HITACHI
Inspire the Next

JP1 Version 12

JP1/IT Desktop Management 2 導入・設計ガイド

3021-3-E12-20

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-2A42-78CL　JP1/IT Desktop Management 2 - Manager　12-50

製品構成一覧および内訳形名

・P-CC2A42-7ACL　JP1/IT Desktop Management 2 - Manager（適用 OS：Windows Server 2019、Windows Server 2016、Windows Server 2012）

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

・P-CC2A42-7CCL　JP1/IT Desktop Management 2 - Network Monitor（適用 OS：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-CC2A42-7DCL　JP1/IT Desktop Management 2 - Asset Console（適用 OS：Windows Server 2019、Windows Server 2016、Windows Server 2012）

・P-CC2A42-7PCL　JP1/IT Desktop Management 2 - Internet Gateway（適用 OS：Windows Server 2019、Windows Server 2016、Windows Server 2012）

●P-2A42-7KCL　JP1/IT Desktop Management 2 - Operations Director　12-50

製品構成一覧および内訳形名

・P-CC2A42-7ACL　JP1/IT Desktop Management 2 - Manager（適用 OS：Windows Server 2019、Windows Server 2016、Windows Server 2012）

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

・P-CC2A42-7CCL　JP1/IT Desktop Management 2 - Network Monitor（適用 OS：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-CC2A42-7PCL　JP1/IT Desktop Management 2 - Internet Gateway（適用 OS：Windows Server 2019、Windows Server 2016、Windows Server 2012）

■ 輸出時の注意

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

なお、不明な場合は、弊社担当営業にお問い合わせください。

■ 商標類

Microsoft Office および Excel は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Microsoft Office および Groove は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Microsoft Office および OneNote は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Microsoft Office および Outlook は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Microsoft Office および PowerPoint は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Microsoft Office および Visio は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。

Microsoft Office Word は、米国 Microsoft Corporation の商品名称です。

MS-DOS は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Norton AntiVirus は、Symantec Corporation 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。

ODBC は、米国 Microsoft Corporation が提唱するデータベースアクセス機構です。

OfficeScan and PC-Cillin are trademark of Trend Micro Incorporated.

OneDrive は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

OpenGL は、Silicon Graphics, Inc.の登録商標です。

Oracle と Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。

Pentium は、アメリカ合衆国および / またはその他の国における Intel Corporation の商標です。

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

RSA および BSAFE は、米国 EMC コーポレーション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。

すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同社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。SPARC 商標がついた製品は、米国 Sun Microsystems, Inc. が開発したアーキテクチャに基づくものです。

Symantec、Symantec AntiVirus は、Symantec Corporation 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。

UNIX は、The Open Group の米国ならびに他の国における登録商標です。

Visual C++は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows Live は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

本製品は、米国 EMC コーポレーションの RSA BSAFE(R)ソフトウェアを搭載しています。

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

2021 年 1 月　3021-3-E12-20

変更内容

変更内容（3021-3-E12-20） JP1/IT Desktop Management 2 12-50

追加・変更内容	変更個所
ネットワークモニタを有効にした機器を強制的に削除できるようにした。	2.8.3
ネットワークモニタ設定で、許可されていない機器がネットワークに接続された時にイベントを発行できるようにした。	2.8.7
資産の関連づけ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。	2.11.9、2.11.10、2.18.12
CentOS 8.1、Red Hat Enterprise Linux(R) Server 8、および Oracle Linux 8 を、エージェントを導入するコンピュータの前提となる OS に追加した。	4.2.3

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 の製品概要、機能、システムの設計方法など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、「付録 A.13　JP1/IT Desktop Management 2 - Operations Director での機能制限」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 の導入検討またはシステムの設計をしている方
- JP1/IT Desktop Management 2 の製品概要や機能詳細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　製品の概要

JP1/IT Desktop Management 2 の概要とシステムを構成する要素について説明しています。

第 2 章　機能の紹介

JP1/IT Desktop Management 2 の機能の詳細について説明しています。

第 3 章　製品ライセンスについて

JP1/IT Desktop Management 2 の製品ライセンスについて説明しています。

第 4 章　システム設計

システムの設計から運用を開始するまでの概要について説明しています。また、システム設計時に必要な検討事項についても説明しています。

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。

付録 B　用語解説

JP1/IT Desktop Management 2 で使用する用語について説明しています。

目次

1 製品の概要

JP1/IT Desktop Management 2 は、組織内のセキュリティ対策や IT 資産管理を実現する製品です。ここでは、JP1/IT Desktop Management 2 の概要とシステムを構成する要素について説明します。

1.1 製品概要

社会の情報化が進む昨今では、組織を効率良く運営したり、運営コストを削減したりするために、IT 機器の必要性が高まっています。しかし、社会の情報化が高度になるにつれて、多大な導入機器の状態把握や詳細なセキュリティ設定・対策方法の理解が必要になるなど、IT 機器の管理の難易度も高くなってきています。このような状況で、どのようにして IT 機器を効率良く、正確に管理するかが重要な課題となっています。

JP1/IT Desktop Management 2 は、業務に沿ったわかりやすい操作性、シンプルな設定項目やスケジューリングによる自動化機能を備え、セキュリティ管理や資産管理の観点から IT 機器の管理を支援します。JP1/IT Desktop Management 2 を導入することで、難易度の高い IT 機器の管理業務に対する管理者の負荷を軽減し、組織のスムーズな運用を実現できます。

1.1.1 この製品でできること

JP1/IT Desktop Management 2 を導入することで、組織のセキュリティ管理および資産管理ができます。

組織内の機器のセキュリティ状況を管理するためには、セキュリティに関するルールを決め、それを各 IT 機器の利用者に遵守させる必要があります。また、セキュリティの現状を把握して、問題点を適宜対策していくことも必要です。

JP1/IT Desktop Management 2 では、セキュリティ管理および資産管理を次の点から支援します。

- IT 機器の現状の把握
- IT 機器に対するセキュリティのルールの徹底
- セキュリティに問題のあるコンピュータの把握と対策
- IT 機器のネットワーク接続の監視
- ソフトウェアの導入と保守
- 遠隔地のコンピュータのリモート操作

IT 機器の現状を把握できます

IT 機器のセキュリティ管理を徹底するためには、ルールを適用する機器をすべて把握しておく必要があります。また、IT 機器を組織内の資産として管理するためには、使用しているハードウェア、ソフトウェアは何かといった情報とそれらが今どのような状態になっているかを把握しておく必要があります。JP1/IT Desktop Management 2 は、定期的にネットワーク内の機器を探索し、機器を発見する機能と発見した機器の情報を自動的に収集する機能を提供しています。探索時に新しい機器を発見すると自動的に情報が収集されるので、最新の正確な情報で IT 機器を管理できます。これによって、管理者が情報収集する負担を軽減できます。

IT 機器に対するセキュリティのルールを徹底できます

組織のセキュリティのルールを決めるための要素の一つに、ISMS があります。ISMS に基づいて組織のセキュリティを管理する場合に、IT 機器に対しては、設定や操作に関するルールを利用者に遵守させる必要があります。JP1/IT Desktop Management 2 では、組織で定めたルールをセキュリティポリシーとして各 IT 機器に設定し、その遵守状況を把握できます。これによって、組織内の IT 機器に対してセキュリティのルールを徹底できます。 また、セキュリティポリシーに違反しているコンピュータに対しては、自動で対策したり、警告メッセージを通知したりできるので、管理者や上長から利用者に対して対策を直接指示する手間を省略できます。

セキュリティに問題のある機器を把握・対策できます

組織内のコンピュータを安全に運用するためには、ウィルス感染や情報漏えいが発生する前にセキュリティに問題のあるコンピュータを特定し、早急に対策する必要があります。しかし、コンピュータのセキュリティ設定、ウィルス対策製品や更新プログラムの適用、情報漏えい対策など多岐に渡る対策状況を手動でチェックして問題点を抽出するには、多大な時間とコストが掛かります。 JP1/IT Desktop Management 2 では、各コンピュータのセキュリティ状況を一覧で確認できるため、セキュリティの問題点を一目で把握できます。また、セキュリティに問題があった場合は、ウィルス対策製品や更新プログラムを自動で適用したり、該当する機器をネットワークから自動で切り離したりして対策できるため、システム全体のセキュリティを効率良く管理できます。

機器のネットワーク接続を監視できます

モバイルコンピュータの普及によって、組織内に個人のコンピュータが持ち込まれるおそれがあります。未確認の機器がネットワークに接続されてしまうと、情報漏えいやウィルス感染などの被害の原因となります。JP1/IT Desktop Management 2 では、このような状況を防ぐために、組織内のネットワークを監視して新たに接続された機器を即座に発見して不正にネットワーク接続されていないかを確認したり、セキュリティ対策がされていない機器をネットワークから自動的に遮断したりできます。ネットワーク接続の監視機能を利用することで、組織内のネットワーク接続状況を把握でき、機器のセキュリティ状態を安全に保てます。

ソフトウェアを導入・保守できます

業務でソフトウェアを使用する場合、各コンピュータにソフトウェアをインストールする必要があります。しかし、コンピュータごとに利用者がインストール作業をするのは手間が掛かります。JP1/IT Desktop Management 2 では、必要なコンピュータにソフトウェアを一括してインストールできます。そのため、頻繁にバージョンアップがあっても迅速に対応できます。また、不具合を修正したりセキュリティ上の問題を修正したりするための更新プログラムを、自動的にコンピュータに配布、適用できます。

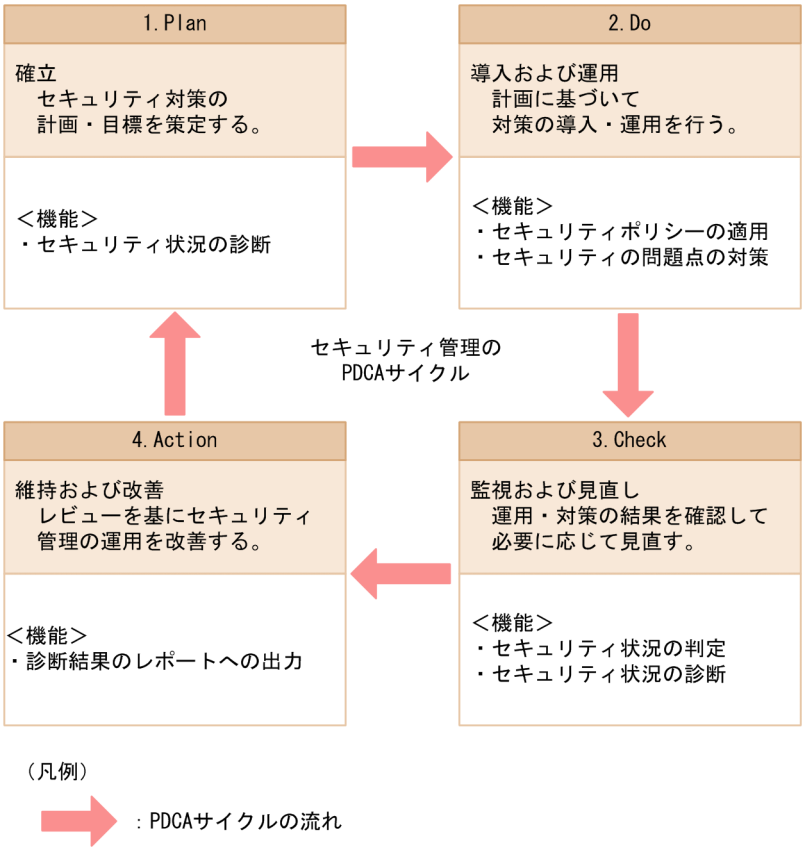
遠隔地の機器をリモートで操作できます

近年の急速な IT の高度化に伴い、アプリケーションのセットアップやトラブル発生時の対処などに不慣れなユーザーが増えてきています。組織内で発生するコンピュータの問題に対しては、専門知識を持つシステム管理者などが対応する場合がほとんどです。しかし、職場が分散していると速やかな対応は難しくなります。 JP1/IT Desktop Management 2 では、システム管理者の手もとのコンピュータから問題の発生したコンピュータを遠隔操作でき、問題に速やかに対応できます。

1.1.2　機能とセキュリティ管理の PDCA サイクルの対応

ISMS では、セキュリティ管理の運用および改善をするアプローチとして、PDCA サイクルの考え方を推奨しています。JP1/IT Desktop Management 2 が提供する機能は、セキュリティ管理の PDCA サイクルの各プロセスで、組織で定めた運用を支援します。

JP1/IT Desktop Management 2 が提供する機能と、セキュリティ管理の PDCA サイクルとの対応を次の図に示します。



PDCA サイクルに沿った、JP1/IT Desktop Management 2 の運用方法（管理者が実施すること）を次に示します。

1.Plan：確立

JP1/IT Desktop Management 2 を使って組織内のコンピュータのセキュリティ状況を診断します。

診断結果を基にシステムのセキュリティ状況を評価し、問題点を抽出します。これを基に、組織のセキュリティルールを策定し、運用方法を検討します。

2.Do：導入および運用

セキュリティポリシーを設定し、JP1/IT Desktop Management 2 を使ってコンピュータにセキュリティポリシーを適用します。

セキュリティに問題があるコンピュータを発見した場合は、JP1/IT Desktop Management 2 を使って問題点を対策します。

3.Check：監視および見直し

JP1/IT Desktop Management 2 を使って、機器のセキュリティ状況に問題がないかを判定します。

判定したセキュリティ状況の結果を基に、JP1/IT Desktop Management 2 を使ってセキュリティ状況を診断します。

診断結果からセキュリティ状況の傾向を確認し、解決していない問題点を把握します。

4.Action：維持および改善

把握した問題点の対策を実施します。

JP1/IT Desktop Management 2 を使ってセキュリティ状況の診断結果をレポートとして出力し、レビューします。

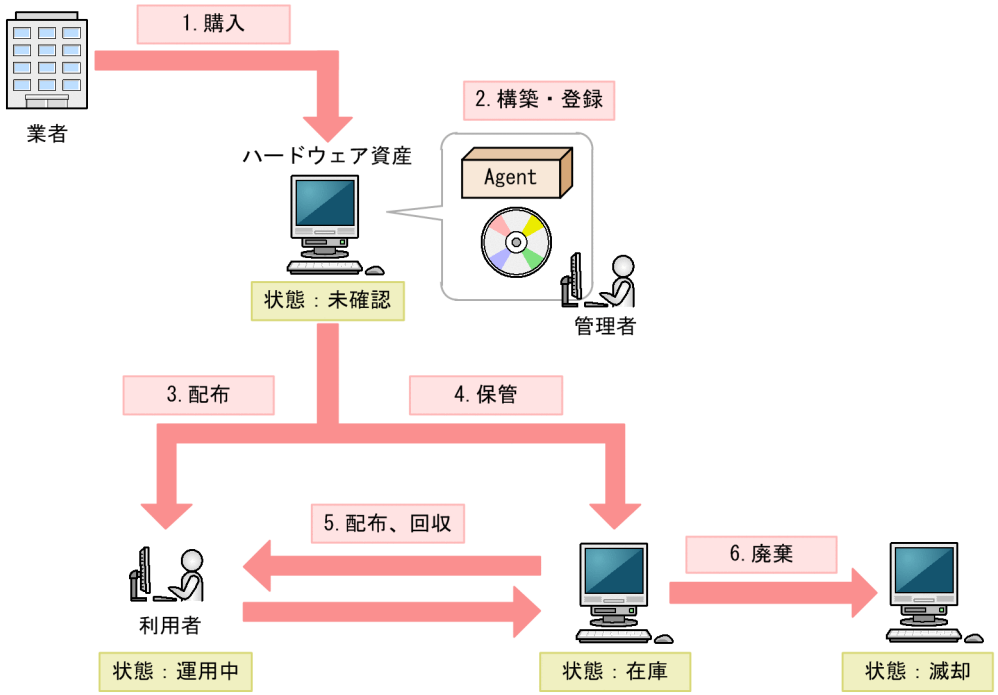
レビュー結果を基に、次回のサイクルでセキュリティルールの改善を計画します。

1.1.3　資産管理の流れ

JP1/IT Desktop Management 2 では、組織内の IT 資産（ハードウェア資産およびソフトウェアライセンス）をまとめて管理できます。また、資産に関する契約もあわせて管理できます。

ハードウェア資産の購入から廃棄まで

ハードウェア資産の購入から廃棄までの流れを次の図に示します。



（凡例）

Agent：JP1/IT Desktop Management 2 - Agent

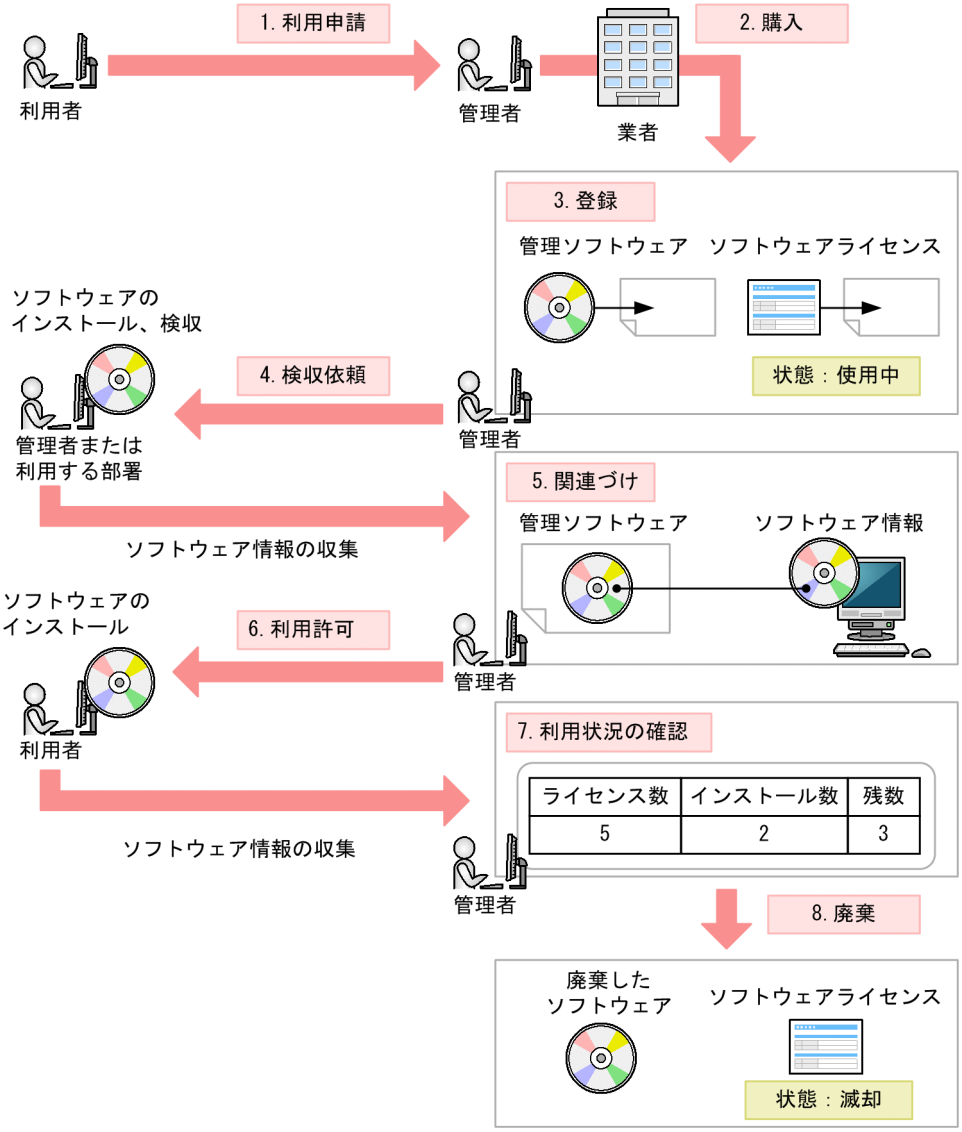
ハードウェア資産を購入したら、ハードウェア資産の環境を構築し、ハードウェア資産情報を JP1/IT Desktop Management 2 に登録します。（図中：1～2）

そのあと、ハードウェア資産を利用者に配布します。ハードウェア資産を利用しない場合は在庫として保管しておきます。リプレースや代替機貸し出しなどの運用に応じて、在庫のハードウェア資産を配布したり、使用中のハードウェア資産を回収したりします。資産の状態に応じて、JP1/IT Desktop Management 2 のハードウェア資産情報をメンテナンスします。(図中：3～5)

ハードウェア資産が不要になった場合は、滅却処理をして廃棄します。資産の状態に応じて、JP1/IT Desktop Management 2 のハードウェア資産情報をメンテナンスします。(図中：6)

ソフトウェアの購入から廃棄まで

ソフトウェアの購入から廃棄までの流れを次の図に示します。



利用者からソフトウェアの利用申請があったら、申請を確認してソフトウェアを購入します。購入後、管理者が利用状況を管理するソフトウェア名（管理ソフトウェア）を決めて、管理ソフトウェア情報とソフトウェアライセンス情報を JP1/IT Desktop Management 2 に登録します。(図中：1～3)

ソフトウェアは、利用者に提供する前に管理者や利用する部署が検収します。検収時にソフトウェアを管理対象のコンピュータにインストールすると、管理用サーバにソフトウェア情報が収集されます。管理者

は、JP1/IT Desktop Management 2 で、収集されたソフトウェア情報と管理ソフトウェア情報を対応づけます。これによって、操作画面から管理ソフトウェアのインストール状況が把握できるようになります。そのあと、利用者からの申請を確認し、ソフトウェアの利用を許可します。利用者のコンピュータにソフトウェアがインストールされると、管理用サーバにソフトウェア情報が収集されて、操作画面からソフトウェアライセンスの利用状況を把握できるようになります。(図中：4～6)

ソフトウェアが不要になった場合は、滅却処理をして廃棄します。このとき、JP1/IT Desktop Management 2 のソフトウェアライセンス情報の状態もメンテナンスします。(図中：7～8)

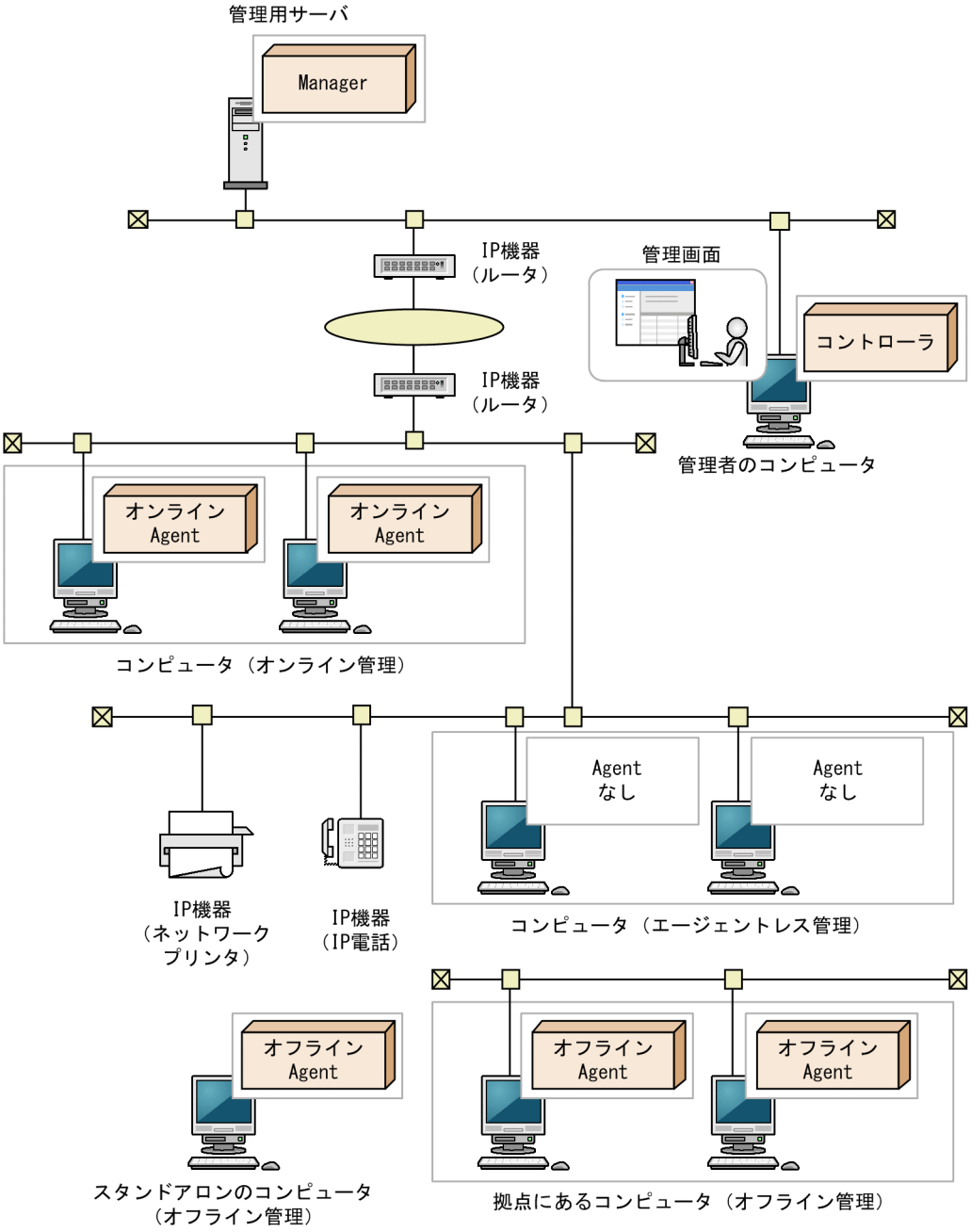
1.2 システム構成要素の紹介

このマニュアルでは、JP1/IT Desktop Management 2 で管理するシステムを説明するに当たり、JP1/IT Desktop Management 2 がインストールされたサーバやコンピュータ、ネットワーク機器などの、システムを構成する各要素の呼び方を定義しています。

JP1/IT Desktop Management 2 の基本的なシステム構成要素の定義を次の表に示します。

構成要素名		定義
管理用サーバ		JP1/IT Desktop Management 2 がインストールされたサーバです。 管理用サーバにはデータベースが生成され、JP1/IT Desktop Management 2 が管理するさまざまな情報が格納されます。 リモートインストールマネージャを使用した配布について説明する場合は、「配布管理システム」または「マネージャ」と呼ぶことがあります。
管理者のコンピュータ		管理者が JP1/IT Desktop Management 2 の操作画面を操作して、各種管理業務をするためのコンピュータです。JP1/IT Desktop Management 2 は Web ブラウザから操作画面を表示して操作します。そのため、管理用サーバにアクセスできるコンピュータであれば、どこからでも操作できます。管理用サーバ自身も、管理者のコンピュータとして使用できます。 また、操作画面からコンピュータをリモートコントロールするためのプログラム（コントローラ）をダウンロードして、利用者のコンピュータをリモートコントロールすることもできます。 リモートインストールマネージャを使用した配布を利用する場合は、Remote Install Manager がインストールされている必要があります。
機器	コンピュータ	OS がインストールされているコンピュータのことです。コンピュータには、次の種類があります。 • エージェントがインストールされているコンピュータ 　• オンライン管理用のエージェントがインストールされているコンピュータ（オンライン管理のコンピュータ） 　• オフライン管理用のエージェントがインストールされているコンピュータ（オフライン管理のコンピュータ） • 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（エージェントレス管理のコンピュータ）
	IP 機器	ルータ、ネットワークプリンタ、IP 電話など、IP アドレスを持つコンピュータ以外の機器です。
	周辺機器	マウス、キーボード、USB デバイスなど、IP アドレスを持たない機器です。

各システム構成要素を配置した、JP1/IT Desktop Management 2 で管理する基本的なシステムの構成例を次の図に示します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager
オンラインAgent：オンライン管理用のJP1/IT Desktop Management 2 - Agent
オフラインAgent：オフライン管理用のJP1/IT Desktop Management 2 - Agent
Agentなし：JP1/IT Desktop Management 2 - Agentなし

また、JP1/IT Desktop Management 2 のコンポーネントを追加したり JP1/IT Desktop Management 2 以外のシステムと連携したりすることで、負荷分散、セキュリティ管理の強化、付加情報の管理など、目的に応じてシステムを管理できます。

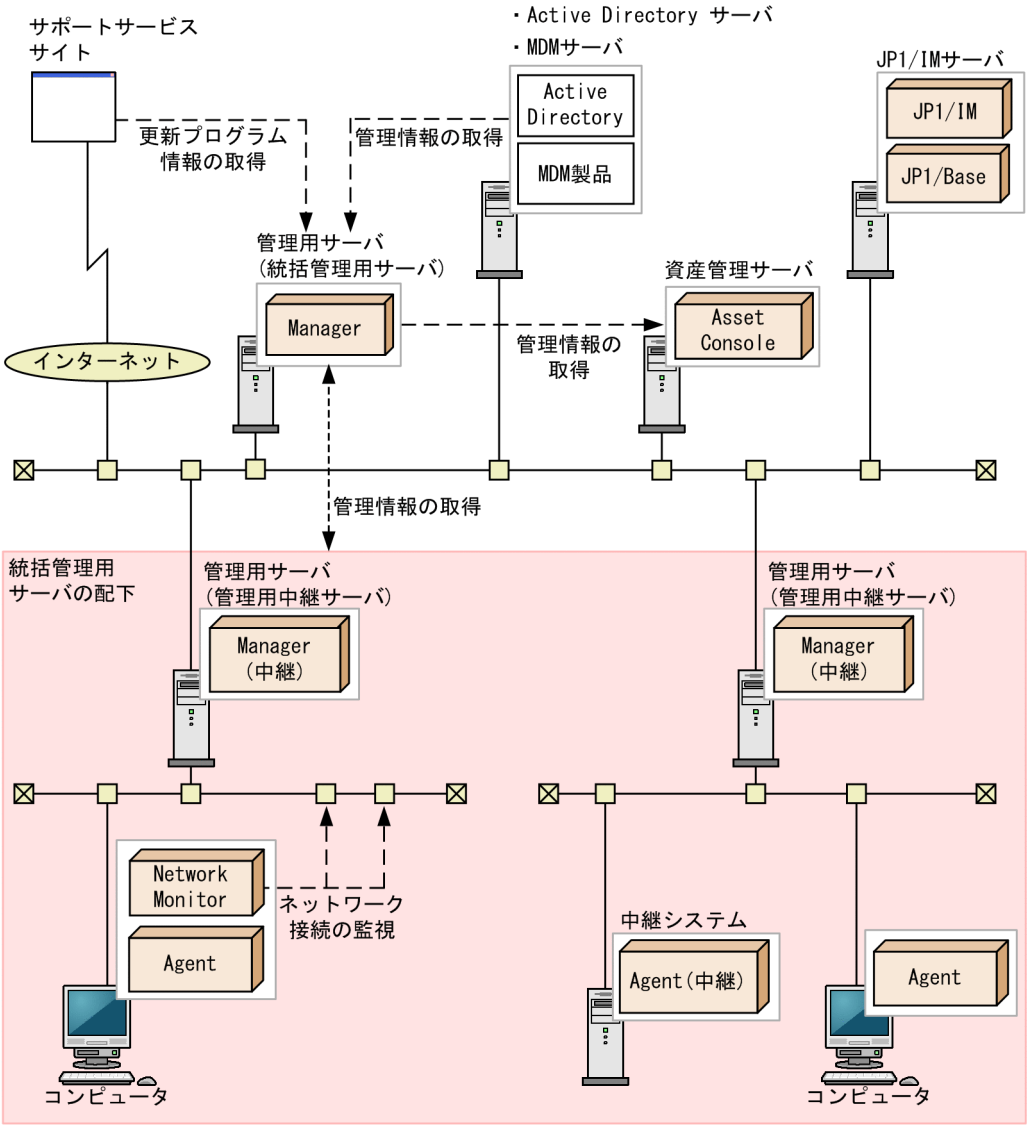
目的に応じて追加するシステム構成要素の定義を次の表に示します。

構成要素名	定義
中継システム※	JP1/IT Desktop Management 2 - Agent を中継システムとしてインストールしたサーバです。 中継システムは、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設置します。中継システムを設置すると、管理用サーバやネットワークに掛かる負荷を軽減できます。 中継システムを設置したシステムを、JP1/IT Desktop Management 2 の「基本構成システム」と呼びます。
管理用中継サーバ※	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サーバです。JP1/IT Desktop Management 2 - Manager のインストール時に、エージェントも自動でインストールされます。このエージェントを「管理用中継サーバ用のエージェント」と呼びます。 管理用中継サーバを設置すると、管理者や管理用サーバの負荷を分散したり、NAT 環境での運用に対応したりできます。部門やネットワーク構成ごとに JP1/IT Desktop Management 2 を運用したい場合は、管理用中継サーバを設置してください。 管理用中継サーバを設置する場合は、統括管理用サーバおよび複数の管理用中継サーバによって、システムを階層化する必要があります。階層化されたシステムを、JP1/IT Desktop Management 2 の「複数サーバ構成システム」と呼びます。複数サーバ構成システムでは、統括管理用サーバと管理用中継サーバを合わせて「管理用サーバ」と呼ぶことがあります。 なお、複数サーバ構成システムに対して、1 台の管理用サーバで JP1/IT Desktop Management 2 を運用するシステムを「単数サーバ構成」と呼びます。
統括管理用サーバ※	JP1/IT Desktop Management 2 - Manager をインストールしたサーバのうち、管理用中継サーバによって階層化されたシステム（複数サーバ構成システム）の最上位に設置するサーバです。複数サーバ構成システムでは、統括管理用サーバと管理用中継サーバを合わせて「管理用サーバ」と呼ぶことがあります。
サポートサービスサイト	日立のサポートサービスを提供する Web サイトです。 JP1/IT Desktop Management 2 からインターネットを介して接続し、最新の更新プログラムおよびウィルス対策製品の情報を取得できます。ここで取得した情報を基に、各コンピュータの更新プログラムおよびウィルス対策製品が最新かどうかが判定されます。 サポートサービスサイトと連携したシステムを、「サポートサービス連携構成システム」と呼びます。
資産管理サーバ※	JP1/IT Desktop Management 2 - Asset Console（Asset Console）がインストールされたサーバです。資産情報を検索する画面のカスタマイズや案件を使用した資産管理業務の実行など、細やかな資産管理をする場合に設置します。
Active Directory サーバ	Active Directory を導入しているサーバです。JP1/IT Desktop Management 2 とは別に、Active Directory のプログラムが必要です。 JP1/IT Desktop Management 2 から、Active Directory で管理している情報を取得できます。 Active Directory と連携したシステムを、「Active Directory 連携構成システム」と呼びます。
MDM サーバ	MDM 製品を導入して、スマートデバイスを管理しているサーバです。JP1/IT Desktop Management 2 とは別に MDM 製品が必要です。JP1/IT Desktop Management 2 から、MDM 製品で管理されているスマートデバイスの情報を取得できます。 MDM 製品と連携したシステムを、「MDM 連携構成システム」と呼びます。

構成要素名	定義
ネットワークモニタエージェント	機器のネットワーク接続を監視および制御するための、JP1/IT Desktop Management 2 のコンポーネントです。 ネットワークモニタエージェントは、オンライン管理のコンピュータに対して、ネットワークモニタを有効にするとインストールされます。 ネットワークモニタエージェントがインストールされると、そのコンピュータが接続しているネットワークセグメントに対して、新規機器のネットワーク接続を検知したり、機器のネットワーク接続を拒否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したシステムを、「ネットワーク監視構成システム」と呼びます。
ネットワーク制御用アプライアンス※	JP1/NETM/NM を導入したアプライアンス製品です。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 2 から制御できます。JP1/NETM/NM - Manager と連携したシステムを「JP1/NETM/NM - Manager 連携構成システム」と呼びます。
JP1/IM サーバ※	JP1 製品などのプログラムを統合的に監視するための JP1/IM を導入したサーバです。JP1/IT Desktop Management 2 とは別に、JP1/IM および JP1/Base が必要です。管理対象のコンピュータで発生した障害を、JP1/IM で JP1 イベントとして一元管理できます。 JP1/IM と連携したシステムを、「JP1/IM 連携構成システム」と呼びます。

注※　JP1/IT Desktop Management 2 - Operations Director ではサポートしていません。

運用に応じてシステム構成要素を配置した、JP1/IT Desktop Management 2 で管理するシステムの構成例を次の図に示します。



(凡例)
Manager : JP1/IT Desktop Management 2 - Manager
Manager (中継) : 管理用中継サーバとしてインストールしたJP1/IT Desktop Management 2 - Manager
Agent : エージェントとしてインストールしたJP1/IT Desktop Management 2 - Agent
Agent (中継) : 中継システムとしてインストールしたJP1/IT Desktop Management 2 - Agent
Network Monitor : ネットワークモニタエージェント

各システム構成の詳細については、「4.4　システム構成の検討」を参照してください。

1.3　操作画面の紹介

JP1/IT Desktop Management 2 では、上部のボタンで画面を切り替えて各機能を使用します。目的に応じて操作画面を選択してください。

操作画面には、複数のコンピュータから同時にログインできます。複数のコンピュータで操作画面を同時に操作しても、それぞれの操作内容がリアルタイムに操作画面に反映されることはありません。

各画面でできることを次に示します。

ホーム画面

ホーム画面では、JP1/IT Desktop Management 2 で管理している情報の概況を各パネルで確認できます。また、各パネルからほかの画面に移動して、管理作業を始められます。

セキュリティ画面

セキュリティ画面では、セキュリティポリシーをコンピュータに割り当ててセキュリティ状況を管理したり、セキュリティ状況に問題があるコンピュータに対策を実行したりできます。また、操作ログを管理して不審な操作について調査することもできます。

資産画面

資産画面では、ハードウェア資産、ソフトウェアライセンスの状態や棚卸日を管理したり、契約情報と関連づけてコストを管理したりできます。組織内の資産を一覧で把握して、効率的な資産運用を実現できます。

機器画面

機器画面では、管理対象の機器の機器情報やソフトウェア情報を確認したり、機器に対する操作を実行したりできます。

配布（ITDM 互換）画面

配布（ITDM 互換）画面では、コンピュータに必要なソフトウェアを配布してインストールしたり、不要なソフトウェアをアンインストールしたりできます。また、ソフトウェアだけではなく必要なファイルを配布することもできます。

なお、UNIX エージェントおよび Mac エージェントへの配布には使えません。UNIX エージェントおよび Mac エージェントへの配布は、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必要があります。

イベント画面

イベント画面では、JP1/IT Desktop Management 2 の運用中に発生したイベントを確認できます。

レポート画面

レポート画面では、ダイジェストレポート、セキュリティ診断レポート、セキュリティ詳細レポート、機器詳細レポート、および資産詳細レポートを確認できます。

設定画面

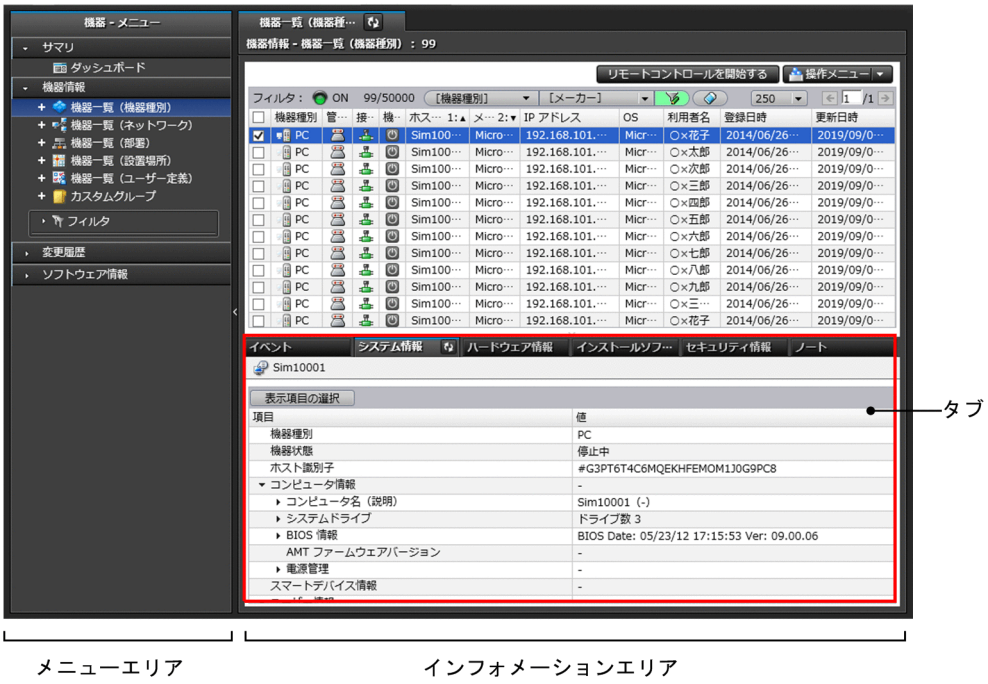
設定画面では、ユーザーアカウントやエージェント設定など JP1/IT Desktop Management 2 の各種設定をカスタマイズできます。また、機器の探索やエージェントの配信なども、この画面から実行できます。

関連リンク

- 1.3.2　ホーム画面でできること
- 1.3.3　セキュリティ画面でできること
- 1.3.4　資産画面でできること
- 1.3.5　機器画面でできること
- 1.3.6　配布（ITDM 互換）画面でできること
- 1.3.7　イベント画面でできること
- 1.3.8　レポート画面でできること
- 1.3.9　設定画面でできること

1.3.1　基本的な画面構成

JP1/IT Desktop Management 2 の基本的な画面構成と、画面内の呼び方について説明します。



メニューエリア

選択した画面に応じてメニューが表示されます。各メニューの項目を選択すると、インフォメーションエリアに対応する情報が表示されます。

インフォメーションエリア

メニューエリアで選択した項目に応じて、情報が表示されます。

タブ

セキュリティ画面、資産画面、機器画面、および配布（ITDM 互換）画面では、インフォメーションエリアの下部にタブが表示されます。タブには、上部で選択した情報の詳細情報が表示されます。

画面上部のメニュー

画面上部のメニューには、各画面で共通の項目が表示されます。

システム

JP1/IT Desktop Management 2 からログアウトできます。

表示

パネルのレイアウト変更、履歴ボタンおよびチェックボックスの表示設定、表示設定の初期化ができます。

実行

［機器の管理を始めましょう］ウィザードの起動、現在ログインしているユーザーアカウントの編集ができます。

ヘルプ

操作画面のサイトマップ、製品ライセンスの情報、および製品のバージョン情報を表示できます。

［ログアウト］ボタン

JP1/IT Desktop Management 2 からログアウトできます。［ログアウト］ボタンの左には、現在ログインしているユーザーアカウントのユーザー ID が表示されます。ユーザー ID をクリックすると、ユーザーアカウントの情報を編集したり、パスワードを変更したりできます。

［ヘルプ］ボタン

現在表示されている画面の内容や、その画面からできることなどについて説明するヘルプを表示できます。ボタンの左側には現在表示されている画面名が表示されます。

画面上部のボタン

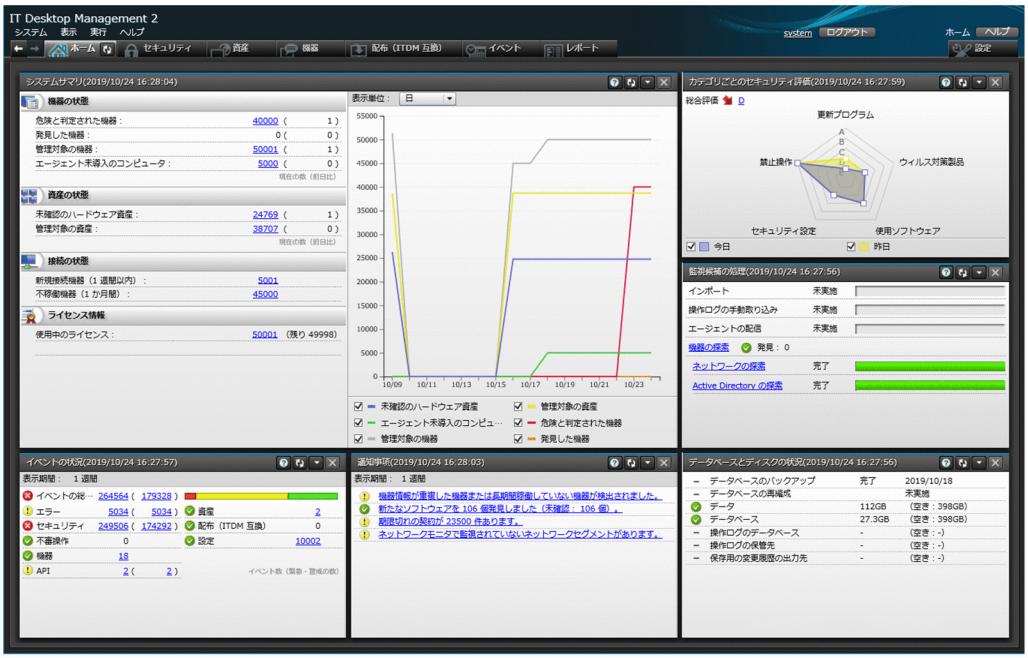
画面上部のボタンで、画面を切り替えて各機能を使用できます。

関連リンク

- 1.3　操作画面の紹介
- 2.18.1　複数サーバ構成の場合の操作画面に表示される情報

1.3.2　ホーム画面でできること

ホーム画面では、JP1/IT Desktop Management 2 で管理している情報の概況を各パネルで確認できます。機器や資産、製品ライセンスの概況を確認したり、イベントや通知事項を確認したりできます。また、機器の探索状況や資産のインポート状況を監視したり、データベースの状況およびハードディスクの状況を確認したりもできます。



> **ヒント**
>
> パネルをドラッグ&ドロップすることで、パネルの位置を変更できます。また、ホーム画面に表示するパネルやパネルの基本レイアウトを変更したい場合は、画面上部の［表示］メニューの［パネルのレイアウト設定］から設定できます。

状況を確認したら、各パネルのリンクからほかの画面に移動し、管理作業を始めてください。

関連リンク

- 2.2.1　表示されるパネル

1.3.3　セキュリティ画面でできること

セキュリティ画面では、セキュリティポリシー（セキュリティのルール）を作成できます。セキュリティポリシーをコンピュータに割り当てると、セキュリティ状況を管理したり、セキュリティ状況に問題があるコンピュータに対策を実行したりできます。また、操作ログを管理して不審な操作について調査したり、更新プログラムが適用されているか確認したりできます。

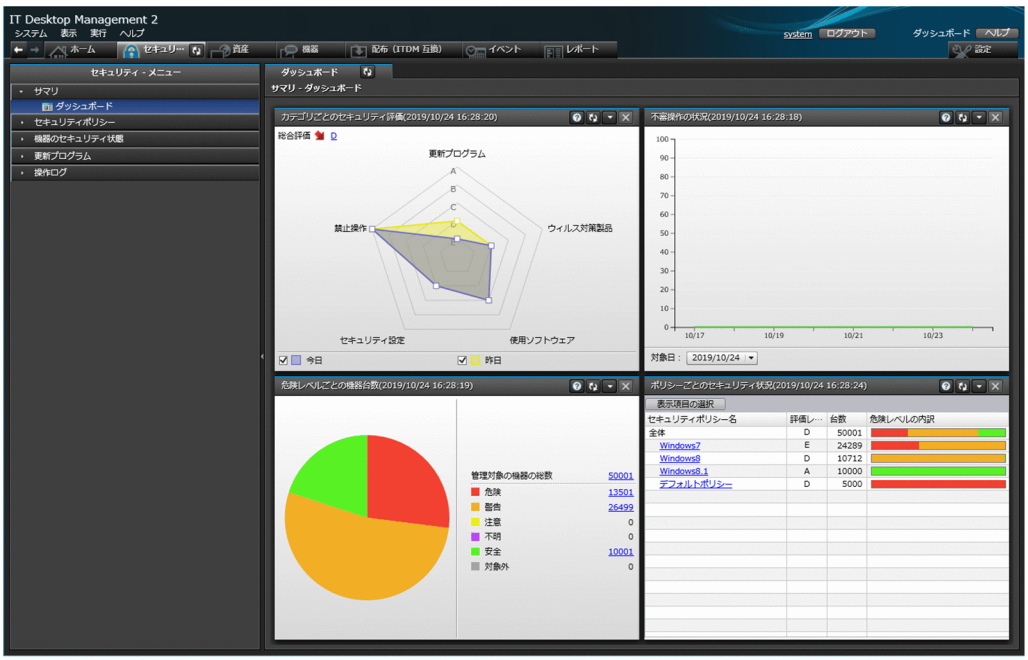
セキュリティ画面には次に示す画面があります。

- ［サマリ］画面
- ［セキュリティポリシー］画面
- ［機器のセキュリティ状態］画面
- ［更新プログラム］画面
- ［操作ログ］画面

各画面について以降で説明します。

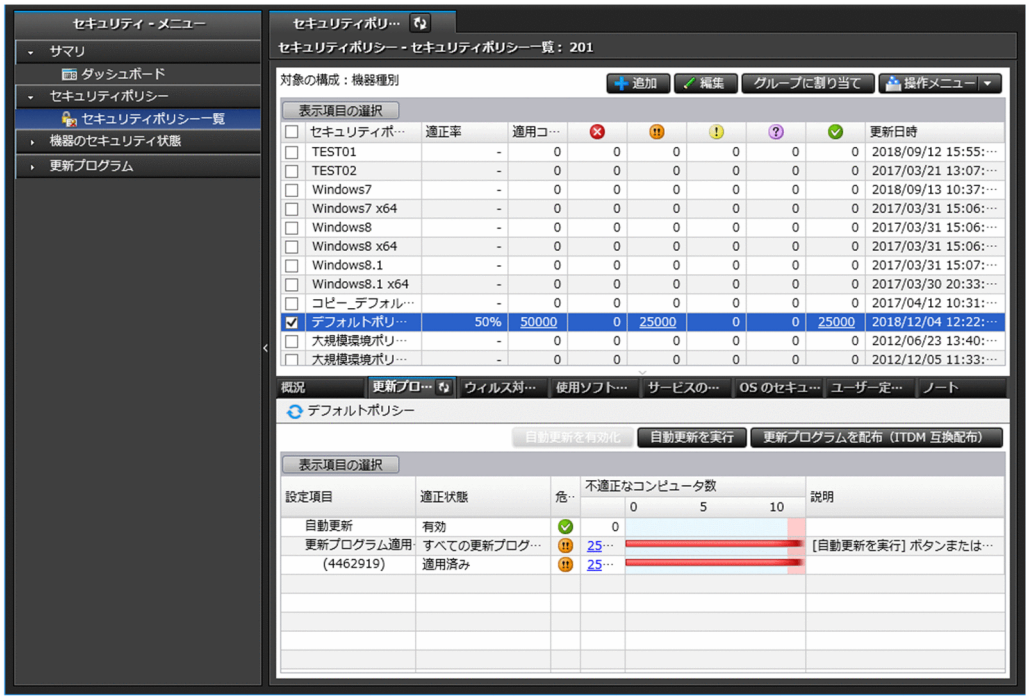
［サマリ］画面

組織内で管理しているコンピュータのセキュリティ状況の概況をパネルで確認できます。



［セキュリティポリシー］画面

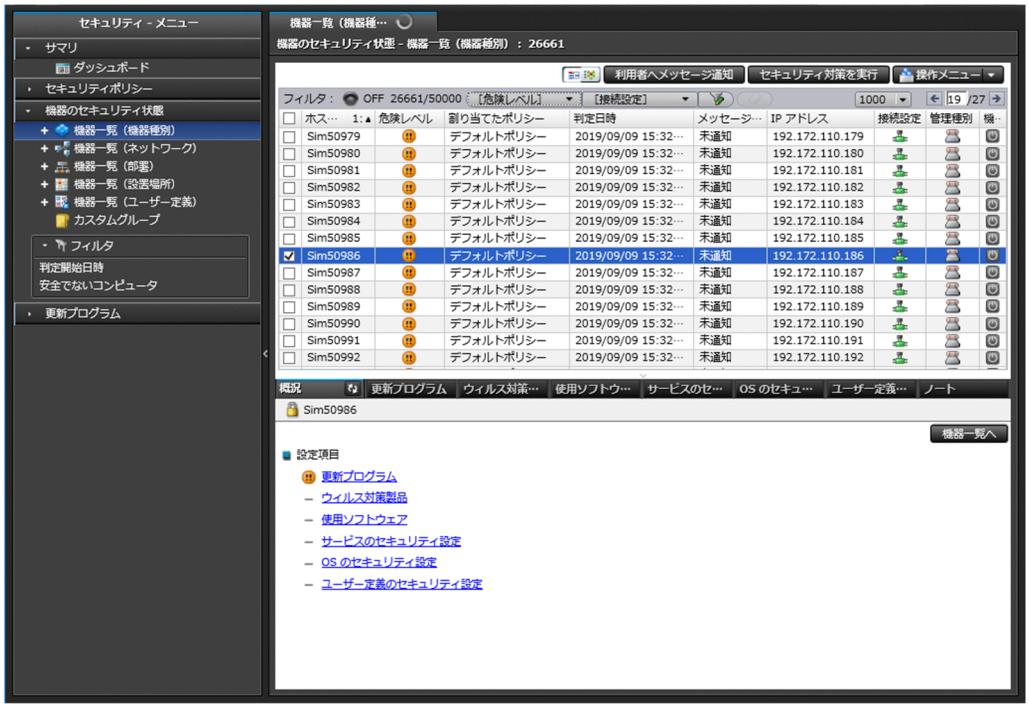
セキュリティポリシーを作成して、グループに割り当てられます。セキュリティポリシーを割り当てることで、組織内のコンピュータを設定したセキュリティのルールで管理できます。



インフォメーションエリアの上部で選択したセキュリティポリシーの遵守状況の詳細が、下部のタブに表示されます。セキュリティ設定項目ごとに遵守状況を確認したり、ポリシー違反の機器に対して対策したりできます。

［機器のセキュリティ状態］画面

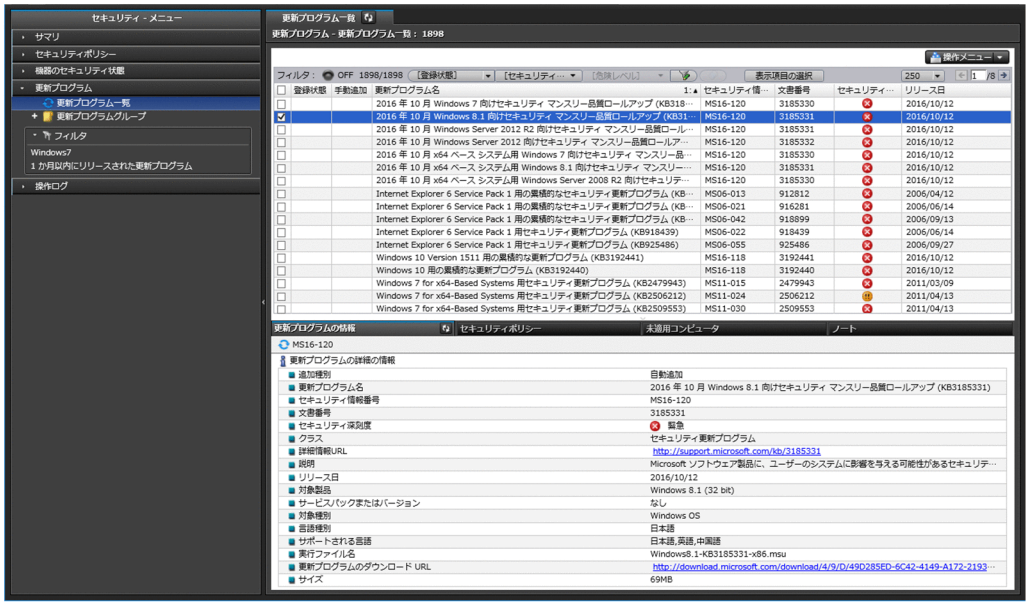
コンピュータごとのセキュリティ状態を確認し、セキュリティポリシーに違反しているコンピュータの利用者にメッセージを通知したり、強制対策したりできます。また、セキュリティポリシーをコンピュータごとに割り当てることができます。



インフォメーションエリアの上部で選択したコンピュータのセキュリティポリシーの遵守状況が、下部のタブに表示されます。セキュリティ設定項目ごとに遵守状況を確認できます。

［更新プログラム］画面

コンピュータに更新プログラムが適用されているかどうかを確認できます。また、セキュリティポリシーで適用状況の判定対象とする更新プログラムを管理できます。判定対象とした更新プログラムは、未適用のコンピュータに自動的に配布、適用できます。

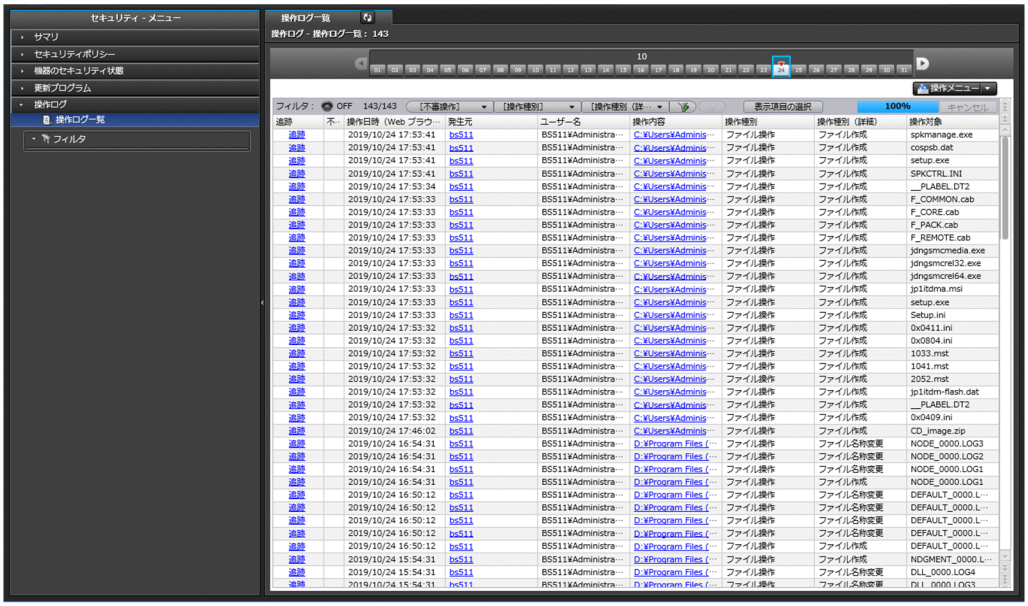


インフォメーションエリアの上部で選択した更新プログラムの情報が、下部のタブに表示されます。セキュリティポリシーへの設定状況や、更新プログラムが未適用のコンピュータを確認できます。

［操作ログ］画面

管理用サーバに取得された操作ログを確認できます。

利用者の操作ログを一覧で確認し、不審操作を調査できます。ファイルの持ち込みまたは持ち出しを追跡したり、操作したコンピュータを特定したりすることで、情報漏えいの早期発見および対策ができます。



なお、管理用サーバに操作ログが取得されていない場合、この画面は表示されません。

1.3.4　資産画面でできること

資産画面では、組織内で管理している機器、ソフトウェアライセンス、契約などの資産情報をまとめて管理できます。各資産を一覧化して台帳のように管理できるほか、資産情報同士の関係を定義することで、機器に対して結んでいる契約を即座に把握したり、ソフトウェアライセンスの利用状況を把握したりできるため、資産管理業務の効率化を図れます。

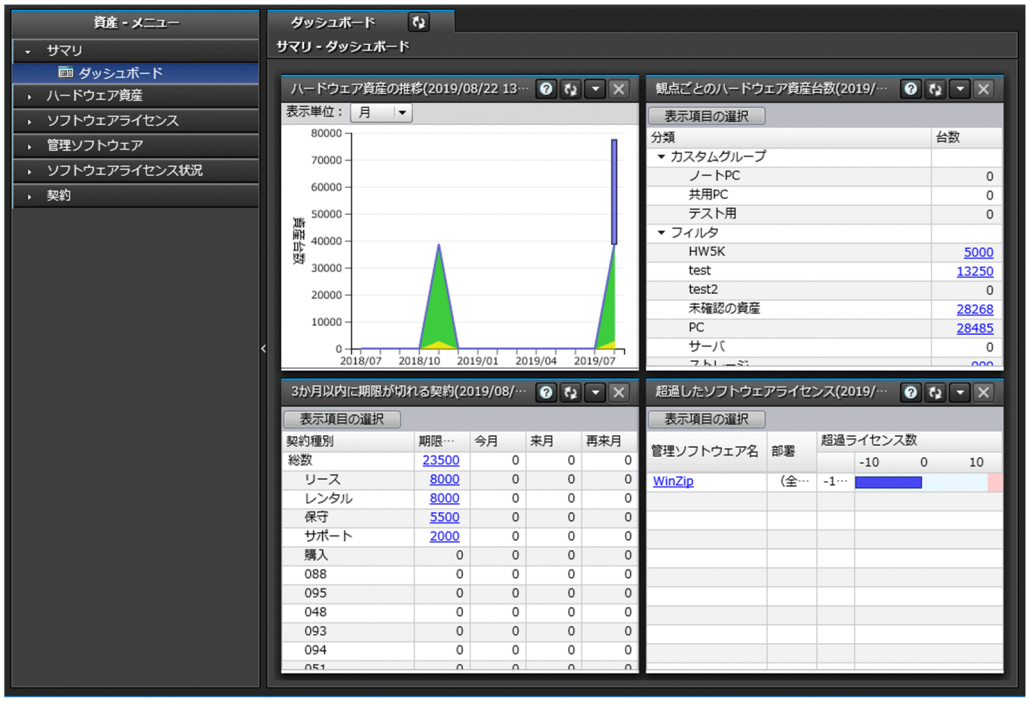
資産画面には次に示す画面があります。

- ［サマリ］画面
- ［ハードウェア資産］画面
- ［ソフトウェアライセンス］画面
- ［管理ソフトウェア］画面
- ［ソフトウェアライセンス状況］画面
- ［契約］画面

各画面について以降で説明します。

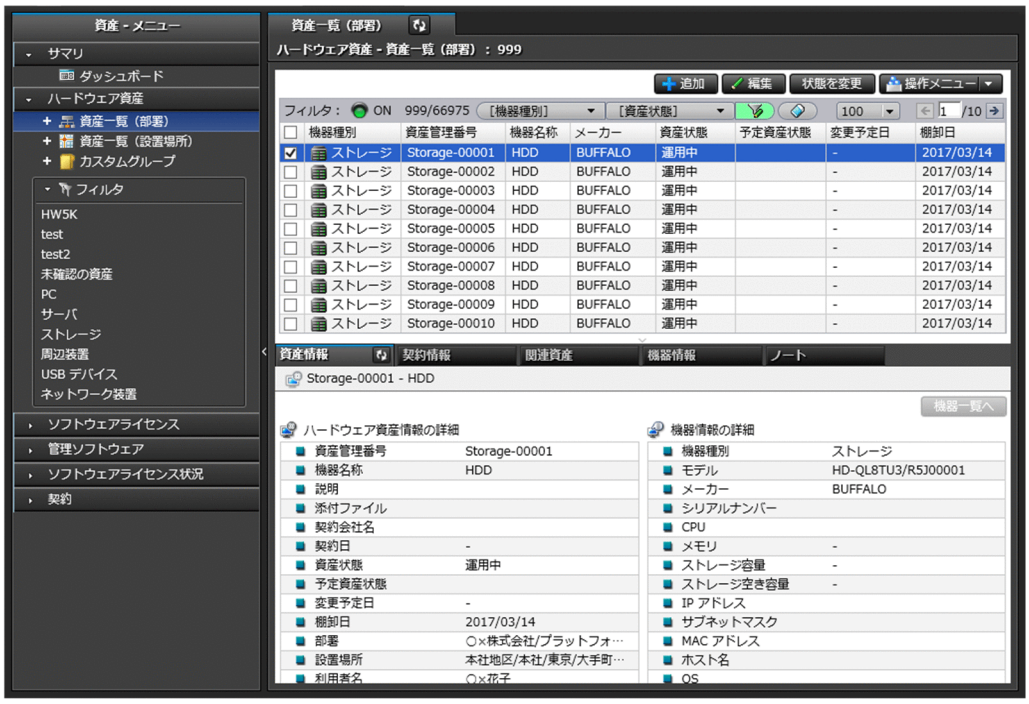
［サマリ］画面

JP1/IT Desktop Management 2 で管理している資産情報の概況をパネルで確認できます。



［ハードウェア資産］画面

組織内のコンピュータやプリンタ、ネットワーク装置などのハードウェア資産の情報を管理できます。また、ハードウェア資産に契約情報を関連づけることもできます。契約情報を関連づけると、ハードウェア資産の契約費用や契約期間などを把握できます。

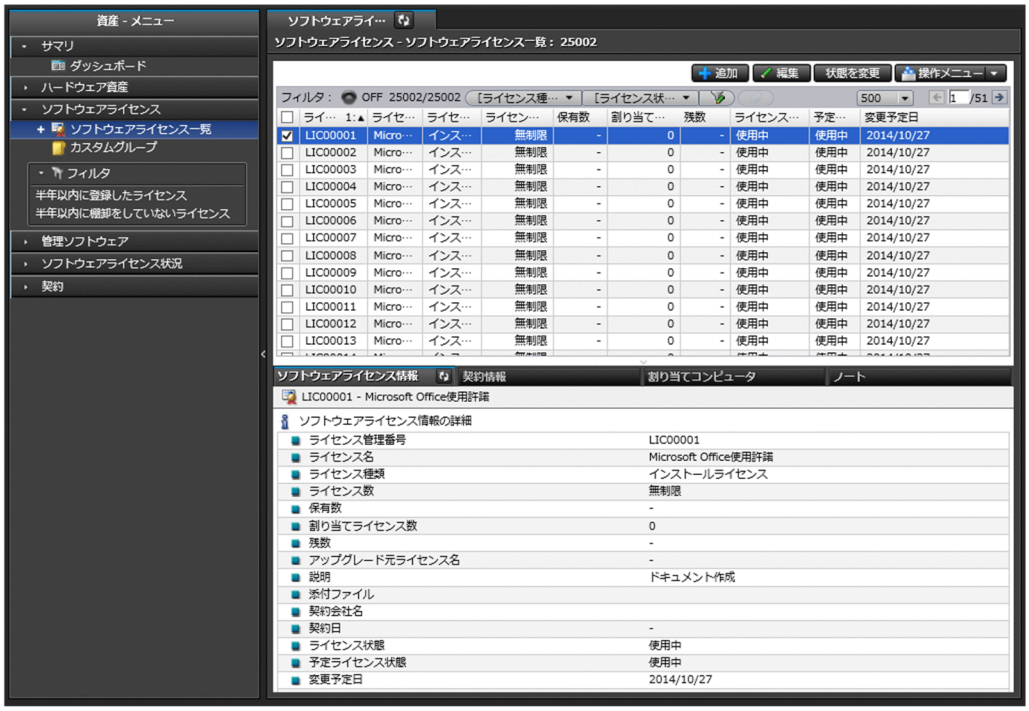


インフォメーションエリアの上部で選択したハードウェア資産の詳細情報が、下部のタブに表示されます。ハードウェア資産に対応する契約、関連する資産、対応する機器などを確認できます。

なお、ハードウェア資産情報が機器情報と関連づいている場合、ハードウェア資産情報のうちの［機器情報］は、収集された機器情報で自動的に更新されます。

［ソフトウェアライセンス］画面

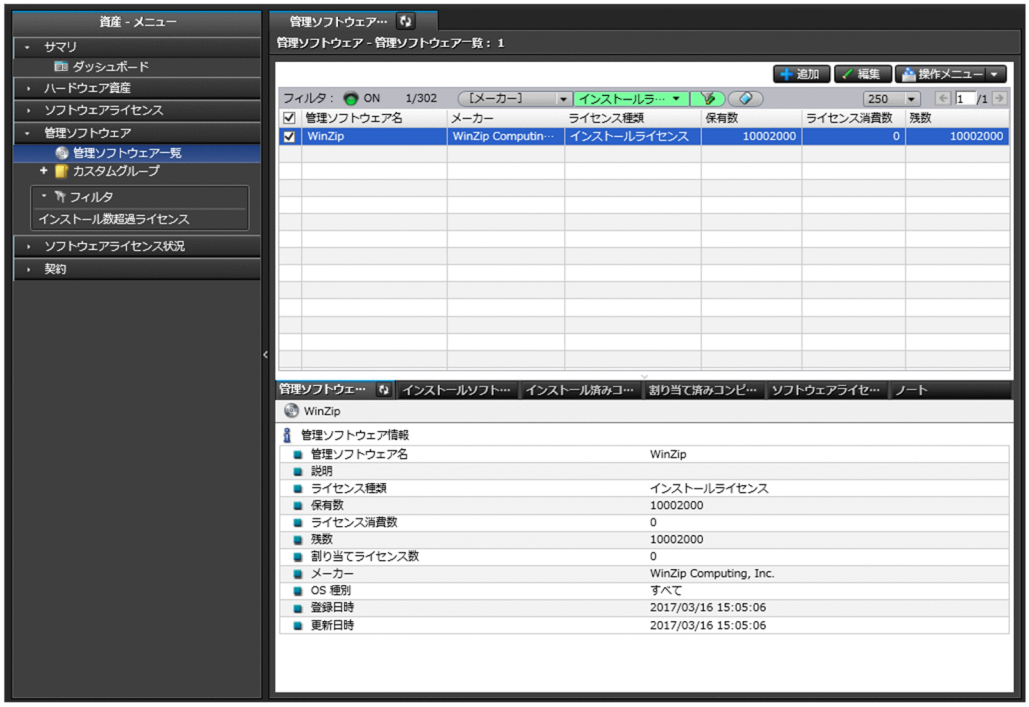
組織で所持しているソフトウェアライセンスの情報を管理できます。また、ソフトウェアライセンスをコンピュータに割り当てることで、ライセンスの利用許可の管理もできます。



インフォメーションエリアの上部で選択したソフトウェアライセンスの詳細情報が、下部のタブに表示されます。ソフトウェアライセンスに対応する契約、ライセンスを割り当てているコンピュータなどを確認できます。

［管理ソフトウェア］画面

管理ソフトウェア（ライセンス消費数をカウントするソフトウェア）の情報を管理できます。管理ソフトウェアを登録すると、ソフトウェアのライセンス消費数が集計され、利用実態を把握できます。



インフォメーションエリアの上部で選択した管理ソフトウェアの詳細情報が、下部のタブに表示されます。ソフトウェアをインストールしているコンピュータ、ソフトウェアライセンスを割り当てているコンピュータ、対応するソフトウェアライセンスなどを確認できます。

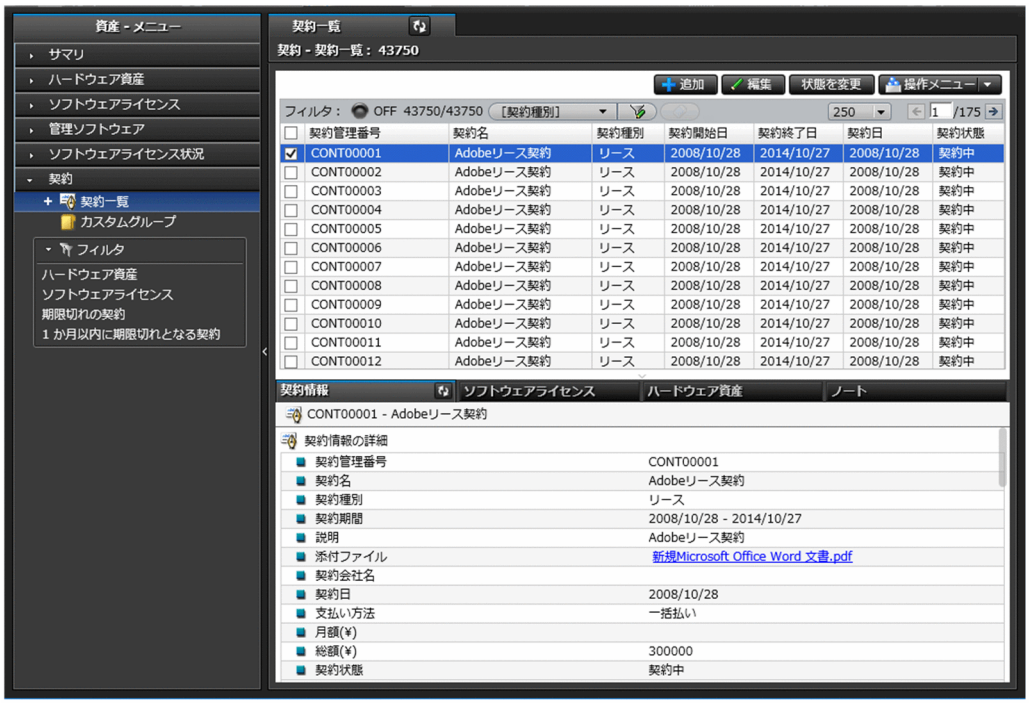
［ソフトウェアライセンス状況］画面

管理ソフトウェアごとのソフトウェアライセンスの利用状況を確認できます。ソフトウェアライセンスの保有数や残数がライセンス種類および部署別に集計され、ソフトウェアライセンスの過不足を把握できます。

インフォメーションエリアの上部で選択した管理ソフトウェアの詳細情報が、下部のタブに表示されます。ソフトウェアをインストールしているコンピュータ、ソフトウェアライセンスを割り当てているコンピュータ、対応するソフトウェアライセンスなどを確認できます。

［契約］画面

ハードウェア資産やソフトウェアライセンスに対する契約の情報を管理できます。契約情報を追加することで、資産に対する契約費用や契約期間などを把握できるようになります。



インフォメーションエリアの上部で選択した契約の詳細情報が、下部のタブに表示されます。契約対象のソフトウェアライセンスやハードウェア資産などを確認できます。

1.3.5　機器画面でできること

機器画面では、管理対象の機器の機器情報やインストールソフトウェア情報を参照して、現状確認できます。また、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場合は、この画面でコンピュータの電源を制御したり、利用者にメッセージを通知したりできます。

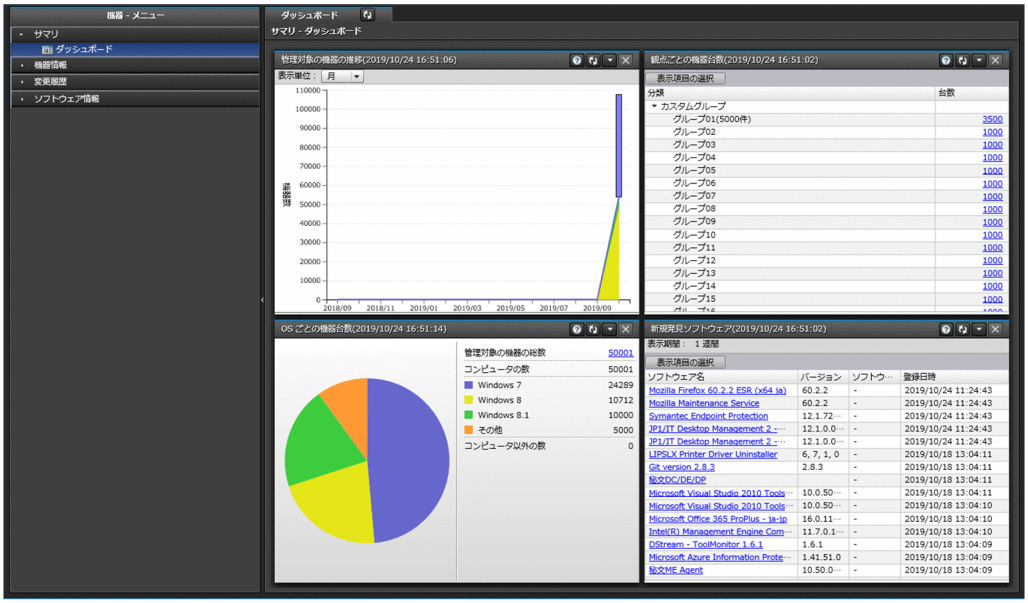
機器画面には次に示す画面があります。

- ［サマリ］画面
- ［機器情報］画面
- ［変更履歴］画面
- ［ソフトウェア情報］画面

各画面について以降で説明します。

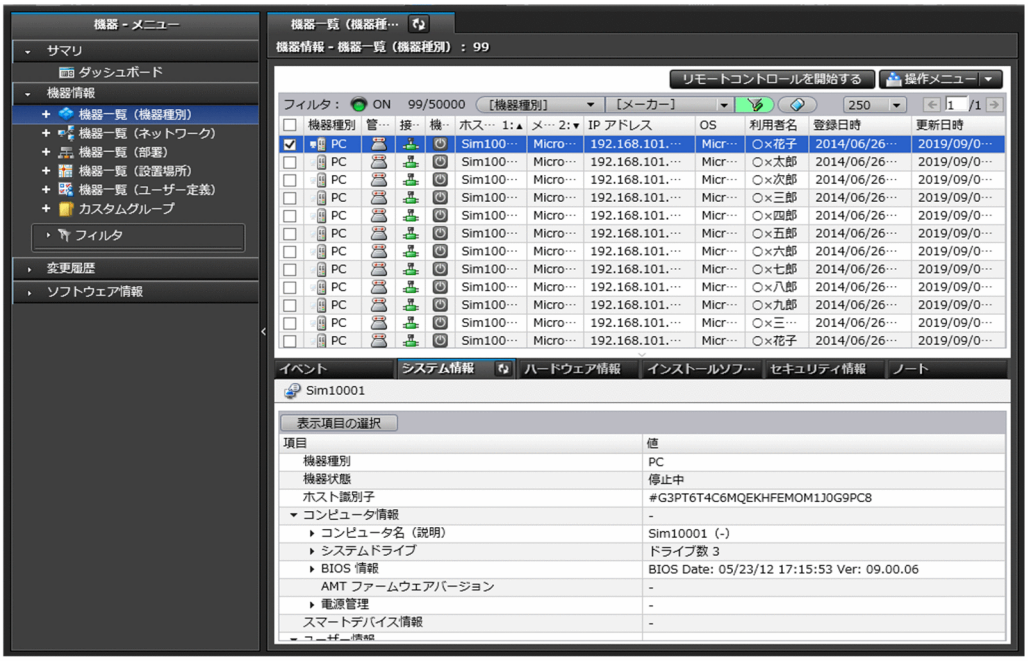
［サマリ］画面

JP1/IT Desktop Management 2 で管理している機器やソフトウェアの概況をパネルで確認できます。



［機器情報］画面

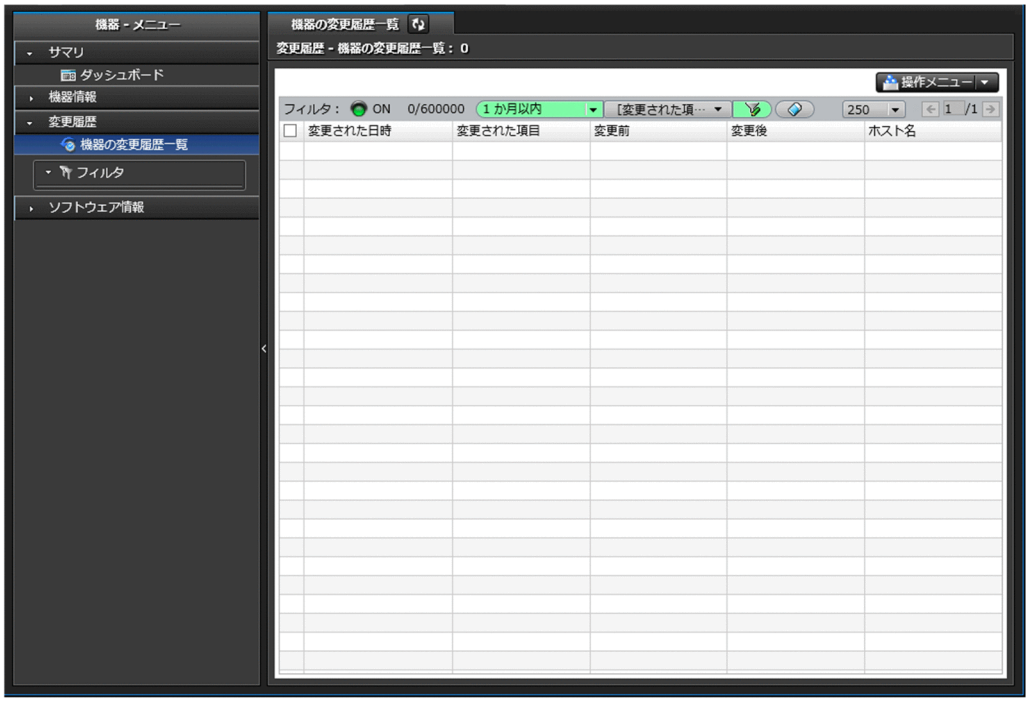
管理対象の機器の情報や電源状態などを確認できます。また、利用者へのメッセージ通知、コンピュータの電源制御、コンピュータのリモートコントロールなど、機器に対する操作を実行できます。



インフォメーションエリアの上部で選択した機器の詳細情報が、下部のタブに表示されます。システム情報、ハードウェア情報、インストールソフトウェア情報、セキュリティ情報などを確認できます。

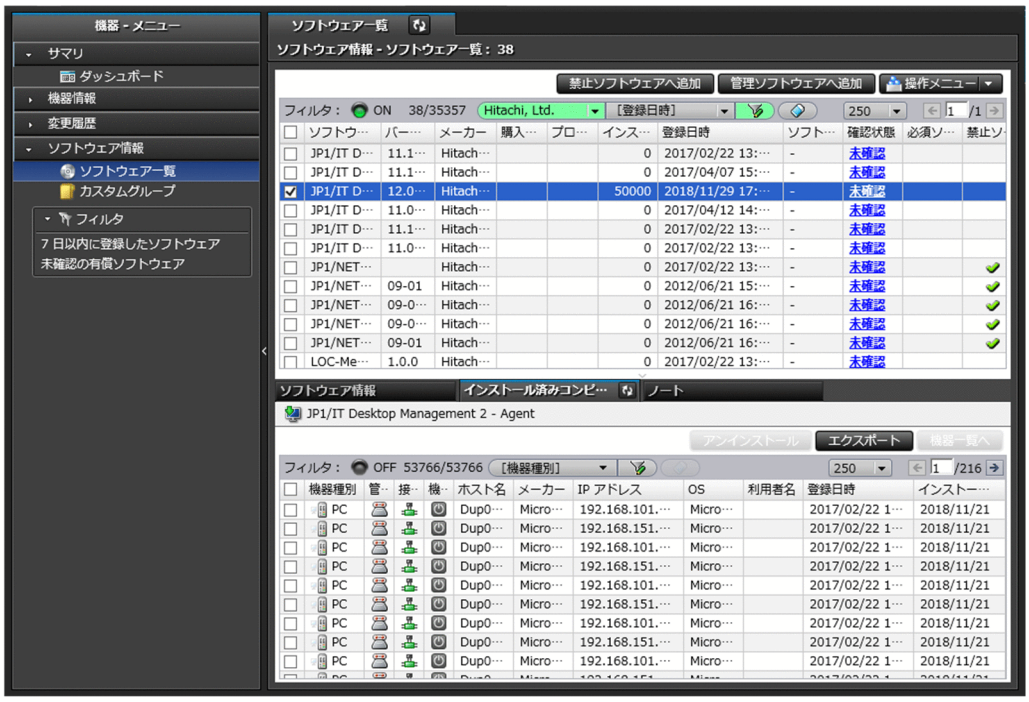
［変更履歴］画面

CPU やメモリ、IP アドレスなど、機器の構成に変更があった場合、 変更履歴として表示されます。その変更履歴を確認することで、不正な構成変更を見つけやすくなります。



［ソフトウェア情報］画面

管理対象のコンピュータにインストールされているソフトウェアの情報を管理できます。ソフトウェアごとにインストールしているコンピュータを確認したり、特定のソフトウェアを使用禁止ソフトウェアとしてセキュリティポリシーに設定したりできます。



インフォメーションエリアの上部で選択したソフトウェアの詳細情報が、下部のタブに表示されます。ソフトウェア情報、インストール済みコンピュータなどを確認できます。

1.3.6　配布（ITDM 互換）画面でできること

配布（ITDM 互換）画面では、コンピュータに必要なソフトウェアを配布してインストールしたり、不要なソフトウェアをアンインストールしたりできます。また、ソフトウェアだけではなく必要なファイルを配布することもできます。

なお、UNIX エージェント、Mac エージェントへの配布には、配布（ITDM 互換）画面を使えません。UNIX エージェント、Mac エージェントへの配布は、リモートインストールマネージャを使用して配布してください。

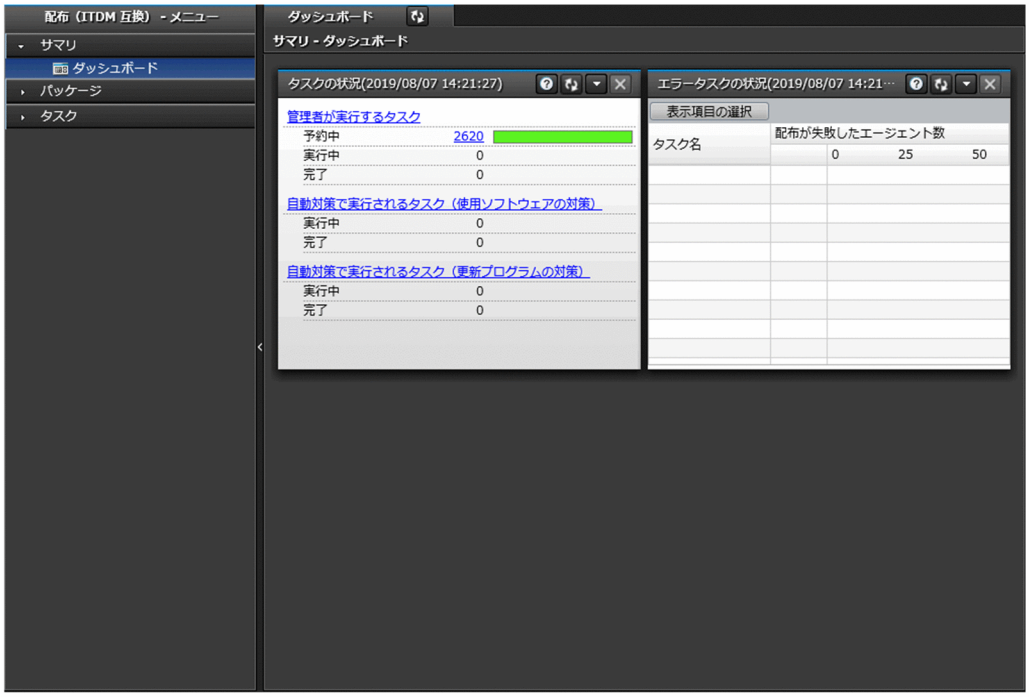
配布（ITDM 互換）画面には次に示す画面があります。

- ［サマリ］画面
- ［パッケージ］画面
- ［タスク］画面

各画面について以降で説明します。

［サマリ］画面

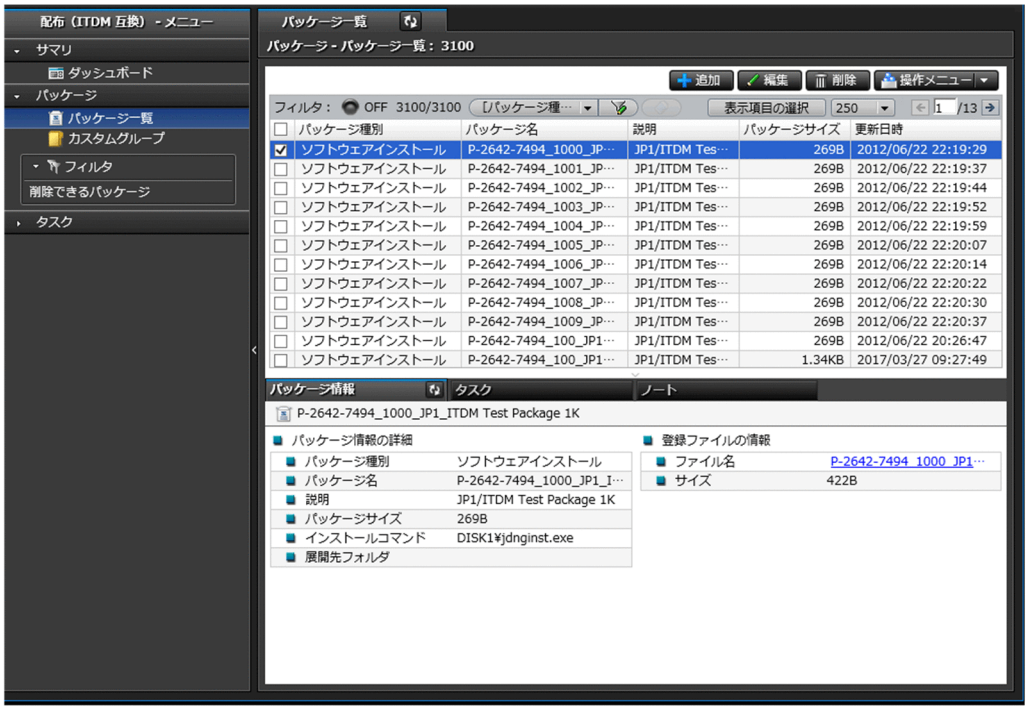
タスクの実行状況やエラーが発生したタスクをパネルで確認できます。



［パッケージ］画面

配布するソフトウェアやファイルを登録したパッケージを管理できます。この画面で、パッケージを追加・編集したり、パッケージ配布タスクを再実行・中止したりできます。

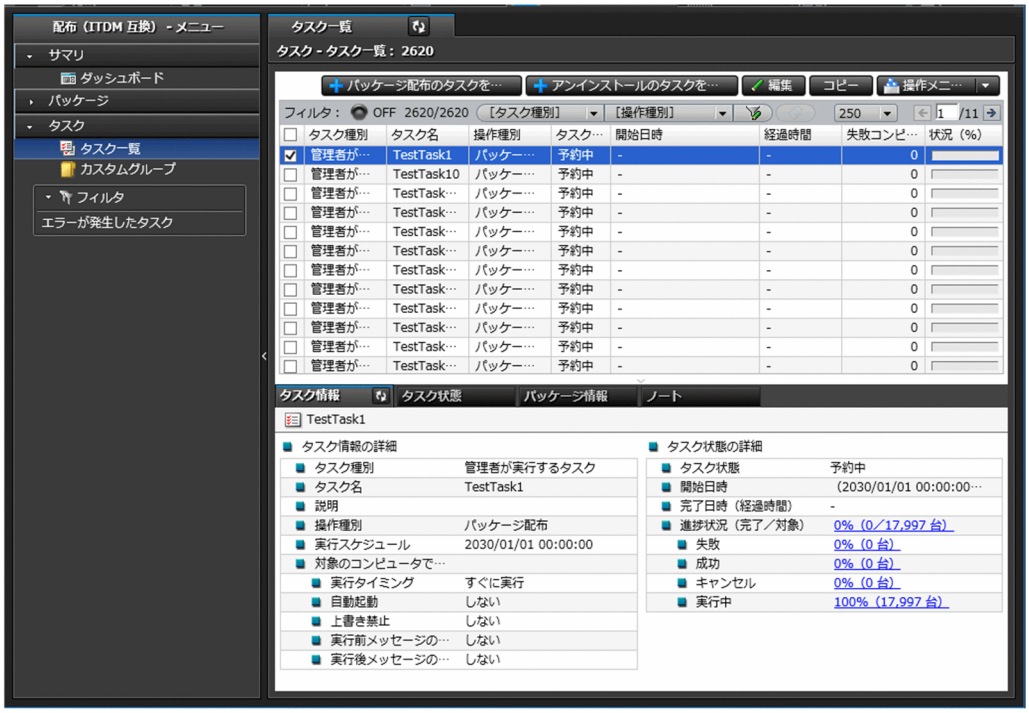
また、ソフトウェアのインストール、ファイルの配布、ソフトウェアのアンインストールを実行するウィザードを起動できます。



インフォメーションエリアの上部で選択したパッケージの詳細情報が、下部のタブに表示されます。パッケージ情報やパッケージを配布するためのタスクなどを確認できます。

［タスク］画面

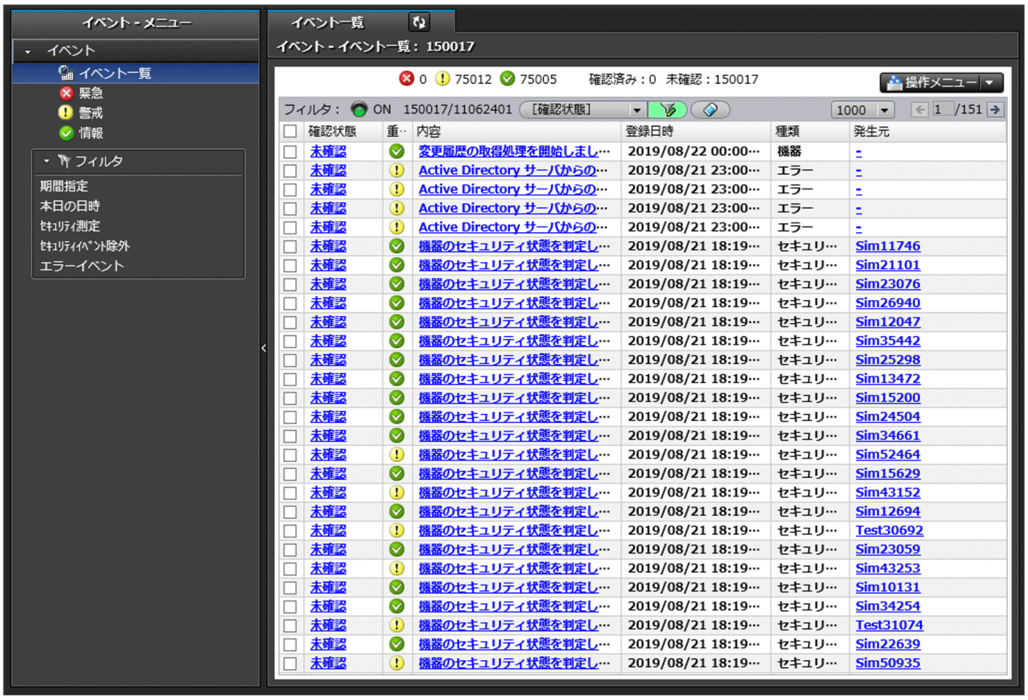
パッケージを配布したり、ソフトウェアをアンインストールしたりするためのタスクを管理できます。この画面で、タスクを追加・編集したり、タスクを再実行・キャンセルしたりできます。



インフォメーションエリアの上部で選択したタスクの詳細情報が、下部のタブに表示されます。タスク情報、タスク状態、パッケージ情報などを確認できます。

1.3.7　イベント画面でできること

イベント画面では、JP1/IT Desktop Management 2 の運用中に発生したイベントを確認できます。セキュリティ判定、機器の探索などの操作が正常に終了したかどうかなどがイベントとして表示されます。



[内容] のリンクをクリックすると、イベントの詳細を確認できます。

イベントの内容によっては早急に対処が必要な場合があります。重大度が［緊急］のイベントを最優先に確認し、次に［警戒］のイベントを確認してください。イベントの内容から原因を特定して対処します。

イベントを確認して対処が完了したら、イベントの［確認状態］を［確認済み］にします。［確認状態］を変更することで、対処が完了したイベントかどうかを区別できます。

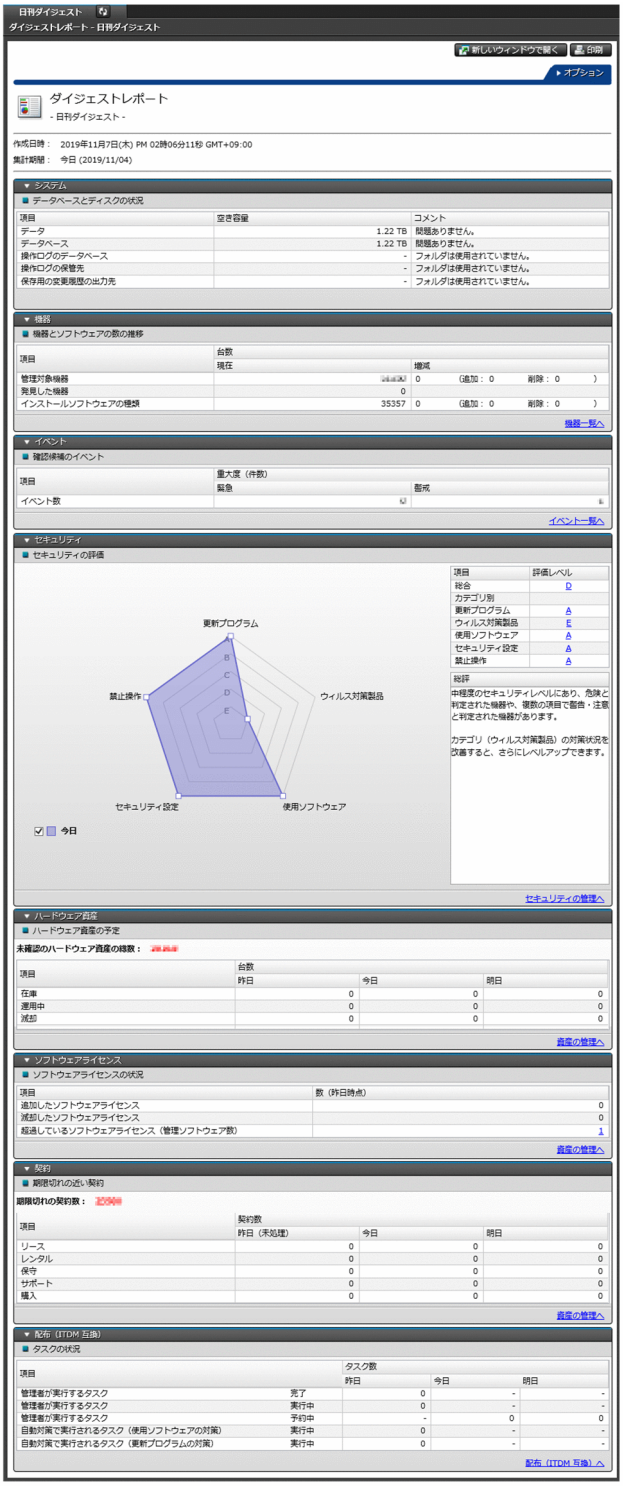
1.3.8　レポート画面でできること

レポート画面では、コンピュータのセキュリティの状態や、管理対象の機器の情報などをレポート形式で確認できます。また、レポートを印刷して報告書としても使用できます。

レポートの例を次に示します。

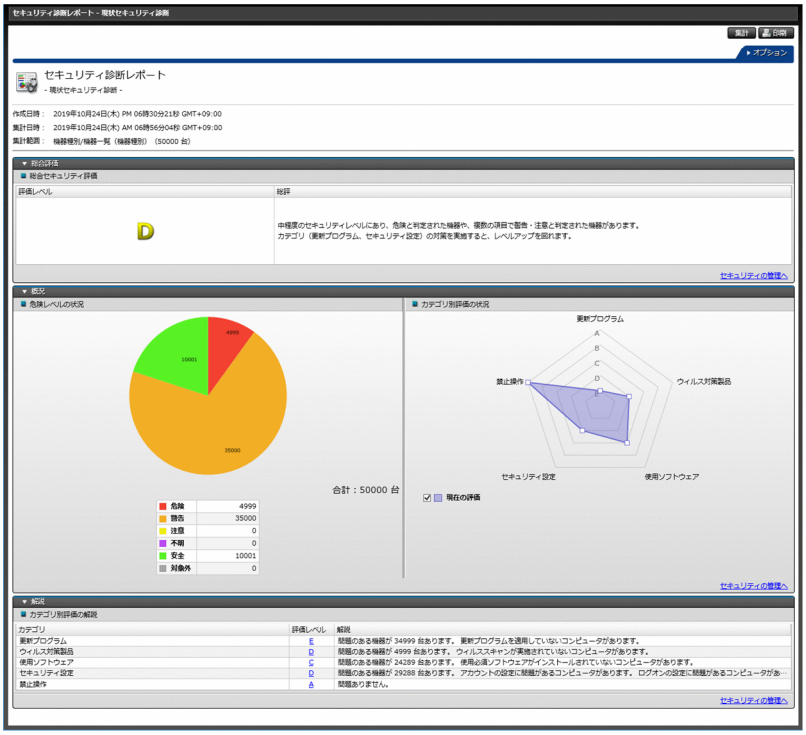
［日刊ダイジェスト］レポート

イベント発生状況、資産状態を変更する予定の資産数、ソフトウェアライセンスの状況、配布の実行状況などを、日単位で確認できます。



［現状セキュリティ診断］レポート

現在のセキュリティ状況の診断結果について確認できます。



1.3.9　設定画面でできること

設定画面では、ユーザーアカウントやエージェント設定など JP1/IT Desktop Management 2 の各種設定をカスタマイズできます。また、機器の探索やエージェントの配信なども、この画面から実行できます。

各画面について以降で説明します。

［設定一覧］画面

設定画面でできることを一覧で確認できます。この画面から、各設定画面に移動して環境をカスタマイズできます。

［サイトマップ］画面

JP1/IT Desktop Management 2 の主な画面を一覧で確認できます。各リンクをクリックすると、直接その画面を表示できます。目的の画面の場所がわからなくなってしまった場合に、この画面から探して表示すると便利です。

各設定画面

［ユーザー管理］画面

JP1/IT Desktop Management 2 のユーザーアカウントを追加、編集、および削除できます。

［エージェント］画面

エージェント設定の作成と編集、およびインストールセットの作成ができます。また、エージェントを配信したり、各エージェントにエージェント設定を割り当てたりできます。

なお、UNIX エージェント、Mac エージェントについては適用できません。

［機器の探索］画面

機器の探索条件を設定したり、探索を即時実行したりできます。また、機器を管理対象にして、JP1/IT Desktop Management 2 での機器の管理を始められます。

［ネットワーク制御］画面

新規に発見した機器をネットワークに接続するかどうかを、ネットワークセグメントごとに設定できます。また、JP1/NETM/NM - Manager との連携や、ネットワーク制御リストに関する設定もできます。

［セキュリティ管理］画面

管理対象のコンピュータのセキュリティ状況を判定するスケジュールを設定できます。また、操作ログの自動取り込みとエクスポートに関する設定や、Windows OS バージョンの設定、更新プログラムのセキュリティ判定の設定もできます。

［資産管理］画面

資産情報の管理項目を設定できます。また、契約会社一覧の情報を追加、編集、および削除できます。なお、資産情報を CSV ファイルからインポートした場合は、資産情報のインポート状況および結果を確認できます。

［機器］画面

Windows の［プログラムと機能］に表示されないソフトウェアの検索条件を追加、編集、および削除できます。また、JP1/IT Desktop Management 2 で AMT を使用するための設定や、変更履歴を取得するための設定もできます。さらに、機器メンテナンスの条件設定や検出の実行ができます。

［レポート］画面

レポートの保存期間および開始日を設定できます。また、ダイジェストレポートを送付するユーザーを設定できます。

［イベント］画面

イベント発生時に通知するユーザー、通知対象にするイベントの重大度や種類、通知対象から外すイベントを設定できます。

［他システムとの接続］画面

メールサーバ、Active Directory、サポートサービス、および MDM システムとの接続を設定できます。

［製品ライセンス］画面

JP1/IT Desktop Management 2 のライセンス情報の確認やライセンスの追加ができます。

2 機能の紹介

ここでは、JP1/IT Desktop Management 2 の機能の詳細について説明します。

2.1 機能一覧

ヒント

JP1/IT Desktop Management 2 - Operations Director の場合、サポート対象外の機能があります。詳細については、「付録 A.13　JP1/IT Desktop Management 2 - Operations Director での機能制限」を参照してください。

機能	概要
システムの概況表示	ホーム画面や各画面のダッシュボードから、さまざまな観点で、運用状況を把握できます。
ユーザーアカウントの管理	権限、業務分掌、または管轄範囲を設定することで、JP1/IT Desktop Management 2 を利用する管理者の役割に応じたユーザーアカウントを作成できます。
運用準備の支援	ウィザードを利用して、JP1/IT Desktop Management 2 の運用を開始するための準備ができます。
エージェントの導入	利用者のコンピュータにエージェントを導入することで、JP1/IT Desktop Management 2 の管理対象となり、各種機能を実行できます。 エージェントは、管理者が手動でインストールしたり、管理用サーバから自動で配信したり、さまざまな方法で導入できます。
機器の管理	機器を管理対象にすると、情報を収集して確認したり、電源状態を把握して制御したりできます。また、セキュリティポリシーによる判定、レポートの集計など、各種機能の対象になります。なお、UNIX エージェント、Mac エージェントは、電源制御の対象外です。 探索機能、ネットワーク監視機能を利用することで、組織内の機器を自動で発見して管理対象にできます。
機器のリモートコントロール	コントローラから利用者のコンピュータの画面を呼び出して遠隔操作できます。このほかに、ファイルの送受信、操作内容の録画と再生、チャットなどもできます。なお、UNIX エージェントは、遠隔操作の対象外です。また、Mac OS のコンピュータは、RFB 接続によるリモートコントロールだけができます。
機器のネットワーク接続の管理	ネットワークを監視して、未許可の機器のネットワーク接続を防いだり、危険なコンピュータを自動的にネットワークから切断したりできます。UNIX エージェントの接続/遮断は手動での操作となります。
セキュリティの管理	セキュリティポリシーを作成し、コンピュータに適用することでセキュリティ状況を判定できます。セキュリティ上問題のあるコンピュータを自動対策することもできます。 また、コンピュータに対してリモートで対策したり、メッセージを通知したりできます。なお、UNIX エージェントは、セキュリティポリシーによるセキュリティ状況の判定やセキュリティ上の問題点の自動対策の対象外です。Mac エージェントは、セキュリティ上の問題点の自動対策の対象外です。
操作ログの管理	利用者がコンピュータ上で操作した履歴を、操作ログとして収集できます。収集した操作ログは、操作画面から一覧で確認できます。 また、情報漏えいにつながるような不審操作を検知して、操作の履歴を追跡調査できます。なお、UNIX エージェント、Mac エージェントは、操作ログ収集の対象外です。
資産の管理	組織が所有するハードウェア資産やソフトウェアライセンスを登録して、運用状況を管理できます。JP1/IT Desktop Management 2 が提供する資産管理には、次の 2 つの方法があります。 • Asset Console を使用して資産管理をする方法

機能	概要
資産の管理	Asset Console を使用して資産管理をします。資産情報を検索する画面のカスタマイズや案件を使用した資産管理業務の実行など、JP1/IT Desktop Management 2 の操作画面を使用した資産の管理よりも細やかな資産管理をしたい場合に適した方法です。 • JP1/IT Desktop Management 2 の操作画面を使用して資産管理をする方法 JP1/IT Desktop Management 2 - Manager の操作画面（資産画面）を使用して資産管理をします。JP1/IT Desktop Management 2 で収集した情報を利用して、簡単に資産管理したい場合に適した方法です。
ソフトウェアおよびファイルの配布	管理者が利用者のコンピュータの場所まで行くことなく、ソフトウェアおよびファイルを配布できます。配布には、次の 2 つの方法があります。 • リモートインストールマネージャを使用して配布する方法 リモートインストールマネージャを使用して配布します。この方法では、配布先のコンピュータの条件や、配布先のコンピュータでの動作を詳細に指定できます。また、リモートインストールマネージャで管理しているソフトウェアおよびファイルは、コマンドでも配布できます。このため、バッチファイルを利用して定期的に配布したり、JP1/AJS と連携して特定の事象が発生したときに自動で配布したりできます。詳細に条件を指定して配布したい場合や、毎日配布したい場合に適した方法です。 • 操作画面を使用して配布する方法（ITDM 互換配布） 操作画面の配布（ITDM 互換）画面を使用して配布します。リモートインストールマネージャを使用した配布とは異なり、条件や動作を詳細に指定できませんが、ウィザード形式の少ない手順で、インストーラーが MSI ファイルのソフトウェアを、配布先のコンピュータに自動的にインストールできます。また、利用者のコンピュータにインストールされている一部のソフトウェアのアンインストールもできます。インストーラーが MSI ファイルのソフトウェアを、週または月に数回だけ配布したい場合に適した方法です。 リモートインストールマネージャを使用した配布と ITDM 互換配布は、異なる機能です。このため、それぞれの機能に関するデータは、それぞれの機能だけで使用できます。例えば、リモートインストールマネージャで管理しているソフトウェアは、ITDM 互換配布機能で配布できません。 なお、UNIX エージェント、Mac エージェントへの配布と実行状況の確認は、リモートインストールマネージャを使用して配布する方法を利用する必要があります。
ファイルの収集	利用者のコンピュータに格納されているファイルを収集できます。利用者が作成したデータや、利用者が使用したソフトウェアが出力した障害ログなどを、一括で収集できます。 なお、Mac エージェントからのファイルの収集はできません。
イベントの表示	JP1/IT Desktop Management 2 の各機能の実行結果、発生した事象などをイベントとして確認できます。
レポートの表示	システム全体の運用状況、セキュリティの診断結果、省電力化の状況、資産に掛かっている費用など、目的に応じた多様なレポートを表示できます。
フィルタの利用	フィルタを利用して、操作画面の各一覧に表示されている情報を絞り込めます。設定したフィルタの条件は、保存しておくこともできます。
複数の部門やネットワークで構成される大規模システムの管理	管理するシステムの規模やネットワーク構成に合わせて複数の管理用サーバを導入することで、管理者や管理用サーバの負荷を分散したり、NAT 環境での運用に対応したりできます。
クラスタシステムでの運用	クラスタシステムで JP1/IT Desktop Management 2 を運用できます。

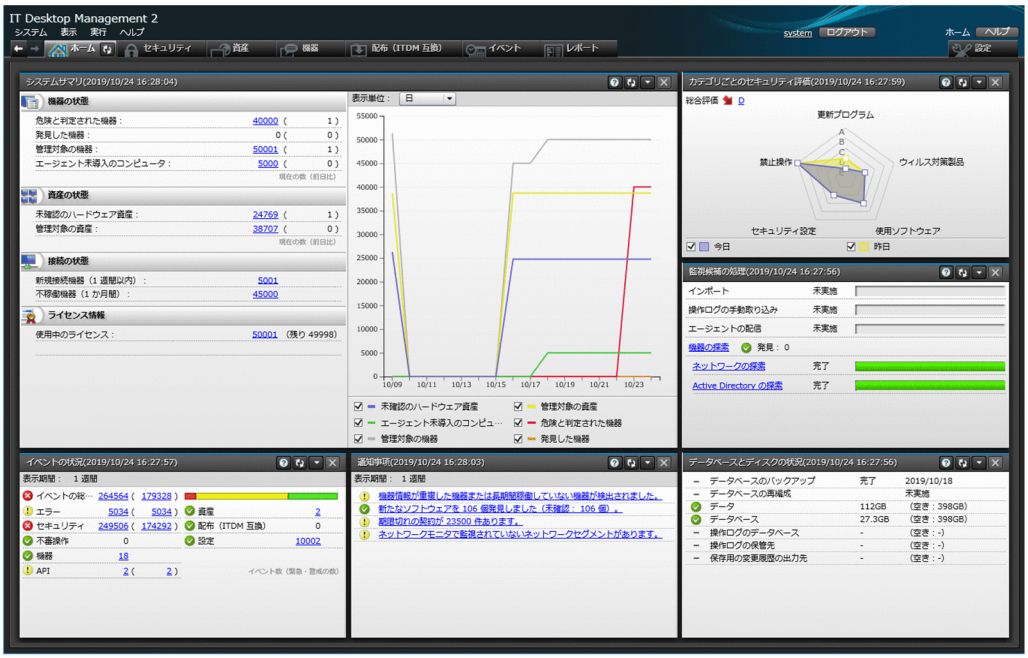
機能	概要
データベースの管理	データベースマネージャを利用して、JP1/IT Desktop Management 2 のデータベースのバックアップやメンテナンスを実行できます。
コマンドの利用	コマンドを利用して、管理情報のインポート、エクスポート、データベースのバックアップ、メンテナンスなどを実行できます。
利用者のコンピュータ上での操作	利用者のコンピュータでは、管理用サーバから通知されるメッセージを確認したり、利用者情報を入力したりできます。なお、UNIX エージェント、Mac エージェントについては、管理用サーバから通知されるメッセージを確認したり、エージェントの利用者情報を入力したりはできません。
スマートデバイスの制御	MDM システムと連携して、スマートデバイスをロックしたり、初期化したりできます。
インターネットを介したコンピュータの管理	インターネットを介して接続されている利用者のコンピュータを管理できます。管理用サーバと利用者のコンピュータが VPN を介して接続している場合だけでなく、VPN を使用せずに接続している場合も管理できます。

2.2　システムの概況表示

JP1/IT Desktop Management 2 では、大量の管理情報に対して管理者が状況を把握するためのホーム画面とダッシュボードを提供しています。これらの画面からは概況を把握するだけなく、確認したい内容のリンクを辿ることで詳細情報を確認できます。

ホーム画面

ホーム画面とは、ログイン後に最初に表示され、JP1/IT Desktop Management 2 の運用の基点となる画面です。ホーム画面には、管理している最新情報を基に、日々の運用で把握しておく必要がある内容が表示されます。そのため、ホーム画面を確認するだけで、システム全体の概況を把握できます。また、ホーム画面の各項目をクリックすることで、詳細な情報を確認できる画面を表示できます。



- ［システムサマリ］パネル

  管理している機器の大まかな状況がわかります。

  - 機器の状態

    セキュリティ状況が「危険」な機器の台数がわかります。その機器のセキュリティ状況を確認し、必要に応じて対策を実施します。また、発見している機器、管理対象の機器、エージェントをインストールしていない機器の台数もわかります。

  - 資産の状態

    資産状態が「未確認」である資産の台数がわかります。その資産の実態を確認し、運用中なのか、在庫なのか、滅却したものなのか状態を明確にします。また、管理対象の資産の台数もわかります。

  - 接続の状態

    1 週間以内にネットワークに新たに接続された機器の台数がわかります。探索で発見した、またはエージェントをインストールすることで管理対象になった新たな機器を確認します。また、1 か月以上ネットワーク経由で存在を確認できない資産の台数もわかります。

- ライセンス情報

  JP1/IT Desktop Management 2 のライセンスを使用している数と残りのライセンスの数がわかります。機器および資産の台数の遷移とライセンスの残数を考慮して、必要に応じてライセンスの追加を検討します。複数サーバ構成で運用している場合、ライセンスを保有していない管理用中継サーバの操作画面には、表示されません。

  なお、ライセンス数は登録したライセンスの総数（Windows、Linux、UNIX 用エージェントのライセンスを登録した場合はその合計）が表示されます。また、総数に占める UNIX および Linux 分を差し引いたライセンス数には Windows 分と Mac OS 分が含まれます（例えば、総数が 150 で UNIX および Linux 分が 50 の場合、100 には Windows 分と Mac OS 分を含みます）。

- [カテゴリごとのセキュリティ評価] パネル

  管理しているコンピュータのセキュリティ状況の評価がわかります。総合評価とカテゴリごとの評価を確認し、評価が低いカテゴリの対策を実施します。

- [監視候補の処理] パネル

  資産情報のインポート、操作ログの手動取り込み、エージェントの配信、および機器の探索についての状況がわかります。完了している場合は結果を確認し、エラーが発生している場合は原因を調査して対策を実施します。

- [イベントの状況] パネル

  まだ確認していないイベントの件数と、そのうち重要度が緊急または警戒であるイベントの件数がわかります。特に緊急度が緊急のイベントがある場合は、早急に内容を確認して対応します。重要度が緊急のイベントがあるかどうかは、イベントの種類の左側に表示されるアイコンでもわかります。

- [通知事項] パネル

  運用中に発生した重要な情報がわかります。通知事項は必ず確認し、問題が発生した場合は早急に対応してください。例えば、次のような情報が通知されます。

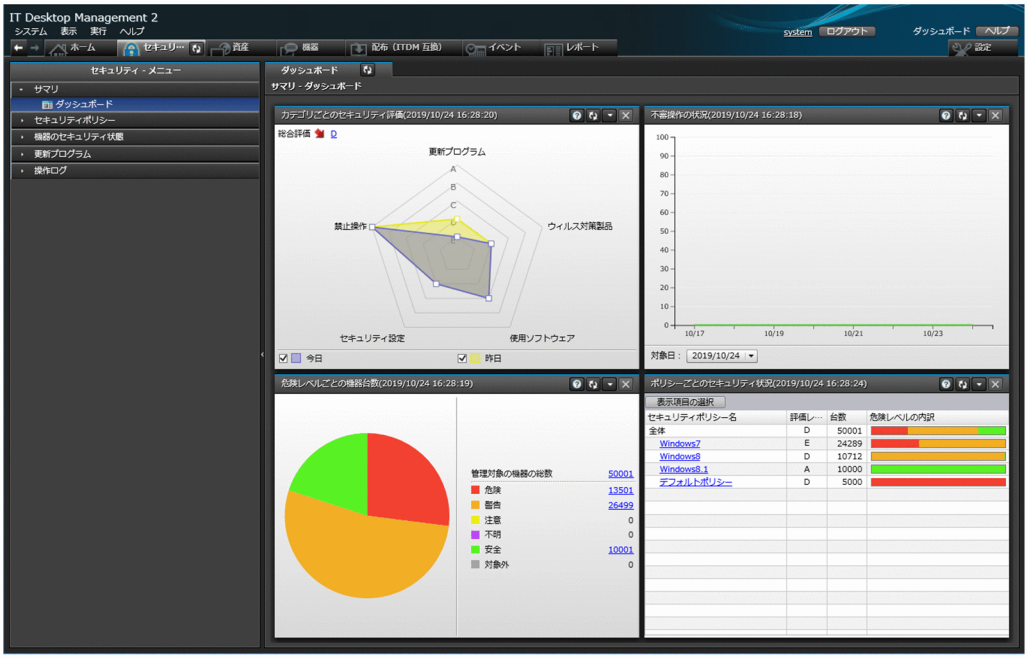
  - データを保存するフォルダの空き容量が少なくなった
  - ライセンス数を超過しているソフトウェアがある
  - 期限切れの契約がある

- [データベースとディスクの状況] パネル

  データベースのバックアップと再編成の実行状況、およびハードディスクの使用状況がわかります。ハードディスクの空き容量が少なくなったら、データベースのバックアップ先を十分に空き容量があるディスク上のフォルダに変更したり、不要なデータを退避したりして空き容量を増やします。

ダッシュボード

ダッシュボードとは、操作画面の上部のメニューから各機能の画面を表示したときに、最初に表示される画面です。ホーム画面と同様にパネルが表示され、各機能の概況を確認できます。例として、セキュリティ画面のダッシュボードを次の図に示します。



ダッシュボードは、セキュリティ画面、資産画面、機器画面、および配布（ITDM 互換）画面で表示できます。

> **ヒント**
>
> ホーム画面およびダッシュボードに表示するパネルは、カスタマイズできます。画面左上の［表示］メニューの［パネルのレイアウト設定］を選択して表示されるダイアログで、パネルのレイアウトと表示するパネルを選択してください。

2.2.1 表示されるパネル

ホーム画面または各画面の［サマリ］－［ダッシュボード］画面に表示されるパネルを次の表に示します。

カテゴリ	パネル名	説明
ホーム	配下の階層構成および稼働状態	自サーバを起点としたシステムの階層構成と、配下の管理用中継サーバの稼働状態を確認できます。また、配下の管理用中継サーバの、操作画面の起動、機器情報の確認、およびリモートコントロールができます。また、配下の管理用中継サーバの情報を削除できます。
	システムサマリ	管理している機器の状態、資産の状態、接続の状態、およびライセンス情報を確認できます。また、機器の台数および資産の数の推移を確認できます。
	監視候補の処理	資産情報のインポート状況、操作ログの手動取り込み状況、エージェントの配信状況、および機器の探索状況について確認できます。エラーが発生している場合は、エラーの内容を確認して必要に応じて対処してください。
	イベントの状況	一定期間内に発生したイベントのうち、未確認のイベント数を確認できます。重大度が「緊急」のイベントについて確認し、対策の起点とすることをお勧めします。

カテゴリ	パネル名	説明
ホーム	通知事項	指定した期間内に発生した通知事項を確認できます。期限切れの契約があったり、製品の残ライセンス数が不足したりしたという重要な情報が通知されます。
	データベースとディスクの状況	JP1/IT Desktop Management 2 のデータベースのバックアップや再編成をいつ実施したか、また、ハードディスクの使用量および空き容量がどれくらいかを確認できます。
セキュリティ	カテゴリごとのセキュリティ評価	コンピュータの総合的なセキュリティ状況、およびカテゴリ別のセキュリティ状況をレベル A～E で評価した結果を確認できます。前日の評価との比較もできるため、セキュリティ対策の効果を確認して対策を見直すことをお勧めします。
	危険レベルごとの機器台数	管理対象の機器の総数と危険レベルごとの台数、および全体の内訳を確認できます。危険レベルが大きい機器を確認して、早急に対策してください。
	不審操作の状況	JP1/IT Desktop Management 2 が検知した不審操作（ファイル持ち出しによる不審操作だけ）の件数を確認できます。リンクからファイル持ち出しによる不審操作の操作ログを確認できるため、無断で持ち出されたデータがないか、などを確認することをお勧めします。
	ポリシーごとのセキュリティ状況	システム全体およびセキュリティポリシーごとのセキュリティ状況を確認できます。評価の低いセキュリティポリシーを確認して、問題のあるコンピュータの対策をしてください。
資産	ハードウェア資産の推移	ハードウェア資産の資産状態ごとの台数の推移を確認できます。例えば、資産状態が「在庫」のハードウェア資産が増加してきているため、古いハードウェア資産を滅却するなどの判断ができます。
	観点ごとのハードウェア資産台数	フィルタおよびカスタムグループごとにハードウェア資産の台数を確認できます。例えば、購入日が古いハードウェア資産が表示されるように設定しておくと、リプレース対象のハードウェア資産を素早く確認できます。
	3 か月以内に期限が切れる契約	契約種別ごとに、期限切れの契約情報や期限切れが近い契約情報の件数が確認できます。件数のリンクから期限切れが近い契約情報を確認して、対処を検討しておくことをお勧めします。
	超過したソフトウェアライセンス	管理ソフトウェアごとにソフトウェアライセンスの超過や余剰をすぐに確認できます。超過している場合は、アンインストールを指示したり、ライセンスを追加したりなどの対処をすることをお勧めします。
機器	管理対象の機器の推移	エージェントの導入状況ごとに、機器の台数の推移を確認できます。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。エージェント未導入のコンピュータを確認して、導入を検討してください。
	観点ごとの機器台数	フィルタおよびカスタムグループごとに管理対象の機器の台数を確認できます。例えば、一定期間使用されていない機器が表示されるように設定しておくと、遊休候補の機器を素早く確認できます。
	OS ごとの機器台数	管理対象のコンピュータにインストールされている OS の割合と台数が確認できます。
	新規発見ソフトウェア	管理対象のコンピュータから新規に収集されたソフトウェア情報を一覧で確認できます。定期的にソフトウェアのインストール状況を確認して、業務に関係ないソフトウェアが表示された場合は禁止ソフトウェアとして登録したり、表示され

カテゴリ	パネル名	説明
機器	新規発見ソフトウェア	たソフトウェアのソフトウェアライセンスの情報を管理するかどうかを検討したりしてください。なお、ソフトウェアライセンスを管理するかどうか検討する際は、ソフトウェア種別を判断基準にできます。例えば、ソフトウェア種別が「有償ソフトウェア」のソフトウェアライセンスだけを管理することもできます。
配布（ITDM互換）	タスクの状況	管理者が実行するタスクと、セキュリティポリシーの自動対策で実行されるタスクの概況を確認できます。エラーが発生したタスクだけを確認したい場合は、[エラータスクの状況]パネルを確認することをお勧めします。
	エラータスクの状況	エラーが発生したタスクを確認できます。エラーの原因を確認して、適切な対策をしてからタスクを再実行してください。タスクの全体の状況を確認したい場合は、[タスクの状況]パネルを確認することをお勧めします。

2.3 ユーザーアカウントの管理

複数の管理者が JP1/IT Desktop Management 2 を使用する場合、管理者ごとに JP1/IT Desktop Management 2 のユーザーアカウントを作成できます。

ユーザーアカウントには、ユーザーの操作範囲や管理情報の開示範囲に応じて次の設定ができます。これらの設定を組み合わせたユーザーアカウントを作成すれば、複数の管理者での業務分担や内部統制を意識した運用ができます。

権限

情報を参照するだけの経営者、機器や資産を管理するシステム管理者、ユーザーアカウントを管理するシステム管理者など、ユーザーの操作範囲に応じて権限を設定できます。

業務分掌

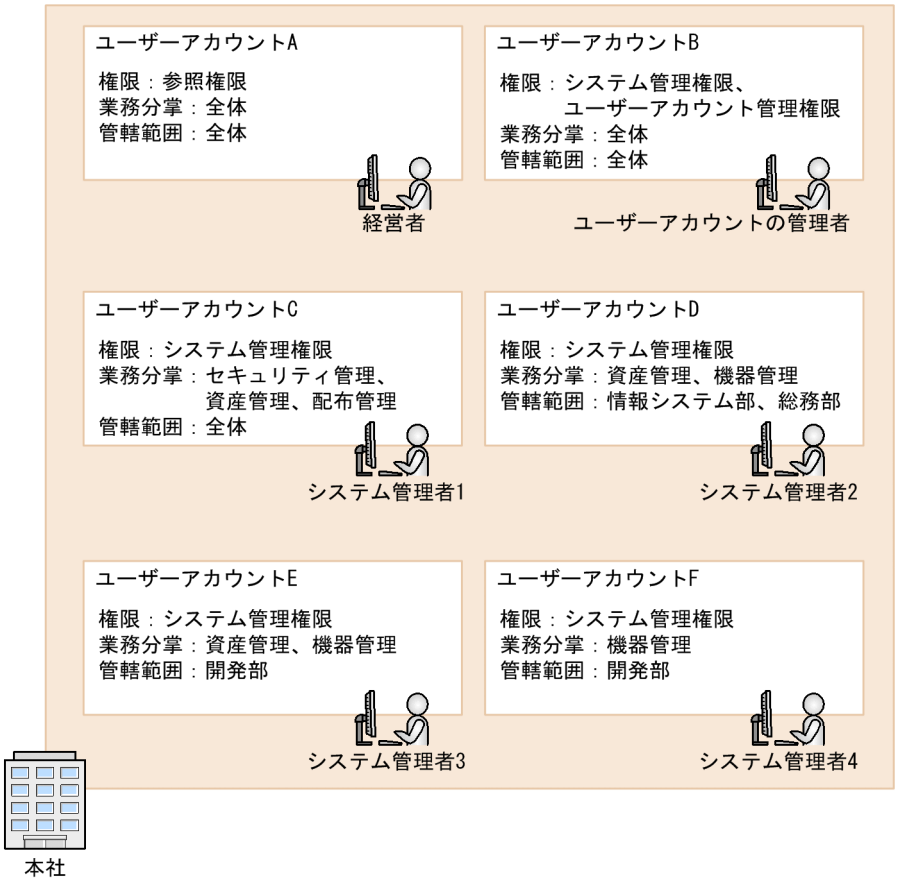
セキュリティ管理、資産管理、機器管理などの業務単位で、権限をさらに限定できます。

管轄範囲

総務部、営業部、開発部などの部門単位で、管理情報の開示範囲を限定できます。

ユーザーアカウントの設定で、業務分掌に配布管理が設定されていてシステム管理権限が付与されている場合に限り、リモートインストールマネージャを使用した配布で操作する画面（リモートインストールマネージャ、パッケージャなど）の操作ができます。

管理者ごとにユーザーアカウントを作成する例を、次の図に示します。



権限の設定でユーザーアカウント管理権限が付与されているユーザーは、ユーザーアカウントを追加、編集、削除できます。

組織内で JP1/IT Desktop Management 2 を利用するユーザーが変更になった場合は、ユーザーアカウントを追加、削除します。管理体制の変更に伴って、ユーザーアカウントのパスワードや権限を変更する場合は、ユーザーアカウントを編集します。なお、ユーザーアカウントのパスワードは定期的に変更する必要があります。パスワードの有効期限が迫ったら、ユーザーアカウントを割り当てられている管理者自身か、ユーザーアカウント管理権限を持つ管理者がパスワードを変更してください。

ヒント

ユーザーアカウントがロックされてしまったユーザーや、パスワードを忘れてしまったユーザーがいる場合、ユーザーアカウント管理権限を持つ管理者が、ユーザーアカウントを編集してロックを解除したり、パスワードを初期化したりできます。

2.3.1 ユーザーアカウントのロック

JP1/IT Desktop Management 2 の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るように設定できます。そのユーザーアカウントはロックが解除されるまでログインできなくなります。

ユーザーアカウントをロックする連続入力失敗の回数は、セットアップ画面の［その他の設定］画面で設定できます。

ロックされているユーザーアカウントがあるかどうかの確認、およびユーザーアカウントのロックの解除は、ユーザーアカウント管理権限を持つユーザーアカウントでログインしたあと、設定画面の［ユーザーアカウントの管理］画面から実施します。

ロックされているユーザーアカウントは、［ユーザーアカウントの管理］画面で、［ロック状態］に［ロック中］と表示されています。

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。

2.3.2 ユーザーアカウントの認証方法

JP1/IT Desktop Management 2 のユーザーアカウントの認証方法には、ITDM2 認証と JP1 認証の 2 種類があります。

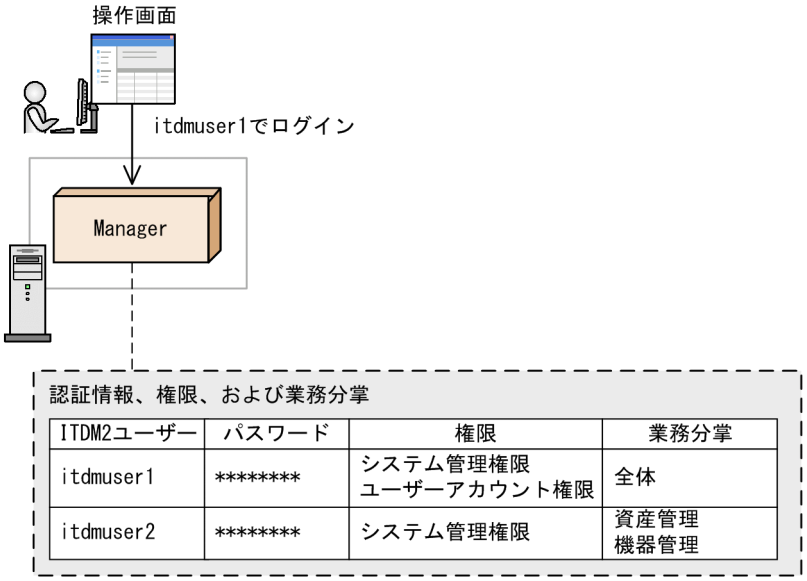
重要

ITDM2 認証と JP1 認証は同時に利用できません。使用するすべてのユーザーアカウントを、どちらかの認証方法に統一する必要があります。

ITDM2 認証

JP1/IT Desktop Management 2 のシステム内でユーザーアカウントを認証する方法です。ユーザーアカウントは JP1/IT Desktop Management 2 の操作画面で作成し、JP1/IT Desktop Management 2 - Manager で管理します。この方法は、JP1/IT Desktop Management 2 システムでの標準のユーザーアカウントの認証方法です。

ITDM2 認証の仕組みを次の図に示します。



（凡例）
Manager：JP1/IT Desktop Management 2 - Manager

JP1 認証

JP1/Base でユーザーアカウントを一元管理し、認証する方法です。ユーザーアカウントは、JP1/Base で JP1 ユーザーとして作成し、認証サーバで管理します。すでにほかの JP1 製品で JP1 認証を使用している場合、そのユーザーアカウントを使用できます。JP1/IM を使用している場合は、メール通知の機能を JP1/IM と連携することもできます。

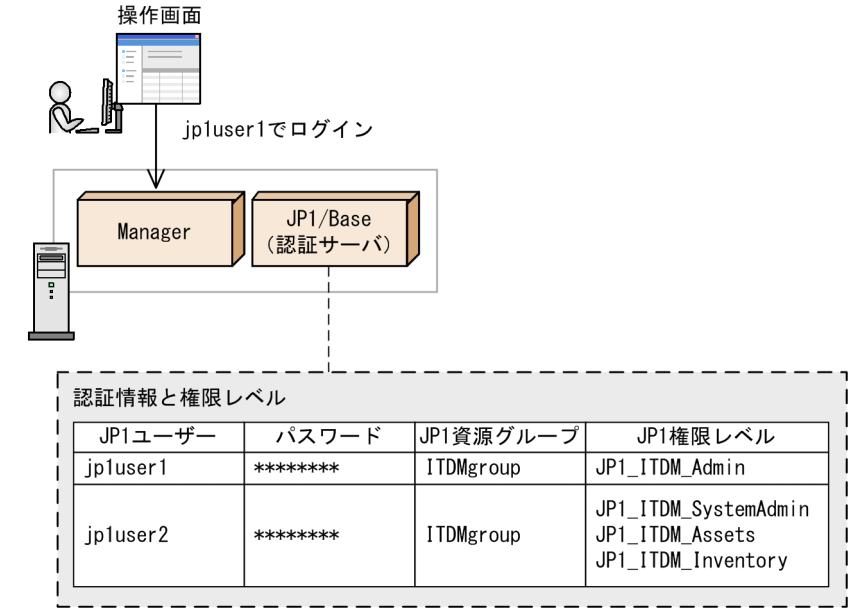
JP1 認証で認証できるプログラムは、次の 3 つです。

- JP1/IT Desktop Management 2 - Manager 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

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。

JP1 認証の仕組みを次の図に示します。



JP1ユーザー	パスワード	JP1資源グループ	JP1権限レベル
jp1user1	********	ITDMgroup	JP1_ITDM_Admin
jp1user2	********	ITDMgroup	JP1_ITDM_SystemAdmin JP1_ITDM_Assets JP1_ITDM_Inventory

（凡例）
Manager：JP1/IT Desktop Management 2 - Manager

2.3.3　ユーザーアカウントの権限

JP1/IT Desktop Management 2 のユーザーアカウントに設定できる権限には、次の 4 種類があります。

- システム管理権限

  ユーザーアカウントの管理を除いて、JP1/IT Desktop Management 2 のすべての機能が利用できる権限です。ユーザーアカウントの追加、編集、および削除以外のすべての操作を実行できます。

- ユーザーアカウント管理権限

  JP1/IT Desktop Management 2 のユーザーアカウントを管理できる権限です。ユーザーアカウントを追加、編集、および削除できます。

- 参照権限

  JP1/IT Desktop Management 2 が管理する情報を参照できる権限です。参照権限はデフォルトで付与されます。

- API 権限

  JP1/IT Desktop Management 2 を API から使用するための権限です。

重要

- システム管理権限、ユーザーアカウント管理権限および参照権限は、API 権限とは同時に設定できません。ユーザーアカウントに API 権限を設定する場合は、API 権限だけを設定してください。

- API 権限を設定したユーザーアカウントでは JP1/IT Desktop Management 2 の操作画面にログインできません。
- API 権限を設定したユーザーアカウントにはメール通知ができません。
- API 権限を設定したユーザーアカウントのパスワードは、ユーザーアカウント管理権限を持つ管理者が変更してください。
- API 権限を設定したユーザーアカウントがロックされた場合は、ユーザーアカウント管理権限を持つ管理者がロックを解除してください。

2.3.4 ユーザーアカウントの権限ごとの操作範囲

ユーザーアカウントに付与されている権限によって、実行できる操作が異なります。操作画面について、業務分掌および管轄範囲を限定していない場合の、権限ごとの操作範囲を次の表に示します。

<table>
<tr><th colspan="2" rowspan="2">操作画面</th><th colspan="4">権限</th></tr>
<tr><th>システム管理権限</th><th>ユーザーアカウント管理権限</th><th>参照権限</th><th>API 権限</th></tr>
<tr><td colspan="2">［機器の管理を始めましょう］ウィザード</td><td>○</td><td>×</td><td>×</td><td>×</td></tr>
<tr><td colspan="2">ホーム画面</td><td>○</td><td>○ ※</td><td>○ ※</td><td>×</td></tr>
<tr><td colspan="2">セキュリティ画面</td><td rowspan="6">○</td><td rowspan="6">○ ※</td><td rowspan="6">○ ※</td><td rowspan="6">×</td></tr>
<tr><td colspan="2">資産画面</td></tr>
<tr><td colspan="2">機器画面</td></tr>
<tr><td colspan="2">配布（ITDM 互換）画面</td></tr>
<tr><td colspan="2">イベント画面</td></tr>
<tr><td colspan="2">レポート画面</td></tr>
<tr><td rowspan="2">設定画面</td><td>［ユーザー管理］画面</td><td>×</td><td>○</td><td>×</td><td>×</td></tr>
<tr><td>［ユーザー管理］画面以外</td><td>○</td><td>×</td><td>×</td><td>×</td></tr>
<tr><td colspan="2">レポートおよびセキュリティポリシーの印刷</td><td colspan="3">○</td><td>×</td></tr>
<tr><td colspan="2">ヘルプの参照</td><td colspan="3">○</td><td>×</td></tr>
</table>

（凡例）○：操作できる　×：操作できない

注※　権限に応じて実行できない操作があります。

2.3.5　ユーザーアカウントの業務分掌

JP1/IT Desktop Management 2 のユーザーアカウントには、管理者の担当業務に合わせて業務分掌を設定できます。この業務分掌と権限とを組み合わせてユーザーアカウントに設定すれば、管理者の操作範囲をそれぞれの担当業務に応じて限定できます。管理者は自分の担当業務に関係がある情報だけを管理できるため、内部統制を意識した運用を実現できます。

業務分掌には次の 5 種類があります。

セキュリティ管理

セキュリティポリシーの編集と適用、危険レベルに応じた機器へのセキュリティ対策、更新プログラムの管理と適用などの業務に限定された業務分掌です。セキュリティ対策ではソフトウェアや更新プログラムの配布を実施する必要があるため、業務分掌にセキュリティ管理を設定すると、配布管理も自動的に設定されます。

資産管理

組織が保有している機器、ソフトウェアライセンス、契約などの資産情報を管理するための業務に限定された業務分掌です。

機器管理

組織が保有している機器情報の管理、機器のリモートコントロール、インストールソフトウェアの管理などの業務に限定された業務分掌です。

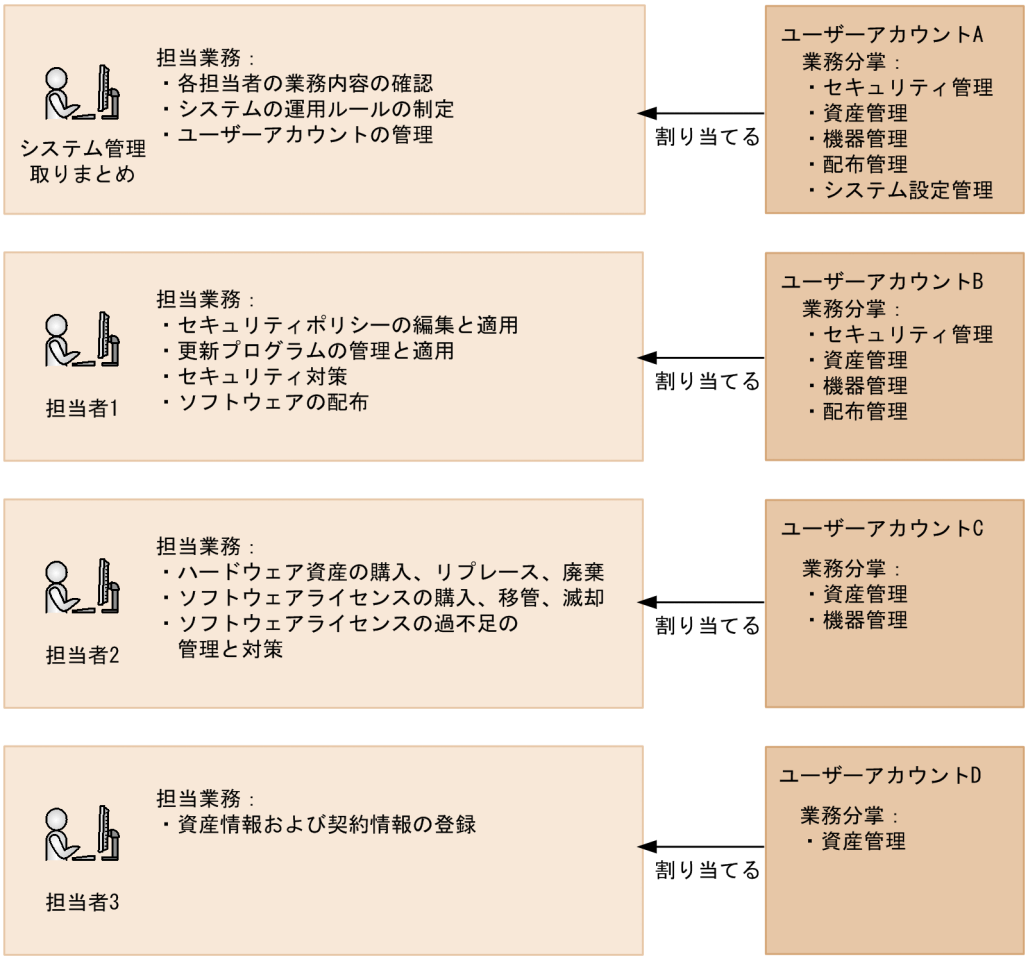
配布管理

ソフトウェアやファイルの配布業務に限定された業務分掌です。セキュリティ管理と組み合わせて設定することで、更新プログラムも配布できます。

システム設定管理

機器の探索の設定、エージェント設定、ネットワーク制御の設定など、JP1/IT Desktop Management 2 の設定情報の管理に限定された業務分掌です。これらの設定情報は JP1/IT Desktop Management 2 の操作に必要な情報のため、業務分掌にシステム設定管理を設定するには、システム管理権限が付与されている必要があります。また、ユーザーアカウントを追加・編集・削除するには、ユーザーアカウント管理権限が付与されている必要があります。

担当業務に合わせてユーザーアカウントに業務分掌を設定して、それぞれの管理者に割り当てる例を、次の図に示します。



システム管理取りまとめ

システム管理全体の取りまとめを実施します。各担当者の業務内容の確認に加えて、システムの運用ルールやユーザーアカウントなど、JP1/IT Desktop Management 2 の設定情報の管理を担当するため、業務分掌にはすべての項目を設定します。

担当者

システム管理の実作業を担当します。業務分掌には、担当業務に必要な項目だけを設定します。

重要

API 権限を設定しているユーザーアカウントには業務分掌を設定できません。

2.3.6 ユーザーアカウントの業務分掌ごとの操作範囲

ユーザーアカウントに業務分掌を設定すると、表示できる画面やメニュー、実行できる操作などの操作範囲を限定できます。操作範囲は、権限と業務分掌の設定の組み合わせで決定します。

重要

業務分掌の操作範囲に含まれる画面またはメニューの中には、ほかの業務分掌に属する項目が一部あります。この場合、その項目が属する業務分掌もユーザーアカウントに設定していないと、画面が表示できなかったり操作が実行できなかったりすることがあります。例えば、資産管理だけを業務分掌に設定している場合、資産画面の［資産一覧］－［資産情報］タブにある［機器一覧へ］ボタンは表示されません。機器一覧画面は、機器管理を業務分掌に設定した場合の操作範囲であるためです。管理者の業務上、機器一覧画面を表示させたいときは、資産管理に加えて機器管理も業務分掌に設定する必要があります。

ヒント

業務分掌に加えて管轄範囲を設定した場合は、業務分掌ごとに限定された操作範囲内で表示される情報が、部門ごとにさらに限定されます。

業務分掌と権限の組み合わせと、それに対応する操作画面の操作範囲を表に示します。

なお、以降の表中では、凡例を次のとおり表記しています。

（凡例） ○：操作できる　△：表示だけできる　×：操作も表示もできない

セキュリティ管理を業務分掌に設定した場合

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
［機器の管理を始めましょう］ウィザード	なし	×	×	×
ホーム画面	なし	○	○	○
セキュリティ画面	サマリ	○	○	○
	セキュリティポリシー	○	△	△
	機器のセキュリティ状態	○※1	△	△
	更新プログラム	○	△	△
	操作ログ	○	△	△
資産画面	全メニュー	×	×	×
機器画面	全メニュー	×	×	×
配布（ITDM 互換）画面	サマリ	○	○	○
	パッケージ	○	△	△
	タスク	○	△	△

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
イベント画面	イベント	○	△	△
レポート画面	サマリ	○※2	○※2	○※2
	ダイジェストレポート	○	○	○
	セキュリティ診断レポート	○	○	○
	セキュリティ詳細レポート	○	○	○
	機器詳細レポート	×	×	×
	資産詳細レポート	×	×	×
設定画面	サマリ	○※3	○※3	×
	ユーザー管理	×	○	×
	エージェント	×	×	×
	機器の探索	×	×	×
	ネットワーク制御	×	×	×
	セキュリティ管理	○	×	×
	資産管理	×	×	×
	機器	×	×	×
	レポート	×	×	×
	イベント	×	×	×
	他システムとの接続	×	×	×
	製品ライセンス	×	×	×

注※1　機器一覧に表示されるグループを編集したい場合は、次の業務分掌が設定されている必要があります。

- 機器種別、ネットワークおよびユーザー定義を編集したい場合：機器管理の業務分掌
- 部署および設置場所を編集したい場合：資産管理の業務分掌

注※2　すべての業務分掌が設定されている場合にだけ、表示または操作できます。

注※3　設定一覧は表示されません。

資産管理を業務分掌に設定した場合

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
[機器の管理を始めましょう] ウィザード	なし	×	×	×
ホーム画面	なし	○	○	○
セキュリティ画面	全メニュー	×	×	×
資産画面	サマリ	○	○	○
	ハードウェア資産	○	△	△
	ソフトウェアライセンス	○	△	△
	管理ソフトウェア	○	△	△
	ソフトウェアライセンス状況	○	△	△
	契約	○	△	△
機器画面	全メニュー	×	×	×
配布（ITDM 互換）画面	全メニュー	×	×	×
イベント画面	イベント	○	△	△
レポート画面	サマリ	○※1	○※1	○※1
	ダイジェストレポート	○	○	○
	セキュリティ診断レポート	×	×	×
	セキュリティ詳細レポート	×	×	×
	機器詳細レポート	×	×	×
	資産詳細レポート	○	○	○
設定画面	サマリ	○※2	○※2	×
	ユーザー管理	×	○	×
	エージェント	×	×	×
	機器の探索	×	×	×
	ネットワーク制御	×	×	×
	セキュリティ管理	×	×	×
	資産管理	○	×	×
	機器	×	×	×
	レポート	×	×	×

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
設定画面	イベント	×	×	×
	他システムとの接続	×	×	×
	製品ライセンス	×	×	×

注※1　すべての業務分掌が設定されている場合にだけ、表示または操作できます。

注※2　設定一覧は表示されません。

機器管理を業務分掌に設定した場合

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
[機器の管理を始めましょう] ウィザード	なし	○	×	×
ホーム画面	なし	○	○	○
セキュリティ画面	全メニュー	×	×	×
資産画面	全メニュー	×	×	×
機器画面	サマリ	○	○	○
	機器情報	○※1	△	△
	変更履歴	○	△	△
	ソフトウェア情報	○	△	△
配布（ITDM 互換）画面	全メニュー	×	×	×
イベント画面	イベント	○	△	△
レポート画面	サマリ	○※2	○※2	○※2
	ダイジェストレポート	○	○	○
	セキュリティ診断レポート	×	×	×
	セキュリティ詳細レポート	×	×	×
	機器詳細レポート	○	○	○
	資産詳細レポート	×	×	×
設定画面	サマリ	○※3	○※3	×
	ユーザー管理	×	○	×

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
設定画面	エージェント	○	×	×
	機器の探索	○	×	×
	ネットワーク制御	×	×	×
	セキュリティ管理	×	×	×
	資産管理	×	×	×
	機器	○	×	×
	レポート	×	×	×
	イベント	×	×	×
	他システムとの接続	×	×	×
	製品ライセンス	×	×	×

注※1　機器一覧に表示されるグループのうち、部署および設置場所を編集したい場合は、資産管理の業務分掌が設定されている必要があります。

注※2　すべての業務分掌が設定されている場合にだけ、表示または操作できます。

注※3　設定一覧は表示されません。

配布管理を業務分掌に設定した場合

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
[機器の管理を始めましょう] ウィザード	なし	×	×	×
ホーム画面	なし	○	○	○
セキュリティ画面	全メニュー	×	×	×
資産画面	全メニュー	×	×	×
機器画面	全メニュー	×	×	×
配布（ITDM 互換）画面	サマリ	○	○	○
	パッケージ	○	△	△
	タスク	○	△	△
イベント画面	イベント	○	△	△
レポート画面	サマリ	○※1	○※1	○※1

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
レポート画面	ダイジェストレポート	○	○	○
	セキュリティ診断レポート	×	×	×
	セキュリティ詳細レポート	×	×	×
	機器詳細レポート	×	×	×
	資産詳細レポート	×	×	×
設定画面	サマリ	×	○※2	×
	ユーザー管理	×	○	×
	エージェント	×	×	×
	機器の探索	×	×	×
	ネットワーク制御	×	×	×
	セキュリティ管理	×	×	×
	資産管理	×	×	×
	機器	×	×	×
	レポート	×	×	×
	イベント	×	×	×
	他システムとの接続	×	×	×
	製品ライセンス	×	×	×

注※1　すべての業務分掌が設定されている場合にだけ、表示または操作できます。

注※2　設定一覧は表示されません。

システム設定管理を業務分掌に設定した場合

操作画面	メニュー	権限	
		システム管理権限	ユーザーアカウント管理権限
[機器の管理を始めましょう]ウィザード	なし	○	×
ホーム画面	なし	○	○
セキュリティ画面	全メニュー	×	×
資産画面	全メニュー	×	×
機器画面	全メニュー	×	×

操作画面	メニュー	権限	
		システム管理権限	ユーザーアカウント管理権限
配布（ITDM 互換）画面	全メニュー	×	×
イベント画面	イベント	○	△
レポート画面	サマリ	○※1	○※1
	ダイジェストレポート	○	○
	セキュリティ診断レポート	×	×
	セキュリティ詳細レポート	×	×
	機器詳細レポート	×	×
	資産詳細レポート	×	×
設定画面	サマリ	○	○※2
	ユーザー管理	×	○
	エージェント	○	×
	機器の探索	○	×
	ネットワーク制御	○	×
	セキュリティ管理	○	×
	資産管理	○	×
	機器	○	×
	レポート	○	×
	イベント	○	×
	他システムとの接続	○	×
	製品ライセンス	○	×

注※1　すべての業務分掌が設定されている場合にだけ、表示または操作できます。

注※2　設定一覧は表示されません。

業務分掌に何も設定しなかった場合

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
［機器の管理を始めましょう］ウィザード	なし	×	×	×
ホーム画面	なし	○	○	○

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
セキュリティ画面	全メニュー	×	×	×
資産画面	全メニュー	×	×	×
機器画面	全メニュー	×	×	×
配布（ITDM 互換）画面	全メニュー	×	×	×
イベント画面	イベント	○	△	△
レポート画面	サマリ	×	×	×
	ダイジェストレポート	○	○	○
	セキュリティ診断レポート	×	×	×
	セキュリティ詳細レポート	×	×	×
	機器詳細レポート	×	×	×
	資産詳細レポート	×	×	×
設定画面	サマリ	×	○※	×
	ユーザー管理	×	○	×
	エージェント	×	×	×
	機器の探索	×	×	×
	ネットワーク制御	×	×	×
	セキュリティ管理	×	×	×
	資産管理	×	×	×
	機器	×	×	×
	レポート	×	×	×
	イベント	×	×	×
	他システムとの接続	×	×	×
	製品ライセンス	×	×	×

注※　設定一覧は表示されません。

複数の業務分掌を設定した場合

複数の業務分掌を設定した場合は、各業務分掌の操作範囲を合わせた範囲が適用されます。資産管理および機器管理を業務分掌に設定した場合を例に、適用される操作範囲を次の表に示します。

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
[機器の管理を始めましょう] ウィザード	なし	○	×	×
ホーム画面	なし	○	○	○
セキュリティ画面	全メニュー	×	×	×
資産画面	サマリ	○	○	○
	ハードウェア資産	○	△	△
	ソフトウェアライセンス	○	△	△
	管理ソフトウェア	○	△	△
	ソフトウェアライセンス状況	○	△	△
	契約	○	△	△
機器画面	サマリ	○	○	○
	機器情報	○	△	△
	変更履歴	○	△	△
	ソフトウェア情報	○	△	△
配布（ITDM 互換）画面	全メニュー	×	×	×
イベント画面	イベント	○	△	△
レポート画面	サマリ	×	×	×
	ダイジェストレポート	○	○	○
	セキュリティ診断レポート	×	×	×
	セキュリティ詳細レポート	×	×	×
	機器詳細レポート	○	○	○
	資産詳細レポート	○	○	○
設定画面	サマリ	○※	○※	×
	ユーザー管理	×	○	×
	機器の探索	○	×	×
	エージェント	○	×	×
	ネットワーク制御	×	×	×
	セキュリティ管理	×	×	×
	資産管理	○	×	×

操作画面	メニュー	権限		
		システム管理権限	ユーザーアカウント管理権限	参照権限
設定画面	機器	○	×	×
	レポート	×	×	×
	イベント	×	×	×
	他システムとの接続	×	×	×
	製品ライセンス	×	×	×

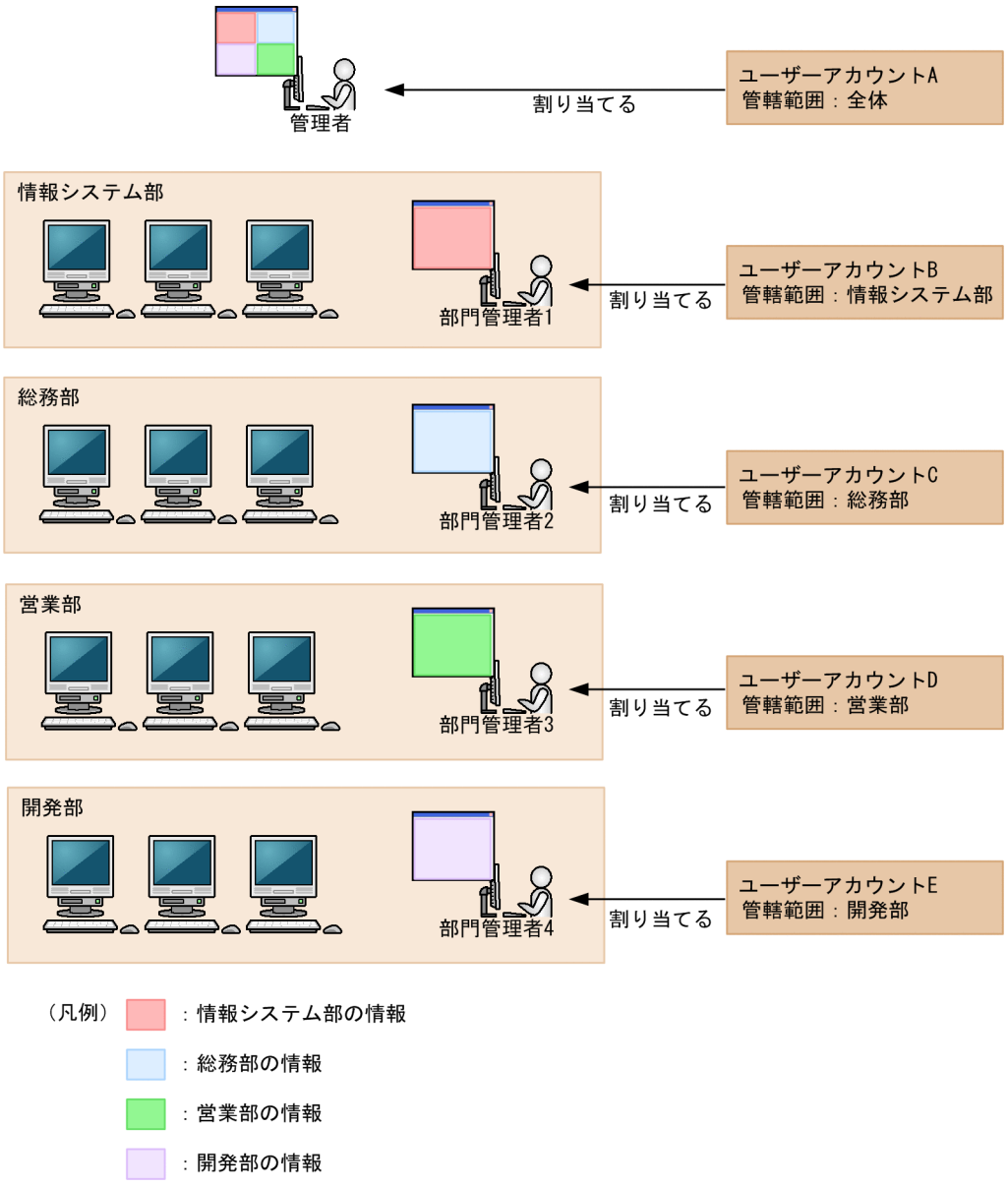
注※　設定一覧は表示されません。

2.3.7　ユーザーアカウントの管轄範囲

JP1/IT Desktop Management 2 のユーザーアカウントには、管理者が担当する部門に合わせて管轄範囲を設定できます。社内全体の機器数が多く、管理者 1 人ではすべての機器の管理が行き届かない場合、部門ごとに管理者を割り当てます。そうすると、部門ごとに割り当てられた管理者は、部門管理者として、部門に限定した機器、ハードウェア資産などを表示して管理できます。

なお、リモートインストールマネージャを使用した配布は、管轄範囲の設定の対象外です。

ユーザーアカウントに管轄範囲を設定してそれぞれの管理者に割り当てる例を、次の図に示します。



管理者

社内全体のシステムを管理します。管轄範囲を限定しないユーザーアカウントを割り当てることで、すべての部門の情報を表示できます。

部門管理者

特定の部門のシステムを管理します。管轄範囲を担当部門に限定したユーザーアカウントを割り当てることで、担当部門の情報だけを表示できます。

重要

API 権限を設定しているユーザーアカウントには管轄範囲を設定できません。

2.3.8　管轄範囲が限定されている場合の操作画面の差異

管轄範囲が限定されているユーザーアカウントでログインすると、その管轄範囲内の情報だけが表示され、実行できる操作を制限できます。管轄範囲が限定されている場合の操作画面の差異を次の表に示します。

操作画面		管轄範囲が限定されている場合の差異
ホーム画面	ホーム画面	次の項目は表示されません。 • ［ようこそ！］のメッセージ • ［始めましょう］ボタン • ［実行］メニューの［機器管理を始めましょう］
	［システムサマリ］パネル	［使用中のライセンス］の表示がリンクではなくなります。
	［イベントの状況］パネル	管轄範囲内の情報だけが表示されます。
	［通知事項］パネル	一部のメッセージの表示がリンクではなくなります。また、一部のメッセージが管轄範囲内の情報に限定されて表示されます。
	［監視候補の処理］パネル	次の表示がリンクではなくなります。 • エラー • ネットワークの探索 • Active Directory の探索
	［データベースとディスクの状況］パネル	－
	［危険レベルごとの機器台数］パネル	管轄範囲内の情報だけが表示されます。
	［ポリシーごとのセキュリティ状況］パネル	－
	［不審操作の状況］パネル	管轄範囲内の情報だけが表示されます。
	［観点ごとの機器台数］パネル	管轄範囲内の情報だけが表示されます。
	［観点ごとのハードウェア資産台数］パネル	管轄範囲内の情報だけが表示されます。
	［カテゴリごとのセキュリティ評価］パネル	管轄範囲内の情報だけが表示されます。
	［ハードウェア資産の推移］パネル	－
	［3 か月以内に期限が切れる契約］パネル	管轄範囲内の情報だけが表示されます。
	［超過したソフトウェアライセンス］パネル	管轄範囲内の情報だけが表示されます。
	［OS ごとの機器台数］パネル	管轄範囲内の情報だけが表示されます。
	［管理対象の機器の推移］パネル	－

操作画面		管轄範囲が限定されている場合の差異
ホーム画面	［新規発見ソフトウェア］パネル	－
	［タスクの状況］パネル	－
	［エラータスクの状況］パネル	管轄範囲内の情報だけが表示されます。
	［配下の階層構成および稼働状態］パネル※1	次の項目は表示されません。 • ［操作メニュー］の［稼働状態の判定方法を変更する］ • 管理用中継サーバのアイコンを右クリックして表示されるメニューの［管理用中継サーバを削除する］
セキュリティ画面	［サマリ］画面※2	パネルによって表示範囲が異なります。
	［セキュリティポリシー］画面	情報の参照だけできます。 インフォメーションエリア下部の各タブでは、管轄範囲が限定されていない場合と同様の操作ができます。
	［機器のセキュリティ状態］画面	管轄範囲内の情報だけが表示されます。 ［操作メニュー］の次の項目は表示されません。 • ［ポリシーを割り当てる］ • ［ポリシーの割り当てを解除する］ • ［ネットワークモニタを有効にする］ • ［ネットワークモニタを無効にする］ ネットワークモニタが無効であることを示すメッセージが、メッセージバーに表示されません。
	［更新プログラム］画面	情報の参照だけできます。 ［操作メニュー］の［サポートサービスからの情報をオフライン更新する］は表示されません。
	［操作ログ］画面	管轄範囲内の情報だけが表示されます。
資産画面	［サマリ］画面※2	パネルによって表示範囲が異なります。
	［ハードウェア資産］画面	管轄範囲内の情報だけが表示されます。 ［操作メニュー］の［［利用者情報の入力］画面を定期的に表示させる］は表示されません。 ハードウェア資産情報を追加・編集するダイアログで、管理項目の左側に表示されるアイコンが表示されません。 各ダイアログで、選択項目を新規追加できません。
	［ソフトウェアライセンス］画面	管轄範囲内の情報だけが表示されます。 ［割り当てコンピュータ］タブには、管轄範囲外の情報も表示されます。管轄範囲外の情報が表示されると、部署の情報が変更された場合に、変更前の部署で不要になったソフトウェアライセンスの割り当てを解除できます。 ソフトウェアライセンス情報を追加・編集するダイアログで、管理項目の左側に表示されるアイコンが表示されません。

操作画面		管轄範囲が限定されている場合の差異
資産画面	［ソフトウェアライセンス］画面	各ダイアログで、［管理ソフトウェア名］以外の選択項目は新規追加できません。
	［管理ソフトウェア］画面	［操作メニュー］の［サポートサービスからの情報をオフライン更新する］は表示されません。 ［インストールソフトウェア］タブの［禁止ソフトウェアへ追加］ボタンは表示されません。
	［ソフトウェアライセンス状況］画面	管轄範囲内の情報だけが表示されます。
	［契約］画面	管轄範囲内の情報だけが表示されます。 契約情報を追加・編集するダイアログで、管理項目の左側に表示されるアイコンが表示されません。 各ダイアログで、選択項目を新規追加できません。
機器画面	［サマリ］画面※2	パネルによって表示範囲が異なります。
	［機器情報］画面	管轄範囲内の情報だけが表示されます。 ［操作メニュー］の次の項目は表示されません。 • ［［利用者情報の入力］画面を定期的に表示させる］ • ［ネットワークモニタを有効にする］ • ［ネットワークモニタを無効にする］ • ［認証情報を設定する］ • ［上位の管理用サーバにすべての機器情報を通知する］※3 ネットワークモニタが無効であることを示すメッセージが、メッセージバーに表示されません。 機器情報を編集するダイアログで、管理項目の左側に表示されるアイコンが表示されません。また、各選択項目を新規追加できません。
	［変更履歴］画面	管轄範囲内の情報だけが表示されます。
	［ソフトウェア情報］画面	［操作メニュー］の［ソフトウェアの削除］、および［サポートサービスからの情報をオフライン更新する］は表示されません。 ［インストールソフトウェア］タブの［禁止ソフトウェアへ追加］ボタンは表示されません。
配布（ITDM 互換）画面	［サマリ］画面※2	パネルによって表示範囲が異なります。
	［パッケージ］画面	－
	［タスク］画面	－
イベント画面		発生元に機器情報または資産情報が表示されるイベントは管轄範囲内の情報だけが表示されます。 一部のメッセージの表示がリンクではなくなります。
レポート画面	［サマリ］画面	－

操作画面		管轄範囲が限定されている場合の差異
レポート画面	ダイジェストレポート	−
	セキュリティ診断レポート	レポートの集計範囲が、管轄範囲内に限定されます。
	セキュリティ詳細レポート	次に示すレポートの集計範囲が、管轄範囲内に限定されます。 • ［危険レベルの状況］レポート • ［更新プログラムの適用状況］レポート • ［ウィルス対策製品の状況］レポート • ［使用必須ソフトウェアのインストール状況］レポート • ［使用禁止ソフトウェアのインストール状況］レポート • ［セキュリティ設定の状況］レポート
	機器詳細レポート	レポートの集計範囲が、管轄範囲内に限定されます。
	資産詳細レポート	レポートの集計範囲が、管轄範囲内に限定されます。
設定画面	［サマリ］画面	［サイトマップ］画面だけが表示されます。
	［ユーザー管理］画面	−
	［エージェント］画面	［Windows エージェント設定とインストールセットの作成］画面は、情報の参照だけできます。 ［Windows エージェント設定の割り当て］画面は、管轄範囲内の情報だけが表示されます。また、インフォメーションエリアの上部にある［対象の構成を変更］ボタンは非表示に、［割り当て］ボタン、および［割り当てを解除］ボタンは非活性になります。 ［Windows エージェントの配信］画面は、管轄範囲内の情報だけが表示されます。また、［配信するエージェントのコンポーネントの設定］の［編集］ボタンが表示されません。 ［エージェントレス管理の設定］画面は表示されません。
	［機器の探索］画面	次の画面だけ表示できます。各画面は、管轄範囲内の情報だけが表示されます。 • ［発見した機器］画面 • ［管理対象機器］画面 • ［除外対象機器］画面 また、［発見した機器］画面および［管理対象機器］画面では、［操作メニュー］の［認証情報を設定する］、および［探索を開始する］は表示されません。
	［ネットワーク制御］画面	表示されません。
	［セキュリティ管理］画面	表示されません。
	［資産管理］画面	［インポート履歴の確認］画面と［削除機器関連ハードウェア資産の資産状態の設定］画面だけ表示できます。

操作画面		管轄範囲が限定されている場合の差異
設定画面	［資産管理］画面	［削除機器関連ハードウェア資産の資産状態の設定］画面は、情報の参照だけできます。
	［機器］画面	［機器メンテナンスの設定と検出結果確認］画面だけ表示されます。 ［機器メンテナンスの検出条件］は情報の参照だけできます。 ［機器メンテナンスの抑止設定］および［削除候補の機器一覧］は、管轄範囲内の情報だけが表示されます。
	［レポート］画面	表示されません。
	［イベント］画面	表示されません。
	［他システムとの接続］画面	表示されません。
	［製品ライセンス］画面	表示されません。

（凡例）－：管轄範囲が限定されていない場合と差異はありません。

注※1　複数サーバ構成の場合に表示されるパネルです。

注※2　［サマリ］画面に表示されるパネルは、ホーム画面と共通です。

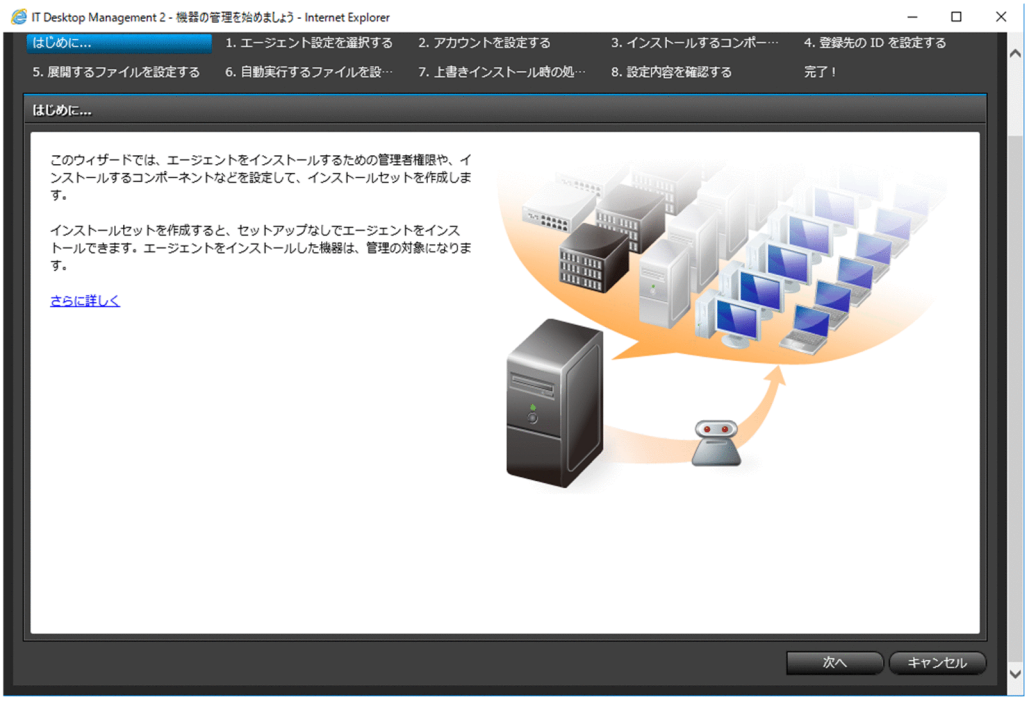
注※3　管理用中継サーバの場合に表示されるメニューです。

ヒント

管轄範囲が限定されているユーザーアカウントでログインした場合、各画面のメニューエリアなどに表示される部署の情報（管理項目の［部署］）は編集できません。

2.4　運用準備の支援

JP1/IT Desktop Management 2 にログインすると、ホーム画面の［始めましょう］ボタンから［機器の管理を始めましょう］ウィザードを起動できます。このウィザードから、JP1/IT Desktop Management 2 で運用を開始するための準備ができます。



ウィザードのガイドに沿って操作を進めることで、コンピュータにエージェントをインストールするためのインストーラーファイル（インストールセット）を作成できます。このファイルを各コンピュータで実行することで、エージェントをインストールできます。詳細については、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の、エージェントを手動でインストールする方法の説明を参照してください。

コンピュータにエージェントをインストールするには、Active Directory を探索する方法と、ネットワークを探索する方法もあります。

2.4.1　機器の探索

管理用サーバごとに、管理対象のネットワークに接続された機器や Active Directory に登録された機器を探索できます。

ネットワークの探索

IP アドレスで指定した範囲のネットワークを探索できます。また、探索時に使用する認証情報を設定できます。これによって、探索時に対象の機器から情報を取得します。

組織内の機器を把握できていない場合に、探索を実行することで機器を確認できるようになります。また、この結果を基に、エージェントの導入計画を立てることもできます。

Active Directory の探索

Active Directory を利用している場合、Active Directory に登録されているコンピュータを探索できます。複数の Active Directory を探索することもできます。探索では、Active Directory に登録されている情報を取得します。

Active Directory で管理している情報を JP1/IT Desktop Management 2 に登録することで、機器管理やレポートなどの機能を利用できるようになります。

探索時には、発見した機器を自動的に管理対象にしたり、発見したコンピュータにエージェントを自動的に配信したりできます。また、新規に機器を発見した場合、探索が完了したときに管理者にメールで通知できます。

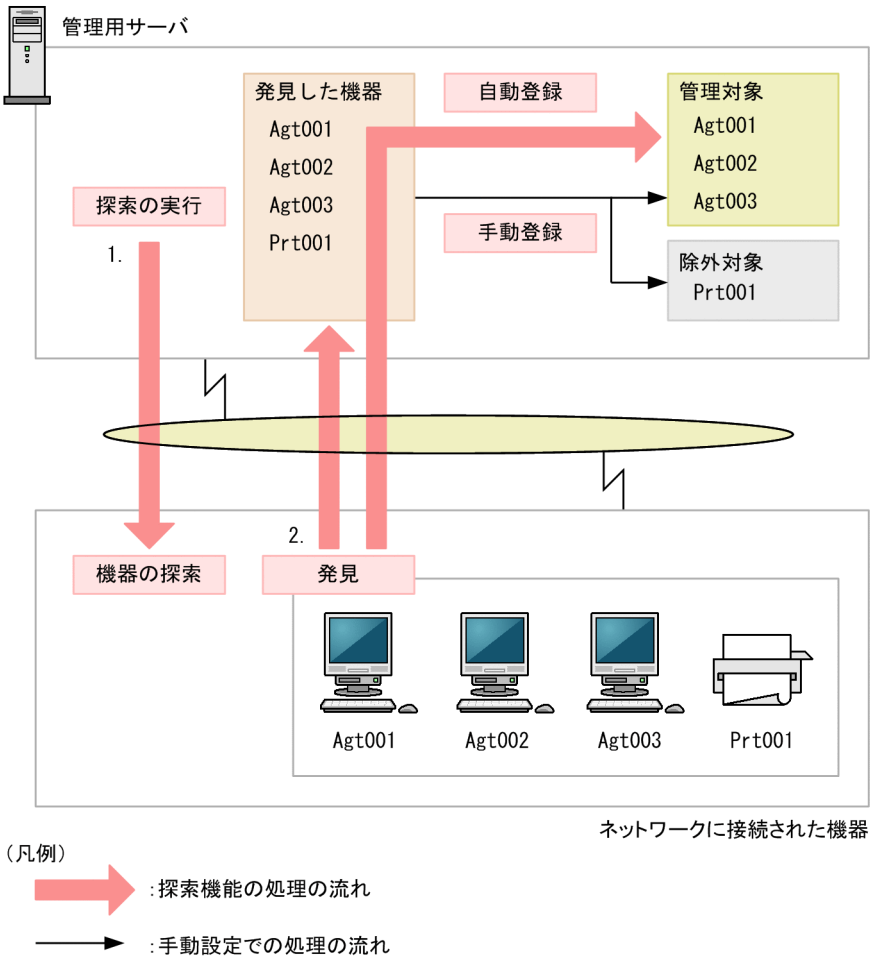
2.4.2 ネットワークに接続されている機器を探索する流れ

ネットワークに接続された機器を探索して、JP1/IT Desktop Management 2 の管理対象に登録できます。

指定した範囲のネットワークに対して探索を実行すると、機器を発見できます。発見された機器のうち、セキュリティ管理したいコンピュータなどの機器を管理対象に、セキュリティ管理の対象外としたいルータなどの機器は除外対象に登録します。

なお、探索で発見した機器に対して自動的に管理対象にしたり、エージェントを自動的に配信したりできます。また、新規に機器を発見した場合、探索が完了したときに管理者にメールで通知できます。

機器を探索して管理対象に登録する流れを次の図に示します。



1. 管理用サーバで、探索するネットワークの範囲、スケジュールなどを設定して定期的に機器の探索を実行します。

> **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。

> **ヒント**
>
> 管理用サーバは、探索対象の機器のうち最大 10 台に同時に接続して機器を探索します。

2. 探索によって発見された機器は、自動的に管理対象に登録したり、いったん「発見した機器」として登録したあとで、手動で管理対象または除外対象に登録したりできます。

関連リンク

- (1)　管理対象にできる機器の種類

- (1)　収集できる機器情報の種類
- (2)　機器の状態として収集できる情報
- (3)　システム情報として収集できる情報
- (4)　ハードウェア情報
- (5)　インストールソフトウェア情報
- (6)　セキュリティ情報
- (7)　資産情報と機器情報の共通管理項目
- (1)　探索の条件
- 付録 A.3　ポート番号一覧

(1)　探索の条件

機器を探索するためには、幾つかの条件を満たしている必要があります。探索の条件は、探索方法によって変わります。

Active Directory の探索

設定画面の［他システムとの接続］－［Active Directory の設定］画面で、接続する Active Directory が正しく設定されている必要があります。

ネットワークの探索

次の条件を満たしている必要があります。

- 探索する機器が管理用サーバと同じセグメントにある場合、管理用サーバからの ARP に応答できる
- 探索する機器が管理用サーバと異なるセグメントにある場合、管理用サーバからの ICMP ECHO（ping）に応答できる
- 探索する機器に IP アドレスが割り当てられている
- 探索範囲が正しく設定されている
- 認証情報が正しく設定されている

探索範囲および認証情報は、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］画面で設定できます。

また、機器を探索して発見するためのネットワーク環境の前提条件を次に示します。

- TCP/IP 通信ができ、使用ポートを通過できる環境（ファイアウォール設定など）である。
- 管理用サーバと管理対象の機器が ICMP 通信などで相互に参照できる。

> **重要**
>
> 仮想マシンは、独立したコンピュータとして発見されます。なお、仮想マシンを探索するためには、ゲスト OS にホスト OS と別の IP アドレスおよび MAC アドレスを割り当てる必要があります。

重要

NAT 環境では、エージェントレスの機器は管理できません。

重要

OS が Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、Windows Server 2008、Windows Vista、Windows Server 2003（Service Pack 2 以降）、または Windows XP（Service Pack 2 以降）のコンピュータの場合、デフォルトでは Windows ファイアウォールの設定によって ICMP を利用できません。ICMP を利用して発見するには、探索対象のコンピュータの設定を、ICMP が利用できるように変更する必要があります。

重要

ループバックアドレスまたはブロードキャストアドレスは、探索範囲から除外してください。ループバックアドレスまたはブロードキャストアドレスが探索範囲に含まれた状態でネットワークの探索を実施すると、機器が誤って発見されることがあります。

ヒント

ネットワーク環境の前提条件を満たしていれば、無線 LAN、WAN、または VPN を利用している機器も探索できます。

なお、探索で発見したコンピュータの OS が Windows の場合、エージェントを自動的に配信して管理対象にできます。エージェントを配信するための条件については、「2.5.2　オンライン管理のコンピュータにエージェントを配信するための条件」を参照してください。

(2)　ネットワークの探索時のデータ転送量の目安

ネットワークの探索時のデータ転送量の目安を次に示します。

SNMP 認証を利用する場合

SNMP 認証に成功した場合は、機器 1 台当たり約 2 キロバイトのデータがコンピュータに転送されます。

Windows の管理共有の認証を利用する場合

Windows の管理共有の認証に成功した場合は、機器 1 台当たり約 2.5 メガバイトのデータがコンピュータに転送されます。なお、エージェントを配信する場合は、約 80 メガバイトのデータ転送量になります。データ転送量は、エージェント設定に応じて増減します。

2.4.3　Active Directory との連携

Active Directory と連携すると、Active Directory で管理している機器を JP1/IT Desktop Management 2 に登録したり、各機器の情報を取得したりできます。ユーザー名、電話番号、メールアドレスなどの JP1/IT Desktop Management 2 では自動収集できない情報も取得できます。

また、「部署」と「設置場所」の情報を Active Directory から取得することで、Active Directory で管理している組織単位（OU）と JP1/IT Desktop Management 2 で管理している機器と資産情報のグループ構成を同期できます。

取得できる機器情報

Active Directory と連携すると、次の表に示すような機能が利用できます。

機能	説明
機器の登録	Active Directory で管理されているコンピュータを発見し、JP1/IT Desktop Management 2 の管理対象として登録できます。また、システム情報を Active Directory 上の情報で更新できます。
情報の取り込み	機器情報とハードウェア資産情報の共通管理項目、およびハードウェア資産情報の追加管理項目の情報を Active Directory で管理されている情報から取り込めます。項目の取得方法を「Active Directory から取得」に設定する必要があります。
組織階層の取り込み	Active Directory で管理している組織単位（OU）の階層を JP1/IT Desktop Management 2 のグループ構成に取り込めます。

Active Directory から取得できる機器情報の種別を次の表に示します。

機器情報の種別		Active Directory との連携	
		機器の登録	情報の取り込み
機器種別	PC（Windows）	○	○
	サーバ（Windows）	○	○
システム情報	コンピュータ情報	○	×
	OS 情報	○	×
	ネットワーク情報	○	×
共通管理項目		○	○
追加管理項目		○	○

（凡例）○：取得できる　×：取得できない

取得できる機器情報の詳細については、「(3)　Active Directory から取得できる機器情報」を参照してください。

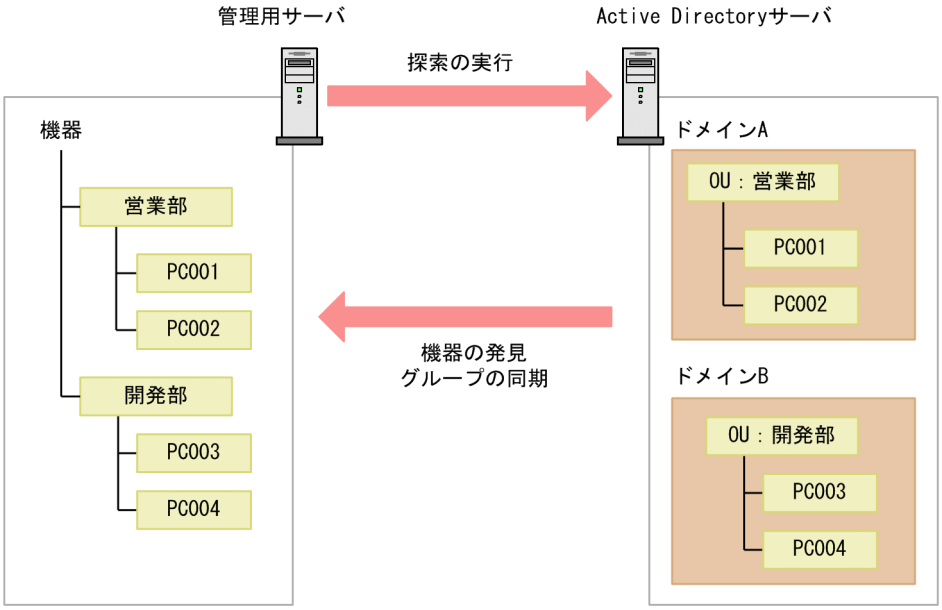
機器情報の取得時刻

Active Directory との連携が設定されている場合、毎日 23:00 に Active Directory の探索が実施されて、機器情報が取得されます。取得時刻や間隔を変更したい場合は、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、探索スケジュールを設定してください。

(1)　Active Directory に登録されている機器の探索

Active Directory のドメインおよびルート OU で管理されているコンピュータを探索して、管理対象に登録できます。すでに Active Directory を利用してコンピュータを管理している場合にお勧めします。

Active Directory を利用した機器の探索の流れを次の図に示します。



機器情報の探索方法

Active Directory に登録されている機器を探索する方法について次に示します。

即時実行

Active Directory に接続して、機器を探索します。発見した機器からは、機器情報が取得されます。初期導入時や Active Directory の情報の変更をすぐに JP1/IT Desktop Management 2 に反映したいときは、この方法をお勧めします。設定画面の［機器の探索］－［探索条件の設定］－［Active Directory の探索］画面で実行できます。

> **ヒント**
>
> 探索を途中で中止した場合は、すでに取得したコンピュータ情報およびグループ情報は、取り込んだ時点の状態になります。

定期実行

Active Directory の探索の設定に従って、機器を定期的に探索します。発見した機器からは、機器情報が取得されます。探索スケジュールは、設定画面で［開始時刻］、［繰り返し単位］（日、週、月）、［繰り返しの方法］を設定できます。デフォルトは、毎日 23:00 です。

> **ヒント**
>
> サービスの停止やシステムのシャットダウンで探索が実行できなかったり、途中で中止されたりした場合は、次回のサービス起動時に実行されます。
>
> 探索が中止された場合は、次回のサービス起動時にすべてのコンピュータを対象に再度探索が実行されます。複数回探索が実行できなかった場合は、最新の 1 回分だけ探索が実行されます。

探索の実行状況を知りたい場合は、設定画面の［機器の探索］－［探索履歴の確認］を確認してください。なお、機器の探索で「完了通知」を設定しておくと、探索が完了次第、管理者にメールが通知されます。

管理対象の機器の削除

Active Directory 上でコンピュータを削除しても、同期しません。Active Directory から発見されたコンピュータを削除する場合、手動で JP1/IT Desktop Management 2 から削除してください。

探索の競合

Active Directory に登録されている機器を探索する場合、ほかの探索と競合することがあります。

ほかの Active Directory の探索と競合する場合

すでに Active Directory の探索が実行されている場合は、あとから実行した Active Directory の探索は中止されます。中止された探索は、次回のスケジュールの探索で実行されます。

ネットワークの探索と競合する場合

すでにネットワークの探索が実行されている場合でも、Active Directory の探索は実行されます。ネットワークの探索と Active Directory の探索で同一の機器を発見した場合、管理共有、SNMP を使用した探索はネットワークの探索結果が優先され、ARP、ICMP を使用した探索は Active Directory の探索結果が優先されます。

関連リンク

- (4)　Active Directory からの部署のグループ構成の取り込み

(2)　Active Directory を探索する場合の接続先の設定

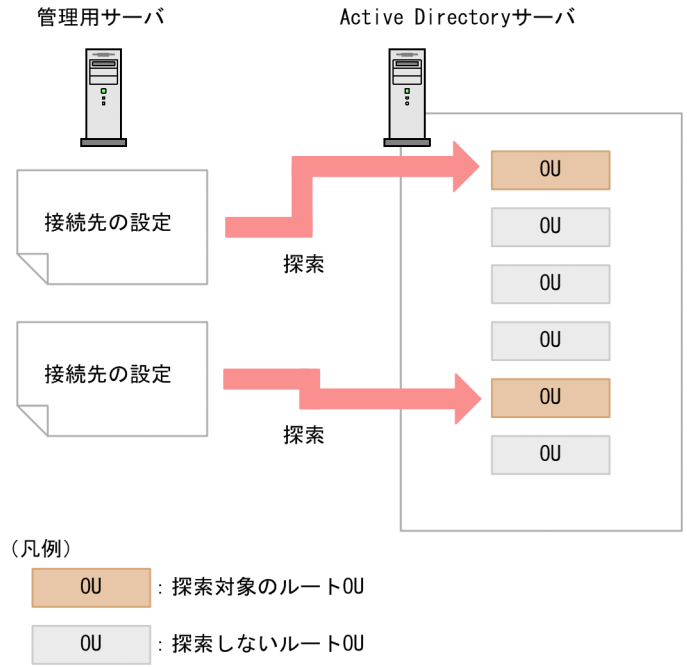
Active Directory を探索して機器を発見するためには、接続先となる Active Directory のサーバおよび探索対象とするドメインのルート OU を設定する必要があります。

接続先は、複数設定できます。接続先の設定には、Active Directory のアドレスとルート OU の組み合わせを設定します。このため、接続先の Active Directory サーバの台数や、探索対象とするルート OU の数に応じて、接続先を設定する必要があります。

Active Directory を探索する場合の接続先の設定例を次に示します。

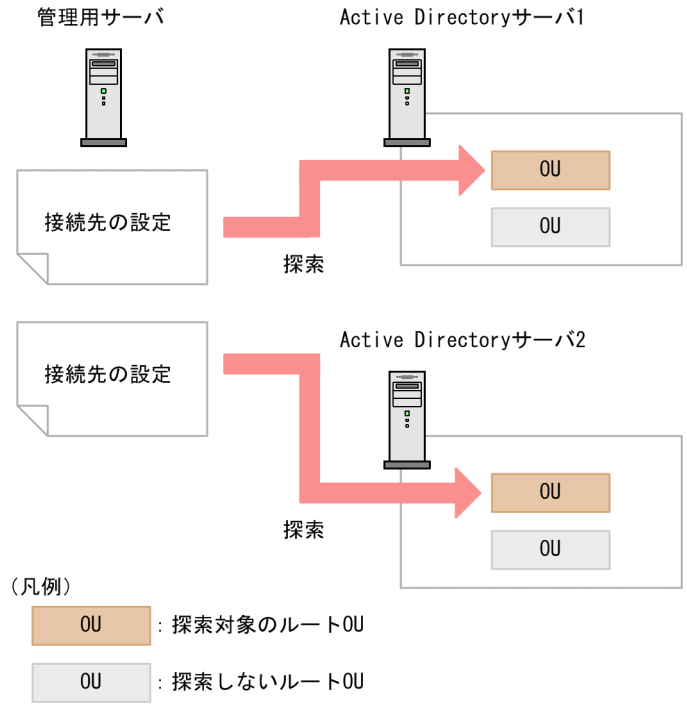
1 台の Active Directory サーバに接続して、複数のルート OU の機器を探索する場合

接続する Active Directory は 1 台ですが、複数のルート OU を探索するので、接続先はルート OU の数だけ設定します。



複数台の Active Directory サーバに接続して機器を探索する場合

探索対象の Active Directory サーバが複数ある場合は、それぞれの Active Directory サーバに対して接続先を設定します。



重要

Active Directory を探索する場合、Active Directory の設定画面で指定したルート OU に属するすべてのオブジェクト、およびオブジェクトが参照するすべてのオブジェクトに、Active Directory の設定画面で指定したユーザー ID に対する読み取り権限を付与してください。読み取り権限が付与されていない場合、Active Directory の探索で、機器の情報やグループの情報が正しく取得できない場合があります。

(3) Active Directory から取得できる機器情報

Active Directory から取得できる機器情報を次の表に示します。

システム情報

機器情報の項目		取得元		内容
		オブジェクト名 (LDAP)	属性名（LDAP）	
機器種別		computer	operatingSystem	OS がクライアント系 OS の場合は、「PC」が設定されます。また、OS がサーバ系 OS の場合は、「サーバ」が設定されます。
コンピュータ情報	コンピュータ名	computer	sAMAccountName	コンピュータの「コンピュータ名」を取得します。
	ホスト名	computer	dNSHostName	DNS 名が設定されている場合は、コンピュータの「DNS 名」を取得します。

機器情報の項目		取得元		内容
		オブジェクト名(LDAP)	属性名（LDAP）	
コンピュータ情報	ホスト名	computer	sAMAccountName	DNS 名が設定されていない場合は、コンピュータの「コンピュータ名」を取得します。
OS 情報	OS	computer	operatingSystem	OS の名称を取得します。
	サービスパックまたはバージョン	computer	operatingSystemServicePack	OS のサービスパックまたはバージョンの情報を取得します。
ネットワーク情報	IP アドレス	－	－	DNS でホスト名称から IP アドレスを取得します。
	MAC アドレス	－	－	ARP で IP アドレスから MAC アドレスを取得します。

（凡例）－：Active Directory から機器情報を取得できますが、取得元の Active Directory では表示されません。

また、ほかに次の表に示す情報も取得できます。

機器情報の項目	説明
登録日時	機器情報の新規登録の場合は、発見した日時を取得します。 機器情報の更新の場合は、日時を更新しません。
更新日時	機器情報を更新した場合は、更新日時を取得します。 機器情報を更新しなかった場合は、日時を更新しません。
管理状態	［自動的に管理対象とする］のオプションがチェックされていて、製品ライセンスがある場合は、「管理」が設定されます。 ［自動的に管理対象とする］のオプションがチェックされていて、製品ライセンスがない場合は、「発見」が設定されます。 ［自動的に管理対象とする］のオプションがチェックされていない場合は、「発見」が設定されます。
管理種別	「エージェントレス管理（認証成功）」が設定されます。
接続設定	「不明」が設定されます。
機器状態	「不明」が設定されます。
管理形態	「エージェント未導入」が設定されます。
最終接続確認日時	Active Directory と連携して、機器を発見したときの日時が設定されます。

共通管理項目

共通管理項目	取得元		内容
	オブジェクト名（LDAP）	属性名（LDAP）	
部署	computer	distinguishedName※1	対応する機器が所属している部署が取得されます。
設置場所	computer	location	対応する機器の設置場所が取得されます。
利用者名	ユーザーまたは InetOrgPerson※2	displayname	対応する機器の利用者名が取得されます。
アカウント	ユーザーまたは InetOrgPerson※2	userPrincipalName	対応する機器の利用者のアカウント名が取得されます。
メールアドレス	ユーザーまたは InetOrgPerson※2	mail	対応する機器の利用者のメールアドレスが取得されます。
電話番号	ユーザーまたは InetOrgPerson※2	telephoneNumber	対応する機器の利用者の電話番号が取得されます。

注※1　属性値の組織単位（OU）の値を変換して所属部署に登録します。例えば、属性値が「CN=PC001,OU=2U,OU=設計 1G,OU=設計部,DC=domain,DC=local」の場合は、「設計部/設計 1G/2U」を所属部署に登録します。

注※2　computer オブジェクトの managedBy 属性に結び付いているユーザーまたは InetOrgPerson オブジェクトです。

追加管理項目

Active Directory から取り込んだ情報と追加管理項目の対応づけの方法を次に示します。以降の表中では、凡例を次のとおり表記しています。

（凡例）○：テンプレートあり　×：テンプレートなし

項目指定

製品が提供するテンプレートを利用して、Active Directory 上のオブジェクトの情報を指定する方法です。

（例）コンピュータのコンピュータ名

ユーザー定義

Active Directory 上で管理されているオブジェクト名および LDAP 属性名を、管理者が入力して指定する方法です。

取得できる追加管理項目は、文字列型のオブジェクトとして取得されます。

Active Directory から情報を取得する際に指定できる対象と、取得対象となるオブジェクトの関係を次の表に示します。

指定できる取得対象	対象となるオブジェクト	説明
コンピュータ	コンピュータ	コンピュータ情報を管理するために使用します。
組織単位（OU）	組織単位（OU）	「コンピュータ」、「ユーザー」、およびほかの「組織単位」などが格納されます。部署・設置場所の情報として使用します。また、コンピュータが所属する組織単位（OU）の情報を取得するためにも使用します。
ユーザー	ユーザー	コンピュータの管理者情報を取得するために使用します。
	InetOrgPerson※	ユーザー種別の一種です。コンピュータの管理者情報を取得するために使用します。

注※　Windows 2000 で使用する場合、InetOrgPerson Kit を適用する必要があります。

「コンピュータ」のオブジェクトから取得できる情報を次の表に示します。

項目名	LDAP 属性名	テンプレートの有無
コンピュータ名	sAMAccountName	○
DNS 名	dNSHostName	○
説明	description	○
名前	operatingSystem	×
バージョン	operatingSystemVersion	×
Service Pack	operatingSystemServicePack	×
場所	location	○
名前	managedBy	○
事業所	_※	×
国/地域	_※	×
都道府県	_※	×
市区町村	_※	×
番地	_※	×
電話番号	_※	×
FAX 番号	_※	×
オブジェクトの正規名	distinguishedName	×

注※　「名前」に指定した値と同じ「ユーザー」または「inetOrgPerson」の属性値情報を表示します。これらの情報を取得するための LDAP 属性名については、後述の「ユーザー」のオブジェクトから取得できる情報の表、または「InetOrgPerson」のオブジェクトから取得できる情報の表を参照してください。

「組織単位（OU)」のオブジェクトから取得できる情報を次の表に示します。

プロパティ名	LDAP 属性名	テンプレートの有無
国/地域	co	○
郵便番号	postalCode	×
都道府県	st	×
市区町村	l	×
番地	street	×
説明	description	×
名前	managedBy	○
グループ ポリシー オブジェクトのリンク	gPLink	×

「ユーザー」のオブジェクトから取得できる情報を次の表に示します。

項目名	LDAP 属性名	テンプレートの有無
姓	sn	○
名	givenName	○
イニシャル	initials	○
表示名	displayName	○
説明	description	○
事業所	physicalDeliveryOfficeName	○
電話番号	telephoneNumber	○
電子メール	mail	○
Web ページ	wWWHomePage	○
国/地域	co	○
郵便番号	postalCode	○
都道府県	st	○
市区町村	l	○
私書箱	postOfficeBox	○
番地	streetAddress	○
ユーザーログオン名	userPrincipalName	○
ユーザーログオン名(Windows 2000 以前)	sAMAccountName	×
ログオン先	userWorkstations	×
ユーザープロファイル プロファイルパス	profilePath	×

項目名	LDAP 属性名	テンプレートの有無
ユーザープロファイル ログオンスクリプト	scriptPath	×
ホームフォルダ ローカルパス	homeDirectory	×
ホームフォルダ 接続ドライブ	homeDrive	×
電話番号 自宅	homePhone	○
電話番号 ポケットベル	pager	○
電話番号 携帯電話	mobile	○
電話番号 FAX	facsimileTelephoneNumber	○
電話番号 IP 電話	ipPhone	○
メモ	info	○
会社名	company	○
部署	department	○
役職	title	○
上司 名前	manager	○
直接報告者	directReports	○

「InetOrgPerson」のオブジェクトから取得できる情報を次の表に示します。

項目名	LDAP 属性名	テンプレートの有無
姓	sn	○
名	givenName	○
イニシャル	initials	○
表示名	displayName	○
説明	description	○
事業所	physicalDeliveryOfficeName	○
電話番号	telephoneNumber	○
電子メール	mail	○
Web ページ	wWWHomePage	○
国/地域	co	○
郵便番号	postalCode	○
都道府県	st	○
市区町村	l	○
私書箱	postOfficeBox	○

項目名	LDAP 属性名	テンプレートの有無
番地	streetAddress	○
ユーザーログオン名	userPrincipalName	○
ユーザーログオン名(Windows 2000 以前)	sAMAccountName	×
ログオン先	userWorkstations	×
ユーザープロファイル プロファイルパス	profilePath	×
ユーザープロファイル ログオンスクリプト	scriptPath	×
ホームフォルダ ローカルパス	homeDirectory	×
ホームフォルダ 接続ドライブ	homeDrive	×
電話番号 自宅	homePhone	○
電話番号 ポケットベル	pager	○
電話番号 携帯電話	mobile	○
電話番号 FAX	facsimileTelephoneNumber	○
電話番号 IP 電話	ipPhone	○
メモ	info	○
会社名	company	○
部署	department	○
役職	title	○
上司 名前	manager	○
直接報告者	directReports	○

重要

これらの表に記載していない項目も属性を指定すれば取得できますが、動作は保証されません。

機器情報の詳細については、次を参照してください。

- (1)　収集できる機器情報の種類
- (2)　機器の状態として収集できる情報
- (3)　システム情報として収集できる情報
- (4)　ハードウェア情報
- (5)　インストールソフトウェア情報
- (6)　セキュリティ情報
- (7)　資産情報と機器情報の共通管理項目

(4) Active Directory からの部署のグループ構成の取り込み

Active Directory の組織単位（OU）を取り込むことで、JP1/IT Desktop Management 2 の部署のグループ構成と同期できます。Active Directory で管理している部署のグループ構成をメンテナンスすることで、管理対象の機器の構成を一元で管理できます。

Active Directory からの組織単位（OU）の取り込みは、機器の探索と同じ契機で行われます。

Active Directory で、取り込みたい組織単位（ルート OU）を指定すると、配下の組織単位（OU）のグループ構成が、部署のグループの直下に自動的に作成されます。Active Directory から部署のグループ構成を取り込む場合は、設定画面の［他システムとの接続］－［Active Directory の設定］画面で［Active Directory の組織の情報を取得して、部署の情報に反映する］をチェックしてください。チェックすると、Active Directory の探索を行ったときに、部署のグループ構成も取り込めます。なお、Active Directory の探索方法については、「(1) Active Directory に登録されている機器の探索」を参照してください。

Active Directory の組織単位（OU）と JP1/IT Desktop Management 2 の部署のグループ構成の取り込み規則を次の表に示します。

Active Directory の組織単位（OU）	JP1/IT Desktop Management 2 の部署のグループ構成	
	存在する	存在しない
存在する	名称が異なる場合はグループ名を更新する。	グループを追加する。
存在しない	グループを削除する。	何もしない。

なお、JP1/IT Desktop Management 2 の部署のグループ構成を変更しても、Active Directory の組織単位（OU）は変更されません。

重要

組織単位（OU）の取り込みを行っている場合は、Active Directory と同期している部署のグループ構成を、手動で追加、変更、および削除しないでください。手動で編集した場合は、次回の組織単位（OU）の取り込みで情報が上書きされます。

Active Directory と同期しているグループに管理対象の機器が関連づけられている場合は、Active Directory の組織単位（OU）にあわせて、所属するグループが変更されます。今まで所属していたグループが削除された場合は、対象の機器は「不明」のグループに所属されます。

ヒント

取り込み先の「ドメイン名」に、上位のドメインとその下位のドメインを同時に指定した場合は、下位のドメインを含めて、上位のドメインの組織単位（OU）が取り込まれます。

(5) Active Directory 連携時の注意事項

Active Directory と連携する場合の注意事項を次に示します。

- 情報の取得先に指定した組織単位（OU）にコンピュータが含まれていない場合、情報は取得できません。
- Active Directory にコンピュータが登録されていても、そのコンピュータが JP1/IT Desktop Management 2 の管理対象になっていない場合は、機器情報は取得されません。
- Active Directory から取得できる情報は文字列型の情報だけになります。
- Active Directory 上の組織単位（OU）の名称に、一部の半角記号およびタブ文字は使用できません。※

注※ 「!」、「"」、「%」、「'」、「*」、「/」、「:」（コロン）、「<」、「>」、「?」、「@」、「¥」、「|」、「+」、「=」、「,」（コンマ）、「;」（セミコロン）は使用しないでください。これらの文字を Active Directory の組織単位（OU）の名称に使用している場合は、連携機能が正しく動作しないおそれがあります。

2.5 エージェントの導入

JP1/IT Desktop Management 2 でコンピュータを管理する場合、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ます。エージェントを導入することで、操作画面からコンピュータの状況を把握したり、動作を制御したりするなど、JP1/IT Desktop Management 2 のすべての機能を利用して効率良く管理できます。

エージェントを導入してコンピュータを管理する方法には、オンライン管理とオフライン管理の 2 つがあります。

> **ヒント**
>
> エージェントを導入しなくても（エージェントレスでも）コンピュータを管理できますが、セキュリティの自動対策やメッセージの通知機能、ソフトウェアやファイルの配布など、一部の機能が利用できません。なお、コンピュータ以外の機器は、エージェントレスで管理します。

コンピュータにエージェントを導入するには、次の方法があります。

オンライン管理の場合

- 管理者がインストールする方法

  次の 2 つの方法があります。

  - 管理用サーバからプログラムを配信して利用者のコンピュータに自動的にインストールする方法
  - 管理者がインストールセット（エージェントのプログラムおよびセットアップ情報を含んだインストーラーファイル）を作成し、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方法

    利用者が Windows にログオンすると、自動的にエージェントがインストールされます。
- 利用者がインストールする方法

  管理者がインストールセットを作成し利用者へ展開します。そのあと、利用者がインストールセットを実行することでインストールする方法です。

オフライン管理の場合

- 管理者がインストールセットを作成し、コンピュータにインストールする方法
- 管理者がインストールセットを作成し、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方法

  利用者が Windows にログオンすると、自動的にエージェントがインストールされます。
- 管理者が提供媒体からコンピュータにエージェントをインストールしたあと、エージェントをセットアップする方法

ヒント

エージェントを導入するとコンピュータが自動的に管理対象になるため、1 台につき製品ライセンスを 1 つ使います。

ヒント

OS が UNIX または Mac OS のコンピュータに対しては、管理用サーバからの配信やインストールセットの利用によって、エージェントを導入することはできません。OS が UNIX のコンピュータへのエージェントの導入については、マニュアル「JP1/IT Desktop Management 2 - Agent(UNIX(R)用) 」を参照してください。OS が Mac OS のコンピュータへのエージェントの導入については、取扱説明書「Mac OS エージェント機能」を参照してください。

2.5.1 オンライン管理のコンピュータへのエージェントの配信

管理用サーバごとに、コンピュータにエージェントを配信してインストールできます。

エージェントの配信方法には次の 2 つがあります。

- 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。

エージェントを配信するための詳細な条件については、「2.5.2 オンライン管理のコンピュータにエージェントを配信するための条件」を参照してください。

ヒント

OS が UNIX または Mac OS のコンピュータに対しては、管理用サーバからの配信によってエージェントを導入することはできません。Windows のコンピュータと UNIX または Mac OS のコンピュータを選択して配信操作をした場合、UNIX または Mac OS のコンピュータへの配信結果は「配信失敗」になります。

2.5.2　オンライン管理のコンピュータにエージェントを配信するための条件

配信先のコンピュータに必要な OS の設定の条件は、エージェントレス管理で Windows の管理共有を利用する場合の条件と同じです。条件については、「4.2.8　エージェントレスで管理するための前提条件」を参照してください。

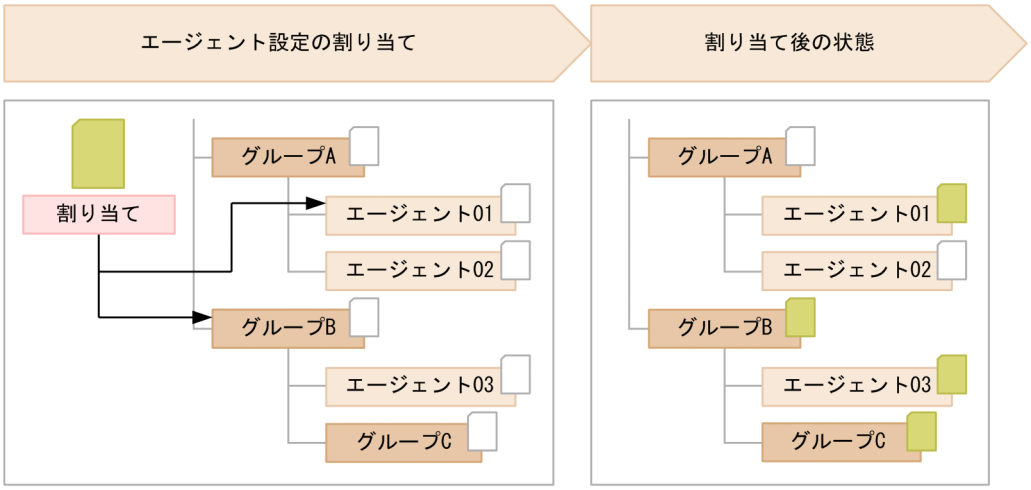
2.5.3　オンライン管理のコンピュータへのエージェント設定の割り当て

エージェントのセットアップ内容は、管理用サーバで設定できるエージェント設定で管理します。エージェント設定の内容を変更すると、そのエージェント設定が割り当てられたすべてのオンライン管理のコンピュータの設定を一括して変更できます。これによって、エージェントのセットアップ内容を効率良く変更できます。エージェント設定は、接続先を自サーバに設定しているエージェントに対してだけ割り当てられます。

エージェント設定は、デフォルトではデフォルトエージェント設定が自動的に割り当てられます。ただし、グループに対してエージェント設定が割り当て済みの場合、新規に管理対象になったオンライン管理のコンピュータが自動的にそのグループに登録されると、グループに対して割り当てられたエージェント設定がデフォルトで適用されます。例えば、OS のグループ「Windows 7 Professional」にエージェント設定「7 用設定」を割り当てておくと、Windows 7 のコンピュータが管理対象になると自動的に「7 用設定」が割り当てられます。

コンピュータ単位またはグループ単位で異なるエージェント設定を適用したい場合は、任意のエージェント設定を作成して、コンピュータまたはグループに割り当てます。ユーザー定義のグループにはエージェント設定を割り当てられません。

エージェント設定をコンピュータに割り当てた場合、対象のコンピュータにエージェント設定が適用されます。エージェント設定をグループに割り当てた場合、そのグループに属するすべてのオンライン管理のコンピュータにエージェント設定が適用されます。エージェント設定の割り当てられ方を次の図に示します。



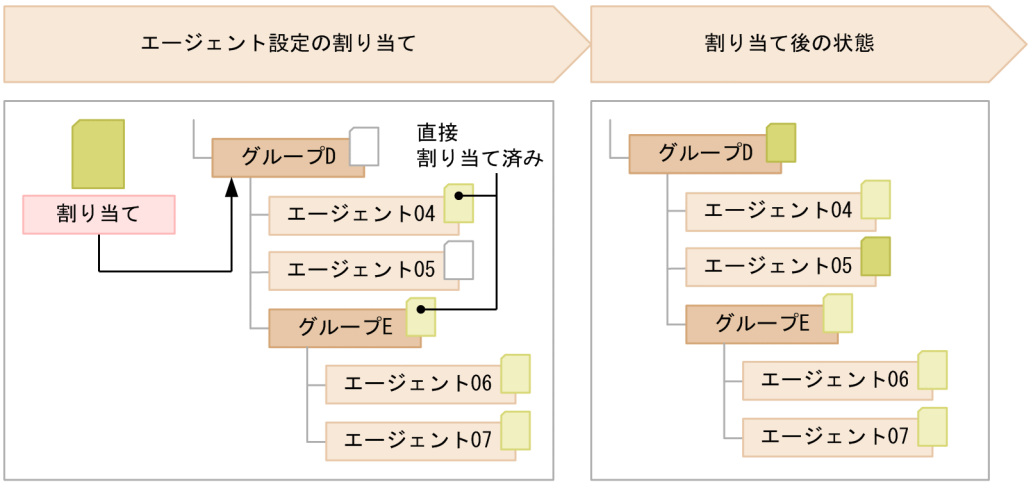
（凡例）

：デフォルトエージェント設定

：任意に作成したエージェント設定

注　「エージェント」はオンライン管理のコンピュータを示します。

コンピュータへの割り当てとグループへの割り当てが重複する場合は、コンピュータに割り当てたエージェント設定が適用されます。また、エージェント設定が直接割り当てられているグループは、上位のグループにエージェント設定を割り当てても、そのエージェント設定は適用されません。割り当てが重複する場合にエージェント設定がどのように割り当たるかを次の図に示します。



（凡例）

：デフォルトエージェント設定

：任意に作成したエージェント設定

注　「エージェント」はオンライン管理のコンピュータを示します。

エージェント設定の割り当てを解除すると、上位のグループに割り当てているエージェント設定が適用されます。

なお、複数のネットワークカードを利用している場合など、コンピュータが複数の IP アドレスのグループに登録されてしまうことがあります。コンピュータが複数のグループに登録されている場合、各登録先の

グループに異なるエージェント設定が割り当てられているときは、そのコンピュータにはデフォルトエージェント設定が適用されます。

ヒント

OS が UNIX または Mac OS のコンピュータの場合、エージェント設定を利用できません。OS が UNIX のコンピュータのセットアップについては、マニュアル「JP1/IT Desktop Management 2 - Agent(UNIX(R)用) 」を参照してください。OS が Mac OS のコンピュータのセットアップについては、取扱説明書 050501「Mac OS エージェント機能」を参照してください。

関連リンク

- 2.18.6　複数サーバ構成での管理対象のコンピュータのエージェント設定

2.6 機器の管理

組織内のネットワークには、コンピュータやサーバ、プリンタ、ネットワーク装置など、さまざまな機器が接続されています。組織内の機器の状況を把握し、セキュリティ管理や資産管理を始めるためには、まず組織内の機器を JP1/IT Desktop Management 2 の管理対象にする必要があります。

機器を管理対象にすると、次に示すような便利な機能を利用して効率良く機器の状況を把握できます。

- 機器を台帳のように一覧で把握できる
- 機器の最新情報を自動的に収集して確認できる
- パネルやレポートなどのグラフィカルな画面で、機器の状況を簡単に把握できる

管理対象にできる機器の台数の上限は 50,000 台です。

機器を管理対象にするには、次の方法があります。

コンピュータにエージェントをインストールする

エージェントをインストールしたコンピュータを管理用サーバに接続すると、自動的に管理対象になります。JP1/IT Desktop Management 2 を利用して組織内の機器を管理する場合、すべてのコンピュータにエージェントをインストールすることをお勧めします。

探索で発見された機器を管理対象にする

探索機能を利用して、ネットワークに接続されている機器または Active Directory で管理されている機器を発見できます。発見された機器を発見されたタイミングで自動的に管理対象にしたり、一覧から管理したい機器を選択して手動で管理対象にしたりできます。コンピュータ以外の機器を管理したい場合は、この方法で管理対象にしてください。

> **ヒント**
>
> 組織内の機器を把握できていない場合は、探索することで機器を把握できるようになります。

MDM システムと連携してスマートデバイスの情報を取得する

MDM 連携機能を利用すると、MDM システムからスマートデバイスの情報を取得して、機器（スマートデバイス）を発見できます。発見されたスマートデバイスを発見されたタイミングで自動的に管理対象にしたり、一覧から管理したいスマートデバイスを選択して手動で管理対象にしたりできます。

外部システムから API を使用して通知された機器を管理対象にする

JP1/IT Desktop Management 2 が提供する API を利用して機器を管理対象にできます。外部システムで管理している機器や発見した機器を、API を使用して JP1/IT Desktop Management 2 に取り込んだり、機器の最新情報を API で JP1/IT Desktop Management 2 に登録したりできます。

なお、機器を管理対象にすると、1 台につきライセンスを 1 つ使います。組織内の機器を管理するためには、管理対象にする機器の台数分のライセンスを準備しておく必要があります。

関連リンク

- 2.6.1　発見された機器を管理対象にする
- 3.1　製品ライセンスの概要

2.6.1　発見された機器を管理対象にする

エージェントがインストールされたコンピュータは自動的に管理対象になりますが、探索によって発見された機器は手動で管理対象にする必要があります。

ヒント

探索の設定で、発見されたコンピュータを自動で管理対象にすることもできます。

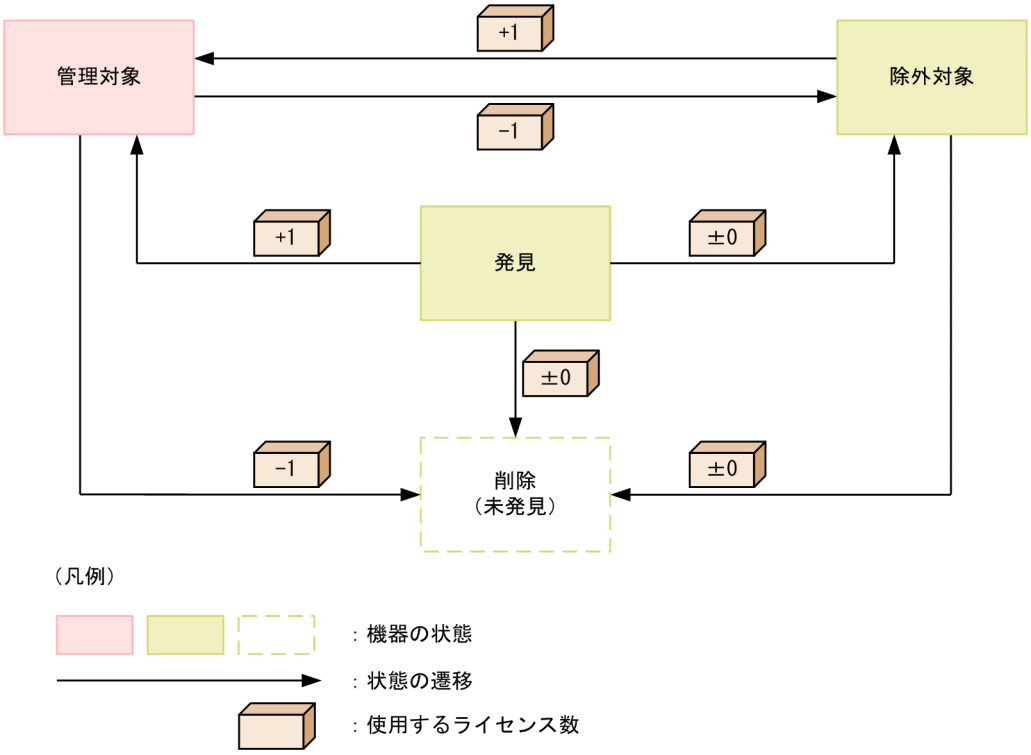
ヒント

機器を探索する時に、ネットワークに接続した未発見機器のコンピュータの電源が OFF の場合は、探索によって機器を発見することはできません。

発見された機器は、管理状態を変更することで管理対象または除外対象にできます。JP1/IT Desktop Management 2 で管理する必要がある機器は管理対象にします。JP1/IT Desktop Management 2 で管理する必要がない機器は、除外対象にします。機器を管理対象にすると、1 台につきライセンスを 1 つ使います。管理対象の機器を除外対象にすると、使用しているライセンス数が 1 つ減ります。

複数サーバ構成の場合、管理状態を変更できるのは、自サーバが発見した機器だけです。なお、機器の管理状態が変更されると、上位の管理用サーバに機器情報が通知され、ライセンスの過不足に関係なく管理状態が更新されます。

機器の管理状態の遷移と使用するライセンス数の関係を次の図に示します。



発見

探索によって発見された状態です。この状態ではライセンスは使用されません。発見状態の機器は、管理対象または除外対象にして、JP1/IT Desktop Management 2 で管理するかどうかを決定します。

なお、発見された機器を自動的に管理対象にする場合、ライセンス数が足りないときもこの状態になります。

管理対象

JP1/IT Desktop Management 2 で管理する対象となった状態です。管理対象の機器 1 台につき、ライセンスを 1 つ使います。機器を管理対象にすることで、JP1/IT Desktop Management 2 の各機能の実行対象になります。

管理対象の機器は除外対象にしたり、削除したりできます。

除外対象

JP1/IT Desktop Management 2 の管理の対象外となった状態です。この状態ではライセンスは使用されません。例えば、コンピュータだけを JP1/IT Desktop Management 2 で管理したい場合は、発見された機器のうちプリンタやネットワーク装置などコンピュータ以外の機器を除外対象にしてください。

> **ヒント**
>
> 除外対象の機器は、探索で発見されなくなります。また、除外対象の機器には、エージェントが配信されなくなります。管理不要な機器を除外対象にしておくと、定期的に機器を探索している場合に、新規に発見された機器だけをチェックできます。

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。

削除

JP1/IT Desktop Management 2 から機器の情報が削除された状態です。機器を削除すると、データベースからその機器の情報が削除されます。

削除された機器は、探索で再度発見できます。この場合、新規機器として扱われ、以前の設定は引き継がれません。

関連リンク

- (1)　収集できる機器情報の種類
- (2)　機器の状態として収集できる情報
- (3)　システム情報として収集できる情報
- (4)　ハードウェア情報
- (5)　インストールソフトウェア情報
- (6)　セキュリティ情報
- (7)　資産情報と機器情報の共通管理項目

(1)　管理対象にできる機器の種類

JP1/IT Desktop Management 2 では、ネットワークに接続されている、IP アドレスを持つ機器を管理対象にできます。管理対象にできる機器の種類を次の表に示します。

機器種別		管理方法				
		エージェント	エージェントレス	Active Directory と連携	MDM システムと連携	API で外部システムと連携
PC およびサーバ（仮想化環境を含む）	Windows	○	○	○	×	○
	UNIX	○	○	×	×	○
	Linux	○	○	×	×	○
	Mac OS	○	○	×	×	○
スマートデバイス		×	×	×	○	○
その他の機器		×	○	×	×	○

（凡例）○：管理できる　×：管理できない

IPv4 形式と IPv6 形式の両方の IP アドレスを使用している機器は、IPv4 形式の IP アドレスだけを利用して管理対象にできます。

なお、IPv6 形式の IP アドレスだけを持つ機器は、Active Directory に登録されている機器を探索する方法でだけ管理対象にできます。ただし、この場合、機器の存在だけを管理できます。

関連リンク

- (1)　収集できる機器情報の種類
- (2)　機器の状態として収集できる情報
- (3)　システム情報として収集できる情報
- (4)　ハードウェア情報
- (5)　インストールソフトウェア情報
- (6)　セキュリティ情報
- (7)　資産情報と機器情報の共通管理項目
- 2.4.2　ネットワークに接続されている機器を探索する流れ

(2)　仮想コンピュータの管理

システム内で仮想コンピュータを使用している場合、仮想コンピュータに OS がインストールされていれば、1 台のコンピュータとして管理対象にできます。これによって、仮想コンピュータの機器情報を収集したり、セキュリティ状況を管理したりできます。

各仮想コンピュータが仮想化サーバと別のコンピュータと認識されるためには、OS がインストールされている仮想コンピュータが、次のどちらかの条件を満たしている必要があります。

- 仮想化サーバと MAC アドレスが異なっている
- 仮想化サーバと MAC アドレスが同じ場合、仮想化サーバと仮想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

MAC アドレスが同じ場合、エージェントをインストールすることで、別のコンピュータと認識されます。

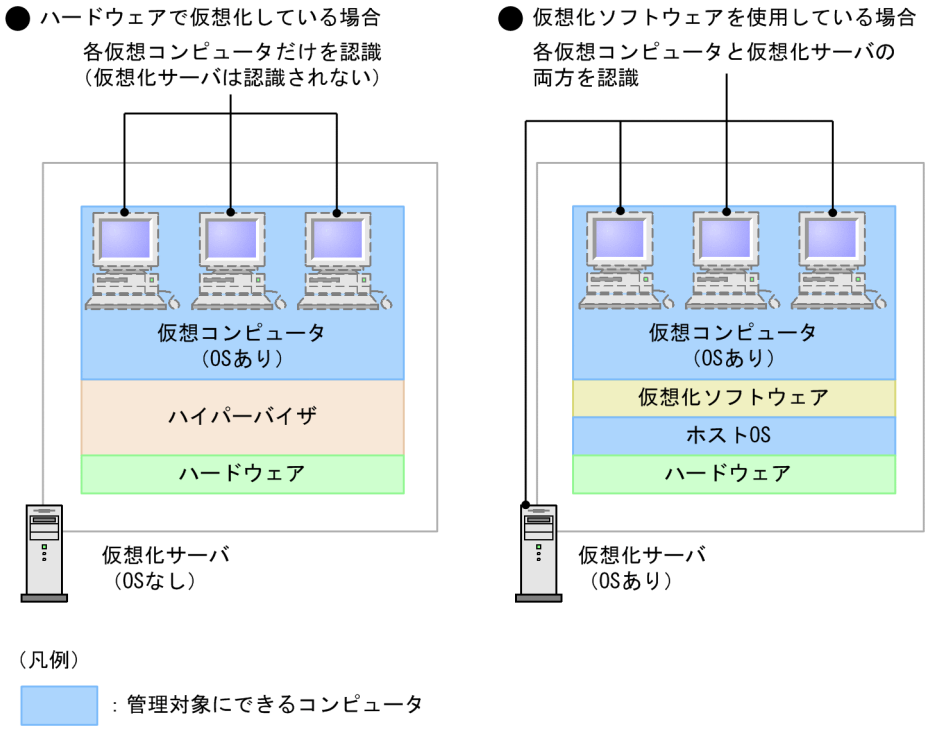
ハードウェアで仮想化している場合

ハードウェア上で直接動作するハイパーバイザによって仮想コンピュータを管理している仮想化サーバでは、仮想コンピュータを個々のコンピュータとして管理できます。ただし、この場合の仮想化サーバには OS がインストールされていないので、1 台のコンピュータとしては認識されないため管理できません。

仮想化ソフトウェアを使っている場合

OS 上で仮想化ソフトウェアを使って仮想コンピュータを管理している仮想化サーバでは、各仮想コンピュータと仮想化サーバに OS がインストールされているので、それぞれコンピュータとして管理できます。

仮想化サーバおよび仮想コンピュータの扱いについて次の図に示します。



共有型 VDI の仮想コンピュータの管理

共有型 VDI の仮想コンピュータを管理することもできます。共有型 VDI の仮想コンピュータは、マスターとなる仮想コンピュータのイメージがユーザごとにコピーされて使用されます。JP1/IT Desktop Management 2 では、コピーされた仮想コンピュータを 1 台のコンピュータとして管理できます。

重要

- 共有型 VDI の仮想コンピュータはエージェントレスで管理できません。
  また、探索時の自動登録によって共有型 VDI の仮想コンピュータがエージェントレスで管理対象となった場合にもライセンスが消費されます。
- 共有型 VDI の仮想コンピュータは Windows エージェントだけが対象です。UNIX エージェントは対象外です。
- 共有型 VDI の仮想コンピュータは中継システム、管理用中継サーバには対応していません。

2.6.2 機器情報の収集

管理対象の機器からは、機器情報が収集されます。また、Active Directory で管理している情報を取得したり、管理者が直接情報を入力したりできます。機器情報は、機器画面で確認できます。

収集できる機器情報の種類については、「(1) 収集できる機器情報の種類」を参照してください。

なお、収集できる機器情報は機器の状態によって次のように異なります。

エージェントをインストールしているコンピュータ

JP1/IT Desktop Management 2 で管理できるすべての機器情報が収集されます。また、Active Directory で管理している情報を取得できます。一部の機器情報は、管理者が直接情報を入力することもできます。

コンピュータに入力画面を表示させて、利用者が入力した情報を収集することもできます。利用者が入力した情報を収集する方法については、「(12)　利用者情報の取得」を参照してください。

また、Windows のコントロールパネルの［プログラムと機能］に登録されていないソフトウェアを検索して情報を収集することもできます。ソフトウェアを検索して情報を収集する方法については、「(11)　情報を収集したいソフトウェアの検索条件の定義」を参照してください。

エージェントレスのコンピュータ

探索時に認証できた範囲で機器情報が収集されます。認証は、Windows の管理共有の認証と、SNMP 認証があります。認証できなかった場合は、ICMP または ARP によって取得できる範囲で機器情報が収集されます。

また、Active Directory で管理している情報を取得できます。一部の機器情報は、管理者が直接情報を入力することもできます。

> **重要**
>
> SNMP 認証の場合、コンピュータにインストールされている SNMP エージェントによっては収集できない機器情報があります。

コンピュータ以外の機器

SNMP 認証または ICMP、ARP によって取得できる範囲で機器情報が収集されます。

また、一部の機器情報は、管理者が直接情報を入力することもできます。

機器情報が収集されるタイミング

機器情報が収集されるタイミングは機器の状態によって次のように異なります。

エージェントをインストールしているコンピュータ

オンライン管理の場合

コンピュータが管理対象になったタイミングで自動的に収集されます。また、コンピュータの情報に変更があったときに、自動的に機器情報が更新されます。

オフライン管理の場合

外部記憶媒体を使用して、コンピュータの機器情報を管理用サーバに通知したタイミングで更新されます。

なお、UNIX エージェント、Mac エージェントの場合、オフライン管理では機器情報を収集できません。

エージェントレスのコンピュータまたはコンピュータ以外の機器

設定したスケジュールに従って定期的に機器情報が更新されます。

エージェントがインストールされている機器の場合、最新の機器情報を任意のタイミングで収集することもできます。

なお、任意のタイミングで機器情報を収集する場合、利用者の情報は最後に入力されたものが収集されます。

(1) 収集できる機器情報の種類

管理対象の機器から機器情報を収集できます。機器情報は、「基本機器情報」と「資産情報と機器情報の共通管理項目」に分類されます。

基本機器情報

デフォルトで収集できる機器の情報です。[システム情報]、[ハードウェア情報]、[インストールソフトウェア情報]、[セキュリティ情報] の 4 つに分類されます。

資産情報と機器情報の共通管理項目

機器の利用者に関する情報です。この情報を利用者が入力するように設定しておくと、入力された内容が機器から収集されます。

なお、収集できる機器情報は、エージェントをインストールしているコンピュータかどうかによって異なります。エージェントレスの機器から収集する場合、認証状態によって収集できる項目が異なります。以降の説明では、エージェントレスの認証状態を次のように分けて説明しています。

- 管理共有：Windows の管理共有の認証を利用できる。
- SNMP：SNMP の認証を利用できる。
- ARP：ARP を利用できる。
- ICMP：ICMP を利用できる。
- Active Directory：Active Directory と連携している。
- MDM：MDM システムと連携している。
- API：API を使用して外部システムと連携している。

Windows の管理共有の認証、または SNMP の認証ができない機器については、ICMP または ARP が利用できる場合に存在だけを確認できます。また、Active Directory と連携している場合、Active Directory から収集できる項目とできない項目があります。

MDM システムと連携してスマートデバイスを管理している場合、MDM システムで管理されている情報を機器情報として取得できます。

外部システムから API を使用する場合、外部システムで管理している情報を機器情報として取得できます。

収集された機器情報は、機器画面の［機器情報］画面および［ソフトウェア情報］画面で確認できます。機器情報が収集されていない場合、機器の電源が OFF、ネットワークに未接続、管理用サーバとの通信に失敗しているなどの原因が考えられます。「−」、「N/A」、または「不明」と表示される項目は、機器の認証状態、機器種別、OS、ソフトウェアなどによって取得できない情報です。また、機器を特定するための情報を取得できなかった場合は、「SNMP 発見（認証情報不足）」と表示されることがあります。

以降で、収集できる機器情報の項目と、エージェント導入済みのコンピュータ、エージェントレスの機器、Active Directory、MDM システム、API からの収集可否を一覧で説明します。

(2) 機器の状態として収集できる情報

機器の状態として収集できる情報について表に示します。

なお、SNMP 認証の場合は、収集できる機器情報はコンピュータにインストールされている SNMP エージェントに依存します。そのため、一部の機器情報が収集できないことがあります。

管理種別

アイコン	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
	エージェント管理 エージェントが導入されている状態です。	○	○	−	−	−	−	−	−
	エージェントレス管理（認証成功） Windows の管理共有または SNMP による認証ができている状態です。Active Directory による探索で新規に発見した機器もこの状態になります。	−	−	○	○	−	○	−	−
	エージェントレス管理（認証失敗） 認証ができていない状態です。	−	−	−	−	○	−	−	−
	エージェント管理（ネットワーク監視用） エージェント導入済みでかつネットワークモニタが有効になっている状態です。	○	−	−	−	−	−	−	−
	エージェント管理（ネットワーク監視用－有効化中） エージェント導入済みでかつネットワークモニタが有効化中の状態です。	○	−	−	−	−	−	−	−

アイコン	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ ICMP	Active Directory	MDM	API
	エージェント管理（ネットワーク監視用－有効化失敗） エージェント導入済みでかつネットワークモニタの有効化が失敗した状態です。	○	－	－	－	－	－	－	－
	エージェント管理（ネットワーク監視用－無効化中） エージェント導入済みでかつネットワークモニタが無効化中の状態です。	○	－	－	－	－	－	－	－
	エージェント管理（ネットワーク監視用－無効化失敗） エージェント導入済みでかつネットワークモニタの無効化が失敗した状態です。	○	－	－	－	－	－	－	－
	エージェント管理（中継システム） 中継システムが導入されている状態です。	○	－	－	－	－	－	－	－
	エージェント管理（中継システム）（ネットワーク監視用） 中継システム導入済みでかつネットワークモニタが有効になっている状態です。	○	－	－	－	－	－	－	－
	エージェント管理（中継システム）（ネットワーク監視用－有効化中） 中継システム導入済みでかつネットワークモニタが有効化中の状態です。	○	－	－	－	－	－	－	－

アイコン	説明	エージェント導入済み		エージェントレス					
		Windows	UNIXまたはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
	エージェント管理（中継システム）（ネットワーク監視用－有効化失敗） 中継システム導入済みでかつネットワークモニタの有効化が失敗した状態です。	○	－	－	－	－	－	－	－
	エージェント管理（中継システム）（ネットワーク監視用－無効化中） 中継システム導入済みでかつネットワークモニタが無効化中の状態です。	○	－	－	－	－	－	－	－
	エージェント管理（中継システム）（ネットワーク監視用－無効化失敗） 中継システム導入済みでかつネットワークモニタの無効化が失敗した状態です。	○	－	－	－	－	－	－	－
	管理用中継サーバ 管理用中継サーバが導入されている状態です。	○ ※	－	－	－	－	－	－	－
	管理用中継サーバ（ネットワーク監視用） 管理用中継サーバ導入済みでかつネットワークモニタが有効になっている状態です。	○ ※	－	－	－	－	－	－	－
	管理用中継サーバ（ネットワーク監視用－有効化中） 管理用中継サーバ導入済みでかつネットワークモニタが有効化中の状態です。	○ ※	－	－	－	－	－	－	－

アイコン	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
	管理用中継サーバ（ネットワーク監視用－有効化失敗） 管理用中継サーバ導入済みでかつネットワークモニタの有効化が失敗した状態です。	○ ※	－	－	－	－	－	－	－
	管理用中継サーバ（ネットワーク監視用－無効化中） 管理用中継サーバ導入済みでかつネットワークモニタが無効化中の状態です。	○ ※	－	－	－	－	－	－	－
	管理用中継サーバ（ネットワーク監視用－無効化失敗） 管理用中継サーバ導入済みでかつネットワークモニタの無効化が失敗した状態です。	○ ※	－	－	－	－	－	－	－
	MDM 連携管理 MDM システムから情報を取得して管理している状態です。	－	－	－	－	－	－	○	－
	API 管理 外部システムから API で情報を取得して管理している状態です。	－	－	－	－	－	－	－	○

（凡例）○：収集できる　－：対象外

注※　管理用中継サーバ用のエージェントです。

接続設定

接続設定は、JP1/IT Desktop Management 2 でのネットワーク接続の設定状態を示します。

アイコン	説明	エージェント導入済み	エージェントレス					
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
	許可 ネットワーク接続できる状態です。	○	○	○	○	○	○	○
	遮断 ネットワーク接続できない状態です。セキュリティポリシーやネットワークモニタ機能によって自動的にネットワーク接続が遮断された場合もこの状態になります。	○	○	○	○	○	○	○
	強制遮断 管理者によってネットワーク接続が遮断された状態です。	○	○	○	○	○	○	○
	利用期間外 ネットワーク制御リストで設定された利用期間ではない状態です。	○	○	○	○	○	○	○
	不明 その機器のネットワーク接続が許可されているかどうかを判定中の状態です。判定後、ほかの状態に変わります。	○	○	○	○	○	○	○

（凡例）○：収集できる

機器状態

アイコン	説明	エージェント導入済み※1		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
	稼働中 コンピュータの電源がONの状態です。	○	×	○	○	○	×	×	○

アイコン	説明	エージェント導入済み※1		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ ICMP	Active Directory	MDM	API
	停止中 コンピュータの電源が OFF の状態です。※2	○ ※3	×	○	○	○	×	×	○
	警告 機器に何らかの問題がある状態です。機器画面の［システム情報］タブおよび［イベント］タブで詳細を確認できます。	○ ※3、※4	×	×	○ ※5	×	×	×	○
	障害 機器に何らかの障害が発生している状態です。機器画面の［システム情報］タブおよび［イベント］タブで詳細を確認できます。	×	×	×	○ ※6	×	×	×	○
	不明 機器の稼働状況が不明な状態です。	×	○	×	○	○	○	○	○
	配下の管理用サーバによる管理 機器の管理元が配下の管理用中継サーバの場合に表示されます。稼働状態の取得の対象外です。	○	○	○	○	○	○	○	○

（凡例）○：収集できる　×：収集できない　－：対象外

注

機器状態の表示条件については、「(8)　機器状態の種類と表示条件」を参照してください。

注※1

オフライン管理のコンピュータの機器情報が初めて取得された場合、機器状態は「停止中」になります。2 回目以降に取得した場合は、以前の機器状態が維持されます。

ただし、コンフィグレーションファイル（jdn_manager_config.conf）の OfflineRegistration_StatusUnknown プロパティに ON が設定されている場合、機器状態は「不明」になります。

注※2

機器と通信できない場合、機器状態は「停止中」になります。

注※3

次の機器の電源が OFF の場合、およびオフライン管理の場合、機器状態は「警告」と表示されます。機器状態が「停止中」と表示されることはありません。

- 中継システム
- ネットワークモニタを有効化したエージェント導入済みのコンピュータ

注※4

ネットワークモニタを有効化したエージェント導入済みのコンピュータで、JP1_ITDM2_Network Monitor のサービスが停止している場合、機器状態は「警告」と表示されます。

注※5

機器がプリンタで、トナーまたは用紙が少なくなった場合、機器状態は「警告」と表示されます。

注※6

機器がプリンタで、トナー切れまたは用紙切れになった場合、機器状態は「障害」と表示されます。

管理形態

アイコン	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ ICMP	Active Directory	MDM	API
	オンライン管理 機器をオンライン管理している状態です。	○	○	－	－	－	－	－	－
	オフライン管理 機器をオフライン管理している状態です。	○	－	－	－	－	－	－	－
－	エージェント未導入 エージェントが導入されていない状態です。	○	－	○	○	○	○	○	○

（凡例）○：収集できる　－：対象外

管理対象の機器が接続する管理用中継サーバの情報

項目	説明	エージェント導入済み	エージェントレス					
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
管理元	管理元の管理用中継サーバのホスト名を表示します。自サーバが管理元の機器の場合は、[(自サーバ)] と表示します。	○	○	○	○	○	○	○
管理元への経路	自サーバから管理元の管理用中継サーバまでの経路を表示します。	○	○	○	○	○	○	○

(凡例) ○：収集できる

(3) システム情報として収集できる情報

システム情報として収集できる情報について説明します。システム情報では、次に示す情報を収集できます。

- 機器種別
- ホスト識別子
- コンピュータ情報
- ユーザー情報
- OS 情報
- ネットワーク情報
- プリンタ情報
- スマートデバイス情報

なお、SNMP 認証の場合は、収集できる機器情報はコンピュータにインストールされている SNMP エージェントに依存します。そのため、一部の機器情報が収集できないことがあります。

機器種別

機器種別	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
PC	取得した OS 種別が次の場合に設定されます。 • Windows 10 • Windows 8.1 • Windows 8 • Windows 7 • Windows Vista • Windows XP • Windows 2000 • Windows OS エディション不明 • Windows OS 種別不明 • Mac OS • OS 不明	○	○ ※1	○	○	×	○	×	○

サーバ	取得した OS 種別が次の場合に設定されます。
	• Windows 2000 Server
	• Windows 2000 Advanced Server
	• Windows Server 2003
	• Windows Server 2008
	• Windows Server 2012
	• Windows Server 2016
	• Windows Server 2019
	• UNIX
	  • AIX
	  • HP-UX
	  • Solaris
	• Linux
		○	○	○	○	×	○	×	○

機器種別	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
サーバ	• CentOS • Red Hat Enterprise Linux • Oracle Linux	○	○	○	○	×	○	×	○
ストレージ	管理者が入力する場合だけ設定できます。	×	×	×	×	×	×	×	○
ネットワーク装置	ネットワークプリンタ以外のネットワーク装置の場合に、自動で収集できます。	×	×	×	○	×	×	×	○
プリンタ	ネットワークプリンタの場合に、自動で収集できます。	×	×	×	○	×	×	×	○
スマートデバイス	MDM システムから情報を取得した場合に設定されます。	×	×	×	×	×	×	○	○
周辺装置	管理者が入力する場合だけ設定できます。	×	×	×	×	×	×	×	○
USB デバイス	次の場合に設定されます。 • 管理者が入力した場合 • [USB デバイスの登録] ダイアログから登録した場合	×	×	×	×	×	×	×	○
ディスプレイ	管理者が入力する場合だけ設定できます。	×	×	×	×	×	×	×	○
その他	管理者が入力する場合だけ設定できます。	×	×	×	×	×	×	×	○
管理者が追加した機器種別 ※2	管理者が入力する場合だけ設定できます。	×	×	×	×	×	×	×	○
不明な機器	機器種別が取得できなかった場合に設定されます。	×	×	×	×	○	×	×	○

（凡例）○：自動で収集できる　×：自動で収集できない

注※1　エージェントを導入できるのは Mac OS（OS X 10.10、OS X 10.11、macOS 10.12、macOS 10.13 または macOS 10.14）です。

注※2　複数サーバ構成の管理用中継サーバで機器種別を変更した場合で、変更後の機器種別の項目が上位の管理用サーバに設定されていないときは、上位の管理用サーバにその機器種別の項目が追加されます。上位の管理用サーバで機器種別に追加できる項目数の上限を超えているときは、上位の管理用サーバで機器情報の更新に失敗します。更新に失敗したかどうかは、上位の管理用サーバのイベントで確認できます。

ヒント

BIG-IP など Linux ベースで実装されている特殊なネットワーク機器は、サーバ(Linux)として発見されることがあります。発見された機器情報を確認し、必要に応じて機器種別を変更してください。

ヒント

ルーターとしての機能を持つプリンタは、ネットワーク機器として発見されることがあります。発見された機器情報を確認し、必要に応じて機器種別を変更してください。

ホスト識別子

項目	説明	エージェント導入済み	エージェントレス					
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
ホスト識別子	ホスト識別子を表示します。	○	○	○	○	○	○	○

（凡例）○：収集できる

注　エージェント導入済みのコンピュータまたは管理共有を使用して情報収集しているコンピュータのホスト識別子は、次の項目を基に機器を識別しています。ハード交換などでこれらの情報が変更された場合は、別機器として登録されることがあります。

- マシン UUID
- マシンシリアルナンバー
- BIOS シリアルナンバー
- マザーボードシリアルナンバー

また、上記情報の変更によって、別機器として登録する回数は 3 回までです。

メモ

共有型 VDI の仮想コンピュータを管理する場合、次のどれかの機器情報を基にホスト識別子を生成できます。

- コンピュータ名※1
- アカウント名※2
- IP アドレス（IPv4）※1

注※1　VMware Horizon View および Citrix Virtual Desktops の MCS（Machine Creation Services）方式を使用する場合に選択できます。

注※2　Citrix Virtual Desktops の PVS（Provisioning Services）方式を使用する場合に選択できます。

また、機器情報が次のすべての条件を満たす場合、ホスト識別子の一部として使用されます。

コンピュータ名

15 文字以内、かつ、半角英数字、「-」および「_」を使用している。

アカウント名

20 文字以内、かつ、半角英数字、半角スペース、および「-」、「!」、「#」、「$」、「'」、「(」、「)」、「.」、「^」、「_」、「`」、「{」、「}」、および「~」を使用している。

重要

共有型 VDI の仮想コンピュータを管理する場合のホスト識別子の生成について、注意事項を次に示します。

- ホスト識別子の生成に使用する機器情報は一意である必要があります。
- ホスト識別子の生成に使用する機器情報は、仮想化方式ごとに正しく選択してください。選択を誤った場合、ライセンスを正しくカウントできないおそれがあります。
- ホスト識別子の生成に IP アドレスを使用する場合、仮想コンピュータに設定する IP アドレスを 1 つとして運用してください。仮想コンピュータに複数の IP アドレスが設定されている場合は、設定されている IP アドレスのどれかを使用してホスト識別子が生成されます。
- Windows で IP アドレスを自動的に取得する設定を有効にしている場合、ホスト識別子の生成には IP アドレス以外の機器情報を使用してください。

コンピュータ情報

項目		説明	エージェント導入済み			エージェントレス					
			Windows	UNIX	MacOS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
コンピュータ情報	コンピュータ名（説明）	コンピュータ名 マイコンピュータのプロパティの［コンピュータ名］パネルから［変更］ボタンをクリックして表示される［コンピュータ名の変更］ダイアログで設定する［コンピュータ名］です。 SNMP 認証の場合は、取得したホスト名です。 スマートデバイスの場合は、MDM システムでスマートデバイスを識別するために表示しているスマートデバイスの名称、または、ユーザー名、契約電話番号およびモデル名をコロン（:）で結合した形式の名称です。※1 コンピュータの説明 マイコンピュータのプロパティの［コンピュータ名］パネルで設定する［コンピュータの説明］です。 SNMP 認証の場合は、機器に関する説明と機器の開発会社固有のオブジェクト ID です。 スマートデバイスの場合は取得できません。	○	○ ※2	○ ※2	○	○	×	○	○	○
	ホスト名	物理的な完全修飾ドメイン名です。 ただし、次の場合はドメインが付かないホスト名または NetBIOS 名が収集されます。 • ドメインに参加していない、またはドメインへの参加が確認できない場合 • SNMP 探索でホスト名を取得した場合	○	○ ※2	○ ※2	○	○	×	○	○	○

項目		説明	エージェント導入済み			エージェントレス					
			Windows	UNIX	MacOS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
コンピュータ情報	ホスト名	スマートデバイスの場合は、MDM システムでスマートデバイスを識別するために表示しているスマートデバイスの名称、または、ユーザー名、契約電話番号およびモデル名をコロン(:)で結合した形式の名称です。※1	○	○ ※2	○ ※2	○	○	×	○	○	○
	モデル(メーカー)	コンピュータの製造元で付与されたコンピュータのモデル名、およびコンピュータの製造元です。	○	○	○	○	×	×	×	○	○
	UUID	コンピュータのユニバーサルユニーク識別子(UUID)です。	○	○	○	○	×	×	×	×	○
	シリアルナンバー	コンピュータのシリアル番号(BIOS 情報)です。	○	○	○	○	×	×	×	○	○
	CPU	CPU の名称です。	○	○	○	○	○	×	×	×	○
	メモリ	コンピュータに搭載されている物理メモリの合計容量です。	○	○	○	○	○	×	×	○	○
	空き容量	ハードディスク(論理ドライブの種類がローカルディスク)の空き容量です。 ローカルディスクの空き容量の合計値が 9,223,372,036,854,775,807 バイトを超える場合は、9,223,372,036,854,775,807 バイトと表示されます。	○	○	○	○	×	×	×	×	○
システムドライブ	システムドライブ	論理ドライブの合計台数です。	○	○	○	○	×	×	×	×	○
	各システムドライブ※3(種類/空き容量/容量/ファイルシステム)	システムドライブが複数ある場合は、次の情報をそれぞれ収集できます。 種類 ハードディスク、CD/DVD ドライブ、リムーバブルディスクなどのドライブの種別です。	○	○	○	○	×	×	×	×	○

項目		説明	エージェント導入済み			エージェントレス					
			Windows	UNIX	MacOS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
システムドライブ	各システムドライブ※3（種類/空き容量/容量/ファイルシステム）	空き容量※4 ドライブの空き容量です。 容量※4 ドライブの容量です。 ファイルシステム※4 FAT32、NTFS などのファイルシステムの名称です。 システムドライブが BitLocker によってロック中の場合、「BitLocker によってロック中」と表示されます。	○	○	○	○	×	×	×	×	○
	ディスク名（容量/インターフェース）※5	ディスク名 ハードディスクのモデル名です。 容量 ハードディスク全体の容量です。 インターフェース IDE、SCSI などのハードディスクのインターフェース名です。	○	○	○	○	○ ※6	×	×	○ ※7	○
BIOS情報	BIOS情報	BIOS の名称です。	○	×	×	○	×	×	×	×	○
	メーカー	BIOS のメーカーです。	○	○	×	○	×	×	×	×	○
	シリアルナンバー	BIOS のシリアルナンバーです。	○	×	×	○	×	×	×	×	○
	バージョン（BIOS/SMBIOS）	BIOS BIOS のバージョンです。 SMBIOS SMBIOS のバージョンです。	○	○	×	○	×	×	×	×	○
	リリース日	BIOS のリリース日です。	○	○	×	○	×	×	×	×	○
AMT ファームウェアバージョン		AMT ファームウェアのバージョンです。	○	×	×	×	×	×	×	×	○

項目		説明	エージェント導入済み			エージェントレス					
			Windows	UNIX	MacOS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
電源管理	モニタの電源を切る（AC/DC）※8、※9	モニタ電源が切れるまでの時間です。 AC 交流電源です。 DC 直流電源（バッテリー電源）です。	○	×	×	○	×	×	×	×	○
	システムスタンバイ（AC/DC）※8	システムスタンバイまでの時間です。 AC 交流電源です。 DC 直流電源（バッテリー電源）です。	○	×	×	○	×	×	×	×	○
	システム休止状態（AC/DC）※8	システムが休止状態に入るまでの時間です。 AC 交流電源です。 DC 直流電源（バッテリー電源）です。	○	×	×	○	×	×	×	×	○
	ハードディスクの電源を切る（AC/DC）※7、※8	ハードディスクの電源が切れるまでの時間です。 AC 交流電源です。 DC 直流電源（バッテリー電源）です。	○	×	×	○	×	×	×	×	○
	プロセッサ調整（AC/DC）※8、※9	プロセッサの電力設定です。 AC 交流電源です。 DC 直流電源（バッテリー電源）です。	○	×	×	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

注※1　スマートデバイスの名称、または、ユーザー名、契約電話番号およびモデル名をコロン（:）で結合した形式の名称のどちらになるかは、「(2)　MDM システムから取得できる機器情報」の「コンピュータ名」、「ホスト名」の説明を参照してください。

注※2　UNIX エージェント、Mac エージェント側で「コンピュータ名」を通知する設定になっている場合は収集されます。また、「ホスト名（完全修飾ドメイン名）」が「コンピュータ名」として収集されます。なお、「コンピュータの説明」は取得できません。

注※3　Windows エージェントの場合はドライブレター（C:、D:など）、UNIX エージェント、Mac エージェントの場合はマウントパスが取得されます。

注※4　Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、および Windows Server 2008 R2 の場合で、BitLocker ドライブ暗号化にロックが掛かっているときは、情報を取得できません。

注※5　Windows Server 2019、Windows Server 2016 および Windows Server 2012 の場合で、記憶域サービスで仮想ディスクを構成しているときは、物理ディスクとして仮想ディスクの情報が取得されます。

注※6　「ディスク名」および「容量」だけを収集できます。

注※7　「容量」だけ収集できます。

注※8　Windows Server 2003、および Windows XP の場合で、Administrator 権限を持たないユーザーがログオンしているときは、直前にログオンした Administrator 権限を持つユーザーの電源設定情報が収集されます。

注※9　これらの機能を利用できない場合、正しい情報を収集できないことがあります。

ユーザー情報

項目	説明	エージェント導入済み			エージェントレス					
		Windows	UNIX	Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
最終ログオンユーザーのユーザー名（アカウント名）	最後にログオンしたユーザーのユーザー名、および最後にログオンしたユーザーのドメイン名（またはコンピュータ名）付きアカウント名です。	○ ※1	×	○	○ ※1	×	×	×	×	○
説明	最後にログオンしたユーザーの説明です。	○ ※1	×	×	○ ※1	×	×	×	×	○

項目	説明	エージェント導入済み			エージェントレス					
		Windows	UNIX	Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
ロケール/タイムゾーン	ロケール 最後にログオンしたユーザーのロケールです。 タイムゾーン 最後にログオンしたユーザーのタイムゾーンです。	○	×	○ ※2	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

注　取得可能なユーザー情報は、コンソールからログオンしたユーザーが対象です。リモートでログオンしたユーザー情報は収集されません。

注※1　最後にログオンしたユーザーのフルネーム、およびユーザーの説明は、ドメインユーザーの場合は収集できません。

注※2　タイムゾーンの情報だけ収集できます。

OS 情報

項目	説明	エージェント導入済み			エージェントレス					
		Windows	UNIX	Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
OS とサービスパックまたはバージョン（OS の言語）※1	OS に適用されているサービスパックまたはバージョン、および OS の言語です。日本語版 Windows、または英語版 Windows などの情報です。ロケール設定ではありません。	○	○ ※2	○ ※2	○	×	×	○ ※3	×	○
カーネルバージョン	Linux のカーネルバージョンです。	×	○	×	×	×	×	×	×	○

項目	説明	エージェント導入済み			エージェントレス					
		Windows	UNIX	Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
シリアルナンバー	OS のシリアル番号です。OS インストール時に要求されるライセンスキーではありません。	○	×	×	○	×	×	×	×	○
所有者（会社名）	所有者 OS インストール時にユーザーが入力した所有者名です。 会社名 OS インストール時にユーザーが入力した会社名です。	○	×	×	○	×	×	×	×	○
OS 最終起動日時	OS の最終起動日時です。	○	○	○	○	×	×	×	×	○
Windows ディレクトリ	OS がインストールされているディレクトリです。	○	×	×	○	×	×	×	×	○
Windows Installer バージョン	Windows Installer のバージョンです。	○	×	×	○	×	×	×	×	○
Windows Update エージェントバージョン	Windows Update エージェントのバージョンです。	○	×	×	○	×	×	×	×	○
IE バージョン（サービスパック）	IE バージョン Internet Explorer のバージョンです。 IE サービスパック Internet Explorer のサービスパックのバージョンです。	○	×	×	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

注※1　エージェントの OS によって収集する情報が異なります。

Windows 10、Windows Server 2019、または Windows Server 2016 以外の場合
　OS のサービスパック情報が収集されます。

Windows 10、Windows Server 2019、または Windows Server 2016 の場合

OS のコマンド「Ver.exe」に表示されるバージョンの情報（「1511」など）が収集されます。

注※2　OS の名称だけ収集できます。

注※3　OS サービスパックまたはバージョンの情報だけ収集できます。

ネットワーク情報

項目	説明	エージェント導入済み※1		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
IP アドレス/サブネットマスク※6	IP アドレスおよびサブネットマスクです。	○	○	○	○	○ ※2、※3	○	×	○
ネットワークアダプタ	ネットワークアダプタの名称です。	○	○	○	○	×	×	×	○
MAC アドレス※6	MAC アドレスです。	○	○	○	○	○ ※3、※4	○	○	○
デフォルトゲートウェイ	デフォルトゲートウェイです。	○	○	○	○	×	×	×	○
WINS サーバアドレス（プライマリ/セカンダリ）	プライマリ プライマリ WINS サーバのアドレスです。 セカンダリ セカンダリ WINS サーバのアドレスです。	○	×	○	×	×	×	×	○
DNS アドレス	DNS サーバのアドレスです。	○	○	○	×	×	×	×	○
DHCP	DHCP の有効/無効の設定状態です。	○	○	○	×	×	×	×	○
DHCP サーバアドレス	DHCP サーバのアドレスです。	○	○	○	×	×	×	×	○
リース取得日時/期限日時	DHCP リース取得日時、および DHCP リース期限日時です。	○	×	○	×	×	×	×	○

項目	説明	エージェント導入済み※1		エージェントレス					
		Windows	UNIXまたはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
ドメイン（ワークグループ）/ロール	ドメイン 所属しているドメイン/ワークグループの名称です。 ドメインロール プライマリドメインコントローラ、メンバワークステーションなど、OSのドメインでの役割です。	○	×	○	○ ※5	×	×	×	○

（凡例）○：収集できる　×：収集できない

注　取得可能なネットワーク情報は、コントロールパネルに表示されるネットワークアダプタだけです

注※1　NICがないオフライン管理のコンピュータの場合は収集できません。

注※2　「IPアドレス」だけ収集できます。

注※3　収集した情報は、機器画面の［機器情報］画面－［システム情報］タブには表示されません。機器一覧をエクスポートすると、収集した情報を確認できます。

注※4　ARPの場合だけ収集できます。

注※5　「ドメイン」だけ収集できます。

注※6　機器画面の［機器情報］画面－［システム情報］タブには、コンピュータが持つすべてのネットワーク接続デバイスの情報が表示されます。機器一覧画面およびシステム構成情報には、上位システムとの通信に使用したネットワーク接続デバイス情報が表示されます。ただし、インターネットゲートウェイとの通信時は、コンピュータが持っているネットワーク接続デバイスの中の任意のデバイス情報が表示されます。

プリンタ情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
印刷方式（方式/色数）	プリンタの印刷方式です。	×	×	×	○	×	×	×	○
消耗品（種別/説明/状態）	インクなどの消耗品の種別と残量の情報です。	×	×	×	○	×	×	×	○
給紙トレイ（種別/名前/状態）	給紙装置の種別と用紙の残量です。	×	×	×	○	×	×	×	○

（凡例）○：収集できる　×：収集できない

スマートデバイス情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
IMEI	移動体通信機器に付与されている識別番号です。	×	×	×	×	×	×	○	○
UDID	Apple 社製のスマートデバイスに付与されている識別子です。	×	×	×	×	×	×	○	○
ICCID	Apple 社製のスマートデバイスの SIM カードに付与されている番号です。	×	×	×	×	×	×	○	○
IMSI	移動体通信機器の加入者に付与されている識別番号（スマートデバイスの SIM カードに付与 されている番号）です。	×	×	×	×	×	×	○	○
契約電話番号	契約しているスマートデバイスの電話番号です。	×	×	×	×	×	×	○	○

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
メールアドレス	契約しているスマートデバイスのメールアドレスです。	×	×	×	×	×	×	○	○
キャリア	スマートデバイスの通信サービスを提供する会社です。	×	×	×	×	×	×	○	○
パスコードまたはパスワードの設定状況	パスコードまたはパスワードの設定の有無です。	×	×	×	×	×	×	○	○
内蔵ストレージ（空き容量）	内蔵ストレージ スマートデバイスに内蔵されたハードディスクの容量です。 空き容量 スマートデバイスに内蔵されたハードディスクの空き容量です。	×	×	×	×	×	×	○	○
外部ストレージ（空き容量）	外部ストレージ スマートデバイスに格納されたメディア（SD カードなど）の容量です。 空き容量 スマートデバイスに格納されたメディア（SD カードなど）の空き容量です。	×	×	×	×	×	×	○	○
RAM（空き容量）	RAM スマートデバイスのメモリの容量です。 空き容量 スマートデバイスのメモリの空き容量です。	×	×	×	×	×	×	○	○

（凡例）○：収集できる　×：収集できない

(4)　ハードウェア情報

ハードウェア情報として収集できる情報について説明します。ハードウェア情報では、次に示す情報を収集できます。

- CPU 情報
- メモリ情報
- ハードディスク情報
- CD-ROM ドライブ情報
- リムーバブルドライブ情報
- プリンタ情報
- ビデオコントローラ情報
- サウンドカード情報
- ネットワークアダプタ情報
- モニタ情報
- キーボード情報
- マウス情報

なお、SNMP 認証の場合は、収集できる機器情報はコンピュータにインストールされている SNMP エージェントに依存します。そのため、一部の機器情報が収集できないことがあります。

CPU 情報

項目	説明	エージェント導入済み	エージェントレス					
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
CPU 情報	プロセッサの個数です。	○	○	×	×	×	×	○
プロセッサ	プロセッサの名称です。	○※	○	○	×	×	×	○

（凡例）○：収集できる　×：収集できない

注※　UNIX エージェントまたは Mac エージェントが導入された機器の情報を、［機器情報］画面の機器一覧に表示またはコマンドで CSV ファイルにエクスポートしたときは、プロセッサが複数ある場合でも 1 個だけ出力されます。UNIX エージェントまたは Mac エージェントが導入された機器のプロセッサ個数は、［機器情報］画面の［ハードウェア情報］タブで確認してください。

メモリ情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIXまたはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
メモリ情報	コンピュータに搭載されている物理メモリの総容量です。	○※2	○	○	×	×	×	×	○
容量	コンピュータに搭載されている物理メモリの容量です。	○※2	○	○	×	×	×	○	○
各スロット	メモリスロットに挿入されている物理メモリの容量です。メモリスロットが複数ある場合は、それぞれ収集できます。	○※2	○※3	○	×	×	×	×	○
仮想メモリ容量※1	仮想メモリの全容量です。	○	×	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

注※1

仮想メモリ容量は、「使用可能物理メモリ」＋「ページファイルの合計」で計算されます。

注※2

物理メモリとスロットの関連づけ情報が存在しない管理対象機器は、これらの情報を取得できません。物理メモリとスロットの関連づけ情報は、次の Windows PowerShell コマンドで確認できます。物理メモリとスロットの関連づけ情報が存在しない場合、コマンドの実行結果は 1 件も出力されません。

```
Get-WMIObject -class Win32_PhysicalMemoryLocation
```

これらの情報を取得するには管理対象機器に、次のレジストリを設定してください。

キー名	• 32 ビット OS の場合 HKLM¥SOFTWARE¥HITACHI¥JP1/IT Desktop Management - Agent • 64 ビット OS の場合 HKLM¥SOFTWARE¥Wow6432Node¥HITACHI¥JP1/IT Desktop Management - Agent
値名	JdngGetAllUseMemoryInfo
型	REG_SZ
値	1

レジストリを設定した場合、物理メモリ以外にビデオメモリなどのメモリ情報も取得します。

※3

最大 127 個まで収集できます。

ハードディスク情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX またはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
ハードディスク情報	ハードディスクの台数です。	○	△※6	○	○	×	×	×	○
各ディスク名（容量/インターフェース）※1	ハードディスクが複数ある場合は、次の情報をそれぞれ収集できます。 ハードディスクのモデル ハードディスクのモデル名です。 容量 ハードディスクの容量です。パーティションとは関係なく、全体の容量です。 インターフェース IDE、SCSI などのハードディスクのインターフェースです。	○	△※6	○	○※2	×	×	○※3	○
各ドライブ（空き容量/容量/ファイルシステム）※4	各ハードディスクにドライブが複数ある場合は、次の情報をそれぞれ収集できます。 空き容量※5 ドライブの空き容量です。 容量※5 ドライブの容量です。 ファイルシステム※5 ファイルシステム名です。 システムドライブが BitLocker によってロック中の場合、「BitLocker によってロック中」と表示されます。	○	×	○	×	×	×	×	○

（凡例）○：収集できる　△：AIX、Linux または Mac OS だけ収集できる　×：収集できない

注　ネットワークドライブのドライブ情報は収集できません。

注※1　Windows Server 2019、Windows Server 2016 および Windows Server 2012 の場合で、記憶域サービスで仮想ディスクを構成しているときは、物理ディスクとして仮想ディスクの情報が取得されます。

注※2 「インターフェース」は収集できません。

注※3 「容量」だけ収集できます。

注※4 Windows エージェントの場合はドライブレター（C:、D:など)、UNIX エージェント、Mac エージェントの場合はマウントパスが取得されます。

注※5 Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、および Windows Server 2008 R2 の場合で、BitLocker ドライブ暗号化にロックが掛かっているときは、情報を取得できません。

注※6 最大 127 個まで収集できます。

CD-ROM ドライブ情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
CD-ROM ドライブ情報	CD/DVD ドライブの台数です。	○	×	○	×	×	×	×	○
各 CD-ROM ドライブ	CD/DVD ドライブのモデル名です。ドライブが複数ある場合は、それぞれ収集できます。	○	×	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

リムーバブルドライブ情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
リムーバブルドライブ情報	リムーバブルドライブの台数です。	○	×	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

プリンタ情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIXまたはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
プリンタ情報	コンピュータに設定されているプリンタの台数です。	○	×	○	×	×	×	×	○
プリンタ名（種別）	プリンタが複数設定されている場合は、次の情報をそれぞれ収集できます。 プリンタ名 　プリンタの名称です。 種別 　プリンタの種別です。	○	×	○	×	×	×	×	○
ドライバ	プリンタドライバです。プリンタが複数設定されている場合は、それぞれ収集できます。	○	×	○	×	×	×	×	○
共有名	プリンタ共有名です。プリンタが複数設定されている場合は、それぞれ収集できます。	○	×	○	×	×	×	×	○
プリンタサーバ名（ポート）	プリンタが複数設定されている場合は、次の情報をそれぞれ収集できます。 プリンタサーバ名 　プリンタサーバ名です。 ポート 　プリンタポートです。	○	×	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

ビデオコントローラ情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIXまたはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
ビデオコントローラ情報	ビデオドライバの個数です。	○	×	○	×	×	×	×	○
ビデオチップ	ビデオチップの名称です。	○	×	○	×	×	×	×	○

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX またはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
VRAM 容量	ビデオカードの VRAM 容量です。	○	×	○	×	×	×	×	○
ビデオドライバ	ビデオドライバの名称です。	○	×	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

サウンドカード情報

項目	説明	エージェント導入済み			エージェントレス					
		Windows	UNIX	Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
サウンドカード情報	サウンドカードドライバの個数です。	○	×	○	○	×	×	×	×	○
製品名（メーカー）	サウンドカードの名称、およびサウンドカードのメーカーです。	○	×	○※	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

注※　サウンドカードの名称だけを収集できます。

ネットワークアダプタ情報

項目	説明	エージェント導入済み	エージェントレス					
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
ネットワークアダプタ情報	ネットワークアダプタの個数です。	○	○	○	×	×	×	○
ネットワークアダプタ	ネットワークアダプタの名称です。	○	○	○	×	×	×	○

（凡例）○：収集できる　×：収集できない

モニタ情報

項目	説明	エージェント導入済み			エージェントレス					
		Windows	UNIX	Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
モニタ情報	モニタの個数です。	○	×	○	○	×	×	×	×	○
モニタ	モニタの名称です。	○	×	○	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

キーボード情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX またはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
キーボード情報	キーボードの個数です。	○	×	○	○	×	×	×	○
キーボード	キーボードの名称です。	○	×	○	○	×	×	×	○

（凡例）○：収集できる　×：収集できない

マウス情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX またはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
マウス情報	マウスの個数です。	○	×	○	○	×	×	×	○
マウス	マウスの名称です。	○	×	○	○	×	×	×	○

（凡例）○：収集できる　×：収集できない

(5) インストールソフトウェア情報

インストールソフトウェア情報として収集できる情報について説明します。インストールソフトウェア情報では、次に示すソフトウェアの情報を収集できます。

なお、SNMP 認証の場合は、収集できる機器情報はコンピュータにインストールされている SNMP エージェントに依存します。そのため、一部の機器情報が収集できないことがあります。

Windows エージェントの場合

[プログラムと機能］に登録されているソフトウェア

Windows のコントロールパネルの［プログラムと機能］に登録されているソフトウェアの情報です。

重要

次に示す両方の条件を満たす場合は、該当するソフトウェアをアンインストールしたあとで、ユーザーアカウントを削除してください。アンインストールする前にユーザーアカウントを削除すると、該当するソフトウェアの情報は削除されないまま、JP1/IT Desktop Management 2 のインストールソフトウェア情報として残ります。

・Windows のコントロールパネルの［プログラムと機能］だけに表示されるソフトウェアを、利用者のコンピュータにインストールしている

・上記条件に該当するソフトウェアをインストールしているユーザーアカウントを削除したい

重要

Windows はコンピュータにインストールしている次のストアアプリ情報を削除できません。このため、Windows の［プログラムと機能］や［アプリと機能］にストアアプリを表示していない場合でも、インストールソフトウェアとして次のストアアプリ情報を検出します。

・システムアプリの Windows ストアアプリの情報

・インストール済みの Windows ストアアプリの情報

・プロビジョニング済み Windows ストアアプリの情報

[ソフトウェア検索条件の設定］に登録したソフトウェア

Windows のコントロールパネルの［プログラムと機能］に登録されていないソフトウェアの情報です。設定画面－［ソフトウェア検索条件の設定］画面に登録した条件で、コンピュータ上から実行ファイル（exe ファイルなど）を検索して情報を収集できます。

インストールされている OS

コンピュータにインストールされている OS の情報です。

ソフトウェア検索条件の詳細については、「(11)　情報を収集したいソフトウェアの検索条件の定義」を参照してください。

UNIX エージェントの場合

検索方法によって、収集できるソフトウェア情報は次のようになります。

［リモートインストールしたソフトウェア］を検索

JP1/IT Desktop Manager 2 でインストールしたソフトウェアの情報です。日立プログラムプロダクト、UAP が対象となります。

［すべてのソフトウェア］を検索

日立プログラムプロダクト（JP1/IT Desktop Manager 2 でインストールしたソフトウェア以外）、他社ソフトウェア、OS パッチ情報に加えて、検索リストによる検索結果の情報です。検索リストを使用すると、検索対象に設定した任意のソフトウェアの情報を検索できます。

UNIX エージェントの場合に収集できるソフトウェア情報の詳細については、マニュアル「JP1/IT Desktop Management 2 - Agent(UNIX(R)用) 」を参照してください。

UNIX エージェントのシステム情報とソフトウェア情報の管理については、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。

Mac エージェントの場合

検索方法として［すべてのソフトウェア］を選択でき、Mac にインストール済みのアプリケーションが対象となります。検索リストを使用すると、検索対象に設定した任意のソフトウェアの情報を検索できます。Mac エージェントのシステム情報とソフトウェア情報の管理については、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。

［プログラムと機能］に登録されているソフトウェア、および Windows ストアアプリ

項目	説明	Windows エージェント導入済み	エージェントレス				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
ソフトウェア名	インストールされたソフトウェアの名称です。更新プログラムがグルーピングされている場合は、更新プログラムグループ名が表示されます。	○	○	×	×	×	×	○
バージョン※	インストールされたソフトウェアのバージョンです。	○	○	×	×	×	×	○
メーカー	インストールされたソフトウェアのメーカーです。	○	○	×	×	×	×	○
サポート情報（URL）	インストールされたソフトウェアのサポートのページです。	○	○	×	×	×	×	○

項目	説明	Windows エージェント導入済み	エージェントレス					
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
購入形態	インストールされたソフトウェアの、購入時の形態です。ボリュームライセンス版か製品版かのどちらかが表示されます。	△	△	×	×	×	×	×
プロダクト ID	インストールされたソフトウェアの、Microsoft Office 製品のプロダクト ID です。 機器画面の［ソフトウェア一覧］画面では、購入形態がボリュームライセンス版の場合だけに表示されます。また、［ソフトウェア一覧］画面では、プロダクト ID の下 5 けたがアスタリスクで表示されます。	△	△	×	×	×	×	×
GUID	インストールされたソフトウェアのグローバル一意識別子（GUID）です。	△	△	×	×	×	×	×
ソフトウェア種別	インストールされたソフトウェアの、SAMAC 辞書の情報を基に分類された種別です。SAMAC 辞書の情報をオフライン更新した場合に、有償ソフトウェア、フリーウェアなどの情報が表示されます。 複数サーバ構成の場合、ソフトウェア種別は上位の管理用サーバに通知されません。管理用サーバごとに収集されます。	○	○	×	×	×	×	×
インストール日付	ソフトウェアがインストールされた日付です。	○	○	×	×	×	×	○
インストールフォルダ	ソフトウェアのインストールパスです。	○	○	×	×	×	×	○
Windows ストアアプリ	対象のソフトウェアが Windows ストアアプリかどうかを示す情報です。	○	×	×	×	×	×	○

（凡例）○：収集できる　△：一部のソフトウェアだけ収集できる　×：収集できない

注　インストールしたユーザーの［プログラムと機能］だけに表示されるソフトウェアは、インストールしたユーザーのログイン中にだけ収集されます。

注※　ソフトウェアが JP1 製品の場合、JP1 製品のバージョン形式で収集されます。ただし、ソフトウェアが JP1/TELstaff、JP1/VERITAS、JP1/秘文の場合、または管理対象がエージェントレスの場合については、［プログラムと機能］に表示されるバージョンが収集されます。

上記凡例の△の項目については、次に示す Microsoft Office 製品の場合だけ収集できます。

日本語版の Microsoft Office 製品

製品名	エディション
Microsoft Office	Microsoft Office Enterprise 2007※1
	Microsoft Office Home and Business 2010※2
	Microsoft Office Personal Edition 2003※2
	Microsoft Office Professional Edition 2003※2
	Microsoft Office Professional Enterprise Edition 2003※1
	Microsoft Office Professional 2007
	Microsoft Office Professional 2010※2
	Microsoft Office Professional Plus 2007※1
	Microsoft Office Professional Plus 2010※1
	Microsoft Office Professional Plus 2013※1、※3
	Microsoft Office Professional Plus 2016※1、※3
	Microsoft Office Standard Edition 2003
	Microsoft Office Standard 2007
	Microsoft Office Standard 2010※1
	Microsoft Office Standard 2013※1、※3
	Microsoft Office Standard 2016※1、※3
	Microsoft Office Ultimate 2007※2
Microsoft Lync	Microsoft Lync 2010※1
	Microsoft Lync 2013※1、※3
Microsoft Skype for Business	Microsoft Skype for Business 2016※1、※3
Microsoft Office Access	Microsoft Office Access 2003※4
	Microsoft Office Access 2007
	Microsoft Access 2010
	Microsoft Access 2013※1、※3
	Microsoft Access 2016※1、※3
Microsoft Office Excel	Microsoft Office Excel 2003※4
	Microsoft Office Excel 2007

製品名	エディション
Microsoft Office Excel	Microsoft Excel 2010
	Microsoft Excel 2013※1、※3
	Microsoft Excel 2016※1、※3
Microsoft Office FrontPage	Microsoft Office FrontPage 2003
Microsoft Office Groove	Microsoft Office Groove 2007
Microsoft Office InfoPath	Microsoft Office InfoPath 2007
	Microsoft InfoPath 2010
	Microsoft InfoPath 2013※1、※3
Microsoft Office InterConnect	Microsoft Office InterConnect 2007
Microsoft Office OneNote	Microsoft Office OneNote 2007
	Microsoft OneNote 2010
	Microsoft OneNote 2013※1、※3
Microsoft Office Outlook	Microsoft Office Outlook 2003※4
	Microsoft Office Outlook 2007
	Microsoft Outlook 2010
	Microsoft Outlook 2013※1、※3
	Microsoft Outlook 2016※1、※3
Microsoft Office PowerPoint	Microsoft Office PowerPoint 2003※4
	Microsoft Office PowerPoint 2007
	Microsoft PowerPoint 2010
	Microsoft PowerPoint 2013※1、※3
	Microsoft PowerPoint 2016※1、※3
Microsoft Office Project	Microsoft Office Project Professional 2003
	Microsoft Office Project Professional 2007
	Microsoft Project Professional 2010
	Microsoft Project Professional 2013※1、※3
	Microsoft Project Professional 2016※1、※3
	Microsoft Office Project Standard 2003
	Microsoft Office Project Standard 2007
	Microsoft Project Standard 2010

製品名	エディション
Microsoft Office Project	Microsoft Project Standard 2013※1、※3
	Microsoft Project Standard 2016※1、※3
Microsoft Office Publisher	Microsoft Office Publisher 2003
	Microsoft Office Publisher 2007
	Microsoft Publisher 2010
	Microsoft Publisher 2013※1、※3
	Microsoft Publisher 2016※1、※3
Microsoft Office SharePoint Workspace	Microsoft SharePoint Workspace 2010
Microsoft Office Visio	Microsoft Office Visio 2003 Professional
	Microsoft Office Visio 2003 Standard
	Microsoft Office Visio 2007 Professional
	Microsoft Office Visio 2007 Standard
	Microsoft Visio 2010 Premium
	Microsoft Visio 2010 Professional
	Microsoft Visio 2010 Standard
	Microsoft Visio Professional 2013※1、※3
	Microsoft Visio Professional 2016※1、※3
	Microsoft Visio Standard 2013※1、※3
	Microsoft Visio Standard 2016※1、※3
Microsoft Office Word	Microsoft Office Word 2003※2、※4
	Microsoft Office Word 2007
	Microsoft Word 2010
	Microsoft Word 2013※1、※3
	Microsoft Word 2016※1、※3

注※1　購入形態がボリュームライセンス版の場合だけ収集できます。

注※2　購入形態が製品版の場合だけ収集できます。

注※3　プロダクト ID は収集できません。

注※4　購入形態は収集できません。

英語版または中国語版の Microsoft Office 製品

製品名	エディション
Microsoft Office	Microsoft Office Enterprise 2007
	Microsoft Office Professional 2007
	Microsoft Office Professional Plus 2007
	Microsoft Office Professional Plus 2010
	Microsoft Office Professional Plus 2013※1、※2
	Microsoft Office Professional Plus 2016※1、※2
	Microsoft Office Standard 2007
	Microsoft Office Standard 2010
	Microsoft Office Standard 2013※1、※2
	Microsoft Office Standard 2016※1、※2
Microsoft Lync	Microsoft Lync 2010
	Microsoft Lync 2013※1、※2
Microsoft Skype for Business	Microsoft Skype for Business 2016※1、※3
Microsoft Office Access	Microsoft Office Access 2007
	Microsoft Access 2010
	Microsoft Access 2013※1、※2
	Microsoft Access 2016※1、※2
Microsoft Office Excel	Microsoft Office Excel 2007
	Microsoft Excel 2010
	Microsoft Excel 2013※1、※2
	Microsoft Excel 2016※1、※2
Microsoft Office Groove	Microsoft Office Groove 2007
Microsoft Office InfoPath	Microsoft Office InfoPath 2007
	Microsoft InfoPath 2010
	Microsoft InfoPath 2013※1、※2
Microsoft Office OneNote	Microsoft Office OneNote 2007
	Microsoft OneNote 2010
	Microsoft OneNote 2013※1、※2
Microsoft Office Outlook	Microsoft Office Outlook 2007
	Microsoft Outlook 2010

製品名	エディション
Microsoft Office Outlook	Microsoft Outlook 2013※1、※2
	Microsoft Outlook 2016※1、※2
Microsoft Office PowerPoint	Microsoft Office PowerPoint 2007
	Microsoft PowerPoint 2010
	Microsoft PowerPoint 2013※1、※2
	Microsoft PowerPoint 2016※1、※2
Microsoft Office Project	Microsoft Office Project Professional 2007
	Microsoft Project Professional 2010
	Microsoft Project Professional 2013※1、※2
	Microsoft Project Professional 2016※1、※2
	Microsoft Office Project Standard 2007
	Microsoft Project Standard 2010
	Microsoft Project Standard 2013※1、※2
	Microsoft Project Standard 2016※1、※2
Microsoft Office Publisher	Microsoft Office Publisher 2007
	Microsoft Publisher 2010
	Microsoft Publisher 2013※1、※2
	Microsoft Publisher 2016※1、※2
Microsoft Office SharePoint Workspace	Microsoft SharePoint Workspace 2010
Microsoft Office Visio	Microsoft Office Visio 2007 Professional
	Microsoft Office Visio 2007 Standard
	Microsoft Visio 2010 Premium
	Microsoft Visio 2010 Professional
	Microsoft Visio 2010 Standard
	Microsoft Visio Professional 2013※1、※2
	Microsoft Visio Professional 2016※1、※2
	Microsoft Visio Standard 2013※1、※2
	Microsoft Visio Standard 2016※1、※2
Microsoft Office Word	Microsoft Office Word 2007
	Microsoft Word 2010

製品名	エディション
Microsoft Office Word	Microsoft Word 2013※1、※2
	Microsoft Word 2016※1、※2

注※1　購入形態がボリュームライセンス版の場合だけ収集できます。

注※2　プロダクト ID は収集できません。

［ソフトウェア検索条件の設定］に登録したソフトウェア

項目	説明	Windows エージェント導入済み	エージェントレス					
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
ソフトウェア名	インストールされたソフトウェアの名称です。更新プログラムがグルーピングされている場合は、更新プログラムグループ名が表示されます。	○	×	×	×	×	×	×
バージョン	インストールされたソフトウェアのバージョンです。	○	×	×	×	×	×	×
メーカー	インストールされたソフトウェアのメーカーです。	○	×	×	×	×	×	×
インストール日付	ソフトウェアがインストールされた日付です。	○	×	×	×	×	×	×
インストールフォルダ	ソフトウェアのインストールパスです。	○	×	×	×	×	×	×

（凡例）○：収集できる　×：収集できない

インストールされている OS

項目	説明	Windows エージェント導入済み	エージェントレス					
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
ソフトウェア名	インストールされたソフトウェアの名称です。	○	○	×	×	×	×	○
バージョン	インストールされたソフトウェアのバージョンです。	○	○	×	×	×	×	○
メーカー	インストールされたソフトウェアのメーカーです。	○	○	×	×	×	×	○

項目	説明	Windows エージェント導入済み	エージェントレス					
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
インストール日付	ソフトウェアがインストールされた日付です。	○	○	×	×	×	×	○
インストールフォルダ	ソフトウェアのインストールパスです。	○	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

(6) セキュリティ情報

セキュリティ情報として収集できる情報について説明します。セキュリティ情報では、次に示す情報を収集できます。

- 更新プログラム情報
- ウィルス対策製品情報
- サービスのセキュリティ設定情報
- OS のセキュリティ設定情報
- 秘文情報
- BitLocker ドライブ暗号化情報

なお、SNMP 認証の場合は、収集できる機器情報はコンピュータにインストールされている SNMP エージェントに依存します。そのため、一部の機器情報が収集できないことがあります。

更新プログラム情報

項目	説明	エージェント導入済み			エージェントレス					
		Windows	UNIX	MacOS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
自動更新※1	自動更新の有効/無効の情報です。	○	×	○	○	×	×	×	×	○
適用済みの更新プログラム※2	適用済み更新プログラムの個数です。	○	×	×	○	×	×	×	×	○

項目	説明	エージェント導入済み			エージェントレス					
		Windows	UNIX	Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
文書番号（適用日付）※3	適用済み更新プログラムの名称、および更新プログラムを適用した日付です。	○	×	×	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

注※1　Windows の場合、OS の「Workstation」サービスが起動しているときに収集されます。

また、自動更新は Windows の場合、次の条件をすべて満たしていると有効と表示されます。

- コントロールパネルの［Windows Update］－［設定の変更］－［重要な更新プログラム］の設定で［更新プログラムを自動的にインストールする］を選択している。
- 「Windows Update」サービスが起動している。ただし、エージェントの OS が Windows 10、Windows Server 2019、または Windows Server 2016 の場合は、「Windows Update」サービスのスタートアップの種類が「自動」または「手動」である。

注※2　適用済み更新プログラムが削除されても、セキュリティの監視間隔の最大 3 回まで情報の更新を保留します。これは、一時的に更新プグラムが取得できなくなったケースでの誤判定の防止を目的としています。

また、取得可能であった適用済み更新プログラムがすべて取得できなくなった場合、情報の取得に失敗したと判断し、取得済みの適用済み更新プログラムの情報は削除しません。

注※3　適用日付の情報を取得できなかった場合は、「-」が表示されます。

ウィルス対策製品情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
製品名	ウィルス対策製品の名称です。	○	×	○	×	×	×	×	×
バージョン	ウィルス対策製品のバージョンです。	○	×	○	×	×	×	×	×
インストール日付	ウィルス対策製品のインストール日付です。	△	×	△	×	×	×	×	×

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIXまたはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
エンジンバージョン	ウィルス対策製品の検索エンジンのバージョンです。	△	×	△	×	×	×	×	×
ウィルス定義ファイルのバージョン	ウィルス対策製品が使用している定義ファイルのバージョン（日付）です。	△	×	△	×	×	×	×	×
自動保護（常駐設定）	ウィルス対策製品の自動保護（常駐/非常駐）の設定です。	△	×	△	×	×	×	×	×
ウィルススキャン最終完了日時	最近のウィルススキャンが完了した日時です。	△	×	△	×	×	×	×	×

（凡例）○：収集できる　△：一部の製品では収集できない　×：収集できない

収集できるウィルス対策製品情報については、「(14)　サポートするウィルス対策製品」を参照してください。

サービスのセキュリティ設定情報

項目	説明	エージェント導入済み※		エージェントレス					
		Windows	UNIXまたはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
サービスのセキュリティ設定情報	セキュリティポリシーで禁止されている Windows サービスのうち、稼働しているサービスの表示名です。	○	×	×	×	×	×	×	×

（凡例）○：収集できる　×：収集できない

注　OS の「Workstation」サービスが起動している場合に収集されます。この機能で管理できるサービスの上限数は 30 です。

注※　オンライン管理の場合だけ収集できます。

OS のセキュリティ設定情報

項目		説明	エージェント導入済み			エージェントレス					
			Windows	UNIX	Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
アカウント情報※1	アカウント名	ローカルアカウント名称です。アカウント名ごとに、アカウント情報が取得されます。	○	×	○	○	×	×	×	×	○
	パスワード更新からの経過日数	パスワードを更新してからの経過日数です。 なお、無効および期限切れのアカウント、次回ログオン時にパスワードの変更が必要なアカウントについては、パスワードの経過日数は取得されません。	○	×	○	○	×	×	×	×	○
	パスワードの安全性※2	パスワードの安全性の高さです。 安全性が低いとされるパスワードは，エージェントのパスワード定義ファイル（jdng_security.xml）で設定できます。詳細は、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の、安全性が低いとされるパスワードのカスタマイズについての説明を参照してください。	○	×	×	○	×	×	×	×	○
	無期限パスワード	無期限パスワードの設定の有効/無効の情報です。	○	×	×	○	×	×	×	×	○
パワーオンパスワード※3		パワーオンパスワードの設定の有効/無効の情報です。	○	×	×	○	×	×	×	×	○
Guest アカウント		Guest アカウントの設定の有効/無効の情報です。	○	×	○	○	×	×	×	×	○
自動ログオン		自動ログオンの設定の有効/無効の情報です。	○	×	○	○	×	×	×	×	○
共有フォルダ		共有フォルダの有無です。	○	×	×	○	×	×	×	×	○
管理共有		管理共有の有効/無効の情報です。	○	×	×	○	×	×	×	×	○

項目		説明	エージェント導入済み			エージェントレス					
			Windows	UNIX	MacOS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
DCOM		DCOMの有効/無効の情報です。	○	×	×	○	×	×	×	×	○
匿名接続		匿名接続での情報取得の有効/無効の情報です。	○	×	×	○	×	×	×	×	○
スクリーンセーバー情報※4	アカウント名	Windowsのローカルアカウント名称です。アカウント名ごとに、スクリーンセーバー情報が取得されます。	○	×	×	○※5	×	×	×	×	○
	スクリーンセーバー	スクリーンセーバーの設定の有効/無効の情報です。	○	×	×	○※5	×	×	×	×	○
	パスワードによる保護	スクリーンセーバーのパスワードによる保護の有効/無効の情報です。	○	×	○※6	○※5	×	×	×	×	○
	起動待ち時間	スクリーンセーバーが起動するまでの待ち時間です。	○	×	×	○※5	×	×	×	×	○
ファイアウォール		ファイアウォールの設定の有効/無効の情報です。	○	×	○	○	×	×	×	×	○
リモートデスクトップ		リモートデスクトップ設定の有効/無効の情報です。	○	×	×	○	×	×	×	×	○

(凡例)○:収集できる　×:収集できない

注　Windowsの場合、OSの「Workstation」サービスが起動しているときに収集されます。

注※1　この機能で管理できるアカウント情報の上限ユーザー数は60です。

ドメインアカウントの場合、パスワードの情報が取得されないことがあります。

また、アカウント情報の上限ユーザー数は、アカウント名とパスワードの情報が取得されたユーザーのユーザー数が対象となります。

注※2　次のどれかの条件に該当するパスワードである場合、パスワードの安全性が「低い」と判定されます。

- 空白の場合
- ユーザーアカウント名と完全一致の場合

- ユーザーアカウント名と同じ文字列を、小文字だけ、大文字だけ、または先頭だけ大文字で表現したパスワードの場合
- コンピュータ名と同じ文字列を、小文字だけ、大文字だけ、または先頭だけ大文字で表現したパスワードの場合
- 「password」、「PASSWORD」、または「Password」の場合
- 「admin」、「ADMIN」、または「Admin」の場合
- 「administrator」、「ADMINISTRATOR」、または「Administrator」の場合

また、無効、期限切れ、ロック状態、または次回ログオン時にパスワードの変更が必要なユーザーアカウントについては、パスワードの安全性は判定されません。

ユーザーアカウントのパスワードの安全性が低い場合、セキュリティ状況が判定されるとパスワードの最終更新日時が変更されます。ただし、パスワードは変更されません。

Windows の管理ツールのローカルセキュリティポリシー（ローカル環境，ドメイン環境）の設定で，［ローカルポリシー］－［監査ポリシー］の［アカウント管理の監査］を有効にしている場合，インベントリ取得時にイベントログが複数出力される場合があります。

注※3　パワーオンパスワードは BIOS の「Power-On Password」で設定されている情報を意味しています。ハードディスクパスワードではありません。機種によってはパワーオンパスワードの情報が取得できずに、「未実装」または「不明」と表示されることがあります。

注※4　ログイン中のユーザーのスクリーンセーバー情報が収集され、最後にログインしてから 30 日間保持されます。なお、この機能で管理できるスクリーンセーバー情報の上限ユーザー数は 60 です。

注※5　管理共有による機器情報の収集時に Windows にログオンしているユーザーの情報だけを取得します。

注※6　Mac OS の場合、ユーザーアカウントごとの判定結果ではなく、全ユーザーアカウントの判定結果になります。

秘文情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
製品名	インストールされている製品※1 の正式名称です。	○	×	×	×	×	×	×	×
バージョン	インストールされている製品のバージョンです。	○	×	×	×	×	×	×	×

項目		説明	エージェント導入済み		エージェントレス					
			Windows	UNIXまたはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
パッチバージョン		インストールされている製品のパッチ情報です。	○	×	×	×	×	×	×	×
ログインユーザー ID		最後に秘文製品にログインしたユーザーのユーザー ID です。	○ ※2	×	×	×	×	×	×	×
ログイン日時		最後に秘文製品にログインした日時です。	○ ※2	×	×	×	×	×	×	×
ログアウト日時		最後に秘文製品からログアウトした日時です。	○ ※2	×	×	×	×	×	×	×
秘文DE(FS)ログイン情報	ログインユーザー ID	最後に秘文ファイルサーバにログインしたユーザーのユーザー ID です。	○ ※3	×	×	×	×	×	×	×
	ログイン日時	最後に秘文ファイルサーバにログインした日時です。	○ ※3	×	×	×	×	×	×	×
	ログアウト日時	最後に秘文ファイルサーバからログアウトした日時です。	○ ※3	×	×	×	×	×	×	×
ドライブ		ローカルドライブです。	○ ※2、※4	×	×	×	×	×	×	×
暗号化状態		ドライブの暗号化の状態です。	○ ※2、※4	×	×	×	×	×	×	×

(凡例) ○：収集できる　×：収集できない

注　エージェント導入済みのコンピュータにインストールされている秘文のバージョンが 09-00 以降の場合に、収集できます。

注※1　バージョンが 9 までの秘文は次に示す製品が判別されますが、バージョン 10 以降は判別されません。

- JP1/秘文 IC と秘文 IC
- JP1/秘文 IF と秘文 IF

- JP1/秘文 IF Mail Option と秘文 IF Mail Option
- JP1/秘文 IS と秘文 IS

注※2　JP1/秘文 IF Mail Option、秘文 IF Mail Option、および秘文 DP の場合は表示されません。

注※3　秘文 DE の場合に表示されます。

注※4　JP1/秘文 IC、秘文 IC、および秘文 DE の場合に表示されます。

BitLocker ドライブ暗号化情報

項目	説明	エージェント導入済み		エージェントレス					
		Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
暗号化状態	ドライブの暗号化の状態です。	○	×	○	×	×	×	×	○

（凡例）○：収集できる　×：収集できない

(7)　資産情報と機器情報の共通管理項目

項目	説明	入力方法/データ型（デフォルト）	エージェント導入済み		エージェントレス					
			Windows	UNIX または Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
部署	コンピュータの利用者の部署です。	管理者による入力/階層型	○	×	×	×	×	○	×	○
設置場所	コンピュータの設置場所です。	管理者による入力/階層型	○	×	×	○ ※	×	○	×	○
利用者名	コンピュータの利用者の氏名です。	管理者による入力/テキスト型	○	×	×	×	×	○	×	○
アカウント	コンピュータの利用者のアカウント名です。	管理者による入力/テキスト型	○	×	×	×	×	○	×	○
メールアドレス	コンピュータの利用者のメールアドレスです。	管理者による入力/テキスト型	○	×	×	×	×	○	×	○

項目	説明	入力方法/データ型（デフォルト）	エージェント導入済み		エージェントレス					
			Windows	UNIXまたはMac OS	管理共有	SNMP	ARP/ICMP	Active Directory	MDM	API
電話番号	コンピュータの利用者の電話番号です。	管理者による入力/テキスト型	○	×	×	×	×	○	×	○

（凡例）○：収集できる　×：収集できない

注※　SNMP エージェントに設置場所の情報が設定されている場合に収集されます。

(8)　機器状態の種類と表示条件

機器状態	表示条件
稼働中	現在時刻が最終確認日時からポーリング間隔＋ 10 分以内。
停止中	次のような場合に表示される。 • 現在時刻が最終確認日時からポーリング間隔＋ 10 分を超過している。 • オフライン管理のコンピュータの機器情報を、初めて取得した。※1
警告	次のような場合に表示される。 • ネットワークモニタを有効化したエージェントで、現在時刻が最終確認日時からポーリング間隔＋ 10 分を超過している。 • オフライン管理しているネットワークモニタを有効化したコンピュータの機器情報を、初めて取得した。※2 • エージェントレスのコンピュータの場合に認証ができていない。 • 機器種別が「プリンタ」の場合に、SNMP によって警告状態であると判別された。（例）トナーの残量が少ない。
障害	機器種別が「プリンタ」の場合に、SNMP によって利用できない状態であると判別された。（例）用紙切れ。
不明	次のような場合に表示される。 • 機器の状態に関する情報を収集できない。 • オフライン管理のコンピュータの機器情報を、初めて取得した。※1
配下の管理用サーバによる管理	複数サーバ構成の場合で、直下の機器以外。

注

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エージェントのように、機器状態が複数検知されるコンピュータでは、操作画面に表示される機器状態は次の流れで決まります。

1. 重要度が最も高い機器状態が表示される（重要度：障害＞警告＞停止中＞稼働中＞不明）。

2. 機器状態の重要度が同じになる場合は、システム構成要素の重要度が最も高い機器状態が表示される（重要度：エージェント＞ネットワークモニタエージェント）。

注※1

コンフィグレーションファイル（jdn_manager_config.conf）の OfflineRegistration_StatusUnknown プロパティにON が設定されている場合、機器状態は「不明」になります。それ以外は「停止中」になります。

2 回目以降に取得したときは、それまでに表示されていた機器状態が維持されます。ただし、コンフィグレーションファイル（jdn_manager_config.conf）の OfflineRegistration_StatusUnknown プロパティにON が設定されている場合、機器状態は「不明」になります。

注※2

2 回目以降に取得したときは、それまでに表示されていた機器状態が維持されます。

(9) 機器情報の収集タイミング

オンライン管理用のエージェントからは、エージェント設定に設定されている監視間隔に従って定期的に機器情報が収集されます。オンライン管理用のエージェントで機器情報の更新が検知された場合は、機器情報が管理用サーバに通知されます。更新がなかった場合は通知されません。

管理用サーバに通知される機器情報を次に示します。

検知項目		通知情報	監視間隔
ホスト識別子		すべての機器情報※1	監視間隔（セキュリティ項目以外）（分）
接続する管理用サーバ		すべての機器情報※2	監視間隔（セキュリティ項目以外）（分）
システム情報		検知した項目の全情報	監視間隔（セキュリティ項目以外）（分）※3
ハードウェア情報		検知した項目の全情報	監視間隔（セキュリティ項目以外）（分）
インストールソフトウェア情報		検知した項目の追加、削除、変更情報	監視間隔（セキュリティ項目）（分）※4
セキュリティ情報	自動更新	検知した項目の全情報	監視間隔（セキュリティ項目）（分）
	ウィルス対策製品情報	検知した項目の全情報	監視間隔（セキュリティ項目）（分）
	サービスのセキュリティ設定情報	検知した項目の全情報	監視間隔（セキュリティ項目）（分）
	OS のセキュリティ設定情報	検知した項目の全情報	監視間隔（セキュリティ項目）（分）
秘文情報		検知した項目の全情報	監視間隔（セキュリティ項目以外）（分）

検知項目		通知情報	監視間隔
BitLocker ドライブ暗号化情報		検知した項目の全情報	監視間隔（セキュリティ項目以外）（分）
共通管理項目	利用者入力	検知した項目のすべての機器情報	利用者の入力が完了したとき
追加管理項目			

注※1　ホスト識別子が変更された場合、エージェントがインストールされている機器が変更されたと判断し、すべての情報が通知されます。

注※2　接続する管理用サーバが変更された場合、変更後の管理用サーバにすべての情報が通知されます。なお、変更前の管理用サーバからの指示は引き継ぎます。

注※3 「コンピュータ情報」の「システムドライブ」の「空き容量」は、24 時間に 1 回の頻度で変更を検知します。

注※4　ソフトウェア検索で発見されたインストールソフトウェア情報は、24 時間に 1 回の頻度で変更を検知します。

(10)　ソフトウェア情報の取得

管理対象のコンピュータからソフトウェア情報を取得できます。ソフトウェア情報は、機器情報と同時に収集され、機器画面の［ソフトウェア情報］画面でソフトウェア名とバージョンごとに確認できます。なお、UNIX エージェント、Mac エージェントの場合、管理対象となる際の自動通知のほかに、「コンピュータ(UNIX)のソフトウェア情報の取得」ジョブの実行によっても、ソフトウェア情報を収集できます。

ヒント

管理対象のコンピュータにソフトウェアが追加されると、イベントが出力されます。イベントをメール通知するように設定しておくと、管理対象のコンピュータにソフトウェアが追加されたことをメールで確認できます。

また、管理対象のコンピュータに、JP1/IT Desktop Management 2 に登録されていないソフトウェアが追加された場合は、ホーム画面の［通知事項］パネルでも、ソフトウェアが新たに発見されたことを確認できます。新たに発見されたソフトウェアの一覧は、機器画面の［サマリ］－［ダッシュボード］画面に表示される［新規発見ソフトウェア］パネルで確認できます。なお、［新規発見ソフトウェア］パネルは、画面上部の［表示］メニュー－［パネルのレイアウト設定］から、ホーム画面に表示できるように設定できます。

ヒント

機器画面の［ソフトウェア情報］－［ソフトウェア一覧］で表示されるソフトウェアは、エージェントがインストールしているコンピュータからソフトウェア情報を取得し表示されます。なお、［ソフトウェア一覧］の［インストール数］は管理対象のコンピュータが対象のため、発

見した機器や除外対象機器からもソフトウェア情報を取得しますが、インストール数には計上されません。

ソフトウェア情報には次の種類があります。それぞれのソフトウェア情報で収集できる項目については、「(5)　インストールソフトウェア情報」を参照してください。

Windows エージェントの場合

[プログラムと機能]に登録されているソフトウェア

Windows のコントロールパネルの［プログラムと機能］に登録されているソフトウェアの情報です。エージェント導入済みのコンピュータ、またはエージェントレスで管理共有の認証ができているコンピュータの場合に収集されます。

[ソフトウェア検索条件の設定]に登録したソフトウェア

Windows のコントロールパネルの［プログラムと機能］に登録されていないソフトウェアの情報です。設定画面－［ソフトウェア検索条件の設定］画面に登録した条件で、コンピュータ上から実行ファイル（exe ファイルなど）を検索して情報を収集できます。エージェント導入済みのコンピュータからだけ収集できます。

なお、ソフトウェアの検索は、コンピュータの起動時および起動から 24 時間ごとに実行されます。 コンピュータのすべてのローカルドライブからソフトウェアが検索され、ソフトウェア検索条件と一致するソフトウェアを発見した場合に情報が取得されます。

インストールされている OS の情報

対象のコンピュータにインストールされている OS の情報です。エージェント導入済みのコンピュータ、またはエージェントレスで管理共有の認証ができているコンピュータの場合に収集されます。

重要

エージェントまたはエージェントレスの OS が Windows 7 の場合、Windows XP モードでインストールしたインストールソフトウェアは情報を取得できません。

UNIX エージェントの場合

検索方法によって、収集できるソフトウェア情報は次のようになります。

[リモートインストールしたソフトウェア]

JP1/IT Desktop Manager 2 でインストールしたソフトウェアの情報です。日立プログラムプロダクト、UAP が対象となります。

[すべてのソフトウェア]

日立プログラムプロダクト（JP1/IT Desktop Manager 2 でインストールしたソフトウェア以外）、他社ソフトウェア、OS パッチ情報に加えて、検索リストによる検索結果の情報です。検索リストを使用すると、検索対象に設定した任意のソフトウェアの情報を検索できます。

UNIX エージェントのソフトウェア情報取得の詳細については、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」を参照してください。

Mac エージェントの場合

検索方法として［すべてのソフトウェア］を選択でき、Mac にインストール済みのアプリケーションが対象となります。検索リストを使用すると、検索対象に設定した任意のソフトウェアの情報を検索できます。Mac エージェントのソフトウェア情報取得の詳細については、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」を参照してください。

ソフトウェア検索条件の設定

ソフトウェアの検索条件には、検索対象の実行ファイル名を指定します。

同じ実行ファイル名で複数のソフトウェア検索条件は作成できません。複数サーバ構成の場合、ほかの管理用サーバの検索条件と重複しても問題ありません。

Windows のコントロールパネルの［プログラムと機能］に同じソフトウェア名が存在する場合は、ソフトウェアの検索で取得されたソフトウェア情報は登録されません。

ソフトウェアの検索で、異なるフォルダに同じファイル名のソフトウェアを複数発見した場合は、それぞれのソフトウェア情報が取得されます（同じソフトウェア名のソフトウェア情報が複数登録されます）。それぞれのソフトウェア情報は、インストールパスで区別されます。

ソフトウェアが複数の検索条件と一致した場合は、該当のソフトウェアが異なるソフトウェア情報としてそれぞれ取得されます。

ソフトウェア検索条件を定義するには、設定画面から直接追加するか、ソフトウェア検索条件一覧をインポートします。定義したソフトウェア検索条件は、エージェント導入済みのすべてのコンピュータに適用されます。コンピュータごとに異なるソフトウェア検索条件を定義することはできません。ソフトウェア検索条件の設定方法については、「(11)　情報を収集したいソフトウェアの検索条件の定義」を参照してください。

インストール済みコンピュータの表示

管理対象のコンピュータからソフトウェア情報が収集されると、ソフトウェアをインストールしたコンピュータ（インストール済みコンピュータ）の一覧を確認できます。インストール済みコンピュータは、［ソフトウェア情報］画面の［インストール済みコンピュータ］タブで確認できます。

［インストール済みコンピュータ］タブで確認できる項目を次の表に示します。

項目	説明
ホスト名	ソフトウェアをインストールしている管理対象のコンピュータのホスト名です。
メーカー	ソフトウェアをインストールしている管理対象のコンピュータのメーカーです。
IP アドレス	ソフトウェアをインストールしている管理対象のコンピュータの IP アドレスです。
OS	ソフトウェアをインストールしている管理対象のコンピュータの OS です。

項目	説明
利用者名	ソフトウェアをインストールしている管理対象のコンピュータの利用者の氏名です。
登録日時	ソフトウェアをインストールしている管理対象のコンピュータが登録された日時です。
インストール日付	管理対象のコンピュータでソフトウェアがインストールされた日時です。

検索リストを利用した UNIX エージェント、Mac エージェントのソフトウェア情報の取得

「コンピュータ（UNIX）のソフトウェア情報の取得」ジョブ作成時に検索対象ソフトウェアとして［すべてのソフトウェア］を指定したジョブでは、検索リストを利用して UNIX エージェント、Mac エージェントにインストールされているソフトウェアを検索できます。ソフトウェア検索リストは、マネージャに保存されている検索リスト、またはエージェントに保存されている検索リストのどちらかを使用します。

- エージェントに存在する検索リスト

  前回検索リストを使用してソフトウェア検索した時に、エージェント側に保存された検索リストです。
- ユーザ指定検索リスト

  検索対象にするソフトウェアを任意に登録できる、マネージャに保存される検索リストです。検索する UNIX エージェント、Mac エージェントの範囲ごとに作成したり、UNIX エージェント、Mac エージェントの OS ごとに作成したり、複数作成できます。

ユーザ指定検索リストの作成方法については、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。

Windows ストアアプリの注意事項

- Windows ストアアプリの情報取得は、OS に初期状態から入っているものも取得します。
  - OS に初期状態から入っている Windows ストアアプリにはスタートメニューやタイルに表示されないものもありますが、JP1/IT Desktop Management 2 は情報を取得します。
  - OS に初期状態から入っている Windows ストアアプリをアンインストールしても、JP1/IT Desktop Management 2 は情報を取得します。
- 同一の機器で、あるユーザーが Windows ストアアプリをアップデートしても、その Windows ストアアプリを使用している他のユーザーがアップデートしていない場合、アップデート前後の Windows ストアアプリの情報を取得します。
- JP1/IT Desktop Management 2 で取得する Windows ストアアプリのソフトウェア名は、スタートメニューやタイルから確認できる Windows ストアアプリのソフトウェア名とは異なることがあります。Windows ストアアプリの資産管理やセキュリティ判定を行う場合は、JP1/IT Desktop Management 2 - Manager に表示されているソフトウェア名を設定してください。
- 表示言語によってソフトウェア名が変わる Windows ストアアプリがあります。Windows ストアアプリの資産管理やセキュリティ判定を行う場合は、管理対象機器の OS の表示言語に合わせたソフトウェア名を設定してください。

(11) 情報を収集したいソフトウェアの検索条件の定義

ソフトウェアライセンスの利用状況を把握したり、セキュリティポリシーで使用禁止ソフトウェアまたは使用必須ソフトウェアの導入状況を監視したり、コンピュータにインストールされているソフトウェアを把握したりするためには、管理対象のコンピュータからソフトウェア情報を収集する必要があります。

ソフトウェア情報の収集方法は、ソフトウェアの種類によって次のように異なります。

Windows の［プログラムと機能］に登録されているソフトウェア、および Windows ストアアプリ

エージェント導入済みのコンピュータ、またはエージェントレスで管理共有の認証ができているコンピュータの場合に、ソフトウェア情報が自動的に収集されます。

Windows の［プログラムと機能］に登録されていないソフトウェア

ソフトウェア検索条件を定義することで、エージェント導入済みのコンピュータだけからソフトウェア情報を収集できるようになります。

ソフトウェア検索条件を定義すると、指定した条件に基づいて、コンピュータ上のソフトウェアを検索します。ソフトウェアを発見できると、ソフトウェア情報が収集されます。なお、ソフトウェアの検索は、コンピュータの起動時および起動から 24 時間ごとに実行されます。

ソフトウェアの名称変更やバージョンアップに伴って、検索条件を変更する必要がある場合は、ソフトウェア検索条件を編集します。

複数のソフトウェア検索条件を編集する場合、ソフトウェア検索条件をエクスポートしたあとで、編集してからインポートすることで一括更新できます。複数サーバ構成の場合、上位の管理用サーバから適用された検索条件は、エクスポートの対象になりません。

ソフトウェアの管理が不要になった場合に、不要なソフトウェア検索条件を削除できます。

(12) 利用者情報の取得

エージェント導入済みのコンピュータに利用者情報の入力画面を表示して、利用者が入力した利用者情報を取得できます。部署名や資産管理番号など、JP1/IT Desktop Management 2 で自動的に収集できない情報を取得できるため、管理者が情報を入力する手間を軽減できます。

取得できる利用者情報には、次の 2 種類があります。

資産情報と機器情報の共通管理項目

機器情報とハードウェア資産情報で共通で利用される情報です。

ハードウェア資産情報の追加管理項目

ハードウェア資産情報に管理者が任意に追加した資産管理項目です。

設定画面では、利用者が利用者情報の入力を開始できる日時を指定できます。日時を指定すると、指定した日時を経過するまでは、利用者情報を入力できなくなります。利用者のコンピュータのローカルタイム

が指定した日時になると、バルーンヒントが表示されて、利用者情報を入力できるようになります。バルーンヒントの表示設定は、エージェント設定の［利用者への通知設定］で選択できます。

また、オンライン管理用のエージェントを導入済みのコンピュータの場合、スケジュールを設定して定期的に利用者情報を取得することもできます。

(13)　レジストリ情報の取得

機器情報とハードウェア資産情報の共通項目、およびハードウェア資産情報の追加管理項目では、コンピュータのレジストリ情報を取得できます。レジストリ情報を取得することで、ユーザー固有の情報を管理したり、アプリケーションが独自に定義する情報を管理したりできます。なお、レジストリ情報は、エージェント導入済みのコンピュータからだけ取得できます。

レジストリ情報を取得するためには、設定画面の［資産管理項目の設定］画面で項目の入力方法を変更する必要があります。

レジストリ情報を取得するときは、レジストリのルートキーとパスを指定する必要があります。指定できるルートキーを次に示します。

- HKEY_CURRENT_USER※
- HKEY_LOCAL_MACHINE
- HKEY_CLASSES_ROOT
- HKEY_USERS
- HKEY_CURRENT_CONFIG

注※　HKEY_CURRENT_USER のレジストリ値を指定した場合、コンソールセッションのユーザーの値が取得されます。

レジストリ値は、データ種別に応じて形式が変換されて取得されます。データの種別ごとのレジストリ値の取得方法を次の表に示します。

データ種別	取得方法
REG_SZ、REG_EXPAND_SZ	文字列がそのまま取得されます。
REG_MULTI_SZ	複数の文字列が「,」（コンマ）で連結され、文字列として取得されます。（例）xxx,yyy,zzz
REG_DWORD※1	数値が 10 進数の文字列として取得されます。
REG_BINARY、REG_QWORD※2	バイナリ値を 1 バイトずつ 16 進数の文字列に変換します。その文字列がスペースで連結され、文字列として取得されます。（例）xx yy zz

注※1　データ種別が REG_DWORD_BIG_ENDIAN の場合は取得されません。

(14)　機器情報の更新

管理用サーバで管理される機器情報は、管理対象のコンピュータから収集された情報で更新されます。

機器情報は、取得方法によって更新の優先順位があります。例えば、エージェント導入済みのコンピュータは、エージェントによって取得された機器情報で更新されるため、SNMP によって取得された機器情報では更新されません。更新の優先順位を次に示します。

1. エージェントによって取得された機器情報※1
2. Windows の管理共有によって取得された機器情報
3. API によって取得された機器情報※3
4. SNMP によって取得された機器情報
5. Active Directory によって取得された機器情報
6. MDM 連携によって取得された機器情報
7. ARP によって取得された機器情報
8. ICMP によって取得された機器情報（存在確認だけ）
9. 管理者によって入力された機器情報※2

注※1　オンライン管理のコンピュータから通知した、オフライン管理のコンピュータ（UNIX エージェント、Mac エージェントは除く）の機器情報も含みます。

注※2　機器情報の［機器種別］は、管理者による入力が最優先になります。複数サーバ構成の場合に、管理者が手動で機器情報を更新したのとほぼ同時に機器情報が機器から収集されると、機器情報が管理元の管理用サーバと上位の管理用サーバ間で不一致になることがあります。機器情報が不一致になったときは、もう一度機器情報を手動で更新してください。

注※3　API によって取得された機器情報の更新の優先順位は、コンフィグレーションファイル（jdn_manager_config.conf）の`RestAPIInventoryUpdatePriorityLow`プロパティに設定する値で変更できます。`RestAPIInventoryUpdatePriorityLow`プロパティの詳細については、「付録 A.5　プロパティ一覧」を参照してください。

なお、機器情報が更新されるかどうかは、登録済みの機器情報と取得方法の組み合わせによって決定されます。登録済みの機器情報と取得方法による機器情報の更新の関係を次の表に示します。

機器情報の取得方法		登録済みの機器情報		
		管理者が入力	機器からの情報取得	未取得
管理者が入力		○ ※1	○	○
機器からの情報取得	情報取得	○ ※2	○	○
	値なしで取得	×	○ ※3	○ ※3

機器情報の取得方法		登録済みの機器情報		
		管理者が入力	機器からの情報取得	未取得
機器からの情報取得	未取得または前回と同じ	×	×	×

（凡例）○：機器情報が更新される　×：機器情報は更新されない

注※1　管理者が入力できる項目は、[ホスト名]、[IP アドレス]、[サブネットマスク]、[OS]、[機器種別]です。

注※2　[機器種別]は、管理者による入力が最優先になります。管理者が入力している場合は、機器から取得した情報では更新されません。

注※3　[ホスト名]が値なしの場合、ホスト識別子で機器情報が更新されます。

ヒント

複数のネットワーク情報を持っている機器から機器情報が収集された場合、複数の機器が機器情報の更新対象になることがあります。この場合、機器の台数を実態と合わせるために、収集された機器情報の最初のネットワーク情報と一致する機器だけが更新対象になります。そのほかのネットワーク情報と一致した機器は削除されます。このとき、削除された機器のエージェントの配信の配信日時および配信完了日時は、残っている機器情報に集約されます。

(15)　機器情報の更新時に取得される情報

定期的な機器の探索および手動で、機器情報を更新する場合に、取得される機器情報を次に示します。

- 機器種別
- システム情報
- ハードウェア情報
- インストールソフトウェア情報
- 更新プログラム情報
- ウィルス対策製品情報
- サービスのセキュリティ設定情報
- OS のセキュリティ設定情報
- 秘文情報
- BitLocker ドライブ暗号化情報
- 機器情報とハードウェア資産情報の共通管理項目の情報
- 追加管理項目の情報

(16) 機器情報の更新時に発生するイベント

特定の機器情報が更新される際に、機器情報の変更、追加、または削除があった場合、イベント画面に該当のイベントが発行されます。

イベント発行の対象を次の表に示します。

機器情報の項目		事象	イベント発行の契機
ハードウェア情報	メモリ情報の容量	変更	更新前と更新後でデータが変化したとき。
ハードディスク	ハードディスク情報の次の項目が対象となります。 • ディスク名 • 容量 • インターフェース	追加	更新前のデータに、更新するデータと同じ（すべて一致する）ものが存在しないとき。
		削除	更新するデータに、更新前のデータと同じ（すべて一致する）ものが存在しないとき。
インストールソフトウェア情報	ソフトウェア名	追加	更新前のデータに、更新するデータと同じ（すべて一致する）ものが存在しないとき。ただし、更新プログラムは除きます。
		削除	更新するデータに、更新前のデータと同じ（すべて一致する）ものが存在しないとき。ただし、更新プログラムは除きます。
	バージョン	変更	更新前と更新後で、同じ「ソフトウェア名」のデータが変化したとき。 ただし、更新プログラムは除きます。
セキュリティ情報	自動更新	変更	更新前と更新後でデータが変化したとき。
	サービスのセキュリティ設定情報	追加	更新前のデータに、更新するデータが存在しないとき。
		削除	更新するデータに、更新前のデータが存在しないとき。
	OS のセキュリティ設定情報のアカウント名	追加	更新前のデータに、更新するデータが存在しないとき。
		削除	更新するデータに、更新前のデータが存在しないとき。
	OS のセキュリティ設定情報のアカウント名の次の項目が対象となります。 • パスワード更新からの経過日数 • パスワードの安全性 • 無期限パスワード	変更	更新前と更新後で、同じ「アカウント名」のどちらかデータが変化したとき。
	OS のセキュリティ設定情報のパワーオンパスワード	変更	更新前と更新後でデータが変化したとき。
	OS のセキュリティ設定情報の Guest アカウント	変更	更新前と更新後でデータが変化したとき。

機器情報の項目		事象	イベント発行の契機
セキュリティ情報	OS のセキュリティ設定情報の自動ログオン	変更	更新前と更新後でデータが変化したとき。
	OS のセキュリティ設定情報の共有フォルダ	変更	更新前と更新後でデータが変化したとき。
	OS のセキュリティ設定情報の管理共有	変更	更新前と更新後でデータが変化したとき。
	OS のセキュリティ設定情報の DCOM	変更	更新前と更新後でデータが変化したとき。
	OS のセキュリティ設定情報の匿名接続	変更	更新前と更新後でデータが変化したとき。
	OS のセキュリティ設定情報のスクリーンセーバー情報の次の項目が対象となります。 • スクリーンセーバー • パスワードによる保護 • 起動待ち時間	変更	更新前と更新後でどちらかのデータが変化したとき。
	OS のセキュリティ設定情報のファイアウォール	変更	更新前と更新後でデータが変化したとき。
	OS のセキュリティ設定情報のリモートデスクトップ	変更	更新前と更新後でデータが変化したとき。

(17)　機器の変更履歴の取得

組織内では、利用者が勝手にコンピュータにメモリを抜き差ししたり、ソフトウェアをインストール、アンインストールしたりするなど、コンピュータの構成を変更してしまう場合があります。このような変更の中に、メモリの盗難や組織内で許可していないソフトウェアのインストールなどがあったとしても、システム管理者は簡単には発見できません。

JP1/IT Desktop Management 2 では、管理対象の機器の機器情報が変更された場合に、変更前と変更後の情報を変更履歴として取得できます。変更履歴では、変更された機器情報だけを確認できるため、組織内の問題のある変更を発見しやすくなります。定期的に変更履歴を確認して、変更履歴の中に不審な変更がないか判定してください。

なお、機器の変更履歴を取得するためには、管理元の管理用サーバの設定画面で、変更履歴を取得するように設定する必要があります。

変更履歴を取得する仕組み

機器情報の変更があった場合、変更後の機器情報がデータベースに保存されます。毎日 0:00 になると、変更前の機器情報と変更後の機器情報の比較が実行されて、1 日分の変更履歴をまとめて取得します。

変更履歴の確認方法

取得した変更履歴の確認方法には、次の 2 種類があります。

操作画面に表示された変更履歴を確認する

機器画面の［変更履歴］画面では、直近の変更履歴を確認できます。［変更履歴］画面には、最大600,000 件の変更履歴が表示されます。変更履歴の件数が 600,000 件を超えた場合は、最も古い情報が新しい情報に上書きされます。

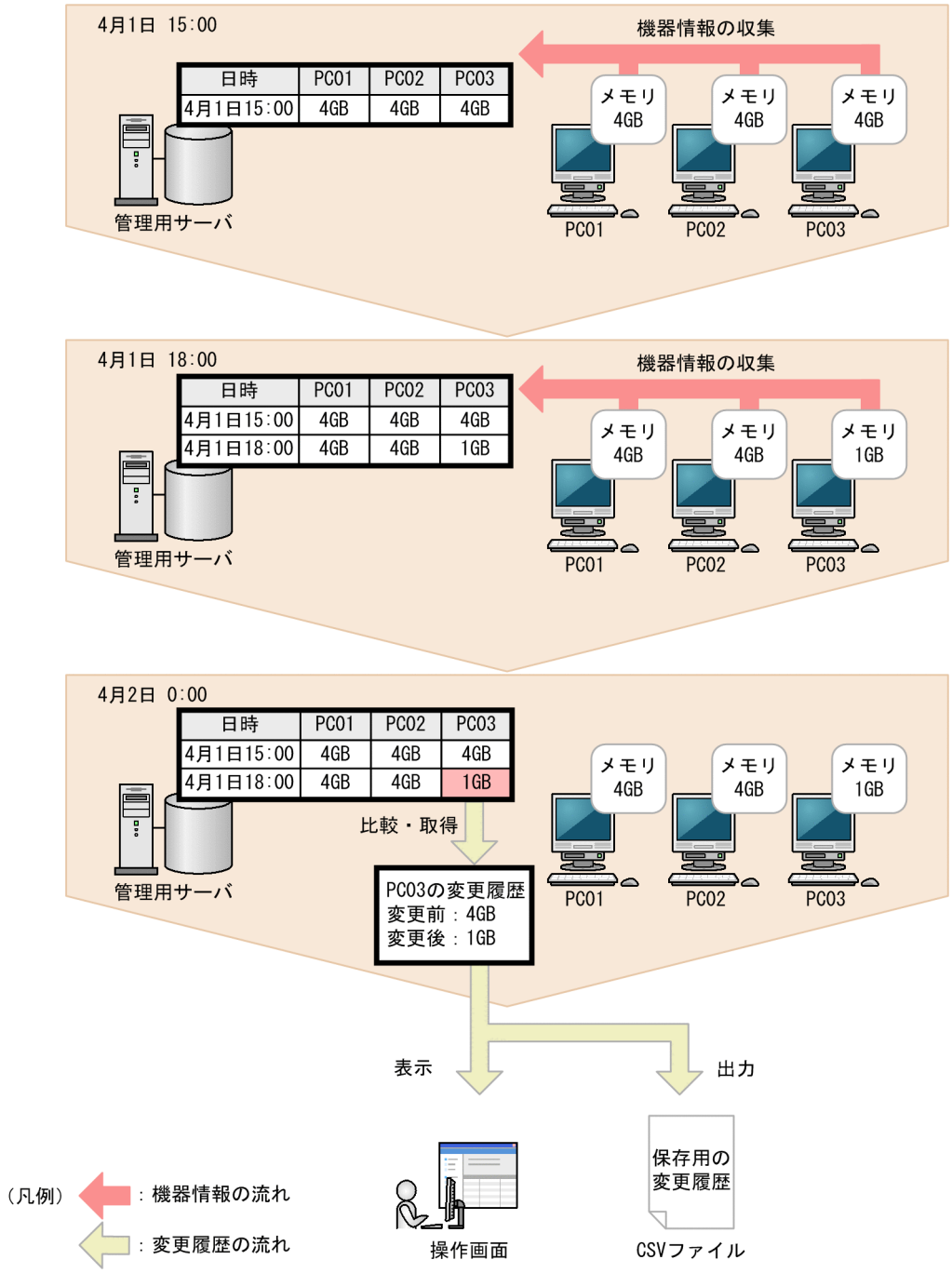
CSV ファイルに出力された保存用の変更履歴を確認する

CSV ファイルに保存用の変更履歴を出力して、確認できます。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。なお、保存用の変更履歴を出力するには、セットアップでの出力設定が必要です。

重要

機器情報を削除した場合、機器画面の［変更履歴］画面には削除された機器のホスト名が表示されません。 削除した機器のホスト名を確認する必要がある場合は、CSV ファイルに出力された保存用の変更履歴を確認してください。

変更履歴を取得して確認するまでの流れを、次の図に示します。



(18)　変更履歴を取得できる機器情報と変更と見なす条件

変更履歴を取得できる機器情報と、その機器情報の変更が JP1/IT Desktop Management 2 によって検知される契機について次の表に示します。

変更履歴を取得できる機器情報	説明	変更と見なす条件
管理状態	管理状態の変更を取得します。管理状態には、発見、管理対象、除外対象の 3 種類があります。	次のとおり管理状態が変更されたときです。 • 発見から管理対象に変更されたとき • 管理対象から除外対象に変更されたとき • 除外対象から管理対象に変更されたとき

変更履歴を取得できる機器情報	説明	変更と見なす条件
管理状態	管理状態の変更を取得します。管理状態には、発見、管理対象、除外対象の 3 種類があります。	• 管理対象の機器情報が削除されたとき
管理種別	次に示す管理種別の変更を取得します。 • エージェント管理 • エージェントレス管理（認証成功） • エージェントレス管理（認証失敗） • MDM 連携管理 • API 管理	機器情報の収集で、前回収集した情報から変更があったとき
ホスト名※1	システム情報のコンピュータ情報として収集される、ホスト名の変更を取得します。	• 機器情報の収集で、前回収集した情報から変更があったとき • 操作画面からホスト名を変更したとき • UNIX エージェント、Mac エージェントはホスト名の大文字/小文字を区別するため、大文字/小文字を変更したとき
UUID（コンピュータ情報）	システム情報のコンピュータ情報として収集される、UUID の変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき ただし、16 進数のアルファベット（A～F および a～f）の大文字・小文字だけが変わった場合は、変更と見なしません。
メモリ（コンピュータ情報）	システム情報のコンピュータ情報として収集される、メモリの変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき
外部ストレージ容量（スマートデバイス情報）	システム情報のスマートデバイス情報として収集される、外部ストレージ容量の変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき
IMSI（スマートデバイス情報）	システム情報のスマートデバイス情報として収集される、IMSI の変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき
IP アドレス（ネットワーク情報）※1、※2、※3	システム情報のネットワーク情報として収集される、IP アドレスの変更を取得します。	• 機器情報の収集で、前回収集した情報から変更があったとき • 操作画面から IP アドレスを変更したとき
MAC アドレス（ネットワーク情報）※2	システム情報のネットワーク情報として収集される、MAC アドレスの変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき ただし、16 進数のアルファベット（A～F および a～f）の大文字・小文字だけが変わった場合は、変更とみなしません。
プロセッサ（CPU 情報）※2	ハードウェア情報の CPU 情報として収集される、プロセッサの変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき
ディスク名（ハードディスク情報）※2	ハードウェア情報のハードディスク情報として収集される、ディスク名の変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき

変更履歴を取得できる機器情報	説明	変更と見なす条件
ハードディスクの容量（ハードディスク情報）※2	ハードウェア情報のハードディスク情報として収集される、ハードディスクの容量の変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき
ドライブ名（CD-ROM ドライブ情報）※2	ハードウェア情報の CD-ROM ドライブ情報として収集される、ドライブ名の変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき
ビデオチップ（ビデオコントローラ情報）※2	ハードウェア情報のビデオコントローラ情報として収集される、ビデオチップの変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき
ビデオチップの VRAM 容量（ビデオコントローラ情報）※2	ハードウェア情報のビデオコントローラ情報として収集される、ビデオチップの VRAM 容量の変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき
ビデオドライバ（ビデオコントローラ情報）※2	ハードウェア情報のビデオコントローラ情報として収集される、ビデオドライバの変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき
サウンドカードの製品名（サウンドカード情報）※2	ハードウェア情報のサウンドカード情報として収集される、サウンドカードの製品名の変更を取得します。	機器情報の収集で、前回収集した情報から変更があったとき
インストールソフトウェア情報	インストールソフトウェア情報のうち、次の項目の変更を取得します。 • ソフトウェア名 • バージョン • プロダクト ID	機器情報の収集で、前回収集した情報から変更があったとき
部署（共通管理項目）	資産情報と機器情報の共通管理項目である、部署の変更を取得します。	• 機器情報の収集で、前回収集した情報から変更があったとき • 操作画面から部署を変更したとき • CSV ファイルによるインポートで、情報が変更されたとき
設置場所（共通管理項目）	資産情報と機器情報の共通管理項目である、設置場所の変更を取得します。	• 機器情報の収集で、前回収集した情報から変更があったとき • 操作画面から設置場所を変更したとき • CSV ファイルによるインポートで、情報が変更されたとき
利用者名（共通管理項目）	資産情報と機器情報の共通管理項目である、利用者名の変更を取得します。	• 機器情報の収集で、前回収集した情報から変更があったとき • 操作画面から利用者名を変更したとき • CSV ファイルによるインポートで、情報が変更されたとき

注※1　DHCP が有効の IP アドレスが 1 つ以上ある機器の場合、次の流れでホスト名または IP アドレスが変更されたときは、2.の変更履歴が取得できません。

1. システム管理者が、操作画面から機器のホスト名または DHCP が無効の IP アドレスを変更する

2. 1.のあとに、DHCP が有効の IP アドレスだけが自動的に変更される

この場合、操作画面に表示される機器情報と変更履歴の値が一時的に不一致になります。翌日以降の初回に実行される機器情報の収集で、新たに変更履歴が取得され、値の不一致が解消されます。

注※2　機器情報に複数の値がある場合、変更前の値のうちどれか 1 つでも追加、変更、および削除があったときは、変更を取得します。ただし、値の順序が変更されただけの場合は、変更を取得しません。ディスク名（ハードディスク情報）を例に、複数の値がある場合の変更履歴の取得有無を次の表に示します。

機器情報の値		変更履歴の取得有無
変更前	変更後	
HDDModel1、HDDModel2	HDDModel2、HDDModel3	○
HDDModel1、HDDModel2	HDDModel1	○
HDDModel1、HDDModel2	HDDModel1、HDDModel2、HDDModel3	○
HDDModel1、HDDModel2	HDDModel2、HDDModel1	×

（凡例）○：取得する、×：取得しない

注※3　変更前、変更後の IP アドレスの DHCP が両方とも有効の場合は、変更履歴を取得しません。変更前、変更後どちらか一方の IP アドレスの DHCP が無効の場合は、変更履歴を取得します。なお、SNMP や ICMP などを利用して機器情報を収集する場合、DHCP 設定を取得できません。DHCP 設定が取得できない場合は、DHCP が無効として IP アドレスの比較を実行します。

(19)　管理対象のコンピュータがネットワークから切り離された場合の動作

管理対象のコンピュータがネットワークから切り離された場合、ネットワークに接続している場合と同様に、エージェント設定で指定した監視間隔に従って、コンピュータに接続しようとします。

この場合、管理用サーバからは、管理対象のコンピュータがネットワークから切断されたのか、電源を OFF にされたのかはわかりません。そのため、管理対象のコンピュータがネットワークから切断された場合、オンライン管理のコンピュータでは、最終接続確認日時から情報取得の間隔＋ 10 分間通信できなかったときに電源 OFF と認識します。エージェントレスの機器の場合は、情報取得できなかった場合に電源 OFF と認識します。

ネットワーク探索では、情報取得ができなかった場合でも管理対象機器の機器状態を電源 OFF にしません。エージェントレスの機器の状態を確認する場合は、機器一覧から［最新の情報を取得する］を実行するか、定期的に更新されてから確認してください。

コンピュータの機器情報は、次回コンピュータがネットワークに接続して JP1/IT Desktop Management 2 が情報を取得できるまでは、ネットワークから切り離される直前の情報が保持されます。

ネットワークから切り離されたオンライン管理のコンピュータの動作

ネットワークから切り離された場合でも、コンピュータにセキュリティポリシーは適用されています。このため、次のような動作が発生します。

- 起動を抑止しているソフトウェアを実行しようとした場合、起動抑止されます。
  起動抑止のイベントは、エージェント導入済みコンピュータに保存されます。
- デバイスなどの使用抑止機能が有効の場合、使用が抑止されます。
- 操作ログが取得されます。
  エージェント導入済みコンピュータのローカルに操作ログが保存されます。

> **ヒント**
>
> エージェントレスのコンピュータの場合は、コンピュータ側での動作は発生しません。エージェントレスのコンピュータは、収集した機器情報を基に管理用サーバでセキュリティ状況が判定されるだけで、コンピュータにはセキュリティポリシーは送信されないためです。

再度ネットワークに接続したときの動作

ネットワークから切り離されたコンピュータを再度ネットワークに接続した場合は、セキュリティの監視項目や、最新の機器情報はすぐにアップロードされません。エージェント設定に指定された監視間隔に従ってアップロードされます。 また、ネットワークから切り離されている間にローカルに保存されたイベントは、次回管理用サーバと通信したときにアップロードされます。

操作ログは、利用者のコンピュータから管理用サーバにアップロードされます。再度ネットワークに接続した場合は、接続後の最初のアップロード時に、コンピュータに保存された操作ログをまとめてアップロードします。

セキュリティ状況の判定について

コンピュータがネットワークから切り離されている間は、保持された情報を基にセキュリティ状況が判定されます。これは、すべてのセキュリティ判定項目について、ネットワークから切り離される直前の情報がデータベースに保持されているためです。

> **ヒント**
>
> UNIX エージェントまたは Mac エージェントの場合、ネットワークから切り離されたときに、管理用サーバからの再接続の試み、電源 ON/OFF の判定、操作ログの取得、およびセキュリティ状況の判定は行われません。

(20) グループの作成方法

グループには、システムが自動的に作成するシステム分類のグループ（機器種別、ネットワーク、部署および設置場所）と、システム管理者が作成するユーザー定義のグループがあります。グループには、機器情報およびハードウェア資産情報に応じて、機器が自動的に振り分けられます。作成したグループは、メニューエリアに表示されます。

グループの作成方法について、グループの種別ごとに説明します。

機器種別

機器から収集された機器種別（PC、サーバ、プリンタなど）に応じてグループが作成されます。機器種別が「PC」または「サーバ」のコンピュータから機器情報が収集された場合、OS 名ごとのグループが作成されます。

ネットワーク

機器の IP アドレスとサブネットマスクを基に、ネットワークアドレスごとのグループが作成されます。

部署

各機器の部署の情報を基にグループが作成されます。設定画面の［資産管理項目の設定］画面で、部署の階層構成を登録した場合、自動的にグループに反映されます。また、Active Directory と連携している場合、部署を取得する OU の階層構成がグループに反映されます。

設置場所

各機器の設置場所の情報を基にグループが作成されます。設定画面の［資産管理項目の設定］画面で、設置場所の階層構成を登録した場合、自動的にグループに反映されます。SNMP で機器情報を収集している場合、各機器から SNMP で取得した設置場所の値がグループに反映されます。Active Directory と連携している場合、各コンピュータの情報として取得した設置場所の値がグループに反映されます。

ユーザー定義

システム管理者が、メニューエリアから表示できる［機器一覧（ユーザー定義）の編集］ダイアログで追加します。ユーザー定義の各グループに設定された条件に従って、管理対象のコンピュータが自動的に対応するグループに振り分けられます。

関連リンク

- 2.4.3　Active Directory との連携

(21)　部署・設置場所の定義およびグループの仕組み

機器の利用者情報のうち、部署および設置場所の定義は、設定画面から編集できます。設定画面で追加した定義は、資産画面や機器画面のメニューエリアに自動でグループとして追加されます。職制変更や部署統合に伴い削除した定義は、資産画面と機器画面のメニューエリアから表示できる［旧体制で使われていた階層の削除］ダイアログで一覧表示し、一括で削除できます。

また、部署および設置場所のグループはメニューエリアで編集できます。

設定画面で定義を編集する場合と、メニューエリアでグループを編集する場合に実施できる操作とその結果を、それぞれ説明します。

設定画面で定義を編集する場合

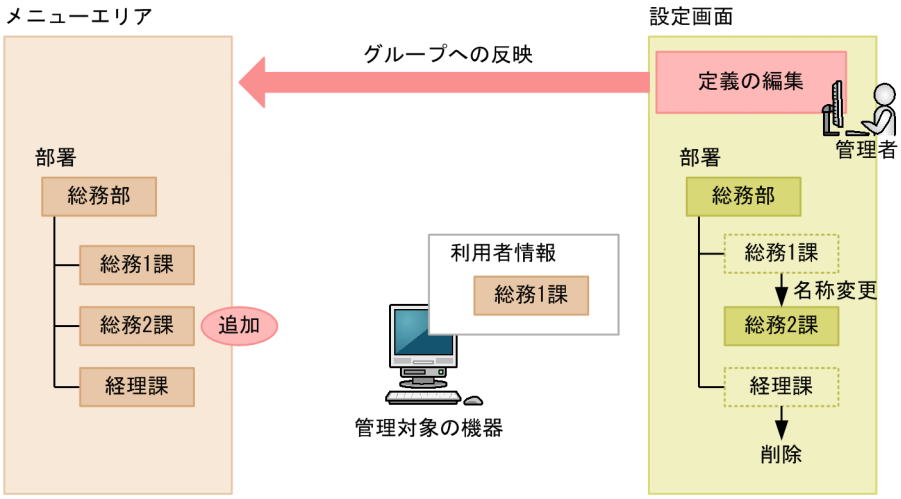
設定画面では、次の編集を実施できます。

- 定義の追加
- 定義の削除

- 定義の名称変更
- 構成の変更（階層定義の場合だけ）

設定画面で編集する場合は、定義だけが更新の対象となり、機器の利用者情報は更新されません。定義の追加、定義の名称変更、構成の変更を実施した場合、定義を編集する前のグループがメニューエリアに残ったまま、編集した定義に対応するグループが新たに追加されます。また、定義を削除した場合も、削除前の定義に対応するグループは残ったままとなります。

設定画面で定義の名称変更および定義の削除を実施した場合に、メニューエリアおよび機器の利用者情報へ反映される結果を次の図に示します。



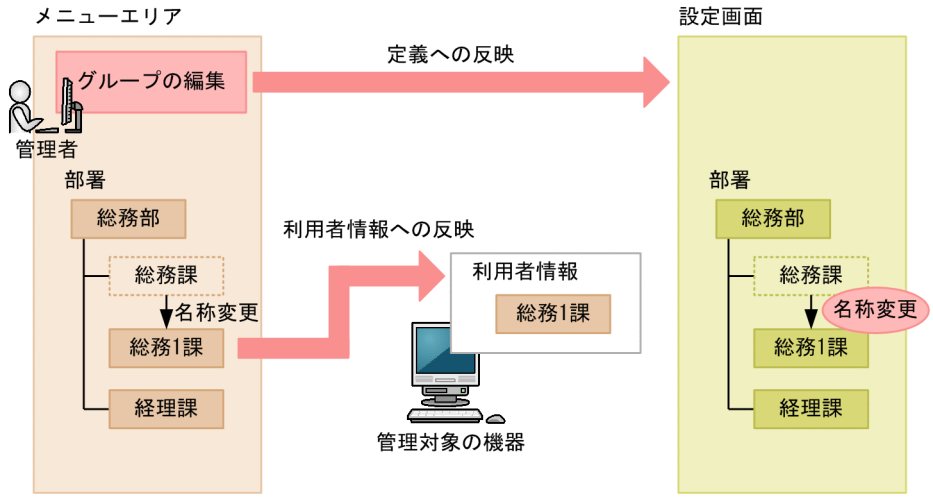
メニューエリアでグループを編集する場合

メニューエリアでは、次の編集を実施できます。

- グループの名称変更
- グループの削除

メニューエリアでグループを編集する場合、そのグループに登録されている機器の利用者情報もあわせて更新されます。また、グループに対応する定義も更新されます。

メニューエリアでグループの名称変更を実施した場合に、定義および機器の利用者情報へ反映される結果を次の図に示します。



ヒント

部署・設置場所の定義には、管理したい構成を設定してください。利用者情報と定義が異なる場合は、利用者情報を更新して定義どおりのグループに機器が登録されるようにします。このようにすることで、管理者が意図したとおりのグループで機器を管理できます。

ヒント

探索によって、設定画面で定義した設置場所以外の情報を収集すると、設置場所が自動生成されます。

定義およびグループを編集したあとに必要な設定

職制変更や部署統合に伴い定義およびグループを編集したあとに必要な設定を次に示します。

部署の定義を追加した場合

追加した部署に、次の項目を設定します。

- セキュリティポリシーの割り当て
- エージェント設定の割り当て
- 部門管理者の管轄範囲への追加

部署の定義を変更した場合

変更した部署に、次の項目を設定します。`ioassetsfieldutil import` コマンドを利用して定義を変更した場合、設定は不要です。

- セキュリティポリシーの割り当て
- エージェント設定の割り当て
- 部門管理者の管轄範囲への追加

また、旧体制の部署に関連づいている次の資産情報を削除します。または、別の部署へ関連づけます。

- ハードウェア資産情報
- ソフトウェアライセンス情報
- 契約情報

部署の定義を削除した場合

削除した部署に関連づいている次の資産情報を削除します。または、別の部署へ関連づけます。

- ハードウェア資産情報
- ソフトウェアライセンス情報
- 契約情報

部署のグループを削除した場合

削除した部署に関連づいている次の資産情報を削除します。または、別の部署へ関連づけます。

- ハードウェア資産情報
- ソフトウェアライセンス情報
- 契約情報

(22) ユーザー定義のグループの仕組み

任意の条件に従って機器を振り分けるユーザー定義のグループは、セキュリティ画面および機器画面のメニューエリアで編集できます。

ユーザー定義のグループには、セキュリティポリシーを割り当てられます。ほかのグループと異なり、エージェント設定の割り当て、およびレポートの集計範囲には適用できません。

ユーザー定義のグループで作成できる階層は 1 階層までです。また、ユーザー定義のグループ名は、ASCII コードの制御文字を除いた文字列を、256 文字以内で指定してください。

機器は、ユーザー定義のグループ条件に設定した機器情報の種別、対象項目、判定条件および判定値に従って振り分けられます。そのため、機器を直接グループに振り分けることはできません。複数のユーザー定義のグループに当てはまる機器は、当てはまるグループすべてに振り分けられます。条件が設定されていないユーザー定義のグループには、機器は振り分けられません。

機器情報の種別
: 対象項目とする機器情報の種別です。システム分類の機器一覧（機器種別、ネットワーク、部署および設置場所）と、システム管理者が追加した追加管理項目を選択できます。

対象項目
: ユーザー定義のグループ条件の対象とする項目です。複数の対象項目を設定した場合は、すべての対象項目の条件を満たす機器だけがグループに振り分けられます。

判定条件
: 対象項目の値と判定値を比較する条件です。比較した結果を基に、機器がグループに振り分けられます。

判定値
: 判定条件に従って、対象項目と比較する値です。

メニューエリアには、あらかじめ［条件に該当しない機器］というグループが表示されています。［条件に該当しない機器］には、システム管理者が作成したユーザー定義のグループに振り分けられていない機器が振り分けられます。

ユーザー定義のグループに設定できる判定条件と判定値

ユーザー定義のグループに設定できる判定条件と判定値は、機器情報の種別によって異なります。機器情報の種別ごとに、設定できる判定条件と判定値を次の表に示します。

機器情報の種別が機器一覧（システム分類）の場合

判定条件	判定値
判定値と等しい	プルダウンメニューに表示される階層
判定値と等しくない	
判定値と等しい（下位の階層も含む）※	
判定値と等しくない（下位の階層も含む）※	

注※　対象項目がネットワークの場合は設定できません。

機器情報の種別が追加管理項目の場合

判定項目のデータ型	判定条件	判定値
テキスト型	判定値と等しい	1～256 文字の文字列 なお、大文字と小文字の違い、および全角と半角の違いは判定時に区別されます。
	判定値と等しくない	
	判定値が前方一致	
	判定値が後方一致	
	判定値を含む	
数値型	判定値と等しい	-2,147,483,647～2,147,483,647
	判定値と等しくない	
	判定値以上	
	判定値以下	
	判定値より大きい	
	判定値より小さい	
選択型	判定値と等しい	プルダウンメニューに表示される値 なお、大文字と小文字の違い、および全角と半角の違いは判定時に区別されます。
	判定値と等しくない	

機器がユーザー定義のグループに振り分けられる契機

設定したユーザー定義のグループ条件に従って、機器がグループに振り分けられる契機を次に示します。

- ユーザー定義のグループ名を変更したとき
- ユーザー定義のグループを削除したとき
- ユーザー定義のグループ条件を編集したとき
- ユーザー定義のグループ条件の、対象項目に設定しているシステム分類のグループに属する機器が、別のグループに移動されたとき
- ユーザー定義のグループ条件の、対象項目に設定している追加管理項目の情報が更新されたとき
- ユーザー定義のグループ条件の、対象項目に設定している追加管理項目を削除したとき

(23) 重複登録された機器情報の削除

OS などの再インストールによって、エージェントが削除された場合、同一の機器が重複して登録されることがあります。重複する機器の削除方法を次に示します。

- 機器画面の［機器情報］画面の更新日時で、長時間更新されない機器を削除します。
- 機器画面の［機器情報］画面で、MAC アドレスで並べ替えます。MAC アドレスが同一の機器のうち片方を削除します。

(24) UNIX エージェントまたは Mac エージェントが導入された機器のインベントリ情報のサイズ

UNIX エージェントまたは Mac エージェントが導入された機器で収集できるインベントリ情報のサイズ制限を次に示します

インベントリ種別	サイズ制限
システム情報	収集する情報のサイズが 200 バイトを超える場合は、200 バイトまで収集できます。
ハードウェア情報	収集する情報のサイズが 200 バイトを超える場合は、200 バイトまで収集できます。 ディスク容量またはドライブ容量が 4 ペタバイトを超える場合は、4 ペタバイトまで収集できます。
インストールソフトウェア情報、ソフトウェア情報	ソフトウェア名が 50 バイトを超える場合は、50 バイトまで収集できます。 バージョンが 8 バイトを超える場合は、8 バイトまで収集できます。

2.6.3 機器の制御

機器を管理対象にすると、対象の機器を制御できるようになります。ここでは、次に示すような機器の制御について説明しています。

利用者にメッセージを通知する

コンピュータの利用者に個別にメッセージを通知できます。複数のコンピュータを指定して、一斉にメッセージを通知することもできます。

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

コンピュータのネットワーク接続を制御する

コンピュータのネットワークの接続可否を設定できます。

利用者情報を取得する

利用者のコンピュータに［利用者情報の入力］画面を表示させて、利用者が入力した情報を取得できます。

コンピュータの電源を制御する

コンピュータの電源を ON/OFF にしたり、再起動したりできます。機器の管理、リモートコントロール、ITDM 互換配布、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利用できます。

最新の機器情報を取得する

任意のタイミングで最新の機器情報を取得できます。

使用禁止ソフトウェアを設定する

コンピュータにインストールされているソフトウェアを確認して、使用禁止ソフトウェアとして設定できます。使用禁止ソフトウェアを設定することで、セキュリティ画面でソフトウェアの利用状況についての危険レベルを確認できるようになります。また、ソフトウェアの使用を抑止したり、アンインストールしたりもできます。

コンピュータからソフトウェアをアンインストールする

コンピュータにインストールされているソフトウェアを確認して、アンインストールできます。

コンピュータをリモートコントロールする

離れた場所にあるコンピュータに接続して、呼び出したコンピュータの画面に対して操作できます。

スマートデバイスを制御する

管理対象のスマートデバイスに対して、スマートデバイスのロック、パスコードのリセット、初期化を実行できます。

ヒント

UNIX エージェント、Mac エージェントの場合、機器の制御として実行できるのは、ネットワークの接続の制御（UNIX エージェントは手動だけ）と、最新の機器情報の取得です。最新の情報を取得する際には、「コンピュータ(UNIX)のシステム情報の取得」ジョブと「コンピュータ(UNIX)のソフトウェア情報の取得」ジョブが実行されます。また、Mac エージェントからはデフォルトで 24 時間ごとに（1 日に 1 度)、システム情報とソフトウェア情報が管理用サーバに通知されます。

ヒント

API を使用する場合は、コンピュータのネットワーク接続の制御だけができます。また、利用者情報は API を使用して登録できます。

(1) 電源制御の条件

コンピュータの電源を制御するための条件について説明します。

コンピュータの電源を ON にするための条件

機器情報の「AMT ファームウェアバージョン」の値がある場合は AMT を利用して、値がない場合は Wake on LAN を利用して電源を ON にします。コンピュータの電源を ON にするためには、次の条件を満たすようにしてください。

重要

次の場合はコンピュータの電源を ON にできません。

- 無線 LAN 環境である
- LAN と無線 LAN が同じサブネットに接続されている
- 電源がバッテリーモードで、コンピュータが停止状態である
- UNIX エージェントである
- Mac エージェントである

管理用サーバ側の条件

AMT を利用する場合

- 設定画面の［機器］－［AMT の設定］画面で、接続先の AMT のユーザー ID とパスワードを登録している。

  複数サーバ構成の場合は、電源を ON にしたい機器の管理元の管理用サーバで設定する必要があります。
- AMT で使用する 16992 ポートで通信できる。
- 電源を ON にしたい機器をホスト名で名前解決できること。

Wake on LAN を利用する場合

- 特になし。

コンピュータ側の条件

AMT を利用する場合

- 対象のコンピュータが管理用サーバと接続している。
- 対象のコンピュータにエージェントが導入されている。
- AMT をサポートしている。

  対象のコンピュータが AMT をサポートしているかどうかは、収集した機器情報の「AMT ファームウェアバージョン」の値が表示されるかどうかで確認できます。
- BIOS の設定で、AMT にアクセスするためのユーザー名とパスワードが設定されている。
- AMT で使用する 16992 ポートで通信できる。

ヒント

エージェント導入済みのコンピュータの場合、エージェント設定から AMT の設定ができます。各コンピュータの BIOS を操作する手間を軽減できます。

ヒント

AMT のユーザー ID とパスワードは管理用サーバに 1 つだけ登録できます。そのため、AMT を利用して電源操作するときは、すべてのコンピュータで AMT の ID とパスワードを統一しておく必要があります。

Wake on LAN を利用する場合

- 対象のコンピュータが管理用サーバと接続している。
- 対象のコンピュータにエージェントが導入されている。
- Wake on LAN をサポートしている。
- Wake on LAN で Magic Packet の設定を有効にしている。

コンピュータの電源を OFF にするための条件

コンピュータの電源を OFF にするためには、次の条件を満たすようにしてください。

重要

次の場合はコンピュータの電源を OFF にできません。

- 管理用中継サーバである
- 中継システムである
- UNIX エージェントである
- Mac エージェントである

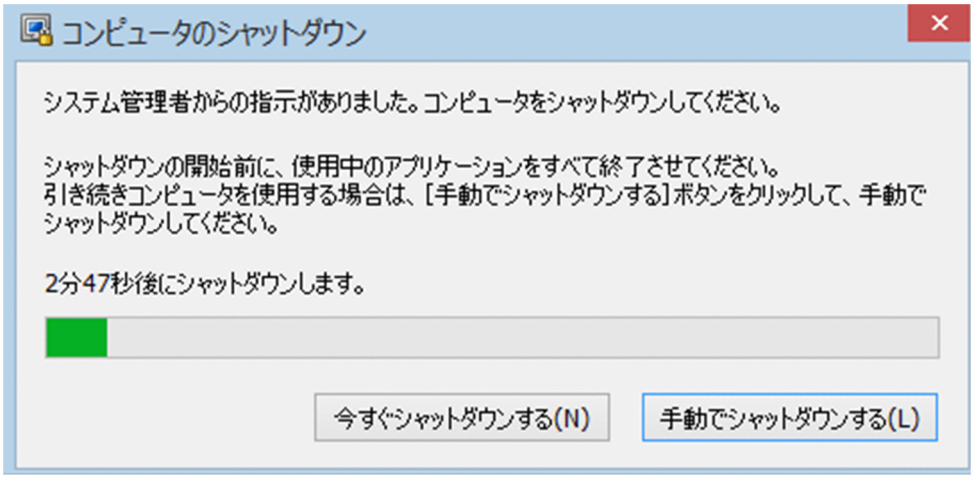
管理用サーバ側の条件

特になし。

コンピュータ側の条件

- 対象のコンピュータが管理用サーバと接続している。
- 対象のコンピュータにエージェントが導入されている。

コンピュータの電源を OFF にする場合、コンピュータ側で［コンピュータのシャットダウン］ダイアログが表示されます。



利用者がダイアログを操作しない場合、ダイアログが表示されてから 180 秒後に自動でシャットダウンされます。

シャットダウン時の注意事項を次に示します。

- スクリーンセーバーが起動しパスワードで保護している場合は、自動的にシャットダウンされません。
- コンピュータをロックしている場合は、自動的にシャットダウンされません。
- 編集中のファイルが存在する場合は、自動的にシャットダウンされません。
- ほかのユーザーがログオンしている場合は、自動的にシャットダウンされません。
- ログオン前の場合は、[コンピュータのシャットダウン] ダイアログが表示されないでシャットダウンされます。
- [コンピュータのシャットダウン] ダイアログの表示中に管理用サーバから電源 OFF の通知を受け取った場合は、後続の通知は無効になります。

コンピュータを再起動するための条件

コンピュータを再起動するためには、次の条件を満たすようにしてください。

重要

次の場合はコンピュータを再起動できません。

- 管理用中継サーバである
- 中継システムである
- UNIX エージェントである
- Mac エージェントである

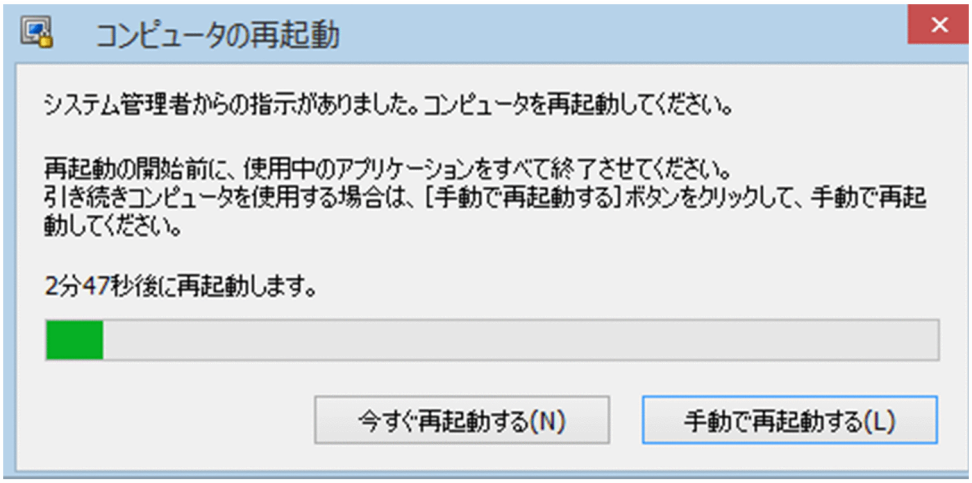
管理用サーバ側の条件

特になし。

コンピュータ側の条件

- 対象のコンピュータが管理用サーバと接続している。
- 対象のコンピュータにエージェントが導入されている。

コンピュータを再起動する場合、コンピュータ側で［コンピュータの再起動］ダイアログが表示されます。



エージェント設定の［利用者への通知設定］－［コンピュータのシャットダウンと再起動の設定］で設定したタイミングで、コンピュータが再起動されます。エージェント設定で［指定する時間内に利用者の応答がない場合に、自動的に開始する］を選択している場合、利用者がダイアログを操作しないときは、ダイアログが表示されてからエージェント設定で指定した時間が経過すると自動的に再起動されます。エージェント設定で［シャットダウンまたは再起動を指示するダイアログでの、利用者の応答に従う］を選択している場合、利用者がダイアログを操作しないときは、ダイアログが表示されたまま自動的に再起動されません。

再起動時の注意事項を次に示します。

- スクリーンセーバーが起動しパスワードで保護している場合は、自動的に再起動されません。
- コンピュータをロックしている場合は、自動的に再起動されません。
- 編集中のファイルが存在する場合は、自動的に再起動されません。
- ほかのユーザーがログオンしている場合は、自動的に再起動されません。
- ログオン前の場合は、［コンピュータの再起動］ダイアログが表示されないで再起動されます。
- ［コンピュータの再起動］ダイアログの表示中に管理用サーバから電源 OFF の通知を受け取った場合は、電源 OFF の通知だけが有効になります。このとき、［コンピュータの再起動］ダイアログはキャンセルされて、［コンピュータのシャットダウン］ダイアログが表示されます。

(2) AMT を利用するための前提条件

AMT のバージョンが 6.0 より前の場合は、DHCP 環境であることが前提です。また、無線 LAN 環境はサポートしていません。

利用する機能に応じて、対象のコンピュータに必要な AMT のバージョンが異なります。

AMT を利用する場合に必要なバージョンを次の表に示します。

機能		説明	必要な AMT のバージョン
コンピュータの電源制御		接続先のコンピュータの電源を制御します。	3.0～9.5
AMT ファームウェアバージョンの取得		AMT のバージョンを機器情報として取得できます。	
IDE リダイレクションの利用※		リモートコントロール時にリモート CD-ROM 機能を利用できます。	
RFB での接続によるリモートコントロールの使用		RFB 接続でリモートコントロールを使用します。	6.1～9.5
AMT の設定	IDE リダイレクションの有効化	AMT の IDE リダイレクション機能を使用できるようにします。	6.1～9.5
	リモート KVM の有効化	エージェント設定で対象のコンピュータのリモート KVM を有効にして、RFB 接続でリモートコントロールできるようにします。 また、対象のコンピュータをリモートコントロールするときの認証情報も設定できます。	
	AMT の有効化および管理者権限のパスワード設定	AMT が無効の場合に有効にします。また、AMT の管理者権限（admin ユーザー）のパスワードを設定します。	7.0～9.5

注※　AMT のバージョンが 7.0 または 8.0 の場合、設定画面－［AMT の設定］画面で AMT を有効化したコンピュータに対しては IDE リダイレクションを利用できません。

コンピュータの AMT を自動的に有効にする場合

AMT を利用した機能を使うためには、コンピュータの AMT が有効になっている必要があります。

コンピュータの AMT を自動的に有効にするには、設定画面－［AMT の設定］画面で、コンピュータの AMT に設定する管理者権限のパスワードを設定してください。

コンピュータの AMT を自動的に有効化して、管理者権限でアクセスできるようになります。

なお、コンピュータの AMT に管理者権限のパスワードが未設定の場合は、ここで設定したパスワードが AMT に登録されます。管理者権限のパスワードが登録済みの場合、パスワードは設定できません。登録済みのパスワードを指定してください。また、管理者権限のパスワードが設定済みでかつ AMT が無効になっているときは、あらかじめコンピュータの AMT を有効にしておく必要があります。

コンピュータの AMT を自動的に有効にする場合、次のサービスが起動されます。

- サービス名：LMS

表示名：Intel(R) Management and Security Application Local Manage

- サービス名：UNS

  表示名：Intel(R) Management and Security Application User Notification Service

また、これらの機能を利用するためには、管理用サーバで次に示す設定が必要です。

AMT を利用してコンピュータの電源を制御する場合

設定画面－［AMT の設定］画面で、コンピュータの AMT と通信するための認証情報（[認証情報]）を設定してください。

コンピュータの電源制御が実行されると、AMT が利用されるようになります。

AMT ファームウェアバージョンを取得する場合

設定画面－［AMT の設定］画面で、コンピュータの AMT と通信するための認証情報（[認証情報]）を設定してください。

機器情報を取得するタイミングで、AMT のファームウェアバージョンが取得されるようになります。

RFB での接続によるリモートコントロールを使用する場合

コンピュータの AMT でリモート KVM 機能が有効になっている必要があります。

設定画面－［Windows エージェント設定とインストールセットの作成］画面からエージェント設定を編集します。このとき、［AMT の設定］で［リモート KVM を有効にする］のチェックをオンにしてください。

コンピュータの AMT が有効な場合、エージェント設定が適用されたタイミングで AMT の設定が変更されます。コンピュータの AMT が無効な場合は、自動的に有効にする設定が必要です。

このように設定することで、リモートコントロール機能でコンピュータに接続する場合に、標準接続に失敗すると RFB で接続されるようになります。［リモートコントロール］ウィンドウの［ファイル］－［接続］メニューから接続するときは、RFB で接続するように指定できます。

IDE リダイレクションを利用する場合

コンピュータの AMT で IDE リダイレクション機能が有効になっている必要があります。ただし、AMT のバージョンが 7.0 または 8.0 の場合、AMT を有効化したコンピュータに対しては IDE リダイレクションを利用できないため、BIOS から AMT を設定する必要があります。

設定画面－［Windows エージェント設定とインストールセットの作成］画面からエージェント設定を編集します。このとき、［AMT の設定］で［IDE リダイレクションを有効にする］のチェックをオンにしてください。

コンピュータの AMT が有効な場合、エージェント設定が適用されたタイミングで AMT の設定が変更されます。コンピュータの AMT が無効な場合は、自動的に有効にする設定が必要です。

このように設定することで、リモートコントロール中に、IDE リダイレクション機能を利用できるようになります。

複数サーバ構成の場合は、コントローラ側からネットワーク接続できる機器であれば、IDE リダイレクション機能を利用できます。

重要

管理画面の［エージェント設定項目］－［AMT の設定］タブで［IDE リダイレクションを有効にする］をチェックした場合、AMT の［SOL/IDER］－［Legacy Redirection Mode］の値も有効に設定されます。エージェントをアンインストールしてもこの項目は無効に設定されないため、無効にする場合は次のどちらかの手順を実施してください。

- エージェントのアンインストール前に、管理画面の［エージェント設定項目］－［AMT の設定］タブで［IDE リダイレクションを有効にする］のチェックを外す。
- エージェントのアンインストール後に、AMT の［SOL/IDER］－［Legacy Redirection Mode］の値を Disable に設定する。

関連リンク

- (1)　電源制御の条件

2.6.4　オフラインでの管理

JP1/IT Desktop Management 2 では、管理用サーバにネットワーク接続しているコンピュータと同様に、スタンドアロンのコンピュータや拠点にあるコンピュータなど、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対象にできます。

ネットワーク接続していないコンピュータを管理するためには、外部記憶媒体を利用してコンピュータにエージェントを導入し、機器情報を取得します。

このように、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を外部記憶媒体を利用して管理することをオフライン管理と呼びます。これに対して、ネットワーク接続しているコンピュータを管理することをオンライン管理と呼びます。

外部記憶媒体に必要な容量

オフライン管理のコンピュータから機器情報を収集する際に、外部記憶媒体に情報収集用ツールを格納します。外部記憶媒体に必要な容量は次のとおりです。

5 メガバイト＋（50 キロバイト×機器情報を収集したいコンピュータの台数）

コンピュータをオフラインで管理する場合、オンラインで管理する場合と比較して、管理用サーバから実行できる機能に差異があります。管理形態による機能差異については、「(1)　管理形態による機能差異」を参照してください。

なお、オフライン管理機能は、Citrix XenApp、Microsoft RDS サーバではサポートしていません。

また、オフライン管理のコンピュータの設定を操作画面で変更した場合は、インストールセット、getinv.vbs コマンド、または setsecpolicy.vbs コマンドツールの再実行が必要となります。これらのコマンドの再実行が必要となる設定項目については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のオフライン管理のコンピュータのツール再実行が必要な条件の説明を参照してください。

(1) 管理形態による機能差異

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には、管理用サーバから実行できる機能に差異があります。エージェント導入済みのコンピュータの場合は、オンライン管理のときとオフライン管理のときでも差異があります。

管理形態による機能差異を次の表に示します。

機能		管理対象のコンピュータ				
		エージェント導入済み				エージェントレス
		オンライン管理			オフライン管理※1	
		Windows	UNIX	Mac OS		
機器情報の収集※2		○	△	△	○	△
セキュリティ状況の診断	セキュリティポリシーの割り当て	○	○	○	○	○
	セキュリティ状況の診断	○	×	△	○	△ ※3
セキュリティポリシーの違反時のアクション	セキュリティの自動対策	○	×	×	△ ※9	×
	印刷の抑止	○	×	×	○	×
	データの持ち出し抑止	○	×	×	△※10	×
	ソフトウェアの起動抑止	○	×	×	○	×
	操作ログの取得	○	×	×	×	×
	メッセージの通知	○	×	×	×	×
	電源の ON および OFF	○	×	×	×	×
資産情報の管理	ハードウェアの管理	○	△ ※4	△ ※4	○ ※5	△
	ソフトウェアライセンスの管理	○	○	○	○	△
	ソフトウェアの管理	○	○	○	○	○
	契約の管理	○	○	○	○	○

機能		管理対象のコンピュータ				
		エージェント導入済み				エージェントレス
		オンライン管理			オフライン管理※1	
		Windows	UNIX	Mac OS		
ソフトウェアおよびファイルの配布	ソフトウェアの配布	○	○ ※6	×	○ ※6	×
	ファイルの配布	○	○ ※6	×	○ ※6	×
	ソフトウェアのアンインストール	○	×	×	×	×
機器のリモートコントロール	コンピュータの操作	○	×	○ ※7	×	○ ※7
	コンピュータからの接続要求	○	×	×	×	×
	ファイル転送	○	×	×	×	×
	チャット	○	×	×	×	×
機器のネットワーク接続の管理	ネットワークモニタの有効化	○	×	×	×	×
	ネットワーク接続の制御	○	○	○	×	○
レポートの作成		○	△ ※8	△ ※8	○	△

（凡例）○：対象となる　△：収集できる機器情報に依存する　×：対象外

注※1　UNIX エージェント、Mac エージェントは除きます。

注※2　管理形態によって、収集できる機器情報が異なります。それぞれのコンピュータから収集できる情報の詳細については、次を参照してください。

- (1)　収集できる機器情報の種類
- (2)　機器の状態として収集できる情報
- (3)　システム情報として収集できる情報
- (4)　ハードウェア情報
- (5)　インストールソフトウェア情報
- (6)　セキュリティ情報
- (7)　資産情報と機器情報の共通管理項目

注※3　エージェントレスでセキュリティ状況を診断したい場合は、Windows の管理共有を利用してください。なお、エージェントレスでは、スクリーンセーバーのセキュリティ判定はアカウント単位に実施できません。

注※4　情報によって対象となるかどうかが異なります。詳細については、「(4)　ハードウェア情報」を参照してください。

注※5　USB デバイスの登録はできません。

注※6　リモートインストールマネージャを使用した配布だけ実行できます。ITDM 互換配布は実行できません。

注※7　RFB で接続した場合だけ、コンピュータを操作できます。

注※8　情報によって対象となるかどうかが異なります。ソフトウェアや機器の管理状況などは対象となりますが、セキュリティ状況は対象外です。

注※9　自動対策できるのは、更新プログラムの自動更新、使用禁止ソフトウェアの起動抑止、サービスまたは OS のセキュリティ設定だけです。

注※10　「登録済み USB デバイスの使用許可」の設定で、「使用を許可する資産の限定」は設定できません。

2.6.5　エージェントレスでの管理

JP1/IT Desktop Management 2 では、エージェントをインストールしない（エージェントレス）でコンピュータを管理対象にできます。コンピュータをエージェントレスで管理することで、研究用のコンピュータや業務用のサーバなどの運用上ソフトウェアをインストールできないコンピュータも、利用者のコンピュータと同じように JP1/IT Desktop Management 2 で管理できます。

コンピュータをエージェントレスで管理するためには、探索で発見されたコンピュータを管理対象にしてください。

> **重要**
>
> エージェントレスで管理するための設定は、セキュリティに関わる設定のため、影響範囲を十分に考慮した上で、エージェントレスで管理するかどうかを判断してください。

エージェントレスでの管理には、Windows の管理共有を利用する方法、SNMP を利用する方法、および Active Directory を利用する方法の 3 種類があります。それぞれの仕組みを次に示します。

Windows の管理共有を利用したエージェントレス管理

Windows の管理共有の認証を利用して、定期的に非常駐の実行プログラムをコンピュータに送り込みます。プログラムは、WMI を使用して、機器情報を収集します。

次のタイミングで機器情報を収集できます。

- 探索を実行するタイミング
- ［エージェントレス管理の設定］画面で指定した更新間隔でのタイミング
- 機器画面の機器一覧で、［操作メニュー］から［最新の情報を取得する］を選択したタイミング

> **ヒント**
>
> コンピュータを右クリックして表示されるポップアップメニューから［最新の情報を取得する］を選択しても、機器情報を収集できます。

> **重要**
>
> エージェントレスでコンピュータを管理する場合、管理用サーバから機器情報収集用の実行プログラムを送信します。この操作は Windows のデフォルト設定ではセキュリティブロックされるため、セキュリティレベルの設定を解除する必要があります。セキュリティレベルの設定解除は、環境を十分考慮した上で判断してください。

SNMP を利用したエージェントレス管理

標準的な通信プロトコルである SNMP の認証を利用して、SNMP によって定期的に機器情報を収集します。機器情報を収集できるタイミングは、Windows の管理共有を利用したエージェントレス管理方法と同じです。

Active Directory を利用したエージェントレス管理

Active Directory で管理している機器情報を収集します。

次のタイミングで機器情報を収集できます。

- 探索を実行するタイミング
- 機器画面の機器一覧で、［操作メニュー］から［最新の情報を取得する］を選択したタイミング

> **重要**
>
> Active Directory を利用したエージェントレス管理は、ドメインコントローラ上の情報を収集します。ドメインコントローラと管理対象機器の情報の同期が取れていない場合は、収集した情報が管理対象の機器と異なる場合があります。

なお、Windows の管理共有、SNMP、または Active Directory を利用するためには、コンピュータの設定が必要です。設定の詳細については、「4.2.8　エージェントレスで管理するための前提条件」を参照してください。

エージェントレスでコンピュータを管理する場合、エージェントをインストールした場合と比較して、管理用サーバから実行できる機能に差異があります。エージェントの有無による機能差異については、「(1) 管理形態による機能差異」を参照してください。

重要

エージェントレスでセキュリティ管理をしたい場合は、Windows の管理共有を利用してください。

(1) 管理形態による機能差異

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には、管理用サーバから実行できる機能に差異があります。エージェント導入済みのコンピュータの場合は、オンライン管理のときとオフライン管理のときでも差異があります。

管理形態による機能差異を次の表に示します。

機能		管理対象のコンピュータ				
		エージェント導入済み				エージェントレス
		オンライン管理			オフライン管理※1	
		Windows	UNIX	Mac OS		
機器情報の収集※2		○	△	△	○	△
セキュリティ状況の診断	セキュリティポリシーの割り当て	○	○	○	○	○
	セキュリティ状況の診断	○	×	△	○	△ ※3
セキュリティポリシーの違反時のアクション	セキュリティの自動対策	○	×	×	△ ※9	×
	印刷の抑止	○	×	×	○	×
	データの持ち出し抑止	○	×	×	△※10	×
	ソフトウェアの起動抑止	○	×	×	○	×
	操作ログの取得	○	×	×	×	×
	メッセージの通知	○	×	×	×	×
	電源の ON および OFF	○	×	×	×	×
資産情報の管理	ハードウェアの管理	○	△ ※4	△ ※4	○ ※5	△

機能		管理対象のコンピュータ				
		エージェント導入済み				エージェントレス
		オンライン管理			オフライン管理※1	
		Windows	UNIX	Mac OS		
資産情報の管理	ソフトウェアライセンスの管理	○	○	○	○	△
	ソフトウェアの管理	○	○	○	○	○
	契約の管理	○	○	○	○	○
ソフトウェアおよびファイルの配布	ソフトウェアの配布	○	○ ※6	×	○ ※6	×
	ファイルの配布	○	○ ※6	×	○ ※6	×
	ソフトウェアのアンインストール	○	×	×	×	×
機器のリモートコントロール	コンピュータの操作	○	×	○ ※7	×	○ ※7
	コンピュータからの接続要求	○	×	×	×	×
	ファイル転送	○	×	×	×	×
	チャット	○	×	×	×	×
機器のネットワーク接続の管理	ネットワークモニタの有効化	○	×	×	×	×
	ネットワーク接続の制御	○	○	○	×	○
レポートの作成		○	△ ※8	△ ※8	○	△

（凡例）○：対象となる　△：収集できる機器情報に依存する　×：対象外

注※1　UNIX エージェント、Mac エージェントは除きます。

注※2　管理形態によって、収集できる機器情報が異なります。それぞれのコンピュータから収集できる情報の詳細については、次を参照してください。

- (1)　収集できる機器情報の種類
- (2)　機器の状態として収集できる情報

- (3)　システム情報として収集できる情報
- (4)　ハードウェア情報
- (5)　インストールソフトウェア情報
- (6)　セキュリティ情報
- (7)　資産情報と機器情報の共通管理項目

注※3　エージェントレスでセキュリティ状況を診断したい場合は、Windows の管理共有を利用してください。なお、エージェントレスでは、スクリーンセーバーのセキュリティ判定はアカウント単位に実施できません。

注※4　情報によって対象となるかどうかが異なります。詳細については、「(4)　ハードウェア情報」を参照してください。

注※5　USB デバイスの登録はできません。

注※6　リモートインストールマネージャを使用した配布だけ実行できます。ITDM 互換配布は実行できません。

注※7　RFB で接続した場合だけ、コンピュータを操作できます。

注※8　情報によって対象となるかどうかが異なります。ソフトウェアや機器の管理状況などは対象となりますが、セキュリティ状況は対象外です。

注※9　自動対策できるのは、更新プログラムの自動更新、使用禁止ソフトウェアの起動抑止、サービスまたは OS のセキュリティ設定だけです。

注※10　「登録済み USB デバイスの使用許可」の設定で、「使用を許可する資産の限定」は設定できません。

(2)　エージェントレスで管理するための前提条件

エージェントレスでコンピュータを管理して機器情報を取得する場合、管理用サーバと利用者のコンピュータで設定が必要です。認証状態によって取得できる機器情報が異なります。取得できる情報が少ないと、セキュリティ状況の一部が判定できなかったり、レポート上で集計されなかったりして、正しく運用できなくなるおそれがあります。運用の目的に応じて、適切な認証方法を選択してください。

なお、Active Directory を利用してコンピュータを管理していると、大部分の機器情報を取得するための設定が容易になります。エージェントレス運用を考えている場合は、まず組織内のコンピュータが Active Directory で管理されているかどうかを確認することをお勧めします。

取得できる機器情報の差異については、「2.6.2　機器情報の収集」を参照してください。

> **重要**
>
> NAT 環境では、エージェントレスの機器は管理できません。

重要

ネットワークの探索で発見した機器をエージェントレスで管理している場合、その機器に対する探索範囲および認証情報を削除しないでください。また、Active Directory の探索で発見した機器をエージェントレスで管理している場合は、その機器が登録されている Active Directory の設定を削除しないでください。削除すると、機器情報が取得されなくなります。削除してしまった場合は、探索範囲、認証情報、または Active Directory の設定を追加したあとにネットワークの探索または Active Directory の探索を再実行して、機器を発見してください。

重要

DHCP 環境の場合、機器の IP アドレスが変更され探索範囲外になると、機器情報が取得されなくなります。

Windows の管理共有を利用してエージェントレス管理する場合

次の条件をすべて満たしている必要があります。

- 利用者のコンピュータで、Windows ファイアウォールが無効になっている。※1
- 利用者のコンピュータで、簡易ファイル共有が無効になっている。
- 利用者のコンピュータで、Windows の管理共有（ADMIN$）が有効になっている。
- 利用者のコンピュータで、プロセス間通信用共有（IPC$）が有効になっている。
- 管理用サーバで、Windows の管理共有を使用して対象のコンピュータにログオンするための情報が、ネットワークの探索の認証情報として設定されている。※2

注※1　有効の場合でも、TCP（ポート番号：445）を許可しておけば条件が満たされます。

注※2　Windows の管理共有を使用して対象のコンピュータにログオンするための認証情報は、次の条件のどちらかを満たしている必要があります。

- 利用者のコンピュータのビルトイン Administrator アカウントとパスワードを使用する。
- 利用者のコンピュータの UAC 機能が無効になっている。

管理用サーバから Windows の管理共有にアクセスできるようにする設定は、利用者のコンピュータの OS によって異なります。Windows の管理共有にアクセスするためには、次の表に示す設定が必要です。

OS	設定内容
Windows 10	• UAC の無効化、または Administrator ユーザーの有効化※1 • ネットワークと共有センターの［ファイルとプリンタの共有］の有効化
Windows 8.1	
Windows 8	
Windows 7	

OS	設定内容
Windows Vista	• UAC の無効化、または Administrator ユーザーの有効化 • ネットワークと共有センターの［ファイル共有］の有効化
Windows XP※2	• 簡易ファイル共有の無効化 • ファイル共有の追加
Windows Server 2019	ネットワークと共有センターの、［ファイル共有］または［ファイルとプリンタの共有］の有効化
Windows Server 2016	
Windows Server 2012	
Windows Server 2008	
Windows Server 2003	設定不要（デフォルトで有効）
Windows 2000	ファイル共有の追加
Windows 以外のコンピュータ	対象外（設定できない）
ネットワーク装置	対象外（設定できない）

注※1　エディションがない Windows 8.1 および Windows 8 の場合は、コマンドプロンプトで net user コマンドを実行して有効化してください。Windows のコントロールパネルからは Administrator ユーザーを有効にできません。

注※2　Windows XP Home Edition(Service Pack 2、3)の場合は、管理共有が使用できません。

これらの条件を満たしている場合、大部分の機器情報を取得できます。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と、取得できる情報に大きな差異はありません。

SNMP を利用してエージェントレス管理する場合

次の条件を満たしている必要があります。

- SNMP を利用できる。
- コミュニティ名を認証できる。

なお、SNMP を使用して機器情報を取得するためには次の表に示す設定が必要です。

OS	設定内容
Windows 10	• SNMP エージェントの導入 • SNMP エージェントの設定
Windows 8.1	
Windows 8	
Windows 7	
Windows Vista	
Windows XP	

OS	設定内容
Windows Server 2019	• SNMP エージェントの導入 • SNMP エージェントの設定
Windows Server 2016	
Windows Server 2012	
Windows Server 2008	
Windows Server 2003	
Windows 2000	
Windows 以外のコンピュータ	
ネットワーク装置	

Active Directory を利用してエージェントレス管理する場合

次の条件をどちらも満たしている必要があります。

- 利用者のコンピュータで、Windows ファイアウォールが無効になっている。※
- Active Directory 連携機能を使用して、管理用サーバで Active Directory が管理する機器情報を収集できる。

注※　有効の場合でも、設定画面の［他システムとの接続］－［Active Directory の設定］画面で指定したポート番号での接続を許可しておけば、条件が満たされます。

ICMP を利用してエージェントレス管理する場合

ICMP を利用できる必要があります。

なお、ICMP を使用して機器情報を取得するためには、次の表に示す設定が必要です。

OS	設定内容
Windows 10	ICMP エコー要求の着信許可※
Windows 8.1	
Windows 8	
Windows 7	
Windows Vista	
Windows XP	
Windows Server 2019	
Windows Server 2016	
Windows Server 2012	
Windows Server 2008	

OS	設定内容
Windows Server 2003	ICMP エコー要求の着信許可※
Windows 2000	
Windows 以外のコンピュータ	
ネットワーク装置	

注※　Windows XP 以降では、Windows ファイアウォールで ICMP を許可する設定をするか、Windows ファイアウォールを解除する必要があります。

関連リンク

- (1)　収集できる機器情報の種類
- (2)　機器の状態として収集できる情報
- (3)　システム情報として収集できる情報
- (4)　ハードウェア情報
- (5)　インストールソフトウェア情報
- (6)　セキュリティ情報
- (7)　資産情報と機器情報の共通管理項目

(3)　エージェントレスの機器の認証情報を設定する手順

エージェントレスの機器からは、ネットワークの探索で設定された探索範囲と認証情報の組み合わせを利用して、機器情報が収集されます。機器情報の収集時は、その機器の IP アドレスが含まれる探索範囲に対して設定された認証情報が利用されます。

エージェントレスの機器に対して使用される認証情報は、探索が完了したあとでも設定できます。

エージェントレスの機器の認証情報を設定するには：

1. 機器画面を表示します。
2. メニューエリアの［機器情報］で任意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、エージェントレスの機器を選択します。
4. ［操作メニュー］の［認証情報を設定する］を選択します。
5. 表示されるダイアログで、認証情報を設定します。
6. ［OK］ボタンをクリックします。

エージェントレスの機器に対して利用される認証情報が設定されます。

ヒント

設定画面の［探索条件の設定］－［ネットワークの探索］画面から、認証情報を設定することもできます。

(4) エージェントレスでの機器情報の収集

エージェントレスの機器からは、次に示す方法で機器情報が収集されます。

管理共有

Windows の管理共有の認証を利用して、機器情報が収集されます。エージェントをインストールした場合に近い情報量を収集できます。

SNMP

SNMP プロトコルの認証を利用して、機器情報を収集します。SNMP によって取得できる一部の機器情報だけ収集できます。

Active Directory

Active Directory で管理している機器情報を参照して、機器情報を収集します。Active Directory で取得できる一部の機器情報だけ収集できます。

ARP

ARP から機器情報を収集します。ARP から取得できる一部の機器情報だけ収集できます。

ICMP

ICMP（PING）を利用して、機器の存在を確認します。IP アドレスの情報だけ収集できます。

管理対象のエージェントレスの機器からは、管理共有または SNMP を利用して機器情報が収集されます。ARP および ICMP は、管理共有または SNMP の認証に失敗している機器だけに利用されます。管理共有または SNMP の認証に成功している機器に対しては、ARP および ICMP は利用されません。

管理共有と SNMP のどちらが利用されるかは、探索設定で設定した探索範囲と認証情報に依存します。エージェントレスの機器から機器情報が収集されるときは、機器の IP アドレスに対して、その IP アドレスが含まれる探索範囲に対応した認証情報を利用して、機器情報の収集が実行されます。機器の IP アドレスが探索範囲外にある、認証情報が設定されていない、認証に失敗したなどの場合は、機器情報は収集されません。

なお、エージェントレスの機器は、機器の種類ごとに利用できる収集方法が異なります。機器の種類と収集方法の利用可否を次の表に示します。

収集方法	機器の種類		
	Windows のコンピュータ	Windows 以外のコンピュータ	ネットワーク装置
管理共有	○	×	×
SNMP	○	○	○

収集方法	機器の種類		
	Windows のコンピュータ	Windows 以外のコンピュータ	ネットワーク装置
Active Directory	○	×	×
ARP	○	○	○
ICMP	○	○	○

（凡例）○：利用できる　×：利用できない

機器情報が収集されるタイミング

エージェントレスの機器からは、機器情報は次のタイミングで収集されます。

- 機器の探索を実行したとき
- 機器画面の機器一覧で、［操作メニュー］から［最新の情報を取得する］を選択したとき

なお、収集される間隔を変更したい場合は、設定画面の［エージェント］－［エージェントレス管理の設定］画面で更新間隔を設定します。デフォルトの更新間隔は 1 時間です。

機器画面の［最新の情報を取得する］を実行することで、任意のタイミングで機器情報を収集することもできます。

また、集中探索が実行されている場合、その期間中は機器情報が収集されません。

> **重要**
>
> Active Directory を利用する場合は、Active Directory に登録されている機器の探索を実行したときに機器情報を収集します。

関連リンク

- (5)　エージェントレスでの管理共有による機器情報の収集の仕組み
- (3)　エージェントレスの機器の認証情報を設定する手順

(5)　エージェントレスでの管理共有による機器情報の収集の仕組み

エージェントレスのコンピュータから管理共有の認証を利用して機器情報を取得する場合、コンピュータに実行プログラムが送信されます。

送信される実行プログラム名は次の 3 種類です。

- jpngmain.exe
- jpnmspushlauncher.exe
- jpnmspushservice.exe

これらの実行プログラムによって、収集した機器情報を通知するための管理共有のファイルが、コンピュータ上に生成されます。このファイルが管理用サーバに通知されることで、エージェントレスのコンピュータの機器情報が更新されます。

なお、実行プログラムは初回およびバージョンアップ時だけ配信されます。また、実行プログラムは自動的には削除されません。管理用サーバをバージョンアップしたときや、実行プログラムのファイルが削除されたときは、実行プログラムが再度送信されます。

重要

上記の実行プログラムは削除しないでください。エージェントレスの機能が正常に動作できなくなるおそれがあります。また、導入しているウィルス対策製品によっては、誤って上記の実行プログラムがウィルスとして検知され、正しく実行できない場合があります。このような場合は、エージェントを導入してコンピュータを管理してください。

ヒント

Windows の管理共有の認証が成功した時点で、約 2.5 メガバイトの実行プログラムがコンピュータに送信されます。

2.6.6 MDM システムとの連携

MDM システムと連携すると、MDM システムで管理しているスマートデバイスの情報を取得し、スマートデバイスを JP1/IT Desktop Management 2 の管理対象にできます。取得した情報を JP1/IT Desktop Management 2 で管理したり、スマートデバイスを JP1/IT Desktop Management 2 から制御したりできます。

複数サーバ構成で MDM システムと連携する場合、管理用サーバごとに MDM システムと連携する必要があります。

MDM システムと連携すると利用できる機能を、次の表に示します。

機能	説明
スマートデバイスの情報の取得	MDM システムで管理されているスマートデバイスの情報を取得し、スマートデバイスを JP1/IT Desktop Management 2 の管理対象にできます。また、MDM システムから定期的に情報を取得して、各スマートデバイスの機器情報、資産情報、およびセキュリティ状況を管理できます。
スマートデバイスの制御	MDM システムで管理しているスマートデバイスに対して、ロック、初期化およびパスコードのリセットができます。

関連リンク

- (1) MDM システムで管理されているスマートデバイスの情報の取得
- (2) MDM システムから取得できる機器情報

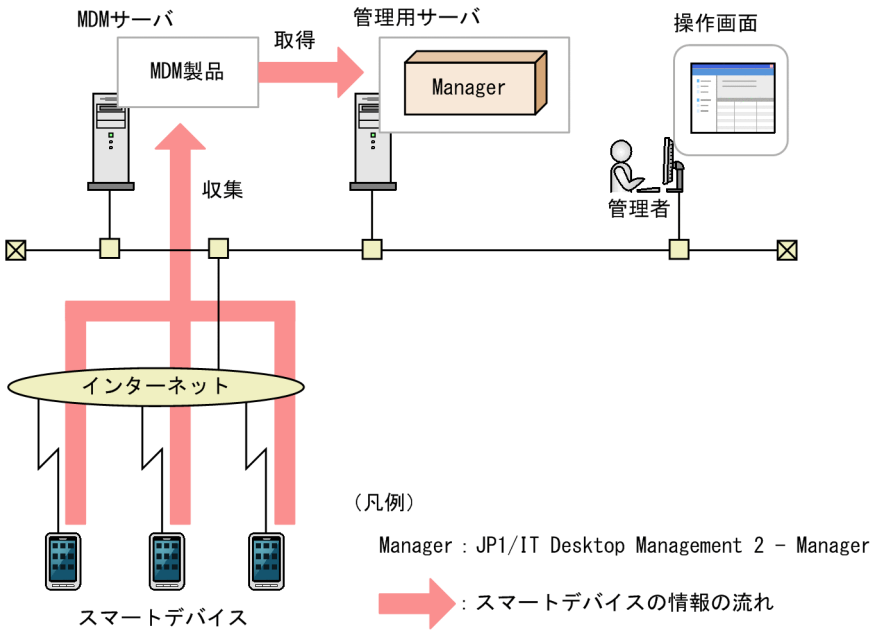
- (4)　MDM 連携時の注意事項
- 2.23　スマートデバイスの制御

(1)　MDM システムで管理されているスマートデバイスの情報の取得

MDM システムで管理されているスマートデバイスの情報を取得できます。スマートデバイスの情報を取得すると、スマートデバイスを JP1/IT Desktop Management 2 の管理対象にして、スマートデバイスの機器情報、資産情報、およびセキュリティ状況を管理できます。また、管理対象のスマートデバイスの情報を取得することで、その機器情報が更新されます。

> **ヒント**
>
> スマートデバイスを JP1/IT Desktop Management 2 の管理対象にすると、ほかの機器と同様に製品ライセンスが消費されます。

MDM システムからスマートデバイスの情報を取得する流れを次の図に示します。



MDM システムで管理されているスマートデバイスの情報を取得する方法を次に示します。

即時実行

MDM システムに接続して、即時にスマートデバイスの情報を取得します。初期導入時や、MDM システムでの情報の変更をすぐに JP1/IT Desktop Management 2 に反映したいときは、この方法をお勧めします。

定期実行

MDM 連携の設定に従って、スマートデバイスの情報を定期的に取得し、自動的に管理対象にします。取得スケジュールは、設定画面で［開始時刻］［繰り返し単位］（日、週、月）［繰り返しの方法］を設定できます。デフォルトは、設定されていません。

ヒント

MDM システム上でスマートデバイスを削除した場合、JP1/IT Desktop Management 2 の機器情報とは同期しません。MDM システムで管理されているスマートデバイスを削除する場合、JP1/IT Desktop Management 2 からも削除したいときは、機器情報を削除してください。

(2) MDM システムから取得できる機器情報

MDM システムから取得できる機器情報を次の表に示します。

システム情報

機器情報の項目		機器情報の取得可否	取得元の MDM システムの対応する項目		内容
			JP1/ITDM2 - SDM※1 の場合	MobileIron の場合	
機器種別		Si、SA、M	−	−	「スマートデバイス」が設定されます。

コンピュータ情報	コンピュータ名（説明）	Si、SA、M	次のどちらかを表示※2
			• [管理対象のスマートデバイス一覧] − [名称]
			• 次の項目を組み合わせて表示
			  • [システム情報] − [利用者]
			  • [システム情報] − [電話番号]
			  • [ハードウェア] − [型番]
				−	MDM システムでスマートデバイスを識別するために表示しているスマートデバイスの名称※2、ユーザー名、契約電話番号、およびモデル名が取得されます。

	ホスト名	Si、M			
	モデル（メーカー）	モデル Si、SA、M メーカー Si※3、SA、M	次の項目を組み合わせて表示 • [ハードウェア] − [型番] • [ハードウェア] − [製造者名]	−	スマートデバイスの製造元で付与されたスマートデバイスのモデル名、およびスマートデバイスの製造元が取得されます。
	シリアルナンバー	Si、SA※3、M	[ハードウェア] − [シリアル番号]	SerialNumber	スマートデバイスのシリアル番号が取得されます。
	メモリ	SA、M	[ハードウェア] − [RAM]	total_ram_size_bytes	スマートデバイスに搭載されているメモリの合計容量です。
OS 情報	OS	Si、SA、M	次の項目を組み合わせて表示	OS	OS の名称とバージョンが取得されます。

機器情報の項目		機器情報の取得可否	取得元の MDM システムの対応する項目		内容
			JP1/ITDM2 - SDM※1 の場合	MobileIron の場合	
OS 情報	OS	Si、SA、M	• [システム情報] − [OS] • [システム情報] − [OS バージョン]	OS	OS の名称とバージョンが取得されます。
ネットワーク情報	MAC アドレス	Si、SA、M	• [ハードウェア] − [WiFi MAC アドレス] • [ハードウェア] − [Bluetooth MAC アドレス]	• WiFiMAC • wifi_mac_addr • BluetoothMAC	MAC アドレスが取得されます。
スマートデバイス情報	IMEI	Si、SA、M	[ハードウェア] − [IMEI]	imei	スマートデバイスに付与されている識別番号である IMEI が取得されます。
	UDID	Si、M	[ハードウェア] − [UDID]	udid	Apple 社製のスマートデバイスに付与されている識別子である UDID が取得されます。
	IMSI	Si、SA、M	[システム情報] − [SIM カード]	• imsi • registration_imsi • current_SIM_module_number	契約通信会社がスマートデバイスの SIM カードに割り当てた識別番号である IMSI が取得されます。
	ICCID	Si、SA、M	[ハードウェア] − [ICCID]	−	スマートデバイスの SIM カードに付与されている番号である ICCID が取得されます。
	モデル（メーカー）	モデル Si、SA、M メーカー Si※3、SA、M	次の項目を組み合わせて表示 • [ハードウェア] − [型番] • [ハードウェア] − [製造者名]	−	スマートデバイスの製造元で付与されたスマートデバイスのモデル名、およびスマートデバイスの製造元が取得されます。
	シリアルナンバー	Si、SA※3、M	[ハードウェアー [シリアル番号]	SerialNumber	スマートデバイスのシリアル番号が取得されます。
	契約電話番号	Si、SA、M	[システム情報] − [電話番号]	Number	スマートデバイスで利用している電話番号が取得されます。
	メールアドレス	Si、SA、M	[システム情報] − [メールアドレス]	−	スマートデバイスで利用しているメールアドレスが取得されます。

機器情報の項目		機器情報の取得可否	取得元の MDM システムの対応する項目		内容
			JP1/ITDM2 - SDM※1 の場合	MobileIron の場合	
スマートデバイス情報	キャリア	Si、SA、M	[システム情報] − [SIM カード]	• current_operator_name • Operator	スマートデバイスの契約通信会社名が取得されます。
	パスコード設定状況またはパスワード設定状況	Si、SA※3、M	−	PasscodePresent	スマートデバイスにパスコードまたはパスワードが設定されているかどうかが取得されます。
	RAM（空き容量）	SA、M	[ハードウェア] − [RAM]	次の項目を組み合わせて表示 • total_ram_size_bytes • free_ram_size_bytes	RAM RAM の容量が取得されます。 空き容量 RAM の空き容量が取得されます。
	内蔵ストレージ（空き容量）	Si、SA、M	[ハードウェア] − [内部ストレージ]	次の項目を組み合わせて表示 • total_storage_size_bytes • free_storage_size_bytes	内蔵ストレージ 内蔵ストレージの容量が取得されます。 空き容量 内蔵ストレージの空き容量が取得されます。
	外部ストレージ（空き容量）	SA、M	[ハードウェア] − [SD カード]	次の項目を組み合わせて表示 • total_media_card_size_bytes • free_media_card_size_bytes	外部ストレージ 外部ストレージの容量が取得されます。 空き容量 外部ストレージの空き容量が取得されます。
メモリ情報	容量	SA、M	[ハードウェア] − [RAM]	total_ram_size_bytes	メモリの容量が取得されます。
ハードディスク情報	容量	Si、SA、M	[ハードウェア] − [内部ストレージ]	total_storage_size_bytes	ハードディスク全体の容量が取得されます。
ソフトウェア情報※4	ソフトウェア名	Si、SA	[ソフトウェア] − [アプリケーション名]	−	インストールされているソフトウェアのソフトウェア名が取得されます。
	バージョン	Si、SA	[ソフトウェア] − [バージョン]	−	インストールされているソフトウェアのバージョンが取得されます。
	メーカー	Si、SA	[ソフトウェア] − [製造元]	−	インストールされているソフトウェアの製造元が取得されます。

（凡例）

Si：JP1/IT Desktop Management 2 - Smart Device Manager と連携している場合で、スマートデバイスの OS が iOS のときに取得できる

SA：JP1/IT Desktop Management 2 - Smart Device Manager と連携している場合で、スマートデバイスの OS が Android のときに取得できる

M：MobileIron と連携している場合に取得できる

－：機器情報の取得可否に関係なく、取得元の MDM システムに対応する項目がない

注※1　JP1/ITDM2 - SDM：JP1/IT Desktop Management 2 - Smart Device Manager

注※2　JP1/IT Desktop Management 2 - Smart Device Manager が 11-00-03 以降の場合、デフォルトでは［管理対象のスマートデバイス一覧］－［名称］がスマートデバイスの名称として表示されます。コンフィグレーションファイル（jdn_manager_config.conf）の SDM_Mapping_Name プロパティを変更することで、［システム情報］－［利用者］、［システム情報］－［電話番号］および［ハードウェア］－［型番］を組み合わせてコロン（:）で結合した形式の名称を表示させることもできます。詳細は、マニュアル「JP1/ITDM2 - Manager 構築ガイド」の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の説明を参照してください。

注※3　JP1/IT Desktop Management 2 - Smart Device Manager が 11-00-04 以降の場合に取得できます。

注※4　このソフトウェア情報を取得するには、定義ファイルsdm_import.properties を作成して、*JP1/IT Desktop Management 2 - Manager のインストールフォルダ*¥mgr¥conf 下に格納する必要があります。定義ファイルsdm_import.properties の詳細については、「(3)　MDM システムからソフトウェア情報を取得する設定」を参照してください。なお、このソフトウェア情報は、機器画面の［ソフトウェア一覧］画面や［インストールソフトウェア］タブ、資産画面の［管理ソフトウェア］画面などに表示されますが、場合によっては、数千件以上の情報が取り込まれることがあります。その場合は視認性の低下を招くので注意してください。

また、ほかに次の表に示す情報も取得できます。

機器情報の項目	説明
管理種別	「MDM 連携管理」が設定されます。
機器状態	MDM システムからスマートデバイスの情報を取得した場合、および初期化したスマートデバイスを再登録した場合は、「不明」が設定されます。 スマートデバイスの初期化が成功した場合は、「警告」が設定されます。
管理形態	「エージェント未導入」が設定されます。
最終接続確認日時	スマートデバイスが MDM システムに接続したときの日時が設定されます。

機器情報の詳細については、次を参照してください。

- (1)　収集できる機器情報の種類
- (2)　機器の状態として収集できる情報

- (3)　システム情報として収集できる情報
- (4)　ハードウェア情報
- (5)　インストールソフトウェア情報
- (6)　セキュリティ情報
- (7)　資産情報と機器情報の共通管理項目

(3)　MDM システムからソフトウェア情報を取得する設定

ここでは、スマートデバイスのソフトウェア情報を取得する場合に必要な定義ファイル（sdm_import.properties）を設定する方法について説明します。

定義ファイル（sdm_import.properties）を設定するには：

1. *Key=Value* の形式で記載した定義ファイル（sdm_import.properties）を作成して、次に示す格納先に格納します。文字コードは UTF-8 で保存してください。

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

定義ファイル（sdm_import.properties）で設定する内容を次の表に示します。

Key	Value の内容	説明
sdm.*N*.name	取り込み対象とする MDM システム（JP1/ITDM2 - SD Manger）との連携情報を設定した MDM 設定名	設定画面の［他システムとの接続］－［MDM 連携の設定］画面で、［MDM 設定名］に指定した内容と同じ値を指定します。 *N* には自然数を設定します。取り込み対象とする連携設定が複数ある場合は 1、2 のように、複数のキーを指定できます。
sdm.*N*.dbhost	JP1/ITDM2 - SDM※1 サーバのデータベースに接続するための IP アドレスまたはホスト名	JP1/IT Desktop Management 2 - Manager をインストールしたコンピュータと同じネットワークセグメント内で、接続できる JP1/ITDM2 - SDM※1 サーバの IP アドレスまたはホスト名※2 を指定します。 *N* には自然数を設定します。取り込み対象とする連携設定が複数ある場合は 1、2 のように、複数のキーを指定できます。
sdm.*N*.dbport	JP1/ITDM2 - SDM※1 サーバのデータベースに接続するためのポート番号	JP1/ITDM2 - SDM※1 サーバのスマートデバイスマネージャー内に構築したデータベースとの通信用のポート番号※3 を指定します。 *N* には自然数を設定します。取り込み対象とする連携設定が複数ある場合は 1、2 のように、複数のキーを指定できます。 省略した場合は、[26066]ポート番号を使用します。

注※1　JP1/ITDM2 - SDM：JP1/IT Desktop Management 2 - Smart Device Manager

注※2　ホスト名を指定する場合は、次の点に注意してください。

- 文字数は 1 ～32 文字です。
- hostname コマンドを実行して表示されたホスト名を指定します。
- ホスト名の大文字と小文字は区別されます。
- ホスト名の別名は指定できません。
- 指定したホスト名は hosts ファイルまたは DNS などに登録し、名前解決しておく必要があります。
- ホスト名を FQDN 形式で指定する場合は、ホスト名を FQDN 形式で定義しておく必要があります。

注※3　JP1/ITDM2 - SDM※1 のスマートデバイスマネージャーサーバで、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、指定したポートを通過（送信／受信 双方向）できるように設定してください。

定義ファイル（sdm_import.properties）の設定例

MDM 設定名が「ITDM2 SD Manager 01」、「ITDM2 SD Manager 02」の MDM 連携製品が登録されている場合の設定例を次に示します。

```
sdm.1.name=ITDM2 SD Manager 01
sdm.1.dbhost=192.168.50.100
sdm.1.dbport=26066
sdm.2.name=ITDM2 SD Manager 02
sdm.2.dbhost=SDM-Server02
sdm.2.dbport=36066
```

(4)　MDM 連携時の注意事項

MDM システムと連携する場合の注意事項を次に示します。

- MDM サーバのホスト名に、「_」は使用できません。
- MDM 連携機能で取得できる機器情報は、スマートデバイスの OS や MDM システムごとに異なります。このため、取得できた項目だけが表示されます。
- スマートデバイスの SIM カードを入れ替えた場合、IMEI は変更されませんが、契約電話番号が変更されます。このため、スマートデバイスの情報を取得した場合、機器情報とスマートデバイスの IMEI が一致しないときは、異なるスマートデバイスとして認識されます。
- MDM サーバからプロキシサーバを通してスマートデバイスの情報を取得する場合、ネットワーク環境や取得するスマートデバイスの台数によって、管理用サーバと MDM サーバの接続がタイムアウトするおそれがあります。必要に応じてプロキシサーバのタイムアウト時間を変更してください。
- 連携する MDM システムではプロファイルが削除されているスマートデバイスに対して、ロック、パスコードのリセット、初期化などの操作はできません。JP1/IT Desktop Management 2 - Manager からプロファイルが削除されているスマートデバイスに対して次の操作をした場合、操作は失敗しますが、イベント、公開ログ、監査ログには操作の成功を示すメッセージが出力されます。

  [MobileIron 5.8 以降と連携する場合]

  　プロファイルが削除されているスマートデバイスに対してパスコードをリセット、または初期化する。

管理するスマートデバイスからは、プロファイルを削除しないようにしてください。

2.6.7 機器の自動メンテナンス

ここでは、重複機器（IP アドレス、ホスト名、MAC アドレスまたは BIOS シリアルナンバーが同一の機器）や不稼働機器（長期間稼働していない機器）の検出条件を設定し、対象と判定された機器の情報を自動的に削除する自動メンテナンスについて説明します。この機器の自動メンテナンスが有効になっていると、設定した条件に従って毎日、重複機器や不稼働機器の有無が検出され、該当する機器がある場合は、削除候補機器（管理が不要と考えられる機器）として一覧表示されて、設定した自動削除基準日時を過ぎると、機器の自動メンテナンスのスケジュールに従って自動的に削除されます。これによって、機器のリプレースや OS の再インストールなどによって新しく機器が追加された場合や機器を破棄する場合に、不要になった機器情報を自動的に削除できます。

機器のリプレースに際して、リプレース前後で同じ IP アドレスまたはホスト名を使用する場合を例に、機器のメンテナンスで不要になった機器情報を削除する運用の流れを次に示します。

1. 管理者が管理用サーバで重複機器の検出条件を設定します。
   重複条件に IP アドレスまたはホスト名を指定し、自動削除設定を有効にします。

   ヒント

   不要になった機器情報を手動で削除する場合は、自動削除設定を無効にします。

2. コンピュータの利用者はエージェントをアンインストールしないで機器をリプレースします。
   リプレース後の設定ではリプレース前に使用していた IP アドレスまたはホスト名を設定し、エージェントをインストールします。
3. エージェントからの通知によって管理用サーバは、リプレース後の機器を新しい機器として登録します。
   このとき、ライセンス不足の場合は発見状態になります。
4. 重複機器の自動削除によってリプレース前の古い機器が削除されます。

   ヒント

   自動削除設定を無効にしている場合、管理者はホーム画面の［通知事項］パネルに表示される削除候補機器存在の通知を参照して、重複機器を確認し、不要な古い機器を削除します。または、削除する必要がない機器の場合には、メンテナンス対象外機器（機器メンテナンスを抑止する機器）として登録します。

5. エージェントからの通知があった時、ライセンスに空きがある場合には、発見状態の機器は管理状態に変更になります。
6. 自動削除された機器を確認するには管理用サーバに出力されるイベントまたは構成変更の公開ログ JDNSTRC*x*.log（x：1～9）を参照します。

メモ

オフライン管理の機器は機器のメンテナンスの対象外です。

メモ

複数サーバ構成の統括管理用サーバ配下の管理用中継サーバが管理する機器は、統括管理用サーバでの機器のメンテナンスの対象外ですが、各管理用中継サーバでの機器のメンテナンスの対象にはなります（管理用中継サーバごとに機器のメンテナンスの設定をする必要があります）。管理用中継サーバが管理する機器が機器のメンテナンスによって削除された場合、管理用中継サーバは機器の削除を上位の管理用サーバに通知します。なお、機器のメンテナンスで削除した機器の情報は、各管理用サーバのJDNSTRC*x*.log（x：1～9）に出力されます。

メモ

機器の削除時には、機器情報の削除に連動してシステム構成情報も削除されます（このとき、あて先グループと ID からも削除されます）が、先にシステム構成情報から機器を削除した場合は、連動して機器情報が削除されることはありません。この場合は、手動で対象の機器情報を削除する必要があります。

ヒント

削除候補機器が、設定画面の［機器］－［機器メンテナンスの設定と検出結果確認］画面の下部に一覧で表示されます。

ヒント

機器情報の削除に連動してハードウェア資産を滅却することができます。

ヒント

重複機器と不稼働機器の自動削除が両方とも設定されている場合、重複機器の削除が先に実行され、そのあと不稼働機器の削除が実行されます。

ヒント

機器のリプレースまたは OS の再インストールによって新しく追加された機器に対して、ソフトウェアライセンスを割り当てる場合は、ソフトウェアライセンスの移管を利用してください。

機器のメンテナンスによって初めて機器情報削除の運用をする場合の留意事項

次に示す手順で対応してください。

1. 管理者が期待していない機器情報が間違って自動的に削除されないように、重複機器設定／不稼働機器設定の自動削除を無効にします。
2. 設定画面の［機器］－［機器メンテナンスの設定と検出結果確認］画面で、［検出を開始］ボタンをクリックして手動で削除候補の機器を検出し、メンテナンスの対象外にするか削除するかを判断してください。

重複機器の定義の設定

次に示す項目の重複条件と未接続日数を指定することで、削除候補となる重複機器の定義を設定できます。設定した重複条件に該当する機器のうちで、最終接続確認日時が古い（最新でない）機器であり、指定した未接続日数以上、管理用サーバに接続されていない機器が削除候補の重複機器と判断されます。なお、重複条件を複数指定した場合には AND 条件となります。また、これらの項目が未設定または無効な値の機器は、重複機器として扱われません。

- IP アドレス

  機器に IP アドレスが複数存在する場合には、管理用サーバとの接続に使用した IP アドレス（代表）を対象とします。
- ホスト名

  大文字小文字を区別する／区別しないを選択できます。
- MAC アドレス

  機器に MAC アドレスが複数存在する場合には、管理用サーバとの接続に使用した MAC アドレス（代表）を対象とします。
- BIOS シリアルナンバー

  MAC アドレスと BIOS シリアルナンバーを重複条件に指定した場合は、AND 条件であるため、BIOS シリアルナンバーが未設定の機器は重複機器に判断されることはありません。

不稼働機器の定義の設定

指定した未接続日数以上、管理用サーバに接続されていない機器が削除候補の不稼働機器と判断されます。

削除候補の検出条件

削除候補の検出条件として選択できるかどうか（対象になるかどうか）を、機器種別、管理形態、管理状態別に以下の表に示します。

機器種別	重複機器	不稼働機器
Windows/Mac エージェント	○	○
UNIX エージェント	○	○
エージェントレスの機器	○	○
スマートデバイス	○	○
ネットワークモニタが有効または有効化中の機器	×	×
中継システム	×	×

機器種別	重複機器	不稼働機器
管理用中継サーバ	×	×
API 管理機器	○	○

（凡例）○：選択できる（対象になる）　×：選択できない（対象にならない）

管理形態	重複機器	不稼働機器
オンライン管理	○（固定）	○（固定）
オフライン管理	×	×

（凡例）○：選択できる（対象になる）　×：選択できない（対象にならない）

管理状態	重複機器	不稼働機器
管理対象の機器	○（固定）	○（固定）
発見状態の機器	○（固定）	○（固定）
除外対象の機器	×	×

（凡例）○：選択できる（対象になる）　×：選択できない（対象にならない）

重複機器を検出する運用の想定例を次の表に示します。

メンテナンスの契機	重複条件				
	エージェント導入済み		エージェントレス	スマートデバイス	API
	Windows/Mac OS	UNIX			
機器のリプレース	IP アドレス	IP アドレス、ホスト名	IP アドレス	ホスト名※1	IP アドレス、ホスト名
HDD 故障／ホスト識別子再生成／OS の入れ替え	BIOS シリアルナンバーまたは MAC アドレス	MAC アドレス	IP アドレス	－	BIOS シリアルナンバー、MAC アドレス、IP アドレス
スマートデバイス再登録（JP1/ITDM2 - SDM※2）	－	－	－	ホスト名※3	－

（凡例）－：対象外

注※1　MobileIron の場合です。ただし、Wi-Fi 端末の場合には使用できません。

注※2　JP1/ITDM2 - SDM：JP1/IT Desktop Management 2 - Smart Device Manager

注※3　Wi-Fi 端末の場合には使用できません。

メンテナンス対象外機器（機器メンテナンスを抑止する機器）の指定

長期出張やクラスタ環境などによって、長期間、管理用サーバへのアクセスのない機器を明示的に指定して機器メンテナンスの対象外にすることができます。メンテナンスの対象外として登録された機器は次に示すように扱われます。

- 設定した検出条件に該当しても、削除候補機器としてカウントされません。
- 削除候補機器の自動削除によって削除されることはありません。

削除候補機器の自動削除の設定

削除候補機器が自動的に削除されるように設定することができます。この際、削除されるまでの期間を決めることができ、この期間内に管理者は機器を確認して、メンテナンス対象外（機器メンテナンスを抑止する機器）に指定することができます。重複機器、不稼働機器の定義それぞれで設定できます。

自動削除の設定をした場合、次のように処理されます。

重複機器

削除候補の重複機器のうち、重複機器の定義の［自動削除されるまでの期間］に［未接続の期間］を加えた期間以上、管理用サーバに接続されていない機器が自動的に削除されます。

不稼働機器

削除候補の不稼働機器のうち、不稼働機器の定義の［自動削除されるまでの期間］に［未接続の期間］を加えた期間以上、管理用サーバに接続されていない機器が自動的に削除されます。

機器の自動メンテナンスのスケジュール

機器の自動メンテナンスのスケジュールは、重複機器、不稼働機器ともに、コンフィグレーションファイル（jdn_manager_config.conf）のDeviceAutoMaintenanceTime プロパティに設定した値に従って実行されます。DeviceAutoMaintenanceTime プロパティについては、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の、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の説明を参照してください。

機器のメンテナンスとシステム構成情報のメンテナンスの関係

機器のメンテナンスで機器が削除されると、削除された機器に対応するシステム構成情報も自動的に削除されます。その際、あて先グループと ID からもその機器が削除されます。なお、この場合、削除したコンピュータの情報はログファイルCLTDEL*n*.LOG（n ：1～4）ではなく、JDNSTRC*x*.log（x：1～9）に出力されます。

なお、削除された機器に対応するシステム構成情報が自動的に削除されるのは、次に示すような機器を削除するほかの操作の場合も同様です。

- 設定画面の［機器］－［機器メンテナンスの設定と検出結果確認］画面に表示される［削除候補の機器一覧］で、対象の機器を選択して［操作］メニューの［機器情報を削除する］を手動でクリックした場合。
- 設定画面の［機器の探索］－［管理対象機器］画面に表示される［管理対象の機器一覧］で、対象の機器を選択して［操作］メニューの［削除する］をクリックした場合。

機器削除と連動してシステム構成情報から削除される機器は、自サーバで管理するエージェント管理機器が対象となります。中継システムは自動削除されません。 機器一覧から中継システムを削除した場合、リモートインストールマネージャでシステム構成情報からも中継システムを削除してください。

メモ

システム構成情報から削除されたホストがあて先としてジョブ定義に残っていても、そのあて先は削除されません。

ヒント

エージェントを導入したコンピュータの MAIN.LOG ファイルに次のメッセージテキストが出力された場合の回復手順について説明します。

MAIN.LOG のメッセージテキスト

System configuration information could not be registered correctly because internal file information was invalid. Maintenance information=*[保守情報]*

このメッセージテキストは、システム構成に情報の追加、更新および削除が正常に通知できなかったことを示します。次の回復手順を実行して，システム構成情報を登録し直してください。

1. 次のファイルを削除します。
2. *JP1/IT Desktop Management 2 のインストール先ディレクトリ*¥CLIENT¥SYSENT¥SYSINFBK
3. エージェントを導入したコンピュータを再起動します。
4. システム構成の属性タブで、更新日時が更新されたことを確認します。

なお、システム構成へ情報の追加、更新および削除が正常に通知できなかった場合に、不要なホスト情報が残存するおそれがあります。その場合は、システム構成から該当のホスト情報を削除してください。

2.6.8 API を使用した機器情報の登録

外部システムから JP1/IT Desktop Management 2 に機器情報を登録できます。

外部システムは JP1/IT Desktop Management 2 が提供する API を使用して、機器を管理対象にします。これによって、JP1/IT Desktop Management 2 は外部システムから機器情報を収集できます。

API を使用して機器を管理することを API 管理と呼びます。また、API を使用して管理されている機器を API 管理機器と呼びます。

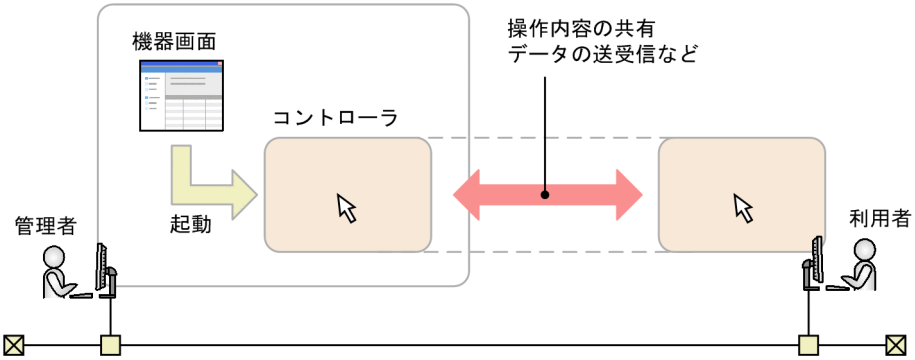
例えば、購入した機器の情報を調達システムから JP1/IT Desktop Management 2 に取り込むことで、エージェントレスで資産台帳を作成したり、購入した機器に紐づく情報を集約したりできます。

また、オペレーショナルテクノロジー機器（OT 機器）を管理する外部システムから JP1/IT Desktop Management 2 に OT 機器の情報を登録することで、エージェントを導入せずに OT 機器の資産台帳の作成や OT 機器の現存確認ができるようになります。

2.7　機器のリモートコントロール

近年の急速な IT の高度化に伴い、アプリケーションのセットアップやトラブル発生時の対処などに不慣れなユーザーが増えてきています。組織内で発生するコンピュータの問題に対しては、専門知識を持つシステム管理者などが対応する場合がほとんどです。しかし、職場が分散していると速やかな対応は難しくなります。

このような場合に、リモートコントロール機能を利用することで、管理者の手もとのコンピュータから問題の発生したコンピュータを遠隔操作して、操作内容を共有したり、データを送受信したりして問題に速やかに対応できます。



2.7.1　リモートコントロールの仕組み

JP1/IT Desktop Management 2 が提供するリモートコントロール機能の仕組みについて説明します。

リモートコントロール機能とは、遠隔地にあるコンピュータに接続し、呼び出したコンピュータの画面に対してキーボード操作やマウス操作ができる機能です。

画面を呼び出す管理者のコンピュータには、リモートコントロールするためのプログラム「コントローラ」が必要です。コントローラをインストールするには、JP1/IT Desktop Management 2 の操作画面からリモートコントロールを実行します。操作中のコンピュータにコントローラをインストールしていない場合でも、コンピュータにコントローラが自動的にダウンロードされてインストールが実行されます。

ヒント

コントローラがインストールされたコンピュータでは、コントローラを直接起動できるようになります。操作画面へログインすることなく、素早くリモートコントロールを開始できます。

リモートコントロールを開始するには、コントローラから対象のコンピュータに接続します。コントローラの接続方法には、次の 2 種類があります。

標準接続

製品が提供するリモートコントロール機能でコンピュータに接続する方法です。エージェントに含まれるプログラム「リモコンエージェント」とコントローラが接続して、リモートコントロールを実現します。通信速度が速く、リモートコントロールの全機能を利用できるため、通常はこちらを利用することをお勧めします。標準接続を利用するためには、対象のコンピュータにエージェントが導入されている必要があります。

RFB で接続

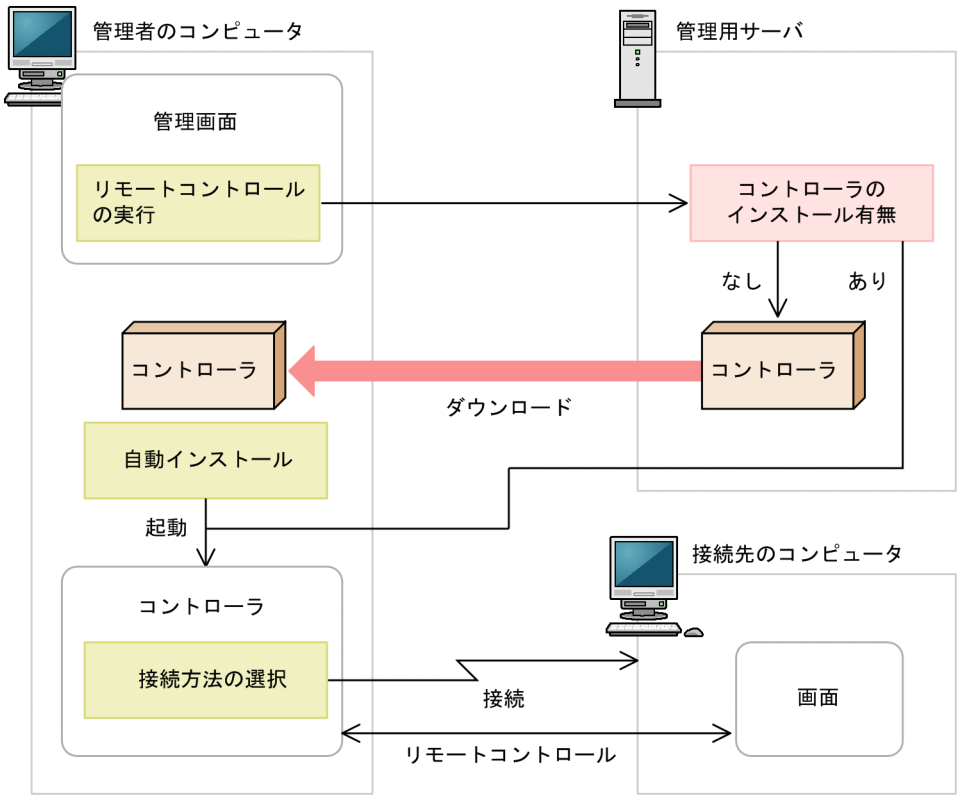
RFB プロトコルを利用してコンピュータに接続する方法です。AMT や VNC サーバ機能を利用できるソフトウェアなどによって、リモートコントロールを実現します。Windows にログオンできないコンピュータや、OS が Linux や Mac OS のエージェントレスのコンピュータに対して接続する場合は、こちらを利用してください。なお、RFB で接続する場合はリモートコントロールで使用できる機能に制限があります。

また、RFB で接続する場合は、コンピュータが RFB での接続をサポートしている必要があります。

接続方法は、コントローラから対象のコンピュータに接続するときに選択できます。接続方法を選択しなかった場合は標準接続になります。標準接続できなかった場合は、RFB で接続されます。

操作画面から接続先のコンピュータを選択してリモートコントロールを実行すると、コントローラが起動して自動的にコンピュータに接続されます。コントローラを直接起動した場合は、コントローラ上で接続先を指定します。

コンピュータへの接続が成功すると、コントローラに接続先のコンピュータの画面が表示されます。コンピュータに接続したあとは、リモートコントロールの機能を利用して、コンピュータの画面を操作できます。



関連リンク

- 4.3.3　リモートコントロールの前提条件
- 2.7.2　リモートコントロールの機能
- 2.7.3　リモートコントロールの接続方法の違いによる機能差異

2.7.2　リモートコントロールの機能

JP1/IT Desktop Management 2 が提供するリモートコントロール機能では、次に示す機能を利用できます。

- コンピュータの操作

  目の前のコンピュータを操作するように、遠隔地にあるコンピュータを操作できます。利用者のコンピュータで予期しないトラブルが発生した場合でも、コンピュータの設置場所まで駆けつけることなく、原因の調査やコンピュータの再起動などができます。コンピュータの操作方法については、「2.7.14 リモートコントロール中のコンピュータの画面の操作」を参照してください。

- ファイルの転送

  リモートコントロール中のコンピュータと、ファイルを送受信できます。エクスプローラと同様の操作で、遠隔地にあるコンピュータのハードディスクの内容を参照できるので、必要なファイルを探しながらファイルを送受信できます。これによって、ファイル共有の設定や特別なソフトウェアを使うことなく、ファイルをやり取りできます。ファイルの転送方法については、「2.7.15　リモートコントロール中のファイル転送」を参照してください。

- 接続先の管理

  よく接続するコンピュータを、JP1/IT Desktop Management 2 の操作画面とは別に登録して管理できます。また、ネットワーク上から接続できるコンピュータを検索することもできます。接続先の管理方法については、「2.7.17　リモートコントロールの接続先の管理」を参照してください。

- コンピュータからコントローラへの接続要求

  ネットワークの制約によってコントローラからコンピュータに接続できない環境の場合に、利用者のコンピュータからコントローラに接続要求をすることで、リモートコントロールを開始できます。コンピュータからコントローラへの接続要求の方法については、「2.7.16　接続先のコンピュータからコントローラへの接続要求」を参照してください。

- リモートコントロールの録画・再生

  リモートコントロール中の画面を録画できます。録画したデータは動画ファイルに変換できるので、トレーニングやトラブルシュート方法の説明に利用できます。リモートコントロールの録画・再生方法については、「2.7.18　リモートコントロールの録画・再生」を参照してください。

- チャットの利用

  複数のコンピュータと同時にチャットができます。電話が使えない環境で対話したり、複数人に同時に指示を出したりできます。チャットの利用方法については、「2.7.19　チャットの利用」を参照してください。

関連リンク

- 4.3.3　リモートコントロールの前提条件

2.7.3　リモートコントロールの接続方法の違いによる機能差異

リモートコントロールの機能は、接続方法やコンピュータの環境によって機能差異があります。接続方法の違いによる機能差異を次の表に示します。

機能		説明	機能有無	
			標準	RFB
コントローラ機能	コンピュータへの接続	コンピュータに接続できる機能	○	○
	認証情報の利用	接続時に認証情報を利用できる機能	○	○
	接続モード	接続時にコントローラとコンピュータの操作を制限できる機能	○	△
	接続状態の表示	接続中の状態を表示できる機能	○	○
	接続中の画面表示	接続先のコンピュータの画面をコントローラに表示できる機能	○	○
	キーボード、マウスの操作	接続先のコンピュータに対して、キーボードとマウスの操作を実行できる機能	○	○
	クリップボードの利用	接続先のコンピュータとクリップボードを同期できる機能	○	△
	リモートコントロールの切断	コンピュータとの接続を切断し、リモートコントロールを終了できる機能	○	○
	電源制御	接続先のコンピュータの電源を制御できる機能	○	△
	リモート CD-ROM	コントローラの CD/DVD ドライブ（ドライブ種別が CD-ROM のドライブ）を、接続先のコンピュータでも使えるようにする機能	△	△
	リモートコントロールの録画、再生、ファイル形式変換	• リモートコントロール中の画面を録画し、動画ファイルを再生できる機能 • 動画ファイルを AVI ファイルに変換できる機能	○	○
	コントローラの環境設定	コントローラの各種設定をカスタマイズできる機能	○	○

機能		説明	機能有無	
			標準	RFB
接続先の管理	接続リストの管理	接続先のコンピュータを JP1/IT Desktop Management 2 の操作画面とは別に管理できる機能	○	○
	コンピュータの検索	ネットワーク上の接続できるコンピュータを検索できる機能	○	○
	コンピュータ側からの接続要求	コンピュータ側からコントローラに対して接続要求をして、リモートコントロールを開始できる機能	○	×
リモコンエージェント機能	接続の確認	コントローラからの接続を受け付け、接続するかどうかを選択できる機能	○	×
	接続モードの確認	接続モードの状況を確認できる機能	○	×
	接続状態の確認	コンピュータ側で、コントローラとの接続状態を確認できる機能	○	×
	接続の切断	コントローラとの接続を切断できる機能	○	×
	画面の非表示	リモートコントロール中に、コンピュータ側の画面を非表示またはロックできる機能	○	×
	リモコンエージェントの環境設定	リモコンエージェントの各種設定をカスタマイズできる機能	○	×
ファイル転送機能	ファイル一覧の表示	コントローラと接続先のコンピュータのハードディスクの内容を表示できる機能	○	×
	ファイルプロパティの編集	コントローラと接続先のコンピュータのファイルのプロパティを編集できる機能	○	×
	ファイルの編集	コントローラと接続先のコンピュータのファイルを編集できる機能	○	×
	ファイルの転送	コントローラと接続先のコンピュータ間でファイルを送受信できる機能	○	×
	マルチ転送	複数のコンピュータに対して、ファイルを一括で転送できる機能	○	×
	転送情報の管理	接続先のコンピュータのファイルを開いたときに、ファイルを自動的にダウンロードしキャッシュする機能	○	×
チャット機能	チャットサーバ機能	ほかのコンピュータからのチャット接続を受け付けて、チャットを開始できる機能	○	×

機能		説明	機能有無	
			標準	RFB
チャット機能	チャットクライアント機能	チャットサーバに接続してチャットを開始できる機能	○	×
	チャットのログの記録	チャット中の対話のログを保存できる機能	○	×
	ログの印刷	チャットのログを印刷できる機能	○	×
	リモートコントロールの開始	チャット中のコンピュータに接続してリモートコントロールを開始できる機能	○	×
操作画面との連携機能	コントローラのインストール	コントローラが未インストールのコンピュータに対して、自動的にコントローラをダウンロードしてインストールできる機能	○	○
	コントローラの自動更新	コントローラがインストールされているコンピュータに対して、自動的にコントローラを更新できる機能	○	○
	コントローラの起動と接続	操作画面で選択したコンピュータに対して、コントローラを起動して接続できる機能	○	○
他プログラム連携		コマンドによってほかのプログラムからコントローラを呼び出し、コンピュータに接続できる機能	○	○
VNC サーバとの接続		VNC サーバ機能を持つソフトウェアを利用してリモートコントロールできる機能	×	○
BIOS の操作		コンピュータの BIOS を表示させて設定変更できる機能	×	○

(凡例) ○：機能あり　△：一部機能あり、または機能はあるがコンピュータの環境によって動作しないことがある　×：機能なし

2.7.4　多言語環境でリモートコントロール機能を利用する場合の注意事項

コントローラ側のコンピュータと接続先のコンピュータで、使用するキーボードの種類が異なる場合、キーの入力が正しくできないことがあります。

2.7.5　ユーザー環境に依存するコントローラ上のファイルについての注意事項

コントローラでは、次のファイルがユーザーの環境設定によって無制限に増加します。これらのファイルは、何らかのタイミングで削除するなどして、対処してください。

ファイル転送時の一時ファイル

［ファイル転送］ウィンドウから表示する［環境の設定］ダイアログで、［ファイル］タブの［コントローラ上のファイルを削除する］のチェックを外していた場合、コントローラ側のファイルは削除されません。この一時ファイルは、［環境の設定］ダイアログの［ファイル］タブで設定したファイル転送時の格納先フォルダに残ります。

録画ファイル

コンピュータの画面情報を録画した録画ファイルは、自動では削除されません。録画ファイルの作成場所は、ユーザーの任意です。また、ファイルサイズもユーザーの操作によって異なります。

2.7.6　コントローラの自動更新

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。

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

2.7.7　リモートコントロールの接続モードの設定

コンピュータをリモートコントロールする場合、接続先のコンピュータに対する操作の権限を設定できます。この権限を接続モードと呼びます。接続モードを設定することで、管理者がリモートコントロール中に利用者に操作されることを防いだり、コントローラ側から画面の参照だけできるようにしたりできます。

接続モードには、「制御モード」、「共有モード」、「監視モード」の 3 種類があります。それぞれのモードについて説明します。

制御モード

コントローラ側だけが操作できるモードです。接続先のコンピュータでは、キーボードやマウスの操作ができません。コントローラ側で操作している最中に利用者に操作されたくない場合は、このモードで接続してください。制御モードを設定して、コンピュータに RFB で接続した場合、自動的に共有モードになります。

重要

RFB で接続している場合、制御モードは利用できません。

共有モード

コントローラ側と接続先のコンピュータ側の両方からコンピュータを操作できるモードです。管理者と利用者の両方が操作するおそれがある場合は、このモードで接続してください。

監視モード

接続先のコンピュータに対して、画面の参照だけができるモードです。コントローラ側のコンピュータでは、キーボードやマウスでの操作ができません。接続先のコンピュータでの操作を参照するだけのときは、このモードで接続してください。

接続モードの決定方式

接続モードは、コントローラの設定とエージェント設定の組み合わせで決定されます。接続モードに設定したモードとリモコンエージェントのステータスウィンドウに表示されるモード名の組み合わせを次に示します。

エージェント設定	コントローラの設定		
	制御モード	共有モード	監視モード
制御モード	パターン 1 コントローラ：監視 エージェント：制御	パターン 2 コントローラ：監視 エージェント：制御	パターン 2 コントローラ：監視 エージェント：制御
共有モード	パターン 3 コントローラ：制御 エージェント：監視	パターン 1 コントローラ：共有 エージェント：共有	パターン 2 コントローラ：監視 エージェント：共有
監視モード	パターン 3 コントローラ：制御 エージェント：監視	パターン 3 コントローラ：共有 エージェント：監視	パターン 1 コントローラ：監視 エージェント：監視

表中のパターン 1～パターン 3 について説明します。

パターン 1 およびパターン 2 の場合

両者が同じリモートコントロールモードを設定した場合（パターン 1)、およびエージェントの方が権限を高く設定した場合（パターン 2）では、エージェントの設定が優先されます。このため、エージェントの設定が「制御」モードの場合、コントローラは自身の設定に関係なく「監視」モードになります。エージェントの設定が「共有」モードまたは「監視」モードの場合、コントローラは自身で設定しているモードになります。

パターン 3 の場合

コントローラの方が権限を高く設定した場合（パターン 3）では、コントローラの設定が優先されます。このため、コントローラの設定が「制御」モードの場合、エージェントは自身の設定に関係なく

「監視」モードになります。コントローラの設定が「共有」モードの場合、エージェントは自身で設定しているモードになります。

(1) 利用者のコンピュータからリモートコントロールの接続モードを変更する手順

接続先のコンピュータが制御モードの場合、利用者がコンピュータを操作しようと思っても、そのままでは操作できません。

利用者がコンピュータを操作する必要がある場合、利用者のコンピュータ側で［Ctrl］＋［Alt］＋［Delete］キーを押すことで共有モードに変更できます。

この操作でコンピュータの接続モードが制御から共有に変わると、この情報がコントローラに通知されます。コントローラでは、コントローラの接続モードを制御から共有に変更するかどうか問い合わせるメッセージが表示されます。共有に変更することを許可しなかった場合、コンピュータは再び制御モードに戻り、利用者はコンピュータを操作できなくなります。

ヒント

利用者のコンピュータ側で［Ctrl］＋［Alt］＋［Delete］キーを押した時点で、接続モードは共有に変更されます。このため、コントローラにメッセージが表示されたときは、すでに接続モードは変更されています。

(2) リモートコントロール（複数接続時）の接続モード

複数のコントローラが 1 台のコンピュータに接続している場合、制御モードで操作できるコントローラは 1 台だけです。このとき、そのほかのコントローラは、監視モードになります。

そのあと、制御モードのコントローラをほかのモードへ変更したり、接続を解除したりした場合、ほかのコントローラに、制御モードが解放されたことを通知するメッセージが表示されます。

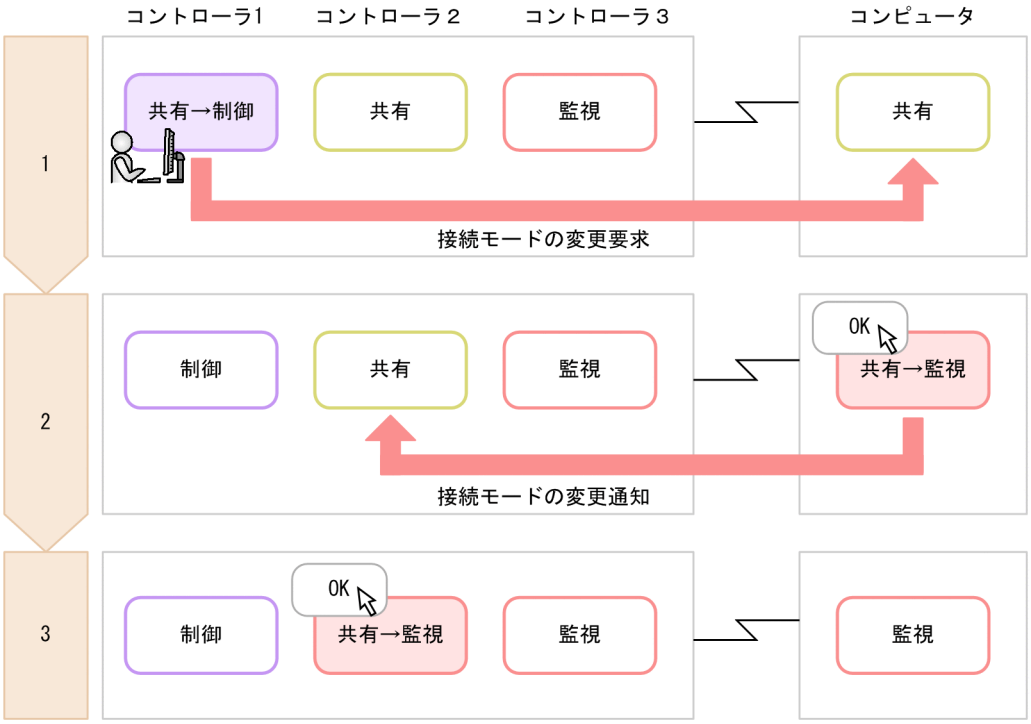
以降では、複数接続時の接続モードの変化について例を示します。

例 1.初期状態

次のような接続モードで、1 台のコンピュータに 3 台のコントローラが接続していると仮定します。

例 2.コントローラ 1 を制御モードに変更する

初期状態から、コントローラ 1 を制御モードに変更した場合、そのほかのコンピュータのモードは次のように変化します。



1. コントローラ 1 を制御モードに変更します。

   接続先のコンピュータ上に、接続モードの変更を要求するメッセージが表示されます。

2. 接続先のコンピュータで［OK］ボタンをクリックします。

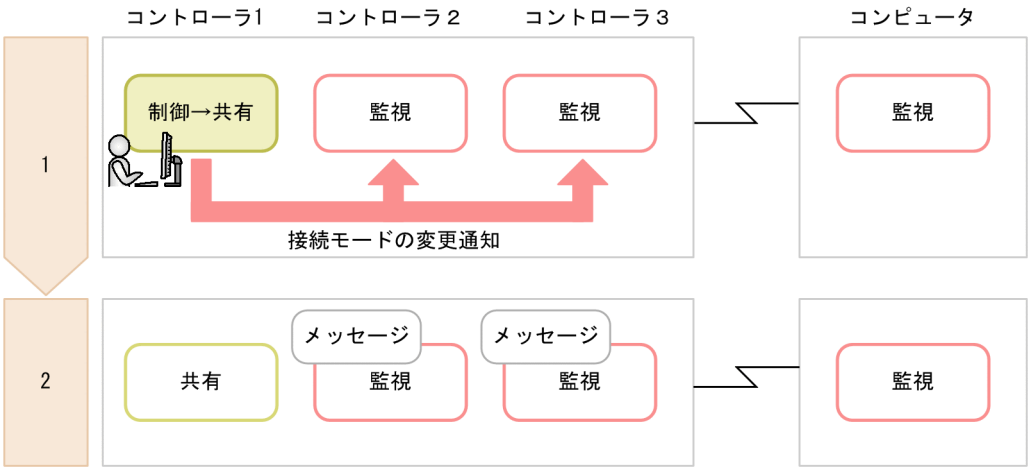
   接続先のコンピュータが監視モードになります。また、コントローラ 2 上に、ほかのコントローラが制御モードを取得したことを通知するメッセージが表示されます。

3. コントローラ 2 で［OK］ボタンをクリックします。

   コントローラ 2 が監視モードになります。

例 3.コントローラ 1 を制御モード以外のモードに変更する

例 2 の状態で、コントローラ 1 を制御モード以外のモードに変更した場合、そのほかのコンピュータのモードは変化しません。コントローラ 1 がコンピュータとの接続を切断した場合も、これと同じ結果となります。

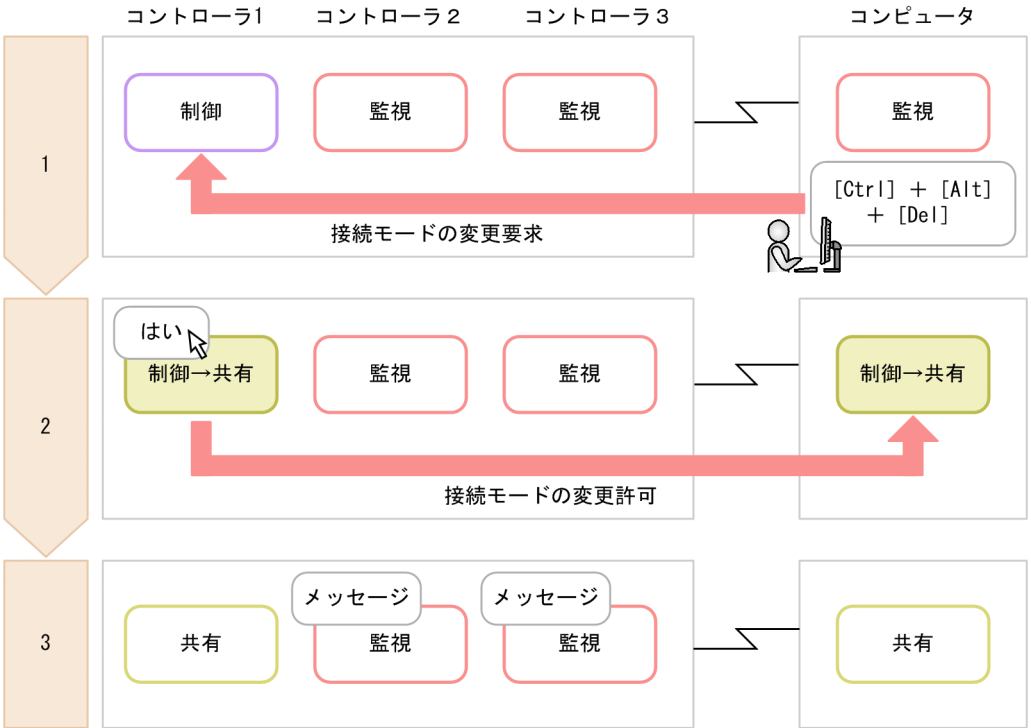


1. コントローラ 1 を共有モードに変更します。

2. コントローラ 2 および 3 上に、コントローラ 1 で制御モードが解除されたことを通知するメッセージが表示されます。ただし、コントローラ 2 の接続モードは監視のままです。

例 4.コントローラが制御モードを取得したあと、接続先のコンピュータで［Ctrl］＋［Alt］＋［Delete］キーを押す

例 2 の状態で、接続先のコンピュータの利用者が［Ctrl］＋［Alt］＋［Delete］キーを押した場合、そのほかのコンピュータのモードは次のように変化します。



1. 接続先のコンピュータの利用者が［Ctrl］＋［Alt］＋［Delete］キーを押します。
   コントローラ 1 上に、接続モードの変更を要求するメッセージが表示されます。

2. コントローラ 1 で［はい］ボタンをクリックします。

コントローラ 1 および接続先のコンピュータが共有モードになります。なお、ここで［いいえ］ボタンをクリックするとモードは変わりません。

3. コントローラ 2 および 3 上に、ほかのコントローラで制御モードが解放されたことを通知するメッセージが表示されます。ただし、コントローラ 2 の接続モードは監視のままです。

2.7.8 リモートコントロールの接続状態の表示

コンピュータに接続すると、コントローラのステータスバーに情報が表示されます。表示される情報を次の表に示します。

項目	表示内容	デフォルト表示
送信データ量	送信データのバイト数が表示されます。右クリックで表示されるメニューで、表示形式の変更や表示の初期化ができます。	×
受信データ量	受信データのバイト数が表示されます。右クリックで表示されるメニューで、表示形式の変更や表示の初期化ができます。	×
経過時間	コンピュータと接続が開始されてからの経過時間が表示されます。 右クリックで表示されるメニューで、時間の表示を初期化できます。	×
リモート CD-ROM の状態	リモート CD-ROM（DVD-ROM）の利用状態が表示されます。 右クリックで表示されるメニューで、リモート CD-ROM（DVD-ROM）の利用可否を切り替えられます。	○ ※
録画の状態	リモートコントロールの内容の録画状態が、アイコンで表示されます。 右クリックで表示されるメニューで、録画の開始、停止、および一時停止を実行できます。	×
送受信の状態	データの送受信量と暗号化の状態が表示されます。 右クリックで表示されるメニューで、データの送受信量の表示を初期化できます。	△
プロトコル	接続に使用しているプロトコル（HRC または RFB）が表示されます。	△
接続モード	コントローラの接続モードが表示されます。 右クリックで表示されるメニューで、接続モードを変更できます。	○

（凡例）○：常に表示される　△：接続中だけ表示される　×：表示されない

注※　RFB で接続している場合に常に表示されます。

次の情報は、［リモートコントロール］ウィンドウのメニューの［表示］－［ステータスバー］から、表示させるかどうかを変更できます。

- 経過時間
- 送受信データ量

2.7.9　NAT 環境、DHCP 環境でのリモートコントロール

NAT 環境の場合

NAT 機能とは、外部ネットワークから内部ネットワークのアドレスが見えないようにしたり、内部ネットワークのアドレスが外部に漏れないようにしたりするためにネットワーク上のアドレスを変換できる機能です。アドレス変換の方式の種類には、「固定アドレス割り当て方式（スタティックモード）」および「動的アドレス割り当て方式（ダイナミックモード）」があります。

NAT 環境でリモートコントロール機能を利用する場合、次のように対応してください。

固定アドレス割り当て方式（スタティックモード）環境の場合

　リモートコントロール機能を利用する上での制限はありません。

動的アドレス割り当て方式（ダイナミックモード）環境の場合

　コントローラからコンピュータに接続できません。この場合、コンピュータからコントローラに接続要求を出すことで、リモートコントロールを開始できます。

DHCP 環境の場合

DHCP 機能とは、ネットワークに接続するコンピュータに IP アドレスを自動的に割り当てる機能です。DHCP 環境の場合は、コンピュータがネットワークに接続するたびに IP アドレスが変更になるため、コントローラからコンピュータに接続できません。この場合、コンピュータからコントローラに接続要求を出すことで、リモートコントロールを開始できます。

なお、静的 DHCP の場合は IP アドレスが変更されないため、コントローラからコンピュータに接続できます。

関連リンク

- 2.7.16　接続先のコンピュータからコントローラへの接続要求

2.7.10　Windows 認証を利用してリモートコントロールする場合に必要なユーザー権限

リモコンエージェントの認証情報の設定で、Windows の認証を使用する場合は、ネットワーク経由でコンピュータへアクセスできるユーザー権限が必要です。ユーザー権限の設定には、Windows の機能を使用します。ここでは、OS の使用状況ごとに必要なユーザー権限について説明します。

OS を使用している状況	必要な権限
ローカルコンピュータ	Administrators グループの権限、または適切な権限。ドメインに参加している場合は、Domain Admins グループの権限。
ドメインに参加しているワークステーション、またはサーバ	Active Directory の Domain Admins グループ、Enterprise Admins グループ、または適切な権限。

OS を使用している状況	必要な権限
Windows Server 2003 管理ツール パックがインストールされたドメインコントローラまたはワークステーション	Active Directory の Domain Admins グループ、Enterprise Admins グループ、または適切な権限。
ドメインコントローラ	

注　セキュリティを考慮する場合は、システム管理者ではないユーザーのアカウントでログオンしてから、システム管理者として実行したあとにセキュリティを設定することを検討してください。

2.7.11　Windows 認証を利用してリモートコントロールする場合に必要なユーザー権限の設定手順

ユーザー権限を設定する手順を、OS の使用状況ごとに説明します。

ヒント

本手順はすべて Windows OS の設定を変更する手順です。Windows OS によっては操作手順や手順内の名称が異なる場合があります。

ローカルコンピュータでユーザー権限を設定するには：

1. [コントロールパネル] で [管理ツール] を選択します。
2. [ローカル セキュリティ ポリシー] をダブルクリックします。
3. コンソールツリーから、[セキュリティの設定] を選択します。
4. [ローカル ポリシー] − [ユーザー権利の割り当て] を選択します。
5. 詳細ウィンドウ領域で、[ネットワーク経由でコンピュータへアクセス]、または [ネットワーク経由でコンピュータへアクセスを拒否する] をダブルクリックします。

表示されるダイアログでユーザー権限を設定できます。

ドメインに参加しているワークステーション、またはサーバでユーザー権限を設定するには：

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択します。
2. 「mmc」と入力して [OK] ボタンをクリックします。
3. コンソールの [ファイル] メニューから、[スナップインの追加と削除] を選択します。
4. [利用できるスナップイン] から [グループ ポリシー オブジェクト エディタ] を選択して、[追加] ボタンをクリックします。
5. [グループ ポリシー オブジェクトの選択] ダイアログで、[参照] ボタンをクリックします。

6. 変更するグループポリシーオブジェクトを設定します。
   設定後は、[完了] または [OK] ボタンをクリックし、[スナップインの追加と削除] ダイアログを閉じます。

7. コンソールのツリーから、[グループ ポリシー オブジェクト] − [*コンピュータ名* ポリシー] で、[コンピュータの構成] − [Windows の設定] − [セキュリティの設定] を選択します。

8. [ローカル ポリシー] − [ユーザー権利の割り当て] を選択します。

9. 詳細ウィンドウ領域で、[ネットワーク経由でコンピュータへアクセス]、または [ネットワーク経由でコンピュータへアクセスを拒否する] をダブルクリックします。

表示されるダイアログでユーザー権限を設定できます。セキュリティ設定が未定義の場合は、[このポリシーの設定を定義する] をチェックします。

Windows Server 2003 管理ツール パックがインストールされたドメインコントローラまたはワークステーションでユーザー権限を設定するには：

1. Windows の [スタート] メニューから [コントロールパネル] − [管理ツール] を選択します。

2. [Active Directory ユーザーとコンピュータ] をダブルクリックします。

3. コンソールツリーで、セキュリティの設定を編集するグループポリシーオブジェクトを右クリックします。

4. [プロパティ] − [グループ ポリシー] タブを選択します。

5. 既存のグループポリシーオブジェクトを編集するには、[編集] を選択します。
   新しいグループポリシーオブジェクトを作成するには、[新規] − [編集] を選択します。

6. [グループ ポリシー オブジェクト] − [*コンピュータ名* ポリシー] で、[コンピュータの構成] − [Windows の設定] − [セキュリティの設定] を選択します。

7. [ローカル ポリシー] − [ユーザー権利の割り当て] を選択します。

8. 詳細ウィンドウ領域で、[ネットワーク経由でコンピュータへアクセス]、または [ネットワーク経由でコンピュータへアクセスを拒否する] をダブルクリックします。

表示されるダイアログでユーザー権限を設定できます。セキュリティ設定が定義されていない場合は、[このポリシーの設定を定義する] をチェックします。

ドメインコントローラでユーザー権限を設定するには：

1. Windows の [スタート] メニューから [コントロールパネル] − [管理ツール] を選択します。

2. [ドメイン コントローラ セキュリティ ポリシー] をダブルクリックします。

3. コンソールのツリーから、[グループ ポリシー オブジェクト] − [*コンピュータ名* ポリシー] で、[コンピュータの構成] − [Windows の設定] − [セキュリティの設定] を選択します。

4. [ローカル ポリシー] − [ユーザー権利の割り当て] を選択します。

5. 詳細ウィンドウ領域で、[ネットワーク経由でコンピュータへアクセス]、または [ネットワーク経由でコンピュータへアクセスを拒否する] をダブルクリックします。

表示されるダイアログでユーザー権限を設定できます。セキュリティ設定が定義されていない場合は、[このポリシーの設定を定義する] をチェックします。

2.7.12 リモートコントロールの認証情報の設定

エージェント導入済みのコンピュータに対して、コントローラからの接続をユーザー単位で制限するための認証情報を設定できます。認証情報は、特定のユーザーに対してリモートコントロールを許可したい場合に設定します。何も設定しない場合は、すべてのユーザーからの接続を許可します。

認証情報の設定には、次の 2 種類のユーザー認証を使用できます。

標準の認証
: 独自のユーザー認証です。認証情報に設定されたユーザー名およびパスワードを持つユーザーだけがコンピュータに接続できます。

Windows の認証
: Windows の認証機能と連携したユーザー認証です。認証情報に設定された Windows のユーザーおよびグループだけがコンピュータに接続できます。このユーザー認証では、パスワードの有効期限や監査など、詳細なセキュリティポリシーを適用できます。ドメインユーザーで認証する場合は、「ユーザー名@ドメイン名」または「ドメイン名¥ユーザー名」の形式で設定を追加してください。

認証情報は、複数のユーザーを登録して管理できます。登録した各ユーザーに対して、共有モードおよび制御モードの設定、シャットダウンなどのリモートコントロール操作の使用可否を設定できます。また、Windows の認証機能と連携したユーザー認証を使用することで、リモートコントロールのセキュリティをさらに強化できます。

なお、 認証情報は、エージェント設定で設定できます。

2.7.13 コントローラからコンピュータへの接続方法

コントローラを直接起動した場合やいったん接続を切断した場合に、コンピュータに接続するにはコントローラで接続先を指定する必要があります。接続先の指定方法には、次の方法があります。

- ホスト名または IP アドレスを直接指定して接続する
- コンピュータを選択して接続する

- 接続履歴から接続する
- コンピュータを検索して接続する

どの方法でも、コンピュータ側で認証情報が設定されている場合は、接続時に認証情報を入力するダイアログが表示されます。この場合、エージェント設定の［リモートコントロールの設定］－［ユーザー認証］に設定された認証情報、または接続先の VNC サーバに設定された認証情報を入力してください。デフォルトエージェント設定では、ユーザー ID が「system」、パスワードが「manager」の認証情報が設定されています。

また、コンピュータ側で接続要求が表示される設定の場合は、要求が拒否されると、コントローラに接続拒否のメッセージが表示されます。

ヒント

1 台のコンピュータに、同時に接続できるコントローラの数は 255 台までです。

ヒント

コンピュータへの接続が拒否されたり、タイムアウトが発生したりした場合は、RFB で再接続を試みます。なお、接続時に、接続先のコンピュータの電源を ON にするよう設定されている場合は、接続先のコンピュータの電源 OFF によって RFB での再接続に失敗（タイムアウト）したときに、Wake on LAN および AMT によって接続先のコンピュータが起動され、再度接続を試みます。

関連リンク

- 2.7.17　リモートコントロールの接続先の管理

2.7.14　リモートコントロール中のコンピュータの画面の操作

リモートコントロール機能で遠隔地のコンピュータを操作する場合、コントローラは対象のコンピュータに対して次のような操作ができます。

キーボードやマウスの操作

呼び出した画面に対して、文字を入力したり、アイコンをドラッグしたりするなど、手もとのコンピュータを操作するのと同じようにキーボード操作、マウス操作ができます。［Ctrl］＋［C］などのショートカットキーは、特殊キーとして登録することで実行できます。

CD-ROM や DVD-ROM の利用

コントローラを使用しているコンピュータの CD/DVD ドライブ（ドライブ種別が CD-ROM のドライブ）を、接続先のコンピュータのドライブとして利用できます。データを転送することなく、接続先のコンピュータにソフトウェアをインストールできます。

シャットダウンと再起動の実行

コントローラから、コンピュータのシャットダウンや再起動を指示できます。再起動時にコンピュータへの再接続を設定しておくと、再起動後に自動的に再接続し、リモートコントロールを継続できます。

クリップボードの転送

コントローラとコンピュータ間でクリップボードのデータを送受信できます。この機能を使用すると、コントローラ側のコンピュータと対象のコンピュータとの間で、テキストやビットマップをコピー&ペーストできます。

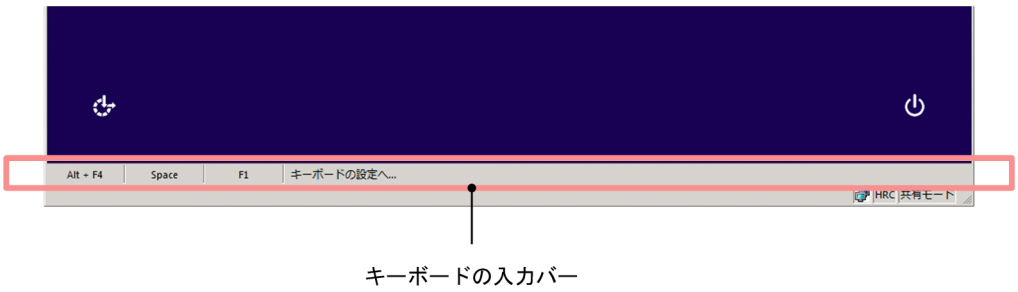
関連リンク

- (1)　リモートコントロール中の特殊キーの登録と入力
- (3)　リモートコントロール中のクリップボードのデータの転送

(1)　リモートコントロール中の特殊キーの登録と入力

機能キー、ショートカットキーなどの特殊キーは、キーボードから入力するとコントローラ自身で実行されてしまいます。このため、コンピュータに対して特殊キーを入力する場合は、コントローラに特殊キーを登録して実行する必要があります。コントローラに特殊キーを登録する方法については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の、コントローラに特殊キーを登録する手順についての説明を参照してください。

登録された特殊キーは、[リモートコントロール] ウィンドウの「キーボードの入力バー」に表示されます。キーボードの入力バーに表示されたボタンをクリックするだけで、特殊キーを対象のコンピュータに入力できます。



ヒント

コントローラ側のコンピュータが日本語キーボードで、接続先のコンピュータが英語キーボードのように入力環境が異なる場合、キーボード操作で特定の文字を入力できないことがあります。このような場合、特殊キーやクリップボードのデータの転送を利用することで、入力環境の違いを意識しないで文字を入力できます。

関連リンク

- (2)　デフォルトでコントローラに提供されている特殊キー
- (3)　リモートコントロール中のクリップボードのデータの転送

(2) デフォルトでコントローラに提供されている特殊キー

コントローラがデフォルトで提供している特殊キーの一覧を次の表に示します。これらは、特殊キーの登録時に［特殊キータイプ］で「デフォルト」を設定すると選択できます。

項番	特殊キー
1	[F1]
2	[Shift] ＋ [F1]
3	[Shift] ＋ [F10]
4	[SpaceBar]
5	[Esc]
6	[Alt]
7	[Alt] ＋ [Tab]
8	[Alt] ＋ [Esc]
9	[Alt] ＋ [SpaceBar]
10	[Alt] ＋ [-]
11	[Alt] ＋ [Enter]
12	[Alt] ＋ [F4]
13	[Alt] ＋ [F6]
14	[Alt] ＋ [PrintScreen]
15	[PrintScreen]
16	[Ctrl] ＋ [C]
17	[Ctrl] ＋ [O]
18	[Ctrl] ＋ [P]
19	[Ctrl] ＋ [S]
20	[Ctrl] ＋ [V]
21	[Ctrl] ＋ [X]
22	[Ctrl] ＋ [Z]
23	[Ctrl] ＋ [Esc]
24	[Ctrl] ＋ [F6]
25	[Ctrl] ＋ [Tab]
26	[漢字]

(3) リモートコントロール中のクリップボードのデータの転送

コントローラまたはコンピュータでクリップボードの内容が更新されたときに、クリップボードのデータを自動的に接続先のコントローラまたはコンピュータに転送できます。コントローラとコンピュータのクリップボードの内容が常に同一となるため、例えば、次のような場合にコントローラとコンピュータの違いを意識しないで作業ができます。

- コントローラ側のコンピュータにメモしてある URL を、接続先のコンピュータの Web ブラウザにペーストして Web サイトを表示する
- 接続先のコンピュータで採取したハードコピーを、コントローラ側のコンピュータで作成中の資料にペーストする

なお、転送できるデータの種類は接続方法によって、次のように異なります。

標準接続の場合

次に示す種類のデータ、およびこれらを組み合わせたデータを送受信できます。

- テキスト
- ビットマップ
- メタファイル
- リッチテキスト
- カラーパレット

RFB の接続の場合

ASCII コードのテキストだけ送受信できます。ほかの文字コードのテキストを送受信できるかどうかは、接続先の環境に依存します。

クリップボードのデータの送受信は、コントローラがアクティブになったタイミングで実行されます。ただし、RFB で接続している場合は、コンピュータ側でクリップボードの内容が更新されるたびにデータが受信されます。

ヒント

標準接続の場合、容量の大きなデータの転送によって動作が遅くなることを防止したいときは、［環境の設定］ダイアログの［高速化］タブで、テキストデータだけを転送するようにも設定できます。

ヒント

データの転送中は、［リモートコントロール］ウィンドウ下部のステータスバーにメッセージおよびプログレスバーが表示されます。予想外に大きなファイルの転送が始まって、なかなか処理が終わらないようなときは、プログレスバー上を右クリックすると表示される［キャンセル］

メニューで転送を中断できます。中断した場合、転送中のデータは破棄され、クリップボードの内容は元に戻ります。

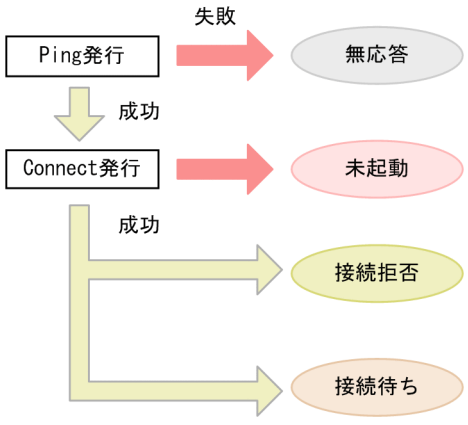
(4)　リモートコントロール接続できるコンピュータの検索範囲の指定方法

ネットワーク上から、リモートコントロールできるコンピュータを検索するための検索範囲は、次の表に示す方法で指定できます。

項番	方法	指定例	指定例の場合の対象範囲
1	単独の IP アドレスを指定する。	172.17.11.10	172.17.11.10
2	IP アドレスを 3 バイト目まで記述し、最終 1 バイトを、ハイフン（-）で区切って 2 つ指定する。連続する複数の IP アドレスの範囲内で検索する場合に使用する。	172.17.11.10-20	172.17.11.10～172.17.11.20
3	IP アドレスを 3 バイト目まで記述し、最終 1 バイトを、コンマ（,）で区切って複数個指定する。連続しない複数の IP アドレスを対象として検索する場合に使用する。	172.17.11.10,11,100,200	172.17.11.10、172.17.11.11、172.17.11.100、172.17.11.200
4	項番 2、3 を組み合わせて指定する。	172.17.11.10,50-100,200	172.17.11.10、172.17.11.50～172.17.11.100、172.17.11.200
5	IP アドレスの 3 バイト目までを指定する。同一サブネット内のすべての IP アドレスを検索対象とする場合に使用する。	172.17.11	172.17.11.0～172.17.11.255

(5)　リモートコントロール接続できるコンピュータの状態

［接続できるコンピュータの検索］ダイアログに表示されるコンピュータの状態は、「無応答」、「未起動」、「接続拒否」、「接続待ち」の 4 種類です。状態の遷移を次の図に示します。



無応答

該当するコンピュータが存在しない、または起動していない状態です。

未起動

該当するコンピュータがリモートコントロールの対象外、またはリモコンエージェントが起動していない状態です。

接続拒否

該当するコンピュータ（エージェント導入済み）でリモコンエージェントは起動しているが、 接続できない状態です。原因として、許可コントローラとして登録されていない、リモートコントロールで使用するポートをほかのアプリケーションで使用しているなどが考えられます。[接続できるコンピュータの検索］ダイアログの［詳細］タブでメッセージを確認してください。

接続待ち

該当するコンピュータが接続できる状態です。

(6) リモートコントロール中（フルスクリーン表示時）のメニューバーからの操作

フルスクリーン表示で表示されるメニューバーから、リモートコントロールの設定、データの送受信状況の確認、画面表示設定などが実行できます。

それぞれのアイコンおよび機能の説明について、次の表に示します。

アイコン画像	アイコン名	説明
	ピンボタン	アイコンをクリックすると、メニューバーを常に表示させるかどうかを設定できます。有効にすると、マウスカーソルが画面上部になくても、常に画面上部にメニューバーが表示されます。デフォルトは、無効です。
	Ctrl+Alt+Deleteボタン	アイコンをクリックすると、接続先の機器に、[Ctrl］＋［Alt］＋［Delete］キーと同様の操作を実行できます。
	最新表示ボタン	アイコンをクリックすると、リモートコントロール中の画面の表示内容を最新の状態に更新できます。画面が乱れて表示画面をリフレッシュしたい場合などに実行します。
	送受信アイコン	リモート接続先との送受信状況や、暗号化の状態を確認できます。かぎ付きのアイコンが表示されている場合は、暗号化されている状態です。 また、右クリックすると表示されるメニューから、送受信データの値を初期化できます。
	最小化ボタン	アイコンをクリックすると、リモートコントロール中の画面を最小化できます。画面には、接続元コンピュータのデスクトップ画面が表示されます。
	元に戻すボタン	アイコンをクリックすると、フルスクリーン表示を解除して、ウィンドウ表示に戻せます。
	閉じるボタン	アイコンをクリックすると、リモートコントロールを終了して、ウィンドウが閉じます。

(7) リモートコントロール時の注意事項

リモートコントロール機能を利用する際の注意事項を次に示します。また、接続先のコンピュータの OS ごとの注意事項についても説明します。

- コンピュータで MS-DOS プロンプトをフルスクリーンで表示すると、コントローラではコンピュータの画面を参照できません。リモートコントロール機能を使用する場合、コンピュータでは MS-DOS プロンプトをフルスクリーン表示ではなくウィンドウで表示させてください。
- コンピュータで Direct X（Direct Draw）、OpenGL を使用して作成された画像は、コントローラでは参照できない場合があります。
- アニメーションは、データ量が多く送信に負荷が掛かるため、リモートコントロール機能を使用している間はコンピュータで表示させないでください。
- コントローラからの切断をコンピュータが認識していないとき、コントローラが再接続しようとすると［二重接続］ダイアログが表示されます。このダイアログでコンピュータとの接続を切断すると、再接続できるようになります。
- 画面の色（カラーパレット）は、256 色以上を使用してください。
- コンピュータで Windows の［コントロールパネル］－［マウス］－［ポインタ］の［ポインタの影を有効にする］をチェックしている場合、コントローラ上でマウスカーソルが二重表示され、コンピュータとコントローラとでマウスカーソルの形状が不一致になるときがあります。このようなときは、次のどちらかの方法で対処してください。
  - コンピュータで Windows の［コントロールパネル］－［マウス］－［ポインタ］の［ポインタの影を有効にする］のチェックを外す。
  - ［リモートコントロール］ウィンドウの［環境の設定］ダイアログの［高速化］タブで、［ウィンドウのアニメーション表示などを抑止する］をチェックする。
- コンピュータが監視モードの場合、次の操作または事象が発生したときはコンピュータのモードが共有モードに変わります。
  - コンピュータで［Ctrl］＋［Alt］＋［Delete］キーを押したとき
  - ハードウェアエラーまたはシステムエラーのメッセージが表示されたとき、およびそのメッセージを閉じたとき
  - Windows の Messenger サービスからメッセージが表示されたとき、およびそのメッセージを閉じたとき
- コンピュータが監視モードの場合、キーボード入力を擬似的に実行するアプリケーションや、キーの割り当てを変換するアプリケーションは正常に動作しません。
- コントローラが制御モードで接続している場合に、コンピュータの画面を非表示にするときは、次の点に注意してください。また、テスト環境で動作を十分に確認してから実行してください。
  - 対象のコンピュータのディスプレイボードとディスプレイが省電力モードに対応している必要があります。

- リモートコントロール時に、対象のコンピュータで CPU 使用率が 100%になったり、数秒間隔で画面に残像が残ったりすることがあります。
- コンピュータの画面の非表示は、強制的に解除されることがあります。画面の非表示が強制解除される要因を次の表に示します。

強制解除の契機	内容
通信の切断	• 管理者がリモートコントロールを切断または終了した。 • 利用者によってリモートコントロールが切断または終了された。 • 通信障害によってリモートコントロールが切断された。
制御モードの解除	• 対象のコンピュータで［Ctrl］＋［Alt］＋［Delete］キーが押された。 • 対象のコンピュータでハードウェアエラー、システムエラーのメッセージが表示された、または表示されたメッセージを閉じた。 • 対象のコンピュータで Windows Messenger サービスからメッセージが表示された、または表示されたメッセージを閉じた。

Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、および Windows Server 2012 のコンピュータと接続する場合の注意事項

- タスクマネージャの ［スタートアップ］ で、次のアプリケーションを無効にしないでください。無効にすると一部の機能が正常に動作しなくなります。
  - jdngrcagent.exe
  - jdngrcchat.exe
- コントロールパネルで ［ハードウェアとサウンド］－［デバイスとプリンター］－ ［マウス］を選択して表示される画面で、［ポインター オプション］ タブの［表示］－［ポインターの軌跡を表示する］のチェックをオンにした場合でも、コントローラにマウスカーソルの軌跡は表示されません。
- 制御モードで接続している場合で、対象のコンピュータの画面を非表示にしているときは、コントローラから［Ctrl］＋［Alt］＋［Delete］キーを送信できません。
- エージェント導入済みのコンピュータにマウスが接続されていない場合、コントローラに表示されるマウスカーソルの形状は、常に矢印カーソルのままとなります。

Windows 7、Windows Server 2008、および Windows Vista のコンピュータと接続する場合の注意事項

- リモートコントロール中は、ウィンドウの半透明表示、タスクバーのサムネイル表示、Windows フリップ 3D などの Windows Aero の機能は無効になります。
- Windows Aero のマウスポインタを使用する場合、リモートコントロール時のマウス操作のパフォーマンスが低下します。マウス操作のパフォーマンスを低下させないためには、マウスポインタのデザインを「なし」に変更してください。マウスポインタのデザインを変更する手順を次に示します。
  1. Windows の［コントロールパネル］－［マウス］をクリックします。
  2. ［マウスのプロパティ］ダイアログの［ポインタ］タブを表示します。
  3. ［デザイン］に［(なし)］を選択します。

4. [OK] ボタンをクリックします。

Windows 10、Windows 8.1、Windows 8、Windows 7 および Windows Vista のコンピュータと接続する場合の注意事項

- コントローラとの接続中に次の操作が実行されると、接続が切断されます。
  - ユーザーのログオフ
  - ユーザーの切り替え
  - リモートデスクトップ機能によるリモート接続

Windows 10 のコンピュータと接続する場合の注意事項

- 制御モードで接続している場合で対象のコンピュータの画面を非表示にしているときは、接続するコンピュータが次の条件のときにロックを解除してもサインイン画面が繰り返し表示されます。
  - 接続するコンピュータがドメイン環境に属している。
  - Windows の［設定］－［アカウント］－［サインインオプション］－［サインインを求める］に「PC がスリープから復帰したとき」が設定されている。

Windows Server 2019、Windows Server 2016、Windows Server 2012 および Windows Server 2008 のコンピュータと接続する場合の注意事項

- コントローラとの接続中に次の操作が実行されると、接続が切断されます。
  - ユーザーのログオフ
  - ユーザーの切り替え
  - リモートデスクトップ機能によるコンソール接続

Windows Server 2003 のコンピュータと接続する場合の注意事項

- Windows Server 2003 のリモートデスクトップ機能によるコンソール接続には対応していません。リモートデスクトップ機能によるコンソール接続が実行されると、以降、コントローラからの接続は拒否されます。コントローラと接続中であれば、コントローラからの接続は切断されます。

  再度接続するには、リモート接続先の Windows Server 2003 のロックを解除してください。

Windows XP のコンピュータと接続する場合の注意事項

- Windows XP のユーザーの切り替え機能とリモートデスクトップ機能には対応していません。

  Windows XP によるユーザーの切り替えやリモートデスクトップ機能によるリモート接続が実行されると、以降、コントローラからの接続は拒否されます。コントローラと接続中であれば、コントローラからの接続は切断されます。

  再度接続するには、次の操作が必要です。
  - ユーザーの切り替え操作によって接続が拒否された場合

    Windows XP ですべてのユーザーをログオフし、最初のユーザーでログオンし直してください。
  - リモートデスクトップ機能によって接続が拒否された場合

リモート接続先の Windows のロックを解除してください。

重要

OS が Windows 7 で Windows XP Mode のコンピュータは、リモートコントロールできません。

2.7.15　リモートコントロール中のファイル転送

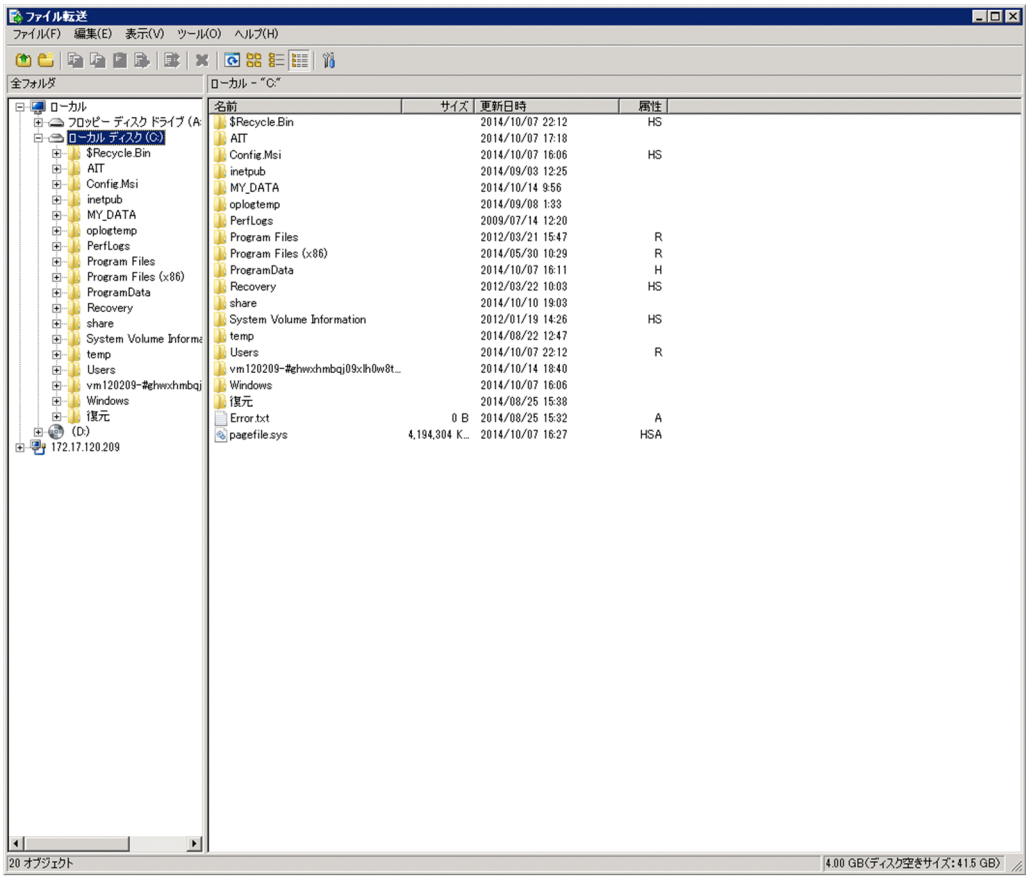
リモートコントロール中に、接続先のコンピュータとファイルの送受信ができます。

接続先のコンピュータのファイルをメンテナンスする際に、接続先のコンピュータのファイルを管理者のコンピュータにコピーして作業したり、トラブルシュートの際に対策ツールを転送して接続先のコンピュータで実行したりするような場合に活用できます。

重要

RFB でコンピュータに接続している場合は、ファイルを転送できません。 また、接続先のコンピュータに割り当てられているエージェント設定で、［リモートコントロールの設定］の［ファイル転送を許可する］が選択されている必要があります。

ファイルの転送は、コントローラから起動できる［ファイル転送］ウィンドウを利用します。



[ファイル転送] ウィンドウでは、Windows のエクスプローラと同様の操作でファイルを参照したり、ドラッグ&ドロップの簡単な操作でファイルを転送したりできます。また、複数の接続先に一括でファイルを転送することもできます。

ヒント

コントローラに表示されているコンピュータの画面に、ファイルをドラッグ&ドロップしてファイルを転送することもできます。この場合、[ファイル転送] ウィンドウが起動したあとすぐにファイルの転送が開始されます。転送したデータは、コンピュータのデスクトップに保存されます。

重要

OS が Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、または Windows Server 2012 R2 の場合、OneDrive を使用した環境でのファイル転送はできません。

(1) リモートコントロール中のファイル転送状況の表示と中断

ファイル転送が開始されると、コントローラとコンピュータの両方で [ファイル転送状況] ダイアログが表示されます（コンピュータでは最小化して表示されます）。

ファイル転送を中断するには、[ファイル転送状況] ダイアログの [キャンセル] ボタンをクリックします。[キャンセル] ボタンは、コントローラとコンピュータの両方からクリックできます。コントローラからキャンセルした場合は、ファイル転送を中断するかどうかを確認するダイアログが表示されますが、コンピュータからキャンセルした場合は、すぐにファイル転送が中断されます。

ファイル転送を中断すると、その時点で転送が完了しているファイルだけが転送先に残ります。また、移動の場合は転送が完了したファイルが転送元から削除されます。

なお、コンピュータ内およびコンピュータからコンピュータへのファイル転送では、直接ではなく、コントローラの一時フォルダを経由して転送されます。このため、コンピュータから一時フォルダまでの転送と、一時フォルダからコンピュータまでの転送の両方で、1 回ずつ（合計 2 回）[ファイル転送状況] ダイアログが表示されます。

(2) リモートコントロール中のファイル転送時の注意事項

ファイル転送機能を使用する場合の注意事項を次に示します。

- 次のような場合は、ファイルを転送できません。
  - [リモートコントロール] ウィンドウでコンピュータと接続していない場合
  - コントローラの接続モードが監視モードの場合
  - コンピュータがログオン前の場合
- コンピュータでファイル転送が許可されていない場合は、ファイルを転送できません。ただし、[ファイル転送] ウィンドウでの操作中にコンピュータでファイル転送を許可しないようオプションを変更しても、リモートコントロールでの接続を切断するまでは、そのままファイルの操作を継続できます。
- 低速回線でのファイル転送中は、メモリ不足による転送失敗を回避するために、[リモートコントロール] ウィンドウでのリモートコントロール（コンピュータの画面に対する操作）をしないようにしてください。
- ファイル転送中に回線障害が発生した場合、回線の切断を検知できないことがあります。この場合、ファイル転送用の再接続に失敗することがありますが、リモートコントロール機能などを利用して、コンピュータ側の [ファイル転送状況] ダイアログで、ファイル転送をキャンセルしてください。
- ファイル転送できるファイルパスの最大長は半角 260 文字です。
- ファイル転送機能でリパースポイント（シンボリックリンクやジャンクション）のフォルダおよびファイルにアクセスすることはできません。

2.7.16 接続先のコンピュータからコントローラへの接続要求

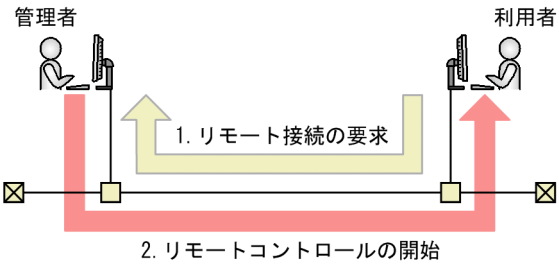
管理者のコンピュータから利用者のコンピュータを参照できない NAT 環境や NAPT 環境の場合、コントローラ側からコンピュータを参照できません。また、機器の IP アドレスが変わってしまう DHCP 環境では、コントローラから IP アドレスを指定して目的のコンピュータに接続するには、毎回 IP アドレスを調べる必要があるため非常に手間が掛かります。

このような環境では、通常利用者のコンピュータから管理者のコンピュータには接続できるため、利用者側からコントローラに対して接続要求を実行してもらうことで、リモートコントロールを開始できます。

> **重要**
>
> コントローラへの接続要求は、オンライン管理のコンピュータからだけ実行できます。

また、利用者から接続要求を実行してもらうことで、管理者が接続先を指定する手間も省けます。さらに、管理者が接続先の指定を誤って接続に失敗したり、コンピュータが管理者以外にリモートコントロールされたりすることを防げます。

利用者からの接続要求を受けて、リモートコントロールを開始する概念を次の図に示します。



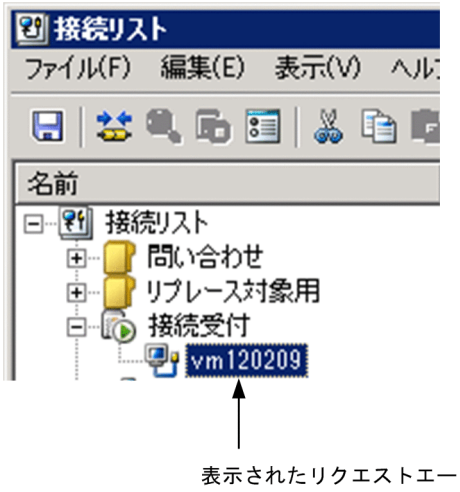
利用者からの接続要求を受信するには、接続リスト上でリクエストサーバを開始する必要があります。リクエストサーバ開始後、利用者からリモート接続の要求を受信すると（図中：1）、利用者のコンピュータが接続リストにアイコン表示されます。このアイコンをダブルクリックすることでリモートコントロールを開始できます（図中：2）。

関連リンク

- (1)　リクエストサーバからの接続要求の受信

(1)　リクエストサーバからの接続要求の受信

リクエストサーバが接続要求を受信すると、リクエストサーバ下に接続要求を出したエージェントが表示されます。この表示されたコンピュータを「リクエストエージェント」といいます。リクエストエージェントが表示された例を次に示します。



リクエストエージェントのアイコンをダブルクリックすると、コンピュータに接続してリモートコントロールを開始できます。

接続要求を拒否する場合は、リクエストエージェントを削除するか、接続リストを閉じてください。

リクエストサーバが停止すると、リクエストエージェントのアイコンは自動的に削除されます。また、エージェントが接続要求を出している間は活性化されていますが、接続要求が拒否された場合は非活性となります。

重要

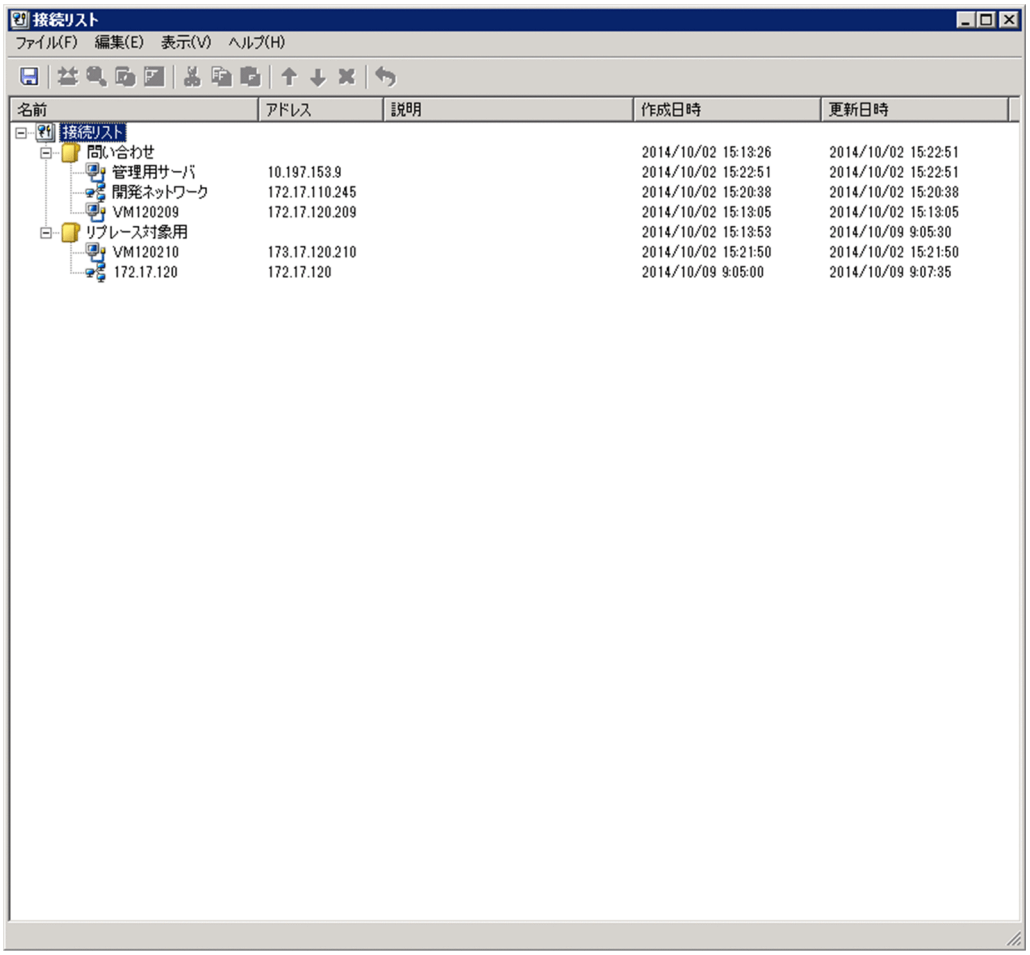
リクエストエージェントは、接続要求を出したエージェントが一時的に表示されたもので、このままでは情報として保存されません（接続リストを閉じると削除されます）。接続要求を出したエージェントの情報を保存したい場合は、ドラッグ&ドロップでアイコンを任意のグループに移動してください。フォルダ下に移動することで、接続リスト上の 1 アイテムとして保存できます。また、通常のコンピュータとして扱えるようになり、名前や説明を変更できます。

2.7.17　リモートコントロールの接続先の管理

接続先のコンピュータを、JP1/IT Desktop Management 2 の操作画面とは別に独自に管理できます。

コンピュータを登録しておくことで、コントローラから直接接続先を選択できるため、操作画面上で接続先のコンピュータを検索する手間を省けます。グループを作成して階層構成で接続先を管理することもできます。

接続先は、接続リストで管理します。



接続リストからは、ネットワーク上のリモートコントロールできるコンピュータを検索して、一覧に追加することもできます。

(1) リモートコントロールの接続環境の設定

リモートコントロールを利用する環境は、LAN だけであったり、WAN と LAN が混在していたりするなど、多様なネットワーク上にコンピュータが存在する場合があります。このような場合、適切な接続環境（接続に関する環境の設定）がコンピュータごとに異なります。しかし、コンピュータとの接続環境はコントローラに設定されているため、このような環境ではコンピュータと接続するたびに環境を設定し直すことになります。

この手間を省くため、コンピュータごとに適切な接続環境を設定できます。これによって、毎回環境を変更することなく、適切な設定でコンピュータと接続できるようになります。なお、接続環境は、コンピュータなどのアイテムの新規作成時にも設定できます。

> **ヒント**
>
> 個々のコンピュータに設定できる接続環境は、コントローラの［環境の設定］ダイアログの［接続環境］タブおよび［高度な設定］タブで設定できるものと同じです。コンピュータごとの接続環境を設定しない場合は、コントローラで設定したオプションが適用されます。

接続環境の引き継ぎ

コンピュータごとに設定した接続環境は、次のように引き継がれます。

- コンピュータを移動またはコピーした場合、接続環境は移動先またはコピー先に引き継がれます。
- グループ下にグループ、コンピュータ、またはネットワークを作成した場合、上位のグループで設定した接続環境が引き継がれます。

(2) リモートコントロールの接続履歴

接続方法のオプションを指定してコンピュータに接続した場合や、接続リストからコンピュータに接続した場合は、［リモートコントロール］ウィンドウの［対象のコンピュータの指定］に表示される接続履歴にコンピュータのパスが表示されます。表示されるパスには、次の 3 種類があります。

hrc://コンピュータ名

接続時にオプションで標準接続を指定したコンピュータです。

rfb://コンピュータ名

接続時にオプションで RFB での接続を指定したコンピュータです。

list://グループ名/コンピュータ名

接続リストから接続したコンピュータです。

コンピュータ名には、コンピュータの IP アドレスまたはホスト名が入ります。グループ名には、接続リストのグループ構成が入ります。接続リストで多階層のグループが構成されている場合、階層構成に沿って複数のグループ名が表示されます。

（例）接続リストの「/開発部/第 3 課」グループに登録されている「PC0001」に接続した場合のパス

list:///開発部/第 3 課/PC0001

2.7.18 リモートコントロールの録画・再生

リモートコントロール中のコンピュータの画面を録画して、動画ファイルとして保存できます。また、動画ファイルはコントローラで再生できます。

動画ファイルは、AVI ファイルに変換して、Windows Media Player のような動画再生ソフトウェアでも再生できます。これによって、コントローラがインストールされていない環境でも、動画を利用して利用者にトラブルの対処方法やアプリケーションの操作手順などを説明できます。

コンピュータの画面の録画は、次のような利用方法があります。

トラブルシュートでの利用

利用者がコンピュータで発生したトラブルを自分で対処するためには、ある程度の習熟度が必要です。管理者がトラブルの対処方法を録画して動画で解説すれば、利用者が理解しやすくなるだけでなく、手順書の作成も不要になるため、問題解決の効率も向上します。

トレーニングでの利用

アプリケーションの操作手順や業務の作業手順などを記録して、教材として利用できます。例えば、手順書では説明しにくい複雑な操作がある場合、動画で説明することで理解しやすくなることがあります。

(1) リモートコントロール中の録画状態の表示

ステータスバーに録画状態を表すステータスアイコンを表示することで、録画状態を確認できます。

ステータスアイコンの表示は、[リモートコントロール] ウィンドウの [環境の設定] ダイアログの [ログ情報] タブで設定できます。なお、ステータスアイコンは、コンピュータに接続していない場合は表示されません。

コンピュータの画面情報の録画状態は、次のアイコンで表示されます。

-  ：録画中
-  ：録画の一時停止
-  ：録画停止

ヒント

ステータスアイコンを右クリックして、表示されるメニューから録画の操作ができます。

(2) リモートコントロール中の画面を効率良く録画するための設定方法

録画を始めるたびに録画ファイルを選択していると作業効率が良くありません。そこで、あらかじめ録画ファイルの保存先とファイル名を設定しておくことで、ファイル選択の手間を省略できます。また、コンピュータと接続すると同時に録画を開始するような設定もできます。

録画のための設定は、[リモートコントロール] ウィンドウのツールバーで [環境の設定] ボタンをクリックして表示されるダイアログの [ログ情報] タブで設定できます。

録画ファイルの設定

[ログ情報] タブで録画ファイルを指定しておくと、コンピュータの画面情報は自動的に指定した録画ファイルに保存されます。このとき、録画ファイル名を特定のファイル名に固定すると、録画するたびに上書きするか、または録画ファイルを設定し直すことになります。 複数の録画ファイルを管理するなど、録画ごとの録画ファイルが必要な場合は、変数を使って録画ファイル名を設定しておきます。変数を利用した場合、録画開始時に変数に値を読み込んでファイル名が付けられます。利用できる変数は、次の 3 種類です。

- $(Agent)
  「コンピュータ名」の変数です。コントローラで指定した接続先（IP アドレス、ホスト名、または別名）が設定されます。
- $(Date)

「日付」の変数です。録画を開始した日付が、*YYYY-MM-DD* の形式で設定されます（*YYYY*：年、*MM*：月、*DD*：日）。

- $(Time)
  「時間」の変数です。録画を開始した時間が、*hhmmss* の形式で設定されます。このとき、hh は 24 時間表記となります（*hh*：時、*mm*：分、*ss*：秒）。

これらを利用した任意のファイル名を指定することもできますし、デフォルトで提供されている 3 種類のテンプレートから選択することもできます。

変数を使ったファイル名の指定例を次に示します。この例では、コンピュータ名を「10.xxx.xxx.4」、日付を「2011 年 4 月 1 日」、時間を「15 時 5 分 45 秒」としています。これらの設定は、［ログ情報］タブから表示した［スクリーン操作の記録先の選択］ダイアログでテンプレートを選択します。

提供されているテンプレートから選択する

［ファイルの種類］のリストから、ファイル名のテンプレートを選択します。

- 「記録ファイル（名前.jcr）」を選択した場合
  （例）10.xxx.xxx.4.jcr
- 「記録ファイル（名前 日付 時間.jcr）」を選択した場合
  （例）10.xxx.xxx.4 2011-04-01 150545.jcr
- 「記録ファイル（日付 時間 名前.jcr）」を選択した場合
  （例）2011-04-01 150545 10.xxx.xxx.4.jcr

変数を利用した任意のファイル名を指定する

［ファイル名］に、変数を使用して直接指定します。

- 「$(Agent) $(Date).jcr」と指定した場合
  （例）10.xxx.xxx.4 2011-04-01.jcr
- 「ユーザー名（nnn）_ $(Date).jcr」と指定した場合
  （例）nnn_2011-04-01.jcr

接続時に録画を開始するための設定

［対象のコンピュータとの接続時に、スクリーン操作の記録を開始する］をチェックすると、コンピュータに接続すると同時に録画を開始します。

(3) リモートコントロールに関する利用者のコンピュータ側での操作

リモコンエージェントは、エージェントに含まれるリモートコントロールを受ける側のプログラムです。通常は特別な操作は必要ありませんが、必要に応じてリモートコントロールを拒否したり、接続状況を確認したりできます。また、コントローラからの接続を待つだけではなく、コントローラに接続要求を出すこともできます。

エージェント設定の［リモートコントロールの設定］で自動起動を指定しておくと、エージェント導入済みのコンピュータの起動時に、リモコンエージェントが自動的に起動します。

自動起動を設定していない場合、利用者のコンピュータ側でリモコンエージェントを手動で起動させてください。手動で起動するには、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］－［リモコンエージェント］－［リモコンエージェント］を選択してください。

リモコンエージェントが起動すると、タスクバーに［リモコンエージェント］アイコン（  ）が表示されます。

なお、エージェント設定でアイコンを表示する設定をしていない場合、リモコンエージェントを起動しても、［リモコンエージェント］アイコンおよびステータスウィンドウは表示されません。

ヒント

 の［リモコンエージェント］アイコンは、コントローラと未接続の状態です。コントローラと接続すると、接続モードに応じてアイコンが変わります。

ヒント

Windows 7 および Windows Server 2008 R2 では、タスクバーに［リモコンエージェント］アイコンは表示されません。タスクバーにアイコンを表示したい場合は、コントロールパネルの［デスクトップのカスタマイズ］－［タスクバーのアイコンのカスタマイズ］を選択し、［リモコンエージェント］アイコンの動作を［アイコンと通知を表示］に設定してください。

(4) コントローラとの接続状態の確認

リモコンエージェントを起動すると表示される［リモコンエージェント］アイコンまたはステータスウィンドウでは、次に示す情報を確認できます。

- コントローラと接続しているかどうか
- 接続しているコントローラの台数
- エージェントの接続モード

［リモコンエージェント］アイコンでの表示

リモコンエージェントは、アイコンの色でコントローラとの接続状態を表しています。

- （灰色）：未接続
- （オレンジ）：監視モードで接続中
- （黄）：共有モードで接続中
- （緑）：制御モードで接続中

なお、[リモコンエージェント] アイコンにマウスポインタを重ねると、接続先のコントローラの台数が表示されます。

ステータスウィンドウでの表示

ステータスウィンドウでは、タイトルバーの色がコントローラとの接続状態を表しています。色の意味は [リモコンエージェント] アイコンと同じです。また、タイトルバーに、接続状況、接続モード、および接続先のコントローラの台数が表示されます。

なお、タイトルバーの、括弧内の数字は、接続先のコントローラの台数を示しています。

2.7.19　チャットの利用

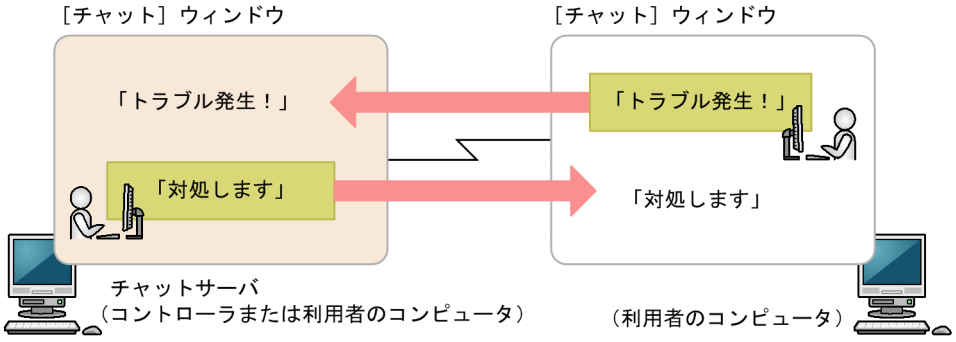
標準接続でリモートコントロール中に利用者と連絡を取る場合、手もとに電話がない環境では、チャットを利用することで利用者と対話できます。チャットはテキストデータで対話するため、IP アドレスや URL などの情報を文字でリアルタイムに連絡したい場合にも便利です。

なお、チャットでは複数の利用者と同時に対話することもできます。

例えば、利用者のトレーニングに利用できます。全員に同じ指示を出せるので、おのおのに説明する手間が省けます。また、トレーニング中の質疑応答では、質問のあった利用者だけに回答したり、必要な場合は全員に回答内容を伝えたりできます。

> **重要**
>
> RFB で接続している場合は、チャットを利用できません。

チャットの概要を次の図に示します。



チャットを開始するためには、チャットサーバを起動する必要があります。チャットサーバを起動後、ほかのコンピュータが [チャット] ウィンドウから接続すると、チャットが開始されます。なお、[チャット] ウィンドウからは、複数のチャットサーバへ接続することもできます。

チャット中は、[チャット] ウィンドウに入力したメッセージを、ほかのコンピュータに送信できます。チャットサーバに接続中のすべてのコンピュータにメッセージを同時に送信したり、個別にメッセージを送信したりできます。

(1) [チャットサーバ] アイコンの利用

チャットサーバが起動すると、タスクバー上に [チャットサーバ] アイコン（  ）が表示されます。

[チャットサーバ] アイコンからは、次の操作ができます。

- 接続中のユーザーの確認

  チャットサーバに接続しているユーザーを確認できます。ただし、接続中のユーザーがいない場合は、この操作はできません（メニューが非活性となります）。
- チャットユーザーとの切断

  接続中のユーザーと切断できます。全ユーザーと切断するだけでなく、選択したユーザーと切断することもできます。
- オプションの設定

  チャットサーバのポート番号や、パスワードを設定できます。

ヒント

Windows 7 および Windows Server 2008 R2 では、タスクバーに [リモコンエージェント] アイコンは表示されません。タスクバーにアイコンを表示したい場合は、コントロールパネルの [デスクトップのカスタマイズ] − [タスクバーアイコンのカスタマイズ] を選択し、[チャットサーバ] アイコンの動作を [アイコンと通知を表示] に設定してください。

2.7.20 リモートコントロールのメニュー一覧

(1) [リモートコントロール] ウィンドウのメニュー一覧

メニューバー	メニュー項目	機能
ファイル	接続	コンピュータと接続します。すでにコンピュータと接続中の場合、新規に [リモートコントロール] ウィンドウを起動して接続します。
	再接続	直前に接続していたコンピュータと再接続します。
	切断	選択したコンピュータとの接続を切断します。
	接続できるコンピュータを検索	ネットワーク上のコンピュータを検索します。
	スクリーンを保存	リモートコントロール中の画面をファイルに保存します。

メニューバー	メニュー項目		機能
ファイル	スクリーン操作を記録	開始	リモートコントロール中の画面情報の記録を開始します。
		一時停止	リモートコントロール中の画面情報の記録を一時的に停止します。
		再開	一時停止した記録を再開します。
		停止	リモートコントロール中の画面情報の記録を停止します。
	スクリーン操作を再生	再生	リモートコントロール中の画面情報を再生します。
		変換	リモートコントロール中の画面情報を記録したファイルを AVI ファイルに変換します。
	終了		コントローラを終了します。
	すべて終了		起動しているすべてのコントローラを終了します。
表示	ツールバー	ツールバー	ツールバーの表示/非表示を切り替えます。
		ボタンラベル	ツールボタンの説明文の表示/非表示を切り替えます。
	ステータスバー	ステータスバー	ステータスバーの表示/非表示を切り替えます。
		経過時間	コンピュータとの接続経過時間の表示/非表示を切り替えます。
		送受信データ量	コンピュータとの転送データ数の表示を設定します。
	キーボードの入力バー	キーボードの入力バー	登録した特殊キーを画面の下辺に表示します。
		キーボードの設定	特殊キーを登録します。
	最新表示		画面の表示内容を最新にします。
	スクリーンカラー	グレースケール	画面情報をグレースケールに減色して表示します。
		256 色	画面情報を 256 色に減色して表示します。
		65,536 色	画面情報を 65,536 色に減色して表示します。
		65,536 色＋ JPEG 圧縮	画面情報を 65,536 色に減色し、さらにデータを圧縮して表示します。
		減色なし	画面情報を減色しないで表示します。
	スクリーンサイズ	自動調整を取消	拡大または縮小した画面を元に戻します。
		サイズ自動調整	[リモートコントロール] ウィンドウのサイズに合わせて画面を自動的に拡大または縮小します。
	フルスクリーン		リモートコントロール中の画面をフルスクリーン表示します。
ツール	環境の設定		コントローラの動作環境を設定します。
	接続モード	監視モード	接続モードを「監視モード」に設定します。
		共有モード	接続モードを「共有モード」に設定します。
		制御モード	接続モードを「制御モード」に設定します。

メニューバー	メニュー項目	機能
ツール	シャットダウン	接続中のコンピュータをシャットダウンします。
	再起動	接続中のコンピュータを再起動します。
	Ctrl+Alt+Del を送信	接続中のコンピュータに［Ctrl］＋［Alt］＋［Delete］キーを送信します。
	CD/DVD のマウント	管理者のコンピュータの CD/DVD ドライブを、リモート CD-ROM ドライブとして利用します。
	CD/DVD のアンマウント	リモート CD-ROM の利用を解除します。
	IDER ブートの有効化	接続先のコンピュータに対して、リモート CD-ROM を利用した CD-ROM 起動ができるようにします。
	ファイル転送	［ファイル転送］ウィンドウを表示します。
	チャット	［チャット］ウィンドウを表示します。
接続リスト	接続リストに追加	現在接続中のコンピュータを接続リストに追加します。
	接続リストを編集	接続リストを表示します。
ウィンドウ	上下に並べて整列	［リモートコントロール］ウィンドウを上下に並べて表示します。
	左右に並べて整列	［リモートコントロール］ウィンドウを左右に並べて表示します。
	左上から順に整列	［リモートコントロール］ウィンドウを上下左右に均等に並べて表示します。
	すべて最小化	すべての［リモートコントロール］ウィンドウをアイコン化します。
	リモートコントロール	選択した［リモートコントロール］ウィンドウを手前に表示します。
ヘルプ	ヘルプ	ヘルプを表示します。
	バージョン情報	バージョン情報を表示します。

［接続］ボタンから表示されるメニュー一覧

メニュー項目	機能
接続	コンピュータに接続します。また、接続できるコンピュータを検索することもできます。
接続リストに追加	現在接続中のコンピュータを接続リストに追加します。
接続リストを編集	接続リストを表示します。

(2) ［ファイル転送］ウィンドウのメニュー一覧

メニューバー	メニュー項目		機能
ファイル	開く		選択したフォルダやファイルを開きます。
	新規作成	フォルダ	新規にフォルダを作成します。
	削除		選択したフォルダやファイルを削除します。
	名前の変更		選択したフォルダやファイルの名前を変更します。
	プロパティ		選択したフォルダやファイルの属性を変更します。
	切断		ファイル転送用の接続を切断します。
	ファイル転送の終了		［ファイル転送］ウィンドウを終了します。
編集	コピーファイル予約		コピーするファイルを登録します。
	移動ファイル予約		移動するファイルを登録します。
	転送		ファイル転送を開始します。
	すべてを選択		選択したドライブまたはフォルダの中の項目すべてを選択します。
	選択の切り替え		選択している項目と選択していない項目を反転させます。
	ファイルを確認	予約ファイル	コピーファイルまたは移動ファイルとして登録されているファイルの情報を確認します。
		選択ファイル	選択しているファイルの情報を確認します。
	マルチ転送		複数のコンピュータに対して、同じ転送先フォルダを指定してファイルを転送します。
表示	ツールバー		ツールバーを表示します。
	ステータスバー		ステータスバーを表示します。
	アイコン		フォルダまたはファイルをアイコンで表示します。
	一覧		フォルダまたはファイルを一覧で表示します。
	詳細		フォルダまたはファイルを詳細項目（名前、サイズ、更新日時、属性）で表示します。
	一つ上のフォルダへ		現在表示しているフォルダよりも、1 つ上のフォルダ中の項目を表示します。
	最新表示		［ファイル転送］ウィンドウに表示される情報を最新にします。
	リモートファイルの一覧		［リモートファイルの一覧］ウィンドウを表示します。
ツール	環境の設定		［ファイル転送］ウィンドウの表示や、ファイルの転送方法についてのオプションを設定します。
ヘルプ	ヘルプ		ヘルプを表示します。
	バージョン情報		バージョン情報を表示します。

(3) リモートファイルの一覧の［ファイル転送］ウィンドウのメニュー一覧

メニューバー	メニュー項目	機能
ファイル	削除	コントローラに保存したファイルを削除します。
	自動的に閉じる	リモートファイルの一覧の［ファイル転送］ウィンドウからすべてのファイルが削除された場合、自動的にリモートファイルの一覧の［ファイル転送］ウィンドウを閉じるかどうかを設定します。
	閉じる	リモートファイルの一覧の［ファイル転送］ウィンドウを閉じます。
編集	転送	ファイルを、コンピュータの元の場所にコピーします。
	転送後に削除	ファイルを、コンピュータの元の場所に移動します。
	すべてを選択	表示されているすべてのファイルを選択します。
	選択の切り替え	選択している項目と、選択していない項目との選択状態を切り替えます。
表示	最新表示	ウィンドウに表示される情報を最新にします。
ヘルプ	ヘルプ	ヘルプを表示します。
	バージョン情報	バージョン情報を表示します。

(4) ［接続リスト］ウィンドウのメニュー一覧

メニューバー	メニュー項目		機能
ファイル	新規作成	グループ	グループを新規に作成します。
		接続先コンピュータ	コンピュータを新規に作成します。
		ネットワーク	接続できるコンピュータの検索範囲を定義するためのネットワークを作成します。
		リクエストサーバ	リクエストサーバを新規に作成します。
		区切り線	区切り線を挿入します。
	インポート	管理ファイルからのインポート	接続リストをバックアップファイルから読み込んで作成します。
		Hosts ファイルからのインポート	接続リストを hosts ファイルから読み込んで作成します。
	接続		選択したコンピュータと接続します。ネットワークまたはリクエストサーバを選択している時は表示されません。
	検索		選択したネットワークに対して検索を実行します。
	開始		選択したリクエストサーバを開始します。
	停止		選択したリクエストサーバを停止します。

メニューバー	メニュー項目		機能
ファイル	削除		選択したアイテムを削除します。
	名前の変更		グループ、コンピュータ、またはリクエストサーバの名前を変更します。
	プロパティ		グループ、コンピュータ、またはリクエストサーバのプロパティを表示・変更します。
	保存		現在の構成情報をデフォルトのバックアップファイルに保存します。
	名前を付けて保存		現在の構成情報に名前を付けてファイルに保存します。
	接続リストの終了		接続リストを閉じます。
編集	やり直し		削除、移動、変更したデータを元に戻します。
	切り取り		選択した項目を切り取ります。
	コピー		選択した項目をコピーします。
	貼り付け		切り取り、コピーした項目を接続リスト上で貼り付けます。
	すべて選択		フォルダ内のすべての項目を選択します。
	選択項目の反転		選択している項目と選択していない項目との選択状態を反転させます。
	上の項目に移動		選択した項目を 1 つ上に移動します。
	下の項目に移動		選択した項目を 1 つ下に移動します。
	項目の検索		接続リスト上の項目を検索するキーワードを設定します。
	次を検索		接続リスト上の項目をキーワードで検索します。
表示	ツールバー		ツールバーを表示します。
	ステータスバー		ステータスバーを表示します。
	折り返し表示		選択した項目を折り返して表示します。
	罫線を表示	行単位	行単位の境界線を表示します。列の境界線を同時に表示することもできます。
		列単位	列単位の境界線を表示します。行の境界線を同時に表示することもできます。
	行全体の選択		選択した項目のアドレス、説明、および作成日時を強調して表示します。
	列幅の自動補正		アドレス、説明、および作成日時をウィンドウ範囲内に表示します。
ヘルプ	ヘルプ		ヘルプを表示します。
	バージョン情報		バージョン情報を表示します。

(5) ［リモコンプレーヤー］ウィンドウのメニュー一覧

メニューバー	メニュー項目		機能
ファイル	新規		リモコンプレーヤーを新規に起動します。
	開く		再生する記録ファイルを選択します。
	プロパティ		記録ファイルを開いている場合、その記録ファイルに関する情報を表示します。
	終了		リモコンプレーヤーを終了します。
再生	再生		一時停止中、または停止中の状態から再度、再生を開始します。
	一時停止		再生を一時的に停止します。
	停止		再生を停止します。
	早送り		記録ファイルを早送りします。
	スロー再生		記録ファイルをスロー再生します。
表示	ツールバー		ツールバーの表示/非表示を切り替えます。
	ステータスバー		ステータスバーの表示/非表示を切り替えます。
	シークバー		シークバーの表示/非表示を切り替えます。
	拡大／縮小	自動	再生画面のウィンドウサイズを、リモコンプレーヤーのウィンドウサイズに合わせて自動的に拡大・縮小します。
		50%	再生画面のウィンドウサイズを 50%に縮小して表示します。
		100%	再生画面のウィンドウサイズを 100%で表示（等倍表示）します。
		200%	再生画面のウィンドウサイズを 200%に拡大して表示します。
	フルスクリーン表示		ビューをコントローラの画面全体に表示します。
ウィンドウ	上下に並べて表示		リモコンプレーヤーのウィンドウを上下に並べて表示します。
	左右に並べて表示		リモコンプレーヤーのウィンドウを左右に並べて表示します。
	左上から順に整列		リモコンプレーヤーのウィンドウを上下左右に均等に並べて表示します。
	すべて最小化		すべてのリモコンプレーヤーのウィンドウをアイコン化します。
	表示幅に合わせる		再生画面のウィンドウサイズに、リモコンプレーヤーのウィンドウサイズを合わせます。
ヘルプ	ヘルプ		ヘルプを表示します。
	バージョン情報		バージョン情報を表示します。

(6) ［チャット］ウィンドウのメニュー一覧

メニューバー	メニュー項目		機能
ファイル	接続		チャットサーバと接続します。すでにチャットサーバと接続中の場合でも、ほかのチャットサーバに接続できます。
	切断		接続中のチャットサーバと切断します。
	チャットユーザー情報の表示		選択しているユーザーの詳細情報を表示します。
	チャットメッセージの送信		メッセージ入力ボックスに入力された、チャットメッセージを送信します。
	ビープ音の送信		接続中の、ほかのチャットユーザーのコンピュータで、ビープ音を 1 回鳴らします。
	上書き保存		現在のチャット内容をファイルに上書き保存します。
	名前を付けて保存		現在のチャット内容を新規に保存します。
	印刷		現在のチャット内容を印刷します。
	印刷プレビュー		現在のチャット内容の印刷結果をプレビューします。
	終了		［チャット］ウィンドウを終了します。チャットサーバとは自動的に切断されます。
表示	ツールバー		ツールバーの表示/非表示を切り替えます。
	ステータスバー		ステータスバーの表示/非表示を切り替えます。
ツール	環境の設定		［チャット］ウィンドウの動作環境を設定します。
	チャットサーバ	チャットサーバを起動	チャットサーバの起動/停止を切り替えます。チャットサーバが起動中の場合はチェックマークが付きます。
		最小化時に隠す	チャットサーバの起動中にウィンドウが最小化された場合、ウィンドウをタスクバーから隠します。最小化が設定されている場合は、チェックマークが付きます。
		スタートアップに登録	チャットサーバをスタートアップに登録または解除します。スタートアップに登録するとチェックマークが付きます。
	リモートコントロールの開始		選択したユーザーに接続して、リモートコントロールを開始します。エージェントで起動した［チャット］ウィンドウでは非活性となります。
ヘルプ	ヘルプ		ヘルプを表示します。
	バージョン情報		バージョン情報を表示します。

(7) リモートコントロール中（フルスクリーン表示時）のメニュー

フルスクリーン表示でリモートコントロールを実行している場合、メニューバー上で右クリックするとメニューを表示できます。メニューからは、画面の色数や接続モードなどを変更できます。

なお、メニューを閉じるには、メニューから［キャンセル］を選択してください。

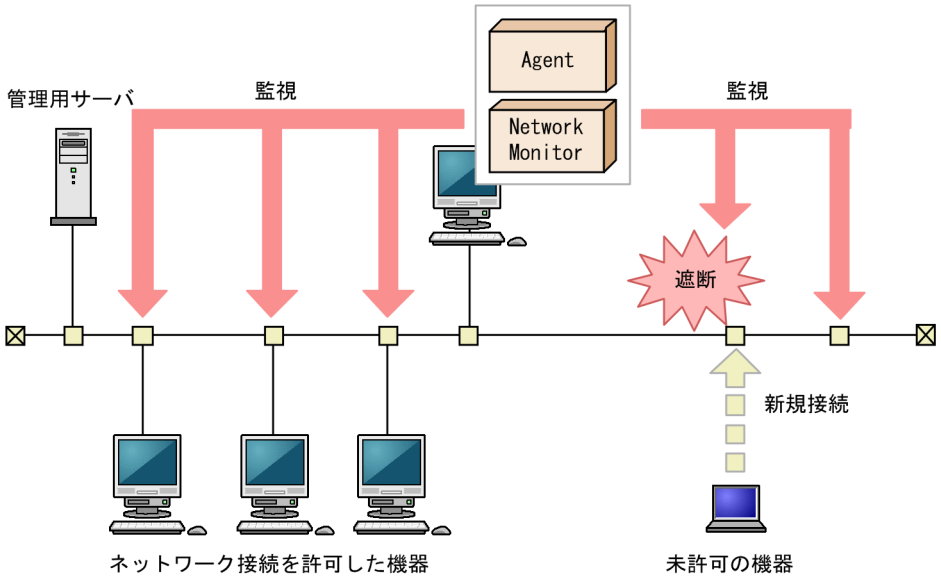
メニューに表示される項目を次の表に示します。

項目			説明
表示	メニューバー	自動的に隠す	マウスカーソルを画面上部へ移動させるたびに、メニューバーが表示されるように設定します。
		常に表示する	マウスカーソルを画面上部へ移動させなくても、常にメニューバーが画面上部に表示されるように設定します。
	最新を表示する		リモートコントロール中の画面の表示内容を最新の状態に更新します。
	スクリーンカラー	グレースケール	画面の色を 8 階調のグレースケールに変換して表示します。
		256 色に減色	画面の色を 256 色に減色して表示します。
		65,536 色に減色	画面の色を 65,536 色に減色して表示します。
		65,536 色に減色+JPEG 圧縮	画面の色を 65,536 色に減色して表示します。色数の多い画面は、JPEG で圧縮されます。
		減色なし	画面の色を減色しないでそのまま表示します。
	最小化		リモートコントロール中の画面を最小化します。
	元に戻す		フルスクリーン表示を解除して、ウィンドウ表示に戻します。
ツール	接続モード	監視モード	接続モードを監視モードに変更します。
		共有モード	接続モードを共有モードに変更します。
		制御モード	接続モードを制御モードに変更します。
	Ctrl+Alt+Del を送信する		接続先のコンピュータに、[Ctrl] ＋ [Alt] ＋ [Delete] キーと同様の操作を実行します。
キャンセル			ポップアップメニューが閉じます。
終了			リモートコントロールを終了して、ウィンドウが閉じます。

2.8　機器のネットワーク接続の管理

無線 LAN やモバイルコンピュータの普及に伴い利便性が向上してきたことで、組織の従業員または組織外の人によって個人が使用するコンピュータが意図的に持ち込まれ、容易に組織内のネットワークに接続されるおそれがあります。セキュリティ対策がされていない機器がネットワーク接続することによるウィルス感染や、機密情報の不正持ち出しといった被害を防ぐためには、ネットワーク接続されている機器を把握して管理する必要があります。

ネットワークモニタ機能を利用して未許可の機器のネットワーク接続を遮断するように管理することで、企業のネットワークを保護できます。また、ネットワークを監視することで、未確認の機器がネットワーク接続されたことをリアルタイムに検知できるようになります。



（凡例）

Agent：JP1/IT Desktop Management 2 - Agent

Network Monitor：ネットワークモニタエージェント

ネットワークモニタ機能を利用するには、セグメント内のコンピュータを選び、このコンピュータにネットワークモニタエージェントをインストールします。ネットワークモニタエージェントをインストールするとネットワークモニタが有効になり、同一セグメント内のコンピュータの接続許可や遮断ができるようになります。 ネットワークモニタエージェントはセグメントごとに管理されるため、複数のセグメントがある場合は、セグメントごとにネットワークモニタエージェントをインストールする必要があります。

なお、管理用サーバ、中継システム、または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は、ネットワーク接続を遮断できません。また、UNIX エージェント、Mac エージェントは、手動でネットワーク接続を許可/遮断できます。

2.8.1　ネットワーク監視機能による機器の検知

機器画面の［機器情報］－［機器一覧（ネットワーク）］画面に表示される各ネットワークセグメントのグループで、ネットワークモニタを有効にすると、新規にネットワークに接続しようとした機器を検知できます。検知された機器には、自動的にネットワークの探索が実行されます。発見された機器は、ネットワークモニタ設定に従って、ネットワーク接続が制御されます。

重要

ネットワークモニタ機能は、ネットワーク接続を許可する機器、および許可しない機器を十分に確認してから使用してください。ネットワークへの接続を制御する方法を誤ると、業務に使用している機器の接続が遮断されるなど、トラブルにつながるおそれがあります。

重要

ネットワークモニタ機能は、共有型 VDI の仮想コンピュータでは利用できません。

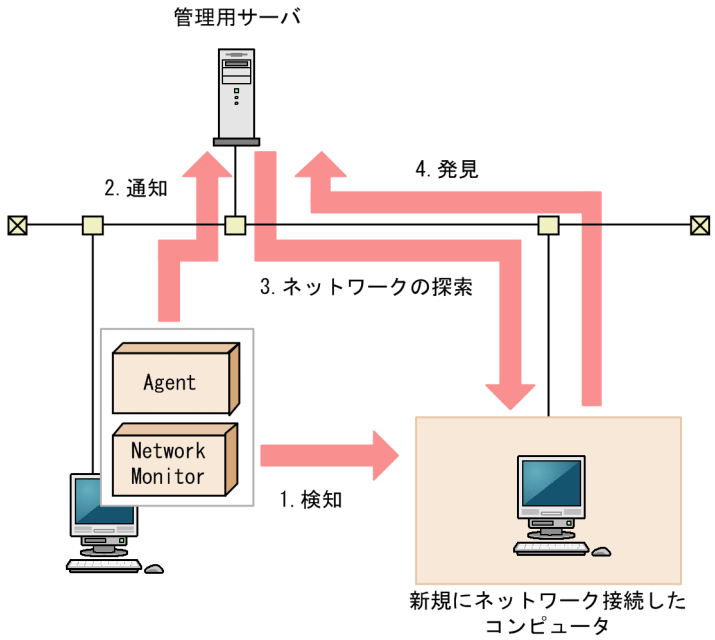
ヒント

管理用サーバ、中継システム、および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、ネットワーク制御によって接続を遮断できません。

ヒント

機器を検知するためには、1 つのネットワークセグメントに対して 1 台のエージェント導入済みコンピュータのネットワークモニタを有効にしてください。複数のネットワークカードを使って複数のネットワークに接続できるコンピュータであれば、ネットワークモニタを有効にしたエージェント導入済みコンピュータ 1 台で、複数のネットワークセグメントを監視できます。また、ネットワークセグメントの範囲の探索範囲を設定し、認証情報を対応づけてください。なお、探索範囲に含まれないネットワークアドレスで機器が検知された場合、認証情報を使用しない探索が実行されるため、MAC アドレスと IP アドレスの情報だけ取得されます。

ネットワークに接続した機器を検知し、JP1/IT Desktop Management 2 に登録する仕組みについて次の図に示します。



（凡例）

Agent：JP1/IT Desktop Management 2 - Agent
Network Monitor：ネットワークモニタエージェント

1. 機器がネットワークに接続しようとすると、ネットワークモニタが有効になったエージェント導入済みのコンピュータが、その機器を検知します。

2. ネットワークモニタが有効になったエージェント導入済みのコンピュータから機器を検知したことが管理用サーバに通知されます。

3. 通知された情報を基に、その機器に対してネットワークの探索を実行します。

重要

機器の探索（ネットワーク探索）がすでに実行されている場合は、終了するまで待ちます。ネットワーク監視機能の機器の検知に時間が掛かる場合は、機器の探索（ネットワーク探索）の探索範囲を縮小するなどで対処してください。

ヒント

発見時にエージェントレスの認証をしたい場合は、ネットワークモニタによって監視されるIP アドレスを含む探索範囲と認証情報をあらかじめ設定してください。

4. 探索の結果、発見された機器は、探索条件によって自動的に管理対象になったりエージェントが自動配信されたりします。

重要

NAT を経由したネットワークなど、管理用サーバから直接通信できないネットワークセグメントは、ネットワークモニタ機能を利用しても機器を検知できません。

NAT を経由したネットワークでネットワークモニタ機能を利用したい場合は、ネットワークセグメントごとに管理用サーバを設置した複数サーバ構成システムを構築してください。

重要

ネットワークの探索で発見した機器に、自動でエージェントを配信するように設定している場合、発見されたコンピュータがネットワーク接続を許可されなくても、そのコンピュータにエージェントは配信されます。

このため、ネットワーク接続が許可されないコンピュータにエージェントが導入された場合、セキュリティポリシーのネットワーク制御の設定およびセキュリティの判定結果によっては、そのコンピュータがネットワーク接続できてしまうことがあります。

重要

ネットワークモニタ機能によって発見された機器を削除した場合、ネットワークをいったん切断して再接続しないと、その機器は再発見できません。また、ネットワークを切断してから再接続するまでの時間が短か過ぎた場合、機器を再発見できないことがあります。

ヒント

ネットワークモニタ設定が許可する/許可しないのどちらの設定でも、ネットワーク接続した機器を発見できます。ネットワークモニタによって発見された機器には、自動的にネットワークの探索が実行されます。このため、ネットワークの探索で、自動的に管理対象とする、またはエージェントを自動配信するよう設定されている場合は、ネットワークモニタによって機器が発見されると、自動的に管理対象になるか、エージェントが自動配信されます。この場合、機器が管理対象になって、製品ライセンスが消費されます。

自動で管理対象にしたくない場合は、探索条件の設定で［自動的に管理対象とする］および［エージェントを自動配信する］のチェックを外して、手動で管理対象にするようにしてください。

ネットワーク監視機能の監視対象は次のとおりです。

- 監視対象のネットワークは IPv4 だけです。IPv6 には対応していません。
- 標準 TCP/IP を使用しているコンピュータに限り、監視対象となります。
- 監視対象となるプロトコルは、TCP/IP のネットワークです。NetBEUI や IPX などには対応していません。
- 無線 LAN に接続したネットワーク接続機器を制御する場合は、MAC アドレスの情報を中継するアクセスポイントとしてください。MAC アドレスの情報を中継しない場合、ネットワーク制御はできません。

2.8.2　ネットワーク接続を制御するための設定

ネットワークセグメントにネットワークモニタ機能を導入すると、ネットワークセグメント内の機器のネットワーク接続を制御できます。機器のネットワーク接続を制御する際は、管理者がネットワークセグメントの状況を把握する必要があります。そのため、管理用サーバごとに機器のネットワーク接続を制御します。ここでは、機器のネットワーク接続を制御する設定について説明します。

ネットワークモニタ機能の導入

ネットワークモニタ機能を導入するためには、監視したい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。ネットワークモニタを有効にすると、そのネットワークセグメントに対して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。なお、ネットワークモニタを有効にできるのは、ネットワークセグメント内のエージェント導入済みのコンピュータ 1 台だけです。2 台目は有効にできません。2 台目を有効にしようとすると、エラーメッセージが表示されます。

重要

ルータ、スイッチ、ネットワークプリンタなどのネットワーク装置は、当該装置からの通信が発生しにくいため、ネットワークモニタを有効にした運用を開始した直後などは、ネットワークモニタによって検知されない場合があります。

ヒント

ネットワークモニタが有効になっていないネットワークセグメントが存在するかどうかは、ホーム画面の［通知事項］パネルで確認できます。ネットワークモニタが有効になっていないネットワークセグメントがある場合、警告メッセージが表示されます。

ネットワーク接続の制御方法の設定

ネットワークモニタを有効にしたネットワークセグメントでは、ネットワーク接続の制御について次の 2 つの設定ができます。

1. 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の設定（ネットワークモニタ設定）

   ネットワークモニタ設定では、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ます。ネットワークモニタ設定は、ネットワークモニタを有効にしたコンピュータに割り当てます。これによって、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、ネットワークセグメントごとに設定できます。割り当てるネットワークモニタ設定は、ネットワークモニタを有効化するときに選択できます。ネットワークモニタ設定の設定や割り当ては、あとから変更することもできます。

   ネットワークモニタ設定の管理については、「2.8.6　ネットワークモニタ設定による制御」を参照してください。

2. 機器ごとにネットワーク接続を許可するかどうかの設定（ネットワーク制御リスト）

   ネットワーク制御リストでは、機器ごとにネットワークへの接続を許可するかどうかを設定できます。発見された機器は自動的にネットワーク制御リストに登録されます。このとき、その機器のネットワーク接続を許可するかどうかは、ネットワークモニタ設定に依存します。各機器のネットワーク制御リス

トの設定を編集することで、機器ごとにネットワーク接続を制御できます。また、利用開始日時と利用終了日時を指定することで、期間を指定してネットワーク接続を制御することもできます。

ヒント

管理用サーバ、中継システム、および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、利用期間を指定できません。

ヒント

発見された機器を管理対象または除外対象にすると、ネットワーク制御リストの設定が自動的にネットワーク接続を許可するように変更されます。これは、その機器が組織内の機器であることを確認できたと見なされるためです。

重要

ルータ、プリンタ、サーバなどの業務上重要な機器については、ネットワーク制御リストの自動更新によって機器が遮断されないよう、ネットワーク制御リストに、その機器の IP アドレスを手動で登録することを推奨します。 この際、MAC アドレスを入力すると、機器情報の更新によってネットワーク制御リストから削除されるおそれがあるため、[MAC アドレス] 欄を空白にしてください。ネットワーク制御リストの自動更新については、「2.8.15 ネットワーク制御リストの自動更新」を参照してください。

ヒント

ネットワーク制御リストの機器情報を新規登録したり、編集したりすると、編集した機器の [マーク] 欄にチェックが表示されます。これは、機器が意図せずに接続許可されたり、遮断されたりすることがないように注意する必要がある目印です。 管理者は [マーク] 欄にチェックが表示されている機器を確認し、問題がなければチェックを解除してください。なお、チェックはいつでも解除できます。

ネットワーク制御リストの管理については、「2.8.8　ネットワーク制御リストの管理」を参照してください。

機器のネットワーク接続の可否は、ネットワークモニタ設定とネットワーク制御リストによって管理されます。これらの設定を組み合わせることで、次のようなネットワーク制御ができます。

- 新規に接続する機器のネットワーク接続は許可するが、ネットワーク制御リストに登録した特定の機器のネットワーク接続は許可しない（ブラックリスト方式）

  ネットワークモニタの設定の［発見した機器への動作］では、［ネットワークへの接続を許可する］を選択してください。この場合、新規機器をネットワークに追加すると、ネットワークへの接続を遮断されることなく運用できます。

- ネットワーク制御リストに登録した機器だけネットワーク接続を許可して、それ以外で新規に接続する機器のネットワーク接続を許可しない（ホワイトリスト方式）

ネットワークモニタの設定の［発見した機器への動作］では、［ネットワークへの接続を許可しない］を選択してください。

この場合で、新規機器のネットワーク接続を自動的に許可させたいときは、セキュリティポリシーの［アクション項目］－［ネットワーク接続制御］で、危険レベルが「安全」と判定された機器の接続を許可するように設定してください。新規機器は、管理用サーバに接続した時点ではネットワーク接続が遮断された状態になりますが、セキュリティ判定が実施されて危険レベルが「安全」と判定されると、ネットワークに接続できるようになります。

遮断された機器の特例接続

ネットワークモニタの機能によってネットワークから遮断された機器は、そ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なコンピュータ、および［ネットワークへの接続を許可しない機器の特例接続］に登録されたコンピュータとだけ通信できます。遮断中の機器の通信については、「2.8.13　遮断中に接続できる機器の登録」を参照してください。

なお、組織内のネットワーク環境によっては、特例接続の設定が必須となる場合があります。特例接続の設定が必須となる場合と、それに対応する［ネットワークへの接続を許可しない機器の特例接続］の設定例を次に示します。

特例接続の設定が必須となる場合	説明	［ネットワークへの接続を許可しない機器の特例接続］の設定例
DNS サーバを使用して組織内の機器の名前解決をしている	DNS サーバを使用して組織内の機器の名前解決をしている場合は、DNS サーバの IP アドレスを［ネットワークへの接続を許可しない機器の特例接続］に設定してください。DNS サーバの IP アドレスが設定がされていないと、［ネットワークへの接続を許可しない機器の特例接続］にほかの IP アドレスが設定されていても、機器の名前解決に失敗するため、ネットワークから遮断された機器が特例接続する際にホスト名によるネットワーク接続ができなくなります。	• 接続先 IP アドレス：DNS サーバの IP アドレス • プロトコル：指定なし • 接続先ポート番号：指定なし • 接続元 IP アドレス：指定なし • 接続元ポート番号：指定なし
組織内に NetBios ブロードキャストで名前解決をしている機器がある	組織内に NetBios ブロードキャストで名前解決をしている機器がある場合は、ブロードキャストアドレスを［ネットワークへの接続を許可しない機器の特例接続］に設定してください。ブロードキャストアドレスが設定がされていないと、機器の名前解決に失敗するため、ネットワークモニタを有効にしている機器とホスト名によるネットワーク接続ができなくなります。	• 接続先 IP アドレス：ブロードキャストアドレス（例：192.168.1.255） • プロトコル：UDP • 接続先ポート番号：137 • 接続元 IP アドレス：指定なし • 接続元ポート番号：指定なし
ネットワークモニタを有効にしている機器が DHCP サーバである※	ネットワークモニタを有効にしている機器が DHCP サーバである場合は、IP アドレス「0.0.0.0」を［ネットワークへの接続を許可しない機器の特例接続］に設定してください。「0.0.0.0」が設定されていないと、IP アドレスの割り当てに失敗するため、IP アドレスが	• 接続先 IP アドレス：0.0.0.0 • プロトコル：UDP • 接続先ポート番号：68

特例接続の設定が必須となる場合	説明	[ネットワークへの接続を許可しない機器の特例接続] の設定例
ネットワークモニタを有効にしている機器が DHCP サーバである※	割り当てられていない機器のネットワーク接続ができなくなります。	• 接続元 IP アドレス：サブネットマスクを CIDR 形式で指定する（例：255.255.255.0/24） • 接続元ポート番号：67

注※　DHCP サーバが IP アドレスを自動的に割り当てることができます。ただし、Windows 環境にネットワークモニタを導入した場合、ネットワークモニタの導入時に有効になっているサービス「Routing and RemoteAccess Service」の、RemoteAccess 機能（着信接続）が IP アドレス 10 個分を確保してしまうため、割り当てできる IP アドレスが 10 個分少なくなってしまいます。次の OS の場合、この現象は、RemoteAccess 機能を停止することで回避できます。

- Windows Server 2019
- Windows Server 2016
- Windows 8.1
- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008 R2

RemoteAccess 機能を停止する手順を次に示します。

1. 管理者権限でコマンドプロンプトを開きます。
2. コマンドプロンプトで`netsh ras show type` コマンドを実行します。
3. コマンドプロンプトで「IPv4 リモートアクセスサーバー」が「有効」と表示されることを確認します。
4. RemoteAccess 機能を停止させるため、コマンドプロンプトで次のコマンドを実行します。

```
netsh ras set type ipv4rtrtype = lanonly ipv6rtrtype = none rastype = none
```

5. サービス「Routing and RemoteAccess Service」を再起動します。
6. コマンドプロンプトで`netsh ras show type` コマンドを実行します。
7. コマンドプロンプトで「IPv4 リモートアクセスサーバー」が「無効」と表示されることを確認します。

関連リンク

- 2.8.10　ホワイトリスト方式を利用した機器のネットワーク接続の管理
- 2.8.9　ブラックリスト方式を利用した機器のネットワーク接続の管理

2.8.3　ネットワーク監視時の注意事項

- ネットワークモニタを有効にしたコンピュータの IP アドレスの変更やコンピュータの滅却をしたり、監視するネットワークを追加したりする場合、事前に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設定の割り当て］画面でネットワークモニタを無効にしたあとで、IP アドレスの変更や監視するネットワークの追加をして、再度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を有効にしたコンピュータを無効にする前に、コンピュータをネットワークから外した場合、ネットワークモニタを無効にすることができなくなります。この場合、コンピュータをネットワークに再接続してネットワークモニタを無効にしたあとで、ネットワークからコンピュータを外してください。
- ネットワークモニタを有効にしたコンピュータまたは JP1/IT Desktop Management 2 - Network Monitor をインストールしたコンピュータでは、Windows ファイアウォールが自動で無効になります。Windows ファイアウォールは無効の状態のままお使いください。Windows ファイアウォールまたはセキュリティ製品などのファイアウォール機能を有効にすると、［ネットワークへの接続を許可しない機器の特例接続］で指定した通信が、遮断されるおそれがあります。
- ネットワークモニタを有効にしたコンピュータまたは JP1/IT Desktop Management 2 - Network Monitor をインストールしたコンピュータでは、「Routing and Remote Access」サービスを使用します。そのため、「Routing and Remote Access」サービスを停止しないでください。また、Windows Server 2012 および Windows Server 2008 R2 の場合は、Windows の役割サービス「ルーティングとリモートアクセスサービス」も無効にしないでください。

  なお、ネットワークモニタを有効にしていた機器のネットワークは、次のタイミングで遮断されることがあります。その場合、「Routing and Remote Access」サービスを停止するか、またはコンピュータを再起動してください。

  - ネットワークモニタを無効にしたあと
  - JP1/IT Desktop Management 2 - Network Monitor をアンインストールしたあと
- ネットワークモニタを有効にしたコンピュータは、有線 LAN での接続を推奨します。 無線 LAN で接続した場合、通信環境が劣化したときに、不正なコンピュータの LAN 接続の検出や排除ができないことがあります。
- ネットワーク接続が遮断された機器が特例接続に設定した機器と通信をするとき、 遮断された機器とネットワークモニタを有効にしたコンピュータ（監視用のコンピュータ）が通信する必要があります。このため、監視用のコンピュータは特例接続のリストに入っていなくても、遮断された機器との通信ができるようになっています。 ファイルサーバなど業務上重要なサーバと監視用のコンピュータを併用しないでください。併用すると、セキュリティ対策が不十分な機器から接続され、監視用のコンピュータ自体のセキュリティが不十分になるなどのおそれがあります。
- ネットワーク接続が遮断された機器に対して、ネットワーク接続を許可しても、ネットワークに接続できるようになるまで数分掛かることがあります。数分経過してもネットワークに接続できない場合は、利用者のコンピュータを再起動してください。
- ネットワークモニタが DHCP サーバを用いて動的に IP アドレスを割り当てるネットワークを監視した場合、DHCP サーバは不正接続のコンピュータにリースしようとした IP アドレスを一定時間使用中と

して管理します。このため、ネットワークモニタがその時間内に多数の不正接続のコンピュータを遮断した場合は、管理している使用できる IP アドレスが少なくなることがあるので、遮断したコンピュータを速やかにネットワークから取り除いてください。

- 特定の仮想ネットワークアダプタが搭載された機器に対してネットワークモニタを有効にすると、ネットワークモニタの初期設定が正常に実行されず、ネットワーク制御ができない場合があります。

  次に示す仮想ネットワークアダプタが搭載されている機器では、これら仮想ネットワークアダプタを無効にしたうえで、ネットワークモニタを有効にしてください。

  - Microsoft Wi-Fi Direct Virtual Adapter
  - Microsoft Failover Cluster Virtual Adapter

2.8.4 ネットワークモニタの動作状態の表示

ネットワークを監視しているとき、どのネットワークセグメントが監視対象になっているかをアイコンで確認できます。ネットワークモニタの動作状態には、次の種類があります。

 ：ネットワークモニタが有効です

ネットワークは監視されています。ネットワークセグメント内のコンピュータのネットワークモニタが有効になっています。

 ：ネットワークモニタを有効化しています

ネットワークは監視されていません。ネットワークセグメント内のコンピュータのネットワークモニタを有効にしています。

 ：ネットワークモニタの有効化に失敗しました

ネットワークは監視されていません。ネットワークモニタの有効化に失敗しています。

 ：ネットワークモニタが無効です

ネットワークは監視されていません。ネットワークセグメント内のコンピュータで、ネットワークモニタが無効になっています。

 ：ネットワークモニタを無効化しています

ネットワークは監視されています。ネットワークセグメント内のコンピュータで有効になっていたネットワークモニタを無効にしています。

 ：ネットワークモニタの無効化に失敗しました

ネットワークは監視されています。ネットワークモニタの無効化に失敗しています。

ネットワークモニタの動作状態は、次の画面で確認できます。

- 機器画面の［機器情報］－［機器一覧（ネットワーク）］画面のメニューエリア
- セキュリティ画面の［機器のセキュリティ状態］－［機器一覧（ネットワーク）］画面のメニューエリア

- 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］画面のインフォメーションエリア

2.8.5　監視用のコンピュータを変更する手順

リプレースや用途の変更などによって、ネットワークモニタを有効にするコンピュータを変更したい場合は、いったんネットワークモニタを無効にしてから、ほかのコンピュータでネットワークモニタを有効にします。

監視用のコンピュータを変更するには：

1. 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と、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、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無効です」になります。このとき、一時的にネットワークの監視が解除されます。

2. 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無効にしたら、監視用にする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することで、そのコンピュータを含むネットワークセグメントが監視されるようになります。

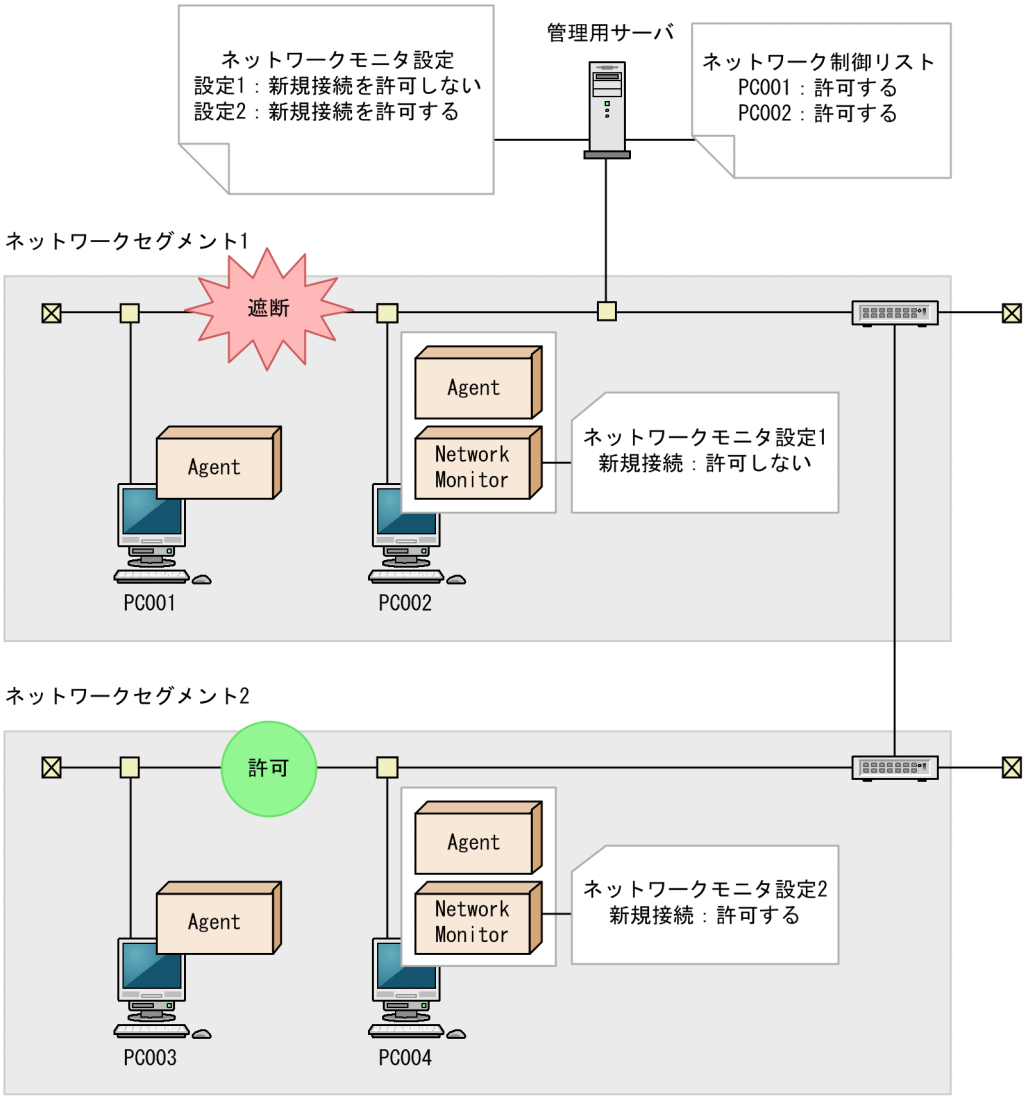
2.8.6　ネットワークモニタ設定による制御

ネットワークモニタを有効にすると、そのコンピュータを含むネットワークセグメント内の機器のネットワーク接続を許可するかどうかを制御できます。ネットワークセグメントごとにネットワーク接続の制御方法を変更するには、ネットワークモニタ設定を各ネットワークセグメントに割り当てる必要があります。

ネットワークモニタ設定を複数作成して割り当てることで、セキュリティを強化したいネットワークセグメントは新規機器の接続を許可しないで、それ以外はネットワーク接続を許可するといった運用ができます。

複数サーバ構成の場合、ネットワークモニタの有効化、無効化、およびネットワークモニタ設定の割り当ては、各管理用サーバ直下のネットワークセグメント内のコンピュータだけに実施できます。

ネットワークモニタ設定の割り当ての概念を次の図に示します。



（凡例）

Agent：JP1/IT Desktop Management 2 - Agent

Network Monitor：ネットワークモニタエージェント

ネットワークセグメントごとにネットワーク接続の設定を変更したい場合は、複数のネットワークモニタ設定を作成してください。ネットワークモニタ設定は、設定画面の［ネットワーク制御］－［ネットワーク制御の設定］画面で作成できます。

作成したネットワークモニタ設定は、各ネットワークセグメントに割り当てる必要があります。ネットワークモニタ設定は、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］画面で割り当てられます。

重要

ネットワークの探索で発見した機器に自動でエージェントを配信するように設定している場合、発見されたコンピュータがネットワーク接続を許可されなくても、そのコンピュータにエージェントは配信されます。

このため、ネットワーク接続が許可されないコンピュータにエージェントが導入された場合、セキュリティポリシーのネットワーク制御の設定およびセキュリティの判定結果によっては、そのコンピュータがネットワーク接続できてしまうことがあります。

重要

複数サーバ構成の場合、同じネットワークセグメント内に管理元の異なるコンピュータを混在させないでください。それぞれの管理元が割り当てたネットワークモニタ設定が競合して、ネットワーク接続を正常に制御できなくなるおそれがあります。

ヒント

ネットワークモニタ設定が許可する/許可しないのどちらの設定でも、ネットワーク接続した機器を発見できます。ネットワークモニタによって発見された機器には、自動的にネットワークの探索が実行されます。このため、ネットワークの探索で、自動的に管理対象とする、またはエージェントを自動配信するよう設定されている場合は、ネットワークモニタによって機器が発見されると、自動的に管理対象になるか、エージェントが自動配信されます。この場合、機器が管理対象になって、製品ライセンスが消費されます。

自動で管理対象にしたくない場合は、探索条件の設定で［自動的に管理対象とする］および［エージェントを自動配信する］のチェックを外して、手動で管理対象にするようにしてください。

2.8.7　ネットワークモニタ設定の管理

ネットワークモニタを設定すると、ネットワークセグメントごとにネットワークを制御できます。

ネットワークモニタ設定は、デフォルトでネットワークへの接続を許可する「(標準設定)」、ネットワークへの接続を許可しない「許可しない設定」、ネットワークへの接続を許可しネットワーク接続を遮断しない「標準設定（遮断しない)」、およびネットワークへの接続は許可しないがネットワーク接続を遮断しない「許可しない設定（遮断しない)」が提供されます。複数のネットワークモニタ設定を使い分ける必要がない場合は、「(標準設定)」をすべてのセグメントに割り当てることで、一括して設定を変更できます。

メモ

ネットワークモニタ設定のデフォルト設定「標準設定（遮断しない)」と「許可しない設定（遮断しない)」は、管理用サーバの新規構築時および再構築時に提供されます。アップグレード時には提供されません。

ネットワークセグメントごとにネットワークモニタ設定を分けたい場合は、ネットワークモニタ設定を作成します。

ネットワーク接続の制御方法を変更する場合、ネットワークモニタ設定を編集します。

運用状況の変更に伴ってネットワークモニタ設定が不要になった場合、ネットワークモニタ設定を削除します。

なお、ネットワークモニタ設定は、作成後にネットワークセグメントごとに割り当てる必要があります。

ネットワークモニタ設定を管理する方法の詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の、ネットワークモニタ設定を管理する方法の説明を参照してください。

ヒント

ネットワークモニタ設定を作成する時に、[ネットワーク制御] − [ネットワーク制御の設定] − [ネットワークモニタ設定の追加] 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。

デフォルトで提供されるネットワークモニタ設定の「標準設定（遮断しない)」と「許可しない設定（遮断しない)」は、[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] がチェックされています。

2.8.8 ネットワーク制御リストの管理

ネットワーク制御リストでは、機器ごとにネットワーク接続を制御できます。また、ネットワーク接続を許可する期間を指定することもできます。なお、発見された機器は、自動的にネットワーク制御リストに登録されます。手動で登録したい場合は、必要に応じて管理者が機器の情報を追加してください。

機器ごとにネットワーク接続を制御したい場合は、機器をネットワーク制御リストに追加します。

機器ごとにネットワーク接続の制御を変更する場合は、すでに登録されている機器の設定を編集します。

手動でネットワーク制御リストに登録した機器、および複数サーバ構成の場合でネットワーク制御リストの自動更新の対象範囲に含まれていない機器は、ネットワーク制御リストから削除することもできます。

また、ネットワーク制御リストに設定されているネットワーク接続可否の情報は、操作画面からエクスポートおよびインポートできます。

ネットワーク制御リストを管理する方法の詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の、ネットワーク制御リストを管理する方法の説明を参照してください。

ヒント

ネットワークモニタ設定とネットワーク制御リストの設定を組み合わせることで、ネットワーク接続の制御をホワイトリスト方式で運用したり、ブラックリスト方式で運用したりできます。

ヒント

ネットワーク制御コマンド（jdnrnetctrl コマンド）を実行することで、管理用サーバのネットワーク制御リストを更新できます。

ヒント

- ［ネットワーク制御リストの自動更新］ダイアログで［すべての自動更新を有効にする］をチェックした場合で、ネットワークへの接続を「許可する」に設定した機器を削除したときは、使いまわしを防ぐためにネットワーク制御リストからも機器の情報が削除されます。また、ネットワークへの接続を「許可しない」に設定した機器を削除したときは、機器が変わっても「許可しない」設定を引き継ぐよう、ネットワーク制御リストに機器の情報が残ります。
- ［ネットワーク制御リストの自動更新］ダイアログで［すべての自動更新を有効にする］をチェックしない（自動更新のうち追加だけを有効）場合は、ネットワークへの接続を「許可する」または「許可しない」の設定に関係なく、機器を削除したときは、機器が変わってもネットワーク制御リストに機器の情報が残ります。

重要

MAC アドレスが入力されている機器は、その機器の機器情報が通知された際に機器情報と関連づけられ、ネットワーク制御リストの一覧にホスト名などの情報が表示されるようになります。 機器と関連づけられたリストは、ネットワーク制御リストの画面からは削除できなくなりますので、不要になった場合は設定画面から機器自体を削除してください。

ヒント

ネットワーク制御リストの機器情報を新規登録したり、編集したりすると、編集した機器の［マーク］欄にチェックが表示されます。これは、機器が意図せずに接続許可されたり、遮断されたりすることがないように注意する必要がある目印です。 管理者は［マーク］欄にチェックが表示されている機器を確認し、問題がなければチェックを解除してください。なお、チェックはいつでも解除できます。

関連リンク

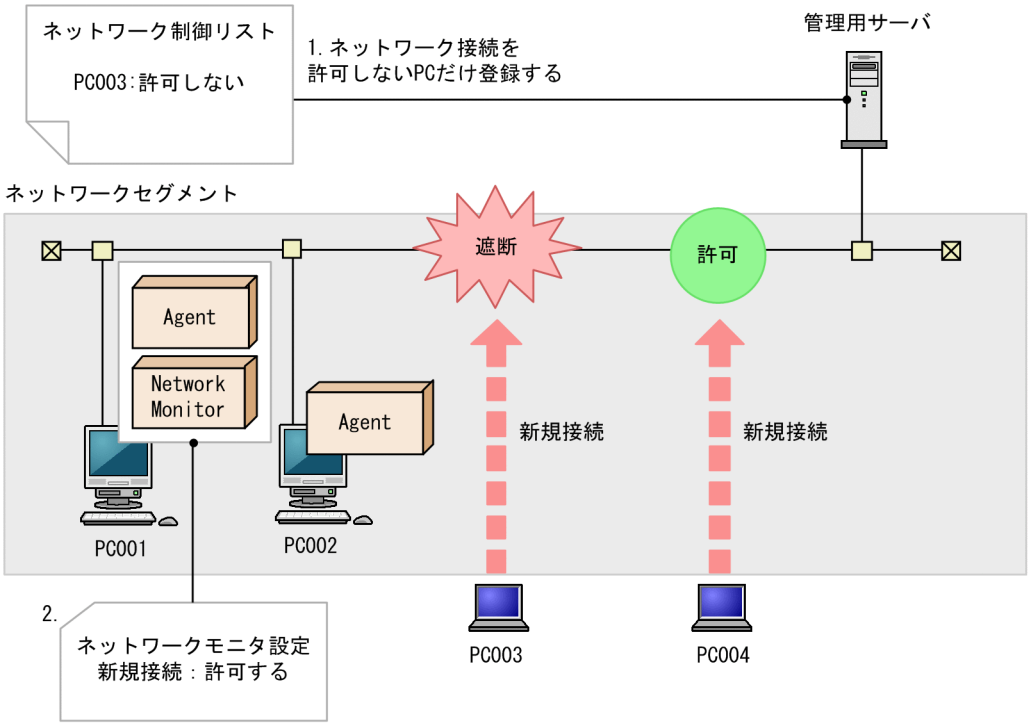
- 2.8.9　ブラックリスト方式を利用した機器のネットワーク接続の管理
- 2.8.10　ホワイトリスト方式を利用した機器のネットワーク接続の管理

2.8.9　ブラックリスト方式を利用した機器のネットワーク接続の管理

ネットワーク接続を許可しない機器を一覧に登録する「ブラックリスト方式」でネットワーク接続を管理できます。スタンドアロンで使用する必要があるコンピュータや、組織内に持ち込まれていた個人用のコンピュータなど、ネットワークに接続させたくない機器が特定されているときは、ブラックリスト方式で管理することをお勧めします。

> **ヒント**
>
> ネットワークの監視を始めたばかりのときは、ネットワーク接続を許可するコンピュータが多く、管理に手間が掛かります。そのようなときは、全体のネットワーク接続を許可したあとに、ネットワーク接続を許可しないコンピュータを登録して、ブラックリスト方式で管理すると便利です。

ブラックリスト方式の管理について、次の図に示します。



（凡例）

Agent：JP1/IT Desktop Management 2 - Agent

Network Monitor：ネットワークモニタエージェント

1.接続を許可しない機器を登録する

設定画面の［ネットワーク制御］－［ネットワーク制御リストの設定］画面で、接続を許可しない機器を登録して、ネットワーク接続を許可しないように設定します。ネットワーク制御リストの設定方法については、「2.8.8　ネットワーク制御リストの管理」を参照してください。

2.すべての機器のネットワーク接続を許可する

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、すべてのネットワークセグメントに対して、ネットワーク接続を許可する設定のネットワークモニタ設定を割り当てます。ネットワークモニタ設定の詳細については、「2.8.7　ネットワークモニタ設定の管理」を参照してください。

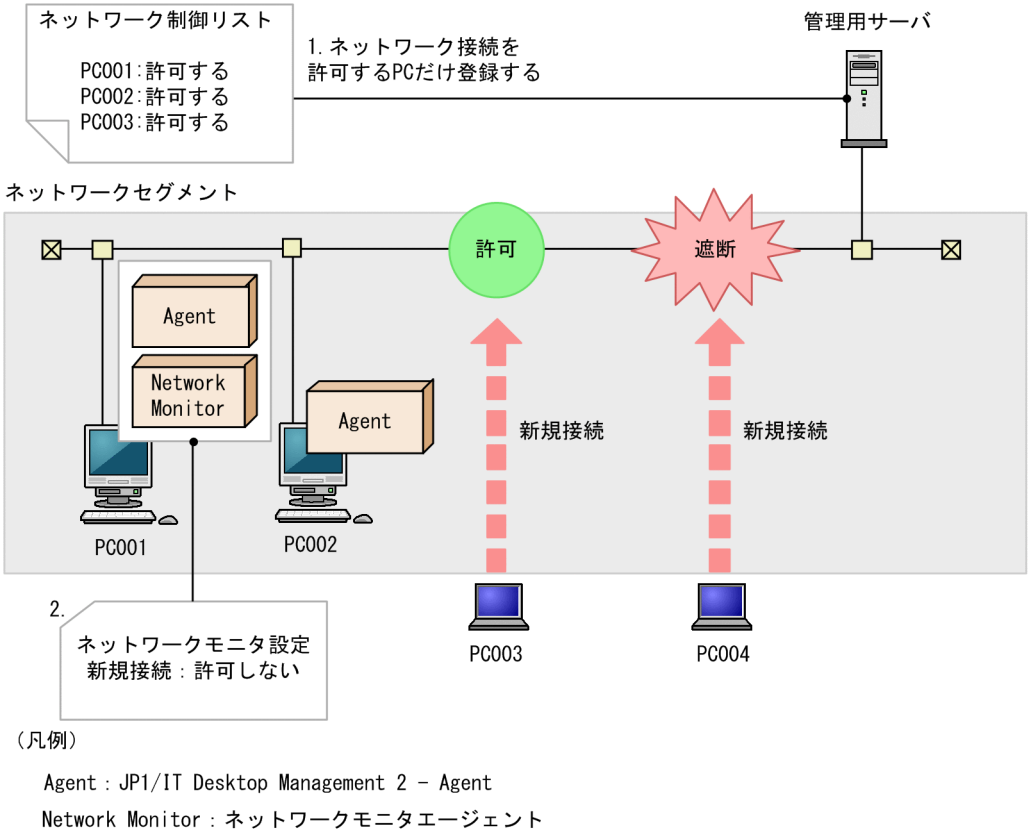
これによって、手順 1 で登録した機器だけネットワーク接続が遮断されるようになります。

許可しない機器がネットワークに接続しようとすると、遮断されるようになります。また、未許可の機器のネットワーク接続を遮断したイベントも出力されます。

2.8.10　ホワイトリスト方式を利用した機器のネットワーク接続の管理

ネットワーク接続を許可する機器を一覧に登録して、それ以外の機器のネットワーク接続を許可しない「ホワイトリスト方式」で、ネットワーク接続を管理できます。より強固なネットワークセキュリティを実現したい場合は、ホワイトリスト方式で管理することをお勧めします。

ホワイトリスト方式の管理について、次の図に示します。



1.接続を許可する機器を登録する

設定画面の［ネットワーク制御］－［ネットワーク制御リストの設定］画面で、接続を許可する機器を登録します。管理用サーバ、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な

ど、常にネットワークに接続させておく必要がある機器は必ず登録してください。なお、機器を発見すると、ネットワーク制御リストに自動的に登録されます。ネットワーク制御リストの設定の詳細については、「2.8.8　ネットワーク制御リストの管理」を参照してください。

2.ネットワーク制御リストに登録していない機器のネットワーク接続を遮断する

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、すべてのネットワークセグメントに対して、ネットワーク接続を許可しない設定のネットワークモニタ設定を割り当てます。これによって、ネットワーク制御リストに登録していない機器がネットワーク接続しようとすると、遮断されます。ネットワークモニタ設定の詳細については、「2.8.7　ネットワークモニタ設定の管理」を参照してください。

許可した機器だけがネットワークに接続できるようになります。未許可の機器がネットワーク接続すると自動的に遮断され、遮断したイベントが出力されます。

ヒント

設定画面の［ネットワーク制御］画面で、新規機器の接続を許可しない設定になっている場合、新規機器がネットワークへ接続しようとすると、遮断されます。この場合に、新規のコンピュータを自動的にネットワーク接続させるためには、コンピュータにエージェントを導入して、セキュリティポリシーの［アクション項目］－［ネットワーク接続制御］ で接続を許可する危険レベルを設定してください。 エージェント導入済みコンピュータがネットワークに接続されると、セキュリティ状況の判定結果に応じてネットワーク接続が制御されます。このとき、接続が許可されると、自動的にネットワーク制御リストに登録されます。

重要

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、ルータ、スイッチ、ネットワークプリンタなど、JP1/IT Desktop Management 2 が管理対象としない機器に対しても、ネットワーク接続を許可するように登録してください。特に、ルータやスイッチなどのネットワーク装置が接続を許可するよう設定されていないと、その配下に接続された機器もネットワークに接続できないため、注意してください。

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は、必要に応じてネットワーク制御リストの自動更新の設定を変更してください。デフォルトでは、自動更新のうち追加だけを有効にする設定になっています。

ネットワーク接続デバイス（NIC など）の使い回しを自動で防止したい場合は、すべての自動更新を有効にしてください。ただし、次に示すときは、ネットワーク接続デバイス（NIC など）を外したと見なされ、ネットワーク制御リストから該当する機器が削除されるため、ネットワークに接続できなくなります。

- ネットワークの無効化（マイネットワークからローカルエリア接続などを無効化に設定する）をしたとき
- 機器からネットワークケーブルを外したとき

- 無線 LAN カードを外したとき

2.8.11　ネットワーク制御リストが更新されるタイミング

ネットワーク制御リストが更新されるタイミングを次の表に示します。

項番	更新のタイミング	具体例	備考
1	ネットワークモニタによる機器の接続検知	ネットワークモニタ機能でネットワークを監視し、機器の接続が検知される。	機器をネットワークに接続したあとすぐに切断するなどの操作をした場合、接続を検知しても IP アドレスや MAC アドレスなどの情報を取得できないため、ネットワーク制御リストに情報を追加できないことがあります。
2	機器の探索による接続機器の発見	機器の探索で、ネットワークに接続している機器が発見される。	－
3	管理対象機器の追加・削除	• 機器画面の［機器情報］－［機器一覧］画面で機器を削除する。 • 設定画面の［機器の探索］－［発見した機器］画面で機器を管理対象にする。 • 設定画面の［機器の探索］－［発見した機器］画面で機器を除外対象にする。 • 設定画面の［機器の探索］－［発見した機器］画面で機器を削除する。 • 設定画面の［機器の探索］－［管理対象機器］画面で機器を除外対象にする。 • 設定画面の［機器の探索］－［管理対象機器］画面で機器を削除する。 • 設定画面の［機器の探索］－［除外対象機器］画面で機器を管理対象にする。 • 設定画面の［機器の探索］－［除外対象機器］画面で機器を削除する。 • 設定画面の［機器］－［機器メンテナンスの設定と検出結果確認］画面の［削除候補の機器一覧］で機器を削除する。	• 管理対象にした機器の機器情報が収集できる状態のときに、その機器が複数のネットワーク接続デバイス（NIC など）を持つ場合は、それらのデバイスもネットワーク制御リストへ追加します。 • 通常は、ネットワークモニタまたは機器の探索で機器を発見した時点でネットワーク制御リストに追加します。この場合、該当機器が手入力によって削除されていないかぎり、管理対象機器の追加・削除のタイミングでのネットワークリストへの追加はありません。 • ホワイトリスト方式で運用している環境では、エージェントをインストールしたコンピュータを管理対象にしても、そのコンピュータのネットワーク接続は許可されません。自動的に許可されるようにする場合は、［セキュリティポリシーの追加］ダイアログまたは［セキュリティポリシーの編集］ダイアログの［アクション項目］－［ネットワーク接続制御］で、ネットワーク接続が許可されるように設定しておいてください。
4	ネットワーク接続デバイス（NIC）などの変更	• 管理対象機器でネットワーク接続デバイス（NIC など）を追加・削除する。	管理対象の機器から機器情報を収集できる状態で、ネットワーク接続デバイス（NIC など）の構成・設定に変更がある場

項番	更新のタイミング	具体例	備考
4	ネットワーク接続デバイス（NIC）などの変更	• 管理対象機器のネットワーク接続デバイス（NIC など）に設定している IP アドレスを変更する（DHCP 環境で IP アドレスが変更される場合も含む）。	合、その変更内容をネットワーク制御リストへ反映します。
5	手入力でのネットワーク接続可否の設定	• 機器画面の［機器情報］－［機器一覧］画面で、「接続を許可する」、または 「接続を許可しない」に設定する。 • セキュリティ画面の［機器のセキュリティ状態］－［機器一覧］画面で、「接続を許可する」、または「接続を許可しない」に設定する。	設定した内容がネットワーク制御リストの［ネットワークへの接続］の設定 （許可する/しない）へ反映されます。
6	セキュリティ判定によるネットワーク接続の自動制御	セキュリティ画面の［セキュリティポリシー］－［セキュリティポリシー一覧］画面で任意に選択したセキュリティポリシーの［セキュリティポリシーの編集］画面で、［アクション項目］－［ネットワーク接続制御］の設定が有効、かつ［接続制御の対象とする危険レベル］が設定されているセキュリティポリシーが割り当たっている機器に対するネットワーク制御が実行される。	セキュリティポリシーの設定によっては、自動的にネットワークへの接続可否を設定します。その自動設定の内容が、ネットワーク制御リストの［ネットワークへの接続］の設定（許可する/しない）へ反映されます。
7	ハードウェア資産の新規登録・変更・滅却	• IP アドレスまたは MAC アドレスが入力されたハードウェア資産を新規追加する 。 • ハードウェア資産の IP アドレスまたは MAC アドレスを変更する。 • ハードウェア資産の［資産状態］を「滅却」にする。	• 機器と関連づいていないハードウェア資産の場合です。機器と関連づいている場合は、機器の情報を反映します。 • 手入力での情報の追加・変更・削除と同じ扱いになります。
8	ネットワーク制御リストの手入手による追加・変更・削除	設定画面の［ネットワーク制御］－［ネットワーク制御リストの設定］画面で、手入力でデータ追加・変更・削除を実行する。	機器やハードウェア資産と関連づいたネットワーク制御リストのデータは、機器、ハードウェア資産、ネットワーク制御リストのどれかに対する最後の変更内容（自動・手入力の両方を含む）を反映します。このため、自動的に変更されるケースに注意してください。
9	配下の管理用中継サーバからの機器情報の通知	複数サーバ構成の場合に、配下の管理用中継サーバが追加・変更・削除した機器情報に基づいて、ネットワーク制御リストを自動更新する。	複数サーバ構成の場合、かつ設定画面の［ネットワーク制御］－［ネットワーク制御リストの設定］画面で、配下の管理用中継サーバが管理している機器を自動更新の対象としている必要があります。
10	CSV ファイルからのネットワーク接続可否の情報のインポート	設定画面の［ネットワーク制御］－［ネットワーク制御リストの設定］画面の［操作メニュー］から、CSV ファイルをインポートする。	－
11	ネットワーク制御コマンド（jdnrnetctrl コマンド）の実行	ネットワーク制御コマンド（jdnrnetctrl コマンド）を実行する。	－

（凡例）－：該当なし

> **重要**
>
> 管理用サーバの負荷が高い状態のときは、ネットワーク制御リストが更新されてからリストの内容が実際に反映されるまで時間が掛かることがあります。

2.8.12　ネットワーク制御リストの設定

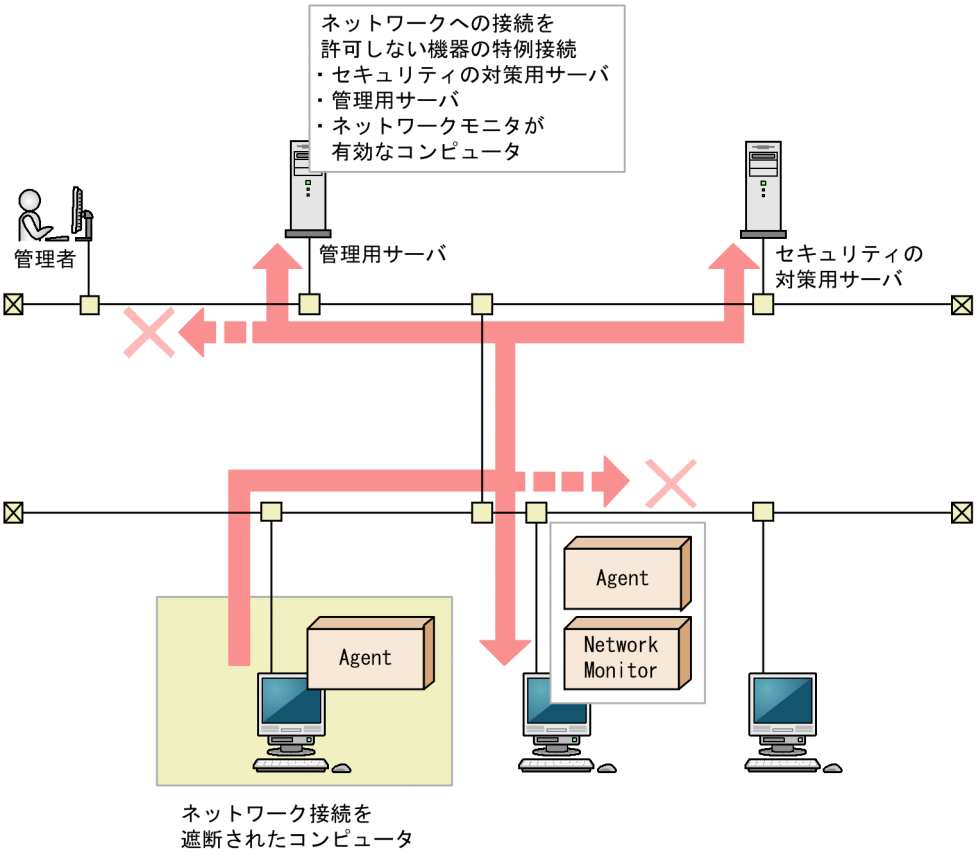
機器の運用方法ごとに必要なネットワーク制御リストの設定を次の表に示します。

機器の運用	ネットワーク制御リストの設定
IP アドレスを固定して機器を運用している場合	すべての NIC の MAC アドレスおよび IP アドレスをリストに登録します。判定形式は任意です。
DHCP 環境で機器を運用している場合	判定形式を「MAC アドレス」に設定します。
1 つの MAC アドレスに複数の IP アドレスを割り当てている場合	判定形式を「MAC アドレス」に設定します。
NIC のチーミングを利用する場合	仮想 MAC アドレスをリストに登録します。
クラスタ環境の場合	物理 IP アドレスおよび論理 IP アドレスをそれぞれリストに登録します。
1 つの NIC を複数の機器で利用する場合	対応する IP アドレスを次の形式でリストに登録します。 • 判定形式：「IP アドレス」 • MAC アドレス：入力しない • IP アドレス：対象の IP アドレス
次の機器のホスト識別子が重複しているおそれがある場合 • プリンタ • ネットワーク機器 • ディスクコピーによってエージェントを導入した機器	

2.8.13　遮断中に接続できる機器の登録

ネットワークモニタの機能によってネットワークから遮断された機器は、そ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なコンピュータ、および［ネットワークへの接続を許可しない機器の特例接続］に登録されたコンピュータとだけ通信できます。［ネットワークへの接続を許可しない機器の特例接続］には、管理用サーバおよび中継システムが自動的に登録されます。

例えば、セキュリティの対策用サーバを［ネットワークへの接続を許可しない機器の特例接続］に追加すると、セキュリティ状況が危険と見なされてネットワーク接続が遮断された機器でも、セキュリティの対策用サーバへ接続してセキュリティ対策を実行できます。セキュリティの対策用サーバを［ネットワークへの接続を許可しない機器の特例接続］に登録した場合の例を次の図に示します。



（凡例）

：ネットワーク接続を遮断されたコンピュータから通信できる

：ネットワーク接続を遮断されたコンピュータから通信できない

Agent：JP1/IT Desktop Management 2 - Agent

Network Monitor：ネットワークモニタエージェント

［ネットワークへの接続を許可しない機器の特例接続］には、検疫中の機器と通信しても問題がない、セキュリティ対策が万全なコンピュータを登録してください。

重要

セキュリティ判定結果に応じて機器のネットワーク接続を制御する場合、［ネットワークへの接続を許可しない機器の特例接続］から管理用サーバを削除しないでください。削除すると、機器のセキュリティ状況を判定できなくなり、判定結果に応じたネットワーク制御ができなくなります。誤って削除してしまった場合は、［ネットワークへの接続を許可しない機器の特例接続］に管理用サーバを手動で追加してください。

重要

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、［ネットワークへの接続を許可しない機器の特例接続］から管理用サーバおよび中継システムを削除しないでください。削除す

ると、配布できなくなります。誤って削除してしまった場合は、［ネットワークへの接続を許可しない機器の特例接続］に管理用サーバおよび中継システムを手動で追加してください。

ヒント

リモートコントロール機能を利用する場合、コントローラを利用するコンピュータを登録しておくと、遮断された機器に対してリモートコントロールできるようになります。

2.8.14　各種機能によるネットワーク接続の自動制御

ネットワークモニタが有効になっている場合、セキュリティポリシーの判定結果やハードウェア資産情報の登録などのタイミングで、ネットワーク接続を自動で制御できます。例えば、セキュリティポリシーに違反したコンピュータのネットワーク接続を自動で遮断して、対策が完了したあとで自動でネットワーク接続を許可するといった制御ができます。

ネットワーク接続の制御には優先度があります。ネットワーク接続を許可しないように、手動で設定しておくと、自動的にネットワーク接続が許可される契機でも、許可されません。そのため、ネットワークに接続してはいけないコンピュータがある場合は、自動的にネットワーク接続が許可されないように、手動で「許可しない」に設定してください。ネットワーク接続を手動で制御する方法については、「2.8.17　手動によるネットワーク接続の制御」を参照してください。

各種機能によってネットワーク接続が自動で変更される契機を次の表に示します。

ネットワーク接続が制御される契機	制御内容
セキュリティポリシーに違反したとき	セキュリティポリシーの［アクション項目］－［ネットワーク接続制御］で、特定の危険レベルの機器はネットワーク接続を許可しないように設定しておくと、セキュリティ状況の判定時に自動でネットワーク接続を遮断できます。なお、ネットワーク接続が遮断されていたコンピュータのセキュリティ状況が改善された場合は、セキュリティポリシーに遵守していると判断されて、ネットワーク接続が自動で許可されます。
ハードウェア資産を追加、または編集したとき	資産画面の［ハードウェア資産］画面で、IP アドレスまたは MAC アドレスを含むハードウェア資産を追加すると、ネットワーク制御リストにその機器が登録されます。また、資産情報の IP アドレスと MAC アドレスを編集すると、変更内容がネットワーク制御リストに反映されます。ハードウェア資産情報をインポートした場合も同様にネットワーク接続が許可されます。 ハードウェア資産と機器が関連づいている場合、IP アドレスおよび MAC アドレスは機器から収集されるため、ハードウェア資産情報を編集してもネットワーク制御リストには反映されません。 なお、ハードウェア資産の資産状態を「滅却」にするか、ハードウェア資産情報を削除すると、対応するネットワーク制御リストの設定は削除されます。 ハードウェア資産情報の MAC アドレスを編集した場合、すでに同じ MAC アドレスのネットワーク制御の設定が存在しているときは、ネットワーク制御リストに編集内容は反映されません。 自動更新のうち追加だけを有効にした場合、変更前のネットワーク制御の設定が残ったまま新しい設定が追加されます。残ったネットワーク制御の設定には「自動更新（追加のみ有効）の影響」の項目に［確認候補］が設定されます。

ネットワーク接続が制御される契機	制御内容
ハードウェア資産を追加、または編集したとき	自動更新を設定する方法については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のネットワーク制御リストの自動更新の設定を編集する手順の説明を参照してください。
ネットワーク接続の利用期間内になったとき	ネットワーク制御リストで、期間を指定してネットワーク接続を許可した場合、利用開始日時になると、対象のコンピュータのネットワーク接続が自動的に許可されます。なお、利用終了日時になると、その機器はネットワーク接続が自動的に許可されなくなります。
発見されたコンピュータを「管理対象」または「除外対象」に設定したとき	新規に発見されたコンピュータを管理対象または除外対象にすると、ネットワーク接続が自動的に許可されます。ネットワークセグメントへの接続が許可されていない場合でも、発見された機器を管理対象または除外対象にすることで、接続を許可できます。 ただし、探索で発見した機器を自動的に管理対象にする場合は、ネットワークモニタ設定に応じてネットワーク接続が制御されます。
新規機器がネットワークに接続されたとき	ネットワークセグメントにネットワークモニタ設定を割り当てておくと、新規機器がネットワークに接続されたときに、ネットワークモニタ設定の設定内容に従って自動でネットワーク接続が制御されます。
機器情報を更新または削除したとき	機器情報の更新によって、機器の MAC アドレスや IP アドレスの情報が更新されると、自動でネットワーク制御リスト※が更新されます。 自動更新のうち追加だけを有効にした場合、変更前のネットワーク制御の設定が残ったまま新しい設定が追加されます。残ったネットワーク制御の設定には「自動更新（追加のみ有効）の影響」の項目に［確認候補］が設定されます。 自動更新の設定を編集する方法については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のネットワーク制御リストの自動更新の設定を編集する手順の説明を参照してください。
ネットワーク接続デバイスの情報が変更されたとき	すべての自動更新を有効にした場合、次に該当するときは、そのネットワークアダプタの情報が削除されたと判断し、そのネットワークアダプタの MAC アドレスをネットワーク制御リストから削除します（ただし、「許可しない」で設定されていたときは、ネットワーク制御リストから削除しません）。 • ネットワークの無効化（マイネットワークからローカルエリア接続などを無効化に設定する）を行ったとき • 機器からネットワークケーブルを外したとき • 無線 LAN カードを外したとき 自動更新のうち追加だけを有効にした場合、変更前のネットワークアダプタの情報が残ったまま新しいネットワークアダプタの情報が追加されます。残ったネットワークアダプタの情報には「自動更新（追加のみ有効）の影響」の項目に［確認候補］が設定されます。 自動更新の設定を編集する方法については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のネットワーク制御リストの自動更新の設定を編集する手順の説明を参照してください。 頻繁にネットワークアダプタを無効にする機器がある場合は、次の内容でネットワーク制御リストに登録してください。 • 判定形式：IP アドレス • MAC アドレス：入力しない • IP アドレス：対象機器の IP アドレス • ネットワークへの接続：許可する そのほかの項目は任意で入力してください。

注※　ネットワーク制御リストの更新の内容については、「2.8.15　ネットワーク制御リストの自動更新」を参照してください。

重要

ネットワークモニタが無効の場合も、ネットワーク接続を許可するかどうかは変更されます。ただし、制御はされません。この場合、次にネットワークモニタが有効になったタイミングでネットワーク接続の変更が適用されます。

ヒント

ネットワーク接続が遮断または許可されると、イベントが出力されます。イベントをメール通知するように設定しておくと、ネットワーク接続が遮断または許可されたことをメールで確認できます。

関連リンク

- 2.9.4　セキュリティポリシーの管理
- 2.11.2　ハードウェア資産情報の管理
- 2.8.8　ネットワーク制御リストの管理

2.8.15　ネットワーク制御リストの自動更新

ハードウェア資産情報や機器情報を追加、更新または削除した場合、自動でネットワーク制御リストが更新されます。自動で行われる更新内容を次に示します。

- ネットワーク制御リストにない MAC アドレスや IP アドレスがハードウェア資産情報に含まれる場合、その MAC アドレスおよび IP アドレスの情報がネットワーク制御リストに追加されます。
- ハードウェア資産の資産状態を「滅却」にするか、ハードウェア資産情報を削除すると、対応するネットワーク制御リストの設定は削除されます。
- ハードウェア資産情報の IP アドレスと MAC アドレスを編集すると、変更内容がネットワーク制御リストに反映されます。ただし、ハードウェア資産と機器が関連づいている場合、IP アドレスおよび MAC アドレスは機器から収集されるため、ハードウェア資産情報を編集してもネットワーク制御リストには反映されません。また、すでに同じ MAC アドレスのネットワーク制御の設定が存在する場合も、ネットワーク制御リストには反映されません。
- ネットワーク制御リストにない MAC アドレスが機器情報に含まれる場合、その MAC アドレスおよび IP アドレスの情報がネットワーク制御リストに追加されます。機器情報を通知した機器がすでに管理用サーバに登録されている場合は、機器の許可状態に従って、次の表に示すようにネットワーク制御リストに追加されます。

機器の許可状態	制御リストの許可状態
許可	許可する
遮断	許可しない
強制遮断	許可しない
利用期間外	許可しない

機器情報を通知した機器が管理用サーバに登録されていない場合は、通知された IP アドレスが所属するネットワークグループに割り当てられたネットワークモニタの設定（発見した機器への動作）に従って、ネットワーク制御リストに登録する際の許可状態が設定されます。

ネットワークモニタ	発見した機器への動作	制御リストの許可状態
導入済み	許可する	許可する
	許可しない	許可しない
未導入		ネットワーク制御設定ファイル※の設定にしたがう

注※　ネットワーク制御設定ファイルの設定にしたがいます。デフォルトは「許可する」で登録されます。ネットワーク制御設定ファイルの設定方法については、マニュアル「JP1/IT Desktop Management 2 構築ガイド」のネットワーク制御設定ファイルを編集する手順の説明を参照してください。

- 前回の機器情報の収集時にあった MAC アドレスの情報が、機器情報からなくなっていた場合、ネットワークカードが抜かれたと見なして、ネットワーク制御リストからその MAC アドレスの情報が削除されます。 ネットワークの状態を無効にした場合も同様に、その MAC アドレスの情報がネットワーク制御リストから削除されます。
- 機器情報の IP アドレスが変更になった場合、［ネットワーク接続可否の追加］ダイアログまたは［ネットワーク接続可否の編集］ダイアログで設定した、機器を特定するための「判定形式」の内容によって動作が異なります。
  - 判定形式が「MAC アドレス」の場合
    ネットワーク制御リストの該当する機器の IP アドレスの情報が変更されます。
  - 判定形式が「IP アドレス」または「MAC アドレス＋ IP アドレス」の場合
    ネットワーク制御リストの該当する機器の情報は変更されません。

このため、IP アドレスを頻繁に変更する運用の場合は、ネットワーク制御リストの判定形式を「MAC のみ」で運用することを推奨します。

ヒント

ネットワーク制御リストの自動更新は、デフォルトでは新規機器の追加だけが有効になっています。10-02 以前のバージョンから JP1/IT Desktop Management 2 をバージョンアップした場合は、追加、変更、削除のすべての自動更新が有効になっています。

なお、自動更新のうち追加だけを有効にした場合、ネットワーク制御の設定は変更または削除されないで残ったままになります（変更時には変更後の新しい設定が追加されます）。残ったネットワーク制御の設定には「自動更新（追加のみ有効）の影響」の項目に［確認候補］が設定されます。

自動更新を設定する方法については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のネットワーク制御リストの自動更新の設定を編集する手順の説明を参照してください。

2.8.16　ネットワークへの接続を許可しない機器の特例接続の管理

ネットワークへの接続を許可しない機器の特例接続では、ネットワーク接続が遮断されている機器に対して、特定の機器への通信だけ許可するようにネットワーク接続を制御できます。例えば、セキュリティの対策用サーバを［ネットワークへの接続を許可しない機器の特例接続］に登録します。これによって、セキュリティの状況が危険と見なされてネットワーク接続が遮断された機器でも、検疫時にセキュリティの対策用サーバと通信することでセキュリティ対策を実行できます。 デフォルトでは、管理用サーバが［ネットワークへの接続を許可しない機器の特例接続］に登録されています。

なお、ネットワークモニタエージェントがインストールされたコンピュータでは、次のとおり自動で環境が設定されます。これらの環境は特例接続の通信時に必要であるため、設定を変更しないでください。

- Windows ファイアウォールが無効になる
- サービス（Routing and Remote Access）が有効になる
- OS が Windows Server 2012 および Windows Server 2008 R2 の場合、Windows の役割サービス（ルーティングとリモートアクセス）が有効になる

ネットワーク接続が遮断された機器に対して、特定の通信だけネットワーク接続を許可したい場合は、特例接続の設定を作成します。

ネットワーク接続が遮断された場合に通信できる機器を変更する場合は、特例接続の設定を編集します。

運用状況の変更に伴って特例接続の設定が不要になった場合、特例接続の設定を削除します。

特例接続を管理する方法の詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の、特例接続を管理する方法の説明を参照してください。

2.8.17　手動によるネットワーク接続の制御

ネットワークモニタが有効になっている場合、手動でネットワーク接続を制御できます。

ネットワーク接続の制御には優先度があります。手動で、ネットワーク接続を許可しない設定にしておくと、自動的にネットワーク接続が許可される契機でも、許可されません。ネットワークに接続してはいけ

ないコンピュータがある場合は、手動で「許可しない」に設定してください。なお、ネットワーク接続を自動で制御する方法については、「2.8.14　各種機能によるネットワーク接続の自動制御」を参照してください。

ヒント

手動でネットワーク接続を許可した場合でも、自動的にネットワーク接続が遮断される契機になると、遮断されます。

ネットワーク接続を手動で変更するには、次の方法があります。

機器画面またはセキュリティ画面でネットワーク接続を制御する

機器画面の［機器情報］画面およびセキュリティ画面の［機器のセキュリティ状態］画面で、機器ごとにネットワーク接続の状態を変更できます。

インフォメーションエリアで対象のコンピュータを選択し、［操作メニュー］から［接続を許可する］または［接続を許可しない］を選択してください。対象のコンピュータのネットワーク接続の状態が変更されます。

コマンドを使用してネットワーク接続を制御する

JP1/IT Desktop Management 2 のネットワーク制御コマンドによって、機器のネットワーク接続を遮断したり、回復したりできます。 ネットワーク制御コマンドは、管理用サーバ以外の環境から実行できます。

2.8.18　ネットワーク接続可否情報のインポート

CSV ファイルを利用してネットワーク接続可否情報をインポートすると、一括でネットワーク制御リストに設定を追加できます。また、エクスポートしたネットワーク接続可否情報を編集してインポートすると、一括でネットワーク制御リストの設定を更新できます。ネットワーク接続可否情報のインポートは、［ネットワーク接続可否情報をインポートしましょう］ウィザードで実行します。

ヒント

複数サーバ構成の場合、システム全体で共通のネットワーク接続可否情報を用意し、それを各管理用サーバでインポートすることで、各管理用サーバでネットワーク制御リストを設定する負担を軽減できます。また、出張などの理由でコンピュータの管理元を一時的に変更する必要があるときにも、ネットワーク接続可否情報を管理用サーバ間で共有することで、管理元を変更するたびにネットワーク接続可否情報を見直す必要がなくなるため便利です。

ヒント

設定画面の［ネットワーク制御リストの設定］画面でインフォメーションエリアに「-」が表示されている項目は、ネットワーク接続可否情報をエクスポートすると、「-」の部分が空文字で

出力されます。これは、エクスポートしたネットワーク接続可否情報をそのままインポートする際に、正常にインポートできるようにするためです。

インポートする CSV ファイルのデータは、規定された記述形式に従っている必要があります。インポートできるネットワーク接続可否情報の項目と記述形式を次の表に示します。

項目	データの記述形式	省略可否
MAC アドレス	16 進数の文字列を次の形式で記述します。x は、0～F です。 • xxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx なお、区切り文字「-」および「:」は混在していても記述できます。 また、CSV ファイル内で MAC アドレスが重複しているデータは、インポート時にエラーとなります。	△ ※1
IP アドレス	次の形式で記述します。 nnn.nnn.nnn.nnn 0.0.0.0～255.255.255.255 の範囲で記述してください。また、記述できるのは IPv4 の IP アドレスだけです。CSV ファイル内に IP アドレスが重複している、かつ MAC アドレスが記述されていないデータは、インポート時にエラーとなります。	△ ※1
ネットワークへの接続	「0」「2」のどちらかを記述します。 0：接続を許可する 2：接続を許可しない	×
判定形式	「0」「1」「2」のどれかを記述します。 0：MAC アドレス 1：IP アドレス 2：MAC アドレス+IP アドレス	×
利用期間の指定	「0」「1」のどちらかを記述します。 0：利用期間を指定しない 1：利用期間を指定する	×
利用開始日時	Web ブラウザのタイムゾーンのローカルタイムを次の形式で記述します。 *YYYY-MM-DD hh:mm:ss* YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒 秒の指定は「00」に切り捨ててインポートします。	△ ※2
利用終了日時	Web ブラウザのタイムゾーンのローカルタイムを次の形式で記述します。 *YYYY-MM-DD hh:mm:ss* YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒 秒の指定は「00」に切り捨ててインポートします。	△ ※2
説明	128 文字以内の任意の文字列を記述します。	○

（凡例）○：記述を省略できる。 △：ほかの項目の値に応じて省略可否が変わる。 ×：記述を省略できない。

注※1 ［判定形式］の値によって、省略可否が次のように変わります。

- ［判定形式］が「0」の場合、［MAC アドレス］を省略できない。
- ［判定形式］が「1」の場合、［IP アドレス］を省略できない。
- ［判定形式］が「2」の場合、［MAC アドレス］および［IP アドレス］のどちらも省略できない。

注※2 ［利用期間の指定］の値が「1」の場合は、［利用開始日時］および［利用終了日時］を記述してください。どちらか一方だけを指定することもできます。

［判定形式］が［MAC アドレス］または［MAC アドレス+IP アドレス］であるデータがインポートされる場合の動作

インポート先のネットワーク制御リストに、インポートするデータと同じ MAC アドレスが指定されたネットワーク接続可否情報があるかどうかで動作が変わります。

同じ MAC アドレスが指定されたネットワーク接続可否情報がある

該当するネットワーク接続可否情報が更新されます。インポート先のネットワーク制御リストの［自動更新（追加のみ有効）の影響］には［影響なし］が設定されます。

同じ MAC アドレスが指定されたネットワーク接続可否情報がない

ネットワーク接続可否情報が新規追加されます。

［判定形式］が「IP アドレス」であるデータがインポートされる場合の動作

インポート先のネットワーク制御リストに、インポートするデータと同じ IP アドレスが指定されたネットワーク接続可否情報があるかどうかで動作が変わります。

同じ IP アドレスが指定されたネットワーク接続可否情報がある

インポートするデータの MAC アドレスと該当するネットワーク接続可否情報の MAC アドレスが異なるときは、ネットワーク接続可否情報が新規追加されます。それ以外のときは、該当するネットワーク接続可否情報が更新されます。インポート先のネットワーク制御リストの［自動更新（追加のみ有効）の影響］には［影響なし］が設定されます。

同じ IP アドレスが指定されたネットワーク接続可否情報がない

ネットワーク接続可否情報が新規追加されます。

関連リンク

- 2.8.15　ネットワーク制御リストの自動更新
- 2.8.19　ネットワーク接続可否情報のエクスポート

2.8.19　ネットワーク接続可否情報のエクスポート

CSV ファイルにネットワーク接続可否情報をエクスポートできます。エクスポートすることで、設定中のネットワーク接続可否情報をほかの管理用サーバと共有できます。また、エクスポートしたネットワーク

接続可否情報を編集してインポートすると、一括でネットワーク制御リストの設定を更新できます。ネットワーク接続可否情報のエクスポートは、設定画面の［ネットワーク制御リストの設定］画面の［操作メニュー］から実行します。

出力されるデータ形式については、関連リンクを参照してください。

関連リンク

- 2.8.18　ネットワーク接続可否情報のインポート

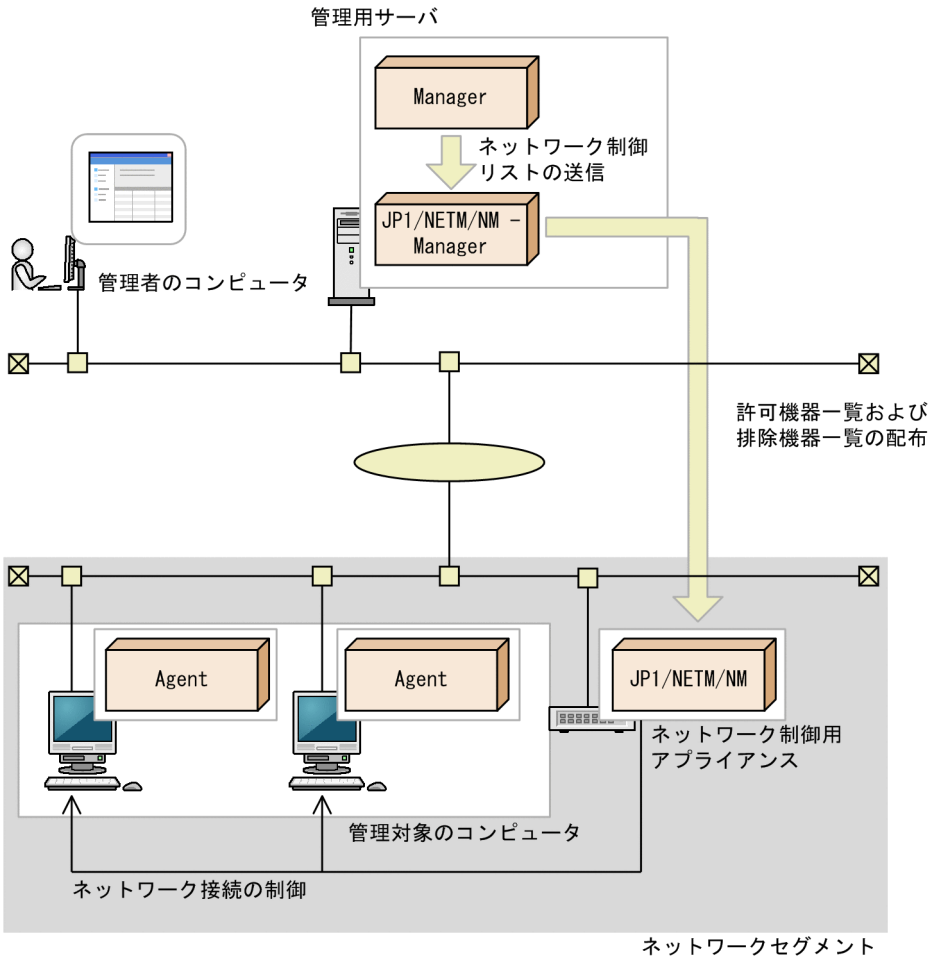
2.8.20　JP1/NETM/NM - Manager 連携によるネットワーク制御機能

JP1/IT Desktop Management 2 と JP1/NETM/NM - Manager と連携することで、ネットワークモニタを有効にしたコンピュータを設置しなくても、ネットワークを制御できます。

JP1/NETM/NM - Manager と連携するには、JP1/NETM/NM - Manager とネットワーク制御用アプライアンスを導入する必要があります。連携できる JP1/NETM/NM - Manager のバージョンは、09-50 以降です。

JP1/NETM/NM - Manager と連携すると、ネットワーク制御用アプライアンスでネットワーク接続を制御できるようになるため、ネットワークモニタを有効にしたコンピュータを拠点ごとに設置したり、管理したりする必要がありません。

JP1/NETM/NM - Manager と連携してネットワークを制御する流れを次の図に示します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager
Agent：JP1/IT Desktop Management 2 - Agent

JP1/IT Desktop Management 2 - Manager から、ネットワーク制御用リストの許可機器一覧および排除機器一覧を JP1/NETM/NM - Manager に送信します。JP1/NETM/NM - Manager からネットワーク制御用アプライアンスに、許可機器一覧および排除機器一覧を配布します。ネットワーク制御用アプライアンスで、配布された許可機器一覧および排除機器一覧に従って、ネットワークセグメントのネットワーク接続を制御します。

JP1/NETM/NM - Manager で管理している機器のネットワーク接続は検知できますが、JP1/IT Desktop Management 2 のネットワーク監視機能とは異なり、ネットワーク探索は自動で実行されません。

JP1/IT Desktop Management 2 では次に示す設定ができないため、JP1/NETM/NM - Manager で設定してください。

- ネットワーク制御用アプライアンスの環境設定
- JP1/NETM/NM - Manager で管理している機器の特例接続の設定

JP1/NETM/NM - Manager での設定については、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」を参照してください。

関連リンク

- 4.4.13　JP1/NETM/NM - Manager 連携構成

2.8.21　NX NetMonitor/Manager 連携によるネットワーク制御機能

JP1/NETM/NM - Manager の代わりに、NX NetMonitor/Manager と連携することができます。連携できる NX NetMonitor/Manager のバージョンは、07-12 以降です。

また、JP1 for IoT - NX NetMonitor 01-00 以降に同梱されている NX NetMonitor/Manager と連携することもできます。

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 セキュリティの管理

組織内のコンピュータのセキュリティを阻害する要因には、ウィルス対策製品の未インストール、ファイル共有ソフトウェアのインストール、OS セキュリティ設定の不備など、多くの要素があります。組織内のセキュリティ状況を安全に保つためには、これらの要因に対するセキュリティのルールを決め、それを各コンピュータの利用者に遵守させる必要があります。また、セキュリティの現状を把握して、問題点を適宜対策することも必要です。

JP1/IT Desktop Management 2 では、組織内のセキュリティのルールを「セキュリティポリシー」として設定し、それらを各コンピュータに適用することで、問題点を発見して管理者に通知したり、自動的に対策したりできます。

セキュリティポリシーを利用することで、次のセキュリティ状況を把握できます。

- 更新プログラムの適用状況
- ウィルス対策製品の適用状況
- 使用を必須とするソフトウェアのインストール状況
- 使用を禁止しているソフトウェアのインストール状況
- サービスの稼働状況
- OS 設定の状況

また、このほかにも、ソフトウェアやデバイスなどの使用抑止、各コンピュータでの不審操作の検知など、セキュリティ管理に関するさまざまな設定ができます。

重要

UNIX エージェントの場合、次に示す制限があります。

- セキュリティポリシーに基づいたセキュリティ状況の判定をしないので、危険レベルは常に「 (不明)」が表示されます。OS パッチの適用状況やウィルス対策製品の設定状況なども判定されません。
- セキュリティ上の問題点の自動対策（OS パッチ、ウィルス対策製品、使用必須ソフトウェアの自動配布など）やメール通知はできません。
- ネットワーク接続の自動制御はできません。手動での制御となります。
- OS パッチや業務で使用するソフトウェアの配布・適用は、リモートインストールマネージャを使用した配布で対策する必要があります。

なお、「パスワードを更新してからの経過日数（アカウント／日数)」および「パワーオンパスワード」は、システム情報として UNIX エージェントから通知されます。また、エージェント側で通知を抑止する設定になっている場合、OS パッチ情報は通知されません。

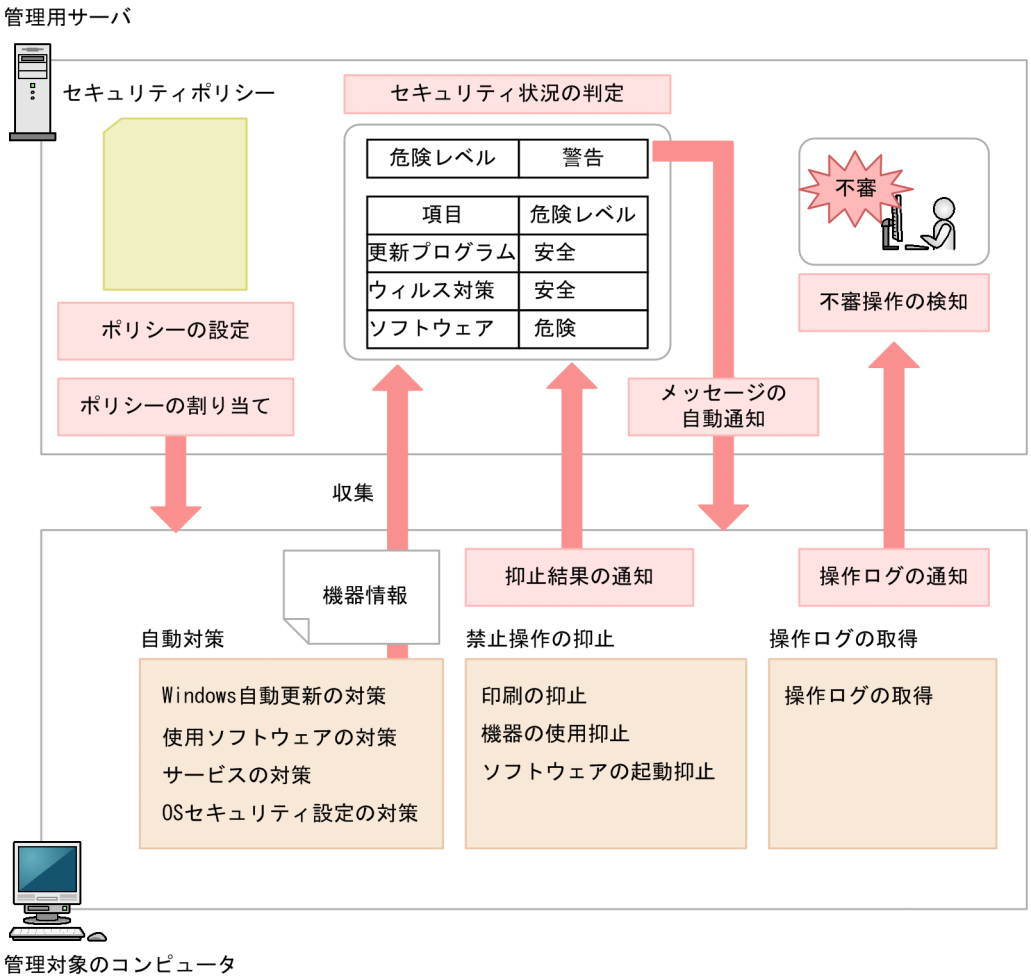
重要

Mac エージェントの場合、次に示す制限があります。

- セキュリティ上の問題点の自動対策（OS パッチ、ウィルス対策製品、使用必須ソフトウェアの自動配布など）やメール通知はできません。
- ネットワーク接続の制御は、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。
- OS パッチや業務で使用するソフトウェアの配布・適用は、リモートインストールマネージャを使用した配布で対策する必要があります。

2.9.1 セキュリティ状況を管理する仕組み

コンピュータのセキュリティ状況は、次の図に示すように管理します。



はじめに、組織のセキュリティのルールに沿ってセキュリティポリシーを設定します。JP1/IT Desktop Management 2 では、管理対象のコンピュータにデフォルトポリシーが自動的に割り当たります。このため、運用開始直後はセキュリティポリシーを作成しなくても、デフォルトポリシーによって判定されたセ

キュリティ状況を確認できます。また、セキュリティの推奨設定をした推奨セキュリティポリシーも提供しています。デフォルトポリシーと推奨セキュリティポリシーの設定内容については、「(3)　製品が提供するセキュリティポリシー」を参照してください。

デフォルトポリシー以外のセキュリティポリシーでセキュリティ状況を判定するためには、セキュリティポリシーを追加して管理対象のコンピュータに割り当てる必要があります。コンピュータにセキュリティポリシーを割り当てると、セキュリティポリシーの設定に基づいて、収集された機器情報を基に管理用サーバでセキュリティ状況が判定されます。また、管理対象のコンピュータで禁止操作の抑止、および操作ログの取得が実行されます。自動対策を設定している場合は、セキュリティポリシーに違反していた場合に対策が実行されます。セキュリティ状況の判定については、「2.9.3　セキュリティ状況の判定」を参照してください。禁止操作の抑止については、「2.9.5　禁止操作の抑止」を参照してください。

セキュリティ状況の判定結果、および禁止操作の抑止結果は管理用サーバに通知され、コンピュータのセキュリティ状況が表示されます。管理者は、セキュリティ状況を確認し、問題点を対策します。セキュリティポリシーにメッセージの自動通知を設定していると、判定結果に応じて管理対象のコンピュータに自動的にメッセージが通知されます。

操作ログは、管理対象のコンピュータで取得されます。不審操作は、取得された操作ログを判定材料にしてセキュリティポリシーの設定に従って検知されます。検知された不審操作を基に、管理者は操作ログを追跡調査して、情報漏えいが発生していないかどうかを確認できます。検知された不審操作を基にした操作ログの追跡調査については、「2.10.3　ファイル持ち出しによる不審操作の、操作ログでの調査」を参照してください。

重要

Active Directory のグループポリシーで組織内のコンピュータのセキュリティ設定を規定している場合、JP1/IT Desktop Management 2 のセキュリティポリシーでセキュリティ設定を自動対策しても、Active Directory での設定が優先されます。

重要

仮想コンピュータのセキュリティ状況を管理する場合、仮想化サーバだけでなく、仮想コンピュータにもエージェントを導入してください。

関連リンク

- (1)　セキュリティポリシーに設定できる項目

2.9.2　セキュリティ管理できる機器

JP1/IT Desktop Management 2 では、管理対象となる機器だけセキュリティ管理できます。

なお、管理対象となる機器は、エージェントが導入されているかどうかで異なります。セキュリティ管理できる機器について次の表に示します。

機種種別	OS 種別	セキュリティ管理機能の実行可否			
		セキュリティの判定	自動対策	アクション	
				メッセージ通知	ネットワーク制御
コンピュータ	Windows Server 2019	○ ※1、※2	△ ※3、※6	△ ※3、※4、※6	○
	Windows Server 2016				
	Windows 10				
	Windows 8.1				
	Windows 8				
	Windows Server 2012 R2				
	Windows Server 2012				
	Windows 7				
	Windows Server 2008 R2				
	Windows Server 2008				
	Windows Vista				
	Windows Server 2003 R2※5				
	Windows Server 2003※5				
	Windows XP				
	Linux • CentOS • Red Hat Enterprise Linux • Oracle Linux	×	×	×	○
	UNIX • AIX • HP-UX • Solaris				
	Mac OS	○	×	×	○
	不明	×	×	×	○
スマートデバイス	iOS	×	×	×	○
	Android				

機種種別	OS 種別	セキュリティ管理機能の実行可否			
		セキュリティの判定	自動対策	アクション	
				メッセージ通知	ネットワーク制御
ストレージ	－	×	×	×	○
ネットワーク装置					
プリンタ					
周辺装置					
USB デバイス					
ディスプレイ					
その他					
管理者が追加した機器種別					
不明な機器					

（凡例）○：実行できる　△：エージェント導入済みの機器だけ実行できる　×：実行できない　－：該当なし

注※1　エディションが「不明」の場合、対象外となります。

注※2　Active Directory の探索、またはネットワークの探索の SNMP 認証で管理対象にしたコンピュータは、セキュリティの判定はできません（判定結果は「不明」になります）。

注※3　対象のコンピュータをオンライン管理しているときだけ実行できます。オフライン管理のコンピュータにセキュリティポリシー違反があった場合は、手動で対策してください。

注※4　Citrix XenApp、Microsoft RDS サーバの場合、メッセージ通知は実行できません。

注※5　Windows Server 2003 と Windows Server 2003 R2 は、同じ OS として扱われます。例えば、[セキュリティポリシーの編集] ダイアログのセキュリティ設定項目の「更新プログラム」で、指定したグループに Windows Server 2003 Standard Edition が含まれる場合、Windows Server 2003 Standard Edition および Windows Server 2003 R2 Standard Edition が対象となります。

注※6　API 管理機器の場合、自動対策およびメッセージ通知は実行できません。

2.9.3　セキュリティ状況の判定

管理対象のコンピュータにセキュリティポリシーを割り当てると、セキュリティポリシーの設定に基づいてセキュリティ状況が判定されます。判定のタイミングになると、セキュリティポリシーのセキュリティ設定項目の条件と、管理対象のコンピュータから収集した機器情報を比較して、危険レベルを判定します。

複数サーバ構成の場合、各管理用サーバでは直下のコンピュータだけにセキュリティポリシーを割り当てられます。NAT 環境で管理用サーバを運用しているときや、各管理用サーバでセキュリティポリシーを統一したいときは、同じセキュリティポリシーを各管理用サーバに設定してください。

なお、セキュリティポリシーのアクション項目でメッセージ通知を設定しておくと、セキュリティ状況の判定結果に応じて、コンピュータにメッセージを自動的に通知できます。メッセージにはセキュリティの問題点が載っているので、メッセージに従って対処するよう指示しておくことで管理者が問題点を対処する手間が省けます。

ヒント

OS のコンポーネントや特定のプログラムによって、OS のユーザーアカウントが自動作成されている場合、利用しないユーザーアカウントのセキュリティ状況まで判定されてしまうと、セキュリティ状況を正しく管理できないおそれがあります。このような場合、利用しないユーザーアカウントを判定の対象外にすることで、適切にセキュリティ状況が判定されるように設定できます。

(1) セキュリティポリシーで判定される危険レベル

セキュリティポリシーにセキュリティの判定条件や対策を定義し、管理対象のコンピュータにこのセキュリティポリシーを割り当てることで、セキュリティポリシーの遵守状況に合わせて、セキュリティの危険レベル（危険度）が判定されます。

セキュリティポリシーで、判定結果が不適正だった場合に表示する危険レベルを、セキュリティ判定項目ごとに設定します。セキュリティポリシーを遵守していない場合は、設定した危険レベルが判定結果となります。コンピュータの総合的な危険レベルは、各項目の危険レベルのうち最も危険度が高い危険レベルが表示されます。

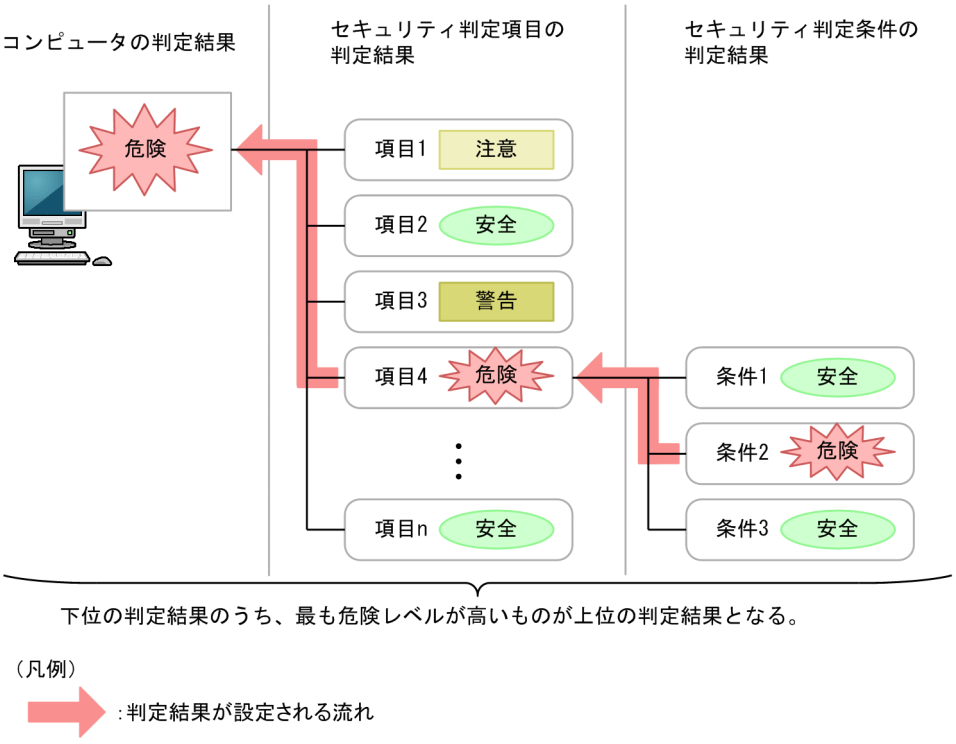
危険レベルの種類を、危険度が高い順に次の表に示します。

危険レベル	アイコン	説明
危険		最も危険度が高い危険レベルです。 直ちに対策しないとシステム全体に被害が拡大し、業務停止など多大な影響を及ぼすおそれがある場合に設定します。
警告		セキュリティが脆弱なコンピュータへの対策を怠ると、通常業務に影響を与えるおそれがある場合に設定します。
注意		通常業務への影響は低いが、システムへの影響度を考慮すると対策した方が安全な場合に設定します。
不明		次に示す判定結果の場合に設定される危険レベルです。 • セキュリティ状況の判定が 1 回も実施されていない場合 エージェントが新規に接続され、セキュリティ状況の判定時にエージェントからセキュリティ情報が通知されていない場合、セキュリティ状況の判

危険レベル	アイコン	説明
不明		定はされません。この場合、危険レベルの判定結果にコンピュータ数はカウントされません。 • セキュリティ状況の判定に必要な情報が不足している場合 この場合、セキュリティ状況を正しく判定するために、コンピュータにエージェントを導入し、判定に必要な情報を収集する必要があります。 • セキュリティ状況が正しく判定されなかった場合 内部的な障害が発生したため、セキュリティ状況が正しく判定できていない状態です。この場合、ログなどのトラブルシュート情報から、障害要因の調査や対策を実施する必要があります。 • OS が Linux、UNIX のコンピュータ セキュリティ状況の判定が実施されないため「不明」となります。
安全		セキュリティ判定項目、および判定条件が遵守されている場合に設定される危険レベルです。
対象外	なし	セキュリティポリシーの判定項目が設定されていない場合に設定される危険レベルです。 また、管理対象の機器のうち次に示すコンピュータ、および IP 機器については、セキュリティポリシーの判定が実施されないため「対象外」となります。 • OS が不明なコンピュータ • Windows のエディションが不明なコンピュータ

危険レベルの判定条件

危険レベルは、セキュリティ判定条件、セキュリティ判定項目、およびコンピュータの単位で判定されます。危険レベルの判定の仕組みを次の図に示します。



まず、セキュリティ判定項目ごとに危険レベルが判定されます。ただし、セキュリティ判定項目に複数のセキュリティ判定条件がある場合は、判定条件ごとに危険レベルが判定されます。セキュリティ判定条件の判定結果のうち、最も危険度が高い判定結果が、該当するセキュリティ判定項目の危険レベルとなります。

そして、セキュリティ判定項目ごとの判定結果のうち、最も危険度が高い判定結果がコンピュータの危険レベルとなります。

この図の場合、セキュリティ判定項目 4 の判定条件 2 が「危険」と判定されているため、ほかの判定条件が「安全」でも、セキュリティ判定項目 4 の判定結果は「危険」となります。そして、セキュリティ判定項目 4 が「危険」となるため、ほかの判定項目が「安全」や「警告」でも、このコンピュータの判定結果は「危険」となります。

セキュリティ判定条件、セキュリティ判定項目については、「(1)　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。

なお、コンピュータがセキュリティポリシーを遵守しているかどうかの判定結果は、セキュリティ画面の［機器のセキュリティ状態］画面で確認できます。

重要

- セキュリティポリシー一覧の適用率と適用コンピュータの台数は、セキュリティ判定を実施した機器の台数を対象に算出します。このため、適用率については、該当のセキュリティポリシーでセキュリティ判定を実施した機器のうち、セキュリティポリシーに違反していない機器の割合を表示します。
- 適用コンピュータについては、該当のセキュリティポリシーでセキュリティ判定を実施した機器の台数を表示します。セキュリティポリシーを割り当ててもセキュリティ判定を実施していない機器は適用率および適用コンピュータの台数の算出対象となりません。
- セキュリティポリシーで禁止操作と操作ログのどちらか、または両方だけを有効にしている場合、およびセキュリティポリシーに設定した判定項目がすべて判定対象外となる場合は、セキュリティ判定が実施されないため、算出対象となりません。

危険レベルのカウント方法

一定期間対策していない機器の利用者にメッセージを通知したり、機器のネットワーク接続を遮断したりするため、機器ごとに、連続で対策されていない日数をカウントします。

危険レベルが「危険」、「警告」、または「注意」と判定された時点から 24 時間ごとに、連続日数が 1 日増加します。カウント方法の例を次に示します。

- 2011/4/1 0:00～2011/4/5 5:59：「危険」と判定
- 2011/4/5 6:00～2011/4/7 12:00：「警告」と判定

この場合、2011/4/1 0:00～2011/4/7 12:00 の期間（6 日と 12 時間）対策をしていないと見なされて、連続日数は「7 日」とカウントされます。

(2) セキュリティ状況の判定のタイミング

セキュリティ状況の判定は、機器情報の更新、スケジュール設定などの各タイミングで行われます。

セキュリティ状況を判定するタイミングごとの詳細を次の表に示します。

タイミング	判定に使用するセキュリティポリシー	判定対象のコンピュータ	説明
セキュリティポリシーが割り当てられたとき	割り当てられているセキュリティポリシー	• セキュリティポリシーが割り当てられているすべての機器 • セキュリティポリシーが割り当てられているグループに所属するすべての機器※	機器またはグループへのセキュリティポリシーの割り当ておよび割り当て解除によって、割り当てられているセキュリティポリシーが変更された場合に判定を実施します。
セキュリティポリシーが更新されたとき	内容を変更したセキュリティポリシー	• 内容を変更したセキュリティポリシーが割り当てられているすべての機器 • 内容を変更したセキュリティポリシーが割り当てられているグループに所属するすべての機器※	セキュリティポリシーの内容を変更した場合に判定を実施します。
システム管理者が操作画面またはコマンドで資産情報を更新したとき	次の優先度でセキュリティポリシーを使用します。 • 機器に割り当てられているセキュリティポリシー • グループに割り当てられているセキュリティポリシー	資産情報を更新した資産に関連する機器	追加した追加管理項目が、ユーザー定義のセキュリティ設定項目として 1 つ以上のセキュリティポリシーに設定されている場合、そのセキュリティポリシーを判定に使用するかどうかに関係なく、判定を実施します。
システム管理者が機器に対応づけられているハードウェア資産を変更したとき	次の優先度でセキュリティポリシーを使用します。 • 機器に割り当てられているセキュリティポリシー • グループに割り当てられているセキュリティポリシー	ハードウェア資産との対応づけを変更した機器	追加した追加管理項目が、ユーザー定義のセキュリティ設定項目として 1 つ以上のセキュリティポリシーに設定されている場合、そのセキュリティポリシーを判定に使用するかどうかに関係なく、判定を実施します。
管理対象のコンピュータの機器情報を操作画面で更新したとき	次の優先度でセキュリティポリシーを使用します。 • 機器に割り当てられているセキュリティポリシー • グループに割り当てられているセキュリティポリシー	機器情報が更新されたすべての機器	オンライン管理の場合 変更された機器情報が管理用サーバに収集され更新されると、判定を実施します。 オフライン管理の場合 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コンピュータから収集した情報を、管理

タイミング	判定に使用するセキュリティポリシー	判定対象のコンピュータ	説明
管理対象のコンピュータの機器情報を操作画面で更新したとき	次の優先度でセキュリティポリシーを使用します。 • 機器に割り当てられているセキュリティポリシー • グループに割り当てられているセキュリティポリシー	機器情報が更新されたすべての機器	用サーバに通知したときに判定を実施します。
管理対象のコンピュータの属するグループが変更されたとき	変更後のグループに割り当てられているセキュリティポリシー	グループを変更した機器※	セキュリティポリシーの対象の構成が、ユーザー定義のグループ以外の場合 機器が所属するグループを変更して、割り当てられているセキュリティポリシーが変更されたときに判定を実施します。 セキュリティポリシーの対象の構成が、ユーザー定義のグループの場合 ユーザー定義のグループ条件が変更されたときに判定を実施します。ユーザー定義のグループ条件が変更される契機を次に示します。 • システム管理者がユーザー定義のグループ条件を変更したとき • ユーザー定義のグループ条件の対象項目に設定されている追加管理項目が削除されたとき • ユーザー定義のグループ条件の対象項目に設定されている選択型の追加管理項目の選択項目が削除されたとき
定期的な判定（デフォルトは毎日0：00）	次の優先度でセキュリティポリシーを使用します。 • 機器に割り当てられているセキュリティポリシー • グループに割り当てられているセキュリティポリシー	すべての機器	設定画面の［セキュリティのスケジュール設定］画面で指定したスケジュールに従って、判定を実施します。

注※　機器単位にセキュリティポリシーが割り当てられている場合は、対象外です。

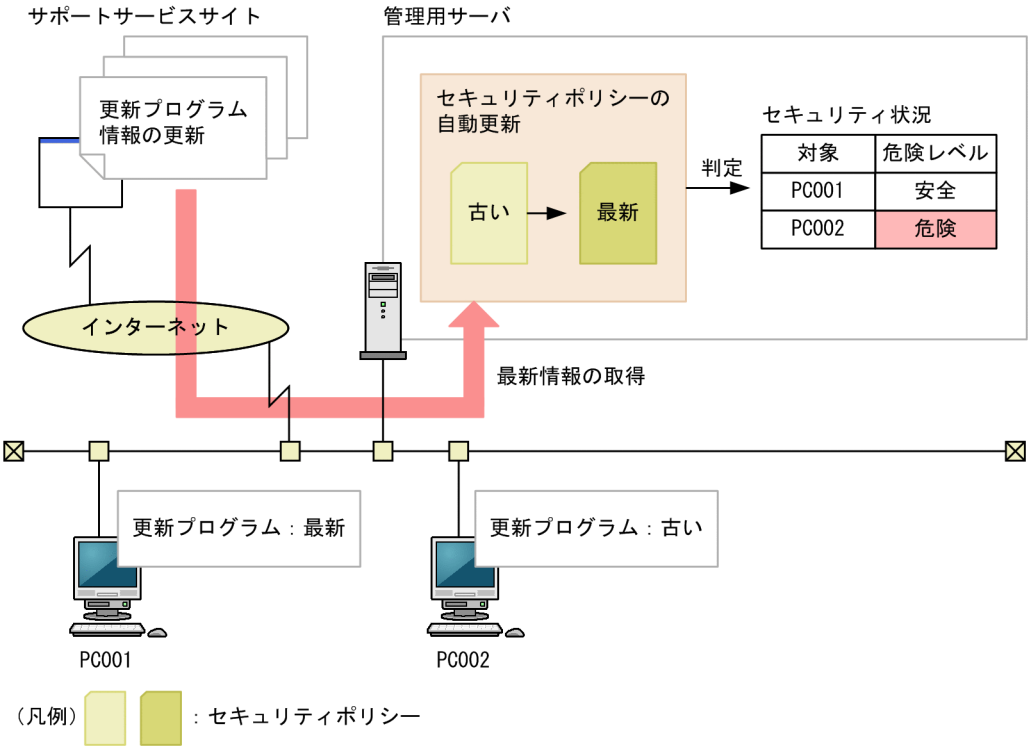
(3)　更新プログラムの適用状況の判定

コンピュータに最新の更新プログラムが適用されているかどうか判定するためには、日本マイクロソフト社の Web サイトを常に監視して、新しい更新プログラムの判定が必要かどうかを判断し、情報を登録する必要があります。この作業は非常に手間が掛かります。

サポートサービスを契約すると、最新の更新プログラム情報をサポートサービスサイトから定期的に自動で取得できます。取得した更新プログラム情報は、セキュリティポリシーに自動的に反映されます。このため、管理者が更新プログラムのバージョンなどを確認することなく、コンピュータに最新の更新プログラム情報が適用されているかどうかを判定できます。また、セキュリティポリシーの設定次第で、最新の更新プログラムが適用されていないコンピュータに対して最新の更新プログラム情報を配布して適用することもできます。

更新プログラム情報を定期的に自動で取得するには、設定画面でサポートサービスサイトへの接続設定および更新プログラム情報の取得スケジュールの設定が必要です。

最新の更新プログラム情報の取得からセキュリティポリシーの更新までの流れを次の図に示します。



ヒント

JP1/IT Desktop Management 2 が取得できる最新の更新プログラム情報は、Windows および Internet Explorer のセキュリティ深刻度が「緊急」または「重要」のセキュリティ問題の修正プログラムです。

更新プログラムの適用状況は、「すべての更新プログラムが適用済み」または「指定した更新プログラムが適用済み」のどちらかで判定します。セキュリティポリシーで、セキュリティの判定時に使用される更新プログラム情報を設定してください。

関連リンク

- 2.9.6　更新プログラムの管理

(4)　最新の更新プログラムの適用状況の判定

管理用サーバに登録されているすべての更新プログラム情報を基に、コンピュータの更新プログラムの適用状況を判定できます。更新プログラム情報が追加されると判定対象に加わるため、自動的に最新の更新プログラムの適用状況を把握できます。また、判定の対象外とする更新プログラムを指定することもできます。

判定で使用される情報を次の表に示します。

情報	説明
最新の更新プログラム	サポートサービスサイトから取得した最新の更新プログラムの情報です。すべての更新プログラムを適用するように指定します。 なお、サポートサービスサイトから取得した最新の更新プログラムは、セキュリティ画面の［更新プログラム一覧］画面で確認できます。
除外する更新プログラム	判定対象から除外する更新プログラムの情報です。セキュリティ画面で更新プログラムのグループを作成して、セキュリティポリシー設定時に該当するグループを指定します。
機器情報	セキュリティポリシーの判定対象となるコンピュータから収集された更新プログラムの情報です。

セキュリティの判定時には、セキュリティポリシーの対象となるコンピュータの機器情報と、サポートサービスサイトから取得した最新の更新プログラムの情報が比較されます。このとき、文書番号またはセキュリティ情報番号の両方とも情報が一致しなかった場合は、最新の更新プログラムが適用されていないと判断され、セキュリティポリシーで定義されている危険レベルが設定されます。除外する更新プログラムが適用されなかった場合は、危険レベルが設定されません。

ヒント

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、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、 最新の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を管理用サーバに手動でコピーしたあと、`updatesupportinfo` 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。これによって、最新の更新プログラムの情報を管理用サーバに適用できます。

ヒント

Windows の累積的な更新プログラムおよびセキュリティマンスリー品質ロールアップの場合、最新の更新プログラムが公開されてからサポートサービスサイトの更新プログラムの情報が更

新されるまでの間であってもセキュリティ判定ができます。また、更新プログラムを適用する猶予期間を考慮したセキュリティ判定もできます。詳細は、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の Windows の累積的な更新プログラムおよびセキュリティマンスリー品質ロールアップの判定の説明を参照してください。

(5) 指定した更新プログラムの適用状況の判定

管理者が指定した更新プログラム情報を基に、コンピュータの更新プログラムの適用状況を判定できます。管理者が指定できる更新プログラムは、Windows のサービスパック、バージョンおよび更新プログラムと、Internet Explorer のサービスパックおよび更新プログラムです。

判定で使用される情報を次の表に示します。

情報	説明
管理者が指定した更新プログラム	管理者が指定したサービスパック、バージョンおよび更新プログラムが適用されていない場合に、危険と判断する更新プログラムの情報です。セキュリティ画面で更新プログラムのグループを作成して、セキュリティポリシー設定時に該当するグループを指定します。
機器情報	セキュリティポリシーの判定対象となるコンピュータから収集された更新プログラムの情報です。

セキュリティの判定時には、セキュリティポリシーの対象となるコンピュータの機器情報と、管理者が指定した更新プログラムの情報が比較されます。このとき、文書番号またはセキュリティ情報番号の両方とも情報が一致しなかった場合は、管理者が指定した更新プログラムが適用されていないと判断され、セキュリティポリシーで定義されている危険レベルが設定されます。同様に、コンピュータの機器情報と管理者が指定したサービスパックまたはバージョンの情報が比較されて一致しなかった場合も、管理者が指定した更新プログラムが適用されていないと判断され、セキュリティポリシーで定義されている危険レベルが設定されます。

関連リンク

- (9) 更新プログラムグループの管理

(6) 自動更新の設定の判定

自動更新の設定の判定で使用する情報および判定条件について説明します。

判定で使用する情報

- セキュリティ設定項目の「OS のセキュリティ設定」の各項目
- 機器情報（セキュリティ情報）の「更新プログラム情報」の各情報

判定条件

セキュリティポリシーに設定した項目ごとに機器情報と比較して判定を行い、判定結果に応じて危険レベルが決定します。

自動対策するように設定されている場合は、必要に応じて対策されます。

関連リンク

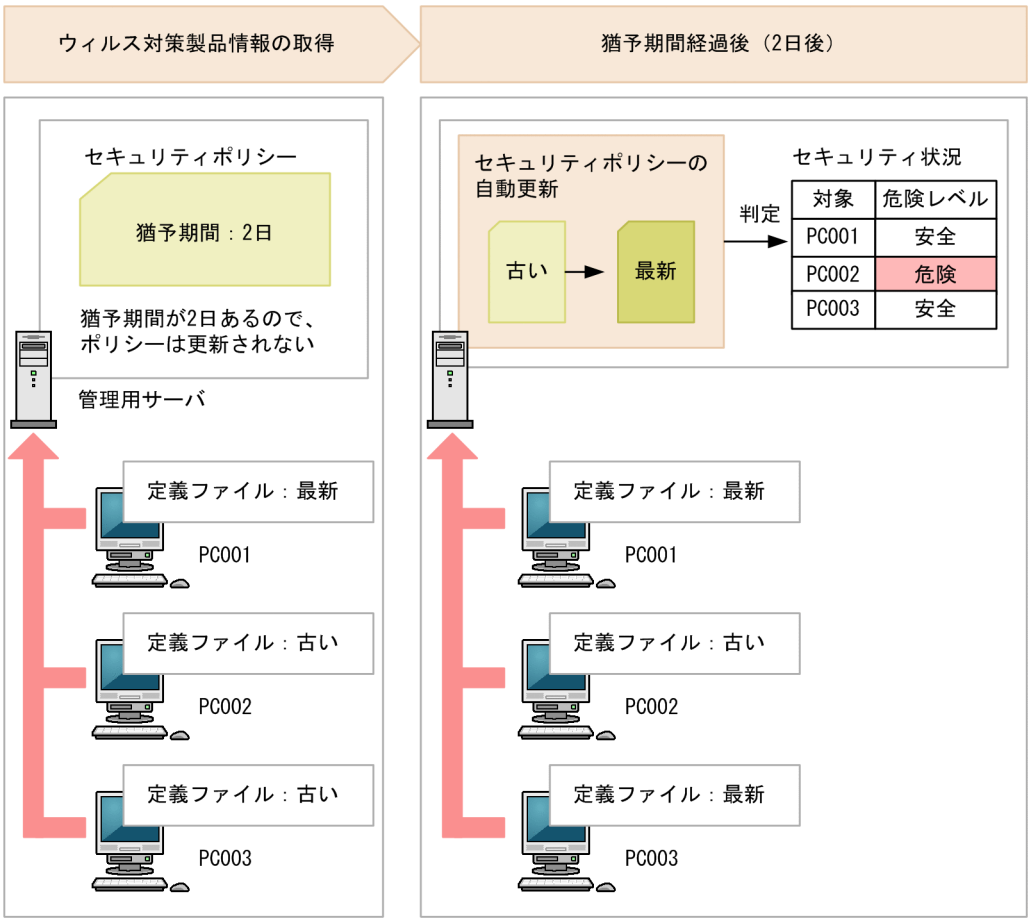
- (14)　サポートするウィルス対策製品

(7)　ウィルス対策製品の判定

ウィルス対策製品の判定では、セキュリティポリシーが適用されたコンピュータのうち最新のエンジンバージョンやウィルス定義ファイルのバージョンを基準に、各コンピュータのウィルス対策製品の状況が比較されます。そのため、管理対象のコンピュータのうち少なくとも 1 台はウィルス対策製品が最新の状態になるようにしてください。

ただし、組織内のコンピュータのウィルス対策製品が一斉に最新になるとは限りません。特定のタイミングでは、最新のものと古いものが混在している状態になります。このような場合に備え、セキュリティポリシーには最新ではない状態を何日まで許容するかの猶予期間を設定できます。

ウィルス対策製品が最新かどうかを判定する流れを次の図に示します。



新規に管理対象となった機器は、最新のセキュリティポリシーの設定に基づいてセキュリティ状況が判定されます。 このため次に示す場合、新規に管理対象となった機器は、新規に管理対象となった時点で、最新のセキュリティポリシーに設定した危険レベルと判定されます。

1. ウィルス対策製品の判定条件に設定した猶予期間を満了して、セキュリティポリシーが最新に更新された
2. 「1.」でセキュリティポリシーが最新に更新されたあと、ウィルス対策製品の状況が最新でない状態の機器が、新規に管理対象となった

サポートするウィルス対策製品（判定対象となるウィルス対策製品）

JP1/IT Desktop Management 2 がサポートするウィルス対策製品については、「(14)　サポートするウィルス対策製品」を参照してください。

判定で使用する情報

- セキュリティ設定項目の「ウィルス対策製品」の各項目
- 機器情報（セキュリティ情報）の「ウィルス対策製品情報」

判定条件

セキュリティポリシーに設定した項目ごとに機器情報と比較して判定を行い、すべての設定項目と機器情報が一致する場合、「安全」と判定されます。不一致がある場合は、設定した危険レベルと判定されます。

自動対策するように設定されている場合は、必要に応じて対策されます。

関連リンク

- (14)　サポートするウィルス対策製品

(8)　使用禁止ソフトウェアの判定

使用禁止ソフトウェアの判定で使用する情報および判定条件について説明します。

判定で使用する情報

- セキュリティ設定項目の「使用禁止ソフトウェア」の各項目
- 機器情報（インストールソフトウェア情報）の各情報

判定条件

使用禁止ソフトウェアでは、インストールソフトウェアごとに危険レベルを判定します。使用禁止ソフトウェアとして設定した情報とインストールソフトウェアのソフトウェア名とバージョンの組み合わせが 1 つでも一致する場合、設定した危険レベルと判定されます。ソフトウェア名、バージョンのどちらか一方または両方とも一致しない場合、「安全」と判定されます。ソフトウェア名は部分一致、バージョンは前方一致で判定します。

なお、 セキュリティ設定項目に「使用禁止ソフトウェア」が設定されていない場合は、「安全」と判定されます。

重要

自動対策するように設定されている場合は、ソフトウェア名は部分一致、バージョンは前方一致で判定するため、複数のソフトウェアの起動が抑止されたり、アンインストールされたりします。

重要

セキュリティポリシーの使用必須ソフトウェアと使用禁止ソフトウェアに、同じソフトウェアを指定して、自動対策を設定しないでください。同じソフトウェアを指定すると、使用必須ソフトウェアと使用禁止ソフトウェアのセキュリティ判定によって、インストールとアンインストールが交互に繰り返されます。

重要

コントロールパネルの［プログラムと機能］からアンインストールできないソフトウェアを使用禁止ソフトウェアとして設定した場合、自動対策によるアンインストールはできません。

(9) 使用必須ソフトウェアの判定

使用必須ソフトウェアの判定で使用する情報および判定条件について説明します。

判定で使用する情報

- セキュリティ設定項目の「使用必須ソフトウェア」の各項目
- 機器情報（システム情報）の「OS 情報」の各情報
- 機器情報（インストールソフトウェア情報）の各情報

判定条件

使用必須ソフトウェアに設定した OS 情報（OS とサービスパックまたはバージョン）が一致する機器を判定対象とします。 使用必須ソフトウェアでは、インストールソフトウェアごとに危険レベルを判定します。インストールソフトウェアのソフトウェア名とバージョンの組み合わせが 1 つでも一致する場合、「安全」と判定されます。ソフトウェア名、バージョンのどちらか一方または両方とも一致しない場合、設定した危険レベルと判定されます。ソフトウェア名は部分一致、バージョンは前方一致で判定します。

なお、 セキュリティ設定項目に「使用必須ソフトウェア」が設定されていない場合は、「不明」と判定されます。

自動対策するように設定されている場合は、必要に応じてソフトウェアがインストールされます。

重要

セキュリティポリシーの使用必須ソフトウェアと使用禁止ソフトウェアに、同じソフトウェアを指定して、自動対策を設定しないでください。同じソフトウェアを指定すると、使用必須ソフトウェアと使用禁止ソフトウェアのセキュリティ判定によって、インストールとアンインストールが交互に繰り返されます。

重要

OS 自体を使用必須ソフトウェアとして設定した場合、自動対策によるインストールはできません。

(10) 使用禁止サービスの判定

使用禁止サービスの判定で使用する情報および判定条件について説明します。

判定で使用する情報

- セキュリティ設定項目の「サービスのセキュリティ設定」の各項目

判定条件

セキュリティポリシーに設定した使用禁止サービスごとに判定を行い、判定結果に応じて危険レベルが決定します。使用禁止サービスとして登録したサービス名に一致するサービスが起動している場合は、セキュリティポリシーで設定した危険レベルと判定されます。一致しない場合は、「安全」と判定されます。

自動対策するように設定されている場合は、必要に応じてサービスが停止して無効になります。

オフライン管理のコンピュータにセキュリティポリシーが割り当たっていない場合は、「安全」と判定されます。

(11) 管理形態によるセキュリティ判定の差異

セキュリティ判定の設定項目には、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での判定可否に差異があります。エージェント導入済みのコンピュータの場合は、オンライン管理のときとオフライン管理のときでも差異があります。また、エージェントレスのコンピュータの場合は、認証方法によっても差異があります。

設定項目ごとの、管理形態による判定可否を次の表に示します。

設定項目		エージェント導入済み			エージェントレス						
		Windows	UNIX	Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	API		
									Windows	Mac OS	その他
更新プログラム	自動更新を実行	○	×	○	○	×	×	×	○	○	×
	すべての更新プログラムの適用状況	○	×	×	○	×	×	×	○	×	×
	指定した更新プログラムの適用状況	○	×	×	○	×	×	×	○	×	×
ウィルス対策製品	インストール	○	×	×	○	×	×	×	×	×	×
	エンジンバージョン	○	×	×	○	×	×	×	×	×	×
	ウィルス定義ファイルのバージョン	○	×	×	○	×	×	×	×	×	×
	自動保護（常駐設定）	○	×	×	○	×	×	×	×	×	×
	ウィルススキャン最終完了日時	○	×	×	○	×	×	×	×	×	×
使用ソフトウェア	使用必須ソフトウェア	○	×	○	○	×	×	×	○	○	×
	使用禁止ソフトウェア	○	×	○	○	×	×	×	○	○	×
サービスのセキュリティ設定		○ ※1	×	×	×	×	×	×	×	×	×
OS のセキュリティ設定	Guest アカウント	○	×	○	○	×	×	×	○	○	×
	パスワードの安全性	○	×	×	○	×	×	×	○	×	×
	無期限パスワード	○	×	×	○	×	×	×	○	×	×
	パスワード更新からの経過日数	○	×	○	○	×	×	×	○	○	×
	自動ログオン	○	×	○	○	×	×	×	○	○	×

設定項目		エージェント導入済み			エージェントレス						
		Windows	UNIX	Mac OS	管理共有	SNMP	ARP/ICMP	Active Directory	API		
									Windows	Mac OS	その他
OS のセキュリティ設定	パワーオンパスワード	○	×	×	○	×	×	×	○	×	×
	スクリーンセーバーのパスワード保護	○	×	○※2	○	×	×	×	○	○	×
	スクリーンセーバー起動までの待ち時間	○	×	×	○	×	×	×	○	×	×
	共有フォルダ	○	×	×	○	×	×	×	○	×	×
	管理共有	○	×	×	○	×	×	×	○	×	×
	匿名接続	○	×	×	○	×	×	×	○	×	×
	ファイアウォール※3	○	×	○	○	×	×	×	○	○	×
	DCOM	○	×	×	○	×	×	×	○	×	×
	リモートデスクトップ	○	×	×	○	×	×	×	○	×	×
ユーザー定義のセキュリティ設定		○	×	○	○	×	×	×	○	○	×

（凡例）○：判定できる　×：判定できない

注　UNIX エージェント、Mac エージェントの場合、およびオフライン管理、エージェントレス管理の場合、セキュリティの自動対策はできません。

注※1　オフライン管理の場合、サービスのセキュリティ設定は判定できません。セキュリティポリシーが割り当たっていないときは、「安全」と判定されます。

注※2　Mac OS の場合、ユーザーアカウントごとの判定結果ではなく、全ユーザーアカウントの判定結果になります。

注※3　ネットワークモニタを有効にしたコンピュータは、ファイアウォールの判定の対象外です。

ヒント

エージェントレスの場合、Windows の管理共有の認証以外ではセキュリティ判定ができません。このため、セキュリティ管理するコンピュータをエージェントレスにする場合、Windows の管理共有で認証できるようにしてください。

関連リンク

- 2.6.5　エージェントレスでの管理

(12)　ユーザー定義のセキュリティ設定の判定

セキュリティポリシーには、ユーザー定義のセキュリティ設定として、コンピュータのセキュリティ設定に関する任意のポリシーを追加できます。JP1/IT Desktop Management 2 が提供するセキュリティ設定項目にはない条件でセキュリティ判定を実施したい場合は、ユーザー定義のセキュリティ設定を追加します。

ユーザー定義のセキュリティ設定を追加すると、コンピュータのセキュリティ設定状況が任意の判定条件で判定されます。また、ユーザー定義のセキュリティ設定を追加したセキュリティポリシーに、アクション項目を設定しておけば、判定結果の危険レベルに応じて利用者へのメッセージ通知およびネットワーク接続制御を実施できます。セキュリティ判定の結果は、セキュリティ画面の［機器のセキュリティ状態］画面で確認できます。

ユーザー定義項目に基づくセキュリティ判定の仕組み

ユーザー定義のセキュリティ設定の判定は、ユーザー定義項目に設定した対象項目、判定条件、判定値に従って実施されます。判定条件を満たす場合は不適正な機器と見なされ、不適正時の危険レベルとして設定した危険レベルに変更されます。なお、対象項目に値がない機器の場合は、不適正時とは異なる危険レベルを設定できます。

対象項目

セキュリティ判定の対象とする項目です。対象項目に対応する値が複数ある場合は、そのうち 1 つでも条件を満たす項目があれば判定し、最初に条件を満たした項目の判定結果が表示されます。

対象項目は、機器情報のシステム情報、ハードウェア情報、およびハードウェア資産情報の追加管理項目から選択できます。設定できる対象項目については、「(1)　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。

判定条件

対象項目の値が、判定値と比較してどのような場合に不適正と見なすかの条件です。

判定値

対象項目が不適正かどうかを判定する際に、比較対象とする値です。

重要

対象項目は、システム管理者が追加したハードウェア資産情報の追加管理項目だけ指定できます。システムが提供する項目は指定できません。

ユーザー定義項目の設定例

Administrator 権限でのログオンを禁止していて、違反があれば危険と判定したい場合を例に、ユーザー定義項目の設定内容を次の表に示します。

ユーザー定義項目		設定例
ユーザー定義項目名		Administrator 権限の禁止
定義内容	機器情報の種別	システム情報
	対象項目	最終ログオンユーザーのユーザー名
	判定条件	判定値と等しい
	判定値	Administrator
	対象項目に値がない場合の動作	安全
不適正時の危険レベル		危険

ユーザー定義項目に設定できる判定条件と判定値

ユーザー定義項目に設定できる判定条件と判定値は、対象項目のデータ型によって異なります。対象項目のデータ型ごとに、設定できる判定条件と判定値を次の表に示します。

対象項目のデータ型	判定条件	判定値
テキスト型	判定値と等しい	文字列 なお、大文字と小文字の違い、および全角と半角の違いは判定時に区別されます。
	判定値と等しくない	
	判定値を含む	
	判定値が前方一致	
	判定値が後方一致	
数値型	判定値と等しい	「0」から「9」の数字、および小数点（.） 単位を選択する場合は、次に示す値 • B（バイト） • KB（キロバイト） • MB（メガバイト） • GB（ギガバイト） • TB（テラバイト） • PB（ペタバイト） • 分
	判定値と等しくない	
	判定値以上	
	判定値以下	
	判定値より大きい	
	判定値より小さい	

対象項目のデータ型	判定条件	判定値
選択型	判定値と等しい	プルダウンメニューに表示される値 なお、大文字と小文字の違い、および全角と半角の違いは判定時に区別されます。
	判定値と等しくない	

ヒント

システム情報またはハードウェア情報の数値型の対象項目（ビデオカードの VRAM 容量やコア数など）に値がない場合は、0 として扱います。この場合、判定結果は対象項目に値がない場合の動作に設定した危険レベルではなく、判定値と 0 を判定条件で判定した結果になります。

(13) ユーザーアカウント単位のセキュリティ判定

OS に複数のユーザーアカウントが存在する場合、一部の OS の設定はユーザーアカウントごとに設定されています。特定の設定項目は、ユーザーアカウントごとにセキュリティ状況を判定できます。これによって、セキュリティに問題のあるユーザーアカウントを抽出し、コンピュータの安全を確保できます。

ユーザーアカウントごとに判定される項目を次に示します。

- パスワードの安全性
- パスワード更新からの経過日数
- スクリーンセーバーのパスワード保護
- スクリーンセーバー起動までの待ち時間

これらの項目では、すべてのユーザーアカウントが適正状態の場合に、機器の危険レベルが「安全」となります。どれか 1 つでもユーザーアカウントに問題があれば、機器の危険レベルは不適正時の危険レベルになります。不適正だった場合、セキュリティ画面の機器のセキュリティ状態には、問題のあるユーザーアカウントが表示されます。また、セキュリティポリシーに自動対策を設定している場合、問題のあるユーザーアカウントだけに対策が実行されます。

重要

次に示す状態のユーザーアカウントは、パスワードの情報を収集できないため、セキュリティ判定の対象外となります。

- 無効化されているユーザーアカウント
- ロックアウトされているユーザーアカウント

また、次に示すユーザーアカウントは、スクリーンセーバーの情報を取得できないため、スクリーンセーバーに関するセキュリティ判定の対象外となります。

- 最後にログインしてから 30 日以上ログインしていないユーザーアカウント

セキュリティポリシーのアクション項目でメッセージ通知を設定している場合は、危険レベルに応じて対策を促すメッセージが自動的に通知されます。メッセージは、すべてのユーザーアカウントに通知されます。ただし、ユーザーアカウントごとに判定される項目については、問題のあるユーザーアカウントだけに対策を促す説明が追記されます。

(14) サポートするウィルス対策製品

JP1/IT Desktop Management 2 では、ここで示すウィルス対策製品をサポートしています。ここで示すウィルス対策製品だけがセキュリティ状況の判定の対象になります。

重要

ここで示す製品およびバージョンは、このマニュアルの対象製品をリリースした時点のものです。

サポートするウィルス対策製品の最新情報は、サポートサービスサイトで確認できます。

ヒント

ここで示す製品のバージョンは［機器情報］画面の［インストールソフトウェア情報］タブで確認できます。

ヒント

サポート対象外のウィルス対策製品はセキュリティ状況を判定できません。ただし、セキュリティポリシーの使用必須ソフトウェアに登録することで、インストールの有無を判定できます。

情報を収集できるウィルス対策製品

日本語版のウィルス対策製品

製品名・バージョンなど			操作画面上で表示される名称
Norton AntiVirus※1、※2、※3	2005		Norton AntiVirus 2005
	2006		Norton AntiVirus 2006
	2007		Norton AntiVirus 2007
	2008	32bit	Norton AntiVirus 2008
		64bit	Norton AntiVirus 2008 64bit
	2009	32bit	Norton AntiVirus 2009
		64bit	Norton AntiVirus 2009 64bit
	2010	32bit	Norton AntiVirus 2010
		64bit	Norton AntiVirus 2010 64bit

製品名・バージョンなど			操作画面上で表示される名称
Norton AntiVirus※1、※2、※3	2011	32bit	Norton AntiVirus 2011
		64bit	Norton AntiVirus 2011 64bit
	2012	32bit	Norton AntiVirus 2012
		64bit	Norton AntiVirus 2012 64bit
	32bit		Norton AntiVirus
	64bit		Norton AntiVirus 64bit
	2014	32bit	Norton AntiVirus 2014
		64bit	Norton AntiVirus 2014 64bit
Symantec AntiVirus Corporate Edition	10.0	32bit	Symantec AntiVirus Corporate Edition 10.0
		64bit	Symantec AntiVirus 64bit
	10.1	32bit	Symantec AntiVirus Corporate Edition 10.1
		64bit	Symantec AntiVirus 64bit
	10.2	32bit	Symantec AntiVirus Corporate Edition 10.2
		64bit	Symantec AntiVirus 64bit
Symantec Client Security	3.0	32bit	Symantec Client Security
		64bit	Symantec AntiVirus 64bit
	3.1	32bit	Symantec Client Security
		64bit	Symantec AntiVirus 64bit
Symantec Endpoint Protection	11.0	32bit	Symantec Endpoint Protection 11.0
		64bit	Symantec Endpoint Protection 11.0 64bit
	12.1（12.1.4）	32bit	Symantec Endpoint Protection 12.1
		64bit	Symantec Endpoint Protection 12.1 64bit
	12.1.5	32bit	Symantec Endpoint Protection 12.1
		64bit	Symantec Endpoint Protection 12.1 64bit
	12.1.6 MP5	32bit	Symantec Endpoint Protection 12.1
		64bit	Symantec Endpoint Protection 12.1 64bit
	14.0	32bit	Symantec Endpoint Protection 14.0
		64bit	Symantec Endpoint Protection 14.0 64bit
	14.0.0 MP2	32bit	Symantec Endpoint Protection 14.0
		64bit	Symantec Endpoint Protection 14.0 64bit

製品名・バージョンなど			操作画面上で表示される名称
McAfee Total Protection Service※2、※3	5.0		McAfee Total Protection Service
McAfee SaaS Endpoint Protection※3	5.2		McAfee SaaS Endpoint Protection
	6.0	32bit	McAfee SaaS Endpoint Protection
		64bit	McAfee SaaS Endpoint Protection 64bit
McAfee VirusScan Enterprise	8.5i	32bit	McAfee VirusScan Enterprise 8.5i
		64bit	McAfee VirusScan Enterprise 8.5i 64bit
	8.7i	32bit	McAfee VirusScan Enterprise 8.7i
		64bit	McAfee VirusScan Enterprise 8.7i 64bit
	8.8、8.8 Patch 8	32bit	McAfee VirusScan Enterprise 8.8
		64bit	McAfee VirusScan Enterprise 8.8 64bit
McAfee Endpoint Security ※2、※3、※4	10.1	32bit	McAfee Endpoint Security 10.1
		64bit	McAfee Endpoint Security 10.1 64bit
	10.2	32bit	McAfee Endpoint Security 10.2
		64bit	McAfee Endpoint Security 10.2 64bit
	10.5	32bit	McAfee Endpoint Security 10.5
		64bit	McAfee Endpoint Security 10.5 64bit
ウイルスバスター	2011 クラウド※3	32bit	ウイルスバスター 2011 クラウド
		64bit	ウイルスバスター 2011 クラウド 64bit
	2012 クラウド※3	32bit	ウイルスバスター 2012 クラウド
		64bit	ウイルスバスター 2012 クラウド 64bit
ウイルスバスター クラウド※3	32bit		ウイルスバスター クラウド
	64bit		ウイルスバスター クラウド 64bit
	7.0	32bit	ウイルスバスター クラウド 7.0
		64bit	ウイルスバスター クラウド 7.0 64bit
	8.0	32bit	ウイルスバスター クラウド 8.0
		64bit	ウイルスバスター クラウド 8.0 64bit
	11.0	32bit	ウイルスバスター クラウド 11.0
		64bit	ウイルスバスター クラウド 11.0 64bit
	12.0※1	32bit	ウイルスバスター クラウド 12.0
		64bit	ウイルスバスター クラウド 12.0 64bit

製品名・バージョンなど			操作画面上で表示される名称
ウイルスバスター コーポレートエディション	8.0※3、10.0※3、10.5※5、10.6、11.0、11.0 SP1 Critical Patch 6077、11.0 SP1 Critical Patch 6206、XG Critical Patch 1440、XG SP1	32bit	OS が 32 ビット版の Windows の場合 ウイルスバスター Corp. OS が 64 ビット版の Windows の場合 ウイルスバスター Corp. 64bit
		64bit	
ウイルスバスター コーポレートエディション アドバンス	8.0※3、10.0※3	32bit	
		64bit	
ウイルスバスター コーポレートエディション サーバ版	8.0※3、10.0※3	32bit	
		64bit	
ウイルスバスター コーポレートエディション サーバ版 アドバンス	8.0※3、10.0※3	32bit	
		64bit	
ウイルスバスター ビジネスセキュリティサービス	5.7.1193	32bit	ビジネスセキュリティサービス
		64bit	ビジネスセキュリティサービス 64bit
Trend Micro ビジネスセキュリティ※3	6.0	32bit	OS が 32 ビット版の Windows の場合 ビジネスセキュリティクライアント OS が 64 ビット版の Windows の場合 ビジネスセキュリティクライアント 64bit
		64bit	
ウイルスバスター ビジネスセキュリティ※3	7.0	32bit	
		64bit	
	9.0、9.0 SP3、9.0 SP3 Critical Patch 4340、9.5	32bit	
		64bit	
ServerProtect for Windows NT/NetWare※6	5.7	32bit	OS が 32 ビット版の Windows の場合 ServerProtect OS が 64 ビット版の Windows の場合 ServerProtect 64bit
		64bit	
	5.8	32bit	
		64bit	
Forefront Client Security※3	1.5.1937.14、1.5.1993.0、1.5.1996.1	32bit	Forefront Client Security
		64bit	Forefront Client Security 64bit
Kaspersky Open Space Security Server※7	6.0.4	32bit	Kaspersky Anti-Virus 6.0 for Windows Servers
		64bit	Kaspersky Anti-Virus 6.0 for Windows Servers 64bit
Kaspersky Open Space Security Workstation※7	6.0.4	32bit	Kaspersky Anti-Virus 6.0 for Windows Workstations

製品名・バージョンなど			操作画面上で表示される名称
Kaspersky Open Space Security Workstation※7	6.0.4	64bit	Kaspersky Anti-Virus 6.0 for Windows Workstations 64bit
Kaspersky Endpoint Security 8 for Windows※7	8	32bit	OS が 32 ビット版の Windows の場合 Kaspersky Endpoint Security 8 for Windows OS が 64 ビット版の Windows の場合 Kaspersky Endpoint Security 8 for Windows 64bit
		64bit	
	8.1	32bit	
		64bit	
Kaspersky Endpoint Security 10 for Windows※2、※7	10.2、SP1 (10.2.4.674)	32bit	OS が 32 ビット版の Windows の場合 Kaspersky Endpoint Security 10 for Windows OS が 64 ビット版の Windows の場合 Kaspersky Endpoint Security 10 for Windows 64bit
		64bit	
ESET Endpoint アンチウイルス※1、※2、※3	5.0	32bit	ESET Endpoint アンチウイルス
		64bit	ESET Endpoint アンチウイルス 64bit
ESET File Security for Microsoft Windows Server※1、※2、※3	4.5	32bit	ESET File Security for Microsoft Windows Server
		64bit	ESET File Security for Microsoft Windows Server 64bit
ESET NOD32 Antivirus※1、※2、※3	4.0	32bit	OS が 32 ビット版の Windows の場合 ESET NOD32 Antivirus OS が 64 ビット版の Windows の場合 ESET NOD32 Antivirus 64bit
		64bit	
	4.2	32bit	
		64bit	
	5.0	32bit	
		64bit	
	5.2	32bit	
		64bit	
	6.0	32bit	
		64bit	
	7.0	32bit	
		64bit	
	8.0	32bit	
		64bit	
Sophos Endpoint Security and Data Protection	9.0	32bit	OS が 32 ビット版の Windows の場合 Sophos Anti-Virus
		64bit	

製品名・バージョンなど			操作画面上で表示される名称
Sophos Endpoint Security and Data Protection	9.5	32bit	OS が 64 ビット版の Windows の場合 Sophos Anti-Virus 64bit
		64bit	
Sophos Security Suite small business solutions	4.0	32bit	
Sophos Computer Security small business solutions		64bit	
Sophos Anti-Virus small business solutions			
Sophos Endpoint Protection - Enterprise	10	32bit	
		64bit	
Sophos Endpoint Protection - Advanced		32bit	
		64bit	
Sophos Endpoint Protection - Basic		32bit	
		64bit	
Sophos Endpoint Security and Control for Windows	10.3	32bit	
		64bit	
	10.3.7	32bit	OS が 32 ビット版の Windows の場合 Sophos Anti-Virus 10.3.7 OS が 64 ビット版の Windows の場合 Sophos Anti-Virus 10.3.7 64bit
		64bit	
	10.3.11	32bit	OS が 32 ビット版の Windows の場合 Sophos Anti-Virus 10.3.11 OS が 64 ビット版の Windows の場合 Sophos Anti-Virus 10.3.11 64bit
		64bit	
	10.3.13	32bit	Sophos Anti-Virus 10.3.13
		64bit	Sophos Anti-Virus 10.3.13 64bit
	10.6.3.537、10.7	32bit	Sophos Anti-Virus 10
		64bit	Sophos Anti-Virus 10 64bit
F-Secure Client Security※1、※2、※3	9.0	32bit	OS が 32 ビット版の Windows の場合 F-Secure Client Security OS が 64 ビット版の Windows の場合 F-Secure Client Security 64bit
		64bit	
	9.1	32bit	
		64bit	
	9.11	32bit	

製品名・バージョンなど			操作画面上で表示される名称
F-Secure Client Security※1、※2、※3	9.11	64bit	OS が 32 ビット版の Windows の場合 F-Secure Client Security OS が 64 ビット版の Windows の場合 F-Secure Client Security 64bit
	9.20	32bit	
		64bit	
	9.31	32bit	
		64bit	
	9.32	32bit	
		64bit	
	11.50	32bit	
		64bit	
	11.60	32bit	
		64bit	

注※1　ウィルス検索エンジンのバージョンは収集できません。

注※2　自動保護（常駐設定）の状態は収集できません。

注※3　ウィルススキャン最終完了日時は収集できません。

注※4　McAfee Endpoint Security をインストールする時のインストールオプションで［Threat Prevention］を選択した場合にセキュリティ情報が取得できます。なお、McAfee Endpoint Security のインストール直後は情報を取得できません。また、McAfee Endpoint Security の定義を更新した直後も最新の情報は取得できません。最新の情報を取得するには、McAfee Endpoint Security の定義を更新したあと、エージェントの OS を再起動してください。

注※5　Patch1 以降を適用している場合だけ、ウィルススキャン最終完了日時が収集できます。

注※6　スキャンを実行中にキャンセルした場合、キャンセルした日時がウィルススキャン最終完了日時として収集されます。

注※7　完全スキャンを実行する場合に「すべてのハードディスク」、「システムメモリ」および「スタートアップオブジェクト」をスキャンしたときだけ、ウィルススキャン最終完了日時が収集できます。

英語版のウィルス対策製品

製品名・バージョンなど			操作画面上で表示される名称
Norton AntiVirus※1、※2、※3	2010	32bit	Norton AntiVirus 2010
		64bit	Norton AntiVirus 2010 64bit
	2011	32bit	Norton AntiVirus 2011
		64bit	Norton AntiVirus 2011 64bit
	32bit		Norton AntiVirus
	64bit		Norton AntiVirus 64bit

製品名・バージョンなど			操作画面上で表示される名称
Symantec AntiVirus Corporate Edition	10.0	32bit	Symantec AntiVirus Corporate Edition 10.0
		64bit	Symantec AntiVirus 64bit
	10.1	32bit	Symantec AntiVirus Corporate Edition 10.1
		64bit	Symantec AntiVirus 64bit
	10.2	32bit	Symantec AntiVirus Corporate Edition 10.2
		64bit	Symantec AntiVirus 64bit
Symantec Client Security	3.0	32bit	Symantec Client Security
		64bit	Symantec AntiVirus 64bit
	3.1	32bit	Symantec Client Security
		64bit	Symantec AntiVirus 64bit
Symantec Endpoint Protection	11.0	32bit	Symantec Endpoint Protection 11.0
		64bit	Symantec Endpoint Protection 11.0 64bit
	12.1	32bit	Symantec Endpoint Protection 12.1
		64bit	Symantec Endpoint Protection 12.1 64bit
	12.1.4	32bit	Symantec Endpoint Protection 12.1
		64bit	Symantec Endpoint Protection 12.1 64bit
	12.1.5	32bit	Symantec Endpoint Protection 12.1
		64bit	Symantec Endpoint Protection 12.1 64bit
	12.1.6 MP5	32bit	Symantec Endpoint Protection 12.1
		64bit	Symantec Endpoint Protection 12.1 64bit
	14.0	32bit	Symantec Endpoint Protection 14.0
		64bit	Symantec Endpoint Protection 14.0 64bit
	14.0.0 MP2	32bit	Symantec Endpoint Protection 14.0
		64bit	Symantec Endpoint Protection 14.0 64bit
McAfee Total Protection Service ※2、※3	5.0		McAfee Total Protection Service
McAfee SaaS Endpoint Protection※3	5.2		McAfee SaaS Endpoint Protection
	6.0	32bit	McAfee SaaS Endpoint Protection
		64bit	McAfee SaaS Endpoint Protection 64bit
McAfee VirusScan Enterprise	8.5i	32bit	McAfee VirusScan Enterprise 8.5i
		64bit	McAfee VirusScan Enterprise 8.5i 64bit

製品名・バージョンなど			操作画面上で表示される名称
McAfee VirusScan Enterprise	8.7i	32bit	McAfee VirusScan Enterprise 8.7i
		64bit	McAfee VirusScan Enterprise 8.7i 64bit
	8.8、8.8 Patch 7	32bit	McAfee VirusScan Enterprise 8.8
		64bit	McAfee VirusScan Enterprise 8.8 64bit
McAfee Endpoint Security※2、※3、※4	10.1	32bit	McAfee Endpoint Security 10.1
		64bit	McAfee Endpoint Security 10.1 64bit
	10.5	32bit	McAfee Endpoint Security 10.5
		64bit	McAfee Endpoint Security 10.5 64bit
PC-cillin	2010	32bit	PC-cillin 2010
		64bit	PC-cillin 2010 64bit
Titanium Internet Security※3	2011	32bit	Titanium Internet Security 2011
		64bit	Titanium Internet Security 2011 64bit
	2012	32bit	Titanium Internet Security 2012
		64bit	Titanium Internet Security 2012 64bit
	2013	32bit	Titanium Internet Security 2013
		64bit	Titanium Internet Security 2013 64bit
	2015	32bit	Titanium Internet Security 2015
		64bit	Titanium Internet Security 2015 64bit
	2017	32bit	Titanium Internet Security 2017
		64bit	Titanium Internet Security 2017 64bit
	2018※1	32bit	Titanium Internet Security 2018
		64bit	Titanium Internet Security 2018 64bit
Worry-Free Business Security-Standard	7.0※1、※2、※3、※5、8.0※3、9.0 SP3※3、9.0 SP3 Patch 1※3、9.0 SP3 Critical Patch 4340※3、9.5※3	32bit	OS が 32 ビット版の Windows の場合 Worry-Free Business Security OS が 64 ビット版の Windows の場合 Worry-Free Business Security 64bit
		64bit	
Worry-Free Business Security-Advanced	7.0※1、※2、※3、※5、8.0※3、9.0 SP3※	32bit	
		64bit	

製品名・バージョンなど			操作画面上で表示される名称
Worry-Free Business Security-Advanced	[3]、9.0 SP3 Patch 1※3、9.0 SP3 Critical Patch 4340※3、9.5※3	64bit	OS が 32 ビット版の Windows の場合 Worry-Free Business Security OS が 64 ビット版の Windows の場合 Worry-Free Business Security 64bit
OfficeScan Corporate Edition	8.0※3、10※3、10.5※6、10.6、11.0、11.0 SP1、XG、XG Critical Patch 1556、XG SP1	32bit	OS が 32 ビット版の Windows の場合 OfficeScan Corp. OS が 64 ビット版の Windows の場合 OfficeScan Corp. 64bit
		64bit	
ServerProtect for Windows NT/Netware	5.7	32bit	OS が 32 ビット版の Windows の場合 ServerProtect OS が 64 ビット版の Windows の場合 ServerProtect 64bit
		64bit	
	5.8	32bit	
		64bit	
Forefront Client Security※3	1.5.1937.14、1.5.1993.0、1.5.1996.1	32bit	Forefront Client Security
		64bit	Forefront Client Security 64bit
Kaspersky Open Space Security Server	6.0.3※1、※2、※3、6.0.4※7	32bit	Kaspersky Anti-Virus 6.0 for Windows Servers
		64bit	Kaspersky Anti-Virus 6.0 for Windows Servers 64bit
Kaspersky Open Space Security Workstation		32bit	Kaspersky Anti-Virus 6.0 for Windows Workstations
		64bit	Kaspersky Anti-Virus 6.0 for Windows Workstations 64bit
Kaspersky Endpoint Security 8 for Windows※7	8、8.1	32bit	OS が 32 ビット版の Windows の場合 Kaspersky Endpoint Security 8 for Windows OS が 64 ビット版の Windows の場合 Kaspersky Endpoint Security 8 for Windows 64bit
		64bit	
Kaspersky Endpoint Security 10 for Windows※2、※7	10.2、SP1 (10.2.4.674)、10.3.0.6294	32bit	OS が 32 ビット版の Windows の場合 Kaspersky Endpoint Security 10 for Windows OS が 64 ビット版の Windows の場合 Kaspersky Endpoint Security 10 for Windows 64bit
		64bit	

製品名・バージョンなど			操作画面上で表示される名称
ESET NOD32 Antivirus※1、※2、※3	4.0、4.2、5.0、5.2	32bit	ESET NOD32 Antivirus
		64bit	ESET NOD32 Antivirus 64bit
ESET Endpoint Antivirus※1、※2、※3	6.5	32bit	ESET Endpoint Antivirus
		64bit	ESET Endpoint Antivirus 64bit
Sophos Endpoint Security and Data Protection	9.0、9.5	32bit	OS が 32 ビット版の Windows の場合 Sophos Anti-Virus OS が 64 ビット版の Windows の場合 Sophos Anti-Virus 64bit
		64bit	
Sophos Security Suite small business solutions	4.0	32bit	
Sophos Computer Security small business solutions		64bit	
Sophos Anti-Virus small business solutions			
Sophos Endpoint Protection - Enterprise	10	32bit	
		64bit	
Sophos Endpoint Protection - Advanced	10	32bit	
		64bit	
Sophos Endpoint Protection - Basic	10	32bit	
		64bit	
Sophos Endpoint Security and Control for Windows	10.3.7	32bit	OS が 32 ビット版の Windows の場合 Sophos Anti-Virus 10.3.7 OS が 64 ビット版の Windows の場合 Sophos Anti-Virus 10.3.7 64bit
		64bit	
	10.3.11	32bit	OS が 32 ビット版の Windows の場合 Sophos Anti-Virus 10.3.11 OS が 64 ビット版の Windows の場合 Sophos Anti-Virus 10.3.11 64bit
		64bit	
F-Secure Client Security※1、※2、※3	9.0、9.31、9.32	32bit	OS が 32 ビット版の Windows の場合 F-Secure Client Security OS が 64 ビット版の Windows の場合 F-Secure Client Security 64bit
		64bit	
Avira Professional Security※2、※8、※9	14.0.4	32bit	OS が 32 ビット版の Windows の場合 Avira Professional Security OS が 64 ビット版の Windows の場合 Avira Professional Security 64bit
		64bit	
	14.0.7	32bit	
		64bit	

注※1　ウィルス検索エンジンのバージョンは収集できません。

注※2　自動保護（常駐設定）の状態は収集できません。

注※3　ウィルススキャン最終完了日時は収集できません。

注※4　McAfee Endpoint Security をインストールする時のインストールオプションで［Threat Prevention］を選択した場合にセキュリティ情報が取得できます。なお、McAfee Endpoint Security のインストール直後は情報を取得できません。また、McAfee Endpoint Security の定義を更新した直後も最新の情報は取得できません。最新の情報を取得するには、McAfee Endpoint Security の定義を更新したあと、エージェントの OS を再起動してください。

注※5　ウィルス定義ファイルのバージョンは収集できません。

注※6　Patch1 以降を適用している場合だけ、ウィルススキャン最終完了日時が収集できます。

注※7　完全スキャンを実行する場合に「すべてのハードディスク」、「システムメモリ」および「スタートアップオブジェクト」をスキャンしたときだけ、ウィルススキャン最終完了日時が収集できます。

注※8　「Manual Update」を実行した場合、情報が更新されません。「Manual Update」後にダウンロードによるアップデートを実行した場合に、バージョンが「Manual Update」時と変わらないときも、同様に更新されません。

注※9　次の Profile でスキャンした場合に情報が更新されます。

- Local Drives
- Local Hard Disks
- Complete system scan

中国語版のウィルス対策製品

製品名・バージョンなど			操作画面上で表示される名称
Symantec Endpoint Protection	11.0	32 bit	Symantec Endpoint Protection 11.0
		64 bit	Symantec Endpoint Protection 11.0 64bit
	12.1	32 bit	Symantec Endpoint Protection 12.1
		64 bit	Symantec Endpoint Protection 12.1 64bit
McAfee SaaS Endpoint Protection※1	5.2		McAfee SaaS Endpoint Protection
McAfee VirusScan Enterprise	8.7i	32 bit	McAfee VirusScan Enterprise 8.7i
		64 bit	McAfee VirusScan Enterprise 8.7i 64bit
	8.8	32 bit	McAfee VirusScan Enterprise 8.8
		64 bit	McAfee VirusScan Enterprise 8.8 64bit
OfficeScan Corporate Edition	10.0、10.5、10.6	32 bit	趋势科技防毒墙网络版客户机
		64 bit	趋势科技防毒墙网络版客户机 64bit
ServerProtect For Microsoft Windows/Novell NetWare	5.7、 5.8	32 bit	ServerProtect
		64 bit	ServerProtect 64 bit
Kaspersky Endpoint Security 8 for Windows	8.1	32 bit	Kaspersky Endpoint Security 8 for Windows
		64 bit	Kaspersky Endpoint Security 8 for Windows 64bit

製品名・バージョンなど			操作画面上で表示される名称
卡巴斯基 网络版 Server	6.0.3※1、※2、※3	Server 32 bit	卡巴斯基反病毒 6.0 Windows 服务器
		Server 64 bit	卡巴斯基反病毒 6.0 Windows 服务器 64bit
		Workstation 32 bit	卡巴斯基反病毒 6.0 Windows 工作站
		Workstation 64 bit	卡巴斯基反病毒 6.0 Windows 工作站 64bit
	6.0.4	Server 32 bit	卡巴斯基反病毒 6.0 Windows 服务器
		Server 64 bit	卡巴斯基反病毒 6.0 Windows 服务器 64bit
		Workstation 32 bit	卡巴斯基反病毒 6.0 Windows 工作站
		Workstation 64 bit	卡巴斯基反病毒 6.0 Windows 工作站 64bit
瑞星杀毒软件网络版※1、※2、※3、※4	2010、2011、2012	32 bit	瑞星杀毒软件网络版
		64 bit	瑞星杀毒软件网络版 64bit
金山毒霸※1、※2、※4	2011	32 bit	金山毒霸 2011
		64 bit	金山毒霸 2011 64bit
	2012	32 bit	金山毒霸 2012
		64 bit	金山毒霸 2012 64bit
新毒霸※1、※2、※4	2013	32 bit	新毒霸 2013
		64 bit	新毒霸 2013 64bit

製品名・バージョンなど			操作画面上で表示される名称
江民杀毒软件	KV2010	32 bit	江民杀毒软件 2010※4
		64 bit	江民杀毒软件 2010 64bit※3、※4
	KV2011	32 bit	江民杀毒软件 2011※4
		64 bit	江民杀毒软件 2011 64bit※3、※4
江民速智版杀毒软件※4	32 bit		江民速智版杀毒软件
	64 bit		江民速智版杀毒软件 64bit

注※1　ウィルススキャン最終完了日時は収集できません。
注※2　ウィルス検索エンジンのバージョンは収集できません。
注※3　ウィルス定義ファイルのバージョンは収集できません。
注※4　自動保護（常駐設定）の状態は収集できません。

ウィルス対策製品の自動保護（常駐設定）の判定条件

ウィルス対策製品からは、一部の製品を除いて自動保護（常駐設定）の状態を収集できます。常駐・非常駐の状態は、ウィルス対策製品の設定によって判定されます。ウィルス対策製品の常駐・非常駐の判定条件を次に示します。

日本語版のウィルス対策製品

製品名	常駐・非常駐の判定条件
Norton AntiVirus	－
Symantec AntiVirus Corporate Edition	[Auto-Protect を有効にする] がオンの場合に常駐となる。
Symantec Client Security	
Symantec Endpoint Protection	[ファイルシステム Auto-Protect を有効にする] がオンの場合に常駐となる。
McAfee Total Protection Service	－
McAfee SaaS EndpointProtection	[オンアクセススキャン] が「有効」の場合に常駐となる。
McAfee VirusScan Enterprise	[システム起動時にオンアクセス スキャンを有効にする] がオンの場合に常駐となる。
ウイルスバスター	[ウイルス/スパイウェアの監視] がオンの場合に常駐となる。
ウイルスバスター クラウド	[リアルタイムスキャン] がオンの場合に常駐となる。

製品名	常駐・非常駐の判定条件
ウイルスバスター コーポレートエディション	ウイルスバスター コーポレートエディションの管理サーバの［リアルタイム検索の設定］－［ウイルス/不正プログラム検索を有効にする］（バージョン 8.0 の場合は［ウィルス検索を有効にする］、バージョン 10.0 の場合は［リアルタイム検索を有効にする］）をオフにして、クライアントに設定を適用した場合、クライアントのリアルタイム検索が停止する。このとき、非常駐となる。
ウイルスバスター コーポレートエディション アドバンス	ウイルスバスター コーポレートエディションの管理サーバの［リアルタイム検索の設定］－［リアルタイム検索を有効にする］（バージョン 8.0 の場合は［ウィルス検索を有効にする］）をオフにして、クライアントに設定を適用した場合、クライアントのリアルタイム検索が停止する。このとき、非常駐となる。
ウイルスバスター コーポレートエディション サーバ版	
ウイルスバスター コーポレートエディション サーバ版 アドバンス	
ビジネスセキュリティ	セキュリティ設定で［リアルタイムのウイルス対策/スパイウェア対策を有効にする］をオフにしてコンピュータに割り当てた場合、コンピュータのリアルタイム検索が停止する。このとき、非常駐となる。
ServerProtect for Windows NT/Netware	インフォメーションサーバの［リアルタイム検索］－［リアルタイム検索を有効にする］をオフにして一般サーバに設定すると、一般サーバのリアルタイム検索が停止する。このとき、非常駐となる。
Forefront Client Security	［リアルタイム保護を使用する］がオンの場合に常駐となる。
Kaspersky Open Space Security Server	［プロテクションを有効にする］がオンの場合に常駐となる。
Kaspersky Open Space Security Workstation	［プロテクションを有効にする］がオンの場合に常駐となる。
Kaspersky Endpoint Security 8 for Windows	［プロテクションとコントロールの一時停止］の［一時停止］がオフの場合に常駐となる。
Kaspersky Endpoint Security 10 for Windows	－
ESET Endpoint アンチウイルス	－
ESET File Security for Microsoft Windows Server	－
ESET NOD32 Antivirus	－
Sophos Endpoint Security and Data Protection	［このコンピュータでオンアクセス検索を実行する］がオンの場合に常駐となる。
Sophos Security Suite small business solutions	
Sophos Computer Security small business solutions	

製品名	常駐・非常駐の判定条件
Sophos Anti-Virus small business solutions	[このコンピュータでオンアクセス検索を実行する] がオンの場合に常駐となる。
Sophos Endpoint Protection - Enterprise	
Sophos Endpoint Protection - Advanced	
Sophos Endpoint Protection - Basic	
Sophos Endpoint Security and Control for Windows	
F-Secure Client Security	－

（凡例）－：常駐・非常駐の状態は収集できない

英語版のウィルス対策製品

製品名	常駐・非常駐の判定条件
Norton AntiVirus	－
Symantec AntiVirus Corporate Edition	[Enable Auto-Protect] がオンの場合に常駐となる。
Symantec Client Security	
Symantec Endpoint Protection	[Enable File System Auto-Protect] がオンの場合に常駐となる。
McAfee Total Protection Service	－
McAfee SaaS EndpointProtection	[On-access scanning] がオンの場合に常駐となる。
McAfee VirusScan Enterprise	[Enable on-access scanning at system startup] がオンの場合に常駐となる。
PC-cillin	[Protection Against Viruses & Spyware] がオンの場合に常駐となる。
Titanium Internet Security	
Worry-Free Business Security-Standard	バージョン 8.0 の場合、[Enable real-time Antivirus/Anti-spyware] がオンのときに常駐となる。
Worry-Free Business Security-Advanced	
OfficeScan Corporate Edition	バージョン 8.0、10、10.5、10.5 Patch1、11.0 の場合は、[Enable virus/malware scan] がオンのときに常駐となる。バージョン 10.6 の場合は、管理サーバの [Real-time Scan Settings] － [Enable virus/malware scan] をオフにしてクライアントに設定を適用すると、クライアントのリアルタイム検索が停止する。このとき、非常駐となる。

製品名	常駐・非常駐の判定条件
ServerProtect for Windows NT/Netware	インフォメーションサーバの［Real-time Scan］－［Enable Real-time Scan］をオフにして一般サーバに設定すると、一般サーバのリアルタイム検索が停止する。このとき、非常駐となる。
Forefront Client Security	［Use real time protection］がオンの場合に常駐となる。
Kaspersky Open Space Security Server	バージョン 6.0.3 の場合は［Enable File Anti-Virus］、バージョン 6.0.4 の場合は［Enable protection］がオンのときに常駐となる。
Kaspersky Open Space Security Workstation	バージョン 6.0.3 の場合は［Enable File Anti-Virus］、バージョン 6.0.4 の場合は［Enable protection］がオンのときに常駐となる。
Kaspersky Endpoint Security 8 for Windows	［Pause protection and control］の［Pause］がオフの場合に常駐となる。
Kaspersky Endpoint Security 10 for Windows	－
ESET NOD32 Antivirus	－
Sophos Endpoint Security and Data Protection	［Enable on-access scanning for this computer］がオンの場合に常駐となる。
Sophos Security Suite small business solutions	
Sophos Computer Security small business solutions	
Sophos Anti-Virus small business solutions	
Sophos Endpoint Protection - Enterprise	
Sophos Endpoint Protection - Advanced	
Sophos Endpoint Protection - Basic	
F-Secure Client Security	－
Avira Professional Security	－

（凡例）－：常駐・非常駐の状態は収集できない

中国語版のウィルス対策製品

製品名	常駐・非常中の判定条件
Symantec Endpoint Protection	［启用文件系统自动防护］がオンの場合に常駐となる。
McAfee SaaS Endpoint Protection	［按访问扫描］がオンの場合に常駐となる。
McAfee VirusScan Enterprise	［启用在系统启动时进行按访问扫描］がオンの場合に常駐となる。
OfficeScan Corporate Edition	バージョン8.0、10、10.5、10.5Patch1の場合は、［启用病毒/恶意软件扫描］がオンのときに常駐となる。バージョン10.6の場合は、管理サーバの［实时扫描设置］－［启用病毒/恶意软件扫描］をオフにしてクライアントに設定を適用すると、クライアントのリアルタイム検索が停止する。このとき、非常駐となる。
ServerProtect for Microsoft Windows/Novell NetWare	インフォメーションサーバの［实时扫描］－［启用实时扫描］をオフにして一般サーバに設定すると、一般サーバのリアルタイム検索が停止する。このとき、非常駐となる。
Kaspersky Endpoint Security 8 for Windows	［暂停保护和控制］の［暂停］がオフの場合に常駐となる。
卡巴斯基 网络版	［启用保护］がオンの場合に常駐となる。
瑞星杀毒软件网络版	－
金山毒霸	－
新毒霸	－
江民杀毒软件	－
江民速智版杀毒软件	－

（凡例）－：常駐・非常駐の状態は収集できない

ヒント

Sophos 社製のウィルス対策製品では、ウィルス定義ファイルを更新する方法によって、同じウィルス定義ファイルであってもバージョンが異なる場合があるため、同じウィルス定義ファイルを適用していても、ウィルス定義ファイルのバージョンのセキュリティ判定が安全とならない場合があります。Sophos 社製のウィルス対策製品でウィルス定義ファイルのバージョンをセキュリティ判定する場合、セキュリティポリシーを割り当てたすべての機器で、ウィルス定義ファイルの更新を同一の方法で実施するようにしてください。

ヒント

エージェントをアップグレードしていない場合、Sophos 社製のウィルス対策製品のウィルス定義ファイルのバージョンのセキュリティ判定が「不明」になります。Sophos 社製のウィル

ス対策製品でウィルス定義ファイルのバージョンをセキュリティ判定する場合、エージェントをアップグレードしてください。

(15) サポートするウィルス対策製品の情報の更新

サポートするウィルス対策製品の情報は、自動更新またはオフライン更新のどちらかの方法で更新できます。サポートするウィルス対策製品の情報を更新すると、セキュリティポリシーのウィルス対策製品の一覧が最新になり、セキュリティーポリシーの判定対象として新しいウィルス対策製品を選択できるようになります。

サポートするウィルス対策製品の情報を更新したあとは、既存のセキュリティポリシーを編集して判定対象となるウィルス対策製品を選択し直すか、新しいセキュリティポリシーを作成して割り当て直してください。

ウィルス対策製品の情報の自動更新

設定画面の［サポートサービスの設定］画面でサポートサービスサイトに接続するよう設定すると、新しいウィルス対策製品がリリースされてから一定期間後に、サポートサービスサイトからサポート情報ファイルが自動的にダウンロードされて、ウィルス対策製品の情報が更新されます。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。

ウィルス対策製品の情報のオフライン更新

サポートサービスサイトからサポート情報ファイルを手動でダウンロードしたあとで、操作画面またはコマンドでウィルス対策製品の情報をオフライン更新します。管理用サーバの環境がサポートサービスサイトと接続できない場合は、この方法で更新します。

操作画面からオフライン更新する

セキュリティ画面の［更新プログラム一覧］画面、資産画面の［管理ソフトウェア一覧］画面、および機器画面の［ソフトウェア一覧］画面の操作メニューから更新できます。

コマンドを実行してオフライン更新する

updatesupportinfo コマンドを実行して更新できます。

(16) セキュリティ状況の判定対象からの除外

次のセキュリティ設定項目は、OS に複数のユーザーアカウントがある場合、ユーザーアカウントごとにセキュリティ状況が判定されます。

- パスワードの安全性
- 無期限パスワード
- パスワード更新からの経過日数
- スクリーンセーバーのパスワード保護
- スクリーンセーバーの起動待ち時間

OS のコンポーネントや特定のプログラムによっては、OS のユーザーアカウントが自動作成される場合があります。実際にコンピュータを利用していないユーザーアカウントのセキュリティ状況まで判定されてしまうと、セキュリティ状況を正しく管理できないおそれがあります。

このような場合に、「判定除外ユーザー設定ファイル」を作成することで、特定のユーザーアカウントが判定されないように設定できます。

ヒント

自動的に作成されるユーザーアカウントのうち一部のものは、JP1/IT Desktop Management 2 が自動的に判定の対象外とします。セキュリティ状況を確認した際に、不明なユーザーアカウントが判定されていたとき、判定除外ユーザー設定ファイルを作成してください。

(17) セキュリティ状況の判定除外ユーザー設定ファイルの形式

ファイル名は、「jdn_except_users.dat」としてください。

ファイル作成後は、*JP1/IT Desktop Management 2 - Manager のインストールフォルダ*¥mgr¥conf に置いてください。

判定除外ユーザー設定ファイルは、次の形式で作成してください。

OS のユーザーアカウント名 1

OS のユーザーアカウント名 2

1 行に 1 つのユーザーアカウント名を指定してください。複数のユーザーアカウントを指定する場合は、複数行で指定できます。

ユーザーアカウント名の前後に半角スペースが含まれている場合、半角スペースは無視されます。

ユーザーアカウント名は 20 文字以内の半角英数字および記号で指定してください。ただし、次の記号は使えません。

「“」、「/」、「¥」、「[」、「]」、「:」、「;」、「|」、「=」、「,」、「+」、「*」、「?」、「<」、「>」

また、「.」（ピリオド）または半角スペースだけを指定することはできません。

ヒント

「HOGE*」のように、末尾に「*」を指定した前方一致でユーザーアカウント名を指定できます。「*」は末尾だけに指定できます。ユーザーアカウント名に「*」だけを指定した場合は無視されます。

2.9.4　セキュリティポリシーの管理

セキュリティ画面の［セキュリティポリシー］画面で、セキュリティポリシーを作成して管理します。ここでは、セキュリティポリシーの管理について説明します。

セキュリティポリシーを作成する

組織のセキュリティ方針を基にセキュリティポリシーを作成します。セキュリティポリシーは複数作成できます。部署ごとに異なるセキュリティポリシーを作成したり、特別な管理が必要なコンピュータ用のセキュリティポリシーを作成したりできます。

オフライン環境のコンピュータに適用するセキュリティポリシーは、［セキュリティポリシー］画面の操作メニュー［オフライン用ポリシー適用ツールを生成する］から生成できます。詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のオフライン管理のコンピュータにセキュリティポリシーを適用する手順の説明を参照してください。

セキュリティポリシーをコンピュータに割り当てる

コンピュータのセキュリティ状況を把握するためには、作成したセキュリティポリシーをコンピュータまたはグループに割り当てる必要があります。

セキュリティポリシーを編集する

セキュリティトレンドが変化したり、組織のセキュリティ方針が変更になった場合は、セキュリティポリシーを編集します。セキュリティトレンドは、コンピュータやネットワークの環境とともに変化しています。常にセキュリティトレンドを組織内に取り込み続けることで、強固なセキュリティ状況の管理を実現できます。

セキュリティポリシーを削除する

管理体制の変更やセキュリティポリシーの統合に伴って、不要になったセキュリティポリシーがある場合は削除します。

重要

UNIX エージェントは、セキュリティポリシーによる管理の対象外です。自動対策もできません。なお、ネットワーク接続の制御は手動による操作となります。

Mac エージェントは、セキュリティポリシーによる管理の対象です。ただし、自動対策はできません。ネットワーク接続の制御は、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。

オフライン環境のコンピュータは、セキュリティポリシーによる管理の対象です。ただし、セキュリティポリシーの適用は、外部記憶媒体を利用して、コンピュータに適用する必要があります。手順については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のオフライン管理のコンピュータにセキュリティポリシーを適用する手順の説明を参照してください。

(1)　セキュリティポリシーに設定できる項目

セキュリティポリシーに設定できる項目を次に示します。

セキュリティ設定項目

更新プログラム

自動更新および更新プログラムの適用状況が適正かどうかを判定できます。不適正だった場合に自動的に対策する設定もできます。

ウィルス対策製品

ウィルス対策製品のインストール状況や設定状況が適正かどうかを判定できます。この項目は、判定に必要な情報をコンピュータから収集できる場合に判定されます。

使用ソフトウェア

ソフトウェアのインストール状況が適正かどうかを判定できます。不適正だった場合に自動的に対策する設定もできます。

サービスのセキュリティ設定

特定のサービスの稼働状況が適正かどうかを判定できます。不適正だった場合に自動的に対策する設定もできます。

OS のセキュリティ設定

OS のユーザーアカウントやスクリーンセーバー、共有フォルダの有無などの、OS のセキュリティ設定が適正かどうかを判定できます。不適正だった場合に自動的に対策する設定もできます。

ユーザー定義のセキュリティ設定

セキュリティ設定に関する任意のポリシーを設定して、セキュリティ設定が適正かどうかを任意の判定条件で判定できます。

禁止操作

印刷操作やデバイスの使用、ソフトウェアの起動を抑止できます。また、デバイスの使用を抑止したことを利用者のコンピュータに表示するように設定することもできます。

操作ログ

操作ログの取得対象や不審と見なす操作の条件を設定できます。

禁止操作と操作ログの共通設定

禁止操作と操作ログの、上位システムへの通知間隔や利用者のコンピュータでの保持期間を設定できます。

アクション項目

利用者へのメッセージ通知

セキュリティ状況の判定結果に応じて、自動的にコンピュータにメッセージを通知できます。

ネットワーク接続制御

セキュリティ状況の判定結果に応じて、自動的にコンピュータのネットワーク接続を制御できます。

割り当てグループ

対象の構成

セキュリティポリシーを割り当てるグループを設定できます。個々のコンピュータにセキュリティポリシーを割り当てたい場合は、セキュリティポリシー作成後に、メニューエリアの［機器のセキュリティ状態］画面から割り当てます。

以降では、セキュリティポリシーに設定できる項目の詳細について説明します。

セキュリティ設定項目

設定項目		説明	自動対策
更新プログラム	自動更新	自動更新が有効になっているかどうかを判定できます。 最新の更新プログラムの適用を徹底するためには、自動更新の適用をお勧めします。自動更新が有効になっているかどうかを確認することで、更新プログラムの適用を徹底できます。	○ ※1
	すべての更新プログラムの適用状況	更新プログラムが適用されているかを判定できます。 更新プログラムの適用状況を確認することで、OS が最新状態または適正な状態に保たれているかどうかを管理できます。	○ ※14
	指定した更新プログラムの適用状況		
ウィルス対策製品	インストール	JP1/IT Desktop Management 2 がサポートするウィルス対策製品が導入されているかどうかを判定できます。セキュリティポリシーに設定した製品のうち、どれか 1 つがインストールされていれば導入されていると見なされます。	－
	エンジンバージョン	ウィルスを検知するためのスキャンエンジンのバージョンが最新かどうかを判定できます。 最新バージョンが検出されてから、スキャンエンジンを更新するまでの猶予期間を設定できます。猶予期間内は、古いバージョンでも適正と見なされます。	
	ウィルス定義ファイルのバージョン	ウィルス定義ファイルが最新かどうかを判定できます。 最新バージョンが検出されてから、ウィルス定義ファイルを更新するまでの猶予期間を設定できます。猶予期間内は、古いバージョンでも適正と見なされます。	
	自動保護（常駐設定）	自動保護（常駐設定）の設定が有効かどうかを判定できます。	
	ウィルススキャン最終完了日時	ウィルススキャン最終完了日時が指定した日数（猶予期間）以内かどうかを判定できます。	
使用ソフトウェア	使用必須ソフトウェア	指定したソフトウェアがインストールされているかどうかを判定できます。	○ ※14

設定項目		説明	自動対策
使用ソフトウェア	使用必須ソフトウェア	組織内で規定したソフトウェアのインストール状況を確認することで、環境の統制をチェックできます。使用必須ソフトウェアは複数設定できます。	○ ※14
	使用禁止ソフトウェア	使用を禁止したソフトウェアがインストールされていないかどうかを判定できます。 セキュリティ上問題のあるファイル共有ソフトウェアなどがインストールされていないかを確認することで、情報漏えいを防止できます。使用禁止ソフトウェアは複数設定できます。	○ ※15
サービスのセキュリティ設定※2		使用を禁止したサービスが稼働していないかどうかを判定できます。組織内で規定した使用を禁止したサービスの稼働を確認することで、コンピュータの不正利用をチェックできます。 なお、サービスは複数設定できます。設定したサービスが稼働しているかどうかで判定されます。	○ ※3
OS のセキュリティ設定	Guest アカウント	有効な Guest アカウントがないかどうかを判定できます。 Guest アカウントがあると、誰でもコンピュータを利用できてしまいます。Guest アカウントを使用できないことを確認することで、コンピュータの不正利用を防止できます。	○
	パスワードの安全性※4	脆弱なパスワードが設定されたアカウントがないかどうかを判定できます。 脆弱なパスワードは、簡単に解読されてしまうおそれがあります。脆弱なパスワードが設定されていないことを確認することで、パスワードの解読によるコンピュータへの不正アクセスを防止できます。	−
	無期限パスワード※4	パスワードが無期限に設定されたアカウントがないかどうかを判定します。 同じパスワードが長期間使われると、その分解読されやすくなります。無期限のパスワードが設定されていないか確認することで、パスワードの解読によるコンピュータへの不正アクセスを防止できます。	○
	パスワード更新からの経過日数※4	パスワードの更新経過日数が、設定した日数を超えていないかどうかを判定できます。 同じパスワードが長期間使われると、その分解読されやすくなります。パスワードの使用日数をチェックすることで、パスワードの解読によるコンピュータへの不正アクセスを防止できます。	−
	自動ログオン	自動ログオンが設定されていないかどうかを判定できます。 OS の自動ログオンが設定されていると、ほかのユーザーがコンピュータを起動しただけで不正に利用できてしまいます。自動ログオンが設定されていないかどうかを確認することで、コンピュータの不正利用を防止できます。	○
	パワーオンパスワード	パワーオンパスワードが設定されているかどうかを判定します。また、パワーオンパスワード機能が実装されているかどうかを判定します。 パワーオンパスワードが設定されているかどうかを確認することで、コンピュータの不正利用を防止できます。	−

設定項目		説明	自動対策
OS のセキュリティ設定	スクリーンセーバーのパスワード保護※4	スクリーンセーバーにパスワードによる保護が設定されているかどうかを判定できます。 スクリーンセーバーのパスワード保護を設定していないと、離席時にコンピュータを不正利用されるおそれがあります。スクリーンセーバーのパスワード保護の設定を確認することで、コンピュータの不正利用を防止できます。	○ ※5
	スクリーンセーバー起動までの待ち時間※4	スクリーンセーバーの起動時間が指定した時間以内に設定されているかどうかを判定できます。 パスワード保護されたスクリーンセーバーが起動していない状態でコンピュータが放置されると、その間に不正利用されるおそれがあります。スクリーンセーバーの起動時間の設定を確認することで、コンピュータの不正利用を防止できます。	○ ※5、※6
	共有フォルダ	共有フォルダが設定されていないかどうかを判定できます。 不用意に共有フォルダが設定されていると、コンピュータへ不正アクセスされるおそれがあります。共有フォルダが無効になっているかどうか確認することで、コンピュータへの不正アクセスを防止できます。	○
	管理共有	管理共有が設定されていないかどうかを判定できます。 管理共有が有効になっていると、コンピュータへ不正アクセスされるおそれがあります。管理共有が無効になっているかどうか確認することで、コンピュータへの不正アクセスを防止できます。	○
	匿名接続	制限なしの匿名接続が設定されていないかどうかを判定できます。 制限なしの匿名接続が有効になっていると、コンピュータへ不正アクセスされるおそれがあります。制限なしの匿名接続が無効になっているかどうか確認することで、コンピュータへの不正アクセスを防止できます。	○
	ファイアウォール※7、※8	ファイアウォールが有効になっているかどうか、および実装されているかどうかを判定できます。 ファイアウォールが有効になっていないと、コンピュータへ不正アクセスされるおそれがあります。ファイアウォールが有効になっているかどうか確認することで、コンピュータへの不正アクセスを防止できます。	○ ※1
	DCOM	DCOM が無効になっているかどうかを判定できます。 DCOM が有効になっていると、コンピュータへ不正アクセスされるおそれがあります。DCOM が無効になっているかどうか確認することで、コンピュータへの不正アクセスを防止できます。	○
	リモートデスクトップ※8	リモートデスクトップが無効になっているかどうか、および実装されているかどうかを判定できます。 リモートデスクトップが有効になっていると、コンピュータへ不正アクセスされるおそれがあります。リモートデスクトップが無効になっているかどうか確認することで、コンピュータへの不正アクセスを防止できます。	○ ※1

設定項目		説明	自動対策
ユーザー定義のセキュリティ設定（システム情報）	ホスト名	コンピュータ情報のホスト名を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	コンピュータ名	コンピュータ情報のコンピュータ名を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	説明	コンピュータ情報のコンピュータの説明を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	コンピュータのモデル	コンピュータ情報のコンピュータのモデルを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	コンピュータのメーカー	コンピュータ情報のコンピュータのメーカーを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	コンピュータの UUID	コンピュータ情報のコンピュータのユニバーサルユニーク識別子（UUID）を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	コンピュータのシリアルナンバー	コンピュータ情報のコンピュータのシリアルナンバーを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	CPU	コンピュータ情報の CPU を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	メモリ	コンピュータ情報のメモリを、判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	ディスクの空き容量	コンピュータ情報のディスクの空き容量を、判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	ドライブ数 ※9	システムドライブのドライブ数を、判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	ドライブレター	システムドライブのドライブレターを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	論理ドライブの空き容量	システムドライブの論理ドライブの空き容量を判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	論理ドライブの容量	システムドライブの論理ドライブの容量を判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－

設定項目		説明	自動対策
ユーザー定義のセキュリティ設定（システム情報）	論理ドライブのファイルシステム	システムドライブの論理ドライブのファイルシステムを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	ハードディスクのモデル	システムドライブのハードディスクのモデルを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	ハードディスクの容量	システムドライブのハードディスクの容量を、判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	ハードディスクのインタフェース	システムドライブのハードディスクのインタフェースを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	BIOS 名	BIOS 情報の BIOS 名を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	BIOS のメーカー	BIOS 情報の BIOS のメーカーを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	BIOS のシリアルナンバー	BIOS 情報の BIOS のシリアルナンバーを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	BIOS のバージョン（BIOS）	BIOS 情報の BIOS のバージョン（BIOS）を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	BIOS のバージョン（SMBIOS）	BIOS 情報の BIOS のバージョン（SMBIOS）を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	AMT ファームウェアバージョン	AMT ファームウェアバージョンを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	モニタの電源を切る（AC）	電源管理のモニタ電源が切れるまでの時間（AC）を、判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 分です。	－
	モニタの電源を切る（DC）	電源管理のモニタ電源が切れるまでの時間（DC）を、判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 分です。	－
	システムスタンバイ（AC）	電源管理のシステムスタンバイまでの時間（AC）を、判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 分です。	－

設定項目		説明	自動対策
ユーザー定義のセキュリティ設定（システム情報）	システムスタンバイ（DC）	電源管理のシステムスタンバイまでの時間（DC）を、判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 分です。	－
	システム休止状態（AC）	電源管理のシステムが休止状態に入るまでの時間（AC）を、判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 分です。	－
	システム休止状態（DC）	電源管理のシステムが休止状態に入るまでの時間（DC）を、判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 分です。	－
	ハードディスクの電源を切る（AC）	電源管理のハードディスクの電源が切れるまでの時間（AC）を、判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 分です。	－
	ハードディスクの電源を切る（DC）	電源管理のハードディスクの電源が切れるまでの時間（DC）を、判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 分です。	－
	最終ログオンユーザーのユーザー名	ユーザー情報の、最後にログオンしたユーザーのユーザー名を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	最終ログオンユーザーのアカウント名	ユーザー情報の、最後にログオンしたユーザーのドメイン名（またはコンピュータ名）付きアカウント名を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	最終ログオンユーザーの説明	ユーザー情報の、最後にログオンしたユーザーの説明を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	OS	OS 情報の OS を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	OS のサービスパックまたはバージョン	OS 情報の OS のサービスパックまたはバージョンを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	OS のシリアルナンバー	OS 情報の OS のシリアルナンバーを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	OS の所有者	OS 情報の OS の所有者を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	OS の会社名	OS 情報の OS の会社名を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－

設定項目		説明	自動対策
ユーザー定義のセキュリティ設定（システム情報）	Windows Installer のバージョン	OS 情報の Windows Installer のバージョンを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	IE バージョン	OS 情報の IE バージョンを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	IE サービスパック	OS 情報の IE サービスパックを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	Windows Update のエージェントバージョン	OS 情報の Windows Update のエージェントバージョンを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	ネットワークアダプタ	ネットワーク情報のネットワークアダプタを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	MAC アドレス	ネットワーク情報の MAC アドレスを、判定の対象項目にできます。 判定値に入力できる値は、1～17 文字です。	－
	ドメイン（ワークグループ）	ネットワーク情報のドメイン（ワークグループ）を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
ユーザー定義のセキュリティ設定（ハードウェア情報）	コア数※9	CPU 情報のコア数を判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	プロセッサ	CPU 情報のプロセッサを判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	メモリ容量	メモリ情報のメモリ容量を、判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	メモリスロット容量	メモリ情報のメモリスロット容量を、判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	仮想メモリ容量	メモリ情報の仮想メモリ容量を、判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	ハードディスク数※9	ハードディスク情報のハードディスク数を判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	ハードディスクのモデル	ハードディスク情報のハードディスクのモデルを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－

設定項目		説明	自動対策
ユーザー定義のセキュリティ設定（ハードウェア情報）	ハードディスクの容量	ハードディスク情報のハードディスクの容量を、判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	ハードディスクのインタフェース	ハードディスク情報のハードディスクのインタフェースを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	論理ドライブのドライブレター	ハードディスク情報の論理ドライブのドライブレターを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	論理ドライブの空き容量	ハードディスク情報の論理ドライブの空き容量を、判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	論理ドライブの容量	ハードディスク情報の論理ドライブの容量を、判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	論理ドライブのファイルシステム	ハードディスク情報の論理ドライブのファイルシステムを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	CD-ROM ドライブ数※9	CD-ROM ドライブ情報の CD-ROM ドライブ数を判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	CD-ROM ドライブのモデル	CD-ROM ドライブ情報の CD-ROM ドライブのモデルを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	リムーバブルドライブ数※9	リムーバブルドライブ情報のリムーバブルドライブ数を、判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	プリンタ数※9	プリンタ情報のプリンタ数を判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	プリンタ名	プリンタ情報のプリンタ名を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	プリンタドライバ	プリンタ情報のプリンタドライバを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	プリンタ共有名	プリンタ情報のプリンタ共有名を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－

設定項目		説明	自動対策
ユーザー定義のセキュリティ設定(ハードウェア情報)	プリンタサーバ名	プリンタ情報のプリンタサーバ名を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	プリンタポート	プリンタ情報のプリンタポートを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	ビデオコントローラ数※9	ビデオコントローラ情報のビデオコントローラ数を判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	ビデオチップ	ビデオコントローラ情報のビデオチップを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	ビデオカードのVRAM容量	ビデオコントローラ情報のビデオカードの VRAM 容量を、判定の対象項目にできます。 判定値に入力できる値は、0～9,223,372,036,854,775,807 バイトです。	－
	ビデオドライバ	ビデオコントローラ情報のビデオドライバを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	サウンドカード数※9	サウンドカード情報のサウンドカード数を判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	サウンドカード名	サウンドカード情報のサウンドカード名を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	サウンドカードメーカー	サウンドカード情報のサウンドカードのメーカーを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	ネットワークアダプタ数※9	ネットワークアダプタ情報のネットワークアダプタ数を判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	ネットワークアダプタ	ネットワークアダプタ情報のネットワークアダプタを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	モニタ数※9	モニタ情報のモニタ数を判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	モニタ	モニタ情報のモニタを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
	キーボード数※9	キーボード情報のキーボード数を判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	キーボード	キーボード情報のキーボードを、判定の対象項目にできます。	－

設定項目		説明	自動対策
ユーザー定義のセキュリティ設定（ハードウェア情報）	キーボード	判定値に入力できる値は、1～256 文字です。	－
	マウス数※9	マウス情報のマウス数を判定の対象項目にできます。 判定値に入力できる値は、0～2,147,483,647 個です。	－
	マウス	マウス情報のマウスを、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
ユーザー定義のセキュリティ設定（追加管理項目）	追加管理項目（数値型）※9	データ型が数値型の追加管理項目を、判定の対象項目にできます。 判定値に入力できる数値は、-2,147,483,647～2,147,483,647 です。	－
	追加管理項目（選択型）	データ型が選択型の追加管理項目を、判定の対象項目にできます。 判定値には、プルダウンメニューに表示される値を設定できます。	－
	追加管理項目（テキスト型）	データ型がテキスト型の追加管理項目を、判定の対象項目にできます。 判定値に入力できる値は、1～256 文字です。	－
禁止操作※2	印刷の抑止	印刷操作を抑止できます。 印刷を許可するパスワードも設定できます。	－
	USB デバイスの使用の抑止	USB デバイスの使用を抑止できます。	－
	登録済み USB デバイスの使用許可※13	ハードウェア資産情報が登録済みの USB デバイスだけ、使用を許可できます。 また、次の条件で使用を許可する資産を限定できます。 • USB デバイスの部署と同じ部署の資産 • USB デバイスの設置場所と同じ設置場所の資産 • USB デバイスに関連づけられている資産	－
	内蔵 CD/DVD ドライブの使用の抑止	内蔵 CD/DVD ドライブの使用を抑止できます。	－
	内蔵 FD ドライブの使用の抑止	内蔵 FD ドライブの使用を抑止できます。	－
	IEEE1394 デバイスの使用の抑止	IEEE1394 デバイスの使用を抑止できます。	－
	内蔵 SD カードの使用の抑止	内蔵 SD カードの使用を抑止できます。	－

設定項目		説明	自動対策
禁止操作※2	Bluetooth デバイスの使用の抑止	Bluetooth デバイスの使用を抑止できます。	−
	イメージングデバイスの使用の抑止	イメージングデバイスの使用を抑止できます。	−
	Windows ポータブルデバイスの使用の抑止	Windows ポータブルデバイスの使用を抑止できます。	−
	抑止メッセージの表示※10	デバイスの使用を抑止したことを示すメッセージを、利用者のコンピュータに表示できます。	−
	リムーバブルディスクの書き込みの抑止	リムーバブルディスクへの書き込みだけを抑止できます。	−
	CD/DVD ドライブの書き込みの抑止	CD/DVD ドライブへの書き込みだけを抑止できます。	−
	FD ドライブの書き込みの抑止	FD ドライブへの書き込みだけを抑止できます。	−
	ソフトウェアの起動抑止	指定したソフトウェアの起動を抑止できます。起動を抑止したいソフトウェアは複数設定できます。	−
操作ログ※12	操作ログの取得対象	操作ログを取得する対象となる操作を設定できます。	−
	添付ファイル付きメールの送受信	添付ファイル付きのメールを送信する際に、不審な操作と見なすかどうかを設定できます。	−
	Web/FTP サーバの使用	Web サーバまたは FTP サーバにファイルをアップロードする際に、不審な操作と見なすかどうかを設定できます。	−
	外部メディア（リムーバブルディスク）へのファイルコピーと移動	外部メディアへファイルをコピーまたは移動する際に、不審な操作と見なすかどうかを設定できます。	−

設定項目		説明	自動対策
操作ログ※12	大量印刷	規定値を超える大量印刷を、不審な操作と見なすかどうかを設定できます。	－
禁止操作と操作ログの共通設定※12	禁止操作／操作ログの、上位システムへの通知間隔	禁止操作の抑止イベントと操作ログを、上位システムに通知する間隔を設定できます。※11	－
	禁止操作／操作ログの、利用者のコンピュータでの保持期間	禁止操作の抑止イベントと操作ログを上位システムに通知するまでの間、利用者のコンピュータ側で保持する期間の最大値を設定できます。	－
	USB デバイスのファイル一覧取得	ハードウェア資産情報が登録済みの USB デバイスに格納されているファイル一覧を、取得するかどうかを設定できます。	－

（凡例）○：設定できる　－：自動対策の対象外

注※1　セキュリティポリシーのセキュリティ設定項目［OS のセキュリティ設定］で、OS のセキュリティ設定のポリシーが無効になっていると、自動対策を実施しません。また、Active Directory を使用している場合にグループポリシーで不適正な設定に固定されていると、コンピュータの設定変更ができないため自動対策が失敗します。

注※2　エージェントレスのコンピュータは対象外です。

注※3　SERVICE_STOP 権のないサービス、または依存しているサービスが稼働中のサービスは停止できないため、自動対策が失敗します。

注※4　OS に複数のユーザーアカウントがある場合、ユーザーアカウントごとに判定されます。ただし、Mac OS の場合、ユーザーアカウントごとの判定結果ではなく、全ユーザーアカウントの判定結果になります。

注※5　OS にログオン中のユーザーアカウントだけ自動対策されます。

注※6　スクリーンセーバーのデータが Windows の「System32」フォルダ配下に存在しない場合、自動対策が失敗します。

注※7　エージェントの OS が Windows Server 2003 Service Pack なしの場合は判定されません。また、自動対策もできません。OS が Windows Server 2008 R2 または Windows 7 で複数のネットワークカードを利用している場合、すべてのネットワークプロファイルに対して自動対策が実行されます。

注※8　エージェントレスの OS が Windows Server 2003 Service Pack なし、Windows XP Service Pack 1、Windows XP Service Pack なし、または Windows 2000 の場合は、判定されません。

注※9　値を設定していないのか、値が 0 なのかを判別できない場合は、0 として扱います。

注※10　Citrix XenApp、Microsoft RDS サーバの場合、サポートしていない設定項目のため、非表示に設定してください。

注※11　通知間隔を小さくすると、上位システムへの負荷が高くなるおそれがあるため、デフォルトの設定（60 分）のままで運用するようにしてください。導入時など、操作ログを早く取得したい場合は、通知間隔を小さくすることができます。

注※12　オフライン管理のコンピュータ向けにセキュリティポリシーを作成する場合は、設定項目はデフォルト値から変更しないでください。

注※13　オフライン管理のコンピュータ向けにセキュリティポリシーを作成する場合は、使用を許可する資産を限定する設定はできません。

注※14　オフライン管理のコンピュータ向けにセキュリティポリシーを作成する場合は、自動対策の設定はデフォルト値から変更しないでください。

注※15　オフライン管理のコンピュータ向けにセキュリティポリシーを作成する場合は、自動対策の「アンインストール」の設定はデフォルト値から変更しないでください。

アクション項目

項目	説明
利用者へのメッセージ通知※	セキュリティの判定結果が危険、警告、または注意だった場合に、自動的にコンピュータにメッセージを通知できます。 通知メッセージは、任意に作成できます。利用者には、作成したメッセージに加えて違反内容が通知されます。
ネットワーク接続制御	セキュリティの判定結果に応じて、コンピュータのネットワーク接続を許可したり遮断したりできます。

注　アクション項目は、対象のコンピュータが管理用サーバと接続している場合だけ実行されます。

注　オフライン管理のコンピュータ向けにセキュリティポリシーを作成する場合は、アクション項目のすべての設定項目はデフォルト値から変更しないでください。

注※　Citrix XenApp、Microsoft RDS サーバの場合、サポートしていない設定項目のため、メッセージを通知しない設定にしてください。

割り当てグループ

項目	説明
対象の構成	セキュリティポリシーを割り当てるグループの構成（OS、ネットワーク、部署、設置場所、ユーザー定義）を指定できます。 指定したグループ構成に対して、どのグループにセキュリティポリシーを割り当てるかを設定できます。

(2) セキュリティポリシーの設定時の注意事項

- オフライン管理のコンピュータ、およびエージェントレスのコンピュータは自動対策できません。
- セキュリティポリシーで USB デバイスの［読み取りと書き込みを抑止する］を有効にしている場合、USB デバイスの抑止後にデバイスが OS に再認識され、抑止メッセージが繰り返し表示される場合があります。抑止された USB デバイスは機器から取り外してください。
- セキュリティポリシーで操作ログを有効にしてコンピュータ起動を取得する設定にしている場合、エージェントの上書きインストールのタイミングで、コンピュータ起動の操作ログが取得されます。
- エージェントをスケールアウトファイルサーバ環境にインストールしている場合、JP1/IT Desktop Management 2 のイベント 1066 が不定期に断続して出力される場合があります。

  次の条件がすべて重なった場合に発生するおそれがあります。

  - スケールアウトファイルサーバ環境である。
  - スケールアウトファイルサーバの共有フォルダが存在する。
  - JP1/IT Desktop Management 2 でセキュリティポリシーの［セキュリティ設定項目］－［OS のセキュリティ設定］－［共有フォルダ］を有効にしている。

  この現象を回避する場合、対象ホストに対してセキュリティポリシーの［セキュリティ設定項目］－［OS のセキュリティ設定］－［共有フォルダ］を無効にしてください。

(3) 製品が提供するセキュリティポリシー

JP1/IT Desktop Management 2 は、次に示すポリシーを提供します。

デフォルトポリシー

管理対象のコンピュータにセキュリティポリシーが割り当てられていない場合に、自動で割り当てられるセキュリティポリシーです。

推奨セキュリティポリシー

エージェントを導入しているコンピュータのセキュリティを強固にするためのセキュリティポリシーです。推奨セキュリティポリシーには、JP1/IT Desktop Management 2 が推奨するセキュリティ設定項目およびアクション項目が設定されています。

これらのポリシーは、新たにセキュリティポリシーを作成するときのサンプルとして、コピーして利用できます。

ヒント

サポートサービスを契約し、設定画面の［サポートサービスの設定］でサポート情報を設定していると、デフォルトポリシーおよび推奨セキュリティポリシーの更新プログラム情報、ならびにウィルス対策製品情報が自動で更新され、最新の状態が保たれます。

デフォルトポリシーと推奨セキュリティポリシーの設定値を次の表に示します。

設定項目		危険レベル	デフォルトポリシー		推奨セキュリティポリシー	
			設定	自動対策	設定	自動対策
更新プログラム	自動更新	警告	○	×	○	○
	すべての更新プログラムの適用状況の判定	警告	○	×	○	○
	指定した更新プログラムの適用状況の判定	警告	×	×	×	×
ウィルス対策製品	インストールの判定	危険	△	−	△	−
	エンジンバージョンの判定	危険	△（1 日）	−	△（1 日）	−
	ウィルス定義ファイルのバージョンの判定	危険	△（1 日）	−	△（1 日）	−
	自動保護（常駐設定）の判定	危険	△	−	△	−
	ウィルススキャン最終完了日時の判定	危険	△（7 日）	−	△（7 日）	−
使用ソフトウェア	使用必須ソフトウェアの判定	危険	×	×	×	×
	使用禁止ソフトウェアの判定	危険	×	×	×	×
サービスのセキュリティ設定		注意	×	×	×	×
OS のセキュリティ設定	Guest アカウントの判定	警告	○	×	○	○
	パスワードの安全性の判定	注意	○	−	○	−
	無期限パスワードの判定	注意	○	×	○	○
	パスワード更新からの経過日数の判定	注意	○（180 日）	−	○（180 日）	−
	自動ログオンの判定	注意	○	×	○	○
	パワーオンパスワードの判定	注意	○	−	○	−

設定項目		危険レベル	デフォルトポリシー		推奨セキュリティポリシー	
			設定	自動対策	設定	自動対策
OS のセキュリティ設定	スクリーンセーバーのパスワード保護の判定	注意	○	×	○	○
	スクリーンセーバー起動までの待ち時間の判定	注意	○（10 分）	×	○（10 分）	○
	共有フォルダの判定	警告	○	×	○	○
	管理共有の判定	警告	○	×	○	○
	匿名接続の判定	警告	○	×	○	○
	ファイアウォールの判定	警告	○	×	○	○
	DCOM の判定	警告	○	×	○	○
	リモートデスクトップの判定	警告	○	×	○	○
ユーザー定義のセキュリティ設定		危険	×	×	×	×
禁止操作	印刷の抑止	−	×	−	×	−
	USB デバイスの使用の抑止	−	×	−	○	−
	登録済 USB デバイスの使用許可	−	×	−	○	−
	格納ファイル一覧の取得	−	×	−	○	−
	内蔵 CD/DVD ドライブの使用の抑止	−	×	−	○	−
	内蔵 FD ドライブの使用の抑止	−	×	−	○	−
	IEEE1394 ドライブの使用の抑止	−	×	−	○	−
	内蔵 SD カードの使用の抑止	−	×	−	○	−
	Bluetooth デバイスの使用の抑止	−	×	−	○	−

設定項目		危険レベル	デフォルトポリシー		推奨セキュリティポリシー	
			設定	自動対策	設定	自動対策
禁止操作	イメージングデバイスの使用の抑止	－	×	－	○	－
	Windows ポータブルデバイスの使用の抑止	－	×	－	○	－
	抑止メッセージの表示（USB デバイスの場合）	－	×	－	○	－
	抑止メッセージの表示（USB デバイス以外のデバイスの場合）	－	×	－	×	－
	リムーバブルディスクの書き込みの抑止	－	×	－	×	－
	CD/DVD ドライブの書き込みの抑止	－	×	－	×	－
	FD ドライブの書き込みの抑止	－	×	－	×	－
	ソフトウェアの起動抑止	－	×	－	○	－
操作ログ	操作ログの取得対象	－	×	－	×	－
	添付ファイル付きメールの送受信	－	×	－	×	－
	Web/FTP サーバの使用	－	×	－	×	－
	外部メディア（リムーバブルディスク）へのファイルコピーと移動	－	×	－	×	－
	大量印刷	－	×	－	×	－
禁止操作と操作ログの共通設定	禁止操作／操作ログの、上位シ	－	○	－	○	－

設定項目		危険レベル	デフォルトポリシー		推奨セキュリティポリシー	
			設定	自動対策	設定	自動対策
禁止操作と操作ログの共通設定	ステムへの通知間隔	－	○	－	○	－
	禁止操作／操作ログの、利用者のコンピュータでの保持期間	－	○	－	○	－
アクション項目	利用者へのメッセージ通知	－	×	－	○（危険、警告、注意）	－

（凡例） ○：有効　△：情報を収集できるウィルス対策製品で有効　×：無効　－：設定の対象外

関連リンク

- (1)　セキュリティポリシーに設定できる項目

(4)　セキュリティポリシーの割り当て

セキュリティ状況を判定するためには、セキュリティポリシーをグループまたはコンピュータに対して割り当てる必要があります。ここでは、セキュリティポリシーが割り当たる範囲について説明します。

ヒント

コンピュータを管理対象にした直後は、自動的にデフォルトポリシーが割り当てられます。

セキュリティポリシーを割り当てる場合

セキュリティポリシーをコンピュータに割り当てた場合、対象のコンピュータにセキュリティポリシーが適用されます。セキュリティポリシーをグループに割り当てた場合、下位のグループを含めそのグループに属するすべてのコンピュータにセキュリティポリシーが適用されます。

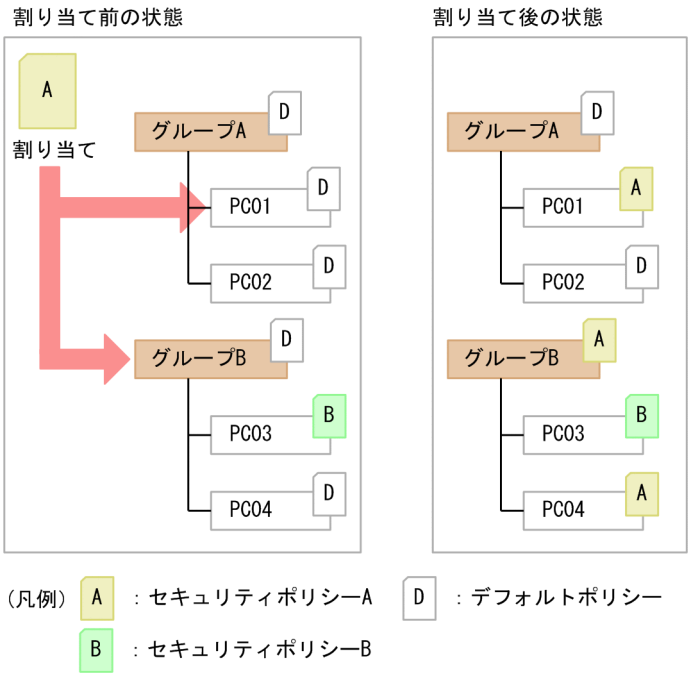
コンピュータへの割り当てとグループへの割り当てが重複する場合は、コンピュータに割り当てられたセキュリティポリシーが適用されます。また、セキュリティポリシーが直接割り当てられているグループは、上位のグループにセキュリティポリシーを割り当てても、そのセキュリティポリシーは適用されません。

なお、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た場合も、割り当てたセキュリティポリシーは適用されたままとなります。

重要

複数のネットワークインターフェースカードを利用している場合など、コンピュータが複数のIP アドレスのグループに登録されてしまうことがあります。コンピュータが複数のグループに登録されている場合、各登録先のグループに異なるセキュリティポリシーが割り当てられているときは、そのコンピュータにはデフォルトポリシーが適用されます。

セキュリティポリシーを割り当てた場合の、割り当て範囲の例を次の図に示します。

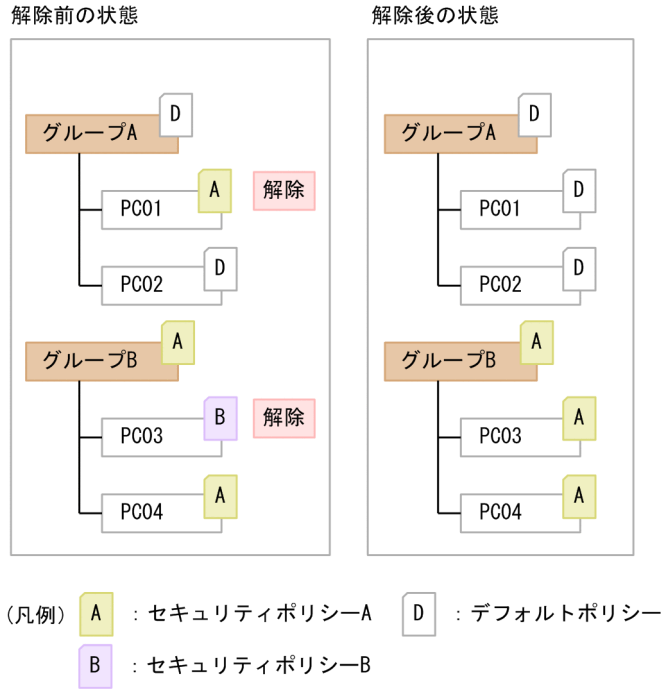


上記の図では、セキュリティポリシー A をコンピュータ PC01 とグループ B に割り当てています。ただし、グループ B のコンピュータ PC03 には個別にセキュリティポリシー B が割り当てられているため、セキュリティポリシー B が優先されます。

セキュリティポリシーを解除する場合

割り当てたセキュリティポリシーは解除できます。セキュリティポリシーを解除すると、上位のグループに割り当てられているセキュリティポリシーが適用されます。上位のグループにセキュリティポリシーが割り当てられていない場合は、デフォルトポリシーが適用されます。

セキュリティポリシーを解除した場合の、割り当て範囲の例を次の図に示します。



上記の図では、コンピュータ PC01 と PC03 に割り当てられたセキュリティポリシーを解除しています。PC01 は上位のグループ A にセキュリティポリシーが割り当てられていないため、デフォルトポリシーが適用されます。PC03 は上位のグループ B に割り当てられているセキュリティポリシー A が適用されます。

(5)　セキュリティ判定時のアクション項目

管理対象のコンピュータにセキュリティポリシーを割り当てておくと、セキュリティ状況が判定されます。このとき、セキュリティの判定結果によって、対象のコンピュータに対して、メッセージを通知したり、ネットワークを制御したりといったアクションを自動的に実行できます。

セキュリティの判定結果によって実行されるアクション項目を次に示します。

メッセージの通知

セキュリティポリシーの判定結果を通知するメッセージを設定できます。通知する危険レベルや通知条件を設定すると、危険レベルが「危険」（ ）のときだけメッセージを通知したり、設定した日数以上セキュリティ状況が危険な状態が続いたときにメッセージを通知したりできます。なお、メッセージを通知できるのは、オンライン管理のコンピュータだけです。

メッセージの通知方法については、「(6)　セキュリティ状況に応じたメッセージの通知」を参照してください。

ネットワーク接続の制御

セキュリティポリシーの判定結果によって、コンピュータのネットワーク接続の状態をどのように変更するかを設定できます。接続制御の対象とする危険レベルや接続拒否の条件を設定すると、危険レベルが「警告」（ ）のコンピュータのネットワーク接続を遮断したり、設定した日数以上セキュリティ状況が危険な状態が続いたときにネットワーク接続を制御したりできます。

ネットワーク接続の制御方法については、「(9)　セキュリティポリシーの判定結果に応じたネットワーク接続の遮断と許可」を参照してください。

(6)　セキュリティ状況に応じたメッセージの通知

セキュリティ状況に問題のあるコンピュータに対して、メッセージを通知できます。メッセージを通知できるのは、オンライン管理のコンピュータだけです。次のどちらかの方法でメッセージを通知できます。

- セキュリティ画面の［機器のセキュリティ状態］－［機器一覧］画面から、任意のタイミングで任意のメッセージを個別に通知する
- セキュリティポリシーの判定結果に応じて、あらかじめ設定したメッセージを自動的に通知する

> **ヒント**
>
> 機器画面の［機器情報］－［機器一覧］画面からメッセージを通知することもできます。

管理用サーバから対象のコンピュータにメッセージが通知されると、利用者の画面にポップアップ画面が表示され、メッセージを参照できます。なお、参照できるのは最新のメッセージだけです。

> **重要**
>
> メッセージの通知に失敗した場合は、1 回だけ再度通知されます。メッセージの通知に 2 回失敗した場合は、以降メッセージは通知されません。

(7)　自動通知の場合のメッセージの内容

自動で通知されるメッセージの内容を次に示します。

メッセージ本文

----- *AAAA*さんのセキュリティ設定の問題 -----
▼OSのセキュリティ設定:△*危険レベル*
▽詳細
BBBB

----- PCのセキュリティ設定の問題 -----
▼更新プログラム:△*危険レベル*
CCCC

▽適用されていない更新プログラム
DDDD

▼ウィルス対策製品:△*危険レベル*
▽インストール状況:△*危険レベル*
▽製品バージョン:△*危険レベル*
▽自動保護(常駐設定):△*危険レベル*
▽ウィルス定義ファイルバージョン:△*危険レベル*
▽エンジンバージョン:△*危険レベル*
▽ウィルススキャン最終完了日時:△*危険レベル*

▼使用ソフトウェア:△*危険レベル*
▽インストールされている使用禁止ソフトウェア
EEEE

▽インストールされていない使用必須ソフトウェア
FFFF

▼使用禁止サービス:△*危険レベル*
▽開始している使用禁止サービス
GGGG

▼OSのセキュリティ設定:△*危険レベル*
▽詳細
HHHH

▼ユーザー定義のセキュリティ設定:△*危険レベル*
▽詳細
IIII

(凡例)
△:半角スペース

項目	説明
メッセージ本文	セキュリティポリシーの［アクション項目］－［利用者へのメッセージ通知］で「メッセージ」の「本文」に指定したメッセージが表示されます。
危険レベル	判定結果に対応した危険レベルに対応して、次のような文字列が表示されます。 • 安全:安全 • 注意:注意 • 警告:警告 • 危険:危険 • 情報不足:不明 • 判定エラー:不明 • 判定未実施:不明 • 判定対応項目なし:対象外
AAAA	危険と判定されたユーザーアカウント名が表示されます。
BBBB	危険と判定されたユーザーアカウントの「OS のセキュリティ設定」のうち、危険と判定された項目の説明が表示されます。表示内容を次に示します。 • 安全性に問題のあるパスワードが設定されています。 • 指定した日数を経過してもパスワードが更新されていません。 • スクリーンセーバーにパスワード保護が設定されていません。 • スクリーンセーバーの起動時間が、適切な時間に設定されていません。

項目	説明
CCCC	Windows の自動更新が無効になっている場合に、メッセージ「Windows 自動更新が無効になっています。」が表示されます。
DDDD	「更新プログラム」の判定で、適用されていないと判定された更新プログラムが表示されます。表示形式を次に示します。 • 文書番号あり：*セキュリティ情報 ID*（*文書番号*） • 文書番号なし：*セキュリティ情報 ID* • サービスパックまたはバージョンあり：*製品名*（*サービスパック名またはバージョン*） なお、5,000 バイトを超える情報は出力されません。出力されない件数は、「その他：*n* 件」と表示されます。
EEEE	「使用ソフトウェア」の判定で、インストールされていると判定された使用禁止ソフトウェアのソフトウェア名とバージョンが表示されます。表示形式を次に示します。 • バージョンあり：*ソフトウェア名△バージョン* • バージョンなし：*ソフトウェア名* なお、6,000 バイトを超える情報は出力されません。出力されない件数は、「その他：*n* 件」と表示されます。
FFFF	「使用ソフトウェア」の判定で、インストールされていないと判定された使用必須ソフトウェアのソフトウェア名とバージョンが表示されます。 • ソフトウェア名あり、バージョンあり：*ソフトウェア名△バージョン* • ソフトウェア名あり、バージョンなし：*ソフトウェア名* なお、6,000 バイトを超える情報は出力されません。出力されない件数は、「その他：*n* 件」と表示されます。
GGGG	「サービスのセキュリティ設定」の判定で、使用されていると判定されたサービス表示名が表示されます。 情報が 6,000 バイトを超えた場合、表示できなかった件数が「その他：*n* 件」の形式で表示されます。
HHHH	「OS のセキュリティ設定」の判定で、危険と判定された項目の説明が表示されます。表示内容を次に示します。 • 有効な Guest アカウントがあります。 • 無期限パスワードが設定されたアカウントがあります。△*アカウント名* • 安全性に問題のあるパスワードが設定されたアカウントがあります。△*アカウント名* • 指定した日数を経過してもパスワードが更新されていないアカウントがあります。△*アカウント名* • 自動ログオンが設定されています。 • パワーオンパスワードが設定されていないか、または実装されていません。 • 共有フォルダが設定されています。 • 匿名接続が設定されています。 • Windows ファイアウォールが無効になっています。 • 管理共有が設定されています。 • DCOM が有効になっています。 • リモートデスクトップが有効になっています。 • スクリーンセーバーにパスワード保護が設定されていません。△*アカウント名* • スクリーンセーバーの起動時間が、適切な時間に設定されていません。△*アカウント名*
IIII	「ユーザー定義のセキュリティ設定」の判定で、危険と判定されたユーザー定義項目名が表示されます。

（凡例）△：半角スペース

(8)　自動通知の場合のメッセージに入力できる埋め込み文字

自動で通知されるメッセージ本文には、次に示す埋め込み文字を入力できます。

埋め込み文字	表示内容
%judgedate%	セキュリティ判定日時
%contdays%	不適正な状態が続いた日数※1
%refusedmsg%	「ネットワークへの接続が遮断されました。」 「あと*n* 日で、ネットワークへの接続が遮断されます。」※2

注※1　セキュリティポリシーの［アクション項目］－［利用者へのメッセージ通知］で［通知条件］を設定している場合に表示されます。

注※2　セキュリティポリシーの［アクション項目］－［ネットワーク接続制御］で［接続拒否の条件］を設定している場合に表示されます。

(9)　セキュリティポリシーの判定結果に応じたネットワーク接続の遮断と許可

セキュリティポリシーの判定結果が設定した危険レベルを超えた場合、対象のコンピュータのネットワーク接続を遮断できます。判定結果が設定した危険レベルを下回った状態になると、遮断したネットワーク接続は自動的に許可されます。ネットワーク接続を遮断および許可するためには、対象のコンピュータが所属するネットワークセグメントが監視されている必要があります。

> **ヒント**
>
> 機器画面の［機器情報］－［機器一覧］画面で対象のコンピュータを選択して、［操作メニュー］からネットワーク接続を遮断または許可することもできます。詳細については、「2.8.17　手動によるネットワーク接続の制御」を参照してください。

ネットワーク接続の制御の優先度

ネットワーク接続の制御は、手動で設定した内容が優先されます。

- 手動で、ネットワーク接続を許可しない設定にしている場合
  自動的にネットワーク接続が許可される契機になっても、許可されません。

ネットワークに接続してはいけないコンピュータがある場合は、手動で、許可しない設定にしてください。

(10)　セキュリティポリシー違反の対策

コンピュータがセキュリティポリシーに違反している場合は、そのコンピュータの設定が適正な状態になるように対策します。JP1/IT Desktop Management 2 では、セキュリティポリシー違反を自動対策、または強制対策できます。

自動対策

セキュリティポリシーに自動対策を設定すると、セキュリティポリシーに違反したコンピュータの設定を自動的に適正状態にできます。詳細については、「(11)　セキュリティポリシー違反の自動対策」を参照してください。

強制対策

セキュリティポリシーに違反したコンピュータを、任意のタイミングで個別に強制対策できます。なお、セキュリティポリシーに違反したコンピュータを強制対策するには、対象のコンピュータにオンライン管理用のエージェントがインストールされている必要があります。

(11)　セキュリティポリシー違反の自動対策

コンピュータがセキュリティポリシーに違反している場合、そのコンピュータの設定を確認して適正な状態になるよう設定変更する必要があります。このような作業を繰り返すのは非常に手間が掛かります。

セキュリティポリシーに自動対策を設定すると、セキュリティポリシーに違反していた場合に、自動的に適正状態となるように対策されるようになります。これによって、管理者が個々のコンピュータの設定状況を意識することなく、組織内のコンピュータのセキュリティ状況を安全に保てます。

セキュリティポリシーに設定できる自動対策

- Windows 自動更新の実行が無効だった場合に有効にする

  Windows 自動更新の実行が無効だった場合に次の対策を実行します。

  - コントロールパネルの［Windows Update］－［設定の変更］－［重要な更新プログラム］の設定で［更新プログラムを自動的にインストールする］を有効にします。
  - 「Windows Update」サービスのスタートアップの種類を「自動」にします。
  - 「Windows Update」サービスを起動します。
- 必須とする更新プログラムグループに含まれる更新プログラムが適用されていない場合に、Windows 自動更新を強制実行、または更新プログラムを自動的に配布する

  必須とする更新プログラムグループに含まれる更新プログラムが適用されていない場合に、Windows 自動更新を強制実行、または更新プログラムを自動的に配布します。Windows 自動更新を強制実行する場合、必須とする更新プログラム以外の更新プログラムも適用されます。
- 使用必須ソフトウェアがインストールされていなかった場合に、ソフトウェアをインストールする※
- 使用禁止ソフトウェアがインストールされていた場合に、ソフトウェアの起動を抑止する
- 使用禁止ソフトウェアがインストールされていた場合に、ソフトウェアをアンインストールする※
- 使用禁止サービスが稼働している場合に、サービスを停止して無効化する

  使用禁止サービスが稼働している場合に、サービスを停止して無効化します。なお、該当サービスに依存したサービスが起動中の場合、サービスの停止に失敗します。
- Guest アカウントが有効な場合に無効にする
- 無期限パスワードが設定されている場合に解除する

- 自動ログオンが設定されている場合に解除する
- スクリーンセーバーのパスワード保護が設定されていない場合に設定する

  スクリーンセーバーのパスワード保護が設定されていない場合、該当ユーザーのログオン時に設定します。
- スクリーンセーバーの待ち時間が規定値を超えている場合に、待ち時間を変更する

  スクリーンセーバーの待ち時間が規定値を超えている場合、該当ユーザーのログオン時に待ち時間をセキュリティポリシーの適正状態に指定した時間に変更します。
- 共有フォルダが設定されている場合に解除する

  共有フォルダが設定されている場合に解除します。プリンタを共有している場合、共有フォルダの設定が解除され、共有プリンタを使用できなくなることがあります。
- 制限なしの匿名接続が設定されている場合に解除する
- Windows ファイアウォールが無効な場合に有効にする
- 管理共有が設定されている場合に解除する
- DCOM が有効な場合に無効にする

  `dcomcnfg` で表示される［コンポーネント サービス］－［マイコンピューターのプロパティ］－［既定のプロパティ］－［このコンピュータ上で分散 COM を有効にする］設定を無効にします。DCOM 機能を使用しているアプリケーションが動作しなくなることがあるため、あらかじめ検証した上で自動対策オプションを設定してください。
- リモートデスクトップが有効な場合に無効にする

注※

Windows ストアアプリの場合、自動対策にインストールおよびアンインストールの設定はできますが、実際のインストールおよびアンインストールは実行されません。Windows ストアアプリのインストール、アンインストールをするときは、対象のコンピュータで個別に実施してください。

自動対策が実行されるタイミング

- セキュリティポリシーが割り当てられたとき
- セキュリティポリシーが更新されたとき
- 管理対象のコンピュータの属するグループが変更されたとき
- 管理対象のコンピュータの機器情報が更新されたとき

これらのタイミングで、セキュリティポリシーの設定に応じて自動対策が実行されます。セキュリティ設定とサービスの自動対策は、管理対象のコンピュータで実行されます。使用必須ソフトウェアのインストールと使用禁止ソフトウェアのアンインストールは、管理用サーバから配布機能が実行されます。

重要

次に示す項目は、セキュリティポリシーが割り当てられているコンピュータが再起動したあとで自動対策されます。コンピュータにセキュリティポリシーが適用されると、再起動を促すバルーンヒントが定期的に表示されます。バルーンヒントの表示は、エージェント設定の［利用者への通知設定］の設定に従います。

- Windows 自動更新の実行
- 匿名接続
- Windows ファイアウォール※
- 管理共有
- DCOM
- リモートデスクトップ

注※　コンピュータの OS が Windows Server 2008、Windows 7、または Windows Vista の場合に限ります。

関連リンク

- (1)　セキュリティポリシーに設定できる項目

(12)　セキュリティポリシー違反の自動対策の注意事項

セキュリティポリシーの適用やセキュリティ対策で自動対策をした場合、JP1/IT Desktop Management 2 の機能を利用して管理対象コンピュータの設定を自動対策前の状態には戻せません。JP1/IT Desktop Management 2 の機能で自動対策前の状態に戻せない項目は次の項目です。

- 更新プログラム
- 使用ソフトウェア
- サービスのセキュリティ設定
- OS のセキュリティ設定

(13)　セキュリティポリシー違反の強制対策の注意事項

対策項目に「更新プログラム適用」、対策内容に「自動更新を実施する」を選択し、セキュリティ対策を実行して更新プログラムのインストールを行いたい場合は、次のすべての条件を満たす必要があります。

- Windows のグループポリシーの設定が次のどちらかである。
  - Windows のグループポリシーで Windows Update の自動更新が構成されていない。
  - Windows のグループポリシーで Windows Update の自動更新が構成されている、かつ、自動更新の構成で更新プログラムを自動的にインストールする設定になっている。

- 次のサービスが起動中である。
  - Background Intelligent Transfer Service

2.9.5 禁止操作の抑止

セキュリティポリシーには、コンピュータでの操作を抑止する設定ができます。操作を抑止することで、外部への情報の持ち出しによる情報漏えいを防止できます。

> **重要**
>
> API 管理機器は禁止操作の抑止ができません。

印刷の抑止

印刷操作を抑止できます。持ち出し禁止の情報を、印刷して持ち出されることを防止できます。

印刷の許可パスワードを設定できるので、印刷を許可する利用者だけにパスワードを教えて、印刷の利用を限定することもできます。

> **重要**
>
> インターネット接続のプリンタは抑止できません。ローカルプリンタで File ポートまたは LAN Manager ポートを使用する場合も抑止できません。また、Windows のネットワーク共有プリンタは、抑止できないことがあります。
>
> 印刷機能を利用した PDF などのファイルへの出力は、利用者のコンピュータに印刷抑止のメッセージが表示されても、ファイルが出力されることがあります。

機器の使用抑止

デバイスの使用を抑止できます。デバイスを利用して情報が持ち出されることを防止できます。使用を抑止できるデバイスを次に示します。

- USB デバイス（通常の USB デバイス）
- USB デバイス（Windows 8 以降で UASP 対応デバイスとして認識される USB デバイス）
- 内蔵 CD/DVD ドライブ
- 内蔵 FD ドライブ
- IEEE1394 デバイス
- 内蔵 SD カード
- Bluetooth デバイス
- イメージングデバイス
- Windows ポータブルデバイス

使用を抑止したことを示すメッセージを、利用者のコンピュータに表示できます。

USB デバイスの使用を抑止した場合、登録した USB デバイスの使用を許可したり、部署、設置場所、または関連づけられている資産を条件に USB デバイスを使用する資産を限定したりできます。また、USB デバイスに格納されているファイルの一覧を取得することもできます。

次のデバイスは書き込みだけを抑止できます。

- リムーバブルディスク
- CD/DVD ドライブ
- FD ドライブ

書き込みだけを抑止できるのは、使用を許可しているデバイスだけです。

ヒント

書き込み抑止を設定した場合は、セキュリティポリシーが割り当てられているコンピュータが再起動したあとで設定が有効になります。コンピュータにセキュリティポリシーが適用されると、再起動を促すバルーンヒントが表示されます。バルーンヒントの表示は、エージェント設定の［利用者への通知設定］の設定に従います。

ソフトウェアの起動抑止

ファイル共有ソフトウェアやメッセンジャーソフトウェアなど、情報漏えいにつながるおそれのあるソフトウェアの起動を抑止できます。

起動を抑止できるのは、次の拡張子の実行ファイルで起動するソフトウェアです。

- exe
- com
- scr

なお、実行ファイル名とフォルダ名を合わせた文字列が 260 文字以上の場合は、起動を抑止できません。

重要

起動後すぐに終了するソフトウェアは、起動を抑止する前にプログラムが終了するおそれがあるため、起動を抑止できないことがあります。

重要

OS や JP1/IT Desktop Management 2 の動作に関係する実行ファイルは、起動を抑止しないでください。起動を抑止すると、OS や JP1/IT Desktop Management 2 が正しく動作しなくなるおそれがあります。

重要

16bit ソフトウェアの場合、ソフトウェアの起動抑止はできません。

重要

エージェントの OS が Windows 7 の場合、Windows XP モードでインストールしたソフトウェアの起動抑止、および Windows XP モード上での機器の使用抑止、印刷の抑止はできません。

(1) 使用を抑止できるデバイス

セキュリティポリシーの禁止操作の設定では、エージェント導入済みのコンピュータでのデバイスの使用を抑止できます。

使用を抑止できるデバイス、および抑止対象の条件を次に示します。

ヒント

セキュリティポリシーの設定が有効になる前からユーザーがアクセスしていたデバイスについては、抑止の対象外となります。

抑止できるデバイス	抑止対象の条件※1※6
USB デバイス（通常の USB デバイス）	USB 接続でデータを記録できるデバイスです。※2 デバイスを接続すると、次の 2 つの条件を満たすデバイスが対象となります。 • ［デバイス マネージャー］の［デバイス（種類別)］で、USB コントローラの配下に表示されるデバイス • デバイスマネージャ上のディスクドライブ、DVD/CD-ROM ドライブ、またはフロッピー ディスクドライブのどれかに表示されるデバイス また、デバイスマネージャ上のディスクドライブ、DVD/CD-ROM ドライブ、またはフロッピー ディスクドライブのどれかに表示されるデバイスの列挙子が「USBSTOR」である必要があります。
USB デバイス（Windows 8 以降で UASP 対応デバイスとして認識される USB デバイス）	USB 接続でデータを記録できるデバイスです。※2 デバイスを接続すると、次の 2 つの条件を満たすデバイスが対象となります。 • ［デバイス マネージャー］の［記憶域コントローラ］で、［USB 接続 SCSI(UAS)マスストレージデバイス］の配下に表示されるデバイス 表示されるデバイスのサービスが「UASPStor」である必要があります。 • デバイスマネージャ上のディスクドライブ、DVD/CD-ROM ドライブ、またはフロッピー ディスクドライブのどれかに表示されるデバイス 表示されるデバイスの列挙子が「SCSI」である必要があります。
内蔵 CD/DVD ドライブ	コンピュータに内蔵されている CD/DVD ドライブが対象となります。 ［デバイス マネージャー］の［デバイス（種類別)］で、DVD/CD-ROM ドライブの配下に表示されるドライブです。DVD/CD-ROM ドライブの列挙子が「IDE」または「SCSI」である必要があります。
内蔵 FD ドライブ	コンピュータに内蔵されている FD ドライブが対象となります。

抑止できるデバイス	抑止対象の条件※1※6
内蔵 FD ドライブ	[デバイス マネージャー] の [デバイス（種類別)] で、フロッピー ディスクドライブの配下に表示されるドライブです。フロッピー ディスクドライブの列挙子が「FDC」である必要があります。
IEEE1394 デバイス	IEEE1394 で接続されたデバイスが対象となります。※3 [デバイス マネージャー] の [デバイス（種類別)] で、ディスクドライブの配下に表示されるドライブです。ディスクドライブの列挙子が「SBP2」である必要があります。
内蔵 SD カード	コンピュータに内蔵されている SD カードスロットから接続された SD カードが対象となります。※3 SD カードでなくても内蔵された SD カードスロットから接続されたデバイスは内蔵 SD カードとして抑止される場合があります。 [デバイス マネージャー] の [デバイス（種類別)] で、ディスクドライブの配下に表示されるドライブです。ディスクドライブの列挙子が「SD」、「RIMMPTSK」または「PCISTOR」である必要があります。 ただし、コンピュータに内蔵されている SD カードスロットでも、USB コントローラを利用しているものは内蔵 SD カードとして扱われない場合があります。
Bluetooth デバイス	コンピュータに USB 接続された Bluetooth デバイスが対象となります。 [デバイス マネージャー] の [デバイス（種類別)] で、Bluetooth の配下に表示されるデバイスです。Bluetooth の列挙子が「USB」で、デバイスのクラスが「Bluetooth」、「BTW」、または「BTM」である必要があります。
イメージングデバイス	コンピュータに USB 接続されたイメージングデバイスが対象となります。※4 [デバイス マネージャー] の [デバイス（種類別)] で、イメージングデバイスの配下に表示されるデバイスです。列挙子が「USB」である必要があります。
Windows ポータブルデバイス	コンピュータに接続された Windows ポータブルデバイスが対象となります。※5 [デバイス マネージャー] の [デバイス（種類別)] で、ポータブルデバイスの配下に表示されるデバイスです。

注※1　OS の設定などによって、表示される項目が異なる場合があります。

注※2　対象となるデバイスは、次に示すデバイスセットアップクラスを持つデバイスです。

Class	ClassGuid
CDROM	{4d36e965-e325-11ce-bfc1-08002be10318}
DiskDrive	{4d36e967-e325-11ce-bfc1-08002be10318}
FloppyDisk	{4d36e980-e325-11ce-bfc1-08002be10318}

デバイスセットアップクラスの Class、および ClassGuid は、Windows 7 の場合、[デバイス マネージャー] でデバイスのプロパティの [詳細] タブを表示し、プルダウンメニューで [デバイス クラス] および [デバイス クラス GUID] を選択したときに表示される文字列です。

デバイスセットアップクラスの Class、および ClassGuid が不明な場合は、デバイスの開発元に確認してください。

注※3　対象となるデバイスは、次に示すデバイスセットアップクラスを持つデバイスです。

Class	ClassGuid
DiskDrive	{4d36e967-e325-11ce-bfc1-08002be10318}

デバイスセットアップクラスの Class、および ClassGuid は、Windows 7 の場合、［デバイス マネージャー］でデバイスのプロパティの［詳細］タブを表示し、プルダウンメニューで［デバイス クラス］および［デバイス クラス GUID］を選択したときに表示される文字列です。

デバイスセットアップクラスの Class、および ClassGuid が不明な場合は、デバイスの開発元に確認してください。

注※4　対象となるデバイスは、次に示すデバイスセットアップクラスを持つデバイスです。

Class	ClassGuid
Image	{6bdd1fc6-810f-11d0-bec7-08002be2092f}

デバイスセットアップクラスの Class、および ClassGuid は、Windows 7 の場合、［デバイス マネージャー］でデバイスのプロパティの［詳細］タブを表示し、プルダウンメニューで［デバイス クラス］および［デバイス クラス GUID］を選択したときに表示される文字列です。

デバイスセットアップクラスの Class、および ClassGuid が不明な場合は、デバイスの開発元に確認してください。

注※5　対象となるデバイスは、次に示すデバイスセットアップクラスを持つデバイスです。

Class	ClassGuid
WPD	{eec5ad98-8080-425f-922a-dabf3de3f69a}

デバイスセットアップクラスの Class、および ClassGuid は、Windows 7 の場合、［デバイス マネージャー］でデバイスのプロパティの［詳細］タブを表示し、プルダウンメニューで［デバイス クラス］および［デバイス クラス GUID］を選択したときに表示される文字列です。

デバイスセットアップクラスの Class、および ClassGuid が不明な場合は、デバイスの開発元に確認してください。

注※6　デバイスの外形に関係なく、Windows 上での認識のされ方が条件に合致するデバイスを抑止対象であると判定します。

関連リンク

- (3)　使用を許可できる USB デバイスの種類
- (7)　デバイスの使用抑止の注意事項

(2) 書き込みだけを抑止できるデバイス

セキュリティポリシーの禁止操作の設定では、エージェント導入済みのコンピュータでデバイスの書き込みだけを抑止できます。書き込み抑止のセキュリティポリシーを変更した場合は、コンピュータの再起動が必要です。

書き込みだけを抑止できるデバイス、該当するデバイスの種類、および抑止対象の条件を次に示します。

デバイス	該当するデバイスの例※1	抑止対象の条件※2
リムーバブルディスク	• USB 接続のハードディスク • USB 接続のフラッシュメモリ(USB メモリ、USB 接続のカードリーダーなど) • IEEE1394 接続のハードディスク	エクスプローラ上でドライブの種類が「リムーバブルディスク」として表示されるドライブ、 USB 接続、および IEEE1394 接続でドライブの種類が「ローカルディスク」として表示されるドライブが対象となります。 また、内蔵と、USB 接続および IEEE1394 接続の両方が対象になります。
CD/DVD ドライブ	• USB 接続の CD/DVD ドライブ • 内蔵 CD/DVD ドライブ	[デバイス マネージャー] の [デバイス (種類別)] で、 [DVD/CD-ROM ドライブ] の配下に表示されるドライブが対象となります。 また、内蔵と USB 接続の両方が対象になります。
FD ドライブ	• USB 接続の FD ドライブ	[デバイス マネージャー] の [デバイス (種類別)] で、[フロッピー ディスク ドライブ] の配下に表示されるドライブが対象となります。 また、内蔵と USB 接続の両方が対象になります。

注※1　該当するデバイスであっても、OS が別のデバイスとして認識した場合は OS の認識に従い、書き込み抑止の対象外となります。

注※2　OS の設定などによって、表示される項目が異なる場合があります。

ヒント

- DVD-RAM の書き込みは抑止できません。
- 書き込みを抑止しているデバイスに対して、ツールなどでアクセスした場合、ツールがエラーになったり、イベントやエラーダイアログが表示されたりすることがあります。
- 書き込み抑止をすると、暗号化機能付き USB デバイスなど、デバイスによっては起動がエラーとなったり、使用できなくなったりする場合があります。
- CD/DVD ドライブの書き込み抑止では、サードパーティ製のソフトウェアによる CD/DVD への書き込みを抑止できない場合があります。そのようなソフトウェアによるファイル持ち出しを防止するには、ソフトウェアの起動抑止を使用して、サードパーティ製のソフトウェアの起動を抑止してください。

書き込みの抑止は、OS ごとに抑止できるデバイスが異なります。抑止できるデバイスと OS との対応を次に示します。

デバイス	Windows 8.1、Windows 8 エディションなし	Windows 10、Windows 8.1、Windows 8 Pro、Enterprise	Windows Server 2019、Windows Server 2016、Windows Server 2012	Windows 7、Windows Server 2008、Windows Vista	Windows Server 2003	Windows XP (Service Pack 2 以降)
リムーバブルディスク	×	○ ※1、※2	○ ※1、※2	○ ※1	×	△※4
CD/DVD ドライブ	×	○ ※1、※2	○ ※1、※2	○ ※1	△※3	△※3
FD ドライブ	×	○ ※1、※2	○ ※1、※2	○ ※1	×	×

（凡例）○：抑止できる　△：抑止できないデバイスがある　×：抑止できない

注※1　Windows のサービスで、「Portable Device Enumerator Service」が、「手動」または「自動」に設定されている必要があります。

注※2　USB デバイスが記憶域プールに割り当てられているときは、抑止されません。

注※3　抑止できるかどうかは、書き込みソフトウェアに依存します。Windows の IMAPI に対応したソフトウェアだけを抑止できます。

注※4　USB 接続のハードディスク、USB 接続の CD/DVD ドライブ、USB 接続の FD ドライブなどの USB デバイスが抑止できます。

USB デバイスの使用を抑止した場合

USB デバイスの使用を抑止した状態で、CD/DVD ドライブ、FD ドライブ、リムーバブルディスクの各デバイスの書き込み抑止を設定したとき、接続機器の登録状況によって有効になる抑止項目と JP1/IT Desktop Management 2 の動作が異なります。詳細を次の表に示します。

USB デバイスの使用を抑止して、USB 接続の CD/DVD ドライブ、リムーバブルディスク、または FD ドライブを接続した場合の動作

抑止項目	接続機器（USB デバイス）の登録状況	JP1/IT Desktop Management 2 の動作
CD/DVD ドライブ、リムーバブルディスク、または FD ドライブの書き込み抑止	未登録	読み取りと書き込み抑止（抑止イベントを送信、抑止メッセージを表示する）
	登録済み	書き込み抑止

関連リンク

- (3)　使用を許可できる USB デバイスの種類
- (7)　デバイスの使用抑止の注意事項

(3) 使用を許可できる USB デバイスの種類

セキュリティポリシーの禁止操作の設定で USB デバイスの使用を抑止している場合に、ハードウェア資産として登録された USB デバイスだけ使用を許可するように設定できます。

> **ヒント**
>
> USB デバイスの識別には、USB 登録時に取得されるデバイスインスタンス ID が利用されます。デバイスインスタンス ID とは、USB デバイスに設定された ID です。USB デバイスには、個別に識別できるユニークな ID を持つデバイスと、接続するポートや環境によって ID が変化するデバイスがあります。

利用を許可できる USB デバイスには、次の 2 種類があります。

個別に許可できる USB デバイス

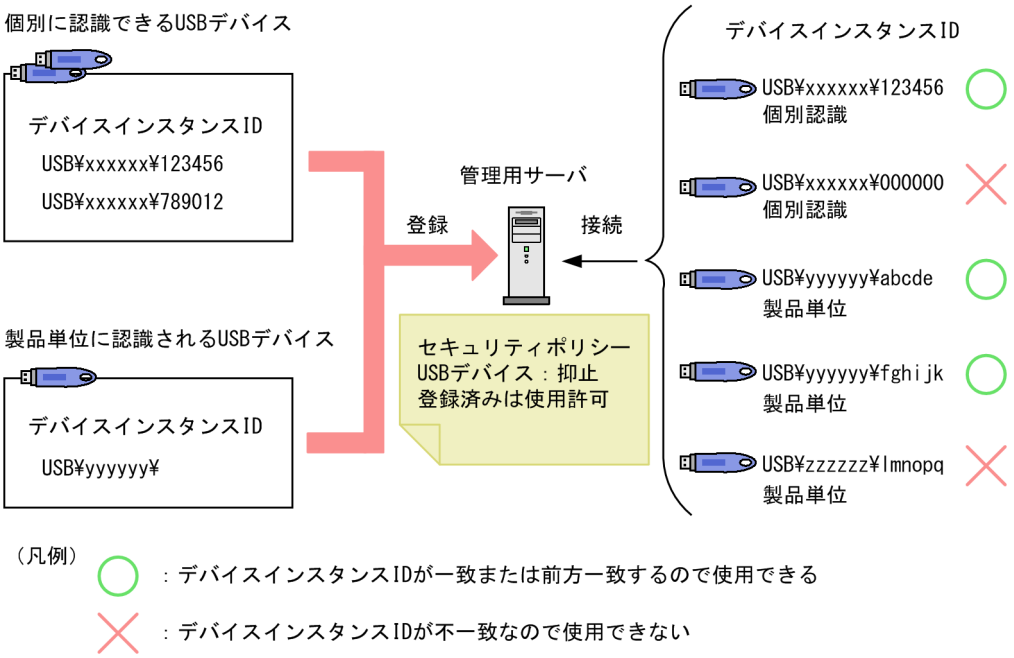
ユニークなデバイスインスタンス ID を持つ USB デバイスは、各デバイスを個別に使用許可できます。

なお、ユニークな ID を持つ USB デバイスは、Windows の［デバイス マネージャー］でデバイスのプロパティの［詳細］タブを表示し、プルダウンメニューで［機能］を選択したときに「CM_DEVCAP_UNIQUEID」と表示されます。

製品単位で許可できる USB デバイス

接続するポートや環境によってデバイスインスタンス ID が変化する USB デバイスは、製品単位でデバイスを登録して許可を設定できます。例えば、同じメーカーの同じ USB メモリを複数所持している場合、その USB メモリのデバイスインスタンス ID がユニークでないときは、1 つのデバイスを登録すれば同一製品の使用がすべて許可されます。

デバイスインスタンス ID が変化するデバイスの場合、ID の一部を利用して USB デバイスが識別されます。USB デバイス登録時にデバイスインスタンス ID を指定し、登録したデバイスインスタンス ID と前方一致した USB デバイスが、同一製品と見なされます。なお、製品単位で許可する USB デバイスの場合、USB デバイスの登録時にメッセージが表示されます。



また、USB デバイスのハードウェア資産情報に登録されている項目を基に、次の条件で USB デバイスの使用を許可する資産を限定できます。

- USB デバイスの部署と同じ部署の資産
- USB デバイスの設置場所と同じ設置場所の資産
- USB デバイスに関連づけられている資産

これらの条件を設定することで、部署、設置場所、または資産（機器）ごとに使用できる USB デバイスを指定できます。

重要

使用を許可する USB デバイスは、オンライン管理のコンピュータから登録します。

重要

製品単位で許可する USB デバイスを登録すると、同じ製品の異なるデバイスを登録しても同じハードウェア資産として扱われます。このため、セキュリティポリシーで USB デバイスの使用抑止を設定している場合、製品単位で USB デバイスの使用が許可されます。

重要

コンピュータとの接続方法（接続インターフェースや接続モード）が複数あるデバイスの場合、コンピュータとの接続方法によっては、そのデバイスの認識結果が異なることがあります。

重要

複数のデバイスを経由して接続する USB デバイスの使用を許可するためには、経由するすべてのデバイスの使用を許可してください。

重要

デバイスインスタンス ID が付与されていないデバイスをコンピュータに接続した場合、OS によって不特定のデバイスインスタンス ID が生成されます。このようなデバイスは、デバイスを接続するコンピュータまたは接続ポートごとにデバイスインスタンス ID が変化するため、使用を許可できないおそれがあります。

ヒント

オンライン管理のコンピュータに、登録済みの個別に認識される USB デバイスを接続すると、USB デバイスに格納されているファイルの情報が収集されます。収集された情報は、資産画面の［ハードウェア資産］画面の［格納ファイル一覧］タブに表示されます。なお、［格納ファイル一覧］タブは［機器種別］が「USB デバイス」の場合だけ表示されます。ただし、セキュリティポリシーでファイル一覧を取得する設定をしていない場合は、［格納ファイル一覧］タブにファイル一覧を取得できないというメッセージが表示されます。

(4)　禁止操作の抑止時の注意事項

セキュリティポリシーに禁止操作のポリシーを設定する場合に、抑止を設定できる対象ごとの注意事項を説明します。

関連リンク

- (5)　ソフトウェアの起動抑止の注意事項
- (6)　印刷の抑止の注意事項
- (7)　デバイスの使用抑止の注意事項

(5)　ソフトウェアの起動抑止の注意事項

- 抑止するソフトウェアは、ファイル名とフォルダ名を合わせた文字列の長さを 260 文字未満にしてください。
- 起動後すぐに終了するソフトウェアは、エージェントが起動を抑止する前にプログラムが終了してしまうことがあるため、起動抑止できない場合があります。
- JP1/IT Desktop Management 2 とそれ以外のプログラムとで同じソフトウェアを起動抑止した場合、JP1/IT Desktop Management 2 では正しく起動抑止できないことがあります。

- 許可時間帯に抑止対象のプログラムを起動したあとで機器のシステムの時刻を変更した場合、許可時間帯を過ぎても抑止できないことがあります。
- 許可時間帯が指定されているプログラムを許可時間内に起動し、コンピュータがスリープまたは休止状態に入った場合、許可時間を経過しても抑止されません。コンピュータがスリープまたは休止状態から起動したあと、しばらくしてから抑止されます。
- Windows のエクスプローラに表示される［正式ファイル名］または［元のファイル名］が、起動抑止するソフトウェアの［ファイル名］に設定したファイル名と一致する場合でも、ソフトウェアの実行ファイルのバージョン情報が破損または矛盾しているときは、起動抑止できないことがあります。
- ソフトウェアの起動抑止が短時間に繰り返し実施されると、OS が次に示すメッセージを表示する場合があります。この場合、利用者はメッセージに従ってソフトウェアを終了してから、OS を再起動する必要があります。

  「アプリケーションを正しく初期化できませんでした。（0xc0000142）［OK］ をクリックしてアプリケーションを終了してください。」
- 指定したプロセスを共有するほかのソフトウェアも起動抑止されることがあります。

(6) 印刷の抑止の注意事項

- 印刷抑止ができるプリンタを次の表に示します。

プリンタ種別	印刷抑止
ローカルプリンタ	○
ネットワーク共有プリンタ	○
インターネットプリンタ	×
仮想プリンタ	○

（凡例）○：抑止できる　×：抑止できない

- 各プリンタのプロパティで、すべてのログオンユーザーに［印刷］と［ドキュメントの管理］が許可されている必要があります。
- 秘文で印刷抑止している場合は、JP1/IT Desktop Management 2 では印刷抑止できません。
- プリンタ追加直後に印刷した場合、印刷抑止できないことがあります。
- OS にログオンした直後に印刷した場合、印刷抑止できないことがあります。
- 印刷操作がエージェントに通知される前に印刷ジョブが完了した場合、印刷抑止はできません。
- プリンタによっては、一度の印刷操作で複数の印刷抑止ログが取得されることがあります。

ネットワーク共有プリンタの場合、以下の注意事項が追加されます。

- サポートするエージェントとプリントサーバの組み合わせを以下に示します。

エージェント	プリントサーバ	印刷抑止
Windows 7 以降	Windows XP/2003	×
Windows 7 以降	Windows Vista 以降	○
任意	上記以外	×

（凡例）○：抑止できる　×：抑止できない

- プリントサーバとエージェント PC 間で RPC による通信ができる必要があります。RPC 通信ができない場合は以下が考えられます。
  - プリントサーバが Internet Printing Protocol（IPP）サーバである
  - プリントサーバとエージェント PC の間にファイアウォール、プロキシまたは NAT がある
  - エージェント PC の Windows ファイアウォールが有効で、かつ［ファイルとプリンターの共有］が［例外］に設定されていない
- エージェント PC で［Microsoft ネットワーク用ファイルとプリンター共有］が有効である必要があります。
- プリントサーバからエージェント PC の名前を解決できる必要があります。
- エージェント PC が Windows 7 以降の場合、エージェント PC とプリントサーバが同一のドメインに参加している、または、エージェント PC の資格認証マネージャにプリントサーバの資格情報が登録されている必要があります。なお、資格情報を追加した場合はエージェント PC を再起動する必要があります。
- IPv6 が有効でクライアントコンピュータで印刷ジョブのレンダリングが動作しない場合は、印刷抑止ができないことがあります。クライアントコンピュータで印刷ジョブのレンダリングを動作させるには以下の設定が必要です。
  - ［クライアント コンピューターで印刷ジョブのレンダリングをする］または［クライアント コンピューターに印刷ジョブを表示する］が有効である
  - ［詳細な印刷機能を有効にする］が有効である
- Citrix XenApp、Microsoft RDS サーバの場合、コンソールセッションでないと［印刷操作をパスワードで保護する］オプションを有効にしても、パスワード入力による印刷抑止の解除はできません。

(7)　デバイスの使用抑止の注意事項

- JP1/IT Desktop Management 2 では、Windows の規定に従ってデバイスを制御します。そのため、Windows の規定に従っていないデバイスは制御できません。対象のデバイスが制御できるかどうか、あらかじめ検証することをお勧めします。なお、デバイスの仕様については製造元のメーカーにお問い合わせください。
- デバイスを接続したコンピュータの OS によっては、デバイスが認識されないことがあります。そのため、使用する OS ごとに正しく制御できるかどうか、あらかじめ検証することをお勧めします。
- Windows がデバイスをどのように認識するかは、デバイスの形状や製品名だけでは判断できません。Windows の［デバイス マネージャー］のプロパティを確認してください。

- 次の場合は、セキュリティポリシーを設定していても抑止できないことがあります。
  - コンピュータの起動直後など、JP1/IT Desktop Management 2 のプロセス起動前にデバイスが接続された場合
- 他製品によるデバイスの使用抑止とは同時に使用できません（Windows のグループポリシー、Active Directory のポリシー適用など）。他製品と同時に機器の使用を抑止した場合、それぞれの製品での設定が正しく実行されないおそれがあります。
- 次の場合は、コンピュータの再起動が必要です。
  - USB デバイス以外のデバイスで、セキュリティポリシーが適用される前から接続しているデバイスを抑止する場合
  - USB デバイス以外のデバイスで、動作中のデバイスを抑止する場合
  - 変更前のセキュリティポリシーで抑止していて、変更後は抑止しないデバイスを利用できるようにする場合
  - 変更前のセキュリティポリシーで抑止していなかったデバイスを変更後に抑止する場合
- ファイルの操作ログを取得している状態で、デバイスの使用を抑止してファイルの操作ログを取得するセキュリティポリシーに変更する場合、変更直前のファイルの操作ログが取得できないおそれがあります。
- 次の場合は、エラーが表示されることがあります。
  - 自動再生機能が有効に設定されているデバイスを抑止した場合
  - 使用を抑止しているデバイスに対して、ツールでアクセスした場合
  - コンピュータに初めて接続するデバイスが抑止対象の場合
  - ファイル操作中にデバイスを抑止する場合
- 他製品で実施したデバイスに対する設定がセキュリティポリシーに反する場合、セキュリティポリシーに従い、設定を変更します。
- 抑止しているデバイスのシステム情報やハードウェア情報は取得できません。
- 抑止対象のデバイスを初めてコンピュータに接続した場合、デバイスドライバのインストールができないおそれがあります。ドライバがインストールできなかったときは、接続したデバイスは利用できません。
- 同じデバイスでも、接続するポートやユーザーが異なる場合はデバイスドライバのインストールが実行されることがあります。このデバイスが抑止する前からコンピュータに接続していた場合、デバイスの抑止はコンピュータの再起動後に有効になります。
- 再起動しないと抑止が有効にならないデバイスが接続された状態で、別のデバイスを接続すると、抑止が有効になっていないデバイスの抑止ダイアログが再度表示されたり、警告メッセージが発行されたりします。
- OS が抑止対象デバイスを別のデバイスとして認識した場合、そのデバイスは抑止できません。ただし、OS の認識が別の抑止対象デバイスと一致した場合は OS が認識したデバイスとして抑止されます。

- 1 つ以上のデバイスを抑止するセキュリティポリシーを Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、Windows Server 2008、または Windows Vista のコンピュータに適用した場合、イベントログにエラーレベルのイベントが記録される場合があります。
- 抑止対象デバイスに対して、ツールなどでアクセスした場合、イベントログにイベントが出力されたり、エラーダイアログが表示されたりすることがあります。
- USB デバイス以外のデバイスで、一度コンピュータに接続して抑止されたデバイスを、デバイスが抑止された状態で再度接続した場合、抑止メッセージの表示、接続・切断・抑止ログ、および抑止イベントの取得はできません。
- Citrix XenApp、Microsoft RDS サーバの場合、接続元の機器に存在するドライブは接続先のセッションでドライブ種別が「その他」のドライブとして表示されます。そのようなドライブに対しては、デバイスの使用を抑止できません。
- デバイスの使用抑止を使用する場合、エージェントで「Portable Device Enumerator Service」サービスが起動している必要があります。このサービスが起動していない場合、デバイスの使用が抑止されない、デバイスが抑止され続ける、など、動作が不安定になる場合があります。

  次の条件がすべて重なった場合に発生する可能性があります。現象を回避する場合、「Portable Device Enumerator Service」の「スタートアップの種類」を確認し、「無効」の場合、「手動」か「自動」に設定してマシンを再起動してください。

  - 「Portable Device Enumerator Service」が起動していない。
  - セキュリティポリシーの［禁止操作］－［機器の使用抑止］－［書き込み抑止デバイスの一覧］で、次の設定のどれかを有効にしたセキュリティポリシーが適用されている、または適用したことがある。
    - リムーバブルディスク
    - CD/DVD ドライブ
    - FD ドライブ
- デバイスの接続抑止が無効であるセキュリティポリシーが適用されていると、コンピュータに存在する無効状態のデバイス※が有効化されることがあります。

  注※　接続抑止できるデバイス（USB デバイス、Bluetooth デバイスなど）すべてを指します。

USB デバイスの使用抑止の注意事項

- USB 接続の CD/DVD ドライブを抑止した場合、抑止された CD/DVD ドライブのトレーが開くことがあります。
- 抑止を設定したセキュリティポリシーを適用する前から接続されていた USB デバイスは抑止されません。この場合、デバイスを一度取り外し、再度接続することで抑止が有効になります。
- USB スキャナなどは USB 接続であってもイメージングデバイスと認識される場合があります。
- 接続方法が USB であっても、USB デバイス、Bluetooth デバイス、およびイメージングデバイスとして認識されないデバイスは抑止できません。

- 抑止対象の USB デバイスをコンピュータに接続した場合、自動再生機能を有効に設定されていると、自動再生が失敗して、エラーメッセージが表示されることがあります。
- 自動再生機能を有効に設定されていると、USB 接続のハードディスクドライブおよび FD ドライブの使用を抑止できません。これらのデバイスの使用を抑止する場合は自動再生機能を無効にしてください。
- Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、Windows Server 2008、または Windows Vista で自動再生機能を有効に設定されていると、USB 接続のハードディスクドライブ、および FD ドライブを抑止できない場合があります。
- セキュリティポリシーで USB デバイスの［使用を抑止する］または［登録済みの USB デバイスは使用を許可する］を有効にしている場合、リムーバブルドライブおよび固定ドライブの自動再生機能が無効になります。自動再生機能が無効になったあとに、USB デバイスの［使用を抑止する］または［登録済みの USB デバイスは使用を許可する］を無効にしたり、エージェントのアンインストールを実施したりした場合でも、自動再生機能の設定は無効のままです。
- 次に示す条件をすべて満たす場合、USB 接続の HD ドライブまたは FD ドライブのファイルコピーを実行しているときは、ファイルコピーが完了するまでは USB デバイスの使用を抑止できません。
  - コンピュータの OS が Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、Windows Server 2008、または Windows Vista である
  - ファイルコピーの実行中に USB デバイスの使用を抑止するセキュリティポリシーを適用した
- USB デバイスの「接続名」で抑止対象から外す設定のセキュリティポリシーを適用した場合、抑止対象から外した USB デバイスをコンピュータに初めて接続すると、「接続名」が取得できないため、USB デバイスが抑止されることがあります。この場合、再度 USB デバイスを接続してください。
- コンピュータの OS が Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8 または Windows Server 2012 の場合で、USB デバイスが記憶域プールに割り当てられているときは、抑止されません。
- 一度コンピュータに接続して抑止されたデバイスを再度を接続した場合、抑止メッセージの表示、接続・切断・抑止ログ、および抑止イベントが取得できないことがあります。
- 同一個体のデバイスであっても、通常認識された場合と UASP 認識された場合では、OS が付与する列挙子やデバイスインスタンス ID が変化します。そのため、両方の認識時に接続を許可するには、両方の認識時に資産登録をする必要があります。

Bluetooth デバイスの使用抑止の注意事項

- Bluetooth デバイスの抑止を設定すると、Bluetooth で接続しているマウスやキーボードなどの使用も抑止されます。
- Bluetooth デバイスをコンピュータに接続すると、次の Bluetooth デバイスのハードウェア ID のレジストリが作成されます。

  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Enum¥USB¥

JP1/IT Desktop Management 2 では、このレジストリの Class の値が「Bluetooth」「BTW」「BTM」の場合を Bluetooth デバイスとして扱います。ハードウェア ID は OS のデバイスマネージャから確認できます。

Windows ポータブルデバイスの使用抑止の注意事項

Windows ポータブルデバイスの使用抑止を設定したコンピュータで、USB デバイスが Windows ポータブルデバイスと認識された場合、Windows ポータブルデバイスとして使用が抑止されます。使用を許可している登録済みの USB デバイスや、[USB デバイスの登録] で接続した USB デバイスも、Windows ポータブルデバイスとしての使用が抑止されます。

2.9.6 更新プログラムの管理

組織内の OS が Windows のコンピュータには、不具合を修正したりセキュリティ上の問題を修正したりするために、必要に応じて更新プログラムを適用します。JP1/IT Desktop Management 2 では、日本マイクロソフト社からリリースされた更新プログラムを、セキュリティポリシーに従って自動的にコンピュータに適用できます。

重要

更新プログラムの最新情報を自動的に取得して、更新プログラムをコンピュータに適用するにはサポートサービス契約が必要です。

ヒント

UNIX エージェント側で通知を抑止していなければ、ソフトウェア情報として UNIX エージェント（AIX、HP-UX、Solaris）から OS パッチを取得できます。ただし、OS パッチの最新情報を自動的に取得して UNIX エージェントに適用することはできません。

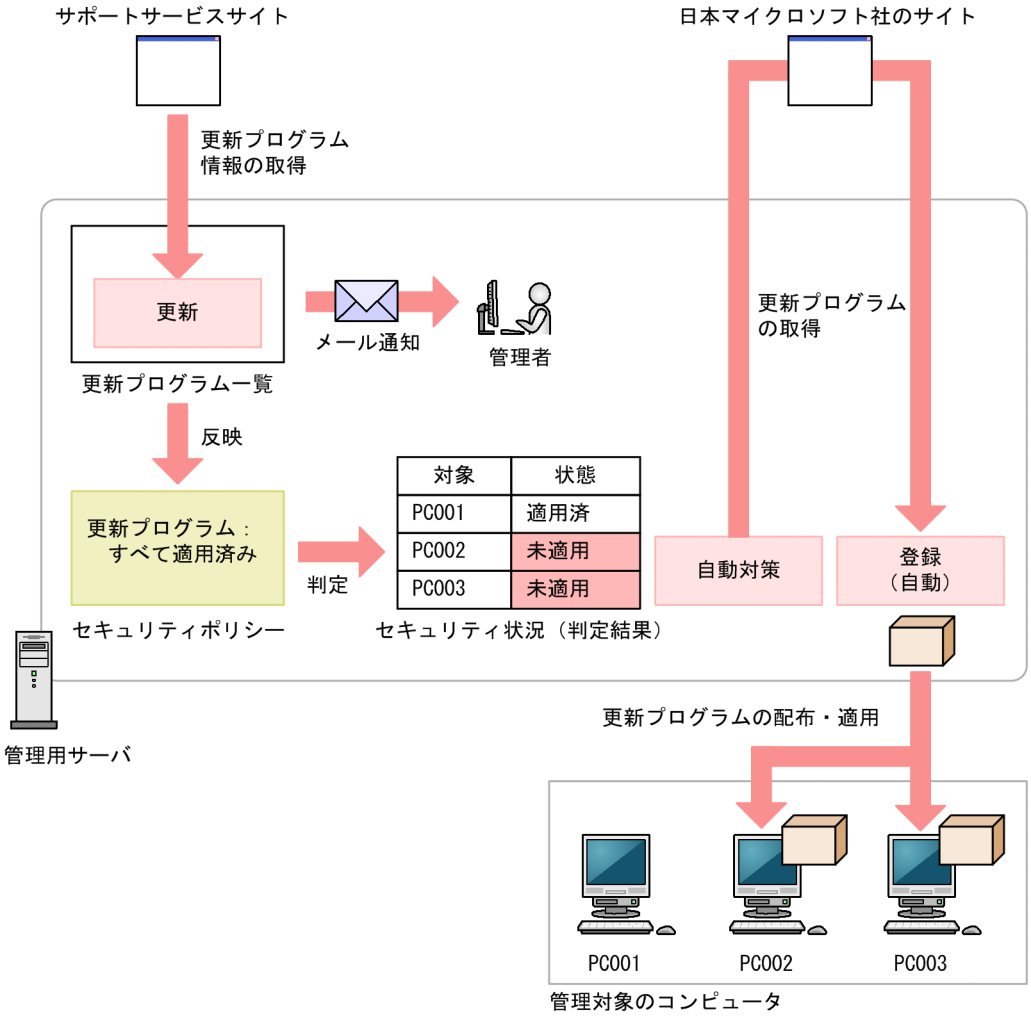
ヒント

Mac エージェントの場合、セキュリティポリシーの更新プログラムの自動更新の項目で、App Store のアップデートの自動確認が有効になっているかどうかを判定できます。ただし、更新プログラムを自動的に取得して Mac エージェントに適用することはできません。

JP1/IT Desktop Management 2 では、次に示すような便利な機能を利用して更新プログラムを管理する手間を軽減できます。

- 更新プログラムのリリースを確認できる
- コンピュータに更新プログラムを自動的に配布、適用できる
- 適用する更新プログラムの組み合わせをグループごとに変えて管理できる

更新プログラムの管理は、セキュリティ画面の［更新プログラム］画面で実行します。更新プログラムを管理する概念を次の図に示します。



日本マイクロソフト社から更新プログラムがリリースされると、サポートサービスサイトから更新プログラムの情報が自動的に取得されます。このとき、管理者に自動的にメール通知できます。更新プログラムの情報が取得されると、更新プログラムの一覧が自動的に更新されます。

セキュリティポリシーで［すべての更新プログラムが適用済み］を設定する場合、一覧に追加された更新プログラムの情報はセキュリティポリシーに反映され、自動的に最新の適用状況が判定されます。未適用のコンピュータがあった場合は、自動的に更新プログラムを配布して適用できます。

また、更新プログラムグループを作成することで、セキュリティポリシーごとに判定対象の更新プログラムを変えられます。テスト用のグループを作成することで、まず組織内のコンピュータに更新プログラムを適用しても問題がないかどうかをテストして、問題がないものだけ自動的に適用するといった運用ができます。

なお、手動で更新プログラムを登録して、配布することもできます。

サポートサービスからの情報の取得については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」を参照してください。

ヒント

セキュリティポリシーによる更新プログラムの自動配布の機能と、Windows の自動更新機能（Windows Update や Microsoft Update）を併用することもできます。ただし、どちらの機能によって更新プログラムが適用されるかを JP1/IT Desktop Management 2 で制御することはできません。 日本マイクロソフト社から適用必須として提供される更新プログラムをすべて適用したい場合は、Windows 自動更新を有効にすることをお勧めします。特定の更新プログラムだけを適用したい場合は、JP1/IT Desktop Management 2 の機能を使用して配布することをお勧めします。

ヒント

Windows の累積的な更新プログラムおよびセキュリティマンスリー品質ロールアップの場合、最新の更新プログラムが公開されてからサポートサービスサイトの更新プログラムの情報が更新されるまでの間であってもセキュリティ判定ができます。また、更新プログラムを適用する猶予期間を考慮したセキュリティ判定もできます。ただし、最新の累積的な更新プログラムおよびセキュリティマンスリー品質ロールアップは、セキュリティポリシーによる更新プログラムの自動配布ができません。詳細は、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の Windows の累積的な更新プログラムおよびセキュリティマンスリー品質ロールアップの判定の説明を参照してください。

ヒント

リモートインストールマネージャで、Windows の更新プログラムおよび Windows 10 の Feature Update をパッケージングして配布することもできます。詳細は、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の更新プログラムを管理する説明を参照してください。

更新プログラムグループの作成

セキュリティポリシーで、[指定した更新プログラムが適用済み] を設定する場合、更新プログラムグループを利用して、管理者が適用を許可した更新プログラムだけをセキュリティポリシーに反映できます。更新プログラムグループについては、「(9)　更新プログラムグループの管理」を参照してください。

関連リンク

- (1)　更新プログラムを取得・配布するための前提条件
- (3)　情報を自動取得できる更新プログラムの種類
- (2)　更新プログラムを取得する場合の注意事項
- (6)　更新プログラムの適用状況の確認

(1) 更新プログラムを取得・配布するための前提条件

サポートサービスサイトから取得した更新プログラム情報を基に、日本マイクロソフト社のサイトから更新プログラムを取得して、コンピュータに自動的に配布するための前提条件を次に示します。

自動でサポートサービスサイトから更新プログラム情報を取得する条件

- サポートサービス契約をしている
- MSXML 4.0 Service Pack 2 または MSXML 6.0 がインストールされている
- 管理用サーバがインターネット接続できる

ヒント

サポートサービスサイトから更新プログラム情報を取得するためには、サポートサービスサイトに接続するための設定が必要です。

ヒント

管理用サーバがインターネット接続できない環境でも、ほかにインターネット接続できるコンピュータがあれば、手動でサポートサービスサイトから更新プログラム情報を取得して登録できます。

自動で日本マイクロソフト社の Web サイトから更新プログラムを取得して配布する条件

- 管理用サーバがインターネット接続できる
- 管理用サーバと配布先のコンピュータが接続されている
- 配布先のコンピュータにエージェントが導入されている

ヒント

更新プログラムをコンピュータに配布するためには、更新プログラムファイルが必要です。日本マイクロソフト社の Web サイトにインターネット接続できる環境の場合、自動的に更新プログラムがダウンロードされ更新プログラムファイルが登録されます。

管理用サーバがインターネット接続できない環境でも、ほかのインターネット接続できるコンピュータを利用して日本マイクロソフト社の Web サイトから更新プログラム（実行ファイル）を取得すれば、手動で更新プログラムファイルを登録できます。

(2) 更新プログラムを取得する場合の注意事項

更新プログラムを取得する場合の注意事項を次に示します。

- 取得した更新プログラムをコンピュータに配布する場合は、対象のコンピュータに正しく配布および適用できるかを十分に確認してから配布してください。コンピュータの環境によっては、更新プログラムの配布または適用が失敗するおそれがあります。
- 次に示す更新プログラムは取得できません。
  - 2006 年 1 月 1 日より前に日本マイクロソフト社から提供された更新プログラム
  - マイクロソフト セキュリティ アドバイザリから提供される更新プログラム
  - PC-98 シリーズのコンピュータに対応した更新プログラム
- 更新プログラム情報に関するファイルは、*JP1/IT Desktop Management 2 のインストール先フォルダ*¥mgr¥OSPATCH 以下に格納されます。このフォルダ配下のファイルは変更または削除しないでください。変更または削除した場合、JP1/IT Desktop Management 2 の動作は保証されません。
- セキュリティポリシーの更新プログラムの自動対策で「Windows 自動更新を実行」を選択している場合、電源が OFF の機器に対して Windows 自動更新が実行されると、該当の機器の電源を自動的に ON にします。Windows 自動更新が完了すると、機器の電源を OFF にします。

関連リンク

- (1)　更新プログラムを取得・配布するための前提条件

(3)　情報を自動取得できる更新プログラムの種類

サポートサービスサイトと接続することで、日本マイクロソフト社からリリースされた更新プログラムの情報を取得して、自動的にセキュリティ判定の対象にできます。また、セキュリティポリシーで自動対策を設定しておくことで、更新プログラムをコンピュータに自動配布して適用できます。

次の表に示すプログラムの更新プログラム情報が、サポートサービスサイトから自動的に取得されます。

プログラム	種類またはバージョン
Windows	Windows Server 2019
	Windows Server 2016
	Windows 10
	Windows 8.1
	Windows 8
	Windows 7
	Windows Server 2012
	Windows Server 2008
	Windows Vista
	Windows Server 2003
	Windows XP

プログラム	種類またはバージョン
Internet Explorer	9.0 以降

また、更新プログラム情報を取得できるのは、これらのプログラムの更新プログラムのうち次の条件を満たすものです。

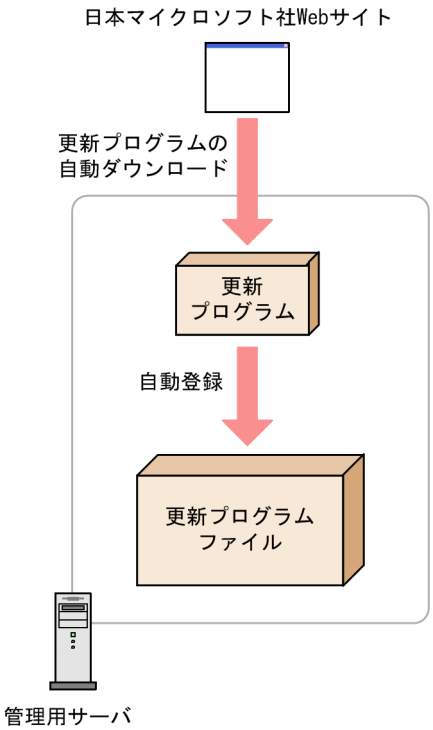
- クラス（更新プログラムの種類）が「更新プログラム」である
- セキュリティ番号が設定されている（空でない）
- セキュリティ深刻度が「緊急」または「重要」である
- 対象 OS のサービスパック番号またはバージョンの情報が存在する

(4)　更新プログラムファイルの自動登録

配布に必要な更新プログラムおよびインストールスクリプトは、日本マイクロソフト社の Web サイトおよびサポートサービスサイトから自動的にダウンロードされ、更新プログラムファイルが登録されます。常に最新の更新プログラムを取得して配布できるため、管理者が更新プログラムを定期的にダウンロードする手間が省けます。

> **重要**
>
> 更新プログラムおよびインストールスクリプトの自動ダウンロードには、サポートサービス契約が必要です。

更新プログラムファイルを自動的に登録する流れを次の図に示します。



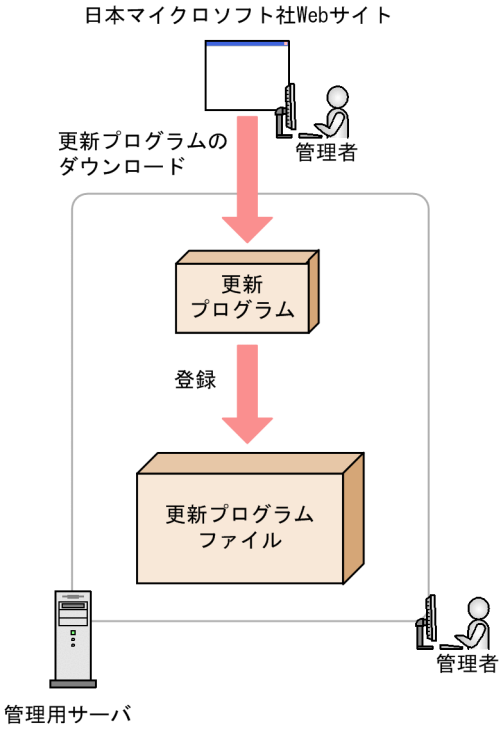
なお、登録された更新プログラムファイルは、配布（ITDM 互換）画面の［パッケージ一覧］には追加されません。更新プログラムファイルは、セキュリティポリシーの自動対策だけで配布できます。手動で更新プログラムを配布するタスクを作成することはできません。実行されたタスクは配布（ITDM 互換）画面で確認できます。

(5)　更新プログラムファイルの手動登録

日本マイクロソフト社の Web サイトから、配布に必要な更新プログラムをダウンロードすることで、管理者が任意のタイミングで管理用サーバに更新プログラムを追加して更新プログラムファイルを登録できます。追加した更新プログラムは、自動的に利用者のコンピュータに適用されます。セキュリティに関する重要な更新プログラムを、JP1/IT Desktop Management 2 の自動配布を待たないで至急配布したいときなどに便利です。

更新プログラムファイルを手動で登録する場合、更新プログラムのダウンロードおよび更新プログラムファイルの登録をすべて管理者自身で行ってください。

更新プログラムファイルを手動で登録する流れを次の図に示します。



ヒント

管理者のコンピュータがインターネットに接続できない環境の場合（更新プログラム一覧をオフラインで更新している場合）、インターネットに接続できるコンピュータで更新プログラムファイルを登録します。

この場合、インターネット接続できるコンピュータで操作画面を表示して、［更新プログラム］画面の［更新プログラムの情報］タブに表示される［更新プログラムのダウンロード URL］か

ら、更新プログラムをダウンロードします。そのあと、[操作メニュー]の[更新プログラムファイルを登録する]を選択し、ダウンロードした更新プログラムを指定することで更新プログラムファイルを登録できます。

なお、作成された更新プログラムファイルは、配布（ITDM 互換）画面の［パッケージ一覧］には追加されません。更新プログラムファイルは、セキュリティポリシーの自動対策だけで配布できます。手動で更新プログラムを配布するタスクを作成することはできません。実行されたタスクは配布（ITDM 互換）画面で確認できます。

ヒント

手動登録した更新プログラムは、セキュリティポリシーの適正状態［すべての更新プログラムが適用済み］では判定されません。セキュリティ判定をするためには、手動登録した更新プログラムを［更新プログラムグループ］に登録し、セキュリティポリシーの［更新プログラム］で次のように設定すると、手動登録した更新プログラムを判定し、違反があれば自動対策も実施します。

設定項目：[更新プログラム適用]をチェックする

適正状態：[指定した更新プログラムが適用済み]－[必須とする更新プログラムグループ：]に、更新プログラムグループを選択する

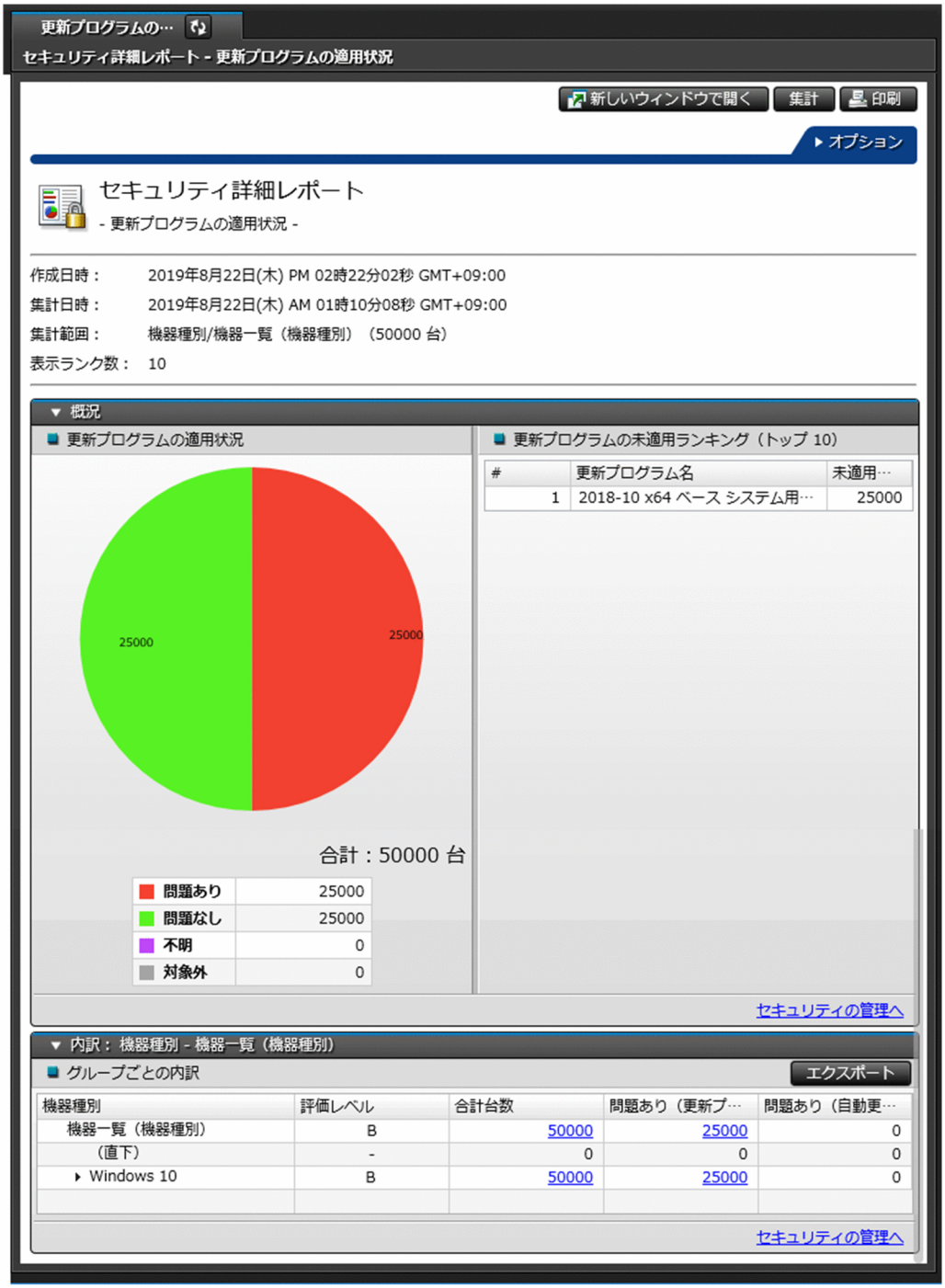
自動対策：チェックし、[更新プログラムを配布]を選択する

(6) 更新プログラムの適用状況の確認

次に示す方法で、更新プログラムの適用状況を確認できます。

未適用のコンピュータが存在する更新プログラムを確認する

セキュリティ詳細レポートの［更新プログラムの適用状況］レポートで、未適用のコンピュータが多い順に、更新プログラムを確認できます。

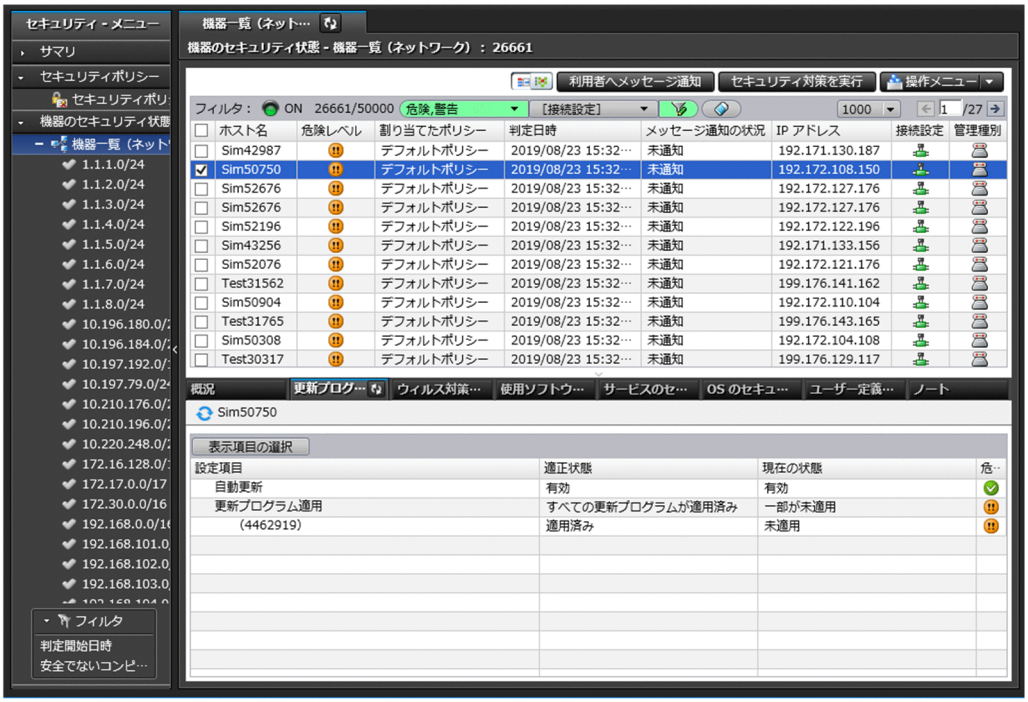


セキュリティポリシーごとに危険レベルを確認する

セキュリティ画面の［セキュリティポリシー一覧］画面の［更新プログラム］タブで、危険レベルを確認できます。危険レベルに問題がある場合は、更新プログラムが未適用のコンピュータが存在するおそれがあります。

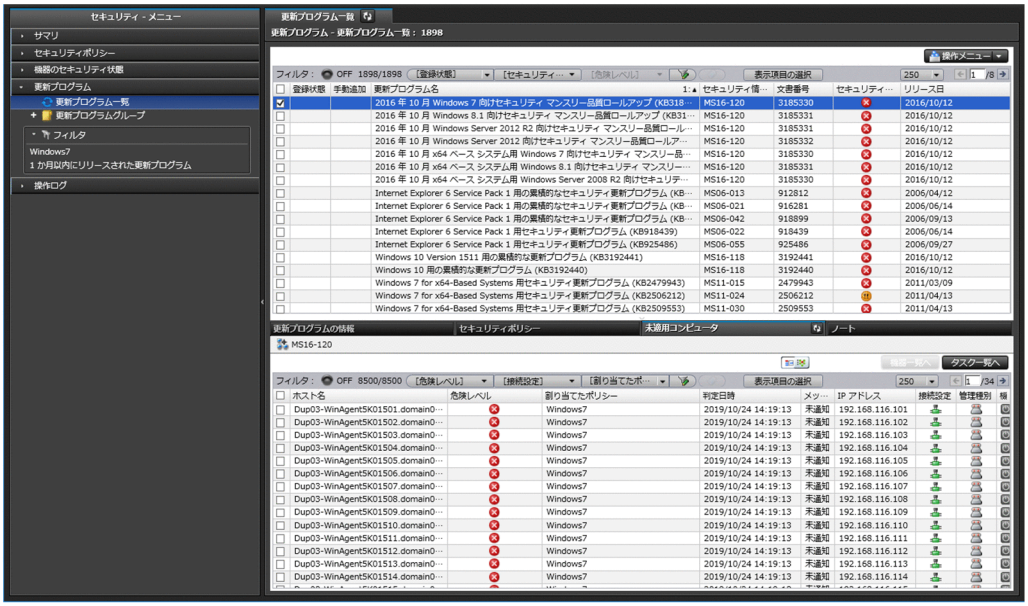
機器ごとに更新プログラムの適用状況を確認する

セキュリティ画面の［機器のセキュリティ状態］画面の［更新プログラム］タブで、各機器の更新プログラムの適用状況を確認できます。コンピュータに未適用の更新プログラムがある場合は、対象の更新プログラムが表示されます。



更新プログラムごとに未適用のコンピュータを確認する

セキュリティ画面の［更新プログラム一覧］画面の［未適用コンピュータ］タブで、更新プログラムごとに未適用のコンピュータを確認できます。



(7)　更新プログラム一覧の更新

管理者が設定したスケジュールやサポート契約情報に基づいて、定期的にサポートサービスサイトへアクセスして、JP1/IT Desktop Management 2 に登録されている古い更新プログラムの一覧を自動的に更新できます。これによって、管理者が特別な操作を実施しなくても、すべてのコンピュータに最新の更新プログラムが適用されているかを確認したり、適用されていない更新プログラムを確認したりできるようになります。

更新プログラム一覧の更新は、1 日 1 回自動的に実施されます。実施するタイミングは、JP1/IT Desktop Management 2 のインストール後に実施するセットアップが完了したときの時間です。分は切り上げとなります。例えば、JP1/IT Desktop Management 2 のセットアップが 10 時 30 分に完了した場合、更新プログラム一覧は、11 時 00 分に更新されます。

重要

サポートサービス契約をしていて、かつ管理用サーバがインターネットに接続できる環境が必要です。

重要

更新プログラムの一覧が自動的に更新されるのは、更新プログラムが日本マイクロソフト社からリリースされてから、約 10 営業日後になります。これは、サポートサービスサイトの情報が更新されるまでに、更新プログラムのリリースから 10 日間ほど掛かるためです。リリースされた更新プログラムの情報をすぐに追加したい場合は、管理者自身が日本マイクロソフト社の Web サイトから更新プログラムおよび更新プログラムの情報を入手して、更新プログラム一覧に手動で追加してください。

関連リンク

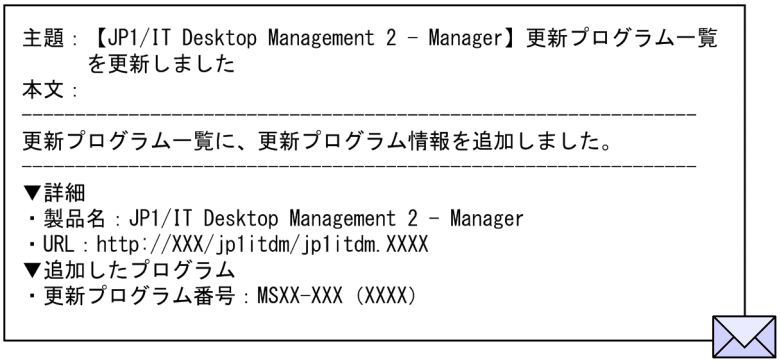
- (3)　情報を自動取得できる更新プログラムの種類
- (5)　更新プログラムファイルの手動登録

(8)　更新プログラム一覧の更新のメール通知

自動的に更新プログラム一覧が更新された場合に、更新された内容を管理者にメールで通知できます。メールには追加された更新プログラムの情報について記載されています。管理者はメールを見るだけで、追加された更新プログラムについて詳細をすぐに把握できます。

> **重要**
>
> 事前にメールサーバの設定、およびサポートサービスの設定が必要です。

通知されるメールの例を次の図に示します。

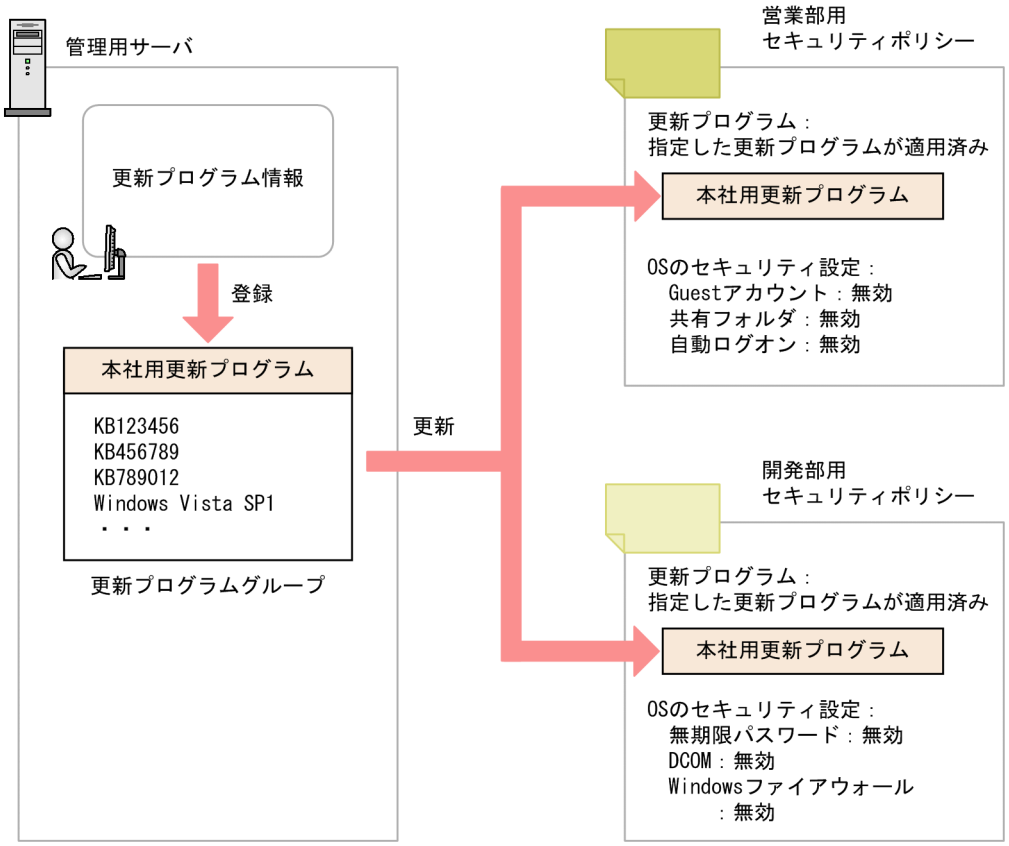


(9)　更新プログラムグループの管理

特定の更新プログラムだけを適用しているかどうか判定する場合、対象とする更新プログラムをまとめた更新プログラムグループを作成します。セキュリティポリシーで更新プログラムグループを指定することで、グループに登録した更新プログラムだけが判定対象になります。

また、更新プログラムグループを利用することで、異なるセキュリティポリシー間で、判定対象とする更新プログラムを一元管理できます。

更新プログラムグループを使用して、判定対象とする更新プログラムを管理する概念を次の図に示します。



例えば、営業部と開発部でセキュリティポリシーを分けている場合でも、適用する更新プログラムを共通化できます。 営業部用と開発部用のセキュリティポリシーで、更新プログラムの判定対象に共通の更新プログラムグループを指定することで、ポリシーの設定を分けながら適用する更新プログラムを共通で管理できます。

また、組織内に適用しても問題ないかどうかを確認してから更新プログラムを配布したい場合も更新プログラムグループを利用してください。サポートサービスから更新プログラムの情報を取得しても、更新プログラムグループには自動的には反映されません。更新プログラムグループに、更新プログラムを追加登録することで、セキュリティポリシーを編集することなく判定対象の更新プログラムを追加できます。このため、テスト済みの更新プログラムを更新プログラムグループに登録することで、管理者が許可した更新プログラムだけを適用管理できます。

(10)　更新プログラムの配布結果の判定

更新プログラムが正常に配布されたかどうかは、更新プログラム適用時の戻り値で判定されます。更新プログラム適用時の戻り値を次に示します。

戻り値	説明
0	インストールが正常終了しました。
1	インストールに失敗しました。
2	環境が不正です（メモリ不足、ファイルが不正など）。

戻り値	説明
3	内部エラーが発生しました。
4	Windows Script Host（WSH）のインストール状態が不正です。
5	内部エラーが発生しました。

(11) 更新プログラム一覧のインポートとエクスポート

管理用サーバに登録している更新プログラム一覧の情報を CSV ファイルにエクスポートできます。エクスポートした更新プログラム一覧の CSV ファイルを「パッチ情報 CSV ファイル」と呼びます。また、エクスポートしたパッチ情報 CSV ファイルを元の管理用サーバや別の管理用サーバにインポートできます。

更新プログラム一覧をインポートまたはエクスポートするコマンドを次に示します。

コマンド	機能
ioutils exportupdatelist	管理用サーバに手動で登録した更新プログラム一覧（パッチ情報 CSV ファイル）をエクスポートします。
ioutils importupdatelist	管理用サーバからエクスポートした更新プログラム一覧（パッチ情報 CSV ファイル）をインポートします。

これらのコマンドを使用することで、複数の管理用サーバを運用している場合に、各管理用サーバに登録されている更新プログラムを同じにすることができます。

2.10　操作ログの管理

セキュリティポリシーに操作ログの取得を設定して、対象のコンピュータにセキュリティポリシーを割り当てると、対象のコンピュータから操作ログを取得できます。

操作ログを取得するためには、対象のコンピュータにエージェントが導入されている必要があります。また、取得した操作ログを管理用サーバに保管する場合、管理用サーバのセットアップで操作ログを取得するように設定されている必要があります。

重要

API 管理機器は操作ログの管理ができません。

取得する操作ログの種類は、セキュリティポリシーの設定で変更できます。不審操作を検知するかどうかも、セキュリティポリシーの設定で変更できます。

不審操作の分類と操作画面での確認方法を次の表に示します。

分類	セキュリティポリシーで選択する不審と見なす操作	確認方法		
		セキュリティ画面－［操作ログ］－［操作ログ一覧］画面	イベント画面－［イベント］－［イベント一覧］	［不審操作の状況］パネル
ファイル持ち出しによる不審操作	［添付ファイル付きメールの送受信］	［不審操作］列 アイコンが表示されます。 ［操作種別（詳細）］列 ［メール送信（添付ファイル付）］が表示されます。	［種類］列に［不審操作］が表示されます。	［添付ファイル付きメールの送信］として表示されます。
	［Web/FTP サーバの使用］	［不審操作］列 アイコンが表示されます。 ［操作種別（詳細）］列 ［ファイルアップロード］または［ファイルダウンロード］が表示されます。	［種類］列に［不審操作］が表示されます。	［Web/FTP サーバの使用］として表示されます。
	［外部メディア（リムーバブルディスク）へのファイルコピーと移動］	［不審操作］列 アイコンが表示されます。 ［操作種別（詳細）］列 ［ファイルコピー］または［ファイル移動］が表示されます。	［種類］列に［不審操作］が表示されます。	［外部メディア（リムーバブルディスク）へのファイルコピーと移動］として表示されます。
印刷による不審操作	大量印刷	－	［種類］列に［不審操作］が表示されます。	－

（凡例）　－：表示されない

セキュリティポリシーでファイル持ち出しによる不審と見なす操作の条件を設定している場合、不審操作として検知されたファイル持ち出しによる不審操作の操作ログの履歴を追跡調査できます。

ファイル持ち出しによる不審操作の詳細については「2.10.3　ファイル持ち出しによる不審操作の、操作ログでの調査」を、印刷による不審操作の詳細については「2.10.5　印刷による不審操作の取得」を参照してください。

ヒント

すべての種類の操作ログを取得するとディスク容量が圧迫されるおそれがあります。情報漏えいに係わりの深い操作ログだけを取得したり、取得対象の操作を指定したりして、ディスク容量を節約できます。

重要

UNIX エージェントおよび Mac エージェントは操作ログ取得の対象外です。

重要

管理対象のコンピュータが 30,000～50,000 台の場合で操作ログを取得する場合は、複数サーバ構成で運用し、統括管理用サーバでは取得せず、管理用中継サーバで取得してください。また、管理用中継サーバから統括管理用サーバに送信しない設定にしてください。

重要

次のような場合、[不審操作の状況] パネルの日ごとの不審操作の数と、アンカーで遷移した操作ログ一覧の不審操作の件数が一致しないことがあります。

- エージェントからマネージャへの不審操作の通知にタイムラグが発生した場合。
  エージェントマシンの停止のタイミングやネットワークの問題により発生することがあります。
- エージェントとマネージャのシステム時刻が合っていない場合。
  操作ログはマネージャへの通知日の以前や以後の操作として登録されることがあります。
- 操作ログを利用している場合で、該当日の操作ログがリストアされていない場合。

この場合、[イベント] 画面で該当日の不審操作イベントを確認し、操作ログ一覧で該当する機器の不審操作を確認してください。もしくは、操作ログ一覧で前後の日付の操作ログを確認してください。

重要

エージェントの OS が Windows 7 の場合、Windows XP モード上での操作ログの取得はできません。

重要

16bit ソフトウェアの場合、プログラム起動/停止ログの取得、およびウインドウ操作ログの取得はできません。

2.10.1 取得できる操作ログの種類

JP1/IT Desktop Management 2 で取得できる操作ログの種類について次の表に示します。

ヒント

セキュリティポリシーで不審操作を検知する設定をしている場合、不審操作かどうかが操作ログを基に判定されます。この判定に使用されるのは、不審操作に関連する一部の種類の操作ログだけです。操作ログのポリシーで［情報漏えいに係わりの深い操作を取得対象にする（推奨)］をチェックすると、不審操作に関連する操作ログだけを取得できます。

操作ログの種類

操作種別	操作種別（詳細）	内容	操作ログのポリシーで［情報漏えいに係わりの深い操作を取得対象にする（推奨)］をチェックした場合の動作
コンピュータの起動と停止、ログオンとログオフ	コンピュータ起動	利用者がコンピュータを起動した。	○
	コンピュータ停止	利用者がコンピュータを停止した。	○
	ログオン	利用者が Windows にログオンした。	○
	ログオフ	利用者が Windows からログオフした。	○
プログラム起動/停止	プログラム起動	利用者がプログラムを起動した。	×
	プログラム停止	利用者がプログラムを停止した。	×
ファイル操作/印刷操作	ファイルコピー※1	利用者がファイルをコピーした。	△
	ファイル移動※1	利用者がファイルを移動した。	△
	ファイル名称変更※1	利用者がファイル名を変更した。	△
	ファイル作成※1	利用者がファイルを新規作成した。	△

操作種別	操作種別（詳細）	内容	操作ログのポリシーで［情報漏えいに係わりの深い操作を取得対象にする（推奨）］をチェックした場合の動作
ファイル操作/印刷操作	ファイル削除※1	利用者がファイルを削除した。	△
	ファイルアップロード※2	利用者が Web ブラウザを利用してファイルをアップロードした。	△
	ファイルダウンロード※2	利用者が Web ブラウザを利用してファイルをダウンロードした。	△
	ファイル送信※2	利用者が Web ブラウザを利用して FTP サーバにファイルを送信した。	△
	ファイル受信※2	利用者が Web ブラウザを利用して FTP サーバからファイルを受信した。	△
	メール送信（添付ファイル付）※3	利用者が添付ファイル付きのメールを送信した。	△
	メール受信（添付ファイル付）※3	利用者が添付ファイル付きのメールを受信した。	△
	添付ファイル保存※3	利用者が添付ファイル付きのメールを受信したあと、添付ファイルを保存した。	△
	印刷※4	利用者がプリンタで印刷をした。	×
フォルダ操作※1	フォルダコピー	利用者がフォルダをコピーした。	×
	フォルダ移動	利用者がフォルダを移動した。	×
	フォルダ名称変更	利用者がフォルダ名を変更した。	×
	フォルダ作成	利用者がフォルダを新規作成した。	×
	フォルダ削除	利用者がフォルダを削除した。	×
デバイス操作	デバイス接続	利用者がコンピュータにデバイスを接続した。	○
	デバイス切断	利用者がコンピュータからデバイスを切断した。	○
	デバイス接続許可	禁止操作で使用できるデバイスを設定している場合に、デバイスの接続を許可した。	○
Web アクセス	Web アクセス※2	利用者が Web ブラウザを利用して Web にアクセスした。	×
ウィンドウ操作	アクティブウィンドウの変更	利用者がアクティブウィンドウを変更した。	×
抑止ログ	プログラム起動抑止	使用禁止ソフトウェアを設定している場合に、プログラムの起動を抑止した。	○
	印刷抑止※4	禁止操作を設定している場合に、印刷を抑止した。	○

操作種別	操作種別（詳細）	内容	操作ログのポリシーで［情報漏えいに係わりの深い操作を取得対象にする（推奨）］をチェックした場合の動作
抑止ログ	デバイス接続抑止	禁止操作を設定している場合に、デバイスの使用を抑止した。	○

（凡例）○：取得する　△：持ち込みチェック条件に該当する場合に取得する　×：取得しない

持ち込みチェック条件については、「2.10.4　持ち込みチェックと持ち出しチェックの条件」を参照してください。

注※1

OS のエクスプローラ上で操作した場合に、操作ログを取得します。

> **重要**
>
> コマンドプロンプトやアプリケーションを使用して操作した場合は、操作ログを取得できません。

注※2

Internet Explorer 9、10、11 を利用している場合にだけ操作ログを取得できます。

> **重要**
>
> Internet Explorer の操作によって別のアプリケーションが起動され、そのアプリケーションで操作した場合は、操作ログを取得できません。

注※3

操作ログを取得できるメーラーを次に示します。

- Microsoft Outlook 2002、2003、2007、2010、2013、2016、2019
- Windows Live メール 2009、2011、2012

注※4

操作ログを取得できるプリンタを次に示します。

- ローカルプリンタ
- ネットワーク共有プリンタ
- 仮想プリンタ

重要

インターネット接続のプリンタでは操作ログを取得できません。また、ローカルプリンタで File ポートを使用する場合は「印刷抑止」の操作ログを取得できません。LAN Manager ポートを使用する場合は「印刷」と「印刷抑止」の操作ログを取得できません。

ヒント

秘文ログを取り込んだ場合は、「2.10.8　管理用サーバへの秘文ログの取り込み」を参照してください。

関連リンク

- (1)　ファイル持ち出しによる不審操作の取得
- 2.10.7　操作ログ取得の前提条件と注意事項

(1)　操作ログの種類ごとに取得される情報

操作ログの種類ごとに取得される情報を次に示します。なお、各情報で取得される内容については、「取得される情報の詳細」を参照してください。以降の表中では、凡例を次のとおり表記しています。

(凡例) ○：取得される　△：デバイスおよびディスクの状態によっては取得できない場合がある　×：取得されない

コンピュータの起動と停止、ログオンとログオフ

取得対象に「コンピュータの起動と停止、ログオンとログオフ」を設定した場合に、取得される情報を次の表に示します。

操作内容	取得される情報		
	発生元	操作日時※	ユーザー名
コンピュータ起動	○	○	×
コンピュータ停止	○	○	×
ログオン	○	○	○
ログオフ	○	○	○

注※　操作日時は、「操作日時（Web ブラウザのロケール）」、「操作日時」、および「タイムゾーン」です。

プログラム起動/停止

取得対象に「プログラム起動/停止」を設定した場合に、取得される情報を次の表に示します。なお、「発生元」、「操作日時（Web ブラウザのロケール）」、「操作日時」、「タイムゾーン」、および「ユーザー名」はすべての操作で取得されます。

操作内容	取得される情報		
	ユーザー名	ファイルバージョン※	ファイル名
プログラムの起動	○	○	○
プログラムの停止	○	○	○

注※　実行ファイルにファイルバージョンが存在する場合に限ります。

ファイル操作/印刷操作

取得対象に「ファイル操作/印刷操作」を設定した場合に、取得される情報を次の表に示します。なお、「発生元」、「操作日時（Web ブラウザのロケール）」、「操作日時」、「タイムゾーン」、および「ユーザー名」はすべての操作で取得されます。

操作内容	取得される情報					
	ファイル作成日時	ファイル更新日時	ファイルサイズ	持ち込み元ドライブ種別/持ち込み日時	持ち出し元ファイル名/ドライブ種別	持ち出し先ファイル名/ドライブ種別
ファイルコピー	○	○	○	○	○	○
ファイル移動	○	○	○	○	○	○
ファイル名称変更	○	○	○	○	○	○
ファイル作成	○	○	○	○	○	×
ファイル削除	○ ※1	○ ※1	○ ※1	○	○	×
ファイルアップロード	○	○	○	○	○	○
ファイルダウンロード	○	○	○	○	○	○
ファイル送信	○	○	○	○	○	○
ファイル受信	○	○	○	○	○	○
メール送信（添付ファイル付）	○	○	○	○	○	○
メール受信（添付ファイル付）	×	×	×	○	○	○

操作内容	取得される情報					
	ファイル作成日時	ファイル更新日時	ファイルサイズ	持ち込み元ドライブ種別/持ち込み日時	持ち出し元ファイル名/ドライブ種別	持ち出し先ファイル名/ドライブ種別
添付ファイル保存	○	○	○	○	○	○
印刷※2	×	×	×	×	×	×

注※1　ファイルの削除方法によっては、ファイル作成日時、ファイル更新日時、またはファイルサイズを取得できないことがあります。

注※2　「プリンタ名」、「印刷ドキュメント名」、「印刷ページ数」の情報だけ取得できます。

フォルダ操作

取得対象に「フォルダ操作」を設定した場合に、取得される情報を次の表に示します。なお、「発生元」、「操作日時（Web ブラウザのロケール）」、「操作日時」、「タイムゾーン」、および「ユーザー名」はすべての操作で取得されます。

操作内容	取得される情報			
	持ち出し元ファイル名	持ち出し元ドライブ種別	持ち出し先ファイル名	持ち出し先ドライブ種別
フォルダコピー	○	○	○	○
フォルダ移動	○	○	○	○
フォルダ名称変更	○	○	○	○
フォルダ作成	○	○	×	×
フォルダ削除	○	○	×	×

デバイス接続/切断

取得対象に「デバイス接続/切断」を設定した場合に、取得される情報を次の表に示します。なお、デバイスによっては、取得できない情報もあります。「発生元」、「操作日時（Web ブラウザのロケール）」、「操作日時」、「タイムゾーン」、および「ユーザー名」はすべての操作で取得されます。

操作内容	取得される情報						
	ドライブ種別※1	ドライブ名※2	デバイス名	シリアルナンバー	デバイスインスタンスID	デバイス種別※3	デバイス区分
デバイス接続	○	○	○	○	○	○	○

操作内容	取得される情報						
	ドライブ種別※1	ドライブ名※2	デバイス名	シリアルナンバー	デバイスインスタンスID	デバイス種別※3	デバイス区分
デバイス切断	△	△	△	△	△	△	△
デバイス接続許可	○	○	○	○	○	○	○

注※1　内蔵 FD ドライブ、Bluetooth デバイス、イメージングデバイス、および Windows ポータブルデバイスの場合は、「その他」が出力されます。

注※2　内蔵 FD ドライブ、Bluetooth デバイス、イメージングデバイス、および Windows ポータブルデバイスの場合は取得できません。

注※3　USB デバイスの場合だけ取得できます。

Web アクセス

取得対象に「Web アクセス」を設定した場合に、取得される情報を次の表に示します。なお、「発生元」、「操作日時（Web ブラウザのロケール）」、「操作日時」、「タイムゾーン」、および「ユーザー名」はすべての操作で取得されます。

操作内容	取得される情報	
	Web ページタイトル	URL
Web アクセス	○	○

ウィンドウ操作

取得対象に「ウィンドウ操作」を設定した場合に、取得される情報を次の表に示します。なお、「発生元」、「操作日時（Web ブラウザのロケール）」、「操作日時」、「タイムゾーン」、および「ユーザー名」はすべての操作で取得されます。

操作内容	取得される情報			
	実行アカウント	ファイルバージョン※	ファイル名	ウィンドウタイトル
ウィンドウ操作	○	○	○	○

注※　実行ファイルにファイルバージョンが存在する場合に限ります。

抑止ログ

「抑止ログ」には、「プログラム起動抑止」、「印刷抑止」、および「デバイス接続抑止」があります。それぞれを設定した場合に、取得される情報を次の表に示します。なお、「発生元」、「操作日時（Web ブラウザのロケール）」、「操作日時」、「タイムゾーン」、および「ユーザー名」はすべての操作で取得されます。

プログラム起動抑止

操作内容	取得される情報				
	ソフトウェア名	ソフトウェアバージョン	ユーザー名	ファイルバージョン※	ファイル名
プログラム起動抑止	○	○	○	○	○

注※　実行ファイルにファイルバージョンが存在する場合に限ります。

印刷抑止

操作内容	取得される情報		
	プリンタ名	印刷ドキュメント名	印刷ページ数
印刷抑止	○	○	×

デバイス接続抑止

操作内容	取得される情報						
	ドライブ種別※1	ドライブ名※2	デバイス名	シリアルナンバー	デバイスインスタンス ID	デバイス種別※3	デバイス区分
デバイス接続抑止	○	○	○	○	○	○	○

注※1　内蔵 FD ドライブ、Bluetooth デバイス、イメージングデバイス、および Windows ポータブルデバイスの場合は、「その他」が出力されます。

注※2　内蔵 FD ドライブ、Bluetooth デバイス、イメージングデバイス、および Windows ポータブルデバイスの場合は取得できません。

注※3　USB デバイスの場合だけ取得できます。

取得される情報の詳細

操作ログで取得される情報の詳細を次に示します。

項目	内容
発生元	操作ログを取得したコンピュータの FQDN（完全修飾ドメイン名）です。 表示例：dmp530
ホスト識別子	システム内でコンピュータを識別するためのユニークな ID です。
操作日時（Web ブラウザのロケール）	操作が発生した日時です。操作ログを表示するコンピュータのローカルタイムに変換して表示されます。 表示例：2011/10/01 22:00:01
操作日時	操作が発生した日時です。操作ログを取得したコンピュータのローカルタイムで表示されます。 表示例：2011/10/02 17:11:51

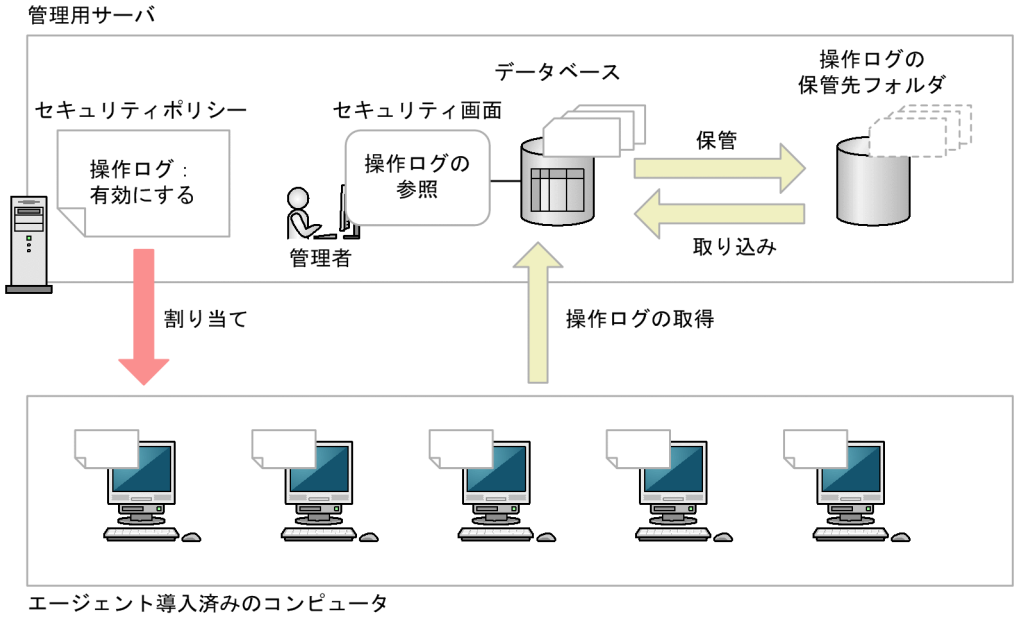
項目	内容
タイムゾーン	操作が発生したコンピュータのタイムゾーンです。UTC との差が表示されます。[操作ログの詳細] ダイアログでは、「操作日時」の項目に表示されます。 表示例：GMT+09:00
ユーザー名	発生元のコンピュータにログオンしている利用者のアカウント名です。 表示例：Hostname¥user1
実行アカウント	発生元のプログラムの実行アカウント名です。 表示例：Hostname¥user1
ファイルバージョン	操作対象のファイルの［プロパティ］ダイアログで、[バージョン情報］タブに表示されているファイル バージョンです。 表示例：1.0.0.111
ファイル名	操作対象のファイルのパスを含むファイル名です。 表示例：C:¥TEMP¥game.exe
ファイル作成日時	操作対象のファイルの作成日時です。 表示例：2011/10/01 22:00:01
ファイル更新日時	操作対象のファイルの更新日時です。 表示例：2011/10/02 22:00:01
ファイルサイズ	操作対象のファイルのファイルサイズです。 表示例：10.2KB
持ち込み元ドライブ種別	ファイル持ち出しによる不審操作を検知したときに、オリジナルのファイルがどこから入力されたものかを示します。 • その他 • ローカルディスク • ネットワークドライブ • リムーバブルディスク • CD-ROM • RAM ディスク • Web • FTP • メール 表示例：RAM ディスク
持ち込み日時	操作ログを取得し始めてから、初めて操作対象のファイルが確認された日時です。 表示例：2011/10/01 22:00:01.159
持ち出し元ファイル名	操作対象のファイル（フォルダ）のフルパス、または URL（Web アップロード、FTP 受信）です。ネットワークドライブの場合は、UNC 形式になります。また、添付ファイルがあるメールを受信した場合はメールヘッダ、添付ファイルを保存した場合はパスを含まないファイル名になります。 表示例：¥¥dmp110¥share
持ち出し元ドライブ種別	操作対象のファイルが格納されているドライブの種別です。 • その他 • ローカルディスク

項目	内容
持ち出し元ドライブ種別	• ネットワークドライブ • リムーバブルディスク • CD-ROM • RAM ディスク • Web • FTP • メール 表示例：ローカルディスク
持ち出し先ファイル名	操作対象のファイル（フォルダ）のフルパス、または URL（Web ダウンロード、FTP 送信）です。ネットワークドライブの場合は、UNC 形式になります。また、添付ファイルがあるメールを送信した場合はメールヘッダ、添付ファイルがあるメールを受信した場合はパスを含まないファイル名になります。 表示例：c:¥work¥program
持ち出し先ドライブ種別	操作先のファイルが格納されているドライブの種別です。 • その他 • ローカルディスク • ネットワークドライブ • リムーバブルディスク • CD-ROM • RAM ディスク • Web • FTP • メール 表示例：ネットワークドライブ
プリンタ名	印刷したプリンタの名称です。 表示例：printserver01
印刷ドキュメント名	印刷したドキュメント名です。 表示例：機能仕様書.doc
印刷ページ数	印刷したページの総数です。取得できない場合は表示されません。 表示例：5
ドライブ種別	コンピュータに接続されたドライブの種別です。情報は数字で表示されます。 • その他 • ローカルディスク • ネットワークドライブ • リムーバブルディスク • CD-ROM • RAM ディスク • Web • FTP • メール

項目	内容
ドライブ種別	表示例：ネットワークドライブ
ドライブ名	コンピュータに接続されたドライブ名です。「A:」から「Z:」のどれかになります。 表示例：G:
デバイス名	接続されたデバイスの名称です。 表示例：Hitachi USB xxxxx
シリアルナンバー	接続されたデバイスのシリアルナンバーです。 表示例：1234567890ABCD
デバイス種別	接続されたデバイスの種類です。 表示例：ディスクドライブ
デバイス区分	デバイスを区別するための種別です。 表示例：内蔵 SD カード
デバイスインスタンス ID	接続されたデバイスのデバイスインスタンス ID です。 表示例：USB¥VID_xxxx&PID_xxxx¥1234567890ABCD
Web ページタイトル	利用者がアクセスした Web のタイトルです。 表示例：日立製作所ホームページ
URL	利用者がアクセスした Web の URL です。 表示例：http://www.hitachi.co.jp/
ウィンドウタイトル	アクティブになっているウィンドウのキャプションです。 表示例：game
ソフトウェア名	起動を抑止したソフトウェアの名称です。セキュリティポリシーに設定された、起動抑止ソフトウェアのソフトウェア名が表示されます。 表示例：game
ソフトウェアバージョン	起動を抑止したソフトウェアのバージョンです。セキュリティポリシーに設定された、起動抑止ソフトウェアのバージョンが表示されます。 表示例：5.1.2600.5512

2.10.2　管理用サーバでの操作ログの管理

オンライン管理のコンピュータから取得された操作ログは、管理用サーバを経由して操作ログの保管先に保管されます。管理用サーバのデータベースに取り込むことにより、セキュリティ画面の［操作ログ］画面から参照できます。



（凡例）

：セキュリティポリシー

：操作ログ

：保管された操作ログ

管理用サーバでの操作ログの保存

管理用サーバに取得された操作ログは、操作ログの保管先に保存されます。なお、操作ログの自動取り込みを有効にすると、自動的に操作ログのデータベースに操作ログを取り込めます。保管先フォルダに保存された操作ログは、保管先フォルダからデータベースに取り込んで参照できます。

取り込んだ操作ログをデータベースから削除することで、異なる期間の操作ログをデータベースに取り込み直すこともできます。これによって、過去の操作ログを参照できます。

操作ログを取り込む場合、取り込み済みのデータに設定した範囲の一部が含まれている場合は、すべて上書きされます。

重要

管理用サーバに操作ログが取得されていない場合、［操作ログ］画面は表示されません。

重要

操作ログの保管先を設定していない場合、操作ログの自動取り込みを有効にすると、操作ログは、操作ログのデータベースに自動的に取り込まれますが、操作ログの保管先フォルダには保管されません。この運用の場合、操作ログのデータベースに障害が発生すると回復できないおそれがあるため、保管先を設定しておくことをお勧めします。

重要

操作ログは大容量のデータを格納するため、ディスク容量が不足するおそれがあります。ディスク容量が不足すると、次のような現象が発生する場合があるため、定期的にメンテナンスを実施してください。

- データベースの閉塞
- エージェントからのインベントリ、操作ログ等の受信失敗
- 変更履歴の更新が失敗
- 操作ログの登録、更新、検索が失敗
- DB バックアップ・リストア・DB 再編成が失敗

ヒント

操作ログの保管先フォルダは長期間にわたって大容量のデータを格納するおそれがあるため、RAID、NAS などのドライブを使用することをお勧めします。

重要

操作ログの保管先フォルダには操作ログのファイル以外のファイルを格納しないでください。

重要

共有型 VDI の仮想コンピュータでは、シャットダウンの操作ログはログオフ後に取得します。このため、次の場合には仮想コンピュータの初期化によって操作ログが削除され、取得できません。

- VMware Horizon View の流動方式、Citrix Virtual Desktops の MCS（Machine Creation Services）のランダム方式、または Citrix Virtual Desktops の PVS（Provisioning Services）方式の仮想コンピュータをシャットダウンした場合
- VMware Horizon View の専用方式、または Citrix Virtual Desktops の MCS（Machine Creation Services）の静的方式の仮想コンピュータをシャットダウンし、マスタを更新した場合

利用者のコンピュータ側での操作ログの保存

コンピュータが管理用サーバとの接続に失敗した場合などに備えて、利用者のコンピュータ側で一定期間、操作ログを保存できます。操作ログを保存する期間（保持期間）は、セキュリティポリシーで設定できます。管理用サーバに通知されなかった操作ログは、コンピュータ内に一時的に保存され、セキュリティポリシーに設定したタイミングで再度通知されます。

操作ログは大容量のデータになりやすいため、次の計算式を参考にして、必要なディスク容量を算出してから操作ログの保持期間を設定してください。

260 × 保持期間（日） ＝ 必要なディスク容量（キロバイト）

Citrix XenApp、Microsoft RDS 環境で操作ログ機能を使用する場合は、さらにログインユーザ数をかけた値になります。

注　操作ログの取得項目やユーザーの操作内容によって、必要なディスク容量は増減します。

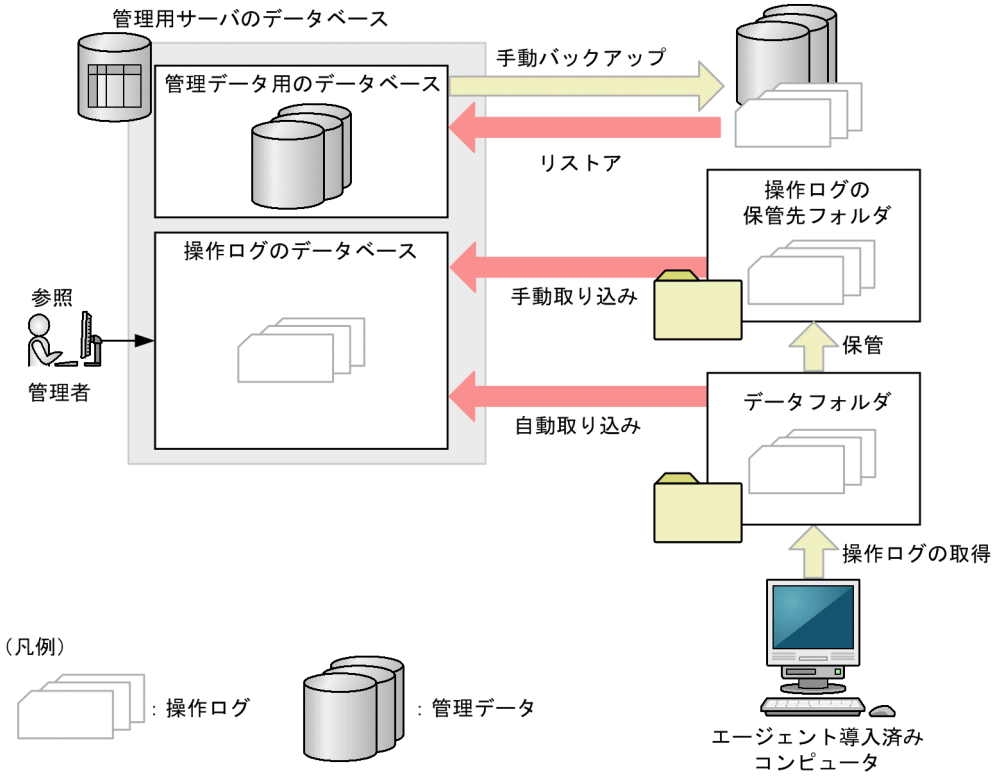
> **重要**
>
> 管理用サーバとの通信中に処理が中断した場合、次回通信時に再度同じデータが通知されるため、一部の操作ログが重複することがあります。

関連リンク

- 2.10.1　取得できる操作ログの種類
- 2.18.11　複数サーバ構成での操作ログの管理

(1)　管理用サーバでの操作ログの保管と取り込み

管理用サーバのセットアップで、操作ログを保管するように設定していると、利用者の操作の履歴情報を操作ログとして取得し、操作ログの保管先フォルダに保存できます。



エージェントを導入したコンピュータから、セキュリティポリシーで設定した間隔で操作ログが取得されます。取得された操作ログは、データフォルダに蓄えられ、操作ログの保管先フォルダに保管されます。また、操作ログのデータベースに自動で取り込むことができます。

操作ログのデータベースに取り込まれた操作ログは、セキュリティ画面の［操作ログ］画面から参照できます。過去の操作ログを参照したい場合は、保管した操作ログを操作ログのデータベースに取り込むことで、［操作ログ］画面から参照できるようになります。操作ログのデータベースは、参照不要な場合はデータをクリアできます。

なお、データベースマネージャを使用してデータベースをバックアップしたりリストアしたりしても、操作ログのデータベースはバックアップされたりリストアされたりしません。操作ログのデータは手動でバックアップおよびリストアする必要があります。

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

コンピュータから取得した操作ログの操作日時が、西暦 2000 年より前、または管理用サーバの現在時刻より 7 日より後の場合は、取得した操作ログは保存されません。

(2) 管理用サーバでの操作ログの保管

コンピュータから取得した操作ログは、データフォルダに蓄えられ、1 時間ごとに操作ログの保管先フォルダに保管されます。

保管されるデータ

操作ログのバックアップファイルは、日付単位でフォルダに分けられ、セットアップで設定した［操作ログの保管先フォルダ］に格納されます。日付フォルダの形式は「OPR_DATA2_*YYYYMMDD*」となります。

保管に必要な容量

次に示す条件で操作ログの保管に必要な容量の算出方法を説明します。

- 管理対象のコンピュータの台数：10,000 台
- 1 日の操作ログの発生件数：2,000 件/台
- 1 件当たりの操作ログのデータサイズ：500 バイト
- ZIP ファイルの圧縮率：6.7%

注　条件はすべて目安になります。

操作ログのデータサイズ

1 台当たりの操作ログのデータサイズ：2,000（件）×500（バイト）＝約 1（メガバイト）

10,000 台の操作ログのデータサイズ：1（メガバイト）×10,000（台）＝ 10（ギガバイト）

10,000 台の 1 か月（出勤日 20 日）当たりの操作ログのデータサイズ：10（ギガバイト）×20（日）＝約 200（ギガバイト）

バックアップファイルのデータサイズ

1 台当たりのバックアップファイルのデータサイズ：1（メガバイト）×6.7%＝約 67（キロバイト）

10,000 台のバックアップファイルのデータサイズ：67（キロバイト）×10,000（台）＝約 670（メガバイト）

10,000 台の 1 か月（出勤日 20 日）当たりのバックアップファイルのデータサイズ：670（メガバイト）×20（日）＝ 13.4（ギガバイト）

このようにして、操作ログとバックアップファイルのデータサイズが計算できます。管理しているコンピュータの数と操作ログの取得期間を考慮して、データベースおよび保管先フォルダ用のドライブの空き容量を確保してください。

空き容量が不足したときのメール通知

保管先の空き容量が不足した場合にメール通知されるように設定できます。メール通知される契機について、次に示します。

保管に失敗した場合

保管先のドライブの容量が不足していたことが原因で保管に失敗した場合、イベント画面に「緊急」のエラーイベントが表示されます。このとき、イベントのメール通知を設定しておくと、自動的に通知先にメールが通知されます。

定期監視で空き容量が不足していた場合

保管先フォルダのドライブの空き容量が不足していた場合、イベント画面にエラーイベントが表示されます。このとき、イベントのメール通知を設定しておくと、自動的に通知先にメールが通知されます。なお、空き容量不足のイベントを出力するしきい値は、コンフィグレーションファイルのプロパティで変更できます。コンフィグレーションファイルのプロパティについては、「付録 A.5　プロパティ一覧」を参照してください。

(3)　管理用サーバへの操作ログの取り込み

操作ログのデータベースに操作ログを取り込むと操作ログを参照できます。操作ログの取り込みには、「自動取り込み」と「手動取り込み」があります。

JP1/IT Desktop Management の操作ログを取り込むこともできます。

ヒント

旧製品（JP1/IT Desktop Management）の操作ログのバックアップファイルが、セットアップで設定した［操作ログの保管先フォルダ］に格納されている場合、［操作ログ一覧］画面上部のタイムチャートのツールチップに「未取り込み（旧製品の操作ログ）」の文字列が表示されます。この場合、件数は表示されません。

ヒント

操作ログのデータベースに取り込める最大日数は管理用サーバのセットアップで設定できます。上限は 500 日です。

自動取り込み

設定画面の［操作ログの設定］で指定された格納期間に合わせて、自動的に操作ログが取り込まれます。

管理対象のコンピュータ 1 台につき、1 日当たり平均で 2,000 件の操作ログが発生します。取り込む操作ログが大量になると、システムに負荷が掛かるおそれがあります。操作ログを取得する操作ログを絞ったり、管理対象のコンピュータの台数を減らしたりして、システムに負荷が掛からないように運用することをお勧めします。

システムに負荷を掛けないで運用する目安として、次の算出式を使用してください。

(a) 管理対象のコンピュータの台数（台） × 2,000（件） × 自動取り込みされる操作ログの格納期間（日） × x < 300,000,000

x：取得する操作ログの係数です。次に示す取得する項目の合計値を指定します。

- プログラム起動／停止：0.26
- ファイル操作、フォルダ操作：0.06
- Web アクセス：0.36
- ウィンドウ操作：0.3

(b) 管理対象のコンピュータの台数（台） × 1 日当たりの操作ログ件数※ < 60,000,000

注※　操作ログと秘文ログの総数です。秘文ログの件数は取得する秘文ログの種類や環境により異なるため、1 週間から 1 か月程度運用して算出してください。

コンピュータの起動と停止、ログオンとログオフ、ネットワーク経由のファイル操作、印刷操作などの操作は、取得する操作ログの量が少ないため、計算は不要です。

例えば、管理対象のコンピュータの台数が 10,000 台で、Web アクセスとウィンドウ操作の操作ログを取得する場合、操作ログの格納期間は次のようになります。

10,000（台） × 2,000（件） × 自動取り込みされる操作ログの格納期間（日） × 0.66 < 300,000,000

自動取り込みされる操作ログの格納期間（日）＝ 22.7（日）≒ 約 1 か月（20 営業日/月）

手動取り込み

調査したい操作ログが含まれる期間を指定して操作ログを取り込めます。また、対象のコンピュータを指定して取り込むこともできます。

手動取り込みでデータベースに取り込める操作ログの最大日数は、セットアップで設定する［操作ログのデータベース格納最大日数］から設定画面で設定する［自動取り込みされる操作ログの格納期間］を差し引いた値です。

ヒント

セキュリティ画面の［操作ログ］画面のタイムチャート上の日付をマウスオーバーしてツールチップに表示される未取り込み件数への反映に時間がかかることがあります。

重要

操作ログの保管先フォルダに保管されるバックアップファイルは、管理用サーバのタイムゾーンに合わせて保管されます。そのため、管理用サーバと Web ブラウザを実行しているコンピュータのタイムゾーンが異なる場合は、操作ログの手動取り込みで指定する日にちも管理用サーバのタイムゾーンに合わせる必要があります。

重要

セキュリティ画面の［操作ログ］画面のタイムチャート上の日付をマウスオーバーしてツールチップに表示されるデータは、管理用サーバが管理している操作ログの状態と件数です。そのため、管理用サーバと Web ブラウザを実行しているコンピュータのタイムゾーンが異なる場合は、ツールチップに表示される操作ログの件数と、日付でフィルタした操作ログの件数が異なることがあります。

重要

環境に依存しますが、200 台のコンピュータの操作ログを 3 か月分取り込む場合、2 時間以上かかることがあります。取り込み時間を短縮するには、取り込み範囲を短く設定してください。

重要

手動取り込みでデータベースに取り込める操作ログの最大日数以上の操作ログを、1 日の間に手動取り込みするには、格納最大日数を「自動取り込み日数」＋「1 日の間に手動取り込みする日数」に設定する必要があります。

（例）半年分（180 日）の操作ログを 1 日の間に手動取り込みする場合、自動取り込み日数を 30 日とすると、格納最大日数は 210 日を設定します。

操作ログのデータベース

操作ログのデータベースは、取り込まれた操作ログの件数分のサイズが拡張されます。管理画面から操作ログを削除した場合でも操作ログのデータベースのサイズは縮小されません。操作ログが削除された場合は、1 日 1 回の操作ログのデータベースのメンテナンス時にデータベース内の空き領域になります。空き領域は操作ログを取り込む際に再利用されます。

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はコンフィグレーションファイルのプロパティで変更できます。コンフィグレーションファイルのプロパティについては、「付録 A.5　プロパティ一覧」を参照してください。

(4)　操作ログの定期エクスポート

操作ログを CSV 形式で保存したい場合や、他のシステムにインポートしたい場合に、取得した操作ログを CSV ファイルでエクスポートできます。設定画面の[操作ログの設定]画面で［操作ログを定期的にエクスポートする］にチェックすると、操作ログの保管先フォルダの export フォルダに 1 時間ごとエクスポートできます。CSV ファイルの出力情報を次に示します。

CSV ファイルの出力先

操作ログの保管先フォルダ¥export

出力ファイル名

oplog_*YYYYMMDD*_*NNN*.csv

YYYYMMDD：定期エクスポートを処理した日時を示します。

NNN：001～999 の連番の数を示します。999 を超える場合はイベントを出力します。

操作ログの受信順に出力されます。

ファイルサイズ

1 ファイルは 2 ギガバイト以内です。2 ギガバイトを超えると、分割されます。

文字コード

UTF-8

出力形式

出力形式については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のエクスポートした操作ログの出力形式の説明を参照してください。

重要

操作ログの定期エクスポートを有効にすると、出力される CSV ファイルは圧縮されないために、多くのディスク容量を必要とします。必要に応じて、圧縮や他のディスクにバックアップしてください。操作ログの定期エクスポートした場合に必要なディスク容量の目安については、「4.5.3　操作ログの保管先フォルダに必要なディスク容量の目安」を参照してください。

(5)　操作ログのデータベースの追加キャッシュ

操作ログの検索性能を向上させるために、管理用サーバのセットアップでキャッシュを設定できます。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。

(6)　操作ログのデータベースのインデックスの再作成

操作ログの検索性能を維持するために、操作ログのデータベースに対し、次のメンテナンスを 1 日に 1 回（01:00 から 02:00 の間）実施します。

- 自動取り込みした操作ログのインデックスの再作成
- 自動取り込みした操作ログのうち格納期間を超えたデータの削除および領域の解放
- 手動取り込み済みの操作ログを削除したデータの領域の解放

重要

管理用サーバを夜間にシャットダウンする運用の場合、操作ログのデータベースのメンテナンスが 1 日 1 回実施されるように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を変更してください。

操作ログのデータベースのインデックスの再作成中は操作ログの検索が遅くなることがあります。また、操作ログのエクスポートコマンド（ioutils exportoplog）はインデクスの再作成後に実行してください。

ヒント

部署、設置場所、発生元、ユーザー名などで検索対象の機器を絞り込むと、操作ログの検索時間を短縮できます。

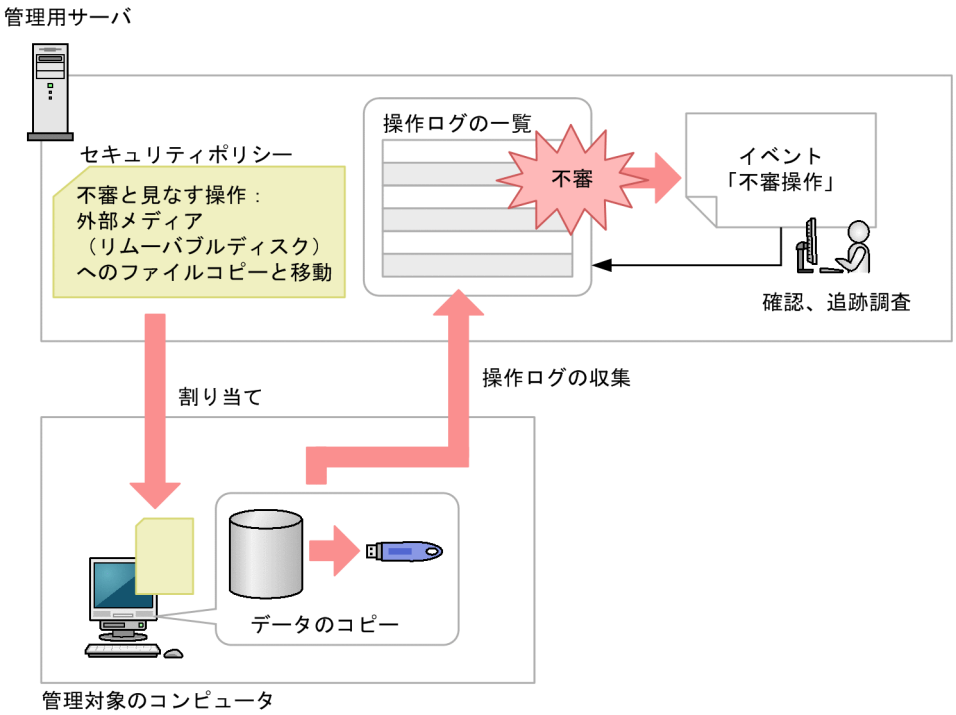
関連リンク

- 付録 A.8　各種機能が自動実行されるタイミング

2.10.3　ファイル持ち出しによる不審操作の、操作ログでの調査

コンピュータの利用者の操作を操作ログとして取得できます。また、セキュリティポリシーに不審と見なす操作の条件を設定することで、情報漏えいにつながる不審な操作が自動的に検知されるようになります。情報漏えいのおそれのある操作が発生するとすぐにチェックできるので、被害が大きくなる前に対処できます。

操作ログを収集して不審操作を調査する流れを次の図に示します。



不審操作を検知するためには、セキュリティポリシーに不審と見なす操作の条件を設定する必要があります。この条件を設定したセキュリティポリシーが適用されているコンピュータに対して、不審操作を検知できます。

ファイルの持ち出しが検知された場合、機密情報が漏えいするのを防ぐために該当するファイルの出所を調査する必要があります。不審操作が検知されると、「不審操作」のイベントとして通知されます。このイベントから、検知された操作ログを確認し、持ち出されたファイルの出所を追跡調査できます。

> **ヒント**
>
> 操作ログは、`ioutils exportoplog` コマンドを実行してエクスポートすることもできます。操作ログの内容を資料に使用したい場合などは、エクスポートすることをお勧めします。

関連リンク

- 2.10.1　取得できる操作ログの種類

(1) ファイル持ち出しによる不審操作の取得

JP1/IT Desktop Management 2 では、操作ログの内容を自動的にチェックして、ファイル持ち出しによる情報漏えいのおそれがある操作を不審な操作と見なして監視できます。

セキュリティポリシーで、不審と見なす操作を指定して、不審と見なす場合の条件を設定してください。

不審と見なす操作

- 監視対象のファイルを、ポリシーに設定したメールアドレス※1、※2 に添付で送信
- 監視対象のファイルを、ポリシーに設定した Web サーバ※1、※2、※3 または FTP サーバ※1、※2、※3 にアップロード
- 監視対象のファイルを外部メディアにコピーまたは移動

監視対象になるファイルは次の条件を満たすものです。

- ポリシーに設定したメールアドレス※1、※4 から添付で受信したファイル
- ポリシーに設定した Web サーバ※1、※3、※4 または FTP サーバ※1、※3、※4 からダウンロードしたファイル
- 組織内で新たに作成したファイル
- 操作ログを取得する前から組織内にあるファイル

注※1　設定したアドレスに部分一致または全文一致したアドレスを対象とします。

注※2　どの設定にも一致しないアドレスへのファイル持ち出しは不審な操作と見なします。

注※3　IP アドレスで設定した場合は、ダウンロード元のアドレスに含まれるホスト名を IP アドレスに変換した値と、設定した IP アドレスが部分一致したアドレスを対象とします。

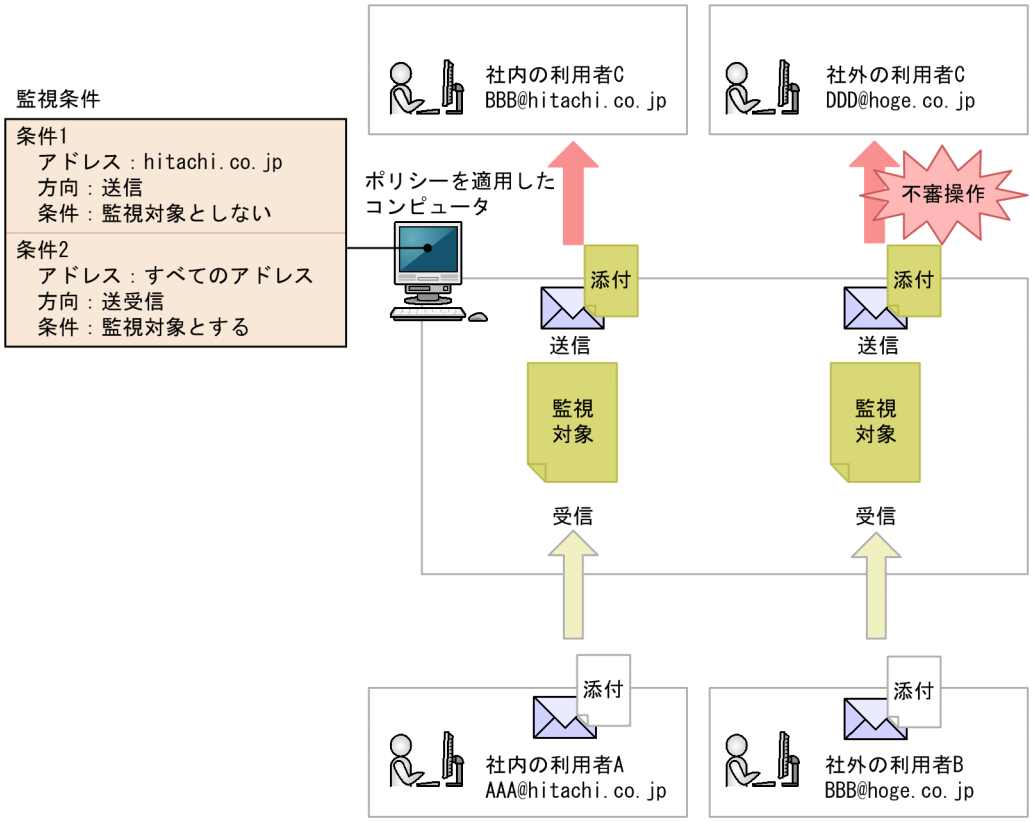
注※4　どの設定にも一致しないアドレスから持ち込んだファイルは監視対象のファイルと見なします。

監視対象のファイルを入手した時点では、不審な操作としては見なされません。監視対象のファイルを持ち出した場合に、不審な操作と見なされイベントが発生します。

添付ファイル付きメールの監視例

例えば、次に示す内容で監視したい場合、図のように設定してください。

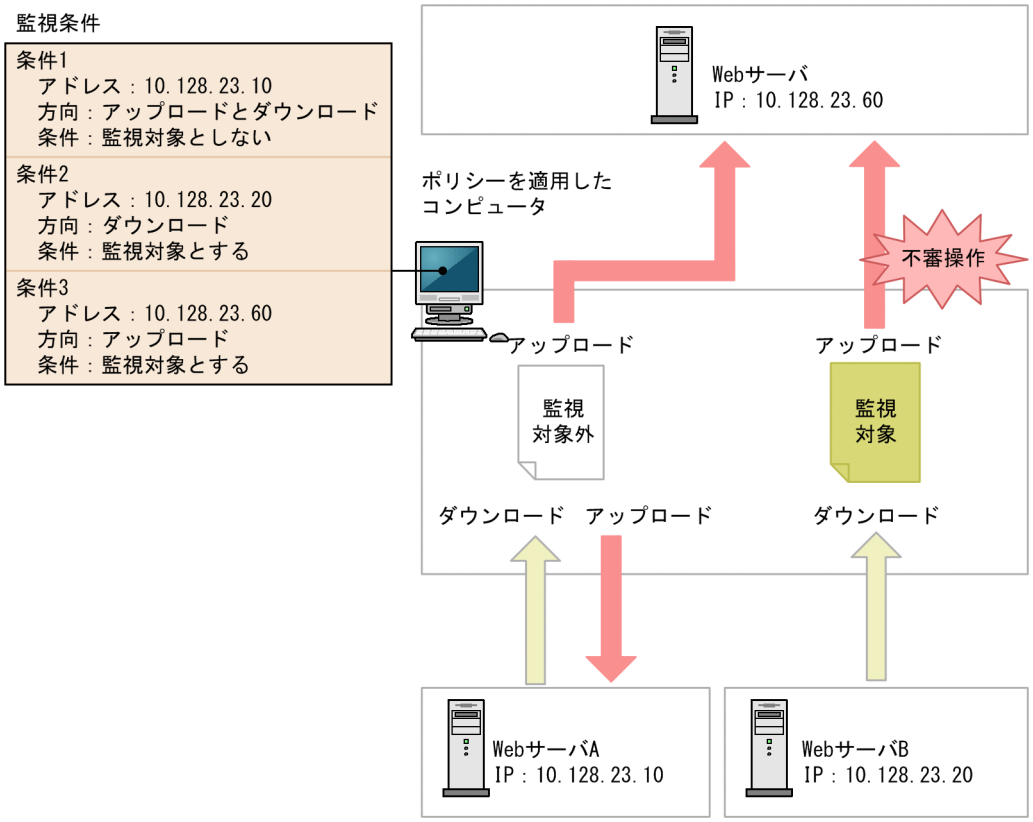
- 社外への添付ファイルの転送は監視する。
- 社内（アドレスが「hitachi.co.jp」）での、添付ファイルの転送は監視しない。



Web サーバ/FTP サーバの監視例

例えば、次に示す内容で監視したい場合、図のように設定してください。

- Web サーバ A のデータは公開できるデータのため、外部へのアップロードは監視しない。
- Web サーバ B のデータは重要データのため、外部へのアップロードを監視する。



不審操作を監視できるサポート製品は、操作ログを取得できるサポート製品と同じです。詳細については、「2.10.1　取得できる操作ログの種類」の注※2、3、および４に記載されているサポート製品を参照してください。

重要

対象のコンピュータのファイルシステムがNTFSの場合だけ、不審操作として正しく検知できます。NTFSでない場合は、持ち込み元情報が設定されず、不審操作として正しく検知できないときがあります。

2.10.4　持ち込みチェックと持ち出しチェックの条件

エージェントを導入しているコンピュータに持ち込まれたファイルを検知した場合、そのファイルを不審操作検知の監視対象とするかどうか持ち込みチェックをします。また、ファイルが持ち出された（コピー、送信など）と検知した場合、そのファイルを不審操作検知の監視対象とするかどうか持ち出しチェックをします。持ち込みチェック、持ち出しチェックの条件をそれぞれ次の表に示します。

持ち込みチェック条件

操作ログ取得項目	持ち込みチェック
ファイルコピー	△※1

操作ログ取得項目	持ち込みチェック
ファイル移動	△※1
ファイル名称変更	△※1
ファイル作成	○
ファイル削除	△※1
ファイルアップロード	△※1※2
ファイルダウンロード	△※3
ファイル送信	△※1
ファイル受信	△※3
メール送信（添付ファイル付き）	△※1
メール受信（添付ファイル付き）	△※3
添付ファイル保存	△※1
印刷	×

（凡例）○：持ち込みと見なす　△：条件によっては持ち込みと見なす　×：持ち込みと見なさない

注※1　ローカルドライブ、リモートドライブ、RAM ドライブ、またドライブ情報が取得できない場合、持ち込みと見なします。また、リムーバブルドライブ、CD-ROM ドライブの場合、持ち込みと見なしません。

注※2　Internet Explorer 10、11 からアップロードされたファイルは持ち込みと見なしません。

注※3　監視対象に合致する、またはすべての条件に合致しない場合、持ち込みと見なします。

持ち出しチェック条件

操作ログ取得項目	持ち出しチェック
ファイルコピー	△※1
ファイル移動	△※1
ファイル名称変更	×
ファイル作成	△※2
ファイル削除	×
ファイルアップロード	△※3、※4、※5
ファイルダウンロード	△※6

操作ログ取得項目	持ち出しチェック
ファイル送信	△※3
ファイル受信	△※6
メール送信（添付ファイル付き）	△※3
メール受信（添付ファイル付き）	×
添付ファイル保存	△※6
印刷	×

（凡例）△：条件によっては持ち出しと見なす　×：持ち出しと見なさない

注※1　条件については、以降の「ファイルコピー、移動の持ち出しチェック条件」の表を参照してください。

注※2　条件については、以降の「ファイル作成操作の持ち出しチェック条件」の表を参照してください。

注※3　監視対象のアドレスに合致する、またはすべての条件に合致しない場合、持ち出しと見なします。

注※4　Internet Explorer 10、11 の場合は、すべてのファイルを持ち出しと見なします。

注※5　Internet Explorer 10、11 の場合は、ファイルのアップロードを開始した時点で持ち出しチェックを実行します。そのため、通信エラーなどでアップロードが中断されても、不審操作として検知できます。条件については、以降の「受信操作の持ち出しチェック条件」の表を参照してください。

注※6　条件については、以降の「受信操作の持ち出しチェック条件」の表を参照してください。

ファイルコピー、移動の持ち出しチェック条件

操作元	操作先					
	ローカルドライブ	リモートドライブ	リムーバブルドライブ	CD-ROM ドライブ	RAM ドライブ	ドライブ情報取得不可
ローカルドライブ	×	×	△※	△※	×	△※
リモートドライブ	×	×	△※	△※	×	△※
リムーバブルドライブ	×	×	×	×	×	×
CD-ROM ドライブ	×	×	×	×	×	×
RAM ドライブ	×	×	△※	△※	×	△※

操作元	操作先					
	ローカルドライブ	リモートドライブ	リムーバブルドライブ	CD-ROM ドライブ	RAM ドライブ	ドライブ情報取得不可
ドライブ情報取得不可	×	×	△※	△※	×	△※

（凡例）△：条件によっては持ち出しと見なす　×：持ち出しと見なさない

注　Citrix XenApp、Microsoft RDS サーバの場合、接続元の機器に存在するドライブは接続先のセッションでドライブ種別が「その他」のドライブとして表示されます。そのようなドライブへのファイルのコピー、移動は持ち出しと判定されません。

注※　セキュリティポリシーで、[外部メディア（リムーバブルディスク）へのファイルコピーと移動]がチェックされている場合に持ち出しと判定します。

受信操作の持ち出しチェック条件

操作元	操作先					
	ローカルドライブ	リモートドライブ	リムーバブルドライブ	CD-ROM ドライブ	RAM ドライブ	ドライブ情報取得不可
任意の操作元	×	×	△※	△※	×	△※

（凡例）△：条件によっては持ち出しと見なす　×：持ち出しと見なさない

注※　セキュリティポリシーで、[外部メディア（リムーバブルディスク）へのファイルコピーと移動]がチェックされている場合に持ち出しと判定します。

ファイル作成操作の持ち出しチェック条件

操作元	操作先					
	ローカルドライブ	リモートドライブ	リムーバブルドライブ	CD-ROM ドライブ	RAM ドライブ	ドライブ情報取得不可
作成元なし	×	×	△※	△※	×	△※

（凡例）△：条件によっては持ち出しと見なす　×：持ち出しと見なさない

注※　セキュリティポリシーで、[外部メディア（リムーバブルディスク）へのファイルコピーと移動]がチェックされている場合に持ち出しと判定します。

関連リンク

- 2.10.1　取得できる操作ログの種類

2.10.5　印刷による不審操作の取得

コンピュータの利用者の大量印刷を、不審操作として取得できます。印刷による不審操作を取得するためには、セキュリティポリシーに不審と見なす操作の条件を設定する必要があります。この条件を設定した

セキュリティポリシーが適用されているコンピュータに対して、印刷による不審操作が検知されます。大量印刷のチェック条件については、「2.10.6　大量印刷のチェック条件」を参照してください。

印刷による不審操作が検知された場合、機密情報が漏えいするのを防ぐために、該当するユーザー名、印刷回数、印刷した時間などを調査する必要があります。不審操作が検知されると、「不審操作」のイベントとして通知されます。このイベントを基に、収集された操作ログで、該当する大量印刷が情報漏えいやコスト面での問題がないかどうかを確認してください。

2.10.6　大量印刷のチェック条件

JP1/IT Desktop Management 2 では、印刷による情報漏えいのおそれがある操作を不審な操作と見なして検知できます。セキュリティポリシーで不審と見なす操作を指定して、不審と見なす場合の条件を設定してください。

不審と見なす操作

- 設定したページ数を超える印刷

不審操作として検知されるのは、印刷操作がされた時刻からさかのぼって 1 時間以内に、同一のユーザーが同一のコンピュータで印刷したページ数の合計が、セキュリティポリシーに設定したページ数以上である場合の印刷操作です。不審操作として検知される印刷ページ数は、1 度だけカウントされます。これは、同一ユーザーで過去 1 時間以内に印刷による不審操作が検知されていた場合、不審と検知された印刷操作を含まないで、次の印刷操作から印刷ページ数をカウントするためです。

イベントとして通知される印刷ページ数は、印刷による不審操作の検知に関係なく、過去 1 時間以内の印刷ページ数が合計されて表示されます。

利用者のコンピュータがシャットダウンされた場合、シャットダウン以前の印刷操作は、不審操作とイベントの印刷ページ数の合計には含まれません。

2.10.7　操作ログ取得の前提条件と注意事項

(1)　操作ログ取得の注意事項

- OS が 64bit 版で、かつ VMWare Server がインストールされている環境のコンピュータに対しては、操作ログを有効にしないでください。操作ログを有効にすると、VMWare Server のゲスト OS が起動しない場合があります。
- エージェントを導入したコンピュータから管理用サーバへ操作ログを送信してから、コンピュータ上の操作ログを削除するまでの間に処理が強制終了された場合、操作ログを重複して取得することがあります。

- エージェントを導入したコンピュータの操作ログのサービスである「JP1_ITDM_Agent Monitor Control」は毎日午前 2 時に再起動しますが、既定の動作によるものであり、エラーが原因ではありません。

(2) 機器の起動/停止で取得される操作ログの注意事項

- エージェントを上書きインストールした場合も、「コンピュータの起動と停止」の操作ログが取得されます。
- OS が Windows Server 2019、Windows Server 2016、Windows 10、Windows Server 2012 R2、Winodws 8.1、Windows Server 2012、および Winodws 8 の場合、高速スタートアップ機能を有効にしていると、コンピュータの起動や停止時に「コンピュータ起動」や「コンピュータ停止」の操作ログが取得できないおそれがあります。
- ユーザがログオンしている状態の PC をシャットダウンまたは再起動をするとき、エージェントが「ログオフ」の操作ログを出力する前に電源がオフになると、「ログオフ」の操作ログが取得されません。確実に「ログオフ」の操作ログを取得するには、ログオフを実施してから、シャットダウンまたは再起動の操作をしてください。

関連リンク

- 2.10.1 取得できる操作ログの種類

(3) プログラムの起動/停止、および抑止で取得される操作ログの注意事項

- ファイル名とフォルダ名を合わせて文字列の長さが 260 文字以上のプログラムは、プログラムの起動/停止、および抑止の操作ログを取得できません。
- 起動後すぐに終了するソフトウェアは、エージェントが起動を抑止する前にプログラムが終了してしまう場合があるため、プログラムの起動/停止、および抑止の操作ログが取得できないことがあります。
- 起動を抑止できるプログラムは、ファイル名に次に示す拡張子を持つプログラムだけです。
  - exe
  - com
  - scr
- *JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*※¥bin フォルダで起動されたプログラムのうち、[スタート] メニューから起動できないプログラムは、プログラム起動/停止の操作ログを取得できません。
- *JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*※¥bin フォルダにあるプログラムから次に示すプログラムが起動された場合、プログラム起動/停止の操作ログを取得できません。
  - cacls.exe
  - cmd.exe
  - conime.exe

- cscript.exe
- jdngsendinv.exe
- jdngsetup.exe
- netsh.exe
- regsvr32.exe
- secedit.exe

注※　複数サーバ構成の管理用中継サーバの場合は、*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*です。

関連リンク

- 2.10.1　取得できる操作ログの種類

(4)　Web アクセスの操作ログ取得の前提条件と注意事項

Web アクセスの操作ログ取得の前提条件と注意事項をそれぞれ説明します。

前提条件

- Internet Explorer の場合、［インターネットオプション］の［詳細設定］タブの［サードパーティ製のブラウザ拡張を有効にする］がチェックされている必要があります。なお、Windows Server 2019、Windows Server 2016、Windows Server 2012 および Windows Server 2008 R2 にインストールされた Internet Explorer では、デフォルトで［サードパーティ製のブラウザ拡張を有効にする］がチェックされていません。
- 利用者のコンピュータに追加される Web アクセス監視用のアドオンが有効になっている必要があります。
- Internet Explorer の場合、［ツール］－［アドオンの管理］を選択すると表示される［ツールバーと拡張機能］で、「JP1/IT Desktop Management 2 BHO」と表示されるアドオンが有効になっている必要があります。

ヒント

エージェントが導入されたコンピュータの Internet Explorer には、下記のアドオンが追加されます。

・Web アクセス監視用のアドオン

・ファイルアップロード監視用のアドオン（バージョン 10 以降の Internet Explorer の場合）

Web アクセスは、Web アクセス監視用のアドオンによって監視・検知されます。HTML フォームや Javascript によるファイルのアップロードは、Internet Explorer がバージョン 9 以前の

場合はエージェントによって監視・検知され、バージョン 10 以降の場合はファイルアップロード監視用のアドオンによって監視・検知されます。

なお、ファイルのダウンロードおよび送受信は、エージェントによって監視・検知されます。

注意事項

- アドオン全般を無効にして Web ブラウザを起動する場合、Web アクセスの操作ログは取得できません。
- ファイルやフォルダを Internet Explorer で開いた場合、Web アクセスの操作ログを取得できます。
- Web ページ上の画像の情報は取得できません。
- 1 秒以内に複数回の Web アクセスが実行された場合、Web アクセスの操作ログが取得できないことがあります。
- Internet Explorer を 15 個以上同時に起動した場合、Web アクセスの操作ログが取得できないことがあります。
- Windows へのログオン直後に Internet Explorer を起動した場合、Web アクセスの操作ログが取得できないことがあります。
- Internet Explorer 10、11 の環境で拡張保護モードが有効な場合、Web アクセスの操作ログを取得できません。
- Web アクセスで、通信エラーやアクセスした URL が存在しないなどの要因で接続エラーとなった場合でも、Web アクセスの操作ログが取得できることがあります。

ヒント

Web アクセス監視用のアドオンが登録された際に登録されたアドオンを有効にするかどうかの確認メッセージが表示されます。メッセージが表示される現象を回避する場合、次の手順を実施して Internet Explorer を再起動してください。

1. 管理者権限を持つユーザでログオンし、[ファイル名を指定して実行] に「gpedit.msc」と入力して実行し、グループポリシーエディタを起動します。
2. 次の「アドオンの一覧」の設定を開きます。
   [ローカルグループポリシーエディター] − [コンピュータの構成] − [管理用テンプレート] − [Windows コンポーネント] − [Internet Explorer] − [セキュリティの機能] − [アドオン管理] − [アドオンの一覧]
3. アドオンの一覧ダイアログで [有効] を選択し、[オプション] の [アドオン一覧] の [表示] ボタンを押します。
4. 次の設定を追加します。
   値の名前:{90CA397B-DA51-47EB-9299-0B7041857FCB}
   値:1

アドオンが無効に設定された場合は、次の手順を実施してください。

1. メッセージが表示される現象を回避する手順を実施します。
2. Internet Explorer の［ツール］－［インターネットオプション］－［プログラム］－［アドオンの管理］から「JP1/IT Desktop Management 2 BHO」の設定を［有効］に変更します。

関連リンク

- 2.10.1　取得できる操作ログの種類

(5)　ファイル、フォルダ操作で取得される操作ログの情報と注意事項

利用者がフォルダをコピー、移動、または削除した場合、そのフォルダのすべてのファイルおよびサブフォルダについても操作の情報を取得できます。なお、フォルダの名前を変更した場合は、その操作の情報は取得できません。

操作ログの取得は、エクスプローラに対する操作を対象とします。そのため、コマンドプロンプト上での COPY コマンドなどの操作は取得できません。

ファイル、フォルダ操作で取得される操作ログの情報と注意事項をそれぞれ説明します。

利用者が、フォルダまたはファイルの操作後に Undo（[元に戻す］メニューまたは［Ctrl］＋［Z］キー）の操作を行った場合、次の表に示す操作ログが取得されます。

Undo 前の操作	Undo 操作時に取得される操作ログ
コピー	コピーしたファイルまたはフォルダの削除
移動	移動したファイルまたはフォルダの元の位置への移動
名前の変更	元のファイル名またはフォルダ名への名前の変更
削除	削除したファイルまたはフォルダの、元の位置への移動

ファイル操作では、Windows の［最近使った項目］フォルダでの操作など、利用者操作に直接関係のないファイル作成、削除の操作ログが出力される場合があります。そのため、次の条件をすべて満たす操作ログは取得されません。

- 操作内容が、ファイル作成、ファイル削除である。
- ファイルのパスが次のどちらかのフォルダである。
  - %USERPROFILE%¥Recent
  - %APPDATA%¥Microsoft¥Office¥Recent
- ファイルの拡張子が「.lnk」である。

また、エージェントおよび管理用中継サーバ用のエージェントの導入フォルダの下位について、次の条件をすべて満たす操作ログは取得されません。

- 操作内容がファイル作成、ファイル削除、ファイル名変更、フォルダ作成、フォルダ削除、フォルダ名変更である。
- ファイルパスが次のどちらかのフォルダ（サブフォルダ含む）である。
  - エージェントの場合：*JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*
- 管理用中継サーバ用のエージェントの場合：*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*¥bin

注意事項

- 利用者が同じファイルまたはフォルダを繰り返しコピーした場合、ファイルまたはフォルダを作成したという情報が取得されることがあります。
- 利用者が Windows の［ごみ箱］へファイルまたはフォルダを移動した場合、移動ではなく、削除として情報が取得されます。
- 利用者が Windows の［ごみ箱］からファイルまたはフォルダを削除した場合、取得されるファイル名またはフォルダ名が、削除前の名称と異なることがあります。
- 利用者が大量のファイルを一括して削除した場合、すべてのファイルの削除の履歴が取得されないことがあります。
- 利用者が大量のファイルまたはフォルダを上書きコピーまたは移動した場合、すべてのファイル操作の情報が取得されないことがあります。
- 利用者がファイル移動時に移動先のファイルを上書きした場合、またはファイル移動の Undo（［元に戻す］メニューまたは［Ctrl］＋［Z］キー）操作をした場合に、ファイル移動の情報に加えて、移動元のファイルを削除した情報が余分に取得されることがあります。
- 圧縮形式（zip 形式）のフォルダに対する操作の情報は取得できません。ただし、OS やユーザー操作によっては、一部の操作の情報が取得される場合があります。
- USB デバイスを抑止している場合、USB 接続デバイス内のファイル操作の情報が取得されないことがあります。
- Windows ポータブルデバイスに対する操作の情報は取得できません。ただし、OS やデバイスによっては、一部の操作の情報が取得される場合があります。
- 特定のファイルを高速で連続コピー（［Ctrl］＋［V］キーを連続で操作するなど）した場合、本来コピー元と同じ値となるコピー先のファイルの更新日時が、コピー操作を実行した日時となる場合があります。
- 共有フォルダ上でファイル作成、ファイル削除、およびファイル名称変更の操作を実施したとき、エージェントが導入されている別のコンピュータが同じ共有フォルダを開いていると、そのコンピュータ上でもファイル操作の操作ログが取得されることがあります。

- 共有フォルダ上でファイル移動の操作を実施したとき、エージェントが導入されている別のコンピュータが同じ共有フォルダを開いていると、そのコンピュータ上で移動元のファイルに対するファイル削除の操作ログが取得されることがあります。

OS が 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、これらの注意事項のほかに、次の注意事項があります。

注意事項（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）

- 全操作
  - アプリケーションやコマンドプロンプトからファイルまたはフォルダが操作された場合でも、一部の操作について操作ログが取得されることがあります。
  - ファイルのシャドウコピーおよびバックアップからの復元に対しての操作の情報は取得できません。なお、一部の操作の情報が取得される場合があります。
- コピー
  - コピーによってファイルが上書きされる場合、[ファイルの上書き確認] ダイアログで［コピーするが両方のファイルを保持する］を選択したときは次の情報が取得されます。

    ・コピー後のファイル名が「コピー前のファイル名（n)」(n は任意の数字）となる情報が取得されます。

    ・コピー操作後に、コピー元のファイルを削除すると、ファイルの移動の情報が追加で取得されることがあります。

    ・コピー元のファイルの更新日時と、上書きされるファイルの更新日時が同じ場合は、コピー前とコピー後のファイル名が同じとなるコピーの情報が取得されます。
  - 1 回のコピーの操作で、[フォルダの上書き確認] ダイアログが複数回表示される場合、フォルダおよびファイルのコピーの履歴が余分に取得されることがあります。
  - 名前に「()」が含まれるファイルまたはフォルダを利用者がコピーした場合、正しく情報が取得されないことがあります。
  - 名前に「(n)」(n は任意の数字）が含まれるファイルまたはフォルダを複数選択して利用者が上書きコピーした場合、[ファイルの上書き確認] ダイアログで［コピーするが両方のファイルを保持する］を選択すると、正しく情報が取得されないことがあります。
  - 利用者が Undo 操作後に［コピーのやり直し］メニューまたは［Ctrl］＋［Y］キーで Redo 操作を行った場合、ファイル操作の情報は取得できません。なお、フォルダに対する Redo 操作は、フォルダのコピーとして情報を取得できます。
  - 名前に「(n)」(n は任意の数字）が含まれるファイルまたはフォルダを連続して利用者がコピーした場合、2 回目以降のコピー操作はファイルまたはフォルダの作成として情報を取得されます。
  - 利用者が複数のファイルまたはフォルダ、または複数のファイルやフォルダが含まれるフォルダを選択してコピーした場合、操作の情報が取得されないことがあります。

- コピー操作時に、上書きを確認するダイアログでコピーをキャンセルした場合、コピー元のファイルの更新日付とコピー先フォルダにある同名のファイルの更新日付が同じときは、コピーとして情報が取得されます。

- 移動
  - 利用者の移動操作によってファイルが上書きされる場合、[ファイルの移動] ダイアログで [移動するが両方のファイルを保持する] を利用者が選択したときは、移動後のファイル名が「移動前のファイル名（n)」(n は任意の数字）となる情報が取得されます。また、移動前と移動後のファイル名が同じとなる移動の情報も余分に取得されます。
  - 名前に「(n)」(n は任意の数字）が含まれるファイルまたはフォルダを複数選択して利用者が移動した場合、[ファイルの上書き確認] ダイアログで「移動するが両方のファイルを保持する」を選択すると、正しく情報が取得されないことがあります。
  - 利用者の移動操作によってフォルダが上書きされる場合、[フォルダの上書きの確認] ダイアログで [はい] ボタンをクリックしてフォルダを統合するときは、次の情報が取得されます。

    ・移動元と移動先のフォルダに同名のファイルがある場合、フォルダの統合時にはファイルだけが移動し、移動元のフォルダは削除されません。このとき、フォルダのコピーの操作の情報が取得されます。

    ・利用者がファイルの上書き確認時に [移動して置換] を選択した場合、移動元のファイルの更新日時と上書きされるファイルの更新日時が同じときは、ファイルの移動ではなく、ファイルのコピーおよび削除の操作の情報が取得されます。

    ・利用者がファイルの上書き確認時に [移動するが両方のファイルを保持する] を選択した場合、移動後のファイル名が「移動前のファイル名（n)」(n は任意の数字）となる操作の情報が取得されます。移動前のファイルと上書きされるファイルの更新日時が同じ場合は、ファイルの移動に加えて、ファイルのコピーおよび削除の操作の情報も余分に取得されます。また、移動前のファイルと上書きされるファイルの更新日時が異なる場合は、移動前と移動後のファイル名が同じとなる移動の操作の情報が余分に取得されます。

    ・Windows 7 以降で、権限昇格が必要なフォルダから NTFS 以外のドライブにファイルの移動操作をした場合、持ち込み元ドライブ種別が取得できないで、正しくファイル追跡がされないことがあります。

- 名前の変更
  - 利用者が名前の変更を行ってフォルダを上書きする場合、[フォルダの上書きの確認] ダイアログが表示されます。このダイアログで利用者が [はい] ボタンをクリックした場合は、次の情報が取得されます。

    ・名前の変更前のフォルダに幾つかのファイルが含まれる場合、上書きしたフォルダへのファイル作成と、名前の変更前のファイルの削除の操作ログが取得されます。なお、名前の変更前のフォルダの削除の操作ログは取得されません。名前の変更前のフォルダにファイルが含まれない場合、名前の変更後のフォルダのサブフォルダの作成の操作ログだけが取得されます。

    ・名前の変更前のフォルダと上書きしたフォルダに、同名のサブフォルダが存在する場合、サブフォルダの作成の操作の情報が取得されます。このとき、名前の変更前のフォルダの削除の操作は取得されません。

・名前の変更前のフォルダに複数のファイルまたはサブフォルダが含まれる場合、一部のファイルの操作は取得されないことがあります。

・名前の変更前のフォルダのサブフォルダ内に存在するファイルの操作の情報が取得されない場合があります。

- 複数のファイルまたはフォルダ、または複数のファイルやフォルダが含まれるフォルダを選択して、一括して名前を変更した場合、操作の情報が取得されないことがあります。

- 削除
  - 利用者がファイルを削除したあとに Undo または［元に戻す］メニューを選択した場合、削除したファイルを元の位置に作成する操作の情報と、Windows の［ごみ箱］からファイルを削除する操作の情報が取得されます。ただし、Windows の［ごみ箱］からファイルを削除する操作の情報では、ファイル名が正しく取得されません。
  - 利用者がファイルを削除したあとに Windows の［ごみ箱］からファイルを移動したときは、削除したファイルの元の位置への移動の操作が取得されます。
  - 利用者が、複数のファイルまたはフォルダ、または複数のファイルやフォルダが含まれるフォルダを選択して削除したあと、［元に戻す］メニューを選択、または Windows の［ごみ箱］からフォルダを移動した場合は、操作の情報が取得されないことがあります。

関連リンク

- 2.10.1　取得できる操作ログの種類

(6)　ファイルのアップロードとダウンロードの操作ログ取得の前提条件と注意事項

Web ブラウザでファイルをアップロードまたはダウンロードした操作を監視し、その操作ログを取得できます。ファイルのアップロードまたはダウンロードの操作ログを取得する場合の前提条件と注意事項について説明します。

前提条件

- Web ブラウザに Internet Explorer 10、11 を使用している場合、［インターネットオプション］の［詳細設定］タブの［サードパーティ製のブラウザ拡張を有効にする］がチェックされている必要があります。なお、Windows Server 2019、Windows Server 2016、Windows Server 2012 および Windows Server 2008 R2 にインストールされた Internet Explorer では、デフォルトで［サードパーティ製のブラウザ拡張を有効にする］がチェックされていません。
- Web ブラウザに Internet Explorer 10、11 を使用している場合、利用者のコンピュータに追加されるファイルのアップロード監視用のアドオンが有効になっている必要があります。

  ファイルのアップロード監視用のアドオンを登録すると、アドオンを有効にするかどうかを選択させるメッセージが表示されます。アドオンを有効にし、Internet Explorer を再起動すると、ファイルのアップロードの監視が開始されます。

- Web ブラウザに Internet Explorer 10、11 を使用している場合、［ツール］－［アドオンの管理］を選択すると表示される［ツールバーと拡張機能］で、「JP1/IT Desktop Management 2 FUO」と表示されるアドオンが有効になっている必要があります。

注意事項

- SOAP、WebDAV、Flash、Silverlight など独自のアップロード処理によって実行される Web アップロードは操作ログが取得されません。
- Internet Explorer のインターネット一時ファイルのフォルダを変更した場合、Web ダウンロードの操作をしていなくても、操作ログが取得される場合があります。操作ログを正しく取得したい場合は、すぐに Internet Explorer を再起動してください。
- Internet Explorer 10、11 の環境で拡張保護モードが有効な場合、ファイルのアップロードおよびダウンロードの操作ログを取得できません。
- Internet Explorer 9 の場合、ファイルのアップロードが完了した時点で操作ログを取得します。Internet Explorer 10、11 の場合、ファイルのアップロードを開始した時点で操作ログを取得します。そのため、Internet Explorer 10、11 では通信エラーなどでアップロード処理が中断されても操作ログが取得できます。
- Internet Explorer 10、11 で HTML5 のアップロードサイトに複数ファイルを同時アップロードした場合、1 つのファイルの操作ログしか取得できません。
- Internet Explorer 10、11 でアップロードを実行した際、ファイルのアップロードに使用した Web ページのエンコードと、ブラウザからアップロード先に送信されるデータのエンコードが異なる場合、ファイル名が文字化けして操作ログが取得されます。また、エンコードの変換の失敗など文字化けをする場合は、ファイルを「unknown」として操作ログを取得します。
- ファイルのダウンロードで、ファイルの保存先のファイルシステムが FAT の場合は、ファイルのダウンロードのログが二重に出力されることがあります。
- 「*ファイル名*をダウンロードできませんでした」というメッセージが表示される場合があります。その場合、ファイルのダウンロードを再実行してください。
- Internet Explorer で PDF ファイルを開いてから保存した場合、ファイルのダウンロードの操作ログが取得できない場合があります。Web アクセスの操作ログによって、Internet Explorer で PDF ファイルを開く操作を監視することもできます。

ヒント

ファイルのアップロード監視用のアドオンが登録された際に、登録されたアドオンを有効にするかどうかの確認メッセージが表示されます。メッセージが表示される現象を回避する場合、次の手順を実施して Internet Explorer を再起動してください。

1. 管理者権限を持つユーザでログオンし、［ファイル名を指定して実行］に「gpedit.msc」と入力して実行し、グループポリシーエディタを起動します。
2. 次の「アドオンの一覧」の設定を開きます。

［ローカルグループポリシーエディター］－［コンピュータの構成］－［管理用テンプレート］－［Windows コンポーネント］－［Internet Explorer］－［セキュリティの機能］－［アドオン管理］－［アドオンの一覧］

3. アドオンの一覧ダイアログで［有効］を選択し、［オプション］の［アドオン一覧］の［表示］ボタンを押します。
4. 次の設定を追加します。

   値の名前:{A36BDD30-8AF5-48AE-AFB9-866F89D167A5}

   値:1

アドオンが無効に設定された場合は、次の手順を実施してください。

1. メッセージが表示される現象を回避する手順を実施します。
2. Internet Explorer の［ツール］－［インターネットオプション］－［プログラム］－［アドオンの管理］から「JP1/IT Desktop Management 2 FUO」の設定を［有効］に変更します。

関連リンク

- 2.10.1　取得できる操作ログの種類

(7)　メール送受信で取得される操作ログの情報と注意事項

利用者がメーラーを使用して送受信するメールのうち、添付ファイルを含むメールの送受信の操作ログを取得できます。メール送受信で取得される操作ログの情報と注意事項について説明します。

操作ログの取得対象となるメーラーを次の表に示します。

メーラー	バージョン
Microsoft Outlook	2002
	2003
	2007
	2010
	2013
	2016
	2019
Windows Live メール	2009、2011、2012

また、操作ログを取得できるメール操作を次の表に示します。なお、複数の添付ファイルを受信または送信した場合、ファイル単位に操作ログが取得されます。

取得できるメール操作	プロトコル
受信	POP3、APOP または IMAP4
送信	SMTP または ESMTP

注意事項

- SMTP over SSL、POP3 over SSL など SSL/TLS によって通信が暗号化されている場合、操作ログは取得されません。
- S/MIME、PGP 暗号などによってメールが暗号化されている場合、操作ログは取得されません。
- メール送信で、同一内容のファイルを複数個以上、同一メールに添付して送信する場合、持ち出したファイルの情報は正しく取得されません。操作元ファイル名およびドライブ種別には、 添付した同一のファイルのうち最後に読み込んだファイルのファイル名およびドライブ種別が表示されます。
- メール送信で、0 バイトのファイルを添付してメールを送信した場合、操作元のファイル名が実際に送信したファイルと異なることがあります。
- メール送信、メール受信ログで、Outlook の TNEF 形式で送信されたメールを送受信すると、添付ファイルの情報が正しく取得されないことがあります。このため、ファイルの追跡や、ファイル持ち出しによる不審操作の検知ができない場合があります。
- 1 メール当たりの添付ファイル数が 200 個を超える場合、操作ログが取得できないことがあります。
- MIME ヘッダの Content-type が次のどちらかの場合には、添付ファイルとして扱われません。
  - application/pkcs7-mime、application/pkcs7-signature、または application/pkcs10（デジタル署名）
  - multipart/alternative（HTML メールなど）

関連リンク

- 2.10.1　取得できる操作ログの種類

(8)　添付ファイル保存で取得される操作ログの注意事項

利用者が特定のメーラーを使用し受信したメールから、添付ファイルをローカルのディスクなどに保存する操作ログを取得できます。添付ファイル保存で取得される操作ログの注意事項について説明します。

操作ログの取得対象となるメーラーを次の表に示します。

メーラー	バージョン
Microsoft Outlook	2002
	2003
	2007※
	2010※

メーラー	バージョン
Microsoft Outlook	2013※
	2016※
	2019※
Windows Live メール	2009、2011、2012

注※　添付ファイルの保存先にネットワークドライブを指定して保存した場合、操作先（保存先）のファイル名が保存したファイル名とは異なるファイル名で取得されます。

注意事項

- メール受信で同一内容の添付ファイルを受信した場合、添付ファイル保存の操作元ファイル名には同一内容のファイルのうち最後に受信したファイル名が表示されます。
- Windows 7 以降で、メーラーの画面上から次の操作をした場合、添付ファイル保存の操作ログが取得されないことがあります。
  - 添付ファイルを選択しエクスプローラまたはデスクトップにドラッグ&ドロップ操作した場合
  - ファイルを選択して［コピー］、［貼り付け］操作によってファイルを保存した場合
- 操作ログを取得する前に受信済みのメールから添付ファイルを保存した場合、添付ファイル保存の操作ログは取得されません。
- Outlook の TNEF 形式のメールを受信した場合、添付ファイル保存の操作ログが正しく取得されないことがあります。
- 1 メール当たりの添付ファイル数が 200 個を超える場合、操作ログが取得できないことがあります。
- MIME ヘッダの Content-type が次のどちらかの場合には、添付ファイルとして扱われません。
  - application/pkcs7-mime、application/pkcs7-signature、または application/pkcs10（デジタル署名）
  - multipart/alternative（HTML メールなど）

関連リンク

- 2.10.1　取得できる操作ログの種類

(9)　ファイル送受信の操作ログ取得の注意事項

利用者が Web ブラウザで FTP サイトにアクセスし、ファイルの送信、または受信した場合の操作を取得できます。対象とする Web ブラウザは、「2.10.1　取得できる操作ログの種類」の前提条件の表を参照してください。ファイル送受信の操作ログ取得の注意事項について説明します。

注意事項

- FTP over SSL/TLS によるファイル送受信の操作ログは取得できません。

- Internet Explorer 10、11 の環境で拡張保護モードが有効な場合、FTP 受信の操作ログを取得できません。
- Internet Explorer でファイル受信の操作ログを取得した場合、操作元ファイル名には FTP サーバの URL が取得されます。
- ファイル送信の操作ログの持ち出し先ファイル情報には、FTP サーバの IP アドレスが取得されます。
- FTP 受信でファイルの保存先のファイルシステムが FAT の場合は、FTP 受信のログが二重に出力されることがあります。

関連リンク

- 2.10.1　取得できる操作ログの種類

(10)　印刷操作で取得される操作ログの情報と前提条件および注意事項

印刷の操作ログを取得できます。印刷の操作ログを取得できるプリンタを次の表に示します。なお、[デバイスとプリンター] で設定してあるプリンタが対象です。なお、[デバイスとプリンター] に表示されるプリンタは、同一機器であれば、ログオンする利用者に関係なく共通です。

プリンタ種別	印刷操作ログの取得
ローカルプリンタ	○
ネットワーク共有プリンタ	○　※
インターネットプリンタ	×
仮想プリンタ	○

（凡例）○：使用できる　×：使用できない

注※　印刷ページ数は取得できません。

前提条件

各プリンタのプロパティで、すべてのログオンユーザーに［印刷］と［ドキュメントの管理］が許可されている必要があります。

ネットワーク共有プリンタの場合、以下の前提条件が追加されます。

- サポートするエージェントとプリントサーバの組み合わせを以下に示します。

エージェント	プリントサーバ	印刷操作ログの取得
Windows 7 以降	Windows XP/2003	×
Windows 7 以降	Windows Vista 以降	○
任意	上記以外	×

（凡例）○：使用できる　×：使用できない

- プリントサーバとエージェント PC 間で RPC による通信ができる必要があります。RPC 通信ができない場合は以下が考えられます。
  - プリントサーバが Internet Printing Protocol（IPP）サーバである
  - プリントサーバとエージェント PC の間にファイアウォール、プロキシまたは NAT がある
  - エージェント PC の Windows ファイアウォールが有効で、かつ［ファイルとプリンターの共有］が［例外］に設定されていない
- エージェント PC で［Microsoft ネットワーク用ファイルとプリンター共有］が有効である必要があります。
- プリントサーバからエージェント PC の名前を解決できる必要があります。
- エージェント PC が Windows 7 以降の場合、エージェント PC とプリントサーバが同一のドメインに参加している、または、エージェント PC の資格認証マネージャにプリントサーバの資格情報が登録されている必要があります。資格情報を追加した場合はエージェント PC を再起動する必要があります。

注意事項

- 秘文によって印刷が抑止されている場合、印刷操作の操作ログは取得できません。
- プリンタ追加直後に印刷した場合、印刷ログの取得ができないことがあります。
- OS にログオンした直後に印刷した場合、印刷ログの取得ができないことがあります。
- 印刷操作がエージェントに通知される前に印刷ジョブが完了した場合、印刷ログの取得はできません。
- プリンタによっては一度の印刷操作で複数の印刷ログが取得される場合があります。

ネットワーク共有プリンタの場合、以下の注意事項が追加されます。

- IPv6 が有効でクライアントコンピュータで印刷ジョブのレンダリングが動作しない場合は、印刷ログの取得ができない場合があります。クライアントコンピュータで印刷ジョブのレンダリングを動作させるには以下の設定が必要です。
  - ［クライアント コンピューターで印刷ジョブのレンダリングをする］または［クライアント コンピューターに印刷ジョブを表示する］が有効である。
  - ［詳細な印刷機能を有効にする］が有効である。
- ネットワーク共有プリンタへの印刷ではページ数が取得できません。そのため、大量印刷の検知、ユーザ活動状況レポート（大量印刷）の対象外となります。

関連リンク

- 2.10.1　取得できる操作ログの種類

(11)　デバイス操作の操作ログ取得の注意事項

デバイスを機器に接続または切断した操作ログを取得できます。また、禁止操作を設定した場合、デバイスの接続抑止や接続許可の操作ログも取得できます。

ドライブへのメディア（CD、DVD、SD カードなど）の挿入、および取り出しは取得できません。デバイス操作の操作ログ取得の注意事項を説明します。

注意事項

- コンソールセッションの利用者を該当の利用者と見なします。コンソールセッションの利用者がいなければ、アカウント名は取得できません。
- 初めて機器に接続されるデバイスの場合、1 回の接続で複数の接続および切断（取り外し）の情報を取得することがあります。
- Windows Server 2019、Windows Server 2016、Windows 10、Windows Server 2012 R2、Winodws 8.1、Windows Server 2012、および Winodws 8 の高速スタートアップ機能が有効な場合、コンピュータに接続されているデバイスをシャットダウン中に取り外すと、その後コンピュータを起動したときに「デバイス切断」の操作ログが取得されます。
- デバイスが抑止される状況で取得したデバイスの接続ログ 、切断ログ、接続抑止ログ、イベントは、取得項目が取得できない場合があります。
- コンピュータ起動直後など、JP1/IT Desktop Management 2 の起動前にデバイスが接続された場合、操作ログは取得できません。
- 複数のデバイスインスタンス ID を持つデバイスが接続された場合、1 つのデバイスに対して複数の操作ログとイベントが取得されます。ただし、切断時は 1 つしか取得されないこともあります。
- デバイスを初めてコンピュータに接続する場合、ドライバのインストールが実施されると複数の同じ操作ログとイベントが取得されることがあります。
- 設定を有効にするために再起動が必要な場合でも、接続抑止ログと接続抑止イベントは設定を実施した時点で取得されます。
- 他製品によってデバイスの設定が変更され、デバイスの接続または切断が検知された場合も、操作ログが取得されます。
- USB 接続のデバイスであっても、USB デバイス、Bluetooth デバイス、イメージングデバイスとして認識されないデバイスの操作ログは取得できません。
- CD または DVD がセットされた状態で CD/DVD ドライブを接続すると、複数のログが取得される場合があります。
- デバイスの抑止が有効となるためにコンピュータの再起動が必要な場合、抑止対象デバイスの抑止ログ、切断ログおよびイベントが取得されません。
- OS がログ取得対象デバイスを別のデバイスとして認識した場合、そのデバイスの操作ログは取得できません。ただし、OS の認識が別のログ取得対象デバイスと一致した場合は OS が認識したデバイスとして抑止されます。
- 同じデバイスの抑止設定を短期間に繰り返し変更した場合、接続ログおよび切断ログが取得できないことがあります。
- Citrix XenApp、Microsoft RDS サーバの場合、接続元の機器に存在するドライブは接続先のセッションでドライブ種別が「その他」のドライブとして表示されます。そのようなドライブについては、デバイスを機器に接続または切断した操作ログを取得できません。

関連リンク

- 2.10.1　取得できる操作ログの種類

(12)　ウィンドウ操作の操作ログ取得の注意事項

OS 上でウィンドウを操作した操作ログを取得できます。ウィンドウ操作の操作ログは、次のような場合に取得できます。

- 新規にウィンドウが起動し、そのウィンドウがアクティブになった場合
- マウス操作や［Alt］＋［Tab］キーによってアクティブなウィンドウが切り替わった場合
- ウィンドウ中の操作によって別ウィンドウが起動し、そのウィンドウがアクティブになった場合

ウィンドウ操作の操作ログ取得の注意事項を説明します。

注意事項

- ログオン直後などにウィンドウ操作の操作ログを取得した場合、ログオンユーザー名が空になることがあります。
- アプリケーションによって生成されるウィンドウのうち、タイトルなしの状態で表示し、その後タイトルが設定されるウィンドウの場合、ウィンドウタイトルは取得されません。

関連リンク

- 2.10.1　取得できる操作ログの種類

(13)　ファイル持ち出しによる不審操作の、入力元情報取得の前提条件と注意事項

エージェントが導入されたコンピュータにファイルが持ち込まれた場合、そのファイルの入力元の情報を取得できます。ファイル持ち出しによる不審操作の、持ち込みファイルの入力元情報取得の前提条件と注意事項をそれぞれ説明します。

前提条件

- エージェントが導入されたコンピュータのファイルシステムが NTFS（5.0 以降）である必要があります。

注意事項

- 次のどれかが有効なセキュリティポリシーが適用されている場合、ファイル操作が実施されるとエージェントは操作対象のファイルに追跡情報や不審操作に関する情報を付与します。
  - ［操作ログ］－［情報漏えいに係わりの深い操作を取得対象にする（推奨）］
  - ［操作ログ］－［操作ログの取得対象］の［ファイルコピー］、［ファイル移動］、［ファイル名称変更］、［ファイル作成］、［ファイル削除］、［Web アップロード］、［Web ダウンロード］、［ファイル

送信]、[ファイル受信]、[メール送信（添付ファイル付)]、[メール受信（添付ファイル付)]、[添付ファイル保存］のどれか

- ［操作ログ］－［不審と見なす操作］の［添付ファイル付きメールの送受信]、[Web/FTP サーバの使用]、[外部メディア（リムーバブルディスク）へのファイルコピーと移動］のどれか

- エージェントによって追跡情報や不審操作に関する情報が付与されたファイルを FAT や ReFS など NTFS 以外でフォーマットされたドライブに移動またはコピーすると、Windows のプロパティの損失のダイアログが表示されます。
- Windows のプロパティの損失のダイアログでファイルの移動またはコピーを続行すると、移動またはコピー先のファイルから追跡情報や不審操作に関する情報が削除されます。そのため、移動またはコピーしたファイルを外部メディアに持ち出すと、ファイル持ち出しによる不審操作を正しく検知できません。ファイルを圧縮または展開などしてデータを加工した場合も同様です。
- Windows のプロパティの損失のダイアログの表示を回避するには、エージェントが導入されたコンピュータに対して操作ログと不審操作の取得をするセキュリティポリシーを適用する前に、レジストリに次の値を設定してください。

キー名	OS が 32 ビット版の場合 HKLM¥SOFTWARE¥HITACHI¥JP1/IT Desktop Management - Agent OS が 64 ビット版の場合 HKLM¥SOFTWARE¥Wow6432Node¥HITACHI¥JP1/IT Desktop Management - Agent
値名	JdngSmcStopWriteTrackingInfo
型	REG_SZ
値	1

  - このオプションを使用できるのは JP1/IT Desktop Management 2 - Agent 11-51-02 以降のバージョンです。
  - このオプションを設定することでエージェントがファイルに追跡情報や不審操作の情報を付与しなくなります。このため次の情報が取得されなくなります。
    - ファイル操作の追跡情報
    - 次のファイル操作に対する不審操作の判定結果
      - 外部メディア(リムーバブルディスク)へのファイルのコピーと移動
      - ファイルアップロード
      - ファイル送信
      - メール送信（添付ファイル付）
  - このオプションを有効化する前にすでにファイルに追跡情報や不審操作の情報が付与されていた場合、そのファイルを NTFS 以外でフォーマットされたドライブに移動またはコピーすると、プロパティの損失のダイアログが表示されます。
  - このオプションを無効化するには上記のレジストリを削除するか、値に 0 を設定してください。

関連リンク

- 2.10.1　取得できる操作ログの種類

2.10.8　管理用サーバへの秘文ログの取り込み

連携する秘文のバージョンが 10-00 以降の場合は、秘文ログを JP1/IT Desktop Management 2 に取り込むことができます。

取り込んだ秘文ログを、セキュリティ画面の［操作ログ］画面で、JP1/IT Desktop Management 2 の操作ログと合わせて、調査することができます。

(1)　JP1/IT Desktop Management 2 と秘文の情報漏えい対策機能の一覧

JP1/IT Desktop Management 2 と秘文の機能を組み合わせることで情報漏えい対策ができます。
JP1/IT Desktop Management 2 と秘文の情報漏えい対策機能の一覧を次に示します。

情報漏えい対策機能	JP1/IT Desktop Management 2 の機能	秘文の機能
データの不正な持ち出しを抑止する	禁止操作の抑止 • 印刷の抑止 • 機器の使用抑止 • ソフトウェアの起動抑止 不審操作の取得 • 大量印刷	持ち出し制御 デバイス制御 許可ネットワーク制御
コンピュータ利用者のファイル操作のログを取得する	操作ログの取得 • ファイル操作/印刷操作 • フォルダ操作 不審操作の取得 • 添付ファイル付きメールの送受信 • Web/FTP サーバの使用 • 外部メディア（リムーバブルディスク）へのファイルコピーと移動	秘文拡張操作ログの取得 • ファイル操作ログ • ドライブ操作ログ
コンピュータ利用者のウィンドウ操作、Web アクセスのログを取得する	操作ログの取得 • ウィンドウ操作 • Web アクセス	秘文拡張操作ログの取得 • アプリケーション操作ログ
コンピュータの起動・停止とログオン・ログオフのログを取得する	操作ログの取得 • コンピュータの起動と停止、ログオンとログオフ	イベントログの取得
デバイスへのアクセスログとプログラムの起動・停止ログを取得する	操作ログの取得 • プログラム起動/停止 • デバイス操作	アクセスログの取得

情報漏えい対策機能	JP1/IT Desktop Management 2 の機能	秘文の機能
デバイスへのアクセスログとプログラムの起動・停止ログを取得する	• 抑止ログ	アクセスログの取得

重要

- JP1/IT Desktop Management 2 と秘文で同じ情報漏えい対策機能を使用すると、同一の操作ログが操作ログ一覧画面に表示されることがあります。
- 「コンピュータ利用者のファイル操作のログを取得する」の機能を使用する場合は、JP1/IT Desktop Management 2 の機能か秘文の機能のどちらか一方だけを使用してください。両方の機能を同時に使用しないでください。
- 操作ログのポリシーの［情報漏えいに係わりの深い操作を取得対象にする（推奨)］をチェックする場合は、「コンピュータ利用者のファイル操作のログを取得する」の秘文の機能は使用しないでください。

  「コンピュータ利用者のファイル操作のログを取得する」の秘文の機能を使用する場合は、操作ログのポリシーの［情報漏えいに係わりの深い操作を取得対象にする（推奨)］のチェックを外してください。

  両方の機能を同時に使用しないでください。

(2) JP1/IT Desktop Management 2 に取り込める秘文ログ

JP1/IT Desktop Management 2 に取り込める秘文ログの種類を次に示します。秘文ログは、CSV 形式のファイルとしてください。

秘文ログの種類	説明
アクセスログ	• 共有機密フォルダへのアクセスや、USB メモリなどのリムーバブルメディアへのファイルの持ち出しなど、秘文クライアント上で行われたユーザーのアクセス操作 • プログラムの起動や終了など、秘文クライアント上で行われたプログラムの動作
イベントログ	ログイン、ログアウト、パスワード変更など、秘文クライアント上で発生したイベントの履歴
秘文拡張操作ログ	クライアント PC でのユーザの操作による、アプリケーション操作やファイル操作のログ

(3) 秘文ログの取り込み

秘文ログを JP1/IT Desktop Management 2 に取り込む手順については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の秘文ログを取り込む説明を参照してください。

操作ログの保管先への保存

JP1/IT Desktop Management 2 に取り込んだ秘文ログは、JP1/IT Desktop Management 2 で取得した操作ログと同様に、操作ログの保管先に保存されます。なお、操作ログの自動取り込みを有効にすると、

自動的に操作ログのデータベースに操作ログを取り込めます。保管先フォルダに保存された操作ログは、保管先フォルダからデータベースに取り込んで参照できます。

保管されるデータ

秘文ログは次に示すように、ログの種類ごと、日付単位でフォルダに分けられて格納されます。

セットアップで設定した［操作ログの保管先フォルダ］¥EXLOG¥*ログの種類*¥*操作日付(YYYYMMDD)*

保管に必要な容量

「4.5.3　操作ログの保管先フォルダに必要なディスク容量の目安」および「4.5.4　操作ログのデータベースに必要なディスク容量の目安」を参照してください。

操作ログのデータベースへの取り込み

操作ログのデータベースに秘文ログを取り込むと秘文ログを参照できます。JP1/IT Desktop Management 2 で取得した操作ログと同様に、「自動取り込み」と「手動取り込み」があります。

自動取り込み

設定画面の［操作ログの設定］で指定された格納期間に合わせて、秘文ログが取り込まれます。

手動取り込み

調査したい操作ログが含まれる期間を指定して操作ログの保管先から秘文ログを取り込めます。また、対象のコンピュータを指定して取り込むこともできます。

関連リンク

- (2)　管理用サーバでの操作ログの保管
- (3)　管理用サーバへの操作ログの取り込み

(4)　JP1/IT Desktop Management 2 に取り込んだ秘文ログの表示

JP1/IT Desktop Management 2 の操作ログのデータベースに取り込んだ秘文ログは、セキュリティ画面の［操作ログ一覧］画面に表示されます。表示される項目を次に示します。

［操作ログ一覧］画面の表示項目	秘文ログを表示する場合の内容
［追跡］ボタン	非活性になります。
［不審操作］列	空になります。
• ［操作日時（Web ブラウザのロケール）］列 • ［操作日時］列 • ［操作時刻］列	次に示す日時が、JP1/IT Desktop Management 2 - Manager のタイムゾーンで表示されます。 アクセスログ 　アクセスした日付および時刻 イベントログ 　イベントが発生した日付および時刻 秘文拡張操作ログ 　ログが出力された日付および時刻

[操作ログ一覧] 画面の表示項目	秘文ログを表示する場合の内容
[発生元] 列	ログを出力したクライアントのコンピュータ名が表示されます。JP1/IT Desktop Management 2 で管理している機器情報と同定できた場合は、リンクで表示されます。リンクをクリックすると、機器一覧画面が表示されます。 JP1/IT Desktop Management 2 の操作ログはコンピュータの FQDN（完全就職ドメイン名）で表示されるため、秘文ログで出力されたコンピュータ名とは異なって表示される場合があります。
[ホスト識別子] 列	JP1/IT Desktop Management 2 で管理している機器情報と同定できた場合は、その機器のホスト識別子が表示されます。 同定できなかった場合は、空になります。
[ユーザー名] 列	Windows ユーザー名が表示されます。
[操作種別] 列	「[操作種別] の表示内容」を参照してください。
[操作種別（詳細）] 列	「[操作種別（詳細）] の表示内容」を参照してください。
[操作対象] 列	次に示す内容が表示されます。 アクセスログ ファイル名が表示されます。ただし、「プロセス生成」、「プロセスの権限更新」、および「プロセス終了」の場合はプロセス名が表示されます。 イベントログ イベントの対象が表示されます。 秘文拡張操作ログ ファイル名が表示されます。
[操作内容] 列	次に示す内容が表示されます。 アクセスログ 「ステータス」、「プロセス名」、「メッセージ 1」、「メッセージ 2」、および「メッセージ 3」が「,」（コンマ）区切りで列挙された内容 イベントログ ステータス 秘文拡張操作ログ 「ステータス」、「プロセス名」、「メッセージ 1」、「メッセージ 2」、および「メッセージ 3」が「,」（コンマ）区切りで列挙された内容
• [ファイル作成日時] 列 • [ファイル更新日時] 列 • [持ち込み日時] 列	空になります。
• [ファイルサイズ] 列 • [持ち出し先ドライブ種別] 列	秘文拡張操作ログのファイル操作ログの場合だけ表示されます。秘文での設定が必要です。
[印刷ページ数] 列	空になります。
[シリアルナンバー] 列	デバイス接続のログの場合に表示されます。また、固体識別ログの場合で「秘文ログの操作値」が「CFL」、「OPN」、「WRI」、「DEL」、「CDR」、「DDR」または「REN」の場合に表示されます。秘文での設定が必要です。

[操作ログ一覧] 画面の表示項目	秘文ログを表示する場合の内容
[シリアルナンバー] 列	シリアル番号が OS から自動的に付与された場合は、末尾に「[*]」が追加されます。
[デバイス区分] 列	デバイス接続のログの場合だけ表示されます。

秘文ログのコンピュータ名と機器のホスト名の同定

秘文ログを取り込む時に、秘文ログのコンピュータ名を JP1/IT Desktop Management 2 の機器のホスト名に引き当てます。引き当て（同定）に成功した場合、秘文ログと JP1/IT Desktop Management 2 の機器を関連づけます。引き当て（同定）に失敗した秘文ログは、セキュリティ画面の［操作ログ］画面でホスト識別子が表示されません。

［操作種別］の表示内容

［操作種別］の表示内容	秘文のアクセスログまたは秘文の拡張操作ログのログタイプ値	検索されるフィルタ
[秘文]暗号化対象ファイルへのアクセス	MYS	操作対象ファイル名（操作種別がファイル操作の場合）
[秘文]ネットワークおよび禁止された制御メディアへのアクセス	RES	操作対象ファイル名（操作種別がファイル操作の場合）
[秘文]許可された制御メディアへのアクセス：暗号文	CMD	操作対象ファイル名（操作種別がファイル操作の場合）
[秘文]許可された制御メディアへのアクセス：平文	PMD	操作対象ファイル名（操作種別がファイル操作の場合）
[秘文]内蔵ハードディスクへのアクセス	NRD	操作対象ファイル名（操作種別がファイル操作の場合）
[秘文]プリンタ出力	PRT	印刷ドキュメント名（操作種別が印刷操作の場合）
[秘文]秘文持ち出しによるアクセス/秘文機密ファイル作成	VFL	操作対象ファイル名（操作種別がファイル操作の場合）
[秘文]共有機密フォルダへのアクセス	NET	操作対象ファイル名（操作種別がファイル操作の場合）
[秘文]メール持ち出しによるアクセス	TCP	
[秘文]デバイスの接続	CON	• デバイス名（操作種別がデバイス操作の場合） • デバイス区分（操作種別がデバイス操作の場合）
[秘文]ネットワークへのアクセス	NAC	
[秘文]ファイル保護	EFP	
[秘文]プログラム起動/終了	CLS	プロセス名（操作種別がプログラムの起動と停止の場合）

[操作種別] の表示内容	秘文のアクセスログまたは秘文の拡張操作ログのログタイプ値	検索されるフィルタ
[秘文]マルウェア検知（CylancePROTECT）	CYL	
[秘文]イベントログ	－	
[秘文]アプリケーション操作ログ	OMA	ウィンドウタイトル（操作種別がウィンドウ操作の場合）
[秘文]ファイル操作ログ	OMF	• 持ち出し先ドライブ種別（操作種別がファイル操作の場合） • 操作対象ファイル名（操作種別がファイル操作の場合）
不明	－	

（凡例）－：該当なし

[操作種別（詳細）] の表示内容

[操作種別（詳細）] の表示内容	秘文ログの操作値	秘文ログの種別
[秘文]ファイルを開く/ファイルを作成する/ファイルを印刷する	CFL	A
[秘文]ファイルを開く	OPN	A
[秘文]ファイルを開く/ファイルを書き込みモードで開く	WRI	A
[秘文]ファイルを削除する	DEL	A
[秘文]フォルダを作成する	CDR	A
[秘文]フォルダを削除する	DDR	A
[秘文]フォルダ・ファイルの名称を変更する/同一ドライブ内で移動する/共有機密フォルダから自フォルダ内でフォルダを移動する	REN	A
[秘文]共有機密フォルダをコピーする	CPD	A
[秘文]共有機密フォルダから自フォルダ外へフォルダを移動する	MVD	A
[秘文]複製ファイル取得機能のコピー操作	CPY	A
[秘文]ライティングソフト起動	MED	A
[秘文]秘文持ち出し：組織外	VFO	A
[秘文]秘文持ち出し：閲覧専用	VFV	A
[秘文]秘文持ち出し：平文	VFP	A
[秘文]秘文機密ファイル作成	ARC	A
[秘文]メールの送信	MAL	A
[秘文]リムーバブルメディアの接続	REM	A

[操作種別（詳細）]の表示内容	秘文ログの操作値	秘文ログの種別
[秘文]外付けハードディスクの接続	EXD	A
[秘文]CD/DVD ドライブの接続	CDD	A
[秘文]赤外線の接続	IRD	A
[秘文]Bluetooth の接続	BTH	A
[秘文]無線 LAN の接続	WLN	A
[秘文]モデムの接続	MDM	A
[秘文]イメージングデバイスの接続	IMG	A
[秘文]Windows ポータブルデバイスの接続	WPD	A
[秘文]Windows モバイルデバイスの接続	WML	A
[秘文]Palm ハンドヘルドデバイスの接続	PLM	A
[秘文]BlackBerry デバイスの接続	BBY	A
[秘文]シリアルポート／パラレルポートの接続	SPP	A
[秘文]その他の制御対象デバイスの接続	OTR	A
[秘文]有線 LAN（USB 接続）の接続	ULN	A
[秘文]有線 LAN（USB 接続以外）の接続	OLN	A
[秘文]有線 LAN の接続	LCN	A
[秘文]無線 LAN の接続（ネットワーク接続ログ）	WCN	A
[秘文]無線 LAN のローミング再接続	WRA	A
[秘文]ネットワークの通信（TCP/IP）	COM	A
[秘文]ファイルアクセス	CRF	A
[秘文]ネットワーク通信	NWA	A
[秘文]プロセス生成	CRP	A
[秘文]プロセスの権限更新	UPP	A
[秘文]プロセス終了	TEP	A
[秘文]プログラムファイルのロード	LOD	A
[秘文]マルウェア検知イベント発生（CylancePROTECT）	MDE	A
[秘文]メモリ保護イベントまたはスクリプト禁止イベント発生（CylancePROTECT）	MWE	A
[秘文]その他のイベント発生（CylancePROTECT）	COE	A
[秘文]不明なイベント発生（CylancePROTECT）	CUK	A
[秘文]秘文 DC または秘文 DE にログイン	LOGIN	E

[操作種別（詳細）]の表示内容	秘文ログの操作値	秘文ログの種別
[秘文]秘文 DC または秘文 DE からログアウト	LOGOUT	E
[秘文]秘文 DC または秘文 DE ログイン失敗	LOGERR	E
[秘文]秘文 DE（FS）にログイン	FSLOGIN	E
[秘文]秘文 DE（FS）からログアウト	FSLOGOUT	E
[秘文]秘文 DE（FS）ログイン失敗	FSLOGERR	E
[秘文]秘文 IC にログイン	ICLOGIN※	E
[秘文]秘文 IC からログアウト	ICLOGOUT※	E
[秘文]秘文 IS にログイン	ISLOGIN※	E
[秘文]秘文 IS からログアウト	ISLOGOUT※	E
[秘文]秘文 IS ログイン失敗	ISLOGERR※	E
[秘文]秘文 IF にログイン	IFLOGIN※	E
[秘文]秘文 IF からログアウト	IFLOGOUT※	E
[秘文]秘文 IF ログイン失敗	IFLOGERR※	E
[秘文]管理者コマンド実行	MNGCMD※	E
[秘文]クライアント設定変更	CNFUPDATE※	E
[秘文]秘文 DC/秘文 DE（FS）/秘文 IF/秘文 IS のパスワードを変更	CHGPASLOC	E
[秘文]スクリーンロック	SCLOCK	E
[秘文]スクリーンロック解除	SCUNLOCK	E
[秘文]端末ロック	PCLOCK	E
[秘文]端末ロック解除	PCUNLOCK	E
[秘文]デバイス使用可否制御設定更新	DEVUPDATE	E
[秘文]許可ネットワーク制御設定更新	NETUPDATE	E
[秘文]社内モード切り替え	INTCHG	E
[秘文]社外モード切り替え	EXTCHG	E
[秘文]ファイル保護設定更新	EFPUPDATE	E
[秘文]PC 起動	PON	E
[秘文]PC 終了	POF	E
[秘文]Windows ログオン	WSI	E
[秘文]Windows ログオフ	WSO	E

[操作種別（詳細）]の表示内容	秘文ログの操作値	秘文ログの種別
[秘文]拡張ログ設定更新	TLSUPDATE	E
[秘文]ウィンドウアクティブ	ACT	H
[秘文]エンジン開始	EST	H
[秘文]休止及び待機状態	PWR	H
[秘文]ログオフおよびシャットダウン	END	H
[秘文]ログ取得開始	LST	H
[秘文]エンジン終了	EEN	H
[秘文]エンジン異常	OME	H
[秘文]ファイル作成	FCR	H
[秘文]ファイルコピー	FCP	H
[秘文]ファイル移動	FMV	H
[秘文]ファイル名変更	FRE	H
[秘文]ファイル削除	FDE	H
[秘文]ファイルオープン	FOP	H
[秘文]ファイル上書き保存	FUD	H
[秘文]ドライブの追加	ADD	H
[秘文]ドライブの削除	DED	H
不明	－	－

（凡例）A：アクセスログ　E：イベントログ　H：秘文拡張操作ログ　－：該当なし

注※　秘文のバージョンが 10-50 以前の操作を示します。

(5)　秘文ログ取り込みの設定

秘文ログを取り込む場合、外部ログインポートコマンド用設定ファイルを変更する必要があります。デフォルトでは秘文ログを取り込まない設定です。外部ログインポートコマンド用設定ファイルの詳細は、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の「ioutils importexlog（外部ログのインポート）」を参照してください。

取り込まない秘文ログの設定

秘文ログを取り込む時に、取り込まない秘文ログを外部ログインポート用設定ファイルで指定できます。デフォルトでは次に示す秘文ログを取り込まない設定です。

- 内蔵ハードディスクのアクセスログ
- ファイル参照ログ

- ネットワークの通信（TCP/IP）ログ

未知の秘文ログの取り込み

「(4)　JP1/IT Desktop Management 2 に取り込んだ秘文ログの表示」の「[操作種別]の表示内容」の表および「[操作種別（詳細）]の表示内容」の表に記載されていない、未知の秘文ログを JP1/IT Desktop Management 2 に取り込む場合、外部ログインポートコマンド用設定ファイルを変更する必要があります。デフォルトでは未知の秘文ログを取り込まない設定です。

操作ログのデータベースに取り込んだ未知の秘文ログは、セキュリティ画面の［操作ログ一覧］画面で、［操作種別］および［操作種別（詳細）］に「不明」と表示されます。この場合、未知の秘文ログの操作の値が、「,」（コンマ）区切りで［操作対象］に表示されます。

(6)　秘文ログ取り込みの注意事項

秘文ログ取り込みの注意事項を次に示します。

- クライアントのコンピュータの時刻を戻した後に取得された秘文ログは、 既に取り込まれているログと判断され、JP1/IT Desktop Management 2 には取り込まれません。
- 操作ログの設定画面で、[操作ログを自動的に取り込む] を無効にする、または［自動取り込みされる操作ログの格納期間］を減らすと、操作ログのデータベースに取り込まれている操作ログは削除されます。削除された期間の秘文ログを、設定を戻した後で取り込む場合は、デフォルト 1 時に実行される「自動取り込みされた操作ログデータベースのメンテナンス」後に実施してください。「自動取り込みされた操作ログデータベースのメンテナンス」の開始時間は、コンフィグレーションファイルで設定できます。

2.11　資産の管理

JP1/IT Desktop Management 2 を利用して、組織内で管理している機器、ソフトウェアライセンス、契約などの資産情報をまとめて管理できます。

各資産を一覧化して台帳のように管理できるほか、資産情報同士の関係を定義することで、機器に対して結んでいる契約を即座に把握したり、ソフトウェアライセンスの利用状況を把握したりできるため、資産管理業務の効率化を図れます。

資産管理には、Asset Console を使用する方法と、JP1/IT Desktop Management 2 の操作画面を使用する方法があります。これらの 2 つの方法の機能差異、および Asset Console を使用した資産管理の詳細については、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。

なお、これらの 2 つの方法は併用できません。資産情報の整合性を保持するために、JP1/IT Desktop Management 2 のシステム構築時に、Asset Console を使用するかどうかを選択する必要があります。

ここでは、JP1/IT Desktop Management 2 の操作画面を使用した資産管理について説明します。

JP1/IT Desktop Management 2 の操作画面を使用して、組織内で管理している機器、ソフトウェアライセンス、契約などの資産情報をまとめて管理できます。各資産を一覧化して台帳のように管理できるほか、資産情報同士の関係を定義することで、機器に対して結んでいる契約を即座に把握したり、ソフトウェアライセンスの利用状況を把握したりできるため、資産管理業務の効率化を図れます。また、IP アドレスを持つ機器だけでなく、ディスプレイや USB メモリなど、IP アドレスを持たない機器も管理できます。お客様固有の情報を拡張情報として追加することもできます。

JP1/IT Desktop Management 2 では、次に示す資産管理業務を支援しています。

ハードウェア資産の管理

コンピュータ、サーバ、プリンタ、ネットワーク装置、USB デバイスなど、所有している機器の情報をハードウェア資産情報として管理できます。各資産の詳細情報を管理できるだけでなく、運用中、在庫、滅却済みなどのステータスも管理でき、組織内のハードウェア資産の状況を把握できます。

ソフトウェアライセンスの管理

所有しているソフトウェアライセンスの情報と、ソフトウェアごとのライセンスの利用状況を管理できます。ライセンスの総数管理だけでなく、個々のコンピュータにライセンスを割り当てて、許可なくライセンスを利用しているコンピュータを確認することもできます。

資産に関する契約の管理

サポート契約やレンタル契約、リース契約など、ハードウェア資産やソフトウェアライセンスに関する契約情報を登録して、それぞれの資産情報と対応づけて管理できます。満了日が近づいている契約情報を把握できるので、今後の作業計画を予定することもできます。

資産に掛かるコストの管理

ハードウェア資産やソフトウェアライセンスに関する契約情報を管理することで、それらに掛かっているコストを確認できます。この情報を活用することで、余計なコストが掛かっていないかチェックしたり、今後の資産運用に掛かるコストを見積もったりできます。

ここでは、各業務に応じた JP1/IT Desktop Management 2 の利用方法を説明しています。目的の業務に応じて説明を参照してください。

2.11.1 資産情報の管理項目一覧

資産情報の管理項目を次に示します。以降の表中では、凡例を次のとおり表記しています。

（凡例）－：対象外

> **ヒント**
>
> ここに記載されている管理項目以外に、独自の管理項目を追加することもできます。

> **ヒント**
>
> 一部の管理項目について、入力方法やデータ型を変更できます。詳細については、「(3) カスタマイズできる資産管理項目の種類」を参照してください。

ハードウェア資産

管理項目	説明	入力方法	データ型
資産管理番号	ハードウェア資産の証書に掲載されている番号や独自に管理しやすいユニークな番号を設定します。[資産管理番号] は、ハードウェア資産情報をインポートするときに、マッピングキーとして使用します。	管理者が入力	テキスト型
機器名称	資産を判別するための名称を設定します。	管理者が入力	テキスト型
説明	資産を識別するための情報を設定します。一覧で表示されたときに確認しやすいような情報にすることをお勧めします。	管理者が入力	テキスト型
添付ファイル	資産に関するファイルを登録します。ハードウェア資産の証書などを電子データ化して登録しておくと、ハードウェア資産の詳細情報を参照したいときに資料を探す手間が省けます。	管理者が入力	－
契約会社名※4	関連づけられた契約情報の契約会社が表示されます。	－	－
契約日※4	関連づけられた契約情報の契約日が表示されます。	－	－
資産状態	資産の状態を設定します。デフォルトでは、[在庫]、[運用中]、または [滅却] を設定できます。	管理者が入力	選択型

管理項目	説明	入力方法	データ型
予定資産状態	資産の状態を変更する予定がある場合は、変更後の資産状態を設定します。デフォルトでは、[在庫]、[運用中]、または［滅却］を設定できます。	管理者が入力	選択型
変更予定日	資産の状態を変更する予定がある場合は、状態を変更する予定日を設定します。予定日を設定しておくと、予定日に近くなった場合、および予定日になった場合に、その資産に対する運用が必要なことがイベントやレポートで通知されます。	管理者が入力	日付型
棚卸日	資産の棚卸を実施した日を設定します。棚卸日を自動的に更新するように設定することもできます。	管理者が入力	日付型
部署※1	資産を利用している部署を設定します。	次の方法を指定できます。 • 管理者が入力 • 利用者が入力 • Active Directory から取得 • レジストリから取得	次のデータ型を指定できます。 • テキスト型 • 選択型 • 階層型
設置場所※1	資産が設置されている場所を設定します。	次の方法を指定できます。 • 管理者が入力 • 利用者が入力 • Active Directory から取得 • レジストリから取得	次のデータ型を指定できます。 • テキスト型 • 選択型 • 階層型
利用者名※1	資産を利用する人の名前を設定します。複数人で利用している場合は、代表者の名前を設定します。	次の方法を指定できます。 • 管理者が入力 • 利用者が入力 • Active Directory から取得 • レジストリから取得	テキスト型
アカウント※1	資産の利用者（代表者）を識別できる情報（社員番号など）を設定します。	次の方法を指定できます。 • 管理者が入力 • 利用者が入力 • Active Directory から取得	テキスト型

管理項目	説明	入力方法	データ型
アカウント※1	資産の利用者（代表者）を識別できる情報（社員番号など）を設定します。	• レジストリから取得	テキスト型
メールアドレス※1	資産の利用者（代表者）のメールアドレスを設定します。	次の方法を指定できます。 • 管理者が入力 • 利用者が入力 • Active Directory から取得 • レジストリから取得	テキスト型
電話番号※1	資産の利用者（代表者）の電話番号を設定します。	次の方法を指定できます。 • 管理者が入力 • 利用者が入力 • Active Directory から取得 • レジストリから取得	テキスト型
登録日時	資産情報が登録された日時が表示されます。	－	－
更新日時	資産情報が更新された日時が表示されます。	－	－
機器種別※2	機器の種別を設定します。デフォルトでは、[PC]、[サーバ]、[ストレージ]、[ネットワーク装置]、[プリンタ]、[スマートデバイス]、[周辺装置]、[USB デバイス]、[ディスプレイ]、[その他]、または［不明な機器］を設定できます。	管理者が入力	選択型
モデル※2	機器のモデルを設定します。	管理者が入力	テキスト型
メーカー※2	機器の製造元を設定します。	管理者が入力	選択型※3
シリアルナンバー※2	機器のシリアルナンバー（BIOS 情報）を設定します。[シリアルナンバー］は、ハードウェア資産情報をインポートするときや、収集した機器情報がハードウェア資産情報に自動で登録されるときに、マッピングキーとして使用します。	管理者が入力	テキスト型
CPU※2	機器の CPU を設定します。	管理者が入力	選択型※3
メモリ※2	機器のメモリのサイズを設定します。	管理者が入力	テキスト型
ストレージ容量※2	機器のハードディスク、SSD など、記憶媒体の論理ディスクの総容量を設定します。	管理者が入力	テキスト型
IP アドレス※2	機器の IP アドレスを設定します。複数の IP アドレスがある場合は、代表で管理する IP アドレスを設定します。[IP アドレス］は、ハードウェア資産情報をインポートするときや、収集した機	管理者が入力	テキスト型

管理項目	説明	入力方法	データ型
IP アドレス※2	器情報がハードウェア資産情報に自動で登録されるときに、マッピングキーとして使用します。	管理者が入力	テキスト型
サブネットマスク※2	機器のサブネットマスクを設定します。	管理者が入力	テキスト型
MAC アドレス※2	機器の MAC アドレスを設定します。複数の MAC アドレスがある場合は、代表で管理する MAC アドレスを設定します。[MAC アドレス] は、ハードウェア資産情報をインポートするときや、収集した機器情報がハードウェア資産情報に自動で登録されるときに、マッピングキーとして使用します。	管理者が入力	テキスト型
ホスト名※2	機器のコンピュータ名またはホスト名を設定します。[ホスト名] は、ハードウェア資産情報をインポートするときや、収集した機器情報がハードウェア資産情報に自動で登録されるときに、マッピングキーとして使用します。	管理者が入力	テキスト型
OS※2	機器にインストールされている OS を設定します。	管理者が入力	選択型※3
デバイスインスタンス ID	「機器種別」が「USB デバイス」の場合だけ、USB デバイスのユニークな ID が表示されます。	−	−
ストレージ空き容量	機器のハードディスク、SSD など、記憶媒体の論理ディスクの空き容量の合計を設定します。	管理者が入力	テキスト型
ディスプレイ種別	ディスプレイの種類を設定します。「CRT(ブラウン管)」、「LCD(液晶ディスプレイ)」、「PDP(プラズマディスプレイ)」、「ビデオプロジェクタ」、「その他」を設定できます。	管理者が入力	選択型
ディスプレイサイズ	ディスプレイのサイズを設定します。	管理者が入力	数値型
ディスプレイ解像度	ディスプレイの解像度を設定します。次の値を設定できます。 「VGA(640×480)」、「SVGA(800×600)」、「XGA(1024×768)」、「WXGA(1280×800)」、「SXGA(1280×1024)」、「WSXGA+(1680×1050)」、「UXGA(1600×1200)」、「FHD(1920×1080)」、「WUXGA(1920×1200)」、「QXGA(2048×1536)」、「その他」	管理者が入力	選択型
UDID	Apple 社製のスマートデバイスに付与されている識別番号を設定します。	管理者が入力	テキスト型
IMEI	移動体通信機器に付与されている識別番号を設定します。IMEI は、ハードウェア資産情報をインポートするときや、収集された機器情報がハードウェア資産情報に自動で登録されるときに、マッピングキーとして使用されます。	管理者が入力	テキスト型
IMSI	移動体通信機器の加入者に付与されている識別番号（スマートデバイスの SIM カードに付与されている番号）を設定します。	管理者が入力	テキスト型
ICCID	Apple 社製のスマートデバイスの SIM カードに付与されている番号を設定します。	管理者が入力	テキスト型
キャリア	スマートデバイスの通信サービスを提供する会社を設定します。	管理者が入力	テキスト型

管理項目	説明	入力方法	データ型
契約電話番号	契約しているスマートデバイスの電話番号を設定します。契約電話番号は、ハードウェア資産情報をインポートするときや、収集された機器情報がハードウェア資産情報に自動で登録されるときに、マッピングキーとして使用されます。	管理者が入力	テキスト型
ホスト識別子	ハードウェア資産情報のインポートで指定されたホスト識別子が表示されます。ハードウェア資産情報のインポート後に管理対象となった機器との同定に使用されます。機器情報と関連づけられたハードウェア資産情報のホスト識別子は「空欄」になります。 機器と資産の同定については、「(2)　機器とハードウェア資産の同定」を参照してください。	管理者が入力	テキスト型

注※1　エージェント導入済みのコンピュータの場合、[利用者情報の入力]画面から入力できます。

注※2　ハードウェア資産情報が機器情報と関連づいている場合、機器情報が更新されると、対応するハードウェア資産情報もあわせて更新されます。

注※3　収集した機器情報を基に、選択項目が自動生成されます。

注※4　契約種別が新規機器を購入する場合に使用する「購入」、「レンタル」、または「リース」の場合だけ表示されます。 詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の機器を購入する流れの説明を参照してください。

ソフトウェアライセンス

管理項目	説明	入力方法	データ型
ライセンス管理番号	ソフトウェアライセンスを一意に判別するための番号を設定します。ソフトウェアライセンスの証書に掲載されている番号や独自に管理しやすいユニークな番号を設定してください。[ライセンス管理番号]は、ソフトウェアライセンス情報をインポートするときに、マッピングキーとして使用します。	管理者が入力	テキスト型
ライセンス名	ソフトウェアライセンスを一覧で管理するための任意の名称を設定します。ライセンスの内容を判別できるような名称にすることをお勧めします。	管理者が入力	テキスト型
ライセンス種類	ソフトウェアライセンスの種別を設定します。	管理者が入力	選択型
ライセンス数	ソフトウェアライセンスの購入数を設定します。	管理者が入力	数値型
保有数	ソフトウェアライセンスの保有数が表示されます。アップグレードライセンスやダウングレードライセンスの場合は、アップグレード後やダウングレード後の保有数が自動的に計算されて表示されます。	－	－
割り当てライセンス数	コンピュータに割り当て済みのライセンス数が表示されます。	－	－
残数	[保有数]から[割り当てライセンス数]を引いた、ソフトウェアライセンスの数が表示されます。	－	－

管理項目	説明	入力方法	データ型
残数	残数がマイナスの場合は、ソフトウェアライセンスが不足して、ライセンス違反となっているおそれがあります。	－	－
アップグレード元ライセンス名	追加するライセンスがアップグレードライセンスの場合に、アップグレード元のソフトウェアライセンスを設定します。	－	－
説明	ソフトウェアライセンスを識別するための情報を設定します。一覧で表示されたときに確認しやすいような情報にすることをお勧めします。	管理者が入力	テキスト型
添付ファイル	資産に関するファイルを設定します。ソフトウェアライセンスの証書などを電子データ化して登録しておくと、ソフトウェアライセンスの詳細情報を参照したいときに資料を探す手間が省けます。	管理者が入力	－
契約会社名	関連づけられた契約情報の契約会社が表示されます。	－	－
契約日	関連づけられた契約情報の契約日が表示されます。	－	－
ライセンス状態	ソフトウェアライセンスの状態を設定します。デフォルトでは、[使用中] または [滅却] を設定できます。	管理者が入力	選択型
予定ライセンス状態	ソフトウェアライセンスの状態を変更する予定がある場合に、変更後の状態を設定します。デフォルトでは、[使用中] または [滅却] を設定できます。	管理者が入力	選択型
変更予定日	ソフトウェアライセンスの状態を変更する予定がある場合に、状態を変更する予定日を設定します。予定日を設定しておくと、予定日に近くなった場合、および予定日になった場合に、そのソフトウェアライセンスに対する運用が必要なことがイベントで通知されます。	管理者が入力	日付型
棚卸日	ソフトウェアライセンスの棚卸を実施した日を設定します。	管理者が入力	日付型
部署	ソフトウェアライセンスを保有している部署を設定します。ソフトウェアライセンスを部署単位で管理しない場合は、設定する必要はありません。	管理者が入力	次のデータ型を指定できます。 • テキスト型 • 選択型 • 階層型
管理ソフトウェア名	ソフトウェアライセンスに対応するソフトウェアを設定します。	管理者が入力	－
メーカー	対応づけられている管理ソフトウェアのメーカーが表示されます。	－	－
登録日時	ソフトウェアライセンス情報が登録された日時が表示されます。	－	－
更新日時	ソフトウェアライセンス情報が更新された日時が表示されます。	－	－

管理ソフトウェア

管理項目	説明	入力方法	データ型
管理ソフトウェア名	ソフトウェアを管理するための名称を設定します。例えば、[インストールソフトウェア名] に「ソフトウェア HOGE 1.0」、「ソフトウェア HOGE 2.0」のように異なるバージョンのソフトウェアを指定した場合、名称を「ソフトウェア HOGE」と登録することで、1 種類のソ	管理者が入力	テキスト型および選択型※

管理項目	説明	入力方法	データ型
管理ソフトウェア名	フトウェアとして管理できます。[管理ソフトウェア名]は、管理ソフトウェア情報をインポートするときに、マッピングキーとして使用します。	管理者が入力	テキスト型および選択型※
説明	ソフトウェアを識別するための情報を設定します。ソフトウェアの内容やインストールソフトウェア情報との対応づけに関する説明などにすることをお勧めします。	管理者が入力	テキスト型
ライセンス種類	関連づけられたソフトウェアライセンス情報のライセンス種類が表示されます。	−	−
保有数	関連づけられたソフトウェアライセンス情報のライセンス数が表示されます。	−	−
ライセンス消費数	管理ソフトウェアがインストールされている機器の総数が表示されます。 OS 種別が「すべて」以外の設定の場合、設定した OS 種別の機器がライセンス消費数のカウント対象になります。	−	−
残数	[保有数]から[ライセンス消費数]を引いた、ソフトウェアライセンスの数が表示されます。 残数がマイナスの場合は、ソフトウェアライセンスが不足して、ライセンス違反となっているおそれがあります。	−	−
割り当てライセンス数	コンピュータに割り当て済みのライセンス数が表示されます。 [割り当てライセンス数]よりも[ライセンス消費数]が多い場合は、利用者が無断でソフトウェアをインストールしているおそれがあります。	−	−
メーカー	ソフトウェアの製造元を設定します。	管理者が入力	テキスト型および選択型※
OS 種別	ソフトウェアのインストール対象となる機器の OS 種別を設定します。OS 種別が「すべて」の場合は、機器の OS 種別を区別しません。	管理者が入力	選択型
登録日時	管理ソフトウェア情報が登録された日時が表示されます。	−	−
更新日時	管理ソフトウェア情報が更新された日時が表示されます。	−	−

注※　収集したソフトウェア情報を基に、選択項目が自動生成されます。

契約

管理項目	説明	入力方法	データ型
契約管理番号	契約書に掲載されている契約番号や独自に管理しやすいユニークな番号を設定してください。[契約管理番号]は、契約情報をインポートするときに、マッピングキーとして使用します。	管理者が入力	テキスト型
契約名	契約を管理するための名称を設定します。契約の内容を判別できる	管理者が入力	テキスト型

管理項目	説明	入力方法	データ型
契約名	ような名称にすることをお勧めします。	管理者が入力	テキスト型
契約種別	契約の種別を設定します。デフォルトでは、[購入]、[リース]、[レンタル]、[保守]、または［サポート］を設定できます。	管理者が入力	選択型
契約期間	契約の期間を設定します。満了日が近づくと定期的に管理者にメール通知されます。	管理者が入力	日付型
説明	契約情報を識別するための情報を設定します。一覧で表示されたときに確認しやすいような情報にすることをお勧めします。	管理者が入力	テキスト型
添付ファイル	契約に関するファイルを設定します。契約書の証書などを電子データ化して登録しておけば、契約の詳細情報を参照したいときに資料を探す手間が省けます。	管理者が入力	－
契約会社名	契約会社の情報を設定します。契約元の連絡先を設定しておくと、契約の更改や次回の見積もり、障害時などに連絡がしやすくなり便利です。	管理者が入力	選択型
契約日	契約会社と契約した日を設定します。契約書に掲載されている契約日を登録します。	管理者が入力	日付型
支払い方法	契約に対する費用の支払い方法を設定します。	管理者が入力	選択型
月額(¥)	契約費用の月額を設定します。	管理者が入力	数値型
総額(¥)	契約費用の総額を設定します。	管理者が入力	数値型
契約状態	契約の状態を設定します。デフォルトでは、[契約中]、[途中解約]または［満了］を設定できます。契約満了日を過ぎても［契約状態］が［満了］または［途中解約］になっていない場合は、期限切れの契約として扱われます。	管理者が入力	選択型
部署	契約対象の資産を保有している部署を設定します。契約を部署単位で管理しない場合は、設定する必要はありません。	管理者が入力	次のデータ型を指定できます。 • テキスト型 • 選択型 • 階層型

管理項目	説明	入力方法	データ型
登録日時	契約情報を登録した日時が表示されます。	−	−
更新日時	契約情報が更新された日時が表示されます。	−	−

関連リンク

- 2.11.7　資産情報のインポート
- (2)　資産管理項目の入力方法
- (1)　資産管理項目のデータ型

(1)　資産管理項目のデータ型

資産管理項目には、次に示すデータ型の種類があります。以降の表中では、凡例を次のとおり表記しています。

（凡例）○：入力できる　×：入力できない

数値型

数値（-2,147,483,647～2,147,483,647）および「-」（ハイフン）だけを入力できる形式です。資産に対する数値を管理したい場合は、このデータ型を選択してください。なお、末尾に入力された半角スペースは無視されます。

日付型

日付を入力するための形式です。資産に対する日付を管理したい場合は、このデータ型を選択してください。

選択型

特定の選択項目から値を選択できる形式です。この形式を選択した場合は、選択項目を作成する必要があります。選択項目は、256 文字以内の任意の文字列で作成できます。入力される値が限定できる情報を管理したい場合は、このデータ型を選択してください。

テキスト型

256 文字以内の任意の文字列を指定できる形式です。任意の値を入力して管理したい場合は、このデータ型を選択してください。入力できる文字を制限することもできます。なお、末尾に入力された半角スペースは無視されます。

階層型

［資産情報と機器情報の共通管理項目］の［部署］と［設置場所］だけに設定できるデータ型です。40 階層までの階層構成の選択項目を設定できます。選択項目に指定できるのは、256 文字以内の「/」を除く文字列です。ここで編集した階層構成は、資産画面や機器画面などのメニューエリアに反映されます。

なお、階層型の選択項目は、その選択項目までのパスが 512 文字以内になるように指定してください。このとき、パスの先頭、末尾、および各選択項目間には、区切りを示す 1 文字をカウントする必要があ

ります。例えば、「[東京支社] − [営業部] − [1 課]」の 3 階層の選択項目を作成した場合、パスの文字数は 13 文字（/東京支社/営業部/1 課/）となります。

> **ヒント**
>
> [部署] と [設置場所] は、選択型またはテキスト型で階層構成の情報を入力することもできます。この場合、「/本社/開発部/開発 2 課/」のように「/」で選択項目を区切って入力します。なお、先頭と末尾の「/」は省略できます。階層構成の情報は、512 文字以内で入力してください。先頭と末尾の「/」を省略する場合は、510 文字以内で入力してください。

テキスト型の場合に設定できる文字制限

テキスト型の場合に設定できる文字制限の種類を次の表に示します。ここで示した種類のほかに、任意の設定もできます。

全般的な文字制限

文字	文字制限						
	すべて入力可	英字だけ	英数字だけ	半角文字	全角英字だけ	全角英数字だけ	全角数字だけ
英字（大文字）	○	○	○	○	×	×	×
英字（小文字）	○	○	○	○	×	×	×
数字	○	×	○	○	×	×	×
ピリオド	○	×	×	○	×	×	×
ハイフン	○	×	×	○	×	×	×
プラス	○	×	×	○	×	×	×
アットマーク	○	×	×	○	×	×	×
空白	○	×	×	○	×	×	×
その他の記号	○	×	×	○	×	×	×
半角カナ	○	×	×	○	×	×	×
全角英字（大文字）	○	×	×	×	○	○	×
全角英字（小文字）	○	×	×	×	○	○	×
全角数字	○	×	×	×	×	○	○
全角空白	○	×	×	×	×	×	×

文字	文字制限						
	すべて入力可	英字だけ	英数字だけ	半角文字	全角英字だけ	全角英数字だけ	全角数字だけ
英数記号以外の文字	○	×	×	×	×	×	×

人名の文字制限

文字	文字制限		
	人名 1	人名 2（全角入力、全角空白区切り）	人名 3（全角入力、空白なし）
英字（大文字）	○	×	×
英字（小文字）	○	×	×
数字	○	×	×
ピリオド	○	×	×
ハイフン	○	×	×
プラス	○	×	×
アットマーク	○	×	×
空白	○	×	×
その他の記号	○	×	×
半角カナ	○	×	×
全角英字（大文字）	×	○	○
全角英字（小文字）	×	○	○
全角数字	×	○	○
全角空白	×	○	×
英数記号以外の文字	○	○	○

電話番号とメールアドレスの文字制限

文字	文字制限			
	電話番号 1（ハイフン区切り）	電話番号 2（ハイフン区切り、国際電話）	電話番号 3（ハイフンなし）	メールアドレス
英字（大文字）	×	×	×	○
英字（小文字）	×	×	×	○
数字	○	○	○	○
ピリオド	×	×	×	○

文字	文字制限			
	電話番号 1（ハイフン区切り）	電話番号 2（ハイフン区切り、国際電話）	電話番号 3（ハイフンなし）	メールアドレス
ハイフン	○	○	×	○
プラス	×	○	×	○
アットマーク	×	×	×	○
空白	×	×	×	×
その他の記号	×	×	×	○
半角カナ	×	×	×	×
全角英字（大文字）	×	×	×	×
全角英字（小文字）	×	×	×	×
全角数字	×	×	×	×
全角空白	×	×	×	×
英数記号以外の文字	×	×	×	×

関連リンク

- 2.11.1　資産情報の管理項目一覧
- (3)　カスタマイズできる資産管理項目の種類

(2)　資産管理項目の入力方法

カスタマイズできる資産管理項目には、次の 4 つの入力方法を設定できます。

管理者が入力

システム管理者が画面上で直接情報を入力するか、CSV ファイルのインポートによって情報を入力します。

利用者が入力

エージェント導入済みのコンピュータに［利用者情報の入力］画面を表示し、利用者によって入力された情報を取得します。

利用者に作業が発生しますが、管理者が利用者固有の情報を調査して入力する手間が省けます。また、取得した情報に応じて部署および設置場所のグループが作成されるため、グルーピングの作業を自動化できます。

Active Directory から取得

Active Directory と連携している場合に、Active Directory 上でコンピュータのプロパティとして管理している情報を取得します。

Active Directory で管理している情報を利用して、機器や資産を管理できるようになります。

レジストリから取得

指定したレジストリ項目の情報を収集します。利用者の環境に依存する情報を管理できます。

> **重要**
>
> Active Directory から取得できる情報は、テキスト型だけです。

関連リンク

- (3)　カスタマイズできる資産管理項目の種類

(3)　カスタマイズできる資産管理項目の種類

設定画面の［資産管理］－［資産管理項目の設定］画面で設定できる資産管理項目の種類、データ型の種類、および入力方法の種類について説明します。

資産管理項目の種類

資産情報と機器情報の共通管理項目

資産画面のハードウェア資産情報と、機器画面の機器情報で共通となる管理項目を設定します。［資産情報と機器情報の共通管理項目］の資産管理項目はシステムであらかじめ設定されているため、追加および削除はできません。

ハードウェア資産情報の追加管理項目

資産画面のハードウェア資産情報の資産管理項目を設定します。次の資産管理項目は削除できません。

- システムであらかじめ設定されている、［資産状態］と［機器種別］
- リモートインストールマネージャで管理している、あて先グループおよび ID の自動メンテナンスの条件に指定している資産管理項目

また、追加管理項目の値を次の条件に指定している場合は、その値の編集および削除はできません。

- フィルタ条件
- あて先グループおよび ID の自動メンテナンスの条件

単数サーバ構成の場合、各項目の表示順は作成順になります。複数サーバ構成の場合、各項目の表示順は UTF-8 の文字コード順になります。

ソフトウェアライセンス情報の追加管理項目

資産画面のソフトウェアライセンス情報の資産管理項目を設定します。［ライセンス状態］と［ライセンス種類］はシステムであらかじめ設定されているため、削除できません。

各項目の表示順は作成順になります。

契約情報の追加管理項目

資産画面の契約情報の資産管理項目を設定します。［契約状態］と［契約種別］はシステムであらかじめ設定されているため、削除できません。

各項目の表示順は作成順になります。

資産管理項目によって編集できる項目が異なります。編集できる項目を次の表に示します。

資産管理項目		項目名	入力方法	説明	データ型
資産情報と機器情報の共通管理項目※	部署	×	○	○	○
	設置場所	×	○	○	○
	利用者名	×	○	○	△1
	アカウント	×	○	○	△1
	メールアドレス	×	○	○	△1
	電話番号	×	○	○	△1
システム固有の資産管理項目※	資産状態	×	×	×	△2
	機器種別	×	×	×	△2
	ライセンス状態	×	×	×	△2
	ライセンス種類	×	×	×	△2
	契約状態	×	×	×	△2
	契約種別	×	×	×	△2
追加した資産管理項目		○	△3	○	○

（凡例）

○：編集できます。

△1：データ型は［テキスト型］以外には変更できませんが、入力できる文字は編集できます。

△2：データ型は［選択型］以外には変更できませんが、選択項目は追加できます。

△3：ソフトウェアライセンス情報と契約情報の追加管理項目は、入力方法が［管理者が入力］だけになります。

×：編集できません。

注※　システムであらかじめ設定されている資産管理項目のため、削除できません。

ヒント

設定画面の［資産管理］－［資産管理項目の設定］画面に設定した内容は、エージェント設定の［エージェント基本動作］の［管理用サーバからの情報を定期的に取得する］に設定した間隔でエージェントに反映され、利用者情報の入力を利用者に促すバルーンヒントが表示されます。

ヒント

［資産情報と機器情報の共通管理項目］の次に示す項目で「利用者が入力」を設定している場合、メニューエリアから該当する項目のグループを変更または削除すると、利用者情報の入力を利用者に促すバルーンヒントが表示されます。

- 部署
- 設置場所

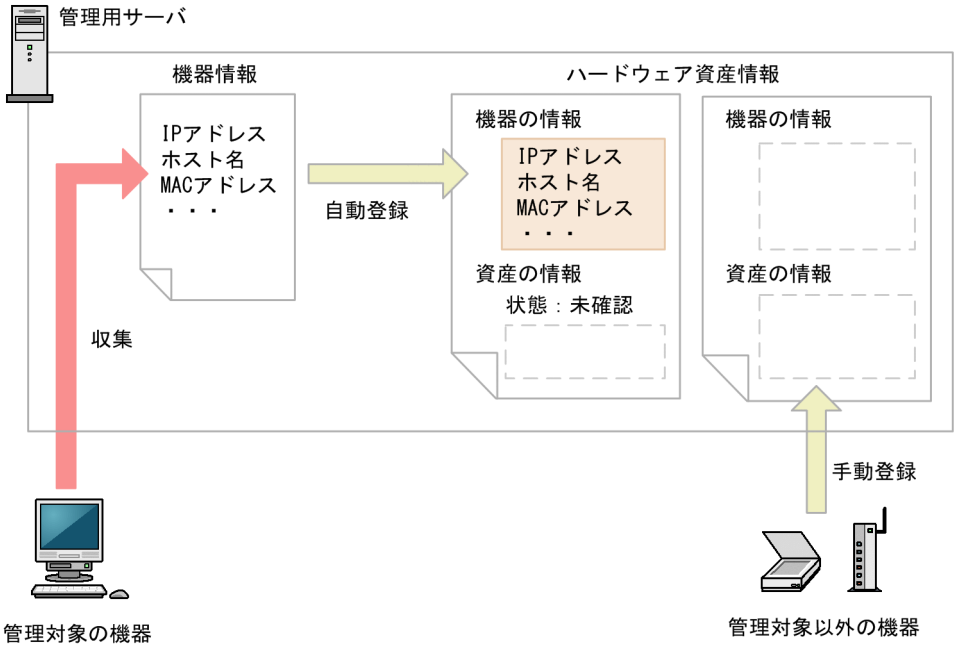
関連リンク

- 2.11.1　資産情報の管理項目一覧
- (1)　資産管理項目のデータ型
- (2)　資産管理項目の入力方法

2.11.2　ハードウェア資産情報の管理

資産画面の［ハードウェア資産］画面で、ハードウェア資産情報を登録して管理できます。

機器を管理対象にすると、機器から収集された情報が機器画面の［機器情報］画面に表示されます。さらに、機器の情報は資産画面の［ハードウェア資産］画面にも新規のハードウェア資産情報として自動的に登録されます。ハードウェア資産情報が登録される流れを次の図に示します。



自動的に登録されたハードウェア資産情報は、［資産状態］が「未確認」となっています。また、機器から収集できた情報だけが登録されています。このため、機器から自動的には収集されない［資産管理番号］、［資産状態］（運用中、在庫など）、利用者情報などを、ハードウェア資産情報にあとから登録する必要があります。

ヒント

機器から収集された情報は、機器情報が更新されるとハードウェア資産情報もあわせて更新されます。

すでに管理台帳を利用してハードウェア資産を管理している場合、今まで管理していた情報を JP1/IT Desktop Management 2 にインポートして利用できます。手持ちの管理台帳がない場合は、自動的に登録されたハードウェア資産情報をメンテナンスしてください。

管理対象の機器以外のハードウェア資産情報を管理したい場合は、ハードウェア資産情報を新規に登録してください。

また、ハードウェア資産情報は、運用に応じてメンテナンスする必要があります。

ハードウェア資産情報は、ほかのハードウェア情報と関連づけて管理したり、対応する契約情報を設定したりできます。

ヒント

ioutils importassetassoc コマンドでも、ハードウェア資産情報と機器情報、ほかのハードウェア資産情報、および契約情報との関連づけができます。

ヒント

1 つのハードウェア資産に複数の機器を関連づけた場合、複数の機器のうちの 1 台を代表の機器として設定します。その代表の機器から収集したハードウェア情報がハードウェア資産情報として資産画面の［ハードウェア資産］画面などに表示されます。

ヒント

代表の機器として設定した機器を削除したり、代表の機器として設定した機器をほかのハードウェア資産情報に関連づけたりした場合、代表の機器は次のように変更されます。

- 代表の機器として設定した機器を削除する時にハードウェア資産に関連づいているほかの機器を代表の機器に変更します。
- 代表の機器として設定した機器をほかのハードウェア資産に関連づける変更をした場合は、当該ハードウェア資産にすでに関連づいている機器が代表の機器となります。

どちらの場合も、削除する機器や関連づけを変更する機器のほかに 2 台以上の機器が関連づいているときには、最終更新日時が最も新しい機器が代表の機器となります。これは機器の自動メンテナンスで重複機器や不稼働機器が自動削除される場合も同様です。

関連リンク

- (6)　ほかの情報と関連づけたハードウェア資産情報の管理
- 2.11.1　資産情報の管理項目一覧

(1)　機器とハードウェア資産の関連づけ

ハードウェア資産管理では、機器情報とハードウェア資産情報を関連づけて管理します。 機器が管理対象になると、自動的にハードウェア資産情報が登録されて機器情報と関連づきますが、機器が管理対象になっていなかったり、ハードウェア資産情報だけを登録していたりすると、機器情報とハードウェア資産情報が関連づかない場合があります。

各契機に対応する、機器とハードウェア資産の関連づけの詳細を次の表に示します。

契機	説明
エージェント導入済みの機器が管理用サーバに接続されたとき	対象の機器の機器情報が登録されて、同時にハードウェア資産情報が自動的に登録されます。ハードウェア資産情報は、機器情報と関連づけられます。
探索で機器が発見されたとき（発見されたコンピュータを自動的に管理対象にするように設定した場合）	対象の機器の機器情報が登録されて、同時にハードウェア資産情報が自動的に登録されます。ハードウェア資産情報は、機器情報と関連づけられます。 なお、［機器種別］が［PC］以外の場合は、自動的に管理対象にはならないため、機器情報とハードウェア資産情報は登録されません。このため、機器情報とハードウェア資産情報は関連づけられません。
探索で機器が発見されたとき（発見されたコンピュータを自動的に管理対象にしないように設定した場合）	機器情報およびハードウェア資産情報は登録されません。
CSV ファイルをハードウェア資産としてインポートしたとき	ハードウェア資産情報が登録されますが、機器情報は登録されないため、機器情報とハードウェア資産情報の関連づけもされません。ただし、機器情報とハードウェア資産情報がすでに関連づいていれば、インポートしたハードウェア資産情報は機器情報と関連づいたままとなります。
USB デバイスを登録したとき	［機器種別］が［USB デバイス］のハードウェア資産情報が登録されますが、機器情報は登録されないため、機器情報とハードウェア資産情報は関連づけられません。
手動で資産画面にハードウェア資産を追加したとき	ハードウェア資産情報が登録されますが、機器情報は登録されないため、機器情報とハードウェア資産情報の関連づけもされません。ただし、機器情報とハードウェア資産情報がすでに関連づいていれば、インポートしたハードウェア資産情報は機器情報と関連づいたままとなります。

また、機器とハードウェア資産が関連づいている場合、機器情報やハードウェア資産情報の状態を変更したり情報を削除したりすることで、関連づけが解除されることがあります。

機器とハードウェア資産が関連づいている場合の、各契機に対応する、関連づけの変化を次の表に示します。

契機	説明
ハードウェア資産の［資産状態］を［滅却］にしたとき	ハードウェア資産情報の［機器情報］が削除され、関連づけが解除されます。また、機器画面の機器一覧から対象の機器が削除されます。 なお、対象の機器にエージェントがインストールされていると、次回の探索を契機に、機器が再び管理対象になります。この場合、ハードウェア資産情報の［資産状態］が［滅却］になっていると、ハードウェア資産情報が新規で登録され、二重で登録されてしまいます。［資産状態］を［滅却］にする場合は、対象の機器をネットワークから切断するか、エージェントをアンインストールすることをお勧めします。また、ハードウェア資産情報の［資産状態］が［滅却］以外になっていると、関連づけが再登録されます。
設定画面の［管理対象機器］画面で対象の機器を削除したとき	ハードウェア資産情報の［機器情報］が削除され、関連づけが解除されます。また、機器画面の機器一覧から対象の機器が削除されます。 なお、エージェントをインストール済みの機器が再び管理対象になった場合の動作は、ハードウェア資産情報の［資産状態］を［滅却］にしたときと同じです。 また、代表の機器として設定されている機器を削除した場合は、当該ハードウェア資産に関連づいているほかの機器（2 台以上の機器が関連づいている場合には最終更新日時が最も新しい機器）が代表の機器として設定されます。
設定画面の［管理対象機器］画面で対象の機器を［除外対象］に設定したとき	機器画面の機器一覧から対象の機器が削除されます。ハードウェア資産情報の［機器情報］は削除されません。 なお、エージェントをインストール済みの機器の場合は、手動で管理対象に戻すと機器一覧に対象の機器が再登録されます。
ハードウェア資産を削除したとき	ハードウェア資産は、［資産状態］が［未確認］または［滅却］の場合だけ削除できます。ハードウェア資産を削除した場合の、機器の動作を次に示します。 ［資産状態］が［未確認］の場合 　機器画面の［機器情報］画面から対象の機器が削除されます。 ［資産状態］が［滅却］の場合 　機器画面の［機器情報］画面から対象の機器がすでに削除されています。 ［資産状態］が［滅却］になっているハードウェア資産を削除時には、ハードウェア資産情報の削除に連動してシステム構成情報は削除されません。

(2)　機器とハードウェア資産の同定

機器が管理対象になると、自動的にハードウェア資産情報が登録され、機器情報と関連づけられます。管理対象にした機器に対応するハードウェア資産情報がすでに登録されている場合は、登録された機器情報との引き当て（同定）が実行されます。同定された機器情報とハードウェア資産情報は関連づけられます。同定されたハードウェア資産情報に、別の機器情報がすでに関連づいている場合、ハードウェア資産情報に設定されている代表の機器は変更されません。

機器情報とハードウェア資産情報の同定には、次の表に示す項目のうち、どれか 1 つが利用されます。

優先順位	同定するときに比較する項目
1	ホスト識別子※1
2	IMEI※2

優先順位	同定するときに比較する項目
3	シリアルナンバー※3
4	ホスト名
5	MAC アドレス
6	契約電話番号※2
7	IP アドレス

注※1　資産情報としてインポートした CSV ファイルにホスト識別子の値が記述されていた場合、機器情報とハードウェア資産情報を同定したあと、別の機器と再び同定されないようにするため、ホスト識別子は「空欄」になります。

注※2　MDM システムと連携してスマートデバイスを管理する場合に、利用されます。

注※3　BIOS 情報のシリアルナンバーです。

同定の際は、優先順位の高い項目の値が比較されます。優先順位の高い項目の値が取得されていない場合、または無効な値の場合は、次に優先順位の高い項目の値が比較されます。

項目の値が一致した場合は、その項目で機器情報とハードウェア資産情報が同定され、ハードウェア資産情報に関連する機器情報が追加されます。項目の値が一致しない場合は、ハードウェア資産情報が新規に登録されます。

重要

あらかじめ機器情報だけが登録されている状態で、あとから対応するハードウェア資産情報を登録しても、機器情報とハードウェア資産情報は同定されません。このような場合は、手動で関連づけてください。

ヒント

ioutils importasset コマンドでハードウェア資産情報と機器の関連づけを設定できます。

(3)　利用者が入力した情報の収集

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場合、利用者のコンピュータに［利用者情報の入力］画面を表示させて、利用者が入力した情報でハードウェア資産情報を自動的に更新できます。

利用者が入力した情報を収集することで、システム管理者がハードウェア資産情報をメンテナンスする手間を省けます。例えば、定期的に利用者側で最新情報を入力してもらうように運用しておくと、大人数の部署異動があっても、システム管理者側で情報をメンテナンスすることなく異動後の利用者情報を把握できます。

重要

管理対象のコンピュータが共有型 VDI の仮想コンピュータの場合、利用者が入力した情報の収集はできません。

利用者が入力できる項目を次に示します。

- 部署
- 設置場所
- 利用者名
- アカウント
- メールアドレス
- 電話番号
- 任意に追加した管理項目

利用者情報を収集するためには、設定画面の［資産管理］－［資産管理項目の設定］画面で、利用者に入力してもらう資産管理項目をあらかじめ設定しておきます。［利用者情報の入力］画面を表示するには、エージェント設定の［利用者への通知設定］で、利用者入力画面が表示されるように設定する必要があります。

また、利用者が情報の入力を開始できるタイミングを、設定画面の［資産管理］－［資産管理項目の設定］画面でシステム管理者が指定することもできます。 複数の項目の設定変更が終わったあとに［利用者情報の入力］画面を表示できるため、期首の職制変更に合わせて情報を更新したいときに便利です。

重要

利用者のコンピュータに導入されているエージェントのバージョンが JP1/IT Desktop Management 10-01 以前または Job Management Partner 1/IT Desktop Management 10-01 以前の場合、入力開始の日時を指定しても、項目の設定を変更するたびに［利用者情報の入力］画面が表示されます。入力開始の日時を指定する場合は、利用者のコンピュータに JP1/IT Desktop Management 10-02 以降または Job Management Partner 1/IT Desktop Management 10-10 以降のバージョンのエージェントを導入してください。

オンライン管理のコンピュータの場合、［利用者情報の入力］画面を一定の間隔で定期的に利用者のコンピュータに表示できます。定期的に［利用者情報の入力］画面を表示させる場合は、エージェント設定の［利用者への通知設定］で、利用者入力画面が表示されるように設定し、設定画面の［資産管理項目の設定］画面では入力開始の日時を指定しないでください。入力開始の日時を指定すると、［利用者情報の入力］画面が定期的に表示されなくなります。オフライン管理のコンピュータの場合は、getinv.vbs コマンドまたはsetsecpolicy.vbs コマンドを実行して機器情報を収集するときに［利用者情報の入力］画面を表示できます。

入力開始の日時を指定している場合で、指定した日時を経過していないときは、利用者のコンピュータで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］－［利用者情報の入力］を選択しても、メッセージだけが表示されて、情報を入力できません。また、オフライン管理のコンピュータでgetinv.vbsコマンドまたはsetsecpolicy.vbsコマンドを実行しても、［利用者情報の入力］画面は表示されません。

(4) 資産状態の管理

ハードウェア資産情報には、その資産が運用中なのか在庫なのかといった資産の状態を設定できます。資産状態を設定することで、所有している資産を一覧で把握できるだけでなく、利用状況も把握できるようになります。また、滅却済みの資産についても、所有している資産とあわせて確認できます。

資産状態には次の種類があります。

未確認

資産情報は登録されていますが、資産として管理されていないことを意味します。機器が管理対象になった際に自動的に登録されたハードウェア資産情報は、この資産状態が設定されます。「未確認」の資産がある場合は、その資産の現品を確認して資産状態を含む資産情報を設定してください。

在庫

資産が利用されていない状態であることを意味します。

運用中

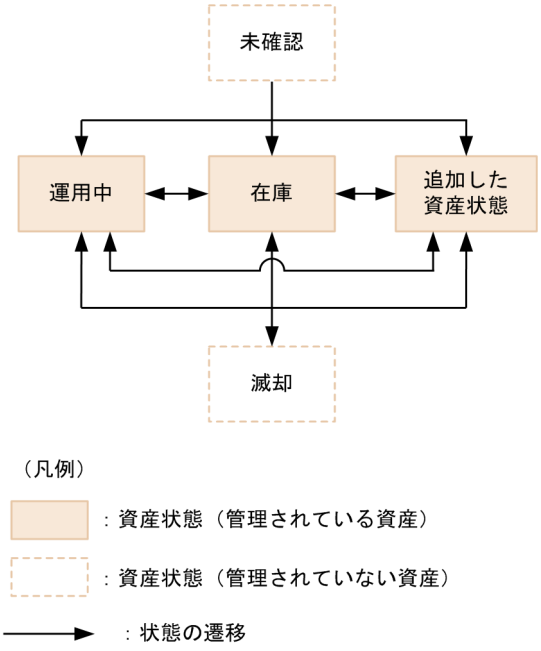
資産が運用中（使用中）であることを意味します。

滅却

資産が滅却済みであることを意味します。

このほかに、管理者が任意の項目を追加できます。項目はデフォルトの項目とは別に100種類まで登録できます。

資産状態の遷移を次の図に示します。



利用状況を把握するため、実態に合わせて資産状態を変更します。

資産を新規登録したときは「未確認」として登録されます。「未確認」の資産を確認して、実態に合わせて「運用中」、「在庫」、または「追加した資産状態」に変更してください。また、「未確認」では資産として登録していないため、関連づけなどができません。関連づけなどを実施する場合は、「未確認」以外に変更する必要があります。

管理が不要になった資産を「滅却」に変更した場合は、「運用中」、「在庫」、または「追加した資産状態」に戻すこともできます。

予定資産状態の管理

将来変更する予定の資産状態を設定できます。予定資産状態を設定することで、資産管理の作業予定を把握できます。

例えば、「在庫」の資産に対して、予定資産状態「滅却」と変更予定日を設定しておくことで、その資産を滅却処理する予定日を把握できるようになります。

設定できる予定資産状態の種類は、資産状態と同じです。

> **重要**
>
> 予定資産状態は、変更予定日を過ぎても自動的には変更されません。変更予定日を目安に、ハードウェア資産そのものの状態が変更されたことを確認してから、管理者が手動で資産状態を変更する必要があります。資産状態を予定資産状態に設定した状態に変更すると、予定資産状態と変更予定日の設定値がクリアされます。

ヒント

予定資産状態を登録すると、ダイジェストレポートで対象の資産を確認できます。また、日刊、週刊、月間のダイジェストレポートの集計が完了すると、それぞれにメール設定した宛先にメール通知がされます。

(5) 棚卸日の更新方法

ハードウェア資産情報およびソフトウェアライセンス情報の［棚卸日］を更新できます。［棚卸日］を更新すると、棚卸で確認できなかった資産がないかどうかを確認できます。

手動で棚卸日を更新する

［棚卸日］を更新する資産情報を選択して、［棚卸日］を更新します。手もとにある少数の資産を、個別に棚卸する場合にお勧めします。

CSV ファイルを基に棚卸日を一括更新する

［資産管理番号］または［ライセンス管理番号］が記載された CSV ファイルを利用して、［棚卸日］を一括更新します。各資産情報の［棚卸日］は同じ日付になります。この方法は、バーコードリーダーを利用して棚卸する場合にお勧めします。バーコードリーダーで読み取った資産管理番号またはライセンス管理番号の一覧を、CSV ファイルで出力してください。

棚卸日の自動更新を設定する

ハードウェア資産情報の場合、棚卸日を自動更新するように設定できます。JP1/IT Desktop Management 2 は、機器のネットワーク接続、機器の利用者の入力、オフライン管理のコンピュータから取得した機器情報の通知で機器の存在を確認します。機器の存在を確認できたら、棚卸日が自動更新されます。棚卸の手間を省きたい場合にお勧めします。

重要

ハードウェア資産情報の場合、［棚卸日の自動更新の設定］ダイアログで［利用者による［利用者情報の入力］画面の入力が完了した日を、棚卸日とする］を選択している場合でも、機器画面の［機器情報］－［機器一覧］画面で、［操作メニュー］から［最新の情報を取得する］を選択したとき、棚卸日が自動更新されます。

ヒント

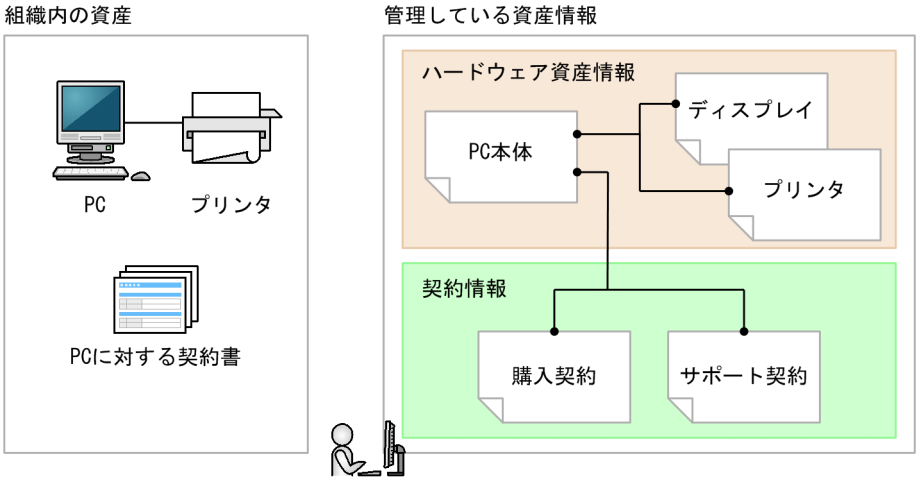
ハードウェア資産情報およびソフトウェアライセンス情報をインポートして、［棚卸日］を一括更新することもできます。この場合は、各資産情報の［棚卸日］に異なった日付を設定できます。

(6) ほかの情報と関連づけたハードウェア資産情報の管理

ハードウェア資産情報は、ほかのハードウェア資産情報と関連づけて管理したり、対応する契約情報を設定したりできます。

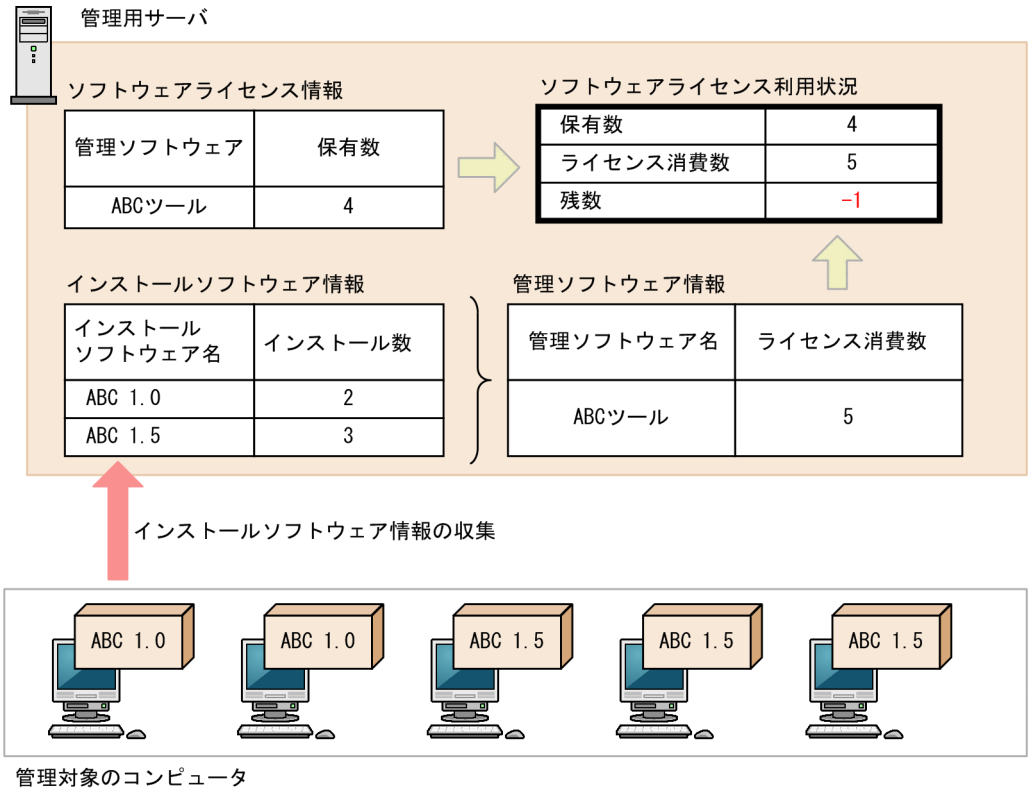
ほかのハードウェア資産情報との関連づけを設定することで、各コンピュータの本体、ディスプレイ、および周辺機器をセットで管理できます。

ハードウェア資産に対応する契約を設定することで、どのコンピュータに対してどの契約を結んでいるのかを把握できるようになります。また、レポートでハードウェア資産に掛かる運用コストを確認できるようになります。



2.11.3　ソフトウェアライセンスの利用状況の把握

ソフトウェアライセンスの管理を始めるには、JP1/IT Desktop Management 2 に管理ソフトウェア情報とソフトウェアライセンス情報を登録する必要があります。管理ソフトウェア情報とソフトウェアライセンス情報を登録することで、ソフトウェアライセンスの利用状況を把握できるようになります。ソフトウェアライセンスの利用数を確認して、ソフトウェアライセンスの過不足を把握する流れを次の図に示します。



管理対象のコンピュータ

ソフトウェアライセンス情報には、所有しているソフトウェアライセンスの情報と対応するソフトウェア名（管理ソフトウェア）を設定します。また、ソフトウェアライセンス情報にソフトウェアライセンスを割り当てる（利用許可する）コンピュータを登録できます。ソフトウェアライセンス情報は、資産画面の［ソフトウェアライセンス］画面で設定します。

管理ソフトウェア情報には、ライセンス消費数をカウントするソフトウェア情報を指定します。複数のソフトウェア情報を指定して、1 種類のソフトウェアとして管理することもできます。これによって、ソフトウェアのインストール数が管理ソフトウェアごとに集計されます。管理ソフトウェア情報は、資産画面の［管理ソフトウェア］画面で設定します。

こうしてソフトウェアライセンス情報と管理ソフトウェア情報を登録すると、資産画面の［ソフトウェアライセンス状況］画面で管理ソフトウェアごとのソフトウェアライセンスの利用状況をまとめて確認できるようになります。例えば、ソフトウェアライセンスを割り当てたコンピュータの台数（割り当てライセンス数）を確認することで、未許可でソフトウェアをインストールしているコンピュータや、利用許可しているのにソフトウェアをインストールしていないコンピュータを把握できます。また、管理ソフトウェアごとのライセンスの保有数や残数が集計され、ソフトウェアライセンスの過不足を把握できます。ソフトウェアライセンスの利用状況は、［ソフトウェアライセンス状況］画面のソフトウェアライセンス状況一覧をエクスポートすることで、CSV ファイルに出力できます。

同名のソフトウェアでインストール先の OS によってライセンス金額やライセンス形態が異なる場合でも、インストール先の OS 種別ごとにライセンス消費数を集計できます。OS 種別は管理ソフトウェア情報に登録します。

なお、[ソフトウェアライセンス状況]画面では、部署ごとにソフトウェアライセンスの利用状況を確認できます。 管理ソフトウェア名およびソフトウェアライセンス情報に指定した値と、ソフトウェアライセンスの利用実態が次のような場合を例に、[ソフトウェアライセンス状況]画面に表示される値を示します。

管理ソフトウェア名およびソフトウェアライセンス情報の指定例と、ソフトウェアライセンスの利用実態

管理ソフトウェア名	ソフトウェアライセンス情報			ソフトウェアライセンスの利用実態	
	部署	保有数	割り当てライセンス数	インストール数	インストール済みコンピュータが所属する部署
ABC ソフトウェア	総務部	10	10	12	総務部
	営業部	10	10	10	営業部
	開発部	5	10	5	開発部
	開発部/A 課	5	10	3	開発部/A 課
	開発部/B 課	5	3	3	開発部/B 課
	－	－	－	3	開発部/C 課
	－	－	－	1	人事部
XYZ ソフトウェア	－	20	2	1	開発部/A 課
				1	開発部/B 課

（凡例）－：設定していない

[ソフトウェアライセンス状況]画面に表示される情報

管理ソフトウェア名	部署	保有数	ライセンス消費数	残数	割り当てライセンス数	説明
ABC ソフトウェア	(全部署累計) ※1	35	37	-2	43	全部署（総務部、営業部、開発部、および人事部）の累計値が表示されます。
	総務部	10	12	-2	10	総務部だけの値が表示されます。
	営業部	10	10	0	10	営業部だけの値が表示されます。
	開発部※2	15	14	1	23	開発部だけの値（開発部、開発部/A 課、開発部/B 課、および開発部/C 課の累計値）が表示されます。
	開発部/A 課※2	5	3	2	10	開発部/A 課だけの値が表示されます。
	開発部/B 課※2	5	3	2	3	開発部/B 課だけの値が表示されます。

管理ソフトウェア名	部署	保有数	ライセンス消費数	残数	割り当てライセンス数	説明
ABC ソフトウェア	開発部/C 課※2	－	3	－	0	開発部/C 課だけの値が表示されます。 ソフトウェアライセンス情報の部署情報に自部署（開発部/C 課）を設定していなくても、部署情報に上位部署（開発部）を設定している場合は、保有数および残数が「－」（ハイフン）で表示されます。
	人事部	0	1	-1	0	人事部だけの値が表示されます。 ソフトウェアライセンス情報の部署情報に自部署（人事部）も上位部署も設定していない場合は、保有数および割り当てライセンス数が「0」で表示されます。残数はマイナスで表示されます。
XYZ ソフトウェア	(全部署累計) ※1	20	2	18	2	全部署（総務部、営業部、開発部、および人事部）の累計値が表示されます。 ソフトウェアライセンス情報に部署を設定していないソフトウェアの保有数および割り当てライセンス数も加算されます。
	開発部※2	－	2	－	2	開発部だけの値（開発部、開発部/A 課、および開発部/B 課の累計値）が表示されます。 ソフトウェアライセンス情報に部署を設定していない場合は、保有数および残数が「－」（ハイフン）で表示されます。
	開発部/A 課※2	－	1	－	1	開発部/A 課だけの値が表示されます。 ソフトウェアライセンス情報に部署を設定していない場合は、保有数および残数が「－」（ハイフン）で表示されます。
	開発部/B 課※2	－	1	－	1	開発部/B 課だけの値が表示されます。 ソフトウェアライセンス情報に部署を設定していない場合

管理ソフトウェア名	部署	保有数	ライセンス消費数	残数	割り当てライセンス数	説明
XYZ ソフトウェア	開発部/B 課※2	－	1	－	1	は、保有数および残数が「－」（ハイフン）で表示されます。

（凡例）－：該当なし

注　メニューエリアで［ソフトウェアライセンス状況一覧］をクリックした場合は、表中の全項目が表示されます。

注※1　メニューエリアで［(全部署累計)］をクリックした場合に表示される項目です。

注※2　メニューエリアで［開発部］をクリックした場合に表示される項目です。

重要

- JP1/IT Desktop Management 09-51 および Job Management Partner 1/IT Desktop Management 10-01 で、ライセンス消費数のカウント方法が変更になりました。バージョンアップした場合、ライセンス消費数が変わることがあります。

  ライセンス消費数には、管理ソフトウェアに対応するインストールソフトウェアのインストール数が表示されます。JP1/IT Desktop Management 09-51 および Job Management Partner 1/IT Desktop Management 10-01 では、同じ管理ソフトウェアに対応するソフトウェアが 1 台のコンピュータに複数インストールされている場合、それぞれをカウントしていました。JP1/IT Desktop Management 09-51 以降および Job Management Partner 1/IT Desktop Management 10-01 以降は、同じ管理ソフトウェアに対応するソフトウェアが 1 台のコンピュータに複数インストールされている場合、1 ライセンスの消費としてカウントされるようになります。
- Windows ストアアプリは、実際に購入したライセンス数と JP1/IT Desktop Management 2 で検知するライセンス数が異なる場合があります。JP1/IT Desktop Management 2 では、該当ソフトウェアがインストールされている機器の台数をライセンス数として検知しますが、Windows ストアアプリは機器ごとではなくアカウントごとにライセンスが割り当てられるためです。

(1)　管理ソフトウェア情報の管理

資産画面の［管理ソフトウェア］画面で、管理ソフトウェア情報を登録して管理できます。

管理ソフトウェア情報を登録するには、手動で登録する方法と、管理ソフトウェア情報の CSV ファイルを作成しインポートする方法があります。

対応するソフトウェアの追加や変更があった場合は、管理ソフトウェア情報をメンテナンスして最新の状態を保つようにします。

なお、管理ソフトウェア情報をエクスポートして、編集した CSV ファイルをインポートすることで一括更新することもできます。また、管理が不要になった管理ソフトウェア情報は削除することもできます。

管理ソフトウェア情報を登録すると、管理ソフトウェアごとのソフトウェアライセンスの利用状況を、資産画面の［ソフトウェアライセンス状況］画面で確認できるようになります。

(2) ライセンス状態の管理

ソフトウェアライセンス情報には、ライセンスが使用中なのか滅却済みなのかといった［ライセンス状態］を設定できます。［ライセンス状態］を設定することで、所有しているソフトウェアライセンスを一覧で把握できるだけでなく、滅却済みのソフトウェアライセンスをあわせて把握できるようになります。

ライセンス状態には次の種類があります。

使用中
　ソフトウェアライセンスが使用中であることを意味します。

滅却
　ソフトウェアライセンスが滅却済みであることを意味します。

このほかに、管理者が任意の項目を追加できます。項目はデフォルトの項目とは別に 100 種類まで登録できます。

予定ライセンス状態の管理

将来変更する予定のライセンス状態を設定できます。予定ライセンス状態を設定することで、ライセンス管理の作業予定を把握できます。設定できる状態の項目は、ライセンス状態の項目と同じです。

例えば、「使用中」のソフトウェアライセンスに対して、予定ライセンス状態「滅却」と変更予定日を設定しておくことで、そのソフトウェアライセンスを滅却処理する予定日を把握できるようになります。

設定できる予定ライセンス状態の種類は、ライセンス状態と同じです。

なお、予定ライセンス状態は、変更予定日を過ぎても自動的には変更されません。変更予定日を目安に、管理者がライセンス状態を変更する必要があります。ライセンス状態を予定ライセンス状態の状態に変更すると、予定ライセンス状態と変更予定日の設定値がクリアされます。

(3) ソフトウェアライセンス情報の管理

資産画面の［ソフトウェアライセンス］画面で、ソフトウェアライセンスの保有数、対象となる契約情報、部署などの情報を登録して管理できます。

ソフトウェアライセンスを管理するかどうか検討する際は、ソフトウェア種別を判断基準にできます。例えば、ソフトウェア種別が有償ソフトウェアのソフトウェアライセンスだけを管理することもできます。ソフトウェア種別は、SAMAC 辞書の情報をオフライン更新すると、資産画面の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、または機器画面のソフトウェア一覧に表示されます。

管理が必要と判断したソフトウェアライセンスは、割り当て先の変更、ソフトウェアの滅却、対象となる契約の追加や削除などの情報をメンテナンスして、ソフトウェアライセンス情報を最新の状態に保つようにします。

ソフトウェアライセンス情報を登録するには、手動で登録する方法と、ソフトウェアライセンス情報をいったんエクスポートして、編集した CSV ファイルを作成しインポートする方法があります。

また、管理が不要になったソフトウェアライセンス情報は削除することもできます。

関連リンク

- (5)　ソフトウェアライセンスの割り当て管理

(4)　棚卸日の更新方法

ハードウェア資産情報およびソフトウェアライセンス情報の［棚卸日］を更新できます。［棚卸日］を更新すると、棚卸で確認できなかった資産がないかどうかを確認できます。

手動で棚卸日を更新する

［棚卸日］を更新する資産情報を選択して、［棚卸日］を更新します。手もとにある少数の資産を、個別に棚卸する場合にお勧めします。

CSV ファイルを基に棚卸日を一括更新する

［資産管理番号］または［ライセンス管理番号］が記載された CSV ファイルを利用して、［棚卸日］を一括更新します。各資産情報の［棚卸日］は同じ日付になります。この方法は、バーコードリーダーを利用して棚卸する場合にお勧めします。バーコードリーダーで読み取った資産管理番号またはライセンス管理番号の一覧を、CSV ファイルで出力してください。

棚卸日の自動更新を設定する

ハードウェア資産情報の場合、棚卸日を自動更新するように設定できます。JP1/IT Desktop Management 2 は、機器のネットワーク接続、機器の利用者の入力、オフライン管理のコンピュータから取得した機器情報の通知で機器の存在を確認します。機器の存在を確認できたら、棚卸日が自動更新されます。棚卸の手間を省きたい場合にお勧めします。

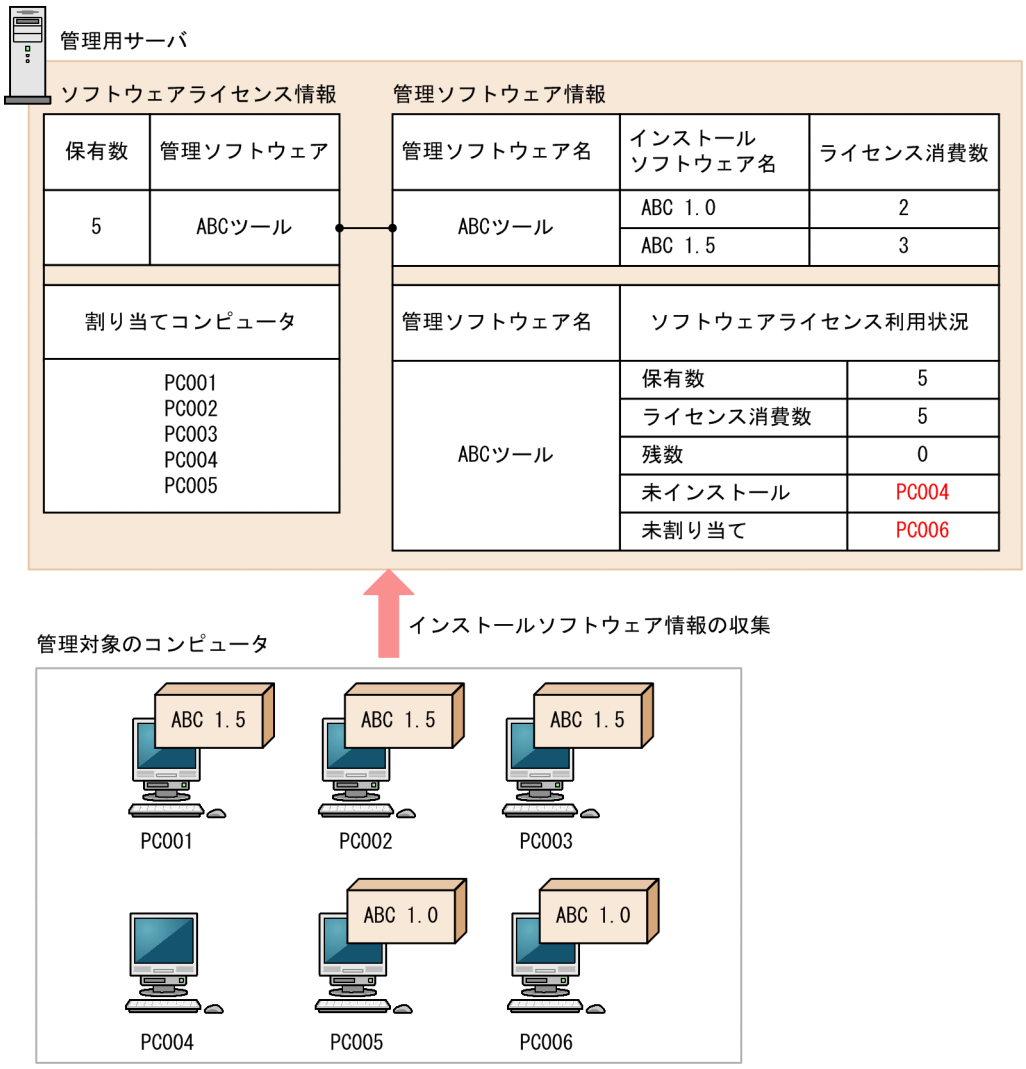
> **重要**
>
> ハードウェア資産情報の場合、［棚卸日の自動更新の設定］ダイアログで［利用者による［利用者情報の入力］画面の入力が完了した日を、棚卸日とする］を選択している場合でも、機器画面の［機器情報］－［機器一覧］画面で、［操作メニュー］から［最新の情報を取得する］を選択したとき、棚卸日が自動更新されます。

> **ヒント**
>
> ハードウェア資産情報およびソフトウェアライセンス情報をインポートして、［棚卸日］を一括更新することもできます。この場合は、各資産情報の［棚卸日］に異なった日付を設定できます。

(5)　ソフトウェアライセンスの割り当て管理

コンピュータにソフトウェアライセンスを割り当てて管理することで、未許可でソフトウェアをインストールしているコンピュータや、利用許可しているのに利用されていないソフトウェアライセンスを把握できるようになります。

コンピュータにソフトウェアライセンスを割り当てて管理するためには、ソフトウェアライセンス情報に割り当てるコンピュータを指定します。そのあと、管理ソフトウェア情報を登録する際に、割り当て先を指定したソフトウェアライセンス情報を関連づけます。これによって、ソフトウェアがインストールされているコンピュータの情報と、ソフトウェアライセンスの割り当て先が比較され、割り当てどおりにソフトウェアライセンスが利用されているかどうかを確認できるようになります。コンピュータにソフトウェアライセンスを割り当てて管理する仕組みを、次の図に示します。



ソフトウェアが割り当てどおりに使われているかどうかは、資産画面の［管理ソフトウェア］画面の［インストール済みコンピュータ］タブおよび［割り当て済みコンピュータ］タブで確認できます。

［インストール済みコンピュータ］タブでは、管理ソフトウェア情報に指定したソフトウェアがインストールされているコンピュータが表示されます。このタブで、［未割り当てコンピュータだけを表示する］を

チェックしてソフトウェアライセンスを割り当てていないコンピュータを表示すると、未許可でソフトウェアをインストールしているコンピュータを把握できます。

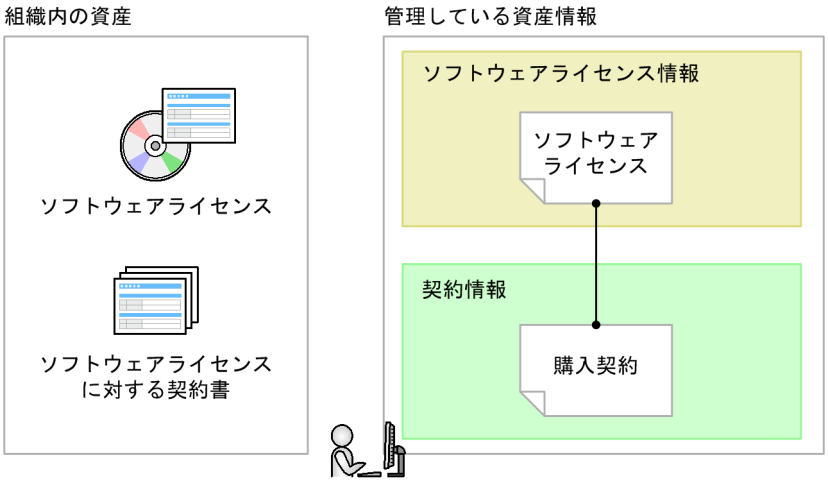
[割り当て済みコンピュータ] タブでは、ソフトウェアライセンスを割り当てたコンピュータが表示されます。このタブで、[未インストールのコンピュータだけを表示する] をチェックしてソフトウェアライセンスを割り当てているのにインストールしていないコンピュータを表示すると、利用されていないソフトウェアライセンスを把握できます。

> **ヒント**
>
> ioutils importassetassoc コマンドでもソフトウェアライセンスの割り当てができます。

(6) 契約情報と関連づけたソフトウェアライセンス情報の管理

ソフトウェアライセンス情報は、対応する契約情報を設定できます。

ソフトウェアライセンスに対応する契約を設定することで、どのソフトウェアライセンスに対してどの契約を結んでいるのかを把握できるようになります。また、レポートでソフトウェアライセンスに掛かる運用コストを確認できるようになります。



ソフトウェアライセンス情報と契約情報は n 対 1 で対応づけられます。

> **ヒント**
>
> ioutils importassetassoc コマンドでもソフトウェアライセンス情報と契約情報の対応づけができます。

(7) アップグレードライセンスとダウングレードライセンスの管理

ソフトウェアのアップグレードやダウングレードが発生する場合、それらのソフトウェアライセンス情報を登録して管理できます。

アップグレードライセンスとダウングレードライセンスを管理する場合、ソフトウェアライセンス情報の登録方法が通常と異なります。

アップグレードライセンスを登録する場合

ソフトウェアをアップグレードする場合、［アップグレード元ライセンス名］にアップグレード元のソフトウェアライセンス情報を登録します。

例えば、「ソフトウェア A」の「Ver 2」のソフトウェアライセンスを 10 個保有していて、「Ver 3」のアップグレードライセンスを 7 個購入した場合、「Ver 3」のソフトウェアライセンス情報を登録するときに、［アップグレード元ライセンス名］に「Ver 2」のソフトウェアライセンス情報を指定します。これによって、「Ver 2」のライセンス数は重複してカウントされないよう 10 から 3 に自動的に変更され、アップグレード後のライセンス数を正しく管理できるようになります。

ヒント

ioutils importassetassoc コマンドでもアップグレードライセンスの登録ができます。

ダウングレードライセンスを登録する場合

ソフトウェアをダウングレードする場合、ダウングレード先の管理ソフトウェア情報に、ダウングレードできるソフトウェアライセンス情報を登録します。

例えば、「ソフトウェア A」の「Ver 2」のソフトウェアライセンスを 5 個、「Ver 3」のソフトウェアライセンスを 10 個保有していて、「Ver 3」のソフトウェアライセンス 6 個を「Ver 2」にダウングレードする場合、「Ver 3」のソフトウェアライセンス情報を通常のソフトウェアライセンス 4 個と、ダウングレード用ライセンス 6 個に分けて登録します。ダウングレード用のソフトウェアライセンス情報には、「Ver 2」の管理ソフトウェア情報を指定します。これによって、「Ver 3」は 4 個、「Ver 2」はダウングレードライセンスと合わせて 11 個保有しているようになり、ダウングレード後のライセンス数を正しく管理できるようになります。

ヒント

ioutils importassetassoc コマンドでもダウングレードライセンスの登録ができます。

2.11.4 契約情報の管理

資産画面の［契約］画面で契約情報を登録して管理できます。

契約情報を登録するには、各契約情報を手動で追加する方法と、契約情報の CSV ファイルを作成しインポートする方法があります。

契約の満了や中止、契約対象の資産の変更、契約期間の延長などがあった場合は、契約情報をメンテナンスして最新の状態を保つようにします。

なお、契約情報をエクスポートして、編集した CSV ファイルをインポートすることで一括更新することもできます。

管理が不要になった契約情報は削除することもできます。

(1) 契約状態の管理

契約情報には、その契約が有効（契約期間内）か無効（契約終了）かの［契約状態］を設定できます。［契約状態］を設定することで、締結している契約の状況を一覧で把握できます。また、終了した契約についても、期間内の契約とあわせて確認できます。

契約状態には次の種類があります。

契約中
: 契約が契約期間内であることを意味します。契約期間が過ぎている場合にこの契約状態のままだと、期限切れの契約として扱われます。

途中解約
: 契約が終了していることを意味します。契約期間内に途中解約した場合は、この契約状態を設定します。

満了
: 契約が終了していることを意味します。

このほかに、管理者が任意の項目を追加できます。項目はデフォルトの項目とは別に 100 種類まで登録できます。

> **ヒント**
>
> 契約状態と契約期間を登録すると、ダイジェストレポートで期限切れの近い契約を確認できます。

(2) ハードウェア資産とソフトウェアライセンスに掛かる費用の把握

ハードウェア資産またはソフトウェアライセンスの運用に掛かる費用をレポートから確認できます。資産に掛かる費用は、［資産詳細レポート］の次のレポートで確認できます。

- ［ハードウェア資産の費用］レポート
- ［ソフトウェアライセンスの費用］レポート
- ［その他の費用］レポート

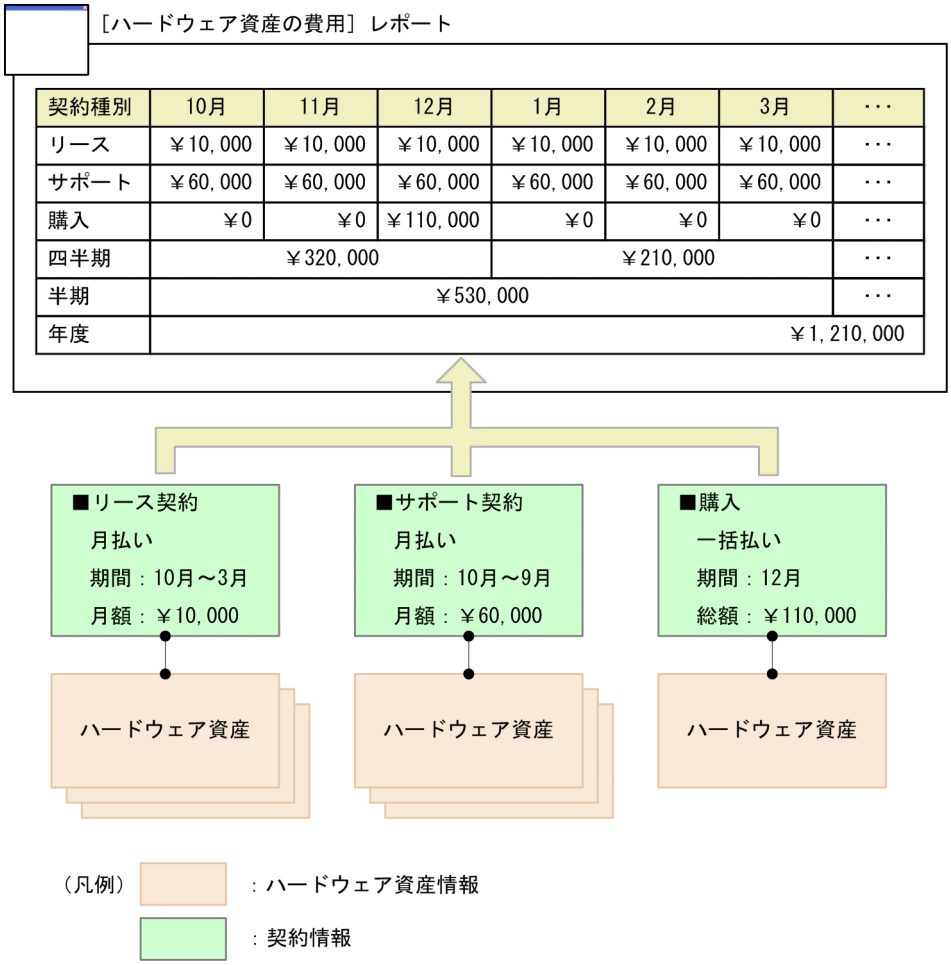
これらのレポートでは、契約種別ごとに月単位、四半期単位、半期単位、年度単位で契約費用を確認できます。

なお、費用を確認するためには、契約情報に費用を設定して、ハードウェア資産情報またはソフトウェアライセンス情報に関連づけておく必要があります。

ヒント

ハードウェア資産情報またはソフトウェアライセンス情報に関連づけていない契約の費用は、［その他の費用］レポートで確認できます。

契約情報を関連づけて費用を把握する概念を次の図に示します。



上の図では、ハードウェア資産と関連づいたリース契約に、10 月～3 月の契約期間の月払いが設定されています。このため、契約期間の 6 か月間、月額¥10,000 が計上されます。同様に、サポート契約も契約期間の 12 か月間、月額¥60,000 が計上されます。購入は一括払いが設定されているため、12 月に¥110,000 が計上されます。

このようにして算出された毎月の金額を集計し、四半期単位、半期単位、年度単位の金額が計上されます。

ヒント

金額は契約単位に集計されます。契約情報に関連づいたハードウェア資産の台数には依存しません。

ヒント

ioutils importassetassoc コマンドでも契約情報とハードウェア資産情報およびソフトウェアライセンス情報の関連づけができます。

(3) ハードウェア資産の費用の計算方法

契約情報とハードウェア資産情報を関連づけると、契約費用が計算されます。ハードウェア資産の費用は、レポート画面の［資産詳細レポート］－［ハードウェア資産の費用］レポートに表示されます。

契約費用の計算方法について、次に示します。

契約種別ごとの費用

各月の費用総額が契約種別ごとに計算されます。この各月の費用を使用して、四半期、半期、年度の累計費用が計算されます。月払いは「月額」、一括払いは「総額」から各月の費用を割り出します。年度の開始月は、設定画面の［レポート］－［保存期間と開始日の設定］画面で設定した値が使用されます。［ハードウェア資産の費用］レポートを表示した日を含む 12 か月分が表示されます。

契約種別ごとに次のような条件に従って、費用が計算されます。

なお、ここでは契約種別が「XXX」の費用を計算する場合について示します。「XXX」には、次の契約種別が入ります。

- リース
- レンタル
- 保守
- サポート
- 購入
- 管理者が追加した契約種別

支払方法	計算方法
月払い	次の条件をすべて満たす契約情報について、「月額」を累計します。 • ［契約種別］が「XXX」になっている。 • ［支払い方法］が「月払い」になっている。 • ［契約対象のハードウェア資産］にハードウェア資産情報が関連づけられている。 • 指定した月に費用発生日が含まれる。 なお、「月払い」の費用発生日は、［契約期間］の契約開始日を基準として［契約期間］が終了するまで 1 か月ごとに出現します。 ［契約期間］が 2011/4/10～2011/6/10 の場合は、費用発生日は、2011/4/10、2011/5/10、2011/6/10 です。そのため、指定した月が 2011 年 4 月、2011 年 5 月、2011 年 6 月の場合に、費用が発生します。
一括払い	次の条件をすべて満たす契約情報について、「総額」を累計します。

支払方法	計算方法
一括払い	• ［契約種別］が「XXX」になっている。 • ［支払い方法］が「一括払い」になっている。 • ［契約対象のハードウェア資産］にハードウェア資産情報が関連づけられている。 • 指定した月に費用発生日が含まれる。 なお、「一括払い」の費用発生日は、「契約日」です。

エクスポート

集計したハードウェア資産の費用は、CSV ファイルに出力できます。出力される CSV ファイルの形式は次のとおりです。

- 「レポート名」、「リスト名」、「作成日時」、「通貨単位」、「集計期間」は、テキスト文字列を「”」（ダブルクォーテーション）なしで出力する。
- 上記以外のデータ部分は、「”」（ダブルクォーテーション）付きで出力する。
- 空白カラムは、「,」（コンマ）区切りだけ出力する。

CSV ファイルの出力例を次に示します。

```
レポート名:資産詳細レポート - ハードウェア資産の費用
リスト名:契約種別ごとの内訳
作成日時:2011年4月22日(金) PM 07時50分20秒 GMT+09:00
通貨単位:(¥)
集計期間:2011

"契約種別","4 月","5 月","6 月","7 月","8 月","9 月","10 月","11 月","12 月","1 月","2 月","3 月"
"リース","0","0","0","300000","300000","300000","300000","300000","300000","300000","300000","300000"
"レンタル","0","0","0","0","0","0","0","0","0","0","0","0"
"保守","50000","50000","50000","50000","50000","50000","20000","20000","20000","20000","20000","20000"
"サポート","0","0","0","0","0","0","0","0","0","0","0","0"
"購入","0","0","600000","0","0","0","0","0","0","0","0","0"
```

なお、デフォルトの契約種別に加えて、カスタマイズした契約種別数分のデータが出力されます。

(4)　ソフトウェアライセンスの費用の計算方法

契約情報とソフトウェアライセンス情報を関連づけると、契約費用が計算されます。ソフトウェアライセンスの費用は、レポート画面の［資産詳細レポート］－［ソフトウェアライセンスの費用］レポートに表示されます。

契約費用の計算方法について、次に示します。

契約種別ごとの費用

各月の費用総額が契約種別ごとに計算されます。この各月の「月額」または「総額」を使用して、四半期、半期、年度の累計費用が計算されます。 年度の開始月は、設定画面の［レポート］－［保存期間と開始日の設定］画面で設定した値が使用されます。年度は、［ソフトウェアライセンスの費用］レポートを表示した日を含む 12 か月分が表示されます。

契約種別ごとに次のような条件に従って、費用が計算されます。

なお、ここでは契約種別が「XXX」の費用を計算する場合について示します。「XXX」には、次の契約種別が入ります。

- リース
- レンタル
- 保守
- サポート
- 購入
- 管理者が追加した契約種別

支払方法	計算方法
月払い	次の条件をすべて満たす契約情報について、「月額」を累計します。 • ［契約種別］が「XXX」になっている。 • ［支払い方法］が「月払い」になっている。 • ［契約対象のソフトウェアライセンス］にソフトウェアライセンス情報が関連づけられている。 • 指定した月に費用発生日が含まれる。 なお、「月払い」の費用発生日は、［契約期間］の契約開始日を基準として［契約期間］が終了するまで 1 か月ごとに出現します。 ［契約期間］が 2011/4/10～2011/6/10 の場合は、費用発生日は、2011/4/10、2011/5/10、2011/6/10 です。そのため、指定した月が 2011 年 4 月、2011 年 5 月、2011 年 6 月の場合に、費用が発生します。
一括払い	次の条件をすべて満たす契約情報について、「総額」を累計します。 • ［契約種別］が「XXX」になっている。 • ［支払い方法］が「一括払い」になっている。 • ［契約対象のソフトウェアライセンス］にソフトウェアライセンス情報が関連づけられている。 • 指定した月に費用発生日が含まれる。 なお、「一括払い」の費用発生日は、「契約日」です。

エクスポート

集計したソフトウェアライセンスの費用は、CSV ファイルに出力できます。出力される CSV ファイルの形式は次のとおりです。

- 「レポート名」、「リスト名」、「作成日時」、「通貨単位」、「集計期間」は、テキスト文字列を「”」（ダブルクォーテーション）なしで出力する。
- 上記以外のデータ部分は、「”」（ダブルクォーテーション）付きで出力する。
- 空白カラムは、「,」（コンマ）区切りだけ出力する。

CSV ファイルの出力例を次に示します。

```
レポート名:資産詳細レポート - ソフトウェアライセンスの費用
リスト名:契約種別ごとの内訳
作成日時:2011年4月22日(金) PM 07時52分10秒 GMT+09:00
通貨単位:(¥)
集計期間:2011

"契約種別","4 月","5 月","6 月","7 月","8 月","9 月","10 月","11 月","12 月","1 月","2 月","3 月"
"リース","0","0","0","0","0","0","0","0","0","0","0","0"
"レンタル","0","0","0","0","0","0","0","0","0","0","0","0"
"保守","0","0","0","0","0","0","0","0","0","0","0","0"
"サポート","0","0","0","0","0","0","0","0","0","0","0","0"
"購入","50000","50000","50000","50000","50000","50000","50000","50000","50000","50000","0","0"
```

なお、デフォルトの契約種別に加えて、カスタマイズした契約種別数分のデータが出力されます。

(5) 契約の期限切れの通知

契約情報の［契約期間］に設定された契約終了日を基に、契約の期限切れをメールで通知できます。

期限切れの通知には、ダイジェストレポートの送付の機能を使用します。ダイジェストレポートの送付先は、設定画面の［レポート］－［ダイジェストレポートの設定］画面で設定できます。

メールでは、期限切れの契約情報の数が通知されます。期限切れと見なされる契約情報の条件を次に示します。

- ［契約状態］が「満了」または「途中解約」以外である。
- 通知日が契約終了日を過ぎている。

期限切れの契約情報について詳細が知りたい場合は、メール本文のリンクをクリックしてください。リンクをクリックすると、レポート画面が表示されます。レポート画面の［ダイジェストレポート］画面で、期限切れの契約情報のリンクをクリックすると、資産画面に遷移して該当する契約情報の詳細を確認できます。

ヒント

契約期限は、［3 か月以内に期限が切れる契約］パネルでも確認できます。

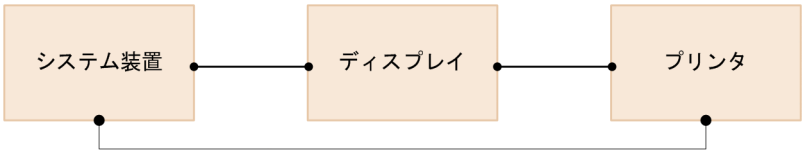
2.11.5 資産情報の関連づけ

複数の資産情報を関連づけて管理できます。資産同士を関連づけることで、例えば、各コンピュータに接続されている周辺機器を把握したり、ソフトウェアライセンスのサポート契約に掛かっている費用を把握したりできます。

ハードウェア資産情報の関連づけ

複数のハードウェア資産情報を関連づけて管理できます。複数の機器をまとめて管理できます。

複数のハードウェア資産情報を関連づけた場合の例を次に示します。



（凡例）　：ハードウェア資産情報

ヒント

ハードウェア資産の関連づけを変更する場合は、インフォメーションエリア下部のタブにある［変更］ボタンでできます。［操作］メニューからの変更は、複数の資産を変更する場合に使用します。

ヒント

ioutils importassetassoc コマンドでも複数のハードウェア資産情報の関連づけができます。

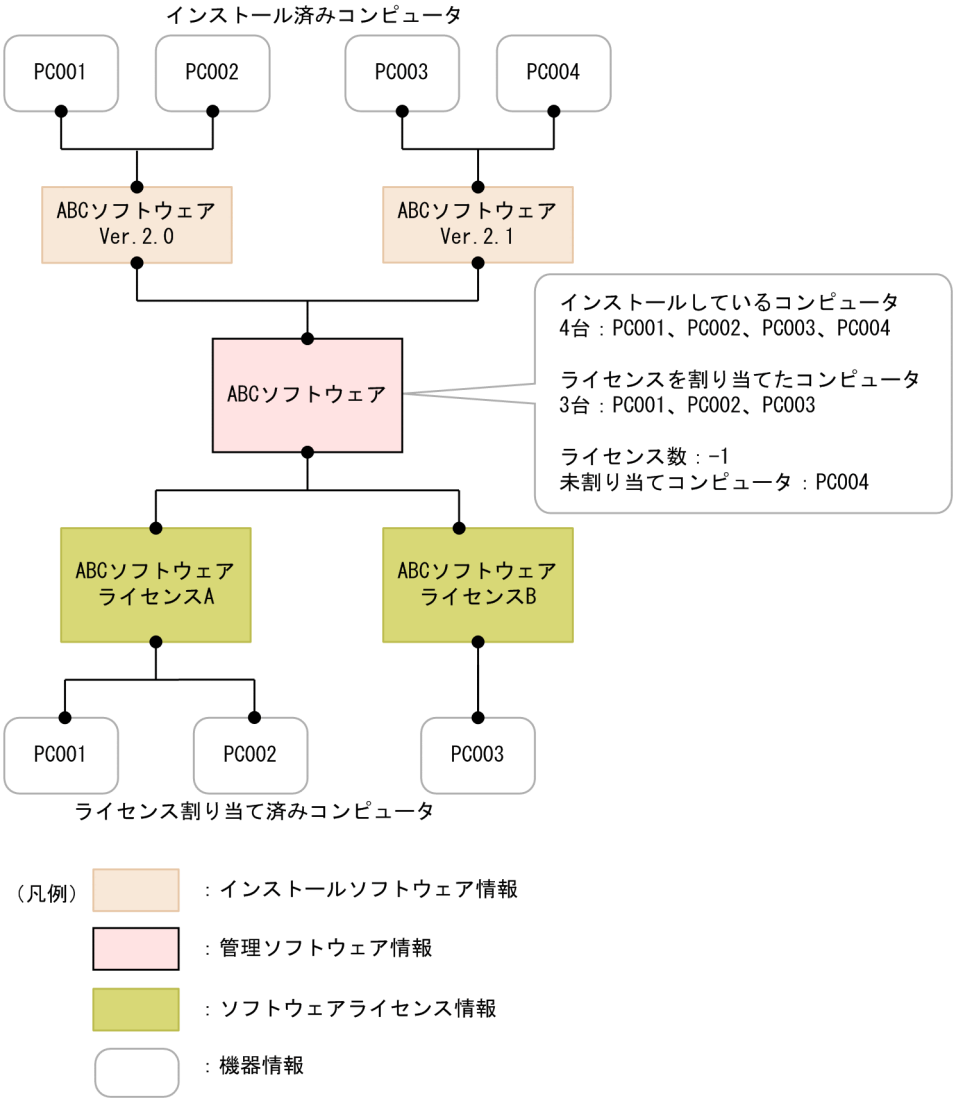
ソフトウェアライセンス情報、管理ソフトウェア情報の関連づけ

ソフトウェアライセンスの利用状況を管理する場合、ソフトウェアライセンス情報と管理ソフトウェア情報を関連づけて管理できます。

管理ソフトウェア情報を、機器から収集したインストールソフトウェア情報と関連づけることで、管理ソフトウェアのライセンス消費数を把握できます。また、管理ソフトウェア情報は、複数のインストールソフトウェア情報を関連づけることもできます。これによって、ボリュームライセンスやバージョンが異なるソフトウェアライセンスを、管理ソフトウェア単位にまとめて管理できます。

ソフトウェアライセンス情報には、ソフトウェアライセンスを割り当てる機器を関連づけられます。これによって、管理ソフトウェア情報で集計されたインストールの実態と比較して、ソフトウェアライセンスが割り当てどおりに利用されているかを把握できるようになります。

ソフトウェアライセンスを機器に割り当てて利用状況を管理する場合の例を次に示します。



ヒント

ioutils importassetassoc コマンドでもソフトウェアライセンス情報と管理ソフトウェア情報の関連づけができます。

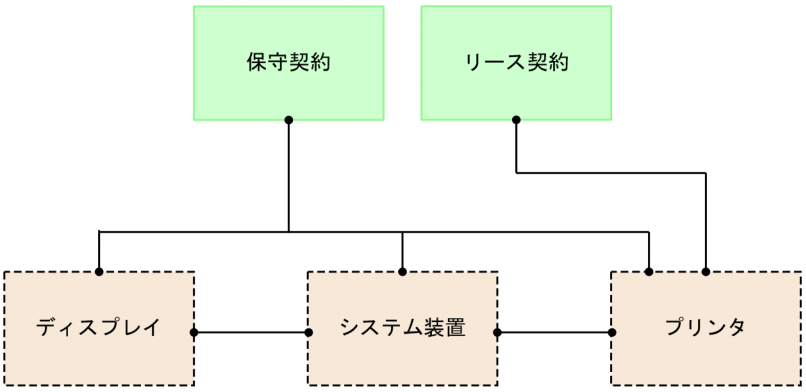
契約情報の関連づけ

契約情報をハードウェア資産情報またはソフトウェアライセンス情報に関連づけて管理できます。例えば、コンピュータのハードウェア資産情報に対して保守契約の契約情報を関連づけて管理しておけば、コンピュータが故障したときに対応する保守契約の情報を素早く把握して、対処できます。

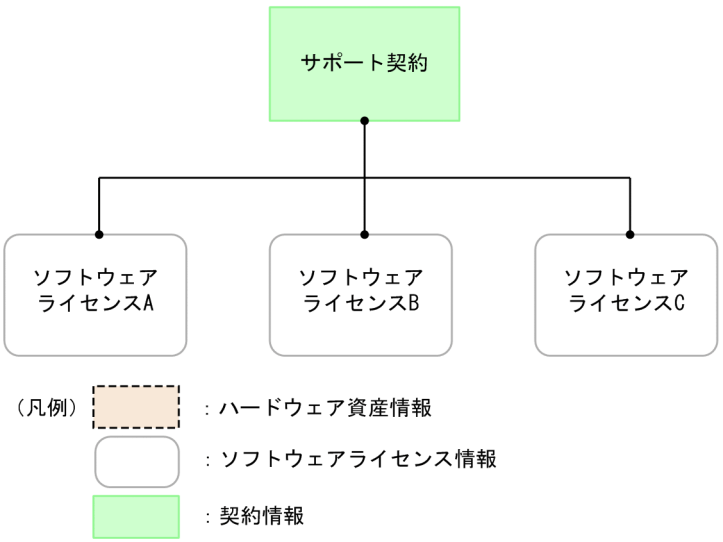
また、契約情報に費用を設定しておくと、ハードウェア資産やソフトウェアライセンスに掛かる費用を把握できます。

ハードウェア資産情報およびソフトウェアライセンス情報に契約情報を関連づけた場合の例を次に示します。

ハードウェア資産情報と契約情報の関連づけ



ソフトウェアライセンス情報と契約情報の関連づけ



ハードウェア資産情報の場合は、契約形態に合わせて、契約情報とハードウェア資産情報を N 対 N で関連づけられます。

ソフトウェアライセンス情報の場合は、ソフトウェアライセンスごとに契約を管理するため、契約情報とソフトウェアライセンス情報を 1 対 N で関連づけます。

ヒント

契約情報とハードウェア資産情報またはソフトウェアライセンス情報を関連づける場合、［契約の追加］画面または［契約情報の編集］画面の［契約対象］で指定します。

ヒント

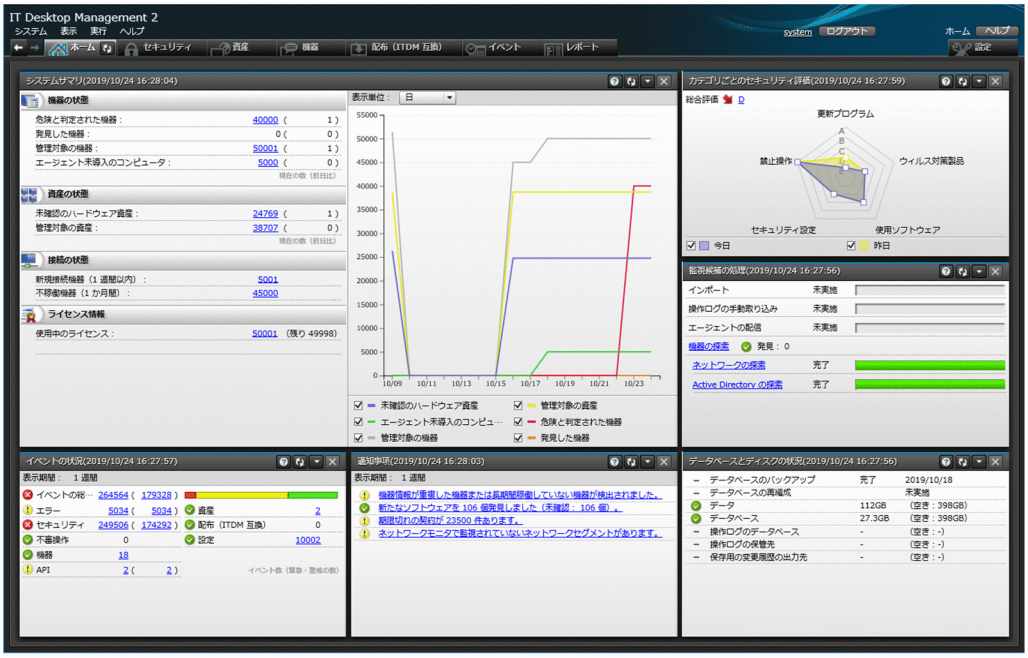
ioutils importassetassoc コマンドでも契約情報とハードウェア資産情報またはソフトウェアライセンス情報の関連づけができます。

2.11.6　資産情報の確認方法

ホーム画面のパネルで確認する

ホーム画面では［システムサマリ］パネルの［未確認のハードウェア資産］から、資産状態が「未確認」のハードウェア資産の台数（新規に登録され、情報が未入力の台数）を確認できます。台数のリンクをクリックすると、資産画面の［ハードウェア資産］画面が表示され、ハードウェア資産情報を確認できます。

なお、［管理対象の資産］からは、資産状態が「未確認」以外のハードウェア資産の総数を確認できます。



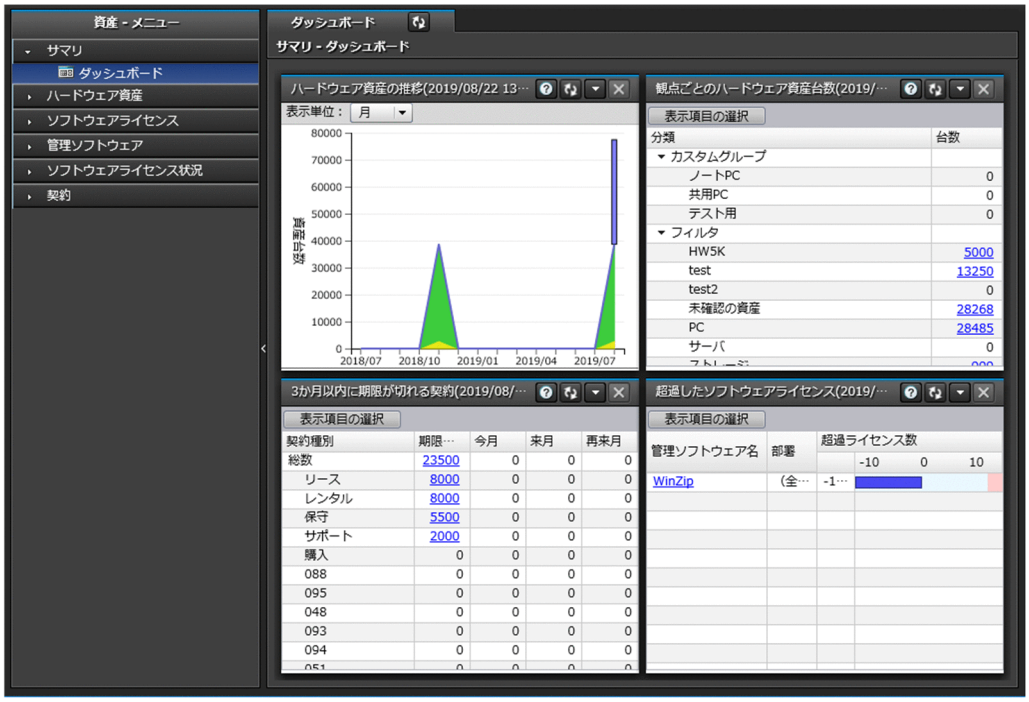
資産画面で確認する

資産画面では、［サマリ］画面、［ハードウェア資産］画面、［ソフトウェアライセンス］画面、［管理ソフトウェア］画面、［ソフトウェアライセンス状況］画面、［契約］画面で資産の状況を確認できます。資産画面は、組織内の資産情報を登録することで、資産台帳として利用できます。

> **ヒント**
>
> ［サマリ］画面以外の各画面では、フィルタを利用して条件に一致する項目を抽出して参照できます。また、メニューエリアからは製品があらかじめ用意しているフィルタも利用できます。フィルタの利用方法については、「2.17　フィルタの利用」を参照してください。

［サマリ］画面で確認する

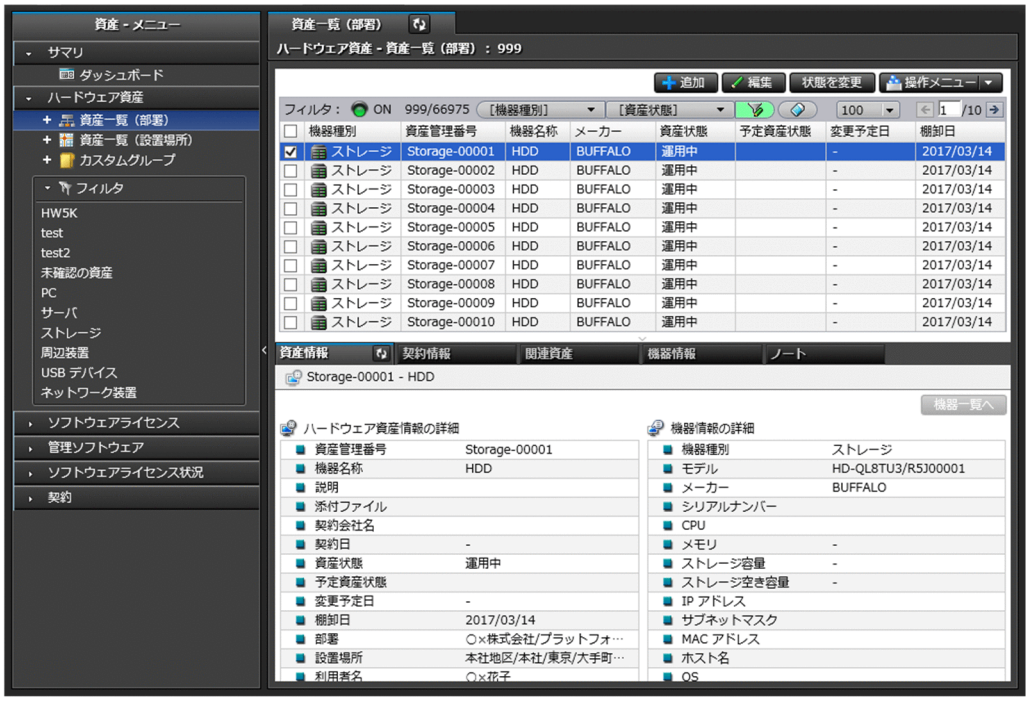
資産の概況を確認できます。各パネルのリンクをクリックすると、詳細を確認できる画面が表示されるので、資産管理に関する作業の入口として利用できます。



［ハードウェア資産］画面で確認する

組織内のハードウェア資産を登録して、状況を一覧で確認できます。FD ドライブ、DVD ドライブなどの周辺装置や USB デバイスもこの画面で管理します。

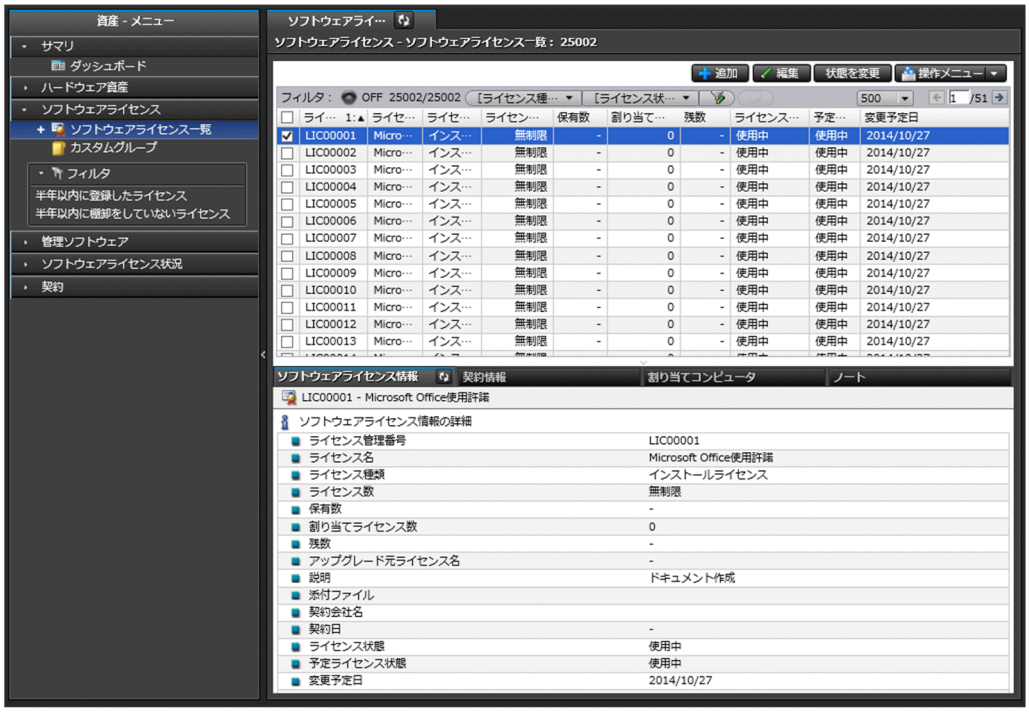
棚卸の実施状況を確認したり、在庫のコンピュータを検索したりできます。ハードウェア資産にサポート契約の契約情報を関連づけることで、特定のハードウェア資産にトラブルが発生したときにサポートセンターの連絡先を調べることもできます。



［ソフトウェアライセンス］画面で確認する

組織で所有しているソフトウェアライセンスを登録して、一覧で管理できます。保有しているライセンス数を把握できるだけなく、どの機器にライセンスの利用許可を与えているかを確認することもできます。

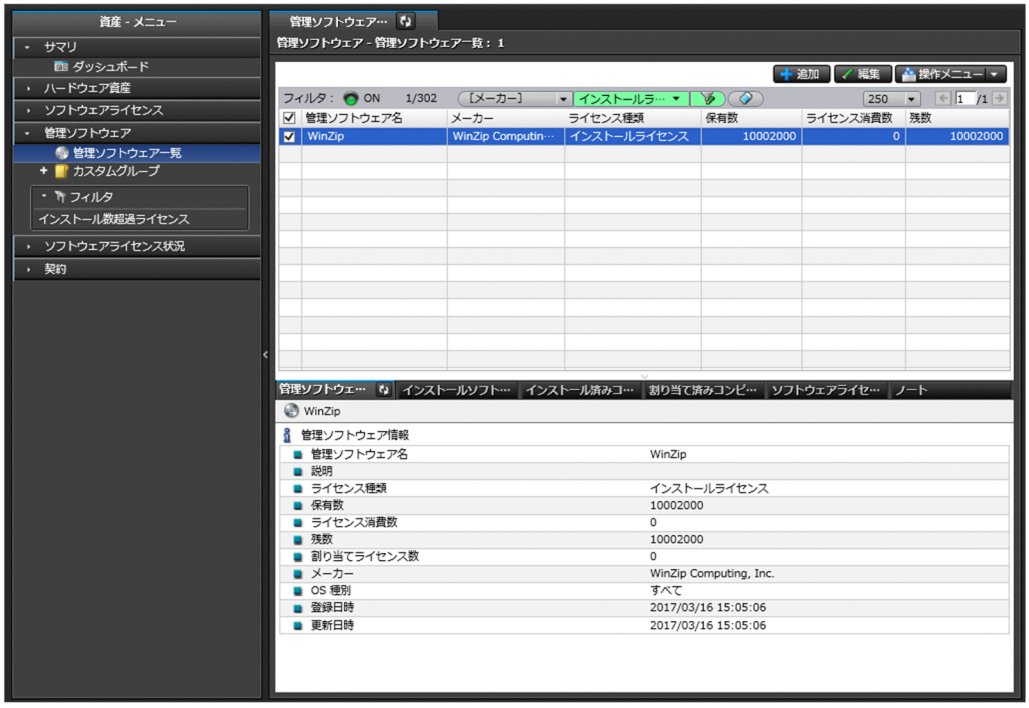
また、ソフトウェアライセンスに契約情報を関連づけることで、ソフトウェアライセンスの契約費用や契約期間などを把握できます。



［管理ソフトウェア］画面で確認する

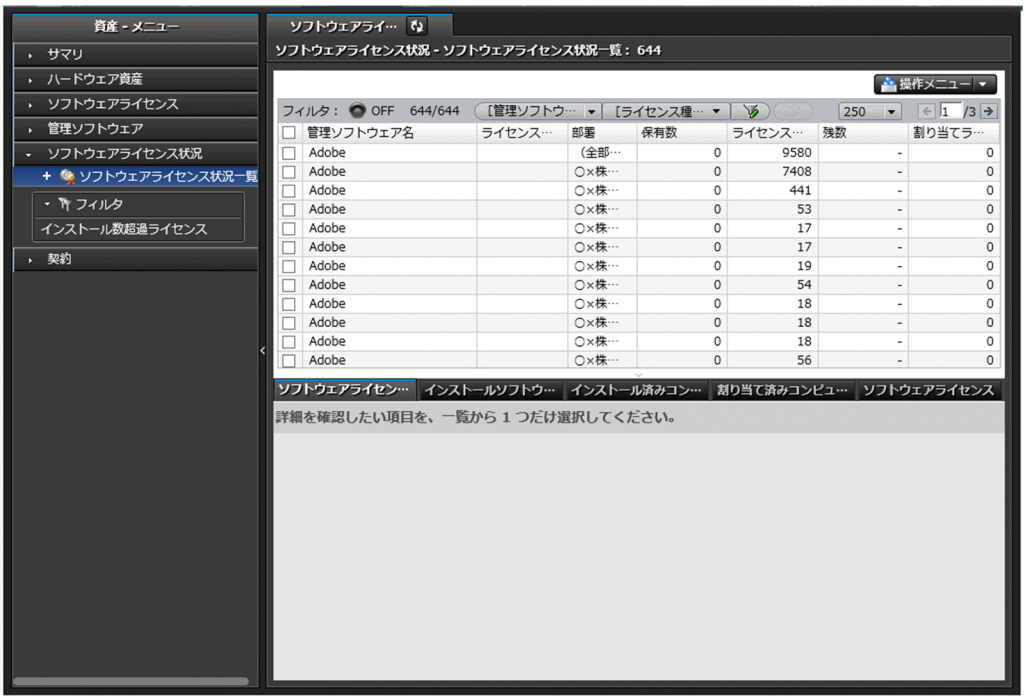
ライセンス消費数をカウントするソフトウェアの情報を登録して、ソフトウェア単位に利用状況を確認できます。管理ソフトウェアとソフトウェアライセンスを関連づけることで、ライセンスの保有数とライセンス消費数の差分を把握できるようになります。

また、各ソフトウェアがどのコンピュータにインストールされているかも確認できます。



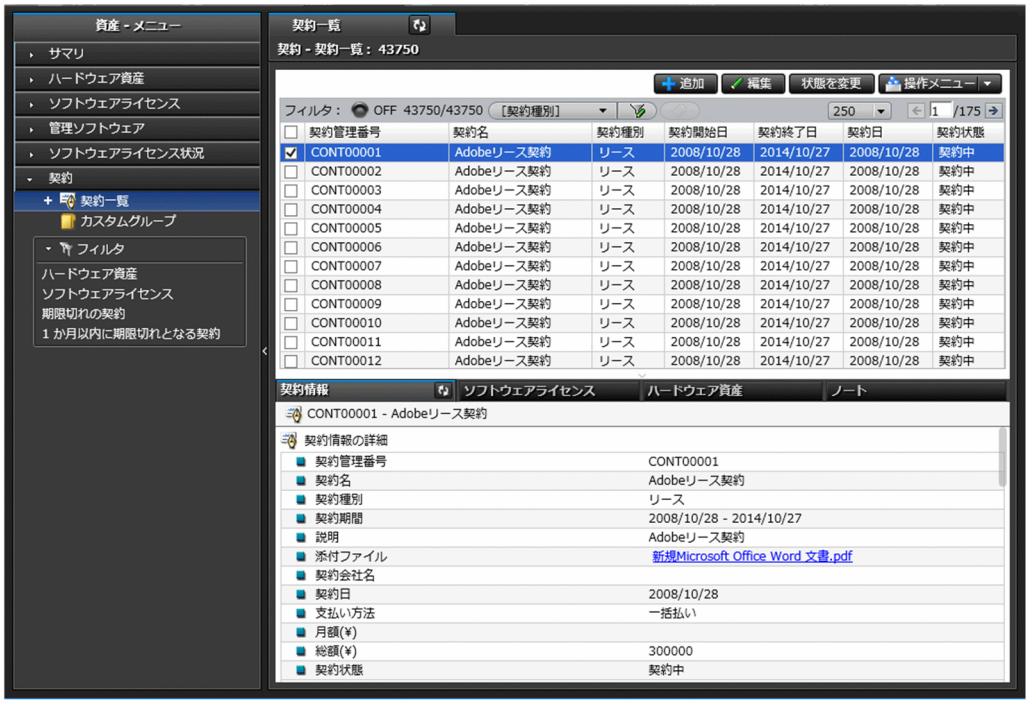
［ソフトウェアライセンス状況一覧］画面で確認する

管理ソフトウェアごとのソフトウェアライセンスの利用状況を管理できます。ソフトウェアライセンスの保有数や残数が集計され、ソフトウェアライセンスの利用状況をまとめて確認できます。



［契約］画面で確認する

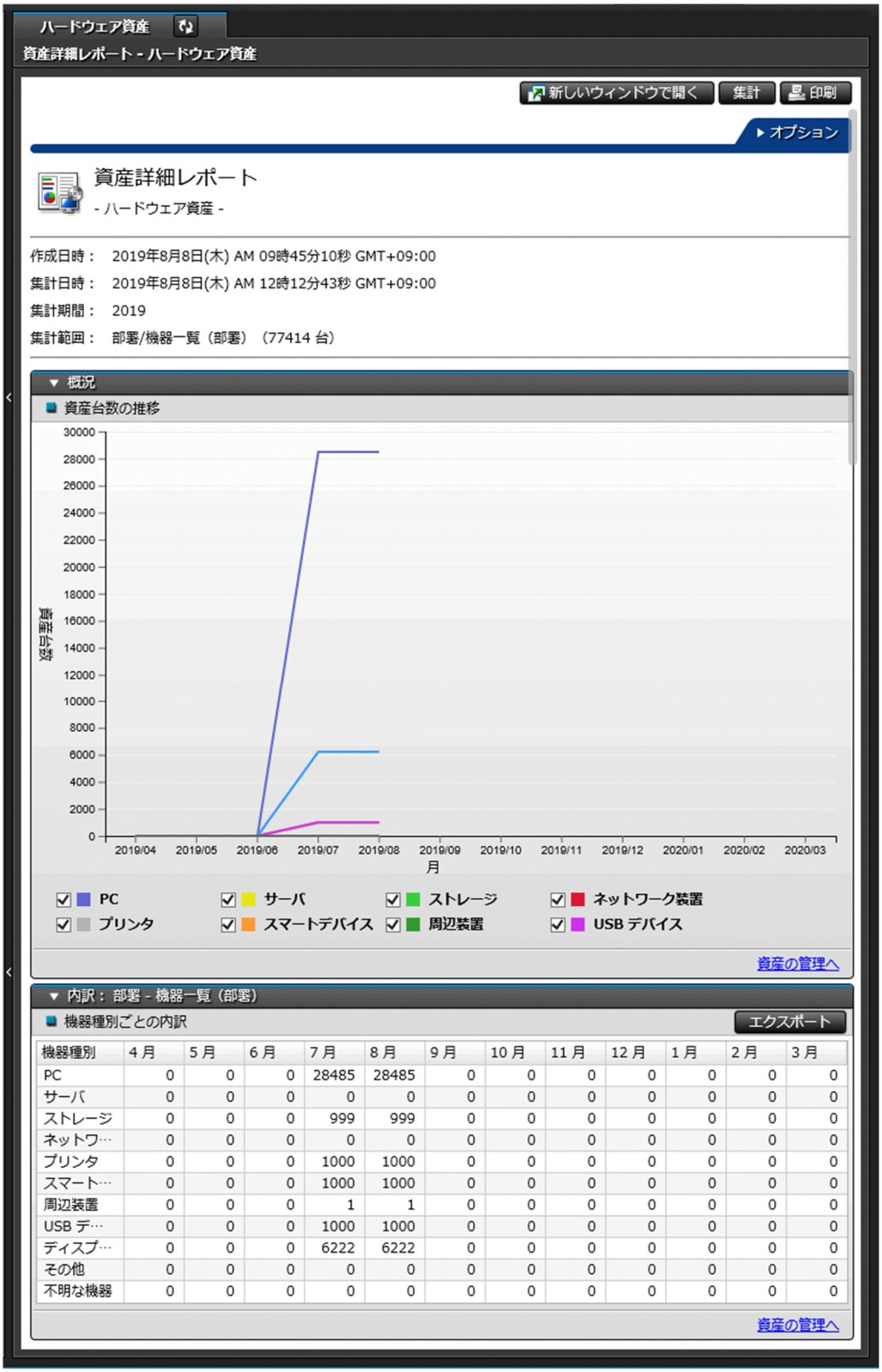
ハードウェア資産やソフトウェアライセンスに対する契約情報を登録して、一覧で管理できます。契約の状態や種類、期限などを確認できます。



レポートで確認する

[ダイジェストレポート]、[資産詳細レポート] で資産の状況を確認できます。

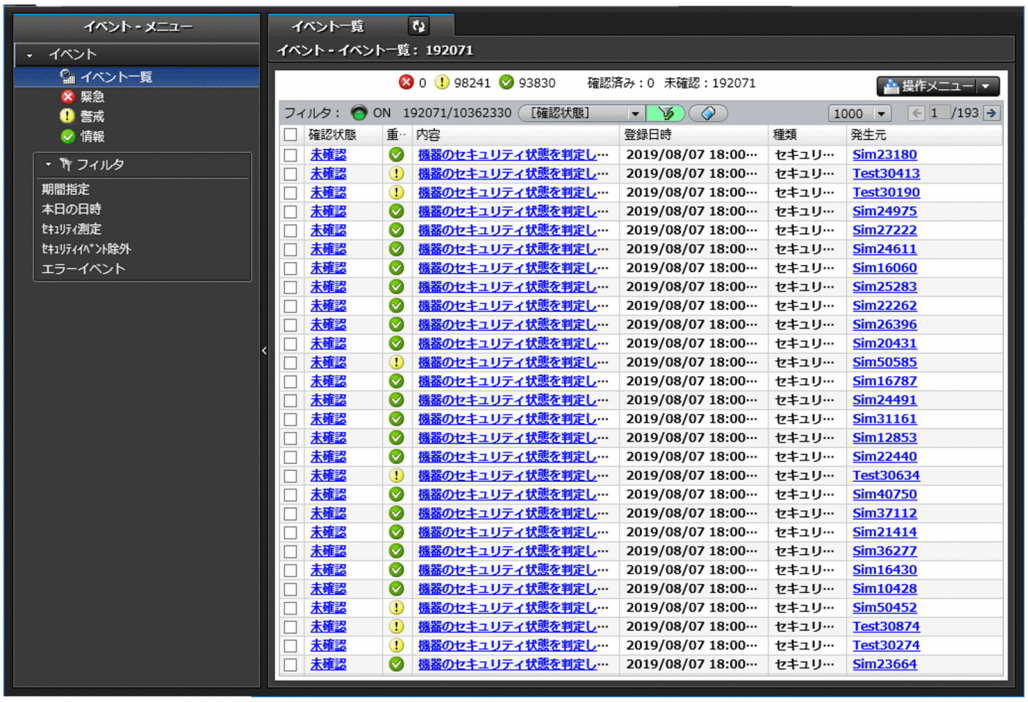
[ダイジェストレポート] では、リプレースを予定しているハードウェア資産、ソフトウェアライセンスの利用状況、期限切れの近い契約などを確認できます。[資産詳細レポート] では、ハードウェア資産の台数の推移や、ソフトウェアライセンスの超過と余剰、資産に掛かっている費用などを確認できます。



機器種別	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月
PC	0	0	0	28485	28485	0	0	0	0	0	0	0
サーバ	0	0	0	0	0	0	0	0	0	0	0	0
ストレージ	0	0	0	999	999	0	0	0	0	0	0	0
ネットワ…	0	0	0	0	0	0	0	0	0	0	0	0
プリンタ	0	0	0	1000	1000	0	0	0	0	0	0	0
スマート…	0	0	0	1000	1000	0	0	0	0	0	0	0
周辺装置	0	0	0	1	1	0	0	0	0	0	0	0
USB デ…	0	0	0	1000	1000	0	0	0	0	0	0	0
ディスプ…	0	0	0	6222	6222	0	0	0	0	0	0	0
その他	0	0	0	0	0	0	0	0	0	0	0	0
不明な機器	0	0	0	0	0	0	0	0	0	0	0	0

イベント画面で確認する

イベント画面で、資産の登録、資産の状態の変更、ソフトウェアライセンスの追加と削除など、資産管理に関するイベントを確認できます。



(1) 機器画面と資産画面の違い

ここでは、機器画面と資産画面の違いについて説明します。

機器画面

機器画面は、現在ネットワークに接続されている機器の状況を把握するための画面です。

機器画面では、管理対象の機器の一覧が表示されます。管理対象の機器は、基本的にネットワークに接続されていて、管理用サーバと通信します。このため、機器画面からは、機器から収集された最新情報を確認したり、表示された機器に対してメッセージを通知したりできます。

> **ヒント**
>
> 機器を管理対象にすると、1 台につき 1 ライセンス消費します。つまり、機器画面に機器を表示させるためには製品ライセンスが必要になります。

また、機器画面の［ソフトウェア情報］画面では、コンピュータから収集されたソフトウェア情報を一覧で確認できます。実際のインストール数や、ソフトウェアの詳細情報を確認できます。

資産画面

資産画面は、組織で所有している資産を管理するための画面です。

［ハードウェア資産］画面では、組織の所有しているハードウェア資産を管理します。所有しているハードウェア資産には、ネットワークに接続されている機器もあれば、在庫としてオフラインで保管されている機器もあります。コンピュータの本体とディスプレイを分けて管理することもあります。また、資産管理業務では、すでに組織に存在しない滅却した資産も管理します。このように、管理用サーバとの通信に関

係なく、組織が所有している資産とその状態を管理するために、[ハードウェア資産]画面を利用します。[ハードウェア資産]画面には、任意にハードウェア資産を登録して管理できます。

ヒント

資産情報の登録にはライセンスは不要です。

ヒント

機器が管理対象になると、自動的にその機器のハードウェア資産情報も[ハードウェア資産]画面に登録されます。このため、製品導入直後は、機器画面と資産画面に同じ機器が表示されることがあります。

さらに、機器画面では機器から収集された情報だけが表示されるのに対して、資産画面では管理者が独自に情報を入力して管理できます。すでに機器の管理台帳が手もとにある場合は、その情報を資産画面にインポートすることで既存の情報を活用できます。

資産画面では、ハードウェア資産のほかにも、ソフトウェアライセンスの利用状況も管理できます。機器画面の[ソフトウェア情報]画面では、ソフトウェアのインストール数を把握できますが、資産画面では組織が保有しているソフトウェアライセンス数を登録して、管理ソフトウェア情報にソフトウェア情報との関連を定義することで、ライセンス消費数と保有数の差分を把握できます。このように、ソフトウェアについても、機器画面は収集された情報を確認するために利用するのに対して、資産画面はソフトウェアライセンスの観点から利用状況を把握するために利用するといった違いがあります。

関連リンク

- (2)　機器とハードウェア資産の同定

2.11.7　資産情報のインポート

CSV ファイルを利用して資産情報をインポートできます。インポートすることで、資産情報を一括で追加したり編集したりできます。資産情報のインポートには、[資産情報をインポートしましょう]ウィザードで実行する方法と、`ioutils importasset` コマンドを実行する方法があります。インポートできる資産情報は次の 5 種類です。

- ハードウェア資産情報
- ソフトウェアライセンス情報
- 管理ソフトウェア情報
- 契約情報
- 契約会社リスト

(1) ハードウェア資産情報の項目とインポート時の CSV ファイルの記述形式

インポートする CSV ファイルのデータは、規定された記述形式に従っている必要があります。インポートできるハードウェア資産情報の項目と記述形式を次の表に示します。

重要

Active Directory から取得した情報またはレジストリから取得した情報がすでに存在する項目は、インポートによる更新ができません。

ヒント

インポート時は、「資産管理番号」、「シリアルナンバー」(BIOS 情報)、「IP アドレス」、「MAC アドレス」、「ホスト名」、「IMEI」、および「契約電話番号」の中から 1 つをマッピングキーとして、既存のハードウェア資産情報と引き当てます。ハードウェア資産情報が引き当てられた場合は、各項目の対応づけに従ってハードウェア資産情報が更新されます。ハードウェア資産情報が引き当てられなかった場合は、新規のハードウェア資産情報として登録するかどうかを選択できます。詳細は、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のハードウェア資産情報をインポートする手順の説明を参照してください。

ヒント

資産画面の［ハードウェア資産］画面でインフォメーションエリアに「−」が表示されている項目は、ハードウェア資産情報をエクスポートすると、「−」の部分が空文字で出力されます。これは、エクスポートしたハードウェア資産情報をそのままインポートする際に、正常にインポートできるようにするためです。

ヒント

JP1/NETM/DM からハードウェア資産情報を移行する場合に、JP1/NETM/DM クライアントに設定されていた「ホスト識別子」を指定します。

JP1/NETM/DM クライアントから JP1/IT Desktop Management 2 エージェントに入れ替えた機器が管理対象機器として登録される際に、資産インポート時に指定したホスト識別子と同じホスト識別子の機器情報がハードウェア資産に関連づけられます。

管理項目	データの記述形式	省略可否
資産管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」	△
機器名称	256 文字以内の任意の文字列。	○

管理項目	データの記述形式	省略可否
棚卸日	次の形式で記述します。 yyyy/mm/dd yyyy：年、mm：月、dd：日 省略すると、新規にハードウェア資産情報が登録されるときは［1970/01/01］が設定されます。	○
説明	1,024 文字以内の任意の文字列。	○
資産状態	［資産状態］に登録されている項目のどれか 1 つ。 ただし、「未確認」は指定できません。 省略すると、新規にハードウェア資産情報が登録されるときは「運用中」が設定されます。	○
予定資産状態※1	［資産状態］に登録されている項目のどれか 1 つ。 ただし、「未確認」は指定できません。	○
変更予定日※1	次の形式で記述します。 yyyy/mm/dd yyyy：年、mm：月、dd：日	○
部署	登録されている部署の階層構成。 階層構成を、512 文字以内かつ 40 階層以内で指定します。各階層名は 256 文字以内で指定してください。また、階層は「/」（スラッシュ）で区切って記述します。最初と最後の「/」は任意です。ただし、省略した場合も 1 文字としてカウントされます。※2 （例）/総務部/総務課/ 指定した階層が存在しない場合は、インポート時に新規に階層が作成されます。 省略すると、新規にハードウェア資産情報が登録されるときは「不明」が設定されます。	○
設置場所	登録されている設置場所の階層構成。 階層構成を、512 文字以内かつ 40 階層以内で指定します。各階層名は 256 文字以内で指定してください。また、階層は「/」（スラッシュ）で区切って記述します。最初と最後の「/」は任意です。ただし、省略した場合も 1 文字としてカウントされます。※2 （例）/A 棟/1F/ 指定した階層が存在しない場合は、インポート時に新規に階層が作成されます。 省略すると、新規にハードウェア資産情報が登録されるときは［不明］が設定されます。	○
利用者名	256 文字以内の任意の文字列。※2	○
メールアドレス	256 文字以内の任意の文字列。※2	○
電話番号	256 文字以内の任意の文字列。※2	○
アカウント	256 文字以内の任意の文字列。※2	○
モデル	256 文字以内の任意の文字列。	○
シリアルナンバー	256 文字以内の任意の文字列。	△

管理項目	データの記述形式	省略可否
メモリ	0～9,223,372,036,854,775,807 の半角数字（単位がバイトの場合）。 サイズの単位 「B」、「KB」、「MB」、「GB」、「TB」、または「PB」を最後に付けることもできます。なお、けた区切りの「,」(コンマ)は入力しないでください。	○
ストレージ容量	0～9,223,372,036,854,775,807 の半角数字（単位がバイトの場合）。 サイズの単位 「B」、「KB」、「MB」、「GB」、「TB」、または「PB」を最後に付けることもできます。なお、けた区切りの「,」(コンマ)は入力しないでください。	○
ストレージ空き容量	0～9,223,372,036,854,775,807 の半角数字（単位がバイトの場合）。 サイズの単位 「B」、「KB」、「MB」、「GB」、「TB」、または「PB」を最後に付けることもできます。なお、けた区切りの「,」(コンマ)は入力しないでください。 ［機器種別］が「ディスプレイ」の場合、この項目はインポートされません。	○
IP アドレス	次の形式で記述します。 nnn.nnn.nnn.nnn 0.0.0.0 ～ 255.255.255.255 の範囲で指定してください。	△
サブネットマスク	次の形式で記述します。 nnn.nnn.nnn.nnn 0.0.0.0 ～ 255.255.255.255 の範囲で指定してください。	○
MAC アドレス	次の形式で記述します。x は、0～F です。 • xxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx なお、区切り文字「-」および「:」は混在していてもインポートできます。	△
ホスト名	256 文字以内の任意の文字列。	△
ディスプレイ種別	［ディスプレイ種別］に登録されている項目のどれか 1 つ。	○
ディスプレイサイズ	0～256 の半角数字。	○
ディスプレイ解像度	［ディスプレイ解像度］に登録されている項目のどれか 1 つ。	○
UDID	128 文字以内の任意の文字列。	○
IMEI	64 文字以内の任意の文字列。	○
IMSI	64 文字以内の任意の文字列。	○
ICCID	64 文字以内の任意の文字列。	○
キャリア	512 文字以内の任意の文字列。	○
契約電話番号	半角数字、「-」、および「+」。	○
機器種別	［機器種別］に登録されている項目のどれか 1 つ。 省略すると、新規にハードウェア資産情報が登録されるときは「不明」が設定されます。	○
CPU	256 文字以内の任意の文字列。	○

管理項目	データの記述形式	省略可否
OS	256 文字以内の任意の文字列。	○
メーカー	256 文字以内の任意の文字列。	○
追加管理項目	設定画面の［資産管理］－［資産管理項目の設定］画面で設定したデータ型。	○ ※3
デバイスインスタンス ID	256 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」	○
ホスト識別子※4	64 文字以内の半角数字、半角の大文字の英字、および次に示す半角記号。 「#」、「-」、「.」	○

（凡例）○：設定を省略できる　△：どれか 1 つは設定が必要

注※1　［予定資産状態］と［変更予定日］は必ずセットでインポートしてください。

注※2　データ型が「テキスト型」の場合、項目に文字制限を設定しているときは、CSV ファイルのデータも従う必要があります。

注※3　入力を必須としている追加管理項目の場合は、必ず設定してください。

注※4　インポートしたファイルにホスト識別子の値が記述されていた場合、インポート後に修正できません。

ヒント

インポートする項目は、「"」（ダブルクォーテーション）で囲まれていてもいなくてもかまいません。ただし、インポートするデータに「,」（コンマ）が含まれる場合、そのデータを「"」で囲んでください。例えば、「AB,CD」をインポートする場合は、「"AB,CD"」と指定します。

(2)　ソフトウェアライセンス情報の項目とインポート時の CSV ファイルの記述形式

インポートする CSV ファイルのデータは、規定された記述形式に従っている必要があります。インポートできるソフトウェアライセンス情報の項目と記述形式を次の表に示します。

ヒント

インポート時は、「ライセンス管理番号」をマッピングキーとして、既存のソフトウェアライセンス情報と引き当てます。ソフトウェアライセンス情報が引き当てられた場合は、各項目の対応づけに従ってソフトウェアライセンス情報が更新されます。ソフトウェアライセンス情報が引き当てられなかった場合は、新規のソフトウェアライセンス情報として登録されます。

管理項目	データの記述形式	省略可否
ライセンス管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」	×
ライセンス名	256 文字以内の任意の文字列。	○
ライセンス種類	[ライセンス種類] に登録されている項目のどれか 1 つ。 省略すると、新規にソフトウェアライセンス情報が登録されるときは「インストールライセンス」が設定されます。	○
ライセンス数	0～2,147,483,647 の半角数字。 省略すると、新規にソフトウェアライセンス情報が登録されるときは「無制限」が設定されます。なお、けた区切りの「,」(コンマ)は入力しないでください。	○
棚卸日	次の形式で記述します。 yyyy/mm/dd yyyy：年、mm：月、dd：日	○
部署	登録されている部署の階層構成。 階層構成を、512 文字以内かつ 40 階層以内で指定します。各階層名は 256 文字以内で指定してください。また、階層は「/」（スラッシュ）で区切って記述します。最初と最後の「/」は任意です。ただし、省略した場合も 1 文字としてカウントされます。※3 （例）/総務部/総務課/ 指定した階層が存在しない場合は、インポート時に新規に階層が作成されます。 省略すると、新規にハードウェア資産情報が登録されるときは「不明」が設定されます。	○
説明	1,024 文字以内の任意の文字列。	○
ライセンス状態	[ライセンス状態] に登録されている項目のどれか 1 つ。 省略すると、新規にソフトウェアライセンス情報が登録されるときは「運用中」が設定されます。	○
予定ライセンス状態※1	[ライセンス状態] に登録されている項目のどれか 1 つ。	○
変更予定日※1	次の形式で記述します。 yyyy/mm/dd yyyy：年、mm：月、dd：日	○
追加管理項目	設定画面の［資産管理］－［資産管理項目の設定］画面で設定したデータ型。	○ ※2

（凡例）○：設定を省略できる　×：設定を省略できない

注※1　［予定ライセンス状態］と［変更予定日］は必ずセットでインポートしてください。

注※2　入力を必須としている追加管理項目の場合は、必ず設定してください。

注※3　データ型が「テキスト型」の場合、項目に文字制限を設定しているときは、CSV ファイルのデータも従う必要があります。

ヒント

インポートする項目は、「"」（ダブルクォーテーション）で囲まれていてもいなくてもかまいません。ただし、インポートするデータに「,」（コンマ）が含まれる場合、そのデータを「"」で囲んでください。例えば、「AB,CD」をインポートする場合は、「"AB,CD"」と指定します。

(3)　管理ソフトウェア情報の項目とインポート時の CSV ファイルの記述形式

インポートする CSV ファイルのデータは、規定された記述形式に従っている必要があります。インポートできる管理ソフトウェア情報の項目と記述形式を次の表に示します。

ヒント

インポート時は、「管理ソフトウェア名」をマッピングキーとして、既存の管理ソフトウェア情報と引き当てます。管理ソフトウェア情報が引き当てられた場合は、各項目の対応づけに従って管理ソフトウェア情報が更新されます。管理ソフトウェア情報が引き当てられなかった場合は、新規の管理ソフトウェア情報として登録されます。

管理項目	データの記述形式	省略可否
管理ソフトウェア名	512 文字以内の任意の文字列。	×
メーカー	128 文字以内の任意の文字列。	○
説明	1,024 文字以内の任意の文字列。	○
OS 種別	次に示す文字列。 • すべて • Windows • Linux • Mac OS • HP-UX • Solaris • AIX	○

（凡例）○：設定を省略できる　×：設定を省略できない

ヒント

インポートする項目は、「"」（ダブルクォーテーション）で囲まれていてもいなくてもかまいません。ただし、インポートするデータに「,」（コンマ）が含まれる場合、そのデータを「"」で囲んでください。例えば、「AB,CD」をインポートする場合は、「"AB,CD"」と指定します。

(4) 契約情報の項目とインポート時の CSV ファイルの記述形式

インポートする CSV ファイルのデータは、規定された記述形式に従っている必要があります。インポートできる契約情報の項目と記述形式を次の表に示します。

ヒント

インポート時は、「契約管理番号」をマッピングキーとして、既存の契約情報と引き当てます。契約情報が引き当てられた場合は、各項目の対応づけに従って契約情報が更新されます。契約情報が引き当てられなかった場合は、新規の契約情報として登録されます。

管理項目	データの記述形式	省略可否
契約管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」	×
契約名	256 文字以内の任意の文字列。	○
契約種別	[契約種別] に登録されている項目のどれか 1 つ。 省略すると、新規に契約情報が登録されるときは「購入」が設定されます。	○
契約対象	次のどれかを記述します。 • ハードウェア資産 • ソフトウェアライセンス • その他 省略すると、新規に契約情報が登録されるときは「その他」が設定されます。	○
契約日	次の形式で記述します。 yyyy/mm/dd yyyy：年、mm：月、dd：日	○
契約開始日	次の形式で記述します。 yyyy/mm/dd yyyy：年、mm：月、dd：日	○ ※1
契約終了日	次の形式で記述します。 yyyy/mm/dd yyyy：年、mm：月、dd：日	○ ※1
契約状態	[契約状態] に登録されている項目のどれか 1 つ。 省略すると、新規に契約情報が登録されるときは「契約中」が設定されます。	○
部署	登録されている部署の階層構成。 階層構成を、512 文字以内かつ 40 階層以内で指定します。各階層名は 256 文字以内で指定してください。また、階層は「/」（スラッシュ）で区切って記述します。最初と最後の「/」は任意です。ただし、省略した場合も 1 文字としてカウントされます。※4 （例）/総務部/総務課/ 指定した階層が存在しない場合は、インポート時に新規に階層が作成されます。 省略すると、新規にハードウェア資産情報が登録されるときは「不明」が設定されます。	○

管理項目	データの記述形式	省略可否
支払い方法	次のどちらかを記述します。 • 月払い • 一括	×
月額	0～9,223,372,036,854,775,807 の半角数字。 ［支払い方法］が「月払い」の場合に記述します。なお、けた区切りの「,」(コンマ)は入力しないでください。	○ ※1
総額	0～9,223,372,036,854,775,807 の半角数字。 ［支払い方法］が「一括」の場合に記述します。なお、けた区切りの「,」（コンマ）は入力しないでください。	○ ※2
説明	1,024 文字以内の任意の文字列。	○
追加管理項目	設定画面の［資産管理］－［資産管理項目の設定］画面で設定したデータ型。	○ ※3

（凡例）○：設定を省略できる　×：設定を省略できない

注※1　支払い方法が［月払い］の場合は［契約開始日］、［契約終了日］、および［月額］を必ず設定してください。

注※2　支払い方法が［一括］の場合は必ず設定してください。

注※3　入力を必須としている追加管理項目の場合は、必ず設定してください。

注※4　データ型が「テキスト型」の場合、項目に文字制限を設定しているときは、CSV ファイルのデータも従う必要があります。

ヒント

インポートする項目は、「"」（ダブルクォーテーション）で囲まれていてもいなくてもかまいません。ただし、インポートするデータに「,」（コンマ）が含まれる場合、そのデータを「"」で囲んでください。例えば、「AB,CD」をインポートする場合は、「"AB,CD"」と指定します。

(5)　契約会社リストの項目とインポート時の CSV ファイルの記述形式

インポートする CSV ファイルのデータは、規定された記述形式に従っている必要があります。インポートできる契約会社リストの項目と記述形式を次の表に示します。

ヒント

インポート時は、「契約会社名」をマッピングキーとして、既存の契約会社情報と引き当てます。契約会社情報が引き当てられた場合は、各項目の対応づけに従って契約会社情報が更新されます。契約会社情報が引き当てられなかった場合は、新規の契約会社情報として登録されます。

管理項目	データの記述形式	省略可否
契約会社名	256 文字以内の任意の文字列。	×
所在地	256 文字以内の任意の文字列。	○
電話番号	256 文字以内の半角数字、「-」、または「+」。	○
メールアドレス	256 文字以内の任意の文字列。	○
担当者名	256 文字以内の任意の文字列。	○
説明	1,024 文字以内の任意の文字列。	○

（凡例）○：設定を省略できる　×：設定を省略できない

ヒント

インポートする項目は、「"」（ダブルクォーテーション）で囲まれていてもいなくてもかまいません。ただし、インポートするデータに「,」（コンマ）が含まれる場合、そのデータを「"」で囲んでください。例えば、「AB,CD」をインポートする場合は、「"AB,CD"」と指定します。

2.11.8　資産情報のエクスポート

CSV ファイルに資産情報をエクスポートできます。エクスポートすることで、資産情報を別の管理用サーバで使用したり、ほかのソフトウェアで使用したりできます。資産情報のエクスポートには操作メニューから実行する方法と、ioutils exportasset コマンドを実行する方法があります。エクスポートできる資産情報は次の 5 種類です。

- ハードウェア資産情報※
- ソフトウェアライセンス情報
- 管理ソフトウェア情報
- 契約情報
- 契約会社リスト

ハードウェア資産情報のホスト識別子は、ioutils exportasset コマンドから実行するときだけエクスポートできます。

ヒント

エクスポートする項目や対象のデータは、管理者が任意に指定できます。目的に応じた一覧を作成できます。

それぞれで出力されるデータ形式については、関連リンクを参照してください。

関連リンク

- (1)　ハードウェア資産情報の項目とインポート時の CSV ファイルの記述形式
- (2)　ソフトウェアライセンス情報の項目とインポート時の CSV ファイルの記述形式
- (3)　管理ソフトウェア情報の項目とインポート時の CSV ファイルの記述形式
- (4)　契約情報の項目とインポート時の CSV ファイルの記述形式
- (5)　契約会社リストの項目とインポート時の CSV ファイルの記述形式

2.11.9　資産の関連づけ情報のインポート

CSV ファイルを利用して資産の関連づけ情報をインポートできます。インポートすることで、資産の関連づけ情報を一括で追加したり編集したりできます。資産の関連づけ情報のインポートには、`ioutils importassetassoc` コマンドを実行します。インポートできる資産の関連づけ情報は次のとおりです。

ハードウェア資産

- 機器
- ハードウェア資産
- 契約

ソフトウェアライセンス

- 管理ソフトウェア
- アップグレード元ライセンス
- 機器
- 契約

管理ソフトウェア

- ソフトウェア
- ソフトウェアライセンス

契約

- ハードウェア資産
- ソフトウェアライセンス
- 契約会社リスト

メモ

以降では資産の関連づけ情報を次のように表記します。

資産情報→関連づけられた資産情報

例えば、ハードウェア資産情報に機器情報が関連づいている場合、「ハードウェア資産→機器」と表記します。

(1) 資産の関連づけ情報インポート時の CSV ファイルの記述形式

インポートする CSV ファイルのデータは、規定された記述形式に従っている必要があります。インポートできる資産の関連づけ情報の項目と記述形式を次に示します。

メモ

資産の関連づけ情報を記述した CSV ファイルは、同じ関連づけ情報ごとに作成する必要があります。例えば、「ハードウェア資産→機器」の関連づけ情報の CSV ファイルと、「ハードウェア資産→契約」の関連づけ情報の CSV ファイルは別に作成してください。

ヒント

インポートする項目は、「"」（ダブルクォーテーション）で囲まれていてもいなくてもかまいません。ただし、インポートするデータに「,」（コンマ）が含まれる場合、そのデータを「"」で囲んでください。例えば、「AB,CD」をインポートする場合は、「"AB,CD"」と指定します。

ヒント

- 「関連なし」は CSV ファイルの第 2 カラム以降を空の値または省略することで記述します。
- 複数の関連づけは、複数行で記述します。
- 複数を関連づけることができる関連は、「関連なし」の行と「関連あり」の行を混在させた場合、「関連なし」の行は不正データと見なします。

ハードウェア資産→機器

CSV ファイルの最上位に記述された関連が、代表機器を表します。

また、1 つの資産管理番号に複数のホスト識別子を関連づけできます。

CSV ファイルのカラム位置	項目	データの記述形式
1	資産管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」
2	ホスト識別子	64 文字以内の半角数字、半角の大文字の英字、および次に示す半角記号。

CSV ファイルのカラム位置	項目	データの記述形式
2	ホスト識別子	「#」、「-」、「.」

ハードウェア資産→ハードウェア資産

1 つの資産管理番号に複数の資産管理番号を関連づけできます。関連先の資産管理番号は、関連元と同じ値を指定できません。

CSV ファイルのカラム位置	項目	データの記述形式
1	資産管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」
2	資産管理番号	

ハードウェア資産→契約

1 つの資産管理番号に複数の契約管理番号を関連づけできます。ソフトウェアライセンスに関連づいている契約の契約管理番号は指定できません。

CSV ファイルのカラム位置	項目	データの記述形式
1	資産管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」
2	契約管理番号	

ソフトウェアライセンス→管理ソフトウェア

1 つのライセンス管理番号に 1 つの管理ソフトウェア名を関連づけできます。

CSV ファイルのカラム位置	項目	データの記述形式
1	ライセンス管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」
2	管理ソフトウェア名	512 文字以内の任意の文字列。

ソフトウェアライセンス→アップグレード元ライセンス

1 つのライセンス管理番号に 1 つのアップグレード元ライセンス管理番号を関連づけできます。

次のどれかの条件に該当するソフトウェアライセンスのライセンス管理番号は指定できません。ソフトウェアライセンスの各情報は、資産画面の［ソフトウェアライセンス］画面またはエクスポートで確認できます。条件に該当する場合は、値を修正後に関連づけを実施してください。

- ライセンスの種類がアップグレード先とアップグレード元で異なる
- アップグレード先とアップグレード元が同一である
- アップグレード元ライセンスのライセンス数がアップグレード先ライセンスのライセンス数の総数より少ない
- アップグレード元ライセンスが有限かつアップグレード先ライセンスが無制限のライセンスである

CSV ファイルのカラム位置	項目	データの記述形式
1	ライセンス管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」
2	アップグレード元ライセンス管理番号	

ソフトウェアライセンス→機器

1 つのライセンス管理番号に複数のホスト識別子を関連づけできます。発見した機器のホスト識別は指定できません。

CSV ファイルのカラム位置	項目	データの記述形式
1	ライセンス管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」
2	ホスト識別子	64 文字以内の半角数字、半角の大文字の英字、および次に示す半角記号。 「#」、「-」、「.」

ソフトウェアライセンス→契約

1 つのライセンス管理番号に 1 つの契約管理番号を関連づけできます。ハードウェア資産に関連づいている契約の契約管理番号は指定できません。

CSV ファイルのカラム位置	項目	データの記述形式
1	ライセンス管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」
2	契約管理番号	

管理ソフトウェア→ソフトウェア

1 つの管理ソフトウェア名に複数のソフトウェア名を関連づけできます。データベースに登録されていないソフトウェア名、プロダクト ID を指定することができます。購入形態が製品版の場合、プロダクト ID は指定できません。

CSV ファイルのカラム位置	項目	データの記述形式
1	管理ソフトウェア名	512 文字以内の任意の文字列。
2	ソフトウェア名	512 文字以内の任意の文字列。
3	購入形態	次のどちらかの値 • ボリュームライセンス版 • 製品版
4	プロダクト ID	64 文字以内の ASCII コードの制御文字を除いた文字列

なお、ソフトウェア名、購入形態、およびプロダクト ID は、次に示す組み合わせを記述できます。

- ソフトウェア名：あり、購入形態：なし、プロダクト ID：なし
- ソフトウェア名：あり、購入形態：あり、プロダクト ID：なし
- ソフトウェア名：あり、購入形態：あり、プロダクト ID：あり

管理ソフトウェア→ソフトウェアライセンス

1 つの管理ソフトウェア名に複数のライセンス管理番号を関連づけできます。

CSV ファイルのカラム位置	項目	データの記述形式
1	管理ソフトウェア名	512 文字以内の任意の文字列。
2	ライセンス管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」

契約→ハードウェア資産

1 つの契約管理番号に複数の資産管理番号を関連づけできます。ソフトウェアライセンスに関連づいている契約にハードウェア資産を関連づけることはできません。

CSV ファイルのカラム位置	項目	データの記述形式
1	契約管理番号	32 文字以内の半角英数字、および次に示す半角記号。
2	資産管理番号	

CSV ファイルのカラム位置	項目	データの記述形式
2	資産管理番号	「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」

契約→ソフトウェアライセンス

1 つの契約管理番号に複数のライセンス管理番号を関連づけできます。ハードウェア資産に関連づいている契約にソフトウェアライセンスを関連づけることはできません。

CSV ファイルのカラム位置	項目	データの記述形式
1	契約管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」
2	ライセンス管理番号	

契約→契約会社リスト

1 つの契約管理番号に 1 つの契約会社名を関連づけできます。

CSV ファイルのカラム位置	項目	データの記述形式
1	契約管理番号	32 文字以内の半角英数字、および次に示す半角記号。 「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」
2	契約会社名	256 文字以内の任意の文字列。

CSV ファイルの記述例

次の「ハードウェア資産→契約」の資産の関連づけ情報を CSV ファイルで記述した例を示します。

- 資産管理番号「AssetNo001」は契約管理番号「ContractNo001」と関連
- 資産管理番号「AssetNo002」はどの契約管理番号とも関連なし
- 資産管理番号「AssetNo003」は契約管理番号「ContractNo003」および「ContractNo004」と関連

```
AssetNo001, ContractNo001
AssetNo002,
AssetNo003, ContractNo003
AssetNo003, ContractNo004
```

2.11.10　資産の関連づけ情報のエクスポート

CSV ファイルに資産の関連づけ情報をエクスポートできます。エクスポートすることで、資産の関連づけ情報を別の管理用サーバで使用したり、ほかのソフトウェアで使用したりできます。資産の関連づけ情報のエクスポートには、ioutils exportassetassoc コマンドを実行します。エクスポートできる資産の関連づけ情報は次のとおりです。

ハードウェア資産

- 機器
- ハードウェア資産
- 契約

ソフトウェアライセンス

- 管理ソフトウェア
- アップグレード元ライセンス
- 機器
- 契約

管理ソフトウェア

- ソフトウェア
- ソフトウェアライセンス

契約

- ハードウェア資産
- ソフトウェアライセンス
- 契約会社リスト

メモ

以降では資産の関連づけ情報を次のように表記します。

資産情報→関連づけられた資産情報

例えば、ハードウェア資産情報に機器情報が関連づいている場合、「ハードウェア資産→機器」と表記します。

メモ

資産管理番号が設定されていないハードウェア資産は、エクスポートされません。

出力されるデータ形式については、関連リンクを参照してください。

関連リンク

- (1)　資産の関連づけ情報インポート時の CSV ファイルの記述形式

2.12 リモートインストールマネージャを使用したソフトウェアおよびファイルの配布

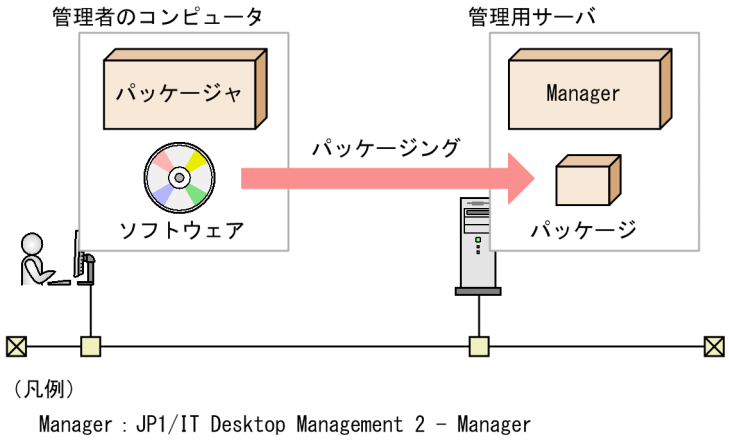
JP1/IT Desktop Management 2 では、管理用サーバから利用者のコンピュータへ、ネットワークを経由してソフトウェアおよびファイルを一括で配布できます。ここでは、リモートインストールマネージャを使用してソフトウェアを配布する流れを説明します。詳細や操作手順については、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」を参照してください。

重要

API 管理機器にはリモートインストールマネージャを使用したソフトウェアおよびファイルの配布ができません。

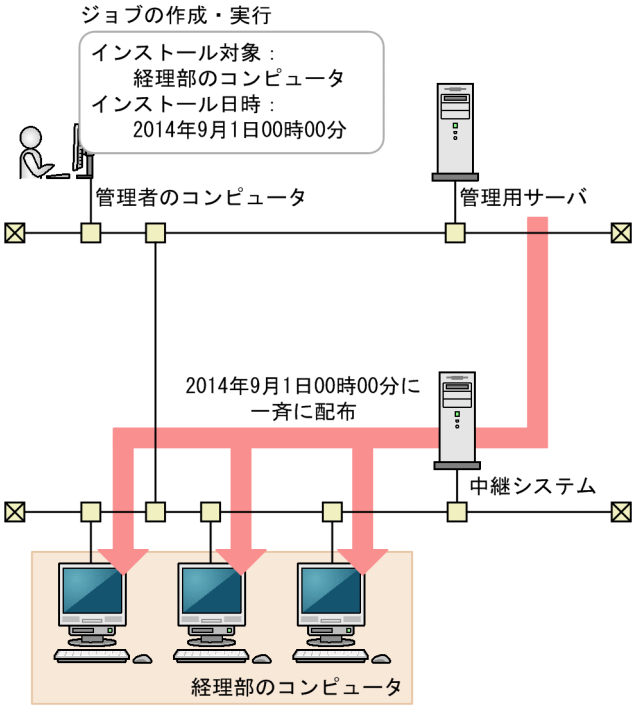
ソフトウェアを配布する流れを次に示します。

1. 配布したいソフトウェアを登録（パッケージング）する



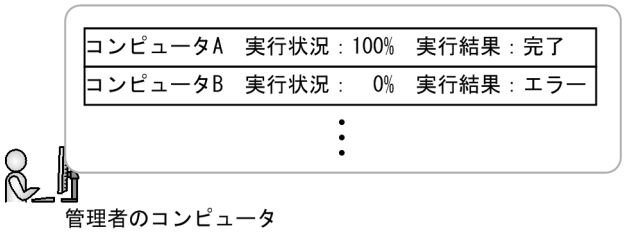
利用者のコンピュータに配布したいソフトウェアを、管理用サーバに登録（パッケージング）します。ソフトウェアをパッケージングするには、JP1/IT Desktop Management 2 - Agent のコンポーネントのパッケージャを使用します。パッケージング時に、配布するソフトウェアのインストール条件を指定できます。パッケージングしたソフトウェアの単位を、パッケージと呼びます。

2. ジョブを実行してパッケージを配布（リモートインストール）する



リモートインストールマネージャで、配布先のコンピュータや配布のスケジュールなどを設定したジョブを作成して実行します。例えば、図のようにジョブを作成して実行すると、2014 年 9 月 1 日になった時点で、経理部のコンピュータだけに一斉にパッケージが配布されます。

3. 配布の実行状況および実行結果を確認する



配布の実行状況および実行結果を、リモートインストールマネージャの［ジョブ実行状況］ウィンドウで確認します。配布に失敗したコンピュータがある場合は、実行結果に応じて対処して、ジョブを再実行します。

システム管理者が利用者のコンピュータに配布するだけではなく、利用者自身がソフトウェアを選択してインストールする方法もあります。

ヒント

リモートインストールマネージャを使用すると、2 ギガバイトを超えるファイルを配布できます。詳細は、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の「2 ギガバイトを超えるファイルを配布する」を参照してください。

ヒント

リモートインストールマネージャで、Windows の更新プログラムおよび Windows 10 の Feature Update をパッケージングして配布することもできます。詳細は、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の「更新プログラムを管理する」を参照してください。

2.12.1 リモートインストールマネージャで効率良く配布する方法

JP1/IT Desktop Management 2 では、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に、効率良く配布できる機能を提供しています。ここでは、効率良く配布するための機能の一部を説明します。

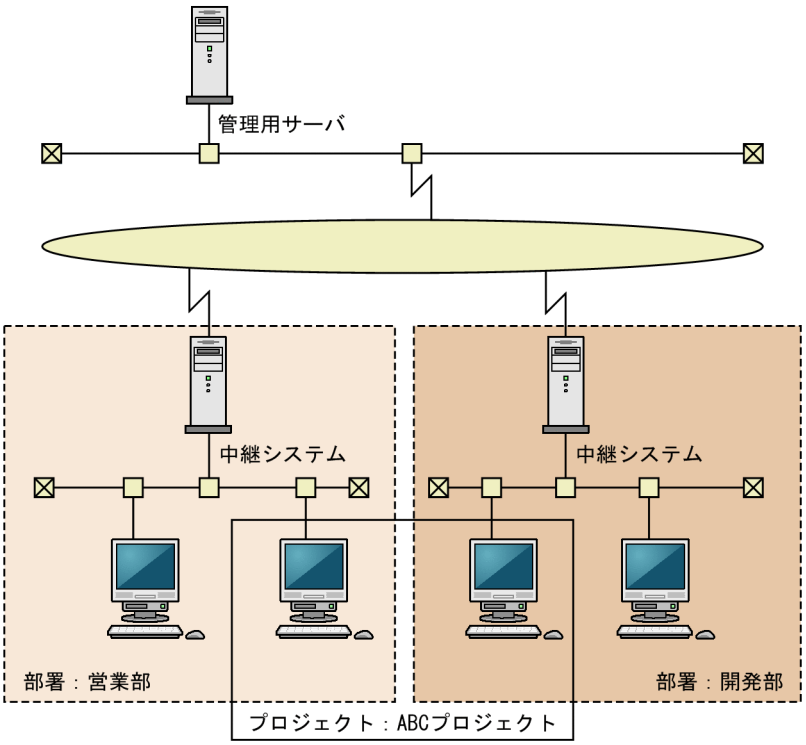
中継システムによる負荷分散

社内のネットワークが大規模である場合や、JP1/IT Desktop Management 2 で管理しているコンピュータの台数が多い場合は、中継システムを設置します。中継システムを設置することで、管理用サーバの負荷を軽減できます。

配布先のコンピュータのグルーピング

配布先のコンピュータを、目的に応じてグルーピングできます。コンピュータをグルーピングしておくと、配布先を一括で指定できます。コンピュータは、複数のグループに所属できます。

部署ごとのグループとプロジェクトごとのグループを設定した例を次の図に示します。



インストール条件の設定

配布先に指定したコンピュータのうち、設定した条件に一致するコンピュータだけにソフトウェアをインストールできます。条件は、パッケージング時またはジョブの作成時に設定して、ジョブの実行時に判定されます。

例えば、OS が Windows 7 のコンピュータにだけインストールするようにしたり、ハードディスクの空き容量が 5 ギガバイト以下のコンピュータにはインストールしないようにしたりできます。ハードウェアに関する条件だけではなく、特定のソフトウェアがインストールされているかどうかを条件に設定したり、ソフトウェアをインストールする前にシステム管理者が用意した外部プログラムを起動させることで、独自の条件を設定したりできます。

配布およびインストールの日時の設定

パッケージを配布する（データを転送する）日時と、コンピュータにソフトウェアをインストールする日時の 2 つを指定して配布できます。

パッケージを配布する日時

ジョブの作成時に、ジョブに対して実行日時を設定できます。例えば、ジョブの実行日時に夜間を設定すると、業務中に、ネットワークに負荷を掛けないでパッケージを配布できます。

コンピュータにソフトウェアをインストールする日時

パッケージング時またはジョブの作成時に、パッケージに対してインストールの実行タイミングを設定できます。実行タイミングを設定することで、配布先のコンピュータで、指定した日時に一斉にプログラムをインストールしたり、バージョンアップしたりできます。

パッケージの分割配布

パッケージを一度に配布しないで、指定した容量に分割して配布できます。分割したデータを転送する間隔（休止時間）も設定できるため、大容量のパッケージを配布する場合のネットワークの負荷を軽減できます。

マルチキャスト配布

通常のユニキャスト配布でパッケージを配布すると、配布先のコンピュータの台数が増加するほど、上位システム（管理用サーバや中継システム）から送信するパケット数が増加します。マルチキャストでパッケージを配布すると、ジョブ 1 つ分のパケット数の送信で済みます。パケットの送信量が削減されるため、ネットワークの負荷を軽減できます。

ジョブの中断と再開

ジョブを一時的に中断できます。例えば、業務停止中に配布する予定だったソフトウェアを業務停止中に配布できなかった場合、ジョブを中断することで配布を一時的に中断し、業務の再停止後に配布を再開できます。

配布先のコンピュータの制御

配布先のコンピュータが AMT または Wake on LAN に対応している場合は、配布先のコンピュータの電源を自動でオンにしたりオフにしたりできます。例えば、ネットワークの負荷が少ない深夜や休日に、電源がオフのコンピュータの電源をオンにして配布できます。

配布による負荷の軽減

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使用されるネットワーク帯域を制御することで、ネットワークの負荷を軽減できます。コンフィグレーションファイル（jdn_rim_distr_bwc.conf）で最大転送速度を設定すると、ネットワーク帯域が制御されて、設定した最大転送速度を上限としてデータが転送されます。1 秒間の送信の合計量が、設定した最大転送速度に達した場合、管理用サーバからのデータ転送が抑止されます。

コンフィグレーションファイル（jdn_rim_distr_bwc.conf）で最大転送速度を設定する方法については、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の配布時に使用されるネットワーク帯域を制御する手順についての説明を参照してください。

なお、最大転送速度の設定値が小さくて配布がタイムアウトになる場合は、次のように対処してください。

- 最大転送速度の設定値を大きくする。
- 同時に接続するエージェントの数を少なくする。
  詳細は、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の同時に接続するホストの台数の調整の説明を参照してください。

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

2.12.2 リモートインストールマネージャを使用したオフライン管理のコンピュータへの配布

ネットワークを経由しないで、オフライン管理のコンピュータにパッケージを配布できます。この機能を、オフラインインストールと呼びます。スタンドアロンのコンピュータに配布したい場合や、ネットワークに負荷を掛けないで容量の大きいパッケージを配布したい場合に便利です。

オフライン管理のコンピュータに配布するには、媒体（CD-R や USB メモリ）にパッケージやオフラインインストールに必要なデータを格納してから、配布先のコンピュータでインストール実行プログラムを実行します。

2.13 オンライン管理のコンピュータへのソフトウェアおよびファイルの配布（ITDM 互換配布）

組織内のコンピュータに新規にソフトウェアをインストールする場合や、利用を禁止しているソフトウェアをコンピュータからアンインストールする場合、管理者が各コンピュータの場所へ行って作業することは非常に手間が掛かります。

JP1/IT Desktop Management 2 では、オンライン管理のコンピュータに対して、ソフトウェアのインストールやアンインストール、ファイルの配布を管理用サーバからリモートで実行できる機能を提供しています。これによって、ソフトウェアの導入や管理に掛かる手間を省けます。また、最新バージョンのソフトウェアを一括でインストールできるなど、ソフトウェアの保守が簡単になります。

また、例えば、組織内のコンピュータに対して業務システムの更新ファイルを一斉適用したい場合、メール添付や利用者によるダウンロードでは、すべてのコンピュータに適用できたかどうかを確認できません。このような場合、JP1/IT Desktop Management 2 を利用してファイルを配布することで、配布状況を把握し確実に適用できるようになります。

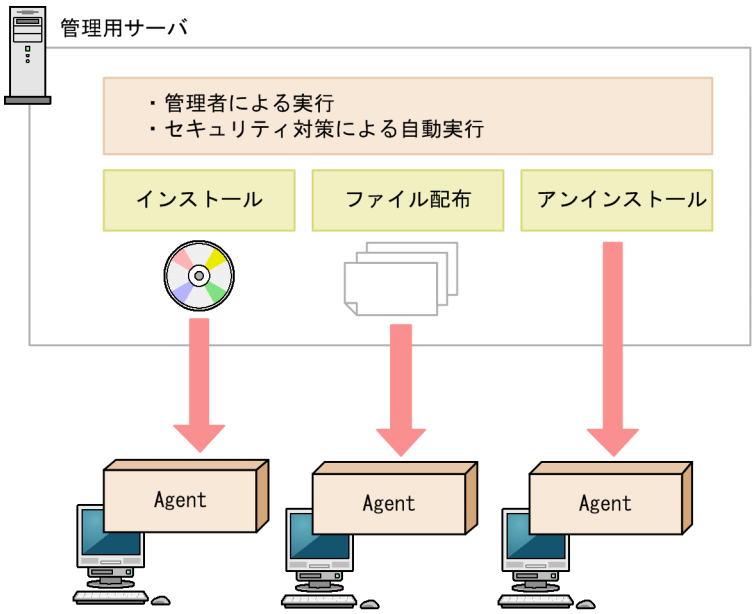
重要

API 管理機器にはソフトウェアおよびファイルの配布ができません。

複数サーバ構成の場合、ITDM 互換配布で配布の対象にできるのは、管理用サーバの直下のコンピュータだけです。配下のすべてのコンピュータを配布の対象にしたい場合は、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してください。また、UNIX エージェント、Mac エージェントに対しては ITDM 互換配布を使用できません。UNIX エージェント、Mac エージェントに対しては、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必要があります。

ヒント

配布機能を利用して、使用ソフトウェアに関するセキュリティの判定結果に基づいて、自動的に使用必須のソフトウェアをインストールしたり、使用禁止のソフトウェアをアンインストールしたりすることもできます。



（凡例）
Agent：JP1/IT Desktop Management 2 - Agent

ヒント

配布する機器の台数が多い場合は、複数回に分けてパッケージを配布することをお勧めします。配布する機器の台数が多い場合に管理用サーバからパッケージを一斉に配布すると、管理用サーバやネットワークに負荷が掛かるためです。

2.13.1　パッケージとタスクの管理（ITDM 互換配布）

対象のコンピュータにソフトウェアをインストールしたり、ファイルを配布したりするためのパッケージやタスクを JP1/IT Desktop Management 2 に登録して管理できます。

パッケージ（ITDM 互換配布用）とタスクの定義

- パッケージ（ITDM 互換配布用）

  ITDM 互換配布のパッケージとは、コンピュータに配布するためのソフトウェアまたはファイルを、操作画面で JP1/IT Desktop Management 2 に登録したものです。ITDM 互換配布のパッケージは、配布（ITDM 互換）画面の［パッケージ］画面で管理できます。この画面で管理しているパッケージは、配布（ITDM 互換）画面で配布するためのパッケージです。リモートインストールマネージャを使用して配布したい場合は、パッケージャでパッケージを作成する必要があります。

  ITDM 互換配布のパッケージとしてソフトウェアを登録した場合は、インストールコマンドを設定して、配布先のコンピュータにサイレントインストールできます。ITDM 互換配布のパッケージとしてファイルを登録した場合は、コンピュータに登録したファイルを配布できます。

  ITDM 互換配布のパッケージの管理については、「(1)　パッケージの管理」を参照してください。

- タスク

タスクとは、ITDM 互換配布のパッケージをコンピュータに配布したり、コンピュータからソフトウェアをアンインストールしたりするときの、実行スケジュールや対象コンピュータでの動作を指定したものです。タスクは、配布（ITDM 互換）画面の［タスク］画面で管理できます。

ITDM 互換配布のパッケージを配布するタスクを作成した場合は、実行スケジュールに従ってコンピュータにパッケージが配布されます。ソフトウェアをアンインストールするタスクを作成した場合は、実行スケジュールに従ってコンピュータからソフトウェアがアンインストールされます。

タスクの管理については、「(2)　タスクの管理」を参照してください。

パッケージ（ITDM 互換配布用）とタスクを利用してできること

- ソフトウェアのインストール

  配布（ITDM 互換）画面の［パッケージ］画面でインストールしたいソフトウェアを ITDM 互換配布のパッケージとして登録したあと、配布（ITDM 互換）画面の［タスク］画面でパッケージ配布タスクを作成してください。インストールウィザードを利用してもソフトウェアをインストールできます。

  ただし、Windows ストアアプリの場合、インストールタスクの登録はできますが、実際のインストールは実行されません。Windows ストアアプリをインストールするときは、対象のコンピュータで個別に実施してください。

- ファイルの配布

  配布（ITDM 互換）画面の［パッケージ］画面で配布したいファイルを ITDM 互換配布のパッケージとして登録したあと、配布（ITDM 互換）画面の［タスク］画面でパッケージ配布タスクを作成してください。ファイル配布ウィザードを利用してもファイルを配布できます。

- ソフトウェアのアンインストール

  配布（ITDM 互換）画面の［タスク］画面でアンインストールタスクを作成してください。アンインストールウィザードを利用してもソフトウェアをアンインストールできます。指定されたソフトウェア名とバージョンに完全に一致するソフトウェアをアンインストールします。

  ただし、Windows ストアアプリの場合、アンインストールタスクの登録はできますが、実際のアンインストールは実行されません。Windows ストアアプリをアンインストールするときは、対象のコンピュータで個別に実施してください。

関連リンク

- 2.13.3　配布のための準備（ITDM 互換配布）

(1)　パッケージの管理

配布（ITDM 互換）画面の［パッケージ］画面で、パッケージを作成して管理できます。

作成したパッケージは編集することもできます。登録したデータは変更できませんが、インストールコマンドや展開先フォルダなどを変更できます。

不要になったパッケージは削除することもできます。

配布したパッケージのアクセス権は、配布先フォルダから継承されます。配布したパッケージのアクセス権を変更したい場合は、配布先のコンピュータで利用者が変更する必要があります。

重要

配布したパッケージと同一ファイルが配布先に存在する場合、配布したパッケージのアクセス権は、既存ファイルのアクセス権を継承します。

パッケージに登録するファイル

作成するパッケージの種類に応じた、ファイルの指定方法を次の表に示します。

種類	パッケージに登録するファイル
ソフトウェアのインストール	インストールするソフトウェアが MSI ファイルまたは EXE ファイル単体の場合は、該当するファイルを登録します。
	MSI ファイルまたは EXE ファイルが複数ある場合や、MSI ファイルまたは EXE ファイル以外にインストールに必要なファイルがある場合は、ZIP ファイルに圧縮して登録します。なお、MSI ファイルまたは EXE ファイルの格納先は、ZIP ファイル内の任意の場所でかまいません。
ファイルの配布	ファイルを 1 つだけ配布したい場合は、該当するファイルを登録します。
	複数ファイルをまとめて配布したい場合は、ZIP ファイルに圧縮して登録します。

ヒント

パッケージに登録できるファイルのサイズは 1 ギガバイトまでです。ZIP ファイルの場合は、さらに解凍後のファイルサイズの合計が 2 ギガバイト以内である必要があります。

ファイルサイズが 2 ギガバイトを超える場合は、1 ギガバイト以内となるようにファイルを分割してから配布し、配布後に分割されたファイルを結合する運用としてください。

ヒント

インストールできるソフトウェアはサイレントインストールを実行できるソフトウェアだけです。サイレントインストールとは、利用者のコンピュータにインストール画面を表示しないで、自動的にインストールする方法のことです。MSI ファイルの場合、パッケージ作成時にサイレントインストールのコマンドが自動的に設定されます。EXE ファイルの場合、サイレントインストールのコマンドを手動で指定する必要があります。

ヒント

インストーラーを持たないソフトウェアは、ファイルとして配布してください。

ヒント

パッケージに ZIP ファイルを登録した場合、コンピュータにパッケージが配布されると ZIP ファイルは自動的に解凍されます。ZIP ファイルそのものを配布したい場合は、配布したい ZIP ファイルをさらに ZIP ファイルに圧縮してからパッケージに登録してください。

ヒント

更新プログラムを配布する場合のパッケージは、［パッケージ］画面には表示されません。

関連リンク

- 2.13.3　配布のための準備（ITDM 互換配布）

(2)　タスクの管理

配布（ITDM 互換）画面の［タスク］画面で、タスクを作成して管理できます。タスクには次の 2 種類があります。

パッケージ配布のタスク

ソフトウェアをインストールまたはファイルを配布するためのタスクです。また、このタスクで、更新プログラムおよび使用ソフトウェアの自動対策も実行されます。

アンインストールのタスク

ソフトウェアをアンインストールするためのタスクです。

作成したタスクは編集することもできます。タスクを編集することで、配布するパッケージやスケジュールはそのままにして配布先だけを変更したり、同じ宛先に対して配布するパッケージの設定を変更したりして実行できます。

また、同じ宛先に対して、複数のパッケージを配布したい場合や複数のソフトウェアをアンインストールしたい場合は、タスクをコピーすると便利です。

完了して不要になったタスクは削除することもできます。

タスクの配布先が 1 台の場合に対象のコンピュータが削除されると、タスク状態が完了になります。タスクの配布先が複数台の場合に対象のコンピュータが削除されると、その機器だけが配布先から削除されます。また、複数サーバ構成の場合に、対象のコンピュータが別の管理用サーバの配下に移動されたときも、削除されたときと同様に処理されます。

配布（ITDM 互換）画面の［タスク］画面では、タスクの実行状況が表示されます。配布に失敗したタスクは、原因を調査して再実行してください。

ヒント

次の場合、タスク一覧からタスクの情報は自動削除されます。

管理者が実行するタスク

・配布完了後 30 日経過した

・タスクの対象の機器台数が 0 件になった

自動対策で実行されるタスク

・配布完了後 7 日経過した

・タスクの対象の機器台数が 0 件になった

・セキュリティポリシーの自動対策の設定を解除した（更新プログラムまたは使用ソフトウェア）

タスクの種別

タスクの種別には、次の 2 種類があります。

管理者が実行するタスク

JP1/IT Desktop Management 2 の管理者によって、配布（ITDM 互換）画面の［タスク］画面で作成されたタスクです。

自動対策で実行されるタスク

セキュリティポリシーの自動対策の設定に基づいて自動で作成されたタスクです。詳細については、「2.13.2　セキュリティの自動対策による配布（ITDM 互換配布）」を参照してください。

関連リンク

- 2.13.3　配布のための準備（ITDM 互換配布）

2.13.2　セキュリティの自動対策による配布（ITDM 互換配布）

セキュリティポリシーの更新プログラム、使用必須ソフトウェア、および使用禁止ソフトウェアの自動対策で配布機能を利用できます。

更新プログラムを自動的に適用する

セキュリティポリシーの更新プログラムの適用を設定する際に、自動対策として更新プログラムの適用を設定できます。

自動対策で更新プログラムの配布を設定すると、セキュリティポリシーが適用されているコンピュータに更新プログラムが適用されていなかった場合に、自動的に更新プログラムが配布されて適用されます。

使用必須ソフトウェアを自動的にインストールする

セキュリティポリシーの使用必須ソフトウェアを設定する際に、自動対策としてソフトウェアのインストールを設定できます。

自動対策でソフトウェアのインストールを設定すると、セキュリティポリシーが適用されているコンピュータに使用必須ソフトウェアがインストールされていなかった場合に、自動的にソフトウェアが配布されてインストールされます。

ただし、Windows ストアアプリの場合、自動対策にインストールの設定はできますが、実際のインストールは実行されません。Windows ストアアプリをインストールするときは、対象のコンピュータで個別に実施してください。

使用禁止ソフトウェアを自動的にアンインストールする

セキュリティポリシーの使用禁止ソフトウェアを設定する際に、自動対策としてソフトウェアのアンインストールを設定できます。

自動対策でソフトウェアのアンインストールを設定すると、セキュリティポリシーが適用されているコンピュータに使用禁止ソフトウェアがインストールされていた場合に、自動的にソフトウェアがアンインストールされます。

ただし、Windows の［プログラムの追加と削除］に表示されないソフトウェアはアンインストールされません。このソフトウェアをアンインストールする場合は、［タスク］画面からアンインストールタスクを作成し、実行してください。アンインストールタスクの実行については、「2.13.1　パッケージとタスクの管理（ITDM 互換配布）」を参照してください。

また、Windows ストアアプリの場合、自動対策にアンインストールの設定はできますが、実際のアンインストールは実行されません。Windows ストアアプリをアンインストールするときは、対象のコンピュータで個別に実施してください。

セキュリティポリシー設定時に自動対策の更新プログラムの配布を設定した場合、更新プログラムファイルとタスクは自動的に作成されます。この場合、タスクは配布（ITDM 互換）画面の［タスク］画面に表示されます。ただし、更新プログラムファイルは［パッケージ］画面には表示されません。更新プログラムファイルが登録されているかは、セキュリティ画面の［更新プログラム］画面から確認してください。

ソフトウェアのインストールまたはアンインストールを設定した場合、セキュリティポリシーを指定するときにパッケージを設定し、タスクは自動的に作成されます。このとき、パッケージとタスクは、配布（ITDM 互換）画面の［パッケージ］画面と［タスク］画面に表示されます。

セキュリティポリシーの自動対策の設定時に作成したタスクのタスク種別は、「自動対策で実行されるタスク」です。自動対策で実行されるタスクは、編集やコピーはできません。また、タスクを削除する場合は、自動対策の設定を解除、またはセキュリティポリシーの使用ソフトウェアの設定を削除してください。セキュリティポリシーの設定に応じて、タスクが自動的に削除されます。

2.13.3　配布のための準備（ITDM 互換配布）

ソフトウェアのインストール、ファイルの配布およびソフトウェアのアンインストールを実行する前に必要な準備について説明します。配布機能を使用するに当たり、共通で準備しておくことと、実行する内容ごとの準備をそれぞれ説明します。

共通の準備

配布機能を使用する場合に、次の内容を検討しておきます。

配布先のコンピュータ

どのコンピュータに対して配布するかを検討しておきます。一度に配布する台数が多い場合は、該当するコンピュータのカスタムグループを作成しておくことをお勧めします。

配布スケジュール

配布を実行するスケジュールを検討しておきます。スケジュールを設定することで、業務に影響しないように夜間に配布したり、複数のタスクを同時に実行したりできます。スケジュールを設定しないですぐに実行することもできます。

自動起動の利用

コンピュータの電源が OFF だった場合に、自動的に電源を ON にして配布できます。夜間の配布や、利用されていないコンピュータへの配布をする場合に、利用を検討してください。なお、コンピュータの電源を制御するためには、AMT または Wake on LAN に対応している必要があります。

実行タイミング

タスクが対象のコンピュータに到達したあとで、ソフトウェアのインストールやアンインストール、ファイルの格納が実行されるタイミングを設定できます。タスク到達後にすぐに実行する、ユーザーがログオンしているときに実行する、コンピュータを次回起動したときに実行するのどれかを設定できます。例えば、業務で使用中のアプリケーションがインストールに干渉する場合、コンピュータを次回起動したときにインストールするように設定します。

表示するメッセージ

パッケージを配布したあと、ソフトウェアのインストール、ファイルの配布、アンインストールが実行される前後に、対象のコンピュータ上にメッセージを表示できます。インストールしたソフトウェアの注意事項や、インストールまたはアンインストールしたことを利用者に知らせたい場合に利用してください。

配布による負荷の軽減

配布機能で使用されるネットワーク帯域を制御することで、ネットワークの負荷を軽減できます。また、コンピュータにパッケージを配布する際の、時間当たりのデータ転送量に上限値を設けることで、エージェント側の通信がパッケージの転送だけで占有されることを防げます。詳細については、「2.13.7　配布による負荷の軽減（ITDM 互換配布）」を参照してください。

ソフトウェアをインストールするための準備

インストールしたいソフトウェアを準備します。インストールできるソフトウェアは、インストーラーが MSI ファイルまたは EXE ファイルのソフトウェアです。ソフトウェアのインストールに複数のファイルが必要な場合は、それらを ZIP ファイルに圧縮しておきます。ZIP ファイルに複数のインストーラーが含まれる場合、どのインストーラーを利用するか確認しておく必要があります。

ヒント

インストールできるソフトウェアはサイレントインストールを実行できるソフトウェアだけです。サイレントインストールとは、利用者のコンピュータにインストール画面を表示しないで、自動的にインストールする方法のことです。

ヒント

インストーラーを持たないソフトウェアは、ファイルとして配布してください。

ファイルを配布するための準備

配布するファイルを準備します。複数のファイルを配布する場合は、ZIP ファイルに圧縮しておきます。また、配布先でファイルが格納されるフォルダを検討しておきます。

ヒント

パッケージに ZIP ファイルを登録した場合、コンピュータにパッケージが配布されると ZIP ファイルは自動的に解凍されます。ZIP ファイルそのものを配布したい場合は、配布したい ZIP ファイルをさらに ZIP ファイルに圧縮してからパッケージに登録してください。

ヒント

ファイルの格納先は、配布対象のコンピュータで共通のフォルダを検討してください。配布先のコンピュータに指定したフォルダがない場合は、指定したフォルダが作成されます。

ファイルを配布する場合、配布後に配布先のコンピュータで任意のコマンドを自動実行できます。例えば、バッチファイルを実行するコマンドを設定すれば、バッチファイルを配布してそのまま実行できます。コマンドを使用する場合は、使用するコマンドが正しく実行されるかをあらかじめ検証するなどして準備しておきます。

ソフトウェアをアンインストールするための準備

アンインストールするソフトウェアの情報が、機器画面の［ソフトウェア情報］画面にあるかどうかを確認します。ない場合は、アンインストールするソフトウェアの実行ファイル名を確認しておきます。

ヒント

Windows の［プログラムと機能］に表示されないソフトウェアをアンインストールする場合、ソフトウェア検索条件（またはタスク作成時に指定したファイル名）によって検索された実行ファイル単体が削除されます。

ヒント

Windows の［プログラムと機能］に表示されるソフトウェアで、Windows インストーラー（MSI）でインストールされたものは、利用者のコンピュータにアンインストール画面を表示しないで自動的にアンインストール（サイレントアンインストール）できます。それ

以外のソフトウェアは、利用者のコンピュータにアンインストール画面を表示して、利用者自身にアンインストールしてもらいます。

関連リンク

- (1)　電源制御の条件

2.13.4　配布機能でアンインストールできるソフトウェアの種類（ITDM 互換配布）

配布機能を利用してアンインストールできるソフトウェアは、次の 2 種類です。

［プログラムと機能］に登録されているソフトウェア

Windows の［プログラムと機能］に登録されているソフトウェアです。

アンインストールコマンドが Windows Installer の場合は、サイレントオプション（/qn）および再起動抑止オプション（ReallySuppress）が指定されてアンインストールが実行されます。戻り値の判定は、次のとおりです。

- ERROR_SUCCESS(0)： 正常終了
- ERROR_SUCCESS_REBOOT_INITIATED(1641) ：再起動が必要
- ERROR_SUCCESS_REBOOT_REQUIRED(3010) ：再起動が必要
- その他のコード：異常終了

アンインストールコマンドが Windows Installer 以外の場合は、指定されたアンインストールコマンドが実行されます。アンインストールコマンドが実行されると、アンインストールが正常終了したと判定されます。

［ソフトウェア検索条件の設定］に登録したソフトウェア

設定画面－［ソフトウェア検索条件の設定］画面に登録した条件で、コンピュータ上から実行ファイル（exe ファイルなど）を検索して情報を収集したソフトウェアです。

2.13.5　配布時の注意事項（ITDM 互換配布）

配布機能を利用してソフトウェアをインストールまたはアンインストールする場合、評価用のテスト環境を準備してローカルシステムアカウント権限でソフトウェアが正常にインストールまたはアンインストールできることを検証してください。そのあとで、タスクの実行を計画してください。配布機能で利用するインストーラーの仕様は、JP1/IT Desktop Management 2 ではなくインストーラーの製造元が決定しており、製造元の作成した仕様に依存するためです。

ソフトウェアのインストール、ファイルの配布、およびソフトウェアをアンインストールする場合の注意事項を次に示します。

- EXE ファイルのソフトウェアを配布してインストールする場合、インストール後に再起動されない場合があります。
- インストールするソフトウェアが EXE ファイルの場合、インストーラーからの戻り値を判定できないため、インストール結果が正しく出力されないことがあります。
- インストールするソフトウェアで、EXE ファイルから別の MSI ファイルを起動して、インストールの結果を待たないで EXE ファイルが終了してしまう場合、インストール結果が正しく表示されないことがあります。
- 配布後に実行するコマンドによって、配布先以外にファイルが配布される場合、ファイル配布の結果が正しく表示されないことがあります。
- 管理用サーバとエージェント導入済みのコンピュータの時刻が異なっている場合、正常に電源を制御できないことがあります。
- アンインストールするソフトウェアが MSI ファイルの場合、サイレントアンインストールとして実行されます。EXE ファイルの場合は、コンピュータにダイアログが表示されます。ダイアログに従って、手動でアンインストールしてください。
- コントロールパネルの［プログラムと機能］からアンインストールできないソフトウェアや OS は、 アンインストールタスクに指定しないでください。指定した場合、アンインストールが失敗します。
- 次に示すソフトウェアおよびファイルはアンインストールしないでください。アンインストールすると、OS や JP1/IT Desktop Management 2 が正しく動作しなくなるおそれがあります。
  - OS の動作に関係するソフトウェアおよびファイル
  - JP1/IT Desktop Management 2 および JP1/IT Desktop Management 2 のコンポーネント
  - JP1/IT Desktop Management 2 の動作に関係するソフトウェアおよびファイル
- インストール時に特定のユーザー権限でファイルやフォルダが作成されるソフトウェアを、配布機能を利用してアンインストールした場合、一部のファイルやフォルダが削除されないときがあります。このとき、アンインストール後に、利用者がファイルやフォルダを削除する必要があります。
- インストール時にデスクトップにショートカットアイコンが作成されるソフトウェアを、配布機能を利用してアンインストールした場合、デスクトップのショートカットアイコンが削除されないときがあります。このとき、アンインストール後に、利用者がショートカットアイコンを削除する必要があります。
- セキュリティポリシーの使用必須ソフトウェアと使用禁止ソフトウェアに同じソフトウェアを指定して、インストールおよびアンインストールの自動対策を設定しないでください。この場合、常にどちらかのセキュリティ設定項目に違反しているため、インストールとアンインストールの自動対策が交互に繰り返されます。
- インストーラーおよびアンインストーラーのダイアログが表示された場合、1 時間経過すると、自動的にインストーラーおよびアンインストーラーは強制終了されます。
- 配布機能を利用してソフトウェアをインストールおよびアンインストールする場合、ローカルシステムアカウント権限で実行されます。また、配布機能を利用して、ファイル配布後にコマンドを実行する場合も、ローカルシステムアカウント権限で実行されます。

- 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インストールする場合、インストール結果は［タスク一覧］画面下部の［タスク情報］タブのリンクから［タスク状態の詳細］ダイアログを表示して確認してください。［詳細情報］に表示されるリターンコードが「0」の場合、インストールに成功しています。
- エージェントでの ITDM 互換配布は、エージェント上ではジョブと同時に実行できません。そのため、ジョブがエージェントで実行中のときは、ITDM 互換配布の状態が実行待ちのままになることがあります。
- Windows ストアアプリの場合、インストールタスクおよびアンインストールタスクの登録はできますが、実際のインストールおよびアンインストールは実行されません。Windows ストアアプリをインストール、アンインストールするときは、対象のコンピュータで個別に実施してください。
- Citrix XenApp、Microsoft RDS サーバに対して、実行タイミングに［ユーザーログオン時に実行］を指定したタスクを配布する場合、Citrix XenApp、Microsoft RDS サーバのローカルコンソールへログオンしている必要があります。
- 64 ビット版 OS でパッケージの配布（ITDM 互換）を行う場合、展開先フォルダ、配布先フォルダに%windir%¥system32 以下のディレクトリを指定すると、OS のリダイレクション機能によって%windir%¥SysWOW64 以下に配布されます。また、インストールコマンド、配布（ITDM 互換）後に実行するコマンドに%windir%¥system32 以下のファイルを指定しても、コマンドを起動できません。

2.13.6 パッケージが配布されたコンピュータでのダウンロードやインストールの延期（ITDM 互換配布）

パッケージが配布されたコンピュータでは、パッケージがダウンロードされて、パッケージに登録されたソフトウェアがインストールされます。

コンピュータの利用者は、都合に応じて、パッケージのダウンロードやソフトウェアのインストールを延期できます。急ぎの業務や重要な業務の最中は、ダウンロードやインストールを延期することで、作業が中断することを防げます。ダウンロードおよびインストールは、何度でも延期できます。

また、インストールの延期と同様に、アンインストールやファイルの配布も延期できます。

> **重要**
>
> リモートデスクトップ機能を使用してログオンしている場合は延期できません。

ダウンロードおよびインストールで延期できる時間を次に示します。

延期の内容	延期できる時間
ダウンロード	30 分間 30 分経過すると、ダウンロードが自動的に再開します。

延期の内容	延期できる時間
インストール	インストールを開始するダイアログを再表示するまでの時間を、次の中から利用者が指定します。 • 10 分後 • 30 分後 • 1 時間後

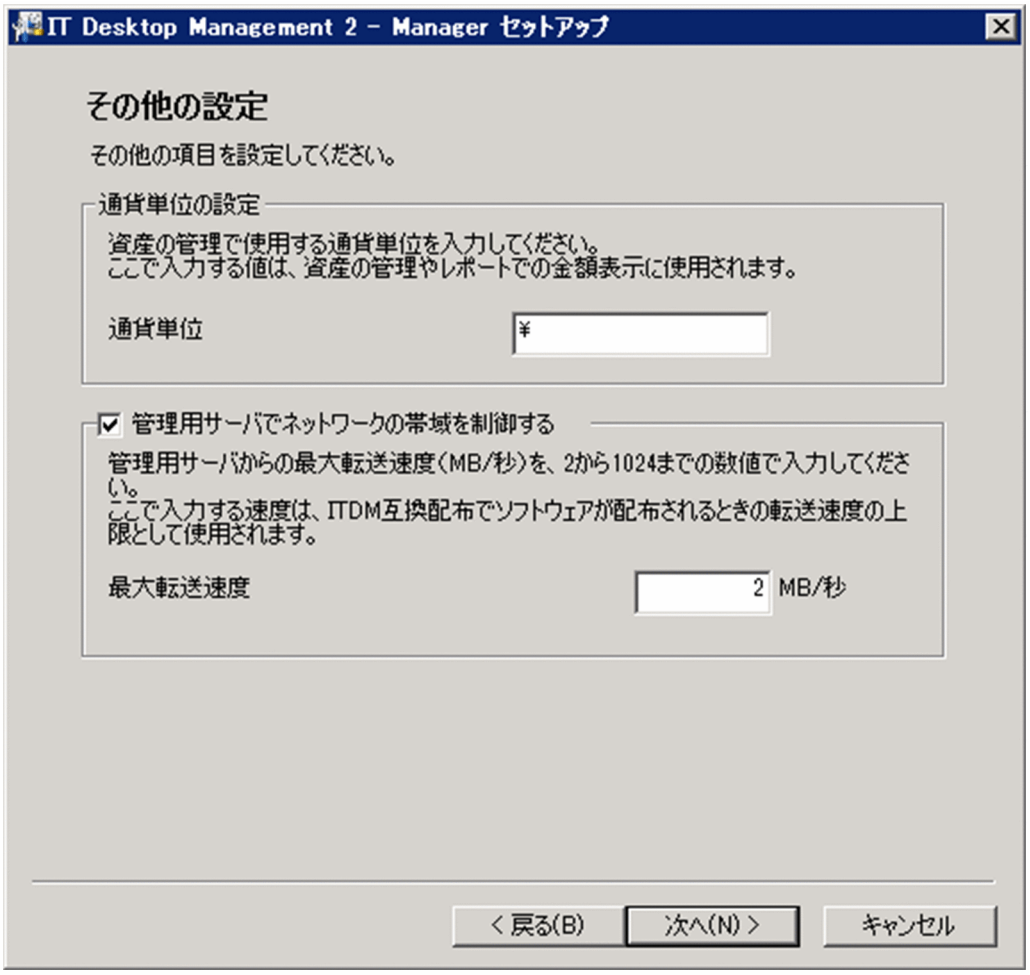
2.13.7 配布による負荷の軽減（ITDM 互換配布）

大容量のソフトウェアやファイルを管理用サーバから利用者のコンピュータに配布する場合、ネットワークやコンピュータに大きく負荷が掛かるおそれがあります。これを防ぐために、配布機能で使用されるネットワーク帯域を制御したり、時間当たりのデータ転送量に上限値を設けたりできます。

ネットワーク帯域を制御する

JP1/IT Desktop Management 2 のセットアップで最大転送速度を設定すると、ネットワーク帯域が制御されて、設定した転送速度の範囲内でデータが転送されます。最大転送速度とは、管理用サーバとエージェント導入済みのコンピュータで送受信するデータ転送速度の上限値です。1 秒間の送受信の合計量が、設定した最大転送速度に達した場合、管理用サーバ側のデータ転送が一時中断されます。これによって、ネットワークに大きく負荷を掛けることなくデータを転送できます。

最大転送速度は、管理用サーバのセットアップで設定できます。



時間当たりのデータ転送量に上限値を設定する

コンピュータにパッケージを配布する際の、時間当たりのデータ転送量に上限値を設定できます。これによって、コンピュータがパッケージのダウンロード間隔を調節しながらダウンロードを実行します。その結果、メール送受信などネットワークを利用する業務への影響を軽減できます。

データ転送量の上限値は、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］－［流量制御］で設定できます。

この項目は、JP1/IT Desktop Management の設定と互換性を保つために使用します。JP1/IT Desktop Management と同じ動作で運用したい場合を除いて、データ転送量の上限値は設定しないでください。設定した場合、ITDM 互換配布が遅延し、ソフトウェアや更新プログラムのインストールに時間が掛かったり、不要なソフトウェアのアンインストールに時間が掛かったりすることがあります。

2.13.8　配布されたパッケージのキャッシュ（ITDM 互換配布）

配布されたパッケージは、配布先のコンピュータに一時的にキャッシュされます。キャッシュされたパッケージは、ソフトウェアのインストールやファイルの配布が成功した場合だけコンピュータから削除されます。失敗した場合は、キャッシュされたパッケージが一定期間残ります。

タスクを再実行すると、パッケージが再送信されることなく、キャッシュされているパッケージを基にインストールやファイルの配布が実行されます。このように一度配布したパッケージがキャッシュされることで、ネットワークに掛かる負荷が軽減できます。

パッケージをキャッシュできる期間は 7 日間です。7 日間を過ぎると、キャッシュされたパッケージは削除されます。

パッケージのキャッシュには、エージェント導入済みのコンピュータのハードディスクの空き容量が、最低 1 ギガバイト必要です。また、キャッシュできるパッケージの容量は最大 2 ギガバイトです。

重要

次の場合、パッケージはキャッシュされません。

- 配布したパッケージが壊れている場合
- 配布先コンピュータのハードディスクの空き容量が 1 ギガバイト未満の場合
- パッケージの容量が 2 ギガバイトを超える場合

2.13.9 利用者がログオフしている場合のタスク実行（ITDM 互換配布）

配布先のコンピュータの利用者がログオフしていても、パッケージを配布したり、インストールしたりできます。また、配布先のコンピュータの電源が OFF になっている場合、配布時に電源を ON にしたり、配布後に電源を OFF にしたりすることもできます。

エージェント導入済みのコンピュータがログオフしている場合のタスクの実行処理について、次の表に示します。

項目	実行の可否
パッケージの配布	○ ※
インストール	
アンインストール	
配布先のコンピュータの電源 ON および OFF	
配布先のコンピュータの再起動	
タスクの実行前および実行後のメッセージ表示	×
ダウンロードの延期	
インストールの延期	

（凡例）○：実行される　×：実行されない

注※　EXE ファイルを使用したアンインストールの場合、利用者がログオンしていないコンピュータからは、アンインストールできません。

関連リンク

- 2.13.10　配布機能での電源制御（ITDM 互換配布）

2.13.10　配布機能での電源制御（ITDM 互換配布）

パッケージ配布タスクの設定で、配布先のコンピュータの自動起動を有効にすると、配布先のコンピュータの電源が OFF の場合でも、電源を ON にしてパッケージを配布できます。これによって、利用者がいない夜間などでもパッケージを配布できます。

配布時に、配布先のコンピュータの電源を ON にするには、タスクの作成時に［対象のコンピュータが稼働していない場合に起動する］をチェックしてください。

ヒント

タスクの作成時に［タスク実行後、自動起動したコンピュータだけをシャットダウンする］を選択した場合、タスクを実行した時刻からコンピュータの電源が ON になった時刻の差が 1 時間以内のときは、シャットダウンを要求するダイアログが出るので、配布完了後にコンピュータを自動的にシャットダウンします。

重要

配布先のコンピュータの電源を制御するためには、AMT または Wake on LAN に対応している必要があります。

重要

すでに配布先のコンピュータの電源が ON になっている場合に、［対象のコンピュータが稼働していない場合に起動する］をチェックすると、パッケージ配布後にシャットダウンまたは再起動を予告するダイアログが配布先のコンピュータの画面に表示されます。

［対象のコンピュータが稼働していない場合に起動する］のチェックの有無	配布後コンピュータの再起動の要否	コンピュータの起動	コンピュータの起動とタスク実行のタイミング	コンピュータの動作※
あり（［タスク実行後、自動起動したコンピュータだけをシャットダウンする］を選択）	不要	すでにコンピュータが起動されている	－	パッケージをダウンロードする
		利用者がコンピュータを起動する	タスクの実行よりもコンピュータの起動が先	パッケージをダウンロード後、シャットダ

［対象のコンピュータが稼働していない場合に起動する］のチェックの有無	配布後コンピュータの再起動の要否	コンピュータの起動	コンピュータの起動とタスク実行のタイミング	コンピュータの動作※
あり（［タスク実行後、自動起動したコンピュータだけをシャットダウンする］を選択）	不要	利用者がコンピュータを起動する	タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間以内	ウンを予告するダイアログが表示される
			タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間を超過	パッケージをダウンロードする
		タスク実行時にコンピュータが自動起動される	タスクの実行よりもコンピュータの起動が先	パッケージをダウンロード後、シャットダウンを予告するダイアログが表示される
			タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間以内	
			タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間を超過	パッケージをダウンロードする
		利用者がコンピュータを再起動する	タスクの実行よりもコンピュータの起動が先	パッケージをダウンロード後、シャットダウンを予告するダイアログが表示される
			タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間以内	
			タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間を超過	パッケージをダウンロードする
	必要	すでにコンピュータが起動されている	－	パッケージをダウンロード後、再起動を予告するダイアログが表示される
		利用者がコンピュータを起動する	タスクの実行よりもコンピュータの起動が先	パッケージをダウンロード後、シャットダウンを予告するダイアログが表示される
			タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間以内	
			タスクが実行されてから、コンピュータが起	パッケージをダウンロードする

［対象のコンピュータが稼働していない場合に起動する］のチェックの有無	配布後コンピュータの再起動の要否	コンピュータの起動	コンピュータの起動とタスク実行のタイミング	コンピュータの動作※
あり（［タスク実行後、自動起動したコンピュータだけをシャットダウンする］を選択）	必要	利用者がコンピュータを起動する	動されるまでの差が 1 時間を超過	パッケージをダウンロードする
		タスク実行時にコンピュータが自動起動される	タスクの実行よりもコンピュータの起動が先	パッケージをダウンロード後、シャットダウンを予告するダイアログが表示される
			タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間以内	
			タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間を超過	パッケージをダウンロード後、再起動を予告するダイアログが表示される
		利用者がコンピュータを再起動する	タスクの実行よりもコンピュータの起動が先	パッケージをダウンロード後、シャットダウンを予告するダイアログが表示される
			タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間以内	
			タスクが実行されてから、コンピュータが起動されるまでの差が 1 時間を超過	パッケージをダウンロードする
	－	すでにコンピュータが起動されている	－	パッケージをダウンロード後、シャットダウンを予告するダイアログが表示される
		利用者がコンピュータを起動する		
		タスク実行時にコンピュータが自動起動される		
		利用者がコンピュータを再起動する		
あり（［タスク実行後、すべての対象のコンピュータをシャットダウンする］を選択）	－	すでにコンピュータが起動されている	－	パッケージをダウンロード後、シャットダウンを予告するダイアログが表示される
		利用者がコンピュータを起動する		
		タスク実行時にコンピュータが自動起動される		

[対象のコンピュータが稼働していない場合に起動する] のチェックの有無	配布後コンピュータの再起動の要否	コンピュータの起動	コンピュータの起動とタスク実行のタイミング	コンピュータの動作※
あり（[タスク実行後、すべての対象のコンピュータをシャットダウンする] を選択）	－	利用者がコンピュータを再起動する	－	パッケージをダウンロード後、シャットダウンを予告するダイアログが表示される
なし	不要	すでにコンピュータが起動されている	－	パッケージをダウンロードする
		利用者がコンピュータを起動する	－	
		利用者がコンピュータを再起動する	－	
	必要	すでにコンピュータが起動されている	－	パッケージをダウンロード後、再起動を予告するダイアログが表示される
		利用者がコンピュータを起動する	－	
		利用者がコンピュータを再起動する	－	

（凡例）－：該当なし

注※　管理用サーバの時刻と配布先のコンピュータの時刻に差異があると、異なった動作をする場合があります。

2.13.11　配布機能でのソフトウェアのインストール実行結果の判定（ITDM 互換配布）

配布機能によるソフトウェアのインストールが成功したかどうかは、パッケージに設定されたインストールコマンドの実行結果を基に判定されます。パッケージに登録したファイルの形式ごとに、判定方法を示します。

MSI ファイルの場合

Windows Installer の戻り値に応じて、インストールの実行結果が判定されます。戻り値の判定は、次のとおりです。

- ERROR_SUCCESS(0)： 正常終了
- ERROR_SUCCESS_REBOOT_INITIATED(1641) ：再起動が必要
- ERROR_SUCCESS_REBOOT_REQUIRED(3010) ：再起動が必要
- その他のコード：異常終了

その他の形式のファイルの場合

パッケージに設定されたインストールコマンドが実行されると、インストールが正常終了したと判定されます。

なお、インストールコマンドの起動が失敗した場合や、インストールコマンドの起動または起動したインストーラーでタイムアウトが発生した場合は、インストールに失敗したと判定されます。

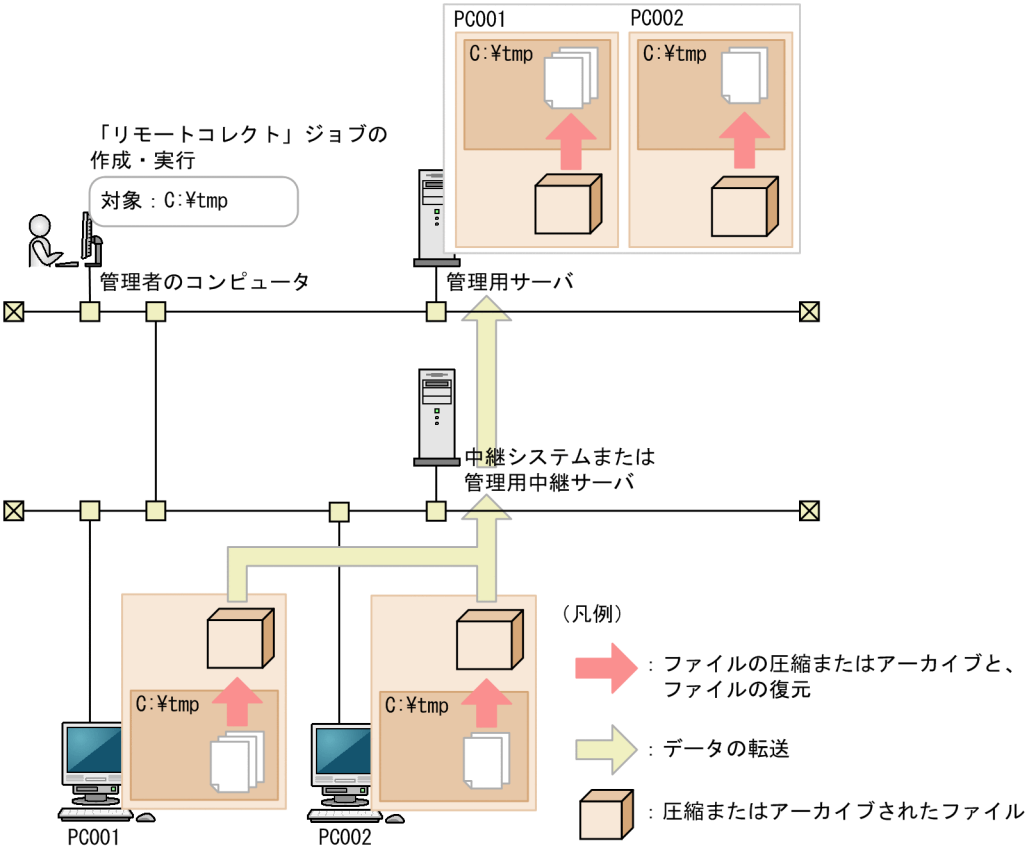
2.14　リモートインストールマネージャを使用したファイルの収集

リモートコレクト機能を利用すると、次のような運用ができます。

- 管理者の業務に必要な利用者の業務データを、一括で収集する
- 利用者のコンピュータで利用しているソフトウェアのトラブル情報やログ情報を収集して解析することで、利用者のトラブルシューティングを支援する

> **重要**
>
> API 管理機器はリモートインストールマネージャを使用したファイルの収集ができません。

リモートコレクトの概要を次の図に示します。



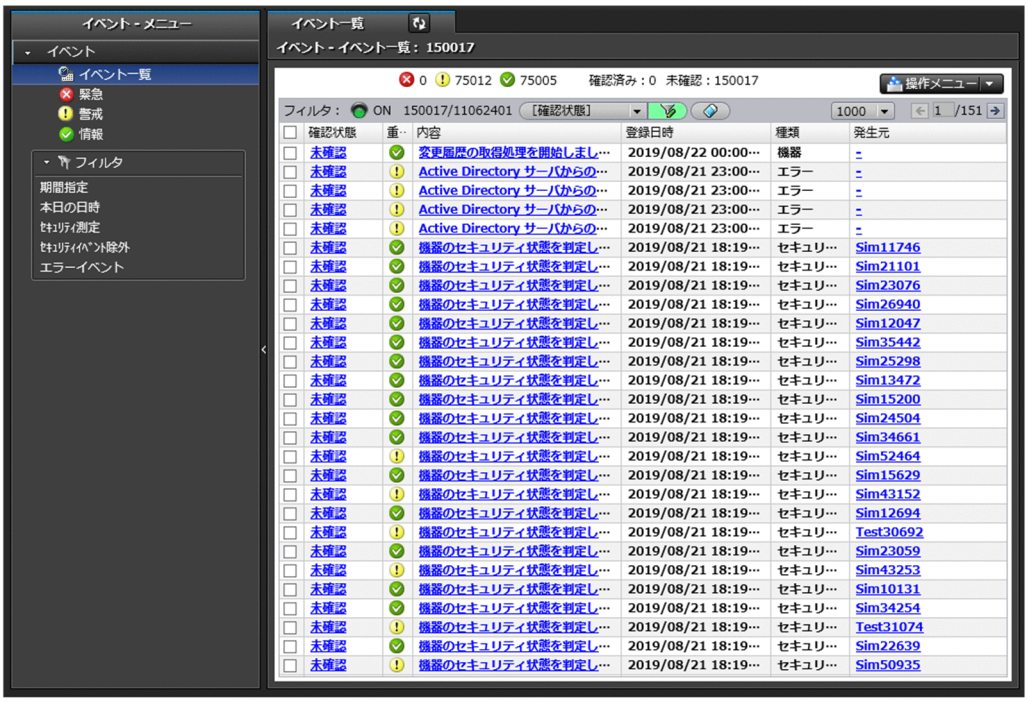
リモートコレクトするには、リモートインストールマネージャでリモートコレクトのジョブを作成して実行します。収集の対象としたファイルは、圧縮またはアーカイブされた状態で管理用サーバに転送されます。圧縮またはアーカイブされたファイルを復元するには、JP1/IT Desktop Management 2 - Manager のコンポーネントであるアンアーカイバを使用します。

なお、Mac エージェントに対しては、リモートインストールマネージャを使用したファイルの収集はできません。

中継システムを設置すると、リモートコレクトによるネットワークの負荷を軽減できます。

2.15　イベントの表示

JP1/IT Desktop Management 2 の運用中に、早急な対処が必要な事象が発生した場合、その事象がイベントとして出力されます。このほかに、各種機能の処理結果なども出力されます。管理者は、イベントを確認することで JP1/IT Desktop Management 2 の運用中に発生した事象を把握できます。



2.15.1　出力されるイベント

JP1/IT Desktop Management 2 の運用中に、機器の発見、資産の登録、セキュリティポリシーの判定など、何らかの事象が起きるとイベントが出力されます。出力されたイベントはイベント画面で確認できます。

イベントは、その内容によって次の 3 つの重大度に分けられます。

（緊急）

すぐに対策が必要なイベントです。イベントの内容を確認して早急に対策してください。

（警戒）

すぐに対策する必要はありませんが、いつかは対策が必要なイベントです。イベントの内容を確認して、必要に応じて対策してください。

（情報）

システムの処理結果に関するイベントです。対策は不要です。

イベントの内容によっては早急に対処が必要な場合があります。重大度が「緊急」、「警戒」の優先順位でイベントを確認し、エラーの内容から原因を特定して対処してください。ホーム画面の［イベントの状況］

パネルですべてのイベントの個数と、イベント種類ごとの個数を把握できます。また、ダイジェストレポートで未確認のイベントの個数を把握できます。

なお、イベントが発生したら、管理者にメールで通知するように設定できます。

ヒント

表示されるイベントの最大数は、管理対象のコンピュータ数×250 + 10,000 で算出されます。イベントの発生件数がこの値を超えた場合、古いイベントから順に上書きされます。過去のイベントを保存しておきたい場合は、バックアップを取得してください。

関連リンク

- 2.15.2　イベントの種類

2.15.2　イベントの種類

出力されるイベントの種類について説明します。

機器
: 機器情報やソフトウェア情報の追加と削除、コンピュータのアカウントの追加と削除など、機器管理に関するイベントです。

セキュリティ
: セキュリティポリシーの変更と割り当て、セキュリティポリシーの判定結果、アクションの結果、起動抑止など、セキュリティ管理に関するイベントです。

資産
: 資産の登録、資産の状態の変更、ソフトウェアライセンスの追加と削除など、資産管理に関するイベントです。

配布（ITDM 互換）
: ソフトウェアのインストール、ファイルの配布、ソフトウェアのアンインストールなど、配布に関するイベントです。

設定
: 機器の発見、管理対象の追加、エージェントの配信など、設定に関するイベントです。

不審操作
: 添付ファイル付きメールの検知、Web サーバ/FTP サーバへのファイルアップロードの検知、外部メディアへのファイルコピー・移動の検知など、不審操作に関するイベントです。

中継
: 管理用サーバ間でのデータの中継に関するイベントです。複数サーバ構成で運用している場合にだけ出力されるイベントの種類です。

API

API に関するイベントです。

エラー

各機能で発生したエラーに関するイベントです。

2.15.3 イベントの形式

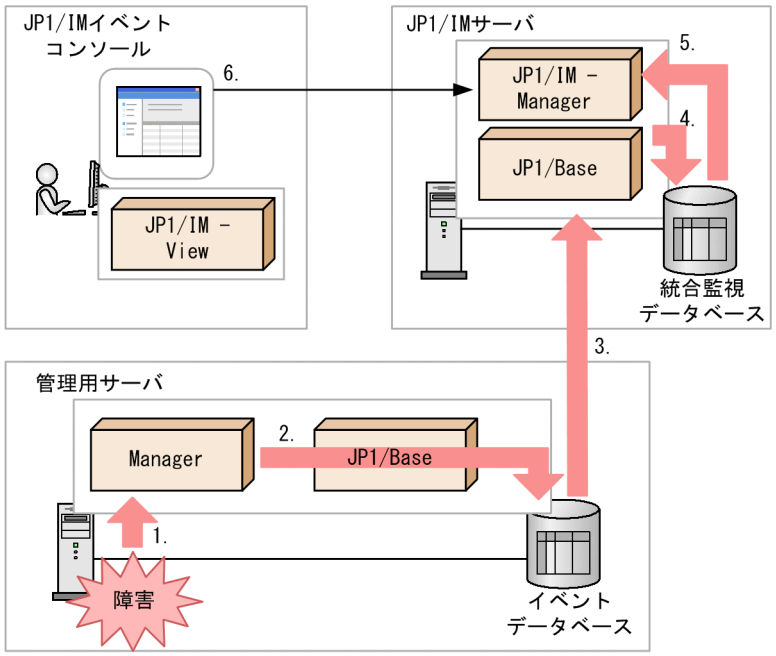
項目	説明
確認状態	イベントの確認状態です。クリックすると状態が切り替わります。 • 未確認 • 確認済み
重大度	イベントの重大度です。次のどれかが表示されます。 • 緊急 すぐに対策が必要なイベントです。 • 警戒 すぐに対策する必要はありませんが、いつかは対策が必要なイベントです。 • 情報 システムの処理結果に関するイベントです。対策は不要です。
登録日時	管理用サーバにイベントが登録された日時が表示されます。
種類	イベントの種類です。次のどれかが表示されます。 • 機器 • セキュリティ • 資産 • 配布（ITDM 互換） • 設定 • 不審操作 • 中継 • エラー
イベント番号	イベントの内容に応じた識別番号が表示されます。
発生元	イベントの対象を特定する情報です。イベントの発生した機器やセキュリティポリシーなどが表示されます。
内容	イベントの詳細情報が表示されます。

2.15.4 JP1/IM のイベントコンソールでのイベントの確認

JP1/IM と連携して、管理対象のコンピュータ（Mac OS 以外）で発生した障害系イベントや管理者の判断が必要な重要イベントを、JP1/IM のイベントコンソールで監視できます。

JP1/IT Desktop Management 2 では、JP1/Base の機能を使用して、管理対象のコンピュータ（Mac OS 以外）で障害が発生したときに JP1 イベントを発行できます。JP1/IM と連携することで、発行された JP1 イベントを JP1/IM のイベントコンソールでタイムリーに監視したり、ほかの JP1 製品などのプログラムを同じ画面で監視したりできます。

JP1/IM のイベントコンソールでイベントを確認する場合のイベントの流れを次の図に示します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager

：イベントの流れ

1. JP1/IT Desktop Management 2 - Manager で障害が発生すると、JP1/IT Desktop Management 2 - Manager にイベントが通知されます。
2. JP1/IT Desktop Management 2 - Manager に通知されたイベントが、JP1 イベントとして JP1/Base のイベントデータベースに登録されます。
3. イベントデータベースに登録された JP1 イベントは、JP1/IM - Manager がある JP1/IM サーバに転送されます。
4. JP1/IM サーバに転送された JP1 イベントは、JP1/IM の統合管理データベースに登録されます。
5. JP1/IM - Manager が統合管理データベースから JP1 イベントを取得します。
6. 取得した JP1 イベントが、JP1/IM のイベントコンソールに表示されます。

JP1/IM のイベントコンソールに出力できるイベントについては、マニュアル「JP1/IT Desktop Management 2 運用ガイド」を参照してください。

2.16　レポートの表示

JP1/IT Desktop Management 2 では、管理している情報を目的別に集計できるレポート機能を提供しています。管理者は、必要に応じてレポートを参照し各種作業の起点として利用したり、印刷して状況報告に利用したりできます。

レポートには、次に示す 5 種類のカテゴリがあります。

- ダイジェストレポート

  管理している情報全体の概況をグラフや一覧で確認できます。現在の状況と今後の予定を確認して、今後の作業計画を立てるために利用できます。

- セキュリティ診断レポート

  セキュリティに関する総合評価、およびカテゴリ別の評価をグラフで確認できます。一覧には、グループ単位の評価レベルと評価ポイントも表示されるので、グループ単位のセキュリティ状況を確認できます。セキュリティの概況を報告する際に利用できます。

- セキュリティ詳細レポート

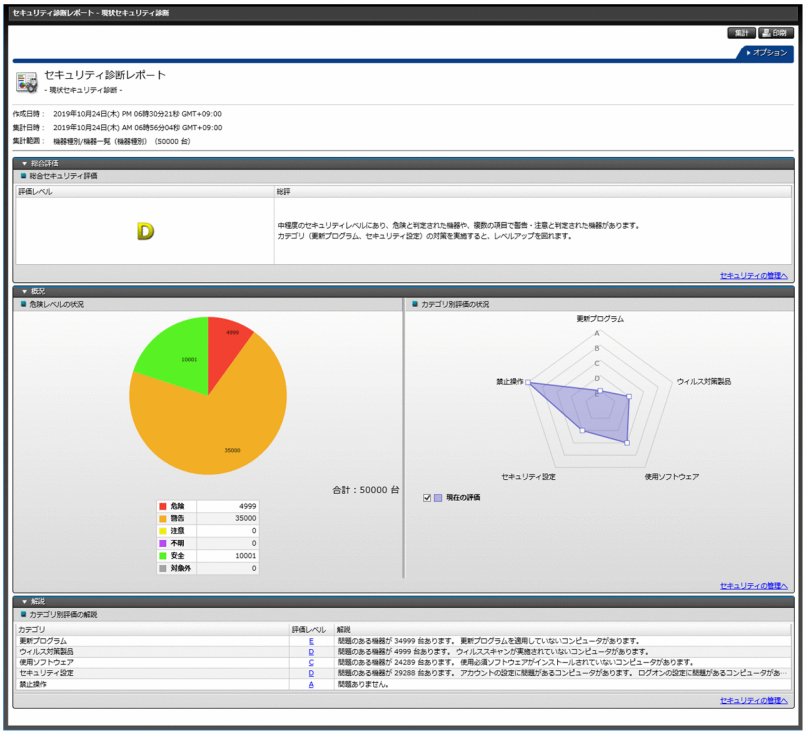
  セキュリティ状況の詳細をグラフや一覧で確認できます。問題のあるコンピュータを特定したり、問題点の詳細を確認したりできるため、セキュリティ対策の起点として利用できます。

- 機器詳細レポート

  管理対象の機器の台数、各コンピュータの省電力の設定状況などを確認できます。特定部署内の台数の内訳やグリーン IT への取り組み状況を把握するために利用できます。

- 資産詳細レポート

  管理対象のハードウェア資産の台数の推移、契約費用の推移、ソフトウェアライセンスの状況を確認できます。資産の数や費用の傾向を把握したり、ソフトウェアライセンスの利用状況を把握するために利用できます。



2.16.1 レポートの参照

レポート画面では、目的に応じて 20 種類のレポートを参照できます。各レポートは、印刷したり CSV ファイルに出力したりできます。複数サーバ構成の場合、レポートには自サーバの保有する情報を集計した結果が出力されます。表示できるレポートを次の表に示します。

カテゴリ	種類	集計範囲へのグループの適用※
ダイジェストレポート	日刊ダイジェスト	×
	週刊ダイジェスト	×
	月刊ダイジェスト	×
セキュリティ診断レポート	現状セキュリティ診断	○
	期間指定セキュリティ診断	○
セキュリティ詳細レポート	危険レベルの状況	○
	更新プログラムの適用状況	○
	ウィルス対策製品の状況	○
	使用必須ソフトウェアのインストール状況	○
	使用禁止ソフトウェアのインストール状況	○
	セキュリティ設定の状況	○
	禁止操作の状況	×

カテゴリ	種類	集計範囲へのグループの適用※
セキュリティ詳細レポート	ユーザーの活動状況	×
機器詳細レポート	機器の管理状況	○
	グリーン IT（省電力設定状況）	○
資産詳細レポート	ハードウェア資産	○
	ハードウェア資産の費用	○
	ソフトウェアライセンスの費用	○
	その他の費用	○
	ライセンス超過ソフトウェア	○
	ライセンス余剰ソフトウェア	○

（凡例）○：適用できる　×：適用できない

注※　レポートの集計範囲に、ユーザー定義のグループは適用できません。

各レポートの概要と活用方法を説明します。

ダイジェストレポート

管理する情報全体の概況を確認できます。現在の状況と今後の予定を確認して、今後の作業計画を立ててください。

日刊ダイジェスト

イベントの発生状況、状態を変更する予定の資産数、ソフトウェアライセンスの状況、配布の実行状況などを、日単位で確認できます。また、データベースの空き容量の現状が表示されます。現在の状況と今後の予定を確認して、日次の作業計画を立てたい場合に活用できます。

週刊ダイジェスト

イベントの発生状況、状態を変更する予定の資産数、ソフトウェアライセンスの状況、配布の実行状況などが、週単位で確認できます。イベントの発生状況は、1 週間の件数の推移が表示されます。現在の状況と今後の予定を確認して、週次の作業計画を立てたい場合に活用できます。

月刊ダイジェスト

イベントの発生状況、状態を変更する予定の資産数、ソフトウェアライセンスの状況、配布の実行状況などを、月単位で確認できます。イベントの発生状況は、1 か月の件数の推移が表示されます。また、資産の運用に掛かるコストの実績と予定が表示されます。現在の状況と今後の予定を確認して、月次の作業計画を立てたい場合に活用できます。

セキュリティ診断レポート

セキュリティに関する総合評価、およびカテゴリ別の評価を確認できます。

現状セキュリティ診断

現在のコンピュータのセキュリティ状況を総合的に評価した結果が表示されます。管理しているコンピュータ全体のセキュリティ状況を確認し、評価が低い項目の対策を検討する場合に活用できます。

期間指定セキュリティ診断

指定した期間のコンピュータのセキュリティ状況を総合的に評価した結果が表示されます。診断結果の推移を確認して、セキュリティ状況の傾向を確認する場合に活用できます。

> **メモ**
>
> ［解説］に表示される機器数には、当該期間で集計された［問題のある機器数］の述べ数を表示しています。

セキュリティ詳細レポート

セキュリティ状況の詳細を確認できます。

危険レベルの状況

危険レベルの状況、および各グループのセキュリティ状況が表示されます。このレポートでコンピュータの危険レベルを確認し、セキュリティ対策がより強固になるように対策を実施する場合に活用できます。

更新プログラムの適用状況

セキュリティポリシーで設定した更新プログラムが適用されていないコンピュータの台数、および各グループの状況が表示されます。更新プログラムが適用されていないコンピュータに対して、更新プログラムを漏れなく適用させる場合に活用できます。

ウィルス対策製品の状況

ウィルス対策を実施していないコンピュータの台数、および各グループの状況が表示されます。ウィルス対策の設定の見直しや更新を指示する場合に活用できます。

使用必須ソフトウェアのインストール状況

セキュリティポリシーで設定した使用必須ソフトウェアがインストールされていないコンピュータの台数、および各グループの状況が表示されます。使用必須ソフトウェアをインストールさせたい場合に活用できます。

使用禁止ソフトウェアのインストール状況

セキュリティポリシーで設定した使用禁止ソフトウェアがインストールされているコンピュータの台数、および各グループの状況が表示されます。使用禁止ソフトウェアのアンインストールを指示する場合に活用できます。

セキュリティ設定の状況

不正アクセスが発生するおそれがあるコンピュータの台数、ユーザー定義のセキュリティ設定の観点で問題があるコンピュータの台数、および各グループの状況が表示されます。どのセキュリティ対策に問題があるかを把握し、各コンピュータに適切なセキュリティ対策を行う場合に活用できます。

禁止操作の状況

印刷の抑止、ソフトウェアの起動の抑止、およびデバイスの使用の抑止が発生したコンピュータの情報が、抑止回数が多い順に表示されます。抑止回数が多い利用者を確認して注意したい場合に活用できます。

ユーザーの活動状況

印刷を実行したコンピュータの情報、およびUSBデバイスを使用したコンピュータの情報が、回数が多い順に表示されます。印刷やUSBデバイスの利用によって情報持ち出しのおそれのあるコンピュータを調査する場合に活用できます。

複数サーバ構成の場合で、下位の管理用中継サーバが操作ログの上位通知を有効にしているときは、下位の管理用中継サーバ配下のコンピュータの操作ログおよび不審操作もレポートに集計されます。

> **メモ**
>
> 業務分掌（部門の管轄範囲）を指定する場合、管理の必要がある機器が存在する部署に対して、管理者（ユーザ）を割り当てる運用を想定しています。セキュリティレポートの集計情報は機器ごとに集計されています。業務分掌（部門の管轄範囲）は部署を指定するため、セキュリティレポートの集計も部署ごとに表示します。セキュリティレポートの表示はレポートの集計情報が存在する部署に限定しており、部署のセキュリティレポートの集計情報がないと表示しません。

機器詳細レポート

管理している機器の台数、各コンピュータの省電力の設定状況などを確認できます。

複数サーバ構成の場合、自サーバの配下の管理用中継サーバで管理している機器の台数もレポートに集計されます。

機器の管理状況

管理している機器の台数や、機器の台数の増減などが表示されます。OS別に機器の増減を把握したり、特定部署内の機器の内訳を把握したりする場合に活用できます。

グリーンIT（省電力設定状況）

管理しているコンピュータの省電力の設定状況から、理想とする消費電力量との差異が表示されます。コンピュータの消費電力を減らしたい場合や、グリーンITの取り組み状況を知りたい場合に活用できます。

資産詳細レポート

管理しているハードウェア資産の台数の推移、契約費用の推移、ソフトウェアライセンスの状況を確認できます。

ハードウェア資産

管理しているハードウェア資産の台数の推移が、機器種別ごとに表示されます。年間を通じての台数の推移の傾向や、機器種別ごとの台数の割合を把握する場合に活用できます。

ハードウェア資産の費用

ハードウェア資産について、年間の費用の推移が表示されます。年間を通じての契約費用の推移の傾向を把握したり、契約費用が適切かどうかを判断したりする場合に活用できます。過去の契約費用を変更した場合、変更内容をすぐに反映して表示します※。

ソフトウェアライセンスの費用

ソフトウェアライセンスについて、年間の費用の推移が表示されます。年間を通じての契約費用の推移の傾向を把握したり、契約費用が適切かどうかを判断したりする場合に活用できます。過去の契約費用を変更した場合、変更内容をすぐに反映して表示します※。

その他の費用

ハードウェア資産およびソフトウェアライセンス以外の契約について、年間の費用の推移が表示されます。年間を通じての契約費用の推移の傾向を把握したり、契約費用が適切かどうかを判断したりする場合に活用できます。過去の契約費用を変更した場合、変更内容をすぐに反映して表示します。

ライセンス超過ソフトウェア

ソフトウェアライセンスが不足しているソフトウェアの情報が、超過数が多い順に表示されます。このレポートに表示されているソフトウェアは、ソフトウェアライセンスが不足して、ライセンス違反となっているおそれがあります。ソフトウェアライセンスの利用状況を確認し、必要に応じてライセンスを追加購入するなどの対策を検討するために活用できます。

ライセンス余剰ソフトウェア

ソフトウェアライセンスが余っているソフトウェアの情報が、余剰数が多い順に表示されます。ソフトウェアライセンスを購入する前にこのレポートを確認することで、購入が不要なものを把握するために活用できます。

注※　過去の契約費用を変更しても前月分に集計した費用を表示するようにもできます。

2.16.2　セキュリティ診断レポートの評価の算出方法

[セキュリティ診断レポート] には、機器のセキュリティ状況の判定結果を集計し、分析、診断した結果が表示されます。セキュリティ状況の総合評価に加え、ウィルス対策状況やセキュリティ設定などのカテゴリ別の評価、評価推移などが表示されます。

セキュリティ診断レポートに表示される各評価は、A～E の 5 段階です。A が最も安全な状態で、E に近づくほど危険な状態になります。この評価は、セキュリティの判定結果に基づく機器ごとのポイントによって決まります。ポイントは、すべて安全な状態は 100 ポイントになり、各セキュリティ判定項目の判定結果に応じて減点されていきます。ポイントの平均値が高くても、危険なコンピュータが判定期間中に 1 台でもあれば評価は低くなります。

セキュリティ診断レポートでは、[カテゴリ別評価の状況] は、評価の低い項目の対策を検討していただくため、危険なコンピュータが 1 台でもあれば低い評価となります。 一方、[カテゴリ別評価と台数の推移] は、セキュリティ状況の傾向を確認していただくため、各カテゴリの平均値を基に評価しています。そのため、[カテゴリ別評価の状況] と [カテゴリ別評価と台数の推移] の評価レベルが異なる場合があります。

危険レベルによって減点されるポイントを次の表に示します。

危険レベル	減点ポイント
危険	25

危険レベル	減点ポイント
警告	16
注意	6
安全	0

なお、セキュリティ判定で判定エラー、判定項目なし、および情報不足の場合は、減点されません。

総合セキュリティ評価の基準を次の表に示します。

評価	ポイントの平均値	ポイントの最小値	判定結果の危険レベル	カテゴリ別評価
A	90～100	90～100	危険、警告ともに 0 件	B 以下がない
B	80～89	80～89	危険が 0 件	C 以下がない
C	65～79	50～79	危険が 0 件	E 以下がない
D	50～64	規定なし	規定なし	規定なし
E	0～49	規定なし	規定なし	規定なし

例えば、ポイントの平均値が 95 点（A 評価対応）、ポイントの最小値が 87 点（B 評価対応）、判定結果の危険レベルが「危険、警告ともに 0 件」（A 評価対応）、カテゴリ別評価が「C 以下がない」（B 評価対応）の場合、総合セキュリティ評価は B になります。このように、上記 4 つの項目のうち、最も低い評価が総合セキュリティ評価になります。

カテゴリ別評価の基準を次の表に示します。

評価	ポイントの平均値	ポイントの最小値	判定結果の危険レベル
A	90～100	90～100	危険、警告ともに 0 件
B	80～89	80～89	危険が 0 件
C	65～79	50～79	危険が 0 件
D	50～64	規定なし	規定なし
E	0～49	規定なし	規定なし

例えば、ポイントの平均値が 95 点（A 評価対応）、ポイントの最小値が 87 点（B 評価対応）、判定結果の危険レベルが「危険、警告ともに 0 件」（A 評価対応）の場合、総合セキュリティ評価は B になります。このように、上記 3 つの項目のうち、最も低い評価がカテゴリ別評価になります。

2.16.3 グリーン IT の適応/未適応の判定基準

[グリーン IT（省電力設定状況）] レポートでは、コンピュータの省電力設定の適応状況を確認できます。コンピュータに省電力設定が適応されているかどうかは、コンピュータから収集された省電力設定値とモ

デルケースの設定値の比較によって判定されます。コンピュータの省電力設定の状態と、判定結果の関係を次の表に示します。

状態	判定
適応	コンピュータの省電力設定≦判定基準の設定値である。 ただし、コンピュータの省電力設定が「なし」の場合は除外する。
未適応	コンピュータの省電力設定＞判定基準の設定値である。または、コンピュータの省電力設定が「なし」である。
不明	省電力設定の判定基準が設定されているが、コンピュータの省電力設定が取得できない。
対象外	判定基準の設定値が設定されていない。

2.16.4　理想消費電力量（理論値）と消費電力量（理論値）の算出方法

理想消費電力量（理論値）は、[グリーン IT の設定] ダイアログで設定した省電力の基準値を基に算出されます。消費電力量（理論値）は、各コンピュータの設定を基に算出されます。

コンピュータの稼働時間については、理想消費電力量（理論値）、消費電力量（理論値）共に、[グリーン IT の設定] ダイアログで設定したモデルケースの値を使用しています。

1 時間当たりの消費電力は、次の表に示す省電力設定の組み合わせによる値の合計で算出されます。

項番	モニタの状態	コンピュータ本体の状態	1 時間当たりの消費電力（ワット）
1	通常時※（30）	通常時※（39）	69
2		ハードディスクの電源を切る（35）	65
3		システムスタンバイ（3）	33
4		システム休止状態（0）	30
5	電源を切る（0）	通常時（39）	39
6		ハードディスクの電源を切る（35）	35
7		システムスタンバイ（3）	3
8		システム休止状態（0）	0

注　括弧内の数字は、1 時間当たりの消費電力（単位：ワット）です。なお、コンピュータ本体の状態は重複することはありません。複数の省電力設定が同時に動作する場合は、消費電力が小さい方になります。

注※　省電力設定が動作していない状態です。

理想消費電力量（理論値）の算出方法

理想消費電力量（理論値）は、[グリーン IT の設定] ダイアログで設定した省電力設定の判定基準がコンピュータに適用され、モデルケースどおりに稼働した場合の値です。

ここでは、次に示す条件で理想消費電力量（理論値）の算出方法を説明します。

- 管理対象のコンピュータの台数：100 台
- ［グリーン IT の設定］ダイアログで設定した省電力設定の基準値（デフォルト）
  - モニタの電源を切る（AC）：5 分以内
  - ハードディスクの電源を切る（AC）：30 分以内
  - システムスタンバイ（AC）：1 時間以内
- ［グリーン IT の設定］ダイアログで設定したモデルケース（デフォルト）
  - コンピュータの稼働時間（1 日当たり）：8 時間
  - コンピュータを操作しない時間：60 分×1 回、10 分×6 回

理想消費電力量（理論値）は、コンピュータの稼働時間を操作している時間と操作していない時間に分けて、上の表で示した値を基に算出します。

操作している時間

モデルケースの設定に従って、1 日当たりの稼働時間（8 時間）からコンピュータを操作しない時間（60 分×1）と（10 分×6）を除きます。この例では、操作時間は次のようになります。

8 時間－2 時間＝ 6 時間

操作時は省電力設定が動作していない状態です。このため、上の表の項番 1 の状態が当てはまります。計算式は次のようになります。

69×6 時間＝ 414（ワット時）

操作しない時間

モデルケースの設定に従い、「60 分×1 回」と「10 分×6 回」の 2 種類になります。

「60 分×1 回」の消費電力量

「モニタの電源を切る」に 5 分が設定されているので、上の表の項番 1 の状態が 5 分続いたあとでモニタが電源 OFF になります。「ハードディスクの電源を切る」に 30 分が設定されているので、上の表の項番 5 の状態が 25 分間続いたあとでハードディスクが電源 OFF になります。そのあとは、「システムスタンバイ」に 1 時間が設定されているので、残りの 30 分が上の表の項番 6 の状態となります。したがって、計算式は次のようになります。

（69×5 分÷60 分）＋（39×25 分÷60 分）＋（35×30 分÷60 分）＝ 39.5（ワット時）

「10 分×6 回」の消費電力量

この消費電力量についても、上記の「60 分×1 回」の消費電力量と同じ方法で計算されます。上の表の項番 1 の状態が 5 分続いたあと、上の表の項番 5 の状態が 5 分続きます。この状態が 6 回となります。したがって、計算式は次のようになります。

{(69×5 分÷60 分）＋（39×5 分÷60 分)｝×6 回＝ 54（ワット時）

理想消費電力量（理論値）

コンピュータを操作している時間と操作しない時間の消費電力量の合計に、コンピュータの台数を掛けた値が理想消費電力量（理論値）になります。したがって、計算式は次のようになります。

（414 + 39.5 + 54）×100 台＝ 50,750（ワット時）

消費電力（理論値）の算出方法

消費電力量（理論値）は、各コンピュータで設定している省電力設定でモデルケース（コンピュータの使用状況）どおりに稼働した場合の値になります。

消費電力量（理論値）の算出方法は、理想消費電力量（理論値）と同じです。コンピュータの台数および設定例と、その設定の場合の消費電力量（理論値）の計算を次に示します。

- 管理対象のコンピュータの台数：100 台
- コンピュータの設定
  - モニタの電源を切る（AC）：10 分
  - ハードディスクの電源を切る（AC）：30 分
  - システムスタンバイ（AC）：90 分

  この例では、すべてのコンピュータで設定が共通とします。
- ［グリーン IT の設定］ダイアログで設定したモデルケース（例）
  - コンピュータの稼働時間（1 日当たり）：8 時間
  - コンピュータを操作しない時間：60 分×1 回、10 分×6 回

消費電力量（理論値）の計算式

1 台当たりの消費電力量（理論値）：（69×6 時間）＋（69×10 分÷60 分）＋（39×20 分÷60 分）＋（35×60 分÷60 分）＋｛(69×10 分÷60）×6 回｝＝ 542.5（ワット時）

100 台の消費電力量（理論値）：542.5×100 台＝ 54,250（ワット時）

このようにして、設定を基に各コンピュータの消費電力量が計算され、消費電力量（理論値）として合計されます。なお、消費電力量（理論値）は、省電力設定の情報が取得できたコンピュータだけを対象に算出されます。

2.16.5　レポートの集計スケジュール

各レポートを表示すると、集計スケジュールに沿って実行された集計結果、または現時点の集計結果が表示されます。レポートの集計スケジュールは、レポートの種類によって異なります。また、集計される期間やデータの保存期間も、レポートの種類によって異なります。各レポートで利用されるデータの集計スケジュールと、集計期間および保存期間を次の表に示します。

レポート		集計対象	スケジュール	集計期間	保存期間	スケジュールの設定可否
ダイジェストレポート	日刊ダイジェスト	すべての情報	毎日 6:00	前日分	7 日分	×

レポート			集計対象	スケジュール	集計期間	保存期間	スケジュールの設定可否
ダイジェストレポート	週刊ダイジェスト		すべての情報	毎週の開始曜日、日刊ダイジェストの集計終了後	前週分	5 週分	○
	月刊ダイジェスト			毎月の開始日、日刊ダイジェストの集計終了後	前月分	3 か月分	○
セキュリティ診断レポート	現状セキュリティ診断		機器（グループ/セキュリティポリシー単位）	オンデマンド※1	実行時点	最新の 1 回分	×
				毎日の定期判定終了後（デフォルトは 0:00）	集計時点		○ ※2
	期間指定セキュリティ診断	週単位	機器（グループ/セキュリティポリシー単位）	毎日 1:00	当週分（日単位）	6 週分	○
		月単位			当月分（日単位）	3 か月分	○
		四半期単位		毎月の開始日（日単位の集計終了後）	当四半期分（月単位）	5 年分※3	○
		半期単位			当半期分（月単位）	5 年分※3	○
		年度単位			当年度分（月単位）	5 年分※3	○
セキュリティ詳細レポート	危険レベルの状況		機器（グループ/セキュリティポリシー単位）	オンデマンド※1	実行時点	最新の 1 回分	×
				毎日 1:10	集計時点		×
				毎月の開始日 0:30	前月分	1 年分	○

レポート		集計対象	スケジュール	集計期間	保存期間	スケジュールの設定可否
セキュリティ詳細レポート	• 更新プログラムの適用状況 • ウィルス対策製品の状況 • 使用必須ソフトウェアのインストール状況 • 使用禁止ソフトウェアのインストール状況 • セキュリティ設定の状況	機器（グループ/セキュリティポリシー単位）	オンデマンド※1	実行時点	最新の 1 回分	×
			毎日 1:10	集計時点		×
	禁止操作の状況	イベント（機器/ユーザーアカウント単位）	イベント発生時	集計時点	−	×
	ユーザーの活動状況					
機器詳細レポート	機器の管理状況	機器（グループ単位）	オンデマンド※1	実行時点	最新の 1 回分	×
			毎日 0:40	集計時点		×
			毎月の開始日 0:30	前月分	1 年分	○
	グリーン IT（省電力設定状況）	機器（グループ単位）	オンデマンド※1	実行時点	最新の 1 回分	×
			毎日 0:40	集計時点		×
			毎月の開始日 0:30	前月分	1 年分	○
資産詳細レポート	ハードウェア資産	ハードウェア資産（グループ単位）	オンデマンド※1	実行時点	最新の 1 回分	×
			毎日 0:10	集計時点		×
			毎月の開始日 0:00	前月分	5 年分※3	○
	ハードウェア資産の費用	契約（契約単位）	毎月の開始日 0:00※4	前月分	5 年分※3	○
			レポート表示時※5	レポート表示時点	−	×
	ソフトウェアライセンスの費用	契約（契約単位）	毎月の開始日 0:00※4	前月分	5 年分※3	○
			レポート表示時※5	レポート表示時点	−	×

レポート		集計対象	スケジュール	集計期間	保存期間	スケジュールの設定可否
資産詳細レポート	その他の費用	契約（契約単位）	レポート表示時	レポート表示時点	－	×
	ライセンス超過ソフトウェア	管理ソフトウェア（管理ソフトウェア単位）	レポート表示時	レポート表示時点	－	×
	ライセンス余剰ソフトウェア					

（凡例） ○：設定できる　×：設定できない　－：対象外

注※1　レポートに表示される［集計］ボタンをクリックすることで、現時点のデータが集計されます。

注※2　設定画面の［セキュリティ管理］－［セキュリティのスケジュール設定］画面で判定スケジュールを設定することで集計スケジュールが変更されます。

注※3　設定画面の［レポート］－［保存期間と開始日の設定］画面で設定できます。

注※4　JP1/IT Desktop Management 2 の 12-10 より前のバージョンから 12-10 以降のバージョンにバージョンアップした場合の集計スケジュールです。

注※5　JP1/IT Desktop Management 2 の 12-10 以降のバージョンを新規インストールした場合の集計スケジュールです。

重要

集計済みのデータがある場合、開始日の設定を変更すると、複数の期間に重複して集計される日や、どの期間にも集計されない日が発生することがあります。開始日を変更した場合、変更後からの集計データを使用してください。

2.16.6　レポートの印刷

レポート画面で表示されるレポートは、表示されている内容がそのまま A4 サイズで印刷されます。ただし、レポートの内容に直接関係しないボタンやスクロールバーなどは印刷されません。ダイジェストレポートなどの表示項目が多いレポートは、表示内容に応じて複数ページで印刷されます。また、ページ番号が各ページの中央下に印刷されます。

重要

レポートを印刷した際に、凡例の各項目の色が表示されない場合があります。

2.16.7　レポートの削除

次に示すレポートは、集計データが蓄積されるため、利用期間に応じてデータが増加します。不要となったレポートを削除することで、ディスクの占有量を削減できます。

- セキュリティ診断レポート－月単位評価
- 資産詳細レポート－ハードウェア資産
- 資産詳細レポート－ハードウェア資産の費用
- 資産詳細レポート－ソフトウェアライセンスの費用

レポートは、保存期間を変更することで削除できます。レポートの保存期間を短縮した場合、保存期間を短縮して保存期間が過ぎてしまったレポートは、設定を変更したあとのレポートの定期集計時（1 日 1 回）に削除されます。例えば、レポートの保存期間を 2 年から 1 年に短縮した場合、1 年 3 か月前のレポートは、レポートの次回定期集計時に削除されます。

レポートの保存期間は、設定画面の［レポート］－［保存期間と開始日の設定］画面で設定できます。デフォルトは 5 年です。

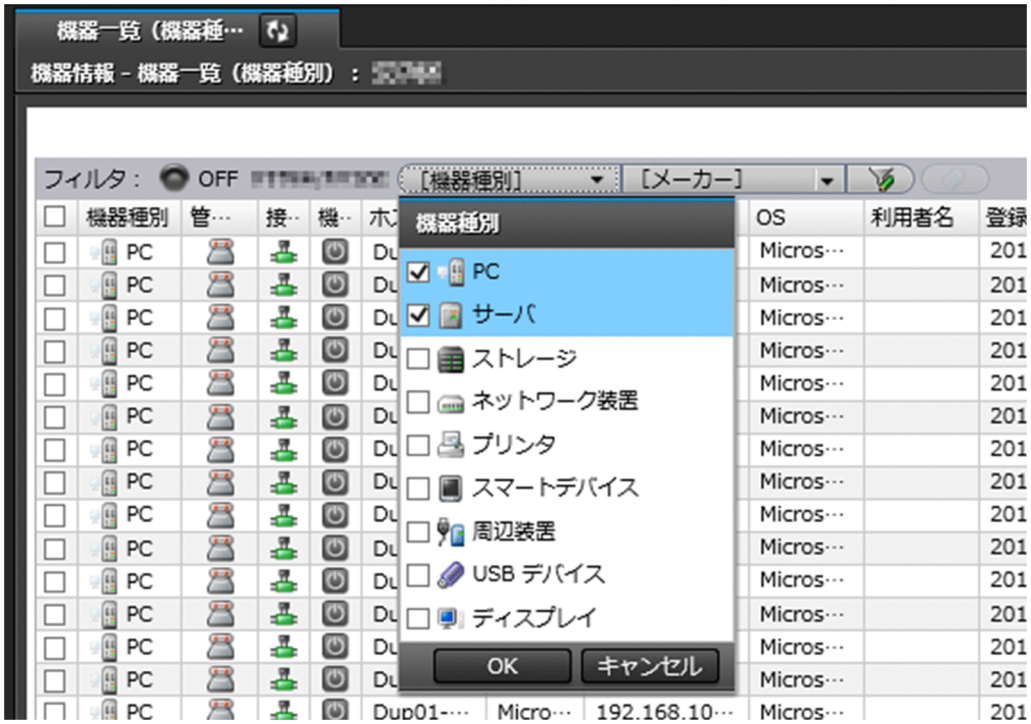
2.17　フィルタの利用

フィルタを利用すると、条件を指定して一覧に表示される情報を絞り込めます。

フィルタは、「簡易フィルタ」と「詳細フィルタ」の 2 種類があります。

簡易フィルタ

簡易フィルタは、用意されたフィルタ項目から一覧に表示したい条件を選択するフィルタです。一覧の上部に表示されているフィルタ項目のプルダウンメニューで、表示したい情報の条件を選択して、素早く情報を絞り込めます。



詳細フィルタ

詳細フィルタは、複数の詳細な条件を組み合わせて設定できるフィルタです。簡易フィルタだけでは目的の情報を絞り込めない場合に、詳細フィルタを利用してください。

詳細フィルタには、JP1/IT Desktop Management 2 が提供するフィルタ項目があります。メニューエリアの［フィルタ］に表示されるフィルタを選択すると、表示している画面に対してフィルタを適用できます。

上の図では、資産画面の［ハードウェア資産］－［資産一覧（部署）］画面に表示される一覧に対して、［PC］のフィルタを適用しています。どの画面に対してどのフィルタを適用しているかは、メニューエリアの左側に青い線で表示されます。

また、任意の条件を指定した詳細フィルタを追加できます。メニューエリアの［フィルタ］にマウスカーソルを合わせて、 をクリックしてください。フィルタ名を入力すると、［フィルタ条件の編集］ダイアログが表示され、目的に応じてさまざまな条件を設定できます。例えば、リプレース対象のコンピュータを絞り込むために、［登録日時］が 3 年以上前かつ［OS］が Windows 7 などの条件を設定できます。

ヒント

よく業務で使用するフィルタ条件を保存しておくと、毎回条件を指定する手間が省けます。保存したフィルタ条件は、メニューエリアで選択することで一覧に適用できます。

ヒント

資産情報のフィルタ条件を設定する場合、［すべてのハードウェア資産項目］を利用すると任意の文字列を含む資産情報を表示できます。

なお、［フィルタ条件の編集］ダイアログは、 ボタンをクリックしても表示できます。

フィルタを適用すると、一覧の上部の［フィルタ：OFF］が［フィルタ：ON］に変わり、緑色のランプが点灯します。また、絞り込まれた台数が表示されます。

フィルタを解除するには、 ボタンをクリックしてください。表示が［フィルタ：OFF］に変わり、条件が解除されます。

ヒント

詳細フィルタの条件は、コマンドを実行してエクスポートおよびインポートできます。

関連リンク

- 2.17.1　製品が提供するフィルタ

2.17.1　製品が提供するフィルタ

JP1/IT Desktop Management 2 が提供するフィルタに設定された条件を説明します。

セキュリティ画面のフィルタ

セキュリティ画面のメニューエリアに表示されるフィルタの条件を、次の表に示します。

［機器のセキュリティ状態］画面のフィルタ

フィルタ名	条件
安全でないコンピュータ	[(危険レベル)]、[どれも含まない]、[対象外、安全]

［更新プログラム］画面のフィルタ

フィルタ名	条件
1 か月以内にリリースされた更新プログラム	• [リリース日]、[以降]、[月]、[1]、[前] • [リリース日]、[以前]、[今日]

資産画面のフィルタ

資産画面のメニューエリアに表示されるフィルタの条件を次の表に示します。

［ハードウェア資産］画面のフィルタ

フィルタ名	条件
未確認の資産	[資産状態]、[どれかを含む]、[未確認]
PC	• [資産状態]、[どれも含まない]、[未確認、滅却] • [機器種別]、[どれかを含む]、[PC]
サーバ	• [資産状態]、[どれも含まない]、[未確認、滅却] • [機器種別]、[どれかを含む]、[サーバ]
ストレージ	• [資産状態]、[どれも含まない]、[未確認、滅却] • [機器種別]、[どれかを含む]、[ストレージ]
周辺装置	• [資産状態]、[どれも含まない]、[未確認、滅却] • [機器種別]、[どれかを含む]、[周辺装置]

フィルタ名	条件
USB デバイス	• [資産状態]、[どれも含まない]、[未確認、滅却] • [機器種別]、[どれかを含む]、[USB デバイス]
ネットワーク装置	• [資産状態]、[どれも含まない]、[未確認、滅却] • [機器種別]、[どれかを含む]、[ネットワーク装置]
プリンタ	• [資産状態]、[どれも含まない]、[未確認、滅却] • [機器種別]、[どれかを含む]、[プリンタ]
スマートデバイス	• [資産状態]、[どれも含まない]、[未確認、滅却] • [機器種別]、[どれかを含む]、[スマートデバイス]
ディスプレイ	• [資産状態]、[どれも含まない]、[未確認、滅却] • [機器種別]、[どれかを含む]、[ディスプレイ]
半年以内に登録した資産	• [資産状態]、[どれも含まない]、[未確認、滅却] • [登録日時]、[以降]、[月]、[6]、[前] • [登録日時]、[以前]、[今日]
半年以内に棚卸をしていない資産	• [資産状態]、[どれも含まない]、[未確認、滅却] • [棚卸日]、[より前]、[月]、[6]、[前]
未確認の USB デバイス	• [資産状態]、[どれかを含む]、[未確認] • [機器種別]、[どれかを含む]、[USB デバイス]

[ソフトウェアライセンス] 画面のフィルタ

フィルタ名	条件
半年以内に登録したライセンス	• [ライセンス状態]、[どれも含まない]、[滅却] • [登録日時]、[以降]、[月]、[6]、[前] • [登録日時]、[以前]、[今日]
半年以内に棚卸をしていないライセンス	• [ライセンス状態]、[どれも含まない]、[滅却] • [棚卸日]、[より前]、[月]、[6]、[前]

[管理ソフトウェア] 画面のフィルタ

フィルタ名	条件
インストール数超過ライセンス	• [ライセンス種類]、[どれかを含む]、[インストールライセンス] • [残数]、[<]、[0]

[ソフトウェアライセンス状況] 画面のフィルタ

フィルタ名	条件
インストール数超過ライセンス	• [ライセンス種類]、[どれかを含む]、[インストールライセンス] • [残数]、[<]、[0]

［契約］画面のフィルタ

フィルタ名	条件
ハードウェア資産	JP1/IT Desktop Management 2 の 12-10 より前のバージョンから 12-10 以降のバージョンにバージョンアップした場合 ［ハードウェア資産］、［>］、［0］ JP1/IT Desktop Management 2 の 12-10 以降のバージョンを新規インストールした場合 ［契約対象］、［どれかを含む］、［ハードウェア資産］
ソフトウェアライセンス	JP1/IT Desktop Management 2 の 12-10 より前のバージョンから 12-10 以降のバージョンにバージョンアップした場合 ［ソフトウェアライセンス］、［>］、［0］ JP1/IT Desktop Management 2 の 12-10 以降のバージョンを新規インストールした場合 ［契約対象］、［どれかを含む］、［ソフトウェアライセンス］
期限切れの契約	• ［契約状態］、［どれも含まない］、［途中解約、満了］ • ［契約終了日］、［より前］、［今日］
1 か月以内に期限切れとなる契約	• ［契約状態］、［どれも含まない］、［途中解約、満了］ • ［契約終了日］、［以前］、［月］、［1］、［後］ • ［契約終了日］、［以降］、［今日］

機器画面のフィルタ

機器画面のメニューエリアに表示されるフィルタの条件を次の表に示します。

［機器情報］画面のフィルタ

フィルタ名	条件
7 日以内に登録した機器	• ［登録日時］、［以降］、［週］、［1］、［前］ • ［登録日時］、［以前］、［今日］
1 か月以上確認していない機器	［最終接続確認日時］、［より前］、［月］、［1］、［前］

［ソフトウェア情報］画面のフィルタ

フィルタ名	条件
7 日以内に登録したソフトウェア	• ［登録日時］、［以降］、［週］、［1］、［前］ • ［登録日時］、［以前］、［今日］
未確認の有償ソフトウェア	• ［管理ソフトウェア］、［等しい］、［なし］ • ［ソフトウェア種別］、［どれかを含む］、［有償ソフトウェア］ • ［確認状態］、［等しい］、［未確認］

配布（ITDM 互換）画面のフィルタ

配布（ITDM 互換）画面のメニューエリアに表示されるフィルタの条件を次の表に示します。

［パッケージ］画面のフィルタ

フィルタ名	条件
削除できるパッケージ	［タスク数］、［＝］、［0］

［タスク］画面のフィルタ

フィルタ名	条件
エラーが発生したタスク	［失敗コンピュータ数］、［＞］、［0］

イベント画面のフィルタ

イベント画面のメニューエリアに表示されるフィルタの条件を次の表に示します。

フィルタ名	条件
エラーイベント	［種類］、［どれかを含む］、［エラー］

［ネットワーク制御リストの設定］画面のフィルタ

設定画面の［ネットワーク制御リストの設定］画面に表示されるフィルタの条件を次の表に示します。

フィルタ名	条件
マークのある機器	［マーク］、［等しい］、［マークあり］

関連リンク

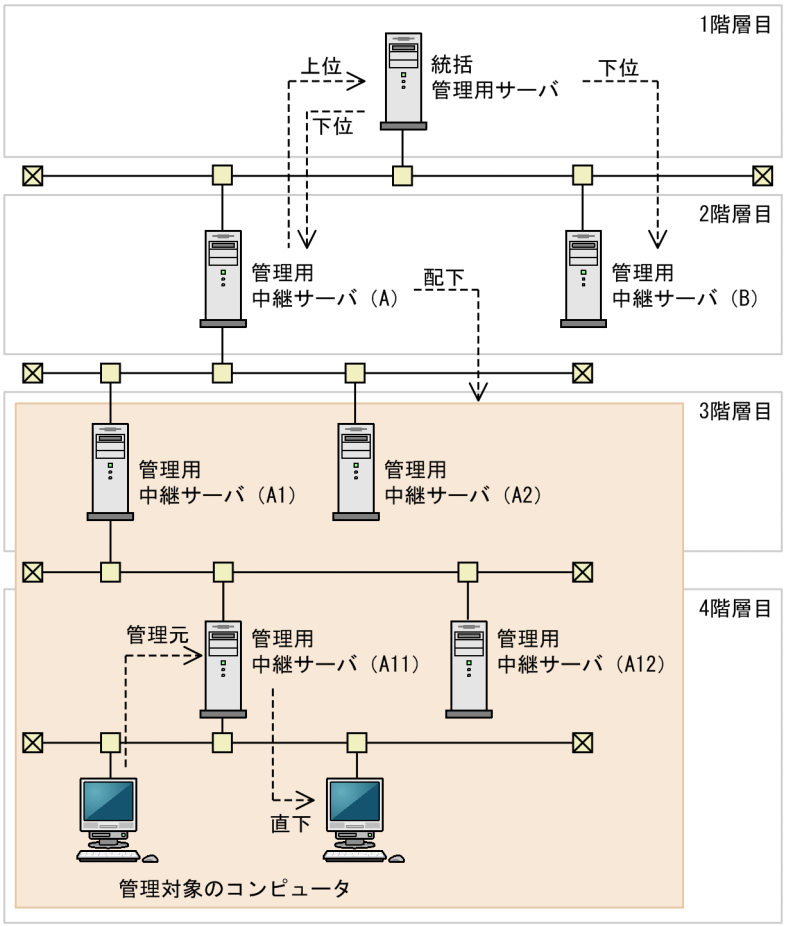
- 2.17　フィルタの利用

2.18　複数の部門やネットワークで構成される大規模システムの管理

組織の規模やネットワーク構成に応じて管理用サーバを複数台設置することで、システム管理者や管理用サーバの負荷を分散したり、NAT 環境を含むシステムの管理に対応したりできます。

管理用サーバを複数台設置したシステム構成を、「複数サーバ構成」と呼びます。複数サーバ構成は、システム全体をまとめる 1 台の統括管理用サーバと、各拠点やネットワーク内を管理する複数台の管理用中継サーバで階層状に構成されます。

4 階層に構築した複数サーバ構成のシステム構成例を次の図に示します。



各管理用中継サーバは、1 つ上の階層にある管理用サーバ（統括管理用サーバまたは管理用中継サーバ）のうちの 1 台に接続し、管理している情報を通知したり、設定が適用されたりします。この接続先の管理用サーバのことを「上位の管理用サーバ」と呼びます。反対に、接続先の管理用サーバから見た管理用中継サーバのことを「下位の管理用中継サーバ」と呼びます。また、下位の管理用中継サーバと、下位の管理用中継サーバに接続している管理用中継サーバを、まとめて「配下の管理用中継サーバ」と呼びます。

上記の構成例の場合、次のとおりとなります。

- 管理用中継サーバ（A）の「上位の管理用サーバ」：統括管理用サーバ
- 統括管理用サーバの「下位の管理用中継サーバ」：管理用中継サーバ（A）または管理用中継サーバ（B）

- 管理用中継サーバ（A）の「配下の管理用中継サーバ」：管理用中継サーバ（A1）、管理用中継サーバ（A2）、管理用中継サーバ（A11）および管理用中継サーバ（A12）

さらに、管理対象のコンピュータが接続している管理用サーバのことを、管理対象のコンピュータから見て「管理元の管理用サーバ」と呼びます。反対に、接続先の管理用サーバから見た管理対象のコンピュータを「直下のコンピュータ」と呼びます。

関連リンク

- 1.2　システム構成要素の紹介
- 4.4.3　複数サーバ構成

2.18.1　複数サーバ構成の場合の操作画面に表示される情報

複数サーバ構成と単数サーバ構成とでは、操作画面に表示される情報に差異があります。単数サーバ構成と比較して、複数サーバ構成の操作画面に表示される情報を次の表に示します。

画面		複数サーバ構成の操作画面に表示される情報
各画面の共通の操作	画面上部のメニュー	配下の管理用中継サーバの操作画面を別ウィンドウで起動するためのプルダウンメニューが追加されます。
	フィルタ	自サーバが管理している情報だけを表示するためのチェックボックスが追加されます。
ログイン画面		ログイン画面から表示できる［製品ライセンス情報］ダイアログの［製品ライセンスの情報］に、次の項目が追加されます。 • ［製品ライセンスの情報の更新日時］ • ［ライセンス総数］ • ［ライセンスを保有する管理用サーバ］ • ［ライセンスの共有範囲］ ただし、ライセンスの管理方法によって各管理用サーバの［製品ライセンスの情報］に表示される項目は変わります。
ホーム画面		• ホーム画面が［自サーバの直下の状況］タブと［配下の管理用サーバの状況］タブの 2 つに分かれます。 • ［配下の管理用サーバの状況］タブに、自サーバ配下の管理用中継サーバの階層構成および概況が表示されます。
セキュリティ画面		下位の管理用中継サーバで操作ログを上位の管理用サーバに通知するように設定している場合、下位の管理用中継サーバが取得した操作ログが表示されます。
資産画面		配下の管理用中継サーバから通知された資産情報が表示されます。
機器画面		配下の管理用中継サーバから通知された機器情報が表示されます。
イベント画面		下位の管理用中継サーバで操作ログを上位の管理用サーバに通知するように設定している場合、下位の管理用中継サーバが管理元であるコンピュータの不審操作イベントが表示されます。
レポート画面		• 機器詳細レポートの集計範囲に配下の管理用中継サーバで管理している機器も含まれます。

画面	複数サーバ構成の操作画面に表示される情報
レポート画面	• 下位の管理用中継サーバで操作ログを上位の管理用サーバに通知するように設定している場合、下位の管理用中継サーバが管理元であるコンピュータの操作ログおよび不審操作もレポートに集計されます。

設定画面	• サイトマップに［配下の階層構成および稼働状態］が追加されます。
	• 自サーバの設定を配下の管理用中継サーバに適用するためのボタンが追加されます。
	• ［製品ライセンスの設定］画面の［製品ライセンスの情報］に、次の項目が追加されます。
	  • ［製品ライセンスの情報の更新日時］
	  • ［ライセンス総数］
	  • ［ライセンスを保有する管理用サーバ］
	  • ［ライセンスの共有範囲］
	ただし、ライセンスの管理方法によって各管理用サーバの［製品ライセンスの情報］に表示される項目は変わります。

2.18.2　管理元が配下の管理用中継サーバである機器に対する操作の制限

複数サーバ構成の場合で、管理元が配下の管理用中継サーバである機器を対象にしたとき、自サーバの操作画面からできる操作が制限されます。

自サーバ直下の機器に対してできる操作と、管理元が配下の管理用中継サーバである機器に対して自サーバの操作画面から操作できるかどうかの対応を次の表に示します。自サーバの操作画面からできない操作については、機器の管理元の操作画面から実施してください。

自サーバ直下の機器に対してできる操作	管理元が配下の管理用中継サーバである機器に対して操作できるかどうか
利用者にメッセージを通知する	×
［利用者情報の入力］画面を定期的に表示させる	○
ネットワークモニタを有効にする	×
ネットワークモニタを無効にする	×
接続を許可する	×
接続を許可しない	×
電源 ON にする	×
電源 OFF にする	×
再起動する	×
スマートデバイスをロックする	×
スマートデバイスのパスコードをクリアする	×
スマートデバイスを初期化する	×
機器情報を編集する	○

自サーバ直下の機器に対してできる操作	管理元が配下の管理用中継サーバである機器に対して操作できるかどうか
最新の情報を取得する	×
最新の情報を取得するファイルを作成する	○
認証情報を設定する	×
ソフトウェアライセンスを移管する	○
削除する	○
機器一覧をエクスポートする	○
機器一覧（詳細）をエクスポートする	○
カスタムグループに追加する	○
リモートコントロールを開始する	○※

（凡例）○：実施できる　×：実施できない

注※　リモートコントロールの起動元の管理用サーバとリモートコントロールの対象とで、使用するポート番号を統一する必要があります。

関連リンク

- 2.6.3　機器の制御

2.18.3　配下の管理用中継サーバの状況確認

複数サーバ構成では、上位の管理用サーバから配下の管理用中継サーバの階層構成を確認したり、不要になった管理用中継サーバを階層構成から削除したりできます。また、各管理用中継サーバの稼働状態を確認できます。

上位の管理用サーバは下位の管理用中継サーバから通知された情報を基に、各管理用中継サーバの階層構成や稼働状態をホーム画面の［配下の階層構成および稼働状態］パネルに表示します。下位の管理用中継サーバが上位の管理用サーバに通知する情報を次に示します。

<table>
<tr><th colspan="2">項目</th><th>通知の契機</th></tr>
<tr><td colspan="2">IP アドレス</td><td rowspan="4">・管理用中継サーバ用のエージェントが機器情報を上位の管理用サーバに自動通知したとき
・管理用中継サーバの管理者が自サーバの機器情報を編集したとき</td></tr>
<tr><td colspan="2">利用者名</td></tr>
<tr><td colspan="2">電話番号</td></tr>
<tr><td colspan="2">メールアドレス</td></tr>
<tr><td rowspan="3">管理用中継サーバの接続情報</td><td>ホスト名</td><td rowspan="3">管理用中継サーバが起動したとき</td></tr>
<tr><td>ホスト識別子</td></tr>
<tr><td>リモコンエージェントのポート番号</td></tr>
</table>

項目		通知の契機
管理用中継サーバの接続情報	HTTP 接続用のポート番号	管理用中継サーバが起動したとき
	操作ログおよび 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かどうか	
	最終接続通知日時※	• 管理用中継サーバが起動したとき • セットアップで設定した上位サーバへの通知間隔（初期設定は 5 分）に従って自動通知したとき

注※　管理用中継サーバが、上位の管理用サーバに接続情報を通知した日時です。

下位の管理用中継サーバは、配下の管理用中継サーバの接続情報と自サーバの接続情報を合わせて上位の管理用サーバに通知します。

管理用サーバの階層構成の確認

自サーバを最上位とした配下の管理用中継サーバの階層構成がツリー形式で表示されます。

不要になった管理用中継サーバの削除

不要になった管理用中継サーバおよびその配下の管理用中継サーバを階層構成から削除できます。また、削除される管理用中継サーバが管理する次の情報も、削除を実施した管理用サーバから削除されます。

- 機器情報
- ネットワークセグメントのグループ

> **ヒント**
>
> 機器情報は、管理元の管理用中継サーバが階層構成から削除されるのに併せて、順次削除されます。

管理用中継サーバの詳細情報の確認

配下の管理用中継サーバの詳細情報を確認できます。確認できる情報を次に示します。

項目		説明
概況	状態	詳細情報を表示している管理用中継サーバの状態
	最終接続通知日時	詳細情報を表示している管理用中継サーバが、最後に上位の管理用サーバに情報を通知した日時
システム情報	稼働状態	詳細情報を表示している管理用中継サーバの稼働状態（稼働中、警告、不明）
	ホスト名	詳細情報を表示している管理用中継サーバのホスト名
	IP アドレス	詳細情報を表示している管理用中継サーバの IP アドレス
	ホスト識別子	詳細情報を表示している管理用中継サーバのホスト識別子

項目		説明
システム情報	自サーバからの経路	自サーバを基準とした、詳細情報を表示している管理用中継サーバのパス
利用者情報	利用者名	詳細情報を表示している管理用中継サーバの利用者名
	メールアドレス	詳細情報を表示している管理用中継サーバの利用者のメールアドレス
	電話番号	詳細情報を表示している管理用中継サーバの利用者の電話番号

稼働状態の判定

稼働状態の判定方法を設定することで、配下の管理用中継サーバが正常に稼働しているかを確認できます。判定方法には、次の種類があります。

指定した日数以上接続が確認されない場合に、稼働状態を［警告］とする

指定した日数（1～30 日）を経過しても接続が確認されない管理用中継サーバを異常と見なして、稼働状態を［警告］に変更します。また、上位の管理用サーバに警告用のイベントを発行したり、ホーム画面に通知を表示したりします。接続が確認されない管理用中継サーバよりも配下の管理用中継サーバについては、最終接続通知日時を上位の管理用サーバが取得できないため、稼働状態を［不明］に変更します。

配下の管理用中継サーバの稼働状態を確認したい場合は、この判定方法を設定してください。

すべての管理用サーバの稼働状態を［稼働中］とする

配下の管理用中継サーバの稼働状態を監視しません。

配下の管理用中継サーバの稼働状態を確認する必要がない場合は、この判定方法を設定してください。

ヒント

ホーム画面の［配下の階層構成および稼働状態］パネルでは、管理用中継サーバの操作画面を別ウィンドウで起動したり、リモートコントロールを開始したりできます。異常のある管理用中継サーバに対処する際に便利です。

関連リンク

- 2.18.4　配下の管理用中継サーバの操作画面へのログイン
- 2.18.8　複数サーバ構成でのリモートコントロール

2.18.4　配下の管理用中継サーバの操作画面へのログイン

複数サーバ構成では、上位の管理用サーバの操作画面から配下の管理用中継サーバの操作画面にログインできます。複数の管理用サーバを 1 人で管理する場合や、NAT 環境で管理用サーバを運用する場合でも、1 度ログインするだけでほかの管理用サーバの操作画面にもログインできるため、ログインの手間を軽減できます。

配下の管理用中継サーバの操作画面にログインする際は、ログイン元の管理用サーバに設定しているユーザーアカウントと同じユーザー ID およびパスワードを、ログイン先の管理用中継サーバにも設定する必要があります。また、操作画面を表示する管理者のコンピュータが、配下の管理用中継サーバのホスト名を名前解決できる必要があります。

なお、どのように配下の管理用中継サーバの操作画面にログインしたかによって、最初に表示される画面が変わります。

画面上部のメニューにある［操作対象とするサーバ］のプルダウンメニューからログインした場合

ログイン元の操作画面に表示されている画面と同じ画面が最初に表示されます。

［配下の階層構成および稼働状態］パネルの管理用サーバのボタンからログインした場合

ログイン元で選択した任意の画面が最初に表示されます。

［管理用中継サーバの詳細］ダイアログの［操作画面を表示］ボタンからログインした場合

ホーム画面が最初に表示されます。

2.18.5 管理用中継サーバへのエージェントの自動インストール

JP1/IT Desktop Management 2 - Manager を管理用中継サーバとしてインストールすると、管理用中継サーバ用のエージェントも自動でインストールされます。また、管理用中継サーバ用のエージェントは、JP1/IT Desktop Management 2 - Manager をアンインストールすると、自動でアンインストールされます。管理用中継サーバ用のエージェントは、単独でインストール、およびアンインストールできません。

JP1/IT Desktop Management 2 - Agent と管理用中継サーバにインストールされるエージェントには機能差異があります。機能差異のある項目と、それぞれのエージェントの機能との対応を次の表に示します。

項目	JP1/IT Desktop Management 2 - Agent の場合	管理用中継サーバ用のエージェントの場合
インストール先	任意のインストール先を指定できる	*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*¥mgr¥
エージェントの機能を設定する画面	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	JP1/IT Desktop Management 2 - Manager のセットアップの次の画面 • ［管理用中継サーバの設定］画面 • ［管理用中継サーバの通信設定］画面 • ［管理用中継サーバのリモートコントロール設定］画面
エージェント設定の割り当て	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］	－
セットアップする画面	JP1/IT Desktop Management 2 - Agent のセットアップ	JP1/IT Desktop Management 2 - Manager のセットアップ

項目	JP1/IT Desktop Management 2 - Agent の場合	管理用中継サーバ用のエージェントの場合
Windows の［スタート］メニューの［すべてのプログラム］に表示されるフォルダ名	［JP1_IT Desktop Management 2 - Agent］	［JP1_IT Desktop Management 2 - Manager］－［エージェント］
Windows のコントロールパネルの［プログラムと機能］での表示	表示される	表示されない※

（凡例）－：設定不要

注※　JP1/IT Desktop Management 2 - Manager に含まれます。

2.18.6　複数サーバ構成での管理対象のコンピュータのエージェント設定

複数サーバ構成の場合、管理対象のコンピュータに対しては、管理元からエージェント設定を割り当てます。自サーバが管理元ではない管理対象のコンピュータに対しては、エージェント設定を割り当てられません。

なお、エージェントを導入する際に使用するインストールセットも、インストールセットを作成した管理用サーバの直下で発見されたコンピュータに対してだけ導入できます。

ヒント

自サーバが管理元ではない管理対象のコンピュータに対してエージェント設定を割り当てたい場合は、管理元の操作画面からエージェント設定を割り当ててください。

統括管理用サーバおよび単数サーバ構成の管理用サーバと、管理用中継サーバで、管理対象のコンピュータに設定できるエージェント設定項目に差異はありません。

管理対象のコンピュータの接続先を変更する場合は、管理元の管理用サーバからエージェント設定を変更します。接続先を変更された管理対象のコンピュータは、変更後の接続先のエージェント設定に従います。

ヒント

管理対象のコンピュータをセットアップでエージェントの接続先を変更する場合、変更前の接続先である管理用サーバからエージェント設定を適用されたタイミングで、接続先が元に戻ってしまうおそれがあります。また、変更後の接続先に変更すると一時的にデフォルトポリシーが割り当たる場合があります。管理対象のコンピュータをセットアップでエージェントの接続先を変更する際は、接続先を変更したコンピュータが変更後の接続先である管理用サーバの機器一覧に管理対象として追加されるまで、変更前の接続先である管理用サーバからエージェント設定を適用しないでください。

2.18.7　複数サーバ構成での機器の管理

複数サーバ構成では、自サーバ直下だけでなく、配下の管理用中継サーバから通知された機器情報も管理できます。

> **ヒント**
>
> 機器のメンテナンスの対象は自サーバで管理する機器です。つまり、複数サーバ構成の場合に配下の管理用中継サーバが管理する機器は、上位の管理用サーバでの機器のメンテナンスの対象外となります。複数サーバ構成の場合、機器のメンテナンスは、管理用サーバと配下の管理用中継サーバそれぞれで運用してください。

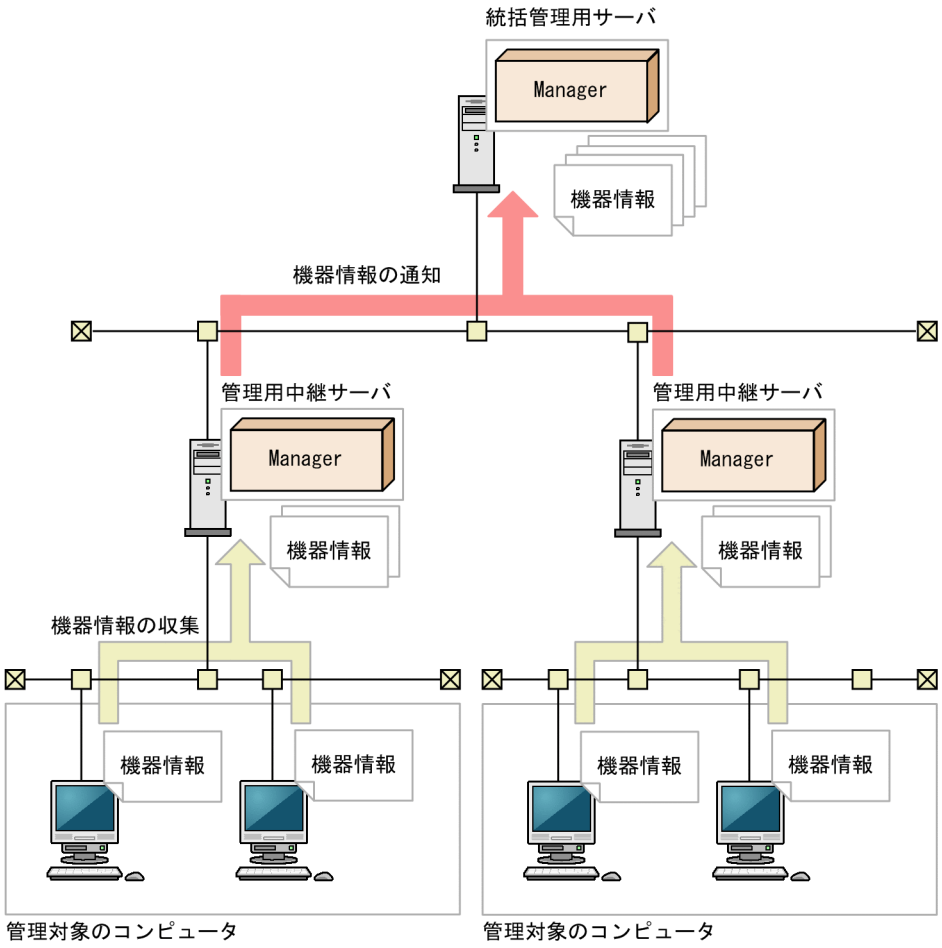
関連リンク

- 2.6.2　機器情報の収集

(1)　上位の管理用サーバへの機器情報の自動通知

複数サーバ構成で運用する場合、管理用中継サーバは機器情報を上位の管理用サーバに自動で通知します。上位の管理用サーバは、直下の機器情報、および配下の管理用中継サーバから通知された機器情報を、まとめて管理できます。

複数サーバ構成での機器情報の通知の流れを次の図に示します。



（凡例）
Manager：JP1/IT Desktop Management 2 - Manager

下位の管理用中継サーバから上位の管理用サーバへ機器情報を通知する契機は、次のとおりです。

- 機器が追加されたとき
- 機器情報が更新されたとき
- 管理者が機器情報を更新したとき

上位の管理用サーバへの通知対象となるのは、エージェント導入済みのコンピュータ、およびエージェントレスのコンピュータの機器情報です。

オフライン管理のコンピュータの機器情報は、管理元が同じ管理者のコンピュータから通知する必要があります。オフライン管理のコンピュータの機器情報は、管理元の管理用サーバに収集情報が通知されたタイミングで上位の管理用サーバにも通知されます。

管理元の管理用中継サーバで機器種別を変更した場合で、変更後の機器種別の項目が上位の管理用サーバに設定されていないとき、上位の管理用サーバにその機器種別の項目が追加されます。

(2) 上位の管理用サーバへの機器情報の手動通知

複数サーバ構成では、管理用中継サーバが収集した機器情報を上位の管理用サーバに手動で通知できます。機器情報を手動で通知することで、管理用サーバ間で失われた機器情報の整合性を回復できます。

次の要因で、ある管理用中継サーバが上位の管理用サーバとの機器情報の整合性を失なった場合は、機器情報を手動で通知してください。

- 上位に新しい管理用サーバを導入した
- 接続先の管理用サーバを変更した
- 接続先の管理用サーバをリストアした

手動で通知した機器情報は、通知元の管理用サーバの接続先だけに反映されます。通知先の管理用サーバより上位の管理用サーバには反映されません。

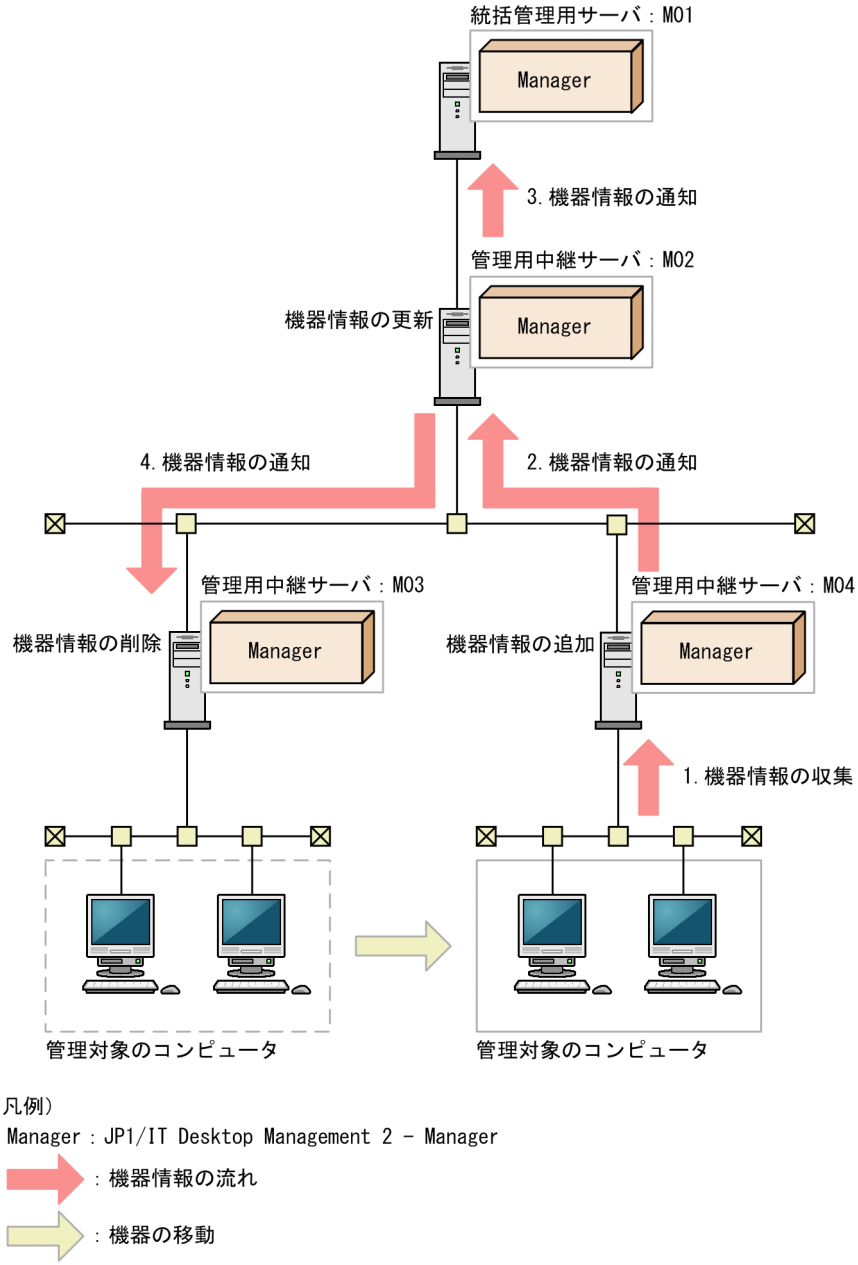
(3) 管理元が配下の管理用中継サーバである機器情報の編集

任意の管理用サーバで、その配下の管理用中継サーバから通知された機器情報を編集できます。自サーバ直下の機器とそれ以外の機器とで、編集できる機器情報に差異はありません。

編集した機器情報の値は、上位の管理用サーバだけに反映されます。配下の管理用中継サーバにも反映したい場合は、配下の管理用中継サーバで値を編集する必要があります。

(4) 複数サーバ構成で機器の管理元を変更する仕組み

管理対象のコンピュータが別の管理用中継サーバの配下に移動した場合、移動先の管理用中継サーバに機器情報が追加され、移動元の管理用中継サーバから機器情報が削除されます。管理対象のコンピュータの移動に伴う機器情報の流れを次の図に示します。



1.機器情報の収集

M03 の管理対象のコンピュータが M04 の配下に移動すると、M04 で機器情報が収集されます。

2.機器情報の通知（M04 から M02）

M04 は機器情報を追加したあと、M02 に機器情報を通知します。

3.機器情報の通知（M02 から M01）

M02 は機器の経路の変更を検知したあと、機器情報を更新します。また、M01 に機器情報を通知します。

4.機器情報の通知（M02 から M03）

M02 は M03 に機器情報の削除を通知します。M03 は機器情報を削除します。

機器情報の削除を通知する契機

管理用サーバ間で機器が移動すると、管理用サーバが持つ構成情報に機器の経路の変更が反映されます。これを契機として、機器情報の削除が移動元の管理用中継サーバに通知されます。

> **重要**
>
> 機器を移動する前に、移動元の管理用中継サーバのエージェント設定で接続先を変更する必要があります。詳細については、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の、エージェントが接続する管理用サーバを切り替える手順の説明を参照してください。

関連リンク

- 2.5.3　オンライン管理のコンピュータへのエージェント設定の割り当て

(5)　配下の管理用中継サーバへのソフトウェア検索条件の適用

複数サーバ構成では、自サーバで作成したソフトウェア検索条件を配下の管理用中継サーバに適用できます。検索条件を適用すると、すべての配下の管理用中継サーバに適用元の検索条件が追加されます。適用された検索条件とは別に、適用先の管理用中継サーバでも検索条件を追加できるため、管理用中継サーバごとに検索条件を運用することもできます。

上位の管理用サーバから適用されたソフトウェア検索条件は、適用先では変更できません。ただし、適用先で検索条件の削除はできます。例えば、上位の管理用サーバが検索条件の削除を適用しないままリプレースされてしまった場合は、不要な検索条件を適用先で削除します。

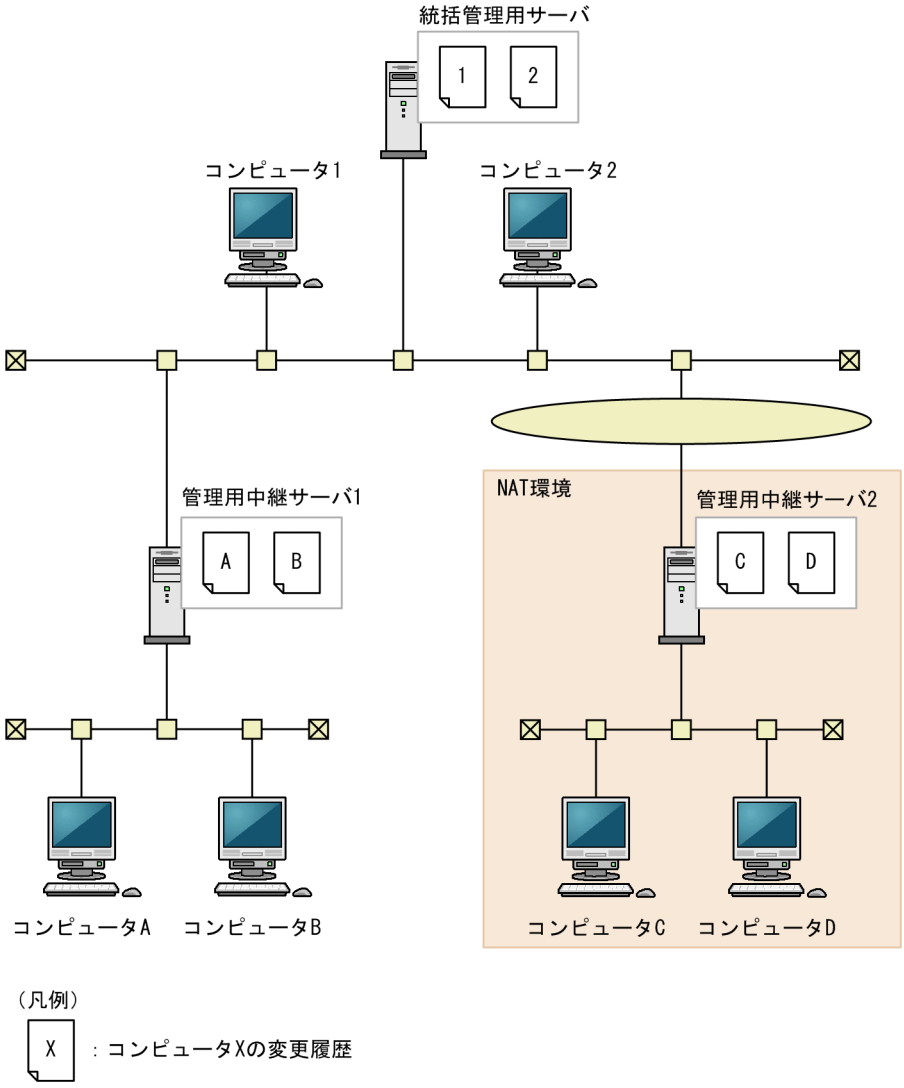
関連リンク

- (11)　情報を収集したいソフトウェアの検索条件の定義

(6)　配下の管理用中継サーバが管理対象とする機器の変更履歴の取得

複数サーバ構成の場合、機器の変更履歴の取得範囲を自サーバ直下の機器だけに絞り込めます。変更履歴の取得による管理用サーバの負荷を分散したいときは、自サーバ直下の機器以外の変更履歴を取得しないように設定してください。デフォルトでは、自サーバ直下の機器以外の変更履歴を取得します。

自サーバ直下の機器以外の変更履歴を取得しないように設定した複数サーバ構成の例を次に示します。



この例では、各管理用サーバが直下のコンピュータの変更履歴だけを取得しています。管理用中継サーバ 2 に管理者がいない場合は、統括管理用サーバの管理者が管理用中継サーバ 2 の操作画面を起動して変更履歴を確認します。

関連リンク

- (17)　機器の変更履歴の取得

(7)　複数サーバ構成での機器情報の削除

管理が不要になった機器を削除したい場合は、管理元の管理用中継サーバで機器情報を削除します。管理元の管理用中継サーバで機器情報が削除されると、上位の管理用サーバに機器情報の削除が通知され、上位の管理用サーバで機器情報が削除されます。

機器情報が削除される契機は、次のとおりです。

機器情報が削除される契機	削除後の処理
管理元の管理用中継サーバの操作画面で機器情報を削除したとき	上位の管理用サーバで機器情報が削除されます。
JP1/IT Desktop Management 2 - Agent をアンインストールしたとき	上位の管理用サーバで機器情報が削除されます。 この処理は、管理元の管理用中継サーバで設定したコンフィグレーションファイルの「State_AfterAgentUninstalling」の値に基づきます。コンフィグレーションファイルの設定によっては、機器情報を削除しないで、管理種別をエージェントレスに変更します。
ハードウェア資産の［資産状態］を［滅却］にしたとき	滅却した資産情報に関連づいている機器情報が、上位の管理用サーバ、および配下の管理用中継サーバから削除されます。
JP1/IT Desktop Management 2 - Asset Console で資産情報を削除したとき	
機器の接続先の管理用中継サーバを変更したとき	移動元の管理用中継サーバから機器情報が削除されます。

ヒント

機器情報の通知に失敗して、上位の管理用サーバと管理元の管理用中継サーバとで機器情報に不整合が起きてしまった場合は、上位の管理用サーバで配下の機器情報を手動で削除することで整合性を取ってください。この時は、機器情報の削除は通知されません。上位の管理用サーバからだけ機器情報が削除されます。

関連リンク

- 付録 A.5　プロパティ一覧

2.18.8　複数サーバ構成でのリモートコントロール

複数サーバ構成の場合、自サーバ直下だけでなく、配下の管理用中継サーバ、および管理元が配下の管理用中継サーバであるコンピュータもリモートコントロールできます。コンピュータの利用者からの問い合わせに対応したり、コンピュータの異常を検知した際に調査したりするのに便利です。

配下の管理用中継サーバ、および管理元が配下の管理用中継サーバであるコンピュータをリモートコントロールする場合、コントローラとリモコンエージェントで、使用するポート番号を統一する必要があります。使用するポート番号が異なる場合は、次のようにしてポート番号を設定し直してください。

- コントローラが使用するポート番号

  統括管理用サーバからコンピュータをリモートコントロールする場合は、コントローラの［環境の設定］ダイアログで設定してください。管理用中継サーバからリモートコントロールする場合は、次のどちらかの方法で設定してください。

  - コントローラの［環境の設定］ダイアログで設定する。
  - 管理用中継サーバのセットアップで設定する。

- リモコンエージェントが使用するポート番号
  次のどちらかの方法で設定してください。
  - 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（管理元が配下の管理用中継サーバであるコンピュータをリモートコントロールする場合）。
  - 管理用中継サーバのセットアップで設定する（管理用中継サーバをリモートコントロールする場合）。

なお、配下の管理用中継サーバ、および管理元が配下の管理用中継サーバであるコンピュータに対するリモートコントロールで次の機能を使用する場合は、コントローラの［環境の設定］ダイアログで AMT に関する設定が必要です。

- AMT を利用した電源 ON
- リモート CD-ROM 機能

2.18.9　複数サーバ構成でのネットワーク接続の管理

複数サーバ構成では、機器のネットワーク接続を統括管理用サーバまたは管理用中継サーバで管理できます。

ネットワーク接続を管理する方法には、次の 2 種類があります。

- JP1/NETM/NM - Manager と連携してネットワーク接続を管理する
- ネットワークモニタ機能を利用してネットワーク接続を管理する

JP1/NETM/NM - Manager と連携してネットワーク接続を管理する

統括管理用サーバで全体のネットワーク接続を管理する場合は、統括管理用サーバだけに JP1/NETM/NM - Manager をインストールします。各管理用サーバで管理対象のネットワーク接続を管理する場合は、各管理用サーバに JP1/NETM/NM - Manager をインストールします。

統括管理用サーバで全体のネットワーク接続を管理する場合は、ネットワーク制御リストの自動更新の対象範囲に統括管理用サーバの配下の管理用中継サーバを含めるように設定します。ネットワーク制御リストの自動更新の対象範囲に配下の管理用中継サーバが管理している機器を含めると、配下の管理用中継サーバから通知された機器情報に基づいて、対応する機器のネットワーク接続可否の情報（MAC アドレスおよび IP アドレス）が自動でネットワーク制御リストに追加、変更、削除されます。なお、デフォルトでは自動更新の対象範囲に配下の管理用中継サーバは含まれません。

ネットワーク制御リストの自動更新の対象範囲に統括管理用サーバの配下の管理用中継サーバを含める運用でも、配下の管理用中継サーバで管理している機器のネットワーク接続設定は、その機器を管理する管理用中継サーバで行ってください。注意事項を次に示します。

- 統括管理用サーバのネットワーク制御リストの設定画面で、配下の管理用中継サーバで管理する機器の接続設定を変更することはできますが、配下の管理用中継サーバの通知により上書きされます。

また、機器に複数の NIC がある場合、配下の管理用中継サーバで 1 個の NIC を許可する設定にすると、統括管理用サーバではすべての NIC が許可する設定になります。

重要

NAT 環境で自動更新の対象範囲に配下の管理用中継サーバが管理している機器を含めると、同じ IP アドレスの機器が重複してネットワーク制御リストに追加されることがあります。そのため、ネットワーク接続可否の判定形式を［IP アドレス］にすると、業務に使用している機器の接続が意図しないで遮断されるなど、トラブルにつながるおそれがあります。NAT 環境で自動更新の対象範囲に配下の管理用中継サーバが管理している機器を含める場合は、ネットワーク接続可否の判定形式を［MAC アドレス］または［MAC アドレス＋ IP アドレス］にすることをお勧めします。

ネットワークモニタ機能を利用してネットワーク接続を管理する

JP1/IT Desktop Management 2 のネットワークモニタ機能を利用して、各管理用サーバで管理対象のネットワーク接続を管理します。

ネットワークモニタ機能を利用してネットワーク接続を管理する場合は、単数サーバ構成でのネットワーク接続の管理と機能差異はありません。

関連リンク

- 2.8　機器のネットワーク接続の管理
- 2.8.8　ネットワーク制御リストの管理
- 2.8.15　ネットワーク制御リストの自動更新
- 4.4.13　JP1/NETM/NM - Manager 連携構成

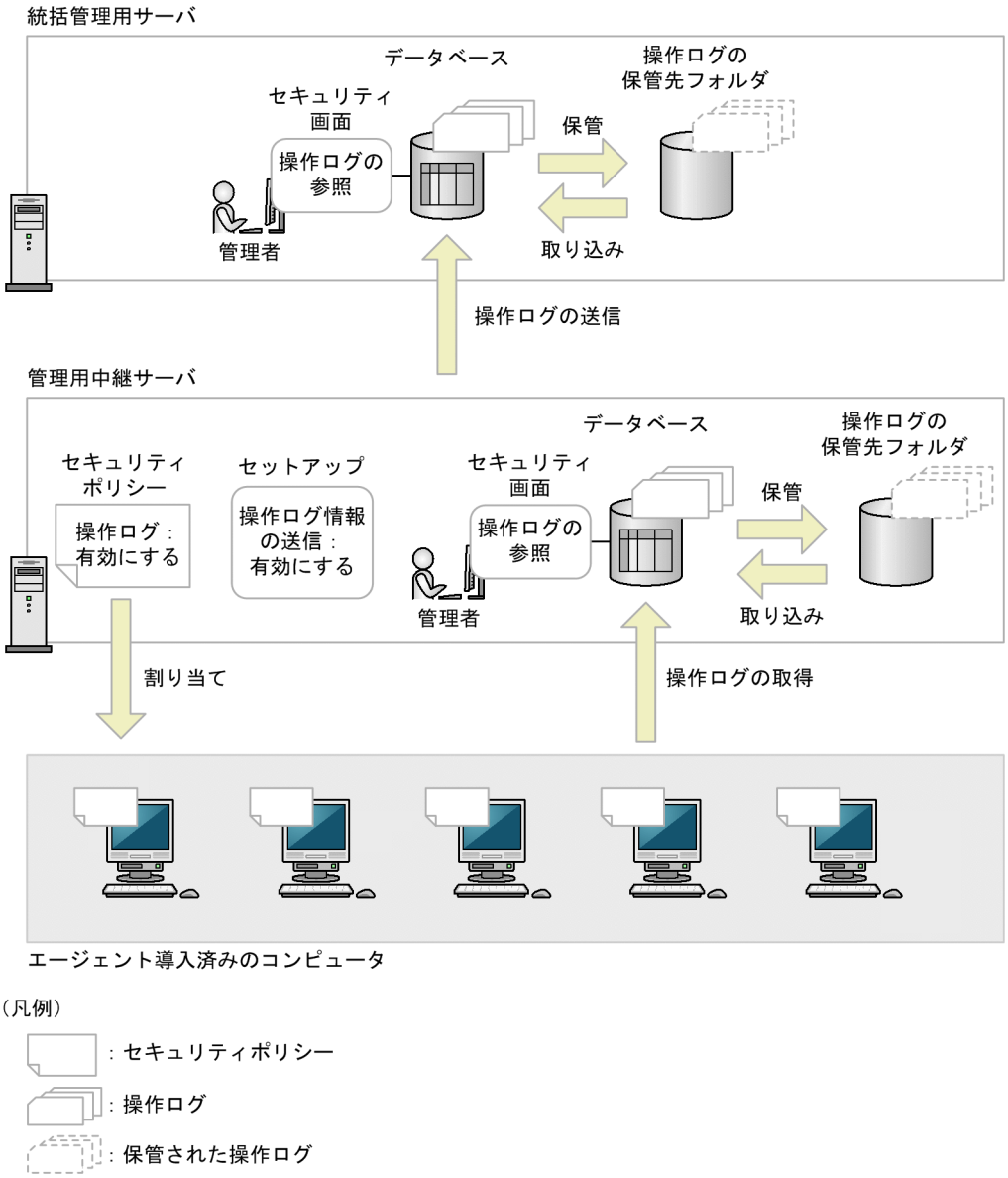
2.18.10　複数サーバ構成でのセキュリティの管理

複数サーバ構成の場合、各管理用サーバで直下のコンピュータのセキュリティを管理します。配下の管理用中継サーバが管理元であるコンピュータに対しては、自サーバからセキュリティポリシーを割り当てられません。そのため、セキュリティポリシーの設定を管理用サーバ間で統一したい場合は、同じ設定内容のセキュリティポリシーを各管理用サーバで作成してください。

2.18.11　複数サーバ構成での操作ログの管理

複数サーバ構成の場合、管理用中継サーバで取得した操作ログを上位の管理用サーバに送信できます。操作ログを上位の管理用サーバに送信すると、上位の管理用サーバの操作画面で下位の管理用中継サーバから送信された操作ログを参照したり、エクスポートしたりできるようになります。

管理用中継サーバで取得した操作ログを統括管理用サーバに送信する場合の操作ログの流れを次の図に示します。



下位の管理用中継サーバが送信した操作ログを上位の管理用サーバで参照するには、下位の管理用中継サーバで次の設定をしてください。

- セキュリティポリシーで操作ログの取得を有効にする。
- セットアップの［管理用中継サーバの設定］画面で操作ログを上位の管理用サーバに送信する設定にする。

セットアップの［管理用中継サーバの設定］画面で操作ログを送信する設定にした場合は、不審操作のログも含めて、すべての操作ログが上位の管理用中継サーバに送信されます。

下位の管理用中継サーバでも操作ログを参照したい場合は、セットアップの［操作ログの設定］画面で操作ログを取得する設定にしてください。

管理用中継サーバのセットアップについては、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の、管理理用中継サーバをセットアップする手順の説明を参照してください。

関連リンク

- 2.10　操作ログの管理

2.18.12　複数サーバ構成での資産の管理

複数サーバ構成の場合、管理用中継サーバが管理元である資産情報も、上位の管理用サーバでまとめて管理できます。あらかじめ、どの管理用サーバで資産を管理するか、管理範囲を決めておくことで漏れなく資産を管理できます。

ハードウェア資産情報

下位の管理用中継サーバに機器情報が追加されると、上位の管理用サーバに機器情報が通知されます。機器情報の通知を契機に上位の管理用サーバでは、機器情報に関連づいた資産情報が登録されます。

> **ヒント**
>
> USB デバイスの登録情報を上位の管理用サーバに送信したい場合は、下位の管理用中継サーバでセットアップしてください。詳細については、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の、管理用中継サーバをセットアップする手順の説明を参照してください。

なお、管理用サーバごとに編集した資産情報は、上位の管理用サーバおよび下位の管理用中継サーバに通知されません。ただし、次に当てはまる資産管理項目の値は、上位の管理用サーバから配下の管理用中継サーバに資産管理項目を適用することで、上位の管理用サーバに通知されるようになります。

- 資産情報と機器情報の共通管理項目
- ハードウェア資産情報の追加管理項目のうち、管理者が追加した追加管理項目

資産情報を滅却した場合は、上位の管理用サーバ、および下位の管理用中継サーバから資産情報の関連づけを解除し、機器情報も削除します。何らかの理由で、上位の管理用サーバ、および下位の管理用中継サーバでの機器情報の削除に失敗して、管理用サーバ間で機器情報の不整合が起きた場合は、機器情報の削除に失敗した管理用サーバ上で手動で機器情報を削除してください。

ソフトウェア情報、契約情報

ソフトウェア情報、契約情報は上位の管理用サーバに通知されません。資産管理の管理範囲の最上位の管理用サーバで更新してください。

> **ヒント**
>
> SAMAC 辞書は、管理用サーバごとに登録してください。

資産の関連づけ情報

資産の関連づけ情報は上位の管理用サーバに通知されません。資産管理の管理範囲の最上位の管理用サーバで更新してください。

関連リンク

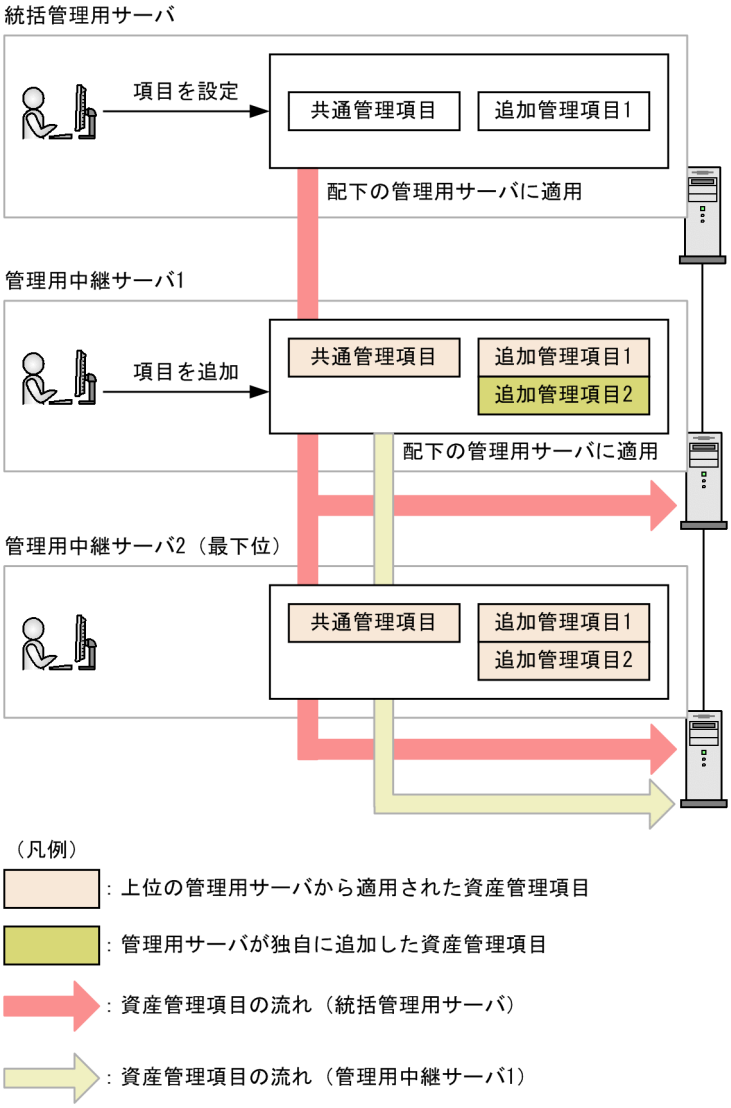
- 2.11　資産の管理

(1)　配下の管理用中継サーバへの資産管理項目の設定の適用

複数サーバ構成では、任意の管理用サーバからその配下の管理用中継サーバに対して自サーバの資産管理項目を適用できます。また、上位の管理用サーバから適用された共通管理項目の設定を編集したり、各管理用サーバで独自に追加管理項目を設定したりできます。配下の管理用中継サーバへの資産管理項目の設定は、設定画面の［資産管理項目の設定］画面から適用できます。

なお、上位の管理用サーバから適用された設定を管理用中継サーバで編集しても、複数サーバ構成内のほかの管理用サーバには反映されません。

配下の管理用中継サーバへの資産管理項目の設定の仕組みを次の図に示します。



配下の管理用中継サーバには利用者入力開始日時、共通管理項目、およびハードウェア資産情報の追加管理項目を適用できます。利用者入力開始日時は、適用先の管理用サーバで任意に編集できます。共通管理項目、およびハードウェア資産情報の追加管理項目の適用先での編集可否は次のとおりです。

資産管理項目		適用先での設定の編集可否					
		項目名	項目値	入力方法	説明	データ型	入力文字制限
共通管理項目	部署※1	×	○※2	×	×	×	×
	設置場所※1	×	○※2	×	×	×	×
	利用者名	×					
	アカウント	×					
	メールアドレス	×					
	電話番号	×					
追加管理項目	ハードウェア資産情報の追加管理項目※3	×					

（凡例）○：編集できる　×：編集できない（参照だけできる）

注※1　データ型が「選択型」または「階層型」の場合で項目値が設定されていないとき、適用元の資産管理項目の設定は配下の管理用中継サーバに適用されません。

注※2　データ型が「選択型」または「階層型」の場合に編集できます。

注※3　資産状態および機器種別の設定は配下の管理用中継サーバに適用されません。

重要

ハードウェア資産情報の追加管理項目を適用すると、適用元に設定されていないハードウェア資産情報の追加管理項目は、適用先のハードウェア資産情報の追加管理項目から削除されます。

ヒント

配下の管理用中継サーバから通知された機器情報に自サーバに登録されていない機器種別が含まれていた場合、自動で自サーバに機器種別が追加されます。

設定の適用に失敗する場合

次のような場合は、配下の管理用中継サーバへの資産管理項目の設定の適用に失敗します。

- 変更または削除される資産管理項目が、適用先の次の設定で使用されている場合
  - フィルタ条件
  - ハードウェア資産情報の追加管理項目の項目値
  - ユーザー定義のグループ条件
  - ユーザー定義のセキュリティ設定
  - あて先グループおよび ID の自動メンテナンスの条件
- 適用先のハードウェア資産情報の追加管理項目の項目数が上限を超える場合
  データ型ごとの項目数の上限は次のとおりです。
  - 数値型：20 件
  - 日付型：10 件
  - 選択型：20 件
  - テキスト型：75 件
- 適用元の追加管理項目と同じ名称の追加管理項目が適用先の管理用中継サーバに設定されている場合
- データベースのアクセスでエラーが発生した場合
- 管理用サーバ間のデータ通信でエラーが発生した場合
- 中継するデータファイルが壊れていた場合

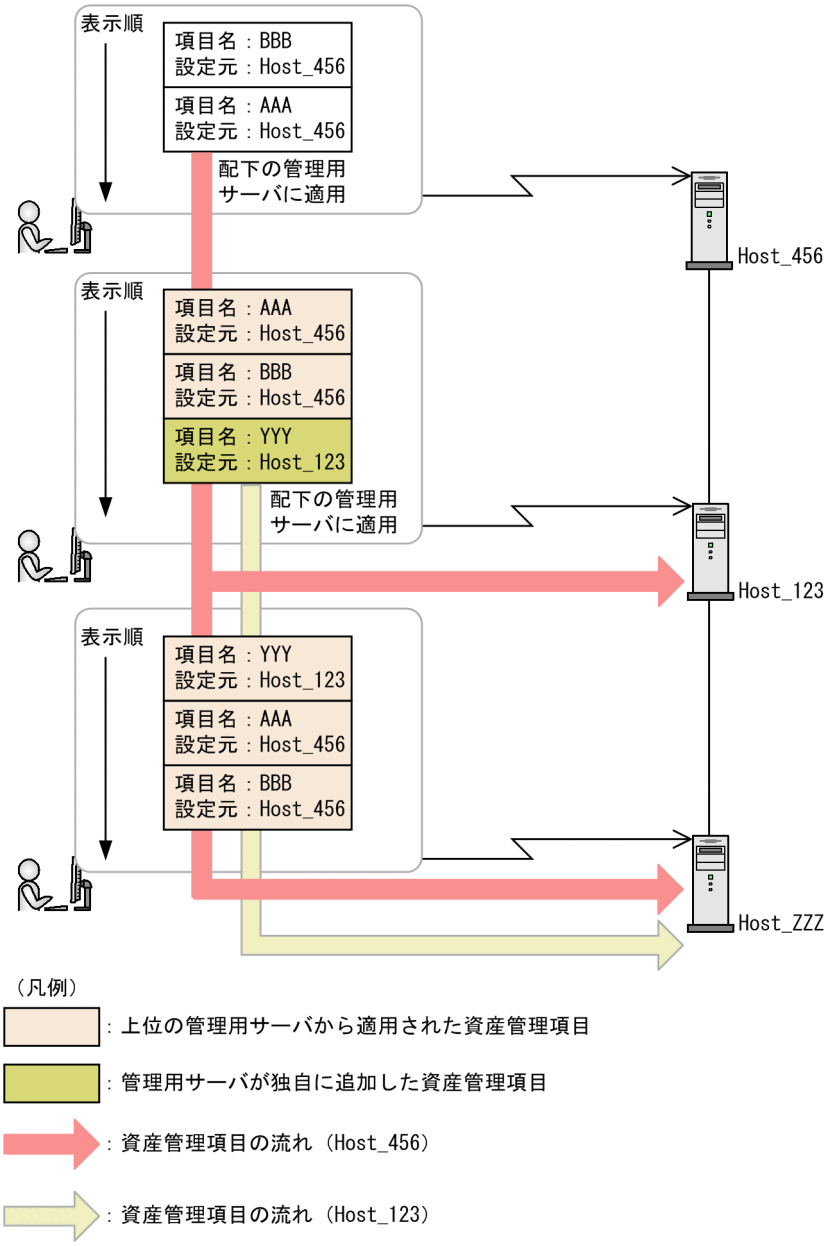
- データフォルダまたはローカルデータフォルダで I/O エラーが発生した場合

> **ヒント**
>
> 失敗した時点で、配下の管理用中継サーバへの資産管理項目の設定の適用は中断されます。

［資産管理項目の設定］画面に表示されるハードウェア資産情報の追加管理項目の表示順

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は、適用元のホスト名の名前順で設定画面の［資産管理項目の設定］画面に表示されます。適用元のホスト名が同じ項目同士は、項目の名前順で表示されます。各管理用サーバで独自に設定した追加管理項目は、上位の管理用サーバから適用された追加管理項目の後ろに続いて定義順で表示されます。

ハードウェア資産情報の追加管理項目の表示例を次の図に示します。



［利用者情報の入力］画面の項目の表示順

［利用者情報の入力］画面の項目の表示順は配下の管理用中継サーバに適用されません。上位の管理用サーバから新たに適用された項目は、表示順のいちばん下に追加されます。適用された項目が複数ある場合は、項目名でソートされた状態で追加されます。また、各管理用サーバで任意の表示順に変更できます。

適用先での部署・設置場所のグループの更新

配下の管理用中継サーバへの資産管理項目の設定の適用によって、適用先の部署や設置場所の項目値が更新された場合、適用先のグループも更新されます。

部署や設置場所の項目値が追加された場合

追加された項目値に対応する部署・設置場所のグループが適用先に追加されます。

部署や設置場所の項目値が変更された場合

変更後の項目値に対応する部署・設置場所のグループが適用先に追加されます。変更前の部署・設置場所のグループはそのまま残ります。

部署や設置場所の項目値が削除された場合

削除された項目値に対応する部署・設置場所のグループは適用先にそのまま残ります。

2.19　クラスタシステムでの運用

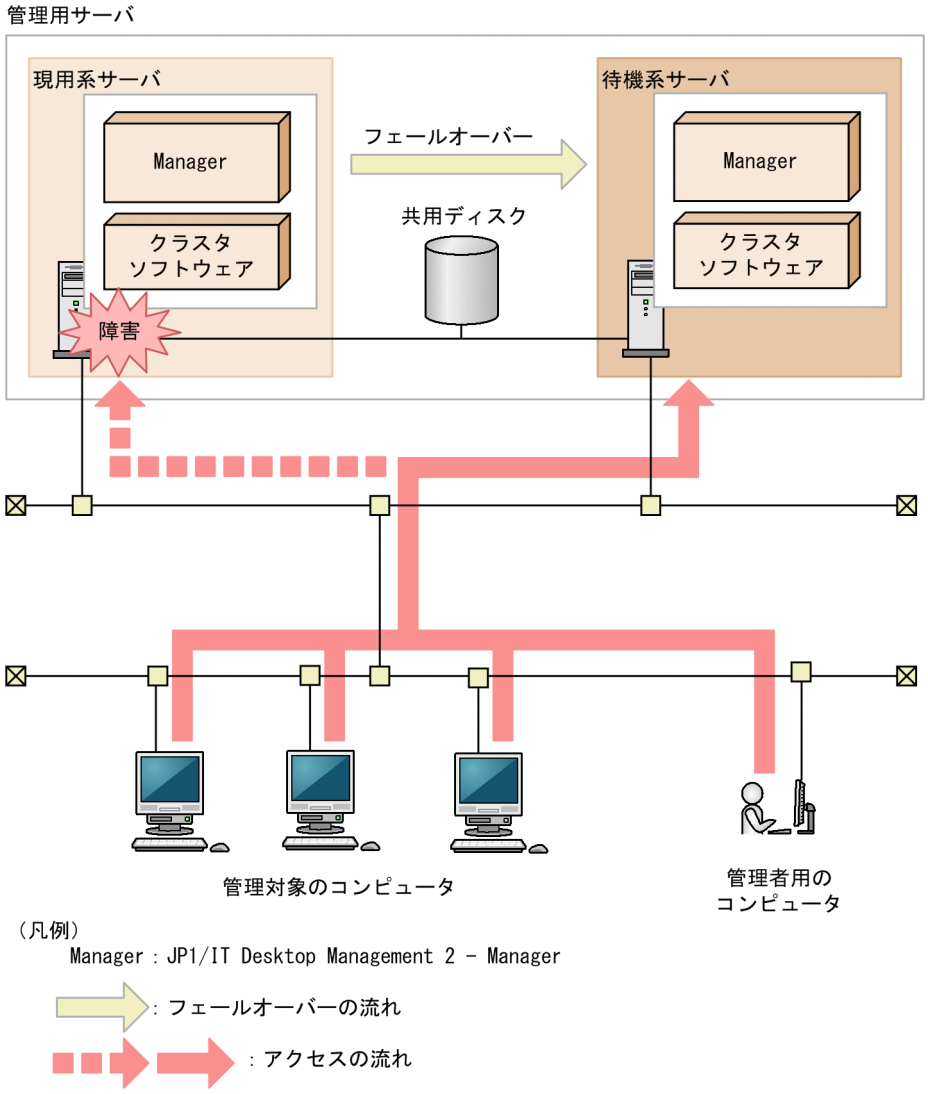
JP1/IT Desktop Management 2 はクラスタシステムでの運用に対応しています。

クラスタシステムとは、稼働中のサーバにトラブルが発生したときに、あらかじめ用意しておいたバックアップ用のサーバへ自動的に運用が切り替わるシステムです。クラスタシステムで運用することで、システム全体が停止することなく安定した運用が実現できます。これによって、トラブルの影響を受けることなく、JP1/IT Desktop Management 2 が提供するサービスを継続できます。

JP1/IT Desktop Management 2 は、Windows Server Failover Cluster を使用したクラスタシステムを導入でき、アクティブ・スタンバイ構成に対応しています。アクティブ・スタンバイ構成とは、サーバを 2 つ用意して、それぞれのサーバを現用系（メインのサーバ）と待機系（バックアップ用のサーバ）として設定します。

なお、バックアップ用のサーバに運用が切り替わることを、「フェールオーバー」といいます。フェールオーバー後は、バックアップ用のサーバで運用している間にメインのサーバを回復させ、運用環境を正常な状態に戻します。

JP1/IT Desktop Management 2 を導入したクラスタシステムの概要を次の図に示します。



クラスタシステムで運用する場合、管理用サーバには論理的なホスト名または IP アドレスが設定されます。管理対象のコンピュータは、このホスト名または IP アドレスに接続します。

論理的なホスト名または IP アドレスには、管理用サーバのホスト名または IP アドレスが対応づけられています。対応づけられたホスト名および IP アドレスが変更されても、論理的なホスト名または IP アドレスは変わりません。そのため、フェールオーバーが発生しても、コンピュータの接続先の設定を変更することなく、運用を続行できます。

重要

クラスタシステムに対応するのは、単数サーバ構成の管理用サーバ、および複数サーバ構成の統括管理用サーバだけです。管理用中継サーバ、およびネットワークモニタのクラスタシステムは構築できません。

2.20 データベースの管理

JP1/IT Desktop Management 2 では、管理用サーバに作成された専用のデータベースに、JP1/IT Desktop Management 2 が管理するさまざまな情報を格納します。

データベースは、障害に備えてバックアップを取得したり、パフォーマンスの効率化のために再編成したりして、定期的にメンテナンスしてください。

データベースのメンテナンスには、JP1/IT Desktop Management 2 が提供するデータベースマネージャを利用します。

データベースマネージャの機能を次に示します。

バックアップ

データベースのバックアップを取得する機能です。ディスク障害が発生した場合などには、データベースの情報が消えてしまったり、データベースが動作しなくなったりするおそれがあります。このため、運用時には定期的にデータベースのバックアップを取得してください。

なお、データベースのバックアップは、exportdb コマンドでも実行できます。

リストア

バックアップ機能またはexportdb コマンドを使用して取得したバックアップから、データベースを復元する機能です。データベースに障害が発生した場合は、取得したバックアップを使用してバックアップ時点の状態にリストアできます。

なお、データベースのリストアは、importdb コマンドでも実行できます。

再編成

データベースの長期間の運用によって領域の断片化が発生し、アクセス速度の低下などの問題が発生するおそれがあります。これを防止するため、JP1/IT Desktop Management 2 ではデータベースを再編成する機能を提供しています。データベースを再編成することでデータの内容を保持したまま格納編成を変更できるので、パフォーマンスの効率化が図れます。データベースの再編成は、目安として、データベース使用率が 80%になる前に実施してください。データベースの使用率はデータベースマネージャで確認できます。

なお、データベースの再編成は、reorgdb コマンドでも実行できます。

また、JP1/IT Desktop Management 2 のセットアップで、データベースのアップグレード、初期化およびフォルダの変更ができます。

バックアップしたデータをリストアできる環境を次の表に示します。

バックアップした環境	リストアする環境		
	単数サーバ構成の管理用サーバ	複数サーバ構成	
		統括管理用サーバ	管理用中継サーバ
単数サーバ構成の管理用サーバ	○	○	○

バックアップした環境		リストアする環境		
		単数サーバ構成の管理用サーバ	複数サーバ構成	
			統括管理用サーバ	管理用中継サーバ
複数サーバ構成	統括管理用サーバ	－	○	○
	管理用中継サーバ	－	－	○

（凡例）○：リストアできる　－：リストアできない

例えば、統括管理用サーバのバックアップを管理用中継サーバにリストアするように、異なる環境にリストアする場合は、別途、管理用サーバの設定を変更する必要があります。詳細については、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の、複数の複数サーバ構成システムを統合する手順の説明を参照してください。

2.20.1　バックアップ時に出力されるデータ

バックアップを実行すると、データベースに格納されている管理情報に加えて、データベース以外のフォルダに保存されている管理データのバックアップファイルが生成されます。バックアップは管理用サーバごとに生成できます。バックアップ時に生成されるファイルを次の表に示します。

ファイル名	説明
jdnexport.info	バックアップ情報が記録されたファイルです。
jdnexportdata.bak	データベース以外の管理データをアーカイブしたバックアップファイルです。
table.*テーブル名*.exp.bin	データベースの各テーブルのバックアップファイルです。
jdnagent.nid	OS のインストール先ディレクトリ（%SystemRoot%）に存在するファイルです。複数サーバ構成の場合に生成されます。

2.21　コマンドの利用

JP1/IT Desktop Management 2 では、各種機能を実行するためのコマンドを提供しています。Windows のタスクスケジューラなどと組み合わせて利用することで、定期的にバックアップを取得したり、最新情報を出力したりといった運用が自動的にできます。

サービスの停止と開始、データベースのバックアップとリストア、トラブルシュート用情報の取得などの主なコマンドについては、マニュアル「JP1/IT Desktop Management 2 運用ガイド」を参照してください。

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コマンドについては、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。

Asset Console を使用した資産管理に関するコマンドについては、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。

2.22　利用者のコンピュータ上での操作

コンピュータの利用者の操作が必要な場合で、コンピュータをオンライン管理しているときは、エージェントによってバルーンヒントやダイアログが表示されます。例えば、セキュリティポリシーに違反した利用者に対策を指示したり、ソフトウェアのダウンロードのタイミングを利用者に選択させたりできます。表示されるメッセージに従って適切に対処してください。

利用者による利用者情報の入力

追加管理項目が設定された場合、利用者の情報を入力してもらうために、ダイアログが各コンピュータに表示されます。利用者がダイアログで入力した情報が機器情報に反映されるため、管理者の入力の手間が省けます。利用者情報の入力の詳細については、「2.22.1　利用者による利用者情報の入力」を参照してください。利用者情報の入力画面の表示は、エージェント設定の［利用者への通知設定］で設定できます。エージェントの設定については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」を、エージェントの設定をする方法については、JP1/IT Desktop Management 2 オンラインヘルプを参照してください。

利用者のコンピュータ上のバルーンヒントの表示

利用者に通知する情報がある場合、コンピュータのタスクトレイのアイコンにバルーンヒントが表示されます。利用者は、バルーンヒントを確認してメッセージに従ってコンピュータを操作します。バルーンヒントの詳細については、「2.22.2　利用者のコンピュータ上のバルーンヒントの表示」を参照してください。バルーンヒントの表示は、エージェント設定の［利用者への通知設定］で設定できます。エージェントの設定については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」を、エージェントの設定をする方法については、JP1/IT Desktop Management 2 オンラインヘルプを参照してください。

利用者が電源 OFF の指示を受けた場合の動作

管理用サーバからコンピュータのシャットダウンの指示があると、コンピュータにその処理を確認するダイアログが表示されます。利用者はすぐにシャットダウンするか、あとで手動でシャットダウンするかを選択できます。詳細な情報については、「2.22.3　利用者が電源 OFF の指示を受けた場合の動作」を参照してください。

利用者が再起動の指示を受けた場合の動作

管理用サーバからコンピュータの再起動の指示があると、コンピュータにその処理を確認するダイアログが表示されます。利用者はすぐに再起動するか、手動で再起動するかを選択できます。詳細な情報については、「2.22.4　利用者が再起動の指示を受けた場合の動作」を参照してください。

利用者のコンピュータに配布が実行された場合の動作

ソフトウェアのダウンロード中に、タスクトレイのアイコンにバルーンヒントが表示されます。利用者は、バルーンヒントをクリックして、ダウンロードを一時停止できます。

また、ダウンロードしたソフトウェアをインストールする場合、インストール前メッセージが設定されていると、利用者に通知されます。利用者はすぐにインストールするか、あとでインストールするか選択できます。

詳細な情報については、「2.22.5　利用者のコンピュータに配布が実行された場合の動作」を参照してください。バルーンヒントの表示はエージェント設定の［利用者への通知設定］で設定できます。エー

ジェントの設定については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」を、エージェントの設定をする方法については、JP1/IT Desktop Management 2 オンラインヘルプを参照してください。

利用者のコンピュータでの操作が抑止された場合の動作

不正なソフトウェアの起動や大量の印刷を行ったり、または禁止されている外部メディアを使用したりすると、機能が抑止されます。情報の持ち出し、持ち込みを制限する場合に使用すると便利です。詳細な情報については、「2.22.6　利用者のコンピュータでの操作が抑止された場合の動作」を参照してください。

リモートコントロールの接続要求

コントローラから機器を参照できない NAT 環境や、機器の IP アドレスが変化する NAPT 環境の場合、コントローラ側からコンピュータにリモート接続することは困難です。このような場合、利用者のコンピュータからコントローラに対して接続要求を実行してもらうことで、リモートコントロールを開始できます。詳細な情報については、「2.7.16　接続先のコンピュータからコントローラへの接続要求」を参照してください。

2.22.1　利用者による利用者情報の入力

管理用サーバで追加管理項目の設定を変更した場合など、オンライン管理のコンピュータで利用者情報を入力する画面を表示できます。利用者情報の入力画面を表示するかどうかはエージェント設定の［利用者への通知設定］で選択できます。

また、利用者情報の入力を要求されている場合は、タスクトレイのアイコン（  ）のコンテキストメニューから利用者情報を入力する画面を表示することもできます。

資産管理項目の入力方法が［利用者が入力］の場合の、利用者情報を入力する画面の表示契機を次に示します。

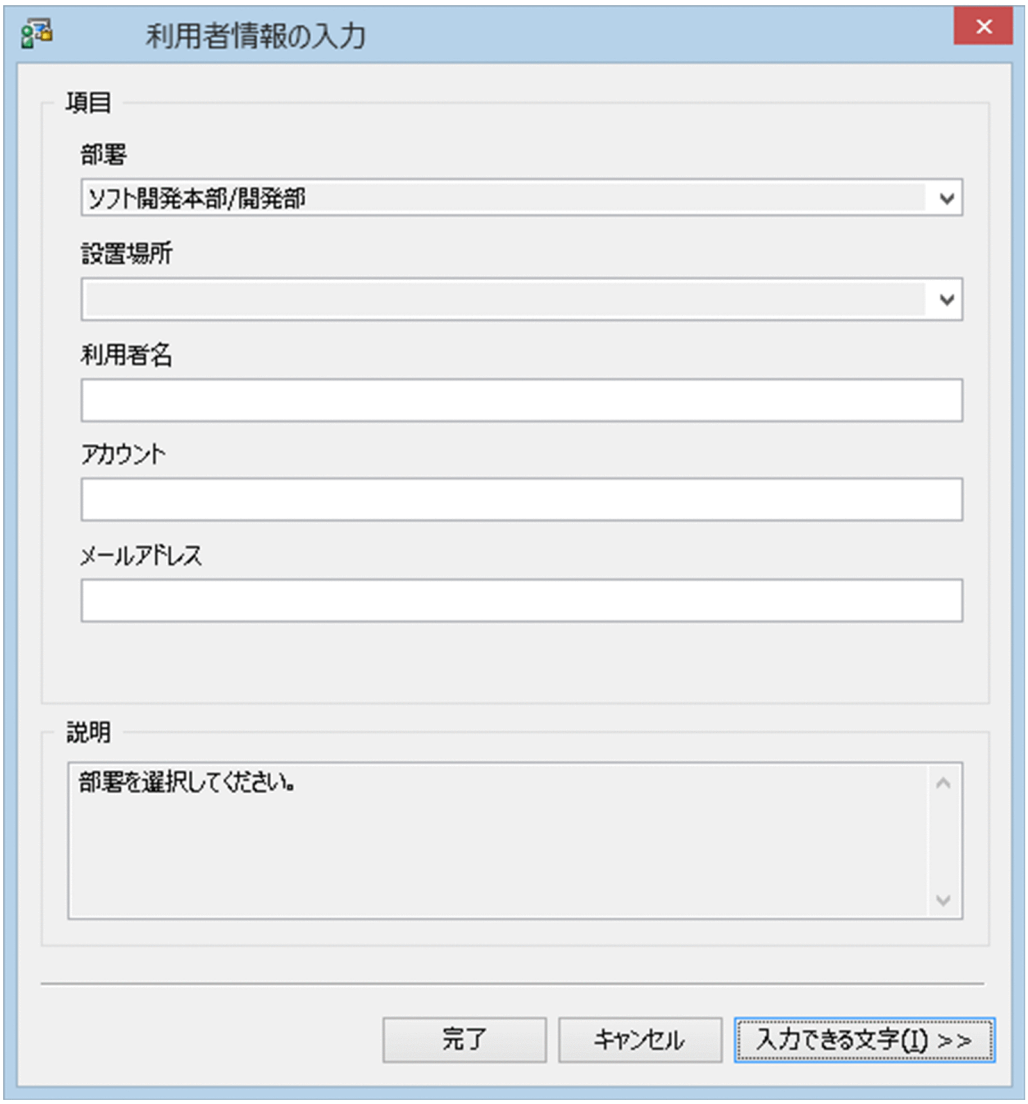
- 管理用サーバで資産管理項目を追加、編集、または削除したとき（削除した場合は、入力方法が［利用者が入力］の資産管理項目がほかにまだあるとき）
- 操作メニューの［最新の情報を取得する］で機器の最新の情報を取得したとき
- 操作メニューの［[利用者情報の入力］画面を定期的に表示させる］に設定されたタイミングに達したとき
- 設定画面の［利用者情報の入力開始日時］－［指定（利用者のコンピュータのローカルタイムで指定する入力開始日時)］を設定し、設定時刻に達したとき
- 前回の利用者情報の入力画面を表示してから 30 分経過したとき
- 利用者情報の入力画面を表示したあと項目を入力しないで画面を閉じて、30 分経過したとき
- 利用者がコンピュータにログオンしたとき

ヒント

資産管理項目の編集、追加、または削除をしたり、[最新情報を取得する]を実行したりすると、[利用者情報の入力開始日時]で設定している日時よりも前に、コンピュータに利用者情報の入力要求が表示されます。

利用者情報は、[利用者情報の入力]画面から入力します。[利用者情報の入力]画面に表示される項目は、管理用サーバで設定された拡張情報によって異なります。

[利用者情報の入力]画面の表示例を次の図に示します。



各項目の入力方法について説明します。なお、*の付いた項目は、必ず情報を入力してください。

テキストを直接入力する項目

テキストは、256 文字以内で入力できます。入力できる文字を確認したい場合は、[入力できる文字]ボタンをクリックして、文字情報を確認してください。

プルダウンメニューから選択する項目

プルダウンメニューから項目を選択します。選択できる項目が、ツリー型で表示される項目もあります。この項目から該当するテキストを選択してください。

[戻る] ボタン

直前のページに戻ります。項目が 6 つ以上の場合に表示されます。先頭ページの場合は表示されません。

[次へ] ボタン

次のページに進みます。項目が 6 つ以上の場合に表示されます。最終ページの場合は表示されません。

[完了] ボタン

入力した利用者情報を管理用サーバに通知し、[利用者情報の入力] 画面を閉じます。必ず入力する項目が未入力の場合は、入力を要求するメッセージが表示されます。

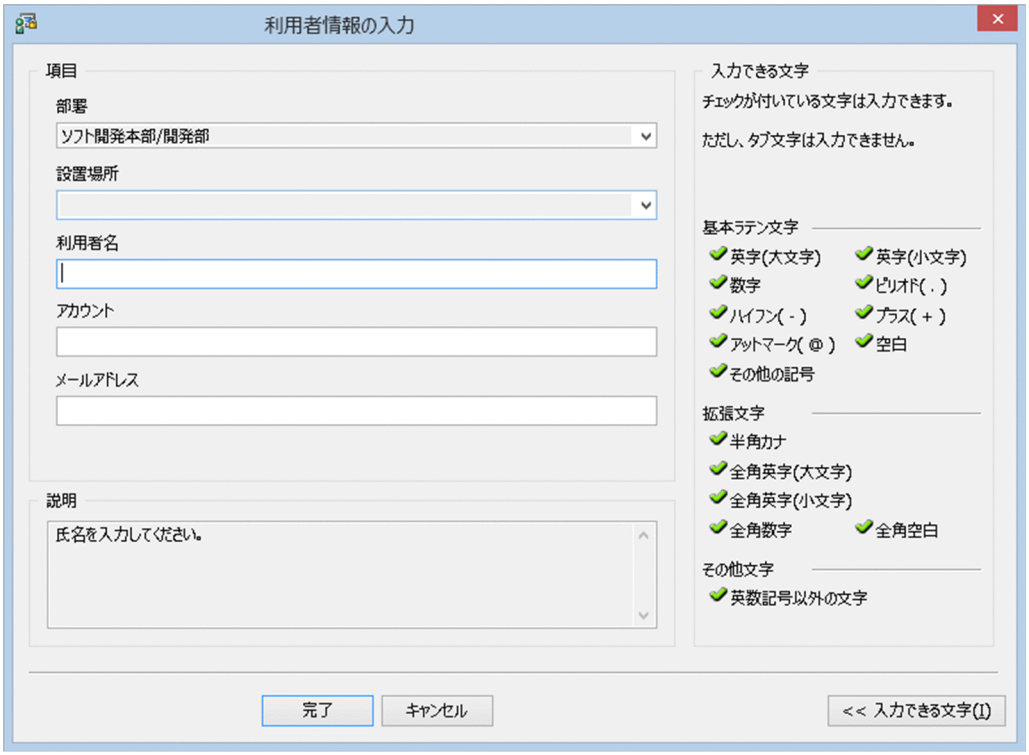
[キャンセル] ボタン

入力情報がキャンセルされます。

[入力できる文字] ボタン

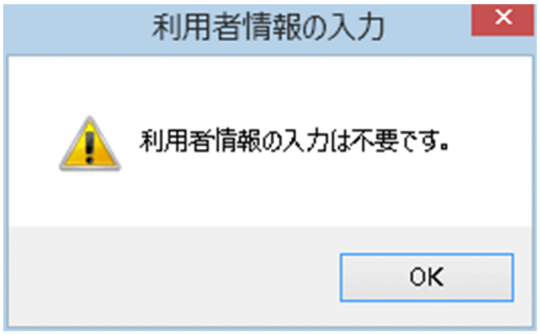
入力したい項目をポイントしてこのボタンをクリックすると、該当する項目で入力できる文字が表示されます。

入力できる文字の説明の表示例を次の図に示します。



入力できる文字の説明を非表示にする場合は、再度［入力できる文字］ボタンをクリックしてください。

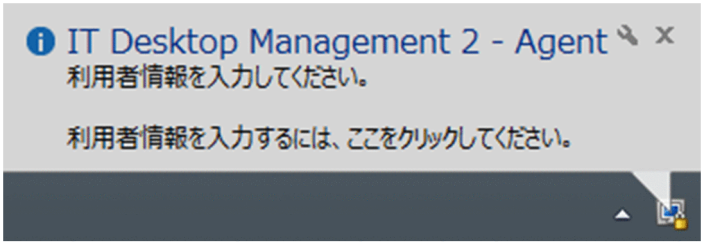
利用者情報の入力開始の日時を指定している場合で、指定した日時を経過していないときに、利用者のコンピュータで Windows の［スタート］メニューから［すべてのプログラム］－［JP1_IT Desktop Management 2 - Agent］－［利用者情報の入力］を選択すると、次の画面が表示されます。



なお、Citrix XenApp、Microsoft RDS サーバの場合は、利用者情報を入力する画面は表示されません。

2.22.2　利用者のコンピュータ上のバルーンヒントの表示

コンピュータの利用者の操作が必要な場合、タスクトレイのアイコンにバルーンヒントが表示されます。利用者はバルーンヒントを確認することで、どのような操作が必要か把握できます。バルーンヒントの表示例を次の図に示します。



バルーンヒントのタイトルの先頭には、メッセージ種別を示すアイコンが表示されます。メッセージ種別を示すアイコンの意味を次に示します。

- ：情報
- ：注意（危険度が低い情報）
- ：警告（危険度が高い情報）

バルーンヒントを表示するかどうかはエージェント設定の［利用者への通知設定］で選択できます。バルーンヒントの表示と非表示について、次の表に示します。

事象	表示されるメッセージ	クリック時の動作	バルーンヒントを非表示にした場合の影響と対処
システム管理者からセキュリティ判定結果のメッセージを受信した場合	システム管理者から、「(メッセージのタイトル)」についてのメッセージが届いています。メッセージを表示するには、ここをクリックしてください。	セキュリティ状況の判定結果のメッセージが表示されます。	利用者がメッセージを確認するには、タスクトレイのアイコンのコンテキストメニューから［メッセージの表示］を選択してください。

事象	表示されるメッセージ	クリック時の動作	バルーンヒントを非表示にした場合の影響と対処
コンピュータの再起動が必要なセキュリティポリシーが適用された場合※	次の理由で、コンピュータの再起動が必要です。コンピュータを再起動してください。 (1)セキュリティポリシーを適用して、コンピュータの設定を変更した。 (2)コンピュータに、最新のエージェントプログラムを適用した。 (3)コンピュータに、ソフトウェアや更新プログラムを適用した。	なし。	コンピュータがすぐに再起動されない場合、コンピュータへのセキュリティ対策が遅れることがあります。 業務中に再起動を促す必要がないコンピュータはバルーンヒントを非表示に、通常は再起動しないサーバは再起動の必要を知らせるためにバルーンヒントを表示に設定してください。
システム管理者から利用者情報の入力を要求された場合	利用者情報を入力してください。 利用者情報を入力するには、ここをクリックしてください。	［利用者情報の入力］画面が表示されます。	利用者情報を入力する画面を表示するには、タスクトレイアイコンのコンテクストメニューから［利用者情報の入力］を選択してください。

注※　再起動が必要なセキュリティポリシーは、「匿名接続の無効化」、「Windows 自動更新の有効化」、「リモートデスクトップ接続の無効化」、「管理共有の無効化」、「DCOM の無効化」、「デバイスの書き込み抑止」、「操作ログ/不審操作の有効・無効化」です。なお、「Windows ファイアウォールの有効化」は、コンピュータが Windows 7 または Windows Server 2008 R2 の場合は、再起動が必要です。

ヒント

バルーンヒントはソフトウェアのダウンロード中にも表示されます。詳細については、「2.22.5 利用者のコンピュータに配布が実行された場合の動作」を参照してください。

複数の事象が重なった場合、バルーンヒントは上記の表の順に重なって表示されます。表示されているバルーンヒントを閉じると、次のバルーンヒントが表示されます。

バルーンヒントは、表示されてから 10 秒経過するか、 ボタンをクリックすると閉じます。また、バルーンヒントをクリックしたときは、必要に応じて動作します。 なお、利用者がバルーンヒントの表示内容に沿った操作を実施しない場合は、前回のバルーンヒントが表示されてから 30 分後に、バルーンヒントが再表示されます。バルーンヒントの表示契機を次の表に示します。

コンピュータの状態	バルーンヒントの表示契機
ログオン中	セキュリティ判定結果のメッセージを受信するなどの事象発生後、すぐに表示されます。
	利用者がバルーンヒントの表示内容に沿った操作を実施しない場合は、前回のバルーンヒント表示から 30 分経過後に表示されます。
	利用者がバルーンヒントの表示内容に沿った操作を実施しない場合は、エージェントサービスの再起動時に表示されます。
ログオフ中	次回ログオン時に表示されます。

コンピュータの状態	バルーンヒントの表示契機
コンピュータのロック中	コンピュータのロック解除時に表示されます。

重要

コンピュータの OS が 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 の場合は、タスクトレイのアイコンは通常、非表示になっています。バルーンヒントの表示以外のときも常にアイコンを表示させる場合は、次のように設定してください。

Windows Server 2019、Windows Server 2016、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、または Windows Server 2008 R2 の場合

タスクバーの通知領域をカスタマイズして、JP1/IT Desktop Management 2 - Agent アイコンの動作を「アイコンと通知を表示」に設定してください。

Windows 10 の場合

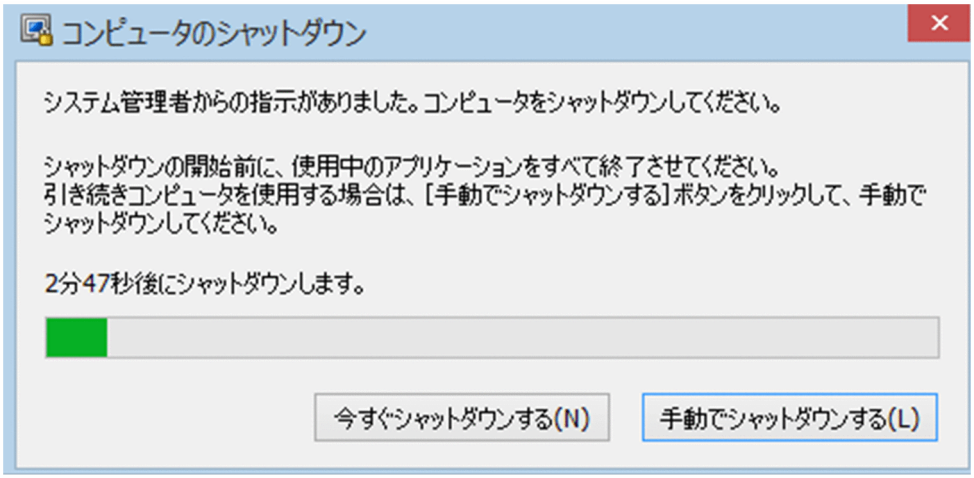
［設定］－［システム］－［通知と操作］－［タスクバーに表示するアイコンを選択してください］から、JP1/IT Desktop Management 2 - Agent のアイコンを ON に設定してください。

2.22.3 利用者が電源 OFF の指示を受けた場合の動作

管理用サーバからエージェント導入済みコンピュータに対して電源 OFF の指示があると、［コンピュータのシャットダウン］ダイアログが表示されます。

エージェント導入済みのコンピュータに［コンピュータのシャットダウン］ダイアログが表示されたあと、180 秒後に自動的にシャットダウンされます。

［コンピュータのシャットダウン］ダイアログを次の図に示します。



[今すぐシャットダウンする］ボタン

すぐにコンピュータがシャットダウンされます。

[手動でシャットダウンする］ボタン

コンピュータのシャットダウンがキャンセルされます。[コンピュータのシャットダウン］ダイアログは再表示されないため、利用者は手動でシャットダウンする必要があります。

シャットダウン時の注意事項を次に示します。

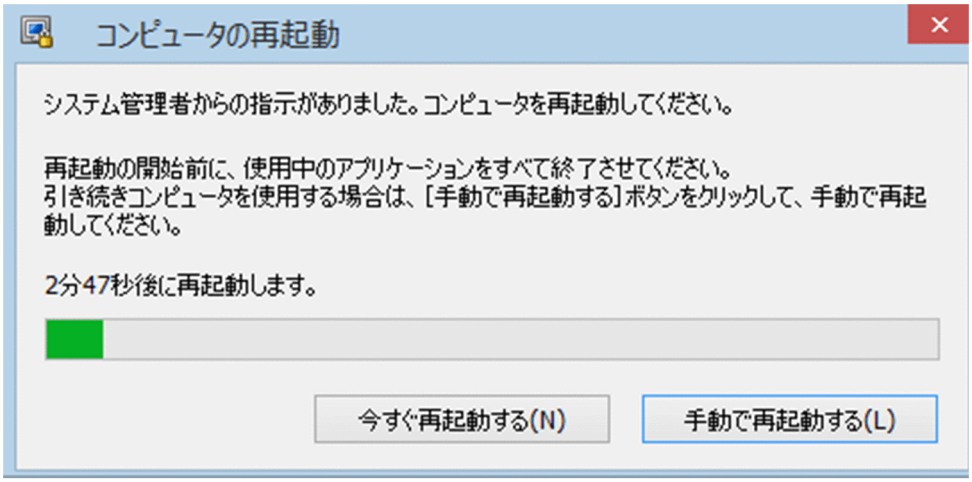
- スクリーンセーバーが起動しパスワードで保護している場合は、自動的にシャットダウンされません。
- コンピュータをロックしている場合は、自動的にシャットダウンされません。
- 編集中のファイルが存在する場合は、自動的にシャットダウンされません。
- ほかのユーザーがログオンしている場合は、自動的にシャットダウンされません。
- ログオン前の場合は、[コンピュータのシャットダウン］ダイアログが表示されないでシャットダウンされます。
- [コンピュータのシャットダウン］ダイアログの表示中に管理用サーバから電源 OFF の通知を受け取った場合は、後続の通知は無効になります。
- [今すぐシャットダウンする］ボタンを押してアプリケーションの終了を拒否した場合、シャットダウンはキャンセルされますが、管理コンソールには電源 OFF 状態として表示されることがあります。

2.22.4　利用者が再起動の指示を受けた場合の動作

管理用サーバからエージェント導入済みコンピュータに対して再起動の指示があると、[コンピュータの再起動］ダイアログが表示されます。このダイアログは、エージェント設定の［利用者への通知設定］－［コンピュータのシャットダウンと再起動の設定］の設定によって動作（再起動のタイミング）が異なります。

- [指定する時間内に利用者の応答がない場合に、自動的に開始する］を選択した場合は、利用者がダイアログを操作しなくても、ダイアログが表示されてからエージェント設定で指定した時間が経過すると、自動的にコンピュータが再起動されます。
- [シャットダウンまたは再起動を指示するダイアログでの、利用者の応答に従う］を選択した場合は、利用者がダイアログを操作すると、コンピュータが再起動されます。自動的には再起動されません。
- エージェント設定の［利用者への通知設定］－［コンピュータのシャットダウンと再起動の設定］の設定を無効にした場合、[コンピュータの再起動］ダイアログは表示されず、再起動もされません。

[指定する時間内に利用者の応答がない場合に、自動的に開始する］を選択した場合の［コンピュータの再起動］ダイアログを次の図に示します。



[今すぐ再起動する] ボタン

すぐにコンピュータが再起動されます。

[手動で再起動する] ボタン

コンピュータの再起動がキャンセルされます。[コンピュータの再起動] ダイアログは再表示されないため、利用者は手動で再起動する必要があります。

再起動時の注意事項を次に示します。

- スクリーンセーバーが起動しパスワードで保護している場合は、自動的に再起動されません。
- コンピュータをロックしている場合は、自動的に再起動されません。
- 編集中のファイルが存在する場合は、自動的に再起動されません。
- ほかのユーザーがログオンしている場合は、自動的に再起動されません。
- ログオン前の場合は、[コンピュータの再起動] ダイアログが表示されないで再起動されます。
- [コンピュータの再起動] ダイアログの表示中に管理用サーバから電源 OFF の通知を受け取った場合は、電源 OFF の通知だけが有効になります。このとき、[コンピュータの再起動] ダイアログはキャンセルされて、[コンピュータのシャットダウン] ダイアログが表示されます。

2.22.5 利用者のコンピュータに配布が実行された場合の動作

ソフトウェアの配布が実行された場合、タスクトレイのアイコンにバルーンヒントやダイアログが表示されます。ソフトウェアを配布するためには、配布（ITDM 互換）画面でパッケージおよびタスクを作成する必要があります。タスクには、ソフトウェアの配布の実行スケジュールや、対象のコンピュータにソフトウェアがダウンロードされたあとの実行タイミング、実行前メッセージなどを設定できます。

それぞれの場合の動作を次に示します。

ダウンロード

ダウンロードが開始されたとき、または利用者がコンピュータにログオンしたとき、タスクトレイのアイコンにバルーンヒントが表示されます。バルーンヒントの表示例を次の図に示します。

バルーンヒントのタイトルの先頭には、メッセージ種別を示すアイコンが表示されます。メッセージ種別を示すアイコンの意味を次の表に示します。

- ：情報
- ：注意（危険度が低い情報）
- ：警告（危険度が高い情報）

バルーンヒントを表示するかどうかはエージェント設定の［利用者への通知設定］で選択できます。バルーンヒントの表示と非表示について、次の表に示します。

事象	表示されるメッセージ	クリック時の動作	バルーンヒントを非表示にした場合の対処
ダウンロード開始	システム管理者から配布されたソフトウェアをダウンロードしています。 ダウンロードを一時停止するには、このアイコンをクリックしてください。	ダウンロードを一時停止する確認ダイアログが表示され、ダウンロードが一時停止されます。	ダウンロードを中断するにはダウンロードアイコンをクリックしてください。
ダウンロード再開			

バルーンヒントは、表示されてから 10 秒経過するか、 ボタンをクリックすると閉じます。また、バルーンヒントをクリックしたときは、必要に応じて動作します。 バルーンヒントの表示契機を次に示します。

コンピュータの状態	バルーンヒントの表示契機
ログオン中	ダウンロードを開始または再開したあと、すぐに表示されます。
	利用者がバルーンヒントの表示内容に沿った操作を実施しない場合は、エージェントサービスの再起動時に表示されます。
ログオフ中	次回ログオン時に表示されます。

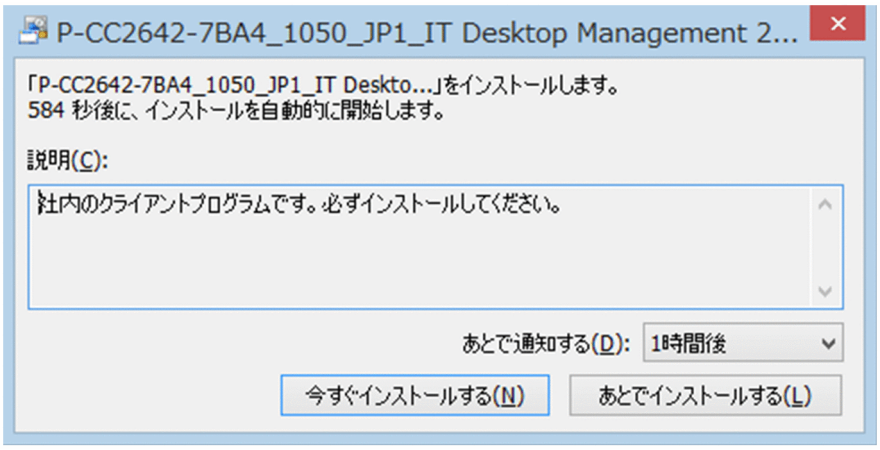
重要

コンピュータの OS が Windows Server 2019、Windows Server 2016、Windows 8.1、Windows 8、Windows Server 2012、Windows 7、または Windows Server 2008 R2 の場合は、タスクトレイのアイコンは通常、非表示になっています。バルーンヒントの表示以外のときも常にアイコンを表示させる場合は、タスクバーの通知領域をカスタマイズして、「jdnglogon」アイコンの動作を「アイコンと通知を表示」に設定してください。

コンピュータの OS が Windows 10 の場合は、JP1/IT Desktop Management 2 - Agent のアイコンを ON に設定してください。

インストール

配布されたソフトウェアをインストールする前に確認が必要なメッセージがある場合は、ダイアログで通知されます。ダイアログの表示例を次の図に示します。



[今すぐインストールする] ボタン

すぐにコンピュータにソフトウェアがインストールされます。

[あとでインストールする] ボタン

ソフトウェアのインストールがキャンセルされます。[あとで通知する] で指定した時間が経過すると、再度ダイアログが表示されます。

ダイアログはソフトウェアのインストールを実行する前に表示されます。ダイアログの表示契機は、コンピュータの状態と管理者が配布タスクに設定したソフトウェアのインストールタイミング（実行タイミング）によって異なります。

ダイアログの表示契機を次に示します。

コンピュータの状態	実行タイミング	ダイアログの表示契機
ログオン中	次回起動時に実行※	すぐに表示されます。
	すぐに実行※	

コンピュータの状態	実行タイミング	ダイアログの表示契機
ログオン中	ユーザーログオン時に実行	すぐに表示されます。
ログオフ中	次回起動時に実行	表示されません。
	すぐに実行	
	ユーザーログオン時に実行	次回ログオン時に表示されます。

注※　インストール確認ダイアログを表示したままの場合、または［あとでインストールする］ボタンをクリックした場合にコンピュータを再起動すると、コンピュータ起動後にインストール確認ダイアログを表示しないでインストールを開始します。

2.22.6　利用者のコンピュータでの操作が抑止された場合の動作

不正なソフトウェアを起動したときや印刷操作をしたとき、または禁止されているデバイスを使用したときに、それぞれの機能が抑止されます。社内のセキュリティを安全に保つために、情報の持ち込み、持ち出しを禁止する場合は、この機能を使うと便利です。

ソフトウェアの起動抑止

許可されていないソフトウェアを起動したときや、時間指定で許可されているソフトウェアを利用しているときに［ソフトウェアの起動抑止］ダイアログが表示されます。利用状況によって、ソフトウェアは自動停止されます。

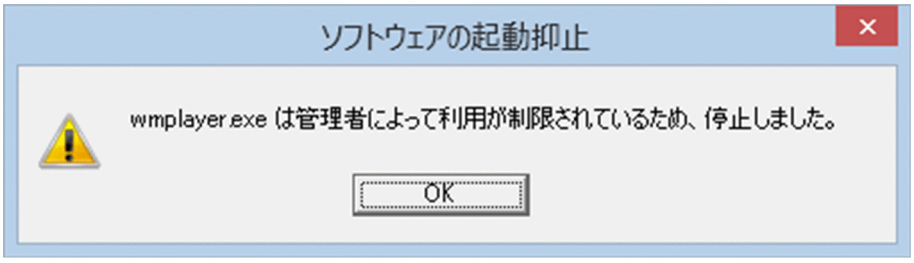
［ソフトウェアの起動抑止］ダイアログの［OK］ボタンをクリックすると、ダイアログが閉じます。

［ソフトウェアの起動抑止］ダイアログに表示される通知について説明します。

なお、利用者のコンピュータの OS が Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8、または Windows Server 2012 の場合、ダイアログはデスクトップに表示されます。

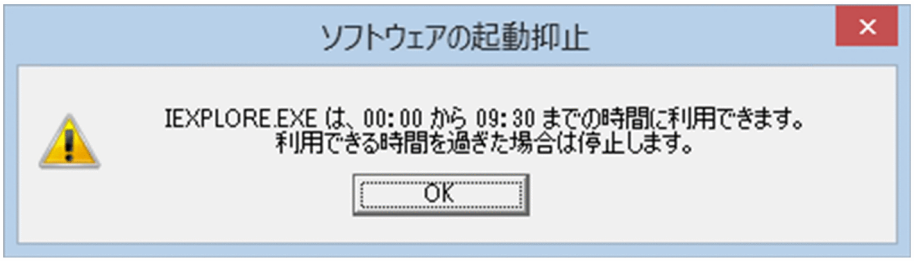
起動抑止の通知

許可されていないソフトウェアを起動しようとした場合に表示されます。表示例を次の図に示します。



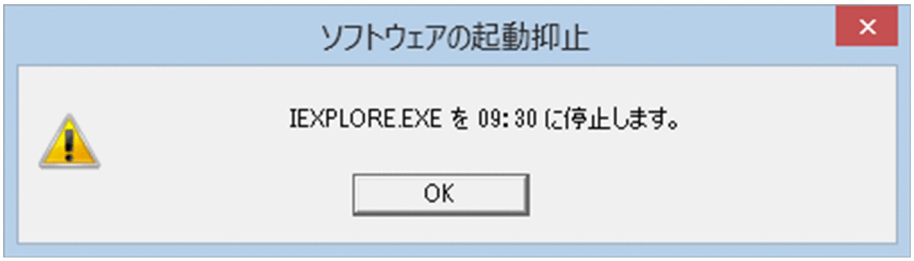
利用許可時間の通知

時間指定で許可されているソフトウェアを許可時間内に利用した場合に表示されます。表示例を次の図に示します。



利用停止時間の通知

時間指定で許可されているソフトウェアの許可時間の終了が間近になった場合に表示されます。利用時間が過ぎた場合は、自動的にソフトウェアが停止されます。表示例を次の図に示します。

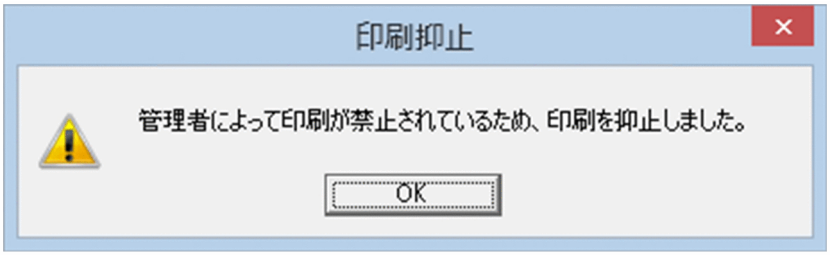


印刷の抑止

印刷を抑止するセキュリティポリシーが適用されているエージェント導入済みコンピュータが印刷を実行すると、印刷を抑止する［印刷抑止］ダイアログが表示されます。［OK］ボタンをクリックすると、このダイアログが閉じます。

なお、利用者のコンピュータの OS が Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8 または Windows Server 2012 の場合、ダイアログはデスクトップに表示されます。

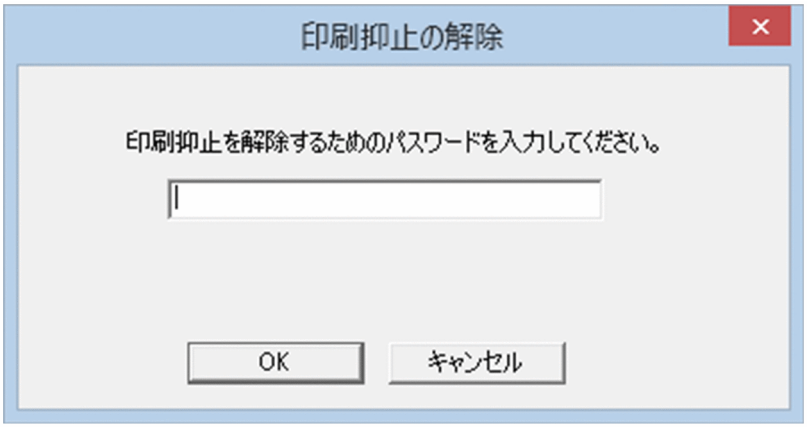
［印刷抑止］ダイアログを次の図に示します。



印刷抑止解除パスワードを利用できる場合は、印刷の抑止を解除できます。印刷抑止解除パスワードを利用して印刷の抑止を解除するには、タスクトレイにある印刷抑止アイコン（ ）をダブルクリックしてください。［印刷抑止の解除］ダイアログ（パスワード入力）が表示されます。印刷を許可できるパスワードを入力し、［OK］ボタンをクリックしてください。

なお、利用者のコンピュータの OS が Windows Server 2019、Windows Server 2016、Windows 10、Windows 8.1、Windows 8 または Windows Server 2012 の場合、ダイアログはデスクトップに表示されます。

［印刷抑止の解除］ダイアログ（パスワード入力）を次の図に示します。



印刷の抑止を解除できた場合は、［印刷抑止の解除］ダイアログ（成功）が表示されて、印刷できるようになります。印刷の抑止の解除に失敗した場合は、［印刷抑止の解除］ダイアログ（失敗）が表示されます。［OK］ボタンをクリックすると、ダイアログが閉じます。

印刷抑止解除パスワードを利用できないときに印刷抑止アイコン（ ）をクリックすると、印刷抑止中ダイアログが表示されます。［OK］ボタンをクリックすると、ダイアログが閉じます。

機器の抑止

セキュリティポリシーでメッセージの表示を設定している場合、デバイスの使用を抑止するセキュリティポリシーが適用されているエージェント導入済みコンピュータがデバイスを使用すると、［デバイスの使用抑止］ダイアログが表示されます。［OK］ボタンをクリックすると、このダイアログが閉じます。

2.22.7　エージェントからの通知対象となるユーザー

複数のユーザーが同一のコンピュータにログオンしている場合、一部のユーザーだけにエージェントによってバルーンヒントやダイアログなどの情報が通知されます。通知対象となるユーザーを制限することで、対応が不要なユーザーが情報を確認する手間を省けます。

エージェントをインストールしているコンピュータの OS ごとに、通知対象となるユーザーを示します。

Windows 10、Windows 8.1、Windows 8、または Windows 7 の場合

- すべてのログオンユーザー
- リモートデスクトップ接続したユーザー

Windows Server 2019、Windows Server 2016、Windows Server 2012、または Windows Server 2008 R2 の場合

- ローカルコンソールにログオンしたユーザー
- リモートデスクトップ接続で最初にログオンした管理者権限のユーザー

2.22.8　利用者がコンピュータを操作する際の注意事項

- 利用者のコンピュータ上で次のアプリケーションを無効にしないでください。無効にすると、JP1/IT Desktop Management 2 の一部の機能が正常に動作しなくなります。
  - jdngrcagent.exe
  - jdngrcchat.exe
  - jdnglogon.exe
  - jdngsmclogin.exe

2.23　スマートデバイスの制御

MDM システムと連携すると、JP1/IT Desktop Management 2 から管理対象のスマートデバイスを制御できます。この機能を使用すると、MDM システムを操作しないでスマートデバイスを制御できるため便利です。

複数サーバ構成の場合、スマートデバイスを制御したい管理用サーバごとに MDM システムと連携する必要があります。

MDM システムと連携すると、スマートデバイスに対して次に示す制御ができます。

スマートデバイスのロック

利用者がスマートデバイスを紛失した場合、拾得者が操作できないように管理者がスマートデバイスをロックできます。

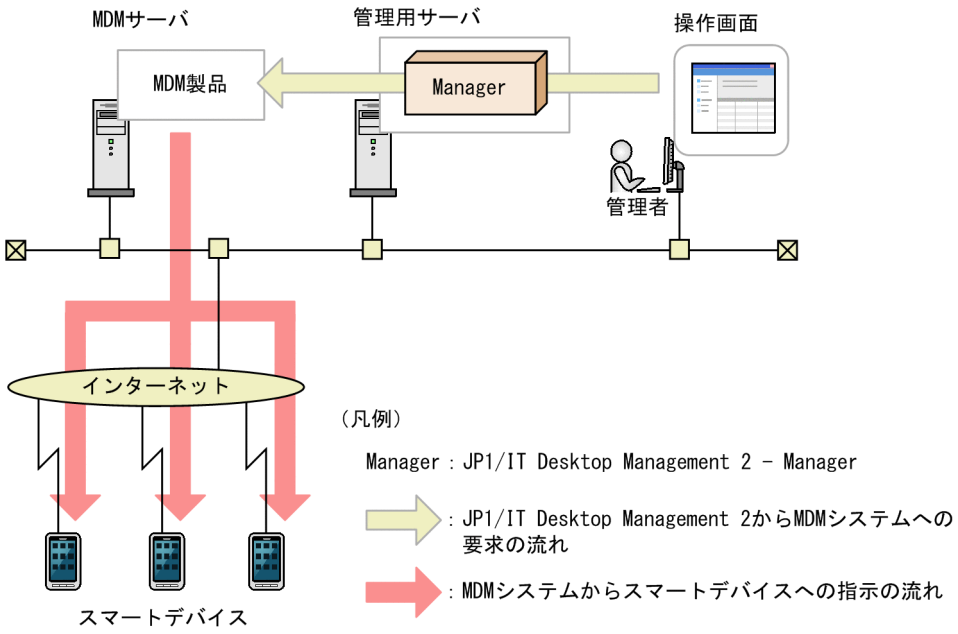
スマートデバイスのパスコードのリセット

利用者がスマートデバイスのパスコードを忘れた場合、利用者がパスコードを再設定できるように、管理者がスマートデバイスのパスコードをリセットできます。

スマートデバイスの初期化

スマートデバイスの利用者を変更したり、スマートデバイスを滅却したりする場合、スマートデバイスを初期化して、工場から出荷されたときの状態にできます。

スマートデバイスの制御は、JP1/IT Desktop Management 2 が出す要求に従って、MDM システムから実行されます。スマートデバイスを制御する流れを次の図に示します。



重要

MDM システムとの連携の設定を削除すると、その MDM システムで管理されているスマートデバイスの制御はできなくなります。

重要

複数サーバ構成の場合、異なる管理用サーバに同じ設定の MDM システムを連携させないでください。それぞれの管理用サーバが MDM システムから情報を取得するタイミングで、スマートデバイスの管理元が意図しないで変更されるため、スマートデバイスを正常に制御できなくなるおそれがあります。

ヒント

JP1/IT Desktop Management 2 は、MDM システムが要求を受けた時点で、スマートデバイスが制御できたと見なします。

関連リンク

- 2.6.6　MDM システムとの連携

2.24　社外で利用する機器の管理

JP1/IT Desktop Management 2 では、管理対象のコンピュータが社外からインターネットを介して接続されている場合でもオンライン管理できます。管理用サーバと利用者のコンピュータが VPN を使用して接続している場合だけでなく、VPN を使用せず接続している場合も管理できます。

> **ヒント**
>
> 管理対象のコンピュータにはエージェントが導入されている必要があります。

VPN 接続

管理対象のコンピュータは、VPN を使用して管理用サーバと接続します。JP1/IT Desktop Management 2 では VPN 接続環境を設定するバッチファイルを提供し、配布機能を使用して VPN 接続環境の設定を簡単にできるようにしています。

インターネット接続

組織ネットワークの DMZ にインターネットゲートウェイサーバを設置し、管理用サーバと接続します。管理対象のコンピュータは、インターネットゲートウェイサーバを介して管理用サーバと接続します。管理対象のコンピュータとインターネットゲートウェイサーバは HTTPS で接続します。

接続形態による機能差異

管理対象のコンピュータが VPN 接続されている場合とインターネット接続の場合では、管理用サーバから実行できる機能に差異があります。接続形態による機能差異を次の表に示します。

機能		管理対象のコンピュータ	
		VPN 接続	インターネット接続
機器情報の収集		○	○
セキュリティ状況の診断	セキュリティポリシーの割り当て	○	○
	セキュリティ状況の診断	○	○
セキュリティポリシーの違反時のアクション	セキュリティの自動対策	○	○
	印刷の抑止	○	○
	データの持ち出し抑止	○	○
	ソフトウェアの起動抑止	○	○
	操作ログの取得	○	○
	メッセージの通知	○	○
	電源の ON	×	×
資産情報の管理	ハードウェアの管理	○	○

機能		管理対象のコンピュータ	
		VPN 接続	インターネット接続
資産情報の管理	ソフトウェアライセンスの管理	○	○
	ソフトウェアの管理	○	○
	契約の管理	○	○
ソフトウェアおよびファイルの配布	ソフトウェアの配布	○	○ ※
	ファイルの配布	○	○ ※
	ソフトウェアのアンインストール	○	○
機器のリモートコントロール	コンピュータの操作	○	×
	コンピュータからの接続要求	○	×
	ファイル転送	○	×
	チャット	○	×
機器のネットワーク接続の管理	ネットワークモニタの有効化	×	×
	ネットワーク接続の制御	×	×
レポートの作成		○	○

（凡例）○：対象となる　×：対象外

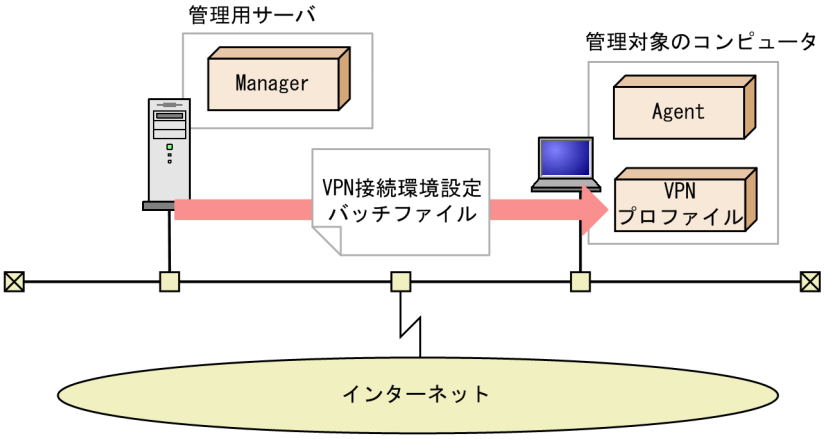
注※　中継システムは使用できません。

2.24.1　VPN で接続する場合の機器の管理

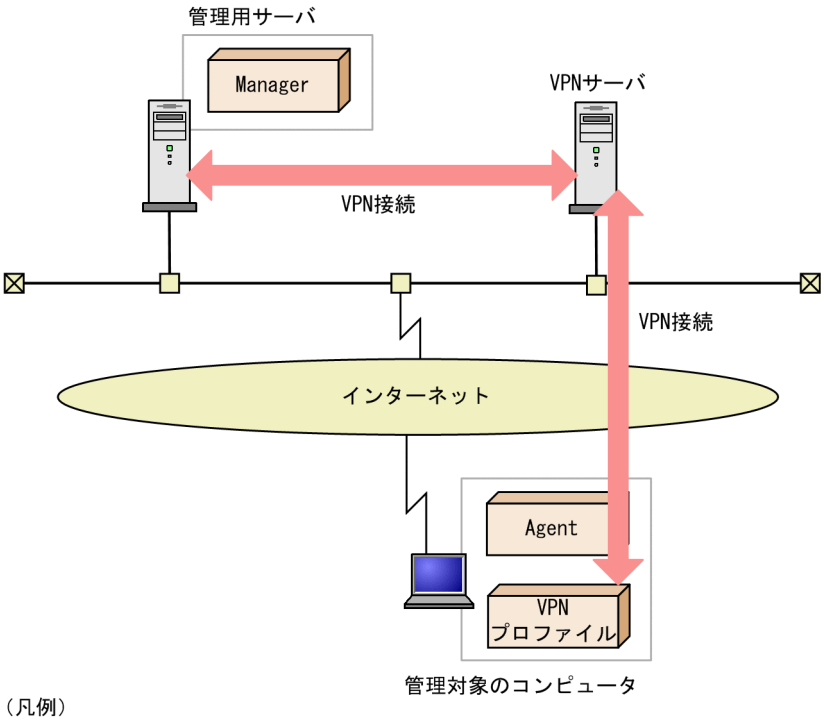
在宅勤務やサテライトオフィス勤務などで社外に持ち出した管理対象のコンピュータを VPN で接続することで、JP1/IT Desktop Management 2 で管理できます。

管理対象のコンピュータを VPN で接続するためには、事前に VPN 接続を設定する必要があります。JP1/IT Desktop Management 2 の配布機能で、VPN 接続環境を設定するバッチファイルを管理対象のコンピュータに配布すると、VPN 接続環境の設定が簡単にできます。

■コンピュータの社外持ち出し前



■コンピュータの社外持ち出し中



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager
Agent：JP1/IT Desktop Management 2 - Agent

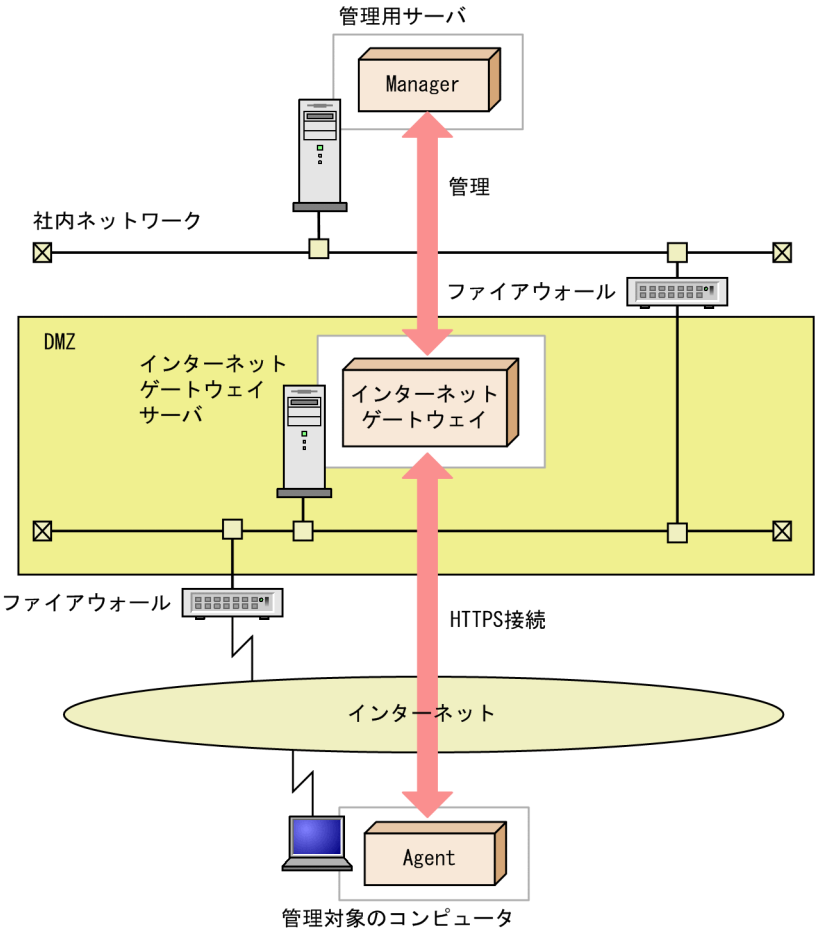
JP1/IT Desktop Management 2 では、Windows 標準の VPN クライアント環境を設定するためのサンプルバッチファイルを提供しています。

管理対象のコンピュータの VPN 接続設定の詳細については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の社外持出し用 PC の VPN 接続設定の説明を参照してください。

2.24.2　インターネットで接続する場合の機器の管理

在宅勤務やサテライトオフィス勤務などで社外に持ち出した管理対象のコンピュータに VPN の設定をせずに JP1/IT Desktop Management 2 で管理することもできます。

この場合、組織ネットワークの非武装地帯（DMZ）にインターネットゲートウェイサーバを設置し、管理用サーバと接続します。管理対象のコンピュータは、インターネットゲートウェイサーバを介して管理用サーバと接続します。管理対象のコンピュータとインターネットゲートウェイサーバは HTTPS で接続します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager
Agent：JP1/IT Desktop Management 2 - Agent

> **重要**
>
> インターネットで接続してコンピュータを管理する場合、VPN で接続する場合とは使用できる機能に差異があります。詳細は、「2.24　社外で利用する機器の管理」を参照してください。

(1)　接続機器の管理

インターネット接続での機器の管理について説明します。

前提条件

インターネット接続で管理する機器の前提条件を次に示します。

- 管理できる機器は、OS が Windows のコンピュータだけです。
- 管理対象コンピュータにエージェントをインストールする必要があります。
- 管理対象コンピュータではネットワークモニタを無効にする必要があります。

> **重要**
>
> エージェントレスの機器は管理できません。

> **重要**
>
> 管理対象のコンピュータを社外に持ち出して使用する時は、意図せずにコンピュータが起動されることを防ぐために、Wake on LAN および AMT の BIOS の設定を無効にしてください。

インターネット接続で機器を管理するには：

管理対象コンピュータの設定画面のエージェント設定で、［基本設定］－［インターネットゲートウェイを経由して上位システムと HTTPS 通信する］をチェックする必要があります。

この設定をすると、エージェントはインターネットゲートウェイ経由で管理用サーバや中継システムと通信します。

ネットワーク接続の制御

管理対象コンピュータを社外で利用している場合、ネットワーク接続の制御はされません。

また、管理対象コンピュータを社外で利用している場合、社内ネットワークで管理されている IP アドレスと異なる IP アドレスが設定されます。このため、ネットワーク接続の制御をネットワーク制御リストで行い、かつ IP アドレスの判定で運用すると、管理対象コンピュータのネットワーク接続の制御が誤作動する恐れがあります。このため、ネットワーク接続の制御をネットワーク制御リストで行う場合は、MAC アドレスの判定で運用してください。

社内に持ち帰った管理対象コンピュータの接続先の切り替え

管理対象のコンピュータを社内に持ち帰った時に、インターネットゲートウェイを経由しないで、管理用サーバや中継システムと直接通信する動作となるように運用できます。

管理対象コンピュータが社内からインターネットゲートウェイに通信できないように、ファイアウォールおよびプロキシサーバの設定が必要です。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説明を参照してください。

(2) インターネット接続管理機器の注意事項

インターネット接続での機器の管理について注意事項を次に示します。

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場合

- セキュリティの自動対策または手動対策は、エージェントからのポーリング時に実行されます。
- 管理者によるコンピュータへの操作は、エージェントからのポーリング時に実行されます。
- ITDM 互換配布でのソフトウェアおよびファイルの配布は、エージェントからのポーリング時に実行されます。
- リモートインストールマネージャを使用するソフトウェアおよびファイルの配布ジョブは、エージェントからのポーリング時に実行されます。
- リモートコレクト機能で 1GB を超えるような容量の大きいファイルを収集する場合には、エージェント設定の［通信設定］－［通信エラーの設定］－［通信エラーと見なすタイミング］－［指定した時間内に通信ソフトからの応答がない場合、通信エラーと見なす］の設定を 120 分に変更します。設定を大きくすると、通信障害・サーバ障害など一時障害によりサーバからの応答がない場合にエラーと判断されるまでに時間がかかるため、次のポーリングまでの時間が長くなります。設定変更後、［基本設定］－［上位システムとの通信のタイミング］－［ポーリングの方法］－［システム起動するたびに、定期的にポーリングする］に設定されている時間以上待ってください。
- リモートインストールマネージャを使用して 50MB 以上のパッケージを配布する場合、通信のタイムアウトが発生する場合があるため、分割配布で 50MB 以内にパッケージサイズを分割して配布してください。
- ITDM 互換配布の実行中に通信エラーにより失敗した場合、次のポーリングのタイミングでリトライします。

管理対象のコンピュータが社内ネットワークに接続されている場合

- 社内ネットワークに接続された管理対象のコンピュータが電源 OFF の状態で、管理用サーバから Wake on LAN または AMT で自動起動させる設定で要求を通知すると、システム起動時のポーリングによって要求を受信します。このため、電源 ON の状態の時よりも低遅延で要求が実行されることがあります。

管理対象のコンピュータが社外ネットワークに接続されている場合

- セキュリティポリシーの判定結果に応じたネットワーク接続の遮断と許可が実行される場合、ネットワーク制御リストは更新されますが、社外ネットワークで利用しているコンピュータのネットワーク接続は制御されません。
- 社外ネットワークで利用しているコンピュータは、Wake on LAN または AMT で起動できません。

管理対象のコンピュータの接続ネットワークを切り替える場合

社内ネットワーク環境のコンピュータへのリモートインストールマネージャを使った配布のジョブが完了する前に、コンピュータをインターネット環境に持ち出した場合、ジョブは中断されます。社内ネットワーク環境への接続時に再開されます。

また、インターネット環境のコンピュータへのリモートインストールマネージャを使った配布のジョブが完了する前に、コンピュータを社内ネットワーク環境に持ち帰った場合もジョブは中断されます。インターネット環境への接続時に再開されます。

3 製品ライセンスについて

ここでは、JP1/IT Desktop Management 2 の製品ライセンスについて説明します。

3.1 製品ライセンスの概要

JP1/IT Desktop Management 2 では、「管理ノード数ライセンス」という方式でライセンスの使用数を管理しています。この方式では、機器を管理対象にすると、機器の種類に関係なく 1 台につきライセンスを 1 つ使用します。つまり、JP1/IT Desktop Management 2 に登録されているライセンス数分だけ、機器を管理できます。なお、ライセンスを使うのは、機器の管理だけです。資産の登録にはライセンスは使用しません。

ライセンスは、JP1/IT Desktop Management 2 を購入した際に提供される製品版のライセンスキーファイルを利用して登録します。登録しているライセンス数の上限に達した場合、機器を追加登録できません。そのため、あらかじめ十分な数のライセンスを用意してください。

登録しているライセンス数よりも管理したい機器の台数が多くなった場合は、ライセンスを追加する必要があります。製品ライセンスを追加する場合は、ライセンスを購入して、登録してください。

なお、探索時の自動登録によって機器を管理対象にする場合、ライセンス数が不足していたときは、「発見した機器」として扱われます。発見された機器は設定画面の［機器の探索］－［発見した機器］画面に表示されますが、管理対象ではありません（ライセンスも使用しません）。また、管理対象に変更できないため、機器情報の取得やセキュリティ判定などの操作はできません。管理対象の機器を除外対象に変更したり、削除したりした場合は、ライセンス使用数が減ります。

ヒント

OS マルチブートの環境では、管理用サーバに通知される情報が OS ごとに異なるため、各 OS が別々の機器として扱われます。

ヒント

JP1/IT Desktop Management 2 ライセンス数は、登録したライセンスの総数（Windows、Linux、UNIX 用エージェントのライセンスを登録した場合はその合計）が、［システムサマリ］パネルの［ライセンス情報］に表示されます。［ライセンス情報］に表示されている数値をクリックすると、ライセンス保有数の総数と内訳（Linux 用と UNIX 用）が表示されます。なお、総数に占める UNIX および Linux 分を差し引いたライセンス数には Windows 分と Mac OS 分が含まれます（例えば、総数が 150 で UNIX および Linux 分が 50 の場合、100 には Windows 分と Mac OS 分を含みます）。

ヒント

Citrix XenApp、Microsoft RDS サーバを管理する場合、サーバを管理するライセンスに加えて、Citrix XenApp、Microsoft RDS を利用するユーザーアカウント数分のライセンスが必要です。なお、Citrix XenApp、Microsoft RDS サーバの管理者が利用するアカウントは、Citrix XenApp、Microsoft RDS を利用するユーザーアカウント数としてカウントする必要はありません。

ヒント

共有型 VDI の仮想コンピュータを管理する場合、次のライセンス数が必要です。

VMware Horizon View および Citrix Virtual Desktops の MCS（Machine Creation Services）方式の場合

仮想コンピュータ数分のライセンス

Citrix Virtual Desktops の PVS（Provisioning Services）方式の場合

仮想コンピュータを利用するユーザーアカウント数分のライセンス

3.2　機器の状態と製品ライセンスの関係

発見した機器を管理対象にしたり、管理対象の機器を除外対象にしたりすると、使用する製品ライセンス数が変化します。機器の状態と使用する製品ライセンスの関係を次の表に示します。

機器の状態	ライセンスの使用	説明
発見	×	ネットワークの探索やネットワークモニタによって機器が発見された状態です。
管理対象	○	管理の対象にした状態です。機器を機器管理、セキュリティ管理および資産管理の対象として管理できます。管理用サーバからの操作や、レポート表示の対象となります。
除外対象	×	管理の対象から除外した状態です。管理が不要な機器は除外対象にします。

（凡例）○：使用する　×：使用しない

機器を JP1/IT Desktop Management 2 の管理対象にするには、機器を「管理対象」にします。機器の状態を「管理対象」にすると製品ライセンスが使われます。機器の状態が「発見」または「除外対象」の場合、製品ライセンスは使われません。「管理対象」の機器を「除外対象」にすると、使用していた製品ライセンスを別の機器に使えるようになります。

3.3　複数サーバ構成での製品ライセンスの管理

複数サーバ構成では、統括管理用サーバですべての製品ライセンスを管理します。なお、管理用中継サーバを管理するための製品ライセンスは不要です。

何らかの理由で、各管理用サーバでライセンスの保有数や残数などを管理したい場合は、統括管理用サーバから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。管理用中継サーバへの製品ライセンスの情報の設定について、詳細を以下に示します。

ライセンスの保有方法について

管理用中継サーバに製品ライセンスの情報を設定する際、ライセンスの保有方法を指定できます。保有方法を指定された管理用中継サーバは、統括管理用サーバと同様に製品ライセンスを管理できるようになります。統括管理用サーバと保有方法を指定された管理用中継サーバを合わせて、「ライセンスを保有する管理用サーバ」と呼びます。

管理用中継サーバに指定できるライセンスの保有方法は、次のどちらか一方だけです。

統括管理用サーバからの分配

この保有方法を指定された管理用中継サーバには、統括管理用サーバに登録されている製品ライセンスの一部が分配されます。後述の共有範囲ごとに管理できる機器の台数を制限したい場合に指定します。

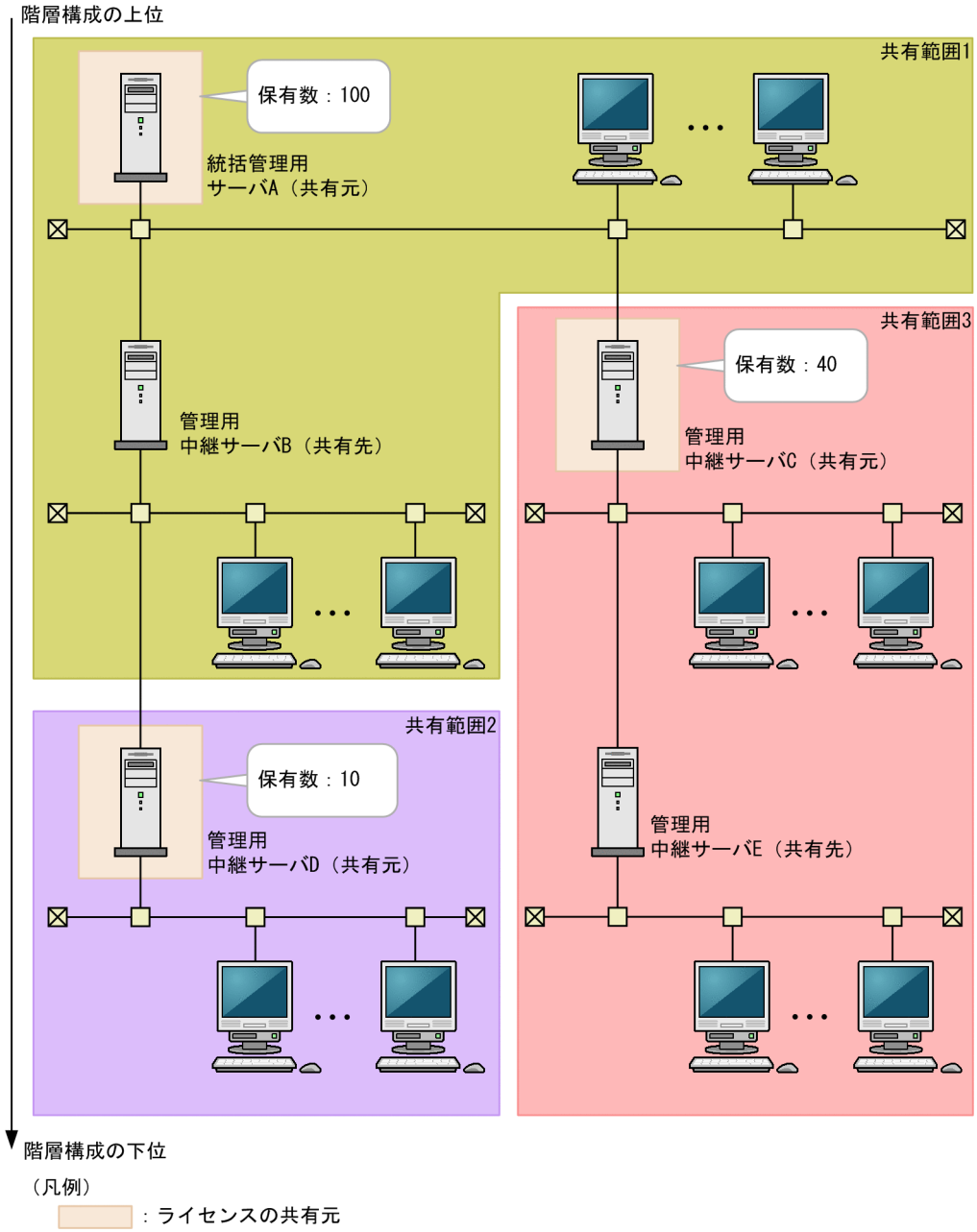
ライセンス登録

この保有方法を指定された管理用中継サーバには、製品ライセンスの登録が許可されます。製品ライセンスを管理用中継サーバごとに購入および登録した上で管理したい場合に指定します。

> **ヒント**
>
> 複数サーバ構成では、統括管理用サーバおよび統括管理用サーバから許可された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。

ライセンスの共有範囲について

管理用中継サーバに製品ライセンスの情報を設定すると、ライセンスの共有範囲が自動で構成されます。ライセンスの共有範囲の構成例を次の図に示します。



ライセンスの共有範囲は、共有元（ライセンスを保有する管理用サーバ）と共有先（ライセンスを保有しない管理用中継サーバ）で構成されます。共有先は、いちばん階層の近い上位の共有元と共有範囲を構成します。上の図の場合、管理用中継サーバ B はいちばん階層の近い上位の共有元である統括管理用サーバ A と共有範囲 1 を構成します。同様に、管理用中継サーバ E は管理用中継サーバ C と共有範囲 3 を構成します。管理用中継サーバ D は配下の管理用中継サーバが存在しないため、単独で共有範囲 2 を構成します。

共有範囲内では、共有元が保有する製品ライセンス数分の機器を管理対象にできます。上の図の場合、共有範囲 1 ではどちらの管理用サーバが管理元であるかに関係なく、100 台の機器を管理対象にできます。同様に、共有範囲 2 では 10 台、共有範囲 3 では 40 台の機器を管理対象にできます。

共有範囲の情報の確認

統括管理用サーバまたは各共有範囲の共有元で、ライセンスの保有数、使用数、残数などの情報を確認できます。統括管理用サーバでは、すべての共有範囲の情報を確認できます。各共有範囲の共有元では、自サーバが属する共有範囲の情報を確認できます。

共有範囲の情報は、[製品ライセンス情報]ダイアログおよび設定画面の［製品ライセンス］－［製品ライセンスの設定］画面の、[製品ライセンスの情報]に表示されます。

> **ヒント**
>
> 共有範囲内で不足しているライセンス数を確認するために各管理用サーバが発見した機器の合計台数を調べる際は、設定画面の［機器の探索］－［発見した機器］画面の一覧を［管理元］でフィルタリングします。[管理元]に共有範囲内の管理用サーバのホスト名を指定して、フィルタ条件に一致した機器の台数を確認してください。

関連リンク

- 3.3.1　管理用中継サーバへの製品ライセンスの分配
- 3.3.2　管理用中継サーバへの製品ライセンスの登録許可

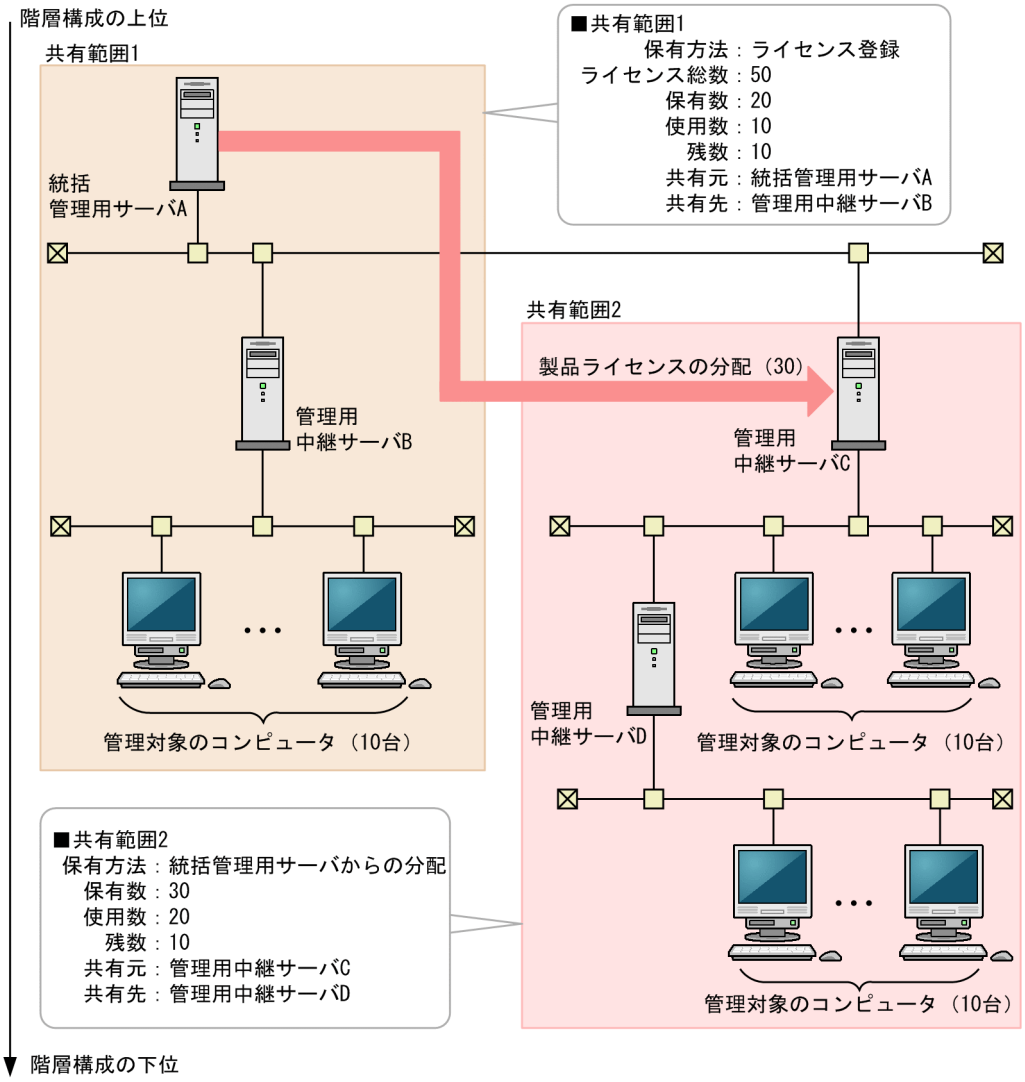
3.3.1　管理用中継サーバへの製品ライセンスの分配

複数サーバ構成の場合、統括管理用サーバに登録されている製品ライセンスの一部を管理用中継サーバに分配できます。共有範囲ごとに管理できる機器の台数を制限したい場合は、管理用中継サーバに製品ライセンスを分配してください。製品ライセンスを分配するには、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。

なお、すでに製品ライセンスが登録されている管理用中継サーバには、製品ライセンスを分配できません。また、管理用中継サーバに登録されている製品ライセンスをほかの管理用中継サーバに分配することもできません。

製品ライセンスを分配すると、ライセンスの共有範囲が自動で構成されます。統括管理用サーバを共有元とする共有範囲のライセンス保有数は、統括管理用サーバのライセンス総数から、各管理用中継サーバに分配したライセンス数を引いた数になります。分配先の管理用中継サーバを共有元とする共有範囲のライセンス保有数は、統括管理用サーバから分配されたライセンス数と同じになります。

製品ライセンスを分配した際の共有範囲の構成例、および各共有範囲の製品ライセンスの情報を次の図に示します。



ヒント

統括管理用サーバの製品ライセンスは、何度でも再分配できます。次のような場合には、各管理用中継サーバに製品ライセンスを再分配してください。

- ライセンスの共有範囲を見直したい場合
- 共有範囲内のライセンス不足に対応するため、統括管理用サーバに製品ライセンスを追加登録した場合

関連リンク

- 3.3　複数サーバ構成での製品ライセンスの管理
- 3.3.2　管理用中継サーバへの製品ライセンスの登録許可

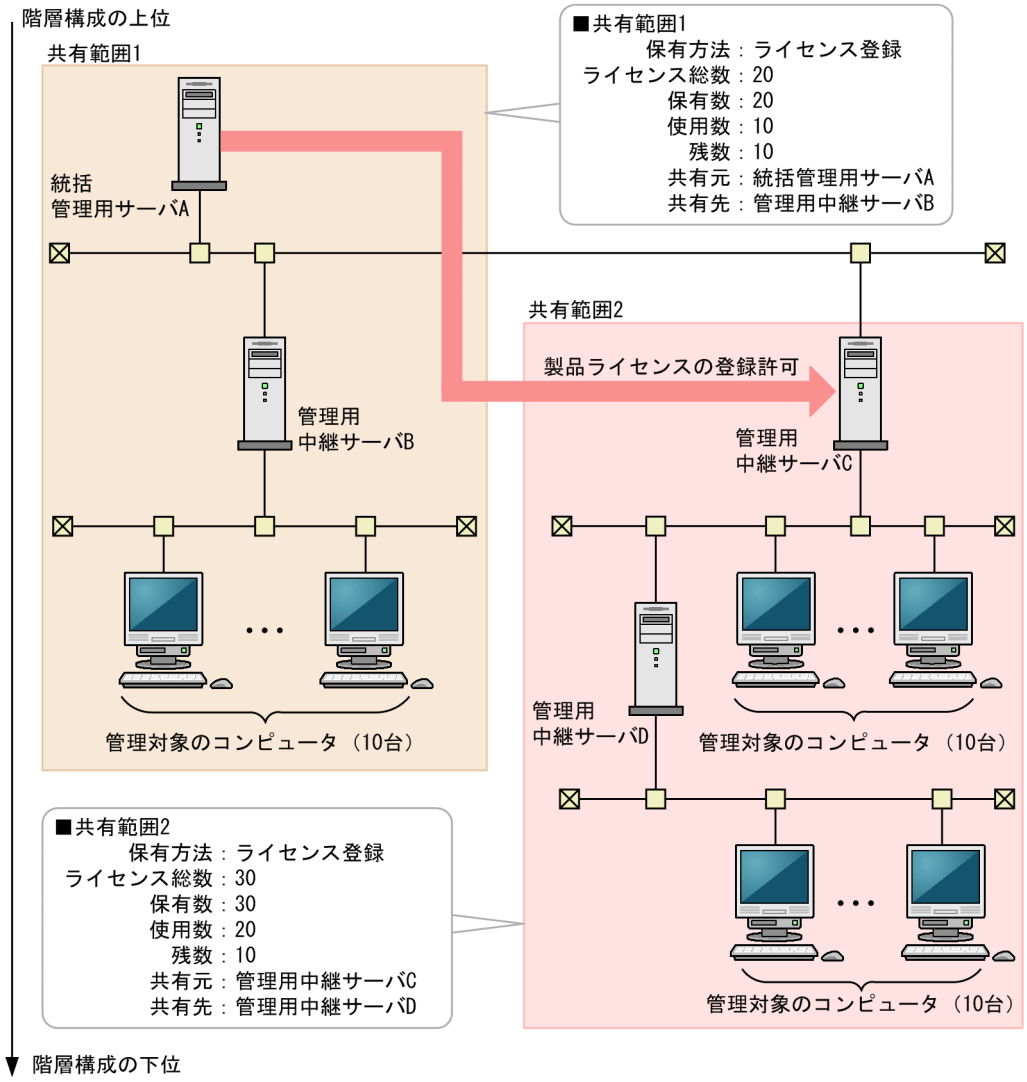
3.3.2　管理用中継サーバへの製品ライセンスの登録許可

複数サーバ構成の場合、統括管理用サーバから許可することで、任意の管理用中継サーバに製品ライセンスを登録できるようになります。製品ライセンスを管理用中継サーバごとに購入および登録した上で管理したい場合は、管理用中継サーバに製品ライセンスの登録を許可してください。管理用中継サーバに製品ライセンスの登録を許可するには、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。

> **重要**
>
> 一度製品ライセンスが登録された管理用中継サーバ、およびその配下の管理用中継サーバには、統括管理用サーバの製品ライセンスを分配できなくなります。そのため、管理用中継サーバに製品ライセンスの登録を許可する場合は、事前にライセンスの共有範囲について十分に検討してください。

製品ライセンスの登録を許可すると、ライセンスの共有範囲が自動で構成されます。統括管理用サーバを共有元とする共有範囲のライセンス保有数は、統括管理用サーバのライセンス総数から、各管理用中継サーバに分配したライセンス数を引いた数になります。製品ライセンスの登録を許可された管理用中継サーバを共有元とする共有範囲のライセンス保有数は、その管理用中継サーバに登録したライセンス総数と同じになります。

製品ライセンスの登録を許可した際の共有範囲の構成例、および各共有範囲の製品ライセンスの情報を次の図に示します。


階層構成の上位
共有範囲1
■共有範囲1
保有方法：ライセンス登録
ライセンス総数：20
保有数：20
使用数：10
残数：10
共有元：統括管理用サーバA
共有先：管理用中継サーバB
統括
管理用サーバA
共有範囲2
製品ライセンスの登録許可
管理用
中継サーバB
管理用
中継サーバC
管理対象のコンピュータ（10台）
管理用
中継サーバD
管理対象のコンピュータ（10台）
■共有範囲2
保有方法：ライセンス登録
ライセンス総数：30
保有数：30
使用数：20
残数：10
共有元：管理用中継サーバC
共有先：管理用中継サーバD
管理対象のコンピュータ（10台）
階層構成の下位

3.4 製品ライセンスに関する注意事項

製品ライセンスは、ライセンスを登録した管理用サーバおよびライセンスを分配された管理用中継サーバだけで利用できます。ほかのコンピュータへの流用はできません。

4 システム設計

JP1/IT Desktop Management 2 のシステム設計では、システム構成、運用方法、システムの見積もりなどについて検討します。

ここでは、JP1/IT Desktop Management 2 の設計から運用を開始するまでの概要について説明します。また、システム設計時に必要な検討事項についても説明します。

なお、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のシステム設計については、マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」のシステム設計の説明を参照してください。また、Asset Console を使用した資産管理をする場合のシステム設計については、マニュアル「JP1/IT Desktop Management 2 - Asset Console 構築・運用ガイド」のシステム設計の説明を参照してください。

4.1　導入と運用の流れ

ここでは、JP1/IT Desktop Management 2 の導入と運用の流れについて説明します。JP1/IT Desktop Management 2 を導入するには、まずシステムの設計を実施します。システム設計でシステム構成や運用方法などを決定したあと、システムを構築し、運用を開始します。JP1/IT Desktop Management 2 の導入と運用の流れを次の図に示します。

システム設計およびシステム構築の流れについては、「4.1.1　導入の流れ」を参照してください。システム運用の流れについては、「4.1.2　運用の流れ」を参照してください。

4.1.1　導入の流れ

JP1/IT Desktop Management 2 を導入するには、システム構成などを設計して、環境を構築します。JP1/IT Desktop Management 2 の導入の流れについて説明します。

1. 組織のルールの検討

   どのようなルールで組織のセキュリティを管理していくかを検討します。ここで検討した内容に基づいて、JP1/IT Desktop Management 2 のシステムを設計、構築および運用します。

2. システムの前提条件の確認

   システム内に配置するサーバやコンピュータの前提条件を確認します。前提条件の確認については、「4.2　システムの前提条件」を参照してください。

3. システム構成の検討

システムの目的に合わせてシステム構成を検討します。システム構成の検討については、「4.4　システム構成の検討」を参照してください。

4. 使用する機能の検討

   運用する環境が、使用する機能の前提条件を満たしているかどうかを確認します。各機能の前提条件については、「4.3　各機能の前提条件」を参照してください。

5. 運用前の検討

   管理対象とする機器や運用のスケジュールなど、システムの運用方法について検討します。運用方法の検討については、「4.6　運用前の検討」を参照してください。

6. データベースの検討

   運用方法に合わせて、使用するデータベースの容量を見積もります。データベースの検討については、「4.5　データベースの検討」を参照してください。

7. システムの見積もり

   流れ 1～6 の内容を踏まえて、構築するシステムの見積もりをします。システムの見積もりについては、「付録 A.6　性能と見積もり」を参照してください。

システム運用の流れについては、「4.1.2　運用の流れ」を参照してください。

4.1.2　運用の流れ

環境構築後、システム設計で検討した運用方法に従って、システムを運用します。JP1/IT Desktop Management 2 のシステム運用の流れについて説明します。

1. 運用のための設定

   運用前に検討した内容に従って、機器の探索スケジュールや探索範囲、セキュリティポリシーなどを設定します。設定には、JP1/IT Desktop Management 2 の操作画面を使用します。

2. 機器情報の収集

   管理用サーバで機器を探索して、最新の IT 機器情報を自動収集します。また、必要に応じてコンピュータにエージェントを導入します。

3. ネットワーク監視および制御

   新しくネットワークに接続されたコンピュータがないか監視します。また、ネットワーク接続を許可していないコンピュータやセキュリティ対策が不十分なコンピュータのネットワーク接続を制御します。

4. セキュリティ状況の判定・診断

   設定したセキュリティポリシーに従っているかどうかを判定し、セキュリティ対策が不十分なコンピュータがないかを確認します。また、JP1/IT Desktop Management 2 では、収集した情報をレポートとして出力できます。出力されたレポートを基にセキュリティの状況を診断します。

5. セキュリティ対策

   診断結果に基づいてセキュリティ対策を実施します。ポリシーを見直す必要がある場合は、流れ 1 に戻ってセキュリティポリシーの設定を変更します。

6. 資産情報の管理

組織内で管理している機器、ソフトウェアライセンス、契約などの資産情報をまとめて管理します。ハードウェア資産やソフトウェアライセンスの利用状況を把握したり、資産の契約情報やコストを確認したりします。

4.2　システムの前提条件

ここでは、システム内に配置する管理用サーバ、エージェントを導入するコンピュータなどのシステム構成要素の前提条件と、ネットワークの前提条件について説明します。

なお、メモリ所要量、ディスク占有量、使用できる CPU については、「付録 A.6　性能と見積もり」もあわせて参照してください。

関連リンク

- 4.2.1　管理用サーバの前提条件
- 4.2.3　エージェントを導入するコンピュータの前提条件
- 4.2.7　ネットワークモニタを有効化するコンピュータの前提条件
- 4.2.5　コントローラをインストールするコンピュータの前提条件
- 4.2.10　ネットワークの前提条件

4.2.1　管理用サーバの前提条件

管理用サーバの前提となる OS およびソフトウェアについて説明します。

なお、JP1/IT Desktop Management 2 - Manager をインストールするサーバのコンピュータ名には、半角英数字およびハイフン（-）だけを使用できます。ただし、コンピュータ名の先頭の文字は半角英字、末尾の文字は半角英数字だけを使用できます。

OS

管理用サーバの前提となる OS を次の表に示します。

OS	詳細
Windows Server 2019 ※	Windows Server 2019 Datacenter
	Windows Server 2019 Standard
Windows Server 2016 ※	Windows Server 2016 Datacenter
	Windows Server 2016 Standard
Windows Server 2012 ※	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard

注※　インストールオプションとして Server Core は使用できません。

ソフトウェア

JP1/IT Desktop Management 2 - Manager をインストールするサーバには、Windows Installer 2.0 以降がインストールされている必要があります。

関連リンク

- 付録 A.6　性能と見積もり

4.2.2　管理者のコンピュータの前提条件

ここでは、操作画面の操作の前提となるソフトウェアと、Remote Install Manager のインストールの前提となる OS およびソフトウェアについて説明します。コントローラとして使用するための前提については、「4.2.5　コントローラをインストールするコンピュータの前提条件」を参照してください。

Remote Install Manager と JP1/IT Desktop Management 2 - Agent（中継システム）は、同じコンピュータにインストールできません。

操作画面の操作の前提となるソフトウェア

JP1/IT Desktop Management 2 の操作画面を操作するコンピュータの前提となるソフトウェアを次の表に示します。

項目	ソフトウェア
Web ブラウザ	次のどれかが必要です。 • Windows Internet Explorer 11 • Firefox ESR 60 以降 • Chrome 78 以降

Remote Install Manager のインストールの前提となる OS

Remote Install Manager をインストールするコンピュータの前提となる OS を次の表に示します。

OS	詳細
Windows Server 2019 ※1	Windows Server 2019 Datacenter
	Windows Server 2019 Standard
Windows Server 2016 ※1	Windows Server 2016 Datacenter
	Windows Server 2016 Standard
Windows 10	Windows 10 Enterprise
	Windows 10 Pro
Windows 8.1	Windows 8.1
	Windows 8.1 Enterprise

OS	詳細
Windows 8.1	Windows 8.1 Pro
Windows 8	Windows 8
	Windows 8 Enterprise
	Windows 8 Pro
Windows Server 2012 ※1	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard
Windows 7※2	Windows 7 Enterprise※3
	Windows 7 Professional※3
	Windows 7 Ultimate※3

注※1

インストールオプションとして Server Core は使用できません。

注※2

XP モードには対応していません。

注※3

Service Pack 1 を含みます。

また、Remote Install Manager を管理用サーバとは別のコンピュータにインストールする場合、Remote Install Manager のバージョンが、管理用サーバの JP1/IT Desktop Management 2 - Manager と一致している必要があります。

Remote Install Manager のインストールの前提となるソフトウェア

Windows Installer 2.0 以降

なお、Remote Install Manager をインストールするサーバのコンピュータ名には、半角英数字およびハイフン（-）だけを使用できます。ただし、コンピュータ名の先頭の文字は半角英字、末尾の文字は半角英数字だけを使用できます。

関連リンク

- 付録 A.6　性能と見積もり

4.2.3　エージェントを導入するコンピュータの前提条件

エージェントを導入するコンピュータの前提となる OS およびソフトウェアについて説明します。

なお、管理用中継サーバにはエージェントをインストールできません。管理用中継サーバには、管理用中継サーバ用のエージェントが自動でインストールされます。

OS

エージェントを導入するコンピュータの前提となる OS を次の表に示します。

OS	詳細
Windows Server 2019※3	Windows Server 2019 Datacenter
	Windows Server 2019 Standard
Windows Server 2016※3	Windows Server 2016 Datacenter
	Windows Server 2016 Standard
Windows 10	Windows 10 Enterprise
	Windows 10 Pro
Windows 8.1	Windows 8.1
	Windows 8.1 Enterprise
	Windows 8.1 Pro
Windows 8※1、※2	Windows 8
	Windows 8 Enterprise
	Windows 8 Pro
Windows Server 2012※3	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard
Windows 7※2、※4、※5	Windows 7 Enterprise
	Windows 7 Home Basic※6
	Windows 7 Home Premium
	Windows 7 Professional
	Windows 7 Starter
	Windows 7 Ultimate
Windows Server 2008 R2※3	Windows Server 2008 R2 Datacenter※5
	Windows Server 2008 R2 Enterprise※5
	Windows Server 2008 R2 Standard※5

OS		詳細
Linux※7	CentOS	CentOS 6
		CentOS 7
		CentOS 8.1
	Red Hat Enterprise Linux Server	Red Hat Enterprise Linux(R) 5 (x86)
		Red Hat Enterprise Linux(R) 5 (AMD/Intel 64)
		Red Hat Enterprise Linux(R) 5 Advanced Platform (x86)
		Red Hat Enterprise Linux(R) 5 Advanced Platform (AMD/Intel 64)
		Red Hat Enterprise Linux(R) Server 6 (32-bit x86)
		Red Hat Enterprise Linux(R) Server 6 (64-bit x86_64)
		Red Hat Enterprise Linux(R) Server 7
		Red Hat Enterprise Linux(R) Server 8
	Oracle Linux	Oracle Linux 6
		Oracle Linux 7
		Oracle Linux 8
UNIX※7	AIX※7	AIX V6.1
		AIX V7.1
		AIX V7.2
	Solaris※7	Solaris 10 (SPARC)
		Solaris 11 (SPARC)
	HP-UX※7	HP-UX 11i V3 (IPF)
Mac	Mac OS	OS X 10.10
		OS X 10.11
		macOS 10.12
		macOS 10.13
		macOS 10.14

注※1　Windows To Go で動作する場合は対応していません。

注※2　エージェントをインストールする際は、ローカルコンソールに接続して実施してください。

注※3　インストールオプションとして Server Core は使用できません。

注※4　XP モードには対応していません。

注※5　Service Pack 1 を含みます。

注※6　中国語（簡体字）だけサポートします。

注※7　総称して UNIX と表記することがあります。なお、前提プログラムなど、エージェントを導入する条件については、マニュアル「JP1/IT Desktop Management 2 - Agent(UNIX(R)用)」を参照してください。

重要

OS の「Workstation」サービスは必ず起動してください。このサービスが停止している環境では OS のアカウント情報を取得できないため、セキュリティーポリシーで判定される危険レベルが「不明」となります。

重要

Windows の言語設定について

- 各言語（日本語/英語/中国語（簡体字））のどれかで利用する場合、言語設定が統一されていることを確認してからインストールしてください。
- インストール後に上記の言語設定は変更しないでください。

画面の表示言語について

JP1/IT Desktop Management 2 では、画面表示にはネイティブ画面（インストーラ、エージェント画面、コマンド）があります。ネイティブ画面の表示言語は、各ネイティブ画面を表示する Windows の言語設定が引き継がれます。

ソフトウェア

エージェントを導入するコンピュータの前提となるソフトウェアを次の表に示します。

項目	ソフトウェア
Web ブラウザ	次のどれかが必要です。 • Windows Internet Explorer 9 • Windows Internet Explorer 10 • Windows Internet Explorer 11

Citrix XenApp、Microsoft RDS サーバ

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 で管理する場合に前提になる OS とサポート対象となる Citrix XenApp を次に示します。

OS

OS	詳細
Windows Server 2019	Windows Server 2019 Datacenter
	Windows Server 2019 Standard
Windows Server 2016	Windows Server 2016 Datacenter
	Windows Server 2016 Standard
Windows Server 2012	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard
Windows Server 2008 R2※	Windows Server 2008 R2 Datacenter
	Windows Server 2008 R2 Enterprise
	Windows Server 2008 R2 Standard

注※　Service Pack 1 だけサポートしています。

Citrix XenApp

製品名	バージョン
Citrix XenApp※1、※2、※3	7.5、7.6、7.7、7.8、7.9、7.11、7.12、7.13、7.14

※1　Long Term Service Release には対応していません。

※2　公開デスクトップおよび公開アプリケーションの画面転送型にだけ対応しています。

※3　Machine Creation Services および Provisioning services には対応していません。

Citrix XenApp、Microsoft RDS に同時にログインできるユーザー数のサポート上限は、60 ユーザーです。

共有型 VDI の仮想コンピュータ

共有型 VDI の仮想コンピュータにエージェントを導入して、JP1/IT Desktop Management 2 で管理する場合にサポート対象となる仮想化製品を次に示します。

仮想化製品

製品名	バージョン
VMware Horizon View	7.0、7.1、7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9
Citrix Virtual Desktops	1906

関連リンク

- 付録 A.6　性能と見積もり

4.2.4　中継システムをインストールするコンピュータの前提条件

中継システムをインストールするコンピュータの前提について説明します。

JP1/IT Desktop Management 2 - Agent（中継システム）と Remote Install Manager は、同じコンピュータにインストールできません。

OS

中継システムをインストールするコンピュータの前提となる OS を次の表に示します。

OS	詳細
Windows Server 2019※1、※2	Windows Server 2019 Datacenter
	Windows Server 2019 Standard
Windows Server 2016※1、※2	Windows Server 2016 Datacenter
	Windows Server 2016 Standard
Windows 10	Windows 10 Enterprise
	Windows 10 Pro
Windows 8.1※1	Windows 8.1
	Windows 8.1 Enterprise
	Windows 8.1 Pro
Windows 8※3	Windows 8
	Windows 8 Enterprise
	Windows 8 Pro
Windows Server 2012※2	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter※1
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard※1
Windows 7※4※5	Windows 7 Enterprise
	Windows 7 Professional
	Windows 7 Ultimate

注※1　OneDrive を使用した環境での動作には対応していません。

注※2　インストールオプションとして Server Core は使用できません。

注※3　Windows To Go で動作する場合は対応していません。

注※4　XP モードには対応していません。

注※5　Service Pack 1 を含みます。

> **重要**
>
> OS の「Workstation」サービスは必ず起動してください。このサービスが停止している環境では OS のアカウント情報を取得できないため、セキュリティーポリシーで判定される危険レベルが「不明」となります。

ソフトウェア

中継システムをインストールするコンピュータの前提となるソフトウェアを次の表に示します。

項目	ソフトウェア
Web ブラウザ	次のどれかが必要です。 • Windows Internet Explorer 9 • Windows Internet Explorer 10 • Windows Internet Explorer 11

関連リンク

- 付録 A.6　性能と見積もり

4.2.5　コントローラをインストールするコンピュータの前提条件

コントローラをインストールするコンピュータの前提となる OS を次の表に示します。

OS	詳細
Windows Server 2019※1、※2	Windows Server 2019 Datacenter
	Windows Server 2019 Standard
Windows Server 2016※1、※2	Windows Server 2016 Datacenter
	Windows Server 2016 Standard
Windows 10	Windows 10 Enterprise
	Windows 10 Pro
Windows 8.1※1	Windows 8.1
	Windows 8.1 Enterprise

OS	詳細
Windows 8.1※1	Windows 8.1 Pro
Windows 8※3	Windows 8
	Windows 8 Enterprise
	Windows 8 Pro
Windows Server 2012※2	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter※1
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard※1
Windows 7※4	Windows 7 Enterprise※5
	Windows 7 Home Premium※5
	Windows 7 Professional※5
	Windows 7 Starter※5
	Windows 7 Ultimate※5
Windows Server 2008※2	Windows Server 2008 R2 Datacenter※5
	Windows Server 2008 R2 Enterprise※5
	Windows Server 2008 R2 Standard※5

注※1　OneDrive を使用した環境での動作には対応していません。

注※2　インストールオプションとして Server Core は使用できません。

注※3　Windows To Go で動作する場合は対応していません。

注※4　XP モードには対応していません。

注※5　Service Pack 1 を含みます。

関連リンク

- 付録 A.6　性能と見積もり

4.2.6　インターネットゲートウェイをインストールするコンピュータの前提条件

インターネットゲートウェイをインストールするコンピュータの前提について説明します。

インターネットゲートウェイには、JP1/IT Desktop Management 2 - Agent（中継システム）または JP1/IT Desktop Management 2 - Agent が必要です。

OS

インターネットゲートウェイをインストールするコンピュータの前提となる OS を次の表に示します。

OS	詳細
Windows Server 2019※1、※2	Windows Server 2019 Datacenter
	Windows Server 2019 Standard
Windows Server 2016※1、※2	Windows Server 2016 Datacenter
	Windows Server 2016 Standard
Windows Server 2012※2	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter※1
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard※1

注※1　OneDrive を使用した環境での動作には対応していません。

注※2　インストールオプションとして Server Core は使用できません。

ソフトウェア

インターネットゲートウェイをインストールするコンピュータの前提となるソフトウェアを次の表に示します。

項目	ソフトウェア
Web サーバ	次のどれかが必要です。 • Microsoft Internet Information Services 8.0 • Microsoft Internet Information Services 8.5 • Microsoft Internet Information Services 10.0

関連リンク

- 付録 A.6　性能と見積もり

4.2.7　ネットワークモニタを有効化するコンピュータの前提条件

ネットワークモニタを有効化するコンピュータの前提となる OS を次の表に示します。

OS

OS	詳細
Windows Server 2019※1、※2	Windows Server 2019 Datacenter
	Windows Server 2019 Standard
Windows Server 2016※1、※2	Windows Server 2016 Datacenter
	Windows Server 2016 Standard
Windows 10	Windows 10 Enterprise
	Windows 10 Pro
Windows 8.1※1	Windows 8.1 Enterprise
	Windows 8.1 Pro
Windows 8	Windows 8 Enterprise
	Windows 8 Pro
Windows Server 2012※2	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter※1
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard※1
Windows 7※3	Windows 7 Enterprise※4
	Windows 7 Professional※4
	Windows 7 Ultimate※4

注※1　OneDrive を使用した環境での動作には対応していません。

注※2　インストールオプションとして Server Core は使用できません。

注※3　XP モードには対応していません。

注※4　Service Pack 1 を含みます。

ソフトウェア

オンライン管理用のエージェントまたは中継システムを導入する必要があります。

ネットワーク環境

- IP アドレスが固定されている
- 同じネットワークセグメント内の IP アドレスを複数所持していない

関連リンク

- 4.2.3　エージェントを導入するコンピュータの前提条件
- 付録 A.6　性能と見積もり

4.2.8　エージェントレスで管理するための前提条件

エージェントレスでコンピュータを管理して機器情報を取得する場合、管理用サーバと利用者のコンピュータで設定が必要です。認証状態によって取得できる機器情報が異なります。取得できる情報が少ないと、セキュリティ状況の一部が判定できなかったり、レポート上で集計されなかったりして、正しく運用できなくなるおそれがあります。運用の目的に応じて、適切な認証方法を選択してください。

なお、Active Directory を利用してコンピュータを管理していると、大部分の機器情報を取得するための設定が容易になります。エージェントレス運用を考えている場合は、まず組織内のコンピュータが Active Directory で管理されているかどうかを確認することをお勧めします。

取得できる機器情報の差異については、「2.6.2　機器情報の収集」を参照してください。

> **重要**
>
> NAT 環境では、エージェントレスの機器は管理できません。

> **重要**
>
> ネットワークの探索で発見した機器をエージェントレスで管理している場合、その機器に対する探索範囲および認証情報を削除しないでください。また、Active Directory の探索で発見した機器をエージェントレスで管理している場合は、その機器が登録されている Active Directory の設定を削除しないでください。削除すると、機器情報が取得されなくなります。削除してしまった場合は、探索範囲、認証情報、または Active Directory の設定を追加したあとにネットワークの探索または Active Directory の探索を再実行して、機器を発見してください。

> **重要**
>
> DHCP 環境の場合、機器の IP アドレスが変更され探索範囲外になると、機器情報が取得されなくなります。

Windows の管理共有を利用してエージェントレス管理する場合

次の条件をすべて満たしている必要があります。

- 利用者のコンピュータで、Windows ファイアウォールが無効になっている。※1
- 利用者のコンピュータで、簡易ファイル共有が無効になっている。

- 利用者のコンピュータで、Windows の管理共有（ADMIN$）が有効になっている。
- 利用者のコンピュータで、プロセス間通信用共有（IPC$）が有効になっている。
- 管理用サーバで、Windows の管理共有を使用して対象のコンピュータにログオンするための情報が、ネットワークの探索の認証情報として設定されている。※2

注※1　有効の場合でも、TCP（ポート番号：445）を許可しておけば条件が満たされます。

注※2　Windows の管理共有を使用して対象のコンピュータにログオンするための認証情報は、次の条件のどちらかを満たしている必要があります。

- 利用者のコンピュータのビルトイン Administrator アカウントとパスワードを使用する。
- 利用者のコンピュータの UAC 機能が無効になっている。

管理用サーバから Windows の管理共有にアクセスできるようにする設定は、利用者のコンピュータの OS によって異なります。Windows の管理共有にアクセスするためには、次の表に示す設定が必要です。

OS	設定内容
Windows 10	• UAC の無効化、または Administrator ユーザーの有効化※1 • ネットワークと共有センターの［ファイルとプリンタの共有］の有効化
Windows 8.1	
Windows 8	
Windows 7	
Windows Vista	• UAC の無効化、または Administrator ユーザーの有効化 • ネットワークと共有センターの［ファイル共有］の有効化
Windows XP※2	• 簡易ファイル共有の無効化 • ファイル共有の追加
Windows Server 2019	ネットワークと共有センターの、［ファイル共有］または［ファイルとプリンタの共有］の有効化
Windows Server 2016	
Windows Server 2012	
Windows Server 2008	
Windows Server 2003	設定不要（デフォルトで有効）
Windows 2000	ファイル共有の追加
Windows 以外のコンピュータ	対象外（設定できない）
ネットワーク装置	対象外（設定できない）

注※1　エディションがない Windows 8.1 および Windows 8 の場合は、コマンドプロンプトで net user コマンドを実行して有効化してください。Windows のコントロールパネルからは Administrator ユーザーを有効にできません。

注※2　Windows XP Home Edition(Service Pack 2、3)の場合は、管理共有が使用できません。

これらの条件を満たしている場合、大部分の機器情報を取得できます。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と、取得できる情報に大きな差異はありません。

SNMP を利用してエージェントレス管理する場合

次の条件を満たしている必要があります。

- SNMP を利用できる。
- コミュニティ名を認証できる。

なお、SNMP を使用して機器情報を取得するためには次の表に示す設定が必要です。

OS	設定内容
Windows 10	• SNMP エージェントの導入 • SNMP エージェントの設定
Windows 8.1	
Windows 8	
Windows 7	
Windows Vista	
Windows XP	
Windows Server 2019	
Windows Server 2016	
Windows Server 2012	
Windows Server 2008	
Windows Server 2003	
Windows 2000	
Windows 以外のコンピュータ	
ネットワーク装置	

Active Directory を利用してエージェントレス管理する場合

次の条件をどちらも満たしている必要があります。

- 利用者のコンピュータで、Windows ファイアウォールが無効になっている。※
- Active Directory 連携機能を使用して、管理用サーバで Active Directory が管理する機器情報を収集できる。

注※　有効の場合でも、設定画面の［他システムとの接続］－［Active Directory の設定］画面で指定したポート番号での接続を許可しておけば、条件が満たされます。

ICMP を利用してエージェントレス管理する場合

ICMP を利用できる必要があります。

なお、ICMP を使用して機器情報を取得するためには、次の表に示す設定が必要です。

OS	設定内容
Windows 10	ICMP エコー要求の着信許可※
Windows 8.1	
Windows 8	
Windows 7	
Windows Vista	
Windows XP	
Windows Server 2019	
Windows Server 2016	
Windows Server 2012	
Windows Server 2008	
Windows Server 2003	
Windows 2000	
Windows 以外のコンピュータ	
ネットワーク装置	

注※　Windows XP 以降では、Windows ファイアウォールで ICMP を許可する設定をするか、Windows ファイアウォールを解除する必要があります。

関連リンク

- (1)　収集できる機器情報の種類
- (2)　機器の状態として収集できる情報
- (3)　システム情報として収集できる情報
- (4)　ハードウェア情報
- (5)　インストールソフトウェア情報
- (6)　セキュリティ情報
- (7)　資産情報と機器情報の共通管理項目

4.2.9　JP1/IM と連携するための前提条件

JP1/IM と連携する場合に必要なソフトウェアを次に示します。

- JP1/IM 10-00 以降または Job Management Partner 1/IM 10-00 以降
- JP1/Base 10-00 以降または Job Management Partner 1/Base 10-01 以降

前提 OS は、JP1/Base の前提 OS に準じます。

4.2.10　ネットワークの前提条件

JP1/IT Desktop Management 2 を導入するネットワーク環境の前提条件を次に示します。

重要

NAT、WAN、または VPN をまたがって通信する場合は、環境によって通信できるかどうかが異なります。そのため、事前に通信できるかを検証してください。

重要

NAT 環境の場合は、コンピュータにエージェントをインストールして管理できますが、エージェントに対する任意のタイミングでの操作（メッセージの通知、最新の機器情報取得など）はできません。これらの操作をした場合、エージェントからのポーリングが発生したタイミングで実行されます。

全体のネットワーク

管理用サーバのグローバル IP アドレスには、固定 IP アドレスを利用してください。

また、JP1/IT Desktop Management 2 および JP1/IT Desktop Management 2 - Agent 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。ポート番号については、「付録 A.3　ポート番号一覧」を参照してください。

ネットワークの接続環境

各システム構成要素のネットワークの接続環境について説明します。

管理用サーバの場合

有線 LAN でネットワークに接続する必要があります。

ネットワークモニタを有効化するコンピュータの場合

有線 LAN または無線 LAN でネットワークに接続する必要があります。ただし、通信環境が劣化している場合、無線 LAN でネットワークに接続している機器のネットワーク接続を遮断できないことがあります。そのため、有線 LAN でネットワークに接続することをお勧めします。

エージェント導入済みのコンピュータの場合

有線 LAN、無線 LAN、WAN、または VPN でネットワークに接続する必要があります。ただし、無線 LAN でネットワークに接続している機器は、電源制御の機能を使用しても電源を ON にできません。電源制御については、「2.6.3　機器の制御」を参照してください。

エージェントレスのコンピュータの場合

有線 LAN、無線 LAN、WAN、または VPN でネットワークに接続する必要があります。

管理用サーバと管理対象のコンピュータ間のネットワーク

管理対象のコンピュータから管理用サーバに対して、ICMP で通信できる必要があります。

管理用サーバから管理対象のコンピュータに対して ICMP で通信できない場合、管理用サーバから管理対象のコンピュータに対する操作（ソフトウェアのインストール、メッセージの通知、最新の機器情報取得など）は、エージェントからのポーリングが発生したタイミングで実行されます。

ヒント

DHCP 環境の場合、コンピュータに動的に IP アドレスが割り振られても、JP1/IT Desktop Management 2 に重複して登録されることはありません。

管理用サーバと操作画面を操作するコンピュータ間のネットワーク

管理用サーバとは別に JP1/IT Desktop Management 2 の操作画面を操作するコンピュータを使用する場合は、Web ブラウザを使用して HTTP 通信できる環境が必要です。

Windows ファイアウォールが設定されているネットワーク

各システム構成要素で必要な設定について説明します。

管理用サーバの場合

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 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）。

ただし、Windows ファイアウォールが無効になっている環境にインストールした場合、インストール後に Windows ファイアウォールを有効にしても通過設定はされません。この場合、管理用サーバで `addfwlist.bat` コマンドを実行してください。Windows ファイアウォールを通過できるように設定されます。コマンドの実行ファイルは、次のフォルダに格納されています。

JP1/IT Desktop Management 2 - Manager のインストール先フォルダ¥mgr¥bin¥

コントローラをインストールしたコンピュータの場合

Windows ファイアウォールの有効無効に関係なく、コントローラのインストール時に自動的に通過設定がされます（例外設定に登録されます）。設定は不要です。

エージェント導入済みのコンピュータの場合

Windows ファイアウォールの有効無効に関係なく、エージェントのインストール時に自動的に通過設定がされます（例外設定に登録されます）。設定は不要です。

エージェントレスのコンピュータの場合

Windows ファイアウォールの例外設定で、TCP（ポート番号：445）の通信を許可してください。

関連リンク

- 4.2.8　エージェントレスで管理するための前提条件

4.3　各機能の前提条件

関連リンク

- 4.3.1　機器管理の前提条件
- 4.3.2　ネットワークモニタの前提条件
- 4.3.3　リモートコントロールの前提条件
- 4.3.4　セキュリティ管理の前提条件
- 4.3.5　操作ログ取得の前提条件
- 4.3.6　資産管理の前提条件
- 4.3.7　配布機能の前提条件
- 4.3.8　レポートの前提条件

4.3.1　機器管理の前提条件

機器管理をするには、管理の対象となる機器がネットワークに接続されている必要があります。また、JP1/IT Desktop Management 2 の操作画面に表示させるためには、機器を管理対象にする必要があります。機器を管理対象にするには、次の 3 種類の方法があります。

- コンピュータにエージェントを導入する（自動的に管理対象になる）
- 機器の探索によって発見された機器を管理対象にする
- ネットワークモニタ機能によって発見された機器を管理対象にする

IPv4 形式と IPv6 形式の両方の IP アドレスを使用している機器は、IPv4 形式の IP アドレスだけを利用して管理対象にできます。

なお、IPv6 形式の IP アドレスだけを持つ機器は、Active Directory に登録されている機器を探索する方法でだけ管理対象にできます。ただし、この場合、機器の存在だけを管理できます。

関連リンク

- 4.2.3　エージェントを導入するコンピュータの前提条件

4.3.2　ネットワークモニタの前提条件

ネットワークモニタ機能を導入するには、ネットワークを監視するためのコンピュータが必要です。ネットワークモニタ機能を導入するネットワークセグメントごとに、オンライン管理のコンピュータを 1 台準備して、そのコンピュータのネットワークモニタを有効にしてください。

また、ネットワークを監視するためのコンピュータに割り当てているエージェント設定の［基本設定］で、次の項目のチェックを外さないでください。

- ［上位システムと通信する］
- ［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］

ネットワークモニタ機能は、エージェントが稼働している間だけ有効です。このため、ネットワークを監視したい時間は、ネットワークモニタを有効にしたコンピュータが稼働している必要があります。

ヒント

常にネットワークを監視するために、24 時間稼働しているコンピュータのネットワークモニタを有効にすることをお勧めします。

重要

ネットワークを監視するためのコンピュータ（ネットワークモニタを有効にしたオンライン管理のコンピュータ）は、セキュリティ対策が不十分などの理由でネットワーク接続が遮断された機器からも接続できるようになっています。このため、ファイルサーバなど業務上重要なサーバは、ネットワークを監視するためのコンピュータに設定しないでください。

重要

UNIX エージェント、Mac エージェント、および Citrix XenApp、Microsoft RDS サーバはネットワークモニタを有効化できません。なお、ネットワーク接続の制御は手動での操作となります。

4.3.3 リモートコントロールの前提条件

コンピュータをリモートコントロールするための前提条件について説明します。

管理者のコンピュータの前提条件

管理者のコンピュータには、コントローラがインストールされている必要があります。コントローラとは、リモートコントロールする側のプログラムです。リモートコントロールの対象となるコンピュータの画面を呼び出して操作できます。

コントローラは、操作画面からリモートコントロールを実行すると、操作画面を表示しているコンピュータに自動的にインストールされます。

接続先のコンピュータの前提条件

接続先のコンピュータは、コントローラの接続方法によって必要な条件が異なります。

標準接続

エージェントが導入済みで、リモコンエージェントが起動している必要があります。リモコンエージェントとは、リモートコントロールされる側のプログラムです。コントローラに自身のコンピュータの画面を提供し、コントローラから指示された操作を画面上で実行します。

リモコンエージェントは、エージェントのプログラムの一部です。エージェントのインストール時に、[インストールするコンポーネント] ダイアログでリモコンエージェントを選択すると、導入されます。リモコンエージェントとコントローラが標準接続することで、すべてのリモートコントロール機能が使用できるようになります。

リモコンエージェントを使用できるバージョンは、JP1/IT Desktop Management 09-50 以降または JP1/IT Desktop Management 2 10-50 以降です。

RFB で接続

RFB で接続すると、リモコンエージェントを使用しないで（エージェントレスで）リモートコントロール機能を使用できます。ただし、RFB で接続するとリモートコントロール機能の一部が制限されます。

RFB で接続するには、次の条件のうちどれかを満たす必要があります。

- VNC サーバ機能を持つソフトウェア（例えば、次のソフトウェア）が実行されている

  ・Intel vPro（AMT 6.0 以降を搭載したコンピュータで、KVM Remote Control が利用できる場合）

  ・RealVNC

  ・UltraVNC

  ・VMware Workstation

- OS が Mac OS X で、画面共有またはリモートマネージメントが有効になっている

重要

リモートコントロールエージェントと、リモートコントロール機能を持つ次の製品を 1 台の PC に一緒に組み込んで使用できません。次の製品がインストールされていないことを確認してから，リモートコントロールエージェントをインストールしてください。

- JP1/Remote Control Agent
- JP1/NETM/Remote Control Agent
- JP1/NETM/DM Manager に含まれる次のリモートコントロールエージェント
  - JP1/NETM/DM Client - Remote Control Feature
  - JP1/NETM/DM Client に含まれるリモートコントロールエージェント
- JP1/NETM/Remote Control Agent for Blade PC※
- その他のリモートコントロール製品

注※　セキュアクライアントソリューションの構成製品です。

重要

RFB 接続によるリモートコントロールは、被コントロール側がフリーソフトウェアなどで実現されていることもあるため、必ずしも動作を保証できるものではありません。また、一部の機能が使えないこともあります。そのため、体験版を使って事前に動作を確認検証いただくことをお勧めします。 なお、RFB 接続での被コントロール側のハードウェアまたはプログラムの環境構築、仕様、設定方法、および障害などについてのお問い合わせには対応できません。

重要

JP1/NETM/Remote Control、JP1/Remote Control、および JP1/NETM/DM のリモートコントロール機能とは接続できません。

重要

OS が UNIX、Mac のコンピュータには、コントローラをインストールできません。また、UNIX エージェント、Mac エージェントにはリモートコントロールされる側に必要なプログラム「リモコンエージェント」が含まれていません。なお、OS が Mac のコンピュータは RFB で接続すると、リモートコントロール機能を使用できます。

重要

Citrix XenApp、Microsoft RDS サーバではリモコンエージェントを使用できません。

関連リンク

- 2.7.2　リモートコントロールの機能
- 2.7.9　NAT 環境、DHCP 環境でのリモートコントロール

4.3.4　セキュリティ管理の前提条件

セキュリティ管理をするには、セキュリティ管理の対象となるコンピュータに、エージェントが導入されている必要があります。オフライン管理のコンピュータの場合は、機器情報の取得が完了している必要があります。

セキュリティ管理の各機能を利用するために必要な前提条件を次に示します。

更新プログラムの適用管理をする場合の前提条件

次の条件をすべて満たす必要があります。

- サポートサービス契約をしている

- MSXML 4.0 Service Pack 2 または MSXML 6.0 がインストールされている

ウィルス対策製品のインストールの有無を判別する場合の前提条件

ウィルス対策製品がインストールされているかどうかを判別する場合の前提条件はありません。

対象のコンピュータに、JP1/IT Desktop Management 2 がサポートするウィルス対策製品がインストールされているかどうかで、ウィルス対策製品のインストールの有無を把握できます。

> **ヒント**
>
> JP1/IT Desktop Management 2 がサポートしていないウィルス対策製品でも、使用必須ソフトウェアとして登録することでインストールの有無を把握できます。

抑止機能を利用する場合の前提条件

機能	前提条件
ソフトウェアの起動抑止	抑止するソフトウェアは、ファイル名とフォルダ名を合わせた文字列の長さが 260 文字未満になっている
印刷の抑止	各プリンタのプロパティで、すべてのログオンユーザーに［印刷］と［ドキュメントの管理］が許可されている※

注※　ネットワーク共有プリンタの場合、以下の前提条件が追加されます。

- サポートするエージェントとプリントサーバの組み合わせを以下に示します。

エージェント	プリントサーバ	印刷抑止
Windows 7 以降	Windows XP/2003	×
Windows 7 以降	Windows Vista 以降	○
任意	上記以外	×

（凡例）○：抑止できる　×：抑止できない

- プリントサーバとエージェント PC 間で RPC による通信ができる必要があります。RPC 通信ができない場合は以下が考えられます。
  - プリントサーバが Internet Printing Protocol（IPP）サーバである
  - プリントサーバとエージェント PC の間にファイアウォール、プロキシまたは NAT がある
  - エージェント PC の Windows ファイアウォールが有効で、かつ［ファイルとプリンターの共有］が［例外］に設定されていない
- エージェント PC で［Microsoft ネットワーク用ファイルとプリンター共有］が有効である必要があります。
- プリントサーバからエージェント PC の名前を解決できる必要があります。

- エージェント PC が Windows 7 以降の場合、エージェント PC とプリントサーバが同一のドメインに参加している、または、エージェント PC の資格認証マネージャにプリントサーバの資格情報が登録されている必要があります。資格情報を追加した場合はエージェント PC を再起動する必要があります。

デバイスの使用抑止の前提条件については、「(1)　使用を抑止できるデバイス」を参照してください。

重要

UNIX エージェント、Mac エージェントはセキュリティ管理の対象ではありません。このため、更新プログラム（OS パッチ）の適用管理、ウィルス対策製品がインストールされているかどうかの判定、抑止機能の利用はできません。

関連リンク

- (14)　サポートするウィルス対策製品

4.3.5　操作ログ取得の前提条件

操作ログを取得するには、操作ログを取得したいコンピュータにエージェントが導入されている必要があります。

操作ログは、種類ごとに取得のための前提条件が異なります。操作ログの種類ごとの前提条件を次の表に示します。

取得する操作ログの種類		前提条件
コンピュータの操作	コンピュータの起動および停止	－
	OS へのログオンおよびログオフ	
プログラムの起動および終了		操作ログを取得するプログラムは、ファイル名とフォルダ名を合わせた文字列の長さが 260 文字未満になっている必要があります。
ファイルおよびフォルダの操作	コンピュータ内のファイルおよびフォルダの操作	－
	Web 上へのアップロードおよびダウンロード	操作ログの取得対象となる Web ブラウザを次に示します。 • Internet Explorer 9、10、11※1 • Web ブラウザに Internet Explorer 10、11 を使用している場合、［インターネットオプション］の［詳細設定］タブの［サードパーティ製のブラウザ拡張を有効にする］がチェックされている必要があります。なお、Windows Server 2012 および Windows Server 2008 R2 にインストールされた Internet Explorer では、デフォルトで［サードパーティ製のブラウザ拡張を有効にする］がチェックされていません。 • Web ブラウザに Internet Explorer 10、11 を使用している場合、［ツール］－［アドオンの管理］を選択すると表示される［ツールバー

取得する操作ログの種類		前提条件
ファイルおよびフォルダの操作	Web 上へのアップロードおよびダウンロード	と拡張機能］で、「JP1/IT Desktop Management 2 FUO」と表示されるアドオンが有効になっている必要があります。
	メールの送受信	操作ログの取得対象となるメーラーを次に示します。 • Microsoft Outlook 2002、2003、2007、2010、2013、2016、2019 • Windows Live メール 2009、2011、2012
	メールに添付されているファイルの保存	
	ファイル送受信	操作ログの取得対象となる Web ブラウザを次に示します。 • Internet Explorer 9、10、11※1
印刷操作		各プリンタのプロパティで、すべてのログオンユーザーに［印刷］と［ドキュメントの管理］が許可されている※2
Web アクセス		• 操作ログの取得対象となる Web ブラウザを次に示します。 • Internet Explorer 9、10、11※1 • ［インターネットオプション］の［詳細設定］タブの［サードパーティ製のブラウザ拡張を有効にする］がチェックされている必要があります。なお、Windows Server 2012 および Windows Server 2008 R2 にインストールされた Internet Explorer では、デフォルトで［サードパーティ製のブラウザ拡張を有効にする］がチェックされていません。 • 利用者のコンピュータに追加される Web アクセス監視用のアドオンが有効になっている必要があります。 • ［ツール］－［アドオンの管理］を選択すると表示される［ツールバーと拡張機能］で、「JP1/IT Desktop Management 2 BHO」と表示されるアドオンが有効になっている必要があります。
デバイスの接続および切断		－
ウィンドウ操作		－

（凡例）－：特になし

注※1　デスクトップ用 Internet Explorer の場合、かつ拡張保護モードを無効にしている場合にだけ、Web アップロード、Web ダウンロード、ファイル受信および Web アクセスの操作ログを取得できます。

注※2　ネットワーク共有プリンタの場合、以下の前提条件が追加されます。

- サポートするエージェントとプリントサーバの組み合わせを以下に示します。

エージェント	プリントサーバ	印刷操作ログの取得
Windows 7 以降	Windows XP/2003	×
Windows 7 以降	Windows Vista 以降	○
任意	上記以外	×

（凡例）○：使用できる　×：使用できない

- プリントサーバとエージェント PC 間で RPC による通信ができる必要があります。RPC 通信ができない場合は以下が考えられます。
  - プリントサーバが Internet Printing Protocol（IPP）サーバである
  - プリントサーバとエージェント PC の間にファイアウォール、プロキシまたは NAT がある
  - エージェント PC の Windows ファイアウォールが有効で、かつ［ファイルとプリンターの共有］が［例外］に設定されていない
- エージェント PC で［Microsoft ネットワーク用ファイルとプリンター共有］が有効である必要があります。
- プリントサーバからエージェント PC の名前を解決できる必要があります。
- エージェント PC が Windows 7 以降の場合、エージェント PC とプリントサーバが同一のドメインに参加している、または、エージェント PC の資格認証マネージャにプリントサーバの資格情報が登録されている必要があります。資格情報を追加した場合はエージェント PC を再起動する必要があります。

重要

UNIX エージェントおよび Mac エージェントは操作ログ取得の対象外です。

4.3.6 資産管理の前提条件

MDM システムと連携してスマートデバイスを管理する場合の前提条件

- 資産管理をする場合、MDM システムと連携してスマートデバイスを管理するスマートデバイスの前提 OS は、iOS または Android です。
- セキュリティポリシーによって USB デバイスの使用を抑止するとき、抑止の対象外とする USB デバイスを資産として登録するためには、オンライン管理のコンピュータが必要です。

SAMAC 辞書の情報を利用する場合の前提条件

SAMAC 辞書の情報を利用する場合は、サポートサービス契約をして、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ダウンロードし、オフライン更新する必要があります。なお、SAMAC ソフトウェア辞書のオフライン更新用ファイルのダウンロードは、日本国内だけでサポートしています。

4.3.7 配布機能の前提条件

配布機能を利用するには、配布先のコンピュータにエージェントが導入されている必要があります。

ソフトウェアをインストールする場合、インストーラーが MSI ファイルまたは EXE ファイルである必要があります。また、サイレントインストールに対応している必要があります。

4.3.8　レポートの前提条件

レポートは、種類ごとに表示の前提条件が異なります。レポートの種類ごとの前提条件を次の表に示します。

レポートの種類		前提条件
ダイジェストレポート	日刊ダイジェスト	• 表示される内容に応じた、管理対象の機器や資産情報が登録されている • 表示する期間に応じた日数が経過している
	週刊ダイジェスト	
	月刊ダイジェスト	
セキュリティ診断レポート	現状セキュリティ診断	• 管理対象の機器が存在する • セキュリティポリシーの設定が有効になっている
	期間指定セキュリティ診断	• 管理対象の機器が存在する • セキュリティポリシーの設定が有効になっている • 表示する期間に応じた日数が経過している
セキュリティ詳細レポート	危険レベルの状況	• 管理対象の機器が存在する • セキュリティポリシーで、各レポートに対応した設定が有効になっている
	更新プログラムの適用状況	
	ウィルス対策製品の状況	
	使用必須ソフトウェアのインストール状況	
	使用禁止ソフトウェアのインストール状況	
	セキュリティ設定の状況	
	禁止操作の状況	
	ユーザーの活動状況	
機器詳細レポート	機器の管理状況	管理対象の機器が存在する
	グリーン IT（省電力設定状況）	
資産詳細レポート	ハードウェア資産	ハードウェア資産情報が登録されている
	ハードウェア資産の費用	契約対象に「ハードウェア資産」が設定されている
	ソフトウェアライセンスの費用	契約対象に「ソフトウェアライセンス」が設定されている
	その他の費用	契約対象に「その他」が設定されている
	ライセンス超過ソフトウェア	管理ソフトウェア情報、およびソフトウェアライセンス情報が登録されている
	ライセンス余剰ソフトウェア	

4.4 システム構成の検討

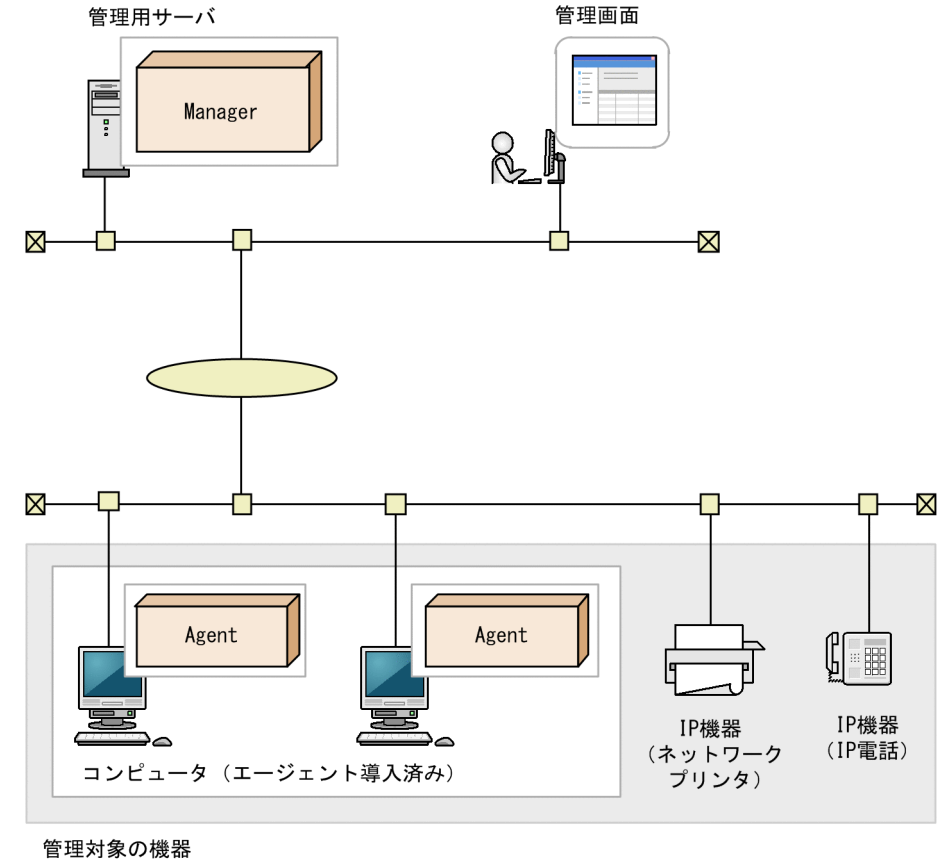
構築するシステムの構成を検討します。システムの目的に従って適切な構成を選択します。JP1/IT Desktop Management 2 で構築できるシステム構成の種類を次の表に示します。

なお、資産管理サーバ（Asset Console）を配置したシステム構成については、マニュアル「JP1/IT Desktop Management 2 - Asset Console 構築・運用ガイド」のシステム構成の説明を参照してください。

システム構成の種類	特徴
最小構成	管理用サーバおよび管理対象となる機器だけを配置した構成です。
基本構成	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に、中継システムを設置して、管理用サーバやネットワークの負荷を分散する構成です。
オフライン管理構成	管理対象となるコンピュータに、管理用サーバにネットワーク接続できないコンピュータを含む構成です。スタンドアロンのコンピュータや、拠点内だけのネットワークに接続しているコンピュータの機器情報を管理できます。
エージェントレス構成	管理対象となるコンピュータにエージェントレスのコンピュータを含む構成です。
サポートサービス連携構成	サポートサービスサイトと連携する構成です。サポートサービスサイトからサポート情報ファイルを管理用サーバにダウンロードして、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セキュリティポリシーに反映できます。また、管理対象のコンピュータに最新の更新プログラムを適用することもできます。
Active Directory 連携構成	Active Directory で管理する機器情報を収集するシステム構成です。Active Directory から収集した情報を管理用サーバに登録できます。
MDM 連携構成	MDM システムと連携してスマートデバイスを管理する構成です。MDM システムで管理しているスマートデバイスを JP1/IT Desktop Management 2 の管理対象にして、ほかの機器と同様に一元管理できます。
ネットワーク監視構成	ネットワークを監視して、機器のネットワーク接続を制御する構成です。管理対象のコンピュータにネットワークモニタエージェントが導入されている場合に、機器のネットワーク接続を制御できます。
JP1/NETM/NM - Manager 連携構成	JP1/NETM/NM - Manager と連携することで、ネットワーク制御用アプライアンスで監視しているネットワーク接続を JP1/IT Desktop Management 2 から制御できます。
リモートコントロール構成	リモートコントロール機能を利用してコンピュータを遠隔操作する構成です。コンピュータ間でファイル転送、チャットなどもできます。
JP1/IM 連携構成	JP1/IM と連携して、JP1/IT Desktop Management 2 で発生した障害イベントを JP1/IM で一元管理する構成です。連携するほかの JP1 製品の情報も一元管理でき、タイムリーに情報を確認できます。
クラスタ構成	管理用サーバをクラスタ化したシステム構成です。稼働中の管理用サーバに障害が発生した場合、待機中の管理用サーバに切り替えて、運用を続行できます。
インターネットゲートウェイ構成	社外で利用するコンピュータを、インターネットゲートウェイ経由で管理する構成です。

4.4.1　最小構成

JP1/IT Desktop Management 2 で構築する最小構成のシステムについて説明します。最小構成のシステムは、1 台の管理用サーバおよび管理対象となる機器で構成されます。最小構成を次の図に示します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager
Agent：JP1/IT Desktop Management 2 - Agent

設定したセキュリティポリシーに従って、管理用サーバはコンピュータのセキュリティ状況を診断します。セキュリティポリシーの設定やセキュリティ診断結果の確認には操作画面を使用します。操作画面は Web ブラウザを使用して表示し、操作します。また、Web ブラウザで管理用サーバにアクセスできる環境であれば、ログインして操作画面を操作できます。

最小構成の前提条件について説明します。

- 管理対象となるコンピュータは 1 台の管理用サーバに接続します。
- TCP/IP 通信ができる環境であれば、LAN、WAN に関係なくコンピュータを管理対象に追加できます。
- 操作画面は Web ブラウザで操作します。このため、管理用サーバと HTTP 通信ができれば、どのコンピュータからでも操作できます。

4.4.2　基本構成

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の、中継システムを設置した構成を、基本構成と呼びます。中継システムを設置すると、ネットワークおよび管理用サーバの負荷を軽減できます。

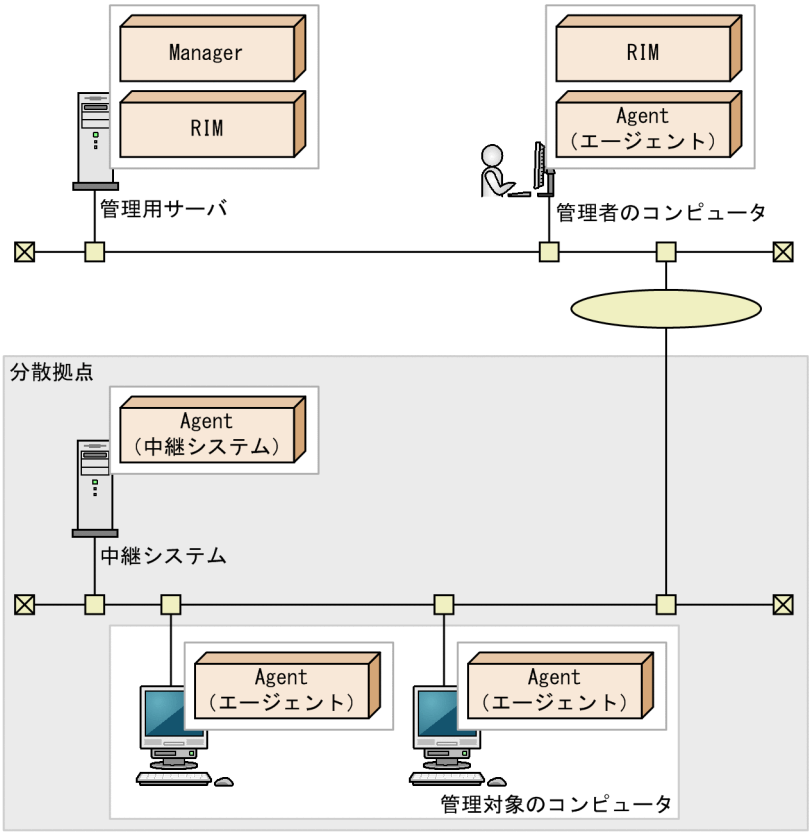
中継システムは、次の条件を目安に設置してください。

- 分散拠点ごとに中継システムを設置する
- 管理対象のコンピュータ 1,000 台につき、中継システムを 1 台設置する

中継システムを構築するには、中継システム専用のエージェント設定を作成して割り当てる必要があります。中継システムに割り当てるエージェント設定を作成する場合の設定内容については、「(4)　エージェント設定のパラメーター 」の各項目の内容を参照してください。

> **ヒント**
>
> 中継システムを設置しなくてもリモートインストールマネージャを使用して配布できますが、ネットワークの負荷が増大するため、中継システムを設置することをお勧めします。

基本構成を次の図に示します。



（凡例）

Manager　：JP1/IT Desktop Management 2 - Manager
RIM　：Remote Install Manager
Agent（エージェント）：
　エージェントとしてインストールしたJP1/IT Desktop Management 2 - Agent
Agent（中継システム）：
　中継システムとしてインストールしたJP1/IT Desktop Management 2 - Agent

分散拠点にある管理対象のコンピュータを対象とした配布は、中継システムからのポーリングが発生したタイミングで実行されます。

NAT 環境の場合に必要な設定

分散拠点のコンピュータに導入する中継システムおよびエージェントのエージェント設定では、接続先となる管理用サーバをグローバル IP アドレスまたはホスト名で指定してください。ホスト名で指定する場合は、DNS サーバや hosts ファイルで名前解決したときの IP アドレスが、グローバル IP アドレスとなるように設定してください。

重要

NAT 環境の場合は、分散拠点にあるネットワーク機器やエージェント未導入の機器を、エージェントレスで管理できません。

4.4.3　複数サーバ構成

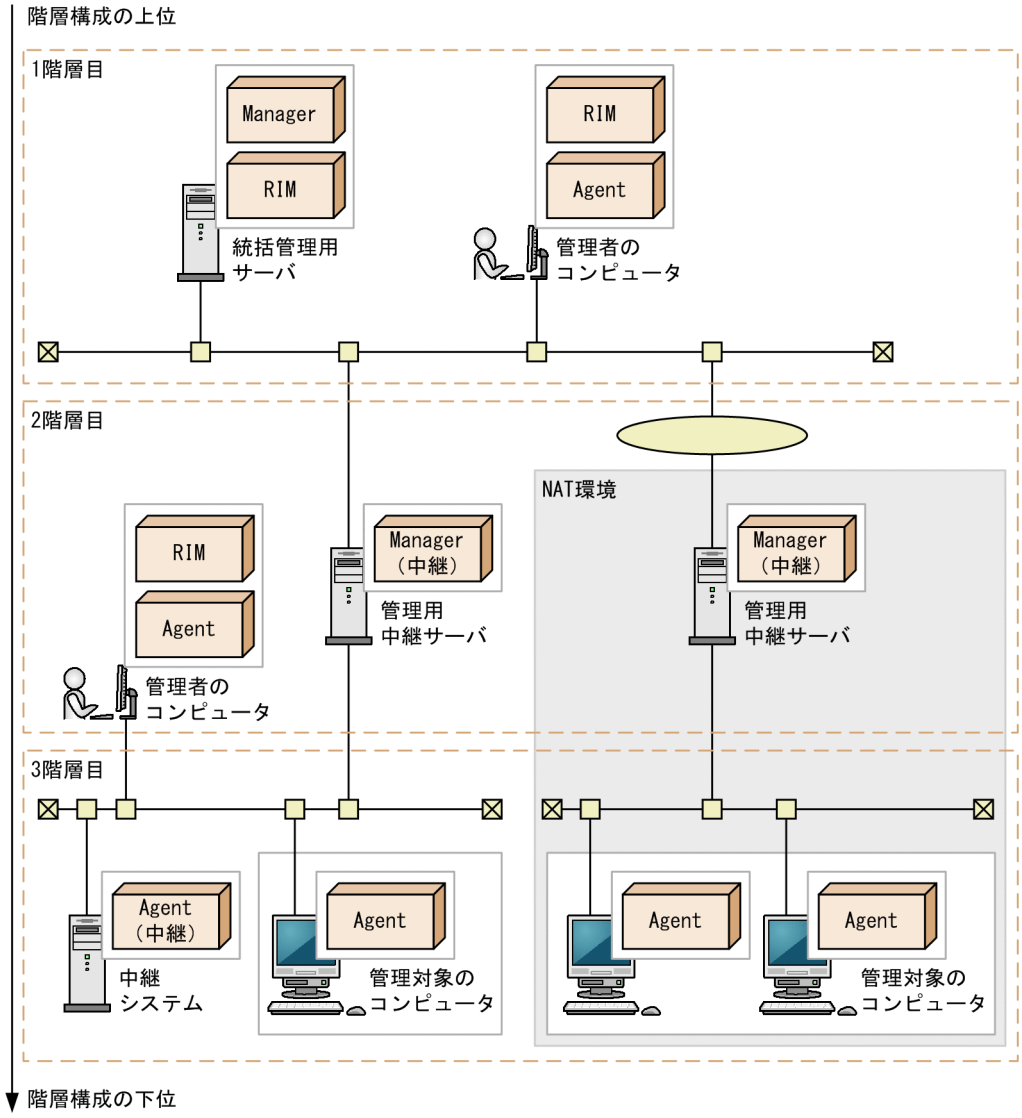
統括管理用サーバおよび複数の管理用中継サーバによって階層化されたシステムを複数サーバ構成と呼びます。管理者や管理用サーバの負荷を分散したり、NAT 環境での運用に対応したりできます。複数サーバ構成では、統括管理用サーバを 1 階層目として、7 階層までシステムを階層化できます。

次のような環境で JP1/IT Desktop Management 2 を運用したい場合は、複数サーバ構成でシステムを構築してください。

- 部門やネットワーク構成ごとに JP1/IT Desktop Management 2 を運用したい場合
- リモートインストールマネージャを使用した配布で、ジョブの実行やパッケージの配布によって掛かるネットワークへの負荷を軽減したい場合

複数サーバ構成では、基本構成と同様に中継システムを設置できます。中継システムは接続先の管理用サーバの 1 階層下に属すると見なされます。中継システムを設置すると、中継システムが属する階層よりも下の階層には、管理用中継サーバを設置できなくなります。また、7 階層目の管理用中継サーバには中継システムを設置できません。中継システムを含むシステム構成の概要については「4.4.2　基本構成」を参照してください。

複数サーバ構成を次の図に示します。



（凡例）
Manager　：JP1/IT Desktop Management 2 - Manager
Manager（中継）：管理用中継サーバとしてインストールしたJP1/IT Desktop Management 2 - Manager
RIM　：Remote Install Manager
Agent　：エージェントとしてインストールしたJP1/IT Desktop Management 2 - Agent
Agent（中継）　：中継システムとしてインストールしたJP1/IT Desktop Management 2 - Agent

1 台の管理用サーバに接続できる管理用中継サーバは 100 台までです。

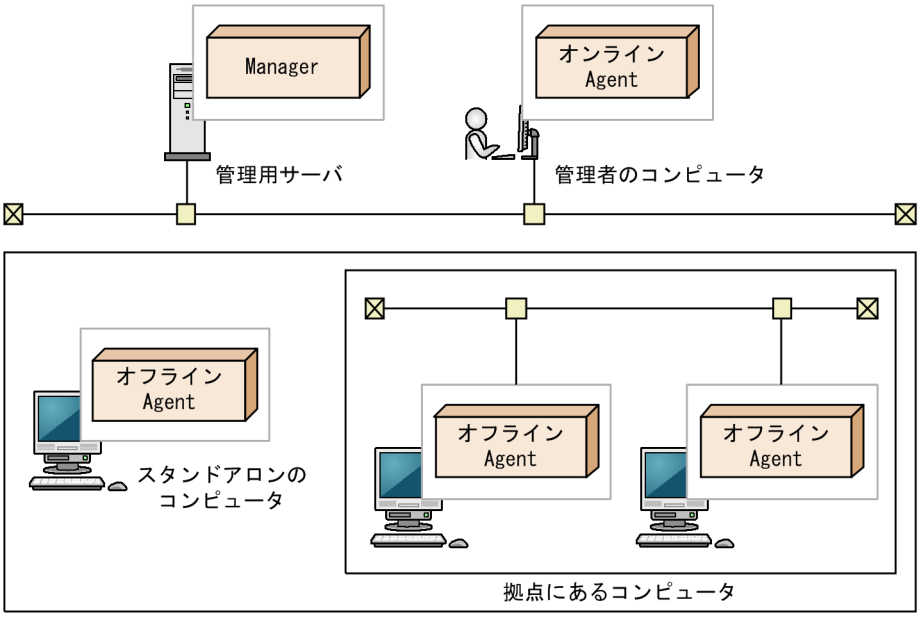
1 台の管理用中継サーバでは、30,000 台まで管理できます。

管理用中継サーバのホスト名の制限事項

統括管理用サーバの直下のホストから最下位のホストまでのホスト名を合計した長さ（ホスト名とホスト名の間の区切り文字を含む）が 255 バイト以内になるように、中継システムおよび管理用中継サーバのホスト名を設定する必要があります。

4.4.4　オフライン管理構成

スタンドアロンのコンピュータや拠点にあるコンピュータなど、管理用サーバにネットワーク接続できないコンピュータも管理できます。オフライン管理のコンピュータを配置した構成を、オフライン管理構成といいます。オフライン管理構成を次の図に示します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager

オンラインAgent：オンライン管理用のJP1/IT Desktop Management 2 - Agent

オフラインAgent：オフライン管理用のJP1/IT Desktop Management 2 - Agent

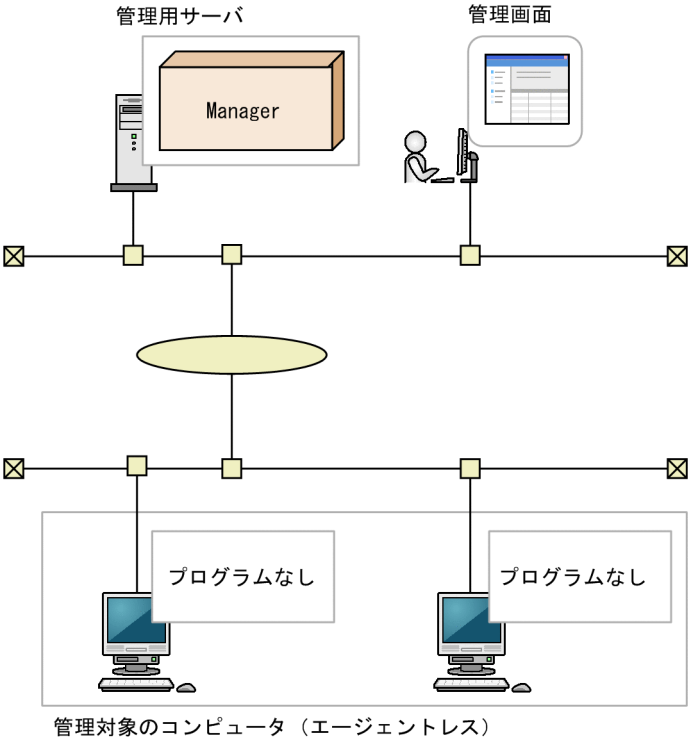
この図のシステム構成では、エージェント導入済みのコンピュータだけで構成されていますが、エージェントレスのコンピュータが混在した構成にすることもできます。

オフライン管理構成の前提条件として、管理者のコンピュータにオンライン管理用のエージェントをインストールする必要があります。オフライン管理のコンピュータを管理対象にするには、外部記憶媒体を使用して対象のコンピュータの機器情報を収集したあと、オンライン管理用のエージェントから管理用サーバへ機器情報を通知する必要があるためです。

> **重要**
>
> オフライン管理のコンピュータの場合、オンライン管理のコンピュータと比較して、機能差異があります。 機能差異については、「(1)　管理形態による機能差異」を参照してください。

4.4.5　エージェントレス構成

管理対象となるコンピュータにエージェントを導入して管理するだけでなく、エージェントを導入しないでコンピュータを管理することもできます。エージェントレスのコンピュータを配置した構成をエージェントレス構成といいます。エージェントレス構成を次の図に示します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager

この図のシステム構成では、エージェントレスのコンピュータだけで構成されていますが、エージェントレスのコンピュータとエージェント導入済みのコンピュータが混在した構成にすることもできます。

エージェントレス構成の前提条件について説明します。

- 管理用サーバから探索機能で直接参照できるコンピュータが対象になります。探索機能とは、指定されたネットワークに接続されている管理対象となる機器を検索する機能です。
- 次のどちらかの認証をできるようにします。
  - 管理対象コンピュータの OS で管理共有を設定し、OS のログオンアカウントを、JP1/IT Desktop Management 2 が認証できるようにする。
  - 管理対象コンピュータを SNMP で認証できるようにする。

エージェントレスのコンピュータを管理するための前提条件については、「4.2.8　エージェントレスで管理するための前提条件」を参照してください。

重要

エージェントレスのコンピュータの場合、エージェントを導入したコンピュータと比較して、機能差異があります。機能差異については、「(1)　管理形態による機能差異」を参照してください。

4.4.6　サポートサービス連携構成

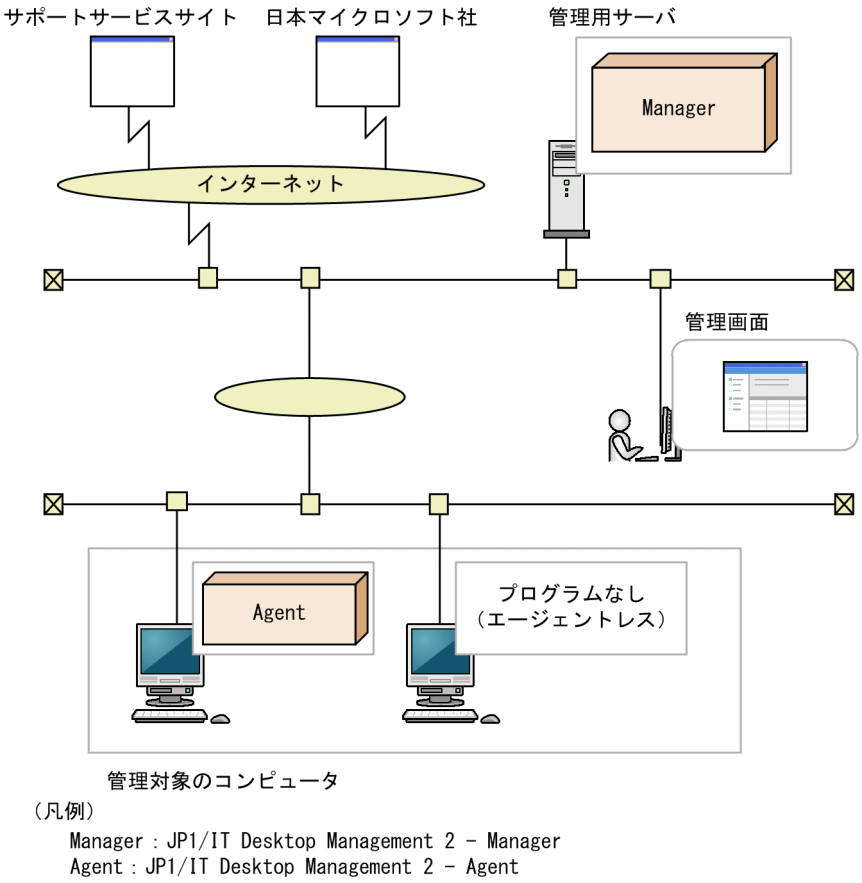
サポートサービスサイトから最新のサポート情報ファイルをダウンロードし、管理用サーバに登録されているセキュリティポリシーの判定項目に最新の更新プログラムおよびウィルス対策製品情報を反映できます。また、日本マイクロソフト社から更新プログラムを自動的にダウンロードして、コンピュータに適用できます。この構成をサポートサービス連携構成といいます。

ウィルス対策製品情報の反映は、日本国内だけでサポートしています。

ヒント

サポートサービス連携構成にするには、サポートサービス契約が必要です。

サポートサービス連携構成を次の図に示します。



更新プログラムファイルを使用して、更新プログラムをコンピュータに配布できます。日本マイクロソフト社の Web サイトにインターネット接続できる環境の場合、自動的に更新プログラムがダウンロードされパッケージが作成されます。

更新プログラム情報の更新は、管理用サーバが定期的に自動で 1 日 1 回（24 時間間隔）実施します。

サポートサービス連携構成の場合、管理用サーバからインターネット経由でサポートサービスサイト、および日本マイクロソフト社の Web サイトに接続します。このため、管理用サーバではインターネットに接続できるようにしてください。また、複数サーバ構成の場合、サポートサービスサイトを利用する管理用サーバごとにサポートサービス連携構成にしてください。 なお、そのほかのシステムの特徴および前提条件については、「4.4.1　最小構成」を参照してください。

ヒント

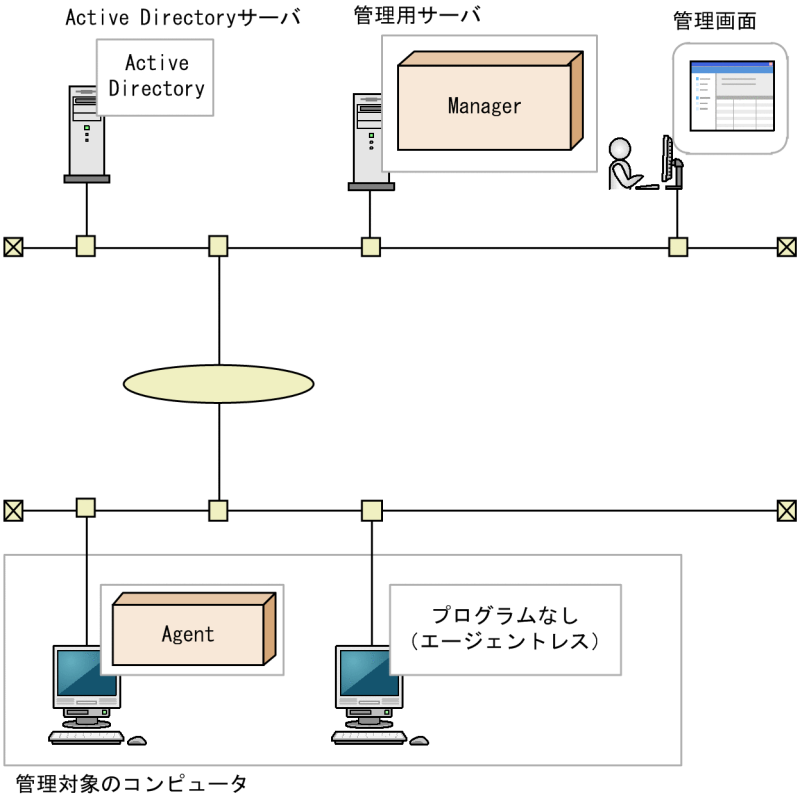
管理用サーバがインターネット接続できない環境でも、更新プログラム情報およびウィルス対策製品情報を管理できます。この場合、管理用サーバ以外のインターネット接続できるコンピュータが、サポートサービスサイトからサポート情報ファイルを取得して、管理用サーバにアップロードします。また、配布する更新プログラムの実行ファイルも、日本マイクロソフト社の Web サイトからコンピュータにダウンロードして、そのあと管理用サーバにアップロードします。

4.4.7　Active Directory 連携構成

JP1/IT Desktop Management 2 は Active Directory と連携できます。Active Directory と連携することで、Active Directory で管理している情報を機器情報として収集できます。Active Directory と連携するには、Active Directory サーバが次の OS であることが前提となります。

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012
- Windows Server 2008
- Windows Server 2003

Active Directory 連携構成を次の図に示します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager
Agent：JP1/IT Desktop Management 2 - Agent

Active Directory 連携構成の環境を構築したら、設定画面の［Active Directory の設定］画面で Active Directory との連携の設定をしてください。また、必要に応じて、追加機器情報として取得する情報の設定もしてください。

ヒント

複数の Active Directory と連携することもできます。複数のドメインで管理している情報を、JP1/IT Desktop Management 2 で一元管理できます。なお、連携できる Active Directory の数に上限はありません。

4.4.8 MDM 連携構成

MDM システムと連携することで、MDM システムで管理しているスマートデバイスを JP1/IT Desktop Management 2 の管理対象にして、ほかの機器や資産と同様に一元管理できます。

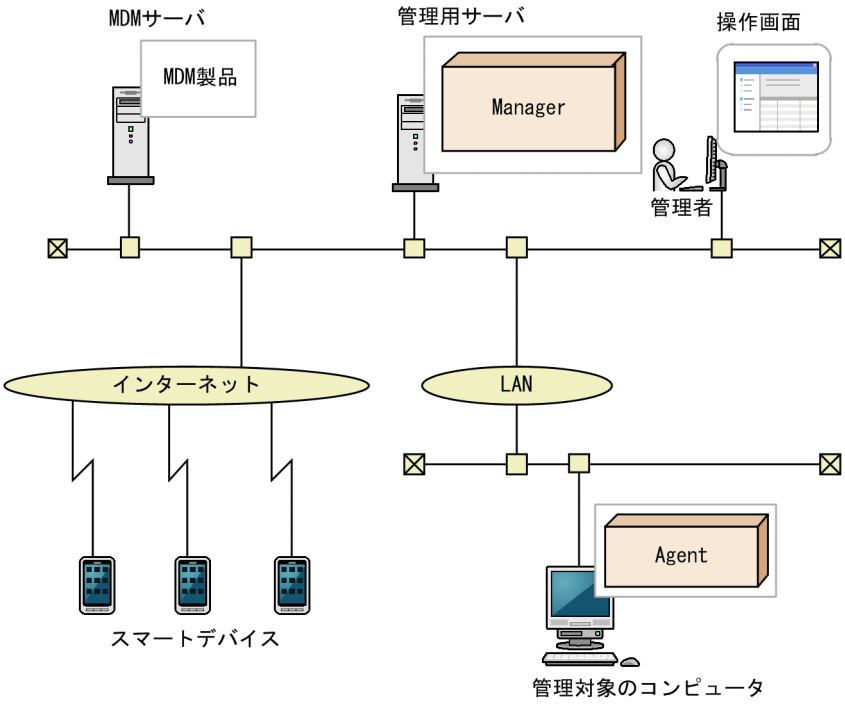
連携できる MDM システムを次に示します。

製品名	バージョン
JP1/IT Desktop Management 2 - Smart Device Manager	11-00

製品名	バージョン
MobileIron	5.8、5.9、7.5、10※

注※　リビジョンを含みます。

MDM システムと連携して、スマートデバイスを管理するシステム構成を次の図に示します。



（凡例）

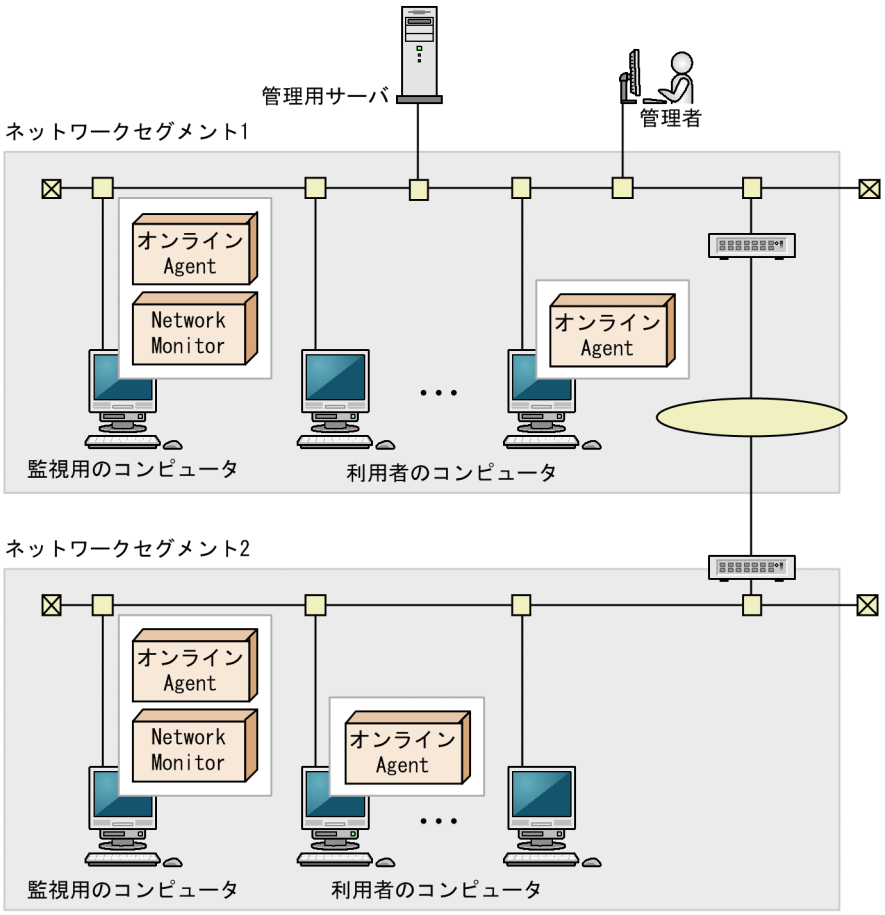
Manager：JP1/IT Desktop Management 2 - Manager
Agent：JP1/IT Desktop Management 2 - Agent

MDM 連携構成を構築したら、設定画面の［MDM 連携の設定］画面で MDM 連携の設定をしてください。設定が完了すると、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。情報が取得されたスマートデバイスは発見された機器として扱われ、 JP1/IT Desktop Management 2 の管理対象にできます。

MDM システム上でスマートデバイスの情報が更新された場合、スマートデバイスの情報を取得したタイミングで、JP1/IT Desktop Management 2 上の情報も更新されます。このため、MDM システムと連携する場合は、定期的に情報を取得するようにスケジュールを設定することをお勧めします。

4.4.9　ネットワーク監視構成

ネットワークを監視して機器のネットワーク接続を制御できます。また、セキュリティ対策が不十分と判断されたコンピュータのネットワーク接続を自動的に遮断できます。ネットワークモニタ機能を利用して、ネットワークを監視するシステム構成を次の図に示します。



（凡例）
オンラインAgent：オンライン管理用のJP1/IT Desktop Management 2 - Agent
Network Monitor：ネットワークモニタエージェント

ネットワークを監視するためには、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たオンライン管理のコンピュータ（ネットワークを監視するためのコンピュータ）が必要です。

ネットワークを監視するためのコンピュータに割り当てているエージェント設定の［基本設定］で、次の項目のチェックを外さないでください。

- ［上位システムと通信する］
- ［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］

機器画面の［機器一覧（ネットワーク）］画面に表示されたネットワークセグメントのグループごと（ブロードキャストドメイン単位）に、コンピュータを 1 台選んで、ネットワークモニタを有効にしてください。

重要

ネットワークモニタ機能を使用する場合、NX NetMonitor および JP1/NETM/NM は JP1/IT Desktop Management 2 と併用できません。ネットワークセグメント内のコンピュータに NX NetMonitor や JP1/NETM/NM がインストールされている場合は、先にアンインストールしてから、ネットワークモニタ機能を使用してください。

ヒント

ネットワークモニタを有効にすると、そのコンピュータにネットワークモニタエージェントがインストールされます。

オンライン管理のコンピュータに、提供媒体から「JP1/IT Desktop Management 2 - Network Monitor」をインストールして、ネットワークモニタを有効にすることもできます。

ネットワークモニタを有効にすることで、新規にネットワーク接続した機器を自動的に発見できます。また、ネットワークモニタの設定に従って、そのネットワークセグメント内のネットワーク接続が制御されるようになります。なお、同じネットワークセグメント内でネットワークモニタを有効にできるのは 1 台だけです。

ヒント

ネットワークモニタを有効化したコンピュータは、24 時間稼働させてください。コンピュータの電源が OFF になっている間は、ネットワーク接続を制御したり、機器を発見したりできません。

ヒント

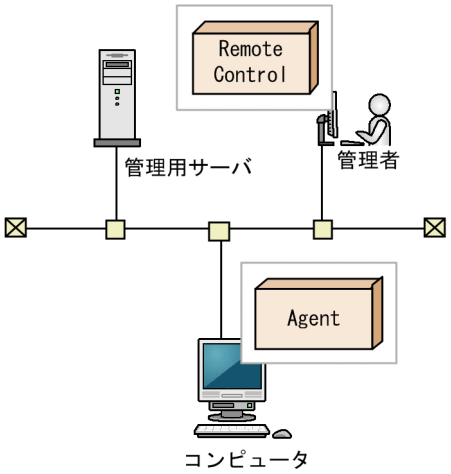
VLAN（Virtual LAN）のトランク接続機能を使用して複数の VLAN を束ねることで、1 台のコンピュータ（かつ、1 つのネットワークカード）で複数のサブネットワーク（VLAN）を監視できます。ただし、次の前提条件を満たす必要があります。

- ネットワークを監視するためのコンピュータのネットワークカードが 、IEEE 802.1Q（VLAN）に対応している
- ネットワークを監視するためのコンピュータを接続するスイッチのポートが、タグ VLAN およびトランク接続（複数の VLAN を通過させる）を設定できる

4.4.10 リモートコントロール構成

遠隔地にあるコンピュータに接続して、キーボードやマウスを直接操作できます。

リモートコントロール構成を次に示します。



（凡例）
Agent：JP1/IT Desktop Management 2 - Agent
Remote Control：コントローラ

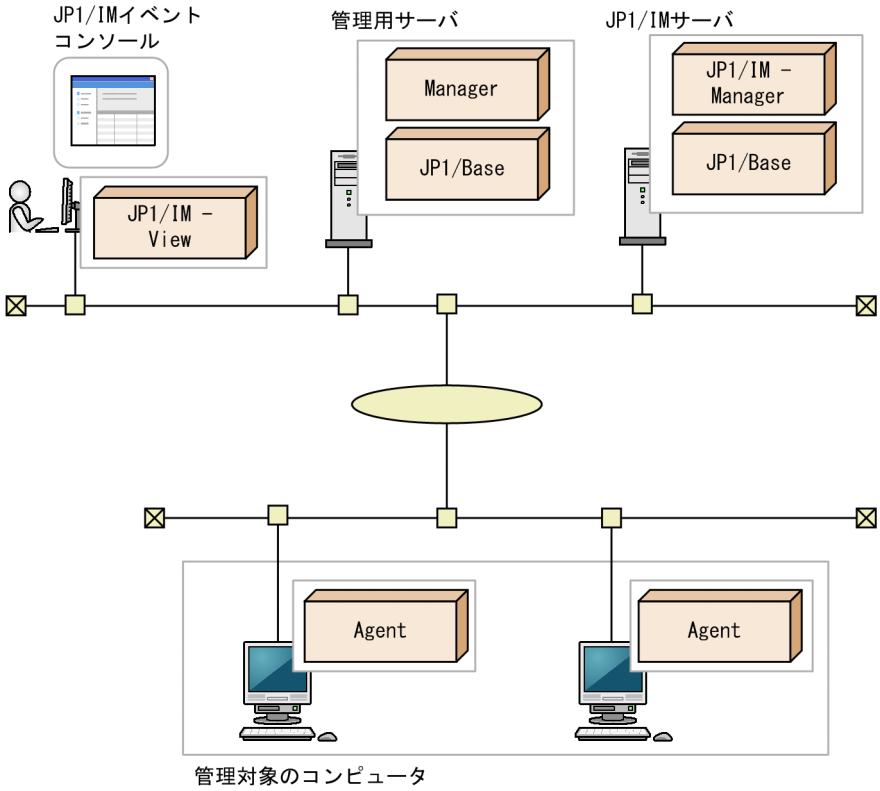
遠隔地にあるコンピュータに接続する管理者のコンピュータには、コントローラが必要です。機器画面から［リモートコントロールを開始する］ボタンをクリックすると、接続する管理者のコンピュータにコントローラが自動的にインストールされます。

重要

OS が UNIX、Mac のコンピュータには、コントローラをインストールできません。また、UNIX エージェント、Mac エージェントにはリモートコントロールされる側に必要なプログラム「リモコンエージェント」が含まれていません。なお、OS が Mac のコンピュータは RFB で接続すると、リモートコントロール機能を使用できます。

4.4.11　JP1/IM 連携構成

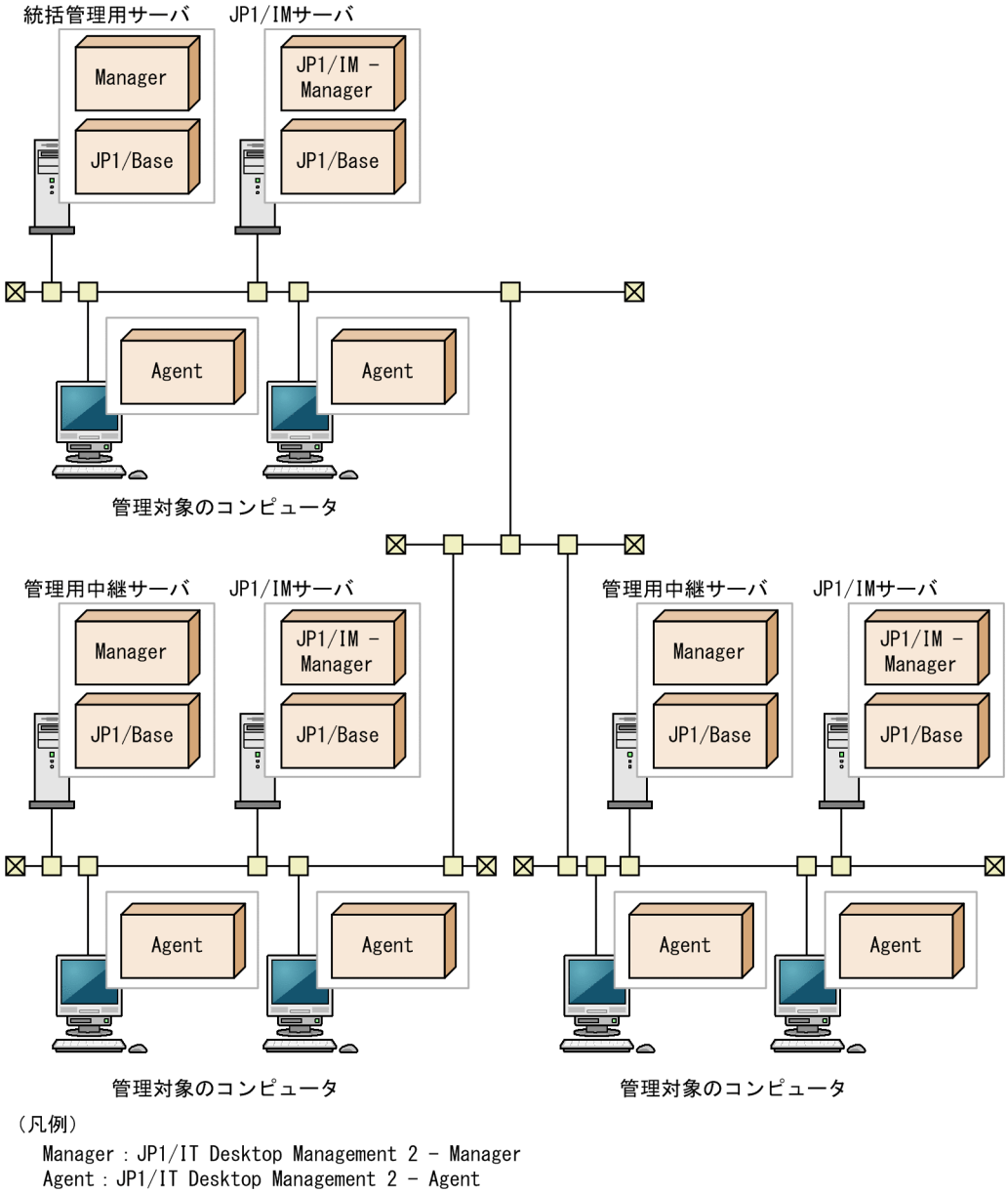
JP1/IM と連携して、管理対象のコンピュータで発生した障害系イベントや管理者の判断が必要な重要イベントを、JP1/IM で JP1 イベントとして一元管理する場合のシステム構成です。JP1/IM 連携構成を次の図に示します。



JP1/IM 連携構成では、JP1/IM および JP1/Base が必要です。

JP1/IM 連携構成の構築では、コンフィグレーションファイル、およびイベント拡張属性定義ファイルを設定します。

発生したイベントの確認および対処は、イベントの発生元である管理用サーバで実施してください。そのため、複数サーバ構成の場合は、拠点管理用に配置した管理用中継サーバごとに JP1/IM サーバを配置した構成で使用してください。複数サーバ構成の場合の、JP1/IM 連携構成を次の図に示します。

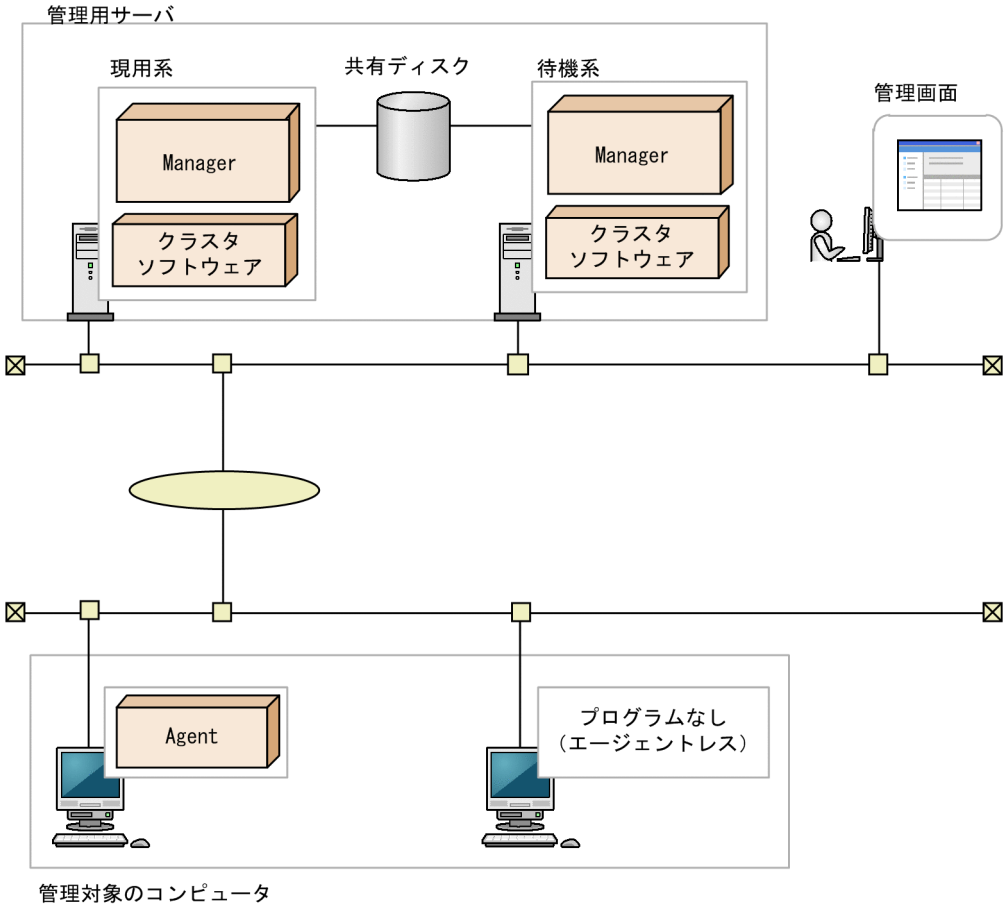


ヒント

すべての拠点を 1 台の JP1/IM サーバで管理することもできます。その場合は、管理用サーバの連携先を同一の JP1/IM サーバに設定して運用してください。

4.4.12 クラスタ構成

管理用サーバをクラスタ構成にできます。実行中のサーバを現用系、待機状態のサーバを待機系といいます。現用系のサーバに障害が発生すると、共有ディスクを介して待機系のサーバに処理を引き継ぎます。サーバをクラスタ構成にしておくことで、サーバに障害が発生しても処理を引き続き実行できます。クラスタ構成を次の図に示します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager
Agent：JP1/IT Desktop Management 2 - Agent

クラスタ構成の前提条件について説明します。

- 使用できるクラスタソフトウェアは Windows Failover Cluster Server です。
- 管理対象となるコンピュータでは、接続先の管理用サーバの設定で論理ネットワーク名および論理 IP アドレスを指定してください。これによって、どちらの管理用サーバに接続しているか、コンピュータ側からは意識する必要がありません。

重要

複数サーバ構成の管理用中継サーバ、ネットワークモニタ、およびインターネットゲートウェイはクラスタ構成にできません。

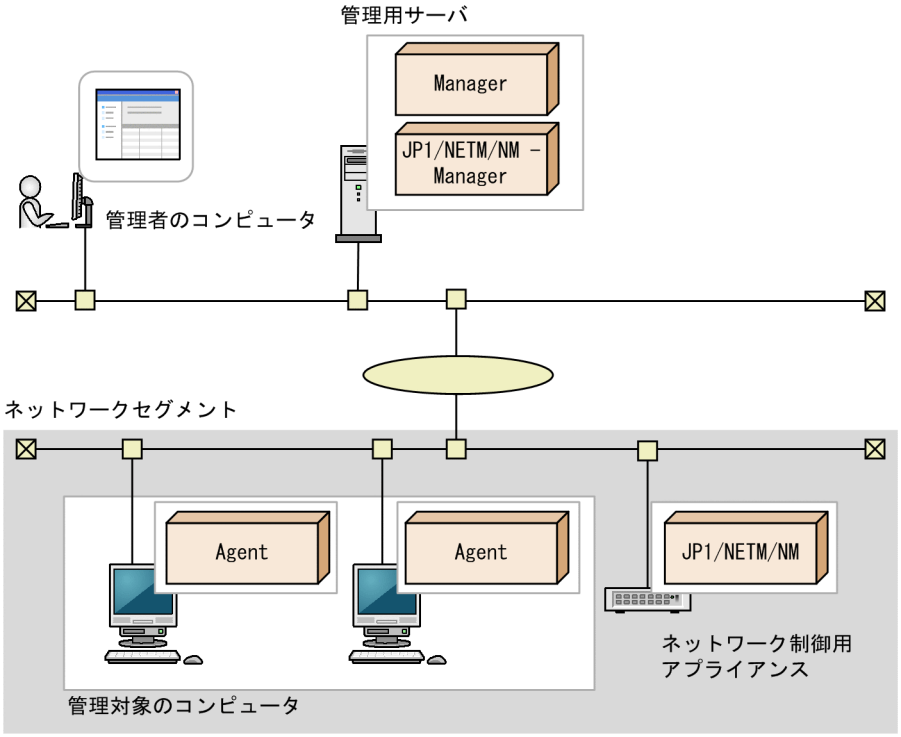
4.4.13 JP1/NETM/NM - Manager 連携構成

JP1/NETM/NM - Manager と連携することで、ネットワーク制御用アプライアンスで監視しているネットワーク接続を JP1/IT Desktop Management 2 から制御できます。

重要

ネットワークモニタを有効にしているネットワークセグメントに、ネットワーク制御用アプライアンスは配置できません。

JP1/NETM/NM - Manager 連携構成を次の図に示します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager
Agent：JP1/IT Desktop Management 2 - Agent

複数サーバ構成の場合、次のどちらかの方法で JP1/NETM/NM - Manager と連携します。

- ネットワーク制御用アプライアンスでネットワーク接続を監視する管理用サーバに、JP1/NETM/NM - Manager をインストールする
- 統括管理用サーバだけに JP1/NETM/NM - Manager をインストールする

  このとき、統括管理用サーバでは、配下の管理用中継サーバが管理している機器をネットワーク制御リストの自動更新の対象にする必要があります。

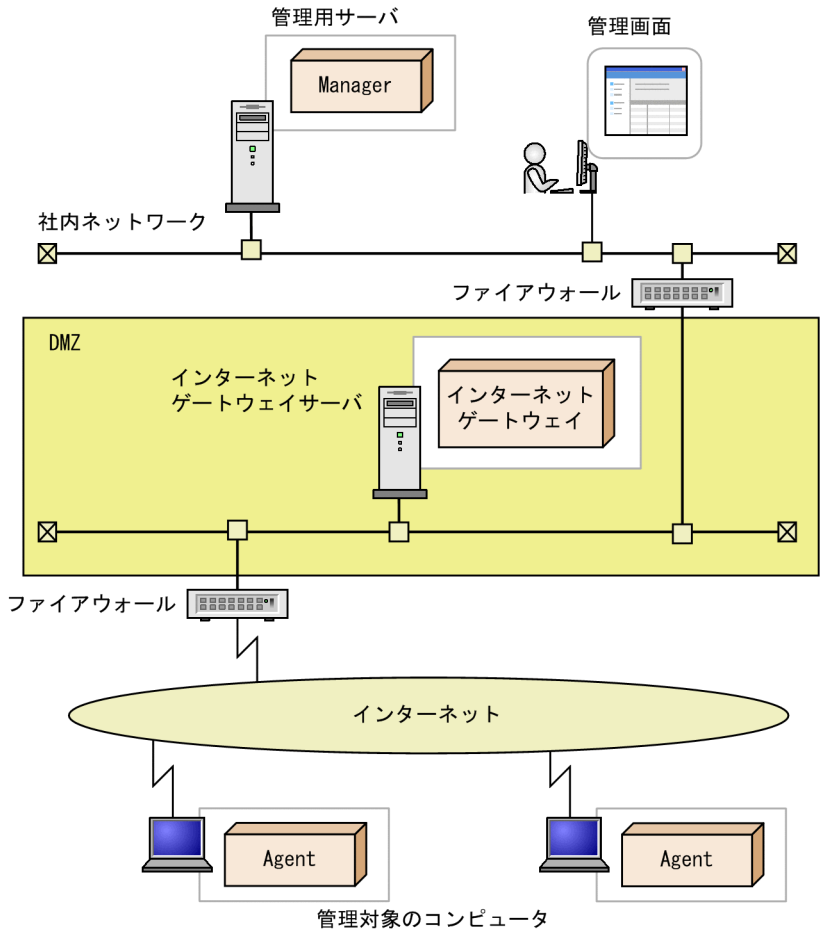
なお、JP1/NETM/NM - Manager は NAT 機器を経由して JP1/NETM/NM を管理できません。NAT 環境のネットワーク接続を JP1/NETM/NM - Manager で制御したい場合は、NAT 環境に設置した管理用中継サーバに JP1/NETM/NM - Manager をインストールしてください。

関連リンク

- 2.8.8　ネットワーク制御リストの管理

4.4.14　インターネットゲートウェイ構成

社外に持ち出した管理対象のコンピュータを、インターネットゲートウェイサーバを経由して JP1/IT Desktop Management 2 で管理することもできます。これをインターネットゲートウェイ構成と呼びます。インターネットゲートウェイ構成を次の図に示します。



（凡例）

Manager：JP1/IT Desktop Management 2 - Manager
Agent：JP1/IT Desktop Management 2 - Agent

社外に持ち出した管理対象のコンピュータは、インターネットゲートウェイを経由して管理用サーバと接続します。管理対象のコンピュータとインターネットゲートウェイは HTTPS で接続します。

1 台のインターネットゲートウェイで 5,000 台まで管理できます。また、複数のインターネットゲートウェイを設置することができます。インターネットゲートウェイおよび中継システムを安定稼動させるために、他のサーバ製品をインストールしないようにしてください。

インターネットゲートウェイ構成の前提条件について説明します。

- インターネットゲートウェイサーバにはエージェントまたは中継システムを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サーバは組織ネットワークの非武装地帯（DMZ）に設置します。

- 管理対象のコンピュータにはエージェントをインストールする必要があります。
- インターネットと DMZ の境界、および DMZ と社内ネットワークの境界に設置するファイアウォールは、それぞれ次に示す通信を許可する必要があります。

  インターネットと DMZ の境界に設置するファイアウォール

  インターネット接続された管理対象のコンピュータから、DMZ の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するためのインバウンド通信

  DMZ と社内ネットワークの境界に設置するファイアウォール

  DMZ のインターネットゲートウェイサーバから、社内ネットワークの管理用サーバに接続できるようにするためのインバウンド通信

4.4.15　NAT 環境構成

JP1/IT Desktop Management 2 を NAT 環境で運用する場合、管理用中継サーバや中継システムを内部ネットワーク内に設置することを検討してください。管理対象の機器台数が多い場合は、外部ネットワークの通信量や接続本数などのネットワーク負荷を軽減することができます。

(1)　内部ネットワークに管理用中継サーバを設置する構成

内部ネットワークに管理用中継サーバを設置する構成について説明します。

- 管理用サーバと同じネットワーク（以下、管理ネットワーク）の NAT 機器（以下、NAT 機器 A）の設定によって、管理用サーバの内部 IP アドレスを外部ネットワークの IP アドレスに静的に割り当ててください。
- 管理用中継サーバの配下の管理対象機器に操作（メッセージ通知、最新の機器情報取得など）をする必要があるときは、管理用中継サーバの管理画面から操作してください。
- 管理ネットワークのリモートインストールマネージャから管理用中継サーバに接続することはできません。

内部ネットワークに管理用中継サーバを設置する場合の設定

管理用中継サーバのセットアップ

管理用中継サーバのセットアップで次の設定値を設定してください。管理用中継サーバのセットアップについては、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の、管理理用中継サーバをセットアップする手順の説明を参照してください。

項目	設定値
上位接続先	管理用サーバの外部 IP アドレス、または管理用サーバの外部 IP アドレスに解決されるホスト名

管理用中継サーバのエージェント設定

管理用中継サーバの管理画面で管理対象機器に割り当たるエージェント設定を次の設定値に設定してください。エージェントの設定については、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の説明を参照してください。

項目	設定値
管理用サーバ	管理用中継サーバの IP アドレス、または管理用中継サーバの IP アドレスに解決されるホスト名
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	管理用中継サーバの IP アドレス、または管理用中継サーバの IP アドレスに解決されるホスト名

内部ネットワークに管理用中継サーバを設置する場合の設定例

IP アドレスの設定

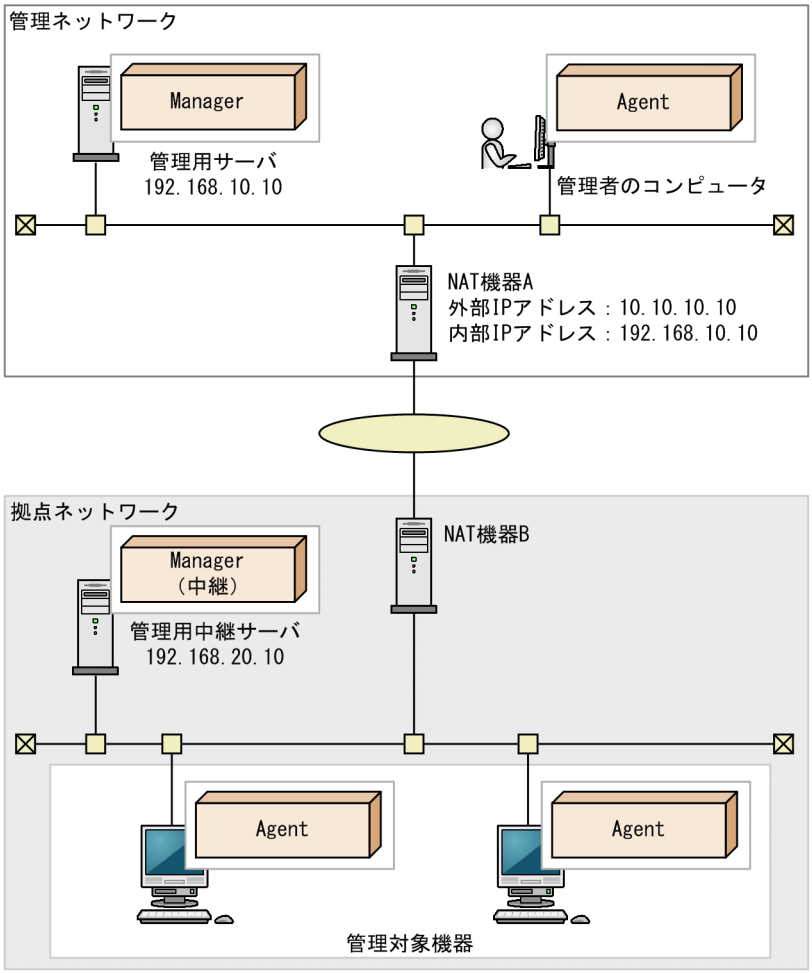
項目	設定値
管理用サーバの IP アドレス（外部ネットワーク）	10.10.10.10
管理用サーバの IP アドレス（内部ネットワーク）	192.168.10.10
管理用中継サーバの IP アドレス（内部ネットワーク）	192.168.20.10

管理用中継サーバのセットアップ

項目	設定値
上位接続先	10.10.10.10

管理用中継サーバのエージェント設定

項目	設定値
管理用サーバ	192.168.20.10
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	192.168.20.10



（凡例）

Manager　　：
　管理用サーバとしてインストールしたJP1/IT Desktop Management 2 - Manager
Manager（中継）：
　管理用中継サーバとしてインストールしたJP1/IT Desktop Management 2 - Manager
Agent　　：JP1/IT Desktop Management 2 - Agent

(2)　内部ネットワークに中継システムを設置する構成

内部ネットワークに中継システムを設置する構成について説明します。

- 管理用サーバと同じネットワーク（以下、管理ネットワーク）の NAT 機器（以下、NAT 機器 A）の設定によって、管理用サーバの内部 IP アドレスを外部ネットワークの IP アドレスに静的に割り当ててください。
- 管理ネットワークと異なるネットワークの管理対象機器に対する操作（メッセージ通知、最新の機器情報取得など）やネットワーク制御は、ポーリングのタイミングで行われます。
- 管理ネットワークと異なるネットワークの管理対象機器をエージェントレス管理することはできません。
- インベントリ情報の通知などは管理対象機器と管理用サーバの間で直接通信が発生します。通信負荷を抑えるには管理用中継サーバの設置を検討してください。

内部ネットワークに中継システムを設置する場合の設定

管理用サーバのエージェント設定

管理用サーバの管理画面で管理対象機器に割り当たるエージェント設定を次の設定値に設定してください。エージェントの設定については、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の説明を参照してください。

項目	設定値
管理用サーバ	管理用サーバの外部 IP アドレス、または管理用サーバの外部 IP アドレスに解決されるホスト名
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	中継システムの IP アドレス、またはホスト名

中継システムのセットアップ

中継システムのセットアップで次の設定値を設定してください。中継システムのセットアップについては、マニュアル「JP1/IT Desktop Management 2 構築ガイド」の、中継システムをセットアップする手順の説明を参照してください。

項目	設定値
上位システムと通信する	チェックする
ホスト名または IP アドレス	管理用サーバの外部 IP アドレス、または管理用サーバの外部 IP アドレスに解決されるホスト名

内部ネットワークに中継システムを設置する場合の設定例

IP アドレスの設定

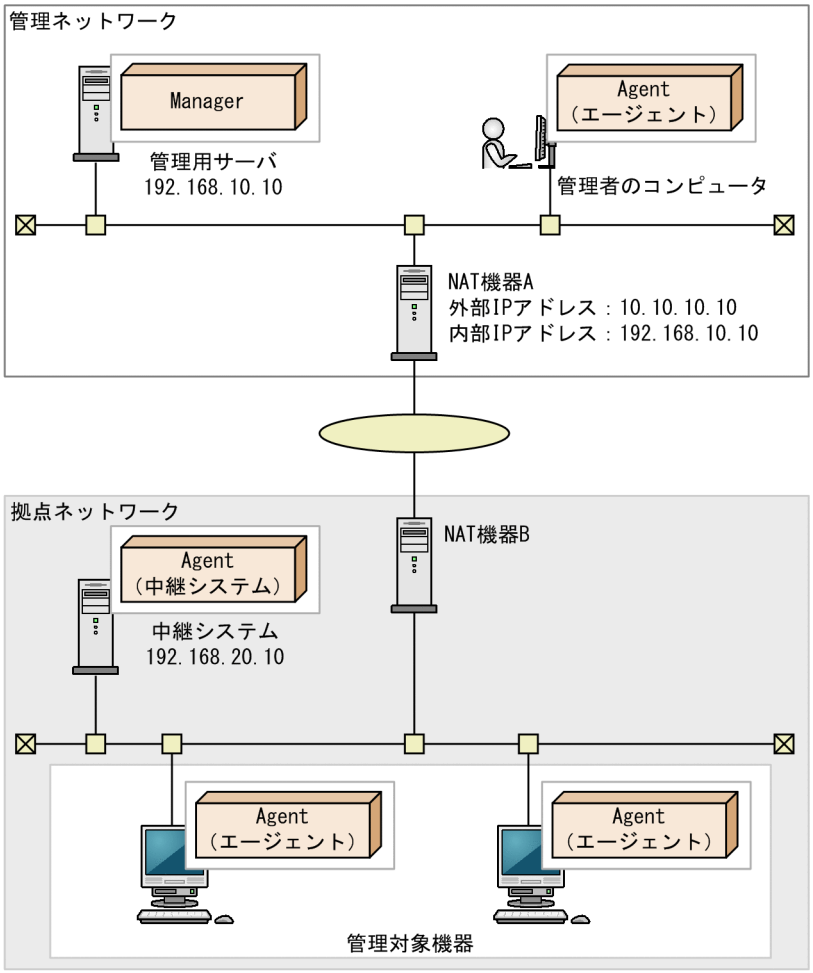
項目	設定値
管理用サーバの IP アドレス（外部ネットワーク）	10.10.10.10
管理用サーバの IP アドレス（内部ネットワーク）	192.168.10.10
中継システムの IP アドレス（内部ネットワーク）	192.168.20.10

管理用サーバのエージェント設定

項目	設定値
管理用サーバ	10.10.10.10
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	192.168.20.10

中継システムのセットアップ

項目	設定値
上位システムと通信する	チェックする
ホスト名または IP アドレス	10.10.10.10



（凡例）

Manager　：JP1/IT Desktop Management 2 - Manager
Agent（エージェント）：
　エージェントとしてインストールしたJP1/IT Desktop Management 2 - Agent
Agent（中継システム）：
　中継システムとしてインストールしたJP1/IT Desktop Management 2 - Agent

(3) 内部ネットワークに管理用中継サーバおよび中継システムを設置しない構成

内部ネットワークに管理用中継サーバおよび中継システムを設置しない構成について説明します。

- 管理用サーバと同じネットワーク（以下、管理ネットワーク）の NAT 機器（以下、NAT 機器 A）の設定によって、管理用サーバの内部 IP アドレスを外部ネットワークの IP アドレスに静的に割り当ててください。
- 管理ネットワークと異なるネットワークの管理対象機器に対する操作（メッセージ通知、最新の機器情報取得など）やネットワーク制御、配布は、ポーリングのタイミングで行われます。

- 管理ネットワークと異なるネットワークの管理対象機器をエージェントレス管理することはできません。
- 管理用サーバと管理対象機器の間で直接通信が発生します。通信負荷を抑えるには管理用中継サーバまたは中継システムの設置を検討してください。

内部ネットワークに管理用中継サーバおよび中継システムを設置しない場合の設定

管理用サーバのエージェント設定

管理用サーバの管理画面で管理対象機器に割り当たるエージェント設定を次の設定値に設定してください。エージェントの設定については、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の説明を参照してください。

項目	設定値
管理用サーバ	管理用サーバの外部 IP アドレス、または管理用サーバの外部 IP アドレスに解決されるホスト名
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	管理用サーバの外部 IP アドレス、または管理用サーバの外部 IP アドレスに解決されるホスト名

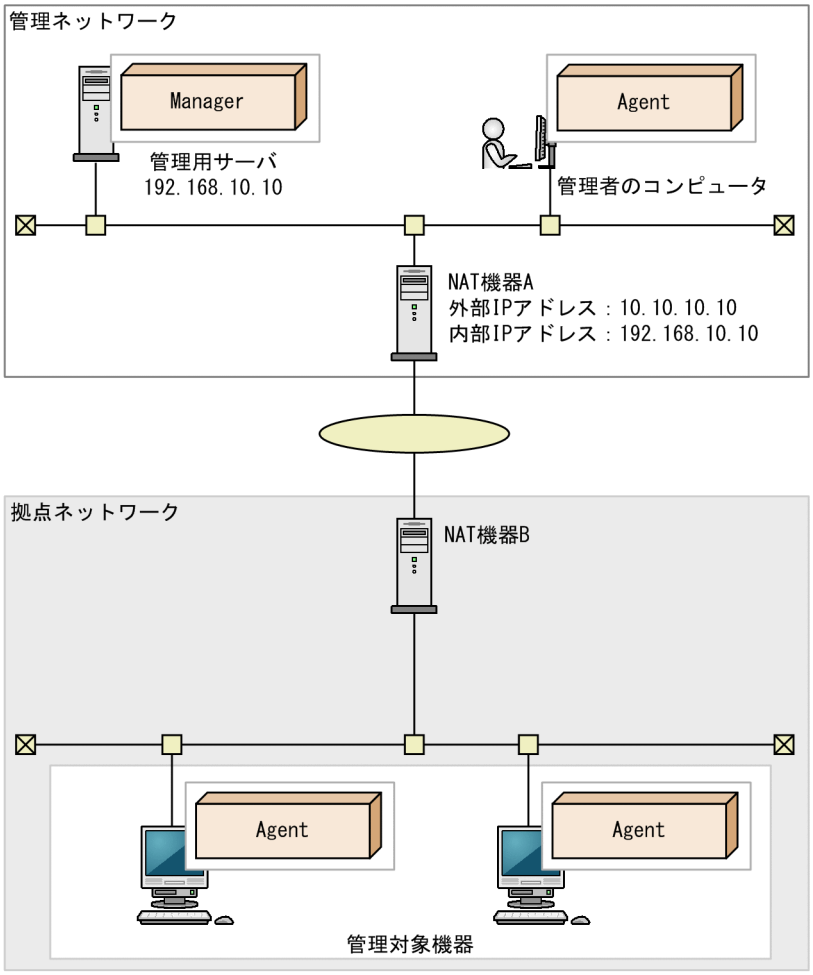
内部ネットワークに管理用中継サーバおよび中継システムを設置しない場合の設定例

IP アドレスの設定

項目	設定値
管理用サーバの IP アドレス（外部ネットワーク）	10.10.10.10
管理用サーバの IP アドレス（内部ネットワーク）	192.168.10.10

管理用サーバのエージェント設定

項目	設定値
管理用サーバ	10.10.10.10
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	10.10.10.10



（凡例）
Manager：JP1/IT Desktop Management 2 - Manager
Agent　：JP1/IT Desktop Management 2 - Agent

(4)　NAT 環境の注意事項

リモートコントロールを NAT 環境で運用する場合、次の注意事項があります。

- コントローラの機器から操作対象のコンピュータに接続できず、操作対象のコンピュータからコントローラの機器が接続可能な場合、操作対象のコンピュータからコントローラに接続要求を実行してください。

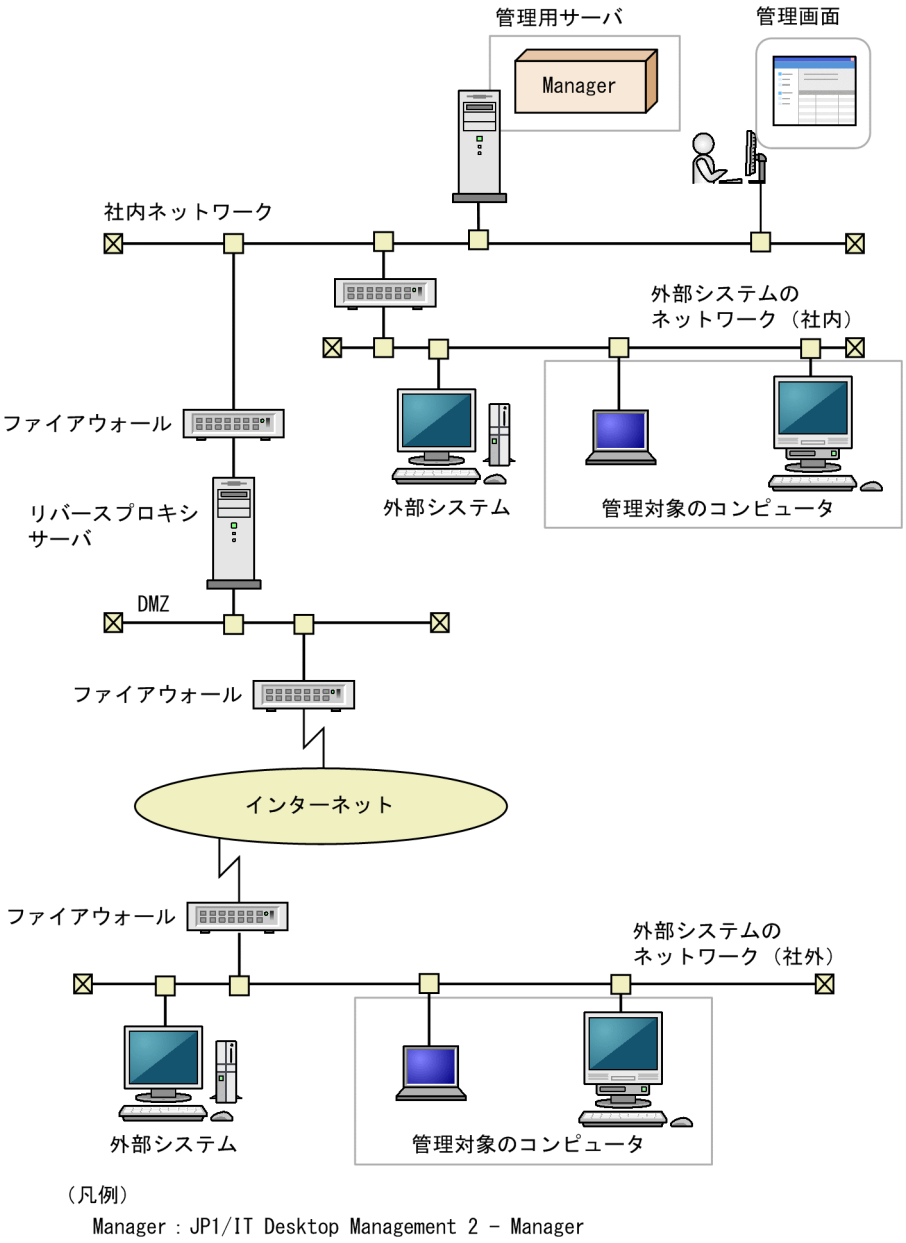
ネットワーク制御を NAT 環境で運用する場合、次の注意事項があります。

- 複数のネットワークが存在する環境ではそれぞれのネットワークで同じ IP アドレスの機器が複数存在することがあります。そのような環境では、ネットワーク接続可否の判定形式を［IP アドレス］にすると、業務に使用している機器の接続が意図しないで遮断されるなど、トラブルにつながるおそれがあります。ネットワーク接続可否の判定形式を［MAC アドレス］または［MAC アドレス＋ IP アドレス］にすることをお勧めします。

4.4.16　外部システム連携構成

外部システムと連携して、機器情報を JP1/IT Desktop Management 2 で管理することもできます。これを外部システム連携構成と呼びます。外部システム連携構成には、外部システムと管理用サーバが社内ネットワークに存在する場合と外部システムがインターネット上に存在する場合があります。

外部システム連携構成を次の図に示します。



外部システムからは HTTP 接続または HTTPS 接続で JP1/IT Desktop Management 2 が提供する API を使用して管理用サーバと通信します。

外部システムがインターネット上に存在する場合は、DMZ にリバースプロキシサーバを設置し、管理用サーバとはリバースプロキシサーバを経由して通信するようにします。

メモ

インターネット上に存在する外部システムから、HTTPS 接続で API を使用して管理用サーバと接続する場合、SSL サーバ証明書を次のように配置してください。

- 外部システム・リバースプロキシサーバ間：リバースプロキシサーバに SSL サーバ証明書を配置
- リバースプロキシサーバ・管理用サーバ間：管理用サーバに SSL サーバ証明書を配置

HTTPS 接続で API を使用して管理用サーバと接続する環境の構築については、マニュアル「JP1/IT Desktop Management 構築ガイド」の「外部システム連携構成で HTTPS を使用する場合の環境構築手順」を参照してください。

4.5　データベースの検討

JP1/IT Desktop Management 2 は、管理対象の機器から収集した情報やレポートの集計情報など、管理に必要な情報をデータベースで管理しています。

データベースは、環境構築時に作成されます。構築するシステム構成や運用方法に応じて、あらかじめ必要なディスク容量を見積もり、環境を準備してください。

> **ヒント**
>
> 運用開始後に管理用サーバのデータベースのバックアップやリストア、効率良く利用するためのメンテナンスを実施する場合、データベースマネージャを利用できます。

関連リンク

- 4.5.1　データベースの概要
- 4.5.2　管理用サーバに必要なディスクの容量
- 4.5.8　推奨ディスク容量の目安
- 4.5.4　操作ログのデータベースに必要なディスク容量の目安
- 4.5.3　操作ログの保管先フォルダに必要なディスク容量の目安

4.5.1　データベースの概要

JP1/IT Desktop Management 2 のデータベースフォルダおよびデータ保管用のフォルダは、データの種類に応じて複数のフォルダに分かれています。

各フォルダの作成先は、管理用サーバのセットアップで設定できます。

各フォルダの詳細について、次の表に示します。

フォルダの種類	説明	作成有無
データベースフォルダ	機器情報、資産情報、セキュリティポリシー、イベント、レポートなどの管理情報が保管されるデータベース領域が作成されます。	○
データフォルダ	登録済みのエージェント、配布機能で作成したパッケージなどのデータが保管されるフォルダです。	○
ローカルデータフォルダ	運用中に管理用サーバの一時フォルダとして使用されるフォルダです。	○
操作ログの保管先フォルダ	操作ログのデータを保存するためのフォルダです。操作画面から操作ログを取り込むことで、ここに格納されているデー	△

フォルダの種類	説明	作成有無
操作ログの保管先フォルダ	タを「操作ログのデータベースフォルダ」に格納して、過去の操作ログを参照できます。	△
操作ログのデータベースフォルダ	コンピュータから収集された操作ログを参照するための、操作ログを格納するデータベース領域です。自動取り込みされた操作ログと手動取り込みされた操作ログが格納されます。	△
変更履歴の出力先フォルダ	保存用の変更履歴を定期的に出力する先のフォルダです。	△
データベース退避フォルダ	データベースフォルダを変更するときに一時退避するためのフォルダです。通常運用では使用しません。	○

（凡例）○：必ず作成される　△：設定に応じて作成される

ヒント

各フォルダは、管理用サーバの OS がローカルドライブと認識したディスクだけ指定できます。ただし、操作ログの保管先フォルダは、ネットワークフォルダも指定できます。そのため、操作ログの保管先フォルダは容量の大きいストレージを利用し、そのほかのフォルダは管理用サーバのハードディスクを利用する運用をお勧めします。ただし、リムーバブルディスクと認識される記憶装置は指定できません。

4.5.2　管理用サーバに必要なディスクの容量

管理用サーバのデータフォルダに必要な、ディスクの容量について説明します。

この表に記載してある以外に、運用のために作業用として使用する、「ローカルデータフォルダ」用として 1 ギガバイトの空き容量を用意することを推奨します。操作ログを取得する場合には、管理対象のコンピュータ 5,000 台あたり、500 メガバイトを追加する必要があります。また、JP1/IT Desktop Management 2 は次の表に記載してある以外にもさまざまな情報を保持していますが、比較的容量が小さいため、見積もりの際にはあまり影響はありません。

データフォルダ	保存されるデータ	保存期間	容量
データベースフォルダ	次に示す、管理用サーバで使用する情報 • セキュリティポリシー • グループ • エージェント設定	削除するまで保存されます。	0.5 ギガバイト
	次に示す資産情報	削除するまで保存されます。	0.1 ギガバイト

データフォルダ	保存されるデータ	保存期間	容量
データベースフォルダ	• ハードウェア資産情報 • 管理ソフトウェア情報 • ソフトウェアライセンス情報 • 契約情報	削除するまで保存されます。	また、次の情報を登録していることを想定しています。各情報には、追加管理項目がないことを想定しています。 • ハードウェア資産情報 20,000 件 • 管理ソフトウェア情報 500 件 • ソフトウェアライセンス情報 100 件 • 契約情報 100 件
	管理対象の機器の機器情報	削除するまで保存されます。	10 ギガバイト 管理対象の機器が 10,000 台の場合を想定しています。
	変更履歴	最大容量に達するまで保存されます。超過したら、古い変更履歴から削除されます。	約 7 ギガバイト 管理対象の機器の台数が 10,000 台の場合で、管理対象の機器 1 台当たりの 1 日に発生する機器情報の変更が、次の件数の合計値であることを想定しています。 • 通常運用で発生する変更の件数：14 件 • 不正な変更の件数：0.1 件（管理対象の機器のうち 10%の機器で 1 件発生）
	イベント	最大容量に達するまで保存されます。超過したら、古いイベントから削除されます。	(250×管理対象のコンピュータ数 10,000 ＋ 10,000）×1.5 キロバイト＝約 4 ギガバイト 次の場合を想定しています。 • 管理対象の機器 1 台当たり、1 日に発生するイベントが 250 件 • 管理対象のコンピュータ数が 10,000 台 • 管理対象の機器の台数に関係なく 1 日に発生するイベントが 10,000 件 • イベント 1 件当たりの容量が 1.5 キロバイト
	保存期間として指定した期間分のレポート	指定した 1～10 年の範囲で保存されます。	10 ギガバイト レポートを 10 年間保存した場合を想定しています。
データフォルダ	次に示す資産情報の添付ファイル • ハードウェア資産情報 • ソフトウェアライセンス情報 • 契約情報	削除するまで保存されます。	5 ギガバイト 実際は、登録した件数だけ容量が増えるため、5 ギガバイトを超えることがあります。 また、次の情報を登録していることを想定しています。各情報には、サイズの大きなファイルを多数登録していないことを想定しています。サイズの大きなファイルを多数登録して管理する場合は、十分な容量を別途確保してください。 • ハードウェア資産情報 20,000 件 • ソフトウェアライセンス情報 100 件 • 契約情報 100 件

データフォルダ	保存されるデータ	保存期間	容量
データフォルダ	配布機能で使用されるパッケージ	削除するまで保存されます。	約 10 ギガバイト 10 メガバイトのパッケージが 1,000 件登録されている場合を想定しています。なお、パッケージには上位の管理用サーバから配布されたパッケージも含まれます。
	操作ログの一時保管データ	操作ログの保管先フォルダに保管するまで保存されます。	約 150 ギガバイト 操作ログを取得する場合に必要です。次の条件で、操作ログの保管先フォルダへの保管処理を 2 週間（5 営業日/週）行わなかった場合を想定しています。 • 管理対象のコンピュータの台数が 10,000 台である。 • すべての操作ログを取得する。 • 操作ログの定期エクスポートを実施しない。
	上位の管理用サーバに送信する情報	上位の管理用サーバに送信するまで保存されます。	24 ギガバイト 管理用中継サーバの場合に必要です。上位の管理用サーバへの情報送信が 2 週間（5 営業日/週）実施されなかった場合を想定しています。
操作ログのデータベースフォルダ	情報漏えいに係わりの深い操作を取得対象にする場合の操作ログ（自動取り込みされた操作ログ）	設定画面の［操作ログの設定］－［自動取り込みされる操作ログの格納期間］で設定した期間の操作ログが保存されます。	約 45 ギガバイト 次の状況を想定しています。 • 管理対象のコンピュータの台数が 10,000 台である。 • コンピュータごとの 1 日当たりの操作ログの容量を 93 キロバイトとする。 • 1 か月分（30 日分）の操作ログを取り込む。
	すべての操作を操作ログの取得対象にする場合の操作ログ（自動取り込みされた操作ログ）	設定画面の［操作ログの設定］－［自動取り込みされる操作ログの格納期間］で設定した期間の操作ログが保存されます。	約 446 ギガバイト 次の状況を想定しています。 • 管理対象のコンピュータの台数が 10,000 台である。 • コンピュータごとの 1 日当たりの操作ログの容量を 1.52 メガバイトとする。 • すべての操作の操作ログを取得することとする。 • 1 か月分（30 日分）の操作ログを取り込む。
	操作ログ一覧で参照するために、保管先から取り込んだ操作ログ（手動取り込みされた操作ログ）	削除するまで保存されます。	約 135 ギガバイト 次の状況を想定しています。 • コンピュータごとの 1 日当たりの操作ログの容量を 1.52 メガバイトとする。

データフォルダ	保存されるデータ	保存期間	容量
操作ログのデータベースフォルダ	操作ログ一覧で参照するために、保管先から取り込んだ操作ログ（手動取り込みされた操作ログ）	削除するまで保存されます。	• すべての操作の操作ログを取得することとする。 • 200 台のコンピュータの 3 か月分（3×30 日分）の操作ログを取り込む。
操作ログの保管先フォルダ	保管された操作ログ	操作ログの保管先を設定している場合に、削除するまで保存されます。 なお、操作ログを取り込んで、操作ログ一覧から参照する場合に、「操作ログのデータベースフォルダ」に取り込まれますが、「操作ログの保管先フォルダ」の操作ログは削除されません。	容量の上限はありません。 管理者が決めた保管期間（日）×管理対象のコンピュータ（台）×70（キロバイト/日/台）を目安に保管先のフォルダを用意してください。 なお、次の状況を想定しています。 • すべての操作の操作ログを取得することとする。 • 操作ログの定期エクスポートを実施しない。
変更履歴の出力先フォルダ	保存用の変更履歴	保存用の変更履歴の出力設定をしている場合に、保存用の変更履歴が CSV ファイル形式で定期的に出力されます。	約 10 ギガバイト 管理対象の機器の台数が 10,000 台で、保存用の変更履歴を 5 年間出力した場合を想定しています。

関連リンク

- 付録 A.6　性能と見積もり

4.5.3　操作ログの保管先フォルダに必要なディスク容量の目安

1 年分の操作ログを保管先フォルダに保管した場合に必要なディスク容量の目安を次の表に示します。

管理対象のコンピュータの台数（台）※1	必要なディスク容量（ギガバイト）	
	操作ログのデータ※2	定期エクスポートで出力される CSV ファイル
500	8（5）	75
1,000	16（10）	151
2,000	32（20）	302
5,000	80（48）	754
10,000	160（96）	1,509
30,000	480（288）	4,526

注　1 年間は 240 日（20 営業日/月）として算出しています。

注※1　Citrix XenApp、Microsoft RDS サーバの操作ログを取得する場合は、Citrix XenApp、Microsoft RDS のユーザー 1 人分の仮想環境をコンピュータ 1 台と置き換えて算出してください。

注※2　括弧内の数値は、1 日あたり 2,000 件の秘文ログを取り込む場合の目安です。秘文ログを取得する場合は、括弧内の数字を足してください。取り込む秘文ログの種類や環境によって異なります。このため、1 週間から 1 か月程度運用して、必要なディスク容量を算出してください。

操作ログの保管先フォルダに必要なディスク容量の目安は、次の式で算出しています。

操作ログのデータ：

機器の台数（台）×69.9（KB）÷1,024÷1,024×日数

定期エクスポートで出力される CSV ファイル：

機器の台数（台）×659.2（KB）÷1,024÷1,024×日数

関連リンク

- 付録 A.6　性能と見積もり

4.5.4　操作ログのデータベースに必要なディスク容量の目安

操作ログをデータベースに自動取り込みする場合に必要なディスク容量の目安は、次の式で算出します。

すべての操作ログを取得する設定の場合

管理対象のコンピュータの台数（台）×自動取り込みされる操作ログの格納期間（日）※×1.52（メガバイト）＝ 自動取り込みで必要なディスク容量（メガバイト）

注※　自動取り込みされる操作ログの格納期間の上限は、300 日です。

ただし、自動取り込みで必要なディスク容量が、「自動取り込みされる操作ログの格納期間（日）×1.5（ギガバイト）」に満たない場合には、「自動取り込みされる操作ログの格納期間（日）×1.5（ギガバイト）」をディスク容量の目安としてください。

秘文ログを取り込む場合、取り込む秘文ログの種類や環境によって必要なディスク容量が異なります。このため、1 週間から 1 か月程度運用し、次の式で 1 日あたりのディスク使用量を求め、安全係数（1.5 倍程度）を掛けて算出してください。

自動取り込みされる操作ログの格納期間（日）×1 日あたりのディスク使用量（メガバイト）×安全係数＝ 自動取り込みで必要なディスク容量（メガバイト）

自動取り込みされる操作ログの件数が 1 億件と 3 億件の場合に必要なディスク容量の目安を次に示します。

1 億件の場合

54.7 ギガバイト

3 億件の場合

161.0 ギガバイト

自動取り込みされる操作ログの件数が 1 億件と 3 億件の場合、操作ログを次の期間データベースに格納できます。

管理対象のコンピュータの台数（台）	格納できる日数の目安	
	1 億件（ディスク容量 54.7 ギガバイト）の場合	3 億件（ディスク容量 164.0 ギガバイト）の場合
500	4 か月	1 年
1,000	2 か月	6 か月
2,000	1 か月	3 か月
5,000	2 週間	1 か月
10,000	1 週間	3 週間
30,000	3 日	1 週間

注　20 営業日/月で計算しています。

操作ログをデータベースに手動取り込みする場合に必要なディスク容量の目安は、次の式で算出します。

すべての操作ログを取得する設定の場合

取り込むコンピュータの台数（台）×1 日に取り込む操作ログの日数（日）×1.52（メガバイト）

計算結果が「1 日に取り込む操作ログの日数（日）×1.5（ギガバイト)」に満たない場合には、「1 日に取り込む操作ログの日数（日）×1.5（ギガバイト)」をディスク容量の目安としてください。

秘文ログを手動取り込みする場合、自動取り込みで必要なディスク容量の算出時に求めた「1 日あたりのディスク使用量（メガバイト）×1 日に取り込む操作ログの日数（日)」をディスク容量の目安としてください。

200 台のコンピュータの操作ログを 3 か月分、手動取り込みする場合

手動取り込みされる操作ログのディスク容量の目安は次の式になります。

90 日×1.5（ギガバイト）＝ 135（ギガバイト）

200 台のコンピュータの半年分（180 日）の操作ログを 1 日の間に手動取り込みする場合、手動取り込みされる操作ログのディスク容量の目安は次の式になります。

180 日×1.5（ギガバイト）＝ 270（ギガバイト）

自動取り込み日数を 30 日とすると、セットアップの操作ログ設定の格納最大日数は 210 日を設定します。

重要

管理画面から操作ログを削除しても操作ログのデータベースのサイズは縮小されません。操作ログの取り込みと削除を行う場合は、削除分を差し引かず、取り込み分をディスク容量の目安としてください。操作ログのデータベースの詳細については、「2.10.2　管理用サーバでの操作ログの管理」を参照してください。

関連リンク

- 付録 A.6　性能と見積もり

4.5.5　操作ログを取得する場合のデータフォルダに必要なディスク容量の目安

操作ログを取得する場合、データフォルダに次のディスク容量を追加する必要があります。

管理対象のコンピュータの台数（台）	必要なディスク容量（ギガバイト）	
	定期エクスポート無効時	定期エクスポート有効時
5,000	75	105
10,000	150	209
30,000	448	627

注　2 週間分（5 営業日/週）の操作ログを保持できるディスク容量を算出しています。操作ログの保管先フォルダや操作ログのデータベースに障害が発生した場合に、データフォルダに操作ログのデータが蓄積されます。2 週間（5 営業日/週）で障害が復旧することを想定しています。

すべての操作ログを取得する設定の場合に必要なディスク容量の目安は、次の式で算出しています。

定期エクスポート無効時：

機器の台数×15.3（MB）÷1,024

定期エクスポート有効時：

機器の台数×21.4（MB）÷1,024

関連リンク

- 付録 A.6　性能と見積もり

4.5.6　保存用の変更履歴の出力に必要なディスク容量の目安

保存用の変更履歴を出力した場合に必要なディスク容量の目安を次の表に示します。

この表に示す値は、次の状況を想定しています。

- 保存用の変更履歴を出力する期間を 5 年間とする。
- 管理対象の機器 1 台当たりに発生する変更の件数を、5 年間で約 100 回とする。

機器の台数（台）	必要なディスク容量（ギガバイト）
500	0.5
1,000	1

機器の台数（台）	必要なディスク容量（ギガバイト）
2,000	2
5,000	5
10,000	10
30,000	30
50,000	49

保存用の変更履歴を出力した場合に必要なディスク容量の目安は、次の式で算出しています。

機器の台数×17.07（KB）÷1024÷1024×月数

4.5.7　変更履歴のデータベースに必要なディスク容量の目安

変更履歴のデータベースに必要なディスク容量の目安を次の表に示します。

この表に示す値は、管理対象の機器 1 台当たりの 1 日に発生する機器情報の変更が、次の件数の合計値であることを想定しています。この件数を超える変更が発生する場合は、十分な容量を別途確保してください。

- 通常運用で発生する変更の件数：14 件
- 不正な変更の件数：0.1 件（管理対象の機器のうち 10%の機器で 1 件発生）

機器の台数（台）	必要なディスク容量（ギガバイト）
2,000 未満	5
5,000	6
10,000	7
30,000	10
50,000	14

変更履歴のデータベースに必要なディスク容量の目安は、次の式で算出しています。

機器の台数×178（KB）÷1024÷1024+4.6（GB）

4.5.8　推奨ディスク容量の目安

JP1/IT Desktop Management 2 で管理するすべてのデータ（操作ログを含む）の推奨ディスク容量の目安を次の表に示します。推奨ディスク容量の目安は、取得する操作ログの種類によって異なります。

なお、管理用中継サーバの場合は推奨ディスク容量の目安に上位の管理用サーバに送信する情報分（24 ギガバイト）を追加してください。

すべての操作を取得対象とする場合

管理対象の機器（台）	推奨ディスク容量（ギガバイト）※1				
	1年※2	2年※2	3年※2	4年※2	5年※2
100	240	242	243	245	247
500	259	267	275	283	291
1,000	281	297	313	329	345
2,000	371	403	435	467	499
3,000	464	512	560	608	656
5,000	645	725	805	885	965
10,000	1,218	1,374	1,538	1,698	1,858
30,000	3,164	3,644	4,124	4,604	5,084

注※1　想定環境に従って、1 日当たりに発生するデータ量に変化がなく、毎日継続してデータが蓄積された場合を想定した値です。

注※2　操作ログの保管期間です。1 年当たり 240 日分（20 営業日/月）のデータ量として計算しています。

情報漏えいに係わりの深い操作だけを取得対象とする場合

管理対象の機器（台）	推奨ディスク容量（ギガバイト）※1				
	1年※2	2年※2	3年※2	4年※2	5年※2
100	236	236	236	236	236
500	237	237	238	238	239
1,000	238	239	240	241	242
2,000	241	243	245	247	249
3,000	246	249	252	254	257
5,000	251	256	261	266	271
10,000	386	396	405	415	425
30,000	614	643	672	701	730

注※1　想定環境に従って、1 日当たりに発生するデータ量に変化がなく、毎日継続してデータが蓄積された場合を想定した値です。

注※2　操作ログの保管期間です。1 年当たり 240 日分（20 営業日/月）のデータ量として計算しています。

推奨ディスク容量を算出する際の想定環境を次の表に示します。

項目	想定環境
機器	• 部署や設置場所などのグループが 100 種類作成されている。 • 除外対象の機器は、管理対象の機器の 15%の台数がある。 • 管理対象の機器 1 台当たり、インストールされているソフトウェア（インストールソフトウェア）が 300 個ある。 • 管理対象の機器 1 台当たり、適用されている更新プログラムが 300 個ある。 • 管理対象の機器 1 台当たり、適用されていない更新プログラムが 100 個ある。
操作ログ	• 情報漏えいに係わりの深い操作だけを取得対象にする場合、操作ログは 1 台当たり 120 件取得される。 • すべての操作を取得対象にする場合、操作ログは 1 台当たり 2,000 件取得される。 • ［自動取り込みされる操作ログの格納期間］に、30 日が指定されている。 • 200 台のコンピュータ 3 か月分（20 営業日/月）の操作ログが手動取り込みされている。ただし、管理対象のコンピュータが 100 台の場合は、100 台分の操作ログが手動取り込みされている。 • 操作ログの定期エクスポートは実施していない。 • セットアップの［キャッシュへの追加容量］には、コンピュータ 2,500 台あたり、1 ギガバイトを設定している。
資産	• ハードウェア資産情報（USB デバイスを除く）は、管理対象の機器の台数の 2 倍の件数が登録されている。 • ハードウェア資産情報（USB デバイス）は、100 件登録されている。 • 管理ソフトウェア情報は、500 件登録されている。 • ソフトウェアライセンス情報は、100 件登録されている。 • 契約情報は、100 件登録されている。 なお、各資産情報には、サイズの大きいファイルが多数登録されていないことを仮定しています。サイズの大きいファイルを多数登録して管理する場合は、上の 2 つの表に記載した値とは別に十分な容量を確保してください。
変更履歴	保存用の変更履歴を定期的に出力しない。
配布	パッケージは、10 ギガバイト分が登録されている。
イベント	管理対象の機器 1 台当たり、1 日に 250 件発生する。

関連リンク

- 付録 A.6　性能と見積もり

4.5.9　エージェントの接続先が電源 OFF の場合の操作ログの取得

操作ログの保管先となる管理用サーバの電源が OFF の場合、利用者がエージェント導入済みのコンピュータ上で操作すると、操作ログがコンピュータに一時保存されます。

その後、管理用サーバの電源を ON にすると、コンピュータに一時保存された操作ログが、管理用サーバにアップロードされます。

重要

操作ログは、セキュリティポリシーの［禁止操作と操作ログの共通設定］－［禁止操作／操作ログの、利用者のコンピュータでの保持期間］で設定した日数だけ、コンピュータに一時保存できます。設定した期間を超過すると、古い操作ログから順に削除されます。このため、古い操作ログが削除される前に接続先の電源を ON にすることをお勧めします。

ヒント

定期的に操作ログを取得するタイミングで、エージェント導入済みのコンピュータに保存されている操作ログが管理用サーバにまとめてアップロードされます。

なお、管理用サーバの電源を長期間 OFF にしないでください。

4.6　運用前の検討

システムを運用する前に、誰に対してユーザーアカウントを与えるか、どの機器を管理対象にするか、管理対象の機器をどのようにグループ分けするかなど、運用時に設定が必要となる内容を検討しておきます。

4.6.1　ユーザーアカウントの検討

JP1/IT Desktop Management 2 の利用者について検討します。ここでは、誰のユーザーアカウントを作成するか、また、作成したユーザーアカウントにどのような権限を与えるかを検討してください。

管理者の用途に合わせてユーザーアカウントに適した権限を設定できます。設定する権限を用途別に次に示します。

- JP1/IT Desktop Management 2 を利用して各種管理業務をしたい場合
  システム管理権限を設定します。
- JP1/IT Desktop Management 2 のユーザーアカウントを追加したり、編集したりしたい場合
  ユーザーアカウント管理権限を設定します。
- 管理している情報を参照したい場合
  権限の設定は不要です（デフォルトで参照権限が設定されます）。
- 管理者の担当業務に応じて JP1/IT Desktop Management 2 の操作範囲を限定したい場合
  業務分掌を設定します。業務分掌には、セキュリティ管理、資産管理、機器管理、配布管理、およびシステム設定管理の 5 種類があります。

また、ユーザーアカウントには権限だけでなく、管轄範囲を設定できます。ユーザーアカウントに管轄範囲を設定すると、管轄範囲の情報だけを管理できます。管轄範囲外の情報を変更させたくない場合や管轄ごとに管理を分担する場合に管轄範囲を設定します。このようにして、複数の管理者で作業分担すると、組織全体の機器、ハードウェア資産などの管理が行き届くようになります。

> **ヒント**
>
> 複数のユーザーアカウントを作成し、利用者の作業内容に応じて権限を設定することで、複数人の管理者での作業の分担や、内部統制を意識した運用ができます。

関連リンク

- 2.3.3　ユーザーアカウントの権限
- 2.3.5　ユーザーアカウントの業務分掌
- 2.3.6　ユーザーアカウントの業務分掌ごとの操作範囲
- 2.3.7　ユーザーアカウントの管轄範囲
- 2.3.8　管轄範囲が限定されている場合の操作画面の差異

4.6.2　内部統制を意識したユーザーアカウントの作成

内部統制を意識する場合、JP1/IT Desktop Management 2 の利用者の用途別に、利用できる機能を限定してユーザーアカウントを登録する必要があります。内部統制を意識して運用する場合の管理体制の例を次の表に示します。

管理体制	役割
システムオーナー	組織内のシステムの利用状況を統括して管理します。JP1/IT Desktop Management 2 の利用許可を承認しますが、JP1/IT Desktop Management 2 は利用しません。
ユーザーアカウント管理者	JP1/IT Desktop Management 2 の利用者を管理します。ユーザーアカウント管理権限を持っています。
システム管理者	JP1/IT Desktop Management 2 を利用して、各種管理業務を実施します。システム管理権限を持っています。
経営者	管理している情報を参照して、組織の運営状況を確認します。参照権限を持っています。

この例に示す体制では、最初から JP1/IT Desktop Management 2 を使用できるのはユーザーアカウント管理者だけです。システム管理者と経営者が JP1/IT Desktop Management 2 を利用するためには、システムオーナーに利用申請をする必要があります。システムオーナーによって利用申請が承認されたら、ユーザーアカウント管理者が必要な権限を設定したユーザーアカウントを登録します。

ユーザーアカウントを登録する際の基本的な流れは次のとおりです。この流れでユーザーアカウントを登録することで、ユーザーの業務に則してシステムを運用できているかを客観的に判断できます。

1. JP1/IT Desktop Management 2 を利用したいユーザーが、システムオーナーに利用申請をする。

   JP1/IT Desktop Management 2 で管理業務を実施したいシステム管理者や、管理している情報を参照したい経営者は、システムオーナーに利用申請をします。

2. システムオーナーが利用を承認する。

3. システムオーナーがユーザーアカウント管理者にユーザーアカウントの作成を依頼する。

4. ユーザーアカウント管理者が、ユーザーアカウントを作成する。

   システム管理者にはシステム管理権限を設定します。また、経営者は参照だけできるように、権限は特に設定しません。

5. ユーザーアカウント管理者が、ユーザーアカウントの作成結果をシステムオーナーに報告する。

6. ユーザーアカウント管理者が、ユーザーアカウントを利用者に連絡する。

   システム管理者および経営者は、機能を限定された状態で JP1/IT Desktop Management 2 を利用できるようになります。

7. 定期監査でユーザーアカウントの登録状況をチェックする。

申請の証跡とユーザーアカウントの登録状況からシステムが正しく運用されているかを監査します。

4.6.3 管理対象の検討

JP1/IT Desktop Management 2 では、機器管理、セキュリティ管理、および資産管理ができます。目的とする管理方法によって、対象にできる機器の範囲が異なります。運用を始める前に、組織内のどの機器を管理するかを検討しておきます。

また、ネットワークに接続できるコンピュータはオンライン管理で、接続できないコンピュータはオフライン管理で管理します。オンライン管理とオフライン管理での機能差異については、「(1) 管理形態による機能差異」を参照してください。

機器管理の対象とする機器

機器管理では、ネットワークに接続された機器から情報を収集して、機器の状態や各種情報を把握できます。組織内の現状を把握したい機器を検討します。

OS を持つコンピュータやネットワークプリンタやルータなどの IP アドレスを持つ機器を機器管理の対象にできます。機器管理するためには、機器を JP1/IT Desktop Management 2 の管理対象として登録する必要があります。機器を管理対象にすると、1 台につき 1 ライセンスを使用します。

IP アドレスを持つ機器であれば、ネットワークを探索して情報を自動収集できます。このため、部署内の機器が不明の場合でも、JP1/IT Desktop Management 2 を使用して組織内の機器の情報を収集し、管理対象にできます。なお、オフライン状態のコンピュータなどの IP アドレスを持たない機器は、オフライン管理とするか、資産として管理します。

マウスやキーボードなどのコンピュータに付帯する周辺機器は、追加機器情報として入力することで、機器情報の一部として管理できます。このため、周辺機器の管理にはライセンスは使いません。

組織内の機器のうち JP1/IT Desktop Management 2 で管理したくない機器は、除外対象に登録します。例えば、セキュリティ管理する機器以外は管理しない場合、ネットワークプリンタやルータなどの機器を除外対象として登録します。このようにすることで、管理対象の機器だけから情報を収集できます。

機器管理の対象は次のように判断します。

- 情報を収集して管理する機器

  管理対象にします。1 台につき 1 ライセンスを使用します。
- 管理しない機器

  除外対象にします。ライセンスは使用しません。

セキュリティ管理の対象とする機器

セキュリティ管理では、管理対象の機器から収集した情報を基に、機器のセキュリティ状況を把握し対策できます。セキュリティ状況を安全に保ちたい機器を検討します。

セキュリティ管理の対象になるのは、OS が Windows の管理対象のコンピュータだけです。

コンピュータにエージェントを導入することで、セキュリティ状況の判定や診断、対策を実行できます。

エージェントレスのコンピュータもセキュリティ管理の対象にできます。エージェントレスのコンピュータをセキュリティ管理の対象にする場合は、管理共有が有効かつ Administrator 権限でログオン認証できる必要があります。ただし、エージェントレスのコンピュータでは、セキュリティ状況の判定、診断はできますが、取得できる機器情報の範囲内での判定と診断になります。一部の情報については、判定と診断は実施できません。また、自動対策機能やソフトウェアの起動抑止機能が使用できないなど、一部の機能に制限があります。

セキュリティ管理の対象は次のように判断します。

- セキュリティ対策も自動的に実施したい
  エージェント導入済みのコンピュータが対象となります。
- セキュリティ状況の判定、診断までできればよい
  OS が Windows の管理対象のコンピュータが対象となります。エージェントレスのコンピュータの場合、一部制限があります。

資産管理の対象とする機器

資産管理では、組織内で所有する機器（ハードウェア資産）の状態を管理できます。ネットワーク接続の有無は関係ありません。組織内の資産として管理したい機器を検討します。なお、ハードウェア資産の管理にライセンスは使用しません。

資産管理の対象になるのは、組織内で所有しているすべての機器です。資産情報は、任意に登録できるため IP アドレスを持たない機器や周辺機器も管理できます。

組織内で所有している機器のうち、資産番号を付与してハードウェア資産として管理したい機器を登録します。ハードウェア資産として登録することで、資産番号以外に、運用中や在庫などの資産の状態や、利用者名や連絡先、関連する契約情報なども管理できるようになります。

JP1/IT Desktop Management 2 の管理対象にした機器は、自動的にハードウェア資産情報が登録されます。管理対象にしない機器を資産として管理する場合は、手動で登録する必要があります。

(1) オンライン管理のコンピュータの機器情報を管理するための検討

日々増減する組織内の機器情報を正確に管理するためには、定期的に探索を実行して、管理対象とする機器をすべて登録する必要があります。また、管理している機器情報は最新に保つ必要があります。

機器情報を管理するためには、探索の範囲やスケジュール、探索で発見したコンピュータにエージェントを配信するかどうかなどを検討します。また、コンピュータの機器情報を収集および更新するための運用スケジュールを検討します。

機器の探索の検討

機器の探索について次の内容を検討します。

- 探索範囲

  機器の探索範囲を検討します。設定時には探索の対象となる IP アドレスを指定するため、探索対象となる機器の IP アドレスの範囲を検討してください。

  探索範囲は複数設定できます。組織内で使用している IP アドレスの範囲だけを設定することをお勧めします。設定した範囲内のすべての IP アドレスに接続を試みるので、使用していない IP アドレスを探索範囲に含めると、探索完了までに時間が掛かってしまいます。

- 探索スケジュール

  機器の探索をいつ実施するかを検討します。定期的に機器の探索を実施する場合は、探索の開始時刻、実施する日などを検討してください。例えば、毎月第 1 月曜日の 8:00 に探索するなどのように、曜日や時間を指定してスケジュールを設定できます。

  なお、電源の入っていない機器は探索で発見できません。このため、JP1/IT Desktop Management 2 を導入して最初の 1 週間程度は、繰り返し探索を実行するように設定して、発見漏れのないようにします。一とおりの機器が登録できたら、組織への機器導入の頻度に合わせて、探索スケジュールを設定します。

- 認証情報の設定と割り当て

  探索時に機器の種別や OS などの情報を収集したい場合は、探索時に使用する認証情報を登録する必要があります。探索時には、SNMP および Windows の管理共有の 2 種類の認証情報を使用します。

  SNMP の認証情報

  SNMP を利用して機器に接続するためのコミュニティ名を登録します。

  ネットワークにコミュニティ名を設定していない場合、コミュニティ名は「public」となります。デフォルトでは「public」が設定された認証情報が登録されているため、コミュニティ名を設定していない場合は、SNMP の認証情報は登録不要です。

  Windows の管理共有の認証情報

  Windows の管理共有にアクセスするための ID とパスワードを登録します。

  登録した認証情報は、探索範囲ごとに使用する情報を設定できます。各探索範囲でコンピュータの認証情報が異なる場合は、必要な認証情報を登録し、探索範囲ごとに設定する必要があります。

  なお、認証情報を登録しない場合、探索時には機器情報を収集できません。機器の存在確認だけできます。

- 発見した機器への操作

  機器の探索を実行して、新しい機器を発見したときのアクションについて検討します。実施できるアクションは次のとおりです。

  - 発見した機器を自動的に管理対象にする

    探索で発見された機器のうち、OS が Windows と認識されたコンピュータが自動的に管理対象になります。

  - 発見した機器に自動的にエージェントを配信する

    エージェントがインストールされると、そのコンピュータが自動的に管理対象となり、セキュリティ管理の対象となります。

なお、エージェントをコンピュータに配信する場合は、Windows の管理共有の認証情報の登録および割り当てが必要です。

機器情報の収集・更新間隔の検討

運用時に、機器情報をどのように収集し、更新するかを検討します。機器情報の更新方法は、管理対象のコンピュータにエージェントを導入するかどうかによって異なります。

- エージェントを導入済みのコンピュータの場合

  エージェントがコンピュータの情報を収集し、定期的に管理用サーバに通知します。これによって、管理用サーバが保持しているコンピュータの情報を最新情報に自動で更新できます。

  また、定期的に自動収集するほかに、コンピュータの情報を任意のタイミングで収集することもできます。

- エージェントレスのコンピュータの場合

  エージェントレスのコンピュータからは、自動的に管理用サーバに情報を通知できません。このため、エージェントレスのコンピュータの機器情報は、定期的に収集・更新されるように設定されています。デフォルトでは、1 時間間隔で情報が収集されるように設定されています。

  エージェントレスのコンピュータの台数が多く、情報収集によってネットワークに負荷が掛かってしまうような場合は、環境に合わせて適切な収集間隔を検討します。

なお、エージェントを導入しているコンピュータの方が、エージェントレスのコンピュータに比べて詳細な情報を収集・管理できます。機器情報をどのように更新するかとあわせて、コンピュータへのエージェントの導入も検討してください。

(2) オンライン管理のコンピュータのセキュリティ対策を実施するための検討

組織のセキュリティのルールに従って、どのようにセキュリティポリシーを設定するかを検討します。また、設定したセキュリティポリシーによる判定スケジュールや、セキュリティの診断結果として作成されるレポートの集計対象、保存期間などを検討します。

セキュリティポリシーの検討

管理対象のコンピュータには、デフォルトで「デフォルトポリシー」が適用されます。組織内のルールが 1 種類の場合、デフォルトポリシーを編集することで、すべてのコンピュータに対してセキュリティポリシーの設定内容を一括して変更できます。一部のコンピュータに特別なセキュリティポリシーが必要な場合、メインで使用するセキュリティポリシーはデフォルトポリシーを利用し、特別なセキュリティポリシーを新規に作成します。

また、セキュリティポリシーの内容（セキュリティ設定項目とアクション項目）についても検討しておきます。

セキュリティ判定項目および自動対策の検討

組織のルールに基づいて、セキュリティポリシーにどの判定項目を設定するかを検討します。また、違反している内容を自動的に対策する項目も検討しておきます。

セキュリティポリシーに違反している場合のアクション項目の検討

セキュリティポリシーに違反している場合、どのようなアクションを実行するかについて検討します。次に示すアクションを実行できます。

- セキュリティポリシーに違反していることを利用者に通知する。
- セキュリティ上問題があるコンピュータのネットワーク接続を拒否する。

セキュリティ判定のスケジュールの検討

設定したセキュリティポリシーに従って、定期的にセキュリティ状況が判定されます。運用に応じて、設定画面で判定タイミングを設定してください。

セキュリティ診断レポートの集計についての検討

セキュリティ状況の判定結果をセキュリティ診断レポートとして集計できます。セキュリティ診断レポートを表示するために、レポートの集計期間、および保存期間などを検討してください。

- 集計期間

  セキュリティ診断レポートは、現在の状況のほかに期間ごとの状況を確認できます。指定できる期間は週、月、四半期、半期、および年度です。組織の運用に合わせて、設定画面で各集計期間の起点となる日を設定できます。

- 保存期間

  集計したセキュリティ診断レポートをどのくらいの期間で保存しておくかを検討します。1 年から 10 年まで保存期間を設定できます。

(3) 資産情報を管理するための検討

組織内で所有している各種資産を管理できます。資産情報ごとに、管理する対象を検討します。

ハードウェア資産

コンピュータ、サーバ、プリンタ、ネットワーク装置、USB デバイスなど、所有している機器の情報をハードウェア資産情報として管理できます。各資産の詳細情報を管理できるだけでなく、運用中、在庫、滅却済みなどのステータスも管理でき、組織内のハードウェア資産の状況を把握できます。

組織内で所有しているハードウェア資産のうち、JP1/IT Desktop Management 2 で管理する資産を検討してください。また、各資産の情報を準備してください。

> **ヒント**
>
> 手もとに資産台帳がある場合は、台帳をインポートして資産情報を登録できます。
>
> JP1/IT Desktop Management 2 では、機器の情報を BIOS シリアルナンバーで関連づけて管理します。複数の機器の BIOS シリアルナンバーが同一である場合は、機器の情報が正しく関連づけられなくなります。機器の情報の関連づけを BIOS シリアルナンバー以外に変更する方法については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」の機器情報の関連づけを変更する手順の説明を参照してください。

ソフトウェアライセンス

所有しているソフトウェアライセンスの情報を管理できます。ソフトウェアライセンスごとに、利用を許可するコンピュータも管理できます。

ソフトウェアライセンスを管理するかどうか検討する際は、ソフトウェア種別を判断基準にできます。例えば、ソフトウェア種別が「有償ソフトウェア」のソフトウェアライセンスだけを管理することもできます。

ソフトウェアライセンスを管理する場合、ソフトウェアライセンスの証書の情報を登録します。組織内で所有しているソフトウェアライセンスの証書を準備してください。

管理ソフトウェア

ソフトウェアライセンスに対応するソフトウェアを登録して、ソフトウェアごとのライセンスの利用状況を管理できます。ライセンスの総数管理だけでなく、個々のコンピュータにライセンスを割り当てて、許可なくライセンスを利用しているコンピュータを確認することもできます。

事前に、実際に利用されているソフトウェアが、どのソフトウェアライセンスに対応しているかを把握しておきます。

契約

サポート契約やレンタル契約、リース契約など、ハードウェア資産やソフトウェアライセンスに関する契約情報を登録して、それぞれの資産情報と対応づけて管理できます。満了日が近づいている契約情報を把握できるので、今後の作業計画を予定することもできます。

契約情報を管理する場合は、契約書の情報を登録します。組織内で所有している、ハードウェア資産やソフトウェアライセンスに関する契約書を準備してください。

管理項目の検討

追加管理項目としてオリジナルの管理項目を作成できます。また、既存の管理項目に対しても、選択肢を追加できます。組織内で独自に管理したい情報がある場合は、あらかじめどのような管理項目を作成するかを検討しておきます。

ヒント

資産情報をインポートして登録する場合、インポートするデータに含まれる管理項目をあらかじめ確認してください。JP1/IT Desktop Management 2 にない項目を管理する場合は、インポートする前に管理項目を作成する必要があります。

4.6.4 グループの検討

管理対象の機器やハードウェア資産情報をグループに分けて管理できます。どのようなグループに分けて管理するか、およびどのようにグループを作成するかを検討します。

グループを設定しておくと、次の内容をグループ単位に設定できます。

- セキュリティポリシーの割り当て（管理用中継サーバのホスト名のグループを除く）

- 配布を実行するコンピュータの設定
- レポートの集計範囲（ユーザー定義のグループを除く）
- エージェント設定の割り当て（ユーザー定義のグループおよび管理用中継サーバのホスト名のグループを除く）

グループの種類と管理方法を次の表に示します。

種類	管理方法
機器種別	コンピュータから収集した「OS」の情報を基に自動でグルーピングされます。コンピュータ以外の機器は、「機器種別」の情報を基に自動でグルーピングされます。
ネットワーク	コンピュータから収集した「IP アドレス」の情報を基に、ネットワークセグメント単位で自動でグルーピングされます。
部署 設置場所	コンピュータから収集した利用者情報の「部署」および「設置場所」を基に自動でグルーピングされます。複数サーバ構成の場合に、上位の管理用サーバから資産管理項目の設定を適用されたタイミングでも自動でグルーピングされます。管理者が手動でグルーピングすることもできます。Active Directory と連携する場合は、Active Directory で管理している部署情報をそのままグループ構成に反映できます。
ユーザー定義	システム管理者が設定した条件を基に、自動で振り分けられます。
管理用中継サーバのホスト名	複数サーバ構成の場合に、配下の管理用中継サーバから収集した「ホスト名」を基に自動でグルーピングされます。グループ名と同名の管理用中継サーバに定義されているネットワークセグメントのグループがグルーピングされます。

ここでは、次の内容を検討します。

1. グループの種類の検討

   次のような場合は、ユーザー定義のグループで管理してください。ユーザー定義のグループで管理する場合は、グループの構成を検討してください。

   - 追加管理項目の値を振り分け条件にして、グループを管理したい場合
   - 追加管理項目の値とシステム分類のグループ（機器種別、ネットワーク、部署、設置場所）を振り分け条件にして、グループを管理したい場合

   部署および設置場所のグループで管理する場合は、デフォルトでは自動でグループが作成されないため、グループの構成を検討してください。

   機器種別およびネットワークのグループで管理する場合は、収集した情報を基に自動でグループが作成されるため、グループの構成の検討は不要です。

2. グループの構成の検討

   ユーザー定義のグループは、どのような条件で機器を振り分けるかを検討してください。

   部署および設置場所のグループは、ツリー構造で管理できます。どのような構造でグループを作成するか、組織内の部署の構成または機器の設置場所とあわせて検討してください。また、Active Directory と連携している場合は、Active Directory で管理しているグループ構成を部署情報として取り込むかどうかを検討してください。

3. グループの作成方法の検討

ユーザー定義のグループは、システム管理者がグループの作成とグループへの振り分け条件の設定をします。ユーザー定義のグループの作成方法については、「(20)　グループの作成方法」、ユーザー定義のグループの仕組みについては「(22)　ユーザー定義のグループの仕組み」を参照してください。

部署および設置場所のグループには、次の 2 種類の作成方法があります。

機器情報の収集によるグループの作成

コンピュータから収集した利用者情報の値を基に、グループを作成します。コンピュータから利用者情報を収集するには、あらかじめ管理用サーバの設定画面で部署および設置場所の構成を設定しておく必要があります。なお、利用者情報を収集できるのは、エージェント導入済みのコンピュータからだけです。

Active Directory で管理しているグループ構成を部署情報として反映する場合は、設定画面で Active Directory との連携を設定する際に、グループ構成を取り込む設定を有効にしてください。

また、コンピュータから収集したレジストリ情報から自動でグループを生成し、コンピュータをグルーピングすることもできます。

管理者によるグループの作成

管理用サーバの設定画面で部署および設置場所の構成を設定して、各コンピュータを手動でグループに登録できます。

ヒント

初期構築時は、機器情報の収集によって自動的にグルーピングする方法をお勧めします。手動での設定は、初期構築時ではなく、すでに作成されたグループ構成を修正する場合などに実施します。

4.6.5　複数サーバ構成で管理するための検討

複数サーバ構成で JP1/IT Desktop Management 2 を運用する場合の検討事項を示します。

階層構成の検討

管理したいシステムの部門やネットワーク構成を考慮して、複数サーバ構成の階層構成について次に示す事項を検討してください。

- 設置する管理用中継サーバの台数
- 各管理用中継サーバの接続先
- 各管理用サーバが管理するコンピュータの範囲
- 中継システムの有無

なお、NAT 環境で JP1/IT Desktop Management 2 のシステムを運用する場合は、NAT 機器の配下に管理用中継サーバを設置する必要があります。

複数サーバ構成の詳細については、「4.4.3　複数サーバ構成」を参照してください。

各管理用サーバのライセンス保有方法およびライセンスの共有範囲の検討

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、各管理用サーバのライセンス保有方法およびライセンスの共有範囲を検討してください。各管理用サーバで管理できる機器の台数を制限したい場合は、統括管理用サーバの製品ライセンスを各管理用中継サーバに分配します。統括管理用サーバとは異なる契約で購入した製品ライセンスを管理用中継サーバに登録したい場合は、管理用中継サーバに製品ライセンスの登録を許可します。

複数サーバ構成での製品ライセンスの管理については、「3.3　複数サーバ構成での製品ライセンスの管理」を参照してください。

操作ログを管理する管理用サーバの検討

複数サーバ構成でのシステム運用に合うように、操作ログを取得する管理用サーバおよび操作ログを保存する管理用サーバを検討してください。また、各管理用サーバで取得した操作ログを上位の管理用サーバに通知するかを検討してください。

複数サーバ構成での操作ログの管理については、「2.18.11　複数サーバ構成での操作ログの管理」を参照してください。

変更履歴を管理する管理用サーバの検討

複数サーバ構成内のどの管理用サーバで機器の変更履歴を管理するか検討してください。また、それに基づいて、各管理用サーバで自サーバ直下の機器以外の変更履歴を取得するか検討してください。NAT 環境で管理者のいない管理用サーバを運用している場合や、各管理用サーバの負荷を分散したい場合などは、自サーバ直下の機器以外の変更履歴を取得しない設定にすることをお勧めします。

複数サーバ構成での変更履歴の管理については、「(6)　配下の管理用中継サーバが管理対象とする機器の変更履歴の取得」を参照してください。

資産情報を管理する管理用サーバの検討

複数サーバ構成内のどの管理用サーバで資産情報を管理するか検討してください。

複数サーバ構成での資産情報の管理については、「2.18.12　複数サーバ構成での資産の管理」を参照してください。

4.6.6　ネットワークを監視するための検討

未確認の機器の持ち込みによる情報漏えいやウィルス被害を防止するためには、ネットワークモニタ機能を利用してネットワークを監視し、組織内のネットワークに未確認の機器を接続させないようにします。

ネットワークを監視するためには、ネットワークの監視方法や監視対象となるネットワーク、ネットワーク接続を許可する機器などを検討します。

ネットワークの監視方法の検討

ネットワークの監視方法には、次の 2 とおりがあります。どちらの監視方法にするか、あらかじめ検討しておきます。

ブラックリスト方式

ネットワーク接続を許可しない機器を指定する方式です。登録した機器のネットワーク接続を遮断できます。それ以外の機器はネットワーク接続できます。ふだんはネットワーク接続を許可しておき、不明な機器が発見された場合にネットワーク接続を許可しないようにするときは、この方法で運用してください。

ブラックリスト方式の場合、ネットワーク制御リストの自動更新の設定は、すべての自動更新を有効にすることをお勧めします。すべての自動更新を有効にすると、ネットワーク制御リストに不要な情報が残りません。一方、自動更新のうち追加だけを有効にすると、ネットワーク制御リストに不要な情報が残るため、管理者が手動でネットワーク制御リストをメンテナンスする必要があります。

自動更新を設定する方法については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のネットワーク制御リストの自動更新の設定を編集する手順の説明を参照してください。

ホワイトリスト方式

あらかじめネットワーク接続を許可する機器を指定する方式です。登録した機器はネットワーク接続できます。それ以外の機器がネットワーク接続した場合、自動的に遮断されます。機器のネットワーク接続で強固なセキュリティを確保したい場合は、この方法で運用してください。

ホワイトリスト方式の場合、ネットワーク制御リストの自動更新の設定について、すべての自動更新を有効にすると、NIC（無線 LAN カードを含む）の使い回しを自動で防止できます。ただし、自動更新の設定をしたタイミングによっては機器のネットワーク接続が遮断されることがあります。また、自動更新のうち追加だけを有効にすると、管理者がネットワーク制御リストをメンテナンスすることで、NIC の使い回しを防止できます。

自動更新を設定する方法については、マニュアル「JP1/IT Desktop Management 2 運用ガイド」のネットワーク制御リストの自動更新の設定を編集する手順の説明を参照してください。

ヒント

監視方法は、ネットワークセグメントごとに設定できます。

監視するネットワークセグメントの検討

ネットワークモニタ機能はネットワークセグメントごとに導入します。このため、組織内のどのネットワークセグメントを監視するかを検討します。

ネットワークを監視するためには、対象となるネットワークセグメント内にネットワークモニタを有効にしたコンピュータを設置する必要があります。複数のネットワークカードを使って複数のネットワークに接続できるコンピュータであれば、ネットワークモニタを有効にしたコンピュータ 1 台で、複数のネットワークセグメントを監視できます。また、ネットワークの監視は、ネットワークモニタ機能が動作している間だけ有効になります。このため、ネットワークモニタを有効にするコンピュータには、24 時間稼働していて、エージェントを導入できるコンピュータを選定してください。

ネットワーク接続の制御対象とする機器の検討

ネットワークの監視方法によって、検討する機器が異なります。

ブラックリスト方式の場合

ネットワーク接続を許可しない機器を検討しておきます。手動で登録するために、IP アドレスと MAC アドレスを確認しておきます。

ホワイトリスト方式の場合

ネットワーク探索機能やエージェントの導入などによって、ネットワーク接続を許可する機器をすべて発見しておきます。なお、ネットワークモニタを有効にすると、そのネットワークセグメントに存在する機器は自動的に発見されます。

ヒント

ネットワーク接続の制御対象となる機器は、次の方法で登録します。

- ネットワーク探索機能やネットワークモニタ機能を利用して発見する（自動登録される）
- エージェント導入済みのコンピュータが接続する（自動登録される）
- 管理者が手動で登録する

ヒント

ホワイトリスト方式で運用するためには、ネットワーク接続を許可する機器をすべて抽出する必要があるため、運用初期は難易度が高くなります。運用初期はブラックリスト方式でネットワークを監視しておき、しばらく運用して機器をすべて抽出できたらホワイトリスト方式に変更するといったこともできます。

ヒント

ネットワークモニタ機能を使用する場合、ネットワーク接続を許可するすべてのコンピュータを管理対象にしてください。コンピュータ以外の機器は、管理対象にしなくてもかまいません。

検疫通信の検討

ネットワーク接続が遮断されている機器が、例外的に通信できる機器を設定できます。組織の運用方法に応じて、対象の機器を検討してください。

例えば、セキュリティ対策用のサーバを設定します。これによって、セキュリティ対策が不十分で自動的に遮断されたコンピュータは、管理用サーバおよびセキュリティ対策用のサーバだけと接続できます。コンピュータは、セキュリティ対策用のサーバから対策ツールを実行して対策し、セキュリティ状況が安全になったら自動的にネットワーク接続できるようになるといった運用を実現できます。

4.6.7　定期メンテナンスを検討する流れ

運用時には次に示すメンテナンスを実施することをお勧めします。どのようなタイミングで実施するか検討しておきます。

- 運用データのバックアップ

  データベース、各種データファイルなどの運用データをバックアップしてください。ディスク障害が発生した場合などには、管理用サーバの情報が消えてしまったり、管理用サーバが動作しなくなったりするおそれがあります。

  このため、運用時には定期的にバックアップを取得してください。管理用サーバに障害が発生した場合は、取得したバックアップを使用してバックアップ時点の状態にリストアできます。

- データベースの再編成

  データベースの長期間の運用によって、領域の断片化や格納効率の低下、アクセス速度の低下などの問題が発生するおそれがあります。これらを防止するため、データベースを再編成する機能を提供しています。データベースの再編成を実施することでデータの内容を保持したまま格納編成を変更できるので、パフォーマンスの効率化が図れます。

  データベースの再編成は、目安として、データベース使用率が 80%になる前に実施してください。

運用データのバックアップおよびデータベースの再編成を、いつ、どのくらいの間隔で実施するかを検討します。バックアップおよびデータベースの再編成をするためには、管理用サーバを停止する必要があります。このため、スケジュールを組む際には、管理用サーバを使用しない曜日、時間などを考慮してください。

> **ヒント**
>
> バックアップやデータベースの再編成は定期的に実施することをお勧めします。

管理用サーバのメンテナンスをするには次の方法があります。

- 任意のタイミングで実施する

  任意のタイミングで実施するには、データベースマネージャまたはコマンドを使用して手動で実行します。

- 定期的に実施する

  Windows のタスクにコマンドを登録し、スケジュールを設定して自動的に実施します。

データベースマネージャを利用してメンテナンスするには：

1. 管理用サーバの［スタート］メニューからデータベースマネージャを起動します。
2. 表示されるダイアログで、実行するメニューを選択します。
3. データベースマネージャの画面に従ってメンテナンスを実行します。

メンテナンスが完了します。

コマンドを利用してメンテナンスするには：

1. stopservice コマンドで管理用サーバを停止します。
2. メンテナンスを実施します。
   - 運用データをバックアップする場合
     exportdb コマンドでバックアップを取得します。
   - データベースを再編成する場合
     reorgdb コマンドでデータベースを再編成します。
3. startservice コマンドで管理用サーバを開始します。

メンテナンスが完了します。

> **重要**
>
> 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がクラスタ構成の場合は、クラスタソフトの機能を使用して管理用サーバのクラスタリソースを開始したり、停止したりします。

管理用サーバがクラスタ構成でない場合、コマンドを利用してメンテナンスする際のexportdb コマンドまたはreorgdb コマンドのオプションに-a を指定してメンテナンスする方法もあります。 その場合、手順 2 だけを実施してください。手順 1 と手順 3 は自動的に実行されます。

> **ヒント**
>
> 管理用サーバに障害が発生したときは、importdb コマンドの引数に取得したバックアップデータを指定するとリストアできます。バックアップ、リストア、およびデータベースの再編成は、データベースマネージャでも操作できます。

4.6.8 ウィルス対策製品と同居時の注意事項

JP1/IT Desktop Management 2 とウィルス対策製品が同居する場合は、次のファイルおよびフォルダをウィルスチェックの対象から外してください。

JP1/IT Desktop Management 2 の停止中にウィルスチェックを実施してから JP1/IT Desktop Management 2 を再起動する場合は、次のファイルおよびフォルダに対してウィルスチェックが完了したことを確認してください。

JP1/IT Desktop Management 2 - Manager の次のファイルおよびフォルダ

- *JP1/IT Desktop Management 2 - Manager のインストールパス*以下すべて
- セットアップで定義したデータベースフォルダ、データフォルダおよびローカルデータフォルダ

- セットアップで定義した操作ログ用データベースフォルダ
- セットアップで定義した操作ログ自動保管先フォルダ
- 操作ログや資産情報などをエクスポートするときの出力先フォルダ

JP1/IT Desktop Management 2 - Agent の次のファイルおよびフォルダ

Windows の場合

- *JP1/IT Desktop Management 2 - Agent のインストールパス*以下すべて
- *JP1/IT Desktop Management 2 - Agent のインストール先システムドライブ*¥JP1ITDMWK¥以下すべて
- %WINDIR%¥JP1ITDM¥UtilMsg.dll
- %WINDIR%¥jdnagent.nid
- %ALLUSERSPROFILE%¥Application Data¥Hitachi¥jp1itdma¥以下すべて
- %ALLUSERSPROFILE%¥Application Data¥Hitachi¥jp1itdmrca¥以下すべて
- %USERPROFILE%¥Application Data¥Hitachi¥jp1itdma¥以下すべて
- %USERPROFILE%¥Application Data¥Hitachi¥jp1itdmrca¥以下すべて
- %SystemRoot%¥jdngshare.dll
- %SystemRoot%¥jdngsrv.exe
- *JP1/IT Desktop Management 2 - Network Monitor のインストールパス*以下すべて

HP-UX の場合※

- /etc/opt/NETMDMW/ 以下すべて
- /opt/NETMDMGF/ 以下すべて
- /opt/NETMDMW/ 以下すべて
- /opt/NETMDMWEX1/ 以下すべて
- /var/opt/NETMDMW/ 以下すべて
- /NETMDMGF/ 以下すべて

AIX および Solaris の場合※

- /opt/NETMRDS/ 以下すべて
- /opt/NETMRDSEX1/ 以下すべて
- /opt/NETMDMGF/ 以下すべて

Linux の場合※

- /opt/NETMDMGF/ 以下すべて
- /opt/NETMDMW/ 以下すべて

- /opt/NETMDMWEX1/ 以下すべて

Mac OS の場合※

/Library/Application Support/jp.co.hitachi.jp1itdm2/ 以下すべて

注※　マニュアル「JP1/IT Desktop Management 2 - Agent(UNIX(R)用)」の作業用ディレクトリの変更手順に従って作業用ディレクトリを変更している場合は、変更後の作業用ディレクトリもウィルスチェックの対象から外してください。

JP1/IT Desktop Management 2 - Internet Gateway の次のファイルおよびフォルダ

- JP1/IT Desktop Management 2 - Internet Gateway のインストール先フォルダ以下すべて

ウィルスチェックの対象から外すフォルダの詳細は、次のマニュアルを参照してください。

- 「付録 A.1　フォルダ一覧」および「付録 A.2　サービス、プロセス一覧」
- マニュアル「JP1/IT Desktop Management 2 - Asset Console 構築・運用ガイド」のフォルダ構成
- マニュアル「JP1/IT Desktop Management 2 - Agent(UNIX(R)用)」の JP1/IT Desktop Management 2 - Agent のファイル構造

重要

ファイルやフォルダをウィルスチェックの対象から外さない場合、ウイルス対策製品の影響で、JP1/IT Desktop Management 2 が使用しているファイルおよびフォルダがウィルス対策製品によって使用中となり、ファイルアクセスでエラーが発生することがあります。これによって、JP1/IT Desktop Management 2 の操作がエラーになったり、プロセスが強制終了したりする場合があります。この影響で、次に示す現象が発生するおそれがあります。

- データベースのバックアップに失敗する場合があります。
- インベントリ情報や操作ログ情報の収集やソフトウェアなどの配布ができなくなる場合があります。
- Internet Explorer でのファイルのアップロードやダウンロードが遅延したり、Internet Explorer が停止したりする場合があります。
- 操作ログや資産情報などのエクスポートが遅延し完了まで時間がかかることがあります。
- ネットワークモニタによる機器の検知、およびネットワーク接続の許可、遮断ができなくなる場合があります。
- コンポーネントの登録時にエラーになる場合があります。
- リモートインストールマネージャのジョブの実行が遅延する場合があります。

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　フォルダ一覧

管理用サーバに作成されるフォルダ

JP1/IT Desktop Management 2 - Manager をインストールした場合に、管理用サーバに作成されるフォルダを次の表に示します。サブフォルダを含むフォルダ名やファイル名を変更しないでください。

フォルダ名	説明
JP1/IT Desktop Management 2 - Manager のインストール先フォルダ	JP1/IT Desktop Management 2 のデータの格納フォルダです。
%WINDIR%¥Temp¥JDNINST	インストールで出力されるログファイルの格納フォルダです。

*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*の配下に作成されるフォルダを次の表に示します。

フォルダ名	説明
log¥	ログの格納フォルダです。
mgr¥	管理用サーバのルートフォルダです。
mgr¥backup¥	デフォルトのバックアップ格納フォルダです。
mgr¥bin¥	実行ファイルの格納フォルダです。
mgr¥conf¥	環境定義ファイルの格納フォルダです。
mgr¥db¥	データベースのインストールフォルダです。
mgr¥dbclt¥	データベースの ODBC ドライバのインストーラ格納フォルダです。
mgr¥definition	連携用定義ファイル格納フォルダです。
mgr¥doc¥	オンラインマニュアルの格納フォルダです。
mgr¥download¥	インストールセットの格納フォルダです。
mgr¥endorsed¥	Java 標準ライブラリ置き換えファイル格納フォルダです。
mgr¥gui¥	J2EE アプリケーション格納フォルダです。
mgr¥license¥	ライセンスファイルの格納フォルダです。
mgr¥log¥	トレースログの格納フォルダです。
mgr¥nma¥	ネットワークモニタエージェントの格納フォルダです。
mgr¥ospatch¥	更新プログラム情報ファイルの格納フォルダです。

フォルダ名	説明
mgr¥script¥	エージェントのスクリプトファイルの格納フォルダです。
mgr¥Setup_Input¥	データベースのセットアップ用入力ファイル格納フォルダです。
mgr¥Setup_Input_HA¥	クラスタ時のデータベースのセットアップ用入力ファイル格納フォルダです。
mgr¥temp¥	一時データの格納フォルダです。
mgr¥tools¥	ツールの格納フォルダです。
mgr¥troubleshoot¥	デフォルトのトラブルシュート情報格納フォルダです。
mgr¥uCPSB¥	アプリケーションサーバのインストールフォルダです。

JP1/IT Desktop Management 2 - Manager のインストールまたはセットアップ時に作成されるフォルダ（インストール先フォルダ以外）を次の表に示します。

フォルダ名	説明
%ProgramFiles%¥Hitachi¥HNTRLib2¥	トレースライブラリのインストールフォルダです。
All User プロファイルのアプリケーションデータフォルダ¥Hitachi¥jp1itdmm¥Database¥※	JP1/IT Desktop Management 2 のデータ格納フォルダです。
All User プロファイルのアプリケーションデータフォルダ¥Hitachi¥jp1itdmm¥LocalData¥※	ローカルディスクの作業用フォルダです。
システムのプログラムメニュー¥JP1_IT Desktop Management 2 - Manager¥	プログラムフォルダです。 複数サーバ構成の管理用中継サーバとしてインストールした場合は、サブフォルダに［エージェント］フォルダが作成されます。

注※　製品の提供時にデフォルトとして設定されているフォルダです。セットアップ時に作成されます。

リモートインストールマネージャ用に作成されるフォルダ

Remote Install Manager をインストールするコンピュータに作成されるフォルダを次の表に示します。サブフォルダを含むフォルダ名やファイル名を変更しないでください。

フォルダ名	説明
Remote Install Manager のインストール先フォルダ	リモートインストールマネージャのデータ格納フォルダです。
%WINDIR%¥Temp¥JDNINST	インストールで出力されるログファイルの格納フォルダです。

*Remote Install Manager のインストール先フォルダ*の配下に作成されるフォルダを次の表に示します。

フォルダ名	説明
log¥	ログの格納フォルダです。
mgr¥	Remote Install Manager のルートフォルダです。
mgr¥bin¥	実行ファイルの格納フォルダです。
mgr¥dbclt¥	データベースの ODBC ドライバのインストーラ格納フォルダです。
mgr¥license¥	ライセンスファイルの格納フォルダです。
mgr¥RMTINS¥	Remote Install Manager 関連フォルダの格納フォルダです。
mgr¥temp¥	一時データの格納フォルダです。
mgr¥troubleshoot¥	デフォルトのトラブルシュート情報格納フォルダです。

Remote Install Manager のインストールまたはセットアップ時に作成されるフォルダ（インストール先フォルダ以外）を次の表に示します。

フォルダ名	説明
システムのプログラムメニュー¥JP1_IT Desktop Management 2 - Manager¥	プログラムフォルダです。

インターネットゲートウェイサーバに作成されるフォルダ

インターネットゲートウェイをインストールするコンピュータに作成されるフォルダを次の表に示します。

フォルダ名	説明
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	インターネットゲートウェイのデータの格納フォルダです。
%WINDIR%¥Temp¥JDNINST	インストールで出力されるログファイルの格納フォルダです。

*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*の配下に作成されるフォルダを次の表に示します。

フォルダ名	説明
igw¥	インターネットゲートウェイのルートフォルダです。
igw¥bin	実行ファイルの格納フォルダです。
igw¥Web	インターネット公開用フォルダです。
log¥	ログの格納フォルダです。

インターネットゲートウェイのインストールまたはセットアップ時に作成されるフォルダ（インストール先フォルダ以外）を次の表に示します。

フォルダ名	説明
システムのプログラムメニュー¥JP1_IT Desktop Management 2 - Internet Gateway¥	プログラムフォルダです。

付録 A.2　サービス、プロセス一覧

JP1/IT Desktop Management 2 の各サービスのサービス名、対応するサービスプロセス名、サービスの説明、およびサービスが自動起動するかどうかを次の表に示します。

JP1/IT Desktop Management 2 - Manager のサービス一覧

サービス名	サービス表示名	サービスプロセス名	説明	サービスの自動起動
JP1_DTNAVI_AGCTRL	JP1_ITDM2_Agent Control	*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*¥mgr¥bin¥jdnagcadm.exe	エージェント制御サービスです。	○
JP1_DTNAVI_MGRSRV	JP1_ITDM2_Service	*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*¥mgr¥bin¥jdnmsservice.exe	マネージャサービスです。	○
JP1_DTNAVI_RLYMGRSRV	JP1_ITDM2_Relay Manager Service	*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*¥mgr¥bin¥jdnrelaymgrsrv.exe	管理用サーバの中継サービスです。	○　※
JP1_DTNAVI_WEBCON	JP1_ITDM2_Web Container	*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*¥mgr¥bin¥jdnwebcon.exe	アプリケーションサーバのサービスです。	○
JP1_DTNAVI_WEBSVR	JP1_ITDM2_Web Server	*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*¥mgr¥uCPSB¥httpsd¥httpsd.exe	Web サーバのサービスです。	○
HiRDBEmbeddedEdition_JE1	JP1_ITDM2_DB Service	*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*¥mgr¥db¥BIN¥pdservice.exe	管理用サーバのデータベースサービスです。	○
HiRDBClusterService_JE1	JP1_ITDM2_DB Cluster Service	*JP1/IT Desktop Management 2 - Manager のインストール先フォルダ*¥mgr¥db¥BIN¥pdsha.exe	管理用サーバのデータベースのクラスタサービスです。	－
Hntr2Service	Hitachi Network Objectplaza Trace Monitor 2	%Program files%¥Hitachi¥HNTRLib2¥bin¥hntr2srv.exe	ログ出力サービスです。	－

（凡例）○：自動起動する　－：自動起動しない

注　クラスタ構成の場合は、クラスタソフトウェアの機能を使用して各サービスを操作するため、自動起動しません。

注※　複数サーバ構成の場合に自動起動します。最小構成および基本構成では自動起動しません。

JP1/IT Desktop Management 2 - Network Monitor のサービス一覧

サービス名	サービス表示名	サービスプロセス名	説明	サービスの自動起動
NXNetMonitor	JP1_ITDM2_Network Monitor	%ProgramFiles%¥Hitachi¥jp1itdmn¥nma¥bin¥nxnmsvc.exe	ネットワークモニタのサービスです。	○

（凡例）○：自動起動する

JP1/IT Desktop Management 2 - Agent および管理用中継サーバ用エージェントのサービス一覧

サービス名	サービス表示名	サービスプロセス名	説明	サービスの自動起動
jdngsrv	JP1_ITDM2_Agent Service	%SystemRoot%¥system32¥jdngsrv.exe	エージェントサービスです。	○
jdngsmcsrv	JP1_ITDM2_Agent Monitor Control	エージェントの場合 *JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*¥bin¥jdngsmcsrv.exe 管理用中継サーバ用のエージェントの場合 *JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*¥mgr¥bin¥jdngsmcsrv.exe	稼働監視サービスです。	○
jdngrcagent	JP1_ITDM2_Agent Remote Control	エージェントの場合 *JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*¥bin¥jdngrcagent.exe 管理用中継サーバ用のエージェントの場合 *JP1/IT Desktop Management 2 - Agent のインストール先フォルダ*¥mgr¥bin¥jdngrcagent.exe	リモコンエージェントのサービスです。	○

（凡例）○：自動起動する

JP1/IT Desktop Management 2 - Manager をインストールしたコンピュータに常駐するプロセス名とその機能を次の表に示します。プロセスは、プロセス名のアルファベット順で並んでいます。

プロセス一覧

プロセス名	機能	プロセスの常駐
cjstartsv.exe	アプリケーションサーバのプロセスです。	○
cprfd.exe	アプリケーションサーバのプロセスです。	○
httpsd.exe	Web サーバ機能のプロセスです。	○
jdnagcadm.exe	サービスプロセスです。	○
jdnagcmain.exe	サービスプロセスです。	○
jdndmpadm.exe※1	サービスプロセスです。	○
jdngschserv.exe	サービスプロセスです。	○
jdngsite.exe※1	サービスプロセスです。	○
jdngsrvmain.exe	サービスプロセスです。	○
jdnmscontroller.exe	サービスプロセスです。	○
jdnmsplugincontroller.exe	サービスプロセスです。	○
jdnmssecurityctrl.exe	サービスプロセスです。	○
jdnmssecuritysplit.exe※2	サービスプロセスです。	○
jdnmsservice.exe	サービスプロセスです。	○
jdnrelaycontroller.exe※1	サービスプロセスです。	○
jdnrelaymgrsrv.exe※1	サービスプロセスです。	○
jdnwebcon.exe	アプリケーションサーバのプロセスです。	○

（凡例）○：常駐する

注※1　管理用中継サーバに常駐するプロセスです。

注※2　管理用サーバをセットアップするときに、サーバ構成の設定の［データベースへのアクセス時のキャッシュ容量］で［16GB］を選択した場合だけ常駐するプロセスです。

データベースのプロセス一覧

プロセス名	機能	プロセスの常駐（常駐数）	プロセス数
pdservice.exe	プロセスサーバを制御する HiRDB サービスプロセスです。	○	1
pdprcd.exe	HiRDB 関連プロセスを管理するプロセスサーバプロセスです。	○	1
pdrsvre.exe	プロセスが異常終了したときに後処理をするための後処理プロセスです。	○	1～3
pdmlgd.exe	メッセージの出力を制御するメッセージログサーバプロセスです。	○	1

プロセス名	機能	プロセスの常駐（常駐数）	プロセス数
pdrdmd.exe	ユニットの起動・停止や接続ユーザーの管理をするシステムマネージャプロセスです。	○	1
pdstsd.exe	ユニット用ステータスファイルを入出力するためのステータスサーバプロセスです。	○	1
pdlogd.exe	システムログの取得やログ関連のプロセスを制御するためのログサーバプロセスです。	○	1
pdscdd.exe	シングルサーバプロセスにトランザクションを割り当てるスケジューラプロセスです。	○	1
pdtrnd.exe	トランザクションを制御するトランザクションサーバプロセスです。	○	1
pdtrnrvd.exe	トランザクションの決着・回復を制御するトランザクション回復プロセスです。	○（1）	1～673
pd_buf_dfw.exe	データベース格納用ディスクに書き込み処理をするデファードライトプロセスです。	○	1
pdlogswd.exe	システムログ関連ファイルの割り当て・解放・入出力管理、およびシンクポイントダンプの取得をするためのログスワッププロセスです。	○	1
pdsds	SQL 処理をするためのシングルサーバプロセスです。	○（20）	1～350
pd*xxx*※	pdsds 以外の、ユティリティプロセスやデータベースの内部プロセスなどのプロセスです。	×	－

（凡例）○：常駐する　×：常駐しない　－：プロセスによって異なる

注※　*xxx* は、3～8 文字の文字列です。

付録 A.3　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。
31006～31009、31011、31012	← →	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。

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
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。
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。
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。

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
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。

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。
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。
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［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。
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.4　パラメーター一覧

ここでは、インストール、セットアップ、および設定画面のパラメーターについて説明します。

(1)　インストール時のパラメーター

JP1/IT Desktop Management 2 - Manager のインストール

JP1/IT Desktop Management 2 - Manager のインストール時のパラメーターを次に示します。

インストールタイプ

項目	内容	設定できる値	デフォルト
インストールタイプ	インストール方法を選択します。	• 簡単インストール • カスタムインストール	簡単インストール

ユーザー登録（カスタムインストールの場合）

項目	内容	設定できる値	デフォルト
ユーザー名	製品を使用するユーザー名を指定します。	制限はありません。	OS のインストール時に設定したユーザー名
会社名	製品を使用する会社名を指定します。	制限はありません。	OS のインストール時に設定した会社名

インストール先のフォルダ（簡単インストールの場合）

項目	内容	設定できる値	デフォルト
JP1/IT Desktop Management 2 - Manager をインストールするフォルダ	インストール先フォルダを指定します。	40 文字以内のパス※1	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¥jp1itdmm¥」）
データベースを作成するフォルダ	データベースを作成するフォルダを指定します。	100 文字以内のパス※2	*All User プロファイルのアプリケーションデータフォルダ*¥Hitachi¥jp1itdmm¥

注※1　使用できる文字は、半角英数字、半角スペース、および「.」（ピリオド）、「(」、「)」、「_」、「¥」です。

注※2　使用できる文字は、半角英数字、半角スペース、および「#」、「.」（ピリオド）、「(」、「)」、「@」、「¥」 です。

データベースの設定（簡単インストールの場合）

項目	内容	設定できる値	デフォルト
ユーザー ID	データベースを使用するためのユーザー ID を指定します。	8 文字以内の文字列※	itdm2m
パスワード	ユーザー ID に対するパスワードを指定します。	28 文字以内の文字列※	（空白）
パスワード確認	確認のため、指定したパスワードを再度入力します。		

注※　使用できる文字は半角英数字で、先頭の文字は英字です。

インストール先のフォルダ（カスタムインストールの場合）

項目	内容	設定できる値	デフォルト
JP1/IT Desktop Management 2 - Manager をインストールするフォルダ	インストール先フォルダを指定します。	40 文字以内のパス※	環境変数%ProgramFiles(x86)%で定義されたフォルダ配下（OS

項目	内容	設定できる値	デフォルト
JP1/IT Desktop Management 2 - Manager をインストールするフォルダ	インストール先フォルダを指定します。	40 文字以内のパス※	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 ¥jp1itdmm¥」）

注※　使用できる文字は、半角英数字、半角スペース、および「.」（ピリオド）、「(」、「)」、「_」、「¥」です。

カスタムインストール（カスタムインストールの場合）

項目	内容	設定できる値	デフォルト
インストールするコンポーネント	インストールするコンポーネントとインストール方法※1を選択します。	• Manager※2 機能の管理やセキュリティ状況の管理など、JP1/IT Desktop Management 2 のメイン機能を提供するコンポーネントです。 • Remote Install Manager※3 リモートインストールマネージャを使用した配布管理の GUI の機能を提供するコンポーネントです。 このコンポーネントは、Manager とは別のコンピュータにインストールできます。別のコンピュータにインストールする場合は、Manager と同じバージョンをインストールしてください。	すべてのコンポーネント

注※1　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。なお、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。］を選択すると、「×」印のアイコンに変わります。

注※2　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。

注※3　Remote Install Manager を Manager とは別のコンピュータにインストールする場合、Manager のプルダウンメニューは［この機能を使用できないようにします。］を選択してください。

インストールする Manager の種別（カスタムインストールの場合）

項目	内容	設定できる値	デフォルト
インストールする Manager の種別	JP1/IT Desktop Management 2 - Manager をインストールするサーバの種別を選択します。	• 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 最小構成の管理用サーバ、基本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としてインストールします。 • 管理用中継サーバ 複数サーバ構成の管理用中継サーバとしてインストールします。JP1/IT Desktop Management 2 - Agent がインストールされているコンピュータにはインストールできません。	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

注　この画面は、カスタムインストール（カスタムインストールの場合）画面で「Manager」を選択した場合に表示されます。

エージェントのコンポーネント設定（カスタムインストールの場合）

項目	内容	設定できる値	デフォルト
エージェントのコンポーネント	管理用中継サーバにインストールするエージェントのコンポーネントを選択します。 管理対象にするコンピュータとは別に、管理用中継サーバ用のエージェントのコンポーネントを設定する必要があります。	• リモコンエージェント • パッケージャ • Automatic Installation Tool	リモコンエージェント

注　この画面は、インストールする Manager の種別（カスタムインストールの場合）画面で「管理用中継サーバ」を選択した場合に表示されます。

インストール完了

項目	内容	設定できる値	デフォルト
セットアップ※1	インストール完了後に、セットアップを起動するかどうかを選択します。	チェックする セットアップを起動します。 チェックしない セットアップを起動しません。	チェックする

項目	内容	設定できる値	デフォルト
コンポーネントの自動更新※2	管理用サーバに登録されているエージェント、ネットワークモニタエージェントなどのコンポーネントが更新された場合に、各コンピュータへコンポーネントを自動的に配布するかどうかを設定します。	チェックする コンポーネントを自動更新します。 チェックしない コンポーネントを自動更新しません。	チェックしない
コンポーネントを配布パッケージとして登録する※2	コンポーネントのパッケージを作成するかどうかを設定します。コンポーネントのパッケージを作成することで、配布機能を利用して更新されたコンポーネントをインストールできます。	チェックする パッケージを作成します。 チェックしない パッケージを作成しません。	チェックしない

注※1　Manager をカスタムインストールした場合に表示されます。

注※2　上書きインストールを実行した場合で、セットアップが不要なときに表示されます。クラスタ構成システムの場合は、現用系サーバで表示されます。

JP1/IT Desktop Management 2 - Agent のインストール

JP1/IT Desktop Management 2 - Agent を提供媒体からインストールする時のパラメーターを次に示します。

インストールタイプ

項目	内容	設定できる値	デフォルト
インストールタイプ	インストール方法を選択します。	• 簡単インストール • カスタムインストール	簡単インストール

インストール先のフォルダ（カスタムインストールの場合）

項目	内容	設定できる値	デフォルト
JP1/IT Desktop Management 2 - Agent をインストールするフォルダ	インストール先フォルダを指定します。	104 バイト以内のパス※	C:¥Program Files¥Hitachi¥jp1itdma¥ 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。

注※　使用できる文字は、半角英数字、半角スペース、および「.」（ピリオド）、「(」、「)」、「:」、「_」、「¥」です。

インストールするコンポーネントの種別（カスタムインストールの場合）

項目	内容	設定できる値	デフォルト
インストールするコンポーネントの種別	インストールするコンポーネントの種別を指定します。	• エージェント • 中継システム	エージェント

インストールするコンポーネント（カスタムインストールの場合）

項目	内容	設定できる値	デフォルト
インストールするコンポーネント	インストールするコンポーネントとサブコンポーネント、そのインストール方法※1 を選択します。	• エージェントまたは中継システム※2（[インストールするコンポーネントの種別] ダイアログで指定した種別） • パッケージャ • Automatic Installation Tool	エージェントまたは中継システム（[インストールするコンポーネントの種別] ダイアログで指定した種別）

注※1　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。なお、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。］を選択すると、「×」印のアイコンに変わります。

注※2　リモコンエージェントは、エージェント、中継システムのサブコンポーネントです。

JP1/IT Desktop Management 2 - Internet Gateway のインストール

JP1/IT Desktop Management 2 - Internet Gateway を提供媒体からインストールする時のパラメーターを次に示します。

インストール先フォルダの変更

項目	内容	設定できる値	デフォルト
JP1/IT Desktop Management 2 - Internet Gateway をインストールするフォルダ	インストール先フォルダを指定します。	104 バイト以内のパス※	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¥jp1itdmg¥」）

注※　使用できる文字は、半角英数字、半角スペース、および「.」（ピリオド）、「(」、「)」、「:」、「_」、「¥」です。

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、インストール先フォルダとして指定しないでください。

(2) セットアップ時のパラメーター

管理用サーバおよびエージェントのセットアップのパラメーターを次に示します。

管理用サーバのセットアップ

セットアップの選択

項目	内容	設定できる値	デフォルト
セットアップの種類	セットアップの種類を選択します。	• 設定変更 • データベースアップグレード • サーバの再構築	データベースのアップグレードが不要な場合 設定変更 データベースのアップグレードが必要な場合 データベースアップグレード

データベースの設定（設定変更の場合）

項目	内容	設定できる値	デフォルト
データベースへのアクセス時のパスワードを変更する	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設定します。	チェックする パスワードを変更します。 チェックしない パスワードを変更しません。	チェックする
現在のパスワード	ユーザー ID に対する変更前のパスワードを指定します。	28 文字以内の文字列※	（空白）
新しいパスワード	ユーザー ID に対する変更後のパスワードを指定します。		
変更後パスワード再入力	確認のため、指定した変更後のパスワードを再度入力します。		

注※　使用できる文字は半角英数字で、先頭の文字は英字です。

サーバ構成の選択

項目	内容	設定できる値	デフォルト
サーバ構成※	サーバ構成を選択します。	• 単数サーバ構成 • 複数サーバ構成	単数サーバ構成

注※　複数サーバ構成から単数サーバ構成へは変更できません。

クラスタ環境

項目	内容	設定できる値	デフォルト
クラスタ構成で JP1/IT Desktop Management 2 - Manager を運用する	管理用サーバをクラスタ構成で運用するかどうかを設定します。	チェックする クラスタ環境で運用します。 チェックしない クラスタ環境では運用しません。	チェックしない
種別	種別を選択します。	• 現用系 • 待機系	現用系
論理ホスト名	ドメイン名を指定します。	半角 255 文字以内の文字列	（空白）
論理 IP アドレス	IP アドレスを指定します。	IPv4 形式の IP アドレス	（空白）
インポートする設定ファイル	インポートする設定ファイルを指定します。	255 文字以内のセットアップファイル（*.conf）	（空白）

注※　複数サーバ構成の管理用中継サーバは、クラスタ構成にできません。

データベースの設定（初期設定の場合）

パスワード設定

項目	内容	設定できる値	デフォルト
ユーザー ID	データベースにアクセスするためのユーザー ID を指定します。	8 文字以内の文字列※1	itdm2m
パスワード	ユーザー ID に対するパスワードを指定します。	28 文字以内の文字列※	（空白）
パスワード再入力	確認のため、指定したパスワードを再度入力します。		

注※　使用できる文字は半角英数字で、先頭の文字は英字です。

アドレス、キャッシュ設定

項目	内容	設定できる値	デフォルト
データベースへのアクセス時の IP アドレス	データベースにアクセスするための管理用サーバの IP アドレスを指定します。	IPv4 形式の IP アドレス	Windows の関数で取得した IP アドレス※
データベースへのアクセス時のキャッシュ容量	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ます。	• 1GB • 16GB	16GB

注※　複数のネットワークカードを利用している場合など、管理用サーバに複数の IP アドレスが設定されている場合は、取得した最初の IP アドレスです。

フォルダの設定

項目	内容	設定できる値	デフォルト
データベースフォルダ※1	データベース情報を格納するフォルダを指定します。クラスタ構成の場合は、共有ディスクのフォルダを指定します。	120 文字以内のパス※2	*All User プロファイルのアプリケーションデータフォルダ*¥Hitachi¥jp1itdmm¥Database¥db¥
データフォルダ※1	管理用サーバで使用するデータを格納するフォルダを指定します。 クラスタ構成の場合は、共有ディスクのフォルダを指定します。	120 文字以内のパス※2	*All User プロファイルのアプリケーションデータフォルダ*¥Hitachi¥jp1itdmm¥Database¥data¥
ローカルデータフォルダ※1	ローカルディスクで使用するデータ領域のフォルダを指定します。なお、共有ディスクのパスは指定できません。	120 文字以内のパス※2	*All User プロファイルのアプリケーションデータフォルダ*¥Hitachi¥jp1itdmm¥LocalData¥
データベース退避フォルダ※1	データベースを一時的に退避するフォルダを指定します。	120 文字以内のパス※2	*All User プロファイルのアプリケーションデータフォルダ*¥Hitachi¥jp1itdmm¥Database¥dbtemp¥

注※1　データベースフォルダ、データフォルダ、ローカルデータフォルダ、およびデータベース退避フォルダには、同一または親子関係のあるフォルダを指定できません。

注※2　使用できる文字は、半角英数字、半角スペース、および「#」、「.」（ピリオド）、「(」、「)」、「@」、「¥」です。

データベースアップグレードの設定

項目	内容	設定できる値	デフォルト
種別	種別を選択します。	• 現用系 • 待機系	現用系
インポートする設定ファイル	現用系ノードからコピーしたセットアップファイルを指定します。	255 文字以内のセットアップファイル（*.conf）※2	（空白）
データベースフォルダ※1	データベース情報を格納するフォルダを指定します。クラスタ構成の場合は、共有ディスクのフォルダを指定します。	120 文字以内のパス※2	*All User プロファイルのアプリケーションデータフォルダ*¥Hitachi¥jp1itdmm¥Database¥db¥
データベース退避フォルダ※1	データベースを一時的に退避するフォルダを指定します。	120 文字以内のパス※2	*All User プロファイルのアプリケーションデータフォルダ*¥Hitachi¥jp1itdmm¥Database¥dbtemp¥

注※1　データベースフォルダ、データフォルダ、ローカルデータフォルダ、およびデータベース退避フォルダには、同一または親子関係のあるフォルダを指定できません。

注※2　使用できる文字は、半角英数字、半角スペース、および「#」、「.」(ピリオド)、「(」、「)」、「@」、「¥」です。

操作ログの設定

項目	内容	設定できる値	デフォルト
操作ログを取得する	エージェント導入済みのコンピュータから操作ログを取得するかどうかを設定します。	チェックする 操作ログを取得します。 チェックしない 操作ログは取得しません。	簡単インストールの場合 チェックしない カスタムインストールの場合 チェックしない
操作ログを保管する	操作ログを保管するかどうかを設定します。	チェックする 操作ログを保管します。 チェックしない 操作ログはデータベースに登録されますが、保管されません。	簡単インストールの場合 チェックしない カスタムインストールの場合 チェックする
操作ログの保管先フォルダ※1	操作ログが保管されるフォルダを指定します。	120 文字以内のパス※2	(空白)
ユーザー名※3	保管先フォルダにアクセスするためのユーザー名を指定します。	半角 158 文字以内の文字列	(空白)
パスワード	ユーザー名に対するパスワードを指定します。	半角 30 文字以内の文字列	(空白)
管理対象の機器の台数	管理対象となる機器の台数を指定します。	50～30000	簡単インストールの場合 50 カスタムインストールの場合 200
操作ログのデータベース格納最大日数	操作ログをデータベースに格納する日数の最大値を指定します。例えば、100 と指定すると、100 日分の操作ログがデータベースに格納されます。※4	30～500	60
操作ログのデータベースフォルダ※5	操作ログを保管するデータベース用のフォルダを指定します。	120 文字以内のパス※6	*All User プロファイルのアプリケーションデータフォルダ*¥Hitachi¥jp1itdmm¥Database¥oplogdb
追加するキャッシュ容量	操作ログの検索性能を向上用としてデータベースのキャッシュに追加する容量を設定します。	0～16	0

注※1　ネットワークドライブ上のフォルダも指定できます。ネットワークドライブを指定する場合は、UNC 形式で指定します。

注※2　使用できる文字は、半角英数字、半角スペース、および「#」、「.」（ピリオド）、「(」、「)」、「@」、「¥」、「-」（ハイフン）です。

注※3　ドメインユーザーの場合は、「ドメイン名¥ユーザー名」の形式で指定してください。

注※4　一度設定した日数より減らすことはできません。

注※5　管理対象のコンピュータが 10,000～30,000 台の場合、操作ログのデータベースのディスクは、独立した別ディスク（物理的に別ディスク）にすることを推奨します。

注※6　使用できる文字は、半角英数字、半角スペース、および「#」、「.」（ピリオド）、「(」、「)」、「@」、「¥」です。

保存用の変更履歴の出力設定

項目	内容	設定できる値	デフォルト
保存用の変更履歴を定期的に出力する	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ます。	チェックする 保存用の変更履歴を定期的に出力します。 チェックしない 保存用の変更履歴を定期的に出力しません。	チェックしない
変更履歴の出力先フォルダ※1	保存用の変更履歴の出力先フォルダを指定します。	120 文字以内のパス※2	（空白）
ユーザー名※3	出力先フォルダにアクセスするためのユーザー名を指定します。	半角 158 文字以内の文字列	（空白）
パスワード	ユーザー名に対するパスワードを指定します。	半角 30 文字以内の文字列	（空白）

注※1　ネットワークドライブ上のフォルダも指定できます。ネットワークドライブを指定する場合は、UNC 形式で指定します。

注※2　使用できる文字は、半角英数字、半角スペース、および「#」、「.」（ピリオド）、「(」、「)」、「@」、「¥」、「-」（ハイフン）です。

注※3　ドメインユーザーの場合は、「ドメイン名¥ユーザー名」の形式で指定してください。

API の設定

項目	内容	設定できる値	デフォルト
API を使用する	API を使用するかどうかを設定します。	チェックする API を使用します。 チェックしない API を使用しません。	チェックしない

ポート番号の設定

項目	内容	設定できる値	デフォルト
管理者のコンピュータからの接続受付ポート番号	管理者のコンピュータから、操作画面をとおして管理用サーバに接続する際に使用されるポート番号を指定します。	2～49151	31080
API の接続受付ポート番号	外部システムから API を使用して管理用サーバへの接続に使用されるポート番号を指定します。	2～49151	31030
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への接続に使用されるポート番号を指定します。	5001～49151	31000
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接続に使用されるポート番号を指定します。	5001～49151	31001
サーバでの使用ポート番号	管理用サーバの内部処理で使用される、連続した 11 個のポート番号の開始値を指定します。	5001～49141	31002
API 処理の使用ポート番号	API で使用される、連続した 4 個のポート番号の開始値を指定します。	5001～49148	31026
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される、連続した 5 個のポート番号の開始値を指定します。	5001～49147	31016
複数サーバ構成の接続ポート番号	管理用サーバ間の中継に使用されるポート番号を指定します。	5001～49151	31023

注　複数サーバ構成の場合、上位の管理用サーバと下位の管理用中継サーバで同一のポート番号を指定してください。

アドレス解決の設定

項目	内容	設定できる値	デフォルト
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を設定します。		• ホスト名 • IP アドレス	ホスト名
アドレス解決の方法※1	ジョブの作成または実行時にアドレス解決する方法を設定します。	• Windows ネットワークを使用する ジョブの作成または実行時に Windows ネット	Windows ネットワークを使用する

項目	内容	設定できる値	デフォルト
アドレス解決の方法※1	ジョブの作成または実行時にアドレス解決する方法を設定します。	ワークから IP アドレスを取得します。※2 • 機器情報とシステム構成情報を使用する ジョブの作成または実行時に JP1/IT Desktop Management 2 のシステム構成からだけ IP アドレスを取得します。※3	Windows ネットワークを使用する
アドレス解決できないあて先へのジョブ※1	ジョブ実行時にあて先のアドレス解決ができなかった場合に、そのジョブをエラーとするかどうかを設定します。	• エラーとする • エラーとしない	エラーとしない

注※1　通信相手のコンピュータを決定する情報の種類（運用キーと呼びます）としてホスト名を選択した場合に設定してください。

注※2　アドレス解決には、hosts ファイルやネームサーバを使用します。アドレス解決に失敗した場合、JP1/IT Desktop Management 2 のシステム構成から IP アドレスを取得します。

注※3　JP1/IT Desktop Management 2 のシステム構成の IP アドレスは、常に正しい状態を保持する必要があります。夜間などネームサーバが停止した状態でジョブを作成および実行するような環境では、「Windows ネットワークを使用する」を選択しても、アドレス解決に失敗し、ジョブを作成できないことがあります。しかし、「IT Desktop Management 2 - Manager の機器およびシステム構成情報を使用する」を選択すると、アドレス解決に失敗するまでに掛かっていた時間を短縮できるメリットがあります。

管理用中継サーバの設定

項目	内容	設定できる値	デフォルト
上位接続先	管理用中継サーバが接続する上位の管理用サーバのホスト名または IP アドレスを指定します。※1	64 文字以内の文字列※2	（空白）
操作ログを送信する	上位の管理用サーバに操作ログを送信するかどうかを設定します。	チェックする 上位の管理用サーバに操作ログを送信します。 チェックしない 上位の管理用サーバに操作ログを送信しません。	チェックしない
USB デバイスの登録情報を送信する	上位の管理用サーバに USB デバイスの登録情報を送信するかどうかを設定します。	チェックする 上位の管理用サーバに USB デバイスの登録情報を送信します。	チェックしない

項目	内容	設定できる値	デフォルト
USB デバイスの登録情報を送信する	上位の管理用サーバに USB デバイスの登録情報を送信するかどうかを設定します。	チェックしない 上位の管理用サーバに USB デバイスの登録情報を送信しません。	チェックしない

注※1　上位の管理用サーバの［アドレス解決の設定］で指定した運用キーに選択している形式で指定してください。

注※2　次の内容に注意して設定してください。

- 使用できる文字は、半角英数字、および「-」（ハイフン）です。
- 「.」（ピリオド）は、ドメイン名の区切り文字としてだけ使用できます。
- ホスト名で指定する場合は、最初の文字が半角英字である必要があります。

管理用中継サーバの通信設定

項目	内容	設定できる値	デフォルト
上位サーバへの通知間隔	上位の管理用サーバに通知する間隔を指定します。	1～60	5
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。	1～720	120
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、［監視時間］に設定した時間を超えた場合、通信エラーとするかどうかを設定します。	チェックする 通信エラーとします。 チェックしない 通信エラーとしません。	チェックする
監視時間	管理用中継サーバにインストールされたエージェントが TCP/IP からの応答を待つ時間を指定します。	1～120	5
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かどうかを設定します。	チェックする 通信をリトライします。 チェックしない 通信をリトライしません。	チェックする
リトライ回数	リトライする回数を指定します。	1～999	5
リトライ間隔	リトライの間隔を指定します。	1～7200	5

ユーザー管理の設定

項目	内容	設定できる値	デフォルト
JP1/Base を使用してユーザー管理する	JP1/Base を使用してユーザー管理するかどうかを設定します。	チェックする JP1/Base を使用してユーザー管理します。 チェックしない JP1/Base を使用してユーザー管理しません。	チェックしない
JP1 資源グループ名	JP1/Base を使用してユーザー管理する場合、JP1/IT Desktop Management 2 - Manager と関連づけるための JP1 資源グループ名を設定します。	64 文字以内の文字列※	（空白）

注※　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「~」

その他の設定

項目	内容	設定できる値	デフォルト
通貨単位の設定	操作画面に表示される金額の単位を指定できます。	半角 10 文字以内の文字列	システムに設定されている通貨単位
管理用サーバでネットワークの帯域を制御する	ITDM 互換配布の機能で、管理用サーバからエージェントへパッケージを送信する場合の最大転送速度を指定するかどうかを設定します。	チェックする 管理用サーバからの最大転送速度を設定します。 チェックしない 管理用サーバからの最大転送速度を設定しません。	チェックしない
最大転送速度	パッケージ転送時の最大転送速度を指定します。	2～1024	2
アカウントをロックする連続入力失敗の回数	何回、連続して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。	0～10	0
ユーザ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を指定します。	0～999	180
操作画面での資産情報の操作を抑止する	Asset Console から資産管理を実施するため、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ます。	チェックする 操作画面での資産情報の操作を抑止します。 チェックしない 操作画面での資産情報の操作を抑止しません。	チェックしない

セットアップの終了

項目	内容	設定できる値	デフォルト
コンポーネントを登録する※1	管理用サーバにエージェント、ネットワークモニタエージェントなどのコンポーネントを登録するかどうかを設定します。	チェックする プログラムを登録します。 チェックしない プログラムを登録しません。	チェックする
コンポーネントの自動更新※2	管理用サーバに登録されているエージェント、ネットワークモニタエージェントなどのコンポーネントが更新された場合に、各コンピュータへコンポーネントを自動的に配布するかどうかを設定します。	チェックする コンポーネントを自動更新します。 チェックしない コンポーネントを自動更新しません。	チェックしない
コンポーネントを配布パッケージとして登録する※2	コンポーネントのパッケージを作成するかどうかを設定します。コンポーネントのパッケージを作成することで、配布機能を利用して更新されたコンポーネントをインストールできます。	チェックする パッケージを作成します。 チェックしない パッケージを作成しません。	チェックしない

注※1　手動でセットアップを起動した場合で、初めてセットアップを実行するときに表示されます。

注※2　インストールの延長でセットアップを起動した場合に表示されます。

リモートインストールマネージャを使用した配布のセットアップ

通信関連

項目	内容	設定できる値	デフォルト
JP1/IT Desktop Management 2 - Manager（管理用サーバ）	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する、管理用サーバのポート番号を指定します。	0～65535	31021
JP1/IT Desktop Management 2 - Agent（中継システム）	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する、中継システムのポート番号を指定します。	0～65535	31002
インターバル転送をする	エージェント、中継システムへのファイル転送が発生する場合、指定した単位ごとにファイルを分割し、インターバルを置	チェックする インターバル転送をします。	チェックしない

項目	内容	設定できる値	デフォルト
インターバル転送をする	いて実行するかどうかを設定します。	チェックしない インターバル転送をしません。	チェックしない
連続転送バッファ数※	1 度にファイル転送するバッファの個数を指定します。	0～4294967295	0
転送インターバル※	インターバル転送する時の、転送と転送との間のインターバル（休止時間）をどのくらいにするかを指定します。	0～4294967295	1000

注※　0 を指定するとインターバル転送されません。

サーバカスタマイズオプション

項目	内容	設定できる値	デフォルト
管理用サーバへの同時接続 JP1/IT Desktop Management 2 - Agent 数	同時に接続する次に示すシステムの数を絞り込んで、いくつまでにするかを指定します。 • エージェント • 中継システム	4～100	30
ジョブを同時実行する JP1/IT Desktop Management 2 - Agent 数※1	ジョブを実行するときに、同時に処理する次に示すシステムの数を指定します。 • エージェント • 中継システム • リモートインストールマネージャ • パッケージャ	0～100	20
ジョブを削除する時刻を指定する※2	ジョブの定義や実行状況を削除したあと、すぐにジョブを削除するかどうかを設定します。 すぐには削除しない場合、いつ削除するかを時刻で指定します。	チェックする すぐにはジョブを削除しません。この場合、削除する時刻を指定します。 0 時 0 分～23 時 59 分 チェックしない すぐにジョブを削除します。	チェックしない
JP1/IT Desktop Management 2 - Agent の起動を監視する	エージェント、中継システムが起動していないためにジョブが実行されない場合、ジョブ実行状態を「起動失敗」に変更し、それを配布管理システムに通知するかどうかを設定します。	チェックする エージェント、中継システムの起動を監視し、配布管理システムに通知します。	チェックしない

項目	内容	設定できる値	デフォルト
JP1/IT Desktop Management 2 - Agent の起動を監視する	エージェント、中継システムが起動していないためにジョブが実行されない場合、ジョブ実行状態を「起動失敗」に変更し、それを配布管理システムに通知するかどうかを設定します。	チェックしない エージェント、中継システムの起動を監視しません。	チェックしない
起動失敗要因を細分化する	エージェント、中継システムが起動に失敗した場合に、その要因を細分化して配布管理システムに通知するかどうかを設定します。	チェックする 起動失敗要因を細分化し、配布管理システムに通知します。 チェックしない 起動失敗要因を細分化しません。	チェックしない
JP1/IT Desktop Management 2 - Agent のファイル転送エラーを監視する	次に示すジョブ種別のジョブが、エージェント、中継システムとのファイル転送時に通信エラーになった場合に、ジョブの実行状態を「通信エラー」に変更し、それを配布管理システムに通知するかどうかを設定します。 • パッケージのインストール • クライアントユーザによるインストール • 中継までのパッケージの転送 • 中継からのコレクトファイル収集 • システム構成情報の取得 • コンピュータ(UNIX)のシステム情報の取得※3 • 中継からの結果通知保留 • 中継の結果通知保留の解除	チェックする ファイル転送エラーを監視し、配布管理システムに通知します。 チェックしない ファイル転送エラーを監視しません。	チェックしない

注※1　0 を指定すると、対象のシステムに起動電文を送信しません。言い換えると、リモートインストールマネージャからのジョブの実行や、エージェント制御を利用したエージェントの起動ができなくなります。

注※2　通常、配布管理では多数のエージェントを管理しているため、ジョブの定義や実行状況を削除すると、データベースの削除に時間が掛かり、操作に支障を来したり、基幹業務に負荷を掛けたりするおそれがあります。ジョブの削除を遅延させることで、都合の良い時刻に一斉に削除できるため、このような問題を回避できます。

注※3　このジョブは、あて先が Mac エージェントの場合にも適用できます。

マルチキャスト配布

項目	内容	設定できる値	デフォルト
マルチキャスト配布	ジョブをマルチキャスト配布する場合に使用するポート番号を指定します。	0～65535	31014
マルチキャスト配布（再送要求時）※1	マルチキャスト配布のジョブの再送要求で使用するポート番号を指定します。	0～65535	31015
マルチキャスト配布のジョブを送信する※2	「マルチキャスト配布」が指定されたジョブを、エージェント、中継システムにマルチキャスト方式で送信する場合に設定します。	チェックする マルチキャスト配布のジョブを送信します。 チェックしない マルチキャスト配布のジョブを送信しません。	チェックしない
マルチキャストアドレス	配布先のマルチキャストグループ※3 に割り当てられた、マルチキャストアドレスを指定します。	224.0.1.0～ 239.255.255.255	238.255.0.1
1 パケットのサイズ	ジョブを配布するときの、1 パケット分のサイズを指定します。	1～60	40※4

注※1　マルチキャスト配布は UDP プロトコルを使用するため、配布中にパケットの再送が起こるので、再送要求のポート番号も設定が必要です。

注※2　IP マルチキャストに対応していないルータを使用している場合はチェックしないでください。IP マルチキャストに対応していないルータを使用しているのにチェックすると、ユニキャスト配布に切り替わるため、ジョブが配布されるまでに時間が掛かります。

注※3　マルチキャストグループは、管理用サーバに接続するエージェントと中継システムをまとめたグループにします。配布先のエージェントと中継システムのマルチキャストアドレスがここで設定したマルチキャストアドレスと一致しない場合、そのエージェントと中継システムにはジョブがユニキャスト配布されます。

注※4　40 キロバイトは、100BASE の通信回線で効率的な値です。通信回線が 10BASE の場合は 4 キロバイトを設定してください。パケットサイズが大き過ぎると、マルチキャスト配布に失敗し、途中からユニキャスト配布になりますので、ご注意ください。

結果記録オプション

項目	内容	設定できる値	デフォルト
ジョブの実行結果の記録※1	ID を指定しないジョブの実行結果をリモートインストールマネージャに記録するかどうかを設定します。	チェックする ID を指定しないジョブの実行結果をリモートインストールマネージャに記録します。	チェックする

項目	内容	設定できる値	デフォルト
ジョブの実行結果の記録※1	ID を指定しないジョブの実行結果をリモートインストールマネージャに記録するかどうかを設定します。	チェックしない ID を指定しないジョブの実行結果をリモートインストールマネージャに記録しません。	チェックする
ジョブの結果を記録するジョブの実行状態	記録するジョブの実行状態を指定します。	エラー 実行状態がエラーのジョブだけをリモートインストールマネージャに記録します。 エラー/正常終了 実行状態が、エラーまたは正常終了のジョブをリモートインストールマネージャに記録します。	エラー/正常終了
ID ジョブのクライアント実行結果の記録※2	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を設定します。	チェックする 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します。 チェックしない 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しません。	チェックする
ID ジョブのクライアント実行結果を記録するジョブの実行状態	記録するジョブの実行状態を指定します。	エラー/完了 実行状態が、エラーまたは完了のジョブをリモートインストールマネージャに記録します。 エラー/完了/正常終了 実行状態が、エラー、完了または正常終了のジョブをリモートインストールマネージャに記録します。	エラー/完了/正常終了

注　不要な実行結果を記録しないことでディスク容量を削減できます。終了したジョブの実行結果が大量に残っていると、リモートインストールマネージャの動作が遅くなることがあるため、確認が必要な実行状態のジョブだけを記録しておくことをお勧めします。

注※1　次に示すジョブは、ジョブが終了しても実行状態を自動的に削除できません。

- 「クライアントユーザによるインストール」ジョブ
- 「コンピュータ(UNIX)のシステム情報の取得」ジョブのうち、エージェントでの実行日時が指定されたジョブ

  このジョブは Mac エージェントにも適用できます。

- 「コンピュータ(UNIX)のソフトウェア情報の取得」ジョブのうち、エージェントでの実行日時が指定されたジョブ

  このジョブは Mac エージェントにも適用できます。

注※2　中継システムが管理する ID に属しているエージェントの実行結果については、すべてのジョブ種別でこの設定が有効になります。配布管理システムが管理する ID に属しているエージェントの場合、次に示すジョブはこの設定が無効になり、すべての実行状態が、配布管理システムに記録されます。

- 「クライアントユーザによるインストール」ジョブ
- 「コンピュータ(UNIX)のシステム情報の取得」ジョブのうち、エージェントでの実行日時が指定されたジョブ

  このジョブは Mac エージェントにも適用できます。
- 「コンピュータ(UNIX)のソフトウェア情報の取得」ジョブのうち、エージェントでの実行日時が指定されたジョブ

  このジョブは Mac エージェントにも適用できます。

システム構成関連

項目	内容	設定できる値	デフォルト
システム構成の変更を同期させる※	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中継システムのシステム構成情報に反映させるかどうかを設定します。	チェックする 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します。 チェックしない 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しません。	チェックする
削除履歴を保管する	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を設定します。	チェックする 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します。 チェックしない 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しません。	チェックしない

注※　複数サーバ構成の場合は、必ず［チェックする］になります。

イベントサービス

項目	内容	設定できる値	デフォルト
イベントサービス機能を使用する	JP1/Base のイベントサービス機能を使用して、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を設定します。	チェックする JP1 イベントとして JP1/IM に通知します。 チェックしない JP1 イベントとして JP1/IM に通知しません。	チェックしない
ジョブ完了イベント－ジョブ正常終了	すべてのあて先に対するジョブがすべて正常終了したことを通知するかどうかを設定します。	チェックする すべてのあて先に対するジョブがすべて正常終了したことを通知します。 チェックしない すべてのあて先に対するジョブがすべて正常終了したことを通知しません。	チェックしない
ジョブ完了イベント－ジョブエラー終了	エラーのジョブが発生したことを通知するかどうかを設定します。	チェックする エラーのジョブが発生したことを通知します。 チェックしない エラーのジョブが発生したことを通知しません。	チェックしない
指令完了イベント－指令正常終了	すべての指令が正常終了したことを通知するかどうかを設定します。	チェックする すべての指令が正常終了したことを通知します。 チェックしない すべての指令が正常終了したことを通知しません。	チェックしない
指令完了イベント－指令エラー終了	エラーの指令が発生したことを通知するかどうかを設定します。	チェックする エラーの指令が発生したことを通知します。 チェックしない エラーの指令が発生したことを通知しません。	チェックしない

JP1/IM に実行結果を通知できるジョブ種別を次に示します。これらのジョブについては、ジョブの実行結果を詳細な単位（指令）で通知することもできます。指令とは、JP1/IT Desktop Management 2 で作成するジョブの最小単位で、あて先または配布するソフトウェアごとに作成されます。例えば、2 つのあて先に対し、2 つのソフトウェアを配布するジョブを作成した場合、1 つのジョブに対し、4 つの指令が作成されます。

- パッケージのインストール
- 中継までのパッケージの転送
- リモートコレクト
- 中継までのリモートコレクト
- 中継からのコレクトファイル収集
- クライアントユーザによるインストール

障害関連

項目	内容	設定できる値	デフォルト	ファイル名※
ログ世代管理数	各ログを何個まで保存するかを指定します。	1～999	5	該当しない。
MAIN ログエントリ数	MAIN ログエントリの出力行数を指定します。	500～9,999	700	MAIN.LOG
USER ログエントリ数	USER ログエントリ数の出力行数を指定します。	500～9,999	700	• BUILD.LOG • SCRIPT.LOG • USER.LOG
COMPO ログエントリ数	COMPO ログエントリ数の出力行数を指定します。	500～9,999	700	• API.LOG • ATRFILE.LOG • BSAPI.LOG • CLTPROTO.LOG • DEFAULT.LOG • EXCFILE.LOG • MNGFILE.LOG • RDBMENTE.LOG • SERVICE.LOG • SRVSOCK.LOG • STSFILE.LOG • WSH.LOG
FUNC ログエントリ数	FUNC ログエントリ数の出力行数を指定します。	500～9,999	2000	• AMTAPI.LOG • CLIENT.LOG • CLTDEL.LOG • DCMAMT.LOG • DISCVRY.LOG • DLL.LOG • INVENTRY.LOG • MLTPROTO.LOG • MONRST.LOG

項目	内容	設定できる値	デフォルト	ファイル名※
FUNC ログエントリ数	FUNC ログエントリ数の出力行数を指定します。	500～9,999	2000	• MONTRACE.LOG • NDGMENT.LOG • PSM.LOG • SCHEDULE.LOG • SCHTRACE.LOG • SERVER.LOG • SITE.LOG • SRVAPI.LOG • SRVLOCK.LOG • USER_CLT.LOG • WRAPPER.LOG
LONG ログエントリ数	LONG ログエントリ数の出力行数を指定します。	500～9,999	700	• DUMP.LOG • NODE.LOG • NODEOPR.LOG • RDBSRV.LOG • USERINV.LOG
イベントビューアへ出力するメッセージ種別	Windows NT のイベントビューアに出力するメッセージの種別を指定します。	エラーメッセージを出力 エラーメッセージを出力します。 エラーメッセージ、警告メッセージを出力 エラーメッセージと警告メッセージを出力します。 エラーメッセージ、警告メッセージ、情報メッセージを出力 エラーメッセージ、警告メッセージおよび情報メッセージを出力します。	エラーメッセージを出力	該当しない。

注※　ここに列挙していないログファイルは、ログ世代管理数およびログエントリ数を設定できません。各ログファイルの容量は、次に示す計算式で算出できます。

ログファイルの容量（バイト）＝（ヘッダ部のサイズ＋（1 エントリのサイズ×エントリ数））×（世代数＋ 1）

ヘッダ部のサイズ：

17 バイト

1 エントリのサイズ：

192 バイト（LONG ログエントリ以外）または 300 バイト（LONG ログエントリ）

監査ログ

項目	内容	設定できる値	デフォルト
監査ログの出力単位	出力する監査ログの粒度を指定します。	• ジョブ単位で出力する • 指令単位で出力する※	ジョブ単位で出力する

注※ 「指令単位で出力する」を選択していると、出力された監査ログの容量がディスク容量を圧迫するおそれがあるので注意してください。

中継システムのセットアップ

接続先設定

項目	内容	設定できる値	デフォルト
上位システムと通信する	管理用サーバと接続するかどうかを指定します。	チェックする 管理用サーバと接続します。 チェックしない 管理用サーバと接続しません。	チェックする
ホスト名または IP アドレス	接続する管理用サーバのホスト名または IP アドレスを指定します。※1	ホスト名※2 または IPv4 形式の IP アドレス	管理用サーバのホスト名または IP アドレス
管理用サーバのポート番号	エージェントが管理用サーバに接続する際に使用されるポート番号を指定します。	5001～49151	31000

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、運用キーのキー項目として指定した内容に一致させてください。

注※2　255 文字以内の文字列で指定します。

通信設定

項目	内容	設定できる値	デフォルト
[ネットワークアダプタの設定] ボタン	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	なし	なし

項目	内容	設定できる値	デフォルト
[ネットワークアダプタの設定]ボタン	線に優先順位を付けたい場合にクリックします。	なし	なし

ネットワークアダプタの設定

項目	内容	設定できる値	デフォルト
使用するネットワークアダプタの優先順位を設定する	ネットワークアダプタが複数ある場合、使用するネットワークアダプタの優先順位を設定するかどうかを設定します。	チェックする ネットワークアダプタの優先順位を設定します。 チェックしない ネットワークアダプタの優先順位を設定しません。	チェックしない
サービス起動時または接続時にネットワークアダプタ情報を自動更新する	サービス起動時または接続時にネットワークアダプタ情報を自動更新するかどうかを設定します。	チェックする ネットワークアダプタ情報を自動更新します。 チェックしない ネットワークアダプタ情報を自動更新しません。	チェックする

エージェントのセットアップ

接続先設定

項目	内容	設定できる値	デフォルト
上位システムと通信する	次に示す上位システムと接続するかどうかを指定します。 • 管理用サーバ • 配布用上位システム	チェックする 上位システムと接続します。 チェックしない 上位システムと接続しません。	チェックする
ホスト名または IP アドレス	接続する管理用サーバのホスト名または IP アドレスを指定します。※1	ホスト名※2 または IPv4 形式の IP アドレス	管理用サーバのホスト名または IP アドレス
管理用サーバのポート番号	エージェントが管理用サーバに接続する際に使用されるポート番号を指定します。	5001～49151	31000
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 HTTPS 通信する	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するかどうかを指定します。	チェックする 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します。	チェックしない

項目	内容	設定できる値	デフォルト
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 HTTPS 通信する	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するかどうかを指定します。	チェックしない 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しません。	チェックしない
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サーバのホスト名または IP アドレスで指定します。 SSL サーバ証明書のコモンネームを設定します。ワイルドカード証明書の場合には、「*」にホスト名、サブドメインを指定します。コモンネームに IP アドレスを設定した場合にはその IP アドレスを指定します。	ホスト名※3 または IPv4 形式の IP アドレス	(空白)
インターネット接続設定のポート番号	インターネットゲートウェイサーバに接続する際に使用するポート番号を指定します。	1～65535	443

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、運用キーのキー項目として指定した内容と一致させてください。

注※2　255 文字以内の文字列で指定します。

注※3　255 文字以内の半角英数字、および次に示す記号で指定します。

「-」および「.」

先頭と末尾は半角英数字を指定する必要があります。

通信設定

項目	内容	設定できる値	デフォルト
[複数のネットワークアダプタの設定] ボタン	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にクリックします。	なし	なし
ユーザー認証する	インターネットゲートウェイサーバへの接続時に、Microsoft Internet Information Services のベーシック認証でユーザー認証するかどうかを指定します。	チェックする ユーザー認証をします。 チェックしない ユーザー認証をしません。	チェックしない
ユーザー認証のユーザー ID	ユーザー認証のユーザー ID を指定します。	276 文字以内の文字列	(空白)
ユーザー認証のパスワード	ユーザー認証のパスワードを指定します。	半角 48 文字以内の文字列	

項目	内容	設定できる値	デフォルト
ユーザー認証のパスワード確認	確認のため、指定したパスワードを再度入力します。	半角 48 文字以内の文字列	(空白)
• 管理用サーバで設定した値を使用する • クライアントで設定した値を使用する	プロキシサーバの設定として、管理用サーバで設定した値を使用するか、クライアントで設定した値を使用するかを選択します。	[管理用サーバで設定した値を使用する] を選択 プロキシサーバの設定として、管理用サーバで設定した値を使用します。 [クライアントで設定した値を使用する] を選択 プロキシサーバの設定として、クライアントで設定した値を使用します。	[管理用サーバで設定した値を使用する]
プロキシサーバを使用する	エージェント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。	チェックする プロキシサーバを使用して通信します。 チェックしない プロキシサーバを使用せずに通信します。	チェックしない
プロキシサーバの設定のホスト名または IP アドレス	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※または IPv4 形式の IP アドレス	(空白)
プロキシサーバの設定のポート番号	プロキシサーバのポート番号を指定します。	1～65535	
プロキシサーバの設定のユーザー ID	プロキシサーバのユーザー ID を指定します。	276 文字以内の文字列	
プロキシサーバの設定のパスワード	プロキシサーバのパスワードを指定します。	半角 48 文字以内の文字列	
プロキシサーバのパスワード確認	確認のため、指定したパスワードを再度入力します。		

注※　249 文字以内の半角英数字、および次に示す記号で指定します。

「-」および「.」

先頭と末尾は半角英数字を指定する必要があります。

ネットワークアダプタの設定

項目	内容	設定できる値	デフォルト
使用するネットワークアダプタの優先順位を設定する※	ネットワークアダプタが複数ある場合、使用するネットワークアダプタの優先順位を設定するかどうかを設定します。	チェックする ネットワークアダプタの優先順位を設定します。	チェックしない

項目	内容	設定できる値	デフォルト
使用するネットワークアダプタの優先順位を設定する※	ネットワークアダプタが複数ある場合、使用するネットワークアダプタの優先順位を設定するかどうかを設定します。	チェックしない ネットワークアダプタの優先順位を設定しません。	チェックしない
サービス起動時または接続時にネットワークアダプタ情報を自動更新する	サービス起動時または接続時にネットワークアダプタ情報を自動更新するかどうかを設定します。	チェックする ネットワークアダプタ情報を自動更新します。 チェックしない ネットワークアダプタ情報を自動更新しません。	チェックする

注※　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、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分散して管理する場合など、エージェントの接続先設定ファイル（itdmhost.conf）を使用する場合は、チェックしないでください。チェックした場合は、エージェントの接続先を決定するために使用する IP アドレスは優先度が一番高いネットワークアダプタから取得されます。なお、管理する機器の IP アドレスを DHCP サーバで自動的に割り当てる場合は、割り当てられる IP アドレスが変わるたびに接続先が変わるおそれがあります。このため、接続先設定ファイルでは、DHCP サーバが自動的に割り当てる範囲の IP アドレスに応じた接続先を設定する必要があります。例えば、DHCP サーバで割り当てる範囲の IP アドレスが 172.17.12.1～172.17.12.250 の場合、接続先設定ファイルに IP アドレスが 172.17.12.1～172.17.12.250 の機器の接続先を指定してください。また、管理する機器が使用する IP アドレスを確実に把握しておいてください。

バージョンアップした場合は、既存の設定項目はそのまま引き継がれて表示され、新しい設定項目はデフォルト値で表示されます。

インターネットゲートウェイのセットアップ

接続先設定

項目		内容	設定できる値	デフォルト
管理用サーバ	ホスト名または IP アドレス	接続する管理用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※1 または IPv4 形式の IP アドレス	（空白）
	ポート番号	インターネットゲートウェイが管理用サーバに接続する際に使用されるポート番号を指定します。	5001～49151	31000
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	• 管理用サーバ • 中継システム	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選択します。	［管理用サーバ］を選択 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として、管理用サーバを指定します。	［管理用サーバ］

項目		内容	設定できる値	デフォルト
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	• 管理用サーバ • 中継システム	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選択します。	[中継システム]を選択 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として、中継システムを指定します。	[管理用サーバ]
	ホスト名または IP アドレス※5	配布用の上位システム（管理用サーバまたは中継システム）のホスト名または IP アドレスを指定します。	ホスト名※2 または IPv4 形式の IP アドレス	（空白）
	ポート番号（管理用サーバ）※3	インターネットゲートウェイが管理用サーバに接続する際に使用されるポート番号を指定します。	1～65535	31021
	ポート番号（中継システム）※4	インターネットゲートウェイが中継システムに接続する際に使用されるポート番号を指定します。	1～65535	31002

注※1　255 文字以内の文字列で指定します。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で、管理用サーバのホスト名が 64 文字を超える場合には、IP アドレスを指定します。

注※2　半角 64 文字以内の文字列で指定します。

注※3　[管理用サーバ]を選択している場合だけ編集できます。

注※4　[中継システム]を選択している場合だけ編集できます。

注※5

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。

(3)　ユーザーアカウントの設定のパラメーター

設定画面の［ユーザー管理］－［ユーザーアカウントの管理］画面のパラメーターを次に示します。

ユーザーアカウント

項目	内容	設定できる値	デフォルト
ユーザーアカウント	JP1/IT Desktop Management 2 のユーザーアカウントを設定します。	ユーザーアカウント	system
ユーザー ID	操作画面へログインするためのユーザー ID を指定します。	半角 64 文字以内の文字列※1	（空白）
パスワード	ユーザー ID に対するパスワードを指定します。	半角 32 文字以内の文字列※2	（空白）
パスワード確認	パスワードを再指定します。	半角 32 文字以内の文字列※2	（空白）
ユーザー名	ユーザーアカウントの名称を指定します。	全角または半角で 128 文字以内の文字列	（空白）
メールアドレス	ユーザーアカウントの利用者のメールアドレスを指定します。	E-mail 形式の文字列	（空白）
説明	ユーザーアカウントの説明を指定します。	全角または半角で 1,024 文字以内の文字列	（空白）
システム管理権限※3	ユーザーアカウントに、システム管理権限を付与するかどうかを設定します。	チェックする システム管理権限を付与します。 チェックしない システム管理権限は付与しません。	チェックしない
ユーザーアカウント管理権限※3	ユーザーアカウントに、ユーザーアカウント管理権限を付与するかどうかを設定します。	チェックする ユーザーアカウント管理権限を付与します。 チェックしない ユーザーアカウント管理権限は付与しません。	チェックしない
セキュリティ管理	ユーザーアカウントの業務分掌に、セキュリティ管理を設定するかどうかを指定します。	チェックする 業務分掌にセキュリティ管理を設定します。 チェックしない 業務分掌にセキュリティ管理は設定しません。	チェックする
資産管理	ユーザーアカウントの業務分掌に、資産管理を設定するかどうかを指定します。	チェックする 業務分掌に資産管理を設定します。	チェックする

項目	内容	設定できる値	デフォルト
資産管理	ユーザーアカウントの業務分掌に、資産管理を設定するかどうかを指定します。	チェックしない 業務分掌に資産管理は設定しません。	チェックする
機器管理	ユーザーアカウントの業務分掌に、機器管理を設定するかどうかを指定します。	チェックする 業務分掌に機器管理を設定します。 チェックしない 業務分掌に機器管理は設定しません。	チェックする
配布管理	ユーザーアカウントの業務分掌に、配布管理を設定するかどうかを指定します。	チェックする 業務分掌に配布管理を設定します。 チェックしない 業務分掌に配布管理は設定しません。	チェックする
システム設定管理	ユーザーアカウントの業務分掌に、システム設定管理を設定するかどうかを指定します。	チェックする 業務分掌にシステム設定管理を設定します。 チェックしない 業務分掌にシステム設定管理は設定しません。	チェックしない
このユーザーアカウントの管轄範囲を設定する	ユーザーアカウントに、管轄範囲を設定するかどうかを指定します。	チェックする ユーザーアカウントの管轄範囲を設定します。 チェックしない ユーザーアカウントの管轄範囲を設定しません。	チェックしない
管轄範囲	管轄範囲を指定します。	部署のグループ	設定されていない。
アカウントロック状態	ユーザーアカウントがロックされている場合だけ表示されます。[ロック中] が選択されている状態では、JP1/IT Desktop Management 2 にログインできません。	解除 ユーザーアカウントのロックを解除できます。 ロック中 ユーザーアカウントはロックされています。	ロック中。

注※1

使用できる文字は、半角英数字、および次に示す記号です。

「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」（ピリオド）、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」、および半角スペース

注※2

ユーザーアカウントに設定するパスワードは、次のルールに沿って設定してください。

- 8 文字以上、32 文字以下
- 半角英数字、および次に示す記号を使用

  「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」（ピリオド）、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」、および半角スペース
- 2 種類以上の文字の組み合わせ
- ユーザー ID と異なる文字列
- パスワードを変更する場合は、現在のパスワードと異なる文字列

注※3

システム管理権限とユーザーアカウント管理権限の両方がチェックされていない場合、ユーザーアカウントには参照権限だけが付与されます。

メールの通知先

項目	内容	設定できる値	デフォルト
メールの通知先	メール通知機能で指定するメール通知先を設定します。	メールの通知先	（空白）
ユーザー名	メール通知先の名称を指定します。	全角または半角で 128 文字以内の文字列	（空白）
メールアドレス	メール通知先のメールアドレスを指定します。	E-mail 形式の文字	（空白）
説明	メール通知先の説明を指定します。	全角または半角で 1,024 文字以内の文字列	（空白）

(4) エージェント設定のパラメーター

設定画面の［Windows エージェント設定とインストールセットの作成］画面から表示できる［エージェント設定の追加］ダイアログ、および［エージェント設定の編集］ダイアログのパラメーターを次に示します。

基本設定

項目		内容	設定できる値	デフォルト
管理用サーバ	ホスト名または IP アドレス	エージェントが接続する管理用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※1 または IPv4 形式の IP アドレス	管理用サーバのホスト名または IP アドレス
	ポート番号	エージェントが管理用サーバに接続する際に使用するポート番号を指定します。	5001～49151	管理用サーバのセットアップで［ポート番号の設定］画面の［エージェントからの接続

項目		内容	設定できる値	デフォルト
管理用サーバ	ポート番号	エージェントが管理用サーバに接続する際に使用するポート番号を指定します。	5001～49151	受付ポート番号］に指定したポート番号
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※2	システム種別	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指定します。次のような場合は、必ず［管理用サーバ］を指定してください。 • 中継システムに割り当てるエージェント設定を作成する場合 • デフォルトエージェント設定を編集する場合	• 管理用サーバ • 中継システム	管理用サーバ
	ホスト名または IP アドレス	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のホスト名または IP アドレスを指定します。次のような場合は、必ず管理用サーバのホスト名または IP アドレスを指定してください。 • 中継システムに割り当てるエージェント設定を作成する場合 • デフォルトエージェント設定を編集する場合	ホスト名※3 または IPv4 形式の IP アドレス	管理用サーバのホスト名または IP アドレス
	配布用ポート番号（管理用サーバ）	エージェントが配布用の管理用サーバに接続する際に使用するポート番号を指定します。	1～65535	管理用サーバのセットアップで、［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］画面の［通信関連］－［ポート番号］－［IT Desktop Management 2 - Manager（管理用サーバ）］に指定したポート番号
	配布用ポート番号（中継システム）	エージェントが配布用の中継システムに接続する際に使用するポート番号を指定します。	1～65535	管理用サーバのセットアップで、［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］画面の［通信関連］－［ポート番号］－［IT Desktop Management 2 - Manager（中継システム）］に指定したポート番号

項目		内容	設定できる値	デフォルト
インターネット接続設定	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HTTPS 通信する	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するかどうかを指定します。	チェックする 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します。 チェックしない 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しません。	チェックしない
	インターネットゲートウェイホスト名またはIP アドレス	インターネットゲートウェイサーバのホスト名または IP アドレスを指定します。 SSL サーバ証明書のコモンネームを設定します。ワイルドカード証明書の場合には、「*」にホスト名、サブドメインを指定します。コモンネームに IP アドレスを設定した場合にはその IP アドレスを指定します。	ホスト名※12 または IPv4 形式の IP アドレス	(空白)
	インターネットゲートウェイポート番号	インターネットゲートウェイサーバに接続する際に使用するポート番号を指定します。	1～65535	443
	エージェントで使用するポート番号	インターネットゲートウェイサーバに接続する際にエージェントの内部で使用するポート番号を指定します。	1～65534	31024
	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どうかを指定します。	チェックする 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します。 チェックしない 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。	チェックしない
上位システムと通信する		上位システムと通信するかどうかを指定します。	チェックする 上位システムと通信します。コンピュータをオンライン管理する場合にチェックします。 チェックしない 上位システムと通信しません。コンピュータをオ	チェックする

項目	内容	設定できる値	デフォルト
上位システムと通信する	上位システムと通信するかどうかを指定します。	フライン管理する場合にチェックを外します。	チェックする
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	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かどうかを指定します。	チェックする 定期的に上位システムに通知します。 チェックしない 上位システムに通知しません。	チェックする
監視間隔（セキュリティ項目）（分）	エージェントのセキュリティに関する機器情報の更新を監視する間隔を指定します。※4	1～9999	10
監視間隔（セキュリティ項目以外）（分）	エージェントのセキュリティ以外の機器情報の更新を監視する間隔を指定します。※4	1～9999	60
流量制御	ITDM 互換配布の機能で管理用サーバからエージェントにパッケージが転送される際に、時間当たりのデータ転送量の上限値を設けて流量制御するかどうかを選択します。 このパラメーターは、JP1/IT Desktop Management の設定と互換性を保つために使用します。JP1/IT Desktop Management と同じ動作で運用したい場合以外は、「しない」を選択してください。	する 流量制御をします。時間当たりのデータ転送量の上限値とする割合を30%～99%（デフォルト：99%）で指定します。 しない 流量制御をしません。	しない
システム起動を基準としたポーリングをする※5	システム起動を基準としたポーリングをするかどうかを選択します。	チェックする システム起動を基準としたポーリングをします。 チェックしない システム起動を基準としたポーリングをしません。	チェックする
ポーリングのタイミング	システム起動時のポーリングのタイミングをドロップダウンリストから選択します。※6	システム起動前 エージェントを起動したとき、先にポーリングしてから、ダウンロード済みのパッケージのインストール処理をします。※7 システム起動後 エージェントを起動したとき、ダウンロード済みのパッケージのインス	システム起動前

項目	内容	設定できる値	デフォルト
ポーリングのタイミング	システム起動時のポーリングのタイミングをドロップダウンリストから選択します。※6	トール処理をしたあとに、ポーリングします。※8	システム起動前
ポーリングの方法	ポーリングする方法を選択します。	システム起動時に 1 度だけポーリングする システム起動時に 1 度だけポーリングします。なお、[ポーリングのタイミング] で [システム起動前] を選択した場合だけ、ドロップダウンリストから [システム起動をするたびにポーリングする] または [初回のシステム起動時だけポーリングする（1 回/1 日)] を選択できます。 システム起動をするたびに、定期的にポーリングする 一定の間隔でポーリングします。ポーリングの間隔は 1～720 分で指定します。	システム起動をするたびに、定期的にポーリングする（30 分）
ポーリングを開始するタイミング	システムを起動してからポーリングを開始するまでの時間とタイミングを指定します。	システム起動時にポーリングを開始する システム起動と同時にポーリングを開始します。 指定するタイミングになるまでにポーリングを開始する エージェントが起動してから、指定した秒数が経過するまでの任意のタイミングでポーリングを開始します。何秒後までにポーリングを開始するかを 1～300 秒（デフォルト：1 秒）で指定します。※9 指定するタイミングでポーリングを開始する エージェントが起動してから、指定した秒数が経過するまで待機したあとにポーリングを開始します。待機する秒数を 1～	システム起動時にポーリングを開始する

項目		内容	設定できる値	デフォルト
ポーリングを開始するタイミング		システムを起動してからポーリングを開始するまでの時間とタイミングを指定します。	7200 秒（デフォルト：1 秒）で指定します。	システム起動時にポーリングを開始する
時刻を指定してポーリングする		1 日に 1 回、決まった時刻にポーリングするかどうかを選択します。	チェックする 決まった時刻にポーリングをします。 チェックしない 決まった時刻にポーリングをしません。	チェックしない
実行時刻		ポーリングの実行時刻を指定します。	0 時 0 分～23 時 59 分	0 時 0 分
JP1/IT Desktop Management 2 - Agent 変更の検知		JP1/IT Desktop Management 2 - Agent のインストールフォルダ配下の内容が変更されたことをイベントとして表示するかどうかを設定します。 管理対象のコンピュータのメモリ使用量を削減する必要がある場合にだけ、このチェックを外してください。チェックを外すと、仮想メモリの使用量が約 8 メガバイト削減されます。 なお、このチェックを外すと JP1/IT Desktop Management 2 - Agent インストールフォルダ配下が監視されなくなります。そのため、コンポーネントを自動的にアップデートするよう設定していても、エージェントが自動的に再インストール（復旧）される機能が動作しなくなりセキュリティが低下するおそれがあります。	チェックする イベントとして表示します。 チェックしない イベントとして表示しません。	チェックする
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	インターネットゲートウェイサーバへの接続時に、Microsoft Internet Information Services のベーシック認証でユーザー認証するかどうかを指定します。	チェックする ユーザー認証をします。 チェックしない ユーザー認証をしません。	チェックしない
	ユーザー認証する	ユーザー認証のユーザー ID を指定します。	276 文字以内の文字列	（空白）

項目		内容	設定できる値	デフォルト
インターネットゲートウェイの通信設定	ユーザー ID	ユーザー認証のユーザー ID を指定します。	276 文字以内の文字列	(空白)
	ユーザー認証するパスワード	ユーザー認証のパスワードを指定します。	半角 48 文字以内の文字列	
	ユーザー認証するパスワード確認	確認のため、指定したパスワードを再度入力します。		
	プロキシサーバを使用する	エージェント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。	チェックする プロキシサーバを使用して通信します。 チェックしない プロキシサーバを使用せずに通信します。	チェックしない
	プロキシサーバを使用するホスト名または IP アドレス	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※13 または IPv4 形式の IP アドレス	(空白)
	プロキシサーバを使用するポート番号	プロキシサーバのポート番号を指定します。	1～65535	
	プロキシサーバを使用するユーザー ID	プロキシサーバのユーザー ID を指定します。	276 文字以内の文字列	
	プロキシサーバを使用するパスワード	プロキシサーバのパスワードを指定します。	半角 48 文字以内の文字列	
	プロキシサーバを使用するパスワード確認	確認のため、指定したパスワードを再度入力します。		
	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	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。	チェックする サーバ証明書の有効期限が切れた場合は、インターネットゲートウェイとの接続をエラーとします。 チェックしない サーバ証明書の有効期限が切れた場合でも、インターネットゲートウェイ	チェックしない

項目		内容	設定できる値	デフォルト
インターネットゲートウェイの通信設定	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	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。	との接続をエラーとしません。	チェックしない
	アップロードファイルの分割サイズ	送信するファイルの分割サイズをキロバイトで設定します。プロキシサーバや Microsoft Internet Information Services などに制限がある場合、この値を変更します。※14	10～102400	1024
エージェント自動配信のインストール設定※10		エージェントをインストールするパスを設定します。	64 文字以内の文字列※11	%ProgramFiles%¥Hitachi¥jp1itdma

注※1　255 文字以内の文字列で指定します。

注※2　この項目の設定値は、[通信設定]の［ポーリング対象とする上位システム］に表示される優先順が 1 位の上位システムの値と常に等しくなるように連動しています。

注※3　64 文字以内の文字列で指定します。使用できる文字は、半角英数字、および「.」(ピリオド)、「-」(ハイフン）です。

注※4　Citrix XenApp、Microsoft RDS サーバの場合、監視間隔が 1 日 1 回となるように「1440」を設定してください。「1440」より小さい値を設定した場合、運用時の負荷が高くなり、機能に影響を与えるおそれがあります。

注※5　ソフトウェアの実行タイミングを「次回起動時に実行」に設定してジョブを実行する場合は、[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もオンにしてください。

注※6　ジョブ実行時にエージェントが起動していなかった場合、この設定によって、「システム起動時インストール」が設定されたパッケージのインストールタイミングを制御できます。

注※7 「システム起動時インストール」が設定されたパッケージが配布管理システムに登録済みの場合、システム起動時のポーリングによってダウンロードした直後にインストールされるため、1 回のシステム起動でインストールが完了します。なお、[ITDM2_Startup]フォルダを作成している場合、[ITDM2_Startup]フォルダに登録されているプログラムの起動は、「システム起動時インストール」が設定されたパッケージのインストール後になります。[ITDM2_Startup]フォルダに登録されているプログラムの起動を早くしたい場合は、「システム起動後」を指定してください。

注※8　ダウンロード済みのパッケージについてはシステム起動時にインストールされますが、そのあとのポーリングによってダウンロードした「システム起動時インストール」が設定されたパッケージは、次回のシステム起動時にインストールされます。

注※9　この設定をしておくと、複数のエージェントが同時に起動した場合でも、同時に上位システムへ接続することがなくなり、ネットワークへの負荷が分散されます。上位システムに接続するエージェントの台数が多くてシステム能力が追い付かない場合や、ネットワークに負荷が掛かり過ぎる場合に、設定値を大きくすることで負荷を軽くできます。

注※10　デフォルトエージェントを設定する場合にだけ表示される項目です。

注※11　使用できる文字は、半角英数字、半角スペース、および「%」、「.」（ピリオド）、「(」、「)」、「¥」、「_」です。

注※12　255 文字以内の半角英数字、および次に示す記号で指定します。

「-」および「.」

先頭と末尾は半角英数字を指定する必要があります。

注※13　249 文字以内の半角英数字、および次に示す記号で指定します。

「-」および「.」

先頭と末尾は半角英数字を指定する必要があります。

注※14　Microsoft Internet Information Services の役割サービス「要求フィルター」をインストールしている場合、アップロードファイルのサイズがデフォルトで 30,000,000 バイトに制限されます。「要求フィルター」は、Microsoft Internet Information Services をインストールする際にデフォルトでインストールされます。

パスワードの設定

項目		内容	設定できる値	デフォルト
エージェント保護の設定	利用者のエージェントの設定変更とアンインストールを、パスワードで保護する	利用者にエージェントのセットアップ内容の変更やアンインストールがされないように、パスワードを設定するかどうかを設定します。	チェックする エージェントのセットアップとアンインストール時にパスワードを要求します。 チェックしない エージェントのセットアップとアンインストール時にパスワードを要求しません。	チェックする
	パスワード	エージェントのセットアップおよびアンインストール時に要求するパスワードを指定します。	1～128 文字の ASCII コードの文字列	（空白）
	パスワード確認	確認のため、指定したパスワードを再度入力します。		

項目		内容	設定できる値	デフォルト
外部記憶媒体を使用した情報通知の保護設定※	外部記憶媒体を使用した情報通知を、パスワードで保護する	利用者に外部記憶媒体を使用した情報通知をされないための、パスワードを設定するかどうかを設定します。	チェックする 外部記憶媒体を使用した情報通知時にパスワードを要求します。 チェックしない 外部記憶媒体を使用した情報通知時にパスワードを要求しません。	チェックしない
	パスワード	外部記憶媒体を使用した情報通知時に要求するパスワードを指定します。	1～128 文字の ASCII コードの文字列	(空白)
	パスワード確認	確認のため、指定したパスワードを再度入力します。		
USB デバイス登録の保護設定	USB デバイスの登録を、パスワードで保護する	利用者に USB デバイスを登録されないための、パスワードを設定するかどうかを設定します。	チェックする USB デバイスの登録時にパスワードを要求します。 チェックしない USB デバイスの登録時にパスワードを要求しません。	チェックしない
	パスワード	USB デバイスの登録時に要求するパスワードを指定します。	1～128 文字の ASCII コードの文字列	(空白)
	パスワード確認	確認のため、指定したパスワードを再度入力します。		

注※　JP1/IT Desktop Management 10-01 より前のバージョンから JP1/IT Desktop Management 2 にバージョンアップした場合は、[エージェント保護の設定] で設定したパスワードが自動で設定されます。

中継システムの設定

項目			内容	設定できる値	デフォルト
ID 登録先システムの設定	管理用サーバ	ホスト名または IP アドレス	ID への登録をする上位システムのホスト名または IP アドレスとして、[基本設定] の [管理用サーバ] で指定したホスト名または IP アドレスが表示されます。	なし	なし
	ID 登録先システム	システム種別	ID 登録先システムの種別を選択します。	• 管理用サーバ • 中継システム	中継システム
		ホスト名または IP アドレス	[ID 登録先システム] の [システム種別] で選択したシス	ホスト名※2 または IPv4 形式の IP アドレス	localhost

項目			内容	設定できる値	デフォルト
ID 登録先システムの設定	ID 登録先システム	ホスト名または IP アドレス	テムの、ホスト名または IP アドレスを指定します。※1 中継システムに割り当てるエージェント設定を作成する場合に、[ID 登録先システム] の [システム種別] で [中継システム] を選択したときは、「localhost」を指定することをお勧めします。	ホスト名※2 または IPv4 形式の IP アドレス	localhost
運用キーの設定			リモートインストールマネージャを使用した配布時に使用する、運用キー（コンピュータを識別するための情報）を選択します。	• ホスト名 この場合、ジョブの作成または実行時にアドレス解決する方法として、ドロップダウンリストから、[Windows ネットワークを使用する] または [IT Desktop Management 2 のシステム構成情報を使用する] を選択します（デフォルト：Windows ネットワークを使用する）。 • IP アドレス	管理用サーバのセットアップで、[アドレス解決の設定] 画面に指定した種類の情報（ホスト名または IP アドレス）
JP1/IT Desktop Management 2 - Manager への通知設定	処理結果ファイルの送信タイミング		下位システムから受信した通知ファイルを、配布管理システムに送信するタイミングを設定します。	• すぐに送信する • 定期的に送信する	すぐに送信する
	ジョブの受信と、処理の結果ファイルの送信を、並列実行する		中継システムが接続する上位システム（管理用サーバ）との間で、ジョブの受信（ダウンロード）と上位システムへの通知ファイルの送信（アップロード）を並行して実行するかどうかを設定します。	チェックする ジョブの受信と、処理の結果ファイルの送信を並行して実行します。 チェックしない ジョブの受信と、処理の結果ファイルの送信を並行して実行しません。	チェックする
	下位の JP1/IT Desktop Management 2 - Agent の分割配布の実行状況を、JP1/IT Desktop Management 2 - Manager に通知する		パッケージを分割配布する場合に、下位システムで実行中の分割配布の進行状況を上位システムへ通知するかどうかを設定します。	チェックする 分割配布の進行状況を上位システムへ通知します。	チェックしない

項目		内容	設定できる値	デフォルト
JP1/IT Desktop Management 2 - Manager への通知設定	下位の JP1/IT Desktop Management 2 - Agent の分割配布の実行状況を、JP1/IT Desktop Management 2 - Manager に通知する	パッケージを分割配布する場合に、下位システムで実行中の分割配布の進行状況を上位システムへ通知するかどうかを設定します。	チェックしない 分割配布の進行状況を上位システムへ通知しません。	チェックしない
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	中継システムに同時に接続できるエージェントの数を指定します。	4～1000※3	50
	JP1/IT Desktop Management 2 - Agent へのジョブダウンロード要求数	ジョブを実行するときに、同時に処理するエージェントの数※4 を指定します。	同時にジョブダウンロード要求を実行する数を設定する 同時に実行指定するジョブの数を 1～9999 で指定します。 ジョブダウンロード要求を実行しない エージェントに対して起動電文を送信しないため、ジョブの実行や、クライアント制御を利用したエージェントの起動ができなくなります。	同時実行する数を指定してジョブを実行する（20）
	ジョブの管理ファイルのキャッシュ	実行されたジョブの情報（管理ファイル）を、中継システムのメモリ上にキャッシュする上限サイズ※5 を指定します。	キャッシュサイズの上限値を指定する メモリ上にキャッシュする上限サイズを 1～1000000KB で指定します。 キャッシュしない 実行されたジョブの情報（管理ファイル）をキャッシュしません。	キャッシュサイズの上限値を指定する（100000KB）
	ジョブ実行時に、JP1/IT Desktop Management 2 - Agent の起動を監視する	エージェントが起動していないためにジョブが実行されない場合、ジョブ実行状態を「起動失敗」に変更し、それを配布管理システムに通知するかどうかを設定します。	チェックする 正常終了した ID ジョブのエージェントでの実行結果を中継システムに通知します。 チェックしない 正常終了した ID ジョブのエージェントでの	チェックする

項目		内容	設定できる値	デフォルト
中継システムの処理の設定	ジョブ実行時に、JP1/IT Desktop Management 2 - Agent の起動を監視する	エージェントが起動していないためにジョブが実行されない場合、ジョブ実行状態を「起動失敗」に変更し、それを配布管理システムに通知するかどうかを設定します。	実行結果を中継システムに通知しません。	チェックする
	起動失敗要因を細分化する	エージェントが起動に失敗した場合に、その要因を細分化して配布管理システムに通知するかどうかを設定します。	チェックする 起動失敗要因を細分化します。 チェックしない 起動失敗要因を細分化しません。	チェックする

注　Citrix XenApp、Microsoft RDS サーバの場合、中継システムはサポートしていません。

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］で指定する運用キーの内容に一致させてください。

注※2　64 文字以内の半角文字列で指定します。

注※3　JP1/IT Desktop Management 10-10 以前、または JP1/IT Desktop Management 2 10-50 からバージョンアップした直後の場合、中継システムへの同時接続 JP1/IT Desktop Management 2 - Agent 数が上限値を超えて設定されていることがあります。この場合、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］画面で該当するエージェント設定の［編集］ボタンをクリックしたときに、上限値の変更を促すダイアログが表示されます。

注※4　具体的には、配布管理システムが、エージェントに対して起動電文を一度に送信する数となります。ここで指定した値よりも多くのエージェントに対してジョブを実行すると、この指定値に応じて分割して実行されます。0 を指定すると下位システムへ起動電文を送信しなくなり、上位システム主導のジョブの実行や、クライアント制御を利用したあて先の起動ができなくなります。なお、配布するファイルの容量が大きい（10 メガバイト以上）と、少数のエージェントの接続でも負荷が高くなることがありますので、ネットワークの性能に合わせた値を指定してください。

注※5　上限サイズを超える管理ファイルが発生すると、ジョブ処理のスループットが低下します。ジョブ処理のスループットの低下を回避するために、管理ファイルのキャッシュの上限サイズは運用規模に応じて適切な値を指定することをお勧めします。指定する値の目安は、次の計算式の各項目の見積もり値を基に算出してください。なお、管理ファイルの増加によって上限サイズを超える場合は、最も参照頻度の低い管理ファイルを削除してから、新しい管理ファイルをキャッシュします。［キャッシュしない］にした場合、エージェントからのポーリング要求のたびに、ディスク上のジョブ管理ファイルにアクセスすることになるため、エージェントへの応答が遅れることがあります。

管理ファイルのキャッシュサイズ（キロバイト）＝中継システムに保管されている実行されたジョブ数×各ジョブのあて先数×各ジョブのパッケージ数（リモートインストールのジョブの場合）×1 キロバイト

利用者への通知設定

項目		内容	設定できる値	デフォルト
コンピュータのシャットダウンと再起動の設定※1	利用者のコンピュータに、シャットダウンまたは再起動を指示するダイアログを表示する	管理者によるコンピュータのシャットダウンと再起動の指示を、利用者のコンピュータが受け付けるようにするかどうかを指定します。※2	チェックする 管理者によるコンピュータのシャットダウンと再起動の指示を受け付けます。 チェックしない 管理者によるコンピュータのシャットダウンと再起動の指示を受け付けません。	チェックする
	シャットダウンと再起動の開始タイミング	更新プログラムや再起動が必要なプログラムを配布する場合に、利用者のコンピュータがシャットダウンや再起動を開始するタイミングを設定します。	指定する時間内に利用者の応答がない場合に、自動的に開始する シャットダウンや再起動が自動的に開始されます。自動的に開始されるまでの時間を 1 分～1440 分で指定します。※3 シャットダウンまたは再起動を指示するダイアログでの、利用者の応答に従う 利用者が応答するまで、シャットダウンや再起動は、開始されません。	指定する時間内に利用者の応答がない場合に、自動的に開始する（3 分）
利用者のコンピュータでの表示設定	アクション項目の利用者へのメッセージ通知時	セキュリティポリシーのアクション項目で設定するセキュリティ判定結果のメッセージを利用者が受信した時に、利用者のコンピュータにバルーンヒントを表示するかどうかを設定します。※4	表示（バルーンヒント） 利用者のコンピュータにバルーンヒントを表示します。 非表示 利用者のコンピュータにバルーンヒントを表示しません。	表示（バルーンヒント）
	利用者へのコンピュータ再起動の指示時	セキュリティポリシーやソフトウェアなどの適用などによってコンピュータの再起動が必要になった時に、利用者のコンピュータにバルーンヒントを表示するかどうかを設定します。※4	表示（バルーンヒント） 利用者のコンピュータにバルーンヒントを表示します。 非表示 利用者のコンピュータにバルーンヒントを表示しません。	表示（バルーンヒント）

項目		内容	設定できる値	デフォルト
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	システム管理者から利用者情報の入力を要求されたことを、利用者のコンピュータに表示するかどうかを設定します。※4	表示（利用者入力画面） 利用者のコンピュータに利用者情報の入力画面を表示します。 表示（バルーンヒント） 利用者のコンピュータにバルーンヒントを表示します。 非表示 利用者のコンピュータに、利用者情報の入力画面もバルーンヒントも表示しません。	表示（バルーンヒント）
	パッケージの配布時（ITDM互換配布）	ソフトウェアの配布が実行された時に、利用者のコンピュータにバルーンヒントを表示するかどうかを選択します。※4	表示（バルーンヒント） 利用者のコンピュータにバルーンヒントを表示します。 非表示 利用者のコンピュータにバルーンヒントを表示しません。	表示（バルーンヒント）
通知ダイアログの表示設定	ジョブの実行に失敗した場合に表示する	ジョブが失敗した場合に、利用者のコンピュータに通知ダイアログを表示するかどうかを設定します。※5	チェックする 利用者のコンピュータに通知ダイアログを表示します。 チェックしない 利用者のコンピュータに通知ダイアログを表示しません。	チェックしない
	［ITDM2_Startup］からの起動に失敗したショートカットがある場合、ショートカットの削除確認を表示する	［ITDM2_Startup］フォルダに登録されているプログラムのうち、実行できないアイコンやショートカットがある場合に、それらの削除について確認するダイアログを表示するかどうかを設定します。※6、※7	チェックする 実行できないアイコンやショートカットの削除について確認するダイアログを表示します。 チェックしない 実行できないアイコンやショートカットの削除について確認するダイアログを表示しません。	チェックしない

注※1　中継システムの場合は、設定が無視されます。

注※2　Citrix XenApp、Microsoft RDS サーバの場合、シャットダウンまたは再起動を指示するダイアログの表示はサポートしていないため、「チェックしない」を設定してください。

注※3　ここで設定した時間が経過するまでの間、利用者のコンピュータに確認ダイアログが表示されます。

注※4　Citrix XenApp、Microsoft RDS サーバの場合、バルーンヒントの表示はサポートしていないため、「非表示」を設定してください。

注※5　Citrix XenApp、Microsoft RDS サーバの場合、ジョブの実行に失敗したときの通知ダイアログの表示はサポートしていないため、「チェックしない」を設定してください。

注※6　［ITDM2_Startup］フォルダに登録されているプログラムの実行ファイルがすでにアンインストールされていて、実行できないことがあります。この場合、実行できないアイコンやショートカットを削除するかどうかを確認するダイアログを表示させることができます。

注※7　Citrix XenApp、Microsoft RDS サーバの場合、実行できないアイコンやショートカットの削除について確認するダイアログの表示はサポートしていないため、「チェックしない」を設定してください。

ジョブの設定

項目		内容	設定できる値	デフォルト
ジョブの処理中ダイアログの表示設定	処理中ダイアログを表示する	エージェントでのダウンロードやインストールの処理の実行中に、処理中であることを示すダイアログを表示するかどうかを設定します。※1	チェックする ダウンロードやインストールの処理中であることを示すダイアログを表示します。 チェックしない ダウンロードやインストールの処理中であることを示すダイアログを表示しません。	チェックする
	パッケージのダウンロード処理中を示すダイアログを表示する	パッケージのダウンロード処理中であることを示すダイアログを表示するかどうかを設定します。	チェックする パッケージのダウンロード処理中であることを示すダイアログを表示します。 チェックしない パッケージのダウンロード処理中であることを示すダイアログを表示しません。	チェックする
	表示するダイアログ	ダウンロード処理中であることを示すダイアログの形式を指定します。	デフォルトのダイアログ JP1/IT Desktop Management 2 が標準で提供しているダイアログを表示します。 プログラムで指定したダイアログ 指定したユーザ作成のダイアログ表示用プログラムを起動して表示します。	デフォルトのダイアログ

項目		内容	設定できる値	デフォルト
ジョブの処理中ダイアログの表示設定	パッケージのインストール処理中を示すダイアログを表示する	パッケージのインストール処理中であることを示すダイアログを表示するかどうかを設定します。	チェックする パッケージのインストール処理中であることを示すダイアログを表示します。 チェックしない パッケージのインストール処理中であることを示すダイアログを表示しません。	チェックする
	表示するダイアログ	インストール処理中であることを示すダイアログの形式を指定します。	デフォルトのダイアログ JP1/IT Desktop Management 2 が標準で提供しているダイアログを表示します。 プログラムで指定したダイアログ 指定したユーザ作成のダイアログ表示用プログラムを起動して表示します。	デフォルトのダイアログ
	ダイアログを最前面に表示する	インストール処理中であることを示すダイアログを最前面に表示するかどうかを指定します。	チェックする インストール処理中であることを示すダイアログを最前面に表示します。 チェックしない インストール処理中であることを示すダイアログを最前面に表示しません。	チェックしない
	ダイアログを表示するためのプログラム	表示するダイアログの形式として［プログラムで指定したダイアログ］を選択した場合、ダイアログを表示するためのプログラム名を指定します。	ユーザが作成したダイアログ表示用プログラム※2（拡張子が exe のプログラムファイル）のパス名	（空白）
リモートインストールまたはリモートコレクトがエラーになった場合のリトライ設定	リトライする	ユーザプログラム・データのリモートインストールまたはリモートコレクトの処理中にエラーが発生した場合にリトライするかどうかを設定します。	チェックする リトライします。 チェックしない リトライしません。	チェックする
	リトライ回数	リトライする回数を指定します。	1～100	10
	リトライ間隔	リトライの間隔を指定します。	定期的にリトライする 間隔を置く秒数を 1～3600 で指定します。	定期的にリトライする （1 秒）

項目		内容	設定できる値	デフォルト
リモートインストールまたはリモートコレクトがエラーになった場合のリトライ設定	リトライ間隔	リトライの間隔を指定します。	すぐにリトライする 間隔を置かないで、指定した回数リトライします。	定期的にリトライする（1 秒）
パッケージの分割配布の設定	分割配布する※3	配布されたパッケージがここで指定したサイズより大きい場合、分割して配布するかどうかを指定します。	チェックする ここで指定したサイズに分割して配布されます。 チェックしない 分割しないままで配布されます。	チェックする
	分割サイズ	パッケージを分割するサイズを指定します。 この分割サイズは、配布されるパッケージごとに適用されます。	キロバイトで指定する場合 1～2097151 メガバイトで指定する場合 1～2047	2097151KB
	配布休止時間	パッケージが分割配布される場合の、配布と配布の間のインターバル（休止時間）を指定します。	1～1440	60
インストール待ち時間の設定	インストーラーからの応答待ち時間	日立プログラムプロダクトをリモートインストールした場合に、インストーラーからの応答を待つ最大時間を指定します。 指定した時間を過ぎても応答がない場合は、上位システムにエラーが通知されます。	180～7200	1800
ジョブの保留許可の設定※4	利用者による、ジョブの保留を許可する	上位システムからジョブが転送されたときに、そのジョブを実行するかどうかを利用者に選択させるかどうかを設定します。※5	チェックする ジョブを実行するかどうかを利用者に選択させます。※6 チェックしない ジョブを実行するかどうかを利用者に選択させません。	チェックしない
	保留を解除するタイミング	ジョブを実行するかどうかを利用者に選択させる場合で、ジョブの実行を一時的に保留するとき、保留を解除するタイミングを指定します。	指定する時間内に利用者の応答がない場合に、自動的に解除する ジョブ実行の保留を解除するまでの時間を、1～1800秒で指定します。※7	指定する時間内に利用者の応答がない場合に、自動的に解除する（180秒）

項目		内容	設定できる値	デフォルト
ジョブの保留許可の設定※4	保留を解除するタイミング	ジョブを実行するかどうかを利用者に選択させる場合で、ジョブの実行を一時的に保留するとき、保留を解除するタイミングを指定します。	利用者の応答があるまで解除しない 利用者の応答があるまでジョブの実行を待ちます。※8	指定する時間内に利用者の応答がない場合に、自動的に解除する（180秒）
通知抑止の設定	リモートインストール待ち、または収集待ちとなっている通知を抑止する	実行状態がリモートインストール待ち、または収集待ちとなっているジョブの上位システムへの通知を抑止するかどうかを設定します。※9	チェックする 上位システムへの通知を抑止します。 チェックしない 上位システムへの通知を抑止しません。	チェックしない
インターバル転送の設定	インターバル転送をする	エージェントへのファイル転送が発生する場合、指定した単位ごとにファイルを分割し、インターバルを置いて実行するかどうかを設定します。	チェックする インターバル転送をします。 チェックしない インターバル転送をしません。	チェックしない
	連続転送バッファ数	1 度にファイル転送するバッファの個数を指定します。	1～4294967295	1
	転送インターバル	インターバル転送する時の、転送と転送との間のインターバル（休止時間）をどのくらいにするかを指定します。	1～4294967295	1000

注※1　Citrix XenApp、Microsoft RDS サーバの場合、ジョブの処理中ダイアログの表示はサポートしていないため、「チェックしない」を設定してください。

注※2　ユーザが作成するダイアログ表示用プログラムは、次に示すパラメーターやウィンドウ名などの条件に従っていれば、表示される画面はダイアログでなくてもかまいません。なお、設定ミスなどによって指定したユーザプログラムによるダイアログが正しく表示されない場合でも、ユーザプログラムの動作に関係なく処理は続行されます。

ダイアログ表示用プログラムに渡される引数（NULL で終わる文字列）の形式を次に示します。ユーザプログラム作成時の参考にしてください。

形式

パラメーター1△パラメーター2△パラメーター3△パラメーター4

パラメーター 1

最前面表示オプション（半角で 1 文字）を指定します。

1：最前面表示をしない

2：最前面表示をする

パラメーター 2

処理中ダイアログの種別（半角で 1 文字）を指定します。

1：ダウンロード中ダイアログ

2：インストール中ダイアログ

パラメーター 3

パッケージ識別 ID（半角で 1～44 文字）

パラメーター 4

パッケージ名称（半角で 1～50 文字、全角で 1～25 文字）

指定例

表示するダイアログごとの指定例を次に示します。

- ダウンロード中ダイアログ

  1 1 *パッケージ識別ID パッケージ名称*

- インストール中ダイアログ（最前面表示をしない場合）

  1 2 *パッケージ識別ID パッケージ名称*

- インストール中ダイアログ（最前面表示をする場合）

  2 2 *パッケージ識別ID パッケージ名称*

表示させるダイアログのウィンドウ名

ウィンドウ名は次のようにしてください。これ以外のウィンドウ名を設定すると、ダイアログを非表示にできなくなります。また、ウィンドウ名内のカタカナは、半角で作成してください。

- ダウンロード中ダイアログ

  [IT Desktop Management 2 - ダウンロード]

- インストール中ダイアログ

  [IT Desktop Management 2 - インストール]

ダイアログの表示停止は、JP1/IT Desktop Management 2 からユーザプログラムに対して PostMessage 関数（WM_CLOSE 指定）を発行して指示します。また、PostMessage 関数を発行したあと、TerminateProcess 関数を発行してユーザプログラムのプロセスを停止します。

注※3　ネットワークの負荷を軽減したい場合に設定してください。なお、分割配布が設定されているパッケージが配布されても、このチェックボックスがオフの場合には、分割配布されません。

注※4　中継システムの場合は、設定が無視されます。

注※5　Citrix XenApp、Microsoft RDS サーバの場合、利用者によるジョブの保留はサポートしていないため、「チェックしない」を設定してください。

注※6　上位システムからジョブが転送されたときに、[JP1/IT Desktop Management 2 ジョブの保留] ダイアログが表示され、そのジョブを実行するかどうかを選択できます。ジョブを即時に実行したくない

場合にジョブの実行を一時的に保留できます。なお、保留の対象となるのは、GUI インストールモードの「パッケージのインストール」ジョブだけです。ただし、実行日時（パッケージのインストール日時またはジョブの実行日時）が指定されている場合は保留できません。

注※7　指定した秒数は［JP1/IT Desktop Management 2 ジョブの保留］ダイアログに、実行までの残り秒数として表示され、0 になると、表示されたジョブの動作を自動的に実行して、ダイアログが閉じます。

注※8　利用者が操作するまで［JP1/IT Desktop Management 2 ジョブの保留］ダイアログが表示されたままとなります。

注※9　通常、ジョブの配布完了後、インストールや収集の完了（またはエラー）を上位システムに通知するまでには間があるため、通知ごとに［ジョブ実行状況］ウィンドウの表示が変わります。しかし、リモートインストール待ちまたは収集待ちであることを通知した直後に「完了」または「エラー」の通知をすることもあります。通知を抑止していると、このような場合に、通知 1 回につき 170 バイト（ID ジョブの場合 340 バイト）の通信量が削減できるため、ネットワークの負荷を軽減できます。また、上位システムでのジョブ実行状態の更新処理も削減できます。なお、通知を抑止できるジョブの種別は、次のとおりです。

- パッケージのインストール
- リモートコレクト
- 中継までのリモートコレクト

通知が抑止されるのは、これらのジョブの実行時に次表の「ジョブの指定」をした場合で、かつ「抑止する条件」をすべて満たしたときです。

ジョブの指定			抑止する条件
「インストール日時」	「システム起動時インストール」	「GUI インストールモード」	
○※1	×	×	ジョブの配布が完了した時点で指定日時が経過した。
×	○	×	• エージェントで［ポーリングのタイミング］に［システム起動前］を設定した。 • システム起動時のポーリングの際にジョブが配布された。
○	○	×	• エージェントで［ポーリングのタイミング］に［システム起動前］を設定した。 • システム起動時のポーリングの際にジョブが配布された。 • ジョブの配布が完了した時点で指定日時が経過した。
×	×	○※2	ジョブの配布が完了した時点でエージェントがログオン済み。
○	×	○※2	• ジョブの配布が完了した時点で指定日時が経過した。 • ジョブの配布が完了した時点でエージェントがログオン済み。

ジョブの指定			抑止する条件
「インストール日時」	「システム起動時インストール」	「GUI インストールモード」	
×	○	○※2	• エージェントで［ポーリングのタイミング］に［システム起動前］を設定した。 • システム起動時のポーリングの際にジョブが配布された。 • ジョブの配布が完了した時点でエージェントがログオン済み。
○	○	○※2	• エージェントで［ポーリングのタイミング］に［システム起動前］を設定した。 • システム起動時のポーリングの際にジョブが配布された。 • ジョブの配布が完了した時点で指定日時が経過した。 • ジョブの配布が完了した時点でエージェントがログオン済み。

（凡例） ○：指定する　×：指定しない

注※1 「リモートコレクト」ジョブおよび「中継までのリモートコレクト」ジョブは抑止の対象外です。

注※2 「パッケージのインストール」ジョブの場合だけ抑止の対象になります。

通信設定

項目		内容	設定できる値	デフォルト
複数の上位システムへのポーリングの設定※1	複数の上位システムにポーリングする	配布管理システムからのジョブの実行経路が複数ある場合に、複数の上位システムにポーリング（配布管理システムからの指示の監視）するかどうかを設定します。※2 ポーリング対象として設定できる上位システムは次のとおりです。 • 管理用サーバ • 中継システム 次のような場合は、複数の上位システムにポーリングする設定にしないでください。 • 中継システムに割り当てるエージェント設定を作成する場合 • デフォルトエージェント設定を編集する場合	チェックする 複数の上位システムにポーリングします。 ポーリング対象とする上位システムを追加するには、［追加］ボタンをクリックし、表示されるダイアログで、上位システムのホスト名または IP アドレス、種別、優先順位を指定します。 追加した上位システムは、［ポーリング対象とする上位システム］に優先順位の高いものから順に表示されます。※3 チェックしない 複数の上位システムにポーリングしません。	チェックしない

項目		内容	設定できる値	デフォルト
複数の上位システムへのポーリングの設定※1	複数の上位システムへのポーリング形態	ポーリング対象の上位システムとしている中継システムが障害などで接続できなくなった場合のポーリング形態をドロップダウンリストから選択します。	ホットスタンバイ ［ポーリング対象とする上位システム］に表示されている上位システムの優先順位の高いものから順番にポーリングし、接続できた上位システムを、その後のポーリングの上位システムとして認識します。※4 ポーリング対象とする上位システムを追加するには、［追加］ボタンをクリックし、表示されるダイアログで、上位システムのホスト名または IP アドレス、種別、優先順位を指定します。 システム起動時（第 1 回目）のポーリング形態については次の 3 種類からを選択します。 • システム起動時に、すべての上位システムにポーリングする • システム起動時に、［優先順］が「1」の上位システムだけにポーリングする • システム起動時に、［優先順］に従ってポーリングする マルチホスト すべての上位システムにポーリングします。	ホットスタンバイ（システム起動時に、すべての上位システムにポーリングする）
実行要求を受信するための通信プロトコル	上位システムへの接続に、受信した IP アドレスを使用する※5	上位システムを名前解決できないときにも上位システムに接続できるようにするかどうかを設定します。	チェックする 上位システムからの実行要求情報を受信したタイミングで実行要求情報中の IP アドレスが保管されるので、上位システムに接続できます。 チェックしない 上位システムを名前解決できないときには上位システムに接続できません。	チェックする

項目		内容	設定できる値	デフォルト
通信エラーの設定	通信エラーと見なすタイミング	エージェントが、通信ソフトからの応答を待って、通信エラーと見なすかどうかを指定します。	指定した時間内に通信ソフトからの応答がない場合、通信エラーと見なす 通信ソフトからの応答待ちの時間を 1～120 分で指定します。※6※12 通信ソフトからの応答を監視しない 通信ソフトからの応答を監視しません。	指定した時間内に通信ソフトからの応答がない場合、通信エラーと見なす（5 分）
エラー発生時のリトライ設定	ソケットコネクションの確立エラー発生時と、上位システムからのファイル転送エラー発生時に、リトライする	ソケットコネクション確立に失敗した場合、および上位システムからエージェントへのファイル転送中に通信障害が発生した場合に、リトライするかどうかを設定します。※7	チェックする リトライします。 チェックしない リトライしません。	チェックする
	リトライ回数	ソケットコネクション確立に失敗した場合、ファイル転送中に通信障害が発生した場合のリトライの回数を指定します。	1～999	5
	リトライ間隔	ソケットコネクション確立に失敗した場合、ファイル転送中に通信障害が発生した場合のリトライの間隔（秒）を指定します。	1～7200	5
未送信の処理結果ファイル	上位システムに未送信の処理結果ファイルを再送する	上位システムに送信していない通知ファイルがある場合に、送信のリトライをするかどうかを設定します。	チェックする リトライします。 チェックしない リトライしません。	チェックする
	リトライ回数	上位システムに送信していない通知ファイルがある場合の送信リトライの回数を指定するかどうかを設定します。	指定する リトライする回数を 1～300 回で指定します。 無制限とする 送信していない通知ファイルがなくなるまでリトライします。	指定する（2）
	リトライ間隔	上位システムに送信していない通知ファイルがある場合の送信リトライの間隔（秒）を指定します。※8	60～3600	300

項目			内容	設定できる値	デフォルト
マルチキャスト配布の設定（リモートインストールマネージャを使用した配布）	ジョブの送信時、マルチキャストアドレスを使用する		リモートインストールマネージャを使用した配布のジョブ送信に、マルチキャストアドレスを使用をするかどうかを設定します。	チェックする リモートインストールマネージャを使用した配布のジョブ送信に、マルチキャストアドレスを使用します。 チェックしない リモートインストールマネージャを使用した配布のジョブ送信に、マルチキャストアドレスを使用しません。	チェックしない
	マルチキャストアドレス		「マルチキャスト配布」が指定されたジョブの送信で使用するマルチキャストアドレスを指定します。 接続先の上位システムに設定されたマルチキャストアドレスと同じ値を設定してください。※9	224.0.1.0～ 239.255.255.255	238.255.0.1
	ジョブ送信パケットサイズの上限値		ジョブを配布するときの、1パケット分のサイズを指定します。	1～60	40※10
	ジョブの受信時、マルチキャストアドレスを使用する		リモートインストールマネージャを使用した配布のジョブ受信に、マルチキャストアドレスを使用をするかどうかを設定します。	チェックする リモートインストールマネージャを使用した配布のジョブ受信に、マルチキャストアドレスを使用します。 チェックしない リモートインストールマネージャを使用した配布のジョブ受信に、マルチキャストアドレスを使用しません。	チェックしない
	ポート番号	通常の受信時	マルチキャスト配布のジョブを受信するのに使用するポート番号を指定します。	1～65535	管理用サーバのセットアップで、[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] 画面の［マルチキャスト配布］－［ポート番号］－［マルチキャスト配

項目			内容	設定できる値	デフォルト
マルチキャスト配布の設定（リモートインストールマネージャを使用した配布）	ポート番号	通常の受信時	マルチキャスト配布のジョブを受信するのに使用するポート番号を指定します。	1～65535	布］に指定したポート番号
		再送の場合の受信時	マルチキャスト配布中にパケットの再送が発生した場合に使用するポート番号を指定します。※11	1～65535	管理用サーバのセットアップで、［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］画面の［マルチキャスト配布］－［ポート番号］－［マルチキャスト配布（再送要求時）］に指定したポート番号
	マルチキャストアドレス		「マルチキャスト配布」が指定されたジョブの受信で使用するマルチキャストアドレスを指定します。 接続先の上位システムに設定されたマルチキャストアドレスと同じ値を設定してください。※9	224.0.1.0～ 239.255.255.255	238.255.0.1

注※1

中継システムの場合は、設定が無視されます。

注※2

通常、配布管理システムからの指示によって、エージェントは要求された処理を実行します。しかし、通信障害や、エージェントが起動していなかったなどの要因で、配布管理システムからの指示が届かない場合があります。このようなとき、ポーリングすることで、指示を受信するようになります。クライアント制御を利用する場合は、ポーリングすることをお勧めします。また、低速な WAN を使用している場合は、ポーリングしないことで、むだなデータ送受信を少なくできます。

注※3

［ポーリング対象とする上位システム］に表示される優先順が 1 位の上位システムは、［基本設定］の［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］に設定した値と常に等しくなるように連動しています。

注※4

ポーリング対象の上位システムが接続できなくなると、そのつど優先順位 1 位の上位システムから順番にポーリングし、ポーリング対象の上位システムを決定します。

注※5

- 運用キーが IP アドレスの場合は設定不要です。

- 上位システムがクラスタシステムの場合、正しく接続できないことがあります。
- 上位システムが複数のネットワークアダプタを使用した環境では、正しく接続できないことがあります。

注※6

エージェントがファイルをダウンロードする処理などを監視できます。

注※7

リトライすると、ファイル転送が中断された時点のファイルから転送が再開されます。通信障害が発生した以前のファイルは再転送されないため、むだな通信量が削減できます。なお、ここで指定したリトライ回数と間隔は、ユニキャスト配布の場合に有効になります。

注※8

上位システムに送信していない通知ファイルがある場合の送信リトライの間隔は、システムの要件に応じた値を指定してください。例えば、セキュリティ監査を行うシステムでは、クライアントからの情報が即時に必要となるため小さい値を指定します。

注※9

接続先の上位システムに設定されたマルチキャストアドレスと同じ値を設定することで、その上位システムが配布先とするマルチキャストグループに登録したことになります。

注※10

40 キロバイトは、100BASE の通信回線で効率的な値です。通信回線が 10BASE の場合は 4 キロバイトを設定してください。パケットサイズが大き過ぎると、マルチキャスト配布に失敗し、途中からユニキャスト配布になりますので、ご注意ください。

注※11

マルチキャスト配布は UDP プロトコルを使用するため、配布中にパケットの再送が発生するので、再送要求のポート番号も設定が必要です。

注※12

［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を経由して上位システムと HTTPS 通信する］を有効にする場合は、［通信エラーと見なすタイミング］に 30 分を設定してください。ただし、リモートコレクト機能で 1GB を超えるような容量の大きいファイルを収集する場合は 120 分を設定してください。設定を大きくすると、通信障害・サーバ障害など一時障害によりサーバからの応答がない場合にエラーと判断されるまでに時間がかかるため、次のポーリングまでの時間が長くなります。

スタートアップの設定

項目	内容	設定できる値	デフォルト
IT Desktop Management 2 独自のスタートアップフォルダ（[ITDM2_Startup]）を作成する※1	Windows の［スタートアップ］グループに登録されたプログラムを移動させるための、「ITDM2_Startup」フォルダを作成するかどうかを設定します。※2	チェックする 「ITDM2_Startup」フォルダを作成します。	チェックしない

項目	内容	設定できる値	デフォルト
IT Desktop Management 2 独自のスタートアップフォルダ（[ITDM2_Startup]）を作成する※1	Windows の［スタートアップ］グループに登録されたプログラムを移動させるための、「ITDM2_Startup」フォルダを作成するかどうかを設定します。※2	チェックしない 「ITDM2_Startup」フォルダを作成しません。	チェックしない
スタートアッププログラムを［ITDM2_Startup］に移行する	「ITDM2_Startup」フォルダを作成する場合に、エージェントで Windows の［スタートアップ］グループに登録されたプログラムを自動的に「ITDM2_Startup」フォルダに移動させるかどうかを指定します。	チェックする Windows の［スタートアップ］グループに登録されたプログラムを自動的に「ITDM2_Startup」フォルダに移動させます。 特定のプログラムを「ITDM2_Startup」フォルダに移動させたい場合は、［追加］ボタンをクリックすると表示されるダイアログで指定できます。指定したプログラムは、［移行するスタートアッププログラム（ショートカット）］に表示されます。 チェックしない Windows の［スタートアップ］グループに登録されたプログラムを自動的に「ITDM2_Startup」フォルダに移動させません。	チェックしない

注※1 ［ITDM2_Startup］フォルダは、デフォルトでは作成されていません。

注※2 「ITDM2_Startup」フォルダに Windows の［スタートアップ］グループに登録されたプログラムを移動させると、「システム起動時インストール」が設定されたパッケージのインストールと Windows の［スタートアップ］グループに登録されたプログラムの起動がエージェントでバッティングして、「システム起動時インストール」が設定されたパッケージのインストールが失敗するのを回避できます。

AMT の設定

項目	内容	設定できる値	デフォルト
IDE リダイレクションを有効にする	AMT の IDE リダイレクション機能を利用して、リモートコントロール時にリモート CD-ROM 機能を利用するかどうかを設定します。	チェックする リモート CD-ROM 機能を利用します。 チェックしない リモート CD-ROM 機能を利用しません。	チェックしない

項目	内容	設定できる値	デフォルト
リモート KVM を有効にする	AMT のリモート KVM 機能を利用して、RFB 接続でコンピュータをリモートコントロールできるようにするかどうかを設定します。	チェックする RFB 接続でコンピュータをリモートコントロールできるようにします。 チェックしない RFB 接続でコンピュータをリモートコントロールできるようにしません。	チェックしない
パスワード	接続先のコンピュータのリモート KVM 機能を使用するためのパスワードを指定します。	半角英数で 8 文字の文字列※	（空白）
パスワード確認	確認のため、指定したパスワードを再度入力します。	半角英数で 8 文字の文字列※	（空白）
接続時に利用者の許可を求める	コンピュータへの接続時に、利用者に接続許可を求めるダイアログを表示させるかどうかを設定します。	チェックする 対象のコンピュータに接続許可を求めるダイアログを表示できるようにします。 チェックしない 対象のコンピュータに接続許可を求めるダイアログを表示できるようにしません。	チェックする
ダイアログの表示時間	接続時に利用者の許可を求めるダイアログの表示時間（秒）を指定します。	10～4095	300
セッションタイムアウト	コンピュータに接続できない場合に、タイムアウトするかどうかを選択します。	する タイムアウトします。タイムアウトまでの待ち時間（分）を 1～255 で指定します。 しない タイムアウトしません。	しない
デフォルトスクリーン	接続先のコンピュータがデュアルディスプレイの場合に、どちらのディスプレイを表示するかを選択します。	• プライマリ • セカンダリ	プライマリ

注※

次に示す 4 種類の文字を、それぞれ 1 文字以上使用する必要があります。

- 英大文字
- 英小文字

- 数字
- 「"」「,」「:」以外の記号

リモートコントロールの設定

項目		内容	設定できる値	デフォルト
開始時と終了時の処理	自動起動する	エージェント起動時に、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。	チェックする 自動的に起動します。 チェックしない 自動的には起動しません。	チェックする
	タスクトレイにアイコンを表示する	リモコンエージェント起動時に、Windows のタスクバーにアイコンを表示するかどうかを設定します。	チェックする アイコンを表示します。 チェックしない アイコンを表示しません。	チェックする
	利用者による終了を許可する	利用者によってリモコンエージェントの終了を許可するかどうかを設定します。	チェックする 利用者による終了を許可します。 チェックしない 利用者による終了は許可しません。	チェックしない
切断時の処理		管理用サーバとリモートコントロールの接続が切断した場合の動作を選択します。	• リモコンエージェントを起動したままにする • リモコンエージェントを終了する	リモコンエージェントを起動したままにする
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	標準接続で使用するポート番号を指定します。	1～65532	管理用サーバのセットアップで［ポート番号の設定］画面の［リモートコントロールでの使用ポート番号］に指定したポート番号
	RFB ポート番号	RFB 接続で使用するポート番号を指定します。	1～65535	5900
リクエストサーバ	リクエスタ接続先	コンピュータからの接続要求時の宛先のデフォルト値を指定します。	ホスト名※または IPv4 形式の IP アドレス	管理用サーバのホスト名または IP アドレス
ファイル転送	管理用サーバとコンピュータ間で、ファイル転送を許可するかどうかを選択します。		• ファイル転送を許可しない • ファイル転送を許可する	ファイル転送を許可する

項目		内容	設定できる値	デフォルト
ファイル転送	リモコンエージェントからのファイルの読み取り	ファイル転送時にコンピュータのファイルの読み取りを許可するかどうかを設定します。	チェックする コンピュータのファイルの読み取りを許可する。 チェックしない コンピュータのファイルの読み取りを許可しない。	チェックする
	リモコンエージェントへのファイルの書き込み	ファイル転送時にコンピュータへのファイルの書き込みを許可するかどうかを設定します。	チェックする コンピュータへのファイルの書き込みを許可する。 チェックしない コンピュータへのファイルの書き込みを許可しない。	チェックする
チャット	リモコンエージェントの起動時に、チャットも開始できる状態にしておく	リモコンエージェントの起動時にチャットサーバを起動するかどうかを設定します。	チェックする チャットサーバを起動します。 チェックしない チャットサーバを起動しません。	チェックしない
	タスクバーにアイコンを表示する	チャットサーバの起動時に、Windows のタスクバーにアイコンを表示するかどうかを設定します。	チェックする アイコンを表示します。 チェックしない アイコンを表示しません。	チェックする
	コントローラとの接続時にチャットを開始する	チャットサーバが起動している場合に、ほかのコンピュータからチャットの接続があったときに自動的に［チャット］ウィンドウを表示するかどうかを設定します。	チェックする 自動的に［チャット］ウィンドウを表示します。 チェックしない 自動的に［チャット］ウィンドウは表示しません。	チェックしない
コントロール許可の設定	許可コントローラ	リモートコントロール機能を使用できるコンピュータを制限したい場合にだけ、許可するコンピュータを指定します。	ホスト名または IPv4 形式の IP アドレス	なし
ユーザー認証	許可ユーザー一覧	リモートコントロールの接続時にコントローラに	Windows の認証情報または任意の認証情報	なし

項目		内容	設定できる値	デフォルト
ユーザー認証	許可ユーザー一覧	要求する認証情報を設定します。	(ユーザー名とパスワード)	なし
接続の確認	利用者のコンピュータに、利用者が応答するためのダイアログを表示する	管理用サーバからの接続時に、リモートコントロールの許可を求めるダイアログを表示するかどうかを設定します。	チェックする 接続時に許可を求めるダイアログを表示します。 チェックしない 接続時に許可を求めるダイアログは表示しません。	チェックしない
	ダイアログの表示	利用者にリモートコントロールの許可を求めるダイアログの表示時間を指定します。	表示時間を指定する 利用者にリモートコントロールの許可を求めるダイアログの表示時間を 1～180 秒で指定します。 応答があるまで表示したままにする 応答があるまで、ダイアログは表示されたままとなります。	表示時間を指定する（10 秒）
	利用者が応答しない場合	利用者がリモートコントロールの許可を求めるダイアログに対して操作しなかった場合の動作を選択します。	• 接続する • 接続しない	接続する
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。	• 制御モード • 共有モード • 監視モード	共有モード

注※

255 文字以内の文字列で指定します。

(5) インストールセットのパラメーター

設定画面の［Windows エージェント設定とインストールセットの作成］画面から表示できる［インストールセットの作成］ダイアログのパラメーターを次に示します。

インストールフォルダの設定

項目	内容	設定できる値	デフォルト
インストールフォルダ	JP1/IT Desktop Management 2 - Agent をインストールするフォルダのパス名を指定します。	104 文字以内のパス※	%ProgramFiles%¥Hitachi¥jp1itdma
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	共有型 VDI の仮想コンピュータにインストールするエージェントで、仮想コンピュータの情報からホスト識別子を生成するかどうかを選択します。	チェックする 仮想コンピュータの情報からホスト識別子を生成します。 チェックしない 仮想コンピュータの情報からホスト識別子を生成しません。	チェックしない
	[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] をチェックした場合、どの情報からホスト識別子を生成するか選択します。	• コンピュータ名 • アカウント名 • IP アドレス	コンピュータ名

注※　使用できる文字は、半角英数字、半角スペース、および「.」（ピリオド）、「(」、「)」、「:」、「_」、「¥」です。

アカウントの設定

項目	内容	設定できる値	デフォルト
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	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ためのアカウント情報を設定するかどうかを選択します。	チェックする 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ためのアカウント情報を設定します。 チェックしない 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ためのアカウント情報を設定しません。	チェックしない
管理者権限を持つアカウント	Administrator 権限を持つアカウント（ユーザー名）を指定します。	276 文字以内の半角文字列	（空白）
パスワード	Administrator 権限を持つアカウント（ユーザー名）に対するパスワードを指定します。	128 文字以内の半角文字列	（空白）
パスワード確認	確認のため、指定したパスワードを再度入力します。		

ヒント

［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］は、管理者権限を持つアカウント/パスワードを不用意に更新しないようにチェックボックスを設けています。管理者権限を持つアカウント/パスワードは、チェックボックスのチェック状態に関係なく、インストールセットに保存されます。

コンポーネントの設定

項目	内容	設定できる値	デフォルト
インストールするコンポーネント	インストールするコンポーネントの種別を指定（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を選択）します。※1	• JP1/IT Desktop Management 2 - Agent（エージェント） • JP1/IT Desktop Management 2 - Agent（中継システム）	エージェント
リモコンエージェント	リモートコントロールエージェントをインストールするかどうかを設定します。※2	チェックする リモートコントロールエージェントをインストールします。 チェックしない リモートコントロールエージェントをインストールしません。	チェックする

注※1　Citrix XenApp、Microsoft RDS サーバの場合、中継システムはサポートしていないため、「エージェント」を選択してください。

注※2　Citrix XenApp、Microsoft RDS サーバの場合、リモートコントロールエージェントはサポートしていないため、「チェックしない」を選択してください。

登録先の ID の設定

項目	内容	設定できる値	デフォルト
登録先 ID	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グループ）を指定します。 ID は、［登録］ボタンをクリックし、表示されるダイアログで ID 名を入力することで作成できます。	32 文字以内の文字列	（空白）

展開するファイルの設定

項目	内容	設定できる値	デフォルト
展開するファイル	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、[追加] ボタンをクリックすると表示されるダイアログで指定します。	展開するファイル 100 文字以内の文字列 展開先のフォルダ 255 文字以内の半角文字列	(空白)

自動実行するファイルの設定

項目	内容	設定できる値	デフォルト
自動実行するプログラムファイル※1	エージェントのインストール後に自動実行するプログラムと、自動実行に必要なファイル、引数※2 を、[追加] ボタンをクリックすると表示されるダイアログで指定します。	自動実行するプログラムと、自動実行に必要なファイルの名前 100 文字以内の文字列※3 ファイルのパス 255 文字以内の半角文字列 このファイルはエージェントのインストール後に自動実行する 設定したファイルを、エージェントのインストール後に自動実行したい場合にチェックします。自動実行するファイルとして ZIP ファイル以外を設定するか、ZIP ファイルを設定した場合は [展開区分] に「この圧縮ファイルは展開せずに使用する」を指定した場合にチェックできます。 引数 設定したファイルをエージェントのインストール後に自動実行する場合、自動実行に必要な引数を、127 文字以内で設定します。 自動実行するファイルとして ZIP ファイルを設定する場合は、次の項目を指定します。 展開区分 ZIP ファイルの展開区分（展開しないで利用するか、展開してエージェントのインストール後に自動実行するか）を指定します。 実行ファイル種別 [展開区分] が「この圧縮ファイルを展開して、エージェン	ファイル名 (空白) このファイルをエージェントのインストール後に自動実行する チェックしない 展開区分 この圧縮ファイルは展開せずに使用する 実行ファイル種別 秘文インストーラ以外 引数 [実行ファイル種別] が秘文インストーラの場合は「/b」 ファイルの展開先フォルダを指定する チェックしない

項目	内容	設定できる値	デフォルト
自動実行するプログラムファイル※1	エージェントのインストール後に自動実行するプログラムと、自動実行に必要なファイル、引数※2 を、[追加] ボタンをクリックすると表示されるダイアログで指定します。	トのインストール後に、自動実行する」の場合、実行するファイルが秘文インストーラか、秘文インストーラ以外かを指定します。 実行ファイルのパス [展開区分] が「この圧縮ファイルを展開して、エージェントのインストール後に、自動実行する 」の場合に、[展開先で自動実行するファイルを選択する] ボタンをクリックすると表示される画面で指定した、エージェントのインストール後に自動実行するプログラムファイル（setup.exe など）のパスが表示されます。 ファイルの展開先フォルダを指定する 圧縮ファイルの展開先フォルダを指定するかどうかを設定します。[実行ファイル種別] が「秘文インストーラ以外」の場合にチェックできます。 展開先フォルダ [実行ファイル種別] が「秘文インストーラ以外」の場合に、展開先のコンピュータで有効なフォルダを 259 文字以内の文字列※4 で指定します。	ファイル名 (空白) このファイルをエージェントのインストール後に自動実行する チェックしない 展開区分 この圧縮ファイルは展開せずに使用する 実行ファイル種別 秘文インストーラ以外 引数 [実行ファイル種別] が秘文インストーラの場合は「/b」 ファイルの展開先フォルダを指定する チェックしない

注※1　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 Version 11 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。

注※2　127 文字以内の文字列で指定します。

注※3　半角文字の「"」、「*」、「/」、「<」、「>」、「?」、「¥」、「¦」および「:」は使用できません。

注※4　半角文字の「"」、「*」、「/」、「<」、「>」、「?」および「¦」は使用できません。

上書きインストールの設定

項目	内容	設定できる値	デフォルト
エージェントを上書きインストールする	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。	チェックする 上書きインストールします。 チェックしない 上書きインストールしません。	チェックする
指定した［登録先 ID］に登録する	上書きインストールする場合に、指定した ID に登録するかどうかを設定します。	チェックする 上書きインストール時に、指定した ID に登録します。 チェックしない 指定した ID に登録しません。	チェックする
指定した［展開するファイル］を展開する	上書きインストールする場合に、指定した［展開するファイル］を展開するかどうかを設定します。	チェックする 上書きインストール時に、指定した［展開するファイル］を展開します。 チェックしない 指定した［展開するファイル］を展開しません。	チェックする
指定した［自動実行するファイル］を実行する	上書きインストールする場合に、指定した［自動実行するファイル］を実行するかどうかを設定します。	チェックする 上書きインストール時に、指定した［自動実行するファイル］を実行します。 チェックしない 指定した［自動実行するファイル］を実行しません。	チェックする

(6) Active Directory の探索設定のパラメーター

設定画面の［探索条件の設定］－［Active Directory の探索］画面のパラメーターを次に示します。

探索スケジュール

項目	内容	設定できる値	デフォルト
スケジュールを設定して、定期的に探索を実行する	スケジュールを設定して、定期的に探索を実行するかどうかを設定します。	チェックする 設定したスケジュールに従って、定期的に探索が実行されます。 チェックしない 定期的な探索は実行されません。	チェックする
開始時刻	探索が実行される時刻を指定します。	00:00～23:59	23:00

項目	内容	設定できる値	デフォルト
繰り返し単位	定期的に探索を繰り返す単位を選択します。	• 日単位 • 週単位 • 月単位	日単位
繰り返しの方法	探索を実行するタイミングを指定します。	[繰り返しの単位]で選択した項目によって異なります。 日単位の場合 1～31 週単位の場合 日曜日～土曜日 月単位の場合 日付（1～31）、または週次（第1～第4、最終）と曜日（日曜日～土曜日）を指定できます。	1

発見した機器への操作

項目	内容	設定できる値	デフォルト
自動的に管理対象とする	探索によって発見されたOSがWindowsのコンピュータの場合、自動的に管理対象にするかどうかを設定します。	チェックする 発見されたコンピュータを、自動的に管理対象にします。 チェックしない 発見されたコンピュータを管理対象にしません。	チェックする
エージェントを自動配信する	探索によって発見されたOSがWindowsのコンピュータの場合、自動的にエージェントを配信するかどうかを設定します。	チェックする 発見されたコンピュータに、自動的にエージェントを配信します。 チェックしない 発見されたコンピュータにエージェントを配信しません。	チェックしない

完了通知

項目	内容	設定できる値	デフォルト
通知先	探索完了時にメール通知する通知先を設定します。	[ユーザーアカウントの管理]画面に登録されているユーザーアカウントおよびメールの通知先	なし

(7) ネットワークの探索設定のパラメーター

設定画面の［探索条件の設定］－［ネットワークの探索］画面のパラメーターを次に示します。

探索範囲の設定内容

項目	内容	設定できる値	デフォルト
探索範囲	ネットワークの探索で使用する探索範囲を設定します。	探索範囲	管理用サーバセグメント※
探索範囲名	探索範囲の名称を指定します。	255 文字以内の名称	新しい探索範囲名
開始	探索範囲の開始値となる IP アドレスを IPv4 形式で指定します。	IPv4 形式の IP アドレス	（空白）
終了	探索範囲の終了値となる IP アドレスを IPv4 形式で指定します。	IPv4 形式の IP アドレス	（空白）
認証情報	指定した範囲を探索するときに使用される認証情報を指定します。	すべて 登録済みのすべての認証情報を使用します。 選択 使用する認証情報を選択します。	すべて

注※ 「管理用サーバセグメント」には、管理用サーバが設置されているネットワークセグメントの IP アドレスの範囲と、［認証情報］に「すべて」が設定されています。

認証情報

項目	内容	設定できる値	デフォルト
認証情報	ネットワークの探索時に使用する認証情報を設定	認証情報	SNMP 標準※1
認証名	認証情報を管理するための名称を設定します。	255 文字以内の名称	新しい認証名
種別	認証情報の種別を選択します。	• SNMP • Windows	SNMP
ポート番号※2	SNMP が使用するポート番号を指定します。	1～65535	161
コミュニティ名※2	コミュニティ名を指定します。	半角 255 文字以内の名称	（空白）
ユーザー ID※3	Windows の管理共有を認証できるユーザー ID を指定します。	276 文字以内の ID	（空白）

項目	内容	設定できる値	デフォルト
ユーザー ID※3	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。	276 文字以内の ID	（空白）
パスワード※3	ユーザー ID に対するパスワードを指定します。	半角 127 文字以内のパスワード	（空白）
パスワード確認※3	パスワードを再指定します。	半角 127 文字以内のパスワード	（空白）

注※1 「SNMP 標準」には、［種別］に「SNMP」、［ポート番号］に「161」、［コミュニティ名］に「public」が設定されています。

注※2 ［種別］が「SNMP」の場合に表示されます。

注※3 ［種別］が「Windows」の場合に表示されます。

探索スケジュール

項目	内容	設定できる値	デフォルト
スケジュールを設定して、定期的に探索を実行する	スケジュールを設定して、定期的に探索を実行するかどうかを設定します。	チェックする 設定したスケジュールに従って、定期的に探索が実行されます。 チェックしない 定期的な探索は実行されません。	チェックしない
開始時刻	探索が実行される時刻を指定します。	00:00～23:59	12:00
繰り返し単位	定期的に探索を繰り返す単位を選択します。	• 日単位 • 週単位 • 月単位	日単位
繰り返しの方法	探索を実行するタイミングを指定します。	［繰り返しの単位］で選択した項目によって異なります。 日単位の場合 1～31	1

項目	内容	設定できる値	デフォルト
繰り返しの方法	探索を実行するタイミングを指定します。	週単位の場合 日曜日～土曜日 月単位の場合 日付（1～31）、または週次（第 1～第 4、最終）と曜日（日曜日～土曜日）を指定できます。	1

発見した機器への操作

項目	内容	設定できる値	デフォルト
自動的に管理対象とする	探索によって発見された OS が Windows のコンピュータを、自動的に管理対象にするかどうかを設定します。	チェックする 発見されたコンピュータを、自動的に管理対象にします。 チェックしない 発見されたコンピュータを管理対象にしません。	チェックする
エージェントを自動配信する	探索によって発見された OS が Windows のコンピュータに、自動的にエージェントを配信するかどうかを設定します。	チェックする 発見されたコンピュータに、自動的にエージェントを配信します。 チェックしない 発見されたコンピュータにエージェントを配信しません。	チェックしない

完了通知

項目	内容	設定できる値	デフォルト
通知先	探索完了時にメール通知する通知先を設定します。	[ユーザーアカウントの管理] 画面に登録されているユーザーアカウントおよびメールの通知先	なし

(8) エージェントの配信のパラメーター

設定画面の［Windows エージェントの配信］画面のパラメーターを次に示します。

項目	内容	設定できる値	デフォルト
配信するエージェントのコンポーネントの設定	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かどうかを設定します。	• リモコンエージェントを含める • リモコンエージェントを含めない	リモコンエージェントを含める

(9) エージェントレス管理の設定のパラメーター

設定画面の［エージェント］－［エージェントレス管理の設定］画面のパラメーターを次に示します。

項目	内容	設定できる値	デフォルト
定期的に更新する	エージェントレスの機器から機器情報を収集するかどうかを選択します。	チェックする エージェントレスの機器から機器情報を収集します。 チェックしない エージェントレスの機器から機器情報を収集しません。	チェックする
更新間隔	エージェントレスの機器から機器情報を収集する間隔を指定します。	1～24	1

(10) セキュリティのスケジュール設定のパラメーター

設定画面の［セキュリティのスケジュール設定］画面のパラメーターを次に示します。

項目	内容	設定できる値	デフォルト
実施時刻	コンピュータのセキュリティ状態の判定を実施する時刻を指定します。	00:00～23:59	00:00
実施間隔（日）	何日ごとにセキュリティ状態を判定するかを指定します。	1～31	1

(11) 操作ログの設定のパラメーター

設定画面の［操作ログの設定］画面のパラメーターを次に示します。

操作ログの自動取り込み

項目	内容	設定できる値	デフォルト
操作ログを自動的に取り込む	受信した操作ログを、自動的に取り込むかどうかを設定します。	チェックする 操作ログを自動的に取り込みます。 チェックしない 操作ログを自動的に取り込みません。	チェックする
自動取り込みされる操作ログの格納期間	自動取り込みされる操作ログが操作ログのデータベースに格納される期間を設定します。	1～300※	30

注※　設定できる値の上限は、管理用サーバのセットアップで指定した［操作ログのデータベース格納最大日数］から手動取り込みした日数を引いた値が設定されます。

操作ログのエクスポート

項目	内容	設定できる値	デフォルト
操作ログを定期的にエクスポートする	受信した操作ログを、定期的にエクスポートするかどうかを設定します。	チェックする 操作ログを定期的にエクスポートします。 チェックしない 操作ログをエクスポートしません。	チェックしない

(12)　ネットワーク制御リストの自動更新の設定のパラメーター

設定画面の［ネットワーク制御］－［ネットワーク制御リストの設定］－［ネットワーク制御リストの自動更新］画面のパラメーターを次に示します。

ネットワーク制御リストの自動更新

項目	内容	設定できる値	デフォルト
すべての自動更新を有効にする	ネットワーク制御リストの自動更新を有効にするかどうかを設定します。	チェックする ネットワーク制御リストのすべての自動更新を有効にします。 チェックしない ネットワーク制御リストの自動更新のうち追加だけを有効にします。	チェックしない

ネットワーク制御リストの自動更新の対象範囲

項目	内容	設定できる値	デフォルト
配下の管理用サーバが管理している機器も自動更新の対象にする	ネットワーク制御リストの自動更新の対象に配下の管理用中継サーバが管理している機器を含めるかどうかを設定します。	チェックする 自サーバ直下の機器および配下の管理用中継サーバが管理している機器を自動更新の対象にします。 チェックしない 自サーバ直下の機器だけを自動更新の対象にします。	チェックしない

(13)　AMT の設定のパラメーター

設定画面の［機器］－［AMT の設定］画面のパラメーターを次に示します。

認証情報

項目	内容	設定できる値	デフォルト
ユーザー ID	管理対象のコンピュータの AMT に接続するためのユーザー ID を入力します。	64 文字以内の ASCII コードの制御文字を除いた文字列です。	（空白）
パスワード	ユーザー ID に対するパスワードを設定します。	64 文字以内の ASCII コードの制御文字を除いた文字列です。	（空白）
パスワード確認	確認のためパスワードを再入力します。	64 文字以内の ASCII コードの制御文字を除いた文字列です。	（空白）

管理者権限のパスワード

項目	内容	設定できる値	デフォルト
パスワード	AMT の管理者権限のパスワードを設定します。	8～32 文字の ASCII コード（0x20～0x7E）※1 の文字列です。 英小文字、英大文字、数字、記号※2 をそれぞれ 1 文字以上含める必要があります。	（空白）
パスワード確認	確認のためパスワードを再入力します。	8～32 文字の ASCII コード（0x20～0x7E）※1 の文字列です。 英小文字、英大文字、数字、記号※2 をそれぞれ 1 文字以上含める必要があります。	（空白）

注※1 「:」、「,」、「"」は指定できません。

注※2 「_」は指定できません。

(14) 変更履歴の設定のパラメーター

設定画面の［機器］－［変更履歴の設定］画面のパラメーターを次に示します。

変更履歴の取得

項目	内容	設定できる値	デフォルト
変更履歴を取得する※1	機器情報の変更履歴を取得するかどうかを設定します。	チェックする 機器情報の変更履歴を取得します。 チェックしない 機器情報の変更履歴を取得しません。	チェックしない

項目	内容	設定できる値	デフォルト
直下の機器の変更履歴を取得する※2	直下の機器情報の変更履歴を取得するかどうかを設定します。	チェックする 直下の機器情報の変更履歴を取得します。 チェックしない 直下の機器情報の変更履歴を取得しません。	チェックしない
配下の機器の変更履歴を取得する※2	下位の管理用中継サーバから通知された機器情報の変更履歴を取得するかどうかを設定します。	チェックする 下位の管理用中継サーバから通知された機器情報の変更履歴を取得します。 チェックしない 下位の管理用中継サーバから通知された機器情報の変更履歴を取得しません。	チェックする

注※1　最小構成または基本構成の場合に表示されます。

注※2　複数サーバ構成の場合に表示されます。

変更履歴の取得対象

項目	内容	設定できる値	デフォルト
機器情報	表示されている機器情報の中から、変更履歴の取得対象を設定します。	チェックする 変更履歴の取得対象とします。 チェックしない 変更履歴の取得対象としません。	すべての機器情報がチェックされている。

(15)　レポートの保存期間と開始日の設定のパラメーター

設定画面の［レポート］－［保存期間と開始日の設定］画面のパラメーターを次に示します。

項目	内容	設定できる値	デフォルト
レポートを保存したい期間を選択してください。	レポートの保存期間を指定します。	1 年～10 年	5 年
週の始めとしたい曜日を選択してください。	レポート集計時の週の開始日を指定します。	日曜日～土曜日	月曜日
月の始めとしたい日を選択してください。	レポート集計時の月の開始日を指定します。	1～31	1

項目	内容	設定できる値	デフォルト
年度の始めとしたい月を選択してください。	レポート集計時の年度の開始月を指定します。	1 月～12 月	4 月

(16) ダイジェストレポートの設定のパラメーター

設定画面の［レポート］－［ダイジェストレポートの設定］画面のパラメーターを次に示します。

日刊ダイジェスト

項目	内容	設定できる値	デフォルト
日刊ダイジェストの送付先を選択してください。	日刊ダイジェストをメール通知するユーザー ID またはメール通知先をチェックします。ユーザー ID にメールアドレスが設定されていない場合は、メールアドレスを入力します。	E-mail 形式の文字列です。	［ユーザーアカウントの管理］画面に登録されているユーザーアカウントおよびメールの通知先が表示される。

週刊ダイジェスト

項目	内容	設定できる値	デフォルト
週刊ダイジェストの送付先を選択してください。	週刊ダイジェストをメール通知するユーザー ID またはメール通知先をチェックします。ユーザー ID にメールアドレスが設定されていない場合は、メールアドレスを入力します。	E-mail 形式の文字列です。	［ユーザーアカウントの管理］画面に登録されているユーザーアカウントおよびメールの通知先が表示される。

月刊ダイジェスト

項目	内容	設定できる値	デフォルト
月刊ダイジェストの送付先を選択してください。	月刊ダイジェストをメール通知するユーザー ID またはメール通知先をチェックします。ユーザー ID にメールアドレスが設定されていない場合は、メールアドレスを入力します。	E-mail 形式の文字列です。	［ユーザーアカウントの管理］画面に登録されているユーザーアカウントおよびメールの通知先が表示される。

(17) イベント通知の設定のパラメーター

設定画面の［イベント］－［イベント通知の設定］画面のパラメーターを次に示します。

メールで受け取りたいイベントの、重大度と種類を設定してください。

項目	内容	設定できる値	デフォルト
緊急、警戒、情報	［緊急］、［警戒］、および［情報］の重大度ごとにメール通知したいイベントを選択します。	チェックする 選択したイベントをメールで通知します。	［緊急］だけチェックされている。

項目	内容	設定できる値	デフォルト
緊急、警戒、情報	[緊急]、[警戒]、および［情報］の重大度ごとにメール通知したいイベントを選択します。	チェックしない 選択しないイベントはメールで通知しません。	[緊急］だけチェックされている。
セキュリティ	ポリシーの変更と割り当て、ポリシーの判定結果、アクションの結果、起動抑止など、セキュリティ管理に関するイベントを設定します。	チェックする 選択したカテゴリをメールで通知します。 チェックしない 選択しないカテゴリはメールで通知しません。	[緊急］のカテゴリだけすべてチェックされている。
不審操作	添付ファイル付きのメールの検知、Web サーバ、FTP サーバへのファイルアップロードの検知、外部メディアへのファイルコピー・移動の検知など、不審操作に関するイベントを設定します。		
資産	資産の登録、資産の状態の変更、ソフトウェアライセンスの追加と削除など、資産管理に関するイベントを設定します。		
配布（ITDM 互換）	ITDM 互換配布の機能による、ソフトウェアのインストール、ファイルの配布、ソフトウェアのアンインストールなどに関するイベントを設定します。		
機器	機器やソフトウェアの追加と削除、コンピュータのアカウントの追加と削除など、機器管理に関するイベントを設定します。		
設定	機器の発見、管理対象の追加、エージェントの配信など、設定に関するイベントを設定します。		
中継	管理用サーバ間でのデータの中継に関するイベントを設定します。複数サーバ構成で運用している場合にだけ出力されるイベントです。		
エラー	各機能で発生したエラーに関するイベントを設定します。		

メールの通知先を選択してください。

項目	内容	設定できる値	デフォルト
メールの通知先を選択してください。	イベントを通知したいユーザー ID またはメール通知先をチェックします。ユーザー ID にメールアドレスが設定されていない場合は、メールアドレスを入力します。	E-mail 形式の文字列です。	[ユーザーアカウントの管理］画面に登録されているユーザーアカウントおよびメールの通知先が表示される。

通知の間隔

項目	内容	設定できる値	デフォルト
通知の間隔（分）	何分ごとに通知するかを設定します。	1～1440	30

(18) メールサーバの設定のパラメーター

設定画面の［他システムとの接続］－［メールサーバの設定］画面のパラメーターを次に示します。

メールサーバ（SMTP サーバ）の設定

項目	内容	設定できる値	デフォルト
ホスト名	SMTP サーバのホスト名を入力します。	SMTP サーバのホスト名	（空白）
セキュリティ保護の接続	SMTP サーバと通信する際に使用するセキュリティ保護を選択します。	• 使用しない • TLS	使用しない
ポート番号	SMTP サーバのポート番号を指定します。	1～65535	25
送信元メールアドレス	通知メールの送信元とするメールアドレスを指定します。	E-mail 形式の文字列です。	（空白）
SMTP 認証を使用する	SMTP サーバでユーザー認証機能（SMTP Authentication）を使用する場合は、［SMTP 認証を使用する］を選択します。	チェックする SMTP 認証を使用します。 チェックしない SMTP 認証を使用しません。	チェックしない
ユーザー ID	ユーザー認証機能で使用するユーザー ID を入力します。	ユーザー認証機能で使用するユーザー ID	（空白）
パスワード	ユーザー ID に対するパスワードを設定します。	ユーザー ID に対するパスワード	（空白）
パスワード確認	確認のためパスワードを再入力します。	確認のためのパスワード	（空白）

(19) Active Directory の設定のパラメーター

設定画面の［他システムとの接続］－［Active Directory の設定］画面のパラメーターを次に示します。

項目	内容	設定できる値	デフォルト
Active Directory の組織の情報を取得して、部署の情報に反映する	Active Directory から組織の階層構成を取得して、部署のグループの構成に反映するかどうかを設定します。	チェックする Active Directory が管理している組織階層の情報を部署のグループの構成に反映します。 チェックしない Active Directory が管理している組織階層の情報を部署のグループの構成に反映しません。	チェックしない
ドメイン名	Active Directory サーバのドメイン名を指定します。	次の文字を除いた、0～255 文字の ASCII コードの文字列です。「.」（ピリオド）は文字列の先頭以外で使用できます。 • ASCII コードの制御文字	（空白）

項目	内容	設定できる値	デフォルト
ドメイン名	Active Directory サーバのドメイン名を指定します。	• 半角スペース、「!」、「"」、「#」、「$」、「%」、「&」、「(」、「)」、「*」、「+」、「,」、「'」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「`」、「{」、「|」、「}」、「~」	（空白）
ホスト名	Active Directory サーバのホスト名（完全修飾ドメイン名）を指定します。	ASCII コードの制御文字を除いた、0～255 文字の文字列です。	（空白）
ポート番号	Active Directory サーバに接続するためのポート番号を入力します。	1～65535	389
ユーザー ID	Active Directory サーバに接続するためのユーザー ID を入力します。	ASCII コードの制御文字を除いた、0～276 文字の文字列です。	（空白）
パスワード	ユーザー ID に対するパスワードを設定します。	ASCII コードの制御文字を除いた、0～64 文字の ASCII コードの文字列です。	（空白）
パスワード確認	確認のためパスワードを再入力します。	ASCII コードの制御文字を除いた、0～64 文字の ASCII コードの文字列です。	（空白）
ルート OU	取得対象とするルートの組織単位（OU）を示すパスを入力します。ドメイン名および OU 名を「/」で区切って入力してください。大文字・小文字は区別されません。例えば、ドメイン名が「hitachi.co.jp」、OU 名が「総務部」「総務課」の場合、「hitachi.co.jp/総務部/総務課」と入力します。なお、ドメイン名は必ず入力してください。OU 名は省略できます。部署の情報を取得する場合は、ここで入力したパス配下の階層構成が部署のグループ構成に反映されます。	ASCII コードの制御文字を除いた、0～256 文字の文字列です。	（空白）
TLS	TLS（Transport Layer Security）通信を有効にするかどうかを設定します。	チェックする TLS を有効にします。 チェックしない TLS を有効にしません。	チェックしない

(20) サポートサービス設定のパラメーター

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］画面のパラメーターを次に示します。

サポートサービスの設定

項目	内容	設定できる値	デフォルト
サポートサービスと接続する	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かどうかを設定します。	チェックする サポートサービスと接続します。 チェックしない サポートサービスと接続しません。	チェックしない
URL	サポートサービスサイトの URL を指定します。	制限はありません。	https://www.hitachi-support.com/jp1itdm
ダウンロードご利用 ID	日立 Web サーバの認証 ID を指定します。	制限はありません。	(空白)
パスワード	ダウンロードご利用 ID に対するパスワードを指定します。	制限はありません。	(空白)
パスワード確認	確認のためパスワードを再入力します。	制限はありません。	(空白)
開始時刻	サポートサービスへ接続する時刻を入力します。	00:00～23:59	管理用サーバをセットアップした時刻の分を切り上げた時刻※
繰り返し単位	接続を繰り返す間隔を［日単位]、[週単位]、[月単位］から選択します。	• 日単位 • 週単位 • 月単位	日単位
繰り返しの方法	探索を実行するタイミングを指定します。	［繰り返しの単位］で選択した項目によって異なります。 日単位の場合 1～31 週単位の場合 日曜日～土曜日 月単位の場合 日付（1～31)、または週次（第 1～第 4、最終）と曜日（日曜日～土曜日）を指定できます。	1
更新プログラム一覧の更新通知先	更新プログラム一覧の更新を通知したいユーザー ID またはメール通知先を選択します。ユーザー ID にメールアドレスが設定されていない場合は、メールアドレスを入力します。	E-mail 形式の文字列です。	[ユーザーアカウントの管理］画面に登録されているユーザーアカウントおよびメールの通知先

注※　例えば、セットアップした時刻が 10:30 の場合、ダウンロード時刻は 11:00 となります。

プロキシサーバの設定

項目	内容	設定できる値	デフォルト
プロキシサーバを使用する	プロキシサーバを使用する場合に選択します。	チェックする プロキシサーバを使用します。 チェックしない プロキシサーバを使用しません。	チェックしない
IP アドレス	プロキシサーバの IP アドレスを入力します。	IPv4 形式の IP アドレス	(空白)
ポート番号	プロキシサーバのポート番号を入力します。	1～65535	(空白)
ユーザー ID	プロキシサーバに接続するためのユーザー ID を入力します。	プロキシサーバに接続するためのユーザー ID	(空白)
パスワード	ユーザー ID に対するパスワードを設定します。	ユーザー ID に対するパスワード	(空白)
パスワード確認	確認のためパスワードを再入力します。	確認のためのパスワード	(空白)

(21) MDM 連携の設定のパラメーター

設定画面の［他システムとの接続］－［MDM 連携の設定］画面のパラメーターを次に示します。

MDM 連携の設定

項目	内容	設定できる値	デフォルト
MDM 設定名	設定の名称を指定します。	255 文字以内の文字列	(空白)
MDM システム	接続する MDM システムを選択します。	• JP1/ITDM2 - SD Manager • MobileIron	(空白)
MDM サーバのホスト名	MDM システムのサーバ証明書に設定されている CommonName（CN）を指定します。 MobileIron の場合、サーバ証明書の CN は FQDN で指定してください。	255 文字以内の文字列	(空白)
MDM サーバのポート番号	MDM 製品に接続するためのポート番号を指定します。	1～65535	(空白)
URL	MDM 製品の URL を指定します。	0～2083 文字の文字列	(空白)
ユーザー ID	MDM システムにログインするためのユーザー ID を指定します。	276 文字以内の文字列	(空白)
パスワード	MDM システムにログインするためのパスワードを指定します。	128 文字以内の文字列	(空白)

項目	内容	設定できる値	デフォルト
パスワード確認	確認のためパスワードを再入力します。	128 文字以内の文字列	(空白)

プロキシサーバの設定

項目	内容	設定できる値	デフォルト
プロキシサーバを使用する	プロキシサーバを使用する場合に選択します。	チェックする プロキシサーバを使用します。 チェックしない プロキシサーバを使用しません。	チェックしない
IP アドレス	プロキシサーバの IP アドレスを入力します。	IPv4 形式の IP アドレス	(空白)
ポート番号	プロキシサーバのポート番号を入力します。	1～65535	(空白)
ユーザー ID	プロキシサーバに接続するためのユーザー ID を入力します。	プロキシサーバに接続するためのユーザー ID	(空白)
パスワード	ユーザー ID に対するパスワードを設定します。	ユーザー ID に対するパスワード	(空白)
パスワード確認	確認のためパスワードを再入力します。	確認のためのパスワード	(空白)

取得スケジュール

項目	内容	設定できる値	デフォルト
開始時刻	MDM システムから情報を取得する時刻を入力します。	00:00～23:59	(空白)
繰り返し単位	情報の取得を繰り返す間隔を［日単位］、［週単位］、［月単位］から選択します。	• 日単位 • 週単位 • 月単位	日単位
繰り返しの方法	情報を取得するタイミングを指定します。	［繰り返しの単位］で選択した項目によって異なります。 日単位の場合 1～31 週単位の場合 日曜日～土曜日 月単位の場合 日付（1～31）、または週次（第 1～第 4、最終）と曜日（日曜日～土曜日）を指定できます。	1

(22) JP1/NETM/NM - Manager 連携の設定のパラメーター

設定画面の［ネットワーク制御］－［ネットワーク制御の設定］－［JP1/NETM/NM - Manager 連携の設定］の［編集］ボタンをクリックすると表示される［JP1/NETM/NM - Manager 連携の設定］ダイアログのパラメーターを次に示します。

項目	内容	設定できる値	デフォルト
JP1/NETM/NM - Manager と連携する	JP1/NETM/NM - Manager と連携するかどうかを設定します。	チェックする JP1/NETM/NM - Manager と連携します。 チェックしない JP1/NETM/NM - Manager と連携しません。	チェックしない

(23) 機器メンテナンスの設定のパラメーター

設定画面の［機器］－［機器メンテナンスの設定と検出結果確認］画面のパラメーターを次に示します。

機器メンテナンスの検出条件（重複機器の場合）

重複機器の検出条件

項目	内容	設定できる値	デフォルト
検出条件名	検出条件の名称を指定します。	256 文字以内の文字列	（空白）
検出対象	重複機器として検出する機器の種別を指定します。	次に示す種別の 1 つ以上を指定します。 • エージェント管理（Windows/Mac OS） • エージェント管理（UNIX） • エージェントレス管理 • MDM 連携管理 • API 管理	すべての種別がチェックされてい る。
重複条件	何が一致していれば重複機器として検出するかを指定します。	次に示す項目の 1 つ以上を指定します。複数を指定した場合は AND 条件となります。 • IP アドレス • ホスト名 大文字と小文字を区別するかどうかを指定できます。 • MAC アドレス • BIOS のシリアルナンバー	どれもチェックされていない。

項目	内容	設定できる値	デフォルト
未接続の期間	検出対象にした種別の機器のうち、重複条件に該当する機器が、何日以上、管理用サーバに接続されていないと重複機器として検出するかを指定します。	1 日～999 日	7 日

自動削除の設定

項目	内容	設定できる値	デフォルト
重複機器と検出された機器のうち、最終接続確認日時が古い機器をすべて自動的に削除する	重複機器として検出された機器を自動的に削除するかどうかを指定します。	チェックする 自動的に削除します。 チェックしない 自動的に削除しません。	チェックしない
自動削除されるまでの期間	自動的に削除されるまでの保留期間（日数）を指定します。	1 日～999 日	14 日

機器メンテナンスの検出条件（不稼働機器の場合）

不稼働機器の検出条件

項目	内容	設定できる値	デフォルト
検出条件名	検出条件の名称を指定します。	256 文字以内の文字列	（空白）
検出対象	不稼働機器として検出する機器の種別を指定します。	次に示す種別の 1 つ以上を指定します。 • エージェント管理（Windows/Mac OS） • エージェント管理（UNIX） • エージェントレス管理 • MDM 連携管理 • API 管理	すべての種別がチェックされてい る。
未接続の期間	検出対象にした種別の機器が何日以上、管理用サーバに接続されていないと不稼働機器として検出するかを指定します。	1 日～999 日	30 日

自動削除の設定

項目	内容	設定できる値	デフォルト
不稼働機器と検出された機器をすべて自動的に削除する	不稼働機器として検出された機器を自動的に削除するかどうかを指定します。	チェックする 自動的に削除します。 チェックしない 自動的に削除しません。	チェックしない
自動削除されるまでの期間	自動的に削除されるまでの保留期間（日数）を指定します。	1 日～999 日	14 日

(24) 削除機器関連ハードウェア資産の資産状態の設定のパラメーター

設定画面の［資産管理］－［削除機器関連ハードウェア資産の資産状態の設定］画面のパラメーターを次に示します。

項目	内容	設定できる値	デフォルト
削除した機器に関連するハードウェア資産の資産状態を変更する	削除した機器に関連するハードウェア資産の資産状態を変更するかどうかを指定します。	チェックする 資産状態を変更します。 チェックしない 資産状態を変更しません。	チェックしない
資産状態	変更後の資産状態を選択します。	• 滅却 • ユーザーが任意で追加した資産状態	滅却

付録 A.5 プロパティ一覧

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を次の表に示します。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。

プロパティ	説明	設定値	デフォルト
Capacity_OplogDBPathWarningThreshold	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	0～1,048,576 メガバイト	操作ログのデータベースの［必要なディスク容量］の 10%
Capacity_OplogDBPathErrorThreshold	操作ログのデータベースフォルダの空き容量の緊急しきい値	0～1,048,576 メガバイト	操作ログのデータベースの［必要なディスク容量］の 3%
Capacity_OplogBKPathWarningThreshold	操作ログの保管先フォルダの空き容量の警戒しきい値（定期エクスポート無効時）	0～1,048,576 メガバイト	操作ログの保管先フォルダに必要なディスク容量の目安の 7 日分
Capacity_OplogBKPathErrorThreshold	操作ログの保管先フォルダの空き容量の緊急しきい値（定期エクスポート無効時）	0～1,048,576 メガバイト	操作ログの保管先フォルダに必要なディスク容量の目安の 3 日分
Capacity_OplogBKPathWarningThreshold_ExportEnabled	操作ログの保管先フォルダの空き容量の警戒しきい値（定期エクスポート有効時）	0～1,048,576 メガバイト	操作ログの保管先フォルダに必要なディスク容量の目安の 7 日分
Capacity_OplogBKPathErrorThreshold_ExportEnabled	操作ログの保管先フォルダの空き容量の緊急しきい値 （定期エクスポート有効時）	0～1,048,576 メガバイト	操作ログの保管先フォルダに必要なディスク容量の目安の 3 日分
Capacity_DataPathWarningThreshold_OpLogEnabled_ExportDisabled	データフォルダの空き容量の警戒しきい値 （操作ログ有効時・定期エクスポート無効時）	0～1,048,576 メガバイト	操作ログのバッファ用データフォルダに必要なディスク容量の目安

プロパティ	説明	設定値	デフォルト
Capacity_DataPathWarningThreshold_OpLogEnabled_ExportDisabled	データフォルダの空き容量の警戒しきい値 （操作ログ有効時・定期エクスポート無効時）	0～1,048,576 メガバイト	の 50%＋ 3,072 メガバイト
Capacity_DataPathErrorThreshold_OpLogEnabled_ExportDisabled	データフォルダの空き容量の緊急しきい値 （操作ログ有効時・定期エクスポート無効時）	0～1,048,576 メガバイト	操作ログバッファ用データフォルダに必要なディスク容量の目安の 30%＋ 500
Capacity_DataPathWarningThreshold_OpLogEnabled_ExportEnabled	データフォルダの空き容量の警戒しきい値 （操作ログ有効時・定期エクスポート有効時）	0～1,048,576 メガバイト	操作ログバッファ用データフォルダに必要なディスク容量の目安の 50%＋ 3,072 メガバイト
Capacity_DataPathErrorThreshold_OpLogEnabled_ExportEnabled	データフォルダの空き容量の緊急しきい値 （操作ログ有効時・定期エクスポート有効時）	0～1,048,576 メガバイト	操作ログバッファ用データフォルダに必要なディスク容量の目安の 30%＋ 500
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	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	ダイジェストレポートを作成する時間	00:00～23:59	06:00
DB_MentenanceTime	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	変更履歴を取得する時間	00:00～23:59	00:00
OpLog_DB_DeleteTime	自動取り込みされた操作ログ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
UNIX_Software_Manage	UNIX エージェントや Mac エージェント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
DeviceAutoMaintenanceTime	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。	なし

プロパティ	説明	設定値	デフォルト
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	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] － [リクエストウィザード] • 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
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	0：マッピングしない※3 1：マッピングする	1

プロパティ	説明	設定値	デフォルト
SDM_Mapping_Name	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
OfflineRegistration_StatusUnknown	オフライン管理のコンピュータの機器情報を初めて取得した場合の機器状態についての設定	ON：機器状態を「不明」にする OFF：機器状態を「停止中」にする ただし、機器状態が「警告」の場合、「警告」が表示されます。	OFF
Mgrsrv_jdnmssecurityctrl	セキュリティ判定の設定	10 管理対象のコンピュータが30,000～50,000台の場合に必ず設定してください。	5
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
RollUpPatch_ExpirationDate	月例ロールアップの判定期限の設定 設定値の日以降は月例ロールアップのセキュリティ判定をしなくなります。設定値は米国東部標準時間で解釈されます。	「*第何週*,*曜日*」のフォーマットまたは0を指定します。*第何週*には1～5を指定します。*曜日*には1～7を指定します。*曜日*の値の意味を次に示します。 1：日曜日 2：月曜日 3：火曜日 4：水曜日 5：木曜日 6：金曜日 7：土曜日 0を指定した場合は判定期限を設けません。	2,3 (第二火曜日)
RestAPIProtocol	APIの通信プロトコルの設定	0：HTTPプロトコル 1：HTTPSプロトコル	0
RestAPIInventoryUpdatePriorityLow	APIによって取得された機器情報の更新の優先順位の設定	APIによって取得された機器情報の更新の優先順位を、次のどれかで指定した方法の1つ上の優先順位とします。 Shares：Windowsの管理共有によって取得された機器情報 SNMP：SNMPによって取得された機器情報	SNMP

プロパティ	説明	設定値	デフォルト
RestAPIInventoryUpdatePriorityLow	API によって取得された機器情報の更新の優先順位の設定	AD：Active Directory によって取得された機器情報 MDM：MDM 連携によって取得された機器情報 ARP：ARP によって取得された機器情報 このプロパティを指定しない場合は、「(14)　機器情報の更新」で記載した 3 番目の優先順位となります。	SNMP

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。

付録 A.6　性能と見積もり

ここでは、製品の各システム構成要素のメモリ所要量、ディスク占有量、および前提となる CPU について説明します。

関連リンク

- (1)　メモリ所要量
- (2)　ディスク占有量
- (3)　前提となる CPU

(1)　メモリ所要量

製品の各システム構成要素のメモリ所要量について示します。

- 管理用サーバ

- 管理用中継サーバ
- 操作画面を表示するコンピュータ
- リモートインストールマネージャをインストールする管理者のコンピュータ
- リモートコントロールのコントローラをインストールする管理者のコンピュータ
- 中継システムのコンピュータ
- 管理対象のコンピュータ
- インターネットゲートウェイのコンピュータ

管理用サーバ

項目	動作環境
メモリ使用量	管理対象のコンピュータが 10,000 台までの場合※1※3※4 10 ギガバイト 管理対象のコンピュータが 10,000～30,000 台の場合※1※3※4 32 ギガバイト 管理対象のコンピュータが 30,000～50,000 台の場合※2※3※4 34 ギガバイト
搭載メモリ	実装メモリとして、OS ごとの推奨メモリに加えて、次の合計値以上が必要です。 • 管理対象のコンピュータが 5,000 台までの場合※1 2 ギガバイト以上 • 管理対象のコンピュータが 5,000～10,000 台の場合※1 • 最小 2 ギガバイト • 推奨 8 ギガバイト以上 • 管理対象のコンピュータが 10,000～30,000 台の場合※1 • 最小 16 ギガバイト • 推奨 32 ギガバイト以上 • 管理対象のコンピュータが 30,000～50,000 台の場合 • 最小 24 ギガバイト • 推奨 40 ギガバイト以上

注※1　操作ログの検索性能を向上させるため、管理用サーバのセットアップで［キャッシュへの追加容量］を指定した場合、その指定値（最大 16 ギガバイト）を追加します。

注※2　管理対象のコンピュータが 30,000～50,000 台の場合で、操作画面を 10 人～20 人で同時に操作する場合は、追加で 1,200 メガバイトのメモリを使用します。

注※3　秘文ログを取り込む場合は追加で 500 メガバイトのメモリを使用します。

注※4　API を使用する場合は追加で 1,600 メガバイトのメモリを使用します。

管理用中継サーバ

項目	動作環境
メモリ使用量	管理対象のコンピュータが 10,000 台までの場合※1※2 10 ギガバイト 管理対象のコンピュータが 10,000～30,000 台の場合※1※2 32 ギガバイト 操作ログの検索性能を向上させるため、管理用サーバのセットアップで［キャッシュへの追加容量］を指定した場合、その指定値（最大 16 ギガバイト）を追加します。
搭載メモリ	実装メモリとして、OS ごとの推奨メモリに加えて、次の合計値以上が必要です。 • 管理対象のコンピュータが 5,000 台までの場合 2 ギガバイト以上 • 管理対象のコンピュータが 5,000～10,000 台の場合 • 最小 2 ギガバイト • 推奨 8 ギガバイト以上 • 管理対象のコンピュータが 10,000～30,000 台の場合 • 最小 16 ギガバイト • 推奨 32 ギガバイト以上 操作ログの検索性能を向上させるため、管理用サーバのセットアップで［キャッシュへの追加容量］を指定した場合、その指定値（最大 16 ギガバイト）を追加します。

注※1　秘文ログを取り込む場合は追加で 500 メガバイトのメモリを使用します。

注※2　API を使用する場合は追加で 1,600 メガバイトのメモリを使用します。

操作画面を表示するコンピュータ

項目	動作環境
搭載メモリ	2.0 ギガバイト以上

リモートインストールマネージャをインストールする管理者のコンピュータ

項目	動作環境
メモリ使用量	次の式で計算した値が必要です。 20 ＋ 0.002×a メガバイト a：表示データ数

項目	動作環境
メモリ使用量	表示データ数は、リモートインストールマネージャの各ウィンドウで表示する次のデータの総数です。なお、同じウィンドウを複数表示する場合は、ウィンドウ数分加算してください。 • ［システム構成］ウィンドウ ホスト情報（管理用中継サーバ、中継システム、エージェント） • ホストごとのシステム情報 • エージェントごとのインストールパッケージ • ［あて先］ウィンドウ • ID（新規作成ホスト、資産管理項目条件） 各グルーピング情報に該当するあて先（経路、エージェント） • あて先グループ（IP アドレス、新規作成ホスト、OS 種別、ハードウェア資産情報の追加管理項目、部署、設置場所） 各グルーピング情報に該当するあて先（経路、エージェント） • エージェントごとのインストールパッケージ • ［ジョブ定義］ウィンドウ フォルダ、ジョブ定義 • ［パッケージ］ウィンドウ キャビネット、パッケージ • ［ジョブ実行状況］ウィンドウ フォルダ、ジョブ（ジョブごとのあて先、ジョブごとのパッケージ） • ［管理情報リスト］ウィンドウ 検索リスト
搭載メモリ	2.0 ギガバイト以上

リモートコントロールのコントローラをインストールする管理者のコンピュータ

項目	動作環境
メモリ使用量	次の値の合計値です。 • 基本機能（リモートコントロール）：(10×接続数）メガバイト • ファイル転送機能：4 メガバイト • チャットサーバ機能：(4 ＋（0.2×接続数)）メガバイト • チャットクライアント機能：(4 ＋（0.4×接続数)）メガバイト
搭載メモリ	実装メモリとして次の合計値以上が必要です。 • OS ごとの推奨メモリ • メモリ使用量×0.5 を 8 の倍数で切り上げた値

中継システムのコンピュータ

項目	動作環境
メモリ使用量	次の値の合計値です。 • 基本機能（機器情報の収集、配布、リモートコントロール）（常に常駐）：58 メガバイト • 操作ログ機能（機能が有効の場合に常駐）：OS が 32 ビット版の場合は 34 メガバイト、OS が 64 ビット版の場合は 43 メガバイト

項目	動作環境
メモリ使用量	• ネットワークモニタ機能（機能が有効の場合に常駐）：2 メガバイト＋（10×監視対象のネットワークセグメント数）メガバイト • 次の式で計算した値 28 ＋ 0.018×（a ＋ 8）＋（b×0.001） a：同時接続台数 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］で［中継システムへの同時接続 JP1/IT Desktop Management 2 - Agent 数］に指定した値です。 b：管理ファイルのキャッシュサイズ 次の計算式で算出してください。 管理ファイルのキャッシュサイズ（キロバイト）＝中継システムに保管されている、上位システムから実行されたジョブ数×各ジョブのあて先数×各ジョブのパッケージ数（リモートインストールのジョブの場合）×1 キロバイト
搭載メモリ	実装メモリとして次の合計値以上が必要です。 • OS ごとの推奨メモリ • メモリ使用量×0.5 を 8 の倍数で切り上げた値

管理対象のコンピュータ

項目	動作環境
メモリ使用量	エージェント導入済みのコンピュータの場合 次の値の合計値です。 • 基本機能（機器情報の収集、配布、リモートコントロール）（常に常駐）：58 メガバイト • 操作ログ機能（機能が有効の場合に常駐）：OS が 32 ビット版の場合は 34 メガバイト、OS が 64 ビット版の場合は 43 メガバイト Citrix XenApp、Microsoft RDS 環境で操作ログ機能を使用する場合は、Citrix XenApp、Microsoft RDS 環境にログインするユーザ 1 人当たり 45 メガバイトのメモリが追加になります。 • ネットワークモニタ機能（機能が有効の場合に常駐）：2 メガバイト＋（10×監視対象のネットワークセグメント数）メガバイト エージェントレスのコンピュータの場合 22 メガバイト
搭載メモリ※	実装メモリとして次の合計値以上が必要です。 エージェント導入済みのコンピュータの場合 • OS ごとの推奨メモリ • メモリ使用量×0.5 を 8 の倍数で切り上げた値 エージェントレスのコンピュータの場合 OS ごとの推奨メモリ＋ 16 メガバイト

注※　ここに記載している値は OS の最小スペックです。快適に利用するためには、対象の機器で同時に動作するほかのプログラムが使用する分も含めた余裕のあるスペックが必要です。

インターネットゲートウェイのコンピュータ

項目	動作環境
メモリ使用量	次の値の合計値です。 • 2.0 ギガバイト • 中継システムのメモリ使用量
搭載メモリ	実装メモリとして次の合計値以上が必要です。 • OS ごとの推奨メモリ • 2.0 ギガバイト • 中継システムの搭載メモリ

注　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インターネットゲートウェイのコンピュータにインストールしてください。

(2)　ディスク占有量

製品の各システム構成要素のディスク占有量について示します。

- 管理用サーバ
- 管理用中継サーバ
- 操作画面を表示するコンピュータ
- リモートインストールマネージャをインストールする管理者のコンピュータ
- リモートコントロールのコントローラをインストールする管理者のコンピュータ
- 中継システムのコンピュータ
- 管理対象のコンピュータ
- パッケージャをインストールするコンピュータ
- Automatic Installation Tool をインストールするコンピュータ
- インターネットゲートウェイをインストールするコンピュータ

管理用サーバ

項目	動作環境
インストールドライブ（本体容量）	管理対象のコンピュータが 10,000 台までの場合※6 2.5 ギガバイト以上 管理対象のコンピュータが 10,000～30,000 台の場合※6 17.5 ギガバイト以上 管理対象のコンピュータが 30,000～50,000 台の場合※7 17.5 ギガバイト以上
データベースフォルダが格納されるドライブ	管理対象のコンピュータが 10,000 台までの場合 次の値の合計値以上です。

項目	動作環境
データベースフォルダが格納されるドライブ	• 基本機能：20 ギガバイト • 変更履歴機能：運用を考慮したデータ容量※2 管理対象のコンピュータが 10,000～30,000 台の場合 次の値の合計値以上です。 • 基本機能：60 ギガバイト • 変更履歴機能：運用を考慮したデータ容量※2 管理対象のコンピュータが 30,000～50,000 台の場合 次の値の合計値以上です。 • 基本機能：120 ギガバイト • 変更履歴機能：運用を考慮したデータ容量※2
操作ログのデータベースフォルダが格納されるドライブ	運用を考慮したデータ容量の見積もりが必要です。※1
データフォルダが格納されるドライブ	次の値の合計値以上です。 • 基本機能：320 メガバイト • すべての配布パッケージ容量の合計 （セキュリティ対策で自動配布される更新プログラムを含みます。） • ハードウェア資産、契約、ライセンスの添付ファイル容量の合計 • インストールセットの［展開するファイル］の容量の合計 • 操作ログで必要な容量 運用を考慮したデータ容量※3 の見積もりが必要です。※7
操作ログの保管先フォルダのドライブ	運用を考慮したデータ容量※4 の見積もりが必要です。※7
変更履歴の出力先フォルダのドライブ	運用を考慮したデータ容量※5 の見積もりが必要です。

注※1　操作ログのデータベースに必要なデータ容量については、「4.5.4　操作ログのデータベースに必要なディスク容量の目安」を参照してください。なお、管理対象のコンピュータが 10,000～30,000 台の場合、操作ログのデータベースのディスクは、独立した別ディスク（物理的に別のディスク）にすることを推奨します。

注※2　変更履歴のデータベースに必要なデータ容量については、「4.5.7　変更履歴のデータベースに必要なディスク容量の目安」を参照してください。

注※3　データフォルダに必要なデータ容量については、「4.5.5　操作ログを取得する場合のデータフォルダに必要なディスク容量の目安」を参照してください。

注※4　操作ログの保管先フォルダに必要なデータ容量については、「4.5.3　操作ログの保管先フォルダに必要なディスク容量の目安」を参照してください。

注※5　変更履歴の出力先フォルダに必要なデータ容量については、「4.5.6　保存用の変更履歴の出力に必要なディスク容量の目安」を参照してください。

注※6　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した場合は、その指定値（最大 16 ギガバイト）が追加で必要になります。

注※7　管理対象のコンピュータが 30,000～50,000 台の場合で操作ログを取得する場合は、複数サーバ構成で運用し、統括管理用サーバでは取得しないため、操作ログは見積もりの対象外です。

配布機能を利用する場合、さらに次に示す空き容量が必要です。

リモートインストールマネージャを使用した配布の場合

項目	動作環境
JP1/IT Desktop Management 2 - Manager がインストールされているドライブ	1.0×パッケージ数×エージェント数＋パッケージ数×0.3（単位：キロバイト）
データフォルダが格納されるドライブ	圧縮後のパッケージサイズの合計＋パッケージ数×2（単位：キロバイト）

ITDM 互換配布の場合

項目	動作環境
JP1/IT Desktop Management 2 - Manager がインストールされているドライブ	パッケージ（圧縮する前）の 2 倍以上の空き容量
データフォルダが格納されるドライブ	
システムドライブ	パッケージ（圧縮する前）の空き容量

自動アップデートでコンポーネントをアップデートさせる場合、さらに次に示す空き容量が必要です。

項目	動作環境
JP1/IT Desktop Management 2 - Manager がインストールされているドライブ	500 メガバイト
データフォルダが格納されるドライブ	
システムドライブ	

API を使用する場合、さらに次に示す空き容量が必要です。

項目	動作環境
JP1/IT Desktop Management 2 - Manager がインストールされているドライブ	356 メガバイト

管理用中継サーバ

項目	動作環境
インストールドライブ（本体容量）	管理対象のコンピュータが 10,000 台までの場合 2.5 ギガバイト以上

項目	動作環境
インストールドライブ（本体容量）	管理対象のコンピュータが 10,000～30,000 台の場合 17.5 ギガバイト以上 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した場合は、その指定値（最大 16 ギガバイト）が追加で必要になります。
データベースフォルダが格納されるドライブ	管理対象のコンピュータが 10,000 台までの場合 次の値の合計値以上です。 • 基本機能：20 ギガバイト • 変更履歴機能：運用を考慮したデータ容量※2 管理対象のコンピュータが 10,000～30,000 台の場合 次の値の合計値以上です。 • 基本機能：60 ギガバイト • 変更履歴機能：運用を考慮したデータ容量※2
操作ログのデータベースフォルダが格納されるドライブ	運用を考慮したデータ容量の見積もりが必要です。※1
データフォルダが格納されるドライブ	次の値の合計値以上です。 • 基本機能：24 ギガバイト • すべての配布パッケージ容量の合計 （セキュリティ対策で自動配布される更新プログラムを含みます。） • ハードウェア資産、契約、ライセンスの添付ファイル容量の合計 • インストールセットの［展開するファイル］の容量の合計 • 操作ログで必要な容量 運用を考慮したデータ容量※3 の見積もりが必要です。
操作ログの保管先フォルダのドライブ	運用を考慮したデータ容量※4 の見積もりが必要です。
変更履歴の出力先フォルダのドライブ	運用を考慮したデータ容量※5 の見積もりが必要です。

注※1　操作ログのデータベースに必要なデータ容量については、「4.5.4　操作ログのデータベースに必要なディスク容量の目安」を参照してください。なお、管理対象のコンピュータが 10,000～30,000 台の場合、操作ログのデータベースのディスクは、独立した別ディスク（物理的に別のディスク）にすることを推奨します。

注※2　変更履歴のデータベースに必要なデータ容量については、「4.5.7　変更履歴のデータベースに必要なディスク容量の目安」を参照してください。

注※3　データフォルダに必要なデータ容量については、「4.5.5　操作ログを取得する場合のデータフォルダに必要なディスク容量の目安」を参照してください。

注※4　操作ログの保管先フォルダに必要なデータ容量については、「4.5.3　操作ログの保管先フォルダに必要なディスク容量の目安」を参照してください。

注※5　変更履歴の出力先フォルダに必要なデータ容量については、「4.5.6　保存用の変更履歴の出力に必要なディスク容量の目安」を参照してください。

配布機能を利用する場合、さらに次に示す空き容量が必要です。

リモートインストールマネージャを使用した配布の場合

項目	動作環境
JP1/IT Desktop Management 2 - Manager がインストールされているドライブ	1.0×パッケージ数×エージェント数＋パッケージ数×0.3（単位：キロバイト）
データフォルダが格納されるドライブ	圧縮後のパッケージサイズの合計＋パッケージ数×2（単位：キロバイト）

ITDM 互換配布の場合

項目	動作環境
JP1/IT Desktop Management 2 - Manager がインストールされているドライブ	パッケージ（圧縮する前）の 2 倍以上の空き容量
データフォルダが格納されるドライブ	
システムドライブ	パッケージ（圧縮する前）の空き容量

API を使用する場合、さらに次に示す空き容量が必要です。

項目	動作環境
JP1/IT Desktop Management 2 - Manager がインストールされているドライブ	356 メガバイト

操作画面を表示するコンピュータ

JP1/IT Desktop Management 2 によるディスクの占有量はありません。

リモートインストールマネージャをインストールする管理者のコンピュータ

項目	動作環境
インストールドライブ（本体容量）	24 メガバイト以上

リモートコントロールのコントローラをインストールする管理者のコンピュータ

項目	動作環境
インストールドライブ（本体容量）	20 メガバイト以上

中継システムのコンピュータ

項目	動作環境
インストールドライブ（本体容量）	次の値の合計値以上です。 • 基本機能（インベントリ収集、配布、リモートコントロール）：71 メガバイト • 操作ログ機能：120 メガバイト • ネットワークモニタ機能：2 メガバイト＋（55×監視対象のネットワークセグメント数）メガバイト

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は、さらに次に示す空き容量が必要です。

項目	動作環境
中継システムがインストールされているドライブ	(80+圧縮後のパッケージサイズの合計+パッケージ数×中継システム配下のエージェント数/1024)メガバイト

自動アップデートで中継システムをアップデートさせる場合、さらに次に示す空き容量が必要です。

項目	動作環境
中継システムがインストールされているドライブ	200 メガバイト
データフォルダが格納されるドライブ	
中継システムージェントがインストールされているコンピュータのシステムドライブ	

管理対象のコンピュータ

項目	動作環境
インストールドライブ（本体容量）	**エージェントレス運用時** JP1/IT Desktop Management 2 によるディスクの占有量はありません。
	エージェント運用時 次の値の合計値以上です。 • 基本機能（インベントリ収集、配布、リモートコントロール）：71 メガバイト • 操作ログ機能：120 メガバイト＋ 260 キロバイト×保持期間（日） Citrix XenApp、Microsoft RDS 環境で操作ログ機能を使用する場合は、次の計算式になります。 120 メガバイト＋ 12 ギガバイト＋ 260 キロバイト×保持期間（日）×ログインユーザ数 • ネットワークモニタ機能：2 メガバイト＋（55×監視対象のネットワークセグメント数）メガバイト

配布機能を利用する場合、さらに次に示す空き容量が必要です。

リモートインストールマネージャを使用した配布の場合

項目	動作環境
エージェントがインストールされているドライブ	パッケージ（圧縮する前）の 3 倍以上の空き容量

ITDM 互換配布の場合

項目	動作環境
エージェントがインストールされているドライブ	• パッケージ種別が［ソフトウェアインストール］の場合：パッケージ（ZIP ファイルに圧縮する前）の 2 倍以上の空き容量 • パッケージ種別が［ファイル配布］の場合：パッケージ（ZIP ファイルに圧縮する前）の 3 倍以上の空き容量
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システムドライブ	パッケージ（ZIP ファイルに圧縮する前）の空き容量

自動アップデートでエージェントをアップデートさせる場合、さらに次に示す空き容量が必要です。

項目	動作環境
エージェントがインストールされているドライブ	50 メガバイト
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システムドライブ	

自動アップデートでネットワークモニタエージェントをアップデートさせる場合、さらに次に示す空き容量が必要です。

項目	動作環境
エージェントがインストールされているドライブ	20 メガバイト
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システムドライブ	

エージェントレスのコンピュータが Windows の管理共有の認証を利用する場合、各機能を実行するために、実行プログラムが送信されます。実行プログラムを格納するために、2.5 メガバイト以上の空き容量が必要です。

パッケージャをインストールするコンピュータ

項目	動作環境
エージェントがインストールされているドライブ	7 メガバイト＋パッケージ（圧縮する前）の 2 倍以上の空き容量

Automatic Installation Tool をインストールするコンピュータ

項目	動作環境
エージェントがインストールされているドライブ	6 メガバイト

インターネットゲートウェイをインストールするコンピュータ

項目	動作環境
インストールドライブ（本体容量）	次の値の合計値以上です。 • 25 メガバイト • 中継システムのディスク占有量 • パッケージサイズ パッケージサイズは、次の式で計算します。 リモートインストールマネージャを使用した配布の場合 100×パッケージの分割サイズ（分割配布） ITDM 互換配布の場合 9 ギガバイト

注　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インターネットゲートウェイのコンピュータにインストールしてください。

関連リンク

- 4.5　データベースの検討

(3)　前提となる CPU

製品の各システム構成要素の前提となる CPU について示します。

- 管理用サーバ
- 操作画面を表示するコンピュータ
- リモートインストールマネージャをインストールする管理者のコンピュータ
- リモートコントロールのコントローラをインストールする管理者のコンピュータ
- 中継システムのコンピュータ
- 管理対象のコンピュータ
- インターネットゲートウェイのコンピュータ

管理用サーバ

管理対象のコンピュータが 5,000 台までの場合

2.0 ギガヘルツ以上のプロセッサ

管理対象のコンピュータが 5,000～10,000 台の場合

- 最小
  2.0 ギガヘルツ以上のプロセッサ
- 推奨

2.0 ギガヘルツ以上の 4 コアプロセッサ

管理対象のコンピュータが 10,000～30,000 台の場合

- 最小
  2.5 ギガヘルツ以上の、Intel Xeon（4 コア）プロセッサ×2
- 推奨
  3.0 ギガヘルツ以上の、Intel Xeon（4 コア）プロセッサ×2

管理対象のコンピュータが 30,000～50,000 台の場合

- 最小
  2.5 ギガヘルツ以上の、Intel Xeon（8 コア）プロセッサ×2
- 推奨
  3.0 ギガヘルツ以上の、Intel Xeon（10 コア）プロセッサ×2

操作画面を表示するコンピュータ

次のどちらかに該当する CPU を前提とします。

- ハイパースレッディング・テクノロジーに対応した Intel Pentium 4 相当以上のプロセッサ
- Intel Core 2 相当以上のプロセッサ

リモートインストールマネージャをインストールする管理者のコンピュータ

- 最小
  1 ギガヘルツのプロセッサ
- 推奨
  2 ギガヘルツ以上のプロセッサ

リモートコントロールのコントローラをインストールする管理者のコンピュータ

コンピュータの OS	動作環境
Windows Server 2019	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows Server 2016	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows 10	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows 8.1	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows 8	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows Server 2012	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows 7	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows Server 2008 R2	1.4 ギガヘルツ以上の 64 ビットプロセッサ

中継システムのコンピュータ

コンピュータの OS	動作環境
Windows Server 2019	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows Server 2016	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows 10	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows 8.1	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows 8	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows Server 2012	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows 7	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ

管理対象のコンピュータ

エージェントレスのコンピュータ

CPU の制限はありません。

エージェントを導入するコンピュータ※

コンピュータの OS	動作環境
Windows Server 2019	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows Server 2016	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows 10	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows 8.1	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows 8	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows Server 2012	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows 7	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows Server 2008 R2	1.4 ギガヘルツ以上の 64 ビットプロセッサ

注※　ここに記載している値は OS の最小スペックです。快適に利用するためには、対象の機器で同時に動作するほかのプログラムが使用する分も含めた余裕のあるスペックが必要です。

ネットワークモニタを有効にするコンピュータ

コンピュータの OS	動作環境
Windows Server 2019	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows Server 2016	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows 10	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows 8.1	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ

コンピュータの OS	動作環境
Windows 8	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
Windows Server 2012	1.4 ギガヘルツ以上の、64 ビットプロセッサ
Windows 7	1.0 ギガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ

インターネットゲートウェイのコンピュータ

- 最小
  2.5 ギガヘルツ以上の、Intel Xeon（4 コア）プロセッサ×2
- 推奨
  3.0 ギガヘルツ以上の、Intel Xeon（4 コア）プロセッサ×2

付録 A.7　制限値一覧

JP1/IT Desktop Management 2 では、管理できる項目について登録数や設定値に制限があります。各項目の制限値を次の表に示します。以降の表中では、凡例を次のとおり表記しています。

（凡例）－：該当なし

ログイン画面

機能	項目	制限値	デフォルト	説明
ログイン	同時ログイン数	上限なし	－	想定する上限は次のとおりです。 • 管理対象のコンピュータが 30,000 台までの場合：20 ユーザー • 管理対象のコンピュータが 30,000～50,000 台までの場合：20 ユーザー

セキュリティ画面

機能	項目	制限値	デフォルト	説明
セキュリティポリシー	セキュリティポリシー	上限なし	2 個	デフォルトでは、「デフォルトポリシー」と「推奨セキュリティポリシー」が登録されています。 管理対象のコンピュータが 30,000 台までの場合に想定する上限は、これらのセキュリティポリシーを含めて 140 個です。 管理対象のコンピュータが 30,000～50,000 台までの場合に想定する上限は、これらのセキュリティポリシーを含めて 200 個です。

機能	項目	制限値	デフォルト	説明
セキュリティポリシーのセキュリティ設定項目	使用必須ソフトウェア	上限なし	0 個	想定する上限は、使用禁止ソフトウェアと合わせて 100 個です。
	使用禁止ソフトウェア	上限なし	0 個	想定する上限は、使用必須ソフトウェアと合わせて 100 個です。
	使用禁止サービス	上限なし	0 個	想定する上限は、30 個です。
	ユーザー定義のセキュリティ設定のユーザー定義項目	上限なし	0 個	想定する上限は、30 個です。
	起動抑止ソフトウェア	上限なし	0 個	想定する上限は、使用必須ソフトウェアと合わせて 100 個です。
更新プログラム	表示件数	上限なし	0 件	－
	手動で追加できる更新プログラム	上限なし	0 個	想定する上限は、1,000 個です。
機器のセキュリティ状態	機器 1 台当たりの未適用の更新プログラム	上限なし	－	想定する上限は、100 個です。
	機器 1 台当たりの未導入の使用必須ソフトウェア	上限なし	－	想定する上限は、50 個です。
	機器 1 台当たりの導入済みの使用禁止ソフトウェア	上限なし	－	想定する上限は、50 個です。
	機器 1 台当たりの OS のセキュリティ設定で確認できるアカウント数	1～50 個	－	－
	機器 1 台当たりのサービスのセキュリティ設定情報で確認できるサービス数	1～30 個	－	－

機能	項目	制限値	デフォルト	説明
USB デバイスの情報	1 デバイス当たりの USB デバイスから収集するファイルの情報	1～10,000 個	－	－
操作ログ	表示件数	上限なし	0 件	－

注　上限がない項目についても、情報を大量に登録すると、検索の性能が悪くなるなど性能面に影響が出ることがあります。

資産画面

機能	項目	制限値	デフォルト	説明
ハードウェア資産	ハードウェア資産情報	上限なし	0 件	管理対象のコンピュータが 30,000 台までの場合に想定する上限は、112,500 件です。そのうち、USB デバイスの想定する上限は、6,000 件です。 管理対象のコンピュータが 30,000～50,000 台までの場合に想定する上限は、187,500 件です。そのうち、USB デバイスの想定する上限は、6,000 件です。
	ハードウェア資産情報 添付ファイル	5	－	－
	資産状態	デフォルトとは別に 0～100 個追加できる	4 個	デフォルトでは、[未確認]、[在庫]、[運用中]、[滅却] の資産状態が登録されています。 この項目は、設定画面の項目と同じです。
	予定資産状態	デフォルトとは別に 0～100 個追加できる	3 個	デフォルトでは、[在庫]、[運用中]、[滅却] の予定資産状態が登録されています。 この項目は、[未確認] を除いて [資産状態] の項目と同じです。
	機器種別	デフォルトとは別に 0～100 個追加できる	11 個	デフォルトでは、[PC]、[サーバ]、[ストレージ]、[ネットワーク装置]、[プリンタ]、[スマートデバイス]、[周辺装置]、[USB デバイス]、[ディスプレイ]、[その他]、[不明な機器] の機器種別が登録されています。 この項目は、設定画面の項目と同じです。

機能	項目	制限値	デフォルト	説明
ハードウェア資産	エクスポートする項目数	1～200 項目	8 項目	デフォルトでは、[機器種別]、[資産管理番号]、[機器名称]、[メーカー]、[資産状態]、[予定資産状態]、[変更予定日]、[棚卸日] がエクスポートする項目としてチェックされています。
ソフトウェアライセンス	ソフトウェアライセンス	上限なし	0 件	管理対象のコンピュータが 30,000 台までの場合に想定する上限は、15,000 件です。 管理対象のコンピュータが 30,000～50,000 台までの場合に想定する上限は、25,000 件です。
	ソフトウェアライセンス添付ファイル	5	－	－
	ライセンス種類	デフォルトとは別に 0～100 個追加できる	2 個	デフォルトでは、[インストールライセンス]、[その他] のライセンス種類が登録されています。 この項目は、設定画面の項目と同じです。
	ライセンス状態	デフォルトとは別に 0～100 個追加できる	2 個	デフォルトでは、[使用中]、[滅却] のライセンス状態が登録されています。 この項目は、設定画面の項目と同じです。
	予定ライセンス状態	デフォルトとは別に 0～100 個追加できる	2 個	デフォルトでは、[使用中]、[滅却] の予定ライセンス状態が登録されています。 この項目は、[ライセンス状態] の項目と同じです。
	エクスポートする項目数	1～200 項目	11 項目	デフォルトでは、[ライセンス管理番号]、[ライセンス名]、[ライセンス種類]、[ライセンス数]、[保有数]、[割り当てライセンス数]、[残数]、[ライセンス状態]、[予定ライセンス状態]、[変更予定日]、[棚卸日] がエクスポートする項目としてチェックされています。
管理ソフトウェア	管理ソフトウェア	上限なし	0 件	管理対象のコンピュータが 30,000 台までの場合に想定する上限は、200 件です。 管理対象のコンピュータが 30,000～50,000 台までの場合に想定する上限は、300 件です。

機能	項目	制限値	デフォルト	説明
管理ソフトウェア	エクスポートする項目数	1～11 項目	7 項目	デフォルトでは、[管理ソフトウェア名]、[メーカー]、[ライセンス種類]、[保有数]、[ライセンス消費数]、[残数] がエクスポートする項目としてチェックされています。
契約	契約情報	上限なし	0 件	管理対象のコンピュータが 30,000 台までの場合に想定する上限は、26,250 件です。 管理対象のコンピュータが 30,000～50,000 台までの場合に想定する上限は、43,750 件です。
	契約種別	デフォルトとは別に 0～100 個追加できる	5 個	デフォルトでは、[リース]、[レンタル]、[保守]、[サポート]、[購入] の契約種別が登録されています。 この項目は、設定画面の項目と同じです。
	契約会社名	上限なし	0 件	想定する上限は、60 件です。 この項目は、設定画面の項目と同じです。
	契約状態	デフォルトとは別に 0～100 個追加できる	3 個	デフォルトでは、[契約中]、[途中解約]、[満了] の契約状態が登録されています。 この項目は、設定画面の項目と同じです。
	エクスポートする項目数	1～200 項目	7 項目	デフォルトでは、[契約管理番号]、[契約名]、[契約種別]、[契約開始日]、[契約終了日]、[契約日]、[契約状態] がエクスポートする項目としてチェックされています。
その他	インポートおよびエクスポートに使用するテンプレート	上限なし	－	管理対象のコンピュータが 30,000 台までの場合に想定する上限は、120 件です。 管理対象のコンピュータが 30,000～50,000 台までの場合に想定する上限は、200 件です。

注　上限がない項目についても、情報を大量に登録すると、検索の性能が悪くなるなど性能面に影響が出ることがあります。

機器画面

機能	項目	制限値	デフォルト	説明
機器情報	機器情報	購入しているライセンス数	0 件	－

機能	項目	制限値	デフォルト	説明
機器情報	機器 1 台当たりの導入済みソフトウェア	上限なし	−	想定する上限は、500 個です。
	機器 1 台当たりのセキュリティ情報-アカウント情報で確認できるアカウント数	1～60 個	−	−
	機器 1 台当たりのセキュリティ情報-サービスのセキュリティ設定情報で確認できるサービス数	1～30 個	−	−
機器一覧（詳細）のエクスポート	管理画面からエクスポートする台数	上限なし	−	想定する上限は、10,000 個です。
	インストールソフトウェア	上限なし	−	想定する上限は、10 個です。
	適用済みの更新プログラム	上限なし	−	想定する上限は、10 個です。
変更履歴	機器の変更履歴一覧に表示できる件数	600,000 件	−	−
ソフトウェア情報	ソフトウェア	収集されるソフトウェアの数	0 件	管理対象のコンピュータが 30,000 台までの場合に想定する上限は、30,000 件です。 管理対象のコンピュータが 30,000～50,000 台までの場合に想定する上限は、35,000 件です。
	エクスポートする項目数	1～9 項目	8 項目	デフォルトでは、[ソフトウェア名]、[バージョン]、[メーカー]、[インストール数]、[登録日時]、[必須ソフトウェア]、[禁止ソフトウェア]、[管理ソフトウェア] がエクスポートする項目としてチェックされています。

配布（ITDM 互換）画面

機能	項目	制限値	デフォルト	説明
パッケージ	パッケージ	0～10,000 個	0 個	－
	パッケージに登録する ZIP ファイルのアーカイブファイル数	上限なし	－	想定する上限は、3,000 個です。
	パッケージに登録するファイルのサイズ	1 ギガバイト以下	－	－
	パッケージに登録する ZIP ファイルの解凍後のファイルサイズの合計	2 ギガバイト未満	－	－
タスク	タスク	0～10,000 個	0 個	－
	対象のコンピュータ	管理対象のコンピュータの数	0 件	－

イベント画面

機能	項目	制限値	デフォルト	説明
イベント	表示できるイベント	管理対象のコンピュータ数×250 + 10,000 件	0 件	－

設定画面

機能	項目	制限値	デフォルト	説明
ユーザー管理	ユーザーアカウント	上限なし	1 件	管理対象のコンピュータが 30,000 台までの場合に想定する上限は、150 件です。 管理対象のコンピュータが 30,000～50,000 台までの場合に想定する上限は、213 件です。 デフォルトでは、ビルトインアカウントが登録されています。
エージェント	エージェント設定	上限なし	1 個	デフォルトでは、デフォルトエージェント設定が登録されています。
	更新間隔（エージェントレス管理の設定）	24 時間	1 時間	－

機能	項目	制限値	デフォルト	説明
エージェント	リモートコントロールの設定 許可コントローラ	256	－	－
	リモートコントロールの設定 許可ユーザー一覧	256	－	－
機器の探索	発見した機器	上限なし	0 件	－
	管理対象機器	購入しているライセンス数	0 件	－
	除外対象機器	上限なし	0 件	－
ネットワーク制御	ネットワークモニタ設定	上限なし	0 個	想定する上限は、10 個です。
	ネットワークへの接続を許可しない機器の特例接続	上限なし	0 個	想定する上限は、110 個です。
	ネットワーク制御リストの設定	上限なし	0 件	管理対象のコンピュータが 30,000 台までの場合に想定する上限は、66,000 件です。 管理対象のコンピュータが 30,000～50,000 台までの場合に想定する上限は、110,000 件です。
セキュリティ管理	Windows OS バージョン	上限なし	0 件	想定する上限は、10 件です。
資産管理	ハードウェア資産情報の追加管理項目	追加できる項目数は、選択するデータ型によって次のように異なる • 数値型：0～20 項目 各項目には、-2147483647～2147483647 を指定できる • 日付型：0～10 項目 各項目には、1900/1/1～9000/12/31 を指定できる • 選択型：0～20 項目	0 個	選択型で追加できる選択肢の数について、想定する上限は、50 個です。

機能	項目	制限値	デフォルト	説明
資産管理	ハードウェア資産情報の追加管理項目	各項目の選択肢の数には、上限なし • テキスト型：0～75 項目 各項目には、0～256 文字を指定できる	0 個	選択型で追加できる選択肢の数について、想定する上限は、50 個です。
	ソフトウェアライセンス情報の追加管理項目	追加できる項目数は、選択するデータ型によって次のように異なる • 数値型：0～10 項目 各項目には、-2147483647～2147483647 を指定できる • 日付型：0～10 項目 各項目には、1900/1/1～9000/12/31 を指定できる • 選択型：0～10 項目 各項目の選択肢の数には、上限なし • テキスト型：0～10 項目 各項目には、0～256 文字を指定できる	0 個	選択型で追加できる選択肢の数について、想定する上限は、50 個です。
	契約情報の追加管理項目	追加できる項目数は、選択するデータ型によって次のように異なる • 数値型：0～10 項目 各項目には、-2147483647～2147483647 を指定できる • 日付型：0～10 項目 各項目には、1900/1/1～9000/12/31 を指定できる • 選択型：0～10 項目 各項目の選択肢の数には、上限なし • テキスト型：0～10 項目 各項目には、0～256 文字を指定できる	0 個	選択型で追加できる選択肢の数について、想定する上限は、50 個です。

機能	項目	制限値	デフォルト	説明
資産管理	資産状態	デフォルトとは別に 0～100 個追加できる	4 個	デフォルトでは、[未確認]、[在庫]、[運用中]、[滅却] の資産状態が登録されています。 この項目は、資産画面の項目と同じです。
	機器種別	デフォルトとは別に 0～100 個追加できる	11 個	デフォルトでは、[PC]、[サーバ]、[ストレージ]、[ネットワーク装置]、[プリンタ]、[スマートデバイス]、[周辺装置]、[USB デバイス]、[ディスプレイ]、[その他]、[不明な機器] の機器種別が登録されています。 この項目は、資産画面の項目と同じです。
	ライセンス状態	デフォルトとは別に 0～100 個追加できる	2 個	デフォルトでは、[使用中]、[滅却] のライセンス状態が登録されています。 この項目は、資産画面の項目と同じです。
	ライセンス種類	デフォルトとは別に 0～100 個追加できる	2 個	デフォルトでは、[インストールライセンス]、[その他] のライセンス種類が登録されています。 この項目は、資産画面の項目と同じです。
	契約状態	デフォルトとは別に 0～100 個追加できる	3 個	デフォルトでは、[契約中]、[途中解約]、[満了] の契約状態が登録されています。 この項目は、資産画面の項目と同じです。
	契約種別	デフォルトとは別に 0～100 個追加できる	5 個	デフォルトでは、[リース]、[レンタル]、[保守]、[サポート]、[購入] の契約種別が登録されています。 この項目は、資産画面の項目と同じです。
	契約会社名	上限なし	0 件	想定する上限は、60 件です。 この項目は、資産画面の項目と同じです。
	エクスポートする項目数(契約会社リスト)	1～6 項目	6 項目	－

機能	項目	制限値	デフォルト	説明
機器	ソフトウェア検索条件	上限なし	0 個	想定する上限は、30 個です。
	機器メンテナンスの検出条件	上限なし	0 個	想定する上限は、10 個です。
他システムとの接続	Active Directory ドメイン	上限なし	0 個	この項目は、ホーム画面（[始めましょう] ボタン）の項目と同じです。
	MDM サーバ情報	上限なし	0 個	想定する上限は、10 個です。

注　上限がない項目についても、情報を大量に登録すると、検索の性能が悪くなるなど性能面に影響が出ることがあります。

機能	項目	制限値	デフォルト	説明
メニューエリア	グループの総数	上限なし	−	管理対象のコンピュータが 30,000 台までの場合に想定する上限は、次のとおりです。 • ユーザー定義のグループを含む場合：1,500 グループ • ユーザー定義のグループを含まない場合：1,200 グループ 管理対象のコンピュータが 30,000～50,000 台までの場合に想定する上限は、次のとおりです。 • ユーザー定義のグループを含む場合：1,900 グループ • ユーザー定義のグループを含まない場合：2,200 グループ
	ユーザー定義のグループ	上限なし	−	想定する上限は、300 グループです。
	ユーザー定義のグループ条件	0～10 個	−	−
	ユーザー定義のグループに振り分けられる機器の延べ台数	上限なし	−	想定する上限は、100,000 台です。
• セキュリティ画面 • 資産画面 • 機器画面	カスタムグループ	上限なし	0 グループ	想定する上限は、画面ごとに 50 グループです。

機能	項目	制限値	デフォルト	説明
• 配布（ITDM 互換）画面	カスタムグループに追加できる項目	上限なし	0 項目	想定する上限は、5,000 項目です。
• セキュリティ画面 • 資産画面 • 機器画面 • 配布（ITDM 互換）画面 • イベント画面	フィルタ	上限なし	各画面で異なる	想定する上限は、画面ごとに 50 個です。
	フィルタ条件	1～10 個	5 個	－
セキュリティ画面	更新プログラムグループ	上限なし	0 グループ	想定する上限は、200 グループです。
	更新プログラムグループに追加できる更新プログラム	上限なし	0 件	想定する上限は、3,000 件です。

注　上限がない項目についても、情報を大量に登録すると、検索の性能が悪くなるなど性能面に影響が出ることがあります。

リモートインストールマネージャ

機能	項目	制限値	デフォルト	説明
パッケージ	パッケージ	0～331,776 個	－	上限の内訳は次のとおりです。 キャビネットの最大個数 1,296 1 キャビネット当たりのパッケージの最大個数 256
ジョブ	ジョブ	上限なし	－	－
	ジョブ 1 つ当たりのエージェント数	上限なし	－	想定する上限は、3,000 個です。

注　上限がない項目についても、情報を大量に登録すると、検索の性能が悪くなるなど性能面に影響が出ることがあります。

付録 A.8　各種機能が自動実行されるタイミング

管理対象の OS が Windows の場合

各種機能が自動的に実行されるタイミングは、それぞれ異なります。実行されるタイミングを次の表に示します。

なお、レポートの集計タイミングについては、「2.16.5　レポートの集計スケジュール」を参照してください。

機能		説明	実行されるタイミング
機器管理	エージェントレスでの情報収集	エージェントレスの機器の情報を定期的に収集して、最新の状態に更新します。	1 時間ごと※1
	Active Directory からの情報の取得	Active Directory で管理しているコンピュータを探索して、JP1/IT Desktop Management 2 に登録します。探索時に自動的にエージェントを配信することもできます。また、部署の構成を自動的に JP1/IT Desktop Management 2 に登録します。	毎日 23:00※1
	利用者情報の収集	資産管理項目の部署、設置場所、利用者名などの入力方法に［利用者が入力］を指定している場合、［利用者情報の入力］画面を利用者のコンピュータの画面に表示して、利用者が入力した情報を収集します。	利用者が情報の入力を完了したとき
	機器の変更履歴の取得	機器情報の変更があった場合、変更前の機器情報と変更後の機器情報の比較が実行されて、変更履歴を取得します。	毎日 0:00※2
	機器のメンテナンスによる削除候補機器の検出	あらかじめ定義した重複機器、不稼働機器の条件を満たす機器を削除候補機器として検出する処理を開始します。	毎日 23:00※2
セキュリティ管理	セキュリティ状況の判定	コンピュータから収集された機器情報を基に、セキュリティポリシーに応じて危険レベルを判定します。	毎日 0:00※1
	サポート情報の定期チェックおよび更新	設定画面の［サポートサービスの設定］に指定した更新ス	毎日決められた時刻（JP1/IT Desktop Management 2 の

機能		説明	実行されるタイミング
セキュリティ管理	サポート情報の定期チェックおよび更新	ケジュールに従って、サポートサービスサイトに接続し、更新プログラムおよび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および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。	セットアップが完了した時刻の分を切り上げた時刻）※1
	ウィルス対策製品の「エンジンバージョン」および「ウィルス定義ファイルバージョン」の更新	各コンピュータから収集された情報の中から、セキュリティポリシーに設定されたウィルス対策製品のエンジンバージョンおよびウィルス定義ファイルバージョンの最新情報を検知し、セキュリティポリシーの「エンジンバージョン」および「ウィルス定義ファイルバージョン」を最新に更新し、セキュリティ判定を実施します。	各コンピュータから収集された情報の中で、エンジンバージョンおよびウィルス定義ファイルのバージョンが更新されていたとき
操作ログ	操作ログの保管	コンピュータから取得した操作ログを保管します。	1 時間ごと
	操作ログの定期エクスポート	コンピュータから取得した操作ログを定期的にエクスポートします。	1 時間ごと
	操作ログの保管先フォルダに対する空き容量の監視	操作ログの保管先フォルダに対する空き容量を取得します。空き容量が不足している場合、イベントを出力します。イベントのメール通知機能を利用することで、管理者が容量不足を把握できます。	毎日 6:00※2
	操作ログのデータベースの削除とインデックスの再作成	操作ログのデータベースの、格納期間を超えた操作ログの削除、およびインデックス情報の再作成を実施します。手動取り込み済みの操作ログを削除した領域も解放され、データベース容量が効率良く使えるようになります。	毎日 1:00※2

機能		説明	実行されるタイミング
イベント	イベント発生の監視	あらかじめ指定したカテゴリおよび重要度のイベントが発生した場合、管理者にメールで通知します。	30 分ごと※1
その他	MDM システムからの情報取得	設定画面の［MDM 連携の設定］に指定した更新スケジュールに従って、MDM システムで管理しているスマートデバイスの情報を取得します。新規に取得したスマートデバイスの場合、新規機器として発見されます。すでに管理対象になっているスマートデバイスの場合、機器情報およびハードウェア資産情報が更新されます。	毎日決められた時刻（JP1/IT Desktop Management 2 のセットアップが完了した時刻の分を切り上げた時刻）※1
	データベースの使用中空きページの定期解放	データベースのデータを削除したときに発生する使用中空きページを解放することで、データベース容量を効率良く使えるようにします。	毎日 5:00※2

注※1　設定画面から実行のタイミングを設定できます。

注※2　コンフィグレーションファイルから実行のタイミングを設定できます。

管理対象の OS が UNIX、Mac の場合

機能が自動的に実行されるタイミングと通知される情報を次に示します。

機能が自動的に実行されるタイミング

契機となる機能	説明
マネージャ接続	OS が UNIX、Mac のコンピュータがエージェントとしてマネージャに接続されたとき、システム構成情報が通知されます。なお、UNIX エージェント、Mac エージェントのシステム構成情報は、リモートインストールマネージャのウィンドウで参照できます。機器画面などの操作画面ではシステム情報に含まれます。
ジョブ実行	「コンピュータ(UNIX)のシステム情報の取得」ジョブ、「コンピュータ(UNIX)のソフトウェア情報の取得」ジョブが実行されたとき、情報が通知されます。これらのジョブが Mac エージェントに対して実行された場合も同様です。
日立プログラムプロダクト配布	リモートインストールマネージャを使用した日立プログラムプロダクトの配布時に情報が通知されます。なお、Mac エージェントに対しては、日立プログラムプロダクトを配布できません。
システム変更	配布ジョブの実行や UNIX エージェント、Mac エージェントからのポーリングを契機に、システム変更を検知すると、情報が通知されます。

システム構成情報の項目

項目	説明
ノード属性	ノードの属性です。UNIX エージェント、Mac エージェントの場合、「エージェント」です。
ホスト識別子	エージェントによって生成される、機器を識別するためのユニークな ID です。UNIX エージェント、Mac エージェントのホスト識別子は、#U で始まる 28 バイトの文字列です。
ホスト名	コンピュータに割り当てられたホスト名（gethostname コマンドで取得されるホスト名）です。動作環境設定用ファイルのDMHOSTNAME が設定されている場合は、DMHOSTNAME の設定値が通知されます。
IP アドレス	ホスト名に割り当てられた IP アドレスです。動作環境設定用ファイルのDMIPADDR が設定されている場合は、DMIPADDR の設定値が通知されます。
MAC アドレス	IP アドレスが割り当てられた NIC の MAC アドレスが通知されます。
システム構成情報の作成日時	UNIX エージェント、Mac エージェントでのシステム構成情報の作成日時が通知されます。

付録 A.9　再起動によって設定が適用されるケース

JP1/IT Desktop Management 2 では、設定を適用するためにコンピュータの再起動が必要な場合があります。 次の場合に、再起動が必要です。

- セキュリティポリシーを編集または割り当てた場合
- 手動でセキュリティ対策を実施した場合

セキュリティポリシーを編集した場合

次の項目のうちどれかを編集したときに、編集したセキュリティポリシーが割り当てられているコンピュータを再起動してください。() 内には、該当するセキュリティ設定項目を示します。再起動すると編集後のセキュリティポリシーがコンピュータに適用されます。

- 自動更新の有効化の自動対策（更新プログラム）
- 管理共有の無効化の自動対策（OS のセキュリティ設定）
- 匿名接続の無効化の自動対策（OS のセキュリティ設定）
- ファイアウォールの有効化の自動対策（OS のセキュリティ設定）
  コンピュータの OS が、Windows Server 2003、および Windows XP の場合は、再起動は不要です。
- DCOM の無効化の自動対策（OS のセキュリティ設定）
- リモートデスクトップの無効化の自動対策（OS のセキュリティ設定）
- 機器の使用抑止（禁止操作）※
- 操作ログの取得（不審と見なす操作の取得を含む）の有効化または無効化（操作ログ）※

注※　機器の使用抑止と操作ログの取得は、セキュリティポリシーが割り当てられたタイミングで適用されます。ただし、機器の使用抑止や操作ログの一部の設定は再起動後に有効になるため、コンピュータの再起動を推奨します。

再起動後に有効となる設定を次に示します。

分類		設定項目
[操作ログ]	操作ログの取得対象	• ファイルコピー • ファイル移動 • ファイル名称変更 • ファイル作成 • ファイル削除 • ファイルアップロード • ファイルダウンロード • ファイル送信 • ファイル受信 • メール送信（添付ファイル付） • メール受信（添付ファイル付） • 添付ファイル保存 • フォルダコピー • フォルダ移動 • フォルダ名称変更 • フォルダ作成 • フォルダ削除
	不審とみなす操作	• 添付ファイル付きメールの送受信 • Web/FTP サーバの使用 • 外部メディア（リムーバブルディスク）へのファイルコピーと移動
[禁止操作]	書き込み抑止デバイスの一覧	• リムーバブルディスク • CD/DVD ドライブ • FD ドライブ

セキュリティポリシーを割り当てた場合

セキュリティポリシーを割り当てたコンピュータを再起動してください。再起動すると、割り当てたセキュリティポリシーがコンピュータに適用されます。

機器の使用抑止と操作ログの取得は、セキュリティポリシーが割り当てられたタイミングで適用されます。ただし、機器の使用抑止や操作ログの一部の設定は、再起動後に有効になることがあります。

手動でセキュリティ対策を実施した場合

次の設定項目を対策した場合に、対策を実施したコンピュータを再起動してください。（）内には、該当するセキュリティ設定項目を示します。再起動すると、セキュリティ対策が実行されます。

- 自動更新の有効化（更新プログラム）
- 管理共有の無効化（OS のセキュリティ設定）
- 匿名接続の無効化（OS のセキュリティ設定）
- ファイアウォールの有効化（OS のセキュリティ設定）
  コンピュータの OS が、Windows Server 2003、および Windows XP の場合は、再起動は不要です。
- DCOM の無効化（OS のセキュリティ設定）
- リモートデスクトップ接続の無効化（OS のセキュリティ設定）

付録 A.10　下位バージョンとの接続性

バージョンが異なる製品を接続した場合の互換性について説明します。

Agent と Manager との接続性

Agent	Manager																		
	09-50 J	09-50 M	09-51 J	10-00 J	10-01 J	10-01 M	10-02 J	10-10 J	10-10 M	10-50 J	10-50 M	11-00 J	11-01 J	11-10 J	11-50 J	11-51 J	12-00 J	12-10 J	12-50 J
09-50 J	○	×	△	△	△	×	△	△	×	△※1	×	△※1	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2
09-50 M	×	○	×	×	×	△	×	×	△	×	△※1	△※1	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2
09-51 J	×	×	○	△	△	×	△	△	×	△※1	×	△※1	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2
10-00 J	×	×	×	○	△	×	△	△	×	△※1	×	△※1	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2
10-01 J	×	×	×	×	○	×	△	△	×	△※1	×	△※1	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2

Agent	Manager																		
	09-50J	09-50M	09-51J	10-00J	10-01J	10-01M	10-02J	10-10J	10-10M	10-50J	10-50M	11-00J	11-01J	11-10J	11-50J	11-51J	12-00J	12-10J	12-50J
10-01M	×	×	×	×	×	○	×	×	△	×	△※1	△※1	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2
10-02J	×	×	×	×	×	×	○	△	×	△※1	×	△※1	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2
10-10J	×	×	×	×	×	×	×	○	×	△※1	×	△※1	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2
10-10M	×	×	×	×	×	×	×	×	○	×	△※1	△※1	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2	△※1、※2
10-50J	×	×	×	×	×	×	×	×	×	○	×	△	△※2	△※2	△※2	△※2	△※2	△※2	△※2
10-50M	×	×	×	×	×	×	×	×	×	×	○	△	△※2	△※2	△※2	△※2	△※2	△※2	△※2
11-00J	×	×	×	×	×	×	×	×	×	×	×	○	△※2	△※2	△※2	△※2	△※2	△※2	△※2
11-01J	×	×	×	×	×	×	×	×	×	×	×	×	○※2	△※2	△※2	△※2	△※2	△※2	△※2
11-10J	×	×	×	×	×	×	×	×	×	×	×	×	×	○※2	△※2	△※2	△※2	△※2	△※2
11-50J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○※2	△※2	△※2	△※2	△※2

Agent	Manager																		
	09-50 J	09-50 M	09-51 J	10-00 J	10-01 J	10-01 M	10-02 J	10-10 J	10-10 M	10-50 J	10-50 M	11-00 J	11-01 J	11-10 J	11-50 J	11-51 J	12-00 J	12-10 J	12-50 J
11-51 J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○ ※2	△ ※2	△ ※2	△ ※2
12-00 J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○ ※2	△ ※2	△ ※2
12-10 J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○ ※2	△ ※2
12-50 J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○ ※2

（凡例）

J：JP1/IT Desktop Management または JP1/IT Desktop Management 2

M：Job Management Partner 1/IT Desktop Management または Job Management Partner 1/IT Desktop Management 2

○：接続できる　△：各バージョンのエージェントの機能範囲内で接続できる　×：接続できない

注※1　禁止操作の抑止のセキュリティポリシーを変更できません。

注※2　Manager が JP1/IT Desktop Management 2 - Operations Director の場合は、JP1/IT Desktop Management 2 - Operations Director の Agent とだけ接続できます。

ネットワークモニタエージェントと Agent との接続性

ネットワークモニタエージェント	Agent																		
	09-50 J	09-50 M	09-51 J	10-00 J	10-01 J	10-01 M	10-02 J	10-10 J	10-10 M	10-50 J	10-50 M	11-00 J	11-01 J	11-10 J	11-50 J	11-51 J	12-00 J	12-10 J	12-50 J
09-50 J	○	×	△	△	△	×	△	△	×	△	×	△	△	△	△	△	△	△	△
09-50 M	×	○	×	×	×	△	×	×	△	×	△	△	△	△	△	△	△	△	△
09-51 J	×	×	○	△	△	×	△	△	×	△	×	△	△	△	△	△	△	△	△
10-00 J	×	×	×	○	△	×	△	△	×	△	×	△	△	△	△	△	△	△	△
10-01 J	×	×	×	×	○	×	△	△	×	△	×	△	△	△	△	△	△	△	△
10-01 M	×	×	×	×	×	○	×	×	△	×	△	△	△	△	△	△	△	△	△
10-02 J	×	×	×	×	×	×	○	△	×	×	×	△	△	△	△	△	△	△	△
10-10 J	×	×	×	×	×	×	×	○	×	△	×	△	△	△	△	△	△	△	△
10-1	×	×	×	×	×	×	×	×	○	×	△	△	△	△	△	△	△	△	△

ネットワークモニタエージェント	Agent																	
	09-50J	09-50M	09-51J	10-00J	10-01J	10-01M	10-02J	10-10J	10-10M	10-50J	10-50M	11-00J	11-01J	11-10J	11-50J	11-51J	12-00J	12-10J	12-50J
0M	×	×	×	×	×	×	×	×	○	×	△	△	△	△	△	△	△	△	△
10-50J	×	×	×	×	×	×	×	×	×	○	×	△	△	△	△	△	△	△	△
10-50M	×	×	×	×	×	×	×	×	×	×	○	△	△	△	△	△	△	△	△
11-00J	×	×	×	×	×	×	×	×	×	×	×	○	△	△	△	△	△	△	△
11-01J	×	×	×	×	×	×	×	×	×	×	×	×	○	△	△	△	△	△	△
11-10J	×	×	×	×	×	×	×	×	×	×	×	×	×	○	△	△	△	△	△
11-50J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	○	△	△	△
12-00J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	○	○

（凡例）

J：JP1/IT Desktop Management または JP1/IT Desktop Management 2

M：Job Management Partner 1/IT Desktop Management または Job Management Partner 1/IT Desktop Management 2

○：接続できる　△：各バージョンのエージェントの機能範囲内で接続できる　×：接続できない

リモコンエージェントとコントローラとの接続性

リモコンエージェント	コントローラ																		
	09-50 J	09-50 M	09-51 J	10-00 J	10-01 J	10-01 M	10-02 J	10-10 J	10-10 M	10-50 J	10-50 M	11-00 J	11-01 J	11-01 J	11-50 J	11-51 J	12-00 J	12-10 J	12-50 J
09-50 J	○	×	△	△	△	×	△	△	×	△	×	△	△	△	△	△	△	△	△
09-50 M	×	○	×	×	×	△	×	×	△	×	△	△	△	△	△	△	△	△	△
09-51 J	×	×	○	△	△	×	△	△	×	△	×	△	△	△	△	△	△	△	△
10-00 J	×	×	×	○	△	×	△	△	×	△	×	△	△	△	△	△	△	△	△
10-01 J	×	×	×	×	○	×	△	△	×	△	×	△	△	△	△	△	△	△	△
10-01 M	×	×	×	×	×	○	×	×	△	×	△	△	△	△	△	△	△	△	△
10-02 J	×	×	×	×	×	×	○	△	×	△	×	△	△	△	△	△	△	△	△
10-10 J	×	×	×	×	×	×	×	○	×	△	×	△	△	△	△	△	△	△	△
10-10 M	×	×	×	×	×	×	×	×	○	×	△	△	△	△	△	△	△	△	△
10-50 J	×	×	×	×	×	×	×	×	×	○	×	△	△	△	△	△	△	△	△

リモコンエージェント	コントローラ																	
	09-50J	09-50M	09-51J	10-00J	10-01J	10-01M	10-02J	10-10J	10-10M	10-50J	10-50M	11-00J	11-01J	11-01J	11-50J	11-51J	12-00J	12-10J	12-50J
10-50M	×	×	×	×	×	×	×	×	×	×	○	△	△	△	△	△	△	△	△
11-00J	×	×	×	×	×	×	×	×	×	×	×	○	△	△	△	△	△	△	△
11-01J	×	×	×	×	×	×	×	×	×	×	×	×	○	△	△	△	△	△	△
11-10J	×	×	×	×	×	×	×	×	×	×	×	×	×	○	△	△	△	△	△
11-50J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	△	△	△	△
11-51J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	△	△	△
12-00J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	△	△
12-10J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	△
12-50J	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○

（凡例）

J：JP1/IT Desktop Management または JP1/IT Desktop Management 2

M：Job Management Partner 1/IT Desktop Management または Job Management Partner 1/IT Desktop Management 2

○：接続できる　△：各バージョンのエージェントの機能範囲内で接続できる　×：接続できない

インターネットゲートウェイと Manager との接続性

インターネットゲートウェイ	Manager			
	11-51 J 以前	12-00 J	12-10 J	12-50 J
12-00 J	×	○	○	○

（凡例）

J：JP1/IT Desktop Management または JP1/IT Desktop Management 2

○：接続できる　×：接続できない

インターネットゲートウェイと Agent との接続性

Agent	インターネットゲートウェイ
	12-00 J
11-51 J 以前	－
12-00 J	○
12-10 J	○
12-50 J	○

（凡例）

J：JP1/IT Desktop Management または JP1/IT Desktop Management 2

○：接続できる　－：該当しない

付録 A.11　Windows エージェント、UNIX エージェント、Mac エージェントの機能差異

Windows 版、UNIX 版、Mac 版の JP1/IT Desktop Management 2 - Agent の機能差異について説明します。

用語の差異

Windows 版と UNIX 版では一部の用語が異なります。UNIX 版の JP1/IT Desktop Management 2 - Agent を使うときは、次のように用語を読み替えてください。

Windows 版の用語	UNIX 版の用語
ID	グループ id
インストール	組み込み※
キャビネット	資源グループ
ジョブ	指令

Windows 版の用語	UNIX 版の用語
パッケージャ	資源登録システム
リモートインストール	パッケージ配布（ソフトウェア配布）
リモートコレクト	ファイル収集

注※　UNIX では、インストールからセットアップまでを「組み込み」と称します。

機能差異

機能差異を次に示します。マネージャからエージェントへの操作のサポート状況を示しています。

リモートインストール（ソフトウェアの配布）

項目	Windows エージェント	UNIX エージェント	Mac エージェント
配布管理システム主導によるインストール	○	○	○
利用者自身によるインストール	○	○	×
JP1/IT Desktop Management 2 - Agent（エージェント）の配布	○	○ ※1	○ ※1
JP1/IT Desktop Management 2 - Agent（中継システム）の配布	○	×	×
システム条件によるインストール抑止	○	×	×
ソフトウェア条件によるインストール抑止	○	×	×
パッケージ条件によるインストール抑止	○	×	×
配布スケジュール	○	○	○
インストール日時の指定	○	○	○
インストールタイミングの指定	○ ※2	○ ※3	○ ※2
インストール後のコンピュータの自動再起動	○	○	○
処理中ダイアログの表示（パッケージの設定）	○	×	×
処理中ダイアログの表示（エージェントセットアップの設定）	○	×	×
リモートインストールと連携した外部プログラム起動	○ ※4	○ ※5	○ ※5
パッケージの自動インストール	○	○	○
AIT ファイルを使ったインストール	○	×	×
あて先グループを指定したインストール	○	○	○
ID を指定したインストール	○	○	○
分割配布	○	○ ※6	○ ※6

項目	Windows エージェント	UNIX エージェント	Mac エージェント
マルチキャスト配布	○	×	×
ジョブの中断と再開	○	○	○
中断中のジョブ配布	○	○	○
クライアント制御によるリモート起動とシャットダウン	○	○ ※7	○ ※7
オフラインインストール	○	×	×

（凡例）○：サポートあり　×：サポートなし

注※1　リモートインストールマネージャを使用した配布ができます。

注※2　通常インストール（[すぐに実行]）、システム起動時インストール（[次回起動時に実行]）

注※3　通常インストール（[すぐに実行]）、システム起動時インストール（[次回起動時に実行]）、システム停止時インストール（[停止時に実行]）

注※4　外部プログラムを起動できるのは配布前後とエラー時です。

注※5　外部プログラムを起動できるのは配布前後です。

注※6　エンド WS の場合だけ分割配布できます。

注※7　ジョブ実行後に UNIX エージェント、Mac エージェントをシャットダウンすることはできません。

パッケージング

項目	Windows エージェント	UNIX エージェント	Mac エージェント
パッケージデータの圧縮	○	○	○

（凡例）○：サポートあり

リモートコレクト（ファイルの収集）

項目	Windows エージェント	UNIX エージェント	Mac エージェント
リモートコレクト	○	○	×
収集パス名※1	○	○	×
収集タイミングの指定	○ ※2	○ ※2	×
リモートコレクトと連携した外部プログラム起動	○	○（収集前後）	×
クライアント制御によるリモート起動とシャットダウン	○	○ ※3	×
収集ファイルの圧縮	○	○	×

（凡例）○：サポートあり　×：サポートなし

注※1　指定できる収集パス名の最大文字数を次に示します。

- Windows エージェント：半角 256 文字
- UNIX エージェント：半角 63 文字

注※2　エージェント起動時、エージェント稼働中

注※3　ジョブ実行後に UNIX エージェントをシャットダウンすることはできません。

リモートコントロール

項目	Windows エージェント	UNIX エージェント	Mac エージェント
エージェントのリモートコントロール	○	×	○ ※
リモートコントロール機能を利用したファイル転送	○	×	×

（凡例）○：サポートあり　×：サポートなし

注※　RFB 接続によるリモートコントロールができます。

インターネットゲートウェイ

項目	Windows エージェント	UNIX エージェント	Mac エージェント
インターネットゲートウェイを介したコンピュータの管理	○	×	×

（凡例）○：サポートあり　×：サポートなし

付録 A.12　Asset Console を使用して資産管理をする場合の制限事項

Asset Console を使用して資産管理をする際に、管理用サーバのセットアップで［操作画面での資産情報の操作を抑止する］をチェックした場合の制限を説明します。

メモ

設定画面の［資産管理］－［削除機器関連ハードウェア資産の資産状態の設定］画面で、［削除した機器に関連するハードウェア資産の資産状態を変更する］をチェックしても、Asset Console で管理している資産情報には反映されません。

資産画面

［ハードウェア資産］画面で、資産情報の追加ができません。また、［機器種別］が［USB デバイス］以外のハードウェア資産情報を削除したり編集したりしても、Asset Console で管理している資産情報には反映されません。

次の画面で、資産情報の追加、編集、削除および参照ができません。

- ［資産情報をインポートしましょう］ウィザード※
- ［ソフトウェアライセンス］画面
- ［管理ソフトウェア］画面
- ［ソフトウェアライセンス状況］画面
- ［契約］画面

注※ ［ハードウェア資産情報］に対する追加および編集はできます。ただし、Asset Console で管理している資産情報には反映されません。

機器画面

次の画面で、ソフトウェアライセンスの移管や管理ソフトウェアの追加ができません。

- ［機器情報］画面
- ［ソフトウェア情報］画面

設定画面

次の画面で、契約者リストの追加・編集・削除や、契約会社一覧のインポートができません。

- ［契約会社リストの設定］画面

付録 A.13　JP1/IT Desktop Management 2 - Operations Director での機能制限

JP1/IT Desktop Management 2 - Operations Director には、JP1/IT Desktop Management 2 - Manager と比較して一部の機能に制限があります。制限されている機能を次の表に示します。

制限されている機能	説明
複数サーバ構成での運用	JP1/IT Desktop Management 2 - Operations Director では、単数サーバ構成での運用だけサポートしています。管理対象にできるコンピュータの台数は 1,000 台までです。 統括管理用サーバ、管理用中継サーバ、および中継システムを設置した、複数サーバ構成での運用はできません。
リモートインストールマネージャを使用した配布	JP1/IT Desktop Management 2 - Operations Director では、JP1/IT Desktop Management 2 の操作画面を使用して配布する方法（ITDM 互換配布）だけサポートしています。Remote Install Manager はサポートしていません。
Asset Console を使用した資産管理	JP1/IT Desktop Management 2 - Operations Director では、JP1/IT Desktop Management 2 の操作画面を使用して資産管理をする方法だけサポートしています。
UNIX 機器の管理	JP1/IT Desktop Management 2 - Operations Director のエージェントは、OS が Windows、Mac のコンピュータをサポートしています。
他 JP1 製品との連携	JP1/IT Desktop Management 2 - Operations Director では、次に示す他 JP1 製品とは連携できません。

制限されている機能	説明
他 JP1 製品との連携	• JP1/NETM/NM - Manager • JP1/IM • JP1/IT Desktop Management 2 - Smart Device Manager JP1/IT Desktop Management 2 - Operations Director が連携できる MDM システムは、MobileIron だけです。 • JP1/Audit Management - Manager

関連リンク

- 2.18　複数の部門やネットワークで構成される大規模システムの管理
- 4.4.3　複数サーバ構成
- 2.12　リモートインストールマネージャを使用したソフトウェアおよびファイルの配布
- 2.11　資産の管理
- 2.5　エージェントの導入
- 2.8.20　JP1/NETM/NM - Manager 連携によるネットワーク制御機能
- 2.15.4　JP1/IM のイベントコンソールでのイベントの確認
- 2.23　スマートデバイスの制御
- 4.4.8　MDM 連携構成

付録 A.14　各バージョンの変更内容

(1)　12-50 の変更内容

(a)　資料番号（3021-3-E12-20）の変更内容

- ネットワークモニタを有効にした機器を強制的に削除できるようにした。
- ネットワークモニタ設定で、許可されていない機器がネットワークに接続された時にイベントを発行できるようにした。
- 資産の関連づけ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。
- CentOS 8.1、Red Hat Enterprise Linux(R) Server 8、および Oracle Linux 8 を、エージェントを導入するコンピュータの前提となる OS に追加した。

(2)　12-10 の変更内容

(a)　資料番号（3021-3-E12-10）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。
- [ハードウェア資産の費用] レポートおよび [ソフトウェアライセンスの費用] レポートに、レポート表示時点の契約情報から集計した費用を表示できるようにした。また、[その他の費用] レポートを追加した。
- 共有型 VDI の仮想コンピュータを管理できるようにした。
- 管理画面を HTML5 に変更した。また、管理者のコンピュータの前提条件から Adobe Flash Player を削除した。
- 管理用サーバのセットアップ時のパラメーターで、[コンポーネントの自動更新] のデフォルト値を「チェックしない」に変更した。
- MDM 連携構成に対応する MobileIron のバージョンに V10 を追加した。

(3) 12-00 の変更内容

(a) 資料番号（3021-3-E12）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
- 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。
- Windows の累積的な更新プログラムおよびセキュリティマンスリー品質ロールアップのセキュリティ判定を改善した。
- エージェントを導入するコンピュータの前提となる OS に次の OS を追加した。
  - macOS 10.13
  - macOS 10.14
- NAT 環境構成を追加した。

(4) 11-51 の変更内容

(a) 資料番号（3021-3-B52-40）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。
- 秘文ログを JP1/IT Desktop Management 2 に取り込めるようにした。
- ハードウェア資産情報のインポート時に、ハードウェア資産情報が引き当てられなかった場合新規のハードウェア資産情報として登録するかどうかを選択できるようにした。
- リモートインストールマネージャで 2 ギガバイトを超えるファイルを配布できるようにした。

(5) 11-50 の変更内容

(a) 資料番号（3021-3-B52-30）の変更内容

- 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。
- 管理ソフトウェア情報にソフトウェアのインストール先の OS 情報を追加し、同名ソフトウェアに対してインストール先の OS ごとにライセンス管理ができるようにした。
- BitLocker によるドライブ暗号化状態の情報を取得できるようにした。
- 機器情報のセキュリティ情報で収集できる、アカウント情報およびスクリーンセーバー情報の上限ユーザー数を 60 に変更した。
- インストールソフトウェア情報として購入形態および GUID を収集できる製品に、次の製品を追加した。
  - Microsoft Office Professional Plus 2016
  - Microsoft Office Standard 2016
  - Microsoft Skype for Business 2016
  - Microsoft Access 2016
  - Microsoft Excel 2016
  - Microsoft Outlook 2016
  - Microsoft PowerPoint 2016
  - Microsoft Project Professional 2016
  - Microsoft Project Standard 2016
  - Microsoft Publisher 2016
  - Microsoft Visio Professional 2016
  - Microsoft Visio Standard 2016
  - Microsoft Word 2016
- コマンドを使用して機器のネットワーク接続を制御できるようにした。

- 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。
- 部署、設置場所、または関連づけられている資産を条件に USB デバイスを使用する資産を限定できるようにした。
- 管理用サーバに登録している更新プログラム一覧の情報を CSV ファイルにエクスポートできるようにした。また、エクスポートしたパッチ情報 CSV ファイルを元の管理用サーバや別の管理用サーバにインポートできるようにした。
- サポートするウィルス対策製品を追加した。

(6) 11-10 の変更内容

(a) 資料番号（3021-3-B52-20）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
- 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（機器種別は「PC」）。
  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
- 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。
- オフライン管理のコンピュータの機器情報を初めて取得した場合の機器状態を設定できるようにした。
- Windows ストアアプリの情報を、インストールソフトウェア情報として収集できるようにした。
- サポートするウィルス対策製品を追加した。

- JP1/IT Desktop Management 2 - Agent の適用 OS として次を追加した。
  Red Hat Enterprise Linux 5
- 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。

(7) 11-01 の変更内容

(a) 資料番号（3021-3-B52-10）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。
- 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できるようにした。
- 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かどうかを設定できるようにした。
- 機器が削除されたときに、関連するハードウェア資産の資産状態を自動で変更できるようにした。
- Windows の OS のバージョンを取得できるようにした。
- システム情報として収集できる情報のカーネルバージョンの説明を修正した。
- Windows エージェントのインストールソフトウェア情報の記載を修正した。
- バージョン 11 の秘文（秘文 DC、秘文 DE および秘文 DP）の情報を収集できるようにした。
- スマートデバイスのソフトウェアを管理できるようにした。
- UNIX エージェントのリモートコントロール機能について記載を削除した。
- サポートするウィルス対策製品を追加した。
- 操作ログの保管先フォルダに、旧製品（JP1/IT Desktop Management）の操作ログのバックアップファイルを格納している場合に表示されるツールチップの説明を修正した。
- 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として、管理用サーバからエージェントへパッケージを送信する場合の最大転送速度を設定できるようにした。
- 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。
- 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。
- 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。
- 下位バージョンとの接続性について、11-01 を追記した。また、Agent と Manager との接続性の表に、禁止操作の抑止のセキュリティポリシーに関する脚注を追加した。

(8) 11-00 の変更内容

(a) 資料番号（3021-3-B52）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。
- ネットワーク制御リストが更新されるタイミングを記載した。
- ネットワーク接続可否の情報をインポートおよびエクスポートできることを追加した。
- 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
- 次の Web ブラウザおよびメーラーを操作ログの取得対象外とした。
  - Internet Explorer 7
  - Internet Explorer 8
  - Microsoft Outlook Express 6
  - Windows メール 6
- MDM 連携構成に対応する MobileIron のバージョンに 7.5 を追加した。
- MDM と連携した場合に、JP1/IT Desktop Management 2 - Smart Device Manager から取得できる機器情報の、取得元を追記した。
- サポートするウィルス対策製品に次の製品を追加した。
  日本語のウィルス対策製品
  - ウイルスバスター クラウド 8.0
  - ウイルスバスター コーポレートエディション 11.0
  - ウイルスバスター ビジネスセキュリティサービス 5.7.1193
  - ESET NOD32 Antivirus 8.0
  - Sophos Endpoint Security and Control for Windows 10.3.11、10.3.13
  - Symantec Endpoint Protection 12.1.5

英語のウィルス対策製品

- Avira Professional Security 14.0.4、14.0.7
- Kaspersky Endpoint Security 10 for Windows 10.2
- McAfee SaaS Endpoint Protection 6.0
- OfficeScan Corporate Edition 11.0
- Sophos Endpoint Security and Control for Windows 10.3.7、10.3.11
- Symantec Endpoint Protection 12.1.4、12.1.5
- Titanium Internet Security 2015

- 日本語版のウィルス対策製品の常駐・非常駐の判定条件に、次のウィルス対策製品の場合の条件を追記した。
  - ESET Endpoint アンチウイルス
  - ESET File Security for Microsoft Windows Server
  - Kaspersky Endpoint Security 8 for Windows
  - Kaspersky Endpoint Security 10 for Windows
  - Sophos Endpoint Protection - Advanced
  - Sophos Endpoint Protection - Basic
  - Sophos Endpoint Protection - Enterprise
  - Sophos Endpoint Security and Control for Windows
- ウィルスバスターおよびウィルスバスタークラウドの常駐・非常駐の判定条件を見直した。
- 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。
- 制限値一覧の記載を更新した。
- JP1/IT Desktop Management 2 - Agent 変更の検知の設定を無効にした場合の説明を追記した。
- 下位バージョンとの接続性について、11-00 を追記した。
- 性能と見積もりの記載を更新した。
- Asset Console を使用して資産管理をする場合の制限事項を追記した。
- 機器情報の収集に関連するリンクを削除した。
- 資産情報の管理項目一覧にホスト識別子を追加した。
- 機器とハードウェア資産の同定で利用できる項目に、ホスト識別子を追加した。
- インポートできるハードウェア資産情報の項目と記述形式に、ホスト識別子を追加した。
- 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(機器種別は「サーバ」)。
- 操作画面を表示できるブラウザのうち、Firefox のバージョンを 31 以降に変更した。
- 操作画面を表示するために必要な Adobe Flash Player のバージョンを 13.0 以降以降に変更した。

- 操作ログを取り込む場合に、取り込み範囲に取り込み済みのデータが含まれているときは、操作ログがすべて上書きされることを追記した。
- 操作ログを手動で取り込む場合に、データベースに取り込める操作ログの最大日数の算出方法について追記した。
- 操作ログの保管先を設定していない場合、操作ログの自動取り込みを有効にすると、操作ログは、操作ログのデータベースに自動的に取り込まれるが、操作ログの保管先フォルダには保管されないことを追記した。
- 操作ログの、Web アクセス監視用のアドオン名を「JP1/IT Desktop Management 2 BHO」に変更した。
- 操作ログの、ファイルのアップロード監視用のアドオン名を「JP1/IT Desktop Management 2 FUO」に変更した。
- デバイスの使用抑止の注意事項に、USB デバイス以外のデバイスをコンピュータに接続して抑止された場合、再度接続しても抑止メッセージの表示、接続・切断・抑止ログ、および抑止イベントの取得はできないことを追記した。
- USB デバイスの使用抑止の注意事項に、同一個体のデバイスであっても、通常認識された場合と UASP 認識された場合の両方を資産に登録する必要があることを追記した。
- [ヘルプ] メニューから JP1/IT Desktop Management 2 のヘルプを削除した。
- （資料番号（3021-3-368）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。

(9) 10-50 の変更内容

(a) 資料番号（3021-3-274、3021-3-368）の変更内容

- 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。
- 次のデバイスの使用を抑止できるようにした。
  - Bluetooth デバイス
  - イメージングデバイス
  - Windows ポータブルデバイス

また、Windows 8、Windows Server 2012、Windows 7、Windows Server 2008、および Windows Vista でリムーバブルディスクとして使用を抑止していた次のデバイスをデバイスの種類ごとに抑止できるようにした。

- USB デバイス
- IEEE1394 デバイス
- 内蔵 SD カード

- 使用を許可した USB デバイスに格納されているファイル一覧の取得を選択できるようにした。
- 機器の使用を抑止したことを示すメッセージを、利用者のコンピュータに表示するかどうかを設定できるようにした。
- [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。
- 次の操作に関わる操作ログを取得する条件を設定できるようにした。
  - ファイル操作
  - プログラムの起動と停止
  - ウィンドウ操作
- デバイス接続許可の操作ログを取得できるようにした。
- 禁止操作の抑止イベントと操作ログを上位システムに通知する間隔、および利用者のコンピュータ側で保持する期間の最大値を設定できるようにした。
- 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
  - JP1/IT Desktop Management 2 - RC Manager
- 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
- リモコンエージェントを使用できるバージョンに、JP1/IT Desktop Management 09-50 以降、および JP1/IT Desktop Management 2 10-50 を追加した。

- AMT の各機能を使用する場合に必要な AMT のバージョンが 9.5 までであることを追記した。
- サポートするウィルス対策製品に次の製品を追加した。
  - Kaspersky Endpoint Security 10 for Windows
  - Sophos Endpoint Security and Control for Windows
- サポートするウィルス対策製品のうち、次の製品の対応バージョンを変更した。
  - Norton AntiVirus
  - Symantec Endpoint Protection
  - McAfee SaaS Endpoint Protection
  - ウイルスバスター クラウド
  - ウイルスバスター ビジネスセキュリティ
  - Forefront Client Security
  - Kaspersky Endpoint Security 10 for Windows
  - ESET NOD32 Antivirus
  - F-Secure Client Security
- 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 MobileIron のバージョンを追加した。
- 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。
- サービス、プロセスを追加および変更した。
- メモリ所要量、ディスク占有量、および前提となる CPU を変更した。
- ネットワーク共有プリンタに対して、印刷の操作ログの取得、および印刷の抑止ができなくなった。
- SMTP サーバと通信する際のセキュリティ保護の接続方法から SSL を削除した。
- Active Directory の設定で、SSL 通信を有効にする機能を削除した。
- 管理用サーバのグローバル IP アドレスには、固定 IP アドレスを利用する必要があることを追記した。
- 使用禁止ソフトウェア、および使用必須ソフトウェアの判定でソフトウェア名は部分一致、バージョンは前方一致で判定することを追記した。
- ［タスク］画面からのアンインストールの対象は、指定されたソフトウェア名とバージョンに完全一致するソフトウェアだけであることを追記した。
- 配布したパッケージと同じ名前のファイルが配布先に存在する場合、配布したパッケージのアクセス権は、既存ファイルのアクセス権を継承することを追記した。
- ［カテゴリ別評価の状況］と［カテゴリ別評価と台数の推移］の評価レベルが異なる場合があることを追記した。

- リモートコントロールのエージェント設定の接続モードについて制御モードと監視モードの表記を入れ替えた。これに伴い、接続モードの決定方式の説明を変更した。
- リモートコントロール中のファイル転送では、OneDrive は使用できないことを追記した。
- 下位バージョンとの接続性について記載した。
- 収集できる機器の情報にホスト識別子を記載した。
- 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。

(10) 10-10 の変更内容

(a) 資料番号（3021-3-152-30）の変更内容

- 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。
- セキュリティ画面および機器画面で、任意の条件に従って管理対象のコンピュータを自動で振り分けられるグループを作成できるようにした。
- 管轄範囲が限定されている場合の操作画面の差異を訂正した。
- ネットワークの探索で、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。
- コンピュータ情報の空き容量の説明を次のように変更した。
  - ハードディスクの説明に論理ドライブの種類がローカルディスクであることを追記した。
  - ローカルディスクの空き容量の合計値が 9,223,372,036,854,775,807 バイトを超える場合は、9,223,372,036,854,775,807 バイトと表示されることを追記した。
- タスクトレイの JP1/IT Desktop Management のアイコンに表示されるバルーンヒントと、利用者情報の入力画面を、利用者のコンピュータに表示させるかどうかを選択できるようにした。
- MDM システムから取得できる機器情報のうち、システム情報の説明を変更した。また、MDM サーバ連携時のホスト名に「_」を使用している場合の説明を削除した。
- DHCP サーバがリースする IP アドレス 10 個が RRAS（Routing and Remote Access Service）の「Remote Access」機能によって確保される回避策を追記した。
- 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。
- サポートするウィルス対策製品のうち、次の製品の対応バージョンを訂正した。
  - ウイルスバスター コーポレートエディション
  - ウイルスバスター コーポレートエディション アドバンス
  - ウイルスバスター コーポレートエディション サーバ版
  - ウイルスバスター コーポレートエディション サーバ版 アドバンス

- ESET Endpoint アンチウイルス
- ESET File Security for Microsoft Windows Server
- OfficeScan Corporate Edition

また、ウィルス対策製品が ServerProtect for Windows NT/NetWare の場合の注意事項を追記した。

- ユーザー定義のセキュリティ設定の判定値に入力できる最小値を追記した。
- Windows のエクスプローラに表示される［正式ファイル名］または［元のファイル名］が、起動抑止するソフトウェアの［ファイル名］に設定したファイル名と一致する場合でも、ソフトウェアの実行ファイルのバージョン情報が破損または矛盾しているときは、起動抑止できないことがある旨を追記した。
- Web アクセス、ファイルのアップロード、およびファイルのダウンロードの操作ログを取得できる Web ブラウザから Firefox を削除した。
- 監視対象になるファイルの条件の説明を追記した。
- エージェントを導入したコンピュータから管理用サーバへ操作ログを送信してから、コンピュータ上の操作ログを削除するまでの間に処理が強制終了された場合、操作ログを重複して取得することがある旨を追記した。
- Internet Explorer 10 の場合、ファイルのアップロードの操作ログを取得できないことがある旨を追記した。
- 配布したパッケージのアクセス権は、配布先フォルダから継承されることを記載した。また、配布したパッケージのアクセス権を変更したい場合は、配布先のコンピュータで利用者が変更する必要があることを記載した。
- 配布による負荷の軽減についての記載を訂正した。
- 配布時の注意事項を追記した。
- MDM システムと連携してスマートデバイスを管理する場合の、スマートデバイスの前提 OS に Android を追加した。
- MDM 連携構成での JP1 スマートデバイス管理サービスの、バージョンの記述を変更した。
- サイトサーバの各データフォルダの空き容量が少なくなっている場合は、空き容量に応じてイベントが出力されたり、自動で JP1/IT Desktop Management の機能の一部が停止されたりするようにした。
- 操作ログのデータベースに必要なディスク容量の目安を変更した。
- 推奨ディスク容量の目安を変更した。
- 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。
- 設定画面の次の項目に設定できる値を修正した。
  - ［エージェント］－［エージェント設定］画面から表示できる［エージェント設定項目］の［USB デバイス登録の設定］の項目
  - ［機器］－［AMT の設定］画面の項目

- ［他システムとの接続］－［Active Directory の設定］画面の項目
- ［他システムとの接続］－［MDM 連携の設定］画面の項目

- 次のサーバのメモリ使用量を変更した。
  - シングルサーバ構成システムの管理用サーバ
  - マルチサーバ構成システムのデータベースサーバ

(b) 資料番号（3021-3-337-10）の変更内容

- 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。
- セキュリティ画面および機器画面で、任意の条件に従って管理対象のコンピュータを自動で振り分けられるグループを作成できるようにした。
- ［ソフトウェアライセンス状況］画面で、管理ソフトウェアごとにソフトウェアライセンスの利用状況を管理できるようにした。
- 機器情報の変更履歴を取得できるようにした。
- ユーザーアカウントに設定した管轄範囲に合わせて、ソフトウェアライセンスおよび契約の表示範囲を限定できるようにした。
- 管轄範囲が限定されている場合の操作画面の差異を訂正した。
- ネットワークの探索で、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。
- 基本構成システムで管理対象にできる機器の上限が、次の台数であるとわかるようにした。
  - 操作ログを取得する場合：3,000 台
  - 操作ログは取得しないが、配布機能を使用する場合：5,000 台
  - 操作ログを取得しないで、配布機能も使用しない場合：10,000 台
- エージェントレス管理（認証成功）のアイコンは、Windows の管理共有または SNMP による認証ができている状態であることを追記した。
- コンピュータ情報のコンピュータ名およびコンピュータの説明に、SNMP 認証の場合およびスマートデバイスの場合の説明を追加した。また、コンピュータ情報の空き容量の説明を次のように変更した。
  - ハードディスクの説明に論理ドライブの種類がローカルディスクであることを追記した。
  - ローカルディスクの空き容量の合計値が 9,223,372,036,854,775,807 バイトを超える場合は、9,223,372,036,854,775,807 バイトと表示されることを追記した。
- インストールソフトウェア情報として購入形態および GUID を収集できる製品に、次の製品を追加した。

  日本語版の Microsoft Office 製品
  - Microsoft Office Access 2003
  - Microsoft Office Excel 2003

- Microsoft Office FrontPage 2003
- Microsoft Office Outlook 2003
- Microsoft Office Personal Edition 2003
- Microsoft Office PowerPoint 2003
- Microsoft Office Professional Edition 2003
- Microsoft Office Professional Enterprise Edition 2003
- Microsoft Office Project Professional 2003
- Microsoft Office Project Standard 2003
- Microsoft Office Publisher 2003
- Microsoft Office Standard Edition 2003
- Microsoft Office Visio 2003 Professional
- Microsoft Office Visio 2003 Standard
- Microsoft Office Word 2003

日本語版、英語版、および中国語版の Microsoft Office 製品

- Microsoft Access 2013
- Microsoft Excel 2013
- Microsoft InfoPath 2013
- Microsoft Lync 2013
- Microsoft Office Professional Plus 2013
- Microsoft Office Standard 2013
- Microsoft OneNote 2013
- Microsoft Outlook 2013
- Microsoft PowerPoint 2013
- Microsoft Project Professional 2013
- Microsoft Project Standard 2013
- Microsoft Publisher 2013
- Microsoft Visio Professional 2013
- Microsoft Visio Standard 2013
- Microsoft Word 2013

- Windows のコントロールパネルの［プログラムと機能］だけに表示されるソフトウェアに関する注意事項を追記した。

- タスクトレイの Job Management Partner 1/IT Desktop Management のアイコンに表示されるバルーンヒントと、利用者情報の入力画面を、利用者のコンピュータに表示させるかどうかを選択できるようにした。
- 利用者が利用者情報の入力を開始できる日時を、システム管理者が設定画面で設定できるようにした。
- メニューエリアに表示されるグループのうち、部署・設置場所の定義から削除した階層に対応するグループを、一括で削除できるようにした。
- 探索時に SNMP だけ認証できたコンピュータを管理対象にしている場合に、あとから Windows の管理共有の認証を設定して認証できるという記述を削除した。
- MDM システムから取得できる機器情報のうち、システム情報の説明を変更した。また、MDM サーバ連携時のホスト名に「_」を使用している場合の説明を削除した。
- リモートコントロール時の注意事項を訂正した。
- 特例接続の設定が必須となる場合と、それに対応する［ネットワークへの接続を許可しない機器の特例接続］の設定例を記載した。また、DHCP サーバがリースする IP アドレス 10 個が RRAS（Routing and Remote Access Service）の「Remote Access」機能によって確保される回避策を追記した。
- ネットワーク接続が遮断された機器に対して、ネットワーク接続を許可した場合の注意事項を追記した。
- 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
- 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。
- ［ネットワークへの接続を許可しない機器の特例接続］に登録するコンピュータには、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必要があるという記述を削除した。
- セキュリティポリシーにコンピュータのセキュリティ設定に関する任意のポリシーを追加し、任意の判定条件でセキュリティ判定できるようにした。
- サポートするウィルス対策製品の説明を次のとおり変更した。

  サポートするウィルス対策製品に次の製品を追加した。
  - ESET Endpoint アンチウイルス （32bit、64bit）
  - ESET File Security for Microsoft Windows Server （32bit、64bit）
  - 英語版 Symantec Endpoint Protection 12.1（32bit、64bit）

  サポートするウィルス対策製品のうち、次の製品の対応バージョンを追加した。
  - 日本語版 Forefront Client Security
  - 英語版 Forefront Client Security

  サポートするウィルス対策製品のうち、次の製品の対応バージョンを訂正した。
  - ウイルスバスター コーポレートエディション

- ウイルスバスター コーポレートエディション アドバンス
- ウイルスバスター コーポレートエディション サーバ版
- ウイルスバスター コーポレートエディション サーバ版 アドバンス
- 日本語版 Forefront Client Security
- OfficeScan Corporate Edition
- 英語版 Forefront Client Security

次の製品で完全スキャンを実行する場合、「すべてのハードディスク」、「システムメモリ」および「スタートアップオブジェクト」をスキャンしたときだけ、ウィルススキャン最終完了日時が収集できることを追記した。

- 日本語版のウィルス対策製品
  - ・Kaspersky Open Space Security Server （32bit、64bit）
  - ・Kaspersky Open Space Security Workstation （32bit、64bit）
  - ・Kaspersky Endpoint Security 8 for Windows （32bit、64bit）
- 英語版のウィルス対策製品
  - ・Kaspersky Open Space Security Server 6.0.4 （32bit、64bit）
  - ・Kaspersky Open Space Security Workstation 6.0.4 （32bit、64bit）

ウィルス対策製品が ServerProtect for Windows NT/NetWare の場合の注意事項を追記した。

- ユーザー定義のセキュリティ設定の判定値に入力できる最小値を追記した。
- Windows のエクスプローラに表示される［正式ファイル名］または［元のファイル名］が、起動抑止するソフトウェアの［ファイル名］に設定したファイル名と一致する場合でも、ソフトウェアの実行ファイルのバージョン情報が破損または矛盾しているときは、起動抑止できないことがある旨を追記した。
- Web アクセス、ファイルのアップロード、およびファイルのダウンロードの操作ログを取得できる Web ブラウザから Firefox を削除した。
- サポート対象の Web ブラウザに、Windows Internet Explorer 11 を追加した。
- 操作ログの取得対象となるメーラーに、Microsoft Office Outlook 2013 および Windows Live メール 2012 を追加した。
- 監視対象になるファイルの条件の説明を追記した。
- エージェントを導入したコンピュータから管理用サーバへ操作ログを送信してから、コンピュータ上の操作ログを削除するまでの間に処理が強制終了された場合、操作ログを重複して取得することがある旨を追記した。
- Internet Explorer 10 の場合、ファイルのアップロードの操作ログを取得できないことがある旨を追記した。
- 配布したパッケージのアクセス権は、配布先フォルダから継承されることを記載した。また、配布したパッケージのアクセス権を変更したい場合は、配布先のコンピュータで利用者が変更する必要があることを記載した。

- 配布による負荷の軽減についての記載を訂正した。
- 配布時の注意事項を追記した。
- Job Management Partner 1/IM との連携で、管理対象のコンピュータで発生した障害系イベントを Job Management Partner 1/IM のイベントコンソールで監視できる、としていた個所を、重要イベントも監視できるという記載に変更した。
- 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。
- エージェントを導入するコンピュータの前提条件を訂正した。
- MDM システムと連携してスマートデバイスを管理する場合の、スマートデバイスの前提 OS に Android を追加した。
- 次の場合はサイトサーバ構成で運用するとわかるようにした。
  - 操作ログを取得する場合で、3,000 台を超える機器を管理対象にするとき
  - 操作ログは取得しないが、配布機能を使用する場合で、5,000 台を超える機器を管理対象にするとき

  また、1 台のサイトサーバで管理できる機器の上限が、次の台数であるとわかるようにした。
  - 操作ログを取得する場合：1,000 台
  - 操作ログを取得しない場合：3,000 台
- 連携できる MDM システムに、MobileIron の 5.8 を追加した。
- サイトサーバの各データフォルダの空き容量が少なくなっている場合は、空き容量に応じてイベントが出力されたり、自動で Job Management Partner 1/IT Desktop Management の機能の一部が停止されたりするようにした。
- 操作ログのデータベースに必要なディスク容量の目安を変更した。
- 推奨ディスク容量の目安を変更した。
- 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。
- 設定画面の次の項目に設定できる値を修正した。
  - ［エージェント］－［エージェント設定］画面から表示できる［エージェント設定項目］の［USB デバイス登録の設定］の項目
  - ［機器］－［AMT の設定］画面の項目
  - ［他システムとの接続］－［Active Directory の設定］画面の項目
  - ［他システムとの接続］－［MDM 連携の設定］画面の項目
- 次のサーバのメモリ使用量を変更した。
  - シングルサーバ構成システムの管理用サーバ
  - マルチサーバ構成システムのデータベースサーバ
- エージェントの更新確認が自動実行される記述を削除した。

(11) 10-02 の変更内容

(a) 資料番号（3021-3-152-20）の変更内容

- 機器情報の変更履歴を取得できるようにした。
- ［ソフトウェアライセンス状況］画面で、管理ソフトウェアごとにソフトウェアライセンスの利用状況を管理できるようにした。
- ユーザーアカウントに設定した管轄範囲に合わせて、ソフトウェアライセンスおよび契約の表示範囲を限定できるようにした。
- 管轄範囲が限定されている場合の操作画面の差異を示した表を訂正した。
- 基本構成システムで管理対象にできる機器の上限が、次の台数であるとわかるようにした。
  - 操作ログを取得する場合：3,000 台
  - 操作ログは取得しないが、配布機能を使用する場合：5,000 台
  - 操作ログを取得しないで、配布機能も使用しない場合：10,000 台
- エージェントレス管理（認証成功）のアイコンは、Windows の管理共有または SNMP による認証ができている状態であることを追記した。
- コンピュータ情報のコンピュータ名およびコンピュータの説明に、SNMP 認証の場合およびスマートデバイスの場合の説明を追加した。
- インストールソフトウェア情報として購入形態および GUID を収集できる製品に、次の製品を追加した。
  - Microsoft Office Personal Edition 2003
  - Microsoft Office Professional Edition 2003
  - Microsoft Office Professional Enterprise Edition 2003
  - Microsoft Office Professional Plus 2013
  - Microsoft Office Standard Edition 2003
  - Microsoft Office Standard 2013
  - Microsoft Lync 2013
  - Microsoft Office Access 2003
  - Microsoft Access 2013
  - Microsoft Office Excel 2003
  - Microsoft Excel 2013
  - Microsoft Office FrontPage 2003
  - Microsoft InfoPath 2013
  - Microsoft OneNote 2013
  - Microsoft Office Outlook 2003

    - Microsoft Outlook 2013
    - Microsoft Office PowerPoint 2003
    - Microsoft PowerPoint 2013
    - Microsoft Office Project Professional 2003
    - Microsoft Project Professional 2013
    - Microsoft Office Project Standard 2003
    - Microsoft Project Standard 2013
    - Microsoft Office Publisher 2003
    - Microsoft Publisher 2013
    - Microsoft Office Visio 2003 Professional
    - Microsoft Office Visio 2003 Standard
    - Microsoft Visio Professional 2013
    - Microsoft Visio Standard 2013
    - Microsoft Office Word 2003
    - Microsoft Word 2013
- Windows のコントロールパネルの［プログラムと機能］だけに表示されるソフトウェアに関する注意事項を追記した。
- 利用者が利用者情報の入力を開始できる日時を、システム管理者が設定画面で設定できるようにした。
- メニューエリアに表示されるグループのうち、部署・設置場所の定義から削除した階層に対応するグループを、一括で削除できるようにした。
- 探索時に SNMP だけ認証できたコンピュータを管理対象にしている場合に、あとから Windows の管理共有の認証を設定して認証できるという記述を削除した。
- リモートコントロール時の注意事項を訂正した。
- 特例接続の設定が必須となる場合と、それに対応する［ネットワークへの接続を許可しない機器の特例接続］の設定例を記載した。
- ネットワーク接続が遮断された機器に対して、ネットワーク接続を許可した場合の注意事項を追記した。
- 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
- ［ネットワークへの接続を許可しない機器の特例接続］に登録するコンピュータには、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必要があるという記述を削除した。

- セキュリティポリシーにコンピュータのセキュリティ設定に関する任意のポリシーを追加し、任意の判定条件でセキュリティ判定できるようにした。
- サポートするウィルス対策製品に次の製品を追加した。
  - ESET Endpoint アンチウイルス （32bit、64bit）
  - ESET File Security for Microsoft Windows Server （32bit、64bit）
- 次の製品で完全スキャンを実行する場合、「すべてのハードディスク」、「システムメモリ」および「スタートアップオブジェクト」をスキャンしたときだけ、ウィルススキャン最終完了日時が収集できることを追記した。

  日本語版のウィルス対策製品
  - Kaspersky Open Space Security Server （32bit、64bit）
  - Kaspersky Open Space Security Workstation （32bit、64bit）
  - Kaspersky Endpoint Security 8 for Windows （32bit、64bit）

  英語版のウィルス対策製品
  - Kaspersky Open Space Security Server 6.0.4 （32bit、64bit）
  - Kaspersky Open Space Security Workstation 6.0.4 （32bit、64bit）
- 操作ログの取得対象となるメーラーに、Microsoft Office Outlook 2013 および Windows Live メール 2012 を追加した。
- JP1/IM との連携で、管理対象のコンピュータで発生した障害系イベントを JP1/IM のイベントコンソールで監視できる、としていた個所を、重要イベントも監視できるという記載に変更した。
- 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。
- 次の場合はサイトサーバ構成で運用するとわかるようにした。
  - 操作ログを取得する場合で、3,000 台を超える機器を管理対象にするとき
  - 操作ログは取得しないが、配布機能を使用する場合で、5,000 台を超える機器を管理対象にするとき

  また、1 台のサイトサーバで管理できる機器の上限が、次の台数であるとわかるようにした。
  - 操作ログを取得する場合：1,000 台
  - 操作ログを取得しない場合：3,000 台
- エージェントの更新確認が自動実行される記述を削除した。

(12) 10-01 の変更内容

(a) 資料番号（3021-3-152-10）の変更内容

- 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。

- 資産管理時に、ソフトウェア種別と、一部のソフトウェアの購入形態、プロダクト ID、および GUID を管理できるようにした。また、ソフトウェア種別を管理するために、SAMAC ソフトウェア辞書のオフライン更新用ファイル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。
- ファイル持ち出しによる不審と見なす操作と、印刷による不審と見なす操作で、画面表示や調査方法などが異なることを明記した。
- ホーム画面および資産画面の、管轄範囲が限定されている場合の差異を訂正した。
- 機器画面の［ソフトウェア情報］画面から、ソフトウェアを管理ソフトウェアに追加できるようにした。
- 探索するネットワークの範囲内にサイトサーバを設定している場合の説明を改善した。
- サイトサーバを設置する場合、ネットワークの探索を実行するには、管理用サーバとサイトサーバが互いに IP アドレスで直接参照できる必要があることを記載した。
- ループバックアドレスまたはブロードキャストアドレスがネットワークの探索の探索範囲に含まれている場合の注意事項を記載した。
- JP1/IT Desktop Management - Agent の適用 OS に、Windows 8 および Windows Server 2012 を追加した。
- Active Directory から取得できるシステム情報を示す表の、凡例の説明を改善した。
- 機器を特定するための情報を取得できなかった場合は、「SNMP 発見（認証情報不足）」と表示されることがあることを記載した。
- システム情報として収集できるコンピュータ情報に、ホスト名を記載した。
- 次の情報を収集するには、管理対象のコンピュータの OS で「Workstation」サービスが起動している必要があることを記載した。
  - 更新プログラム情報の Windows 自動更新
  - サービスのセキュリティ設定情報
  - OS のセキュリティ設定情報
- ［インストール済みコンピュータ］タブで確認できる項目の「登録日時」の説明を訂正した。
- コンピュータの電源を制御するための条件を訂正した。
- ［エージェント設定の追加］ダイアログおよび［エージェント設定の編集］ダイアログで、コンピュータの再起動のタイミングを設定できるようにした。これに伴い、エージェント導入済みのコンピュータに表示される［コンピュータのシャットダウン］ダイアログと［コンピュータの再起動］ダイアログの説明を変更した。
- 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、4.2.7 に集約した。
- MDM システムから取得できるシステム情報の取得可否を明確にした。また、凡例の説明を改善した。
- リモートコントロール時にエージェント導入済みのコンピュータにマウスが接続されていない場合、コントローラに表示されるマウスカーソルの形状は常に矢印カーソルのままとなることを記載した。

- ネットワーク接続を制御している場合で、新規機器のネットワーク接続を自動的に許可させたいときの方法を記載した。
- 機器の運用方法ごとに必要なネットワーク制御リストの設定を記載した。
- ネットワークモニタを有効化したコンピュータは、Windows ファイアウォールの判定の対象外であることを記載した。
- サポートするウィルス対策製品に次の製品を追加した。
  - Norton AntiVirus（32bit、64bit）
  - ウイルスバスター クラウド（32bit、64bit）
  - ウイルスバスター ビジネスセキュリティ 7.0（32bit、64bit）
  - Kaspersky Endpoint Security 8 for Windows 8.1（32bit、64bit）
  - ESET NOD32 Antivirus 5.2（32bit、64bit）
  - F-Secure Client Security 9.32（32bit、64bit）
- セキュリティポリシーの設定時の注意事項を 2.9.4(2)に集約した。また、コンピュータに印刷抑止または操作ログの取得が設定されたセキュリティポリシーを割り当てた場合の、注意事項および対処方法を記載した。
- JP1/IT Desktop Management とそれ以外のプログラムとで同じソフトウェアを起動抑止した場合の注意事項を訂正した。
- セキュリティポリシーで USB デバイスの［読み取りと書き込みを抑止する］を有効にしている場合の注意事項を記載した。
- 自動で日本マイクロソフト社の Web サイトから更新プログラムを取得して配布する条件を訂正した。
- 操作ログ取得の設定時の注意事項を 2.10.8(1)に集約した。また、OS が 64bit 版で、かつ VMWare Server がインストールされている環境のコンピュータに関する注意事項を記載した。
- 操作ログを取得できる Web ブラウザに Windows Internet Explorer 10 および Firefox 5 を追加した。
- 操作ログとして取得される「持ち込み日時」の説明の内容を訂正した。
- `recreatelogdb` コマンドについての注意事項を訂正した。
- NTFS 以外でフォーマットされたドライブにファイルを移動またはコピーした場合の、持ち込みファイルの入力元情報取得に関する注意事項に、ReFS の場合も含まれることを明記した。
- 機器とハードウェア資産の同定の仕組みの説明を訂正した。
- 機器画面の［ソフトウェア情報］画面から未確認のソフトウェアを確認できるようにした。
- ネットワークモニタを有効化するコンピュータはクラスタ構成にできないことを記載した。
- `ioutils exportoplog` コマンドを実行できるサーバの説明を訂正した。
- 利用者がコンピュータを操作する際の注意事項を記載した。
- エージェントを導入するコンピュータの前提となるソフトウェアに Windows Internet Explorer 10 を追加した。

- サイトサーバの前提条件を訂正した。
- ネットワークモニタを有効化するコンピュータの前提条件を訂正した。
- JP1/IM と連携するための前提条件を記載した。
- 連携できる JP1 スマートデバイス管理サービスのバージョンを変更した。
- 必要なディスクの最大容量を、シングルサーバ構成システムの管理用サーバ、マルチサーバ構成システムの管理用サーバとデータベースサーバ、およびサイトサーバの場合で分けて記載した。
- サービス一覧を次のとおり変更した。
  - JP1/IT Desktop Management - Manager のサービスとサイトサーバのサービスを分けて記載した。
  - ネットワークモニタのサービスおよびエージェントのサービスを記載した。
  - サービスが自動起動するかどうかを記載した。

  また、プロセス一覧に、プロセスが常駐するかどうかを記載した。
- 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。
- 10-00 以前のバージョンから JP1/IT Desktop Management をバージョンアップした場合の、セットアップおよびエージェント設定の設定値について記載した。
- 次のイベントの追加に伴い、イベント通知の対象外として設定できる値を「0～1124」に変更した。
  1117、1118、1123、1124
- JP1 スマートデバイス管理サービスと連携する場合に自動で入力される MDM サーバのホスト名を、「www.jp1sdm.hitachi.jp」に変更した。
- MDM 連携時に設定できる取得スケジュールの開始時刻のデフォルト値を（空白）に変更した。
- 製品の各システム構成要素のメモリ所要量を変更した。
- 製品の各システム構成要素のディスク占有量を変更した。
- 製品の各システム構成要素の前提となる CPU を変更した。
- 制限値一覧の記載を更新した。
- MDM システムからの情報取得の自動実行について、説明とタイミングを訂正した。
- このマニュアルに記載している Windows のメニュー名の表記について記載した。

(b) 資料番号（3021-3-337）の変更内容

- 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。
- 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、および GUID を管理できるようにした。

- ファイル持ち出しによる不審と見なす操作と、印刷による不審と見なす操作で、画面表示や調査方法などが異なることを明記した。
- ホーム画面および資産画面の、管轄範囲が限定されている場合の差異を訂正した。
- 機器画面の［ソフトウェア情報］画面から、ソフトウェアを管理ソフトウェアに追加できるようにした。
- 探索するネットワークの範囲内にサイトサーバを設定している場合の説明を改善した。
- サイトサーバを設置する場合、ネットワークの探索を実行するには、管理用サーバとサイトサーバが互いに IP アドレスで直接参照できる必要があることを記載した。
- ループバックアドレスまたはブロードキャストアドレスがネットワークの探索の探索範囲に含まれている場合の注意事項を記載した。
- JP1/IT Desktop Management - Agent の適用 OS に、Windows 8 および Windows Server 2012 を追加した。
- Active Directory から取得できるシステム情報を示す表の、凡例の説明を改善した。
- 機器を特定するための情報を取得できなかった場合は、「SNMP 発見（認証情報不足）」と表示されることがあることを記載した。
- システム情報として収集できるコンピュータ情報に、ホスト名を記載した。
- 次の情報を収集するには、管理対象のコンピュータの OS で「Workstation」サービスが起動している必要があることを記載した。
  - 更新プログラム情報の Windows 自動更新
  - サービスのセキュリティ設定情報
  - OS のセキュリティ設定情報
- ［インストール済みコンピュータ］タブで確認できる項目の「登録日時」の説明を訂正した。
- コンピュータの電源を制御するための条件を訂正した。
- ［エージェント設定の追加］ダイアログおよび［エージェント設定の編集］ダイアログで、コンピュータの再起動のタイミングを設定できるようにした。これに伴い、エージェント導入済みのコンピュータに表示される［コンピュータのシャットダウン］ダイアログと［コンピュータの再起動］ダイアログの説明を変更した。
- MDM システムから取得できるシステム情報の取得可否を明確にした。また、凡例の説明を改善した。
- リモートコントロール時にエージェント導入済みのコンピュータにマウスが接続されていない場合、コントローラに表示されるマウスカーソルの形状は常に矢印カーソルのままとなることを記載した。
- ネットワーク接続を制御している場合で、新規機器のネットワーク接続を自動的に許可させたいときの方法を記載した。
- 機器の運用方法ごとに必要なネットワーク制御リストの設定を記載した。
- ネットワークモニタを有効化したコンピュータは、Windows ファイアウォールの判定の対象外であることを記載した。
- サポートするウィルス対策製品に次の製品を追加した。

- Norton AntiVirus 2012 （32bit、64bit）
- Norton AntiVirus（32bit、64bit）
- ウイルスバスター 2012 クラウド（32bit、64bit）
- ウイルスバスター クラウド（32bit、64bit）
- ウイルスバスター コーポレートエディション 10.6（32bit、64bit）
- ウイルスバスター ビジネスセキュリティ 7.0（32bit、64bit）
- Kaspersky Endpoint Security 8 for Windows 8.1（32bit、64bit）
- Kaspersky Endpoint Security 8 for Windows （32bit、64bit）
- ESET NOD32 Antivirus 5.0 （32bit、64bit）
- ESET NOD32 Antivirus 5.2（32bit、64bit）
- Sophos Endpoint Protection - Enterprise 10 （32bit、64bit）
- Sophos Endpoint Protection - Advanced 10 （32bit、64bit）
- Sophos Endpoint Protection - Basic 10 （32bit、64bit）
- F-Secure Client Security 9.11 （32bit、64bit）
- F-Secure Client Security 9.20 （32bit、64bit）
- F-Secure Client Security 9.31 （32bit、64bit）
- F-Secure Client Security 9.32（32bit、64bit）

また、サポートするウィルス対策製品から次の製品を削除した。

- ウイルスバスター 2010 （32bit、64bit)
- F-Secure Client Security 8.01 （32bit、64bit)

- コンピュータに印刷抑止または操作ログの取得が設定されたセキュリティポリシーを割り当てた場合の、注意事項および対処方法を記載した。
- JP1/IT Desktop Management とそれ以外のプログラムとで同じソフトウェアを起動抑止した場合の注意事項を訂正した。
- セキュリティポリシーで USB デバイスの［読み取りと書き込みを抑止する］を有効にしている場合の注意事項を記載した。
- OS が 64bit 版で、かつ VMWare Server がインストールされている環境のコンピュータに関する操作ログ取得の設定時の注意事項を記載した。
- 操作ログを取得できる Web ブラウザに Windows Internet Explorer 10 および Firefox 5 を追加した。
- 操作ログとして取得される「持ち込み日時」の説明の内容を訂正した。
- `recreatelogdb` コマンドについての注意事項を訂正した。
- NTFS 以外でフォーマットされたドライブにファイルを移動またはコピーした場合の、持ち込みファイルの入力元情報取得に関する注意事項に、ReFS の場合も含まれることを明記した。

- 機器とハードウェア資産の同定のしくみの説明を訂正した。
- 機器画面の［ソフトウェア情報］画面から未確認のソフトウェアを確認できるようにした。
- ネットワークモニタを有効化するコンピュータはクラスタ構成にできないことを記載した。
- ioutils exportoplog コマンドを実行できるサーバの説明を訂正した。
- 利用者がコンピュータを操作する際の注意事項を記載した。
- エージェントを導入するコンピュータの前提となるソフトウェアに Windows Internet Explorer 10 を追加した。
- サイトサーバの前提条件を訂正した。
- ネットワークモニタを有効化するコンピュータの前提条件を訂正した。
- JP1/IM と連携するための前提条件を記載した。
- 必要なディスクの最大容量を、シングルサーバ構成システムの管理用サーバ、マルチサーバ構成システムの管理用サーバとデータベースサーバ、およびサイトサーバの場合で分けて記載した。
- サービス一覧を次のとおり変更した。
  - JP1/IT Desktop Management - Manager のサービスとサイトサーバのサービスを分けて記載した。
  - ネットワークモニタのサービスおよびエージェントのサービスを記載した。
  - サービスが自動起動するかどうかを記載した。
    また、プロセス一覧に、プロセスが常駐するかどうかを記載した。
- 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。
- 09-50 以前のバージョンから JP1/IT Desktop Management をバージョンアップした場合の、セットアップおよびエージェント設定の設定値について記載した。
- 次のイベントの追加に伴い、イベント通知の対象外として設定できる値を「0～1123」に変更した。
  1117、1118、1123
- MDM 連携時に設定できる取得スケジュールの開始時刻のデフォルト値を（空白）に変更した。
- 製品の各システム構成要素のメモリ所要量を変更した。
- 製品の各システム構成要素のディスク占有量を変更した。
- 製品の各システム構成要素の前提となる CPU を変更した。
- 制限値一覧の記載を更新した。
- MDM システムからの情報取得の自動実行について、説明とタイミングを訂正した。
- このマニュアルに記載している Windows のメニュー名の表記について記載した。
- 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。
- ユーザーアカウントに設定した業務分掌に合わせて、表示される情報や実行できる操作を制限できるようにした。

- FD ドライブおよびリムーバブルディスクも書き込みだけを抑止できるようにした。
- JP1/IM と連携して、JP1 イベントを通知できるようにした。
- Active Directory との接続情報のルート OU の設定は、大文字・小文字を区別されないことを記載した。
- Active Directory から「部署」、「国/地域」、「都道府県」などの情報を取得するための LDAP 属性名についての説明を記載した。
- セキュリティ対策で自動対策をした場合、JP1/IT Desktop Management の機能を利用して、管理対象コンピュータの設定を自動対策前の状態には戻せないことを記載した。
- ネットワーク監視時の注意事項として、次の注意事項を記載した。
  - 「Routing and Remote Access」サービスに関する注意事項
  - ネットワークモニタを有効にしたコンピュータは、有線 LAN での接続を推奨する
  - ファイルサーバなど業務上重要なサーバは、ネットワーク監視用のコンピュータ（ネットワークモニタを有効にしたコンピュータ）に設定しない
  - DHCP サーバを用いて動的に IP アドレスを割り当てるネットワークを監視した場合の注意事項
- ネットワーク制御リストが更新されるタイミングを記載した。
- 機器情報を更新または削除した場合に、自動でネットワーク制御リストのメンテナンスが実施されることを記載した。
- ネットワークモニタの機能によってネットワークから遮断された機器は、そ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なコンピュータ、および［ネットワークへの接続を許可しない機器の特例接続］に登録されたコンピュータとだけ通信できることを記載した。
- ネットワーク監視機能の監視対象となるネットワーク、コンピュータの OS、プロトコルについて記載した。
- ネットワークモニタ機能によって発見された機器を削除した場合、ネットワークをいったん切断して再接続しないと、その機器は再発見できないことを記載した。
- MAC アドレスが入力され、機器と関連づけられたリストは、ネットワーク制御リストの画面からは削除できなくなることを記載した。
- サイトサーバが自動的に［ネットワークへの接続を許可しない機器の特例接続］に登録されることを記載した。
- ネットワークモニタエージェントをインストールした場合、自動でサービスが有効に、ファイアウォールが無効になることを記載した。
- インポート時にマッピングキーにできるシリアルナンバーは、BIOS 情報であることを記載した。
- 配布機能を利用してソフトウェアをインストールおよびアンインストールする場合、ローカルシステムアカウント権限で実行されることを記載した。
- コンピュータと管理用サーバの接続が失敗した場合は、操作ログはコンピュータ内に一時保存されることを記載した。

- ネットワーク制御リストから機器を削除した場合、ネットワークへの接続が「許可する」に設定した機器は、ネットワーク制御リストからも機器の情報が削除され、「許可しない」に設定した機器は、ネットワーク制御リストに機器の情報が残ることを記載した。
- Citrix XenApp または Windows のターミナルサービスがインストールされているサーバは、エージェントをインストールして管理できないことを記載した。
- Windows の管理共有の認証、または SNMP の認証ができない機器についての説明を変更した。
- エージェントを導入するコンピュータは、OS の「Workstation」サービスを起動しておく必要があることを記載した。
- エージェントを導入するコンピュータにネットワーク共有プリンタが登録されている環境で、プリンタサーバやネットワークのパフォーマンス低下があった場合の注意事項を記載した。
- エージェントレスでの管理について、次のことを記載した。
  - エージェントレスでの管理を採用する際の注意事項
  - 機器情報が収集されるタイミング
  - 機器情報収集用の実行プログラムの配信タイミング
  - エージェントレスのコンピュータを管理するために必要な設定
- Windows 7、Windows Vista、および Windows Server 2008 の場合に、エージェントレスの機器から Windows の管理共有を有効にして機器情報を取得するために必要な設定を変更した。
- 資産状態が未確認のハードウェア資産を削除した場合は、機器画面の［機器情報］画面から対象の機器が削除されることを記載した。
- VMware vSphere と VMware View を組み合わせた仮想環境はサポートしていないことを記載した。
- Windows 認証を利用してリモートコントロールする場合に必要なユーザー権限の設定手順を記載した。
- 手動でネットワーク制御リストに登録した機器は、ネットワーク制御リストから削除することもできることを記載した。
- 常にネットワークに接続させておく必要がある機器は、接続を許可する機器としてネットワーク制御リストに必ず登録することを記載した。
- ネットワーク接続が自動で変更される契機として、機器情報を更新または削除したとき、およびネットワーク接続デバイスの情報が変更されたときを追加した。
- 使用禁止ソフトウェアおよび使用禁止サービスの判定で使用する情報と判定条件の説明を訂正した。
- セキュリティ判定の対象外となるユーザーアカウントを記載した。
- セキュリティポリシーに設定できる項目のうち、禁止操作の説明を訂正した。
- OS ごとの抑止対象となる外部メディアについて補足説明を記載した。
- 次に示す種類の操作ログ取得の前提条件を変更した。
  - プログラムの起動および終了
  - ファイルおよびフォルダの操作

- Web アクセス

- ファイル削除の操作ログで、ファイルの削除方法によっては取得できない情報があることを記載した。
- 利用者がファイルを削除したあとに Undo または［元に戻す］メニューを選択した場合に、取得される操作ログの情報を記載した。
- メール送受信で取得される操作ログの注意事項に、MIME ヘッダの Content-type が添付ファイルとして扱われない場合の説明を記載した。
- 持ち込みファイルの入力元情報取得の注意事項に、FAT など NTFS 以外でフォーマットされたドライブにファイルを移動またはコピーした場合の説明を記載した。
- 次のハードウェア資産情報をインポートする際の、CSV ファイルの記述形式を変更した。
  - メモリ
  - ストレージ容量
  - ストレージ空き容量
  - ディスプレイサイズ
- 推奨ディスク容量を修正した。 また、サイトサーバで不審操作に関する操作ログだけを収集する場合の推奨ディスク容量を記載した。
- パッケージの配布について、機器の台数が多いときは、サイトサーバを利用するか、複数回に分けてパッケージを配布するよう記載した。
- `ioutils exportdevice` コマンドを使用して、機器情報をエクスポートできるようにした。
- `ioutils exportdevicedetail` コマンドを使用して、詳細な機器情報をエクスポートできるようにした。
- コンピュータの再起動が必要なセキュリティポリシーが適用された場合に、利用者のコンピュータ上に表示されるバルーンヒントのメッセージを変更した。
- ネットワークの前提条件に、システム構成要素ごとのネットワークの接続環境を追加した。
- リモートコントロール時に RFB で接続するための条件を変更した。また、注意事項として、RFB 接続によるリモートコントロールは必ずしも動作を保証できるものではないことを記載した。
- サイトサーバ構成で運用する場合のシステムの環境、および 1 台のサイトサーバが管理できる機器の台数を記載した。
- インストール先フォルダの配下に作成されるフォルダに「mgr¥definition」を追加した。
- 次に示す機能の自動実行について、説明とタイミングを訂正した。
  - 利用者情報の収集
  - サポート情報の定期チェックおよび更新
  - ウィルス対策製品の「エンジンバージョン」および「ウィルス定義ファイルバージョン」の更新
- プロセス一覧の記載内容を訂正した。
- 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。

- 管理ソフトウェア情報に、インストールされている機器の総数（ライセンス消費数）を表示するようにした。
- ユーザーアカウントに設定した管轄範囲に合わせて、表示される情報や実行できる操作を制限できるようにした。
- NAT 環境では、エージェントレスの機器は管理できないことを記載した。
- 管理用サーバから直接通信できないネットワークセグメントでは、ネットワークモニタ機能を利用しても機器が検知できないことを記載した。
- 複数のネットワークカードを使って複数のネットワークに接続できるコンピュータであれば、ネットワークモニタを有効にしたエージェント導入済みコンピュータ 1 台で、複数のネットワークセグメントを監視できることを記載した。
- 管理用サーバ、エージェントを導入するコンピュータ、およびサイトサーバの前提条件に、Windows Server 2008 R2 Datacenter を追加した。
- 管理対象のコンピュータにソフトウェアが追加された場合の確認方法を記載した。
- 部署および設置場所の定義の仕組みを記載した。また、メニューエリアから部署および設置場所の名称を変更できるようにした。
- イベントをメール通知するように設定しておくと、ネットワーク接続が遮断または許可されたことをメールで確認できることを記載した。
- リムーバブルディスクを抑止している場合、USB 接続のリムーバブルディスクをハードウェア資産として登録しても、使用を許可できないことを記載した。
- セキュリティポリシーによる更新プログラムの自動配布の機能と、Windows の自動更新機能（Windows Update や Microsoft Update）を併用できることを記載した。
- 同じ管理ソフトウェアに対応するソフトウェアが 1 台のコンピュータに複数インストールされている場合、1 ライセンスの消費としてカウントするようにした。
- インフォメーションエリアに「－」が表示されている場合、エクスポートすると空文字が出力されることを記載した。
- 配布機能を利用してアンインストールできるソフトウェアの種類を記載した。
- コマンドを実行して、サイトサーバの操作ログを削除できるようにした。
- ネットワークモニタを有効化するコンピュータの前提条件に、Windows 7 を追加した。
- ネットワークの前提条件の説明を改善した。
- NAT 環境の場合は、操作ログの保管先に指定するサイトサーバを、管理用サーバと同一のネットワークセグメントに設置することを記載した。
- 1 年分の操作ログをバックアップした場合に必要なディスク容量の目安を変更した。
- JP1/IT Desktop Management で管理するすべてのデータ（操作ログを含む）の推奨ディスク容量の目安を変更した。
- 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。

- ユーザーアカウントに設定するパスワードのルールを記載した。
- 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。
- カスタムインストールの場合、操作ログを取得するときは、データベース格納フォルダのドライブに 20 ギガバイト以上の空き容量が必要であることを記載した。

(13) 10-00 の変更内容

(a) 資料番号（3021-3-152）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。
- ユーザーアカウントに設定した業務分掌に合わせて、表示される情報や実行できる操作を制限できるようにした。
- FD ドライブおよびリムーバブルディスクも書き込みだけを抑止できるようにした。
- MDM サービスと連携してスマートデバイス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。
- サポートするウィルス対策製品に次の製品を追加した。
  - Norton AntiVirus 2012 （32bit、64bit）
  - ウイルスバスター 2012 クラウド（32bit、64bit）
  - ウイルスバスター コーポレートエディション 10.6（32bit、64bit）
  - ESET NOD32 Antivirus 5.0 （32bit、64bit）
  - Sophos Endpoint Protection - Enterprise 10 （32bit、64bit）
  - Sophos Endpoint Protection - Advanced 10 （32bit、64bit）
  - Sophos Endpoint Protection - Basic 10 （32bit、64bit）
  - Kaspersky Endpoint Security 8 for Windows （32bit、64bit）
  - F-Secure Client Security 9.11 （32bit、64bit）
  - F-Secure Client Security 9.20 （32bit、64bit）
  - F-Secure Client Security 9.31 （32bit、64bit）

  また、サポートするウィルス対策製品から次の製品を削除した。
  - ウイルスバスター 2010 （32bit、64bit)
  - F-Secure Client Security 8.01 （32bit、64bit)
- Active Directory との接続情報のルート OU の設定は、大文字・小文字を区別されないことを記載した。
- Active Directory から「部署」、「国/地域」、「都道府県」などの情報を取得するための LDAP 属性名についての説明を記載した。

- セキュリティ対策で自動対策をした場合、JP1/IT Desktop Management の機能を利用して、管理対象コンピュータの設定を自動対策前の状態には戻せないことを記載した。
- ネットワーク監視時の注意事項として、次の注意事項を記載した。
  - 「Routing and Remote Access」サービスに関する注意事項
  - ネットワークモニタを有効にしたコンピュータは、有線 LAN での接続を推奨する
  - ファイルサーバなど業務上重要なサーバは、ネットワーク監視用のコンピュータ（ネットワークモニタを有効にしたコンピュータ）に設定しない
  - DHCP サーバを用いて動的に IP アドレスを割り当てるネットワークを監視した場合の注意事項
- ネットワーク制御リストが更新されるタイミングを記載した。
- 機器情報を更新または削除した場合に、自動でネットワーク制御リストの更新が実施されることを記載した。
- ネットワークモニタの機能によってネットワークから遮断された機器は、そ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なコンピュータ、および［ネットワークへの接続を許可しない機器の特例接続］に登録されたコンピュータとだけ通信できることを記載した。
- ネットワーク監視機能の監視対象となるネットワーク、コンピュータの OS、プロトコルについて記載した。
- ネットワークモニタ機能によって発見された機器を削除した場合、ネットワークをいったん切断して再接続しないと、その機器は再発見できないことを記載した。
- MAC アドレスが入力され、機器と関連づけられたリストは、ネットワーク制御リストの画面からは削除できなくなることを記載した。
- サイトサーバが自動的に［ネットワークへの接続を許可しない機器の特例接続］に登録されることを記載した。
- ネットワークモニタエージェントをインストールした場合、自動でサービスが有効に、ファイアウォールが無効になることを記載した。
- インポート時にマッピングキーにできるシリアルナンバーは、BIOS 情報であることを記載した。
- 配布機能を利用してソフトウェアをインストールおよびアンインストールする場合、ローカルシステムアカウント権限で実行されることを記載した。
- コンピュータと管理用サーバの接続が失敗した場合は、操作ログはコンピュータ内に一時保存されることを記載した。
- ネットワーク制御リストから機器を削除した場合、ネットワークへの接続が「許可する」に設定した機器は、ネットワーク制御リストからも機器の情報が削除され、「許可しない」に設定した機器は、ネットワーク制御リストに機器の情報が残ることを記載した。
- Citrix XenApp または Windows のターミナルサービスがインストールされているサーバは、エージェントをインストールして管理できないことを記載した。
- Windows の管理共有の認証、または SNMP の認証ができない機器についての説明を変更した。

- エージェントを導入するコンピュータは、OS の「Workstation」サービスを起動しておく必要があることを記載した。
- エージェントを導入するコンピュータにネットワーク共有プリンタが登録されている環境で、プリンタサーバやネットワークのパフォーマンス低下があった場合の注意事項を記載した。
- エージェントレスでの管理について、次のことを記載した。
  - エージェントレスでの管理を採用する際の注意事項
  - 機器情報が収集されるタイミング
  - 機器情報収集用の実行プログラムの配信タイミング
  - エージェントレスのコンピュータを管理するために必要な設定
- Windows 7、Windows Vista、および Windows Server 2008 の場合に、エージェントレスの機器から Windows の管理共有を有効にして機器情報を取得するために必要な設定を変更した。
- 資産状態が未確認のハードウェア資産を削除した場合は、機器画面の［機器情報］画面から対象の機器が削除されることを記載した。
- VMware vSphere と VMware View を組み合わせた仮想環境はサポートしていないことを記載した。
- Windows 認証を利用してリモートコントロールする場合に必要なユーザー権限の設定手順を記載した。
- 手動でネットワーク制御リストに登録した機器は、ネットワーク制御リストから削除することもできることを記載した。
- 常にネットワークに接続させておく必要がある機器は、接続を許可する機器としてネットワーク制御リストに必ず登録することを記載した。
- ネットワーク接続が自動で変更される契機として、機器情報を更新または削除したとき、およびネットワーク接続デバイスの情報が変更されたときを追加した。
- 使用禁止ソフトウェアおよび使用禁止サービスの判定で使用する情報と判定条件の説明を訂正した。
- セキュリティ判定の対象外となるユーザーアカウントを記載した。
- セキュリティポリシーに設定できる項目のうち、禁止操作の説明を訂正した。
- OS ごとの抑止対象となる外部メディアについて補足説明を記載した。
- 次に示す種類の操作ログ取得の前提条件を変更した。
  - プログラムの起動および終了
  - ファイルおよびフォルダの操作
  - Web アクセス
- ファイル削除の操作ログで、ファイルの削除方法によっては取得できない情報があることを記載した。
- 利用者がファイルを削除したあとに Undo または［元に戻す］メニューを選択した場合に、取得される操作ログの情報を記載した。
- メール送受信で取得される操作ログの注意事項に、MIME ヘッダの Content-type が添付ファイルとして扱われない場合の説明を記載した。

- 持ち込みファイルの入力元情報取得の注意事項に、FAT など NTFS 以外でフォーマットされたドライブにファイルを移動またはコピーした場合の説明を記載した。
- 次のハードウェア資産情報をインポートする際の、CSV ファイルの記述形式を変更した。
  - メモリ
  - ストレージ容量
  - ストレージ空き容量
  - ディスプレイサイズ
- 推奨ディスク容量を修正した。 また、サイトサーバで不審操作に関する操作ログだけを収集する場合の推奨ディスク容量を記載した。
- パッケージの配布について、機器の台数が多いときは、サイトサーバを利用するか、複数回に分けてパッケージを配布するよう記載した。
- ioutils exportdevice コマンドを使用して、機器情報をエクスポートできるようにした。
- ioutils exportdevicedetail コマンドを使用して、詳細な機器情報をエクスポートできるようにした。
- コンピュータの再起動が必要なセキュリティポリシーが適用された場合に、利用者のコンピュータ上に表示されるバルーンヒントのメッセージを変更した。
- ネットワークの前提条件に、システム構成要素ごとのネットワークの接続環境を追加した。
- リモートコントロール時に RFB で接続するための条件を変更した。また、注意事項として、RFB 接続によるリモートコントロールは必ずしも動作を保証できるものではないことを記載した。
- サイトサーバ構成で運用する場合のシステムの環境、および 1 台のサイトサーバが管理できる機器の台数を記載した。
- インストール先フォルダの配下に作成されるフォルダに「mgr¥definition」を追加した。
- 次に示す機能の自動実行について、説明とタイミングを訂正した。
  - 利用者情報の収集
  - サポート情報の定期チェックおよび更新
  - ウィルス対策製品の「エンジンバージョン」および「ウィルス定義ファイルバージョン」の更新
- このマニュアルで使用する英略語 に「CF」を記載した。
- プロセス一覧の記載内容を訂正した。

(14) 09-51 の変更内容

(a) 資料番号（3020-3-S93-10）の変更内容

- 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。
- 管理ソフトウェア情報に、インストールされている機器の総数（ライセンス消費数）を表示するようにした。

- ユーザーアカウントに設定した管轄範囲に合わせて、表示される情報や実行できる操作を制限できるようにした。
- NAT 環境では、エージェントレスの機器は管理できないことを記載した。
- 管理用サーバから直接通信できないネットワークセグメントでは、ネットワークモニタ機能を利用しても機器が検知できないことを記載した。
- 複数のネットワークカードを使って複数のネットワークに接続できるコンピュータであれば、ネットワークモニタを有効にしたエージェント導入済みコンピュータ 1 台で、複数のネットワークセグメントを監視できることを記載した。
- 管理用サーバ、エージェントを導入するコンピュータ、およびサイトサーバの前提条件に、Windows Server 2008 R2 Datacenter を追加した。
- 管理対象のコンピュータにソフトウェアが追加された場合の確認方法を記載した。
- 部署および設置場所の定義の仕組みを記載した。また、メニューエリアから部署および設置場所の名称を変更できるようにした。
- イベントをメール通知するように設定しておくと、ネットワーク接続が遮断または許可されたことをメールで確認できることを記載した。
- リムーバブルディスクを抑止している場合、USB 接続のリムーバブルディスクをハードウェア資産として登録しても、使用を許可できないことを記載した。
- セキュリティポリシーによる更新プログラムの自動配布の機能と、Windows の自動更新機能（Windows Update や Microsoft Update）を併用できることを記載した。
- 同じ管理ソフトウェアに対応するソフトウェアが 1 台のコンピュータに複数インストールされている場合、1 ライセンスの消費としてカウントするようにした。
- インフォメーションエリアに「−」が表示されている場合、エクスポートすると空文字が出力されることを記載した。
- 配布機能を利用してアンインストールできるソフトウェアの種類を記載した。
- コマンドを実行して、サイトサーバの操作ログを削除できるようにした。
- ネットワークモニタを有効化するコンピュータの前提条件に、Windows 7 を追加した。
- ネットワークの前提条件の説明を改善した。
- NAT 環境の場合は、操作ログの保管先に指定するサイトサーバを、管理用サーバと同一のネットワークセグメントに設置することを記載した。
- 1 年分の操作ログをバックアップした場合に必要なディスク容量の目安を変更した。
- JP1/IT Desktop Management で管理するすべてのデータ（操作ログを含む）の推奨ディスク容量の目安を変更した。
- 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。
- ユーザーアカウントに設定するパスワードのルールを記載した。

- 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、操作画面を表示するコンピュータ、およびネットワークモニタを有効にするコンピュータに必要なメモリ所要量をそれぞれ変更した。
- カスタムインストールの場合、操作ログを取得するときは、データベース格納フォルダのドライブに 20 ギガバイト以上の空き容量が必要であることを記載した。

付録 A.15　このマニュアルの参考情報

(1)　関連マニュアル

- JP1 Version 12 資産・配布管理 基本ガイド（3021-3-E11）
- JP1 Version 12 JP1/IT Desktop Management 2 導入・設計ガイド（3021-3-E12）
- JP1 Version 12 JP1/IT Desktop Management 2 構築ガイド（3021-3-E13）
- JP1 Version 12 JP1/IT Desktop Management 2 運用ガイド（3021-3-E14）
- JP1 Version 12 JP1/IT Desktop Management 2 配布機能 運用ガイド（3021-3-E15）
- JP1 Version 12 JP1/IT Desktop Management 2 - Asset Console 構築・運用ガイド（3021-3-E16）
- JP1 Version 12 JP1/IT Desktop Management 2 - Asset Console アクセス定義ファイル作成ガイド（3021-3-E17）
- JP1 Version 12 JP1/IT Desktop Management 2 メッセージ（3021-3-E18）
- JP1 Version 12 JP1/IT Desktop Management 2 - Smart Device Manager（3021-3-E21）
- JP1 Version 12 JP1/IT Desktop Management 2 - Agent(UNIX(R)用)（3021-3-E22）
- JP1 Version 12 JP1/秘文 セットアップガイド（管理者用）（3021-3-E29）
- JP1 Version 12 JP1/秘文 管理者ガイド（運用編）（3021-3-E30）
- JP1 Version 12 JP1/秘文 コマンド操作ガイド（3021-3-E33）
- JP1 Version 9 JP1/NETM/Network Monitor（3020-3-S73）
- JP1 Version 9 JP1/NETM/Network Monitor - Manager（3020-3-S74）
- JP1 Version 10 JP1/NETM/Network Monitor（3021-3-169）
- JP1 Version 10 JP1/NETM/Network Monitor - Manager（3021-3-170）

(2)　関連ドキュメント

- JP1/IT Desktop Management 2 オンラインヘルプ

(3) このマニュアルでの表記

このマニュアルに記載している Windows のメニュー名の表記は、次の OS を前提としています。

管理用サーバ、ネットワークモニタを有効化するコンピュータ、およびコントローラをインストールするコンピュータの場合

Windows Server 2012

エージェントを導入するコンピュータの場合

Windows 7

Windows Server 2019、Windows Server 2016、Windows 8.1、Windows 8、または Windows Server 2012 の場合は［スタート］メニューが表示されないため、画面左下から表示できる［スタート］画面からメニューを選択してください。

このマニュアルでは、製品名称を次のように表記しています。

略称		正式名称
AMT		Intel(R) Active Management Technology
Chrome		Google Chrome
Citrix XenApp		Citrix XenApp(R)
		Citrix Virtual Apps
Firefox		Firefox(R)
Linux		Linux(R)
Mac	Mac OS	OS X 10.10
		OS X 10.11
		macOS 10.12
		macOS 10.13
		macOS 10.14
NetWare		NetWare(R)
Pentium		Intel Pentium(R)
VMWare		VMWare(R)
Asset Console		JP1/IT Desktop Management 2 - Asset Console
JP1/AJS		JP1/Automatic Job Management System 2
		JP1/Automatic Job Management System 3
JP1/IM	JP1/IM - Manager	JP1/Integrated Management - Manager
		JP1/Integrated Management 2 - Manager

略称		正式名称
JP1/IM	JP1/IM - View	JP1/Integrated Management - View
		JP1/Integrated Management 2 - View
JP1/IT Desktop Management 2		JP1/IT Desktop Management 2 - Manager
		JP1/IT Desktop Management 2 - Operations Director
JP1/NETM/NM		JP1/NETM/Network Monitor
秘文	JP1/秘文 IC	JP1/秘文 Advanced Edition Information Cypher
	JP1/秘文 IF	JP1/秘文 Advanced Edition Information Fortress
	JP1/秘文 IF Mail Option	JP1/秘文 Advanced Edition Information Fortress Mail Option
	JP1/秘文 IS	JP1/秘文 Advanced Edition Information Share
	秘文 IC	秘文 Advanced Edition Information Cypher
	秘文 IF	秘文 Advanced Edition Information Fortress
	秘文 IF Mail Option	秘文 Advanced Edition Information Fortress Mail Option
	秘文 IS	秘文 Advanced Edition Information Share
	秘文 DC	JP1/秘文 Device Control 秘文 Device Control
	秘文 DE	JP1/秘文 Data Encryption 秘文 Data Encryption
	秘文 DP	JP1/秘文 Data Protection 秘文 Data Protection

このマニュアルでは、機能名を次のように表記しています。

略称	正式名称
プログラムと機能	アプリケーションの追加と削除
	プログラムの追加と削除
	プログラムと機能

このマニュアルでは、マイクロソフト製品の名称を次のように表記しています。

表記		製品名
Active Directory		Microsoft(R) Active Directory
Internet Explorer	Windows Internet Explorer	Windows(R) Internet Explorer(R)
Microsoft.NET		Microsoft(R).NET

表記			製品名
Microsoft Cluster Service			Microsoft(R) Cluster Service
Microsoft Excel			Microsoft(R) Excel(R)
Microsoft Office Excel			Microsoft(R) Office Excel(R)
Microsoft Forefront			Microsoft(R) Forefront(TM)
Microsoft Internet Information Services または IIS			Microsoft(R) Internet Information Services
Microsoft Lync			Microsoft(R) Lync
Microsoft Office			Microsoft(R) Office
Microsoft Office Access			Microsoft(R) Office Access(R)
Microsoft Office InfoPath			Microsoft(R) Office InfoPath(R)
Microsoft Office OneNote			Microsoft(R) Office OneNote
Microsoft Office Outlook			Microsoft(R) Office Outlook(R)
Microsoft Outlook			
Microsoft Office PowerPoint			Microsoft(R) Office PowerPoint(R)
Microsoft Office Project			Microsoft(R) Office Project
Microsoft Office Publisher			Microsoft(R) Office Publisher
Microsoft Office Visio			Microsoft(R) Office Visio(R)
Microsoft OneNote			Microsoft(R) OneNote
Microsoft Outlook Express			Microsoft(R) Outlook(R) Express
Microsoft Project			Microsoft(R) Project
Microsoft Publisher			Microsoft(R) Publisher
Microsoft Visio			Microsoft(R) Visio(R)
Microsoft InfoPath			Microsoft(R) InfoPath(R)
MS-DOS			Microsoft(R) MS-DOS(R)
Windows	Windows 2000	Windows 2000 Advanced Server	Microsoft(R) Windows(R) 2000 Advanced Server Operating System
		Windows 2000 Professional	Microsoft(R) Windows(R) 2000 Professional Operating System
		Windows 2000 Server	Microsoft(R) Windows(R) 2000 Server Operating System

表記				製品名
Windows	Windows 7		Windows 7 Enterprise	Microsoft(R) Windows(R) 7 Enterprise
			Windows 7 Home Basic	Microsoft(R) Windows(R) 7 Home Basic
			Windows 7 Home Premium	Microsoft(R) Windows(R) 7 Home Premium
			Windows 7 Professional	Microsoft(R) Windows(R) 7 Professional
			Windows 7 Starter	Microsoft(R) Windows(R) 7 Starter
			Windows 7 Ultimate	Microsoft(R) Windows(R) 7 Ultimate
	Windows 8		Windows 8	Windows(R) 8
			Windows 8 Enterprise	Windows(R) 8 Enterprise
			Windows 8 Pro	Windows(R) 8 Pro
	Windows 8.1		Windows 8.1	Windows(R) 8.1
			Windows 8.1 Enterprise	Windows(R) 8.1 Enterprise
			Windows 8.1 Pro	Windows(R) 8.1 Pro
	Windows 10		Windows 10 Enterprise	Windows(R) 10 Enterprise
			Windows 10 Pro	Windows(R) 10 Pro
	Windows Server 2003	Windows Server 2003※	Windows Server 2003 Enterprise Edition	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
			Windows Server 2003 Standard Edition	Microsoft(R) Windows Server(R) 2003, Standard Edition
			Windows Server 2003 Enterprise	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
			Windows Server 2003 Standard	Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
		Windows Server 2003 R2	Microsoft Windows Server 2003 R2 Enterprise	Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
			Microsoft Windows Server 2003 R2 Standard	Microsoft(R) Windows Server(R) 2003 R2, Standard Edition

表記				製品名
Windows	Windows Server 2003	Windows Server 2003 R2	Microsoft Windows Server 2003 R2 Enterprise	Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
			Microsoft Windows Server 2003 R2 Standard	Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
	Windows Server 2008	Windows Server 2008※	Windows Server 2008 Enterprise	Microsoft(R) Windows Server(R) 2008 Enterprise
				Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(R)
			Microsoft Windows Server 2008 Standard	Microsoft(R) Windows Server(R) 2008 Standard
				Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(R)
		Windows Server 2008 R2	Windows Server 2008 Datacenter	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
			Windows Server 2008 Enterprise	Microsoft(R) Windows Server(R) 2008 R2 Enterprise
			Windows Server 2008 Foundation	Microsoft(R) Windows Server(R) 2008 R2 Foundation
			Windows Server 2008 Standard	Microsoft(R) Windows Server(R) 2008 R2 Standard
	Windows Server 2012	Windows Server 2012※	Windows Server 2012 Datacenter	Microsoft(R) Windows Server(R) 2012 Datacenter
			Windows Server 2012 Standard	Microsoft(R) Windows Server(R) 2012 Standard
		Windows Server 2012 R2	Windows Server 2012 R2 Datacenter	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
			Windows Server 2012 R2 Standard	Microsoft(R) Windows Server(R) 2012 R2 Standard
	Windows Server 2016		Windows Server 2016 Datacenter	Microsoft(R) Windows Server(R) 2016 Datacenter
			Windows Server 2016 Standard	Microsoft(R) Windows Server(R) 2016 Standard
	Windows Server 2019		Windows Server 2019 Datacenter	Microsoft(R) Windows Server(R) 2019 Datacenter

表記			製品名
Windows	Windows Server 2019	Windows Server 2019 Standard	Microsoft(R) Windows Server(R) 2019 Standard
	Windows Vista	Windows Vista Business	Microsoft(R) Windows Vista(R) Business
		Windows Vista Enterprise	Microsoft(R) Windows Vista(R) Enterprise
		Windows Vista Home Basic	Microsoft(R) Windows Vista(R) Home Basic
		Windows Vista Home Premium	Microsoft(R) Windows Vista(R) Home Premium
		Windows Vista Ultimate	Microsoft(R) Windows Vista(R) Ultimate
	Windows XP	Windows XP Home Edition	Microsoft(R) Windows(R) XP Home Edition Operating System
		Windows XP Professional (x86)	Microsoft(R) Windows(R) XP Professional Operating System
Windows 95			Microsoft(R) Windows(R) 95 Operating System
Windows 98			Microsoft(R) Windows(R) 98 Operating System
Windows Live メール			Windows Live(TM) メール
Windows Me			Microsoft(R) Windows(R) Millennium Edition Operating System
Windows Media Player			Windows Media(R) Player
Windows NT 4.0			Microsoft(R) Windows NT(R) Server Enterprise Edition Version 4.0
			Microsoft(R) Windows NT(R) Server Network Operating System Version4.0
			Microsoft(R) Windows NT(R) Workstation Operating System Version4.0
Windows NT 3.51			Microsoft(R) Windows NT(R) Server Network Operating System Version3.51

表記	製品名
Windows NT 3.51	Microsoft(R) Windows NT(R) Workstation Operating System Version3.51
Windows Server Failover Cluster	Microsoft(R) Windows Server(R) Failover Cluster
Windows メール	Windows(R) メール

注※　Windows Server 2003 R2 を併記している場合は、Windows Server 2003 に Windows Server 2003 R2 は含みません。Windows Server 2008、Windows Server 2012 の場合も同様です。

(4)　このマニュアルで使用する英略語

英略語	英字での表記
API	Application Programming Interface
ARP	Address Resolution Protocol
AVI	Audio Video Interleave
BIOS	Basic Input / Output System
BMP	Bit Map
CA	Certificate Authority
CD	Compact Disc
CD-R	Compact Disc Recordable
CD-ROM	Compact Disc Read Only Memory
CF	CompactFlash
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
CSV	Comma Separated Values
DB	Database
DBMS	Database Management System
DCOM	Distributed Component Object Model
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DVD	Digital Versatile Disc
FC	Fibre Channel

英略語	英字での表記
FD	Floppy Disk
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICCID	Integrated Circuit Card ID
ICMP	Internet Control Message Protocol
ID	IDentification
IDE	Integrated Drive Electronics
IEEE	Institute of Electrical and Electronic Engineers
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
ISAPI	Internet Server Application Programming Interface
ISMS	Information Security Management System
IT	Information Technology
JSON	JavaScript Object Notation
KVM	Keyboard Video Mouse
LAN	Local Area Network
MAC	Media Access Control
MDM	Mobile Device Management
NAPT	Network Address Port Translation
NAS	Network Attached Storage
NAT	Network Address Translation
NTFS	NT File System
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PDCA	Plan Do Check Action
PGP	Pretty Good Privacy
RAM	Random Access Memory
REST	Representational State Transfer

英略語	英字での表記
RFB	Remote Framebuffer
RFC	Request for Comments
SAMAC	association of SAM Assessment & Certification
SD	Secure Digital
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSD	Solid State Drive
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Account Control
UAP	User Application Program
UDID	Unique Device IDentifier
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Universal Time, Coordinated
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VPN	Virtual Private Network
VRAM	Video Random Access Memory
WAN	Wide Area Network
WMI	Windows Management Instrumentation
XML	Extensible Markup Language

(5) このマニュアルで使用している書式について

説明文で使用する書式

書式	説明
文字列	可変の値を示します。 （例）日付は *YYYYMMDD* の形式で指定します。
[ ] − [ ]	メニューを連続して選択することを示します。 （例）［ファイル］メニュー − ［新規作成］を選択します。 上記の例では、［ファイル］メニュー内の［新規作成］を選択することを示します。
[ ] + [ ]	キーボードのキーを同時に押すことを示します。 （例）［Ctrl］＋［Alt］＋［Delete］は、［Ctrl］キー、［Alt］キー、および［Delete］キーを同時に押すことを示します。
・	この記号で区切られている項目は、複数項目のすべてを示します。 （例） A・B は、「A および B」を示します。
/	この記号で区切られている項目は、複数項目のうちどれかを示します。 （例） A/B は、「A または B」を示します。

文法で使用する書式

書式	説明
△	半角スペースを示します。
文字列	可変の値を示します。
[ ]	この記号で囲まれている項目は任意に指定できます（省略もできます）。 （例）［A］は「何も指定しない」か「A を指定する」ことを示します。
{ }	この記号で囲まれている複数の項目の中から、必ず 1 組の項目を選択します。項目の区切りは|で示します。 （例）{A|B|C} は、「A、B または C のどれかを指定する」ことを示します。
|	この記号で区切られている項目は、複数項目のうちどれかを指定できます。 （例） A|B|C は、「A、B、または C」を示します。

(6) オンラインヘルプについて

JP1/IT Desktop Management 2 では、次に示すオンラインヘルプを提供しています。

画面説明のヘルプ

表示中の操作画面について説明するヘルプです。操作画面に表示される［ヘルプ］ボタンから起動できます。

(7) KB（キロバイト）などの単位表記について

1KB（キロバイト）、1MB（メガバイト）、1GB（ギガバイト）、1TB（テラバイト）、1PB（ペタバイト）はそれぞれ 1,024 バイト、$1,024^2$ バイト、$1,024^3$ バイト、$1,024^4$ バイト、$1,024^5$ バイトです。

付録 B　用語解説

ここでは、JP1/IT Desktop Management 2 で使用する用語について説明します。

(英字)

Active Directory サーバ

Active Directory を導入しているサーバです。Active Directory と連携して機器を管理するときに、JP1/IT Desktop Management 2 と接続します。

Citrix XenApp、Microsoft RDS サーバ

Citrix XenApp および Microsoft RDS（リモートデスクトップサービス）がインストールされているサーバのことです。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 で管理できます。

Asset Console を使用した資産管理

JP1/IT Desktop Management 2 のコンポーネントである Asset Console を使用して資産管理をする機能のことです。操作画面を使用した資産管理に対してこう呼びます。

ITDM2 認証

JP1/IT Desktop Management 2 のシステム内でユーザーアカウントを認証する方法です。ユーザーアカウントは JP1/IT Desktop Management 2 の操作画面で作成します。この方法は、JP1/IT Desktop Management 2 システムでの標準のユーザーアカウントの認証方法です。

ITDM2 ユーザー

JP1/IT Desktop Management 2 で登録・管理されるユーザーアカウントです。JP1/IT Desktop Management 2 の操作画面でアカウントを作成します。

これに対して、JP1/Base の認証サーバで登録・管理されるユーザーアカウントは JP1 ユーザーと呼びます。

ITDM 互換配布

JP1/IT Desktop Management 2 が提供する 2 つの配布機能のうち、操作画面の配布（ITDM 互換）画面を使用して配布する機能のことです。リモートインストールマネージャを使用した配布に対してこう呼びます。

JCR ファイル

拡張子が JCR の、JP1/IT Desktop Management 2 が提供する動画用のファイル形式です。リモートコントロール中に録画された動画は、JCR ファイルで保存されます。JCR ファイルは、リモコンプレーヤーで再生できます。

JP1/IT Desktop Management 2
機器管理、セキュリティ管理、資産管理の観点から、IT 資産を管理するシステムです。

JP1/IT Desktop Management 2 - Agent
JP1/IT Desktop Management 2 で管理される側のコンピュータにインストールするプログラムです。

JP1/IT Desktop Management 2 - Asset Console
資産管理サーバにインストールするプログラムです。

JP1/IT Desktop Management 2 - Manager
JP1/IT Desktop Management 2 のサーバ機能を提供するプログラムです。

JP1/IT Desktop Management 2 - Network Monitor
ネットワークの監視用のコンピュータにインストールするプログラムです。

JP1/IT Desktop Management 2 - Operations Director
管理対象のコンピュータが 1,000 台以下の、中小企業向けのシステムです。JP1/IT Desktop Management 2 - Manager と比較して、機能が一部制限されています。

JP1/IT Desktop Management 2 - Smart Device Manager
スマートデバイスの運用管理およびセキュリティ対策を実現するプログラムです。

JP1/NETM/Network Monitor
ネットワークを監視して、機器のネットワーク接続を制御するプログラムです。ネットワーク制御用アプライアンスに導入されています。

JP1/NETM/Network Monitor - Manager
JP1/NETM/Network Monitor を統合管理するプログラムです。JP1/NETM/NM - Manager と連携する場合に、管理用サーバにインストールします。

JP1 権限レベル
管理対象（資源）に対して JP1 ユーザーがどのような操作ができるかを表しています。JP1/IT Desktop Management 2 では、権限と業務分掌に応じて、操作項目を定めています。管理対象（資源）の種類と、それに対する操作項目の幾つかを組み合わせた形式で JP1 ユーザーのアクセス権限を管理します。

JP1 資源グループ
管理対象（資源）を幾つかのグループに分けて管理します。この管理対象（資源）を分けたグループのことを JP1 資源グループと呼びます。JP1/IT Desktop Management 2 では、JP1/IT Desktop Management 2 - Manager 単位で管理します。

JP1 認証

JP1/Base でユーザーアカウントを一元管理し、認証する方法です。ユーザーアカウントは、JP1/Base で JP1 ユーザーとして作成します。すでにほかの JP1 製品で JP1 認証を使用している場合、そのユーザーアカウントを使用できます。

JP1 ユーザー

JP1/Base の認証サーバで登録・管理されるユーザーアカウントです。JP1/Base でアカウントを作成します。

これに対して、JP1/IT Desktop Management 2 で登録・管理されるユーザーアカウントは ITDM2 ユーザーと呼びます。

MDM サーバ

MDM 製品を導入しているサーバです。MDM 製品と連携してスマートデバイスを管理するときに、JP1/IT Desktop Management 2 と接続します。

MDM システム

スマートデバイスを管理する MDM 製品のシステムです。

MDM 製品

スマートデバイスを管理する製品で、MDM サーバにインストールします。JP1/IT Desktop Management 2 と連携して、スマートデバイスを管理します。

Remote Install Manager

JP1/IT Desktop Management 2 のコンポーネントです。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インストールします。

RFB

ネットワーク上の離れたコンピュータにアクセスするための通信プロトコルです。主に VNC で使用されていて、異なる OS 間でも接続できます。JP1/IT Desktop Management 2 では、エージェントレスのコンピュータや OS が Windows 以外のコンピュータをリモートコントロールする際に、RFB を使用します。

SAMAC 辞書

SAMAC が提供するソフトウェア辞書を JP1/IT Desktop Management 2 に登録した情報です。JP1/IT Desktop Management 2 で管理するソフトウェアの情報の一つです。

SAMAC ソフトウェア辞書のオフライン更新用ファイル

SAMAC が提供するソフトウェア辞書を JP1/IT Desktop Management 2 の SAMAC 辞書に登録するためのファイルです。

VNC

ネットワーク上の離れたコンピュータを遠隔操作するためのソフトウェアです。

（ア行）

印刷による不審操作

セキュリティポリシーで、不審と見なす操作の［大量印刷］をチェックした場合に検知される不審操作です。

インストールセット

JP1/IT Desktop Management 2 - Agent のインストールとセットアップを一度に実行できる、エージェントの導入を支援するプログラムです。管理用サーバで作成します。

インストールソフトウェア

管理対象のコンピュータにインストールされているソフトウェアです。インストールソフトウェアの情報は、機器情報として自動で収集されます。

インターネットゲートウェイサーバ

管理対象のコンピュータが、社外などインターネットを経由して接続している場合に、JP1/IT Desktop Management 2 で管理するために使用するサーバです。組織ネットワークの非武装地帯（DMZ）に設置します。

インフォメーションエリア

操作画面の右側に表示されるエリアです。左側のメニューエリアで選択した項目に応じて、情報が表示されます。

エージェント

JP1/IT Desktop Management 2 で管理される側のコンピュータにインストールするプログラムです。JP1/IT Desktop Management 2 - Manager に情報を通知したり、JP1/IT Desktop Management 2 - Manager からの指示でコンピュータを制御したりします。プログラム名は「JP1/IT Desktop Management 2 - Agent」です。

なお、「JP1/IT Desktop Management 2 - Agent」には、Windows 用、UNIX 用、Linux 用、Mac 用があります。必要に応じて、Windows 用のエージェントがインストールされている場合を Windows エージェント、UNIX 用または Linux 用のエージェントがインストールされている場合を UNIX エージェント、Mac 用のエージェントがインストールされている場合を Mac エージェントと区別して表記します。

エージェント設定

管理用サーバ側で管理する、エージェントのセットアップの設定内容です。操作画面でエージェント設定を作成し、エージェントに割り当てることで、エージェントのセットアップをリモートで変更できます。

エージェントレス

JP1/IT Desktop Management 2 - Agent がインストールされていない管理対象の機器のことです。

エンド WS

UNIX エージェント、Mac エージェントのうち、中継システムを経由しないで配布管理システムと直接接続するものを指します。

オフライン管理

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を外部記憶媒体を利用して管理する方法です。オンライン管理に対してこう呼びます。

オフライン管理構成システム

スタンドアロンのコンピュータや拠点にあるコンピュータなど、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を管理する構成です。

オフライン管理用のエージェント

エージェント設定で、管理用サーバと接続しない設定にしたエージェントのことです。オフライン管理したいコンピュータにインストールします。オンライン管理用のエージェントに対してこう呼びます。

オフライン用ポリシー適用ツール

オフライン管理のコンピュータに導入されたエージェントにセキュリティポリシーを適用するツールです。setsecpolicy.vbs コマンドとセキュリティポリシーの適用に必要な情報を含むファイルで構成されています。

オンライン管理

管理用サーバにネットワーク接続しているコンピュータを管理する方法です。オフライン管理に対してこう呼びます。

オンライン管理用のエージェント

エージェント設定で、上位システムと通信する設定にしたエージェントのことです。オンライン管理したいコンピュータにインストールします。オフライン管理用のエージェントに対してこう呼びます。

（カ行）

外部記憶媒体

書き込みができるUSBメモリやハードディスクのことです。オフライン管理用のエージェントをインストールしたり、オフライン管理のコンピュータから機器情報を収集したりする際に利用します。

カスタムグループ

管理者の目的に応じて任意に作成できるグループです。JP1/IT Desktop Management 2で管理する情報をグルーピングできます。

管轄範囲

ユーザーアカウントに設定した、管理者が管理する組織内の範囲です。

管理者のコンピュータ

JP1/IT Desktop Management 2の管理者が、ふだんJP1/IT Desktop Management 2にログインするコンピュータです。

管理ソフトウェア情報

JP1/IT Desktop Management 2で管理できる資産情報の一つです。ソフトウェアライセンスの利用状況を管理するためのソフトウェアの単位です。管理ソフトウェア単位に保有しているソフトウェアライセンス数や利用数を集計・表示できます。複数バージョンのソフトウェアを、1種類のライセンス利用単位として管理できます。

管理元

任意の機器や資産などを指した場合に、それらを管理している管理用サーバです。例えば「コンピュータの管理元」と呼んだ場合、コンピュータに導入されているエージェントの接続先に設定された管理用サーバを指します。

管理用サーバ

JP1/IT Desktop Management 2 - Managerがインストールされているコンピュータです。リモートインストールマネージャを使用した配布について説明する場合は、「配布管理システム」または「マネージャ」と呼ぶことがあります。

管理用中継サーバ

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サーバです。複数サーバ構成システムでは、統括管理用サーバと管理用中継サーバを合わせて「管理用サーバ」と呼ぶことがあります。

部門やネットワーク構成ごとにJP1/IT Desktop Management 2を運用したい場合に設置します。また、中継システムと同様、リモートインストールマネージャを使用した配布でジョブの実行やパッケージの配布でネットワークに掛かる負荷を軽減できます。

機器情報

JP1/IT Desktop Management 2 が管理対象の機器から収集する情報です。管理対象のコンピュータでのハードウェアの使用状況やインストールされているソフトウェアの種類など、コンピュータの管理に必要な情報です。機器情報は、機器画面の［機器情報］画面で確認できます。

危険レベル

コンピュータのセキュリティ対策の危険度を示すレベルのことです。セキュリティポリシーの判定結果によって設定されます。危険レベルは、「危険」、「警告」、「注意」、「安全」、「不明」、「対象外」の 6 種類があります。

業務分掌

ユーザーアカウントに設定した、管理者の担当業務です。業務分掌と権限とを組み合わせてユーザーアカウントに設定すると、管理者の操作範囲をそれぞれの担当業務に応じて限定できます。

クライアント WS

UNIX エージェント、Mac エージェントのうち、中継システムを経由して配布管理システムと接続するものを指します。

契約会社情報

JP1/IT Desktop Management 2 で管理できる資産情報の一つです。組織で保有する機器（ハードウェア資産）やソフトウェアライセンスに対する契約を結んでいる会社の連絡先情報を登録します。

契約会社リスト

契約会社情報を管理するための一覧です。

契約情報

JP1/IT Desktop Management 2 で管理できる資産情報の一つです。組織で保有する機器（ハードウェア資産）やソフトウェアライセンスに対する契約の情報です。

更新プログラム

日本マイクロソフト社が公開する、Windows や Internet Explorer を更新するためのプログラムです。

更新プログラムグループ

適用する更新プログラム、または除外する更新プログラムをグループ化したものです。更新プログラムグループをセキュリティポリシーに指定することで、セキュリティポリシーが割り当てられたコンピュータに、そのグループ内の更新プログラムを適用したり、除外したりできます。

コントローラ

管理対象のコンピュータをリモートコントロールするためのプログラムです。

（サ行）

サポートサービスサイト

サポートサービスを提供する Web サイトです。 JP1/IT Desktop Management 2 からインターネットを介して接続し、OS および Internet Explorer についての最新の更新プログラム情報、およびウィルス対策製品を取得できます。

サポート情報ファイル

最新の更新プログラム情報を JP1/IT Desktop Management 2 に登録するためのファイルです。

参照権限

JP1/IT Desktop Management 2 のユーザーアカウントを作成すると設定される権限です。設定画面以外の画面を参照できます。各画面での情報追加、設定変更などはできません。

自サーバ

任意の管理用サーバを指した場合に、その管理用サーバ自身のことです。

システム管理権限

JP1/IT Desktop Management 2 のユーザーアカウントに設定できる権限の一つです。この権限をユーザーアカウントに設定することで、ユーザーアカウントの管理を除いて、JP1/IT Desktop Management 2 を管理する機能全般を使用できます。

使用禁止ソフトウェア

組織内のコンピュータで使用を禁止とするソフトウェアの定義です。セキュリティポリシーに設定します。

使用必須ソフトウェア

組織内のコンピュータで使用を必須とするソフトウェアの定義です。セキュリティポリシーに設定します。

情報収集用ツール

オフライン管理のコンピュータから機器情報を収集するツールです。getinv.vbs コマンドと、機器情報の収集に必要な情報を含んだファイルで構成されています。

診断

セキュリティ状況の判定結果に基づいて、システムが安全かどうかを評価することです。診断結果は、レポートで確認できます。

推奨セキュリティポリシー

JP1/IT Desktop Management 2 が提供するセキュリティポリシーです。強固なセキュリティ環境で運用するための設定がされています。

スマートデバイス

携帯式の小型端末機です。スマートフォン、タブレット PC、PDA などが該当します。

セキュリティポリシー

危険レベルの判定条件とアクションの条件を設定したルールです。管理用サーバで設定して、管理対象のコンピュータに割り当てます。

セキュリティポリシーには、コンピュータの危険レベルを判定するための条件や、自動的に対策する項目を設定できます。また、判定された危険レベルに応じて利用者への警告メッセージの通知を設定できます。

接続リスト

リモートコントロールする際に、接続先のコンピュータを、JP1/IT Desktop Management 2 の操作画面とは別に独自に管理できる機能です。

操作ログ

管理対象のコンピュータ上での操作のログ情報です。オンライン管理のコンピュータから収集できます。

ソフトウェアライセンス情報

JP1/IT Desktop Management 2 で管理できる資産情報の一つです。組織で購入したソフトウェアライセンスを購入単位（資産単位）で管理する情報です。

（タ行）

タスク

管理用サーバからコンピュータにソフトウェアを配布してインストール、ファイルを配布、またはソフトウェアのアンインストールを指令する単位です。ソフトウェアを配布してインストールまたはファイルを配布する場合は、指定したパッケージを配布します。

探索

指定されたネットワークの範囲でネットワークに接続されている機器、または Active Directory に登録されている機器を発見することです。

単数サーバ構成

1 台の管理用サーバで JP1/IT Desktop Management 2 を運用するシステムです。最小構成および基本構成が単数サーバ構成に該当します。

チャットサーバ

チャットを開始するために、各コンピュータからの接続先となる機能です。

中継システム

JP1/IT Desktop Management 2 - Agent を中継システムとしてインストールしたサーバです。中継システムを設置すると、リモートインストールおよびリモートコレクトによる、管理用サーバおよびネットワークの負荷を軽減できます。プログラム名は「JP1/IT Desktop Management 2 - Agent」です。

直下

任意の管理用サーバを指した場合に、その管理用サーバを管理元とする機器や設定のことです。例えば「自サーバ直下のコンピュータ」と呼んだ場合、エージェントの接続先を自サーバに設定しているコンピュータを指します。

追加管理項目

JP1/IT Desktop Management 2 の各資産情報に任意に追加できる管理項目です。追加管理項目を作成することで、独自の情報を管理できるようになります。

データベースマネージャ

データベースのバックアップやリストア、データベース領域の再編成をするためのツールです。

デフォルトエージェント設定

エージェントをセットアップする際に必要な、管理用サーバの接続先やインストールの設定などの項目について JP1/IT Desktop Management 2 が提供するエージェント設定です。

デフォルトポリシー

JP1/IT Desktop Management 2 が提供するセキュリティポリシーです。基本的なセキュリティ環境を維持するために必要な設定がされています。

デフォルトポリシーは、管理対象のコンピュータにデフォルトで割り当てられます。また、セキュリティポリシーの割り当てを解除した場合に、間接的に割り当てられるセキュリティポリシーがないときは、デフォルトポリシーが割り当てられます。

統括管理用サーバ

JP1/IT Desktop Management 2 - Manager をインストールしたサーバのうち、複数サーバ構成の最上位に設置されたサーバです。複数サーバ構成システムでは、統括管理用サーバと管理用中継サーバを合わせて「管理用サーバ」と呼ぶことがあります。

（ナ行）

認証サーバ

JP1 ユーザーのアクセス権限を管理するサーバです。一つのユーザー認証圏に 1 台設置する必要があります。このサーバを利用して JP1 ユーザーを一括で管理します。

ネットワーク制御リスト

機器ごとにネットワーク接続を許可するかどうかの設定です。接続を許可する期間も設定できます。

ネットワーク制御用アプライアンス

JP1/NETM/NM を導入したアプライアンス製品です。JP1/NETM/NM - Manager と連携することで、ネットワーク制御用アプライアンスが監視しているネットワークセグメントのネットワーク接続を、JP1/IT Desktop Management 2 から制御できます。

ネットワークモニタ

ネットワーク接続が許可されていない機器（管理対象または除外対象に登録されていない機器）がネットワークに接続されたことを自動的に検知して、ネットワーク接続を制御する機能です。

ネットワークモニタエージェント

ネットワークを監視するコンピュータにインストールするプログラムです。操作画面からオンライン管理のコンピュータを選択してネットワークモニタを有効にすると自動的にインストールされます。プログラム名は「JP1/IT Desktop Management 2 - Network Monitor」です。

ネットワークモニタ設定

ネットワークモニタを有効にしたネットワークセグメントに新規に接続された機器のネットワーク接続の制御方法を定義した設定です。

（ハ行）

ハードウェア資産情報

JP1/IT Desktop Management 2 で管理できる資産情報の一つです。組織で保有する機器（ハードウェア資産）の情報を登録します。

パッケージ（ITDM 互換配布用）

コンピュータに配布したいソフトウェアまたはファイルを、配布（ITDM 互換）画面で JP1/IT Desktop Management 2 に登録したものです。配布（ITDM 互換）画面で配布できます。

判定

JP1/IT Desktop Management 2 が収集した各コンピュータの機器情報と、セキュリティポリシーでの判定項目の設定を比較して、各判定項目およびコンピュータ自身のセキュリティのレベル（危険レベル）を付与することです。

判定除外ユーザー設定ファイル

セキュリティ状況の判定対象から除外する OS のユーザーアカウントを指定するファイルです。

秘文ログ

秘文によって取得されたログです。

ファイル持ち出しによる不審操作

セキュリティポリシーで、次に示す不審と見なす操作の項目をチェックした場合に検知される不審操作です。

・[添付ファイル付きメールの送受信]

・[Web/FTP サーバの使用]

・[外部メディア（リムーバブルディスク）へのファイルコピーと移動]

複数サーバ構成

統括管理用サーバおよび複数の管理用中継サーバによって階層化されたシステムです。システムの構成要素に中継システムを含むことがあります。

ブラックリスト方式

ネットワークへの接続を許可しない機器を指定して、機器のネットワークへの接続を制御する方式です。指定した機器以外のネットワークへの接続が許可されます。

変更履歴

管理対象のコンピュータの機器情報に変更があった場合に、変更の履歴として取得できる情報のことです。操作画面から参照したり、保存用の変更履歴として CSV ファイルに出力したりできます。

保存用の変更履歴

CSV ファイルに出力される、保存を目的とした変更履歴のことです。

ホワイトリスト方式

ネットワークへの接続を許可する機器を指定して、機器のネットワークへの接続を制御する方式です。指定した機器以外のネットワークへの接続が遮断されます。

（マ行）

メニューエリア

操作画面の左側に表示されるエリアです。選択した画面に応じてメニューが表示されます。各メニューの項目を選択すると、操作画面の右側のインフォメーションエリアに、対応する情報が表示されます。

（ヤ行）

ユーザーアカウント管理権限

JP1/IT Desktop Management 2 のユーザーアカウントに設定できる権限の一つです。
JP1/IT Desktop Management 2 のユーザーアカウントを追加したり、削除したりできます。

（ラ行）

ライセンスキーファイル

JP1/IT Desktop Management 2 のライセンスを購入した際に提供されるファイルです。ライセンス登録時に使用します。

リクエスタウィザード

コンピュータからコントローラに接続要求を出す際に、 接続方法を設定するウィザードです。

リクエストサーバ

リモートコントロール機能で、コンピュータからの接続要求を受け付ける機能です。

リムーバブルディスク

ディスクドライブからディスクを取り出して交換できる記録媒体です。

リモートインストール

管理用サーバから利用者のコンピュータへ、ネットワークを経由してソフトウェアおよびファイルを一括で配布する機能です。

リモートインストールマネージャ

Remote Install Manager のことです。

リモートインストールマネージャを使用した配布

JP1/IT Desktop Management 2 が提供する 2 つの配布機能のうち、JP1/IT Desktop Management 2 のコンポーネントである Remote Install Manager を使用して配布する機能のことです。コマンドを使用して配布することもできます。ITDM 互換配布に対してこう呼びます。

リモートコレクト

管理対象のコンピュータに格納されているファイルを、リモートインストールマネージャを使用して一括で収集する機能です。

リモートコントロール機能

遠隔地にあるコンピュータに接続し、呼び出したコンピュータの画面に対してキーボード操作やマウス操作ができる機能です。

リモコンエージェント

エージェントのプログラムの一部です。 リモコンエージェントとコントローラが標準接続することで、すべてのリモートコントロール機能が使用できるようになります。

リモコンプレーヤー

リモートコントロールで、録画したファイルを目的に応じて再生を一時停止したり、再生の一部をスキップしたりして、再生をコントロールする動画プレーヤーです。

レポート

JP1/IT Desktop Management 2 で管理している情報を、目的別に集計した画面のことです。表示されているイメージをそのまま印刷できます。

索引

あ

い

う

え

お

か

き

く

け

す

せ

そ

た

ち

て

と

な

に

ね

は

れ

ろ

わ

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