動作環境

ソフトウェア名	サーバ動作 OS	クライアント動作 OS
Systemwalker Desktop Patrol V16	Microsoft® Windows Server®	管理コンソール Windows® クライアント / 自動検知 PC Windows® Microsoft® Windows Server®
Systemwalker Desktop Keeper V16	Microsoft® Windows Server®	Windows® Microsoft® Windows Server®

※各OSのバージョン、その他動作環境の詳細については、Webサイトにてご確認ください。
※Citrix XenAppクライアント（仮想デスクトップ）上での操作記録は、別途、Systemwalker Desktop Keeperのオプション商品を導入いただくことで対応可能です。

標準価格

Systemwalker Desktop Patrol V16

商品名	標準価格（税別）
Systemwalker Desktop Patrol サーバライセンス for Windows (SL＆S)	9,790円（月額）より
Systemwalker Desktop Patrol クライアントライセンス for Windows (SL＆S)	380円（月額）より
Systemwalker Desktop Patrol メディアパック(64bit)V16	11,000円

Systemwalker Desktop Keeper V16

商品名	標準価格（税別）
Systemwalker Desktop Keeper サーバライセンス for Windows (SL＆S)	19,100円（月額）より
Systemwalker Desktop Keeper クライアントライセンス for Windows (SL＆S)	530円（月額）より
Systemwalker Desktop Keeper メディアパック(64bit)V16	11,000円

※メディアパックは、インストール用媒体商品で使用権は付属しておりません。別途、必要なライセンス商品をご購入ください。
※クライアントが 10台以上の場合は、割引価格でご購入頂けます。
　また、クライアントが300台以内限定でご利用の場合は、別途、キャンペーン商品をご利用頂くことができます。詳細は、お問い合わせください。

動作環境の詳細、全機能のご説明は Web サイトに掲載しています

Systemwalker Desktop Patrol
https://www.fujitsu.com/jp/software/systemwalker/desktop-patrol/

Systemwalker Desktop Keeper
https://www.fujitsu.com/jp/software/systemwalker/desktop-keeper/

Green Policy Innovation

製品・サービスについてのお問い合わせは
富士通コンタクトライン（総合窓口）
0120-933-200
受付時間 9:00～12:00および13:00～17:30 (土曜・日曜・祝日・当社指定の休業日を除く)
富士通株式会社 〒105-7123 東京都港区東新橋1-5-2 汐留シティセンター
https://www.fujitsu.com/jp/software/systemwalker/

CZ4300-8-2024年1月

FUJITSU

システムウォーカー デスクトップ パトロール

Fujitsu Software Systemwalker Desktop Patrol

システムウォーカー デスクトップ キーパー

Fujitsu Software Systemwalker Desktop Keeper

情報漏えい対策ソリューション

パソコンの資産管理、セキュリティ対策
パソコンからの情報漏えい防止

充実した管理機能で
確実に情報漏えいリスクを低減し
将来にわたり安心できる
情報セキュリティ対策を実現します。

近年、利便性の向上や業務効率化を目的とし、従来のパソコン環境に加えて
モバイルパソコンの活用など、デバイスの多様化が進んでいます。
デバイスの多様化は、セキュリティリスクを増大させる要因にもなるため、
情報セキュリティ対策の強化がますます重要になります。
『Systemwalker Desktop Patrol』『Systemwalker Desktop Keeper』は、国内外のお客様に
10年以上にわたりご提供するなかで、日本企業の海外進出や個人情報保護法、省エネ法への対応、
仮想化、ワークスタイル変革などICT環境の変化に合わせ、エンハンスを重ねてきました。
本製品の充実した機能により、変化の激しい社会でも、継続的に情報セキュリティ対策を強化できます。

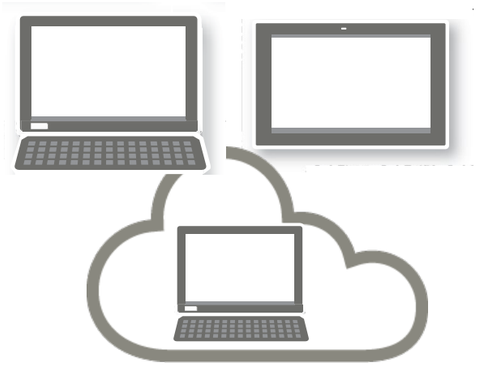
製品の特長

利用者のミスによる情報漏えいを防止

情報漏えいの原因には、重要な情報を保存しているUSBの紛失や、ファイルを添付したメールの誤送信など、利用者の過失に加え、利用者の不正によるものも多く挙げられます。過失と不正、どちらにも対策を講じ、情報漏えいを防ぎます。

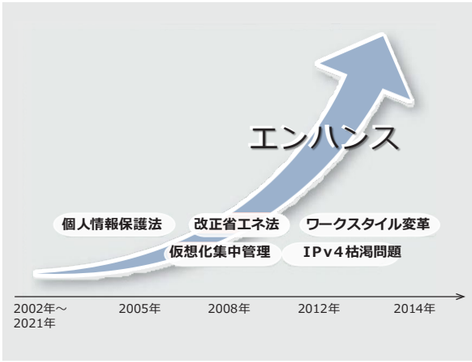
パソコンだけではなく、仮想デスクトップやシンクライアントもまとめて管理

パソコンだけではなく、仮想デスクトップやシンクライアントもまとめて管理し、より安全なセキュリティ対策を講じることができます。



ICT環境の変化によるセキュリティ対策の要件にスピーディーに対応

日本企業の海外進出、法改正、ICT環境の変化などにより生じるお客様のセキュリティ対策の要件にスピーディーに対応します。

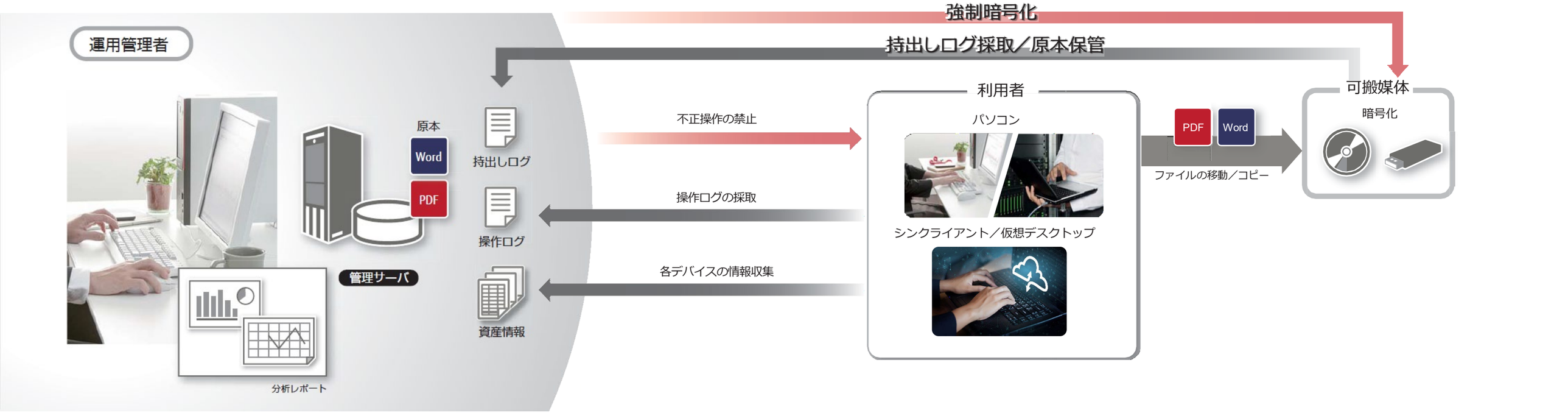


セキュリティ情報の見える化から対処まで実施

パソコンのセキュリティ対策などの運用状況と問題点を一目でわかるように表示し、問題のあるパソコンに強制的にセキュリティパッチを適用するなどの対処を実施できます。

様々なシーンでお客様の課題を解決し、安心してご利用いただける情報漏えい対策ソリューションをご提供いたします。

『Systemwalker Desktop Patrol 』『Systemwalker Desktop Keeper』 では、業務の利便性を考慮お客 した柔軟なセキュリティ対策を実施できます。
様の課題を解決し、安心してご利用いただける情報漏えい対策ソリューションをご提供いたしま す。



情報漏えい対策

利用者の過失による情報漏えいを防ぐ

利用者の故意による情報漏えいを防ぐ

ICT 資産管理／セキュリティ管理

セキュリティリスクを把握する／対策を講じる

レポートで対策状況を分析する

機能一覧

利用者の過失による情報漏えいを防ぐ

可搬媒体紛失による情報漏えいを防ぎたい

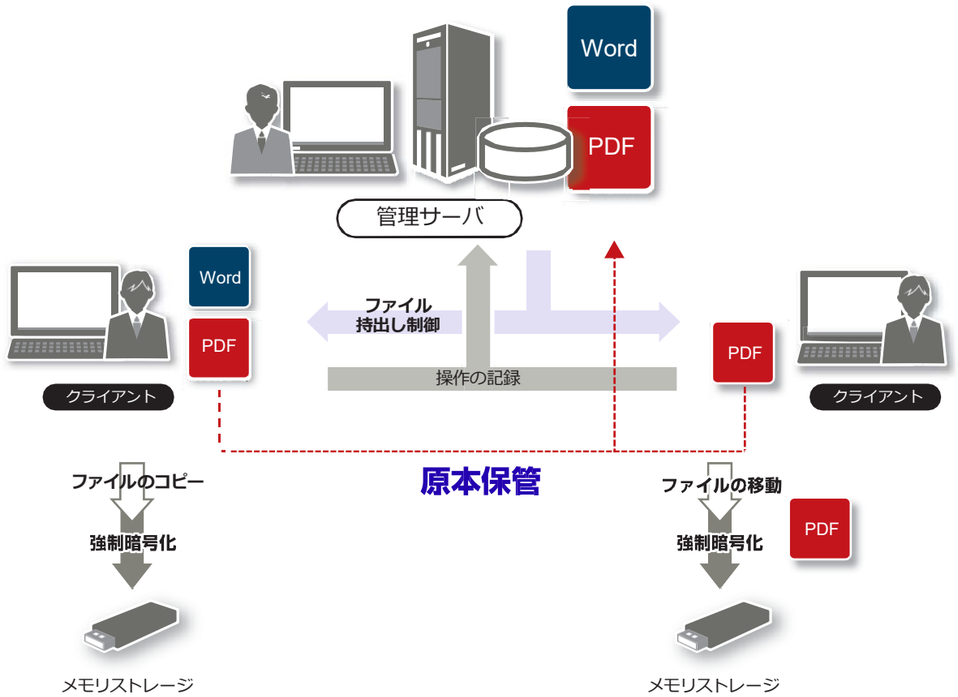
Systemwalker Desktop Keeper

利用者の業務を考慮したファイル持出し時の制御

USBなどの可搬媒体の紛失による情報漏えいを防ぐために、利用者が可搬媒体でファイルを持出せないように設定できます。
しかし、利用者の業務によってはファイルの持出しが必要な場合もあります。
このような場合には、ファイルの暗号化や原本を保管する機能により、万が一、可搬媒体を紛失した時も情報漏えいを防いだり、紛失した可搬媒体に保存していた情報を特定したりできます。

■ 強制的に暗号化
持出すファイルを強制的に暗号化します。また、ファイルを暗号化する時に利用者が復号する操作について制限できます（復号化のためのパスワード、パスワード入力を試行できる回数、復号できる期間）。このように可搬媒体に保存される情報を暗号化することにより、紛失してもファイルに保存されている内容を参照されません。

■ 原本の保管
ファイルを持出した時のログが記録されるとともに、持出したファイルの複製を原本として保管します。可搬媒体を紛失した時にファイルに保存されていた内容を確認して対応策を検討し、迅速に対処できます。



自己復号型暗号化ファイル:
暗号形式を自己復号型にすると、復号するパソコンにSystemwalker Desktop Keeperがなくても復号パスワードを入力することで復号できます。

メール誤送信による情報漏えいを防ぎたい

Systemwalker Desktop Keeper

メールの添付ファイル制限

誤送信により、第三者に情報を参照されることを防ぎます。
メールを介した情報漏えいを防ぐために、添付するファイルを制限できます。
- 暗号化されていないファイルは添付不可とする
- 特定の拡張子のファイルは添付不可とする、もしくは特定の拡張子のファイルのみ添付を許可する

また、メール送信時に、メール本文および添付ファイルの内容を記録します。

メール送信時の宛先確認

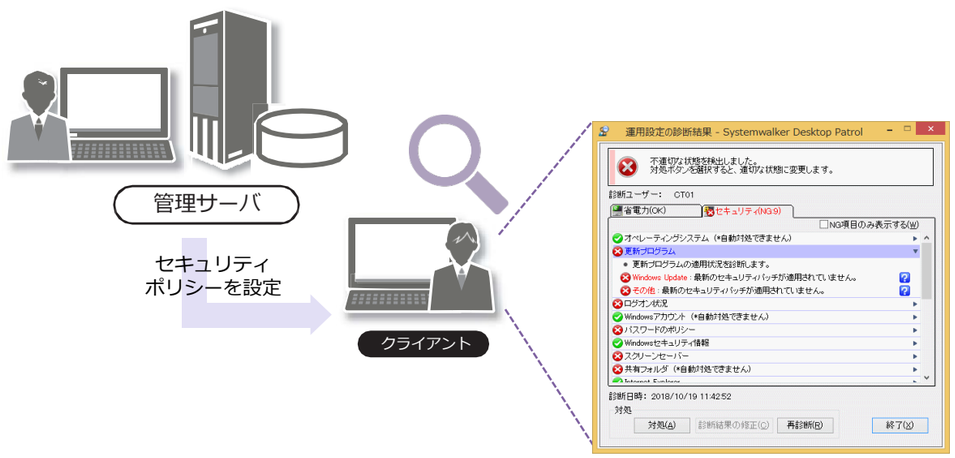
メールの誤送信を防ぐために送信時に宛先を確認します。
送信しようとしたメールの宛先に、許可されたドメイン以外が含まれている場合は、宛先確認のメッセージが表示され、送信が保留にされます。利用者は、メッセージに表示されている宛先一覧を確認して、正しければ送信し、誤っていれば送信をキャンセルできます。
対象メールソフト：・SMTPプロトコルを使用するメールソフト
・Microsoft Outlook（Microsoft Outlook 2013以降）

利用者の端末セキュリティ設定ミスによる情報漏えいを防ぎたい

Systemwalker Desktop Patrol

端末設定の自動確認／警告

利用者の設定ミスで端末セキュリティが低下しないよう、端末のセキュリティ設定を自動で確認し、社内のポリシー水準に達していない場合は自動で利用者に警告をします。また、改善されるまで警告を通知し、利用者自らが対処することで利用者の意識の向上を図ります。



主なセキュリティ診断項目:
オペレーティングシステム、更新プログラム、ログオン状況、Windowsアカウント、パスワードのポリシー、共有フォルダ、Windowsセキュリティ情報、スクリーンセーバー、ファイアウォール、BIOSハードディスクパスワード、ウイルス対策ソフトウェア、暗号化ソフトウェア、Google デスクトップの状況、禁止ソフトウェア

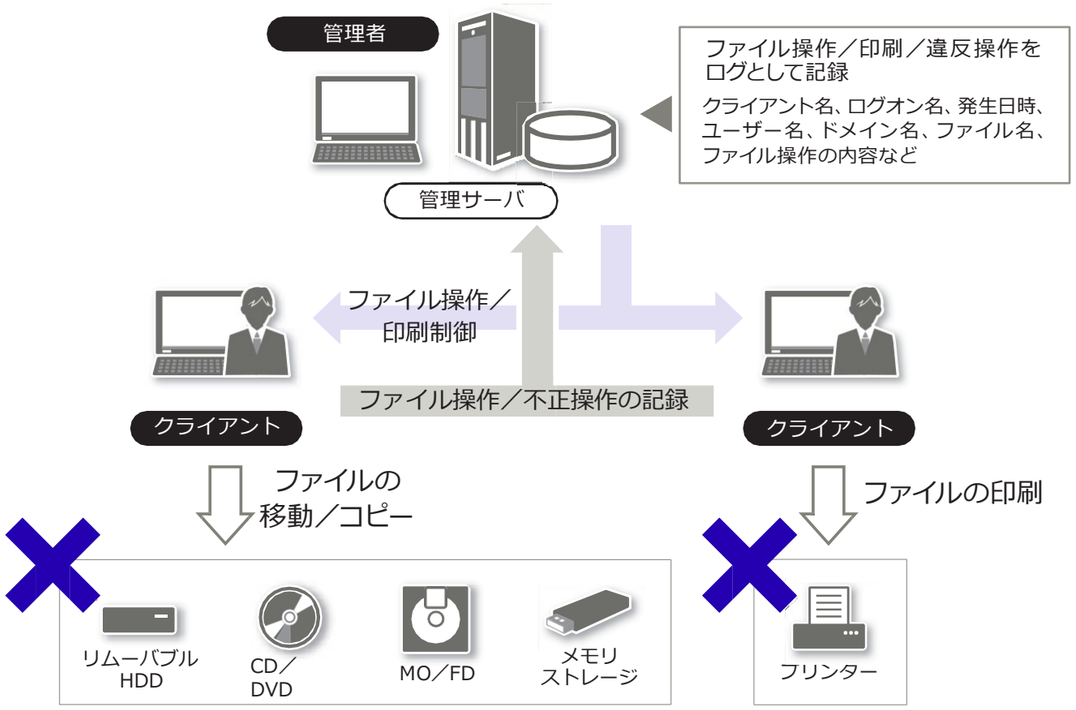
利用者の故意による情報漏えいを防ぐ

利用者による不正操作を禁止したい

Systemwalker Desktop Keeper

クライアントにおける各種の不正操作を強制的に禁止

利用者の故意による情報漏えいを防ぐため、利用者に不正な操作をさせないようにする必要があります。
本製品の導入により、例えば、「ファイルの持出し」「 禁止しているアプリケーションからの印刷 」など、
セキュリティポリシーに基づき、これらの不正操作を利用者に禁止することができます。



なお、業務でファイルを持出さなくてはならない場合に、その利用者に対し期間や時間帯を指定して、一時的にファイルの持出しを許可することができます。許可した期間が過ぎると、自動的にファイルの持出しが禁止されている状態に戻るため、手動操作による戻し忘れの心配がありません。

禁止機能:
業務に関係ないアプリケーションの起動、ネットワークドライブへの書き込みなど、情報漏えいにつながる操作や、業務やシステム運用の妨げとなる操作を禁止できます。
禁止できる内容については、P.14 機能一覧の 「禁止機能」をご覧ください。

操作ログを管理して違反操作を発見したい

Systemwalker Desktop Keeper

パソコン/仮想デスクトップの操作をログとして採取、管理サーバに記録

「いつ」「誰が」「何をしているのか」といった操作をログとして管理サーバに記録し、一元管理します。
また、利用者が違反操作をした場合に、管理者にメールで通知することもできます。ログとして記録されることにより、利用者に情報漏えいにつながる操作を意識させ、情報漏えいを未然に防ぐ心理的な効果が期待できます。

例:アプリケーションの起動と終了のログ

名称	発生日時	ユーザー名	ドメイン名	種別	区分	付帯	内容
PC001	2021/12/21 08:37:05	suzuki	PC001	PC起動	正規		コンピュータを起動しました。起動モード:[通常モード起動]
PC001	2021/12/21 08:58:59	suzuki	PC001	PC接続	正規		コンピュータ[VPC-DTCT(物理PC)]からコンピュータ[PC001(仮想PC
PC001	2021/12/21 08:59:03	suzuki	PC001	ログオン	正規		ログオンしました。認証先:[PC001]
PC001	2021/12/21 08:59:06	suzuki	PC001	アプリケーション起動	正規		[cmd]を起動しました。
DTSV	2021/12/21 08:59:08	Administrator	DTSV	ファイル操作	正規		操作:[作成]、ファイル名:[C:¥Users¥Administrator¥Desktop¥見積
DTSV	2021/12/21 08:59:17	Administrator	DTSV	ファイル操作	正規		操作:[削除]、ファイル名:[C:¥Users¥Administrator¥Desktop¥おしら
DTSV	2021/12/21 08:59:17	Administrator	DTSV	ファイル操作	正規		操作:[変名]、ファイル名:[C:¥Users¥Administrator¥Desktop¥見積
PC001	2021/12/21 08:59:18	suzuki	PC001	アプリケーション終了	正規		[cmd]を終了しました。

■ 主なクライアント操作の記録

- アプリケーションの起動／終了
- スプール経由の印刷情報（印刷時刻、文書名など）
- ファイルサーバやローカルデバイスに対するファイル操作
- 運用中の機器構成の変化（Plug＆Play、USB デバイス装着など）

記録できる内容については、P.14 機能一覧の「記録機能」をご覧ください。

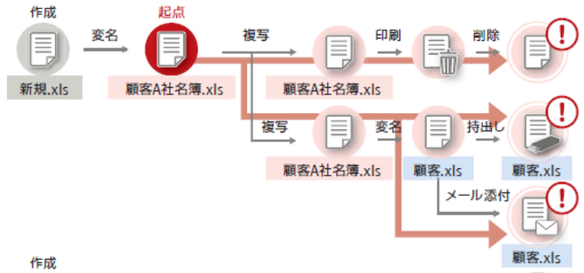
不正操作を追跡し利用者を特定したい

Systemwalker Desktop Keeper

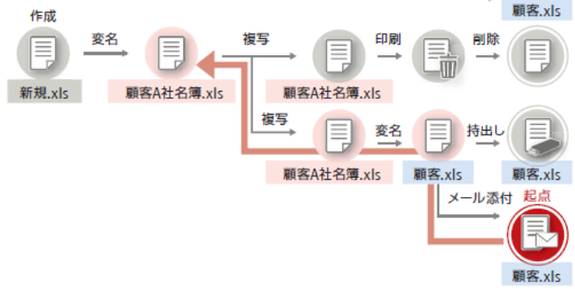
不正操作の追跡や利用者を特定

収集・記録したログに対して、キーワードや期間、時間帯、曜日を指定し、検索できます。

■ フォワードトレース
該当ファイルの操作履歴を、過去から現在に向かって追跡することで、特定の操作を行っているクライアントや利用者を判別できます。



■ バックトレース
情報漏えいや外部への持出しの可能性があるファイルを特定できた場合に、該当ファイルの操作履歴を検索できます。



セキュリティリスクを把握する／対策を講じる

セキュリティ状況を一目で把握したい

Systemwalker Deskztop Patrol
Systemwalker Desktop Keeper

セキュリティ状況を見える化、対策の実施

次の3つの操作でセキュリティ状況の把握から解決まで導きます。

1. クライアントの運用状況を把握

クライアントの運用状況が項目ごとに集計されるため、問題の有無を把握できます。問題が発生している場合は、その台数が表示されます。

2.セキュリティ上問題があるクライアントを特定

リンクをクリックすると、対象のパソコンの一覧が表示され、問題があるクライアントを特定できます。

3. セキュリティパッチの強制適用

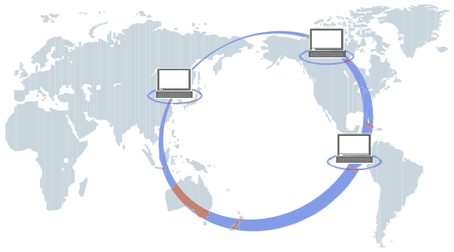
対処を選択して実行することで、セキュリティパッチを強制適用できます。

海外を含む各拠点のセキュリティを統制したい

Systemwalker Desktop Patrol
Systemwalker Desktop Keeper

国内、海外拠点のパソコンを一元管理

国内と同じセキュリティポリシーで、海外拠点のパソコンの操作ログの収集、操作制御、およびICT資産の管理ができます。 また、拠点ごとに運用管理者を分ける必要がないため、世界中のどこの 拠点でもセキュリティを統制できます。国別に管理したいときには、国 ごとに異なるセキュリティポリシーを設定することもできます。



ICT 資産を一括管理したい

Systemwalker Desktop Patrol

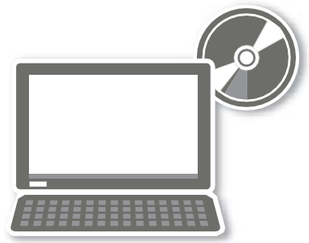
ICT 資産を自動検知して台帳管理

ネットワークに接続されたICT機器を自動検知し、収集された資産（インベントリ）情報により資産状況を把握できます。コンピュータ名、ドメイン名、TCP／IP情報などのハードウェア固有情報を自動取得します。
また、自動取得した情報を基に資産管理台帳を常に最新に維持し、ICT機器の棚卸を支援します。

ソフトウェアの導入／利用状況を把握

パソコンから自動的にソフトウェア情報を収集し、ソフトウェアの導入／利用状況を把握することで、以下のようなことができます。

- 遊休ライセンスの活用やライセンスの過不足管理によるコスト削減
- リース契約切れパソコンに残っている不要なライセンスの再利用による効率的な資産管理
- ソフトウェア資産管理＊1に必要な資産管理台帳をもとに、規格＊2に則したライセンスの使用状況の適切な管理



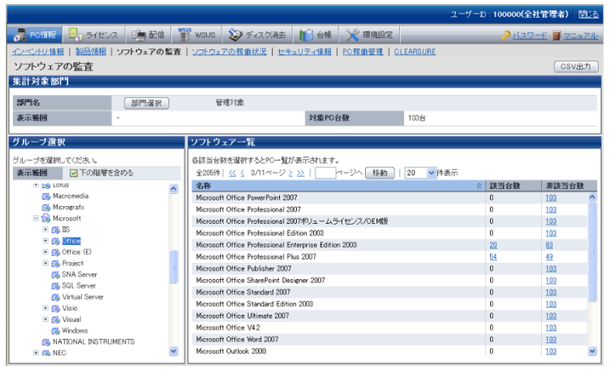
＊1：Software Asset Management に対応
＊2：国際規格ISO／IEC 19770-1:2006、日本工業規格JIS X0164-1:2010

セキュリティレベルを確実に維持したい

Systemwalker Desktop Patrol

セキュリティパッチの監査と自動適用で、セキュリティレベルを確実に維持

最新のセキュリティパッチやウイルスパターンが適用されていない「セキュリティに問題のあるパソコン」を簡単に確認できます。
クライアントへの配信、適用、適用状況の把握まで、セキュリティパッチの一連の作業を自動化できます。
セキュリティパッチが新たに発行された場合は、Microsoft社の専用サイトから取得し自動適用します。
WSUSと連携することで、FeatureUpdateのような大型のセキュリティパッチも自動適用できます。
また、WSUSでは更新管理ができないクイック実行形式のOfficeについても、セキュリティパッチを自動適用できます。



レポートで対策状況を分析する

セキュリティの監査や統制状況をレポート形式で確認したい

Systemwalker Desktop Patrol

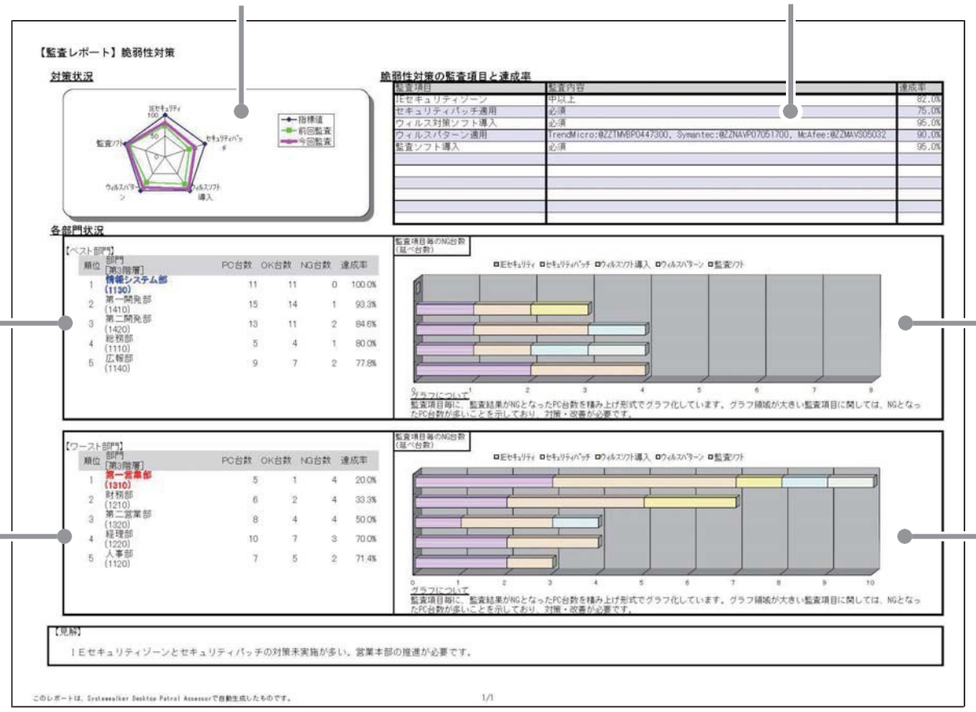
監査レポートで対策状況の把握、リスクのある部門やパソコンの把握

利用者がセキュリティ対策を正しく実施しているかの調査から、対策状況の把握や分析まで、内部監査の迅速化を支援します。
例えば、利用者がBIOSパスワードやスクリーンセーバーを設定しているかなど、対策項目ごとに監査し、対策の実施状況を集計、グラフ化してレポート出力します。
出力したレポートは、セキュリティ対策の運用の見直しやリスクへの早期対策に活用できます。

対策ごとのセキュリティ設定の監査状況レポート

前回と今回の対策状況をレーダーチャートで出力

監査項目に対する監査内容と結果を出力



ベスト部門、ワースト部門を出力

監査項目ごとにNGとなったパソコン台数をグラフ化

主な監査可能な項目:

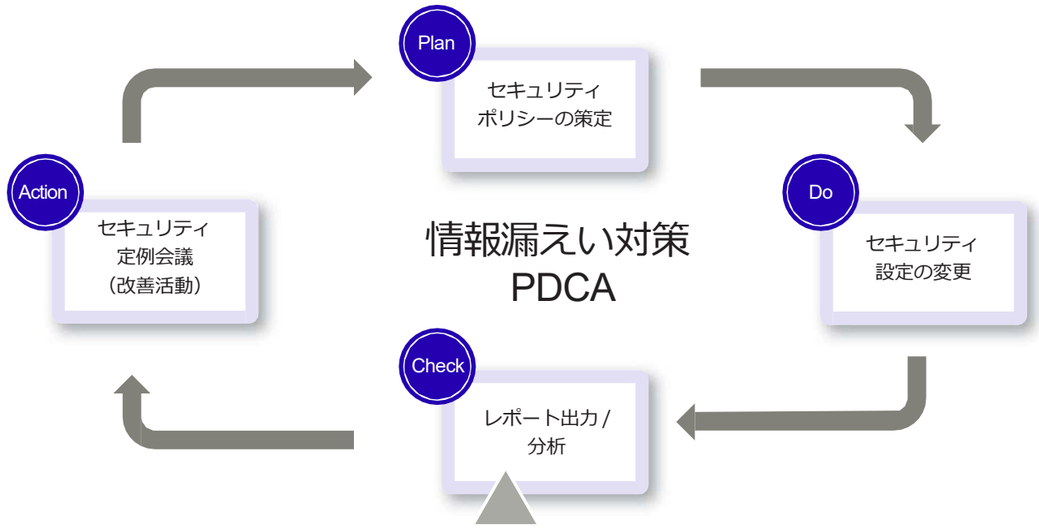
- オペレーティングシステム（サポート状況）
- Windows更新プログラム（適用状況）
- ログオン状況
- パスワードポリシー
- Windows Update（自動更新の設定）
- 共有フォルダ（設定状況）
- Internet Explorer（セキュリティゾーン設定状況）
- BIOSパスワード
- ウイルスパターン状況
- 定時スキャン状況
- 禁止ソフトウェア導入状況

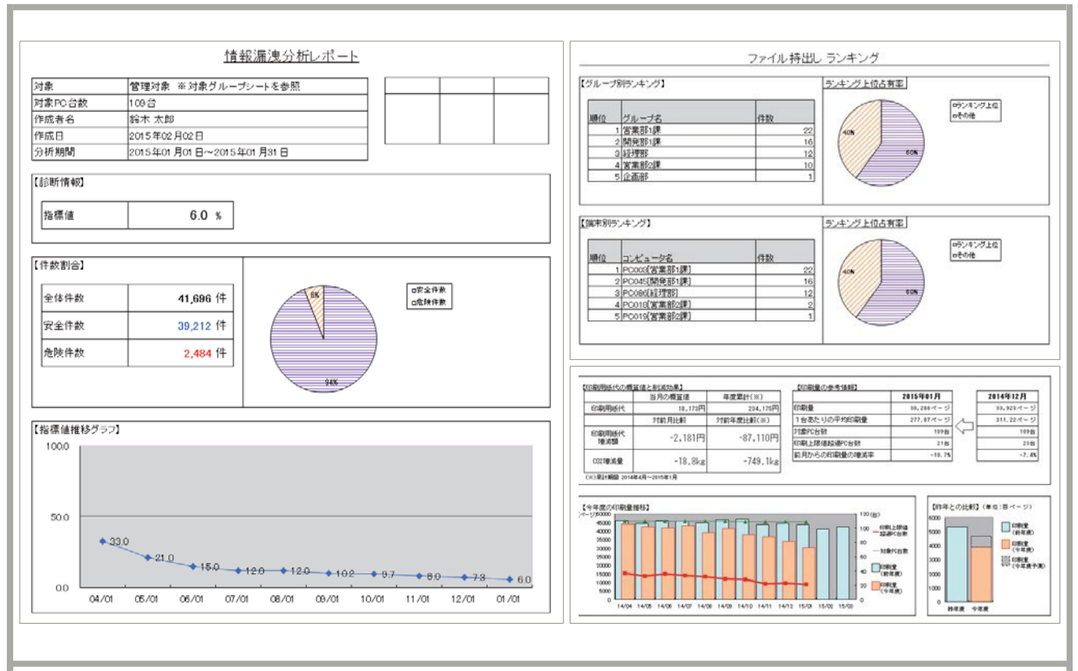
セキュリティ状況を定期的に評価／分析してリスクの低減につなげたい

Systemwalker Desktop Keeper

情報漏えい対策の実施効果を確認、対策改善の PDCA 支援

様々な視点でのログ分析やレポート出力により、不正操作や持出し操作などを確認でき、セキュリティ状況の見える化を実現します。
コンプライアンス状況／セキュリティリスク状況を把握し、セキュリティ対策の見直しやセキュリティリスク回避のためのPDCAサイクルの運用を支援します。





出力できるレポート

- 情報漏えい分析レポート ・ 端末利用分析レポート ・ 違反操作分析レポート
- 総合分析レポート ・ 印刷量監査レポート

機能一覧

Systemwalker Desktop Patrol

■ インベントリ情報管理

- 自動インベントリ収集（パソコン） P.10 でご紹介！
- インベントリ収集負荷の軽減
- 非常駐インベントリ収集処理
- ネットワークに接続していない機器のインベントリ収集
- インベントリ取込みユーザー情報の定義
- Windows BitLockerとの連携
- シンクライアントPCの管理
- UNIX サーバのインベントリ収集（Systemwalker Centric Manager 連携での UNIX サーバの資産管理）

■ セキュリティパッチの自動適用

- 自動セキュリティ監査
- セキュリティパッチの自動ダウンロードと適用 P.10 でご紹介！
- セキュリティパッチ適用の選択
- WSUS（Windows Server Update Services）との連携
- シンクライアントPCへのセキュリティパッチ適用

■ ソフトウェアの監査

- 使用禁止ソフトウェアの検出
- 実行ファイルの制御

■ 資産管理台帳

- 機器管理
- 契約管理
- 棚卸支援

■ パソコンのデータ消去と管理

- パソコンのデータ消去と管理

■ モバイルパソコン運用

- モバイルパソコンの資産管理のための設定
- モバイルパソコンの負荷軽減のための設定

■ セキュリティ監査／統制

- パソコンのセキュリティ監査／統制
- 省電力の監査／統制（グリーン ICT 対応）
- レポート出力による複合機の稼働状況の確認
- 省電力とセキュリティの両立
- ネットワークセキュリティ製品連携による検疫
- セキュリティパッチのダウンロード先切替（ローカルブレイクアウト機能）

■ ライセンス管理

- ソフトウェア辞書
- ソフトウェア資産管理（SAM：Software Asset Management）
- ライセンス割当・ライセンス使用状況の確認
- ライセンス一括割当・一括解除
- ライセンス違反アラーム通知

■ ソフトウェアの配信

- ソフトウェアの配信先の指定
- 配信ソフトウェア実行時の権限変更

■ レポート出力機能 P.11でご紹介!

- 資産稼働状況
- 契約状況
- 棚卸状況
- ライセンス使用状況
- 消費電力量の監査
- 省電力設定監査
- 複合機／プリンター稼働状況
- セキュリティ監査

■ 運用管理の効率化

- 運用状況の表示 P.9 でご紹介!
- リモート操作
- CSV ダウンロード
- クライアント分散設置などへの対応
- インターネット対応
- 大規模運用への対応

Systemwalker Desktop Keeper

■ 禁止機能

- アプリケーション起動禁止
- 許可のない USB 媒体の使用禁止 P.7 でご紹介！
- ログオン制御
- 印刷の禁止 P.7 でご紹介！
- 紙の印刷量削減（グリーン ICT 対応）
- PrintScreen キーの無効化
- メール添付ファイルの禁止 P.6 でご紹介!
- ファイル持出し禁止 P.5 でご紹介！
- サービス／プロセス起動制御
- リムーバブルメディアからのデータ読み込み禁止
- URL アクセス禁止
- Web サーバへのファイルのアップロード、ダウンロードの禁止
- FTP サーバへの操作禁止
- 仮想 PC とパソコン間のクリップボード操作を禁止
- ネットワークドライブの操作禁止
- DVD ／ CD ドライブからの読み込み禁止
- クライアント（CT）への緊急対処

■ 管理機能

- 管理コンソール
- ポリシー設定、配付（PC／PCのグループ単位またはユーザー単位）
- 部門管理
- メール通知、イベントログ出力
- 自己版数管理
- ログビューアー
- ファイル追跡
- ログフィルター
- クライアントパソコンの状況表示 P.9 でご紹介!
- バックアップログの閲覧
- Systemwalker Desktop Patrol の資産管理画面の呼び出し
- クライアント（CT）へ用紙使用状況の通知
- PC使用時間の通知

■ 記録機能 P.8 でご紹介!

- クライアント操作の記録
- デバイス構成変更の記録
- 画面キャプチャーの記録
- ファイル持出しの記録（原本保管）
- Citrix XenApp クライアント(仮想デスクトップ)上での操作の記録
- Web サーバからのファイルアップロード、ダウンロード記録
- FTP サーバへの操作記録
- 仮想PCとパソコン間のクリップボード操作ログ
- 仮想環境への接続・切断ログ
- クリップボード操作ログ

■ ログ分析機能

- 情報漏えい予防診断
- 目的別集計
- 利用者操作の追跡（ログ追跡） P.8でご紹介!
- 内部不正リスク検出

■ レポート出力機能 P.12 でご紹介！

- 情報漏えい分析
- グリーン ICT 対応