

Fujitsu Software

システムウォーカー デスクトップ ナビ

Systemwalker Desktop Navi

製品ご紹介資料

2023年7月

富士通株式会社



1. 製品コンセプト・特長

- 端末運用における環境変化
- 端末運用における今後の対策
- Systemwalker Desktop Navi とは
- CAPDo運用サイクルとは
- 製品特長 (1)
- 製品特長 (2)
- 製品特長 (3)

端末運用における環境変化

企業の管理対象となる端末は、『スマートフォンやタブレット等のビジネス利用普及に伴う多様化』、『ワークスタイル変革やグローバル化に伴う利用ロケーションの拡大』など、従来と比較して様々な環境変化が起こり続けています。

	従来	現状	
管理対象 (デバイス)	・Windows PC 	・Android™タブレット/スマートフォン ・iPad/iPhone 	多様化 (マルチデバイス)
調達	・情シスによる一括調達 	・現場による調達 ・海外拠点による現地調達 	調達一元化 困難
ロケーション	・社内 	・社外 (ワークスタイル) ・海外拠点 	ロケーション 拡大
セキュリティ マネジメント	・ウィルス感染 	・情報漏えい (内部犯行) ・サイバー攻撃 (外部犯行) 	対策予測 不可
デバイス 利用用途	・情シスによる限定した 利用用途 	・現場部門による柔軟な 利用用途 	利用用途 拡大

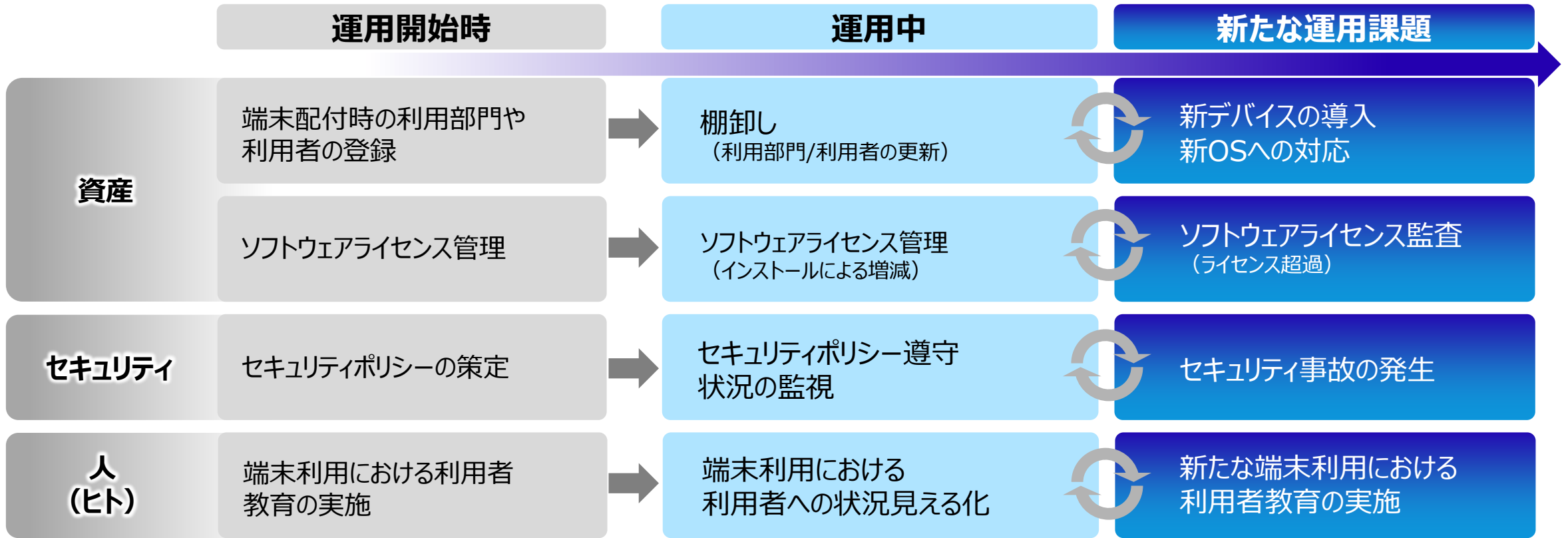


端末運用が多様化・複雑化

「外部の環境変化」と「内部の利用用途」への柔軟な運用対応が必要

端末運用における今後の対策

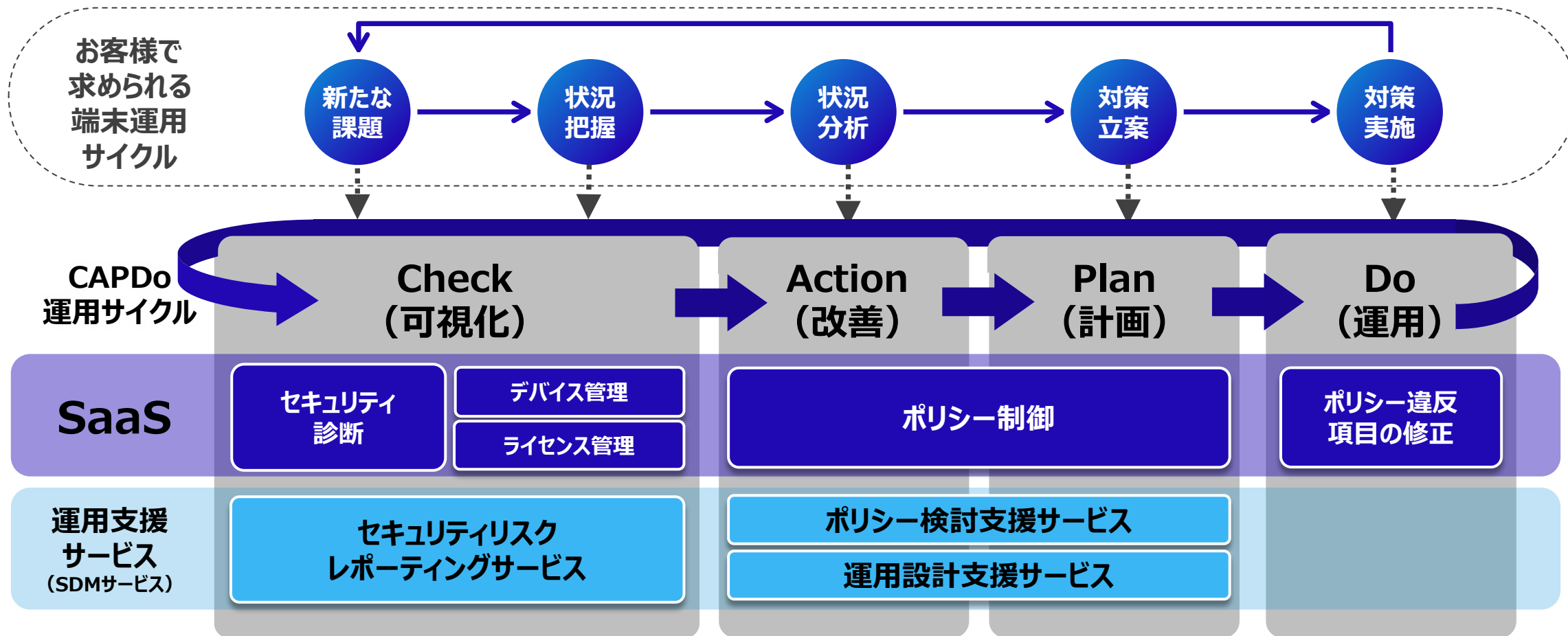
今後も発生し続けることが予想される環境変化や課題に対応するため、端末運用サイクルについても継続的な見直しが必要となります。また、端末運用サイクルの見直しだけでなく、端末を使用する人（ヒト）の知識・意識についても環境変化に対応するための施策を推進することが重要となります。



今後の端末運用には「資産」「セキュリティ」「人(ヒト)」を軸とした“継続的な運用サイクル”の実行が重要

Systemwalker Desktop Navi とは

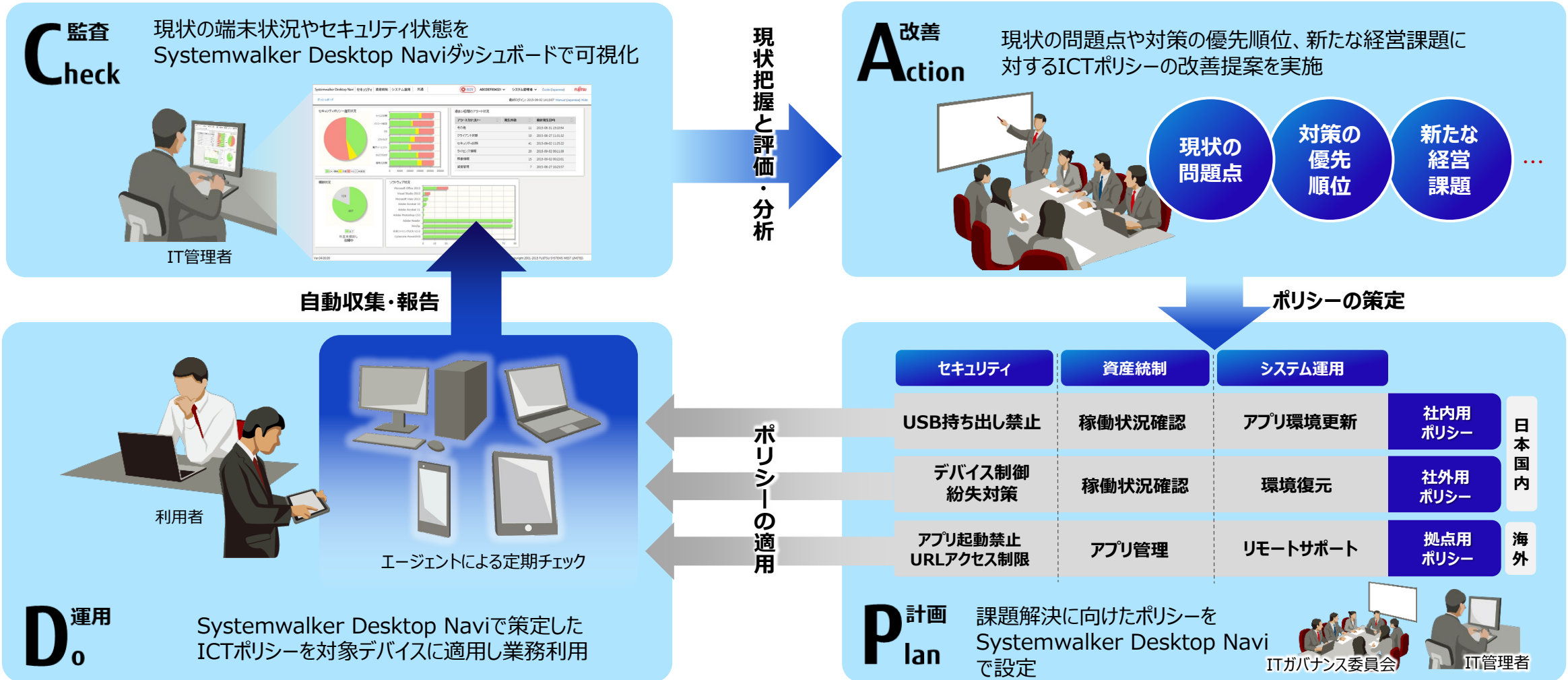
「Fujitsu Software Systemwalker Desktop Navi」は、お客様におけるICT端末運用サイクルにおける様々な環境変化や課題に対応し、運用サイクルを強化することで、お客様のICTガバナンス構築を支援するサービスです。



Systemwalker Desktop Navi

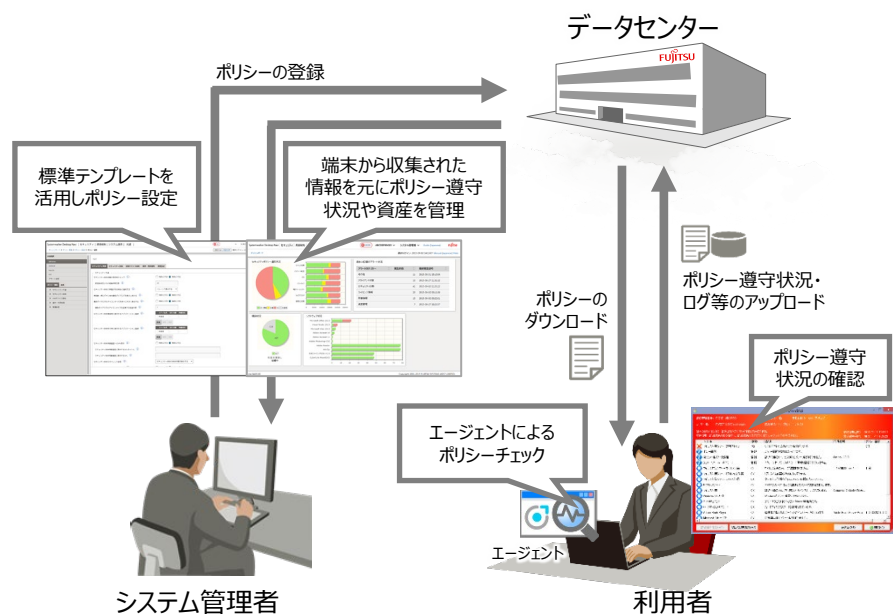
CAPDo運用サイクルとは

Systemwalker Desktop Naviは、従来の"計画"から始まるPDCAサイクルではなく、現状の可視化（Check）からお客様の課題を発見し、評価・分析から改善・計画・運用につながるCAPDo運用サイクルでお客様の端末運用を支援します。



クラウドサービスで簡単導入

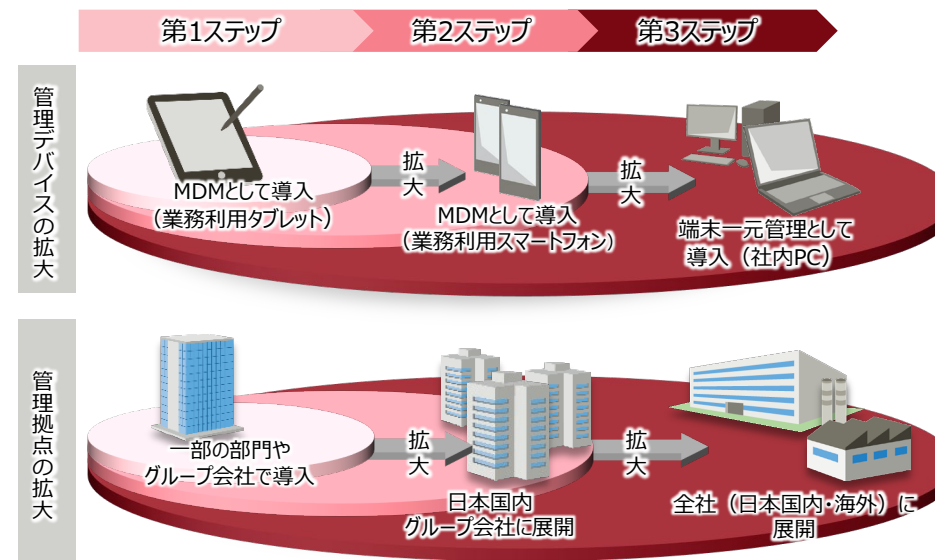
Systemwalker Desktop Naviはクラウドサービスのご提供となり、管理対象となるパソコンやスマートデバイスにエージェントプログラムをインストールするだけで、ご利用を開始いただけます。
専用のサーバー機器やストレージ、ネットワーク機器などの導入は不要です。



■ Systemwalker Desktop Navi 全体動作概要

ステップ展開が可能

オンプレミス型ソリューションと異なり、導入当初から全社展開を見込んだサーバー機器を導入する必要はありません。
始めたい処（デバイス、場所）からスタートし、順次その対象範囲を拡大させるというステップ展開が可能です。



■ Systemwalker Desktop Navi のステップ展開例

ダッシュボードによる可視化

システム管理者は、ブラウザから「管理者向けダッシュボード」にアクセスし、組織のポリシー遵守状況をひとめで把握することができます。
ポリシーに違反している端末も、ドリルダウン操作で容易に絞り込むことができます。



管理者向けWebダッシュボード

利用者端末上での可視化

利用者の端末上にもポリシー遵守状況がわかりやすく表示されます。
ポリシーに違反している項目については、その改善方法も併せて提示されるため、利用者自身での改善が可能で、利用者のリテラシー向上にも繋げることができます。

The user interface displays policy violation status and remediation tips. Key sections include:

- ポリシー違反状態**: A table of policy violations with remediation instructions.
- セキュリティ遵守状態**: A table of security compliance status.

項目	状態	説明	取付情報	ポリシー設定
ウイルス対策ソフトのインストール	NG	ウイルス対策ソフトがインストールされていません。		相
ウイルス対策ソフトの更新	情報	ウイルス対策ソフトの更新が完了しています。		
電子メールの送信	情報	電子メールの送信が完了しています。	Outlook 2010	
スクリーンセーバーのインストール	情報	スクリーンセーバーのインストールが完了しています。		
ウイルス対策ソフトのインストール	OK	ウイルス対策ソフトがインストールされています。	2015/08/09 rev.7	1日
ウイルス対策ソフトの更新	OK	ウイルス対策ソフトの更新が完了しています。		
スクリーンセーバーのインストール	OK	スクリーンセーバーがインストールされています。		
Windows Firewall	OK	Windows Firewallが有効になっています。	Symantec Endpoint Protection	
Guestアカウント	OK	ゲストアカウントが有効になっています。		
ハードディスクのフォーマット	OK	ハードディスクがフォーマットされています。		
Adobe Flash Player	OK	管理者が指定したバージョンがインストールされています。	Adobe Flash Player Avt... 10.3.182.22/10.183.103.182	
Microsoft Office XP	OK	対象製品がインストールされています。		

項目	状態	説明	取付情報	ポリシー設定
ウイルス対策	OK	ウイルス対策ソフトがインストールされています。		
スクリーンセーバー	OK	スクリーンセーバーがインストールされています。		
電子メールの送信	OK	電子メールの送信が完了しています。		
スクリーンセーバーのインストール	OK	スクリーンセーバーのインストールが完了しています。		
ウイルス対策ソフトのインストール	OK	ウイルス対策ソフトがインストールされています。	2015/08/09 rev.7	1日
ウイルス対策ソフトの更新	OK	ウイルス対策ソフトの更新が完了しています。		
スクリーンセーバーのインストール	OK	スクリーンセーバーがインストールされています。		
Windows Firewall	OK	Windows Firewallが有効になっています。	Symantec Endpoint Protection	
Guestアカウント	OK	ゲストアカウントが有効になっています。		
ハードディスクのフォーマット	OK	ハードディスクがフォーマットされています。		
Adobe Flash Player	OK	管理者が指定したバージョンがインストールされています。	Adobe Flash Player Avt... 10.3.182.22/10.183.103.182	
Microsoft Office XP	OK	対象製品がインストールされています。		

■ ダッシュボードによる可視化

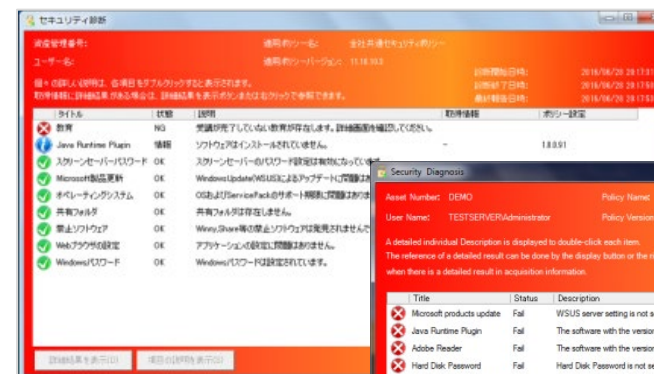
内部不正、とりわけ中途退職者による情報漏えいが大幅に増加しています。ログ強化オプションのシグネチャ検知機能は利用者による不正・危険操作を事前に把握に活用いただけます。



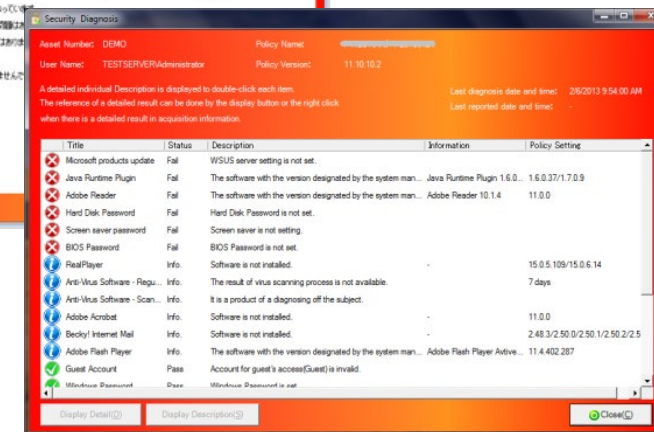
■ 幅広い用途に対応

お客様のワークスタイル変革に対応し、端末種別や利用場所を問わずご利用いただけます。

また、管理者向けダッシュボードやエージェントのUIは日本語以外にも英語、中国語（簡体字・繁体字）の多言語表示に対応し、海外拠点の管理にも活用いただけます。



(日本語表示)



(英語表示)

2. Systemwalker Desktop Navi による お客様課題解決

- お客様の課題解決に向けて
- Systemwalker Desktop Navi による課題解決
- セキュリティに関する課題
- 資産統制に関する課題
- リテラシーに関する課題
- システム運用に関する課題

Systemwalker Desktop Navi

Systemwalker Desktop Naviは、お客様の様々な課題をCAPDo運用サイクルで可視化し対策への取り組みを支援します。また、これら課題解決に向けた取り組みを組織に定着化させることで、組織全体のITガバナンス強化に貢献します。

セキュリティ

- 情報漏えい事件が多発しているので対策したい
- モバイルデバイスを業務利用したいが紛失が怖い
- セキュリティポリシーを策定しているが、社員がポリシーを遵守しているかわからない

ログ管理

- 内部犯行による情報漏えい事故が多発しているので対策したい
- テレワークを導入したが従業員の勤務状況が把握できずに困っている

資産統制

- 社内にどのようなICT機器があるのか把握できない
- ソフトウェアメーカーによる監査でライセンスの不正利用を指摘されることがあるようだ
- 棚卸しをしたいが、IT部門や一般従業員の負荷が大きく、かつ時間もかかる

リテラシー

- 従業員に社内セキュリティポリシーに違反している設定や操作を認識させ、ポリシーの定着化を図りたい
- また、問題がある設定を自身で修正できるスキルを身につけさせたい

システム運用

- モバイルデバイス上のデータやアプリを効率的に更新したい
- 支店や支社の遠隔地でトラブルが発生したとき、対応に時間がかかって困っている

ICT機器利活用に関するお客様の課題

「Fujitsu Software Systemwalker Desktop Navi」は、マルチデバイスのエンドポイントに対応し、お客様におけるICT端末運用サイクルにおける様々な環境変化や課題に対応し、運用サイクルを強化することで、お客様のICTガバナンス構築を支援するクラウドサービスです。

Systemwalker Desktop Navi

	セキュリティ			ログ管理		資産統制			リテラシー	システム運用	
課題	情報漏えい対策	紛失対策	ポリシー遵守・把握	内部不正対策	勤怠状況把握	ICT資産の効率的な把握	コンプライアンス遵守	棚卸しコスト削減	利用者リテラシー向上	運用・メンテナンスコスト削減	現場の生産性向上
対応機能	利用制限 操作ログ収集	リモートロック ワイプ	セキュリティチェック ダッシュボード	操作ログ収集	ログオン ログオフ ログ収集	インベントリ 収集	ソフトウェア ライセンス 管理	オンライン 棚卸し	セキュリティ チェック結果 可視化	資源配付	リモート モニタリング 操作



Android



Windows



iOS

🔒 セキュリティ

課題	情報漏えい対策	ICT機器の紛失	ポリシー遵守・把握
背景	標的型攻撃や社内の人間により、端末に保存されている個人情報や機密情報が外部に流出するという事件が多発している	スマートフォンやタブレットといったスマートデバイスの業務利用の普及に伴い、端末の紛失や盗難といった事件が多発している	社内でセキュリティに関するポリシーは策定されているものの、社員への周知・徹底が難しい
リスク	賠償金などの金銭的損失 社会的信用の失墜	賠償金などの金銭的損失 社会的信用の失墜	意図的・無意識に関わらず、 ポリシー不遵守による セキュリティ事故が発生する
望まれる対策	情報漏えい元となるルートを適切に制限・監視する	モバイルデバイス紛失時、遠隔での位置情報取得や、デバイス上のデータを消去できる	策定したセキュリティポリシーの遵守を徹底し、遵守状況を容易に把握できる
Systemwalker Desktop Navilによる対策			
	<ul style="list-style-type: none"> ● ソフトウェア起動禁止 ● URLアクセス禁止※ ● ファイル持出禁止 ● 許可のないUSB媒体の使用禁止 ● 印刷禁止 ● アプリ起動終了ログ ● メール送信ログ ● URLアクセスログ ● セキュリティ診断サービス ● USBストレージ機器接続分析サービス 	<ul style="list-style-type: none"> ● リモートロック・リモートワイプ ● ローカルロック・ローカルワイプ ● 端末位置情報取得 ● リモートデータ削除 <ul style="list-style-type: none"> ・指定ファイル、フォルダ ・電話帳 ・ブラウザ履歴など 	<ul style="list-style-type: none"> ● スケジュール実行可能なセキュリティ診断 <ul style="list-style-type: none"> ・ソフトウェアバージョンチェック ・パスワードチェック ・禁止、必須ソフトウェアチェック ● ダッシュボードでセキュリティ診断結果確認 ● ポリシー検討支援サービス ● セキュリティ診断サービス



ログ管理

課題	内部不正対策	勤務状況の把握	ICT資産の利用状況把握
背景	社内の人間が業務中や退職時に、端末に保存されている個人情報や機密情報が外部に流出させるという事件が多発している	テレワークを導入し、従業員の勤務状況が把握しにくくなった また、サービス残業やといった不正な労働が問題となっている	社内で保有するICT機器やソフトウェアを有効に活用されているかどうか判断できない
リスク	賠償金などの金銭的損失 社会的信用の失墜	生産性の低下 コンプライアンス違反による 社会的信用の失墜	余剰資産によるコスト増
望まれる対策	情報漏えい元となるルートを監視し、事故発生時に速やかに原因究明できる	従業員の勤務開始・終了時刻など勤務実態を把握できる	PCやインストールされているソフトウェアが有効に利用されているかどうかを把握できる
Systemwalker Desktop Navilによる対策			
	<ul style="list-style-type: none"> ● アプリケーション起動終了ログ ● メール送信ログ、WEBメール送信※ ● URLアクセスログ※ ● セキュリティ診断サービス ● USBストレージ機器接続分析サービス ● ファイル操作ログ※ ● 印刷ログ※ <p style="text-align: right;">※オプションサービスで別途ご契約が必要です</p>	<ul style="list-style-type: none"> ● PC起動・終了ログ ● ログイン・ログオフログ ● アプリ起動終了ログ 	<ul style="list-style-type: none"> ● PC起動・終了ログ ● ログイン・ログオフログ ● アプリ起動終了ログ

資産統制

課題	ICT資産の効率的な把握	コンプライアンスの遵守	棚卸コストの削減
背景	社内で保有するICT機器やソフトウェアを詳細に把握できていないため、これら資産が最適に配備されているかどうか判断できない	社内の端末にインストールされているソフトウェアの状況を正確に把握しておらず、ソフトウェアメーカーの監査等によって不正な利用を指摘されるという事件が発生している	ICT資産の棚卸しは、組織が保有している資産把握のために重要な作業であるが、管理者・利用者の負荷が大きいため、実施頻度が減る傾向にある
リスク	<p>余剰資産によるコスト増 機器・性能不足による生産性低下</p>	<p>賠償金などの金銭的損失 社会的信用の失墜</p>	<p>棚卸し作業負荷の増加 棚卸し漏れによるライセンスの不正利用</p>
望まれる対策	社内外に散在するICT資産の機器情報・利用状況を効率的に把握できる	保有しているライセンス数の範囲でソフトウェアが適切に利用されていることを確認できる	管理者・端末利用者の棚卸し作業負荷を低減し、効率的かつ正確な棚卸しを実施できる
Systemwalker Desktop Navilによる対策			
	<ul style="list-style-type: none"> ● ハードウェア情報収集 (CPU種別、メモリ容量、ディスク容量、ネットワーク設定など) ● ソフトウェア情報収集 (OS情報、ウイルス対策ソフト情報、インストールされているソフト情報など) 	<ul style="list-style-type: none"> ● ソフトウェアインストール数と保有しているライセンス数の比較 ● 組織割り当てのライセンス管理 ● 機器割り当てのライセンス管理 ● オンラインソフトウェア棚卸し、など ● ソフトウェアライセンス分析サービス 	<ul style="list-style-type: none"> ● 管理者の指示により、端末利用者が「機器利用者氏名」「機器設置場所」「機器の状況」などをオンラインで棚卸し回答可能 ● 棚卸し終了期限が近づいた際の督促

リテラシー

利用者リテラシーの向上

課題

背景

全社でセキュリティやコンプライアンス等のポリシーは策定するものの、ポリシーを遵守した運用を利用者に周知徹底させることが難しい

ポリシー遵守のために必要な設定方法・変更方法がわからず、システム管理者への問い合わせが増加する

リスク

ポリシー不遵守によるセキュリティ事故やコンプライアンス違反が発生

管理者がQA対応や設定代行などの業務に追われ、本来の業務に集中できない

望まれる対策

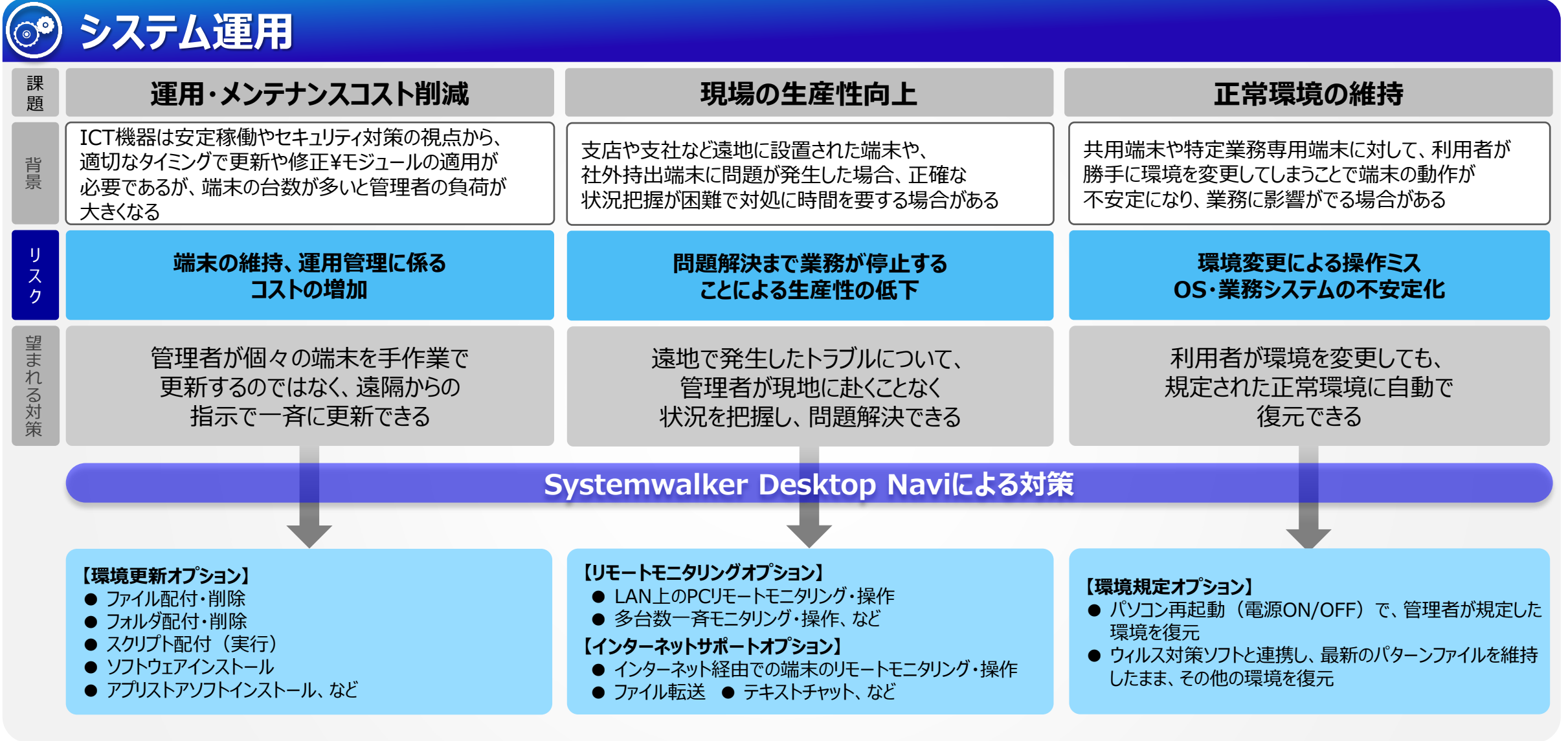
ポリシー遵守状況を利用者に見える化し、利用者にポリシー違反を認識させることができる

ポリシー遵守のために必要な設定を利用者自身で実施できる

Systemwalker Desktop Navilによる対策

- 利用者端末上にセキュリティ診断結果を表示し、ポリシー違反状況を利用者自身に見える化

- ポリシー違反時、診断結果と合わせて改善方法も提示し、利用者自身で設定を修正可能



3. 機能紹介 ～基本サービス～

■ セキュリティ

- ポリシー遵守状況の可視化
- セキュリティ診断
- 汎用セキュリティ診断
- 利用制限
- 利用制限（デバイス接続制限）
- 利用制限（モバイルデバイス）
- 紛失対策

■ ログ管理

- ログ収集
- 勤怠管理・ICT資産管理支援
- 情報漏えい・不正操作対策
- ログ強化オプション
- ログ強化オプション ～ファイル操作の追跡～
- ログ強化オプション ～フォワードトレース～
- ログ強化オプション ～バックトレース～
- ログ強化オプション ～機能概要～
- ログ強化オプション ～ログの保存期間について～

■ 資産統制

- インベントリ自動収集
- レジストリ情報収集
- ソフトウェアインストール状況からのライセンス管理
- ライセンス情報登録とライセンス割り当て
- オンライン棚卸しによる利用者と端末状態の一斉確認
- Windows10更新支援機能

■ 管理者向けWebダッシュボード

- Systemwalker Desktop Navi
- 導入展開支援
- ミニインストーラ
- エージェントのキッティング対応



以降の頁に記載されている機能につきましては、管理対象端末のOSにより利用可否が異なります。頁右上や機能名の横に記載されているOS略名アルファベットをご確認ください。
 （ W : Windows OSで利用できる機能 A : Android OSで利用できる機能 I : iOSで利用できる機能）

ポリシー遵守状況の可視化

ポリシーの遵守状況は管理者、利用者双方に分かりやすい形で可視化されます。これにより管理者は容易に問題点を絞り込むことができ、利用者はポリシー遵守に向けて改善が必要であることを認識することができます。

Systemwalker Desktop Navi | セキュリティ | 資産統制 | システム運用 | 共通

ダッシュボード

セキュリティポリシー違反状況

過去14日間のアラート状況

アラートカテゴリ	発生件数	最終発生日時
その他	11	2015-08-31 15:10:54
クライアント状態	10	2015-08-27 11:31:32
セキュリティ診断	41	2015-09-02 11:25:22
ライセンス情報	20	2015-09-02 00:11:39
稼働情報	15	2015-09-02 00:22:01
資産管理	7	2015-08-27 10:23:57

Copyright 2011-2015 FUJITSU SYSTEMS WEST LIMITED.

● 管理者向けダッシュボード

管理者は、組織全体のポリシー遵守状況をWebダッシュボードから一目で確認することができます。



セキュリティ診断

資産管理番号: PC-10 通用ポリシー名: 全社共通ポリシー

ユーザー名: 通用ポリシーバージョン: 11.10.10.7

タイトル	状態	説明	取得情報	ポリシー設定
教育	NG	受講が完了していない教育が存在します。詳細画面を確認...		
スクリーンセーバパスワード	NG	スクリーンセーバの待ち時間が10分を超えています。		
Webブラウザの設定	NG	Internet Explorerのオートコンプリートでユーザー名がバウ...	Internet Explorer 11.1494.1...	
ウイルス対策ソフト...	OK	ウイルスス...		
Windowsパスワード	OK	全てのドライ...		
ウイルス対策ソフト...	OK	ウイルス定...		
ウイルス対策ソフト...	OK	リアルタイム...		
オペレーティングシステム	OK	OSおよびSe...		
Microsoft製品更新	OK	WindowsU...		
共有フォルダ	OK	共有フォル...		
Adobe Flash Player	OK	管理者が指...		
Adobe Reader	OK	管理者が指...		
Java Runtime Pla...	OK	管理者が指...		

● セキュリティ診断結果 (※Windows®のみ)

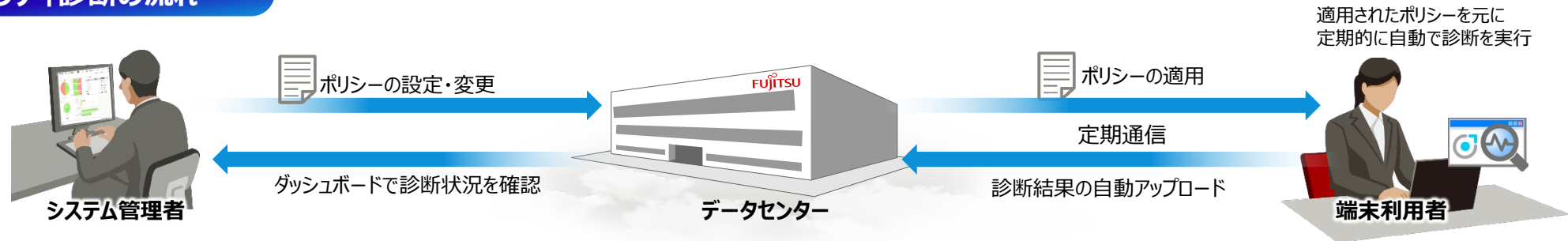
利用者は、セキュリティ診断結果でポリシー違反状況を端末上で確認することができます。



セキュリティ診断

システム管理者は運用方針に則りセキュリティポリシーを作成します。作成したポリシーは、パソコンやスマートデバイス上のエージェントに配信され、定期的に診断を行います。

セキュリティ診断の流れ



セキュリティ診断項目

Windows

- ウィルス対策ソフトウェア診断
 - ・製品
 - ・バージョン
 - ・定義ファイルバージョン
 - ・スキャン対象設定など
- OSバージョン診断
- OS更新プログラム診断
- 汎用ソフトウェアバージョン診断
 - ・Adobe Reader
 - ・Adobe Flash Player
 - ・Oracle Java Runtimeなど
- ブラウザ・メーラー設定診断
- パスワード診断
 - ・BIOSパスワード
 - ・HDDパスワード
 - ・ログオンパスワード
 - ・スクリーンセーバパスワードなど
- 必須ソフトウェア
- 禁止ソフトウェア
- 不正ソフトウェア
- 暗号化設定
- USB機器接続診断

Android

- ウィルス対策ソフトウェア診断
 - ・製品診断
- OSバージョン診断
- 汎用ソフトウェアバージョン診断
 - ・Adobe Reader
 - ・Adobe Flash Player
- パスワード診断
 - ・スクリーンロックパスワードなど
- 必須ソフトウェア診断

iOS

- 必須ソフトウェア診断
- 禁止ソフトウェア診断

汎用セキュリティ診断

標準で用意されている約30種類のセキュリティ診断項目に加え、PC上のファイル・レジストリを診断条件とした、お客様独自のセキュリティ診断項目を最大5つまで追加できます。

汎用セキュリティ診断の流れ

① 事前確認

新規に追加したいセキュリティ診断項目が、PC上のファイルの有無、またはレジストリキーの存在や値などからチェックできるかどうかを確認します。



〇〇ソフトのバージョンはこのレジストリに記録されているな。

② ポリシー設定・適用

事前確認でPC上のファイル・レジストリが診断条件に利用できることが確認できたら、その内容をもとにポリシーを編集します。



「〇〇ソフトバージョン診断」をポリシーに登録

③ 利用者PC上でのセキュリティ診断

利用者PC上でポリシーを最新化し、セキュリティ診断を実行します。

診断結果画面には、ポリシー追加時に設定した診断項目名とその診断結果が表示されます。



〇〇ソフトのバージョンを診断するようになったんだ。最新化しないと!

診断条件に利用できる項目

項目	判断条件
ファイル	<ul style="list-style-type: none"> 指定したファイルが存在するか 指定したファイルのバージョン、更新日付が一致するか
レジストリ	<ul style="list-style-type: none"> 指定したレジストリキーが存在するか 指定したレジストリキーの値が条件を満たすか（完全一致・以上・以下・より大きい・より小さい）

⚠ 本機能に関する留意事項

本機能は、お客様が指定したファイルやレジストリを診断条件としてセキュリティ診断を行うものです。診断条件として指定したファイルまたはレジストリが、お客様が意図するセキュリティ診断の診断条件として適さないものであった場合、誤診断が発生する場合があります。このため、診断条件として使用するファイルやレジストリは、事前確認の時点で十分ご確認いただくとともに、ポリシー設定後も継続して確認・見直しを行うことをおすすめいたします。

■ 操作・利用制限

対象OS : W、A

パソコン・スマートデバイス利用時のリスク軽減を図るため、様々な機能を制御・制限することができます。



ソフトウェア起動禁止

W、A

インストールされているソフトウェア情報を取得し、任意のソフトウェアの起動を禁止します。

URLアクセス禁止

W、A

管理者が指定した任意のURLについて、ブラウザからのアクセスを禁止します。

許可のないUSB媒体の使用禁止

W

管理者が特定のUSBメモリのみに使用を限定させることで、データの持ち出しに関する安全性が向上します。

ファイル持出禁止

W

指定ドライブへのアクセスを監視し、書き込み（持出し）を禁止します。

印刷禁止

W

管理者が指定した、任意のソフトウェアからの印刷操作を禁止します。

リムーバブルメディアからのデータ読み込み禁止

W

リムーバブルメディアからはデータを読み込ませない設定ができます。これにより、リムーバブルメディアを介した不正なデータやソフトウェアの持ち込みを防止できます。

■ 操作・利用制限（デバイス接続制限）

パソコンからの情報漏えいに繋がる、Wi-Fi接続やBluetooth接続などの各種外部接続を制限することができます。

Wi-Fi接続禁止

W

Wi-Fi接続を全面禁止したり、管理者が指定したWi-Fiアクセスポイント※のみアクセスを許可することができます。

※特定のアクセスポイントへの接続を許可する場合、アクセスポイントはBSSID（アクセスポイントのMACアドレス）で指定する必要があります。

Bluetooth接続禁止

W

Bluetoothでの外部デバイス接続を全面禁止したり、任意のBluetoothデバイス種別※を指定して許可・禁止することができます。

※PC、周辺機器、ウェアラブルといった機器種別を指定することができます。機器を個別識別して許可・禁止することはできません。

赤外線接続禁止

W

赤外線通信ポート（IrDAポート）が搭載されているPCで、赤外線通信による外部接続を禁止することができます。

PCカード接続禁止

W

PCMCIAや、PCIExpressのカードスロットが搭載されているPCで、スロットに挿入されているカードの利用を禁止することができます。
また、メーカーIDや製品ID、シリアル番号を持つカードの場合、個体を識別して利用を許可することができます。

IEEE1394接続禁止

W

IEEE1394ポート経由での外部機器接続を禁止することができます。

パラレル・シリアルポート接続禁止

W

パラレルポート、シリアルポート経由での外部機器接続を禁止することができます。

■ 操作・利用制限（モバイルデバイス）

対象OS：A、I

スマートフォンに内蔵されたデバイスや機能を制御・制限することで、スマートフォンの業務利用時におけるセキュリティレベルを確保します。

ハードウェア 利用制限

電話発信制限 A

プライベート通話など業務外利用を抑止できます。

内蔵カメラ利用禁止 A、I

カメラで撮影・保存した情報の流出を抑止できます。

Bluetooth利用禁止 A

Bluetooth経由での通信による情報流出を抑止できます。

無線LAN利用禁止 A

無線LAN経由の通信による情報流出を抑止できます。

USB接続禁止 A

PC経由での情報流出やウイルス侵入を抑止できます。

SDカード利用禁止 A

SDカードからの情報流出やウイルス侵入を抑止できます。

デザリング禁止 A

意図しないデバイスが接続されることによる情報漏えいや個人所有PCを接続しての業務外利用を抑止します。

ソフトウェア 利用制限

URLアクセス禁止 A

業務外でのWebサイトへのアクセスや、悪意のあるWebサイトからのウイルス侵入を抑止します。

ソフトウェア起動制限 A、I

業務に不要なソフトウェアの起動を制限し、業務外の利用を抑止します。
iOSデバイスではiTunesやSiri、SafariなどのOS標準アプリの起動を制限することができます。

ソフトウェアインストール禁止 A

業務に不要なソフトウェアのインストールを抑止します。

スクリーンショット取得制限 I

取得されたスクリーンショット画像からの情報漏えいを抑止します。

紛失対策

スマートデバイスやPCを紛失した場合、各種リモート機能で情報漏えいを防ぎます。



リモートロック

W、A、I

遠隔操作で、スマートデバイスやPCのロックを行います。
Windows®の場合、ローカルアカウントを無効化することにより不正なログインを防止します。

リモートワイプ

W、A、I

遠隔操作で、スマートデバイスやPCをワイプ（初期化）することができます。

リモートデータ削除

W、A

遠隔操作で、スマートデバイスやPC上のデータを削除することができます。

リモート3G通信遮断

A

遠隔操作で、スマートデバイスのLTE通信を遮断することができます。

位置情報取得

A

デバイスの位置情報を取得することができます。

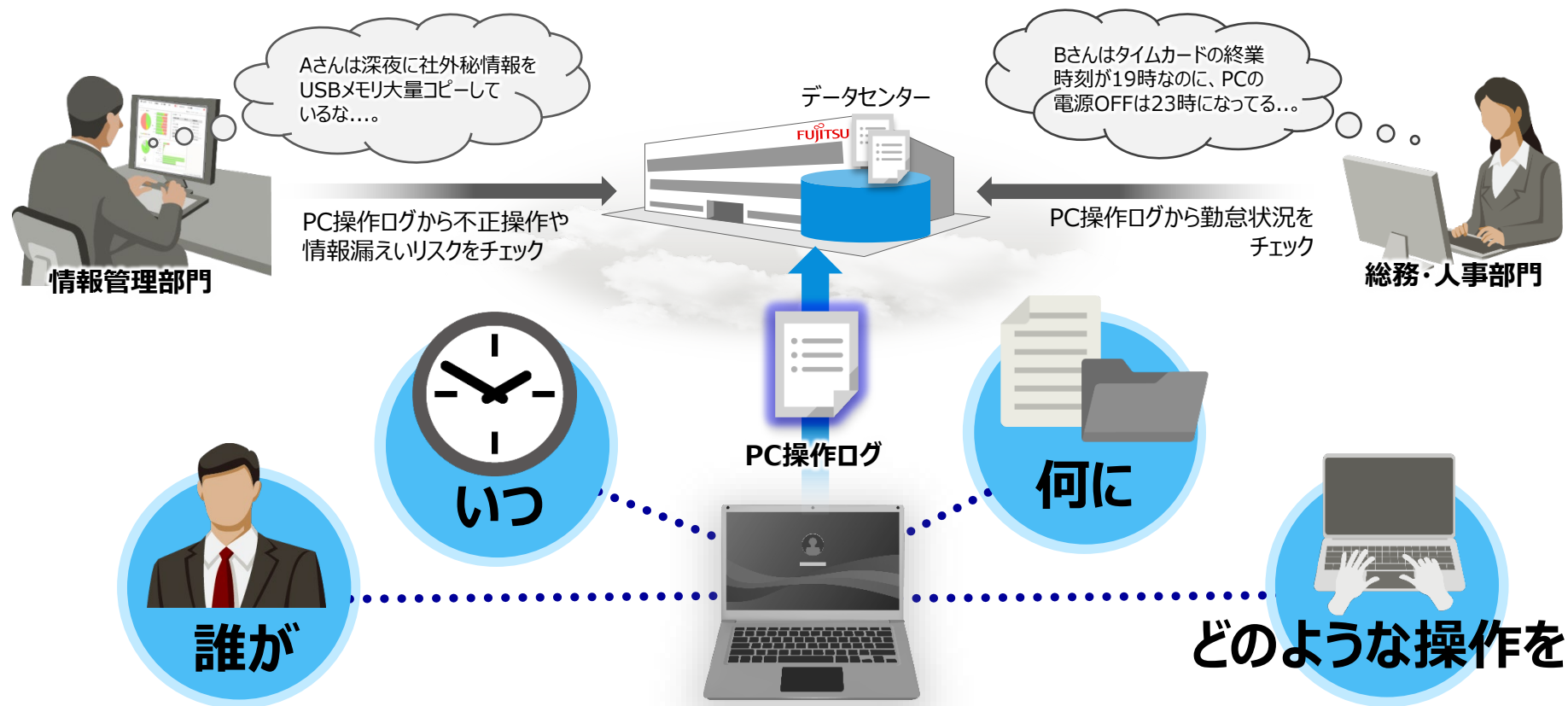
■ リモート指示を受信できない場合でも（ローカルロック・ワイプ・データ削除） W、A、I



スクリーンロック解除やログオンに指定回数失敗した場合、スマートデバイスの初期化（ローカルワイプ）やPC上に保存されているローカルデータを削除することができます。

PCの操作ログ収集は、情報漏えい対策、社員のセキュリティ意識向上、勤怠管理などに活用できます。PC操作ログ管理をすることで、「誰が」「いつ」「何に」アクセスをして、「どのような操作を行なったか」を記録、管理できるようになります。

PC操作ログを管理することで、社内のICT資産が適正に利用が行われているかを管理者が把握できます。また、PC操作ログが企業・組織によって管理されていることを従業員へ周知することで、従業員の情報セキュリティに対する意識向上につなげることができます。



■ 勤怠管理・ICT資産管理支援

PC操作ログを収集することで、従業員の働き方を把握することができます。また、ICT資産が有効に活用されているかどうかについても把握することが可能となります。

PC起動・終了ログ

W

PCの起動時刻や終了時刻のログを収集できます。また、スリープやスタンバイについても開始・復帰時刻もログとして収集できます。



勤怠状況の把握

PCの電源ON・OFF時刻や、利用者のPCへのログオン・ログオフ時刻を勤怠管理システムに記録された出勤・退勤時刻と比較することで、サービス残業の抑止といった**適正な勤怠管理**が可能。

ログオン・ログオフログ

W

利用者のPCへのログオン・ログオフ時刻をログとして収集できます。



ICT資産の有効活用

ソフトウェアの起動状況を把握し、利用されていない**ソフトウェアを削減することで、コスト削減を実現**。

ソフトウェア起動・終了ログ

W、A

ソフトウェア名および起動・終了^{*}時刻をログとして収集できます。
※Android OSの場合、ソフトウェアの起動のみログとして収集できます。



情報漏えい・不正操作対策

高度なセキュリティ対策実施には、ログ情報の管理が必要不可欠です。情報漏えいに繋がる可能性のある操作のログを取得・周知することで、利用者の不正な操作を抑止するとともに、問題発生時の調査・分析に活用できます。

メール送信ログ

W

Microsoft Outlook やSMTPを使用するメールソフトを対象に、メール送信時の宛先、件名、送信日時等のログを収集できます。

URLアクセスログ

W、A

Webブラウザ[※]からアクセスしたWebサイトのURLをログとして収集できます。

Webアップロード・ダウンロードログ

W

Webブラウザを使用して、任意のWebサイトに関するファイルのアップロードやファイルのダウンロードをログとして収集できます。

ファイル持ち出しログ

W

USBメモリや書き込み可能な光学ドライブへのファイル書き出しをログとして収集できます。
[※]ファイル持ち出しログは「ファイル持ち出しユーティリティ」を利用する必要があります。

ソフトウェア起動・終了ログ

W、A

ソフトウェア名および起動・終了[※]時刻をログとして収集できます。
[※]Android OSの場合、ソフトウェアの起動のみログとして収集できます。



情報漏えいの抑止・原因究明

USBメモリなどの外部記憶装置や、電子メールやWebストレージなどインターネットを介したデータ持ち出しがログとして記録されるため、データ持ち出しが管理されていることを従業員が意識することで、**情報漏えいを目的としたデータ持ち出しを抑止することが可能**となります。



マルウェア感染の抑止・原因究明

マルウェアは電子メールや悪意を持ったWebサイトへのアクセスなど様々な経路で感染する場合があります。
万が一こうした経路で**マルウェアに感染した場合でも、感染経路の特定が容易**となります。



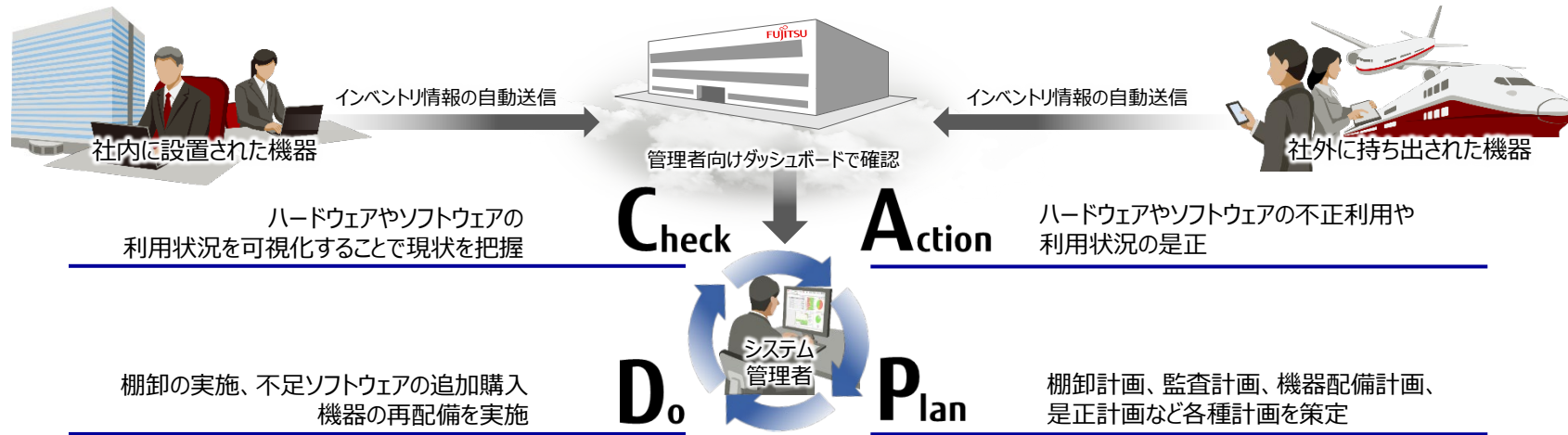
また、**業務に不要なWebアクセスやソフトウェアの使用といった行為も把握・抑止**することが可能です。



インベントリ自動収集

端末上のエージェントが定期的にハードウェア・ソフトウェアインベントリをセンターへ送信します。管理者は収集されたインベントリ情報を管理者向けダッシュボードで確認でき、資産管理についてもCAPDoサイクルで運用することができます。

収集されたインベントリ情報はCSVファイルとしても出力可能で、お客様独自の分析にもお役立ていただけます。



※自動収集可能な項目はOSによって異なります。

自動収集項目

【ハードウェア情報】

CPU関連（種別、クロック）、メモリ関連（物理、仮想）、PC関連（種別、型名、メーカー、製造番号）、ネットワーク関連（アダプタ名、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）ほか

【スマートフォン専用情報】

電話番号、キャリア、IMEI、MEID

【ソフトウェア情報】

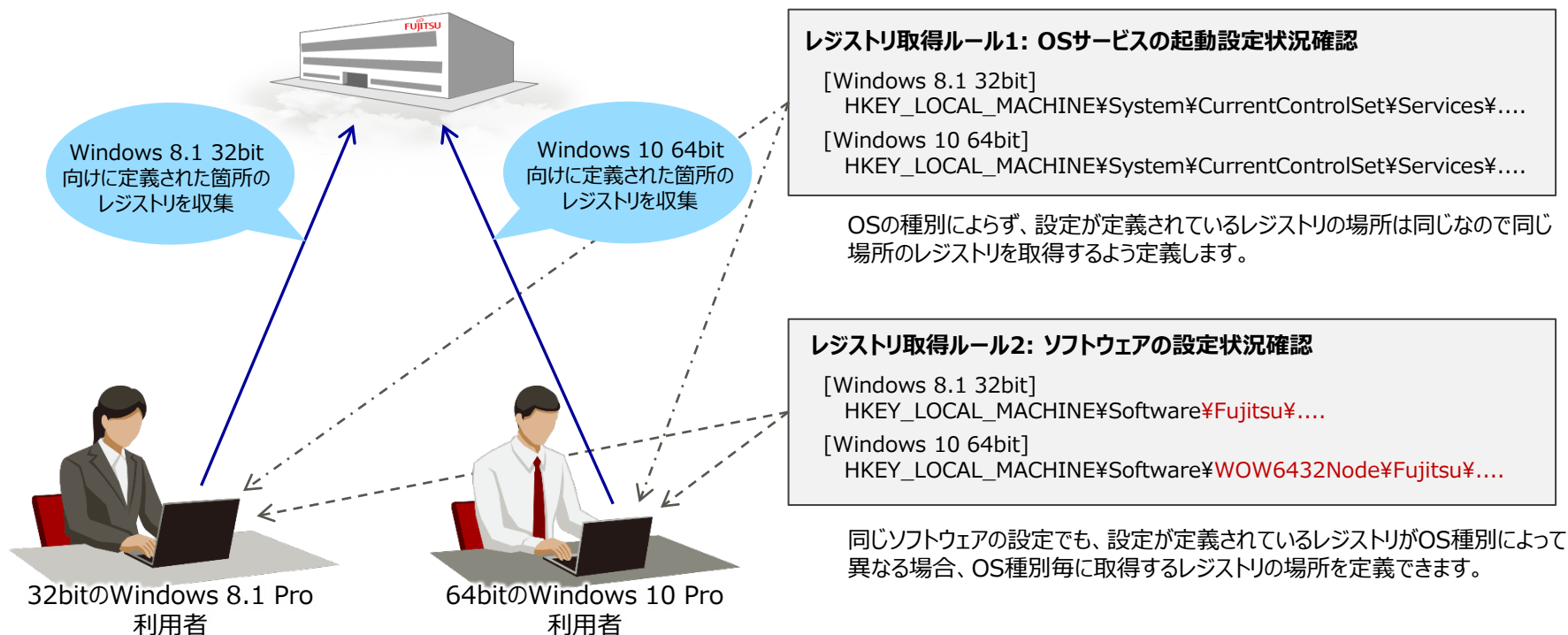
OS、サービスパック、ウィルス対策ソフトウェア名、インストールソフトウェア名、クライアント情報、システム全般、ログ全般・詳細

追加入力可能項目

機器管理番号、登録日、導入責任者、導入形式、購入日、購入先、購入金額、リース/レンタル情報（開始日、終了日、取引先、経費、管理番号、契約番号）管理部署、管理者、使用部署、使用者、設置場所、メモ、など

レジストリ情報収集

Windows PC上の任意のレジストリ情報を収集します。収集したレジストリ情報は、管理者向けダッシュボードからCSVファイルとして出力し、確認することができます。OS種別によって異なる箇所のレジストリを収集できますので、OSやソフトウェアの設定状況確認等にご利用いただけます。

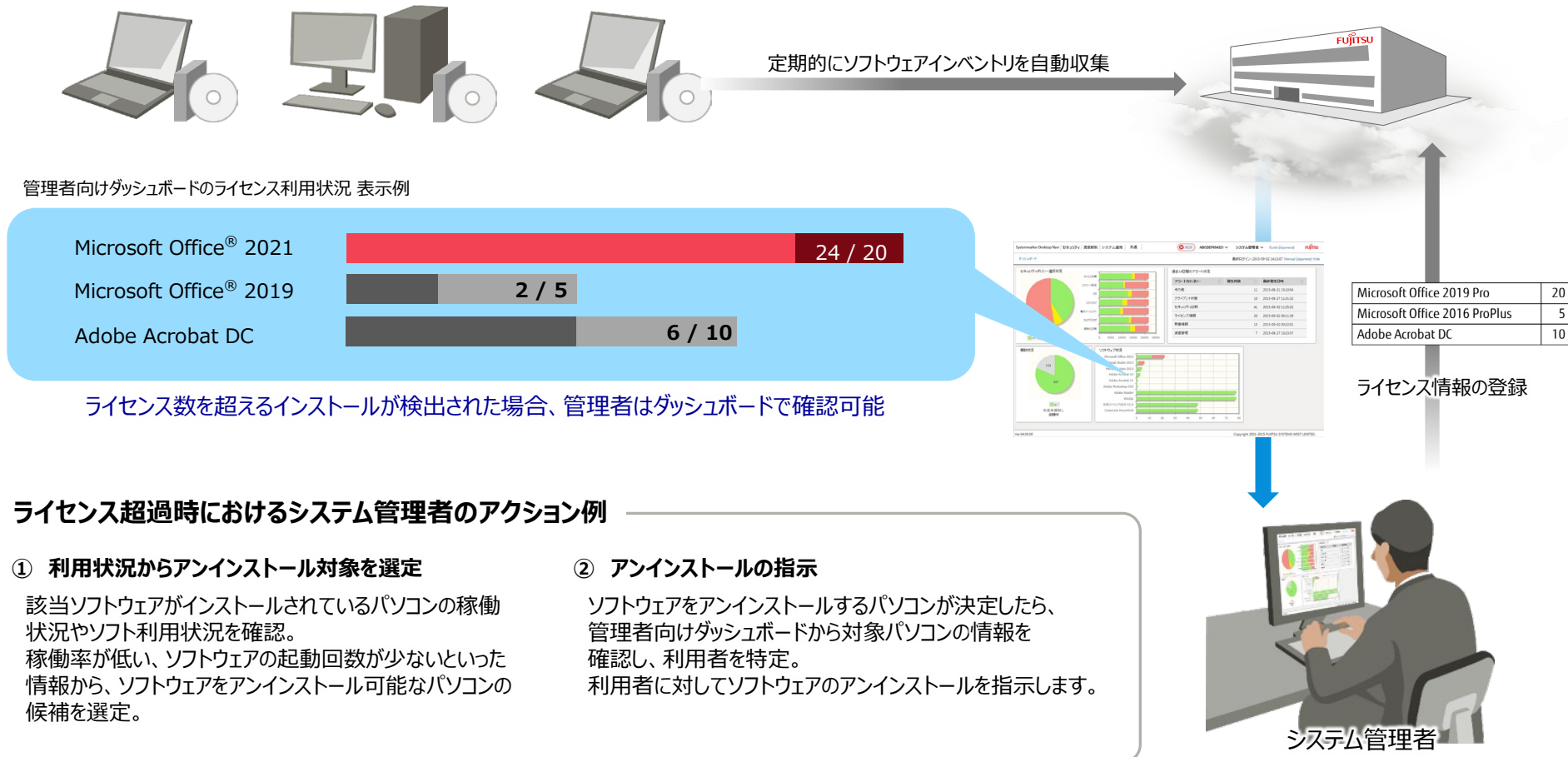


⚠ 本機能に関する留意事項

本機能で収集できるのは、「HKEY_CLASSES_ROOT」、「HKEY_LOCAL_MACHINE」、「HKEY_CURRENT_CONFIG」配下にある情報のみです。「HKEY_CURRENT_USER」や「HKEY_USERS」配下の情報を収集することはできません。

ソフトウェアインストール状況からのライセンス管理

各機器から自動収集されたインストール済みソフトウェアインベントリを基に、ライセンス管理を行うことができます。



ライセンス超過時におけるシステム管理者のアクション例

① 利用状況からアンインストール対象を選定

該当ソフトウェアがインストールされているパソコンの稼働状況やソフト利用状況を確認。稼働率が低い、ソフトウェアの起動回数が少ないといった情報から、ソフトウェアをアンインストール可能なパソコンの候補を選定。

② アンインストールの指示

ソフトウェアをアンインストールするパソコンが決定したら、管理者向けダッシュボードから対象パソコンの情報を確認し、利用者进行特定。利用者に対してソフトウェアのアンインストールを指示します。

ライセンス情報登録とライセンス割り当て

管理者は詳細なソフトウェアライセンス情報を登録できるとともに、登録したライセンス情報を『端末単位』あるいは『組織単位』で割り当てて管理することができます。登録したライセンスの利用状況は管理者向けダッシュボードのライセンス情報一覧画面で確認することができます。

ライセンス情報の登録

管理者向けダッシュボードを使用して、ライセンス管理対象とするソフトウェアの情報を登録します。



ライセンス情報として登録可能な情報は下記項目です。

- ライセンス情報のタイトル
- ライセンスキー（シリアルキー）
- 購入数
- 購入金額
- 購入日
- 備考
- ソフトウェア種別（有償・無償・その他）
- ライセンス種別
- ライセンス種別備考
- 媒体管理場所（ライセンス媒体種別・ライセンス媒体保管場所・備考）



ライセンスの割り当て

登録したライセンスは、『端末単位』や『組織単位』に割り当てて、ライセンスの利用状況を確認することができます。

■ 端末単位の割り当て



ライセンスを任意の端末に割り当てて管理します。ライセンスが割り当てられていない端末上で該当ソフトが検出された場合、ライセンス違反と判断します。

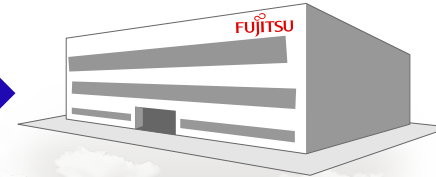
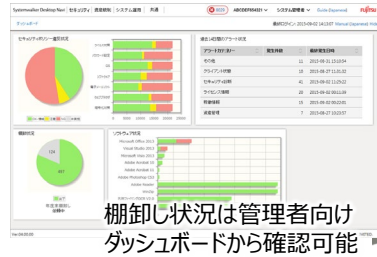
■ 組織単位の割り当て



ライセンスを任意の組織に割り当てて管理します。組織に所属する端末にインストールされている該当ソフトの総数が、割り当てられたライセンス数を超過している場合、ライセンス違反と判断します。また、ライセンスが割り当てられていない組織の端末で該当ソフトが検出された場合も、ライセンス違反と判断します。

オンライン棚卸による利用者・端末状態の一斉確認

面倒な棚卸し作業を、対象機器及び期間を指定し一斉に実施できます。
長期間アクセスのない機器、存在が確認できない機器を発見した場合は、管理者へ通知します。

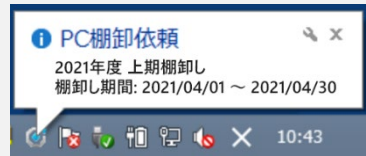


棚卸し依頼

棚卸し状況確認

棚卸し依頼

管理者が「棚卸し依頼」を指示すると、利用者のパソコン上に棚卸し依頼がポップアップされます。



棚卸し回答

利用者は「利用者氏名」、「設置場所」、「利用部門」などを棚卸し回答画面に入力し、送信します。

【 Windows®パソコン上での棚卸し 】

2021年度 上期の棚卸し
棚卸し期間: 2021/04/01 ~ 2021/04/30

メッセージ:

管理情報

資産管理番号(A):

コンピュータ名(M):

利用部門:

利用者氏名(L):

棚卸実施者(C):

設置場所:

その他

利用状況(S):

備考(Q):

棚卸する(C) キャンセル

棚卸し依頼

棚卸し回答

棚卸し依頼

棚卸し回答



Windows® 10 更新支援機能

対象OS : W

Windows® 10 機能更新プログラム適用に関連する様々な課題解決を支援します。

機能更新プログラムの適用延期が可能

Webダッシュボードからの指示で、社内のWindows® 10 PCに対して機能更新プログラムの適用を一斉に延期することができます。これにより、意図しない機能更新プログラム適用が原因で、業務で利用しているソフトウェアが利用できなくなるといったトラブルを防止することができます。

機能更新プログラムのバージョン選択が可能

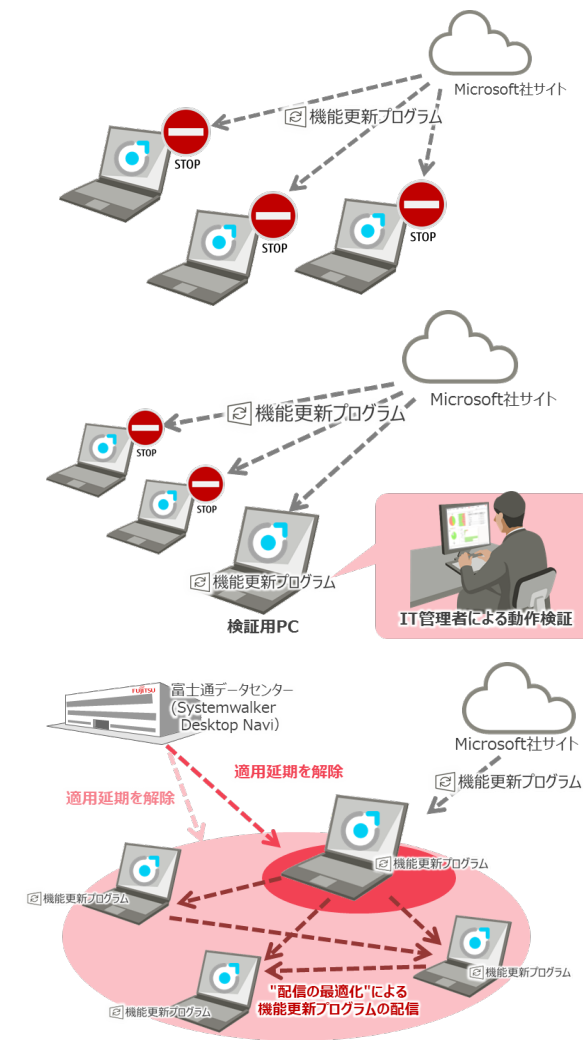
Windows 10に対して、適用する機能更新プログラムのバージョンを端末単位で指定することができます。これにより、PC上で利用しているアプリケーションの機能更新プログラムへの対応状況や、PCの利用用途などにあわせて最適な機能更新プログラムの適用制御が可能です。

機能更新プログラムダウンロードによるネットワーク負荷を軽減

機能更新プログラムの適用延期・延期解除を段階的に制御することにより、Windows® 10が持つ「配信の最適化※」機能を効率よくコントロールすることができます。

これにより、インターネット接続回線の負荷や社内ネットワークの負荷を低減できます。

※ 配信の最適化:
機能更新プログラム・品質更新プログラムなどをマイクロソフトのサーバーからだけでなく、既にアップデートなどを受信した他のPCからも受信することができる、Windows 10に搭載された機能。



Windows® 10 更新支援機能

機能更新プログラム適用支援

- Windows® 10 PCに対して、機能更新プログラムの適用を最大365日延期できます。
- 機能更新プログラムの適用延期・延期解除は、Webダッシュボードから複数のWindows® 10 PCに対して一斉に指示できます。
- 機能更新プログラムの適用延期を解除したPCに対して、最新の機能更新プログラムが適用されたことを検知して、自動で再度適用を延期させることができます。
- 『配信の最適化』に関するパラメータ（帯域幅、アップロード上限など）を制御することができます。

可視化

Webダッシュボードから、

- 登録されているWindows® 10PCのバージョン情報を一覧で確認できます。
- 機能更新プログラムの延期指示状況を確認できます。
- Windows® 10 のバージョンを指定して、PCを検索・抽出できます。

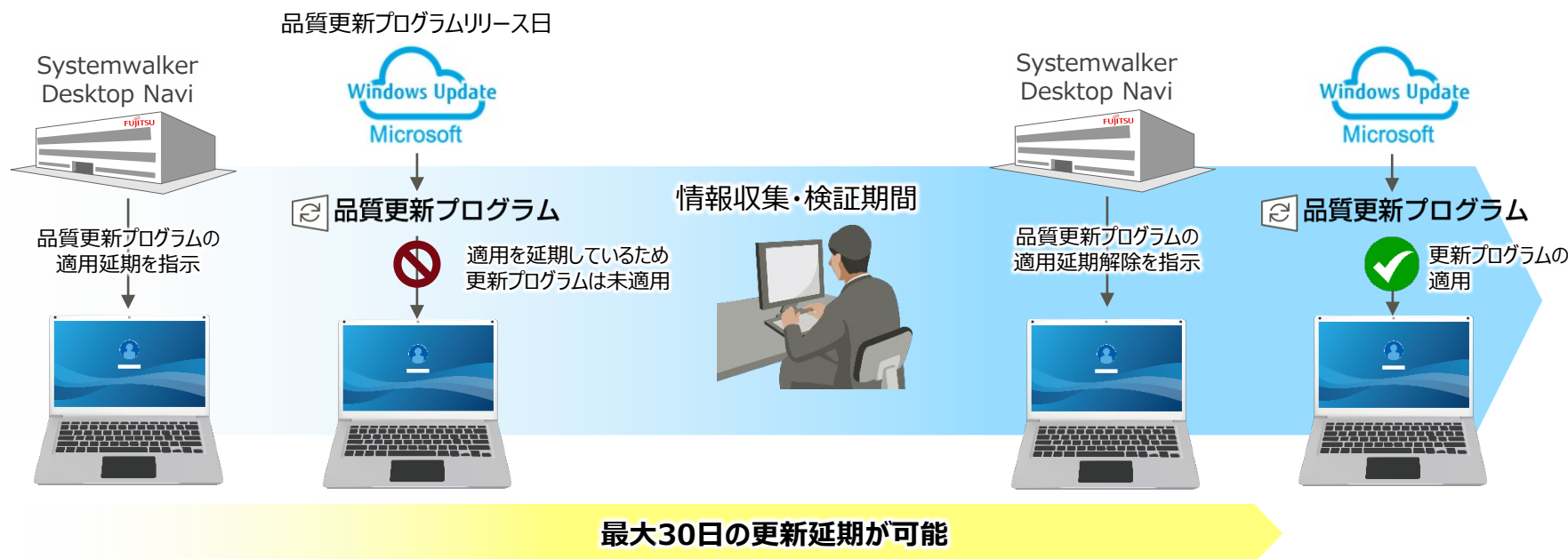
本機能に関する留意事項

- 本機能を使用して、Windows® 10 Homeの機能更新プログラム適用は制御できません。
- OSの仕様として、機能更新プログラムの適用を延期できる期間は、対象機能更新プログラムの公開日から最大365日となります。この期間を超えた時点、または既にこの期間を超えているバージョンのWindows® 10については、本機能を使用して機能更新プログラムの適用を延期できません。
- 機能更新プログラムの検出・ダウンロード・適用はOSの動作仕様に従います。このため、Microsoft社が機能更新プログラムを公開した後であっても、PC側での機能更新プログラム検出に時間を要する場合があります。
- 本機能は、2020年1月時点のWindows® 10のOS仕様に基づいており、これらOSの仕様は今後変更される場合があります。このため、Microsoft社の仕様変更によっては、将来にわたって本機能の動作を保証できない場合があります。
- 指定可能な機能更新プログラムのバージョンは、Microsoft社のサポート期限内のバージョンのみとなります。既にサポート期限が終了している機能更新プログラムは指定することができません。

Windows®10 更新支援機能

品質更新プログラムの適用延期指示 / 延期解除指示

従来のWindows10に対する機能更新プログラムの適用延期指示に加え、**品質更新プログラムについても最大30日間、適用の延期を指示できます。**
 Windows10の品質プログラムは適用の自動化が進んでおり、セキュリティ維持の面ではメリットはあるものの、品質更新プログラムに障害が含まれていた場合、障害の内容によっては、利用者がPCを利用できなくなるなどの致命的な結果に繋がる可能性があります。
 本機能を利用することで、品質更新プログラムのリリース直後は適用を延期し、事前検証や情報収集の時間を確保することができます。

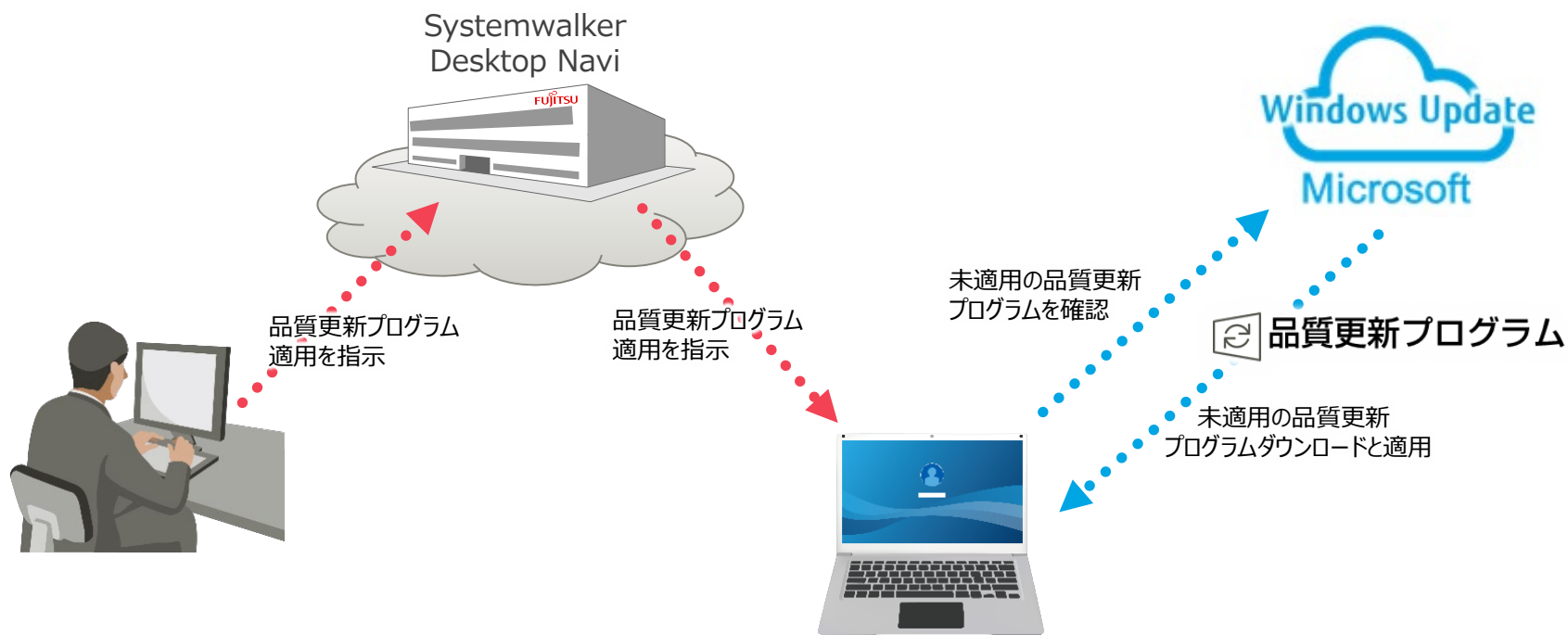


Windows®10 更新支援機能

品質更新プログラムの適用指示

Windows10に対して、**未適用の品質更新プログラムが存在する場合、未適用の品質更新プログラムの適用を指示できます。**

これにより、利用者が最新の品質更新プログラムの適用を放置しているような場合でも、管理者からの指示で品質更新プログラムの適用を促すことができます。



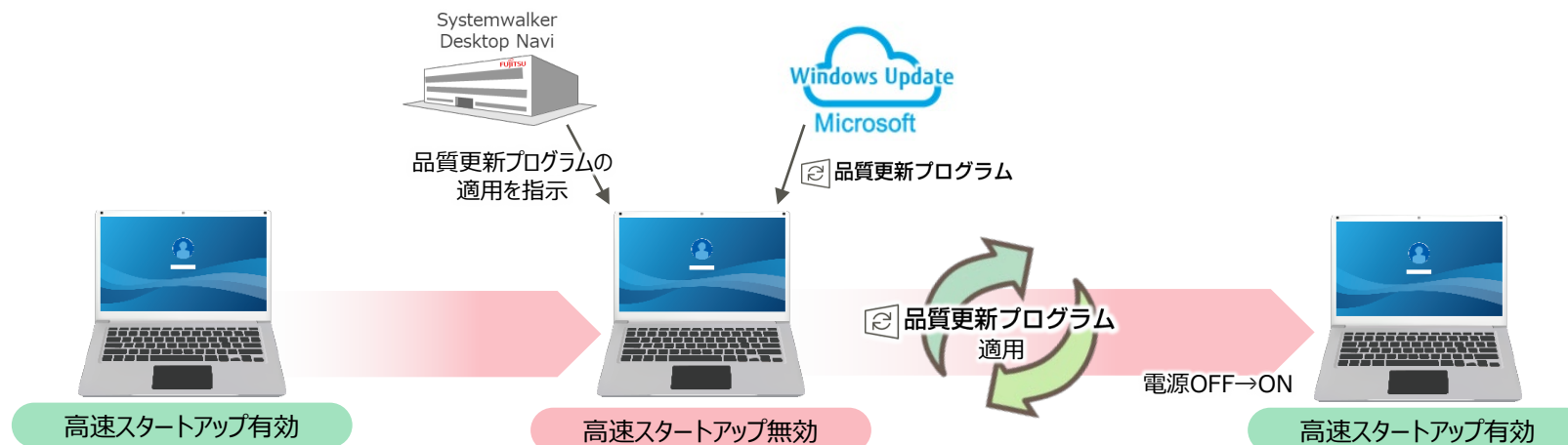
Windows® 10 更新支援機能

更新プログラム適用後の一時的な高速スタートアップ無効化

Windows 8 以降のOSでは高速スタートアップという機能が搭載されています。本機能は、PCの起動時間が大幅に短縮されるというメリットがある一方、Windows Updateが正しく適用されないといったデメリットもあります。

この結果、利用者はWindows Updateを実行済みと考えているにもかかわらず、内部的には更新プログラムが正しく適用されていないということがありました。

こうした問題を回避するため、Systemwalker Desktop Naviからの適用指示で更新プログラムを適用した場合、一時的に高速スタートアップ機能を無効にして、次回PC起動時に正しく更新プログラムを適用できるようになっています。



⚠ 本機能に関する留意事項

高速スタートアップが無効となるため、更新プログラム適用後の次回PC起動には時間がかかる場合があります。高速スタートアップが無効化されるのは更新プログラム適用後のPC起動時のみで、2回目以降の起動時には高速スタートアップ機能が再度有効となります。
(※高速スタートアップを自動切換するかどうかは設定で変更可能です)

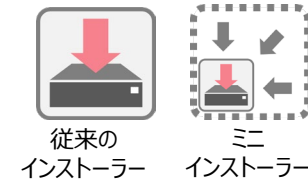
ミニインストーラー

Windows PCを管理対象としてSystemwalker Desktop Naviをご利用いただく場合、管理対象PCにエージェントプログラムのインストールが必須となりますが、ファイルサイズの大きいインストーラーを利用者に配付する場合、お客様環境によっては「メールに添付して利用者に送付することができない」、「利用者がアクセスできるファイルサーバを用意する必要がある」等の問題が発生する場合があります。

「ミニインストーラー（ダウンローダー）作成機能」は、上記のような環境下でもSystemwalker Desktop Naviのエージェント展開を可能にする機能です。本機能で作成したミニインストーラーはファイルサイズが小さく、メールでの配付も可能となります。ミニインストーラーを実行すれば、データセンターに保存されたインストーラー本体をダウンロードしてインストールします。

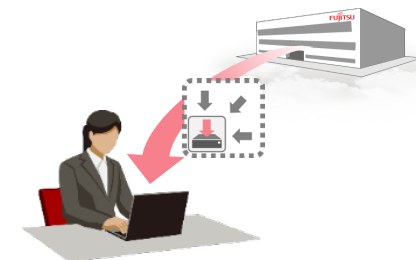
インストーラーサイズを大幅に縮小し、利用者への配付が容易に

スタンドアロンインストーラーと比較して、ファイルサイズを大幅に縮小したミニインストーラーを作成できます。作成したミニインストーラーを保存しておくためのファイルサーバなどを用意する必要もなく、メールに添付して利用者へインストーラーを配付できるようになります。



インストーラーをクラウド保存可能

作成したミニインストーラーはデータセンターに保存され、利用者も直接データセンターからダウンロードして入手できます。管理者は、利用者に対してダウンロードURLを通知するだけでエージェントを配付できます。



⚠ 本機能に関する留意事項

- ミニインストーラー実行時、インストール用プログラム本体はデータセンターからダウンロードされます。このため、ミニインストーラー実行時にはインターネット接続環境が必須となります。
- データセンターに保存できるミニインストーラー（とインストーラー本体）は最大5種類となります。

エージェントのキッティング対応

PCを大量展開する場合、1台のPCで環境を整えた上でそのPCのディスクイメージを雛形として展開するという手法（キッティング）が用いられます。Systemwalker Desktop Navi のWindowsエージェントプログラムはキッティングによる展開に対応しており、またキッティング展開時における資産管理番号も柔軟な採番が可能です。

雛形PCにエージェントを導入してキッティングによる展開が可能

キッティング用インストーラーを使用してSystemwalker Desktop NaviをインストールしたPCを雛形(マスタイメージ)として展開することで、Systemwalker Desktop Naviを容易に展開できます。展開後のPCでは、Systemwalker Desktop Naviエージェントの動作開始時点で資産管理番号が自動採番され、データセンターに登録されます。これにより、Systemwalker Desktop Navi展開時におけるシステム管理者・端末利用者双方の作業負荷を大幅に削減できます。



柔軟な資産管理番号の自動採番

コンピュータ名を使用した資産管理番号の自動採番方法に加え、

- PCの個体識別情報（HDDのシリアル番号、MACアドレス）による自動採番
- プレフィックス + 連番による自動採番
- PCのレジストリキーの値による自動採番
- ユーザー定義辞書に基づく自動採番

が可能です。これにより柔軟な資産管理番号の自動採番と、自動採番時における資産管理番号の重複エラー発生を防止します。

4. 機能紹介 ～オプションサービス～

- ログ強化 オプション
- 環境更新 オプション
- リモートモニタリング オプション
- インターネットサポート オプション

ファイル操作ログ収集機能とは

『ログ強化オプション』をご利用いただくと、利用者によるPC上のファイル操作やフォルダ操作をログとして取得することができます。ファイル操作ログを取得することで、利用者の不正なファイル操作を抑止するとともに、万が一情報漏えい事故などのセキュリティインシデントが発生した場合においても、ログ履歴の分析から、原因特定までに要する時間や作業負荷を大幅に削減することが可能となります。



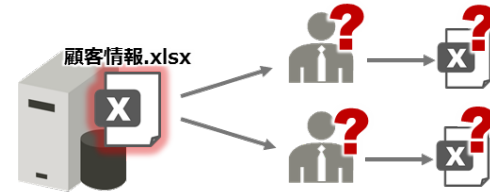
■ ファイル操作ログ収集機能 ～ファイル操作の追跡～

情報漏えいが発生した場合、いつ、誰が、どのようにして情報を漏えいさせたのかを究明する必要があります。その際に有効なのがファイル操作ログの追跡機能です。ファイル操作ログの追跡機能では、任意のファイル操作ログを起点として、その前後のファイル操作を確認することができます。

追跡のケース① 流出した情報の中身から、ファイルサーバに保存されている「顧客情報.xlsx」が流出したと思われる。



この情報はファイルサーバ上の「顧客情報.xlsx」のようだ。
誰が「顧客情報.xlsx」にアクセスしたんだろう...？

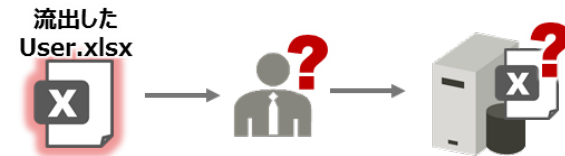


このようなケースでは、**流出した情報が記載されているファイルに誰がアクセスしたのか**ということを起点に、アクセスした人がファイルをその後どうしたのか、**未来に向かって操作を追跡**する必要があります。

追跡のケース② 顧客情報が記載された「User.xlsx」が流出したことが判明したが流出元の情報が不明。



流出した情報の出所が不明だ...。
まずは流出した「User.xlsx」というファイルを扱っている人がいないか確認してみよう。

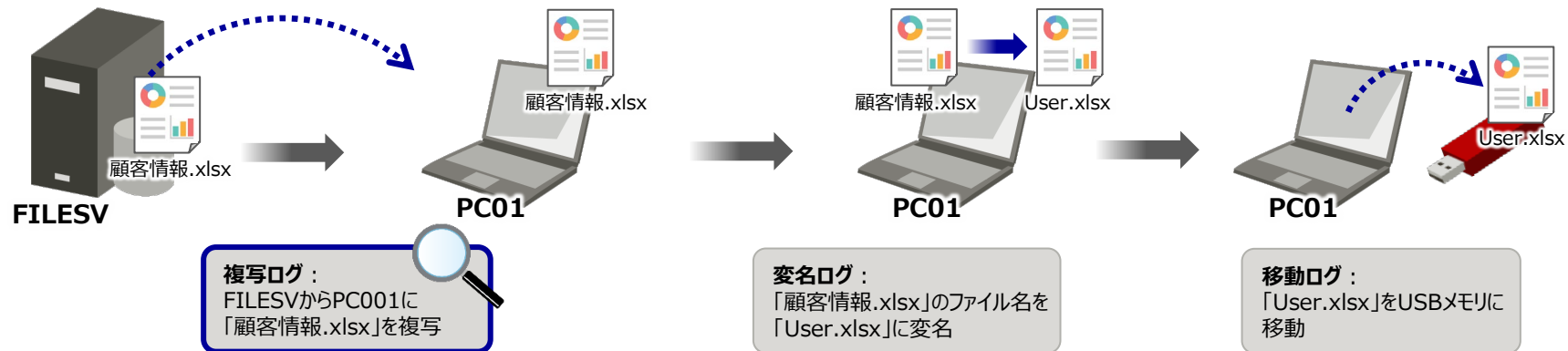


このようなケースでは、**流出したファイル名を扱っている人がいないか**ということを起点に、そのファイルが何を元に作成されたものなのか**過去に遡って操作を追跡**する必要があります。

■ ファイル操作ログ収集機能 ～フォワードトレース～

追跡のケース①

流出した情報の中身から、ファイルサーバに保存されている「顧客情報.xlsx」が流出したと思われる。
ファイル操作ログを検索すると、PC01で「顧客情報.xlsx」を「User.xlsx」という名前に変名しているログが見つかった。



フォワードトレース： 任意のファイル操作ログを起点に以降のファイル操作を追跡

フォワードトレースを行うことで、

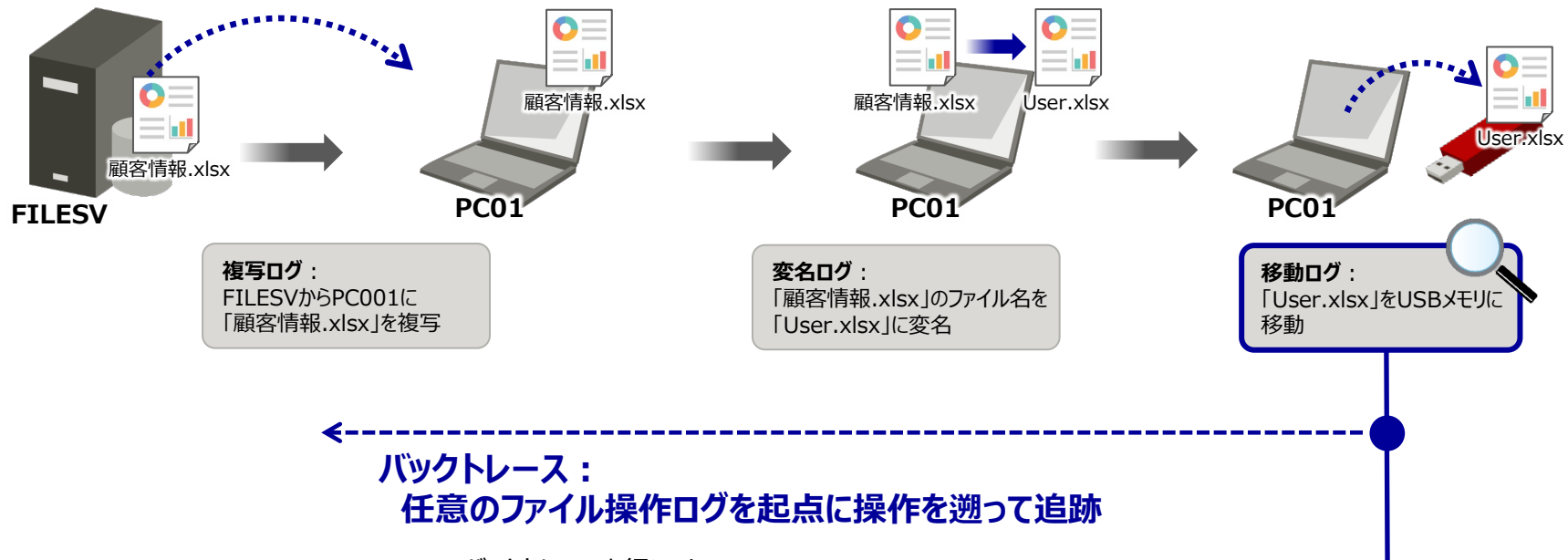
- ・ 「顧客情報.xlsx」を「User.xlsx」に変名した
- ・ 「User.xlsx」をUSBメモリに移動した

ことを追跡できます。

■ ファイル操作ログ収集機能 ～バックトレース～

追跡のケース②

顧客情報が記載された「User.xlsx」が流出したことが判明したが流出元の情報が不明。
ログ強化を検索すると、PC01で「User.xlsx」を参照しているログが見つかった。



バックトレースを行うことで、

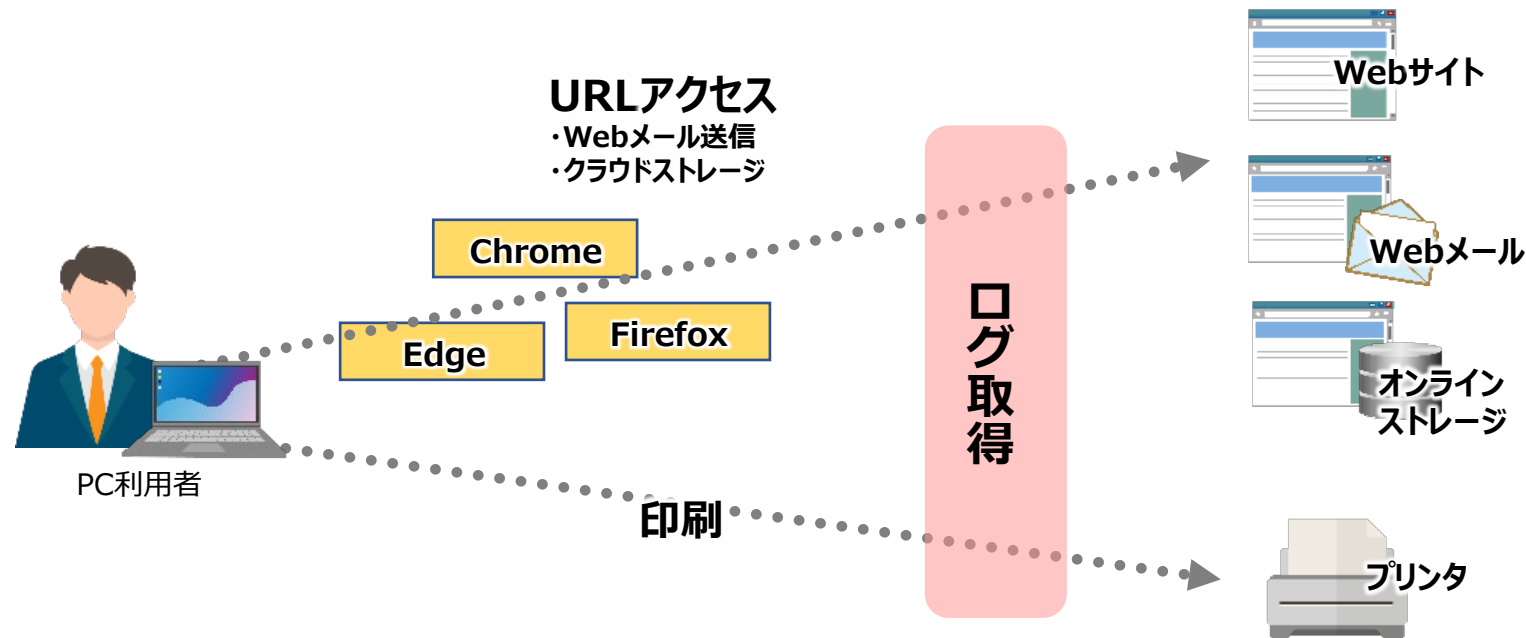
- ・「User.xlsx」は「顧客情報.xlsx」を変名した
- ・「顧客情報.xlsx」は、FILESV上に保存されていたものをPC01にコピーしたことを追跡できます。

Webアクセスログ収集

近年、企業におけるIT基盤（メール、ストレージ等）のSaaS利用が普及し、Webブラウザは従来のWebサイト閲覧に止まらず、様々な用途に利用されています。このため、従業員の行動を把握するためにはWebブラウザ上での操作を把握することが重要になってきます。

ログ強化オプションでは、基本サービスでサポートしているInternet ExplorerでのURLアクセスログ取得に加え、Chrome、Edge、Firefox上でのWebサイト閲覧・Webメール送信・オンラインストレージへのアクセスログ収集に対応します。

また、印刷された紙媒体による情報漏えいに備え、印刷ログの取得にも対応します。



シグネチャ検知



システム管理者がファイル操作に関する検出ルールとなるシグネチャ（操作時間帯、ファイル名キーワード、対象ファイル数など）を事前設定することで、管理者に代わり採取したログを常時監視して、シグネチャに該当するファイル操作が発生した場合を危険行為として判断して管理者に対してアラートを通知します。これにより情報漏えいの危険性がある操作を早期に検知できます。

ログ強化オプションがカバーする情報漏えい対策範囲



Systemwalker Desktop Navi のシグネチャ検知機能

● 特定WEBサイトへのアクセス

- ① アクセス先に含まれるキーワード
- ② アクセス曜日
- ③ アクセス時間帯

● 社外へのファイル持ち出し

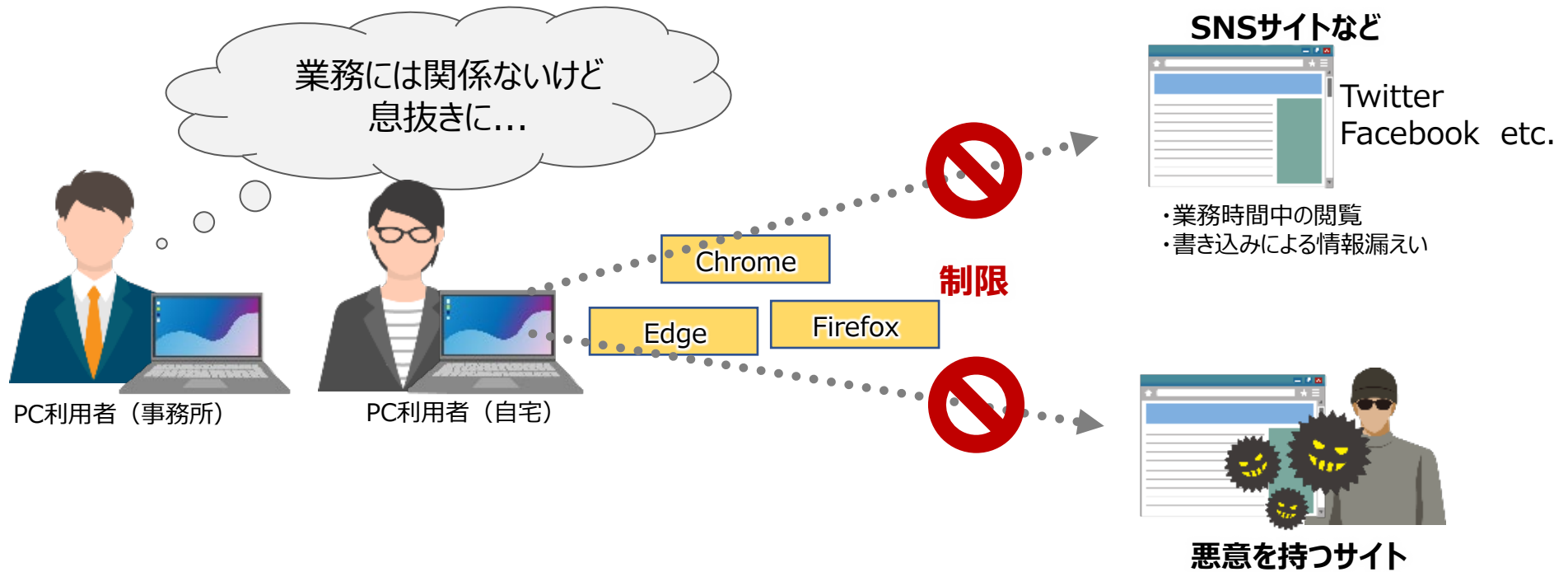
- ① 持ち出しデバイス（USB,CD/DVD,メール）
- ② 持ち出すファイル名に含まれるキーワード
- ③ アクセス曜日
- ④ アクセス時間帯

● 個人メール利用

- ① 宛先に含まれるキーワード
- ② 件名に含まれるキーワード
- ③ 発信曜日
- ④ 発信時間帯

Webアクセス制限

Chrome、Edge、Firefoxを使用したWebサイトへのアクセスやデータアップロード・ダウンロード制限に対応し、これらの操作を行った際に記録されるアラートもログの一つとして分析対象とすることができます。



■ ファイル・フォルダのリモート配信・削除 W

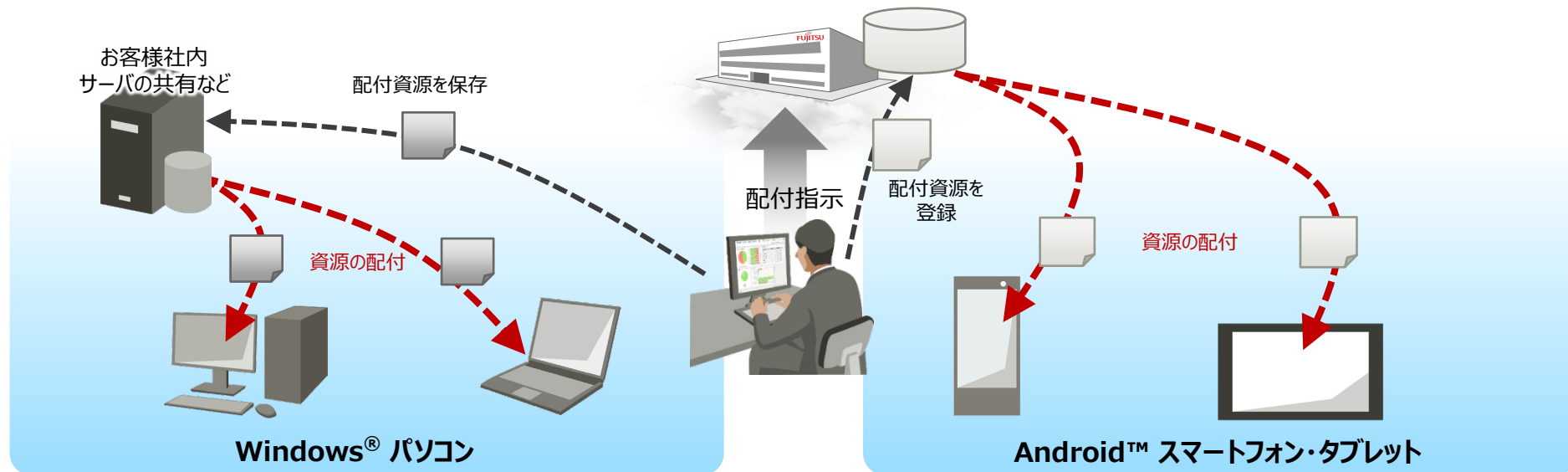
管理者が作成したスクリプト（BAT、WSHなど）を配信資源として登録し、パソコンに配信して実行できます。パソコンの設定変更やソフトウェアのインストールに利用できます。

■ ソフトウェアのリモートインストール A

Androidソフトウェア（apk）を配信資源として登録し、Androidスマートフォン・タブレットに配信・インストールできます。

■ ファイル・フォルダのリモート配信・削除 W、A

管理者が指定した任意のファイルやフォルダを配信資源として登録し、パソコンやAndroidスマートフォン・タブレットに配信できます。また、配信だけでなく、パソコンやAndroidスマートフォン・タブレット上に存在しているファイル・フォルダを削除することもできます。



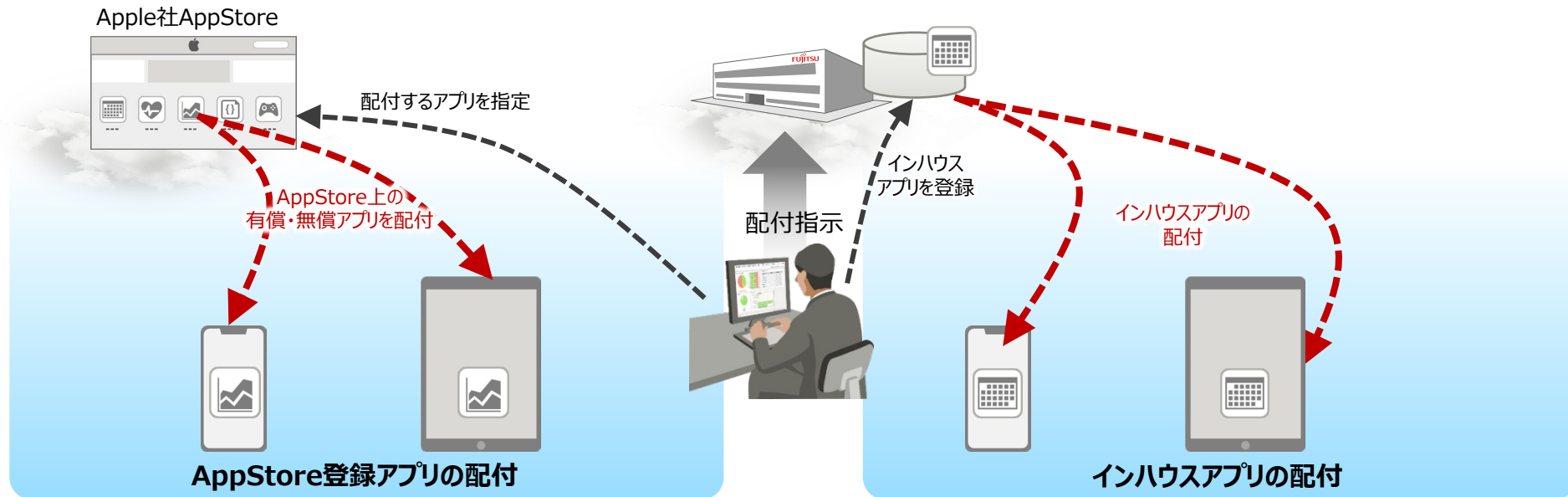
⚠️・Windows®で本機能をご利用いただく場合、配信先のパソコンから参照可能なファイルサーバをお客様環境内にご用意いただき、インストーラーやファイル・フォルダを格納していただく必要があります。
・Android端末への環境更新につきましては、本書「留意事項・制限事項」の「Android™・iOS端末への資源配信について」をご確認ください。

■ AppStoreに登録されているアプリの配付※1

Apple社のAppStoreに登録されているアプリをiOSデバイスに配付することができます。

■ インハウスアプリの配付※2

お客様が独自で開発したインハウスアプリをiOSデバイスに配付することができます。



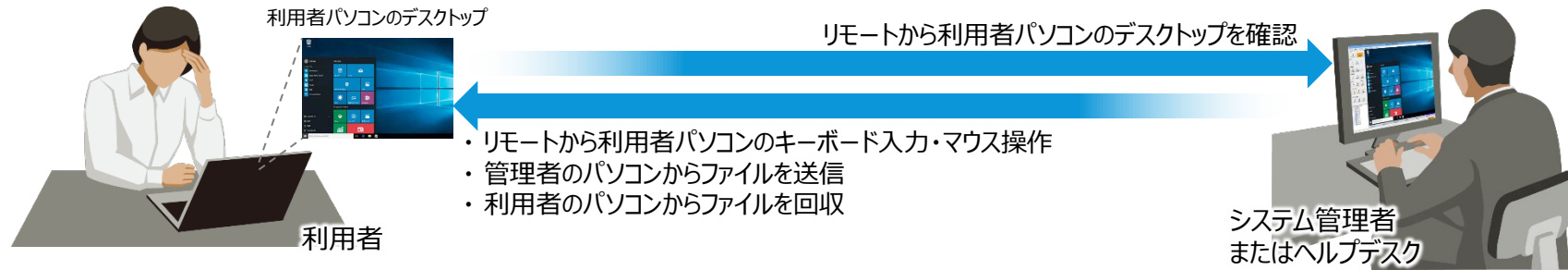
※1：有償アプリを配付する場合、AppStore ボリュームライセンスプログラムでアプリをご購入いただく必要があります。有償アプリ配付時には、アプリ購入時に入手できる引換券コードを指定していただく必要があります。

※2：インハウスアプリを配付する場合、お客様はApple社と「iOS Developer Enterprise Program」をご契約いただく必要があります。

⚠️・iOS端末の環境更新につきましては、本書「留意事項・制限事項」の「Android™・iOS端末への資源配付について」をご確認ください。

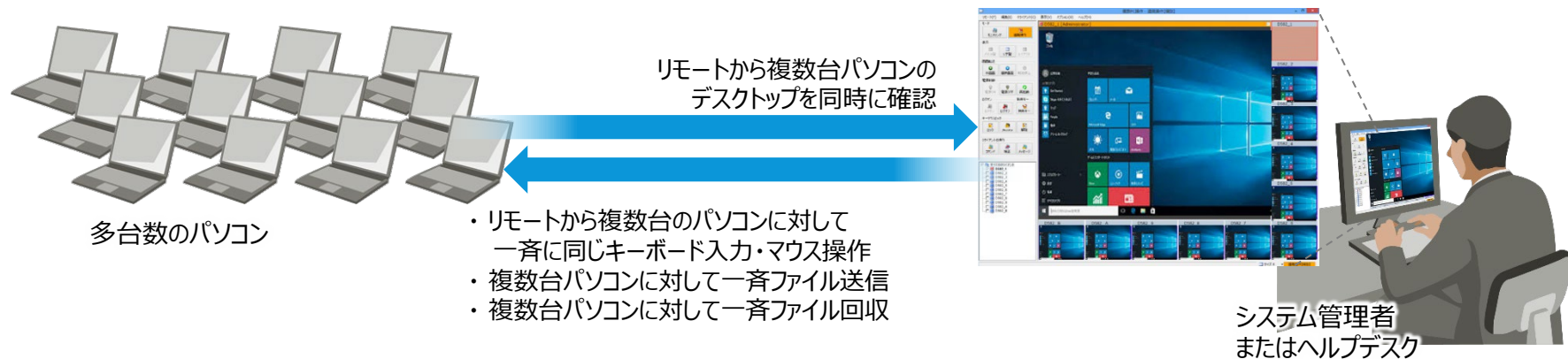
1対1のモニタリングでトラブル対応コスト削減

利用者のパソコンのデスクトップをリモートから確認・操作することができます。本機能を利用することで、システム管理者はトラブル発生時の状況確認や対応をスムーズに行うことができます。



多台数パソコン一斉操作で作業コスト削減

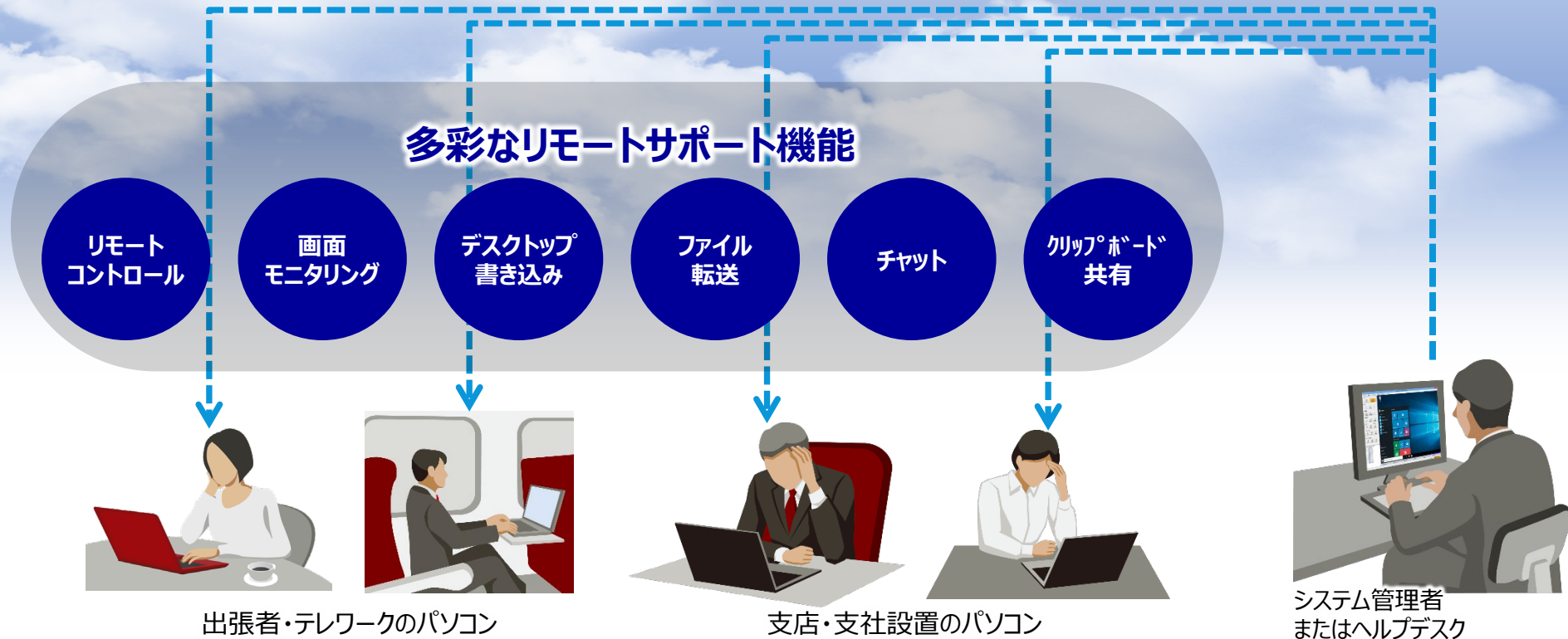
複数台のパソコンを一斉にモニタリング・操作することができます。本機能を利用することで、システム管理者は利用者パソコンのセットアップや環境変更時の作業負荷を大幅に削減することができます。



インターネット経由のモニタリングで遠隔地のトラブル対応を効率化

システム管理者は、インターネットを経由して利用者パソコンをリモートモニタリング・操作することができます。「支店・支社に設置されたパソコン」、「出張者が社外に持出中のパソコン」や「テレワーク社員のパソコン」など、遠隔地のパソコンのサポート作業を大幅に効率化することができます。

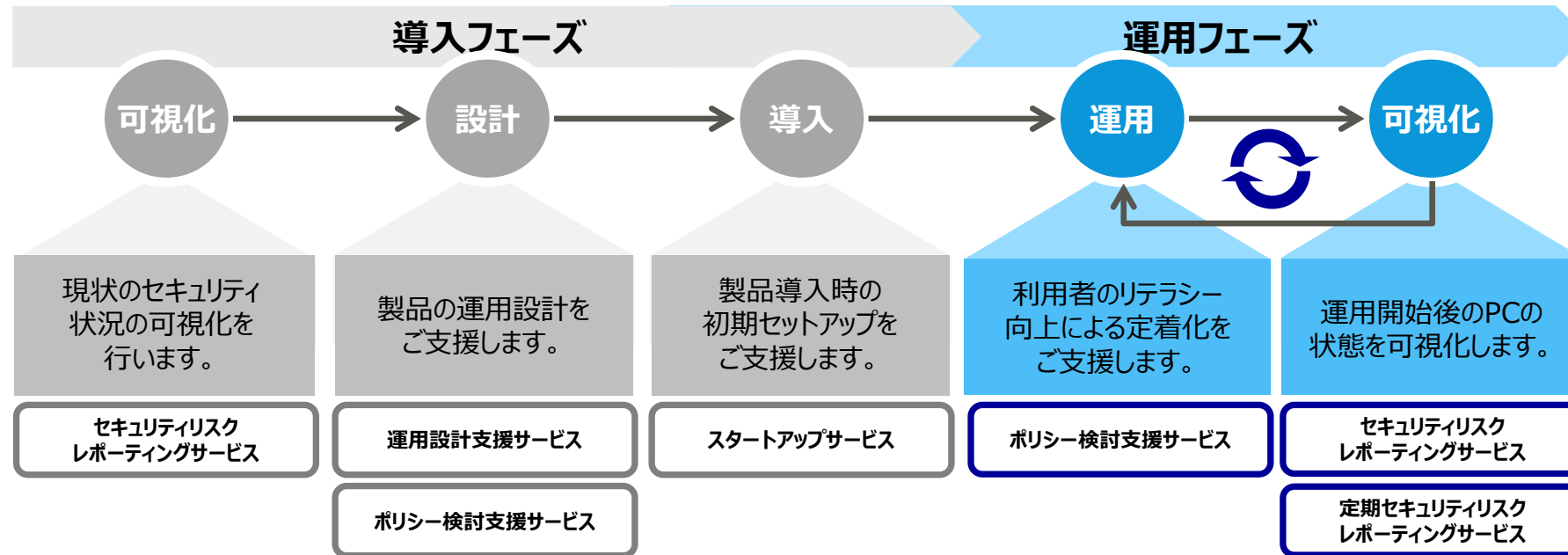
通信データはSSLで暗号化 第三者による盗聴から通信内容を保護



5. SDMサービス

- SDMサービスとは
- SDMサービス サービスメニュー概要

SDMサービスは、お客様にSystemwalker Desktop Naviをご活用いただくため、お客様環境へのスムーズなサービス導入とセキュリティ定着化をご支援する各種サービス群です。



導入フェーズ ポリシーや運用設計のご支援や、製品導入の初期作業のご支援を行うサービスをご提供しており、Systemwalker Desktop Naviのスムーズな導入をご支援します。

運用フェーズ Systemwalker Desktop Naviが収集した情報をもとに、端末上のセキュリティリスクを分析し、報告書にまとめご報告するサービスを提供しており、セキュリティ運用の定着化をご支援します。

導入フェーズ向けSDMサービス

運用設計支援サービス

Systemwalker Desktop Navi導入の運用設計フェーズにおいて、Systemwalker Desktop Naviの運用方法および設定するパラメタ設計作業をご支援いたします。

ポリシー検討支援サービス

Systemwalker Desktop Navi導入の運用設計フェーズにおいて、お客様のセキュリティポリシーや運用ルールに則り、ポリシーの検討作業をご支援いたします。

スタートアップサービス

Systemwalker Desktop Naviの製品導入フェーズにおいて、サービスを利用開始するための動作環境の作成（ポリシー設定の代行、クライアント端末へのエージェント導入など）をご支援いたします。

運用フェーズ向けSDMサービス

セキュリティリスクレポートサービス

Systemwalker Desktop Naviが収集したハードウェア・ソフトウェアインベントリやセキュリティ診断結果を元に、お客様が保有するPC等のセキュリティリスクを分析し報告するサービスです。診断結果は、「セキュリティ診断結果報告書」としてまとめ、お客様に提出いたします。

定期セキュリティリスクレポートサービス

「セキュリティリスクレポートサービス」同様、Systemwalker Desktop Naviが収集したハードウェア・ソフトウェアインベントリやセキュリティ診断結果を元に、お客様が保有するPC等のセキュリティリスクを分析して報告するサービスです。

本サービスをご契約期間中、定期的（毎月一回等）にセキュリティリスクの分析の実施と報告書を提出いたします。

6. サービス機能一覧

- 基本サービス
- オプションサービス

基本サービス①

			Windows® Client OS	Windows Server® OS	Android™	iOS
セキュリティ						
セキュリティ診断						
1	OS診断	管理者が指定したバージョンのOSが使用されているか、メーカーのサポート期限が切れたOSを使用していないかなどを診断します。また、適切にOSパッチが適用されているかどうかの診断もできます。	○	○	○	-
2	ウイルス対策ソフト診断	ウイルス対策ソフト導入状況や、定義ファイルの更新状況などを診断します。また、ウイルススキャンの設定内容等についても診断できます。	○	○	○※1	-
3	ソフトウェアバージョン診断	インストールされているAdobe Reader・Acrobat・Flash Player、Java Runtimeなどバージョンについて診断します。	○	○	○※2	-
4	パスワード設定診断	ログオンパスワード（ロックパスワード）、スクリーンセーバのパスワード、PCのHDDやBIOSのパスワードの設定状況を診断します。	○	○	○※3	○※4
5	ソフトウェア設定診断	IEやOutlookなどの設定内容について診断します。	○	○	-	-
6	禁止ソフトウェア診断	管理者が指定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診断します。	○	○	-	○
7	必須ソフトウェア診断	管理者が指定したソフトウェアがインストールされていることを診断します。	○	○	○	○
8	暗号化診断	内蔵HDDがハードウェアまたはソフトウェア的に暗号化されているかどうかを診断します。	○	○	-	-
9	汎用セキュリティ診断	PC上のファイルの有無やレジストリの値を診断条件として、任意のセキュリティ診断項目を追加できます。	○	○	-	-
10	オフライン端末診断	ネットワークに接続されていないオフライン端末についてセキュリティ診断します。	○	○	-	-

※1：ウイルス対策ソフトのインストール有無のみ診断できます。

※2：Adobe Flash Player、Adobe Reader のみ診断できます。

※3：「パスコード以上」、「PINコード以上」など、指定したセキュリティロックレベルを強制適用します。

※4：iOSデバイスのパスコード設定を強制します。

基本サービス②

			Windows® Client OS	Windows Server® OS	Android™	iOS
セキュリティ						
操作・利用制限						
1	ソフトウェア起動制限	管理者が指定した任意のソフトウェアの起動を制限できます。	○	—	○	○※5
2	印刷制限	管理者が指定した任意のソフトウェアからの印刷を制限できます。	○	—	—	—
3	URLアクセス制限	管理者が指定した任意のURLについて、ブラウザでのアクセスを制限できます。	○	—	○	—
4	Webサイトアップロード・ダウンロード制限	許可されたWebサイト（URL）以外のサイトに対して、ファイルのダウンロードやアップロードを制限できます。	○	—	—	—
5	メール送信制限	許可された宛先ドメイン以外へのメール送信やメールでのファイルの添付を制限できます。	○	—	—	—
6	ネットワークドライブ利用制限	ネットワークドライブの利用を制限できます。	○	—	—	—
デバイス接続制限						
1	USBデバイス利用制限	USBメモリやハードディスクなど、USBデバイスの利用を制限できます。	○	—	—	—
2	CD/DVDドライブ利用制限	CDやDVDといった光学ドライブの利用を制限できます。	○	—	—	—
3	Wi-Fi接続制限	Wi-Fi接続を制限できます。また、管理者が登録した任意のアクセスポイントのみ接続を許可することが出来ます。	○※6	—	○	—
4	Bluetooth接続制限	Bluetoothによる外部デバイスの接続をすべて制限したり、任意のBluetoothデバイス種別を指定して許可・禁止することが可能です。	○※7	—	○	—
5	赤外線接続制限	赤外線通信ポート（IrDAポート）が搭載されているPCで、赤外線通信による外部接続を制限できます。	○	—	—	—
6	PCカード接続制限	PCMCIAや、PCIExpressのカードスロットが搭載されているPCで、スロットに挿入されているカードの利用を制限できます。	○	—	—	—
7	IEEE1394接続制限	IEEE1394ポート経由での外部機器接続を制限できます。	○	—	—	—
8	パラレル・シリアルポート接続制限	パラレルポート、シリアルポート経由での外部機器接続を制限できます。	○	—	—	—

※5：Safari、SiriといったiOS標準アプリの一部のみ起動を制限できます。

※6：接続を許可するアクセスポイントはBSSID（アクセスポイントのMACアドレス）で指定します。

※7：PC、周辺機器、ウェアラブルといったBluetoothの機器種別を指定して制限できます。機器を個体識別して許可・禁止することはできません。

基本サービス③

			Windows® Client OS	Windows Server® OS	Android™	iOS
セキュリティ						
紛失対策						
1	リモートロック	リモートから端末をロックできます。	○※8	—	○	○
2	ローカルロック	端末へのログインに任意の回数失敗した場合、端末をロックできます。	○※8	—	○	—
3	リモートデータ通信遮断	リモートからスマートフォンのデータ通信を無効化できます。	—	—	○	—
4	リモートデータ削除	リモートから端末上に保存されているデータを削除できます。	○	—	○	—
5	リモートワイプ	リモートから端末を初期化できます。	○※9	—	○	○
6	ローカルワイプ	端末へのログインに任意の回数失敗した場合、端末を初期化できます。	○※9	—	○	○
7	位置情報取得	端末の位置情報を取得して確認することができます。	—	—	○	—
スマートフォン向け操作・利用制限						
1	電話発信先制限	指定した電話番号以外への電話発信を制限できます。	—	—	○	—
2	内蔵カメラ利用制限	内蔵カメラを無効化して利用を制限できます。	—	—	○	○
3	Bluetooth利用制限	内蔵Bluetoothを無効化して利用を制限できます。	—	—	○	—
4	Wi-Fi利用制限	内蔵Wi-Fiを無効化して利用を制限できます。 また、無線アクセスポイント（SSID）を指定して、指定されたアクセスポイント以外の利用を制限できます。	—	—	○	—
5	SDカード利用制限	SDカードの利用を制限できます。	—	—	○	—
6	USB接続制限	スマートフォンへのUSB接続を制限できます。	—	—	○	—
7	テザリング制限	テザリングを制限できます。	—	—	○	—
8	Androidホームアプリ	ホーム画面上のショートカットを固定し、利用者が起動できるソフトウェアを制限できます。	—	—	○	—

※8：対象のPC上に登録されているローカルユーザアカウントを無効化します。

詳細は「8.留意事項・制限事項」の「Windowsの紛失対策について」をご確認ください。

※9：Windowsによるワイプ処理を行うには対象のPCのHDDがBitLockerで暗号化されている必要があります。

詳細は「8.留意事項・制限事項」の「Windowsの紛失対策について」をご確認ください。

基本サービス④

			Windows® Client OS	Windows Server® OS	Android™	iOS
ログ管理						
ログ収集						
1	ソフトウェア起動・終了ログ	ソフトウェアの起動や終了をログとして収集できます。	○	—	○※10	—
2	ソフトウェアインストール・アンインストールログ	ソフトウェアのインストールやアンインストールのログを収集できます。	—	—	○	—
3	メール送信ログ	メール送信時の宛先、件名、送信日時等のログを収集できます。	○※11	—	—	—
4	URLアクセスログ	ブラウザからアクセスしたURLをログとして収集できます。	○※12	—	○	—
5	ファイル持ち出しログ	USBメモリや書き込み可能な光学ドライブへのファイル書き出しをログとして収集できます。	○	—	—	—
6	Webアップロード・ダウンロードログ	ブラウザを使用して、任意のWebサイトに関するファイルのアップロードやファイルのダウンロードをログとして収集できます。	○※12	—	—	—
7	ログオン・ログオフログ	端末へのユーザのログオン・ログオフをログとして収集できます。	○	—	—	—
8	電源状態ログ	端末の電源ON・OFF、スリープ移行・復帰などの電源状態をログとして収集できます。	○	—	○	—
資産統制						
1	ハードウェアインベントリ収集	端末のハードウェア情報を収集できます。	○	○	○	○
2	ソフトウェアインベントリ収集	端末にインストールされたソフトウェアの情報を収集できます。	○	○	○	○
3	ソフトウェアライセンス管理	ソフトウェアライセンス情報を登録し、端末から収集されたソフトウェアライセンスを突合し、ライセンスの利用状況を確認することができます。	○	○	—	—
4	レジストリ情報収集	任意のレジストリ情報を収集することができます。	○	○	—	—
5	オンライン棚卸	管理者が棚卸し指示を行うとクライアント側に通知が行われ、利用者自身で棚卸し処理を行うことができます。	○	○	—	—

※10：ソフトウェアの起動ログのみ取得可能です。

※11：Microsoft Outlookでのメール送信およびSMTPでのメール送信ログが取得できます。

※12：Microsoft Internet Explorerのみログが取得できます。

オプションサービス①

オプションサービスをご利用いただく場合、基本サービスのご契約が必須となります。

			Windows® Client OS	Windows Server® OS	Android™	iOS
システム運用						
環境更新オプション						
1	ファイル配付・フォルダ配付	任意のファイルやフォルダを配付することが出来ます。	○	—	○	—
2	スクリプト配付実行	作成したスクリプト（バッチファイル、WindowsScriptファイル等）を配付して、配付先の端末上で実行できます。	○	—	—	—
3	アプリケーション配付	AppStoreに登録されているiOSアプリのインストールを指示できます。 また、任意のapkファイルやお客様で作成したiOSアプリを配付・インストールすることもできます。	—	—	○	○
ログ強化オプション						
1	ファイル操作のログ取得	端末の上のファイル操作（参照・作成・更新・削除・複写など）をログとして記録することができます。	○	—	—	—
2	ファイル操作の追跡	任意のファイル操作ログを起点として、その前後のファイル操作を追跡することができます。	○	—	—	—
3	URLアクセスログ	Chrome、Edge、FirefoxでURLアクセスログが取得できる。	○	—	—	—
4	Webアップロード・ダウンロードログ	Chrome、Edge、FirefoxでWebサイトのデータアップロード・ダウンロードログが取得できる。	○	—	—	—
5	Webメール送信ログ	Webメール上でのメール送信ログを取得できる。	○	—	—	—
6	オンラインストレージログ	オンラインストレージへのアクセスログを取得できる。	○	—	—	—
7	印刷ログ	利用者が印刷したファイルのファイル名ログを取得できる。	○	—	—	—
8	URLアクセス制限	Chrome、Edge、FirefoxでURLアクセス制限ができる。	○	—	—	—
9	Webアップロード・ダウンロード制限	Chrome、Edge、FirefoxでWebサイトのデータアップロード・ダウンロードを制限できる。	○	—	—	—
10	操作ログからのシグネチャ検知	定義した閾値（シグネチャ）を外れるまたは超えるようなファイル操作を利用者が実行した場合、不正な操作の可能性があるとアラートする。	○	—	—	—
ログ強化 追加ストレージオプション ※ログ強化オプションのご契約が必須						
1	ログ強化オプション 保存ストレージ領域の拡張	ログ強化オプションで取得したログが記録されるデータベース（が格納されるストレージ）の領域を拡張することができます。 追加の単位は100GBです。	○	—	—	—

オプションサービス②

オプションサービスをご利用いただく場合、基本サービスのご契約が必須となります。

			Windows® Client OS	Windows Server® OS	Android™	iOS
システム運用						
リモートモニタリングオプション						
1	複数PCモニタリング・操作	管理者用PCから複数のPCを一斉にモニタリング・操作できます。	○	○	—	—
2	ファイル配付・回収	管理者用PCから複数のPCに対してファイルを配付したり回収できます。	○	○	—	—
3	クリップボード共有	管理者用PCのクリップボードに格納されたデータを複数のPC端末に送信できます。	○	○	—	—
インターネットサポートオプション						
1	インターネット経由のモニタリング・操作	管理者用PCからインターネットに接続されているPC（1台）をモニタリング・操作できます。	○	○	—	—
2	ポインタ・デスクトップペン	管理者用PCから接続先PCのデスクトップにペン描画して具体的に操作指示することができます。	○	○	—	—
3	ファイル転送	管理者用PCと接続先PCの双方向で、ドラッグ&ドロップのファイル転送が可能です。転送するファイルサイズに制限はありません。	○	○	—	—
4	テキストチャット	接続先PCのデスクトップに定型の画像（丸や矢印）を表示して、操作の指示、誘導を行います。	○	○	—	—

7. 動作環境

- 動作環境（管理対象機器）
- 動作環境（Webダッシュボード・オプションコンソール）
- ネットワーク環境
- サービスの基本動作概要

エージェント

Systemwalker Desktop Naviで管理対象にできる機器は、下記のOSが稼働する端末となります。
Windows、Android端末にはエージェントプログラムが、iOS端末には構成プロファイルがインストールされます。

Windows®		Android™ ※2	iOS・iPadOS
クライアントOS	サーバOS		
<ul style="list-style-type: none"> Windows® 10 Home ※1 Windows® 10 Pro ※1 Windows® 10 Pro for Workstations ※1 Windows® 10 Enterprise ※1 Windows® 10 Education ※1 Windows® 11 Home ※1 Windows® 11 Pro ※1 Windows® 11 Pro for Workstations ※1 Windows® 11 Enterprise ※1 Windows® 11 Education ※1 	<ul style="list-style-type: none"> Windows Server® 2012 Standard Windows Server® 2012 Datacenter Windows Server® 2012 R2 Standard Windows Server® 2012 R2 Datacenter Windows Server® 2016 Standard Windows Server® 2016 Datacenter Windows Server® 2019 Standard Windows Server® 2019 Datacenter Windows Server® 2022 Standard Windows Server® 2022 Datacenter 	<ul style="list-style-type: none"> Android™ 6.x Android™ 7.x Android™ 8.x Android™ 9.x Android™ 10.x Android™ 11.x Android™ 12.x Android™ 13.x 	<ul style="list-style-type: none"> iOS 5.x iOS 6.x iOS 7.x iOS 8.x iOS 9.x iOS 10.x iOS 11.x iOS 12.x iOS 13.x iPadOS 13.x iOS 14.x iPadOS 14.x iOS 15.x iPadOS 15.x iOS 16.x iPadOS 16.x

※1 ・ Windows® 10, 11では従来のデスクトップソフトウェアに加え、Windows® ストアソフトウェアが利用できますが、Systemwalker Desktop Naviのインベントリ収集機能では、Windows®ストアソフトウェアの情報を取得できません。
 ・ UEFI規格のパソコンをBIOS互換モードを使用している場合、セキュリティ診断機能のBIOSパスワード診断は正常に動作いたしません。

※2 動作検証済みのAndroid™端末およびAndroid OSバージョン毎の機能利用可否につきましては、弊社製品ホームページをご確認ください。

Systemwalker Desktop Navi ホームページ

<https://www.fujitsu.com/jp/software/systemwalker/desktop-navi/>



【OS提供元がサポートを終了したOS（サービスパック・機能アップデート含む）について】

Systemwalker Desktop Navi 動作環境OSに関してまして、OS提供元のサポート終了後のOS固有の問題、ならびにOS固有の問題に起因して発生する Systemwalker Desktop Navi の不具合等につきましては、対応いたしかねますのでご了承ください。

■ 管理者向けダッシュボード

管理者向けWebダッシュボードにアクセスするには、以下のWebブラウザが必要です。

- Microsoft® Edge ※1
- Mozilla Firefox 42.0 以降※2

※1 Chromium版 Edgeブラウザのみをサポートします。

※2 Windows® Operating System上で動作するWebブラウザのみをサポートします。

■ オプションコンソール

「環境既定オプション」、「リモートモニタリングオプション」、「インターネットサポートオプション」をお使いいただく場合、管理用パソコンにオプション用のコンソールプログラムをインストールしていただく必要があります。オプションコンソールの動作環境は、利用者端末と同一要件のWindows® Operating Systemと同一となります。

■ エージェント・オプションコンソール共通

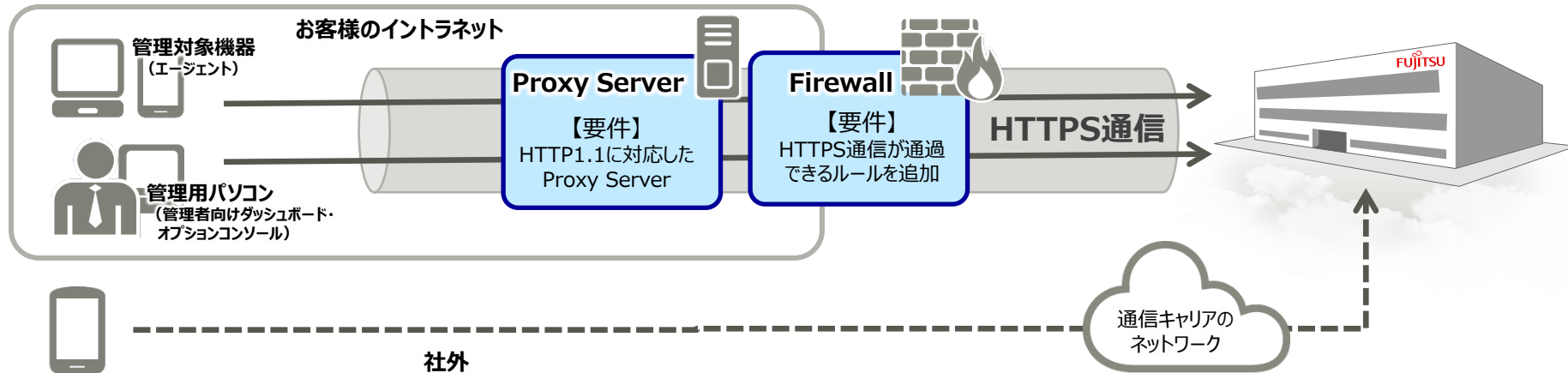
Windowsにエージェントまたはオプションコンソールをインストールする場合、事前に「Microsoft® .NET Framework 3.5」を導入していただく必要があります。



64ビットOSの場合でも、32ビット版.NET Frameworkをインストールしてください。
Windows® 8以降、Windows Server® 2012以降は、OSインストール時にMicrosoft® .NET Framework 3.5が自動的にインストールされません。
コントロールパネルの「プログラムと機能」から.NET Framework 3.5を有効にしてください。

ネットワーク要件

Systemwalker Desktop Naviをご利用いただく場合、管理対象機器および管理者向けダッシュボード、オプションコンソールを利用するパソコンはインターネットに接続されている必要があります。



- インターネットへの接続にプロキシサーバを経由する場合、プロキシサーバはHTTP1.1に対応している必要があります。
- インターネットへの接続にファイアウォールを経由する場合、ファイアウォールでHTTPS通信を許可するルールを追加していただく必要があります。



【Android™、iOSデバイスをWi-Fi環境のみで利用する場合】

Android™やiOSデバイスをWi-Fi環境のみでご利用いただく場合で、かつインターネット接続にファイアウォールを経由する場合、ファイアウォールで「5223/tcp」ポートが開放されている必要があります。



【参考情報】iOSデバイスをWi-Fi環境でご利用いただく場合のファイアウォールの詳細設定につきましては、以下のApple社公開情報を参照してください。

- ・Apple のプッシュ通知が届かない場合
<https://support.apple.com/ja-jp/HT203609>
- ・iOS Developer Library “Technical Note TN2265: Troubleshooting Push Notifications”
https://developer.apple.com/library/ios/technotes/tn2265/_index.html

■ 定期通信と手動通信による動作

Systemwalker Desktop Naviエージェントと弊社データセンター間の通信には、「定期通信」と「手動による通信」の2種類の通信があります。「定期通信」はポリシーで定義された時間間隔でサーバーと自動で通信を行います。通信間隔は初期値「3時間」です。

※ スマートデバイスに対する紛失対策指示については、即時通信を行い命令を発行します。

■ セキュリティ診断の実行頻度

Systemwalker Desktop Naviのセキュリティ診断は、管理者が任意のタイミングでスケジュール実行することができます。

- ・ Windows® : 最大3回/日 実行曜日・時刻を指定可能
- ・ Android™ : 診断間隔を指定可能
- ・ iOS : 指定不可

■ データセンターに送信・保存されるデータ

Systemwalker Desktop Naviを導入いただいた場合、お客様のパソコンやスマートデバイスから以下のような情報が弊社データセンターに送信され保存されます。

種別	データの内容
必須で送信される情報	パソコン : コンピュータ名、ネットワーク設定（IPアドレス、サブネットマスク、DNSサーバ、デフォルトゲートウェイ）、PCメーカー、PC型名、CPU情報、メモリ容量、HDD容量、HDD型名、BIOS情報（バージョン等）、Windows OS種別（SPLレベル含む）、ログオンアカウント名、インストールされているソフトウェアの名前およびバージョン、前回の終了日時など スマートフォン : OSバージョン、通信キャリア名、スマートフォンのモデル名、SIM番号、電話番号、MACアドレス（Wi-Fi）、インストールされているソフトウェアの名前、IMEI(International Mobile Equipment Identity)、シリアル番号など
使用する機能や管理者が任意で入力した際に送信される情報	共通 : 組織名、機器使用者の氏名、機器管理番号、購買情報（担当者氏名、費用など）、リース/レンタル情報（開始終了日・リース先情報・契約番号・費用など）

8. 留意事項・制限事項

- 基本サービスのログ保存期間について
- ログ強化オプションサービスのログ保存期間について
- Windows®の紛失対策について
- Android™ OSの制限事項について
- Android™・iOS端末への資源配付について

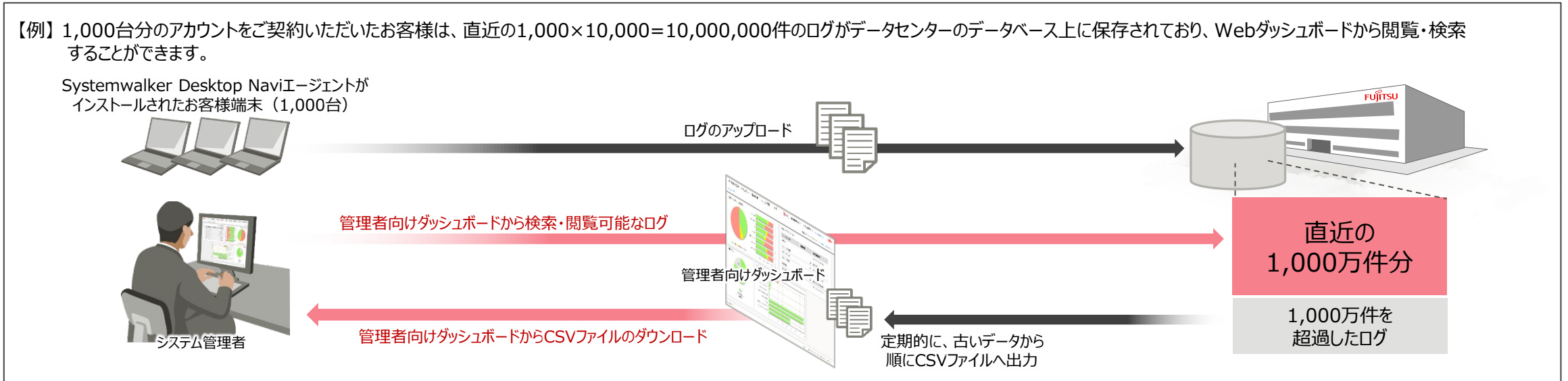


Systemwalker Desktop Naviをお使いいただく場合、本章でご紹介させていただく内容以外にもいくつかの制限事項・留意事項がございます。
製品ホームページにある「[Systemwalker Desktop Navi ご利用に際しての制限事項/留意事項について](#)」を事前にご確認くださいようお願い申し上げます。

<https://www.fujitsu.com/jp/software/systemwalker/desktop-navi/>

■ 管理者向けダッシュボードで閲覧可能なログ

お客様の端末から収集された各種ログについて、データセンター上に保存されます。
管理者向けダッシュボードから閲覧や検索が可能なログの件数は、**直近の『ご契約端末台数×10,000』(件)**となります。



データベース上での保存上限を超えたログに関しては、古いものから順に定期的にCSV形式のログファイルとして出力されます。
出力されたCSVログファイルは、お客様のWebダッシュボードからダウンロードしていただくことができます。

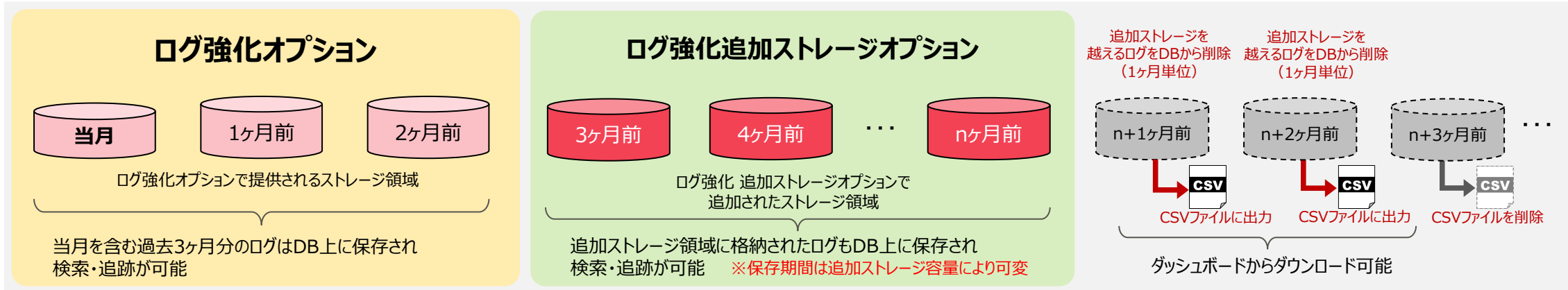
■ CSV出力されたログファイルの保存期間

出力されたCSVログファイルは管理者向けダッシュボードからダウンロードすることができます。

管理者向けダッシュボードからCSVログファイルがダウンロード可能な期間は、各CSVログファイルが出力されてから2ヶ月間となっており、この期間を超えると自動的に削除されますのでご注意ください。

管理者向けダッシュボードで閲覧可能なログ

ログ強化オプションをご契約いただいた場合、PCから収集した各種操作ログは**最大で当月を含む過去3ヶ月分がデータベース上に記録され、Webダッシュボード上で表示・検索できます**。ログ強化 追加ストレージオプションを別途ご契約いただくと、各種操作ログが記録されるデータベース領域を100GB単位で拡張^{※1}することができ、データベースへのログ保存期間を延長^{※2}できます。



データベース上での保存上限を超えたログに関しては、古いものから順に定期的にCSV形式のログファイルとして出力されます。出力されたCSVログファイルは、お客様のWebダッシュボードからダウンロードしていただくことができます。

※1: 拡張できる最大のデータベース領域は14TBです。

※2: ログ強化追加ストレージオプションでデータベース領域を拡張して延長できる保存期間はお客様環境に依存します。Webダッシュボード上では拡張したデータベース領域でどの程度保存期間が延長できるのかの目安を確認できます。

CSV出力されたログファイルの保存期間

出力されたCSVログファイルは管理者向けダッシュボードからダウンロードすることができます。

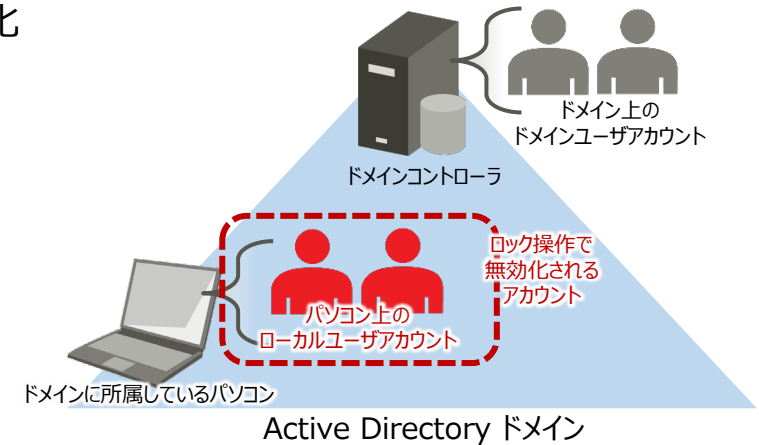
管理者向けダッシュボードからCSVログファイルがダウンロード可能な期間は、各CSVログファイルが出力されてから2ヶ月間となっており、この期間を超えると自動的に削除されますのでご注意ください。

Windows® のロック操作について

Windows®のリモートロックおよびローカルロックは、OS上に作成されたユーザアカウントを一時的に無効化することで実現しております。

なお、**無効化することができるのはパソコン上に作成されているローカルユーザアカウントのみとなり、ドメインユーザアカウントを無効化することはできません。**

ドメイン環境でパソコンをご利用の場合は、ドメインセキュリティポリシー（アカウントロックアウトポリシー）を使用して、アカウントを保護することをお奨めいたします。



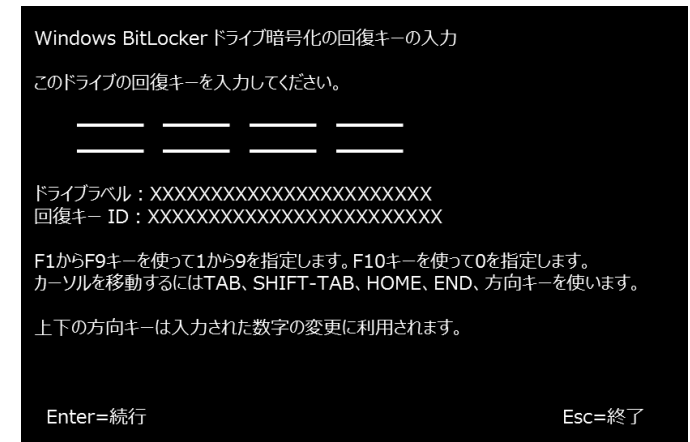
Windows® のワイプ操作について

【前提条件】

Windows®のワイプ機能をお使いいただく場合、**対象となるパソコン上のハードディスクはBitLocker®暗号化機能を使用して暗号化されている必要があります。**

Windows®のリモートワイプ・ローカルワイプ指示を受け取った**パソコンは、パソコン起動時にBitLocker®暗号化の回復キーの入力を求められるようになります。**

正しい回復キーを入力しない限り、パソコンを起動することはできません。また、パソコンからハードディスクドライブを取り出して、他のパソコンに接続した場合も、BitLocker暗号化によりドライブが暗号化されているため、ハードディスクの中身を読み取ることはできません。



■ 起動時のBitLocker®ドライブ回復キー入力画面（例）

Android™ OSのバージョンによる機能差異について

Android™ 4.2以降のOSや5.0以降のAndroid™ OSが搭載された端末では、OSの仕様変更起因して、以下に示すいくつかの機能が利用できなくなっております。Android™端末でSystemwalker Desktop Naviをご利用いただく場合、事前に製品ホームページにて公開しております[動作確認機種](#)ならびに[機能一覧](#)をご確認いただきますようお願いいたします。

機能カテゴリ	対象機能	利用不可対象OS
紛失対策	ローカルワイプが実行されるまでのスクリーン解除操作失敗回数の指定	Android™ 5.0以降
	リモート3G遮断	Android™ 5.0以降
	リモートデータ削除によるSMSメッセージの削除	Android™ 5.0以降
	リモートデータ削除によるSDカードのデータ削除	Android™ 6.0以降
	リモートデータ削除によるブラウザ履歴の削除	Android™ 6.0以降
利用制限	3G通信の利用制限	Android™ 5.0以降
	USBの利用制限	Android™ 4.2以降
	SDカードの利用制限	Android™ 4.2以降
	特定ソフトウェアの起動禁止	Android™ 5.0以降
	Webアクセス制限（URLフィルタリング）	Android™ 6.0以降
ログ取得	ソフトウェア起動ログの収集	Android™ 5.0以降
	URLアクセスログ	Android™ 6.0以降
その他	Androidエージェントのアンインストール防止	Android™ 7.0以降

 特定のメーカー・機種によっては、上記以外の機能につきましても正常に動作しない場合があります。動作検証済みの機種につきましては、製品ホームページをご確認くださいませよう、お願いいたします。

■ 環境更新オプション（Android、iOS向け）の処理性能

環境更新オプションにてAndroid™端末やiOS端末に対して資源配付を実施する際、『資源配付の運用形態』や『端末の回線状況』等によっては、お客様が想定されている運用に対して十分な性能が得られない場合があります。

【運用例】

- ・多台数のAndroid™端末に対して、ファイルサイズの大きいデータやソフトウェアプログラムを登録・一斉配信する
- ・多台数のiOS端末に対して、ファイルサイズの大きいインハウスアプリを登録・一斉配信する

【回線例】

- ・Wi-Fi接続はできず、3G等の低速回線のみでしかインターネットに接続できない
- ・インターネット接続回線にダウンロード速度制限が設けられている

環境更新オプションのご契約を検討されており、かつ上記の例に該当するお客様向けに事前トライアルをご用意しておりますので、本トライアルにてお客様が想定されている運用が可能かについて、必ず事前にご確認いただきますようお願い申し上げます。

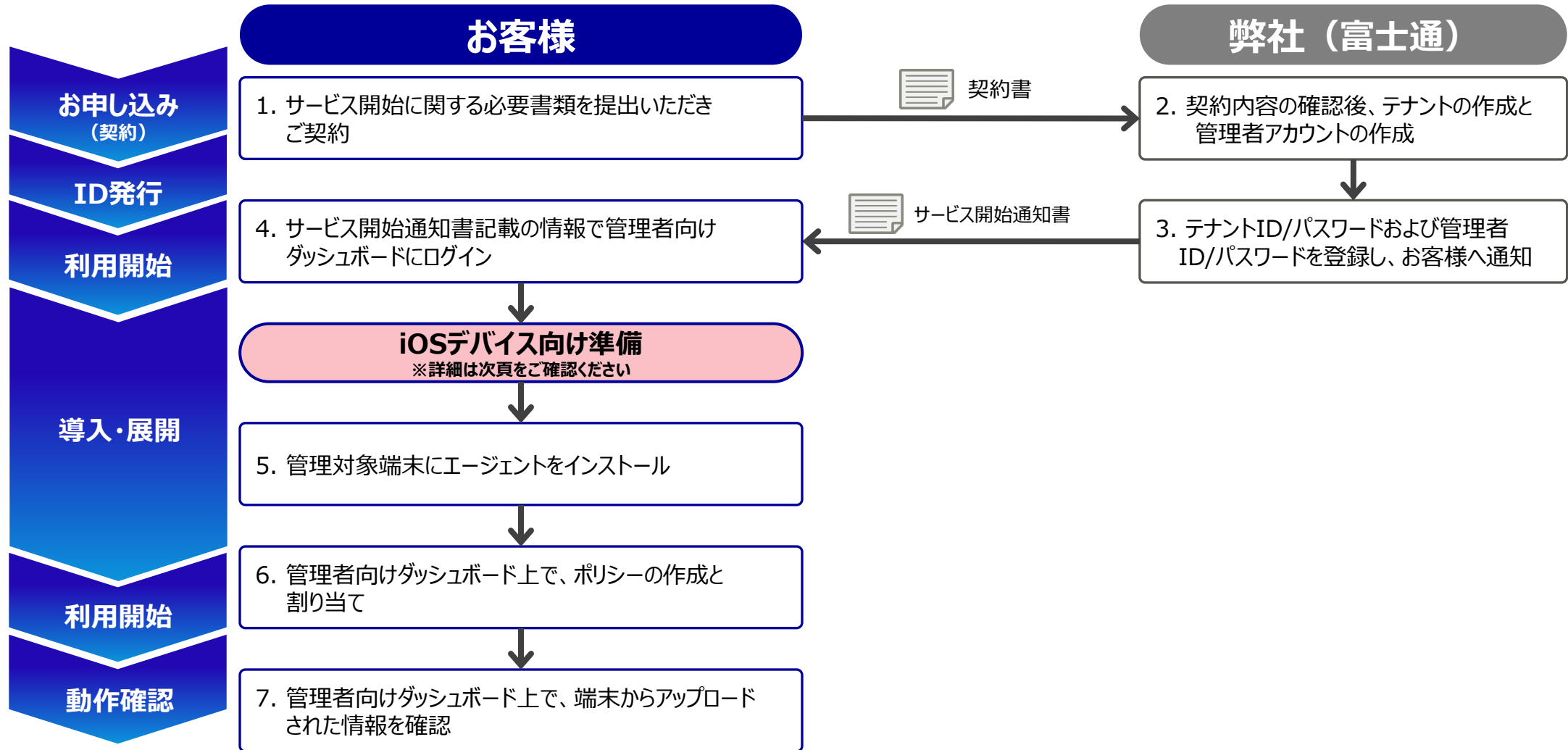


事前トライアルをご希望のお客様は、本書「お問い合わせ先」記載の連絡先までご連絡ください。

9. 導入・サポート、商標

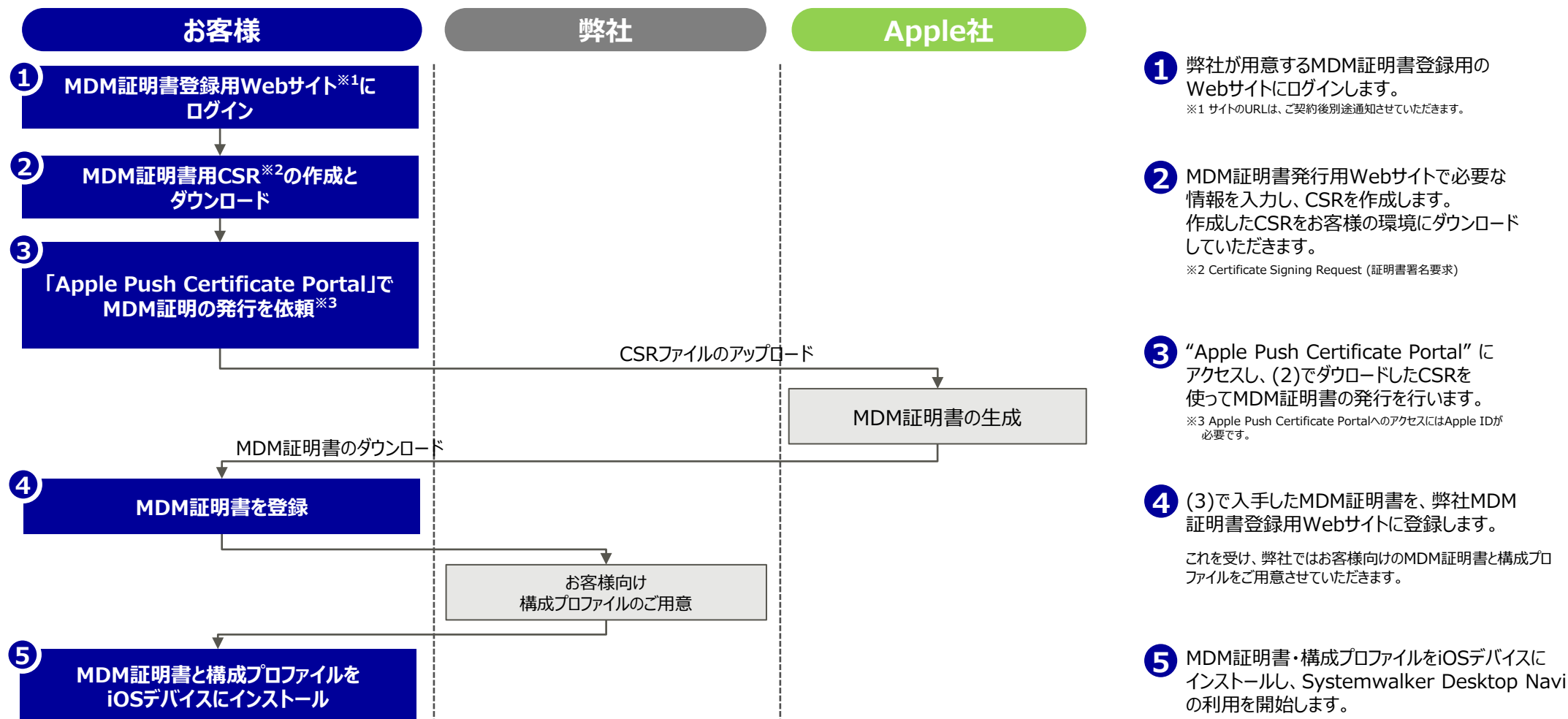
- お申し込みから利用開始まで
- iOSをご利用いただく場合のお客様作業
- サービス時間・サポート受付時間
- 登録商標

お申し込みから利用開始まで



iOSでご利用いただく場合のお客様作業

iOSデバイス（iPhone、iPad）で Systemwalker Desktop Naviをご利用いただく場合、利用を開始する前にApple社Push MDM証明書を弊社サーバに登録していただく必要があります。Apple社からPush MDM証明書の発行を受けるためには、以下に示すお客様作業が発生します。



- 1 弊社が用意するMDM証明書登録用のWebサイトにログインします。
※1 サイトのURLは、ご契約後別途通知させていただきます。
- 2 MDM証明書発行用Webサイトで必要な情報を入力し、CSRを作成します。作成したCSRをお客様の環境にダウンロードしていただきます。
※2 Certificate Signing Request (証明書署名要求)
- 3 “Apple Push Certificate Portal” にアクセスし、(2)でダウンロードしたCSRを使ってMDM証明書の発行を行います。
※3 Apple Push Certificate PortalへのアクセスにはApple IDが必要でです。
- 4 (3)で入手したMDM証明書を、弊社MDM証明書登録用Webサイトに登録します。
これを受け、弊社ではお客様向けのMDM証明書と構成プロファイルをご用意させていただきます。
- 5 MDM証明書・構成プロファイルをiOSデバイスにインストールし、Systemwalker Desktop Naviの利用を開始します。

■ サービス提供時間

Systemwalker Desktop Naviのサービス提供時間は以下の通りです。

24時間 365日

ただし、データセンターの定期保守やサービスプログラムの定期メンテナンス等により一時的にサービスを停止させていただく場合があります。緊急の場合を除き、サービスの停止を行う場合は、事前に管理者向けダッシュボードにてお客様にスケジュールをご案内させていただきます。

■ サポート受付時間

フリーダイヤル、電子メールによる受付時間は以下の通りです。

平日 9:00～12:00、13:00～17:00



- ・お問い合わせに対する弊社からの回答につきましても上記時間帯に限るものとします。
- ・土日祝日、年末年始および弊社の指定する休業日（別途スケジュールを事前にご案内いたします）につきましては、終日サポート受付時間外となります。
- ・サポート受付用フリーダイヤル番号、電子メールアドレスは、サービス開始通知書にてご案内いたします。

※その他、サービスレベルにつきましては、「サービス仕様書」にて規定しておりますのでご確認ください。

- Microsoft、Windows、およびWindows Serverまたはその他のマイクロソフト製品の名称および製品名は、米国 Microsoft 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。
- OracleとJavaは、Oracle Corporation およびその子会社、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。
- Adobe、Acrobat、Flash、Flash Playerは、Adobe Systems Incorporated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。
- Apple、iPad、iPhoneは、米国および他の国々で登録されたApple Inc.の商標です。iPhoneの商標は、アイホン株式会社のライセンスにもとづき使用されています。
- Google、Android、Google Play（旧 Android マーケット）、YouTubeおよびYouTube ロゴ、Google Chromeは、Google Inc.の商標または登録商標です。
- Bluetoothは、Bluetooth SIGの登録商標で、富士通へライセンスされています。
- Wi-FiおよびWi-Fiロゴは、Wi-Fi Allianceの登録商標です。
- その他の製品名は、各社の商標または登録商標です。

