Fujitsu Software Systemwalker Desktop Keeper 機能ご紹介

2024年1月

富士通株式会社

目次

FUJITSU

本資料は、以下の製品を対象とします。
・Fujitsu Software Systemwalker Desktop Keeper V16(以降、DTK)
・Fujitsu Software Systemwalker Desktop Patrol V16(以降、DTP)

機能概要

- 製品特長
- 日常運用の簡便性
- 問題操作状況の表示（ダッシュボード機能）
- 状況画面の監査項目
- 報告レポートの作成
- 管理者へのメール通知
- 機能概要
- V16強化機能

製品特長

FUJITSU

パソコン、仮想端末のログ収集を実現
パソコン操作の禁止と記録、原本保管により漏えい時の追跡も可能

操作ログの収集（閲覧）

- 利用者単位でのパソコンの操作記録を一元管理。
- パソコンの16種類のログを収集。

操作ログの収集（追跡）

- キーワード、期間などにより検索し、絞り込んだ操作に対して前後の操作を追跡。
- バックトレースログで漏えい元を追跡。

操作禁止

- 情報漏えいリスクのある操作を禁止。
- セキュリティポリシーに基づき、利用者の業務に不必要な操作を禁止。
- 暗号化済みの添付ファイルのみのメール送信。

レポート機能

- セキュリティ対策やセキュリティリスクの状況、パソコン利用実態の把握。

日常運用の簡便性

FUJITSU

■ 日常運用を週次、月次、問題発生時に応じて支援し、管理者の負担を軽減

週次

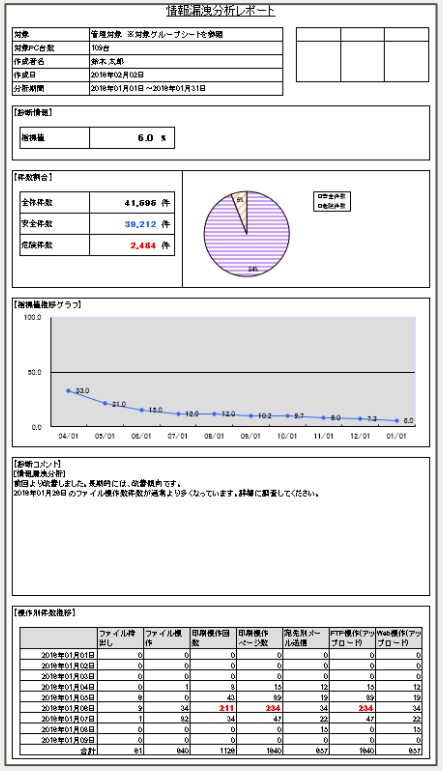
ダッシュボード機能による違反状況の把握と詳細確認

GUI上で確認

問題操作を実施した
端末がある場合は、
管理者へメールで通知

月次

報告レポートの作成



問題発生時

違反操作時の
管理者への通知

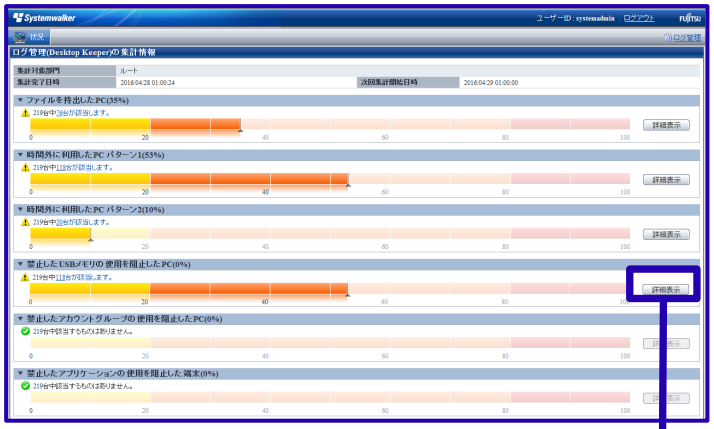
- **違反操作が行われた場合、管理者へメールで通知**

問題操作状況の表示（ダッシュボード機能）

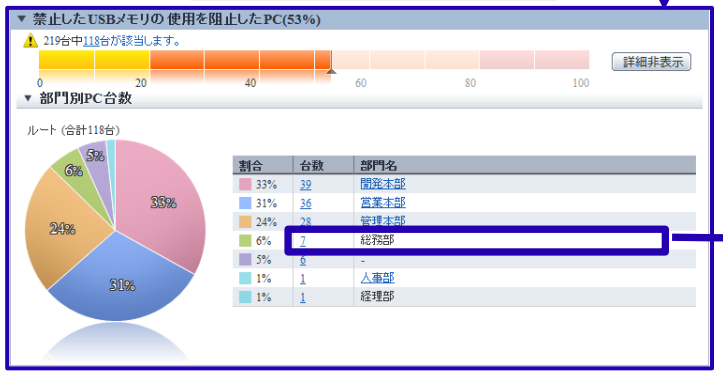
FUJITSU

- 全社・部門単位に集計した情報漏えいにつながる問題操作の発生状況を可視化できます。
- 管理者はひと目で問題の有無を確認できます。問題がある場合には問題操作が行われた端末、問題操作の詳細確認、利用者の特定まで一連の操作でできます。

問題操作状況の把握

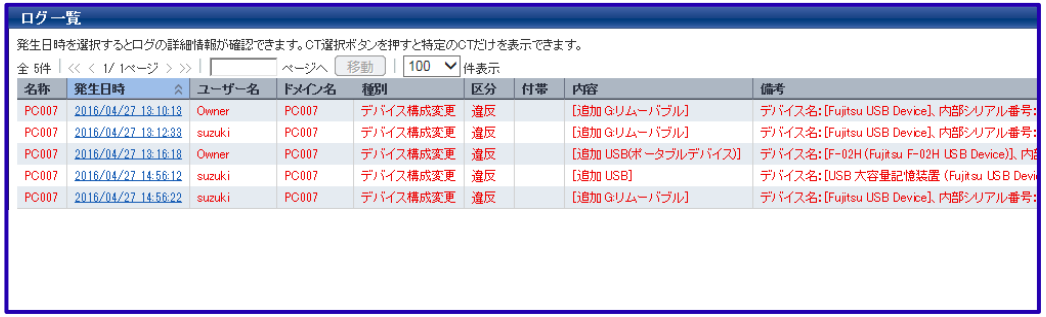


問題操作状況の把握（詳細）



問題操作が行なわれた端末の確認

問題操作の詳細確認



状況画面の監査項目

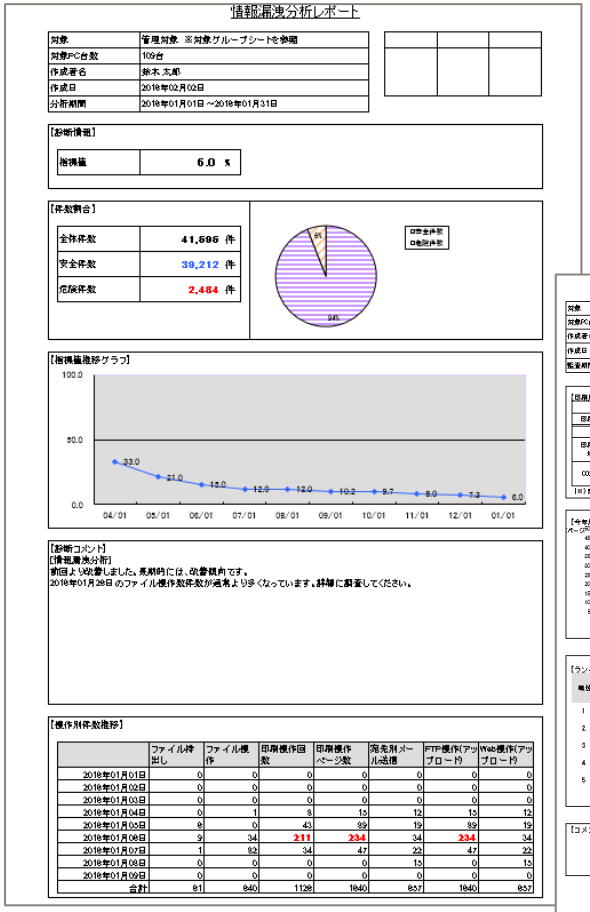
FUJITSU

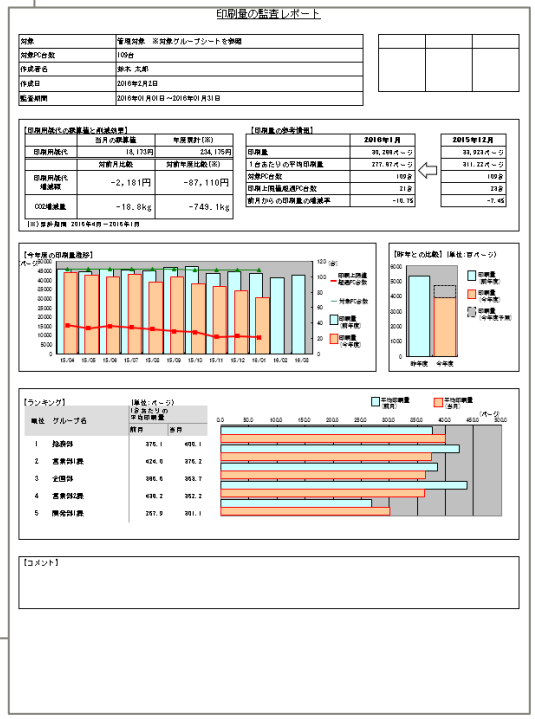
監査項目	説明
ファイルを持出したPC	ファイル持出し操作が行われたパソコンの数を表示します。持出し先の外部記憶媒体のドライブ種別（リムーバブル、CD/DVD、ネットワーク）で絞り込みもできます。
時間外に利用したPC（パターン１）	管理者が、パソコン利用時間外と設定した時間帯（曜日、時間）にログオン/ログオフされたパソコンの数を表示します。
時間外に利用したPC（パターン２）	
禁止したデバイス/メディアの使用を阻止したPC	許可していないデバイス/メディアの使用を試みたパソコンの数を表示します。
禁止したアカウントグループの使用を阻止したPC	ログオンを禁止しているアカウントグループに属するユーザーIDでログオンを試みたパソコンの数を表示します。
禁止したアプリケーションの使用を阻止した端末	使用を禁止しているアプリケーションの使用を試みたパソコンの数を表示します。
禁止した印刷を阻止したPC	禁止している印刷操作を試みたパソコンの数を表示します。
禁止した添付ファイル付メール送信を阻止したPC	禁止している条件の添付ファイル付きメールの送信を試みたパソコンの数を表示します。
不審なアクセスが行われたPC	パソコンに対する不審なアクセスをしたパソコンの数を表示します。集計対象は「セーフモードによる起動」、「ローカルユーザーによるログイン」、「管理者権限によるログイン」から選択できます。
長期間未接続のPC	長期間ネットワークに接続されていないパソコンの数を表示します。

報告レポートの作成

- レポート出力ツールにより、セキュリティ対策やセキュリティリスクの状況、パソコン利用実態を把握できます。
- 出力できるレポートは全28種です。

レポート名	種類
情報漏洩分析レポート	8種
端末利用分析レポート	4種
違反操作分析レポート	6種
総合分析レポート	1種
印刷量監査レポート	9種

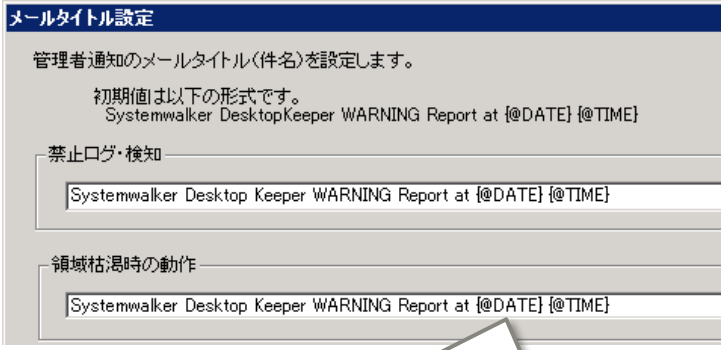




管理者へのメール通知

- 利用者が違反操作を行った際に、管理者へメール通知します。これにより管理者は即時に利用者の違反操作を検知することができます。
  - 部門管理者を設定している場合には、その部門管理者に対してもメールを通知します。
- サーバのディスク容量不足を検知した際に管理者にメール送信します。これにより管理者はサーバの予防保守ができます。
- クライアント(CT)への緊急対処依頼および緊急対処解除時に管理者へメール通知します。これにより管理者は緊急対処の状況を把握することができます。

メールタイトル設定画面



{@DATE} を記載することで操作日時に変換

設定項目	タイトル例
禁止ログ・検知	【警告】{@USER}が{@COMP}にて{@DATE}{@TIME}に禁止機能を操作しています
領域枯渇時の動作	【サーバのディスク容量不足】{@SV}のディスクが減少しています。確認してください。

キーワード	意味
{@DATE}	操作日付
{@TIME}	操作時刻
{@KIND}	操作種別
{@SV}	管理サーバ名

キーワード	意味
{@CT}	CT名
{@COMP}	コンピュータ名
{@USER}	ユーザ名
{@ERR}	エラーの内容

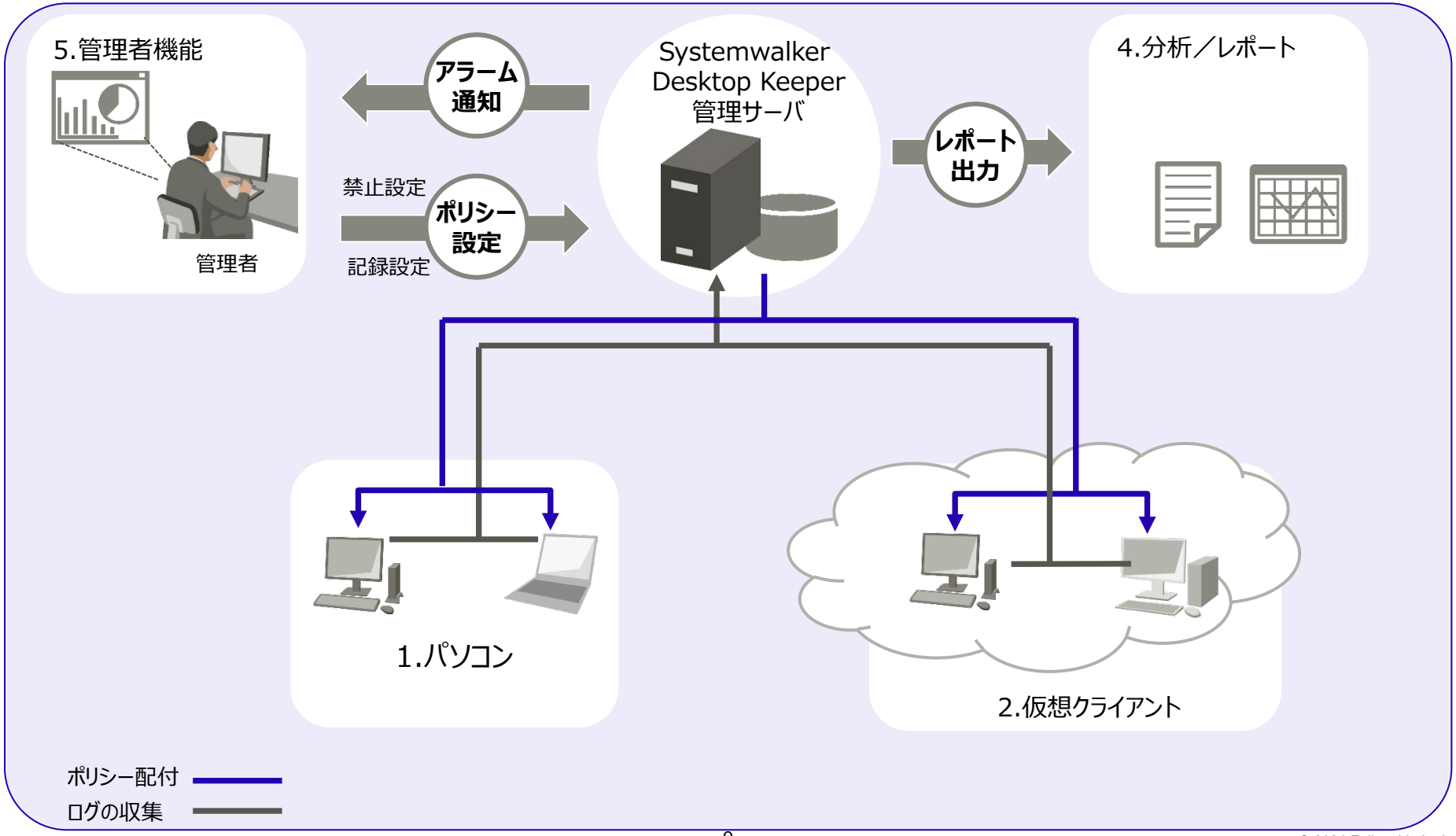
通知メール例

件名：【警告】不正な操作が実行されました。2016/4/1 23:15:00

操作種別：アプリケーション起動禁止
管理サーバ：DTSV(192.168.32.20)
ユーザー名：suzuki
端末：PC001(192.168.32.100)
CTバージョン：4.5.0.1
操作日時： 2016/4/1 23:15:00
詳細：[NOTEPAD]の起動を強制終了しました。

機能概要①

■ パソコンや仮想クライアントを使う利用者の業務内容や環境に合わせた情報漏えい対策ができます。



機能概要②

FUJITSU

■ パソコンの操作記録と禁止

機能名			
ログオン操作記録と禁止	アプリケーション起動／終了記録と起動禁止	PrintScreenキー操作記録と禁止	メール送信／送信中止記録
メール送信時の添付ファイル禁止	メール受信記録	印刷操作記録と禁止	ウィンドウタイトル記録と画面キャプチャ
URLアクセス禁止	Web操作記録	Webアップロード／ダウンロード禁止	FTPサーバ操作の記録と接続禁止
クライアントサービス制御とプロセス制御	ファイル操作の記録と禁止	特定ネットワークドライブへのアクセス許可	時間帯指定・暗号化強制による持出し許可
持出しユーティリティを利用した場合の記録	持出しファイルの原本保管	デバイス/メディアを限定した持出し許可	デバイス構成変更記録
コマンドプロンプト操作記録	連携アプリケーションの記録	環境変更ログ	

■ 仮想クライアントの操作記録と禁止

機能名			
XenAppクライアントの操作記録	仮想環境とパソコン間のクリップボード操作記録と禁止	仮想環境への接続／切断記録	仮想環境とローカル端末の操作の横断検索

機能概要③

FUJITSU

■ ログ分析／出力機能

機能名			
情報漏洩予防診断	操作別集計結果表示	違反操作ランキング	目的別集計機能について
集計結果表示	目的別集計機能項目一覧	分析レポートの出力	情報漏洩分析レポート
端末利用分析レポート	違反操作分析レポート	紙のコストとCO2排出量の『見える化』	複合機／プリンタの紙の使用状況の『見える化』
用紙使用状況の通知			

■ 管理機能

機能名			
ファイル追跡機能	ログフィルター機能	バックアップした過去ログの閲覧	複数管理サーバの統合的なログ閲覧
利用者操作の追跡機能	部門管理機能	USBデバイス登録用の部門管理者権限	自己版数管理機能
ネットワークへの負荷低減	覗き見検知	PC使用時間の把握	Microsoft Teamsアプリ操作証跡管理
操作記録通知による利用者けん制	管理業務の一元管理/現地管理者での独自管理を両立		

■ セキュリティリスクへの対処

機能名			
内部不正リスク検出	緊急対処		

V16強化機能①

FUJITSU

■ Microsoft Teamsに対する操作記録機能に対応

Microsoft Teams(アプリ）に対するファイルのアップロード・ダウンロードの記録に対応しました。
※操作はWeb操作ログ（Webアップロード・Webダウンロード）として記録されます。

■ 英語OS対応

クライアント(CT)、管理コンソールについて英語OSに対応します。

- クライアントのインストールが、Windowsの表示言語（日本語/英語）に合わせて自動的にインストールされます。英語OSの場合、クライアント画面は英語で表示されます。
- 管理画面において、ブラウザの言語設定に応じて自動的に日本語/英語で表示可能となります。

海外拠点にてクライアント(CT)を利用する場合、国内の管理サーバから海外拠点PCと国内PCの一元管理が可能になります。

■ 管理サーバ・ログアナライザーサーバの性能強化 NEW

管理サーバ一台で管理できるクライアント台数を最大5,000台へ、統合管理サーバで管理できるクライアント台数を最大50,000台へ拡大しました。ログアナライザーサーバでは取り扱うことのできるログ量を拡大しました。

■ 統合ログ閲覧データベースの追加 NEW

複数台の管理サーバのログを移入可能な大規模環境でのログ閲覧用高性能データベースを提供します。
（大量ログの検索性能向上、運用面ではログのリストア処理の高速化などの特徴があります。）

NEW V16.2.0からの新機能です。

V16強化機能②

FUJITSU

■ 新環境対応 NEW

以下の環境でのクライアントの動作をサポートします。

- リモート接続環境：Microsoft Entra アプリケーション プロキシ
  （旧称 Azure Active Directory アプリケーション プロキシ）
- 仮想デスクトップ環境：Citrix Cloud with Azure Virtual Desktop
  （FJDaaS with Citrix Cloud）

■ 監視メッセージのポップアップ表示 NEW

端末に対してログオンを行った際、監視開始のメッセージや実際に操作したログの一部をポップアップ表示する機能（操作記録通知）を提供します。テレワーク等、周囲に人がおらず意識が緩みがちな環境でも、監視警告による牽制を自動で行うことにより利用者のセキュリティ意識の低下を防止します。

■ 操作ログ取得の監査強化 NEW

「PrintScreenキー操作記録／禁止」機能において、PrintScreenキー以外のキーの指定が可能になりました。

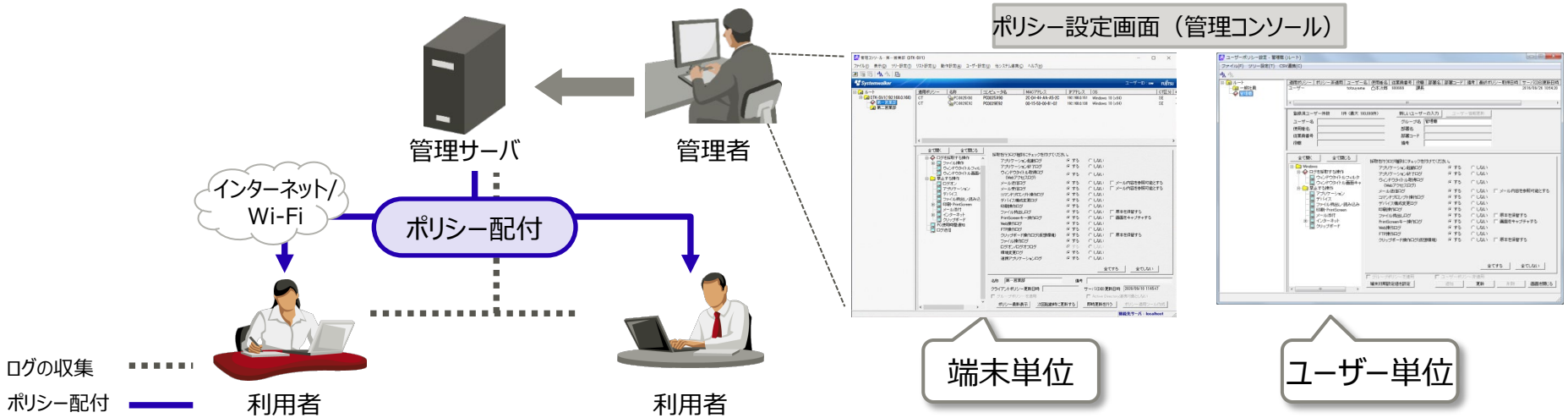
NEW V16.2.0からの新機能です。

記録と禁止

- ポリシー管理と配布
- ログ閲覧
- 本資料中でのログ表示例について

ポリシー管理と配布

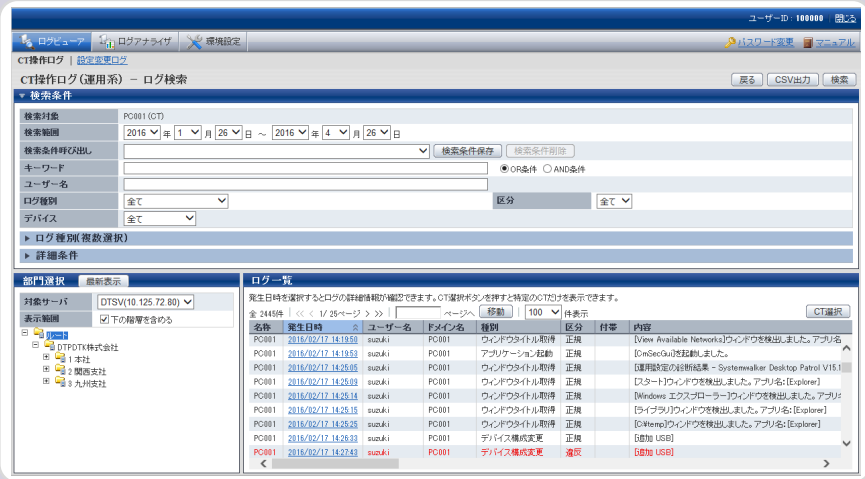
- 管理者は管理コンソールから禁止、記録する対象の操作を設定し、各端末に設定情報（ポリシー）を配付します。
- 設定可能なポリシーの単位
  - 端末/端末グループ単位
    支店や部門、開発部門や営業部門などグループごとに、一括で設定できます。
    端末ごとに設定も可能なため、部門が所有する共有端末など一部の端末のみ例外的に異なる設定で運用ができます。
  - ユーザー単位/ユーザーグループ単位
    ログオンユーザーごとにポリシーを設定することができます。設定している場合は、端末のポリシーより優先して適用されます。共有端末運用の場合、端末に対しては禁止操作を多く設定しておき、一部のログオンユーザーについてのみ操作を許可する運用ができます。必要に応じてユーザーグループ単位で設定できます。



ログ閲覧

- 管理者はサーバに収集された操作ログを、ログ閲覧画面（ログビューア）から閲覧し、利用者の操作を把握します。
- ログ閲覧時は、部門または端末を指定し、検索条件による絞り込みが可能です。

ログ閲覧画面（ログビューア）



検索条件	説明
検索範囲(必須入力)	検索範囲となる日付（範囲）を指定します。
検索条件呼び出し	過去に検索条件として保存した条件で検索します。
キーワード	キーワードによる絞込みをします。
ユーザー名	ユーザー名(Windowsログインユーザー名)による絞込みをします。
ログ種別	ログ種別による絞込みをします。（複数種別指定可）
デバイス	デバイス種別を指定して絞込みをします。（すべて、PC）
区分	区分を指定して絞込みをします。（すべて、正規、違反） ※禁止している操作が「違反」ログ、禁止していない操作が「正規」ログとして収集されています。
ドライブ種別	操作の対象となったファイルのドライブ種別による絞込みをします。（リムーバブル、リモート、CD/DVD、固定）
時間	時間帯の指定による絞込みをします。
曜日	曜日の指定により絞込みをします。

本資料中でのログ表示例について

FUJITSU

- 本資料で記載しているログ表示例は、ログ種別で個別に異なる「内容」部分を記載しています。すべてのログは共通項目として「名称」「発生日時」「ユーザー名」「ドメイン名」「種別」「区分」が出力されます。実際はログ閲覧画面（ログビューア）では下記のように表示されます。

  - 正規ログの場合

共通情報　固有情報

名称	発生日時	ユーザー名	ドメイン名	種別	区分	付帯	内容	備考	固有情報の説明
PC001	2016/04/07 08:47:04	suzuki	DOMAIN	アプリケーション起動	正規		[EXCEL]を起動しました。		起動したアプリケーション名

  - 各スライドには固有情報のみ、記載しています。

●●ログ表示例●●

	内容	固有情報の説明
PC起動時	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]	・ 起動モード：通常モード、セーフモード

  - 禁止ログの場合は、ログが赤で表示されます。

●●違反ログ表示例●●

内容	固有情報の説明
[dmn-user(Domain Users)]のログオンを[ログオフ]しました。結果：[成功]	・ 禁止したユーザー名(グループ) ・ 禁止処理([ログオフ]または[シャットダウン]) ・ 禁止結果([成功]または[失敗])

パソコンの操作記録と禁止

- パソコンの操作記録と禁止
- ログオン操作記録と禁止
- アプリケーション起動／終了記録と起動禁止
- PrintScreenキー操作記録と禁止
- メール送信／送信中止記録
- メール送信時の添付ファイル禁止
- メール受信記録
- 印刷操作記録と禁止
- ウィンドウタイトル記録と画面キャプチャ
- URLアクセス禁止
- Web操作記録
- Webアップロード／ダウンロード禁止
- FTPサーバ操作の記録と接続禁止
- クライアントサービス制御とプロセス制御
- ファイル操作の記録と禁止
- 特定ネットワークドライブへのアクセス許可
- ファイル持出し許可について
- 時間帯指定・暗号化強制による持出し許可
- 持出しユーティリティを利用した場合の記録
- デバイス/メディアを限定した持出し許可
- 持出しファイルの原本保管
- デバイス構成変更記録
- コマンドプロンプト操作記録
- 連携アプリケーションの記録
- 環境変更ログ

パソコンの操作記録と禁止

FUJITSU

- 記録と禁止の範囲
  - セーフモードで起動されたパソコンでも操作記録/禁止ができます。
  - ファストユーザースイッチ操作（※）で切り替えられたユーザーの操作も記録できます。
    （※）ログオフせずに他のユーザーでログインして操作できる機能（Windows XP以降、Windows Server 2008以降）
  - インターネット経由で接続されたパソコンでも操作記録/禁止ができます。
- インストール方法
  - パソコンに対する操作記録と禁止を実施するには、Systemwalker Desktop Keeperのクライアントソフトをインストールする必要があります。
  - インストールの方法
    - ウィザード形式でのインストール
      - ユーザーによって対話形式で入力された設定値をもとに行うインストールです。
    - サイレントでのインストール
      - 事前に管理者が定めた設定値に従い自動的に行うインストールです。これにより以下の自動化が可能です。
        - ✓ 利用者のダブルクリックによるインストール
        - ✓ Active Directoryのグループポリシーを使用した自動インストール
        - ✓ 資産管理ソフトウェアSystemwalker Desktop Patrolを利用した自動インストール
- 導入方法
  - マスタパソコンを使用した導入について
    - マスタパソコンを使用した導入を実施する場合は、管理サーバとネットワーク接続が行われていない状態でクライアントソフトをインストールし、マスタイメージを作成してください。

ログオン操作記録

FUJITSU

■ ログオン記録

■ ログオン/ログオフ、PCの起動/終了/休止/復帰/接続/切断のログを記録できます。

●●ログ表示例●●

	内容	固有情報の説明
PC起動時	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]	• 起動モード：通常モード、セーフモード
PC終了時	コンピュータを終了しました。起動時間:[6時間28分]、OS起動時間:[6時間28分]	• 起動時間：PC起動時、または前回の復帰時からシャットダウンまでの時間 • OS起動時間：PC起動時からシャットダウンまでの時間
PC休止時	コンピュータを休止しました。起動時間:[3時間12分]	• 起動時間：PC起動時、または前回の復帰時から休止までの時間
PC復帰時	コンピュータを復帰しました。	–
ログオン時	ログオンしました。認証先:[D-DOMAIN] 接続方法：[ローカル]、操作端末：[CLIENT1]、ログオン方法：[ドメインログオン]、ログオン権限：[ユーザー権限]、セッション番号：[0]	• 認証先：自コンピュータ名(local認証の場合)、ドメイン名(ドメイン認証の場合) • 接続方法：ローカル、リモート • 操作端末：自コンピュータ名(local認証の場合)、接続操作を行ったコンピュータ名(リモート接続の場合) • ログオン方法：ローカルログオン、ドメインログオン • ログオン権限：ユーザー権限、管理者権限 • セッション番号：セッション番号
ログオフ時	ログオフしました。	–
PC接続時	コンピュータ[AAA(物理PC)]からコンピュータ[BBB(物理PC)]に接続しました。	• 接続元コンピュータ名 • 接続先コンピュータ名
PC切断時	コンピュータ[AAA(物理PC)]からコンピュータ[BBB(物理PC)]への接続を終了 しました。	• 接続元コンピュータ名 • 接続先コンピュータ名

★★ポイント★★

パソコンの利用状況を把握することにより、社員の勤怠状況の把握に役立ちます。

ログオン操作の禁止

FUJITSU

■ ログオン禁止

- ■ ログオンを禁止するグループを設定し、該当グループに所属するユーザーでのログオンを禁止します。
- ■ 禁止されているログオン操作がされた場合、禁止ログを記録します。

禁止時の設定項目

・・・・・・・・ログオン禁止グループ・・・・・・・・

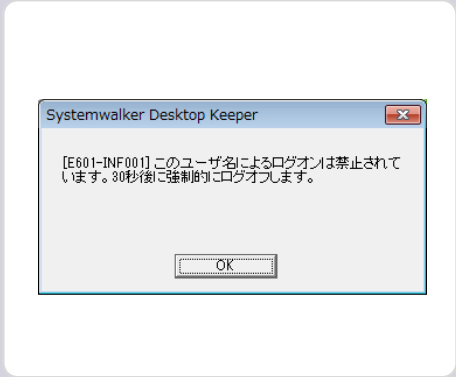
- Administrators
- Backup Operators
- Debugger Users
- Power Users
- Guests
- Replicator
- Users
- Domain Admin
- Domain Guests
- Domain Users
- Enterprise Admins
- Group Policy Owners
- Microsoft　アカウント

・・・・・・・・・・・・禁止後の操作・・・・・・・・・・・・・

- ログオフ
- シャットダウン

設定画面（管理コンソール）

利用者禁止画面



●●違反ログ表示例●●

内容	固有情報の説明
[dmn-user(Domain Users)]のログオンを[ログオフ]しました。結果：[成功]	・禁止したユーザー名(グループ) ・禁止処理([ログオフ]または[シャットダウン]) ・禁止結果([成功]または[失敗])

★★ポイント★★

利用者に管理者権限を与えない運用の場合に、本機能でAdministratorsへのログオン禁止をしておくと管理者権限のログオンパスワードが万が一漏れてもログオンできません。

アプリケーション起動／終了記録

FUJITSU

- アプリケーション起動／終了記録（※）
  - アプリケーションを起動／終了したときのログです。

●●ログ表示例●●

	内容	固有情報の説明
起動時	[EXCEL]を起動しました。	起動したアプリケーション名
終了時	[EXCEL]を終了しました。	終了したアプリケーション名

（※）ウィンドウを持たないアプリケーションの場合は、アプリケーション起動/終了ログを収集できません。
画面を表示しない（不可視ウィンドウを保有している）アプリケーションの起動ログは収集されます。

アプリケーション起動の禁止

FUJITSU

■ アプリケーション起動禁止

- ■ 起動を禁止するアプリケーション（EXE名）を設定し、該当アプリケーションの起動を禁止します。
- ■ 禁止されているアプリケーションが起動された場合、禁止ログを記録します。

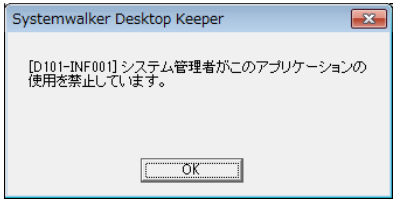
禁止時の設定項目

・・・・・・・起動禁止アプリケーション名一覧・・・・・・・

- 起動禁止アプリケーションEXE名
- 備考

設定画面（管理コンソール）

利用者禁止画面



●●違反ログ表示例●●

内容	固有情報の説明
[sol]の起動を[強制終了]しました。結果：[成功]	・禁止したアプリケーション名 ・禁止処理([強制終了]) ・禁止結果([成功]または[失敗])

★★ポイント★★

業務利用外のソフト、ゲーム、情報漏えいリスクのあるファイル共有ソフトなどを起動禁止にして組織ポリシーの徹底・情報漏えいの防止ができます。

PrintScreenキー(※)操作記録と禁止

FUJITSU

■ PrintScreenキー操作の記録

- ■ PrintScreenキーの利用を禁止した時のログです。
- ■ 設定に応じ、[付帯]情報としてPrintScreenキー操作時の画面キャプチャ（png形式）を記録します。

●●ログ表示例●●

	内容	固有情報の説明
PrintScreenキー押下時	PrintScreenキーが押下されました。	–

■ PrintScreenキーの禁止

- ■ キーボードのPrintScreenキーを使用しての画面のハードコピーを禁止できます。
- ■ 設定に応じ、禁止時にログの[付帯]情報として画面キャプチャ（png形式）を記録します。

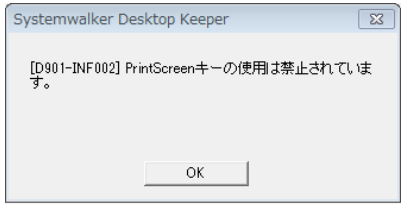
禁止時の設定項目

・・・・・・・Printscreenキー無効化・・・・・・・

- する
  - 画面をキャプチャする
- しない

設定画面（管理コンソール）

利用者禁止画面



●●違反ログ表示例●●

内容	固有情報の説明
PrintScreenキーが押下されました。	–

（※）PrintScreenキー以外で画面キャプチャを行うケースに備え記録／禁止対象とするキーの追加設定に対応しています。

メール送信／送信中止記録

FUJITSU

■ メール送信 (※1) (※2) (※3)

- ■ メールを送信した時のログです。
- ■ 設定に応じて[付帯]情報としてメールの原本(※4) を保管します。

●●ログ表示例●●

	内容	固有情報の説明
メール送信時	メール送信されました。[件名：本日の業務報告について From：Mail Address-A To：Mail Address-B CC：Mail Address-C Mail BCC：Address-D 添付：添付ファイル名]	・ メールのタイトル ・ 送信元アドレス ・ 送信先アドレス(To、Cc、Bccの情報) ・ 添付ファイル名

■ メール送信中止 (※1)

- ■ メール送信時に、宛先を確認するメッセージが表示され、送信をキャンセルした時に記録されるログです。

●●ログ表示例●●

	内容	固有情報の説明
メール送信中止時	メール送信が中止されました。警告アドレス[Address-A]	・ 許可されていないドメインのメールアドレス

（※1）SMTPプロトコルを使用するメールソフト、Microsoft®Outlook® 2013以降のバージョンのOutlookが対象です。
（※2）Webメールのメール送信ログは、Gmail、Outlook.com、Outlook for Microsoft 365 (旧Office 365)が対象となります。それ以外のWebメールはメール送信ログが採取されません。
本機能は、Microsoft Edge™ 85～92、Firefox 49～8091、およびGoogle Chrome 53～8092で動作します。
（※3）Webメールでメールを送信する場合、メールにファイルが添付された場合はWebアップロードログが採取され、続いてメール送信ログが採取されます。
（※4）利用者が利用しているメールソフトがMicrosoft®Outlook®の場合はmsg形式で、その他のメールソフトを利用している場合はeml形式で原本を保管します。

メール送信時の添付ファイル禁止

FUJITSU

■ メール送信時の添付ファイル禁止（※）

- ■ 禁止対象となるファイルをメールに添付して、送信することを禁止できます。
- ■ 禁止対象のファイルをメールに添付して、送信しようとした際に禁止ログとして記録します。

禁止時の設定項目

・・・・・・・メール送信時宛先確認・・・・・・・・

- 確認しない
- 確認する

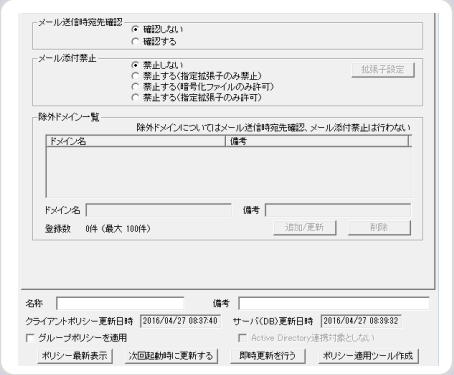
・・・・・・・・・・・メール添付禁止・・・・・・・・・・・・

- 禁止する（指定拡張子のみ禁止）
- 禁止する（暗号化ファイルのみ許可）
- 禁止する（指定拡張子のみ許可）
- 禁止しない

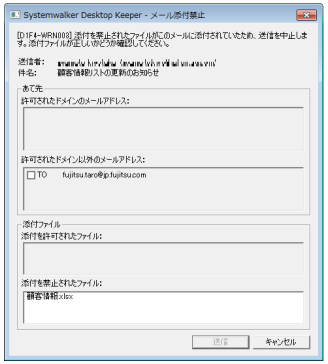
・・・・・・・・・・・除外ドメイン名・・・・・・・・・・・・

- ドメイン名

設定画面（管理コンソール）



利用者禁止画面



●●違反ログ表示例●●

内容	固有情報の説明
[顧客情報一覧.xlsx]のメール添付を禁止しました。アプリ名：[xxx]	・ 禁止されたファイル名 ・ メールソフトのアプリケーション名

★★ポイント★★

除外ドメインを入力する事で例えば社内へのメール送信時は任意の添付ファイル許可できます。
社外ドメインへのメール送信時は暗号化ファイルのみ許可するといった運用が可能です。

※SMTPプロトコルを使用するメールソフト、Microsoft®Outlook® 2013以降のバージョンのOutlookが対象です。

メール受信記録

FUJITSU

- メール受信 (※1) (※2) (※3)
  - メールを受信した時のログです。
  - 設定に応じて[付帯]情報としてメールの原本(※4) を保管します。

●●ログ表示例●●

	内容	固有情報の説明
メール受信時	[送信日時：Fri May 26 2018 11:22:33 GMT+0900 件名：本日の業務報告について From：sender@example.com To：recipient@example.com CC：cc@example.com 添付：添付ファイル名]	・送信日時 ・メールのタイトル ・送信元アドレス ・送信先アドレス(To、Ccの情報) ・添付ファイル名

（※1）Microsoft Outlookがインストールされている環境でのみメール受信ログを採取します。
（※2）Microsoft Outlookに、Systemwalker Desktop Keeperのアドインを追加しています。このアドインを無効化したり、削除したりすると、Outlookが強制終了するため行わないでください。
なお、そのPCに複数のユーザーがログオンしている場合、アドインを無効化・削除したユーザーだけでなく、全員のOutlookが強制終了することがあります。
（※3）POP3/IMAP以外を利用している場合でも受信したメールのログが取得されます。ただし、Microsoft Outlook未起動時にサーバが受信したメールのログは採取されません。
また、Microsoft Outlook起動直後に受信したメールはログが取得されません。
（※4）Microsoft Outlookでメールを受信し、原本保管した場合、ログビューアよりメール原本を取り出すとファイルの拡張子はtxtになります。ファイルはUTF-8で保存されます。

印刷操作記録と禁止

FUJITSU

■ 印刷操作記録

- ■ 印刷をした時のログです。

●●ログ表示例●●

	内容	固有情報の説明
印刷時	[imgfilelist.xls]が印刷されました。プリンタ名：[KONICA MINOLTA 750/600 PCL]、ページ数：[1]、印刷日付：[2016/04/11 19:44:59]	• 印刷ファイル名 • 印刷を行ったプリンタ名 • 印刷ファイルの総ページ数 • 印刷を行った日付

■ 印刷操作禁止

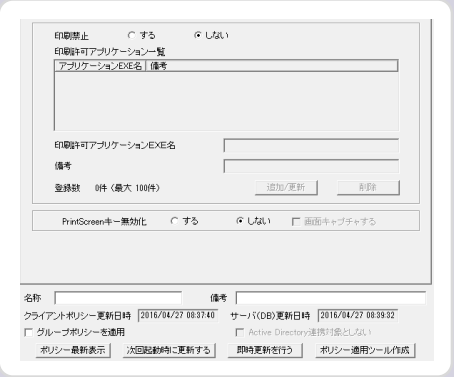
- ■ 許可したアプリケーション以外の印刷を禁止できます。
- ■ 印刷を許可されていないアプリケーションで印刷しようとした際、禁止ログとして記録します。

禁止時の設定項目

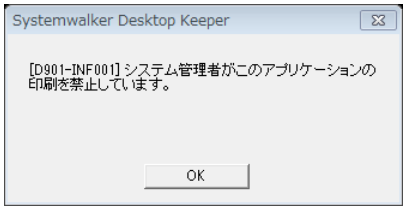
・・・印刷禁止・・・
- する
- しない

・・・印刷許可アプリケーション・・・
- 印刷許可アプリケーションEXE名
- 備考

設定画面（管理コンソール）



利用者禁止画面



●●違反ログ表示例●●

内容	固有情報の説明
[顧客情報.doc]の印刷を禁止しました。 アプリ名：[C:¥Program Files¥Microsoft Office¥OFFICE11¥WINWORD.EXE]	• 禁止した印刷ファイル名 • 禁止したアプリケーション名

ウィンドウタイトル記録

FUJITSU

■ ウィンドウタイトル記録

- ■ ウィンドウを持つアプリケーションを起動した場合のウィンドウタイトルを記録します。
- ■ ブラウザを使用している場合、ウィンドウタイトルとともに、「アクセスしたURL情報」を記録します。（※）

●●ログ表示例●●

	内容	備考	固有情報の説明
通常アプリケーションの場合	[Microsoft Excel]ウィンドウを検出しました。アプリ名：[EXCEL]		【内容の固有情報】 ・ アプリケーションのウィンドウタイトル名 ・ 起動したアプリケーション名 【備考の固有情報】 ・ ブラウザで表示したページのURL
Internet Explorerの場合	[勤怠管理システム - TOP - - Internet Explorer]ウィンドウを検出しました。アプリ名：[iexplore]	http://mysystem.aaa.fujitsu.com/	
Google Chromeの場合	[勤怠管理システム - TOP -]ウィンドウを検出しました。アプリ名：[chrome]	http://mysystem.aaa.fujitsu.com/	
Firefoxの場合	[勤怠管理システム - TOP -]ウィンドウを検出しました。アプリ名：[firefox]	http://mysystem.aaa.fujitsu.com/	

（※）URL情報の取得はMicrosoft Internet Explorer 11、Microsoft Edge™、Firefox 49以降およびGoogle Chrome 53以降をサポート。

ウィンドウタイトル記録（画面キャプチャ）

FUJITSU

■ ウィンドウタイトル画面キャプチャ

■ 指定したアプリケーション、指定したキーワードでウィンドウタイトルが記録された場合に、画面キャプチャ（png形式）を記録します。

設定項目

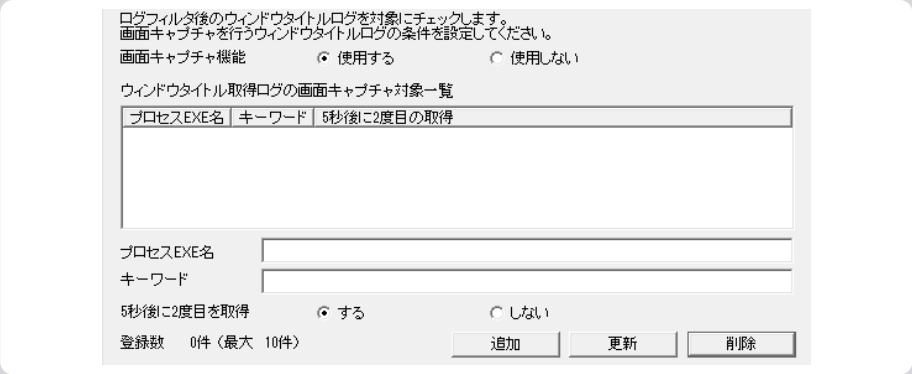
・・・・・・・・・・画面キャプチャ機能・・・・・・・・・・

- 使用する
- 使用しない

・・・ウィンドウタイトル取得ログの画面キャプチャ対象・・・

- プロセスEXE名
- キーワード
- ５秒後に２度目の取得
  - する
  - しない

設定画面（管理コンソール）



★★ポイント★★

あらかじめ、機密情報が含まれるファイルのファイル名をキーワードに登録しておくことで、機密情報が開かれた瞬間の画面キャプチャを記録し、証拠として記録する事ができます。

URLアクセス禁止

FUJITSU

■ URLアクセス禁止（※1）

- ■ 管理者が許可していないURLへのアクセスを禁止できます。（※2）
- ■ 許可していないURLへのアクセスが禁止された場合、禁止ログとして記録します。

禁止時の設定項目

・・・・・・・・・・URLアクセス禁止・・・・・・・・・・

- 禁止する
- 禁止しない

・・・・・・・URLアクセス禁止の設定・・・・・・・

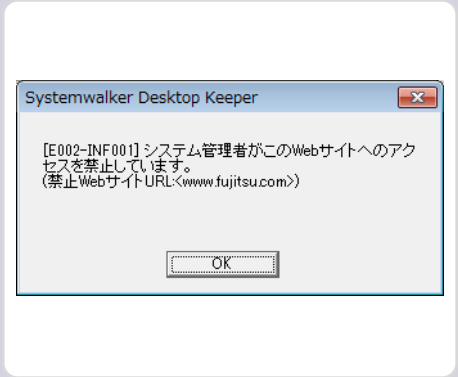
- 登録したサイトへのアクセスを禁止する
- 登録したサイト以外へのアクセスを禁止する

・・・・・・・アクセス禁止URL文字列・・・・・・・

- URL文字列
- 備考

設定画面（管理コンソール）

利用者禁止画面



●●違反ログ表示例●●

内容	固有情報の説明
[www.aaa.com]への接続を禁止しました。アプリ名：[iexplore]	・ Webページを表示したアプリケーション名

（※1）Microsoft Internet Explorer 11、Microsoft Edge™ 85～92、Firefox 49～8091、およびGoogle Chrome 53～8092をサポート。
（※2）URL文字列入力された文字列を含むドメイン名のサイトに対して、アクセスが禁止・許可されます。

Web操作記録

FUJITSU

- Web操作記録（※1）（※2）
  - クライアントからWebサイトにアップロード／ダウンロードした時のログを記録します。
  - ファイル送信または受信を開始後、異常が発生したり、ユーザーによってファイル送信または受信がキャンセルされた場合においても、ログを記録します。

●●ログ表示例●●

	内容	固有情報の説明
アップロード時	[www.aaa.com]へのアップロード操作が行われました。 アプリ名：[iexplore]、ファイル名：[c:¥test¥test.txt]	• Webページを表示したアプリケーション名 • アクセス先のURL文字列 • ファイル名
ダウンロード時	[www.aaa.com]からダウンロード操作が行われました。 アプリ名：[msedge]、ファイル名：[c:¥test¥test.txt]	

（※1）Microsoft Internet Explorer 11、Microsoft Edge™ 85～92、Firefox 49～8091、およびGoogle Chrome 53～8092をサポート。
（※2）Active Xやプラグインによって動作するサイト上では、アップロード/ダウンロード操作の記録ができません。

Webアップロード／ダウンロード禁止（※1）（※2）（※3）

FUJITSU

- Webアップロード禁止
  - 管理者が許可したWebサイト以外へのアップロードを禁止できます。
  - 許可されたサイト以外へのアップロードは禁止され、禁止ログとして記録します。
- Webダウンロード禁止
  - 管理者が許可したWebサイト以外からのダウンロードを禁止できます。
  - 許可されたサイト以外からのダウンロードは禁止され、禁止ログとして記録します。

禁止時の設定項目

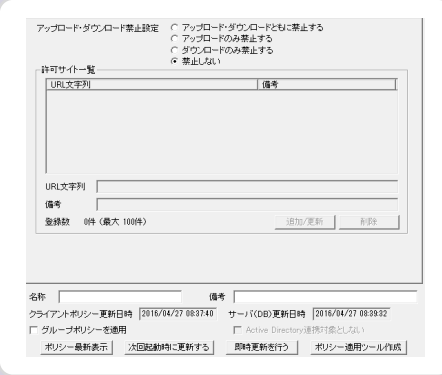
・・・・・アップロード・ダウンロード禁止設定・・・・・

- アップロード・ダウンロードともに禁止する
- アップロードのみ禁止する
- ダウンロードのみ禁止する
- 禁止しない

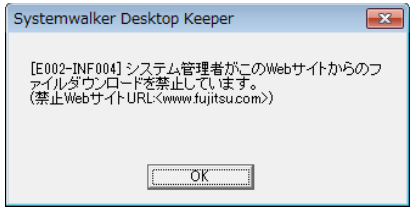
・・・アップロード・ダウンロード許可サイトURL・・・

- URL文字列
- 備考

設定画面（管理コンソール）



利用者禁止画面



●●違反ログ表示例●●

内容	固有情報の説明
• [www.aaa.com]へのアップロードを禁止しました。アプリ名：[iexplore] • [www.aaa.com]からのダウンロードを禁止しました。アプリ名：[iexplore]	• Webページを表示したアプリケーション名 • アクセス先のURL文字列

（※1）Microsoft Internet Explorer 11、Microsoft Edge™ 85～92、Firefox 49～8091、およびGoogle Chrome 53～8092をサポート。
（※2）URL文字列に入力した文字列を含むURLのサイトに対して操作が禁止・許可されます。
（※3）Active Xやプラグインによって動作するサイト上では、アップロード/ダウンロード操作の禁止ができません。

FTPサーバ操作の記録

FUJITSU

- FTPサーバ操作記録
  - クライアントからFTPサーバへのアップロード／ダウンロードした時のログを記録します。
  - ファイル転送開始後、異常が発生したり、ユーザーによってファイル転送がキャンセルされた場合においても、ログとして記録します。

●●ログ表示例●●

	内容	固有情報の説明
アップロード操作時	[192.168.1.100]へのアップロード操作が行われました。アプリ名：[FTP.EXE]、ファイル名:[Test.txt]	• FTPクライアントプログラム名 • FTPサーバのIPアドレス • ファイル名
ダウンロード操作時	[192.168.1.100]からダウンロード操作が行われました。アプリ名：[FTP.EXE]、ファイル名:[Test.txt]	

FTPサーバ接続禁止

FUJITSU

- FTPサーバ接続禁止
  - 管理者が許可したFTPサーバ以外へのアクセスを禁止できます。
  - 許可されたFTPサーバ以外への接続は禁止され、禁止ログとして記録します。

禁止時の設定項目

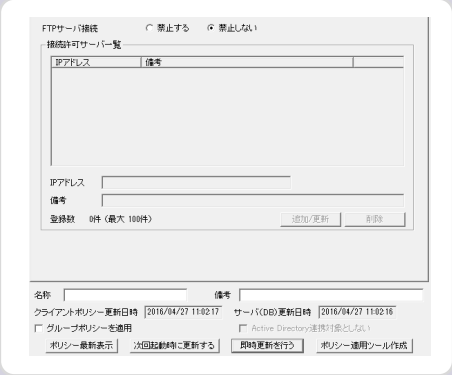
・・・・・・・・・・・・FTPサーバ接続・・・・・・・・・・・・

- 禁止する
- 禁止しない

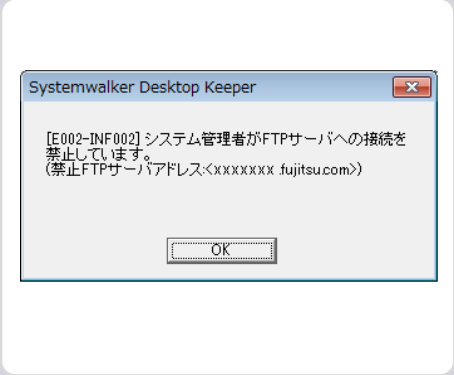
・・・・・接続許可サーバIPアドレス設定・・・・・

- IPアドレス
- 備考

設定画面（管理コンソール）



利用者禁止画面



●●違反ログ表示例●●

内容	固有情報の説明
[xxxxxx.fujitsu.com]への接続を禁止しました。アプリ名：[FTP.EXE]	• FTPクライアントプログラム名 • FTPサーバのIPアドレス

クライアントサービス制御とプロセス制御

FUJITSU

■ クライアントサービス制御

- ■ 指定したクライアントに登録されているサービスの一覧が参照できます。
- ■ 登録されているサービスの状態およびスタートアップの種類を変更できます。

設定変更項目

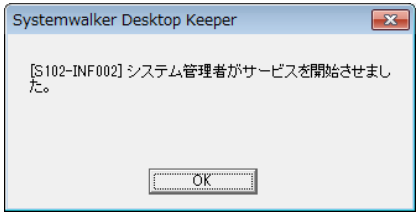
- 開始
- 停止
- 自動
- 手動
- 無効

★★ポイント★★

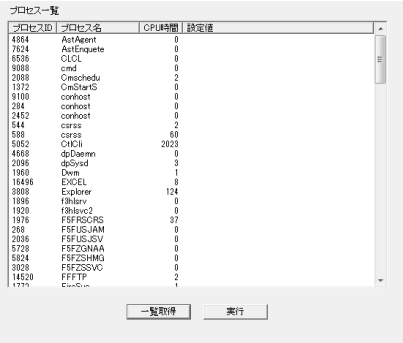
重要機密情報を扱う端末に対してリモートアクセスサービスを
無効にすることで、ネットワークを介した情報漏えいを防止できます。

設定画面（管理コンソール）

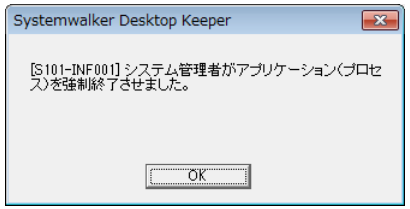
利用者画面



設定画面（管理コンソール）



利用者画面



ファイル操作の記録（標準）

FUJITSU

■ ファイル操作の記録

■ エクスプローラ、コマンドプロンプト、コピーコマンドでのファイル/フォルダの操作（作成、更新、削除、複写、移動、変名）を記録します。

●●ログ表示例●●

	内容	固有情報の説明
作成時	操作：[作成]、ファイル名：[C:¥Users¥Owner¥Desktop¥a.txt]、ドライブ種別：[固定]、アプリ名：[Explorer.exe]	作成ファイル名（フルパス※1）、ドライブ種別、作成したアプリケーション名
更新時	操作：[更新]、ファイル名：[¥¥aaa.fujitsu.com¥売り上げ.xlsx]、ドライブ種別：[リモート]、アプリ名：[Explorer.exe]	更新ファイル名（フルパス※1）、ドライブ種別、更新したアプリーション名
削除時	操作：[削除]、ファイル名：[G:¥名簿.xlsx]、ドライブ種別：[リムーバブル]、アプリ名：[Explorer.exe]	削除ファイル名（フルパス※1）、ドライブ種別、削除したアプリケーション名
複写時	操作：[複写]、ファイル名元：[C:¥Users¥Owner¥Documents¥価格.xlsx]、ドライブ種別元：[固定]、ファイル名先：[G:¥価格.xlsx]、ドライブ種別先：[リムーバブル]、アプリ名：[Explorer.exe]	複写元ファイル名（フルパス※1）、複写元のドライブ種別、複写先ファイル名（フルパス※1）、複写先のドライブ種別、複写したアプリケーション名
移動時	操作：[移動]、ファイル名元：[C:¥構成.ppt]、ドライブ種別元：[固定]、ファイル名先：[C:¥Users¥Owner¥Desktop¥構成.ppt]、ドライブ種別先：[固定]、アプリ名：[Explorer.exe]	移動元ファイル名（フルパス※1）、移動元ドライブ種別、移動先ファイル名（フルパス※1）、移動先ドライブ種別、移動したアプリケーション名
変名時	操作：[変名]、ファイル名元：[C:¥Users¥スペック情報1.xlsx]、ドライブ種別元：[固定]、ファイル名先：[C:¥Users¥サーバスペック 情報2.xlsx]、ドライブ種別先：[固定]、アプリ名：[Explorer.exe]	元のファイル名（フルパス※1）、元のドライブ種別、変名後のファイル名（フルパス※1）、変名後のドライブ種別、変名したアプリケーション名

（※1）ネットワークドライブの場合、UNC表記または、UNC表記のマシン名の部分がIPアドレスで表示されます

ファイル操作の記録（記録対象のカスタマイズ）

FUJITSU

■ ファイル操作の記録対象のカスタマイズ

- ファイル操作の記録対象とするソフトウェアを追加できます（プロセス名を指定）。
- 追加したプロセスについて、ファイル参照操作を記録対象とするのか設定できます。
- 拡張子、ドライブ種別、記録対象外フォルダを指定して、条件に該当するファイル操作のみ記録対象とすることができます。
- ファイル操作の記録（標準）で取得される情報に加え、以下2項目のログを取得できます。

●●ログ表示例●●

	内容	固有情報の説明
参照時	操作：[参照]、ファイル名：[¥¥aaa.fujitsu.com¥機密情報¥顧客名簿.doc]、ドライブ種別：[リモート]、アプリ名：[winword.exe]	参照ファイル名（フルパス※）、ドライブ種別、操作したアプリーション名
別名保存時	操作：[別名保存]、ファイル名元：[C:¥Users¥Owner¥Desktop¥顧客情報.xlsx]、ドライブ種別元：[固定]、ファイル名先：[C:¥Users¥Owner¥Desktop¥お知らせ.xlsx]、ドライブ種別先：[固定]、アプリ名：[excel.exe]	元ファイル名（フルパス※）、保存元ドライブ種別、保存先ファイル名（フルパス※）、保存先ドライブ種別、別名保存したアプリケーション名

（※）ネットワークドライブの場合、UNC表記または、UNC表記のマシン名の部分がIPアドレスで表示されます

★★設定前の知識★★

ファイル操作の記録対象追加時のプロセス名の例は以下の通りです

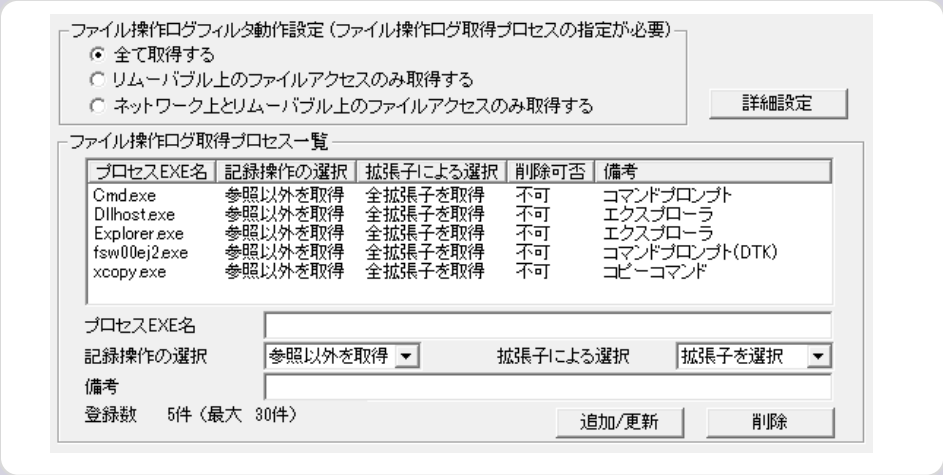
Microsoft Word ・・・ WINWORD.EXE
Microsoft Excel ・・・ EXCEL.EXE
Microsoft PowerPoint ・・・ POWERPNT.EXE
メモ帳 ・・・ notepad.exe
ワードパッド ・・・ wordpad.exe

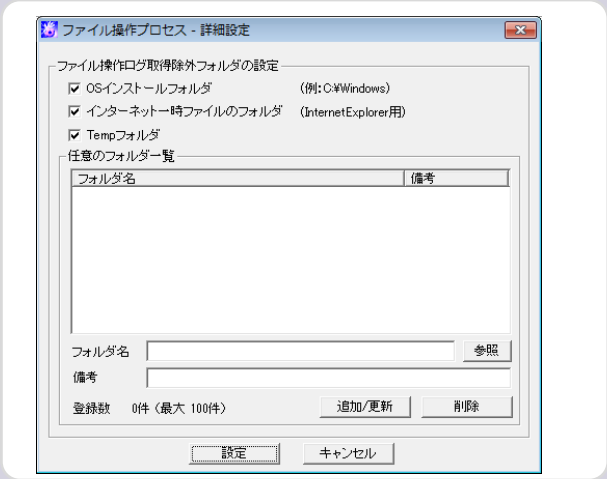
（補足）ファイル操作の記録-画面例-

FUJITSU

ファイル操作記録（記録対象のカスタマイズ）

設定画面（管理コンソール）





ファイル操作の禁止

FUJITSU

■ ファイル操作の禁止

- ■ リムーバブル、 DVD/CDドライブ、ネットワークドライブのファイル読み込みを禁止します。
- ■ 内蔵ドライブ、リムーバブル、 DVD/CDドライブ、ネットワークドライブへの持ち出し（ファイルの作成、移動、複写）を禁止します。
- ■ ポータブルデバイス/イメージングデバイスの接続を禁止（デバイスを無効化）します。

禁止時の設定項目

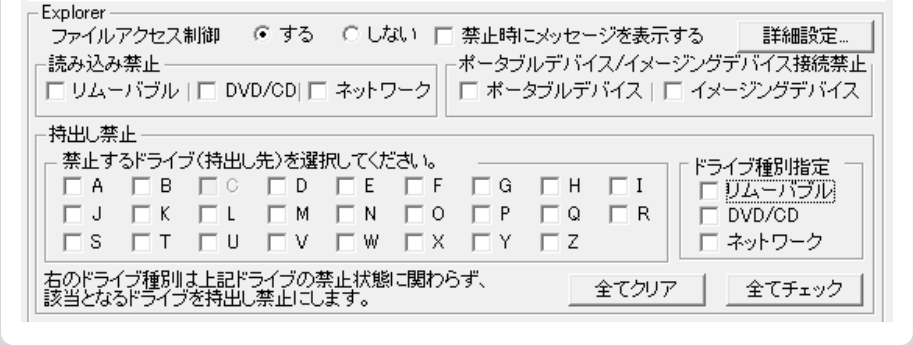
・・・・ファイルアクセス制御・・・・
- する
- しない

・・・・・・読み込み禁止・・・・・・
- リムーバブル
- DVD/CD
- ネットワーク

・・・・・・・持ち出し禁止・・・・・・・・
- ドライブ（A~Z）
- リムーバブル
- DVD/CD
- ネットワーク

・・・ポータブルデバイス/イメージングデバイス接続禁止・・・
- ポータブルデバイス
- イメージングデバイス

設定画面（管理コンソール）



★★設定前の知識★★

- リムーバブルへのファイル操作を禁止すると、USBハードディスク、USBメモリ、SDカード、CFカード、フロッピーディスクなどWindowsでリムーバブルディスクと認識されるデバイスへの操作が禁止されます（※）
- ポータブルデバイス/イメージングデバイス接続を禁止すると、スマートフォン、タブレット、デジタルカメラなどWindowsでポータブルデバイス/イメージングデバイスと認識されるデバイスの接続が禁止されます（※）
- ドライブへの操作禁止はOSがインストールされているドライブは指定できません

※記載のデバイス例は一例であり、デバイスによってはWindowsでの認識のされ方が　異なる場合があります。

特定ネットワークドライブへのアクセス許可

FUJITSU

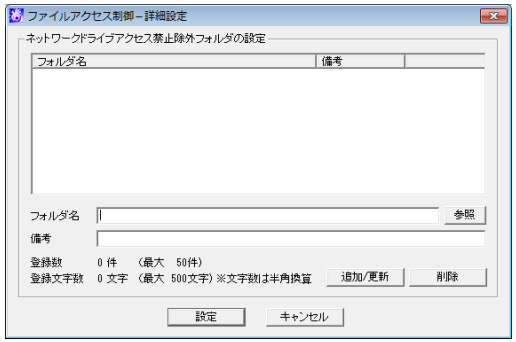
- 特定ネットワークドライブのアクセス許可
  - 管理者が許可したネットワークドライブに対してのみ利用者はアクセスできます。

設定項目

・・ネットワークドライブアクセス禁止除外フォルダの設定・・

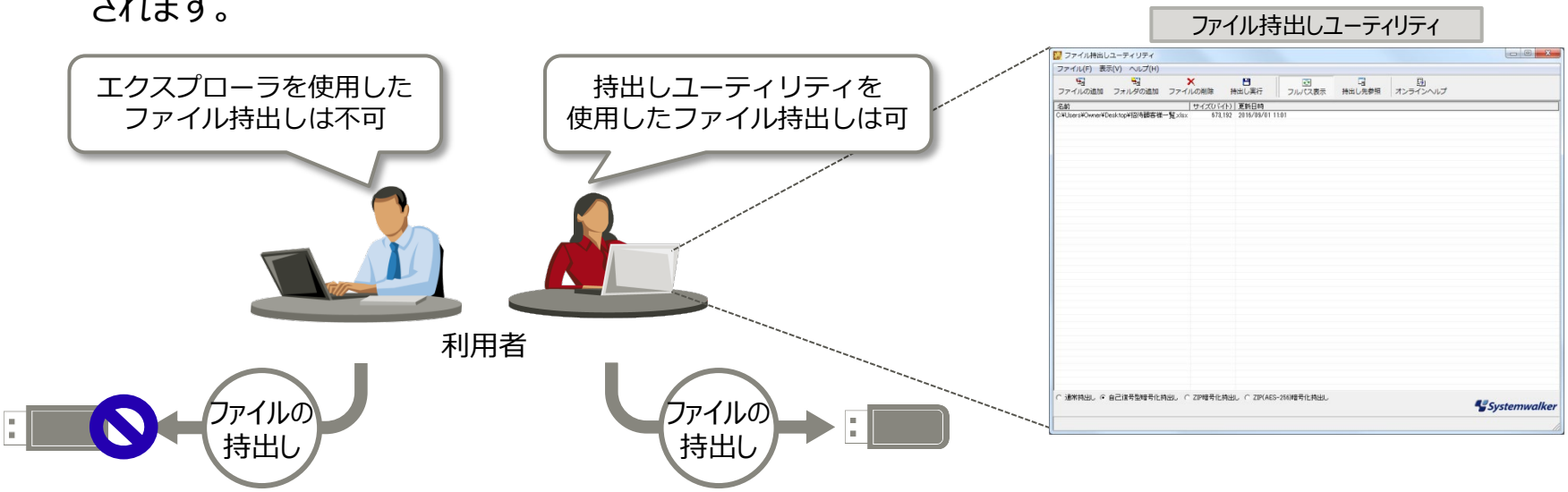
- フォルダ名
- 備考

設定画面（管理コンソール）



ファイル持出し許可について

- Systemwalker Desktop Keeperではファイル操作の禁止により、持出しを一律禁止し、業務を考慮して必要に応じて持出しを許可します。
- ファイルの持出しを許可するパターン
  - 時間帯（曜日や時間）を指定し持出しを許可
  - ファイルの暗号化を強制することで持出しを許可
  - 業務上利用可能なUSBデバイスに限定して持出しを許可
- ツールを用いた持出しについて
  - 利用者がファイル持出しする際には持出し用ツール（持出しユーティリティ）を使用します。利用者は管理者が許可した条件で本ツールを使用しファイルを持出しできます。
  - 本ツールを利用した持出しは通常の「ファイル操作」ログとは区別され、「ファイル持出し」ログとして記録されます。



時間帯指定・暗号化強制による持出し許可

FUJITSU

■ 時間帯指定・暗号化強制による持出し許可

- ■ 期間や時間帯を指定した持出し許可、持出し時に暗号化を強制した持出し許可ができます。
- ■ 暗号化してファイルを持ち出す場合、暗号化方式や復号するためのパスワード長、パスワード試行回数、復号可能日数、暗号化後のファイルの拡張子を指定できます。（※1）（※2）
- ■ 持出し時に利用者に持出し理由の入力を強制できます。
- ■ 利用者は持出しユーティリティを使用して暗号化を実施し、持出しをします。

設定項目例

・・・持出しユーティリティ機能の設定・・・

- フォーマット機能を起動させない
- リムーバブルとDVD/CDのみ持ち出し先として表示
- 持出し理由を入力する

・・・持出しユーティリティ起動可能日時設定・・・

- 使用する期間を限定する
- 使用する時間を限定する

・・・暗号化方式-ファイル持出しユーティリティ・・・

- 自己復号型暗号化
- ZIP暗号化
- ZIP(AES-256)暗号化

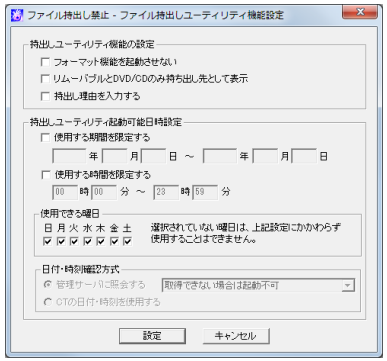
・・・パスワード長・・・

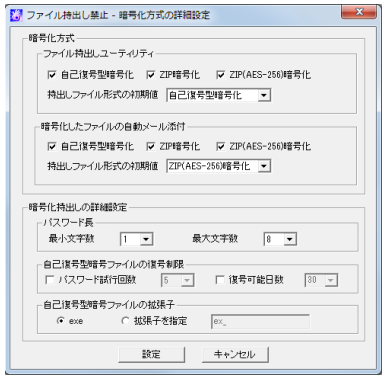
- 最小文字数
- 最大文字数

・・・自己復号型ファイルの復号制限・・・

- パスワード試行回数
- 復号可能日数

設定画面（管理コンソール）





（※1）暗号化持ち出し時には、自己復号型暗号化ファイル、ZIP暗号化ファイル、またはZIP(AES-256)暗号化ファイルが作成されます。Systemwalker Desktop Keeperが導入されていないパソコンでも解凍可能です。
（※2）パスワード試行回数、復号可能日数を超えた際、ファイルは削除されます。

持出しユーティリティを利用した場合の記録

FUJITSU

- ファイルの持出し記録
  - 持出しユーティリティを利用してファイルを持出した場合にログを記録します。
  - ファイル持出しログという種別でログが記録します。

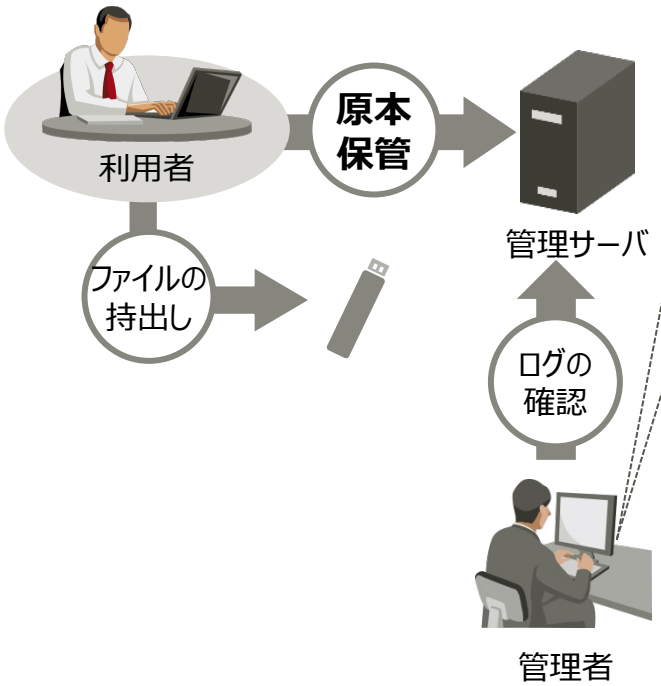
●●ログ表示例●●

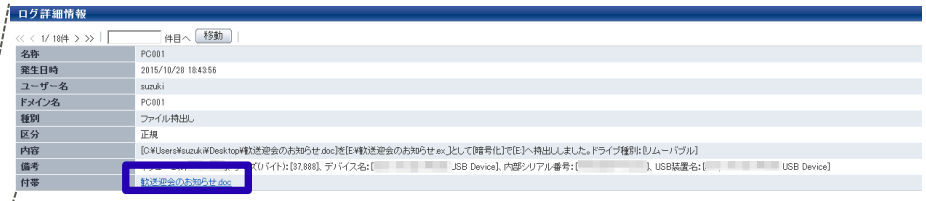
	内容	固有情報の説明
暗号化持出し時	[C:¥Users¥Administrator¥Desktop¥顧客情報一覧.xlsx]を[G:¥顧客情報一覧.exe]として[暗号化]で[G:]へ持出ししました。ドライブ種別：[リムーバブル]	• 持出し元のファイル名 • 持出し先のファイル名 • 持出し方法(平文または暗号化) • 持出し先のドライブレター • 持出し先のドライブの種別 • 持出し理由
平文持出し時	[D:¥製品顧客2015年10月度.xlsx]を[E:¥製品顧客2015年10月度.xlsx]として[平文]で[E:]へ持出ししました。ドライブ種別：[CD/DVD]	
暗号ファイルの持出し先をUNC(先頭が“¥¥”で始まるアドレス)指定した場合：	[D:¥Users¥Administrator¥Desktop¥新規文書.txt]を[¥¥Server1¥UserDocument¥新規文書.ex_]として[暗号化]で[リモート]へ持出ししました。ドライブ種別：[リモート]	
持出し理由を入力するポリシー設定の場合：	持出し理由を入力するポリシー設定の場合：[C:¥Users¥Administrator¥Desktop¥A社様重要顧客情報.xlsx]を[E:¥顧客情報.ex_]として[暗号化]で[E:]へ持出ししました。ドライブ種別：[リムーバブル]、持出し理由：[××業務で○○委託先に□□情報を持出すため]	

持出しファイルの原本保管

FUJITSU

- 持出しファイルの原本保管
  - ファイル持出しユーティリティでのファイル持出し時に、持出したファイルの原本を強制的にサーバに保管します。
  - ファイルの原本はファイル持出しログの[付帯]情報として記録します。
  - ファイルの原本のサイズが大きい場合は、分割して保存できます。





★★ポイント★★

重要機密情報を扱う端末など、持出し管理を強化する場合に活用し、利用者が持出したファイルの中身を管理者が確認できます。

デバイス/メディアを限定した持出し許可

FUJITSU

■ デバイス/メディアを限定した持出し許可

- 管理サーバに事前登録したデバイス/メディア（※）のうち、管理者が指定したデバイス/メディアへだけ、持ち出しを許可することができます。
- 管理者は持出しユーティリティからのみ持出しを許可するか、Explorer操作（ドラッグ＆ドロップ）でも持出しを許可するかデバイス/メディア単位に設定できます。

設定項目例

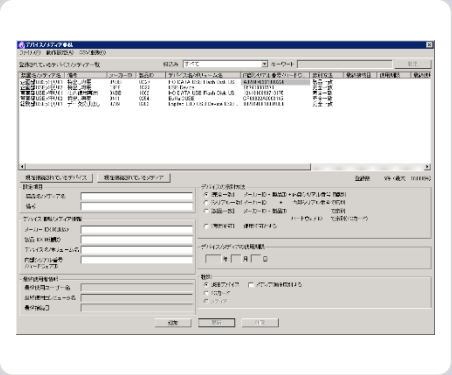
・・・デバイス/メディアの識別方法・・・

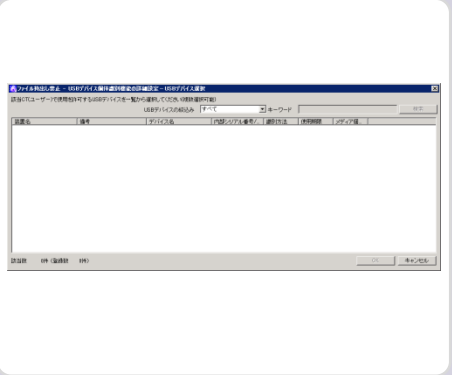
- [完全一致]　メーカーID＋製品ID＋内部シリアル番号で識別
- [シリアル一致]メーカーID＋内部シリアル番号で識別
- [製品一致]　メーカーID＋製品IDで識別
  ハードウェアIDで識別(PCカード)
- [使用不可]　使用不可とする

・・・アクセス設定・・・

- 読み込み専用
- 読み書き可能
  読み書きともファイル持出しユーティリティに限定
  書き込みはファイル持出しユーティリティに限定

設定画面（管理コンソール）





★★ポイント★★

登録されているデバイス/メディアのみ持出しを許可できます。
更に、登録されているデバイス/メディアと同一機種のデバイス/メディアは持出しを許可する、といった柔軟な設定ができます。

（※）デバイス/メディアの登録は、管理コンソールでデバイス/メディアを認識して１つずつ登録する方法と、CSVによる一括登録が可能です。

デバイス構成変更記録

FUJITSU

■ デバイス構成変更の記録

■ クライアントでの内蔵ディスクの追加やネットワークドライブの作成、デバイス(USBデバイス、Wi-Fi接続、Bluetooth接続、PCカード)の接続により、デバイスの構成が変更された場合のログを記録します。

●●ログ表示例●●

	内容	備考	固有情報の説明
追加時	[追加 D:固定]	ボリューム[Windows2008]	• [追加]または[変更] • ドライブレター、USB、Wi-Fi接続、Bluetooth接続、またはPCカード • ドライブの種別、または、ポータブルデバイス/イメージングデバイスの種別)
	[追加 G:リムーバブル]	デバイス名[Fujitsu USB Flash Disk USB Device]、内部シリアル番号[BXXXXX]、メーカーID：[1111]、製品ID：[2222]	
	[追加 G:リモート]	ボリューム[SV1]、サーバ名・共有名[¥¥Server1¥機密情報]	
	[追加 USB(ポータブルデバイス)]	デバイス名：[Android Composite ADB Interface (Fujitsu USB Device)]、内部シリアル番号：[TG12345678]、メーカーID：[0930]、製品ID：[0D85]	
	[追加 USB]	デバイス名：[HID 準拠マウス (Mouse USB Device)]、内部シリアル番号：[ ]、メーカーID：[046D]、製品ID：[C018]	
	[追加 Wi-Fi接続]	アクセスポイントBSSID：[00:11:22:33:44:55]、アクセスポイントSSID：[Osaka-branch-A101]、DNSサーバIPアドレス：[192.168.0.101]、Wi-Fi接続先名：[大阪支社会議室A101]	

■ 許可していないUSBデバイスを接続した場合、利用者にメッセージが表示され禁止ログが記録されます。

●●違反ログ表示例●●

	内容	備考	固有情報の説明
追加時	[追加 G:リムーバブル]	デバイス名[Fujitsu USB Flash Disk USB Device]、内部シリアル番号[BXXXXX]、メーカーID：[1111]、製品ID：[2222]	• [追加]または[変更] • ドライブレター、または、USB • ドライブの種別、または、ポータブルデバイス/イメージングデバイスの種別

利用者禁止画面

コマンドプロンプト操作記録

FUJITSU

- コマンドプロンプト操作の記録（※）
  - Windowsの[コマンドプロンプト]での操作を記録します。

●●ログ表示例●●

	内容	固有情報の説明
記録時	--[2016/01/10 23:04:48]-- Microsoft Windows [Version 6.X.XXXX] Copyright (c) 201X Microsoft Corporation. All rights reserved. E:¥Users¥dtk-user>dir ドライブ E のボリューム ラベルがありません。 ボリューム シリアル番号は XXXX-XXXX です E:¥Users¥dtk-user のディレクトリ 2015/04/16 22:39 <DIR> . 2015/04/16 22:39 <DIR> .. 2015/04/16 22:39 <DIR> Favorites 2015/11/28 21:13 <DIR> My Documents 0 個のファイル 0 バイト 4 個のディレクトリ 10,149,437,440 バイトの空き領域 E:¥Users¥dtk-user>exit	クライアントのコマンドプロンプトで入力したコマンドおよびコマンドの結果

（※）Windowsの[コマンドプロンプト]のショートカットから起動された場合のみ記録します。cmd.exeやcommand.comを直接起動した場合はログを記録しません。

連携アプリケーションの記録①

FUJITSU

■ 連携アプリケーションの記録

■ クライアントと連携するアプリケーションから送信されるログを記録します。

連携アプリケーション	説明
SMARTACCESS/Premium	SMARTACCESSで実施した認証ログを取得します。 DTKのログ検索画面で、静脈認証ログと操作ログを一連のログとして参照することができ、複数の利用者で共通のログオンIDを使用していても、利用者を特定できます。
Interstage Print Manager Standard Edition V9.0.0/V9.0.1/V9.1.0/V9.1.1/V9.1.2/V9.1.3	Interstage Print Managerで記録された、印刷内容の原本（先頭1ページ）(※)を取得します。 DTKのログ検索画面で、印刷操作ログと印刷された内容の原本を一連のログとして参照することができ、印刷物からの情報漏えい対策を強化できます。
Sense YOU Technology Biz	Sense YOU Technology Bizが覗き見検知時または他人検知時に、クライアント(CT)のデスクトップ画面のハードコピーを取得します。覗き見によって漏えいした可能性のある情報を確認できます。
PalmSecure LOGONDIRECTOR	PalmSecure LOGONDIRECTORの手のひら静脈認証時のログを取得します。 システムログオン認証およびアプリケーションのログオン認証情報を確認できます。
FUJITSU Security Solution AuthConductor	AuthConductorの認証時のログを取得します。 システムログオン認証およびアプリケーションのログオン認証情報を確認できます。

（※）Interstage Print Managerの設定により、原本として取得するページを先頭1ページから、他の任意の1ページに変更可能です。

連携アプリケーションの記録②

FUJITSU

■ 連携アプリケーションの記録

●●ログ表示例●●

	内容	固有情報の説明
SMARTACCESS/Premium連携時	製品名：[SMARTACCESS/Premium]、識別子：[60100007]、[[][Windows]Windowsにログオンしました。ID=test,DOMAIN=[saadmin]] 製品名：[SMARTACCESS/Premium]、識別子：[60100006]、[[]コンピュータをロックしました。[saadmin]] 製品名：[SMARTACCESS/Premium]、識別子：[60100005]、[[]コンピュータのロックを解除しました。[saadmin]]	・連携アプリケーションが通知する製品名 ・連携アプリケーションが通知するメッセージコード ・連携アプリケーションが通知するメッセージ
Interstage Print Manager連携時	製品名：[Print Manager]、識別子：[00049605]、[印刷が完了しました。ユーザ名:Administrator、ドキュメント名:議事録.txt、プリンタ名:PRINTER-B、7]	
Sense YOU Technology Biz連携時	製品名：[Sense YOU Technology Biz]、識別子：[19]、[覗き見を検知しました]	
PalmSecure LOGONDIRECTOR連携時	製品名：[SafetyDomain]、識別子：[5749]、[DEV14,3TEST2012G00000,3TEST2012G00000,,91,Winログオン]	
FUJITSU Security Solution AuthConductor連携時	製品名：[AuthConductor]、識別子：[5649]、[DEV14,user1,user1,,81,PCログオン設定ツール[静脈]]	

環境変更の記録

FUJITSU

- 環境変更の記録
  - クライアント(CT)環境で以下を変更したときのログを記録します。
    - IPアドレスが変更された場合
    - 緊急対処を実施/解除した場合

●●ログ表示例●●

	内容	固有情報の説明
IPアドレス変更時	種別：[IPアドレス変更]、変更前：[198.51.100.1]/[2001:db8:3::c]、変更後：[192.0.2.1]/[2001:db8:10::ee1]	・クライアント(CT)のIPアドレスが変更された場合 – 変更前のIPアドレス – 変更後のIPアドレス
緊急対処実施時	種別：[緊急対処]、[実施]	・緊急対処を実施/解除した場合 – 種別：[緊急対処](固定値) – [実施]または[解除]
緊急対処解除時	種別：[緊急対処]、[解除]	

仮想環境の操作記録と禁止

- 仮想環境における機能について
- 物理環境と仮想環境の機能差
- XenAppクライアントの操作記録
- 仮想環境とパソコン間のクリップボード操作記録
- 仮想環境とパソコン間のクリップボード操作の禁止
- 仮想環境への接続／切断記録
- 仮想環境とローカル端末の操作の横断検索

仮想環境における機能について

FUJITSU

- 仮想化の方式としては、デスクトップ仮想化（VDI方式）、アプリケーション仮想化（SBC方式）があります。通常のパソコンと仮想化パソコンのサポート範囲は以下のとおりです。

	禁止機能	記録機能	導入方法	対応仮想化ソフトウェア
物理パソコン	○	○	各パソコンにDTKクライアントを導入する	-
VDI方式 （※１）（※２）	○	○	各仮想デスクトップにDTKクライアントを導入する	VMWare vSphere VMWare Horizon Citrix XenDesktop Citrix Virtual Apps and Desktops Microsoft Hyper-V
SBC方式 （※３）	× （※3）	△	仮想化の対象となるサーバに、オプション製品Systemwalker Desktop Keeper for XenAppを導入する	VMware Horizon RDSH

（※1）VDI方式による仮想化の場合、永続化（パーシステント）方式により作成した仮想デスクトップをご利用ください。
（※2）VDI方式による仮想化の場合、USBデバイスへの持ち出し制御は、USBリダイレクトにより仮想デスクトップへ接続している場合のみ可能です。（ドライブマッピングによる接続時には対象外です。）
（※3）SBC方式による仮想化の場合、禁止機能は仮想化ソフトウェアが有しています。仮想化ソフトウェアを用いた操作禁止機能と、Systemwalker Desktop Keeperの操作記録機能を用いて、運用を行ないます。

- 仮想環境固有の機能
  - クリップボード操作の記録、禁止
    - 仮想環境へ業務や機密データを集約し運用を行なう場合に想定される、仮想環境からローカルパソコンへの情報漏えい対策としてクリップボード操作による情報持出しの記録、禁止ができます。
  - 仮想環境への接続、切断の記録
    - 仮想環境への接続、切断を記録し、接続元の端末と接続先の仮想環境を横断的にログの追跡ができます。

物理環境と仮想環境の機能差

FUJITSU

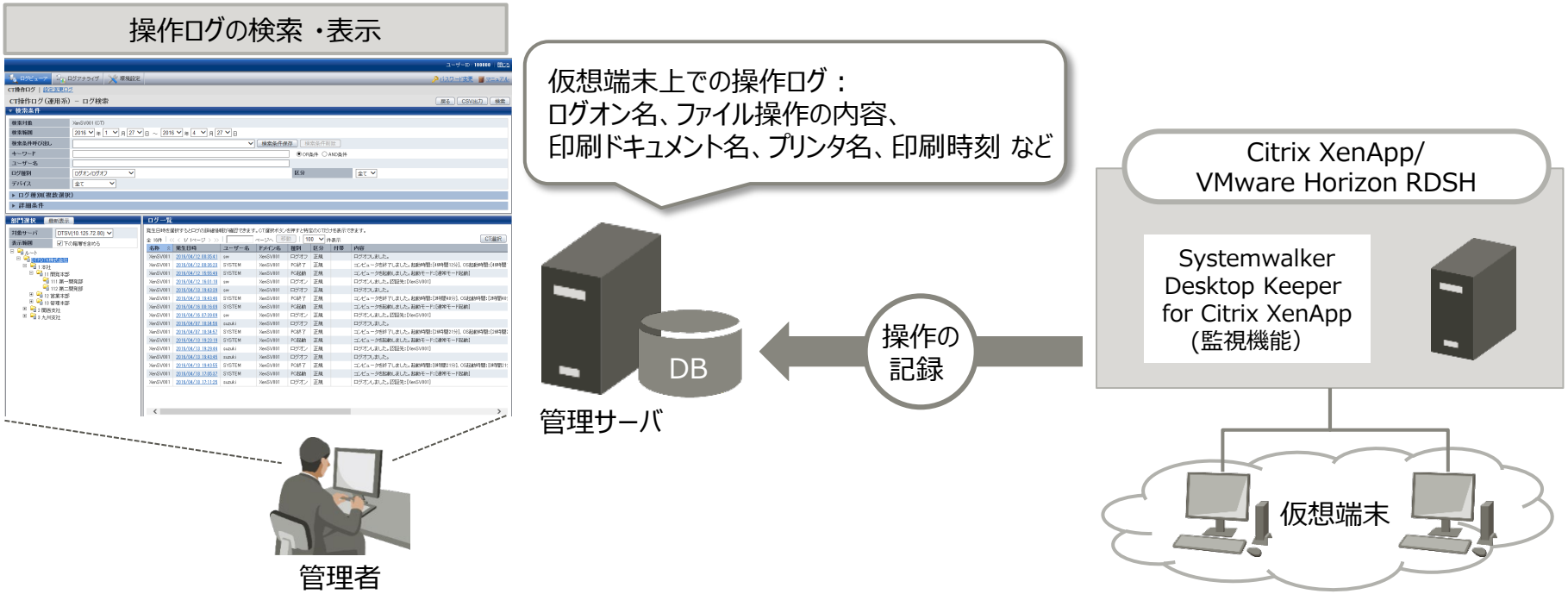
機能	機能名	物理パソコン	VDI方式	SBC方式	補足
記録	ログオン/ログオフ	○	○	○	仮想環境の場合、接続、切断の記録が合わせて行われます。
	アプリケーション起動/終了	○	○	○	
	PrintScreenキー操作	○	○	○	
	メール送信	○	○	×	
	印刷操作	○	○	○	
	ウィンドウタイトル	○	○	○	
	ウィンドウタイトル（画面キャプチャ）	○	○	○	
	Web操作（アップロード/ダウンロード）	○	○	○	
	FTP操作	○	○	○	
	ファイル操作	○	○	○	
	ファイル操作（記録対象のカスタマイズ）	○	○	×	
	原本保管	○	○	×	
	デバイス構成変更	○	○	×	VDI方式では、USBデバイス接続のログは、仮想環境へUSBリダイレクト方式で接続した場合にのみ記録します。（ドライブマッピング方式として接続した場合は、ネットワークドライブとして仮想デスクトップ上認識されるため）
	コマンドプロンプト操作	○	○	○	
	連携アプリケーション	○	○	×	
	クリップボード操作	-	○	○	
禁止	ログオン操作	○	○	×	
	アプリケーション起動	○	○	×	
	PrintScreenキー操作	○	○	×	
	メール添付操作	○	○	×	
	印刷操作	○	○	×	
	URLアクセス	○	○	×	
	Webアップロード/ダウンロード	○	○	×	
	FTPサーバ接続	○	○	×	
	サービスの制御	○	○	×	
	プロセスの制御	○	○	×	
	ファイル操作	○	○	×	
	特定ネットワークドライブ以外へのアクセス禁止	○	○	×	
	特定条件での持出許可(時間帯)	○	○	×	
	特定条件での持出許可(暗号化持出し)	○	○	×	
	特定条件での持出許可(特定USBデバイス)	○	○	×	VDI方式では、USBデバイスへの持出し制御は、仮想環境へUSBリダイレクト方式で接続した場合のみ動作します。（ドライブマッピング方式で接続した場合は、ネットワークドライブとして仮想デスクトップ上認識されるため）
	クリップボード操作	-	○	×	

※SBC方式の場合、ユーザーポリシー設定（ユーザーごとに収集するログの種別を設定）は使用できません。

XenAppクライアントの操作記録

FUJITSU

- Systemwalker Desktop Keeperのオプション製品で、XenApp監視を導入することでCitrix XenApp/VMware Horizon RDSHクライアント(仮想端末)上の操作について、ログを記録し、監査が可能になります。



取得ログ一覧			
ログオン／ログオフ	ファイル操作	印刷	コマンドプロンプト操作
アプリケーション起動/終了	ウィンドウタイトル	PrintScreenキー操作	FTP操作ログ
Web操作ログ	クリップボード操作ログ		

仮想環境とパソコン間のクリップボード操作記録

FUJITSU

■ クリップボード操作記録

- 仮想環境から物理環境または物理環境から仮想環境へクリップボードを経由して情報をコピーした時のログを記録します。
- 設定に応じて[付帯]情報としてクリップボード操作の原本を保管します。

●●ログ表示例●●

	内容	固有情報の説明
テキストコピー時	異なる環境間でクリップボード操作が行われました。方向：[仮想側→物理側]、操作元PC[PC001]、操作先PC[PC002]、アプリ名：[Notepad.exe]、形式：[テキスト]、内容：[クリップボードコピー]	• 方向 • 操作元PC • 操作先PC • アプリ名 • 形式
画像コピー時	異なる環境間でクリップボード操作が行われました。方向：[仮想側→物理側]、操作元PC[PC001]、操作先PC[PC002]、アプリ名[Notepad.exe]、形式：[画像]、内容：[クリップボードコピー]	
ファイルコピー時	異なる環境間でクリップボード操作が行われました。方向：[仮想側→物理側]、操作元PC[PC001]、操作先PC[PC002]、アプリ名：[Notepad.exe]、形式：[ファイル]、内容：[クリップボードコピー]	

★★ポイント★★

クリップボード経由で情報をコピーした場合の原本取得内容は、コピーする情報により異なります。
- テキストの場合：コピーしたテキストの内容
- 画像の場合：コピーした画像データの内容
- ファイルの場合：コピーしたファイルのパス

仮想環境とパソコン間のクリップボード操作の禁止

FUJITSU

■ クリップボード操作禁止

- ■ クライアントがインストールされている仮想環境と物理環境間でクリップボードを経由した情報のコピーを禁止できます。
- ■ 仮想環境から物理環境または物理環境から仮想環境へクリップボードを経由して情報のコピーを禁止したときのログと設定に応じて[付帯]情報として原本を保管します。

禁止時の設定項目

・・・・・・・・・・・異なる環境でのクリップボード操作・・・・・・・・・

- 禁止する
  - 原本を保管する
- 禁止しない

設定画面（管理コンソール）

●●違反ログ表示例●●

	内容	固有情報の説明
テキストコピー時	異なる環境間でのクリップボード操作を禁止しました。方向：[仮想側→物理側]、操作元PC[VM001]、操作先PC[PC002]、アプリ名：[Notepad.exe]、形式：[テキスト]、内容：[コピーしたテキスト内容]	• 方向 • 操作元PC • 操作先PC • アプリ名 • 形式 • 内容
画像コピー時	異なる環境間でのクリップボード操作を禁止しました。方向：[仮想側→物理側]、操作元PC[VM001]、操作先PC[PC002]、アプリ名：[mspaint.exe]、形式：[画像]、内容：[]	
ファイルコピー時	異なる環境間でのクリップボード操作を禁止しました。方向：[物理側→仮想側]、操作元PC[PC002]、操作先PC[VM001]、アプリ名：[explorer.exe]、形式：[ファイル]、内容：[c:¥temp¥test.csv]	

★★ポイント★★

クリップボード経由で情報をコピーした場合の原本取得内容は、コピーする情報により異なります。

- テキストの場合：コピーしようとしたテキストの内容
- 画像の場合：コピーしようとした画像データの内容
- ファイルの場合：コピーしようとしたファイルのパス

仮想環境への接続／切断記録

FUJITSU

■ 仮想環境への接続記録

■ パソコンから仮想パソコンへの接続および切断した際のログを記録できます。

●●ログ表示例●●

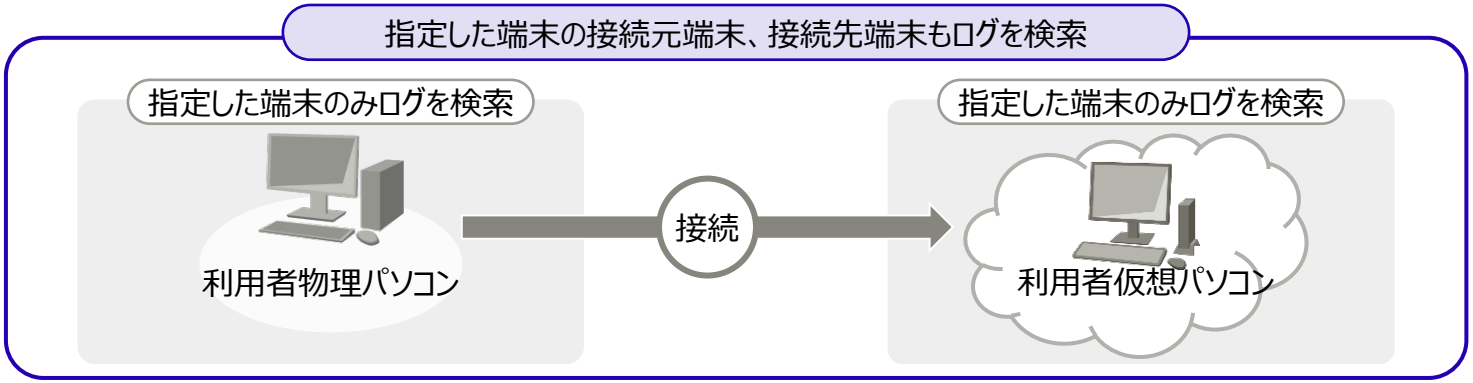
	内容	固有情報の説明
接続時	コンピュータ[AAA(物理PC)]からコンピュータ[BBB(仮想PC)]に接続しました。	・ 接続元端末のコンピュータ名 ・ 接続先端末のコンピュータ名
接続終了時	コンピュータ[AAA(物理PC)]からコンピュータ[BBB(仮想PC)]への接続を終了しました。	

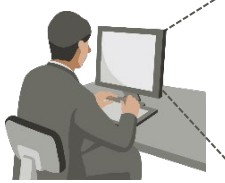
仮想環境とローカル端末の操作の横断検索

FUJITSU

■ 仮想環境とローカル端末の操作の横断検索

■ 仮想環境への接続ログを元に仮想パソコン上の操作と物理パソコン側の操作を自動で紐づけて検索することができます。





管理者

ログ検索設定

ログ検索設定

ログ検索時の動作設定を行います。

接続元・接続先端末のログ検索	○ 指定した端末のみログ検索をする	◉ 指定した端末の接続元端末、接続先端末もログを検索する

ログ検索結果

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	2016/04/27 14:57:33	suzuki	PC001	ファイル操作	正規		操作:[複写]、ファイル名元:[C:¥Users¥Owner¥Desktop¥お知らせ.xlsx]、ドライブ種別元:[固定]、ファイル名先:[G:¥お知らせ.
PC001	2016/04/27 14:55:41	suzuki	PC001	ファイル操作	正規		操作:[変名]、ファイル名元:[C:¥Users¥Owner¥Desktop¥見積明細.csv]、ドライブ種別元:[固定]、ファイル名先:[C:¥Users¥Ow
PC001	2016/04/27 14:55:27	suzuki	PC001	ファイル操作	正規		操作:[作成]、ファイル名:[C:¥Users¥Owner¥Desktop¥見積明細.xlsx]、ドライブ種別:[固定]、アプリ名:[Explorer.exe]
DTSV	2016/04/27 14:54:11	Administrator	DTSV	クリップボード操作	正規	1	異なる環境間でクリップボード操作が行われました。方向:[仮想側→物理側]、操作元PC:[DTSV]、操作先PC:[PC001]、アプ
DTSV	2016/04/27 14:52:29	Administrator	DTSV	ファイル操作	正規		操作:[作成]、ファイル名:[C:¥temp¥メモ.txt]、ドライブ種別:[固定]、アプリ名:[Explorer.exe]
PC001	2016/04/27 14:52:23	suzuki	PC001	PC接続	正規		コンピュータ[PC001(物理PC)]からコンピュータ[DTSV(仮想PC)]に接続しました。
DTSV	2016/04/27 14:51:17	Administrator	DTSV	ログオン	正規		ログオンしました。認証先:[DTSV]

PC接続を基点に接続元、接続先端末のログを自動で紐付け

★★ポイント★★

端末ごとに操作を確認するのではなく、互いの端末の操作を同時に参照することができ、利用者の操作を明確に把握することができます。

ログ分析／出力機能

- 情報漏洩予防診断について
- 操作別集計結果表示
- 違反操作ランキング
- 目的別集計機能について
- 集計結果表示
- 目的別集計機能項目一覧
- 分析レポートの出力
- 情報漏洩分析レポート
- 端末利用分析レポート
- 違反操作分析レポート
- 紙のコストとCO2排出量の『見える化』
- 複合機／プリンタの紙の使用状況の『見える化』
- 用紙使用状況の通知

情報漏洩予防診断について

- ファイル持出し操作、ファイル操作、印刷操作、メール送信操作を集計できます。
- 各端末の集計値を分析し、結果を表示できます。
- キーワードによる絞込条件や、端末単位の除外条件により業務実態に合わせ、精度の高い分析ができます 。
- 集計結果うち、外部流出の可能性がある操作件数を表示します。その中で一番件数の多い操作を赤マーク表示することで、一目で状況を把握できます。

[ログアナライザ]画面

カレンダーから過去1年間のデータを参照

集計結果のうち、外部流出の可能性がある操作件数を表示

情報漏えいにつながる可能性のある操作の動向を数値化し、リスク傾向を把握できます。

操作別集計結果表示

FUJITSU

- 指定された日の下記の操作について件数を表示します。
- 各操作の件数が最大値となる日は、注意すべき日として赤色で表示されます。
- 操作対象のファイル名に管理者が事前登録したキーワードを含む操作に絞った集計も可能です。
  - 重要ファイル名をキーワード登録しておくことで、注意すべき操作に絞って確認できます。

集計操作	集計内容
ファイル持出し操作	持出しユーティリティを使用して、可搬媒体（リムーバブルおよびCD/DVD）へファイル持出しを行った操作回数を集計します。
ファイル操作	ドライブ種別がリムーバブルおよびCD/DVDに、ファイルの作成、更新、移動、複写を行った 操作回数を集計します。
印刷操作	印刷を行った操作回数の集計と、印刷を行った総ページ数を集計します。
メール送信操作	メール発信操作回数を集計します。
FTPアップロード操作	FTPサーバにアップロードした操作回数を集計します。
Webアップロード操作	Webサーバにアップロードした操作回数を集計します。

[ログアナライザ]画面

操作別集計結果

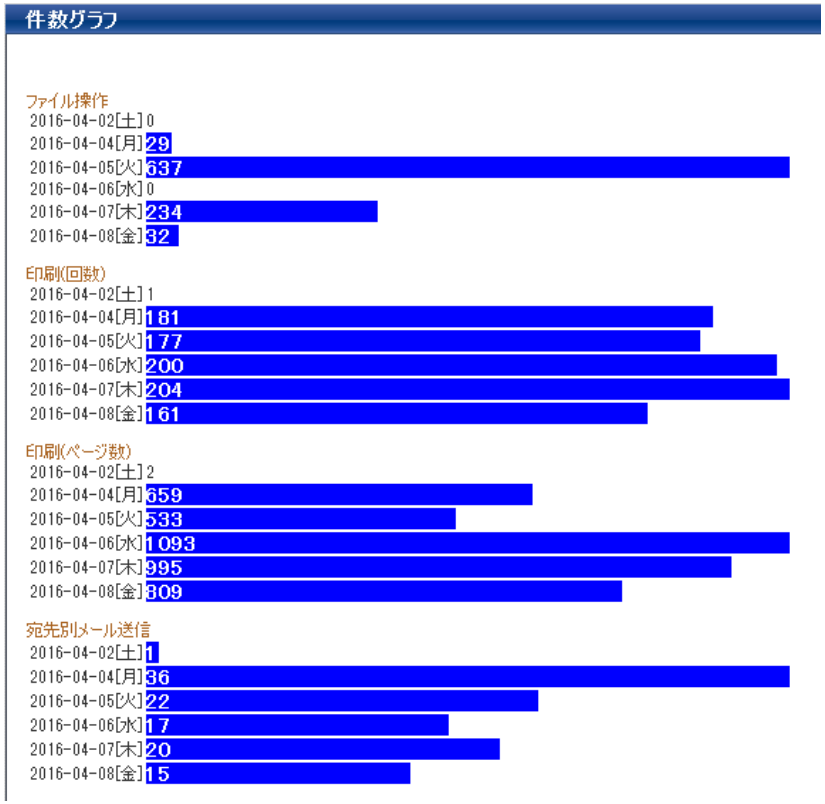
操作名	4/2 (土)	4/3 (日)	4/4 (月)	4/5 (火)	4/6 (水)	4/7 (木)	4/8 (金)	合計
ファイル持出し	0	0	0	0	0	0	0	0
ファイル操作	0	0	29	**637**	0	234	32	932
印刷操作(回数)	1	0	181	177	200	**204**	161	924
印刷操作(ページ数)	2	0	659	533	**1093**	995	809	4091
宛先別メール送信	1	0	**36**	22	17	20	15	111
FTP操作(アップロード)	0	0	40	**69**	14	25	51	199
Web操作(アップロード)	1	0	58	119	99	85	**125**	487

（補足）操作別集計結果表示-表示例-

FUJITSU

- 操作別集計結果をグラフで表示できます。
- グループ別、端末別、ユーザー別、端末別かつユーザー別のランキングを表示できます。

操作別集計結果



ランキング

No.	件数	端末名¥ユーザー名	グループ名
1	389	ME-PC017¥tanaka	営業本部
2	132	ME-PC102¥takada	営業本部
3	83	ME-PC098¥suzuki	営業本部
4	53	DE-PC010¥takahashi	開発本部
5	50	AE-PC001¥sakamoto	総務部

違反操作ランキング

- Systemwalker Desktop Keeper で禁止されているパソコン操作を行った際に記録されるログを集計できます。
- 禁止操作を行った回数を違反操作回数として、操作ごとに1日単位で合計値をとり、グループ単位でのランキング表示ができます。

[ログアナライザ]画面

情報漏洩予防診断

操作別集計結果

操作名	4/7 (木)	4/8 (金)	4/9 (土)	4/10 (日)	4/11 (月)	4/12 (火)	4/13 (水)	合計
ファイル持出し	0	0	0	0	0	0	0	0
ファイル操作	3	3	0	0	1	1	0	8
印刷操作(回数)	0	0	0	0	0	0	0	0
印刷操作(ページ数)	0	0	0	0	0	0	0	0
宛先別メール送信	0	0	0	0	0	0	0	0
FTP操作(アップロード)	0	0	0	0	0	0	0	0
Web操作(アップロード)	0	0	0	0	0	0	0	0

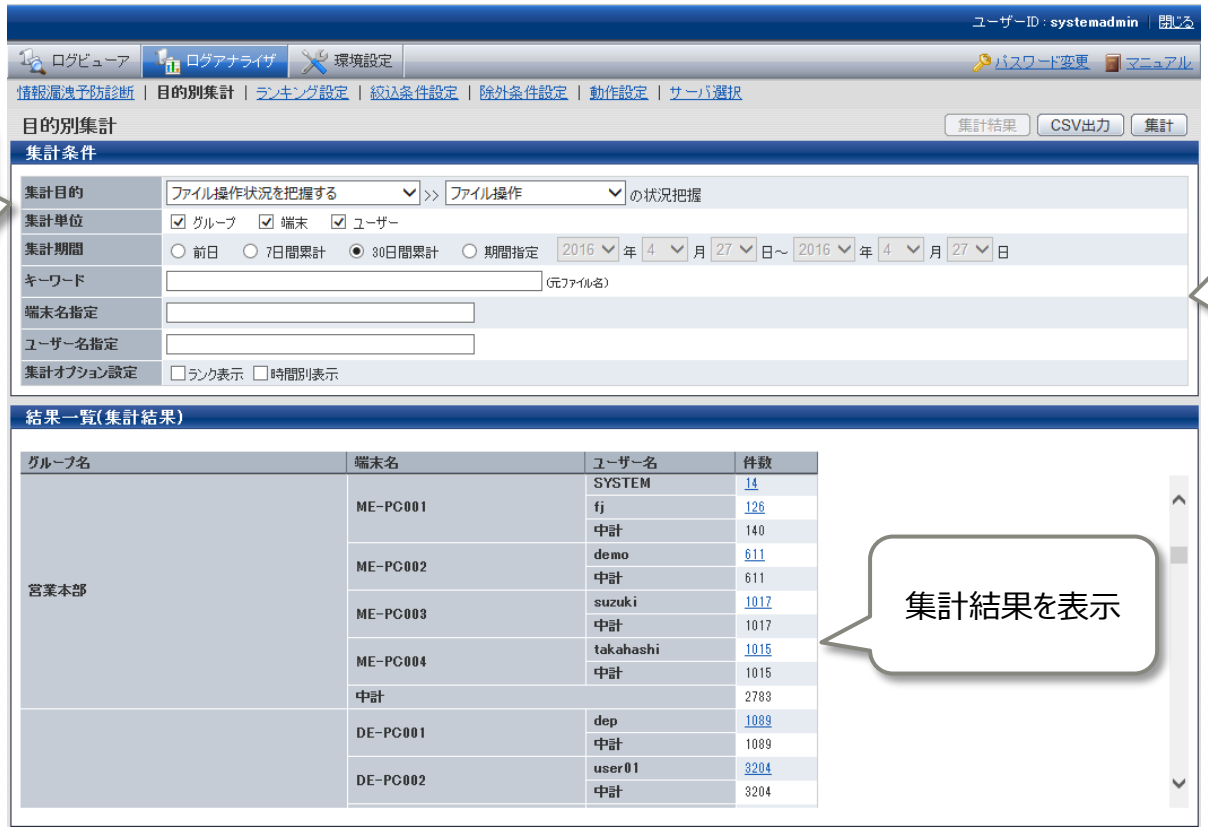
違反操作ランキング 対象日:2016/04/13 (水)

No.	グループ名	端末名	アプリケーション起動禁止	印刷禁止	ログオン禁止	PrintScreenキー禁止	メール添
1	DTPDTK株式会社/1 本社/13 管理本部/131 情報システム部	PC001	1	0	0	0	

目的別集計機能について

- 目的別に集計単位や集計期間などの条件を設定してログを集計します。
- 情報漏えいの可能性のある各種操作毎にリスク傾向を分析できます。

[ログアナライザ]画面



「目的別一覧」から集計目的（集計対象）を選択

集計単位、集計期間、キーワード、端末名、ユーザー名などの「集計条件」を設定

集計結果を表示

情報漏えいのもととなる操作をより細密に分析し、ユーザー毎のリスク傾向を把握できます。

集計結果表示

- 目的別集計結果は、表形式で表示されます。
- 目的別集計では、集計結果または詳細結果をＣＳＶ形式でファイルに出力することができ、データの利用/加工が容易にできます。

［結果一覧（集計結果）］画面

結果一覧(集計結果)

グループ名	件数
開発部	3

集計単位ごとの集計値を表示
集計値をクリックし、内訳の詳細情報を表示

［結果一覧（詳細結果）］画面

結果一覧(詳細結果)

全3件 | << < 1/1ページ > >> | 1 ページへ 移動

グループ名	アプリケーション名	URL	ウィンドウタイトル	発生日時
開発部	IEXPLORE	http://localhost/dwl.html	Systemwalker - Microsoft Internet Explorer	2015/06/15 10:53:52
開発部	IEXPLORE	http://localhost/	Systemwalker - Microsoft Internet Explorer	2015/06/15 10:54:01
開発部	IEXPLORE	http://localhost/dwl.html	Systemwalker - Microsoft Internet Explorer	2015/06/15 10:55:53

指定した集計単位（「グループ名」「端末名」「ユーザー名」のうち選択したもの）の名前を表示

（補足）集計結果表示例

FUJITSU

表示例：違反操作状況の把握（アプリケーション起動禁止）

結果一覧(詳細結果)

全2件 | << < 1/1ページ > >> | 1 ページへ 移動

グループ名	アプリケーション名	発生日時
開発部	winny	2015/06/15 12:44:34
開発部	winny	2015/06/15 12:44:34

表示例：ファイル持出し状況の把握

結果一覧(詳細結果)

全2件 | << < 1/1ページ > >> | 1 ページへ 移動

グループ名	持出し元ファイル名	持出し先ファイル名	持出し先種別	持出種
開発部	C:¥Documents and Settings¥デスクトップ¥(UNC).xls	D:¥test.exe	1	暗号化
開発部	C:¥Documents and Settings¥デスクトップ¥(UNC).xls	D:¥test.exe	1	暗号化

表示例：ファイル操作状況の把握

結果一覧(詳細結果)

全997件 | << < 1/1ページ > >> | 1 ページへ 移動

グループ名	操作種別	元ファイル名	元ドライブ種別	先ファイル名
Local/開発部/システム開発部	複写	C:¥F4ANsetup.log	固定	C:¥DTK¥F4ANsetup.log
Local/開発部/システム開発部	複写	¥¥Device¥RdpDr¥tsclient¥F¥Printtool¥Disk1¥_Setup.dll	リモート	C:¥Users¥Administrator¥Desktop¥Printtool¥[
Local/開発部/システム開発部	複写	¥¥Device¥RdpDr¥tsclient¥F¥Printtool¥Disk1¥ISSetup.dll	リモート	C:¥Users¥Administrator¥Desktop¥Printtool¥[
Local/開発部/システム開発部	複写	¥¥Device¥RdpDr¥tsclient¥F¥Printtool¥Disk1¥data1.cab	リモート	C:¥Users¥Administrator¥Desktop¥Printtool¥[
Local/開発部/システム開発部	作成	C:¥Users¥Administrator¥Desktop¥Printtool¥Disk1	固定	－
Local/開発部/システム開発部	作成	C:¥Users¥Administrator¥Desktop¥Printtool	固定	－
Local/開発部/システム開発部	複写	¥¥Device¥RdpDr¥tsclient¥F¥Printtool¥Disk1¥data2.cab	リモート	C:¥Users¥Administrator¥Desktop¥Printtool¥[
Local/開発部/システム開発部	複写	¥¥Device¥RdpDr¥tsclient¥F¥Printtool¥Disk1¥data1.hdr	リモート	C:¥Users¥Administrator¥Desktop¥Printtool¥[
Local/開発部/システム開発部	複写	¥¥Device¥RdpDr¥tsclient¥F¥Printtool¥Disk1¥setup.exe	リモート	C:¥Users¥Administrator¥Desktop¥Printtool¥[
Local/開発部/システム開発部	複写	¥¥Device¥RdpDr¥tsclient¥F¥Printtool¥Disk1¥setup.inx	リモート	C:¥Users¥Administrator¥Desktop¥Printtool¥[
Local/開発部/システム開発部	複写	¥¥Device¥RdpDr¥tsclient¥F¥Printtool¥Disk1¥layout.bin	リモート	C:¥Users¥Administrator¥Desktop¥Printtool¥[

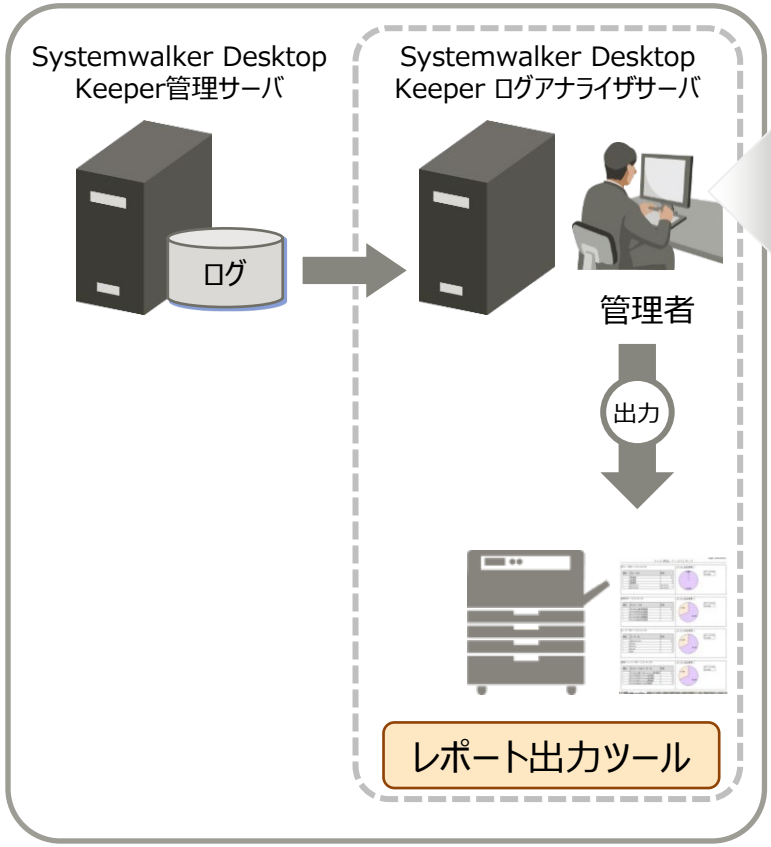
目的別集計機能項目一覧

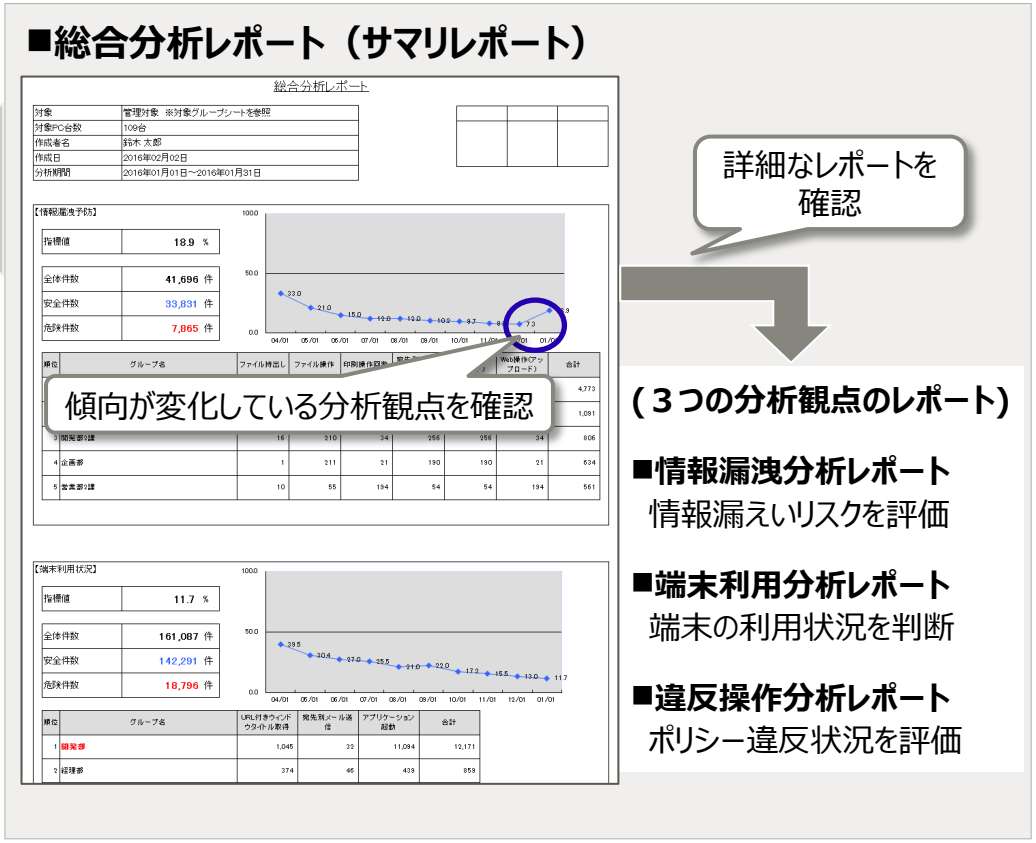
FUJITSU

	集計目的(禁止操作種別)	集計内容	詳細表示項目
違反操作 状況の把握	アプリケーション起動禁止の状況把握	アプリケーション起動禁止に該当する件数を集計します。	アプリケーション名、発生日時
	印刷禁止の状況把握	印刷禁止に該当する件数を集計します。	印刷ファイル名、発生日時
	ログオン禁止の状況把握	ログオン禁止に該当する件数を集計します。	ユーザー名、発生日時
	PrintScreenキー禁止の状況把握	PrintScreenキー禁止に該当する件数を集計します。	発生日時
	メール添付禁止の状況把握	メール添付禁止に該当する件数を集計します。	添付ファイル名、発生日時
ファイル持出し 状況の把握	ファイル持出しの状況把握	ファイル持出し件数を集計します。	持出し元ファイル名、持出し先ファイル名、 先ドライブ種別、持出種別、発生日時
	ファイル持出し(ドライブ別)の状況把握	ファイル持出し件数を、持出し先ドライブ種別単位で集計します。	持出し元ファイル名、持出し先ファイル名、 持出種別、発生日時
ファイル操作 状況の把握	ファイル操作の状況把握	ファイル操作件数を集計します。	操作種別、元ファイル名、先ファイル名、 先ドライブ種別、アプリケーション名、発生日時
	ファイル操作(リモート)の状況把握	ネットワーク上のファイル操作件数を集計します。	操作種別、元ファイル名、先ファイル名、 先ドライブ種別、アプリケーション名、発生日時
	ファイル操作(リムーバブル)の状況把握	リムーバブルメディア上のファイル操作件数を集計します。	操作種別、元ファイル名、先ファイル名、 先ドライブ種別、アプリケーション名、発生日時
アプリケーション・ メール状況の把握	アプリケーション起動の状況把握	アプリケーション動作件数を集計します。	発生日時
	宛先別メール送信の状況把握	メール送信件数を集計します。	件名、From、To、CC、BCC、添付、発生日時
印刷操作 状況の把握	印刷操作(回数)の状況把握	印刷操作件数を集計します。	印刷ファイル名、ページ数、プリンタ名、発生日時
	印刷操作(ページ数)の状況把握	印刷総ページ数を集計します。	ページ数、印刷ファイル名、発生日時
Webアクセス 状況の把握	URL付きウィンドウタイトル 取得の状況把握	URL付きウィンドウタイトルを集計します。	アプリケーション名、URL、ウィンドウタイトル、 発生日時
	URL付きウィンドウタイトル 取得(サイト別)の状況把握	URL付きウィンドウタイトルを、サイト単位で集計します。	アプリケーション名、URL、ウィンドウタイトル、 発生日時

分析レポートの出力

- セキュリティ状況やパソコンの利用状況を分析し、Excel形式のレポートを出力できます。これにより、組織上層部に対し、状況を報告するための資料作成の負荷が軽減します。
- 分析レポートの出力は全社または部門ごとに出力できます。
- 管理者は総合分析レポートから傾向が変化している分析観点を確認し、各分析観点のレポートを確認できます。





情報漏洩分析レポート

FUJITSU

- 情報漏えいの危険性を分析する観点でログを集計・分析した結果を出力します。
- 外部へ情報が流出する可能性のある操作(※)（例：USBデバイスへのコピー、外部ドメインへのメール、印刷、等）を集計します。
- 重要ファイル名をキーワード登録しておくことで、注意すべき操作に絞って状況把握ができます。

レポート（一例）

概要

情報漏洩分析レポート

対象	管理対象 ※対象グループシートを参照
対象PC台数	109台
作成者名	鈴木 太郎
作成日	2016年02月02日
分析期間	2016年01月01日～2016年01月31日

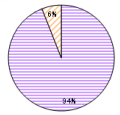
【診断情報】

指標値	6.0 %

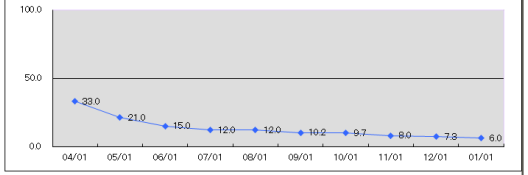
全体の危険件数が一目でわかる

【件数割合】

全体件数	41,696 件
安全件数	39,212 件
危険件数	2,484 件



【指標値推移グラフ】



【診断コメント】
【情報漏洩分析】
前回より改善しました。長期的には、改善傾向です。
2016年01月26日のファイル操作数件数が通常より多くなっています。詳細に調査してください。

過去からの傾向がグラフ/コメントでわかる

日毎の危険件数が一目でわかる

【操作別件数推移】

	ファイル持出し	ファイル操作	印刷操作回数	印刷操作ページ数	宛先別メール送信	FTP操作(アップロード)	Web操作(アップロード)
2016年01月01日	0	0	0	0	0	0	0
2016年01月02日	0	0	0	0	0	0	0
2016年01月03日	0	0	0	0	0	0	0
2016年01月04日	0	1	8	15	12	15	12
2016年01月05日	6	0	43	89	19	89	19
2016年01月06日	9	34	211	234	34	234	34
2016年01月07日	1	82	34	47	22	47	22
2016年01月08日	0	0	0	0	15	0	15
2016年01月09日	0	0	0	0	0	0	0
2016年01月10日	0	0	0	0	0	0	0
2016年01月11日	0	15	12	18	34	18	34
2016年01月12日	4	67	134	154	32	154	32
2016年01月13日	3	83	24	48	19	48	19
2016年01月14日	0	0	55	74	18	74	18
2016年01月15日	0	0	0	0	0	0	0
2016年01月16日	4	0	0	0	0	0	0
2016年01月17日	1	45	46	83	76	83	76
2016年01月18日	1	16	122	222	33	222	33
2016年01月19日	2	9	112	176	89	176	89
2016年01月20日	3	1	34	47	16	47	16
2016年01月21日	7	18	21	45	26	45	26
2016年01月22日	0	0	0	0	0	0	0
2016年01月23日	0	0	0	0	0	0	0
2016年01月24日	0	5	19	32	36	32	36
2016年01月25日	2	2	28	32	23	32	23
2016年01月26日	15	216	37	48	22	48	22
2016年01月27日	1	12	68	78	26	78	26
2016年01月28日	2	26	59	69	29	69	29
2016年01月29日	0	0	0	0	0	0	0
2016年01月30日	0	0	0	0	0	0	0
2016年01月31日	0	8	59	129	76	129	76
合計	61	640	1126	1640	657	1640	657

詳細

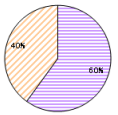
作成日：2016年02月02日

ファイル持出し ランキング

【グループ別ランキング】

順位	グループ名	件数
1	営業部1課	22
2	開発部1課	16
3	経理部	12
4	営業部2課	10
5	企画部	1

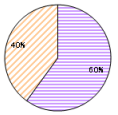
ランキング上位占有率



【端末別ランキング】

順位	コンピュータ名	件数
1	PC003[営業部1課]	22
2	PC045[開発部1課]	16
3	PC086[経理部]	12
4	PC018[営業部2課]	2
5	PC019[営業部2課]	1

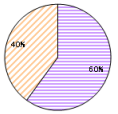
ランキング上位占有率



【ユーザー別ランキング】

順位	ユーザー名	件数
1	u003	22
2	u045	16
3	u086	12
4	u018	2
5	u019	1

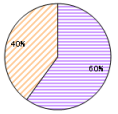
ランキング上位占有率



【端末＋ユーザー別ランキング】

順位	コンピュータ名+ユーザー名	件数
1	PC003+u003[営業部1課]	22
2	PC045+u045[開発部1課]	16
3	PC086+u086[経理部]	12
4	PC018+u018[営業部2課]	2
5	PC019+u019[営業部2課]	1

ランキング上位占有率



操作(※)毎の危険件数をグループ/端末/ユーザーの切り口でチェック

(※) ファイル持出し、ファイル操作、印刷操作（回数/ページ数）、メール送信、FTPアップロード、Webアップロード

端末利用分析レポート

FUJITSU

- コンプライアンス上の適正利用の観点で、ログを集計・分析した結果を出力します。
- Webアクセス、メール送信、アプリケーション起動について、あらかじめ登録したドメインやアプリケーション以外の操作を危険件数として集計します。
- 社内ドメインや業務アプリを登録しておくことで、注意すべき操作に絞って状況把握ができます。

レポート（一例）

概要

端末利用分析レポート

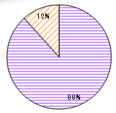
対象	管理対象　※対象グループシートを参照
対象PC台数	109台
作成者名	鈴木 太郎
作成日	2016年02月02日
分析期間	2016年01月01日～2016年01月31日

【診断情報】

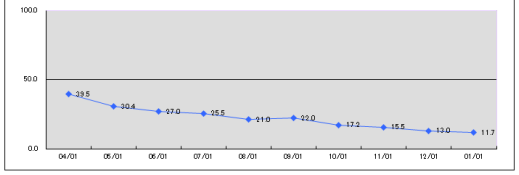
指標値	11.7 %

【件数割合】

全体件数	161,087	件
安全件数	142,291	件
危険件数	18,796	件



【指標値推移グラフ】



【診断コメント】
[端末利用分析]
前回より改善しました。長期的には、改善傾向です。
2016年01月12日の宛先別メール送信件数が通常より多くなっています。詳細に調査してください。

全体の危険件数が一目でわかる

過去からの傾向がグラフ/コメントでわかる

【操作別件数推移】

	URL付きウィンドウタイトル取得	宛先別メール送信	アプリケーション起動
2016年01月01日	0	0	0
2016年01月02日	0	0	0
2016年01月03日	0	0	0
2016年01月04日	183	2	536
2016年01月05日	343	3	562
2016年01月06日	282	0	672
2016年01月07日	183	5	652
2016年01月08日	45	0	233
2016年01月09日	0	0	0
2016年01月10日	3	0	3
2016年01月11日	263	6	628
2016年01月12日	183	177	728
2016年01月13日	187	22	748
2016年01月14日	226	0	627
2016年01月15日	0	0	0
2016年01月16日	13	0	182
2016年01月17日	173	0	784
2016年01月18日	228	6	647
2016年01月19日	170	33	663
2016年01月20日	181	18	837
2016年01月21日	182	0	822
2016年01月22日	28	0	481
2016年01月23日	0	0	0
2016年01月24日	182	0	824
2016年01月25日	167	0	645
2016年01月26日	183	24	634
2016年01月27日	212	0	1022
2016年01月28日	221	22	845
2016年01月29日	33	0	554
2016年01月30日	0	0	0
2016年01月31日	273	0	55
合計	4144	318	14334

日毎の危険件数が一目でわかる

詳細

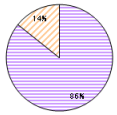
作成日：2016年02月02日

URL付きウィンドウタイトル取得 ワーストランキング

【グループ別ワーストランキング】

順位	グループ名	件数
1	企画部	1022
2	開発部1課	945
3	営業部1課	719
4	経理部	534
5	営業部2課	332

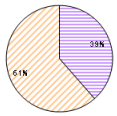
ワースト上位占有率



【端末別ワーストランキング】

順位	コンピュータ名	件数
1	PC076[企画部]	473
2	PC046[開発部1課]	337
3	PC014[営業部1課]	308
4	PC085[経理部]	276
5	PC070[経理部]	203

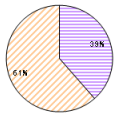
ワースト上位占有率



【ユーザー別ワーストランキング】

順位	ユーザー名	件数
1	u076	473
2	u046	337
3	u014	308
4	u085	276
5	u070	203

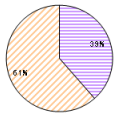
ワースト上位占有率



【端末＋ユーザー別ワーストランキング】

順位	コンピュータ名+ユーザー名	件数
1	PC076+u076[企画部]	473
2	PC046+u046[開発部1課]	337
3	PC014+u014[営業部1課]	308
4	PC085+u085[経理部]	276
5	PC070+u070[経理部]	203

ワースト上位占有率



操作(※)毎の危険件数をグループ/端末/ユーザーの切り口でチェック

違反操作分析レポート

- ポリシー違反の観点で、ログを集計・分析した結果を出力します。
- ポリシーにより禁止されている操作を利用者が試みた回数を、危険件数として集計します。
- 禁止操作を繰り返し試みた形跡のある端末、ユーザーを確認することで、不正行為につながる予兆を検知することができます。

レポート（一例）

概要

違反操作分析レポート

対象	管理対象 ※対象グループシートを参照
対象PC台数	109台
作成者名	鈴木 太郎
作成日	2016年02月02日
分析期間	2016年01月01日～2016年01月31日

【診断情報】

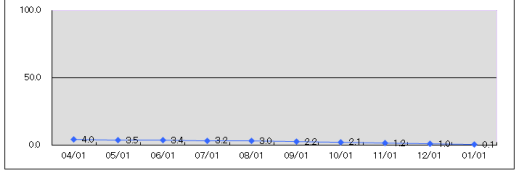
指標値	0.1 %

全体の危険件数が一目でわかる

【件数割合】

全体件数	202,952 件
安全件数	202,783 件
危険件数	169 件

【指標値推移グラフ】



【診断コメント】
【違反操作分析】
前回と変化ありません。長期的には、改善傾向です。
2016年01月07日のログオン禁止件数が通常より多くなっています。詳細ご調査してください。

過去からの傾向がグラフ/コメントでわかる

日毎の危険件数が一目でわかる

【操作別件数推移】

	アプリケーション起動禁止	印刷禁止	ログオン禁止	PrintScreenキー禁止	メール添付禁止
2016年01月01日	0	0	0	0	0
2016年01月02日	0	0	0	0	0
2016年01月03日	0	0	0	0	0
2016年01月04日	3	0	0	0	0
2016年01月05日	0	2	0	0	0
2016年01月06日	4	3	0	4	5
2016年01月07日	0	2	21	0	1
2016年01月08日	0	0	0	0	0
2016年01月09日	0	0	0	0	0
2016年01月10日	0	0	0	0	0
2016年01月11日	0	1	0	0	3
2016年01月12日	5	5	0	0	0
2016年01月13日	6	1	0	0	0
2016年01月14日	0	1	1	4	6
2016年01月15日	0	0	0	0	0
2016年01月16日	0	0	0	0	0
2016年01月17日	0	3	0	0	3
2016年01月18日	10	6	0	0	0
2016年01月19日	23	3	0	0	4
2016年01月20日	0	2	0	0	0
2016年01月21日	0	4	0	5	1
2016年01月22日	0	0	0	0	0
2016年01月23日	0	0	0	0	0
2016年01月24日	0	2	0	0	0
2016年01月25日	1	1	0	0	2
2016年01月26日	4	1	0	0	0
2016年01月27日	8	1	0	0	0
2016年01月28日	6	0	0	0	0
2016年01月29日	0	0	0	0	0
2016年01月30日	0	0	0	0	0
2016年01月31日	0	1	0	0	0
合計	70	39	22	13	25

詳細

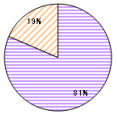
作成日：2016年02月02日

アプリケーション起動禁止 ワーストランキング

【グループ別ワーストランキング】

順位	グループ名	件数
1	営業部2課	22
2	開発部1課	17
3	営業部1課	10
4	企画部	5
5	経理部	3

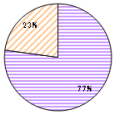
ワースト上位占有率



【端末別ワーストランキング】

順位	コンピュータ名	件数
1	PC024[営業部2課]	18
2	PC048[開発部1課]	17
3	PC010[営業部1課]	10
4	PC074[企画部]	5
5	PC030[営業部2課]	4

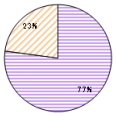
ワースト上位占有率



【ユーザー別ワーストランキング】

順位	ユーザー名	件数
1	u024	18
2	u048	17
3	u010	10
4	u074	5
5	u030	4

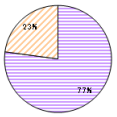
ワースト上位占有率



【端末＋ユーザー別ワーストランキング】

順位	コンピュータ名+ユーザー名	件数
1	PC024+u024[営業部2課]	18
2	PC048+u048[開発部1課]	17
3	PC010+u010[営業部1課]	10
4	PC074+u074[企画部]	5
5	PC030+u030[営業部2課]	4

ワースト上位占有率



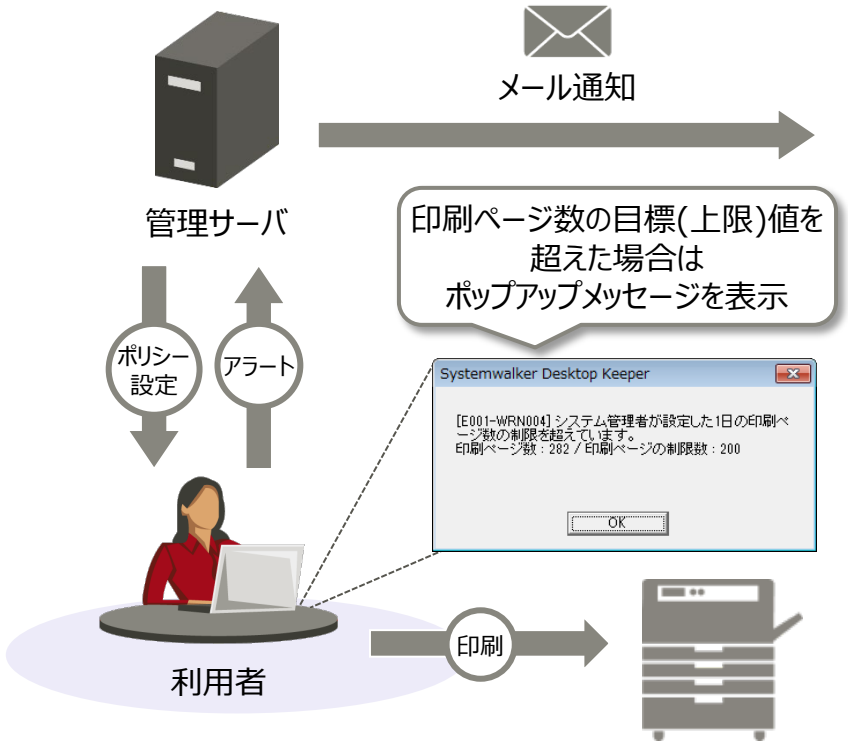
操作(※)毎の危険件数をグループ/端末/ユーザーの切り口でチェック

※ アプリケーション起動禁止、印刷禁止、ログオン禁止、PrintScreenキー禁止、メール添付禁止

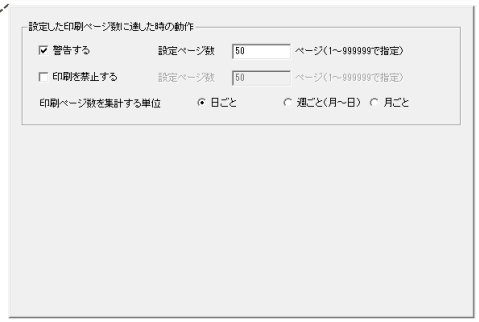
紙のコストとCO2排出量の『見える化』

FUJITSU

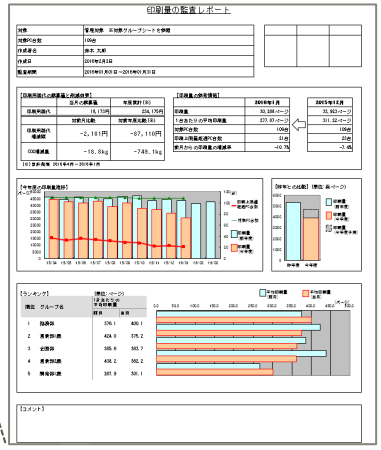
- 紙のコストとCO2排出量の推移をグラフ表示して推移や削減効果を見える化できます。
- 削減目標値（※）を設定し、傾向から目標値を超過しそうな利用者にはポップアップメッセージを表示して改善を促します。また、目標値を超過した利用者の印刷禁止設定ができます。
- Excel ファイル（またはレポート）に出力して報告書を作成できます。



印刷ページ目標(上限)設定



印刷量監査レポート

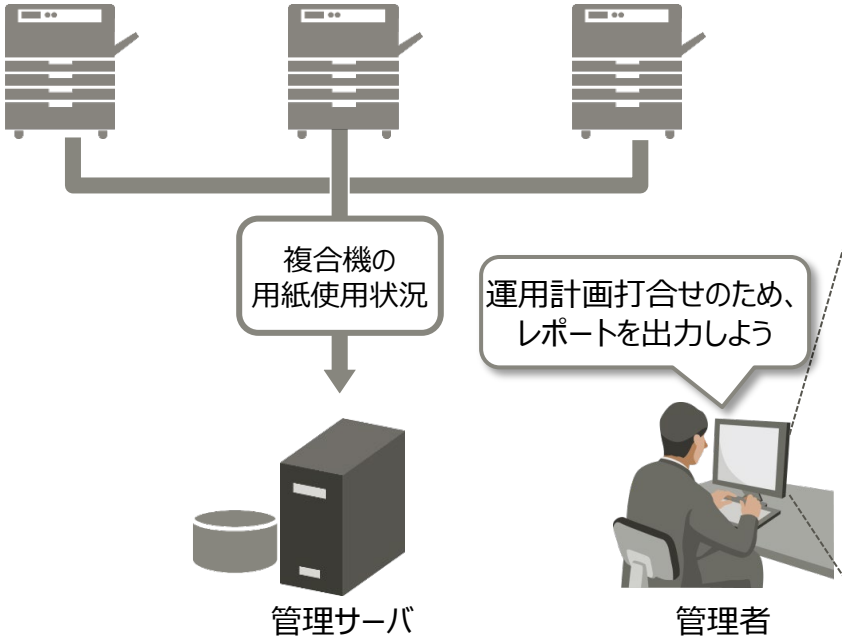


（※）目標(上限)値は日、週、月単位で設定できます。

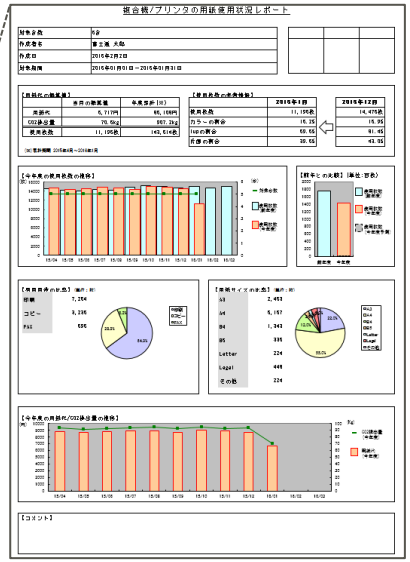
複合機／プリンタの紙の使用状況の『見える化』（※）

FUJITSU

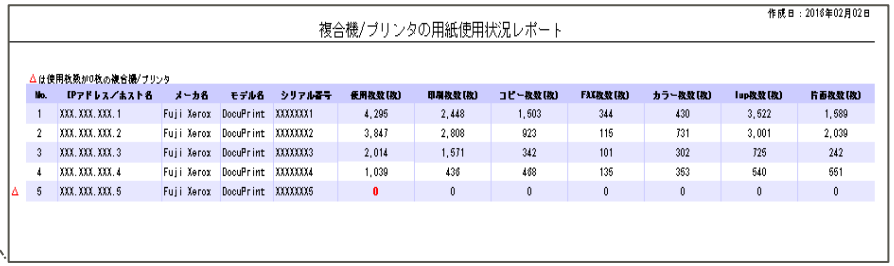
- 複合機の紙の使用量とCO2排出量換算の結果をレポート出力します。
  実績値を「見える化」することで無駄な印刷を抑止し、CO2排出量の削減に貢献します。
- 複合機ごとの使用状況を「見える化」することで複合機の削減や導入などの運用計画を支援します。



複合機/プリンタの用紙使用状況レポート



用紙代の概算値、
使用枚数の推移、
利用用途比、用紙サイズ、
CO2排出量の推移などを表示



作成日：2016年02月02日

複合機/プリンタの用紙使用状況レポート

△は使用枚数が0枚の複合機/プリンタ

	No.	IPアドレス/ホスト名	メーカ名	モデル名	シリアル番号	使用枚数(枚)	印刷枚数(枚)	コピー枚数(枚)	FAX枚数(枚)	カラー枚数(枚)	lap枚数(枚)	片面枚数(枚)
	1	XXX.XXX.XXX.1	Fuji Xerox	DocuPrint	XXXXXXX1	4,295	2,448	1,503	344	430	3,622	1,989
	2	XXX.XXX.XXX.2	Fuji Xerox	DocuPrint	XXXXXXX2	3,847	2,808	923	116	731	3,001	2,039
	3	XXX.XXX.XXX.3	Fuji Xerox	DocuPrint	XXXXXXX3	2,014	1,571	342	101	302	725	242
	4	XXX.XXX.XXX.4	Fuji Xerox	DocuPrint	XXXXXXX4	1,039	436	468	135	363	640	661
△	5	XXX.XXX.XXX.5	Fuji Xerox	DocuPrint	XXXXXXX5	0	0	0	0	0	0	0

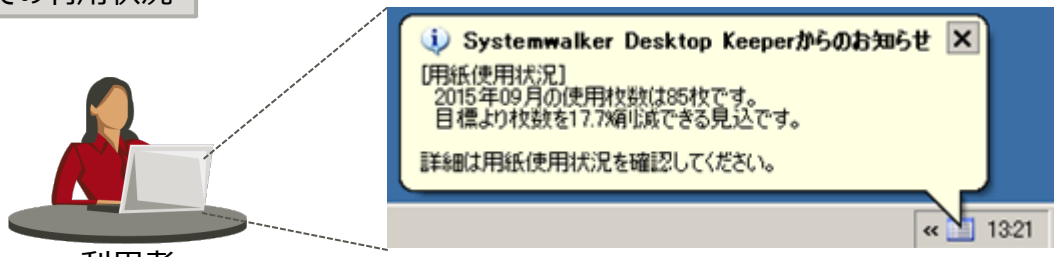
（※）連携可能な複合機/プリンタは、ソフトウェア説明書に記載のプリンタベンダーまでお問い合わせください。

用紙使用状況の通知(※1)(※2)

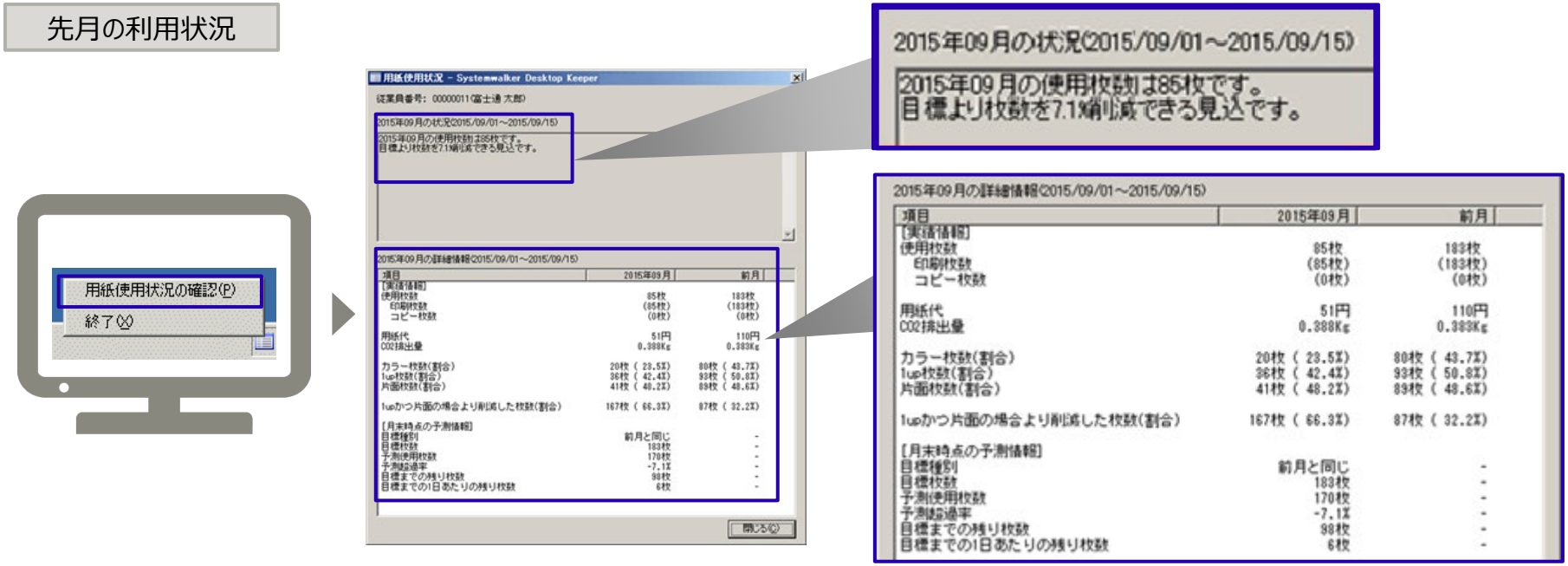
FUJITSU

- ログオン時に前日までの複合機/プリンタの利用状況を利用者へ通知します。
- 利用者は先月の紙の利用状況や目標の削減状況を把握できます。紙の削減に貢献します。

前日までの利用状況



先月の利用状況



（※1）画面上の用紙代やCO2排出量は、総使用枚数から係数を掛けて算出したもので、あくまで目安です。
（※2）連携可能な複合機/プリンタは、ソフトウェア説明書に記載のプリンタベンダーまでお問い合わせください。

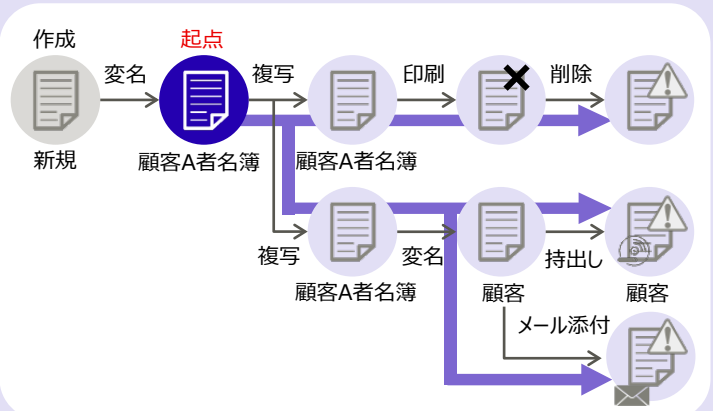
管理機能

- ファイル追跡機能
- ログフィルター機能
- バックアップした過去ログの閲覧
- 複数管理サーバの統合的なログ閲覧
- 利用者操作の追跡機能
- 部門管理機能
- デバイス/メディア登録用の部門管理者権限
- 自己版数管理機能
- ネットワークへの負荷低減
- 覗き見検知
- PC使用時間の把握
- Microsoft Teamsアプリ操作証跡管理
- 操作記録通知による利用者けん制
- 管理業務の一元管理/現地管理者での独自管理を両立

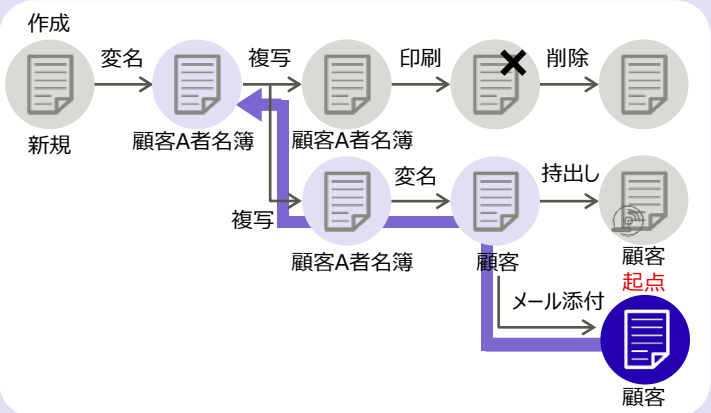
ファイル追跡機能

- ログビューアの検索結果から特定のファイルの操作履歴を追跡することができます。
  - バックトレース
    該当ファイルへの操作履歴（ファイル操作(参照、作成、更新、削除、複写、移動、変名）、ファイル持出し、FTPアップロード/ダウンロードファイルとWebアップロード/ダウンロードファイル）を過去に遡って検索できます。
  - フォワードトレース
    該当ファイルの操作履歴（ファイル操作(参照、作成、更新、削除、複写、移動、変名）、ファイル持出し、印刷、印刷禁止、メール送信、メール添付禁止、FTPアップロード/ダウンロードファイルとWebアップロード/ダウンロードファイル）を時系列にそって検索できます。
- 検索キーワードに、ドライブ種別(リムーバブル、リモート、CD/DVD、固定)を指定できます。

■ フォワードトレース
※追跡したいファイルのある時点を起点に、それ以降に行われた操作（コピー、変名）を調べる時に使用します。

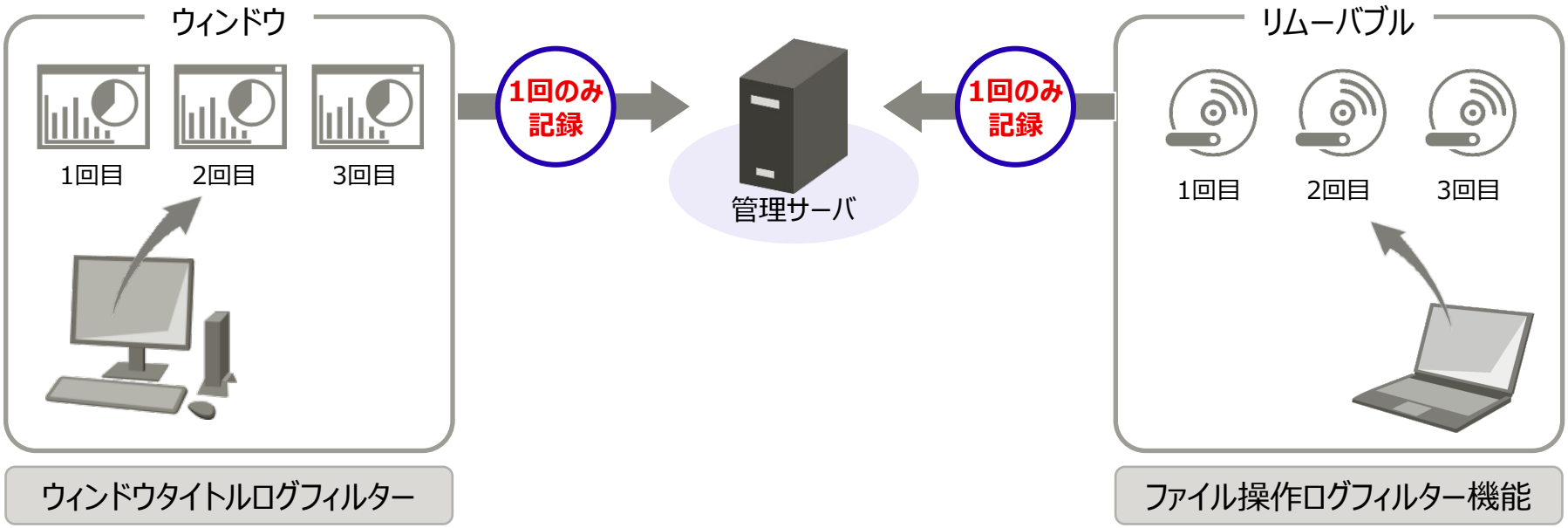


■ バックトレース
※追跡したいファイルのある時点を起点に、それ以前に行われた操作（コピー、変名）を調べる時に使用します。



ログフィルター機能

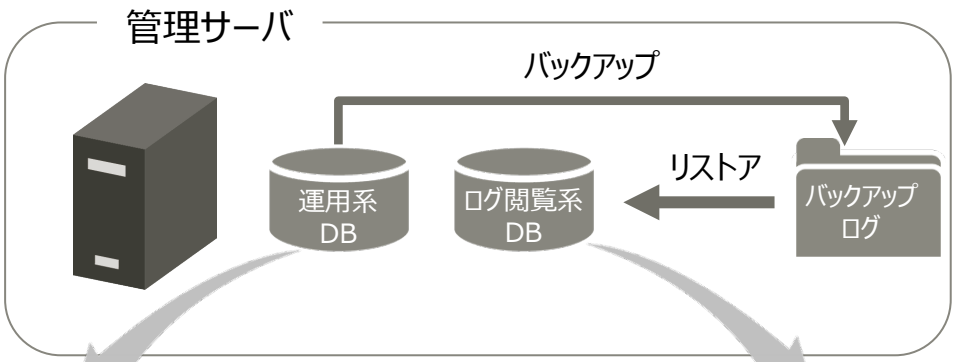
- ウィンドウタイトルログフィルター
  - 冗長なウィンドウタイトルログを取得しないようにできます。
    - 重複ログフィルター　：同じログが発生した場合にサプレスします。
    - キーワードフィルター：プロセス名,キーワードによりログの記録の要/不要を指定できます。
- ファイル操作ログフィルター機能
  - ドライブ種別（リモート、リムーバブル）によるログの記録の要/不要を指定できます。
    パソコン外へのファイル操作（情報漏えいに直結）に対してのみログを取得します。

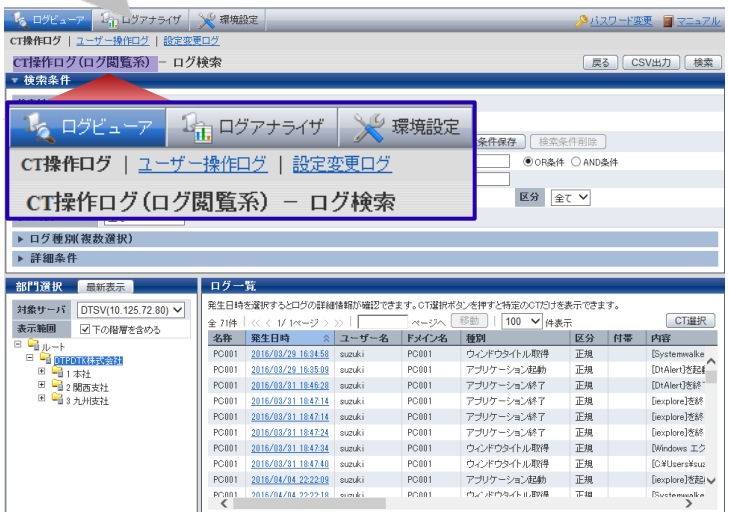


バックアップした過去ログの閲覧

FUJITSU

- 運用系データベースでバックアップした過去のログを閲覧用データベースにリストアすることにより、運用系システムを停止することなく、過去のバックアップログを参照できます。





複数管理サーバの統合的なログ閲覧

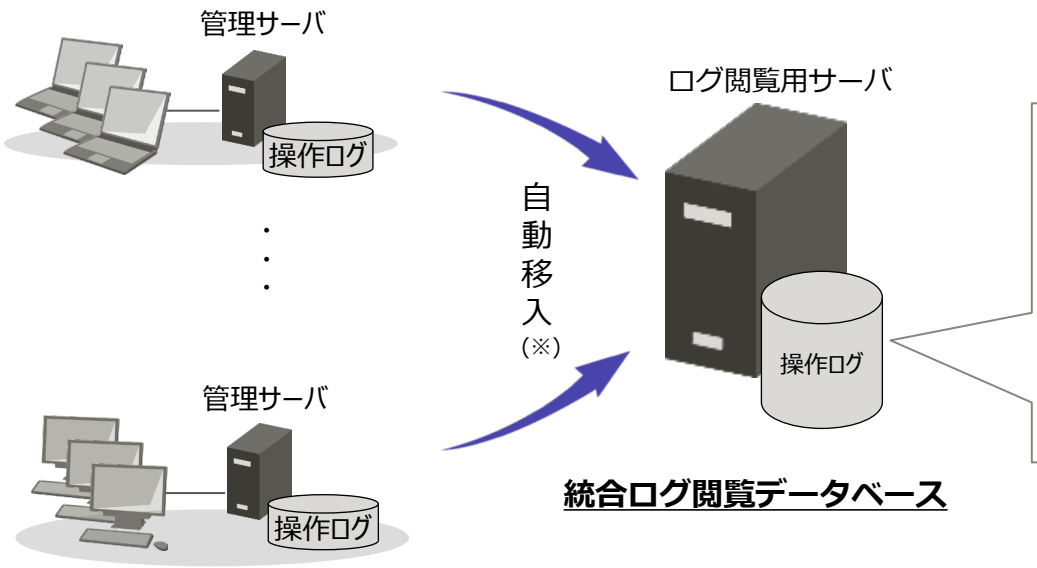
FUJITSU

■ 大規模環境向けに特化した大規模ログ閲覧用の高性能データベース対応により、
各管理サーバで実施していたログ閲覧運用を集約し、日々のログ閲覧運用を大幅改善しました。

富士通独自

収集された大量のログを動的に解析して
最適なデータ格納を実施、
これにより入力された検索期間を基にした
並列分散検索での高速化を実現
特許出願済

全管理サーバのログを横断検索



クライアント8000台の際の実測例

従来	改善後
各管理サーバで **28分**	1度の検索で **3分**

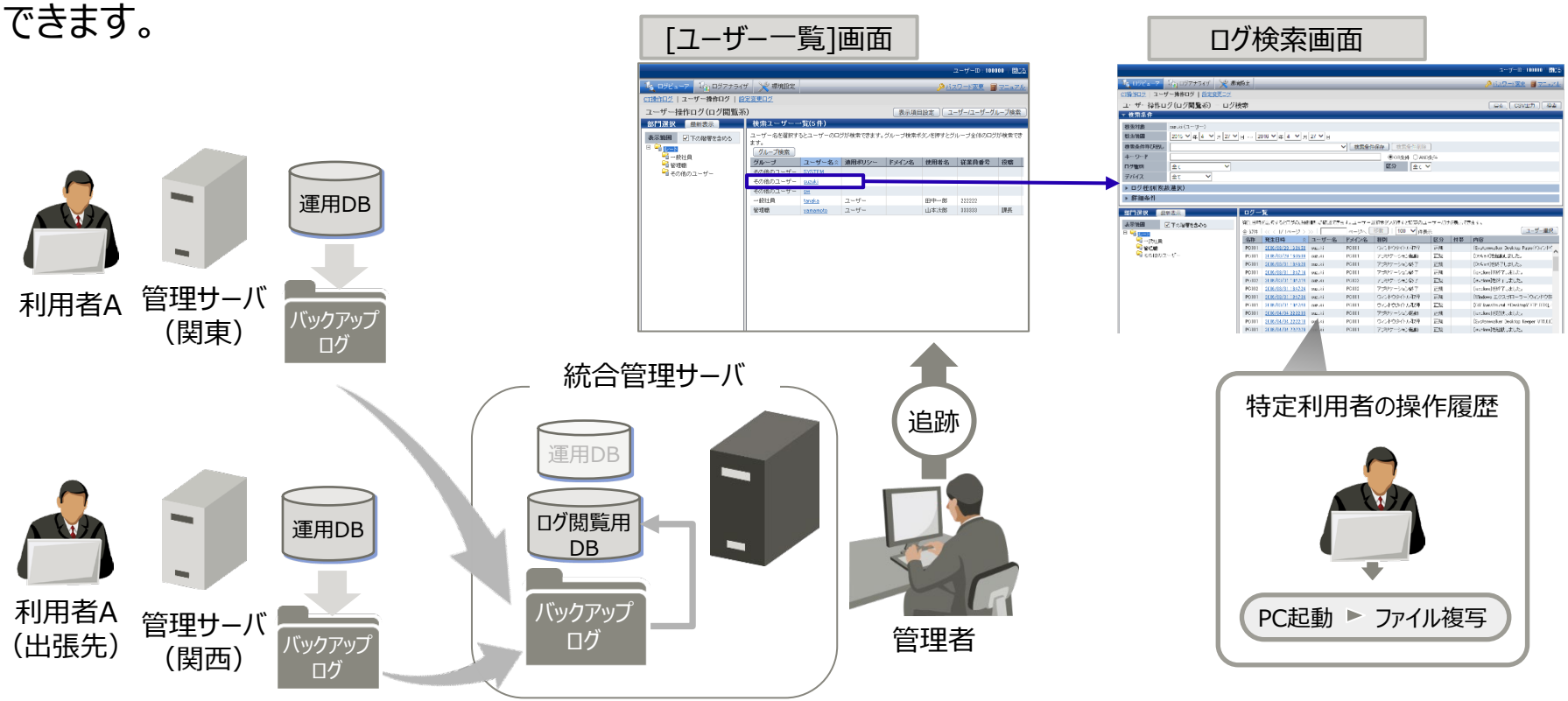
(※)管理サーバからのログの移出、および、ログ閲覧データベースへの移入コマンドを提供します。
管理サーバから出力したログをバッチファイル等でログ閲覧用サーバへコピーいただき、移入することで自動移入を実現します。

★★ポイント★★

複数台の管理サーバがあるような大規模のお客様向けに特殊チューニングをしたデータベースの提供に対応し数千～数万台のお客様であっても短時間で目的となるログの閲覧運用が可能になります。

利用者操作の追跡機能

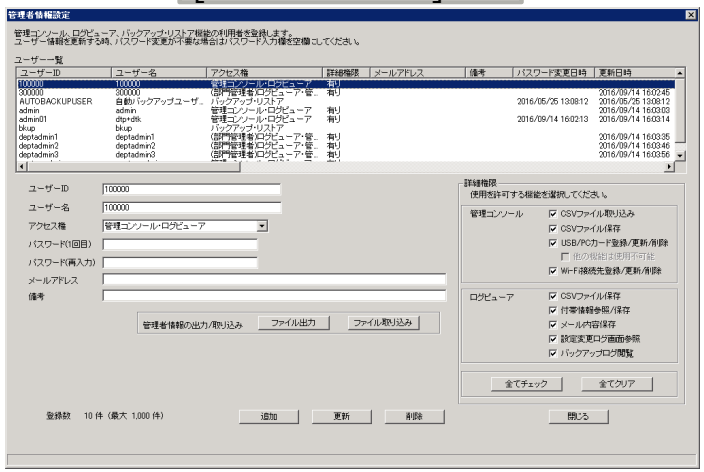
- ログ閲覧データベースにリストアしたバックアップデータから特定の利用者の操作を追跡できます。
  - バックアップデータから全ユーザのリストを自動作成できます。
  - ユーザーリストから、ユーザーを選択し、端末/管理サーバに依存せず横断的に操作を検索できます。
  - 検索したすべてのログ情報を時系列で参照できるので、利用者の操作内容をわかりやすく追跡できます。
- 検索条件(検索期間、キーワード、ログ種別、デバイス)の指定により、ログ情報を効率よく追跡できます。



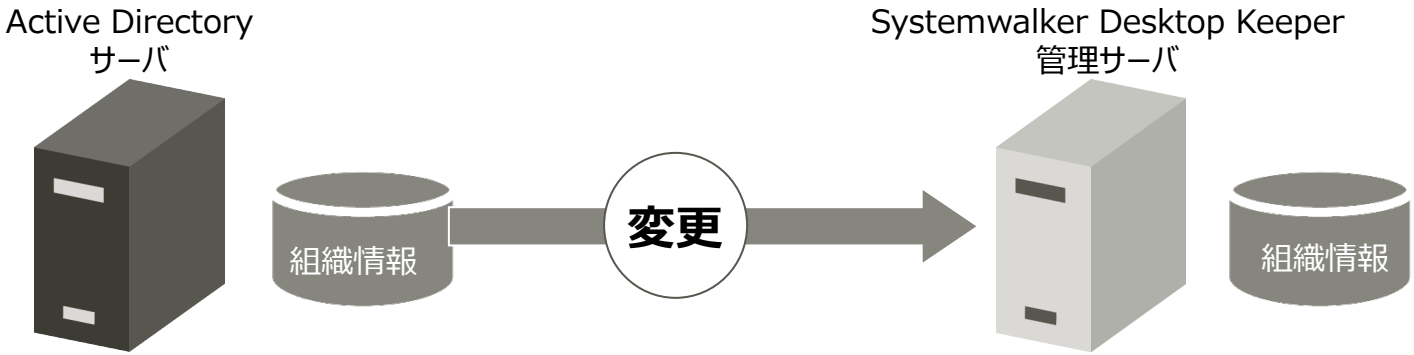
部門管理機能

- 部門ごとの管理者による各種設定管理により、部門統制環境の構築ができます。
  管理者権限は、システム全体の管理者と部門管理者の2段階で設定でき、それぞれの部門における運用状況、管理状況を全体管理者が監査することも可能です。

[管理者情報設定]画面

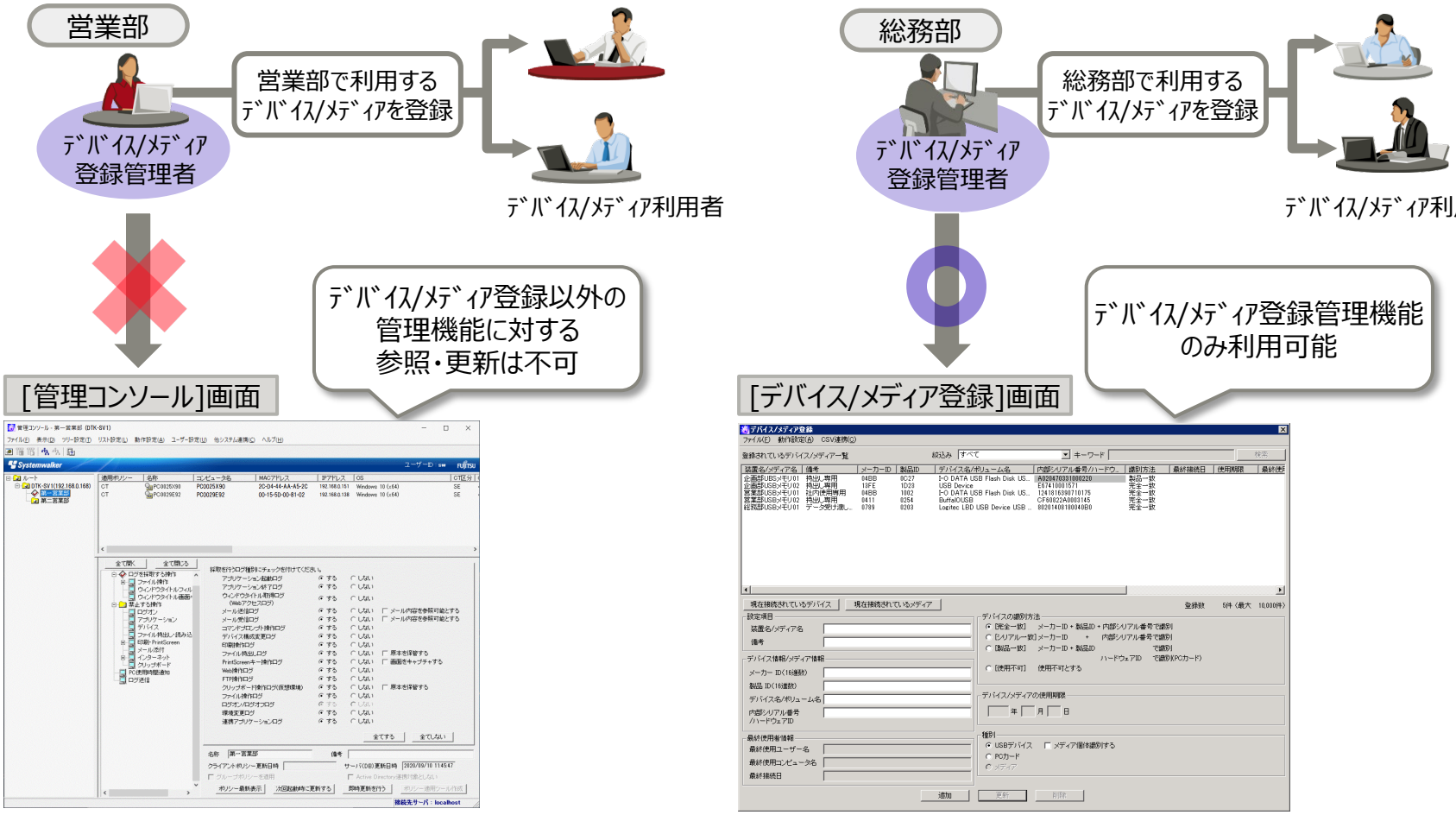


- Active Directoryの組織(OU)情報、ユーザー情報を自動で反映します。人事異動や組織変更にも迅速に対応できます。



デバイス/メディア登録用の部門管理者権限

- 利用可能なデバイス/メディアを登録できる管理者(デバイス/メディア登録管理者)の登録ができます。
- デバイス/メディアの登録作業を委譲することで管理者の負担が軽減します。
- デバイス/メディア登録管理者は他の機能を利用できません。



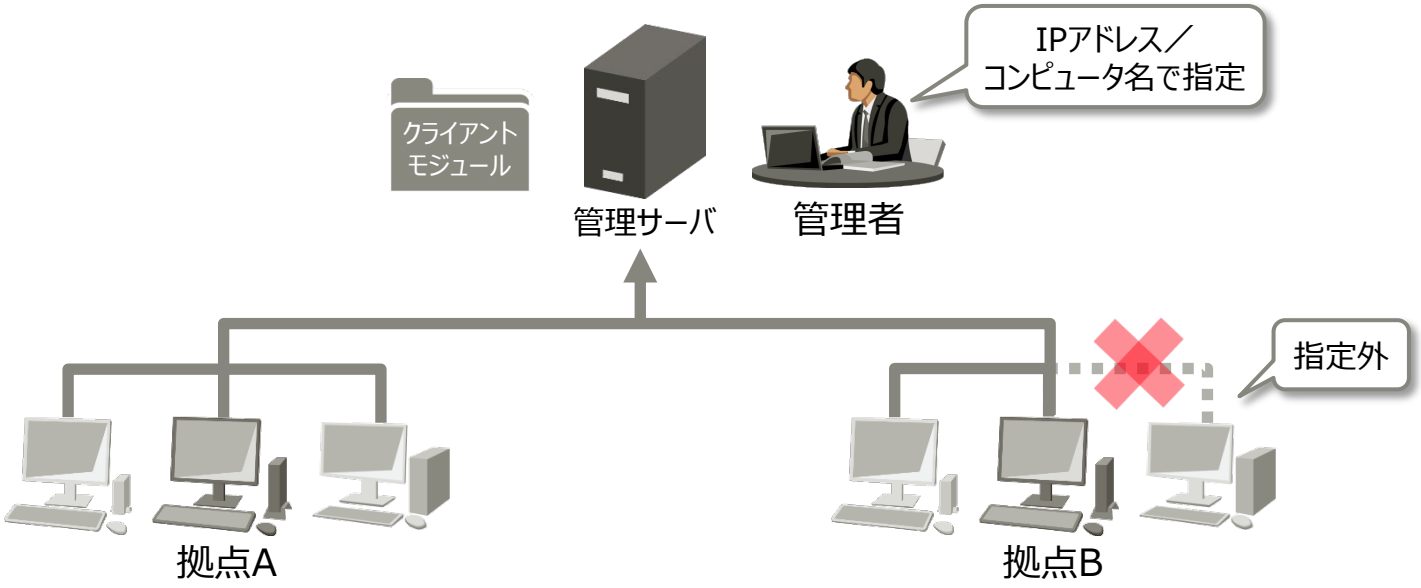
自己版数管理機能

FUJITSU

- 管理者が管理サーバにクライアントモジュールを登録するだけで、各クライアントは自動で最新の状態に更新されます。

版数チェックのタイミング	Windowsのログオン時
版数が異なる場合	クライアント側で、更新を「即時に行う」か「後から行う」かの選択が可能

- 全クライアント一斉に更新を実施せず、段階的に更新対象のクライアントを指定して更新することもできます。クライアントはIPアドレスまたはコンピュータ名で指定します。

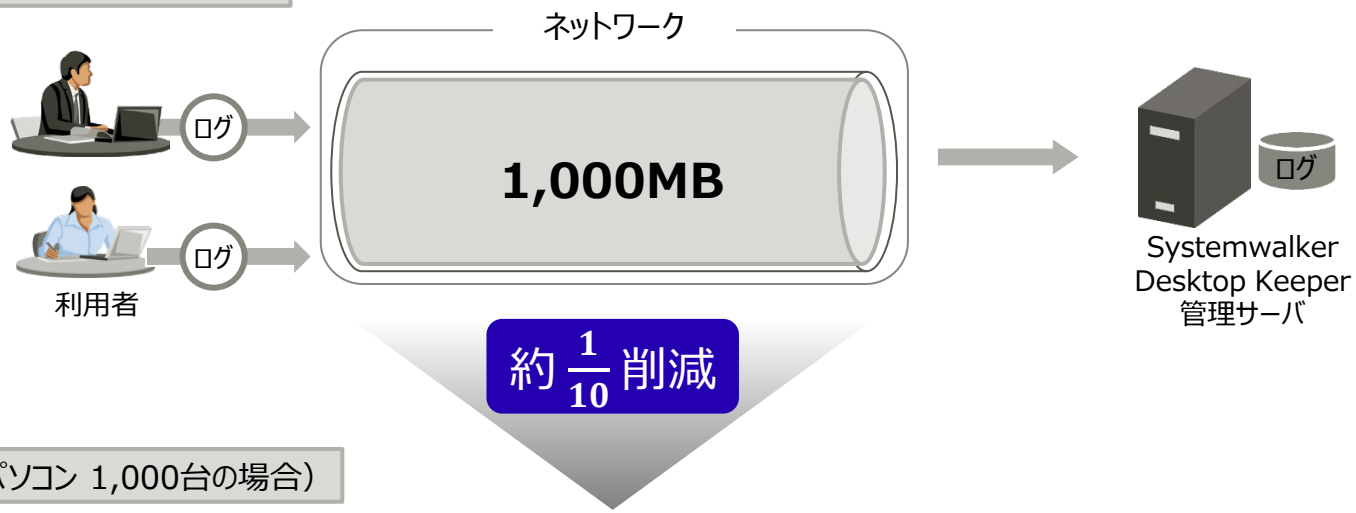


ネットワークへの負荷低減

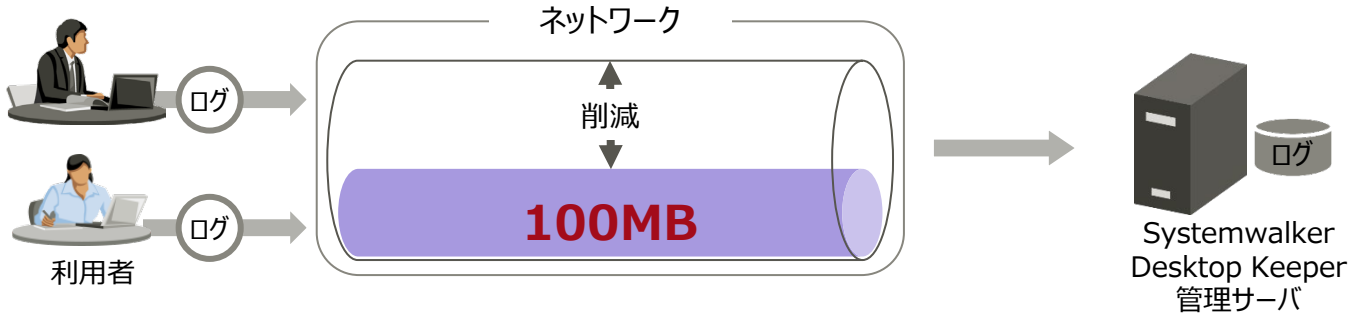
FUJITSU

■ 各パソコンと管理サーバ間のネットワークに流れるログを圧縮しました。これにより、業務で通信が多い環境や、帯域の狭いWANでもネットワークの負担を軽減します。

V14.2まで（パソコン 1,000台の場合）



V14.3以降（パソコン 1,000台の場合）

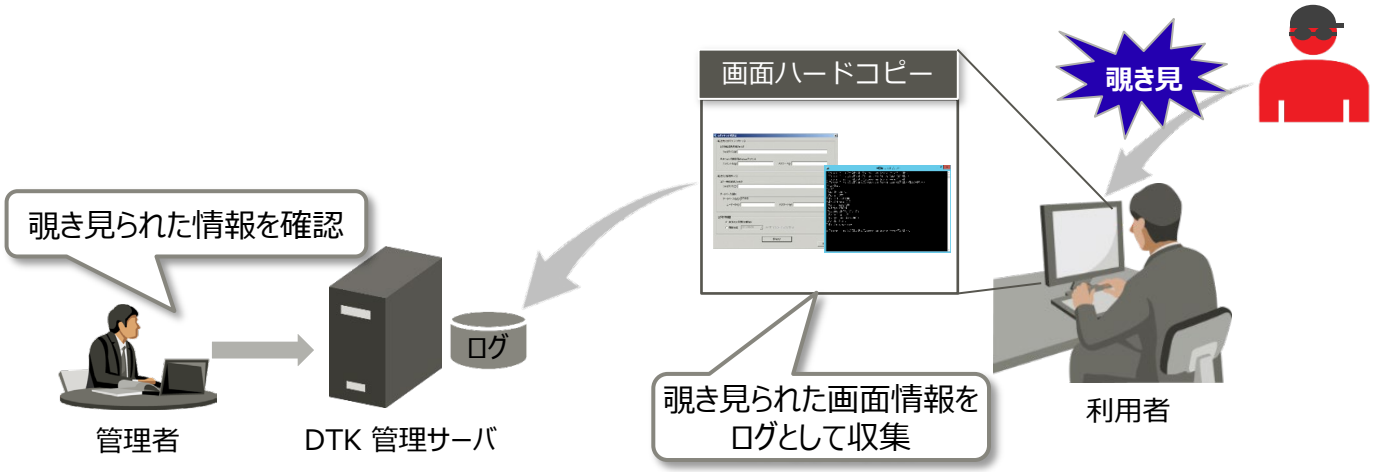


※1ログ(約1KB) ×1,000(ログ/日) = (1日1人あたり) 約1MB

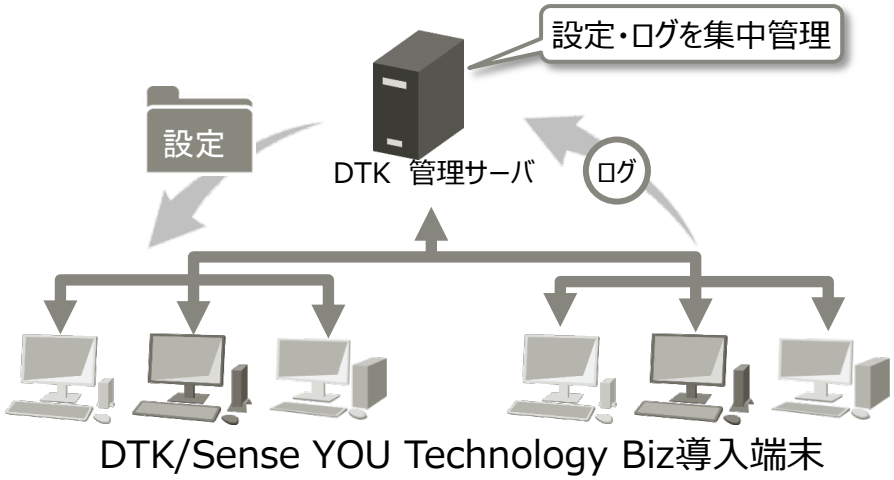
※ネットワーク上のログサイズを圧縮するもので、DBの容量を圧縮するものではありません。

覗き見検知

- Sense YOU Technology Bizと連携することで、覗き見検知時に、クライアント(CT)のデスクトップ画面のハードコピーをログとして取得できます。



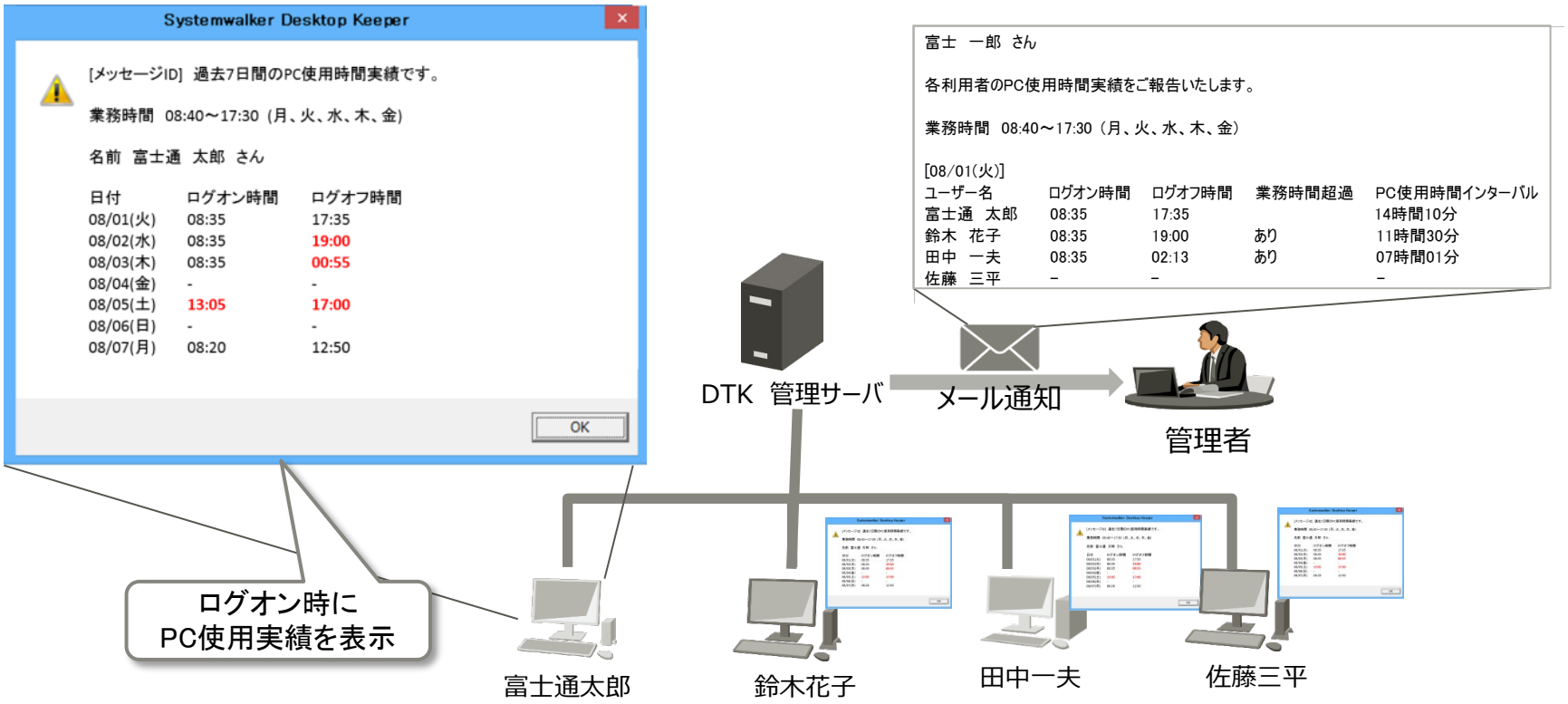
- Sense YOU Technology Bizの設定情報とログ情報をDTKで集中管理できます。



DTK:Systemwalker Desktop Keeper

PC使用時間の把握

- 利用者のPC使用時間を、管理者および利用者へ通知できます。
  - 各利用者のPC使用時間実績が、管理者にメール通知されます。
  - 利用者がクライアント(CT)にログオンした際に、PC使用実績が表示されます。

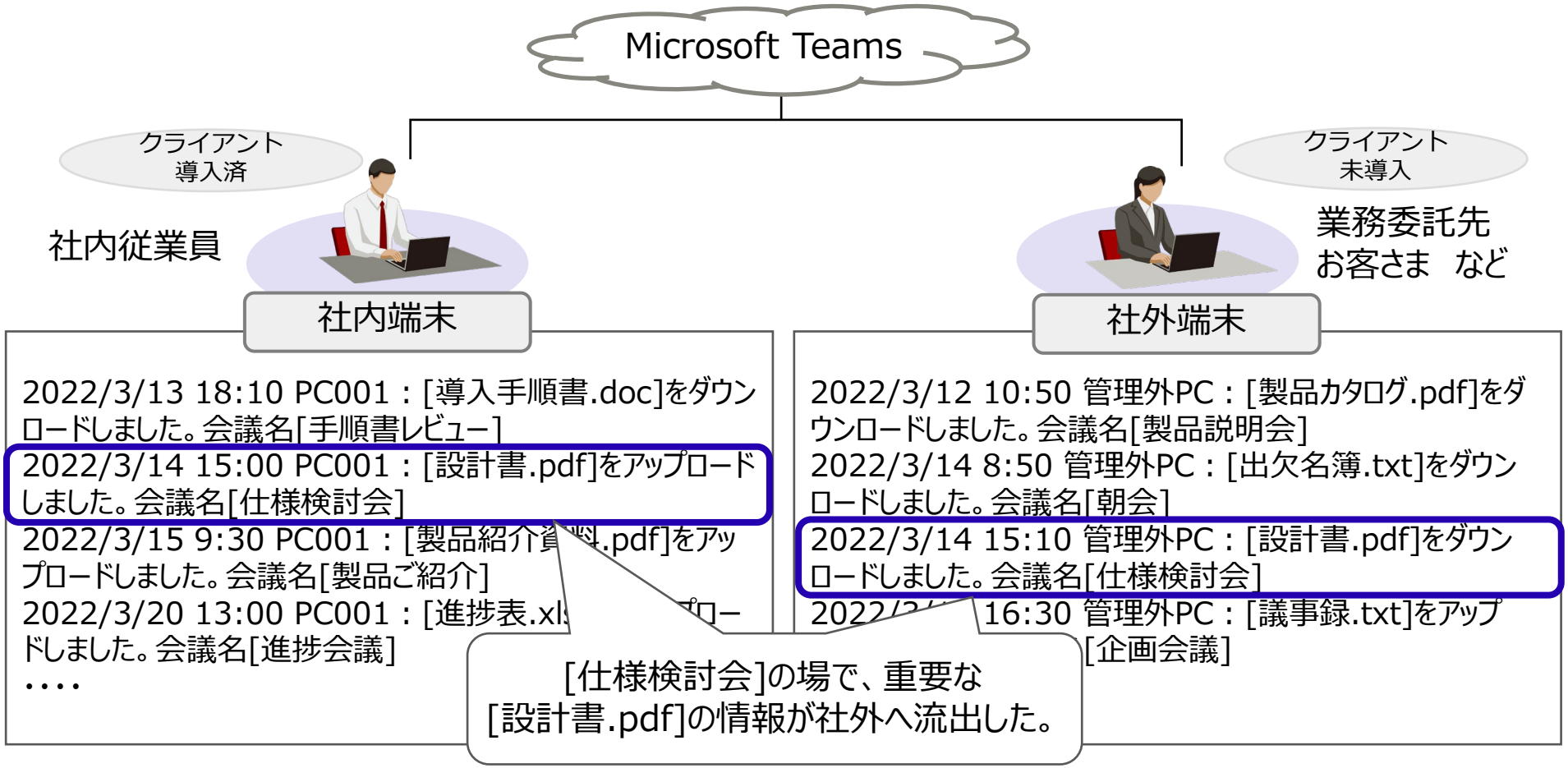


DTK:Systemwalker Desktop Keeper

Microsoft Teamsアプリ操作証跡管理

FUJITSU

■ Microsoft Teams上でのファイル操作（アップロード/ダウンロード）を記録し、社外への機密情報持出しの把握を支援します。(※)



社外の管理外端末を含めた、Teams上での操作記録を実現

(※)Webアップロード／Webダウンロードのログとして記録されます。

（補足）TeamsでのWeb操作ログについて

FUJITSU

本機能はクラウド上のMicrosoft 365管理センターで記録されているTeamsのユーザー使用履歴と、DTKが持つ端末情報を突合し、利用元端末の特定/社内社外端末を判定し記録することで漏洩時の追跡を一層強化するものです。

- Microsoft 365管理センターからのデータ取得に際し、管理サーバからインターネットへの通信許可、お客様が使用するテナント側の接続許可が必要になります。
- Teamsの使用履歴と端末の紐づけは、Teamsの利用IDと端末のログオンユーザーIDの一致で行います。このため、IDが一元管理されているMicrosoft Entra ID（旧称 Azure Active Directory）が導入されているお客様を前提とします。
- 上記でマッチしない端末（DTKクライアント未導入端末）を“管理外PC”という表記で社外PCであると判定します。

●●ログ表示例●●

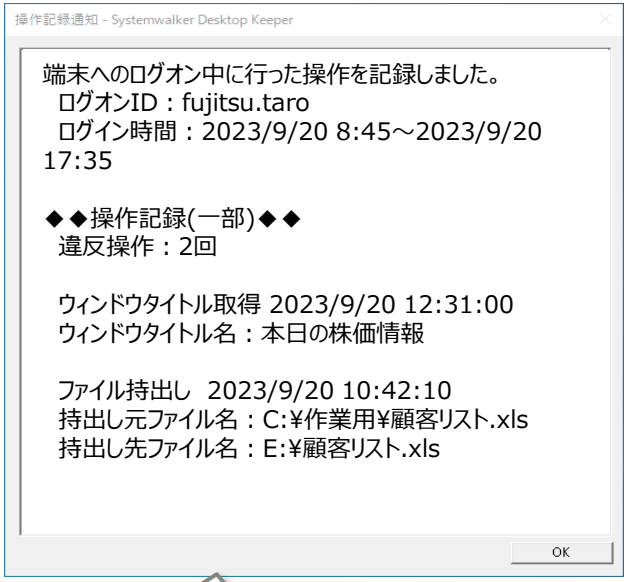
種別	内容	備考	固有情報の説明
Webアップロード	[https://xxxxx.sharepoint.com/sites/all/Shared Documents]へのアップロード操作が行われました。 アプリ名：[Microsoft Teams]、ファイル名：[製品紹介.pdf]	会議名： [製品説明会]	• アクセス先のURL文字列 • ファイル名 • Microsoft Teamsの会議名
Webダウンロード	[https://xxxxx.sharepoint.com/sites/all/Shared Documents]からダウンロード操作が行われました。 アプリ名：[Microsoft Teams]、ファイル名：[製品紹介.pdf]	会議名： [製品説明会]	

操作記録通知による利用者けん制

FUJITSU

■ ハイブリッドワークで作業場所が多岐に渡る中で、端末操作監視中であることを利用者に可視化し、セキュリティ意識の低下を防止します。

出社時（ログオン時）に記録の開始と、前回の操作記録実績を表示



Windowsログオン時に操作記録の開始を通知

前回のログオンからログオフの間に行われた代表的な操作のログを表示します

★★ポイント★★

テレワーク等、周囲に人がおらず意識が緩みがちな環境でも、監視警告による牽制を自動で行うことにより利用者のセキュリティ意識を保ちます。

管理業務の一元管理 /現地管理者での独自管理を両立

FUJITSU

■ 管理画面の拠点管理者に合わせた表示言語の自動切換えに対応し、国内/海外PCの一元管理機能を一層強化します。

日本語で表示

英語で表示

システムを一元管理しながら現地での独自管理を継続

(注)海外拠点で本商品のご利用に際しては、弊社営業までご相談ください。

補足：海外拠点でのご利用について

FUJITSU

海外拠点を持つ日本企業向けに、国内外端末の一元管理をしつつ一部運用を海外に移譲することを目的に、管理画面の言語切替を実現します。

[補足]

- 管理画面の言語は、ユーザが利用する言語によって、日本語/英語の切り替え(※1)
- クライアント端末の言語は、日本語/英語に対応
- 国内からの一元管理を想定し管理サーバの構築は、国内（日本語OS）のみサポート
- 国内運用部門が全体管理/現地指導をする想定で、出力するExcelレポート/マニュアルは日本語のみサポート

海外拠点(※2)での本商品の利用については、弊社営業までお問い合わせください。

※1 日本語の場合は日本語、その他言語の場合は英語で表示
※2 クライアント機能の展開に際しては一部現地国の法律に基づき暗号化機能を有した状態では出荷できないケースがあります。弊社営業までお問い合わせください。

セキュリティリスクへの対応

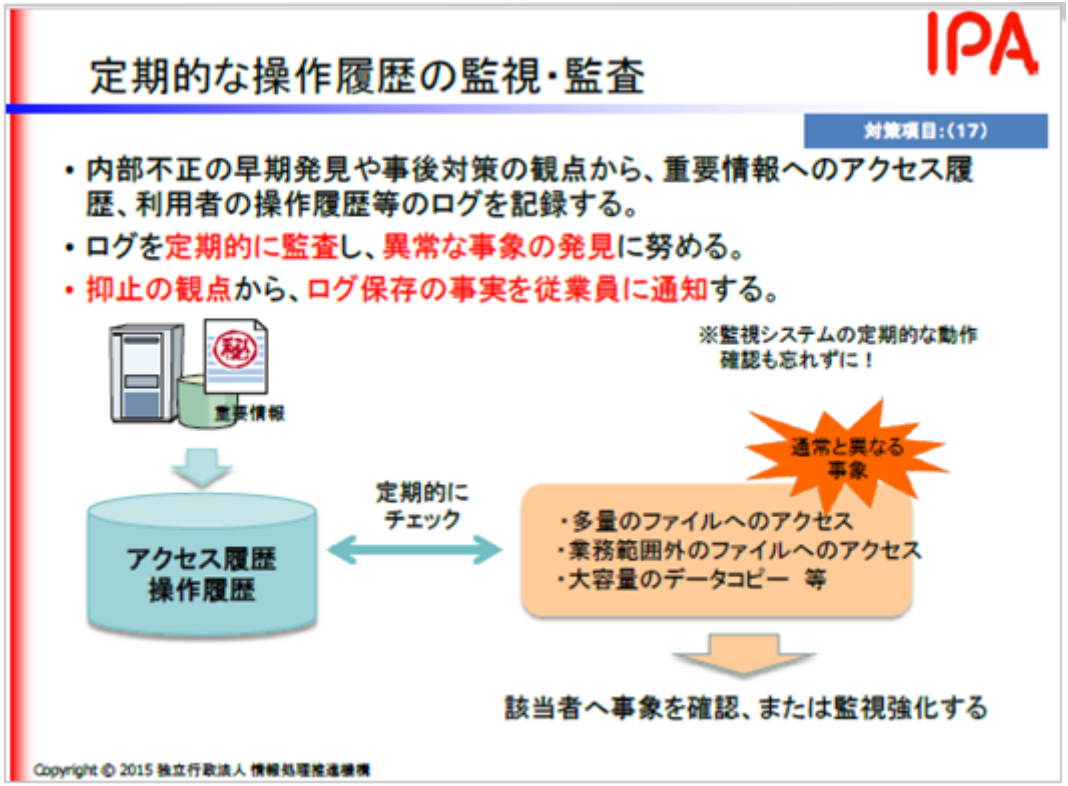
- 内部不正リスク検出
- 緊急対処

PC操作ログを活用した不正行動の発見

FUJITSU

- 不正な行動の発見は、ユーザーがPC上でどのような行動をしているか把握することが重要

- 蓄積されたPCの操作ログを活用した分析で行動を把握し不正な持ち出し行動を発見



出典：IPA「内部不正の現状とその対策～内部不正防止ガイドラインより有効な対策を探る～」

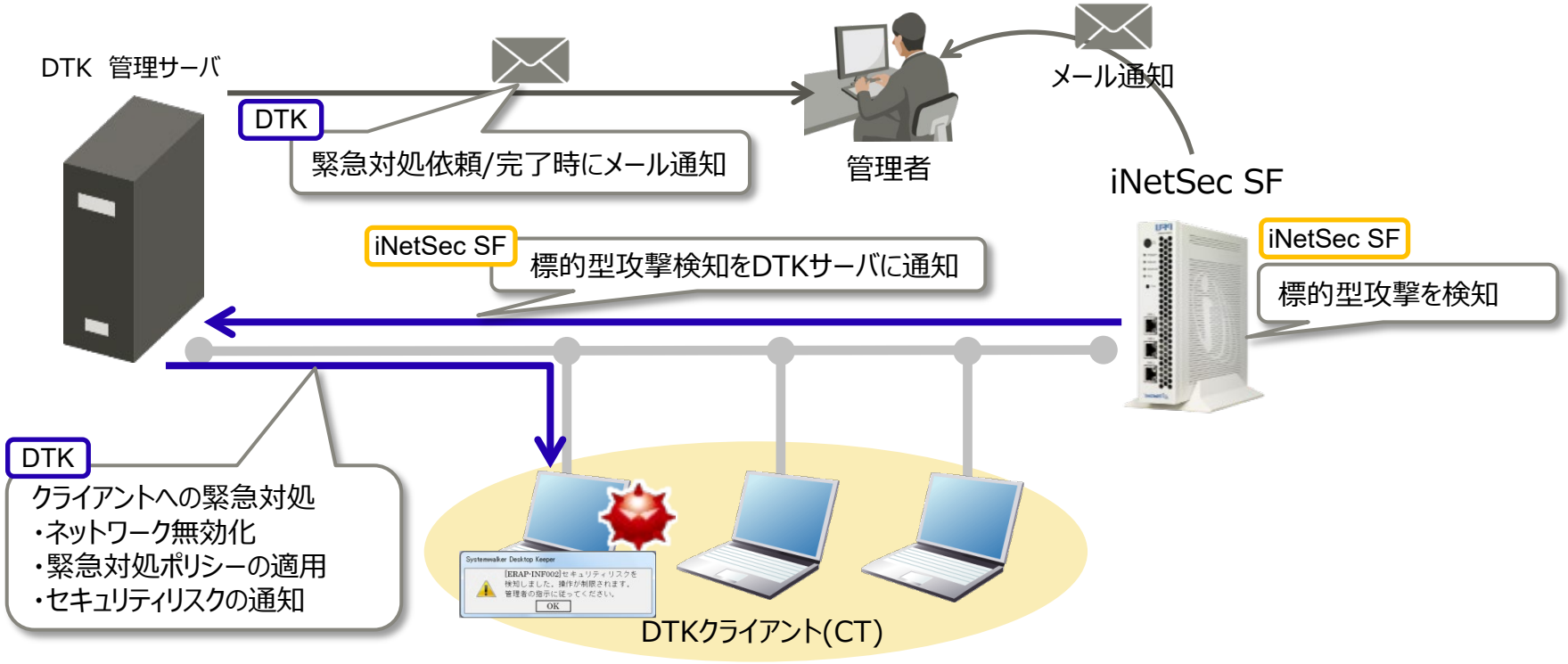
悩み 膨大なログの中から異常行動を見つけ出すのは困難

内部不正の防止に向け、お客様自身でPC操作ログを分析

緊急対処(iNetSec SFとの連携)

FUJITSU

- 管理者がセキュリティリスクの検知時に、クライアント(CT)への緊急対処(ネットワークの無効化、緊急対処ポリシーの適用、セキュリティリスクの通知)ができるようになります。
- iNetSec SFと連携している場合は、iNetSec SFがマルウェアを自動で検知し、ネットワークを遮断します。クライアント(CT)への緊急対処を行うことで、セキュリティリスクへの早期対処と被害拡大防止を行うことができるようになります。



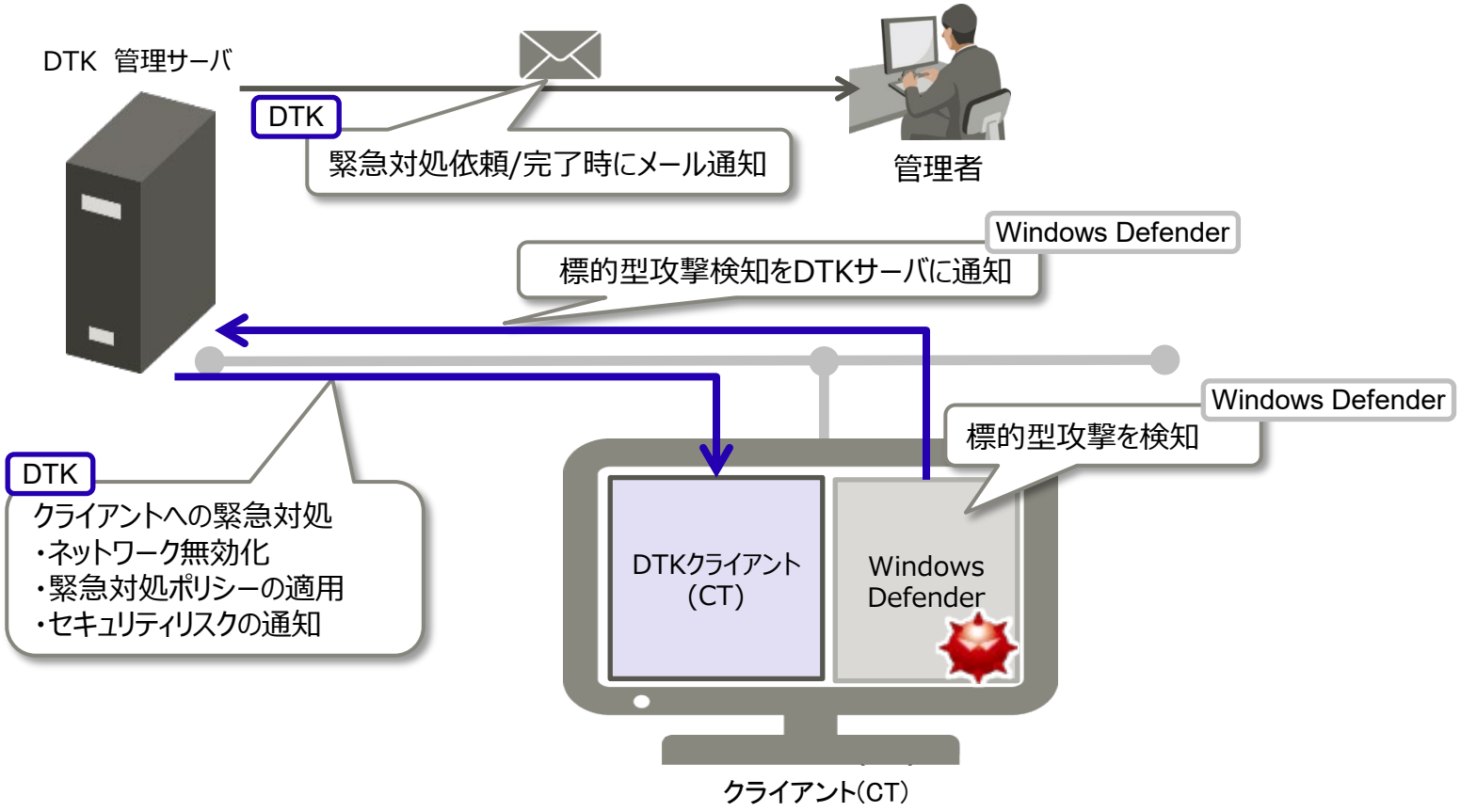
（※）上記以外の検知製品との連携については、弊社営業までお問い合わせください。

DTK:Systemwalker Desktop Keeper

緊急対処(Windows Defenderとの連携)

FUJITSU

- Window Defenderとの連携により、Windows Defenderがマルウェアを検知すると、クライアント(CT)への緊急対処(緊急対処設定ポリシーの適用)が行われます。さらに、管理者による判断で緊急対処(ネットワーク無効化)することで、セキュリティリスクへの早期対処と被害の拡大を防止できます。



DTK:Systemwalker Desktop Keeper

Systemwalker Desktop Patrolとの連携

- 製品特長
- Systemwalker Desktop Patrolの構成自動取込み
- Systemwalker Desktop Patrol連携

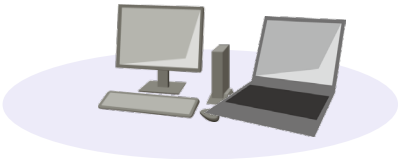
製品特長

FUJITSU

“ＩＣＴ資産の統合管理”と”セキュリティおよび省電力対策”を実現

ICT資産管理

- ICT資産を自動検知し台帳管理。
- ソフトウェア導入状況や利用状況を把握。



セキュリティ統制

- セキュリティパッチの適用状況を把握。
- 最新のセキュリティパッチを自動的に適用。

レポート機能

- 対策状況の把握、リスクのある部門やパソコンを把握。

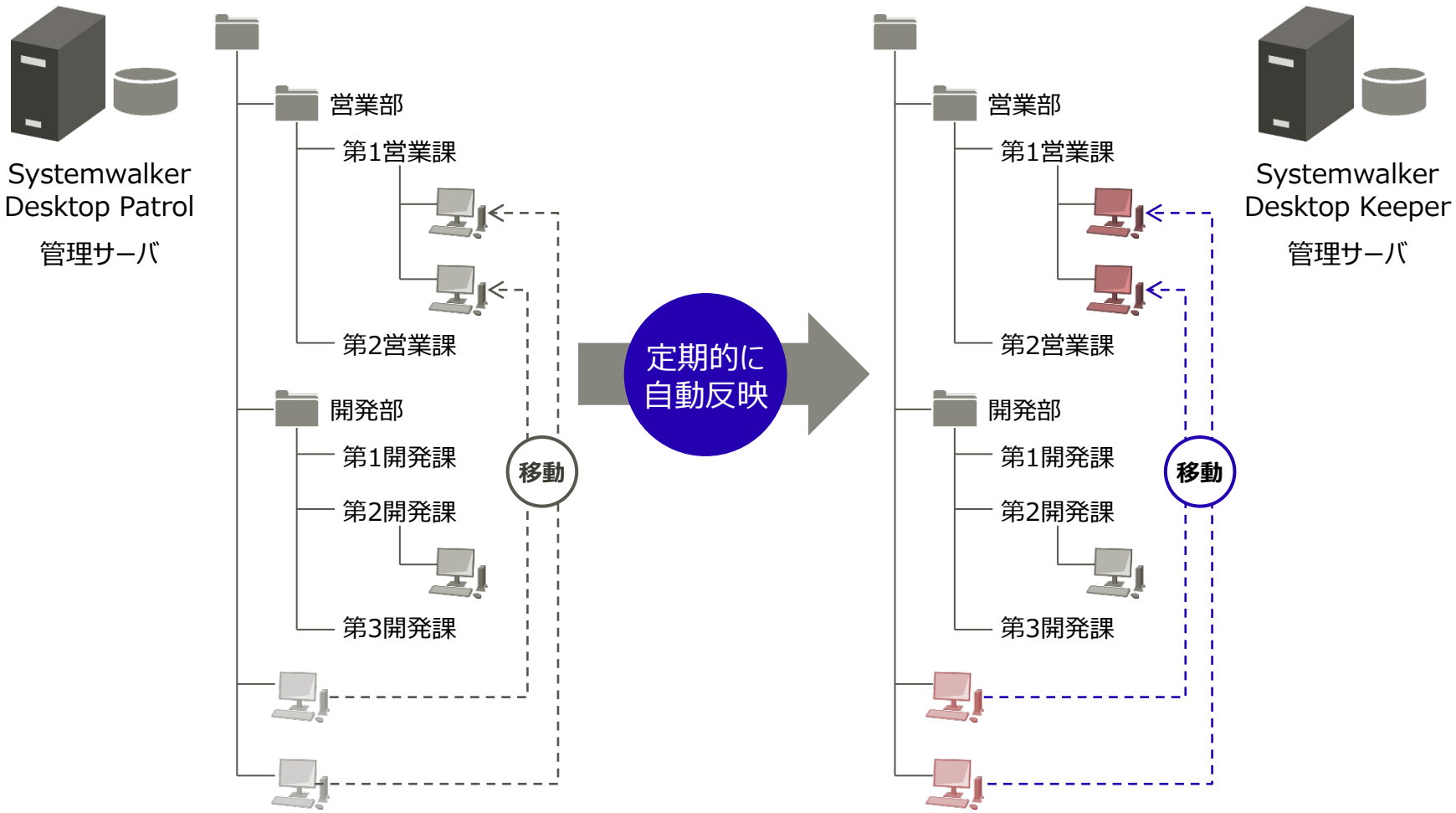
廃棄パソコンのデータ消去と管理

- データ消去ツールにより、ハードディスクの情報を完全消去。
- 廃棄の計画をもとに情報消去までの進捗を管理。

Systemwalker Desktop Patrolの構成自動取込み

FUJITSU

- Systemwalker Desktop Patrolの組織情報を定期的に自動で取り込みます。
- 人事異動が発生しても組織情報のメンテナンス作業を減らせます。



Systemwalker Desktop Patrol連携①

FUJITSU

■ 問題操作の発生状況の把握に加え、Systemwalker Desktop Patrolと連携することで問題のある社内資産の有無を一画面で把握できます。

Systemwalker Desktop Patrolの運用状況	Systemwalker Desktop Keeperの運用状況

Systemwalker Desktop Patrol連携②

FUJITSU

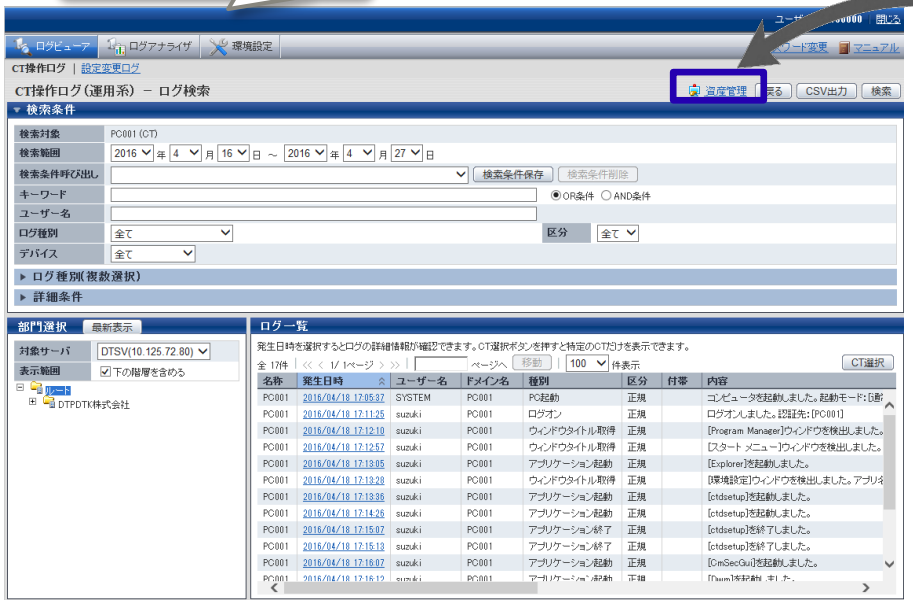
- Systemwalker Desktop Patrol との連携により、利用者の操作ログを参照した後、そのパソコンの資産情報を１クリックで参照できます。

Systemwalker Desktop Keeper

Systemwalker Desktop Patrol

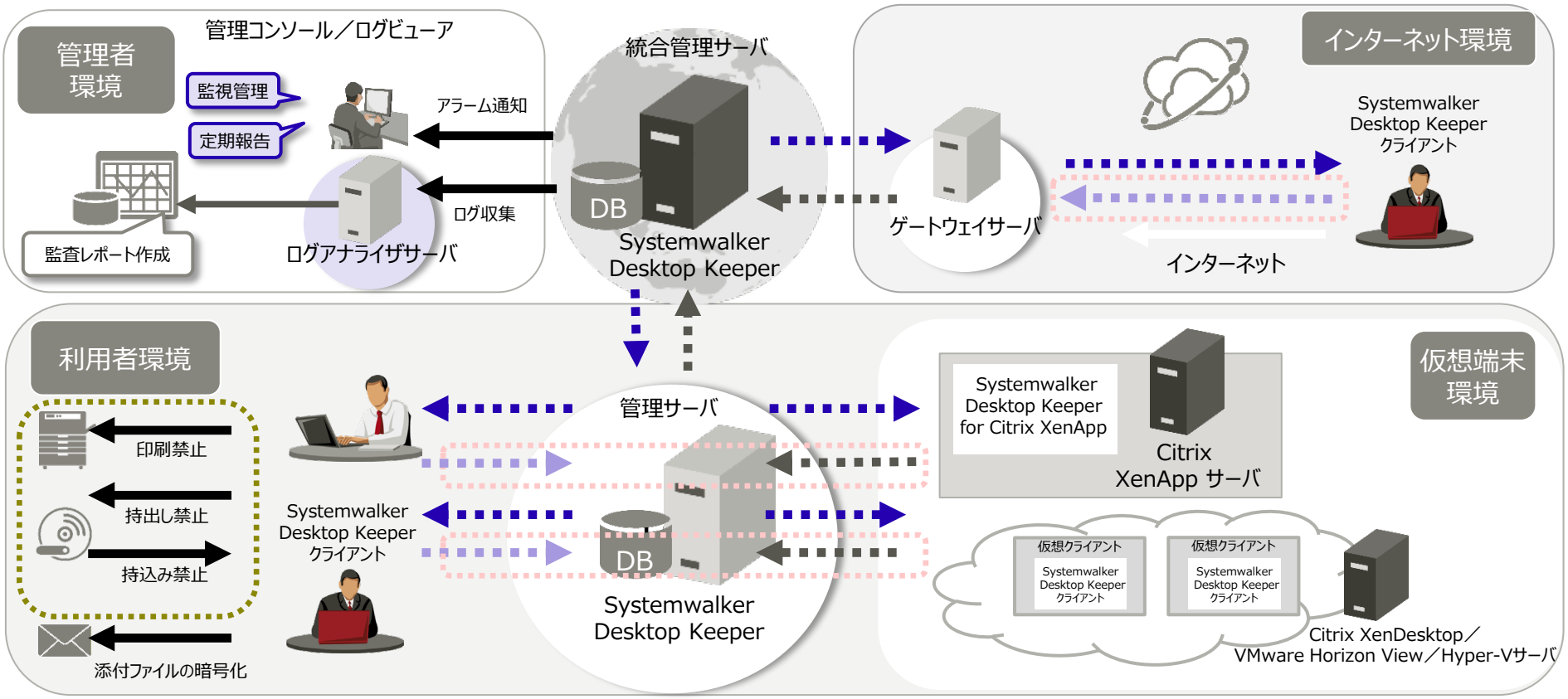
操作ログ検索

相互参照



パソコンの資産情報

機能イメージ図



補足）日本国内のみならず、海外拠点も含め1つの管理サーバで、多言語環境のパソコンを管理できます。

★管理者環境について★

ログビューア	ログの検索や参照を行うWebコンソールです。
ログアナライザ	ログの集計・分析結果を参照するWebコンソールです。

★システム構成★

管理サーバ	パソコンの操作記録を収集し、ログやポリシーを管理するサーバです
統合管理サーバ	管理サーバ機能に加え、複数の管理サーバに対し、ユーザーポリシーの一元管理を行うことができる管理サーバです。
ゲートウェイサーバ	パソコンの操作記録を収集し、(統合）サーバへ転送します。
Citrix XenApp サーバ	Citrix XenApp のクライアント（仮想端末）の操作ログを収集し、管理サーバへ転送します。
Citrix Xen Desktop/VMWare View/Microsoft Hyper-Vサーバ	仮想クライアントを構成するサーバです。Systemwalker Desktop Keeperクライアントは各仮想クライアントに導入します。

動作環境①

	統合管理サーバ/ 管理サーバ/ ログアナライザサーバ/ 中継サーバ	Citrix Presentation Server監視機能/ Citrix XenApp監視機能	レポート出力ツール
対 応 O S	Windows Server 2016 DC/SE/ES Windows Server 2019 DC/SE/ES Windows Server 2022 DC/SE/ES	Windows Server 2016 DC/SE/ES Windows Server 2019 DC/SE/ES Windows Server 2022 DC/SE/ES	Windows 10 Pro/Enterprise/Education Windows 11 Pro/Enterprise/Education
必須・関連ソフトウェア	[関連ソフトウェア] Systemwalker Desktop Patrol	[必須ソフトウェア] VMware Horizon RDSH 7.13 ESB、8 2006～8 2306	[必須ソフトウェア] Microsoft Excel 2016 以降 Excel for Microsoft 365 (旧Office 365)
仮想環境	VMware vSphere 7.0～8.0 Microsoft Hyper-V KVM		

※SEは「Standard Edition」、EEは「Enterprise Edition」、FEは「Foundation Edition」、DCは「DataCenter」、 ESは「ESsentials」、Busは「Business」、Entは「Enterprise」、Ultは「Ultimate」、SPは「Service Pack」の略称です。
※x64 Editionを使用する際の注意事項
32ビット互換モードで動作します。
※Windows Serverを使用する際の注意事項
Server Coreは使用できません。
※Windows Server 2016以降を使用する際の注意事項
Nano Serverは使用できません。
※本製品は、次のいずれの環境においても動作します。(IPv4のみの環境、IPv4/v6混在環境、IPv6のみの環境(*1))
*1) IPv4をアンインストール(netsh interface ipv4 uninstallを実行)しないでください。
※レポート出力ツールはMicrosoft Excel 2016の場合、32bit版のみ動作します。

動作環境②

	管理コンソール	クライアント(CT)
対 応 O S	Windows Server 2016 DC/SE/ES Windows Server 2019 DC/SE/ES Windows Server 2022 DC/SE/ES Windows 10 Pro/Enterprise/Education Windows 10 IoT Enterprise LTSC Windows 11 Pro/Enterprise/Education	Windows 10 Home/Pro/Enterprise/Education Windows 10 IoT Enterprise LTSC Windows 11 Home/Pro/Enterprise/Education Windows Server 2016 DC/SE/ES Windows Server 2019 DC/SE/ES Windows Server 2022 DC/SE/ES
必須・関連ソフトウェア	[必須ソフトウェア(ログビューアのみ)] Microsoft Internet Explorer 11 Microsoft Edge™ [関連ソフトウェア] Systemwalker Desktop Patrol	[関連ソフトウェア] Systemwalker Desktop Patrol
仮想環境		VMware vSphere 7.0～8.0 VMware Horizon 7.13 ESB、8 2006～8 2306 Citrix XenDesktop 7.15LTSR、7.6 LTSR Citrix Virtual Apps and Desktops 1912 LTSR、2103～2112 Microsoft Hyper-V

※SEは「Standard Edition」、EEは「Enterprise Edition」、FEは「Foundation Edition」、DCは「DataCenter」、 ESは「ESsentials」、Busは「Business」、Entは「Enterprise」、Ultは「Ultimate」、SPは「Service Pack」の略称です。
※x64 Editionを使用する際の注意事項
32ビット互換モードで動作します。
※Windows Serverを使用する際の注意事項
Server Coreは使用できません。
※Windows Server 2016以降を使用する際の注意事項
Nano Serverは使用できません。
※Windows 10、Windows Server 2016以降のWindowsストアアプリを使用する際の注意事項
クライアント(CT)の以下の記録機能あるいは禁止機能は動作しません。
[記録機能]
・Webアップロードログ
・FTP操作 (アップロード、ダウンロード)
・クリップボード操作ログ
・印刷枚数カウント
[禁止機能]
・FTPサーバ接続禁止
・Webアップロード禁止
・クリップボード操作禁止
※本製品は、次のいずれの環境においても動作します。(IPv4のみの環境、IPv4/v6混在環境、IPv6のみの環境(*1))
*1) IPv4をアンインストール(netsh interface ipv4 uninstallを実行)しないでください。

登録商標

- Microsoft、Windows、Windows NT、Windows Vista、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。
- Citrix、Xen、Citrix XenApp、Citrix XenServer、Citrix XenDesktop、Citrix Virtual Apps and DesktopsおよびCitrix Presentation Serverは、Citrix Systems, Inc.の米国またはその他の国における登録商標または商標です。
- VMwareは、VMware,Inc.の米国及びその他の国における登録商標または商標です。
- 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。
- 会社名、製品名等の固有名詞は各社の商号、商標または登録商標です。
- その他、本資料に記載されている会社名、システム名、製品名等には必ずしも商標表示(TM・®) を付記しておりません。

Thank you