HITACHI
Inspire the Next

統合システム運用管理　資産・配布管理

多様化するビジネス環境を踏まえたIT資産管理

～フレキシブルかつスマートに管理できるJP1/ITDM～

2011/11/17

株式会社 日立製作所
情報・通信システム社　ソフトウェア事業部
販売推進部　主任技師　伊庭　健一

uVALUE

HITACHI
Inspire the Next

Contents

uVALUE

HITACHI
Inspire the Next

1
JP1/IT Desktop Managementの概要

１.多様化するビジネス環境での課題
２.IT資産のライフサイクル管理を効率良く実現
３.JP1/IT Desktop Managementの機能

uVALUE

1-1. 多様化するビジネス環境での課題

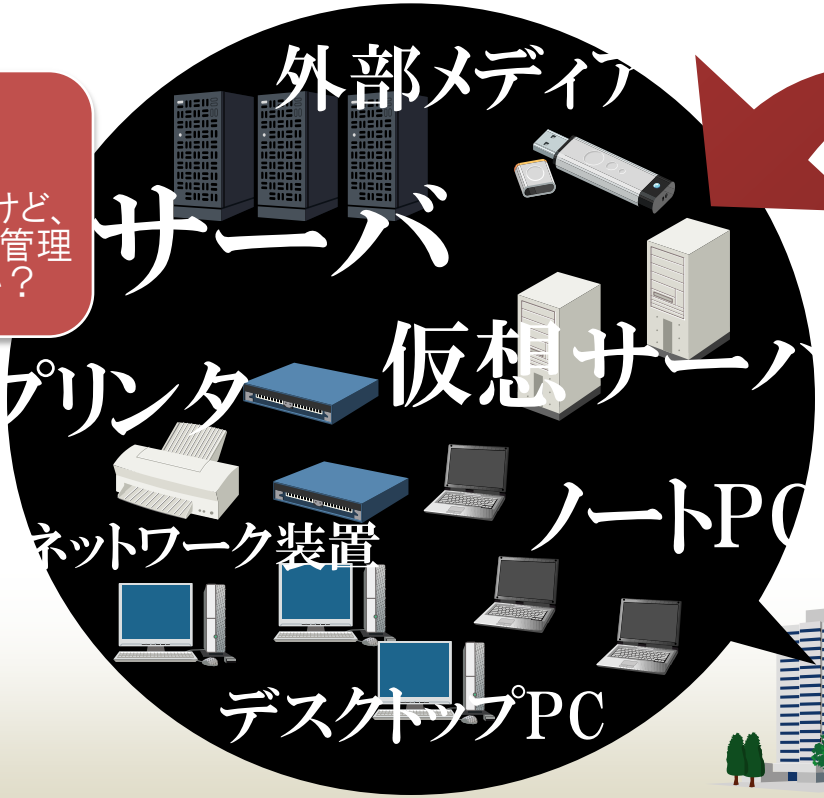
HITACHI
Inspire the Next

課題

スマートフォンや仮想デスクトップなど
ビジネス環境の多様化・複雑化に伴い、
IT資産管理業務の負担が増大している。

IT資産管理の対象は
増加する一方・・・

効率化を求められるけど、
混沌とした環境をどう管理
すればよいのだろうか？



uVALUE

HITACHI
Inspire the Next

JP1/IT Desktop Managementで組織内のIT資産を一元管理！

これで解決！

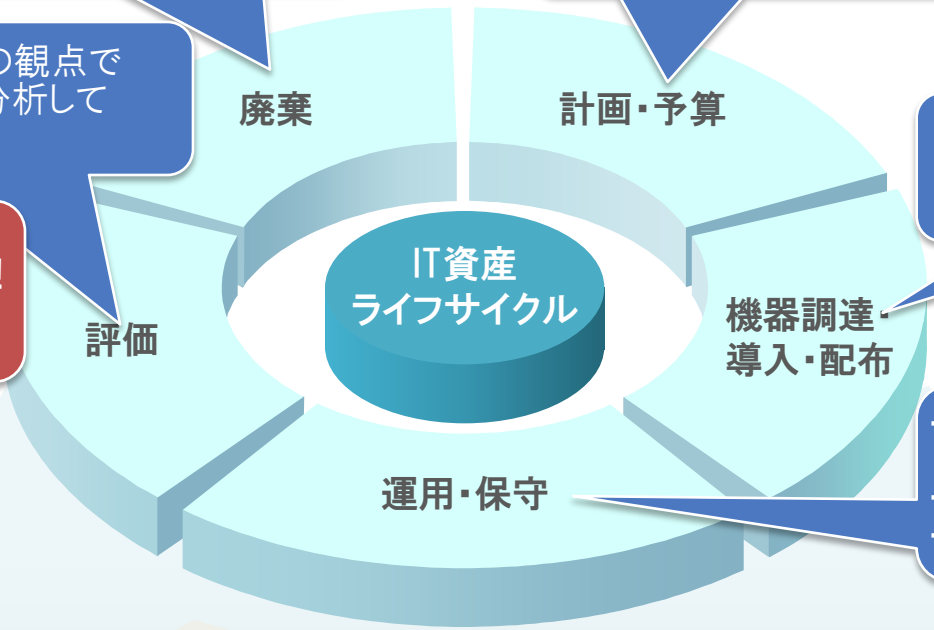
・不要な機器、ソフトウェアの廃棄

・現状把握
・IT資産の中長期計画の策定
・予算の検討

・コストやコンプライアンスの観点でIT資産の推移と状況を分析して評価

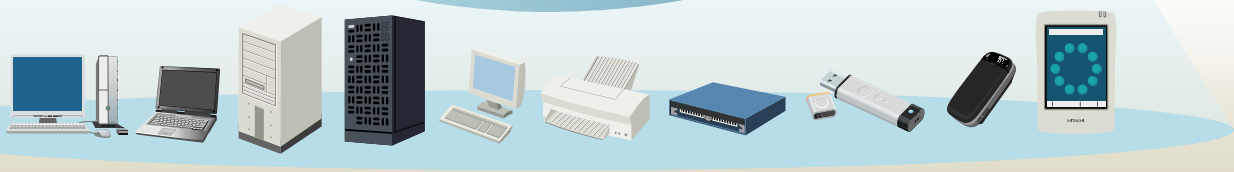
一つの製品で、全IT資産のライフサイクル管理ができる！

運用もよりシンプルに！



・機器の調達や導入
・ソフトウェアのインストール

・分散するIT資産をさまざまな視点で管理
・セキュリティリスクへの対応
・ヘルプデスク対応



uVALUE

1-3. JP1/IT Desktop Managementの機能

HITACHI
Inspire the Next

操作性と機能美の追求によって生まれた

一貫したユーザインターフェース

×

歴史あるJP1シリーズで培った

実力派の機能ラインナップ

IT資産管理	セキュリティ管理	リモートコントロール
インベントリ管理	自動対策	配布管理
ライセンス管理	USBデバイス抑止	エンタープライズ対応
棚卸支援	操作ログ	システム構築効率化
コスト把握	更新プログラム管理	
	禁止操作抑止	
	ネットワークモニタ	

uVALUE

HITACHI
Inspire the Next

2
IT資産の現状把握

1. 現状の把握
2. 組織内の全体像の把握
3. セキュリティ状況の見える化
4. 資産状況の確認
5. 提供レポート一覧

uVALUE

HITACHI
Inspire the Next

ホーム画面を見るだけでIT資産やセキュリティの概況を把握

ホーム画面では、ネットワークに接続された機器から収集した情報をもとに、前日からの変化や重要なお知らせがまとめて確認できます。この1画面を見るだけで、資産やセキュリティの概況がすぐにわかります。また、各パネルにあるリンクをクリックすれば、詳細な情報が表示され、IT機器のセキュリティを確保するためのさまざまな対策を実施できます。

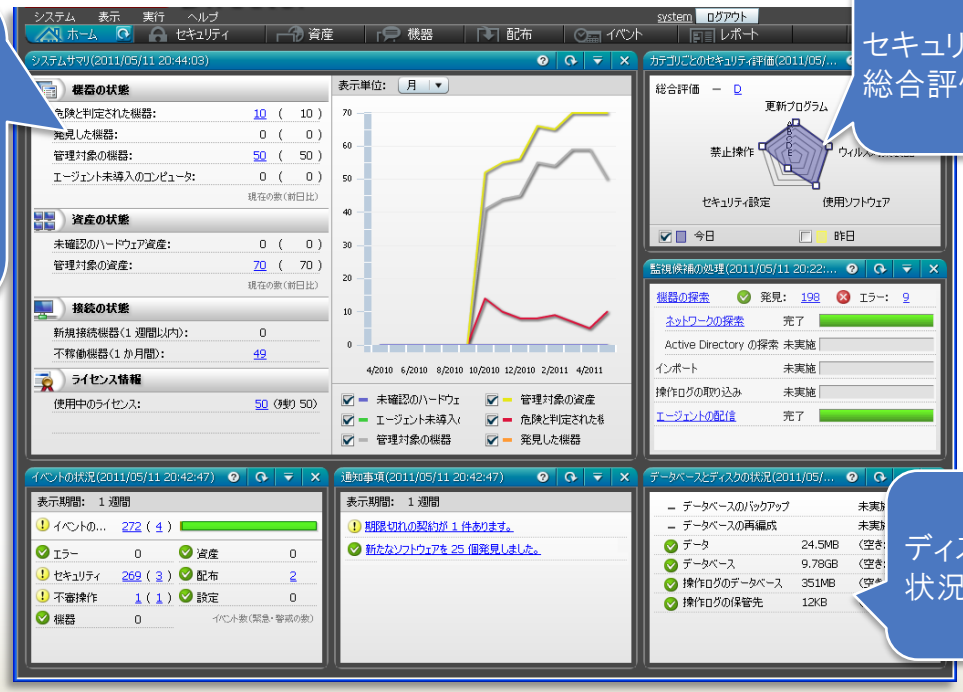
システムの状況のサマリを表示

こんなことも一目瞭然。

- ☑ 危険なPCはないか？
- ☑ 新たに接続されたPCや機器はないか？
- ☑ 長期間、稼働が確認できない機器はないか？
- ☑ 全体の状況や推移はどうか？

ホーム画面中の小さな画面「パネル」は、
表示内容とレイアウトを変更できます。
日々の運用でチェックしたいパネルに
置き替えて、自分専用の画面を構成できます。

「ホーム – レイアウト設定」ウィンドウ



ホーム画面

2-1. 現状の把握(追加できるパネルの詳細)

HITACHI
Inspire the Next

■追加できるパネルの詳細(1/3)

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。
	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、対策の起点にできます。
	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。
	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	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。

2-1. 現状の把握(追加できるパネルの詳細)

HITACHI
Inspire the Next

■追加できるパネルの詳細(2/3)

カテゴリ	パネル名	説明
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確認できます。
	危険レベルごとの機器台数	管理対象の機器の総数と危険レベルごとの台数、および全体の内訳を確認できます。
	不審操作の状況	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。
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。
	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。
	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。
	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。

2-1. 現状の把握(追加できるパネルの詳細)

HITACHI
Inspire the Next

■追加できるパネルの詳細(3/3)

カテゴリ	パネル名	説明
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。
	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。
	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。
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。
	エラータスクの状況	エラーが発生したタスクを確認できます。

HITACHI
Inspire the Next

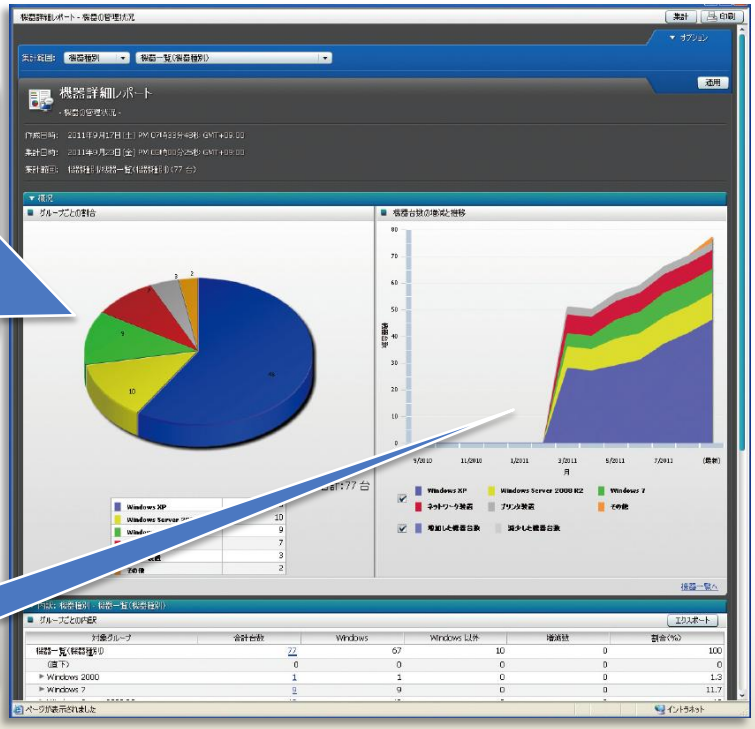
膨大な数のIT機器もレポート1枚で全体像を把握

機器詳細レポート「機器の管理状況」では、管理対象の機器が各部署や設置場所に何台あるかや、機器の台数が月にどのくらい増減しているのかをグラフで確認できます。台数の増減の推移に合わせて新規機器の導入を検討したり、古くなった機器の入れ替えを検討したりするのに役立ちます。

管理対象の機器の台数を種別ごとに表示

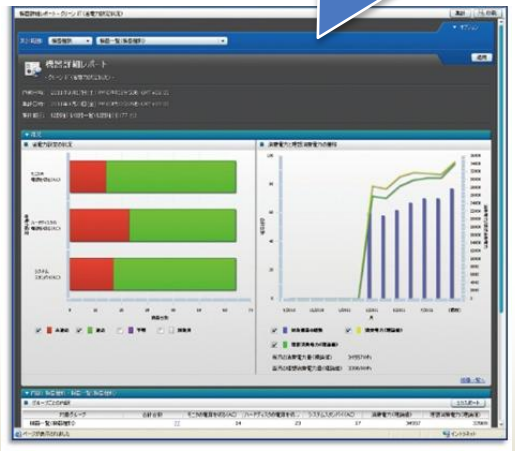
Windows XP	46
Windows Server 2008 R2	10
Windows 7	9
ネットワーク装置	7
プリンタ装置	3
その他	2

管理対象の機器の台数の推移を表示



機器詳細レポート「機器の管理状況」

さらに…
コンピュータの省電力設定の状況や、消費電力（理論値）と理想消費電力（理論値）の推移も表示可能



機器詳細レポート「グリーンIT（省電力設定状況）」

2-3. セキュリティ状況の見える化

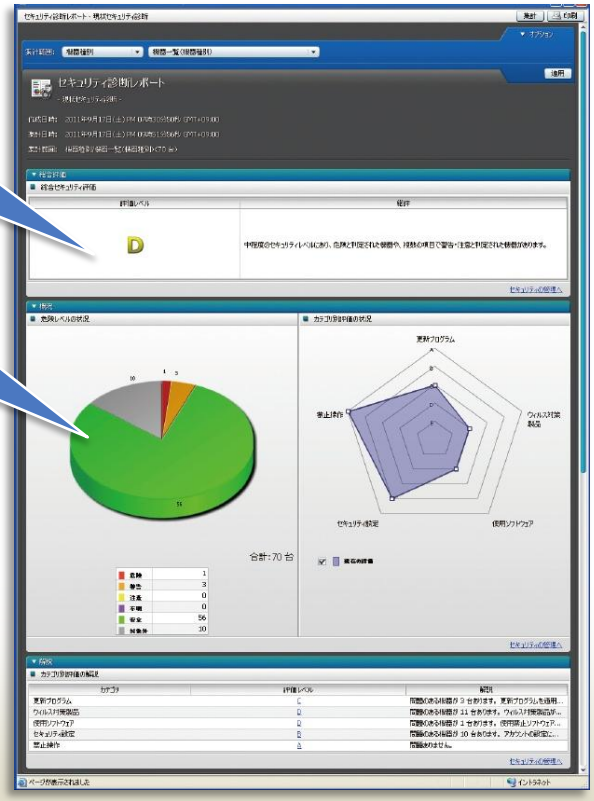
HITACHI
Inspire the Next

セキュリティの診断結果とその詳細でシステムの弱点を把握

セキュリティ診断レポートでは、セキュリティ状況を分析し診断した結果の、総合評価やカテゴリごとの評価を確認できます。これを見れば、どこが弱くて、どのような対策を実施すればよいかが簡単に把握できます。また、問題のあるカテゴリについて、さらに詳細なセキュリティ状況を確認することもできます。

セキュリティ状況の総合評価をA～Eの5段階で表示

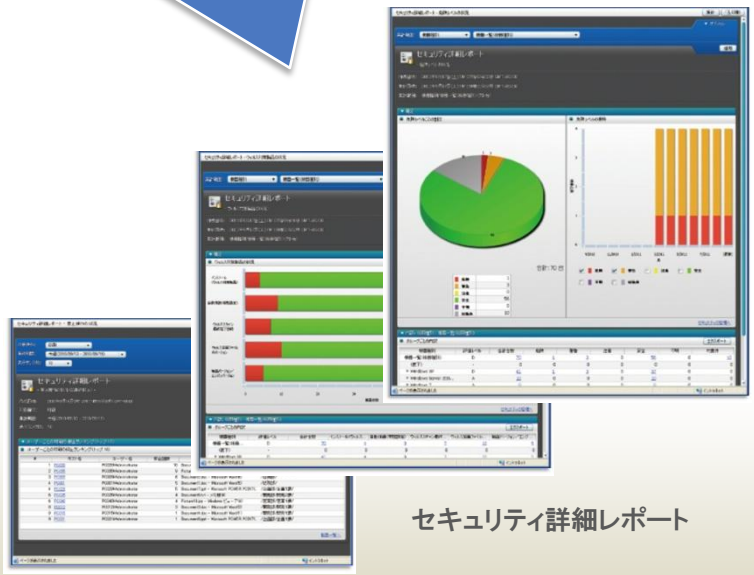
危険レベルごとの機器の台数をグラフで表示



セキュリティ診断レポート
「現状セキュリティ診断」

さらに…

ウィルス対策状況やWindows更新プログラムの適用状況、禁止操作の発生状況など、さまざまな観点でセキュリティ状況の詳細なレポートを表示

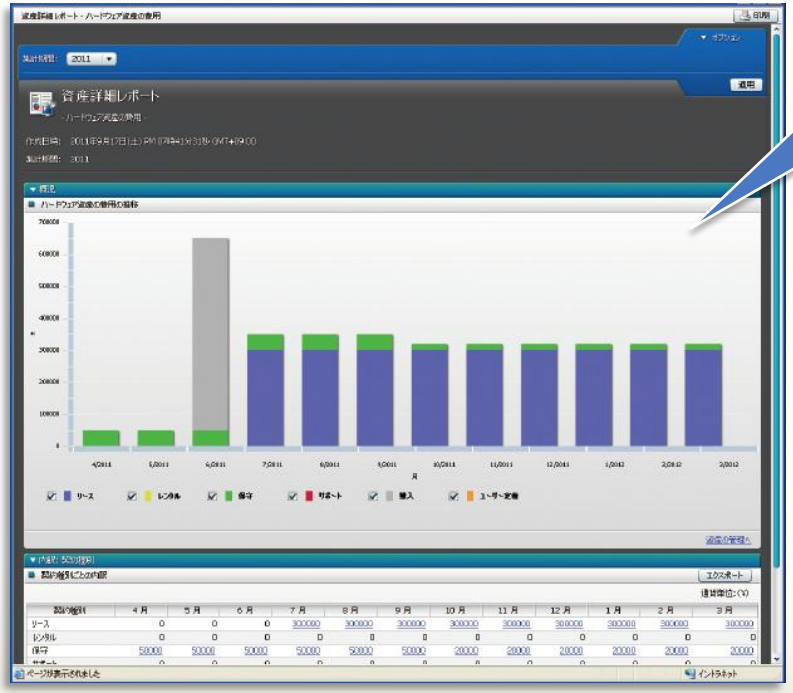


セキュリティ詳細レポート

HITACHI
Inspire the Next

資産にかかる費用やライセンスの管理状況を把握

資産詳細レポートでは、JP1/IT Desktop Management に登録されているハードウェア資産情報やライセンス情報にもとづいた、資産の管理状況の詳細を確認できます。
定期的に確認すれば、資産購入時の予算の見積もりやソフトウェアライセンスの管理に役立ちます。



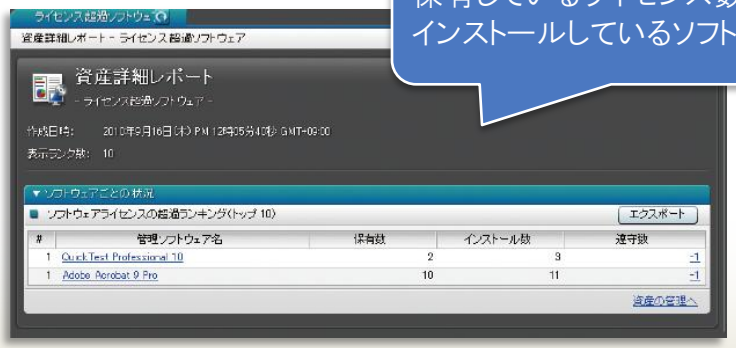
ハードウェア資産にかかる費用の推移を表示

こんな状況が確認できます。

- ☑ ハードウェア資産の費用は月ごとにどれくらいかかるか
- ☑ 契約種別ごとの費用がどのように推移しているか

資産詳細レポート「ハードウェア資産の費用」

保有しているライセンス数を超過して
インストールしているソフトウェアを表示



資産詳細レポート「ライセンス超過ソフトウェア」

uVALUE

2-5. 提供レポート一覧

HITACHI
Inspire the Next

■提供するレポート（20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
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 ・セキュリティ設定の状況（Windows® 自動更新、パスワードなどの設定） ・ウィルス対策製品の状況 ・使用禁止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 インストールランキング（トップ10）） ・更新プログラムの適用状況（更新プログラムの未適用ランキング（トップ10）など） ・使用必須ソフトウェアのインストール状況（使用必須ソフトウェア 未インストールランキング（トップ10）など） ・禁止操作の状況（ユーザーごとのソフトウェアの起動抑止ランキング（トップ10）など） ・ユーザーの活動状況（USBデバイスの使用ランキング（トップ10）など）
機器管理詳細レポート	・機器の管理状況（PC台数の内訳、推移など） ・グリーンIT（省電力の設定状況）
資産管理詳細レポート	・ハードウェア資産（資産台数の増減と推移など） ・ハードウェア資産の費用（推移など） ・ソフトウェアライセンスの費用（推移など） ・ライセンス超過ソフトウェア（超過ランキング） ・ライセンス余剰ソフトウェア（余剰ランキング）

HITACHI
Inspire the Next

3
システム構築とIT資産管理

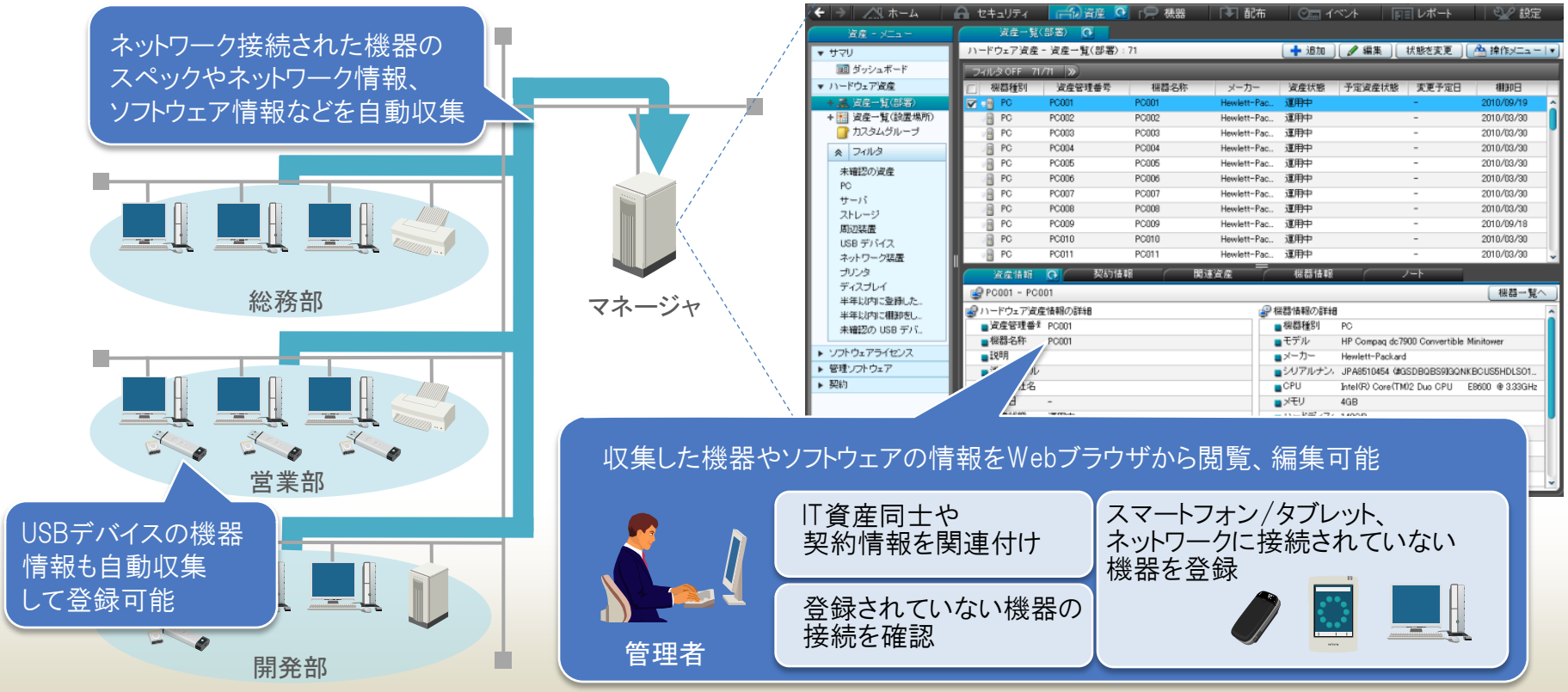
1. 多様化するIT資産の一元管理
2. システム構築の効率化
3. ソフトウェアライセンスの管理
4. 棚卸の効率化

uVALUE

HITACHI
Inspire the Next

IT資産の管理台帳は、収集した情報で自動生成、自動更新

組織内のネットワークを探索し、ハードウェアやソフトウェアの情報を自動収集します。
スマートフォンやネットワークに接続されていない機器を追加して、IT資産として一元管理できます。
さらに、契約情報（契約種別や期限など）を登録し、IT資産情報と関連付けて管理できます。

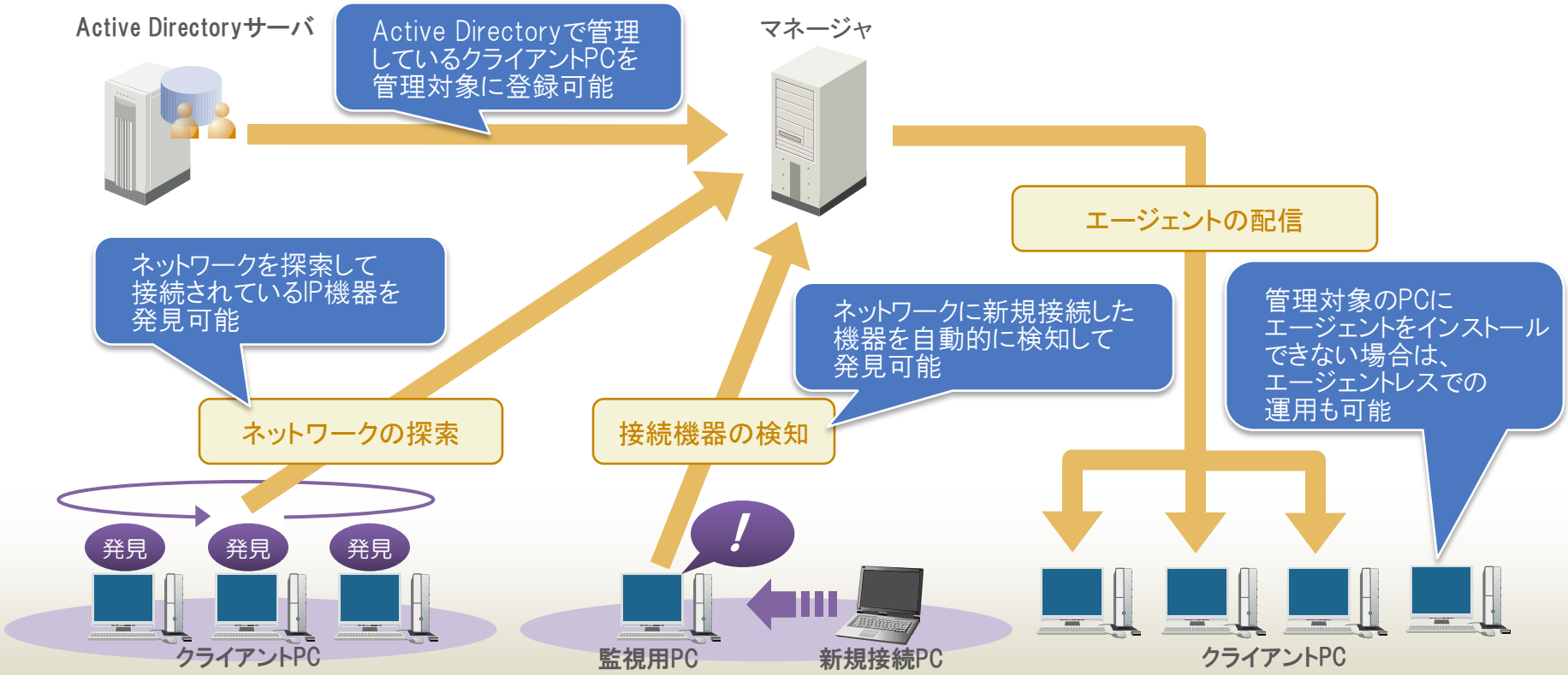


uVALUE

HITACHI
Inspire the Next

インストールや登録の手間を掛けずにシステム構築

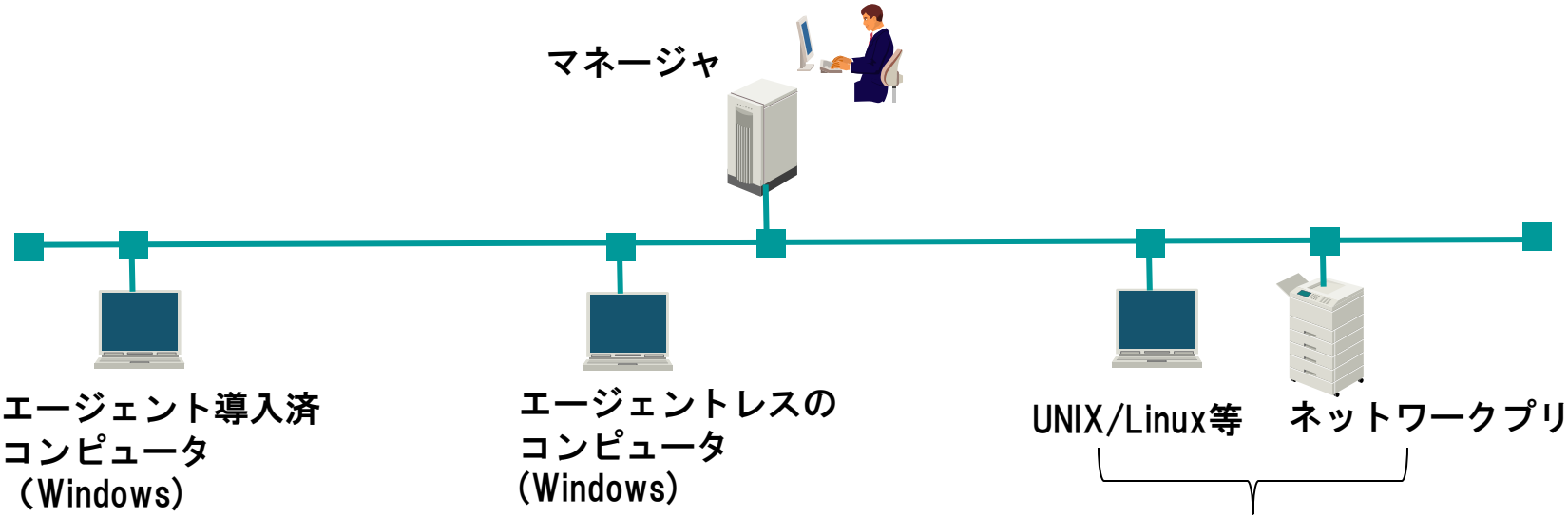
ネットワークを探索して、機器を発見したり、ネットワーク接続した機器を自動検知したりして管理対象にすることもできます。また、 Active Directoryでクライアント PCを管理している場合、Active Directoryで管理しているPCをそのまま管理対象にできます。さらに、PCにエージェントを配信して導入できるため、効率良くシステムを構築できます。



uVALUE

3-2.（1）機器から情報を収集する

●収集できる情報は、エージェントの有無、OS等で差があります。
●機器の情報は、定期的に取得します （取得間隔の指定可）



（エージェント経由で取得）
・システム情報
・ハードウェア情報
・ソフトウェア情報
・ウイルス対策製品情報
・操作ログ
・JP1/ITDMのイベント
・エンドユーザの入力する情報

（管理共有が有効の場合）
・システム情報
・ハードウェア情報（一部を除く）
・ソフトウェア情報
（プログラムの追加/削除のみ）

（SNMPで情報を取得）
・システム情報（一部のみ）
・ハードウェア情報（一部のみ）
・プリンタ情報（プリンタのみ）

3-2. (2)Windowsからの情報収集

HITACHI
Inspire the Next

収集できる情報の例(Windowsの場合 -1/2)

カテゴリ		説明
システム情報	機器種別	機器の種別 (例)PC、サーバ
	デバイス状態	機器の状態 (例)起動中、停止中
	コンピュータ情報	コンピュータの基本的な情報 (例)モデル、製造元
	ユーザー情報	コンピュータのログオンしたユーザの情報 (例)ユーザの説明
	OS情報	コンピュータのOSの情報 (例)所有者名(会社名)
	ネットワーク情報	コンピュータのネットワーク設定の情報 (例)MACアドレス、IPアドレス
ハードウェア情報		ハードウェアの情報 (例)プロセッサ名、メモリ等

3-2. (2)Windowsからの情報収集

HITACHI
Inspire the Next

収集できる情報の例(Windowsの場合 -2/2)

カテゴリ		説明
インストールソフトウェア情報 ※1		OSやソフトウェアのインストール状況 (例)ソフトウェア名、バージョン
セキュリティ情報	更新プログラム情報	OSのセキュリティ更新プログラムの適用状況 (例)適用済み更新プログラム
	ウイルス対策製品情報 ※2	ウイルス対策製品の設定状況 (例)ウイルス定義ファイルバージョン
	サービスのセキュリティ設定情報	セキュリティに付随するWindowsサービスの設定情報 (例)使用禁止サービス
	OSのセキュリティ設定情報	セキュリティに付随するOSの設定情報 (例)パスワードの更新経過日数
	秘文情報 ※2	秘文の情報です。(例)暗号化状態
操作ログ※2		管理対象のコンピュータで利用者の操作を記録します。 (例)ファイルのコピー

※1 「プログラムの追加と削除」の情報です。ファイルをキーにした情報は、エージェントがインストールされている場合に取得できます。
※2 エージェントがインストールされている場合に取得できます。

3-2. (3)Windows以外のPCから情報を収集する

HITACHI
Inspire the Next

収集できる情報の例（UNIX/Linuxのコンピュータ） ※1

カテゴリ		説明
システム情報	機器種別	機器の種別 （例）PC、サーバ
	コンピュータ情報	コンピュータ名
	OS情報	コンピュータのOSの情報
	ネットワーク情報	コンピュータのネットワーク設定の情報 （例）MACアドレス、IPアドレス
ハードウェア情報		下記ハードウェアの情報。 プロセッサ名、ネットワークアダプタ、メモリ容量、ハードディスクモデル、ハードディスク容量、キーボード、マウス

※1　SNMP経由で情報を取得しますので、SNMP応答をしない機器からは情報を取得できません。
（ARP応答により、存在の把握は可能です）。

3-2. (4)PC以外の機器から情報を収集する

HITACHI
Inspire the Next

収集できる情報の例（IPアドレスを持つ機器から収集できる情報） ※1

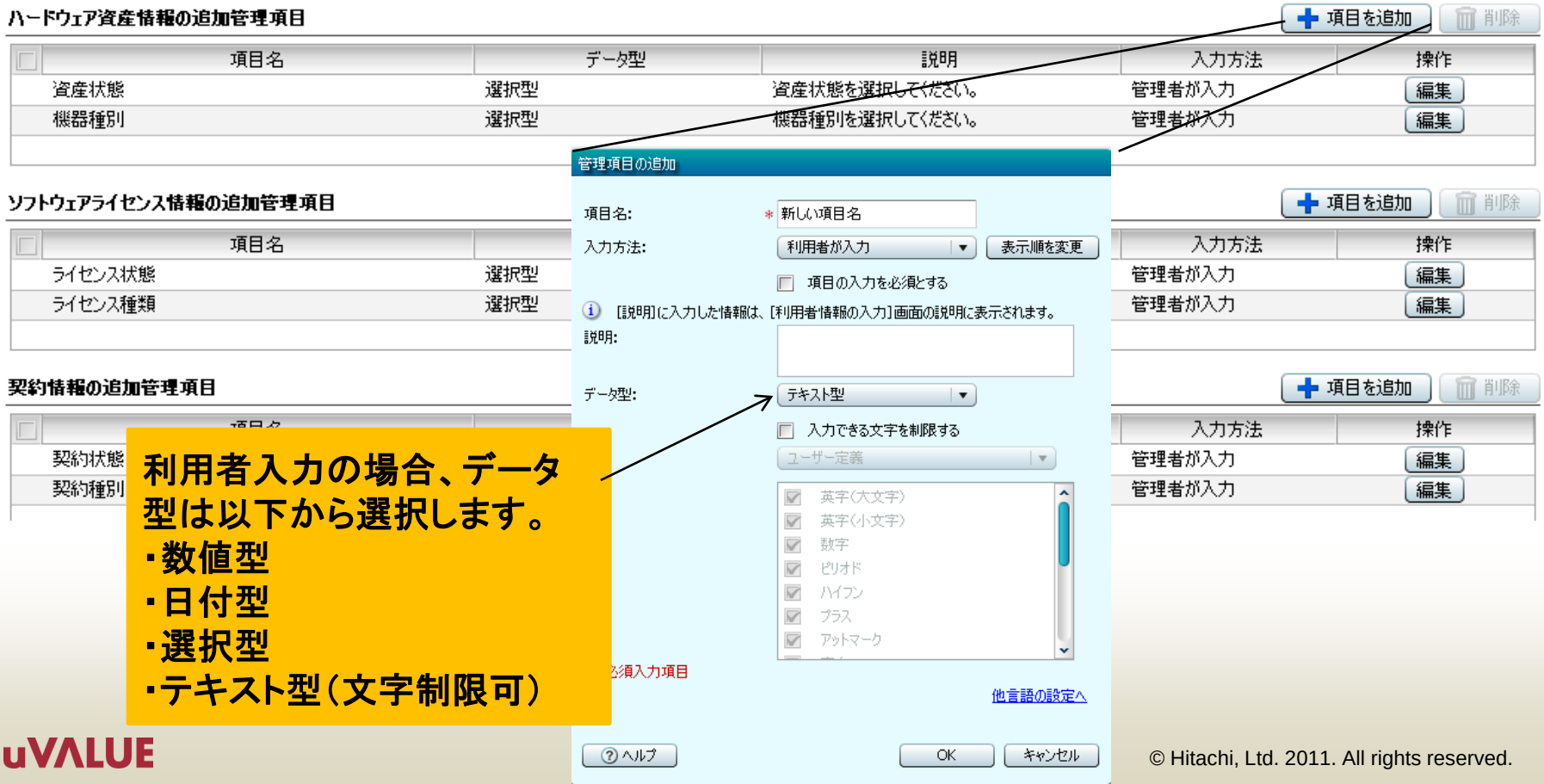
カテゴリ		説明
システム情報	機器種別	機器の種別
	ネットワーク情報	コンピュータのネットワーク設定の情報 （例）MACアドレス
	プリンタ情報※2	プリンタの情報 （例）印刷方式

※1　SNMP経由で情報を取得しますので、SNMP応答をしない機器からは情報を取得できません。
（ARP応答により、存在の把握は可能です）

※2　プリンタからのみ取得可能です。

3-2. （5）管理項目の追加

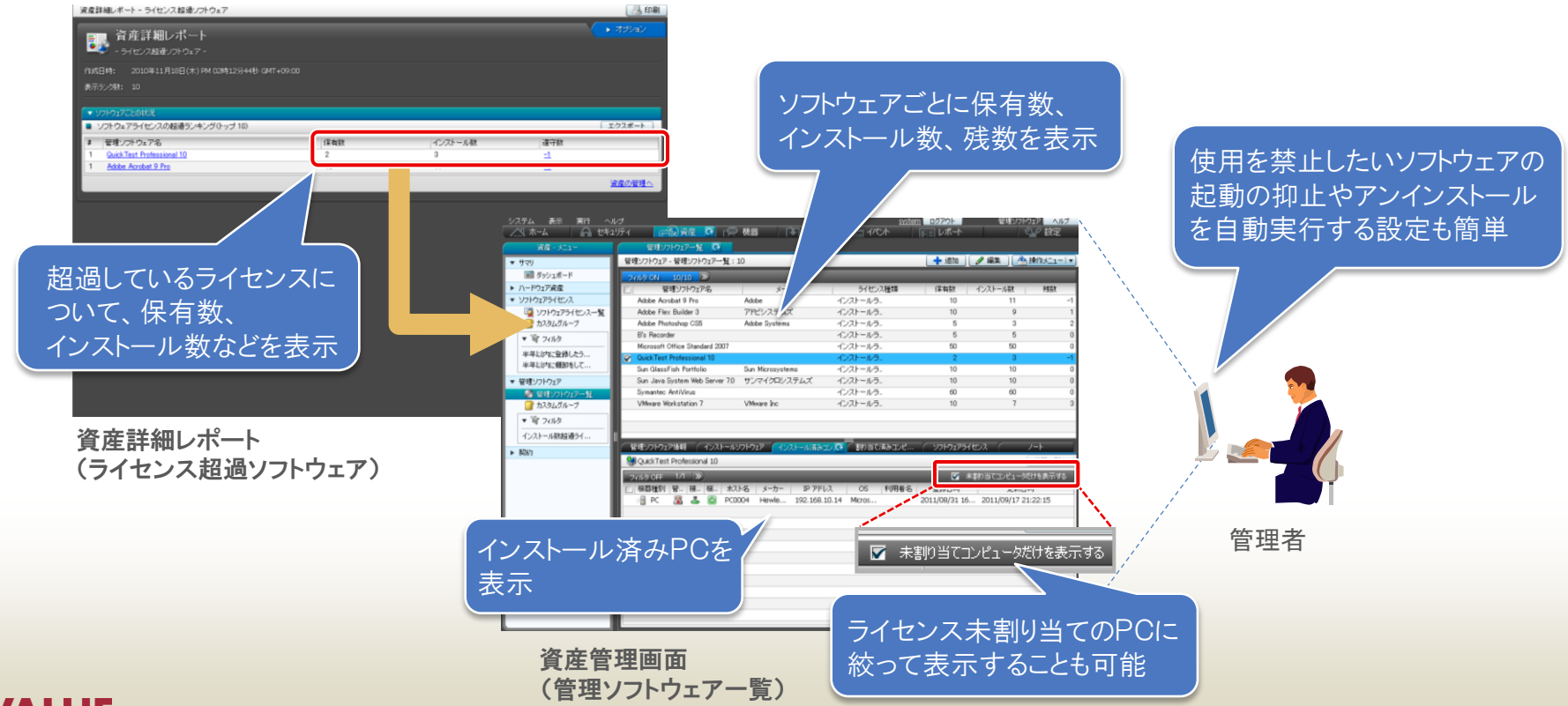
●ハードウェア資産、ソフトウェアライセンス、契約について、任意の項目を追加できます。
●追加したハードウェア資産項目については、管理者の入力・利用者の入力・Active Directory・レジストリのいずれかから情報を取得できます。
●ソフトウェアライセンス、契約の追加項目は、管理者の入力固定です。



HITACHI
Inspire the Next

ライセンス違反を確認、違反したコンピュータも簡単に対策

PCにインストールされているソフトウェアの情報を自動収集し、超過ライセンスや余剰ライセンスについての集計結果を確認できます。ソフトウェアごとに、ライセンス保有数、割り当て数、残数を表示できるため、ライセンス違反をしていないことの証明に役立ちます。使用を禁止したいソフトウェアがインストールされていた場合、一覧画面から1クリックで簡単に禁止ソフトウェアに設定できます。



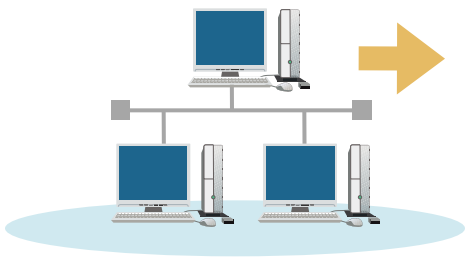
uVALUE

3-4. 棚卸の効率化

HITACHI
Inspire the Next

現場に行かなくても、ネットワーク経由で自動的に棚卸

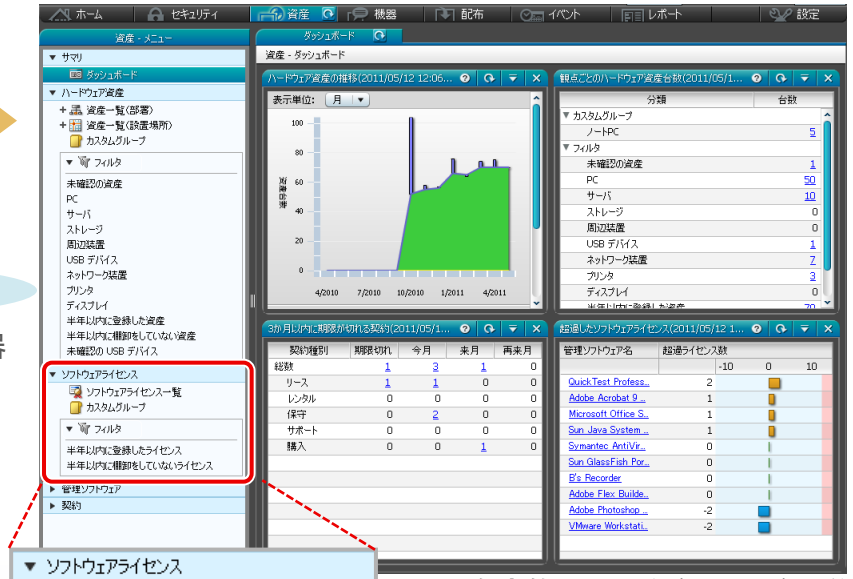
ネットワークを介して機器情報を自動で収集し、機器の棚卸情報も自動的に更新できます。新規追加になった機器を登録したり、既存機器の管理元を変更したりするだけで、IT資産情報はいつも最新の状態に保てます。ネットワークに接続していない資産についても、これらを出力したリストを現物確認に利用することで、効率的な棚卸ができます。



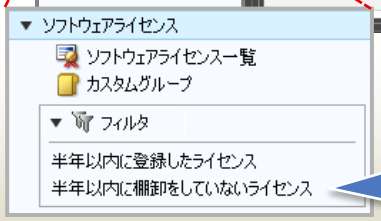
ネットワークに接続している機器

定期的にIPアドレスなどの機器情報を収集

存在が確認できたら棚卸情報も更新



資産管理画面(ダッシュボード)



棚卸が必要なソフトウェアライセンスの抽出も簡単

ネットワークに
接続していない機器は・・・

IT資産情報リストを出力し、手間なく現品確認へ

uVALUE

HITACHI
Inspire the Next

4

セキュリティ対策

1. セキュリティ対策の徹底
2. セキュリティポリシー
3. USBデバイスの使用制限
4. 禁止操作の抑止
5. 情報漏えいリスクの検知
6. 操作ログの参照
7. Windows更新プログラムの適用
8. アクション項目（ネットワークからの遮断）

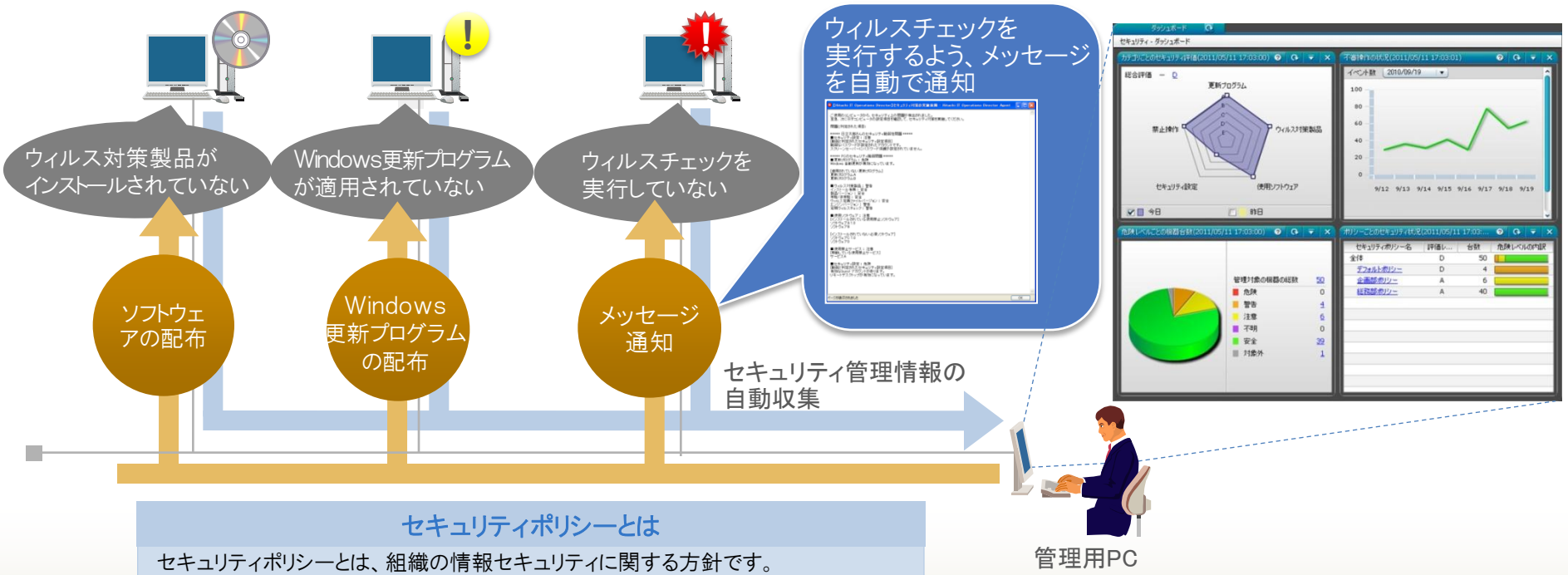
uVALUE

4-1. セキュリティ対策の徹底

HITACHI
Inspire the Next

セキュリティの問題点を把握して手遅れになる前に問題を解決

管理しているPCから情報を収集。「セキュリティ脆弱に関するリスク」「禁止操作に関するリスク」「情報漏えいに関するリスク」など、社内のセキュリティリスクに対する状況を把握し、適切に対処できます。



セキュリティポリシーとは

セキュリティポリシーとは、組織の情報セキュリティに関する方針です。
管理対象のPCにセキュリティポリシーを適用することで、セキュリティ対策を実現します。セキュリティポリシーには必要な項目があらかじめ設定されているので、すぐに管理が始められます。
部署単位やPCごとにセキュリティポリシーを変えることもできます。

4-2. セキュリティポリシー （追加方法）

HITACHI
Inspire the Next

- JP1/ITDMには、「デフォルトポリシー」「推奨セキュリティポリシー」があらかじめ準備されています。
- 任意のポリシーの作成を行いたい場合には、上記をコピーして編集するか、または新規作成してください。

4-2. セキュリティポリシー （判定と自動対策）

HITACHI
Inspire the Next

■セキュリティポリシー（判定および自動対策）（1/2）

項目		検知できる内容	自動対策内容
更新プログラム		**・Windows自動更新が有効か** **・すべての更新プログラムが適用されているか** ・指定した更新プログラム、OSサービスパック、IEサービスパックが適用されているか	**・自動更新を有効にする** **・更新プログラムを適用する**
ウイルス対策製品	製品の有無	ウイルス対策製品がインストールされているか	－
	エンジンバージョン	エンジンバージョンが最新か （猶予期間あり）	－
	ウイルス定義ファイルのバージョン	ウイルス定義ファイルのバージョンが最新か （猶予期間あり）	－
	自動保護（常駐設定）	自動保護（常駐設定）が有効か	－
	ウイルススキャン最終完了日時	最終完了日時が猶予期間以内か	－
使用ソフトウェア	**必須ソフトウェア**	**必須ソフトウェア（ソフトウェア名/ファイル名指定可）がインストールされているか**	**指定パッケージをインストール**
	禁止ソフトウェア	**禁止ソフトウェア（ソフトウェア名/ファイル名指定可）がインストールされていないか**	**起動を抑止する　または アンインストールを実行**
使用禁止サービス		**指定したサービスが稼働していないか**	**サービスを停止し無効化**

太字は自動対策可能な内容

4-2. セキュリティポリシー （判定と自動対策）

HITACHI
Inspire the Next

■セキュリティポリシー（判定および自動対策）（2/2）

項目		検知できる内容	自動対策内容
OSのセキュリティポリシー	Guestアカウント	Guestアカウントが無効、またはないか	Guestアカウント無効
	パスワード安全性	OSに脆弱なパスワードが設定されているアカウントがないか	–
	無期限パスワード	OSに無期限パスワードが設定されているアカウントがないか	無期限パスワード設定の解除
	パスワード更新からの経過日数	パスワード更新からの日数が、指定した日数を超えるアカウントがないか	–
	自動ログオン	OSに自動ログオンの設定がされていないか	自動ログオンの設定解除
	BIOSパスワード	BIOSパスワードが設定されているか	–
	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にパスワード保護が設定されているか	パスワード保護を設定
	スクリーンセーバー起動待ち時間	スクリーンセーバー起動までの待ち時間が、指定した時間以内か	指定した時間に設定
	共有フォルダ	共有フォルダがないか	共有フォルダ設定を解除
	匿名接続	匿名接続が制限されているか	匿名接続を制限
	Windowsファイアウォール	Windowsファイアウォールが有効か	Windowsファイアウォール有効
	DCOM	DCOMが無効か	DCOM無効
	リモートデスクトップ	リモートデスクトップが無効か	リモートデスクトップ無効

4-2. セキュリティポリシー（対応するウイルス対策製品）

HITACHI
Inspire the Next

Norton AntiVirus*1*2*3	2010	32bit	McAfee VirusScan Enterprise	8.5i	32bit	Forefront Client Security*2	1.5	32bit
		64bit			64bit			64bit
	2011	32bit		8.7i	32bit	Kaspersky Open Space Security*1*2*4	6.0	32bit
		64bit			64bit			64bit
Symantec AntiVirus Corporate Edition	10	32bit	ウイルスバスター	2010	32bit	ESET NOD32 Antivirus*1*2*3	4	32bit
		64bit			64bit			64bit
	10.1	32bit		2011 *2	32bit		4.2	32bit
		64bit			64bit			64bit
	10.2	32bit	Trend Micro ビジネスセキュリティ*2	6.0	32bit	Sophos Endpoint Security and Data Protection	9.0	32bit
		64bit			64bit		9.5	64bit
Symantec Client Security	3.0	32bit	ServerProtect for Windows NT/Netware	5.7	32bit	Sophos Security Suite small business soluteions 4/	-	32bit
		64bit			64bit	Sophos Computer Security small business solutions 4		
	3.1	32bit		5.8	32bit	Sophos Anti-Virus small business solutions 4		64bit
		64bit			64bit			
Symantec Endpoint Protection	11.0	32bit	ウイルスバスターCorp.エディション（アドバンス、サーバ版、サーバ版 アドバンスを含む）	8.0*2		F-Secure Client Security*1*2*3	8.0 9.0	32bit
		64bit		10.0/10.5*2				64bit
McAfee Total Protection Service*2*3	5.0			10.5 Patch1 以降				

※1 ウィルス検出エンジンのバージョンは収集できません。
※2 最終スキャン完了日時は収集できません。
※3 常駐/非常駐の状態は収集できません。
※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。

4-3. USBデバイスの使用制限

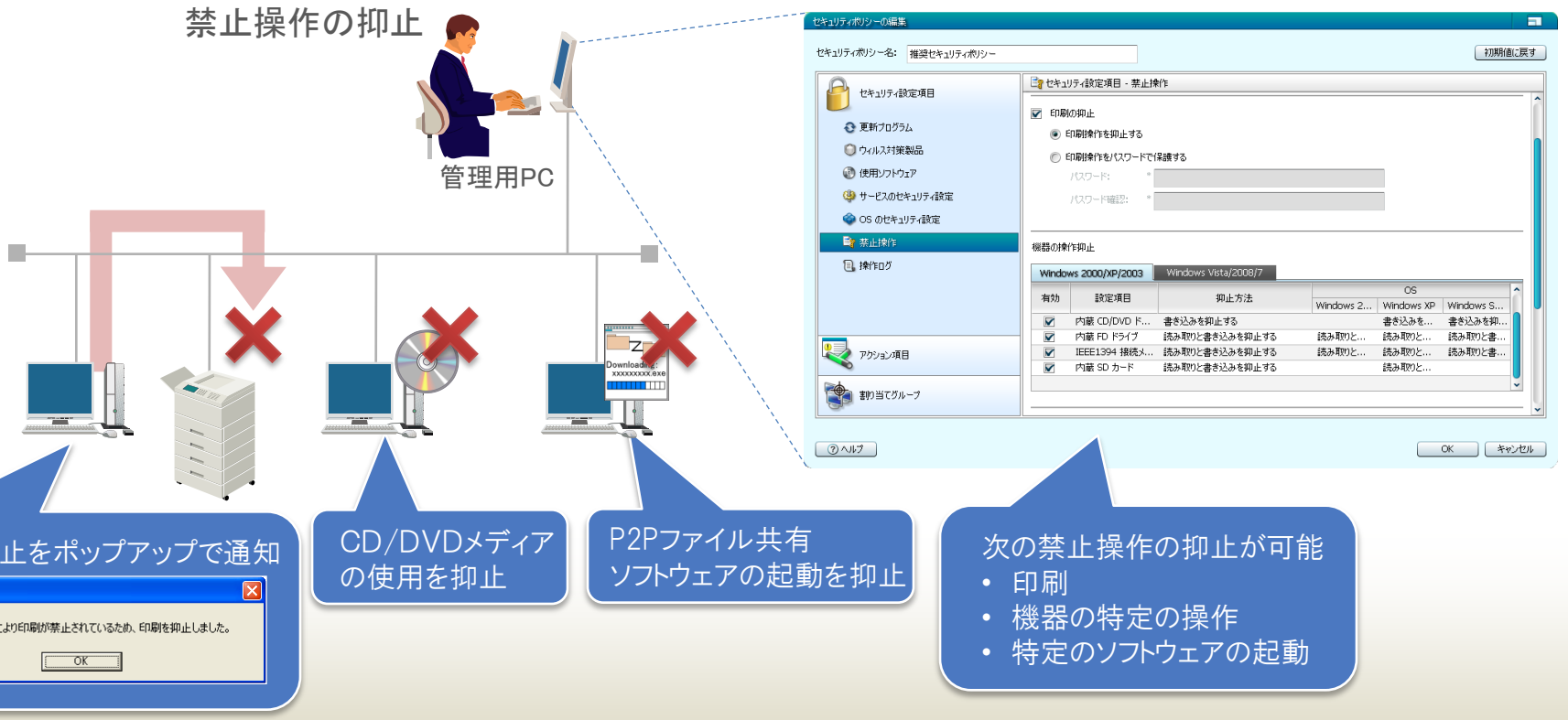
使用できるUSBデバイスを限定して情報漏えいを未然に防止

個人所有などのUSBデバイスは、PCに接続しても使用できないので、USBデバイスを介した情報漏えいの防止に役立ちます。
さらに、使用を許可したUSBデバイスに保存されているファイル名も確認できます。

HITACHI
Inspire the Next

禁止操作を抑止して、情報漏えいを未然に防止

情報漏えい対策として、印刷を抑止したり、CD/DVDドライブの書き込みを抑止したりできます。
また、P2Pファイル共有ソフトウェアや、業務に関係ないゲームなどの起動を抑止することもできます。



4-4. 禁止操作の抑止 （禁止操作一覧）

HITACHI
Inspire the Next

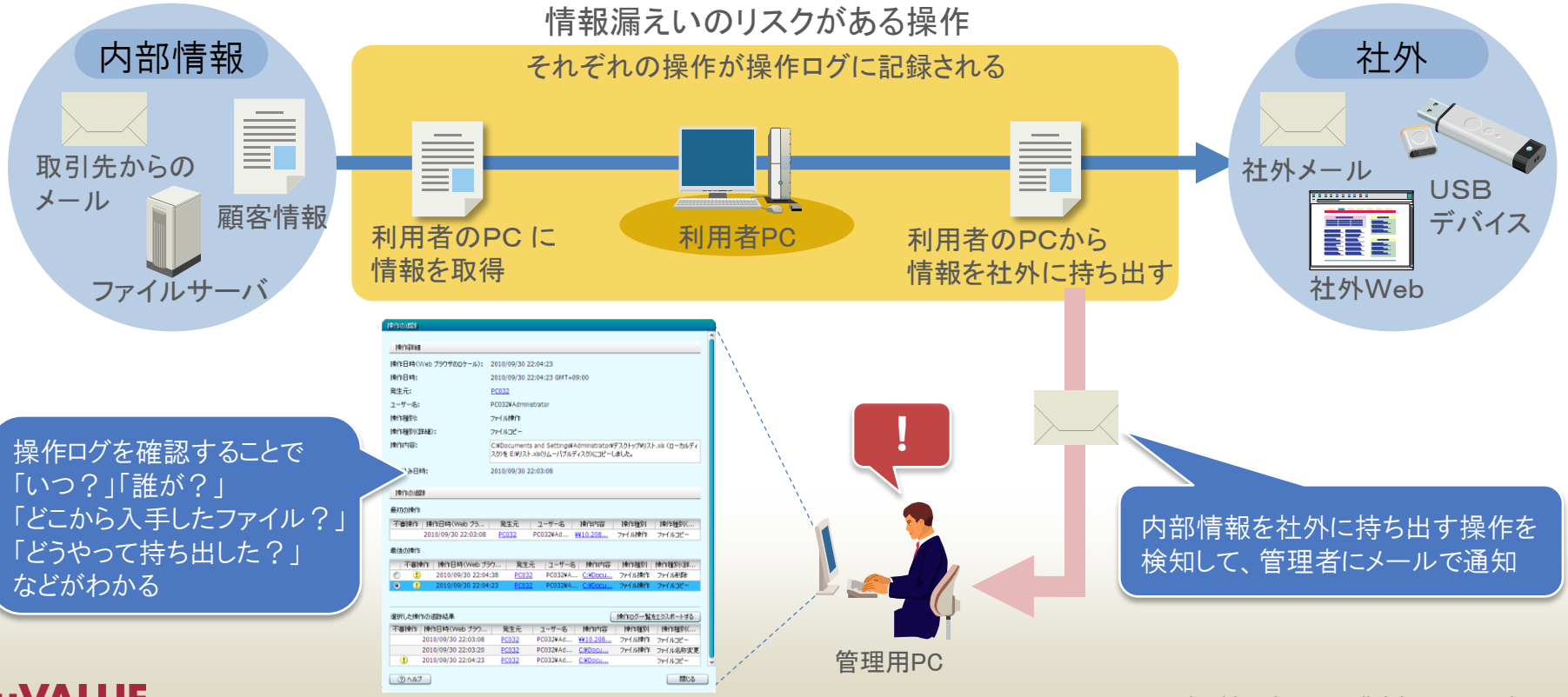
■セキュリティポリシー（禁止操作）

項目		禁止できる内容	備考
印刷操作		・印刷の抑止 ・印刷操作をパスワードで保護	
機器の操作抑止	USBデバイスの使用	・読み取りと書き込みの抑止 ・読み取りと書き込みを抑止 （登録済みのUSBデバイスを除外） ・書き込みだけを抑止	・「書き込みだけを抑止」はWindowsXPのみ可能。
	CDROM/DVDドライブの使用	書き込みを抑止	Windows2000/XP/2003は内蔵ドライブのみに限定
	FDドライブの使用	読み取りと書き込みを抑止	Windows2000/XP/2003は内蔵ドライブのみに限定
	IEEE1394接続メディア	読み取りと書き込みを抑止	Windows2000/XP/2003のみサポート
	内蔵SDカード	読み取りと書き込みを抑止	Windows2000/XP/2003のみサポート
	リムーバブルディスク	読み取りと書き込みを抑止	・WindowsVista/7/2008のみサポート ・USBデバイス抑止と併用不可
ソフトウェアの起動抑止		・指定したソフトウェアの起動抑止 ・指定したソフトウェアの起動抑止 （指定した利用者・グループは除外） （指定した時間帯は除外）	ソフトウェアには実行形式ファイル名を指定

HITACHI
Inspire the Next

情報持ち出しの形跡を自動通知
原因は操作ログから追跡・調査

情報漏えいのリスクがある「社外Webへのアップロード」「メール送信」「USBデバイスへのコピー」といった、内部情報を社外に持ち出す操作を検知して、管理者に通知できます。また、これらの操作を記録、追跡できます。



uVALUE

4-6. 操作ログの参照

●操作ログを一覧することができます。
●大量の操作ログを各種フィルタで絞り込むことにより、効率的に参照できます。

各種フィルタによる絞り込み
（操作日時、発生元、ユーザ名、操作対象ファイル名等）

あらかじめ設定した、
特定の操作（リスクのある
操作）を検知

スクロールボタンによる参照位置移動
（ページ単位、一日単位、一月単位で移動）

4-6. 取得可能な操作ログ

HITACHI
Inspire the Next

■セキュリティポリシー（操作ログ）

項目	取得できる内容	備考
取得可能な操作ログ	コンピュータの起動・停止・ログオン・ログオフ	コンピュータの起動/停止、利用者のログオン/ログオフ
	プログラム起動/停止	利用者のプロセス起動/停止
	ファイル操作/印刷抑止	ファイルコピー/移動/名称変更/作成/削除【注意】、ファイルアップロード/ダウンロード(※1)、ファイル送信/受信(※1)、添付ファイルつきメール送信/受信(※2)、添付ファイル保存(※2)、印刷(※3)
	フォルダ操作	フォルダコピー/移動/名称変更/作成/削除【注意】
	外部メディア接続／切断	利用者による外部メディア接続/切断
	Webアクセス	※1
	ウインドウ操作	アクティブウインドウの変更
	抑止ログ	プログラム起動抑止、印刷抑止、外部メディア接続抑止

【注意】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。

※1 操作ログを取得できるWebブラウザは、Internet Explorer 6/7/8、Firefox 3.5/3.6です。
※2 操作ログを取得できるメールソフトは、Microsoft Outlook Express 6 、Microsoft Outlook 2002/2003/2007/2010 Windows メール 6、Windows Live メール 2009です。
※3 操作ログを取得できるプリンタは、ローカルプリンタ、ネットワーク共有プリンタまたはコンピュータに接続されているプリンタ、仮想プリンタです。

uVALUE

4-6. 特定の操作として検知可能な動作

HITACHI
Inspire the Next

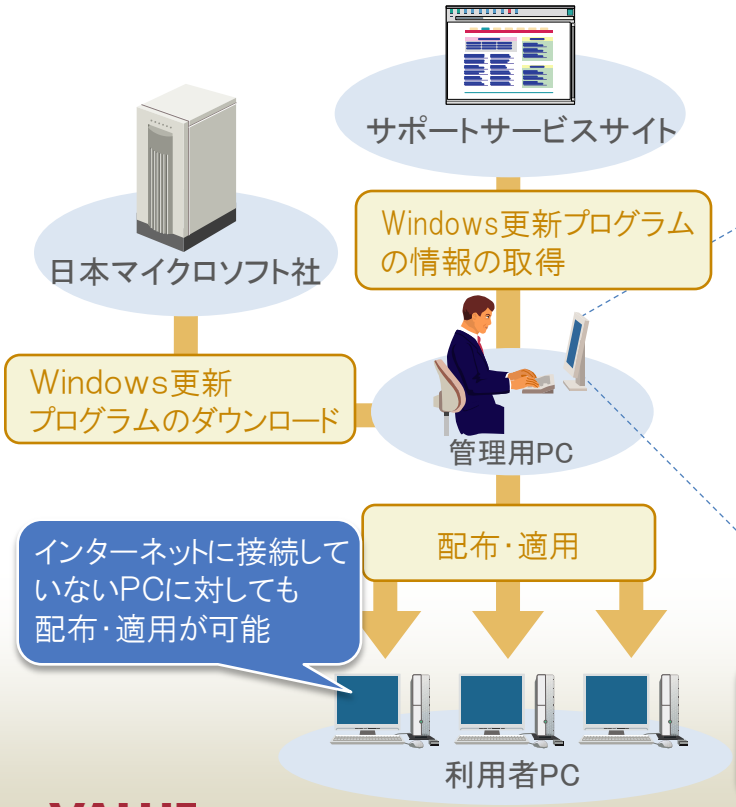
■セキュリティポリシー（「特定の操作」として検知可能な操作）

項目	詳細
添付メールつきファイルの送受信	添付ファイル付きメールの送受信を「特定の操作」と見なすかどうかの基準を、メールアドレス単位に設定できます。 （すべてのアドレス指定も可能です）
Web/FTPサーバの使用	Web/FTP サーバの使用を不審な操作と見なすかどうかの基準を、アドレス単位に設定できます。設定したアドレスからダウンロード（受信）したファイルは、監視中のファイルとして扱います。 「特定の操作」と見なす操作は、監視中のファイルまたは組織内で作成したファイルを、[監視する]と設定したアドレスにアップロード（送信）する操作です。
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	組織内で作成、コピー、移動したファイルは、監視中のファイルとして扱います。 「特定の操作」と見なす操作は、監視中のファイルまたは組織内で作成したファイルを、外部メディア（リムーバブルディスク）へ出力する操作です。
大量印刷	時間以内に印刷したページ数の合計が設定ページ数に達する印刷操作を、「特定の操作」と見なします。

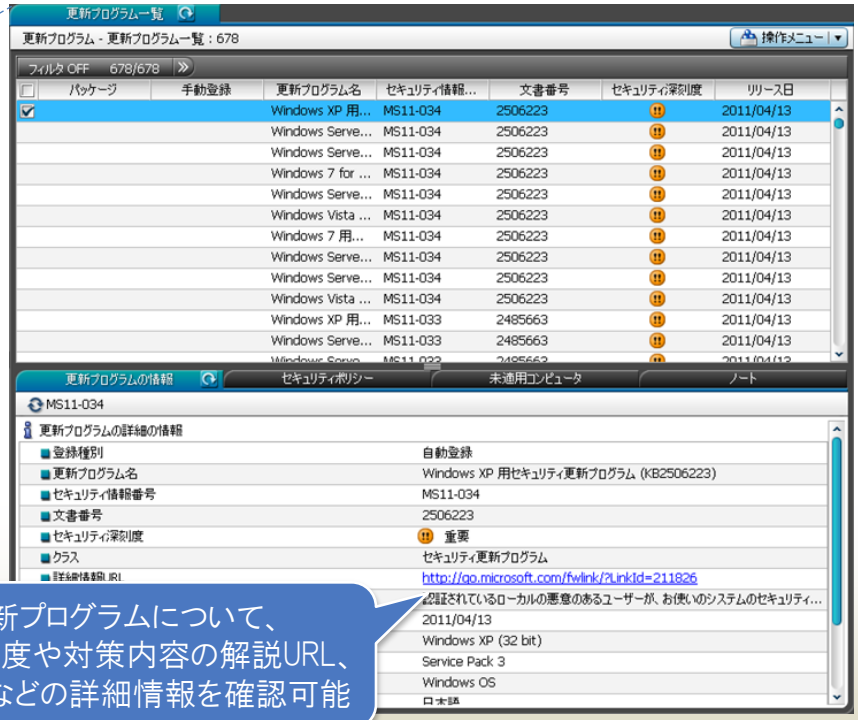
HITACHI
Inspire the Next

Windows更新プログラムをすべてのPCにもれなく適用

Windows自動更新の設定が無効になっているPCは、自動的に有効にして、最新のWindows更新プログラムを適用できます。
また、適用させたくないWindows更新プログラムがある場合は、特定のWindows更新プログラムだけを配布・適用することも可能です。



「更新プログラム一覧」ウィンドウ

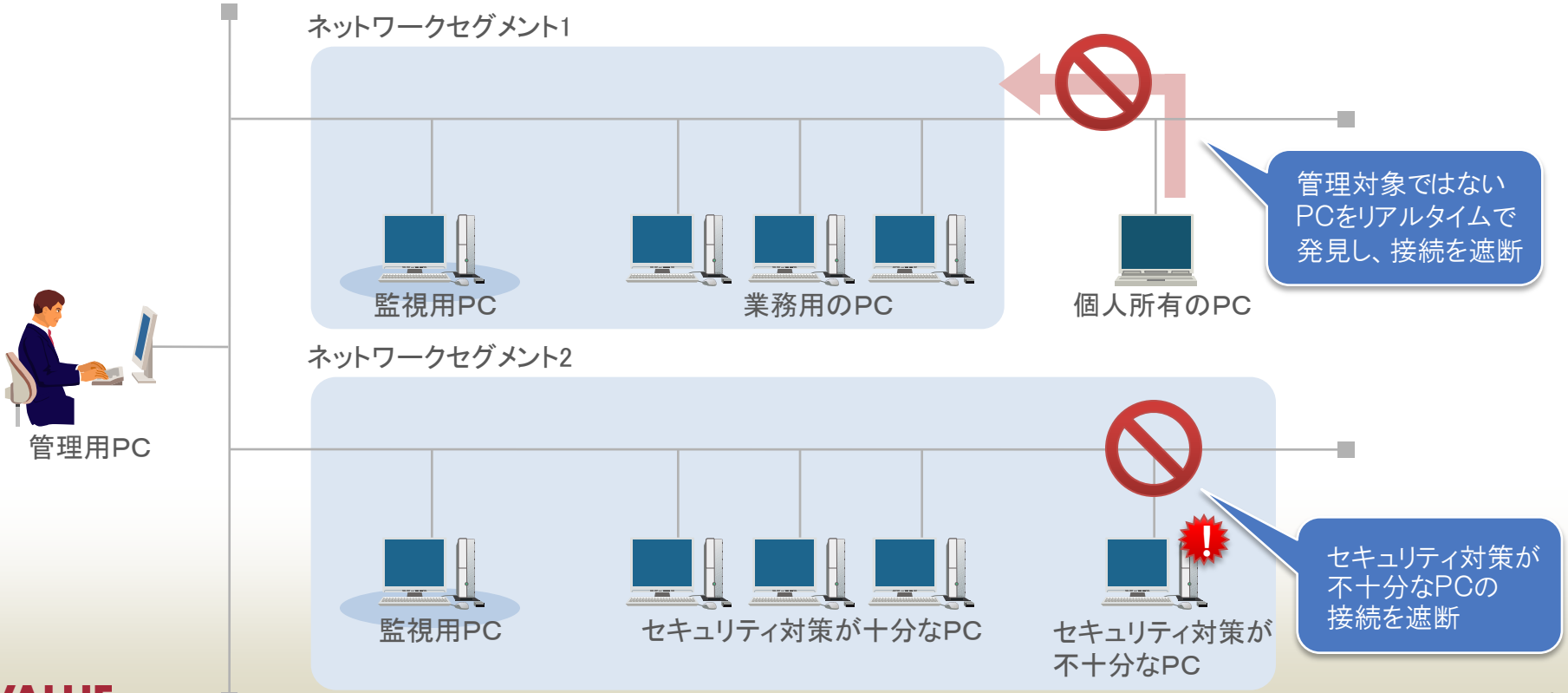


各Windows更新プログラムについて、セキュリティ深刻度や対策内容の解説URL、ダウンロードURLなどの詳細情報を確認可能

HITACHI
Inspire the Next

セキュリティリスクが高いPCは自動的にネットワークから遮断

管理対象ではないPCのネットワーク接続をすぐに検知して、自動的に遮断できます。
これにより、個人所有のPCなどが不用意に社内ネットワークに接続できなくなります。
また、管理対象PCのセキュリティ対策ができていることを確認してから、ネットワークへの接続を許可するような運用を自動化できます。



uVALUE

5

スマートデバイス管理

1. スマートデバイスの特徴と課題

2. JP1/ITDMのスマートデバイス管理

HITACHI
Inspire the Next

スマートデバイスの特徴と管理上の課題

メリット

デメリット

管理上の課題

小型軽量
持ち運び容易

社内外問わず
移動して使用可

現品棚卸
困難

台帳作成・維持
負荷の低減

機器紛失
リスク大

紛失時の
対応方法

安価でPC並の
性能・表現力

大量導入可能

関連契約・
発生費用
の把握

多用途
拡張性あり

用途の
限定困難

5-2. JP1/ITDMのスマートデバイス管理

HITACHI
Inspire the Next

スマートデバイスも、他のIT資産と同じコンソールで一元管理。

スマートデバイスをIT 資産台帳に
手入力で登録

関連契約等の情報を追加

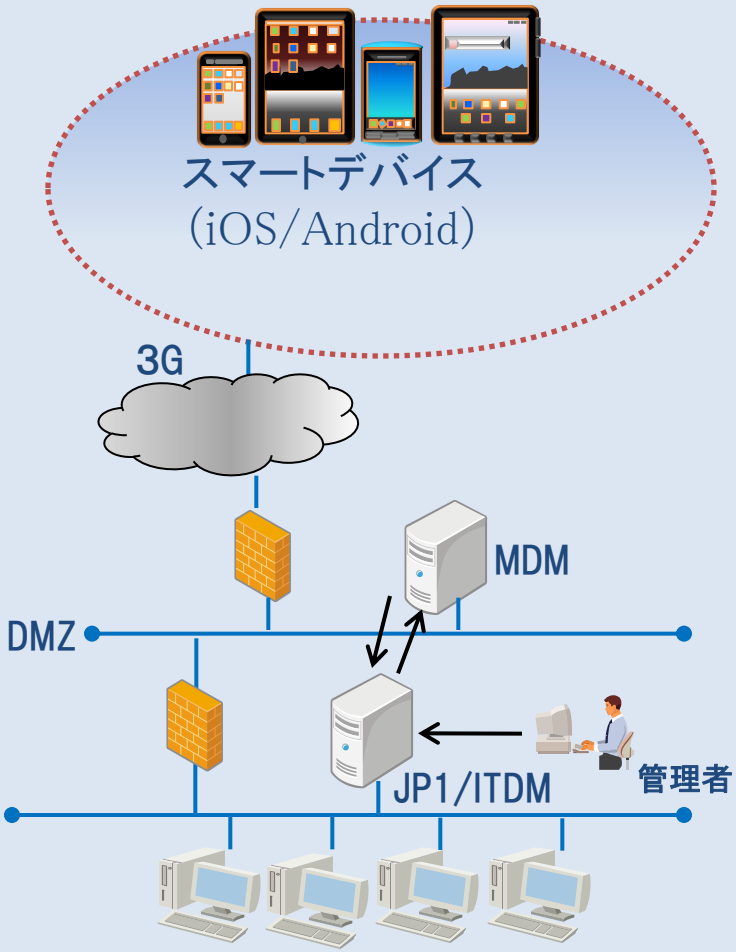
今後対応予定

・MDM（Mobile Device Management）
からスマートデバイスの情報取り込み
★他のIP機器同様、自動取り込み可。
管理負荷減少。

関連契約等の情報を追加

今後対応予定

・JP1/ITDMコンソールから
デバイスロック・ワイプ（消去）指示可能
★紛失対応時の利便性向上。



HITACHI
Inspire the Next

6
ヘルプデスクサポート

1. 機器のリモートメンテナンス

uVALUE

HITACHI
Inspire the Next

離れた場所にあるPCを自席からリモート操作して対処

離れた場所にあるPCでトラブルが発生した場合、現場に行かずにリモート操作できます。
リモートメンテナンスに必要なファイルやデータを接続先のPCとやり取りしたり、PCの利用者とチャットで対話して状況を確認したりすることもできます。また、リモートメンテナンスの作業記録を画面録画し、あとでほかの利用者へのレクチャーなどに利用できます。

uVALUE

HITACHI
Inspire the Next

7
配布管理

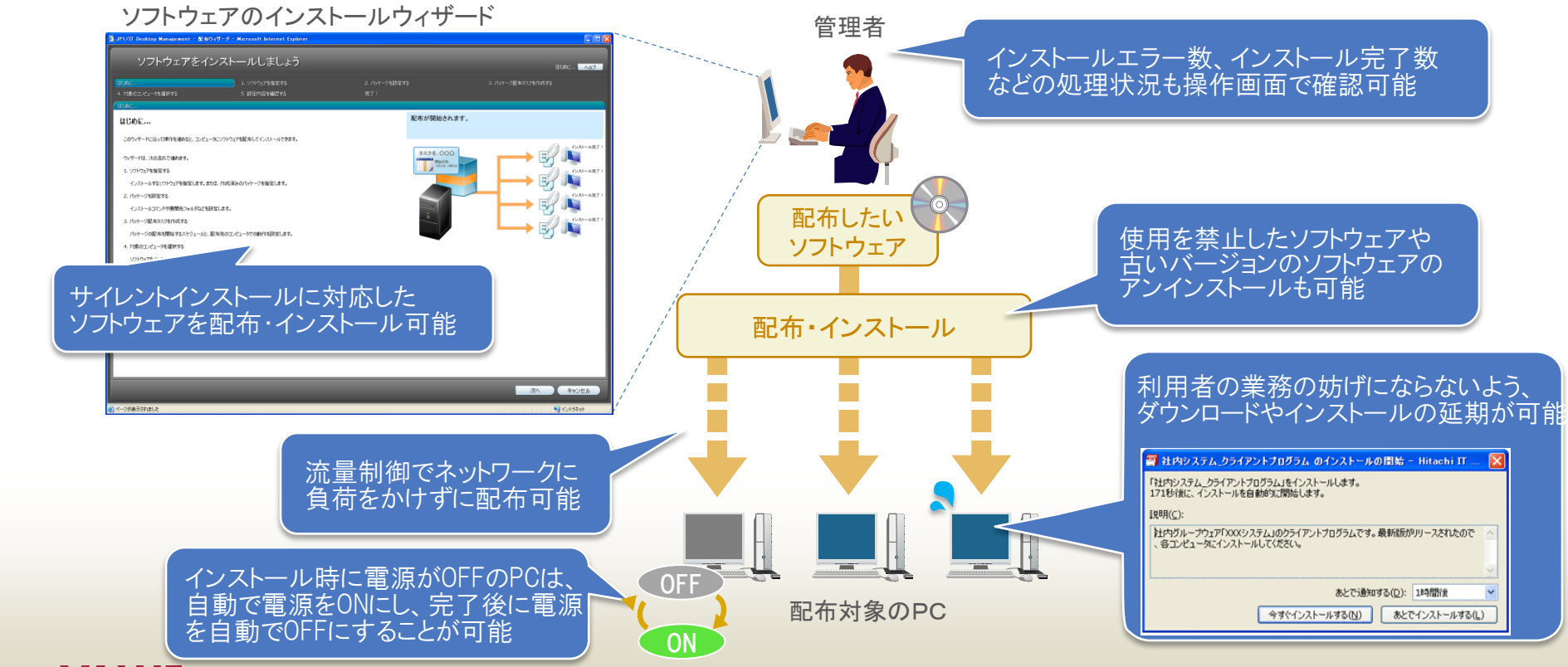
1. ソフトウェアの配布・インストール

uVALUE

HITACHI
Inspire the Next

PCのある場所まで行かなくても ソフトウェアを一括インストール

ウィルス対策製品のバージョンが古くて危険なPCには、新しいウィルス対策製品を配布・インストールできます。また、配布したいソフトウェアを登録し、インストールウィザードに従って操作すると、簡単に対象のPCに配布・インストールできます。使用を禁止しているソフトウェアのアンインストールも可能です。



uVALUE

HITACHI
Inspire the Next

8

さまざまな管理形態への対応

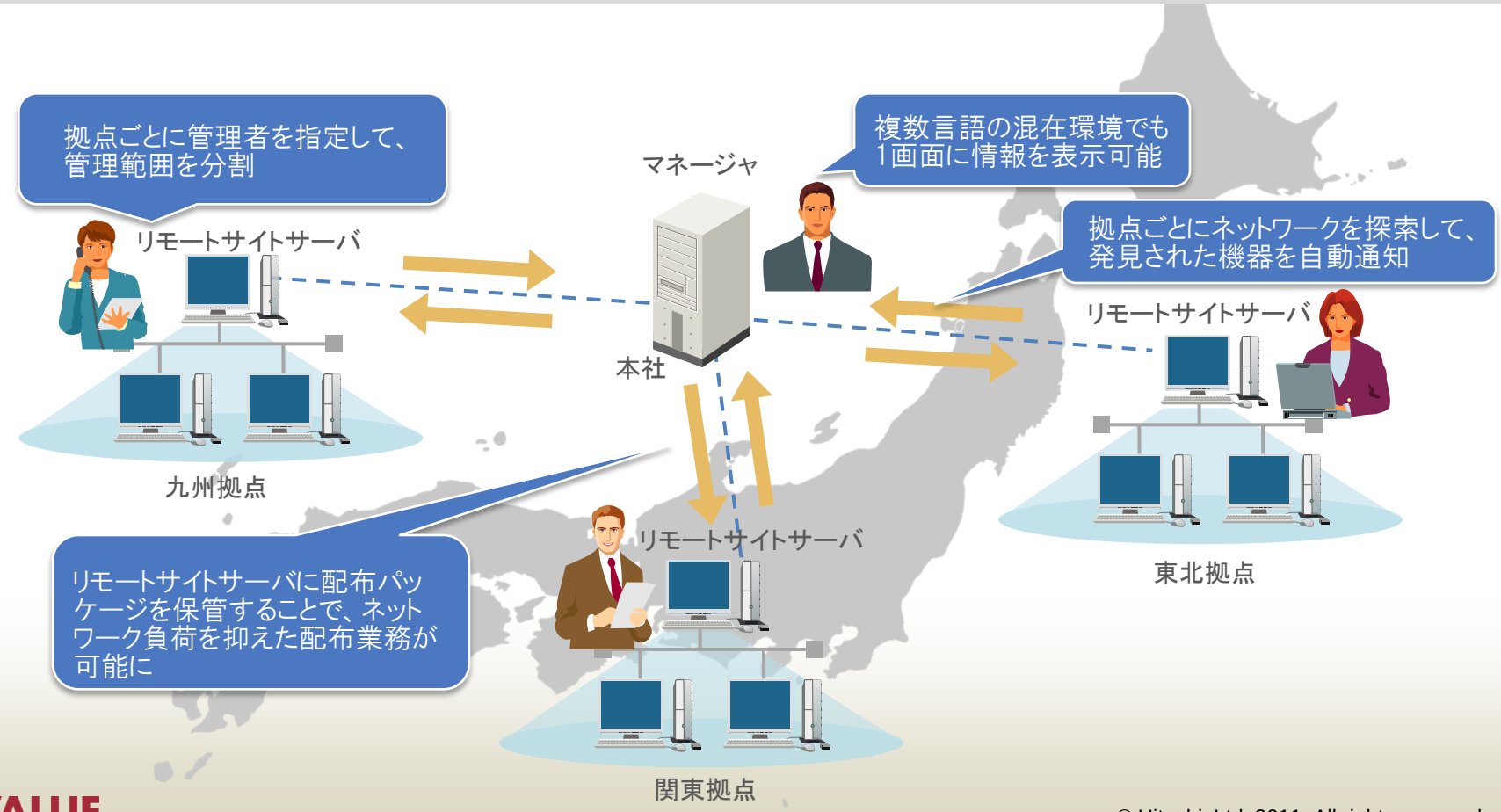
1. エンタープライズ対応
2. リモートサイトサーバの役割

uVALUE

HITACHI
Inspire the Next

1台のマネージャで全国の拠点を一元管理

大規模集約化環境でもマネージャ1台で全体を管理できます。拠点ごとに管理者を指定して、管理範囲を分割した運用にも対応します。また、英語、中国語などが混在する多言語環境でも、一つの操作画面から管理できます。

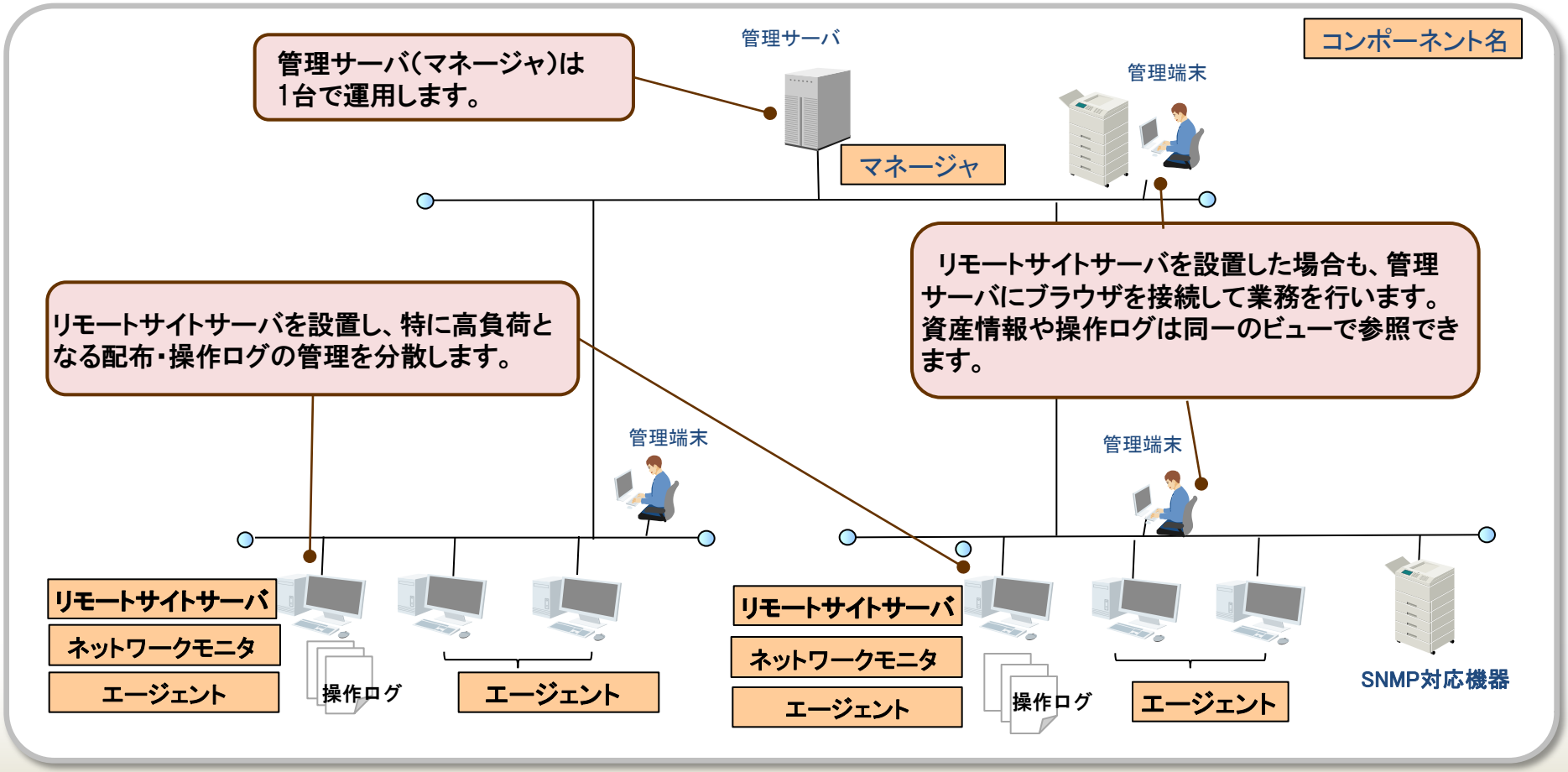


8-2. リモートサイトサーバの役割

HITACHI
Inspire the Next

拠点毎に中継(リモートサイトサーバ)を設置することで、以下の効果が得られます。

- **プログラム/データ配信時の配布に伴うネットワーク負荷低減**
- **操作ログを分散格納した場合の検索性能劣化低減**



HITACHI
Inspire the Next

A
付録

１．他製品とJP1/ITDMの違い
２．取得・管理可能な情報
３．コマンド一覧
４．システム構成例
　　ネットワーク制御を行う場合
　　拠点毎に中継を設置する場合
５．ライセンス/価格

uVALUE

A-1. HITO DirectorとJP1/ITDMの違い(1)

HITACHI
Inspire the Next

■スケール、サービス、製品構成等に以下のような相違があります。

	HITO Director 3.0	JP1/ITDM 09-50
スケーラビリティ	・小/中規模向け ・1,000ノードまで管理可能	・中/大規模向け ・10,000ノードまで管理可能
ライフサイクル	・最新版のみ販売 ・製品発売から2年間または 販売終了から1年間サポート提供	・最新2メジャーバージョン販売 ・各バージョンの販売期間最低5年 ・各バージョンのサポート期間は 販売終了から5年以上
サポート	・窓口対応:9時～17時 ・24時間対応なし ・価格は500ノードまで定額	・窓口対応:8時～19時 ・24時間対応あり ・価格はノード数に応じて変動
体験・試用	・試用版を無償提供 (提供サイトからダウンロード可) ・試用版に関する問い合わせ可能 ・ライセンスを購入することで、 試用版から製品版への移行可能	・体験版を無償提供 ・体験版から製品版への移行不可
ライセンス移行	・JP1/NETMからHITODへのライ センス移行パスなし(新規購入)	・JP1/NETMからJP1/ITDMへの ライセンス移行パスあり

A-1. HITO DirectorとJP1/ITDMの違い(2)

■機能上の主な相違は、以下のとおりです。
　当該バージョン時点の比較ですので、今後のバージョンで変更される可能性があります。

	HITO Director 3.0	JP1/ITDM 09-50
管理サーバアクティベーション/管理対象上限数登録	アクティベーションあり 管理対象上限数登録あり	アクティベーションなし 管理対象上限数登録あり
中継(リモートサイトサーバ)および中継による負荷分散	なし	あり
スコープ機能 (管理者毎に情報の可視範囲を制限)	なし	あり
HITO Analyzerとの連携機能	あり	なし
スマートデバイスの管理機能	なし (種別の追加は可能)	あり

A-1. JP1/NETM と JP1/ITDMの違い(1)

大項目	小項目	JP1/NETM V9 (DM+AIM+CSC＋NM)	JP1/ITDM 09-50
全体	手配方法	DM(Manager,Agent)、AIM、CSC、NM それぞれ別形名で手配	単一の形名で手配 (フルパッケージ＋ライセンスパック <管理ノード数ライセンス>)
	マネージャのRDBMS	・DM・AIMそれぞれにDBMSを構築要 ・内蔵DB、SQL Server、Oracle8i/9i選択	・単一のDB ・内蔵DBのみ
	マネージャのコンソール	製品毎に別コンソール	単一のWebコンソール
グルーピング・スコーピング等	・部署・設置場所等による機器の自動グルーピング ・管理者任意による機器のグルーピング	○	○
	管理者毎の操作内容限定	DM:一部可 AIM:○	×※
	管理者毎の情報可視範囲限定	DM:× AIM:○	○
配布管理	GUIインストールモード・AITによる自動インストール	○	× 管理者権限によるバックグラウンドインストール固定
	PUSHインストール	○	○
	PULLインストール	○	×

※ システム管理権限、ユーザ管理権限、参照権限からの選択となります。任意に業務限定はできません。

凡例 ○：サポート ×：非サポート

A-1. JP1/NETM と JP1/ITDMの違い(2)

大項目	小項目	JP1/NETM V9 (DM+AIM+CSC＋NM)	JP1/ITDM 09-50
資産管理(AIM)	ハードウェア管理・ソフトウェア管理・契約管理など	○	○
	案件管理	○	×
	問題点管理	○	△ [機器毎にノートの登録・検索可]
	ユーザレポート機能	○	×
セキュリティ管理(CSC/DM/AIM)	ポリシーによる判定と通知	○	○
	判定結果によるOS設定変更	×	○
	日立サポートサイトからのパッチ取得・適用	○	○
	操作ログの取得・参照	○	○
	外部デバイス利用の制御	○	○
	プログラム起動抑止	○	○
	プログラム稼動時間の取得	○	×
ネットワーク制御	遮断・検疫	○	○
レポート機能	-	○ インベントリビューア、AIMで表形式、棒グラフ、円グラフ等を出力可	○ 予め20種類の定形的なレポートを準備
リモコン	遠隔操作・録画・チャット等	○	○
	Intel vPro リモートKVM対応端末との接続	×	○

凡例　○：サポート　×：非サポート　△：代替機能

A-2. 取得・管理可能な情報

HITACHI
Inspire the Next

■端末から取得できる情報

管理対象機器一覧情報		機器の種別、最終生存確認日時など。
システム情報	コンピュータ情報	コンピュータ名、ホスト名、製造元、シリアル番号など。
	ユーザー情報	ユーザーアカウント名、ロケールなど。
	OS情報	OSの名称、適用されているサービスパックなど。
	ネットワーク情報	IPアドレス、DNSサーバのアドレス、DHCPの設定、ドメインなど。
ハードウェア情報		CPU、メモリ、ディスクドライブなど。
インストールソフトウェア情報		インストールされているソフトウェアの名称、バージョンなど。
セキュリティ情報	Windows Update情報	OSに適用されているパッチの名称など。
	ウィルス対策製品情報	ウィルス対策製品の名称、バージョン、常駐/非常駐の設定など。
	禁止Windowsサービス情報	セキュリティポリシーで禁止しているWindowsサービスのうち、稼働しているサービスの内部名。
	OSセキュリティ設定情報	脆弱パスワードの有無、共有フォルダや管理共有の設定など。
プリンタ情報		プリンタの種別(インクジェット)、消耗品(トナー)の情報など

■資産情報として管理できる情報

ハードウェア資産情報	コンピュータ・サーバ・USBデバイスなどの種別、運用中/在庫といったステータスなど。
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、ライセンスの利用状況など。
契約情報	サポート契約やレンタル契約、リース契約などの契約の種類、満了日など。

A-3. コマンド一覧

■使用可能なコマンドの一覧(1/2)

コマンド名	機能
ioutils exportasset	ハードウェア資産情報をエクスポートします。
ioutils importasset	ハードウェア資産情報をインポートします。
ioutils exportfield	追加管理項目の設定をエクスポートします。
ioutils importfield	追加管理項目の設定をインポートします。
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。
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。
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。
ioutils importpolicy	セキュリティポリシーの設定をインポートします。
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。
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。
ioutils exportoplog	操作ログをエクスポートします。

A-3. コマンド一覧

■使用可能なコマンドの一覧(2/2)

コマンド名	機能
ioutils exportfilter	フィルタの設定をエクスポートします。
ioutils importfilter	フィルタの設定をインポートします。
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。
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。
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。
reorgdb	データベースを再編成します。
stopservice	管理用サーバのサービスを停止します。
startservice	管理用サーバのサービスを開始します。
getlogs	トラブルシュート用情報を取得します。
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。
addfwlist.bat	Windowsファイアウォールの例外許可を設定します。

A-4. システム構成例1（ネットワーク制御を行う場合）

HITACHI
Inspire the Next

管理ビューア
Windows
Internet Explorer
JP1/ITDM
（Remote Control Manager）

マネージャー
Windows
JP1/ITDM
（Manager）

ネットワーク監視サーバ
Windows
JP1/ITDM
（Network Monitor）
JP1/ITDM
（Agent）

接続許可していないPCの遮断

個人持ち込みPC等

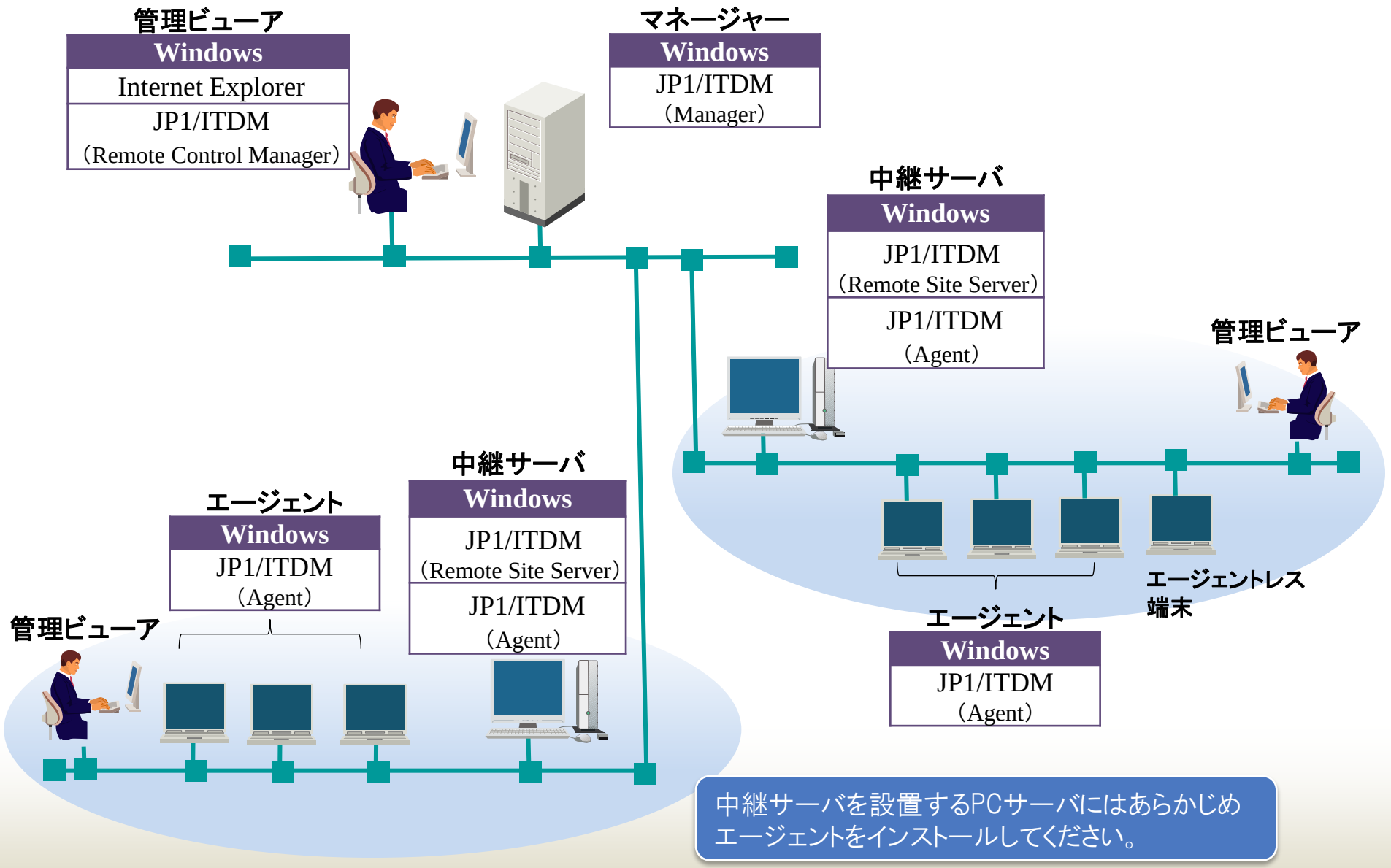
セキュリティポリシーに適合しなくなったPCの遮断

ネットワーク監視サーバは、
監視するセグメント毎に1台ずつ必要になります。

ネットワーク監視サーバにするPCサーバにはあらかじめエージェントをインストールしてください。

エージェント
Windows
JP1/ITDM
（Agent）

A-4. システム構成例2（拠点毎に中継を設置する場合）



中継サーバを設置するPCサーバにはあらかじめ
エージェントをインストールしてください。

A-5. ライセンス/価格

HITACHI
Inspire the Next

日本語版 製品価格・ライセンス一覧

#	製品名 （形名）	ライセンス区分	プラットフォーム	オプションコード	税抜価格（円）	管理できるノード数
1	JP1/IT Desktop Management - Manager (P-2642-7394)	管理ノード数ライセンス	Windows	&UWN	250,000	フルパッケージ＋10
2				&U1	13,500	1（追加）
3				&UK	135,000	10（追加）
4				&UN	1,250,000	100（追加）
5				&UQ	5,100,000	500（追加）
6				&UR	9,800,000	1,000（追加）
7				&US	18,500,000	2,000（追加）
8				&UT	37,500,000	5,000（追加）
9				&UU	63,000,000	10,000（追加）

他社商品名、商標等の引用に関する表示

HITACHI
Inspire the Next

・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。
・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。
・Microsoft、Windows、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。
・Windows Serverは、米国Microsoft Corporationの米国及びその他の国における登録商標です。
・ 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。
・ Symantec，Symantec AntiVirusは，Symantec Corporation の米国およびその他の国における商標または登録商標です。
・ McAfee，VirusScan,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。
・ ウイルスバスターは，トレンドマイクロ株式会社の登録商標です。
・ 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。
・ 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。
・ Kasperskyは，米国におけるKaspersky Labの登録商標です。
・ ESET，NOD32は，ESET，LLCならびにESET，spol. s.r.o.の登録商標です。
・ Sophos Anti-Virusは，Sophos Plc.の商品名称です。
・ Sophos Computer Securityは，Sophos Plc.の商品名称です。
・ Sophos Endpoint Security and Data Protectionは，Sophos Plc.の商品名称です。
・ Sophos Security Suiteは，Sophos Plc.の商品名称です。
・ F-Secureは，フィンランドF-Secure Corporationの登録商標です。

その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

◇本製品を輸出される場合には、外国為替 及び 外国貿易法 並びに 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。

●画面表示をはじめ、製品仕様は、改良のため変更することがあります。

uVALUE