Fujitsu Software

Systemwalker Desktop Navi

システムウォーカー デスクトップ ナビ

ご紹介

2025年1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

企業で利用するPCの運用管理は、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、巧妙化するサイバー犯罪の増加などの様々な環境変化を受けて大きく変化し続けています。

	従 来	現 状	
管理対象（デバイス）	・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（ワークスタイル変革） ・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

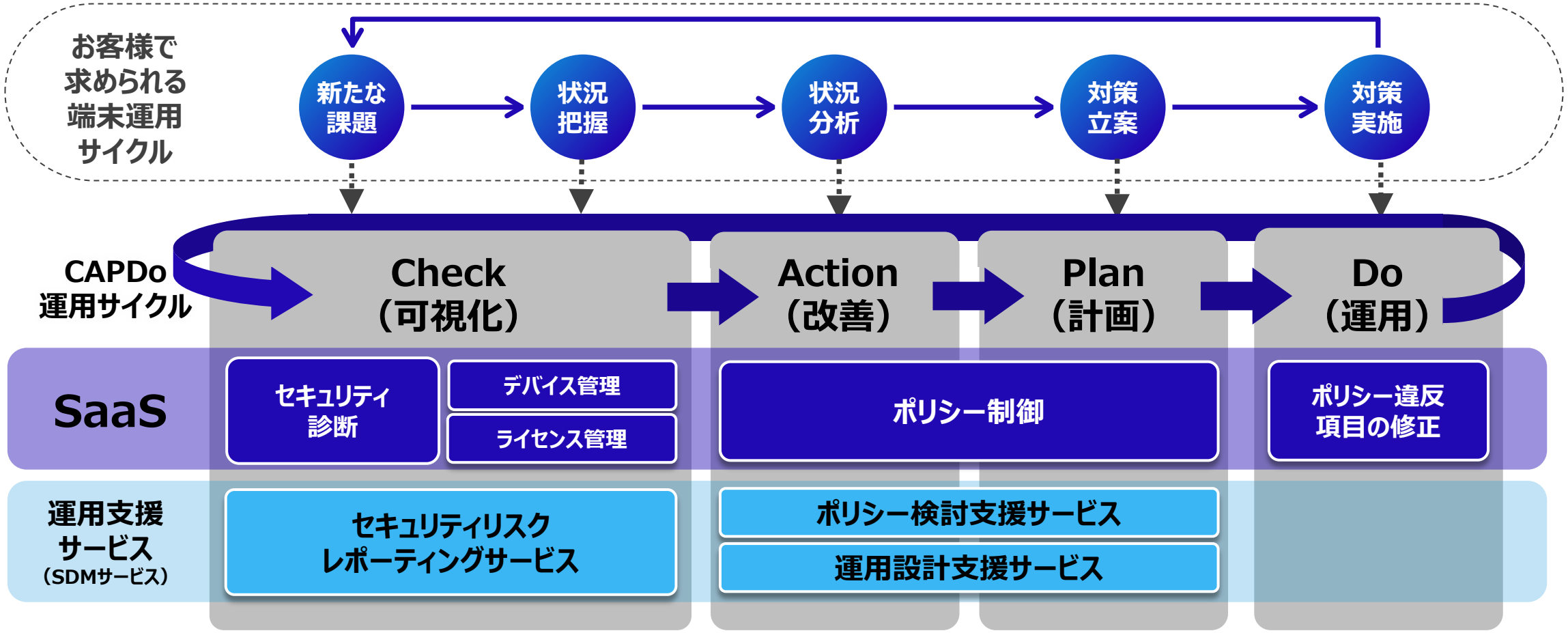
今後も発生し続けることが予想される環境変化や課題に対応するため、端末運用サイクルについても継続的な見直しが必要となります。また、端末運用サイクルの見直しだけでなく、端末を使用する人（ヒト）の知識・意識についても環境変化に対応するための施策を推進することが重要となります。

	運用開始時	運用中	新たな運用課題
資産	端末配付時の利用部門や利用者の登録	棚卸し（利用部門/利用者の更新）	新デバイスの導入 新OSへの対応
資産	ソフトウェアライセンス管理	ソフトウェアライセンス管理（インストールによる増減）	ソフトウェアライセンス監査（ライセンス超過）
セキュリティ	セキュリティポリシーの策定	セキュリティポリシー遵守状況の監視	セキュリティ事故の発生
人（ヒト）	端末利用における利用者教育の実施	端末利用における利用者への状況見える化	新たな端末利用における利用者教育の実施

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PC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・運用につなげるCAPDo運用サイクルでお客様の端末運用を支援します。

C 監査 Check

現状の端末状況やセキュリティ状態を
Systemwalker Desktop Naviダッシュボードで可視化

現状把握と評価・分析

A 改善 Action

現状の問題点や対策の優先順位、新たな経営課題に
対するICTポリシーの改善提案を実施

現状の問題点
対策の優先順位
新たな経営課題
…

ポリシーの策定

セキュリティ	資産統制	システム運用		
USB持ち出し禁止	稼働状況確認	アプリ環境更新	社内用ポリシー	日本国内
デバイス制御 紛失対策	稼働状況確認	アプリ環境更新	社外用ポリシー	
アプリ起動禁止 URLアクセス制限	アプリ管理	リモートサポート	拠点用ポリシー	海外

ポリシーの適用

P 計画 Plan

課題解決に向けたポリシーを
Systemwalker Desktop Navi
で設定

自動収集・報告

エージェントによる定期チェック

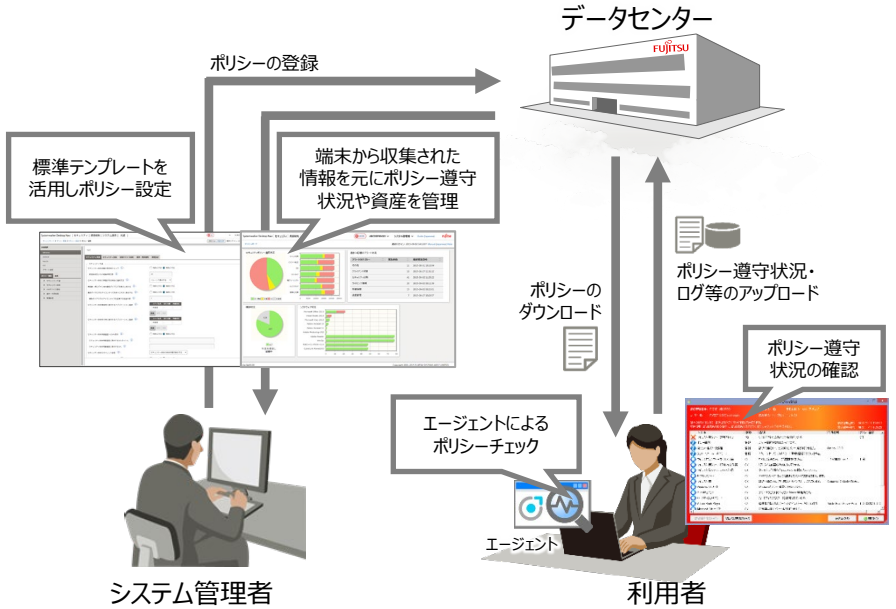
D 運用 Do

Systemwalker Desktop Naviで策定した
ICTポリシーをPCに適用し業務利用

製品特長（1）

クラウドサービスで簡単導入

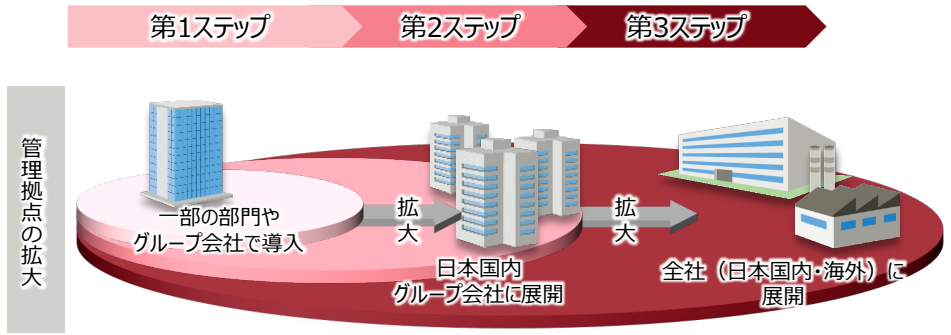
Systemwalker Desktop Naviはクラウドサービスのご提供となり、管理対象となるPCにエージェントプログラムをインストールするだけで、ご利用を開始いただけます。
専用のサーバー機器やストレージ、ネットワーク機器などの導入は不要です。



■ 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（ロケーション）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

製品特長（2）

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。

製品特長（3）

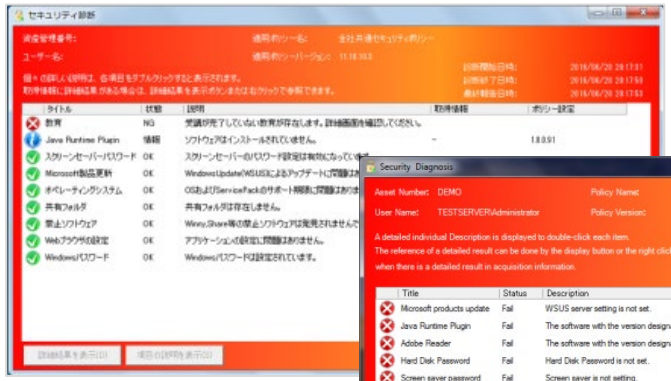
ダッシュボードによる可視化

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。

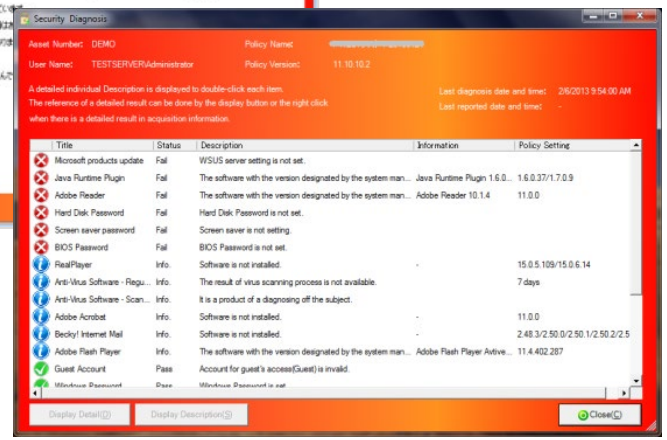
幅広い用途に対応

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

お客様の課題解決に向けて

FUJITSU

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
- 業務PCの社外利用を推進したいが、紛失や盗難が怖い
- 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PC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

- 社内のPC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

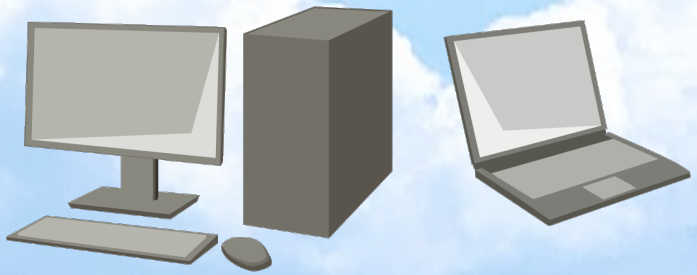
PC利活用に関するお客様の課題

Systemwalker Desktop Navi による課題解決

「Fujitsu Software Systemwalker Desktop Navi」は、お客様におけるPC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	PC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



Windows PC

セキュリティに関する課題

セキュリティ

課題	情報漏えい対策	PCの盗難・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	テレワークなどにおけるPCの社外利用の普及に伴い、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	PC盗難・紛失時、遠隔での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 Naviによる対策

- 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

- 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
- リモートデータ削除
  ・指定ファイル、フォルダ

- スケジュール実行可能なセキュリティ診断
  ・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
- 管理者向け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

ログ管理に関する課題

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PCやソフトウェアが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 Naviによる対策

● 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※ ※オプションサービスで別途ご契約が必要です	● 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	● 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

資産統制に関する課題

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	**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**	**賠償金などの金銭的損失 社会的信用の失墜**	**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**
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 Naviによる対策

● 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、ウィ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）	● 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を比較し、ソフトウェアライセンスの適正利用を管理	● 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

リテラシーに関する課題

リテラシー

課題	利用者リテラシーの向上	
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 Navi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

システム運用に関する課題

システム運用

課題	運用・メンテナンスコスト削減	現場の生産性向上
背景	ICT機器は安定稼働やセキュリティ対策の視点から、適切なタイミングで更新や修正モジュールの適用が必要であるが、端末の台数が多いと管理者の負荷が大きくなる	支店や支社など遠地に設置された端末や、社外持出PCに問題が発生した場合、正確な状況把握が困難で対処に時間を要する場合がある
リスク	**端末の維持、運用管理に係るコストの増加**	**問題解決まで業務が停止することによる生産性の低下**
望まれる対策	管理者が個々の端末を手作業で更新するのではなく、遠隔からの指示で一斉に更新できる	遠地で発生したトラブルについて、管理者が現地に赴くことなく状況を把握し、問題解決できる

Systemwalker Desktop Naviによる対策

【環境更新オプション】
- ファイル配付・削除
- フォルダ配付・削除
- スクリプト配付（実行）
- ソフトウェアインストール、など

【インターネットサポートオプション】
- インターネット経由での端末のリモートモニタリング・操作
- ファイル転送
- テキストチャット、など

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）
- 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
- 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

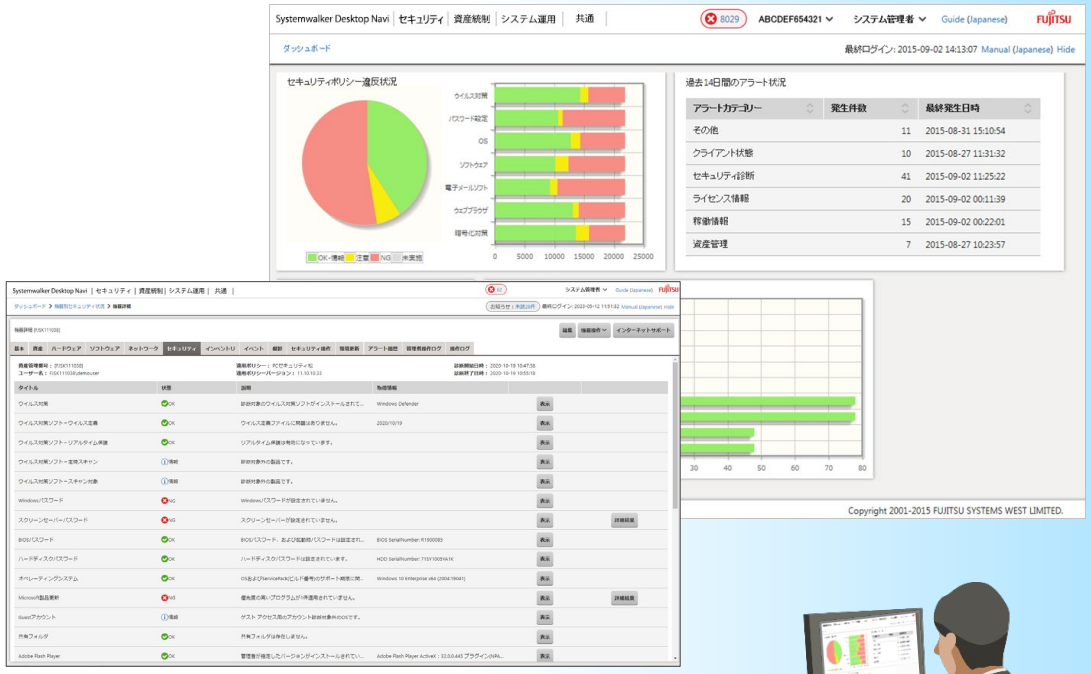
■ 管理者向けWebダッシュボード

■ 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

セキュリティ

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。



●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。

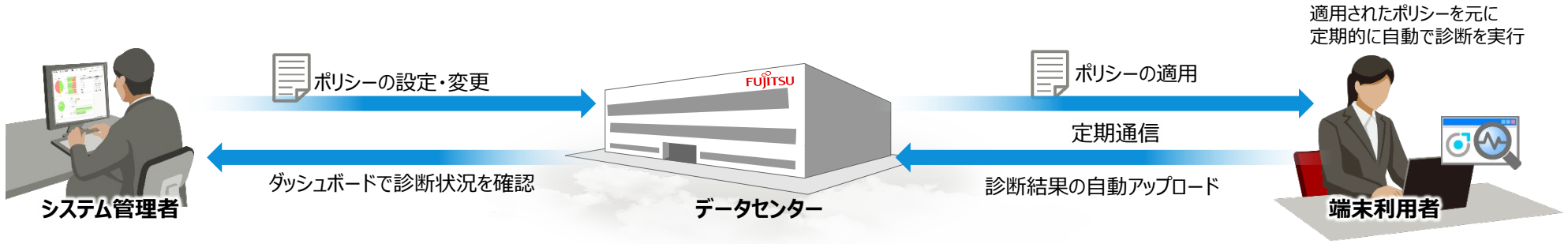
●セキュリティ診断結果

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、PC上のエージェントに配付され、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

- 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

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10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。

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。

「○○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。

診断条件に利用できる項目

項目	判断条件
ファイル	・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	・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。

セキュリティ

操作・利用制限

PC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

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

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

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

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

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

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）

PC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出来ます。

Wi-Fi接続禁止

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

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。機器を個体識別して許可・禁止することはできません。

赤外線接続禁止

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

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出来ます。

IEEE1394接続禁止

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

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。

紛失対策

リモートオフィスなどの社外での勤務時や移動時に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

遠隔操作でPCのロックを行います。
Windows®上の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

BitLockerドライブ暗号化で暗号化されているPCの起動時に回復キーの入力を求めるようにできます。
PCからドライブを取り外した場合でも、ドライブが暗号化されているため情報の漏えいを防止できます。

リモートデータ削除

遠隔操作でPC上のデータを削除することができます。
PC上の任意のフォルダやファイルを指定して削除できます。

⚠ 本機能の動作詳細につきましては、「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。

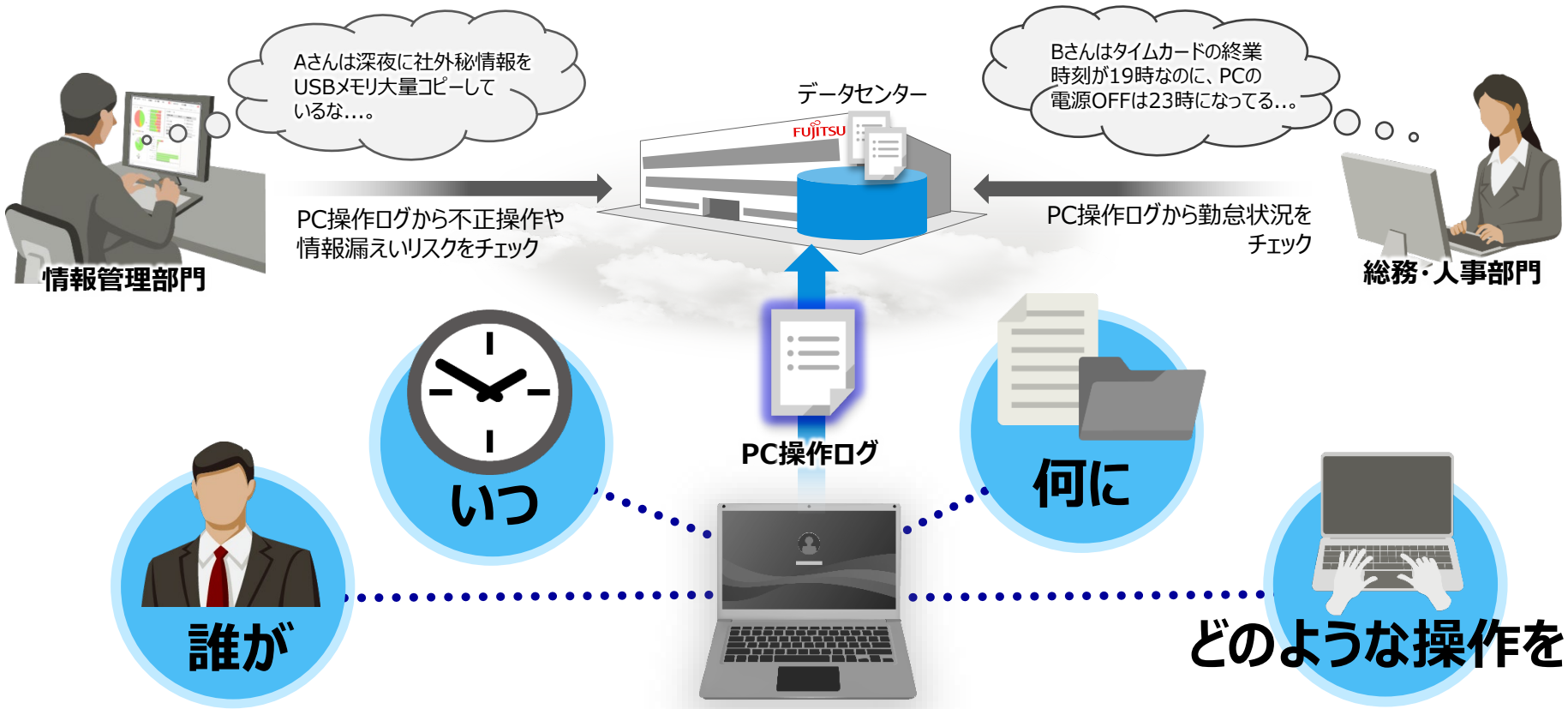
■リモート指示を受信できない場合でも（ローカルロック・データ削除）

ログオンに指定回数失敗した場合、PCのロックや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。

ログ管理

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、業務PC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者へ周知することで、従業者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。



ログ管理

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、業務用PC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

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。

ログオン・ログオフログ

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。

ソフトウェア起動・終了ログ

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。

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**。

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**。

ログ管理

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

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

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

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

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

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。

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

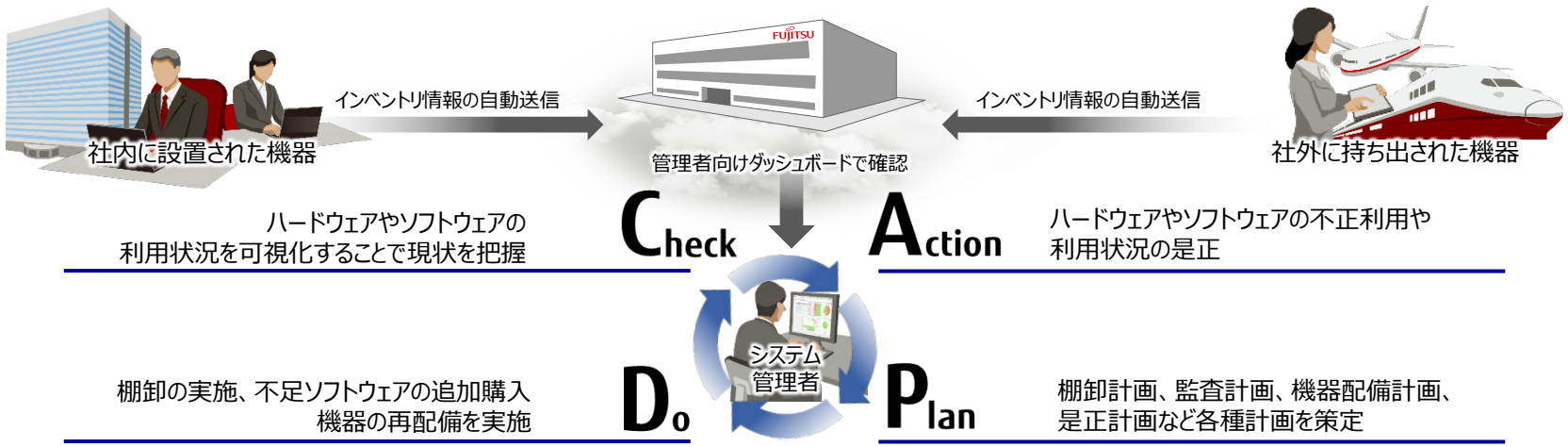
マルウェアは電子メールや悪意を持ったWebサイトへのアクセスなど様々な経路で感染する場合があります。
万が一こうした経路で**マルウェアに感染した場合でも、感染経路の特定が容易**となります。

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。

資産統制

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

【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

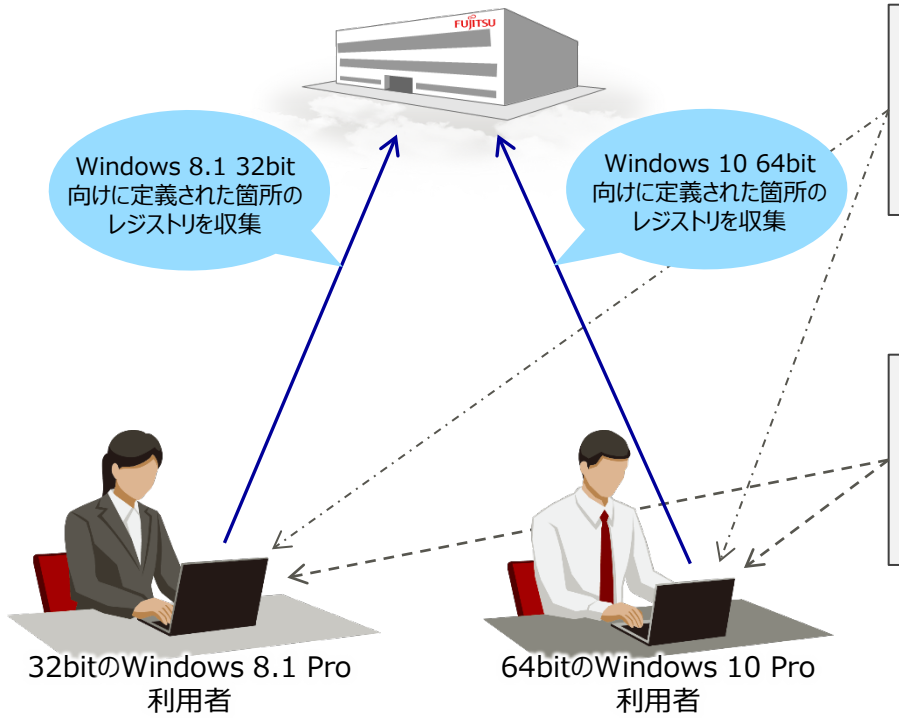
追加入力可能項目

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

資産統制

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。



レジストリ取得ルール1: OSサービスの起動設定状況確認

[Windows 8.1 32bit]
HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥....

[Windows 10 64bit]
HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥....

OSの種別によらず、設定が定義されているレジストリの場所は同じなので同じ場所のレジストリを取得するよう定義します。

レジストリ取得ルール2: ソフトウェアの設定状況確認

[Windows 8.1 32bit]
HKEY_LOCAL_MACHINE¥Software¥Fujitsu¥....

[Windows 10 64bit]
HKEY_LOCAL_MACHINE¥Software¥WOW6432Node¥Fujitsu¥....

同じソフトウェアの設定でも、設定が定義されているレジストリがOS種別によって異なる場合、OS種別毎に取得するレジストリの場所を定義できます。

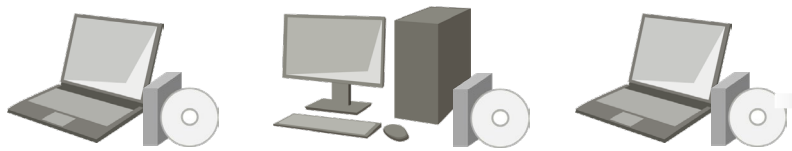
⚠ 本機能に関する留意事項

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。

資産統制

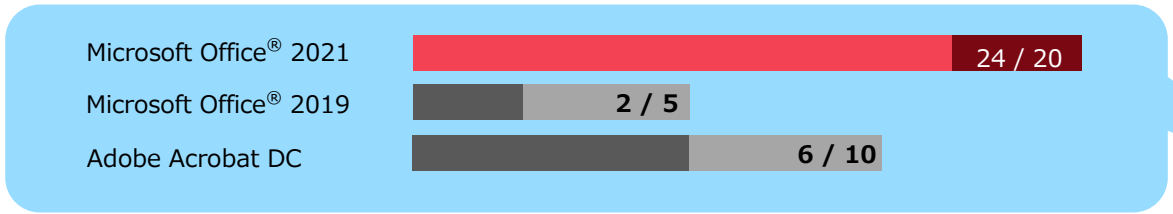
ソフトウェアインストール状況からのライセンス管理

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。

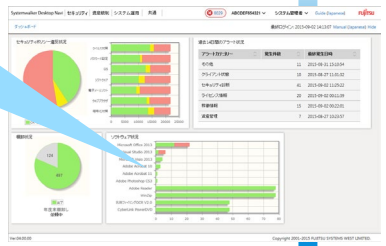


定期的にソフトウェアインベントリを自動収集

管理者向けダッシュボードのライセンス利用状況 表示例



ライセンス数を超えるインストールが検出された場合、管理者はダッシュボードで確認可能



Microsoft Office 2019 Pro	20
Microsoft Office 2016 ProPlus	5
Adobe Acrobat DC	10

ライセンス情報の登録

システム管理者

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PC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PCの候補を選定。

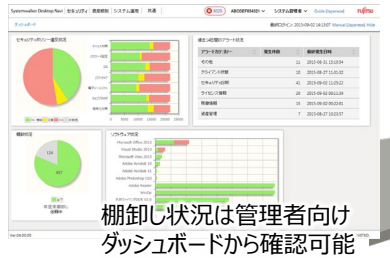
② アンインストールの指示

ソフトウェアをアンインストールするPCが決定したら、管理者向けダッシュボードから対象PCの情報を確認し、利用者を特定。
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。

資産統制

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。

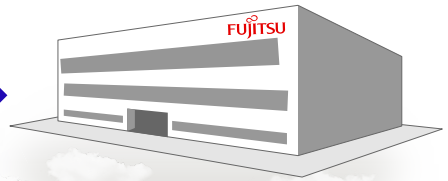


棚卸し状況は管理者向け
ダッシュボードから確認可能

システム管理者

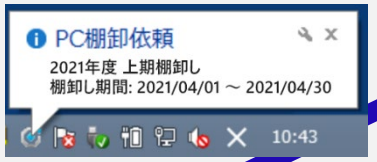
棚卸し依頼

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
PC上に棚卸し依頼が
ポップアップされます。



【 PC上での棚卸し 】

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。

棚卸し
回答

棚卸し
依頼

利用者
(Windows)

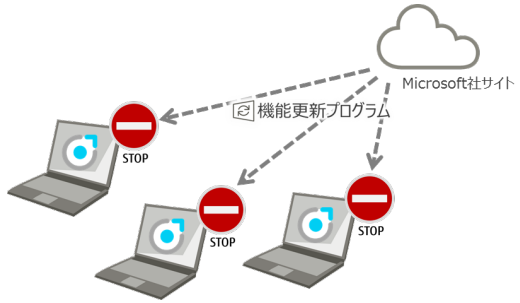
Windows®10 更新支援機能

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。

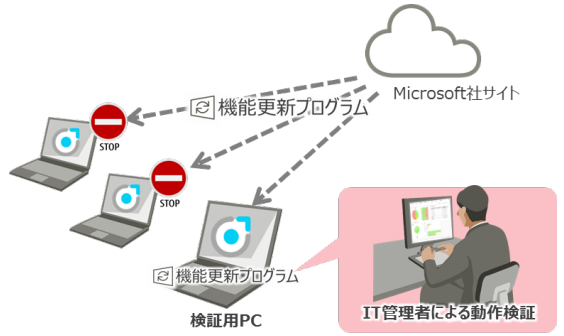
これにより、意図しない機能更新プログラム適用が原因で、業務で利用しているソフトウェアが利用できなくなるといったトラブルを防止することができます。



機能更新プログラムのバージョン選択が可能

Windows10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**。

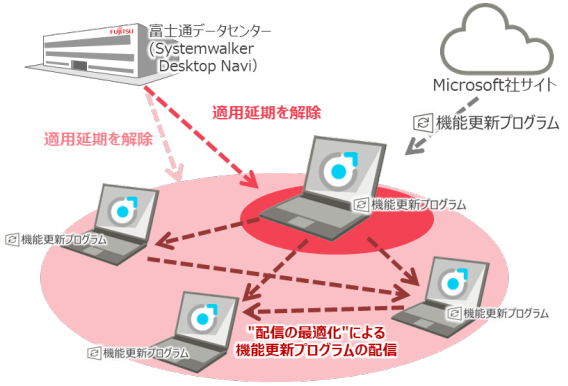
これにより、PC上で利用しているアプリケーションの機能更新プログラムへの対応状況や、PCの利用用途などにあわせて最適な機能更新プログラムの適用制御が可能です。



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。

FUJITSU

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。

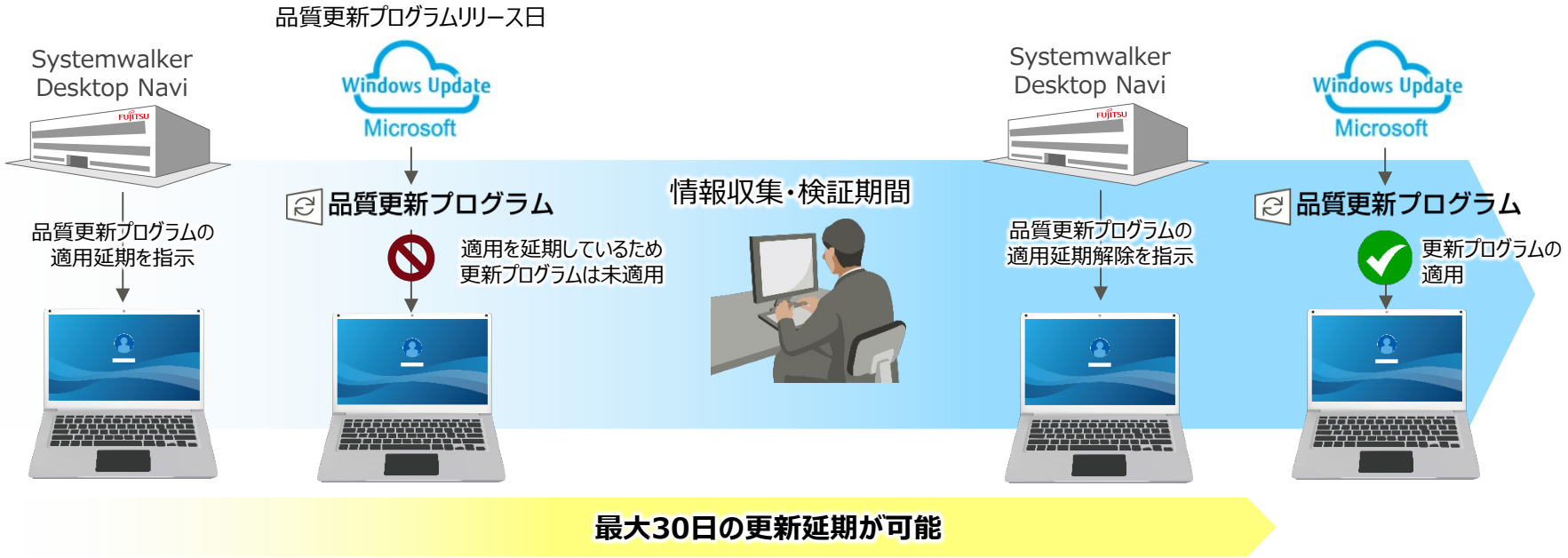
本機能に関する留意事項

- 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もあります。
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。

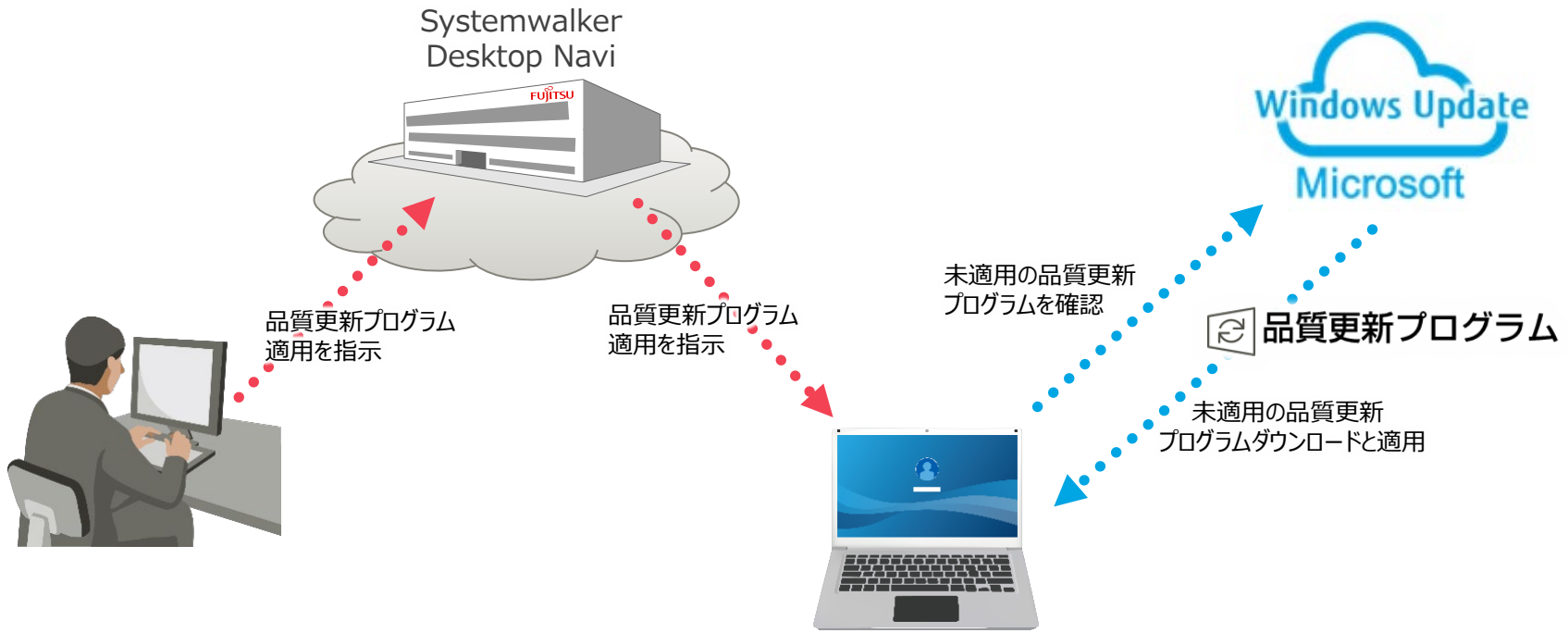


Windows®10 更新支援機能

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。



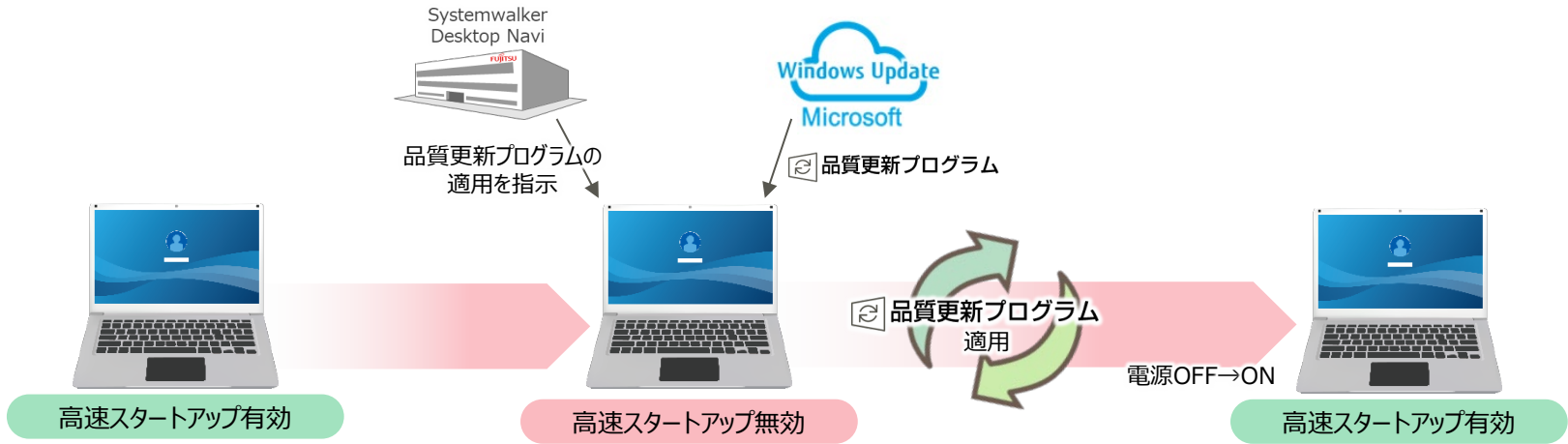
Windows®10 更新支援機能

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関わらず、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）

導入・展開支援

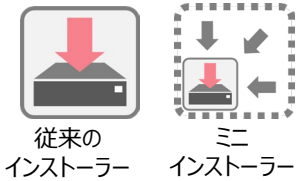
ミニインストーラー

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。

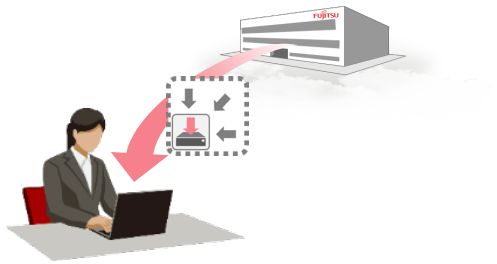
インストーラーサイズを大幅に縮小し、利用者への配付が容易に

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に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。

導入・展開支援

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。

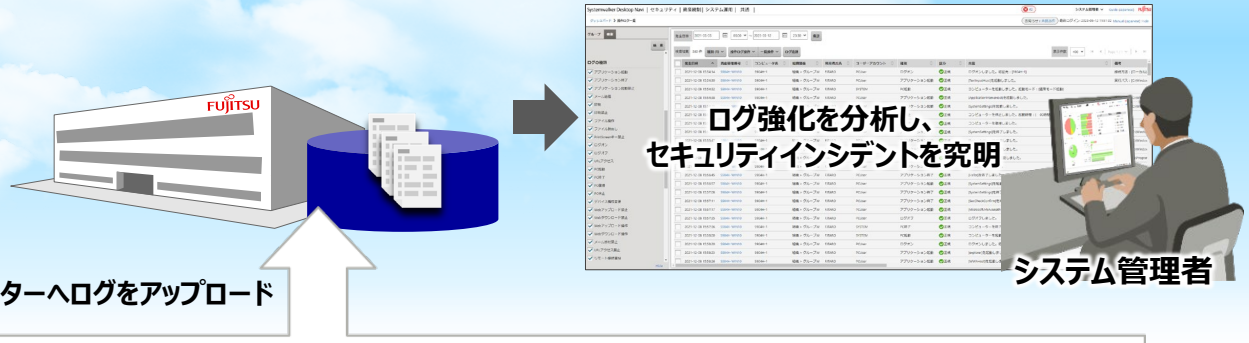
4. 機能紹介 ～オプションサービス～

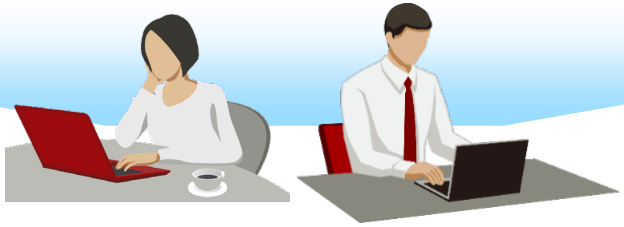
- ログ強化 オプション
- 環境更新 オプション
- インターネットサポート オプション

ログ強化オプション（操作ログ収集：ファイル操作ログ収集）

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。





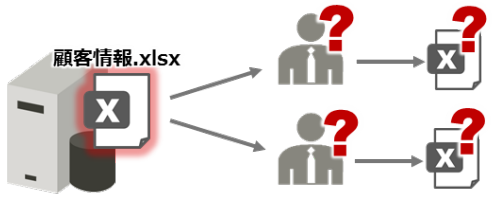
ログ強化オプション（操作ログ収集：ファイル操作ログ収集）

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…？



この様なケースでは、**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。

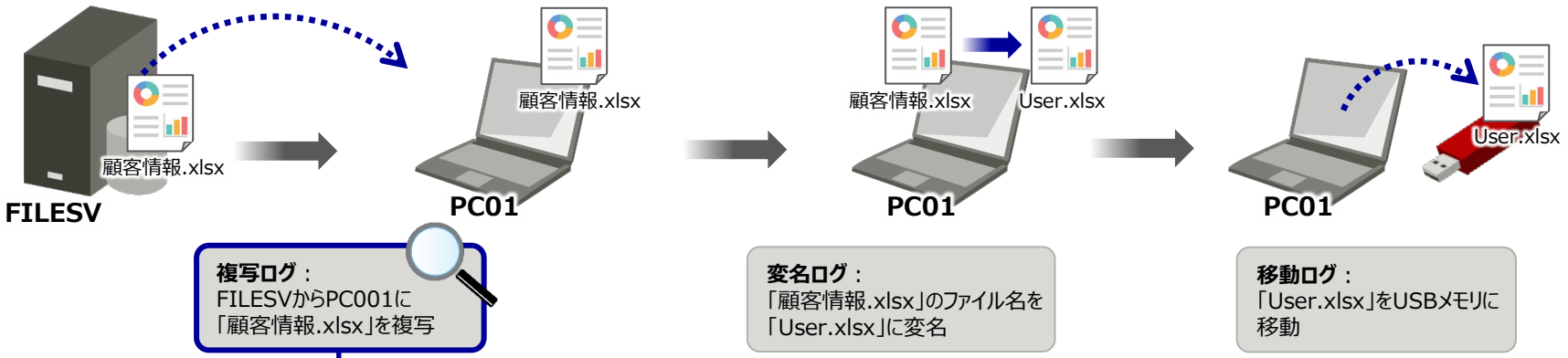
流出した情報の出所が不明だ…。
まずは流出した「User.xlsx」というファイルを扱っている人がいないか確認してみよう。

この様なケースでは、**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。

ログ強化オプション（操作ログ収集：ファイル操作ログ収集）

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。



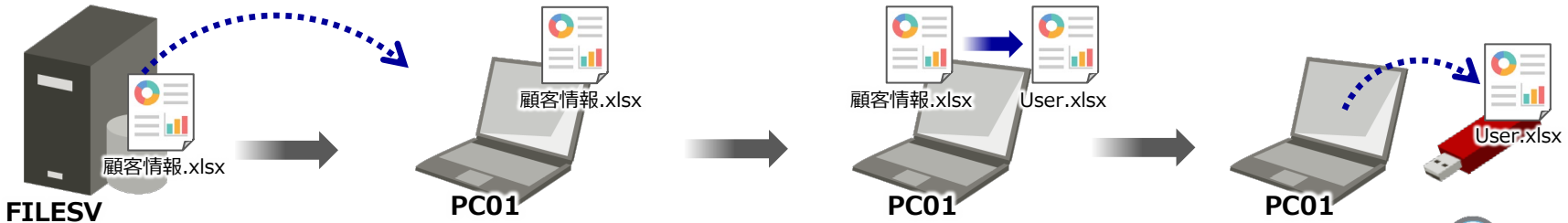
フォワードトレース：
任意のファイル操作ログを起点に以降のファイル操作を追跡

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。

ログ強化オプション（操作ログ収集：ファイル操作ログ収集）

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。



複写ログ：
FILESVからPC001に
「顧客情報.xlsx」を複写

変名ログ：
「顧客情報.xlsx」のファイル名を
「User.xlsx」に変名

移動ログ：
「User.xlsx」をUSBメモリに
移動

バックトレース：
任意のファイル操作ログを起点に操作を遡って追跡

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。

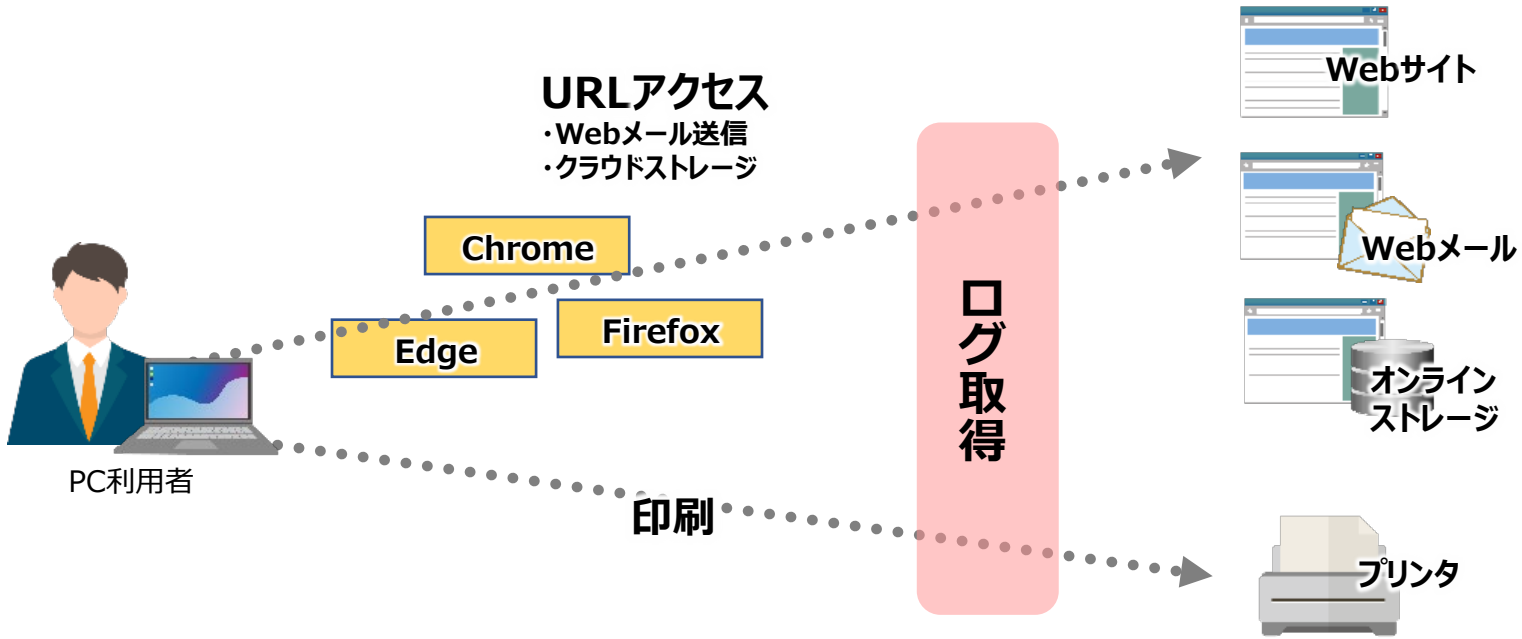
ログ強化オプション（操作ログ収集：Webアクセスログ収集）

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。



ログ強化オプション（不正操作検知：シグネチャ検知機能）

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

予兆検知：不正操作検知

漏えい事故発生の抑止

漏えい事故発生前

漏えい事故発生

原因究明：ファイル操作の追跡

漏えい事故原因・影響範囲の早期究明

漏えい事故発生後

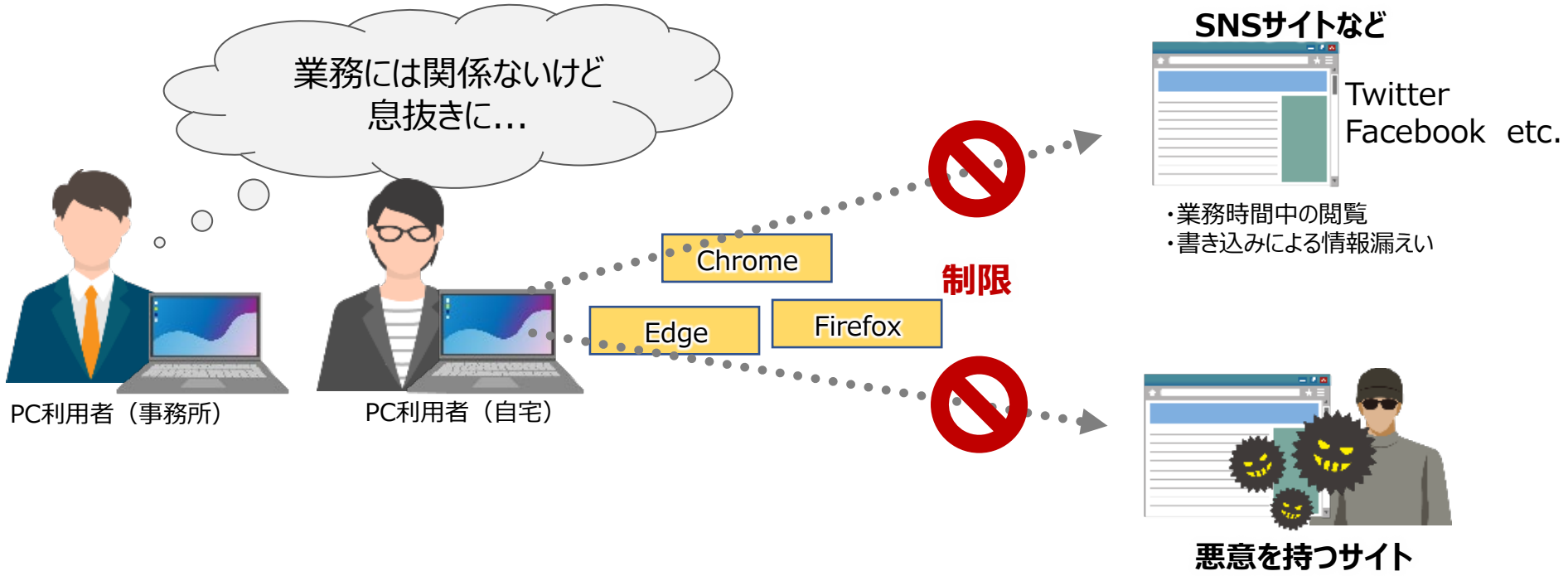
Systemwalker Desktop Navi のシグネチャ検知機能

- **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

ログ強化オプション（不正操作制御：Webアクセス制御機能）

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。



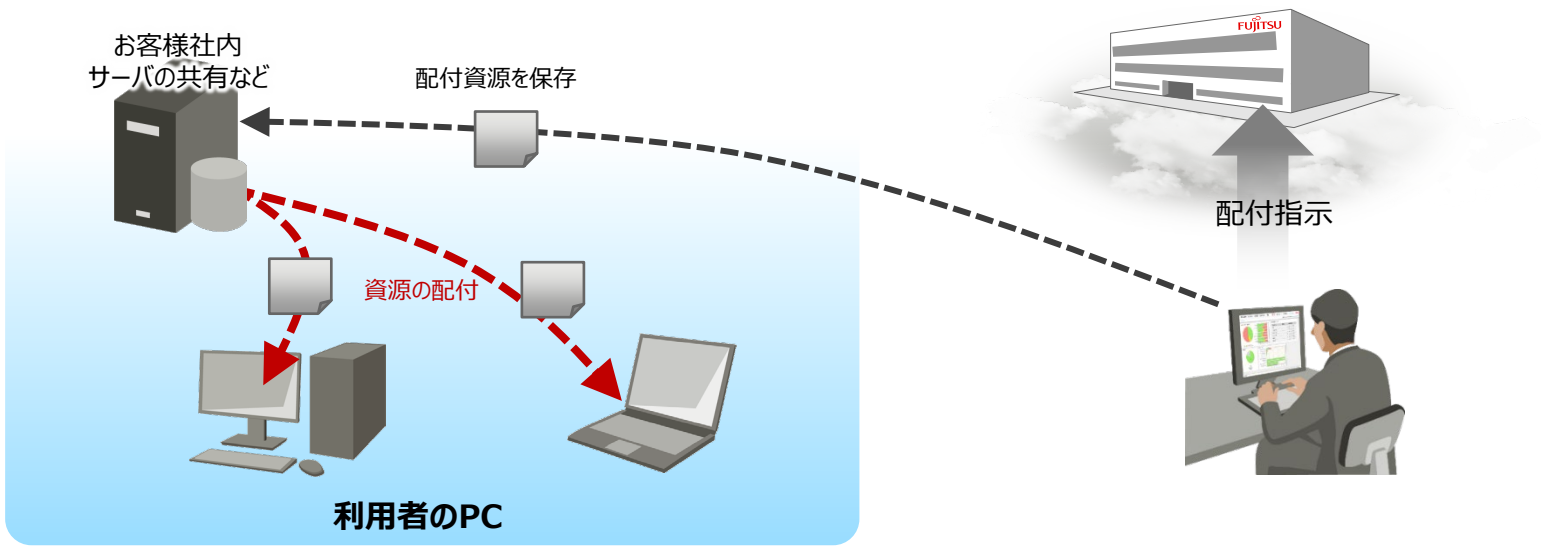
環境更新オプション

ファイル・フォルダのリモート配付・削除

管理者が作成したスクリプト（BAT、WSHなど）を配付資源として登録し、PCに配付して実行できます。
PC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。

ファイル・フォルダのリモート配付・削除

管理者が指定した任意のファイルやフォルダを配付資源として登録し、PCに配付できます。 また、配付だけでなく、PC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。



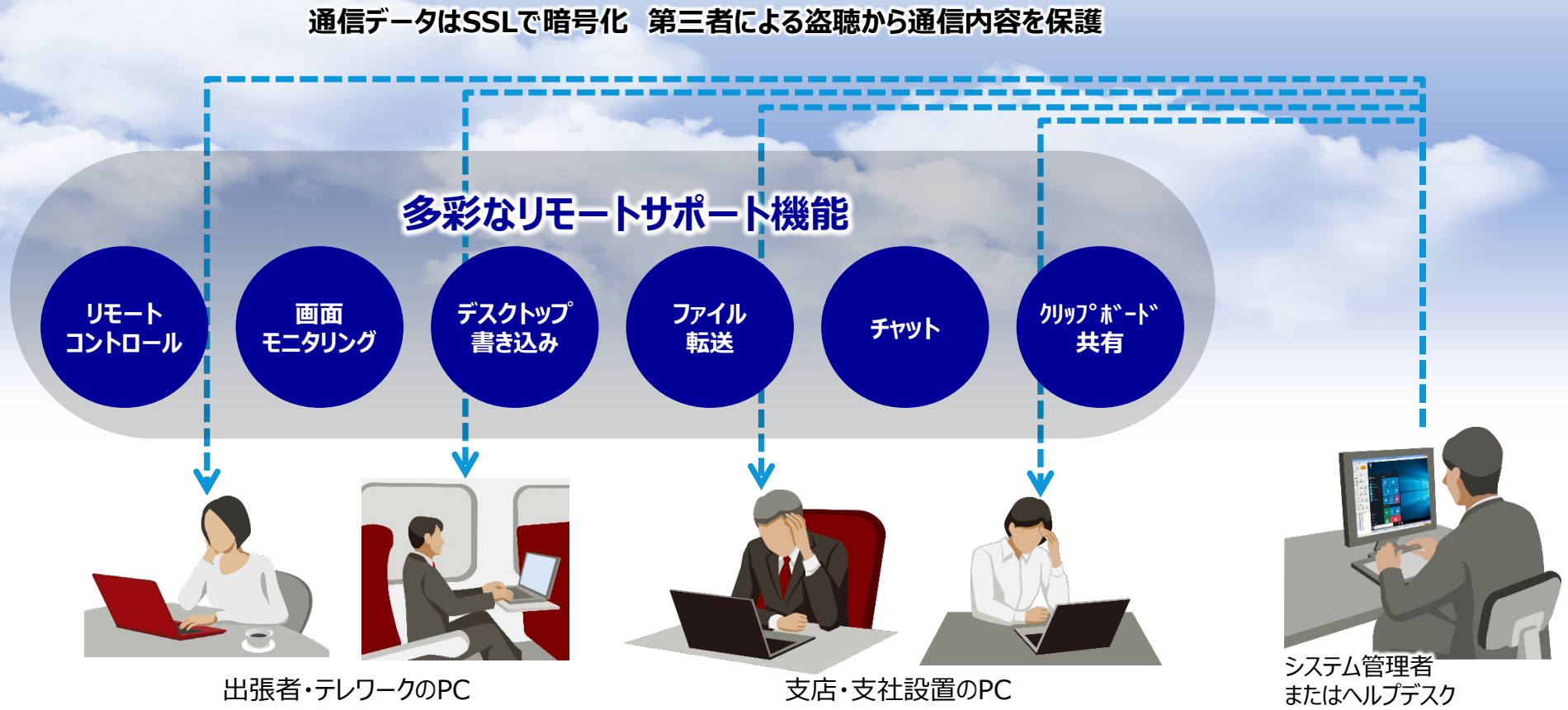
⚠ 本機能に関する留意事項

本機能をご利用いただく場合、配付先のPC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。

インターネットサポートオプション

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PC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PC」、「出張者が社外に持出中のPC」や「テレワーク社員のPC」など、遠隔地のPCのサポート作業を大幅に効率化することができます。

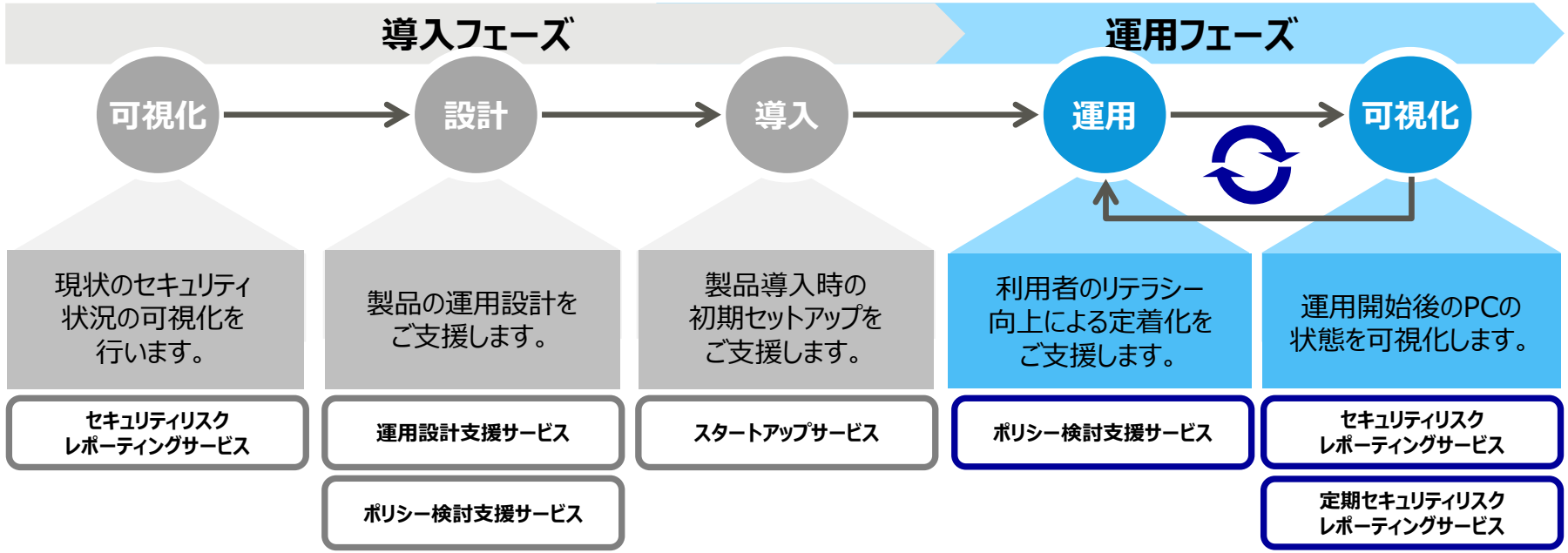


5. SDMサービス

- SDMサービスとは
- SDMサービス　サービスメニュー概要

SDMサービスとは

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。

SDMサービス　サービスメニュー概要

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ティングサービス

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ティングサービス

「セキュリティリスクレポーティングサービス」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

サービス機能一覧

基本サービス①

			Windows® Client OS	Windows Server® OS
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	ウィルス対策ソフト診断	ウィ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、ウィルススキャンの設定内容等についても診断できます。	○	○
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。	○	○
4	パスワード設定診断	ログオンパスワード、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。	○	○
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。	○	○

サービス機能一覧

基本サービス②

			Windows® Client OS	Windows Server® OS
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。	○	–
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。	○※1	–
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。	○※2	–
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。	○	–

※1：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。
※2：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。

サービス機能一覧

基本サービス③

			Windows® Client OS	Windows Server® OS
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。	○※3	–
2	ローカルロック	端末へのログオンに任意の回数失敗した場合、端末をロックできます。	○※3	–
3	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。	○	–
4	リモートワイプ	リモートから端末を初期化できます。	○※4	–
5	ローカルワイプ	端末へのログオンに任意の回数失敗した場合、端末を初期化できます。	○※4	–

※3：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。
※4：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。

サービス機能一覧

基本サービス④

			Windows® Client OS	Windows Server® OS
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。	○	–
2	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。	○※5	–
3	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。	○※5	–
4	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。	○	–
5	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。	○※6	–
6	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。	○	–
7	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。	○	○

※5：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。
※6：Microsoft Internet Explorerのみログが取得できます。

サービス機能一覧

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
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。	○	–
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、その前後のフィ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メーラ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してアラートする。	○	–
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できます。 追加の単位は100GBです。	○	–

サービス機能一覧

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
システム運用				
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（管理者向けダッシュボード・エージェント）
- ネットワーク環境
- サービスの基本動作概要

動作環境（管理対象機器）

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®	
クライアントOS	**サーバOS**
• 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	• Windows Server® 2016 Standard • Windows Server® 2016 Datacenter • Windows Server® 2019 Standard • Windows Server® 2019 Datacenter • Windows Server® 2022 Standard • Windows Server® 2022 Datacenter

※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PC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。

【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。

動作環境（管理者向けダッシュボード・エージェント）

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。

エージェント

Windowsにエージェントをインストールする場合、事前に「Microsoft® .NET Framework 4.6.2 」を導入していただく必要があります。

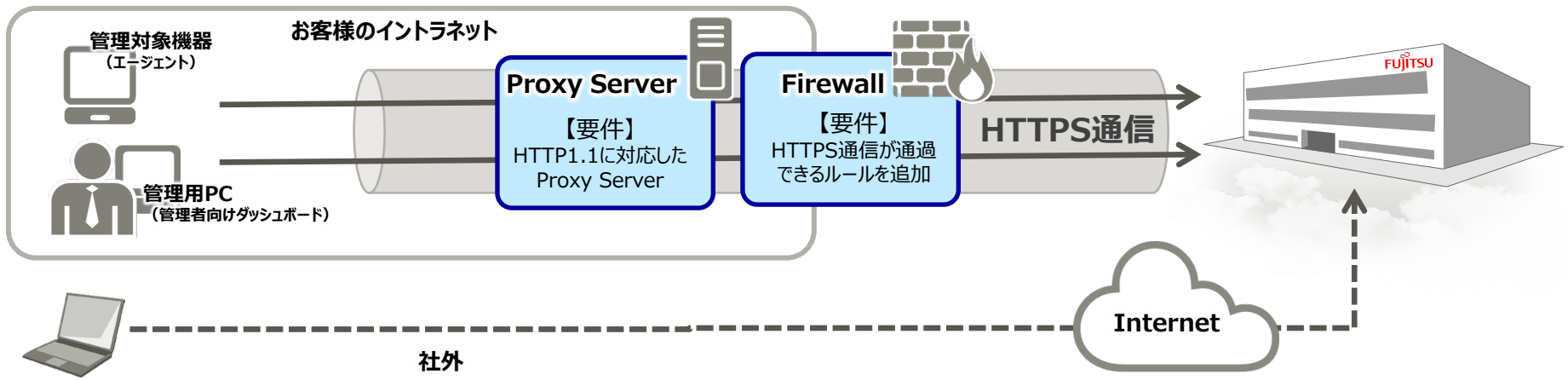
64 ビット OS の場合でも、32 ビット版.NET Framework をインストールしてください。

日本語以外での他言語表記を行う場合はMicrosoft .NET Framework 3.5が必須となります。
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。

ネットワーク環境

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を利用するPC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。

サービスの基本動作概要

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。

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。

・最大3回/日　実行曜日・時刻を指定可能

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PC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	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、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（SP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
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

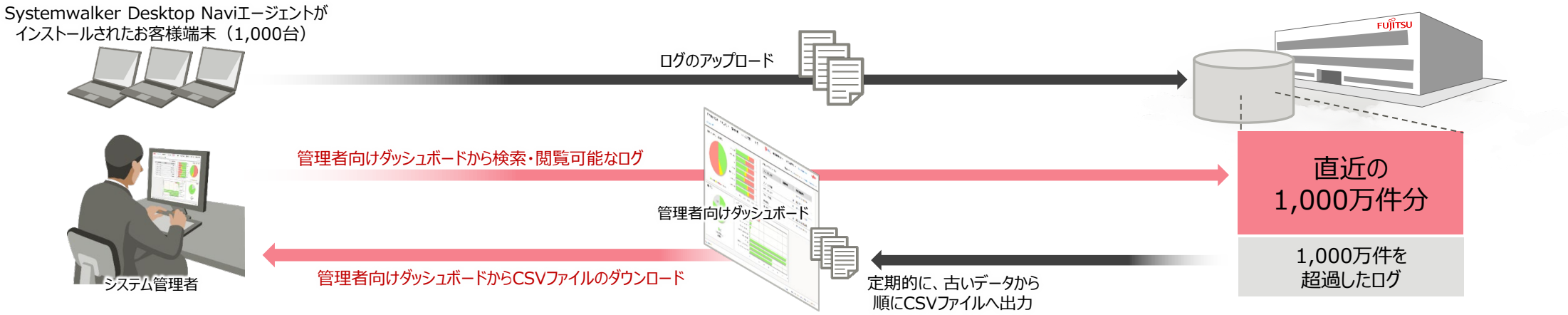
Systemwalker Desktop Naviをお使いいただく場合、本章でご紹介させていただく内容以外にもいくつかの制限事項・留意事項がございます。
製品ホームページにある「Systemwalker Desktop Navi ご利用に際しての制限事項/留意事項について」を事前にご確認くださいますようお願い申しあげます。
https://www.fujitsu.com/jp/software/systemwalker/desktop-navi/

基本サービスのログ保存期間について

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。

【例】1,000台分のアカウントをご契約いただいたお客様は、直近の1,000×10,000=10,000,000件のログがデータセンターのデータベース上に保存されており、Webダッシュボードから閲覧・検索することができます。



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。

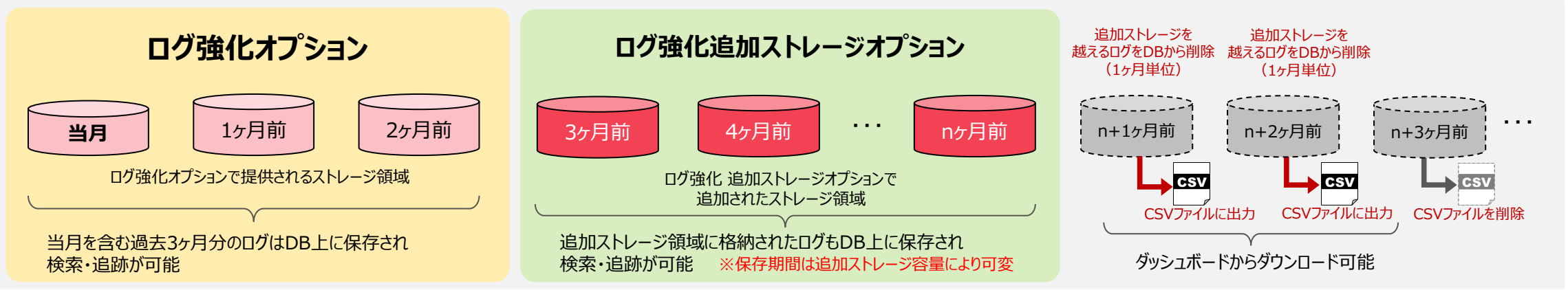
CSV出力されたログファイルの保存期間

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。

ログ強化オプションサービスのログ保存期間について

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。

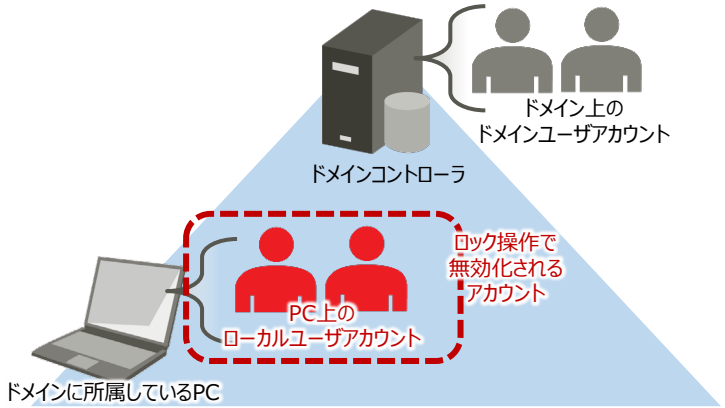
Windows® の紛失対策について

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PC上に作成されているローカルユーザーアカウントのみとなり、ドメインユーザー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PC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。



Active Directory ドメイン

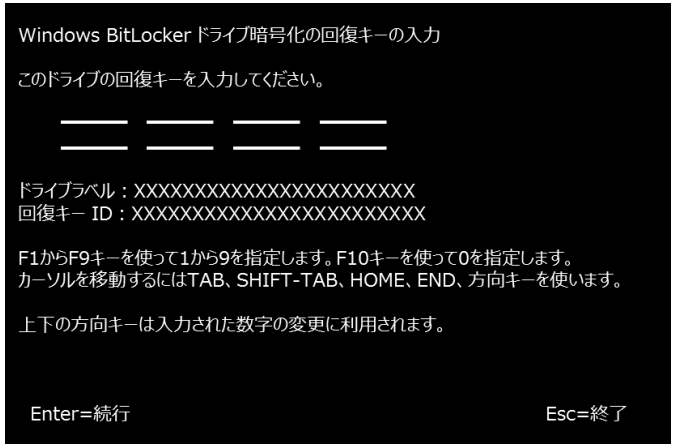
Windows® のワイプ操作について

【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PC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**PCは、PC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、PCを起動することはできません。また、PCからハードディスクドライブを取り出して、他のPC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。

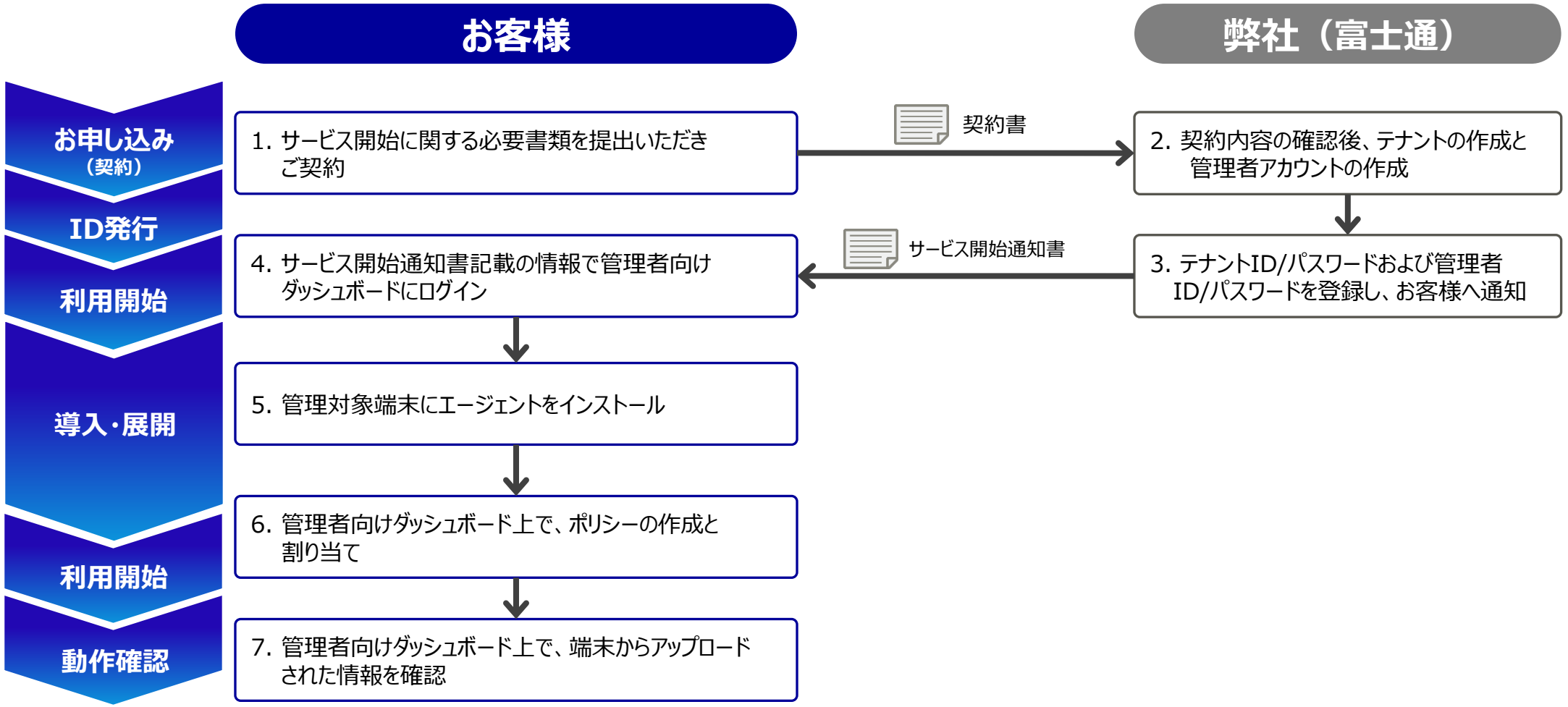


■ 起動時のBitLocker®ドライブ回復キー入力画面（例）

9. 導入・サポート、商標

- お申し込みから利用開始まで
- 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



サービス時間・サポート受付時間

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。

登録商標

- 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。
- 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。

FUJITSU