HITACHI
Inspire the Next

統合システム運用管理

エンドポイント管理

エンドポイント管理
JP1 Cloud Service/Endpoint Managementのご紹介
～エンドポイントを適切に管理し、セキュリティリスクから守る～

株式会社 日立製作所

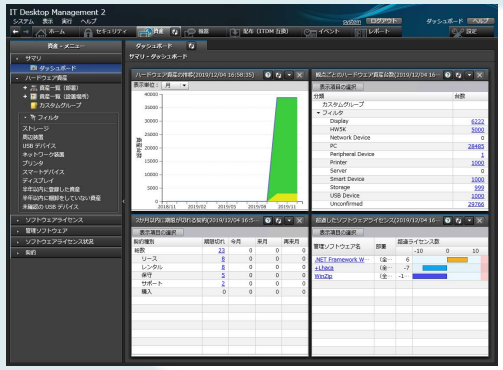
Contents

エンドポイント管理 JP1 Cloud Service/Endpoint Management の概要

HITACHI
Inspire the Next

多様化するエンドポイントを適切に管理し、セキュリティリスクから守る

PCやサーバ、仮想デスクトップ、スマートデバイスといった、多様化するIT環境のソフトウェア情報、ハードウェア情報、セキュリティ情報、操作ログなどを自動収集し、現状を可視化。脆弱性対策や情報漏えい防止策などのセキュリティ対策の徹底や、機器、ソフトウェア、IT資産・契約情報の適正な管理を実現します。

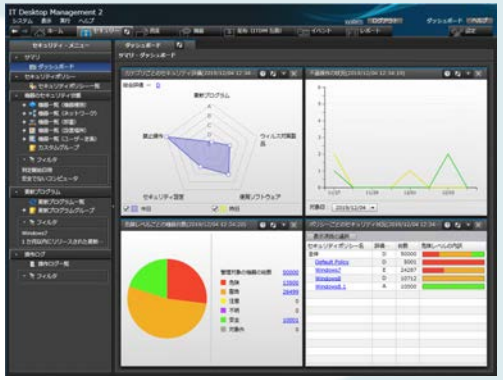


配布管理

ソフトウェアを計画的に配布・適用

資産管理

IT資産の最新情報を収集し、一元管理



セキュリティ管理

セキュリティ対策状況を把握・対処

ソフトウェア情報 ・ ハードウェア情報 ・ セキュリティ情報 ・ 操作ログ

DaaS: Desktop as a Service

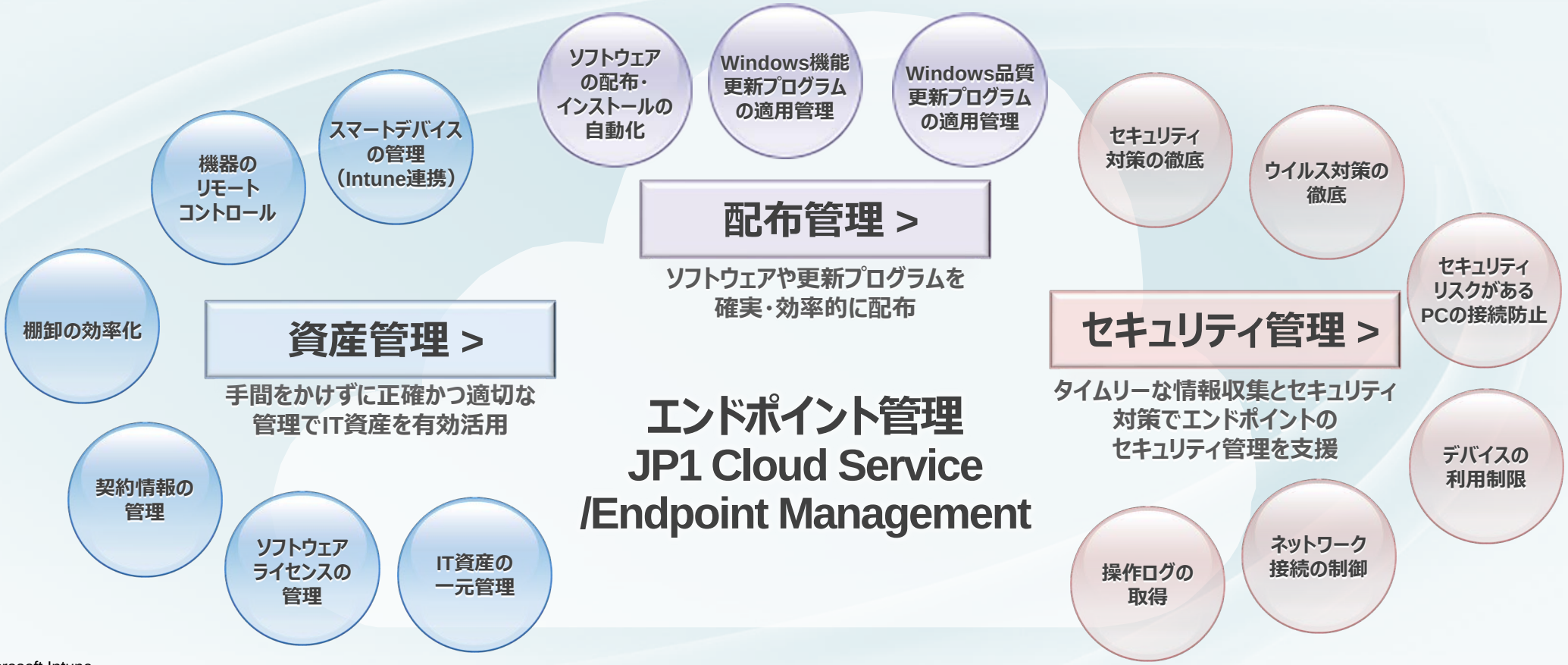
できること

- エンドポイント管理 JP1 Cloud Service/Endpoint Management でできること
- 現状の把握
- 資産管理
- 配布管理
- セキュリティ管理
- 複数管理者での業務分担

エンドポイント管理 JP1 Cloud Service/Endpoint Management でできること

HITACHI
Inspire the Next

やさしいインタフェースと豊富な管理機能で、多様化するIT資産を守ります。



Intune: Microsoft Intune

現状の把握 >
複数管理者での業務分担 >
機能一覧 >
システム構成例 >
できること > | 資産管理 > | 配布管理 > | セキュリティ管理 >

現状の把握　【前日からの変化・重要なイベント】

HITACHI
Inspire the Next

ネットワークに接続されたPCや機器の情報を自動的に収集し、日々の情報をホーム画面にまとめて表示します。
ログイン後、最初に表示されるホーム画面を見るだけで前日からの変化や重要なイベントの発生状況など、全体の概況と対策事項がわかります。

☑ 前日と変わったところはないか？

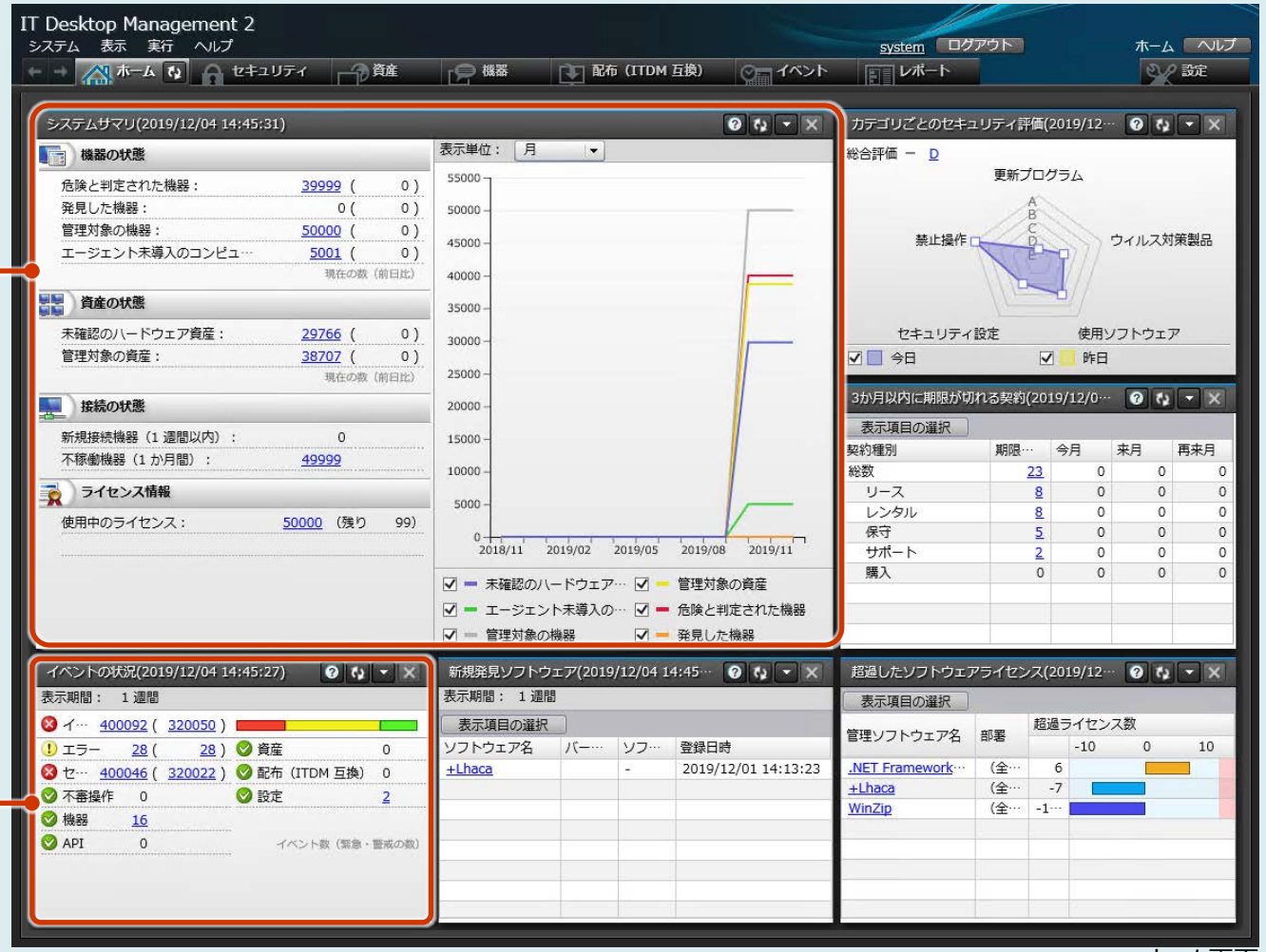
システムサマリで、前日からの差異が確認できます。

- ☑ 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、稼働が確認できていない機器はないか？
- ☑ 全体の状況や推移はどうか？

前日と比べて変化がなく、システムが安全に保たれていることが確認できればOK。問題がある場合は、項目をクリックして詳細な情報を確認できるので、対処もスムーズに行えます。

☑ 重要なイベントが発生していないか？

発生したイベントを集計して表示。どんな種類のイベントが何件発生しているかがすぐにわかります。各イベントの詳細は、1クリックで確認できます。



ホーム画面

ITDM: JP1/IT Desktop Management

現状の把握　【更新プログラム・不要なインストール・ライセンス違反】

HITACHI
Inspire the Next

Windows品質更新プログラムなどのセキュリティ対策状況、不要なソフトウェアのインストールやソフトウェアライセンス違反の有無などを、ホーム画面で確認できます。

☑ Windows品質更新プログラムなどのセキュリティ対策は適切か？

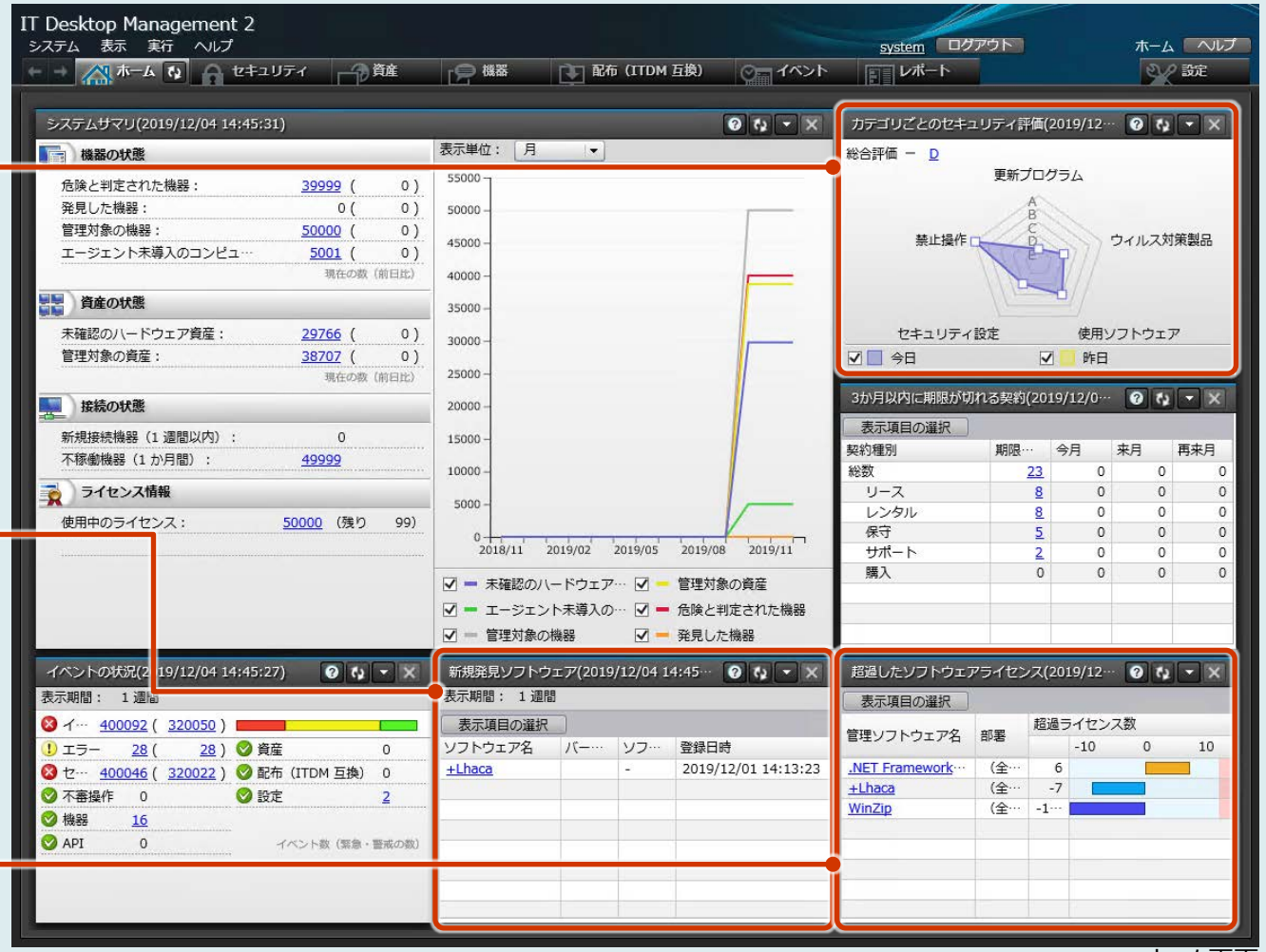
Windows品質更新プログラムやウイルス対策、セキュリティ設定など、カテゴリ別のセキュリティ対策状況を総合評価。
セキュリティ対策状況がひと目でわかります。

☑ 不要なインストールは行われていないか？

新しいソフトウェアやWindowsストアアプリがPCにインストールされたことを検知できます。定期的にチェックすることで、業務に必要のないソフトウェアがインストールされていないかを確認できます。

☑ ソフトウェアライセンス違反はないか？

保有するライセンス数に対しての超過の有無を管理ソフトウェアごとに確認できます。

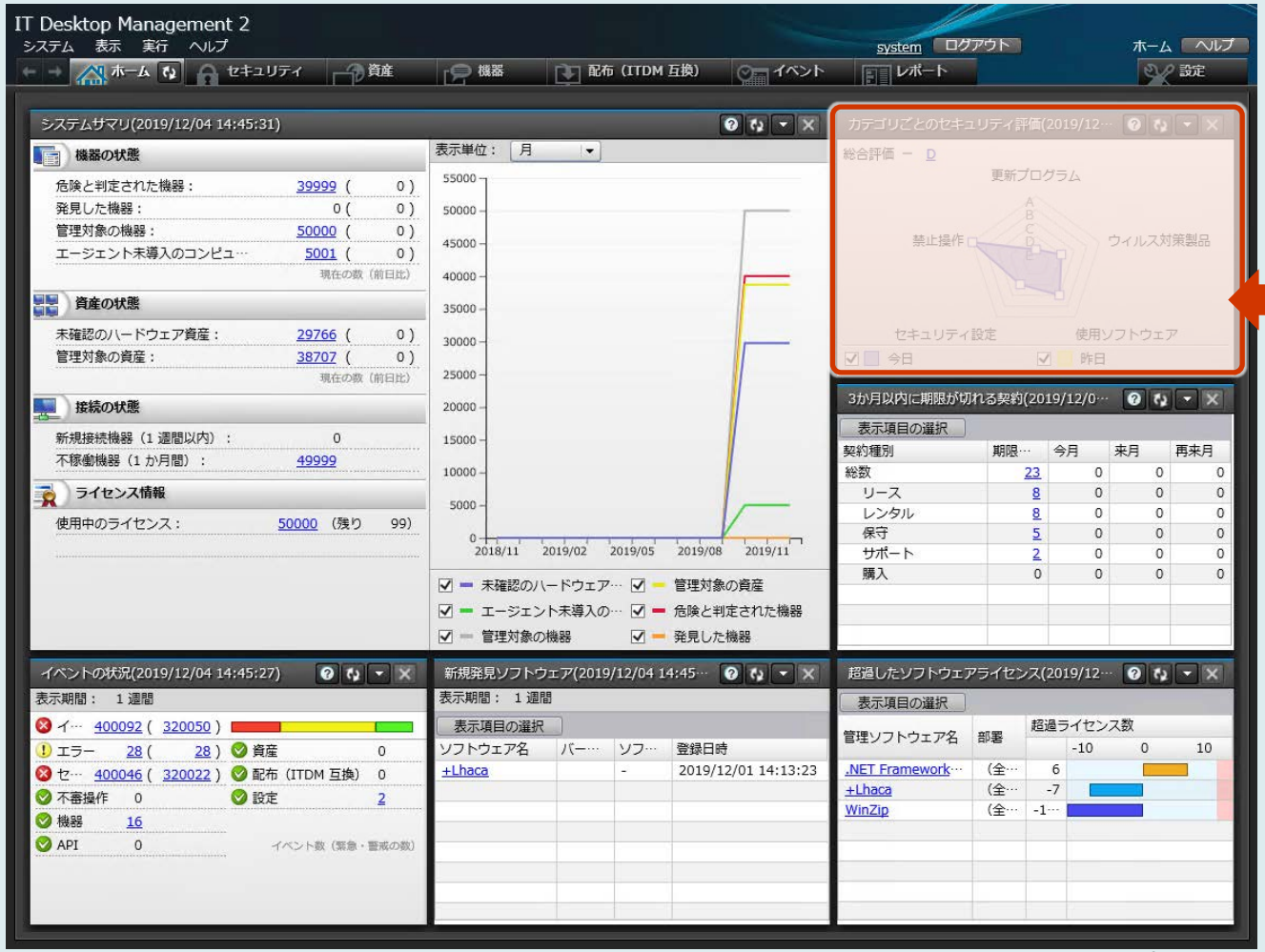


ホーム画面

ITDM: JP1/IT Desktop Management

現状の把握　【ホーム画面のカスタマイズ】

ホーム画面中の小さな画面「パネル」は、さまざまな情報のサマリ（要約）になっています。パネルの中から日々の運用でチェックしたいパネルを選んで、自分専用の画面を構成できます。



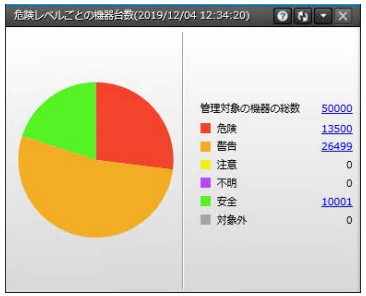
ホーム画面

ITDM: JP1/IT Desktop Management

3種類のレイアウトから選択可能

チェックしたいサマリ情報に置き換え可能

☑ **セキュリティ対策が必要なPCはないか？**



「危険レベルごとの機器台数」パネル

資産管理

このようなお悩み、ありませんか？

HITACHI
Inspire the Next

☑ PCや機器の台数、インストールされているソフトウェアを正確に把握できていない。

IT資産の一元管理 p. 9

ネットワーク経由で、ハードウェアやソフトウェアの情報を自動収集します。また、ネットワークに常時接続していないノートPCやリモートワークで社外に持ち出したノートPC、シンクライアント、スマートデバイスも管理できます。さらに、契約情報（契約種別や期限など）を登録して、IT資産情報と関連付けて管理できます。

☑ さまざまなソフトウェアを購入しているが、ライセンスが足りているか確証がない。

ソフトウェアライセンスの管理 p. 12

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できます。ソフトウェアのライセンス保有数、ライセンス消費数、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。
また、ソフトウェアをインストールしているのに、ライセンスの割り当てがないPCも特定できます。

☑ 契約書がたくさんあり過ぎて、簡単に探し出せない。

契約情報の管理 p. 13

契約種別、契約開始日、契約終了日、契約状態といった契約情報と、IT資産を関連付けて管理できます。
契約書をスキャンした電子データを契約情報の添付データとして保存できるので、実際の書類を探さなくても、画面上ですぐに契約書の内容を確認できます。

☑ IT資産の棚卸に多くの手間と時間がかかっている。

棚卸の効率化 p. 14

社内で使用しているPCやサーバなどの機器情報を収集できます。新規に追加され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。
これらをリストに出力して、資産の現物確認にも利用できるので、効率的な棚卸ができます。

☑ PCのトラブル対応で、PCのある場所までわざわざ出向いている。

機器のリモートコントロール p. 15

離れた場所にあるPCでトラブルが発生した場合、現場に行かずに自席からリモートコントロールできます。
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、リモートコントロールの作業記録を録画しておき、あとでほかの利用者にレクチャーしたりすることもできます。

☑ スマートデバイスを導入したが、きちんと管理できているか不安がある。

スマートデバイスの管理（Intune連携） p. 17

スマートフォンやタブレットなどのスマートデバイスの情報を収集して、PCやサーバなどのコンピュータと一緒に管理できます。
また、スマートデバイスの紛失時に、ロックや初期化といったスマートデバイスへの操作が管理者側からでき、リスクを回避できます。

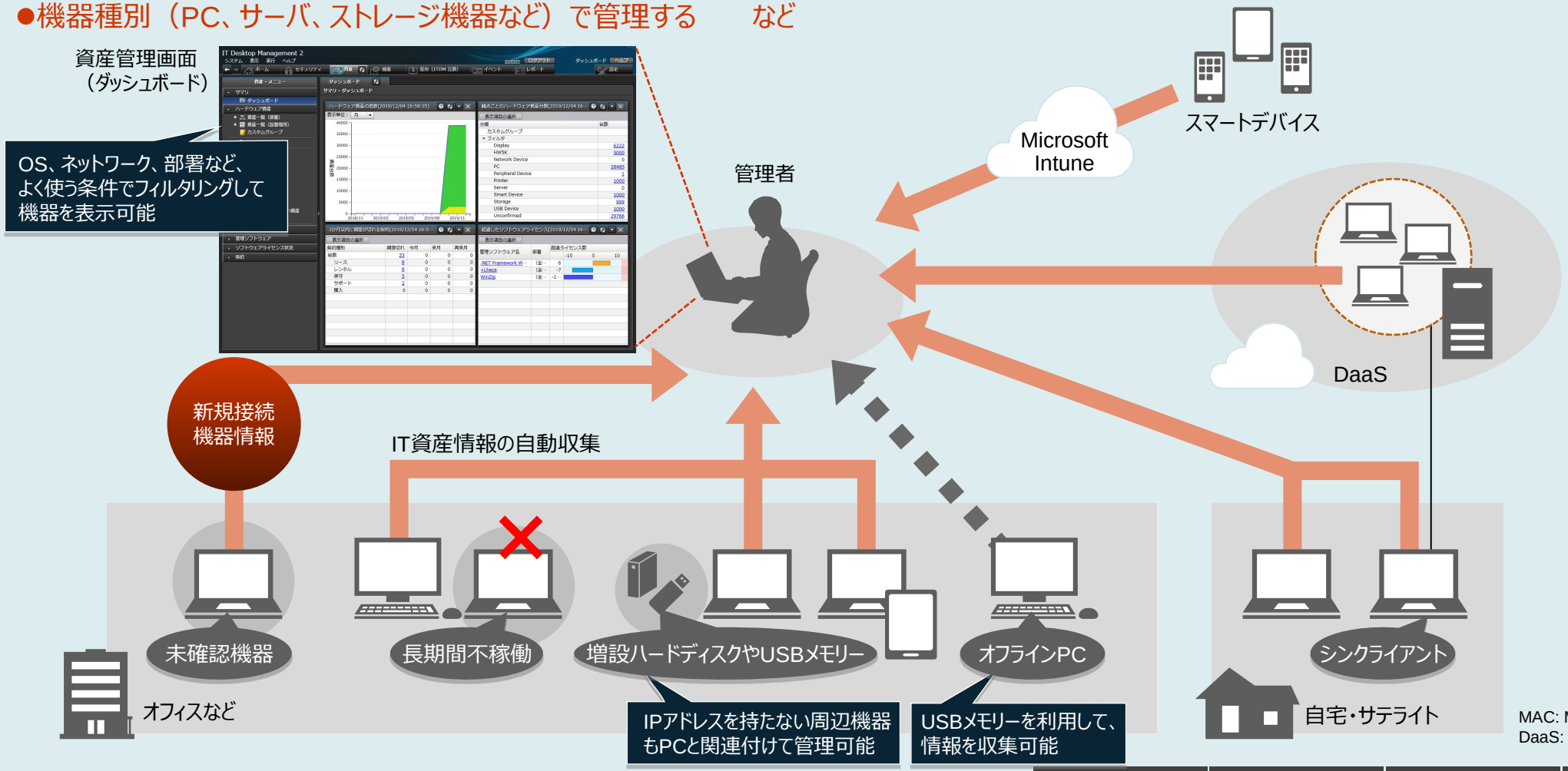
Intune: Microsoft Intune

IT資産の一元管理　【機器の管理】

HITACHI
Inspire the Next

PCのOS、メモリー、ハードディスク容量といったスペック情報や、IPアドレス、MACアドレスなどのネットワーク情報、利用者や部署などの情報を収集できます。
これらの情報をもとにして、資産として登録されていない機器が接続されたら未確認機器として通知します。

例
- ●長期間ネットワークに接続されていないPCを抽出する
- ●機器種別（PC、サーバ、ストレージ機器など）で管理する　など



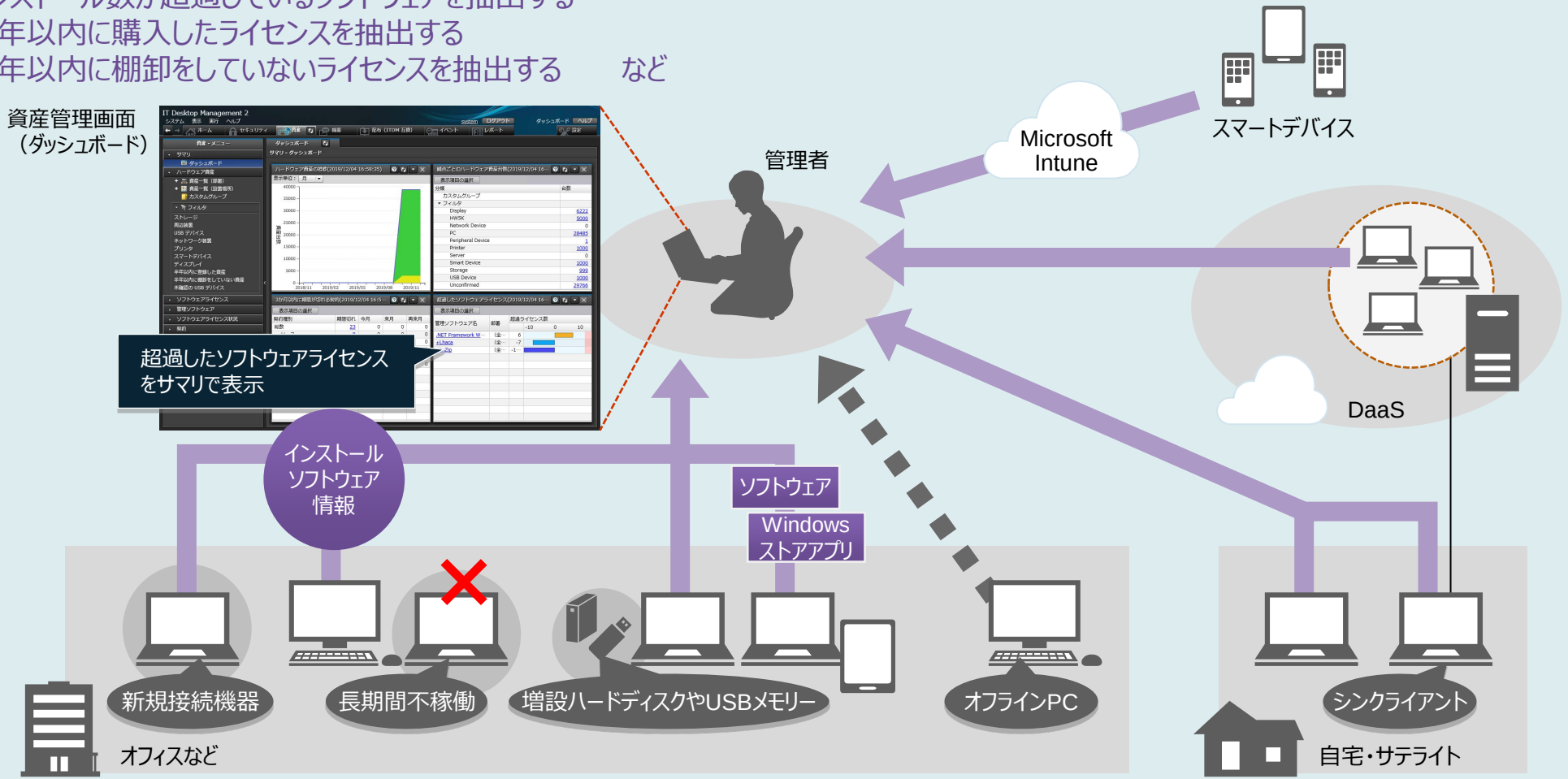
MAC: Media Access Control
DaaS: Desktop as a Service

IT資産の一元管理　【ソフトウェアの管理】

HITACHI
Inspire the Next

インストールしているソフトウェアやWindowsストアアプリの名称、バージョン、インストール日付などの情報を収集できます。インストールしているソフトウェアは、ライセンスの割り当て状況を自動集計できます。実際にインストールされている数と保有しているライセンス数がひと目でわかるので、適正なライセンス管理ができます。

例
- ●インストール数が超過しているソフトウェアを抽出する
- ●半年以内に購入したライセンスを抽出する
- ●半年以内に棚卸をしていないライセンスを抽出する　など



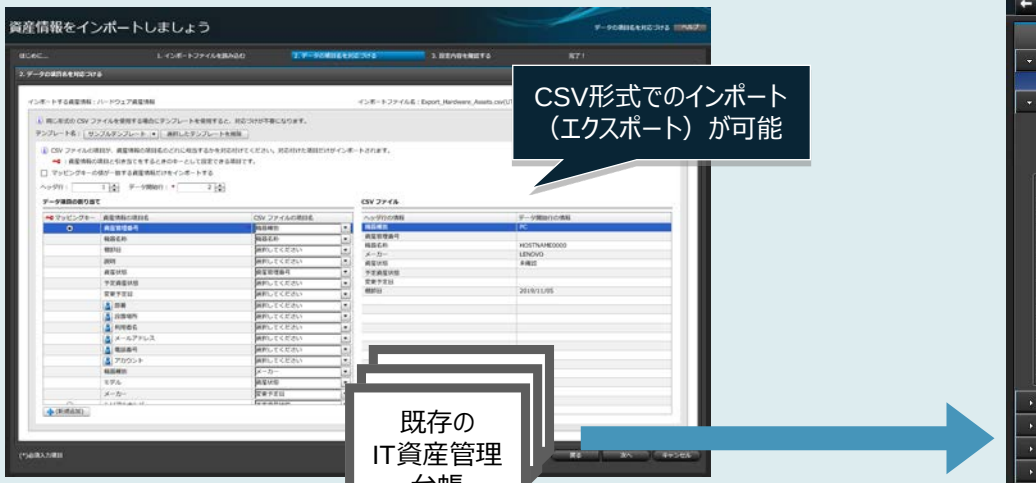
DaaS: Desktop as a Service

IT資産の一元管理　【IT資産・契約情報の一元管理】

HITACHI
Inspire the Next

既存のIT資産管理台帳の情報（データ）を取り込み、自動収集した「機器情報」「ソフトウェア情報」、さらには契約種別や契約期間などの「契約情報」と合わせて一元管理できます。台帳などで管理している契約情報（会社名や連絡先など）も登録して管理可能。既存のIT資産管理台帳のデータは、ウィザード画面に従うだけで簡単にインポートできます。

資産情報のインポートウィザード



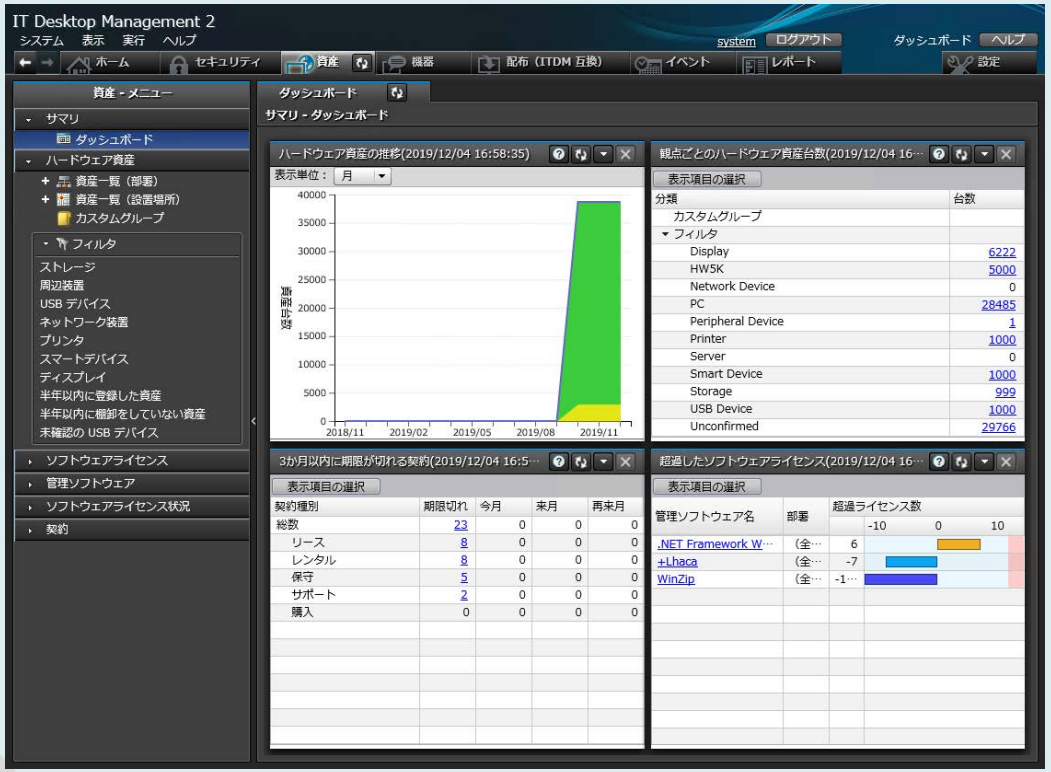
既存のIT資産管理台帳

契約情報も合わせて一元管理

契約情報（会社名や連絡先など）

管理者

資産管理画面（ダッシュボード）

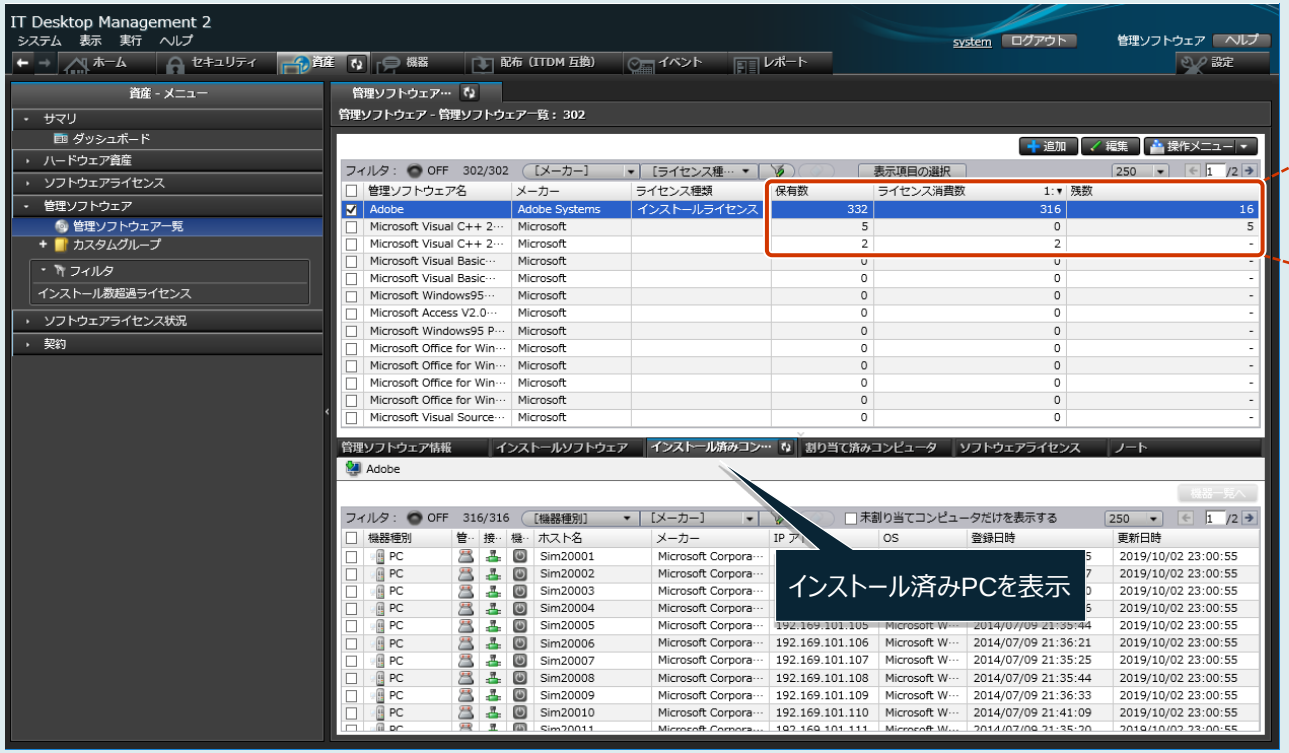


ITDM: JP1/IT Desktop Management

ソフトウェアライセンスの管理

ソフトウェアライセンスの割り当て数や割り当て済みPC、実際のインストール数やインストール済みPCがわかります。
ライセンスが割り当てられていないのにソフトウェアをインストールしているPCの利用者に対しては、使用許可を得てインストールするように指導することで、未許可のインストールやライセンス違反を防止できます。

資産管理画面（管理ソフトウェア一覧）



ソフトウェアごとに保有数、ライセンス消費数、残数を表示

保有数	ライセンス消費数	1:	残数
332	316		16
5	0		5
2	2		-

ソフトウェアの情報が登録されたSAMAC ソフトウェア辞書を取り込むことで、有償ソフトウェアやフリーソフトウェアを区別できます。ライセンス管理が必要なソフトウェアだけを管理することで、ライセンス管理の効率を向上できます。

ITDM: JP1/IT Desktop Management

さらに

- Microsoft Office製品は、製品版とボリュームライセンス版を区別して管理できます。ボリュームライセンス版はプロダクトIDを利用して、ライセンスをまとめて管理できます。*
- ソフトウェアのライセンス消費数を自動集計し、保有しているライセンスの数と比較して余剰ライセンスと超過ライセンスをレポート表示できます。

＊ 一部のMicrosoft Office製品は、プロダクトIDを利用して管理できない場合があります。

契約情報の管理

サポート契約やレンタル契約、リース契約などの契約情報を登録して、それぞれの資産情報と対応付けて管理できます。
満了日が近づいている契約情報を前もって把握できるため、期限満了前に適切に対応することが可能です。

資産管理画面（契約一覧）

ITDM: JP1/IT Desktop Management

「3か月以内に期限が切れる契約」パネル
（ホーム画面）

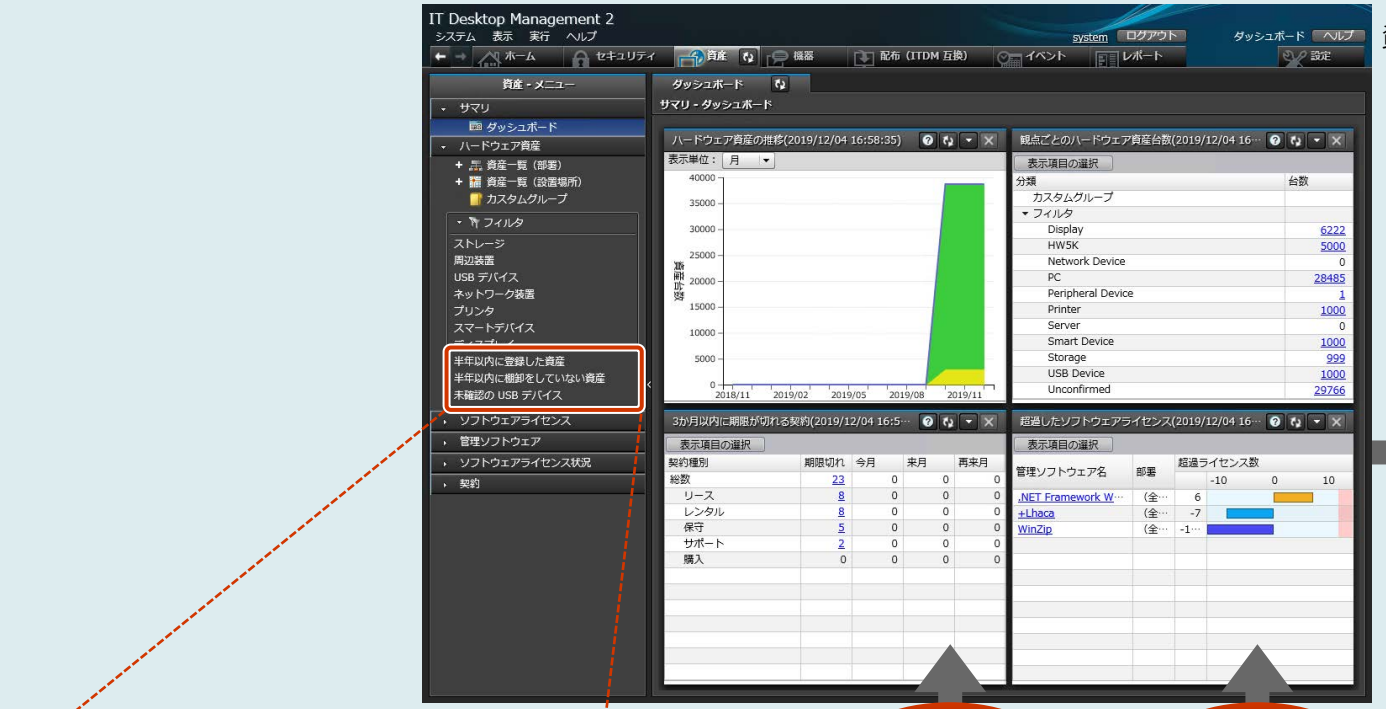
契約種別	期限…	今月	来月	再来月
総数	23	0	0	0
リース	8	0	0	0
レンタル	8	0	0	0
保守	5	0	0	0
サポート	2	0	0	0
購入	0	0	0	0

さらに

- 契約期限はホーム画面に表示するように設定できるので、期限が迫っている契約をすぐに確認できます。
- 日次・週次・月次に通知されるダイジェストレポートでも契約期限を把握できるので、契約更新漏れを防止できます。

棚卸の効率化

部署の異動や移管などでPCや機器の管理元が変わってしまっても、ネットワーク経由で存在を確認できます。
IPアドレス情報などから機器の存在場所を特定して確認することも容易になり、棚卸の効率が向上します。

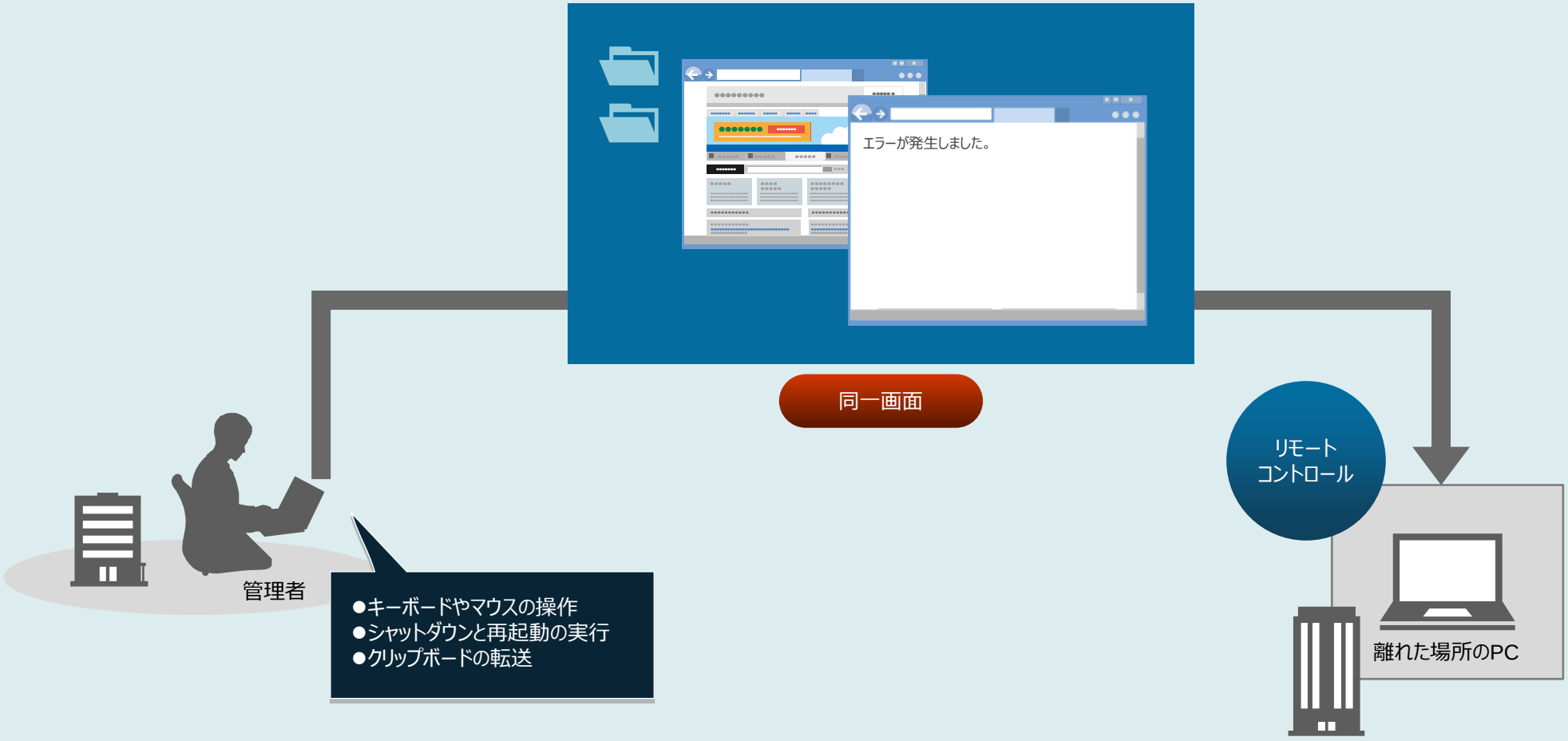


ITDM: JP1/IT Desktop Management

機器のリモートコントロール　【接続先PCの操作】

HITACHI
Inspire the Next

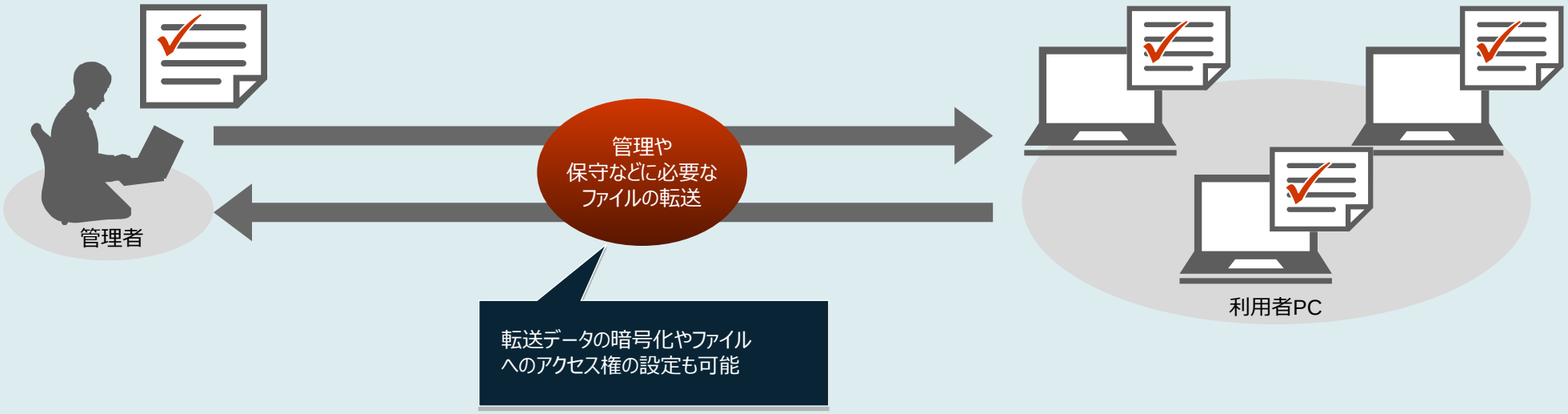
管理者のPC画面上に接続先PCの画面を表示して、自席のPC画面を操作するのと同じ感覚で、接続先PCの画面を操作できます。



機器のリモートコントロール　【ファイルの転送】

HITACHI
Inspire the Next

**Windowsのエクスプローラーと同様の操作で、接続先PCの管理や保守などに必要なファイルを参照したり、ドラッグ&ドロップでファイルを転送したりできます。
また、複数の接続先PCに一括でファイルを転送することもできます。
たとえば、トラブルが発生したPCのログファイルを収集して解析したり、接続先PCに必要なデータを転送したりできます。**



さらに

- ●操作内容を録画・再生したり、チャットを利用して接続先PCの利用者とリアルタイムに会話ができます。
- ●社内のPCが不正にリモートコントロールされないように、リモートコントロールを許可するPCやユーザーを設定できます。
- ●接続先PCがインテル社のAMT（Active Management Technology）＊の場合は、管理者のPCのCD-ROM/DVD-ROMドライブを、接続先PCのドライブとして利用できます。

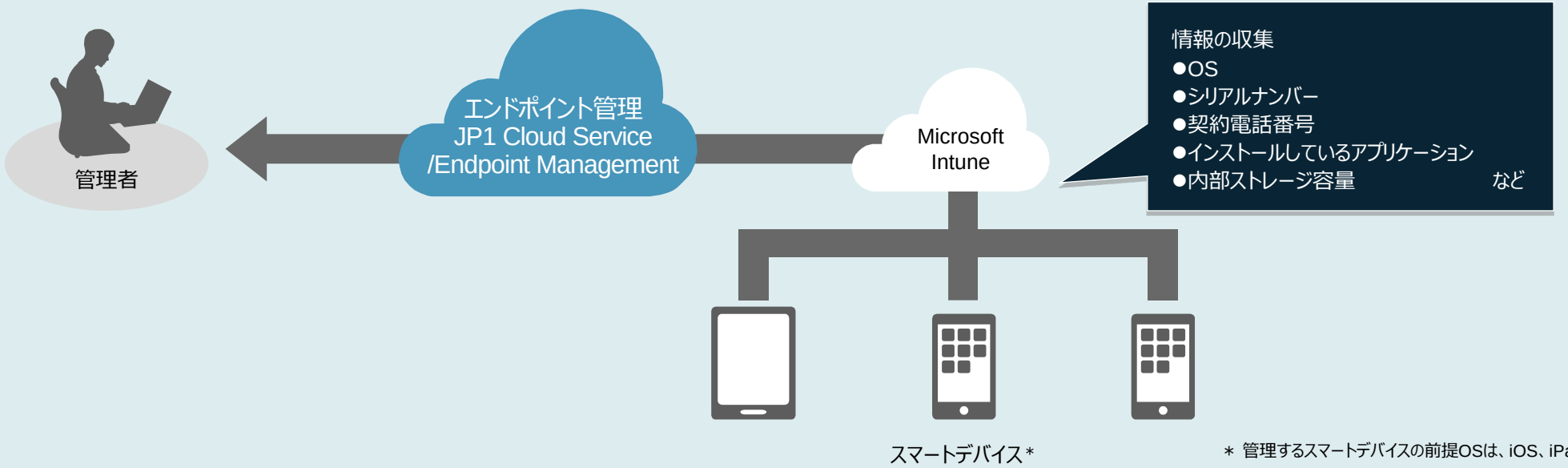
＊ 対応バージョンについては、マニュアルでご確認ください。

スマートデバイスの管理（Intune連携）

HITACHI
Inspire the Next

■スマートデバイスの情報収集

Microsoft Intuneと連携することで、スマートデバイスのOS、シリアルナンバー、契約電話番号などの情報を収集できます。
収集したスマートデバイスの情報は、PCやサーバなどの情報と一緒に一元管理できます。



＊ 管理するスマートデバイスの前提OSは、iOS、iPadOS、またはAndroidです。

■スマートデバイスの制御

スマートデバイスを制御することで、業務で使用する際に起こり得るリスクを未然に防ぐことができます。
たとえば、利用者がスマートデバイスを紛失した場合に、利用されないようにロックしたり、情報漏えいを防ぐために初期化するなどの操作を離れた場所から実施できます。

Intune: Microsoft Intune

このようなお悩み、ありませんか？

HITACHI
Inspire the Next

☑ 社内のPCやサーバにソフトウェアを配布・インストールする作業が頻繁に発生する。

ソフトウェアの配布・インストールの自動化 p. 19

遠隔地にある社内のPCやサーバに、自動でソフトウェアを配布・インストールできます。
特定の部署に範囲を限定してソフトウェアを配布したり、配布・インストールの日時を指定したりするなど、さまざまな設定ができるため、きめ細かい運用が可能になります。

☑ Windowsの機能アップデートによって業務が中断されることがある。

Windows機能更新プログラムの適用管理 p. 20

Windows 11の機能更新プログラムの適用延期や自動更新の無効化により、自動的にOSがアップデートされてしまうことを防ぎます。
配布時のネットワーク負荷の軽減や、インストールタイミングの制御により、大規模環境でも、業務への影響を抑えて計画的にOSをアップデートできます。

☑ Windows品質更新プログラムを適用していないPCがあるかもしれない。

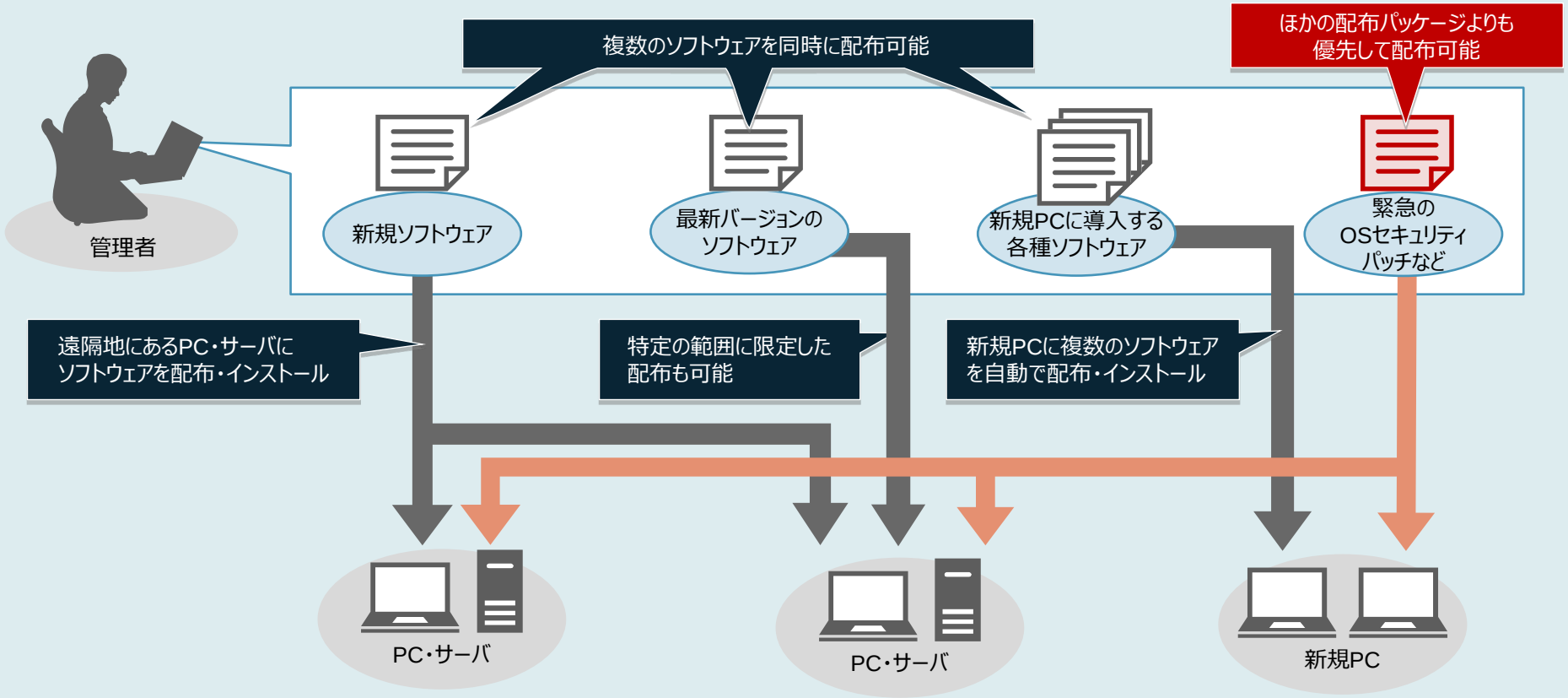
Windows品質更新プログラムの適用管理 p. 21

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品質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品質更新プログラムがある場合は、特定のプログラムを選んで配布・適用することも可能です。

ソフトウェアの配布・インストールの自動化

HITACHI
Inspire the Next

最新ソフトウェアへの一斉バージョンアップ、新規PCへのソフトウェアの導入など、管理者側で用意したソフトウェアを社内に配布し、インストールする作業を離れた場所から効率的に実施できます。

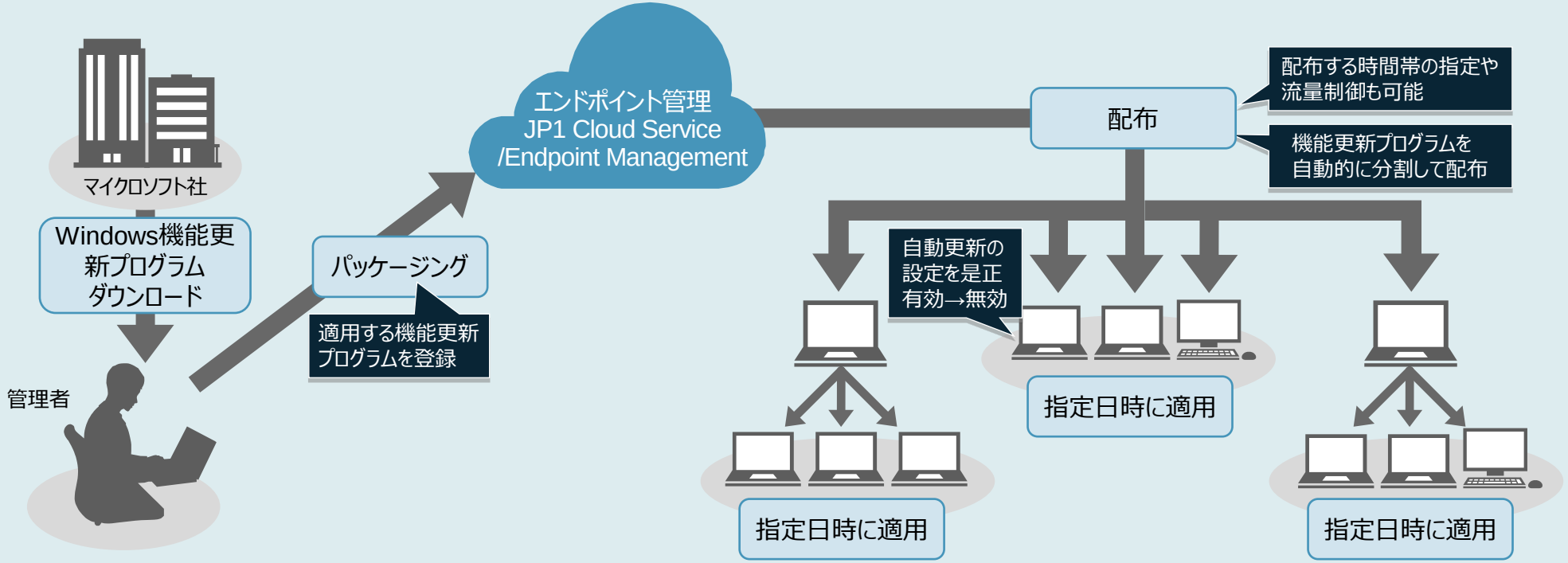


さらに

1度のデータ送信で複数のPCやサーバに同じファイルを配布したり、容量の大きいデータを分割して転送間隔を制御したりできるので、
ネットワークに負荷をかけないソフトウェアやファイルの配布運用が可能です。

Windows機能更新プログラムの適用管理

管理者側でダウンロードしたWindows機能更新プログラムを、ネットワークに負荷をかけないように多数のPCへ計画的に配布し、あらかじめ指定した日時に一斉に適用するなど、社内のPCへのWindows機能更新プログラムの適用をコントロールできます。

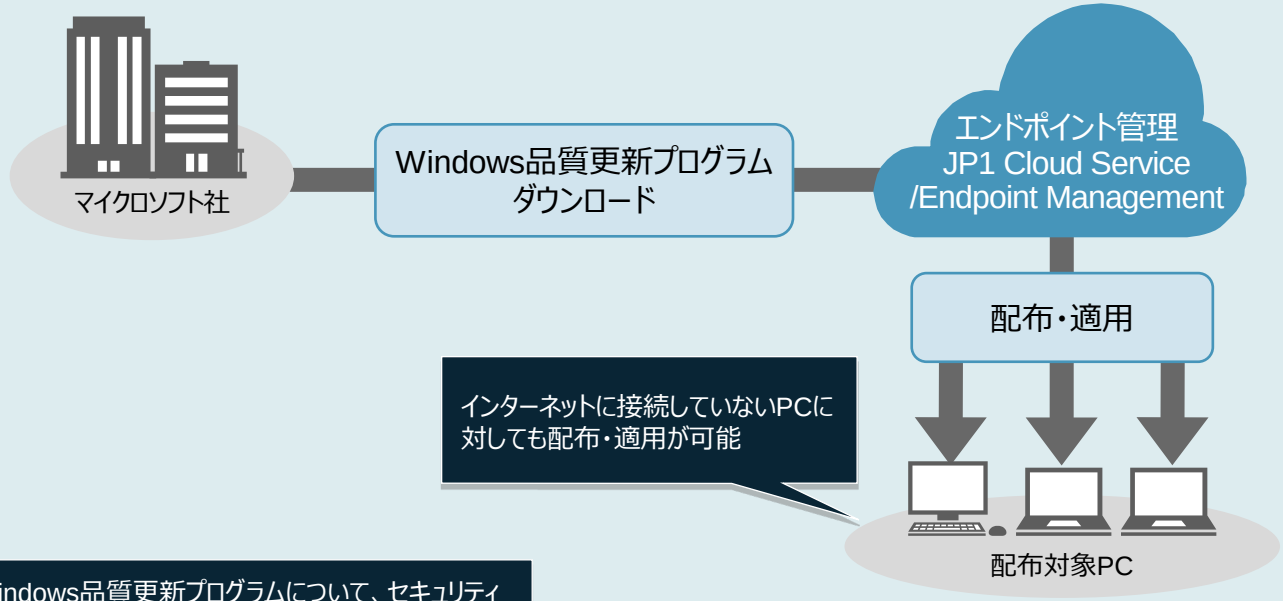


さらに　社内のPCへのWindows機能更新プログラムの適用状況は、CSVファイルに出力した一覧で容易に確認できます。

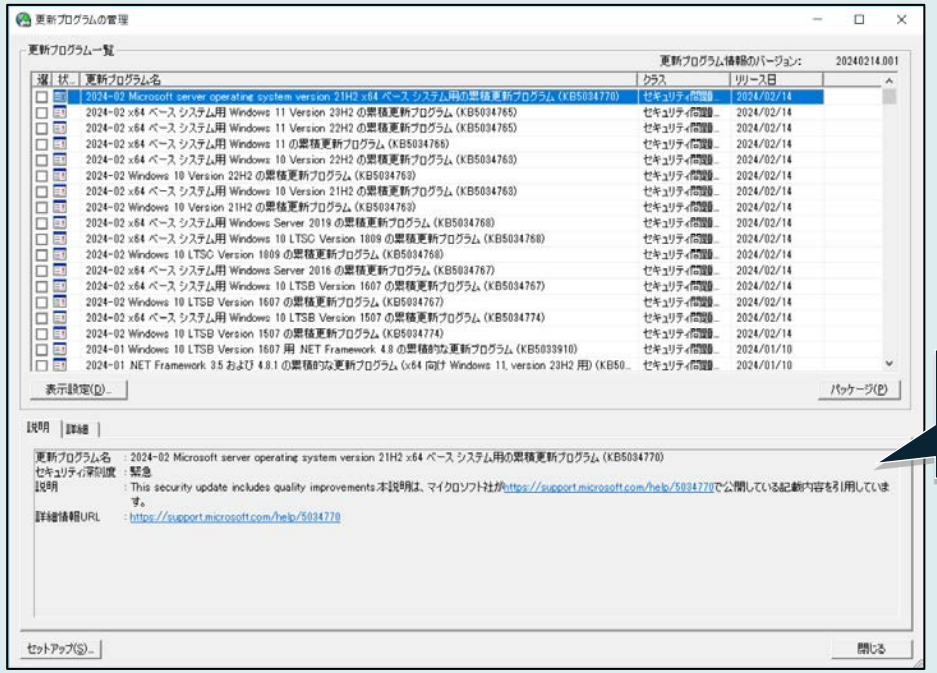
Windows品質更新プログラムの適用管理

HITACHI
Inspire the Next

自動でWindows品質更新プログラムを入手して、各PCに配布・適用できます。
緊急度が高く個別に適用したいWindows品質更新プログラムがある場合は、手動で配布・適用もできます。



更新プログラムの管理画面



各Windows品質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

新しいWindows品質更新プログラムが提供されると、更新プログラム一覧に自動で追加されます。
これにより、現在提供されているWindows品質更新プログラムを簡単に把握できます。

※ Windows品質更新プログラムを自動的に配布できるようになるには、Windows品質更新プログラムの提供から2週間ほどの期間が必要です。
※ 自動的に配布できるWindows品質更新プログラムは、重要な更新プログラムおよびセキュリティ更新プログラムです。サービスパック、Microsoft Officeなどのソフトウェアの更新プログラムは含まれません。

このようなお悩み、ありませんか？

HITACHI
Inspire the Next

☑ 社内のセキュリティリスクに対する対策状況を把握できていない。

セキュリティ対策の徹底 p. 23

「PCのセキュリティ対策状況のチェック」、「デバイスの利用制限・ネットワーク接続の制御」、「PC上のユーザー操作のログ取得」により、状況を把握してセキュリティ対策を徹底できます。

☑ ウイルス対策製品のバージョンが古くて危険なPCがあるかもしれない。

ウイルス対策の徹底 p. 26

セキュリティ対策ができているかを確認し、不備のあるPCにはメッセージの通知によって対策を促すことができます。
さらに、ウイルス対策製品のバージョンが古くて危険なPCには、新しいウイルス対策製品を配布・インストールできます。

☑ 個人所有のPCを持ち込んで、社内ネットワークに接続しているかもしれない。

セキュリティリスクがあるPCの接続防止 p. 27

管理対象ではないPCのネットワーク接続を拒否することができます。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することを防止できます。
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といった運用を自動化できます。

☑ USBメモリーによるデータの持ち出しが自由にできてしまう。

デバイスの利用制限 p. 28

USBメモリーなどデバイスの利用を部署や利用者ごとに許可・禁止したり、許可していないネットワークに接続した場合にPC操作を禁止したりして、不正なデータの持ち出しや利用による情報漏えいを防止できます。

☑ ネットワーク経由での情報漏えいが心配。

ネットワーク接続の制御 p. 30

社内ではWi-Fi制御により管理者が許可したアクセスポイントのみを表示、社外ではインターネット接続時に社内VPNへ接続を強制、といった制御により、不審なネットワークへの接続による情報漏えいを防止できます。

☑ 情報漏えいのリスクがある操作が日常的に行われているかもしれない。

操作ログの取得 p. 31

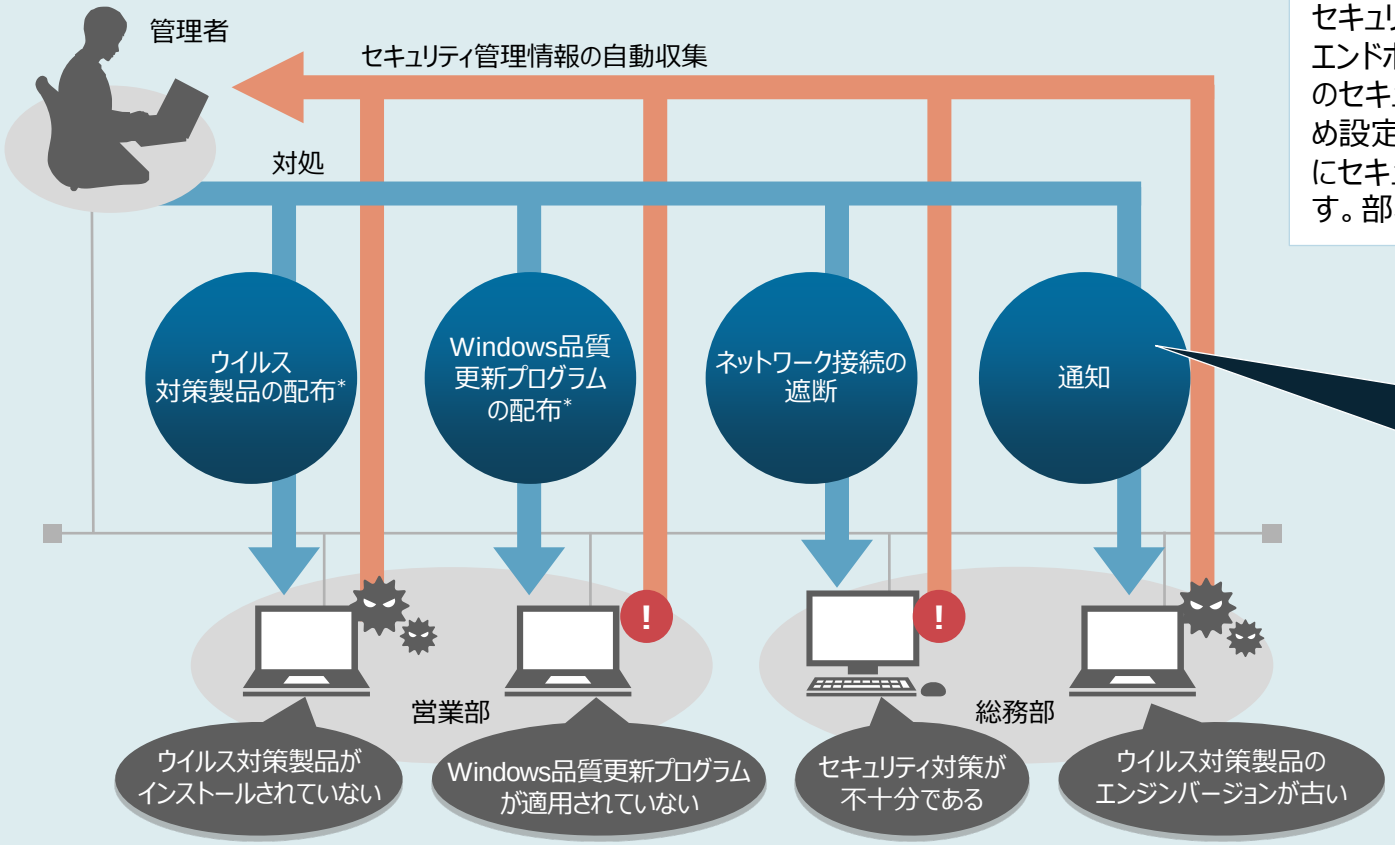
情報漏えいのリスクがある「社外Webサイトへのアップロード」「メール送信」「USBメモリーへのコピー」といった、PC上のユーザー操作をログとして取得できます。取得した操作ログを確認することで、不正なデータ持ち出しなど違反の検出が可能。また、ログ管理を周知することで不正行為の抑止効果も期待できます。

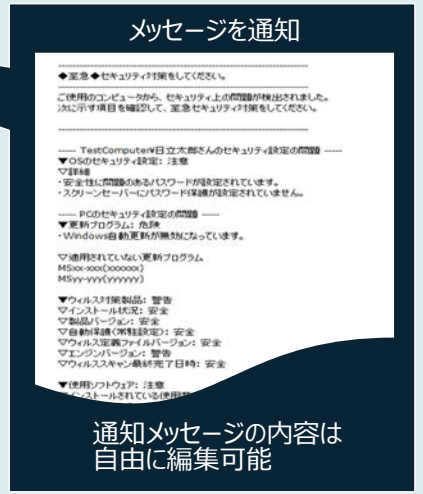
セキュリティ対策の徹底　【セキュリティ対策状況のチェック・対処】

HITACHI
Inspire the Next

各PCのセキュリティ対策状況をチェックできます。また、チェック結果に応じて対処できます。

例
- ●ウイルス対策製品や必須ソフトウェアを配布・インストールする
- ●最新のWindows品質更新プログラムが適用されているかどうかを確認し、適用する
- ●セキュリティ対策が不十分な場合、ネットワーク接続を遮断する
- ●対策要求をメッセージで通知する　など





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。エンドポイント管理 JP1 Cloud Service/Endpoint Management のセキュリティポリシーにはPCで対策する必要がある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。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。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。

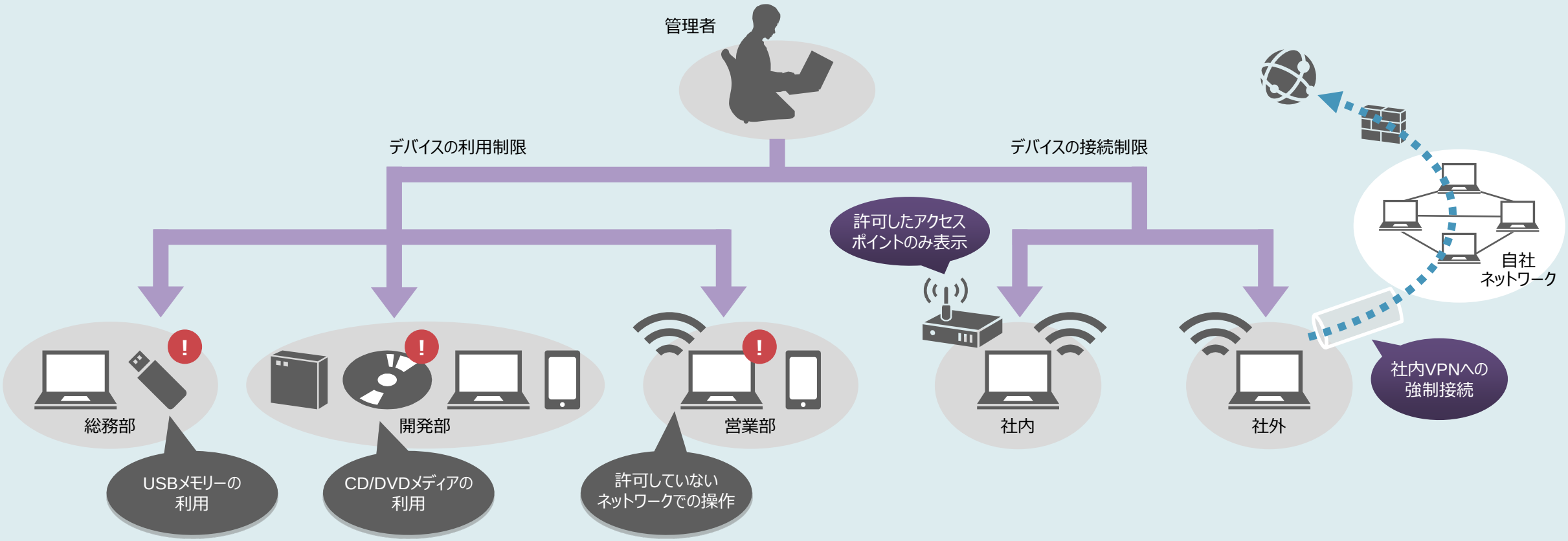
＊ スタンダードプランをご契約いただく必要があります。

セキュリティ対策の徹底　【情報漏えいの防止】

HITACHI
Inspire the Next

デバイスの利用やネットワーク接続を制御して、情報漏えいを防止できます。禁止操作を実行した場合には、ポップアップでメッセージを通知することもできます。

例
- ●USBメモリー、CD/DVDメディアの利用を抑止する
- ●許可していないネットワークでのPC操作を抑止する
- ●許可したアクセスポイントのみ表示する
- ●社外でのインターネット接続時に社内VPNへの接続を強制する　など

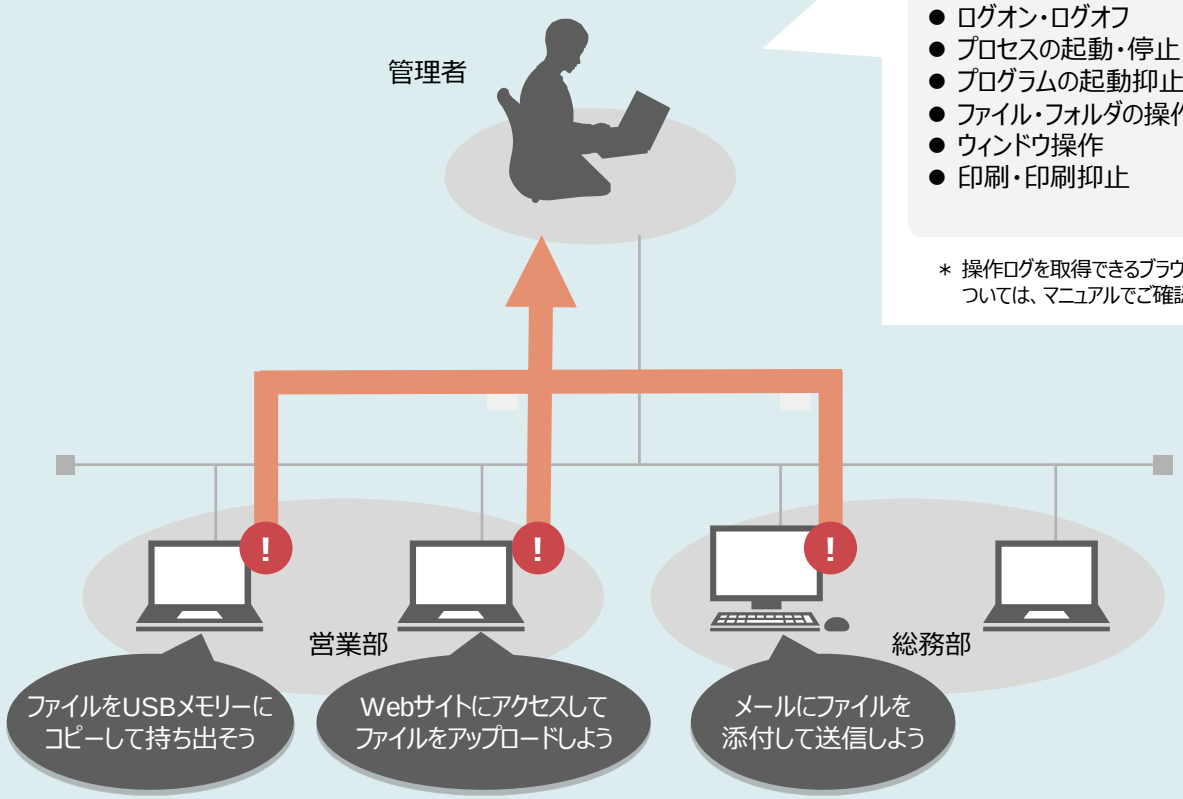


セキュリティ対策の徹底　【情報漏えいリスクの確認】

HITACHI
Inspire the Next

ファイルをPC外に持ち出そうとする操作など、PC上のさまざまなユーザー操作をログとして取得できます。

例
- ●ファイルをUSBメモリーにコピーして持ち出そうとする操作のログを取得する
- ●Webサイトにアクセスしてファイルをアップロードした操作のログを取得する
- ●メールにファイルを添付して送信した操作のログを取得する　など



取得できる操作ログ

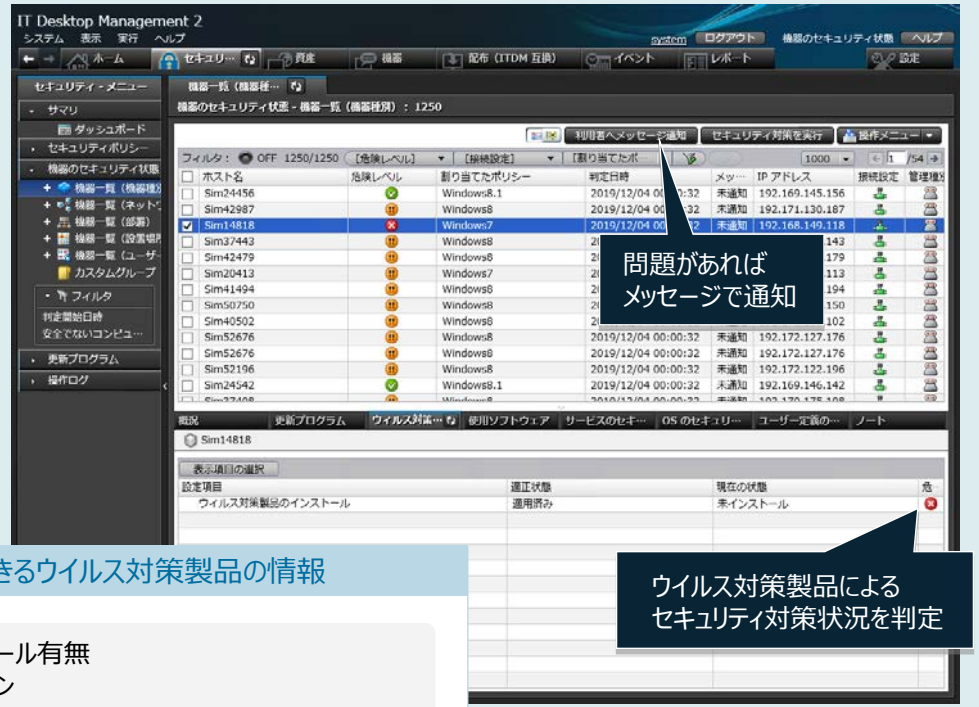
- PCの起動・停止
- ログオン・ログオフ
- プロセスの起動・停止
- プログラムの起動抑止
- ファイル・フォルダの操作
- ウィンドウ操作
- 印刷・印刷抑止
- 外部メディアの接続・切断
- 外部メディアの接続抑止
- Webアクセス・アップロード・ダウンロード*
- FTP送信・受信*
- 添付ファイル付きメールの送信・受信*
- メール添付ファイルの保存*
- クリップボード操作
- リモートデスクトップ接続
- ネットワーク接続・通信
- ドライブ追加・削除

＊ 操作ログを取得できるブラウザ（Microsoft Edge、Google ChromeおよびFirefox）およびメーラー（Outlookなど）については、マニュアルでご確認ください。

ウイルス対策の徹底

ウイルス対策製品によるセキュリティの対策状況に問題がないかどうかを確認し、ウイルス対策製品のバージョンが古いPCに最新バージョンを配布・インストールできます。

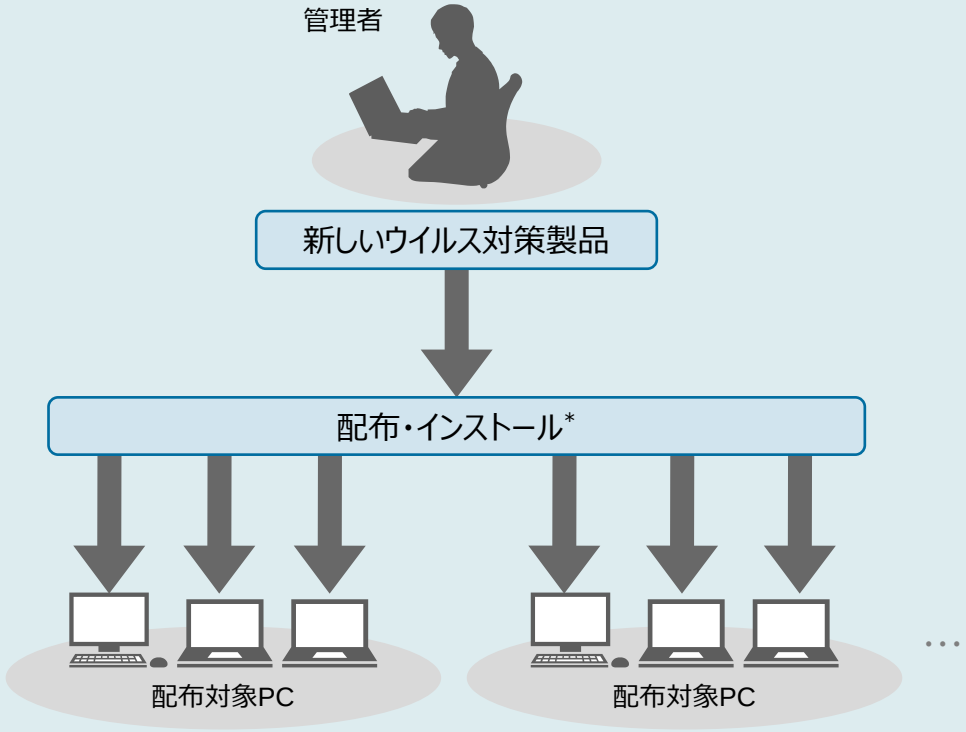
セキュリティ管理画面（機器一覧）



確認できるウイルス対策製品の情報

- 製品のインストール有無
- 製品のバージョン
- エンジンバージョン
- ウイルス定義ファイルのバージョン
- ウイルススキャンの最終完了日時　など

※ ウイルス対策製品によっては、収集できない情報もあります。
詳細はマニュアルをご確認ください。

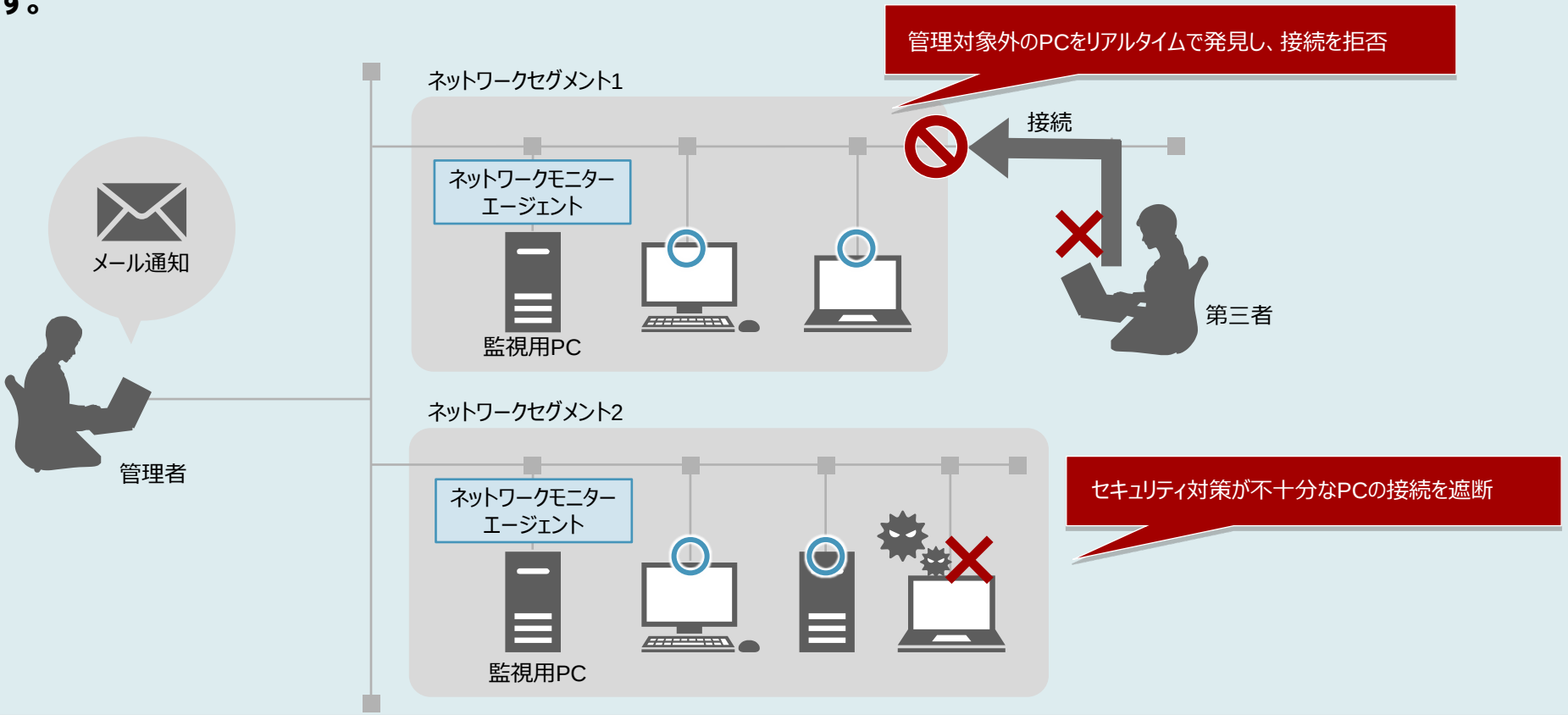


＊ スタンダードプランをご契約いただく必要があります。

ITDM: JP1/IT Desktop Management

セキュリティリスクがあるPCの接続防止

ネットワーク監視用のPCがあるネットワークセグメントに、管理対象外のPCを接続しようとすると、新しい機器として検知し、ネットワーク接続を拒否できます。また、セキュリティ対策が不十分なPCがある場合は、ネットワークへの接続を自動的に遮断できます。さらに、ネットワーク接続を拒否・遮断したことをメールで通知することもできます。



さらに

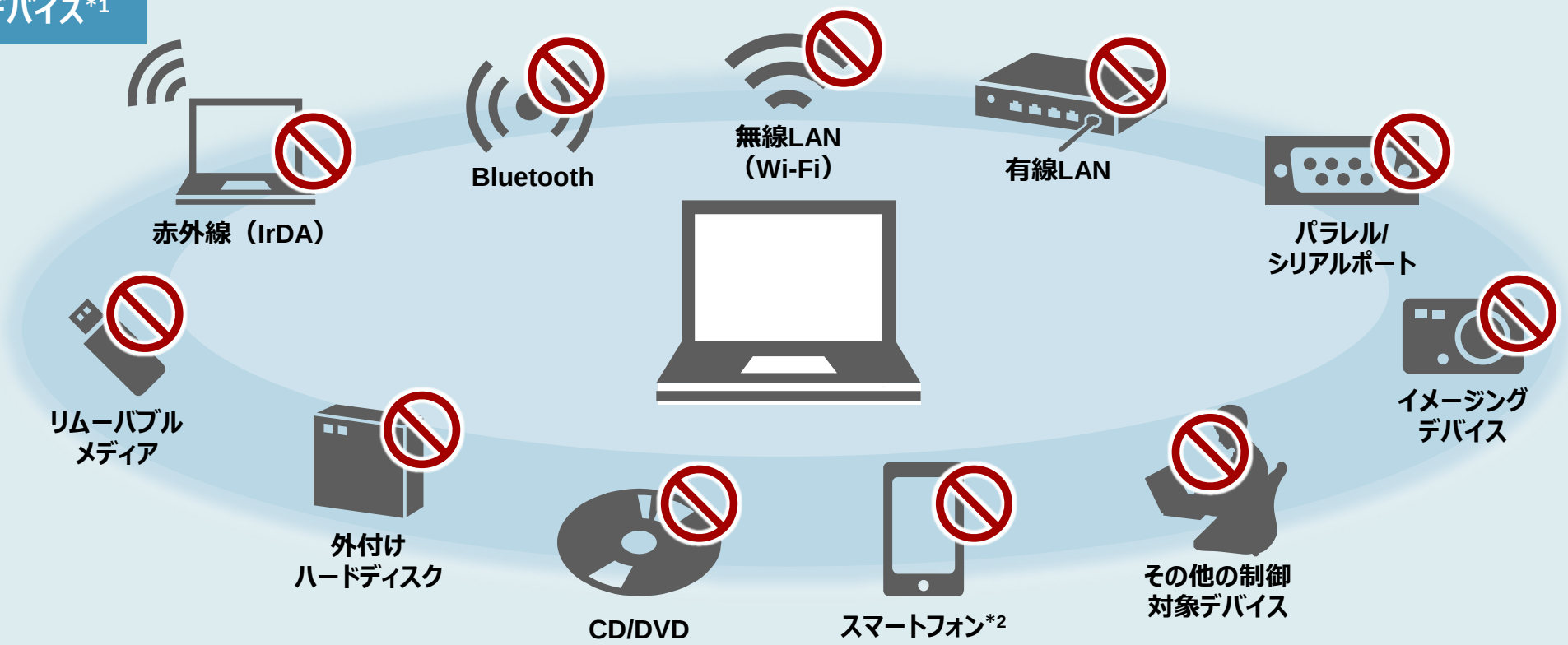
- セキュリティ対策が不十分なPCのネットワーク接続を遮断した場合、自動または手動でセキュリティ対策を実施したあとに再判定を行います。
  対策されたことが確認できると、自動的にネットワーク接続を許可します。
- 管理対象外のPCに対して、ネットワーク接続を拒否せずに、ネットワーク接続の検知だけ実施することもできます。

デバイスの利用制限【許可していない外部デバイスやネットワークの利用を禁止】

HITACHI
Inspire the Next

さまざまなデバイスの利用やネットワーク接続を制限することで、不正なデータの持ち出しによる情報漏えいを防ぎます。特定の機種のみ利用を許可することや、部署や利用者ごとに許可・禁止を設定できるため、お客さまの状況にあわせた柔軟な運用が可能です。

制限できるデバイス*1



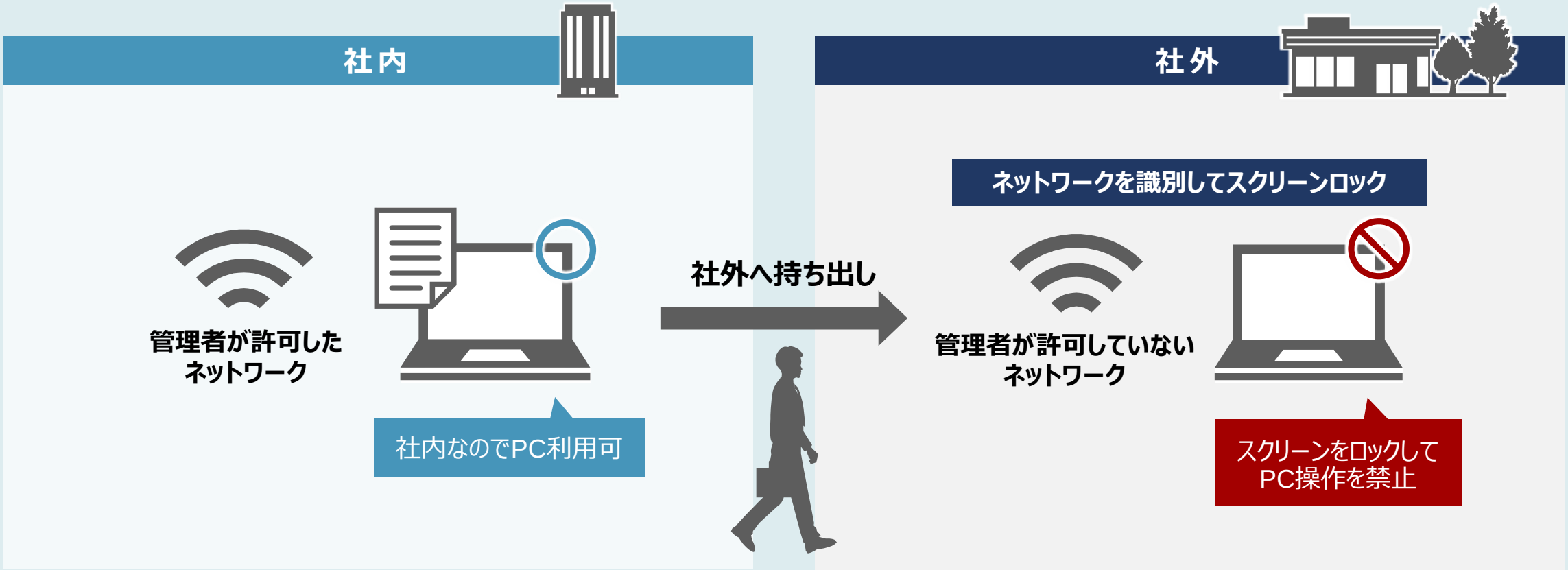
IrDA: Infrared Data Association

*1 キーボード、マウスなどのヒューマンインタフェースデバイスは対象外です。
*2 スマートフォンは、OS、製造メーカー、接続方法などの違いによって、さまざまなデバイスとして認識されます。
エンドポイント管理 JP1 Cloud Service/Endpoint Managementは、これらのすべてのデバイスを利用禁止にすることで、スマートフォンへのデータコピーを防止します。

デバイスの利用制限【ネットワーク識別によるスクリーンロック】

HITACHI
Inspire the Next

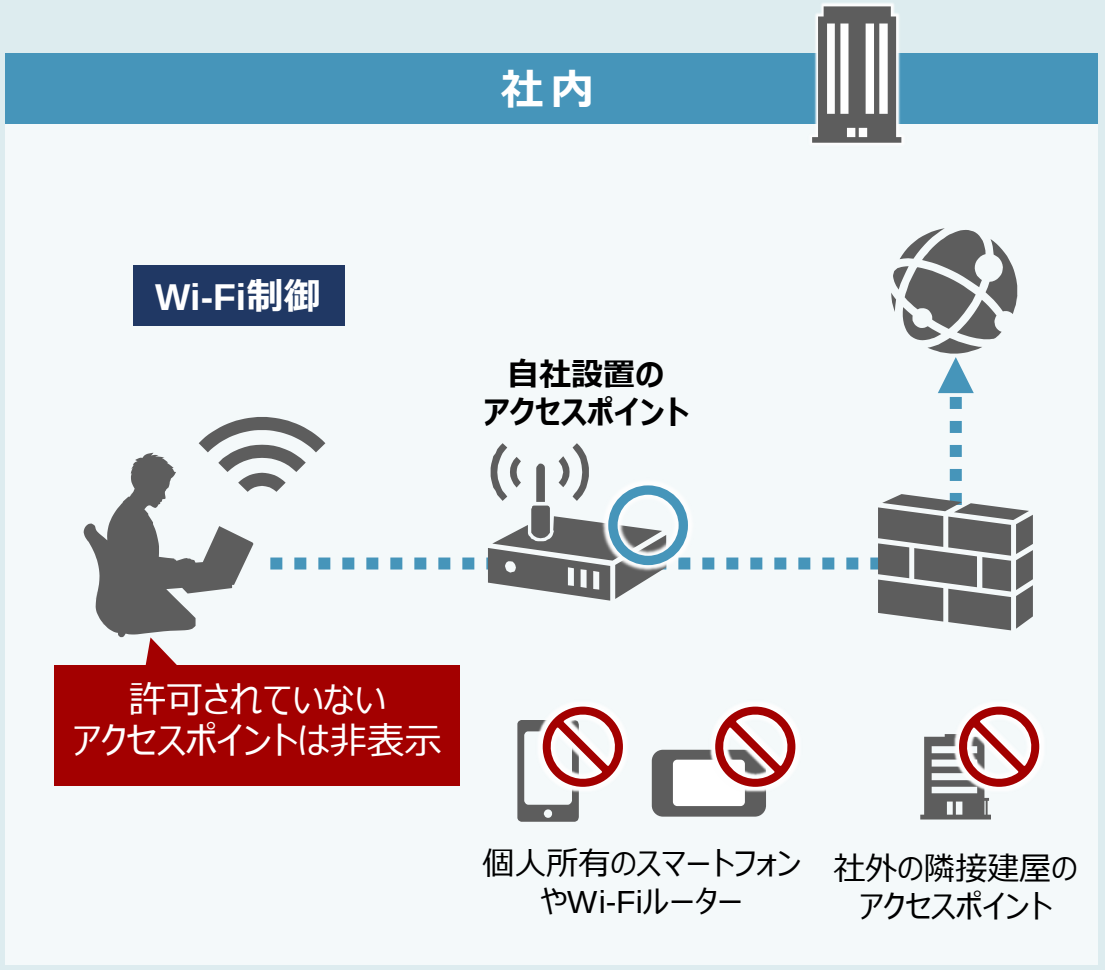
管理者が許可したネットワークに接続していない場合、スクリーンロックによりPC操作を禁止します。ノートPCなどを社外に持ち出しても、スクリーンロックにより不正なデータ利用が防止できます。

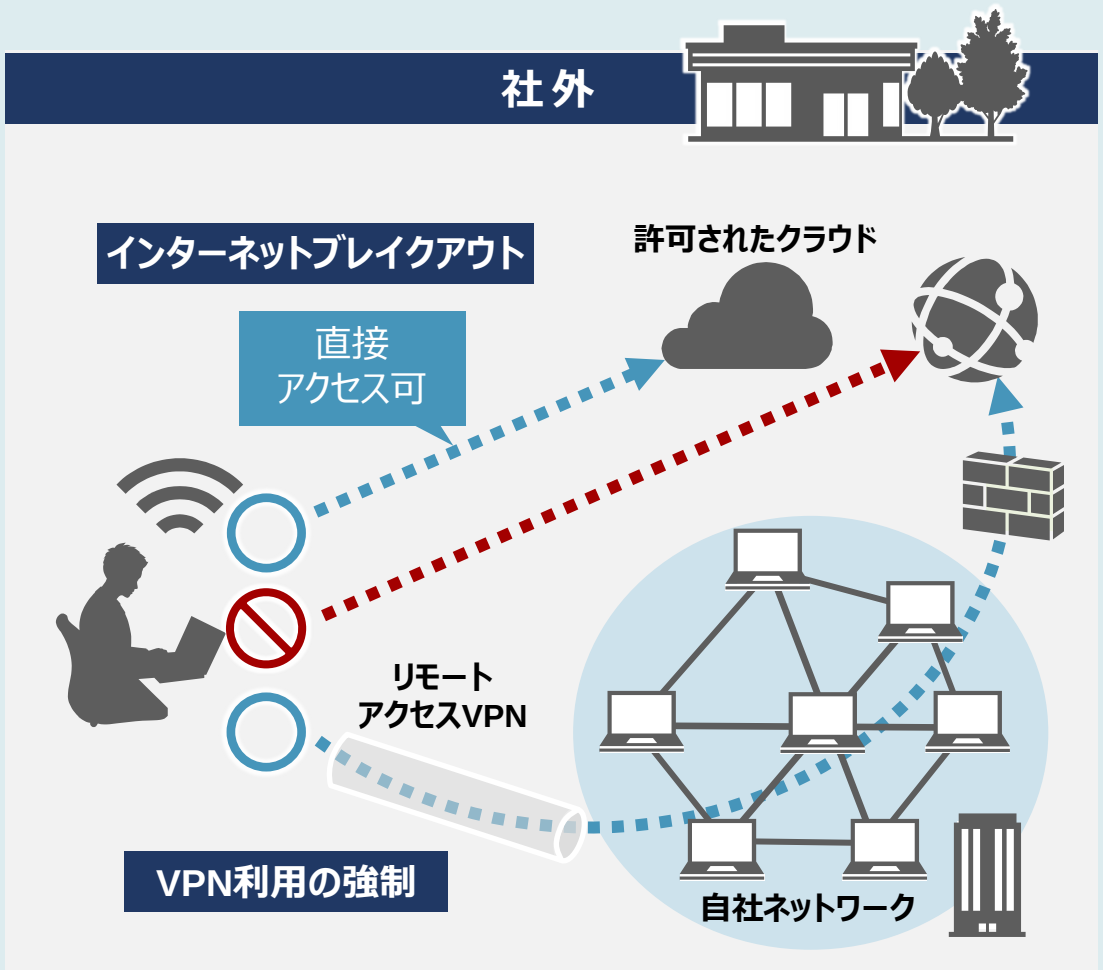


ネットワーク接続の制御

HITACHI
Inspire the Next

**社内ではWi-Fi制御により、管理者が許可したアクセスポイントのみを表示し、それ以外のアクセスポイント利用を禁止できます。
社外では、インターネット接続時に社内VPNへの接続を強制することで、安全性を確保します。許可されたクラウドサービスへの接続時は、
インターネットブレイクアウトを利用して直接アクセスできるようにすることで、クラウドサービスの快適な利用を実現します。**





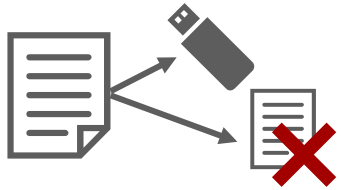
操作ログの取得　【情報漏えいのリスクがある操作を取得・管理】

HITACHI
Inspire the Next

PC上のさまざまなユーザー操作ログを取得できます。USBメモリーへのデータコピーといったファイル操作ログを確認することで、不正なデータ持ち出しなど違反の検出が可能。また、ログ管理を周知することで不正行為の抑止効果も期待できます。

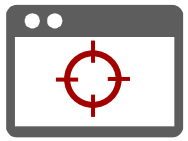
取得できる主なログ*

ファイル操作ログ



ブラウザ操作ログ

クリップボード操作ログ



アプリケーション操作ログ

リモートデスクトップ接続ログ

Windowsサインイン・サインアウトログ

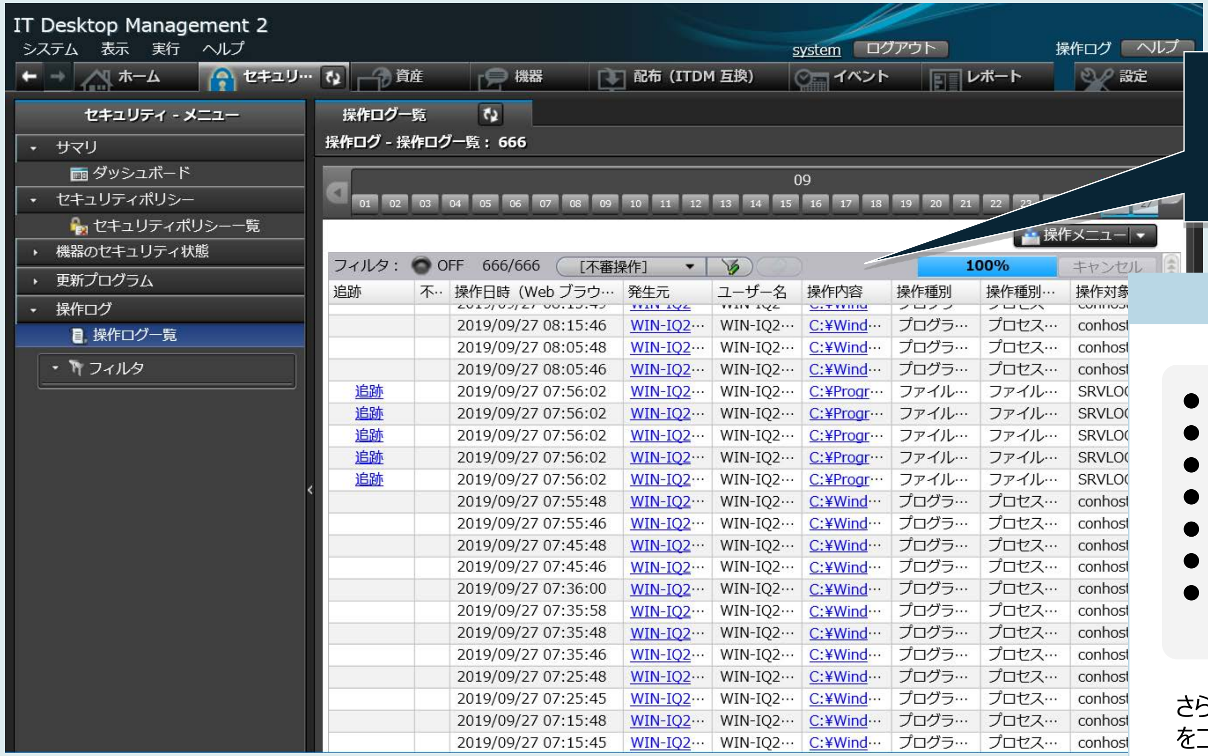
* 取得可能な操作ログの詳細についてはお問い合わせください。

操作ログの取得　【情報漏えいのリスクがある操作を絞り込み】

HITACHI
Inspire the Next

情報漏えいのリスクがある操作だけに絞り込むことで、効率よく操作ログを確認できます。

セキュリティ管理画面（操作ログ一覧）



操作ログ一覧画面のフィルタで、条件を指定

・ファイル名に「顧客」を含むファイルを操作したログ
・特定のPCの操作ログ　　など

取得できる操作ログ

- PCの起動・停止
- ログオン・ログオフ
- プロセスの起動・停止
- プログラムの起動抑止
- ファイル・フォルダの操作
- ウィンドウ操作
- 印刷・印刷抑止
- 外部メディアの接続・切断
- 外部メディアの接続抑止
- Webアクセス・アップロード・ダウンロード＊
- FTP送信・受信＊
- 添付ファイル付きメールの送信・受信＊
- メール添付ファイルの保存＊
- クリップボード操作
- リモートデスクトップ接続
- ネットワーク接続・通信
- ドライブ追加・削除

さらに、情報漏えいのリスクがある操作に絞ってログを取得できるので、ログを保存するデータベースの容量をコンパクトにできます。

＊ 操作ログを取得できるブラウザ（Microsoft Edge、Google ChromeおよびFirefox）およびメーラー（Outlookなど）については、マニュアルでご確認ください。

ITDM: JP1/IT Desktop Management

複数管理者での業務分担　【ユーザーごとに操作範囲を設定】

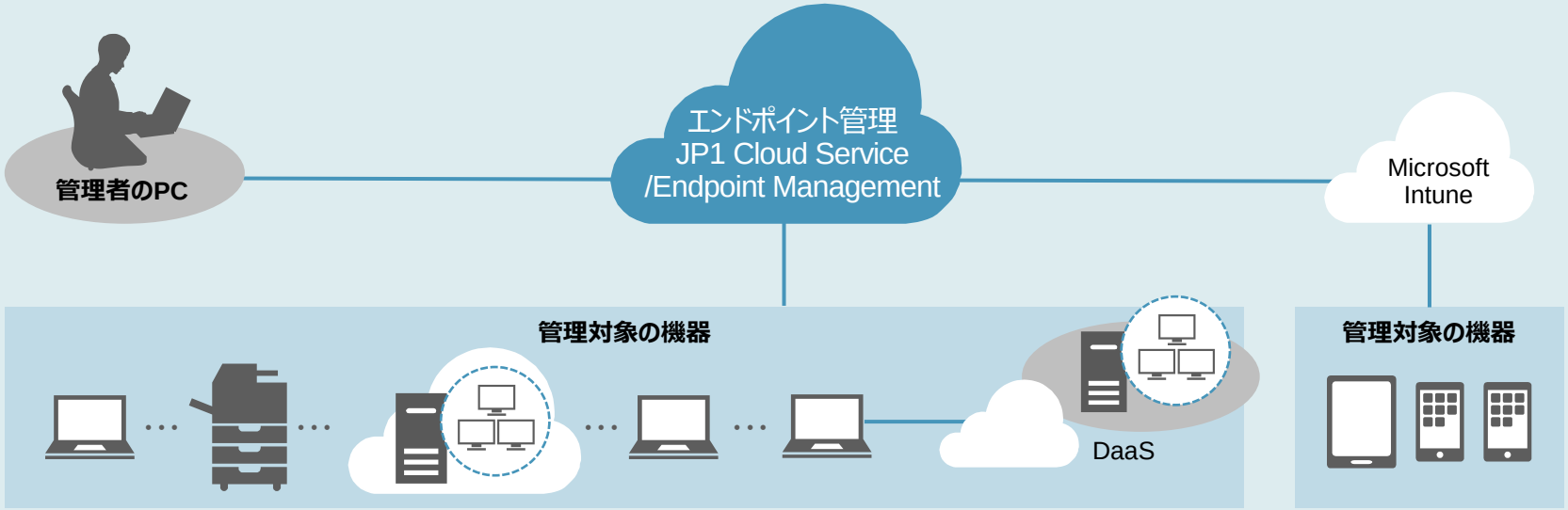
HITACHI
Inspire the Next

管理対象の機器が多い場合や、場所が離れている場合などに、複数人の管理者で業務を分担できます。管理する担当部署や担当業務に特化した専用画面で必要な情報を確認できるため、管理業務を効率的に行うことができます。
たとえば、とりまとめの管理者は全社の情報を、各拠点の管理者は担当する拠点のIT資産情報だけを参照・更新するといったように、操作範囲を限定した管理が可能です。

システム構成例とサービスメニュー

- システム構成例
- エンドポイント管理 JP1 Cloud Service/Endpoint Management メニュー

システム構成例



■管理者のPC

Webブラウザ（Microsoft EdgeまたはGoogle Chrome）がインストールされていることが前提です。

■管理対象の機器

【適用OS】
- Windows 11 / 10 / 8.1 / 8 / 7
- Windows Server 2022 / 2019 / 2016 / 2012 R2 / 2012 / 2008 R2
- macOS 13 / 12 / 11 / 10.15 / 10.14 / 10.13 / 10.12
- OS X 10.11 / 10.10
- Red Hat® Enterprise Linux® 9 / 8 / 7 / 6 / 5
- Oracle Linux 9 / 8 / 7 / 6
- CentOS 8 / 7 / 6
- AIX 7.3 / 7.2 / 7.1 / 6.1
- HP-UX 11iV3
- Solaris 11 / 10

【スマートデバイスの前提OS】
iOS、iPadOS、またはAndroid

DaaS: Desktop as a Service

※ スマートデバイスを管理する場合は、Microsoft Intuneが必要です。システム構成の詳細はマニュアルをご確認ください。

エンドポイント管理 JP1 Cloud Service/Endpoint Management メニュー

HITACHI
Inspire the Next

メニュー	説明
プラン＊1	
スタンダード＊2	エンドポイント管理の資産管理、配布管理、セキュリティ管理をご利用いただけます。
ライトA	エンドポイント管理の資産管理、配布管理をご利用いただけます。
ライトB＊2	エンドポイント管理の資産管理、セキュリティ管理をご利用いただけます。
オプション	
管理用中継サーバ追加オプション＊3	部門やネットワーク構成ごとに管理者を立てて運用し管理者の負荷を分散できる、管理用中継サーバ構成の環境をご利用いただけます。 JP1/IT Desktop Management 2での管理用中継サーバ構成のまま、エンドポイント管理 JP1 Cloud Service/Endpoint Management に移行したい場合は、このオプションをご利用ください。

＊1 管理対象1ノードごとに、本サービス1契約が必要です。新規に契約する場合、100ノード以上の契約が必要です。
＊2 最大過去180日分の操作ログをWebコンソールで閲覧いただけます。また、月に1回、CSV形式で操作ログデータをダウンロードいただけます。
＊3 管理用中継サーバの台数ごとに本サービスの契約が必要です。

価格については、当社担当営業にお問い合わせください。

HITACHI
Inspire the Next

システム運用を最適化するシステム運用管理SaaS

- エンドポイント管理をSaaSで提供
- 多様なシステム環境に対応
- 安定稼働・セキュリティへの取り組み
- JP1 Cloud Serviceへの効率的な移行を支援

エンドポイント管理をSaaSで提供

HITACHI
Inspire the Next

エンドポイント管理 JP1 Cloud Service/Endpoint Management は、豊富な実績があるIT資産管理ツール JP1/IT Desktop Management 2 - Manager の機能をSaaSで利用できるサービスです。さらに、JP1/秘文の豊富な機能を取り入れ、セキュリティ機能を強化しています。

JP1のSaaSのメリット	
機器購入・環境構築不要で初期コストを抑制 	● エンドポイント管理環境（管理用サーバ、インターネットゲートウェイ環境）の機器購入費用が不要、構築・保守の費用を低減 ● 端末の増設・廃棄に合わせて必要な分だけ利用
機器メンテナンス不要で本来業務に注力できる 	● エンドポイント管理環境（管理用サーバ、インターネットゲートウェイ環境）の稼働管理、維持保守（OSのパッチ適用、セキュリティ点検、バックアップ・復旧計画など）は日立が実施するため作業不要 ● お客さまは本来業務に注力可能
導入も簡単でスピーディー 	● 長年のシステム開発・運用で蓄積された日立の高度な技術やノウハウを活用できるため、独自で導入・運用するよりもスピーディーに高信頼・高効率な運用管理システムを利用可能 ● 契約から約1か月で利用可能

多様なシステム環境に対応

HITACHI
Inspire the Next

お客さまの環境に合わせて、必要なものを無駄なく選べます。

必要な機能に合わせてプランを選択できる

ケース1

- エンドポイントのIT資産管理、セキュリティリスクの管理と対策をまとめて実施できるようにしたい

プラン：スタンダード

- 資産管理
- 配布管理
- セキュリティ管理

ケース2

- Microsoft Intuneで端末を管理しているが、ソフトウェアの配布はきめ細かく制御したい
- 操作ログの取得・管理は不要

プラン：ライトA

- 資産管理
- 配布管理

ケース3

- Microsoft Intuneで端末を管理しているが、操作ログを取得して管理したい
- きめ細かい配布制御は不要

プラン：ライトB

- 資産管理
- セキュリティ管理

安定稼働・セキュリティへの取り組み

HITACHI
Inspire the Next

基幹システムの運用管理基盤としてもご利用いただけるよう、
安定稼働・セキュリティへの取り組みを実施しています。

セキュリティ確保のための予防保守

- セキュリティ脆弱性の定期点検
- サービスで使用するOSやソフトウェアに関連する脆弱性情報の監視
- サービスで使用するOSへのパッチ適用
- サービスで使用するソフトウェアのアップデート

サービスで使用するクラウド環境の稼働監視／リソース監視

- 異常検知時の通知および復旧

サービスで使用するソフトウェアの稼働監視

- 異常検知時の通知および復旧

ログおよびデータの管理

- バックアップ、復旧計画
- DBメンテナンス

JP1 Cloud Serviceへの効率的な移行を支援

HITACHI
Inspire the Next

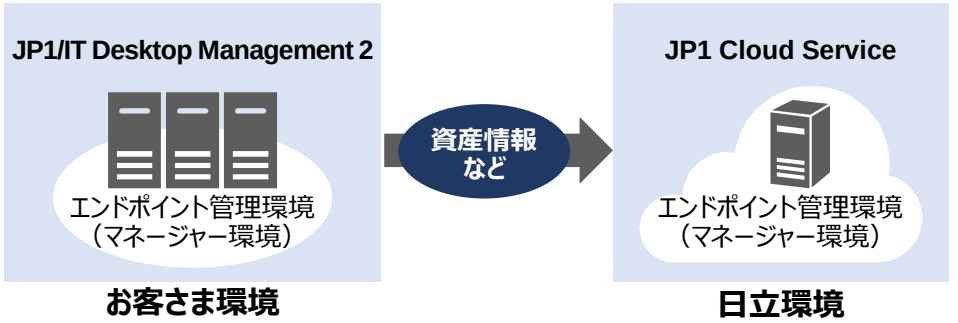
JP1のプロフェッショナルの支援により、JP1 Cloud Serviceへ効率的に移行できます。

JP1/IT Desktop Management 2や他社製品・サービスからのスムーズな移行を支援します。

JP1/IT Desktop Management 2 からの移行

保有資産を生かして移行

お客さまの保有している資産情報などをJP1 Cloud Serviceのエンドポイント管理環境（マネージャー環境）に移行して使用できるようにします。
経験豊富なJP1のプロフェッショナルが、移行のためのコンサルティングやアセスメントを実施し、スピーディーな移行を支援します。



他社製品・サービスからの移行

課題を明確にしてスピーディーに移行

お客さまのIT資産管理運用の現状を把握・分析してJP1 Cloud Serviceへ移行する場合の課題を明確にします。経験豊富なJP1のプロフェッショナルが、移行のためのコンサルティングやアセスメントを実施し、お客さまがお使いの製品やサービスからのスピーディーな移行を支援します。

※ JP1のプロフェッショナルは、JP1技術者資格認定制度に基づいて認定された、JP1の一定以上のスキルを有する技術者です。
※ JP1 Cloud Serviceへの移行は、JP1 Cloud Serviceの技術支援サービスでご支援します。

機能一覧

■ 機能一覧

機能一覧（1/3）

HITACHI
Inspire the Next

カテゴリ	分類	項目
資産管理	ハードウェア資産の管理	・資産情報（追加・編集・削除、状態変更、棚卸日の更新、追加管理項目、CSVファイルのインポート／エクスポートなど） ・契約情報 ・関連資産（ディスプレイ、ハードディスク、プリンタ、USBデバイスなど） ・機器情報（定期的な自動収集）
	ソフトウェアライセンスの管理	・ソフトウェアライセンス情報（追加・編集・削除、状態変更、棚卸日の更新、CSVファイルのインポート／エクスポートなど） ・契約情報 ・割り当てコンピュータ
	ソフトウェアの管理	・管理ソフトウェア情報（追加・編集・削除、CSVファイルのインポート／エクスポートなど） ・インストール済みソフトウェア* ・インストール済みコンピュータ* ・ライセンスを割り当て済みのコンピュータ ・ソフトウェアライセンス * Windowsストアアプリをインストールしている場合も把握できます。
	USBデバイスの管理	・許可したUSBデバイス以外の使用抑止 ・特定PCでのUSBデバイスの使用抑止 ・USBデバイスの使用履歴確認 ・USBデバイスの格納ファイル情報確認
	契約	・契約情報（追加・編集・削除、状態変更、CSVファイルのインポート／エクスポートなど） ・契約情報に対応するソフトウェア ・契約情報に対応するハードウェア
	資産情報の確認	■ダッシュボード ・ハードウェア資産の推移 ・ハードウェア資産台数（フィルタ、カスタムグループごとの表示） ・ソフトウェアライセンスの残数が少ないソフトウェア（100件まで） ・3か月以内に期限が切れる契約の情報
	機器状況の確認	■ダッシュボード ・観点ごとの機器台数（フィルタ、カスタムグループごとの表示） ・OSごとの機器台数 ・新規発見ソフトウェア ・管理対象の機器の推移（エージェントの導入状態ごとに表示）

カテゴリ	分類	項目
資産管理	機器情報	・システム情報 （コンピュータ名、シリアルナンバー、CPU、メモリー、空き容量、最終ログオンユーザー名、OSとサービスパック、IPアドレス、ドメインなど） ・ハードウェア情報（CPU、メモリー、ディスクドライブなどの情報） ・インストールソフトウェア情報（ソフトウェアおよびWindowsストアアプリの名称、バージョン、インストール日付、Microsoft Office製品のプロダクトIDや購入形態などの情報） ・セキュリティ情報（更新プログラム情報、ウイルス対策製品情報、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） ・機器情報の変更履歴の取得と保管
	ソフトウェア情報	・インストール済みコンピュータの一覧* ・SAMAC ソフトウェア辞書によるソフトウェア種別（有償ソフトウェア・フリーソフトウェア）の取得 * Windowsストアアプリをインストールしている場合も把握できます。
	機器情報・ソフトウェア情報の収集	・定期的な自動収集 ・最新情報の収集 ・オフライン管理のコンピュータからの機器情報の収集 ・CSVファイルへのエクスポート
	リモートコントロール	・キーボードやマウスの操作 ・CD-ROMやDVD-ROMを利用したリモートメンテナンス* ・ファイルの送信／受信 ・転送データの暗号化／ファイルへのアクセス権の設定 ・複数コンピュータへの一括転送 ・コンピュータからコントローラへの接続要求 ・リモートコントロールの録画・再生 ・チャットの利用 ・シャットダウンと再起動の実行 ・クリップボードの転送 * 接続先PCがAMTの場合に利用できます。対応バージョンについては、マニュアルでご確認ください。
	スマートデバイス管理*	・概況確認（スマートデバイスの状態HDDの使用状況や空き容量など） ・端末の制御（スマートデバイスのロック、初期化） * Microsoft Intuneが必要です。

カテゴリ	分類	項目
配布管理	配布タスク	・インストールソフトウェア* ・ファイル ・更新プログラム ・インストールソフトウェアのアンインストール* * インストールおよびアンインストールできるソフトウェアの条件については、マニュアルでご確認ください。
	実行スケジュールの指定	・指定した日時 ・ユーザーログイン時 ・次回起動時 ・コンピュータ自動起動 ・新規に追加した機器への自動配布
	配布・インストールの実行	・実行前メッセージ／実行後メッセージ ・ネットワークの空き状況に応じて転送間隔を制御 ・セキュリティポリシーに従った配布タスクの実行 ・グルーピングした配布先への配布・インストール ・優先度をつけた配布・インストール ・オフラインPCへのソフトウェアの配布・インストール ・利用者によるインストール（PULL配布）
	インストール条件の設定	・システム条件（HDDの空き容量、実装メモリーのチェック） ・ソフトウェア条件（前提ソフトウェアとそのバージョンのチェック） ・インストール方法（GUIまたはバックグラウンド） ・インストール後のPC再起動 ・処理中ダイアログの表示／非表示設定 ・インストール直前・直後・エラー時のアクション設定 ・会社名、所有者名などの情報設定 ・スクリプトファイルによるインストール処理の応答
	ネットワーク負荷の分散	・配布の流量制御 ・中継システムの設置 ・パッケージの分割配布 ・マルチキャスト配布
	品質更新プログラム	更新プログラム一覧の表示、更新プログラム情報の自動取得、更新プログラムのパッケージ作成

機能一覧（2/3）

カテゴリ	分類	項目
セキュリティ管理	セキュリティポリシーの作成支援	・デフォルトポリシー（セキュリティのチェック） ・推奨ポリシー（セキュリティの強化）
		セキュリティポリシーの編集
	セキュリティポリシーの内容	■更新プログラムの判定 ・自動更新の有効/無効が規定に従っているかのチェック ・適用すべき品質更新プログラム、機能更新プログラムが適用されているかのチェック
		■ウイルス対策製品の判定 ・ウイルス対策製品のチェック（製品およびエンジンバージョン、定義ファイルバージョン、常駐設定、最終ウイルススキャン完了日など）
		■使用ソフトウェアの判定 ・使用禁止のソフトウェアやWindowsストアアプリがインストールされていないかのチェック ・必須のソフトウェアやWindowsストアアプリがインストールされているかのチェック
		■サービスのセキュリティ設定の判定 ・禁止サービスが稼働していないかのチェック
		■OSのセキュリティ設定の判定 ・有効なGuestアカウントがないかのチェック ・脆弱なパスワード設定のアカウントがないかのチェック ・無期限パスワード設定のアカウントがないかのチェック ・パスワードの更新経過日数が、指定した日数を超えていないかのチェック ・自動ログオンが設定されていないかのチェック ・パワーオンパスワードの設定がされているかのチェック ・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のチェック ・スクリーンセーバーの起動時間が、指定した時間以内であるかのチェック ・共有フォルダが設定されていないかのチェック ・管理共有が設定されていないかのチェック ・制限なしの匿名接続が設定されていないかのチェック ・ファイアウォールが無効になっていないかのチェック ・DCOMが有効になっていないかのチェック ・リモートデスクトップが有効になっていないかのチェック
		■任意機器項目のユーザー定義による監視
セキュリティ管理	セキュリティポリシーの内容	■印刷抑止の設定 ・印刷操作の抑止 ・印刷操作をパスワードで保護 ■機器の操作抑止の設定 ・USBデバイスの使用の抑止（登録済みのUSBデバイスは使用を許可、未登録のUSBデバイスは読み込み・持ち出し禁止/書き込みのみ禁止） ・フラッシュメモリ/メモリスティック/スマートメディアの使用の抑止 ・内蔵CD/DVDドライブの使用の抑止 ・内蔵FDドライブの使用の抑止 ・IEEE1394デバイスの使用の抑止 ・内蔵SDカードの使用の抑止 ・赤外線（IrDA）の使用の抑止 ・Bluetoothの使用の抑止 ・有線LAN、無線LANの使用の抑止 ・Windowsポータブルデバイスの使用の抑止 ・イメージングデバイスの使用の抑止 ・内蔵ハードディスクの使用の抑止 ・外付けハードディスクの使用の抑止 ■ソフトウェア起動抑止の設定 ・指定したソフトウェアの起動抑止 （例外許可ユーザー、および許可時間の設定が可能）
		■操作ログの設定 ・操作ログの取得 （PCの起動・停止、ログオン・ログオフ、プロセスの起動・停止、ファイル・フォルダ操作、印刷、外部メディアの接続・切断、ウィンドウ操作、プログラム起動抑止、印刷抑止、外部メディア接続抑止、Webアクセス・アップロード・ダウンロード*、FTP送信・受信*、添付ファイル付きメールの送信・受信*、メール添付ファイルの保存*、クリップボード操作、リモートデスクトップ接続、ネットワーク接続・通信、ドライブ追加・削除） ・不審操作に限定した操作ログの取得 * 操作ログを取得できるブラウザ（Microsoft Edge、Google ChromeおよびFirefox）およびメーラー（Outlookなど）については、マニュアルでご確認ください。
セキュリティ管理	セキュリティポリシーの割り当て方法	・デフォルトポリシーの自動割り当て ・グループ単位での個別割り当て ・PCごとの個別割り当て
	セキュリティポリシー違反時の動作	・利用者へのメッセージ通知 ・ネットワーク接続の制御 ・セキュリティ設定の強制変更 ・操作抑止 ・抑止操作ログの取得
	セキュリティポリシーの自動更新	・ウイルス定義ファイルが最新かどうかの自動チェック ・更新プログラムが最新かどうかの自動チェック
	セキュリティ状況の確認	■ダッシュボード ・危険レベルごとの機器台数（安全／注意／警告／危険の4段階表示） ・カテゴリごとのセキュリティ評価（セキュリティ状況をレベルA～Eで評価） ・ポリシーごとのセキュリティ状況 ・不審操作の状況
		セキュリティポリシー一覧、機器のセキュリティ状態の表示
	セキュリティリスクがあるPCの接続防止	・新規にネットワークに接続された機器の検知（接続許可／接続拒否） ・ネットワークセグメントごとの接続制御 ・機器ごとの接続制御 ・遮断機器から特定機器への接続許可 ・セキュリティ対策済みPCの接続許可
	デバイスの利用制限	・デバイス（リムーバブルメディア、赤外線（IrDA）、Bluetooth、無線LAN（Wi-Fi）、有線LAN、パラレル/シリアルポート、イメージングデバイス、外付けハードディスク、CD/DVD、スマートフォン、その他の制御対象デバイス）の利用制限 ・ネットワーク識別によるスクリーンロック
	ネットワーク接続の制御	・接続先Wi-Fiの制御 ・VPN利用の強制 ・インターネットブレイクアウトの利用
	操作ログ	操作ログ一覧の表示、操作ログの追跡

機能一覧（3/3）

HITACHI
Inspire the Next

カテゴリ	分類	項目
導入	導入支援	・ウィザード形式での導入支援 ・エージェントのPUSH配信（リモートインストール）* * エージェントをPUSH配信する場合の条件については、マニュアルでご確認ください。
	導入時の現状把握	・ホーム画面 ・現状セキュリティ診断レポート
運用	運用支援	ホーム画面（前日比で変化を把握、19種類のパネルから専用のホーム画面を構成）
		新規接続機器の発見
		エージェントレスでの運用* * エージェントレスで運用する場合の条件や利用できる機能については、マニュアルでご確認ください。
	イベント表示	・機器イベント（ハードウェアやソフトウェアの追加、セキュリティ設定の変更など） ・セキュリティイベント（セキュリティ判定、禁止操作の抑止など） ・資産イベント（資産の登録、ソフトウェアライセンスの追加など） ・配布イベント（ファイルの配布、ソフトウェアのインストール） ・設定イベント（機器の発見、エージェントの配信など） ・不審操作イベント ・エラーイベント（エラー情報）
レポート	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	■セキュリティレベルの5段階評価、前月比、説明、トピックなど ・現状セキュリティ診断 ・期間指定セキュリティ診断

カテゴリ	分類	項目
レポート	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） ・ウイ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）15.38 ・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）
	レポート出力支援	CSVファイル出力
		集計範囲の指定 （部署、機器種別、設置場所、ネットワーク、セキュリティポリシー）

カテゴリ	分類	項目
便利な機能	–	・電源ON・OFF制御* ・管理者へのイベントメール通知 ・利用者への任意のメッセージ通知 ・セキュリティ設定の強制変更 ・VPNクライアントの一括設定 ・ソフトウェアライセンスの移管 ・パスワードによるエージェント設定の保護 * 電源ONには、Wake on LANまたはAMTを利用
その他	Active Directoryとの連携	機器情報の取り込み
	仮想化対応	・Windows Server 2019 Hyper-V ・Windows Server 2016 Hyper-V ・Windows Server 2012 Hyper-V ・Windows Server 2012 R2 Hyper-V ・Windows Server 2008 R2 Hyper-V ・VMware ESX ・VMware ESXi ・VMware Horizon View ・日立サーバ論理分割機構 ・Citrix Virtual Apps and Desktops ・Citrix Virtual Apps ・Citrix Virtual Desktops ・Citrix XenDesktop ・Citrix XenApp ・Microsoft Remote Desktop Services ・Azure ・Azure Virtual Desktop ・Amazon Elastic Compute Cloud (Amazon EC2) ・Amazon WorkSpaces
	–	・管理用中継サーバによる管理の分散、階層化

他社商品名、商標等の引用に関する表示

本資料で紹介する JP1/IT Desktop Management 2 とは、JP1/IT Desktop Management 2 - Manager、JP1/IT Desktop Management 2 - Additional License for Linux
および JP1/IT Desktop Management 2 - Operations Director の総称です。
本サービスには、一般社団法人 IT資産管理評価認定協会が著作権を有している部分が含まれています。
TMEng.dllの著作権、特許権または商標権等の知的財産権は、トレンドマイクロ株式会社へ独占的に帰属します。

- Adobeは、米国およびその他の国におけるAdobe社の登録商標または商標です。
- AIX は、世界の多くの国で登録された International Business Machines Corporation の商標です。
- Amazon Web Services、AWS、Powered by AWS ロゴ、および Amazon Elastic Compute Cloud (Amazon EC2) は、Amazon.com, Inc. またはその関連会社の商標です。
- Bluetooth® ワードマークおよびロゴは登録商標であり、Bluetooth SIG, Inc. が所有権を有します。
- iPadOS、macOS、および OS X は、米国およびその他の国で登録されたApple Inc.の商標です。
- Linuxは、Linus Torvalds氏の米国およびその他の国における登録商標です。
- Microsoft、Access、Azure、Hyper-V、Microsoft Edge、Microsoft Intune、Outlook、Visual Basic、Visual C++、Windows、および Windows Server は、マイクロソフト 企業グループの商標です。
- Oracle®、Java、MySQLおよびNetSuiteは、Oracle、その子会社および関連会社の米国およびその他の国における登録商標です。
- Red Hat, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the United States and other countries.
- インテルは、Intel Corporation またはその子会社の商標です。
- 本書に記載されているCitrix®、Citrixロゴ、およびその他のマークは、Citrix Systems, Inc.および/またはその1つ以上の子会社の商標であり、米国の特許商標庁および他の国において登録されている場合があります。
- その他記載の会社名、商品名は、それぞれの会社の商標または登録商標です。

●本カタログで紹介するエンドポイント管理 JP1 Cloud Service/Endpoint Management は、日本でのみ販売しているサービスです。
●記載の仕様は、改良などのため予告なく変更することがあります。
●掲載している画面イメージは、実際の画面の色調とは異なる場合があります。
●マイクロソフト製品のスクリーンショットは、マイクロソフトの許諾を得て使用しています。
●掲載している単位表記は、1KB（キロバイト）＝1,024バイト、1MB（メガバイト）＝1,048,576バイト、1GB（ギガバイト）＝1,073,741,824バイト、
1TB（テラバイト）＝1,099,511,627,776バイトです。
●輸出される場合には、外国為替および外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。
なお、ご不明な場合は、当社担当営業にお問い合わせください。
●JP1 Webサイトで最新情報をご確認ください。

HITACHI
Inspire the Next

END

統合システム運用管理

エンドポイント管理

エンドポイント管理 JP1 Cloud Service/Endpoint Managementのご紹介

～エンドポイントを適切に管理し、セキュリティリスクから守る～

株式会社 日立製作所

GSA26j-01 | 2024.4