HITACHI
Inspire the Next

JP1 Version 9 JP1/IT Desktop Management

導入・設計ガイド

3020-3-S93-10

対象製品

P-2642-7394 JP1/IT Desktop Management - Manager 09-51 （適用 OS：Windows 7 Professional、Windows 7 Enterprise、Windows 7 Ultimate、Windows Server 2008 Datacenter、Windows Server 2008 Enterprise、Windows Server 2008 Standard、Windows Vista Business、Windows Vista Enterprise、Windows Vista Ultimate 、Windows Server 2003、Windows XP Professional（Service Pack 2、3））

輸出時の注意

本製品を輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。
なお、ご不明な場合は、弊社担当営業にお問い合わせください。

商標類

Acrobat は、Adobe Systems Incorporated（アドビシステムズ社）の商標です。
Active Directory 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。
Adobe、および Flash は、Adobe Systems Incorporated（アドビシステムズ社）の米国ならびに他の国における商標または登録商標です。
Android は、Google Inc. の登録商標です。
Apple Remote Desktop は、Apple Inc.の商標です。
AppLocker 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。
「B's Recorder」の名称は、ソースネクスト株式会社の日本国内における登録商標です。
BSAFE は、EMC 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。
Citrix XenApp は、Citrix Systems, Inc.の米国およびその他の国における商標です。
F-Secure は、F-Secure Corporation の登録商標です。
Firefox は Mozilla Foundation の登録商標です。
Intel vPro は、アメリカ合衆国およびその他の国における Intel Corporation の商標です。
Internet Explorer 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。
iOS は、Apple Inc の OS 名称です。
Kaspersky は、米国における Kaspersky Lab の登録商標です。
Linux は、Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。
Mac OS は、米国および他の国々で登録された Apple Inc.の商標です。
McAfee、VirusScan、NetShield は、米国法人 McAfee, Inc. またはその関係会社の米国またはその他の国における登録商標です。
Microsoft .NET は、お客様、情報、システムおよびデバイスを繋ぐソフトウェアです。
Microsoft および Forefront 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 および Hyper-V 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 は、米国 Microsoft Corporation の商品名称です。
Microsoft、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。
MobileIron は、米国における MobileIron の登録商標です。
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。
OfficeScan and PC-Cillin are trademark of Trend Micro Incorporated.
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。
PC-98 は、日本電気(株)の商品名称です。
Pentium は、アメリカ合衆国およびその他の国における Intel Corporation の商標です。
PGP は、米国およびその他の国における PGP Corporation の登録商標です。
Photoshop は、Adobe Systems Incorporated（アドビ システムズ社）の商標です。
RSA は、EMC 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。
ServerProtect は、米国におけるトレンドマイクロ株式会社の登録商標です。
SOAP（Simple Object Access Protocol）は、分散ネットワーク環境において XML ベースの情報を交換するための通信プロトコルの名称です。
Sophos Anti-Virus は、Sophos Plc.の商品名称です。

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

Microsoft Corporation のガイドラインに従って画面写真を使用しています。

発行
2012 年 4 月　3020-3-S93-10

目次

はじめに

このマニュアルは、JP1/IT Desktop Management 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。

- 対象読者
- マニュアルの構成
- マイクロソフト製品の表記について
- マニュアルで使用しているアイコンと書式について
- オンラインヘルプについて
- 変更内容

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 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 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、次に示す章から構成されています。

第 1 章　製品の概要

JP1/IT Desktop Management の概要とシステムの構成要素、および特長について説明しています。

第 2 章　機能の紹介

JP1/IT Desktop Management 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 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。

マイクロソフト製品の表記について

このマニュアルでは、マイクロソフト製品の名称を次のように表記しています。

表記			製品名
Active Directory			Microsoft(R) Active Directory
AppLocker			Microsoft(R) AppLocker
Internet Explorer	Microsoft Internet Explorer		Microsoft(R) Internet Explorer(R)
	Windows Internet Explorer		Windows(R) Internet Explorer(R)
Microsoft.NET			Microsoft(R).NET
Microsoft Cluster Service			Microsoft(R) Cluster Service
Microsoft Forefront			Microsoft(R) Forefront(TM)
Microsoft Outlook			Microsoft(R) Outlook(R)
Microsoft Outlook Express			Microsoft(R) Office Outlook(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
	Windows 7		Microsoft(R) Windows(R) 7 Enterprise
			Microsoft(R) Windows(R) 7 Home Premium

表記			製品名
			Microsoft(R) Windows(R) 7 Professional
			Microsoft(R) Windows(R) 7 Starter
			Microsoft(R) Windows(R) 7 Ultimate
	Windows Server 2003	Windows Server 2003	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
			Microsoft(R) Windows Server(R) 2003, Standard Edition
			Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
			Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
		Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
			Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
			Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
			Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
	Windows Server 2008	Windows Server 2008 Datacenter	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
		Windows Server 2008 Enterprise	Microsoft(R) Windows Server(R) 2008 Enterprise
			Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V
			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
			Microsoft(R) Windows Server(R) 2008 Standard
			Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V
	Windows Vista		Microsoft(R) Windows Vista(R) Business
			Microsoft(R) Windows Vista(R) Enterprise
			Microsoft(R) Windows Vista(R) Home Basic
			Microsoft(R) Windows Vista(R) Home Premium
			Microsoft(R) Windows Vista(R) Ultimate
	Windows XP	Windows XP Home Edition	Microsoft(R) Windows(R) XP Home Edition Operating System
		Windows XP Professional	Microsoft(R) Windows(R) XP Professional Operating System

表記	製品名
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 メール	Windows(R) メール

マニュアルで使用しているアイコンと書式について

このマニュアルで使用するアイコンと書式について説明します。

説明文で使用するアイコン

アイコン	意味
	知っておくと便利な情報や補足情報です。
	注意しないと、操作や処理の失敗につながるおそれのある情報です。
	注意しないと、ご利用の環境に影響が及ぶおそれのある情報です。

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。
[ ] ー [ ]	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］メニューー［新規作成］を表示します。 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。

オンラインヘルプについて

JP1/IT Desktop Management では、次に示すオンラインヘルプを提供しています。

製品の操作方法のヘルプ

製品の運用例、各機能の操作方法、トラブルシュートなどを説明するヘルプです。JP1/IT Desktop Management の操作画面の［ヘルプ］－［JP1/IT Desktop Management のヘルプ］から起動できます。

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。

変更内容

変更内容（3020-3-S93-10）JP1/IT Desktop Management 09-51

追加・変更内容	変更個所
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。	1.2、1.3.9、2.1、2.6、2.6.1(1)、2.6.2(1)(8)、2.6.3、2.6.5、2.9.2、2.11.1、2.11.2(2)、2.11.7(1)、2.21、4.3.6、4.4、4.4.6、A.4.18、A.6、A.7、用語解説
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。	1.3.4、2.11.1、2.11.3、2.11.5、2.11.6、2.15.1、A.6
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。	2.3.4
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。	2.4.2(1)
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。	2.4.4、2.8.1
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。	2.4.4、2.8.1、4.6.9

追加・変更内容	変更個所
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。	2.5.2、4.2.1、4.2.2、4.2.3、4.2.4、4.2.5、A.5.3
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。	2.6.2(4)
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。	2.6.2(13)
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。	2.8.12
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。	2.9.5(1)
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。	2.9.6
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。	2.11.3
インフォメーションエリアに「ー」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。	2.11.7(1)
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。	2.12.5
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。	2.16、2.19.1
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。	4.2.5、A.5.3
ネットワークの前提条件の説明を改善した。	4.2.7
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。	4.4.3
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。	4.5.3
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。	4.5.5
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。	A.3
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。	A.4.4
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。	A.4.6

追加・変更内容	変更個所
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。	A.5.1
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。	A.5.2

単なる誤字・脱字などはお断りなく訂正しました。

1

製品の概要

JP1/IT Desktop Management 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 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 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 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 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 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 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 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わた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 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 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 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。

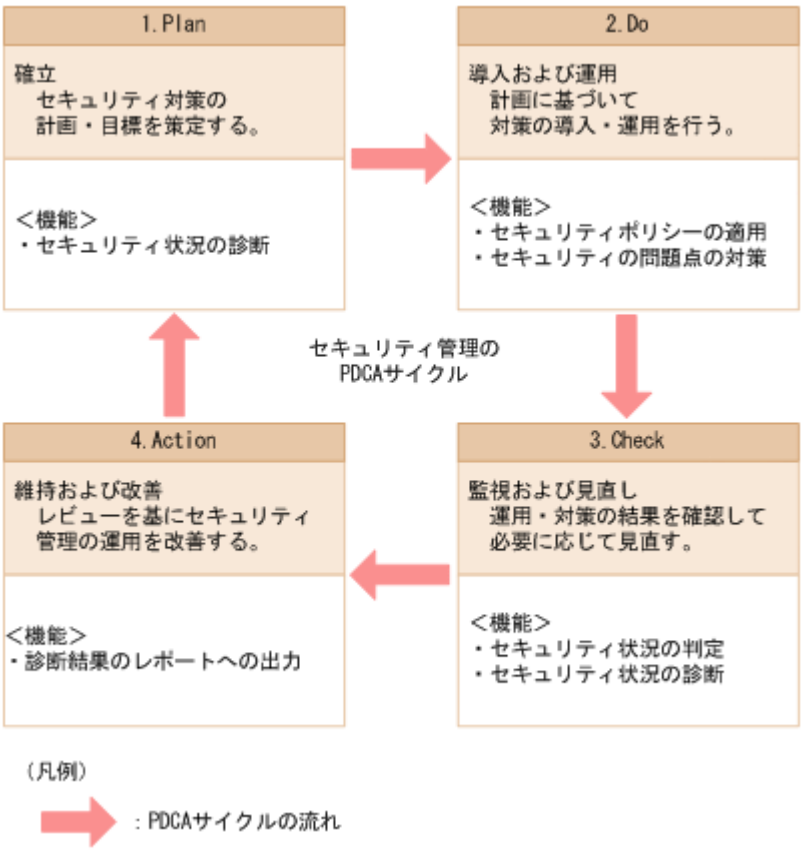
遠隔地の機器をリモートで操作できます

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 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 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 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 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 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 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 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 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 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 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。

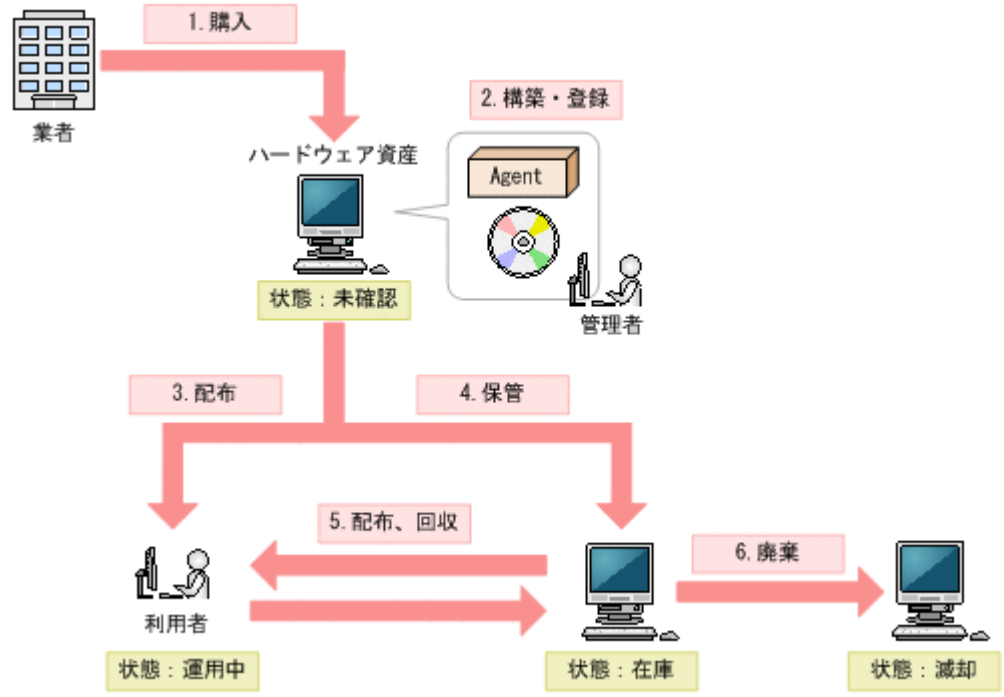
レビュー結果を基に、次回のサイクルでセキュリティルールの改善を計画します。

1.1.3 資産管理の流れ

JP1/IT Desktop Management 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。



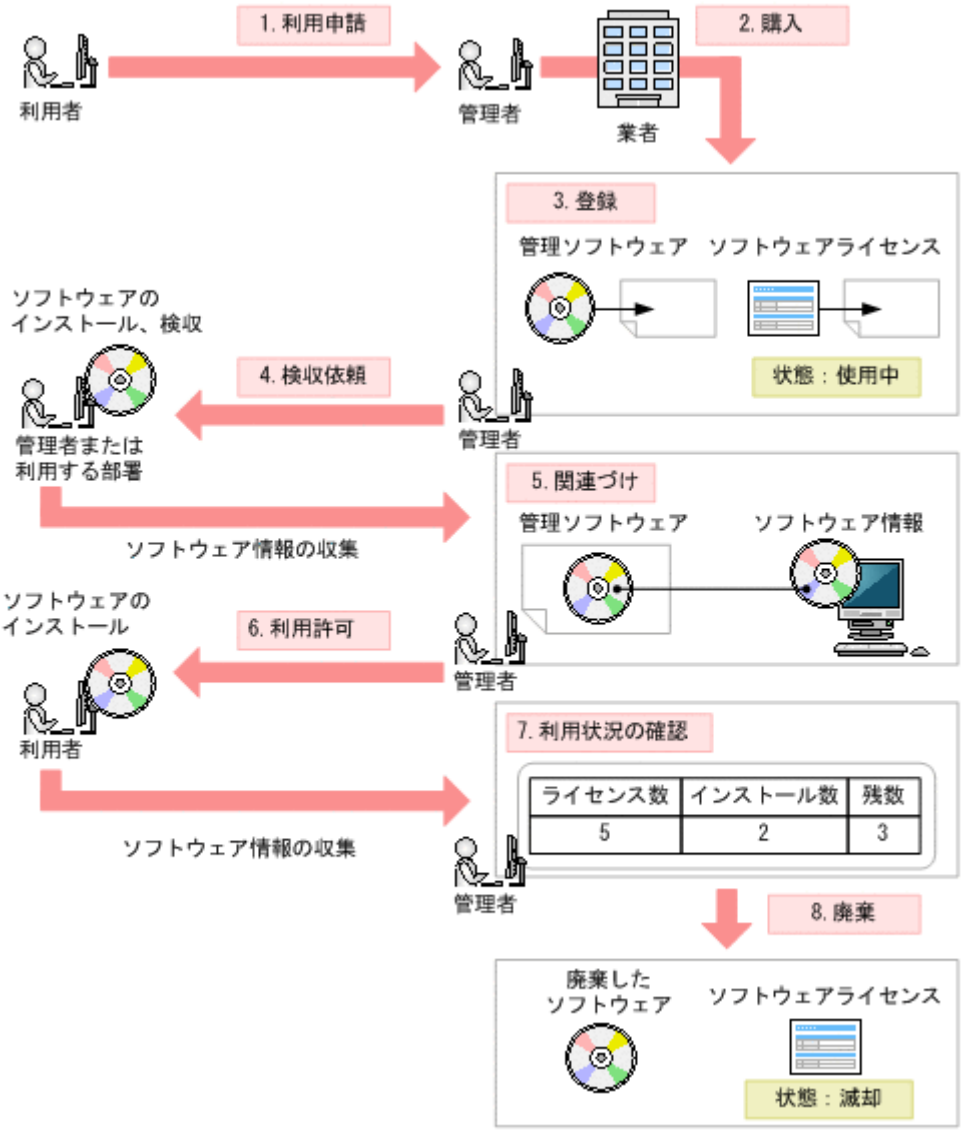
ハードウェア資産を購入したら、ハードウェア資産の環境を構築し、ハードウェア資産情報を JP1/IT Desktop Management に登録します。（図中：1～2）

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 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 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 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 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 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）

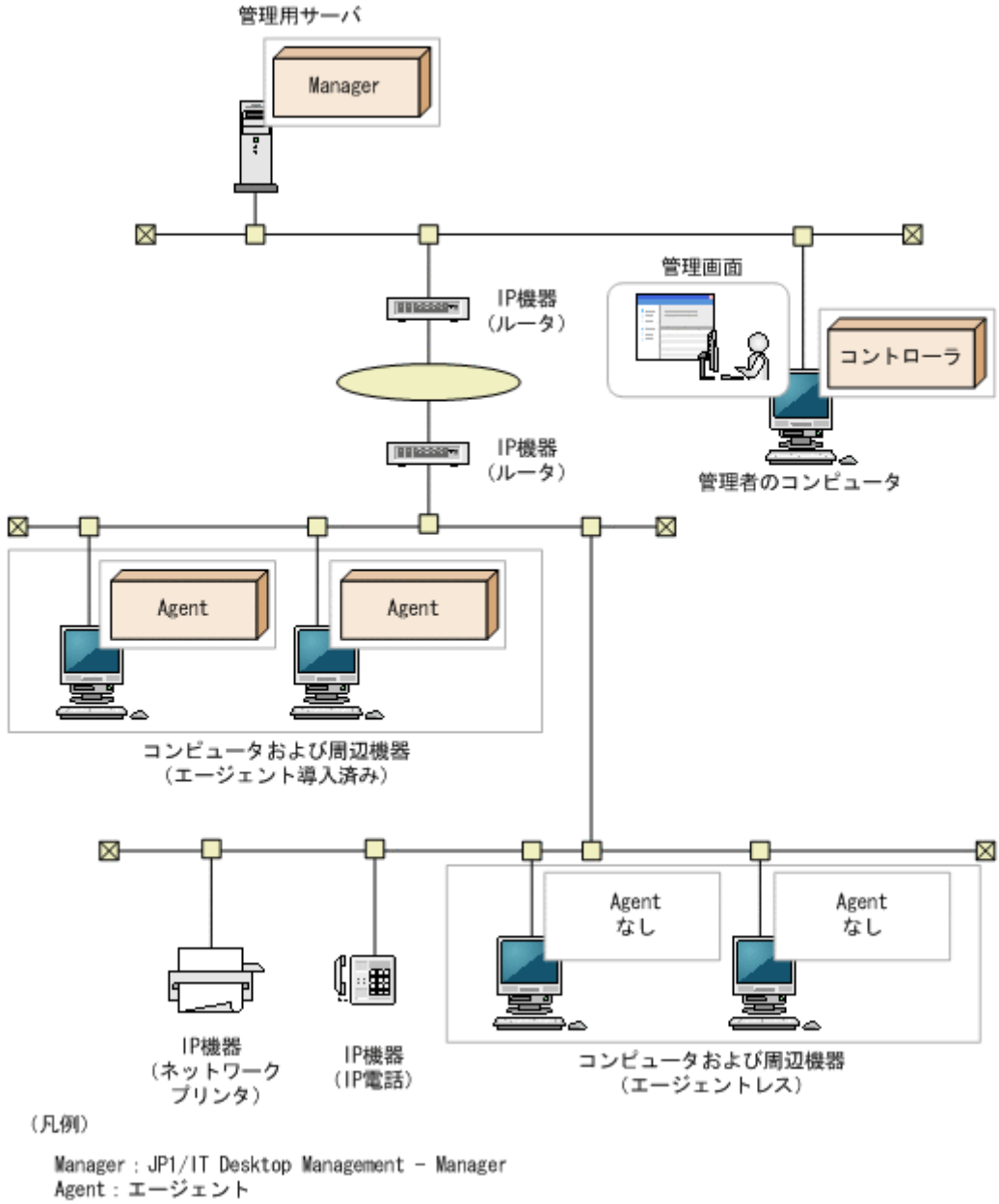
1.2 システム構成要素の紹介

このマニュアルでは、JP1/IT Desktop Management で管理するシステムを説明するに当たり、JP1/IT Desktop Management 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 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 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 が管理するさまざまな情報が格納されます。
管理者のコンピュータ		管理者が JP1/IT Desktop Management 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 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。
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。 エージェントがインストールされているコンピュータとインストールされていないコンピュータ（エージェントレスのコンピュータ）があります。
	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 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。



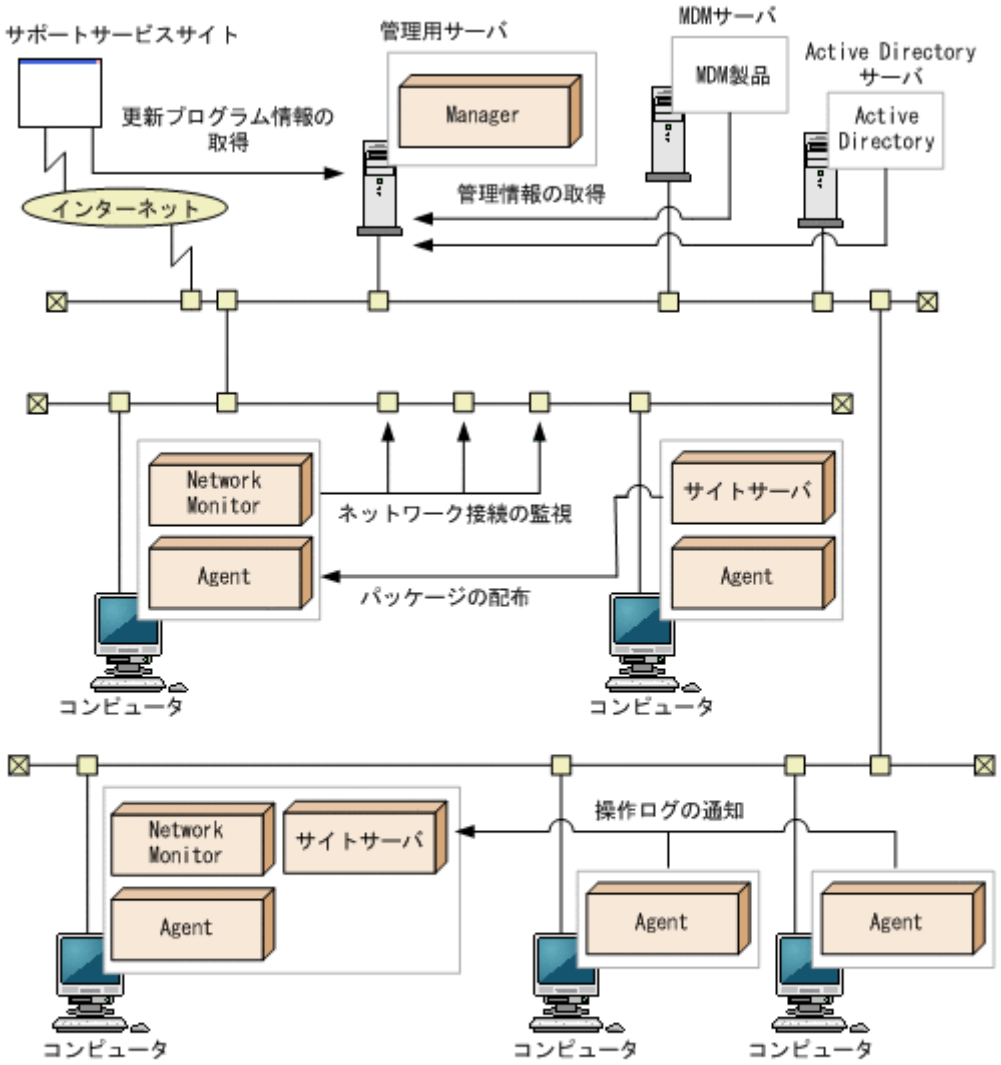
また、JP1/IT Desktop Management のコンポーネントを追加したり JP1/IT Desktop Management 以外のシステムと連携したりすることで、負荷分散、セキュリティ管理の強化、付加情報の管理など、目的に応じてシステムを管理できます。

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
サイトサーバ	管理用サーバやネットワークに掛かる負荷を分散するための、JP1/IT Desktop Management のコンポーネントです。 拠点ごとやネットワークセグメントごとにサイトサーバを設置することで、エージェント導入済みのコンピュータから取得した操作ログを保管して管理用サーバの負荷を軽減したり、配布用のパッケージを保管して配布時のネットワークの負荷を軽減したりできます。 サイトサーバを利用したシステムを、「サイトサーバ構成システム」と呼びます。
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 からインターネットを介して接続し、OS や Internet

構成要素名	定義
	Explorer についての最新の更新プログラムの情報を取得できます。ここで取得した情報を基に、各コンピュータに適用されている更新プログラム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、「更新プログラム管理構成システム」と呼びます。
Active Directory サーバ	Active Directory を導入しているサーバです。JP1/IT Desktop Management とは別に、Active Directory のプログラムが必要です。 JP1/IT Desktop Management 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 とは別に MDM 製品が必要です。JP1/IT Desktop Management 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。
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 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、エージェント導入済み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。

運用に応じてシステム構成要素を配置した、JP1/IT Desktop Management 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 - Manager
Agent：エージェント
サイトサーバ：サイトサーバプログラム
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 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。

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 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。

配布画面

配布画面では、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。

イベント画面

イベント画面では、JP1/IT Desktop Management 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 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 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 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

JP1/IT Desktop Management のヘルプ、操作画面のサイトマップ、関連 Web サイト、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 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

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 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、資産のインポート状況などの監視したり、データベースおよびハードディスクの状況を確認したりもできます。

参考 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－［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。

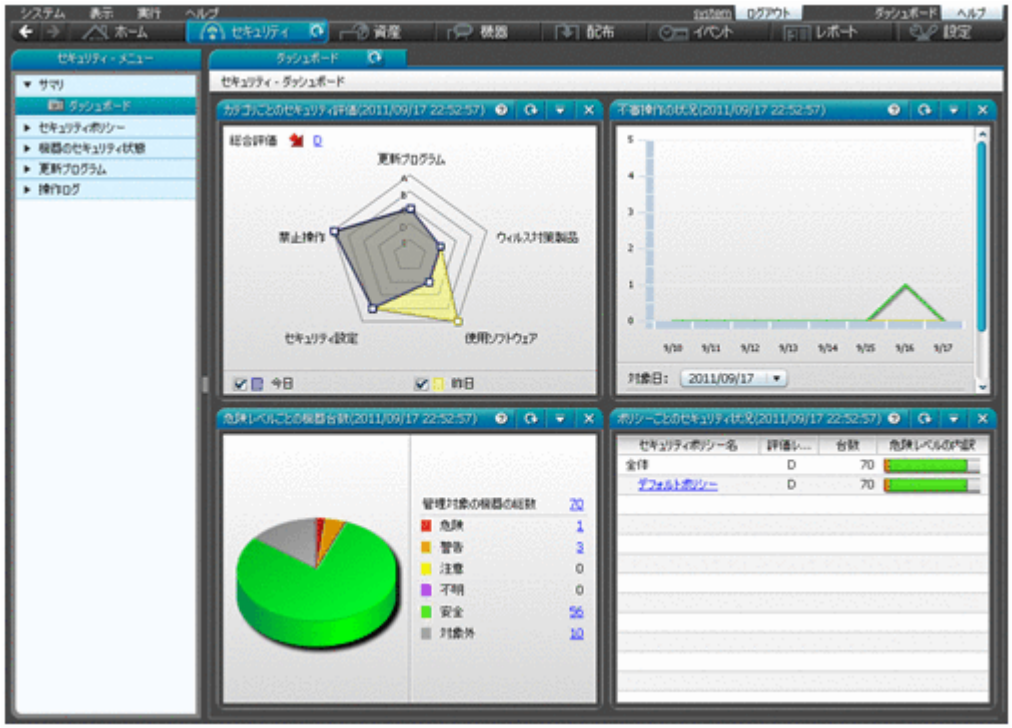
セキュリティ画面には次に示す画面があります。

- ［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
- ［操作ログ（分散操作ログ）］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。



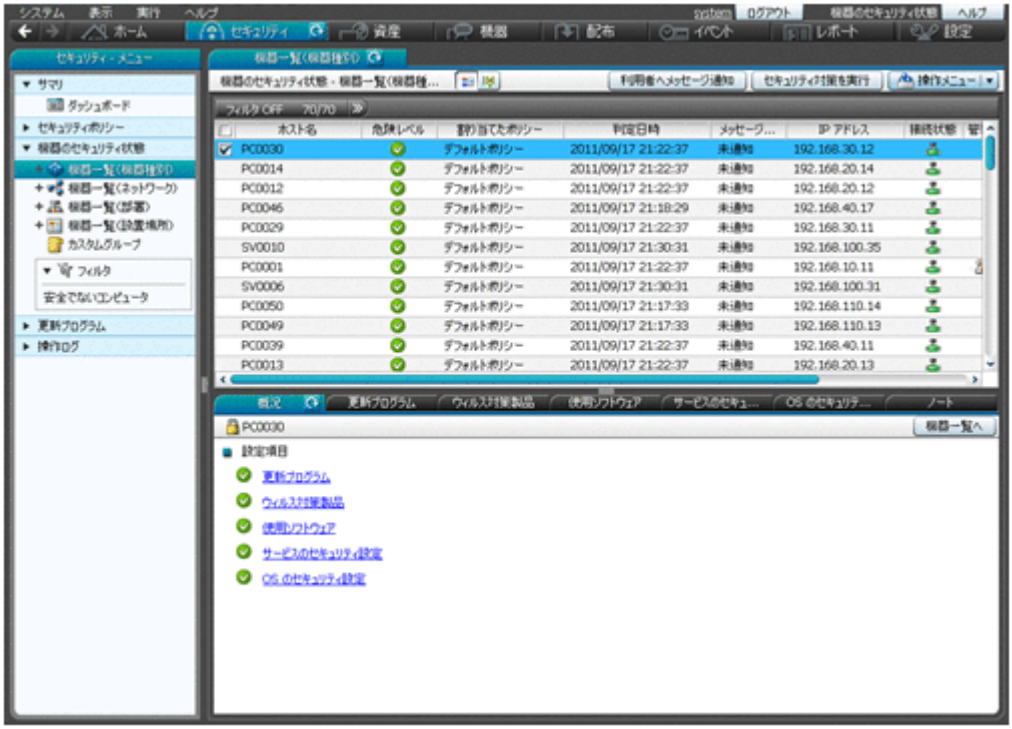
［セキュリティポリシー］画面

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

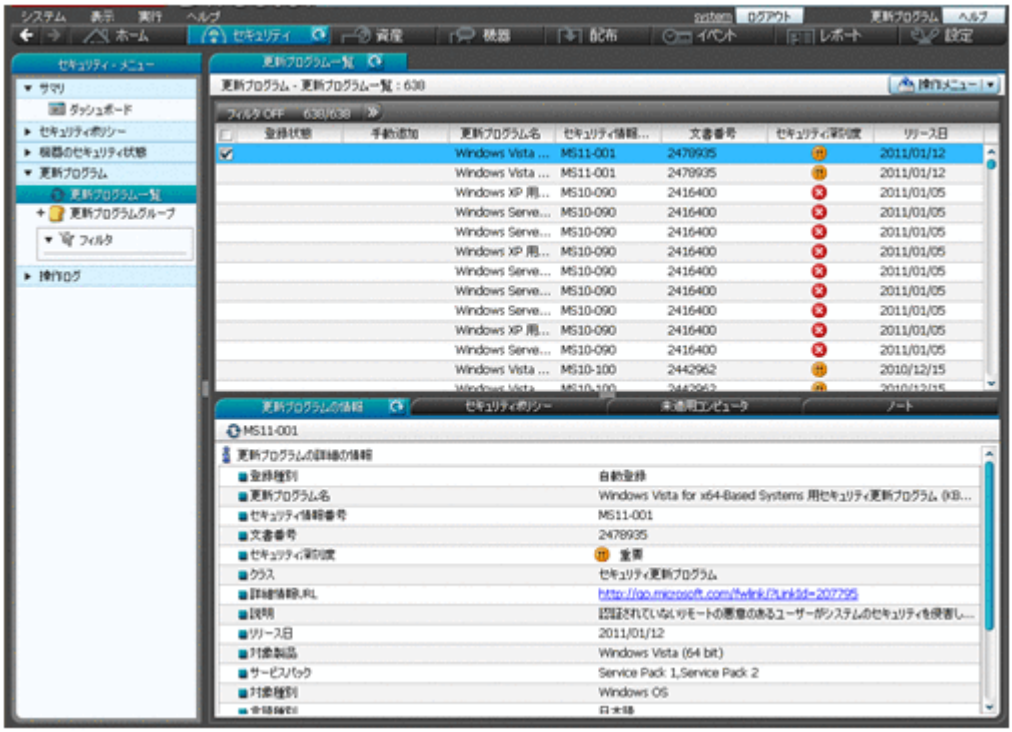
コンピュータごとのセキュリティ状態を確認し、セキュリティポリシーに違反しているコンピュータの利用者にメッセージを通知したり、強制対策したりできます。また、セキュリティポリシーをコンピュータごとに割り当てることができます。



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。

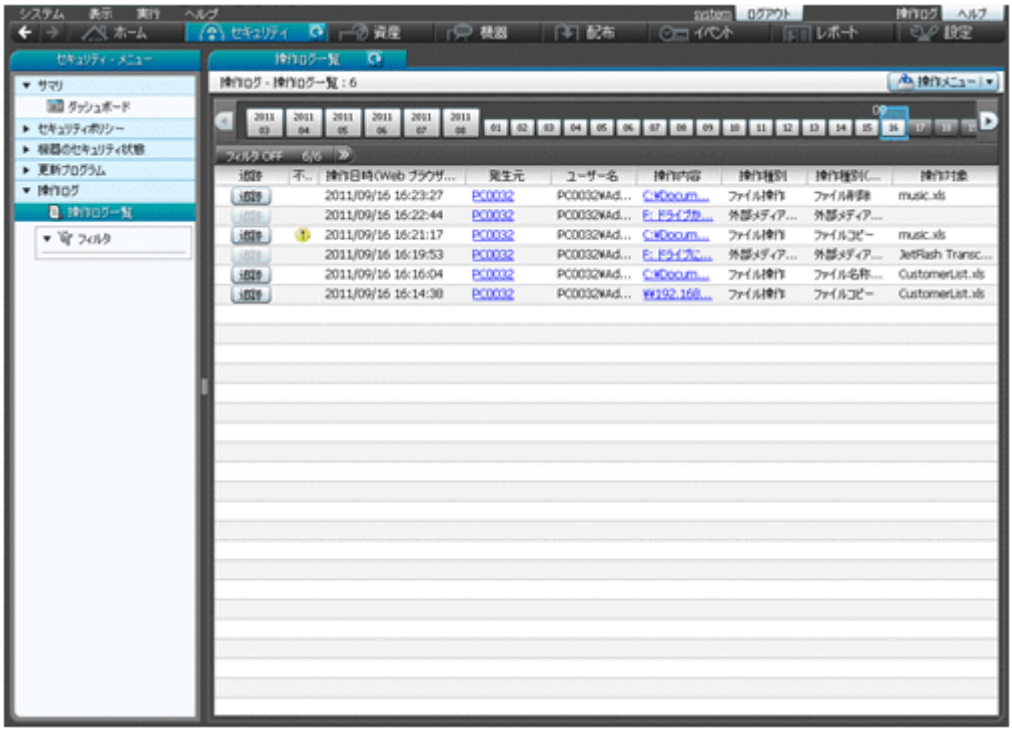


インフォメーションエリアの上部で選択した更新プログラムの情報が、下部のタブに表示されます。セキュリティポリシーへの設定状況や、更新プログラムが未適用のコンピュータを確認できます。

［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。

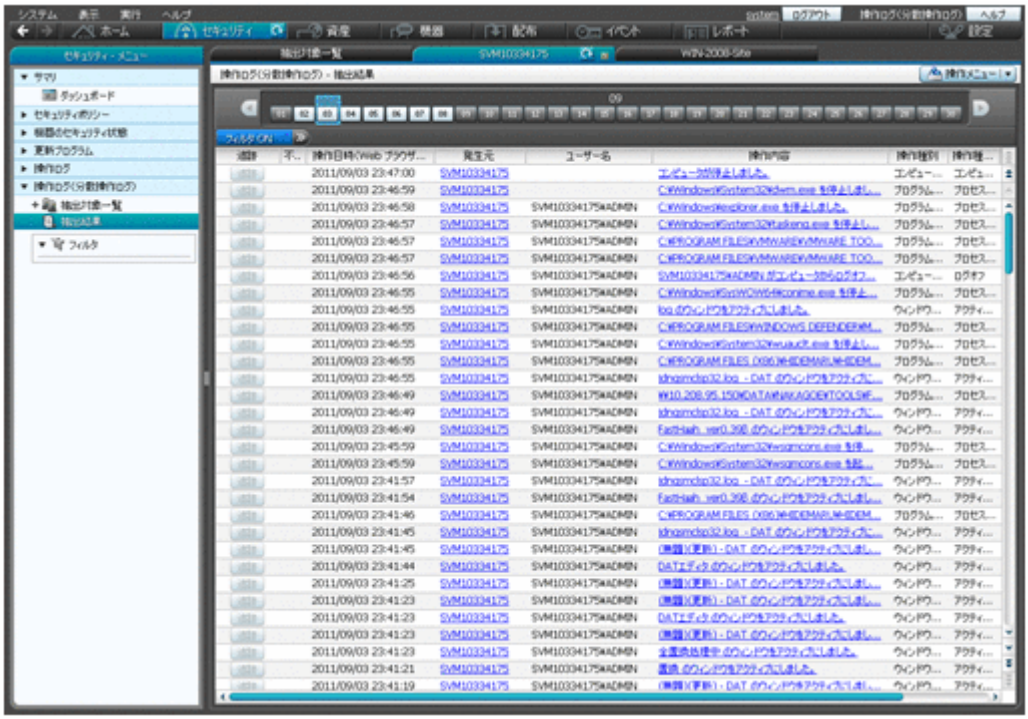


なお、管理用サーバに操作ログが取得されていない場合、この画面は表示されません。

［操作ログ（分散操作ログ）］画面

サイトサーバに取得された操作ログ（分散操作ログ）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、サイト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。

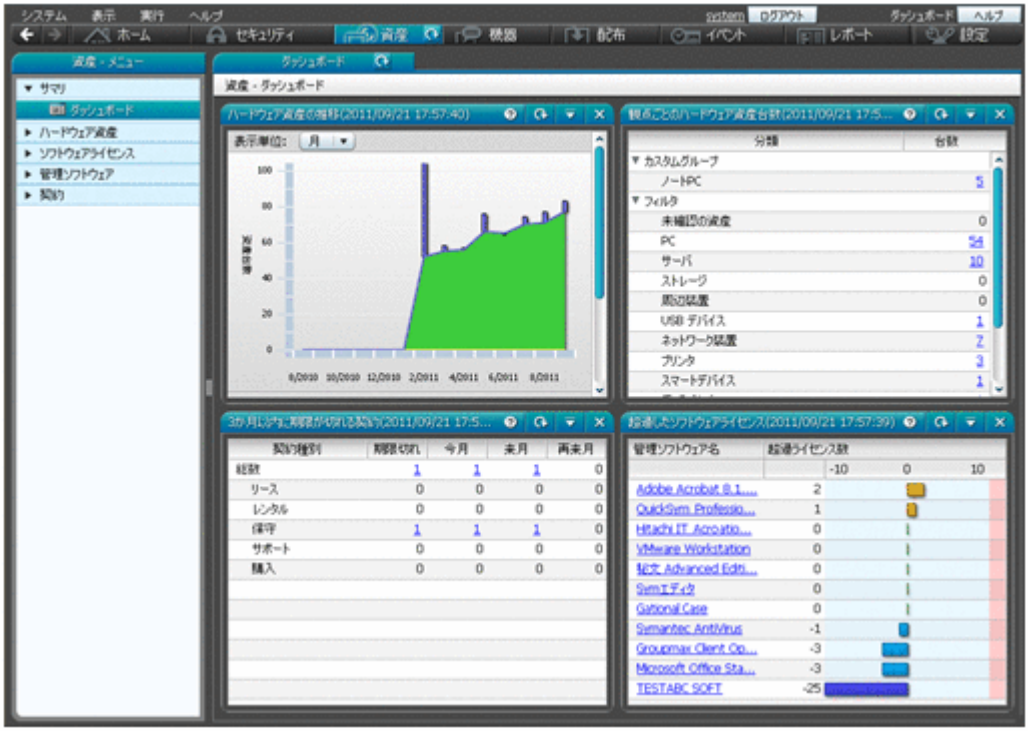
資産画面には次に示す画面があります。

- ［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
- ［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 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。

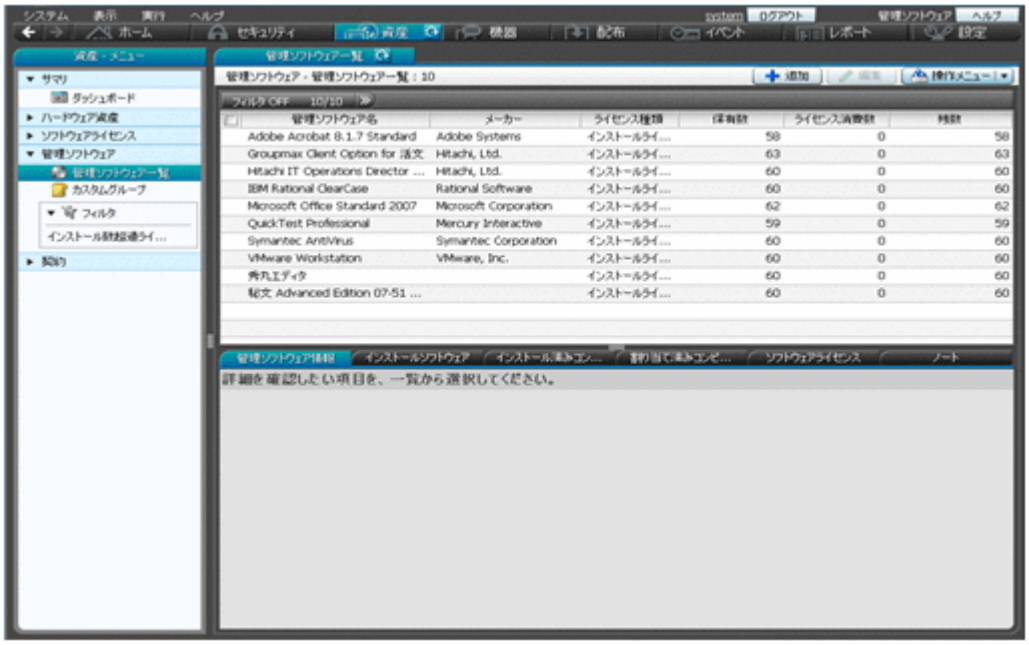
［ソフトウェアライセンス］画面

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。また、対応するソフトウェアライセンス情報が設定されている場合は、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。



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。

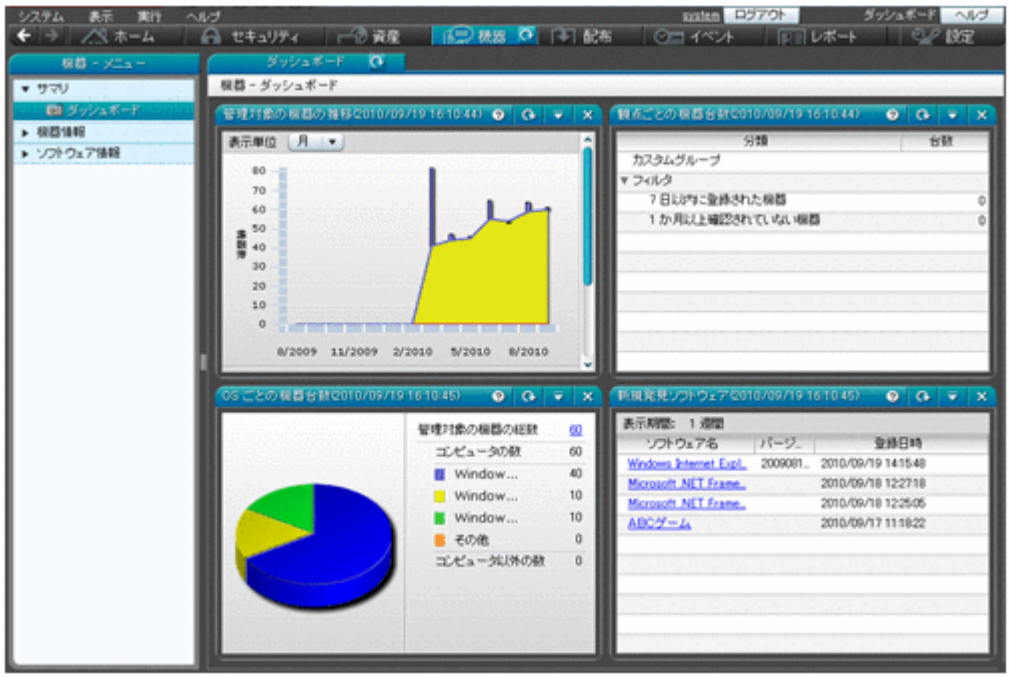
機器画面には次に示す画面があります。

- ［サマリ］画面
- ［機器情報］画面
- ［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。

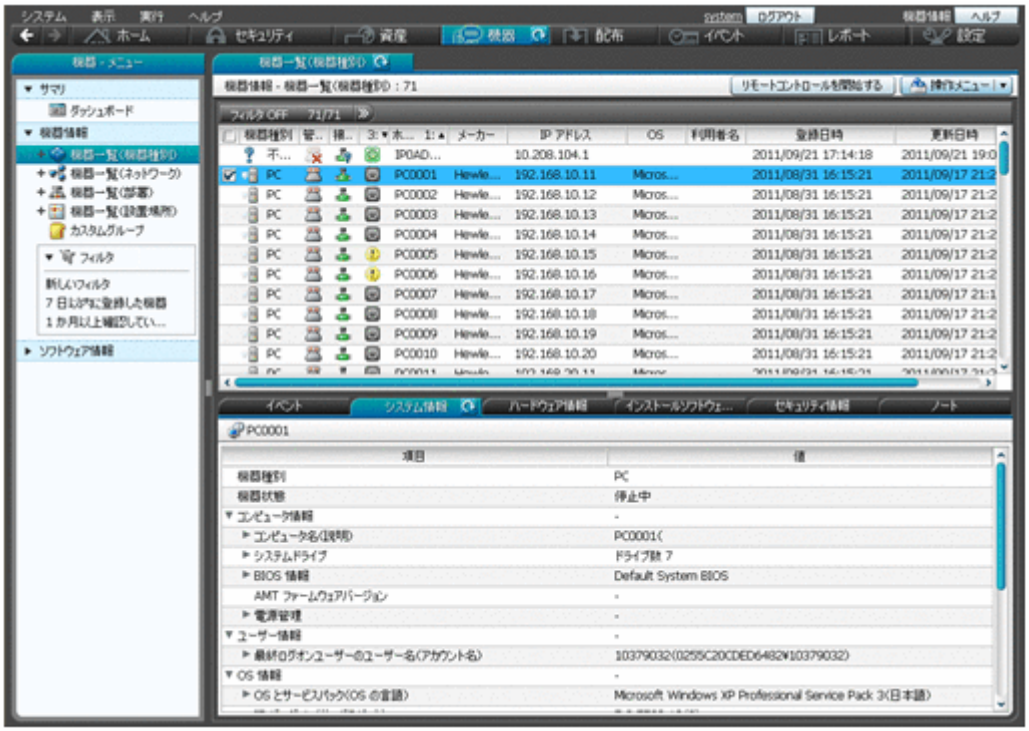
［サマリ］画面

JP1/IT Desktop Management 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

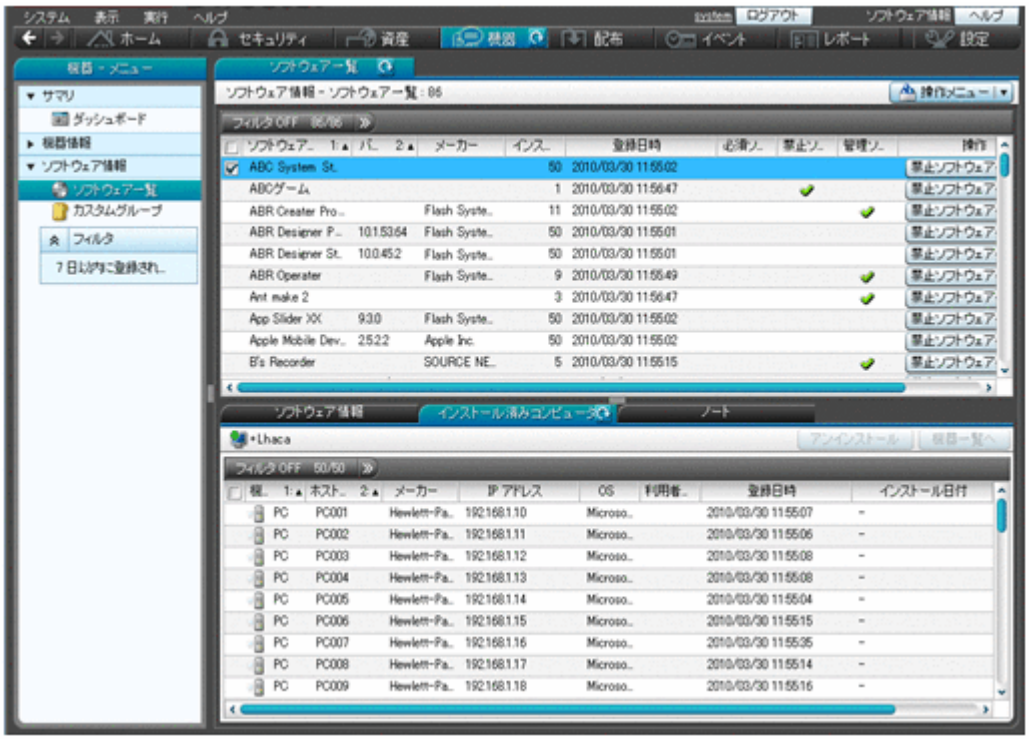
管理対象の機器の情報や電源状態などを確認できます。また、利用者へのメッセージ通知、コンピュータの電源制御、コンピュータのリモートコントロールなど、機器に対する操作を実行できます。



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。

［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 配布画面でできること

配布画面では、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。

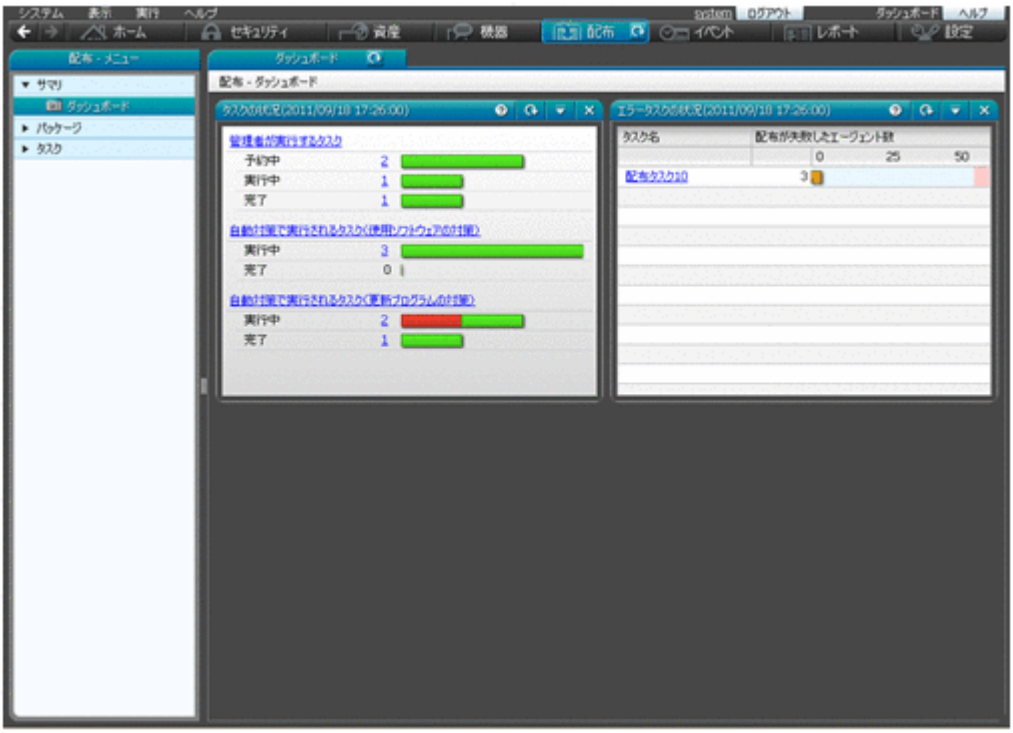
配布画面には次に示す画面があります。

- ［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

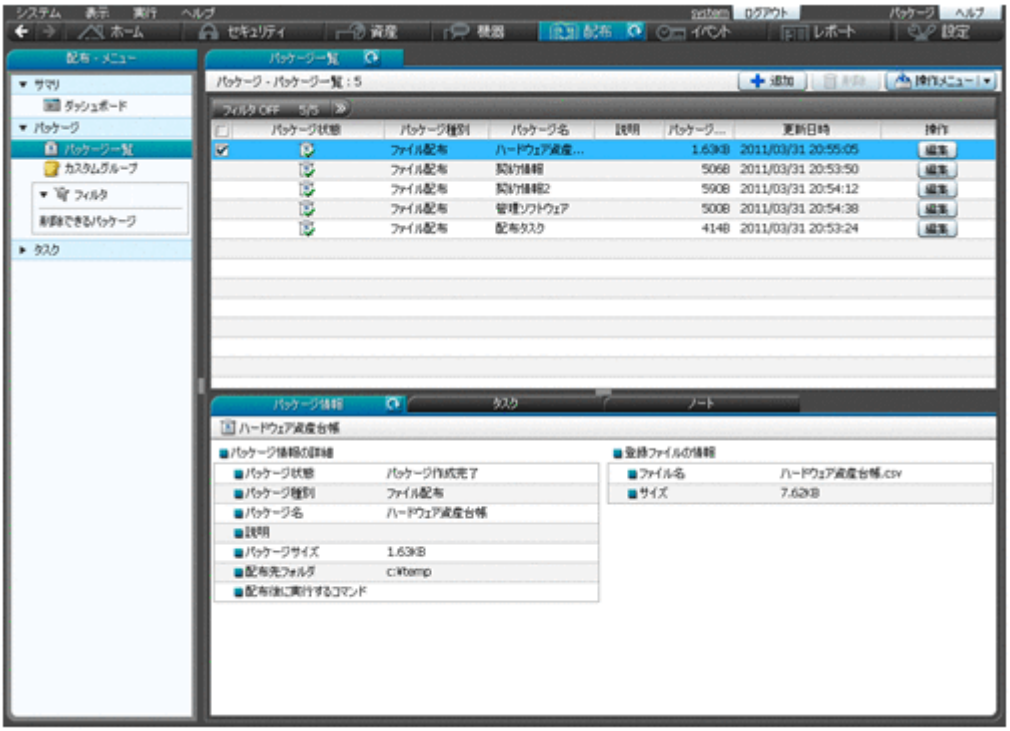
タスクの実行状況やエラーが発生したタスクをパネルで確認できます。



［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。

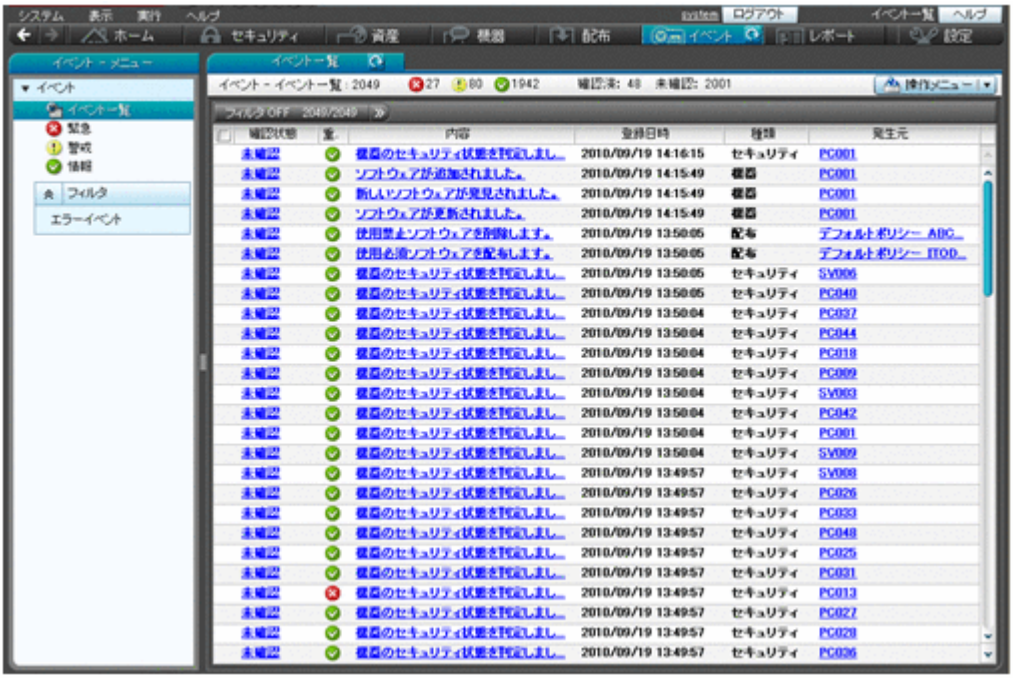
［タスク］画面

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。

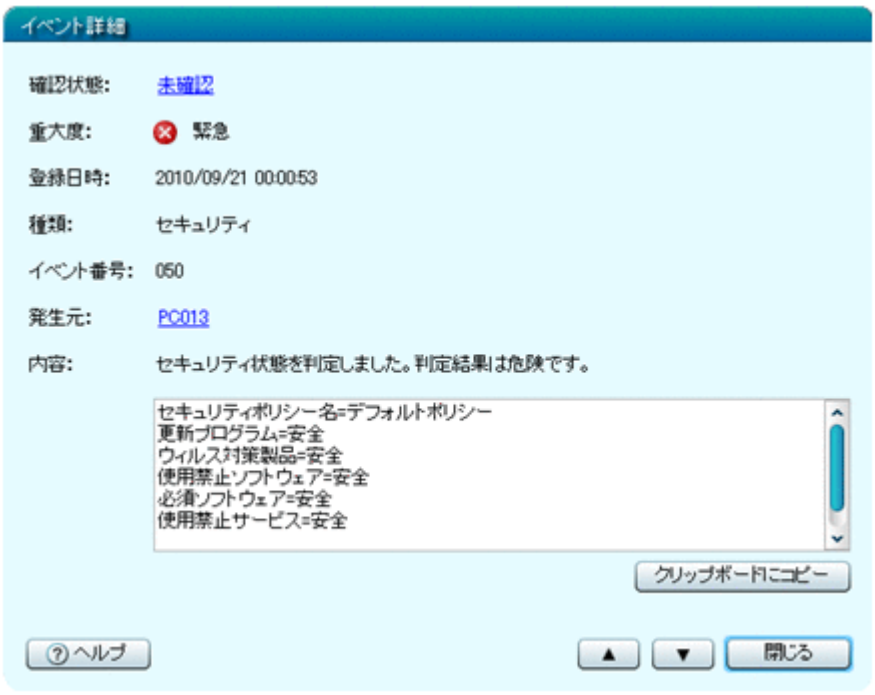
インフォメーションエリアの上部で選択したタスクの詳細情報が、下部のタブに表示されます。タスク情報、タスク状態、パッケージ情報などを確認できます。

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 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。

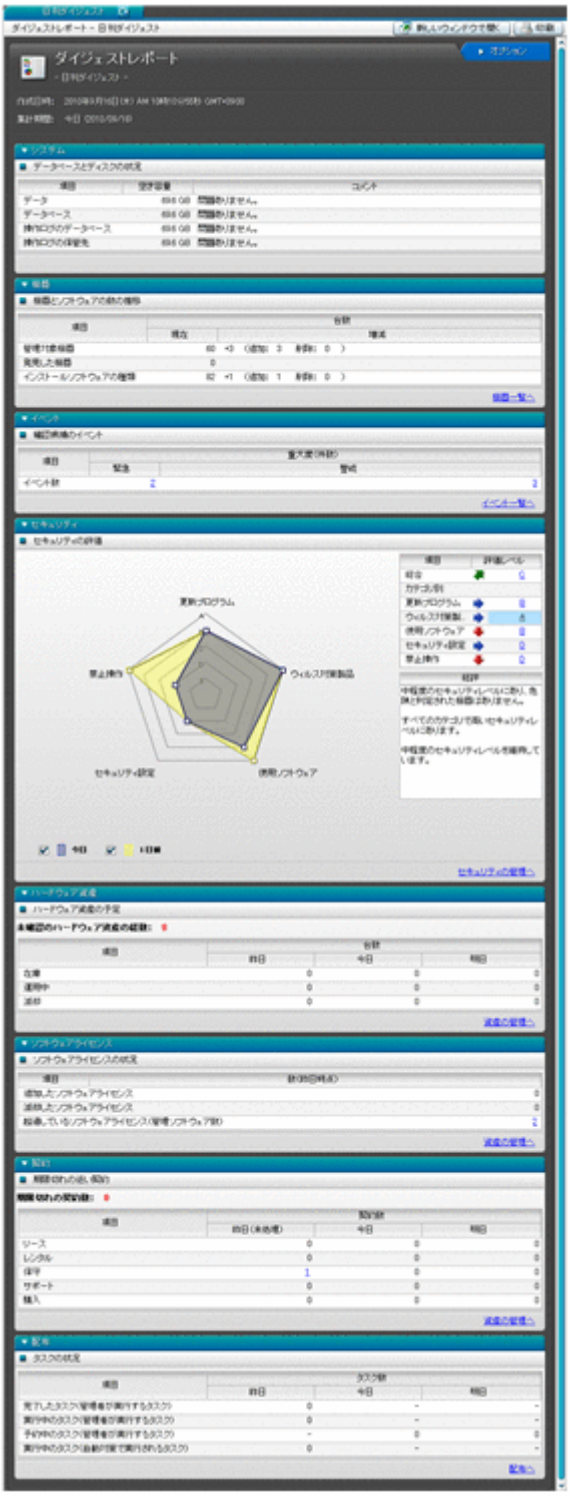
1.3.8 レポート画面でできること

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。

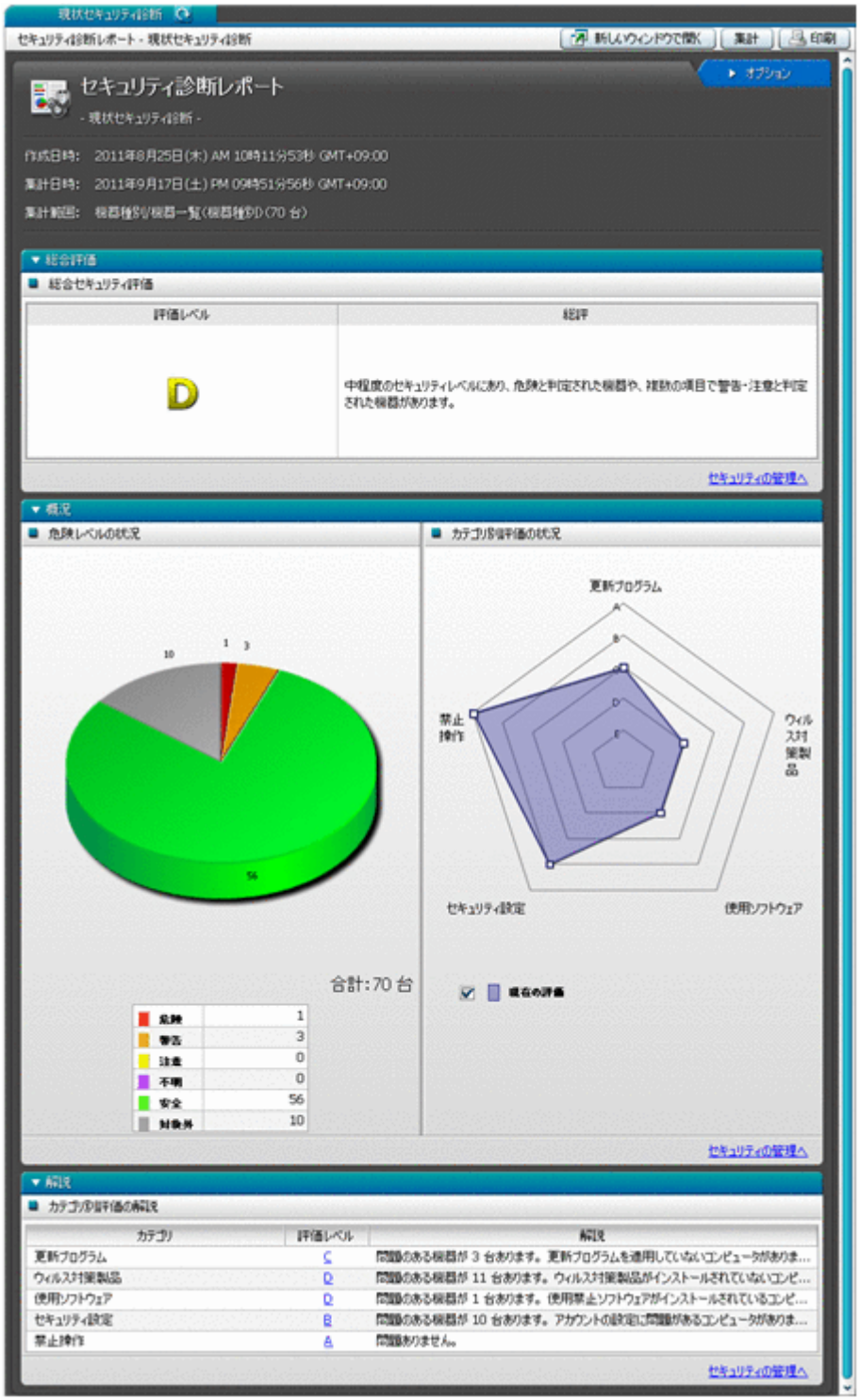
[日刊ダイジェスト] レポート

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 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 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 のユーザーアカウントを追加、編集、および削除できます。

［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 での機器の管理を始められます。

［エージェント］画面

エージェントを配信できます。また、エージェント設定を作成したり、各エージェントに割り当てたりできます。

［サーバ構成］画面

複数のサイトサーバをグルーピングしたサイトサーバグループを作成し、ネットワークセグメントごとにどのサイトサーバグループを接続先とするかを設定できます。

［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、ネットワークへの接続が許可されていない機器に、例外的に接続してよい通信先を設定できます。

［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。

［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 で AMT を使用するための設定もできます。

［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 製品との接続を設定できます。

［製品ライセンス］画面

JP1/IT Desktop Management 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 の主な機能について紹介します。

- 2.19 コマンドの利用
- 2.20 エージェントの操作
- 2.21 スマートデバイスの制御

2.1 機能一覧

JP1/IT Desktop Management で使用できる主な機能の一覧を次に示します。

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	権限や管轄範囲を設定することで、JP1/IT Desktop Management 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 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 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。 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。
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。
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。
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。
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。
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、ソフトウェアを配布してインストールできます。同様に、ファイルを配布したり、ソフトウェアをアンインストールしたりできます。
イベントの表示	JP1/IT Desktop Management 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。
サイトサーバの利用	サイトサーバを設置することで、操作ログの管理に掛かる負荷と、ソフトウェアおよびファイルの配布に掛かる負荷を分散できます。
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 を運用できます。
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 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。

機能	概要
エージェントの操作	エージェント導入済み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。
スマートデバイスの制御	MDM 製品と連携して、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。

2.2 システムの概況表示

JP1/IT Desktop Management 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 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 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。

- ［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

  機器の探索、資産情報のインポート、操作ログの取り込み、およびエージェントの配信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。

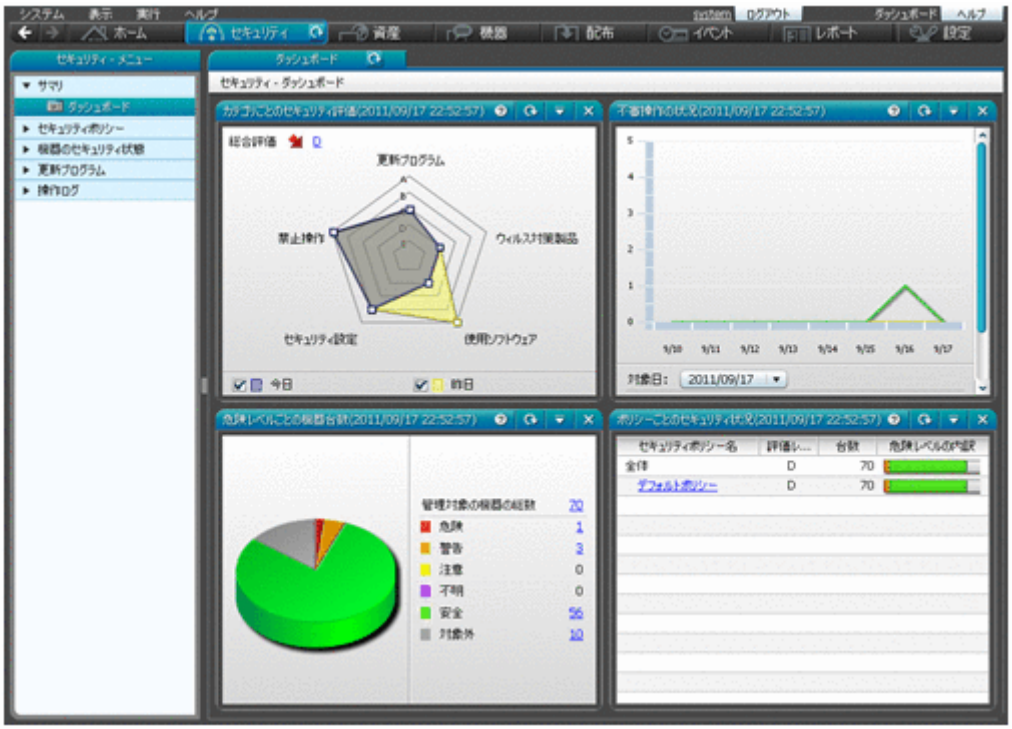
  - データを保存するフォルダの空き容量が少なくなった
  - ライセンス数を超過しているソフトウェアがある
  - 期限切れの契約がある

- ［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、および配布画面で表示できます。

参考 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－［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	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	機器の探索状況、資産情報のインポート状況、操作ログの読み込み状況、およびエージェントの配信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。
	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、製品の残りライセンス数が 0 になっ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 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。

カテゴリ	パネル名	説明
	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 が検知した不審操作の件数を確認できます。リンクから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減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 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ください。業務に関係ないソフトウェアを禁止ソフトウェアとして登録することをお勧めします。
配布	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。

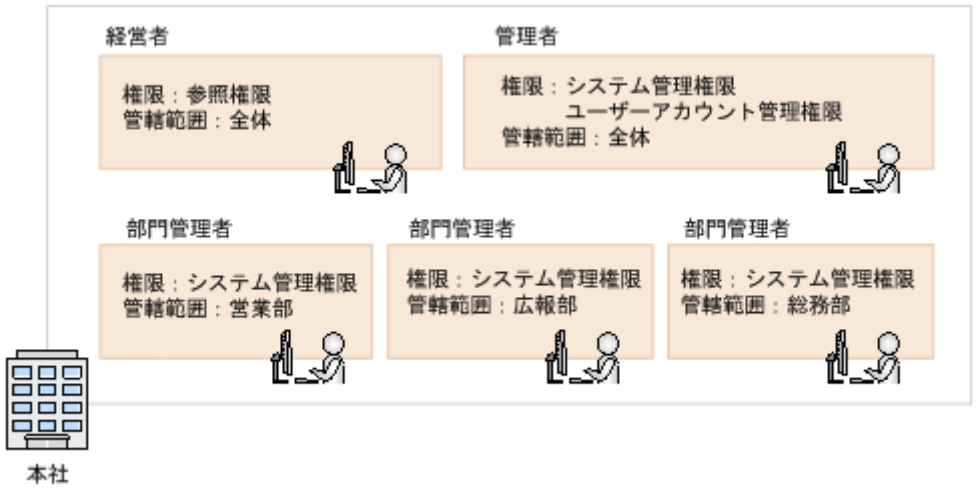
2.3 ユーザーアカウントの管理

部門管理者、経営者など、管理者以外にも JP1/IT Desktop Management を利用するユーザーがいる場合、それぞれに JP1/IT Desktop Management 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、管理情報の開示範囲に応じた権限を指定できます。 機器や資産を管理するシステム管理者、情報を参照できればよい経営者、部内の責任者など、用途に応じたユーザーアカウントを作成できます。

また、ユーザーアカウントには、管轄範囲を指定できます。 社内全体の機器数が多く、管理者一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。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。

管理情報の開示範囲に応じた権限と管轄範囲の設定の例を次の図に示します。



経営者

権限に参照権限を、管轄範囲に全体を設定します。そうすることで、操作画面で社内全体の管理状況を参照できます。ただし、設定画面の操作はできません。

管理者

権限にシステム管理権限とユーザーアカウント管理権限を、管轄範囲に全体を設定します。そうすることで、社内全体を管理できます。また、ユーザーアカウントを設定できます。

部門管理者

権限にシステム管理権限を、管轄範囲に担当の部署を設定します。そうすることで、部門管理者が管理できる機器やハードウェア資産が、管轄範囲に限定されます。また、ユーザーアカウントの管理を除いて、すべての機能を利用できます。

ユーザーアカウント管理権限が設定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 を利用するユーザー数に応じてユーザーアカウントを追加してください。

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、ユーザーアカウントを編集します。また、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。

管理体制の変更に伴ってユーザーアカウントが不要になった場合、ユーザーアカウントを削除してください。

参考 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 のログインに 3 回続けて失敗すると、ユーザーアカウントがロックされます。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。

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。

参考 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権限

JP1/IT Desktop Management のユーザーアカウントに設定できる権限には、次の 3 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 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 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 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。

2.3.3 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、表示できる画面および実行できる操作が異なります。権限ごとに表示できる画面および実行できる操作を次の表に示します。

画面		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		○	×	×
ホーム画面		○	△	△
セキュリティ画面		○	△	△
資産画面				
機器画面				
配布画面				
イベント画面				
レポート画面				
設定画面	［ユーザー管理］画面	×	○	×

画面		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
	［ユーザー管理］画面以外	○	×	×
レポートおよびセキュリティポリシーの印刷		○		
ヘルプの参照		○		

（凡例）○：操作できる　△：表示だけできる　×：表示および操作できない

2.3.4 管轄範囲を設定した場合の操作画面の差異

管轄範囲を設定したユーザーアカウントでログインすると、設定した管轄範囲の情報だけが表示され、実行できる操作を制限できます。管轄範囲を設定した場合の操作画面の差異を次の表に示します。

操作画面		管轄範囲が設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。 ・ ［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］ ・ ［ヘルプ］メニューの［操作画面サイトマップ］ また、サイトサーバを追加または削除したときに表示されるメッセージバーのメッセージが、リンクではなくなります。
	［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。
	［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	－

操作画面		管轄範囲が設定されている場合の差異
	［3 か月以内に期限が切れる契約］パネル	－
	［超過したソフトウェアライセンス］パネル	－
	［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	－
	［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。
セキュリティ画面	［サマリ］画面※	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。
	［機器のセキュリティ状態］画面	－
	［更新プログラム］画面	情報の参照だけできます。
	［操作ログ］画面	次のメニューは表示されません。 ・ ［保管した操作ログを取り込む］ ・ ［取り込んだ操作ログを削除する］
	［操作ログ（分散操作ログ）］画面	－
資産画面	［サマリ］画面※	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	［［利用者情報の入力］画面を定期的に表示させる］メニューは表示されません。 ソフトウェアライセンス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。 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	ソフトウェアライセンス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。 各ダイアログで、選択項目を新規追加できません。
	［管理ソフトウェア］画面	［インストールソフトウェア］タブの［禁止ソフトウェアへの追加］ボタンは表示されません。
	［契約］画面	契約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。 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※	パネルによって表示範囲が異なります。
	［機器情報］画面	次のメニューは表示されません。 ・ ［［利用者情報の入力］画面を定期的に表示させる］ ・ ［認証情報を設定する］

操作画面		管轄範囲が設定されている場合の差異
		ネットワークモニタが無効の場合に表示されるメッセージバーのメッセージが、リンクではなくなります。 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。
	［ソフトウェア情報］画面	［禁止ソフトウェアへの追加］ボタンおよび［ソフトウェアの削除］メニューは表示されません。
配布画面	［サマリ］画面※	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		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	－
	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	［ハードウェア資産］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	表示されません。
	［ユーザー管理］画面	－
	［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
	［エージェント］画面	［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。 ［エージェント設定］画面は、情報の参照だけできます。 ［エージェント設定の割り当て］画面は、情報の参照だけできます。また、管轄範囲内の情報だけが表示されます。 ［エージェントレス管理の設定］画面は表示されません。
	［サーバ構成］画面	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。

操作画面		管轄範囲が設定されている場合の差異
	［資産管理］画面	［インポート履歴の確認］画面だけ表示できます。［インポート履歴の確認］画面は、管轄範囲内の情報だけが表示されます。
	［機器］画面	表示されません。
	［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）－：管轄範囲を設定していない場合と差異はありません。

注※　［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。

参考 管轄範囲を設定した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 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 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、次の操作ができます。

Active Directory を探索する

組織内の機器を Active Directory で管理している場合、Active Directory サーバに登録されている機器を探索して、管理対象にできます。このとき、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て導入することもできます。

ネットワークを探索する

組織内のネットワークに接続されている機器を探索し、発見された機器を管理対象にできます。発見されたコンピュータには、自動的にエージェントを配信して導入することもできます。

インストールセットを作成する

コンピュータにエージェントを導入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、エージェントを導入できます。

2.4.1 機器の探索

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して、発見された機器を管理対象にできます。

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 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。

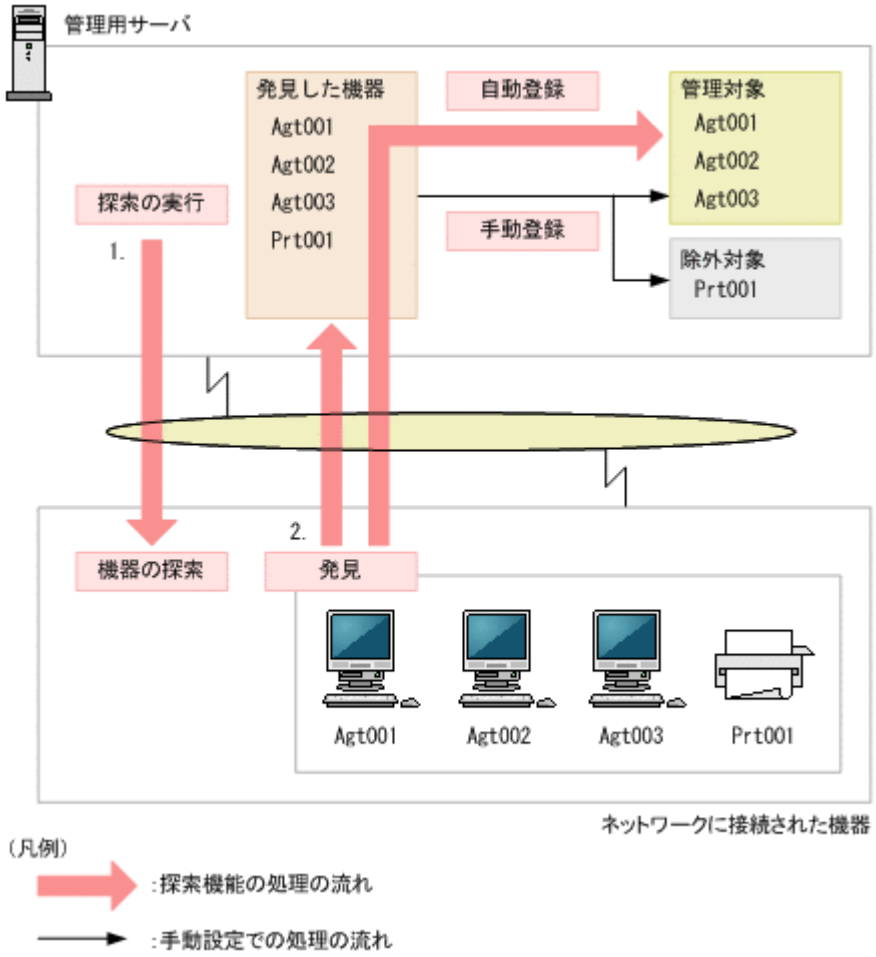
2.4.2 ネットワークに接続されている機器の探索

ネットワークに接続された機器を探索して、JP1/IT Desktop Management 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。

   探索するネットワークの範囲内にサイトサーバを設置している場合、サイトサーバから探索が実行されるため、管理用サーバからは直接参照できない機器も探索できます。組織内のすべての機器を発見したい場合は、サイトサーバの設置をお勧めします。なお、探索するネットワークの範囲内にサイトサーバが複数あるときは、各サイトサーバに範囲が割り振られ、並行して探索が実行されます。

参考 管理用サーバおよびサイトサーバは、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。

探索の実行時間の目安

ネットワークの速度が 100Mbps の場合、探索対象の機器が 10 台のときは探索に約 1.5 分掛かります。また、300 台の探索の Windows 認証がすべて成功するには約 15 分掛かります。

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
- (1) 探索の条件
- 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またはサイトサーバと同じセグメントにある場合、管理用サーバまたはサイトサーバからの ARP に応答できる
- 探索する機器が管理用サーバまたはサイトサーバと異なるセグメントにある場合、管理用サーバまたはサイトサーバからの 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。
- 管理用サーバまたはサイト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。

注意 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。

注意 NAT 環境では、エージェントレスの機器は管理できません。

注意 OS が 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。

参考 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 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 19 メガバイトのデータ転送量になります。

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 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 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 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 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 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。

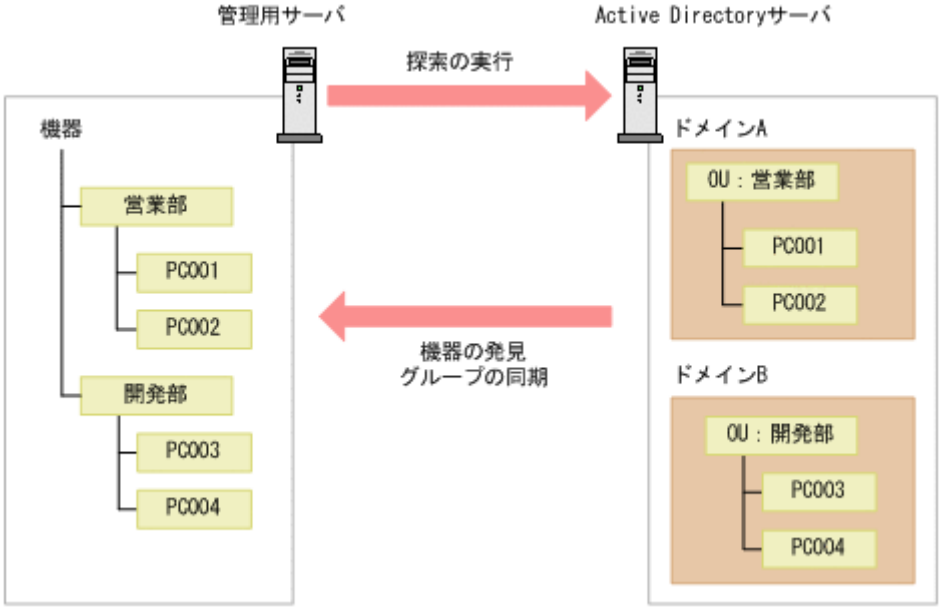
機器情報の取得時刻

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 に反映したいときは、この方法をお勧めします。［機器の管理を始めましょう］ウィザードまたは設定画面の［機器の探索］－［探索条件の設定］－［Active Directory の探索］画面で実行できます。

参考 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。

参考 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 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、管理共有を使用した探索はネットワークの探索結果が優先され、SNMP、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

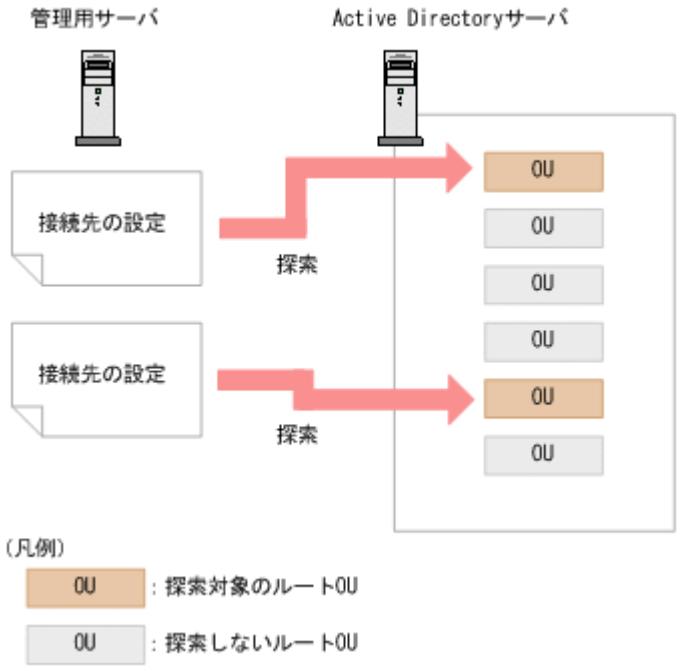
Active Directory を探索して機器を発見するためには、接続先となる Active Directory のサーバおよび探索対象とするドメインのルート OU を設定する必要があります。

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。

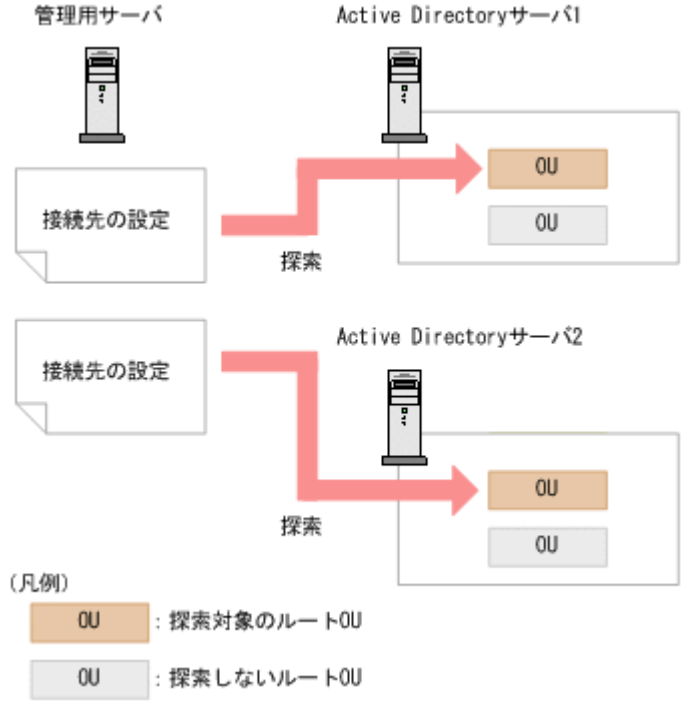
1 台の Active Directory サーバに接続して、複数のルート OU の機器を探索する場合

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。



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

システム情報

機器情報の項目		取得元		
		オブジェクト名（LDAP）	属性名（LDAP）	内容
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。
		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。
	OS サービスパック	computer	operatingSystem ServicePack	OS のサービスパック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。

機器情報の項目		取得元		
		オブジェクト名（LDAP）	属性名（LDAP）	内容
	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）－：該当なし

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。
接続状態	「不明」が設定されます。
機器状態	「不明」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		
	オブジェクト名（LDAP）	属性名（LDAP）	内容
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。

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	○
部署	_※	×
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	×

（凡例）○：テンプレートあり　×：テンプレートなし

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。

「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	×

（凡例）○：テンプレートあり　×：テンプレートなし

「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	×
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	○

項目名	LDAP 属性名	テンプレートの有無
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	○

（凡例）○：テンプレートあり　×：テンプレートなし

「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	○
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	○

項目名	LDAP 属性名	テンプレートの有無
上司 名前	manager	○
直接報告者	directReports	○

（凡例）○：テンプレートあり　×：テンプレートなし

注意 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、動作は保障されません。

(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 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 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 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 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。

注意 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。

参考 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 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。

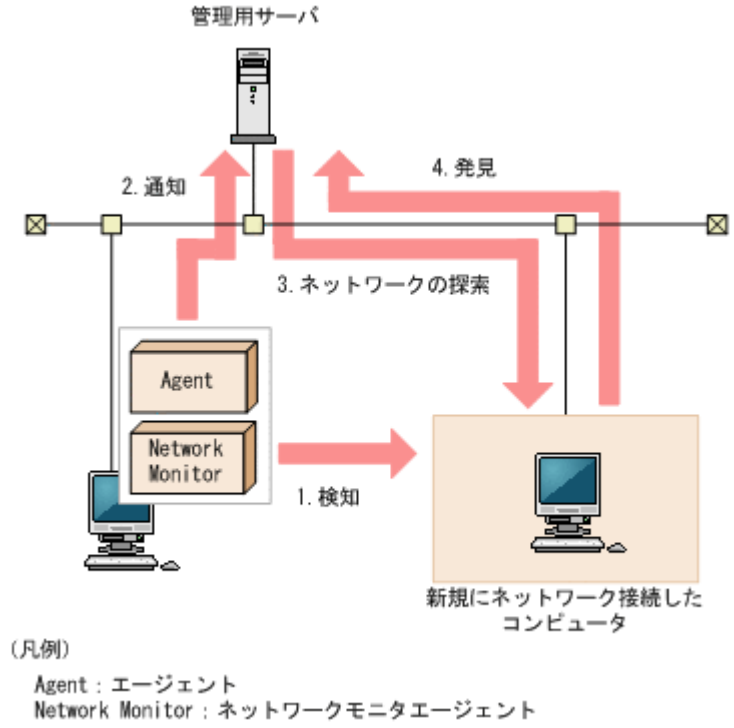
2.4.4 ネットワーク監視機能による機器の検知

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。

注意 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。

参考 機器を検知するためには、一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 に登録する仕組みについて次の図に示します。



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。

参考 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。

注意 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。

注意 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。

参考 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］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。

2.5 エージェントの導入

JP1/IT Desktop Management 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 のすべての機能を利用して効率良く管理できます。

参考 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。

- 管理者がインストールする方法

  次の二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。

参考 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一つ使います。

2.5.1 エージェントの配信

管理用サーバから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二つがあります。

- 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。

なお、サイトサーバを設置している場合、環境に応じてエージェントはサイトサーバからも配信されます。このため、サイトサーバを設置することで、管理用サーバとサイトサーバ間のネットワークの負荷を軽減できます。

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 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。

2.5.2 エージェントを配信するための条件

エージェントを配信するためには、配信先のコンピュータが次の条件を満たす必要があります。

OS

エージェントを配信できるのは、次の表に示す Windows の OS だけです。表にない Windows の OS や、UNIX、Linux、Mac OS のコンピュータには、エージェントは配信できません。

OS	エディション
Windows 7	Ultimate
	Enterprise
	Professional
	Home Premium
	Starter
Windows Server 2008 R2	Datacenter
	Foundation
	Enterprise
	Standard
Windows Server 2008	Enterprise without Hyper-V
	Standard without Hyper-V
	Enterprise
	Standard
Windows Vista	Ultimate
	Enterprise
	Business
	Home Premium
Windows Server 2003 R2	Enterprise x64 Edition
	Standard x64 Edition

OS	エディション
	Enterprise Edition
	Standard Edition
Windows Server 2003	Enterprise x64 Edition
	Standard x64 Edition
	Enterprise Edition
	Standard Edition
Windows XP	Professional（Service Pack 2、3）
Windows 2000	Advanced Server（Service Pack 4）
	Server（Service Pack 4）
	Professional（Service Pack 4）

OS の設定

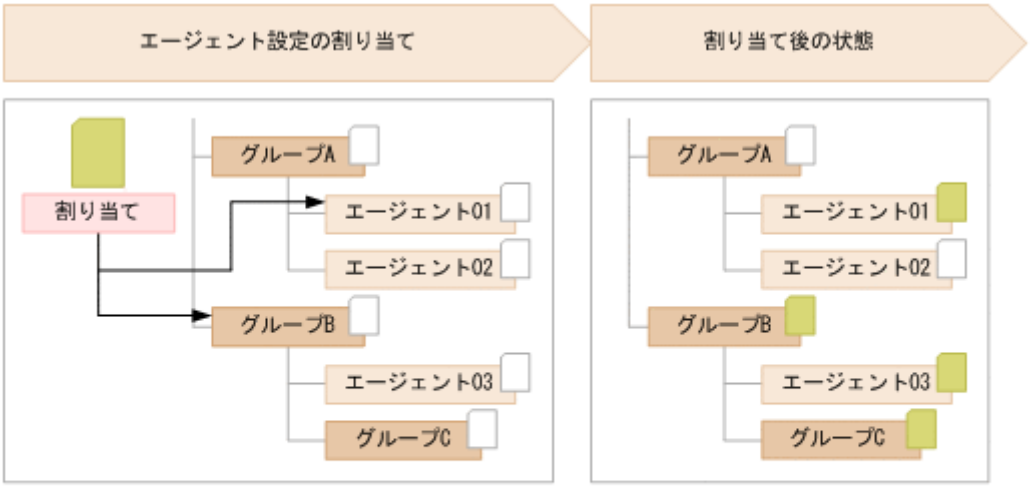
配信先のコンピュータに必要な OS の設定の条件は、エージェントレスでセキュリティ管理をする場合（大部分の機器情報を取得する場合）の、Active Directory を利用しないときの条件と同じです。条件については、「(2) エージェントレスで管理するための条件」の、セキュリティ管理をする場合（大部分の機器情報を取得する場合）にある、Active Directory を利用しないときの条件を参照してください。

2.5.3 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適用されたすべて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、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 XP Professional」にエージェント設定「XP 用設定」を割り当てておくと、Windows XP のコンピュータが管理対象になると自動的に「XP 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。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。



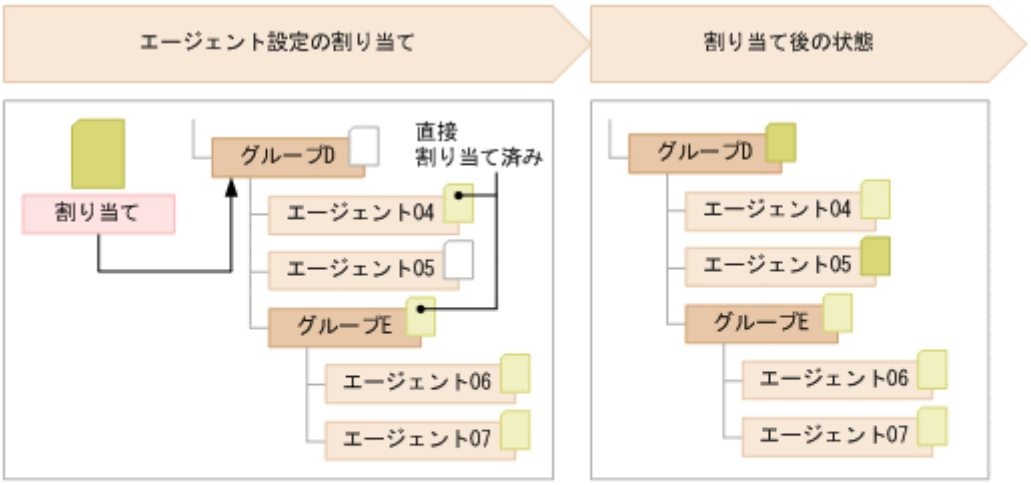
（凡例）

：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」はエージェント導入済み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」はエージェント導入済み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。

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 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

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 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。

参考 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 製品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 製品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。

なお、機器を管理対象にすると、1 台につきライセンスを一つ使います。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。

注意 管理対象にできる機器の上限は、サイトサーバを設置している場合は 10,000 台、サイトサーバを設置していない場合は 3,000 台です。ただし、各サイトサーバが管理できる機器の上限は 1,000 台です。

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

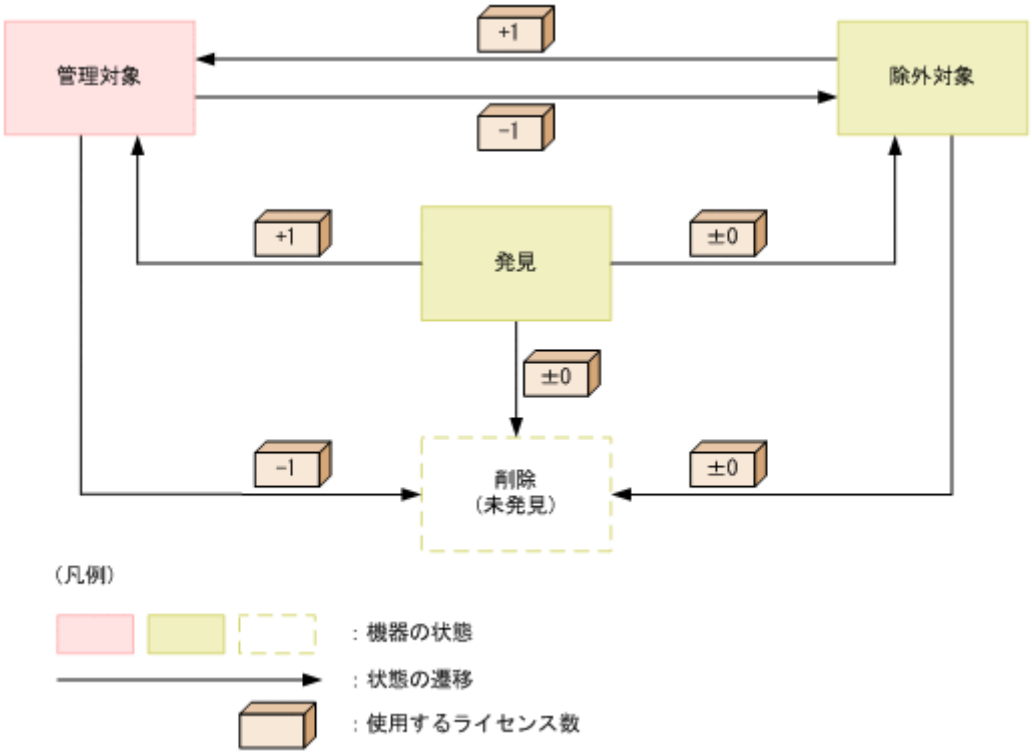
エージェントがインストールされたコンピュータは自動的に管理対象になりますが、探索によって発見された機器は手動で管理対象にする必要があります。

参考 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。

発見された機器は、管理対象または除外対象にできます。JP1/IT Desktop Management 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 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一つ使います。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一つ減ります。

機器の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 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 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、ライセンスを一つ使います。機器を管理対象にすることで、JP1/IT Desktop Management 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 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 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。

参考 除外対象の機器は、探索で発見されなくなります。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 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

(1) 管理対象にできる機器の種類

JP1/IT Desktop Management 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 製品と連携
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
- 2.4.2 ネットワークに接続されている機器の探索

(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。

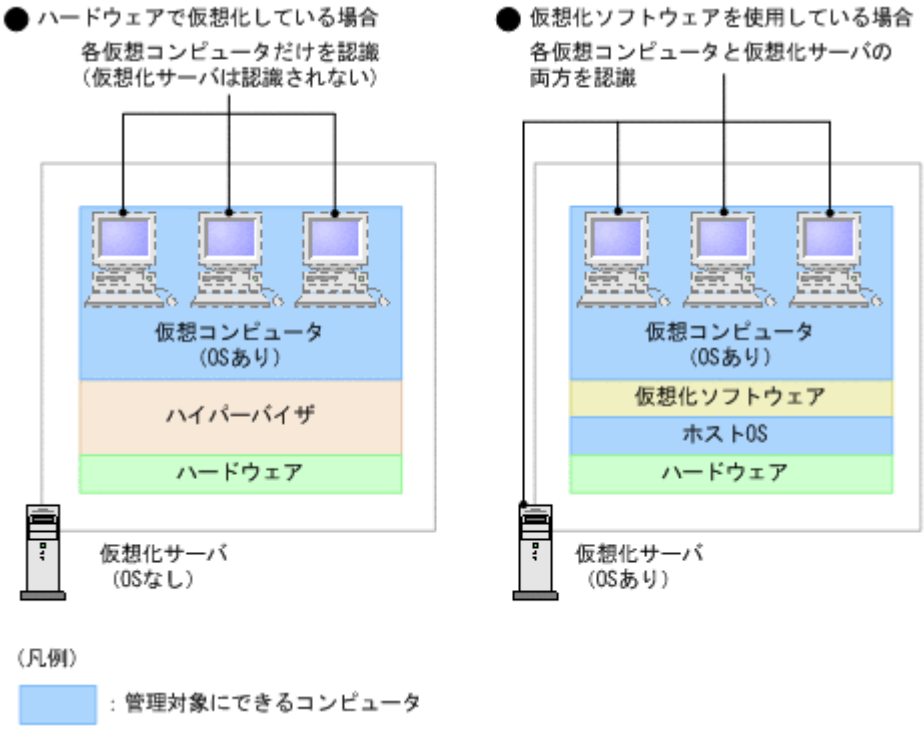
ハードウェアで仮想化している場合

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

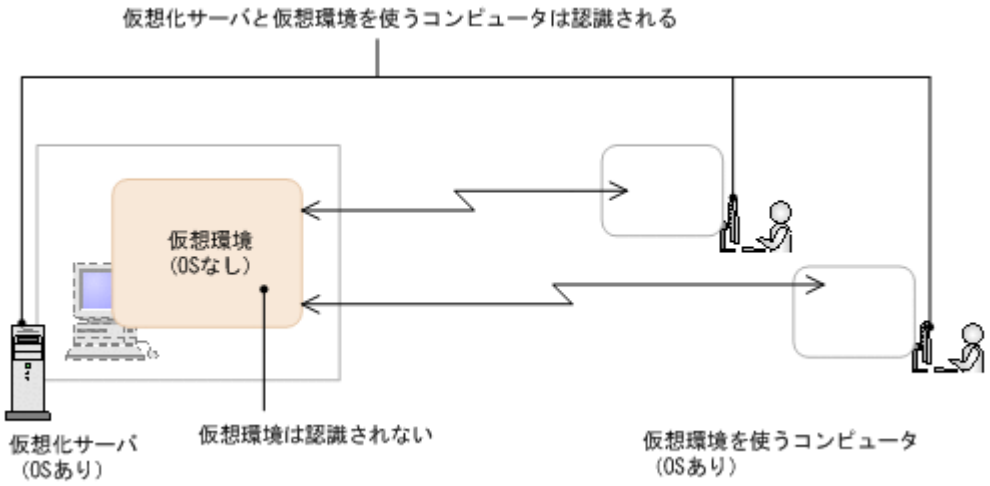
OS 上で仮想化ソフトウェアを使って仮想コンピュータを管理している仮想化サーバでは、各仮想コンピュータと仮想化サーバに OS がインストールされているので、それぞれコンピュータとして管理できます。

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。



また、Citrix XenApp や Windows のターミナルサービスのように、一つの仮想環境を複数のユーザーがリモート接続して使用する環境は、OS を使用していますが個別に OS がインストールされていないので機器として認識されません。

一つの仮想環境を複数のユーザーがリモート接続して使用する環境での仮想コンピュータの扱いを次の図に示します。



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 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、「(6) 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、「(5) 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。

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

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。

利用者の入力による情報を収集する場合、収集する項目を設定したタイミングで利用者のコンピュータ上に入力画面が表示され、利用者が入力した情報を収集できます。定期的に情報を入力してもらうためには、入力画面を表示させるスケジュールを設定してください。

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。

関連リンク

- (5) 情報を収集したいソフトウェアの検索条件の定義

(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「ハードウェア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] の四つに分類されます。

ハードウェア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 製品と連携している。

Windows の管理共有、SNMP、および ARP の認証ができない機器は、ICMP が利用できる場合に存在だけ確認できます。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 製品と連携してスマートデバイスを管理している場合、MDM 製品で管理され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。また、「－」、「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。

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 製品からの収集可否を一覧で説明します。

機器の状態

機器の状態として収集できる情報について次の表に示します。

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
	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。	○	－	－	－	－	－
	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	○	－	－	－	－	－

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
	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（サイトサーバ） エージェント導入済みでかつサイトサーバプログラムがインストールされた状態です。	○	－	－	－	－	－
	エージェント管理（ネットワーク監視用）（サイトサーバ） エージェント導入済みおよびサイトサーバプログラムがインストール済みでかつ、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）（サイトサーバ） エージェント導入済みおよびサイトサーバプログラムがインストール済みでかつ、ネットワークモニタが有効化中の状態です。	○	－	－	－	－	－
	エージェント管理（ネットワーク監視用－有効化失敗）（サイトサーバ） エージェント導入済みおよびサイトサーバプログラムがインストール済みでかつ、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）（サイトサーバ）	○	－	－	－	－	－

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
	エージェント導入済みおよびサイトサーバプログラムがインストール済みでかつ、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）（サイトサーバ） エージェント導入済みおよびサイトサーバプログラムがインストール済みでかつ、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 製品から情報を取得して管理している状態です。	－	－	－	－	－	○

接続状態

アイコン	説明	エージェント導入済み	エージェントレス				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
	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						

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
	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。						

機器状態

アイコン	説明	エージェント導入済み	エージェントレス				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
	稼働中 コンピュータの電源がON の状態です。	○	○	○	×	×	×
	停止中 コンピュータの電源がOFF の状態です。	○ ※1	○	○	×	×	×
	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。	○ ※2	○	○	×	×	×
	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。	×	×	○	×	×	×
	不明 機器の稼働状況が不明な状態です。	×	×	○	○	○	○

（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、「(2) 機器状態の種類と表示条件」を参照してください。

注※1

ネットワークモニタが有効の場合は収集できません。

注※2

ネットワークモニタが無効の場合は収集できません。

システム情報

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
- 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

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
PC	取得した OS 種別が次の場合に設定されます。 ・ 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	○	○	○	×	○	×
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 ・ UNIX ・ 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	×	×	○	×	×	×

機器種別	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
	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 製品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	管理者が入力する場合だけ設定できます。	×	×	×	×	×	×
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	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

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				
				管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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。 コンピュータの説明※1 マイコンピュータのプロパティの［コンピュータ名］	○	○	○ ※2	×	○	○

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
		パネルで設定する［コンピュータの説明］です。						
	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メモリの合計容量です。	○	○	○	×	×	○
	空き容量	ハードディスクの空き容量です。	○	○	×	×	×	×
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（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。 空き容量 ドライブの空き容量です。 容量 ドライブの容量です。 ファイルシステム FAT32、NTFS などのファイルシステムの名称です。	○	○	×	×	×	×
	ディスク名（容量/インターフェース）	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。	○	○	×	×	×	○ ※3
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	○	○	×	×	×	×

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
		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。	○	×	×	×	×	×
電源管理	モニタの電源を切る（AC/DC）※4、※5	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）※4	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）※4	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）※3、※4	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）※1、※4、※5	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　コンピュータの OS が Windows 2000 の場合、収集できません。

注※2　「コンピュータ名」だけ収集できます。

注※3　「容量」だけ収集できます。

注※4　Windows Server 2003、Windows XP、および Windows 2000 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※5　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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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。	○ ※	○ ※	×	×	×	×
説明	最後にログオンしたユーザーの説明です。	○ ※	○ ※	×	×	×	×
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。	○	○	×	×	×	×

（凡例）○：収集できる　×：収集できない

注※　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。

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
OS サービスパック（OS の言語）	OS に適用されているサービスパックおよび 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。	○	○	×	×	○ ※	×
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。	○	○	×	×	×	×
Windows Installer バージョン	Windows Installer 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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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※　OS サービスパック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	エージェントレス				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
IP アドレス/サブネットマスク	IP アドレスおよびサブネットマスクです。	○	○	○	○ ※1、※2	○	×
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	MAC アドレスです。	○	○	○	○ ※2、※3	○	○
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	○	○	×	×	×	×

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
	リース期限日時です。						
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。	○	○	○ ※4	×	×	×

（凡例）○：収集できる　×：収集できない

注※1　「IP アドレス」だけ収集できます。

注※2　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※3　ARP の場合だけ収集できます。

注※4　「ドメイン」だけ収集できます。

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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。	×	×	×	×	×	○
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。	×	×	×	×	×	○
パスコードの設定状況	パスコ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

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

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
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

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
メモリ情報	コンピュータに搭載されているメモリの総容量です。	○	○	×	×	×	×
容量	コンピュータに搭載されているメモリの容量です。	○	○	×	×	×	○
各スロット	メモリスロットに挿入されているメモリの容量です。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。	○	○	×	×	×	×
仮想メモリ容量※	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※　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。ただし、コンピュータの OS が Windows Server 2003（サービスパックなし）、または Windows XP の場合、システム情報の仮想メモリ容量には「ページファイルの合計」だけが表示されます。

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
ハードディスク情報	ハードディスクの台数です。	○	○	×	×	×	×
各ディスク名（容量/インターフェース）	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。	○	○	○ ※1	×	×	○ ※2
各ドライブ（空き容量/容量/ファイルシステム）	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 ドライブの空き容量です。 容量 ドライブの容量です。 ファイルシステム ファイルシステム名です。	○	○	×	×	×	×

（凡例）○：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　「インターフェース」は収集できません。

注※2　「容量」だけ収集できます。

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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

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。

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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

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。

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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。	○	○	×	×	×	×
VRAM 容量	ビデオカードの VRAM 容量です。	○	○	×	×	×	×

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
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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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

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
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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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

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。

［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。

［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。設定画面ー［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。

なお、ソフトウェア検索条件の詳細については、「(5) 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。

［プログラムと機能］に登録されているソフトウェア

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
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。 ソフトウェアがグルーピングされている場合、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。	○	○	×	×	×	×

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
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。	○	○	×	×	×	×
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

［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	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
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。 ソフトウェアがグルーピングされている場合、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	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
OS 情報	コンピュータにインストールされている OS の情報です。	○	○	×	×	×	×

（凡例）○：収集できる　×：収集できない

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

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
Windows 自動更新	Windows 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	適用済み更新プログラムの個数です。	○	○	×	×	×	×
文書番号（適用日付）	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

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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。	△	△	×	×	×	×
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、「(13) 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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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

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				
				管理共有	SNMP	ARP/ICMP	Active Directory	MDM
アカウント情報	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、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※	パスワードの安全性の高さです。 Windows のローカルセキュリティポリシー（ローカル環境およびドメイン環境）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（成功または失敗）にしている場合、パスワードの安全性を判定するときに、イベントログが出力されます。	○	○	×	×	×	×
	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		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		Windows 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。	○	○	×	×	×	×
DCOM		DCOM 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				
				管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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	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。	○	○	×	×	×	×
	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。	○	○	×	×	×	×
	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。	○	○	×	×	×	×
	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。	○	○	×	×	×	×
Windows ファイアウォール		Windows 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※　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、またはロック状態の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。

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				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
製品名	インストールされている製品の正式名称です。	○	×	×	×	×	×

項目	説明	エージェント導入済み	エージェントレス				
			管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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。	○	×	×	×	×	×
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。	○	×	×	×	×	×
ログイン日時	最後に秘文製品にログインした日時です。	○	×	×	×	×	×
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。	○	×	×	×	×	×
ドライブ	ローカルドライブです。	○	×	×	×	×	×
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

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。

ハードウェア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				
				管理共有	SNMP	ARP/ICMP	Active Directory	MDM
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	○	×	×	×	○	×
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。

(2) 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	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。
警告	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。 • サイトサーバのサービスが停止している。 • ネットワークモニタエージェントが停止している。 • 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	機器の状態に関する情報を収集できない。

注

サイトサーバや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。

a. 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）。

b. 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＞サイトサーバ（操作ログの保管＞配布機能の中継））。

(3) 機器情報の収集タイミング

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。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※1		すべての機器情報※2	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※3	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）※4
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）※5
セキュリティ情報	Windows 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）

検知項目		通知情報	監視間隔
	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）
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　ホスト識別子とは、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。

注※2　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※3　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※4　「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※5　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。

(4)　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。

参考　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 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。

ソフトウェア情報には次の 3 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、「(1) 収集できる機器情報の種類」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

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。

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。

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、「(5) 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。
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	インストールするソフトウェア情報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。

(5) 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

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。

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。

(6) 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 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。

ハードウェア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。

利用者情報は、取得する項目を任意に作成できます。また、スケジュールを設定して定期的に取得することもできます。

なお、コンピュータの OS によって、利用者情報の入力画面を表示できるユーザーが異なります。OS ごとの利用者情報の入力画面を表示できるユーザーを次の表に示します。

OS	利用者情報の入力画面を表示できるユーザー
Windows Server 2008	• ローカルコンソールにログオンしたユーザー • リモートセッションで最初にログオンしたユーザー
Windows Server 2003	• ローカルコンソールにログオンしたユーザー • リモートセッションで最初にログオンしたユーザー • リモートデスクトップ接続でコンソールセッションに接続したユーザー
Windows 2000 Server	• ローカルコンソールにログオンしたユーザー • リモートセッションで最初にログオンしたユーザー
Windows 7	全ログオンユーザー
Windows Vista	
Windows XP	
Windows 2000 Professional	

(7) 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。

注※2　コンピュータの OS が Windows Server 2003、Windows XP、または Windows 2000 の場合は取得されません。

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

注※　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。

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
	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。ホスト識別子とは、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。

参考 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。

(9)　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
- 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

参考 機器画面でそれぞれの機器の［更新日時］を見ると、機器情報の取得がいつ行われたかを確認できます。また、機器一覧を［更新日時］でフィルタリングすると、管理対象の機器の変化を監視することもできます。

(10)　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	Windows 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。
	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。

機器情報の項目		事象	イベント発行の契機
	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 Windows 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。

(11) 管理対象のコンピュータがオフラインになった場合の動作

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（オフラインになった）場合、オンライン接続の場合と同様に、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、エージェント導入済み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。

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 が情報を取得できるまでは、オフラインになる直前の情報が保持されます。

オフラインのエージェント導入済みコンピュータの動作

オフラインになった場合でも、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。
- USB 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、コンピュータの稼働時間で最大 1,000 時間分が保存されます。

参考 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。

再度オンラインにしたときの動作

オフラインのコンピュータを再度オンラインにした場合は、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、オフライン中に、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、通常 1 時間に 1 回の周期で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。再度オンラインにした場合は、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

管理用サーバには、すべてのセキュリティ判定項目について、オフラインになる直前の情報がデータベースに保持されています。そのため、コンピュータがオフラインの間は、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。

(12) グループの自動作成

機器画面の［機器情報］画面と資産画面の［ハードウェア資産］画面では、収集した機器情報に応じて自動的にグループが作成されます。また、各機器およびハードウェア資産の情報は、自動的に対応するグループに登録されます。

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生成されます。

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は、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 で機器情報を収集する場合、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は、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。

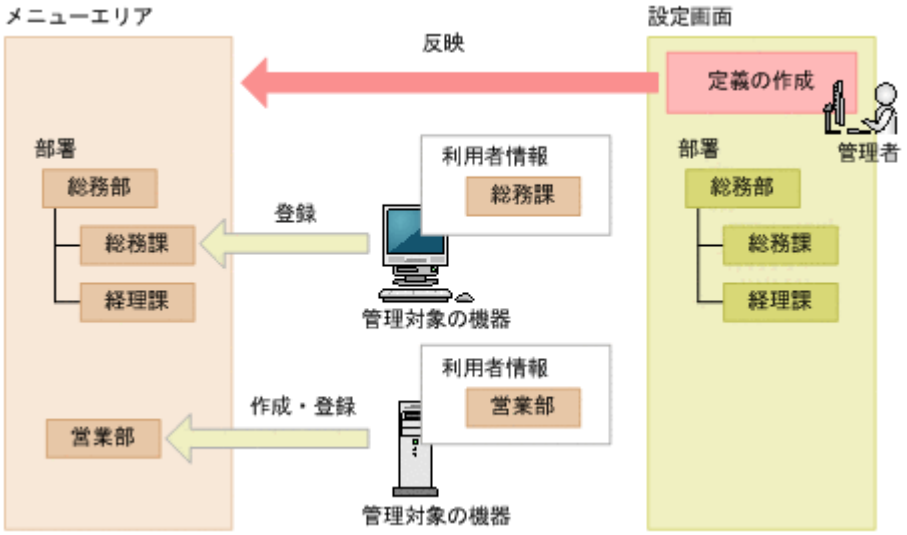
関連リンク

- 2.4.3 Active Directory との連携

(13) 部署・設置場所のグループを定義する仕組み

機器の利用者情報のうち、部署および設置場所は、設定画面からグループを定義して管理できます。

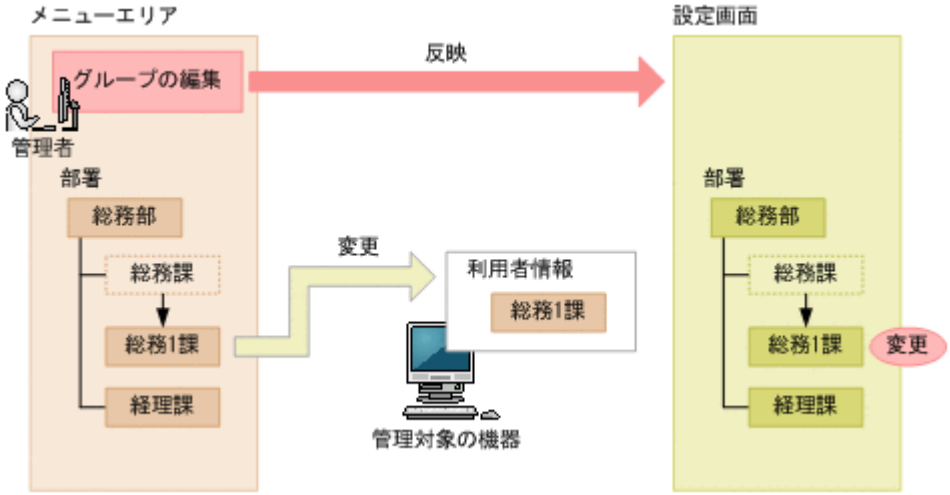
部署・設置場所の定義を作成すると、資産画面や機器画面のメニューエリアに反映されます。管理対象の機器は、利用者情報（実態）に設定されたグループ名に基づいて、メニューエリアのグループに登録されます。なお、定義が存在しないグループ名が利用者情報に設定された場合は、実態に基づいてメニューエリアにグループが作成されます。



グループの定義は、メニューエリアと設定画面の両方で編集できます。ただし、それぞれで操作した場合の影響が異なります。それぞれについて説明します。

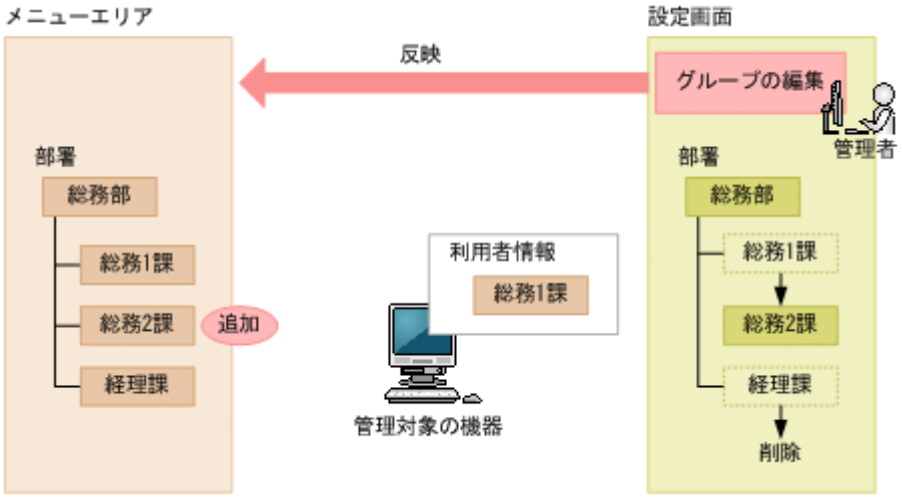
メニューエリアから編集した場合

メニューエリアからは、グループ名の変更とグループの削除ができます。メニューエリアからグループを編集した場合、定義に加えて、そのグループに登録されている機器の利用者情報も変更されます。



設定画面から編集した場合

設定画面からは、グループの追加、削除、グループ名の変更、構成変更（階層定義の場合）ができます。設定画面からグループを編集した場合は、定義だけが対象となり、機器の利用者情報は変更されません。グループの追加、グループ名の変更、構成変更をした場合は、変更後のグループがメニューエリアに追加され、変更前のグループは残ったままとなります。また、グループを削除した場合も、削除前のグループは残ったままとなります。



参考 グループの定義には、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、利用者情報を編集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。

(14) 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。

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。

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。

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。

(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。

注意 無線 LAN 環境の場合、コンピュータの電源を ON にできません。

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。
- AMT で使用する 16992 ポートで通信できる。

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。

参考 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。

参考 AMT のユーザー ID とパスワードは管理用サーバに一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。

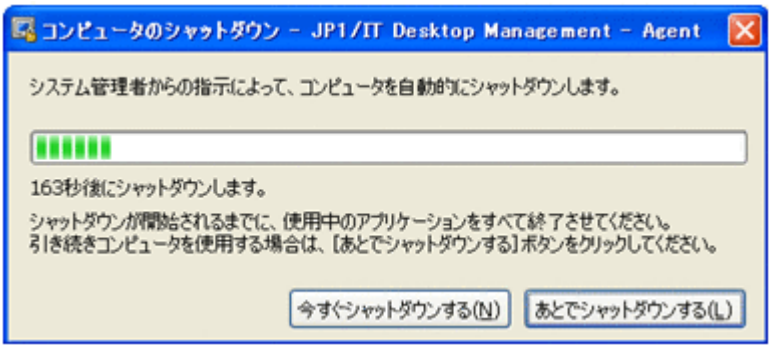
管理用サーバ側の条件

特になし。

コンピュータ側の条件

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。ただし、次に示す状態の場合はシャットダウンされません。

- パスワードで保護されたスクリーンセーバーが起動している場合
- コンピュータがロックされている場合
- 編集中のファイルが存在する場合

なお、コンピュータが OS にログオンする前の状態のときは、［コンピュータのシャットダウン］ダイアログは表示されないでシャットダウンされます。

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。

管理用サーバ側の条件

特になし。

コンピュータ側の条件

エージェントがインストールされている。

コンピュータを再起動する場合、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。

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 秒後に自動で再起動されます。ただし、次に示す状態の場合は再起動されません。

- パスワードで保護されたスクリーンセーバーが起動している場合
- コンピュータがロックされている場合
- 編集中のファイルが存在する場合

なお、コンピュータが OS にログオンする前の状態のときは、［コンピュータの再起動］ダイアログは表示されないで再起動されます。

(2) AMT を利用するための前提条件

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。	2.0 以降
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。	6.0 以降
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 以降
	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 以降

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。

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。

AMT を利用してコンピュータの電源を制御する、および 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。

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。また、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も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、および IDE リダイレクションを利用する場合

コンピュータの AMT でリモート KVM 機能と 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。

設定画面ー［エージェント設定］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］および［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］ー［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。また、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。

関連リンク

- (1) 電源制御の条件

2.6.4 エージェントレスでの管理

JP1/IT Desktop Management 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 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。

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と SNMP を利用する方法の 2 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

参考 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。

注意 OS が Windows XP Home Edition（Service Pack 2、3）の場合は、管理共有が使用できません。

注意 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。

なお、Windows の管理共有または SNMP 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、「(2) エージェントレスで管理するための条件」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) エージェントの有無による機能差異」を参照してください。

(1) エージェントの有無による機能差異

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。

エージェントの有無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
機器情報の収集※1		○	△
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	○	△ ※2
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 および OFF	○	×
資産情報の管理	ハードウェアの管理	○	△
	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	○	○
ソフトウェアまたはファイル配布の管理	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	○	○ ※3

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
	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　△：収集できる機器情報に依存する　×：対象外

注※1　エージェントの有無によって、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、「(1) 収集できる機器情報の種類」を参照してください。

注※2　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※3　RFB で接続した場合だけ、コンピュータを操作できます。

(2)　エージェントレスで管理するための条件

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。

注意 NAT 環境では、エージェントレスの機器は管理できません。

注意 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、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。
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。

セキュリティ管理をする場合（大部分の機器情報を取得する場合）

利用者のコンピュータで、次の条件をすべて満たしている必要があります。

- Windows ファイアウォールが無効になっている。※
- 簡易ファイル共有が無効になっている。
- ファイルとプリンタの共有が有効になっている。
- Windows の管理共有（ADMIN$）が有効になっている。
- プロセス間通信用共有（IPC$）が有効になっている。

注※　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。

また、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必要もあります。ただし、OS が Windows Vista または Windows Server 2008 の場合、UAC（ユーザーアカウント制御）の認証なしにログオンできるようにしてください。

なお、Windows の管理共有を有効にして機器情報を取得するためには次の表に示すような設定が必要です。

OS	設定内容
Windows 7	UAC の無効化
Windows Vista	・　共有ウィザードの無効化 ・　Administrator ユーザーの有効化
Windows XP	・　簡易ファイル共有の無効化 ・　ファイル共有の追加
Windows Server 2008	ネットワークと共有センターで［ファイル共有］と［プリンタ共有］を有効にする。
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）

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。

機器管理だけをする場合（一部の機器情報を取得する場合）

Active Directory を利用するとき

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。※
- 管理用サーバで、Active Directory を探索して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。

SNMP を利用するとき

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 7	・　SNMP エージェントの導入 ・　SNMP エージェントの設定
Windows Vista	
Windows XP	
Windows Server 2008	
Windows Server 2003	
Windows 2000	
Windows 以外のコンピュータ	

OS	設定内容
ネットワーク装置	

これらの条件を満たしている場合、機器種別やコンピュータ名などの一部の機器情報を取得できます。セキュリティ管理が不要な場合は、こちらの方法で機器を管理できます。

機器の存在を確認する場合

ICMP を利用して、機器の存在を確認します。

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 7	ICMP エコー要求の着信許可※
Windows Vista	
Windows XP	
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

(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。例えば、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。

参考 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。

注意 機器の IP アドレスが含まれる探索範囲が削除されてしまうと、機器情報が収集できなくなります。このため、エージェントレスで機器を管理する場合は、その機器の IP アドレスが含まれる探索範囲は削除しないでください。

(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セキュリティ管理できる機器収集されます。

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。

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、ネットワークの探索時の情報収集だけに利用されます。

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	○	○	○
ARP	○	○	○
ICMP	○	○	○

（凡例）○：利用できる　×：利用できない

エージェントレスの機器から収集できる機器情報を次の表に示します。

機器情報		機器の種類		
		Windows のコンピュータ	Windows 以外のコンピュータ	ネットワーク機器
システム情報	機器種別	○	○	○

機器情報		機器の種類		
		Windows のコンピュータ	Windows 以外のコンピュータ	ネットワーク機器
	コンピュータ情報	○	△（「コンピュータ名」、「ホスト名」だけ）	×
	OS 情報	○	△（「OS」だけ）	×
	ネットワーク情報	○	△（「IP アドレス」、「MAC アドレス」、「サブネットマスク」、「デフォルトゲートウェイ」、「ネットワークアダプタ」だけ）	△（「IP アドレス」、「MAC アドレス」、「サブネットマスク」、「デフォルトゲートウェイ」、「ネットワークアダプタ」だけ）
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		○	×	×

（凡例）○：収集できる　△：一部収集できる　×：収集できない

注※　エージェントレスの場合、［プログラムと機能］に登録されているソフトウェアの情報だけ取得できます。

参考 エージェントレスの機器から収集できる機器情報の詳細については、「(1) 収集できる機器情報の種類」を参照してください。

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、機器情報は定期的に収集されます。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。

任意のタイミングでの収集はできません。

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。

注意 エージェントレスの機器の台数が多い場合、設定した更新間隔以内に情報収集が完了しないことがあります。情報収集の間隔は、エージェントレスの機器 1,000 台ごとに 1 時間の間隔を設定してください。 例えば、エージェントレスの機器が 1,500 台ある場合は、2 時間ごとに更新されるように設定します。 なお、エージェントレスの機器の情報収集に掛かっている時間は、JDNMAINn.log に出力されるメッセージ（KDEX5020-I および KDEX5021-I）に表示される時刻の差分から確認できます。

関連リンク

- (5) 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)　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。

注意 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。

参考 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。

2.6.5 MDM 製品との連携

MDM 製品と連携すると、MDM 製品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 の管理対象にできます。取得した情報を JP1/IT Desktop Management で管理したり、スマートデバイスを JP1/IT Desktop Management から制御したりできます。

MDM 製品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 製品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 の管理対象にできます。また、MDM 製品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 製品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

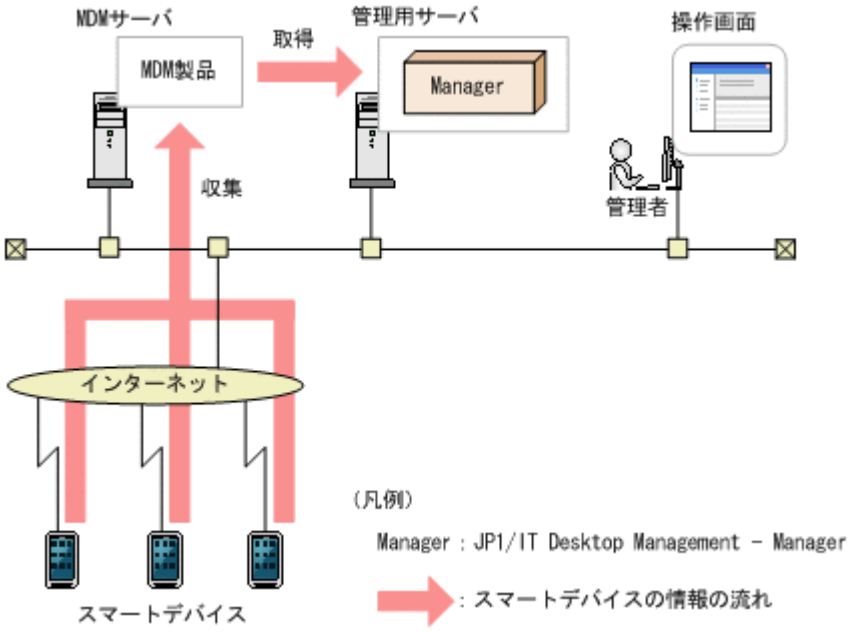
- (1) MDM 製品で管理されているスマートデバイスの情報の取得
- (2) MDM 製品から取得できる機器情報
- (3) MDM 連携時の注意事項
- 2.21 スマートデバイスの制御

(1) MDM 製品で管理されているスマートデバイスの情報の取得

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。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 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。

参考 スマートデバイスを JP1/IT Desktop Management 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 製品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 製品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 製品に接続して、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 製品での情報の変更をすぐに JP1/IT Desktop Management 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、毎日 23:30 です。

参考 MDM 製品上でスマートデバイスを削除した場合、JP1/IT Desktop Management の機器情報とは同期しません。MDM 製品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 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 製品から取得できる機器情報

MDM 製品から取得できる機器情報を次の表に示します。機器情報の詳細については、「(1) 収集できる機器情報の種類」を参照してください。

システム情報

機器情報の項目		取得元	
		MDM 製品（MobileIron）での項目名	内容
機器種別		－	「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）	－	MDM 製品でスマートデバイスを識別するために表示しているユーザー名、契約電話番号、およびモデル名が取得されます。
	モデル（メーカー）	－	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。

機器情報の項目		取得元	
		MDM 製品（MobileIron）での項目名	内容
	シリアルナンバー	－	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	－	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。
システムドライブ	容量	－	ハードディスク全体の容量が取得されます。
OS 情報	OS	• os • OS version	OS の名称が取得されます。
ネットワーク情報	MAC アドレス	－	MAC アドレスが取得されます。
スマートデバイス情報	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	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	imsi	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	－	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。
	契約電話番号	• number • phone 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	user email	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。
	キャリア	currant_operator_name	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	－	スマートデバイスにパスコ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）	• 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）	• total_strage_size_bytes • free_strage_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）	• 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。

（凡例）－：該当なし

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 製品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。
最終接続確認日時	スマートデバイスが MDM 製品に接続したときの日時が設定されます。

(3) MDM 連携時の注意事項

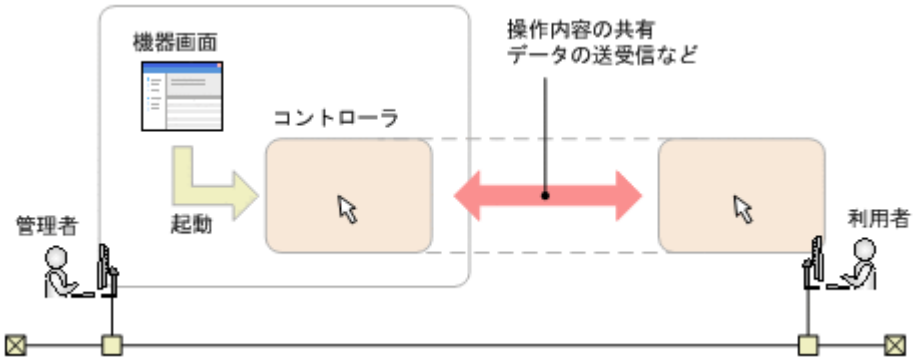
MDM 製品と連携する場合の注意事項を次に示します。

- MDM サーバのホスト名に、「_」は使用できません。ホスト名に「_」を使用している場合は、接続先の MDM サーバを IP アドレスで指定してください。
- 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 製品ごとに異なります。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。

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 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。

画面を呼び出す側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 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。

参考 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

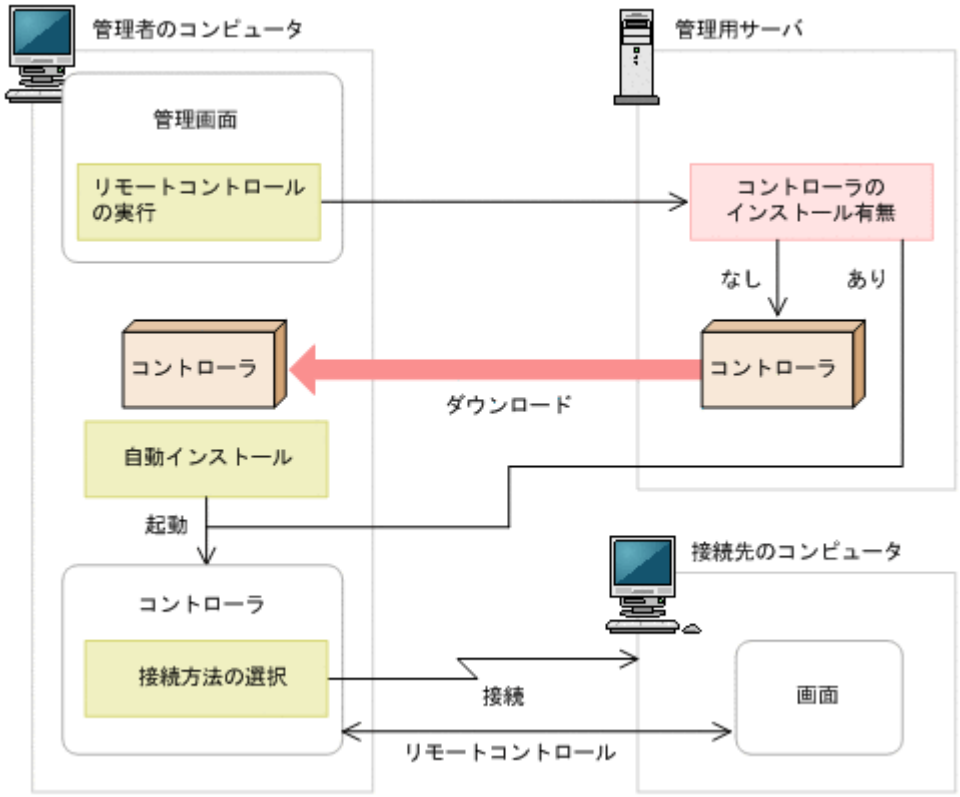
RFB プロトコルを利用してコンピュータに接続する方法です。AMT や VNC サーバ機能を利用できるソフトウェアなどによって、リモートコントロールを実現します。Windows にログオンできないコンピュータや、OS が Linux や Mac OS のエージェントレスのコンピュータに対して接続する場合は、こちらを利用してください。なお、RFB で接続する場合はリモートコントロールで使用できる機能に制限があります。

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 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 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、「2.7.13 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、「2.7.14 ファイルの転送」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 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、「2.7.16 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、「2.7.15 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、「2.7.17 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、「2.7.18 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 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、	• 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	○	○

機能		説明	機能有無	
			標準	RFB
	再生、ファイル形式変換	• 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	○	○
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 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 のバージョンアップなど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。

注意 次の場合、コントローラの自動更新は実施されません。

- 使用している Web ブラウザが Internet Explorer 6 の場合。
- プロキシサーバを介して JP1/IT Desktop Management 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 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、「監視モード」、「共有モード」、「制御モード」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。

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。

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可能性がある場合は、このモードで接続してください。

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。

注意 RFB で接続している場合、制御モードは利用できません。

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。

エージェント設定のモード	コントローラのモード	接続時のモード
監視モード	監視モード	監視モード
	共有モード	
	制御モード	

エージェント設定のモード	コントローラのモード	接続時のモード
共有モード	監視モード	監視モード
	共有モード	共有モード
	制御モード	
制御モード	監視モード	監視モード
	共有モード	共有モード
	制御モード	制御モード

エージェント設定が「監視モード」の場合

コントローラがどのモードに設定されていても、監視モードで接続されます。

エージェント設定が「共有モード」の場合

コントローラが監視モードの場合は、監視モードで接続されます。それ以外のモードの場合は、共有モードで接続されます。

エージェント設定が「制御モード」の場合

コントローラ側で設定したモードで接続されます。

(1) コンピュータ側からの制御モードの変更

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、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。

参考 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) 複数接続時の接続モード

複数のコントローラが一つ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一つだけです。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。

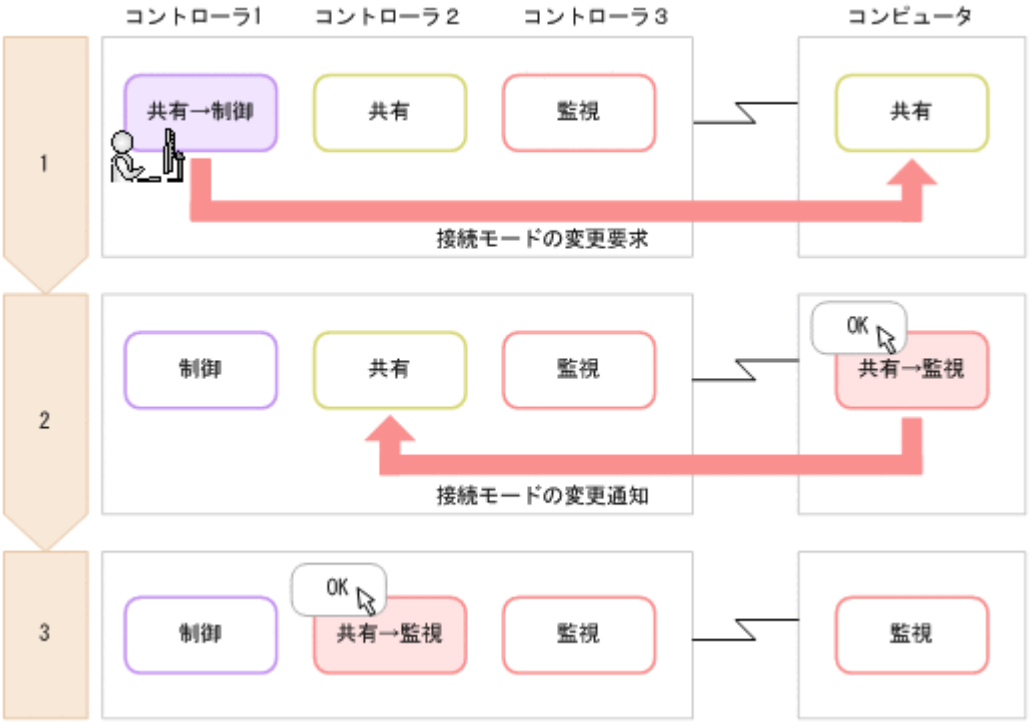
以降では、複数接続時の接続モードの変化について例を示します。

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

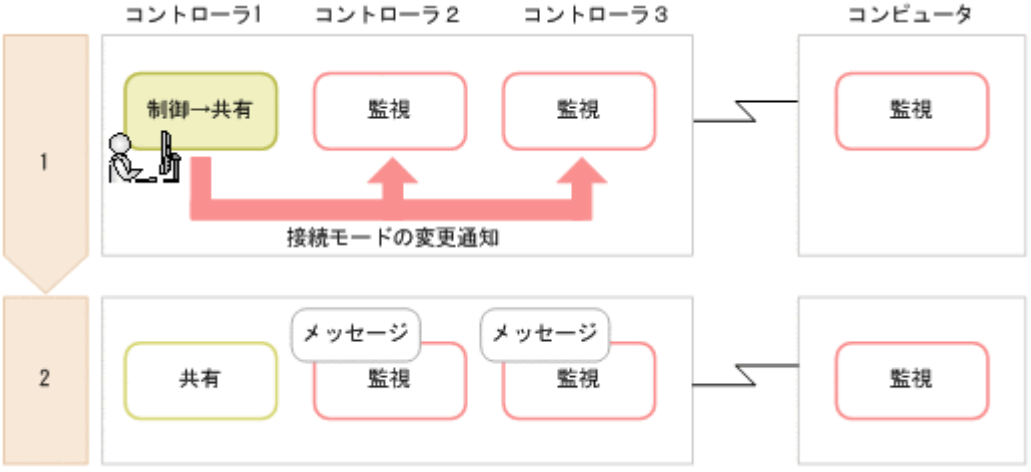
初期状態から、コントローラ 1 を制御モードに変更した場合、その他のコンピュータのモードは次のように変化します。



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、その他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。

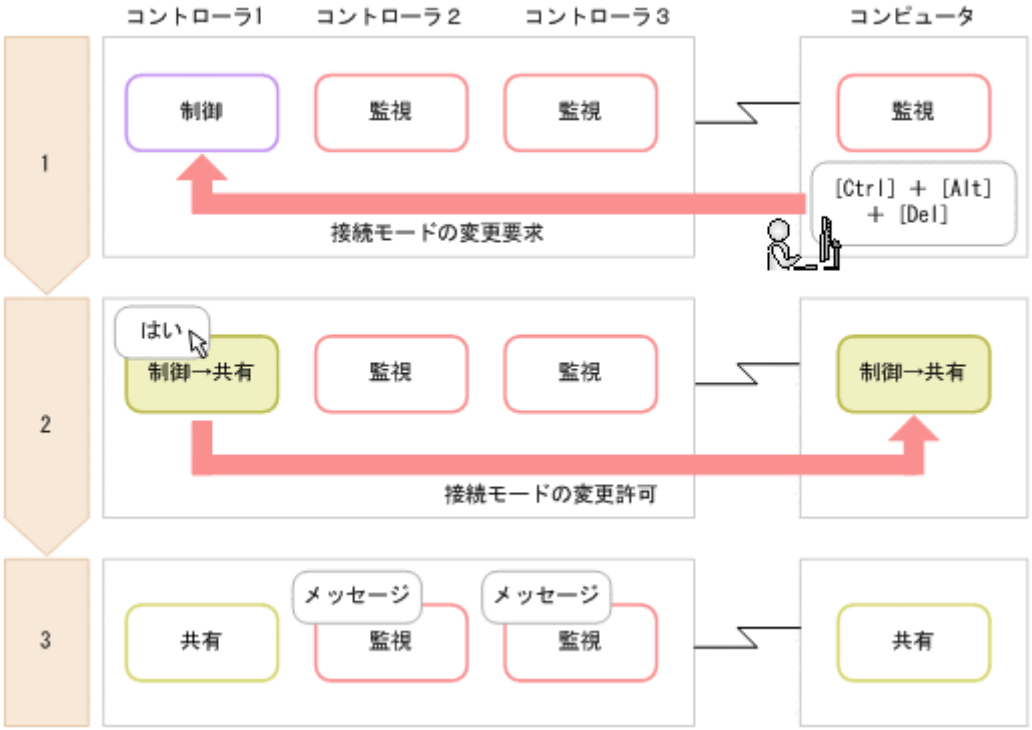


1. コントローラ 1 を共有モードに変更します。

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、その他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 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。	×

項目	表示内容	デフォルト表示
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 環境および DHCP 環境でのリモートコントロールについて説明します。

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

- 2.7.15 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と、Windows のユーザー権限の設定方法について説明します。

必要なユーザー権限

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。
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	
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。

ユーザー権限の設定方法

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。

ローカルコンピュータの場合

a. ［コントロールパネル］で［管理ツール］を選択します。
b. ［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。
c. 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。
d. ［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。
e. 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、またはサーバの場合

a. 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。
b. 「mmc」と入力して［OK］ボタンをクリックします。
c. 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。
d. ［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。

e. ［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。

f. 変更するグループポリシーオブジェクトを設定します。

g. 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。

h. ［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。

i. 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の場合

a. 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。

b. ［Active Directory ユーザーとコンピュータ］をダブルクリックします。

c. 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。

d. ［プロパティ］－［グループ ポリシー］タブを選択します。

e. 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。

f. ［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。

g. ［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。

h. 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の場合

a. 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。

b. ［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。

c. 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。

d. ［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。

e. 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。

2.7.11 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。

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。

2.7.12 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セキュリティの設定］－［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。

参考 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。

参考 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

- 2.7.16 接続先の管理

2.7.13 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。

参考 コントローラは、マルチディスプレイ環境のコンピュータも操作できます。

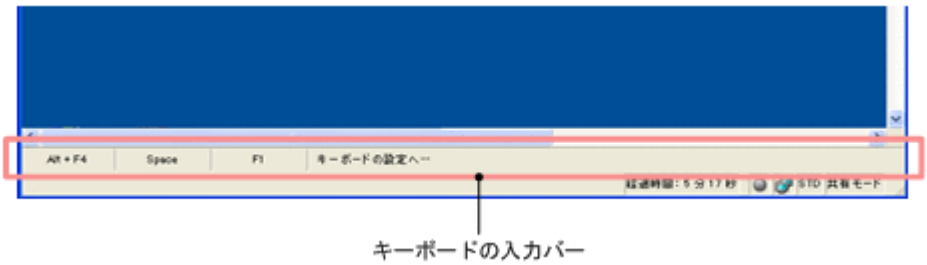
関連リンク

- (1) 特殊キーの登録と入力
- (3) クリップボードのデータの転送

(1) 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。

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。



参考 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) デフォルトで提供されている特殊キー
- (3) クリップボードのデータの転送

(2) デフォルトで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) 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。

参考 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。

参考 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。

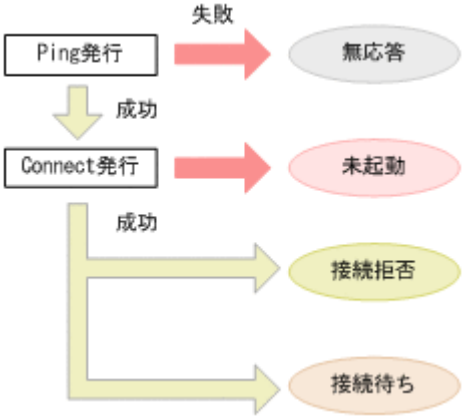
(4) 検索範囲の指定方法

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 5 とおりの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（-）で区切って二つ指定する。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) 検索された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) 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動作設定、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。

アイコン画像	アイコン名	説明
		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 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。

  a. Windows の［コントロールパネル］－［マウス］をクリックします。
  b. ［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。
  c. ［デザイン］に［(なし)］を選択します。
  d. ［OK］ボタンをクリックします。

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 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。

注意 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。

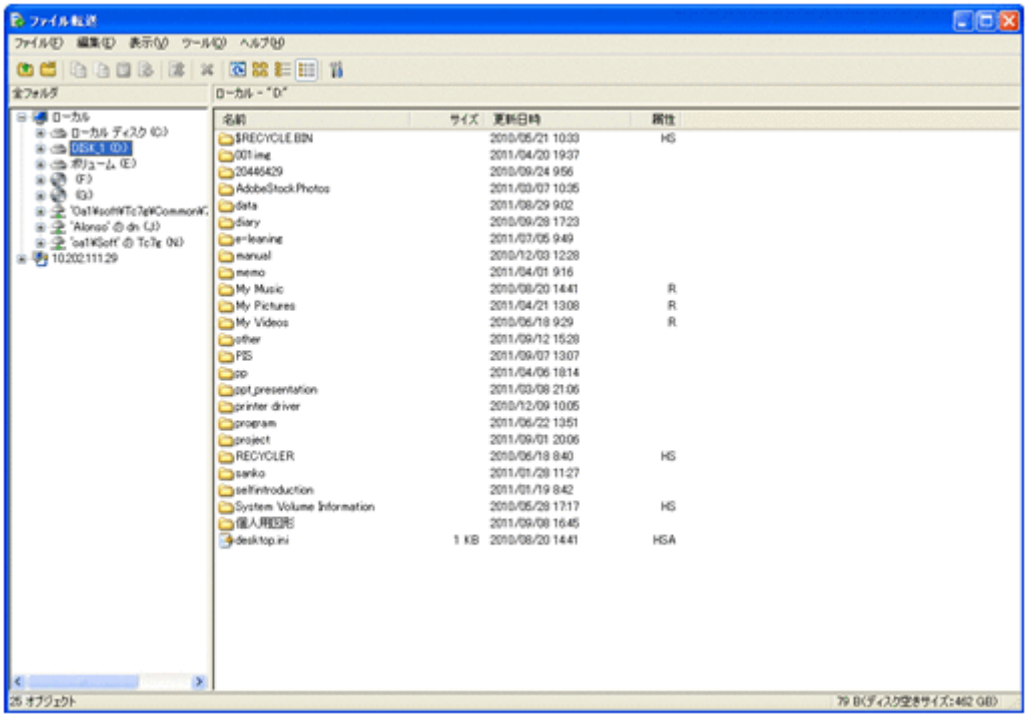
2.7.14 ファイルの転送

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。

注意 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動作］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。

参考 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。

(1) ファイルの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) 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。

2.7.15 接続先のコンピュータからコントローラへの接続要求

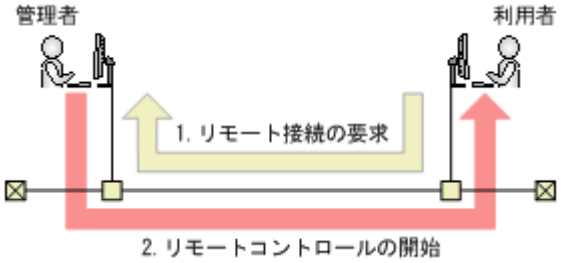
管理者のコンピュータから利用者のコンピュータを参照できない NAT 環境や NAPT 環境の場合、コントローラ側からコンピュータを参照できません。また、機器の IP アドレスが変わってしまう DHCP 環境では、コントローラから IP アドレスを指定して目的のコンピュータに接続するには、毎回 IP アドレスを調べる必要があるため非常に手間が掛かります。

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。

注意 コントローラへの接続要求は、エージェント導入済み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。



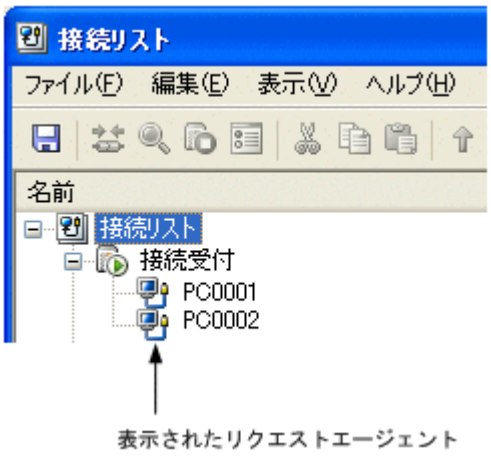
利用者からの接続要求を受信するには、接続リスト上でリクエストサーバを開始する必要があります。リクエストサーバ開始後、利用者からリモート接続の要求を受信すると（図中：1）、利用者のコンピュータが接続リストにアイコン表示されます。このアイコンをダブルクリックすることでリモートコントロールを開始できます（図中：2）。

関連リンク

- (1) 接続要求の受信

(1) 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。

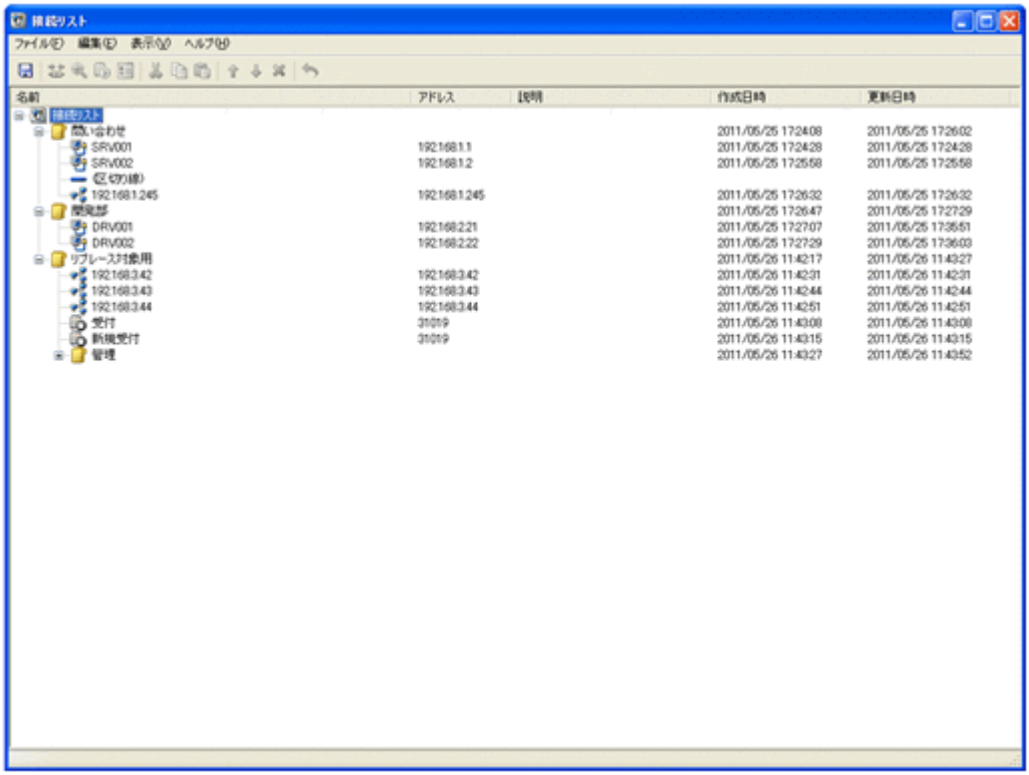
注意 リクエストエージェントは、接続要求を出したエージェントが一時的に表示されたもので、このままでは情報として保存されません（接続リストを閉じると削除されます）。接続要求を出したエージェントの情報を保存したい場合は、ドラッグ&ドロップでアイコンを任意のグループに移動してください。フォルダ下に移動することで、接続リスト上の 1 アイテムとして保存できます。また、通常のコンピュータとして扱えるようになり、名前や説明を変更できます。

2.7.16 接続先の管理

接続先のコンピュータを、JP1/IT Desktop Management 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) コンピュータごとの接続環境の設定

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。

参考 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) コンピュータのパスの記録

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

2.7.17 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) 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

参考 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) 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（AgentName.jcr)」を選択した場合
  （例）10.xxx.xxx.4.jcr
- 「記録ファイル（AgentName Date Time.jcr)」を選択した場合
  （例）10.xxx.xxx.4 2011-04-01 150545.jcr
- 「記録ファイル（Date Time AgentName.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、ログの取得を開始する］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) 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動作設定］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 - 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。

参考  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。

参考 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。

2.7.18 チャットの利用

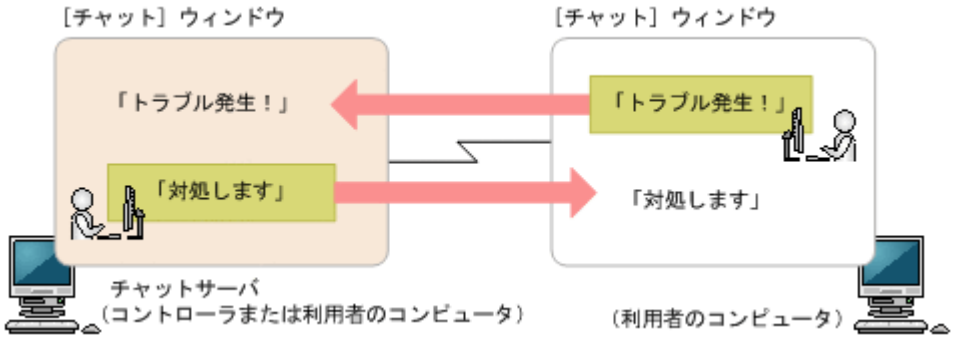
標準接続でリモートコントロール中に利用者と連絡を取る場合、手もとに電話がない環境では、チャットを利用することで利用者と対話できます。チャットはテキストデータで対話するため、IP アドレスや URL などの情報を文字でリアルタイムに連絡したい場合にも便利です。

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。

注意 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。

参考 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。

2.7.19 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。
	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。

メニューバー	メニュー項目		機能
		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。
	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。
エージェント	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。

メニュー項目	機能
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、一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。

メニューバー	メニュー項目	機能
	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。
	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。

メニューバー	メニュー項目		機能
	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		選択した項目を一つ上に移動します。
	下の項目に移動		選択した項目を一つ下に移動します。
	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。

メニューバー	メニュー項目		機能
		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

メニューバー	メニュー項目		機能
			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) 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。

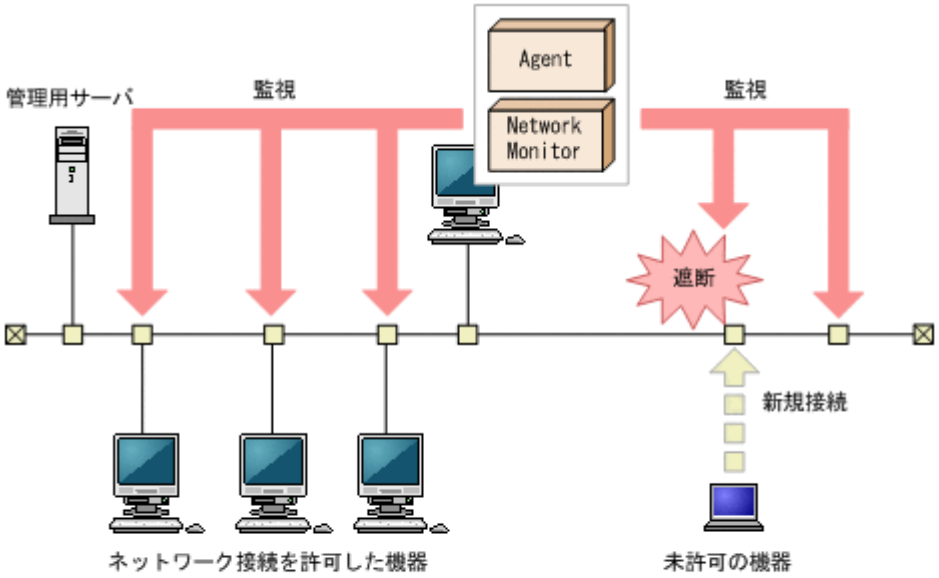
メニューに表示される項目を次の表に示します。

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。
	スクリーンから―	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：エージェント

Network Monitor：ネットワークモニタエージェント

なお、管理用サーバ、サイトサーバ、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。

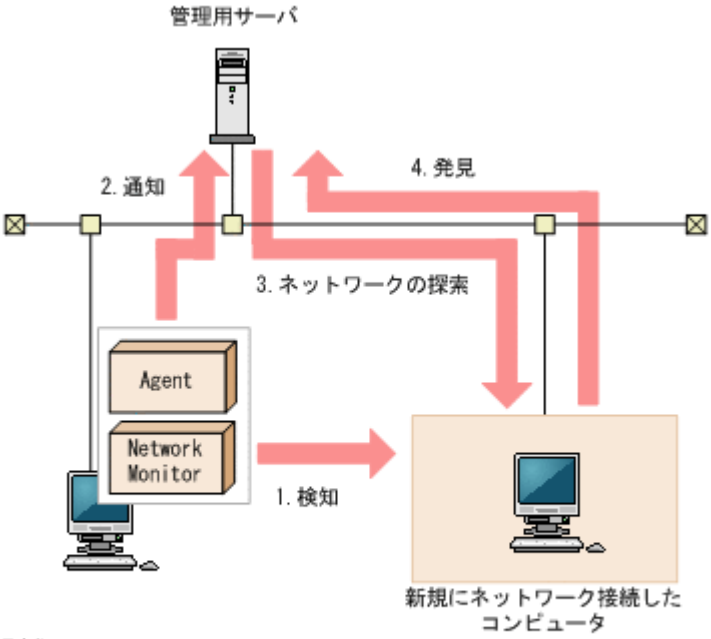
2.8.1 ネットワーク監視機能による機器の検知

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。

注意 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。

参考 機器を検知するためには、一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 に登録する仕組みについて次の図に示します。



（凡例）

Agent：エージェント
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。

参考 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。

注意 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。

注意 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。

参考 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］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。

2.8.2 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。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。

参考 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二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。

参考 管理用サーバ、サイトサーバ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。

参考 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。

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）

遮断された機器の特例設定

ネットワーク接続が遮断された機器でも、特定の機器と通信できるように設定できます。遮断中の機器の通信については、「2.8.11 遮断中に接続できる機器の登録」を参照してください。

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 アドレスを変更したり、監視するネットワークを追加したりした場合、一度ネットワークモニタを無効にしないと、最新の情報が適用されません。［ネットワークモニタ設定の割り当て］画面で一度ネットワークモニタを無効にしたあと、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は、Windows ファイアウォールが無効になります。また、セキュリティポリシーで Windows ファイアウォールの設定を有効にしていても、セキュリティの判定で、Windows ファイアウォールの判定が「対象外」になります。そのため、Windows ファイアウォールが無効になっても問題ないコンピュータでネットワークモニタを有効にしてください。

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。

注意 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の無効化に失敗しました）になった場合は、ネットワークモニタエージェントのアンインストールが失敗しています。この場合、新しい監視用のコンピュータでネットワークモニタを有効にすると、既存の監視用のコンピュータからネットワークモニタエージェントが自動的にアンインストールされます。

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。

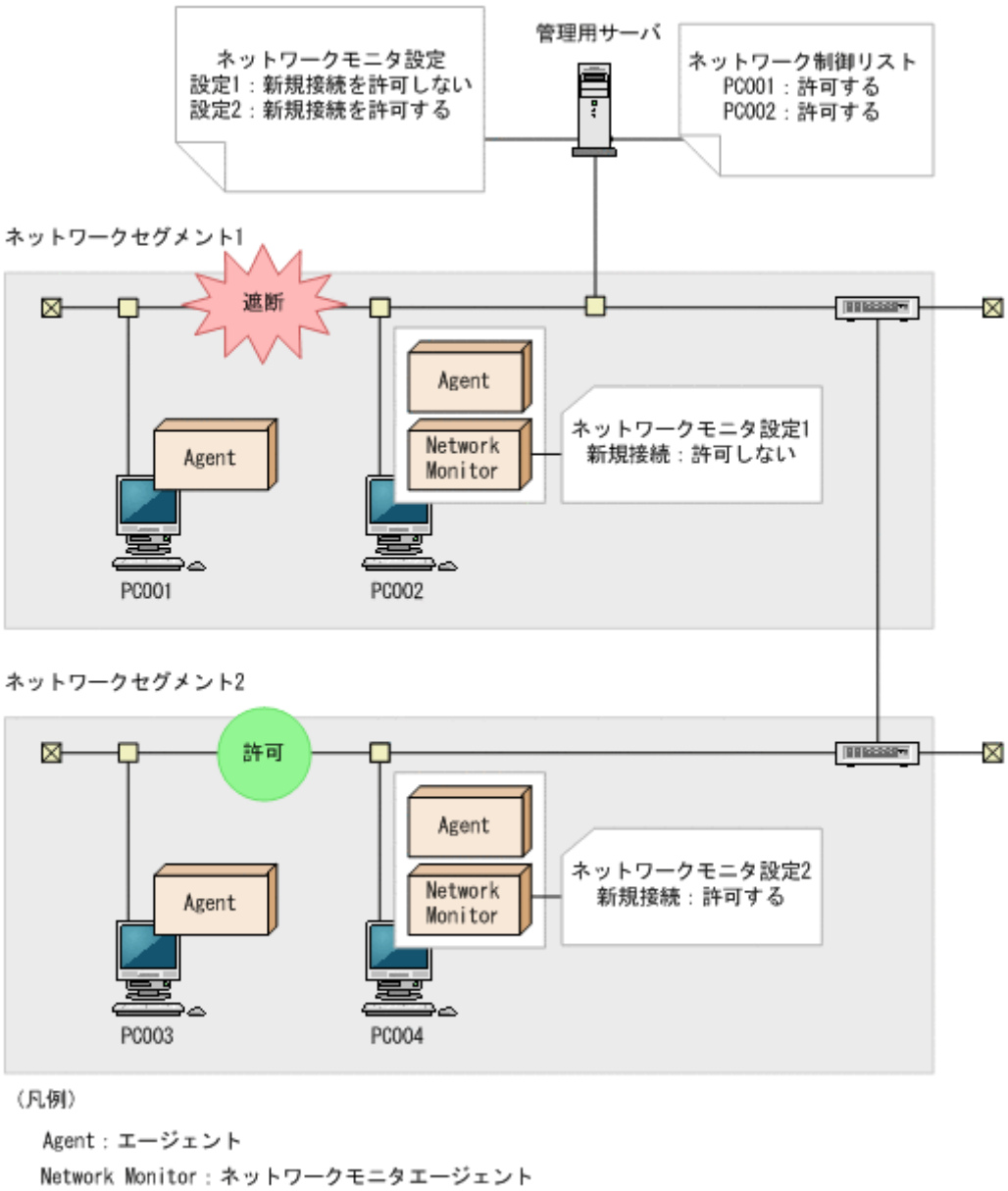
   ネットワークモニタを有効にすることで、そのコンピュータを含むネットワークセグメントが監視されるようになります。

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。

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：エージェント

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。

注意 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。

参考 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］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「(標準設定)」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。

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。

割り当てるネットワークモニタの種類を変更する場合、割り当てるネットワークモニタの種類を指定します。

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。

運用状況の変更に伴って、機器のネットワーク接続制御をやめる場合、ネットワーク制御リストから機器を削除します。

参考 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。

関連リンク

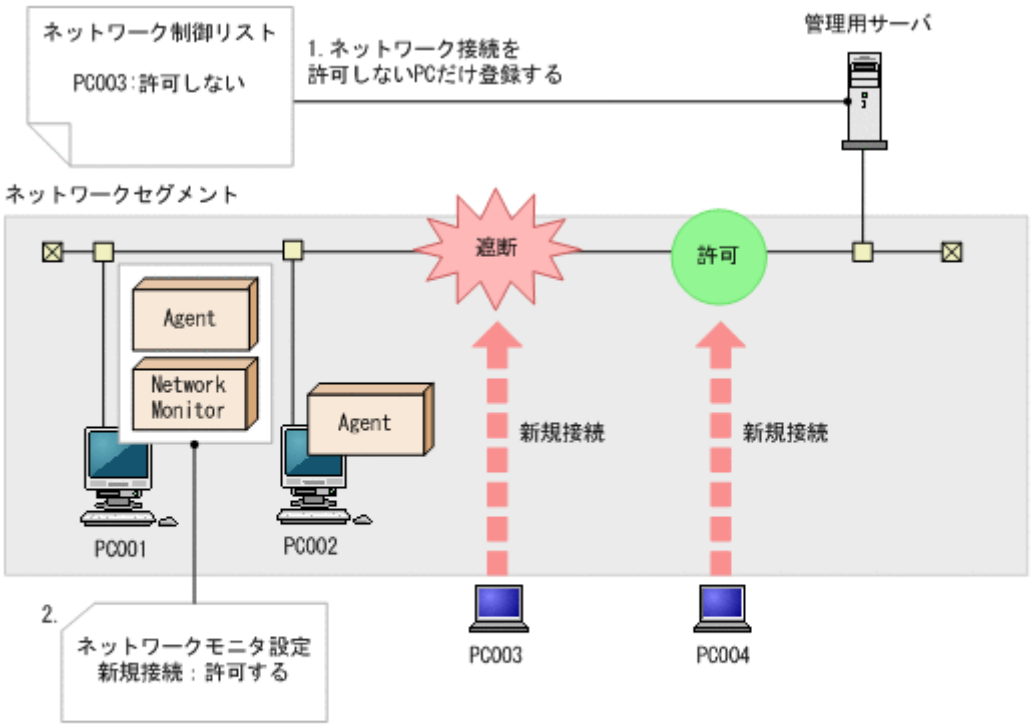
- 2.8.9 ブラックリスト方式を利用した機器のネットワーク接続の管理
- 2.8.10 ホワイトリスト方式を利用した機器のネットワーク接続の管理

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。

参考 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：エージェント

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。

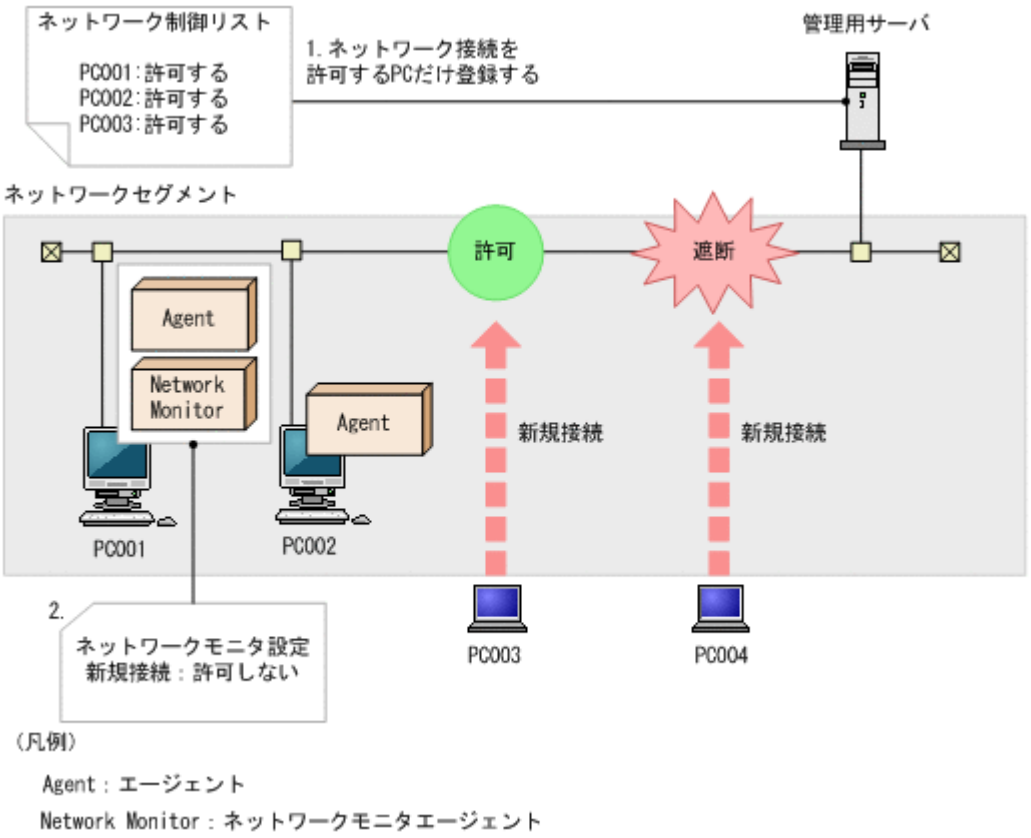
これによって、手順１で登録した機器だけネットワーク接続が遮断されるようになります。

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。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。

参考 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。

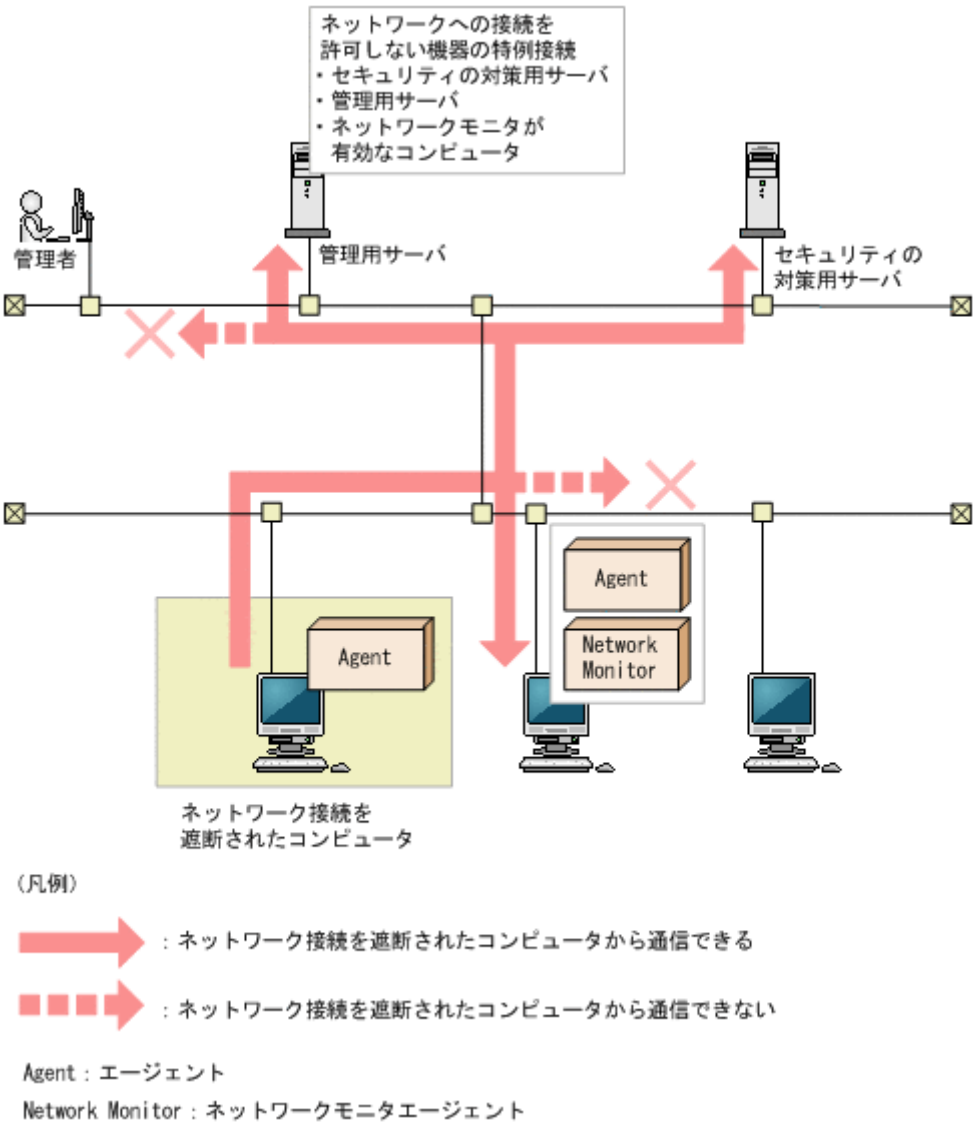
注意 ホワイトリスト方式でネットワーク接続を管理する場合、ルータ、スイッチ、ネットワークプリンタなど、JP1/IT Desktop Management が管理対象としない機器に対しても、ネットワーク接続を許可するように登録してください。特に、ルータやスイッチなどのネットワーク装置が接続を許可するよう設定されていないと、その配下に接続された機器もネットワークに接続できないため、注意してください。

2.8.11 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、[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、およびネットワークモニタを有効にしたコンピュータとだけ通信できます。

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。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。なお、管理用サーバは、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、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。

注意 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。

参考 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。

2.8.12 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、「2.8.14 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。
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。

注意 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。

参考 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

2.8.13 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。

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。

2.8.14 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、「2.8.12 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。

参考 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。

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 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。

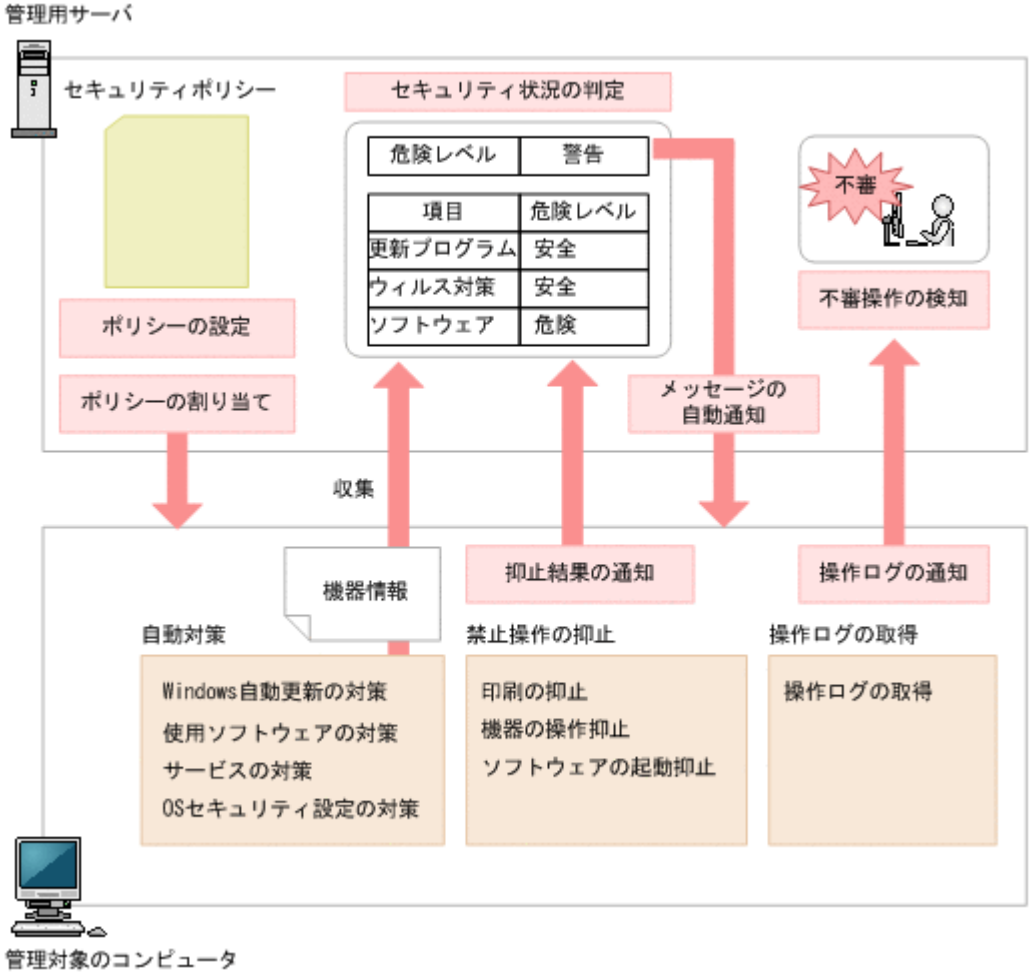
セキュリティポリシーを利用することで、次のセキュリティ状況を把握できます。

- 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 USB デバイスなどの利用抑止、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。

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 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、「(2) 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。

操作ログは定期的に収集され、セキュリティポリシーの設定に従って不審操作が検知されます。検知された操作を基に、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。操作ログの取得と不審操作の検知については、「2.10.4 操作ログに基づく不審操作の調査」を参照してください。

注意 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 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。

注意 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 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 7	○ ※1、※2	△	△	○
	Windows Server 2008 R2				
	Windows Server 2008				
	Windows Vista				
	Windows Server 2003 R2※3				
	Windows Server 2003※3				
	Windows XP				
	Windows 2000				
	Linux	×	×	×	○
	UNIX				
	Mac OS				
	不明				

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
スマートデバイス	iOS	×	×	×	○
	Android				
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　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。

2.9.3 セキュリティ状況の判定

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。

セキュリティ状況は次のタイミングで判定されます。

- 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機器情報が更新されたとき
- 管理対象のコンピュータが属するグループが変更されたとき
- 定期的な判定（デフォルトは毎日 0：00）

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。

参考 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。

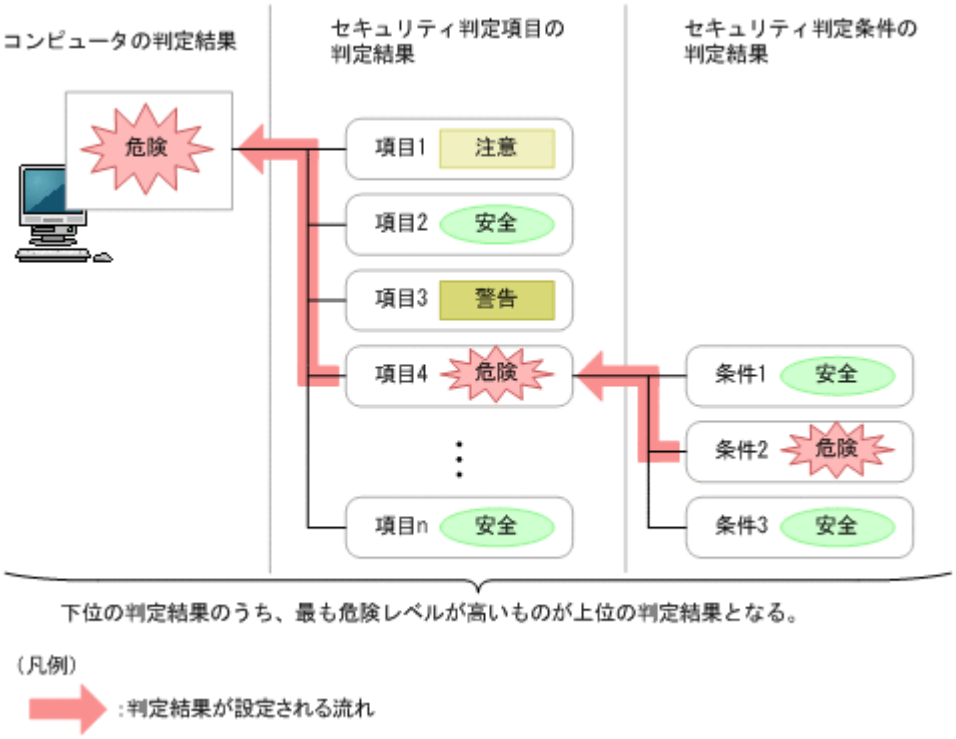
セキュリティポリシーで、判定結果が不適正だった場合に表示する危険レベルを、セキュリティ判定項目ごとに設定します。セキュリティポリシーを遵守していない場合は、設定した危険レベルが判定結果となります。コンピュータの総合的な危険レベルは、各項目の危険レベルのうち最も危険度が高い危険レベルが表示されます。

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 • 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。
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 • OS が Linux、UNIX、または Mac OS のコンピュータ

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。

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。
管理対象のコンピュータの機器情報が更新されたとき	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	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。
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※	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場合に判定を実施します。
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。

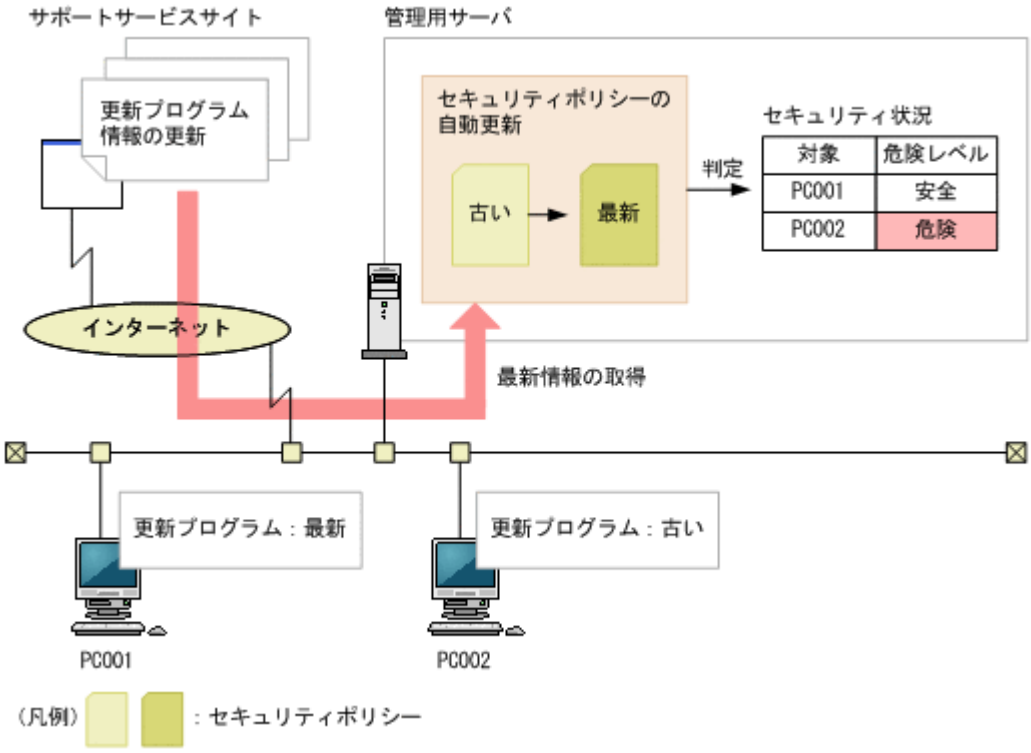
(3) 更新プログラムの適用状況の判定

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、古い更新プログラムが適用されているコンピュータに、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



参考 JP1/IT Desktop Management 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。

参考 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。

(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 および Internet Explorer のサービスパックと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) Windows 自動更新の設定の判定

Windows 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「OS のセキュリティ設定情報」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

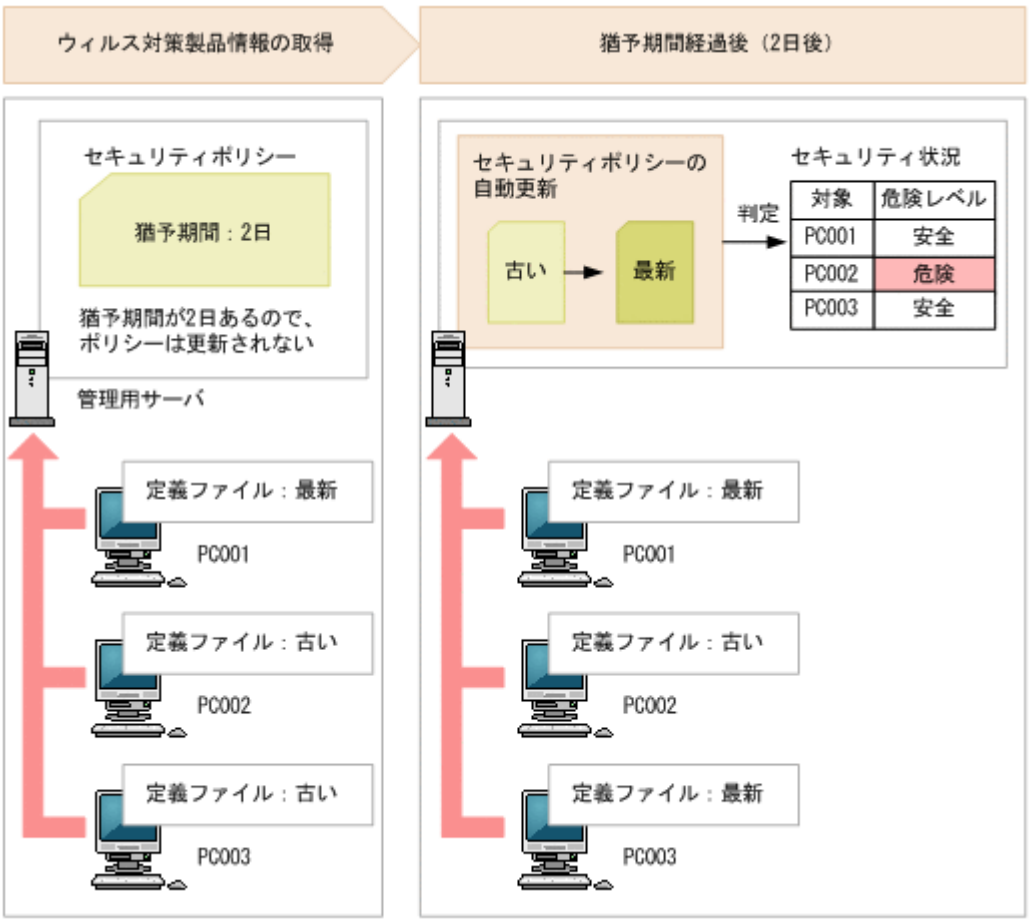
- (13) サポートするウィルス対策製品

(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。



JP1/IT Desktop Management がサポートする（判定の対象にできる）ウィルス対策製品は、新しい製品やバージョンがリリースされると、一定期間後に自動的に更新されます。ご利用の環境で最新情報を利用できるようにするためには、サポートサービスサイトに接続できるように設定されている必要があります。

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

- (13) 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（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

使用禁止ソフトウェアに設定した OS 情報（OS と OS サービスパック）が一致する機器を判定対象とします。 使用禁止ソフトウェアでは、ソフトウェアごと（管理ソフトウェアごと）に危険レベルを判定します。管理ソフトウェアと対応づけられた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一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。

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。

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。

注意 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。

注意 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 自体を 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 OS サービスパック）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、ソフトウェアごと（管理ソフトウェアごと）に危険レベルを判定します。管理ソフトウェアと対応づけられた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一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。

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。

注意 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。

注意 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
- 機器情報（システム情報）の「OS 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。OS 情報のサービス名が使用禁止サービスと一致する場合、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、「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。

(11) エージェントの有無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。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、エージェント有無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			
			管理共有	SNMP	ARP/ICMP	Active Directory
更新プログラム	Windows 自動更新を実行	○	○	×	×	×

設定項目		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
	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		○	×	×	×	×
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	○	○	×	×	×
	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	○	○	×	×	×
	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	○	○	×	×	×
	Windows ファイアウォール	○	○	×	×	×
	DCOM	○	○	×	×	×
	リモートデスクトップ	○	○	×	×	×

（凡例）○：判定できる　×：判定できない

注　エージェントレスの場合、セキュリティの自動対策はできません。

参考 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

- 2.6.4 エージェントレスでの管理

(12) 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。どれか一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。

注意 ユーザーアカウント単位に取得された機器情報が有効期限を過ぎている場合、そのユーザーアカウントは判定対象外となります。各情報の有効期限は次のとおりです。

- パスワードの安全性：期限なし
- パスワード更新からの経過日数：OS で設定されたパスワードの有効期間
- スクリーンセーバーのパスワード保護：30 日間
- スクリーンセーバー起動までの待ち時間：30 日間

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。

(13) サポートするウィルス対策製品

JP1/IT Desktop Management 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。

注意 ここで示す製品およびバージョンは、JP1/IT Desktop Management バージョン 09-51 リリース時のものです。
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。

参考 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。

参考 JP1/IT Desktop Management がサポートするウィルス対策製品は、新しい製品やバージョンがリリースされると、一定期間後に自動的に更新されます。ご利用の環境で最新情報を利用できるようにするためには、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できるように設定されている必要があります。

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

製品名・バージョンなど			操作画面上で表示される名称
	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
	2011	32bit	Norton AntiVirus 2011
		64bit	Norton AntiVirus 2011 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	32bit	Symantec Endpoint Protection 12.1
		64bit	Symantec Endpoint Protection 12.1 64bit
McAfee Total Protection Service※2、※3	5.0		McAfee Total Protection Service
McAfee SaaS Endpoint Protection※3	5.2		McAfee SaaS Endpoint Protection
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	32bit	McAfee VirusScan Enterprise 8.8
		64bit	McAfee VirusScan Enterprise 8.8 64bit
ウイルスバスター	2010	32bit	ウイルスバスター 2010
		64bit	ウイルスバスター 2010 64bit
	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
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※3、10.5 Patch1	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
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		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 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※3	6.0	32bit	ビジネスセキュリティクライアント
		64bit	ビジネスセキュリティクライアント 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	32bit	Forefront Client Security
		64bit	Forefront Client Security 64bit
Kaspersky Open Space Security Workstation	6.0.4	32bit	Kaspersky Anti-Virus 6.0 for Windows Workstations
		64bit	Kaspersky Anti-Virus 6.0 for Windows Workstations 64bit
Kaspersky Open Space Security Server	6.0.4	32bit	Kaspersky Anti-Virus 6.0 for Windows Servers
		64bit	Kaspersky Anti-Virus 6.0 for Windows Servers 64bit
ESET NODE32 Antivirus※1、※2、※3	4.0	32bit	ESET NOD32 Antivirus
		64bit	ESET NOD32 Antivirus 64bit
	4.2	32bit	ESET NOD32 Antivirus
		64bit	ESET NOD32 Antivirus 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 OS が 64 ビット版の Windows の場合 Sophos Anti-Virus 64bit
		64bit	
	9.5	32bit	
		64bit	
Sophos Security Suite small business solutions	4.0	32bit	
Sophos Computer Security small business solutions		64bit	
Sophos Anti-Virus small business solutions			
F-Secure Client Security※1、※2、※3	8.01	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	
	9.0	32bit	
		64bit	
	9.1	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。

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
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
McAfee Total Protection Service※2、※3	5.0		McAfee Total Protection Service
McAfee SaaS Endpoint Protection※3	5.2		McAfee SaaS Endpoint Protection
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	32bit	McAfee VirusScan Enterprise 8.8
		64bit	McAfee VirusScan Enterprise 8.8 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
Worry-Free Business Security-Standard※1、※2、※3、※4	7.0	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※1、※2、※3、※4	7.0	32bit	
		64bit	
OfficeScan Corporate Edition	8.0※3、10※3、	32bit	OS が 32 ビット版の Windows の場合 OfficeScan Corp.
		64bit	

製品名・バージョンなど			操作画面上で表示される名称
	10.5※3、10.5 Patch1		OS が 64 ビット版の Windows の場合 OfficeScan Corp. 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	32bit	Forefront Client Security
		64bit	Forefront Client Security 64bit
Kaspersky Open Space Security Server	6.0.3※1、※2、※3、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		32bit	Kaspersky Anti-Virus 6.0 for Windows Workstations
		64bit	Kaspersky Anti-Virus 6.0 for Windows Workstations 64bit
ESET NOD32 Antivirus※1、※2、※3	4.0、4.2	32bit	ESET NOD32 Antivirus
		64bit	ESET NOD32 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			
F-Secure Client Security※1、※2、※3	8.01、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	

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　ウィルス定義ファイルのバージョンは収集できません。

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。

製品名	常駐・非常駐の判定条件
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	［リアルタイム検索］がオンの場合に常駐となる。
ウイルスバスター 2011 クラウド	［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。
ウイルスバスターコーポレートエディション	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	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。
ESET NODE32 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	
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。
OfficeScan Corporate Edition	［Enable virus/malware scan］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	－
Worry-Free Business Security-Advanced	
OfficeScan Corporate Edition	［Enable virus/malware scan］がオンの場合に常駐となる。
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。
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。

製品名	常駐・非常駐の判定条件
Sophos Security Suite small business solutions	
Sophos Computer Security small business solutions	
Sophos Anti-Virus small business solutions	
F-Secure Client Security	－

（凡例）－：常駐・非常駐の状態は収集できない

(14) サポートするウィルス対策製品の自動更新

サポートサービスサイトと接続することで、セキュリティポリシーの判定対象となるウィルス対策製品の情報を自動更新できます。このため、エージェント導入済みコンピュータにインストールされている最新のウィルス対策製品の情報をセキュリティ状況の判定に反映できます。

参考 サポートサービスサイトと接続するためには、サポートサービス契約をしている必要があります。

サポートサービスサイトからは、次の情報が定期的にダウンロードされます。

- ウィルス対策製品の一覧

  セキュリティポリシーの判定対象となるウィルス対策製品の一覧です。サポートサービスサイトからダウンロードされると、セキュリティポリシーのウィルス対策製品の一覧に反映されます。

- コンピュータからウィルス対策製品の情報を収集するスクリプト

  エージェント導入済みのコンピュータで、コンピュータにインストールされているウィルス対策製品の情報を収集するために実行するスクリプトです。サポートサービスサイトからダウンロードされると、エージェント導入済みのコンピュータに配信されます。

(15) 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。

参考 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 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。

(16) 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。

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 行に一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。

参考 「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。

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。

(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

Windows 自動更新の実行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。

禁止操作

印刷操作や各種デバイスの利用、ソフトウェアの利用を抑止できます。

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。

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	Windows 自動更新を実行	Windows 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。Windows 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

設定項目		説明	自動対策
	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。	○
	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 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、どれか一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。 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。	○
	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。	○
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、だれ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。	○

設定項目		説明	自動対策
	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。	―
	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。	○

設定項目		説明	自動対策
	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。	○
	Windows ファイアウォール ※7、※8	Windows 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。 Windows 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。 Windows 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、※9	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
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 デバイスの読み取りと書き込みの抑止 ※10	USB デバイスの書き込みと読み取りを抑止できます。	−
	登録済 USB デバイスの使用許可	ハードウェア資産情報が登録済みの USB デバイスだけ、書き込みと読み取りを許可できます。	−
	USB デバイスの書き込みの抑止※10、※11	USB デバイスの書き込みだけを抑止できます。	−
	内蔵 CD/DVD ドライブの書き込みの抑止 ※11、※12	内蔵 CD/DVD への書き込みを抑止できます。	−
	内蔵 FD ドライブの読み取りと書き込みの抑止	内蔵 FD への書き込みと読み取りを抑止できます。	−

設定項目		説明	自動対策
	IEEE1394 接続メディアの読み取りと書き込みの抑止※11	IEEE1394 接続メディアへの書き込みと読み取りを抑止できます。	―
	内蔵 SD カードの読み取りと書き込みの抑止※11	内蔵 SD カードへの書き込みと読み取りを抑止できます。	―
	リムーバブルディスクの読み取りと書き込みの抑止※11	リムーバブルディスクへの書き込みと読み取りを抑止できます。	―
	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※2	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。	―
	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。	―

（凡例）○：設定できる　―：自動対策の対象外

注※1　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。

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、または Windows 2000 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　エージェントの OS が Windows 2000 の場合は判定されません。また、自動対策もできません。

注※10　USB 接続の FD ドライブ、CD/DVD ドライブ、ハードディスク、フラッシュメモリなどの使用を抑止する場合は、USB デバイスの抑止を設定してください。

注※11　抑止対象のコンピュータの OS によって、抑止の可否が異なります。

注※12　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。

注意 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。

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。

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）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)　製品が提供するセキュリティポリシー

JP1/IT Desktop Management 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。デフォルトポリシーは、サポートサービス契約をしていることを前提としています。

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 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。推奨セキュリティポリシーは、サポートサービス契約をしていることを前提としています。

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。

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	Windows 自動更新の実行の判定	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	△	−	△	−
	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	△（1 日）	−	△（1 日）	−
	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	○	×	○	○

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
	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	○	−	○	−
	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	○	×	○	○
	Windows 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	○	×	○	○
禁止操作	印刷の抑止	−	×	−	×	−
	USB デバイスの読み取りと書き込みの抑止	−	×	−	○	−
	登録済 USB デバイスの使用許可	−	×	−	○	−
	USB デバイスの書き込みの抑止	−	×	−	×	−
	内蔵 CD/DVD ドライブの書き込みの抑止	−	×	−	○	−
	内蔵 FD ドライブの読み取りと書き込みの抑止	−	×	−	○	−

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
	IEEE1394 接続メディアの読み取りと書き込みの抑止	－	×	－	○	－
	内蔵 SD カードの読み取りと書き込みの抑止	－	×	－	○	－
	リムーバブルディスクの読み取りと書き込みの抑止	－	×	－	×	－
	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	－	×	－	×	－
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

(3)　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。

参考　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。

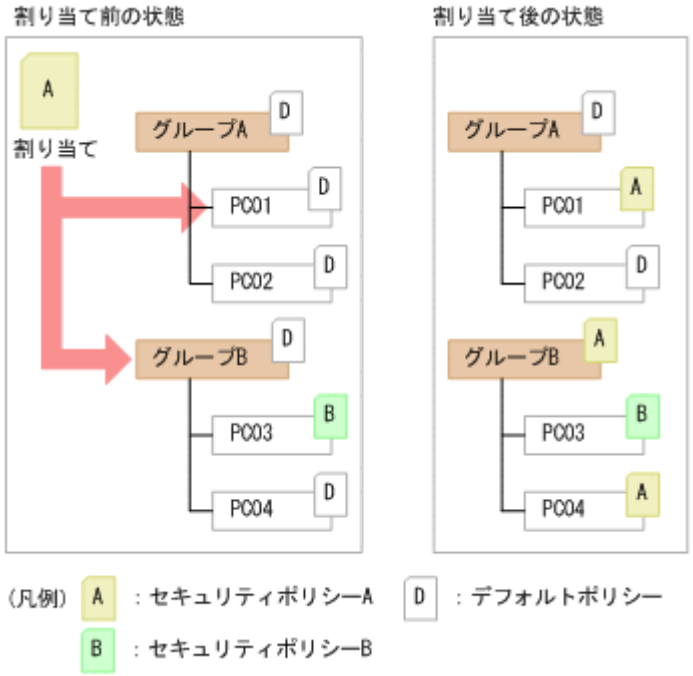
セキュリティポリシーを割り当てる場合

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。

注意 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。

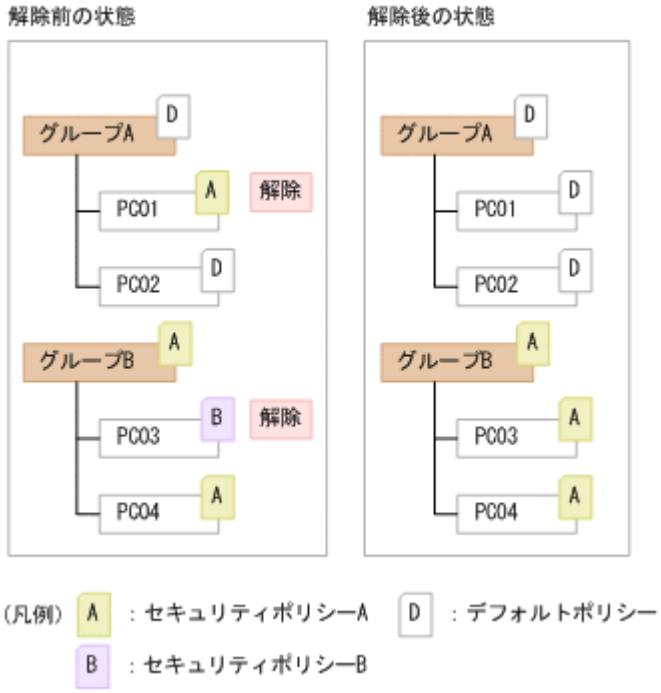


上記の図では、セキュリティポリシー A をコンピュータ PC01 とグループ B に割り当てています。ただし、グループ B のコンピュータ PC03 には個別にセキュリティポリシー B が割り当てられているため、セキュリティポリシー B が優先されます。

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。

(4) 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、エージェントがインストールされている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、「(5) 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、「(6) ネットワーク接続の遮断と許可」を参照してください。

(5) 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、エージェントがインストールされている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

参考 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。

注意 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。

自動で通知されるメッセージの内容

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

(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

項目	説明
	• 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。
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** • サービスパックあり：**製品名（サービスパック名）** 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**

項目	説明
	• 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**

（凡例）△：半角スペース

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。

(6)　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。

参考 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、「2.8.14 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する設定にしている場合
  自動的にネットワーク接続が遮断される契機になっても、遮断されません。
- 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。

(7)　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 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、「(8) 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。

(8) 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
- 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
- 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
- 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
- 共有フォルダが設定されている場合に解除する
- 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
- リモートデスクトップが有効な場合に無効にする

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。

注意 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。

- Windows 自動更新を実行
- 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 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

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。

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。

注意 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場合があります。

印刷機能を利用した PDF 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、PDF ファイルが出力されることがあります。

機器の操作の抑止

USB デバイスや CD/DVD ドライブの利用を抑止できます。外部メディアを利用して情報が持ち出されることを防止できます。抑止できるのは、次の機器の操作です。

- USB デバイスの読み取りと書き込み
- 内蔵 CD/DVD ドライブの書き込み
- 内蔵 FD ドライブの読み取りと書き込み
- IEEE1394 接続メディアの読み取りと書き込み
- 内蔵 SD カードスロットの読み取りと書き込み
- リムーバブルディスクの読み取りと書き込み

抑止対象の USB デバイスは、デバイスのプロパティの［ハードウェア］タブを表示したときに、［デバイスの機能］に「USB 大容量記憶装置」と表示されます。

IEEE1394 接続メディア、および内蔵 SD カードスロットは、OS の［ハードウェアの安全な取り外し］ダイアログでデバイスコンポーネントを表示したときに、次のように表示されます。

- IEEE 1394 SBP2 Drive

- Secure Digital Storage Device

参考 抑止対象のコンピュータの OS によって、抑止できる項目が異なります。

参考 機器の操作の抑止は、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定期的に表示されます。

警告 JP1/IT Desktop Management 以外の、外部メディアの使用を抑止する製品（Windows のグループポリシーや Active Directory のポリシー適用など）とは、同時に使用しないでください。同時に使用すると、JP1/IT Desktop Management での設定内容が他製品によって変更されたり、他製品での設定内容が JP1/IT Desktop Management によって変更されたりするおそれがあります。

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。

注意 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。

警告 OS や JP1/IT Desktop Management 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 が正しく動作しなくなるおそれがあります。

(1) 抑止対象となる外部メディア

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 USB デバイス、CD/DVD ドライブなどの利用を抑止できます。抑止項目、コンピュータの OS ごとの抑止の可否、および抑止の対象を次の表に示します。

Windows 7、Windows Server 2008、Windows Vista

抑止項目	Windows 7	Windows Server 2008	Windows Vista	抑止の対象※1
USB デバイスの読み取りと書き込み※2	○	○	○	次の手順で対象のデバイスを確認してください。 1. ［スタート］メニューから［デバイスとプリンター］を選択します。 2. 表示されるダイアログで、デバイスのアイコンを右クリックして［プロパティ］を選択します。 表示されるダイアログの［ハードウェア］タブの［デバイスの機能］に「USB 大容量記憶装置」

抑止項目	Windows 7	Windows Server 2008	Windows Vista	抑止の対象※1
				と表示されるデバイスが対象となります。
CD/DVD ドライブの書き込み	△	△ ※4	△	［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 ドライブの読み取りと書き込み	△	△ ※4	△	［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。
リムーバブルディスクの読み取りと書き込み※3	△	△ ※4	△	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、および USB 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 接続の両方が対象になります。

（凡例）○：抑止できる（抑止のイベントが送信される、抑止のメッセージが表示される）
△：抑止できる（抑止のイベントが送信されない、抑止のメッセージが表示されない）

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　USB デバイスを抑止する場合でも、登録済みの USB デバイスだけ使用を許可する運用ができます。

注※3　ここでのリムーバブルディスクとは、内蔵 SD カード、USB 接続の SD カードなどのデバイスを指します。

注※4　機器に依存して、抑止できない場合があります。

参考 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、使用は許可できません。

参考 Windows 7、Windows Server 2008、および Windows Vista の場合、USB デバイスまたはリムーバブルディスクのどちらか一方だけ抑止設定ができます。このため、抑止対象としたいデバイスがどのように OS に認識されるか検証してから、抑止設定をすることをお勧めします。

Windows Server 2003、Windows XP、Windows 2000

抑止項目		Windows Server 2003	Windows XP	Windows 2000	抑止の対象※1
USB デバイス	読み取りと書き込み※2	○	○	○	［ハードウェアの安全な取り外し］ダイアログで、［デバイスコンポーネントを表示する］をチェックしたときに「USB 大容量記憶装置デバイス」と表示されるドライブが対象となります。
	書き込み	× ※3	△	× ※3	
内蔵 CD/DVD ドライブの書き込み※4		△	△	×	CD/DVD ドライブのプロパティで［書き込み］タブが表示されるデバイスが対象となります。
内蔵 FD ドライブの読み取りと書き込み※4		△	△	△	［マイコンピュータ］で、［リムーバブル記憶域があるデバイス］に表示されるデバイスが対象となります。
IEEE1394 接続メディアの読み取りと書き込み		△	△	△	［ハードウェアの安全な取り外し］ダイアログで、［デバイス コンポーネントを表示する］を チェックしたときに「IEEE 1394 SBP2 Device」と表示されるドライブが対象となります。
内蔵 SD カードスロットの読み取りと書き込み※4		×	△	×	［ハードウェアの安全な取り外し］ダイアログで、［デバイス コンポーネントを表示する］をチェックしたときに「Secure Digital Storage Device」と表示されるドライブが対象となります。

（凡例）○：抑止できる（抑止イベントの送信、抑止メッセージの表示ができる）　△：抑止できる（抑止イベントの送信、抑止メッセージの表示ができない）　×：抑止できない

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　USB デバイスを抑止する場合でも、登録済みの USB デバイスだけ使用を許可する運用ができます。

注※3　USB デバイスの書き込みを抑止した場合、読み取りと書き込みが抑止されます。

注※4　「内蔵」とは、各種メディアのスロットがコンピュータに内蔵されているタイプのものを指します。コンピュータの本体の中で、スロット装置が USB 接続されているタイプもありますが、その場合は「内蔵」に該当しません。

なお、抑止の対象となる USB デバイスは、USB 接続でデータを記録できるデバイスです。 USB 接続でデータを記録できるデバイスは、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。

デバイスセットアップクラス	ClassGuid
CD-ROM	{4d36e965-e325-11ce-bfc1-08002be10318}
Disk Drive	{4d36e967-e325-11ce-bfc1-08002be10318}
Floppy Disk	{4d36e980-e325-11ce-bfc1-08002be10318}

参考 デバイスセットアップクラスの ClassGuid については、デバイスの開発元に確認してください。

関連リンク

- (6) 外部メディアの抑止の注意事項
- (2) 使用を許可できる USB デバイスの種類

(2) 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。

参考 使用を許可できる USB デバイスの種類は、USB ストレージデバイスだけです。次の手順で対象の USB デバイスを確認してください。

1. ［スタート］メニューから［デバイスとプリンター］を選択します。
2. 表示されるダイアログで、デバイスのアイコンを右クリックして［プロパティ］を選択します。

表示されるダイアログの［ハードウェア］タブの［デバイスの機能］に「USB 大容量記憶装置」と表示される USB デバイスが対象となります。

参考 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

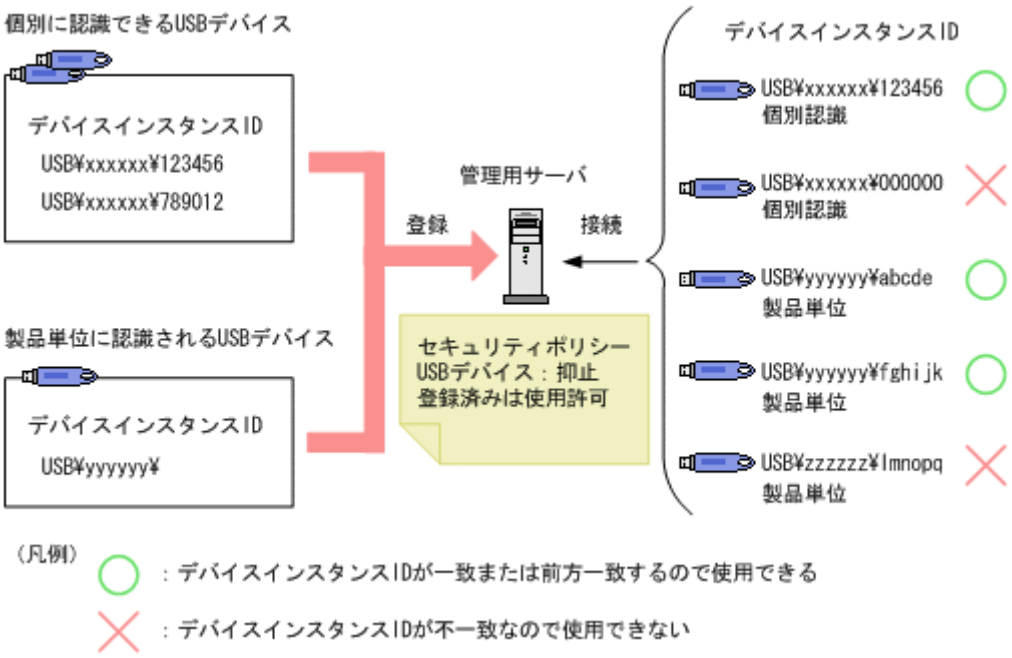
ユニークなデバイスインスタンス ID を持つ USB デバイスは、各デバイスを個別に使用許可できます。

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、一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。



注意 使用を許可する USB デバイスは、エージェント導入済みのコンピュータから登録します。なお、資産画面の［ハードウェア資産］画面でも USB デバイスの資産情報を直接登録できますが、この方法で登録しても利用は許可されません。

注意 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。

注意 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。

注意 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。

注意 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。

参考 エージェントをインストールしているコンピュータに、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。なお、製品単位で認識される USB デバイスの場合、ファイルの情報は収集されません。

(3) 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

- (4) ソフトウェアの起動抑止の注意事項
- (5) 印刷の抑止の注意事項
- (6) 外部メディアの抑止の注意事項

(4) 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、起動抑止ができない場合があります。
- Windows 7 の AppLocker 機能でもソフトウェアを起動抑止する場合、同じソフトウェアを指定すると、AppLocker 機能の起動抑止が先に実行されます。このため、JP1/IT Desktop Management でソフトウェアを起動抑止できません。
- 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されない場合があります。
- 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。」

(5) 印刷の抑止の注意事項

- 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、プリンタサーバとなる機器で、印刷操作を行った機器の名前解決ができる必要があります。
- ネットワーク共有プリンタの場合、プリンタサーバとなる機器で、プリンタの［プロパティ］ダイアログの［セキュリティ］タブで「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、またはほかのコンピュータに接続されたプリンタの場合、 コントロールパネルの［Windows ファイアウォール］－［Windows ファイアウォールによるプログラムの許可］－［例外］タブで「ファイルとプリンタの共有」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、またはほかのコンピュータに接続されたプリンタの場合、抑止対象のコンピュータで Win32_PrintJob クラスがサポートされた WMI が起動し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 では印刷抑止できません。
- ネットワークプリンタを使用している環境で、プリンタサーバとコンピュータの両方で印刷抑止されている場合、コンピュータの印刷抑止だけを解除しても印刷はできません。なお、この場合、コンピュータで印刷操作の操作ログが取得されます。
- プリンタドライバのインストール時にテスト印刷した場合、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。
- プリントサーバの OS が Windows Vista の場合、ネットワーク共有プリンタ、またはほかのコンピュータに接続されたプリンタは印刷抑止できません。

(6) 外部メディアの抑止の注意事項

- JP1/IT Desktop Management 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 の規定に準拠し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。
- 次に示す条件をすべて満たす場合、USB 接続のハードディスクまたは USB 接続の FD ドライブへ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 USB デバイスの操作は抑止できません。
  - クライアントの OS が Windows 7 または Windows Server 2008 R2 である
  - ファイルコピーの実行中に、USB デバイスを抑止するセキュリティポリシーが適用される
- デバイスのプロパティの［ハードウェア］タブで、［デバイスの機能］に「USB 大容量記憶装置」と表示されない USB デバイスが抑止されることがあります。その場合は、コンピュータを抑止対象外とするか、抑止された USB デバイスを登録して利用を許可するように設定してください。
- ［ハードウェアの安全な取り外し］アイコンの実行、または［デバイス マネージャー］で USB デバイスを右クリックして［削除］を実行した場合、機器の操作を抑止できない場合があります。
- Windows の設定で、CD および DVD の自動再生機能が無効に設定されていると、USB デバイスの書き込みだけを抑止する場合に、USB 接続の CD/DVD ドライブへの書き込みが抑止されないことがあります。
- コンピュータの OS が Windows 7、Windows Server 2008、または Windows Vista の場合、USB デバイスの抑止で、セキュリティポリシーの［登録済みの USB デバイスは使用を許可する］をチェックするときは、IEEE 1394 接続メディアおよび内蔵 SD カードスロットは抑止しないでください。抑止する設定をすると、［登録済みの USB デバイスは使用を許可する］の設定が無効になり、すべての USB デバイスに対して、書き込みと読み出しが抑止されます。
- コンピュータの OS が Windows 2000 の場合、セキュリティポリシーの［登録済みの USB デバイスは使用を許可する］をチェックしていると、USB 接続の FD ドライブの操作が抑止できません。この USB デバイスの操作を抑止する場合は、このチェックを外してください。
- コンピュータの OS が Windows 2000 の場合、セキュリティポリシーの［登録済みの USB デバイスは使用を許可する］をチェックしていると、システムにログインする前から接続されている USB 接続の FD ドライブおよび USB 接続のハードディスクを抑止できません。これらの USB デバイスを抑止したい場合は、このチェックを外してください。
- コンピュータの OS が Windows 7、Windows Server 2008、または Windows Vista の場合、セキュリティポリシーの［登録済みの USB デバイスは使用を許可する］をチェックして、かつ Windows の設定で自動再生機能を有効にしていると、USB 接続の FD ドライブおよび USB 接続のハードディスクの操作が抑止できません。これらの USB デバイスの操作を抑止する場合は、チェックをオフにするか、または自動再生機能を無効にしてください。
- コンピュータの OS が Windows Server 2003、Windows XP、または Windows 2000 の場合、内蔵 FD ドライブの操作を抑止すると、ドライブ自体が存在しない状態となります。そのため、内蔵 FD ドライブの操作を抑止しているコンピュータからは、内蔵 FD ドライブの機器情報は取得できません。
- USB 接続リンクケーブルの使用を抑止する場合、OS に認識される USB デバイスの種別に応じて、操作の抑止を設定してください。ただし、デバイスによっては USB 接続リンクケーブルの使用を抑止できない場合があります。
- 抑止対象の USB デバイスをコンピュータに接続した場合、USB デバイスの自動再生機能が有効に設定されていても、自動再生が失敗しエラーメッセージが表示されることがあります。
- 抑止対象の USB デバイスを機器に接続した場合、USB デバイスの自動再生機能が有効になっていると、自動再生が失敗することがあります。
- USB 接続メディアを抑止した場合、操作ログを取得する設定にしていても、 USB 接続メディア内のファイルの操作について操作ログを取得できない場合があります。

- 次の場合、OS のエラーメッセージが表示されることがあります。
  - コンピュータの OS が Windows 2000 でデバイスドライバがインストールされていない状態で、抑止対象の USB デバイスが接続された場合
  - USB デバイスの操作中に、その USB デバイスの操作を抑止するセキュリティポリシーが適用された場合
- 内蔵 SD カードスロットを抑止をする場合、セキュリティポリシーを適用したあとでコンピュータを再起動すると有効になります。
- DVD ドライブやカードリーダーなどのデバイスで、抑止時にメディアが挿入されていない場合、抑止ログにドライブ種別とドライブ名は取得されません。
- コンピュータの OS が Windows Server 2003 または Windows XP の場合、CD/DVD ドライブの［プロパティ］の［書き込み］タブにある［このドライブで CD 書き込みを有効にする］のチェックを外すと、内蔵 CD/DVD への書き込みは抑止できません。なお、DVD-RAM に書き込む場合は、［このドライブで CD 書き込みを有効にする］のチェックを外す必要があるため、書き込みを抑止できません。
- 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。
- コンピュータの OS が Windows Server 2008、Windows 7、Windows Vista の場合、セキュリティポリシーに外部メディアの抑止を設定したときは、コンピュータを再起動したあとで抑止が有効になります。
- 他製品による外部メディアの抑止機能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操作を抑止した場合、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。
- 外部メディアの抑止は、抑止を実行するサービスを停止しても解除されません。外部メディアの抑止を解除するには、セキュリティポリシーで抑止を解除するか、エージェントをアンインストールする必要があります。
- 外部メディアの抑止が Active Directory や利用者の操作によって解除された場合、コンピュータでのサービス再起動時に再度外部メディアの抑止が設定されます。
- 外部メディアをいったん抑止したあとで抑止を解除した場合、各コンピュータでデバイスドライバを再インストールするなどして、デバイスドライバが正常に動作する状態にする必要があります。
- USB デバイスの読み取りと書き込みを抑止している場合、コンピュータ上で［USB デバイスの登録］ダイアログが表示されている間は、そのコンピュータで一時的に USB デバイスの抑止機能が無効になります。

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 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。

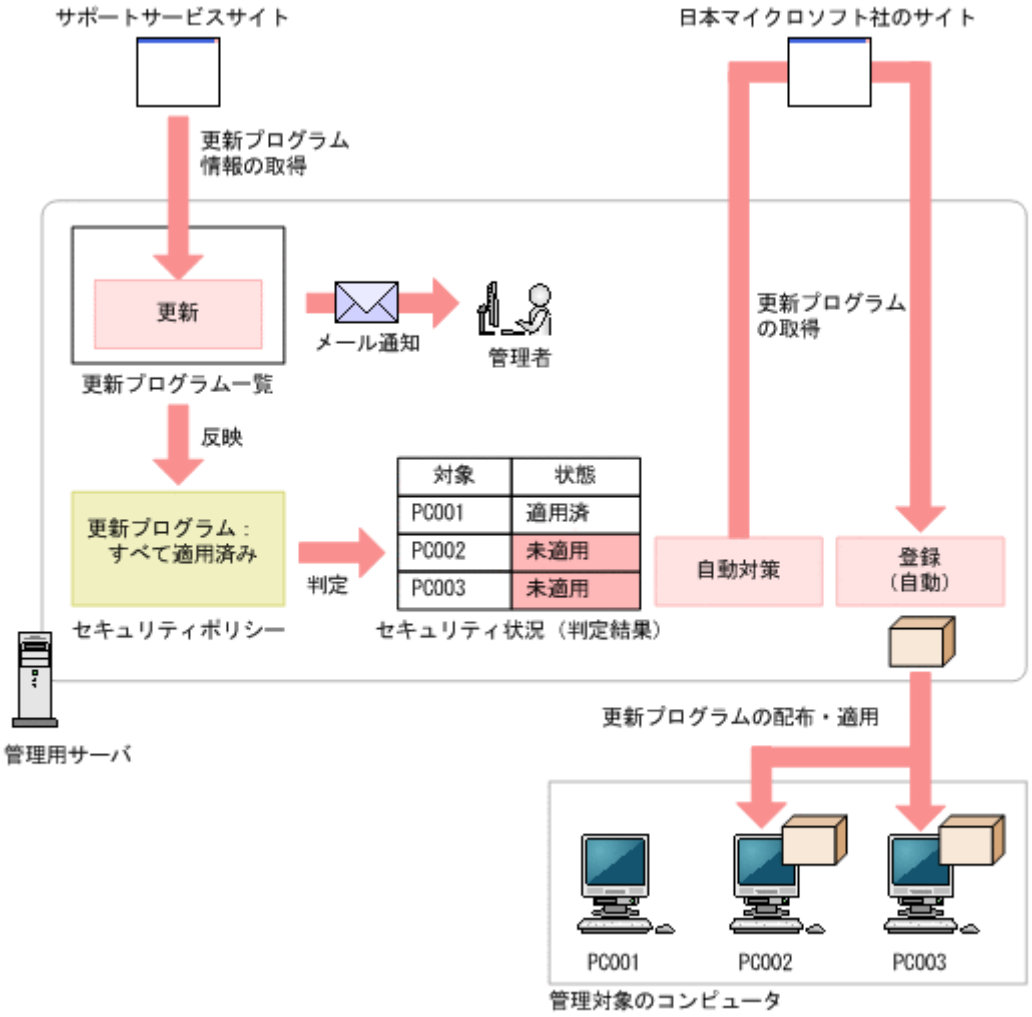
注意 更新プログラムの最新情報を自動的に取得して、更新プログラムをコンピュータに適用するにはサポートサービス契約が必要です。

JP1/IT Desktop Management 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。

参考 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 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 の機能を使用して配布することをお勧めします。

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

参考 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。

参考 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
- 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

参考 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 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 の動作は保証されません。

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 7
	Windows Server 2008
	Windows Vista
	Windows Server 2003
	Windows XP
	Windows 2000
Internet Explorer	6.0、7.0 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。

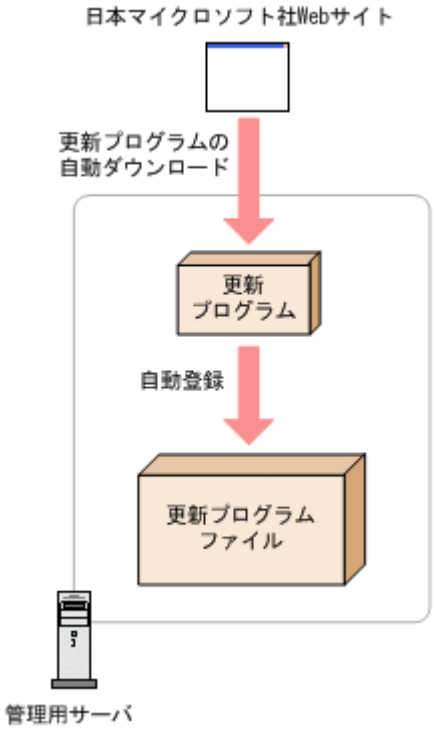
- クラス（更新プログラムの種類）が「更新プログラム」である
- セキュリティ番号が設定されている（空でない）
- セキュリティ深刻度が「緊急」または「重要」である
- 対象 OS のサービスパック番号の情報が存在する

(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。

注意 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。



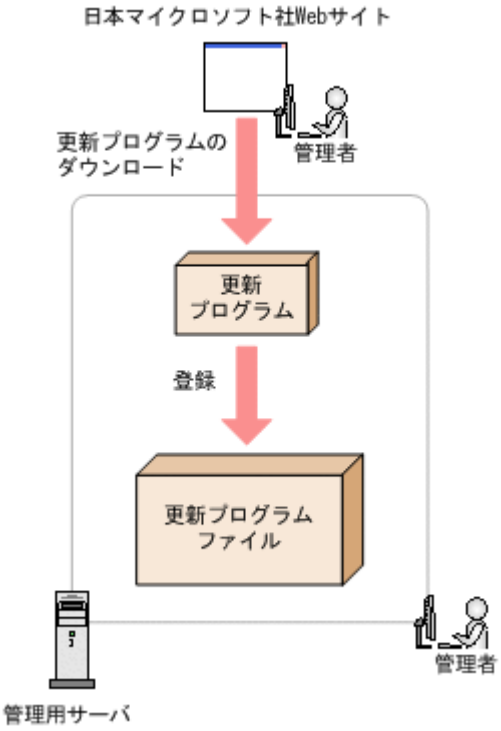
なお、登録された更新プログラムファイルは、配布画面の［パッケージ一覧］には追加されません。更新プログラムファイルは、セキュリティポリシーの自動対策だけで配布できます。手動で更新プログラムを配布するタスクを作成することはできません。実行されたタスクは配布画面で確認できます。

(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 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。



参考 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。

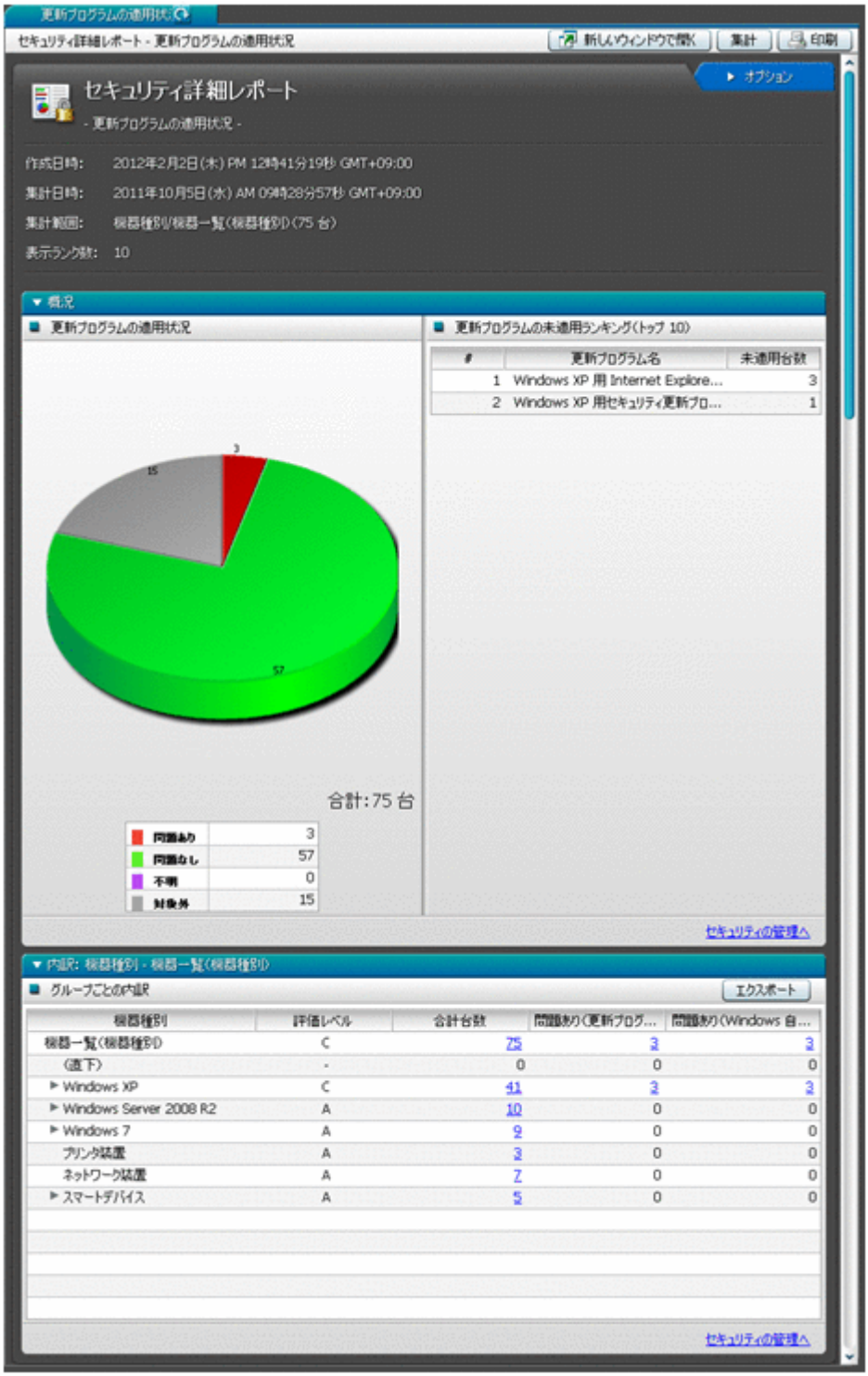
なお、作成された更新プログラムファイルは、配布画面の［パッケージ一覧］には追加されません。更新プログラムファイルは、セキュリティポリシーの自動対策だけで配布できます。手動で更新プログラムを配布するタスクを作成することはできません。実行されたタスクは配布画面で確認できます。

(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。

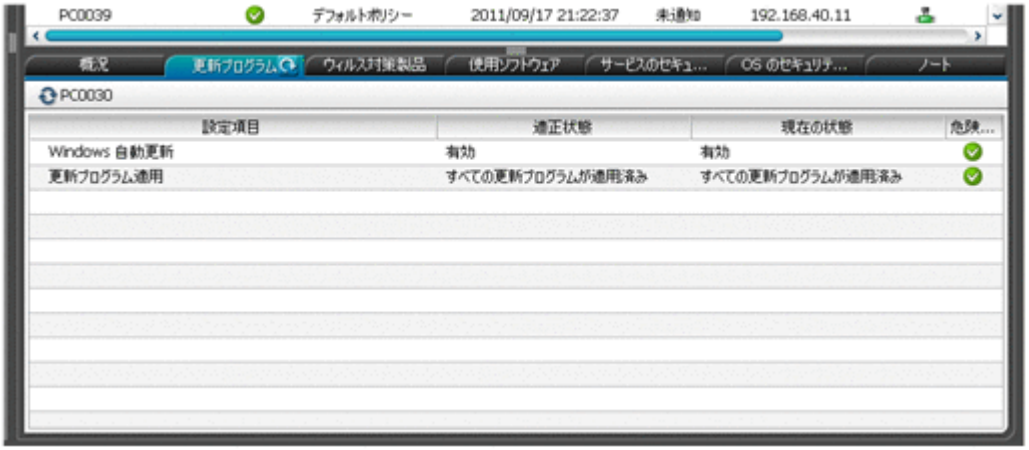


セキュリティポリシーごとに危険レベルを確認する

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。

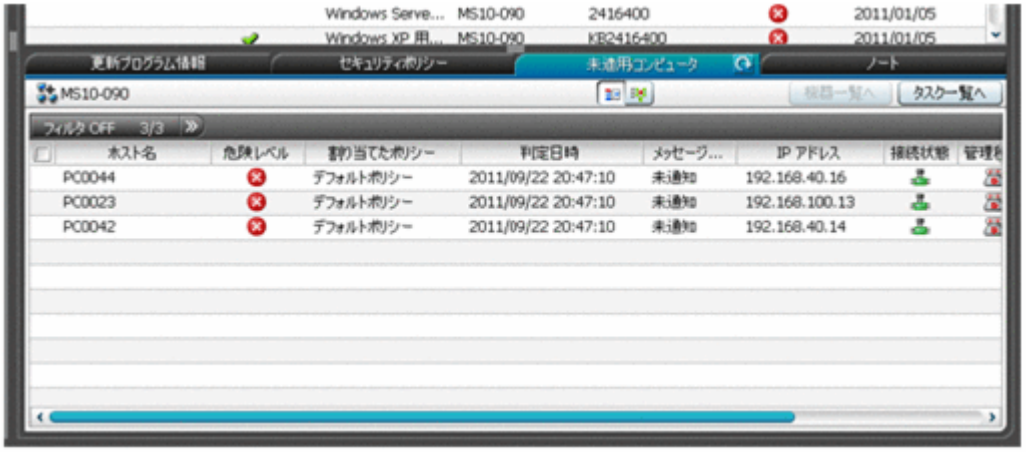
機器ごとに更新プログラムの適用状況を確認する

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 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 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 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。

注意 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。

注意 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

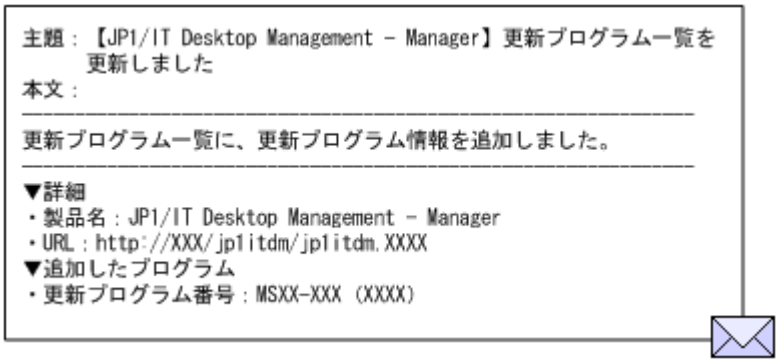
- (3) 情報を自動取得できる更新プログラムの種類
- (5) 更新プログラムファイルの手動登録

(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。

注意 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。

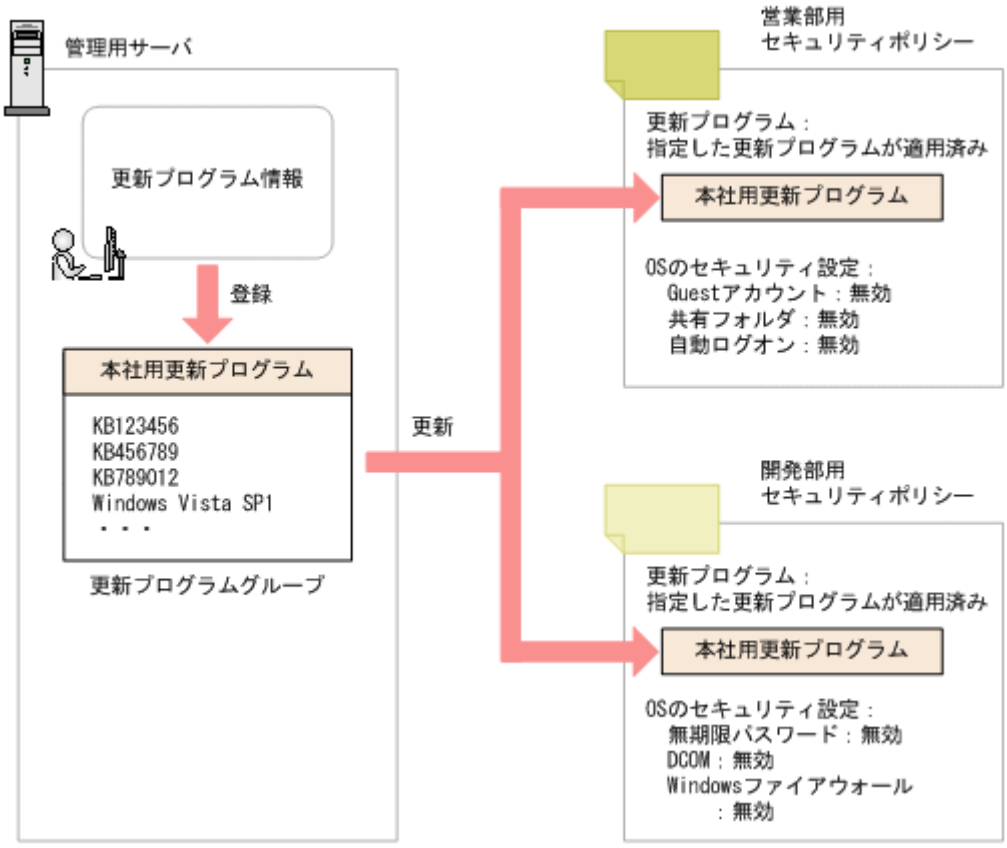


(9) 更新プログラムグループの管理

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）。
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。

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。

取得され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。

取得した操作ログは、操作画面から確認できます。セキュリティポリシーで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操作ログの履歴を追跡調査できます。

参考 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。情報漏えいにかか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。

参考 機器の台数が多い場合、管理用サーバ 1 台で操作ログを管理すると、管理用サーバやネットワークに負荷が掛かります。 機器の台数が多い場合や拠点が物理的に離れている場合などは、負荷を分散するためにサイトサーバを構成することをお勧めします。
なお、サイトサーバに保管された操作ログと管理用サーバに保管された操作ログは、同時には参照できません。このため、サイトサーバを利用する場合は、サイトサーバだけに操作ログを保管し、管理用サーバには操作ログを保管しないことをお勧めします。

関連リンク

- 2.10.2 管理用サーバでの操作ログの管理
- 2.10.3 サイトサーバでの分散操作ログの管理
- 2.10.1 取得できる操作ログの種類
- 2.10.4 操作ログに基づく不審操作の調査

2.10.1 取得できる操作ログの種類

JP1/IT Desktop Management 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。

参考 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、取得した操作ログを基に不審操作かどうかが判定されます。このとき、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	不審操作に関連する操作ログ
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	プロセス起動	利用者がプログラムを起動した。	×
	プロセス停止	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	利用者がファイルをコピーした。	△
	ファイル移動	利用者がファイルを移動した。	△
	ファイル名称変更	利用者がファイル名を変更した。	△

操作種別	操作種別（詳細）	内容	不審操作に関連する操作ログ
	ファイル作成	利用者がファイルを新規作成した。	△
	ファイル削除	利用者がファイルを削除した。	△
	ファイルアップロード※1、※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※1、※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※1、※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※1、※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	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。	×
外部メディア接続/切断	外部メディア接続	利用者がコンピュータに外部メディアを接続した。	○
	外部メディア切断	利用者がコンピュータから外部メディアを切断した。	○
Web アクセス	Web アクセス※1	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。	○
	外部メディア接続抑止	禁止操作を設定している場合に、外部メディアの接続を抑止した。	○

（凡例）○：関連する　△：不審操作の条件によって監視対象となる場合に関連する　×：関連しない

注※1

操作ログを取得できる Web ブラウザを次に示します。

- Internet Explorer 6、7、8、9
- Firefox 3.5、3.6、4、5

ただし、ファイル送受信の操作ログについては、Internet Explorer を利用している場合だけ取得できます。

注※2

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。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※3

操作ログを取得できるメーラーを次に示します。

- Microsoft Outlook Express 6
- Microsoft Outlook 2002、2003、2007、2010
- Windows メール 6
- Windows Live メール 2009、2011

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、またはほかのコンピュータに接続されているプリンタ
- 仮想プリンタ

注意 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。

関連リンク

- (1) 監視できる不審操作の種類
- 2.10.5 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。

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	○	○	○

（凡例）○：取得される　×：取得されない

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（実行アカウント名）	ファイルバージョン※	プロセス名
プロセスの起動	○	○	○
プロセスの停止	○	○	○

（凡例）○：取得される

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	オリジナルファイル取得元/取得日時	操作元（操作対象）ファイル名/ドライブ種別	操作先ファイル名/操作先ドライブ種別
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	×	×	×	○	○	×
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	○	○	○	○	○	○

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	オリジナルファイル取得元/取得日時	操作元（操作対象）ファイル名/ドライブ種別	操作先ファイル名/操作先ドライブ種別
印刷※	×	×	×	×	×	×

（凡例）○：取得される　×：取得されない

注※　「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			
	操作元（操作対象）ファイル名	操作元（操作対象）ドライブ種別	操作先ファイル名	操作先ドライブ種別
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	○	○	×	×

（凡例）○：取得される　×：取得されない

外部メディア接続/切断

取得対象に「外部メディア接続/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、「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	ドライブ名	デバイス名	シリアルナンバー	デバイスの種類	デバイスインスタンス ID
外部メディア接続	○	○	○	○	○	○
外部メディア切断	×	○	×	×	×	×

（凡例）○：取得される　×：取得されない

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	
	タイトル	URL
Web アクセス	○	○

（凡例）○：取得される

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			
	ユーザー名（実行アカウント名）	ファイルバージョン※	プロセス名	ウィンドウタイトル
アクティブウィンドウの変更	○	○	○	○

（凡例）○：取得される

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「外部メディア接続抑止」の 3 種類があります。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（実行アカウント名）	ファイルバージョン※	プロセス名
プログラム起動抑止	○	○	○	○	○

（凡例）○：取得される

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	ドキュメント名	印刷ページ数
印刷抑止	○	○	×

（凡例）○：取得される　×：取得されない

外部メディア接続抑止

操作内容	取得される情報					
	ドライブ種別	ドライブ名	デバイス名	シリアルナンバー	デバイスの種類	インスタンス ID
外部メディア接続抑止	○	○	○	○	○	○

（凡例）○：取得される

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。

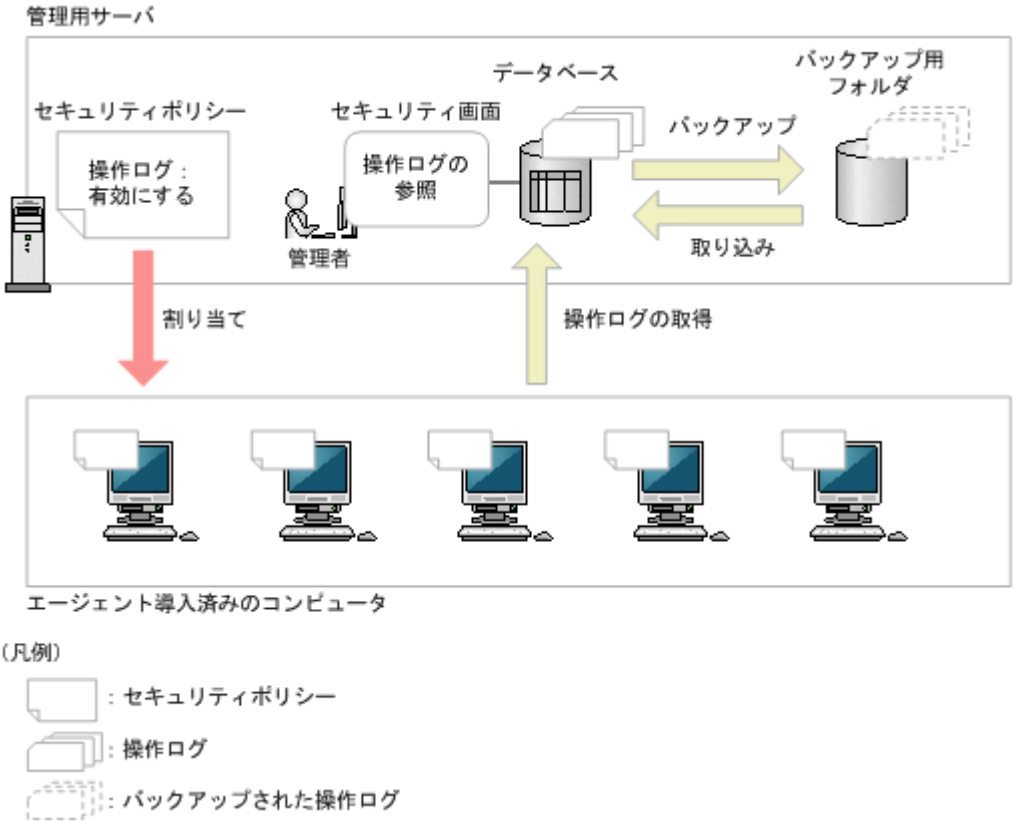
項目	内容
発生元	操作ログを取得したコンピュータのホスト名です。 表示例：dmp530
操作日時（Web ブラウザのロケール）	操作が発生した日時です。操作ログを表示するコンピュータのローカルタイムに変換して表示されます。 表示例：2011/10/01 22:00:01
操作日時	操作が発生した日時です。操作ログを取得したコンピュータのローカルタイムで表示されます。 表示例：2011/10/02 17:11:51
タイムゾーン	操作が発生したコンピュータのタイムゾーンです。UTC との差が表示されます。［操作ログの詳細］ダイアログでは、「操作日時」の項目に表示されます。 表示例：GMT+09:00
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
ユーザー名（実行アカウント名）	発生元のプロセス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
プロセス名	操作対象のファイルのパスを含むプロセス名です。 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。キロバイト単位で表示されます。 表示例：10.2KB
オリジナルファイル取得元	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。 ・ その他または不明 ・ Local disk ・ Network drive ・ Removable ・ CDROM ・ RAMDISK ・ Web ・ FTP ・ Mail 表示例：RAMDISK
オリジナルファイル取得日時	管理用サーバがファイルを発見した日時です。 表示例：2011/10/01 22:00:01.159

項目	内容
操作元（操作対象）ファイル名（フォルダ名・URL）	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 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
操作元（操作対象）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。 ・ その他または不明 ・ Local disk ・ Network drive ・ Removable ・ CDROM ・ RAMDISK ・ Web ・ FTP ・ Mail 表示例：Local disk
操作先ファイル名（フォルダ名・URL）	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
操作先ドライブ種別	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。 ・ その他または不明 ・ Local disk ・ Network drive ・ Removable ・ CDROM ・ RAMDISK ・ Web ・ FTP ・ Mail 表示例：Network drive
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。 ・ その他または不明 ・ Local disk ・ Network drive ・ Removable ・ CDROM ・ RAMDISK ・ Web ・ FTP ・ Mail 表示例：Network drive
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

項目	内容
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
デバイスの種類	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
デバイスインスタンス ID	接続されたデバイスのユニークな ID です。 表示例：USB¥VID_xxxx&PID_xxxx¥1234567890ABCD
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

サイトサーバに操作ログを保管しない場合、エージェント導入済みのコンピュータから取得された操作ログは、管理用サーバのデータベースに格納されます。管理用サーバに取得された操作ログは、セキュリティ画面の［操作ログ］画面から参照できます。



管理用サーバに取得された操作ログは、約 1 か月分がデータベースに保存されます。約 1 か月よりも古い操作ログは、自動的にデータベースから削除されます。

なお、セットアップで操作ログの自動バックアップを設定している場合、毎日自動的に操作ログのバックアップが取得されます。バックアップされた操作ログは、一時的にバックアップ用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。ただし、管理用サーバでバックアップした操作ログは、サイトサーバで取り込めません。また、サイトサーバでバックアップした操作ログは、管理用サーバで取り込めません。

注意 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。

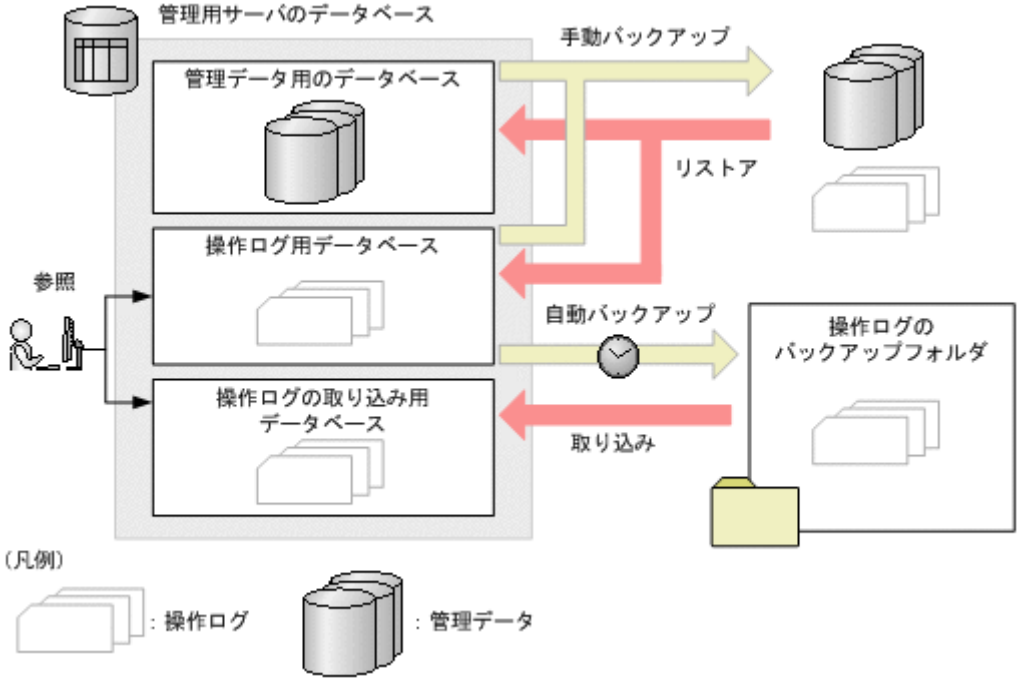
参考 バックアップ用のフォルダは長期間にわたって大容量のデータを格納する可能性があるため、RAID、NASなどのドライブを使用することをお勧めします。

関連リンク

- 2.10.1 取得できる操作ログの種類

(1) 管理用サーバでの操作ログのバックアップとリストア

情報漏えいなどの問題をあとで調査できるように、利用者の操作の履歴情報を操作ログとして取得し、データベースに保存できます。



エージェントを導入したコンピュータから、1時間に1回操作ログが取得されます。取得された操作ログは、操作ログ用データベースに格納されます。データベースに格納された操作ログは、セキュリティ画面の［操作ログ］画面から参照できます。

操作ログの自動バックアップを設定している場合は、操作ログ用データベースから、操作ログのバックアップフォルダに操作ログが自動的にバックアップされます。自動バックアップは1日に1回実施されます。

操作ログは操作ログ用データベースの容量を超えると、古いログから自動的に上書きされます。このため、過去の操作ログを参照したい場合は、自動バックアップした操作ログを取り込み用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。取り込み用データベースは、参照不要な場合はデータをクリアできます。

データベースマネージャやコマンドを使用して手動バックアップした場合は、管理データ用のデータベースと操作ログ用データベースのデータがバックアップされます。

参考 手動バックアップする場合、操作ログの自動バックアップが有効なときは、自動バックアップされていない日付の操作ログだけがバックアップされます。自動バックアップが無効な場合は、操作ログ用データベース内のすべて操作ログがバックアップされます。

手動バックアップした操作ログは、データベースマネージャやコマンドを使用してリストアできます。操作ログをリストアした場合、バックアップデータのうち最新の 7 日間分が操作ログ用データベースに格納されます。

注意 操作ログの自動バックアップを実施した場合、バックアップ用ドライブの空き容量がないとバックアップされません。そのため、操作ログ用データベースに新しい操作ログが格納されると、古い操作ログをバックアップをしないで削除してしまう場合があります。バックアップ用ドライブは、十分な空き容量を確保することをお勧めします。

注意 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。

注意 コンピュータから取得した操作ログの操作日時が、操作ログの表示期間（[操作ログ一覧] 画面で「オンライン」の期間）より前の場合は、取得した操作ログは保存されません。

参考 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できない場合に、エージェントを導入したコンピュータで操作ログを一時的に保存できます。一時的に保存できる操作ログは、最大 1,000 時間分です。

(2) 操作ログの自動バックアップ

コンピュータから取得した操作ログは、管理用サーバのデータベースに格納されます。操作ログは約 1 か月分を参照できますが、過去の操作ログを参照したい場合はバックアップから取り込む必要があります。操作ログを自動でバックアップするように設定している場合、前日分までの操作ログが、毎日自動でバックアップされます。このため、必要なタイミングで過去の操作ログを確認できます。

操作ログの自動バックアップは、セットアップで設定します。

参考 データベースマネージャを使用すると、操作ログを含む JP1/IT Desktop Management のデータベース全体をバックアップできます。

バックアップされるデータ

次の条件を満たす操作ログのデータがバックアップされます。なお、バックアップは毎日 4:00 に実行されます。

- 自動バックアップが実行された日の、前日までの操作ログ
- バックアップされていない操作ログ

操作ログのバックアップのデータは、ZIP ファイルに圧縮され、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。格納されるデータの形式を次に示します。

種類	ファイル名	説明
DATA ファイル	OPR_DATA_**YYYYMMDD**.zip	日付ごとの操作ログのデータです。**YYYYMMDD** は、バックアップを取得した日付が設定されます（YYYY：年、MM：月、DD：日）。同じ日付のファイルが存在する場合は、上書きされます。
OTHER ファイル	OPR_OTHER.zip	操作ログのバックアップ用データです。2 回目のバックアップ以降は、すでに格納されている OTHER ファイルを上書きしま

種類	ファイル名	説明
		す。なお、手動でバックアップする場合は、「操作ログの保管先フォルダ」とデータベースの「バックアップ先フォルダ」に同じファイルを作成します。

バックアップデータの容量

次に示す条件で操作ログとバックアップの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：100 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：10%

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）

100 台の操作ログのデータサイズ：1（メガバイト）×100（台）＝ 100（メガバイト）

100 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：100（メガバイト）×20（日）＝約 2（ギガバイト）

バックアップのデータサイズ

1 台当たりのバックアップのデータサイズ：1（メガバイト）×10%＝約 100（キロバイト）

100 台のバックアップのデータサイズ：100（キロバイト）×100（台）＝約 10（メガバイト）

100 台の 1 か月（出勤日 20 日）当たりのバックアップのデータサイズ：10（メガバイト）×20（日）＝ 200（メガバイト）

このようにして、操作ログとバックアップ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バックアップ用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

バックアップ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。

自動でのバックアップに失敗した場合

バックアップ先のドライブの容量が不足していたことが原因で自動バックアップが失敗した場合、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

1 日に 1 回、バックアップ先のドライブの空き容量が取得されます。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。

(3)　管理用サーバへの操作ログの取り込み

管理用サーバで管理する操作ログ一覧に表示されていない操作ログを調査したい場合に、自動的にバックアップされた操作ログを取り込んで、追跡したり詳細を確認したりできます。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。

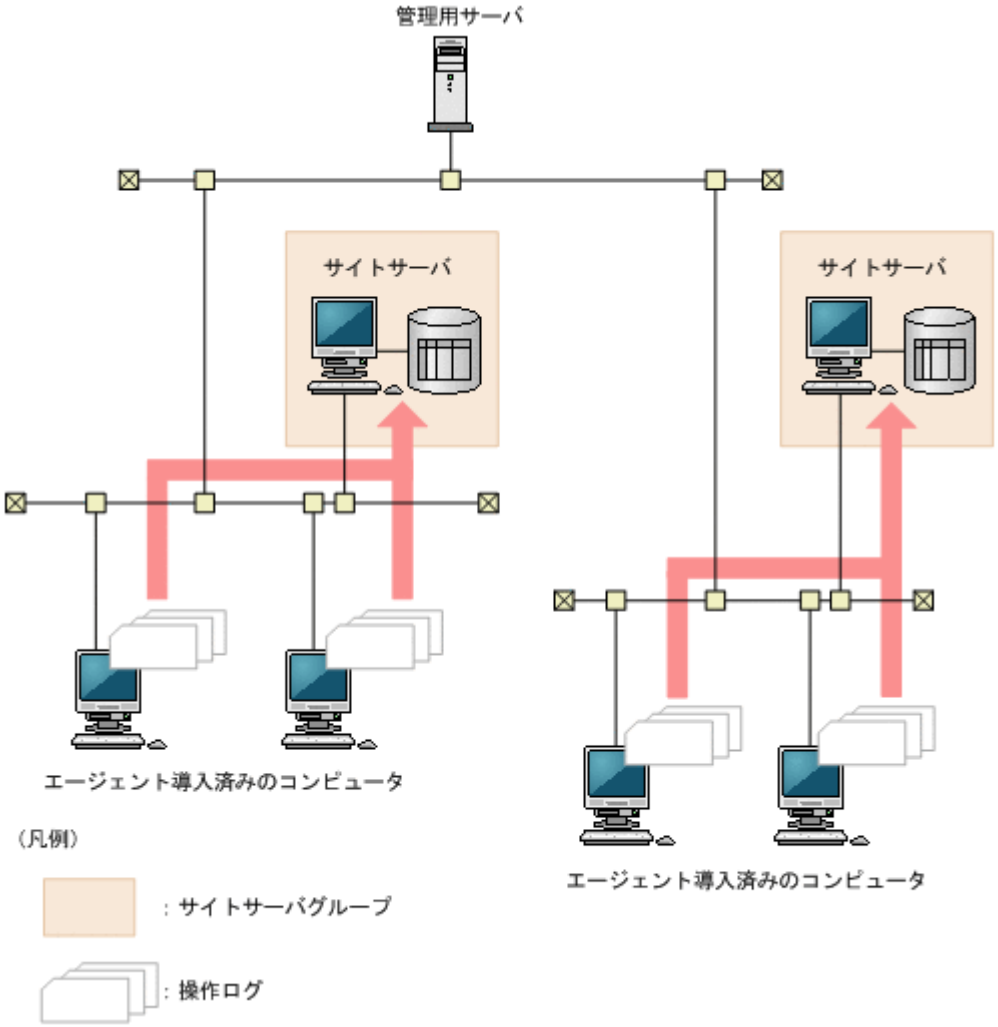
ただし、操作ログ用データベースの最大容量を超えた場合は、超過分は取り込まれません。

参考 データベースマネージャまたはコマンドでデータベースをリストアした場合、リストア実行日から過去 7 日間分の操作ログが操作ログ用データベースにリストアされます。これ以外の期間の操作ログを表示したい場合は、操作ログをバックアップから取り込む必要があります。

2.10.3 サイトサーバでの分散操作ログの管理

サイトサーバ構成システムの場合、エージェント導入済みのコンピュータから取得した操作ログをサイトサーバに分散して保管することで、管理用サーバのディスク容量の圧迫やネットワーク負荷の増大を防止できます。このような、サイトサーバに保管される操作ログを、分散操作ログと呼びます。

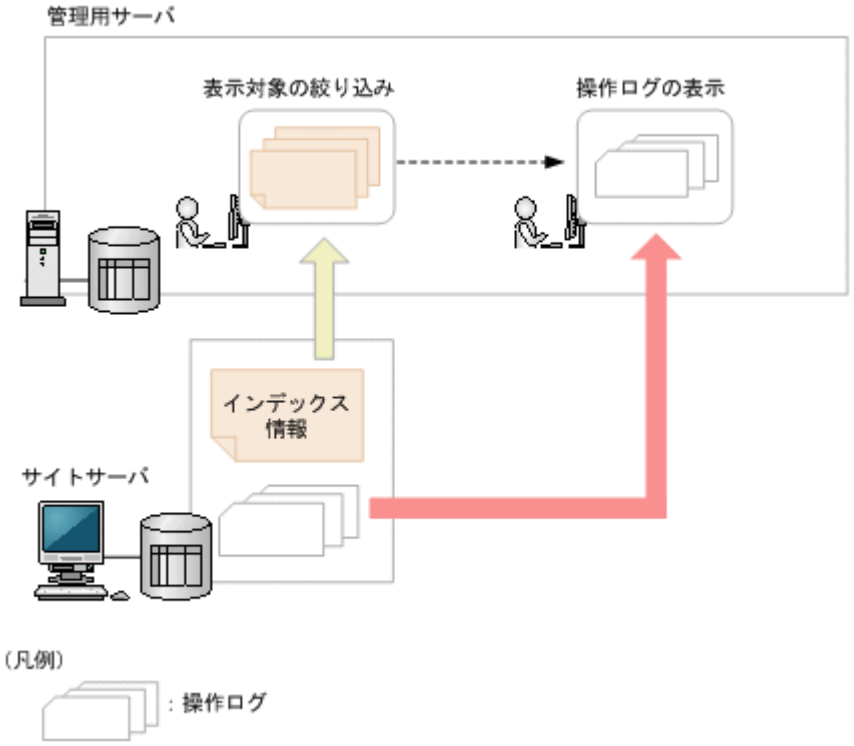
サイトサーバに操作ログを保管する場合、ネットワークセグメントごとに、操作ログを保管するサイトサーバを指定します (サーバ構成の設定)。エージェント導入済みのコンピュータから取得した操作ログを、指定したサイトサーバに分散して保管します。



注意 コンピュータが、サイトサーバグループに登録されたすべてのサイトサーバと接続が失敗した場合、操作ログはサイトサーバおよび管理用サーバには通知されないで、コンピュータ内に一時保存されます。コンピュータに一時保存できる操作ログは最大 1,000 時間分です。1,000 時間分を超過すると、古い操作ログから順に削除されます。一時保存された操作ログは、次回コンピュータがサイトサーバに接続できたタイミングで通知されます。

サイトサーバに操作ログを保管する場合、収集した操作ログはサイトサーバのデータベースに保管されます。管理用サーバとは異なり、操作ログのデータベースは収集した分だけ単調増加します。自動バックアップや古い操作ログの自動削除はされません。このため、ハードディスク容量が不足するときは、保管先の変更、ハードディスクの増設、不要な操作ログの削除などをして対処してください。ほかのサイトサーバに操作ログのデータを移動してもかまいません。なお、サイトサーバの空きディスク容量が少なくなると、操作画面にイベントが通知されます。

分散操作ログは、セキュリティ画面の［操作ログ（分散操作ログ）］画面から参照できます。参照する場合は、サイトサーバから管理用サーバに通知される操作ログのインデックス情報を基に、操作ログを表示する対象を絞り込む必要があります。なお、バックアップした操作ログをサイトサーバに取り込んで、古い操作ログを参照できます。ただし、管理用サーバでバックアップした操作ログは、サイトサーバで取り込めません。また、サイトサーバでバックアップした操作ログは、管理用サーバで取り込めません。



注意 サイトサーバ上で手動で操作ログを削除したり、管理用サーバでインデックス情報のファイルが破損したりして、操作ログのインデックス情報と実際のデータに差異がある場合は、サイトサーバに保管された操作ログを正しく参照できません。このような場合は、recreatelogdb コマンドを利用してインデックス情報を作成し直してください。
なお、recreatelogdb コマンドの実行中はサイトサーバが停止するため、その間に発生した操作ログ（不審と見なす操作を含む）は、コマンド実行が完了するまで確認できません。recreatelogdb コマンド完了後、サイトサーバを開始したタイミングで、操作ログのインデックス情報の作成を開始します。インデックス情報の作成中はサイトサーバの負荷が高くなるため、操作ログのデータ量によっては、作成が完了するまでに数日掛かることがあります。また、インデックス情報の作成中に取得した操作ログは、インデックス情報の作成が完了するまで確認できないため、不審と見なす操作の検知が遅れるおそれがあります。これらの事項の影響を考慮して recreatelogdb コマンドを実行してください。

注意 分散操作ログが取得されていない場合、［操作ログ（分散操作ログ）］画面は表示されません。

注意 サイトサーバに保管された操作ログと管理用サーバに保管された操作ログは、同時には参照できません。このため、サイトサーバを利用する場合は、サイトサーバだけに操作ログを保管し、管理用サーバには操作ログを保管しないことをお勧めします。

関連リンク

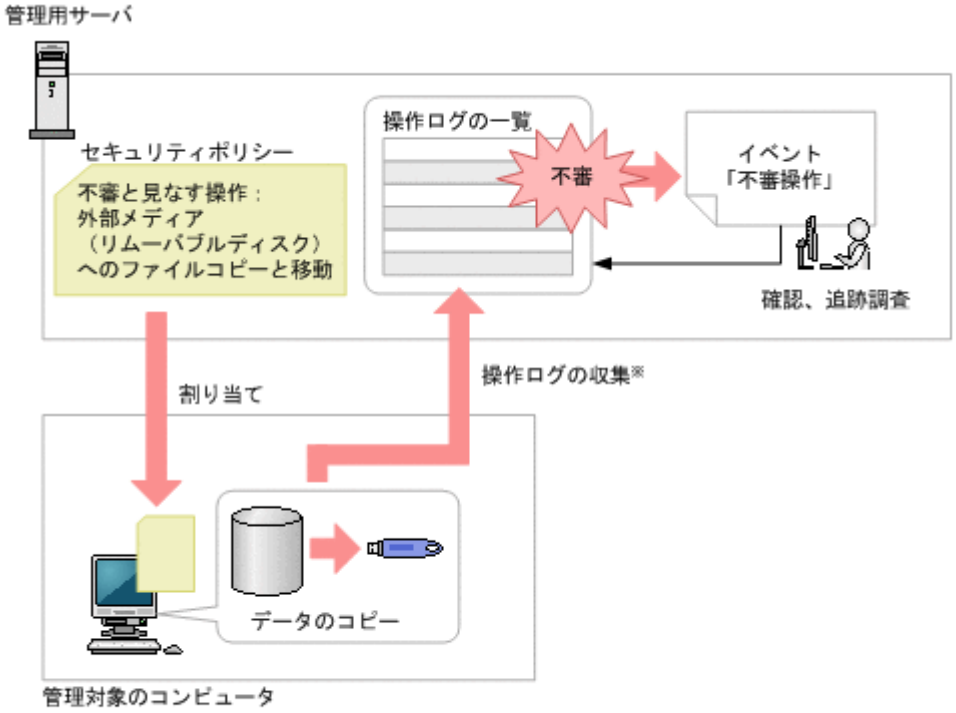
- 2.10.1 取得できる操作ログの種類
- 4.4.3 サイトサーバ構成

2.10.4 操作ログに基づく不審操作の調査

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。操作ログを収集して不審操作を検知させることで、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。



注※　サイトサーバ構成システムを構築している場合、サーバ構成の設定に従ってサイトサーバまたは管理用サーバに収集されます。

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。

参考　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) 監視できる不審操作の種類

(1)　監視できる不審操作の種類

JP1/IT Desktop Management では、操作ログの内容を自動的にチェックして、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 サーバまたは FTP サーバにアップロード
- 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
- 設定した基準値を超える大量印刷

監視対象になるファイルは次の条件を満たすものです。

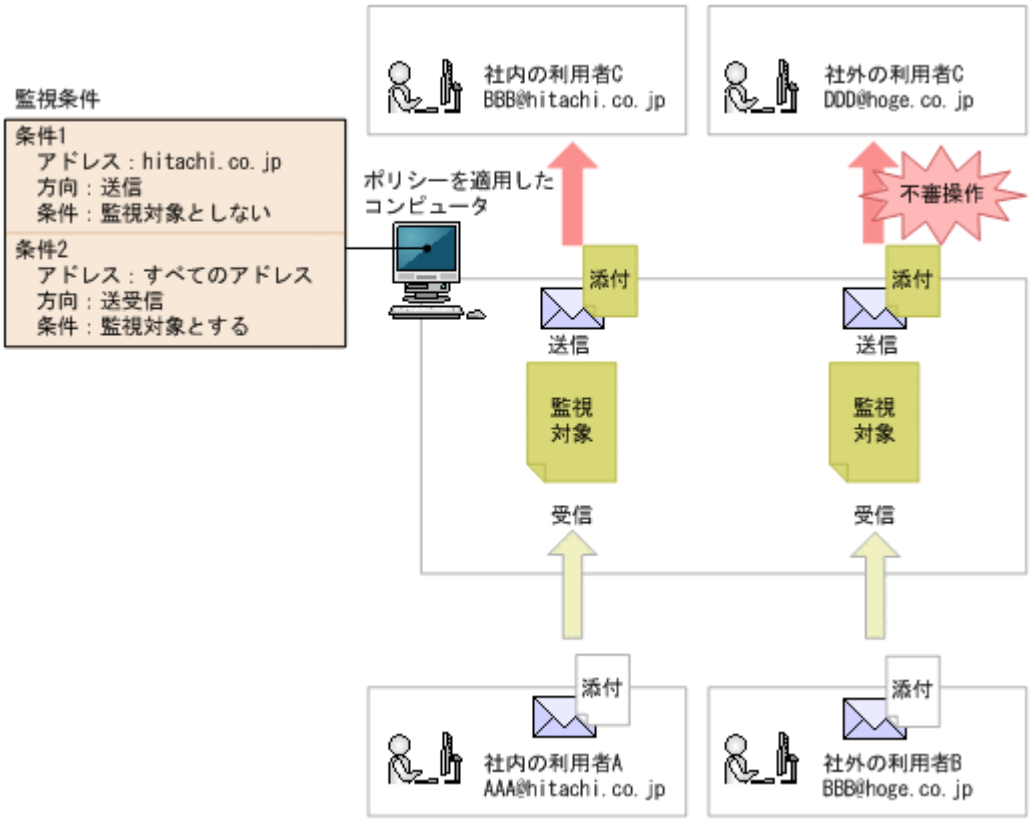
- ポリシーに設定したメールアドレスから添付で受信したファイル
- ポリシーに設定した Web サーバまたは FTP サーバからダウンロードしたファイル
- 組織内で新たに作成したファイル
- 操作ログを取得する前から組織内にあるファイル

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。

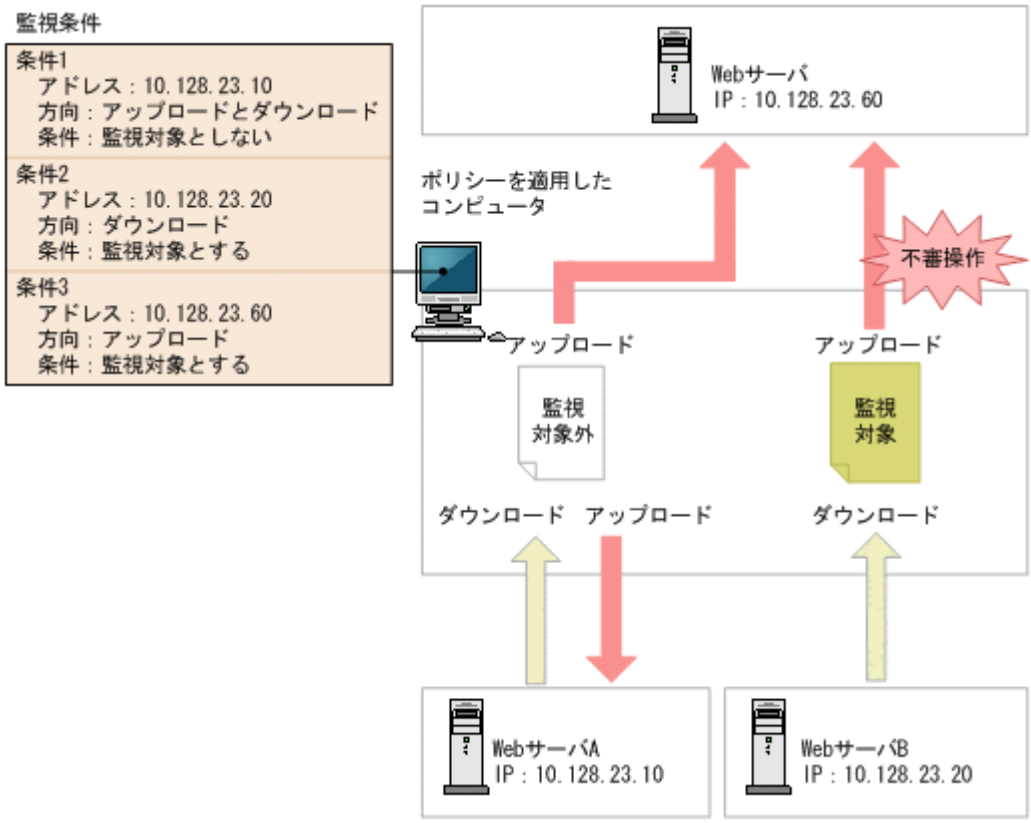
- 社外への添付ファイルの転送は監視する。
- 社内（アドレスが「hitachi.co.jp」）での、添付ファイルの転送は監視しない。



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※1、2、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。

注意 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（大量印刷の不審操作は除きます）。

2.10.5 操作ログ取得の前提条件と注意事項

ここでは、各操作ログを取得するための前提条件と注意事項について説明します。

(1) プログラムの起動と抑止で取得される操作ログの情報と注意事項

管理者が不正と判断したプログラムや、使用を制限するプログラムに対して、プログラムの起動を抑止できます。管理者がプログラムをセキュリティポリシーに設定すると、プログラムの起動を許可したり、抑止したりします。プログラムの起動と抑止で取得される操作ログの情報と注意事項を次に示します。

取得される操作ログの情報

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です。

- exe
- com
- scr

次に示すプログラムは、プログラム起動および抑止のログは取得されません。

- cacls.exe

- cmd.exe
- cscript.exe
- conime.exe
- jdngsetup.exe
- netsh.exe
- secedit.exe

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、プログラム起動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、プログラムの起動と抑止の操作ログが取得でき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

(2) 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する］がチェックされている必要があります。なお、Windows Server 2008、Windows Server 2003 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 - Agent」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。
- Firefox の場合、［ツール］－［アドオン］を選択すると表示される［拡張機能］で、「JP1/IT Desktop Management - Agent」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。

参考 エージェントが導入されたコンピュータの Web ブラウザに監視用のアドオンが追加されます。このアドオンによって、Web アクセス、HTML フォームや Javascript によるファイルのアップロード、ダウンロードが検知されます。アドオンが監視・検知する操作を次に示します。

- Internet Explorer 6、7、8、9 の場合

  Web アクセスを監視・検知します。なお、ファイルのアップロード、およびダウンロードは、エージェントで監視・検知します。
- Firefox 3.5、3.6、4、5 の場合

  Web アクセス、ファイルのアップロード、およびダウンロードを監視・検知します。

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 アクセスログを取得できます。
- Internet Explorer 6 の環境で、Windows のエクスプローラから Web アクセスした場合、エクスプローラからの Web アクセスとなるため、Web アクセスの操作ログは取得できません。

- 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 アクセスログが取得できないことがあります。
- 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 アクセスログが取得できることがあります。

関連リンク

- 2.10.1 取得できる操作ログの種類

(3) 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。なお、ログオン中のすべての利用者の操作ログを取得できます。

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。または、シェルでファイルの保存操作をした Web ダウンロード、FTP 受信、添付ファイル保存である。
- 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。またはシェルでファイルの保存操作をした Web ダウンロード、FTP 受信、添付ファイル保存である。

- ファイルパスが次のどれかのフォルダ（サブフォルダ含む）である。
  - **JP1/IT Desktop Management - Agent のインストール先フォルダ**¥agent¥
  - **JP1/IT Desktop Management - Agent のインストール先フォルダ**¥log¥
  - **JP1/IT Desktop Management - Agent のインストール先フォルダ**¥remocon¥

注意事項

- 利用者がファイルまたはフォルダをコピーして、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場合があります。
- 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。

OS が Windows 7、Windows Server 2008 または Windows Vista 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 7、Windows Server 2008 または Windows Vista 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 Vista 以降で、権限昇格が必要なディレクトリから 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うことによ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［元に戻す］メニューを選択した場合、ファイル削除の操作ログが取得されます。なお、Windows の［ごみ箱］によるファイル削除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

(4) 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。

なお、ファイルのアップロードとダウンロードを検知するために、エージェントを導入しているコンピュータの Web ブラウザに監視用のアドオンが追加されます。アドオンの対象となる Web ブラウザについては、「(2) Web アクセスの操作ログ取得の前提条件と注意事項」を参照してください。

前提条件

- Firefox の場合、エージェントを導入しているコンピュータに追加されるアドオンが有効となっている必要があります。

注意事項

- Firefox の場合、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 アップロード、ダウンロードは取得されません。
- 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。
- Firefox の場合、ダウンロードするファイルの HTTP レスポンスヘッダの Content-type エンティティが text/*である場合、Web ダウンロードのログは取得されません。

- Internet Explorer 6 からの Web ダウンロードで、[名前を付けて画像を保存] をした場合、Web ダウンロードの操作ログは取得されません。
- 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。

関連リンク

- 2.10.1 取得できる操作ログの種類

(5) 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 Express	6
Microsoft Outlook	2002
	2003
	2007
	2010
Windows メール	6
Windows Live メール	2009、2011

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ません。このため、ファイルの追跡や、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。

関連リンク

- 2.10.1 取得できる操作ログの種類

(6) 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 Express	6
Microsoft Outlook	2002
	2003
	2007
	2010
Windows メール	6
Windows Live メール	2009、2011

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 Vista 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
- Outlook 2007、Outlook 2010 で、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。
- 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を取得できません。
- 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

(7) 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) Web アクセスの操作ログ取得の前提条件と注意事項」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 によるファイル送信、受信は操作ログを取得できません。
- FTP 受信ログは、Internet Explorer 6 の場合、操作元ファイル名には FTP サーバの IP アドレスが取得されます。また Internet Explorer 7、8 の場合、操作元ファイル名には URL が取得されます。
- FTP 送信ログの操作先ファイル名には FTP サーバの IP アドレスが取得されます。

関連リンク

- 2.10.1 取得できる操作ログの種類

(8) 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、またはほかのコンピュータに接続されているプリンタ	○ ※
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

- プリンタのプロパティのアクセス許可で、すべてのログオンユーザーに［印刷］および［ドキュメントの管理］の［許可］がチェック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、プリンタサーバとなる機器で、印刷操作をした機器の名前解決ができる必要があります。
- ネットワーク共有プリンタ、またはほかのコンピュータに接続されたプリンタの場合、 コントロールパネルの［Windows ファイアウォール］－［Windows ファイアウォールによるプログラムの許可］－［例外］タブで「ファイルとプリンタの共有」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、またはほかのコンピュータに接続されたプリンタの場合、管理対象となるコンピュータで Win32_PrintJob クラスがサポートされた WMI が起動されている必要があります。

注意事項

- プリンタをインストールする際のテスト印刷は、印刷操作の操作ログが取得できないことがあります。

- ログオン直後に印刷を実行した場合、印刷操作の操作ログが取得できないことがあります。
- 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。
- ネットワーク共有プリンタ、またはほかのコンピュータに接続されたプリンタの場合、Windows Vista をプリンタサーバとしたネットワーク共有プリンタ環境では印刷操作の操作ログは取得できません。

関連リンク

- 2.10.1 取得できる操作ログの種類

(9) 外部メディア操作の操作ログ取得の注意事項

外部メディアを機器に接続または切断した操作ログを取得できます。外部メディアを接続または切断した操作ログは、ドライブが追加されたことを契機に取得します。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。外部メディア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。
- 外部メディアをコンピュータから取り外した場合、該当するドライブが存在しない状態になるため、外部メディアの種別が「その他」となることがあります。
- シリアルナンバーがサポートされている USB デバイスを接続した場合、前回接続時のドライブ名（ドライブレター）が USB デバイスに割り当てられます。この場合、ドライブ名の重複によって接続が失敗すると、前回接続時のドライブ名で情報が取得されます。
- マルチスロットのメモリカードなど、接続すると複数のドライブが割り当てられる機器を接続した場合は、ドライブごとに複数の接続の情報を取得できます。なお、同じ機器を切断（取り外し）した場合には、ドライブ一つの切断の情報だけを取得できます。
- 初めて機器に接続される外部メディアの場合、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。
- 外部メディアが取り外しできる MO ドライブやカードリーダーなどのデバイスで、デバイス接続時に外部メディアが挿入されていない場合、デバイス名、デバイスの種類、デバイスインスタンス ID、シリアルナンバーが取得できません。

関連リンク

- 2.10.1 取得できる操作ログの種類

(10) 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

- OS が Windows 7、Windows Server 2008、または Windows Vista の場合、ユーザー権限が昇格されたウィンドウの操作ログは取得できません。
- 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

(11) 持ち込み、持ち出しの検知対象の操作

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
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
ファイルダウンロード	△※2
ファイル送信	△※1
ファイル受信	△※2
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）	△※2
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、持ち込みではないと見なします。

注※2　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
ファイルダウンロード	△※4
ファイル送信	△※3
ファイル受信	△※4
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	△※4
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　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	×	×	△※	△※	×	△※
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※　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

(12)　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

エージェントが導入されたコンピュータに不審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。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

- 操作元ファイルまたは操作先ファイル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

- 代替ストリームが付加されたファイルを、代替ストリーム機能がないファイルシステム（FAT など）に移動しコピーした場合、代替ストリームが削除されるため、不審操作として検出されません。また、ファイルを圧縮、解凍などしてデータを加工した場合、代替ストリームが削除されるため不審操作として検出されません。
- 代替ストリームが付加されたファイルを代替ストリーム機能がないファイルシステムに、エクスプローラ上で移動、コピーする場合、ダイアログが表示されます。

関連リンク

- 2.10.1 取得できる操作ログの種類

2.11 資産の管理

JP1/IT Desktop Management 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。

JP1/IT Desktop Management 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 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。

参考 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。

参考 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や構成などを電子データ化して登録しておくと、	管理者が入力	−

管理項目	説明	入力方法	データ型
	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。		
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。	―	―
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
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

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。	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
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

管理項目	説明	入力方法	データ型
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

（凡例）－：対象外

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］画面から利用者に入力できます。

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。

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。 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。	－	－

管理項目	説明	入力方法	データ型
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
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	ソフトウェアの販売会社を設定します。	管理者が入力	テキスト型
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。	－	－

（凡例）－：対象外

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。	－	－
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。	－	－

管理項目	説明	入力方法	データ型
メーカー	ソフトウェアの製造元が表示されます。	管理者が入力	テキスト型および選択型※
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。	－	－

（凡例）－：対象外

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。契約書の証書や構成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	テキスト型
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

管理項目	説明	入力方法	データ型
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
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。	－	－

（凡例）－：対象外

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。

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

[ハードウェア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。

参考 ［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	○	×	×	×	×	×	×
英数記号以外の文字	○	×	×	×	×	×	×

（凡例）○：入力できる　×：入力できない

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）	○	×	×

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）
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	○	○	○

（凡例）○：入力できる　×：入力できない

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	×	×	×	○
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	×	×	×	×

（凡例）○：入力できる　×：入力できない

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、次の四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。

注意 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

ハードウェア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。［ハードウェア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。［資産状態］と［機器種別］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。

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。

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。

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
ハードウェア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。

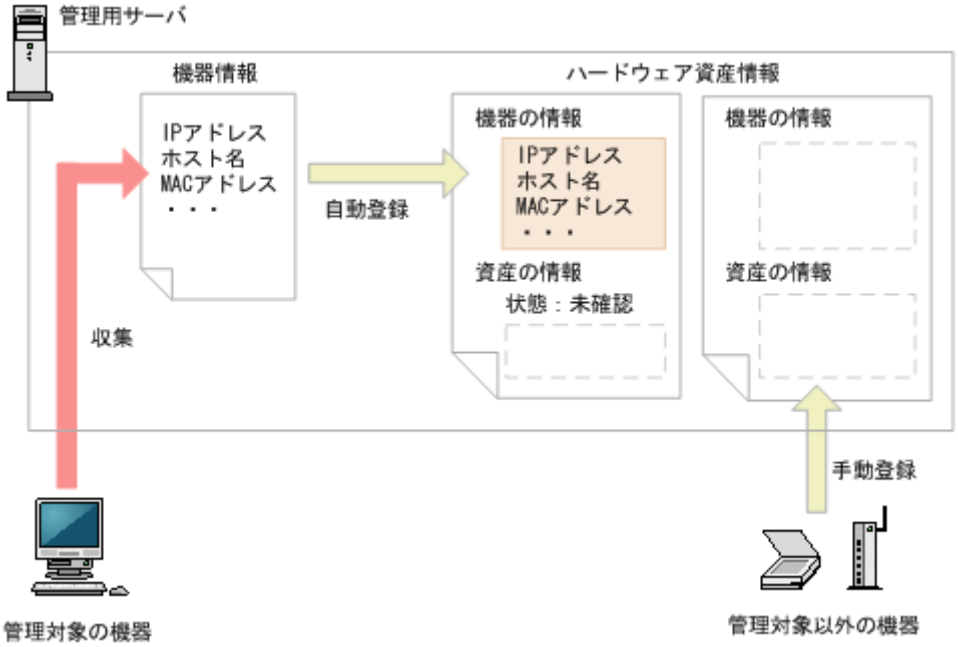
関連リンク

- 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。

参考 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 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。

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。
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。

契機	説明
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は削除されません。 ［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。

(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。登録済みのハードウェア資産情報が存在する場合は、登録された機器情報との引き当て（同定）が行われます。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。

機器情報とハードウェア資産情報の同定は、次の項目を基に実行されます。

1. IMEI※
2. シリアルナンバー
3. ホスト名
4. MAC アドレス
5. 契約電話番号※
6. IP アドレス

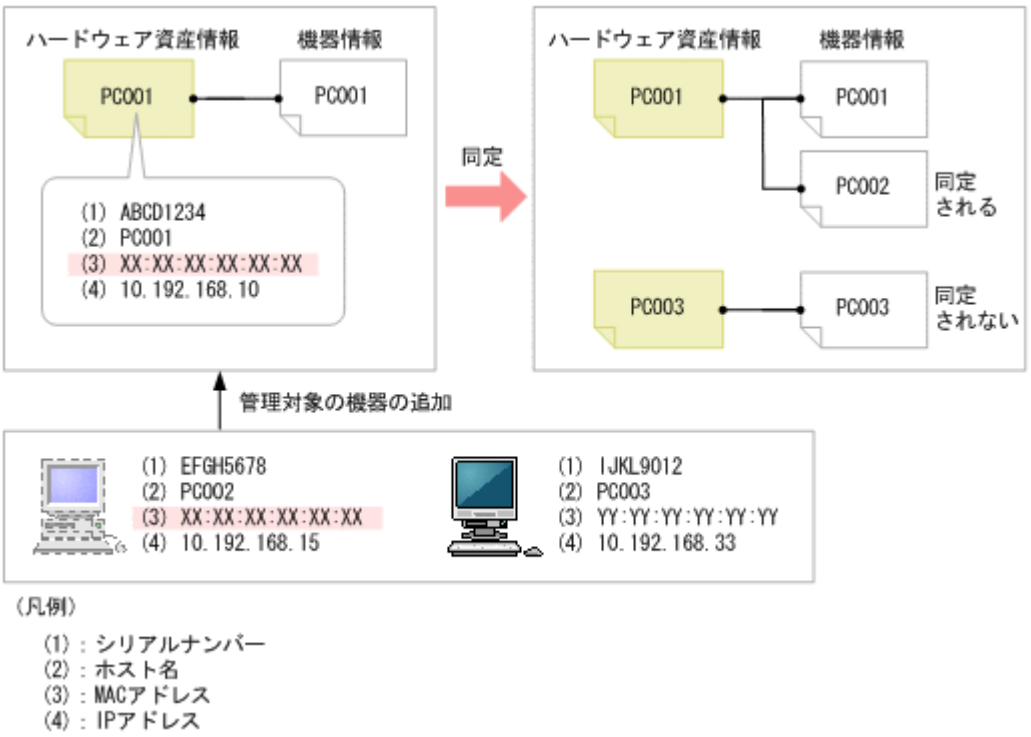
注※　MDM 製品と連携してスマートデバイスを管理する場合に、利用されます。

上位の項目から順に値が一致するかどうかが比較され、一致する項目が存在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ます。同定されると、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。

値が一致する項目が存在しない場合は、同定する情報はなしと判断され、ハードウェア資産情報が新規に登録されます。

例えば、物理コンピュータ上で稼働している仮想コンピュータを新たに管理対象にする場合、物理コンピュータと仮想コンピュータの MAC アドレスが同じときは、物理コンピュータのハードウェア資産情報に同定されます。これによって、物理コンピュータのハードウェア資産情報に、物理コンピュータと仮想コンピュータの機器情報が関連づけられ、実態のとおりに管理できます。

コンピュータを管理する場合の、機器とハードウェア資産の同定の概念を次に示します。



注意 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、手動で対応づけをしてください。

(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、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、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。

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。利用者に入力してもらうように項目を設定すると、自動的に、利用者のコンピュータに［利用者情報の入力］画面が表示されるようになります。

なお、［利用者情報の入力］画面は、一定の間隔で利用者のコンピュータに表示できます。

(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、減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

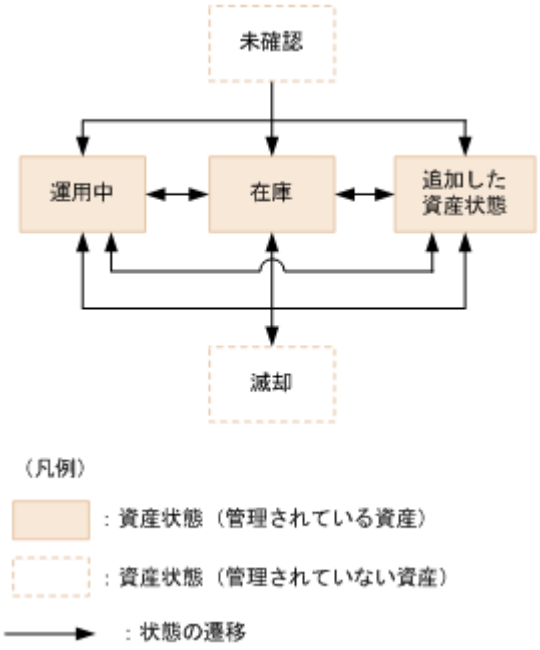
資産が運用中（使用中）であることを意味します。

減却

資産が減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。管理が不要になった資産は、資産状態を「減却」に変更します。なお、「減却」にした資産を「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。

なお、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。

参考 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。

(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 は機器のネットワーク接続または機器の利用者の入力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。

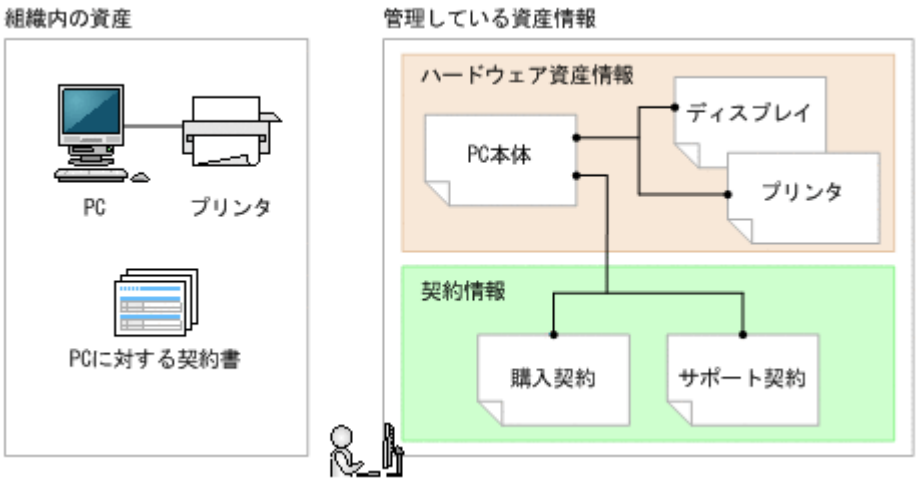
参考 ハードウェア資産情報およびソフトウェアライセンス情報をインポートして、［棚卸日］を一括更新することもできます。この場合は、各資産情報の［棚卸日］に異なった日付を設定できます。

(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。

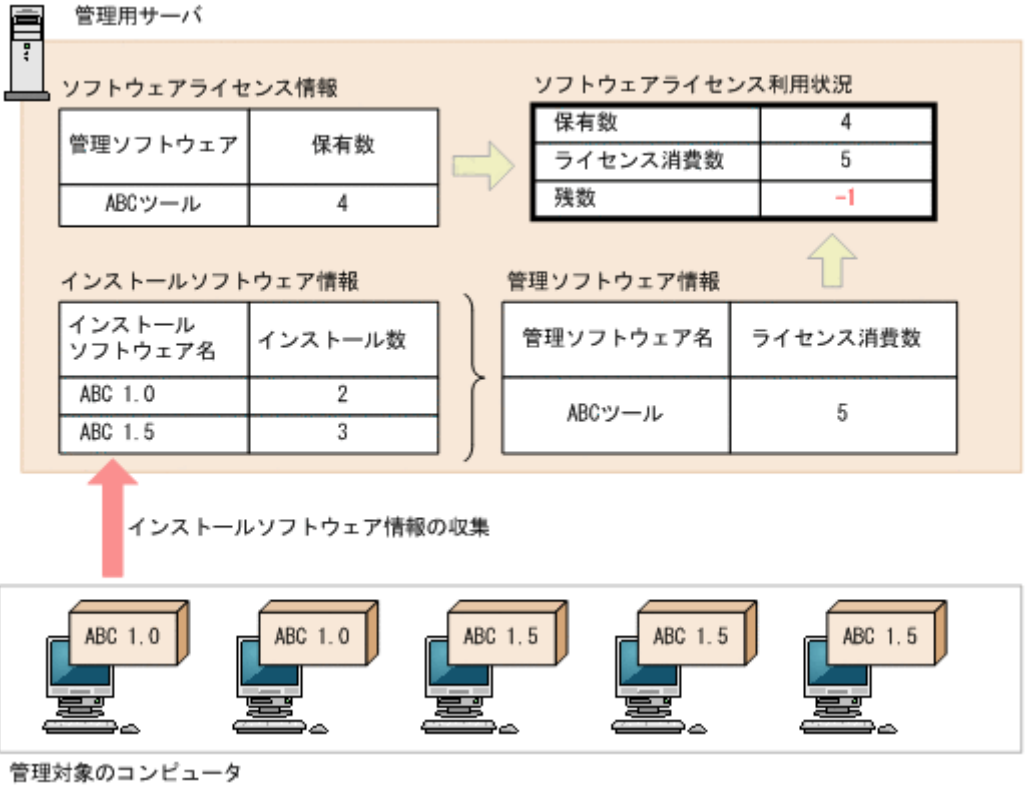
ほかのハードウェア資産情報との関連づけを設定することで、各コンピュータの本体、ディスプレイ、および周辺機器をセットで管理できます。

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 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状況を把握する流れを次の図に示します。



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。

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集計され、利用実態を把握できます。また、対応するソフトウェアライセンス情報が設定されている場合は、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。

なお、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をコンピュータに割り当てることで、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るようになります。

注意 JP1/IT Desktop Management 09-51 から、ライセンス消費数のカウント方法が変更になりました。このため、09-50 からバージョンアップした場合は、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。09-50 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。09-51 からは、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。

(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。

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。

(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情報を登録して管理できます。

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の CSV ファイルを作成しインポートする方法があります。

ソフトウェアライセンスの割り当て先の変更、ソフトウェアの滅却、対象となる契約の追加や削除などがあった場合は、ソフトウェアライセンス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、ソフトウェアライセンス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。

ソフトウェアライセンス情報には、対応する契約情報を設定できます。

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

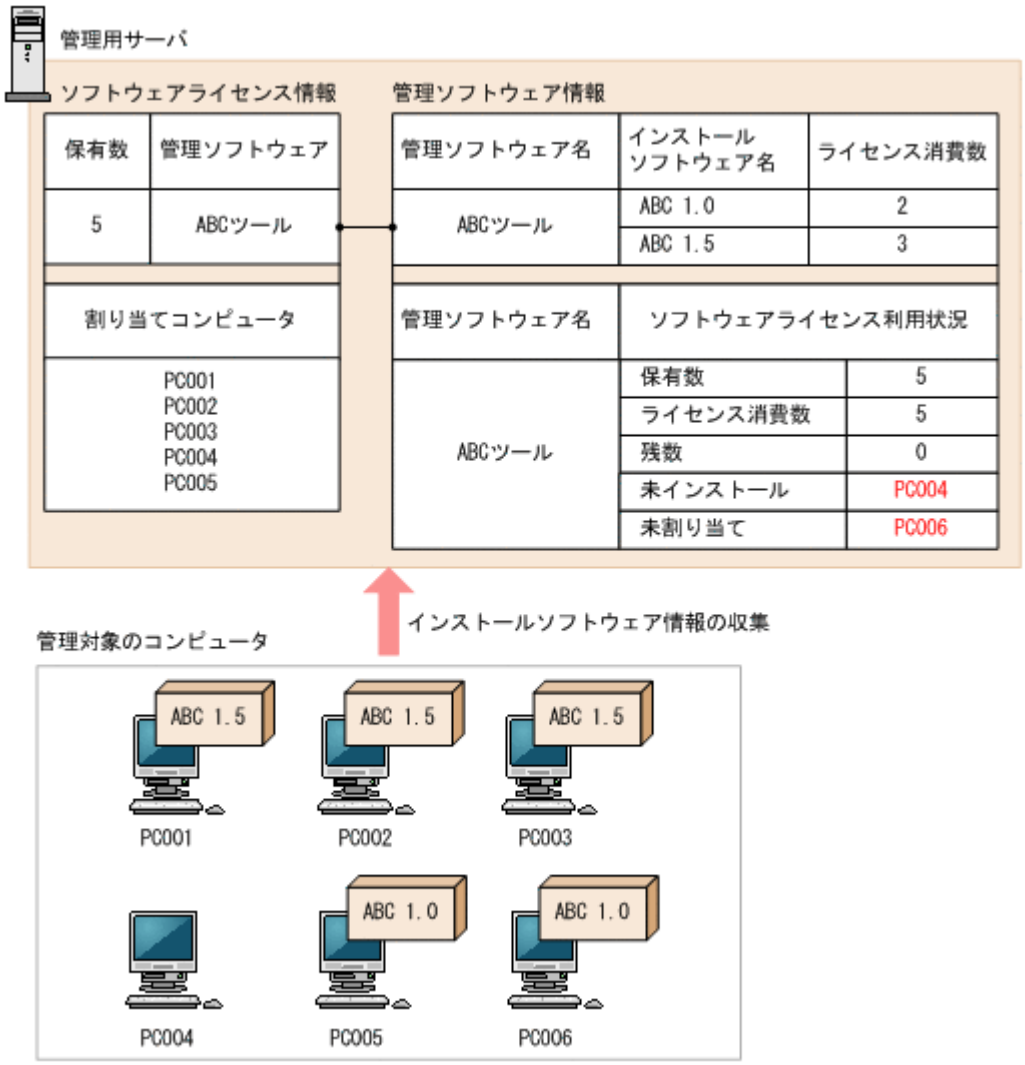
ハードウェア資産情報の場合、棚卸日を自動更新するように設定できます。JP1/IT Desktop Management は機器のネットワーク接続または機器の利用者の入力で機器の存在を確認します。機器の存在を確認できたら、棚卸日が自動更新されます。棚卸の手間を省きたい場合にお勧めします。

参考 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。

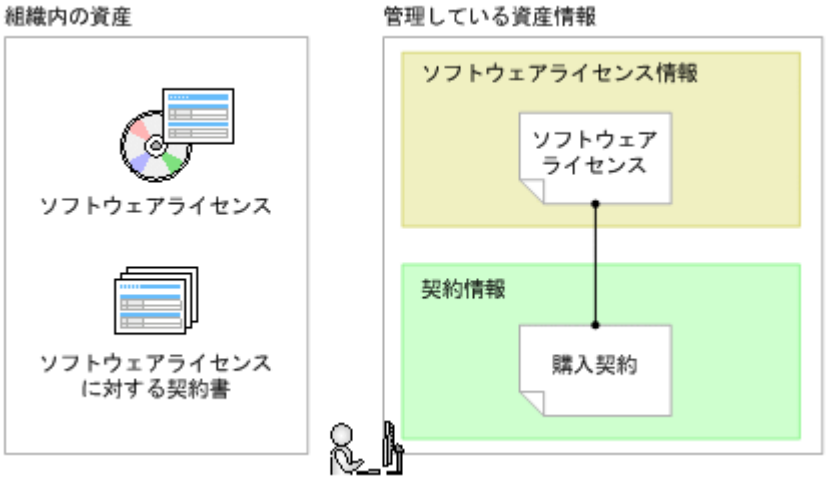
［インストール済みコンピュータ］タブでは、管理ソフトウェア情報に指定したソフトウェアがインストールされているコンピュータが表示されます。このタブで、［未割り当てコンピュータだけを表示する］をチェックしてソフトウェアライセンスを割り当てていないコンピュータを表示すると、未許可でソフトウェアをインストールしているコンピュータを把握できます。

［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。

(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。

(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。

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。

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。

参考 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

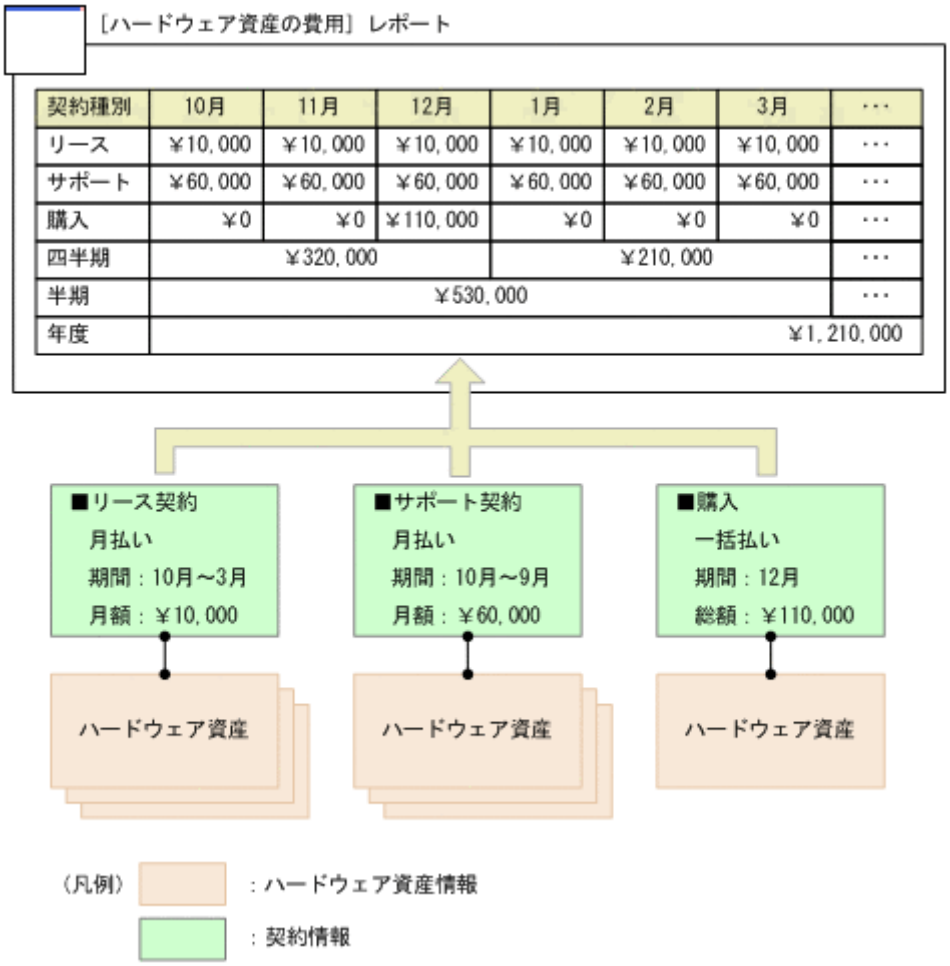
ハードウェア資産またはソフトウェアライセンスの運用に掛かる費用をレポートから確認できます。資産に掛かる費用は、［資産詳細レポート］の次のレポートで確認できます。

- ［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

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。

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。

参考 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。

(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

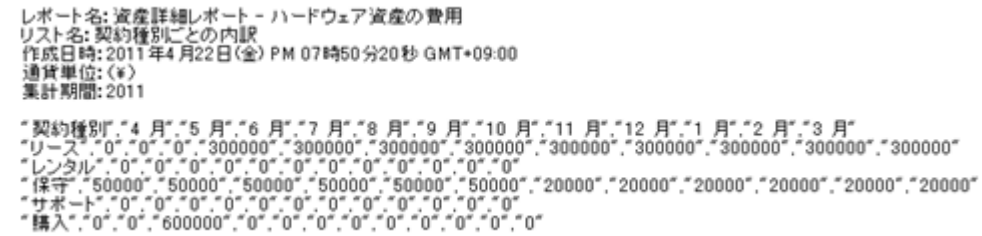
支払方法	計算方法
月払い	次の条件をすべて満たす契約情報について、「月額」を累計します。 ・ ［契約種別］が「XXX」になっている。 ・ ［支払い方法］が「月払い」になっている。 ・ ［契約対象のハードウェア資産］にハードウェア資産情報が関連づけられている。 ・ 指定した月に費用発生日が含まれる。 なお、「月払い」の費用発生日は、［契約期間］の契約開始日を基準として［契約期間］が終了するまで 1 か月ごとに出現します。 ［契約期間］が 2011/4/10～2011/6/10 の場合は、費用発生日は、2011/4/10、2011/5/10、2011/6/10 です。そのため、指定した月が 2011 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。 ・ ［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。

参考 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。

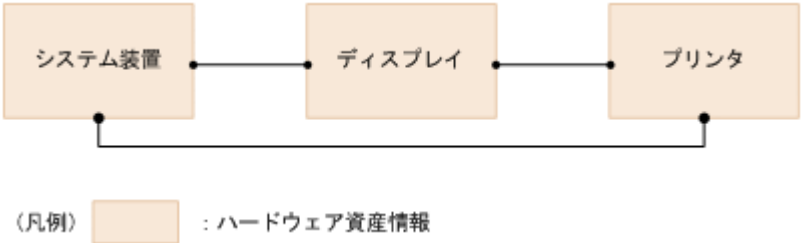
2.11.5 資産情報の関連づけ

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によって、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。



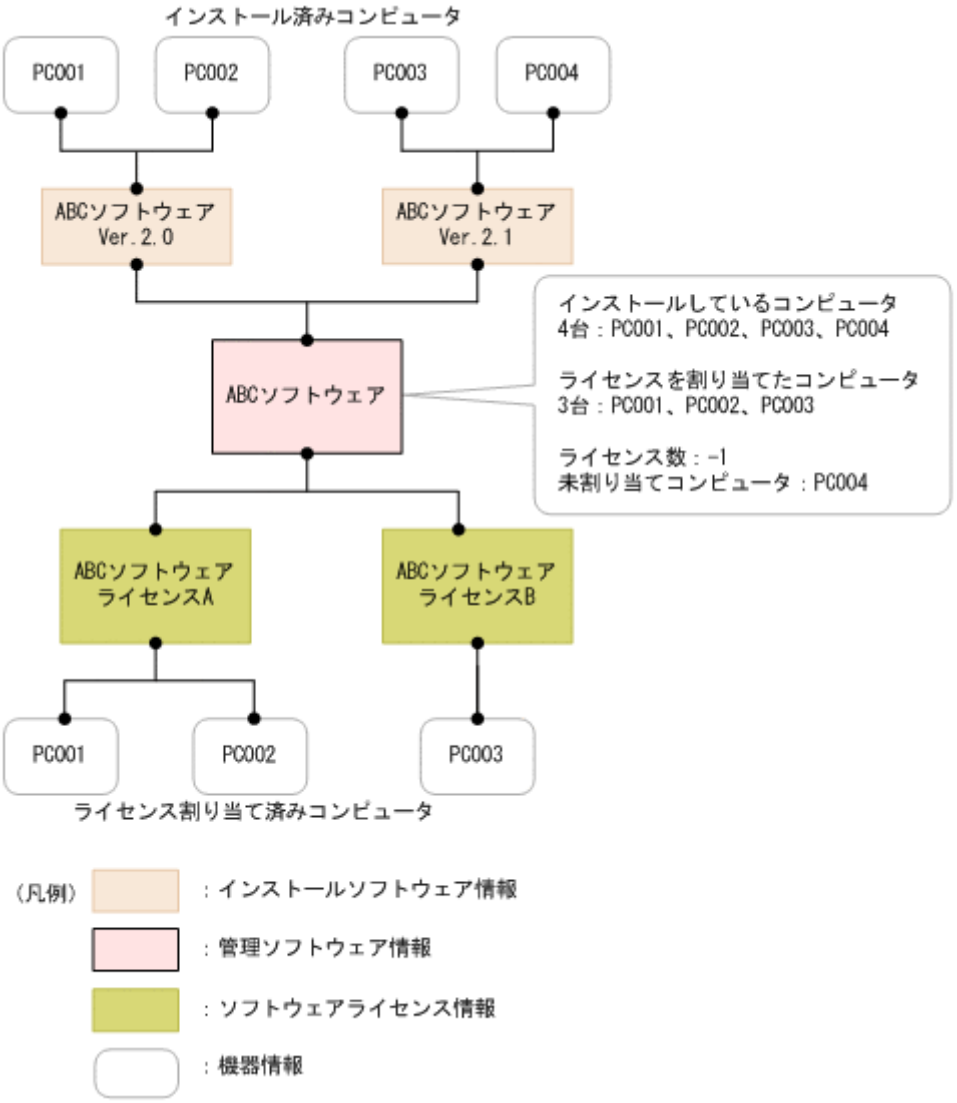
ソフトウェアライセンス情報、管理ソフトウェア情報の関連づけ

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、製品バージョンの違いを意識することなく、管理ソフトウェア単位にソフトウェアライセンス数を管理できます。

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。



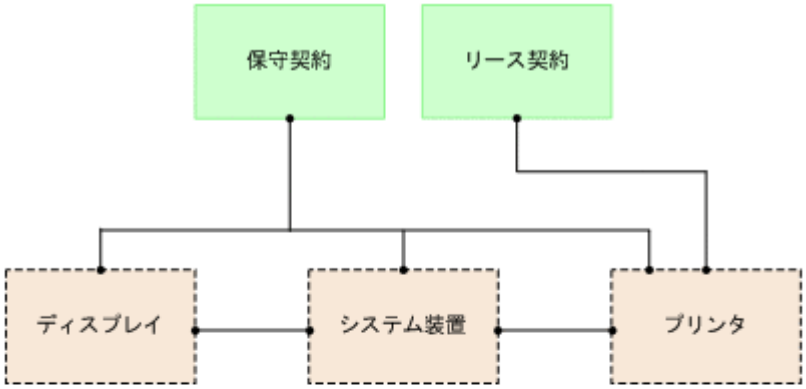
契約情報の関連づけ

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。

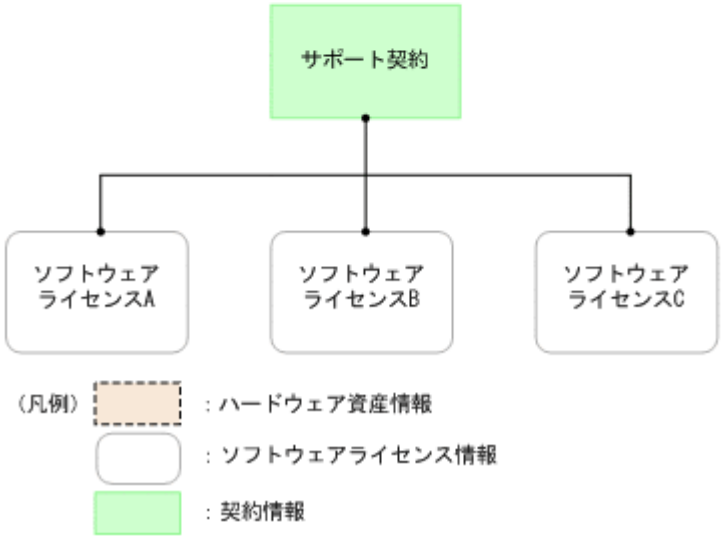
また、契約情報に費用を設定しておくと、ハードウェア資産やソフトウェアライセンスに掛かる費用を把握できます。

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。

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。

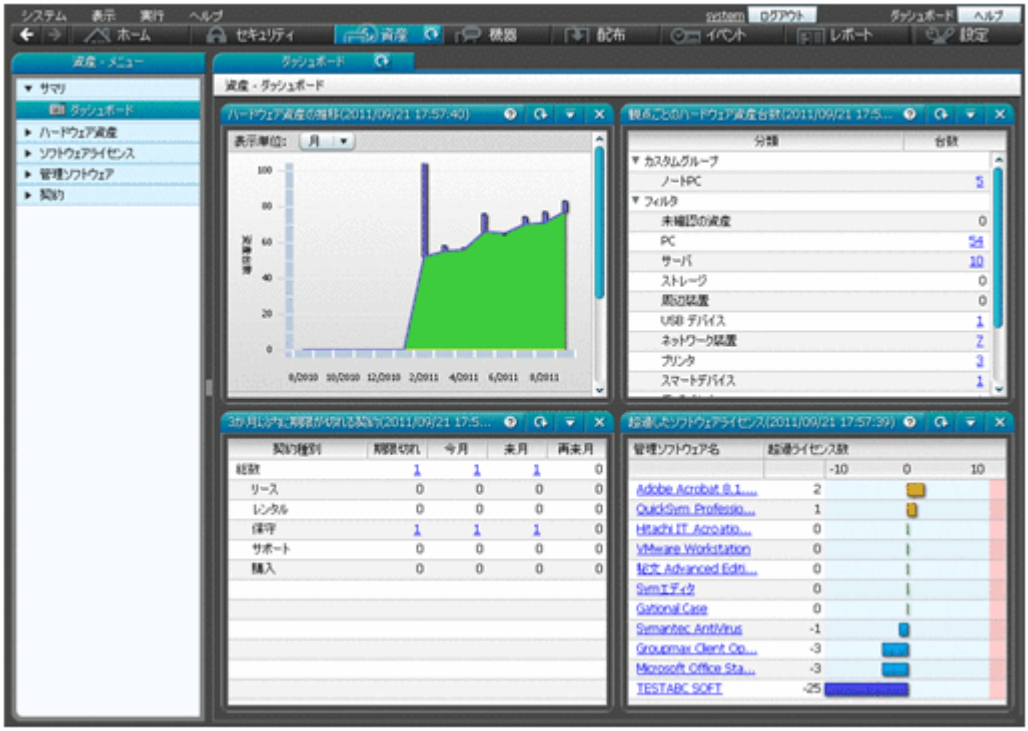
資産画面で確認する

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、［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。

参考　［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、「2.15 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。

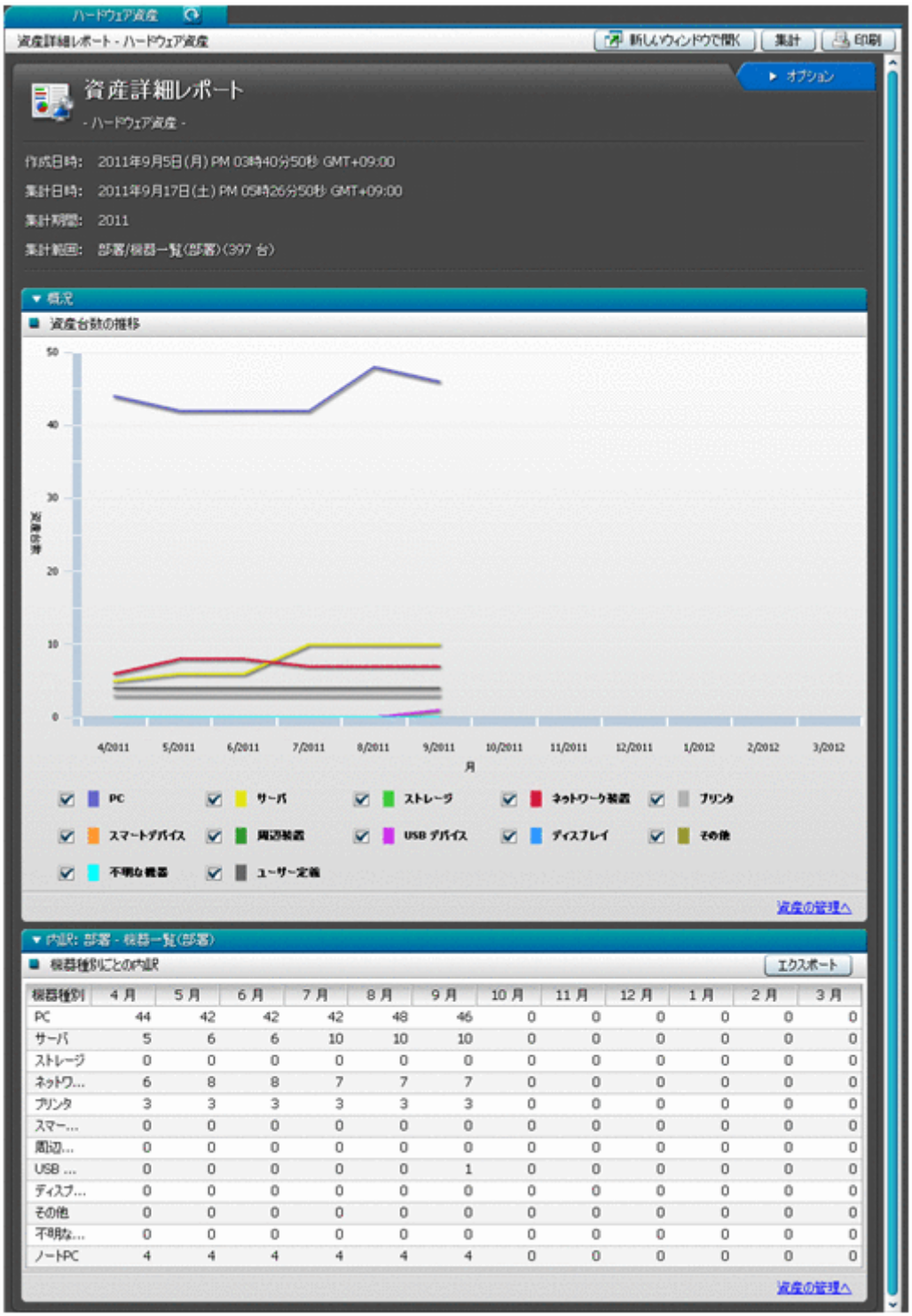
［契約］画面で確認する

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

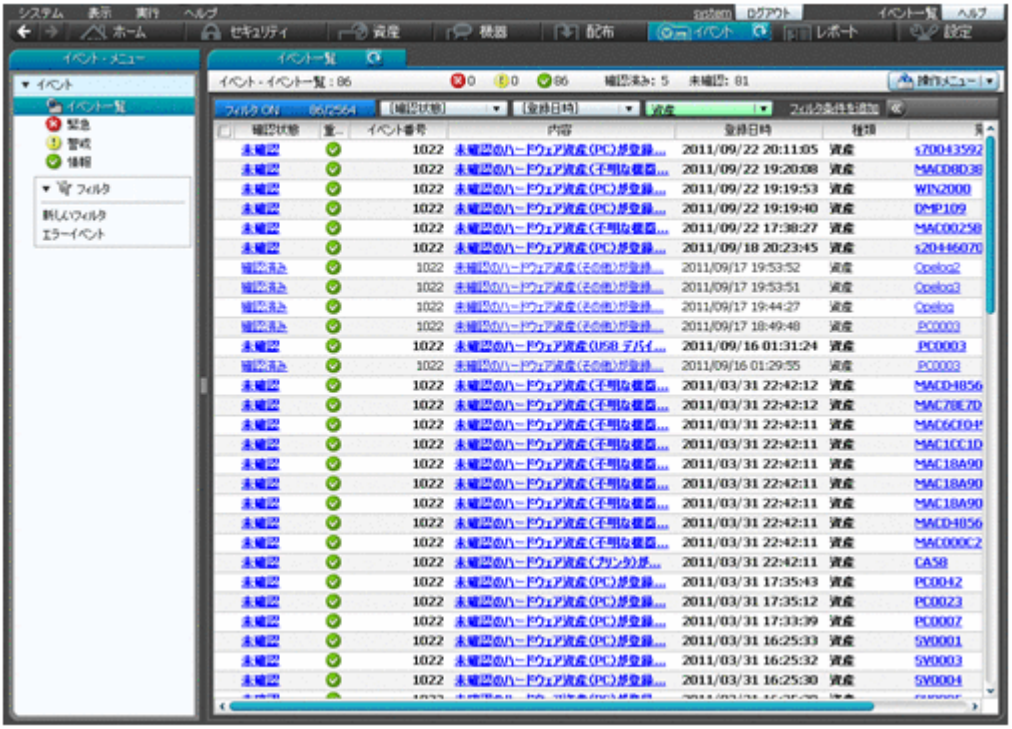
［ダイジェストレポート］、［資産詳細レポート］で資産の状況を確認できます。

［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。



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。

参考 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。

参考 資産情報の登録にはライセンスは不要です。

参考 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 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。

参考 インポート時は、「資産管理番号」、「シリアルナンバー」、「IP アドレス」、「MAC アドレス」、「ホスト名」、「IMEI」、および「契約電話番号」の中から一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されます。

参考 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「ー」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、「ー」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。

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。	○
棚卸日	次の形式で記述します。 yyyy/mm/dd	○

管理項目	データの記述形式	省略可否
	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一つ。 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一つ。 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。	△
メモリ	0～8,388,607 の半角数字。 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	0～8,388,607 の半角数字。 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	0～8,388,607 の半角数字。	○

管理項目	データの記述形式	省略可否
	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一つ。	○
ディスプレイサイズ	0～8,388,607 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一つ。	○
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一つ。 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。	○
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。 コマンドを実行してハードウェア資産情報をインポートする場合、項目のデータ型が「選択型」のときは、CSV ファイルのデータに正規表現を使用できます。	○　※3

（凡例）○：設定を省略できる　△：どれか一つは設定が必要

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。

参考 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 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。

参考 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一つ。 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	○
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一つ。 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一つ。	○
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。

参考 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 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。

参考 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。	○

（凡例）○：設定を省略できる　×：設定を省略できない

参考 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 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。

参考 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一つ。 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一つ。 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。	○
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。	○

管理項目	データの記述形式	省略可否
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。

参考 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 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。

参考 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

参考 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

参考 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、関連するトピッ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 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 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 CSV ファイルの記述形式
- (4) 契約情報の項目と CSV ファイルの記述形式
- (5) 契約会社リストの項目と CSV ファイルの記述形式

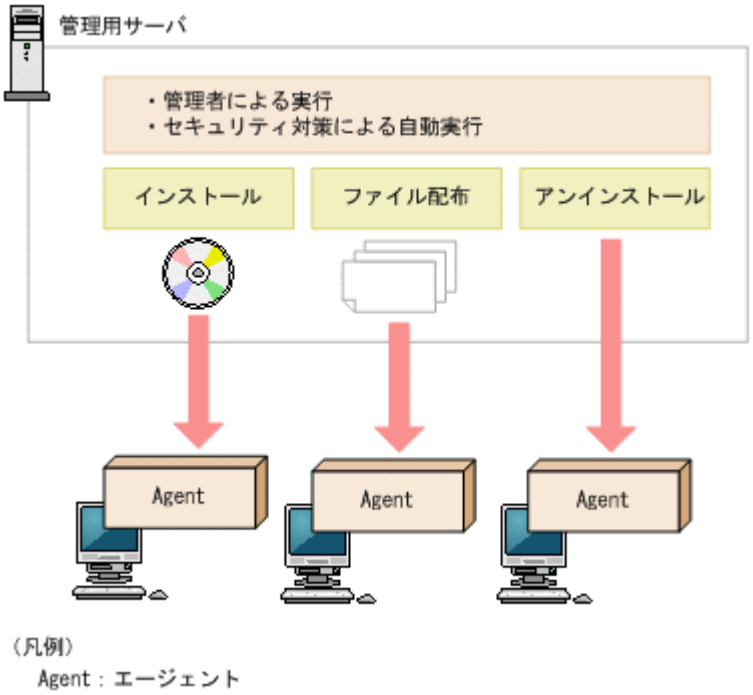
2.12 ソフトウェアおよびファイルの配布

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 では、管理用サーバからエージェント導入済み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 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。

参考 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。



サイトサーバを利用すると、配布するパッケージ（ソフトウェアやファイル）をサイトサーバに保管して、サイトサーバからパッケージが配布されるようになります。サイトサーバにパッケージを保管することで、ネットワークの負荷を軽減できます。

2.12.1 パッケージとタスクの管理

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 に登録して管理できます。

パッケージとタスクの定義

- パッケージ

  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、JP1/IT Desktop Management に登録したものです。パッケージは、配布画面の［パッケージ］画面で管理できます。

  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。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。

  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、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、配布画面の［タスク］画面で管理できます。

  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のパッケージを登録したあと、配布画面の［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。

- ファイルの配布

  配布画面の［パッケージ］画面で配布したいファイルのパッケージを登録したあと、配布画面の［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。

関連リンク

- 2.12.4 配布のための準備

(1) パッケージの管理

配布画面の［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。

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	ファイルを一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。

参考 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。

参考 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。

参考 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。

参考 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。

参考 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

- 2.12.4 配布のための準備

(2) タスクの管理

配布画面の［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、同じあて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、同じあて先に対して、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。

配布画面の［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。

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 の管理者によって、配布画面の［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、「2.12.2 セキュリティの自動対策による配布」を参照してください。

関連リンク

- 2.12.4 配布のための準備

2.12.2 セキュリティの自動対策による配布

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。

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。

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。

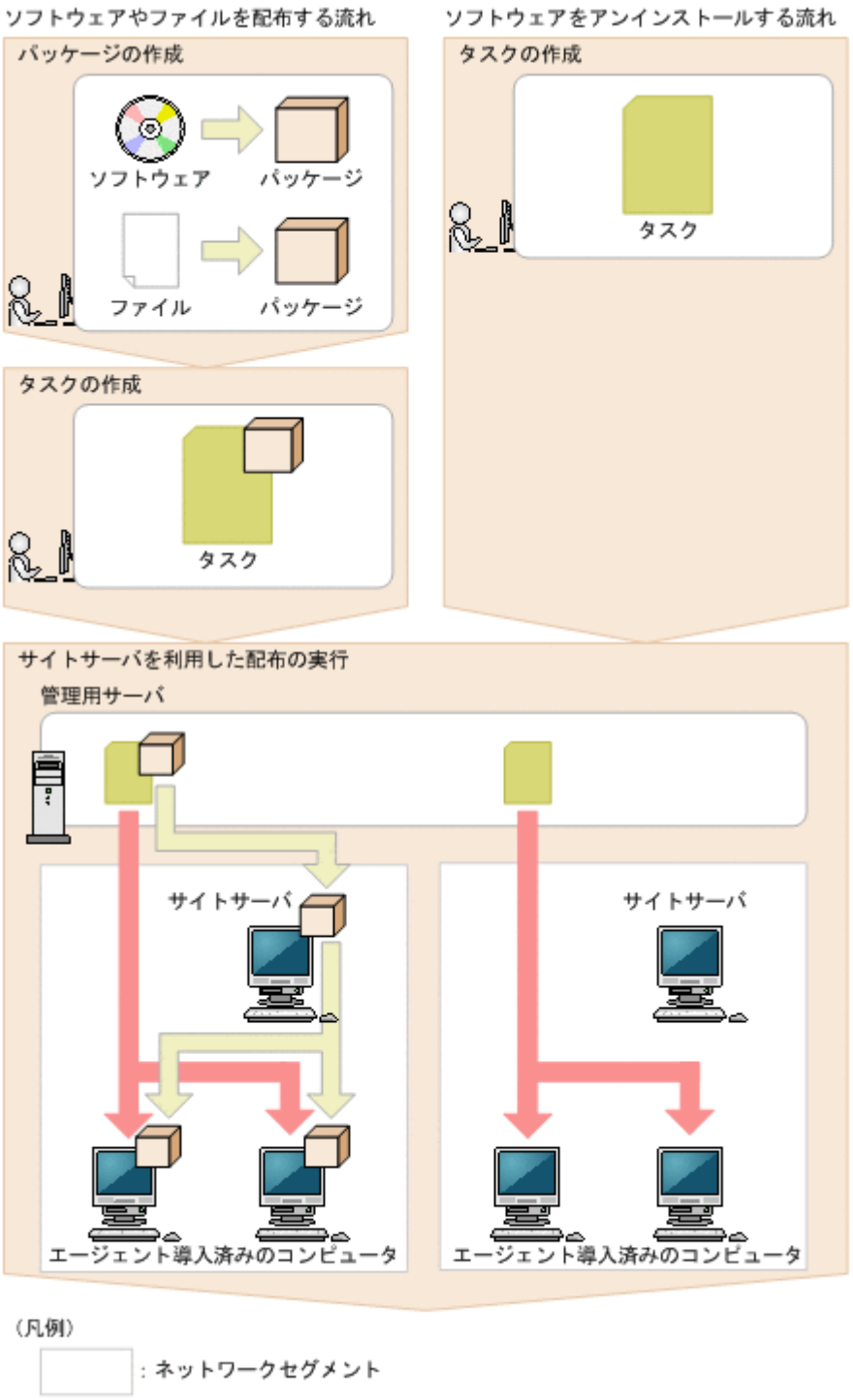
2.12.3 サイトサーバを利用したソフトウェアやファイルの配布

サイトサーバを利用すると、ソフトウェアやファイルの配布に伴うネットワークの負荷を分散できます。

参考 サイトサーバを利用して配布機能を実行するためには、あらかじめサイトサーバ構成システムを構築している必要があります。

参考 配布に関する操作（パッケージ管理、タスク管理）でサイトサーバを意識する必要はありません。構築時に実施するサーバ構成の設定に従って、自動的にサイトサーバ経由でタスクが実行されます。

サイトサーバを利用した配布の流れを、次の図に示します。



最初に、インストールするソフトウェアまたは配布するファイルをパッケージとして管理用サーバに登録します。登録によって管理用サーバのパッケージが変更された旨は、管理用サーバからサイトサーバに通知されるため、管理用サーバとサイトサーバのパッケージは自動的に同一の内容になります。次に、パッケージの配布を開始するスケジュールや、配布先のコンピュータでの動作を指定したタスクを作成します。作成したタスクは、管理用サーバから組織内のコンピュータに直接配布されます。作成したパッケージは、タスクに指定したスケジュールに従って、サイトサーバから組織内のコンピュータに配布されます。

ソフトウェアをアンインストールする場合は、アンインストール用のタスクを作成します。アンインストールの場合、パッケージの作成は不要です。

パッケージとタスクの管理については、「2.12.1 パッケージとタスクの管理」を参照してください。

参考 サイトサーバを配布に利用する場合、管理用サーバに登録される全パッケージと同等の容量を使用します。

関連リンク

- 2.9.6 更新プログラムの管理
- 2.12 ソフトウェアおよびファイルの配布

2.12.4 配布のための準備

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。

ネットワーク負荷

配布機能で使用されるネットワークの帯域を制限して、ネットワークの負荷を軽減できます。ネットワークの帯域を制限したい場合は、管理用サーバのセットアップおよびエージェント設定で、流量制御を設定してください。また、サイトサーバを設置している場合、サイトサーバから対象のコンピュータに対してソフトウェアやファイルのデータが配布されるようになり、ネットワーク負荷を軽減できます。サイトサーバを利用する場合、あらかじめサイトサーバ構成システムを構築してください。

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。

参考 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。

参考 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。

参考 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。

参考 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。

参考 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。

参考 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

2.12.5 アンインストールできるソフトウェアの種類

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。

2.12.6 配布時の注意事項

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 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 および JP1/IT Desktop Management のコンポーネント
  - JP1/IT Desktop Management 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。
- エージェント、ネットワークモニタエージェント、サイトサーバプログラム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。

2.12.7 利用者側でのダウンロードやインストールの延期

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

注意 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。
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

2.12.8 配布時に使用するネットワーク帯域の制御

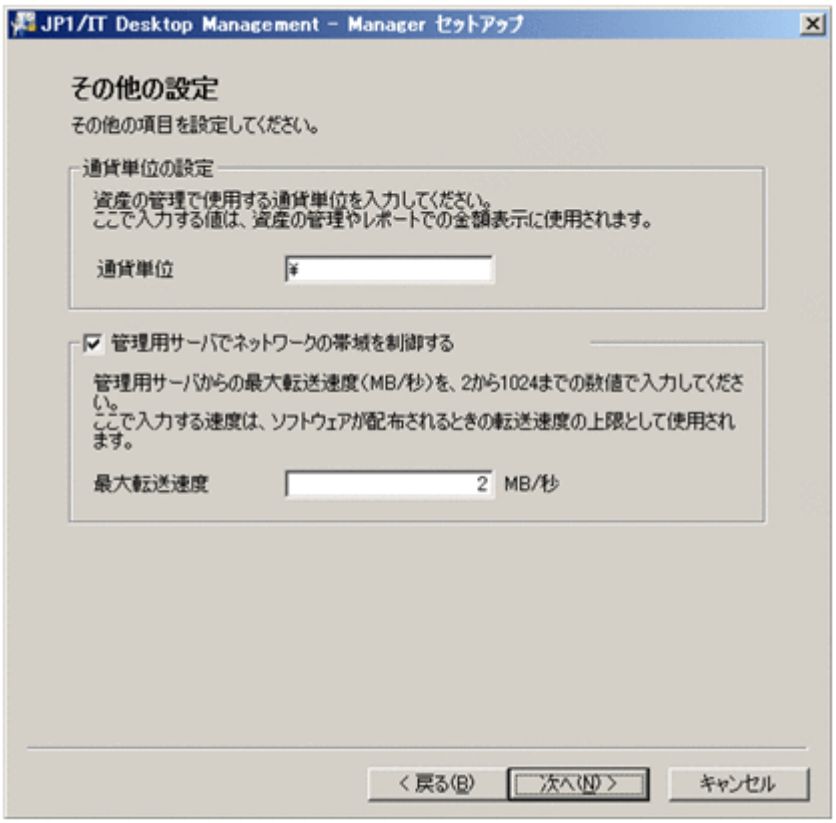
大容量のソフトウェアやファイルを管理用サーバから利用者のコンピュータに配布する場合、ネットワークに大きく負荷が掛かるおそれがあります。これを防ぐために、あらかじめデータ転送の速度を設定できます。

管理用サーバのネットワークの帯域を設定する

JP1/IT Desktop Management のセットアップで最大転送速度の上限値を指定すると、指定した転送速度の範囲内でデータを転送できます。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、指定した上限値に達した場合、管理用サーバ側のデータ転送を一時中断します。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。

データ転送速度を制御できるネットワークの範囲は、管理用サーバと利用者のコンピュータ間のネットワークです。エージェント導入済みのコンピュータは、パブリックネットワーク上に設置されている場合も対象となります。ただし、リモートオフィス上のコンピュータは対象外です。

データ転送の速度は、JP1/IT Desktop Management のセットアップで、ネットワーク帯域を制御するように設定します。



コンピュータがパッケージをダウンロードする際に使用するネットワークの帯域を設定する

パッケージのダウンロードに使用するネットワーク帯域の割合を指定できます。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、パッケージのダウンロード中に、メール送受信などネットワークを利用する業務に支障が出ないようにできます。

ネットワーク帯域の割合はエージェント設定で設定します。エージェント設定の［エージェント基本動作］で［流量制御］に［する］を選択して、ネットワーク帯域の割合を指定してください。

2.12.9 パッケージのキャッシュ

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。

注意 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

2.12.10 複数の利用者がログオンしている場合のタスク実行

エージェント導入済みのコンピュータに複数の利用者がログオンしている場合でも、タスクを同時に実行できます。ただし、それぞれの利用者のログオン状態によって、タスクの実行処理は異なります。利用者のログオンの状態について、次の三つのパターンに分類できます。

- すべての利用者が直接ログオンしている
- 直接ログオンしている利用者と、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利用者が混在している
- すべての利用者が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

それぞれのパターンとタスクの実行処理の関係を次の表に示します。

タスクの実行処理	全員直接ログオン	直接ログオンとリモートデスクトップ機能によるログオンが混在	全員リモートデスクトップ機能によるログオン
ダウンロードの延期	○	△	×
タスクの実行前および実行後のメッセージ表示			
インストールの延期	○	△	○
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			

（凡例）○：実行される　△：直接ログオンしている利用者だけに実行される　×：実行されない

関連リンク

- 2.12.12 配布機能での電源制御

2.12.11 利用者がログオフしている場合のタスク実行

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	

項目	実行の可否
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

- 2.12.12 配布機能での電源制御

2.12.12 配布機能での電源制御

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。

参考 タスクを実行する時刻からコンピュータの電源を ON にする時刻までの差が 1 時間以内の場合、ダイアログが出るので、配布完了後にコンピュータの電源を自動的に OFF にできます。

注意 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。

注意 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	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

［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※
		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

[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※
		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
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。

2.12.13 ソフトウェアのインストール実行結果の判定

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

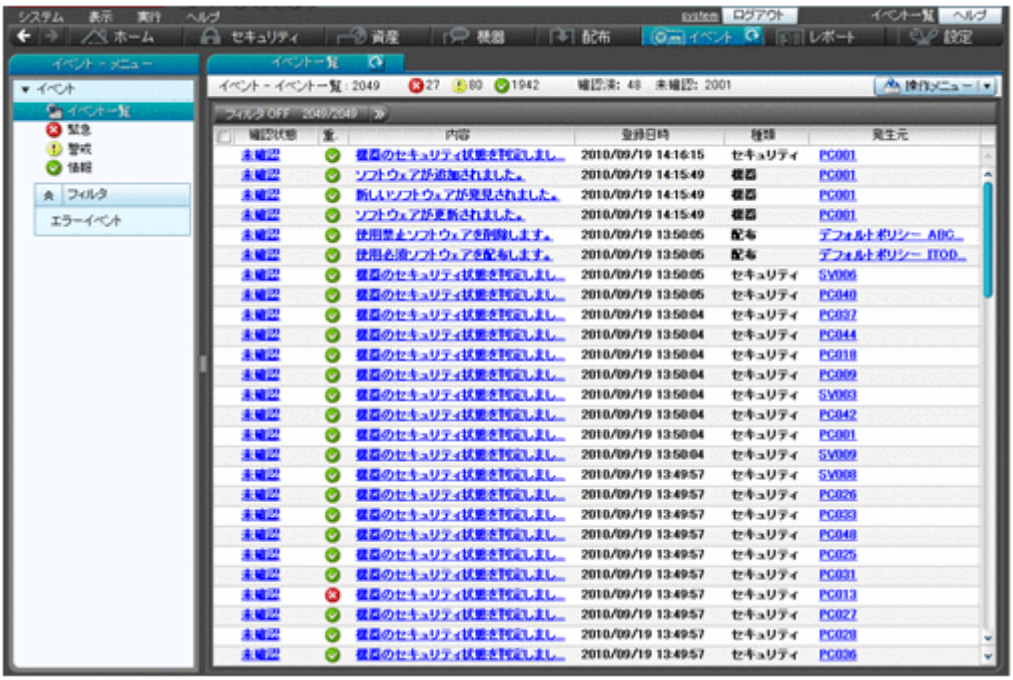
その他の形式のファイルの場合

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。

2.13 イベントの表示

JP1/IT Desktop Management 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 の運用中に発生した事象を把握できます。



2.13.1 出力されるイベント

JP1/IT Desktop Management 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三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。

参考 表示されるイベントの最大数は、保有している製品ライセンス数×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

- 2.13.2 イベントの種類

2.13.2 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

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。

エラー

各機能で発生したエラーに関するイベントです。

2.13.3 イベントの形式

出力されるイベントの形式を次の表に示します。

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。

項目	説明
	• 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 • 設定 • 不審操作 • 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。

2.14 レポートの表示

JP1/IT Desktop Management 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

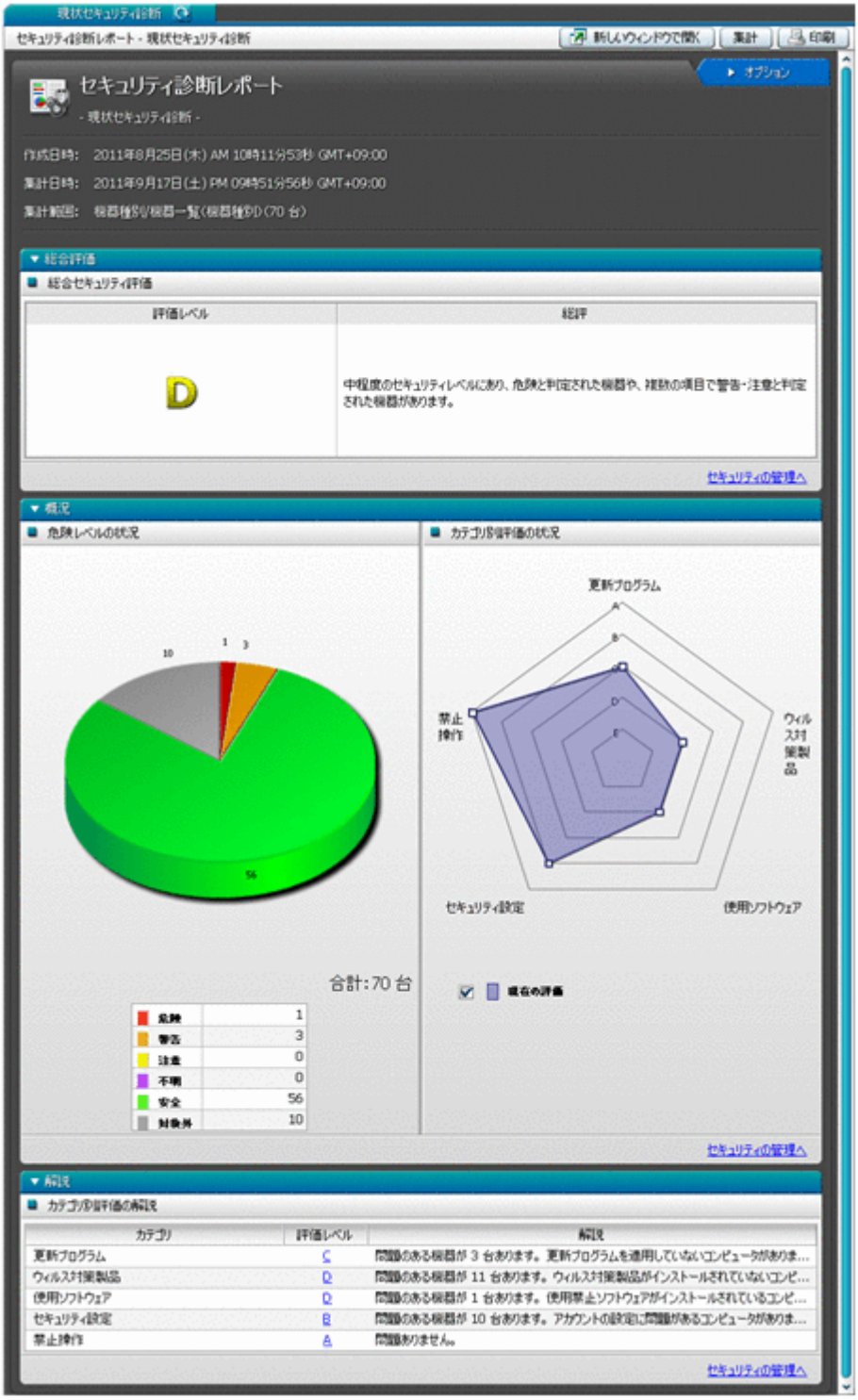
  セキュリティ状況の詳細をグラフや一覧で確認できます。問題のあるコンピュータを特定したり、問題点の詳細を確認したりできるため、セキュリティ対策の起点として利用できます。

- 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。



2.14.1 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。表示できるレポートを次の表に示します。

カテゴリ	種類
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

カテゴリ	種類
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
	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
	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

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。

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、および各コンピュータの詳細な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、および各コンピュータの詳細な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、および各コンピュータの詳細な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、および各コンピュータの詳細な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、および各コンピュータの詳細な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、および各コンピュータの詳細な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 USB 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。

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。

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。

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。

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。

2.14.2 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。

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
警告	16
注意	6

危険レベル	減点ポイント
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

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

2.14.3 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。

2.14.4 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。

2.14.5 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	×
	週刊ダイジェスト			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	○
	• 更新プログラムの適用状況 • ウィルス対策製品の状況		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		×

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
	• 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	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	前月分	5 年分※3	○
	ソフトウェアライセンスの費用					
	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。

注意 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。

2.14.6 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。

2.14.7 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、保存期間を短縮したことによっ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。

2.15 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

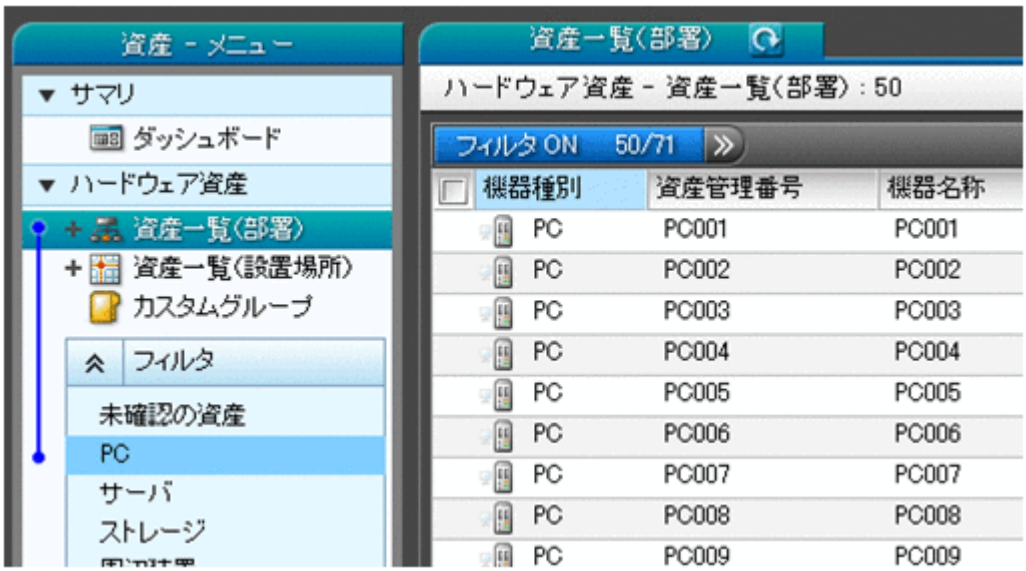
簡易フィルタは、用意されたフィルタ項目から一覧に表示したい条件を選択するフィルタです。一覧の上部に表示されているフィルタ項目のプルダウンメニューで、表示したい情報の条件を選択して、素早く情報を絞り込めます。

簡易フィルタは、上部にフィルタが表示されている一覧で利用できます。  をクリックすると、フィルタ項目が表示されます。

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 が提供するフィルタがあります。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、［登録日時］が 3 年以上前かつ［OS］が Windows 2000 などの条件を設定して、リプレース対象のコンピュータを絞り込んだりできます。

参考 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。

参考 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、［フィルタ OFF］ボタンまたは［フィルタ条件を追加］のリンク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、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、［フィルタ ON］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。

参考 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

- 2.15.1 製品が提供するフィルタ

2.15.1 製品が提供するフィルタ

JP1/IT Desktop Management 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］
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
ライセンス消費数超過ライセンス	• ［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	［ハードウェア資産］、［>］、［0］
ソフトウェアライセンス	［ソフトウェアライセンス］、［>］、［0］
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］

配布画面のフィルタ

配布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

- 2.15 フィルタの利用

2.16 サイトサーバの利用

JP1/IT Desktop Management で管理するコンピュータの台数が多くなるほど、管理用サーバで処理するデータ量やコンピュータとの通信量が増え、管理用サーバおよびネットワークに負荷が掛かります。この対策のために、JP1/IT Desktop Management ではサイトサーバによる負荷分散の機能を提供しています。

サイトサーバを設置することで、次の負荷分散を実現できます。

操作ログの保管先の分散によるディスク容量およびネットワーク負荷の軽減

エージェント導入済みのコンピュータから取得する操作ログを、サイトサーバに分散して保管することで、管理用サーバのディスク所要量の増大や通信の集中によるネットワーク負荷の増大を防止できます。サイトサーバに格納された操作ログは、操作画面から参照できます。

なお、サイトサーバのディスク容量が少なくなると、操作画面にイベントが表示されます。必要に応じてデータの移動、保管先の変更などのメンテナンスを実行してください。サイトサーバに保管している操作ログのメンテナンスには、recreatelogdb コマンド（インデックス情報の再作成）、movelog コマンド（操作ログの移動）、および deletelog コマンド（操作ログの削除）を利用します。

パッケージ配布時のネットワーク負荷の軽減

管理用サーバで配布用のパッケージを作成すると、自動的にサイトサーバにも格納されます。そのあとで配布機能を実行すると、サイトサーバからコンピュータに対してパッケージが転送されます。これによって、配布機能を利用する際の管理用サーバとサイトサーバ間でのネットワーク負荷を軽減できます。

サイトサーバは、エージェント導入済みのコンピュータにインストールして構築します。コンピュータにサイトサーバプログラムをインストールすると、機器画面の［管理種別］欄のエージェントを示すアイコンに、サイトサーバを示すアイコンが追加で表示されます。（例） 

各コンピュータの接続先となるサイトサーバを指定するには、JP1/IT Desktop Management のサーバ構成を設定します。サーバ構成の設定では、複数のサイトサーバをグルーピングしたサイトサーバグループを作成し、ネットワークセグメントごとにどのサイトサーバグループを接続先とするかを指定します。なお、接続先のサイトサーバグループは、操作ログの保管先と、配布機能の中継地点のそれぞれで異なるグループを指定できます。

参考 サイトサーバは、上記のほかにネットワークの探索、エージェントレスの機器からの機器情報収集、セキュリティポリシーの送信、JP1/IT Desktop Management のコンポーネント（エージェント、ネットワークモニタエージェント、サイトサーバ）の配布などにも利用されます。ただし、環境に応じて、サイトサーバを利用するかどうかをシステムが自動的に判断するため、運用時に意識する必要はありません。また、セキュリティポリシーは、配布機能の中継地点に指定したサイトサーバを経由して送信されるようになります。

関連リンク

- 4.4.3 サイトサーバ構成

2.17 クラスタシステムでの運用

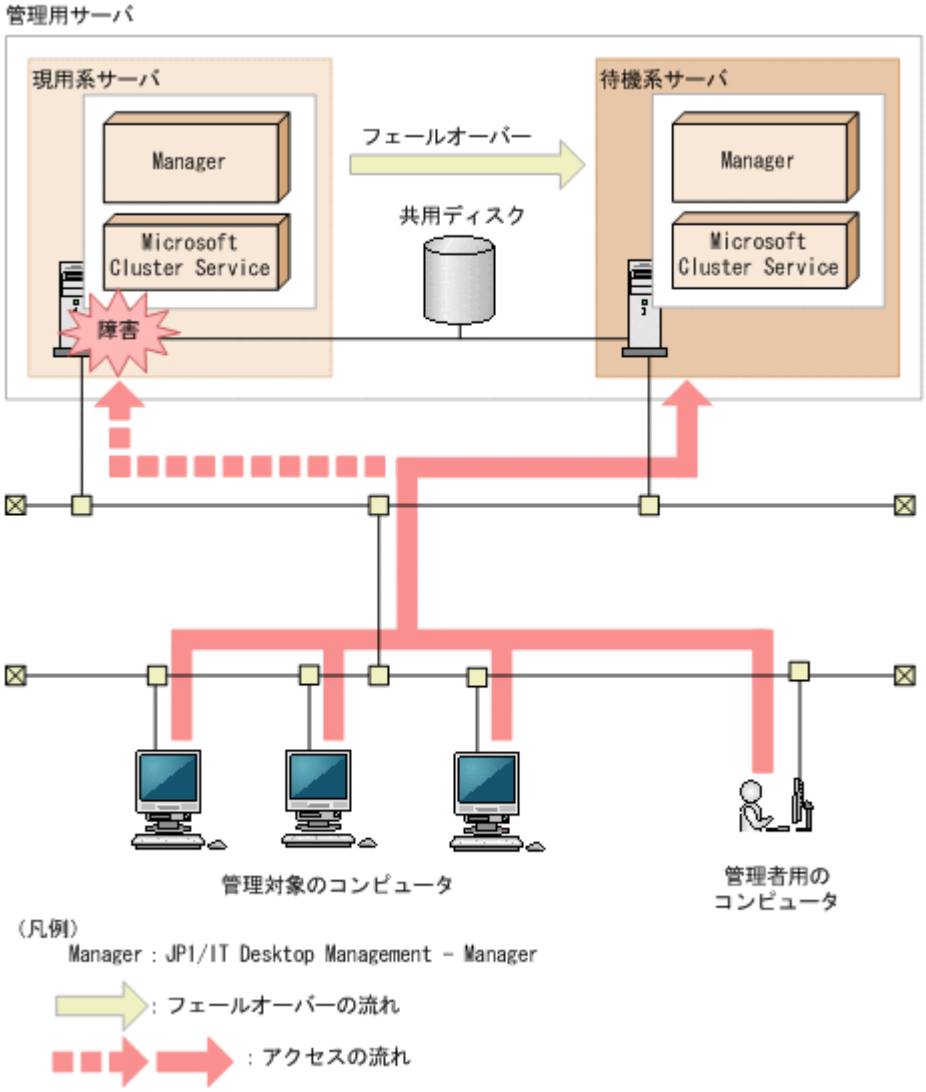
JP1/IT Desktop Management はクラスタシステムでの運用に対応しています。

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 が提供するサービスを継続できます。

JP1/IT Desktop Management は、Microsoft Cluster Service または 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、サーバを二つ用意して、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 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。

注意 クラスタシステムに対応するのは、管理用サーバだけです。サイトサーバのクラスタシステムは構築できません。

2.18 管理用サーバのデータベースの管理

JP1/IT Desktop Management 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 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。

管理用サーバのデータベースのメンテナンスには、JP1/IT Desktop Management 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、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。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。

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 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 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。

なお、サイトサーバのデータベースのメンテナンスには、データベースマネージャは使用しません。必要に応じて、サイトサーバの操作ログを手動でコピーして、バックアップを取得してください。

2.18.1 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**.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。

操作ログを取得している場合は、上記のファイルに加えて次の表に示すファイルが出力されます。

ファイル名	説明
OPR_DATA_**YYYYMMDD**※.zip	日付ごとの操作ログのバックアップデータです。 操作ログの自動バックアップが有効な場合は、自動バックアップされていない日付の操作ログがバックアップされます。 操作ログの自動バックアップが無効な場合は、
OPR_CATALOG_**YYYYMMDD**※.csv	

ファイル名	説明
	操作画面に表示されている操作ログがバックアップされます。
OPR_OTHER.zip	操作ログに関連するバックアップデータです。

注※　**YYYYMMDD** は、バックアップを取得した日付が設定されます（**YYYY**：年、**MM**：月、**DD**：日）。

2.19 コマンドの利用

JP1/IT Desktop Management 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。

2.19.1 コマンド一覧

JP1/IT Desktop Management で使用できるコマンドの一覧を次の表に示します。

コマンド名	機能	実行できるシステム
ioutils exportasset	ハードウェア資産情報をエクスポートします。	管理用サーバ
ioutils importasset	ハードウェア資産情報をインポートします。	管理用サーバ
ioutils exportfield	追加管理項目の設定をエクスポートします。	管理用サーバ
ioutils importfield	追加管理項目の設定をインポートします。	管理用サーバ
ioutils exporttemplate	資産情報をインポートする際に使用する、項目名の対応づけのテンプレートをエクスポートします。	管理用サーバ
ioutils importtemplate	資産情報をインポートする際に使用する、項目名の対応づけのテンプレートをインポートします。	管理用サーバ
ioutils exportpolicy	セキュリティポリシーの設定をエクスポートします。	管理用サーバ
ioutils importpolicy	セキュリティポリシーの設定をインポートします。	管理用サーバ
ioutils exportupdategroup	更新プログラムグループの設定をエクスポートします。	管理用サーバ
ioutils importupdategroup	更新プログラムグループの設定をインポートします。	管理用サーバ
ioutils exportoplog	操作ログをエクスポートします。	管理用サーバ
recreatelogdb	サイトサーバに格納されている操作ログのインデックス情報を再作成します。	サイトサーバ
movelog	サイトサーバ上で、操作ログのデータを移動します。	サイトサーバ
deletelog	サイトサーバ上の、操作ログのデータを削除します。	サイトサーバ

コマンド名	機能	実行できるシステム
ioutils exportfilter	フィルタの設定をエクスポートします。	管理用サーバ
ioutils importfilter	フィルタの設定をインポートします。	管理用サーバ
updatesupportinfo	サポートサービスサイトからダウンロードしたサポート情報を登録します。	管理用サーバ
exportdb	管理用サーバが管理するデータのバックアップを取得します。	管理用サーバ
importdb	管理用サーバが管理するデータを、バックアップ取得時の状態に復元します。	管理用サーバ
reorgdb	データベースを再編成します。	管理用サーバ
stopservice	管理用サーバのサービスを停止します。	管理用サーバ
startservice	管理用サーバのサービスを開始します。	管理用サーバ
getlogs	管理用サーバのトラブルシュート用情報を取得します。	管理用サーバ
getinstlogs	インストール時のトラブルシュート用情報を取得します。	管理用サーバ サイトサーバ
addfwlist.bat	Windows ファイアウォールの例外許可に JP1/IT Desktop Management を設定します。	管理用サーバ
resetnid.vbs	エージェントによって生成された、機器を識別するためのユニークな ID（ホスト識別子）をリセットします。	エージェント

2.20 エージェントの操作

コンピュータの利用者の操作が必要な場合は、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。利用者は、ダイアログに情報を入力して、管理用サーバに送信します。管理者の入力の手間が省けるため便利です。利用者情報の入力の詳細については、「2.20.1 利用者情報の入力」を参照してください。

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、「2.20.2 バルーンヒントの表示」を参照してください。

電源 OFF または再起動の指示があった場合の動作

管理用サーバからコンピュータのシャットダウンや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。利用者はすぐにシャットダウン（再起動）するか、あとでシャットダウン（再起動）するか選択できます。詳細な情報については、「2.20.3 電源 OFF または再起動の指示を受けた場合の動作」を参照してください。

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、「2.20.4 配布が実行された場合の動作」を参照してください。

抑止機能を受けた場合の動作

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、「2.20.5 抑止機能を受けた場合の動作」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、「2.7.15 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。

2.20.1 利用者情報の入力

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追加管理項目の設定が実行されると、エージェント導入済みコンピュータでは利用者情報を入力するダイアログが表示されます。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ダイアログを表示することもできます。

利用者情報は、[利用者情報の入力] ダイアログから入力します。[利用者情報の入力] ダイアログ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] ダイアログ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。項目が六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。項目が六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] ダイアログを閉じます。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。

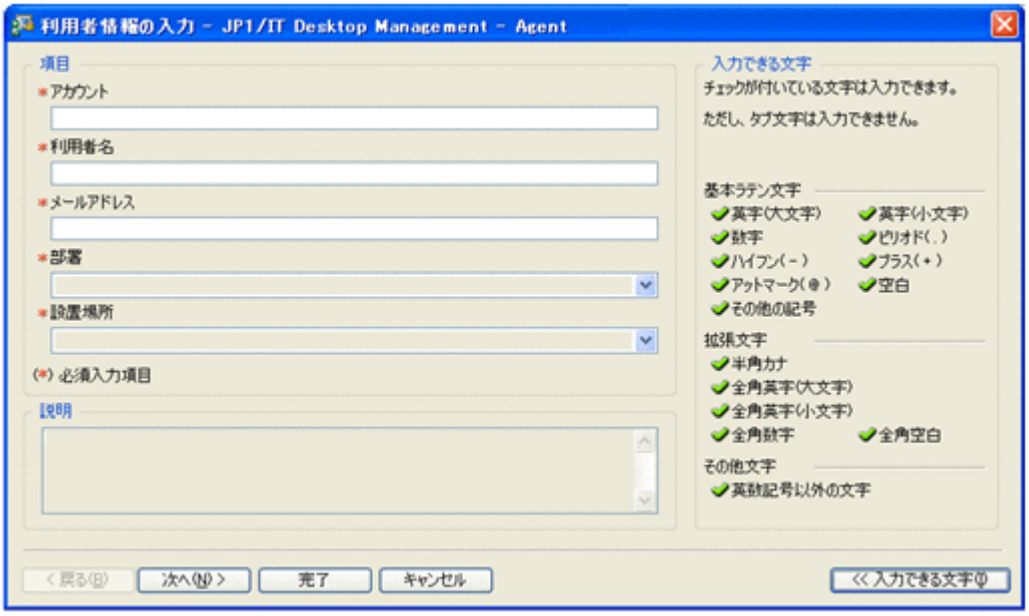
[キャンセル] ボタン

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。

2.20.2 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）

バルーンヒントが表示される事象とクリック時の動作を次の表に示します。

事象	表示されるメッセージ	クリック時の動作
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※1	Windows 2000 以外の場合 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。 Windows 2000 の場合 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ためには、このアイコンを右クリックして、［メッセージの表示］を選択してください。	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。
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	Windows 2000 以外の場合 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。 Windows 2000 の場合 利用者情報を入力してください。 利用者情報を入力するためには、このアイコンを右クリックして、［利用者情報の入力］を選択してください。	［利用者情報の入力］ダイアログが表示されます。
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※2	システム管理者から通知された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ました。 コンピュータを再起動してください。	なし。

注※1　セキュリティ判定で、機器単位のメッセージ通知とユーザー単位のメッセージ通知をどちらとも受信し、表示条件に合致した場合は、二つのメッセージが表示されます。

注※2　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」、「外部メディア抑止」、「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、Windows Server 2008、Windows Vista の場合は、再起動が必要です。

参考 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、「2.20.4 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。 ただし、Windows Server 2000

では、 ボタンの表示はありません。バルーンヒントが表示されてから 10 秒経過すると、自動的に閉じます。また、バルーンヒントをクリックしても動作しません。 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。
コンピュータのロック中	コンピュータのロック解除時に表示されます。ただし、Windows 2000 の場合、ロック解除時にバルーンヒントは表示されません。

注意 コンピュータの OS が 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。

2.20.3 電源 OFF または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。また、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。

［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。

エージェント導入済みコンピュータに［コンピュータのシャットダウン］ダイアログまたは［コンピュータの再起動］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または再起動されます。

［今すぐシャットダウンする］ボタンまたは［今すぐ再起動する］ボタン

すぐにコンピュータがシャットダウンまたは再起動されます。

［あとでシャットダウンする］ボタンまたは［あとで再起動する］ボタン

コンピュータのシャットダウンまたは再起動がキャンセルされます。

シャットダウンおよび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、自動的にシャットダウンおよび再起動されません。
- コンピュータをロックしている場合は、自動的にシャットダウンおよび再起動されません。

- 編集中のファイルが存在する場合は、自動的にシャットダウンおよび再起動されません。
- ほかのユーザーがログオンしている場合は、自動的にシャットダウンおよび再起動されません。
- ログオン前の場合は、［コンピュータのシャットダウン］ダイアログおよび［コンピュータの再起動］ダイアログが表示されないでシャットダウンおよび再起動されます。
- ［コンピュータのシャットダウン］ダイアログおよび［コンピュータの再起動］ダイアログが表示され、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。
- ［コンピュータの再起動］ダイアログが表示されているときに、管理用サーバから電源 OFF の通知を受け取った場合は、後続の通知を有効にします。そのとき、［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］ダイアログのカウントダウンがやり直されます。

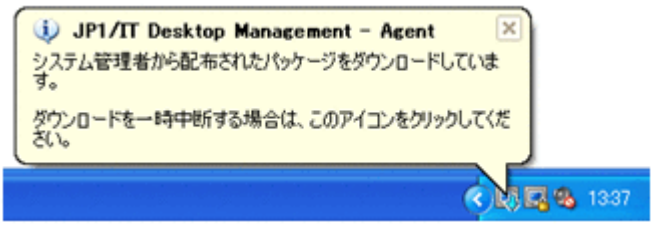
2.20.4 配布が実行された場合の動作

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）

バルーンヒントが表示される事象とクリック時の動作を次に示します。

事象	表示されるメッセージ	クリック時の動作
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。 ただし、Windows 2000 Server

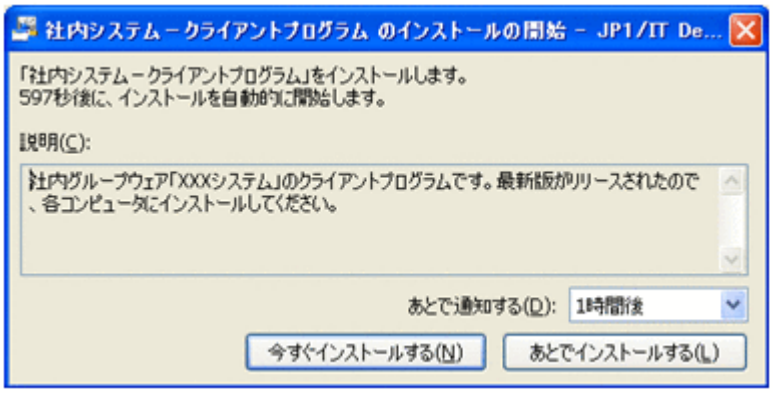
では、ボタンの表示はありません。バルーンヒントを表示してから 10 秒経過すると、自動的に閉じます。また、バルーンヒントをクリックしても動作しません。 バルーンヒントの表示契機を次に示します。

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。

注意 コンピュータの OS が 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。

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。

注意 複数のユーザーがログオンしている場合、ダイアログは、エージェントの通知対象となるユーザーだけに表示されます。通知対象となるユーザーの定義については、「2.20.6 エージェントからの通知対象となるユーザー」を参照してください。

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※	
	ユーザーログオン時に実行	
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	

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
	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。

2.20.5 抑止機能を受けた場合の動作

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外部メディアを使用したときに、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。

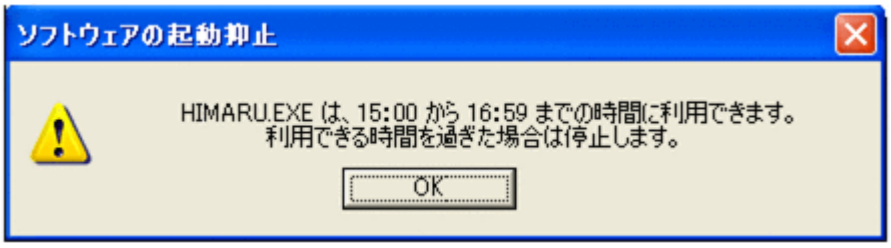
［ソフトウェアの起動抑止］ダイアログに表示される通知について説明します。

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

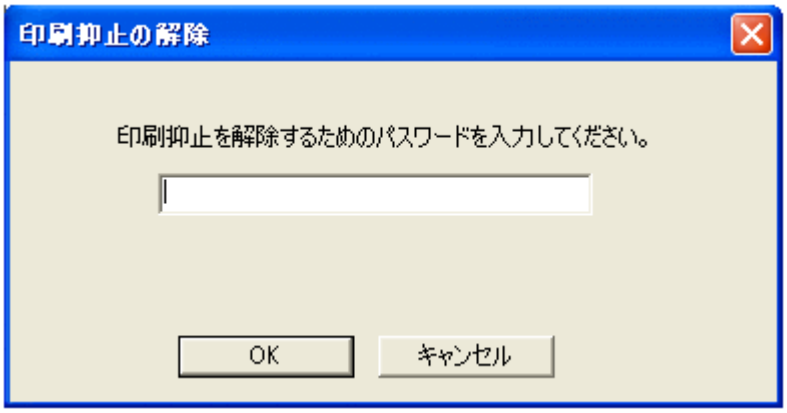
時間指定で許可されているソフトウェアの許可時間の終了が間近になった場合に表示されます。利用時間が過ぎた場合は、自動的にソフトウェアが停止されます。表示例を次の図に示します。

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、管理用サーバから印刷を抑止する［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。

［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。［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

USB デバイスなどの外部メディアの読み込みまたは書き込み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は、外部メディアの読み込みまたは書き込みを実行できません。

2.20.6 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 7 、Windows Vista、Windows XP、または Windows 2000 Professional 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 2008 または Windows 2000 Server 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

Windows Server 2003 の場合

- ローカルコンソールにログオンしたユーザー
- 「/console」、「/admin」オプションを指定してリモートデスクトップ接続したユーザー※

注※　対象のユーザーがいない場合は、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を通知対象とします。

2.21 スマートデバイスの制御

MDM 製品と連携すると、JP1/IT Desktop Management 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 製品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。

MDM 製品と連携すると、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。

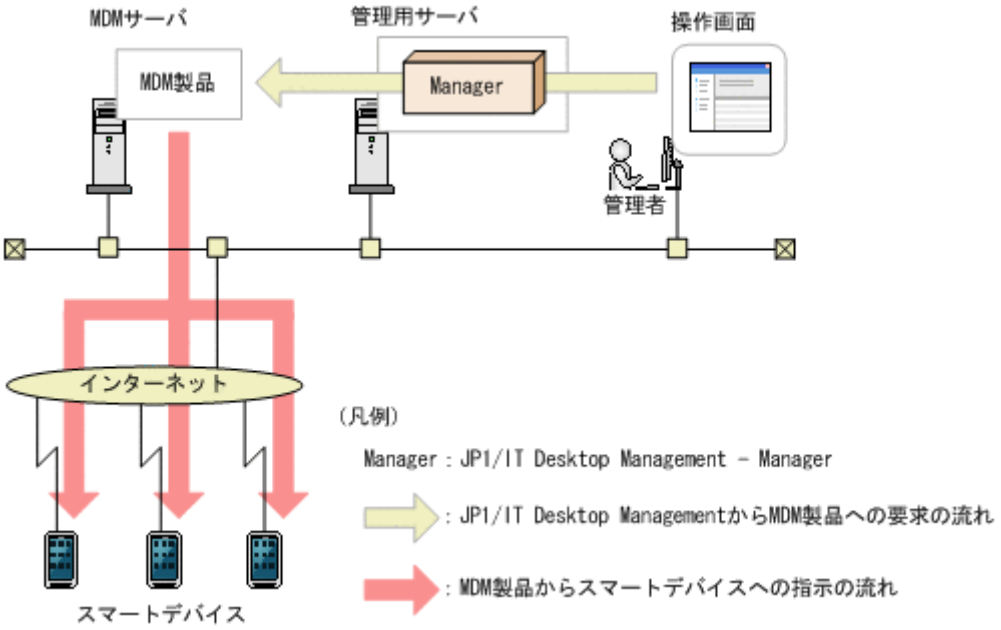
スマートデバイスのパスコードのリセット

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 が出す要求に従って、MDM 製品から実行されます。スマートデバイスを制御する流れを次の図に示します。



注意 MDM 製品との連携の設定を削除すると、その MDM 製品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。

参考 JP1/IT Desktop Management は、MDM 製品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

- 2.6.5 MDM 製品との連携

3

製品ライセンスについて

ここでは、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 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一つ使用します。つまり、JP1/IT Desktop Management 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 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。

参考 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。

参考 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。

参考 リモートコントロール機能を使用する場合、対象とする機器を管理対象にしてください。

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 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 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コンピュータ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 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 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。

4.1 導入と運用の流れ

ここでは、JP1/IT Desktop Management の導入と運用の流れについて説明します。JP1/IT Desktop Management 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 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 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 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 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、「A.5 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 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 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 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、サイトサーバ、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、「A.5 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
- 4.2.2 エージェントを導入するコンピュータの前提条件
- 4.2.3 サイトサーバの前提条件

- 4.2.5 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
- 4.2.4 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
- 4.2.7 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 - 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 7※1	Windows 7 Enterprise※2
	Windows 7 Professional※2
	Windows 7 Ultimate※2
Windows Server 2008※3	Windows Server 2008 R2 Datacenter※2
	Windows Server 2008 Enterprise※4
	Windows Server 2008 Enterprise without Hyper-V※4
	Windows Server 2008 R2 Enterprise※2
	Windows Server 2008 Standard※4
	Windows Server 2008 Standard without Hyper-V※4
	Windows Server 2008 R2 Standard※2
Windows Server 2003	Windows Server 2003, Enterprise Edition※2、※4
	Windows Server 2003, Enterprise x64 Edition※2、※4
	Windows Server 2003 R2, Enterprise Edition※4
	Windows Server 2003 R2, Enterprise x64 Edition※4
	Windows Server 2003, Standard Edition※2、※4
	Windows Server 2003, Standard x64 Edition※2、※4
	Windows Server 2003 R2, Standard Edition※4
	Windows Server 2003 R2, Standard x64 Edition※4

注※1　XP モードには対応していません。

注※2　Service Pack 1 を含みます。

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　Service Pack 2 を含みます。

ソフトウェア

JP1/IT Desktop Management - 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。

また、JP1/IT Desktop Management の操作画面を操作するには、次の表に示すソフトウェアが必要です。

項目	ソフトウェア
Web ブラウザ	次のどれかが必要です。 ・ Microsoft Internet Explorer 6 ・ Windows Internet Explorer 7 ・ Windows Internet Explorer 8 ・ Windows Internet Explorer 9 ・ Firefox 3.5 以降
ブラウザプラグイン	Adobe Flash Player 10.3 以降

なお、操作画面は管理用サーバ以外のコンピュータからも操作できます。この場合、操作するコンピュータにも前提ソフトウェアが必要です。

参考 JP1/IT Desktop Management のログイン画面にアクセスしたときに、Adobe Flash Player のバージョンアップを要求するダイアログが表示された場合は、この要求に応えてバージョンアップしてください。

関連リンク

- A.5 性能と見積もり

4.2.2 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 を次の表に示します。

OS	詳細
Windows 7※1	Windows 7 Enterprise※2
	Windows 7 Home Premium※2
	Windows 7 Professional※2
	Windows 7 Starter※2
	Windows 7 Ultimate※2
Windows Server 2008※3	Windows Server 2008 R2 Datacenter※2
	Windows Server 2008 Enterprise※4
	Windows Server 2008 Enterprise without Hyper-V※4
	Windows Server 2008 R2 Enterprise※2
	Windows Server 2008 Standard※4
	Windows Server 2008 Standard without Hyper-V※4
	Windows Server 2008 R2 Standard※2
Windows Vista	Windows Vista Business※2、※4
	Windows Vista Enterprise※2、※4
	Windows Vista Home Basic※2、※4
	Windows Vista Home Premium※2、※4
	Windows Vista Ultimate※2、※4
Windows Server 2003	Windows Server 2003, Enterprise Edition※2、※4
	Windows Server 2003, Enterprise x64 Edition※2、※4
	Windows Server 2003 R2, Enterprise Edition※4
	Windows Server 2003 R2, Enterprise x64 Edition※4

OS	詳細
	Windows Server 2003, Standard Edition※2
	Windows Server 2003, Standard x64 Edition※2、※4
	Windows Server 2003 R2, Standard Edition※4
	Windows Server 2003 R2, Standard x64 Edition※4
Windows XP	Windows XP Home Edition Operating System(Service Pack 2、3)
	Windows XP Professional Operating System（Service Pack 2、3）
Windows 2000	Windows 2000 Advanced Server Operating System (Service Pack 4)
	Windows 2000 Professional Operating System (Service Pack 4)
	Windows 2000 Server Operating System (Service Pack 4)

注※1　XP モードには対応していません。

注※2　Service Pack 1 を含みます。

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　Service Pack 2 を含みます。

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。 ・ Microsoft Internet Explorer 6 ・ Windows Internet Explorer 7 ・ Windows Internet Explorer 8 ・ Windows Internet Explorer 9

関連リンク

- A.5 性能と見積もり

4.2.3 サイトサーバの前提条件

サイト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。

OS

サイトサーバの前提となる OS を次の表に示します。

OS	詳細
Windows 7※1	Windows 7 Enterprise※2
	Windows 7 Professional※2
	Windows 7 Ultimate※2
Windows Server 2008※3	Windows Server 2008 R2 Datacenter※2
	Windows Server 2008 Enterprise※4
	Windows Server 2008 Enterprise without Hyper-V※4
	Windows Server 2008 R2 Enterprise※2

OS	詳細
	Windows Server 2008 Standard※4
	Windows Server 2008 Standard without Hyper-V※4
	Windows Server 2008 R2 Standard※2
Windows Server 2003	Windows Server 2003, Enterprise Edition※2、※4
	Windows Server 2003, Enterprise x64 Edition※2、※4
	Windows Server 2003 R2, Enterprise Edition※4
	Windows Server 2003 R2, Enterprise x64 Edition※4
	Windows Server 2003, Standard Edition※2、※4
	Windows Server 2003, Standard x64 Edition※2、※4
	Windows Server 2003 R2, Standard Edition※4
	Windows Server 2003 R2, Standard x64 Edition※4

注※1　XP モードには対応していません。

注※2　Service Pack 1 を含みます。

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　Service Pack 2 を含みます。

ソフトウェア

エージェントを導入する必要があります。

4.2.4 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 7※1	Windows 7 Enterprise※2
	Windows 7 Home Premium※2
	Windows 7 Professional※2
	Windows 7 Starter※2
	Windows 7 Ultimate※2
Windows Server 2008※3	Windows Server 2008 R2 Datacenter※2
	Windows Server 2008 Enterprise※4
	Windows Server 2008 Enterprise without Hyper-V※4
	Windows Server 2008 R2 Enterprise※2
	Windows Server 2008 Standard※4
	Windows Server 2008 Standard without Hyper-V※4
	Windows Server 2008 R2 Standard※2
Windows Vista	Windows Vista Business※2、※4
	Windows Vista Enterprise※2、※4
	Windows Vista Home Basic※2、※4
	Windows Vista Home Premium※2、※4

OS	詳細
	Windows Vista Ultimate※2、※4
Windows Server 2003	Windows Server 2003, Enterprise Edition※2、※4
	Windows Server 2003, Enterprise x64 Edition※2、※4
	Windows Server 2003 R2, Enterprise Edition※4
	Windows Server 2003 R2, Enterprise x64 Edition※4
	Windows Server 2003, Standard Edition※2、※4
	Windows Server 2003, Standard x64 Edition※2、※4
	Windows Server 2003 R2, Standard Edition※4
	Windows Server 2003 R2, Standard x64 Edition※4
Windows XP	Windows XP Home Edition Operating System(Service Pack 2、3)
	Windows XP Professional Operating System（Service Pack 2、3）

注※1　XP モードには対応していません。

注※2　Service Pack 1 を含みます。

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　Service Pack 2 を含みます。

関連リンク

- A.5 性能と見積もり

4.2.5 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 7※1	Windows 7 Enterprise※2
	Windows 7 Professional※2
	Windows 7 Ultimate※2
Windows Server 2008※3	Windows Server 2008 R2 Datacenter※2
	Windows Server 2008 Enterprise※4
	Windows Server 2008 Enterprise without Hyper-V※4
	Windows Server 2008 R2 Enterprise※2
	Windows Server 2008 Standard※4
	Windows Server 2008 Standard without Hyper-V※4
	Windows Server 2008 R2 Standard※2
Windows Server 2003	Windows Server 2003, Standard Edition※2、※4
	Windows Server 2003 R2, Standard Edition※4
	Windows Server 2003, Enterprise Edition※2、※4
	Windows Server 2003 R2, Enterprise Edition※4

注※1　XP モードには対応していません。

注※2　Service Pack 1 を含みます。

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　Service Pack 2 を含みます。

ソフトウェア

エージェント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

- 4.2.2 エージェントを導入するコンピュータの前提条件
- A.5 性能と見積もり

4.2.6 エージェントレスで管理するための条件

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。

注意 NAT 環境では、エージェントレスの機器は管理できません。

注意 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、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。
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。

セキュリティ管理をする場合（大部分の機器情報を取得する場合）

利用者のコンピュータで、次の条件をすべて満たしている必要があります。

- Windows ファイアウォールが無効になっている。※
- 簡易ファイル共有が無効になっている。
- ファイルとプリンタの共有が有効になっている。
- Windows の管理共有（ADMIN$）が有効になっている。
- プロセス間通信用共有（IPC$）が有効になっている。

注※　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。

また、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必要もあります。ただし、OS が Windows Vista または Windows Server 2008 の場合、UAC（ユーザーアカウント制御）の認証なしにログオンできるようにしてください。

なお、Windows の管理共有を有効にして機器情報を取得するためには次の表に示すような設定が必要です。

OS	設定内容
Windows 7	UAC の無効化
Windows Vista	• 共有ウィザードの無効化 • Administrator ユーザーの有効化
Windows XP	• 簡易ファイル共有の無効化 • ファイル共有の追加
Windows Server 2008	ネットワークと共有センターで［ファイル共有］と［プリンタ共有］を有効にする。
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）

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。

機器管理だけをする場合（一部の機器情報を取得する場合）

Active Directory を利用するとき

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。※
- 管理用サーバで、Active Directory を探索して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。

SNMP を利用するとき

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 7	• SNMP エージェントの導入 • SNMP エージェントの設定
Windows Vista	
Windows XP	
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	

これらの条件を満たしている場合、機器種別やコンピュータ名などの一部の機器情報を取得できます。セキュリティ管理が不要な場合は、こちらの方法で機器を管理できます。

機器の存在を確認する場合

ICMP を利用して、機器の存在を確認します。

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 7	ICMP エコー要求の着信許可※
Windows Vista	
Windows XP	
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

4.2.7 ネットワークの前提条件

JP1/IT Desktop Management 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。

注意 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。

注意 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

JP1/IT Desktop Management および JP1/IT Desktop Management - 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、「A.3 ポート番号一覧」を参照してください。

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。

参考 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 に重複して登録されることはありません。

管理用サーバとサイトサーバ間のネットワーク

サイトサーバ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。

管理用サーバからサイトサーバに対して ICMP で通信できない場合、次に示す制限があります。

- サイトサーバ経由の探索を利用して、エージェントレスの機器を管理できません。
- 配布用のパッケージは、サイトサーバからのポーリングが発生したタイミングで、管理用サーバからサイトサーバにダウンロードされます。

サイト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サイトサーバに対して、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 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。

管理用サーバまたはサイトサーバの場合

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 またはサイトサーバプログラム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、管理用サーバまたはサイトサーバで `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 - Manager またはサイトサーバプログラム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

- (2) エージェントレスで管理するための条件

4.3 各機能の前提条件

ここでは、JP1/IT Desktop Management の各機能を利用するための前提条件について説明します。

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 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

- 4.2.2 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。そのため、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、エージェント導入済みのコンピュータを 1 台準備してください。また、そのコンピュータのネットワークモニタを有効にする必要があります。

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。

参考 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。

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。つまり、エージェントを導入すると、自動的にリモコンエージェントも導入されます。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。

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 サーバ機能を持つ次のソフトウェアのうち、どれかが実行されている
  - ・Intel vPro
  - ・RealVNC
  - ・UltraVNC
  - ・VMware Workstation
- OS が Mac OS X で、Apple Remote Desktop Service が実行されている
- 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

注意 上記の条件以外で、RFB 接続を利用する場合、一部の機能が使用できないおそれがあります。事前に動作を確認してからリモートコントロール機能を利用してください。

注意 JP1/NETM/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。

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。

また、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 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。

参考 JP1/IT Desktop Management 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 • ネットワーク共有プリンタの場合、プリンタサーバとなる機器で、印刷操作をした機器の名前解決ができる • ネットワーク共有プリンタの場合、プリンタサーバとなる機器で、プリンタの［プロパティ］ダイアログの［セキュリティ］タブで［ドキュメントの管理］が許可されている • ネットワーク共有プリンタ、またはほかのコンピュータに接続されたプリンタの場合、コントロールパネルの［Windows ファイアウォール］－［Windows ファイアウォールによるプログラムの許可］－［例外］タブで［ファイルとプリンタの共有］が許可されている • ネットワーク共有プリンタ、またはほかのコンピュータに接続されたプリンタの場合、抑止対象のコンピュータで Win32_PrintJob クラスがサポートされた WMI が起動されている
外部メディアの抑止	コンピュータの OS が Windows Server 2003 または Windows XP の場合に、内蔵 CD/DVD への書き込みを抑止するときは、CD/DVD ドライブの［プロパティ］ダイアログの［書き込み］タブにある［このドライブで CD 書き込みを有効にする］がチェックされている

関連リンク

- (13) 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。

また、操作ログの保管先を分散させて、管理用サーバの負荷を軽減するためには、システム構成にサイトサーバが必要です。

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		－
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	使用している Web ブラウザが Firefox の場合、［ツール］－［アドオン］を選択すると表示される［拡張機能］で、「JP1/IT Desktop Management - Agent」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	－
	メールに添付されているファイルの保存	
	FTP の送受信	
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 • ネットワーク共有プリンタの場合、プリンタサーバとなる機器で、印刷操作をした機器の名前解決ができる • ネットワーク共有プリンタの場合、プリンタサーバとなる機器で、プリンタの［プロパティ］ダイアログの［セキュリティ］タブで［ドキュメントの管理］が許可されている • ネットワーク共有プリンタ、またはほかのコンピュータに接続されたプリンタの場合、 コントロールパネルの［Windows ファイアウォール］－［Windows ファイアウォールによるプログラムの許可］－［例外］タブで［ファイルとプリンタの共有］が許可されている • ネットワーク共有プリンタ、またはほかのコンピュータに接続されたプリンタの場合、抑止対象のコンピュータで Win32_PrintJob クラスがサポートされた WMI が起動されている
Web アクセス		• 使用している Web ブラウザが Internet Explorer の場合、［インターネットのプロパティ］ダイアログで、［詳細設定］タブにある［サードパーティ製のブラウザ拡張を有効にする（再起動が必要)］がチェックされている • 使用している Web ブラウザが Internet Explorer の場合、［ツール］－［アドオンの管理］から表示されるダイアログで、［JP1/IT Desktop Management - Agent］の状態が［有効］になっている • 使用している Web ブラウザが Firefox の場合、［ツール］－［アドオン］を選択すると表示される［拡張機能］で、「JP1/IT Desktop Management - Agent」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。
外部メディアの接続および切断		－
ウィンドウ操作		－

（凡例）－：特になし

4.3.6 資産管理の前提条件

資産管理をする場合、MDM 製品と連携してスマートデバイスを管理するときは、スマートデバイスの OS が iOS または Android である必要があります。

また、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、エージェント導入済みのコンピュータが必要です。

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。

配布時のネットワーク負荷を分散させる場合は、配布用の機能の中継地点としてサイトサーバを使用する必要があります。

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	契約情報にハードウェアの費用が設定されている

レポートの種類		前提条件
	ソフトウェアライセンスの費用	契約情報にソフトウェアライセンスの費用が設定されている
	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 で構築できるシステム構成の種類を次の表に示します。

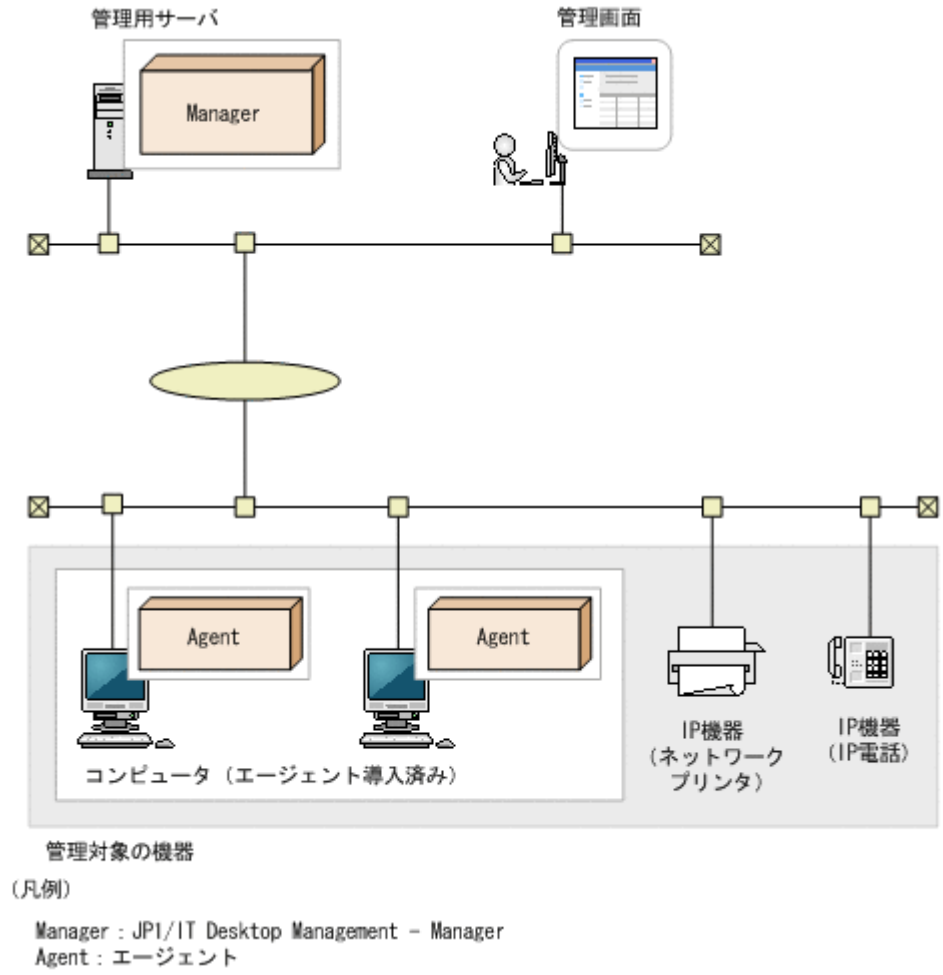
システム構成の種類	特徴
基本構成	管理用サーバおよび管理対象となる機器を配置した基本的な構成です。
エージェントレス構成	管理対象となるコンピュータにエージェントレスのコンピュータを含む構成です。
サイトサーバ構成	サイトサーバを配置して、操作ログの保管先または配布機能の中継地点として設定することで、管理用サーバやネットワークの負荷を分散する構成です。
更新プログラム管理構成	サポートサービスサイトと連携する構成です。最新の更新プログラム情報を管理用サーバにダウンロードして、管理対象のコンピュータに最新の更新プログラムを適用できます。
Active Directory 連携構成	Active 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 製品と連携してスマートデバイスを管理する構成です。MDM 製品で管理しているスマートデバイスを JP1/IT Desktop Management 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。
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。
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。

関連リンク

- 4.4.1 基本構成
- 4.4.2 エージェントレス構成
- 4.4.3 サイトサーバ構成
- 4.4.4 更新プログラム管理構成
- 4.4.5 Active Directory 連携構成
- 4.4.6 MDM 連携構成
- 4.4.7 ネットワーク監視構成
- 4.4.8 リモートコントロール構成
- 4.4.9 クラスタ構成

4.4.1 基本構成

JP1/IT Desktop Management で構築する基本的な構成システムについて説明します。基本構成のシステムは、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。基本構成を次の図に示します。



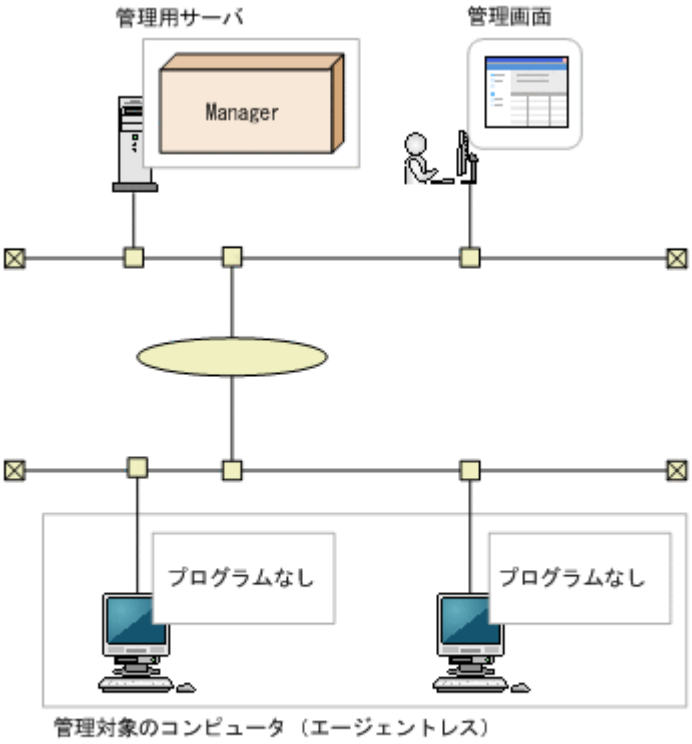
設定したセキュリティポリシーに従って、管理用サーバはコンピュータのセキュリティ状況を診断します。セキュリティポリシーの設定やセキュリティ診断結果の確認には操作画面を使用します。操作画面は Web ブラウザを使用して表示し、操作します。また、Web ブラウザで管理用サーバにアクセスできる環境であれば、ログインして操作画面を操作できます。

基本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 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 - 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 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。

また、エージェントレスのコンピュータを管理するためには、次の設定が必要です。

- エージェントレスの各コンピュータに管理共有を設定する。
- 管理対象の全コンピュータで共通のアクセスアカウントを設定する。

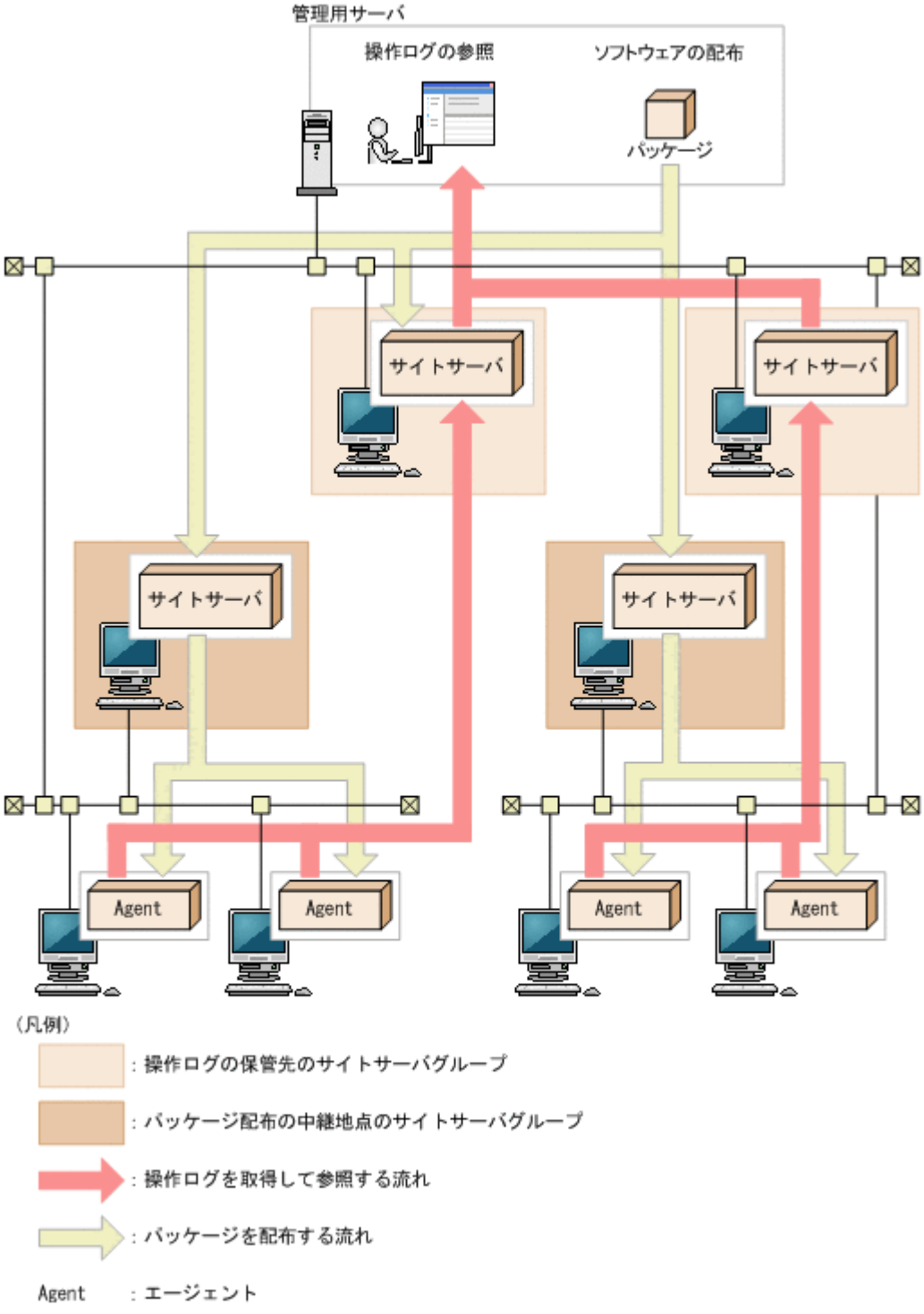
注意 エージェントレスのコンピュータの場合、エージェントを導入したコンピュータと比較して、機能差異があります。

4.4.3 サイトサーバ構成

サイトサーバを配置して、エージェント導入済みのコンピュータから収集した操作ログの保管先、または配布機能の中継地点として設定することで、管理用サーバやネットワークの負荷を分散できます。この構成をサイトサーバ構成といいます。

参考 サイトサーバは、管理用サーバにはインストールできません。

サイトサーバ構成を次の図に示します。



操作ログの保管先と配布機能の中継地点をどのサイトサーバにするかは、ネットワークセグメントごとに設定できます。

機能の可用性を高めるため、各ネットワークセグメントには、個々のサイトサーバではなく複数のサイトサーバをグループ化したものを設定します。これをサイトサーバグループと呼びます。 サイトサーバグループを定義する際は、必要に応じてグループ内のサイトサーバに優先順位を設定す

ることで接続先を制御できます。また、優先順位をランダムにして、毎回不特定のサイトサーバに接続することで、特定のサーバに負荷が集中することを避けることもできます。

操作ログの保管先

サイトサーバを操作ログの保管先として設定すると、各エージェント導入済みのコンピュータから収集した操作ログが、サイトサーバに保管されます。各サイトサーバに保管された操作ログは、操作画面から参照できます。これによって、操作ログの収集による管理用サーバのディスク容量の圧迫やネットワーク負荷の増大を防ぐことができます。サイトサーバを操作ログの保管先として利用する場合、各ネットワークセグメントに指定するサイトサーバグループには、1 台のサイトサーバだけを設定することをお勧めします。これによって、1 台のコンピュータの操作ログが 1 台のサイトサーバに集約され、操作ログを管理しやすくなります。

注意 操作ログの保管先にサイトサーバを利用する場合、負荷分散や運用効率の観点から、すべての操作ログをサイトサーバに保管して、管理用サーバには操作ログを保管しないことをお勧めします。

注意 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してください。

配布機能の中継地点

サイトサーバを配布機能の中継地点として設定すると、管理用サーバからサイトサーバに配布用のパッケージが自動的にダウンロードされ、サイトサーバからエージェントに配布がされるようになります。これによって、各エージェントにパッケージを配布する際のネットワーク負荷を軽減できます。配布機能の中継地点として利用する場合は、サイトサーバグループに複数のサイトサーバを設定することをお勧めします。これによって、1 台のサイトサーバに障害が発生しても、ほかのサイトサーバに接続できるため、可用性の高いシステムを実現できます。この場合、サイトサーバグループ内の各サイトサーバに接続の優先順位を付けることも、優先順位をランダムに設定することもできます。どのように負荷分散させるかを考慮して、サイトサーバグループの構成を検討してください。

また、配布機能の中継地点となるサイトサーバは、パッケージ以外に次のデータの配信にも利用されます。

- セキュリティポリシー
- 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

参考 操作ログの保管先と配布機能の中継地点には、それぞれ異なるサイトサーバグループを指定できます。ディスク容量に余裕のあるコンピュータのサイトサーバグループを操作ログの保管先にして、ほかのサイトサーバグループは配布機能の中継地点にするなど、環境に応じたシステムを構築できます。

注意 管理対象にできる機器の上限は、サイトサーバを設置している場合は 10,000 台、サイトサーバを設置していない場合は 3,000 台です。ただし、各サイトサーバが管理できる機器の上限は 1,000 台です。

関連リンク

- 2.10.3 サイトサーバでの分散操作ログの管理
- 2.12.3 サイトサーバを利用したソフトウェアやファイルの配布
- 4.6.6 サイトサーバを設置するための検討

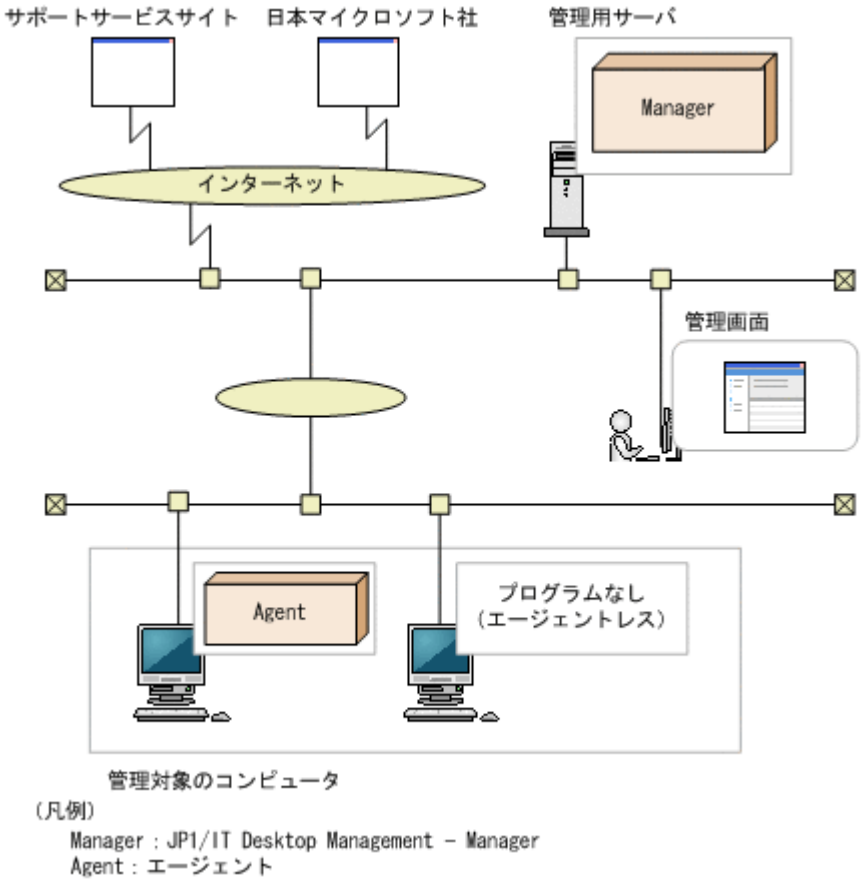
4.4.4 更新プログラム管理構成

サポートサービスサイトから最新の更新プログラム情報をダウンロードし、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自動的に反映できます。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。この構成を更新プログラム管理構成といいます。

参考 更新プログラム管理構成にするには、サポートサービス契約が必要です。

更新プログラム管理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。

更新プログラム管理構成の場合、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。 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 基本構成」を参照してください。

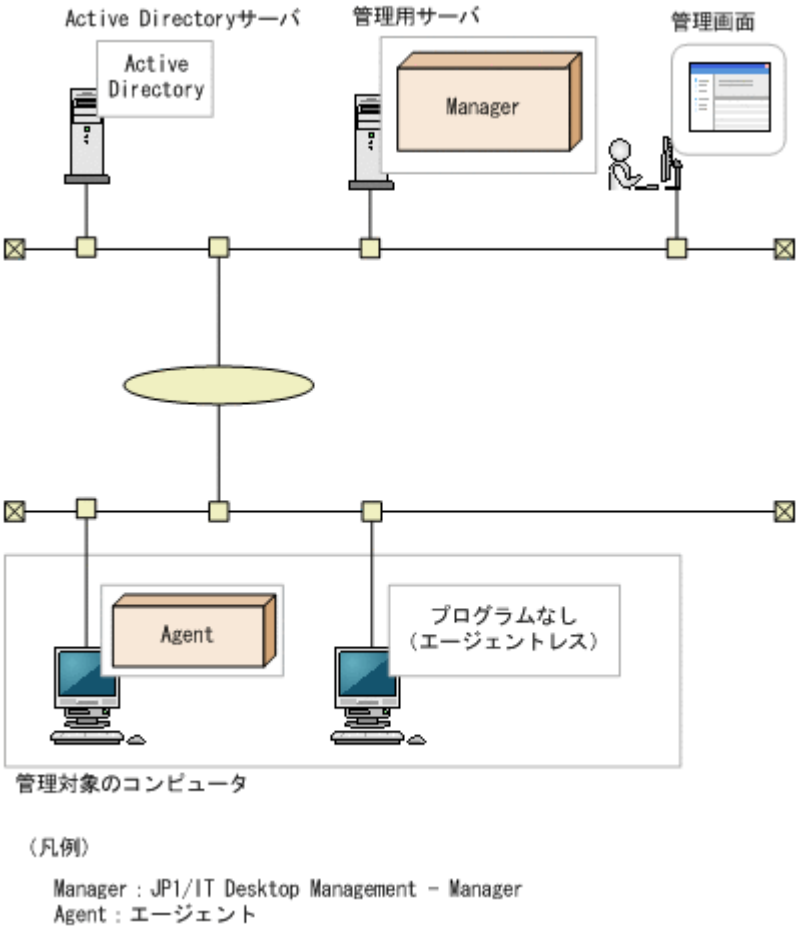
参考 管理用サーバがインターネット接続できない環境でも、更新プログラムを管理できます。この場合、管理用サーバ以外のインターネット接続できるコンピュータが、サポートサービスサイトから更新プログラム情報を取得して、管理用サーバにアップロードします。また、配布する更新プログラムの実行ファイルも、日本マイクロソフト社の Web サイトからコンピュータにダウンロードして、そのあと管理用サーバにアップロードします。

4.4.5 Active Directory 連携構成

JP1/IT Desktop Management 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 2008
- Windows Server 2003
- Windows 2000 Advanced Server
- Windows 2000 Server

Active Directory 連携構成を次の図に示します。



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。

参考 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 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。

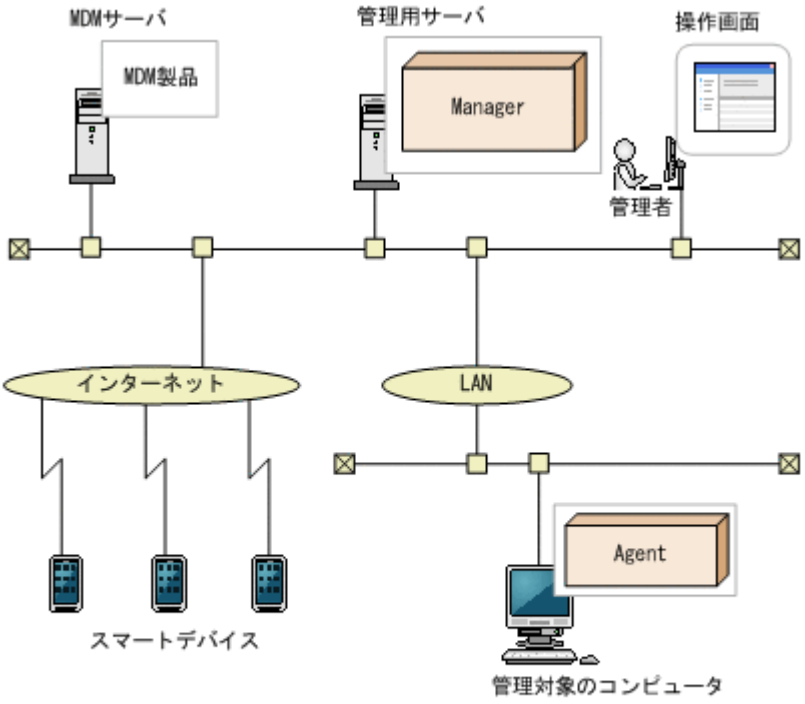
4.4.6 MDM 連携構成

MDM 製品と連携することで、MDM 製品で管理しているスマートデバイスを JP1/IT Desktop Management 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 製品を次に示します。

製品名	バージョン
MobileIron	4.5

MDM 製品と連携して、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）

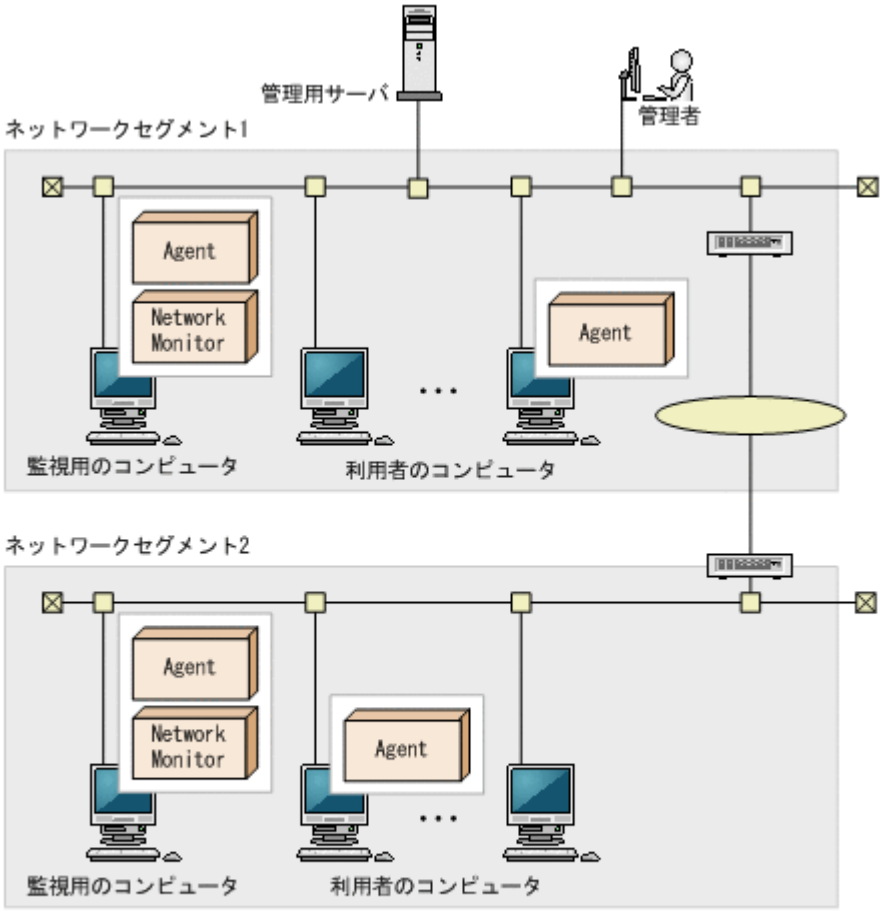
Manager：JP1/IT Desktop Management - Manager
Agent：エージェント

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 製品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 の管理対象にできます。

MDM 製品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 上の情報も更新されます。このため、MDM 製品と連携する場合は、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。

4.4.7 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）
Agent：エージェント
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エージェント導入済みのコンピュータ（監視用のコンピュータ）が必要です。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。

注意 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/Network Monitor は JP1/IT Desktop Management 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/Network Monitor を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。

参考 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。
エージェント導入済みのコンピュータに、提供媒体から「JP1/IT Desktop Management - 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。

参考 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。

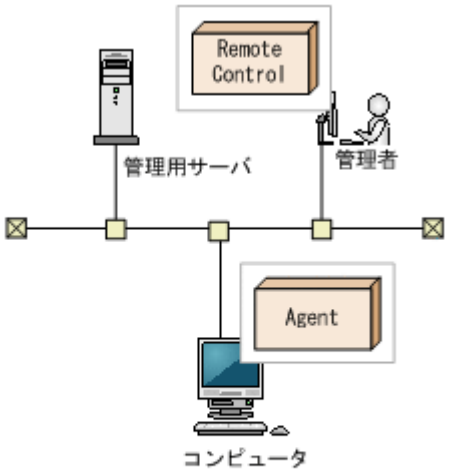
参考 VLAN（Virtual LAN）のトランク接続機能を使用して複数の VLAN を束ねることで、1 台のコンピュータ（かつ、一つのネットワークカード）で複数のサブネットワーク（VLAN）を監視できます。ただし、次の前提条件を満たす必要があります。

- 監視用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
- 監視用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

4.4.8 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。

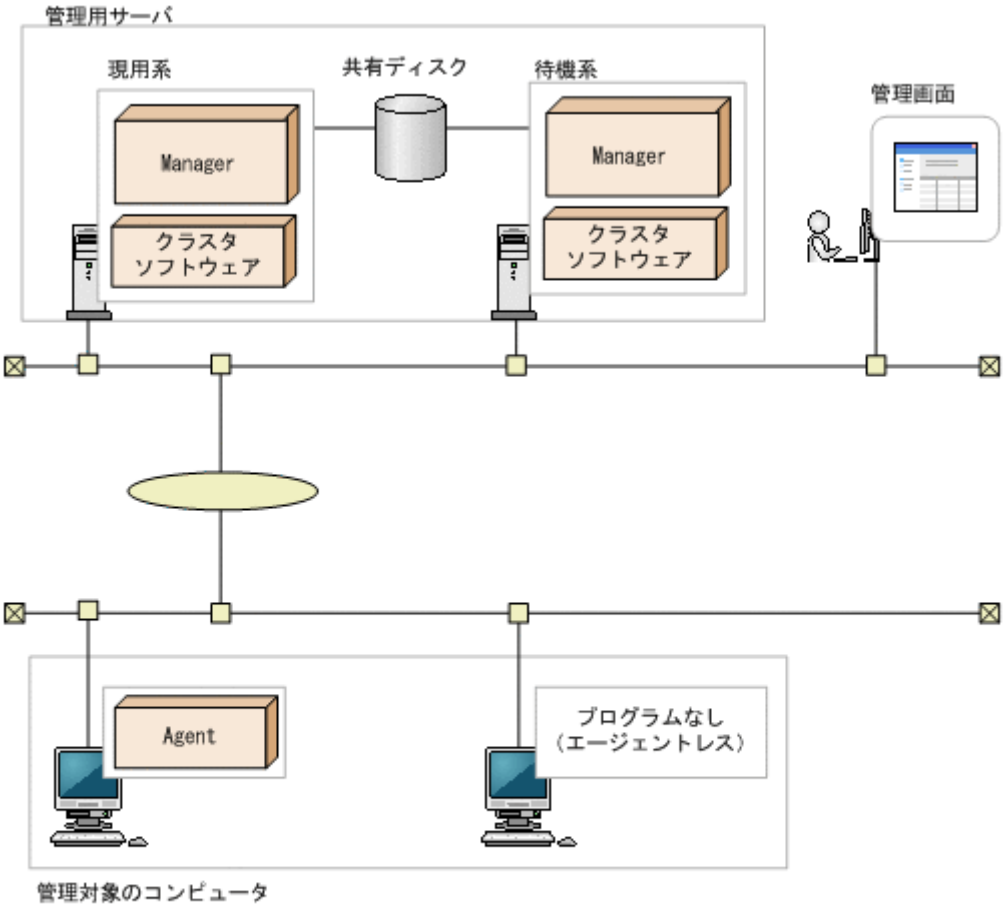


（凡例）
Agent：エージェント
Remote Control：コントローラ

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。

4.4.9 クラスタ構成

管理用サーバをクラスタ構成にできます。実行中の管理用サーバを現用系、待機状態の管理用サーバを待機系といいます。現用系の管理用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管理用サーバに処理を引き継ぎます。管理用サーバをクラスタ構成にしておくことで、管理用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 - Manager
Agent：エージェント

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 Microsoft Cluster Service および 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。

注意 サイトサーバはクラスタ構成にできません。

4.5 データベースの検討

JP1/IT Desktop Management 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。

参考 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 データフォルダで必要なディスクの最大容量
- 4.5.5 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 操作ログのバックアップ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 のデータベース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。ここでは、JP1/IT Desktop Management のデータベースおよびデータ保管用のフォルダについて説明します。

管理用サーバのデータベース

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、保持および参照するためのデータベース領域が作成されるフォルダです。 次の 2 種類の領域が作成されます。 オンライン用 現在から約 30 日分の容量の操作ログが保管される領域です。※ セットアップで設定した、[管理対象の機器の台数] の値に応じて、自動的に容量が設定されます。 取り込み用 バックアップされた操作ログを取り込んで参照するための領域です。最大 500 日分までの操作ログを取り込めます。取り込んだ操作ログを削除することもできます。 セットアップで設定した、[管理対象の機器の台数] と [操作ログの最大取り込み期間] の値に応じて、自動的に容量が設定されます。	△
操作ログの保管先フォルダ	自動的にバックアップされた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タを「操作ログのデータベースフォルダ」の「取り込み用」領域に格納して、過去の操作ログを参照できます。	△
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

注※　件数が管理対象のコンピュータ数 ×30 日×2,700 件を超えた場合、または 500 日を経過した場合は、日付の古いものから削除されます。

参考 各フォルダは、管理用サーバのローカルディスクだけ指定できます。ただし、操作ログの保管用のフォルダは任意のフォルダを指定できます。このため、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といった運用ができます。

注意 操作ログの保管用のフォルダは任意のネットワークディスクを指定できます。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。

サイトサーバのデータベース

各フォルダの作成先は、サイト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	操作ログ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	管理用サーバに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。	○
操作ログのデータフォルダ	コンピュータから収集された操作ログが保管されるフォルダです。	○

（凡例）○：必ず作成される

注意 サイトサーバのデータベース容量は、収集される操作ログや作成したパッケージの量に応じて単調増加します。空きディスク容量が少なくなるとイベントが表示されるので、必要に応じてデータの削除やハードディスクの増設を検討してください。

4.5.2 データフォルダで必要なディスクの最大容量

JP1/IT Desktop Management のデータフォルダのディスクの最大容量について説明します。

管理用サーバで必要なディスクの最大容量

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。また、JP1/IT Desktop Management 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	最大容量
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。	5 ギガバイト

データフォルダ	保存されるデータ	保存期間	最大容量
	• 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		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、追加管理項目がないこと、および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 • 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。
	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×所有ライセンス数 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 • 所有ライセンス数（管理対象の機器）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	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。
操作ログのデータベースフォルダ	不審操作に関する操作を取得対象にする場合の操作ログ（操作ログ一覧で参照できる操作ログのうち、保管先から取り込んでいないもの）	次のうち、どちらか早い方のタイミングまで保存されます。自動保存の設定をしておくと、削除される際に、古い操作ログが操作ログの保管先に自動保管されます。 • 操作ログが最大件数に達するまで 最大件数は、エージェント導入済みのコンピュータ（台）×2,700（件/日/台）×30（日）です。最大件数を超過したら、古い操作ログから削除されます。 • 操作ログが 500 日分取得されるまで	• 操作ログが最大件数に達するまで 30 日×管理対象のコンピュータ 3,000 台×80 キロバイト＝ 7.2 ギガバイト※1 • 操作ログが 500 日分取得されるまで 7.2 ギガバイト

データフォルダ	保存されるデータ	保存期間	最大容量
		500 日を超過したら、古い操作ログから削除されます。	
	すべての操作を取得対象にする場合の操作ログ（操作ログ一覧で参照できる操作ログのうち、保管先から取り込んでいないもの）	次のうち、どちらか早い方のタイミングまで保存されます。自動保存の設定をしておくと、削除される際に、古い操作ログが操作ログの保管先に自動保管されます。 ・ 操作ログが最大件数に達するまで 最大件数は、エージェント導入済みのコンピュータ（台）×2,700（件/日/台）×30（日）です。最大件数を超過したら、古い操作ログから削除されます。 ・ 操作ログが 500 日分取得されるまで 500 日を超過したら、古い操作ログから削除されます。	・ 操作ログが最大件数に達するまで 30 日×管理対象のコンピュータ 3,000 台×1.5 メガバイト＝ 135 ギガバイト※2 ・ 操作ログが 500 日分取得されるまで 135 ギガバイト
	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	削除するまで保存されます。	500 日×エージェント導入済みのコンピュータの台数×1.5 メガバイト※3
操作ログの保管先フォルダ	自動バックアップされた操作ログ	自動保管の設定をしている場合に、「操作ログのデータベースフォルダ」から超過した分を 1 日 1 回保管し、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。※2 管理者が決めた保管期間（日）×エージェント導入済みのコンピュータ（台）×1.5（メガバイト/日/台）×圧縮率 0.5 を目安に保管先のフォルダを用意してください。

注※1

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 80 キロバイトとする。
- 不審操作に関連する操作ログをすべて取得することとする。

注※2

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 1.5 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。

注※3

次の状況を想定しています。

- 保管先から操作ログを取り込む期間を 500 日とする。
- コンピュータごとの 1 日当たりの操作ログの容量を 1.5 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。

計算の詳細については、「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。

サイトサーバで必要なディスクの最大容量

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。また、JP1/IT Desktop Management 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	最大容量
データベースフォルダ	サイトサーバで使用する管理情報	削除するまで保存されます。	容量の上限はありません。 日数×接続するコンピュータの台数×150 キロバイトを目安に、フォルダを用意してください。
データフォルダ	次に示す情報 ・ 配布機能で使用されるパッケージ ・ エージェント、ネットワークモニタエージェントなどのプログラム ・ セキュリティポリシー	削除するまで保存されます。	約 10 ギガバイト 管理用サーバに登録されたパッケージと同じデータが格納されます。管理用サーバには、10 メガバイトのパッケージが 1,000 件登録されると想定しています。
操作ログのデータフォルダ	操作ログ	削除するまで保存されます。	容量の上限はありません。 日数×接続するコンピュータの台数×1.5 メガバイトを目安に、保管先のフォルダを用意してください。

関連リンク

- A.5 性能と見積もり

4.5.3 操作ログのバックアップに必要なディスク容量の目安

1 年分（365 日分）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次の表に示します。

機器の台数（台）	必要な容量（ギガバイト）		
	すべての操作を取得する場合	不審操作に関する操作だけ取得する場合	Web アクセスの操作ログだけ取得する場合※
100	29	1.3	14
300	89	3.8	42
500	147	6.2	70
700	206	8.7	98
1,000	293	13.0	139

機器の台数（台）	必要な容量（ギガバイト）		
	すべての操作を取得する場合	不審操作に関する操作だけ取得する場合	Web アクセスの操作ログだけ取得する場合※
3,000	645	39.0	408

注※　取得する必要のない Web サーバアドレスを設定しておくことで、取得する Web アクセスの操作ログの容量を少なくできますが、ここでは考慮していません。

すべての操作を取得対象にする場合、「すべての操作を取得する場合」の容量がそのまま該当します。不審と見なす操作の設定を変更しても、取得する操作ログの容量は変化しません。すべての操作ログのうち、不審と見なす操作ログの条件だけが変更になるためです。

操作ログを保管する場合の容量の見積もり例を次に示します。

見積もり例 1

管理対象の機器が 300 台の場合、すべての操作を取得対象とするが、Web アクセスの操作ログは取得しないときの容量は、次のように見積もれます。

89 ギガバイト－42 ギガバイト＝ 47 ギガバイト

見積もり例 2

管理対象の機器が 700 台の場合、不審操作に関する操作や Web アクセスの操作を含むすべての操作を取得するときの容量は、次のように見積もれます。

206 ギガバイト

関連リンク

- A.5 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

管理用サーバとサイトサーバでの、操作ログのデータベースに必要なディスク容量の目安について説明します。

管理用サーバでの目安

操作ログを取得する機器の台数とバックアップされた操作ログを取り込む期間ごとに、操作ログのデータベース（操作ログのデータベースフォルダ）に必要なディスク容量の目安を次の表に示します。

管理対象の機器（台）	必要な容量（ギガバイト）						
	取り込まない	10 日※1	30 日※1	50 日※1	100 日※1	300 日※1	500 日※1
100	23	40	44	48	59	102	144
200	29	48	56	64	87	172	257
300	35	56	68	80	115	242	369
400	41	65	81	97	142	312	482
500	49	74	96	117	170	382	595
600	53	80	105	129	198	452	601
700	60	89	117	145	225	523	607
800	65	97	129	161	253	593	614
900	71	104	141	178	280	620※2	620※2
1,000	81	117	160	202	308	627※2	627※2

管理対象の機器（台）	必要な容量（ギガバイト）						
	取り込まない	10 日※1	30 日※1	50 日※1	100 日※1	300 日※1	500 日※1
3,000	209	288	415	542	755※2	755※2	755※2

注※1　保管した操作ログを取り込む期間です。

注※2　データベースの最大レコード数（5 億件）に達した場合の値です。操作ログを取得する機器の台数によってレコード 1 件当たりの容量が異なるため、データベースに必要な容量が異なっています。

サイトサーバでの目安

サイトサーバに接続する機器の台数と運用する期間に応じて、データベースフォルダに必要なディスク容量の目安を次の表に示します。

サイトサーバに接続する機器（台）	必要な容量（ギガバイト）				
	1 年	2 年	3 年	4 年	5 年
100	9	14	19	25	31
300	19	35	51	67	82
500	31	56	82	109	135
1,000	56	108	161	213	265

注　1 台につき 1 日当たり 2,700 件の操作ログが発生すると想定した場合の値です。

関連リンク

- A.5 性能と見積もり

4.5.5 推奨ディスク容量の目安

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。

すべての操作を取得対象とする場合（管理用サーバ）

管理対象の機器（台）	推奨ディスク容量（ギガバイト）				
	1 年※	2 年※	3 年※	4 年※	5 年※
100	96	125	154	183	213
200	137	196	254	297	370
300	179	266	353	440	526
400	221	337	454	570	685
500	266	411	555	700	845
600	304	479	653	826	1,000
700	347	549	751	955	1,157
800	388	620	851	1,083	1,314
900	429	691	951	1,212	1,472
1,000	477	767	1,057	1,346	1,637
3,000	1,087	1,732	2,377	3,022	3,667

注※　操作ログの保管期間です。1 年当たり 365 日分のデータ量として計算しています。

不審操作に関する操作だけを取得対象とする場合（管理用サーバ）

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	69	70	71	73	75
200	82	86	88	91	93
300	96	100	104	108	112
400	111	116	122	127	132
500	128	134	141	147	154
600	138	147	155	162	170
700	153	162	171	181	190
800	167	177	187	198	208
900	180	193	204	216	227
1,000	200	214	227	240	254
3,000	481	520	559	598	637

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 365 日分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	・　不審操作に関する操作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 2,700 件取得される。 ・　過去の操作ログを閲覧するための「操作ログの最大取り込み期間」に、30 日が指定されている。
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、上の二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。
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。

サイトサーバで操作ログを収集する場合

サイトサーバに接続する機器（台）	推奨ディスク容量（ギガバイト）				
	1 年	2 年	3 年	4 年	5 年
100	24	49	73	97	122
300	73	146	219	292	365
500	122	244	365	487	609
1,000	244	487	731	975	1,218

注　1 台につき 1 日当たり 2,700 件の操作ログが発生すると想定した場合の値です。

関連リンク

- A.5 性能と見積もり

4.5.6 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またはサイトサーバの電源が 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、管理用サーバまたはサイトサーバの電源を ON にすると、コンピュータに一時保存された操作ログが、管理用サーバまたはサイトサーバにアップロードされます。

注意 コンピュータに一時保存できる操作ログは最大 1,000 時間分です。1,000 時間分を超過すると、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。

参考 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またはサイトサーバにまとめてアップロードされます。
なお、約 1 か月を超えて管理用サーバの電源が OFF になっている場合、管理用サーバにある操作ログの保存先フォルダに保存できる期間を超えるため、超過分の操作ログは取得できません。 そのため、操作ログを取得する設定の場合、管理用サーバの電源を長期間 OFF にするときは、約 1 か月を目安に電源を ON にしてください。サイトサーバの場合は、この制限はありません。

4.6 運用前の検討

ここでは、運用前の検討項目について説明します。

システムを運用する前に、だれ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。

関連リンク

- 4.6.1 ユーザーアカウントの検討
- 4.6.3 管理対象の検討
- 4.6.4 グループの検討
- 4.6.5 機器情報を管理するための検討
- 4.6.7 セキュリティ対策を実施するための検討
- 4.6.8 資産情報を管理するための検討
- 4.6.9 ネットワークを監視するための検討
- 4.6.10 定期メンテナンスの検討

4.6.1 ユーザーアカウントの検討

JP1/IT Desktop Management の利用者について検討します。ここでは、だれ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 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 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）。

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。

参考 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

- 2.3.2 ユーザーアカウントの権限
- 2.3.4 管轄範囲を設定した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

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 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 の利用許可を承認しますが、JP1/IT Desktop Management は利用しません。
ユーザーアカウント管理者	JP1/IT Desktop Management 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 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 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 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、業務分掌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 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 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 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 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。

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 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 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、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 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 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。

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機器を管理するかを検討し、さらにグループの作成方法も検討します。

グループを設定しておくと、同一のセキュリティポリシーを割り当てたり、グループごとの情報を管理したりできます。また、各種レポートをグループごとに表示して状況を確認することもできます。

グループの種類と管理方法の検討

どのようなグループで機器を管理するかを検討します。グループの種類と管理方法を次の表に示します。

種類	内容	管理方法
機器種別	コンピュータの OS の種別ごと、および機器種別ごとに自動的にグループが作成されます。	コンピュータから収集した「OS」の情報を基に自動的に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」の情報を基に自動的にグルーピングされます。
ネットワーク	ネットワークごとに自動的にグループが作成されます。	コンピュータから収集した「IP アドレス」の情報を基に自動的にグルーピングされます。
部署	機器が所属する部署ごとにグループを作成します。	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」を基に自動的に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 で管理している構成をそのままグループ構成に反映できます。
設置場所	機器の設置場所ごとにグループを作成します。	
カスタムグループ	管理者が任意にグループを作成します。	管理者が目的に合わせて手動でグルーピングします。

ここでは、次の内容を検討します。

1. 部署および設置場所でグループを管理するかどうか

   機器種別およびネットワークのグループの場合、自動でグループが作成されます。部署または設置場所の場合、デフォルトでは自動でグループが作成されないため、部署構成または設置場所ごとにグループを作成して管理するかどうか検討してください。

2. グループの構成の検討

   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取り込むかどうかを検討してください。

   なお、機器種別およびネットワークでのグループの場合、収集した情報を基に自動でグループが構成されるので、構成の検討は不要です。

グループの作成方法の検討

部署または設置場所でグループを作成する場合、グループの作成方法には次の 2 種類があります。

- 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的にグループを生成し、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。

参考 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 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。

  なお、組織内のすべての機器を発見したい場合は、探索範囲内にサイトサーバを設置することをお勧めします。サイトサーバ経由でネットワークが探索されるため、管理用サーバから直接参照できない機器も発見できるようになります。

- 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 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

  セキュリティ管理しない機器も管理対象とするときや、保有している機器の管理表を作成または更新するときに設定します。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

  機器をセキュリティ管理の対象とするときや、セキュリティ管理するコンピュータの管理表を作成または更新するときに設定します。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。

4.6.6 サイトサーバを設置するための検討

JP1/IT Desktop Management のシステムは、サイトサーバを設置することで、管理用サーバのディスク容量やネットワークに掛かる負荷を軽減できます。サイトサーバを設置する場合は、サイトサーバの台数、用途、グルーピングなどを検討します。

設置するネットワークと台数の検討

管理用サーバとエージェント導入済みのコンピュータ間のネットワークで、使用できるネットワーク帯域が少ない環境には、サイトサーバを設置することをお勧めします。

操作ログを取得するコンピュータが 3,000 台を超える場合は、サイトサーバを設置して操作ログの保管先にしてください。

注意 サイトサーバに保管された操作ログと管理用サーバに保管された操作ログは、同時には参照できません。このため、サイトサーバを利用する場合は、サイトサーバだけに操作ログを保管し、管理用サーバには操作ログを保管しないことをお勧めします。

また、エージェントを導入して管理するコンピュータが 5,000 台を超えるときは、サイトサーバを設置して配布機能の中継地点としてください。

サイトサーバは、システム内に複数設置できます。台数の制限はありません。

サイトサーバの台数は、次の事項を目安に検討してください。

- 1 台のサイトサーバに接続するコンピュータの台数は、1,000 台以内にしてください。
- ネットワークセグメントごとに 1 台以上のサイトサーバを設置してください。

また、ネットワークの探索を実行する場合、探索範囲内にサイトサーバを設置していると、サイトサーバ経由でネットワークが探索されるため、管理用サーバから直接参照できない機器も発見できます。このため、ネットワークの探索で組織内の機器をすべて発見したい場合は、管理用サーバまたはサイトサーバから機器を直接参照できるようにサイトサーバの設置を検討してください。

参考 常に負荷分散できる環境を実現するためには、サイトサーバグループに登録されているサイトサーバが、常に 1 台以上稼働している必要があります。24 時間稼働させるサイトサーバを構築する場合、機器のネットワーク接続を監視するコンピュータ（24 時間稼働を推奨）をサイトサーバにすることで、常時稼働しているコンピュータの台数を減らすことができます。

サイトサーバの用途の検討

サイトサーバは、操作ログの保管先と配布機能の中継地点の二つの役割があります。ネットワークセグメントごとにそれぞれの役割で使用するサイトサーバグループを指定できます。同じサイトサーバグループを指定することもできます。

操作ログは毎日取得されるため、大量のデータが蓄積されます。このため、操作ログを格納するサイトサーバには、十分なディスク容量があるコンピュータを選択することをお勧めします。

サイトサーバグループの検討

コンピュータがどのサイトサーバグループに接続するかは、ネットワークセグメントごとに対応するサイトサーバグループを選択することで決まります。その後は、サイトサーバグループに設定した優先度に従ってコンピュータとサイトサーバが接続します。

サイトサーバを操作ログの保管先として利用する場合、各ネットワークセグメントに指定するサイトサーバグループには、1 台のサイトサーバだけを設定することをお勧めします。これによって、1 台のコンピュータの操作ログが 1 台のサイトサーバに集約され、操作ログを管理しやすくなります。

配布機能の中継地点として利用する場合は、サイトサーバグループに複数のサイトサーバを設定することをお勧めします。これによって、1 台のサイトサーバに障害が発生しても、ほかのサイトサーバに接続できるため、可用性の高いシステムを実現できます。この場合、サイトサーバグループ内の各サイトサーバに接続の優先順位を付けることも、優先順位をランダムに設定することもできます。どのように負荷分散させるかを考慮して、サイトサーバグループの構成を検討してください。

注意 サイトサーバグループ内のサイトサーバのうち、どれか 1 台は稼働しているようにしてください。サイトサーバが稼働していない場合、システムが負荷分散できなくなります。

関連リンク

- 4.4.3 サイトサーバ構成

4.6.7 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。デフォルトでは、毎日 0:00 に判定されます。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。

4.6.8 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 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。

参考 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。

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。

参考 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 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。

4.6.9 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。

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。

参考 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。

参考 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

参考 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。

参考 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。

4.6.10 定期メンテナンスの検討

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。

- サイトサーバに保管された操作ログのバックアップ

  エージェント導入済みのコンピュータから取得した操作ログをサイトサーバに保管している場合、取得した操作ログを必要に応じてバックアップしてください。

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。

また、サイトサーバに保管された操作ログをバックアップするスケジュールも検討してください。

参考 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。

サイトサーバのメンテナンスをする場合、手動で操作ログのファイルをバックアップしてください。そのほかの作業は不要です。

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。

注意 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、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。

参考 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。

A

参考情報

ここでは、JP1/IT Desktop Management を使用する上での参考情報について説明します。

A.1 フォルダー一覧

管理用サーバに作成されるフォルダ

JP1/IT Desktop Management - 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。

フォルダ名	説明
JP1/IT Desktop Management - Manager のインストール先フォルダ	JP1/IT Desktop Management 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¥	インストールで出力されるログファイルのコピー先フォルダです。
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¥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。
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 - 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 のデータ格納フォルダです。

フォルダ名	説明
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 - Manager¥	プログラムフォルダです。

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。

サイトサーバに作成されるフォルダ

サイトサーバプログラムをインストールした場合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
サイトサーバプログラムのインストール先フォルダ	サイトサーバ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¥	インストールで出力されるログファイルのコピー先フォルダです。
mgr¥	管理用サーバ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¥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¥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¥log¥	トレースログ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¥shareAgt¥	エージェントと共通で利用される作業用フォルダです。
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¥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。

サイトサーバプログラム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¥jp1itdms¥Database¥※	サイトサーバのデータ格納フォルダです。
システムのプログラムメニュー¥JP1_IT Desktop Management - Remote Site Server¥	プログラムフォルダです。

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。

A.2 サービス、プロセス一覧

JP1/IT Desktop Management 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および説明を次の表に示します。

サービス名	サービス表示名	サービスプロセス名	説明
JP1_DTNAVI_AGCTRL	JP1_ITDM_Agent Control	**JP1/IT Desktop Management - 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_ITDM_Service	**JP1/IT Desktop Management - 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_SITESRV	JP1_ITDM_Remote Site Service	**サイトサーバプログラムのインストール先フォルダ**¥mgr¥bin¥jdnmssiteservice.exe	サイトサーバのサービスです。
JP1_DTNAVI_WEBCON	JP1_ITDM_Web Container	**JP1/IT Desktop Management - 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_ITDM_Web Server	**JP1/IT Desktop Management - 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_ITDM_DB Service	**JP1/IT Desktop Management - 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。
HiRDBEmbeddedEdition_JE2	JP1_ITDM_DB Service	**サイトサーバプログラムのインストール先フォルダ**¥mgr¥db¥BIN¥pdservice.exe	サイトサーバのデータベースサービスです。
HiRDBClusterService_JE1	JP1_ITDM_DB Cluster Service	**JP1/IT Desktop Management - 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。
HiRDBClusterService_JE2	JP1_ITDM_DB Cluster Service	**サイトサーバプログラムのインストール先フォルダ**¥mgr¥db¥BIN¥pdsha.exe	サイト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。

JP1/IT Desktop Management の各プロセスの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。

プロセス名	機能
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。
jdnagtpk.exe	エージェント登録のプロセスです。
jdnmscontroller.exe	サービスプロセスです。
jdnmsnetconservice.exe	サービスプロセスです。
jdnmsnodeinfwatch.exe	サービスプロセスです。
jdnmsremoteservice.exe	サービスプロセスです。
jdnmsrmservice.exe	サービスプロセスです。

プロセス名	機能
jdnmssecurityctrl.exe	サービスプロセスです。
jdnmsservice.exe	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。
pdxxx.exe※	データベースのプロセスです。
reorgdb.exe	コマンド（データベース再編成）のプロセスです。
startservice.exe	コマンド（開始）のプロセスです。
stopservice.exe	コマンド（停止）のプロセスです。
updatesupportinfo.exe	コマンド（サポート情報オフラインアップデート）のプロセスです。

注※　xxx は、3～7 文字の文字列です。

A.3 ポート番号一覧

JP1/IT Desktop Management で使用するポート番号について説明します。

JP1/IT Desktop Management - Manager のポート番号一覧

JP1/IT Desktop Management - Manager で使用するポート番号を次の表に示します。

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
31000	←	コンピュータ［ephemeral］	TCP	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。
31001	→	コンピュータ［ephemeral］	TCP	管理用サーバからコンピュータへの通信に使用されます。
31080	←	各画面［ephemeral］	TCP	各画面から管理用サーバへの通信に使用されます。
16992	→	エージェント［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。
31002～31013	なし	なし	TCP	JP1/IT Desktop Management の内部処理に使用されます。

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。

また、JP1/IT Desktop Management - Manager と JP1/IT Desktop Management - 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。

JP1/IT Desktop Management - Manager とエージェントレスのコンピュータの間のネットワークでは、次に示すポートを通過できるように設定してください。

「ファイルとプリンタの共有」で使用するポート

- プロトコル：TCP または UDP、ポート番号：445
- プロトコル：TCP、ポート番号：139
- プロトコル：UDP、ポート番号：137 および 138

SNMP プロトコルで使用するポート

- プロトコル：UDP、ポート番号：161

なお、プロトコルのポートは次の手順で設定できます。

1. Windows のコントロールパネルの［Windows ファイアウォール］－［詳細設定］を選択します。
2. 表示されるダイアログのツリーから［受信の規則］を選択してから、操作ウィンドウの［新しい規則］を選択します。
   表示される［新規の受信の規則ウイザード］に従って、プロトコルのポートを設定してください。

サイトサーバのポート番号一覧

サイトサーバで使用するポート番号を次の表に示します。

サイト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
31000	←	コンピュータ［ephemeral］	TCP	コンピュータからサイトサーバへの通信に使用されます。
31010	なし	なし	TCP	サイトサーバの内部処理に使用されます。

このポート番号は、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、サイト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。

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

コントローラおよびリモコンエージェントで使用するポート番号を次の表に示します。

コントローラまたはリモコンエージェント［ポート番号］	接続方向	接続対象［ポート番号］	プロトコル	用途
リモコンエージェント［31016］	←	コントローラ［31016］	TCP	コントローラからリモコンエージェントへの通信待機に使用されます。
リモコンエージェント［31017］	←	コントローラ［31017］	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］	← →	リモコンエージェントまたはコントローラ［31018］	TCP	リモコンエージェントとコントローラの間でのチャットに使用されます。
リモコンエージェント［31019］	→	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［31020］	→	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。

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動作設定］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 - Agent のポート番号一覧

JP1/IT Desktop Management - Agent で使用するポート番号を次の表に示します。

エージェントのポート番号	接続方向	接続対象［ポート番号］	プロトコル	用途
31000	→	管理用サーバ［ephemeral］	TCP	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。
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。
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。

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。

また、JP1/IT Desktop Management - Manager と JP1/IT Desktop Management - 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。

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。

A.4.1 インストール時のパラメーター

JP1/IT Desktop Management - 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

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 - Manager	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	C:¥Program Files¥Hitachi¥jp1itdmm¥

項目	内容	設定できる値	デフォルト
をインストールするフォルダ			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¥jp1itdmm¥」）になります。
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。

ユーザー登録

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（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 - 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	C:¥Program Files¥Hitachi¥jp1itdmm¥ 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¥jp1itdmm¥」）になります。

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	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※	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。	チェックする。
コンポーネントを配布パッケージとして登録する※	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※　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。

A.4.2 サイトサーバインストール時のパラメーター

サイトサーバのインストール時のパラメーターを次に示します。

ユーザー登録

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

項目	内容	設定できる値	デフォルト
サイトサーバ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	C:¥Program Files¥Hitachi¥jp1itdms¥ 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¥jp1itdms¥」）になります。

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	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。

A.4.3 セットアップ時のパラメーター

管理用サーバ、サイトサーバ、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 • データベース再作成	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

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 - 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)

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¥

項目	内容	設定できる値	デフォルト
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	チェックする 操作ログを取得します。 チェックしない	簡単インストールの場合 チェックする。

項目	内容	設定できる値	デフォルト
	作ログを取得するかどうかを設定します。	操作ログは取得しません。	カスタムインストールの場合 チェックしない。
管理対象の機器の台数	管理対象となる機器の台数の目安を指定します。	50～10000	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
操作ログの最大取り込み期間	自動的にバックアップされた操作ログを、データベースに取り込んで参照できるようにする期間を指定します。	0～500	簡単インストールの場合 0 カスタムインストールの場合 30
操作ログのデータベースフォルダ	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※	**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※　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。

操作ログの自動保管の設定

項目	内容	設定できる値	デフォルト
操作ログを自動的に保管する	操作ログを自動的にバックアップする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バックアップします。 チェックしない 操作ログは自動的にはバックアップされません。	チェックしない。
操作ログの保管先フォルダ※1	バックアップした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)

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)、「(」、「)」、「@」 、「¥」 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。

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
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
管理用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
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

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	配布機能で、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

セットアップの終了

項目	内容	設定できる値	デフォルト
媒体の登録※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	チェックする コンポーネントを自動更新します。	チェックする。

項目	内容	設定できる値	デフォルト
	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。	チェックしない コンポーネントを自動更新しません。	
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。

サイト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 • データベース再作成	設定変更

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。	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¥jp1itdms¥Database¥db¥
データフォルダ※1	サイト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。	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¥jp1itdms¥Database¥data¥
操作ログのデータフォルダ※1	操作ログのデータを格納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¥jp1itdms¥Database¥oplogf

注※1　データベースフォルダ、データフォルダ、および操作ログのデータフォルダには、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。

ポート番号の設定

項目	内容	設定できる値	デフォルト
サイトサーバで使用するポート番号	サイトサーバの内部処理で使用されるポート番号を指定します。	5001～49151	31010

その他の設定

項目	内容	設定できる値	デフォルト
サイトサーバでネットワークの帯域を制御する	配布機能で、サイト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 サイト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 サイト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

セットアップの終了

項目	内容	設定できる値	デフォルト
操作ログ情報再作成コマンド実行	サイトサーバに格納されている操作ログのインデックス情報を再作成するコマンドを実行するかどうかを設定します。	チェックする コマンドを実行します。 チェックしない コマンドを実行しません。	チェックする。

エージェントのセットアップ

項目	内容	設定できる値	デフォルト
接続する管理用サーバ	接続する管理用サーバの IP アドレスまたはホスト名を指定します。	IPv4 形式の IP アドレス、またはホスト名	管理用サーバのホスト名
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

A.4.4 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。

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 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

項目	内容	設定できる値	デフォルト
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 256 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 256 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。
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。

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

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が付与されます。

A.4.5 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
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	チェックする 発見されたコンピュータに、自動的	チェックしない。

項目	内容	設定できる値	デフォルト
	にエージェントを配信するかどうかを設定します。	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。	

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ユーザーアカウントを設定します。	登録されているユーザーアカウント	なし

A.4.6 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

項目	内容	設定できる値	デフォルト
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 20 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。 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。	20 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 255 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 255 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	日単位

項目	内容	設定できる値	デフォルト
		• 月単位	
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。	チェックしない。
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ユーザーアカウントを設定します。	登録されているユーザーアカウント	なし

A.4.7 エージェント設定のパラメーター

設定画面の［エージェント設定］画面から表示できる［エージェント設定の追加］ダイアログのパラメーターを次に示します。

エージェント基本動作

項目	内容	設定できる値	デフォルト
管理用サーバ	エージェントが接続する管理用サーバを指定します。	制限はありません。	管理用サーバのホスト名
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。	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。	1～9999	60
管理用サーバからの情報取得の間隔（分）	エージェントが管理用サーバにポーリングする間隔を指定します。	1～9999	30
流量制御	配布機能で管理用サーバからパッケージが転送された際に、エージェント側で使用するネットワーク帯域を制限するかどうかを選択します。	する 流量制御をします。パッケージの転送時に使用するネットワークの帯域の割合を 30%～99%で指定します。 しない 流量制御をしません。	しない
パスワード保護の設定	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。	チェックしない。
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。	制限はありません。	（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。	制限はありません。	（空白）

USB デバイス登録の設定

項目	内容	設定できる値	デフォルト
USB デバイスの登録を、パスワードで保護する	利用者から自由に USB デバイスを登録されないように、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 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	チェックしない。

項目	内容	設定できる値	デフォルト
		USB デバイスの登録時にパスワードを要求しません。	
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。	制限はありません。	（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。	制限はありません。	（空白）

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。
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

項目	内容	設定できる値	デフォルト
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動作設定

項目	内容	設定できる値	デフォルト
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
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。	1～65535	31016

項目	内容	設定できる値	デフォルト
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
リクエスタ接続先	コンピュータからの接続要求時のあて先のデフォルト値を指定します。	制限はありません。	管理用サーバのホスト名
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
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。
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。

リモートコントロールセキュリティの設定

項目	内容	設定できる値	デフォルト
許可コントローラ	リモートコントロールの接続を許可するコンピュータを指定します。	IPv4 形式の IP アドレスまたはホスト名	なし

項目	内容	設定できる値	デフォルト
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要求する認証情報を設定します。	Windows の認証情報または任意の認証情報(ユーザー名とパスワード)	なし
接続時に利用者の許可を求める	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。
ダイアログの表示時間	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（秒）を指定します。	0～180	10
利用者が応答しない場合の動作	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。	• 接続を許可する • 接続を拒否する	接続を許可する
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。	• 監視モード • 共有モード • 制御モード	共有モード

A.4.8 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

A.4.9 サーバ構成の設定のパラメーター

設定画面の［サーバ構成］－［サーバ構成の管理］画面のパラメーターを次に示します。

サーバ構成の設定

項目	内容	設定できる値	デフォルト
パッケージ配布の中継地点	パッケージの配布元となるサイトサーバグループを選択します。	サイトサーバグループ	選択されていない。
操作ログの保管先	エージェントの操作ログの通知先となるサイトサーバグループを選択します。	サイトサーバグループ	選択されていない。

管理用サーバ

項目	内容	設定できる値	デフォルト
ホスト名または IP アドレス	管理用サーバの IP アドレスまたはホスト名を設定します。	IPv4 形式の IP アドレス、またはホスト名	管理用サーバのホスト名

サイトサーバのグループ設定

項目	内容	設定できる値	デフォルト
グループ名	サイトサーバグループ名を指定します。	全角または半角で 512 文字以内の文字列	（空白）
サイトサーバ	サイトサーバグループに含めるサイトサーバを指定します。	サイトサーバの IP アドレスまたはコンピュータ名、およびエージェントの接続先となる優先順位	（空白）
接続先の優先順位	エージェントからの接続先となるサイトサーバの決定方法を選択します。	• 指定した優先順位に従って接続先を決定する • ランダムに接続先を決定する	指定した優先順位に従って接続先を決定する。
説明	サイトサーバグループ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）

A.4.10 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

A.4.11 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。	制限はありません。	（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。	半角英数で 8～64 文字の文字列※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。	半角英数で 8～64 文字の文字列※です。	（空白）

注※　「_」は指定できません。

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。	英小文字、英大文字、数字、記号をそれぞれ 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。	英小文字、英大文字、数字、記号をそれぞれ 1 文字以上含める必要があります。※	（空白）

注※　「_」は指定できません。

A.4.12 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
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

A.4.13 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 をチェックします。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］画面で設定されているユーザーアカウント

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 をチェックします。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] 画面で設定されているユーザーアカウント

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 をチェックします。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] 画面で設定されているユーザーアカウント

A.4.14 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。

メール通知されたいイベントの、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。 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	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。		

項目	内容	設定できる値	デフォルト
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。		

通知の対象外とするイベントを選択してください。

項目	内容	設定できる値	デフォルト
イベント番号	通知の対象外とするイベントを選択します。	0～1104	選択されていない。

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 をチェックします。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］画面で設定されているユーザーアカウント

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

A.4.15 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 ・ SSL ・ 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。

項目	内容	設定できる値	デフォルト
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）

A.4.16 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。	0～255 文字の文字列	（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。	0～255 文字の文字列	（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
SSL	SSL（Secure Sockets Layer）通信を有効にするかどうかを設定します。	チェックする SSL を有効にします。 チェックしない SSL を有効にしません。	チェックしない。
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。	Active Directory 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）
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。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	制限はありません。	（空白）

項目	内容	設定できる値	デフォルト
	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。		

A.4.17 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やウィルス対策製品情報など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	15:00
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 を選択します。メールアドレスが設定されていない場合は、	E-mail 形式の文字列です。	［ユーザーアカウントの管理］画面で設定されているユーザーアカウント

項目	内容	設定できる値	デフォルト
	メールアドレスを入力します。		

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)

A.4.18 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 文字以内の名称	(空白)
MDM 製品	接続する MDM 製品を選択します。	MobileIron	(空白)
MDM サーバのホスト名	MDM 製品をインストールしているコンピュータのホスト名を指定します。	制限はありません。	(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。	制限はありません。	(空白)
ユーザー ID	MDM 製品にログインするためのユーザー ID を指定します。	制限はありません。	(空白)
パスワード	MDM 製品にログインするための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)

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 製品から情報を取得する時刻を入力します。	00:00～23:59	23:30
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

A.4.19 その他のパラメーター

内部で設定されているパラメーターを次の表に示します。なお、ここで示すパラメーターは変更できません。

探索およびエージェント配信

項目	内容	設定されている値
探索の多重度	指定された探索範囲内の各 IP アドレスに対して、同時に探索を実行する数	10
エージェント配信の多重度	エージェントの配信を同時に実行できる数	10

項目	内容	設定されている値
ARP の使用	探索時に ARP を使うかどうか	使う
ICMP の使用	探索時に ICMP を使うかどうか	使う
SNMP のバージョン	SNMP の認証の探索時に使用される SNMP のバージョン	v1
ARP リトライ回数	探索時に ARP を使う場合のリトライ回数	0 回
ARP 送信間隔	探索時に ARP を使う場合の、ARP の応答の送信間隔	1 秒
ICMP リトライ回数	探索時に ICMP を使う場合のリトライ回数	0 回
ICMP 応答監視時間	探索時に ICMP を使う場合の、ICMP の応答の監視時間	2 秒
SNMP リトライ回数	探索時に SNMP を使う場合のリトライ回数	2 回
SNMP 応答監視時間	探索時に SNMP を使う場合、SNMP の応答の監視時間	3 秒
ICMP 送信時の TTL	ICMP を使う場合の TTL（ホップ数）	128
エージェント配信のリトライ間隔	エージェント配布に失敗した場合にリトライするまでの間隔	180 分
エージェント配信のリトライ回数	エージェント配布に失敗した場合にリトライする回数	5 回
エージェントのインストール確認時間	エージェント配信後にエージェントが正常にインストールされたかを確認する時間	10 分

Active Directory 連携

項目	内容	設定されている値
コンピュータ引き当てキー	JP1/IT Desktop Management に登録されているホスト名と引き当てる LDAP の属性名	コンピュータの「DNS 名」または「コンピュータ名」
LDAP 通信接続タイムアウト時間	LDAP サービスプロバイダの接続タイムアウト時間	30 秒
LDAP 通信リトライ回数	LDAP サービスプロバイダのリトライ回数	0 回
LDAP 通信リトライ間隔	LDAP サービスプロバイダのリトライ間隔	0 秒

更新プログラム情報の取得

項目	内容	設定されている値
接続リトライ回数	日立 Web サーバに接続失敗した場合の接続リトライ回数	10 回
接続リトライ間隔	日立 Web サーバに接続失敗した場合の接続リトライ間隔	300 秒

稼働監視

項目	内容	設定されている値
ソフトウェア稼働監視履歴の保存	下位システムから通知された操作ログおよび抑止履歴を保存するかどうかの設定	保存する
抑止履歴最大イベント数	すべてのエージェント分を合わせて保存されるソフトウェア起動抑止の抑止履歴の最大イベント数 設定された件数を超えた場合、古い抑止履歴から削除されます。	1,000 件

データベース接続

項目	内容	設定されている値
データベース接続リトライ回数	データベース接続失敗時のリトライ回数	0 回
データベース接続リトライ間隔	データベース接続失敗時のリトライ間隔	0 秒

操作ログ

項目	内容	設定されている値
リストアオンライン期間	データベースマネージャまたはコマンドからバックアップをリストアした場合に、オンラインとして復元する操作ログの日数	7 日
未来日付データの格納しきい値	管理用サーバより日付が未来の操作ログが収集されてきたときに、データベースに格納する期間のしきい値	7 日

配布機能

項目	内容	設定されている値
タスク実行チェック間隔	スケジュール実行されるタスクの有無をチェックする間隔	60 秒
タスク削除チェック間隔	実行完了後、一定期間が経過して削除対象となったタスクの有無をチェックする間隔	60 分
タスク削除期限	完了したタスクが削除されるまでの期限	30 日
MSI コマンドライン	MSI ファイルをパッケージングする際に、自動的に設定されるサイレントインストール用のコマンドライン	`Msiexec /i "%s" /qn REBOOT=ReallySuppress`
ポリシーベースタスク削除チェック間隔	実行完了後、一定期間が経過して削除対象となったポリシーベースのタスクの有無をチェックする間隔	60 分
ポリシーベースタスク削除期限	完了したポリシーベースのタスクが削除対象となるまでの期限	7 日

項目	内容	設定されている値
ポリシーベースタスクエラーリトライ回数	セキュリティ対策によるポリシーベースタスクがエラーになった場合のリトライ回数	5 回
更新プログラムファイル自動作成エラーリトライ回数	更新プログラムファイルの自動作成のリトライ回数	5 回

ユーザーアカウントの管理

項目	内容	設定されている値
アカウントロックとなる連続失敗回数	連続してパスワード入力に失敗した回数（アカウントがロックされるまでの回数）	3 回

容量の監視

項目	内容	設定されている値
データベースフォルダの警告しきい値	データベースフォルダの空き容量に設定されている警告しきい値	3,072 メガバイト
データベースフォルダのエラーしきい値	データベースフォルダの空き容量に設定されているエラーしきい値	500 メガバイト
データフォルダの警告しきい値	データフォルダの空き容量に設定されている警告しきい値	3,072 メガバイト
データフォルダのエラーしきい値	データフォルダの空き容量に設定されているエラーしきい値	500 メガバイト
操作ログのデータベースフォルダの警告しきい値	操作ログのデータベースフォルダの空き容量に設定されている警告しきい値	操作ログのデータベース容量見積もり値※の 10%
操作ログのデータベースフォルダのエラーしきい値	操作ログのデータベースフォルダの空き容量に設定されているエラーしきい値	操作ログのデータベース容量見積もり値※の 3%
操作ログの保管先フォルダの警告しきい値	操作ログの保管先フォルダの空き容量に設定されている警告しきい値	操作ログのデータベース容量見積もり値※の 10%
操作ログの保管先フォルダのエラーしきい値	操作ログの保管先フォルダの空き容量に設定されているエラーしきい値	操作ログのデータベース容量見積もり値※の 3%

注※　管理用サーバのセットアップで設定します。

監査ログ

項目	内容	設定されている値
監査ログの出力	監査ログを出力するかどうか	出力する

管理用サーバオプション

項目	内容	設定されている値
同時に接続できる下位システム数	同時に接続する下位システムの数	1,000 台
下位システムの同時実行要求数	エージェントへの要求を実行するときに、同時に処理する下位システムの数	100 台

項目	内容	設定されている値
接続要求受信スレッド数	エージェントからの接続要求を受け付けるためのスレッド本数	20 本
起動実行要求リトライ回数	エージェントへの起動要求に失敗したときのリトライ回数	3 回
起動応答受信タイムアウト	エージェントへ起動要求送信後、応答待ちまでのタイムアウト時間	30 秒
起動スレッド数	エージェントへ起動要求送信するスレッドの数	100 本
電源 ON リトライ間隔	コンピュータの電源 ON に失敗したときのリトライ間隔	30 秒
電源 ON リトライ回数	コンピュータの電源 ON に失敗したときのリトライ回数	5 回
電源 ON リトライ監視間隔	コンピュータの電源 ON に失敗した対象エージェントへのリトライ要否チェック間隔	30 秒
同期制御同時接続数	同期制御通信の同時接続数	64 本
通信スレッドプールタイムアウト	エージェント通信およびマネージャ内同期の処理用スレッドの再利用待機時間	30,000 ミリ秒
ファイル送信状態監視時間	ファイルの転送処理で送信できるかを監視する最大時間	10 分
電源状態監視間隔	電源状態監視間隔	30 分
エージェント制御サービス自動リトライ回数	エージェント制御サービス内部でエラーとなった場合のリトライ回数	3 回
エージェント制御サービス自動リトライ間隔	エージェント制御サービス内部でエラーとなった場合のリトライを行う期間	900 秒
配布接続可否の接続数のしきい値	配布接続可否の接続数のしきい値	80%

マネージャサービス

項目	内容	設定されている値
通信リトライ回数	マネージャサービスの内部通信でエラーとなった場合のリトライ回数	0 回
通信リトライ間隔	マネージャサービスの内部通信でエラーとなった場合のリトライ間隔	0 秒
通信タイムアウト時間	マネージャサービスの内部通信の応答待ち時間	1 秒
マネージャサービス終了待ち時間	マネージャサービスの各サービスの終了待ち時間	15 秒
メール通知リトライ回数	メール通知時にエラーとなった場合のリトライ回数	0 回
メール通知リトライ間隔	メール通知時にエラーとなった場合のリトライ間隔	0 秒
メール通知タイムアウト時間	メール通知時の応答待ち時間	10 秒

項目	内容	設定されている値
メッセージ通知リトライ回数	メッセージ通知時にエラーとなった場合のリトライ回数	3 回
メッセージ通知リトライ間隔	メッセージ通知時にエラーとなった場合のリトライ間隔	1 秒
メッセージ通知タイムアウト時間	メッセージ通知時の応答待ち時間	10 秒
データベースコネクション最大プール数	マネージャサービスの各サービスが同時に使用する最大コネクション数	10 個
インベントリ情報監視間隔	インベントリ情報が更新されているかを確認する間隔	60 秒
プロセス起動待ち時間	マネージャサービスの各プロセスの起動待ち時間	10 秒
プロセス終了待ち時間	マネージャサービスの各プロセスの終了待ち時間	5 秒

通信設定

項目	内容	設定されている値
通信先の決定方法	通信先を決定する情報の種類	ホスト名
アドレスの解決方法	ジョブ作成または実行時に IP アドレスを取得する方法	Windows ネットワークを使用する※
起動プロトコル	エージェントを起動するときに使用するプロトコル	TCP

注※　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 のシステム構成から IP アドレスを取得します。

A.5 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

- A.5.1 メモリ所要量
- A.5.2 ディスク占有量
- A.5.3 前提となる CPU

A.5.1 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それぞれ表に示します。

- 管理用サーバ
- 操作画面を表示するコンピュータ
- サイトサーバプログラムをインストールするコンピュータ
- エージェントを導入するコンピュータ
- ネットワークモニタを有効にするコンピュータ
- エージェントレスのコンピュータ

- 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

管理用サーバ

実装メモリ：最低 2 ギガバイト（3 ギガバイト以上を推奨）

仮想メモリ：最大 2.8 ギガバイト

操作画面を表示するコンピュータ

実装メモリ：2 ギガバイト以上を推奨

サイトサーバプログラムをインストールするコンピュータ

実装メモリ：最低 1.5 ギガバイト（2 ギガバイト以上を推奨）

仮想メモリ：最大 1.5 ギガバイト

エージェントを導入するコンピュータ

項目	動作環境	
実装メモリ	Windows 7 の場合	1 ギガバイト（OS 推奨メモリ）＋ 20 メガバイト以上
	Windows Server 2008 または Windows Vista の場合	512 メガバイト（OS 推奨メモリ）＋ 20 メガバイト以上
	Windows Server 2003 または Windows XP の場合	128 メガバイト（OS 推奨メモリ）＋ 20 メガバイト以上
	Windows 2000 の場合	64 メガバイト（OS 推奨メモリ）＋ 20 メガバイト以上
仮想メモリ	40 メガバイト	

操作ログを取得するには、さらに次に示す容量が必要です。

項目	動作環境	
実装メモリ	OS が 32 ビット版の Windows の場合	仮想メモリに必要な容量×0.5 を、8 の倍数で切り上げた値以上
	OS が 64 ビット版の Windows の場合	
仮想メモリ	OS が 32 ビット版の Windows の場合	34 メガバイト＋ 11 メガバイト×（エージェントを導入するコンピュータにログオンしているユーザー数－1）以上
	OS が 64 ビット版の Windows の場合	43 メガバイト＋ 16 メガバイト×（エージェントを導入するコンピュータにログオンしているユーザー数－1）以上

（例）OS が 32 ビット版の Windows の場合、エージェントを導入するコンピュータにログオンしているユーザー数が三つのときに必要な容量

- 実装メモリ

  28 メガバイト※を 8 の倍数で切り上げた値＝ 32 メガバイト

  注※　28 メガバイトは、仮想メモリに必要な容量 56 メガバイト×0.5 です。
- 仮想メモリ

  34 メガバイト＋ 11 メガバイト×2 ＝ 56 メガバイト

ネットワークモニタを有効にするコンピュータ

実装メモリ：1 ギガバイト+20 メガバイト以上

仮想メモリ：最大 22 メガバイト+（10×**監視する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

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。実行プログラムの実行時のメモリ使用量は、22 メガバイトです。

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	
実装メモリ	Windows 7 の場合	1 ギガバイト（OS 推奨メモリ）+α※以上
	Windows Server 2008 の場合	512 メガバイト（OS 推奨メモリ）+α※以上
	Windows Vista の場合	512 メガバイト（OS 推奨メモリ）+α※以上
	Windows Server 2003 の場合	128 メガバイト（OS 推奨メモリ）+α※以上
	Windows XP の場合	128 メガバイト（OS 推奨メモリ）+α※以上

注※　α は次に示す A～D の合計値です。

A：描画用の一時バッファ（5.0 メガバイト（標準的なアプリケーション操作時）×接続エージェント数）

B：ファイル転送中の一時バッファ（2.0 メガバイト）

C：チャットサーバ用のバッファ（2.0+（0.1×接続数）メガバイト）

D：チャットクライアント用のバッファ（2.0+（0.2×接続数）メガバイト）

A.5.2 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それぞれ表に示します。

- 管理用サーバ
- 操作画面を表示するコンピュータ
- サイトサーバプログラムをインストールするコンピュータ
- エージェントを導入するコンピュータ
- ネットワークモニタを有効にするコンピュータ
- エージェントレスのコンピュータ
- 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

管理用サーバ

管理用サーバに必要なドライブの空き容量を次に示します。

項目	動作環境
インストールドライブ（本体容量）	2.4 ギガバイト以上（推奨は 3 ギガバイト）
システムドライブ（作業領域分の容量）	500 メガバイト
データベース格納フォルダのドライブ（データ容量）	35 ギガバイト以上（簡単インストールの場合）

項目	動作環境
	13 ギガバイト以上（カスタムインストールの場合）

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、さらに次に示す空き容量が必要です。

項目	動作環境
データベース格納フォルダのドライブ（データ容量）	20 ギガバイト※以上

注※　セットアップ画面の操作ログの設定で、［管理対象の機器の台数］を 50 台、［操作ログの最大取り込み期間］を 0 日とした場合に必要な空き容量です。

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。

項目	動作環境
JP1/IT Desktop Management - Manager がインストールされているドライブ	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
データフォルダが格納されるドライブ	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
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 - 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	

操作画面を表示するコンピュータ

JP1/IT Desktop Management によるディスクの占有量はありません。

サイトサーバプログラムをインストールするコンピュータ

サイトサーバに必要なドライブの空き容量を次に示します。

項目	動作環境
インストールドライブ（本体容量）	2.4 ギガバイト以上（推奨は 3 ギガバイト）
データベース格納フォルダのドライブ（データ容量）	4 ギガバイト以上

自動アップデートでサイトサーバプログラ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
サイトサーバプログラ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	
システムドライブ	

エージェントを導入するコンピュータ

20 メガバイト以上（40 メガバイト以上推奨）の空き容量が必要です。

操作ログを取得する場合、さらに次に示す空き容量が必要です。

項目	動作環境
エージェントがインストールされているドライブ	120 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。

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（ZIP ファイルに圧縮する前）の 2 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	

ネットワークモニタを有効にするコンピュータ

エージェントを導入するコンピュータのディスク占有量に加えて、20 メガバイト以上（40 メガバイト以上推奨）の空き容量が必要です。

エージェントレスのコンピュータ

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。

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

20 メガバイト以上の空き容量が必要です。

関連リンク

- 4.5 データベースの検討

A.5.3 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 についてそれぞれ表に示します。

- 管理用サーバ
- 操作画面を表示するコンピュータ
- サイトサーバプログラムをインストールするコンピュータ
- エージェントを導入するコンピュータ
- ネットワークモニタを有効にするコンピュータ
- エージェントレスのコンピュータ
- 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

管理用サーバ

2.0 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

操作画面を表示するコンピュータ

- 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

サイトサーバプログラムをインストールするコンピュータ

2.0 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

エージェントを導入するコンピュータ

項目	動作環境	
CPU	Windows 7 の場合	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 の場合	1.0 ギガヘルツ以上の 32 ビットプロセッサ、または 1.4 ギガヘルツ以上の 64 ビットプロセッサ
	Windows Vista の場合	800 メガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
	Windows Server 2003 の場合	133 メガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
	Windows XP の場合	300 メガヘルツ以上の 32 ビットプロセッサ
	Windows 2000 の場合	133 メガヘルツ以上の 32 ビットプロセッサ

ネットワークモニタを有効にするコンピュータ

項目	動作環境	
CPU	Windows 7 の場合	1.0 ギガヘルツ以上の 32 ビット（x86） または 64 ビット（x64）プロセッサ
	Windows Server 2008 の場合	1.0 ギガヘルツ以上の 32 ビット（x86）、 または 1.4 ギガヘルツ以上の 64 ビット（x64）プロセッサ
	Windows Server 2003 の場合	133 メガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ

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。

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	
CPU	Windows 7 の場合	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 の場合	1.0 ギガヘルツ以上の 32 ビットプロセッサ、または 1.4 ギガヘルツ以上の 64 ビットプロセッサ
	Windows Vista の場合	800 メガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
	Windows Server 2003 の場合	133 メガヘルツ以上の、32 ビットプロセッサまたは 64 ビットプロセッサ
	Windows XP の場合	300 メガヘルツ以上の 32 ビットプロセッサ

A.6 制限値一覧

JP1/IT Desktop Management 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。

ログイン画面

項目	制限値	デフォルト	説明
連続でログインに失敗してもロックが掛からない回数	0～2 回	－	－

（凡例）－：該当なし

ホーム画面（[始めましょう] ボタン）

機能	項目	制限値	デフォルト	説明
Active Directory を探索する方法	Active Directory ドメイン	上限なし	0 個	想定する上限は、100 個です。この項目は、設定画面の項目と同じです。
ネットワークを探索する方法	探索範囲	上限なし	1 個	想定する上限は、50 個です。デフォルトでは、管理用サーバセグメントの探索範囲が登録されています。
	認証情報	上限なし	1 個	想定する上限は、50 個です。デフォルトでは、SNMP 標準の認証情報が登録されています。

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。

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。 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 100 個です。
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、使用禁止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。
	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。

機能	項目	制限値	デフォルト	説明
更新プログラム	表示件数	上限なし	0 件	想定する上限は、15,000 件です。
操作ログ	表示件数	次のうち早いタイミングの方 ・ エージェント導入済みのコンピュータ（台）×2,700（件/日/台）×30（日） ・ 500 日で取得する件数	0 件	―
分散操作ログ	表示件数	上限なし	0 件	日付、発生元機器の延べ台数および操作ログの件数の一覧を表示させる場合、想定する上限は、2,000 件です。 発生元、管理元のサイトサーバ数および操作ログの件数の一覧を表示させる場合、想定する上限は、10,000 件です。

（凡例）―：該当なし

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	想定する上限は、37,500 件です。
	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、[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	10 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。
	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

機能	項目	制限値	デフォルト	説明
				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	想定する上限は、6,000 件です。
	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、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	想定する上限は、100 件です。
	エクスポートする項目数	1〜10 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	想定する上限は、9,750 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。

機能	項目	制限値	デフォルト	説明
	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。

（凡例）－：該当なし

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	－
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	－
	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。

（凡例）－：該当なし

配布画面

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	－
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	－

（凡例）－：該当なし

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	保有している製品ライセンス数×250 ＋ 10,000 件	0 件	－

（凡例）－：該当なし

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	想定する上限は、50 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。
機器の探索	発見した機器	上限なし	0 件	想定する上限は、100 件です。 －
	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	－
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	－
サーバ構成	サーバ構成の設定	上限なし	0 個	想定する上限は、50 個です。機器画面の［機器一覧（ネットワーク）］で表示されるネットワークセグメントが表示されます。
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、100 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、100 個です。
	ネットワーク制御リストの設定	上限なし	0 件	想定する上限は、10,000 件です。ここでは、管理対象と除外対象のコンピュータの総数を 2 倍した件数を想定しています。
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 各項目の選択肢の数には、上限なし ・ テキスト型：0～75 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
		各項目には、0～256文字を指定できる		
	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。
	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	10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。

機能	項目	制限値	デフォルト	説明
				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。
他システムとの接続	Active Directory ドメイン	上限なし	0 個	想定する上限は、100 個です。 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、5 個です。

（凡例）－：該当なし

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。

メニューエリア

機能	項目	制限値	デフォルト	説明
• セキュリティ画面 • 資産画面 • 機器画面 • 配布画面	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。
	カスタムグループに追	上限なし	0 項目	想定する上限は、5,000 項目です。

機能	項目	制限値	デフォルト	説明
	加できる項目			
• セキュリティ画面 • 資産画面 • 機器画面 • 配布画面 • 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。

（凡例）－：該当なし

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。

A.7 各種機能が自動実行されるタイミング

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、「2.14.5 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 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 に登録します。	毎日 23:00※1
	利用者情報の収集	部署、設置場所、利用者名などの利用者情報の入力画面を定期的に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。	毎月 1 日（指定された日）※2

機能		説明	実行されるタイミング
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］に指定した更新スケジュールに従って、サポートサービスサイトに接続し、次に示す情報が自動的に最新の情報に更新されます。 ・ 更新プログラムの情報 ・ ウィルス対策製品の情報 ・ JP1/IT Desktop Management がサポートする OS やサービスパックの情報 ・ エージェントの修正パッチの情報 サポートサービスサイトから最新の情報を取得すると、管理対象のコンピュータに最新の更新プログラムやウィルス対策製品が適用されているかどうかを、セキュリティポリシーで判定できるようになります。 また、エージェントの修正パッチを自動的に適用したり、最新 OS のコンピュータを自動的に判別したりできるようになります。	毎日決められた時刻（JP1/IT Desktop Management 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
	ウィルス定義ファイルの更新	コンピュータから収集した情報を基に、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を最新に更新して、セキュリティ判定を実施します。	ウィルス定義ファイルのバージョンが更新されたとき
	エージェントの更新確認	サポートサービスサイトに接続して、エージェントの最新バージョンまたは修正パッチがリリースされている場合に、自動的にダウンロードして適用します。	毎日決められた時刻（JP1/IT Desktop Management 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

機能		説明	実行されるタイミング
操作ログ	操作ログの自動バックアップ	コンピュータから取得した操作ログをバックアップします。	毎日 4:00
	操作ログのバックアップ先フォルダに対する空き容量の監視	操作ログのバックアップ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
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で重要度の高い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 製品からの情報取得	MDM 製品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 23:30※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。	管理用サーバの場合、毎日 5:00 サイトサーバの場合、毎日 2:00

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　機器画面から実行のタイミングを設定できます。

A.8 再起動によって設定が適用されるケース

JP1/IT Desktop Management 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。

- JP1/IT Desktop Management - Manager をインストールした場合（Windows XP Professional Service Pack 2 または 3 のとき）
- 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

JP1/IT Desktop Management - Manager をインストールした場合（Windows XP Professional Service Pack 2 または 3 のとき）

JP1/IT Desktop Management - Manager をインストールしたコンピュータを再起動してください。再起動すると、インストールが完了します。ただし、日立の他製品の、動作処理の流れをトレースする機能（HNTRLib2）がインストールされていれば、再起動は不要です。

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。

- Windows 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）
- Windows 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、Windows XP、および Windows 2000 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）
- USB デバイスの読み取りと書き込みの抑止（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）

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。

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。

- Windows 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）
- Windows 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、Windows XP、および Windows 2000 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）

A.9 このマニュアルの参考情報

A.9.1 関連マニュアル

関連マニュアルを次に示します。必要に応じてお読みください。

- JP1 Version 9 JP1/IT Desktop Management 導入・設計ガイド（3020-3-S93）

- JP1 Version 9 JP1/IT Desktop Management 構築ガイド（3020-3-S94）
- JP1 Version 9 JP1/IT Desktop Management 運用ガイド（3020-3-S95）

A.9.2 関連ドキュメント

関連ドキュメントを次に示します。必要に応じてお読みください。

- JP1/IT Desktop Management オンラインヘルプ

A.9.3 このマニュアルでの表記

このマニュアルでは、製品名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
Firefox		Firefox(R)
Linux		Linux(R)
Pentium		Intel Pentium(R)
VMWare		VMWare(R)
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

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

A.9.4 このマニュアルで使用する英略語

このマニュアルで使用する英略語を次に示します。

英略語	英字での表記
ARP	Address Resolution Protocol
AVI	Audio Video Interleave
BIOS	Basic Input / Output System
BMP	Bit Map
CD	Compact Disc
CD-R	Compact Disc Recordable
CD-ROM	Compact Disc Read Only Memory
CIDR	Classless Inter-Domain Routing

英略語	英字での表記
CPU	Central Processing Unit
CSV	Comma Separated Values
DB	Database
DBMS	Database Management System
DCOM	Distributed Component Object Model
DHCP	Dynamic Host Configuration Protocol
DVD	Digital Versatile Disc
FC	Fibre Channel
FD	Floppy Disk
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
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
ISMS	Information Security Management System
IT	Information Technology
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
RFB	Remote Framebuffer
SD	Secure Digital
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

英略語	英字での表記
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Account Control
UDID	Unique Device IDentifier
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Universal Time, Coordinated
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

A.9.5 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。

用語解説

JP1/IT Desktop Management 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 と接続します。

JCR ファイル
拡張子が JCR の、JP1/IT Desktop Management 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
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 - Agent
JP1/IT Desktop Management 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 - Manager
JP1/IT Desktop Management のサーバ機能を提供するプログラムです。

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 と接続します。

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 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。

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）

インストールセット
JP1/IT Desktop Management - 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 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 - Manager に情報を通知したり、JP1/IT Desktop Management - 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 - Agent」です。

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。管理用サーバ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 - 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。

（カ行）

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 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 の管理者が、ふだん JP1/IT Desktop Management 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 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。

管理用サーバ
JP1/IT Desktop Management - Manager がインストールされたコンピュータです。

機器情報
JP1/IT Desktop Management が管理対象の機器から収集する情報です。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。

契約会社情報

JP1/IT Desktop Management 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 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）

サイトサーバ

サイトサーバプログラムがインストールされたコンピュータです。サイトサーバを配置して、操作ログの保管先や配布機能の中継地点として利用することで、管理用サーバやネットワークの負荷を分散できます。

サイトサーバグループ

一つ以上のサイトサーバをグループ化したものです。サイトサーバを配置する際は、サイトサーバグループを設定し、各ネットワークセグメントの操作ログの保管先や配布機能の中継地点として指定します。サイトサーバグループに複数のサイトサーバを登録しておくと、あるサイトサーバに接続できなかった場合も自動的にグループ内のほかのサイトサーバに接続され、サイトサーバの機能の可用性が高まります。

サイトサーバプログラム

管理用サーバの負荷分散に利用する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 - Manager およびエージェントと通信して、操作ログ関連の機能および配布関連の機能をサポートします。プログラム名は「JP1/IT Desktop Management - Remote Site Server」です。

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 からインターネットを介して接続し、最新のエージェント、OS および Internet Explorer についての最新の更新プログラムの情報などを取得できます。

参照権限

JP1/IT Desktop Management 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。

システム管理権限

JP1/IT Desktop Management 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 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。

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 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。

製品版ライセンス
購入したライセンスのことです。使用期限はありません。

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 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。エージェント導入済みのコンピュータから収集できます。

ソフトウェア検索リスト
自動的には収集されないソフトウェア情報を収集するための条件を指定したリストです。ここで指定した条件でコンピュータ内のソフトウェアが検索され、発見されるとソフトウェア情報として収集されます。

ソフトウェアライセンス情報
JP1/IT Desktop Management 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。

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。

追加管理項目
JP1/IT Desktop Management 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、インストールの設定などの項目について JP1/IT Desktop Management が提供するエージェント設定です。エージェントをコンピュータに導入したときは、このエージェント設定がデフォルトで適用されます。

デフォルトポリシー
JP1/IT Desktop Management 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。

（ナ行）

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。操作画面からエージェント導入済み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 - 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 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
コンピュータに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ためのデータを登録したものです。

判定

JP1/IT Desktop Management 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。

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。

分散操作ログ

サイトサーバに保管されている操作ログです。操作画面からは、管理用サーバに保管されている操作ログとは別に参照できます。

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 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 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 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 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

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

て

と

な

に

ね

は

ひ

ふ

ほ

ま

み

め

も

ゆ

よ

ら

り

れ

ろ

わ