2025年04月 現在

Fujitsu Software
Systemwalker Desktop Keeper V16.2.1

Systemwalker Desktop Keeperは、セキュリティポリシーに基づき、パソコンの情報漏洩リスクとなりうるクライアント操作を「記録」または「禁止」する、情報漏洩対策ソフトウェアです。記録したログを分析することで漏洩リスクを診断したり、万が一情報漏洩が発生した場合にはログを検索・追跡することで漏洩経路をたどることができます。これに加え、紙のコストやCO2排出量をレポート出力して見える化することで、削減計画の支援とグリーンICTを実現できます。クライアント数十台程度の部門規模から全社レベルの大規模システムに適用可能です。

適応機種　概要

- **統合管理サーバ**

  PRIMEQUEST 4000シリーズ / PRIMEQUEST 3000/2000シリーズ / PRIMEQUEST 1000シリーズ / マルチベンダーサーバ・クライアント / PRIMERGY / FUJITSU Hybrid IT Service FJcloud-0 IaaS / FUJITSU Hybrid IT Service for Microsoft Azure 仮想マシン / FUJITSU Cloud Service S5 / パブリッククラウド

- **管理サーバ**

  PRIMEQUEST 4000シリーズ / PRIMEQUEST 3000/2000シリーズ / PRIMEQUEST 1000シリーズ / マルチベンダーサーバ・クライアント / PRIMERGY / FUJITSU Hybrid IT Service FJcloud-0 IaaS / FUJITSU Hybrid IT Service for Microsoft Azure 仮想マシン / FUJITSU Cloud Service S5 / パブリッククラウド

- **ログアナライザサーバ**

  PRIMEQUEST 4000シリーズ / PRIMEQUEST 3000/2000シリーズ / PRIMEQUEST 1000シリーズ / マルチベンダーサーバ・クライアント / PRIMERGY / FUJITSU Hybrid IT Service FJcloud-0 IaaS / FUJITSU Hybrid IT Service for Microsoft Azure 仮想マシン / FUJITSU Cloud Service S5 / パブリッククラウド

- **管理コンソール**

  PRIMEQUEST 4000シリーズ / PRIMEQUEST 3000/2000シリーズ / PRIMEQUEST 1000シリーズ / マルチベンダーサーバ・クライアント / FMV / PRIMERGY / FUJITSU Hybrid IT Service FJcloud-0 IaaS / FUJITSU Hybrid IT Service for Microsoft Azure 仮想マシン / FUJITSU Cloud Service S5 / パブリッククラウド

- **クライアント（CT)**

  PRIMEQUEST 4000シリーズ / PRIMEQUEST 3000/2000シリーズ / PRIMEQUEST 1000シリーズ / マルチベンダーサーバ・クライアント / FMV / PRIMERGY / FUJITSU Hybrid IT Service FJcloud-0 IaaS / FUJITSU Hybrid IT Service for Microsoft Azure 仮想マシン / FUJITSU Cloud Service S5 / パブリッククラウド

- **Citrix XenApp 監視**

  PRIMEQUEST 4000シリーズ / PRIMEQUEST 3000/2000シリーズ / PRIMEQUEST 1000シリーズ / マルチベンダーサーバ・クライアント / PRIMERGY / FUJITSU Hybrid IT Service FJcloud-0 IaaS / FUJITSU Hybrid IT Service for Microsoft Azure 仮想マシン / FUJITSU Cloud Service S5 / パブリッククラウド

- **レポート出力ツール**

  FMV / マルチベンダーサーバ・クライアント

- **ゲートウェイサーバ(中継サーバ)**

  PRIMEQUEST 4000シリーズ / PRIMEQUEST 3000/2000シリーズ / PRIMEQUEST 1000シリーズ / マルチベンダーサーバ・クライアント / PRIMERGY / FUJITSU Hybrid IT Service FJcloud-0 IaaS / FUJITSU Hybrid IT Service for Microsoft Azure 仮想マシン / FUJITSU Cloud Service S5 / パブリッククラウド

適応OS　概要

- **統合管理サーバ**

  Windows Server 2022(64-bit) / Windows Server 2019(64-bit) / Windows Server 2016(64-bit)

- **管理サーバ**

  Windows Server 2022(64-bit) / Windows Server 2019(64-bit) / Windows Server 2016(64-bit)

- **ログアナライザサーバ**

  Windows Server 2022(64-bit) / Windows Server 2019(64-bit) / Windows Server 2016(64-bit)

- **管理コンソール**

  Windows 11(64-bit) / Windows 10(64-bit) / Windows 10 / Windows Server 2022(64-bit) / Windows Server 2019(64-bit) / Windows Server 2016(64-bit)

- **クライアント（CT)**

  Windows 11(64-bit) / Windows 10(64-bit) / Windows 10 / Windows Server 2022(64-bit) / Windows Server 2019(64-bit) / Windows Server 2016(64-bit)

- **Citrix XenApp 監視**

  Windows Server 2022(64-bit) / Windows Server 2019(64-bit) / Windows Server 2016(64-bit)

- **レポート出力ツール**

  Windows 11(64-bit) / Windows 10(64-bit) / Windows 10

- **ゲートウェイサーバ(中継サーバ)**

  Windows Server 2022(64-bit) / Windows Server 2019(64-bit) / Windows Server 2016(64-bit)

機能説明

1. グリーンICT

(1) 印刷量監視機能

各ユーザーの印刷を監視し、印刷量の多いユーザーに「警告」すると共に、「管理者に通知」します。

また、ユーザー毎/部門毎／組織全体の印刷量をレポート化し、削減目標と実績値の差分を見える化することにより、無駄な印刷を抑止してCO2削減に貢献します。

(2)複合機連携

複合機の印刷、コピー、FAXにおける以下の情報を見える化してレポートを出力します。

これにより用紙コスト、CO2排出量の削減目標の設定や業務の見直しができます。

- 用紙の使用量
- CO2排出量
- 用紙のコスト情報
- 印刷方法別(Nup/両面/カラー)の詳細情報

---

2. 禁止機能

(1) アプリケーション起動禁止

各クライアントにインストールされているアプリケーション情報を取得・管理し、指定アプリケーションの起動を抑止することで、ファイル共有ソフト等による情報漏洩を未然に防止したり、業務端末でのゲームソフトの起動を禁止できます。

(2) ログオン禁止

ログオンしようとするユーザーの所属グループをチェックし、セキュリティポリシーに違反するIDでのログオン操作を無効に(強制ログオフ、シャットダウン) します。

(3) PrintScreenキーの禁止

PrintScreenキーによる画面ハードコピー取得を無効にして、情報漏洩を未然に防止します。

PrintScreenキーの代わりに任意のキーを設定することもできます。

(4) ファイル持ち出し

ドライブ、ネットワークドライブ、リムーバブルドライブ、MO、FD、CDまたは、DVDへの書き込みを監視して、書き込みを禁止したり、強制的にファイルを暗号化します。

書き込み抑止、強制暗号化をすることでデバイスの盗難や紛失時にも第三者による情報漏洩を防止できます。

暗号化方式は、自己復号型暗号化、ZIP暗号化及び、ZIP(AES-256)暗号化を選択することができます。

(5) 印刷の禁止

許可されたアプリケーション以外からの印刷を無効にして、印刷物による情報漏洩を防止できます。

(6) メール添付ファイルの禁止

管理者の設定したポリシーにより、ファイルが添付されたメール送信を禁止することができます。 また、メールの転送時にもファイル添付を禁止することができます。

以下のいずれかのポリシーを設定することが可能です。

- メール添付禁止しない

- 暗号化されていないファイル添付不可
- ファイルの拡張子指定による添付不可

メール添付ファイルの禁止をできるのは、「SMTPを使用するメールソフト」およびOutlookです。

グループウェアのメール、Webメールについては、メールへのファイル添付禁止機能の対象とはなりません。

(7) サービス/プロセス起動禁止

各クライアントで登録されているサービス一覧/プロセス一覧を取得して、情報漏洩に結びつく可能性のあるサービス/プロセスを強制終了・起動抑止することで、情報漏洩を未然に防止します。

(8) 許可のないUSB媒体の使用

ファイルの持ち出しを許可する場合に、個々のUSB媒体のメーカーおよびシリアル番号を識別し、特定のUSBに対してのみデータの持ち出しを許可することができます。管理者が特定のUSBメモリのみに使用を限定させることで、データの持ち出しに関する安全性が向上します。

(9) リムーバブルドライブ、ネットワークドライブまたは、DVD/CDからのデータ読み込み

リムーバブルドライブ、ネットワークドライブまたは、DVD/CDからはデータを読み込ませない設定ができます。これにより、リムーバブルドライブ、ネットワークドライブまたは、DVD/CDを介した不正なデータやソフトウェアの持ち込みを防止できます。

(10)Webサーバ/FTPサーバへのアクセス禁止

以下のWebサーバ、FTPサーバへのアクセスを禁止できます。

- 設定されたURLへのアクセスを禁止して、警告メッセージを表示できます。(※)
- 許可されたWebサイト以外からのアップロード・ダウンロード操作を禁止できます。(※)

Webアップロード・ダウンロード禁止が対象とするWebサービスはDropbox、Dropbox Business、Google Drive、Google Drive for Work、OneDrive、OneDrive for Business、BOXです。

- FTPサーバへのアクセスを禁止して、警告メッセージを表示できます。

(※) Microsoft Internet Explorer、Microsoft Edgeに加え、Firefox、Google Chromeの各ブラウザで動作します。

(11) 未許可のネットワークドライブへの操作の禁止

管理者が許可していないサーバへのファイルの読み書きを禁止した場合、利用者へ警告メッセージを表示します。

(12) 仮想環境とパソコン間のクリップボード操作の禁止

クリップボードを利用して仮想端末から物理端末へのコピー、物理端末から仮想端末へのコピーを禁止できます。コピー禁止時にはクリップボードの内容を取得することができます。

(13) 仮想環境への接続・切断の記録

物理端末から仮想端末への接続および切断した時間と物理仮想端末のコンピューター名が把握できます。物理環境から仮想環境の操作の流れをトータルに把握できます。

(14)デバイスの禁止

Windowsにおいて以下の接続方法によるデバイスを禁止できます。

Bluetooth,赤外線,Wi-Fi,PCカード,PCI ExpressCard,IEEE1394,シリアルポート/パラレルポート

3．記録機能

(1) ファイル持出し記録

ファイル持出しの禁止設定されている場合に、持ち出しユーティリティを使用して、暗号化したファイルやフォルダの持出しを行った際の操作を記録します。これにより、外部に持ち出されたファイルの経路の追跡、特定ができます。

(2) クライアント操作記録

クライアント操作(アプリケーション起動・終了、ウィンドウ・ダイアログタイトル取得によるWeb閲覧監視、コマンドプロンプト内操作、メール送信、セーフモード起動時の操作)を記録できます。これにより情報漏洩につながる危険のある操作を防止することができます。

(3) デバイス構成変更記録

ドライブレターの変更をともなう機器構成の変化(Plug&Play、ネットワーク共有、USBメモリデバイスの記録媒体追加等)を記録します。これにより情報漏洩が発生した場合にデータを持ち出した媒体を特定し、追跡・調査することができます。

(4) 印刷操作記録

スプール経由の印刷(ファイル名、頁数)を記録することができます。これにより、持ち出したファイルの追跡・調査ができます。

(5) ファイル操作記録

クライアントでのアプリケーションによるファイル操作(参照、作成、更新、削除、複写、移動、改名) を記録することができます。

ファイル操作を記録することで、ファイルをコピーしたり名前を変えて持ち出した場合でも追跡・調査が可能になります。

また、操作ログの取得範囲を絞りこみ、ローカルシステムフォルダ、TEMPフォルダの操作ログを取得しない設定もできます。

(6) ログオン/ログオフ/パソコン起動/パソコン終了の記録

パソコンへの"ログオン"、"ログオフ"、パソコンの起動、パソコンの終了を記録します。

他の操作ログと照らしあわせ、「誰」が「いつ」「何」をしたかを明らかにすることができます。

(7) PrintScreenキー操作の記録

PrintScreenキーにより、画面コピーをとる操作を記録します。

記録されていることをユーザーに周知することで、ポリシーに違反する操作への心理的抑止効果を発揮します。

PrintScreenキーの代わりに任意のキーを設定することもできます。

(8)Webサーバ/FTPサーバへのアクセス記録

以下のWebサーバ、FTPサーバへのアクセスを記録できます。

- 設定されたURLへのアクセスを記録できます。(※)
- Webブラウザからファイルをアップロード・ダウンロードする操作を記録できます。(※)

Webアップロード・ダウンロード記録が対象とするWebサービスはDropbox、Dropbox Business、Google Drive、Google Drive for Work、OneDrive、OneDrive for Business、BOX、Microsoft Teamsです。

- FTPサーバへのアクセスを記録できます。

(※) Microsoft Internet Explorer、Microsoft Edgeに加え、Firefox、Google Chromeの各ブラウザで動作します。

(9) 原本保管

管理者により、持ち出し抑止設定されているリムーバブルメディア(CD, MO, FD, HD, メモリスティック等）に対し、利用者が「持ち出しユーティリティ」を使用して、ファイルをコピーした場合、持ち出しログ情報の付属情報として、コピーしたファイル（原本）が管理サーバに送信され、保管されます。

管理者は、原本データをログビューアからダウンロードすることができ、必要に応じて持ち出されたファイルの内容を監査することが可能となります。

外部に持ち出されたデータを収集することで、管理者はどのような情報が出力されたか把握できます。また、利用者に原本保管を告知することで、ファイルの外部持ち出しに対する心理的抑止効果を発揮します。

(10) 用紙使用状況の通知

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、紙の削減に貢献します。

(11)仮想環境でのログ取得

VMware Horizon RDSH/Citrix XenDesktop/Citrix Virtual Desktops/Citrix Virtual Apps and Desktopsでは、一部制限(注)を除き物理環境と同じ種別のログが取得可能です。

Citrix XenApp/Citrix Virtual Appsでは、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、アプリの起動/終了、ウィンドウタイトル、Printscreenキー操作、FTP操作、Web操作、クリップボード操作のログが取得可能です。（Citrix XenApp 監視が必要です）

(注) Citrix XenDesktop/Citrix Virtual Desktops/Citrix Virtual Apps and Desktopsの場合、デバイス構成変更ログ/ファイル操作ログについてはUSBリダイレクト接続時のみ取得可能です(ドライブマッピングは対象外)

(12)メール送信ログの記録

「SMTPを使用するメールソフト」Outlook、および以下のWebメール送信を行った時のログ採取を行います。

Gmail、Outlook.com、Outlook for Microsoft 365(旧称Office 365)

(13)Sense YOU Technology Bizと連携する場合

Sense YOU Technology Bizによる覗き見検知時および他人検知時に、クライアント(CT)のデスクトップ画面のハードコピーをログとして取得できます。

(14)環境変更ログの記録

クライアントの環境が変更されたときのログを記録します。

・クライアントの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

(15)メール受信ログの記録

Microsoft Outlookのメール受信ログを採取します。

4. 管理機能

(1) 管理コンソール

クライアントを一括して設定管理(ポリシー設定、ログ参照/検索等)できる管理コンソールを提供します。

管理コンソールおよびクライアント(CT)は英語OSに対応しています。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の一元管理を行うことができます。

(2) 階層管理

1台の統合管理サーバから複数の管理サーバを統合管理することができます。

統合管理サーバでは各管理サーバで設定されたポリシーの参照、更新および管理サーバのログを参照することができます。

(3) 運用管理

部門統制環境における管理者のポリシー管理機能を提供します。管理者権限については、システム全体の管理者と部門管理者の2階層とし、それぞれ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が可能です。

(4) アクセスコントロール

管理対象部門全体のパソコンの操作制限を管理する、部門管理者によるポリシー制御機能です。ユーザーをグループ化し、グループ毎にポリシー管理を行うことができます。

(5) 自己版数管理

クライアントが自己のモジュールの版数を管理して、版数アップ時には自動的に更新します。

(6) メール/メッセージ通知

セキュリティ設定に問題のあるPCの利用者や部門管理者に対して、対処依頼のメール、メッセージを自動的に作成して通知します。

(7) Systemwalker Desktop Patrol連携

Systemwalker Desktop Patrolで管理している組織の構成情報の移入を行い、データを共有できます。

(8) バックアップ・リストア機能

各種操作ログをCSV形式ファイルとしてバックアップしたり、CSV形式ファイルからリストアすることができます。

(9) ログ送信時間の設定

クライアントから管理サーバへのログ送信の時間帯設定ができます。

(10) 監査証跡

部門統制ツールとして、 ログビューアから部門管理者権限により、自部門内の操作ログ検索/表示や、ログのCSV出力ができます。

(11) バックアップしたログの閲覧

すでにバックアップしたログファイルをログビューアで参照することができます。ログ閲覧用のデータベース(ログ閲覧データベース、統合ログ閲覧データベース)により快適にログを参照可能です。

(12) Systemwalker Desktop Patrolへの呼び出し

Systemwalker Desktop Patrolの組織情報を定期的に自動的に取り込みます。人事異動が発生しても組織情報を即時に反映します。

(13) クライアント仮想環境への対応

VMware Horizon、Citrix XenDesktop/Citrix Virtual Apps and Desktops/VMware Horizon RDSH/Citrix XenApp/Citrix Virtual Appsに対応しています。

(14) 部門管理者権限によるUSBデバイス及び、SDカード管理

USBデバイス及び、SDカード管理権限を持った部門管理者は、部門ごとに利用可能なUSBデバイス及び、SDカードの登録ができます。この部門管理者でログインすると、USBデバイス及び、SDカードの登録などの管理だけが利用でき、その他の機能の参照および変更はできません。

(15) 標的型攻撃への対応

管理者がセキュリティリスクを検知した時に、クライアントへの緊急対処(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)を行うことができます。緊急対処ポリシーを適用することで重要なファイルの持ち出しなどを禁止することができ、セキュリティリスクを軽減することができます。連携できる製品・機能は、iNetSec SFです。

（16) デバイス情報取得ツール

クライアント(CT)の利用者が、USBデバイス及び、SDカードのデバイス情報を取得して一覧ファイルを出力できます。取得した一覧ファイルを管理者に提供することで、管理者は個体識別機能の登録処理を簡単に行うことができます。

個体識別機能により、USBデバイス及び、SDカードで持出しユーティリティやエクスプローラなどからファイルやフォルダを持ち出す場合に、使用できるUSBデバイス及び、SDカードを個別に制限できます。

（17) スタンドアロン環境での利用(Systemwalker Desktop Keeper for Standalone)

管理サーバが構築できない環境向けに、クライアント端末単独でポリシーを設定の上、機能を限定したクライアント（CT）の機能が利用できます（※）。

利用可能な機能範囲は禁止機能(ファイル持出し禁止、デバイスの禁止)、記録機能（ファイル/フォルダ操作、デバイス構成変更の記録）、操作記録通知機能です。

（※）本機能は、通常のクライアント（CT）と同時にインストールできません。Windows 11を搭載する富士通機のみサポートします。

5．ログ分析

(1) レポート出力機能

紙のコストの変化(金額、CO2排出量)やセキュリティリスクの診断結果，組織内部のコンプライアンス状況を、管理者や組織上層部に対する報告資料として診断結果をまとめ、グラフ表示などの視覚効果も考慮したレポートを出力します。

(2) 情報漏洩予防診断

システム負荷の少ない夜間に、バッチ処理(夜間バッチ集計機能)にて、各端末のログを収集し、情報漏洩につながる以下の操作ログに対して集計を行います。

- ファイル持ち出し操作ログ
- ファイル操作ログ
- 印刷操作ログ
- メール送信操作ログ
- Webアップロード、FTPアップロード

直近7日間の各端末で発生した操作ログ件数の集計結果から、違反操作のランキングを行い、情報漏洩の予防診断として利用できます。

(3) 目的別集計機能

■ファイル操作ログ分析

- 日付単位でファイルの操作件数を収集します。
- ユーザー単位/グループ単位でファイルの操作内容を分析・表示します。
- PC単位に操作した内容(複写、移動、変名など)を集計します。
- 直近7日間，過去30日間、または 期間を指定してログ集計が可能です。
- キーワードを指定してログの分析が可能です。

■ファイル持ち出しログの傾向分析

- 日付単位での外部持出ししたファイルの件数を集計します。
- ユーザー単位/グループ単位での外部持出ししたファイルの内容を分析・表示します。
- PC単位にファイルの外部持ち出し内容を集計します。
- 直近7日間，過去30日間、または 期間を指定してログ集計が可能です。
- キーワードを指定してログの分析が可能です。

■ 違反操作ログ分析

- 日付単位でSystemwalker Desktop Keeper 管理者ポリシー違反操作の件数を集計します。
- ユーザー単位/グループ単位で Systemwalker Desktop Keeperの管理者ポリシーに対する違反操作の内容を分析・表示します。
- 直近7日間、過去30日間、または、期間を指定してログ集計が可能です。

■印刷操作ログ分析

- 日付単位での印刷操作の件数を集計します。
- ユーザー単位/グループ単位で印刷操作の内容(印刷タイトル/印刷総ページ数)を分析・表示します。
- 直近7日間、過去30日間、または、期間を指定してログ集計が可能です。
- キーワードを指定してログの分析が可能です。

■アプリケーション動作ログ分析

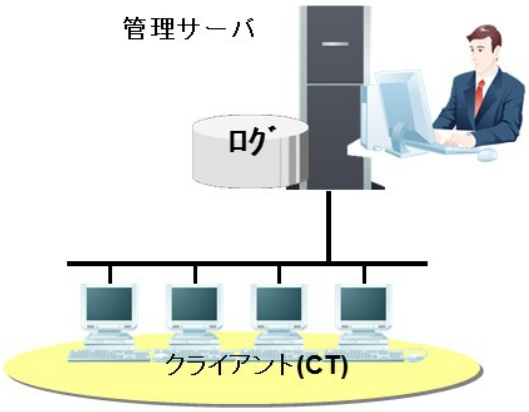
- 日付単位でアプリケーション起動の件数を集計します。
- ユーザー単位/グループ単位でアプリケーション起動の内容を分析・表示します。
- 直近7日間，過去30日間、または 期間を指定してログ集計が可能です。
- キーワードを指定してログの分析が可能です。

(4)内部不正リスクの検知

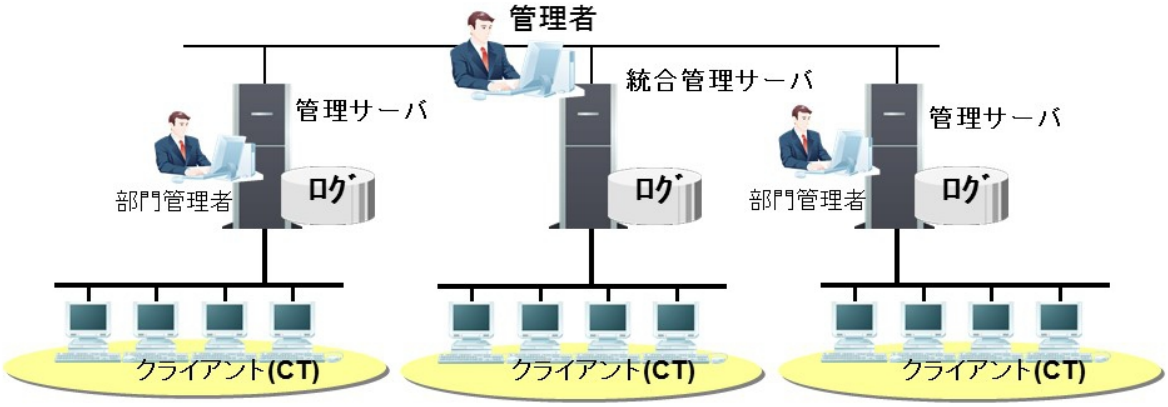
操作ログから、内部不正リスクを検出します。

内部不正の防止に向け、検知ルールを用いてPCの操作ログを調べることで、内部不正リスク（不審な持出し予兆行動、不審な持出し行動）の早期発見を支援します。

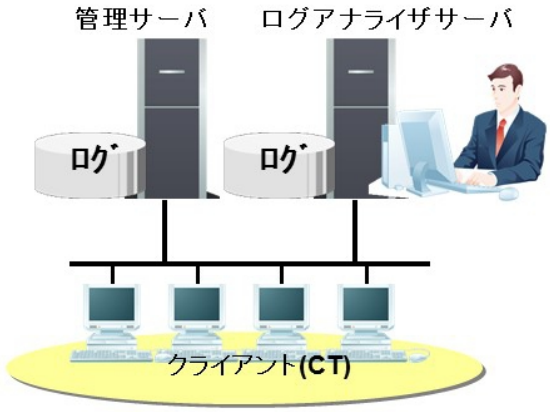
[標準構成]



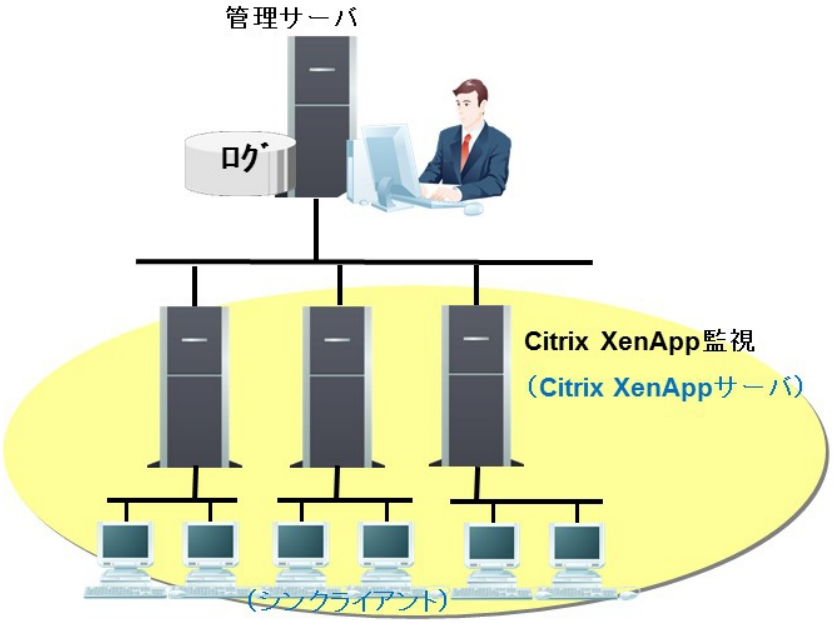
[統合管理サーバによるサーバの階層管理を行う場合]



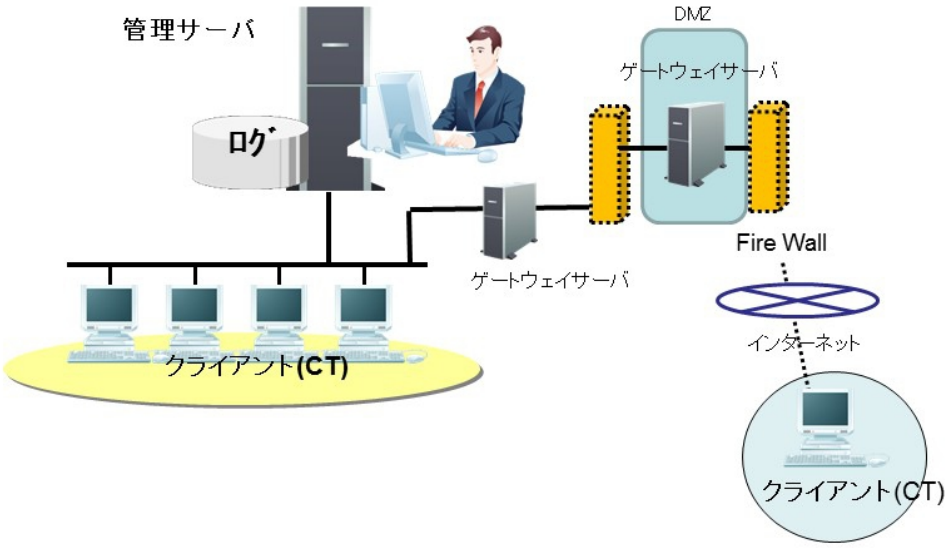
[ログ分析を行う場合]



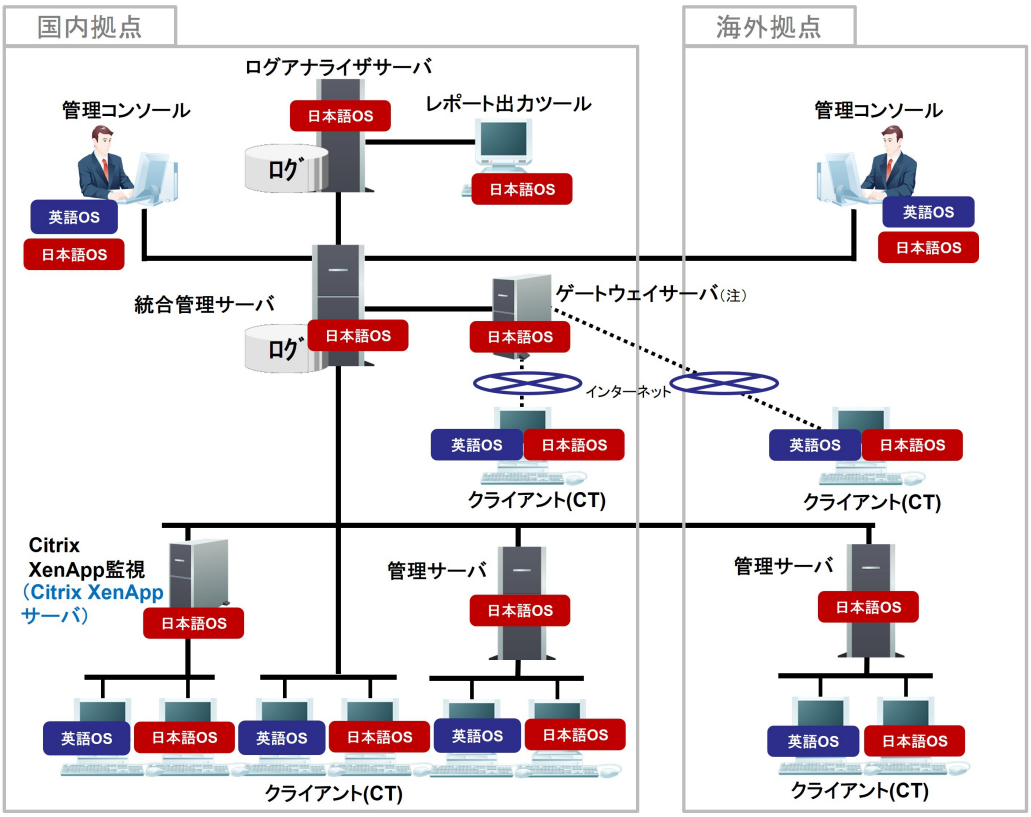
[Citrix XenApp監視機能を行う場合]



[CT利用環境を拡張した場合]



[海外拠点の端末を管理する場合]



（注）インターネット経由でCTを管理する場合は[CT利用環境を拡張した場合]を参照

システム構成要素

システムの構成要素について以下に説明します。

【管理サーバ】
管理サーバ配下のPCのセキュリティポリシーの設定定義、各PCへのポリシーの配付、配下のPCから収集したログの保管を行うサーバです。

【統合管理サーバ】
管理サーバが複数ある場合に設置します。統合管理サーバに、管理コンソールやログビューアを接続して、各管理サーバで定義したポリシーの参照および変更、ログの参照ができます。

【Citrix XenApp監視】
Citrix XenApp(Citrix社製)のクライアント(仮想端末)の操作(アプリケーション起動・終了、ログオン/ログオフ、ファイル操作、コマンドプロンプト、印刷、FTP操作、Web操作、クリップボード操作)ログを採取し、管理サーバへ転送します。

【管理コンソール】
管理サーバに対する定義、CTポリシーおよびユーザーポリシーの定義、クライアント(CT)へのポリシーの配付や、クライアント(CT)から収集するログの定義を一括操作するコンソールです。

【クライアント(CT)】
管理対象となるPCにインストールするクライアントモジュールです。セキュリティポリシーの配付をうけ、設定されたポリシーに従って、各種ログの保存、およびポリシーに違反した操作の禁止を行います。

【ゲートウェイサーバ】
インターネット経由でクライアント(CT)を接続する場合に(統合)管理サーバの間に設置します。

V16.2.0からV16.2.1の機能強化項目は以下のとおりです。

1. 新環境対応

以下のOSに対応しました。

－Windows 11 IoT Enterprise LTSC 2024

以下の仮想環境に対応しました。

－VMware Horizon 8 2306/2309/2312/2406

－Citrix Virtual Apps and Desktops 2308/2311/2402 LTSR/2407

以下のソフトウェアに対応しました。

－Microsoft Office 2024

－Microsoft LTSC Office 2024

2. 管理者通知機能の強化

管理者通知の対象に以下のエラーを追加しました。

－データベースに未登録のクライアント(CT)から受信があった場合

　クライアント(CT)を登録後にデータベースを再構築した場合など、当該クライアント(CT)の再登録を行うまでログの採取が行えない状況を管理者が把握しやすくなります。

3. スタンドアロン環境への対応(Systemwalker Desktop Keeper for Standalone)

管理サーバが構築できない環境向けに、機能を限定したクライアント(CT)の機能を提供しました。提供機能範囲は禁止機能(ファイル持出し禁止、デバイスの禁止)、記録機能（ファイル/フォルダ操作、デバイス構成変更の記録）、操作記録通知機能です。Windows 11を搭載する富士通機のみサポートします。

標準添付品

- **オンラインマニュアル**
  - Systemwalker Desktop Keeper V16 リリース情報
  - Systemwalker Desktop Keeper V16 解説書
  - Systemwalker Desktop Keeper V16 導入ガイド
  - Systemwalker Desktop Keeper V16 運用ガイド 管理者編
  - Systemwalker Desktop Keeper V16 運用ガイド クライアント編
  - Systemwalker Desktop Keeper V16 リファレンスマニュアル
  - Systemwalker Desktop Keeper トラブルシューティングガイド
  - Systemwalker Desktop Keeper ユーザーズガイド

商品体系

【メディア】

・Systemwalker Desktop Keeper メディアパック (64bit) V16.2.1

【サブスクリプションライセンス／サポート】

[サブスクリプションライセンス／サポート(月額払い)]

・Systemwalker Desktop Keeper サーバライセンス　for Windows (SL&S)
・Systemwalker Desktop Keeper for Citrix XenApp　for Windows (SL&S)
・Systemwalker Desktop Keeper ゲートウェイサーバライセンス　for Windows (SL&S)
・Systemwalker Desktop Keeper 1クライアントライセンス　for Windows (SL&S)
・Systemwalker Desktop Keeper 10クライアントライセンス　for Windows (SL&S)
・Systemwalker Desktop Keeper 100クライアントライセンス　for Windows (SL&S)
・Systemwalker Desktop Keeper 500クライアントライセンス　for Windows (SL&S)
・Systemwalker Desktop Keeper 1000クライアントライセンス　for Windows (SL&S)

[サブスクリプションライセンス／サポート(まとめ払い)]

・Systemwalker Desktop Keeper サーバライセンス for Windows (SL&S) 7年
・Systemwalker Desktop Keeper for Citrix XenApp for Windows (SL&S) 7年
・Systemwalker Desktop Keeper ゲートウェイサーバライセンス for Windows (SL&S) 7年
・Systemwalker Desktop Keeper 1クライアントライセンス for Windows (SL&S) 7年
・Systemwalker Desktop Keeper 10クライアントライセンス for Windows (SL&S) 7年
・Systemwalker Desktop Keeper 100クライアントライセンス for Windows (SL&S) 7年
・Systemwalker Desktop Keeper 500クライアントライセンス for Windows (SL&S) 7年
・Systemwalker Desktop Keeper 1000クライアントライセンス for Windows (SL&S) 7年

※クライアントPCのセキュリティ環境を一括して管理する製品「Systemwalker Desktop Patrol」と、情報漏洩対策を行う製品「Systemwalker Desktop Keeper」の機能を、管理対象クライアント300台限定で使用できるセット商品があります。

詳細は、「Systemwalker Desktop Patrol/Keeper キャンペーン V16.2.1」ソフトウェア・ガイドを参照してください。

購入方法

1. メディアパックの種類について

本商品のメディアパックは64bit版のみです。

2. メディアパックについて

メディアパックは、媒体（DVD）のみの提供です。使用権は許諾されておりませんので、別途、ライセンスを購入する必要があります。初回購入時には、最低1本のメディアパックとサブスクリプションライセンス／サポートを同時にご購入ください。

本メディアパックの購入でバージョンアップ／レベルアップおよび、32ビット商品と64ビット商品間での切り替えをすることはできません。

バージョンアップ／レベルアップする場合は本メディアパックを購入せず、アップグレード権を行使してメディアを入手してください。

3. サーバライセンスについて

(1) 統合管理サーバ/管理サーバは、サーバ台数分、サーバライセンスを購入してください。

(2) 統合管理サーバは管理サーバを兼ねることができます。

(3) 管理コンソール、レポート出力ツール、ログアナライザサーバは、インストールフリーです。

(4) ゲートウェイサーバは、サーバ台数分、ゲートウェイサーバライセンスを購入してください。

4. クライアントライセンスについて

(1) クライアントは、クライアントモジュールをインストールする台数分、ライセンスを購入してください。

(2) 本ライセンスはWindows OSのPCに対応します。

5. 仮想環境におけるライセンスの考え方

仮想環境における必要ライセンス数の考え方は以下のとおりです。

(1)クライアントOS上で動作する仮想クライアントPC

仮想クライアントPCに接続する物理PC台数分のクライアントライセンスが必要です。

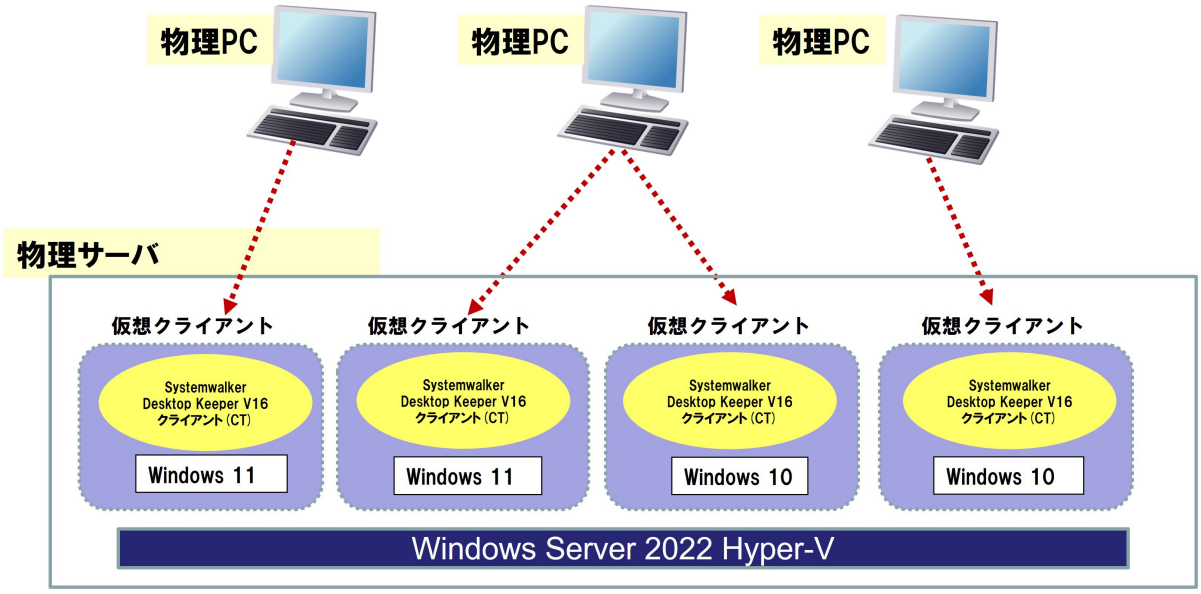
(2)サーバOS上の仮想クライアントPC、および仮想サーバのライセンス

関連URL(お客様向けURL)に記載の「ソフトウェア：富士通（インフォメーション&ダウンロード）」内、「富士通製ソフトウェアのライセンス体系」の「仮想環境利用時のライセンス購入方法」をご参照ください。

(3)仮想環境における必要ライセンスの考え方（例）

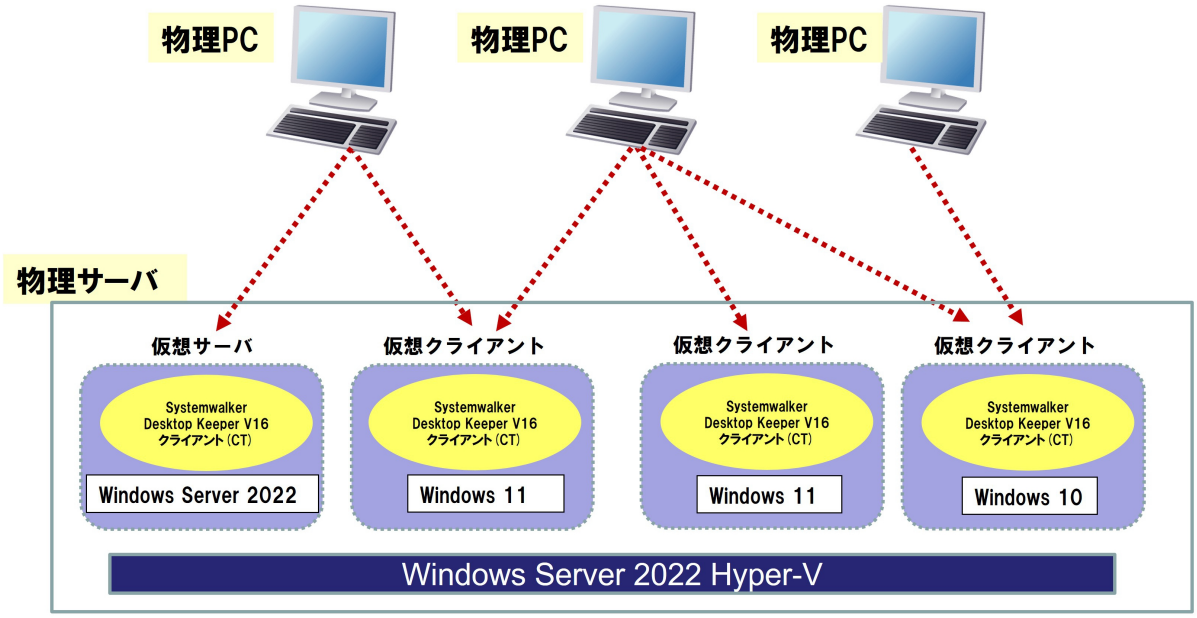
仮想環境におけるSystemwalker Desktop Keeperのライセンス購入の考え方は以下のとおりです。

(購入例1) 仮想クライアントのすべてがクライアントOS上で動作する場合



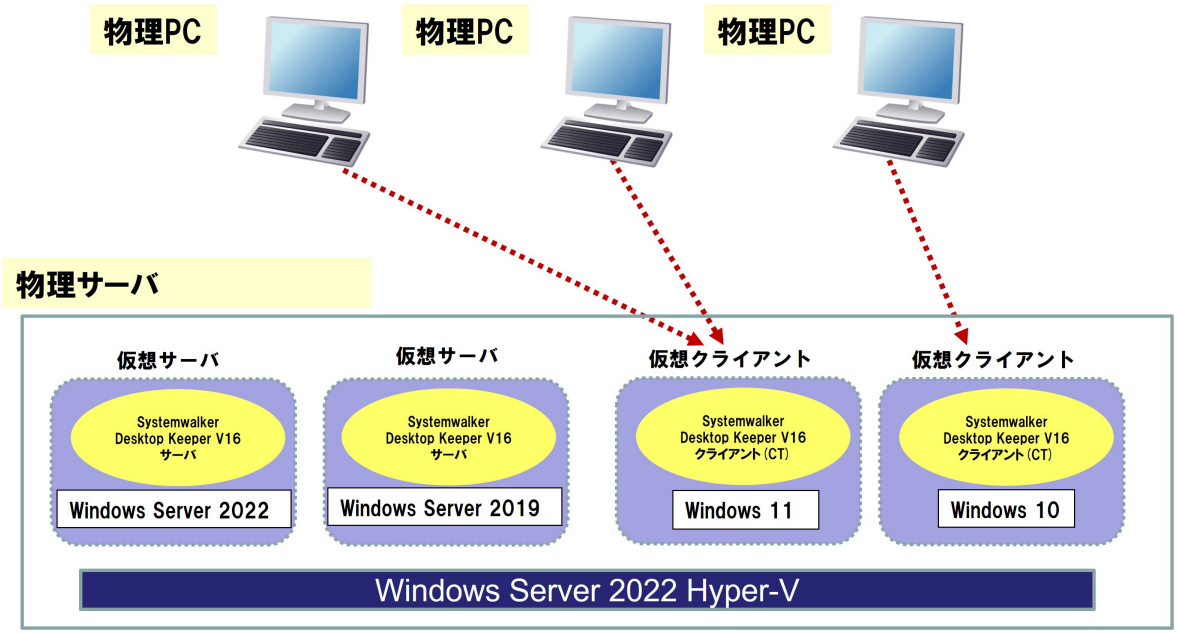
購入数の考え方	対象製品	購入数
仮想クライアント (Systemwalker Desktop Keeper V16 がクライアントOS上で動作) に接続する物理PC台数分	Systemwalker Desktop Keeper 1クライアントライセンス for Windows	3

(購入例2) サーバOSで動作する仮想クライアントがある場合



購入数の考え方	対象製品	購入数
仮想クライアント (Systemwalker Desktop Keeper V16 がクライアントOS上で動作) に接続する物理PC台数分	Systemwalker Desktop Keeper 1クライアントライセンス for Windows	3
仮想サーバ (Systemwalker Desktop Keeper V16が サーバOS上で動作) が動作する物理サーバ台数分	Systemwalker Desktop Keeper 1クライアントライセンス for Windows	1
		合計：4

(購入例3) 仮想サーバと仮想クライアントが混在する場合



購入数の考え方	対象製品	購入数
Systemwalker Desktop Keeper V16が動作する仮想クライアントPCに接続する物理PC台数分	Systemwalker Desktop Keeper 1クライアントライセンス for Windows	3
仮想サーバ(Systemwalker Desktop Keeper V16がサーバOS上で動作)が動作する物理サーバ台数分	Systemwalker Desktop Keeper サーバライセンス for Windows	1

6. Citrix XenApp/Citrix Virtual Apps サーバ 運用時のライセンスについて

本商品を、Citrix XenApp/Citrix Virtual Appsの仮想端末での操作ログを採取するために導入する場合、Citrix XenApp/Citrix Virtual Appsサーバ台数分のSystemwalker Desktop Keeper for Citrix XenApp V16を購入してください。

(注) 管理サーバ/統合管理サーバとCitrix XenApp/Citrix Virtual Appsサーバは、同一マシンで運用することはできません。

7. ダウングレード使用について

本商品には、旧バージョン製品へのダウングレード使用権はありません。

8. 運用形態による購入例

以下のシステム構成の場合、購入対象商品の購入数は下記のようになります。

(1)ログ取得をしない場合

管理サーバ1台あたりクライアント5000台以下で構築してください。

[システム構成]

管理サーバ: 1台

クライアント: 5000台

[対象製品と購入数]

-Systemwalker Desktop Keeper メディアパック (64bit) V16.2.1 → 1本

-Systemwalker Desktop Keeper サーバライセンス for Windows (SL&S) → 1本

-Systemwalker Desktop Keeper 1000クライアントライセンス for Windows (SL&S) → 5本

(2)ログ取得をする、かつ、ログ分析機能を使用しない場合

管理サーバ1台あたりクライアント5000台以下で構築してください。
(1日あたりPC1台のログ数が1000ログの環境の場合)
[システム構成]
統合管理サーバ: 1台
管理サーバ: 1台
クライアント: 5000台
[対象製品と購入数]
-Systemwalker Desktop Keeper メディアパック (64bit) V16.2.1 → 1本
-Systemwalker Desktop Keeper サーバライセンス for Windows (SL&S) → 1本
-Systemwalker Desktop Keeper 1000クライアントライセンス for Windows (SL&S) → 5本

(3)ログ取得をする、かつ、ログ分析機能を使用する場合
[システム構成]
統合管理サーバ: 1台
管理サーバ: 2台
ログアナライザサーバ: 2台
クライアント: 10000台
[対象製品と購入数]
-Systemwalker Desktop Keeper メディアパック (64bit) V16.2.1 → 1本
-Systemwalker Desktop Keeper サーバライセンス for Windows (SL&S) → 3本
-Systemwalker Desktop Keeper 1000クライアントライセンス for Windows (SL&S) → 10本

(4)ログ取得をする、かつ、Citrix XenApp/Citrix Virtual Appsサーバ監視を行う場合
[システム構成]
統合管理サーバ: 1台
管理サーバ: 1台 (注1)
クライアント: 1000台
Citrix XenApp/Citrix Virtual Appsサーバ: 10台(注1)
[対象製品と購入数]
-Systemwalker Desktop Keeper メディアパック (64bit) V16.2.1 → 1本
-Systemwalker Desktop Keeper サーバライセンス for Windows (SL&S) → 2本
-Systemwalker Desktop Keeper 1000クライアントライセンス for Windows (SL&S) → 1本
-Systemwalker Desktop Keeper for Citrix XenApp for Windows (SL&S) → 10本
(注1)Citrix XenApp/Citrix Virtual AppsサーバとSystemwalker Desktop Keeper管理サーバは同居できません。

(5)ログ取得をする、かつ、インターネット環境からCTを接続して利用する場合
[システム構成]
統合管理サーバ: 1台
管理サーバ: 1台
クライアント: 1000台
ゲートウェイサーバ: 2台
[対象製品と購入数]
-Systemwalker Desktop Keeper メディアパック (64bit) V16.2.1 → 1本

-Systemwalker Desktop Keeper サーバライセンス for Windows (SL&S) → 2本

-Systemwalker Desktop Keeper 1000クライアントライセンス for Windows (SL&S) → 1本

-Systemwalker Desktop Keeper ゲートウェイサーバライセンス for Windows (SL&S) → 2本

9. サブスクリプションライセンス／サポートでの最新プログラムの提供について

サブスクリプションライセンス／サポート契約 の一環として、最新バージョン/レベルのプログラムを提供いたします。（お客様からのご要求が必要です。）

10. パッケージ構成について

Systemwalker Desktop Keeper メディアパックには、以下のプログラムおよびマニュアルが同梱されています。

- サーバプログラム(サーバ機能)
- クライアントプログラム(クライアント機能)
- オンラインマニュアル

11. VMware Horizon RDSH運用時のライセンスについて

本商品をVMware Horizon RDSHの役割をインストールした仮想端末で操作ログを採取するために導入する場合、VMware Horizon RDSHの役割をインストールしたWindowsサーバ台数分のSystemwalker Desktop Keeper for Citrix XenApp V16を購入してください。

(注) デバイスマッピングされたドライブに対するファイル操作ログは取得できません。

(注) 管理サーバ/統合管理サーバとCitrix XenApp/Citrix Virtual Appsサーバは、同一マシンで運用することはできません。

12. キャンペーン商品について

クライアントパソコンのセキュリティ環境を一括して管理する製品「Systemwalker Desktop Patrol」と、情報漏洩対策を行う製品「Systemwalker Desktop Keeper」の機能を、管理対象クライアント300台限定で使用できるセット商品を提供します。

なお、本商品は管理対象クライアント300台を超えてのご利用はできません。管理対象クライアント300台を超える場合は、通常の「Systemwalker Desktop Patrol」、「Systemwalker Desktop Keeper」をご利用ください。

13. 海外拠点端末の管理について

日本国内から海外拠点端末の管理を行う場合は、弊社営業／SEにお問い合わせください。

14. 購入時の特約事項

サブスクリプションライセンス／サポートの契約におけるライセンス使用条件の特約事項について記載します。

【V16.0.0以降】

[サーバライセンス for Windows (SL&S) に適用されるライセンス使用条件]

(1) 運用待機構成時

お客様が対象プログラムをインストールするコンピュータが、常時対象プログラムが稼働するコンピュータ（以下「運用系コンピュータ」といいます）と、運用系コンピュータが障害などの理由により使用できない場合にのみ対象プログラムが稼働するコンピュータ（以下「待機系コンピュータ」といいます）により構成されたシステムの場合は、1つのシステムを1台のコンピュータとみなします。その場合、お客様は、サブスクリプションライセンス／サポート製品のサービス仕様書記載の第3項「サービスの内容」第(1)号、またはライセンス条件説明書の第1項「基本的なご使用方法①」第(1)号により運用系コンピュータに対象プログラムをインストールして使用することに加え、待機系コンピュータに対して、サブスクリプションライセンス／サポート製品のサービス仕様書、またはライセンス条件説明書に定めるライセンス数分、対象プログラムをインストールして使用することができます。

(2) 一部機能の使用について

対象プログラムに含まれる機能の一部である、管理コンソール、レポート出力ツール、およびログアナライザサーバーについては、お客様は、サブスクリプションライセンス／サポート製品のサービス仕様書記載の第3項「サービスの内容」第(1)号、またはライセンス条件説明書の第1項「基本的なご使用方法①」第(1)号にかかわらず、日本国内において複数のコンピュータにインストールして使用することができます。

(3) オープンソースソフトウェア等について

本製品等のうち、富士通が別途定めるオープンソースソフトウェア等（以下「OSS」という）については、サブスクリプションライセンス／サポートのサービス仕様書、またはライセンス条件説明書に加えて、ソフトウェア説明書に記載されるライセンス条件が適用されます。ソフトウェア説明書に記載されるライセンス条件にサブスクリプションライセンス／サポートのサービス仕様書、またはライセンス条件説明書と異なる定めがある場合は、ソフトウェア説明書に記載されるライセンス条件の定めが優先して適用されるものとします。

(4) 改造について

サブスクリプションライセンス／サポート製品のサービス仕様書記載の第3項「サービスの内容」第(1)号i.、またはライセンス条件説明書記載の第5項「共通事項」第(4)号を下記のとおり変更するものとします。なお本項により変更された条項以外の条項は、有効に存続するものとします。

「お客様は、対象プログラムについて、改造したり、逆アセンブル、逆コンパイルを伴うリバースエンジニアリングを行うことはできません。ただし、本製品等のうちソフトウェア説明書に特定されたプログラムについては、本製品等とともに使用するオープンソースソフトウェアに適用されるGNU LESSER GENERAL PUBLIC LICENSEにより許される範囲に限り、改変を行えるものとします。」

[for Citrix XenApp for Windows (SL&S) / ゲートウェイサーバライセンス for Windows (SL&S)に適用されるライセンス使用条件]

(1) 運用待機構成時

お客様が対象プログラムをインストールするコンピュータが、常時対象プログラムが稼働するコンピュータ（以下「運用系コンピュータ」といいます）と、運用系コンピュータが障害などの理由により使用できない場合にのみ対象プログラムが稼働するコンピュータ（以下「待機系コンピュータ」といいます）により構成されたシステムの場合は、1つのシステムを1台のコンピュータとみなします。その場合、お客様は、サブスクリプションライセンス／サポート製品のサービス仕様書記載の第3項「サービスの内容」第(1)号、またはライセンス条件説明書の第1項「基本的なご使用方法①」第(1)号により運用系コンピュータに対象プログラムをインストールして使用することに加え、待機系コンピュータに対して、サブスクリプションライセンス／サポート製品のサービス仕様書、またはライセンス条件説明書に定めるライセンス数分、対象プログラムをインストールして使用することができます。

(2) オープンソースソフトウェア等について

本製品等のうち、富士通が別途定めるオープンソースソフトウェア等（以下「OSS」という）については、サブスクリプションライセンス／サポートのサービス仕書、またはライセンス条件説明書に加えて、ソフトウェア説明書に記載されるライセンス条件が適用されます。ソフトウェア説明書に記載されるライセンス条件にサブスクリプションライセンス／サポートのサービス仕様書、またはライセンス条件説明書と異なる定めがある場合は、ソフトウェア説明書に記載されるライセンス条件の定めが優先して適用されるものとします。

(3) 改造について

サブスクリプションライセンス／サポート製品のサービス仕様書記載の第3項「サービスの内容」第(1)号i.、またはライセンス条件説明書記載の第5項「共通事項」第(4)号を下記のとおり変更するものとします。なお本項により変更された条項以外の条項は、有効に存続するものとします。

「お客様は、対象プログラムについて、改造したり、逆アセンブル、逆コンパイルを伴うリバースエンジニアリングを行うことはできません。ただし、本製品等のうちソフトウェア説明書に特定されたプログラムについては、本製品等とともに使用するオープンソースソフトウェアに適用されるGNU LESSER GENERAL PUBLIC LICENSEにより許される範囲に限り、改変を行えるものとします。」

【V16.2.1以降】

[1クライアントライセンス for Windows (SL&S) / 10クライアントライセンス for Windows (SL&S) / 100クライアントライセンス for Windows (SL&S) / 500クライアントライセンス for Windows (SL&S) / 1000クライアントライセンス for Windows (SL&S)に適用されるライセンス使用条件]

(1) オープンソースソフトウェア等について

本製品等のうち、富士通が別途定めるオープンソースソフトウェア等（以下「OSS」という）については、サブスクリプションライセンス／サポートのサービス仕書、またはライセンス条件説明書に加えて、ソフトウェア説明書に記載されるライセンス条件が適用されます。ソフトウェア説明書に記載されるライセンス条件にサブスクリプションライセンス／サポートのサービス仕様書、またはライセンス条件説明書と異なる定めがある場合は、ソフトウェア説明書に記載されるライセンス条件の定めが優先して適用されるものとします。

(2) 改造について

サブスクリプションライセンス／サポート製品のサービス仕様書記載の第3項「サービスの内容」第(1)号i.、またはライセンス条件説明書記載の第5項「共通事項」第(4)号を下記のとおり変更するものとします。なお本項により変更された条項以外の条項は、有効に存続するものとします。

「お客様は、対象プログラムについて、改造したり、逆アセンブル、逆コンパイルを伴うリバースエンジニアリングを行うことはできません。ただし、本製品等のうちソフトウェア説明書に特定されたプログラムについては、本製品等とともに使用するオープンソースソフトウェアに適用されるGNU LESSER GENERAL PUBLIC LICENSEにより許される範囲に限り、改変を行えるものとします。」

【V16.0.0～V16.2.0】

[1クライアントライセンス for Windows (SL&S) / 10クライアントライセンス for Windows (SL&S) / 100クライアントライセンス for Windows (SL&S) / 500クライアントライセンス for Windows (SL&S) / 1000クライアントライセンス for Windows (SL&S)に適用されるライセンス使用条件]

特約事項の適用なし。

関連ソフト

1. Systemwalker Desktop Patrol と連携して構成定義の簡易化を行う場合

資産管理ソフトウェアと連携して構成定義の簡易化を行う場合は、以下の商品が必要です。

・Systemwalker Desktop Patrol V15.1.3以降

2. VMware Horizon RDSH/Citrix XenApp/Citrix Virtual Appsの仮想端末上での操作ログを採取する場合

VMware Horizon RDSH/Citrix XenApp 監視をCitrix XenApp/Citrix Virtual Appsの仮想端末上での操作ログを収集する場合には、以下のソフトウェアと組み合わせください。

・Citrix XenApp 7.15 LTSR/7.6 LTSR

・Citrix Virtual Apps and Desktops 1912 LTSR、2203 LTSR、2308/2311/2402 LTSR/2407

・VMware Horizon RDSH 7.13 ESB、8.0
2006/2012/2103/2106/2111/2203/2206/2209/2212/2303/2306/2309/2312/2406

(注) 別途Systemwalker Desktop Keeper for Citrix XenApp V16が必要

3. 暗号化ファイルの送信、保存について

Systemwalker Desktop Keeperのメール添付抑止機能を使用して、Systemwalker Desktop Keeperのファイル持出しユーティリティで作成された暗号化ファイルを使用しないで暗号化ファイルだけを送信または保存可能とする場合、以下のいずれかのソフトウェアが必要です。

・SecureBOX V2.0/V2.1

・Fence Pro V5/V6

4. レポート出力機能について

レポート出力機能を使用する場合には、以下のいずれかのソフトウェアが必要です。(「Web版」を除きます。)

・Microsoft Excel 2016

・Microsoft Excel 2019

・Microsoft Excel 2021

・Microsoft Excel 2024

・Excel for Microsoft 365(旧称Office 365)

5. Sense YOU Technology Bizと連携する場合

Sense YOU Technology Bizによる覗き見検知時および他人検知時に、クライアント(CT)のデスクトップ画面のハードコピーをログとして取得する場合、以下のソフトウェアが必要です。

Sense YOU Technology Biz

動作保証周辺機器

1. iNetSec SF

iNetSec SFと連携することにより、iNetSec SFがマルウェアを検知するとネットワークを遮断し、管理サーバ/統合管理サーバへ通知を行います。さらに、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可能です。

留意事項

1. Windows サーバOS (64-bit)上での動作

本商品の統合管理サーバ/管理サーバ/ログアナライザサーバは、以下のOS上で64ビットアプリケーションとして動作します。 (注1)

- Windows Server 2016 (64-bit)
- Windows Server 2019 (64-bit)
- Windows Server 2022 (64-bit)

(注1) 統合管理サーバ/管理サーバ/ログアナライザサーバ以外は、WOW64(注)サブシステム上で、32ビットアプリケーションとして動作します。

注：Windows 32-bit On Windows 64-bit

2. Windows デスクトップOS (64-bit)上での動作について

本商品の管理コンソール、クライアント、レポート出力ツールは、以下のOSのWOW64(注)サブシステム上で、32ビットアプリケーションとして動作します。

- Windows 10 (64-bit)
- Windows 11 (64-bit)

注：Windows 32-bit On Windows 64-bit

3. Hyper-VのゲストOS上での動作について

ゲストOSでSystemwalker Desktop Keeperのクライアントを動かす場合、Hyper-Vが動作するホストOSでSystemwalker Desktop Keeper のクライアントが動作していれば、以下の機能はホストOSでのポリシー 設定にしたがいます。

- 外部記憶媒体への持出し抑止
- ファイル持出しユーティリティによる書き込み

4. 統合管理サーバ、管理サーバ、クライアントについて

Systemwalker Desktop Keeper 統合管理サーバと管理サーバは同一のバージョン、レベル、エディションを使用してください。

Systemwalker Desktop Keeper 統合管理サーバと管理サーバはクライアントより上位のバージョン、レベル、エディションを使用してください。

ただし、使用できる機能は、各クライアントのバージョンレベルの機能範囲となります。

5. NAT環境で利用する時の注意

統合管理サーバ/管理サーバとクライアント間がNAT(Network Address Translation)で構成されている環境では、以下の通信は行えません。

- 管理サーバ/統合管理サーバからクライアント(CT)に対するポリシーの即時送信
- 管理サーバ/統合管理サーバからクライアント(CT)に対するリモート資料採取
- 管理サーバ/統合管理サーバからクライアント(CT)に対するCTデバッグトレースの設定
- 管理サーバ/統合管理サーバからクライアント(CT)に対するサービス一覧取得/サービス制御
- 管理サーバ/統合管理サーバからクライアント(CT)に対するプロセス一覧取得/プロセス制御
- V15.0以前のクライアント(CT)から管理サーバ/統合管理サーバに対する自己版数管理機能の通信

(注) CTがインストール時に指定する中継サーバのアドレス(実際にアクセスするアドレス)と中継サーバでセキュア通信用に生成する証明書のサブジェクトが一致していない場合、通信することができません。

6. リモートデスクトップ接続を行う場合の注意

V13.2以前からバージョンアップ、またはレベルアップした環境で、リモートデスクトップ接続による、以下の機能は使用できません。

- 運用環境保守ウィザード(環境構築・削除)
- 運用環境保守ウィザード(情報開示・再構築)
- バックアップツール
- バックアップコマンド
- リストアツール

7. 混在運用できない製品について

本商品の混在運用できない製品に関する情報は、マニュアル「Systemwalker Desktop Keeper 解説書」をご覧ください。

マニュアルについては、「関連URL」に記載の「ソフトウェア：富士通（マニュアル）」を参照してください。

8. 仮想環境での運用について

(1)対応製品

以下の製品に対応しています。

- VMware vSphere 7.0/8.0
- VMware Horizon 7.13 ESB、8 2006/2012/2103/2106/2111/2203/2206/2209/2212/2303/2306/2309/2312/2406
- Citrix XenDesktop 7.15LTSR、7.6 LTSR
- Citrix Virtual Apps and Desktops 1912 LTSR、2203 LTSR、2308/2311/2402 LTSR/2407
- Microsoft Hyper-V
- KVM
- VMware Horizon RDSH 7.13 ESB、8 2006/2012/2103/2106/2111/2203/2206/2209/2212/2303/2306/2309/2312/2406(注)

(注) 別途Systemwalker Desktop Keeper for Citrix XenApp V16が必要

(2)仮想環境での運用における留意事項

- USBデバイス個体識別機能は動作しません。
- 上記対応製品を仮想環境で運用する場合は、PC台数分のクライアントライセンスをご購入ください。

9. サーバの階層管理を行う場合について

統合管理サーバによる管理サーバの階層管理を行う場合、1台の統合管理サーバで管理できるサーバ台数は10台を目安としてください。

10. IPv6での通信

以下のOSでIPv6での通信に対応します。

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

11. インストールについて

本商品はDVDで提供されます。

インストールにはDVDドライブユニットが必要です。

DVDドライブユニットが搭載されていないマシンの場合は別途手配が必要です。

DVDドライブユニットを入手できない場合は、Windowsのファイル共有を利用したネットワークインストールが可能です。

(ただし、ローカルのDVDドライブユニットと比べて作業時間を要します。)

12. Systemwalker Desktop Keeperで扱う文字コードについて

Systemwalker Desktop Keeperで扱える文字コードは、Shift JIS/ UNICODE（JIS X 0213:2004を含む）の2種類です。以下の注意事項があります。

- ログアナライザサーバでの注意事項

ログアナライザサーバで設定する文字列(インストールパスやフォルダパス、ユーザーID/パスワードなど)に、Shift JIS以外の文字(JIS X 0213:2004を含めて、Shift JISに対応コードを持たないUNICODE文字など)は使用できません。また、Windowsへのログオン時のユーザー名にも、Shift JIS以外の文字は使用できません。

- クライアント(CT)の持出しユーティリティでの注意事項

Windowsへのログオン時のユーザー名にUNICODE文字が含まれる場合、持出しユーティリティを使用してDVD/CDメディアへの暗号化持出しはできません。

持出しユーティリティの以下の持出しにおいては、持出し元、持出し先ともに、ファイル名、フォルダ名にUNICODE文字を指定できません。

・DVD/CDへの通常持出し、暗号化持出し

・DVD/CD以外への暗号化持出し

- 管理サーバ/統合管理サーバ/中継サーバにインストールされるツール/コマンド、およびポリシー適用ツールでの注意事項

Windowsへのログオン時のユーザー名にUNICODE文字を使用しないでください。正常に動作しない場合があります。

- 上記および管理コンソール以外のツールやコマンドでは、UNICODE文字の入力、表示はできません。

13. 対応パブリッククラウドについて

パブリッククラウドのご利用にあたっては、弊社営業／SEにお問い合わせください。

14. 「新しいOutlook」について

Systemwalker Desktop Keeperの禁止機能、記録機能において、「新しいOutlook」は動作保証外です。

15. 標的型攻撃への対応におけるWindows Defenderとの連携について

Windows Defenderによるセキュリティリスク検知時のクライアント(CT)への緊急対処については、2024年12月からサポート対象外となりました。

16. Systemwalker Desktop Keeper for Standaloneについて

Systemwalker Desktop Keeper for Standaloneのご利用を検討の場合、Systemwalker Desktop Keeper for Standaloneの機能、導入、運用に関する情報は、マニュアル「Systemwalker Desktop Keeper ユーザーズガイド」をご覧ください。

マニュアルについては、「関連URL」に記載の「ソフトウェア：富士通（マニュアル）」を参照してください。

17. 前版との差異について

Windows Defenderによるセキュリティリスク検知時のクライアント(CT)への緊急対処について、サポート対象外となりました。

関連URL

お客様向けURL

- **ソフトウェア：富士通（Systemwalker Desktop Keeper）**

  製品概要や動作環境、導入事例、価格等、製品紹介資料を幅広く提供しております。
  https://www.fujitsu.com/jp/software/systemwalker/desktop-keeper/

- **ソフトウェア：富士通（ソフトウェアの一覧表（システム構成図）と各種対応状況）**

  価格/型名の一覧（システム構成図）を提供しております。
  https://www.fujitsu.com/jp/products/software/resources/condition/configuration/

- **ソフトウェア：富士通（インフォメーション&ダウンロード）**

  「ライセンスについて、くわしく知る」の項で

  富士通製ミドルウェア製品のライセンスに関する解説、サポート期間などの情報を提供しております。
  https://www.fujitsu.com/jp/products/software/information-download/

- **ソフトウェア：富士通（マニュアル）**

  富士通のソフトウェア製品に添付されているマニュアルが閲覧できます。
  https://www.fujitsu.com/jp/products/software/resources/manual/