携構成システムの構築

2.8.1 JP1/NETM/NM - Manager 連携構成システムを構築する流れ

JP1/NETM/NM - Manager と連携するには、まず最小構成システムを構築し、そのあとでネットワーク制御用アプライアンスを配置します。それから、JP1/NETM/NM - Manager を導入し、JP1/NETM/NM - Manager 連携を有効にします。

JP1/NETM/NM - Manager をインストールする手順およびセットアップする手順については、マニュアル「JP1 Version 9 JP1/NETM/Network Monitor - Manager」またはマニュアル「JP1 Version 10 JP1/NETM/Network Monitor - Manager」のインストールとセットアップの説明を参照してください。JP1/NETM/NM - Manager を設定する手順は、マニュアル「JP1 Version 9 JP1/NETM/Network Monitor」またはマニュアル「JP1 Version 10 JP1/NETM/Network Monitor」の操作方法の説明を参照してください。

1. 最小構成システムを構築します。
2. ネットワーク制御用アプライアンスを監視対象のネットワークセグメントに配置し、セットアップします。
3. 管理用サーバに JP1/NETM/NM - Manager をインストールします。
4. JP1/NETM/NM - Manager をセットアップします。

   JP1/IT Desktop Management 2 をクラスタシステムで運用する場合は、同じ待機系サーバを利用して JP1/NETM/NM - Manager もクラスタシステムで運用してください。
5. JP1/NETM/NM - Manager で監視対象のネットワークセグメントとグループを登録します。
6. JP1/NETM/NM - Manager でネットワーク制御用アプライアンスの環境設定を実施します。
7. ネットワーク制御用アプライアンスで検疫通信情報の設定（特例接続の設定）を実施します。
8. JP1/IT Desktop Management 2 の［設定］－［ネットワーク制御］－［ネットワークモニタ設定の割り当て］画面で、JP1/NETM/NM - Manager に登録した監視対象のネットワークセグメントを、非監視時に通知しない設定にします。

   ブラックリスト方式でネットワーク接続を管理する場合は、手順 9.は不要です。ホワイトリスト方式でネットワーク接続を管理する場合だけ手順 9.を実施してください。
9. 管理用サーバに格納されている、ネットワーク制御設定ファイル（jdn_networkcontrol.conf）を編集します。手順については、「4.6.6 ネットワーク制御設定ファイルを編集する手順」を参照してください。
10. JP1/IT Desktop Management 2 で、JP1/NETM/NM - Manager 連携を有効にします。

手順については、「4.6.5　JP1/NETM/NM - Manager 連携の設定を有効にする手順」を参照してください。

JP1/NETM/NM - Manager 連携構成システムの構築が完了します。

重要

JP1/NETM/NM - Manager と連携する場合、ネットワーク制御用アプライアンスの許可機器一覧および排除機器一覧は、JP1/IT Desktop Management 2 - Manager のネットワーク制御リストの内容に置き換わります。このため、JP1/IT Desktop Management 2 - Manager と連携する前に、ネットワーク制御用アプライアンスの許可機器一覧および排除機器一覧を登録していた場合、その内容が失われます。ネットワーク制御リストの内容と JP1/IT Desktop Management 2 - Manager と連携する前に登録していた許可機器一覧および排除機器一覧に差異がある場合は、必要に応じてネットワーク制御リストに登録してから、JP1/NETM/NM - Manager と連携する設定をしてください。

重要

JP1/NETM/NM - Manager と連携する場合、ネットワーク制御用アプライアンスの検疫通信情報に次のサーバを登録し、機器がネットワークから遮断されてもこれらのサーバと通信できるようにしてください。

- 管理用サーバ

関連リンク

- 1.1.1　最小構成システムを構築する流れ

2.8.2　NX NetMonitor/Manager 連携構成システムを構築する流れ

NX NetMonitor/Manager と連携する場合は、このマニュアルに記載している「JP1/NETM/NM - Manager」を「NX NetMonitor/Manager」に読み替えてください。

2.9 JP1/IM 連携構成システムの構築

2.9.1 JP1/IM 連携構成システムを構築する流れ

JP1/IM 連携構成システムを構築するには、まず管理用サーバを構築します。そのあとで、JP1/IM をインストールして、必要な設定をします。

1. 管理用サーバを構築します。
2. 管理用サーバに JP1/Base をインストールします。
3. コンフィグレーションファイルにプロパティを設定します。
4. JP1/IM - Manager、および JP1/IM - View をインストールします。
5. イベント拡張属性定義ファイルを JP1/IM の所定のフォルダにコピーします。

   イベント拡張属性定義ファイルのコピー元ファイル

   JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥definition¥hitachi_jp1_itdm_attr_ja.conf

   JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥definition¥hitachi_jp1_itdm_attr_en.conf

   JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥definition¥hitachi_jp1_itdm_attr_zh.conf

   イベント拡張属性定義ファイルのコピー先フォルダ

   JP1/IM - Manager の Console パス¥conf¥console¥attribute

   デフォルトの JP1/IM - Manager の Console パスは、次のとおりです。

   システムドライブ:¥Program Files¥HITACHI¥JP1Cons
6. JP1/IM - Manager を再起動します。

   再起動後にイベント拡張属性定義ファイルの設定が有効になります。
7. JP1/Base と JP1/IM の接続設定をします。
8. JP1/IT Desktop Management 2 と JP1/Base を再起動します。

   JP1/IM 連携構成システムの構築が完了し、通知対象のイベントが発生すると、JP1/IM に通知されます。

JP1/Base のインストール手順や設定については、マニュアル「JP1/Base 運用ガイド」を参照してください。JP1/IM のインストール手順や設定については、マニュアル「JP1/Integrated Management - Manager 構築ガイド」を参照してください。イベント拡張属性定義ファイルの配置やフォーマットについては、マニュアル「JP1/Integrated Management - Manager コマンド・定義ファイルリファレンス」を参照してください。

重要

JP1/IM と JP1/Base が接続できていない場合、システムの運用時に、通知対象のエラーメッセージやイベントは JP1/IM には通知されません。JP1/IM 連携システムの構築時に、JP1/IM と JP1/Base の接続状況を確認してください。

関連リンク

- 4.7.1　JP1/IM と連携するためのコンフィグレーションファイルを設定する手順

2.10　クラスタシステムの構築

2.10.1　クラスタシステムを構築する流れ

クラスタシステムを構築する場合、管理用サーバの構築から開始します。

クラスタシステムを構築するには：

1. 現用系サーバと待機系サーバに JP1/IT Desktop Management 2 - Manager をインストールします。
   インストールタイプは、カスタムインストールを選択してください。また、インストール完了後は、続けてセットアップを実行しないでください。
2. 現用系サーバでリソースグループを作成します。
3. 現用系サーバをセットアップします。
4. 現用系サーバのセットアップ完了時に出力されるファイルを待機系サーバにコピーします。
5. 待機系サーバでセットアップを実行するために、手順 2.で作成したリソースグループの所有者を待機系サーバに移動します。
6. 待機系サーバをセットアップします。
7. クラスタシステムの運用を開始するために、手順 2.で作成したリソースグループの所有者を現用系サーバに移動します。
8. JP1/IT Desktop Management 2 の一部のサービスリソースをオンラインにします。
   Windows Server Failover Cluster で管理用サーバのグループに登録したサービスリソース（汎用サービス）のリソースのうち、「JP1_ITDM2_Service」と「JP1_ITDM2_Agent Control」以外をオンライン状態にします。
9. 操作画面からライセンス登録をします。
10. JP1/IT Desktop Management 2 のサービスリソースをオンラインにします。
    「JP1_ITDM2_Service」と「JP1_ITDM2_Agent Control」をオンライン状態にします。

クラスタシステムの構築が完了します。

関連リンク

- 1.2.2　JP1/IT Desktop Management 2 - Manager をインストールする手順（単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバの場合）
- 2.10.2　現用系サーバでリソースグループを作成する手順
- 2.10.3　現用系サーバで JP1/IT Desktop Management 2 をセットアップする

• 2.10.4　待機系サーバで JP1/IT Desktop Management 2 をセットアップする

2.10.2　現用系サーバでリソースグループを作成する手順

JP1/IT Desktop Management 2 のインストール後は、Windows Server Failover Cluster で JP1/IT Desktop Management 2 のグループを作成し、リソースを登録します。リソースを登録する手順を次に示します。

1. 管理用サーバのグループを作成します。

   管理用サーバ用に新しく空の役割を作成してください。

2. 作成したグループに必要なリソースを登録します。

   グループに登録が必要なリソースを次の表に示します。

リソースの種類	リソース名
JP1/IT Desktop Management 2 のサービスリソース以外のリソース	クライアントアクセスポイント※1
	記憶域（共有ディスク）
JP1/IT Desktop Management 2 のサービスリソース（汎用サービス）	JP1_ITDM2_DB Service
	JP1_ITDM2_DB Cluster Service
	JP1_ITDM2_Web Container
	JP1_ITDM2_Web Server※2
	JP1_ITDM2_Service
	JP1_ITDM2_Agent Control
	JP1_ITDM2_Relay Manager Service※3

   注※1　ネットワーク名には JP1/IT Desktop Management 2 で利用する論理ホスト名を指定します。IP アドレスには JP1/IT Desktop Management 2 で利用する論理 IP アドレスを指定します。

   注※2　Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016 および Windows Server 2012 の場合はリソースを登録した後に、コマンドを実行します。

   Administrator 権限を持つユーザーで、コマンドプロンプトから Windows PowerShell を起動し、次に示すコマンドを実行してください。

   Get-ClusterResource△"*JP1_ITDM2_Web Server サービスリソースの名前*"△|△Set-ClusterParameter△-Name△StartupParameters△-value△""

   （凡例）△：半角スペース

   注※3　複数サーバ構成の統括管理用サーバの場合だけ実施してください。

3. 現用系サーバを優先サーバに設定します。

4. JP1/IT Desktop Management 2 のサービスリソース以外のリソースをオンライン状態にします。

JP1/IT Desktop Management 2 のサービスリソース（汎用サービス）はオフライン状態のままです。

以降で、各リソースの設定項目および設定内容を説明します。

JP1/IT Desktop Management 2 のサービスリソース以外のリソースの設定内容

リソース名	設定項目	設定内容
• クライアントアクセスポイント • 記憶域（共有ディスク）	再起動期間（群:ss）	15:00（推奨値）
	指定期間内での再起動の試行回数	1（推奨値）
	保留タイムアウト（mm:ss）	05:00（推奨値）

JP1_ITDM2_DB Service の設定内容

リソース名	設定項目	設定内容
JP1_ITDM2_DB Service	名前	任意の名称を指定する。
	種類	「汎用サービス」
	サービス名	「HiRDBEmbeddedEdition_JE1」を設定する。
	依存関係	「クライアントアクセスポイント」および「記憶域（共有ディスク）」のリソースを設定する。
	再起動期間（mm:ss）	00:00（固定）
	指定期間内での再起動の試行回数	0（固定）
	保留タイムアウト（mm:ss）	05:00（推奨値）
	実行可能な所有者	現用系および待機系の 2 台のサーバを設定する。
	レジストリのレプリケーション	指定しない。

JP1_ITDM2_DB Cluster Service の設定内容

リソース名	設定項目	設定内容
JP1_ITDM2_DB Cluster Service	名前	任意の名称を指定する。
	種類	「汎用サービス」
	サービス名	「HiRDBClusterService_JE1」を設定する。
	依存関係	「JP1_ITDM2_DB Service」のリソースを設定する。
	再起動期間（mm:ss）	15:00（推奨値
	指定期間内での再起動の試行回数	1（推奨値）

リソース名	設定項目	設定内容
JP1_ITDM2_DB Cluster Service	保留タイムアウト（mm:ss）	05:00（推奨値）
	実行可能な所有者	現用系および待機系の 2 台のサーバを設定する。
	レジストリのレプリケーション	指定しない。

JP1_ITDM2_Web Container の設定内容

リソース名	設定項目	設定内容
JP1_ITDM2_Web Container	名前	任意の名称を指定する。
	種類	「汎用サービス」
	サービス名	「JP1_DTNAVI_WEBCON」を設定する。
	依存関係	「JP1_ITDM2_DB Cluster Service」のリソースを設定する。
	再起動期間（mm:ss）	15:00（推奨値）
	指定期間内での再起動の試行回数	1（推奨値）
	保留タイムアウト（mm:ss）	05:00（推奨値）
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	レジストリのレプリケーション	指定しない。

JP1_ITDM2_Web Server の設定内容

リソース名	設定項目	設定内容
JP1_ITDM2_Web Server	名前	任意の名称を指定する。
	種類	「汎用サービス」
	サービス名	「JP1_DTNAVI_WEBSVR」を設定する。
	依存関係	「クライアントアクセスポイン」のリソースを設定する。
	再起動期間（mm:ss）	15:00（推奨値）
	指定期間内での再起動の試行回数	1（推奨値）
	保留タイムアウト（mm:ss）	05:00（推奨値）
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	レジストリのレプリケーション	指定しない。

JP1_ITDM2_Service の設定内容

リソース名	設定項目	設定内容
JP1_ITDM2_Service	名前	任意の名称を指定する。
	種類	「汎用サービス」
	サービス名	「JP1_DTNAVI_MGRSRV」を設定する。
	依存関係	「JP1_ITDM2_DB Cluster Service」のリソースを設定する。
	再起動期間（mm:ss	15:00（推奨値）
	指定期間内での再起動の試行回数	1（推奨値）
	保留タイムアウト（mm:ss）	05:00（推奨値）
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	レジストリのレプリケーション	指定しない。

JP1_ITDM2_Agent Control の設定内容

リソース名	設定項目	設定内容
JP1_ITDM2_Agent Control	名前	任意の名称を指定する。
	種類	「汎用サービス」
	サービス名	「JP1_DTNAVI_AGCTRL」を設定する。
	依存関係	「JP1_ITDM2_DB Cluster Service」のリソースを設定する。
	再起動期間（mm:ss）	15:00（推奨値）
	指定期間内での再起動の試行回数	1（推奨値）
	保留タイムアウト（mm:ss）	05:00（推奨値）
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	レジストリのレプリケーショ	指定しない。

JP1_ITDM2_Relay Manager Service の設定内容

リソース名	設定項目	設定内容
JP1_ITDM2_Relay Manager Service	名前	任意の名称を指定する。
	種類	「汎用サービス」

リソース名	設定項目	設定内容
JP1_ITDM2_Relay Manager Service	サービス名	「JP1_DTNAVI_RLYMGRSRV」を設定する。
	依存関係	「JP1_ITDM2_DB Cluster Service」のリソースを設定する。
	再起動期間（mm:ss）	15:00（推奨値）
	指定期間内での再起動の試行回数	1（推奨値）
	保留タイムアウト（mm:ss）	05:00（推奨値）
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	レジストリのレプリケーション	指定しない。

2.10.3 現用系サーバで JP1/IT Desktop Management 2 をセットアップする

ここでは、セットアップ画面のうち、クラスタシステムを運用するための設定が必要なものについて説明します。

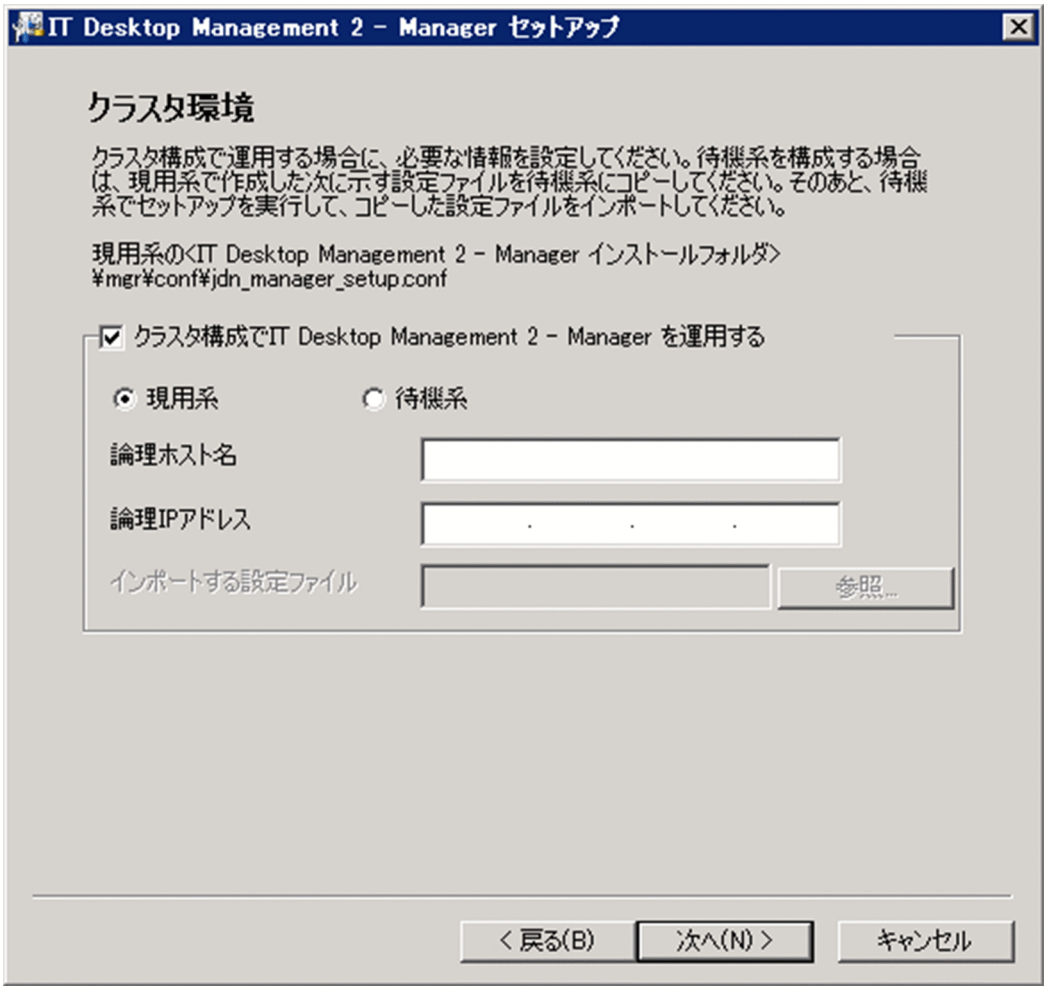
重要

コンピュータが Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016 または Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- *システムドライブ*:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

［クラスタ環境］画面の設定内容

セットアップの［クラスタ環境］画面で、クラスタシステムを運用するための設定をします。［クラスタ環境］画面を次の図に示します。



次のように設定してください。

- ［クラスタ構成で IT Desktop Management 2 - Manager を運用する］をチェックする。
- ［現用系］を選択する。
- ［論理ホスト名］および［論理 IP アドレス］を設定する。

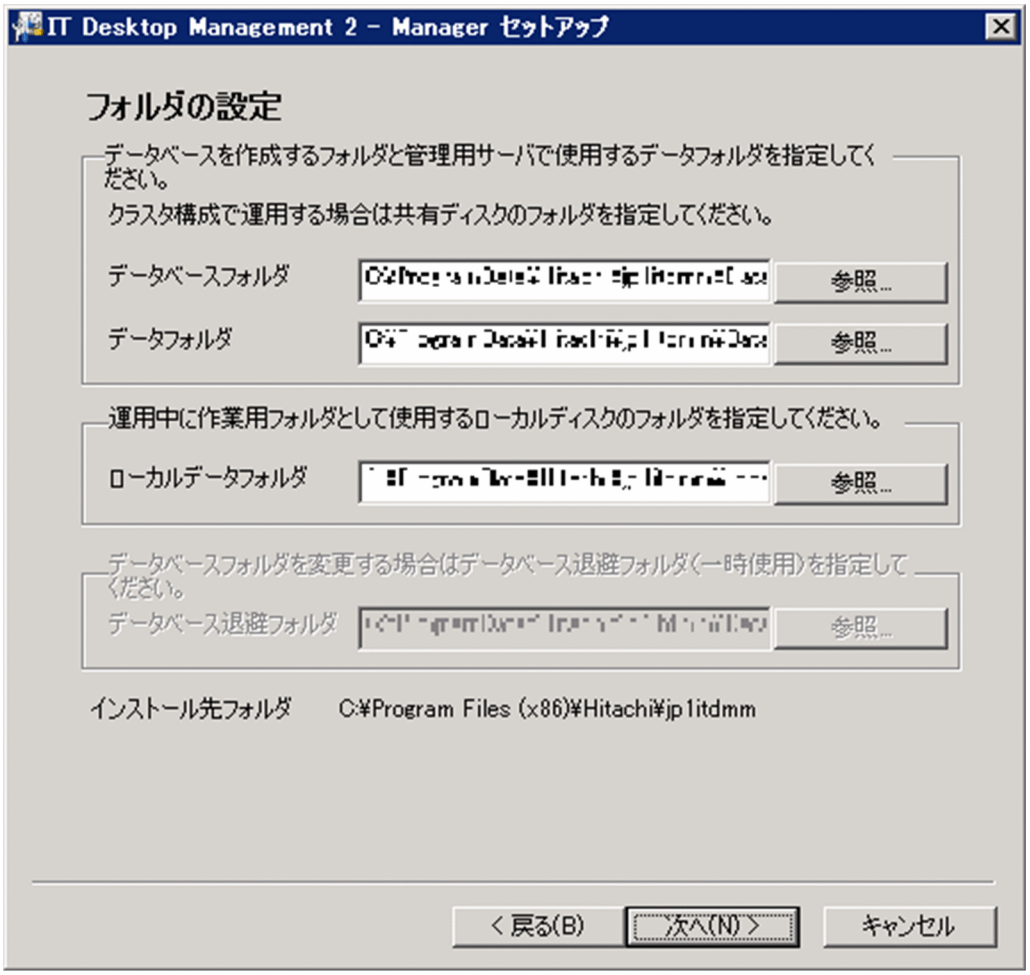
このとき、［インポートする設定ファイル］は設定不要です。

セットアップが完了すると、次に示すファイルが出力されます。このファイルを待機系サーバにコピーしてください。

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥conf¥jdn_manager_setup.conf

［フォルダの設定］画面の設定内容

セットアップの［フォルダの設定］画面で、クラスタシステムを運用するための設定をします。［フォルダの設定］画面を次の図に示します。



次に示す項目に共有ディスクのパスを設定してください。

- [データベースフォルダ]
- [データフォルダ]

また、以降の画面で、次に示す項目に共有ディスクのパスを設定してください。

- [操作ログの設定]画面の[操作ログのデータベースフォルダ](操作ログを取得する場合)、および[操作ログの保管先フォルダ](操作ログの保管先フォルダにローカルディスク上のフォルダを指定する場合)
- [保存用の変更履歴の出力設定]画面の[変更履歴の出力先フォルダ](変更履歴の出力先フォルダにローカルディスク上のフォルダを指定する場合)

このほかの項目については、通常のセットアップと同じです。

関連リンク

- 1.2.4　単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順

2.10.4　待機系サーバで JP1/IT Desktop Management 2 をセットアップする

現用系サーバでの設定と同様に、待機系サーバでのセットアップを実行します。

ここでは、セットアップ画面のうち、クラスタシステムを運用するための設定が必要なものについて説明します。

セットアップの［クラスタ環境］画面では、次のように設定してください。

- ［クラスタ構成で IT Desktop Management 2 - Manager を運用する］をチェックする。
- ［待機系］を選択する。
- ［インポートする設定ファイル］に現用系サーバでの設定でコピーしたファイルを指定する。

［フォルダの設定］画面の設定内容は、通常のセットアップと同じです。ただし、待機系サーバをセットアップする場合は、次に示す項目は非活性表示され設定できません。

- ［データベースフォルダ］
- ［データフォルダ］
- ［データベース退避フォルダ］

また、待機系サーバでエージェントを登録する必要はありません。

関連リンク

- 1.2.4　単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順

2.11　社外で利用する機器を管理する環境の構築

2.11.1　インターネットゲートウェイを構築する手順

インターネットゲートウェイを構築するには、まず管理用サーバを構築します。そのあとで、Microsoft Internet Information Services およびインターネットゲートウェイをインストールします。インターネットゲートウェイの構築手順を次に示します。

重要

インターネットゲートウェイは、クラスタシステムをサポートしていません。

重要

インストール先のドライブは、ローカルディスクを使用してください。ネットワーク接続のディスク（NFS、NAS など）をマウントしインストールしないでください。

インターネットゲートウェイを構築する流れ

インターネットゲートウェイを構築する流れを次に示します。なお、手順 1 から手順 5 はインターネットゲートウェイのサーバ、手順 6 はインターネットと DMZ の間および DMZ と社内ネットワークの間のファイアウォール、手順 7 から手順 8 は管理対象のコンピュータで、それぞれ実施します。

1. エージェントまたは中継システムを導入します。リモートインストールマネージャを使用した配布を使用する場合は、中継システムを導入してください。

   中継システムを導入する場合、中継システムへの同時接続数の設定を 50 から 100 に変更してください。エージェント設定の［中継システムの設定］－［中継システムの処理の設定］－［中継システムへの同時接続 JP1/IT Desktop Management 2 - Agent 数］の設定値を変更します。

2. Microsoft Internet Information Services をインストールします。
3. インターネットゲートウェイをインストールします。
4. インターネットゲートウェイをセットアップします。
5. Microsoft Internet Information Services を設定します。
6. ファイアウォールを設定します。
7. JP1/IT Desktop Management 2 の管理対象とするコンピュータに、インターネット接続用のエージェントをインストールします。
8. 管理対象のコンピュータでインターネットゲートウェイへの接続確認をします。

関連リンク

- 2.11.1　インターネットゲートウェイを構築する手順
- (1)　Microsoft Internet Information Services をインストールする手順
- (2)　インターネットゲートウェイをインストールする手順
- (3)　インターネットゲートウェイをセットアップする手順
- (4)　Microsoft Internet Information Services を設定する手順
- 2.11.2　ファイアウォールの設定
- 2.11.3　社外で利用する機器のエージェントを構築する手順

(1)　Microsoft Internet Information Services をインストールする手順

インターネットゲートウェイのサーバに Microsoft Internet Information Services をインストールします。サーバーの役割として「Web サーバー(IIS)」を次の表の内容で追加します。

項目		役割サービス
Web サーバー	HTTP 共通機能	HTTP エラー
		ディレクトリの参照
		既定のドキュメント
		静的なコンテンツ
	セキュリティ	基本認証
	アプリケーション開発	ISAPI 拡張
管理ツール		IIS 管理コンソール

(2)　インターネットゲートウェイをインストールする手順

インターネットゲートウェイのインストールを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

重要

インストール前は、すべての Windows アプリケーションを終了させてください。

重要

JP1/IT Desktop Management 2 を含む他製品がインストールされているフォルダを、インターネットゲートウェイのインストール先のフォルダとして指定しないでください。

重要

インストール先のドライブは、ローカルディスクを使用してください。

ネットワーク接続のディスク（NFS、NAS など）をマウントしインストールしないでください。

インターネットゲートウェイをインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Internet Gateway］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。
4. ［インストール先のフォルダ］ダイアログで、インストール先のフォルダを指定して［次へ］ボタンをクリックします。
5. インストールの開始準備の完了を示すダイアログで、［インストール］ボタンをクリックします。
   インストールが実行されます。
6. インストールの完了を示すダイアログで、［完了］ボタンをクリックします。

インターネットゲートウェイのインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

(3) インターネットゲートウェイをセットアップする手順

JP1/IT Desktop Management 2 - Internet Gateway をインストールした場合、インストール直後にセットアップを実行する必要があります。

インターネットゲートウェイをセットアップするには：

1. World Wide Web Publishing Service サービス※1 が開始されている場合、停止します。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Internet Gateway］－［インターネットゲートウェイセットアップ］を選択します。

3. [IT Desktop Management 2 - Internet Gateway 設定] ダイアログでインターネットゲートウェイの上位システムを設定します※2。

4. [OK] ボタンをクリックします。

注※1　Windows Server 2025、Windows Server 2022、Windows Server 2019 または Windows Server 2016 の場合、「World Wide Web 発行サービス」です。

注※2

リモートインストールマネージャを使用した配布を使用する場合

インターネットゲートウェイサーバに中継システムをインストールし、「リモートインストールマネージャを使用した配布用の上位システム」に［中継システム］、「ホスト名または IP アドレス」に localhost を設定します。

リモートインストールマネージャを使用した配布を使用しない場合

「リモートインストールマネージャを使用した配布用の上位システム」に［管理用サーバ］、「ホスト名または IP アドレス」に管理用サーバのホスト名または IP アドレスを設定します。

(4)　Microsoft Internet Information Services を設定する手順

インターネットゲートウェイのセットアップ後に、Microsoft Internet Information Services を設定する必要があります。Microsoft Internet Information Services の詳細な設定方法については、Microsoft Internet Information Services のマニュアルを参照してください。

Microsoft Internet Information Services の設定の流れ：

1. ISAPI の制限を設定します。

2. サーバー証明書を設定します。

3. アプリケーションを追加して設定します。

4. フォルダ権限を設定します。

5. World Wide Web Publishing Service サービス※を開始します。

注※　Windows Server 2025、Windows Server 2022、Windows Server 2019 または Windows Server 2016 の場合、「World Wide Web 発行サービス」です。

ISAPI の制限を設定するには：

インターネットゲートウェイサーバの「ISAPI および CGI の制限」で、次の設定を追加します。

［ISAPI または CGI パス］	［拡張パスの実行を許可する］
インターネットゲートウェイのインストール先フォルダ¥igw¥web¥itdm¥jdngwsvr.dll	チェックする
インターネットゲートウェイのインストール先フォルダ¥igw¥web¥dm¥jdngwsvr_dm.dll	チェックする

[ISAPI または CGI パス]	[拡張パスの実行を許可する]
インターネットゲートウェイのインストール先フォルダ¥igw¥web¥relay¥jdngwsvr_relay.dll	チェックする

サーバ証明書を設定するには：

インターネットゲートウェイサーバの「サーバー証明書」で、サーバ証明書の要求を完了します。

証明書の要求の完了する証明機関によって証明されたサーバー証明書

証明機関によって証明されたサーバー証明書のファイルパス※

注※　サーバ証明書ファイルはインターネットゲートウェイのインストール先フォルダに格納しないでください。

フレンドリ名

任意

アプリケーションの追加と設定をするには：

Microsoft Internet Information Services に次の構成を追加します。

Microsoft Internet Information Services の項目	設定項目	設定内容		
サイト	名前	Default Web Site		
	サイトバインド※1	• 種類：https • IP アドレス：未使用の IP すべて • ポート番号：443※2 • ホスト名：インターネットゲートウェイサーバの FQDN • サーバ名表示を要求する：チェックする • SSL 証明書：「サーバ証明書を設定するには：」で設定したフレンドリ名		
	有効なプロトコル	https		
	認証	• 基本認証：有効※3 • 匿名認証：無効		
アプリケーション	エイリアス	jp1itdmigw1	jp1itdmigw2	jp1itdmigw3
	アプリケーションプール	AppPooljp1itdmigw1	AppPooljp1itdmigw2	AppPooljp1itdmigw3
	物理パス	*インターネットゲートウェイのインストール先フォルダ*¥igw¥web¥itdm	*インターネットゲートウェイのインストール先フォルダ*¥igw¥web¥dm	*インターネットゲートウェイのインストール先フォルダ*¥igw¥web¥relay¥
	有効なプロトコル	https		
	「ハンドラーマッピング」の「機能のアクセス許可の編集」	実行：有効		

Microsoft Internet Information Services の項目	設定項目	設定内容		
アプリケーション	HTTP 応答ヘッダー	• 名前：X-Content-Type-Options 値：nosniff • 名前：X-XSS-Protection 値：1; mode=block • 名前：Content-Security-Policy 値：frame-ancestors 'none'		
アプリケーションプール	「全般」の「名前」	AppPooljp1itdmigw1	AppPooljp1itdmigw2	AppPooljp1itdmigw3
	「全般」の「32 ビットアプリケーションの有効化」	True		
	「プロセスモデル」の「アイドルタイムアウトの操作」	• Windows Server 2012（IIS 8.0）の場合：設定項目なし • Windows Server 2012 R2（IIS 8.5）以降の場合：Suspend		
	「リサイクル」の「定期的な時間（分）」	0		

注※1　デフォルトで設定されている「種類：http ポート：80」の行は削除してください。

注※2　設定内容をエージェント設定の［インターネット接続設定］－［インターネットゲートウェイ］－［ポート番号］に指定してください。

注※3　必要に応じて有効または無効を設定してください。また、設定内容をエージェント設定の［インターネットゲートウェイの通信設定］に指定してください。

フォルダ権限を設定するには：

次のフォルダに対して、認証に使用するユーザー※に「変更」権限を付与してください。

- *インターネットゲートウェイのインストール先フォルダ*¥log
- *インターネットゲートウェイのインストール先フォルダ*¥igw¥Web¥work

エージェント設定の［インターネットゲートウェイの通信設定］－［ユーザー認証する］－［ユーザー ID］に指定するユーザーが該当します。［ユーザー ID］を指定しない場合（サイトの認証に「匿名認証」を使用する場合）は「IUSR」が該当します。

2.11.2　ファイアウォールの設定

インターネットゲートウェイとインターネットの間にあるファイアウォール

インターネットゲートウェイとインターネットの間にあるファイアウォールでは、設定画面のエージェント設定で、［基本設定］－［インターネット接続設定］－［インターネットゲートウェイ］の［ホスト名またはIPアドレス］および［ポート番号］に設定したホストおよびポートを通過できるように、インターネットからDMZへのインバウンド通信を許可する設定をしてください。

インターネットゲートウェイと管理用サーバおよびリモートインストールマネージャの間にあるファイアウォール

インターネットゲートウェイと管理用サーバおよびリモートインストールマネージャの間にあるファイアウォールでは、管理用サーバおよびリモートインストールマネージャとの通信で使用するポートが通過できるように、DMZから社内ネットワークへのインバウンド通信を許可する設定をしてください。詳細は、「付録 A.1　ポート番号一覧」を参照してください。

2.11.3　社外で利用する機器のエージェントを構築する手順

社外で利用するコンピュータをJP1/IT Desktop Management 2で管理する場合、コンピュータにエージェントをインストールして、インターネットゲートウェイを経由して上位システムと接続できるように設定します。

管理対象のコンピュータにエージェントをインストールする手順の詳細は、「1.6.2　エージェントをコンピュータに導入する方法」を参照してください。

エージェントのセットアップ手順の詳細は、「1.6.10　エージェントをセットアップする手順」を参照してください。

インターネットゲートウェイを経由して上位システムと接続できるように設定する手順の詳細は、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の「社外で利用する機器を管理する手順」の説明を参照してください。

接続確認をするには：

エージェントのセットアップ後に、インターネットゲートウェイとの接続確認をします。接続確認は、エージェントのログファイルを参照します。

ログファイルには次のように出力されます。

```
KDSF0350-I Connect to internet gateway. URL=インターネットゲートウェイのURL
KDSF0351-I Connect result=接続結果
KDSF0352-I HTTP response code=HTTPレスポンスコード
```

*接続結果*に「SUCCESS」、*HTTPレスポンスコード*に「200」がそれぞれ出力されている場合は、エージェントからインターネットゲートウェイの接続に成功しています。これ以外の内容が出力されている場

合は、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の「インターネットゲートウェイのトラブルシューティング」を参照し、エラー要因と対処方法を確認してください。

2.11.4　操作画面に HTTPS で接続する手順

管理用サーバの操作画面に HTTPS で接続するには、Microsoft Internet Information Services の設定が必要です。Microsoft Internet Information Services の詳細な設定方法については、Microsoft Internet Information Services のマニュアルを参照してください。

> **ヒント**
>
> 管理用サーバの操作画面に接続するための Microsoft Internet Information Services としてインターネットゲートウェイサーバに構築したものを使用する場合、以降の手順はインターネットゲートウェイサーバの Microsoft Internet Information Services に対して実施してください。

Microsoft Internet Information Services の追加モジュールのインストール：

次の表に示す Microsoft Internet Information Services の追加モジュールを入手し、インストールします。

モジュール名	入手元
アプリケーション要求ルーティング Microsoft Application Request Routing 3.0 (x64)	https://www.microsoft.com/en-us/download/details.aspx?id=47333
URL 書き換えモジュール	https://iis-umbraco.azurewebsites.net/downloads/microsoft/url-rewrite

サーバ証明書の設定：

「サーバー証明書」で、サーバ証明書の要求を完了します。

証明書の要求の完了する証明機関によって証明されたサーバー証明書

　証明機関によって証明されたサーバー証明書のファイルパス※

　注※　サーバ証明書ファイルは JP1/IT Desktop Management 2 - Manager のインストール先フォルダに格納しないでください。

フレンドリ名

　任意

> **ヒント**
>
> 管理用サーバの操作画面に接続するための Microsoft Internet Information Services としてインターネットゲートウェイサーバに構築したものを使用する場合、サーバ証明書はインターネットゲートウェイサーバで設定した「サーバー証明書」を使用します。

リバースプロキシの有効化：

Microsoft Internet Information Services の次の項目を設定します。

Microsoft Internet Information Services の項目	設定項目	設定内容
Application Request Routing Cache [Server Proxy Settings]- [Application Request Routing]	Enable proxy	チェックする

アプリケーションの追加と設定：

Microsoft Internet Information Services に次の構成を追加します。

Microsoft Internet Information Services の項目	設定項目	設定内容
サイト	名前	Default Web Site
	サイトバインド	種類：https IP アドレス：未使用の IP すべて ポート番号：任意(例：443) ホスト名：サーバの FQDN サーバ名表示を要求する：チェックする SSL 証明書：「サーバ証明書の設定：」で設定したフレンドリ名
	有効なプロトコル	https
	認証	基本認証：有効 匿名認証：有効
アプリケーション	エイリアス	jp1itdm
	アプリケーションプール	AppPooljp1itdm
	物理パス	任意のフォルダ ただし、認証に使用するユーザー（匿名認証の場合は（IUSR））に「変更」権限を付与してください。
	有効なプロトコル	https
アプリケーションプール	「全般」の「名前」	AppPooljp1itdm

URL 書き換えの設定：

Microsoft Internet Information Services の次の項目を設定します。

Microsoft Internet Information Services の項目	項目	設定項目	設定内容
URL 書き換え 　リバースプロキシ規則	受信規則	HTTP 要求が転送されるサーバー名または IP アドレスを入力してください	管理用サーバのホスト名または IP アドレス
	送信規則	宛先	「アプリケーションの追加と設定：」の表の設定項目「サイトバインド」で指定したホスト名
URL 書き換え 　空の規則※	受信規則	次項「受信規則の編集：」を参照してください。	

注※　管理用サーバの操作画面に接続するための Microsoft Internet Information Services としてインターネットゲートウェイサーバに構築したものを使用する場合だけ設定してください。

受信規則の編集：

「URL 書き換えの設定：」で「URL 書き換え－リバースプロキシ規則」として追加した「受信規則」を次の内容で設定します。

項目	設定項目	設定内容
URL の一致	要求された URL	パターンに一致する
	使用	正規表現
	パターン	(.*)
	大文字と小文字を区別しない	チェックする
アクション	アクションの種類	書き換え
	URL の書き換え	http://*管理用サーバのホスト名または IPアドレス*:*管理者のコンピュータからの接続受付ポート番号(例：31080)*/{R:1}
	クエリ文字列の追加	チェックする
－	後続の規則の処理を停止する	チェックする

管理用サーバの操作画面に接続するための Microsoft Internet Information Services としてインターネットゲートウェイサーバに構築したものを使用する場合は、「URL 書き換えの設定：」で「URL 書き換え－空の規則」として追加した「受信規則」を次の内容で設定します。

項目	設定項目	設定内容
名前	名前	受信規則を識別するための任意の名前
URL の一致	要求された URL	パターンに一致する

項目	設定項目	設定内容
URL の一致	使用	正規表現
	パターン	^(jp1itdmigw)
	大文字と小文字を区別しない	チェックする
アクション	アクションの種類	なし
−	後続の規則の処理を停止する	チェックする

次に、受信規則の優先順を次の内容で設定します。

Microsoft Internet Information Services の項目	順序	設定内容	アクションの種類
URL 書き換え：要求された URL アドレスに適用される受信規則	1	「URL 書き換えの設定：」で「URL 書き換え－空の規則」として追加した「受信規則」	なし
	2	「URL 書き換えの設定：」で「URL 書き換え－リバースプロキシ規則」として追加した「受信規則」	書き換え

ヒント

管理用サーバと直接接続できる PC があるイントラネットで、http 接続での管理画面へのアクセスを遮断したい場合は、「管理者のコンピュータからの接続受付ポート番号（デフォルト：31080)」に他の機器からアクセスできないように、ファイアウォールを設定してください。

2.12　IDaaS 連携を使用した構成システムの構築

2.12.1　IDaaS 連携を使用した構成システムを構築する手順（Keycloak を使用する場合）

ID プロバイダー（IdP）として Kerycloak を使用して、IDaaS 連携を使用した構成システムを構築する手順について説明します。

以下に示す Keycloak の設定を実施した後に、IdP を使用する認証に変更してください。IdP を使用する認証への変更手順の詳細は、「2.12.4　認証方法を変更する手順」を参照してください。

ルート証明書の登録

使用する Keycloak サーバ用のルート CA 証明書を JP1/IT Desktop Management 2 - Manager がインストールされた PC の Java キーストアに登録する必要があります。

Java キーストアにこのルート CA 証明書を登録する場合は、ルート CA 証明書ファイルをダウンロードして、次のコマンドをコマンドプロンプトで実行してください。

JP1/IT Desktop Management 2 - Manager のインストールフォルダ¥mgr¥uCPSB¥jdk¥jre¥bin¥keytool.exe -import -file *証明書ファイル名* -alias *エイリアス名（識別用の任意の名前）* -keystore *JP1/IT Desktop Management 2 - Manager のインストールフォルダ*¥mgr¥uCPSB¥jdk¥jre¥lib¥security¥cacerts

コマンドを実行するとルート証明書をインポートするためのパスワードを要求されます。パスワードを入力してください。デフォルトのパスワードは「changeit」です。

Java キーストアに登録後、JP1/IT Desktop Management 2 のサービスを再起動してください。

レルムの追加および設定

Keycloak のレルムの設定を変更します。設定項目および設定値を次の表に示します。

機能		設定項目	設定値	デフォルト
一般	レルム名	－	任意のレルム名	なし
セッション	SSO Session Settings	SSO セッション・アイドル	連続し管理画面を操作する時間※1	30 分
		SSO セッション最大	任意※2	10 時間

（凡例）－：該当なし

注※1　操作画面のセッションタイムアウト時間は最終操作から 65 分です。ログインから SSO セッション・アイドルに設定された値を経過すると、IdP のセッションが切れるため、短い時間を設定した場合、シームレスログイン時に IdP の再認証が必要となる場合があります。

注※2　SSO セッション・アイドルより長い時間を指定してください。

クライアントの追加および設定

Keycloak のレルムに JP1/IT Desktop Management 2 用のクライアントを追加します。設定項目および設定値を次の表に示します。

設定項目			設定値	デフォルト
設定	General settings	クライアントタイプ	OpenID Connect※1	OpenID Connect
		クライアント ID	任意の ID※2	なし
	Access settings※3	有効なリダイレクト URI※4	http://*管理用サーバのホスト名*:*ポート番号*※5/jp1itdm/idaas.jsp	/*
	Capability config	クライアント認証	オン	オフ
	認可		オン	オフ
	Authentication flow		スタンダードフロー： 　チェックする ダイレクトアクセスグラント： 　チェックする	スタンダードフロー： 　チェックする ダイレクトアクセスグラント： 　チェックする
クレデンシャル	クライアント認証		Client Id and Secret	Client Id and Secret
	クライアント・シークレット		自動生成された値※6	クライアントシークレット値

注※1　クライアントを追加する時だけ設定できます。

注※2　IDaaS 連携用設定ファイル（jdn_idaas_auth.conf）のクライアント ID「param.auth_code.client_id」および「param.ropc.client_id」に指定します。

注※3　クライアントを追加する時は「Login settings」ステップの名称です。

注※4　複数の JP1/IT Desktop Management 2 - Manager の URI を追加する場合は、クライアントの設定で追加の URI を設定してください。

注※5　デフォルトのポート番号は 31080 です。JP1/IT Desktop Management 2 - Manager のセットアップ画面で「管理者のコンピュータからの接続受付ポート」に設定したポート番号を URL に指定してください。

注※6　IDaaS 連携用設定ファイル（jdn_idaas_auth.conf）のクライアントシークレット「param.auth_code.client_secret」および「param.ropc.client_secret」に、本項目値を難読化して指定します。

注意事項

ログイン時の認証方法は認証フローで指定してください。クライアントにデフォルトで設定されているフローを次の表に示します。

フロー		デフォルトのフロー	備考
認証フロー	ブラウザーフロー	Built-in の「browser」フロー	操作画面のログインで使用するフロー
	ダイレクトグラントフロー	Built-in の「direct grant」フロー	リモートインストールマネージャ、パッケージャ、およびネットワーク制御コマンドで使用するフロー

認証フローは運用に応じてカスタマイズできます。ただし、リモートインストールマネージャ、パッケージャ、およびネットワーク制御コマンドを使用する場合、ダイレクトグラントフローのカスタマイズはせずにデフォルトのフローを設定してください。

2.12.2 IDaaS 連携を使用した構成システムを構築する手順（Microsoft Entra ID を使用する場合）

ID プロバイダー（IdP）として Microsoft Entra ID を使用して、IDaaS 連携を使用した構成システムを構築する手順について説明します。

以下に示す Microsoft Entra ID の設定を実施した後に、IdP を使用する認証に変更してください。IdP を使用する認証への変更手順の詳細は、「2.12.4　認証方法を変更する手順」を参照してください。

操作画面の HTTPS 接続対応

Microsoft Entra ID を使用する場合、管理用サーバの操作画面を HTTPS 接続で使用するように設定を変更する必要があります。

操作画面を HTTPS 接続で使用するための設定の詳細は、「2.11.4　操作画面に HTTPS で接続する手順」を参照してください。

操作画面のログイン URL は「`https://`*リバースプロキシサーバのホスト名*`:`*ポート番号*`/jp1itdm/jp1itdm.jsp`」を使用します。

> **重要**
>
> リモートインストールマネージャ、パッケージャ、およびネットワーク制御コマンドからは JP1/IT Desktop Management 2 - Manager と HTTP 通信を使用します。このため、管理用サーバの HTTP 通信用のポート番号（31080）はファイアウォールで接続を許可するようにしてください。

ルート証明書の登録

Microsoft Entra ID を使用する場合、次のルート CA 証明書を JP1/IT Desktop Management 2 - Manager がインストールされた PC の Java キーストアに登録する必要があります。Java キーストアに登録後、JP1/IT Desktop Management 2 のサービスを再起動してください。

- Micorosoft 社の Azure 証明機関の詳細サイト※に記載されているルート証明機関および下位証明機関すべての証明書

Java キーストアに上記の証明書が登録されていない場合は、Azure 証明機関の詳細サイト※から証明書ファイルをダウンロードして、すべての証明書について次のコマンドをコマンドプロンプトで実行してください。

JP1/IT Desktop Management 2 - Managerのインストールフォルダ¥mgr¥uCPSB¥jdk¥jre¥bin¥keytool.exe -import -file *インポートする証明書ファイルのパス* -alias *重複しない任意の名称* -keystore *JP1/IT Desktop Management 2 - Managerのインストールフォルダ*¥mgr¥uCPSB¥jdk¥jre¥lib¥security¥cacerts

コマンドを実行するとルート証明書をインポートするためのパスワードを要求されます。パスワードを入力してください。デフォルトのパスワードは「changeit」です。

注※ https://learn.microsoft.com/ja-jp/azure/security/fundamentals/azure-ca-details?tabs=root-and-subordinate-cas-list

Microsoft Entra ID へのアプリの登録

Microsoft Entra ID にアプリを使用した認証の認証情報を設定します。設定項目および設定値を次の表に示します。

認可コードフロー用のクライアントとパスワード認証用の 2 件のアプリを登録してください。アプリの名前以外は同じ値を設定します。

認可コードフローは管理画面からの認証に、パスワード認証はリモートインストールマネージャ、パッケージャ、およびネットワーク制御コマンドからの認証に使用されます。

機能	設定項目		設定値	デフォルト
アプリの登録	名前		任意の値を入力	－
	サポートされているアカウントの種類		この組織ディレクトリのみ含まれるアカウント	この組織ディレクトリのみ含まれるアカウント
	プラットフォームの選択		Web	－
	リダイレクト URI		https://*リバースプロキシサーバのホスト名またはIPアドレス*:*ポート番号*/jp1itdm/idaas.jsp	－
	アプリケーション（クライアント ID）		自動生成された値※1	－
認証	暗黙的な許可およびハイブリッド フロー		ID トークン（暗黙的およびハイブリッド フローに使用）	－
証明書とシークレット	クライアントシークレット	説明	任意の値を入力	－
		有効期限	任意の値を入力	推奨：180 日（6 か月）
		値	自動生成された値※2	－

（凡例）－：該当なし

注※1　IDaaS 連携用設定ファイル（jdn_idaas_auth.conf）のクライアントシークレット「param.auth_code.client_secret」に、認可コードフロー用アプリの本項目値を指定します。「param.ropc.client_id」には、パスワード認証用アプリの本項目値を指定します。

注※2　IDaaS 連携用設定ファイル（jdn_idaas_auth.conf）のクライアントシークレット「param.auth_code.client_secret」に、認可コードフロー用アプリの本項目値を難読化して指定します。「param.ropc.client_secret」には、パスワード認証用アプリの本項目値を難読化して指定します。

ユーザーレベルでの多要素認証の無効化

次に示す手順でユーザーレベルでの多要素認証（MFA）を無効化します。

1. Microsoft ユーザーで Microsoft Entra ID にログインします。
2. 「ユーザー」－「すべてのユーザー」－「ユーザーごとの MFA」を開きます。
3. JP1/IT Desktop Management 2 と連携するユーザーを選択します。
4. 「MFA を無効にする」をクリックします。

条件付きアクセス ポリシーの作成

アプリレベルで多要素認証を制御するため、アプリに条件付きアクセスのポリシーを作成します。この操作は MS Entra ID で条件付きアクセス管理者が実施します。

> **メモ**
>
> リモートインストールマネージャ、パッケージャ、およびネットワーク制御コマンド用のアプリは、条件付きアクセスポリシーの作成は不要です。

設定項目および設定値を次の表に示します。

機能	設定項目	設定値	デフォルト
条件付きアクセス ポリシー	名前	任意の値を入力	－
	ユーザー	JP1/IT Desktop Management 2 と連携するユーザーを選択	なし
	ターゲットリソース	リソース（以前のクラウド アプリ）	リソース（以前のクラウド アプリ）
		対象	対象
		リソースの選択	なし
	フィルターの編集	なし	なし

機能	設定項目	設定値	デフォルト
条件付きアクセス ポリシー	選択	「Microsoft Entra ID へのアプリの登録」で作成した、JP1/IT Desktop Management 2 - Manager のアプリ名※1	なし
	ネットワーク	未構成	未構成
	条件	未構成	未構成
	許可	アクセス権の付与	アクセス権の付与
		任意の認証方法を設定	－
		任意の値を設定	選択したコントロールすべてが必要
	セッション	未構成※2	未構成

（凡例）－：該当なし

注※1　認可コードフロー用に登録したアプリの名前を指定します。

注※2　サインインの頻度は SSO セッションの最大時間でありセッション・アイドルではありません。

2.12.3　IDaaS 連携用設定ファイル（jdn_idaas_auth.conf）

IDaaS 連携を使用する場合、IDaaS 連携用設定ファイル（jdn_idaas_auth.conf）を作成する必要があります。

IDaaS 連携用設定ファイルの作成方法を次に示します。

IDaaS 連携用設定ファイルの格納先

JP1/IT Desktop Management 2 - Managerのインストールフォルダ¥mgr¥conf

IDaaS 連携用設定ファイルの記述形式

IDaaS 連携用設定ファイルの仕様を次の表に示します。

項目	説明
ファイル形式	• 「キー=値」の形式で指定します。 • 「#」で始まる行はコメント行です。 • 行頭または行末に半角スペースや全角スペースは指定できません。 • 値の大文字と小文字は区別されます。
文字コード	UTF-8（BOM なし）

IDaaS 連携用設定ファイルの記述形式を次の表に示します。

カテゴリー	キー	説明	必須/任意	難読化の要否※1	備考
URL 情報	authorization_endpoint	認可エンドポイント URL を指定します。	○	−	※2
	token_endpoint	トークンエンドポイント URL を指定します。	○	−	※2
認可コードフロー用リクエストパラメータ（操作画面用）	param.auth_code.client_id	IdP のクライアント ID を指定します。	○	−	
	param.auth_code.client_secret	クライアントシークレットを指定します。	○	○	※3
	param.auth_code.redirect_uri	リダイレクト URI として、IDaaS 連携用のログイン画面 URL を指定します。 JP1/IT Desktop Management 2 の操作画面ログイン URL の「jp1itdm.jsp」を「idaas.jsp」に変更した値を指定します。	○	−	※4
	param.auth_code.response_type	レスポンスタイプを指定します。	−	−	※5
	param.auth_code.scope	スコープを指定します。複数指定する場合はスペース区切りで指定します。	−	−	※6
リソース・オーナー・パスワード・クレデンシャルズフロー用リクエストパラメータ（リモートインストールマネージャ、パッケージャ、およびネットワーク制御コマンド用）	param.ropc.client_id	クライアント ID を指定します。 • IdP の設定で、認可コードフロー用のクライアントとパスワード認証用のクライアントを分ける場合は、パスワード認証用のクライアントの情報を指定します。 • 認可コードフロー用のクライアントと同じクライアントを使用する場合は、認可コードフロー用リクエストパラメータと同じ値を指定します。	○	−	
	param.ropc.client_secret	クライアントシークレットを指定します。	○	○	※7
	param.ropc.scope	スコープを指定します。複数指定する場合はスペース区切りで指定します。	−	−	※6
プロキシ情報	use_proxy	プロキシサーバを使用するかどうかを指定します。 0：プロキシサーバを使用しない	−	−	省略時は「0」を仮定します。

カテゴリー	キー	説明	必須/任意	難読化の要否※1	備考
プロキシ情報	use_proxy	1：プロキシサーバを使用する	－	－	省略時は「0」を仮定します。
	proxy_server	プロキシサーバ名を指定します。	※8	－	
	proxy_port	プロキシサーバのポート番号を指定します。	※8	－	
	proxy_user	プロキシサーバのユーザー名を指定します。	－	－	
	proxy_password	プロキシサーバのパスワードを指定します。	－	○	※9

（凡例） ○：必須または難読化必要　－：任意または難読化不要

注※1　難読化が必要なキーの値は、文字列難読化コマンドで生成したものを指定します。文字列難読化コマンドの詳細は、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の itdm2encodetext.exe（難読化コマンド）の説明を参照してください。

注※2　認可エンドポイント URL およびトークンエンドポイント URL は、Keycloak の場合は Keycloak のドキュメント、Microsoft Entra ID の場合は設定画面でそれぞれ確認できます。例を次の表に示します。

IdP	キー	設定値の例
Keycloak	authorization_endpoint	*認証サーバのURL*/realms/*レルム名*/protocol/openid-connect/auth
	token_endpoint	*認証サーバのURL*/realms/*レルム名*/protocol/openid-connect/token
Microsoft Entra ID	authorization_endpoint	*認証サーバのURL*/*テナント名*/oauth2/v2.0/authorize
	token_endpoint	*認証サーバのURL*/*テナント名*/oauth2/v2.0/token

注※3　キー「param.auth_code.client_id」に指定したクライアント ID 用のクライアントシークレットを指定してください。

注※4　指定例：http://*管理用サーバのホスト名*:31080/jp1itdm/idaas.jsp

Idp の設定画面で指定したリダイレクト URI と同じ URL を指定します。大文字と小文字が区別されます。

注※5　通常は省略してください。指定する場合は値に「code」を指定してください。

注※6　通常は省略してください。指定する場合は値に「openid△profile」（△：半角スペース）を指定してください。

注※7　キー「param.ropc.client_id」に指定したクライアント ID 用のクライアントシークレットを指定してください。

注※8　キー「use_proxy」で値に「1」を指定した場合は必須です。

注※9　キー「proxy_user」が指定されていない場合、このキーの値は使用しません。

IDaaS 連携用設定ファイルの例

IDaaS 連携用設定ファイルの例を次に示します。

```
#IDaaS連携用設定ファイル

# Keycloakの設定
authorization_endpoint=https://idpserver:8443/realms/ itdm2-realm/protocol/openid-connect/au
th
token_endpoint=https://idpserver:8443/realms/ itdm2-realm/protocol/openid-connect/token

# Microsoft Entra IDの設定
#authorization_endpoint=https://login.microsoftonline.com/itdm2-tenant/oauth2/v2.0/authorize
#token_endpoint=https://login.microsoftonline.com/itdm2-tenant/oauth2/v2.0/token

#リクエストパラメータ（認可コードフロー用）
param.auth_code.client_id= itdm2-client
param.auth_code.client_secret=TSgxJ0d3Jlc4NmBFKzNBQXUmK0p3Q0EvOFk2WDpYKDd8ejJNRmlmTFFqRmYpen
0hZ0tbLiNZWVB0TEVSPW9rWHNtTDZlMXhIMyxrY2pdTnhLZFVwbiR0fVgzM0dIXnB7XkFWYW5SUHJITTg4SGRYSj4raF
J9NkR4e3lieiw+JSc7Oz9rWF5iYV8lS2ZFdk0uKkw+XEBzYz4iJ2laN3BDWyVkOy59NzVqclpmNEdZJzhmNXF3NUVBRH
wyLzxQajlw
param.auth_code.redirect_uri= http://itdm2server:31080/jp1itdm/idaas.jsp
param.auth_code.response_type=code
param.auth_code.scope=openid profile
# リクエストパラメータ（リソース・オーナー・パスワード・クレデンシャルズフロー用）
param.ropc.client_id=itdm2-client
param.ropc.client_secret=TSgxJ0d3Jlc4NmBFKzNBQXUmK0p3Q0EvOFk2WDpYKDd8ejJNRmlmTFFqRmYpen0hZ0t
bLiNZWVB0TEVSPW9rWHNtTDZlMXhIMyxrY2pdTnhLZFVwbiR0fVgzM0dIXnB7XkFWYW5SUHJITTg4SGRYSj4raFJ9NkR
4e3lieiw+JSc7Oz9rWF5iYV8lS2ZFdk0uKkw+XEBzYz4iJ2laN3BDWyVkOy59NzVqclpmNEdZJzhmNXF3NUVBRHwyLzx
Qajlw
param.ropc.scope=openid profile
# プロキシの設定
use_proxy=1
proxy_server=proxy.proxyserver.com
proxy_port=80
proxy_user=user1
proxy_password=U1x2RTF6LHI5c2RuZ3Ajc2sjcjRvPVl4PHkiIylwNGFcc080UGhzKFBWOmF8Q3YrfjlTSU8xSDBEM
U9LSVtgbzBFc29kaS9PUHg9Ni0kIVA2JG9NfFw2QiZfbmhBdVBm
```

2.12.4　認証方法を変更する手順

IDaaS 連携を使用する場合に、認証方法を変更する手順を次に示します。

ITDM2 認証から IDaaS 連携での認証に変更する手順

1. IDaaS 連携を使用した構成システムを構築する手順に従って、使用する IdP に合わせて設定します。

   Keycloak を使用する場合は「2.12.1　IDaaS 連携を使用した構成システムを構築する手順（Keycloak を使用する場合）」を参照してください。

Microsoft Entra ID を使用する場合は「2.12.2　IDaaS 連携を使用した構成システムを構築する手順（Microsoft Entra ID を使用する場合）」を参照してください。

2. IdP に登録されているユーザーのうち、JP1/IT Desktop Management 2 の操作画面、リモートインストールマネージャ、パッケージャ、またはネットワーク制御コマンドを使用するユーザーを、JP1/IT Desktop Management 2 の設定画面の［ユーザー管理］－［ユーザーアカウントの管理］画面で追加します。

> **重要**
>
> IdP に登録されているユーザー ID と JP1/IT Desktop Management 2 のユーザーアカウント管理で登録するユーザー ID は同じにする必要があります。

> **重要**
>
> JP1/IT Desktop Management 2 のユーザーアカウント管理で登録する時に初期パスワードを指定する必要があります。IdP での認証時はこのパスワードは使用しませんが、IdP での認証から ITDM2 認証に切り替える場合はこの初期パスワードを使用してログインする必要があります。

> **メモ**
>
> JP1/IT Desktop Management 2 ですでに登録されているユーザーアカウントを使用する場合は、IdP に同じユーザー ID でユーザーを登録します。

3. 管理用サーバのサービスを停止します。

4. コンフィグレーションファイル（jdn_manager_config.conf）を編集します。

   次のキーおよび値をコンフィグレーションファイルに設定します。

   ```
   IDaaS_Auth=ON
   ```

   コンフィグレーションファイルのキー「IDaaS_Auth」についての詳細は、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」のプロパティ一覧についての説明を参照してください。

5. IDaaS 連携用設定ファイル（jdn_idaas_auth.conf）を編集します。

   使用する IdP に合わせて、設定を編集してください。詳細は、「2.12.3　IDaaS 連携用設定ファイル（jdn_idaas_auth.conf）」を参照してください。

6. 管理用サーバのサービスを開始します。

JP1/IT Desktop Management 2 の操作画面を使用する場合は、Web ブラウザーで操作画面のログイン画面の URL に接続すると、IdP の認証画面で IdP に登録したユーザーのパスワードを指定してログインできます。IdP の設定で多要素認証を有効とした場合は多要素認証の操作も必要となります。

JP1 認証から IDaaS 連携での認証に変更する手順

1. ユーザー管理の設定を変更して、JP1 認証から ITDM2 認証に切り替えます。
   ユーザー管理の設定を変更する手順は、「3.10　ユーザー管理の設定を変更する手順」を参照してください。

2. ITDM2 認証から IDaaS 連携での認証に変更します。
   手順の詳細は、「ITDM2 認証から IDaaS 連携での認証に変更する手順」を参照してください。

IDaaS 連携での認証から ITDM2 認証に変更する手順

1. 管理用サーバのサービスを停止します。

2. コンフィグレーションファイル（jdn_manager_config.conf）を編集します。
   次のキーおよび値をコンフィグレーションファイルに設定します。
   ```
   IDaaS_Auth=OFF
   ```
   コンフィグレーションファイルのキー「IDaaS_Auth」についての詳細は、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」のプロパティ一覧についての説明を参照してください。

3. 管理用サーバのサービスを開始します。

4. JP1/IT Desktop Management 2 へのユーザーアカウント追加時に設定した初期パスワードをユーザーに連絡します。

JP1/IT Desktop Management 2 の操作画面の URL に接続すると、ログイン画面で IdP のユーザー ID と手順 4 で連絡した初期パスワードを使用してログインできます。

IDaaS 連携での認証から JP1 認証に変更する手順

1. IDaaS 連携での認証から ITDM2 認証に変更します。
   手順の詳細は、「IDaaS 連携での認証から ITDM2 認証に変更する手順」を参照してください。

2. ユーザー管理の設定を変更して、ITDM2 認証から JP1 認証に切り替えます。
   ユーザー管理の設定を変更する手順は、「3.10　ユーザー管理の設定を変更する手順」を参照してください。

2.12.5　IDaaS 連携の注意事項

IDaaS 連携の注意事項を次に示します。

IdP への初回ログインおよび IdP の設定変更時の注意事項

IdP に登録した新しいユーザーの初回ログイン時や IdP の設定変更時などに初期設定用のユーザー操作※が必要な場合があります。

注※　初期設定用のユーザー操作には、多要素認証用の設定、パスワードの変更、ユーザー属性の設定などがあります。

JP1/IT Desktop Management 2 の操作画面へのログイン時に IdP の認証画面に表示される場合は、その案内に従ってください。

リモートインストールマネージャ、パッケージャ、およびネットワーク制御コマンドの認証に使用するユーザーの初期設定が完了していないと、認証に失敗する場合があります。この場合、JP1/IT Desktop Management 2 の操作画面へログインして確認してください。

Microsoft Entra ID を使用する場合の Web ブラウザーの制限

Microsoft Entra ID を使用してユーザー認証する場合、Web ブラウザーとして Internet Explorer および Microsoft Edge の IE モードは使用できません。JP1/IT Desktop Management 2 の操作画面は、Microsoft Edge のネイティブモード、Google Chrome、または Mozilla Firefox で使用してください。

3 セットアップ内容の変更

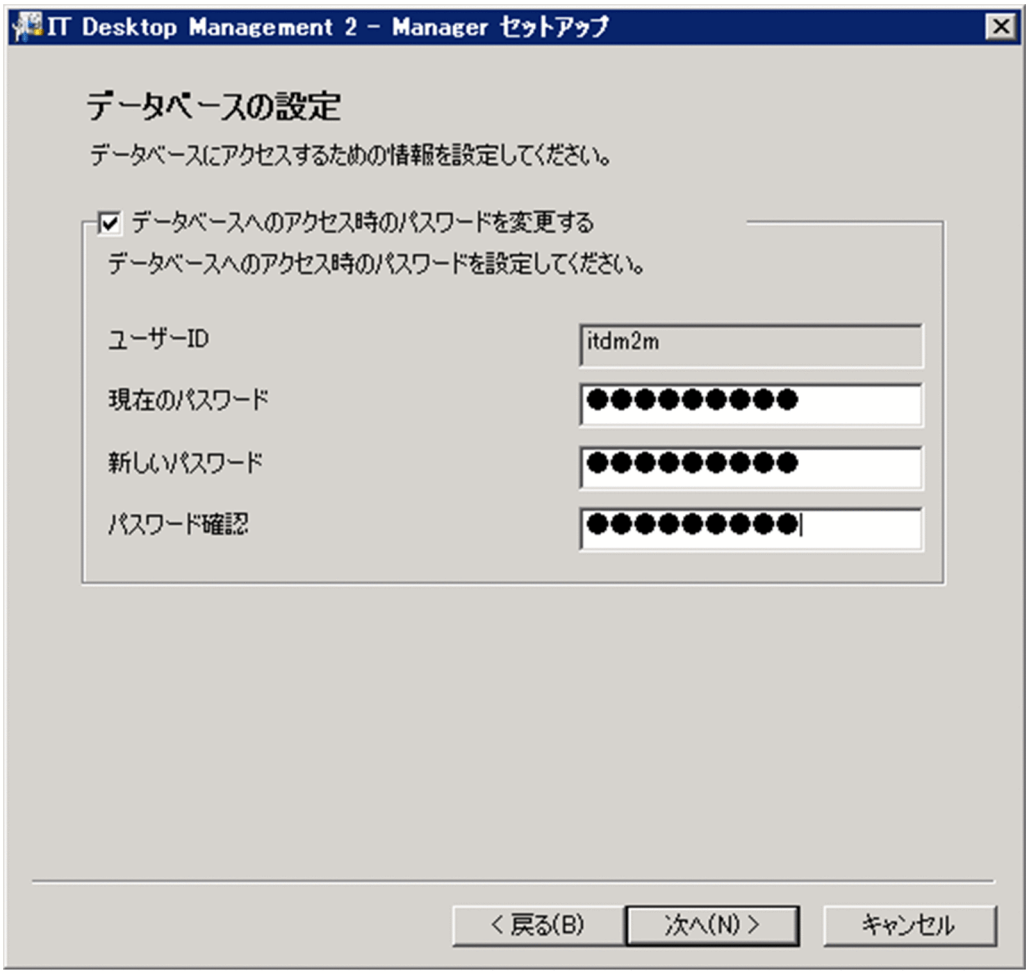
ここでは、管理用サーバでセットアップ時に設定した内容の変更について説明します。

3.1　データベースへの接続設定を変更する手順

JP1/IT Desktop Management 2 にアクセスするためのパスワードやデータベース接続アドレスを変更できます。

データベースにアクセスするためのパスワードを変更するには：

1. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
2. セットアップ画面で［次へ］ボタンをクリックします。
3. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
4. ［データベースの設定］（パスワード変更）画面で、［データベースへのアクセス時のパスワードを変更する］をチェックし、現在のパスワードと新しいパスワードを入力して［次へ］ボタンをクリックします。



5. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックします。

   リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、［OK］ ボタンをクリックしてください。クラスタ

システム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

6. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。
   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了する と、[セットアップを終了します] 画面が表示されます。

7. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

JP1/IT Desktop Management 2 のデータベースにアクセスするためのパスワードが変更されます。

データベース接続アドレスを変更するには：

1. 管理用サーバでstopservice コマンドを実行し、サービスを停止します。

2. Windows の [スタート] メニューから [すべてのプログラム] − [JP1_IT Desktop Management 2 - Manager] − [ツール] − [セットアップ] を選択します。

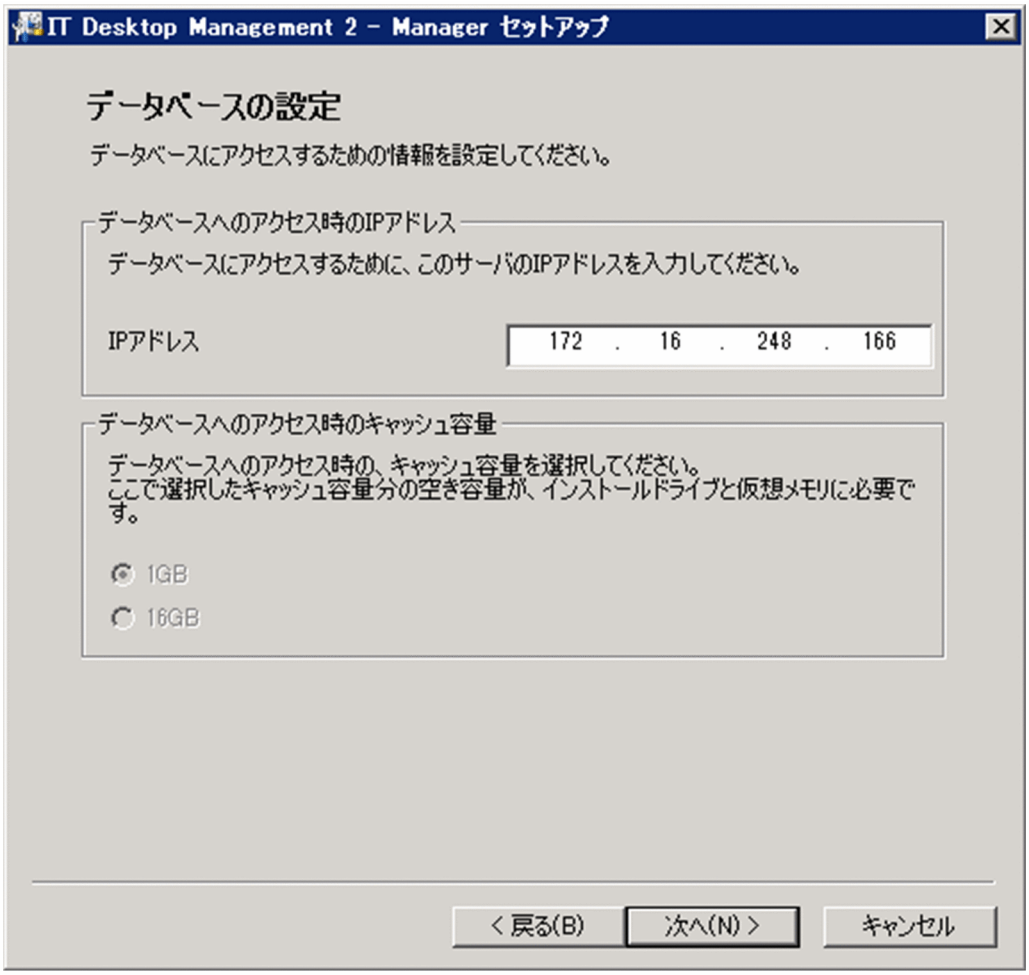
3. セットアップ画面で [次へ] ボタンをクリックします。

4. [セットアップの選択] 画面で、[設定変更] を選択して [次へ] ボタンをクリックします。

5. [データベースの設定] (パスワード変更) 画面でパスワードを変更しないで、[次へ] ボタンをクリックします。

6. [クラスタ環境] 画面で、クラスタ構成で運用しない設定にして、[次へ] ボタンをクリックします。

7. [データベースの設定] (IP アドレス、キャッシュ設定) 画面で、データベースにアクセスするための管理用サーバの IP アドレスを変更して [次へ] ボタンをクリックします。



8. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。

9. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

   リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。

10. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

    セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

11. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

    停止したサービスはセットアップ終了後、自動的に開始されます。

JP1/IT Desktop Management 2 のデータベース接続アドレスが変更されます。

データベースへのアクセス時のキャッシュ容量を変更するには：

データベースへのアクセス時のキャッシュ容量は、初期セットアップ時に設定した値をセットアップ画面から変更できません。下記の手順で変更してください。

1. データベースのバックアップを取得します。

   データベースのバックアップは、データベースマネージャを利用してください。バックアップ先フォルダのドライブは、目安として 20 ギガバイト以上の空き容量を確保してください。

2. JP1/IT Desktop Management 2 - Manager をアンインストールします。

   JP1/IT Desktop Management 2 - Manager をアンインストールする手順は、「6.2　JP1/IT Desktop Management 2 - Manager をアンインストールする手順」を参照してください。

3. JP1/IT Desktop Management 2 - Manager をインストールします。

   JP1/IT Desktop Management 2 - Manager をインストールする手順は、「1.2.2　JP1/IT Desktop Management 2 - Manager をインストールする手順（単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバの場合）」を参照してください。

4. セットアップでキャッシュ容量を設定します。

   キャッシュ容量の設定については、「1.2.4　単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順」を参照してください。

5. 手順 1.でバックアップしたデータベースをリストアします。

   リプレース先のコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［データベースマネージャ］から JP1/IT Desktop Management 2 - Manager のデータベースマネージャを起動して、データベースのリストアを実行してください。

3.2 使用するフォルダを変更する手順

管理用サーバで使用するフォルダを変更できます。データベースに使用するディスク容量が不足した場合は、十分な空き容量があるディスクにデータベースのフォルダを変更してください。

重要

コンピュータが Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2 または Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- *システムドライブ*:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

使用するフォルダを変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［フォルダの設定］画面が表示されるまで、［次へ］ボタンをクリックします。
6. 必要に応じてフォルダを変更します。
7. ［セットアップの確認］画面が表示されるまで、［次へ］ボタンをクリックします。
8. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックします。

データベースフォルダについては、変更前のフォルダからデータベースが削除され、変更後のフォルダにデータベースが作成されます。データベース内の操作ログ以外のデータは、変更前の状態で引き継がれますが、変更前の操作ログデータは削除されます。必要に応じて操作ログの手動取り込みを実施してください。

データフォルダのデータは、変更後のフォルダに移動されます。

操作ログの保管先フォルダは、変更前のフォルダとそのフォルダに格納されているデータがそのまま残ります。変更後のフォルダには、フォルダの変更後に取得される操作ログのデータが格納されます。1 つのフォルダに操作ログのデータをまとめておきたいときは、変更前のフォルダに格納されているデータを、変更後のフォルダに移動してください。

操作ログのデータベースフォルダを変更すると、変更前のデータは削除されます。必要に応じて操作ログの手動取り込みを実施してください。

3.3 操作ログの取得を設定する手順

管理用サーバのセットアップ項目です。

利用者の操作をログとして記録できます。操作ログを取得すると、ファイルの持ち込みまたは持ち出しを追跡したり、不審操作を行ったコンピュータを特定したりできます。

なお、操作ログを取得できるのは、オンライン管理のコンピュータ（Windows エージェント）だけです。

ヒント

操作ログの取得の有無は、セットアップとセキュリティポリシーの両方で設定が必要です。操作ログを取得する場合、ここでの設定とあわせて、セキュリティポリシーで操作ログの取得を有効に設定してください。また、取得する操作ログの種類はセキュリティポリシーで設定できます。

重要

管理用サーバのセットアップで操作ログを取得しない設定にしている場合、セキュリティポリシーで操作ログの取得を有効にしても、コンピュータから取得した操作ログは保存されません。

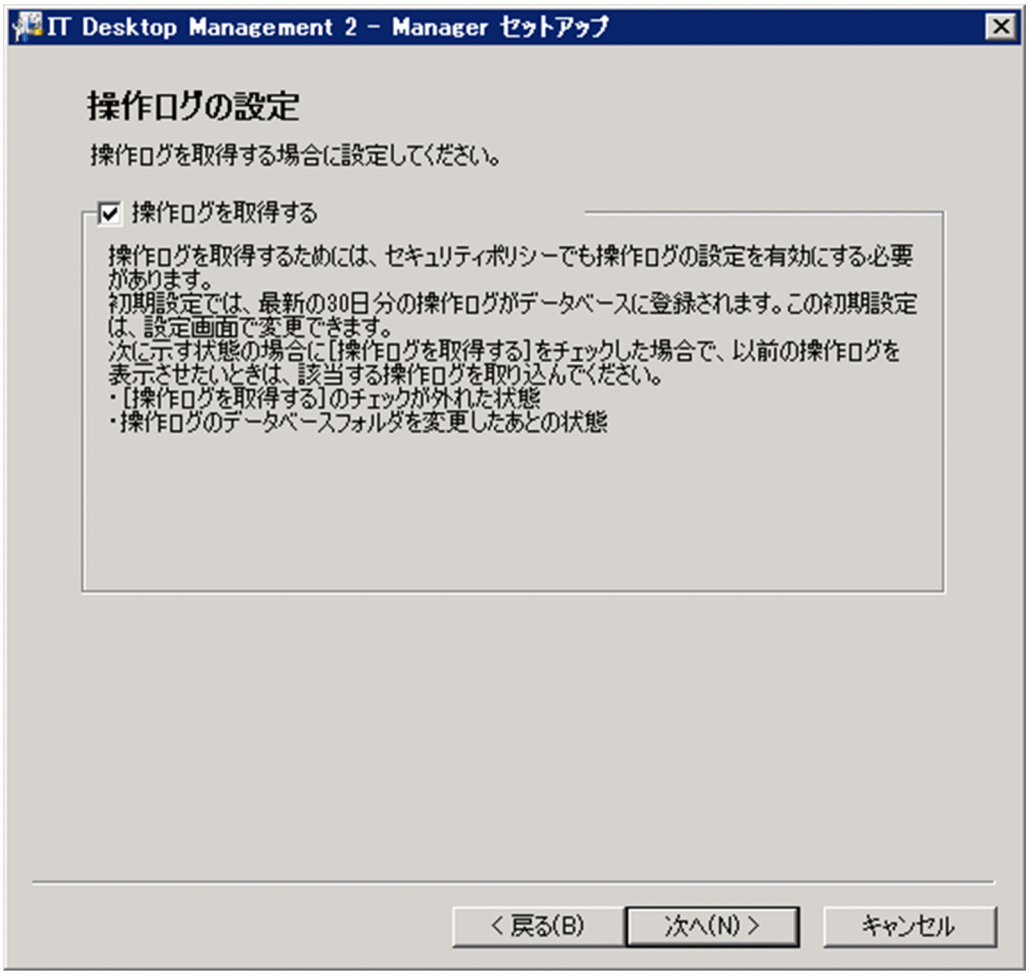
重要

コンピュータが Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2 または Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- *システムドライブ*:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

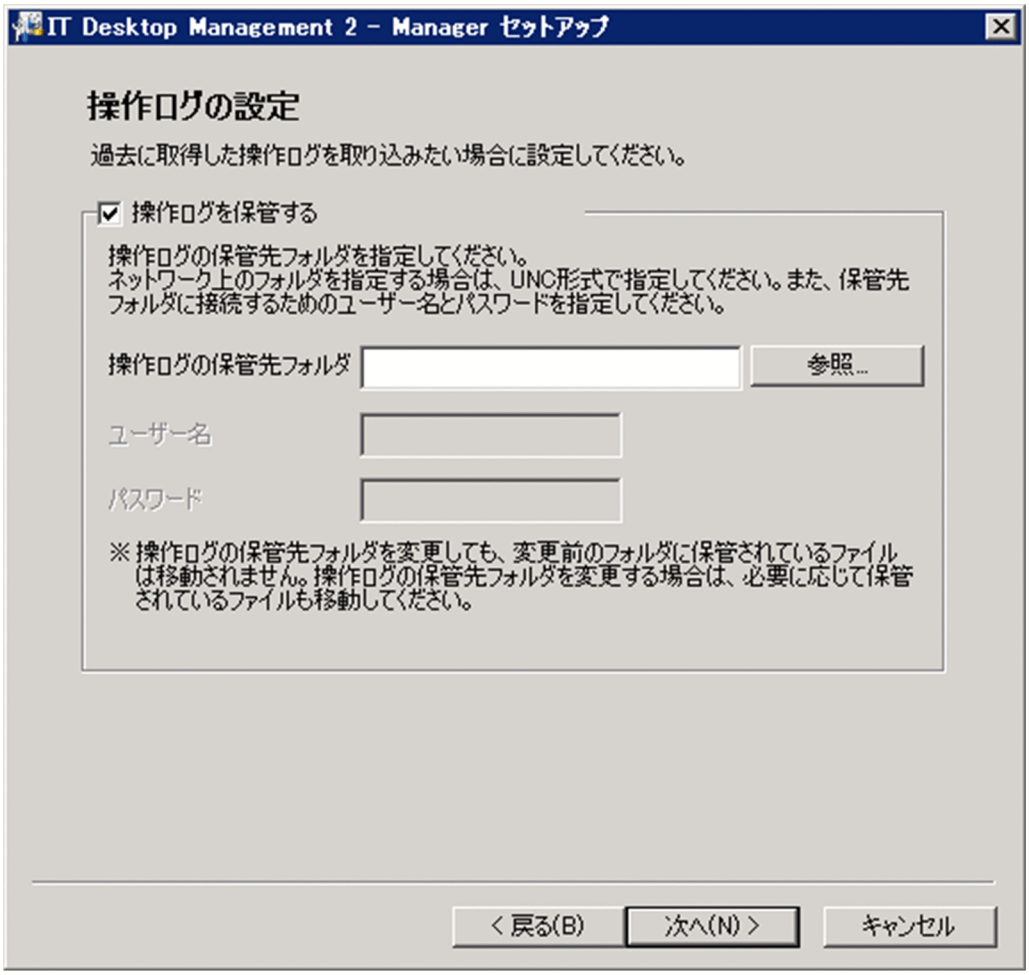
操作ログの取得を設定するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［操作ログの設定］画面が表示されるまで、［次へ］ボタンをクリックします。



6. [操作ログを取得する] をチェックして、[次へ] ボタンをクリックします。

7. 操作ログを保管する場合は、表示された画面で [操作ログを保管する] をチェックして、[操作ログの保管先フォルダ] を指定します。また、必要に応じて、保管先フォルダに接続するためのユーザー名とパスワードを指定します。



8. [次へ] ボタンをクリックします。

9. 表示された画面で、次の項目を設定します。

- [管理対象の機器の台数]

  操作ログを取得するコンピュータの大よその台数を指定します。

- [操作ログのデータベース格納最大日数]

  操作ログを操作ログのデータベースに何日分取り込むか（「自動取り込み」と「手動取り込み」の合計）を指定します。デフォルトは 60 日です。なお、操作ログの自動取り込みを設定した場合、利用者の操作ログはデフォルトでは最新 30 日分が、[操作ログのデータベースフォルダ] で指定したフォルダに自動的に保存されます。自動取り込みされる操作ログの格納期間は、[操作ログの設定] で変更できます。

- [必要なディスク容量]

  [管理対象の機器の台数] および [操作ログのデータベース格納最大日数] の指定に基づいて、自動で算出されます。

  計算式は次のとおりです。

  [管理対象の機器の台数] × [操作ログのデータベース格納最大日数] ×1.52（メガバイト）

  計算結果が「[操作ログのデータベース格納最大日数] ×1.5（ギガバイト）」に満たない場合には、次の計算式になります。

［操作ログのデータベース格納最大日数］×1.5（ギガバイト）

［必要なディスク容量］の値は、操作ログのデータベースフォルダの空き容量の警戒しきい値および緊急しきい値のデフォルト値に使用されます。

警戒しきい値および緊急しきい値は、コンフィグレーションファイル（jdn_manager_config.conf）で変更できます。

- ［操作ログのデータベースフォルダ］

  操作ログを保存するためのデータベースを作成するフォルダを指定します。

> **ヒント**
>
> ［操作ログのデータベース格納最大日数］および［必要なディスク容量］は目安です。取り込める操作ログの期間や使用するディスク容量は、実際に管理している機器の台数や操作ログの情報量によって異なります。

10. ［次へ］ボタンをクリックします。

11. 操作ログの検索性能を向上させるために、データベースのキャッシュを追加する場合は、表示された画面で、追加するキャッシュ容量を指定します。

    管理対象のコンピュータ 2,500 台あたり、1 ギガバイトを設定してください。

12. ［次へ］ボタンをクリックします。

13. ［セットアップの確認］画面が表示されるまで、［次へ］ボタンをクリックします。

14. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックします。

    リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、［OK］ボタンをクリックしてください。クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、［OK］ボタンをクリックしてください。

15. ［リモートインストールマネージャを使用した配布のセットアップ］画面で、［OK］ボタンをクリックします。

    セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、［セットアップを終了します］画面が表示されます。

16. ［セットアップを終了します］画面で、［OK］ボタンをクリックします。

操作ログを取得できるようになります。

> **重要**
>
> 操作ログの取得に関する設定を変更する場合、すでに操作ログを取得しているときは、［管理対象の機器の台数］および［操作ログのデータベース格納最大日数］を現在の設定値より小さくすることはできません。

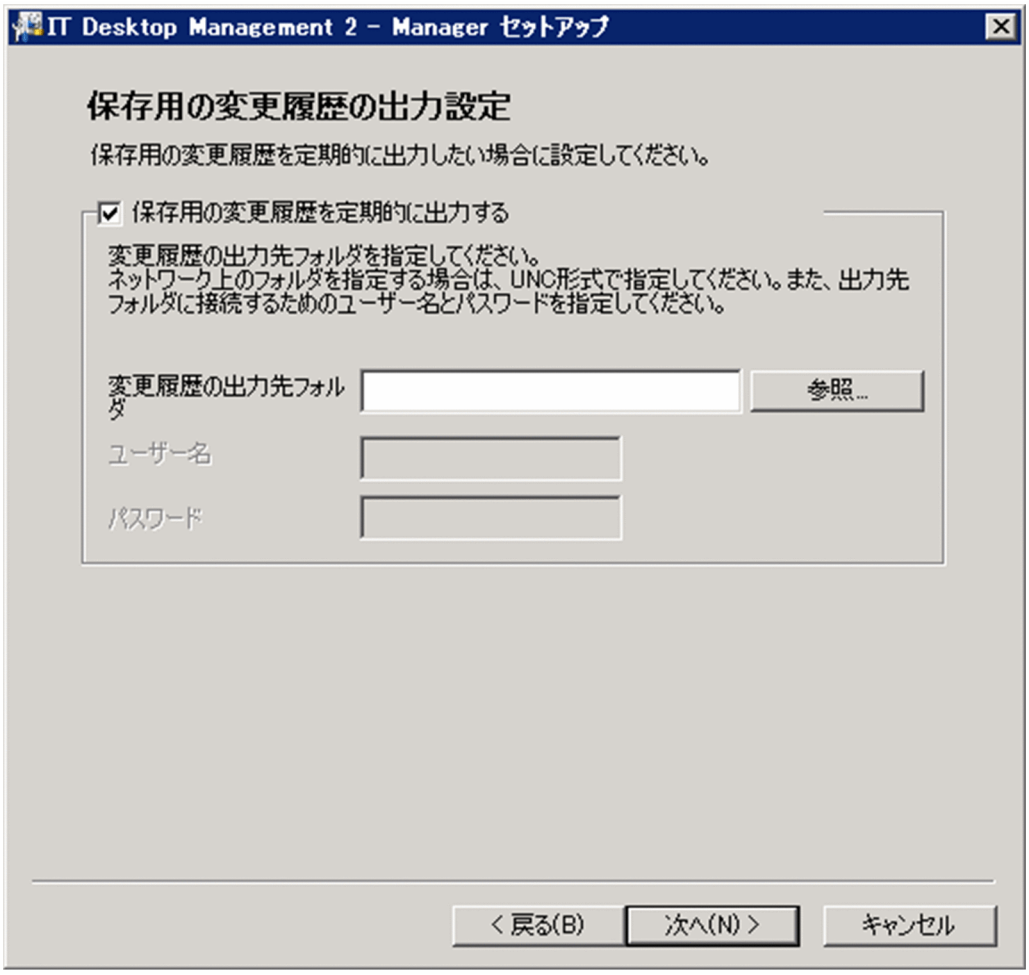
3.4　保存用の変更履歴の出力を設定する手順

管理用サーバのセットアップ項目です。

保存用の変更履歴の出力を設定すると、CSV ファイルに保存用の変更履歴が定期的に出力されます。保存用の変更履歴を出力しておけば、変更履歴が 600,000 件を超える場合も変更の内容を保持できます。

保存用の変更履歴の出力を設定するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［保存用の変更履歴の出力設定］画面が表示されるまで、［次へ］ボタンをクリックします。



6. ［保存用の変更履歴を定期的に出力する］をチェックして［変更履歴の出力先フォルダ］を指定します。

重要

コンピュータが Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2 または Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- *システムドライブ*:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

7. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。

8. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

   リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

9. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了する と、[セットアップを終了します] 画面が表示されます。

10. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

保存用の変更履歴が定期的に出力されるようになります。保存用の変更履歴では、次の項目が CSV ファイルに出力されます。

変更履歴の項目	説明
変更された日時	機器情報に変更が発生した日時（機器情報の更新日時と同じ日時）が出力されます。 なお、外部記憶媒体を使用して機器情報を管理用サーバに通知した場合は、情報収集用ツール、またはオフライン用ポリシー適用ツールで機器情報を収集した日時を出力します。
変更された項目	変更された機器情報の項目が出力されます。
変更前	変更前の機器情報が出力されます。
変更後	変更後の機器情報が出力されます。
変更発生時のホスト名	機器情報が変更された時点の、機器のホスト名を出力します。変更された項目がホスト名の場合は、変更後のホスト名を出力します。変更が発生した機器を特定するための情報です。

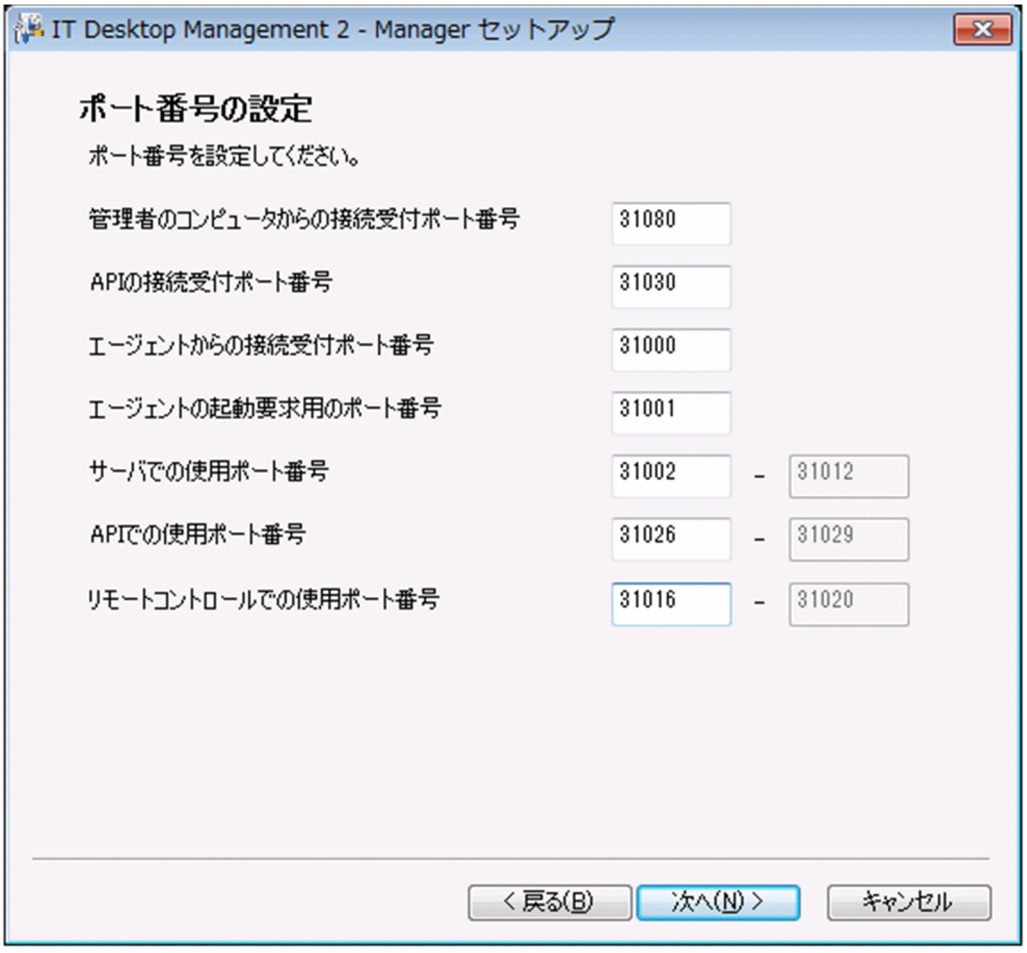
3.5　ポート番号を変更する手順

管理用サーバで使用するポート番号を変更できます。

> **重要**
>
> 運用中にポート番号を変更すると、エージェントからの接続ができなくなります。ポート番号を変更する場合は、エージェントでもポート番号の設定を変更してください。

ポート番号を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［ポート番号の設定］画面が表示されるまで、［次へ］ボタンをクリックします。



6. 必要に応じてポート番号を変更します。

変更できる内容を次に示します。

[管理者のコンピュータからの接続受付ポート番号]

JP1/IT Desktop Management 2 を操作するコンピュータから管理用サーバの接続に使用するポート番号を入力します。

[API の接続受付ポート番号]

API を使用した外部システムから管理用サーバの接続に使用するポート番号を入力します。

[エージェントからの接続受付ポート番号]

エージェントから管理用サーバの接続に使用するポート番号を入力します。

[エージェントの起動要求用のポート番号]

管理用サーバからエージェントへの通信に使用するポート番号を入力します。

[サーバでの使用ポート番号]

JP1/IT Desktop Management 2 が使用するポート番号を入力します。

[API での使用ポート番号]

API の使用時に管理用サーバが使用するポート番号を入力します。

[リモートコントロールでの使用ポート番号]

リモートコントロール機能で使用するポート番号を入力します。

[複数サーバ構成の接続ポート番号]

複数サーバ構成の場合に、管理用中継サーバで使用するポート番号を入力します。

ポート番号の詳細については、「付録 A.1　ポート番号一覧」を参照してください。

7. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。

8. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

9. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

10. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

ポート番号が変更されます。

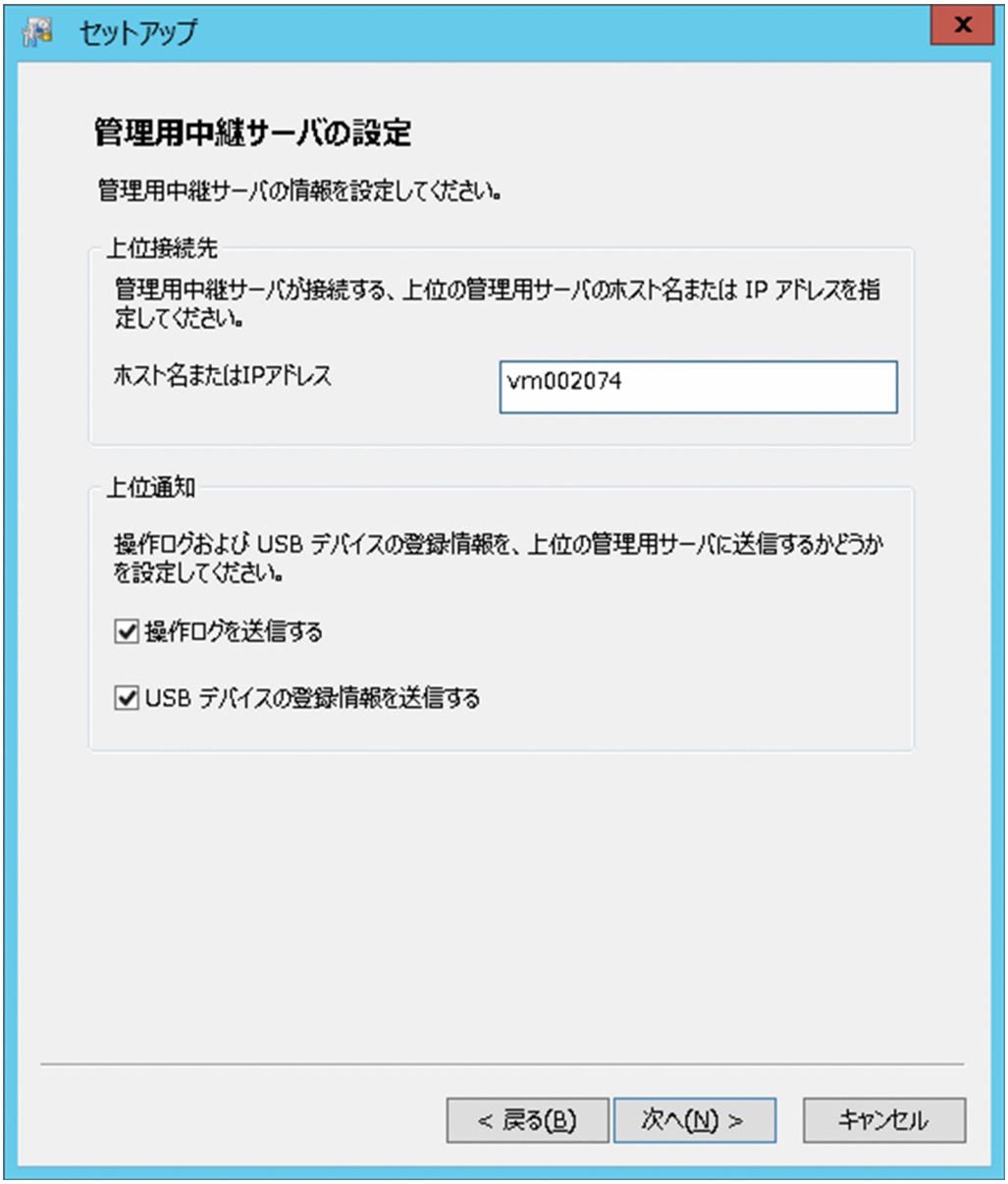
3.6　管理用中継サーバの上位接続先の設定を変更する手順

管理用中継サーバのセットアップ項目です。

管理用中継サーバの上位接続先の設定を変更できます。

上位接続先の設定を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［管理用中継サーバの設定］画面が表示されるまで、［次へ］ボタンをクリックします。



6. [ホスト名または IP アドレス] に接続先のホスト名または IP アドレスを指定し、[次へ] ボタンをクリックします。

   接続先は、上位の管理用サーバの［アドレス解決の設定］画面で選択した運用キーで指定してください。

7. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。

8. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

   リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

9. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

10. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

管理用中継サーバの上位接続先の設定が変更されます。

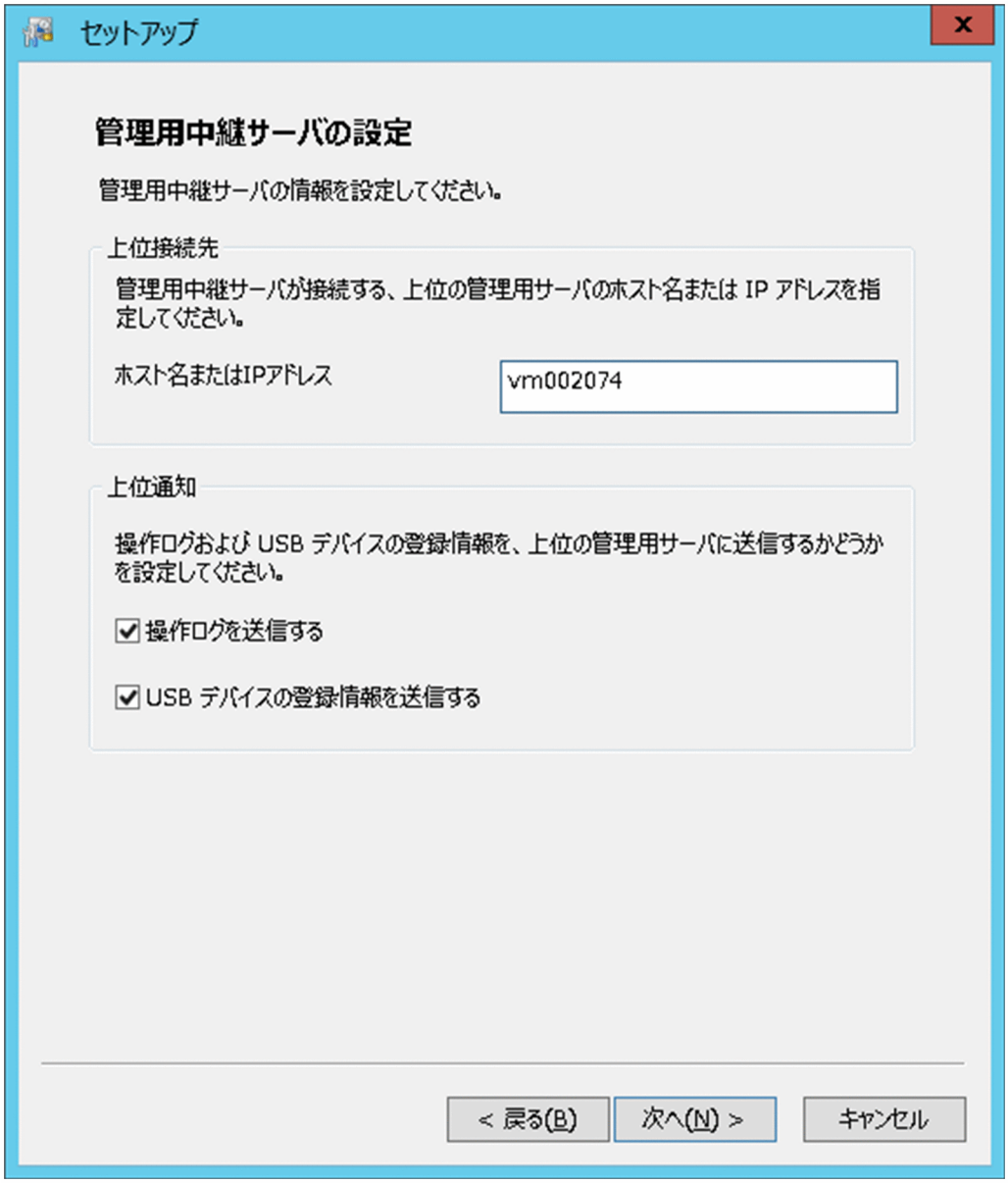
3.7　管理用中継サーバの上位通知の設定を変更する手順

管理用中継サーバのセットアップ項目です。

上位通知の設定をすると、収集した操作ログ情報と USB デバイスの登録情報を、上位の管理用サーバに送信できます。上位の管理用サーバは、直下の機器の情報、および配下の管理用中継サーバから送信された情報をまとめて管理できます。

上位通知の設定を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［管理用中継サーバの設定］画面が表示されるまで、［次へ］ボタンをクリックします。



6. 必要に応じて次の項目を変更し、[次へ] ボタンをクリックします。

- 操作ログを送信する
  収集した操作ログを上位の管理用サーバに送信する場合に選択します。
- USB デバイスの登録情報を送信する
  収集した USB デバイスの登録情報を、上位の管理用サーバに送信する場合に選択します。

> **ヒント**
>
> 操作ログを取得するには、管理元の管理用中継サーバで、セキュリティポリシーの操作ログの取得を有効にしてください。

7. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。

8. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console が使用中でないことの確認を促すダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。

クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

9. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

10. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

管理用中継サーバの上位通知の設定が変更されます。

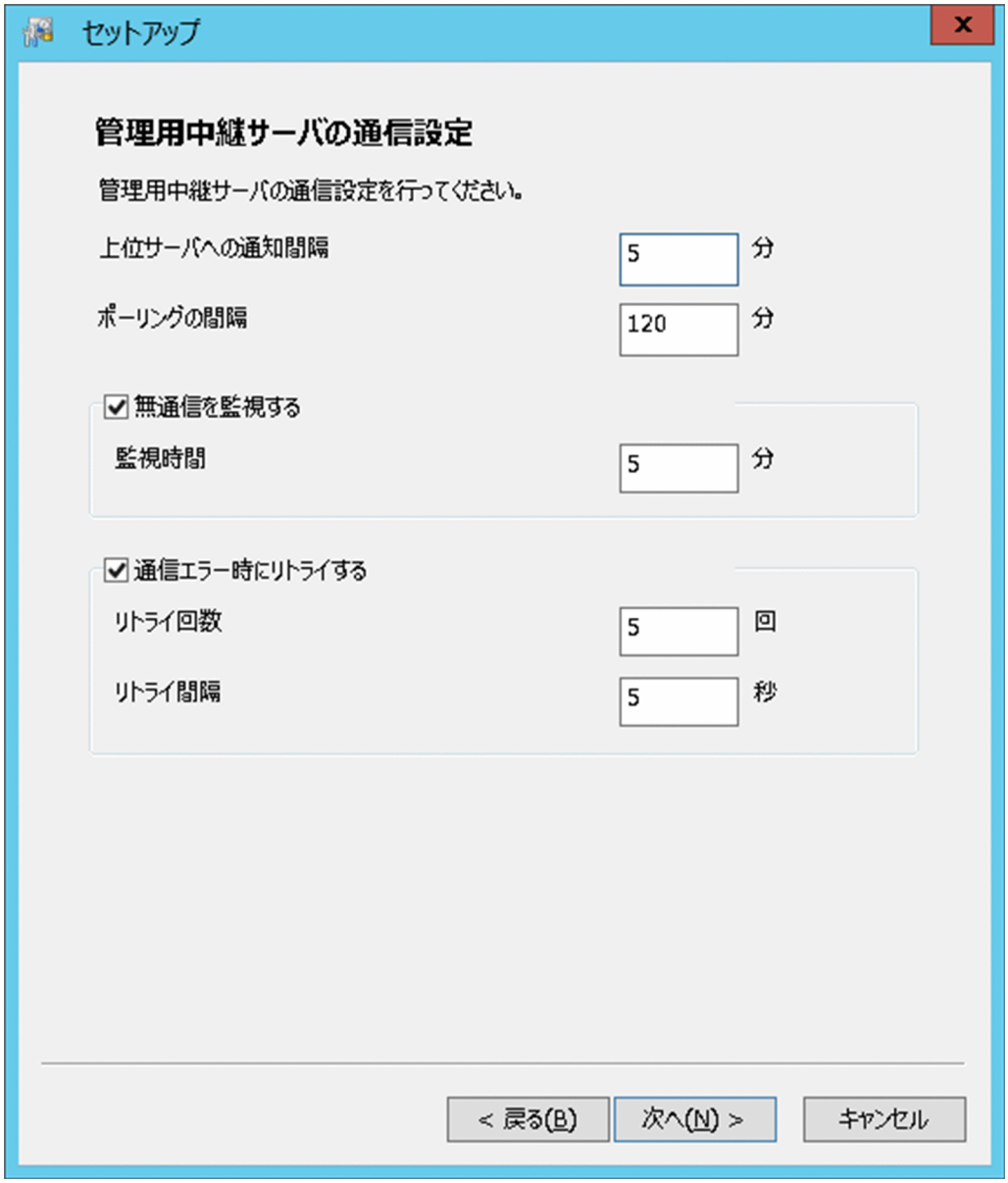
3.8　管理用中継サーバの通信設定を変更する手順

管理用中継サーバのセットアップ項目です。

管理用中継サーバの通信設定を変更できます。

通信設定を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［管理用中継サーバの通信設定］画面が表示されるまで、［次へ］ボタンをクリックします。



6. 必要に応じて次の項目を変更し、[次へ] ボタンをクリックします。

- 上位サーバへの通知間隔

  上位の管理用サーバに機器情報および機器に関連するデータを通知する間隔を指定します。

- ポーリングの間隔

  管理用中継サーバと上位の管理用サーバ間のポーリングの間隔を指定します。

- 無通信を監視する

  上位の管理用サーバから応答のない時間が、設定した時間を超えた場合に通信エラーとするときに選択します。[監視時間] に無通信と判定する時間を指定します。

- 通信エラー時にリトライする

  通信エラーが発生した場合、通信をリトライするときに選択します。[リトライ回数] と [リトライ間隔] を指定します。

7. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。

8. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

   リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console が使用中でないことの確認を促すダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。

   クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

9. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

10. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

管理用中継サーバの通信の設定が変更されます。

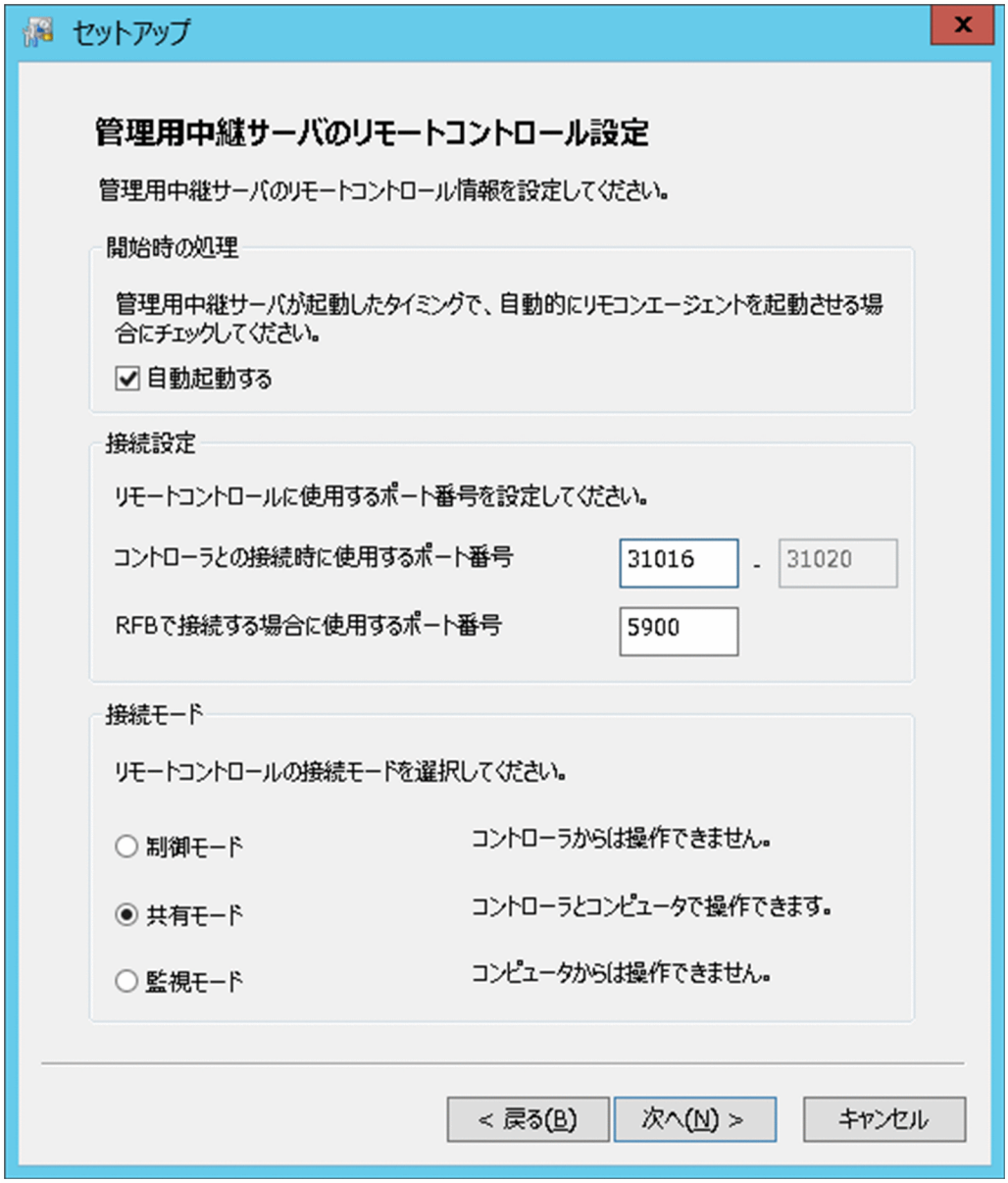
3.9　管理用中継サーバのリモートコントロール設定を変更する手順

管理用中継サーバのセットアップ項目です。

管理用中継サーバのリモートコントロールの設定を変更できます。

リモートコントロールの設定を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［管理用中継サーバのリモートコントロール設定］画面が表示されるまで、［次へ］ボタンをクリックします。



6. 必要に応じて次の項目を変更し、[次へ] ボタンをクリックします。

- 開始時の処理

  管理用中継サーバ用のエージェントを起動した時に、自動的にリモコンエージェントを起動させるかどうかを設定します。

- 接続設定

  [コントローラとの接続時に使用するポート番号] には標準接続で使用するポート番号を、[VNC サーバなど RFB プロトコルで利用するポート番号] には RFB 接続で使用するポート番号を指定します。

- 接続モード

  接続先のコンピュータが、どの接続モードを許可するかを選択します。

7. 表示された画面で、必要に応じて次の設定をし、[次へ] ボタンをクリックします。

- コントロール許可の設定

  リモートコントロール機能の使用を許可するコントローラを指定したい場合に、許可するコントローラを追加します。

- ユーザー設定

  コントローラとの接続時にユーザー認証を指定したい場合に、ユーザーの［名前］と［種別］を追加します。

8. ［セットアップの確認］画面が表示されるまで、［次へ］ボタンをクリックします。

9. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックします。

   リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、［OK］ボタンをクリックしてください。クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、［OK］ボタンをクリックしてください。

10. ［リモートインストールマネージャを使用した配布のセットアップ］画面で、［OK］ボタンをクリックします。

    セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、［セットアップを終了します］画面が表示されます。

11. ［セットアップを終了します］画面で、［OK］ボタンをクリックします。

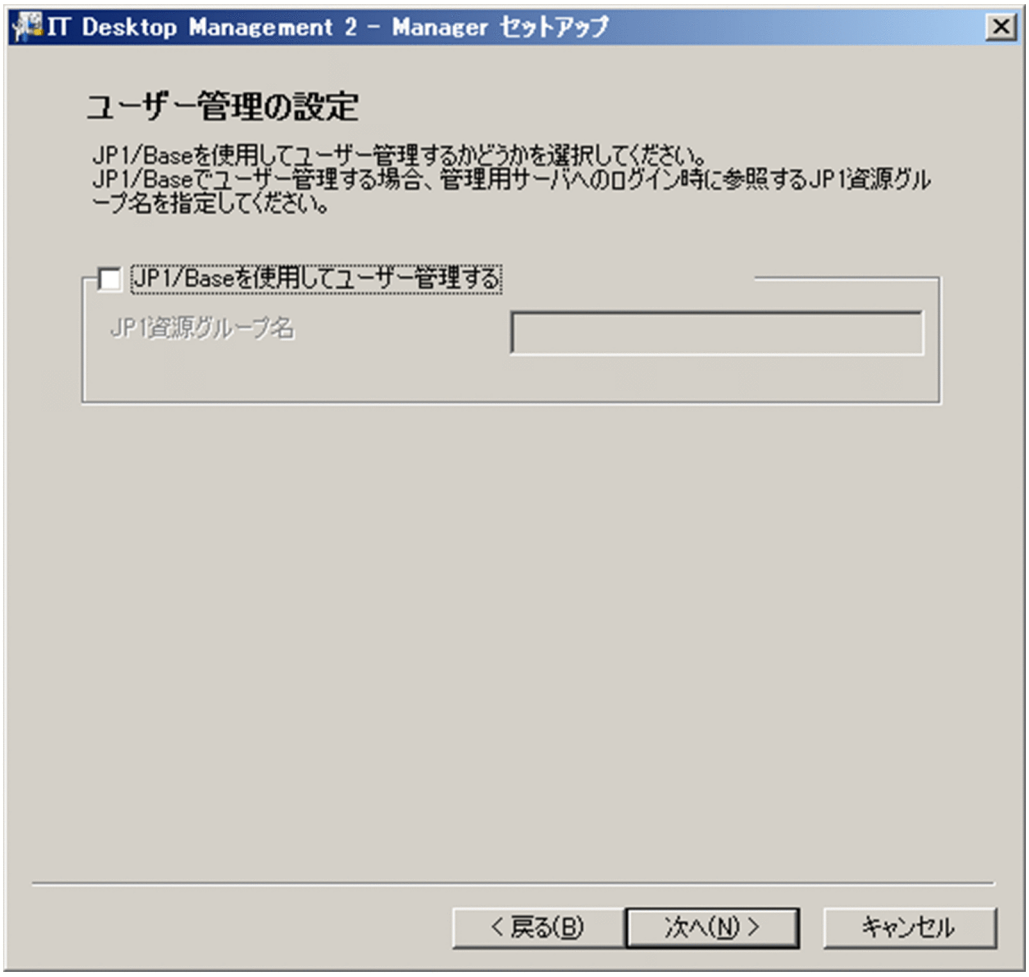
管理用中継サーバのリモートコントロールの設定が変更されます。

3.10　ユーザー管理の設定を変更する手順

JP1/Base を使用してユーザー管理するかどうかを変更できます。 設定を変更すると、ログイン時の認証方法を ITDM2 認証または JP1 認証のどちらかに切り替えられます。

ユーザー管理の設定を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［ユーザー管理の設定］画面が表示されるまで、［次へ］ボタンをクリックします。



6. 必要に応じて次の項目を変更し、［次へ］ボタンをクリックします。
   - JP1/Base を使用してユーザー管理する

ログイン時の認証方法を JP1 認証にする場合は、この項目をチェックします。 この場合、JP1/IT Desktop Management 2 の運用開始前に JP1/Base の認証サーバに JP1 ユーザーを登録する必要があります。なお、JP1/IT Desktop Management 2 ではユーザーアカウントのロックおよびパスワードの有効期限の設定ができなくなります。

ログイン時の認証方法を ITDM2 認証にする場合は、この項目のチェックを解除します。

- JP1 資源グループ名

  [JP1/Base を使用してユーザー管理する] をチェックした場合は、JP1 資源グループ名も指定します。JP1 資源グループ名は、JP1 ユーザーを登録した際に設定した JP1 資源グループ名と一致させてください。

7. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。

8. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

   リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console が使用中でないことの確認を促すダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。

   クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

9. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

10. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

ユーザー管理の設定が変更されます。

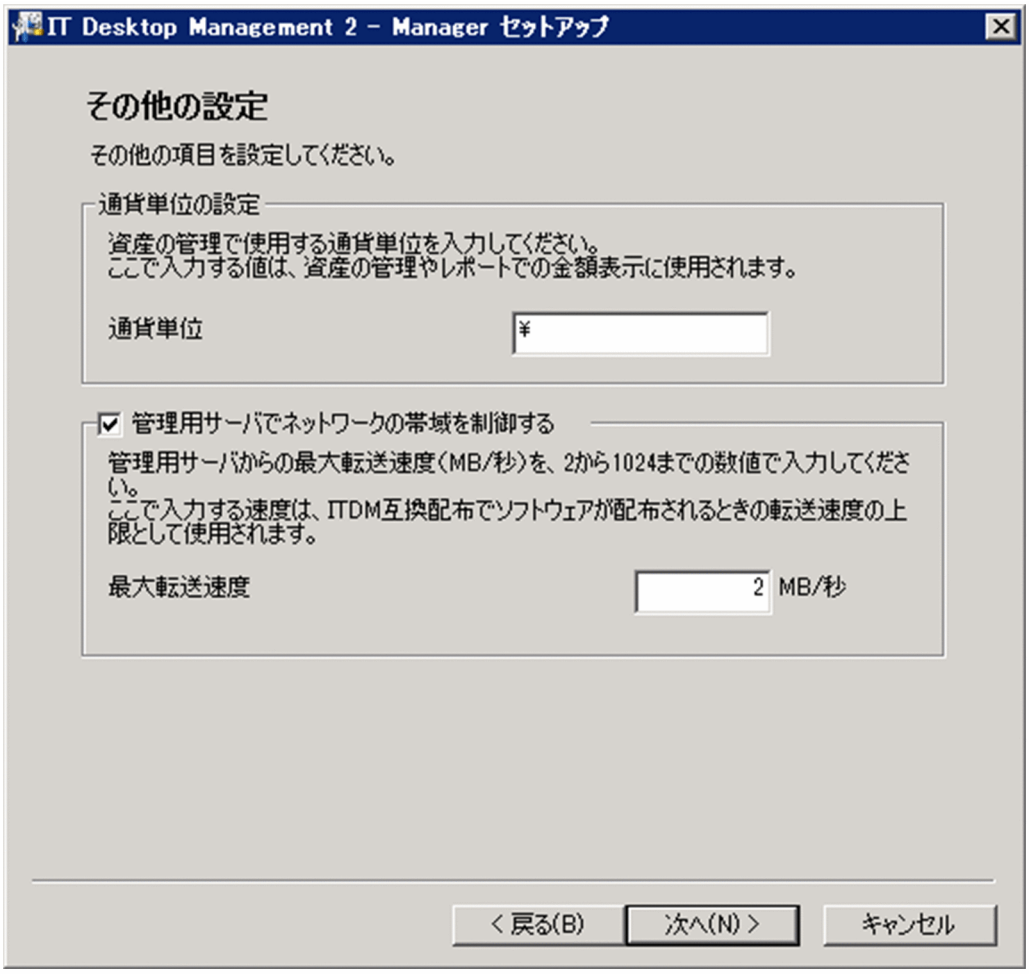
3.11　通貨単位を変更する手順

管理用サーバのセットアップ項目です。

資産管理で使用する通貨単位を変更できます。

通貨単位を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［その他の設定］画面が表示されるまで、［次へ］ボタンをクリックします。



6. ［通貨単位の設定］で［通貨単位］を入力し、［次へ］ボタンをクリックします。
7. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックします。

リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console が使用中でないことの確認を促すダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。

クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

8. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

9. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

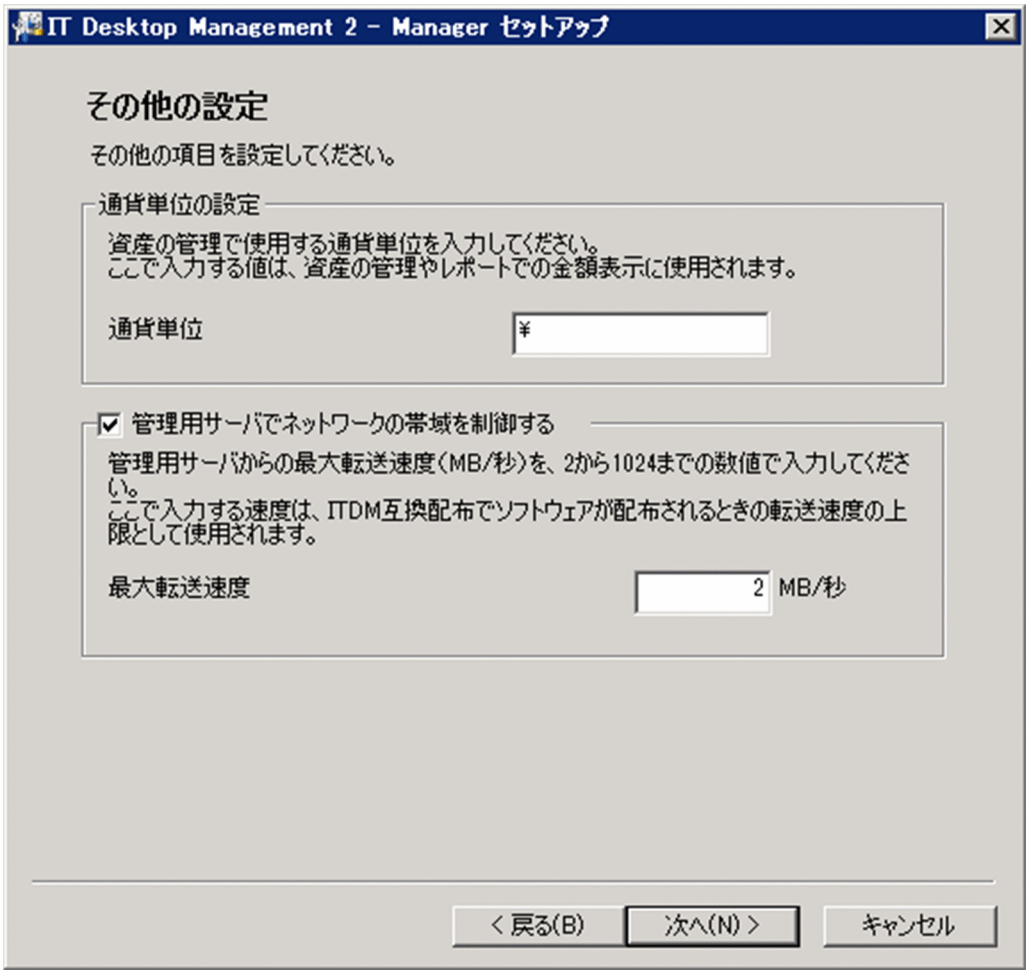
通貨単位が変更されます。

3.12　配布時に使用されるネットワーク帯域を制御する手順

管理用サーバから管理対象のコンピュータにソフトウェアやファイルを配布するときに、すべてのネットワーク帯域を使用しないように最大転送速度を設定して、ネットワーク帯域を制御できます。

ITDM 互換配布のネットワーク帯域を制御するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［その他の設定］画面が表示されるまで、［次へ］ボタンをクリックします。



6. ［管理用サーバでネットワークの帯域を制御する］をチェックして［最大転送速度］を入力し、［次へ］ボタンをクリックします。
7. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックします。

リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console が使用中でないことの確認を促すダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。

クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

8. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

9. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

ネットワーク帯域が制御されるようになります。

リモートインストールマネージャを使用した配布のネットワーク帯域を制御するには：

1. JP1/IT Desktop Management 2 - Manager のサービスを停止します。
2. コンフィグレーションファイルに設定を追加します。

   コンフィグレーションファイル（jdn_rim_distr_bwc.conf）の格納先は次のとおりです。

   JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥conf
3. JP1/IT Desktop Management 2 - Manager のサービスを起動します。

ネットワーク帯域が制御されるようになります。

コンフィグレーションファイルで設定する定義を次の表に示します。

セクション	キー	説明	初期値	省略可否
BandwidthCtrl	Function	リモートインストールマネージャを使用した配布時に流量制御するかどうかを指定します。 • ON：流量制御する。 • OFF：流量制御しない。	OFF	必須
Setting*N*※1	MinIP※2	0.0.0.0～255.255.255.255 の範囲で、IP アドレスの範囲の開始値を指定します。	0.0.0.0	必須
	MaxIP	0.0.0.0～255.255.255.255 の範囲で、IP アドレスの範囲の終了値を指定します。	255.255.255.255	必須
	MaxTransSpeedKbps	Kbps 単位の整数（32※3～8,388,608※4 の範囲）で、最大転送速度を指定します。	15360	必須

注※1　*N* は 1～30 の数値です。IP アドレスの範囲を複数設定する場合は、Setting1、Setting2、Setting3 のように定義します。なお、IP アドレスの範囲を複数設定する場合、各Setting*N* セクションの IP アドレスの範囲が重ならないように設定してください。

注※2　MaxIP より小さい値を指定します。MaxIP の値より大きい値を指定した場合、そのSetting*N* セクションの設定は無効になります。

注※3　KB 単位に換算すると 4KB/秒です（32 ÷ 8（bit） ＝ 4）。

注※4　KB 単位に換算すると 1,048,576KB/秒です（8388608 ÷ 8（bit） ＝ 1048576）。MB 単位に換算すると 1,024MB/秒です（8388608 ÷ 8（bit） ÷ 1024 ＝ 1024）。

コンフィグレーションファイルの設定例を次に示します。

管理用サーバが属する LAN 全体のネットワーク帯域の流量制御をする場合

```
[BandwidthCtrl]
Function=ON

[Setting1]
MinIP=0.0.0.0
MaxIP=255.255.255.255
MaxTransSpeedKbps=1024
```

特定のネットワーク帯域の流量制御をする場合

```
[BandwidthCtrl]
Function=ON

[Setting1]
MinIP=192.168.0.0
MaxIP=192.168.0.255
MaxTransSpeedKbps=1024

[Setting2]
MinIP=192.168.100.0
MaxIP=192.168.100.255
MaxTransSpeedKbps=320
```

コンフィグレーションファイルについての注意事項を次に示します。

- セクションが重複している場合、先に定義したセクションが有効となります。
- キーが重複している場合、セクション内で先に定義したキーが有効となります。
- Setting*N* セクションの IP アドレスの範囲が次に示すように重なっている（192.168.100.*の範囲が Setting1 とSetting2 の両方に含まれている）場合は、優先順位が上位（*N* の値に依存してSetting1 が 1 番上）のセクションの設定で動作します。つまり、IP アドレスが 192.168.100.*（*：0～255）のエージェントへの配布は、最大転送速度が 1,024Kbps となります。

```
[BandwidthCtrl]
Function=ON

[Setting1]
```

```
MinIP=192.168.0.0
MaxIP=192.168.100.255
MaxTransSpeedKbps=1024

[Setting2]
MinIP=192.168.100.0
MaxIP=192.168.200.255
MaxTransSpeedKbps=320
```

- BandwidthCtrl セクションのFunction キーにOFF を指定した場合は、有効なSetting*N* セクションがあっても、流量制御されません。
- BandwidthCtrl セクションのFunction キーにON を指定した場合に、有効なSetting*N* セクションが 1 個もないときには流量制御されません。
- コンフィグレーションファイル（jdn_rim_distr_bwc.conf）のオープンに失敗した場合は、流量制御されません。

ヒント

リモートインストールマネージャを使用した配布機能での流量制御の適用状況は、管理用サーバ起動時に出力される MAIN.LOG ファイルか Windows イベントログのメッセージで確認できます。

ヒント

次の場合、流量制御されません。

- リモートコレクト機能によるファイルの収集
- マルチキャスト配布を設定した場合の配布

中継システムでリモートインストールマネージャを使用した配布のネットワーク帯域を制御するには：

1. 中継システムのコンフィグレーションファイルに設定を追加します。

   コンフィグレーションファイル（jdn_rim_distr_bwc.conf）の格納先は次のとおりです。

   JP1/IT Desktop Management 2 - Agent のインストール先フォルダ¥conf¥jdn_rim_distr_bwc.conf

   コンフィグレーションファイルで設定する定義を次の表に示します。

セクション	キー	説明	初期値	省略可否
BandwidthCtrl	Function	リモートインストールマネージャを使用した配布時に中継システムで流量制御するかどうかを指定します。 • ON：流量制御する。 • OFF：流量制御しない。	OFF	必須

セクション	キー	説明	初期値	省略可否
Setting	MaxTransSpeed Kbps	Kbps 単位の整数（32※1～8,388,608※2 の範囲）で、最大転送速度を指定します。	15360	必須

注※1　KB 単位に換算すると 4KB/秒です（32 ÷ 8（bit） ＝ 4）。

注※2　KB 単位に換算すると 1,048,576KB/秒です（8388608 ÷ 8（bit） ＝ 1048576）。MB 単位に換算すると 1,024MB/秒です（8388608 ÷ 8（bit） ÷ 1024 ＝ 1024）。

中継システム用のコンフィグレーションファイルの設定例を次に示します。

```
[BandwidthCtrl]
Function=ON

[Setting]
MaxTransSpeedKbps=1024
```

コンフィグレーションファイルについての注意事項を次に示します。

- セクションが重複している場合、先に定義したセクションが有効となります。
- キーが重複している場合、セクション内で先に定義したキーが有効となります。
- BandwidthCtrl セクションのFunction キーにOFF を指定した場合は、有効なSetting セクションがあっても、流量制御されません。
- BandwidthCtrl セクションのFunction キーにON を指定した場合に、有効なSetting セクションが 1 個もないときには流量制御されません。
- コンフィグレーションファイル（jdn_rim_distr_bwc.conf）のオープンに失敗した場合は、流量制御されません。

2. 中継システムの OS を再起動します。

3. 中継システムの MAIN.LOG ファイルを確認します。

   リモートインストールマネージャを使用した配布機能での流量制御の適用状況に関するメッセージで、設定ファイルに指定した設定がすべて出力されていることを確認してください。

中継システムでリモートインストールマネージャを使用した配布のネットワーク帯域の制御を無効にする場合は、コンフィグレーションファイルのBandwidthCtrl セクションのFunction キーにOFF を指定してから同じ手順で実行してください。

管理者がリモートインストールマネージャから配下の中継システムへ設定ファイルを配布するには：

1. 管理者の端末で、中継システムに配布するコンフィグレーションファイルを作成します。

   作成するコンフィグレーションファイルの詳細は、「中継システムでリモートインストールマネージャを使用した配布のネットワーク帯域を制御するには」の手順 1 を参照してください。

2. 管理者の端末で、作成したコンフィグレーションファイルをパッケージャからパッケージングします。

3. リモートインストールマネージャから、パッケージングしたコンフィグレーションファイルを中継システムに配布ジョブで配布します。

配布ジョブの作成時に、[パッケージ] パネルで [変更] ボタンをクリックして表示される [インストール条件の変更] ダイアログボックスで、次の項目を設定してください。

[システム条件] パネル

・[インストール先ディレクトリ] に次のパスを指定

JP1/IT Desktop Management 2 - Agent のインストール先フォルダ¥conf

・[同じパッケージがあったら上書き] チェックボックスをオン

[オプション] パネル

[インストール後コンピュータを再起動する] チェックボックスをオン

ジョブ作成の詳細は、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」のリモートインストールの実行についての説明を参照してください。

4. リモートインストールマネージャのジョブ実行状況画面で、中継システムへの配布ジョブが完了したことを確認します。

5. リモートインストールマネージャでリモートコレクトジョブを実行し、中継システムから配布したコンフィグレーションファイルと公開ログを収集します。

収集対象として次のファイルを指定してください。

- 配布したコンフィグレーションファイル
- 公開ログ：*JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*¥log¥MAIN_0000.log

6. 収集したコンフィグレーションファイルが手順 1 で作成したファイルと同じ内容であるか確認します。

7. 収集した公開ログを確認します。

リモートインストールマネージャを使用した配布機能での流量制御の適用状況に関するメッセージで、設定ファイルに指定した設定がすべて出力されていることを確認してください。

中継システムでリモートインストールマネージャを使用した配布のネットワーク帯域の制御を無効にする場合は、コンフィグレーションファイルのBandwidthCtrl セクションのFunction キーにOFF を指定してから同じ手順で実行してください。

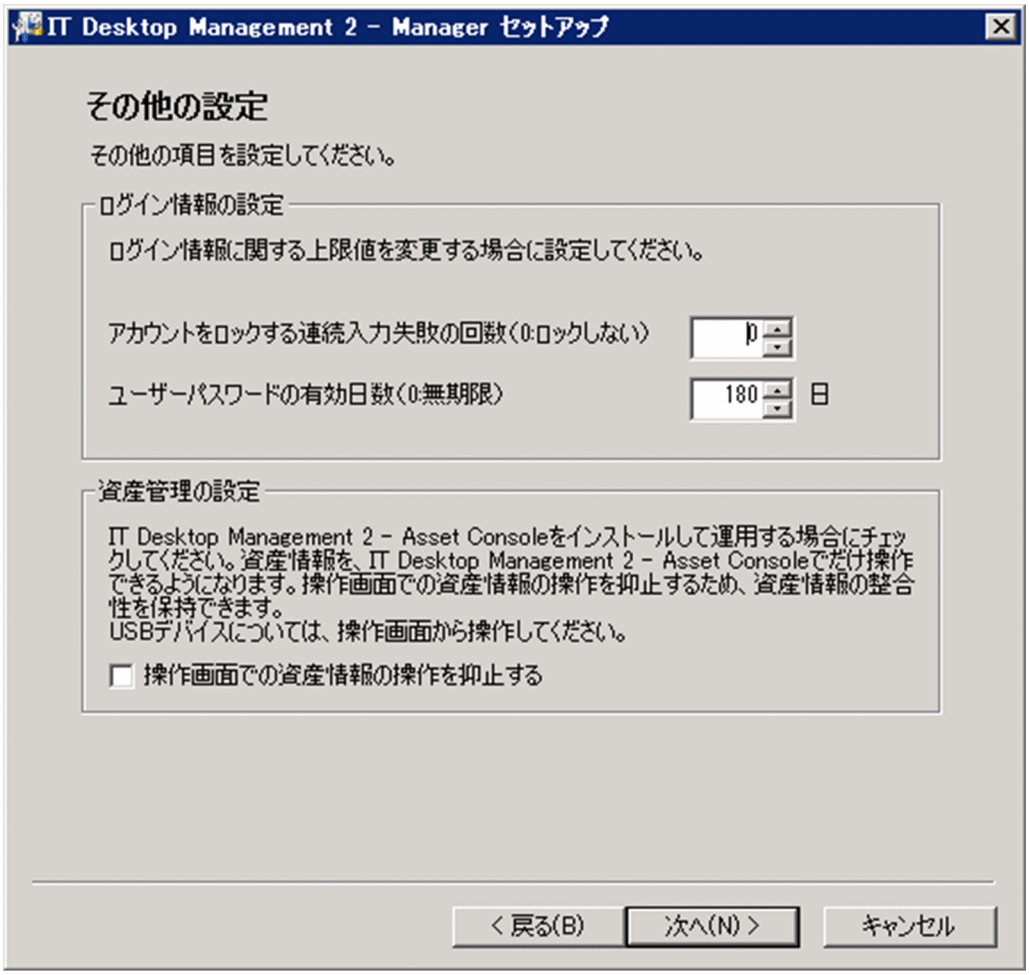
3.13　ログイン制限情報を変更する手順

連続して何回ログインに失敗したらアカウントをロックするかやログインユーザーのパスワードの有効期限を変更できます。

> **重要**
>
> セットアップの［ユーザー管理の設定］画面で JP1 認証を使用するよう設定した場合、JP1/IT Desktop Management 2 ではユーザーアカウントのロックおよびパスワードの有効期限の設定ができなくなります。この場合、［その他の設定］画面の［ログイン情報の設定］に設定した値は適用されません。

アカウントをロックする連続入力失敗の回数やログインユーザーのパスワードの有効期限を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［その他の設定］画面が表示されるまで、［次へ］ボタンをクリックします。
   ［その他の設定］画面の例を次に示します。



6. 必要に応じて次の項目を変更し、[次へ] ボタンをクリックします。

   - アカウントをロックする連続入力失敗の回数

     連続して何回ログインに失敗したら、アカウントをロックするかを指定します。

   - ユーザーパスワードの有効日数

     ログインユーザーのパスワードの有効期限として、パスワードが有効な日数を指定します。

7. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

   リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

8. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

9. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

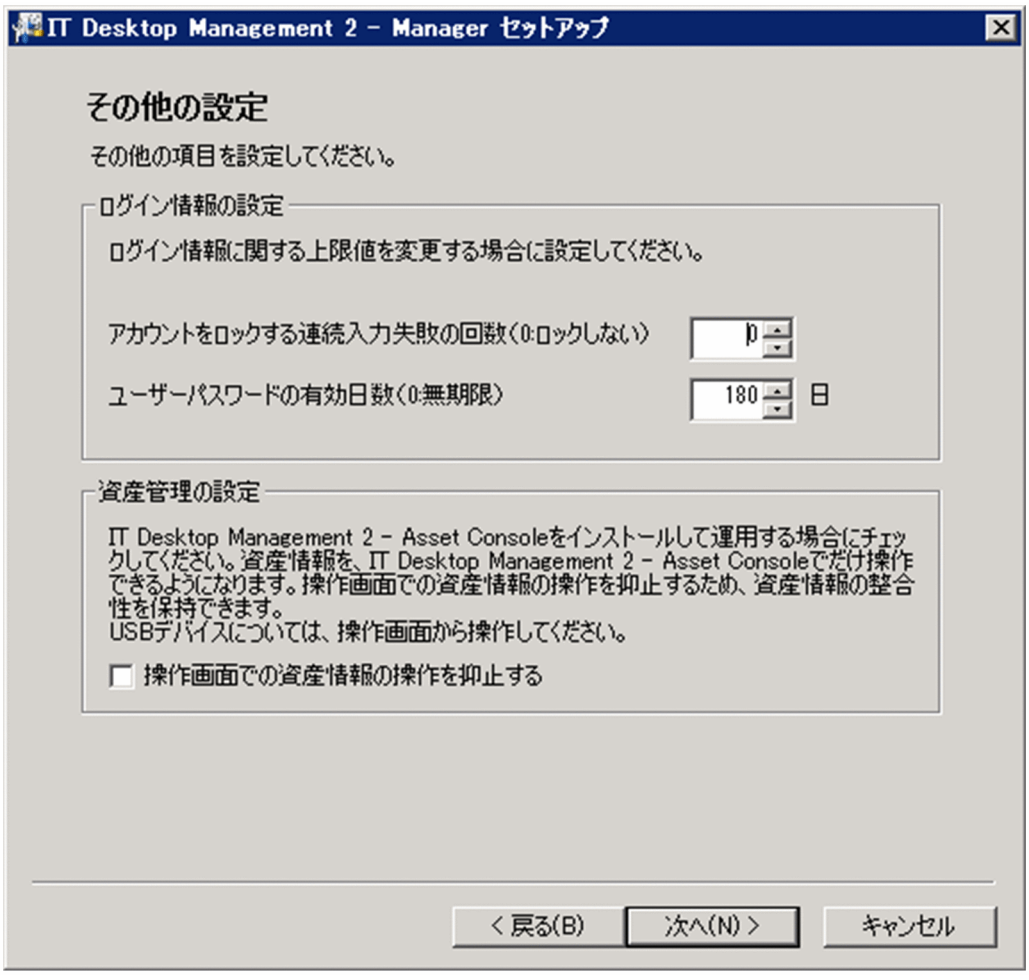
ログイン制限情報が変更されます。

3.14　資産情報の登録と編集を抑止する手順

Asset Console を使用して資産管理をする場合、操作画面での資産情報の登録と編集を抑止するように設定できます。

資産情報の登録と編集を抑止するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［その他の設定］画面が表示されるまで、［次へ］ボタンをクリックします。
   ［その他の設定］画面の例を次に示します。



6. ［操作画面で資産情報の操作を抑止する］をチェックし、［次へ］ボタンをクリックします。
7. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックします。

リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、[OK] ボタンをクリックしてください。クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、[OK] ボタンをクリックしてください。

8. [リモートインストールマネージャを使用した配布のセットアップ] 画面で、[OK] ボタンをクリックします。

   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

9. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

操作画面での資産情報の登録と編集が抑止されます。

3.15　データベースをアップグレードする手順

管理用サーバのセットアップ項目です。

JP1/IT Desktop Management 2 を上書きインストールした場合に、データベースのアップグレードが必要なときは、データベースをアップグレードしてください。

> **重要**
>
> 上書きインストールの完了時に［セットアップ］のチェックを外していた場合、セットアップは実行されません。このため、次の手順でデータベースをアップグレードしてください。

データベースをアップグレードするには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で［データベースアップグレード］を選択して、［次へ］ボタンをクリックします。

   JP1/IT Desktop Management 2 がデータベースのアップグレードが必要と判断しているときだけ、［データベースアップグレード］を選択できます。［データベースアップグレード］を選択できない場合、データベースのアップグレードは不要です。この場合、［キャンセル］ボタンをクリックしてセットアップを終了してください。
5. ［データベースアップグレードの設定］画面でアップグレードの設定をして、［次へ］ボタンをクリックします。

   データベースフォルダを変更した場合、データベース内の操作ログ以外のデータは、変更前の状態で引き継がれますが、変更前の操作ログデータは削除されます。必要に応じて操作ログの手動取り込みを実施してください。
6. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックします。
7. セットアップの完了を示すダイアログで、セットアップに続いてコンポーネントを登録するかどうかを設定して［OK］ボタンをクリックします。

   コンポーネントとは、エージェントおよびネットワークモニタエージェントを指します。これらのプログラムを管理用サーバに登録しておくことで、エージェントを配信したり、ネットワークモニタエージェントを操作画面からインストールしたりできるようになります。

   コンポーネントを登録する場合は、［コンポーネントの登録］ダイアログが表示されるので、コンポーネントの登録とアップデートについて設定します。

> **ヒント**
>
> インストールの続きでセットアップを起動した場合は、セットアップの完了を示すダイアログ上でコンポーネントのアップデートについて設定できます。

コンポーネントのアップデートについては、「5.8　コンポーネントのアップデート方法」を参照してください。

データベースがアップグレードされます。

3.16　データベースを初期化する手順

JP1/IT Desktop Management 2 が使用するデータベースを初期化できます。

データベースを初期化するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［サーバの再構築］を選択します。
5. ［次へ］ボタンをクリックして、各画面でデータベースの設定をします。
6. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックします。

   リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、［OK］ボタンをクリックしてください。クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、［OK］ボタンをクリックしてください。
7. セットアップの完了を示すダイアログで、セットアップに続いてコンポーネントを登録するかどうかを設定して［OK］ボタンをクリックします。

   コンポーネントとは、エージェントおよびネットワークモニタエージェントを指します。これらのプログラムを管理用サーバに登録しておくことで、エージェントを配信したり、ネットワークモニタエージェントを操作画面からインストールしたりできるようになります。

   コンポーネントを登録する場合は、［コンポーネントの登録］ダイアログが表示されるので、コンポーネントの登録とアップデートについて設定します。

   コンポーネントのアップデートについては、「5.8　コンポーネントのアップデート方法」を参照してください。

データベースが初期化されます。

> **重要**
>
> データベースを初期化しても、フォルダに格納されているファイルは削除されません。作業用フォルダや操作ログのバックアップデータの保存フォルダのデータが不要な場合は、手動で削除してください。

3.17　API の使用を設定する手順

管理用サーバのセットアップ項目です。

管理用サーバで API を使用できるように設定を変更できます。

API の使用を設定するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択します。
3. セットアップ画面で［次へ］ボタンをクリックします。
4. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックします。
5. ［API の設定］画面が表示されるまで、［次へ］ボタンをクリックします。
6. ［API を使用する］のチェックボックスを選択し、［次へ］ボタンをクリックします。
7. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックします。
   リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、［OK］ボタンをクリックしてください。クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、［OK］ボタンをクリックしてください。
8. ［リモートインストールマネージャを使用した配布のセットアップ］画面で、［OK］ボタンをクリックします。
   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、［セットアップを終了します］画面が表示されます。
9. ［セットアップを終了します］画面で、［OK］ボタンをクリックします。

API を使用できるようになります。

4 構築時の設定のカスタマイズ

ここでは、構築時の設定で、カスタマイズできる項目について説明します。

4.1　最小構成システムの構築時の設定

4.1.1　探索条件を設定する手順（ネットワークの探索）

ネットワークの機器を探索する場合の探索条件を設定できます。

探索条件を設定するには：

1. 設定画面を表示します。
2. メニューエリアで［機器の探索］－［探索条件の設定］－［ネットワークの探索］を選択します。
3. ［探索範囲の設定内容］で探索範囲の IP アドレスを設定します。

   探索範囲には、最初から「管理用サーバセグメント」という名称の探索範囲が設定されています。管理用サーバセグメントとは、管理用サーバが含まれるセグメントのことです。

   探索範囲を追加する場合は［探索範囲の追加］ボタンをクリックします。すでに登録済みの探索範囲を変更する場合は、編集したい探索範囲名の［編集］ボタンをクリックします。探索範囲の追加と編集で探索範囲を設定できるダイアログが表示するので、探索開始 IP アドレスと探索終了 IP アドレスを設定します。

   IP アドレスを設定したら［認証情報］を設定します。認証情報が未登録の場合、先に手順 4 を実施してください。

   登録した認証情報をすべて利用する場合は［すべて］にチェックします。認証情報を選択して利用する場合は［選択］をチェックし、Windows または SNMP で登録した認証情報を選択してください。
4. ［認証情報］で認証情報を設定します。

   認証情報を利用して探索する場合に、認証情報を設定してください。認証情報を登録したら、［探索範囲の設定内容］で探索範囲ごとに認証情報を割り当ててください。

   認証情報については、「4.1.2　ネットワークの探索時に使用する認証情報」を参照してください。
5. ［探索スケジュール］を編集します。

   スケジュールを決めて定期的に探索を実行する場合に、探索スケジュールの［編集］ボタンをクリックして、スケジュールを設定してください。

   スケジュールを設定していない場合は探索を実行しません。この場合、［探索を開始］ボタンをクリックして即時実行してください。
6. ［発見した機器への操作］を編集します。

   機器の探索時に新しい機器が発見された場合の操作を設定してください。

   発見した機器への操作の［編集］ボタンをクリックすると、［発見した機器への操作］ダイアログが表示されます。このダイアログで、発見した機器を自動的に管理対象にしたり、エージェントを自動配信したりできます。
7. ［完了通知］を編集します。

機器の探索が完了したら JP1/IT Desktop Management 2 の管理者にメールで通知する場合に、通知先を設定してください。

利用するメールサーバ（SMTP サーバ）の情報を設定していない場合は、［メールサーバの設定へ］のリンクをクリックして表示される画面で、メールサーバの情報を設定してください。

探索条件の設定が完了します。

設定した探索条件で探索を即時実行する場合は、［探索を開始］ボタンをクリックしてください。即時実行しない場合は、［探索スケジュール］に従って実行されます。

探索の実行状況と実行結果は、設定画面の［探索履歴の確認］－［ネットワークの探索］画面で確認できます。

関連リンク

- 1.7.3　機器の探索状況の確認
- 4.1.2　ネットワークの探索時に使用する認証情報

4.1.2　ネットワークの探索時に使用する認証情報

ネットワークの探索では、ARP と ICMP を利用して機器が発見されますが、それだけでは機器の詳細情報は収集されません。探索時に機器の詳細情報も収集するためには、発見された機器に対して SNMP または Windows の管理共有を利用して接続できるように認証情報を設定する必要があります。

SNMP の認証情報

コミュニティ名

Windows の管理共有の認証情報

- Administrator 権限のユーザー ID
- パスワード

SNMP を利用できる機器の場合、コミュニティの認証ができるときは、発見と同時に機器種別の判別、および一部の機器情報を収集できます。

Windows の管理共有が有効なコンピュータの場合、Administrator 権限でログオン認証できるときは、コンピュータを発見すると同時に機器種別の判別、および大部分の機器情報を収集できます。さらに、エージェントを配信してインストールすることもできます。

重要

OS が Windows Me、Windows 98、Windows 95、および Windows NT 4.0 のコンピュータは、発見されても機器種別が「不明な機器」として扱われることがあります。

重要

1 台の機器にネットワークカードが複数ある場合、ICMP が使用されて探索されたとき、複数台の機器として発見されます。

ヒント

Windows の管理共有の認証で使用するユーザー ID は、ドメインユーザーで認証する場合は、「*ユーザー ID@FQDN（完全修飾ドメイン名）*」または「*ドメイン名*¥*ユーザー ID*」の形式で指定してください。FQDN とは、ホスト名やドメイン名を省略しないで記述する形式です。例えば、「User001@PC001.hitachi.com」のように指定します。

ヒント

Windows の管理共有の認証を利用する場合、コンピュータ側で管理共有の設定を有効にしておく必要があります。

探索は、各探索範囲に対して認証情報を組み合わせて実行します。デフォルトでは、設定したすべての認証情報が使われますが、部署ごとに SNMP のコミュニティ名を分けている場合や、Windows の認証情報がコンピュータによって異なる場合などでは、探索範囲ごとに必要な認証情報だけを選択して実行することもできます。

なお、ネットワークの探索で使用する認証情報は、エージェントを配信するときにも利用されます。探索したあとでエージェントを配信する場合は、設定画面の［機器の探索］－［探索条件の設定］－［ネットワークの探索］画面で、配信先のコンピュータが含まれる探索範囲に対して Windows の管理共有の認証情報を設定しておく必要があります。

重要

Windows 認証を使用したネットワーク探索では、探索対象の機器間で共通のアカウントがなく、機器ごとに異なる認証情報を使用する環境では、ネットワーク探索を実施したときに探索対象の機器のアカウントがロックアウトされることがあります。アカウントがロックアウトされるのは、次に示す条件がすべて重なった場合です。

- 探索範囲に Windows 認証情報を設定している。
- 探索対象の機器でアカウントロックアウトのポリシーを設定している。
- 探索対象の機器で失敗する認証情報がある。
  探索対象の機器間で共通のアカウントがなく、機器ごとに異なる認証情報を使用する必要がある環境の場合に該当します。
- ネットワーク探索を実施する。

アカウントロックアウトのポリシーを設定している機器に対して Windows 認証を使用したネットワーク探索を実施する場合は、探索範囲を分けて認証情報の数を少なくしたり、不要な認証情報を削除したりすることで、認証情報の数がアカウントのロックアウトのしきい値より少なくなるようにしてください。

4.1.3 エージェント設定を追加する手順

コンピュータによってエージェント設定を分けたい場合、エージェント設定を追加します。

エージェント設定を追加するには：

1. 設定画面を表示します。
2. メニューエリアで［エージェント］－［Windows エージェント設定とインストールセットの作成］を選択します。
3. インフォメーションエリアで［エージェント設定を追加］ボタンをクリックします。
4. 表示される［エージェント設定の追加］ダイアログでエージェント設定の情報を入力して、［OK］ボタンをクリックします。

   エージェント設定の情報については、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」のエージェント設定のパラメーターを参照してください。

エージェント設定が追加され、エージェント設定の一覧に表示されます。

追加したエージェント設定は、［Windows エージェント設定の割り当て］画面でエージェント設定を割り当てることで、エージェント導入済みのコンピュータにも適用できます。

4.1.4 中継システムの設定を追加する手順

リモートインストールマネージャを使用して配布する場合で、中継システムによって、ID 登録先システム、運用キー、管理用サーバへの通知、中継システムでの処理の設定などを分けたいときは、中継システムの設定を追加できます。なお、中継システムの設定はエージェント設定の一部として設定します。

中継システムの設定を追加するには：

1. 設定画面を表示します。
2. メニューエリアで［エージェント］－［Windows エージェント設定とインストールセットの作成］を選択します。
3. インフォメーションエリアで［エージェント設定を追加］ボタンをクリックします。

4. 表示されるダイアログで［中継システムの設定］を選択し、設定情報を入力します。

5. 必要に応じて、ほかのメニュー項目についても設定情報を入力して、［OK］ボタンをクリックします。

中継システム用のエージェント設定が追加され、エージェント設定の一覧に表示されます。

追加したエージェント設定は、［Windows エージェント設定の割り当て］画面でエージェント設定を割り当てることで、中継システム導入済みのコンピュータにも適用できます。

4.1.5 コンフィグレーションファイルで処理の設定を変更する手順

処理の開始時刻や JP1/IT Desktop Management 2 - Agent をアンインストールした時に、機器の廃棄として扱うか、JP1/IT Desktop Management 2 - Agent のアンインストールとして扱うかどうかの指定などは、コンフィグレーションファイルの設定を変更することで有効になります。なお、コンフィグレーションファイルの設定は、JP1/IT Desktop Management 2 のサービスの再起動後に適用されます。

コンフィグレーションファイルで設定できるプロパティについては、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」のプロパティ一覧を参照してください。

コンフィグレーションファイル（jdn_manager_config.conf）を設定するには：

1. コンフィグレーションファイルに設定を追加します。

   コンフィグレーションファイル（jdn_manager_config.conf）の格納先は次のとおりです。

   JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥conf

コンフィグレーションファイルで設定する定義を次の表に示します。

プロパティ	説明	設定値	デフォルト
State_AfterAgentUninstalling※1	JP1/IT Desktop Management 2 - Agent をアンインストールした時に、機器の廃棄として扱うか、JP1/IT Desktop Management 2 - Agent のアンインストールとして扱うかどうかの指定	• 0：アンインストールとして扱う • 1：機器の廃棄として扱う	0
Report_Data_MakeTime※4	レポートの集計データを作成する時間	00:00～23:59	23:00
Report_Digest_MakeTime※4	ダイジェストレポートを作成する時間	00:00～23:59	06:00

プロパティ	説明	設定値	デフォルト
DB_MentenanceTime※4	データベースをメンテナンスする時間	00:00～23:59	05:00
ChangeHistory_GetTime※4	変更履歴を取得する時間	00:00～23:59	00:00
OpLog_DB_DeleteTime※4	自動取り込みされた操作ログのデータベースのメンテナンスを実施する時間	00:00～23:59	01:00
DeviceAutoMaintenanceTime※4	機器のメンテナンスが有効な場合にメンテナンス処理を開始する時間	00:00～23:59	23:00
AgentStartMenu_Display	インストールセット、エージェントの配信による、エージェントでのスタートメニューの表示についての設定	• ON：エージェントのすべてのスタートメニューを表示する。 • OFF：エージェントのすべてのスタートメニューを表示しない。※2 • SELECT:*xxx*,*xxx*,... ：表示するスタートメニューを選別する。 *xxx* に指定できるメニュー項目を次に示します。複数を指定する場合は項目間をコンマ（,）で区切ってください。 • IDR：[ID への登録] • UINF：[利用者情報の入力] • PSM：[パッケージセットアップマネージャ] • RCCHAT：[リモコンエージェント] － [チャット] • RCREQ：[リモコンエージェント] － [リクエスタウィザード] • RCAGT：[リモコンエージェント] － [リモコンエージェント] • ATAIT：[管理者ツール] － [Automatic Installation Tool] • ATUSB：[管理者ツール] － [USB デバイスの登録] • ATSET：[管理者ツール] － [セットアップ] • ATPACK：[管理者ツール] － [パッケージャ] • ATSEND：[管理者ツール] － [収集情報の通知] 例えば、[パッケージセットアップマネージャ] と [USB デバイスの登録] を表示する場合は、次のように指定します。 SELECT:PSM,ATUSB	なし

プロパティ	説明	設定値	デフォルト
SDM_Mapping_Name	JP1/IT Desktop Management 2 - Smart Device Manager に登録したスマートデバイスの名称を、JP1/IT Desktop Management 2 の操作画面に表示するホスト名、コンピュータ名または機器名称としてマッピングするかどうかの設定	0：マッピングしない※3 1：マッピングする	1
Mgrsrv_Patch_AutoPackageKind	更新プログラムの自動取得を行うかどうかの指定	0：更新プログラムの自動取得を行わない 1：更新プログラムの 自動取得を行う	1
ExcludeNetworkGroup※5	ネットワークグループの自動作成を抑止する設定	32 その他の値は指定できません。	なし
AbortDeviceIdentify※6	機器の登録時の同定を行わない設定	MAC アドレスを 1 つ以上指定 MAC アドレスはセパレータを含めて 17 文字で指定します。 英字部分は大文字、小文字を区別しません。 MAC アドレスのセパレータは":"か"-"を指定します。 MAC アドレスを複数指定する場合は項目間をコンマ（,）で区切ってください。 例えば、00:05:9a:3c:7a:00 と 00:09:0f:fe:00:01 を指定する場合は、次のように指定します。 00:05:9a:3c:7a:00,00:09:0f:fe:00:01 指定できる MAC アドレスの上限は 30 個です。	なし
DisableNCListUpdate※7	ネットワーク制御リストの自動更新を抑止する設定	MAC アドレスを 1 つ以上指定 次のどちらか、または、組み合わせて指定します。 • 複数の機器で重複する MAC アドレス MAC アドレスをセパレータを含めて 17 文字で指定します。 • ランダム MAC アドレス ランダム MAC アドレスと前方一致する 17 文字以内で指定します。 英字部分は大文字、小文字を区別しません。 MAC アドレスのセパレータは“:”か”-”を指定します。 複数を指定する場合は項目間をコンマ（,）で区切ってください。例えば、00:05:9a:3c:7a:00 と	なし

プロパティ	説明	設定値	デフォルト
DisableNCListUpdate※7	ネットワーク制御リストの自動更新を抑止する設定	00:09:0f:fe:00:01 を指定する場合は、次のように指定します。 00:05:9a:3c:7a:00,00:09:0f:fe:00:01 前方一致は“$”を含めて指定します。 例えば、先頭「02:05:」が一致する MAC アドレスを指定する場合は、次のように指定します。 02:05:$ 指定できる MAC アドレスの上限は 100 個です。	なし
NetworkControlListWarningThreshold	ネットワーク制御リストの警戒しきい値	0～262140	162140
NetworkControlListNoticeOption	ネットワーク制御リストの登録数が警戒しきい値に達した場合と上限に達した場合のメッセージをホーム画面の通知事項に通知するかどうかの設定	ON：通知する OFF：通知しない	ON

注※1

エージェントからのアンインストール通知を受信できなかった場合は、これまでと同様に機器情報は変更されません。この場合は、必要に応じて機器情報を削除するなどして、対処してください。また、ネットワークモニタが有効なコンピュータは、機器情報が削除されません。ネットワークモニタを無効化したあと、機器情報を削除するなどして、対処してください。

注※2

Citrix XenApp、Microsoft RDS サーバの場合、エージェントのスタートメニューの表示をサポートしていないため、すべてのスタートメニューを非表示に設定してください。

注※3

「0」を設定した場合は、JP1/IT Desktop Management 2 - Smart Device Manager から取得したスマートデバイスに関する情報の利用者名、電話番号およびモデル名を組み合わせて区切り文字のコロン(:）で結合した形式の名称（例：佐藤大輔:09012345678:iPhone）が JP1/IT Desktop Management 2 の操作画面のホスト名、コンピュータ名または機器名称として表示されるようになります。

注※4

デフォルト値から時間を変更する場合は、各処理が重なることで管理用サーバの負荷が高くなることを避けるため、各設定値をデフォルトから同じ時間ずらした値を設定してください。 例えば、8 時間ずらす場合は、デフォルト 23:00 に実行されている機能を 07:00 に、デフォルト 00:00 に実行されている機能を 08:00 に設定します。

注※5

サブネットマスク情報が 255.255.255.255 で通知されたときにネットワークグループを作成せず、ネットワークグループ数の増加する状態を防ぎます。機器がどのネットワークグループにも属さない場合は「不明」グループに属します。

注※6

複数の機器で重複する MAC アドレスを指定します。機器から通知された MAC アドレスが設定値に指定したいずれかの MAC アドレスと一致する場合は、機器の同定を行いません。

注※7

機器から通知された MAC アドレスが設定値に指定した MAC アドレスのどれかと一致する場合は、ネットワーク制御リストの更新を行いません。

コンフィグレーションファイルの設定例を次に示します。

```
#
# コンフィグレーションファイル
#
# 変更履歴を取得する時間
ChangeHistory_GetTime=00:00
```

コンフィグレーションファイルの設定は、JP1/IT Desktop Management 2 のサービスの再起動後に適用されます。

4.1.6 エージェントの監視項目を変更する手順

エージェント導入済みのコンピュータを定期的に監視する項目を、インベントリ設定ファイル（jdng_inventory.conf）を使用することで変更できます。

エージェントの監視項目を変更するには：

1. 次の表に示す内容を入力したインベントリ設定ファイル（jdng_inventory.conf）をテキストエディタで作成し、%ALLUSERSPROFILE%¥HITACHI¥jp1itdma¥conf フォルダに格納します。

セクション	キー名	説明	設定値	デフォルト
SystemInventory	DHCPLeaseExpires	DHCP リース期限日時の変更を監視するかどうかを指定できます。 セクションやキー名が存在しない場合、または無効な値が設定されている場合は、デフォルト値 0 として動作します。	• 0：監視しない • 1：監視する	0
	DHCPLeaseObtained	DHCP リース取得日時の変更を監視するかどうかを指定できます。 セクションやキー名が存在しない場合、または無効な値が設定されている場合は、デフォルト値 0 として動作します。	• 0：監視しない • 1：監視する	0

エージェントの監視項目が変更されます。

DHCP リース期限日時と DHCP リース取得日時を監視対象項目とする場合の、インベントリ設定ファイルの設定例を次に示します。この場合の監視間隔は、エージェント設定の［基本設定］－［上位システムとの通信のタイミング］－［監視間隔（セキュリティ項目以外）(分)］に指定した値になります。

```
[SystemInventory]
DHCPLeaseExpires=1
DHCPLeaseObtained=1
```

なお、インベントリ設定ファイルで設定した内容は、次に機器情報を取得するタイミングから自動的に適用されます。

4.1.7 UNIX エージェント、Mac エージェントのソフトウェア情報管理の設定を変更する手順

UNIX や Mac のソフトウェア情報を取得して JP1/IT Desktop Management 2 の操作画面で管理するには、コンフィグレーションファイル（jdn_manager_config.conf）を編集する必要があります。コンフィグレーションファイルを編集すると、管理対象の UNIX や Mac のコンピュータから通知されたり、ジョブの実行で UNIX エージェントや Mac エージェントから収集したりした、UNIX や Mac のソフトウェア情報を機器画面に表示できるようになります。また、UNIX 用や Mac 用のソフトウェアライセンス管理もできるようになります。ただし、OS によっては 1,000 件以上の情報が通知され、視認性の低下を招くおそれがあります。

コンフィグレーションファイル（jdn_manager_config.conf）を設定するには：

1. コンフィグレーションファイルの設定を変更します。

   コンフィグレーションファイル（jdn_manager_config.conf）の格納先は次のとおりです。

   JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥conf

コンフィグレーションファイルで設定する定義を次の表に示します。

プロパティ	説明	設定値	デフォルト
UNIX_Software_Manage	UNIX や Mac のソフトウェア情報を管理するかどうかの指定	• YES：管理する • NO：管理しない	NO

コンフィグレーションファイルの設定は、JP1/IT Desktop Management 2 のサービスの再起動後に適用されます。

他社ソフトウェア/パッチ情報※については、バージョンなど、ソフトウェア情報の一部の情報を拡張して取得できます。

注※　対象 OS は、マニュアル「JP1/IT Desktop Management 2 - Agent(UNIX(R)用)」のソフトウェア情報の取得についての説明を参照してください。

コンフィグレーションファイルで設定する定義を次の表に示します。

プロパティ	説明	設定値	デフォルト
Expand_LinuxSoftwareInformation	ソフトウェア情報の一部の情報を拡張して取得するかどうかの指定	• YES：取得する • NO：取得しない	NO

コンフィグレーションファイルの設定は、JP1/IT Desktop Management 2 のサービスの再起動後に適用されます。設定を変更する場合、事前にリモートインストールマネージャから Linux 機器のインストールパッケージ情報を削除してください。

設定を有効にした場合、ソフトウェア情報は次のように取得されます。

[ソフトウェア名]

ソフトウェア名の文字数が 50 文字から最大 255 文字に拡張されます。

[バージョン]

・バージョンの文字数が 6 文字から最大 128 文字に拡張されます。

・バージョンに大文字英数字以外が含まれる場合でも、省略することなく通知されます。

4.1.8　安全性が低いと判定されるパスワードをカスタマイズする

[OS のセキュリティ設定情報] － [アカウント情報] － [パスワードの安全性] 項目で安全性が低いと判定されるパスワードを、パスワード定義ファイル（jdng_security.xml）を使用することで変更できます。

(1)　新規インストールするエージェントに対して適用する場合

「(3)　jdng_security.xml の設定内容」に示す内容を入力したパスワード定義ファイル（jdng_security.xml）をテキストエディタで作成します。

設定画面の [エージェント] － [Windows エージェント設定とインストールセットの作成] 画面から、パスワード定義ファイルを適用したいエージェント設定名の行にある [インストールセットを作成] ボタンをクリックします。

表示される [インストールセットの作成] ダイアログの [インストールセット設定項目] － [展開するファイルの設定] の [追加] ボタンをクリックして、次の情報を指定してください。

展開するファイル：jdng_security.xml

展開先フォルダ：「%ITDM2AGT%¥conf」をプルダウンから選択して指定ください。

(2)　既存環境に対して適用する場合

エージェント管理の場合：

「(3)　jdng_security.xml の設定内容」に示す内容を入力したパスワード定義ファイル（jdng_security.xml）をテキストエディタで作成し、*JP1/IT Desktop Management 2 - Agent のインストールフォルダ*¥jp1itdma¥conf フォルダに格納します。

エージェントレス管理の場合：

「jdng_security.xml の設定内容」に示す内容を入力したパスワード定義ファイル（jdng_security.xml）をテキストエディタで作成し、*JP1/IT Desktop Management 2 - Manager のインストールフォルダ*¥bin¥miniagent フォルダに格納します。

なお、探索済みのエージェントレス端末には適用されないため、探索実施前に定義ファイルを格納してください。

(3)　jdng_security.xml の設定内容

jdng_security.xml は XML の形式です。エージェントをインストール後の XML ファイルの内容は、次に示す内容になっています。

```
<?xml version="1.0" encoding="UTF-8"?>
<Security CreationDate="2009-04-03T00:00:00.000Z">
<PasswordCheck>
<NoPassword>1</NoPassword>
<UserAccount>15</UserAccount>
<ComputerName>7</ComputerName>
<Password>password</Password>
<Password>PASSWORD</Password>
<Password>Password</Password>
<Password>admin</Password>
<Password>ADMIN</Password>
<Password>Admin</Password>
<Password>administrator</Password>
<Password>ADMINISTRATOR</Password>
<Password>Administrator</Password>
</PasswordCheck>
</Security>
```

<Security>/<PasswordCheck>下のエレメント値を編集することで、安全性が低い判定とされるパスワードを変更できます。

エレメント	説明	設定値	デフォルト
NoPassword	空白のパスワードをチェックするかどうか設定します。	0：空白のパスワードをチェックしない	1

エレメント	説明	設定値	デフォルト
NoPassword	0 または 1 以外を指定した場合は、「空白のパスワードをチェックする」として動作します。	1：空白のパスワードをチェックする	1
UserAccount	パスワードにユーザーアカウント名が使用されているかどうかのチェック方法を設定します。 チェックしたい項目の値を足した合計値を 1～15 で指定します。 負の値、空白、範囲を超えた数値を指定した場合は、「すべての組み合わせをチェックする」として動作します。	0：チェックしない 1：すべて小文字の場合をチェックする 2：すべて大文字の場合をチェックする 4：先頭だけ大文字の場合をチェックする 8：ユーザーアカウントと完全一致の場合をチェックする	15
ComputerName	パスワードにコンピュータ名が使用されているかどうかのチェック方法を設定します。 チェックしたい項目の値を足した合計値を 1～7 で指定します。 負の値、空白、範囲を超えた数値を指定した場合は、「すべての組み合わせをチェックする」として動作します。	0：チェックしない 1：すべて小文字の場合をチェックする 2：すべて大文字の場合をチェックする 4：先頭だけ大文字の場合をチェックする	7
Password	特定のキーワードがパスワードに使用されているかどうかをチェックする場合に、チェックするキーワードを指定します。	任意のパスワード	password PASSWORD admin ADMIN Admin administrator ADMINISTRATOR Administrator

パスワードをチェックしない場合の設定例を次に示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<Security CreationDate="2009-04-03T00:00:00.000Z">
<PasswordCheck>
<NoPassword>0</NoPassword>
<UserAccount>0</UserAccount>
<ComputerName>0</ComputerName>
</PasswordCheck>
</Security>
```

4.2　エージェントレス構成システムの構築時の設定

4.2.1　エージェントレスの機器の情報を定期的に更新する手順

エージェントを導入していない（エージェントレスの）機器から定期的に情報を収集して更新するかどうか、また、更新する頻度を設定できます。

エージェントレスの機器の情報を定期的に更新するには：

1. 設定画面を表示します。
2. メニューエリアで［エージェント］－［エージェントレス管理の設定］を選択します。
3. インフォメーションエリアで、［定期的に更新する］にチェックします。
4. ［更新間隔］に、何時間ごとに更新するかを設定します。

> **ヒント**
>
> 情報を効率良く収集・更新するためには、エージェントレスの機器 1,000 台ごとに 1 時間の間隔を設定してください。例えば、エージェントレスの機器が 800 台ある場合は、1 時間ごとに更新されるように設定します。

5. ［適用］ボタンをクリックします。

設定した更新頻度で、エージェントレスの機器から情報が収集されて更新されます。

［定期的に更新する］のチェックを外すと、エージェントレスの機器から情報が収集されなくなります。

> **ヒント**
>
> JP1/IT Desktop Management 2 では、より安全なセキュリティ管理をするため、管理対象のコンピュータにエージェントを導入することをお勧めしています。

> **ヒント**
>
> ［エージェントレス管理の設定］画面で設定する定期更新では、前回のネットワーク探索で成功した認証情報を元に認証を行います。認証情報の設定を変更しただけでは、前回のネットワーク探索で成功した認証情報は更新されません。この場合、［ネットワークの探索］画面から探索を実行し、認証を成功させることで、認証情報が更新されます。なお、［最新の情報を取得する］を実行した場合は、認証をやり直すため、新しい認証情報を使用しますが、認証が成功しても、前回のネットワーク探索で成功した認証情報は更新されません。

4.3　サポートサービス連携構成システムの構築時の設定

4.3.1　サポートサービスと接続するための情報を設定する手順

Windows の更新プログラムが最新かどうかを判定する場合や、最新のウィルス対策製品をセキュリティポリシーの判定項目にする場合、最新の更新プログラムやウィルス対策製品の情報をサポートサービスサイトから定期的にダウンロードする必要があります。このために、サポートサービスサイトと接続するための情報を設定しておく必要があります。

サポートサービスサイトに接続すると、更新プログラムの情報とウィルス対策製品の情報が自動的に最新の情報に更新されるようになります。

サポートサービスサイトから最新の情報を取得すると、管理対象のコンピュータに最新の更新プログラムやウィルス対策製品が適用されているかどうかを、セキュリティポリシーで判定できるようになります。

重要

サポートサービスサイトと接続するためには、サポートサービス契約をしている必要があります。

サポートサービスと接続するための情報を設定するには：

1. 設定画面を表示します。
2. メニューエリアで［他システムとの接続］－［サポートサービスの設定］を選択します。
3. インフォメーションエリアで、接続するサポートサービスの情報を設定します。

   接続するサポートサービスの情報については、リリースノートを確認してください。［接続テスト］ボタンをクリックすると、設定したサポートサービスに接続できるかどうかを確認できます。

   ［更新スケジュールの編集］で、サポートサービスサイトから最新の更新プログラム情報およびウィルス対策製品情報を取得するスケジュールを設定できます。

   また、［更新プログラム一覧の更新通知先］で、セキュリティ画面の更新プログラム一覧が更新されたことをメール通知する宛先も設定できます。
4. ［適用］ボタンをクリックします。

［更新スケジュールの編集］で設定したスケジュールに従って、サポートサービスサイトから最新のサポート情報がダウンロードされます。また、ダウンロードされた結果、更新プログラム一覧が更新された場合は、設定した宛先にメール通知されます。

ヒント

管理用サーバが外部のネットワークに接続できない場合は、外部に接続できるコンピュータを利用してサポートサービスサイトからサポート情報をダウンロードしてください。ダウンロー

ドしたサポート情報は、[サポートサービスからの情報のオフライン更新] ダイアログ、または updatesupportinfo コマンドで管理用サーバに登録できます。

ヒント

サポートサービスサイトから情報を取得してセキュリティポリシーが更新されると、更新のタイミングで機器のセキュリティ状況が判定されます。

関連リンク

- 8.3 updatesupportinfo（サポートサービスからの情報の登録）

4.4 Active Directory 連携構成システムの構築時の設定

4.4.1 Active Directory と接続するための情報を設定する手順

Active Directory に登録されている機器を JP1/IT Desktop Management 2 の管理対象にしたり、組織階層の情報を取り込んだりするためには、探索対象の Active Directory のドメイン情報を設定する必要があります。

Active Directory と接続するための情報を設定するには：

1. 設定画面を表示します。
2. メニューエリアで［他システムとの接続］－［Active Directory の設定］を選択します。
3. Active Directory から組織階層の情報を取得したい場合は、インフォメーションエリアの［Active Directory の組織の情報を取得して、部署の情報に反映する］にチェックします。
4. 接続する Active Directory の情報を設定します。
   Active Directory の情報を複数設定する場合は、［追加］ボタンをクリックして情報を追加します。
5. ［接続テスト］ボタンをクリックして、設定した Active Directory に接続できるかどうかを確認します。
6. 接続に問題がないことを確認できたら、［適用］ボタンをクリックします。

Active Directory の探索を開始すると、ここで設定した Active Directory の情報が収集されます。

Active Directory の探索と同時にエージェントを配信する場合は、この画面で設定した認証情報が利用されます。

関連リンク

- 4.4.4 探索条件を設定する手順（Active Directory の探索）

4.4.2 追加管理項目として Active Directory から取得する情報を設定する手順

Active Directory で管理されている各機器の詳細情報を、追加管理項目として取得できます。Active Directory で管理されている情報を追加管理項目として取得するには、追加管理項目の入力方法に［Active Directory から取得］を指定します。取得対象となる Active Directory の管理項目も設定します。

追加管理項目として Active Directory から取得する情報を設定するには：

1. 設定画面を表示します。

2. ［資産管理］ − ［資産管理項目の設定］を選択します。

3. Active Directory から情報を取得する項目を作成または編集します。

［資産管理項目の設定］画面で、項目を新規作成する場合は［項目を追加］ボタンをクリックします。項目を編集する場合は、項目を選択して［編集］ボタンをクリックします。

4. 表示されるダイアログで［入力方法］を［Active Directory から取得］に設定します。

［管理項目の追加］および［管理項目の編集］ダイアログで、［入力方法］のプルダウンメニューから［Active Directory から取得］を選択します。

> **重要**
>
> 追加する項目、または編集する項目が Active Directory から取得できない項目は、［入力方法］を［Active Directory から取得］に設定できません。

5. 取得対象となる Active Directory の管理項目を設定します。

Active Directory から取得する項目名、説明、データ型、取得内容、取得対象、および属性名を設定します。その後、［OK］ボタンをクリックします。

このように設定することで、Active Directory で管理されている情報が、各機器の追加管理項目として取得されるようになります。

4.4.3 Active Directory に登録されている機器を探索する手順

機器を探索する方法の一つです。Active Directory に登録されている機器を探索できます。

設定画面の［他システムとの接続］ − ［Active Directory の設定］画面で、探索する Active Directory のドメイン情報を設定したあと、設定画面の［機器の探索］ − ［探索条件の設定］ − ［Active Directory の探索］画面で探索スケジュールなどを設定します。［探索を開始］ボタンをクリックすると、設定したスケジュールに従って探索が開始されます。

Active Directory に登録されている機器を探索するには：

1. 設定画面の［他システムとの接続］ − ［Active Directory の設定］画面を表示します。

2. 接続する Active Directory のドメイン情報を設定します。

［接続テスト］ボタンをクリックすると、設定した Active Directory に接続できるかどうかを確認できます。

> **重要**
>
> 複数サーバ構成の場合、異なる管理用サーバに同じ Active Directory のドメイン情報を設定しないでください。それぞれの管理用サーバが機器を発見したタイミングで、機器情報の

管理元が意図しないで変更されるため、機器情報を正常に管理できなくなるおそれがあります。

3. 設定画面の［機器の探索］－［探索条件の設定］－［Active Directory の探索］画面を表示します。
4. ［探索スケジュール］で探索スケジュールを設定します。
5. ［発見した機器への操作］で、発見した機器を自動的に管理対象にするかどうか、エージェントを自動配信するかどうかを設定します。
6. 探索の完了を管理者にメールで通知したい場合は、［完了通知］で通知先を設定します。
7. 画面右上の［探索を開始］ボタンをクリックします。

設定画面の［機器の探索］－［探索履歴の確認］－［Active Directory の探索］画面に移動し、設定した探索スケジュールに従って探索が実行されます。

関連リンク

- 4.4.4　探索条件を設定する手順（Active Directory の探索）
- 1.7.3　機器の探索状況の確認

4.4.4　探索条件を設定する手順（Active Directory の探索）

Active Directory に登録されている機器を探索する場合の探索条件を設定できます。

探索条件を設定するには：

1. 設定画面を表示します。
2. メニューエリアで［機器の探索］－［探索条件の設定］－［Active Directory の探索］を選択します。
3. ［探索スケジュール］を編集します。
   スケジュールを決めて定期的に探索を実行する場合に、スケジュールを設定してください。
4. ［発見した機器への操作］を編集します。
   機器の探索時に新しい機器が発見された場合の操作を設定してください。
5. ［完了通知］を編集します。
   機器の探索が完了したら JP1/IT Desktop Management 2 の管理者にメールで通知する場合に、通知先を設定してください。
   JP1/IT Desktop Management 2 が利用するメールサーバ（SMTP サーバ）の情報を設定していない場合は、［メールサーバの設定へ］のリンクをクリックして表示される画面で、メールサーバの情報を設定してください。

重要

接続する Active Directory のドメインを設定していないと探索は実行できません。[Active Directory の設定] 画面で、Active Directory のドメインを設定してください。

探索条件の設定が完了します。

設定した探索条件で探索を即時実行する場合は、[探索を開始] ボタンをクリックしてください。即時実行しない場合は、[探索スケジュール] に従って実行されます。

探索の実行状況と実行結果は、設定画面の [探索履歴の確認] − [Active Directory の探索] 画面で確認できます。

関連リンク

- 1.7.3 機器の探索状況の確認

4.4.5 機器を管理対象にする手順

探索で発見された機器や除外対象の機器のうち、管理する機器は、管理対象にします。

機器を管理対象にすることで、機器情報を収集したり、セキュリティ状況を把握したりできるようになります。

機器を管理対象にするには：

1. 設定画面を表示します。
2. メニューエリアで [機器の探索] − [発見した機器] を選択します。
3. 管理対象にする機器を選択します。
4. [管理対象にする] ボタンをクリックします。

機器が管理対象になります。

管理対象の機器は、機器画面で収集された機器情報を確認できます。

ヒント

ネットワークモニタ機能が導入されている場合、機器が発見された時点では、ネットワークモニタ設定やネットワーク制御リストの設定に基づいて、機器のネットワーク接続が制御されます。機器を管理対象に設定すると、自動的にネットワーク接続が許可されます。

重要

機器を管理対象にすると、1 台につきライセンスを 1 つ使用します。ライセンスが不足している場合は、機器を管理対象にできません。この場合、ライセンスを購入して追加する必要があります。

4.5 MDM 連携構成システムの構築時の設定

4.5.1 MDM システムと連携するための情報を設定する手順

MDM システムからスマートデバイスの情報を取得して JP1/IT Desktop Management 2 で管理するためには、MDM システムとの接続情報や情報の取得スケジュールなどを設定する必要があります。

重要

MDM 連携の設定は、1 台の MDM サーバにつき 1 つとしてください。1 台の MDM サーバに対して複数の設定があると、JP1/IT Desktop Management 2 からスマートデバイスを制御できないことがあります。

JP1/IT Desktop Management 2 - Smart Device Manager と連携するための情報を設定するには：

1. JP1/IT Desktop Management 2 の設定画面を表示します。
2. メニューエリアで［他システムとの接続］－［MDM 連携の設定］を選択します。
3. インフォメーションエリアの［MDM 連携の設定］で、［追加］ボタンをクリックします。
4. 表示されるダイアログで、次のように設定します。

MDM システム

「JP1/ITDM2 - SD Manager」を選択します。

MDM サーバのホスト名およびポート番号

JP1/IT Desktop Management 2 - Smart Device Manager のスマートデバイスマネージャーをインストールしたマシンのホスト名を設定します。IP アドレスは指定しないでください。ポート番号には、JP1/IT Desktop Management 2 との連携用(SSL 通信用) のポート番号を指定してください。デフォルトのポート番号は、26055 です。

URL

次の形式で URL を設定します。

`http://`*`ホスト名`*`:`*`ポート番号`*`/jp1itdm2sdm/jp1itdm2sdm-login.htm`

*ホスト名*には、JP1/IT Desktop Management 2 - Smart Device Manager のスマートデバイスマネージャーをインストールしたマシンのホスト名を設定してください。*ポート番号*には、JP1/IT Desktop Management 2 - Smart Device Manager の 管理画面用ポート番号を指定してください。デフォルトのポート番号は 26080 です。

例：`http://SDMServer:26080/jp1itdm2sdm/jp1itdm2sdm-login.htm`

ユーザー ID およびパスワード

JP1/IT Desktop Management 2 - Smart Device Manager の管理画面で作成したユーザーアカウントおよびパスワードを設定します。ユーザー ID は、次のフォーマットに従ってください。

ユーザー ID：JP1MDM*YYYXX*@server01.jp1mdm.hitachi.jp

YYY:001～999 の数値、*XX*:01～05 の数値

権限：システム管理者権限

5. [接続テスト] ボタンをクリックして、JP1/IT Desktop Management 2 - Smart Device Manager に接続できるかどうかを確認します。

6. [取得スケジュール] を編集します。

スケジュールを決めて定期的にスマートデバイスの情報を更新する場合に、スケジュールを設定してください。

7. [OK] ボタンをクリックします。

8. インフォメーションエリアの［発見した機器への操作］で、［編集］ボタンをクリックします。

9. 表示されるダイアログで、発見されたスマートデバイスを自動的に管理対象にするかどうかを設定します。

MDM システムと連携するための情報を設定するには：

MDM システムとして Microsoft Intune を使用する場合には、#1～#3 の手順は不要です。代わりに、下記の「MDM システムとして Microsoft Intune を使用する場合の追加設定」にあるルート CA 証明書の Java キーストアへの登録の手順を実施してください。

1. MDM 製品のルート証明書を入手します。

1. Web ブラウザで MDM 製品のポータル画面にアクセスします。
2. ルート証明書をファイルにエクスポートします。

Internet Explorer の場合

(i)画面上で右クリックして［プロパティ］－［証明書］－［詳細］－［ファイルにコピー］を選択します。

(ii)証明書のエクスポートウィザードで、証明書を「DER encoded binary X.509」形式でエクスポートします。

Firefox の場合

(i)画面上で右クリックして［ページの情報を表示］－［セキュリティ］－［証明書を表示］－［詳細］－［エクスポート］を選択します。

(ii)証明書の保存ダイアログで、証明書を「X.509 証明書(DER)」形式で保存します。

2. 手順 1.で入手したルート証明書を管理用サーバにコピーします。

3. ルート証明書を管理用サーバにインポートします。

管理用サーバのコマンドプロンプトで次のコマンドを実行してください。

JP1/IT Desktop Management 2 - Manager のインストール先フォルダ¥mgr¥uCPSB¥jdk¥jre¥bin¥keytool.exe -import -keystore *JP1/IT Desktop Management 2 -*

Manager のインストール先フォルダ¥mgr¥uCPSB¥jdk¥jre¥lib¥security¥cacerts -file *ルート証明書のパス* -alias *ルート証明書の別名*※

注※　ルート証明書のパスとは、手順 2.でコピーしたルート証明書のパスです。ルート証明書の別名とは、インポートするルート証明書の別名称のことで、任意の名前を設定できます。

コマンドを実行するとルート証明書をインポートするためのパスワードを要求されます。パスワードを入力してください。デフォルトのパスワードは「changeit」です。

4. JP1/IT Desktop Management 2 の設定画面を表示します。
5. メニューエリアで［他システムとの接続］－［MDM 連携の設定］を選択します。
6. インフォメーションエリアの［MDM 連携の設定］で、［追加］ボタンをクリックします。
7. 表示されるダイアログで、接続する MDM システムの情報を設定します。
8. ［接続テスト］ボタンをクリックして、設定した MDM システムに接続できるかどうかを確認します。
9. ［取得スケジュール］を編集します。

   スケジュールを決めて定期的にスマートデバイスの情報を更新する場合に、スケジュールを設定してください。
10. ［OK］ボタンをクリックします。
11. インフォメーションエリアの［発見した機器への操作］で、［編集］ボタンをクリックします。
12. 表示されるダイアログで、発見されたスマートデバイスを自動的に管理対象にするかどうかを設定します。

［MDM 連携の設定］で設定したスケジュールに従って、MDM システムからスマートデバイスの情報が取得されます。

なお、MobileIron と連携する場合、［MDM 連携の設定］で指定したユーザー ID に対して、MobileIron で「API」権限を割り当てる必要があります。

MDM システムとして Microsoft Intune を使用する場合の追加設定：

Microsoft Intune と連携する場合、次のルート CA 証明書を JP1/IT Desktop Management 2 - Manager がインストールされた PC の Java キーストアに登録する必要があります。Java キーストアに登録後、JP1/IT Desktop Management 2 のサービスを再起動してください。

- DigiCert Global Root CA

Java キーストアにこのルート CA 証明書が登録されていない場合は、DigiCert 社の Web サイトからルート CA 証明書ファイルをダウンロードして、次のコマンドをコマンドプロンプトで実行してください。

JP1/IT Desktop Management 2 - Manager のインストールフォルダ
¥mgr¥uCPSB¥jdk¥jre¥bin¥keytool.exe -import -file *DigiCertGlobalRootCA.crt のパス* -alias

DigiCertGlobalRootCA -keystore *JP1/IT Desktop Management 2 - Manager のインストールフォルダ*¥mgr¥uCPSB¥jdk¥jre¥lib¥security¥cacerts

コマンドを実行するとルート証明書をインポートするためのパスワードを要求されます。パスワードを入力してください。デフォルトのパスワードは「changeit」です。

また、Microsoft Entra ID で、JP1/IT Desktop Management 2 - Manager が Microsoft Intune と通信するためのアプリの登録をしてください。次に示す項目を設定します。記載のない設定項目は初期値のままで構いません。登録したアプリのアプリケーション（クライアント）ID、ディレクトリ（テナント）ID を MDM サーバ情報に設定します。

認証－パブリック クライアント フローを許可する

はい

証明書とシークレット

「証明書」または「クライアントシークレット」のどちらかを選択

「証明書」の場合には、証明機関から取得したクライアント証明書の公開キーの証明書ファイルを Microsoft Entra ID にアップロードし、秘密キーの証明書ファイルを管理用サーバの下記のフォルダに格納します。ファイル名は IntuneCert.pem とします。

JP1/IT Desktop Management 2 - Manager のインストールフォルダ¥mgr¥temp

マルチテナント管理用サーバの場合：

JP1/IT Desktop Management 2 - Manager のインストールフォルダ¥mgr¥tenant¥テナント名¥mgr¥temp

「シークレット」の場合には、生成されたクライアントシークレット値を MDM サーバ情報に設定します。

API のアクセス許可

アクセスを許可する API として「Microsoft Graph」を指定してください。

また、次の項目を設定してください。

アプリケーションに必要なアクセス許可の種類

アプリケーションの許可

アクセス許可の名前

- DeviceManagement-ManagedDevices.Read.All
- DeviceManagement-ManagedDevices.PrivilegedOperations.All

MDM システムとして Google Workspace を使用する場合の追加設定：

Google Workspace と連携する場合、次のルート CA 証明書を JP1/IT Desktop Management 2 - Manager がインストールされた PC の Java キーストアに登録する必要があります。Java キーストアに登録後、JP1/IT Desktop Management 2 のサービスを再起動してください。

- DigiCert Global Root CA

Java キーストアにこのルート CA 証明書が登録されていない場合は、DigiCert 社の Web サイトからルート CA 証明書ファイルをダウンロードして、次のコマンドをコマンドプロンプトで実行してください。

JP1/IT Desktop Management 2 - Manager のインストールフォルダ¥mgr¥uCPSB¥jdk¥jre¥bin¥keytool.exe -import -file *DigiCertGlobalRootCA.crt のパス* -alias DigiCertGlobalRootCA -keystore *JP1/IT Desktop Management 2 - Manager のインストールフォルダ*¥mgr¥uCPSB¥jdk¥jre¥lib¥security¥cacerts

コマンドを実行するとルート証明書をインポートするためのパスワードを要求されます。パスワードを入力してください。デフォルトのパスワードは「changeit」です。

そして、次に示す手順で設定してください。

1. Google Workspace でドメインの所有権の証明が完了しているかを確認します。 ドメインの所有権の証明ができていない場合、Google Workspace で手続きを実施してください。

2. 次のルート CA 証明書を JP1/IT Desktop Management 2 - Manager がインストールされた PC の Java キーストアに登録します。Java キーストアに登録後、JP1/IT Desktop Management 2 のサービスを再起動してください。

   - GTS Root R1

     Java キーストアにこのルート CA 証明書が登録されていない場合は、次のルート CA 証明書ファイルをダウンロードします。

     ダウンロードサイト

     Google Trust Services

     `https://pki.goog/repository/`

     証明機関

     GTS Root R1

     証明書の種類

     Certificate (DER)

     ファイル名：r1.crt

     次のコマンドをコマンドプロンプトで実行してください。

     JP1/IT Desktop Management 2 - Manager のインストールフォルダ¥mgr¥uCPSB¥jdk¥jre¥bin¥keytool.exe -import -file *r1.crt のパス* -alias GTSRootR1 -keystore *JP1/IT Desktop Management 2 - Manager のインストールフォルダ*¥mgr¥uCPSB¥jdk¥jre¥lib¥security¥cacerts

     コマンドを実行するとルート証明書をインポートするためのパスワードが要求されます。パスワードを入力してください。デフォルトのパスワードは「changeit」です。

3. Google Workspace で次の設定をします。

   - Google Cloud プロジェクトの作成および API の有効化
   - Admin SDK API の有効化

- OAuth 同意画面の設定
- 秘密鍵ファイルを作成可能とするように組織ポリシーを変更
- サービスアカウントの作成、キーの作成、および秘密鍵ファイルの取得
- ドメイン全体の権限をサービスアカウントに委任

Google Workspace の設定項目および設定値を次の表に示します。

機能	設定項目	設定値	デフォルト
Google Cloud プロジェクトの作成	プロジェクト名	任意の値を入力	−
	組織	任意の組織を選択	組織なし
	場所	任意の場所を選択	−
Admin SDK API の有効化	Admin SDK API 有効にする	［有効にする］をクリック	−
OAuth 同意画面の設定	ユーザーの種類	「外部」を選択	−
	アプリ名	任意の値を入力	−
	ユーザー サポート メール	任意の値を入力	−
	デベロッパーの連絡先情報	任意の値を入力	−
	機密性の高いスコープ	次の値を設定 https://www.googleapis.com/auth/admin.directory.device.chromeos.readonly	−
サービスアカウントの作成	サービス アカウント名	任意の値を入力	−
	サービス アカウント ID	任意の値を入力	−
	秘密鍵ファイル	秘密鍵の作成で「JSON 形式」を選択し、秘密鍵ファイルをダウンロード※	−
	ドメイン全体の委任を有効にする	設定不要	オン
ドメイン全体の権限をサービスアカウントに委任	クライアント ID	サービス アカウントの秘密鍵で取得したクライアント ID を入力	−
	OAuth スコープ	次の値を設定 https://www.googleapis.com/auth/admin.directory.device.chromeos.readonly	−

（凡例）−：該当なし

注※　ダウンロードした秘密鍵ファイルは、［MDM サーバ情報（GWS 連携）の追加］画面または［MDM サーバ情報（GWS 連携）の編集］画面の［秘密鍵ファイル］に指定します。

重要

サービスアカウントキーの作成は、組織のポリシーでデフォルトでは作成が無効化されています。このため、次の手順で組織ポリシーを変更して、サービスアカウントキーの作成を有効にしてください。

1. 特権管理者ロールを割り当てた Google Workspace ユーザーで、Google Cloud にログインし、次の表に示す内容で秘密鍵ファイルを作成するユーザーに組織のポリシーを管理するためのロールを割り当てる。

機能	項目	設定内容
リソースを選択	名前	作成した Google Cloud プロジェクト名
[IAM と管理] − [IAM] − [アクセス許可]	プリンシパル	秘密鍵ファイルを作成する Google Cloud ユーザー
権限の編集	ロール	次のロールを割り当て • 組織の管理者 • 組織ポリシー管理者

2. 手順 1 でロールを割り当てたユーザーで Google Cloud にログインし、次の表に示す内容で組織のポリシーを設定する。

機能	項目	設定内容
リソースを選択	名前	ドメインと同じ名前の組織タイプのプロジェクト
[IAM と管理] − [IAM] − [組織のポリシー]	ポリシー名	constraints/iam.disableServiceAccountKeyCreation
	ポリシーのソース	親のポリシーをオーバーライドする
	ルール	オフ

なお、ポリシーが適用されるまで 15 分程度の時間がかかることがあります。サービスアカウントの秘密鍵ファイルが作成できない場合は、時間をおいてから秘密鍵ファイルの作成を再実行してください。

重要

JP1/IT Desktop Management 2 - Manager 11-01 から JP1/IT Desktop Management 2 - Manager 12-50 以降にバージョンアップインストールを行う場合、JP1/IT Desktop Management 2 - Manager 12-50 以降にバージョンアップ後ルート証明書の再インポートを実施してください。

ヒント

発見されたスマートデバイスは、［発見した機器への操作］の設定に従って管理対象になります。発見された機器を自動的に管理対象にする設定にしていない場合、スマートデバイスを管理するためには、設定画面の［発見した機器］画面で、スマートデバイスを管理対象にする必要があります。

ヒント

MDM システムから取得したルート証明書を、管理用サーバにインポートしたあとで変更する場合は、変更後のルート証明書を再取得し、管理用サーバに再インポートする必要があります。

関連リンク

- 1.7.5　発見した機器を確認する手順
- 1.7.6　管理対象の機器を確認する手順

4.6　ネットワーク監視構成システムの構築時の設定

4.6.1　ネットワーク制御リストの機器を編集する手順

設定画面の［ネットワーク制御リストの設定］画面のネットワーク制御リストに登録されている機器の設定を編集できます。

ネットワーク制御リストの機器を編集するには：

1. 設定画面を表示します。
2. メニューエリアで［ネットワーク制御］－［ネットワーク制御リストの設定］を選択します。
3. インフォメーションエリアで、編集したい機器を選択して［編集］ボタンをクリックします。
   編集したい機器を複数選択することもできます。
4. 表示される［ネットワーク接続可否の編集］ダイアログで情報を編集して、［OK］ボタンをクリックします。
   判定形式、ネットワークの接続の許可などの設定ができます。MAC アドレスは編集できません。
   編集する機器を複数選択している場合は、［ネットワーク接続可否の編集］ダイアログ内の編集したい項目をチェックすることで編集できます。この場合、ホスト名、MAC アドレス、および IP アドレスは編集できません。

選択した機器のネットワーク制御の設定が更新されます。

ネットワーク制御の詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の、機器のネットワーク接続の管理についての説明を参照してください。

4.6.2　ネットワーク制御リストの自動更新の設定を編集する手順

設定画面の［ネットワーク制御リストの設定］画面で、ネットワーク制御リストの自動更新の設定を編集できます。

ネットワーク制御リストの自動更新の設定を編集するには：

1. 設定画面を表示します。
2. メニューエリアで［ネットワーク制御］－［ネットワーク制御リストの設定］を選択します。
3. インフォメーションエリアで、［ネットワーク制御リストの自動更新］の［編集］ボタンをクリックします。
4. 表示されるダイアログで、ネットワーク制御リストの自動更新について設定します。

5. [OK] ボタンをクリックします。

   手順 6.～手順 8.は、統括管理用サーバで複数サーバ構成全体のネットワーク接続を管理する場合に、統括管理用サーバだけで実施します。

6. インフォメーションエリアで、[ネットワーク制御リストの自動更新の対象範囲] の [編集] ボタンをクリックします。

7. 表示されるダイアログで、自動更新の対象範囲について設定します。

8. [OK] ボタンをクリックします。

ネットワーク制御リストの自動更新の設定が更新されます。

4.6.3 ネットワークモニタ設定を追加する手順

設定画面の［ネットワーク制御の設定］画面の一覧に、ネットワークモニタ設定を追加できます。ネットワークモニタ設定を追加すると、ネットワークセグメントごとに新規に発見された機器のネットワーク接続を許可するかどうかを設定できるようになります。

ネットワークモニタ設定を追加するには：

1. 設定画面を表示します。

2. メニューエリアで［ネットワーク制御］ − ［ネットワーク制御の設定］を選択します。

3. インフォメーションエリアで［ネットワークモニタ設定］の［追加］ボタンをクリックします。

4. 表示されるダイアログでネットワークモニタ設定名と、発見した機器への動作を設定して、[OK] ボタンをクリックします。

ネットワークモニタ設定が追加され、［ネットワークモニタ設定］の一覧に表示されます。

なお、ネットワークモニタ設定を追加しただけでは、ネットワークを制御できません。このあと、ネットワークモニタ設定の割り当てを実施してください。

> **ヒント**
>
> 手順 4 で表示されるダイアログの［機器の検知のみ行い、ネットワークへの接続を遮断しない］をチェックすると、遮断対象となる機器がネットワークに接続されるとイベントが発行され、ネットワークの探索が実行されます。

4.6.4　ネットワークモニタ設定の割り当てを変更する手順

設定画面の［ネットワークモニタ設定の割り当て］画面から、ネットワークセグメントに割り当てられているネットワークモニタ設定を変更できます。

> **ヒント**
>
> ネットワークモニタが無効になっている場合、ネットワークモニタ設定の割り当てを変更できません。ネットワークモニタ設定の割り当てを変更する場合、先にネットワークモニタを有効にしてください。

ネットワークモニタ設定の割り当てを変更するには：

1. 設定画面を表示します。
2. メニューエリアで［ネットワーク制御］－［ネットワークモニタ設定の割り当て］を選択します。
3. インフォメーションエリアの上部で、ネットワークモニタ設定の割り当てを変更するネットワークセグメントを選択して、［ネットワークモニタ設定を変更］ボタンをクリックします。
4. 表示されるダイアログで、割り当てるネットワークモニタ設定を選択して、［OK］ボタンをクリックします。

選択したネットワークセグメントに、ネットワークモニタ設定の割り当てが変更されます。

4.6.5　JP1/NETM/NM - Manager 連携の設定を有効にする手順

JP1/NETM/NM - Manager 連携を有効にすると、JP1/NETM/NM - Manager で管理しているネットワークセグメントを JP1/IT Desktop Management 2 でネットワーク接続制御できます。

JP1/NETM/NM - Manager 連携の設定を有効にするには：

1. 設定画面を表示します。
2. メニューエリアで［ネットワーク制御］－［ネットワーク制御の設定］を選択します。
3. インフォメーションエリアで、［JP1/NETM/NM - Manager 連携の設定］の［編集］ボタンをクリックします。
4. 表示されるダイアログで、［操作を続行する］が表示された場合、表示されたメッセージの内容を確認した上でチェックします。
5. ［JP1/NETM/NM - Manager と連携する］をチェックします。
6. ［OK］ボタンをクリックします。

JP1/NETM/NM - Manager 連携の設定が有効になります。

4.6.6　ネットワーク制御設定ファイルを編集する手順

JP1/NETM/NM - Manager と連携している場合で、ホワイトリスト方式でネットワーク接続を管理するときは、ネットワーク制御設定ファイル（jdn_networkcontrol.conf）を編集する必要があります。ネットワーク制御設定ファイルを編集すると、発見された機器がネットワーク接続を「許可しない」設定でネットワーク制御リストに登録されるようにできます。

ネットワーク制御設定ファイルの設定は、ネットワークモニタで監視しているネットワークセグメントを除いた、JP1/IT Desktop Management 2 で管理しているすべてのネットワークセグメントに適用されます。すでにネットワーク制御リストに登録されている機器のネットワーク接続設定には適用されません。

クラスタ構成で運用している場合は、管理用サーバの現用系サーバと管理用サーバの待機系サーバでネットワーク制御設定ファイルを編集してください。

ネットワーク制御設定ファイルを編集するには：

1. 管理用サーバでstopservice コマンドを実行します。
   管理用サーバのサービスが停止します。

2. ネットワーク制御設定ファイルで「NetworkControl_Default」の指定値を「1」に編集します。
   ネットワーク制御設定ファイルの格納先は次のとおりです。
   JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥conf
   ネットワーク制御設定ファイルで設定する定義を次の表に示します。

プロパティ	説明	指定値	デフォルト
NetworkControl_Default	発見された機器がネットワーク制御リストに登録されるときのネットワーク接続設定を指定します。	• 0：許可する • 1：許可しない	0

3. 管理用サーバでstartservice コマンドを実行します。
   管理用サーバのサービスが開始します。

ネットワーク制御設定ファイルの編集が完了します。

ネットワーク制御設定ファイルでネットワーク接続を「許可しない」に設定する例を次に示します。

```
[NetworkControl]
NetworkControl_Default=1
```

ヒント

ホワイトリスト方式からブラックリスト方式に運用を変更する場合は、ネットワーク制御設定ファイルでネットワーク接続を「許可する」設定に編集してください。

4.6.7 ネットワークモニタを有効にしたコンピュータをネットワーク制御用アプライアンスにリプレースする手順

ネットワークモニタを有効にしたコンピュータをネットワーク制御用アプライアンスにリプレースするには、コンピュータのネットワークモニタを無効にしてから、ネットワーク制御用アプライアンスを導入します。JP1/NETM/NM - Manager がインストール済を前提とした手順を次に示します。

JP1/NETM/NM - Manager を設定する手順は、マニュアル「JP1 Version 9 JP1/NETM/Network Monitor」またはマニュアル「JP1 Version 10 JP1/NETM/Network Monitor」の操作方法の説明を参照してください。

1. ネットワークモニタを有効にしたコンピュータのネットワークモニタを無効にします。
2. ネットワーク制御用アプライアンスを監視対象のネットワークセグメントに配置し、セットアップします。
3. JP1/NETM/NM - Manager で監視対象のネットワークセグメントとグループを登録します。
4. JP1/NETM/NM - Manager でネットワーク制御用アプライアンスの環境設定を実施します。

4.7 JP1/IM 連携構成システムの構築時の設定

4.7.1 JP1/IM と連携するためのコンフィグレーションファイルを設定する手順

JP1/IT Desktop Management 2 の JP1/IM と連携するための機能は、コンフィグレーションファイルの設定を変更することで有効になります。

コンフィグレーションファイル（jdn_manager_config.conf）を設定するには：

1. コンフィグレーションファイルに設定を追加します。

   コンフィグレーションファイル（jdn_manager_config.conf）の格納先は次のとおりです。

   JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥conf

コンフィグレーションファイルで設定する定義を次の表に示します。

プロパティ	説明	指定値	デフォルト
JP1IM_EventOption	JP1/IM と連携するかどうかを指定します。連携する場合、システムで発生したイベントを定期的に監視し、JP1/IM のイベントコンソールに出力する対象のイベントを JP1/Base に通知します。 定期監視の際に、このプロパティに「ON」が設定されていることを検知した日時を基準に 24 時間以内に発生したイベントのうち、JP1/IM のイベントコンソールに出力する対象のイベントが取得されます。	• ON：JP1/IM と連携する。 • OFF：JP1/IM と連携しない。	OFF

JP1/IM と連携する場合のコンフィグレーションファイルの設定例を次に示します。

```
#
# コンフィグレーションファイル
#
# サーバカスタマイズオプション
JP1IM_EventOption=ON
```

コンフィグレーションファイルの設定は、JP1/IT Desktop Management 2 のサービスの再起動後に適用されます。

なお、JP1/IM と連携しない設定にする場合は、コンフィグレーションファイルに追加した「JP1IM_EventOption=ON」の行を削除するか、「JP1IM_EventOption=OFF」に変更して、JP1/IT Desktop Management 2 のサービスを再起動してください。

4.8　30,000 台～50,000 台のコンピュータを管理する場合の設定

JP1/IT Desktop Management 2 11-10-02 以降を使用してください。

4.8.1　操作ログを取得する場合の設定手順

30,000 台～50,000 台のコンピュータを管理する場合は、操作ログを取得することができません。操作ログを管理する場合は、複数サーバ構成で運用してください。管理用中継サーバのセットアップでは、管理対象のコンピュータから収集した操作ログ情報を上位の管理用サーバに通知しない設定にしてください。

4.8.2　セキュリティ判定を実施する場合の設定手順

30,000 台～50,000 台のコンピュータを管理する場合は、セキュリティ判定の設定を変更してください。変更する手順は次のとおりです。

> **ヒント**
>
> セキュリティ判定の設定の変更が必要な管理用サーバは、直接管理しているエージェントが 1 台で 30,000 台を超えてセキュリティ判定を実施する管理用サーバです。

1. コンフィグレーションファイルに設定を追加します。
   コンフィグレーションファイル（jdn_manager_config.conf）の格納先は次のとおりです。
   JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥conf
   コンフィグレーションファイルに「Mgrsrv_jdnmssecurityctrl=10」の行を追加してください。
2. JP1/IT Desktop Management 2 のサービスを再起動します。

4.8.3　操作画面を 10 人～20 人で同時に操作する場合

> **ヒント**
>
> バージョン 12-10 までの、操作画面を 10 人～20 人で同時に操作する設定は不要になります。

操作画面を 10 人～20 人で同時に操作する場合は、次の項目について検討してください。

- 一覧画面の「1 ページ当たりの表示件数」を「100」に設定して使用してください。
- ホーム画面、各画面のダッシュボードに表示するポートレットを必要なものだけに変更してください。

5 製品の上書きインストールおよびコンポーネントのアップデート

ここでは、JP1/IT Desktop Management 2 - Manager の上書きインストール、およびコンポーネント（エージェント、中継システムおよびネットワークモニタエージェント）のアップデートについて説明します。

5.1 JP1/IT Desktop Management 2 - Manager を上書きインストールする手順

JP1/IT Desktop Management 2 - Manager の上書きインストールを実行するには、インストール対象のバージョンが、すでにインストールされているバージョン以上である必要があります。また、上書きインストール中は、ハードディスクに最低 2.5 ギガバイトの空き容量が必要です。

重要

上書きインストールする前に、JP1/IT Desktop Management 2 からログアウトして、操作画面を閉じてください。操作画面を表示したまま上書きインストールすると、インストール完了後に操作画面が正しく表示されない場合があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

重要

インストール前は、すべての Windows アプリケーションを終了させてください。誤って JP1/IT Desktop Management 2 - Manager のプログラムを起動したままインストールを実行した場合は、インストールの実行結果に関係なく OS を再起動してください。OS を再起動しても、サービスが起動しない場合や、JP1/IT Desktop Management 2 - Manager のプログラムが動作しない場合は、次に示す手順でインストールを再実行してください。

1. すべての Windows アプリケーションを終了させてください。
2. サービス（JP1_ITDM2_Service）を停止してください。
3. 上書きインストールを再実行してください。サービスが開始されます。

重要

次に該当する環境は、上書きインストールでのセットアップ（データベースのアップグレード）後に、データベースのバージョンアップが実行されます。

(a)Hitachi IT Operations Director から JP1/IT Desktop Management 2 12-50 以降に上書きインストール

(b)Hitachi IT Operations Director から JP1/IT Desktop Management 2 12-10 以前に上書きインストールした環境を JP1/IT Desktop Management 2 12-50 以降に上書きインストール※

注※　<JP1/IT Desktop Management 2 のインストールフォルダ>¥mgr¥db¥CLIENT¥UTL フォルダに PDC LTM64.dll ファイルが存在しない環境が該当します。

次に注意事項を示します。

- Hitachi IT Operations Director からの上書きインストールでは、操作ログデータベースは移行されません。
- 非クラスタ環境、またはクラスタ環境の現用系では、データベース退避フォルダには、データベースフォルダとデータフォルダのディスク占有量の合計値以上の空き容量を確保してください 。
- バージョンアップ後のデータベースに操作ログのデータを移行するには、数時間かかる場合があります。環境に依存しますが、1,000 機器・30 日分の操作ログの移行に 1 時間以上かかる場合があります。また、データベース退避フォルダには 、データベースフォルダとデータフォルダ、および操作ログのデータベースフォルダのディスク占有量の合計値以上の空き容量を確保してください。
- データベースのバージョンアップの処理は次の(1)～(8)の順に実行され、処理の進捗は次のメッセージで確認することができます。

  KDEX4490-I データベースのバージョンアップの進捗 処理=[処理], 進捗=[進捗を表す数値]/[進捗の全体（各処理毎）を表す数値]

  [処理]には次の値が表示されます。

  (1)Backup Data

  (2)Backup Data (Operation Log)

  (3)Uninstall Database

  (4)Install Database

  (5)Build Database

  (6)Restore Data

  (7)Restore Data (Operation Log)

  (8)Start Service

JP1/IT Desktop Management 2 - Manager を上書きインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。

2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Manager］を選択して、［インストール実行］ボタンをクリックします。

3. インストール開始のダイアログで［次へ］ボタンをクリックします。

4. ［使用許諾契約］ダイアログで、内容を確認してから［使用許諾契約の条項に同意します］を選択し、［次へ］ボタンをクリックします。

   同一のバージョンで上書きインストールする場合は手順 5.へ、異なるバージョンで上書きインストールする場合は手順 8.へ進んでください。

5. コンポーネントを選択するダイアログで、設定内容を確認し、［次へ］ボタンをクリックします。

6. ［インストールする Manager の種別］ダイアログで、Manager の種類を確認して［次へ］ボタンをクリックします。

   ［管理用中継サーバ］を選択している場合は手順 7.へ、［単数サーバ構成の管理用サーバ、または複数サーバ構成の統括管理用サーバ］を選択している場合は手順 8.へ進んでください。

7. ［エージェントのコンポーネント設定］ダイアログで、管理用中継サーバに含めるエージェントのコンポーネントを選択して［次へ］ボタンをクリックします。

8. インストールの開始準備の完了を示すダイアログで、内容を確認し、［インストール］ボタンをクリックします。

   インストールが実行されます。なお、クラスタ構成の場合は、必要に応じてサービス停止を促すダイアログが表示されます。表示内容に従って操作してください。

9. インストールの完了を示すダイアログで、コンポーネントのアップデートに関する設定をして、［完了］ボタンをクリックします。

   コンポーネントのアップデートについては、「5.8　コンポーネントのアップデート方法」を参照してください。

   ヒント

   データベースのアップグレードが必要な場合は、上書きインストールの完了を示すダイアログに、セットアップを起動するための［セットアップ］が表示されます。ここをチェックするか、またはスタートメニューからセットアップを起動して実行してください。この場合、コンポーネントに関する設定は、セットアップの完了を示すダイアログに表示されます。

JP1/IT Desktop Management 2 - Manager の上書きインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

注意事項

上書きインストールを実行すると、ホーム画面の［監視候補の処理］に表示するインポートの実行状況は引き継ぎません。バージョンアップ後にインポートを実行すると実行状況が更新されます。

関連リンク

- 1.2.4　単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順

5.2 エージェントを提供媒体から上書きインストールする手順

エージェントの上書きインストールを実行するには、インストール対象のバージョンが、すでにインストールされているバージョン以上である必要があります。また、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

重要

JP1/IT Desktop Management - Agent がインストールされているコンピュータに JP1/IT Desktop Management 2 - Agent を上書きインストールする場合、JP1/IT Desktop Management - Agent のインストール先フォルダのパス長が 104 バイトを超えていると、インストールエラーで終了します。JP1/IT Desktop Management - Agent をアンインストールしてから、インストールしてください。

エージェントを上書きインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Agent］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。
4. ［インストールするコンポーネントの種別］ダイアログで、［エージェント］を選択して［次へ］ボタンをクリックします。

   ヒント

   ［中継システム］を選択するとエージェントを中継システムに変更できます。ただし、一度中継システムにすると、エージェントに変更することはできません。

> **ヒント**
>
> 管理用中継サーバ以外の管理用サーバ（統括管理用サーバを含む）の場合、[中継システム]を選択することはできません。この場合、エージェントだけをインストールできるため、[エージェント]が選択済みとなります。また、これを変更することはできません。

5. **[インストールするコンポーネント]ダイアログで、インストールするほかのコンポーネント、サブコンポーネント、およびそのインストール方法を指定して［次へ］ボタンをクリックします。**
   デフォルトでは初回インストール時に選択したコンポーネントが設定された状態になっています。

6. **インストールの開始準備の完了を示すダイアログで、[インストール]ボタンをクリックします。**
   インストールが実行されます。

7. **インストールの完了を示すダイアログで、[完了]ボタンをクリックします。**

エージェントの上書きインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

5.3 中継システムを提供媒体から上書きインストールする手順

中継システムの上書きインストールを実行するには、インストール対象のバージョンが、すでにインストールされているバージョン以上である必要があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

重要

JP1/IT Desktop Management のサイトサーバとして利用していた（JP1/IT Desktop Management - Remote Site Server がインストールされている）コンピュータに中継システムをインストールする場合、JP1/IT Desktop Management - Remote Site Server をアンインストールしてから、インストールしてください。

中継システムを上書きインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Agent］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。
4. ［インストールするコンポーネント］ダイアログで、インストールするほかのコンポーネント、サブコンポーネント、およびそのインストール方法を指定して［次へ］ボタンをクリックします。
   デフォルトでは初回インストール時に選択したコンポーネントが設定された状態になっています。

   ヒント

   インストールするコンポーネントおよびサブコンポーネントを変更したり、そのインストール方法を変更したりする場合は、文字列の左にあるアイコンをクリックして、プルダウンメニューから選択します。
5. インストールの開始準備の完了を示すダイアログで、［インストール］ボタンをクリックします。
   インストールが実行されます。

6. インストールの完了を示すダイアログで、[完了] ボタンをクリックします。

中継システムの上書きインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

5.4 ネットワークモニタエージェントを提供媒体から上書きインストールする手順

ネットワークモニタエージェントの上書きインストールを実行するには、インストール対象のバージョンが、すでにインストールされているバージョン以上である必要があります。また、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

ネットワークモニタエージェントを上書きインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Network Monitor］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。
4. インストールの開始準備の完了を示すダイアログで、［インストール］ボタンをクリックします。
   インストールが実行されます。
5. インストールの完了を示すダイアログで、［完了］ボタンをクリックします。

ネットワークモニタエージェントの上書きインストールが完了します。再起動は不要です。

重要

ネットワークモニタの有効化が完了する前にネットワークモニタエージェントを上書きインストールした場合、上書きインストールした機器を再起動してください。

5.5 インターネットゲートウェイを提供媒体から上書きインストールする手順

インターネットゲートウェイの上書きインストールを実行するには、インストール対象のバージョンが、すでにインストールされているバージョン以上である必要があります。また、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータに上書きインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

重要

上書きインストール前は、すべての Windows アプリケーションを終了させてください。

インターネットゲートウェイを上書きインストールするには：

1. World Wide Web Publishing Service サービス※を停止します。
2. 提供媒体を CD/DVD ドライブにセットします。
3. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Internet Gateway］を選択して、［インストール実行］ボタンをクリックします。
4. インストール開始のダイアログで［次へ］ボタンをクリックします。
5. インストールの開始準備の完了を示すダイアログで、［インストール］ボタンをクリックします。
   インストールが実行されます。

   メモ

   ［インストール］ボタンをクリックした後に、セットアップで更新できないファイルまたはサービスがあることを通知するウィンドウが表示された場合は、World Wide Web Publishing Service サービスが停止していないことが考えられます。［キャンセル］ボタンでインストールを終了させ、手順 1 から再実行してください。
6. インストールの完了を示すダイアログで、［完了］ボタンをクリックします。

インターネットゲートウェイの上書きインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

7. World Wide Web Publishing Service サービス※を開始します。

注※　Windows Server 2025、Windows Server 2022、Windows Server 2019 または Windows Server 2016 の場合、「World Wide Web 発行サービス」です。

5.6 JP1/IT Desktop Management 2 のシステム全体をバージョンアップする流れ

JP1/IT Desktop Management 2 のシステム全体のバージョンアップは、配布機能または提供媒体を使用する場合と、管理用サーバに登録されたプログラムでコンポーネントを自動的にアップデートする場合とで、流れが異なります。

配布機能または提供媒体を使用してバージョンアップするには：

管理者が任意のタイミングでバージョンアップする場合は、事前に、管理用サーバに登録されたプログラムの自動アップデートの機能を無効にしてください。

1. 管理用サーバに新しいバージョンのプログラムを上書きインストールすることで、JP1/IT Desktop Management 2 - Manager をバージョンアップします。
2. 次のコンポーネントをアップデートします。
   - 中継システムがインストールされているコンピュータの中継システム
   - ネットワークモニタエージェントがインストールされているコンピュータのエージェントおよびネットワークモニタエージェント
   - 管理者のコンピュータにインストールされているリモートコントロール機能のコントローラ
   - 管理者のコンピュータにインストールされているリモートインストールマネージャ
3. ネットワークモニタエージェントがインストールされていないコンピュータのエージェントをアップデートします。

管理用サーバに登録されたプログラムでコンポーネントを自動的にアップデートすることでバージョンアップするには：

1. 管理用サーバに新しいバージョンのプログラムを上書きインストールすることで、JP1/IT Desktop Management 2 - Manager をバージョンアップします。
2. 管理用サーバにエージェントおよびネットワークモニタのコンポーネントを登録し、自動的にアップデートするよう設定します。

> **重要**
>
> JP1/IT Desktop Management 2 - Manager のバージョンアップ後に、リモートコントロールを実行する場合は、事前にコントローラをバージョンアップしてください。

> **重要**
>
> JP1/IT Desktop Management - Agent がインストールされているコンピュータに JP1/IT Desktop Management 2 - Agent を上書きインストールする場合、JP1/IT Desktop

Management - Agent のインストール先フォルダのパス長が 104 バイトを超えていると、インストールエラーで終了します。JP1/IT Desktop Management - Agent をアンインストールしてから、インストールしてください。

重要

マルチサーバ構成で運用していた JP1/IT Desktop Management は、JP1/IT Desktop Management 2 にバージョンアップできません。

重要

JP1/IT Desktop Management 2 のバージョン 10 またはバージョン 11 を介してバージョンアップすると、次に示す管理画面の表示項目と表示順の設定は初期化されます。

- ［セキュリティ］－［機器のセキュリティ状態］－［機器一覧］
- ［資産］－［管理ソフトウェア］－［管理ソフトウェア一覧］の［インストールソフトウェア］タブ
- ［機器］－［機器情報］－［機器一覧］
- ［機器］－［機器情報］－［機器一覧］の［インストールソフトウェア情報］タブ
- ［機器］－［ソフトウェア情報］－［ソフトウェア一覧］
- ［設定］－［機器の探索］－［探索履歴の確認］－［ネットワークの探索］

ヒント

MDM システムと連携するときは、MDM システムのルート証明書を確認されたあと連携が開始されます。「4.5　MDM 連携構成システムの構築時の設定」を参照して設定してください。また、MDM サーバのホスト名が正しく設定されているかを確認してください。詳細については、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」の、MDM 連携の設定のパラメーターの説明を参照してください。

関連リンク

- 5.7　JP1/IT Desktop Management 2 - Manager をバージョンアップする手順
- 5.8　コンポーネントのアップデート方法

5.7 JP1/IT Desktop Management 2 - Manager をバージョンアップする手順

管理用サーバで、新しいバージョンのプログラムを上書きインストールすることで、JP1/IT Desktop Management 2 - Manager をバージョンアップします。

重要

- バージョンアップする前に、JP1/IT Desktop Management 2 からログアウトして、操作画面を閉じてください。操作画面を表示したままバージョンアップすると、バージョンアップ後に操作画面が正しく表示されない場合があります。

JP1/IT Desktop Management 2 - Manager をバージョンアップするには：

1. データベースのバックアップを取得します。

   障害に備えて、バックアップを取得してください。

   データベースのバックアップは、データベースマネージャを利用してください。バックアップ先フォルダのドライブは、目安として 20 ギガバイト以上の空き容量を確保してください。

2. 管理用サーバの JP1/IT Desktop Management 2 - Manager を上書きインストールします。

   上書きインストール中は、ハードディスクに最低 2.4 ギガバイトの空き容量が必要です。

   重要

   上書きインストールに失敗した場合は、上書きインストール前の環境に戻してから手順 2.以降の作業をしてください。上書きインストール前の環境に戻すには、旧バージョンのプログラムをインストールしてライセンスを登録したあと、手順 1.でバックアップしたデータベースをリストアします。データベースのリストアは、データベースマネージャを利用してください。

   ヒント

   上書きインストール時にコンポーネントを自動的にアップデートする設定にしている場合、利用者のコンピュータにインストールされているエージェントおよびネットワークモニタエージェントが自動的に更新されます。

   ヒント

   エージェントおよびネットワークモニタエージェントが自動的に更新される際に、管理用サーバから各コンピュータにデータが送信されます。エージェント導入済みのコンピュータには、1 台当たり約 80 メガバイトのデータが送信されます。これに追加して、ネットワークモニタエージェントがインストールされているエージェント導入済みのコンピュータには、1 台当たり約 5 メガバイトのデータが送信されます。

3. データベースをアップグレードします。

セットアップで、データベースをアップグレードします。

> **ヒント**
>
> データベースのアップグレードが完了したら、手順 1.で取得したデータベースのバックアップを削除してかまいません。

JP1/IT Desktop Management 2 - Manager のバージョンアップが完了します。

> **ヒント**
>
> MDM システムと連携するときは、MDM システムのルート証明書を確認されたあと連携が開始されます。「4.5　MDM 連携構成システムの構築時の設定」を参照して設定してください。また、MDM サーバのホスト名が正しく設定されているかを確認してください。詳細については、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」の、MDM 連携の設定のパラメーターの説明を参照してください。

5.8 コンポーネントのアップデート方法

コンポーネントとは、エージェントおよびネットワークモニタエージェントを指します。これらのプログラムには、次に示すアップデート方法があります。

重要

JP1/IT Desktop Management - Agent がインストールされているコンピュータに JP1/IT Desktop Management 2 - Agent を上書きインストールする場合、JP1/IT Desktop Management - Agent のインストール先フォルダのパス長が 104 バイトを超えていると、インストールエラーで終了します。JP1/IT Desktop Management - Agent をアンインストールしてから、インストールしてください。

重要

JP1/IT Desktop Management のサイトサーバとして利用していた（JP1/IT Desktop Management - Remote Site Server がインストールされている）コンピュータに中継システムをインストールする場合、JP1/IT Desktop Management - Remote Site Server をアンインストールしてから、インストールしてください。

管理用サーバに登録されたプログラムで自動的にアップデートする

管理用サーバに新しいバージョンのプログラムを登録し、自動配信してアップデートします。

システム全体のバージョンアップの際など、JP1/IT Desktop Management 2 - Manager を含めて複数のプログラムをアップデートする場合は、JP1/IT Desktop Management 2 - Manager の上書きインストール時にコンポーネントの自動アップデートを設定することで、新しいバージョンのエージェントおよびネットワークモニタエージェントが管理用サーバに自動で登録され、配信されます。

コンポーネントの自動アップデートの設定、および各プログラムの管理用サーバへの登録は、JP1/IT Desktop Management 2 - Manager の上書きインストール完了を示すダイアログ、または管理用サーバの［スタート］メニューから表示する［コンポーネントの登録］ダイアログで実施できます。

ITDM 互換配布機能を使用してアップデートする

管理用サーバにパッケージを登録し、タスクを作成して配布することでアップデートします。ネットワークに負荷が掛かるタイミングを制御したいなどの理由で、自動ではアップデートしたくない場合に便利です。自動アップデートしたくない場合は事前に管理用サーバに登録されたプログラムの自動アップデートの機能を無効にする必要があります。

システム全体のバージョンアップの際など、JP1/IT Desktop Management 2 - Manager を含めて複数のプログラムをアップデートする場合は、JP1/IT Desktop Management 2 - Manager の上書きインストール時にコンポーネントのパッケージ登録を設定することで、新しいバージョンのエージェントおよびネットワークモニタエージェントがパッケージとして管理用サーバに自動で登録されます。

コンポーネントのパッケージ登録の設定、および各プログラムの管理用サーバへの登録は、JP1/IT Desktop Management 2 - Manager の上書きインストール完了を示すダイアログ、または管理用サーバの［スタート］メニューから表示する［コンポーネントの登録］ダイアログで実施できます。

自動的に登録されるパッケージの名称は［*プログラム形名_バージョン番号_各コンポーネントのプログラム名*］（例：[P-CC2642-7BA4_1050_JP1_IT Desktop Management 2 - Agent]）です。このパッケージを指定したタスクを追加して配布してください。タスクを追加する際は、コンポーネントが「5.6 JP1/IT Desktop Management 2 のシステム全体をバージョンアップする流れ」に記載されている順番でアップデートされるようにしてください。

ヒント

コンポーネントのパッケージ登録が完了すると、自動登録されたパッケージ名がメッセージに表示します。同じバージョンのパッケージが登録済みの場合でも同じメッセージが表示され、上書き登録はされません。このメッセージに表示されたパッケージが登録されたかどうかは、配布（ITDM 互換）画面の［パッケージ］－［パッケージ一覧］からパッケージの更新日時で確認してください。パッケージの更新日時が更新されていない場合は、パッケージの再配布は不要です。

提供媒体を使用してアップデートする

新しいバージョンの提供媒体から各プログラムを上書きインストールすることでアップデートします。

上書きインストールは、「5.6　JP1/IT Desktop Management 2 のシステム全体をバージョンアップする流れ」に記載されている順番でアップデートされるようにしてください。

コントローラをアップデートする

JP1/IT Desktop Management 2 のバージョンアップに伴ってコントローラが更新された場合は、操作画面からリモートコントロールを実行したタイミングで自動的に上書きインストールされます。

なお、［スタート］メニューからリモートコントロールを実行しても、コントローラは上書きインストールされません。［スタート］メニューからリモートコントロールを実行する運用のときは、エージェントをアップデートする前に、操作画面からリモートコントロールを実行して、コントローラをバージョンアップしてください。

重要

次の場合、コントローラは自動的に上書きインストールされません。

- プロキシサーバを介して JP1/IT Desktop Management 2 に接続している環境で、インターネットオプションのプロキシサーバが正しく設定されていない場合
- Internet Explorer がオフラインモードになっている場合

重要

ネットワークモニタの有効化が完了する前にネットワークモニタをアップデートした場合、アップデートした機器を再起動してください。

関連リンク

- 5.9　コンポーネントを登録する手順

5.9 コンポーネントを登録する手順

コンポーネントとは、エージェントおよびネットワークモニタエージェントのことです。

アップデート版のコンポーネントまたは修正パッチがリリースされた場合、それらのプログラムを管理用サーバに登録して、自動アップデートするように設定すると便利です。

ネットワークに負荷が掛かるタイミングを制御したいなどの理由で、自動ではアップデートしたくない場合も、管理用サーバにアップデート版のプログラムを登録することで、パッケージの自動登録ができます。この場合は、自動登録されたパッケージを指定してタスクを作成し、配布します。

ヒント

JP1/IT Desktop Management 2 - Manager をバージョンアップする場合は、JP1/IT Desktop Management 2 - Manager の上書きインストールの際にコンポーネントの自動アップデートやパッケージ登録を設定できます。この場合、アップデート版のコンポーネントが自動的に管理用サーバに登録されて配信またはパッケージ登録されるので、ここで説明する操作は不要です。

ヒント

エージェントおよびネットワークモニタエージェントが自動的に更新される際に、管理用サーバから各コンピュータにデータが送信されます。エージェント導入済みのコンピュータには、1 台当たり約 80 メガバイトのデータが送信されます。これに追加して、ネットワークモニタエージェントがインストールされているエージェント導入済みのコンピュータには、1 台当たり約 5 メガバイトのデータが送信されます。

コンポーネントを登録するには：

1. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［コンポーネントの登録］を選択します。
2. 表示されるダイアログで［参照］ボタンをクリックして、ダウンロードしたフォルダにあるアップグレード版のコンポーネントまたは修正パッチを指定します。
3. 登録したコンポーネントについて、自動アップデートおよびパッケージ登録について設定します。
4. ［OK］ボタンをクリックします。

アップグレード版のコンポーネントまたは修正パッチが管理用サーバに登録され、設定内容に応じて、配信またはパッケージ登録されます。

ヒント

登録するコンポーネントのバージョンがすでに登録済みのバージョンと同じか古い場合、「パッケージは既に登録されています。登録済みのパッケージを削除したあと、パッケージを再登録してください。」のエラーメッセージが出力されます。

5.10　クラスタシステムで上書きインストールする流れ

クラスタシステムで JP1/IT Desktop Management 2 を上書きインストールするには、現用系サーバで上書きインストールしたあと、待機系サーバで上書きインストールします。

クラスタシステムを上書きインストールするには：

1. 現用系サーバの JP1/IT Desktop Management 2 のサービスリソースをオフラインにします。
   オフラインにするサービスリソースについては、「2.10.2　現用系サーバでリソースグループを作成する手順」の、グループに登録が必要なリソースの表にある「JP1/IT Desktop Management 2 のサービスリソース（汎用サービス）」を参照してください。クライアントアクセスポイント、および記憶域（共有ディスク）は、オンラインのままです。
2. 現用系サーバで JP1/IT Desktop Management 2 - Manager を上書きインストールします。
3. 現用系サーバでセットアップを起動し、データベースアップグレードを実行します。
   データベースのアップグレードが不要な場合は、この手順は実行不要です。
4. 現用系サーバのセットアップ完了時に出力されるファイルを待機系サーバにコピーします。
5. リソースグループの所有者を待機系サーバに移動します。
6. 待機系サーバで JP1/IT Desktop Management 2 - Manager を上書きインストールします。
7. 待機系サーバでセットアップを起動し、データベースアップグレードを実行します。
   データベースのアップグレードが不要な場合は、この手順は実行不要です。
8. リソースグループの所有者を現用系サーバに移動します。
9. 手順 1.でオフラインにしたサービスリソースをオンラインにします。

クラスタシステムの上書きインストールが完了します。

関連リンク

- 5.1　JP1/IT Desktop Management 2 - Manager を上書きインストールする手順

5.11 JP1/IT Desktop Management および他製品から JP1/IT Desktop Management 2 への上書きインストール

JP1/IT Desktop Management 2 は、旧製品の JP1/IT Desktop Management と同じコンピュータ上に共存することはできませんが、JP1/IT Desktop Management を導入済みのコンピュータに JP1/IT Desktop Management 2 を上書きインストールすることはできます。

JP1/IT Desktop Management から上書きインストール時のセキュリティポリシー

JP1/IT Desktop Management 2 - Manager では、セキュリティポリシーの［機器の使用抑止］の設定値について JP1/IT Desktop Management 2 - Agent 用と JP1/IT Desktop Management - Agent 用の設定値を保持します。管理画面で表示・編集可能なのは、JP1/IT Desktop Management 2 - Agent 用の設定だけです。

- JP1/IT Desktop Management - Manager から移行したセキュリティポリシーの場合
  - JP1/IT Desktop Management - Agent 用は、JP1/IT Desktop Management - Manager で設定していた設定値が引き継がれます。
  - JP1/IT Desktop Management 2 - Agent 用は、設定値はありません。JP1/IT Desktop Management - Agent 用の設定で制御します。
- JP1/IT Desktop Management - Manager から移行したセキュリティポリシーを編集した場合
  - JP1/IT Desktop Management - Agent 用は、JP1/IT Desktop Management - Manager で設定していた設定値が保持されます。
  - JP1/IT Desktop Management 2 - Agent 用：JP1/IT Desktop Management 2 - Manager の編集画面で設定した設定値に変更されます。
- JP1/IT Desktop Management - Manager から移行したセキュリティポリシーを複製した場合
  - JP1/IT Desktop Management - Agent 用は、複製元の JP1/IT Desktop Management - Manager で設定していた設定値が保持されます。
  - JP1/IT Desktop Management 2 - Agent 用：複製元の設定値が保持されます。
- JP1/IT Desktop Management 2 - Manager でセキュリティポリシーを新規作成した場合
  - JP1/IT Desktop Management - Agent 用は、［機器の使用抑止］の設定値がすべて無効になります。機器の使用は抑止されません。
  - JP1/IT Desktop Management 2 - Agent 用は、JP1/IT Desktop Management 2 - Manager の編集画面で設定した設定値になります。

JP1/IT Desktop Management 2 - Manager で［機器の使用抑止］を使用するには、JP1/IT Desktop Management 2 - Agent を導入してください。JP1/IT Desktop Management 2 - Manager で JP1/IT Desktop Management - Agent に対して［機器の使用抑止］の制御を切り替える方法を次に示します。

- セキュリティポリシーの割り当てを切り替える

［機器の使用抑止］の設定が異なるセキュリティポリシーを JP1/IT Desktop Management - Agent に対して割り当てを変更することで、［機器の使用抑止］の制御を切り替えます。なお、JP1/IT Desktop Management - Manager で［機器の使用抑止］の設定が異なる複数のセキュリティポリシーを作成していて、JP1/IT Desktop Management 2 - Manager に移行している場合に実施できます。

JP1/NETM/DM と JP1/IT Desktop Management 2 の共存

JP1/NETM/DM と JP1/IT Desktop Management 2 は、同じコンピュータ上に共存することはできますが、JP1/NETM/DM から JP1/IT Desktop Management 2 への上書きインストールはできません。共存についての詳細を次の表に示します。なお、共存していても、相互接続（JP1/NETM/DM で管理している機器を JP1/IT Desktop Management 2 で管理することやその逆）はできません。

JP1/NETM		JP1/IT Desktop Management 2						
		管理用サーバ	エージェント	中継システム	コントローラ	リモコンエージェント	ネットワークモニタ	Asset Console
JP1/NETM/DM Manager（リモートコントロールマネージャを含む）	マネージャ	×	○	○	○	○	○	○
	中継マネージャ	×	○	○	○	○	○	○
JP1/NETM/DM Client※1（リモートコントロールエージェントを含む）	中継システム※2	○	○	○	○	○	○	○
	クライアント	○	○	○	○	○	○	○
JP1/NETM/DM Manager（Asset Information Manager Limited の場合）	マネージャ	×	○	○	○	○	○	×
	中継マネージャ	×	○	○	○	○	○	×
JP1/NETM/Asset Information Manager		×	○	○	○	○	○	×
JP1/NETM/Client Security Control	Manager	×	○	○	○	○	○	×
	Agent	○	○	○	○	○	○	○
JP1/NETM/NM	Manager	○	○	○	○	○	○	○

JP1/NETM		JP1/IT Desktop Management 2						
		管理用サーバ	エージェント	中継システム	コントローラ	リモコンエージェント	ネットワークモニタ	Asset Console
JP1/NETM/NM	Agent	○	○	○	○	○	×	○

（凡例）○：共存できる　×：共存できない

注※1　JP1/NETM/DM Client - Base および次のオプション製品を含みます。

- JP1/NETM/DM Client - Operation Log Feature
- JP1/NETM/DM Client - Delivery Feature
- JP1/NETM/DM Client - Remote Control Feature

注※2　JP1/NETM/DM SubManager を含みます。

JP1/IT Desktop Management から JP1/IT Desktop Management 2 に上書きインストールする方法については、「5.6　JP1/IT Desktop Management 2 のシステム全体をバージョンアップする流れ」を参照してください。

上書きインストール時の JP1/IT Desktop Management の操作ログの自動取り込み

JP1/IT Desktop Management の操作ログのデータベースに格納されているオンライン領域の最大 30 日分の操作ログを、JP1/IT Desktop Management 2 への上書きインストール時に、JP1/IT Desktop Management 2 の操作ログのデータベースに自動的に取り込むことができます。セットアップの完了画面で［旧製品の操作ログの取り込み］にチェックしてください。なお、自動的に取り込んだ操作ログは、設定画面の［操作ログの設定］画面－［自動取り込みされる操作ログの格納期間］の設定値を過ぎると自動的に削除されます。

重要

- JP1/IT Desktop Management の操作ログを自動的に取り込むには、上書きインストール前に JP1/IT Desktop Management のセットアップで操作ログの保管先を設定しておく必要があります。
- JP1/IT Desktop Management の操作ログの取り込みには、1 日以上かかる場合があります。
- JP1/IT Desktop Management の操作ログの取り込みの進捗は、ホーム画面の［監視候補の処理］、またはセキュリティ画面の［操作ログの手動取り込み］ダイアログで確認できます。
- JP1/IT Desktop Management の操作ログの取り込みには、JP1/IT Desktop Management 2 の手動取り込みを使用するため、イベントやメッセージには「手動取り込み」と表示されます。

- JP1/IT Desktop Management と JP1/IT Desktop Management 2 の操作ログの管理方式の違いにより、JP1/IT Desktop Management の操作ログの場合は、操作ログ一覧画面上部のタイムチャートで、操作ログの存在する日付の前後一日が活性して表示されることがあります。

ヒント

JP1/IT Desktop Management のセットアップで操作ログの保管先が設定されていない場合、JP1/IT Desktop Management の操作ログのデータベースに格納されているオンライン領域の操作ログデータは、JP1/IT Desktop Management 2 への上書きインストールでデータベース退避フォルダに出力されます。出力先はセットアップの完了画面にも表示されます。JP1/IT Desktop Management 2 の操作ログのデータベースに取り込むには、JP1/IT Desktop Management 2 の管理用サーバのセットアップで操作ログの保管先を設定して、次のファイルをコピーして、手動取り込みを実施してください。

- OPR_CATALOG_*YYYYMMDD*.csv
- OPR_DATA_*YYYYMMDD*.zip
- OPR_OTHER.zip

サイトサーバを利用している環境のバージョンアップ

JP1/IT Desktop Management のサイトサーバを利用している（JP1/IT Desktop Management - Remote Site Server がインストールされている）場合、JP1/IT Desktop Management 2 - Manager へのバージョンアップ前に次の操作を実施してください。実施しない場合、ITDM 互換配布および操作ログの収集ができません。

- JP1/IT Desktop Management - Manager から JP1/IT Desktop Management 2 - Manager に バージョンアップインストールする前に、［サーバ構成の管理］画面から［パッケージ配布の中継地点］および［操作ログの保管先フォルダ］の設定をサイトサーバから 管理用サーバに変更してください。

重要

JP1/IT Desktop Management のサイトサーバとして利用していた（JP1/IT Desktop Management - Remote Site Server がインストールされている）コンピュータに中継システムをインストールする場合、JP1/IT Desktop Management - Remote Site Server をアンインストールしてから、インストールしてください。

JP1/IT Desktop Management から引き継がれない設定

JP1/IT Desktop Management を導入済みのコンピュータに JP1/IT Desktop Management 2 を上書きインストールすると、 次の表示項目および表示順の設定は引き継がれず初期化されます。

- ［セキュリティ］-［機器のセキュリティ状態］-［機器一覧］

- ［資産］-［管理ソフトウェア］-［管理ソフトウェア一覧］-［インストールソフトウェア］
- ［機器］-［機器情報］-［機器一覧］
- ［機器］-［機器情報］-［機器一覧］-［インストールソフトウェア情報］
- ［機器］-［ソフトウェア情報］-［ソフトウェア一覧］
- ［設定］-［機器の探索］-［探索履歴の確認］-［ネットワークの探索］

6 製品のアンインストール

ここでは、JP1/IT Desktop Management 2 の各種プログラムをアンインストールする方法について説明します。

6.1　システム全体でのアンインストールの流れ

1. 機器のネットワーク接続を監視している場合は、各ネットワークセグメントのネットワークモニタを無効にします。
2. エージェント導入済みのコンピュータからエージェントをアンインストールします。
3. 中継システムをインストールしたコンピュータから中継システムをアンインストールします。
4. リモートインストールマネージャをインストールした管理者のコンピュータからリモートインストールマネージャをアンインストールします。
5. 管理用サーバから JP1/IT Desktop Management 2 - Manager をアンインストールします。

このほか、リモートコントロール機能を使用している場合は、管理者のコンピュータからコントローラをアンインストールする必要があります。コントローラのアンインストールは、どのタイミングで実施しても問題ありません。

また、Asset Console を使用している場合は、対象のコンピュータから Asset Console をアンインストールする必要があります。Asset Console のアンインストールは、どのタイミングで実施しても問題ありません。アンインストールの詳細については、マニュアル「JP1/IT Desktop Management 2 - Asset Console 構築・運用ガイド」を参照してください。

さらに、インターネットゲートウェイを使用している場合は、対象のコンピュータからインターネットゲートウェイをアンインストールする必要があります。インターネットゲートウェイのアンインストールは、どのタイミングで実施しても問題ありません。

ヒント

リモコンエージェントは、エージェントをアンインストールすると自動的にアンインストールされます。

ヒント

アンインストールは、管理者権限で実施してください。また、アンインストールしたあとは、コンピュータを再起動してください。

関連リンク

- 6.6　ネットワークモニタを無効にする手順
- 6.4　エージェントをアンインストールする手順
- 6.2　JP1/IT Desktop Management 2 - Manager をアンインストールする手順
- 6.7　コントローラをアンインストールする手順
- 6.9　インターネットゲートウェイをアンインストールする手順

6.2 JP1/IT Desktop Management 2 - Manager をアンインストールする手順

JP1/IT Desktop Management 2 - Manager を再インストールする場合や管理用サーバを変更したい場合は、JP1/IT Desktop Management 2 - Manager をアンインストールします。

重要

アンインストールの実行中に、OS をシャットダウンしないでください。シャットダウンすると、アンインストールを再実行した場合に、正常にアンインストールされないことがあります。

重要

アンインストール前は、すべての Windows アプリケーションを終了させてください。誤って JP1/IT Desktop Management 2 - Manager のプログラムを起動したままアンインストールを実行した場合は、アンインストールの実行結果に関係なく OS を再起動してください。

JP1/IT Desktop Management 2 - Manager をアンインストールするには：

1. Windows のコントロールパネルで［プログラムと機能］を起動します。
2. 「JP1/IT Desktop Management 2 - Manager」を選択し、［変更］ボタンをクリックします。
3. JP1/IT Desktop Management 2 - Manager 用のインストールウィザードで［次へ］ボタンをクリックします。
4. アンインストールの確認画面で［削除］ボタンをクリックします。
5. アンインストールの終了画面で［完了］ボタンをクリックします。

JP1/IT Desktop Management 2 - Manager がアンインストールされます。

ヒント

JP1/IT Desktop Management 2 - Manager をアンインストールしても、各コンピュータのエージェントをアンインストールする必要はありません。ただし、コンピュータに常駐するプロセスがあるため、JP1/IT Desktop Management 2 を利用しない場合は、エージェントはアンインストールすることをお勧めします。

関連リンク

- 6.7　コントローラをアンインストールする手順
- 6.8　クラスタシステムで JP1/IT Desktop Management 2 - Manager をアンインストールする手順

6.3 リモートインストールマネージャをアンインストールする手順

管理者のコンピュータにリモートインストールマネージャを再インストールする場合や、リモートインストールマネージャをインストールした管理者のコンピュータを変更したい場合は、リモートインストールマネージャをアンインストールします。

重要

アンインストールの実行中に、OS をシャットダウンしないでください。シャットダウンすると、アンインストールを再実行した場合に、正常にアンインストールされないことがあります。

重要

アンインストール前は、すべての Windows アプリケーションを終了させてください。

リモートインストールマネージャをアンインストールするには：

1. Windows のコントロールパネルで［プログラムと機能］を起動します。
2. 「JP1/IT Desktop Management 2 - Manager」を選択し、［変更］ボタンをクリックします。
3. JP1/IT Desktop Management 2 - Manager 用のインストールウィザードで［次へ］ボタンをクリックします。
4. アンインストールの確認画面で［削除］ボタンをクリックします。
5. アンインストールの終了画面で［完了］ボタンをクリックします。

リモートインストールマネージャがアンインストールされます。

6.4 エージェントをアンインストールする手順

JP1/IT Desktop Management 2 で詳細な情報を管理する必要がなくなったコンピュータからは、エージェントをアンインストールします。エージェントをアンインストールしたオンライン管理のコンピュータは、自動的にエージェントレスのコンピュータになります。

重要

ネットワークモニタが有効になっていると、エージェントをアンインストールできません。対象のコンピュータのネットワークモニタを無効にしてから、エージェントをアンインストールしてください。

エージェントをアンインストールするには：

1. Windows のコントロールパネルで［プログラムと機能］を起動します。
2. 「JP1/IT Desktop Management 2 - Agent」を選択し、［アンインストール］ボタンをクリックします。
3. アンインストールの確認画面で［はい］ボタンをクリックします。
   JP1/IT Desktop Management 2 のエージェントがアンインストールされます。
4. コンピュータを再起動します。

重要

エージェントのアンインストール後にコンピュータを再起動しない場合、ほかのアプリケーションのネットワーク通信が失敗することがあります。

コンピュータの廃棄やリース返却などに伴い、JP1/IT Desktop Management 2 での管理が不要になったコンピュータは、機器情報を削除します。

重要

エージェントにパスワード保護が設定されている場合、手順 3.のあとにパスワードの入力画面が表示されます。該当するエージェント設定に設定したパスワードを入力してください。パスワードのデフォルトは「manager」です。

重要

オンライン管理用のエージェントをアンインストールする際、管理用サーバと接続できなかった場合は、アンインストール続行の確認画面が表示されます。再度管理用サーバに接続を試みるか、接続を確認しないでアンインストールを続行するかを選択できます。管理用サーバに接続しないでアンインストールした場合、管理用サーバでは対象のコンピュータをエージェント導入済みのコンピュータとして扱います。エージェントレスのコンピュータとして管理するた

めには、いったん機器情報を削除してから探索で発見するなどして、コンピュータを登録し直してください。

オフライン管理用のエージェントをアンインストールする際は、アンインストール続行の確認画面は表示されません。

関連リンク

- 6.6　ネットワークモニタを無効にする手順

6.5 中継システムをアンインストールする手順

中継システムとして管理する必要がなくなったり、中継システムとして使用していたコンピュータを変更したりしたい場合は、中継システムをアンインストールします。

> **重要**
>
> ネットワークモニタが有効になっていると、中継システムをアンインストールできません。対象のコンピュータのネットワークモニタを無効にしてから、中継システムをアンインストールしてください。

中継システムをアンインストールするには：

1. Windows のコントロールパネルで［プログラムと機能］を起動します。
2. 「JP1/IT Desktop Management 2 - Agent」を選択し、［アンインストール］ボタンをクリックします。
3. アンインストールの確認画面で［はい］ボタンをクリックします。
   中継システムがアンインストールされます。
4. コンピュータを再起動します。

> **重要**
>
> 中継システムのアンインストール後にコンピュータを再起動しない場合、ほかのアプリケーションのネットワーク通信が失敗することがあります。

コンピュータの廃棄やリース返却などに伴い、JP1/IT Desktop Management 2 での管理が不要になったコンピュータは、機器情報を削除します。

> **重要**
>
> パスワード保護が設定されている中継システムの場合、手順 3.のあとにパスワードの入力画面が表示されます。該当するエージェント設定に設定したパスワードを入力してください。パスワードのデフォルトは「manager」です。

> **重要**
>
> 中継システムをアンインストールする際、管理用サーバと接続できなかった場合は、アンインストール続行の確認画面が表示されます。再度管理用サーバに接続を試みるか、接続を確認しないでアンインストールを続行するかを選択できます。管理用サーバに接続しないでアンインストールした場合、管理用サーバでは対象のコンピュータをエージェント導入済みのコンピュータとして扱います。エージェントレスのコンピュータとして管理するためには、いったん機器情報を削除してから探索で発見するなどして、コンピュータを登録し直してください。

関連リンク

- 6.6　ネットワークモニタを無効にする手順

6.6　ネットワークモニタを無効にする手順

特定のネットワークセグメントだけネットワーク接続を監視しないで運用したい場合や、ネットワークの監視を中止したい場合は、ネットワークモニタを無効にします。

ネットワークモニタを無効にするには：

1. 機器画面を表示します。
2. メニューエリアの［機器情報］で、［機器一覧（ネットワーク）］から該当するネットワークセグメントのグループを選択します。
3. インフォメーションエリアでネットワークモニタを有効にしているコンピュータを選択します。

   ネットワークモニタが有効になっているコンピュータは、管理種別に  、  または  が表示されています。
4. ［操作メニュー］の［ネットワークモニタを無効にする］を選択します。

選択したコンピュータのネットワークモニタが無効になり、ネットワークが監視されなくなります。

> **ヒント**
>
> ネットワークモニタを無効にすると、対象のコンピュータからネットワークモニタエージェントがアンインストールされます。

ネットワークモニタが無効になると、管理種別は  、  または  に戻ります。

なお、メニューエリアに表示されるネットワークモニタの動作状態が「ネットワークモニタを無効化しています」の場合は、ネットワークモニタを無効にできません。

> **重要**
>
> ネットワークモニタエージェントをインストールしているコンピュータの動作状態が「ネットワークモニタを無効化しています」または「ネットワークモニタの無効化に失敗しました」の場合は、コンピュータを「除外対象」にできません。

> **重要**
>
> ネットワークモニタを無効にする場合、あらかじめ管理用サーバにコンポーネント（ネットワークモニタエージェント）が登録されている必要があります。

重要

複数サーバ構成の場合、ネットワークモニタを無効化できるのは、自サーバ直下のコンピュータだけです。

ヒント

設定画面の［ネットワーク制御］－［ネットワークモニタ設定の割り当て］画面でもネットワークモニタを無効にできます。

ヒント

ネットワークモニタを無効にしたコンピュータが複数のネットワークセグメントに所属している場合、所属しているすべてのネットワークセグメントでネットワークモニタが無効になります。

ヒント

ネットワークモニタエージェントをインストールしているコンピュータが管理用サーバに接続できない環境の場合、そのコンピュータで、Windows のコントロールパネルの［プログラムと機能］から［JP1/IT Desktop Management 2 - Network Monitor］を選択して削除することで、ネットワークモニタを無効にできます。ただし、この方法で無効にするときも、まずは操作画面からの無効化の手順に従って操作し、管理用サーバ上の情報（対象のコンピュータの管理種別）を変更する必要があります。

関連リンク

- 2.6.2　ネットワークモニタを有効にする手順

6.7　コントローラをアンインストールする手順

リモートコントロールを実行する必要のないコンピュータからは、コントローラをアンインストールします。

コントローラをアンインストールするには：

1. Windows のコントロールパネルで［プログラムと機能］を起動します。
2. 「JP1/IT Desktop Management 2 - RC Manager」を選択し、［アンインストール］ボタンをクリックします。
3. 表示されるダイアログで［はい］ボタンをクリックします。

コントローラがアンインストールされます。

> **ヒント**
>
> リモコンエージェントは、エージェントをアンインストールすると自動的にアンインストールされます。

6.8 クラスタシステムで JP1/IT Desktop Management 2 - Manager をアンインストールする手順

クラスタシステムで JP1/IT Desktop Management 2 - Manager をアンインストールするには、現用系サーバでアンインストールしたあとで、待機系サーバでアンインストールします。

クラスタシステムで JP1/IT Desktop Management 2 - Manager をアンインストールするには：

1. 現用系サーバの JP1/IT Desktop Management 2 - Manager のサービスリソースをオフラインにします。
   オフラインにするサービスリソースについては、「2.10.2　現用系サーバでリソースグループを作成する手順」の、グループに登録が必要なリソースの表にある「JP1/IT Desktop Management 2 のサービスリソース（汎用サービス）」を参照してください。クライアントアクセスポイント、および記憶域（共有ディスク）は、オンラインのままです。
2. 現用系サーバで JP1/IT Desktop Management 2 - Manager をアンインストールします。
3. リソースグループの所有者を待機系サーバに移動します。
4. 待機系サーバで JP1/IT Desktop Management 2 をアンインストールします。

クラスタシステムでのアンインストールが完了します。

関連リンク

- 6.2　JP1/IT Desktop Management 2 - Manager をアンインストールする手順

6.9　インターネットゲートウェイをアンインストールする手順

インターネットゲートウェイをアンインストールするには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

重要

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータでアンインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

重要

アンインストールの実行中に、OS をシャットダウンしないでください。シャットダウンすると、アンインストールを再実行した場合に、正常にアンインストールされないことがあります。

重要

アンインストール前は、すべての Windows アプリケーションを終了させてください。

インターネットゲートウェイをアンインストールするには：

1. World Wide Web Publishing Service サービス※を停止します。

   注※　Windows Server 2025、Windows Server 2022、Windows Server 2019 または Windows Server 2016 の場合、「World Wide Web 発行サービス」です。

2. Windows のコントロールパネルで［プログラムと機能］を起動します。

3. 「JP1/IT Desktop Management 2 - Internet Gateway」を選択し、［アンインストール］ボタンをクリックします。

4. アンインストールの確認画面で［はい］ボタンをクリックします。

   インターネットゲートウェイがアンインストールされます。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

   メモ

   ［はい］ボタンをクリックした後に、セットアップで更新できないファイルまたはサービスがあることを通知するウィンドウが表示された場合は、World Wide Web Publishing Service サービスが停止していないことが考えられます。［キャンセル］ボタンでインストールを終了させ、手順 1 から再実行してください。

5. 「(4)　Microsoft Internet Information Services を設定する手順」で作成した、Microsoft Internet Information Services の構成を削除します。

6. 2.11.2　ファイアウォールの設定でファイアウォールに設定した内容を解除します。

7 環境の移行

ここでは、JP1/IT Desktop Management 2 で環境を移行する方法について説明します。

7.1　管理用サーバをリプレースする

管理用サーバのリプレースとは、JP1/IT Desktop Management 2 - Manager がインストールされているコンピュータとは別のコンピュータを、管理用サーバとして利用できるようにすることです。

管理用サーバをリプレースするときの注意事項を次に示します。

重要

リプレース先のコンピュータにインストールする JP1/IT Desktop Management 2 - Manager は、リプレース元と製品のバージョン情報が一致している必要があります。

重要

管理用サーバのリプレース時に JP1/IT Desktop Management 2 - Manager のバージョンアップはできません。リプレース完了後にバージョンアップするか、バージョンアップ後にリプレースしてください。バージョンアップの手順については、「5.7　JP1/IT Desktop Management 2 - Manager をバージョンアップする手順」を参照してください。

重要

コンピュータが Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016 または Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- *システムドライブ*:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

重要

リプレース先のコンピュータの IP アドレスが、リプレース元のコンピュータから変更になる場合、エージェントの接続先を変更するには、リプレース先の管理用サーバとエージェントの間で互いに直接参照できるネットワーク構成が必要です。直接参照できるネットワークとは、ホスト名および IP アドレスで参照できる、相互に ICMP などで通信できるネットワークです。また、管理用サーバとエージェントが使用する TCP プロトコルのポートを通過できるようにしておく必要があります。

重要

管理用サーバがリプレース元のシステム構成を引き継ぐためには、管理対象の機器の IP アドレスがリプレースの前後で一致している必要があります。

例えば、管理用サーバのリプレース中に、設置場所の変更によって管理対象のコンピュータのIP アドレスが変更になる場合、そのコンピュータはリプレース先の管理用サーバには接続されません。このようなときは、リプレース先の管理用サーバでインストールセットを作成し、そのコンピュータにエージェントを導入し直してください。これによって、コンピュータが管理用サーバに接続されるようになります。

重要

リプレース元のコンピュータで取得したデータベースのバックアップは、管理用サーバのユーザー ID/パスワードと同様に、管理者以外が参照できないように管理してください。このバックアップを不正に入手してリストアすれば、その管理用サーバから管理対象の機器の操作ができてしまうためです。

重要

リプレース元の管理用サーバで管理していた機器を、リプレース先の管理用サーバで引き続き管理する場合、リプレース元のコンピュータでバックアップしたデータベースを、リプレース先のコンピュータにリストアしてください。データベースのリストアを実施しないと、管理対象の機器にインストールされているエージェントがリプレース先の管理用サーバに接続されません。

なお、リプレース後の管理用サーバで新たに機器管理を始める場合は、データベースのバックアップとリストアは不要です。このとき、リプレース前と同じ機器を管理するには、リプレース完了後に次のように対処してください。

- エージェント導入済みのコンピュータ：リプレース後の管理用サーバで作成したインストールセットを利用して、エージェントを再インストールしてください。
- エージェントレスの機器：探索を実行して、機器を管理対象にしてください。

重要

JP1/IT Desktop Management 2 - Manager をアンインストールしないで、リプレース元の管理用サーバをネットワークに接続した場合、リプレース先の管理用サーバで正しくエージェントを管理できなくなります。

これは、リプレース元とリプレース先の管理用サーバが、それぞれエージェントに接続できてしまうためです。それぞれの管理用サーバから異なる指示があると、エージェントが管理者の意図しない状態になることがあります。また、エージェントがリプレース元の管理用サーバに接続して通知した情報は、リプレース先の管理用サーバには通知されないため、管理している情報に差異が発生してしまいます。

7.1.1　単数サーバ構成の管理用サーバをリプレースする手順

単数サーバ構成の管理用サーバをリプレースする手順を次に示します。リプレース先のコンピュータに JP1/IT Desktop Management 2 - Manager をインストールして、リプレース元のコンピュータからデータを移行することで、管理用サーバをリプレースします。リプレース時の注意事項については、「7.1　管理用サーバをリプレースする」を参照してください。

単数サーバ構成の管理用サーバをリプレースするには：

1. JP1/IT Desktop Management 2 のサービスを停止します。

   データベースのバックアップ後に、エージェントから通知された操作ログが新規に保管されないよう、あらかじめサービスを停止しておきます。

   Windows の［スタート］メニューから［管理ツール］－［サービス］を選択してください。表示されるダイアログで、サービス名を右クリックして［停止］を選択すると、サービスを停止できます。停止するサービスを次に示します。

   - JP1_ITDM2_Agent Control
   - JP1_ITDM2_Service
   - JP1_ITDM2_Web Container

2. データベースのバックアップを取得します。

   リプレース元のコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［データベースマネージャ］から JP1/IT Desktop Management 2 - Manager のデータベースマネージャを起動して、データベースのバックアップを実行してください。バックアップ先フォルダのドライブは、目安として 20 ギガバイト以上の空き容量を確保してください。

3. 操作ログのバックアップデータを退避します。

   操作ログを保管する設定にしている場合は、セットアップで指定している「操作ログの保管先フォルダ」に格納されているバックアップデータを退避してください。

   操作ログを保管する設定にしているかどうかは、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、［操作ログの設定］画面で［操作ログを保管する］がチェックされているかどうかで確認します。チェックされている場合は、操作ログを保管する設定になっています。

4. 変更履歴のバックアップデータを退避します。

   保存用の変更履歴を出力する設定にしている場合は、セットアップで指定している「変更履歴の出力先フォルダ」に格納されているバックアップデータを退避してください。

   保存用の変更履歴を出力する設定にしているかどうかは、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、［保存用の変更履歴の

出力設定］画面で［保存用の変更履歴を定期的に出力する］がチェックされているかどうかで確認します。チェックされている場合は、保存用の変更履歴を出力する設定になっています。

5. 設定ファイルを退避します。

コンフィグレーションファイル（jdn_manager_config.conf）に設定を追加している場合は、コンフィグレーションファイルを退避します。コンフィグレーションファイル（jdn_manager_config.conf）の格納先は次のとおりです。

JP1/IT Desktop Management 2 - Manager のインストール先フォルダ¥mgr¥conf

その他の設定ファイルを追加・編集している場合は、同様に退避してください。

6. リプレース先のコンピュータに、操作ログのバックアップデータを格納します。

手順 3.で操作ログのバックアップデータを退避した場合は、インストール前に、リプレース先のコンピュータで「操作ログの保管先フォルダ」に指定する予定のフォルダに格納しておきます。なお、このフォルダには、操作ログのバックアップデータ以外のデータは格納しないでください。

7. リプレース先のコンピュータに、変更履歴のバックアップデータを格納します。

手順 4.で変更履歴のバックアップデータを退避した場合は、インストール前に、リプレース先のコンピュータで「変更履歴の出力先フォルダ」に指定する予定のフォルダに格納しておきます。なお、このフォルダには、変更履歴のバックアップデータ以外のデータは格納しないでください。

8. リプレースの前後で管理用サーバの IP アドレスおよびホスト名が変わらない場合、リプレース元のコンピュータをネットワークから切断します。

9. リプレース先のコンピュータに、JP1/IT Desktop Management 2 - Manager をインストールします。

10. JP1/IT Desktop Management 2 - Manager をセットアップします。

リプレース先のコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、セットアップを実行してください。

操作ログを保管する設定にしている場合は、［操作ログの自動保管の設定］画面で「操作ログの保管先フォルダ」に、手順 6.でバックアップデータを格納したフォルダを指定してください。

保存用の変更履歴を出力する設定にしている場合は、［保存用の変更履歴の出力設定］画面で「変更履歴の出力先フォルダ」に、手順 7.でバックアップデータを格納したフォルダを指定してください。

11. リプレース先のコンピュータに、退避した設定ファイルを格納します。

手順 5.でコンフィグレーションファイル（jdn_manager_config.conf）を退避した場合は、リプレース先に格納してください※。コンフィグレーションファイル（jdn_manager_config.conf）の格納先は次のとおりです。

JP1/IT Desktop Management 2 - Manager のインストール先フォルダ¥mgr¥conf

その他の設定ファイルを退避した場合は、同様に格納してください※。

注※　すでに設定ファイルが存在する場合は、ファイルを上書きしてください。

12. 手順 2.でバックアップしたデータベースをリストアします。

リプレース先のコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［データベースマネージャ］から JP1/IT Desktop Management 2 - Manager のデータベースマネージャを起動して、データベースのリストアを実行してください。

13. ライセンスを登録します。

リプレース先のコンピュータにインストールした JP1/IT Desktop Management 2 - Manager のログイン画面で、［ライセンス］ボタンをクリックします。表示されるダイアログで［ライセンスを登録］ボタンをクリックして、ライセンスを登録します。

14. リプレースの前後で管理用サーバの IP アドレスまたはホスト名が変更になる場合、次の手順を参照して必要な設定を実施します。

- 7.9.1　管理用サーバのホスト名を変更する手順
- 7.9.2　管理用サーバの IP アドレスを変更する手順

15. 正しく運用できることを確認します。

リプレース先のコンピュータにインストールした JP1/IT Desktop Management 2 - Manager で、エージェントが管理用サーバに接続されたかどうかを確認します。機器画面の［機器一覧］画面で、［最終接続確認日時］が更新されていることを確認してください。

［最終接続確認日時］はデフォルトでは表示されていないため、表示されていない場合は［機器一覧］画面の一覧の項目を右クリックして、［表示項目の選択］から表示されるダイアログで確認してください。［最終接続確認日時］が更新されない場合、利用者のコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Agent］－［管理者ツール］－［セットアップ］からエージェントのセットアップを起動して、接続先にリプレース先の管理用サーバが設定されているかどうかを確認してください。

16. リプレース元のコンピュータで、JP1/IT Desktop Management 2 - Manager をアンインストールします。

管理用サーバのリプレースが完了します。

ヒント

リプレース元のコンピュータで取得したバックアップは、リプレース完了後に、必要に応じて削除してください。

ヒント

リプレース完了後にエージェントが管理用サーバに接続されたかどうかは、機器画面の［機器一覧］画面で、［最終接続確認日時］が更新されていることで確認できます。エージェントが接続されない場合、利用者のコンピュータで、エージェントのセットアップから接続先が正しく設定されているかどうか確認してください。

関連リンク

- 1.2.2　JP1/IT Desktop Management 2 - Manager をインストールする手順（単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバの場合）
- 1.2.4　単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順
- 2.10.1　クラスタシステムを構築する流れ
- 7.1　管理用サーバをリプレースする

7.1.2　複数サーバ構成の管理用サーバをリプレースする手順

複数サーバ構成の管理用サーバをリプレースする手順を次に示します。リプレース先のコンピュータに JP1/IT Desktop Management 2 - Manager をインストールして、リプレース元のコンピュータからデータを移行することで、管理用サーバをリプレースします。リプレース時の注意事項については、「7.1　管理用サーバをリプレースする」を参照してください。

なお、統括管理用サーバ、管理用中継サーバのどちらをリプレースする場合でも、同じ手順でリプレースできます。

複数サーバ構成の管理用サーバをリプレースするには：

1. JP1/IT Desktop Management 2 のサービスを停止します。

   データベースのバックアップ後に、エージェントから通知された操作ログが新規に保管されないよう、あらかじめサービスを停止しておきます。

   Windows の［スタート］メニューから［管理ツール］－［サービス］を選択してください。表示されるダイアログで、サービス名を右クリックして［停止］を選択すると、サービスを停止できます。停止するサービスを次に示します。

   - JP1_ITDM2_Agent Control
   - JP1_ITDM2_Service
   - JP1_ITDM2_Web Container
   - JP1_ITDM2_Relay Manager Service

2. データベースのバックアップを取得します。

   リプレース元のコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［データベースマネージャ］から JP1/IT Desktop Management 2 - Manager のデータベースマネージャを起動して、データベースのバックアップを実行してください。バックアップ先フォルダのドライブは、目安として 20 ギガバイト以上の空き容量を確保してください。

3. 操作ログのバックアップデータを退避します。

   操作ログを保管する設定にしている場合は、セットアップで指定している「操作ログの保管先フォルダ」に格納されているバックアップデータを退避してください。

操作ログを保管する設定にしているかどうかは、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、［操作ログの設定］画面で［操作ログを保管する］がチェックされているかどうかで確認します。チェックされている場合は、操作ログを保管する設定になっています。

4. 変更履歴のバックアップデータを退避します。

保存用の変更履歴を出力する設定にしている場合は、セットアップで指定している「変更履歴の出力先フォルダ」に格納されているバックアップデータを退避してください。

保存用の変更履歴を出力する設定にしているかどうかは、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、［保存用の変更履歴の出力設定］画面で［保存用の変更履歴を定期的に出力する］がチェックされているかどうかで確認します。チェックされている場合は、保存用の変更履歴を出力する設定になっています。

5. 次のファイルを退避します。

Windows インストール先フォルダ¥jdnagent.nid

重要

インターネットゲートウェイサーバと接続する管理用中継サーバの場合は、最後に使用したインターネット接続設定ファイルも退避してください。「rlyigwsetconf -o」コマンドを使用すると、パスワード情報以外のインターネット接続設定ファイルを出力できます。rlyigwsetconf コマンドの詳細は、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の rlyigwsetconf（管理用中継サーバにインターネット接続情報を設定）についての説明を参照してください。

6. 設定ファイルを退避します。

コンフィグレーションファイル（jdn_manager_config.conf）に設定を追加している場合は、コンフィグレーションファイルを退避します。コンフィグレーションファイル（jdn_manager_config.conf）の格納先は次のとおりです。

JP1/IT Desktop Management 2 - Manager のインストール先フォルダ¥mgr¥conf

その他の設定ファイルを追加・編集している場合は、同様に退避してください。

7. リプレース先のコンピュータに、操作ログのバックアップデータを格納します。

手順 3.で操作ログのバックアップデータを退避した場合は、インストール前に、リプレース先のコンピュータで「操作ログの保管先フォルダ」に指定する予定のフォルダに格納しておきます。なお、このフォルダには、操作ログのバックアップデータ以外のデータは格納しないでください。

8. リプレース先のコンピュータに、変更履歴のバックアップデータを格納します。

手順 4.で変更履歴のバックアップデータを退避した場合は、インストール前に、リプレース先のコンピュータで「変更履歴の出力先フォルダ」に指定する予定のフォルダに格納しておきます。なお、このフォルダには、変更履歴のバックアップデータ以外のデータは格納しないでください。

9. リプレースの前後で管理用サーバの IP アドレスおよびホスト名が変わらない場合、リプレース元のコンピュータをネットワークから切断します。

10. リプレース先のコンピュータに、JP1/IT Desktop Management 2 - Manager をカスタムインストールでインストールします。

11. 手順 5.で退避したファイル（jdnagent.nid）を、リプレース先のコンピュータの *Windows インストール先フォルダ* に格納します。

12. 次に示す内容を入力したインベントリ設定ファイル（jdng_inventory.conf）をテキストエディタで作成し、%ALLUSERSPROFILE%¥HITACHI¥jp1itdma¥conf フォルダに格納します。

```
[NodeID]
ReproductionLimit=0
```

13. JP1/IT Desktop Management 2 - Manager をセットアップします。

    リプレース先のコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、セットアップを実行してください。

    管理用中継サーバのリプレースの場合、上位接続先の管理用サーバはリプレース元と同じにしてください。

    操作ログを保管する設定にしている場合は、［操作ログの自動保管の設定］画面で「操作ログの保管先フォルダ」に、手順 7.でバックアップデータを格納したフォルダを指定してください。

    保存用の変更履歴を出力する設定にしている場合は、［保存用の変更履歴の出力設定］画面で「変更履歴の出力先フォルダ」に、手順 8.でバックアップデータを格納したフォルダを指定してください。

14. リプレース先のコンピュータに、退避した設定ファイルを格納します。

    手順 6.でコンフィグレーションファイル（jdn_manager_config.conf）を退避した場合は、リプレース先に格納してください※。コンフィグレーションファイル（jdn_manager_config.conf）の格納先は次のとおりです。

    JP1/IT Desktop Management 2 - Manager のインストール先フォルダ¥mgr¥conf

    その他設定ファイルを退避した場合は、同様に格納してください※。

    注※　すでに設定ファイルが存在する場合は、ファイルを上書きしてください。

15. 手順 2.でバックアップしたデータベースをリストアします。

    リプレース先のコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［データベースマネージャ］から JP1/IT Desktop Management 2 - Manager のデータベースマネージャを起動して、データベースのリストアを実行してください。

16. 各管理用サーバで製品ライセンスを管理している場合は、統括管理用サーバでdistributelicense コマンドを実行して、管理用中継サーバに製品ライセンスの情報を設定します。

17. 統括管理用サーバまたはライセンスの登録を許可されている管理用中継サーバをリプレースしている場合、リプレース先の管理用サーバにライセンスを登録します。

リプレース先のコンピュータにインストールした JP1/IT Desktop Management 2 - Manager のログイン画面で、[ライセンス] ボタンをクリックします。表示されるダイアログで [ライセンスを登録] ボタンをクリックして、ライセンスを登録します。

18. リプレースの前後で管理用サーバの IP アドレスまたはホスト名が変更になる場合、次の手順を参照して必要な設定を実施します。

- 7.9.1　管理用サーバのホスト名を変更する手順
- 7.9.2　管理用サーバの IP アドレスを変更する手順

19. 正しく運用できることを確認します。

リプレース先のコンピュータにインストールした JP1/IT Desktop Management 2 - Manager で、エージェントが管理用サーバに接続されたかどうかを確認します。機器画面の [機器一覧] 画面で、[最終接続確認日時] が更新されていることを確認してください。

[最終接続確認日時] はデフォルトでは表示されていないため、表示されていない場合は [機器一覧] 画面の一覧の項目を右クリックして、[表示項目の選択] から表示されるダイアログで確認してください。[最終接続確認日時] が更新されない場合、利用者のコンピュータで、Windows の [スタート] メニュー－ [すべてのプログラム] － [JP1_IT Desktop Management 2 - Agent] － [管理者ツール] － [セットアップ] からエージェントのセットアップを起動して、接続先にリプレース先の管理用サーバが設定されているかどうかを確認してください。

> **重要**
>
> インターネットゲートウェイサーバと接続する管理用中継サーバの場合は、手順 5 で退避したインターネット接続設定ファイルを、リプレース先の管理用中継サーバとインターネットゲートウェイにあわせてインターネット接続設定ファイルを編集し、適用してください。インターネット接続設定ファイルを適用する手順の詳細は、「7.18　管理用中継サーバをインターネットゲートウェイに接続する手順」を参照してください。

20. リプレース元のコンピュータで、JP1/IT Desktop Management 2 - Manager をアンインストールします。

管理用サーバのリプレースが完了します。

> **ヒント**
>
> リプレース元のコンピュータで取得したバックアップは、リプレース完了後に、必要に応じて削除してください。

ヒント

リプレース完了後にエージェントが管理用サーバに接続されたかどうかは、機器画面の［機器一覧］画面で、［最終接続確認日時］が更新されていることで確認できます。エージェントが接続されない場合、利用者のコンピュータで、エージェントのセットアップから接続先が正しく設定されているかどうか確認してください。

関連リンク

- 1.2.2　JP1/IT Desktop Management 2 - Manager をインストールする手順（単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバの場合）
- 1.2.4　単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順
- 7.1　管理用サーバをリプレースする
- 8.11　distributelicense（ライセンスの分配）

7.2 単数サーバ構成システムの管理用サーバを複数サーバ構成システムの統括管理用サーバに切り替える手順

単数サーバ構成システムの管理用サーバを、複数サーバ構成システムの統括管理用サーバに切り替えるには、[セットアップ]の[サーバ構成の選択]画面で[複数サーバ構成]を選択します。

単数サーバ構成システムの管理用サーバを複数サーバ構成システムの統括管理用サーバに切り替えるには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の[スタート]メニューから[すべてのプログラム]－[JP1_IT Desktop Management 2 - Manager]－[ツール]－[セットアップ]を選択します。
3. セットアップ画面で[次へ]ボタンをクリックします。
4. [セットアップの選択]画面で、[設定変更]を選択して[次へ]ボタンをクリックします。
5. [サーバ構成の選択]画面が表示されるまで、[次へ]ボタンをクリックします。
6. [サーバ構成]で[複数サーバ構成]を選択します。
7. [セットアップの確認]画面が表示されるまで、[次へ]ボタンをクリックします。
8. [セットアップの確認]画面で設定内容を確認して、[次へ]ボタンをクリックします。
9. [リモートインストールマネージャを使用した配布のセットアップ]画面で、[OK]ボタンをクリックします。

   セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します]画面が表示されます。

   サービスの停止が必要な場合は、サービスの停止を確認するダイアログが表示されます。[OK]ボタンをクリックしてサービスを停止してください。
10. [セットアップを終了します]画面で、[OK]ボタンをクリックします。

単数サーバ構成システムの管理用サーバが複数サーバ構成システムの統括管理用サーバに切り替えられます。

> **ヒント**
>
> 切り替えと同時に JP1/IT Desktop Management 2 - Manager をバージョンアップしたい場合は、先にバージョンアップしてからサーバ構成を切り替えてください。

関連リンク

- 5.1 JP1/IT Desktop Management 2 - Manager を上書きインストールする手順

7.3　管理用サーバを管理用中継サーバに切り替える手順

単数サーバ構成システムの管理用サーバおよび複数サーバ構成システムの統括管理用サーバを複数サーバ構成システムの管理用中継サーバに切り替えるには、［インストールする Manager の種別］で［管理用中継サーバ］を選択して上書きインストールします。そのあと、管理用中継サーバの上位接続先を指定します。

ヒント

クラスタ環境の管理用サーバ、および JP1/IT Desktop Management 2 - Agent がインストールされたコンピュータは、管理用中継サーバに切り替えられません。

また、管理用中継サーバを上書きインストールするときは、Manager の種別を変更できません。

管理用サーバを管理用中継サーバに切り替えるには：

1. 管理用サーバの JP1/IT Desktop Management 2 - Manager を切り替え先の複数サーバ構成システムと同一のバージョンで上書きインストールします。
   上書きインストール時に、［インストールする Manager の種別］で［管理用中継サーバ］を選択してください。
2. 管理用中継サーバの上位接続先を指定します。

単数サーバ構成システムの管理用サーバおよび複数サーバ構成システムの統括管理用サーバを、複数サーバ構成システムの管理用中継サーバに切り替えられます。

ヒント

切り替えと同時に JP1/IT Desktop Management 2 - Manager をバージョンアップしたい場合は、先にバージョンアップしてからインストールする Manager の種別を切り替えてください。

ヒント

単数サーバ構成システムの管理用サーバを複数サーバ構成システムの管理用中継サーバに切り替えた場合、単数サーバ構成システムの管理用サーバに登録されていた製品ライセンスを、複数サーバ構成システムの統括管理用サーバに登録できます。なお、複数サーバ構成システムで製品ライセンスを管理用中継サーバごとに管理する場合は、統括管理用サーバで `distributelicense` コマンドを実行して、各管理用中継サーバに製品ライセンスの情報を設定する必要があります。

関連リンク

- 1.3.3　管理用中継サーバに製品ライセンスの情報を設定する手順
- 5.1　JP1/IT Desktop Management 2 - Manager を上書きインストールする手順

- 3.6　管理用中継サーバの上位接続先の設定を変更する手順
- 5.1　JP1/IT Desktop Management 2 - Manager を上書きインストールする手順

7.4 リモートインストールマネージャだけを導入済みのコンピュータをリプレースする手順

リモートインストールマネージャを導入済みのコンピュータをリプレースするには：

1. リプレース元のコンピュータから必要に応じて、Remote Install Manager をアンインストールします。
2. コンピュータをリプレースします。
3. リプレース後のコンピュータに、Remote Install Manager をインストールします。
   インストールタイプは［カスタムインストール］を選択し、インストールするコンポーネントとして Remote Install Manager を選択します。なお、Manager はインストールする必要がないので、Manager のプルダウンメニューで［この機能を使用できないようにします。］を選択します。

リモートインストールマネージャを導入済みのコンピュータのリプレースが完了します。

関連リンク

- 1.9.1　リモートインストールマネージャだけをインストールする手順

7.5　エージェント導入済みのコンピュータをリプレースする手順

エージェント導入済みのコンピュータをリプレースするには：

1. コンピュータから、エージェントをアンインストールします。
2. コンピュータをリプレースします。
3. リプレース後のコンピュータに、エージェントをインストールします。

エージェント導入済みのコンピュータのリプレースが完了します。

7.6　中継システムをリプレースする手順

中継システムのリプレースとは、現在中継システムがインストールされているコンピュータの中継システムとしての機能を、別のコンピュータに移し替えることです。

中継システムをリプレースするには、リプレース前のコンピュータの情報をバックアップし、リプレース後のコンピュータにリストアする必要があります。

リプレース前のコンピュータの情報をバックアップするには：

1. リプレース前の中継システムを導入済みのコンピュータで中継システムのサービスを停止します。

   ［コントロールパネル］－［管理ツール］－［サービス］で、エージェントサービス（JP1_ITDM2_Agent Service）を停止します。なお、エージェントサービスは中継システムの場合だけ停止できます。

2. プロセスがすべて停止したことを確認します。

   エージェントサービスを停止すると、次のプロセスが終了します。タスクマネージャなどで、次のプロセスが表示されていないことを確認してください。表示されている場合、プロセスは動作中のため、プロセスが終了して表示が消えるまで待機してください。

   - jdngdmpsetup.exe
   - jdngwinst.exe
   - jdngsite.exe
   - jdngschserv.exe
   - jdngsrvmain.exe

3. リプレース前の中継システムで、次のレジストリをバックアップします。

   OS のレジストリエディターを起動してエクスポートすることで、レジストリをバックアップできます。

   OS が 32 ビット版の場合

   HKEY_LOCAL_MACHINE¥SOFTWARE¥HITACHI¥JP1/IT Desktop Management - Agent¥DMP

   OS が 64 ビット版の場合

   HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Hitachi¥JP1/IT Desktop Management - Agent¥DMP

4. 次のファイルをバックアップします。

   次のパス下のファイルおよびフォルダを、手動でバックアップしてください。

   - *中継システムのインストール先フォルダ*¥MASTER¥DB 下のファイル
   - *中継システムのインストール先フォルダ*¥SCHEDULE 下のファイル
   - *中継システムのインストール先フォルダ*¥SERVER 下のファイル

- *中継システムのインストール先フォルダ*¥SITESRV 下のファイル
- *中継システムのインストール先フォルダ*¥DMPSITE¥¥COLLECTION 下のファイル
- *Windows インストール先フォルダ*¥jdnagent.nid

リプレース前の中継システムの情報がバックアップされます。

リプレース後のコンピュータにバックアップ情報をリストアするには：

1. リプレース後のコンピュータに中継システムをインストールします。
   インストールが完了すると、セットアップ画面が表示されます。
2. セットアップ画面の［キャンセル］ボタンをクリックします。
3. リプレース後の中継システムでサービスを停止します。
   ［コントロールパネル］－［管理ツール］－［サービス］で、エージェントサービス（JP1_ITDM2_Agent Service）を停止します。なお、エージェントサービスは中継システムの場合だけ停止できます。
4. プロセスがすべて停止したことを確認します。
   エージェントサービスを停止すると、次のプロセスが終了します。タスクマネージャなどで、次のプロセスが表示されていないことを確認してください。表示されている場合、プロセスは動作中のため、プロセスが終了して表示が消えるまで待機してください。
   - jdngdmpsetup.exe
   - jdngwinst.exe
   - jdngsite.exe
   - jdngschserv.exe
   - jdngsrvmain.exe
5. リプレース後の中継システムにバックアップした情報をリストアします。
   リプレース前にバックアップしたファイル情報とレジストリをリストアします。ファイル情報のリストア先は、バックアップしたフォルダと同じ場所です。レジストリは、OS のレジストリエディターを起動しインポートすることでリストアできます。
6. 次のように入力したインベントリ設定ファイル（jdng_inventory.conf）をテキストエディタで作成し、%ALLUSERSPROFILE%¥HITACHI¥jp1itdma¥conf フォルダに格納します。
   [NodeID]
   ReproductionLimit=0
7. リプレース後の中継システムをセットアップします。
   スタートメニューの［JP1_IT Desktop Management 2 - Agent］－［管理者ツール］からセットアップを起動します。セットアップの起動後、［管理用サーバ］の［ホスト名または IP アドレス］および［ポート番号］を入力し、［OK］ボタンをクリックします。

8. 中継システムのコンピュータからいったんログオフしたあと、再度ログインします。

中継システムのリプレースが完了します。

> **重要**
>
> リプレース前の中継システムを上位システムとして設定しているエージェントは、エージェント設定の［基本設定］で、上位システムをリプレース後の中継システムに変更する必要があります。

関連リンク

- 1.8.1　中継システムのインストール方法
- 1.8.2　中継システムを提供媒体からインストールする手順
- 1.8.3　中継システムをセットアップする手順
- 6.5　中継システムをアンインストールする手順
- 1.8.3　中継システムをセットアップする手順

7.7　ネットワークモニタを有効にしたコンピュータをリプレースする手順

ネットワークモニタを有効にしたコンピュータをリプレースするには、いったんネットワークモニタを無効にする必要があります。ネットワークモニタを無効にする手順および有効にする手順については、「6.6 ネットワークモニタを無効にする手順」および「2.6.2　ネットワークモニタを有効にする手順」を参照してください。

ネットワークモニタを有効にしたコンピュータをリプレースするには：

1. リプレース元のコンピュータのネットワークモニタを無効にします。
2. リプレース元のコンピュータから、エージェントをアンインストールします。
3. コンピュータをリプレースします。
4. リプレース先のコンピュータに、エージェントをインストールします。
5. リプレース先のコンピュータの、ネットワークモニタを有効にします。

ネットワークモニタを有効にしたコンピュータのリプレースが完了します。

7.8　インターネットゲートウェイをリプレースする手順

インターネットゲートウェイをリプレースするには：

> **重要**
>
> リプレース前後で、インターネットゲートウェイの IP アドレスおよびホスト名は同一にしてください。

1. World Wide Web Publishing Service サービス※を停止します。

   注※　Windows Server 2025、Windows Server 2022、Windows Server 2019 または Windows Server 2016 の場合、「World Wide Web 発行サービス」です。

2. コンピュータから、エージェントをアンインストールします。

3. インターネットゲートウェイに中継システムを導入している場合、リプレース前のコンピュータの情報をバックアップします。

   詳細な手順は、「7.6　中継システムをリプレースする手順」を参照してください。

4. リプレース先のコンピュータでインターネットゲートウェイを構築します。

   詳細な手順は、「2.11.1　インターネットゲートウェイを構築する手順」を参照してください。

5. リプレース後に中継システムを導入する場合、手順 3 でバックアップしたコンピュータの情報をリストアします。

   詳細な手順は、「7.6　中継システムをリプレースする手順」を参照してください。

インターネットゲートウェイのリプレースが完了します。

7.9　システム構成要素のホスト名および IP アドレスを変更する

7.9.1　管理用サーバのホスト名を変更する手順

管理用サーバのホスト名を変更したい場合は、次の項目を再設定します。

- エージェントの接続先（接続先をホスト名で指定している場合）
- リモートインストールマネージャのログイン画面の接続先（接続先をホスト名で指定している場合）
- Asset Console のデータソース

> **重要**
>
> 管理用中継サーバのホスト名を変更した場合、管理用中継サーバを再起動したあと、リモートインストールマネージャを起動して、管理用中継サーバのシステム構成情報のホスト名が変更されていることを確認してください。ホスト名が変更されていなかったときは、ホスト名を変更した管理用中継サーバのシステム構成情報を削除し、しばらく経過したあと、変更後のホスト名でシステム構成情報が登録されていることを確認してください。

配下の管理用中継サーバの接続先（複数サーバ構成の場合に接続先をホスト名で指定しているとき）

配下の管理用中継サーバで、セットアップの［管理用中継サーバの設定］－［ホスト名または IP アドレス］に、変更後のホスト名を設定します。手順の詳細については、「3.6　管理用中継サーバの上位接続先の設定を変更する手順」を参照してください。

配下の管理用中継サーバの接続先のホスト名が変更されます。

エージェントの接続先（接続先をホスト名で指定している場合）

1. エージェントの上位システムへの接続方法に応じて、情報を変更します。

   上位システムへの接続に接続先設定ファイル（itdmhost.conf）を使用しているときは、エージェントの接続先設定ファイル（itdmhost.conf）を変更してください。

   上位システムへの接続に上位接続先情報ファイル（dmhost.txt）を使用しているときは、エージェントの上位接続先情報ファイル（dmhost.txt）を変更してください。

   上位システムへの接続に上位システムアドレス格納ファイル（SERVERIP.ini）を使用しているときは、エージェントの上位システムアドレス格納ファイル（SERVERIP.ini）を変更してください。

   > **ヒント**
   >
   > 設定ファイルの変更については次に示す個所を参照してください。
   >
   > 接続先設定ファイル（itdmhost.conf）
   >
   > (2)　接続先設定ファイル（itdmhost.conf）の作成

上位接続先情報ファイル（dmhost.txt）

マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、上位接続先情報ファイル（dmhost.txt）の作成についての説明

上位システムアドレス格納ファイル（SERVERIP.ini）

マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、上位システムアドレス格納ファイルの形式についての説明

2. **エージェント設定の［基本設定］－［管理用サーバ］の［ホスト名または IP アドレス］に、変更後のホスト名を設定します。**

   ただし、エージェント設定を変更したときに電源が入っていないコンピュータは、個別にエージェントのセットアップ画面から設定を変更する必要があります。

エージェントの接続先が変更されます。

リモートインストールマネージャのログイン画面の接続先（接続先をホスト名で指定している場合）

リモートインストールマネージャのログイン画面の［管理用サーバ］にホスト名を指定している場合、変更後のホスト名に変更します。

Asset Console のデータソース

Asset Console のセットアップ画面から、次の手順に従ってデータソースを再作成します。

1. **サーバセットアップを起動します。**
2. **［データソースの作成］をクリックします。**
3. **［接続先一覧］で［JP1/Desktop Management 2 - Manager］を選択し、［次へ］ボタンをクリックします。**
4. **［サーバ］にホスト名を設定している場合は、変更後のホスト名を入力します。**
5. **［OK］ボタンをクリックします。**

Asset Console のデータソースが再作成されます。

7.9.2 管理用サーバの IP アドレスを変更する手順

管理用サーバの IP アドレスを変更したい場合は、セットアップで IP アドレスの設定を変更したあと、次の項目を再設定します。

- エージェントの接続先（接続先を IP アドレスで指定している場合）
- ネットワークへの接続を許可しない機器の特例接続の設定
- リモートインストールマネージャのログイン画面の接続先（接続先を IP アドレスで指定している場合）

- Asset Console のデータソース

> **重要**
>
> 管理用中継サーバの IP アドレスを変更した場合、管理用中継サーバを再起動したあと、リモートインストールマネージャを起動して、管理用中継サーバのシステム構成情報の IP アドレスが変更されていることを確認してください。IP アドレスが変更されていなかったときは、IP アドレスを変更した管理用中継サーバのシステム構成情報を削除し、しばらく経過したあと、変更後の IP アドレスでシステム構成情報が登録されていることを確認してください。

管理用サーバの IP アドレスを変更するには：

1. Asset Console やリモートインストールマネージャなどで実行中の処理を停止します。
2. 管理用サーバでstopservice コマンドを実行し、サービスを停止します。※

   注※　管理用サーバのサービス起動時点で既に有効であった IP アドレスに変更する場合は、 管理用サーバのサービス停止は不要です。。
3. JP1/IT Desktop Management 2 - Manager のセットアップを起動し、［データベースの設定］画面のデータベースへのアクセス時の IP アドレスに、変更後の IP アドレスを設定し、セットアップを実行します。

管理用サーバの IP アドレスが変更されます。引き続き、次のとおり各項目を再設定します。

配下の管理用中継サーバの接続先（複数サーバ構成の場合に接続先を IP アドレスで指定しているとき）

配下の管理用中継サーバで、セットアップの［管理用中継サーバの設定］－［ホスト名または IP アドレス］に、変更後の IP アドレスを設定します。手順の詳細については、「3.6　管理用中継サーバの上位接続先の設定を変更する手順」を参照してください。

配下の管理用中継サーバの接続先の IP アドレスが変更されます。

エージェントの接続先（接続先を IP アドレスで指定している場合）

1. エージェントの上位システムへの接続方法に応じて、情報を変更します。

   上位システムへの接続に接続先設定ファイル（itdmhost.conf）を使用しているときは、エージェントの接続先設定ファイル（itdmhost.conf）を変更してください。

   上位システムへの接続に上位接続先情報ファイル（dmhost.txt）を使用しているときは、エージェントの上位接続先情報ファイル（dmhost.txt）を変更してください。

   上位システムへの接続に上位システムアドレス格納ファイル（SERVERIP.ini）を使用しているときは、エージェントの上位システムアドレス格納ファイル（SERVERIP.ini）を変更してください。

   > **ヒント**
   >
   > 設定ファイルの変更については次に示す個所を参照してください。

接続先設定ファイル（itdmhost.conf）

(2)　接続先設定ファイル（itdmhost.conf）の作成

上位接続先情報ファイル（dmhost.txt）

マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、上位接続先情報ファイル（dmhost.txt）の作成についての説明

上位システムアドレス格納ファイル（SERVERIP.ini）

マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、上位システムアドレス格納ファイルの形式についての説明

2. エージェント設定の［基本設定］－［管理用サーバ］の［ホスト名または IP アドレス］に、変更後の IP アドレスを設定します。

ただし、エージェント設定を変更したときに電源が入っていないコンピュータは、個別にエージェントのセットアップ画面から設定を変更する必要があります。

エージェントの接続先が変更されます。

ネットワークへの接続を許可しない機器の特例接続の設定

［ネットワーク制御の設定］画面で、［ネットワークへの接続を許可しない機器の特例接続］から変更前の管理用サーバの IP アドレスを削除し、変更後の管理用サーバの IP アドレスを追加してください。

リモートインストールマネージャのログイン画面の接続先（接続先を IP アドレスで指定している場合）

リモートインストールマネージャのログイン画面の［管理用サーバ］に IP アドレスを指定している場合、変更後の IP アドレス名に変更します。

Asset Console のデータソース

Asset Console のセットアップ画面から、次の手順に従ってデータソースを再作成します。

1. サーバセットアップを起動します。
2. ［データソースの作成］をクリックします。
3. ［接続先一覧］で［JP1/Desktop Management 2 - Manager］を選択し、［次へ］ボタンをクリックします。
4. ［サーバ］に IP アドレスを設定している場合は、変更後の IP アドレスを入力します。
5. ［OK］ボタンをクリックします。

Asset Console のデータソースが再作成されます。

7.9.3　中継システムのホスト名または IP アドレスを変更する手順

中継システムのホスト名または IP アドレスを変更するには：

1. リモートインストールマネージャで実行中のジョブを削除します。
   ホスト名または IP アドレスを変更する中継システムを経由するジョブをすべて削除してください。
2. 中継システムのホスト名または IP アドレスを変更します。
3. 操作画面の［機器一覧］画面およびリモートインストールマネージャの［システム構成］ウィンドウで、ホスト名または IP アドレスが変更されたことを確認します。
4. ホスト名または IP アドレスを変更した中継システムに接続しているエージェント機器の接続先を変更します。
   操作画面の設定画面から［Windows エージェント設定とインストールセットの作成］を選択し、ホスト名または IP アドレスを変更した中継システムに接続しているエージェントに適用しているエージェント設定の［編集］ボタンをクリックしてください。
   表示されたエージェント設定の［基本設定］－［リモートインストールマネージャを使用した配布用の上位システム］－［ホスト名または IP アドレス］を変更後のホスト名または IP アドレスに変更してください。

中継システムのホスト名または IP アドレスの変更が完了します。

7.9.4　クラスタシステムの論理ホスト名を変更する手順

クラスタシステムの論理ホスト名を変更したい場合は、セットアップでホスト名の設定を変更したあと、次の項目を再設定します。

- エージェントの接続先（接続先をホスト名で指定している場合）
- リモートインストールマネージャのログイン画面の接続先（接続先をホスト名で指定している場合）
- Asset Console のデータソース

クラスタシステムの論理ホスト名を変更するには：

1. Asset Console やリモートインストールマネージャなどで実行中の処理を停止します。
2. 「2.10.2　現用系サーバでリソースグループを作成する手順」に記載されているリソースをオフラインにします。
3. 現用系サーバのセットアップの［クラスタ環境］画面で論理ホスト名を変更後のホスト名に設定し、セットアップを実行します。
4. セットアップで出力された次のセットアップファイルを待機系サーバにコピーします。

JP1/IT Desktop Management 2 - Manager のインストールフォルダ
¥mgr¥conf¥jdn_manager_setup.conf

5. リソースグループの所有者を待機系サーバに移動します。

6. 待機系サーバでセットアップを起動し、手順 4.でコピーしたセットアップファイルを指定して、セットアップを実行します。

7. リソースグループの所有者を現用系サーバに移動します。

8. 「2.10.2　現用系サーバでリソースグループを作成する手順」に記載されているリソースをオフラインにします。

クラスタシステムの論理ホスト名が変更されます。引き続き、次のとおり各項目を再設定します。

エージェントの接続先（接続先をホスト名で指定している場合）

1. エージェントの上位システムへの接続方法に応じて、情報を変更します。

   上位システムへの接続に接続先設定ファイル（itdmhost.conf）を使用しているときは、エージェントの接続先設定ファイル（itdmhost.conf）を変更してください。

   上位システムへの接続に上位接続先情報ファイル（dmhost.txt）を使用しているときは、エージェントの上位接続先情報ファイル（dmhost.txt）を変更してください。

   上位システムへの接続に上位システムアドレス格納ファイル（SERVERIP.ini）を使用しているときは、エージェントの上位システムアドレス格納ファイル（SERVERIP.ini）を変更してください。

   ヒント

   設定ファイルの変更については次に示す個所を参照してください。

   接続先設定ファイル（itdmhost.conf）

   (2)　接続先設定ファイル（itdmhost.conf）の作成

   上位接続先情報ファイル（dmhost.txt）

   マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、上位接続先情報ファイル（dmhost.txt）の作成についての説明

   上位システムアドレス格納ファイル（SERVERIP.ini）

   マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、上位システムアドレス格納ファイルの形式についての説明

2. エージェント設定の［基本設定］－［管理用サーバ］の［ホスト名または IP アドレス］に、変更後のホスト名を設定します。

   ただし、エージェント設定を変更したときに電源が入っていないコンピュータは、個別にエージェントのセットアップ画面から設定を変更する必要があります。

エージェントの接続先が変更されます。

リモートインストールマネージャのログイン画面の接続先（接続先をホスト名で指定している場合）

リモートインストールマネージャのログイン画面の［管理用サーバ］にホスト名を指定している場合、変更後のホスト名に変更します。

Asset Console のデータソース

Asset Console のセットアップ画面から、次の手順に従ってデータソースを再作成します。

1. サーバセットアップを起動します。
2. ［データソースの作成］をクリックします。
3. ［接続先一覧］で［JP1/Desktop Management 2 - Manager］を選択し、［次へ］ボタンをクリックします。
4. ［サーバ］にホスト名を設定している場合は、変更後のホスト名を入力します。
5. ［OK］ボタンをクリックします。

Asset Console のデータソースが再作成されます。

7.9.5　クラスタシステムの論理 IP アドレスを変更する手順

クラスタシステムの論理 IP アドレスを変更したい場合は、セットアップで IP アドレスの設定を変更したあと、次の項目を再設定します。

- エージェントの接続先（接続先を IP アドレスで指定している場合）
- ネットワークへの接続を許可しない機器の特例接続の設定
- リモートインストールマネージャのログイン画面の接続先（接続先を IP アドレスで指定している場合）
- Asset Console のデータソース

クラスタシステムの論理 IP アドレスを変更するには：

1. Asset Console やリモートインストールマネージャなどで実行中の処理を停止します。
2. 「2.10.2　現用系サーバでリソースグループを作成する手順」に記載されているリソースをオフラインにします。
3. 現用系サーバのセットアップの［クラスタ環境］画面で論理 IP アドレスを変更後の IP アドレスに設定し、セットアップを実行します。
4. セットアップで出力された次のセットアップファイルを待機系サーバにコピーします。

   JP1/IT Desktop Management 2 - Manager のインストールフォルダ
   ¥mgr¥conf¥jdn_manager_setup.conf

5. リソースグループの所有者を待機系サーバに移動します。

6. 待機系サーバでセットアップを起動し、手順 4.でコピーしたセットアップファイルを指定して、セットアップを実行します。

7. リソースグループの所有者を現用系サーバに移動します。

8. 「2.10.2　現用系サーバでリソースグループを作成する手順」に記載されているリソースをオフラインにします。

クラスタシステムの論理 IP アドレスが変更されます。引き続き、次のとおり各項目を再設定します。

エージェントの接続先（接続先を IP アドレスで指定している場合）

1. エージェントの上位システムへの接続方法に応じて、情報を変更します。

   上位システムへの接続に接続先設定ファイル（itdmhost.conf）を使用しているときは、エージェントの接続先設定ファイル（itdmhost.conf）を変更してください。

   上位システムへの接続に上位接続先情報ファイル（dmhost.txt）を使用しているときは、エージェントの上位接続先情報ファイル（dmhost.txt）を変更してください。

   上位システムへの接続に上位システムアドレス格納ファイル（SERVERIP.ini）を使用しているときは、エージェントの上位システムアドレス格納ファイル（SERVERIP.ini）を変更してください。

   > **ヒント**
   >
   > 設定ファイルの変更については次に示す個所を参照してください。
   >
   > 接続先設定ファイル（itdmhost.conf）
   >
   > (2)　接続先設定ファイル（itdmhost.conf）の作成
   >
   > 上位接続先情報ファイル（dmhost.txt）
   >
   > マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、上位接続先情報ファイル（dmhost.txt）の作成についての説明
   >
   > 上位システムアドレス格納ファイル（SERVERIP.ini）
   >
   > マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、上位システムアドレス格納ファイルの形式についての説明

2. エージェント設定の［基本設定］－［管理用サーバ］の［ホスト名または IP アドレス］に、変更後の IP アドレスを設定します。

   ただし、エージェント設定を変更したときに電源が入っていないコンピュータは、個別にエージェントのセットアップ画面から設定を変更する必要があります。

エージェントの接続先が変更されます。

ネットワークへの接続を許可しない機器の特例接続の設定

［ネットワーク制御の設定］画面で、［ネットワークへの接続を許可しない機器の特例接続］から変更前の管理用サーバの IP アドレスを削除し、変更後の管理用サーバの IP アドレスを追加してください。

リモートインストールマネージャのログイン画面の接続先（接続先を IP アドレスで指定している場合）

リモートインストールマネージャのログイン画面の［管理用サーバ］に IP アドレスを指定している場合、変更後の IP アドレス名に変更します。

Asset Console のデータソース

Asset Console のセットアップ画面から、次の手順に従ってデータソースを再作成します。

1. サーバセットアップを起動します。
2. ［データソースの作成］をクリックします。
3. ［接続先一覧］で［JP1/Desktop Management 2 - Manager］を選択し、［次へ］ボタンをクリックします。
4. ［サーバ］に IP アドレスを設定している場合は、変更後の IP アドレスを入力します。
5. ［OK］ボタンをクリックします。

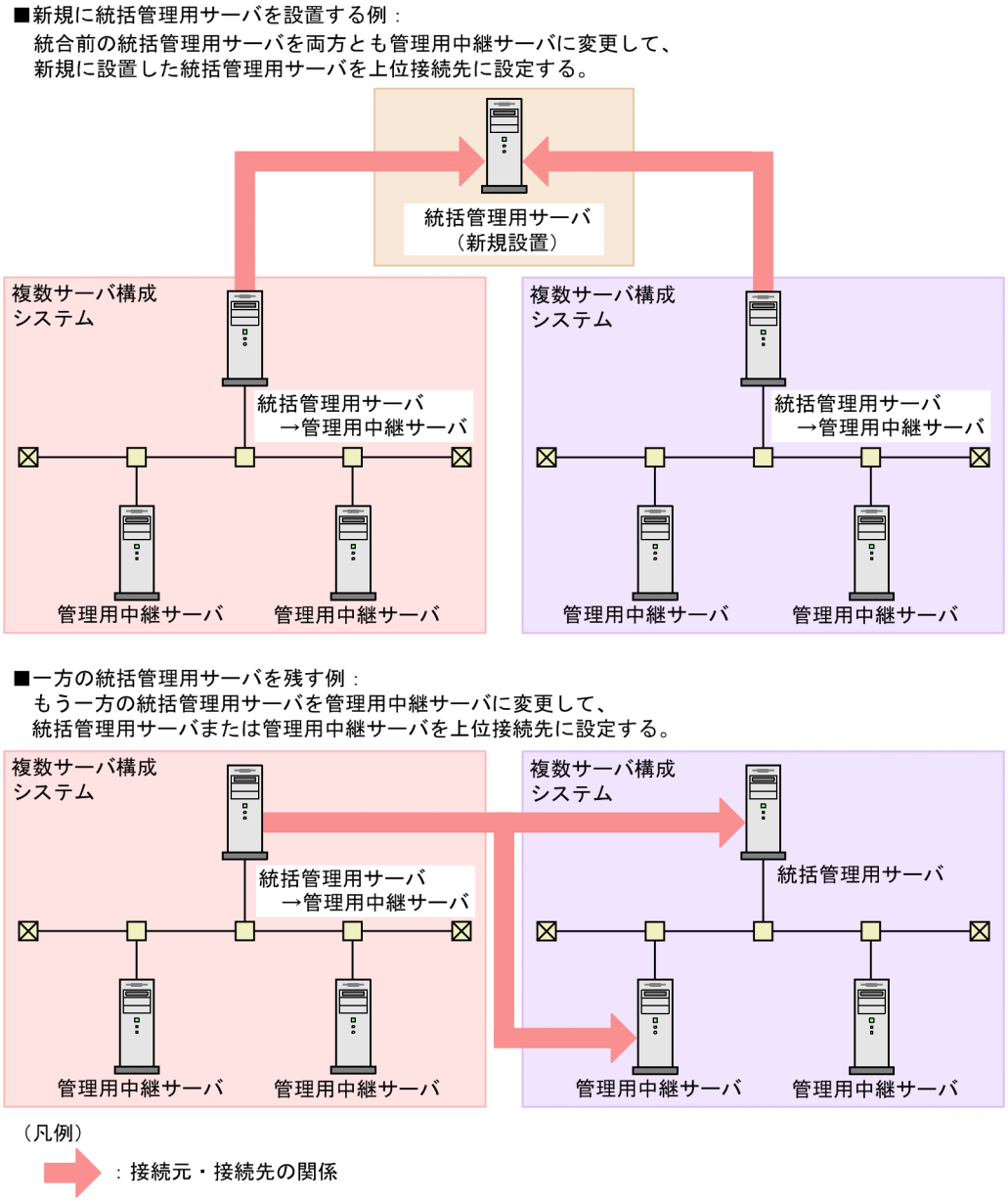
Asset Console のデータソースが再作成されます。

7.10　複数サーバ構成システムを統合する手順

ある複数サーバ構成システムを別の複数サーバ構成システムと統合するには、次に示す方法があります。

- 新規に統括管理用サーバを設置し、統合前の統括管理用サーバを両方とも管理用中継サーバに変更する
- 一方の統括管理用サーバを残し、もう一方を管理用中継サーバに変更する

複数サーバ構成システムの統合の例を次の図に示します。



複数サーバ構成システムを統合する手順を次に示します。

複数サーバ構成システムを統合するには：

1. システムの統合に当たって新規に統括管理用サーバを設置する場合は、統括管理用サーバにするコンピュータに JP1/IT Desktop Management 2 をインストールします。

2. 管理用中継サーバ（統合前の統括管理用サーバ）に、JP1/IT Desktop Management 2 を上書きインストールします。

3. 管理用中継サーバ（統合前の統括管理用サーバ）に登録されていた製品ライセンスを、統合後の統括管理用サーバに登録します。

4. 管理用中継サーバ（統合前の統括管理用サーバ）に統合後の上位接続先を設定します。

   管理用中継サーバ（統合前の統括管理用サーバ）で、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、セットアップを実行してください。

5. 管理用中継サーバ（統合前の統括管理用サーバ）が手順 4.で設定した上位接続先の下位に接続されていることを確認します。

   手順 4.で設定した上位接続先のホーム画面の［配下の管理用サーバの状況］タブで複数サーバ構成システムの階層構成を確認できます。

6. 統合後の複数サーバ構成システムで製品ライセンスを管理用サーバごとに管理する場合は、統合後の統括管理用サーバで`distributelicense` コマンドを実行して、各管理用中継サーバに製品ライセンスの情報を設定します。

7. 統合後の複数サーバ構成システムでリモートインストールマネージャを使用した配布を利用する場合、手順 4.で設定した上位接続先、およびその上位の管理用サーバのリモートインストールマネージャで、管理用中継サーバ（統合前の統括管理用サーバ）をあて先とした「システム構成情報の取得」ジョブを実行します。

   リモートインストールマネージャでのジョブの作成および実行については、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、ジョブの作成についての説明を参照してください。

8. 管理用中継サーバ（統合前の統括管理用サーバ）で、上位の管理用サーバにすべての機器情報を通知します。

   上位の管理用サーバにすべての機器情報を通知するには、機器画面の［機器情報］－［機器一覧］画面で、［操作メニュー］の［上位の管理用サーバにすべての機器情報を通知する］を選択します。

> **重要**
>
> 上位の管理用サーバに通知する機器情報との整合性を保つため、通知が完了するまで、操作画面およびコマンドで管理用中継サーバ（統合前の統括管理用サーバ）の機器情報を更新しないでください。すべての機器情報の通知が完了したかどうかは、管理用中継サーバ（統合前の統括管理用サーバ）のイベント画面で確認できます。

9. 手順 8.の通知先が管理用中継サーバの場合は、統括管理用サーバが機器情報を受信するまで、下位の階層から順に、手順 8.と同様の手順で上位の管理用サーバに機器情報を通知します。

10. 必要に応じて、手順 4.で設定した上位接続先で JP1/IT Desktop Management 2 の設定を見直します。

関連リンク

- 1.2.2　JP1/IT Desktop Management 2 - Manager をインストールする手順（単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバの場合）
- 1.2.3　JP1/IT Desktop Management 2 - Manager をインストールする手順（管理用中継サーバの場合）
- 1.2.4　単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順
- 1.2.5　管理用中継サーバをセットアップする手順
- 1.3.3　管理用中継サーバに製品ライセンスの情報を設定する手順
- 8.7　startservice（サービス開始）
- 8.11　distributelicense（ライセンスの分配）

7.11　管理用中継サーバの上位接続先を切り替える手順

管理用中継サーバの上位接続先を複数サーバ構成内の別の管理用サーバに切り替えるには、上位接続先をセットアップで変更します。管理用中継サーバの上位接続先を切り替える手順を次に示します。

管理用中継サーバの上位接続先を切り替えるには：

1. 切り替え元の管理用中継サーバの上位接続先を、セットアップで変更します。

   切り替え元の管理用中継サーバで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、セットアップを実行してください。

2. 切り替え元の管理用中継サーバが手順 1.で設定した上位接続先の下位に接続されていることを確認します。

   手順 1.で設定した上位接続先のホーム画面の［配下の管理用サーバの状況］タブで複数サーバ構成システムの階層構成を確認できます。

3. 各管理用サーバで製品ライセンスを管理している場合は、統括管理用サーバでdistributelicense コマンドを実行して、各管理用中継サーバに製品ライセンスの情報を設定します。

4. リモートインストールマネージャを使用した配布を利用する場合、手順 1.で設定した上位接続先、およびその上位の管理用サーバのリモートインストールマネージャで、切り替え元の管理用中継サーバをあて先とした「システム構成情報の取得」ジョブを実行します。

   リモートインストールマネージャでのジョブの作成および実行については、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の、ジョブの作成についての説明を参照してください。

5. 切り替え元の管理用中継サーバおよびその配下の管理用サーバに、切り替え前の上位の管理用サーバから適用されたハードウェア資産情報の追加管理項目およびソフトウェア検索条件が残っている場合は、それぞれの設定を削除します。

   ハードウェア資産情報の追加管理項目を削除するには、設定画面の［資産管理］－［資産管理項目の設定］画面で削除したい項目を選択して［削除］ボタンをクリックします。

   ソフトウェア検索条件を削除するには、設定画面の［機器］－［ソフトウェア検索条件の設定］画面で削除したい条件を選択して［削除］ボタンをクリックします。

6. 切り替え元の管理用サーバで、上位の管理用サーバにすべての機器情報を通知します。

   上位の管理用サーバにすべての機器情報を通知するには、機器画面の［機器情報］－［機器一覧］画面で、［操作メニュー］の［上位の管理用サーバにすべての機器情報を通知する］を選択します。

> **重要**
>
> 上位の管理用サーバに通知する機器情報との整合性を保つため、通知が完了するまで、操作画面およびコマンドで切り替え元の管理用サーバの機器情報を更新しないでください。すべての機器情報の通知が完了したかどうかは、切り替え元の管理用サーバのイベント画面で確認できます。

7. 手順 6.の通知先が管理用中継サーバの場合は、統括管理用サーバが機器情報を受信するまで、下位の階層から順に、手順 6.と同様の手順で上位の管理用サーバに機器情報を通知します。

8. 必要に応じて、手順 1.で設定した上位接続先で JP1/IT Desktop Management 2 の設定を見直します。

関連リンク

- 1.2.2　JP1/IT Desktop Management 2 - Manager をインストールする手順（単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバの場合）
- 1.2.3　JP1/IT Desktop Management 2 - Manager をインストールする手順（管理用中継サーバの場合）
- 1.2.4　単数サーバ構成の管理用サーバまたは複数サーバ構成の統括管理用サーバをセットアップする手順
- 1.2.5　管理用中継サーバをセットアップする手順
- 1.3.3　管理用中継サーバに製品ライセンスの情報を設定する手順
- 8.7　startservice（サービス開始）
- 8.11　distributelicense（ライセンスの分配）

7.12　エージェントが接続する管理用サーバを切り替える手順

エージェントが接続する管理用サーバを切り替えるには：

1. 切り替え元の管理用サーバの操作画面で設定画面を表示します。
2. メニューエリアで［エージェント］－［Windows エージェント設定とインストールセットの作成］を選択します。
3. インフォメーションエリアで、接続先を切り替えたいエージェントに割り当てられているエージェント設定の［編集］ボタンをクリックします。
4. ［エージェント設定の編集］ダイアログで［基本設定］－［管理用サーバ］－［ホスト名または IP アドレス］を切り替え先の管理用サーバのホスト名または IP アドレスに変更します。

   ［ホスト名または IP アドレス］に指定する値は、セットアップの［アドレス解決の設定］で選択した項目によって異なります。

   ［アドレス解決の設定］で「ホスト名」を選択したとき

   - ホスト名で指定してください。
   - DNS サーバを使用している環境では、完全修飾ドメイン名（ホスト名のあとにピリオドとドメイン名を表記した名前）で指定してください。
   - 管理用サーバにネットワークアダプタが複数あり、かつ同じセグメントに接続している場合、管理用サーバが動作する OS で設定されているバインド順で、優先順位が最も高いホスト名を指定してください。

   ［アドレス解決の設定］で「IP アドレス」を選択したとき

   - IP アドレスで指定してください。

エージェントが接続する管理用サーバが切り替わります。

なお、切り替え元の管理用サーバでネットワーク接続可否情報を設定していた場合は、切り替え先の管理用サーバに切り替え元の管理用サーバのネットワーク接続可否情報をインポートしてください。詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のネットワーク接続可否情報をインポートする手順についての説明を参照してください。

> **重要**
>
> 管理用サーバを切り替えた直後は、グループに間接割り当てされたエージェント設定が割り当たります。接続先の管理用サーバを切り替える前に、グループに割り当てられたエージェント設定が適切かどうかを見直してから、必要に応じてグループの作成と割り当てをしてください。ただし、機器種別のグループおよびネットワークのグループは操作画面で作成できないため、対象のグループに属する機器を事前に接続して、対象のグループが作成されてから、エージェント設定を割り当ててください。

ヒント

エージェントに接続先設定ファイル（itdmhost.conf）を使用した運用の場合、接続先管理サーバに変更した接続先設定ファイル（itdmhost.conf）を配布してください。配布後、エージェントを再起動するか、エージェントのポーリングが実行されると、接続先サーバが変更されます。

7.13　特定のエージェントの接続先を複数サーバ構成内の別の管理用サーバに切り替える手順

管理元からエージェント設定を変更して接続先を切り替えると、そのエージェント設定が割り当てられているすべてのエージェントの接続先が切り替わります。特定のエージェントだけ接続先を切り替えたい場合は、エージェントの接続先をセットアップで変更します。特定のエージェントの接続先を複数サーバ構成内の別の管理用サーバに切り替える手順を次に示します。

特定のエージェントの接続先を複数サーバ構成内の別の管理用サーバに切り替えるには：

1. **切り替え先の管理用サーバでデフォルトエージェント設定の内容を確認し、エージェントの接続先に自サーバが設定されていることを確認します。**

   デフォルトエージェント設定の内容を確認するには、設定画面の［エージェント］－［Windows エージェント設定とインストールセットの作成］画面で、一覧のデフォルトエージェント設定の列に表示される［編集］ボタンをクリックします。

2. **接続先を切り替えたいエージェントがインストールされているコンピュータに Administrator 権限を持つ OS ユーザーでログオンし、エージェントの接続先をセットアップで変更します。**

   該当するコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Agent］－［管理者ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Agent のセットアップを起動して、セットアップを実行してください。

   エージェントにパスワード保護が設定されている場合、パスワードの入力画面が表示されます。該当するエージェント設定に設定したパスワードを入力してください。パスワードのデフォルトは「manager」です。

3. **切り替え先の管理用サーバで、接続先を切り替えたエージェントにエージェント設定を割り当てます。**

   エージェント設定を割り当てるには、設定画面の［エージェント］－［Windows エージェント設定の割り当て］画面で、接続先を切り替えたエージェントがインストールされているコンピュータを選択して［割り当て］ボタンをクリックします。表示されるダイアログで割り当てるエージェント設定を選択してください。

なお、切り替え元の管理用サーバでネットワーク接続可否情報を設定していた場合は、切り替え先の管理用サーバに切り替え元の管理用サーバのネットワーク接続可否情報をインポートしてください。詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のネットワーク接続可否情報をインポートする手順についての説明を参照してください。

関連リンク

- 1.6.10　エージェントをセットアップする手順
- 7.12　エージェントが接続する管理用サーバを切り替える手順

7.14　エージェントが接続する中継システムを切り替える手順

切り替え元の中継システムに接続している、すべてのエージェントの接続先を切り替えるには：

1. 設定画面を表示します。
2. メニューエリアで［エージェント］－［Windows エージェント設定とインストールセットの作成］を選択します。
3. インフォメーションエリアで、切り替えたいエージェント設定の［編集］ボタンをクリックします。
4. ［エージェント設定の編集］ダイアログで［基本設定］－［リモートインストールマネージャを使用した配布用の上位システム］－［ホスト名または IP アドレス］を切り替え先の中継システムのホスト名または IP アドレスに変更します。

   ［ホスト名または IP アドレス］に指定する値は、セットアップの［アドレス解決の設定］で選択した項目によって異なります。

   ［アドレス解決の設定］で「ホスト名」を選択したとき

   - ホスト名で指定してください。
   - DNS サーバを使用している環境では、完全修飾ドメイン名（ホスト名のあとにピリオドとドメイン名を表記した名前）で指定してください。
   - 中継システムにネットワークアダプタが複数あり、かつ同じセグメントに接続している場合、中継システムが動作する OS で設定されているバインド順で、優先順位が最も高いホスト名を指定してください。

   ［アドレス解決の設定］で「IP アドレス」を選択したとき

   - IP アドレスで指定してください。

切り替え元の中継システムに接続している、すべてのエージェントの接続先が切り替わります。

> **重要**
>
> エージェント設定の割り当てを解除すると、自動的にデフォルトエージェント設定が割り当たります。また、ID を使用した配布を実施している場合、デフォルトエージェント設定が割り当たることによって、管理用サーバから ID ジョブが実行されることがあります。その後、エージェント設定を割り当て直した際に、切り替え先の中継システムからも ID ジョブが実行されることがあります。

7.15　特定のエージェントの接続先の中継システムを切り替える手順

切り替え元の中継システムに接続している、特定のエージェントの接続先だけを切り替えるには：

1. 設定画面を表示します。
2. メニューエリアで［エージェント］－［Windows エージェント設定の割り当て］を選択します。
3. 機器を選択し、［割り当てを解除］ボタンをクリックします。
   割り当たっているエージェント設定が解除され、デフォルトエージェント設定が割り当たります。
4. ［割り当て］ボタンをクリックし、［Windows エージェント設定の割り当て］ダイアログで切り替え先の中継システムに接続するためのエージェント設定を割り当てます。

切り替え元の中継システムに接続している、特定のエージェントの接続先が切り替わります。

> **重要**
>
> エージェント設定の割り当てを解除すると、自動的にデフォルトエージェント設定が割り当たります。また、ID を使用した配布を実施している場合、デフォルトエージェント設定が割り当たることによって、管理用サーバから ID ジョブが実行されることがあります。その後、エージェント設定を割り当て直した際に、切り替え先の中継システムからも ID ジョブが実行されることがあります。

7.16　インターネットゲートウェイが接続する管理用サーバを切り替える手順

管理用サーバに接続しているインターネットゲートウェイの接続先を切り替えるには：

1. World Wide Web Publishing Service サービス※を停止します。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Internet Gateway］－［インターネットゲートウェイセットアップ］を選択します。
3. [IT Desktop Management 2 – Internet Gateway 設定］ダイアログでインターネットゲートウェイの上位システムを設定します。
4. [OK］ボタンをクリックします。
5. World Wide Web Publishing Service サービス※を開始します。

   注※　Windows Server 2025、Windows Server 2022、Windows Server 2019 または Windows Server 2016 の場合、「World Wide Web 発行サービス」です。

管理用サーバに接続しているインターネットゲートウェイの接続先が切り替わります。

7.17　大規模管理用のオプションを切り替える手順

大規模管理用のオプションは、JP1/IT Desktop Management 2 - Manager のインストール時に設定します。大規模管理用のオプションを無効から有効に切り替える手順を次に示します。

> **ヒント**
>
> 大規模管理用のオプションを有効から無効に切り替える手順も同様の手順となります。
>
> ただし、50,000 台以上の機器を管理している場合には、大規模管理用のオプションを有効から無効に切り替えないでください。

大規模管理用のオプションを無効から有効にに切り替えるには：

1. JP1/IT Desktop Management 2 のサービスを停止します。

   データベースのバックアップ後に、エージェントから通知された操作ログが新規に保管されないよう、あらかじめサービスを停止しておきます。

   Windows の［スタート］メニューから［管理ツール］－［サービス］を選択してください。表示されるダイアログで、サービス名を右クリックして［停止］を選択すると、サービスを停止できます。停止するサービスを次に示します。

   - JP1_ITDM2_Agent Control
   - JP1_ITDM2_Service
   - JP1_ITDM2_Web Container

2. 移行前の管理用サーバのデータベースのバックアップを取得します。

   移行前の管理用サーバのコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［データベースマネージャ］から JP1/IT Desktop Management 2 - Manager のデータベースマネージャを起動して、データベースのバックアップを実行してください。バックアップ先フォルダのドライブは、目安として 20 ギガバイト以上の空き容量を確保してください。

3. 操作ログのバックアップデータを退避します。

   操作ログを保管する設定にしている場合は、セットアップで指定している「操作ログの保管先フォルダ」に格納されているバックアップデータを退避してください。

   操作ログを保管する設定にしているかどうかは、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、［操作ログの設定］画面で［操作ログを保管する］がチェックされているかどうかで確認します。チェックされている場合は、操作ログを保管する設定になっています。

4. 変更履歴のバックアップデータを退避します。

保存用の変更履歴を出力する設定にしている場合は、セットアップで指定している「変更履歴の出力先フォルダ」に格納されているバックアップデータを退避してください。

保存用の変更履歴を出力する設定にしているかどうかは、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、［保存用の変更履歴の出力設定］画面で［保存用の変更履歴を定期的に出力する］がチェックされているかどうかで確認します。チェックされている場合は、保存用の変更履歴を出力する設定になっています。

5. 移行前の管理用サーバのコンピュータで、JP1/IT Desktop Management 2 - Manager をアンインストールします。

6. JP1/IT Desktop Management 2 - Manager をインストールします。Manager の種別では、[大規模管理用の管理用サーバ]をチェックしてください。

7. JP1/IT Desktop Management 2 - Manager をセットアップします。

移行後の管理用サーバのコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］から JP1/IT Desktop Management 2 - Manager のセットアップを起動して、セットアップを実行してください。

操作ログを保管する設定にしている場合は、［操作ログの自動保管の設定］画面で「操作ログの保管先フォルダ」に、移行前の「操作ログの保管先フォルダ」を指定してください。

保存用の変更履歴を出力する設定にしている場合は、［保存用の変更履歴の出力設定］画面で「変更履歴の出力先フォルダ」に、移行前の「変更履歴の出力先フォルダ」を指定してください。

8. 手順 2.でバックアップしたデータベースをリストアします。

移行後の管理用サーバのコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［データベースマネージャ］から JP1/IT Desktop Management 2 - Manager のデータベースマネージャを起動して、データベースのリストアを実行してください。

9. 正しく運用できることを確認します。

エージェントが移行後の管理用サーバに接続されたかどうかを確認します。機器画面の［機器一覧］画面で、［最終接続確認日時］が更新されていることを確認してください。

［最終接続確認日時］はデフォルトでは表示されていないため、表示されていない場合は［機器一覧］画面の一覧の項目を右クリックして、［表示項目の選択］から表示されるダイアログで確認してください。［最終接続確認日時］が更新されない場合、利用者のコンピュータで、Windows の［スタート］メニュー－［すべてのプログラム］－［JP1_IT Desktop Management 2 - Agent］－［管理者ツール］－［セットアップ］からエージェントのセットアップを起動して、接続先に移行後の管理用サーバが設定されているかどうかを確認してください。

10. パラメタを設定します。

ここでのすべての手順が終了したら、パラメタを設定します。

マニュアル「JP1/IT Desktop Management 2 運用ガイド」の大規模環境での運用方法についての説明を参照してください。

11. データベースのバックアップならびに操作ログおよび変更履歴のバックアップデータを必要に応じて削除します。

ヒント

- JP1/IT Desktop Management 2 12-60 より前のバージョンからバージョンアップした場合は、大規模管理用のオプションは無効になります。
- JP1/NETM/DM から JP1/IT Desktop Management 2 に移行する場合で、大規模管理用のオプションを有効で運用する場合は、いったん大規模管理用のオプションを無効にした管理用サーバに移行した後、大規模管理用のオプションを有効に切り替えてください。

ヒント

操作画面のオーバービューおよび一覧表示のレイアウトの設定は、ログインユーザーごとに保持されています。大規模管理用のオプションを切り替えても、移行前の管理用サーバでの表示設定がそのまま引き継がれます。移行後の管理用サーバでの運用時に次の表示項目が適切でない場合、手動で設定を変更してください。

- ホーム画面のパネルレイアウト、および各パネルの設定内容
- セキュリティ画面のダッシュボードのパネルレイアウト、および各パネルの設定内容
- 資産画面のダッシュボードのパネルレイアウト、および各パネルの設定内容
- 機器画面のダッシュボードのパネルレイアウト、および各パネルの設定内容
- 配布画面のダッシュボードのパネルレイアウト、および各パネルの設定内容
- 各種一覧の 1 ページあたりの表示件数、一覧に表示する項目、および一覧項目の表示順

7.18　管理用中継サーバをインターネットゲートウェイに接続する手順

管理用中継サーバをインターネットゲートウェイに接続するには：

> **重要**
>
> 管理用中継サーバをインターネットゲートウェイに接続するには、管理用中継サーバのセットアップがすべて完了している必要があります。管理用中継サーバのセットアップについては、「1.2.5　管理用中継サーバをセットアップする手順」を参照してください。

以下の手順は、管理用中継サーバで実施してください。

1. [JP1ITDM2 Utility Console] を起動します。
   [JP1ITDM2 Utility Console] の起動方法は、「8.1　コマンドを実行する手順」を参照してください。

2. 表示されるウィンドウで、次のコマンドを実行します。
   `rlyigwsetconf△-o△`*出力先インターネット接続設定ファイル名*
   管理用中継サーバをセットアップした直後の場合、インターネット接続設定ファイルのひな型がファイルに出力されます。すでにインターネットゲートウェイ接続の設定が完了している管理用中継サーバの場合、現在の設定内容のインターネット接続設定ファイルが出力されます。
   rlyigwsetconf コマンドの詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の rlyigwsetconf（管理用中継サーバにインターネット接続情報を設定）についての説明を参照してください。

3. 手順 2 で出力したインターネット接続設定ファイルを編集します。
   接続するインターネットゲートウェイの情報を設定します。インターネット接続設定ファイルの詳細は、「インターネット接続設定ファイルについて：」を参照してください。

4. [JP1ITDM2 Utility Console] を起動し、次のコマンドを実行します。
   `rlyigwsetconf△-i△`*手順3で編集したインターネット接続設定ファイル名*
   rlyigwsetconf コマンドの詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の rlyigwsetconf（管理用中継サーバにインターネット接続情報を設定）についての説明を参照してください。

5. 管理用中継サーバがインターネットゲートウェイと接続できているか、接続確認を実施します。
   次のログファイルを確認します。
   JP1/IT Desktop Management 2 - Managerのインストール先`¥mgr¥log¥USER_CLT_`*nnnn*`.log`
   ログファイルの確認方法の詳細は、「2.11.3　社外で利用する機器のエージェントを構築する手順」の「接続確認をするには：」を参照してください。

インターネット接続設定ファイルについて：

インターネット接続設定ファイルの形式を次に示します。

```
[HTTPGW]
UseInternetGateway=インターネットゲートウェイを経由した上位サーバとの接続可否
ConnectHost=インターネットゲートウェイのホスト名またはIPアドレス
HTTPSPort=インターネットゲートウェイと接続するためのポート番号
AcceptPort=インターネットゲートウェイとの接続時に内部で使用するポート番号
AcceptPortRelay=インターネットゲートウェイとの接続時に内部で使用するポート番号
SSLIgnoreWarning=サーバ証明書有効期限切れ時のインターネットゲートウェイとの接続可否
[BasicAuthN]
UseWWWAuth=インターネットゲートウェイサーバ接続時のユーザー認証可否
ChangeBasicAuth=ユーザー認証のユーザーIDとパスワードの変更可否
Username=ユーザー認証のユーザーID
Password=ユーザー認証のパスワード
[Proxy]
ProxyType=インターネットゲートウェイとの接続時のプロキシサーバ使用可否
ProxyHost=プロキシサーバのホスト名またはIPアドレス
ProxyPort=プロキシサーバのポート番号
ChangeProxyAuth=プロキシサーバのユーザーIDとパスワードの変更可否
ProxyUser=プロキシサーバのユーザーID
ProxyPass=プロキシサーバのパスワード
RangeTransferSize=アップロードファイルの分割サイズ
```

インターネット接続設定ファイルの設定項目を次の表に示します。

セクション	項目	説明	入力できる値	省略可否
HTTPGW	管理用中継サーバが接続するインターネットゲートウェイサーバを設定します。			必須
	UseInternetGateway	インターネットゲートウェイを経由して上位サーバと HTTPS 接続するかどうかを指定します。	半角英字で次のどちらかを指定します。大文字と小文字は区別しません。 YES：接続する NO：接続しない	必須
	ConnectHost	インターネットゲートウェイのホスト名または IP アドレスを指定します。	ホスト名の場合は半角英数字 255 文字以下 IP アドレスの場合は半角数字で「xxx.xxx.xxx.xxx」の形式	UseInternetGateway が YES の場合必須。 NO の場合、省略可。
	HTTPSPort	インターネットゲートウェイのポート番号を指定します。	半角数字で 1～65535 の範囲の数値	必須
	AcceptPort	管理用中継サーバがインターネットゲートウェイに接続する際に内部で使用するポート番号を指定します。	半角数字で 1～65535 の範囲の数値	必須
	AcceptPortRelay	管理用中継サーバがインターネットゲートウェイに接続する際に内部で使用するポート番号を指定します。	半角数字で 1～65535 の範囲の数値	必須
	SSLIgnoreWarning	サーバ証明書の有効期限が切れた場合に、インターネットゲートウェイとの接続をエラーにするかどうかを指定します。	半角数字で次のどちらかを指定します。 0：エラーとする 2：エラーとしない	必須

セクション	項目	説明	入力できる値	省略可否
BasicAuthN	インターネットゲートウェイサーバのユーザー認証情報を設定します。			必須
	UseWWWAuth	インターネットゲートウェイへの接続時にユーザー認証するかを指定します。	半角数字で次のどちらかを指定します。 1：認証する 0：認証しない	必須
	ChangeBasicAuth	ユーザー認証のユーザー ID とパスワードを変更するかどうかを指定します。	半角英字で次のどちらかを指定します。大文字と小文字は区別しません。 YES：変更する NO：変更しない	UseInternetGateway が YES の場合かつ、UseWWWAuth が 1 の場合は必須。その他の場合は省略可で、NO とみなします。
	Username	インターネットゲートウェイの認証時のユーザー ID を指定します。	ASCII 制御文字以外の ASCII 文字 276 文字以内	UseInternetGateway が YES の場合かつ、UseWWWAuth が 1 の場合かつ、ChangeBasicAuth が YES の場合は必須。 その他の場合、省略可で値は無視されます。
	Password	インターネットゲートウェイの認証時のパスワードを指定します。	ASCII 制御文字以外の ASCII 文字 48 文字以内	UseInternetGateway が YES の場合かつ、UseWWWAuth が 1 の場合かつ、ChangeBasicAuth が YES の場合は必須。 その他の場合、省略可で値は無視されます。
Proxy	管理用中継サーバがインターネットゲートウェイサーバに接続する時のプロキシサーバの情報を設定します。			必須
	ProxyType	管理用中継サーバがプロキシサーバを使用してインターネットゲートウェイと通信するかどうかを指定します。	半角数字で次のどちらかを指定します。 1：使用する 0：使用しない	必須

セクション	項目	説明	入力できる値	省略可否
Proxy	ProxyHost	プロキシサーバを使用してインターネットゲートウェイと通信する場合に、プロキシサーバのホスト名または IP アドレスを指定します。	ホスト名の場合は半角英数字 249 文字以下 IP アドレスの場合は半角数字で「xxx.xxx.xxx.xxx」の形式	UseInternetGateway が YES の場合かつ、ProxyType が 1 の場合は必須。その他の場合は省略可
	ProxyPort	プロキシサーバのポート番号を指定します。	半角数字で 5001～49151 の範囲の数値	必須
	ChangeProxyAuth	プロキシサーバのユーザー ID とパスワードを変更するかどうかを指定します。	半角英字で次のどちらかを指定します。大文字と小文字は区別しません。 YES：変更する NO：変更しない	UseInternetGateway が YES の場合かつ、ProxyType が 1 の場合は必須。その他の場合は省略可で、NO とみなします。
	ProxyUser	プロキシサーバへの接続時にユーザー認証する場合のユーザー ID を指定します。	ASCII 制御文字以外の ASCII 文字 276 文字以内	ChangeProxyAuth が YES の場合、省略可。NO の場合は無効。
	ProxyPass	プロキシサーバへの接続時にユーザー認証する場合のパスワードを指定します。	ASCII 制御文字以外の ASCII 文字 48 文字以内	ChangeProxyAuth が YES の場合、省略可。NO の場合は無効。
	RangeTransferSize	アップロードファイルの分割サイズをバイトで指定します。 プロキシサーバや Microsoft Internet Information Services などに制限がある場合、この値を変更してください。	半角数字で 10240～104857600 の範囲の数値	必須

インターネット接続設定ファイルの注意事項を次に示します。

- 値の先頭や末尾の半角スペースは無視され、前後の半角スペースを除去した値が指定値とみなされます。
- 先頭と末尾が「"」または「'」で囲まれた値の場合、先頭および末尾の「"」または「'」を除いた文字列を値として読み込みます。
- 「"」または「'」で囲んだ値を指定したい場合は、前後を「""」で囲みます。
  例：「"abc"」を値として指定する場合は「""abc""」と指定します。
- rlyigwsetconf コマンドでインターネット接続設定ファイルを出力する場合、「"」、「'」または半角スペースで囲まれた値の場合は、「""」で囲んで出力されます。

8 構築関連で使用するコマンド

ここでは、システムの構築、設定変更、リプレースなどで使用する JP1/IT Desktop Management 2 のコマンドについて説明します。

8.1 コマンドを実行する手順

JP1/IT Desktop Management 2 のコマンドは、専用のコマンドプロンプト（[JP1ITDM2 Utility Console]）および Windows のコマンドプロンプトから実行できます。

管理用サーバでコマンドを実行する場合は、[JP1ITDM2 Utility Console] を利用すると便利です。[JP1ITDM2 Utility Console] を利用すると、コマンドを入力する際にコマンドの実行ファイルの格納先を指定する必要がありません。[JP1ITDM2 Utility Console] 起動時に、自動的にコマンドの実行ファイルの格納先がカレントフォルダになります。Windows のコマンドプロンプトからもコマンドを実行できます。

getinv.vbs コマンド、setsecpolicy.vbs コマンド、および upldoplog コマンド以外のコマンドは、Administrator 権限を持つユーザーで実行してください。コマンドを実行する OS が Windows Server 2025、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、または Windows Server 2008 R2 の場合で、ユーザーアカウント制御（UAC）が有効なときは、[JP1ITDM2 Utility Console] または Windows のコマンドプロンプトを起動する際に、右クリックして［管理者として実行］を選択してください。getinv.vbs コマンド、setsecpolicy.vbs コマンド、および upldoplog コマンドは、それぞれのコマンドが格納されているフォルダに対するフルコントロールのアクセス権限を持つユーザーで実行してください。

エージェントでコマンドを実行する場合は、Windows のコマンドプロンプトを利用してください。

管理用サーバでコマンドを実行するには：

1. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［コマンド］を選択します。
2. 表示されるウィンドウで、実行したいコマンドを入力します。

コマンドが実行されます。

エージェントでコマンドを実行するには：

1. Windows のコマンドプロンプトを起動します。
2. 表示されるウィンドウで、実行したいコマンドを入力します。

コマンドが実行されます。

ヒント

Windows のタスクにコマンドを登録することで、JP1/IT Desktop Management 2 のコマンドをスケジュール実行できます。

データベースのバックアップ、リストア、および再編成をコマンドで実行する場合、管理用サーバのサービスを停止する必要があります。そのため、これらのコマンドを Windows のタスクに登録する際は、JP1/IT Desktop Management 2 を使用しない曜日、時間などにコマンドが実行されるよう考慮してください。

注意事項

コマンド実行中には、コマンド実行元の管理用サーバで、次の操作をしないでください。コマンド実行中にこれらの操作をすると、コマンドが強制終了され、タイミングによってはデータベースなどの重要なデータが破損したりエージェント制御サービスが停止したりするおそれがあります。また、コマンドの戻り値が正しく出力されません。

- [Ctrl] + [c] キーを押す
- [JP1ITDM2 Utility Console] または Windows のコマンドプロンプトを終了する
- Windows からログアウトする
- Windows をシャットダウンする

コマンド実行中にこれらの操作をした場合は、ログファイルのメッセージを確認してください。また、コマンドが正常終了したメッセージが出力されていない場合は、必要に応じてコマンドを再実行してください。エージェント制御サービスが停止したメッセージが出力されている場合は、エージェント制御サービスを起動してください。

この注意事項は、次のコマンドには適用されません。

- stopservice
- startservice
- getlogs
- getinstlogs
- addfwlist.bat
- resetnid.vbs
- getinv.vbs
- setsecpolicy.vbs
- upldoplog
- prepagt.bat

8.2　コマンドの説明形式

コマンドは、機能、形式、引数などの項目に分けて説明しています。コマンドの説明形式を次の表に示します。

項番	説明項目	内容
1	機能	コマンドの機能について説明しています。
2	形式	コマンドの入力形式について説明しています。
3	引数	コマンドの引数について説明しています。
4	格納先	コマンドの実行ファイルの格納先について説明しています。
5	注意事項	コマンドを実行する上での注意事項について説明しています。
6	戻り値	コマンドの戻り値について説明しています。
7	使用例	コマンドの使用例について説明しています。

8.3 updatesupportinfo（サポートサービスからの情報の登録）

サポートサービスサイトからダウンロードした情報を管理用サーバに登録するupdatesupportinfo コマンドについて説明します。

機能

管理用サーバがサポートサービスサイトに接続できない場合や、SAMAC 辞書の情報を更新したい場合は、最新情報を手動で管理用サーバに登録する必要があります。

まず、外部のネットワークに接続できるコンピュータでサポートサービスサイトに接続して、サポートサービスから最新情報をダウンロードしてください。ダウンロードした情報を管理用サーバに手動でコピーしてこのコマンドを実行すると、最新情報を管理用サーバに登録できます。

なお、このコマンドは管理用サーバで実行してください。

形式

```
updatesupportinfo△-i△サポート情報ファイル名またはSAMACソフトウェア辞書のオフライン更新用ファイル名
```

引数

-i△*サポート情報ファイル名または SAMAC ソフトウェア辞書のオフライン更新用ファイル名*

管理用サーバに登録するサポート情報ファイルまたは SAMAC ソフトウェア辞書のオフライン更新用ファイルの、ファイル名を絶対パスで指定します。空白を含むパスを指定する場合は、パスをダブルクォーテーション（"）で囲んでください。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- このコマンドは、次のコマンドと同時に実行できません。
  - exportdb
  - importdb
  - ioassetsfieldutil export
  - ioassetsfieldutil import
  - ioutils exportasset
  - ioutils exportassetassoc
  - ioutils exportdevice

- ioutils exportdevicedetail
- ioutils exportfield
- ioutils exportfilter
- ioutils exportoplog
- ioutils exportpolicy
- ioutils exporttemplate
- ioutils exportupdategroup
- ioutils exportupdatelist
- ioutils importasset
- ioutils importassetassoc
- ioutils importexlog
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- ioutils importupdatelist
- reorgdb
- startservice
- stopservice
- deletenwgroup
- deletepackage
- distributelicense

- このコマンドは、管理用サーバでセットアップまたはデータベースマネージャが実行されている場合は実行できません。

戻り値

updatesupportinfo コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたファイルが不正、またはファイルがありません。

戻り値	説明
31	ほかのコマンドを実行中です。
51	コマンドの実行権限がありません。
53	管理用サーバのサービスが開始されていません。
54	管理用サーバがセットアップされていません。
101	一部またはすべてのサポート情報の更新に失敗しました。
150	そのほかのエラーでコマンドの実行が中断しました。

使用例

C:¥temp に格納したサポート情報ファイル supportinfo.zip を管理用サーバに登録する場合の使用例を次に示します。

updatesupportinfo -i C:¥temp¥supportinfo.zip

関連リンク

- 8.1　コマンドを実行する手順

8.4 exportdb（バックアップの取得）

管理用サーバが管理するデータのバックアップを取得するexportdb コマンドについて説明します。

機能

管理用サーバが管理するデータのバックアップを取得します。取得したバックアップは、トラブル発生時のデータの復元に利用できます。

このコマンドを実行すると、引数に指定したバックアップ先フォルダに *YYYYMMDDhhmmss*※のフォルダ名でバックアップ格納先フォルダが作成され、そのフォルダ内にバックアップファイルが作成されます。

注※　YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒

なお、このコマンドは管理用サーバで実行してください。

形式

```
exportdb[△-f△バックアップ先フォルダ名][△-s]
```

引数

-f△*バックアップ先フォルダ名*

バックアップを取得するフォルダを絶対パスで指定します。指定できるフォルダは、ローカルドライブのフォルダだけです。バックアップファイルの容量は運用内容や JP1/IT Desktop Management 2 の利用期間によって異なります。バックアップ先フォルダのドライブは、データベースフォルダとデータフォルダのディスク占有量の合計値以上の空き容量を確保してください。

空白を含むパスを指定する場合は、パスをダブルクォーテーション（"）で囲んでください。フォルダ名は末尾の「¥」を除いて 135 バイト以内で指定してください。また、使用できる文字は、半角英数字、半角スペース、および次に示す半角記号です。

「#」、「(」、「)」、「.」（ピリオド）、「@」、「¥」

JP1/IT Desktop Management 2 のインストール先フォルダ名にこれらの文字以外の文字を使用している場合は、この引数を必ず指定してください。この引数を省略した場合は、次に示すフォルダがバックアップ先フォルダとなります。

- 引数を指定した場合

  引数に指定したフォルダ¥*YYYYMMDDhhmmss*

- 引数を省略した場合

  JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥backup¥*YYYYMMDDhhmmss*

（例）

2011 年 1 月 1 日 2 時 30 分 00 秒にこのコマンドを実行した場合

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥backup¥20110101023000

-S

管理用サーバのサービスの停止（stopservice コマンド）、データのバックアップの取得（exportdb コマンド）、および管理用サーバのサービスの開始（startservice コマンド）を自動で実行する場合に指定します。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- このコマンドは、管理用サーバのセットアップが完了し、かつ管理用サーバが停止している状態で実行してください。
- このコマンドは、同時に複数実行できません。
- このコマンドは、次のコマンドと同時に実行できません。
  - importdb
  - ioassetsfieldutil export
  - ioassetsfieldutil import
  - ioutils exportasset
  - ioutils exportassetassoc
  - ioutils exportdevice
  - ioutils exportdevicedetail
  - ioutils exportfield
  - ioutils exportfilter
  - ioutils exportoplog
  - ioutils exportpolicy
  - ioutils exporttemplate
  - ioutils exportupdategroup
  - ioutils exportupdatelist
  - ioutils importasset
  - ioutils importassetassoc
  - ioutils importexlog
  - ioutils importfield
  - ioutils importfilter

- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- ioutils importupdatelist
- reorgdb
- startservice
- stopservice
- updatesupportinfo
- deletenwgroup
- deletepackage
- distributelicense

- 引数「-s」は、クラスタ環境では指定できません。この引数を指定した場合、コマンドはエラーになります。

戻り値

exportdb コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	バックアップの取得に成功しましたが、管理用サーバの自動開始に失敗しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたフォルダが不正、またはフォルダがありません。
31	ほかのコマンドを実行中です。
32	同一時刻に作成されたバックアップ格納先フォルダがあります。
33	ディスク容量が不足しています。
34	データベースの開始に失敗しました。
35※	コマンド実行時に管理用サーバが開始処理中です。
36	コマンド実行時にデータベースが停止処理中です。
51	コマンドの実行権限がありません。
52	クラスタ環境で、引数「-s」が指定されています。
53	管理用サーバが停止していません。
54	管理用サーバがセットアップされていません。
55	デフォルトのバックアップ格納先フォルダが使用できません。

戻り値	説明
61	操作ログのバックアップ先フォルダに接続できません。
62	操作ログのバックアップ先フォルダにログインできません。
63	操作ログ関連のフォルダ容量が不足しています。
64	そのほかのエラーで操作ログのバックアップが中断しました。
101	バックアップの取得に失敗しました。
102	管理用サーバの自動停止に失敗しました。
110	ライセンスに問題があるためコマンドの実行に失敗しました。
150	そのほかのエラーでコマンドの実行が中断しました。

注※　引数「-s」を指定した場合の戻り値です。

使用例

バックアップを C:¥tmp¥backup に取得し、管理用サーバのサービスの停止、データのバックアップの取得、および管理用サーバのサービスの開始を自動で実行する場合のコマンドの使用例を示します。

exportdb -f C:¥tmp¥backup -s

関連リンク

- 8.1　コマンドを実行する手順

8.5 importdb（バックアップデータのリストア）

管理用サーバが管理するデータをバックアップ取得時の状態に復元（リストア）するimportdb コマンドについて説明します。

機能

ディスク障害などが発生した場合に、管理用サーバが管理するデータをバックアップ取得時の状態に復元します。データの復元には、exportdb コマンドで取得したバックアップファイルを使用します。

なお、このコマンドは管理用サーバで実行してください。

形式

```
importdb[△-f△データ格納フォルダ名][△-w△作業用フォルダ名][△-s]
```

引数

-f△*データ格納フォルダ名*

復元する時点のバックアップファイルが格納されているフォルダを絶対パスで指定します。指定できるフォルダは、ローカルドライブのフォルダだけです。

空白を含むパスを指定する場合は、パスをダブルクォーテーション（"）で囲んでください。フォルダ名は末尾の「¥」を除いて 150 バイト以内で指定してください。また、使用できる文字は、半角英数字、半角スペース、および次に示す半角記号です。

「#」、「(」、「)」、「.」（ピリオド）、「@」、「¥」

JP1/IT Desktop Management 2 のインストール先フォルダ名にこれらの文字以外の文字を使用している場合は、この引数を必ず指定してください。

この引数を指定した場合、および省略した場合に、コマンド実行時にデータの復元に使用されるデータ格納先フォルダを次に示します。

引数を指定した場合

引数で指定したフォルダをデータ格納先フォルダとして使用します。

引数を省略した場合

次のフォルダ下にあるフォルダのうち、フォルダ名から最新のデータ格納先フォルダを判断して使用します。

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥backup¥

例えば、「¥20110101023000」、「¥20110102023000」、および「¥20110103023000」のフォルダがある場合、「¥20110103023000」フォルダが復元に使用するデータ格納先フォルダになります。

-w△*作業用フォルダ名*

バックアップ取得時の状態に復元するときに使用する作業用フォルダを絶対パスで指定します。指定できるフォルダは、ローカルドライブのフォルダだけです。作業用フォルダのドライブには、10,000 台の機器を管理する場合は 10 ギガバイト以上の空き容量が必要です。

空白を含むパスを指定する場合は、パスをダブルクォーテーション（"）で囲んでください。フォルダ名は末尾の「¥」を除いて 150 バイト以内で指定してください。また、使用できる文字は、半角英数字、半角スペース、および次に示す半角記号です。

「#」、「(」、「)」、「.」（ピリオド）、「@」、「¥」

JP1/IT Desktop Management 2 のインストール先フォルダ名にこれらの文字以外の文字を使用している場合は、この引数を必ず指定してください。指定したフォルダがない場合はエラーとなります。

この引数を省略した場合は、次に示すフォルダが作業用フォルダとなります。

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥temp

-s

管理用サーバのサービスの停止（stopservice コマンド）、バックアップからのリストア（importdb コマンド）、および管理用サーバのサービスの開始（startservice コマンド）を自動で実行する場合に指定します。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- このコマンドは、管理用サーバのセットアップが完了し、かつ管理用サーバが停止している状態で実行してください。
- このコマンドは、同時に複数実行できません。
- このコマンドは、次のコマンドと同時に実行できません。
  - exportdb
  - ioassetsfieldutil export
  - ioassetsfieldutil import
  - ioutils exportasset
  - ioutils exportassetassoc
  - ioutils exportdevice
  - ioutils exportdevicedetail
  - ioutils exportfield
  - ioutils exportfilter
  - ioutils exportoplog
  - ioutils exportpolicy
  - ioutils exporttemplate

- ioutils exportupdategroup
- ioutils exportupdatelist
- ioutils importasset
- ioutils importassetassoc
- ioutils importexlog
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- ioutils importupdatelist
- reorgdb
- startservice
- stopservice
- updatesupportinfo
- deletenwgroup
- deletepackage
- distributelicense

- 引数「-s」は、クラスタ環境では指定できません。この引数を指定した場合、コマンドはエラーになります。

戻り値

importdb コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	バックアップからのリストアに成功しましたが、管理用サーバの自動開始に失敗しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたデータ格納フォルダが不正、またはフォルダがありません。
13	指定されたデータ格納フォルダに、バックアップファイルがありません。
14	指定された作業用フォルダが不正、またはフォルダがありません。
15	ディスク容量が不足しています。
31	ほかのコマンドを実行中です。

戻り値	説明
34	データベースの開始に失敗しました。
35※	コマンド実行時に管理用サーバが開始処理中です。
36	コマンド実行時にデータベースが停止処理中です。
51	コマンドの実行権限がありません。
52	クラスタ環境で、引数「-s」が指定されています。
53	管理用サーバが停止していません。
54	管理用サーバがセットアップされていません。
55	デフォルトのデータ格納フォルダおよび作業用フォルダが使用できません。
56	古いバージョンのバックアップ情報です。
61	操作ログのバックアップ先フォルダに接続できません。
62	操作ログのバックアップ先フォルダにログインできません。
63	操作ログ関連のフォルダ容量が不足しています。
64	そのほかのエラーで操作ログのリストアが中断しました。
101	バックアップからのリストアに失敗しました。
102	管理用サーバの自動停止に失敗しました。
110	ライセンスに問題があるためコマンドの実行に失敗しました。
150	そのほかのエラーでコマンドの実行が中断しました。

注※　引数「-s」を指定した場合の戻り値です。

使用例

2011 年 1 月 3 日 2 時 30 分 00 秒にバックアップを取得した時点のデータ（バックアップ格納先フォルダ：C:¥tmp¥backup¥20110103023000）を使用し、管理用サーバのサービスの停止、バックアップからのリストア、および管理用サーバのサービスの開始を自動で実行する場合のコマンドの使用例を示します。

importdb -f C:¥tmp¥backup¥20110103023000 -s

関連リンク

- 8.1　コマンドを実行する手順

8.6 stopservice（サービス停止）

機能

JP1/IT Desktop Management 2 - Manager のサービスを停止して、管理用サーバを停止状態にします。

なお、このコマンドは管理用サーバで実行してください。

形式

```
stopservice
```

引数

引数はありません。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- このコマンドは、管理用サーバのセットアップが完了している状態で実行してください。
- このコマンドは、同時に複数実行できません。
- このコマンドは、次のコマンドと同時に実行できません。
  - exportdb
  - importdb
  - ioassetsfieldutil export
  - ioassetsfieldutil import
  - ioutils exportasset
  - ioutils exportassetassoc
  - ioutils exportdevice
  - ioutils exportdevicedetail
  - ioutils exportfield
  - ioutils exportfilter
  - ioutils exportoplog
  - ioutils exportpolicy
  - ioutils exporttemplate

- ioutils exportupdategroup
- ioutils exportupdatelist
- ioutils importasset
- ioutils importassetassoc
- ioutils importexlog
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- ioutils importupdatelist
- reorgdb
- startservice
- updatesupportinfo
- deletenwgroup
- deletepackage
- distributelicense

戻り値

stopservice コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	管理用サーバがすでに停止しています。
11	コマンドの引数の指定形式に誤りがあります。
31	ほかのコマンドを実行中です。
35	コマンド実行時に管理用サーバが開始処理中です。
51	コマンドの実行権限がありません。
52	クラスタ環境ではこのコマンドを実行できません。
54	管理用サーバがセットアップされていません。
101	管理用サーバのサービスの停止に失敗しました。
150	そのほかのエラーでコマンドの実行が中断しました。

使用例

管理用サーバのサービスを停止するコマンドの使用例を次に示します。

stopservice

関連リンク

- 8.1　コマンドを実行する手順

8.7 startservice（サービス開始）

機能

管理用サーバの関連サービスを起動し、管理用サーバを起動状態にします。

なお、このコマンドは管理用サーバで実行してください。

形式

```
startservice
```

引数

引数はありません。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- このコマンドは、管理用サーバのセットアップが完了している状態で実行してください。
- このコマンドは、同時に複数実行できません。
- このコマンドは、次のコマンドと同時に実行できません。
  - exportdb
  - importdb
  - ioassetsfieldutil export
  - ioassetsfieldutil import
  - ioutils exportasset
  - ioutils exportassetassoc
  - ioutils exportdevice
  - ioutils exportdevicedetail
  - ioutils exportfield
  - ioutils exportfilter
  - ioutils exportoplog
  - ioutils exportpolicy
  - ioutils exporttemplate

- ioutils exportupdategroup
- ioutils exportupdatelist
- ioutils importasset
- ioutils importassetassoc
- ioutils importexlog
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- ioutils importupdatelist
- reorgdb
- stopservice
- updatesupportinfo
- deletenwgroup
- deletepackage
- distributelicense

戻り値

startservice コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	管理用サーバがすでに開始しています。
11	コマンドの引数の指定形式に誤りがあります。
31	ほかのコマンドを実行中です。
35	コマンド実行時に管理用サーバが停止処理中です。
51	コマンドの実行権限がありません。
52	クラスタ環境ではこのコマンドを実行できません。
54	管理用サーバがセットアップされていません。
101	管理用サーバのサービスの開始に失敗しました。
110	ライセンスに問題があるためコマンドの実行に失敗しました。
150	そのほかのエラーでコマンドの実行が中断しました。

使用例

管理用サーバのサービスを開始するコマンドの使用例を次に示します。

startservice

関連リンク

- 8.1　コマンドを実行する手順

8.8 getlogs（トラブルシュート用情報の取得）

機能

原因不明なトラブルや、解決が困難なトラブルなどが発生した場合に、サポートサービスに問い合わせるときに必要なトラブルシュート用情報を一括で取得します。

取得できるトラブルシュート用情報は、一次用ファイル（tsinf_1st.dat）と二次用ファイル（tsinf_2nd.dat）の 2 つのファイルに分けて出力されます。

管理用中継サーバでgetlogs コマンドを実行した場合、管理用中継サーバ用のエージェントに関するトラブルシュート用情報も併せて取得します。管理用中継サーバ用のエージェントのトラブルシュート用情報は、*JP1/IT Desktop Management 2 のインストール先フォルダ*¥mgr¥log に格納されます。取得される情報については、マニュアル「JP1/IT Desktop Management 2 構築ガイド」のエージェントインストール時のトラブルシューティングの説明を参照してください。

なお、このコマンドは管理用サーバまたはリモートインストールマネージャを導入したコンピュータで実行してください。

形式

```
getlogs[△-f△トラブルシュート用情報格納先フォルダ名]
```

引数

-f△*トラブルシュート用情報格納先フォルダ名*

トラブルシュート用情報格納先フォルダを絶対パスで指定します。なお、指定できるフォルダは、ローカルドライブのフォルダだけです。

空白を含むパスを指定する場合は、パスをダブルクォーテーション（"）で囲んでください。フォルダ名は末尾の「¥」を除いて 150 バイト以内で指定してください。また、使用できる文字は Windows でフォルダ名に使用できる文字です。

この引数を省略した場合、トラブルシュート用情報ファイルは次に示すフォルダに格納されます。

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥troubleshoot

なお、トラブルシュート用情報の取得時に、トラブルシュート用情報格納先フォルダに一時フォルダとして tsinf フォルダが作成され、コマンド終了時に削除されます。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- トラブルシュート用情報格納先フォルダに次に示すフォルダまたはファイルがすでに存在した場合、これらのフォルダまたはファイルが削除されてから、コマンドが実行されます。
  - tsinf フォルダ
  - tsinf_1st.dat
  - tsinf_2nd.dat

  ただし、タスクスケジューラなどの機能を使用する場合、これらのフォルダまたはファイルがすでに存在すると、getlogs コマンドの実行に失敗します。そのため、これらのトラブルシュート用情報を削除してから実行するよう設定してください。
- getlogs コマンドでは、一時フォルダとしてユーザー環境変数 TEMP に設定したフォルダを使用します。getlogs コマンドでメッセージ（KDEX4041-E）が出力される場合は、このフォルダの空き容量が十分かどうかを確認してください。

戻り値

getlogs コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	一部のトラブルシュート用情報の取得に失敗しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたフォルダが不正、またはフォルダがありません。
51	コマンドの実行権限がありません。
101	そのほかのエラーでコマンドの実行が中断しました。

使用例

トラブルシュート用情報を C:¥tmp¥troubleshoot に取得する場合のコマンドの使用例を次に示します。

getlogs -f C:¥tmp¥troubleshoot

関連リンク

- 8.1　コマンドを実行する手順

8.9 getinstlogs（インストール時のトラブルシュート用情報の取得）

JP1/IT Desktop Management 2 - Manager または Remote Install Manager をインストールしたときの、トラブルシュート用情報を取得するための`getinstlogs` コマンドについて説明します。

機能

管理者が JP1/IT Desktop Management 2 - Manager または Remote Install Manager をインストールした際に、原因不明なトラブルや、解決が困難なトラブルなどが発生した場合に、サポートサービスに問い合わせるときに必要なトラブルシュート用情報を一括で取得します。

なお、このコマンドは管理用サーバまたはリモートインストールマネージャを導入したコンピュータで実行してください。

形式

`getinstlogs[△-f△`*トラブルシュート用情報格納先フォルダ名*`]`

引数

-f△*トラブルシュート用情報格納先フォルダ名*

トラブルシュート用情報格納先フォルダを絶対パスで指定します。ネットワークドライブも指定できます。

空白を含むパスを指定する場合は、パスをダブルクォーテーション（"）で囲んでください。フォルダ名は末尾の「¥」を除いて 150 バイト以内で指定してください。また、使用できる文字は Windows でフォルダ名に使用できる文字です。

この引数を省略した場合、トラブルシュート用情報ファイルはデスクトップに格納されます。

格納先

JP1/IT Desktop Management 2 の提供媒体のルート¥_PPDIR¥*8～11 文字の英数字*¥DISK1¥

注意事項

- トラブルシュート用情報格納先フォルダに JDNINST フォルダまたはファイルがすでに存在した場合、このフォルダまたはファイルが削除されてから、コマンドが実行されます。
- トラブルシュート用情報格納先フォルダを指定する場合、すでに存在するフォルダを指定してください。

戻り値

`getinstlogs` コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	一部のトラブルシュート用情報の取得に失敗しました。

戻り値	説明
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたフォルダにアクセスできない、またはフォルダがありません。
13	指定されたデータ格納フォルダに、バックアップファイルを書き込めません。
51	コマンドの実行権限がありません。
101	そのほかのエラーでコマンドの実行が中断しました。

使用例

インストール時のトラブルシュート用情報を C:¥tmp¥troubleshoot¥install に取得する場合のコマンドの使用例を次に示します。

getinstlogs -f C:¥tmp¥troubleshoot¥install

関連リンク

- 8.1　コマンドを実行する手順

8.10 resetnid.vbs（ホスト識別子のリセット）

エージェントによって生成された、機器を識別するためのユニークな ID（ホスト識別子）をリセットするためのresetnid.vbs コマンドについて説明します。

機能

エージェントを導入すると、自動的にホスト識別子が生成されます。

ディスクコピーによってエージェントを導入する場合、コピー先のコンピュータのホスト識別子が新規に生成されるよう、あらかじめコピー元のコンピュータでホスト識別子をリセットしておく必要があります。コピー元のコンピュータでresetnid.vbs コマンドを実行することで、エージェントのホスト識別子がリセットされます。これによって、ディスクコピーを利用してエージェントを導入したときに、新規にホスト識別子が生成され、コンピュータがユニークに識別されるようになります。

ヒント

VMWare などの仮想環境を複製して使用する場合も、resetnid.vbs コマンドを実行してください。

重要

共有型 VDI の仮想コンピュータを管理する場合、resetnid.vbs コマンドではホスト識別子をリセットできません。

ヒント

resetnid.vbs コマンドを実行しないままディスクコピーしてエージェントを導入した場合、ディスクコピー先のコンピュータが、ディスクコピー元のコンピュータと同一の機器として識別されます。複数のコンピュータが同一の機器として識別されてしまったときは、それらのコンピュータ上でresetnid.vbs コマンドを実行したあとに、設定画面の［機器の探索］－［管理対象機器］でコンピュータの機器情報をいったん削除してください。

一度 JP1/IT Desktop Management 2 に識別されたコンピュータでresetnid.vbs コマンドを実行すると、コマンドの実行前と実行後のホスト識別子が JP1/IT Desktop Management 2 に両方登録されます。そのため、1 台のコンピュータに対して 2 つの機器情報が表示されますが、設定画面の［機器の探索］－［管理対象機器］で 2 つの機器情報をいったん削除すれば、新しい機器情報だけが表示されるようになります。

重要

ネットワークモニタを導入している機器ではresetnid.vbs コマンドを実行しないでください。

resetnid.vbs コマンドを実行すると、1 台のコンピュータに対して 2 つの機器情報が表示されますが、ネットワークモニタを導入している機器でこれを解消するためには、一度ネットワークモニタを無効にしたあとで、設定画面の［機器の探索］－［管理対象機器］で 2 つの機器情報をいったん削除する必要があります。

なお、このコマンドは、エージェント導入済みのコンピュータ上で実行してください。

また、リターンコードを表示させるには、後述の使用例のように Windows の start コマンドで/wait オプションを指定し、Cscript.exe を実行してください。

形式

```
resetnid.vbs△/nodeid［△/i |△/s］
```

引数

/nodeid

この引数は必ず指定してください。引数を省略した場合、コマンドは実行されません。

/i

利用者のコンピュータに、コマンドを実行するかどうかを選択させるダイアログと、実行結果を示すダイアログを表示します。引数を省略した場合も、ダイアログを表示します。

/s

ダイアログを表示しないでコマンドを実行します。コマンドの実行結果は戻り値で確認してください。

格納先

エージェントのインストール先フォルダ¥bin¥

注意事項

resetnid.vbs コマンドを実行してから新規のホスト識別子が生成されるまでには、エージェント設定の［基本設定］－［上位システムとの通信のタイミング］に設定した次の項目のうち、最も短い間隔だけ時間が掛かります。

- ［監視間隔（セキュリティ項目）（分）］
- ［監視間隔（セキュリティ項目以外）（分）］
- ポーリングの設定で指定した間隔

戻り値

resetnid.vbs コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
10001	利用者のコンピュータで、コマンドの実行がキャンセルされました。
10011	コマンドの引数の指定形式に誤りがあります。
10051	コマンドの実行権限がありません。
10101	ホスト識別子のリセットに失敗しました。
10150	ホスト識別子のリセットに失敗しました。

使用例

エージェントのインストール先フォルダが「C:¥Program Files¥Hitachi¥jp1itdma」の場合の、ホスト識別子をリセットするコマンドの使用例を次に示します。

```
cd "C:¥Program Files¥Hitachi¥jp1itdma¥bin"

start /wait Cscript.exe resetnid.vbs /nodeid

echo %errorlevel%
```

関連リンク

- 8.1　コマンドを実行する手順

8.11 distributelicense（ライセンスの分配）

機能

管理用中継サーバに対して、ライセンスの分配またはライセンスの登録許可をします。

なお、このコマンドは統括管理用サーバで実行してください。

形式

```
distributelicense{△-i△ファイル名|△-d}
```

引数

-i

分配先や分配するライセンス数などを設定したファイル名を、259 バイト以内の絶対パスで指定します。

-d

配下の管理用中継サーバに対するライセンスの分配およびライセンス登録の許可の設定を初期化します。分配していたライセンスはすべて統括管理用サーバに回収されます。-d オプションを指定した場合は、確認メッセージが表示されます。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

ファイルの記述形式

引数-i で指定するファイルの記述形式を次の表に示します。各項目は「,」（コンマ）で区切ってください。

項目	必須/任意	説明	入力値
管理用中継サーバのホスト名	必須	分配する管理用中継サーバのホスト名を設定します。 設定するホスト名はファイル内で重複しないようにしてください。	ホスト名の形式
保有方法	必須	ライセンスを分配するか、またはライセンス登録を許可するかを設定します。 • 分配の場合 DIST • 登録許可の場合 REG	「REG」または「DIST」
分配する製品ライセンス数	分配の場合必須	管理用中継サーバに分配するライセンス数を設定します。 • 分配の場合 1 以上の整数を設定します。	1 以上の整数

項目	必須/任意	説明	入力値
分配する製品ライセンス数	分配の場合必須	• 登録許可の場合 値の設定なし	1 以上の整数
コメント	任意	コメントを設定します。	128 文字以内の任意の文字列

記述例を次に示します。

Host1,DIST,100,comment

Host2,DIST,50,

Host3,REG,,

注意事項

- このコマンドはデータベースのサービスを開始している状態で実行してください。
- このコマンドは、同時に複数実行できません。
- このコマンドは、次のコマンドと同時に実行できません。
  - exportdb
  - importdb
  - ioassetsfieldutil export
  - ioassetsfieldutil import
  - ioutils exportasset
  - ioutils exportassetassoc
  - ioutils exportdevice
  - ioutils exportdevicedetail
  - ioutils exportfield
  - ioutils exportfilter
  - ioutils exportoplog
  - ioutils exportpolicy
  - ioutils exporttemplate
  - ioutils exportupdategroup
  - ioutils exportupdatelist
  - ioutils importasset
  - ioutils importassetassoc
  - ioutils importexlog

- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- ioutils importupdatelist
- reorgdb
- startservice
- stopservice
- updatesupportinfo
- deletenwgroup
- deletepackage

戻り値

distributelicense コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたファイルのパスが不正です。またはアクセス権がありません。
31	ほかのコマンドを実行中です。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
58	管理用サーバ以外でコマンドを実行しました。
80	指定したファイルの形式が不正です。
101	そのほかのエラーでコマンドの実行が中断しました。
110	ライセンスに問題があるためコマンドの実行に失敗しました。
120	データベースのアクセスエラーです。

使用例

C:¥temp¥に作成したライセンスの分配情報「ライセンス分配.csv」を使ってライセンスを分配する場合のコマンドの使用例を次に示します。

distributelicense -i C:¥temp¥ライセンス分配.csv

関連リンク

- 8.1　コマンドを実行する手順

8.12 dmpclint.exe（リモートインストールマネージャを利用した配布機能で生成された情報のリセット）

リモートインストールマネージャを利用した配布機能で生成された情報をリセットするためのdmpclint.exeコマンドについて説明します。

機能

リモートインストールマネージャを利用した配布機能を利用した際に生成された実行中のジョブや配布履歴などの情報をリセットします。ディスクコピーによってエージェントを導入する場合、コピー元のコンピュータでdmpclint.exeコマンドを実行することで、生成された情報をリセットし、コピー先のコンピュータにコピーされないようにします。

形式

```
dmpclint.exe△/ALL
```

引数

/ALL

この引数は必ず指定してください。引数を省略した場合、コマンドは実行されません。

格納先

エージェントのインストール先フォルダ¥bin¥

戻り値

dmpclint.exeコマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	初期化に失敗しました。
2	コマンドの引数に誤りがあります。
3	リセットに失敗しました。

使用例

エージェントのインストール先フォルダが「C:¥Program Files¥Hitachi¥jp1itdma」の場合の、リセットするコマンドの使用例を次に示します。

```
cd "C:¥Program Files¥Hitachi¥jp1itdma¥bin"

start /wait dmpclint.exe /ALL

echo %errorlevel%
```

8.13 checkitdmhost（接続先設定ファイルのフォーマットチェック）

エージェントの接続先を自動設定する接続先設定ファイル（itdmhost.conf）が、ファイルフォーマットを満たしているかどうかをチェックするするための checkitdmhost コマンドについて説明します。

機能

接続先設定ファイル（itdmhost.conf）のファイルフォーマットを満たしているかどうかをチェックします。

このコマンドを実行すると、引数に指定した接続先設定ファイルが 1 行ずつチェックされ、形式が不正な行は行番号がメッセージとして出力されます。形式不正が見つかっても終了しないで、引き続き次の行のチェックが実施されます。最終行まで到達するとチェック処理を終了します。ただし、形式不正の行が 100 行を越えた場合は、フォーマットエラーを表示してチェック処理を終了します。なお、チェックの途中でほかのエラーが発生した場合は、フォーマットチェックを中止し、そのエラーを表示して終了します。

次の場合に、接続先設定ファイルのその行の形式を不正とします。

- 必須項目を省略した場合
- IP アドレスに無効な値を指定した場合
- 「接続先」として入力できる文字数以上の値を指定した場合
- DM セクションの「接続種別」として「netmdm」、「netmdmw」以外を指定した場合
- DM セクションの「マルチキャスト配布用アドレス」として無効な値を指定した場合
- 1 行に指定できる項目以外の項目を指定した場合
- セクション名として無効な値を指定した場合
- セクションを重複して指定した場合
  重複して指定した場合も、そのセクションの項目のチェック処理は実施されます。
- セクション指定がない場合
- ITDM セクションと DM セクションのどちらか一方だけを指定した場合

次の場合は、不正とはしないで、その行や記述を無視します。

- セミコロンに続く記述
  コメントとして扱われます。
- 改行だけの行
- 各項目の先頭や末尾に含まれる半角スペース

なお、このコマンドは管理用サーバで実行してください。

形式

```
checkitdmhost△-i△入力ファイル名
```

引数

-i

フォーマットチェックをする接続先設定ファイル（itdmhost.conf）を 200 バイト以内の絶対パスで指定します。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

戻り値

checkitdmhost コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定された接続先設定ファイルのアクセスエラーです。
13	指定された接続先設定ファイルのファイル名が不正です。
80	指定された接続先設定ファイルの形式が不正です。
101	メモリ不足でコマンドの実行に失敗しました。
150	そのほかのエラーでコマンドの実行が中断しました。

使用例

C:¥work1¥に作成した接続先設定ファイルのフォーマットチェックをする場合のコマンドの使用例を次に示します。

```
checkitdmhost -i C:¥work1¥itdmhost.conf
```

8.14 checkitdmigw（インターネットゲートウェイ接続先設定ファイルのフォーマットチェック）

エージェントの接続先インターネットゲートウェイサーバを自動設定するインターネットゲートウェイ接続先設定ファイル（itdmigw.conf）が、ファイルフォーマットを満たしているかどうかをチェックし、指定したインターネットゲートウェイ接続先設定ファイル（itdmigw.conf）を難読化するための checkitdmigw コマンドについて説明します。

機能

インターネットゲートウェイ接続先設定ファイル（itdmigw.conf）のファイルフォーマットを満たしているかどうかをチェックし、難読化したインターネットゲートウェイ接続先設定ファイルを出力します。

このコマンドを実行すると、引数に指定したインターネットゲートウェイ接続先設定ファイルが 1 行ずつチェックされ、形式が不正な行は行番号がメッセージとして出力されます。形式不正が見つかっても終了しないで、引き続き次の行のチェックが実施されます。最終行まで到達するとチェック処理を終了します。ただし、形式不正の行が 100 行を越えた場合は、フォーマットエラーを表示してチェック処理を終了します。なお、チェックの途中でほかのエラーが発生した場合は、フォーマットチェックを中止し、そのエラーを表示して終了します。

次の場合に、インターネットゲートウェイ接続先設定ファイルのその行の形式を不正とします。

- 必須項目を省略した場合
- IP アドレスに無効な値を指定した場合
- 各項目に入力できる文字数以上の値を指定した場合
- 1 行に指定できる項目以外の項目を指定した場合
- セクション名として無効な値を指定した場合
- セクションを重複して指定した場合
  重複して指定した場合も、そのセクションの項目のチェック処理は実施されます。
- セクション指定がない場合

次の場合は、不正とはしないで、その行や記述を無視します。

- セミコロンに続く記述
  コメントとして扱われます。
- 改行だけの行
- 各項目の先頭や末尾に含まれる半角スペース

なお、このコマンドは管理用サーバまたはエージェントで実行してください。

形式

```
checkitdmigw△-i△入力ファイル名△-o△出力フォルダ
```

引数

-i

フォーマットチェックをするインターネットゲートウェイ接続先設定ファイル（itdmigw.conf）を 200 バイト以内の絶対パスで指定します。パスに半角空白を含む場合はパス全体を「”」で囲んでください。

ファイル名は必ず「itdmigw.conf」としてください。

-o

フォーマットチェック後に難読化したインターネットゲートウェイ接続先設定ファイル（itdmigw.conf）の出力先フォルダを 200 バイト以内の絶対パスで指定します。パスに半角空白を含む場合はパス全体を「”」で囲んでください。

-i オプションで指定した入力ファイルと同じフォルダは指定できません。

戻り値

checkitdmigw コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたインターネットゲートウェイ接続先設定ファイルのアクセスエラーです。
13	指定されたインターネットゲートウェイ接続先設定ファイルのファイル名が不正です。
15	ファイル出力時のファイルのアクセスエラー、またはディスク容量が不足しています。
80	指定されたインターネットゲートウェイ接続先設定ファイルの形式が不正です。
101	メモリ不足でコマンドの実行に失敗しました。
150	そのほかのエラーでコマンドの実行が中断しました。

使用例

C:¥work1¥に作成したインターネットゲートウェイ接続先設定ファイルのフォーマットをチェックし、難読化したインターネットゲートウェイ接続先設定ファイルを C:¥work2¥に出力する場合のコマンドの使用例を次に示します。

```
checkitdmigw -i C:￥work1￥itdmigw.conf -o C:￥work2￥
```

9 トラブルシューティング

ここでは、JP1/IT Desktop Management 2 の構築時にトラブルが発生した場合の対処方法について説明します。

9.1　構築時のトラブルシューティングの流れ

サーバおよびエージェントの環境を構築しているときにトラブルが発生した場合は、次の手順で対処してください。

1.エラーメッセージを確認する

ログファイルに出力されたエラーメッセージの内容を確認してください。

> **ヒント**
>
> エラーを通知するダイアログから、エラーメッセージの内容を確認することもできます。

2.トラブルの要因および対処方法を確認して、エラーを対処する

ログファイルに出力されたメッセージから、トラブルの要因およびエラーの対処方法を確認して、エラーを対処します。

発生したトラブルに対処できます。

メッセージの出力形式

出力されるメッセージの形式を次に示します。

- KDEX*nnnn*-*Z* メッセージテキスト
- KFPH*nnnnn*-*Z* メッセージテキスト

メッセージ ID は、次の内容を示しています。

K

システム識別子を示します。

DEX

JP1/IT Desktop Management 2 のメッセージ（データベース以外）であることを示します。

FPH

JP1/IT Desktop Management 2 のデータベースに関するメッセージであることを示します。

nnnn

メッセージの通し番号を示します。JP1/IT Desktop Management 2 のデータベースに関するメッセージの通し番号は 5 けたです。

Z

メッセージの種類を示します。

- E：エラーメッセージを示します。
- W：警告メッセージを示します。
- I：通知メッセージを示します。
- Q：ユーザーが応答する必要のあるメッセージを示します。

関連リンク

- 9.2　最小構成システムの構築時のトラブルシューティング
- 9.2.1　管理用サーバ構築時のトラブルシューティング
- 9.2.2　エージェントインストール時のトラブルシューティング
- 9.4　エージェントレス構成システムの構築時のトラブルシューティング
- 9.5　サポートサービス連携構成システムの構築時のトラブルシューティング
- 9.6　Active Directory 連携構成システムの構築時のトラブルシューティング
- 9.7　MDM 連携構成システムの構築時のトラブルシューティング
- 9.8　ネットワーク監視構成システムの構築時のトラブルシューティング
- 9.9　クラスタシステムの構築時のトラブルシューティング

9.2　最小構成システムの構築時のトラブルシューティング

機器を探索しても発見できない

ネットワークに接続した機器を探索しても発見できない場合は、設定画面の［機器の探索］－［探索条件の設定］画面で、探索範囲や認証情報の設定内容が正しいか確認してください。

管理対象の機器と管理用サーバ間で通信できない

提供媒体を使用して管理対象の機器にエージェントを導入した場合、エージェントのセットアップ情報は自動で設定されません。セットアップ情報が設定されていることを確認してください。設定されている場合は、次に示す内容を確認してください。

- 管理対象の機器に導入されているエージェントのセットアップ情報で、接続先の管理用サーバの名称およびポート番号の設定が正しいか。
- 管理用サーバのセットアップ情報で、ポート番号の設定が正しいか。

9.2.1　管理用サーバ構築時のトラブルシューティング

管理用サーバに JP1/IT Desktop Management 2 - Manager をインストールできない場合は、次に示す内容を確認してください。

- JP1/IT Desktop Management 2 - Manager に対応している OS かどうか。
- Administrator 権限を持つアカウントで Windows にログオンしたかどうか。

必要に応じて、インストール時のトラブルシュート用情報を`getinstlogs` コマンドで取得できます。`getinstlogs` コマンドについては、「8.9　getinstlogs（インストール時のトラブルシュート用情報の取得）」を参照してください。

取得できるログの種類

ログの種類	出力先	ファイル名	説明
インストーラートレースログファイル	• 正常に JP1/IT Desktop Management 2 - Manager がインストールされた場合 *JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*¥log • 正常に JP1/IT Desktop Management 2 - Manager がインストールされなかった場合	JDNINS01.log	インストーラーのトレースログファイルです。JP1/IT Desktop Management 2 - Manager をインストールするときに出力されます。

ログの種類	出力先	ファイル名	説明
インストーラートレースログファイル	%WINDIR%¥Temp¥JDNINST	JDNINS01.log	インストーラーのトレースログファイルです。JP1/IT Desktop Management 2 - Manager をインストールするときに出力されます。

9.2.2 エージェントインストール時のトラブルシューティング

コンピュータにエージェントをインストールできない場合、次に示す内容を確認してください。

- エージェントを導入するコンピュータの前提となる OS かどうか。
- Administrator 権限を持つアカウントで Windows にログオンしたかどうか。
- すでにインストールされているエージェントより古いバージョンのエージェントをインストールしようとしていないか。

また、必要に応じてエージェントのトラブルシュート用情報を採取してください。

エージェントのトラブルシュート用情報を採取するには：

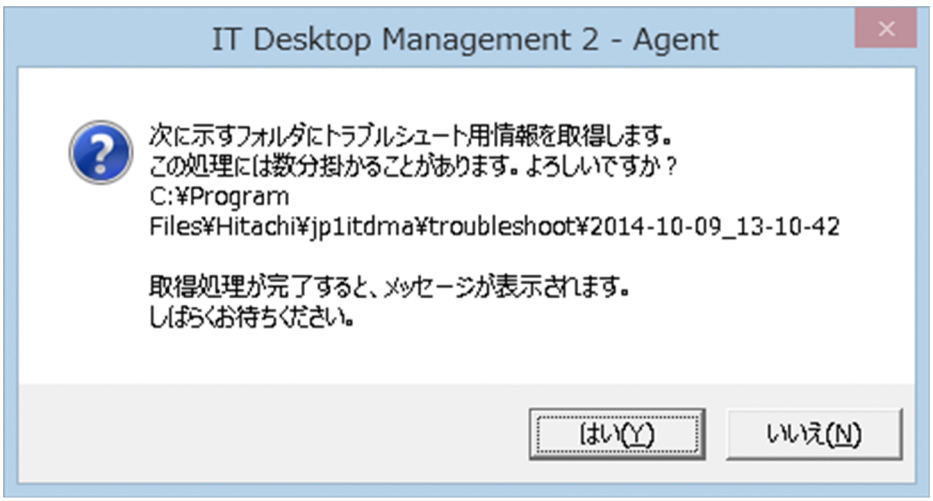
トラブルシュート用情報の採取は、トラブルが発生したコンピュータで実行してください。なお、Administrator 権限を持つユーザーで実行してください。

1.`getlogs.vbs` をダブルクリックする

`getlogs.vbs` の格納場所を次に示します。

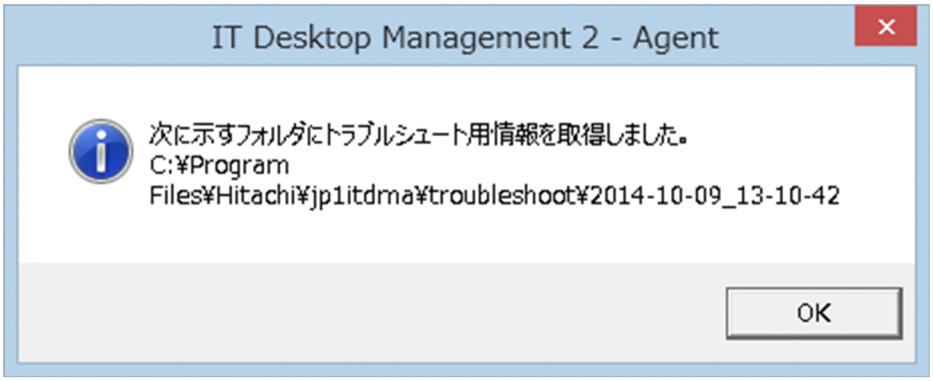
JP1/IT Desktop Management 2 - Agent のインストール先フォルダ¥bin

トラブルシュート用情報の取得を確認するダイアログが表示されます。



2.［はい］ボタンをクリックする

トラブルシュート用情報の採取が開始されます。トラブルシュート用情報の採取が終了すると、トラブルシュート用情報の採取が終了したことを示すダイアログが表示されます。



採取したトラブルシュート用情報は、次に示す場所に格納されます。

JP1/IT Desktop Management 2 - Agent のインストールフォルダ¥troubleshoot¥YYYY-MM-DD_hh-mm-ss※

注※　YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒

3. [OK] ボタンをクリックする

トラブルシュート用情報の採取が終了したことを示すダイアログが閉じます。

上記の方法で採取できるトラブルシュート用情報を次の表に示します。

トラブルシュート用情報	採取内容
エージェントのログ	*JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*¥log

システム情報	• システム情報
	msinfo32/nfo の結果
	• 環境変数
	SET コマンドの結果
	• レジストリ情報
	  • HKEY_LOCAL_MACHINE¥SOFTWARE¥Hitachi 以下のレジストリ
	  • HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Windows¥RemovableStorageDevices 以下のレジストリ
	• デバイス情報
	デバイスのプロパティ、状態
	• ファイル情報
	*JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*以下のサブフォルダおよびファイルの一覧
	• イベントログ
	アプリケーション、システム、セキュリティ

タスクスケジューラなどの機能を使用してバックグラウンドで実行する場合：

トラブル情報取得開始時およびトラブル情報取得完了時の確認メッセージを非表示にするための/s オプションを指定して、プログラム名および引数を設定してください。

（例）タスクスケジューラなどによるコマンド実行時に指定するコマンドライン

cscript.exe //B "*JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*¥bin¥getlog.vbs" /s

9.2.3 1 台のコンピュータに対して 2 つの機器情報が表示される場合のトラブルシューティング

1 台のコンピュータに対して 2 つのホスト識別子が登録されていると、JP1/IT Desktop Management 2 の操作画面では、1 台のコンピュータに対して 2 つの機器情報があるように表示されます。

この場合、設定画面の［機器の探索］－［管理対象機器］で 2 つの機器情報をいったん削除すれば、新しい機器情報だけが表示されるようになります。

9.3　オフライン管理構成システムの構築時のトラブルシューティング

次に示す場合は、管理形態を切り替えてください。管理形態を切り替える手順については、「9.3.1　オフライン管理からオンライン管理に切り替える手順」または「9.3.2　オンライン管理からオフライン管理に切り替える手順」を参照してください。

- オフライン管理したいコンピュータに対して、誤ってオンライン管理用のエージェントをインストールした場合
- オンライン管理したいコンピュータに対して、誤ってオフライン管理用のエージェントをインストールした場合

誤ったエージェントをインストールしたかどうかを判断するには、エージェントのセットアップ内容を確認してください。

また、ネットワークモニタを有効化するコンピュータに対して、誤ったエージェント設定を割り当てた場合は、設定の内容に応じて次の手順で対処してください。

[上位システムと通信する]のチェックを外したエージェント設定を割り当てた場合に対処するには：

1. 管理形態をオフライン管理からオンライン管理に切り替えます。
2. ネットワークモニタのサービスを、手動で開始します。

[コンピュータから収集した情報を、定期的に上位システムに通知する]のチェックを外したエージェント設定を割り当てた場合に対処するには：

1. エージェント設定の［基本設定］で、［コンピュータから収集した情報を、定期的に上位システムに通知する］をチェックします。

9.3.1　オフライン管理からオンライン管理に切り替える手順

利用者のコンピュータをオフライン管理からオンライン管理に切り替える場合は、エージェント設定を変更してから、利用者のコンピュータでセットアップを実行する必要があります。オンライン管理に切り替える手順を次に示します。

オンライン管理に切り替えるには（エージェント設定の変更）：

> **重要**
>
> オフライン管理からオンライン管理に変更した場合、利用者のコンピュータに適用されているセキュリティポリシーは、オンライン管理のコンピュータまたはグループへのセキュリティポリシーが自動的に適用されます。

1. エージェント設定の［基本設定］で、［上位システムと通信する］をチェックして［OK］ボタンをクリックします。

エージェント設定の変更が完了したら、利用者のコンピュータでのセットアップを実行します。

オンライン管理に切り替えるには（利用者のコンピュータでのセットアップ）：

1. エージェントをインストールしているコンピュータにログインします。
2. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Agent］－［管理者ツール］－［セットアップ］を選択します。

> **ヒント**
>
> セットアップを実行した時に、パスワードを入力するためのダイアログが表示される場合があります。このダイアログは、エージェントに割り当てたエージェント設定に、エージェントを保護するパスワードを設定している場合に表示されます。この場合、エージェント設定に設定した、エージェントを保護するパスワードを入力してください。

3. ［セットアップ（エージェント）］ダイアログで、［上位システムと通信する］をチェックして［OK］ボタンをクリックします。
4. 表示される確認ダイアログで［はい］ボタンをクリックします。

設定が完了し、対象のコンピュータはオンライン管理となります。

9.3.2 オンライン管理からオフライン管理に切り替える手順

利用者のコンピュータをオンライン管理からオフライン管理に切り替える場合は、エージェント設定を変更します。オフライン管理に切り替える手順を次に示します。

> **重要**
>
> オフライン管理に切り替える場合、再度オンライン管理に切り替える際の作業を考慮しておく必要があります。ネットワークに接続されていないコンピュータをオフライン管理からオンライン管理に切り替える場合は、切り替え対象となるすべてのコンピュータの、エージェントのセットアップでも変更が必要です。

オフライン管理に切り替えるには（エージェント設定の変更）：

> **重要**
>
> 対象のコンピュータに操作ログの取得を有効にしたセキュリティポリシーを割り当てている場合は、操作ログの取得を無効にしたセキュリティポリシーを割り当てたあとで、オンライン管

理に切り替えてください。操作ログの取得を有効にしたセキュリティポリシーを割り当てたままにした場合、利用者のコンピュータに操作ログのファイルが取得され続けます。

1. 設定画面の［エージェント］－［Windows エージェント設定とインストールセットの作成］を選択し、表示されたエージェント設定一覧から変更したいエージェント設定の［編集］ボタンをクリックします。
2. ［エージェント設定の編集］ダイアログの［基本設定］で、［上位システムと通信する］のチェックを外して［OK］ボタンをクリックします。
3. 表示される［上位システムとの通信の確認］ダイアログで、［OK］ボタンをクリックします。

設定が完了し、対象のコンピュータはオフライン管理となります。

9.4　エージェントレス構成システムの構築時のトラブルシューティング

エージェントレスのコンピュータを認証できない場合は、次に示す内容を確認してください。

管理用サーバの確認

- SNMP を利用して機器に接続するためのコミュニティ名が正しいか。
- Windows の管理共有のユーザー ID やパスワードが正しいか。

コンピュータの確認

- SNMP エージェントのサービスが正しく動作しているか。
- エージェントレスでの管理に必要な条件が満たされているか。

9.5　サポートサービス連携構成システムの構築時のトラブルシューティング

更新プログラム情報やウィルス対策製品情報を取得する際に、サポートサービスサイトに接続できない場合は、設定画面の［他システムとの接続］－［サポートサービスの設定］画面で設定した URL、ダウンロードご利用 ID、パスワードなどが正しいか確認してください。設定内容を変更した場合、［接続テスト］ボタンをクリックして、接続できるかどうか確認してください。

9.6 Active Directory 連携構成システムの構築時のトラブルシューティング

Active Directory に接続できない場合は、設定画面の［他システムとの接続］－［Active Directory の設定］画面で設定した内容が正しいか確認してください。

9.7 MDM 連携構成システムの構築時のトラブルシューティング

MDM 連携構成システムの構築時に、トラブルが発生した場合の対処方法について説明します。

スマートデバイスの情報が取得されない

接続先の MDM システムで認証できていない場合、スマートデバイスの情報は取得できません。

対処方法

イベント番号「1118」のイベント、またはメッセージ ID「KDEX5427-E」のメッセージが出力されていないか確認してください。出力されていた場合は、設定画面の［MDM 連携の設定］画面で設定したパスワードが誤っているおそれがあります。正しいパスワードを設定してください。

9.8　ネットワーク監視構成システムの構築時のトラブルシューティング

ネットワークモニタを有効にした場合に、ネットワークセグメント内に設置されているすべての機器がネットワーク接続できなくなったときは、ルータなどのネットワーク機器のネットワーク接続が許可されているか確認してください。許可されていない場合は、ルータなどのネットワーク機器のネットワーク接続を許可するように設定してください。

9.9　クラスタシステムの構築時のトラブルシューティング

稼働中の管理用サーバにトラブルが発生した場合に、バックアップ用のサーバへ自動的に運用が切り替わらない場合、セットアップで設定した内容を確認してください。

［クラスタ環境］画面での設定内容の確認

- ［クラスタ構成で IT Desktop Management 2 - Manager を運用する］がチェックされているか。
- 一方の管理用サーバで［現用系］が、もう一方の管理用サーバで［待機系］が選択されているか。
- 指定されている論理ホスト名、論理 IP アドレスは正しいか。

［フォルダの設定］画面での設定内容の確認

- 共有ディスクのフォルダが指定されているか。
- 指定されているフォルダのパスが正しいか。

9.10　JP1/NETM/NM - Manager 連携時のトラブルシューティング

JP1/NETM/NM - Manager 連携時にトラブルが発生した場合、JP1/NETM/NM - Manager の障害情報を収集します。収集した障害情報を、JP1/IT Desktop Management 2 のトラブルシュートの情報とあわせて、サポートサービスへ連絡してください。

収集の方法については、マニュアル「JP1 Version 9 JP1/NETM/Network Monitor - Manager」またはマニュアル「JP1 Version 10 JP1/NETM/Network Monitor - Manager」の障害時の対応の説明を参照してください。

付録

付録 A　参考情報

ここでは、JP1/IT Desktop Management 2 を使用する上での参考情報について説明します。

付録 A.1　ポート番号一覧

JP1/IT Desktop Management 2 で使用するポート番号について説明します。

特に断りがなければ、「管理用サーバ」は「統括管理用サーバ」と「管理用中継サーバ」を含みます。

ヒント

JP1/IT Desktop Management 2 - Manager と JP1/IT Desktop Management 2 - Operations Director で使用するポート番号はすべて同じ番号です。

JP1/IT Desktop Management 2 - Manager のポート番号一覧

管理用サーバ

管理用サーバのポート番号	接続方向	接続対象［ポート番号］	プロトコル	用途
ephemeral	→	JP1/Base の認証サーバ［20240］	TCP	JP1 ユーザーの認証時に、管理用サーバから認証サーバへの通信に使用されます。
31080	←	管理者のコンピュータ［ephemeral］	TCP	操作画面の参照または操作時に、管理者のコンピュータから管理用サーバへの通信に使用されます。 管理者のコンピュータにインストールされたリモートインストールマネージャ、パッケージャ、ネットワーク制御コマンドから管理用サーバへの通信でも使用されます。
31000	←	エージェント、中継システム、またはインターネットゲートウェイ［ephemeral］	TCP	エージェント、中継システム、またはインターネットゲートウェイから管理用サーバへの通信に使用されます。
31002	←	リモートインストールマネージャまたは管理用サーバ［ephemeral］	TCP	リモートインストールマネージャから管理用サーバへの通信に使用されます。
ephemeral	→	管理用中継サーバ、エージェント、または中継システム［31001］	TCP	リモートインストールマネージャを使用した配布をする場合に、管理用サーバから管理用中継サーバ、エージェント、中継システムへの通信に使用されます。

管理用サーバのポート番号	接続方向	接続対象［ポート番号］	プロトコル	用途
31006～31009、31011～31013	⬅ ➡	管理用サーバ［ephemeral］	TCP	管理用サーバ上で行われる内部処理の通信に使用されます。
31010	⬅	• リモートインストールマネージャ［ephemeral］ • Asset Console（jamTakeITDM2Info.exe）［ephemeral］	TCP	リモートインストールマネージャ、Asset Console から管理用サーバへの通信や内部処理に使用されます。
ephemeral	➡	管理用中継サーバ、エージェント、または中継システム［31001］	UDP	Wake On LAN を利用した電源制御をする際に使用されます。
ephemeral	➡	エージェントまたは中継システム［31014］	UDP	マルチキャスト配布をする場合に管理用サーバからエージェントまたは中継システムへの通信に使用されます。
31015	⬅	エージェントまたは中継システム［ephemeral］	UDP	マルチキャスト配布の再送要求をする場合にエージェントまたは中継システムから管理用サーバへの通信に使用されます。
31021	⬅	• リモートインストールマネージャ［ephemeral］ • エージェント［ephemeral］ • 中継システム［ephemeral］ • パッケージャ［ephemeral］ • 管理用中継サーバ［ephemeral］ • 管理用サーバ［ephemeral］ • インターネットゲートウェイ［ephemeral］	TCP	リモートインストールマネージャを使用した配布をする場合にリモートインストールマネージャ、エージェント、中継システム、パッケージャ、管理用中継サーバ、管理用サーバ、およびインターネットゲートウェイから管理用サーバへの通信に使用されます。
31023	⬅ ➡	管理用サーバまたは管理用中継サーバ［ephemeral］	TCP	管理用サーバと管理用中継サーバ間の通信に使用されます。

管理用サーバのポート番号	接続方向	接続対象［ポート番号］	プロトコル	用途
31026～31029	⬅ ➡	管理用サーバ［ephemeral］	TCP	API の使用時に、管理用サーバ上で行われる内部処理の通信に使用されます。
31030	⬅	外部システム［ephemeral］	TCP	API を使用した外部システムと管理用サーバ間の通信に使用されます。
ephemeral	➡	管理用中継サーバ、エージェント、または中継システム［16992］	TCP	AMT を使用したコンピュータの電源制御に使用されます。

各ポート番号は、製品の提供時にデフォルトとして設定されています。ご利用のシステム環境で、表に示すポート番号をすでに使用している場合は、セットアップで、重複しないポート番号に変更してください。

管理用サーバで、Windows ファイアウォールによってポート番号を制御している場合は、これらのポートを通過できるように設定してください。また、内部処理の通信に使用されるポートについても、同様にポートを通過できるように設定してください。なお、Windows ファイアウォールが有効になっている環境に JP1/IT Desktop Management 2 - Manager をインストールすると、自動的に Windows ファイアウォールを通過できるように設定されます（例外設定に登録されます）。

管理者のコンピュータ（リモートインストールマネージャ）

管理者のコンピュータのポート番号	接続方向	接続対象［ポート番号］	プロトコル	用途
ephemeral	➡	管理用サーバ［31002、31010、31021、31080］	TCP	リモートインストールマネージャを使用した配布をする場合に、リモートインストールマネージャから管理用サーバへの通信に使用されます。
ephemeral※	⬅ ➡	管理用サーバ［ephemeral※］	TCP	リモートインストールマネージャの内部処理に使用されます。
ephemeral	➡	中継システム［31021］	TCP	リモートインストールマネージャを使用して、中継システム上のパッケージを削除する場合に使用されます。

注※　データベースのエージェント接続で使用するポート番号を固定する手順を次に示します。

管理用サーバ(接続先)のポート番号を固定する場合

1. stopservice コマンドを実行し、管理用サーバのサービスを停止します。
2. *JP1/IT Desktop Management 2 - Manager インストール先フォルダ*¥mgr¥db¥CONF に格納されている pdsys ファイルをテキストエディタで開きます。
3.「set pd_service_port = *ポート番号*」の記述を追加し、ポート番号部分には固定したいポート番号を記述します。

（例）使用するポート番号に 10000 を指定する場合

```
set pd_service_port = 10000
```

4. startservice コマンドを実行し、管理用サーバのサービスを開始します。

リモートインストールマネージャ(接続先)のポート番号を固定する場合

受信用ポートは、デフォルトでは OS が自動でポート番号を割り当てます。なお、受信用ポートは 10 個以上使用されます。

1. リモートインストールマネージャおよびそのほかの JP1/IT Desktop Management 2 のアプリケーションを停止します。
2. *Remote Install Manager インストール先フォルダ*¥mgr¥dbclt に格納されている HiRDB.ini をテキストエディタで開きます。

   Remote Install Manager を管理用サーバと同じコンピュータにインストールした場合、HiRDB.ini は *JP1/IT Desktop Management 2 - Manager インストール先フォルダ*¥mgr¥dbclt に格納されています。
3. 「PDCLTRCVPORT=」に使用するポート番号の範囲を「*ポート番号-ポート番号*」の形式で指定します。なお、PDCLTRCVPORT= のあとに何も指定しないか「0」を指定した場合、使用するポート番号の範囲は設定されません。デフォルトでは、使用するポート番号の範囲は設定されていません。

   （例）使用するポート番号の範囲に 10000～10500 を指定する場合

   ```
   PDCLTRCVPORT=10000-10500
   ```
4. リモートインストールマネージャおよびそのほかの JP1/IT Desktop Management 2 のアプリケーションを起動します。

各ポート番号は、製品の提供時にデフォルトとして設定されています。ご利用のシステム環境で、表に示すポート番号をすでに使用している場合は、セットアップで、重複しないポート番号に変更してください。

管理者のコンピュータで、Windows ファイアウォールによってポート番号を制御している場合は、これらのポートを通過できるように設定してください。なお、Windows ファイアウォールが有効になっている環境に Remote Install Manager をインストールすると、自動的に Windows ファイアウォールを通過できるように設定されます（例外設定に登録されます）。

中継システムのポート番号一覧

中継システムのポート番号	接続方向	接続対象［ポート番号］	プロトコル	用途
16992	⬅	管理用サーバ［ephemeral］	TCP	AMT を使用したコンピュータの電源制御に使用されます。
31001	⬅	管理用サーバ［ephemeral］	TCP	リモートインストールマネージャを使用した配布をする場合に、管理用サーバから中継システムへの通信に使用されます。

中継システムのポート番号	接続方向	接続対象［ポート番号］	プロトコル	用途
31001	←	管理用サーバ [ephemeral]	UDP	Wake On LAN を利用した電源制御をする際に使用されます。
31002	←	• エージェント [ephemeral] • インターネットゲートウェイ [ephemeral]	TCP	リモートインストールマネージャを使用した配布をする場合に、エージェントおよびインターネットゲートウェイから中継システムへの通信に使用されます。
31014	←	管理用サーバ [ephemeral]	UDP	マルチキャスト配布をする場合に、管理用サーバから中継システムへの通信に使用されます。
31015	←	エージェント [ephemeral]	UDP	マルチキャスト配布の再送要求をする場合に、エージェントから中継システムへの通信に使用されます。
31021	←	リモートインストールマネージャ [ephemeral]	TCP	リモートインストールマネージャを使用して、中継システム上のパッケージを削除する場合に使用されます。
ephemeral	→	管理用サーバ [31015]	UDP	マルチキャスト配布の再送要求をする場合に、中継システムから管理用サーバへの通信に使用されます。
ephemeral	→	管理用サーバ [31021]	TCP	リモートインストールマネージャを使用した配布をする場合に、中継システムから管理用サーバへの通信に使用されます。
ephemeral	→	エージェント [16992]	TCP	AMT を使用したコンピュータの電源制御に使用されます。
ephemeral	→	エージェント [31001]	UDP	Wake On LAN を利用した電源制御をする際に使用されます。
ephemeral	→	エージェント [31014]	UDP	マルチキャスト配布をする場合に、中継システムからエージェントへの通信に使用されます。
ephemeral	→	エージェント [31001]	TCP	中継システムからエージェントへの通信、およびリモートインストールマネージャを使用した配布に使用されます。

コントローラおよびリモコンエージェントのポート番号一覧

コントローラまたはリモコンエージェント [ポート番号]	接続方向	接続対象［ポート番号］	プロトコル	用途
リモコンエージェント [31016]	←	コントローラ [ephemeral]	TCP	コントローラからリモコンエージェントへの画面操作に使用されます。
リモコンエージェント [31017]	←	コントローラ [ephemeral]	TCP	コントローラからリモコンエージェントへのファイル転送に使用されます。

コントローラまたはリモコンエージェント[ポート番号]	接続方向	接続対象［ポート番号］	プロトコル	用途
リモコンエージェントまたはコントローラ[31018]（チャットサーバとして使用している場合）	⬅ ➡	リモコンエージェントまたはコントローラ［ephemeral］	TCP	チャットに使用されます。
リモコンエージェント[ephemeral]	➡	コントローラ[31019]	TCP	リモコンエージェントからコントローラへのリモート接続の要求に使用されます。
リモコンエージェント[ephemeral]	➡	コントローラ[31020]	TCP	リモコンエージェントからコントローラへのコールバックによるファイル転送に使用されます。
コントローラ[ephemeral]	➡	RFB 接続対象機器[5900]	TCP	RFB 接続によるリモートコントロールをする際に使用されます。
コントローラ[ephemeral]	➡	リモコンエージェント［16992］	TCP	AMT を使用したコンピュータの電源制御に使用されます。
コントローラ[ephemeral]	➡	リモコンエージェント［31016］	UDP	Wake On LAN を利用した電源制御をする際に使用されます。

コントローラをインストールしたコンピュータおよびリモートコントロールの対象のコンピュータで、Windows ファイアウォールによってポート番号を制御している場合は、これらのポートを通過できるように設定してください。なお、Windows ファイアウォールが有効になっている環境にコントローラおよびリモコンエージェントをインストールすると、自動的に Windows ファイアウォールを通過できるように設定されます（例外設定に登録されます）。

各ポート番号は、製品の提供時にデフォルトとして設定されています。ご利用のシステム環境で、表に示すポート番号をすでに使用している場合は、次のようにして重複しないポート番号に変更してください。

- コントローラのポート番号
  コントローラの［環境の設定］ダイアログで設定する。
- リモコンエージェントのポート番号
  エージェント設定の［リモートコントロールの設定］で設定する。
- チャット機能のポート番号
  ［チャット］ウィンドウの［環境の設定］ダイアログー［接続］タブで設定する。

JP1/IT Desktop Management 2 - Agent のポート番号一覧

エージェントのポート番号	接続方向	接続対象［ポート番号］	プロトコル	用途
31001	⬅	管理用サーバ[ephemeral]	TCP	管理用サーバからエージェントへの通信に使用されます。

エージェントのポート番号	接続方向	接続対象［ポート番号］	プロトコル	用途
31001	←	管理用サーバまたは中継システム［ephemeral］	UDP	Wake On LAN を利用した電源制御をする際に使用されます。
16992	←	管理用サーバまたは中継システム［ephemeral］	TCP	AMT を使用したコンピュータの電源制御に使用されます。
ephemeral	→	中継システム［31002］	TCP	リモートインストールマネージャを使用した配布をする場合に、エージェントから中継システムへの通信に使用されます。
31014	←	管理用サーバまたは中継システム［ephemeral］	UDP	マルチキャスト配布をする場合に、管理用サーバまたは中継システムからエージェントへの通信に使用されます。
ephemeral	→	管理用サーバまたは中継システム［31015］	UDP	マルチキャスト配布の再送要求をする場合に、エージェントから管理用サーバ、中継システムへの通信に使用されます。
ephemeral	→	管理用サーバ［31021］	TCP	リモートインストールマネージャを使用した配布をする場合に、エージェントから管理用サーバへの通信に使用されます。
31024	←	エージェント［ephemeral］	TCP	インターネットゲートウェイを経由して上位システムと通信するエージェントで、エージェントとインターネットゲートウェイの間で通信する場合に、エージェント内部での通信に使用されます。
31025	←	エージェントまたは管理用中継サーバ［ephemeral］	TCP	インターネットゲートウェイを経由して上位システムと通信するエージェントまたは管理用中継サーバで、エージェントまたは管理用中継サーバとインターネットゲートウェイの間で通信する場合に、エージェントまたは管理用中継サーバ内部での通信に使用されます。
ephemeral	→	インターネットゲートウェイ［443］	TCP	インターネットゲートウェイを経由した通信に使用されます。

各ポート番号は、製品の提供時にデフォルトとして設定されています。ご利用のシステム環境で、表に示すポート番号をすでに使用している場合は、管理用サーバのセットアップで重複しないポート番号に変更してください。

エージェント導入済みのコンピュータで、Windows ファイアウォールによってポート番号を制御している場合は、ポートを通過できるように設定してください。なお、Windows ファイアウォールが有効になっている環境にエージェントをインストールすると、自動的に Windows ファイアウォールを通過できるように設定されます（例外設定に登録されます）。

また、JP1/IT Desktop Management 2 - Manager と JP1/IT Desktop Management 2 - Agent の間のネットワークで、ファイアウォールによってポートを制御している場合は、表に示すポートを通過できるように設定してください。

エージェントレスの機器のポート番号

エージェントレスの機器の場合、機器の認証状態によって、Windows の管理共有または SNMP のポート番号が使用されます。

インターネットゲートウェイのポート番号一覧

インターネットゲートウェイのポート番号	接続方向	接続対象［ポート番号］	プロトコル	用途
443	←	エージェント［ephemeral］	TCP	インターネットゲートウェイを経由した通信に使用されます。

付録 A.2　エージェントの環境を変更した場合の認識方法

エージェントを導入したコンピュータは、機器を識別するためのユニークな ID（ホスト識別子）が生成されます。

コンピュータの環境を変更した場合、変更方法によってホスト識別子が再生成されるかどうかが異なります。ホスト識別子が再生成されると、環境を変更する前の機器とは異なる機器として認識されます。

ホスト識別子は、次のような場合に再生成されます。

- OS を再インストールした場合
- OS がインストールされたハードディスクを交換した場合
- マザーボードを交換した場合※
- ディスクコピーを利用して、ほかのコンピュータにエージェントを導入した場合※
- resetnid.vbs コマンドを実行した場合
- ホスト識別子管理ファイルが不正となり、再作成された場合

注※　すでにホスト識別子が再生成されていた場合は、環境を変更する前の機器と同じ機器として認識されます。

上記以外の場合は、ホスト識別子は再生成されません。例えば、次のような場合は、ホスト識別子は再生成されません。

- エージェントをアンインストールした場合
- エージェントをアンインストールしたあとに、エージェントを再インストールした場合
- エージェントを上書きインストールした場合

- CPU、メモリ、またはネットワークカードを交換した場合
- OS をアップグレードした場合
- ハードディスクを増設した場合

> **ヒント**
>
> 異なる機器として認識された場合は、環境を変更する前の機器情報やハードウェア資産情報が管理用サーバに残った状態になります。必要に応じて情報を削除してください。

付録 A.3　Citrix XenApp、Microsoft RDS サーバ環境構築手順

Citrix XenApp、Microsoft RDS サーバを JP1/IT Desktop Management 2 で管理するために必要な手順について説明します。

- インストールセットの作成
- エージェントのインストール
- セキュリティポリシーの割り当て
- あて先グループのポリシーの作成

(1)　インストールセットの作成

Citrix XenApp、Microsoft RDS サーバにインストールするためのエージェントのインストールセットの作成手順を次に示します。なお、インストールセットは、管理者が作成してください。

また、エージェントを管理用サーバに登録しておく必要があります。エージェントを管理用サーバに登録する手順の詳細については、「5.9　コンポーネントを登録する手順」を参照してください。

ここでは、Citrix XenApp、Microsoft RDS サーバを管理するための手順について説明しています。その他の必要な設定については、「1.6　エージェントを手動でインストールする」を参照してください。

1. **管理用サーバのサービスを停止する。**

   サービスの停止は、`stopservice` コマンド（サービス停止）を実行します。

2. **コンフィグレーションファイル（jdn_manager_config.conf）を編集する。**

   AgentStartMenu_Display の値を OFF に設定してください。（エージェントの接続先を変更する場合など、セットアップの実行が必要な場合は、*エージェントのインストールフォルダ*¥bin¥jdngsetup.exe を実行してください。）

   コンフィグレーションファイル（jdn_manager_config.conf）の詳細については、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」のプロパティ一覧を参照してください。

3. **管理用サーバのサービスを開始する。**

サービスの開始は、startservice コマンド（サービス開始）を実行します。

4. JP1/IT Desktop Management 2 の操作画面にログインする。

5. エージェント設定を追加する。

設定画面のメニューエリアにある［Windows エージェント設定とインストールセットの作成］を選択し、［Windows エージェント設定とインストールセットの作成］画面で［エージェント設定を追加］ボタンをクリックします。［エージェント設定の追加］ダイアログボックスで、Citrix XenApp、Microsoft RDS サーバのエージェント設定を追加します。推奨するエージェント設定については、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」のパラメーター一覧を参照してください。

6. インストールセット設定項目を設定する。

［Windows エージェント設定とインストールセットの作成］画面から、作成したエージェント設定を選択して［インストールセットを作成］ボタンをクリックします。［インストールセットの作成］ダイアログボックスで、インストールセットの設定項目を設定します。

［インストールするコンポーネントの設定］では、［JP1/IT Desktop Management 2 - Agent(エージェント)］を選択し、［リモコンエージェント］のチェックをオフにしてください。

7. インストールセットを作成する。

(2) エージェントのインストール

Citrix XenApp、Microsoft RDS サーバにエージェントをインストールする手順を次に示します。この手順では、管理者がインストールセットを作成し、エージェントをインストールしたマスターイメージを作成します。

ここでは、Citrix XenApp、Microsoft RDS サーバを管理するための手順について説明しています。その他の必要な設定については、「1.6 エージェントを手動でインストールする」を参照してください。

1. エージェントのインストール先の Citrix XenApp、Microsoft RDS サーバに管理者権限でログインする。

2. インストールセットを使用してエージェントをインストールする。

インストールは管理者権限で実行してください。

3. Citrix XenApp、Microsoft RDS サーバを一般の Windows のコンピュータと区別する設定をレジストリへ設定する。

レジストリエディタなどを使用して、Citrix XenApp、Microsoft RDS サーバにレジストリ情報を追加してください。設定するレジストリ情報の例を次に示します。

キー	HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Hitachi¥JP1/IT Desktop Management - Agent
値名	RdsServerType
型	REG_SZ

値	XenApp_RDS_Server

4. 管理者権限で起動したコマンドプロンプトから、次のコマンドを実行する。

```
エージェントのインストールフォルダ¥bin¥jdngsetrdsconf.bat LOGSETTING
```

このコマンドは、エージェントの内部ログのサイズ拡張を設定するコマンドです。実行後、次のメッセージが表示されることを確認してください。※

```
The operation completed successfully.
```

注※　コマンド実行時に発生する可能性のあるエラーと対処を次に示します。

Inputted parameter is invalid.

対処：コマンド実行時の LOGSETTING オプションが正しく指定されていることを確認してください。

Access to the registry is denied.

対処：管理者権限でコマンドを実行していることを確認してください。

Failed to create an INI file.

対処 1：管理者権限でコマンドを実行していることを確認してください。

対処 2：*エージェントのインストールフォルダ*¥conf フォルダへのアクセス権があることを確認してください。

5. Windows ファイアウォールにエージェントの通信用ポートの例外を登録する。

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。

```
netsh advfirewall firewall add rule name="JP1/IT Desktop Management 2 - Agent Service" dir=in action=allow protocol=TCP localport=エージェントの起動要求用のポート番号
```

実行例を次に示します。

```
netsh advfirewall firewall add rule name="JP1/IT Desktop Management 2 - Agent Service" dir=in action=allow protocol=TCP localport=31001
```

なお、管理用サーバで、セットアップの［エージェントの起動要求用のポート番号］をデフォルト値（31001）から変更する場合は、実行するコマンドの*エージェントの起動要求用のポート番号*も変更してください。

6. resetnid.vbs コマンド（ホスト識別子のリセット）を実行する。

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。

```
cscript.exe エージェントのインストールフォルダ¥bin¥resetnid.vbs /nodeid /i
```

resetnid.vbs コマンド（ホスト識別子のリセット）の詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のホスト識別子のリセット（resetnid.vbs）の説明を参照してください。

7. ツールなどでマスターイメージを作成する。

8. マスターイメージを Citrix XenApp、Microsoft RDS サーバにコピーしてから OS を再起動する。

9. ログインする。

エージェントが動作します。

(3) セキュリティポリシーの割り当て

Citrix XenApp、Microsoft RDS サーバのセキュリティポリシーを作成し、割り当てる手順を次に示します。その他の必要な設定については、「1.6 エージェントを手動でインストールする」を参照してください。

1. JP1/IT Desktop Management 2 の操作画面にログインする。

2. 追加管理項目を設定する。

設定画面の［資産管理項目の設定］画面にある［ハードウェア資産情報の追加管理項目］で、「(2) エージェントのインストール」で設定したレジストリ情報を取得するための項目を追加してください。

追加管理項目の例を次に示します。

項目名		Citrix XenApp、Microsoft RDS サーバ識別情報
入力方法		レジストリから取得
データ型		テキスト型
レジストリパス	ルートキー	HKEY_LOCAL_MACHINE
	パス	SOFTWARE¥Wow6432Node¥Hitachi¥JP1/IT Desktop Management - Agent
	レジストリ名	RdsServerType

3. ユーザー定義のグループを追加する。

セキュリティ画面または機器画面のメニューエリアにある［機器一覧（ユーザー定義）］で、追加管理項目を条件とするユーザー定義のグループを追加してください。

ユーザー定義グループの例を次に示します。

グループ名		Citrix XenApp、Microsoft RDS サーバ
条件	対象項目	Citrix XenApp、Microsoft RDS サーバ識別情報
	判定条件	判定値と等しい
	判定値	XenApp_RDS_Server

4. セキュリティポリシーを作成する。

セキュリティ画面のメニューエリアにある［セキュリティポリシー一覧］を選択し、［セキュリティポリシー一覧］画面で［追加］ボタンをクリックし、［セキュリティポリシーの追加］ダイアログボックスでセキュリティポリシーを作成してください。推奨するセキュリティポリシーについては、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」のセキュリティポリシーに設定できる項目を参照してください。

5. セキュリティポリシーを割り当てる。

セキュリティ画面のメニューエリアにある［機器一覧（ユーザー定義）］から、作成したユーザ定義のグループを選択します。Citrix XenApp、Microsoft RDS サーバの一覧が表示されるので、すべて選択します。［操作メニュー］－［ポリシーを割り当てる］を選択して、［ポリシーの割り当て］ダイアログボックスを表示します。作成した Citrix XenApp、Microsoft RDS サーバのセキュリティポリシーを選択して、割り当てます。

(4) あて先グループのポリシーの作成

リモートインストールマネージャを使用した配布を行う場合は、あて先グループのポリシーを作成することで、Citrix XenApp、Microsoft RDS サーバのあて先グループを作成することができます。

ここでは、Citrix XenApp、Microsoft RDS サーバのあて先グループを作成するための、ポリシー作成手順について説明します。その他の必要な設定については、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」を参照してください。

1. JP1/IT Desktop Management 2 のリモートインストールマネージャにログインする。

2. ［ハードウェア資産情報の追加管理項目によるグルーピング］ダイアログボックスを表示する。

［あて先］ウィンドウのメニューから、［ファイル］－［グループの新規作成］－［あて先グループのポリシーの作成］を選択して［ポリシーの設定］ダイアログボックスを表示します。［追加］ボタンをクリックして、［あて先グループの自動メンテナンス］を選択し、［ハードウェア資産情報の追加管理項目によるグルーピング］を選択すると、［ハードウェア資産情報の追加管理項目によるグルーピング］ダイアログボックスが表示されます。

3. Citrix XenApp、Microsoft RDS サーバを区別するための追加管理項目を設定したポリシーを追加する。

あて先グループのポリシーの例を次に示します。

ポリシー種別	ハードウェア資産情報の追加管理項目によるグルーピング	
ハードウェア資産情報の追加管理項目	1 階層目	Citrix XenApp、Microsoft RDS サーバ識別情報
	2 階層目	（指定なし）
	3 階層目	（指定なし）
	4 階層目	（指定なし）
	5 階層目	（指定なし）
	6 階層目	（指定なし）
経路	（指定なし）	

付録 A.4　共有型 VDI の環境構築手順

共有型 VDI の仮想コンピュータを JP1/IT Desktop Management 2 で管理するために必要な手順について説明します。

インストールセットの作成およびインストール

共有型 VDI の仮想コンピュータにエージェントをインストールする手順を次に示します。この手順では、管理者がインストールセットを作成し、マスタ PC にエージェントをインストールしたマスターイメージを作成します。

ここでは、VMware Horizon View、Citrix Virtual Desktops の仮想コンピュータを管理するための手順について説明しています。その他の必要な設定については、「1.6　エージェントを手動でインストールする」を参照してください。

1. JP1/IT Desktop Management 2 の操作画面にログインする。

2. エージェント設定を追加する。

   設定画面のメニューエリアにある［Windows エージェント設定とインストールセットの作成］を選択し、［Windows エージェント設定とインストールセットの作成］画面で［エージェント設定を追加］ボタンをクリックします。［エージェント設定の追加］ダイアログボックスで、共有型 VDI の仮想コンピュータのエージェント設定を追加します。

   ［利用者への通知設定］－［利用者のコンピュータでの表示設定］－［利用者入力画面の表示時］を「非表示」に設定します。

   エージェント設定については、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」のパラメーター一覧を参照してください。

3. インストールセット設定項目を設定する。

   ［Windows エージェント設定とインストールセットの作成］画面から、作成したエージェント設定を選択して［インストールセットを作成］ボタンをクリックします。［インストールセットの作成］ダイアログボックスで、インストールセットの設定項目を設定します。

   ［インストールフォルダの設定］－［ホスト識別子生成時の設定］－［仮想コンピュータの情報を基にホスト識別子を生成する］をチェックします。また、管理する仮想コンピュータの展開方式に合わせて、使用する機器情報を選択します。

   VMware Horizon View を使用する場合、または Citrix Virtual Desktops で MCS（Machine Creation Services）方式を使用する場合

   　コンピュータ名または IP アドレス

   Citrix Virtual Desktops で PVS（Provisioning Services）方式を使用する場合

   　アカウント名

   インストールセット設定項目については、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」のパラメーター一覧を参照してください。

4. インストールセットを作成する。

5. エージェントのインストール先のマスタ PC に管理者権限でログインする。

6. インストールセットを使用してエージェントをインストールする。

インストールは管理者権限で実行してください。

ログオフスクリプトの登録

仮想コンピュータの操作ログを管理する場合は、マスタ PC のログオフスクリプトにコマンドを登録します。

1. [ローカルグループポリシー] − [Windows の設定] − [スクリプト（ログオン/ログオフ)] − [ログオフ] を選択する。

[ログオフのプロパティ] ダイアログが表示されます。

2. スクリプトを追加する。

upldoplog コマンドをスクリプトとして登録します。

スクリプト名

エージェントのインストールフォルダ¥bin¥upldoplog.exe

スクリプトのパラメータ

/upload

upldoplog コマンドの詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の「upldoplog（操作ログのアップロード)」を参照してください。

重要

共有型 VDI の仮想コンピュータでは、ログオフすると仮想コンピュータが初期化されるため、ログオフ前にupldoplog コマンドでエージェントの操作ログを管理用サーバにアップロードする必要があります。操作ログのアップロードについての注意事項を次に示します。

- 操作ログのアップロード中に操作した分の操作ログはアップロードされず、ログオフすると操作ログが削除されます。
- 操作ログのアップロード中に障害が発生しアップロードに失敗すると、操作ログは削除されます。

マスタ PC の設定

1. 仮想コンピュータに割り当てるセキュリティポリシーを作成し、マスタ PC に割り当てる。

セキュリティポリシーの利用手順は、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の「セキュリティポリシーを利用する」を参照してください。

> **メモ**
>
> マスタ PC が複数ある場合は、ホスト名などでフィルタを作成すると確認が容易になります。フィルタの詳細は、マニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」の「フィルタの利用」を参照してください。

2. **仮想コンピュータで使用するソフトウェアや更新プログラムなどをマスタ PC にインストールする場合は、ソフトウェアを配布する。**

   ソフトウェアの配布の詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の「ソフトウェアやファイルを配布する」を参照してください。

3. **機器画面で、ホスト識別子が機器情報から生成されていることを確認する。**

   機器画面に［ホスト識別子］が表示されていない場合は、一覧の項目名を右クリックして［表示項目の選択］を選択してください。表示されるダイアログで［ホスト識別子］をチェックして［OK］ボタンをクリックすると、表示項目に［ホスト識別子］が表示されます。

一般化およびマスタイメージ作成

マスタイメージを作成するために、エージェントの固有情報を削除し一般化します。次のコマンドを実行します。

```
upldoplog /upload
prepagt.bat /prep
```

コマンドの詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」を参照してください。

> **メモ**
>
> `prepagt.bat` コマンドは、アップロードしていない操作ログを削除します。このため、マスタ PC の操作ログを管理する場合は、事前に操作ログをアップロードするために、`upldoplog` コマンドを実行します。

一般化したら、マスタ PC からマスタイメージを作成します。マスタイメージの作成方法については、各仮想化製品のマニュアルを参照してください。

展開

マスタイメージから仮想コンピュータを作成します。仮想コンピュータの作成方法については、各仮想化製品のマニュアルを参照してください。

> **重要**
>
> インスタントクローンで展開する場合は、作成した仮想コンピュータを再起動してください。

仮想コンピュータの利用状況確認

仮想コンピュータの利用状況は、機器画面で確認します。機器画面のフィルタ条件で［ホスト識別子（部分一致)］を選択し、次の先頭文字列を指定します。

- コンピュータ名：#GII
- アカウント名：#GIO
- IP アドレス：#GIY

> **メモ**
>
> フィルタされた機器一覧には、マスタ PC も含まれます。マスタ PC を機器一覧のフィルタから除外するには、マスタ PC のホスト名を含まないようにフィルタ条件を設定してください。

仮想コンピュータの利用者の操作ログは、セキュリティ画面の［操作ログ］－［操作ログ一覧］で確認できます。

付録 A.5　外部システム連携構成で HTTPS を使用する場合の環境構築

ここでは、外部システム連携構成で HTTPS 接続を使用する場合の環境構築およびコマンドについて説明します。

(1)　環境構築の流れ

外部システム連携構成で、HTTPS 接続を使用する場合に必要な手順について説明します。

管理用サーバの SSL 通信用証明書の取得

管理用サーバの SSL 通信用証明書（ルート証明書および SSL サーバ証明書）は、証明書発行機関から取得します。

管理用サーバの SSL 通信用証明書を取得する流れを次に示します。

1. Web サーバの秘密鍵を作成する。(openssl.bat genrsa コマンド)
2. 証明書発行要求（CSR）を作成する。(openssl.bat req コマンド)
3. 証明書発行要求（CSR)の内容を表示する。(openssl.bat req コマンド)
   必要に応じて証明書発行要求（CSR）の内容を確認します。
4. 証明書発行要求（CSR）を認証局（CA）に提出する。
5. 認証局（CA）から署名済みの証明書を取得する。

ヒント

取得した証明書の内容はopenssl.bat x509 コマンドで確認できます。

ヒント

取得した証明書の"-----BEGINCERTIFICATE-----"から、"-----END CERTIFICATE----"の部分をhttpsd.pem ファイルに保存します。

関連リンク

- (a) Web サーバの秘密鍵の作成（openssl.bat genrsa）
- (b) 証明書発行要求（CSR）の作成（openssl.bat req）
- (c) 証明書発行要求（CSR）の内容表示（openssl.bat req）
- (d) 証明書の内容表示（openssl.bat x509）
- (e) 証明書の形式変換（openssl.bat x509）

管理用サーバのセットアップ

1. Administrator 権限を持つユーザーで OS にログオンする。
2. 管理用サーバの JP1/IT Desktop Management 2 のサービスを停止する。

   次のコマンドを実行します。

   ```
   stopservice
   ```

   コマンドの詳細は、マニュアル「JP1/IT Desktop Management 2 運用ガイド」を参照してください。
3. SSL サーバ証明書および秘密鍵を管理用サーバの次のフォルダに格納する。

   ```
   JP1/IT Desktop Management 2 - Managerのインストールフォルダ¥mgr¥uCPSB¥httpsd¥conf¥ssl¥server
   ```

   格納するファイルを次に示します。

   - SSL サーバ証明書ファイル：httpsd.pem
   - 秘密鍵ファイル：httpsdkey.pem

   メモ

   HTTPS 接続の設定から HTTP 接続の設定に変更する場合、格納した SSL サーバ証明書および秘密鍵を削除してください。
4. コンフィグレーションファイルに設定を追加する。

   コンフィグレーションファイル（jdn_manager_config.conf）の格納先は次のとおりです。

JP1/IT Desktop Management 2 - Managerのインストールフォルダ¥mgr¥conf

コンフィグレーションファイルに「RestAPIProtocol=1」の行を追加してください。

メモ

HTTPS 接続の設定から HTTP 接続の設定に変更する場合、コンフィグレーションファイルの「RestAPIProtocol=1」の行を「RestAPIProtocol=0」に変更してください。追加した RestAPIProtocol の行は削除しないでください。

5. Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Manager］－［ツール］－［セットアップ］を選択する。
6. セットアップ画面で［次へ］ボタンをクリックする。
7. ［セットアップの選択］画面で、［設定変更］を選択して［次へ］ボタンをクリックする。
8. ［API の設定］画面が表示されるまで、［次へ］ボタンをクリックする。
9. ［API を使用する］をチェックする。
10. ［次へ］ボタンをクリックする。
11. ［セットアップの確認］画面が表示されるまで、［次へ］ボタンをクリックする。
12. ［セットアップの確認］画面で設定内容を確認して、［次へ］ボタンをクリックする。

    リモートインストールマネージャ、JP1/IT Desktop Management 2 - Asset Console の停止を確認するダイアログが表示されます。確認したあとに、［OK］ボタンをクリックしてください。クラスタシステム構成の場合は、ダイアログに表示されたサービスに関連づけされたクラスタリソースをオフラインにしたあとに、［OK］ボタンをクリックしてください。
13. ［リモートインストールマネージャを使用した配布のセットアップ］画面で、［OK］ボタンをクリックする。

    セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、［セットアップを終了します］画面が表示されます。

重要

手順 13 で「サービスの開始に失敗しました。サービス名＝ JP1_ITDM2_Web Server」のダイアログが表示された場合、［OK］ボタンをクリックしてダイアログを閉じ、セットアップを完了させてください。次に手順 3 の SSL サーバ証明書ファイルおよび秘密鍵ファイルを見直して、JP1_ITDM2_Web Server のサービスを直接起動してください。また、「セットアップ中にエラーが発生しました。」のダイアログが表示される場合は、手順 4 の RestAPIProtocol の設定値が正しく設定されていることを確認してください。

14. ［セットアップを終了します］画面で、［OK］ボタンをクリックする。

メモ

クラスタシステムの場合は、現用系サーバおよび待機系サーバに設定してください。

(2) SSL 通信用証明書の取得に使用するコマンド

SSL 通信用証明書の取得に使用するコマンドについて説明します。

コマンドは次のフォルダに格納されています。

JP1/IT Desktop Management 2 - Managerのインストールフォルダ¥mgr¥uCPSB¥httpsd¥sbin

(a) Web サーバの秘密鍵の作成（openssl.bat genrsa）

機能

Web サーバの秘密鍵を作成します。

形式

openssl.bat△genrsa△-rand△*ファイル名*[:*ファイル名...*]△-out△*鍵ファイル*△[512|1024|2048|4096]

オペランド

-rand△*ファイル名*[:*ファイル名...*]

乱数生成に利用する任意のファイルを指定します。

-out△*鍵ファイル*

Web サーバの秘密鍵を出力するファイルを指定します。

512¦1024¦2048¦4096

作成する Web サーバの秘密鍵のビット長を指定します。このオペランドを省略した場合、「2048」が仮定されます。

注意事項

3 文字以下のパスワードを入力した場合、4 文字以上 1,023 文字以下の入力を促すメッセージが出力されますが、このバージョンでは 4 文字以上 64 文字以下でパスワードを入力してください。なお、パスワード入力時に 65 文字以上入力した場合でもエラーになりません。

使用例

Web サーバの秘密鍵httpsdkey.pem を作成する場合の使用例を次に示します。

```
openssl.bat genrsa -rand C:¥WINNT¥NOTEPAD.EXE -out httpsdkey.pem 2048
```

関連リンク

- (b)　証明書発行要求（CSR）の作成（openssl.bat req）

(b)　証明書発行要求（CSR）の作成（openssl.bat req）

機能

証明書発行要求（CSR）を作成します。ここで作成した CSR ファイルを認証局（CA）に提出して、署名済みの証明書を発行してもらいます。CSR は、PKCS#10 に準拠した形式で作成されます。

形式

```
openssl.bat△req△-new△-sha256△-key△鍵ファイル△-out△CSRファイル
```

オペランド

-sha256

　CSR 作成時の署名アルゴリズムとして、sha256WithRSAEncryption を使用することを指定します。

-key△*鍵ファイル*

　Web サーバの秘密鍵のファイルを指定します。

-out△*CSR ファイル*

　作成した CSR を出力するファイルを指定します。

使用例

Web サーバの秘密鍵`httpsdkey.pem` を使用して証明書発行要求（CSR）を作成する場合の使用例を次に示します。

```
openssl.bat req -new -sha256 -key httpsdkey.pem -out httpsd.csr
```

Web サーバの秘密鍵作成時にパスワードを設定した場合は、パスワードの入力要求があります。また、設定する項目については証明書発行要求（CSR）を提出する認証局（CA）の指示に従ってください。

(c)　証明書発行要求（CSR）の内容表示（openssl.bat req）

機能

証明書発行要求（CSR）の内容を表示します。

形式

```
openssl.bat△req△-in△CSRファイル△-text
```

オペランド

-in△*CSR ファイル*

表示する CSR ファイルを指定します。

使用例

証明書発行要求httpsd.csr を表示する場合の使用例を次に示します。

```
openssl.bat req -in httpsd.csr -text
```

(d) 証明書の内容表示（openssl.bat x509）

機能

証明書ファイルの内容を表示します。"-----BEGIN CERTIFICATE-----"から、"-----END CERTIFICATE----"の証明書ファイルの内容を表示します。

形式

```
openssl.bat△x509△-in△証明書ファイル△-text
```

オペランド

-in△*証明書ファイル*

表示する証明書ファイルを指定します。

使用例

証明書httpsd.pem を表示する場合の使用例を次に示します。

```
openssl.bat x509 -in httpsd.pem -text
```

(e) 証明書の形式変換（openssl.bat x509）

機能

証明書の形式を変換します。必要に応じて使用します。

形式

```
openssl.bat△x509△-inform△入力形式△-outform△出力形式△-in△入力ファイル△-out△出力ファイル
```

オペランド

-inform△*入力形式*

変換前の証明書ファイルの入力形式を指定します。指定できる入力形式は次のとおりです。

- DER
- PEM

-outform△*出力形式*

変換後の証明書ファイルの出力形式を指定します。指定できる出力形式は次のとおりです。

- DER
- PEM

-in△*入力ファイル*

変換前の証明書ファイルを指定します。

-out△*出力ファイル*

変換後の証明書ファイルを指定します。

付録 A.6　各バージョンの変更内容

(1)　13-50 の変更内容

(a)　資料番号（3021-3-L73-40）の変更内容

- Windows Server 2025 を次の製品の適用 OS に追加した。
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
  - JP1/IT Desktop Management 2 - Asset Console
  - JP1/IT Desktop Management 2 - Internet Gateway
- JP1/IT Desktop Management 2 の認証を認証プロバイダーで実行できる IDaaS 連携機能を追加した。

(2)　13-11 の変更内容

(a)　資料番号（3021-3-L73-30）の変更内容

- 連携する MDM システムとして Google Workspace を使用する場合、Chromebook デバイスを管理できるようにした。

(3) 13-10 の変更内容

(a) 資料番号（3021-3-L73-20）の変更内容

- インターネット経由で管理用中継サーバからインターネットゲートウェイサーバに接続できるようにした。
- checkitdmigw（インターネットゲートウェイ接続先設定ファイルのフォーマットチェック）コマンドを追加した。

(4) 13-01 の変更内容

(a) 資料番号（3021-3-L73-10）の変更内容

- 中継システムで流量制御ができるようにした。
- 連携する MDM システムに Microsoft Intune を追加した。

(5) 13-00 の変更内容

(a) 資料番号（3021-3-L73）の変更内容

- Windows Server 2022 を次の製品の適用 OS に追加した。
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
  - JP1/IT Desktop Management 2 - Asset Console
  - JP1/IT Desktop Management 2 - Internet Gateway
- Windows 11 を次の製品の適用 OS に追加した。
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
- Windows Server 2012 を次の製品の適用 OS 外とした。
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Asset Console
  - JP1/IT Desktop Management 2 - Internet Gateway
- コンフィグレーションファイルで設定できるプロパティに次の項目を追加した。
  - ネットワークグループの自動作成を抑止する設定
  - 機器の登録時の同定を行わない設定
  - ネットワーク制御リストの自動更新を抑止する設定

- ネットワーク制御リストの警戒しきい値
- ネットワーク制御リストの登録数が警戒しきい値に達した場合と上限に達した場合のメッセージをホーム画面の通知事項に通知するかどうかの設定

(6) 12-60 の変更内容

(a) 資料番号（3021-3-E13-20）の変更内容

- 最大で 300,000 台の機器を管理できるようにした。
- 操作ログで取得される情報に、「操作日時（UTC）」を追加した。

(7) 12-50 の変更内容

(a) 資料番号（3021-3-E13-20）の変更内容

- API の使用を設定する手順を追加した。
- 操作画面を 10 人～20 人で同時に操作する場合の説明を変更した。

(8) 12-10 の変更内容

(a) 資料番号（3021-3-E13-10）の変更内容

- Windows Server 2019 を次の製品の適用 OS に追加した。
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
  - JP1/IT Desktop Management 2 - Asset Console
  - JP1/IT Desktop Management 2 - Internet Gateway
  - Remote Install Manager
- 外部システムから API を使用して機器を管理できるようにした。
- 共有型 VDI の仮想コンピュータを管理できるようにした。

(9) 12-00 の変更内容

(a) 資料番号（3021-3-E13）の変更内容

- Windows Server 2008 R2 を次の製品の適用 OS 外とした。
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Network Monitor

- JP1/IT Desktop Management 2 - Asset Console
- Remote Install Manager

- 上位システムの接続先を自動で切り替えてファイルを配布できるようにした。
- インターネットを介してコンピュータを管理できるようにした。

(10) 11-51 の変更内容

(a) 資料番号（3021-3-B53-40）の変更内容

- オフライン管理の機器にセキュリティポリシーを設定できるようにした。

(11) 11-50 の変更内容

(a) 資料番号（3021-3-B53-30）の変更内容

- Citrix XenApp、Microsoft RDS がインストールされているサーバにエージェントを導入して、JP1/IT Desktop Management 2 で管理できるようにした。
- Mac エージェントに対して、ソフトウェアおよびファイルの配布（リモートインストール）をできるようにした。 また、セキュリティポリシーによるセキュリティ状況の判定をできるようにした。

(12) 11-10 の変更内容

(a) 資料番号（3021-3-B53-20）の変更内容

- Windows Server 2016 を次の製品の適用 OS に追加した。
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
  - JP1/IT Desktop Management 2 - Asset Console
  - Remote Install Manager
- JP1/Base と連携して、JP1 認証で JP1/IT Desktop Management 2 にログインできるようにした。
- OS が Mac のコンピュータにエージェントを導入して管理できるようにした。
  提供する機能
  - システム情報およびソフトウェア情報の取得
  - RFB 接続によるリモートコントロール（エージェントレスでは提供済み）
  - ネットワーク制御（オンデマンドでの接続/遮断）

  提供しない機能（提供予定の機能を含む）
  - ソフトウェアやファイルの配布（リモートインストール）

- ファイル収集（リモートコレクト）
- エージェント設定やエージェントの配信
- セキュリティ管理（セキュリティ判定・自動対策）
- 操作ログ
- デバイス制御

- インスールセットの自動実行するファイルとして、秘文などの連携製品のインストーラーの ZIP ファイルを設定できるようにした。
- 最大で 50,000 台の機器を管理できるようにした。

(13) 11-01 の変更内容

(a) 資料番号（3021-3-B53-10）の変更内容

- 対象製品に JP1/IT Desktop Management 2 - Operations Director を追加した。
- Windows 10 を JP1/IT Desktop Management 2 - Network Monitor の適用 OS に追加した。
- 接続先設定ファイル（itdmhost.conf）でエージェントの接続先を設定できるようにした。
- Remote Install Manager だけをインストールする手順について、次の内容を修正した。
  - コンポーネントを選択するダイアログの説明
  - インストール後の起動に必要な情報の説明
- リモートインストールマネージャを使用した配布をするときに流量制御するかどうかを設定（パッケージ転送時の最大転送速度を指定）できるようにした。
- 機器のメンテナンス（重複機器や不稼働機器の判定条件を設定することで、対象と判定された機器を削除候補機器として検出し、自動または手動で削除）ができるようにした。
- エージェントのスタートメニューに表示するメニュー項目を選択できるようにした。
- 管理用サーバの上位接続先を変更した場合、下位の階層の管理用中継サーバから順に統括管理用サーバまで機器情報を手動で通知する必要があることを手順に追加した。
- 管理者のコンピュータ（リモートインストールマネージャ）および中継システムで使用するポート番号を追加した。

(14) 11-00 の変更内容

(a) 資料番号（3021-3-B53）の変更内容

- JP1/IT Desktop Management 2 を複数サーバ構成システムで運用することによって、拠点ごとの管理、および統括管理をできるようにした。
- JP1/IT Desktop Management 2 - Manager をインストールする手順を変更した。
- 管理用サーバをセットアップする手順を変更した。

- JP1/IT Desktop Management 2 - Manager を上書きインストールする手順を変更した。
- ネットワーク接続可否情報をインポートおよびエクスポートできるようにした。
- Windows 10 を次の製品の適用 OS に追加した。
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - RC Manager
  - Remote Install Manager
- Windows Server 2003 および Windows Server 2008（Windows Server 2008 R2 を除く）を次の製品の適用 OS 外とした。
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
  - JP1/IT Desktop Management 2 - RC Manager
- ウィルス対策製品情報をサポートサービスサイトから取得できるようにした。
- OS が UNIX のコンピュータにエージェントを導入して管理できるようにした。
- resetnid.vbs（ホスト識別子のリセット）コマンドの引数に「/s」を追加した。
- （資料番号（3021-3-369）からだけの変更内容）資産管理時に、一部のソフトウェアの購入形態、プロダクト ID、GUID、およびソフトウェア種別を管理できるようにした。

(15) 10-50 の変更内容

(a) 資料番号（3021-3-275、3021-3-369）の変更内容

- resetnid.vbs（ホスト識別子のリセット）コマンドでリターンコードを表示させる方法を追記し、使用例を修正した。
- サイトサーバ構成システムの機能を削除し、リモートインストールマネージャを使用した配布を利用する場合に必要なシステムとして、中継システムを追加した。
- リモートインストールマネージャを使用した配布機能によって、管理対象のコンピュータの条件や、コンピュータでの動作を詳細に指定して配布できるようにした。
- ネットワーク装置を含めたハードウェア情報、ソフトウェア情報、契約情報などをデータベースで一元管理できるようにした。
- 管理対象のコンピュータに格納されているファイルを一括で収集できるようにした。
- [機器の管理を始めましょう] ウィザードでは、エージェントをインストールする方法で機器を管理できるようにした。
- マルチサーバ構成システムの機能を削除し、1 台の管理用サーバで 30,000 台の機器を管理できるようにした。

- ユーザーアカウントをロックする連続入力失敗の回数、およびパスワードの有効期限を設定できるようにした。
- 製品構成の変更に伴い、インストール、セットアップ、およびエージェント設定の設定内容を変更した。
- Windows 8.1 および Windows Server 2012 R2 を次の製品の適用 OS に追加した。
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
- Windows 8、Windows 7 を次の製品の適用 OS 外とした。
  - JP1/IT Desktop Management 2 - Manager
- Windows 2000 を次の製品の適用 OS 外とした。
  - JP1/IT Desktop Management 2 - Agent
- サポートする Internet Explorer のバージョンを変更した。
- サポートするクラスタソフトウェアから、Microsoft Cluster Service を削除した。
- 一部のポート番号を変更した。
- 製品構成の変更に伴い、JP1/IT Desktop Management 2 - Manager の配下に作成されるフォルダ構成を変更した。

(16) 10-10 の変更内容

(a) 資料番号（3021-3-153-30）の変更内容

- インストール時、上書きインストール時、およびアンインストール時の注意事項を追記した。
- ネットワークに接続されている機器の探索で、期間を指定して集中的に探索する場合は、探索範囲に含まれる IP アドレスの数が 50,000 件以下になるように設定する必要があることを追記した。
- JP1/NETM/NM - Manager と連携することで、JP1/NETM/NM を導入したアプライアンス製品で監視しているネットワーク接続を JP1/IT Desktop Management から制御できるようにした。
- 管理用サーバにサーバ証明書をインポートしたあとに、MDM システムのサーバ証明書を変更する場合の説明を追加した。また、サーバ証明書の入手時の Internet Explorer のバージョンの記述を削除した。また、JP1 スマートデバイス管理サービスと連携する場合の設定について追記した。
- ネットワーク制御リストの自動更新について、すべての自動更新を有効にするか、自動更新のうち追加だけを有効にするかを設定できるようにした。
- 製品の上書きインストールおよびコンポーネントのアップデートの説明を訂正した。
- JP1/IT Desktop Management のシステム全体、および JP1/IT Desktop Management - Manager をバージョンアップする手順に説明を追加した。
- シングルサーバ構成システムの管理用サーバをリプレースする手順にサイトサーバの接続先を変更する手順を追加した。

- コマンドの実行権限に関する記載を「FUN_T_CMDEXECUTE コマンドを実行する手順」に集約した。また、getinv.vbs コマンド以外のコマンドを実行する場合で、OS のユーザーアカウント制御（UAC）が有効なときの説明を追記した。
- コマンド実行中の注意事項を記載した。
- resetnid.vbs コマンドに/i オプションを追加して、利用者のコンピュータに、コマンドを実行するかどうかを選択させるダイアログと、実行結果を示すダイアログが表示されるようにした。
- ポートの設定についての説明を修正した。また、JP1/IT Desktop Management - Remote Site Server とエージェントレスのコンピュータ間のネットワークの説明を追記した。

(b) 資料番号（3021-3-338-10）の変更内容

- 次のプログラムの適用 OS に、Windows 8 および Windows Server 2012 を追加した。
  - Job Management Partner 1/IT Desktop Management - Manager
  - Job Management Partner 1/IT Desktop Management - Remote Site Server
  - Job Management Partner 1/IT Desktop Management - Network Monitor
- インストール時、上書きインストール時、およびアンインストール時の注意事項を追記した。
- 機器情報の変更履歴を取得できるようにした。
- ネットワークに接続されている機器の探索で、期間を指定して集中的に探索する場合は、探索範囲に含まれる IP アドレスの数が 50,000 件以下になるように設定する必要があることを追記した。
- Job Management Partner 1/NETM/NM - Manager と連携することで、Job Management Partner 1/NETM/NM を導入したアプライアンス製品で監視しているネットワーク接続を Job Management Partner 1/IT Desktop Management から制御できるようにした。
- 管理用サーバにサーバ証明書をインポートしたあとに、MDM システムのサーバ証明書を変更する場合の説明を追加した。また、サーバ証明書の入手時の Internet Explorer のバージョンの記述を削除した。
- ネットワーク制御リストの自動更新について、すべての自動更新を有効にするか、自動更新のうち追加だけを有効にするかを設定できるようにした。
- 製品の上書きインストールおよびコンポーネントのアップデートの説明を訂正した。
- Job Management Partner 1/IT Desktop Management のシステム全体、および Job Management Partner 1/IT Desktop Management - Manager をバージョンアップする手順に説明を追加した。
- シングルサーバ構成システムの管理用サーバをリプレースする手順にサイトサーバの接続先を変更する手順を追加した。
- コマンドの実行権限に関する記載を「8.1 コマンドを実行する手順」に集約した。また、getinv.vbs コマンド以外のコマンドを実行する場合で、OS のユーザーアカウント制御（UAC）が有効なときの説明を追記した。
- エージェント導入済みのコンピュータでコマンドを実行する手順を追記した。また、コマンド実行中の注意事項を記載した。
- 共通管理項目と追加管理項目の定義を、CSV 形式でエクスポートおよびインポートできるようにした。

- 次のコマンドで利用するフォルダ名に指定できる文字についての説明を追記した。
  - exportdb コマンド
  - getlogs コマンド
  - getinstlogs コマンド
  - importdb コマンド
- resetnid.vbs コマンドに/i オプションを追加して、利用者のコンピュータに、コマンドを実行するかどうかを選択させるダイアログと、実行結果を示すダイアログが表示されるようにした。また、次の説明を追記した。
  - サイトサーバをインストールしたコンピュータでホスト識別子をリセットする場合の手順
  - ネットワークモニタを導入している機器で resetnid.vbs コマンドを実行した場合の注意事項
- ポートの設定についての説明を修正した。また、Job Management Partner 1/IT Desktop Management - Remote Site Server とエージェントレスのコンピュータ間のネットワークの説明を追記した。

(17) 10-02 の変更内容

(a) 資料番号（3021-3-153-20）の変更内容

- 次のプログラムの適用 OS に、Windows 8 および Windows Server 2012 を追加した。
  - JP1/IT Desktop Management - Manager
  - JP1/IT Desktop Management - Remote Site Server
  - JP1/IT Desktop Management - Network Monitor
- 機器情報の変更履歴を取得できるようにした。
- エージェント導入済みのコンピュータでコマンドを実行する手順を追記した。
- 共通管理項目と追加管理項目の定義を、CSV 形式でエクスポートおよびインポートできるようにした。
- 次のコマンドで利用するフォルダ名に指定できる文字についての説明を追記した。
  - exportdb コマンド
  - getlogs コマンド
  - getinstlogs コマンド
  - importdb コマンド
- サイトサーバをインストールしたコンピュータでホスト識別子をリセットする場合の手順を記載した。
- ネットワークモニタを導入している機器ではresetnid.vbs コマンドを実行しないよう、注意事項を記載した。

(18) 10-01 の変更内容

(a) 資料番号（3021-3-153-10）の変更内容

- インストールセットのデフォルトのファイル名が「ITDMAgt.exe」であることを記載した。
- CD-R をエージェントインストール用の媒体にする場合に、Autorun.inf を使用してエージェントのインストールを自動で開始できることを記載した。
- オフライン管理機能によって、管理用サーバにネットワーク接続していないコンピュータも管理できるようにした。
- ウィルス対策製品情報を含むサポートサービスの情報を取得して、JP1/IT Desktop Management の情報を更新できるようにした。
- JP1/IM 連携システムで、JP1/IM と JP1/Base が接続できていない場合の注意事項の説明を改善した。
- 機器をエージェントレスで管理している場合に、その機器に対する探索範囲、認証情報、またはその機器が登録されている Active Directory の設定を削除したときの注意事項を、マニュアル「JP1 Version 10 JP1/IT Desktop Management 導入・設計ガイド」に集約した。
- サポートサービスサイトからウィルス対策製品情報を取得して、JP1/IT Desktop Management の情報を更新できるようにした。
- MDM システムと連携するための情報を設定する手順を訂正した。
- JP1/IT Desktop Management のシステム全体をバージョンアップする流れを記載した。
- JP1/IT Desktop Management - Manager をバージョンアップする手順を訂正した。
- コンポーネントのアップデート方法の説明を訂正した。
- マルチサーバ構成システムで、JP1/IT Desktop Management - Manager を上書きインストールする流れを記載した。
- マルチサーバ構成システムで、JP1/IT Desktop Management - Manager をバージョンアップする流れを記載した。
- サイトサーバをリプレースする手順、およびサイトサーバをリプレースする場合の`recreatelogdb` コマンドについての注意事項を訂正した。
- ネットワークモニタを有効にしたコンピュータをリプレースする手順を記載した。
- サポートサービスサイトから SAMAC ソフトウェア辞書のオフライン更新用ファイルを取得して、JP1/IT Desktop Management の情報を更新できるようにした。
- 引数「-node」以外を指定して`recreatelogdb` コマンドを実行した場合の注意事項を訂正した。
- 構築関連で使用するコマンドとして、`stopservice`（サービス停止）コマンドの説明を記載した。
- `getlogs` コマンドでは、一時フォルダとしてユーザー環境変数 TEMP に設定したフォルダを使用することを記載した。
- `resetnid.vbs` コマンドを実行しないままディスクコピーしてエージェントを導入した場合の参考情報の説明を改善した。

- JP1/IT Desktop Management - Manager で使用するポート番号を、シングルサーバ構成の場合とマルチサーバ構成の場合に分けて記載した。

(b) 資料番号（3021-3-338）の変更内容

- 次の情報をマニュアル「Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 導入・設計ガイド」に集約した。
  - マイクロソフト製品の表記について
  - マニュアルで使用しているアイコンと書式について
  - オンラインヘルプについて
  - 関連マニュアル
  - 関連ドキュメント
  - このマニュアルでの表記
  - このマニュアルで使用する英略語
  - KB（キロバイト）などの単位表記について
  - 用語解説
- インストールセットのデフォルトのファイル名が「ITDMAgt.exe」であることを記載した。
- CD-R をエージェントインストール用の媒体にする場合に、Autorun.inf を使用してエージェントのインストールを自動で開始できることを記載した。
- オフライン管理機能によって、管理用サーバにネットワーク接続していないコンピュータも管理できるようにした。
- サポートサービスの情報を取得して、JP1/IT Desktop Management の情報を更新できるようにした。
- JP1/IM 連携システムで、JP1/IM と JP1/Base が接続できていない場合の注意事項の説明を改善した。
- MDM システムと連携するための情報を設定する手順を訂正した。
- JP1/IT Desktop Management のシステム全体をバージョンアップする流れを記載した。
- JP1/IT Desktop Management - Manager をバージョンアップする手順を訂正した。
- コンポーネントのアップデート方法の説明を訂正した。
- マルチサーバ構成システムで、JP1/IT Desktop Management - Manager を上書きインストールする流れを記載した。
- マルチサーバ構成システムで、JP1/IT Desktop Management - Manager をバージョンアップする流れを記載した。
- サイトサーバをリプレースする手順、およびサイトサーバをリプレースする場合の`recreatelogdb` コマンドについての注意事項を訂正した。
- ネットワークモニタを有効にしたコンピュータをリプレースする手順を記載した。
- 引数「-node」以外を指定して`recreatelogdb` コマンドを実行した場合の注意事項を訂正した。

- 構築関連で使用するコマンドとして、stopservice（サービス停止）コマンドの説明を記載した。
- getlogs コマンドでは、一時フォルダとしてユーザ環境変数 TEMP に設定したフォルダを使用することを記載した。
- resetnid.vbs コマンドを実行しないままディスクコピーしてエージェントを導入した場合の参考情報の説明を改善した。
- JP1/IT Desktop Management - Manager で使用するポート番号を、シングルサーバ構成の場合とマルチサーバ構成の場合に分けて記載した。
- マルチサーバ構成システムでの運用によって、最大で 50,000 台の機器を管理できるようにした。
- JP1/IM と連携して、JP1 イベントを通知できるようにした。
- JP1/IT Desktop Management のログイン画面の URL を記載した。
- ［インストールセットの作成］ダイアログの［エージェントをインストールする際の、管理者権限を持つアカウントを設定する］で設定する内容は、OS が Windows 2000、Windows XP、および Windows Server 2003 のコンピュータにエージェントをインストールする場合に限り有効であることを記載した。
- 設定画面の［他システムとの接続］－［サポートサービスの設定］にある［更新スケジュールの編集］で、サポートサービスサイトから最新の更新プログラム情報を取得するスケジュールを設定できることを記載した。
- ディスクコピーでエージェントを導入する際に、複数の機器が 1 つの機器として識別されてしまった場合の対処方法を記載した。
- resetnid.vbs コマンドを実行してから新規のホスト名が生成されるまでに掛かる時間を記載した。
- コントローラおよびリモコンエージェントのポート番号を修正した。
- ホスト識別子が再生成されるタイミングを記載した。
- ログイン時にパスワードの変更が要求されるタイミングを記載した。また、パスワードを設定してから 180 日が経過すると、ログイン時にパスワードの変更が必要になることを記載した。
- ユーザーアカウントのロックを解除する手順を記載した。
- MDM 製品と連携してスマートデバイスを管理できるようにした。
- Windows の管理共有の認証で使用するユーザー ID は、ドメインユーザーで認証する場合は、「ユーザー ID@FQDN（完全修飾ドメイン名）」または「ドメイン名¥ユーザー ID」の形式で指定することを記載した。
- 管理用サーバをリプレースする手順を詳細に記載した。
- サイトサーバの操作ログを削除するコマンド（deletelog コマンド）を実行した場合の作業用フォルダに、実行状況の記録ファイル（deletelog_lasttime.txt）が存在しているときの対処方法について記載した。
- サイトサーバのポート番号一覧に、ポート番号 31000 を追加した。

(19) 10-00 の変更内容

(a) 資料番号（3021-3-153）の変更内容

- マルチサーバ構成システムでの運用によって、最大で 50,000 台の機器を管理できるようにした。
- JP1/IM と連携して、JP1 イベントを通知できるようにした。
- JP1/IT Desktop Management のログイン画面の URL を記載した。
- ［インストールセットの作成］ダイアログの［エージェントをインストールする際の、管理者権限を持つアカウントを設定する］で設定する内容は、OS が Windows 2000、Windows XP、および Windows Server 2003 のコンピュータにエージェントをインストールする場合に限り有効であることを記載した。
- 設定画面の［他システムとの接続］－［サポートサービスの設定］にある［更新スケジュールの編集］で、サポートサービスサイトから最新の更新プログラム情報を取得するスケジュールを設定できることを記載した。
- ディスクコピーでエージェントを導入する際に、複数の機器が 1 つの機器として識別されてしまった場合の対処方法を記載した。
- resetnid.vbs コマンドを実行してから新規のホスト名が生成されるまでに掛かる時間を記載した。
- コントローラおよびリモコンエージェントのポート番号を修正した。
- ホスト識別子が再生成されるタイミングを記載した。
- 次の情報をマニュアル「JP1 Version 10 JP1/IT Desktop Management 導入・設計ガイド」に集約した。
  - マイクロソフト製品の表記について
  - マニュアルで使用しているアイコンと書式について
  - オンラインヘルプについて
  - 関連マニュアル
  - 関連ドキュメント
  - このマニュアルでの表記
  - このマニュアルで使用する英略語
  - KB（キロバイト）などの単位表記について
  - 用語解説

(20) 09-51 の変更内容

(a) 資料番号（3020-3-S94-10）の変更内容

- ログイン時にパスワードの変更が要求されるタイミングを記載した。また、パスワードを設定してから 180 日が経過すると、ログイン時にパスワードの変更が必要になることを記載した。

- ユーザーアカウントのロックを解除する手順を記載した。
- MDM 製品と連携してスマートデバイスを管理できるようにした。
- Windows の管理共有の認証で使用するユーザー ID は、ドメインユーザーで認証する場合は、「ユーザー ID@FQDN（完全修飾ドメイン名）」または「ドメイン名¥ユーザー ID」の形式で指定することを記載した。
- 管理用サーバをリプレースする手順を詳細に記載した。
- サイトサーバの操作ログを削除するコマンド（deletelog コマンド）を実行した場合の作業用フォルダに、実行状況の記録ファイル（deletelog_lasttime.txt）が存在しているときの対処方法について記載した。
- サイトサーバのポート番号一覧に、ポート番号 31000 を追加した。

索引

え

お

か

き

く

こ

さ

し

せ

そ

た

ち

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