Fujitsu Software Systemwalker Desktop Keeper V16 ご紹介

2024年1月

富士通株式会社

目次

FUJITSU

- 製品ご紹介
  - Systemwalker Desktop Keeper とは
- 操作ログの収集(閲覧／追跡)
  - 操作ログ収集の流れ
  - ログの収集
  - ログの管理（操作の追跡）
  - ログの管理（ファイルの原本保管）
- 操作の禁止運用
  - 操作禁止の流れ
  - 操作の禁止
  - 操作の禁止（非暗号化ファイルのメール送信）
  - 操作の禁止（USBデバイスの使用許可）
- レポート機能
  - レポート出力
- 製品情報
  - 事例（参考）
  - 登録商標

© 2024 Fujitsu Limited

製品ご紹介

■ Systemwalker Desktop Keeper とは

© 2024 Fujitsu Limited

Systemwalker Desktop Keeper とは

FUJITSU

■操作ログの収集(閲覧／追跡)と操作禁止の重要性

社内にあるPCから業務とは関係ないファイルへのアクセスや、機密情報のプリンターへの印刷、USBメモリへのコピーなどの操作の記録だけでは、情報の流出を防ぐことはできません。

情報漏えいのリスクを低くするために、印刷やコピーを禁止すると、業務に支障をきたす場合があります。

機密情報を守る上で、PCに対する情報漏えい対策に加え、業務利用が広がった仮想デスクトップへの対策も重要になります。

■Systemwalker Desktop Keeperが解決できること！

操作ログの収集 (閲覧／追跡)	PCにおける操作、またはプリンターやUSBメモリなどを使用した操作を記録し、問題が発生した後でも、手早く対処できます。
操作禁止	全社や部門に適したセキュリティポリシーを決め、業務上、必要ではない操作は禁止します。必要に応じて、ファイルを暗号化するなどリスクを低減できます。
レポート機能	組織内のセキュリティ状況の診断結果や組織内部のコンプライアンス状況を、レポートとして印刷やファイル出力できます。

© 2024 Fujitsu Limited

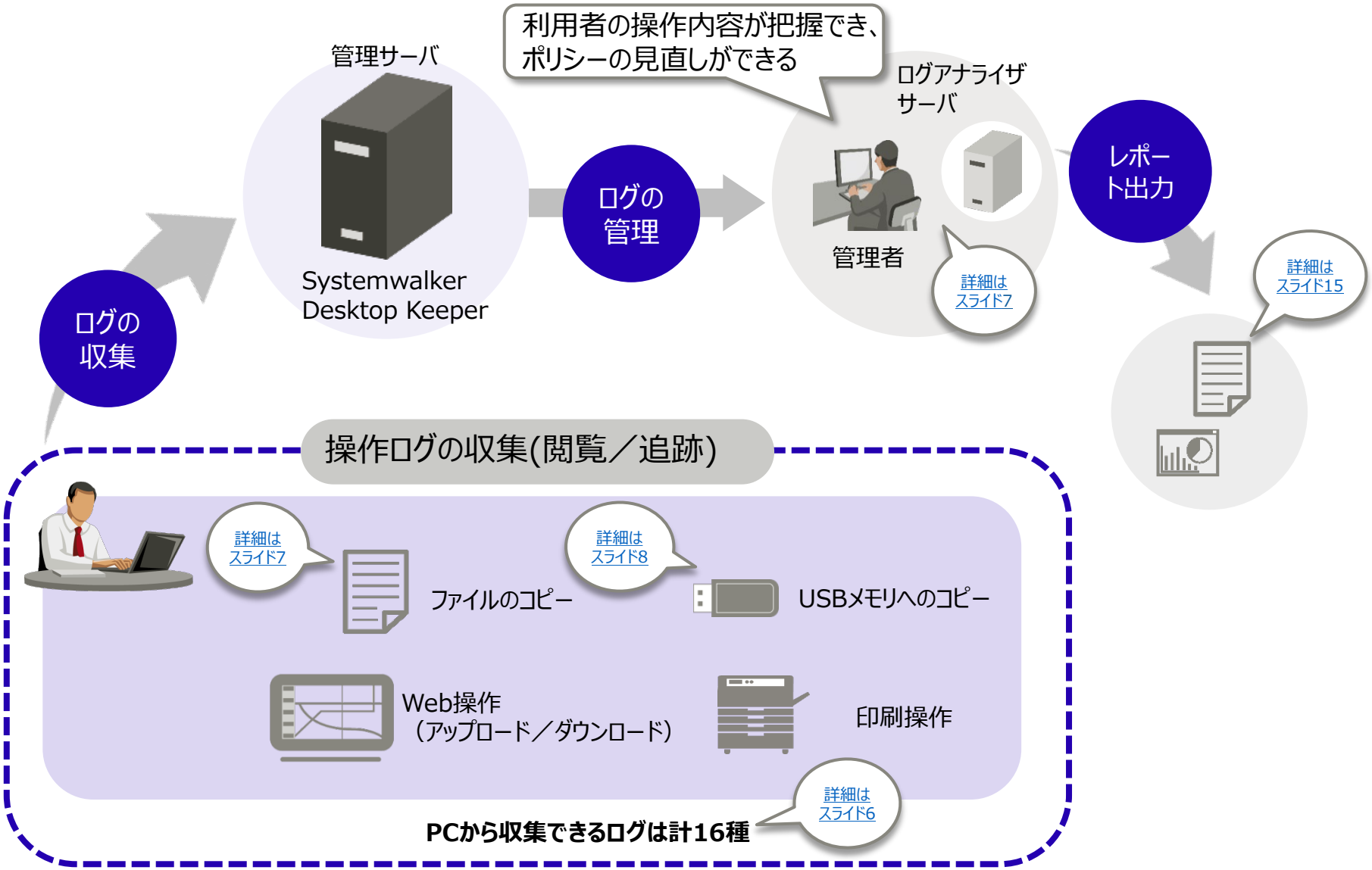
操作ログの収集(閲覧／追跡)

- 操作ログ収集の流れ
- ログの収集
- ログの管理（操作の追跡）
- ログの管理（ファイルの原本保管）

© 2024 Fujitsu Limited

操作ログ収集の流れ

FUJITSU

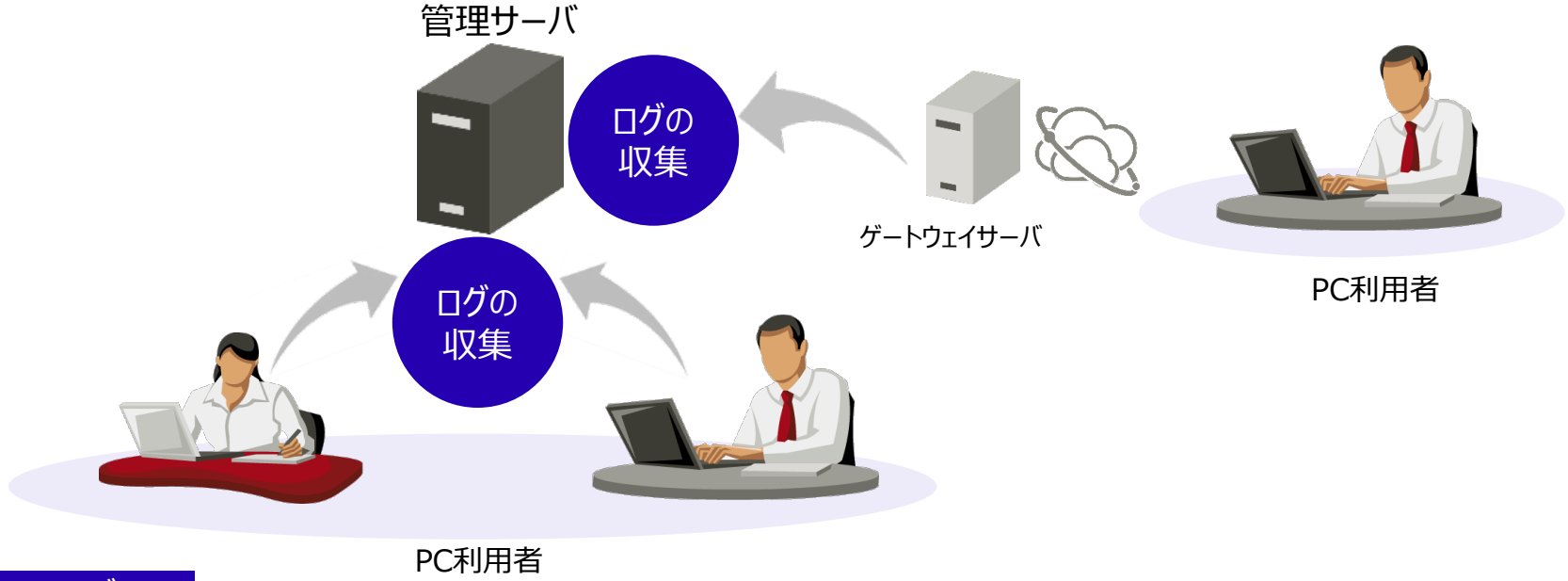


© 2024 Fujitsu Limited

ログの収集

FUJITSU

■ 利用者単位でのPCの操作記録を一元的に管理できます。



PCから収集するログ※1

- アプリケーション起動／終了
- ウィンドウタイトル収集
  （Webアクセスログ）
- メール送信
- メール受信
- コマンドプロンプト操作
- デバイス構成変更
- 印刷操作
- ファイル持出し
- PrintScreenキー操作
- Web操作（アップロード／ダウンロード）
- クリップボード操作 ※2
- FTPサーバ操作
  （アップロード／ダウンロード）
- ファイル操作
- ログオン／ログオフ ※3
- 環境変更ログ
- 連携アプリケーションログ

計：16種類

※1 仮想環境では収集できないログもあります。詳細は機能ご紹介資料をご参照ください。

※2 仮想PC(Citrix XenDesktop／VMware View)とPC間のクリップボード経由でのコピー操作のログを収集

※3 PCの電源ON／OFFのログも合わせて収集

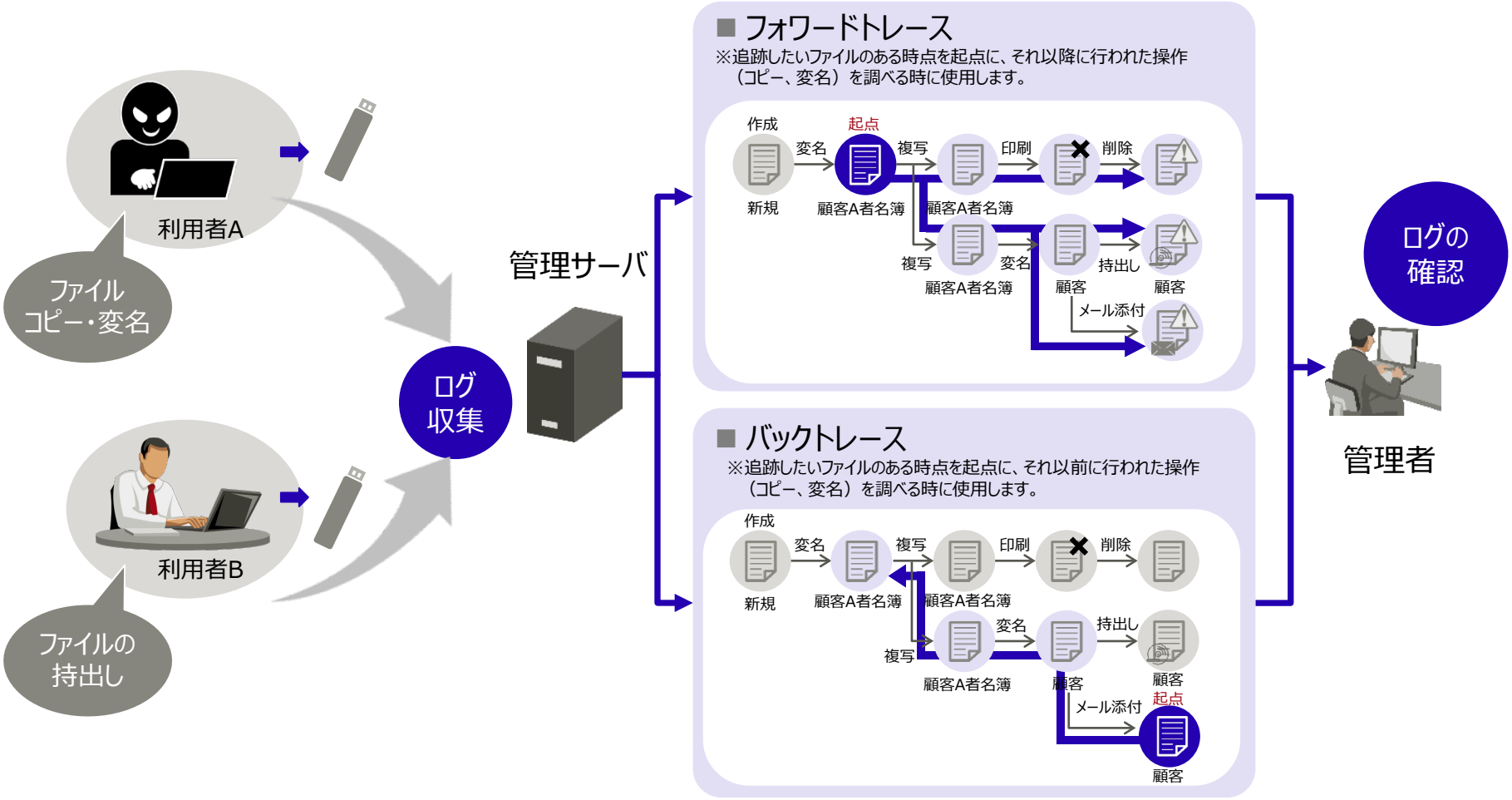
© 2024 Fujitsu Limited

ログの管理（操作の追跡）

操作ログの収集
(閲覧／追跡)

FUJITSU

■キーワード、期間などを利用してログを検索し、絞り込んだ操作に対して前後の操作を追跡できます。



操作ログの検索により、万が一の場合でも操作履歴を追跡し、迅速に対処できます。

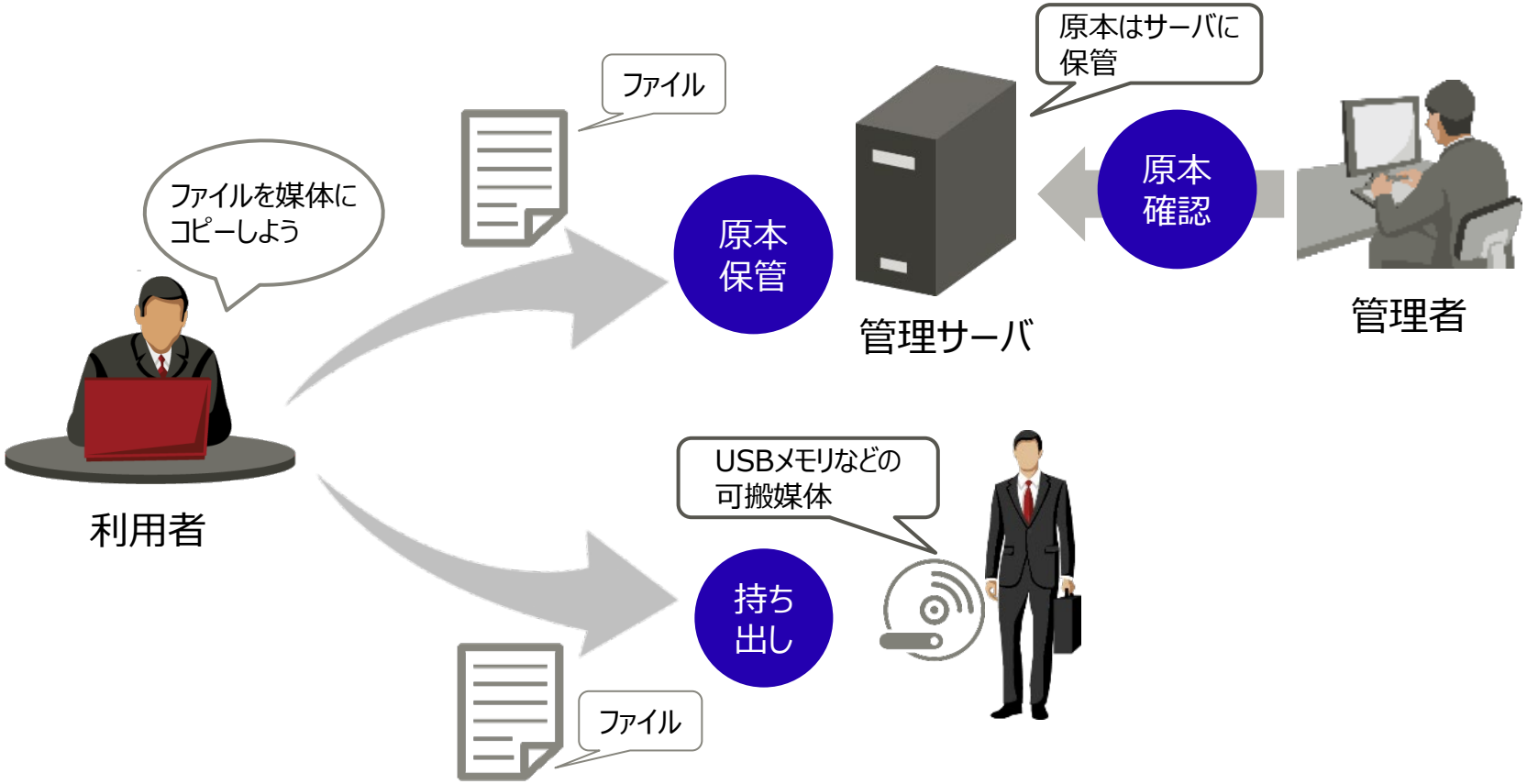
© 2024 Fujitsu Limited

ログの管理（ファイルの原本管理）

操作ログの収集
(閲覧／追跡)

FUJITSU

- 持出しを許可している可搬媒体に対しては、ファイルをコピーする際に暗号化を強制できます。
- 持出し時のファイル（原本）を操作ログと一緒に保管できます。 富士通独自



万が一、ファイルが漏えいしても、管理者は保管された原本に応じて対策を立てることができます。

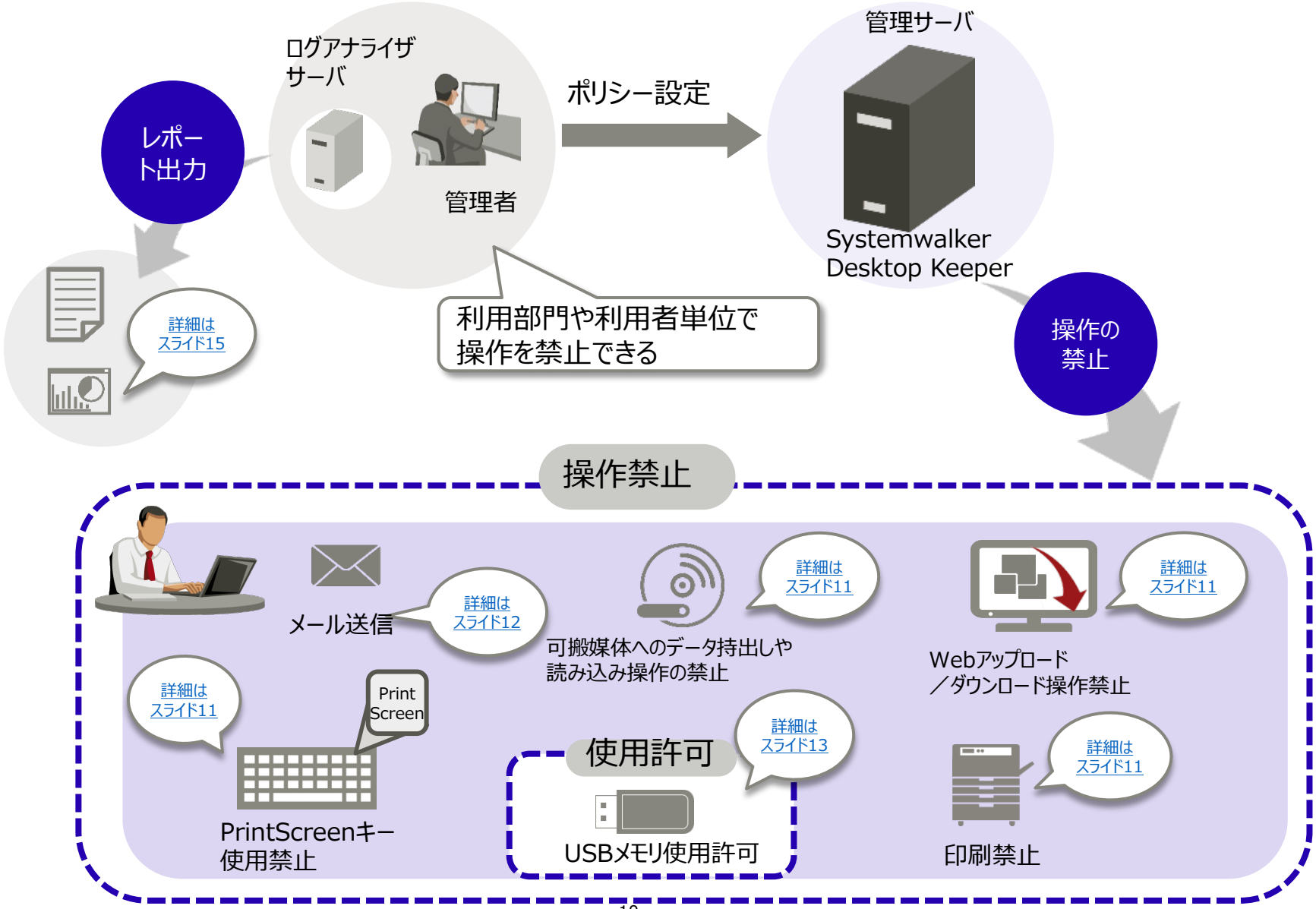
© 2024 Fujitsu Limited

操作の禁止運用

- 操作禁止の流れ
- 操作の禁止
- 操作の禁止（非暗号化ファイルのメール送信）
- 操作の禁止（USBデバイスの使用許可）

© 2024 Fujitsu Limited

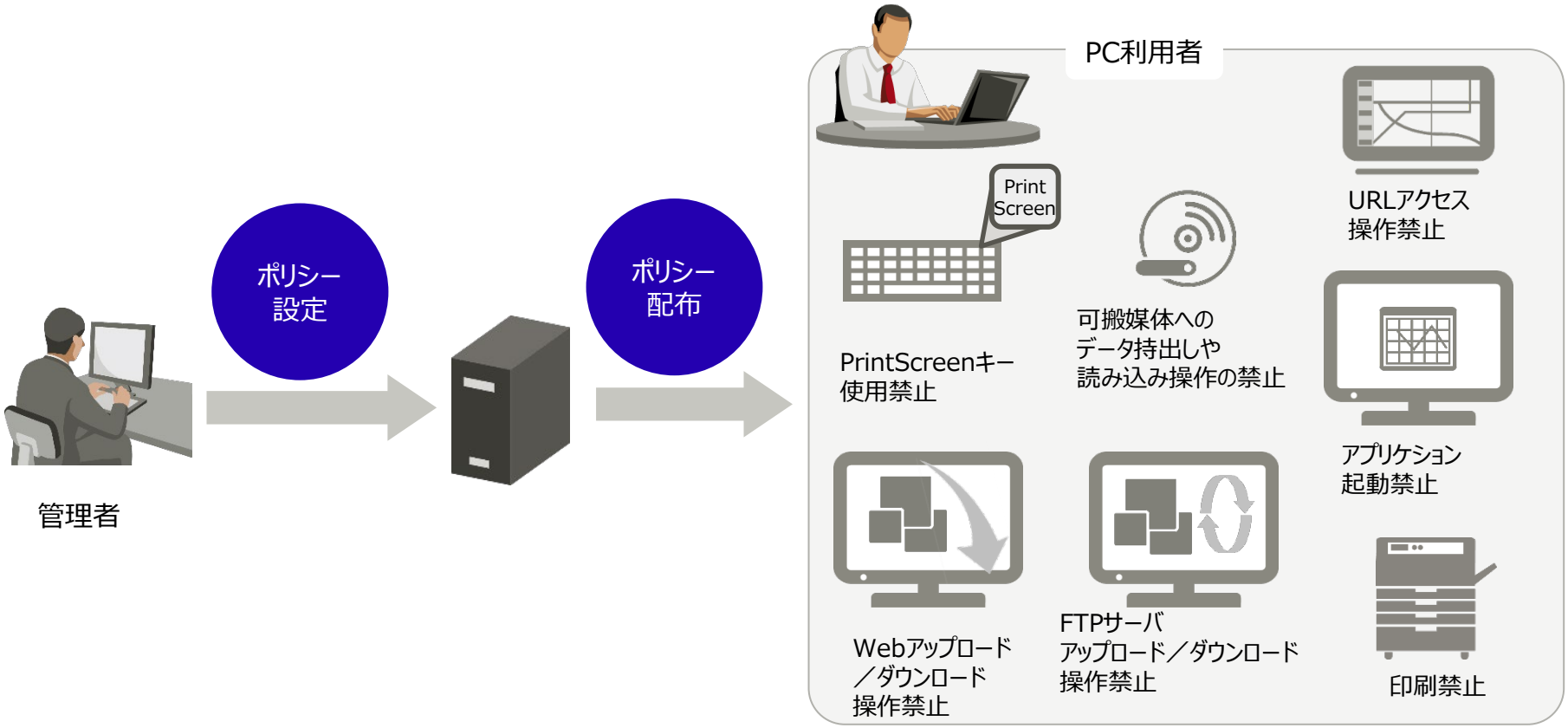
操作禁止の流れ



© 2024 Fujitsu Limited

操作禁止

- 情報漏えいリスクのある操作を禁止できます。
- 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します。
- グループ単位、ユーザー単位にポリシーを設定できます。



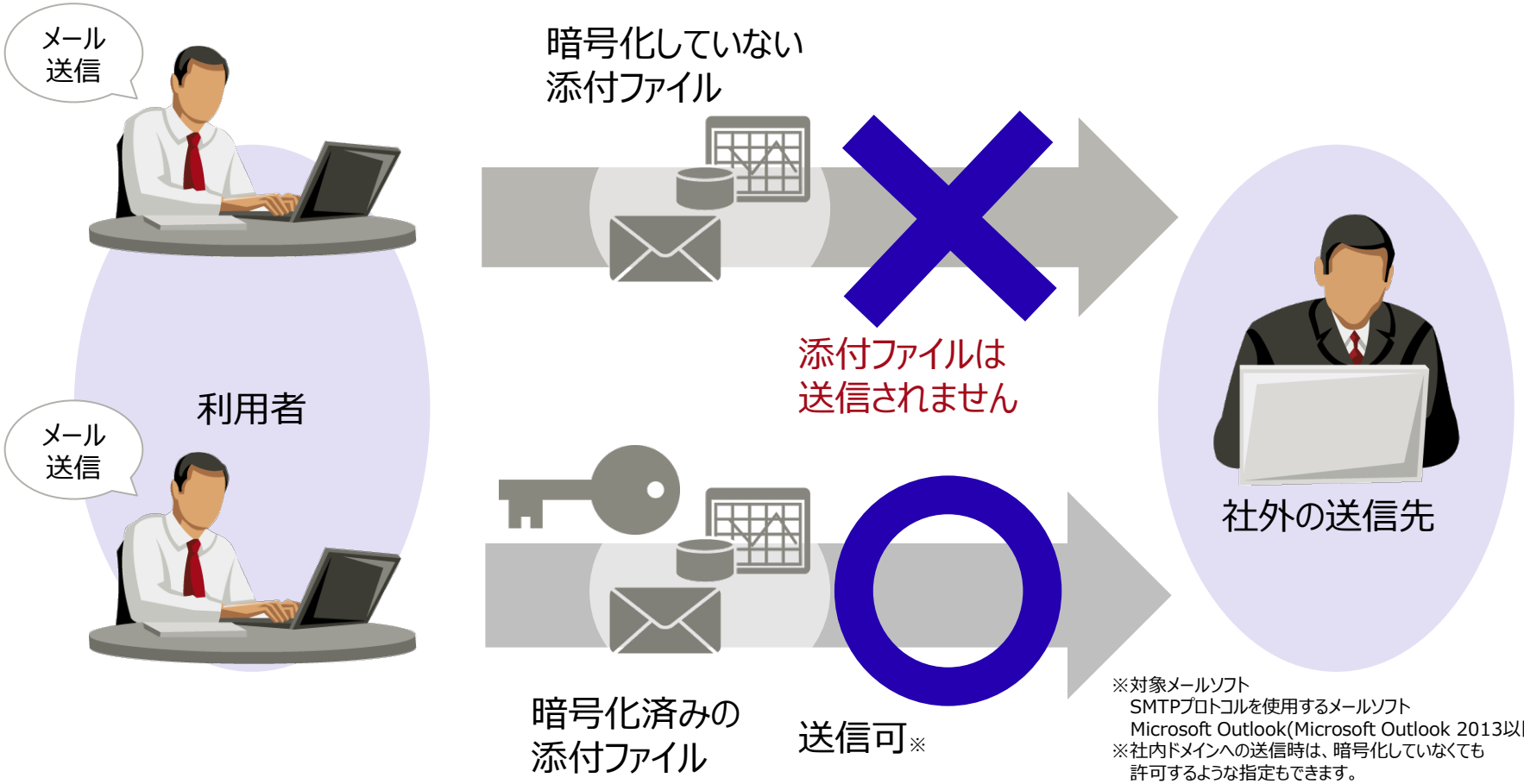
PCの情報漏えいリスクのある操作を禁止できます。

© 2024 Fujitsu Limited

操作禁止（非暗号化ファイルのメール送信）

FUJITSU

■ 暗号化済みの添付ファイルのみ送信できます。



※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)
※社内ドメインへの送信時は、暗号化していなくても
許可するような指定もできます。

暗号化済みの添付ファイルのみメール送信できるため
万が一の誤送信でも、添付ファイルを閲覧されません。

© 2024 Fujitsu Limited

操作禁止（メディアの使用許可）

/操作の禁止運用

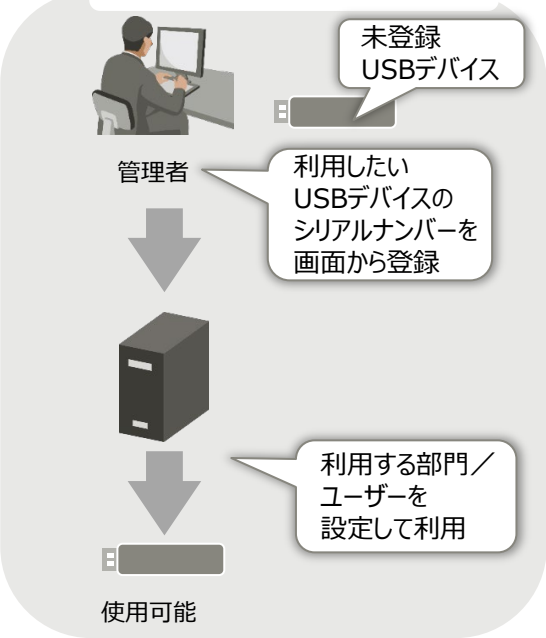
FUJITSU

■メディア個体識別機能により、業務上、許された人やデバイスに限定して持出しを許可できます。

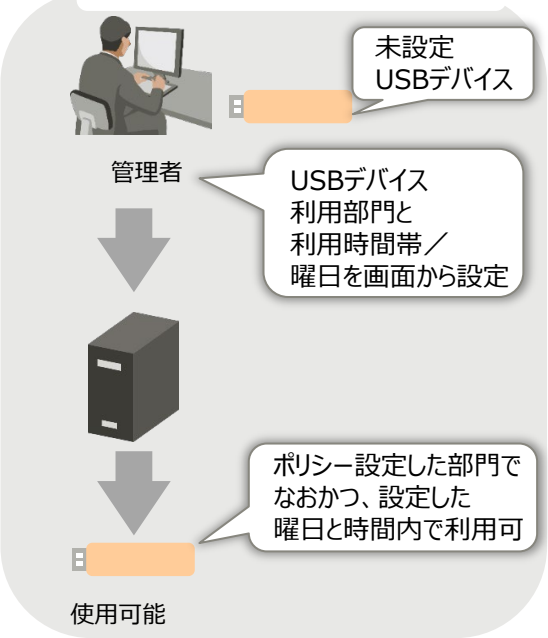
■時間や曜日を指定し、持出しを許可できます。 富士通独自

■ファイルを暗号化することで持出しを許可できます。 富士通独自

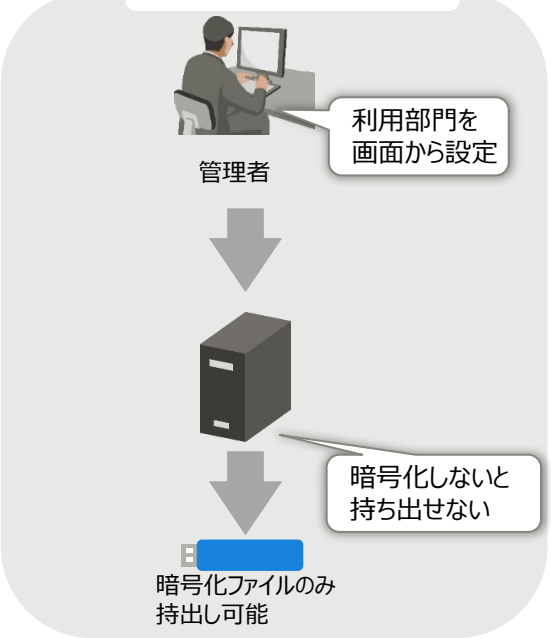
USB個体識別機能の場合



時間や曜日を指定する場合



暗号化持出しの場合



USBメモリ以外に以下の制御ができます。
- Android端末(※)（ポータブル／イメージング）
- iOS端末（ポータブル）
- デジタルカメラ（ポータブル）
- スキャナ（ポータブル）
- SDカード、miniSDカード、microSDカード

(※)スマートデバイスなどでは、USBメモリと異なるファイル転送方式PTP/MTP*を採用し、転送時のファイル破損を回避します。
* PTP : Picture Transfer Protocol
* MTP : Media Transfer Protocol

ファイルを持ち出す際にセキュリティポリシーに合わせて個別の使用を許可できます。

© 2024 Fujitsu Limited
Copyright 2021 FUJITSU LIMITED

レポート機能

■ レポート出力

© 2024 Fujitsu Limited

レポート出力

FUJITSU

■ 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、PC利用実態を把握できます。

出力可能レポート（全28種）

- 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
- 統合分析レポート・・・・・・・・1種
- 印刷量監査レポート・・・・・・9種

定期的に評価／分析した結果を見える化し、ポリシーの見直しができます。

© 2024 Fujitsu Limited

製品情報

- 事例（参考）
- 登録商標

© 2024 Fujitsu Limited

事例１ – 某通信キャリア様(参考)

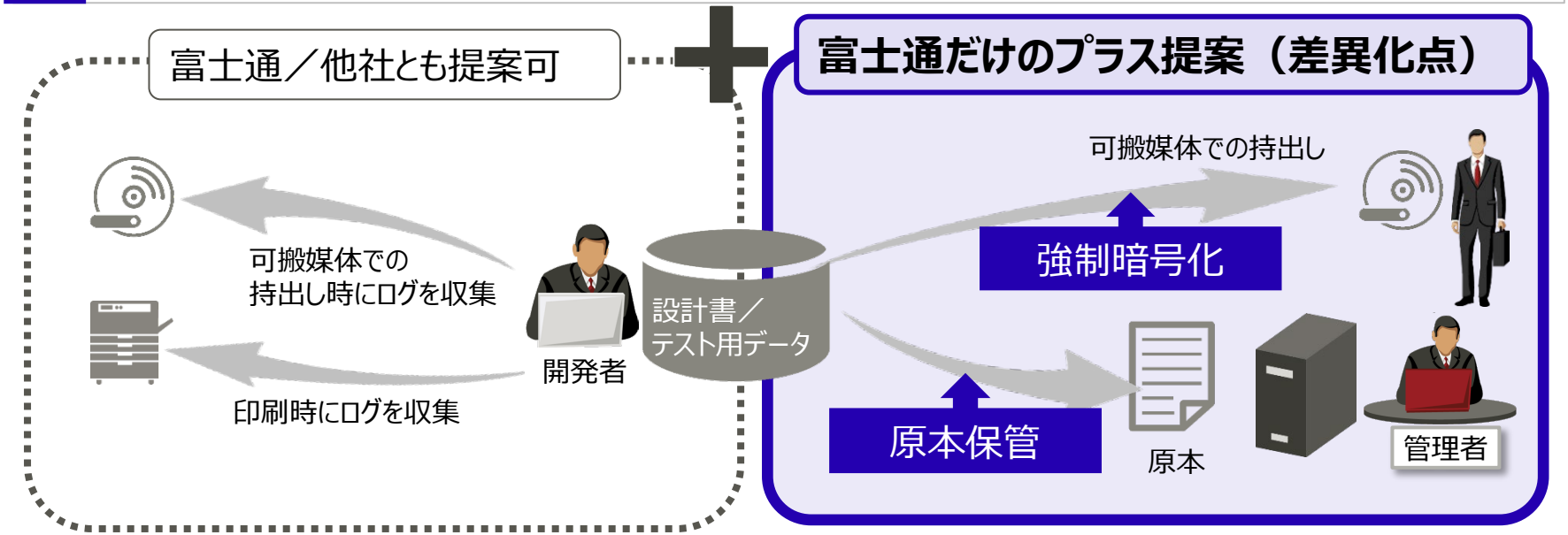
暗号化／原本保管

FUJITSU

■ 開発作業の生産物をUSBなどで持ち出す際のセキュリティ対策を強化

要件：システム開発者の作業効率を損なうことなく、情報漏えい対策を講じたい。

課題	■システム開発者が、設計書やテスト用データを持ち出す際の、紛失による情報漏えいが心配。 ■操作ログの収集や、持出しファイルの状況を把握したい。
解決	■Systemwalker Desktop Keeperの機能を用い、ファイルを可搬媒体に持ち出す場合は、強制的に暗号化。さらにファイルの原本が自動的にサーバへ保管されるので、紛失時に原本からファイルの内容を確認でき、迅速な対処へ。 ■システム開発者が使用する端末の操作ログを収集することで、セキュリティポリシーに違反している不正操作の追跡を実現。



© 2024 Fujitsu Limited

事例２ – 某金属会社様(参考)

PCの
ログ収集／検索

FUJITSU

■ 国内／海外拠点で同一のポリシーによりセキュリティ統制

要件：国内と同じセキュリティポリシーを海外に展開して、PCのログの一元管理をしたい。

課題

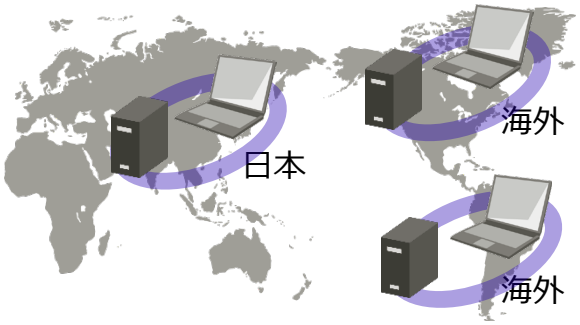
- 国内と海外拠点5か国(タイ、ベトナム、中国、シンガポール、マレーシア)とでは、別の管理者が運用しているが、海外拠点は国内ほどセキュリティポリシーが守られていない。
- 国内から一括で、海外拠点にセキュリティポリシーを展開し、全社統一のセキュリティレベルを維持したい。

解決

- Systemwalker Desktop Keeperは、日本語OS以外でもクライアントの動作を保証しているため、海外拠点のPCを国内から集中管理できる(注)。
- 国内／海外一括で同一レベルのセキュリティポリシー運用が可能。

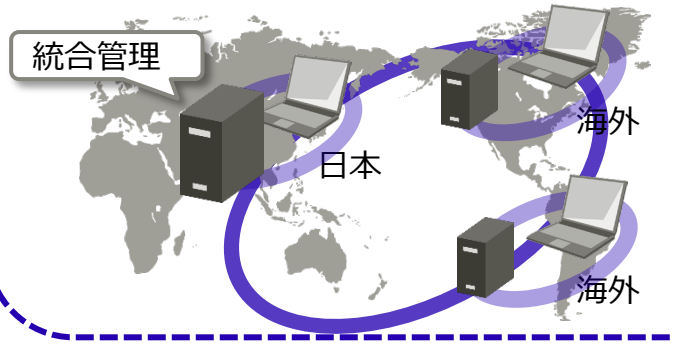
他社の提案可能範囲

国内と海外で別の管理者／別のサーバで
ポリシー配付、ログの収集



富士通の提案

各拠点でポリシー配付／ログ収集し、日本で統合管理



(注)海外拠点で本商品のご利用に際しては、詳細を弊社営業までご連絡ください。

© 2024 Fujitsu Limited

登録商標

- Microsoft、Windows、およびWindows Serverまたはその他のマイクロソフト製品の名称および製品名は、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。
- 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。
- その他の製品名は、各社の商標または登録商標です。

© 2024 Fujitsu Limited

Thank you

© 2024 Fujitsu Limited