FUJITSU

FUJITSU Software
Systemwalker Desktop Patrol

解説書

Windows

B1WD-3549-01Z0(00)
2022年3月

まえがき

本書の目的

本書は、以下の製品の紹介、機能概要、および製品を使用する上での必要な知識について説明しています。

- Systemwalker Desktop Patrol V16.0.0

Systemwalkerとは、富士通株式会社が提供する分散システムの運用管理製品の総称です。

本書の読者

本書は、以下のような読者を対象に書かれています。

- Systemwalker Desktop Patrolの導入を検討している方
- Systemwalker Desktop Patrolがどういう製品か知りたい方
- Systemwalker Desktop Patrolの機能概要を知りたい方
- Systemwalker Desktop Patrolを使用するために何が必要かを知りたい方

また、本書を読むためには、以下の知識が必要です。

- パーソナルコンピュータに関する一般的な知識
- Windowsに関する一般的な知識
- インターネットに関する一般的な知識

本書の構成

本書の構成は、以下のとおりです。

第1章 Systemwalker Desktop Patrolの概要

Systemwalkerの製品体系での、Systemwalker Desktop Patrolの位置付けや、Systemwalker Desktop Patrolの導入効果および特長について説明しています。

また、Systemwalker Desktop Patrolを使用する時に、必要な知識、考え方について説明しています。

第2章 Systemwalker Desktop Patrolの機能

Systemwalker Desktop Patrolの機能について説明しています。

第3章 動作環境

Systemwalker Desktop Patrolを動作させるために必要な環境について説明しています。

第4章 他製品との連携

Systemwalker Desktop Patrolと他製品との連携方法について説明します。

用語集

Systemwalker Desktop Patrolで使用されている各用語について説明しています。

本書の位置づけ

Systemwalker Desktop Patrolのマニュアルにおける本書の位置づけは、以下のとおりです。

マニュアル名称	内容
リリース情報	Systemwalker Desktop Patrolの追加機能、および非互換項目について説明します。

マニュアル名称	内容
解説書(本書)	Systemwalker Desktop Patrolの概要、特長、機能など、基本的な知識について説明します。
導入ガイド	Systemwalker Desktop Patrolの導入方法、動作環境の変更方法、および保守について説明します。
運用ガイド 管理者編	Systemwalker Desktop PatrolのPC情報の収集、セキュリティパッチの適用、ソフトウェア配信、ライセンス管理、ディスク消去管理、および管理台帳の運用方法および環境設定について説明します。
運用ガイド クライアント編	クライアント側の導入方法、操作方法、設定の変更方法について説明します。また、クライアントで出力されるエラーメッセージの対処方法も説明します。
リファレンスマニュアル	Systemwalker Desktop Patrolで使用するコマンド、ファイル、およびポート番号について説明します。また、Systemwalker Desktop Patrolが出力するエラーメッセージの対処方法も説明します。
トラブルシューティングガイド	Systemwalker Desktop Patrolで想定されるトラブルの原因と対処方法について説明します。

また、Systemwalker Live Helpのマニュアルとして、以下のマニュアルが同梱されています。リモート操作機能(Systemwalker Live Helpの機能)を使用する場合に参照してください。

マニュアル名称	内容
Systemwalker Live Help ユーザーズガイド	Systemwalker Live Helpのインストール方法、ハードウェアとソフトウェア用件、使用方法、サポートセンター関連の設定方法を説明します。また、Live Help Connection Manager管理の方法についても説明しています。
Systemwalker Live Help Clientガイド	Systemwalker Live Help Clientのインストール方法、使用方法、設定方法について説明します。

ソフトウェア技術情報ホームページでは、最新のマニュアルやSystemwalkerの応用方法などを公開しています。最初に、ソフトウェア技術情報ホームページを参照することをお勧めします。

ソフトウェア技術情報 URL :

https://www.fujitsu.com/jp/software/technical/

Systemwalker Desktop Patrol 技術情報 URL :

https://www.fujitsu.com/jp/software/technical/systemwalker/desktoppatrol/

本書の表記について

本書では、説明のために、以下に示す名称、記号および略称を使用しています。

コマンドで使用する記号について

コマンドで使用している記号について以下に説明します。

記号の意味

記 号	意 味
[ ]	この記号で囲まれた項目を省略できることを示します。
|	この記号を区切りとして並べられた項目の中から、どれか1つを選択することを示します。
{ }	この記号で囲まれた項目の中から、どれか1つを選択することを示します。

マニュアルの記号について

マニュアルでは以下の記号を使用しています。

注意

特に注意が必要な事項を説明しています。

ポイント

知っておくと便利な情報を説明しています。

DTPインストールディレクトリについて

「Systemwalker Desktop Patrol CS」、「Systemwalker Desktop Patrol DS」、「Systemwalker Desktop Patrol AC」、「Systemwalker Desktop Patrol ADT」、「Systemwalker Desktop Patrol AT」、「Systemwalker Desktop Patrol CT」、または「Systemwalker Desktop Patrol SS」をインストールしたときの、インストール先のディレクトリをDTPインストールディレクトリと表示しています。

略称について

本書では、製品表示名をそれぞれ以下のように略称している箇所があります。

製品表示名	略称
Systemwalker Desktop Patrol CS	CS
Systemwalker Desktop Patrol DS	DS
Systemwalker Desktop Patrol AC	AC
Systemwalker Desktop Patrol ADT	ADT
Systemwalker Desktop Patrol AT	AT
Systemwalker Desktop Patrol CT	CT
Systemwalker Desktop Patrol SS	SS

本書では、以下のようにオペレーティングシステム名を略して表記しています。

略称	正式名称
Windows Server 2019	Microsoft® Windows Server® 2019 Datacenter Microsoft® Windows Server® 2019 Standard Microsoft® Windows Server® 2019 Essentials
Windows Server 2016	Microsoft® Windows Server® 2016 Datacenter Microsoft® Windows Server® 2016 Standard Microsoft® Windows Server® 2016 Essentials
Windows Server 2012 R2	Microsoft® Windows Server® 2012 R2 Standard Microsoft® Windows Server® 2012 R2 Essentials Microsoft® Windows Server® 2012 R2 Foundation Microsoft® Windows Server® 2012 R2 Datacenter
Windows Server 2012	Microsoft® Windows Server® 2012 Standard Microsoft® Windows Server® 2012 Essentials Microsoft® Windows Server® 2012 Foundation Microsoft® Windows Server® 2012 Datacenter Microsoft® Windows Server® 2012 R2 Standard Microsoft® Windows Server® 2012 R2 Essentials

略称	正式名称
	Microsoft® Windows Server® 2012 R2 Foundation Microsoft® Windows Server® 2012 R2 Datacenter
Windows 11	Windows® 11 Home Windows® 11 Pro (注1) Windows® 11 Enterprise Windows® 11 Education
Windows 10	Windows® 10 Home Windows® 10 Pro (注2) Windows® 10 Enterprise Windows® 10 Education Windows® 10 Home 64ビット版 Windows® 10 Pro 64ビット版 (注2) Windows® 10 Enterprise 64ビット版 Windows® 10 Education 64ビット版
Windows 8.1	Windows® 8.1 Windows® 8.1 Pro Windows® 8.1 Enterprise Windows® 8.1 64ビット版 Windows® 8.1 Pro 64ビット版 Windows® 8.1 Enterprise 64ビット版
Windows	Microsoft® Windows Server® 2019 Datacenter Microsoft® Windows Server® 2019 Standard Microsoft® Windows Server® 2019 Essentials Microsoft® Windows Server® 2016 Datacenter Microsoft® Windows Server® 2016 Standard Microsoft® Windows Server® 2016 Essentials Microsoft® Windows Server® 2012 R2 Standard Microsoft® Windows Server® 2012 R2 Essentials Microsoft® Windows Server® 2012 R2 Foundation Microsoft® Windows Server® 2012 R2 Datacenter Microsoft® Windows Server® 2012 Standard Microsoft® Windows Server® 2012 Essentials Microsoft® Windows Server® 2012 Foundation Microsoft® Windows Server® 2012 Datacenter Windows® 11 Home Windows® 11 Pro (注1) Windows® 11 Enterprise Windows® 11 Education Windows® 10 Home Windows® 10 Pro (注2) Windows® 10 Enterprise Windows® 10 Education Windows® 10 Home 64ビット版 Windows® 10 Pro 64ビット版 (注2) Windows® 10 Enterprise 64ビット版 Windows® 10 Education 64ビット版 Windows® 8.1 Windows® 8.1 Pro Windows® 8.1 Enterprise Windows® 8.1 64ビット版 Windows® 8.1 Pro 64ビット版 Windows® 8.1 Enterprise 64ビット版

略称	正式名称
IIS	Internet Information Services 8.0 Internet Information Services 8.5 Internet Information Services 10.0
IE	Windows® Internet Explorer® 11
Edge	Microsoft Edge™

注1）Windows® 10 Pro for Workstationsにも対応しています。

注2）Windows® 11 Pro for Workstationsにも対応しています。

Windows 8.1およびWindows Server 2012の[スタート]画面のショートカットについて

[スタート]画面のショートカットがどの製品のものかを確認するためには、対象のショートカットを右クリックし、画面に表示されるメニューから[ファイルの場所を開く]を選択してください。表示されるエクスプローラから、製品名を確認することができます。

半角文字について

本書において、半角文字として扱える文字の制限を記述している箇所を除き、半角文字として扱う文字とは、以下のASCII文字のことを指します。

- 半角空白
- 半角記号

  「!」、「"」、「#」、「$」、「%」、「&」、「'」、「(」、「)」、「*」、「+」、「,」、「-」、「.」、「/」、「:」、「;」、「<」、「=」、「>」、「?」、「@」、「[」、「¥」、「]」、「^」、「_」、「`」、「{」、「|」、「}」、「~」
- 半角数字

  「0」「1」・・・「9」
- 半角英字

  「A」「B」・・・「Z」

  「a」「b」・・・「z」

上記の以外の文字は全角文字として扱います。

輸出管理規制について

本ドキュメントを輸出または第三者へ提供する場合は、お客様が居住する国および米国輸出管理関連法規等の規制をご確認のうえ、必要な手続きをおとりください。

商標について

NETM/DMは株式会社日立製作所の商標です。

Google、Googleロゴ、GmailおよびGmailロゴは、Google Inc. の商標または登録商標です。

Wi-Fiは、Wi-Fi Allianceの登録商標です。

その他のすべての商標は、それぞれの所有者に帰属します。

Microsoft Corporationのガイドラインに従って画面写真を使用しています。

2022年3月

改版履歴
2013年 8月 初 版
2014年 2月 第2版
2014年 3月 第3版
2015年 2月 第4版
2015年11月 第5版
2016年10月 第5.1版
2017年 2月 第6版
2017年12月 第7版
2018年12月 第8版
2019年 3月 第9版
2020年 2月 第10版
2021年 1月 第11版
2021年 2月 第11.1版
2021年 4月 第11.2版
2022年 3月 第12版

目　次

第1章 Systemwalker Desktop Patrolの概要

本章では、Systemwalkerの製品体系での、Systemwalker Desktop Patrolの位置付け、Systemwalker Desktop Patrolの導入効果および特長を説明します。

1.1 製品の位置付け

Systemwalker Desktop シリーズのコンセプト、およびSystemwalker Desktop Patrolの位置付けについて説明します。

Systemwalker Desktopシリーズコンセプト

Systemwalker Desktopシリーズは、資産を把握し、業務の内容や環境によるリスクに応じてセキュリティパッチの適用、パソコンの操作制限、ログ収集/分析、ファイル操作制限、不正パソコンの遮断等のセキュリティ対策に加え、グリーンICT対策を実現するための製品群です。

Systemwalker Desktop Patrolの位置づけ

Systemwalker Desktop Patrolは、パソコン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まで簡単に適用できるICT資産管理ソフトウェアです。Systemwalker Desktop Patrolにより、高いセキュリティ性を保持できる環境を提供した上で、PCの消費電力の削減、ソフトウェア資産の有効利用によるTCO削減、ファイルのダウンロード、廃棄PCのデータ消去、クライアントへの遠隔操作による運用効率化を実現します。

また、Systemwalker Desktop Patrolで収集した情報やExcelなどの外部で管理されていたICT資産情報を台帳として管理することにより、ICT全般統制の実現（システムの正しい運用の実現とその証明／監査）を強力に支援します。

グリーンICT対策

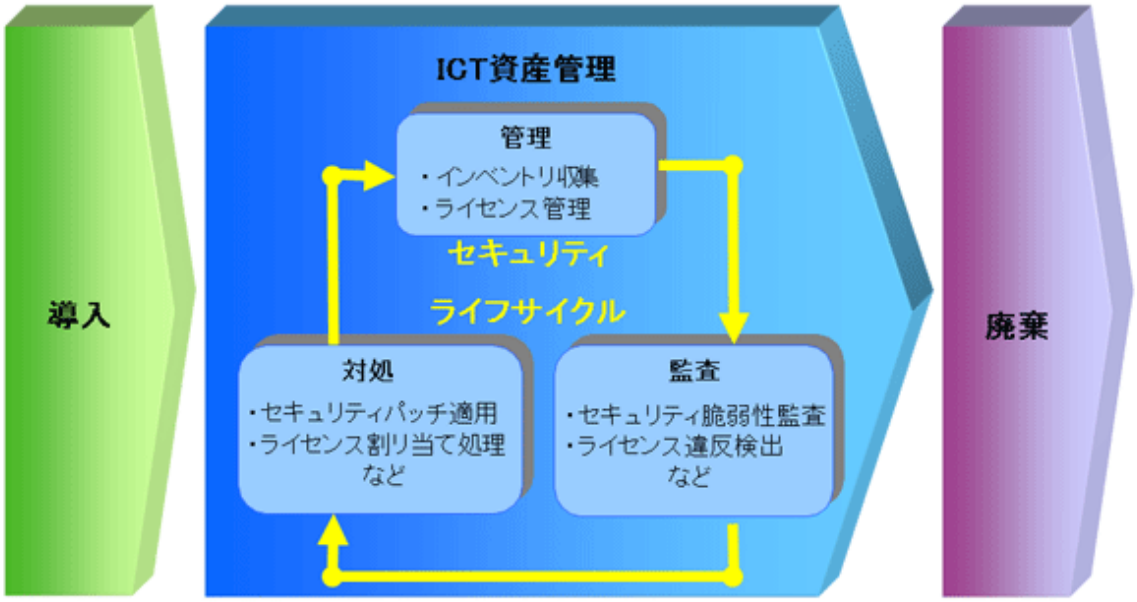
環境問題の深刻化により、環境保護への意識の高まり、また省エネ法の改正によりオフィスでのエネルギー消費の実態の把握・改善が企業に求められています。Systemwalker Desktop Patrolは、従来のクライアント管理機能に加え、PCのムダな消費電力を削減するための機能を提供することにより、オフィスのグリーンICTを支援し、CO2排出量の低減に貢献します。

全社または部門単位の利用形態に合わせてパソコンの省電力ポリシーを設定し、ポリシーに違反したパソコンの設定を強制的に変更して、省電力状態を維持します。これにより、パソコンの電力の浪費を抑制し、消費電力削減に貢献します。

セキュリティ管理

インターネットがビジネスに不可欠になった現在、機密情報・個人情報の流出防止と不正アクセスやコンピュータウイルス感染などからシステムを守る情報セキュリティ対策が最重要課題になってきています。Systemwalker セキュリティ管理ソリューションは、パソコンなどのエンドポイントからの重要なデータの流出防止や、ユーザー認証による安全な情報流通を実現します。さらに、各種セキュリティ製品を1つに束ねて統合管理することにより、セキュリティ運用の負担を軽減できます。

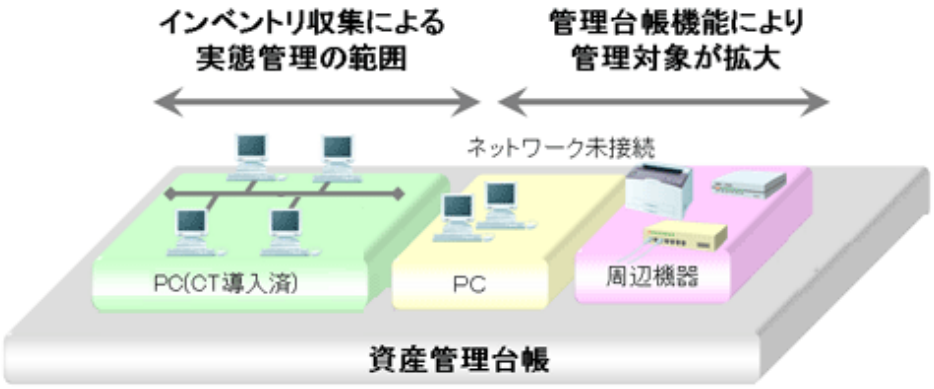
Systemwalker Desktop Patrolでは、情報漏洩対策機能を強化し、ICT資産をセキュリティ上の脅威から守ります。これにより、導入から廃棄までの流れの中で、安全なセキュリティライフサイクルを維持できます。



台帳による資産管理

企業におけるパソコンの普及に伴い、TCO（Total Cost of Ownership：総所有管理経費）最適化への取り組み、違法コピー対策、ウイルス対策、セキュリティ対策、予算策定などを適切に行うためには、システム運用者、経理担当者、部門の情報担当者など、多方面の管理者が資産の実際の利用状況を正確に把握できる環境が必要です。Systemwalker資産管理ソリューションは、資産の実態情報を正確に把握し、遊休ライセンスの有効利用や一括購入によるコスト削減が可能です。

Systemwalker Desktop Patrolでは、クライアントセキュリティ管理に加えて、機器（PCおよび什器）の資産管理の機能を提供します。これにより、機器（PCおよび什器）の資産管理、運用管理、およびセキュリティ監査をトータルにサポートできます。



1.2 特長

企業にとってICT投資は、戦略的に重要な投資です。ICT投資には、ハードウェアやソフトウェアといった資産コストそのものもありますが、トラブル対応、ハードウェアの所在管理、ソフトウェアの導入、ライセンス管理、セキュリティパッチの適用、情報漏洩の防止など、目に見えないコストもあります。これらの投資が無駄なく、投資対効果のバランスのとれたものであることが望まれます。

また、近年のPCの導入は、大変な勢いで進んでおり、その管理もユーザー任せになっています。このため、「ウイルス感染した」、「ライセンスの監査がはいった」といった事態が発生したとき、PCの管理責任者は、「PCの購入台帳はあるがその実態がまったく分からない」、「ヘルプ依頼がきているがとても現場を回りきれない」といった状態に陥ることが多々有り、これらの問題を簡単に解決するツールに期待が寄せられています。

さらに、機器（PCおよび什器）資産管理は、クライアントセキュリティ管理に加えて、企業運営での重要な課題です。

機器（PCおよび什器）資産管理には、資産情報の台帳の管理、機器のリース/レンタル契約の管理、全社資産の運用状況の管理などがあります。例えば、機器ごとの利用者や設置場所の管理やリース/レンタル契約終了日の管理などは、機器が増大するにつれて業務の負担も増加するため、このような管理業務を簡単に行うツールに期待が寄せられています。

法改正により内部統制が義務付けられ、内部統制の監査基準として、業務の有効性・効率性、財務報告の信頼性、法令遵守、および資産の保全が求められるようになります。

Systemwalker Desktop Patrolは、以下のような特長をもっています。

簡単な導入

専門家がサポートしなくても簡単に導入できます。

様々な環境に対応

数台のPCを使用した小規模なシステムを構築されているお客様から、全社レベルの大規模なシステムを構築されているお客様まで、柔軟に対応できます。

PCの資産を管理することが可能

- ハードウェアやソフトウェアの利用状況が簡単に把握できます。
- ソフトウェアのライセンス管理が簡単に行えます。

ICT資産の一元管理

PCや複合機/プリンタなどのICT資産の設置場所・台数・利用実態を資産情報レポートで確認でき、無駄なコストを削減できます。

自動収集したインベントリ情報から、管理者が資産情報の登録/更新/削除を行うことができ、変更履歴も管理できます。

資産管理台帳による定期的な棚卸

定期的な棚卸により、機器の盗難や紛失を検知し、ICT資産の保全を図ります。現状を短時間で確実に把握することで、資産運用を見直し、適切な投資を行うことができます。

省電力状態を維持することが可能

管理者がPCの「電源オプション」設定を一括管理し、全社または部門単位の利用形態に合わせて省電力ポリシーとして設定できます。

省電力ポリシーに違反したPCは、利用者に警告画面を表示したり、強制的に設定を変更することで、PCの省電力状態を維持できます。

セキュリティを維持・向上することが可能

- セキュリティパッチやウイルス定義ファイルの適用状況を簡単に監査できます。
- セキュリティパッチを自動取得、自動適用できます。セキュリティパッチの適用が不十分なPCに対して、管理者が強制的にパッチを適用することもできます。
- システムのセキュリティ状況、ログインユーザーのセキュリティ状況など、セキュリティ対策状況を簡単に監査できます。管理者が設定したセキュリティポリシーに違反したPCは、利用者に警告画面を表示したり、強制的に設定を変更することで、PCのセキュリティを維持することができます。

情報漏洩の抑止

リース期限切れPCの返却やPCの入れ替えで発生する廃棄PCに対し、ハードディスクの情報を消去して情報の漏洩を防ぎます。

管理者の負担を軽減

- トラブル時のEnd-to-Endの管理が簡単に行えます。
- 遠隔地にあるPCをリモートで操作できます。
- ほとんどの管理機能は、Webブラウザから行えます。

1.3 システム構成

Systemwalker Desktop Patrolを使用する場合の基本的なシステム構成について説明します。

1.3.1 Systemwalker Desktop Patrolを構成するコンポーネント

Systemwalker Desktop Patrolは、以下のコンポーネントにより構成されています。

Systemwalker Desktop Patrol CS（Corporate Server）

インベントリ情報の収集条件やソフトウェア配信の運用条件をポリシーとして定義し、各PCに配信するサービスを受け持つサーバです。

ICT資産の情報(ICTリポジトリ)、人、組織などの組織情報を格納したデータベースにより、セキュリティパッチの配信、セキュリティの監査やライセンスの管理をWebブラウザから行うサービス（Web GUI）を提供します。通常は企業に1台導入されます。

Systemwalker Desktop Patrol AC（Asset Console）

資産、セキュリティ、省電力などの各種レポートの出力やバーコードの出力などを行う管理者用コンソールです。

Systemwalker Desktop Patrol DS（Domain Server）

運用ポリシー、インベントリ情報、配信ソフトウェアなどの集配信の中継／格納をサービスするサーバです。

負荷分散するためなどの目的のために設置します。クライアントが遠隔地にあり、低速回線の場合、または配信するソフトウェアの容量が大きい場合などに有効です。

Systemwalker Desktop Patrol AT（Asset Terminal）

資産情報から作成したバーコードラベルを読み込み、資産の棚卸や資産情報の確認を行う専用端末です。

Systemwalker Desktop Patrol ADT（Auto Detection Terminal）

セグメント毎に設置し、同一セグメント内のネットワークに接続されている機器を自動検知します。また、検知した機器の情報を、管理サーバ(CS) に通知します。

Systemwalker Desktop Patrol CT（Client Terminal）

管理されるクライアントです。インベントリ収集により資産を管理するPCに導入します。「Systemwalker Desktop Patrol CT」で、配信ソフトウェアのダウンロード、セキュリティパッチの受信を行います。

また、管理者の設定により、省電力ポリシーの違反、セキュリティポリシーの違反があると、対処を促す画面が表示されます。

Web GUI

「Systemwalker Desktop Patrol CS」が提供するサービスを利用し、WebブラウザからSystemwalker Desktop Patrolの運用操作を行うための操作ビューです。

また、Systemwalker Desktop Patrolのポリシーを設定できます。

Web GUIには、「メインメニュー」および「ダウンロードメニュー」があります。

Systemwalker Desktop Patrol SS（Secure server[ゲートウェイサーバ]）

インターネットで使用可能な、セキュア通信を行えるCT（以降、セキュア版CTと呼びます）の接続を受け付けるための中継サーバです。

セキュア版CTを管理する場合に、導入が必要なサーバです。

Live Help Expert

「Live Help Client」をリモート操作するためのソフトウェアです。クライアントユーザーが、PCの操作に困っている場合などで、直接クライアントユーザーのPCに接続して、支援できます。

詳細は、Systemwalker Live Helpのマニュアルを参照してください。

Live Help Client

「Live Help Expert」からリモート操作されるソフトウェアです。支援を必要とするクライアントユーザーのPCや、リモート操作で運用するサーバに導入します。クライアント側は、「画面上のメッセージに対して、どう応えたらいいのかわからない」や、「アプリケーションの操作方法がわからない」などの場合に、「Live Help Expert」からの遠隔操作によって、支援を受けることができます。

詳細は、Systemwalker Live Helpのマニュアルを参照してください。

1.3.2 ソフトウェア辞書

ソフトウェア辞書とは

Systemwalker Desktop Patrolのインベントリ収集機能を用いてソフトウェアの情報を収集するためには、そのソフトウェアを判定するための検索条件を定義する必要があります。

Systemwalker Desktop Patrolでは、その定義を「ソフトウェア辞書」と呼びます。

収集したソフトウェアの情報は、メインメニューの[PC情報]-[ソフトウェアの監査]で確認できます。

「ソフトウェア辞書」には、以下の2種類があります。

- サポートセンター定義

  Systemwalkerサポートセンターから配信されるソフトウェアの検索条件です。

  代表的なソフトウェア、Microsoft社のセキュリティパッチ、ウイルス対策ソフトウェアのウイルス定義ファイルなどに対する検出条件です。「サポートセンター定義」は、最新の「ソフトウェア辞書」を適用することによって更新できます。

- ユーザー定義

  企業内の独自のソフトウェアなど、サポートセンター定義に定義されていないユーザー独自のソフトウェアの検索条件です。

また、一般社団法人 ソフトウェア資産管理評価認定協会(SAMAC)のソフトウェア辞書をSystemwalker Desktop Patrolに移入して運用できます。

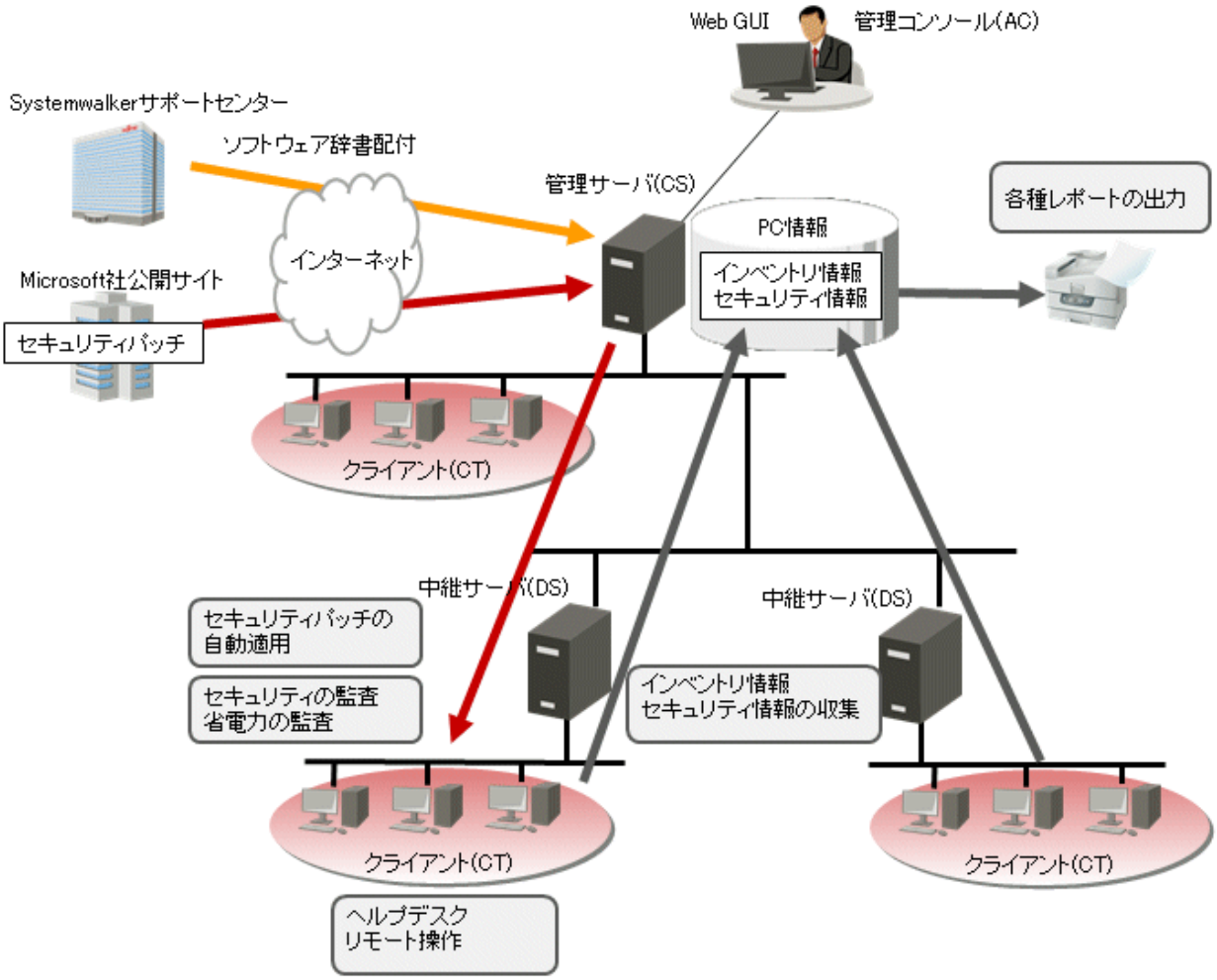
SAMACのソフトウェア辞書には、以下の特徴があります。

- 有償ソフトウェアからフリーウェア、ドライバまでを網羅しています。
- “プログラムと機能”にある“プログラムのアンインストール”や”インストールされた更新プログラムを表示”に表示されているインストール名称をベースに作成されています。

SAMACのソフトウェア辞書を移入するには、ユーザーがSAMACと契約し、事前に入手しておく必要があります。

1.3.3 システム構成

Systemwalker Desktop Patrolを使用したクライアント管理運用(セキュリティ監査/インベントリ収集)、およびトラブル対処運用のイメージ図を以下に示します。



セキュリティパッチ適用の流れ

1. ソフトウェア辞書の受信

   Systemwalkerサポートセンターからソフトウェア辞書(ソフトウェア/セキュリティパッチを検出するための定義体)を自動受信および適用します。または、Systemwalkerサポートセンターの公開サイトからソフトウェア辞書を手動でダウンロードおよび適用します。

2. 管理対象ソフトウェア/セキュリティパッチの選択

   管理対象とするソフトウェアを選択します。

   また、ソフトウェア辞書にはMicrosoft社の公開サイトからセキュリティパッチを自動ダウンロードするための情報が記載されています。自動パッチ適用を行うセキュリティパッチを選択します。

3. セキュリティパッチの配信/適用

   選択したセキュリティパッチがMicrosoft社の公開サイトから自動ダウンロードされます。

   運用設定にしたがって、ダウンロードしたセキュリティパッチが配信、適用されます。

4. インベントリ情報の収集

   ソフトウェア辞書で選択したソフトウェアの導入状況やハードウェア情報などが自動収集されます。

   また、セキュリティパッチの適用状況が自動的に収集されます。

5. 確認

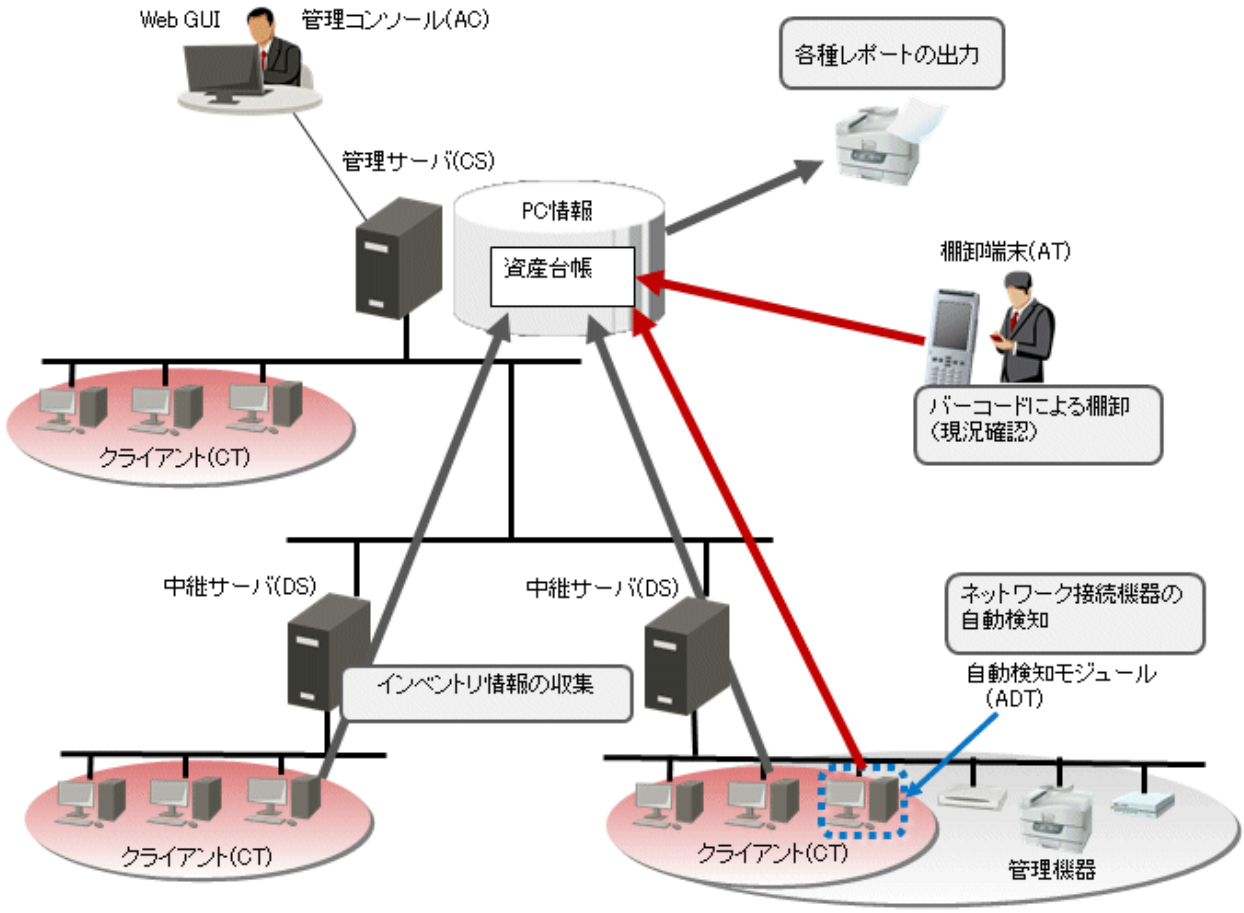
   管理者は、選択したソフトウェアの導入状況やハードウェア情報を確認します。

   また、必要なセキュリティパッチが適用されているかを確認します。

リモート操作の流れ

1. トラブルが発生したPCでリモート操作クライアントを起動します。
2. 管理者は、リモート操作エキスパート機能を使用してクライアントPCに接続します。
3. 管理者からクライアントPCのGUI操作が可能となり、トラブル要因を取り除くことができます。

Systemwalker Desktop Patrolを使用したICT資産管理のイメージ図を以下に示します。



1. 資産情報の登録/変更

   以下のどれかの方法で資産情報を登録/変更します。

   a. インベントリ情報の登録/変更

      Systemwalker Desktop Patrolで収集されたインベントリ情報を、管理台帳で管理する資産情報として手動または自動で登録/変更します。

   b. 台帳の登録/変更

      台帳として管理していた既存の資産情報を、管理台帳で管理する資産情報として手動で登録/変更します。

   c. 機器情報の自動検知による登録/変更

      ADTで自動検知された機器情報が、CSに自動通知されます。未登録の機器については未登録機器管理の画面から機器情報を個々に登録します。または未登録機器一覧をファイルに出力して一括で登録することも可能です。

   d. 画面からの登録/変更

      メインメニューから資産情報を個々に登録/変更します。

2. 資産情報の確認

以下のどちらかの方法で資産情報を確認します。

a. 画面からの確認

メインメニューから、機器情報、契約情報および棚卸状況を確認します。

b. バーコードの読み込み

事前に作成したバーコードラベルをATで読み込み、機器情報と契約情報を確認します。

3. 棚卸作業

以下のどれかの方法で棚卸を行います。

a. インベントリ情報の収集

PCから収集されたインベントリ情報により棚卸を行います。

b. 機器情報の自動検知

ADTで自動検知された機器情報により棚卸を行います。

c. バーコードの読み込み

事前に作成したバーコードラベルをATで読み込み、棚卸を行います。棚卸の結果は管理台帳で管理する資産情報に反映します。

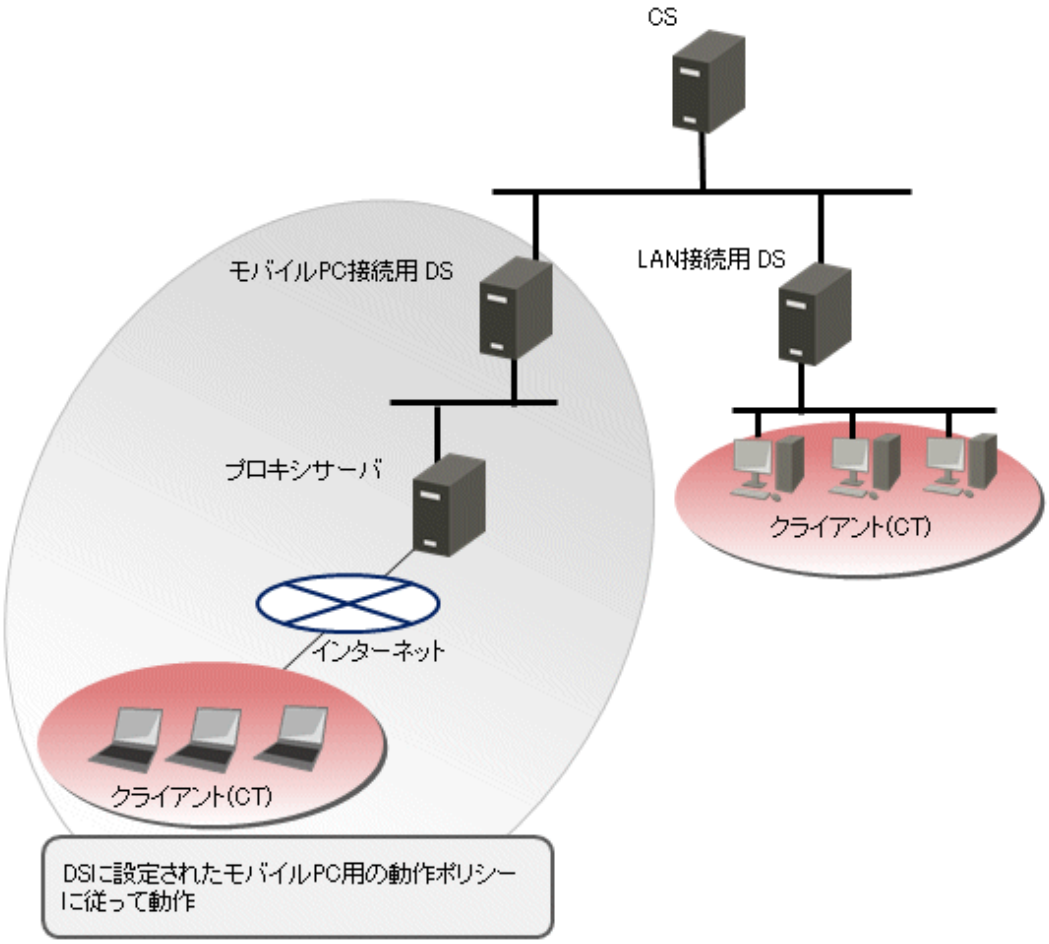
d. 画面からの設定

メインメニューで、手動で棚卸状態（棚卸済み/棚卸未完）を設定します。

4. レポート出力

管理台帳で管理する資産情報から資産稼働状況、契約状況、棚卸状況の結果をレポートとして出力し、運用状況の把握や監査を行います。

社外からVPN（Virtual Private Network）を使用して社内に接続するようなモバイル運用を行う場合のシステム構成を以下に示します。



モバイルPC接続用にDSを設置し、そのDSに対してモバイルPC用の動作ポリシーを設定します。モバイルPCは、このDSに接続することにより、設定された動作ポリシーに従って動作します。

ネットワークに常時接続しないモバイルPCにおいても、Systemwalker Desktop Patrolによる資産管理の運用を行えます。

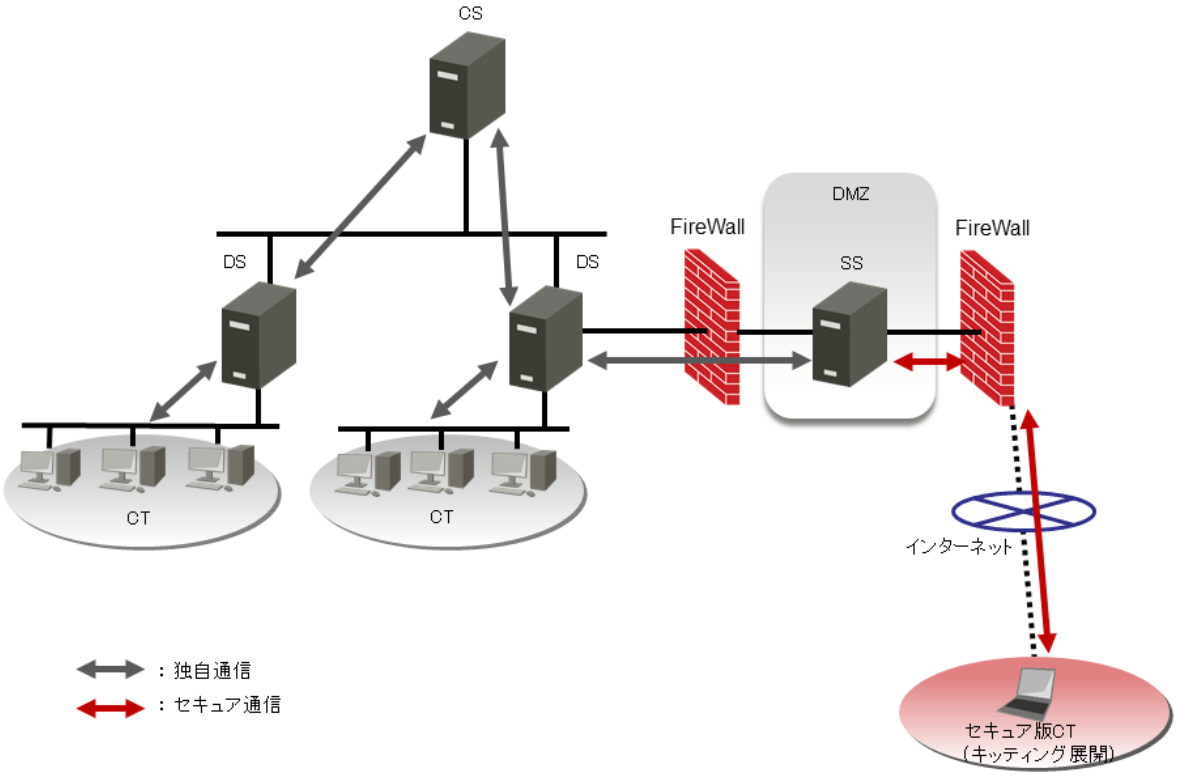
インターネット対応環境のシステム構成

社外からインターネットを使用して社内に接続するような場合のシステム構成を以下に示します。

以下の対応を行うことで、インターネット環境での運用が可能となります。

- DMZへSSを導入したサーバを配置し、インターネットから接続可能とする設定を行う。

・ インターネットで使用可能な、セキュア通信を行えるセキュア版CTをPCに導入する。
セキュア版CTの導入方法の詳細は、“導入ガイド”の“セキュア版CTを導入する”を参照してください。



・ セキュア版CTとSS間のデータ送受信は、暗号化されたセキュア通信で実施します。
・ セキュア通信以外の環境は、独自通信となります。
  ー 社内に導入した通常のCTおよびV15.1.1以前のCTと、CS/DS間のデータ送受信
  ー CS-DS間のデータ送受信

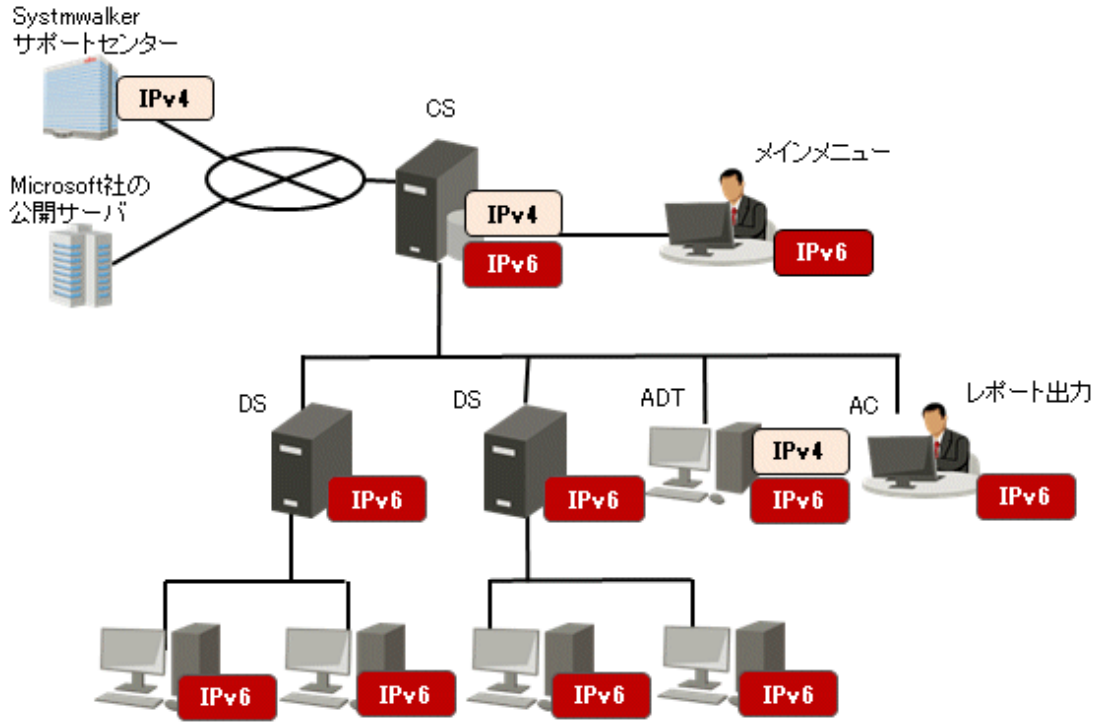
IPv6対応のシステム構成

Systemwalker Desktop Patrolでサポートするの対応のネットワーク構成を、以下に示します。

注意

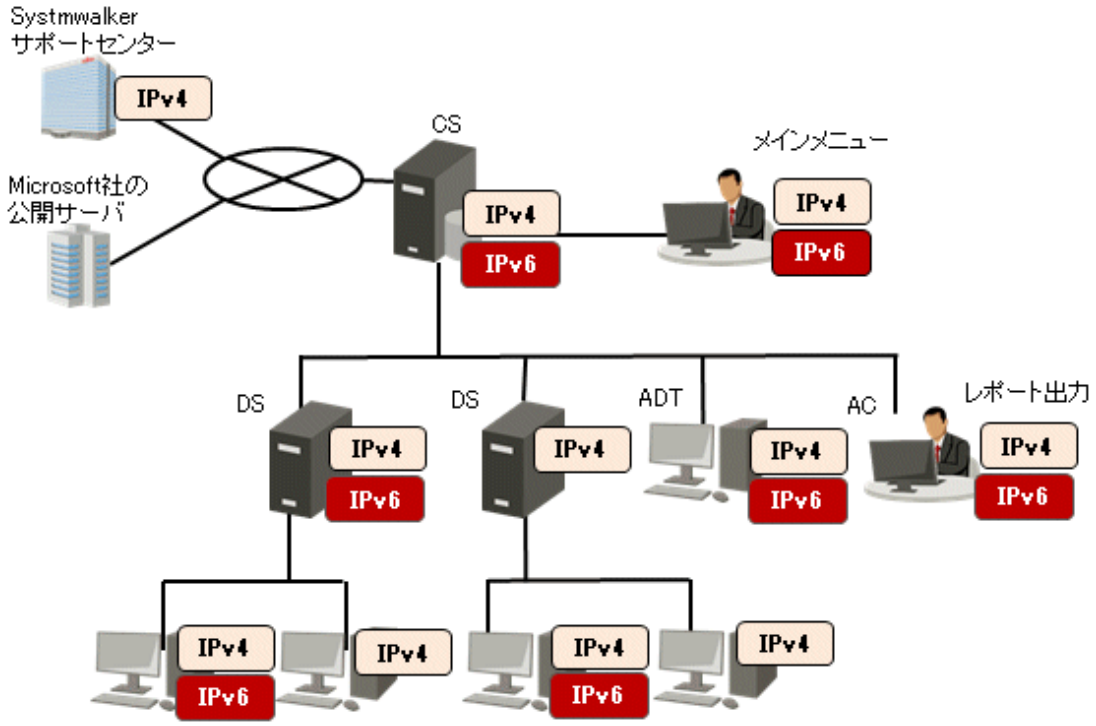
・ 「Systemwalker Desktop Patrol CS」がIPv6のみの環境にある場合、Systemwalkerサポートセンターに接続できません。CSは、デュアルスタックでの環境を構築する必要があります。
・ IPv6のみの環境の場合、IPv4をアンインストール(netsh interface ipv4 uninstallを実行)しないでください。

・ IPv6のみの場合



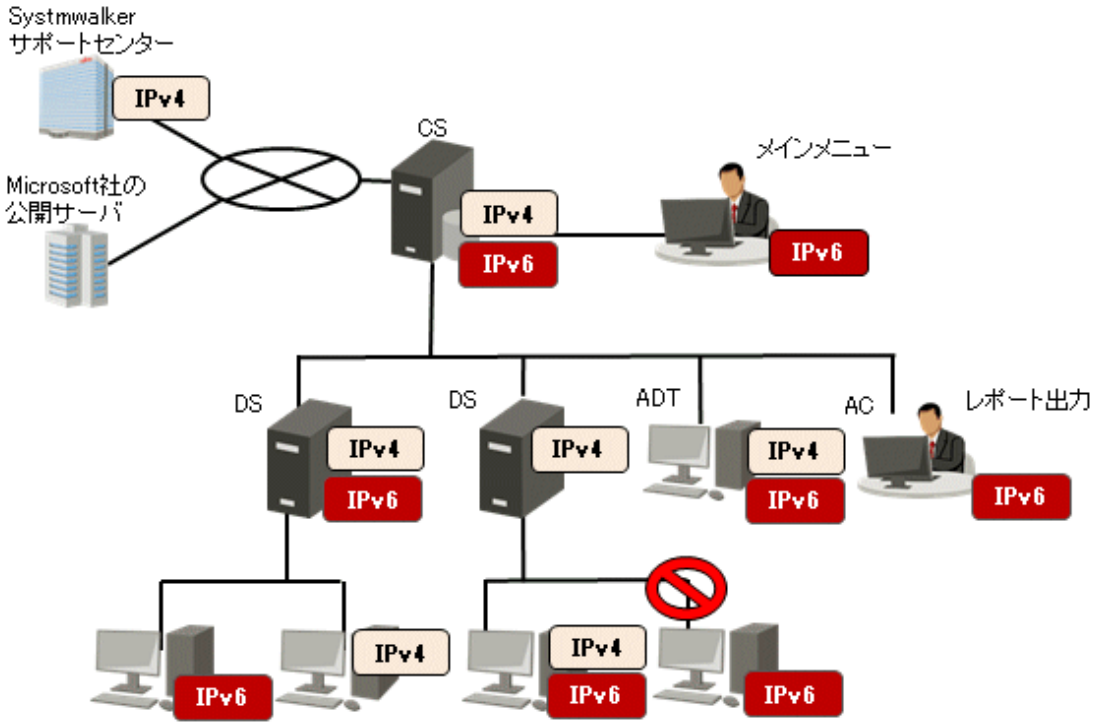
機能	動作結果
インベントリ情報	CTでIPv6のネットワーク情報を収集し、メインメニューでIPv6の情報が参照できます。
ネットワーク通信	IPv6のネットワーク環境を使用し通信を行います。
未登録機器の検知（ADT）	IPv6のみの環境はサポートしません。
Systemwalkerサポートセンター	IPv4のみサポートします。
CS	デュアルスタックでの環境を構築する必要があります。 IPv6のみの環境にある場合、Systemwalkerサポートセンターに接続できません。

・ IPv4とIPv6デュアルスタック環境の場合



機能	動作結果	備考
インベントリ情報	CTでIPv4とIPv6のネットワーク情報を収集し、メインメニューでIPv4とIPv6の情報が参照できます。	収集対象がV14.2.1以前の場合は、IPv4の情報のみの収集・表示が可能です。
ネットワーク通信	デュアルスタックのCT環境では、最初に取得したIPアドレスでのみ通信を試みます。	

・ IPv4とIPv6のネットワーク環境が混在する場合



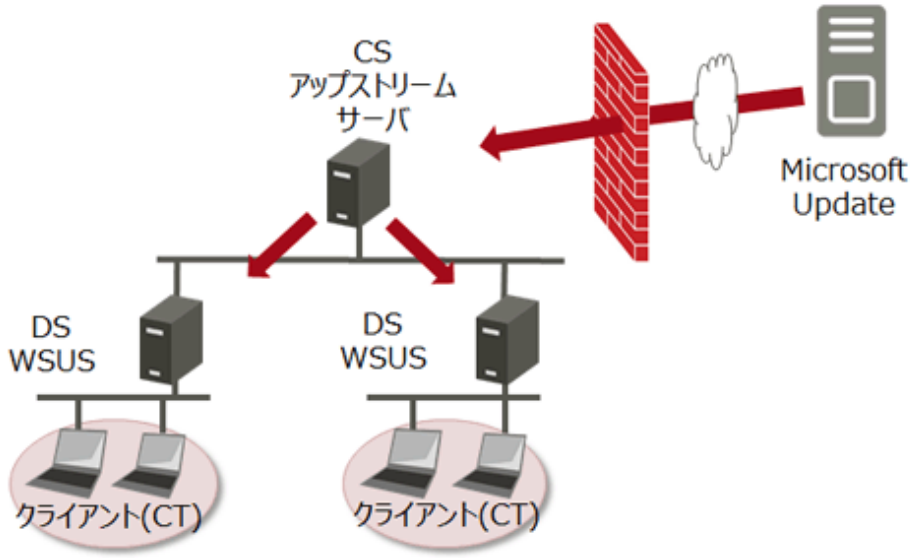
機能	動作結果	備考
インベントリ情報	CTでIPv4とIPv6のネットワーク情報を収集し、メインメニューでIPv4とIPv6の情報が参照できます。 ・ IPv4のみのCT環境ではIPv4のみ収集・参照 ・ IPv6のみのCT環境ではIPv6のみ収集・参照 ・ デュアルスタックのCT環境ではIPv4/IPv6の収集・参照	
ネットワーク通信	以下のように通信を行います。 ・ IPv4のみのCT環境ではIPv4で通信 ・ IPv6のみのCT環境ではIPv6で通信 ・ デュアルスタックのCT環境では、最初に取得したIPアドレスでのみ通信を試みます。	上位サーバの通信環境のレベルが低い場合は、通信できません。

WSUSと連携する場合のシステム構成

WSUSとSystemwalker Desktop PatrolのCS/DSが連携し、配下のクライアントに更新プログラムを適用・監査を行う場合、以下の構成で運用します。

- Microsoft Updateと接続するアップストリームサーバがCSと同居する

  代表的な運用パターンとして、CSがインターネット接続できる環境では本構成となります。

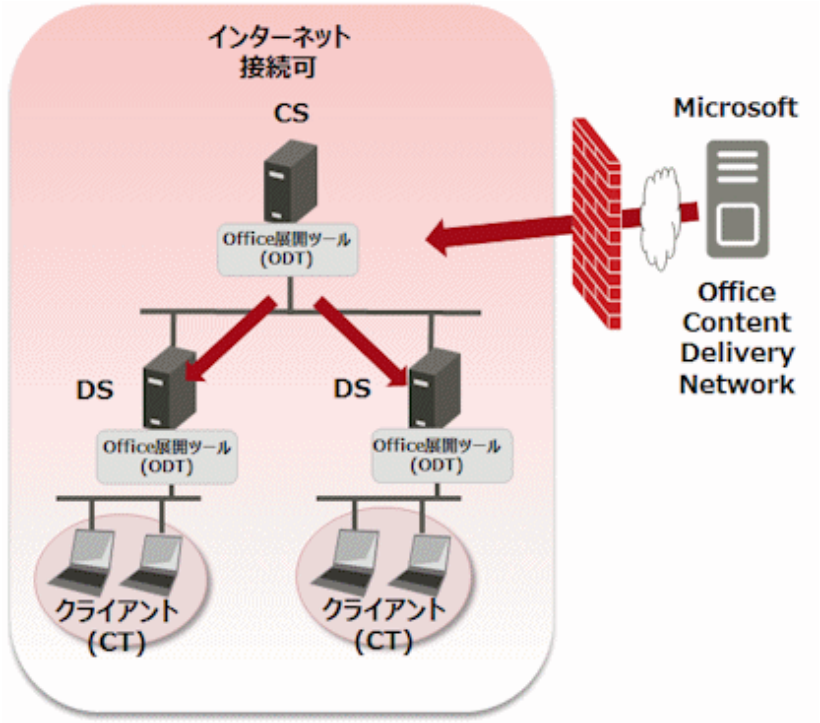


クイック実行形式のセキュリティパッチの配信/適用を行う場合のシステム構成

クイック実行形式のセキュリティパッチを、Microsoft社のOffice Content Delivery NetworkからSystemwalker Desktop Patrol配下のクライアントに配信/適用を行う場合、以下の構成で運用します。

- CSがインターネット接続できる環境の場合

  代表的な運用パターンとして、CSがインターネット接続できる環境では本構成となります。



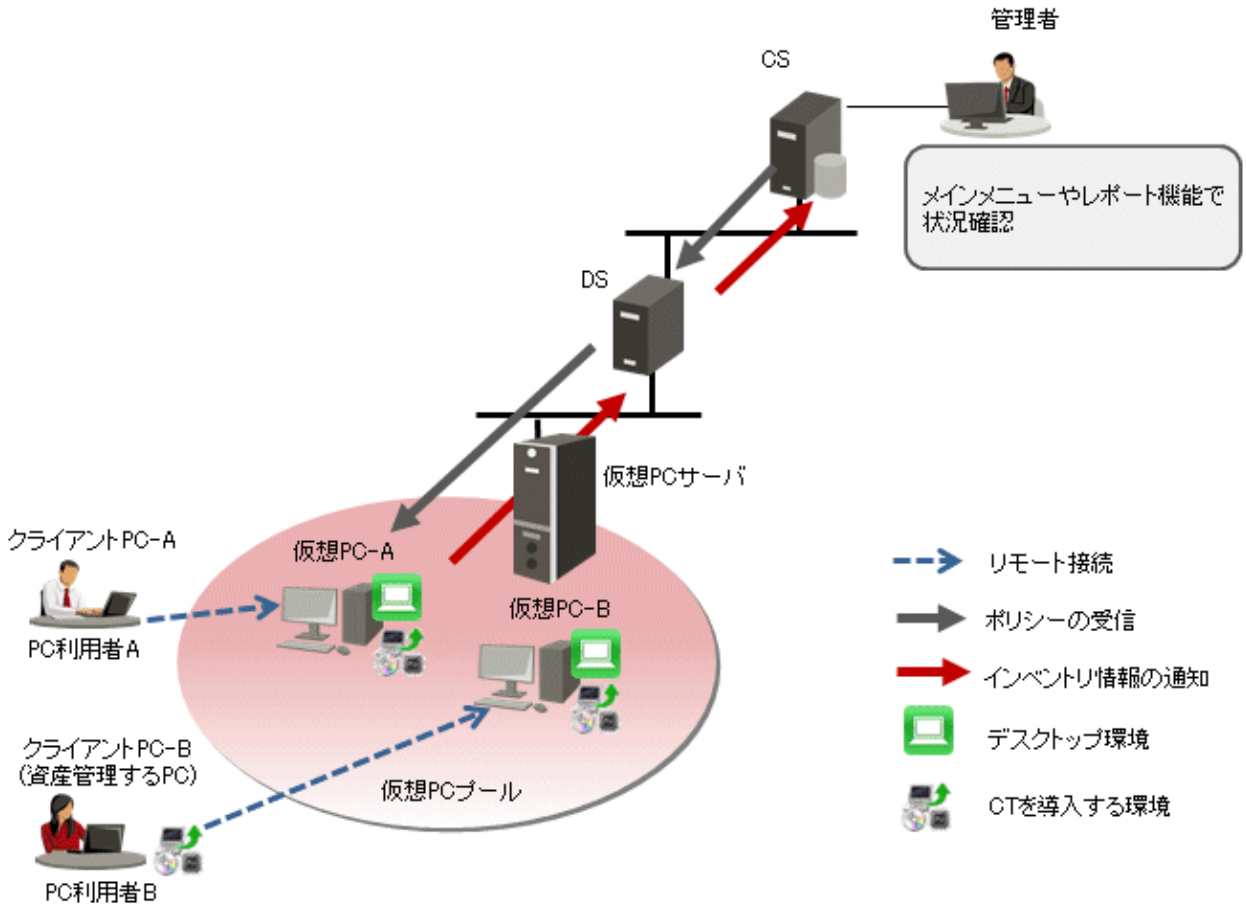
1.3.4 仮想デスクトップ環境のCT導入時のシステム構成

Systemwalker Desktop Patrol CTを仮想デスクトップ環境で導入する場合、以下のシステム構成の運用パターンがあります。

仮想PCサーバを使用したパターン

仮想PCにCTを導入し、仮想PCのWindowsに導入されているソフトウェア等の資産管理およびWindowsのセキュリティ監査を行います。また、メインメニューから仮想PCで情報を収集したことが判断できます。

サーバ(CSおよびDS)からのポリシー受信、サーバへのインベントリ情報の通知については、通常のCTと同じです。

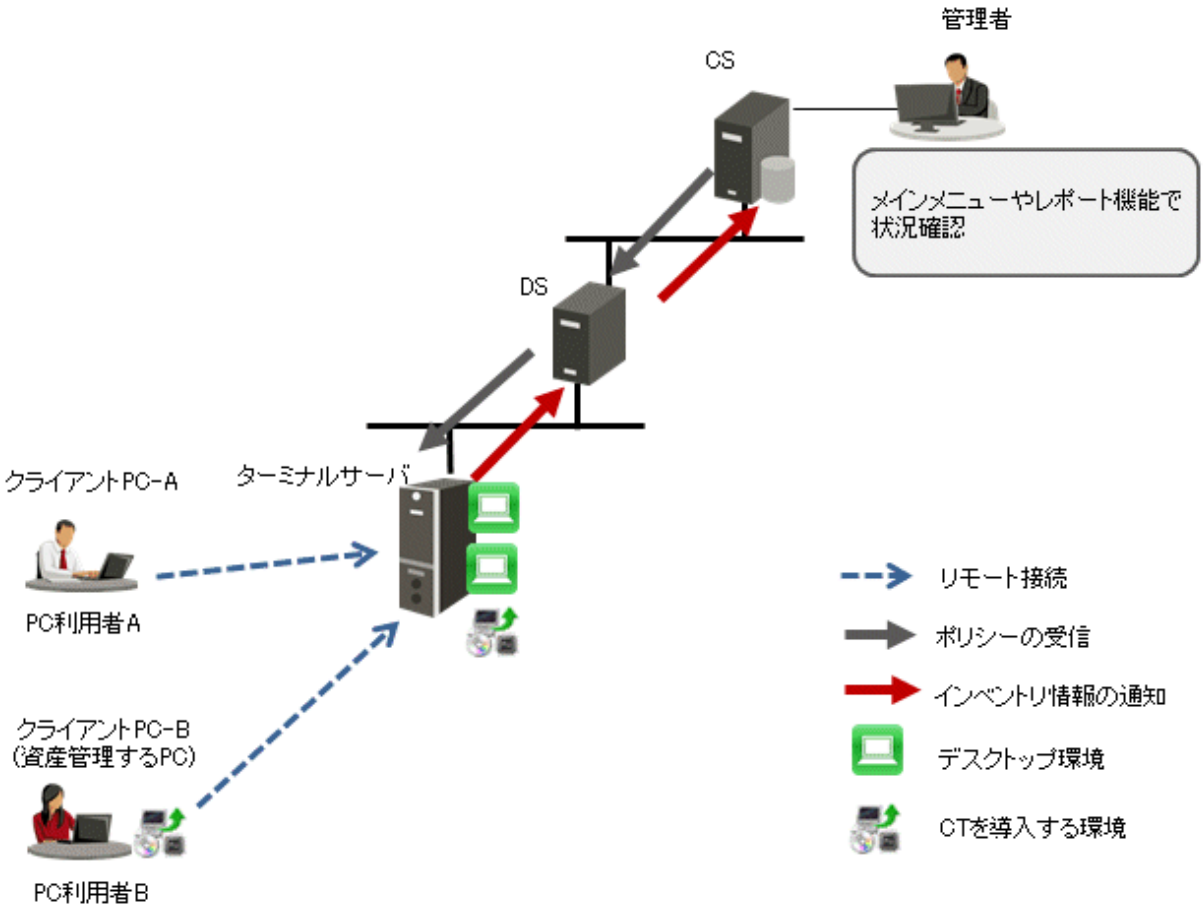


仮想PCサーバ:VMware ESX、VMware vSphere、Microsoft Hyper-Vなどの製品を導入しているマシン
クライアントPC:通常のノートPCまたはデスクトップPC
仮想PCプール:仮想PCサーバ上に展開された仮想PCをグループ化したもの

ターミナルサーバを使用したパターン

ターミナルサーバのWindowsにCTを導入し、ターミナルサーバに導入されているソフトウェア等の資産管理およびWindowsのセキュリティ監査を行います。

サーバ(CSおよびDS)からのポリシー受信、サーバへのインベントリ情報の通知については、通常のCTと同じです。

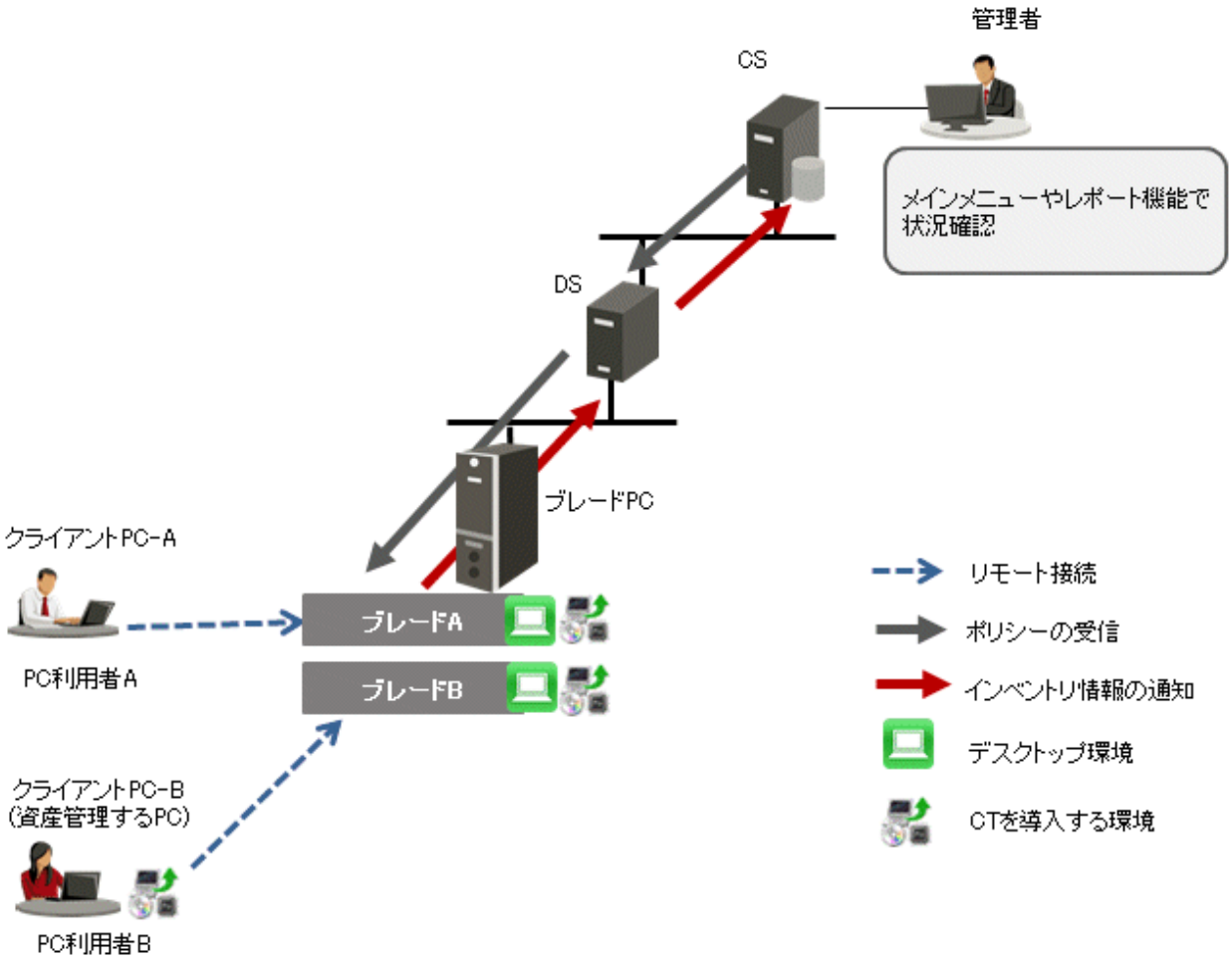


ターミナルサーバ：Windowsサーバ製品の役割として、「ターミナルサーバー」または「リモートデスクトップセッションホスト」が導入されている環境
クライアントPC ：通常のノートPCまたはデスクトップPC

ブレードPCを使用したパターン

ブレードPCの各ブレードのWindowsにCTを導入し、ブレードのWindowsに導入されているソフトウェア等の資産管理およびWindowsのセキュリティ監査を行います。

サーバ（CSおよびDS）からのポリシー受信、サーバへのインベントリ情報の通知については、通常のCTと同じです。



ブレードPC :複数のブレードを専用筐体に集約して搭載したマシン
クライアントPC:通常のノートPCまたはデスクトップPC

1.3.5 通信のセキュリティ

Systemwalker Desktop Patrolでは通信のセキュリティのために、以下の機能に対応しています。

プロキシサーバ

プロキシサーバを設定できます。

SSL通信

以下のサーバ間で、通信を暗号化するためのSSL通信が可能です。

- Systemwalkerサポートセンターと「Systemwalker Desktop Patrol CS」の間

  ソフトウェア辞書をSystemwalkerサポートセンターから暗号化した状態で配信できるため、ネットワークのセキュリティを強化できます。

第2章 Systemwalker Desktop Patrolの機能

Systemwalker Desktop Patrolの機能について説明します。Systemwalker Desktop Patrolは、以下の機能を提供します。

- PC情報の収集/参照機能
- PCの監査/統制機能
- ライセンス管理機能
- ファイル配信機能
- ソフトウェア配信機能
- セキュリティパッチの配信/適用機能
- WSUS連携機能
- クイック実行形式のセキュリティパッチの配信/適用機能
- ディスク消去機能
- 管理台帳機能
- レポート出力機能
- ロケーションマップ機能
- 環境設定機能
- リモート操作機能
- アップデータ機能
- クライアント抑止機能

なお、各機能の設定方法、操作方法および留意事項などの詳細については、“運用ガイド 管理者編”を参照してください。

2.1 PC情報の収集/参照機能

Systemwalker Desktop PatrolのPC情報の収集/参照機能について説明します。

Systemwalker Desktop Patrolでは、PCのソフトウェア、ハードウェアの情報をインベントリ情報と呼びます。このインベントリ情報を各PCから収集し、データベースに登録してCSで一元管理することができます。

Systemwalker Desktop Patrolの資産管理機能は、企業で様々なニーズに対応できるよう多くのバリエーションを備えています。

この機能を使用することによって収集できる情報を、各情報の表示画面とともに説明します。

2.1.1 収集方法

インベントリ情報は、以下の2つの方法で収集できます。

- エージェントモード
  - ー ユーザーに意識させない、負担をかけない収集方法です。
  - ー ソフトウェアの実行状況なども収集可能です。
- コマンドモード
  - ー USBメモリなど外部媒体での情報収集が可能です。
  - ー メール送信機能付きコマンド（インベントリ収集から、メール送信まで、自動的に行うコマンド）での収集が可能です。

エージェントモード

CTをPCにインストールすることにより、自動的に最新の情報を収集し、PC情報のデータベースを構築できます。

メインメニューで設定したクライアントポリシーに従って、CTは、収集したインベントリ情報を接続サーバに転送します。各CTで収集されたインベントリ情報は、最終的には最上位のCSに転送され、CSのデータベースに登録されます。

コマンドモード

ネットワークから切り離したPCや回線速度の遅いネットワークなどで、インベントリ収集を行う場合は、コマンドモードを使用します。

コマンドモードは、CTを導入していなくても、インベントリ情報を収集できます。

コマンドモードは、以下の2つが用意されています。

インベントリ収集のみ:CTOffline.exe

コマンドを実行すると、インベントリ情報の収集を行い、カレントディレクトリにインベントリ情報ファイル(“ユーザーID＋PC名”)を作成します。作成されたファイルをCSまたはDSの指定ディレクトリに格納することにより、インベントリ情報を取り込むことができます。

インベントリ収集＋メール送信:CTMail.exe

インベントリ情報の収集を行い、インベントリ情報ファイル(“ユーザーID＋PC名”)をメールで、CSまたはDSに送信します。

収集項目

収集方法により収集可能な情報が異なります。収集可能な情報を以下に示します。

収集情報	収集方法	
	エージェントモード	コマンドモード
基本情報(OS情報、ハードウェア情報)	○	○
ソフトウェア情報	○	○
ウイルス対策ソフトウェア	○	○
製品情報	○	○
ユーザー情報	○	○
EXE情報	○	○
レジストリ情報	○	○
未適用パッチ情報	○	○
セキュリティ情報: システムセキュリティ情報 ユーザーセキュリティ情報	○	○
セキュリティ情報: Desktop Keeper情報 Desktop Encryption情報	○	×
省電力監査情報: 省電力設定値	○	○
省電力監査情報: 省電力運転状況	○	×
ソフトウェア稼働状況	○	×
ファイル収集	○	×
簡易操作ログ収集	○	×

○:収集可能

×:収集不可

2.1.2 インベントリ情報

収集された情報がどの部門の情報か、誰が管理しているPCかすぐ分かるように、Systemwalker Desktop Patrolのインベントリ収集機能では、インベントリ情報に、ユーザーID、PC名を付与して一緒に収集します。これにより、部門改編が頻繁に行われるような場合や、PCが移動されるような場合でも、PCの所在、部門を追跡できます。

インベントリ情報として収集・参照できる内容は以下のとおりです。

- 基本情報(OS情報、ハードウェア情報)
- ソフトウェア情報
- ウイルス対策ソフトウェア
- 製品情報
- ユーザー情報
- EXE情報
- レジストリ情報
- 未適用パッチ情報
- 契約情報
- セキュリティ情報
- 省電力情報

これらの情報は、メインメニューの[PC情報]-[インベントリ情報]画面で表示されます。

また、V14.2.0以降のSystemwalker Desktop Keeperを導入しているシステムでは、「ログ検索画面」および「ログ詳細画面」の「資産情報」のリンクをクリックすることで、Systemwalker Desktop Patrolの上記の情報を表示できます。

各情報の表示内容、および表示イメージは以下のとおりです。

基本情報(OS情報、ハードウェア情報)

PCの基本情報(OS情報、ハードウェア情報)を収集します。

ハードウェア情報は、使用しているOS（Operating System）によって、収集可能なインベントリ情報が異なり、確認できる項目が異なります。
以下の表に、それぞれ収集できるハードウェア情報を示します。

分類	項目名	8.1/10	8.1 64bit/10 64bit/11 64bit	2012/ 2016/ 2019	備考
基本情報	PC属性	○	○	○	
	BIOSバージョン	△	△	△	
	コンピュータ名	○	○	○	
	ドメイン名	○	○	○	ドメインの設定がされていない場合は、ワークグループ名を獲得します。
	ログイン名	○	○	○	
	CPU名	○	○	○	
	クロック数	△	△	△	
	CPU数	○	○	○	
	CPU詳細	○	○	○	
	メモリサイズ	○	○	○	[コントロールパネル]-[システム]に表示される[実装メモリ(RAM)]とは異なります。
	スワップファイルサイズ	○	○	○	
	キーボードタイプ名	○	○	○	
	インストール言語	○	○	○	
	マウスタイプ名	○	○	○	
	マウスボタン数	○	○	○	
	PCベンダ名	△	△	△	
	PCモデル	△	△	△	
	PCシリアル番号	△	△	△	
	1次キャッシュ/ 2次キャッシュ	△	△	△	
OS情報	OS	○	○	○	
	OSビルド番号	○	○	○	
	サービスパック	○	○	○	「ServicePack X」のように表示されます。 例）Service Pack 1
	DOSバージョン	○	×	×	
	OSの使用者名	△	△	△	Windows 8.1、Windows 10、Windows 11の場合、OSインストール時に最初に作成したユーザー名を収集します。 2012、2016、2019の場合、“Windows ユーザー”を収集します。
	OSの組織名	－	－	－	
	OSのプロダクトID	○	○	○	
	Windowsディレクトリ名	○	○	○	

分類	項目名	8.1/10	8.1 64bit/10 64bit/11 64bit	2012/ 2016/ 2019	備考
	システムディレクトリ名	○	○	○	
	書き込み保護（注1）	○	○	○	
	WSUSの使用(注2)	○	○	○	
	イントラネットのMicrosoft更新サービス(注3)	○	○	○	
	コンピュータグループの設定(注2)	○	○	○	
	コンピュータグループ名(注3)	○	○	○	
	Office入手先	○	○	○	Microsoft 365(旧Office 365)の場合に収集します。
		△	△	△	Office2019の場合、Windows 10、Windows 11およびWindows Server 2019で収集します。
ディスプレイ情報	画面解像度(注4)	○	○	○	
	ビデオアダプタ	○	○	○	
	ビデオメモリサイズ	○	○	○	
	色数	○	○	○	
	スクリーンセーバー名（注4）	△	△	△	
	モニタ名	○	○	○	
	画面リフレッシュレート(注4)	△	△	△	
ドライブ情報（注4）	ドライブ名	△	△	△	
	ドライブ種別	△	△	△	
	ドライブ容量	△	△	△	
	ドライブ空き容量	△	△	△	
	ボリュームラベル	△	△	△	
	ファイルシステム種別	△	△	△	
	BitLocker状態（注7）	△	△	△	
BitLocker回復パスワード（注7）	パスワードID	△	△	△	
	回復パスワード	△	△	△	
CD-ROM情報	装置名	△	△	△	
ディスク情報	メーカ名	△	△	△	

分類	項目名	8.1/10	8.1 64bit/10 64bit/11 64bit	2012/ 2016/ 2019	備考
	モデル名	△	△	△	
	ディスク容量	○	○	○	
	ディスクIF	△	△	△	
	説明	○	○	○	
メモリ情報	デバイスロケータ	△	△	△	
	サイズ	△	△	△	
ネットワークカード情報（注5）	ネットワークカード	△	△	△	複数獲得できます。 複数枚のネットワークカードをグルーピングしている場合は、論理名を獲得します。
	MACアドレス	○	○	○	複数獲得できます。
TCP/IP情報（注6）	ホスト名	○	○	○	複数獲得できます。
	IPアドレス	○	○	○	
	サブネットマスク	○	○	○	
	デフォルトゲートウェイ	○	○	○	
	DHCPサーバ	○	○	○	
	DNSサーバ	△	△	△	
ネットワーク共有情報（注4）	ネットワークパス名	△	△	△	
	ネットワークプロバイダ名	△	△	△	
	ドライブ名	△	△	△	
プリンタ情報（注4）	プリンタ名	△	△	△	
	プリンタ種別	△	△	△	

○：収集できます。

△：OSや機種によっては、収集できない場合があります。

×：収集できません。

－：収集しない、または該当情報なし。

8.1：Windows 8.1

8.1 64bit：Windows 8.1 64ビット版

10：Windows 10

10 64bit：Windows 10 64ビット版

11 64bit: Windows 11 64ビット版

2012：Windows Server 2012

2016：Windows Server 2016

2019：Windows Server 2019

注1）

－ Windows10およびWindows 11以外のOSでは“なし”が収集されます。

ー Windows10およびWindows 11ではPCの状態（なし/無効/有効）が収集されます。

ー 収集に失敗した場合は“なし”が収集されます。

注2）

ー Windows 10 HomeおよびWindows 11 Homeでは“使用しない”が収集されます。

ー Windows 10 HomeおよびWindows 11 Home以外のOSではPCの状態（使用する/使用しない）が収集されます。

ー 収集に失敗した場合は“使用しない”が収集されます。

注3）

ー Windows 10 HomeおよびWindows 11 Homeでは“ ”（空文字列）が収集されます。

ー Windows 10 HomeおよびWindows 11 Home以外のOSではPCの設定状態が収集されます。

ー 収集に失敗した場合は“ ”（空文字列）が収集されます。

注4）

エージェントモードのインベントリ収集では、以下のハードウェア情報を収集できません。コマンドモードのインベントリ収集は、問題なく情報の収集が行えます。

ー 画面解像度

Windows 8.1、Windows 10、Windows 11、Windows Server 2012、Windows Server 2016およびWindows Server 2019 においては、1024x768となります。

ー スクリーンセーバー名

「画面のプロパティ」でユーザーが設定したスクリーンセーバーは、収集できません。ログオン時に表示するようにあらかじめOSが設定しているWindows ロゴのスクリーンセーバーを収集します。

ー 画面リフレッシュレート

Windows 8.1、Windows 10、Windows 11、Windows Server 2012、Windows Server 2016およびWindows Server 2019においては、60Hzとなります。

ー ドライブ情報

ネットワークドライブはログインユーザー単位の動的な情報のため、ログインユーザーが実行するコマンドモードCTでは収集できます。サービス経由(SYSTEM権限)のエージェントモードでは情報が参照できません。

CTが参加しているドメインに属するマシンの共有フォルダをネットワークドライブに割り当てている場合は収集できます。

ー ネットワーク共有情報

ネットワーク共有情報は、収集できません。

ー プリンタ情報

ネットワークプリンタの情報は、コマンドモードでインベントリ収集を行う場合は収集できます。エージェントモードでインベントリ収集を行う場合は収集できません。

注5）

ー DHCP運用時に、DHCPサーバが存在しないなどにより、IPアドレスを解決できない場合は、APIPA（Automatic Private IP Addressing）を使って、ネットワーク接続のIP（Internet Protocol）構成が自動化されます。そのとき、PCは、Microsoft社が予約している169.254.0.1から169.254.255.254 までのIP アドレス範囲で、アドレスを決めるため、プライベートIPアドレスが自動的に割り当てられ、その値を獲得します。

ー TCP/IP代替アドレスの設定がされている場合は、DHCPサーバで割り振られたTCP/IPの値を獲得します。

ー DHCPサーバが存在しない場合には、自動プライベートIPアドレス、またはユーザー構成で設定されているTCP/IPの値を獲得します。DHCP運用している場合にDHCPサーバを獲得します。

ー 以下の場合、インベントリ収集時にネットワークカード情報とTCP/IP情報は獲得されません。または、IPアドレスにNULLが設定されます。または、インベントリ情報が収集されません。

- ネットワークカードが実装されていなかった場合

- ネットワークカードが無効となっていた場合
- ネットワークケーブルが外れていた場合
- DHCP環境でIPアドレスが割り当たらなかった場合
- 無線LAN環境でIPアドレスが割り当たらなかった場合
- 有効なIPアドレスを持つ「イーサネットアダプター」がない場合

インベントリ情報が収集されない場合は、以下のどれかの方法でインベントリ収集を行ってください。

1. コマンドモードCTでインベントリ収集する。
2. 既存の「イーサネットアダプター」にLANケーブルを接続し、リンクアップする。
3. アダプターの属性が「イーサネットアダプター」となる、VPN機構をPPP上で利用する。

注6）

PCのネットワーク設定がIPv6環境であった場合、IPv6のネットワーク情報を収集して、サーバに通知します。また、IPv4環境とのデュアルスタック環境であった場合は、IPv4のネットワーク情報も合わせて収集し、サーバに通知します。

サーバに通知したインベントリ情報は、メインメニューで参照および検索できます。

ー IPv6環境のインベントリ収集

IPv6のネットワーク情報としての以下の項目を収集します。

収集項目	IPv6	IPv4	備考
IPアドレス	○	○	リンクローカルアドレスは収集されません。
サブネットマスク	○	○	IPv6ではプレフィックス長（サブネットプレフィックスの長さ）を通知します。
デフォルトゲートウェイ	○	○	IPv6では複数のIPアドレスの指定が可能です。
DNSサーバ	○	○	
DHCPサーバ	ー	○	

○：収集する
ー：収集しない

注7）

ー BitLockerの暗号化状態および回復パスワードは、利用者が各ドライブを利用できる状態（ドライブの暗号化が解除されている）の場合に収集します。このため、利用者が端末入手後一度も利用していないなど、一度もロックが解除されていないドライブについては収集できません。

ー BitLockerの暗号化状態および回復パスワードは、コマンドモードでは収集できません。

ソフトウェア情報

Systemwalker Desktop Patrolの「ソフトウェア辞書」に基づき検索したインストールソフトウェアを収集します。

検索条件を以下に示します。

・ ファイル検索

ー ファイル（ディレクトリを含む）の名前検索

ー ファイル日付の完全一致、範囲検索

ー ファイルサイズの条件（等しい、以上、以下）検索

ー ファイルバージョンの条件（等しい、以上）検索

・ レジストリ検索

　― 「プログラムのアンインストールまたは変更」情報の名前での検索

　― 任意レジストリでの検索（キー名、キーの値の名前を指定した検索）

ウイルス対策ソフトウェア

PCにインストールされている“ウイルス対策ソフトウェア”を収集します。

製品情報

PCの“プログラムと機能”にある“プログラムのアンインストール”や”インストールされた更新プログラムを表示”の一部を収集します。

ユーザー情報

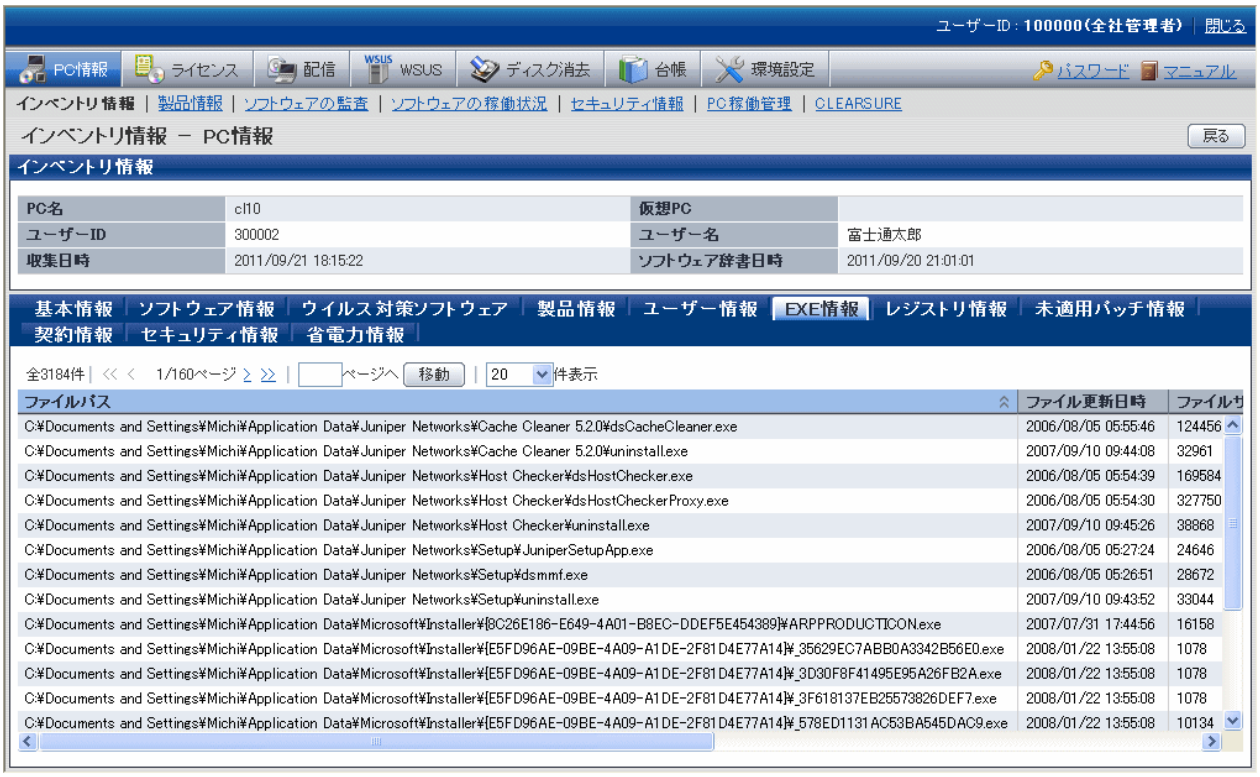
システム管理者が設定した任意の情報を、“ユーザー情報”としてインベントリ情報と一緒に収集します。

ユーザー情報は、PCユーザー自身がPC上で画面入力した情報が収集されます。

ユーザー情報の項目は最大10項目まで登録、変更できます。

EXE情報

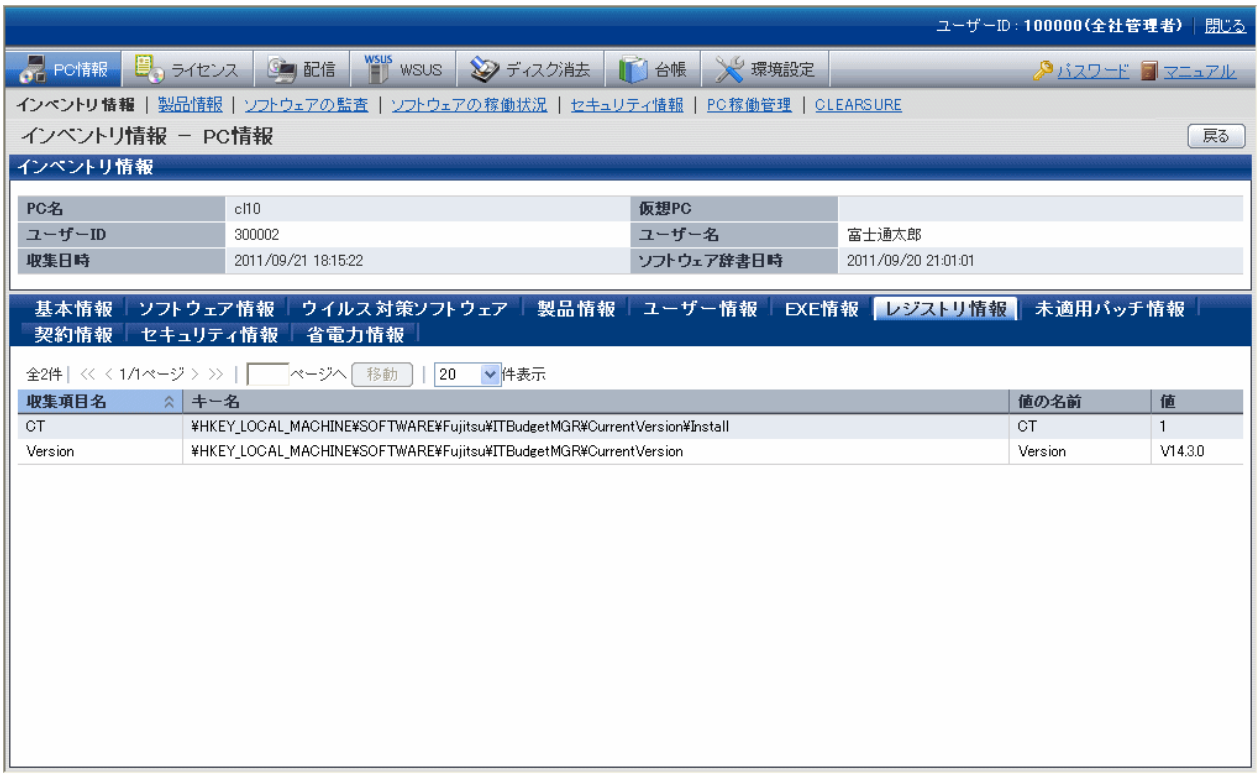
PCに存在するすべての実行ファイル（拡張子が.exeのファイル）のプロパティ情報を収集します。



レジストリ情報

OSのレジストリに記述されている情報を「キー名」、「値の名前」を指定することにより収集できます。

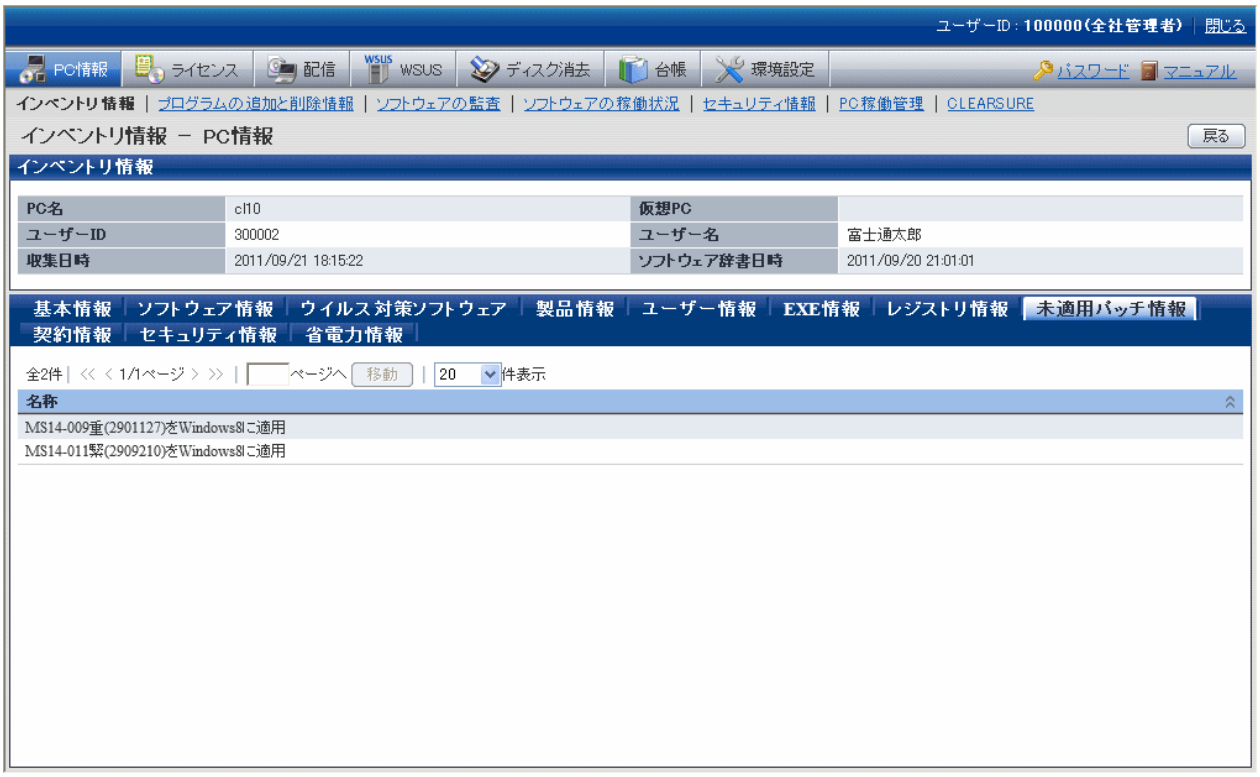
レジストリ情報は、メインメニューで以下のように表示されます。



未適用パッチ情報

自動適用対象のパッチのうち、CTに適用されていないパッチ情報を参照できます。

未適用パッチ情報は、メインメニューで以下のように表示されます。



契約情報

PCの契約情報（リース/レンタル/保守）を参照できます。

セキュリティ情報

PCのセキュリティ情報を参照できます。

省電力情報

PCの省電力情報を参照できます。

Systemwalker Desktop Keeperのログ検索画面の表示

V14.2.0以降のSystemwalker Desktop Keeperを導入しているシステムでは、Systemwalker Desktop Patrolのメインメニューの[PC情報]-[インベントリ情報]画面の「ログ管理」リンクのクリックで、Systemwalker Desktop Keeperの「ログ検索画面」を表示できます。

2.1.3 製品情報

「プログラムと機能」にある「プログラムのアンインストール」や「インストールされた更新プログラムを表示」で表示されるソフトウェアの一覧を自動収集します。

PCに存在するすべてのユーザーのソフトウェア情報を収集します。

ライセンス管理を行う場合にこの情報を利用することができます。

なお、OSの更新プログラム以外の更新プログラム（Microsoft Officeなど）については、収集されません。

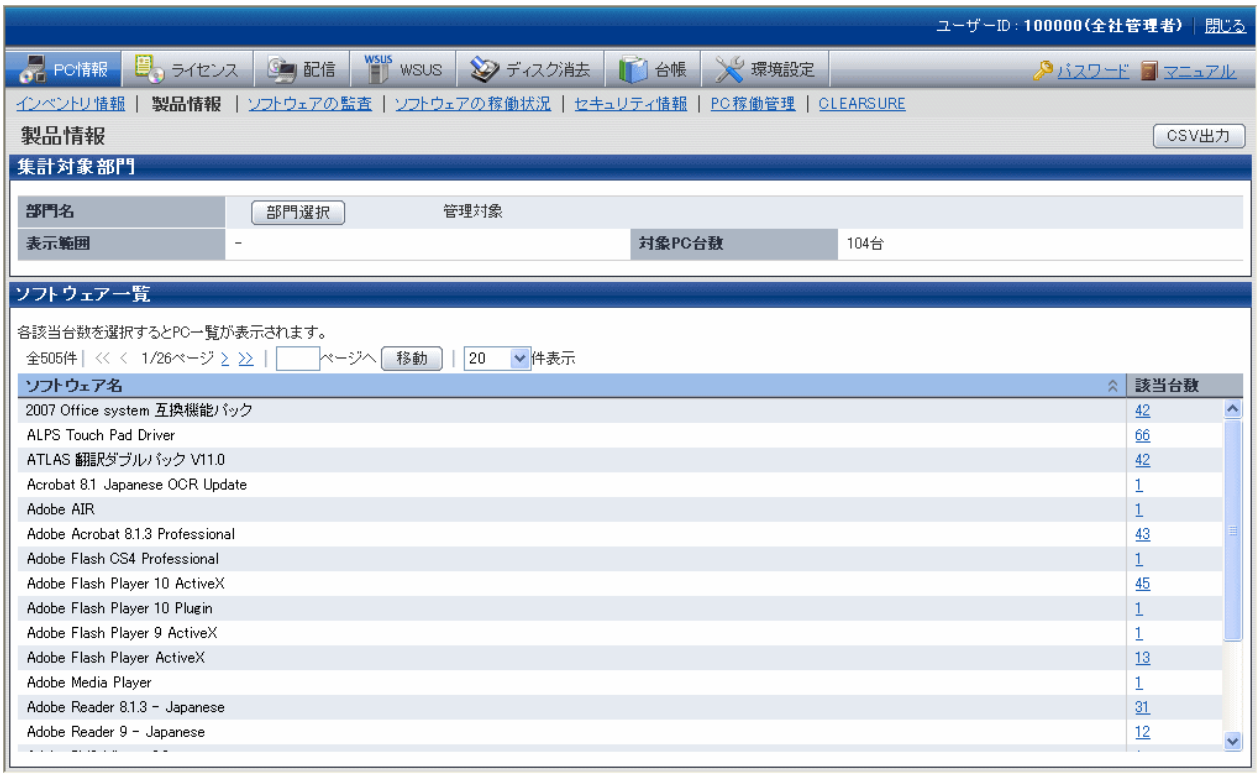
注意

ソフトウェア情報が収集されない場合について

PCにインストールされているWindows Installerのバージョンが3.0よりも古い場合、個々のユーザーにインストールされるソフトウェア情報が収集されない場合があります。

製品情報は、メインメニューの[PC情報]-[製品情報]画面で表示されます。

表示イメージは以下のとおりです。



2.1.4 ソフトウェアの監査情報

監査対象となるソフトウェアの導入状況が参照できます。

参照可能な監査情報は以下のとおりです。

- ソフトウェアの導入状況
- ウイルス対策ソフトウェアの導入状況
- セキュリティパッチの適用状況

Microsoft社から提供されるセキュリティパッチが適用されていないPCを特定できます。

コンピュータウイルス対策ソフトウェアがインストールされていないPCを特定できます。

コンピュータウイルス対策ソフトウェアの最新のパターンファイルが適用されていないPCを特定できます。

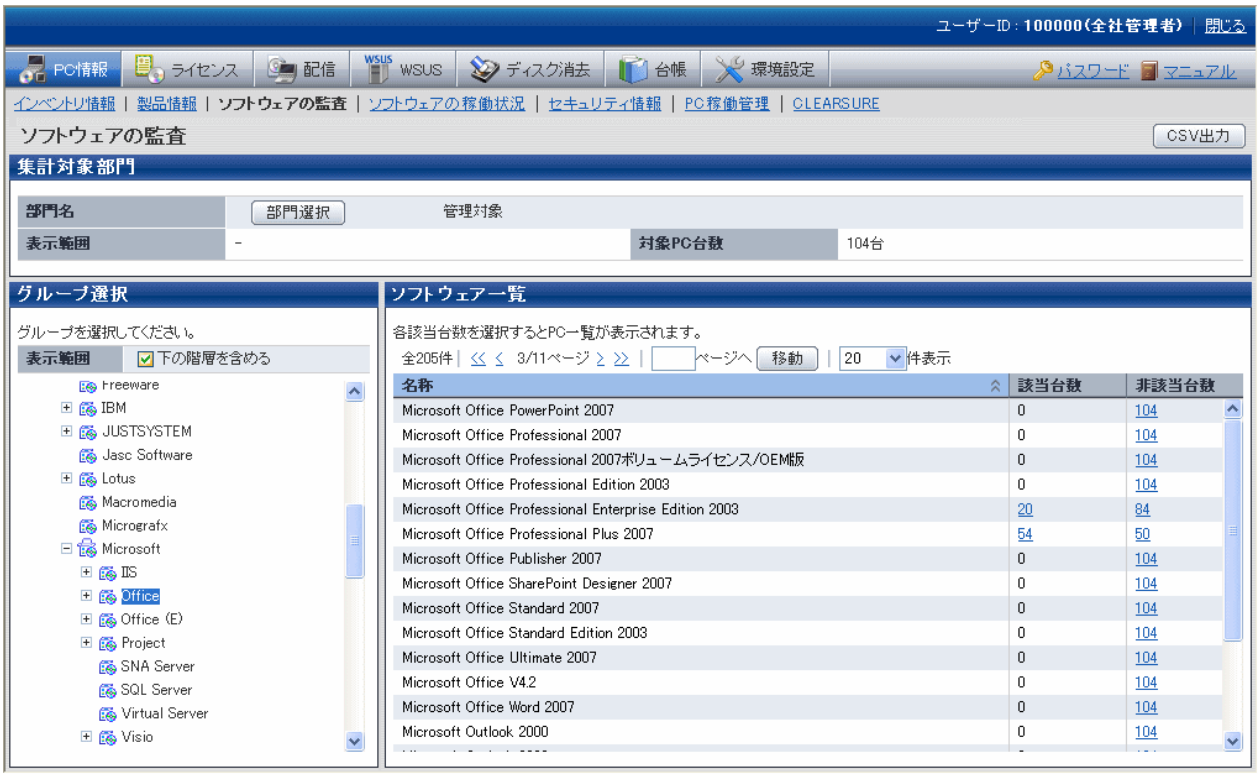
管理者は、コンピュータウイルスの脅威やセキュリティホールなど、セキュリティ上の問題のあるPCを特定でき、PCの防御能力を高めます。

これらの情報は、メインメニューの[PC情報]-[ソフトウェアの監査]画面で表示されます。

各情報の表示内容、および表示イメージは以下のとおりです。

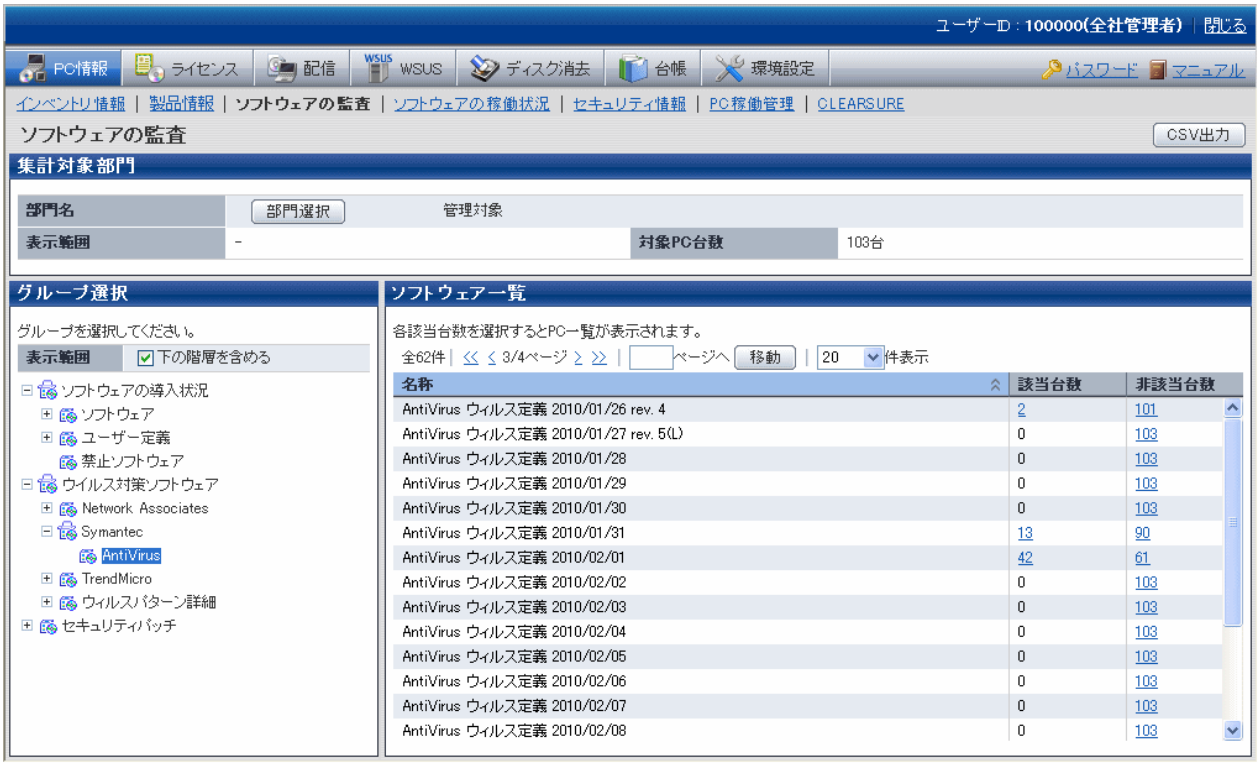
ソフトウェアの導入状況

ライセンス管理されているソフトウェアや、ユーザー定義されたソフトウェアのインストール状況が参照できます。



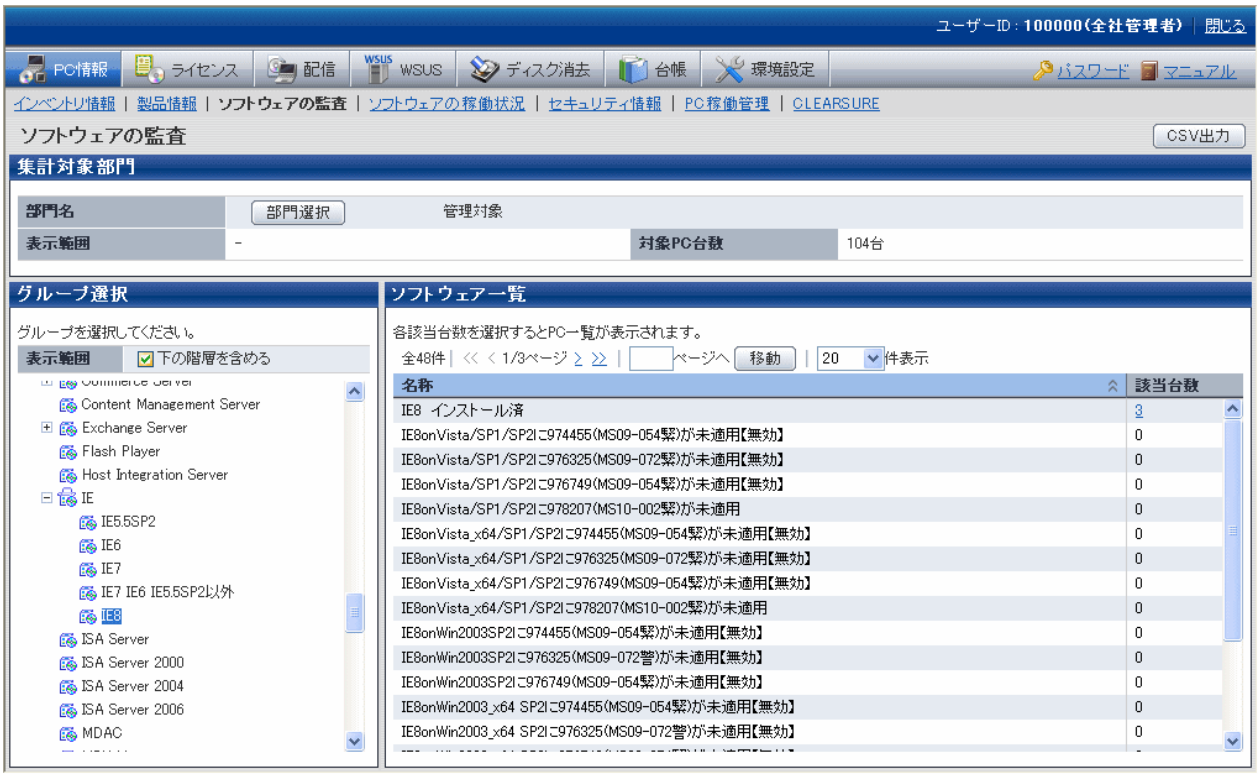
ウイルス対策ソフトウェアの導入状況

ウイルス対策ソフトウェアの導入状況が参照できます。



セキュリティパッチの適用状況

セキュリティパッチの適用状況が参照できます。



2.1.5 ソフトウェア稼働状況

ソフトウェアがインストールされているだけでなく実際に動作したかどうか、ソフトウェアの稼働状況を収集できます。

ソフトウェア稼働状況は、ソフトウェア情報と連動しており、「ソフトウェア辞書」の「ソフトウェア稼働状況」で、実際にそのソフトウェアが動作したかどうかが分かる実行ファイルを登録しておくことにより、「ソフトウェア辞書」で登録した分かりやすい名前で参照できます。

ソフトウェア稼働状況を参照することにより、資産を有効に利用できます。例えば、ライセンスが割り当てられ、ソフトウェアをインストールしていても、使用していないソフトウェアの場合、他に必要なユーザーにライセンスを割り当てることで、遊休資産を削減できます。

なお、ソフトウェア稼働状況は、コマンドモードでは収集できません。

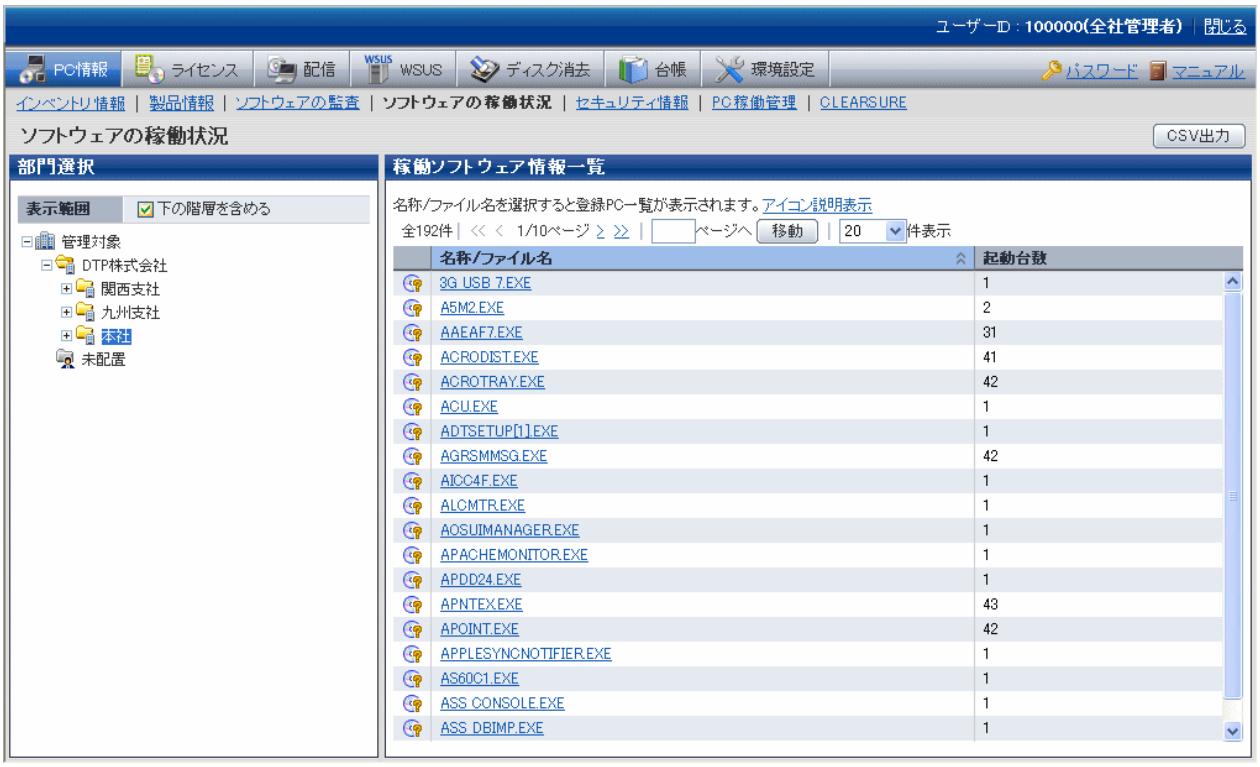
注意

ソフトウェア稼働状況の取得で、以下のEXEは収集できません。

- Windowsインストール時にインストールされる .exeファイル(notepad.exe, iexplore.exe, wordpad.exeなど)
- Systemwalker Desktop PatrolのCS/DS/CT上の各プロセス

ソフトウェア稼働状況は、メインメニューの[PC情報]-[ソフトウェアの稼働状況]画面で表示されます。

各情報の表示内容および表示イメージは、以下のとおりです。



2.1.6 セキュリティ情報

セキュリティ情報として、以下の機能を提供します。

自動ログオン、スクリーンセーバー起動など、セキュリティ設定が低いPCを特定できます。

管理者は、コンピュータウイルスの脅威やセキュリティホールなど、セキュリティ上の問題のあるPCを特定でき、PCの防御能力を高めます。

セキュリティ情報は、メインメニューの[PC情報]-[セキュリティ情報]画面で表示されます。

ただし、Systemwalker Desktop Patrol V13.0.0より前のバージョンがインストールされているPCのセキュリティ情報は参照できません。

セキュリティ情報（システムセキュリティ情報とユーザーセキュリティ情報）は、使用しているOSによって、収集可能なセキュリティ情報が異なり、確認できる項目が異なります。

注意

ユーザーセキュリティ情報は、ログオン時に収集されます。CTインストール後、一度もログオンされていないCTでは収集されていません。

収集できるセキュリティ情報、および表示イメージは以下のとおりです。

システムセキュリティ情報

OSごとに収集可能なシステムセキュリティ情報を以下に示します。

分類	情報	8.1/10	8.1 64bit/10 64bit/11 64bit	2012/ 2016/ 2019	備考
ハードウェア（注1）	BIOS起動パスワード	△	△	△	
	BIOS設定パスワード	△	△	△	
	BIOSハードディスクパスワード	△	△	△	
OS	自動ログオン	○	○	○	
	ようこそ画面	○	○	○	
	最後のユーザー名	○	○	○	
	Guestアカウントのセキュリティ	○	○	○	
	自動更新の設定	○	○	○	
	ユーザーアカウント制御（UAC）	○	○	○	
	安全でない共有フォルダ	○	○	○	
	スタンバイ回復時のパスワード入力	○	○	○	
	複雑なパスワードを必要とする設定	○	○	○	

分類	情報	8.1/10	8.1 64bit/10 64bit/11 64bit	2012/ 2016/ 2019	備考
アプリケーション	ファイアウォール（注2）	○	○	○	
	ウイルス対策ソフトウェアのリアルタイム検索（注3）	○	○	○	
	ウイルス対策ソフトウェアの定時スキャン状況（注4）	○	○	○	
	ウイルス対策ソフトウェアのスキャン対象範囲（注5）	○	○	○	

○：収集できます。

△：OSや機種によっては、収集できない場合があります。

－：収集しない、または該当情報なし。

8.1：Windows 8.1

8.1 64bit：Windows 8.1 64ビット版

10：Windows 10

10 64bit：Windows 10 64ビット版

11 64bit：Windows 11

2012：Windows Server 2012

2016：Windows Server 2016

2019：Windows Server 2019

Systemwalker Desktop Patrolでサポートしている上記OSの各Service Packの詳細については、“3.2.1 動作OS”を参照してください。

注1）

機種によっては、情報が収集できない場合があります。情報が収集できなかった場合は「収集不可」が設定されます。サポートしているか機種かどうかを確認するためのコマンド（BIOSパスワード設定状況確認ツール）が、Systemwalker技術情報ホームページで公開されていますので、このコマンドを使用して事前確認を行ってください。

また、コマンドモードCTでは管理者権限で実行しない場合、BIOSハードディスクパスワードは「収集不可」となります。

注2）

各製品のファイアウォール機能は以下の表記ですが、本書では総称して「ファイアウォール」とよびます。

- Microsoft Windowsの場合：「Windowsファイアウォール」
- Trend Micro ウイルスバスターの場合：「パーソナルファイアウォール」
- McAfee VirusScanの場合：「ポートブロック」

注3）

各ウイルス対策ソフトウェアのリアルタイムスキャン機能は以下の表記ですが、本書では総称して「リアルタイム検索」とよびます。

- Trend Micro ウイルスバスターの場合：「リアルタイム検索機能」
- McAfee VirusScanの場合：「オンアクセススキャン機能」

注4）

各ウイルス対策ソフトウェアの定時スキャン機能は以下の表記ですが、本書では総称して「定時スキャン状況」とよびます

ー Trend Micro ウイルスバスターの場合:「予約検索」

ー McAfee VirusScanの場合:「オンデマンドスキャン」

注5)

各ウイルス対策ソフトウェアのスキャン対象範囲は以下の表記ですが、本書では総称して「スキャン対象範囲」とよびます

ー Trend Micro ウイルスバスターの場合:「検索するファイル」

ー McAfee VirusScanの場合:「スキャンアイテム」

サポート対象の製品一覧および監査可能なリアルタイム検索、ファイアウォール、定時スキャン状況、スキャン対象範囲は以下のとおりです。

表2.1 サポート対象の製品一覧(2022年2月時点)

メーカ	製品名	バージョン	ファイアウォール	リアルタイム検索	定時スキャン状況	スキャン対象範囲
Microsoft	Windows 8.1	なし	○	ー	ー	ー
	Windows 10	なし	○	ー	ー	ー
	Windows 11	なし	○	ー	ー	ー
	Windows Server 2012	なし	○	ー	ー	ー
	Windows Server 2012 R2	なし	○	ー	ー	ー
	Windows Server 2016	なし	○	ー	ー	ー
	Windows Server 2019	なし	○	ー	ー	ー
TrendMicro	ウイルスバスター コーポレートエディション	Ver10.6, 11.0, XG	○(注1)	○	ー	○
Symantec	Endpoint Protection	12.1(注2), 14.x	○	○	○	○
McAfee	VirusScan Enterprise	8.8	○	○	○	○

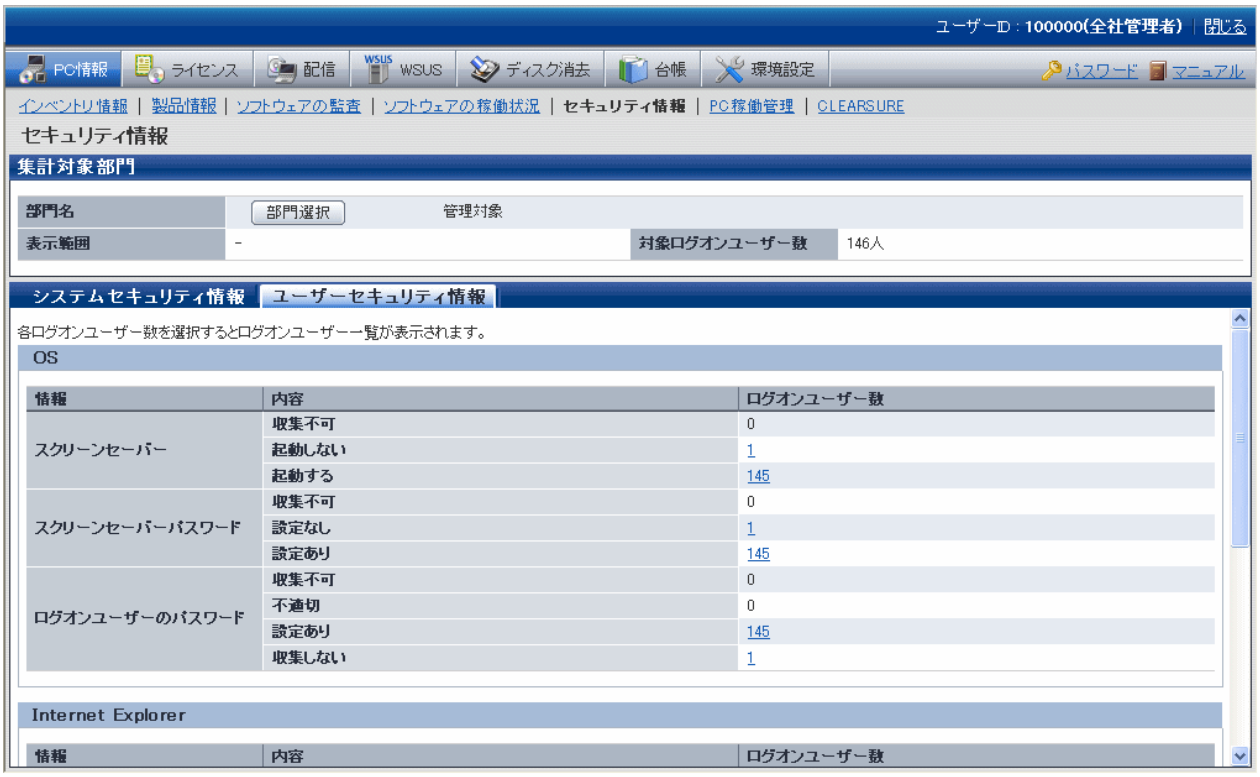
○:監査できます。

ー:監査しない、または該当機能なし。

注1)Client/Server Suite Premiumなどファイアウォール機能を有する製品で有効にした場合

注2)Symantec Endpoint Protection 12.1は、RU1 MP1(12.1.1100)以降をサポートします。

ユーザーセキュリティ情報



OSごとに収集可能なユーザーセキュリティ情報を以下に示します。

分類	情報	8.1/10	8.1 64bit/ 10 64bit/11 64bit	2012/2016 2019	備考
OS	スクリーンセーバー	○	○	○	
	スクリーンセーバー起動までの時間	○	○	○	
	スクリーンセーバーパスワード	○	○	○	
	ログオンユーザーのセキュリティ	○	○	○	
Internet Explorer	インターネットゾーン(注1)	○	△	○	
アプリケーション	Googleデスクトップ「複数のコンピューター上のデータ検索」	○	○	○	

○：収集できます。

△：OSや機種によっては、収集できない場合があります。

8.1：Windows 8.1

8.1 64bit：Windows 8.1 64ビット版

10：Windows 10

10 64bit：Windows 10 64ビット版

11 64bit：Windows 11 64ビット版

2012：Windows Server 2012

2016：Windows Server 2016

2019：Windows Server 2019

注1）

－ Windows 11では“収集不可”が収集されます。

2.1.7 PC稼働管理

PC稼働管理機能は、インテルvProおよびインテルCentrino Proの技術の1つであるインテルAMT（アクティブ・マネジメント・テクノロジー）により、電源OFF状態のPCに対してもリモートから制御できる機能です。

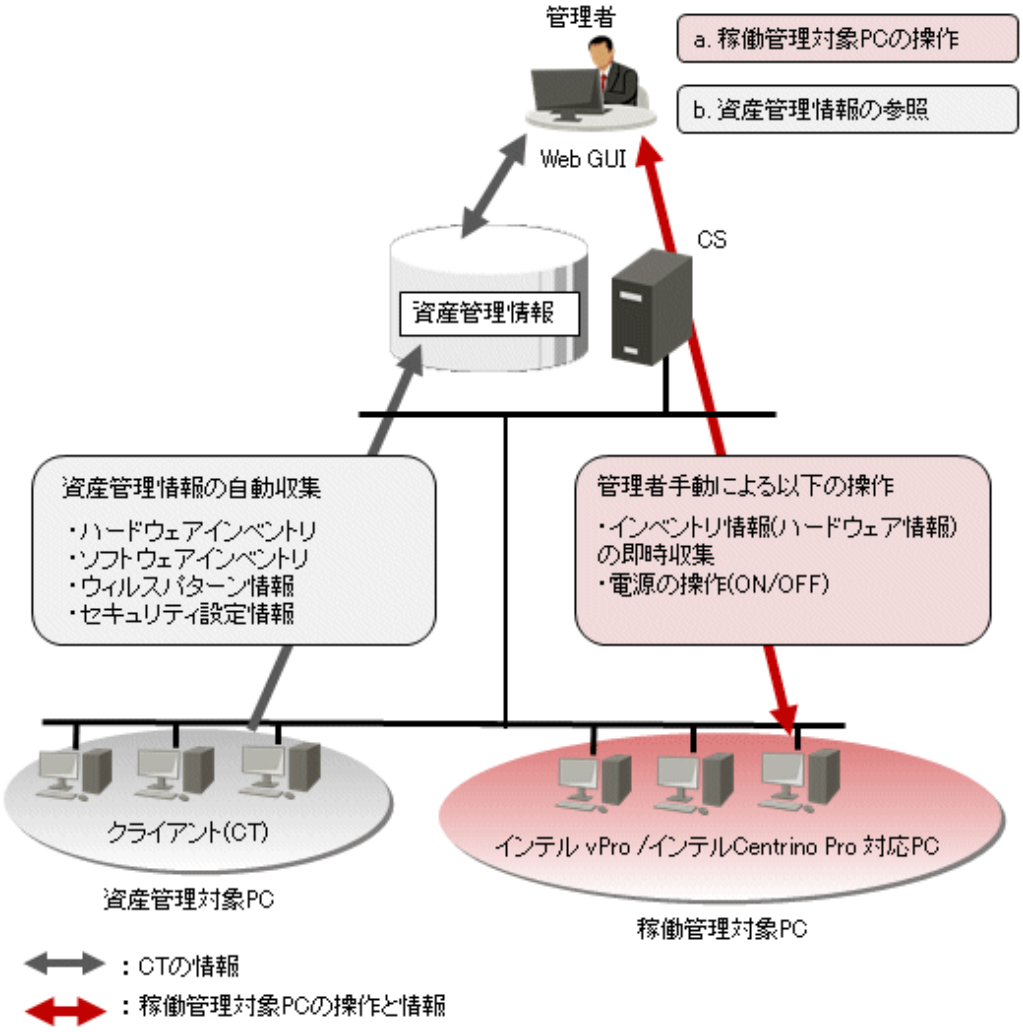
PC稼働管理機能には、以下の機能があります。

- インベントリ情報（ハードウェア情報）の即時収集（注）
- 電源の操作（ON、OFF）

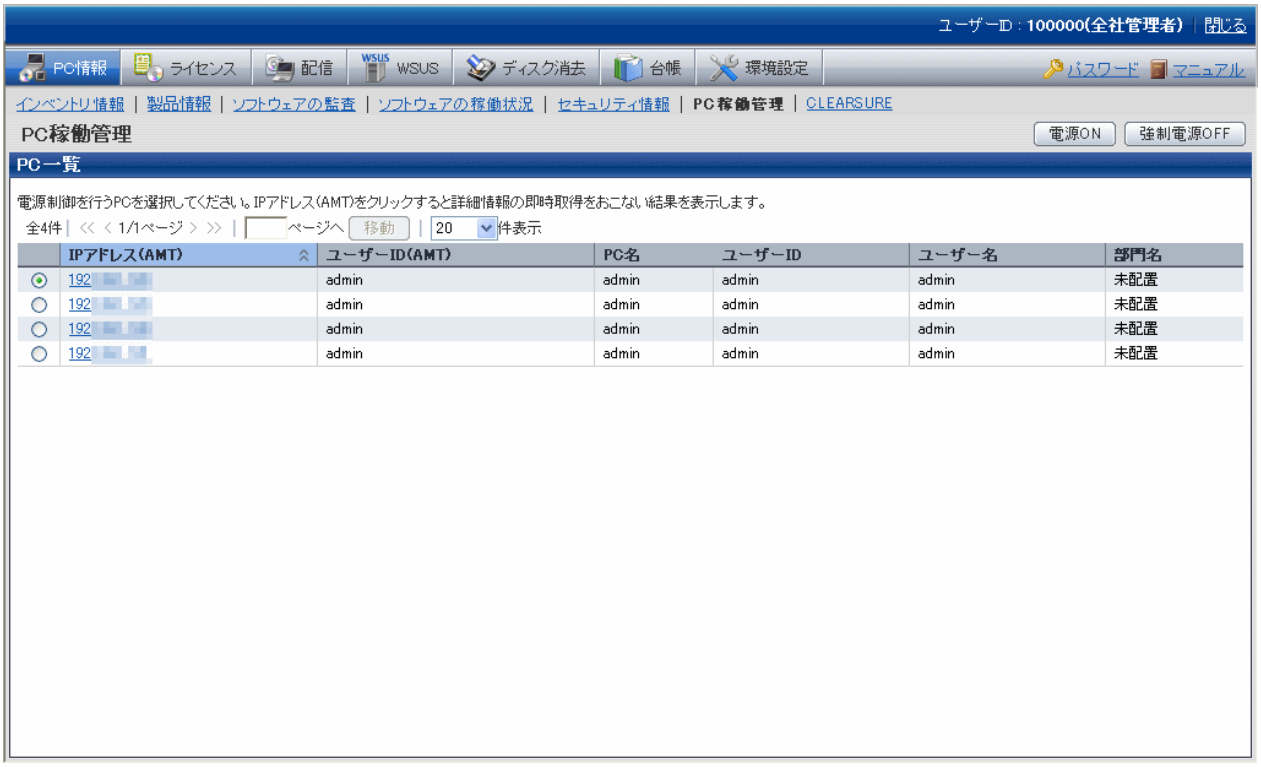
注）

本機能で収集できるインベントリ情報は、インテルAMTを利用したもので、メインメニューの[PC情報]-[インベントリ情報]で参照できるインベントリ情報とは取得内容が異なります。

PC稼働管理機能の概要を以下に示します。



PC稼働管理は、メインメニューの[PC情報]画面で表示されます。



2.1.8 CLEARSURE対応PC

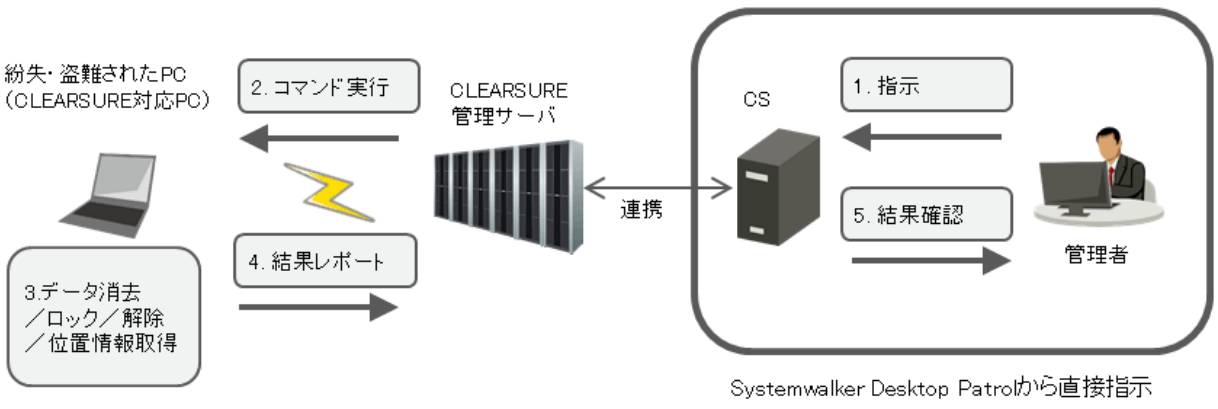
CLEARSUREとは、コンピュータの盗難、紛失時にコンピュータのロックやハードディスクのデータ消去を行うことにより、情報漏えいのリスクを軽減する富士通のソリューションです。

Systemwalker Desktop Patrolは、収集したインベンリ情報からCLEARSURE対応PCの一覧を参照できます。また、CLEARSURE管理サーバと連携することにより、Systemwalker Desktop Patrolの一覧画面から、直接CLEARSURE対応PCの操作が行えます。

注意

「CLEARSURE 3G/LTE」は本連携機能の対象外となりますので、ご注意ください。

Systemwalker Desktop Patrolを使った運用イメージを以下に示します。



CLEARSURE対応PCの表示

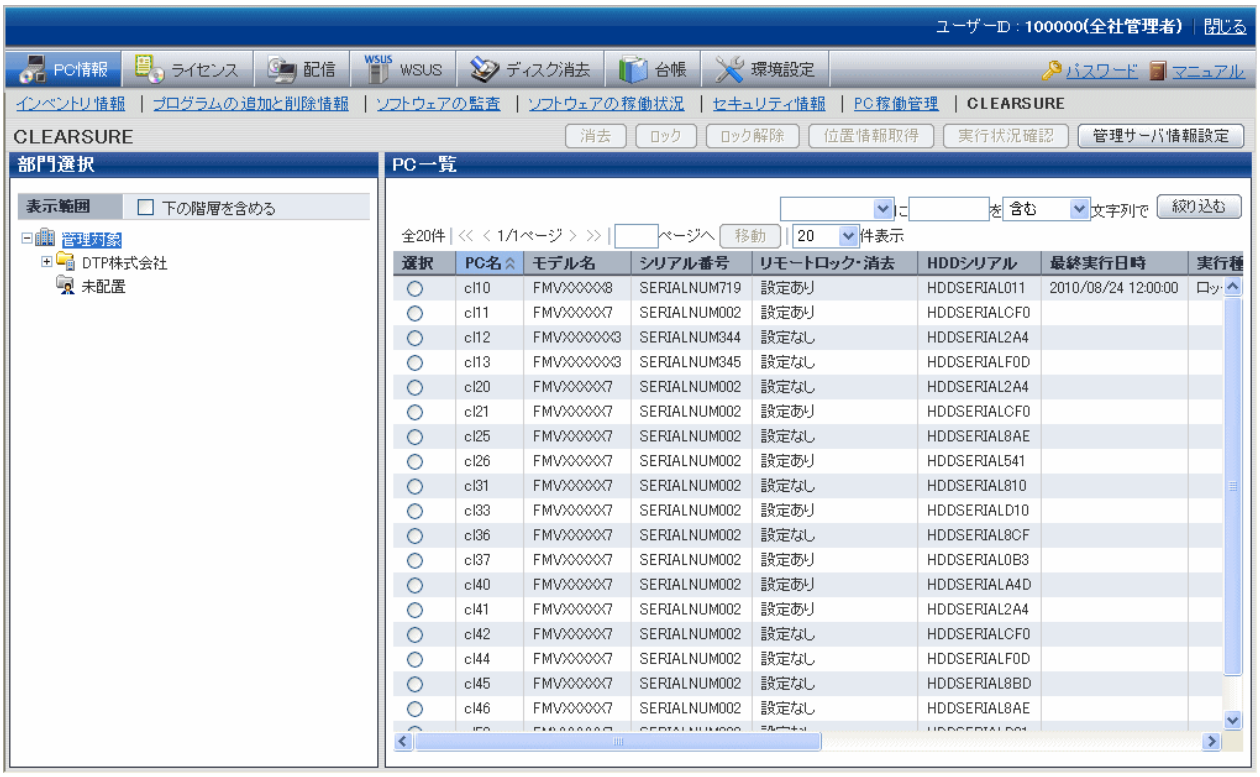
Systemwalker Desktop Patrolで収集したインベンリ情報から、CLEARSUREに対応しているPCの一覧を参照できます。

CLEARSURE対応PCは、メインメニューの[PC情報]画面で表示されます。

CLEARSURE対応PCの操作

Systemwalker Desktop Patrolのメインメニューから、CLEARSURE対応PCに対して、以下の操作を行うことができます。

- 消去
- ロック
- ロック解除
- 位置情報取得



2.1.9 ファイル収集

指定したファイルを収集する機能です。

例えば、アプリケーションのログファイルを収集することで、CTがインストールされたPCの状況などを確認できます。

収集したファイルは、CSに保存されます。

2.1.10 運用状況の表示と運用対処

運用状況の表示

メインメニューのトップ画面「状況画面」で、Systemwalker Desktop Patrolの運用状況が短時間で把握できる機能です。

「状況画面」の集計情報一覧を表示・参照することで、以下のことが可能となります。

1. 「状況画面」を参照するだけで、業務への影響の有無が一目で把握できます。

2. 複数観点の集計項目別の状況が把握できるため、業務を遂行していくために何が問題となってくるのかが即座に判断できます。

   各集計項目は、以下のとおりです。

   - インベントリ情報が収集されていないPC
   - セキュリティパッチが適用されていないPC
   - WSUSに正常で報告されていないコンピュータ
   - セキュリティポリシーに違反しているPC
   - 省電力ポリシーに違反しているPC
   - ライセンスがないソフトウェアを導入しているPC
   - 期限が超過している契約
   - 期限が近づいている契約
   - 棚卸が完了していない機器
   - 未登録機器として検出された機器

3. 集計項目別に詳細な情報が表示されますので、項目に関する問題点の絞り込みが容易となります。

   詳細情報は、以下のとおりです。

   - 部門別の集計
   - 項目別の集計

4. 集計項目別に該当PC/機器/契約を表示しますので、該当PC/機器/契約を絞り込む手間が省け、即座に該当PC/機器/契約に対する対処が可能となります。

5. Systemwalker Desktop Keeperを導入しているシステムでは、Systemwalker Desktop Keeperへのログイン操作の手順が省け、更に「状況画面」でSystemwalker Desktop Keeperの状況（操作ログ結果等）も含めて表示されますので、「状況画面」1画面で、個々の製品観点での確認が可能となります。

運用対処

「状況画面」の集計項目別の結果から問題のあるPC/機器/契約を検出/参照した操作の延長で、資産管理の見直し、各PC/機器/契約に対する自動対処、利用者に対する注意喚起などの運用対処も可能となります。

「状況画面」で可能な運用対処は、以下のとおりです。

1. メッセージ送信

   - 問題のあるPC/機器/契約にメッセージを送信し、PC/機器/契約の利用者に対して運用上問題のある利用方法であることを自覚してもらうことができます。
   - 運用設定の診断結果画面を使用した運用を実施しているにも関わらず集計項目に該当するPC/機器/契約は、利用者が運用設定の診断結果画面で対処を実施していないことになりますので、メッセージ送信を利用して対処を促すことができます。
   - メッセージ送信はインベントリ情報画面からも対処可能です。利用者にメッセージを送りたい時に利用できます。

2. インベントリ収集

   インベントリを収集します。
   インベントリを収集のスケジュールを待たずに即座に収集できます。

3. インベントリ削除

   インベントリを削除します。
   Systemwalker Desktop Patrolの管理上、不要となったインベントリ情報をすべて削除できます。

4. セキュリティパッチの適用

   セキュリティパッチを適用します。
   利用者がセキュリティパッチを適用しない、セキュリティパッチの適用方法が分からない時に使用します。

5. セキュリティ設定の変更

   セキュリティポリシーに従った内容で、セキュリティ設定を変更します。

   以下のような場合に使用できます。

   ー システム管理者や部門管理者が複数PC/機器/契約を管理している場合の一括対処

   ー 診断画面を使用しない運用において、利用者がセキュリティ設定の変更方法が分からない場合のリモートによる対処

6. 省電力設定の変更

   省電力ポリシーに従った内容で、省電力設定を変更します。

   利用者が省電力設定を変更しない、省電力設定の変更方法が分からない時に使用します。

7. その他、各項目に沿った対処が行えます。

2.1.11 CT動作状況チェックコマンド

CTの動作状況を画面で確認することができる機能です。

CSおよび該当CT上の画面で、CSで設定したポリシーの設定どおりCTが動作しているのか、CTがどのように動作して次はいつ動作するのかを確認することができます。

本機能は、以下のような場合に使用できます。

・ 運用開始時

  管理者がSystemwalker Desktop Patrolを新規に導入する際、およびシステムの構成変更、運用ポリシーの設定変更する際に、CSで設定したポリシーが管理者の意図どおりに正しく動作しているか確認する場合

・ トラブル発生時

  Systemwalker Desktop Patrolを運用中、CTでセキュリティパッチが適用されないなど、何らかのトラブルが発生した場合
  コマンドの出力結果からCTの動作状況を確認して、どのような問題があるのかを確認することができます。

2.1.12 簡易操作ログファイル収集

CTがインストールされたPCでユーザーが行った操作をログとして保存し、そのログファイルを収集する機能です。

簡易操作ログを確認することで、以下の効果が期待できます。

・ 情報漏洩に対する抑止効果

・ PCでの問題発生時の操作追跡

簡易操作ログファイルには、以下の情報が保存されます。簡易操作ログファイルを元に、実際にユーザーが行った操作を推測することが可能となります。

・ ユーザーが表示したウィンドウタイトルの取得

  ー 実行されたプログラムの名前

  ー ウィンドウタイトル

  ー ウィンドウがアクティブになっていた時間

・「実行ファイルの制御」で指定したファイルの起動による警告や停止情報

・ ユーザーのログオン/ログオフ状況

・ システムの起動時刻/終了時刻

2.2 PCの監査/統制機能

管理者が決定した省電力ポリシー／セキュリティポリシーでPCを監査できます。ポリシー違反があった場合は、PCの画面に警告を表示して利用者に対処を促します。

また、ポリシー違反項目を強制的に変更することもできます。(注)

注) 項目によっては強制的に変更できないものがあります。

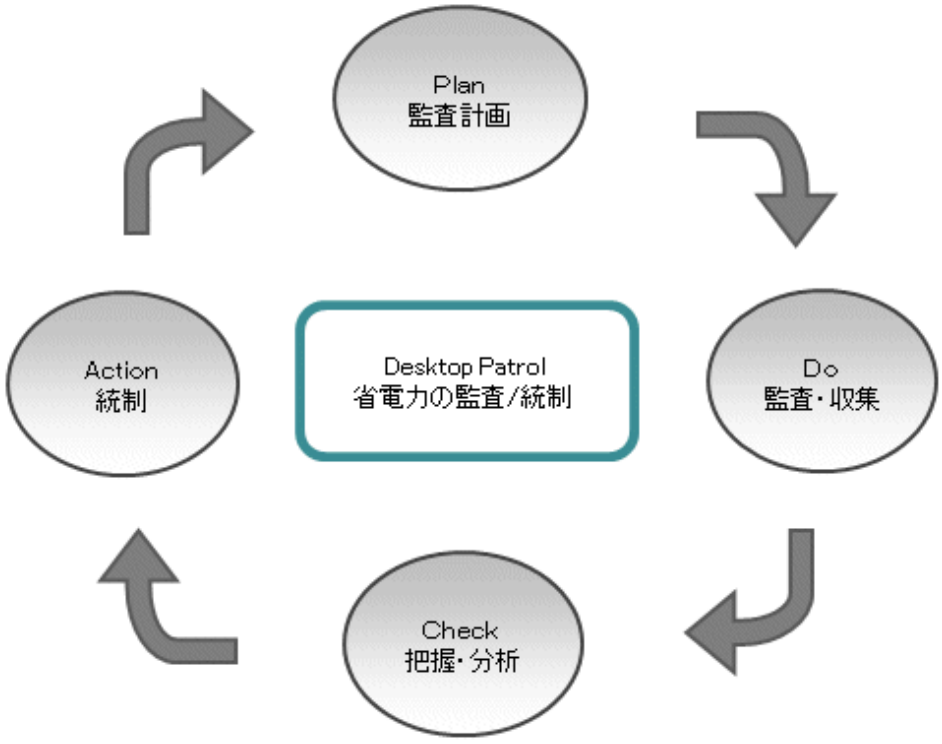
省電力とセキュリティの監査／統制では、以下の機能を利用できます。

- ポリシーに違反したPCへの警告画面の表示／設定の強制変更
- レポート出力によるセキュリティ／省電力の統制状況の確認

2.2.1 省電力設定の監査/統制

PCの省電力の監査/統制は以下の流れで運用を行います。

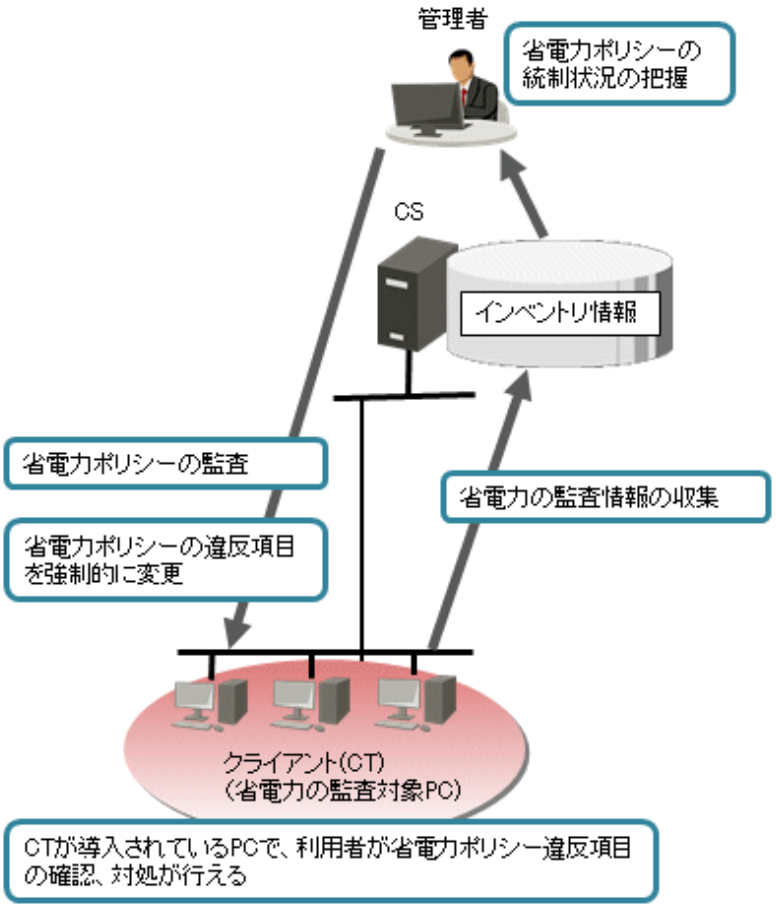
- 監査計画：運用システムにおける省電力の監査計画を行います。
- 監査・収集：PCの省電力設定状況の情報を収集します。
- 把握・分析：PCの省電力設定状況の確認・分析を行います。
- 統制：分析の結果対策が必要なPCに対して統制を実施します。



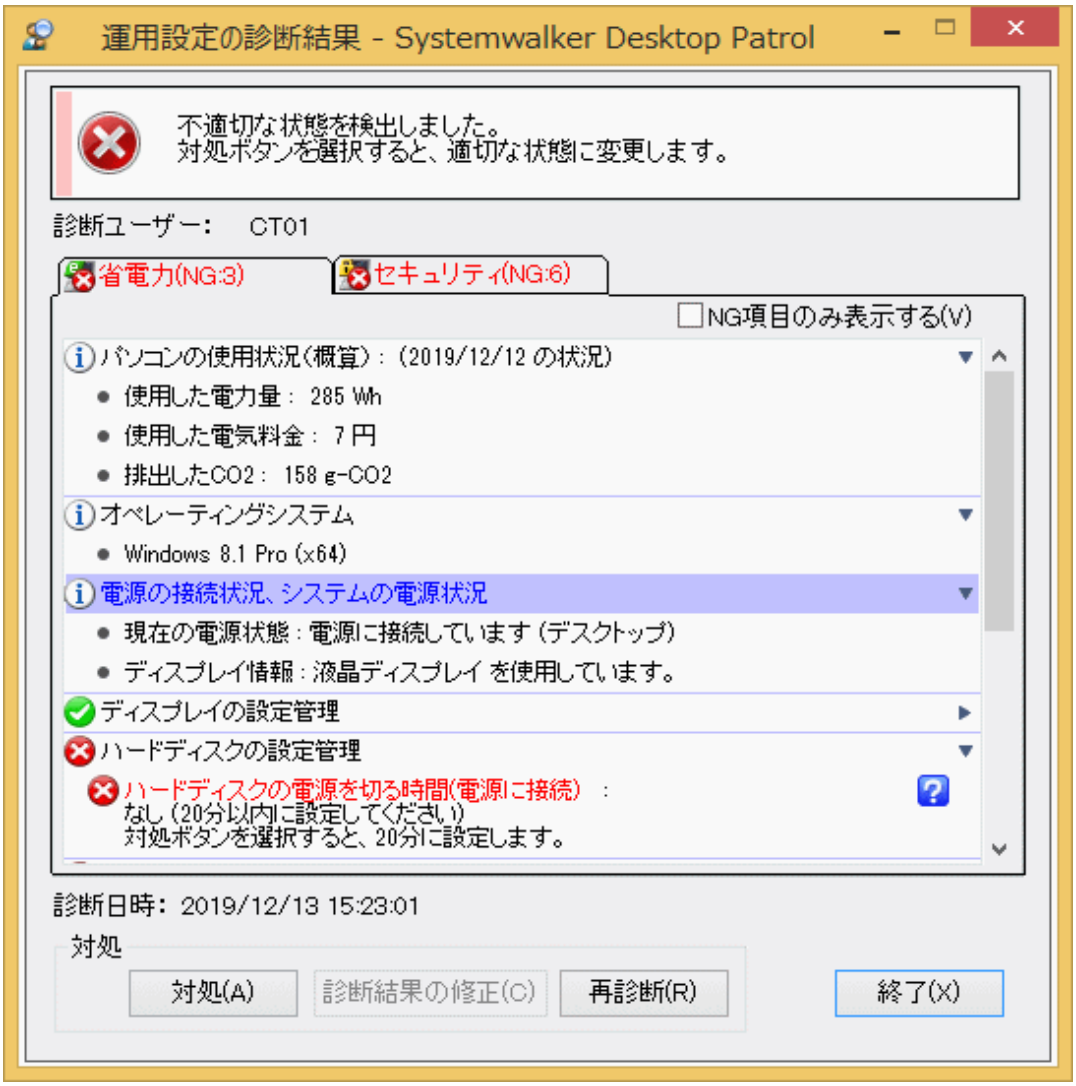
この監査/統制のPDCAサイクルを、Systemwalker Desktop Patrolの機能を利用して実現する場合の動作概要を以下に示します。

省電力の監査、統制の状況および消費電力量は、以下のレポートで確認できます。

- 省電力設定状況レポート
- 消費電力量の監査レポート



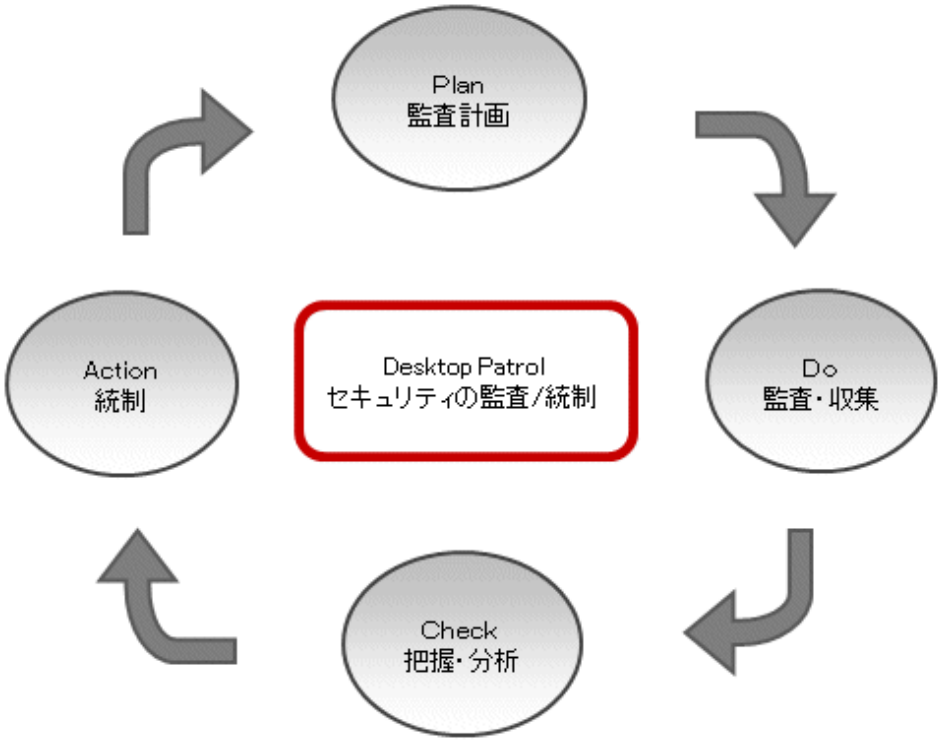
クライアント側で表示される省電力設定の診断結果画面を以下に示します。



2.2.2 セキュリティ設定の監査/統制

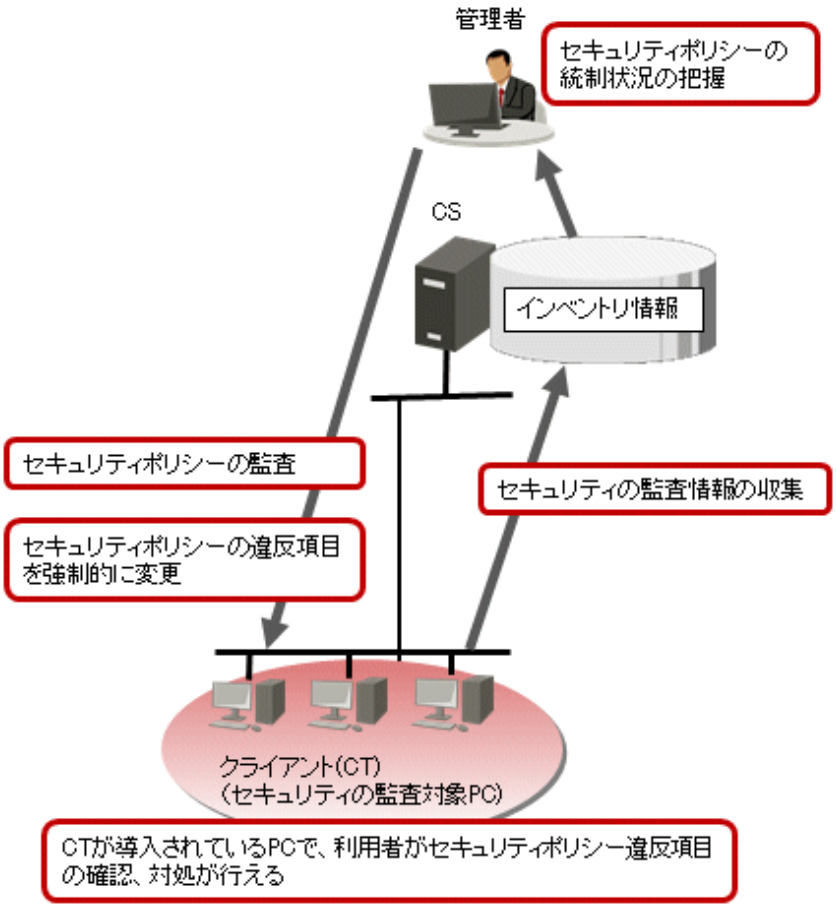
PCのセキュリティの監査/統制は以下の流れで運用を行います。

- 監査計画：運用システムにおけるセキュリティの監査計画を行います。
- 監査・収集：PCのセキュリティ設定状況の情報を収集します。
- 把握・分析：PCのセキュリティ設定状況の確認・分析を行います。
- 統制：分析の結果対策が必要なPCに対して統制を実施します

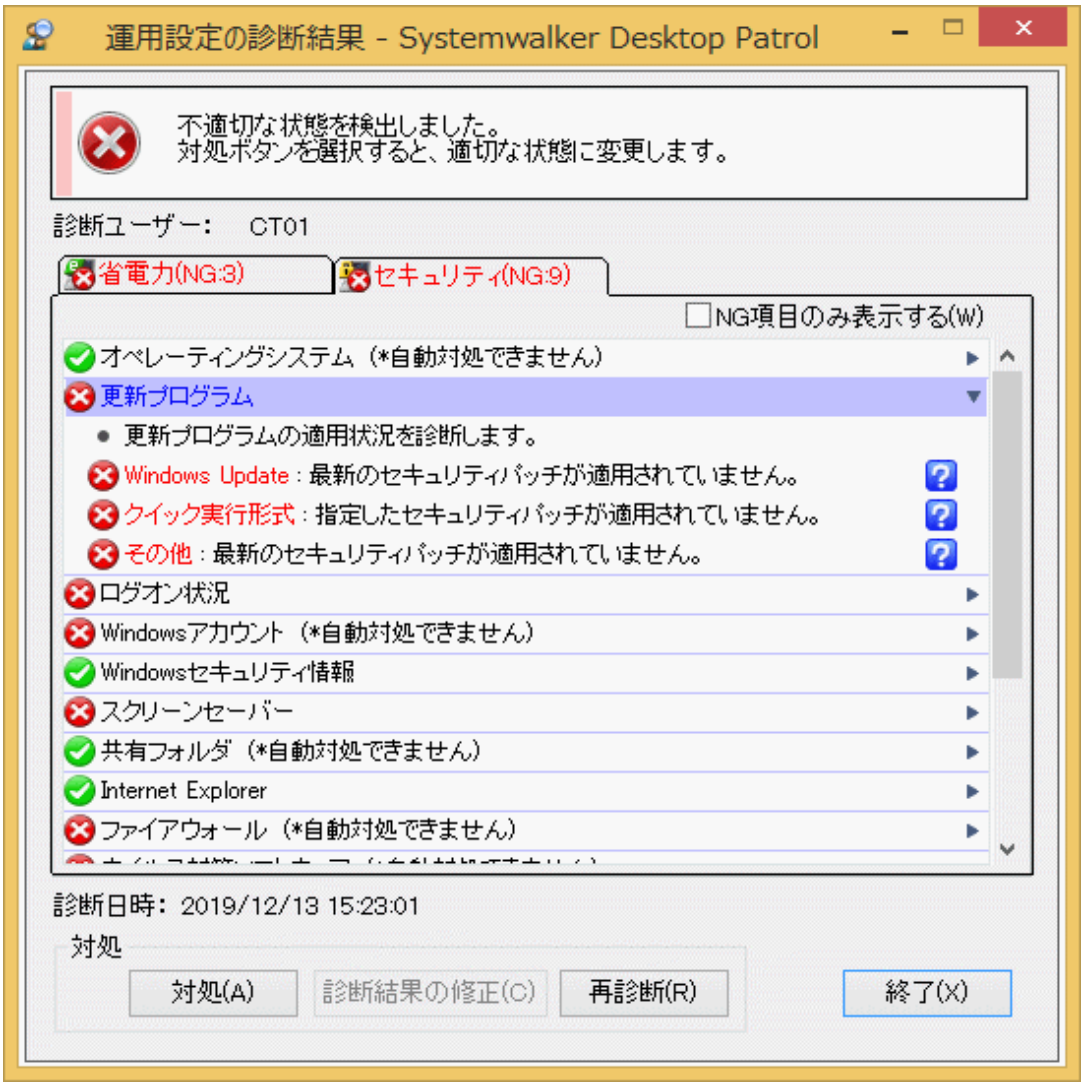


この監査/統制のPDCAサイクルを、Systemwalker Desktop Patrolの機能を利用して実現する場合の動作概要を以下に示します。

セキュリティポリシーの統制状況は、セキュリティ監査レポートで確認できます。



クライアントで表示されるセキュリティ設定の診断結果画面を以下に示します。



2.3 ライセンス管理機能

Systemwalker Desktop Patrolのライセンス管理機能について説明します。

2.3.1 ライセンス管理

Systemwalker Desktop Patrolのライセンス管理は、個々のPCにライセンスを割り当てることでライセンスを管理します。

ライセンス管理を行うためには、以下の3つの前提条件があります。

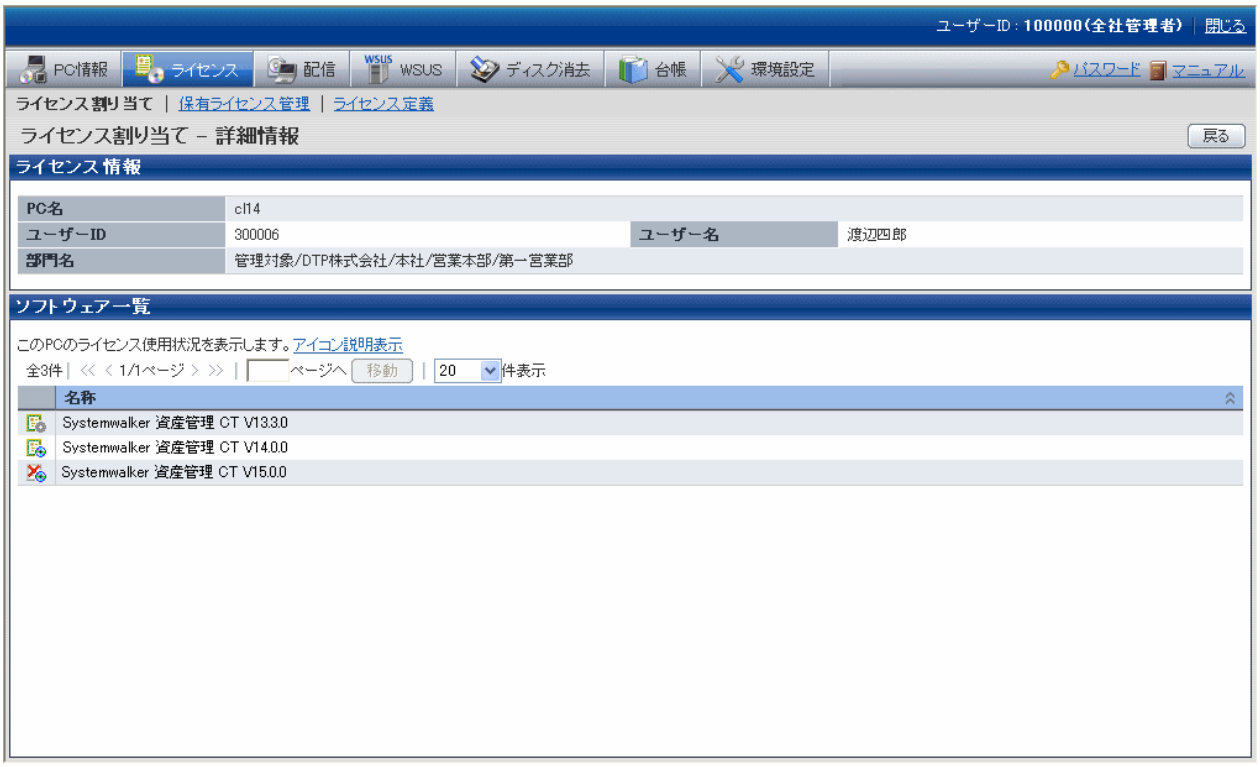
- 「ソフトウェア辞書」が登録されていること
- メインメニューの[ライセンス]-[ライセンス定義]で、ライセンスとソフトウェア（辞書コード）の関係が定義されていること
- メインメニューの[ライセンス]-[保有ライセンス管理]で、各部門にライセンス数が設定されていること

メインメニューの[ライセンス]-[ライセンス割り当て]で、各PCで利用するソフトウェア毎にライセンスを割り当てることにより、ライセンス数の管理を行います。

割り当てられたソフトウェアの使用状況は、メインメニューの[ライセンス]-[ライセンス割り当て]で確認できます。

イベント設定を行うことで、ライセンスの割り当てがないソフトウェアを利用しているPCを発見した時、メールで違反を管理者に通知したり、イベントログにエラーログを書き出したりできます。

ライセンスの使用状況の詳細は、メインメニューの[ライセンス]-[ライセンス割り当て]画面で、PC名を選択することで以下のように表示されます。



ユーザー資産ソフトウェア辞書の作成機能

管理を行いたいソフトウェア製品がソフトウェア辞書のサポートセンター定義に定義されていない場合は、ソフトウェア辞書のユーザー定義を追加する必要があります。

ユーザー資産ソフトウェア辞書作成機能は、このソフトウェア辞書のユーザー定義を、インベントリ情報として収集した“製品情報”から簡単に定義できる機能です。

各PCに導入済みのソフトウェア製品を容易にライセンス管理の対象にできるため、ICT資産の有効活用とソフトウェアライセンスの不足分を把握できます。

SAMACのソフトウェア辞書の移入

一般社団法人 ソフトウェア資産管理評価認定協会(SAMAC)のソフトウェア辞書を、Systemwalker Desktop Patrolに移入して運用できます。

移入したSAMACのソフトウェア辞書のデータは、ユーザー定義として運用します。

監査対象のソフトウェアを選択することで、ソフトウェアの導入状況の検出やライセンス管理が可能です。

2.3.2 実行ファイルの制御

業務上使用する必要がないアプリケーションを「実行ファイルの制御」として定義し、インストールされたPCを検出できます。

また、クライアントでの使用を抑止するために、該当のアプリケーションを起動した場合、ユーザーに警告メッセージを出したり、該当のアプリケーションの起動を抑止できます。

2.4 ファイル配信機能

Systemwalker Desktop Patrolのファイル配信機能について説明します。

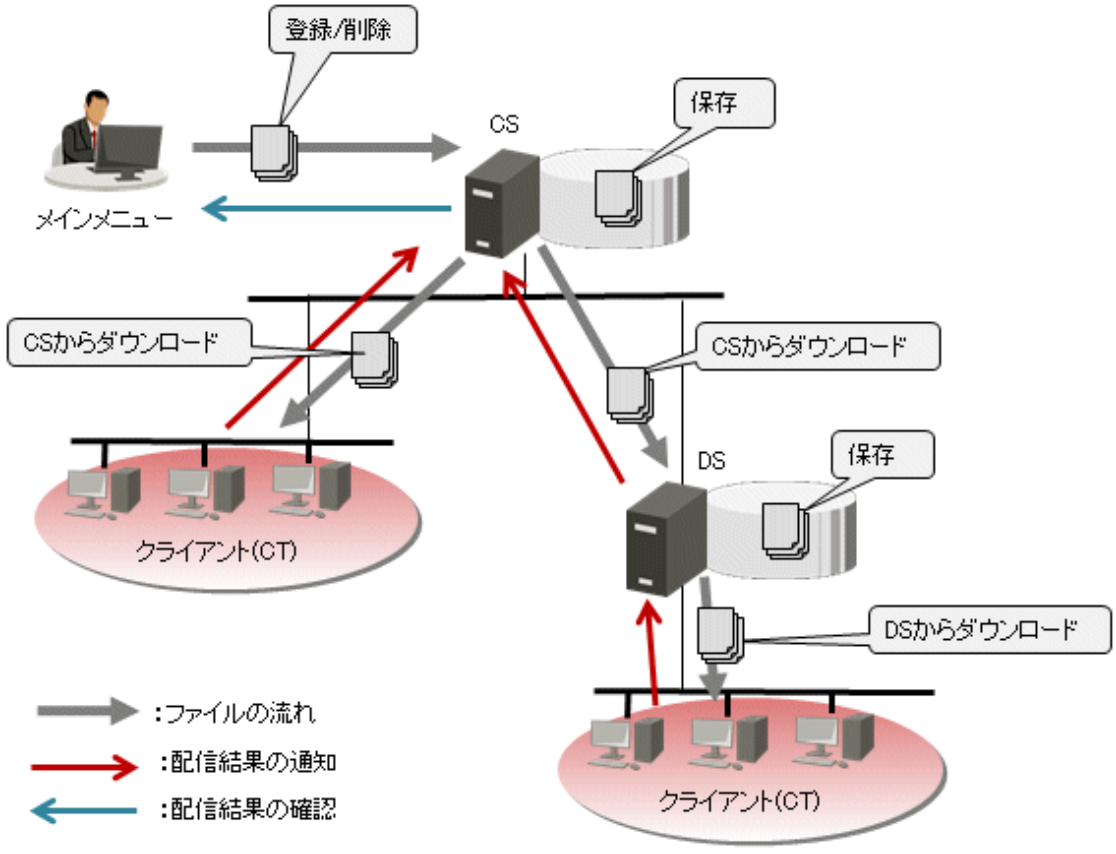
ファイル配信機能は、CS上の操作だけで、CSから複数のCTに複数ファイルを配信できる機能です。また、配信結果についても、CSで確認することができます。

本機能は、定義ファイルや実行ファイルのファイル置換えなど、容易にファイルの配信を実施したい場合の使用をおすすめします。

ソフトウェアのインストールまでを含めた配信を実施したい場合は“2.5 ソフトウェア配信機能”を使用してください。また、セキュリティパッチの適用を行いたい場合は、“2.6 セキュリティパッチの配信/適用機能”を使用してください。

Systemwalker Desktop Patrolのファイル配信機能は、以下の3つから構成されます。

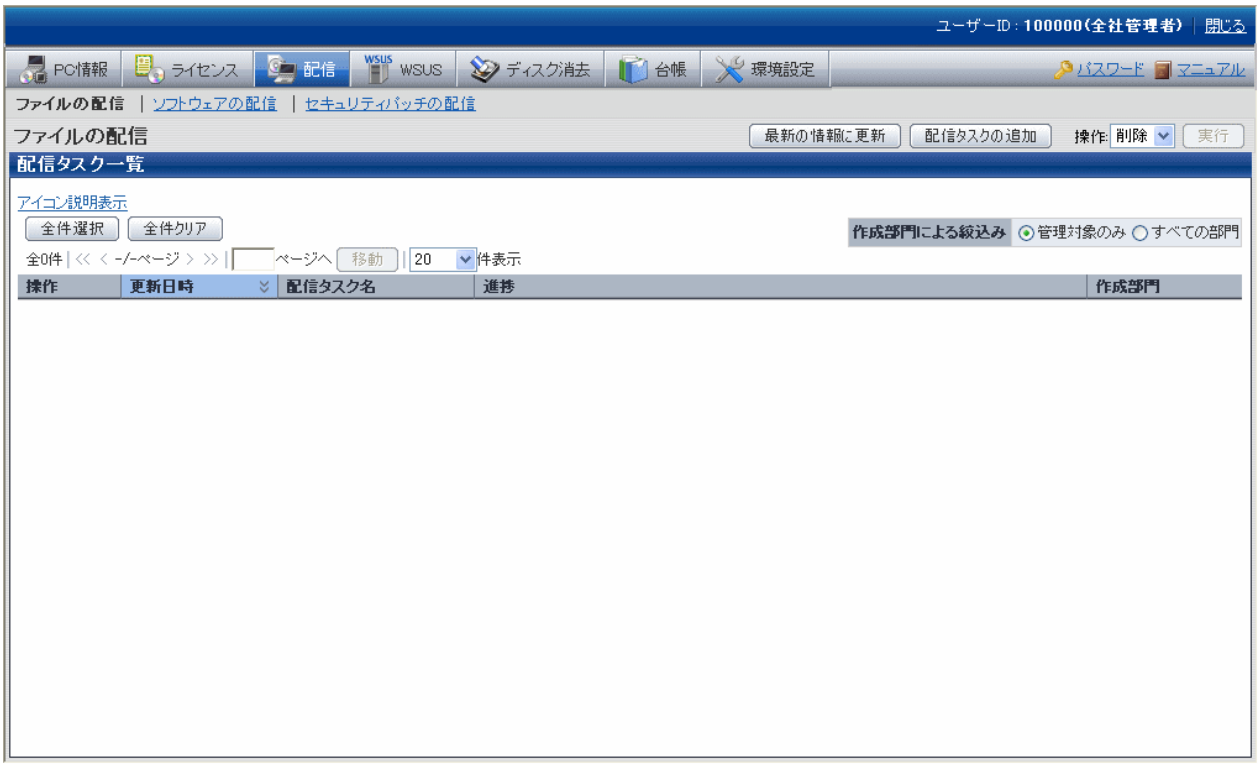
- ファイルと配信先の配信設定
- ファイルのダウンロード
- 配信結果の確認



2.4.1 ファイルと配信先の配信設定

配信したいファイルを配信ファイルとして設定し、CTを配信先として設定します。

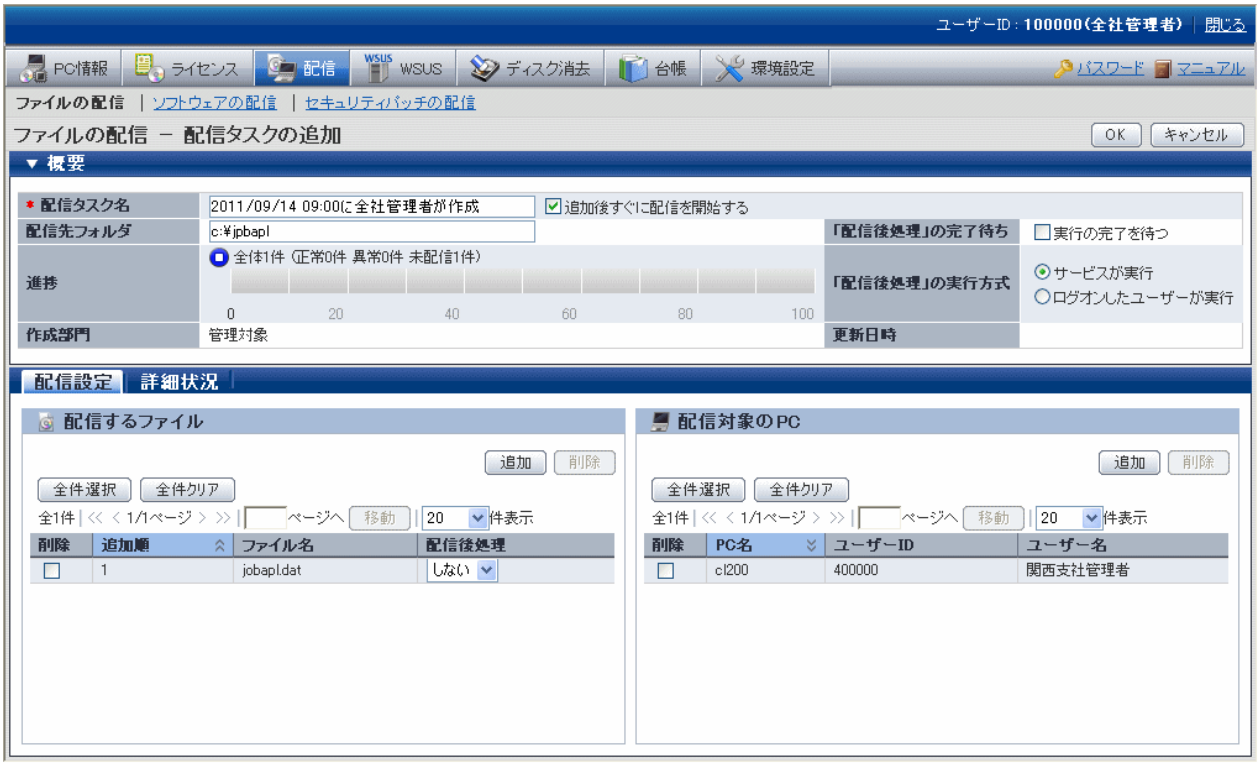
配信設定は、CSのメインメニューの[配信]-[ファイルの配信]の初画面で行います。



2.4.2 ファイルのダウンロード

設定内容に応じて配信が開始され、配信ファイルがダウンロードされます。

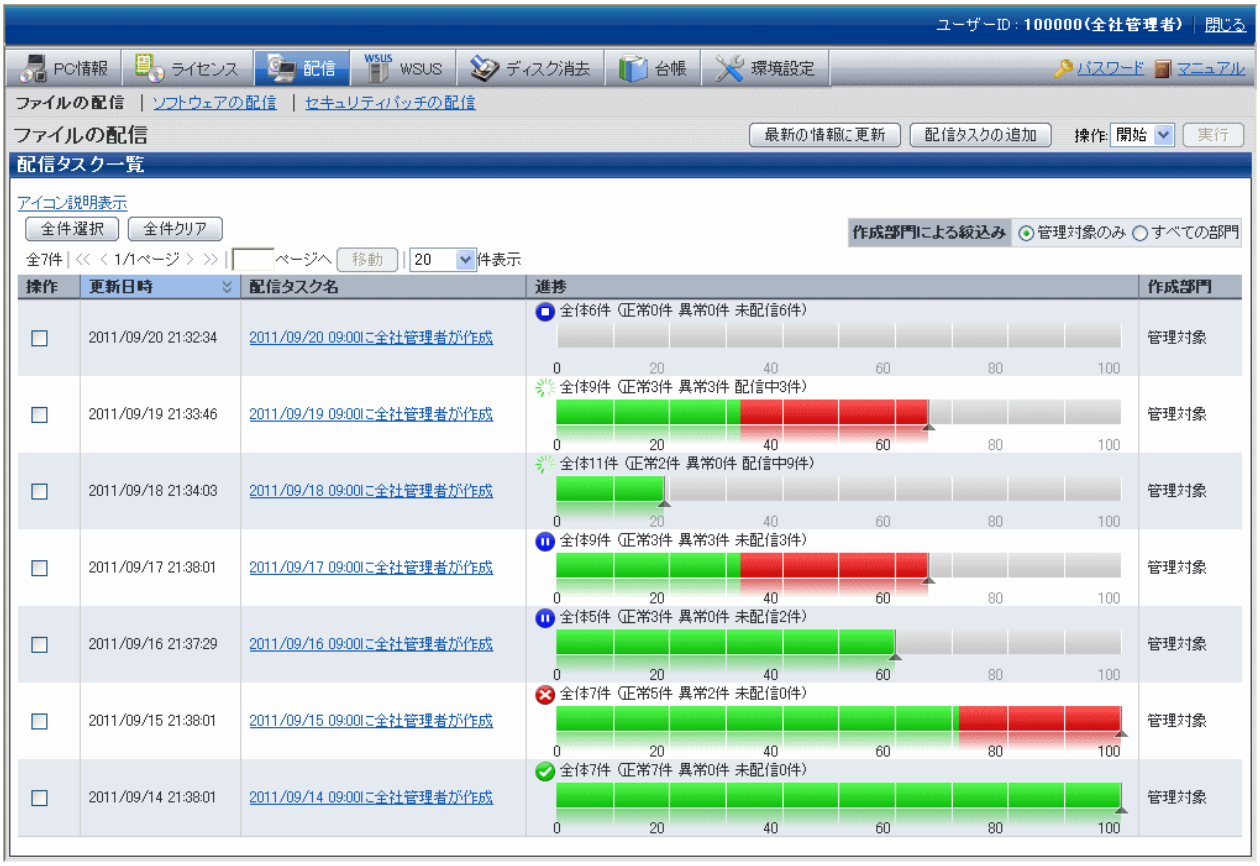
メインメニューでの配信設定後、すぐに配信を開始する設定にした場合、設定画面で[OK]ボタンをクリックすると、配信が開始されます。



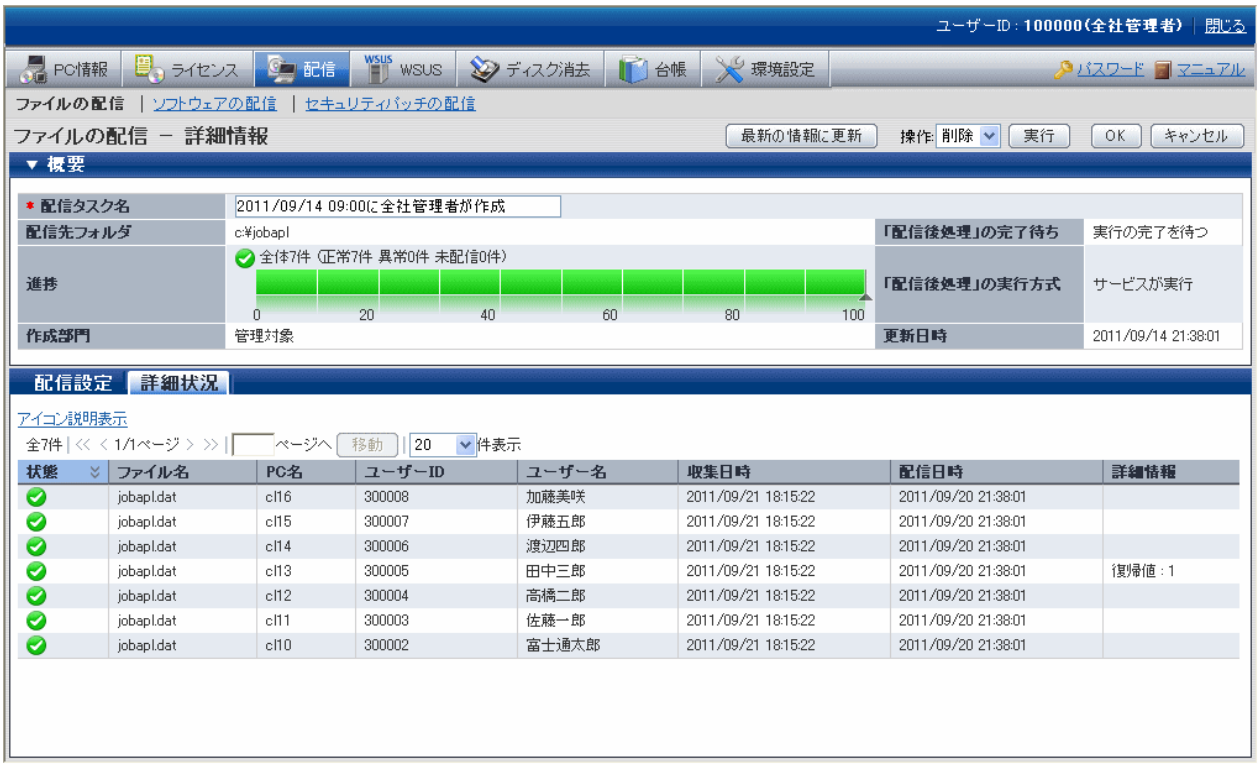
2.4.3 配信結果の確認

配信した結果は、[ファイルの配信]の初画面で確認できます。

メインメニューでの配信設定後、すぐに配信を開始する設定にした場合、約20分前後で配信結果を確認できます。



個々の配信タスクの配信結果の詳細を確認したい場合は、配信タスクのリンクをクリックすると、詳細情報についても確認できます。



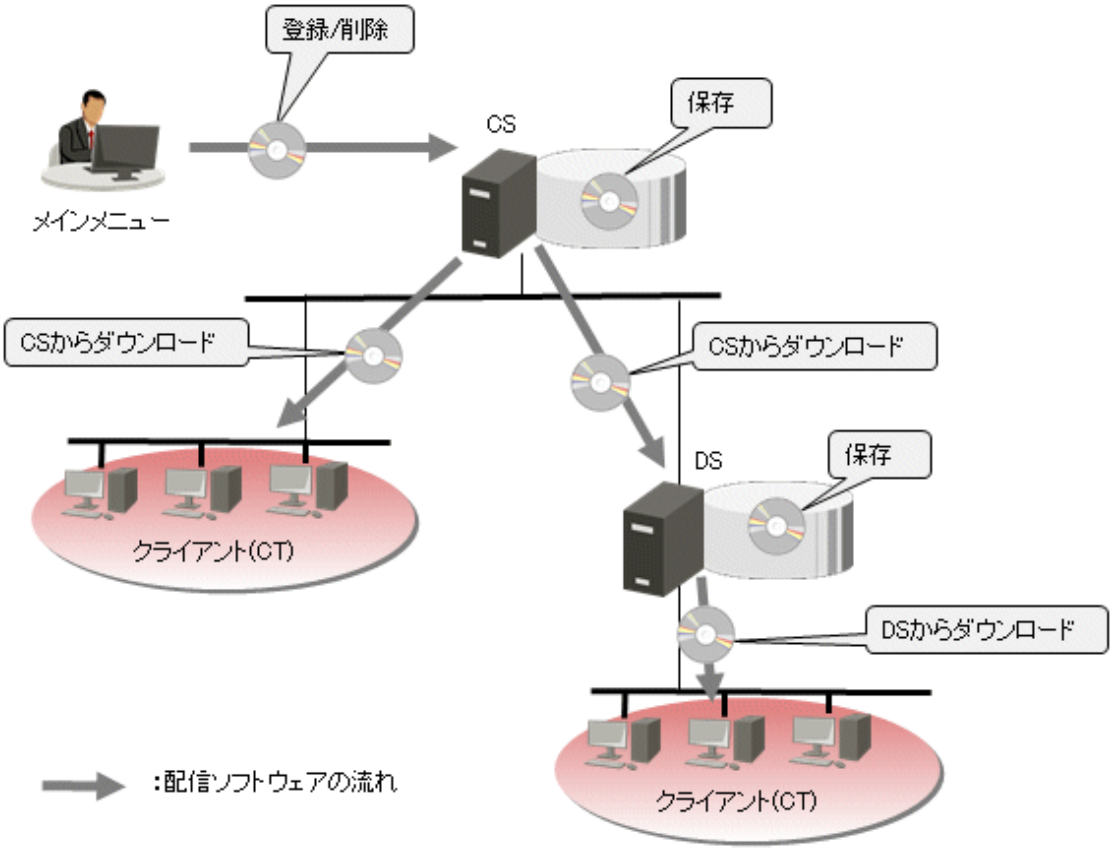
2.5 ソフトウェア配信機能

ソフトウェア配信機能は、ファイル単位からソフトウェア単位までの配信対象のデータを上位サーバで管理し、配信先に指定されたサーバまたはPCが、上位サーバからダウンロードできる機能です。

Systemwalker Desktop Patrolのソフトウェア配信機能は、以下の3つから構成されます。

- 配信ソフトウェアの管理
- ソフトウェアの配信先の設定
- 配信ソフトウェアのダウンロード

Systemwalker Desktop Patrolのソフトウェア配信機能では、ファイルだけでなくソフトウェアも配信できます。

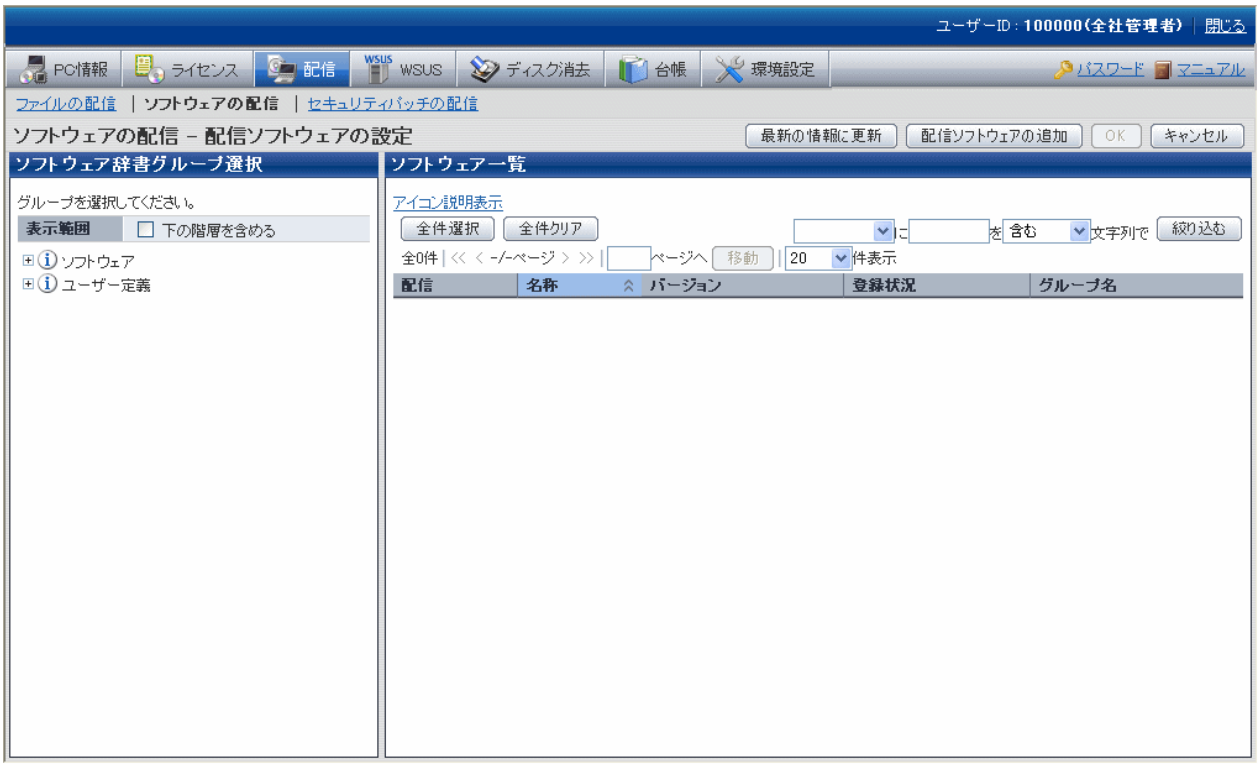


2.5.1 配信ソフトウェアの管理

配信ソフトウェアを管理するため、以下のことができます。

- 配信ソフトウェアの新規登録、更新または削除
- 配信ソフトウェアグループの作成

配信ソフトウェアの管理は、メインメニューの[配信]-[ソフトウェアの配信]-[配信用ソフトウェアグループの追加]-[配信ソフトウェアの設定]画面で行います。



配信ソフトウェア

Systemwalker Desktop Patrolでは、ファイルやソフトウェアを、配信ソフトウェアとして登録できます。

配信ソフトウェアには、名称、バージョン、有効期間、サイズなどの項目を設定できます。

配信ソフトウェアの「有効期間」で指定した期間だけ管理下のPCが配信ソフトウェアを参照・ダウンロードできます。(ニュースコンテンツなどのように、ある期間だけ意味を持つようなものに使用します。)

配信ソフトウェアをサーバやクライアントにダウンロードしたときに、自動適用(インストール)するための実行ファイル(ダウンロード後実行ファイル)を指定できます。実行するために管理者権限が必要なソフトウェアについては、サービス権限を設定できます。

配信用ソフトウェアグループ

配信ソフトウェアを分類管理するために、グループを作成できます。グループには、配信先サーバを設定できます。

配信用ソフトウェアグループに設定する「配信先サーバ」は、そのグループの配信ソフトウェアをどのサーバに配信するかを指定するものです。配信先に指定されたサーバが上位サーバから配信ソフトウェアをダウンロードします。CTは、上位サーバから配信ソフトウェアをダウンロードできます。

2.5.2 ソフトウェアの配信先の設定

ソフトウェアの配信先として、以下の配信先を設定できます。

- CS

  物理的なサーバです。CS配下のPCだけにソフトウェアを配信したい場合に指定します。

- DS

  物理的なサーバです。DS配下のPCだけにソフトウェアを配信したい場合に指定します。

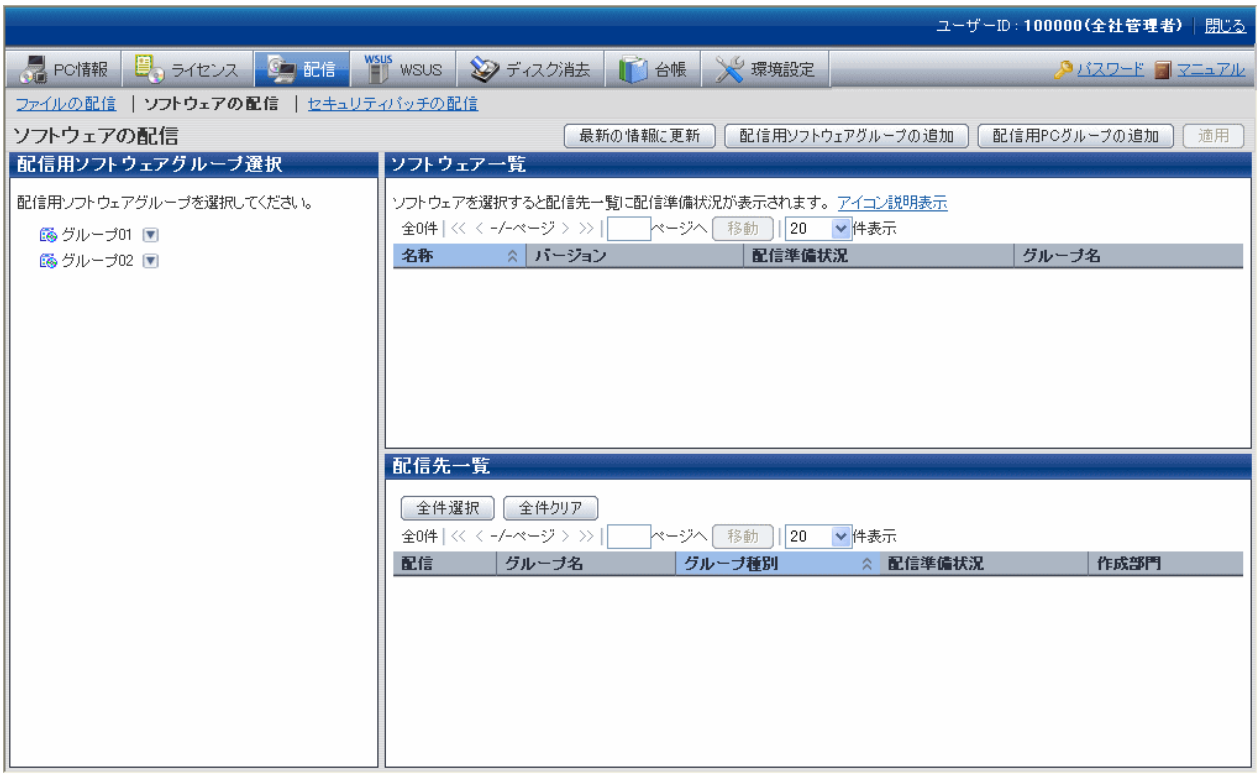
- ポリシーグループ

  ポリシーグループに登録されているPCに配信したい場合に指定します。

・ 配信用PCグループ

配信用PCグループに登録されているPCに配信したい場合に指定します。

配信先の設定は、メインメニューの[配信]-[ソフトウェアの配信]画面で行います。



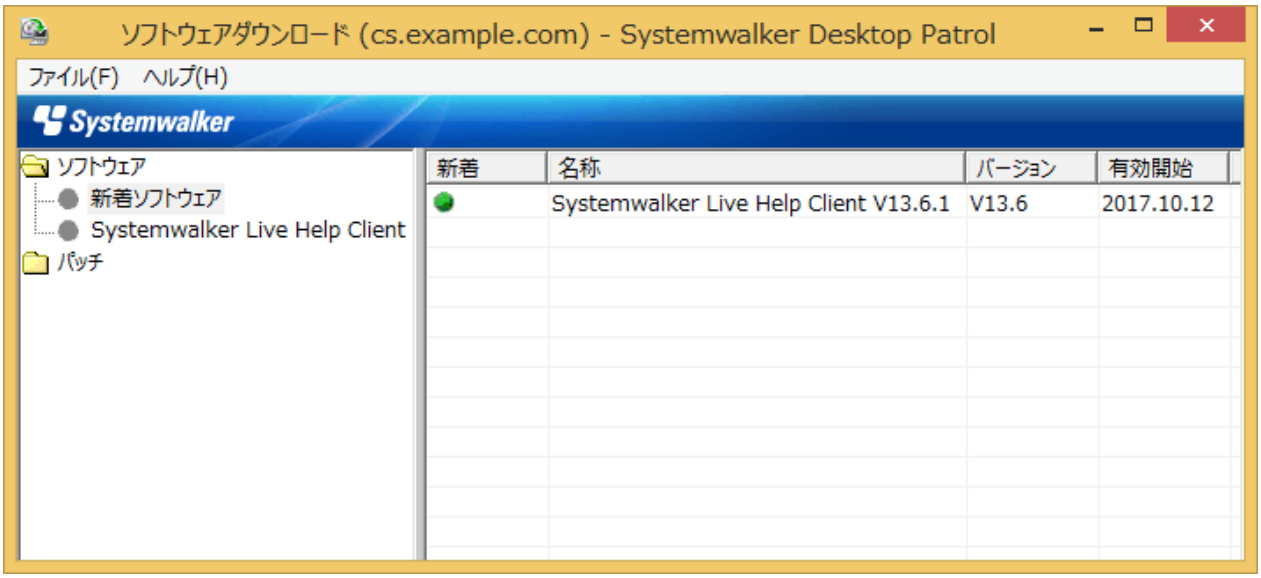
2.5.3 配信ソフトウェアのダウンロード

配信ソフトウェアのダウンロードとは、配信ソフトウェアを上位サーバからCTへダウンロードする機能です。

CTでは、手動ダウンロードを行う場合は、[ソフトウェアダウンロード]画面を起動し、ダウンロード操作を行います。

CTでの配信ソフトウェアダウンロード

CTでの配信ソフトウェアダウンロードは、CTの[ソフトウェアダウンロード]を起動するか、または新着ソフトウェアを知らせるメッセージに応答することにより、実行できます。



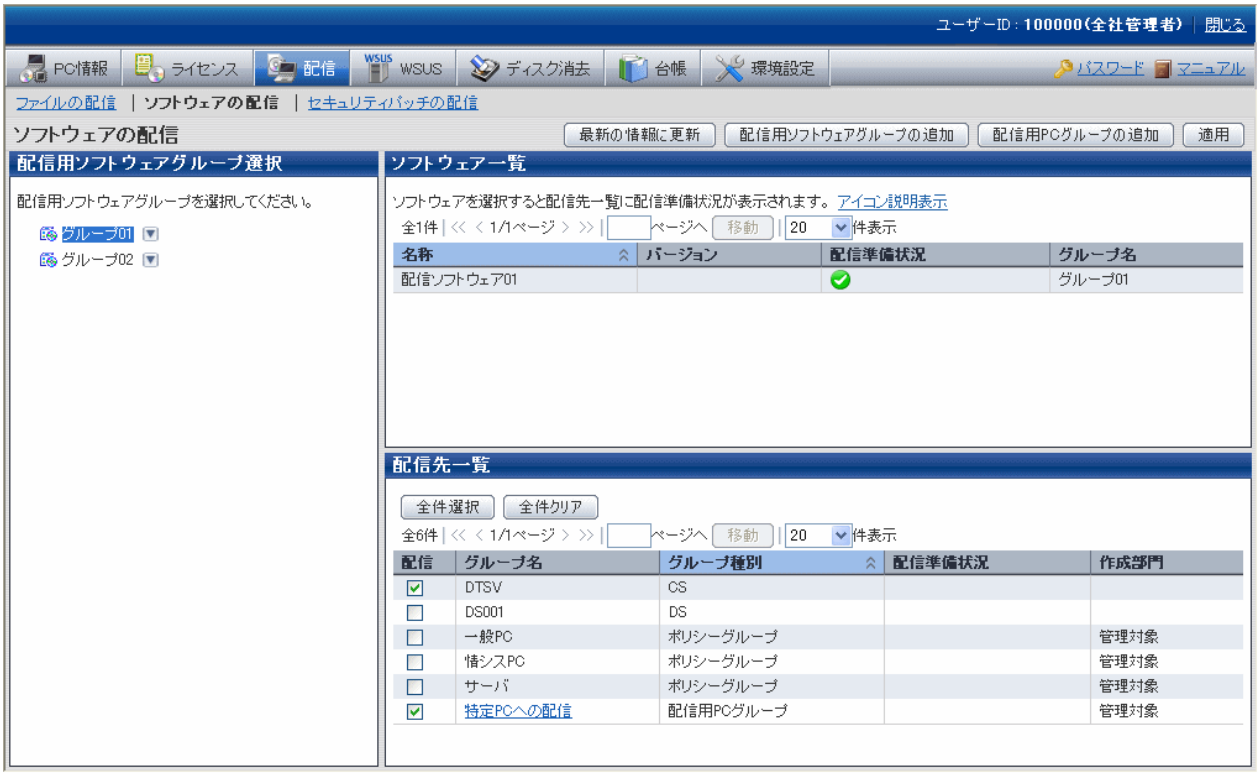
CTでの配信ソフトウェアダウンロード方法については、“運用ガイド クライアント編”を参照してください。

DSでの配信ソフトウェアダウンロード

DSのポリシーにダウンロードスケジュールを設定しておくことにより、上位サーバから定期的に配信ソフトウェアをダウンロードできます。ポリシーは、メインメニューで設定できます。

ダウンロード状況確認機能

メインメニューで、配信ソフトウェアごとに配信状況を確認できます。配信ソフトウェア登録時に指定した配信先サーバの状態と途中経過を確認できます。



2.6 セキュリティパッチの配信/適用機能

Systemwalker Desktop Patrolが提供する“ソフトウェア辞書”を使用した、セキュリティパッチの配信/適用機能について説明します。

インストール形式がクイック実行形式のセキュリティパッチの配信/適用機能については、“2.8 クイック実行形式のセキュリティパッチの配信/適用機能”を参照してください。

注意

Windows 10、Windows 11のセキュリティパッチおよび2016年10月以降にMicrosoft社から公開されるセキュリティパッチについて

- Windows 10、Windows 11のセキュリティパッチおよび2016年10月以降にMicrosoft社から公開されるWindows 8.1、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019のセキュリティパッチは、複数の脆弱性に対する修正が1つのセキュリティパッチにまとめられたロールアップで提供されます。個々のセキュリティパッチが対応している脆弱性の詳細については、[ソフトウェア一覧]の[名称]のリンクをクリックして表示されるMicrosoft社の情報(「ソフトウェアの情報」の中の「詳細情報」)を参照してください。
- 上記の1つにまとめられたセキュリティパッチはサイズが増加していますので、ネットワーク負荷分散のために、セキュリティパッチの配信時間をグループ単位に分散することを推奨します。配信時間の設定方法は、“運用ガイド 管理者編”の“セキュリティパッチ適用間隔と配信間隔を設定する”を参照してください。

注意

2018年4月2日より公開のソフトウェア辞書(V15.1.0以降用)において、以下の製品のセキュリティパッチの監査および配信に対応しています。

- Adobe Reader
- Adobe Flash Player
- Oracle Java Runtime Environment (JRE)

本機能が利用可能なCTのバージョンは以下の通りです。

- 監査

  V15.1.0以降

- パッチ適用

  V15.2.0以降(※)
  ※古いCTの場合、適用対象にならない、自動適用が行えないなど、適用が正しく行えません。

パッチ適用においては、Adobe社/Oracle社のライセンス条項を遵守し、再配布契約等の手続を行う必要があります。また、パッチは事前にダウンロードし手動でCSに登録する必要があります。

対応する製品バージョン、パッチの内容や入手方法、運用方法など詳細については“Systemwalker サポートセンターからのお知らせ”をご確認ください。また対応内容や方針は予告なく変更となる場合がありますので、定期的に“Systemwalker サポートセンターからのお知らせ”を確認してください。

注意

CTでのセキュリティパッチ適用は、ソフトウェア辞書によるセキュリティパッチ、WSUSによるセキュリティパッチの順で動作します。

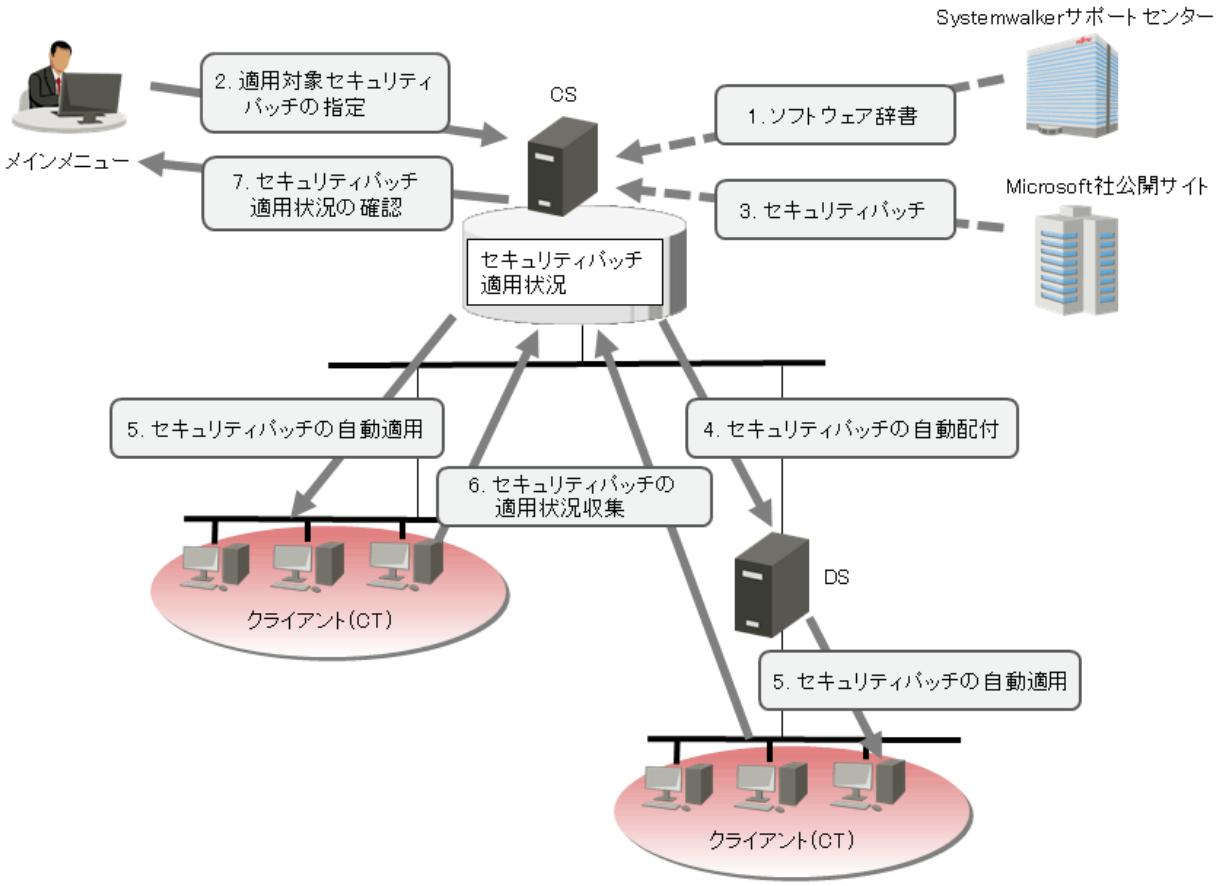
併用運用した場合、ソフトウェア辞書による配信でWindowsの再起動が必要なセキュリティパッチを配信すると、パッチ適用完了後にWindowsの再起動が必要とのパッチ適用後メッセージを表示する場合があります。Windows再起動後、次回のパッチ適用のタイミングでWSUSによる配信が動作します。

2.6.1 セキュリティパッチの自動適用

Microsoft社から提供されるセキュリティパッチを上位サーバから、CTに自動で配信、適用できます。

Systemwalker Desktop Patrolでは、Microsoft社から提供されるセキュリティパッチを「Microsoft社の公開サーバ」からダウンロードし、CSに自動的に登録できます。これにより、セキュリティパッチの取得から、クライアントへの適用まで、すべての作業が自動で行えるようになります。

セキュリティパッチを自動適用することにより、CTを使用するユーザーは、面倒なアップデート作業を行うことなく、セキュリティの確保が可能です。また、セキュリティパッチ適用漏れを防止できます。



1. 収集するインベントリ情報が定義された「ソフトウェア辞書」が、Systemwalkerサポートセンターから随時配信されます。
2. CSの管理者は、適用対象とするセキュリティパッチを指定します。
3. Microsoft社から提供されるセキュリティパッチを「Microsoft社の公開サーバ」からダウンロードし、CSに自動的に登録します。
4. DSを使用している場合は、CSからDSへ、セキュリティパッチが自動配信されます。
5. 上位サーバであるCSまたはDSから、CTへ、セキュリティパッチが自動適用されます。
6. CTから、CSまたはDSへ、セキュリティパッチの適用状況が収集されます。
7. CSの管理者は、セキュリティパッチの適用状況を確認します。

2.から6.までが、Systemwalker Desktop Patrolによるセキュリティパッチの自動適用です。

2.6.2 セキュリティパッチの手動適用

緊急性の高いセキュリティパッチが公開された場合や、モバイル環境等で利用者の任意のタイミングで適用したい場合には、即座にセキュリティパッチの適用を行うことができます。

上位サーバにセキュリティパッチが登録されている環境で、[スタート]-[プログラム]-[Systemwalker Desktop Patrol CT]-[パッチ適用]、または[アプリ]-[Systemwalker Desktop Patrol CT]-[パッチ適用]を選択すると、PCに適用すべきセキュリティパッチの検出および適用を行うことができます。

2.6.3 特定のPCに適用するセキュリティパッチの選択

特定のPCに対してセキュリティパッチを選択して適用したい場合に、ポリシーグループごとに適用するセキュリティパッチを設定できます。

これにより、特定のセキュリティパッチを適用すると運用上問題のあるPCに対して、例外的なパッチ適用の運用が行えます。

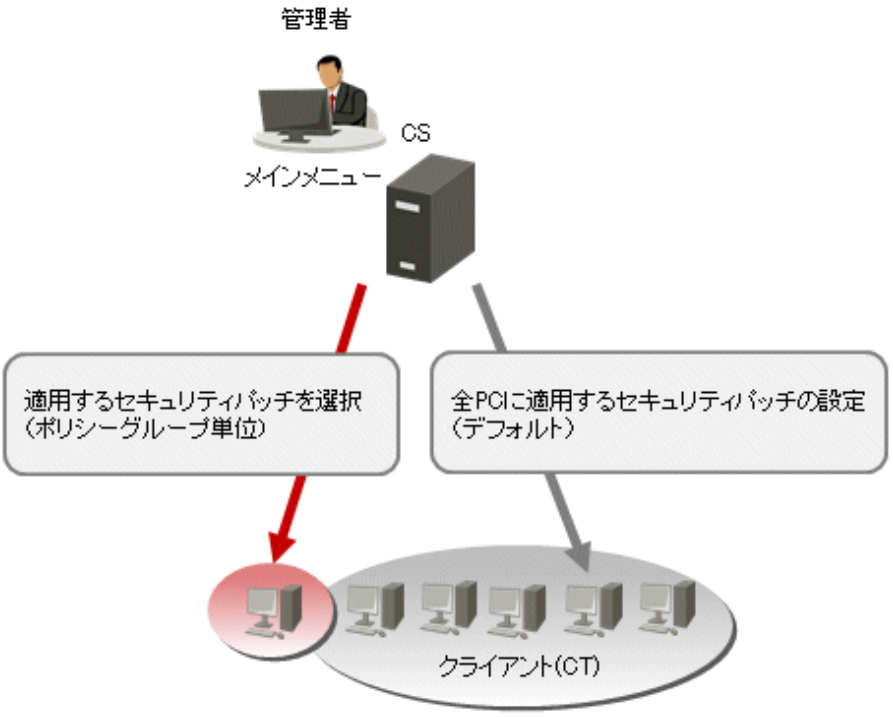
適用するセキュリティパッチの選択時には、以下の設定を行うことができます。

- 特定のPCに対して、セキュリティパッチを選択する設定
- 特定のPCに対して、現状以降に提供されるセキュリティパッチを適用しない設定

上記の設定を組み合わせて運用することもできます。

運用のイメージ

特定のPCに対し、セキュリティパッチを選択して適用する運用のイメージ図を以下に示します。



ポリシーグループに所属しないCTについては、メインメニューの[配信]-[セキュリティパッチの配信]画面で選択したセキュリティパッチの設定に従ってパッチの適用が行われます。

特定のPCに対して適用するセキュリティパッチを選択する場合は、メインメニューの[環境設定]-[ポリシーグループ管理]-[各種ポリシーのカスタマイズ]タブ-[パッチ設定ポリシー]タブで、適用しないセキュリティパッチのチェックを外します。

これにより、ポリシーグループに所属するPCに対して、セキュリティパッチ選択して適用する運用を行えます。

2.7 WSUS連携機能

WSUS連携機能とは、Systemwalker Desktop PatrolのCS/DSがWSUSと連携を行い、WSUSを利用した更新プログラムの適用や監査を行う機能です。

WSUS連携機能は、WSUS未導入/導入済どちらの環境においても、Systemwalker Desktop Patrolを導入することで、WSUSを利用した運用を行えます。

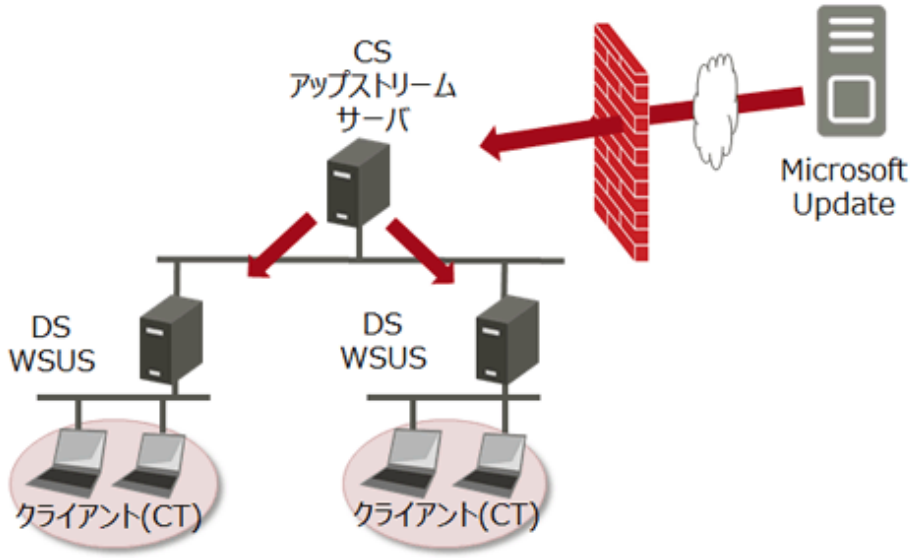
- WSUS未導入の環境：Systemwalker Desktop PatrolがWSUS構築/設定を実施して連携します。
- WSUS導入済の環境：WSUSの既存設定を利用してSystemwalker Desktop Patrolと連携します。

WSUS連携機能の概要・システム構成を以下に示します。

WSUSとSystemwalker Desktop PatrolのCS/DSが連携し、配下のクライアントに更新プログラムを適用・監査を行います。

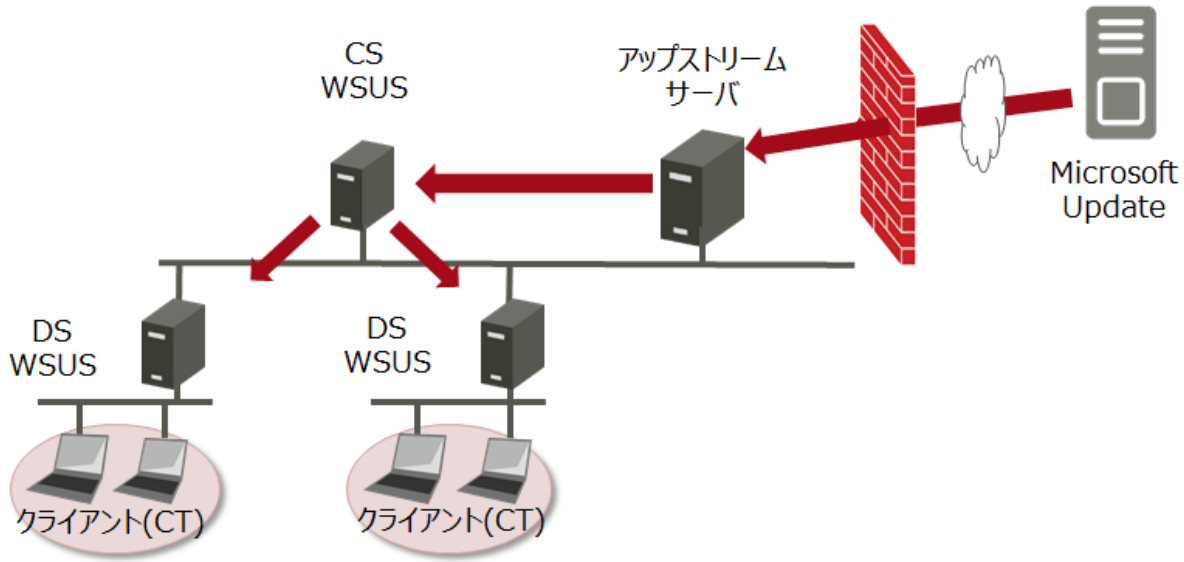
- Microsoft Updateと接続するアップストリームサーバがCSと同居できる場合

  CSがインターネット接続できる環境の場合に、本構成となります。



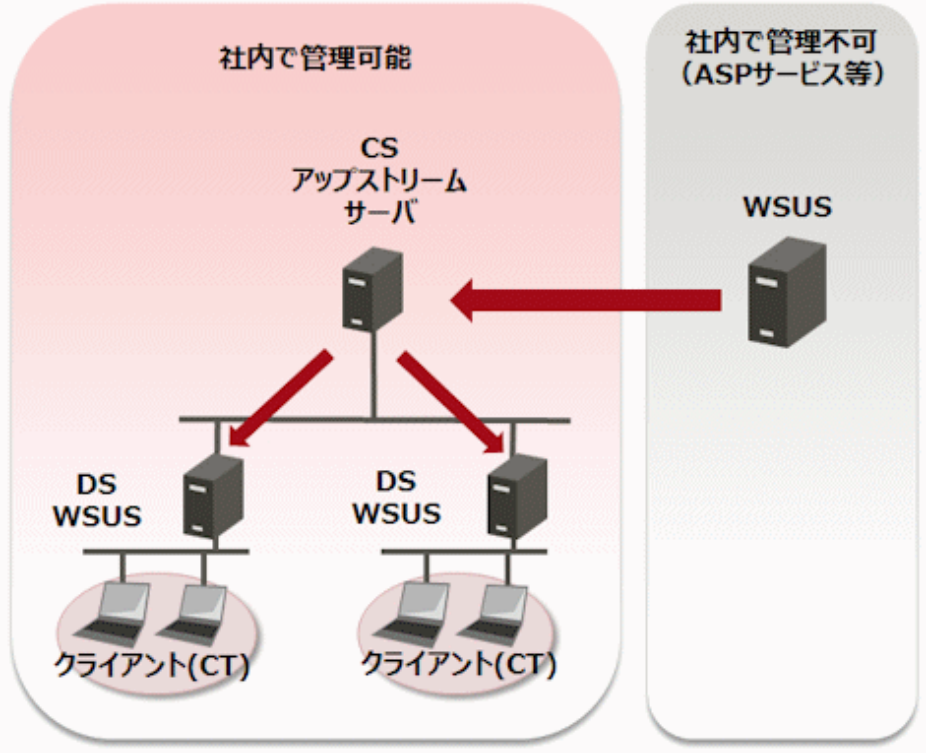
- Microsoft Updateと接続するアップストリームサーバがCSと同居できない場合

  CSがインターネット接続できない場合、または、CSとアップストリームサーバを非同居にする場合に本構成となります。



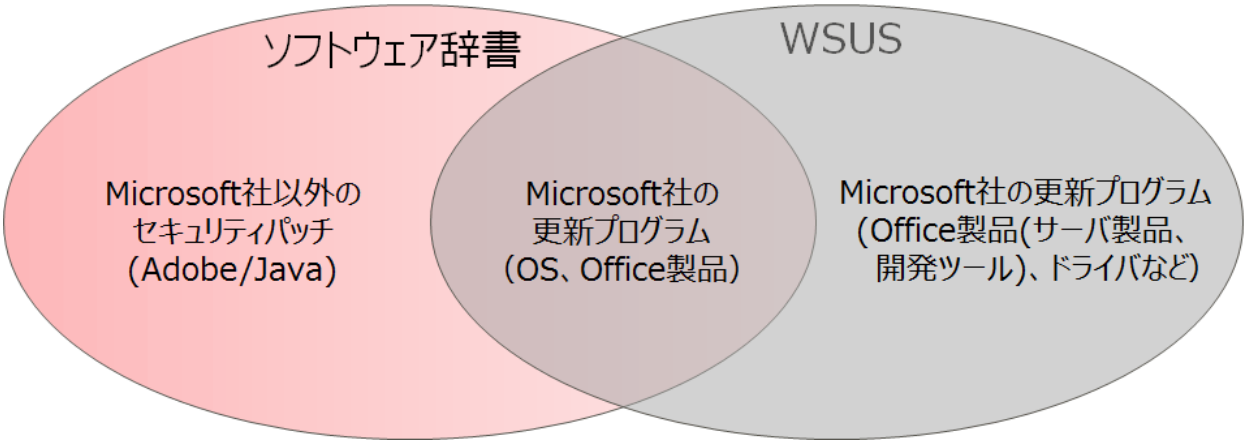
・ ASPサービスで外部から提供を受けているなど、社内では管理できないWSUSを介して更新プログラムが提供される場合

社内のアップストリームサーバが外部のWSUSから更新プログラムを取得の上、更新プログラムの管理が可能となります。



設定方法の詳細については、“運用ガイド 管理者編”の“管理外のアップストリームサーバと接続する”を参照してください。

WSUS連携機能と従来のソフトウェア辞書によるセキュリティパッチの配信との関係は下図のようになり、ソフトウェア辞書とWSUS連携両方の活用によって、利用者に必要な更新プログラムの適用と監査を進められます。



以下の運用を推奨します。

・ Windows 10およびWindows 11への移行でネットワーク負荷軽減を検討されている、または、これからSystemwalker Desktop Patrolを導入されるお客様

　― Microsoft社の更新プログラムの配信/監査は、WSUSを使用

　― Microsoft社以外（Adobe/Java）のセキュリティパッチについては、ソフトウェア辞書によるセキュリティパッチの配信/監査を使用

- 既にソフトウェア辞書によるセキュリティパッチの配信/監査を実施しているお客様
  - 配信をWSUS連携に切り替えることで、WSUS独自のネットワーク負荷対策（高速インストール、独自の圧縮技術など）の利用が可能
  - ソフトウェア辞書には提供されていないMicrosoft社の更新プログラムを配信/監査する場合はWSUSを使用

注意

WSUS連携機能を利用する場合の前提条件

WSUS連携機能には、利用時に以下の前提条件があります。

- WSUSサーバが動作するOS
  - Windows Server 2012

    KB3095113が適用済みであること
  - Windows Server 2012 R2

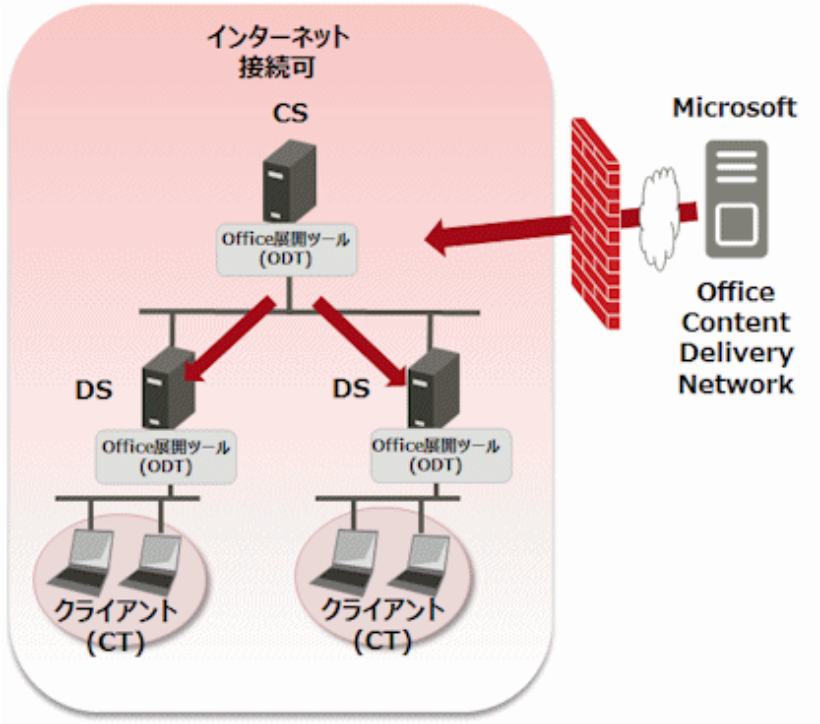
    KB3095113が適用済みであること
  - Windows Server 2016
  - Windows Server 2019
- 利用可能なCS
  - Systemwalker Desktop Patrol 64ビット版のCSのみ
- 適用不可のCT
  - CTがWindows 10 HomeおよびWindows 11 Homeの場合は、WSUS連携のパッチ適用はできません。

2.8 クイック実行形式のセキュリティパッチの配信/適用機能

クイック実行形式のセキュリティパッチの配信/適用機能とは、インストール形式がクイック実行形式のOffice(Microsoft 365(旧Office 365)、Office2019)に対して、Microsoft社から提供されているOffice展開ツール(ODT)を利用し、Officeのセキュリティパッチを配信/適用する機能です。

Microsoft 365(旧Office 365)やOffice2019といったクイック実行形式のOfficeに対して、セキュリティ強化や社内統制を行いたい情報システム部門のお客様が本機能を利用することにより、Officeを展開するためのWebサーバ構築工数の削減やネットワーク負荷軽減に向け柔軟な設計が可能となります。

クイック実行形式のセキュリティパッチの配信/適用機能のシステム構成例を以下に示します。



注意

クイック実行形式のセキュリティパッチの配信/適用機能を利用する場合の前提条件

クイック実行形式のセキュリティパッチの配信/適用機能には、利用時に以下の前提条件があります。

- 利用可能なCS
  - Systemwalker Desktop Patrol 64ビット版のCSのみ
- WindowsストアアプリのOfficeは、未サポートとなります。

2.9 ディスク消去機能

ディスク消去機能とは、ディスク消去時期が近づいているPCを計画的に管理し、確実なディスク消去処理を実施できる機能です。

ディスク消去機能は、「ディスク消去計画」、「ディスク消去実行」、「ディスク消去情報管理」の3つを柱としています。

ディスク消去計画

管理者は、ディスク消去時期が近づいているPCをグループに分け、グループごとにディスクの消去方法を指定します。操作は、「Desktop Patrol メインメニュー」で行います。

ディスク消去実行

管理者からディスク消去指示された、ディスク消去対象PCのユーザーは、ディスク消去処理用のフロッピィディスク、USBメモリ、またはCDを使用して、PCのハードディスクを消去します。消去した結果は、「ディスク消去レポート」として管理者にアップロードします。

ディスク消去情報管理

ディスク消去情報は、CSで一元管理します。

管理者は、以下のことができます。

- 情報の一覧をCSVファイルにダウンロードする

- ディスク消去状況を確認する
- ディスク消去PCのインベントリ情報（ハードウェア情報およびリース情報）を参照する

  ユーザーから、ディスク消去レポートがアップロードされると、該当PCのライセンス情報とインベントリ情報は自動的に消滅します。

注意

ディスク消去用の媒体にUSBメモリを使用する場合

- Windows10およびWindows 11では、フロッピィディスクかCDを使用してください。（USBメモリは使用できません）
- USBメモリを使用する場合は、Windows8.1のみで、2GBより大きい容量のUSBメモリを使用してください。

2.10 管理台帳機能

Systemwalker Desktop Patrolの管理台帳機能について説明します。

2.10.1 機器の管理

管理対象機器について、機器（PCおよび什器）の資産状況の確認や操作をする機能で、操作として以下があります。

- 部門別/分類別/場所別による機器情報の確認
- 機器情報の登録/変更/削除
- 機器情報の台帳保存

さらに、ATと連携する場合には、以下の操作ができます。

- ATによる資産情報の確認

これらの情報は、「Desktop Patrol メインメニュー」の[台帳]-[機器管理]画面で表示されます。

各情報の表示内容、および表示イメージは以下のとおりです。

部門別/分類別/場所別による機器情報の確認

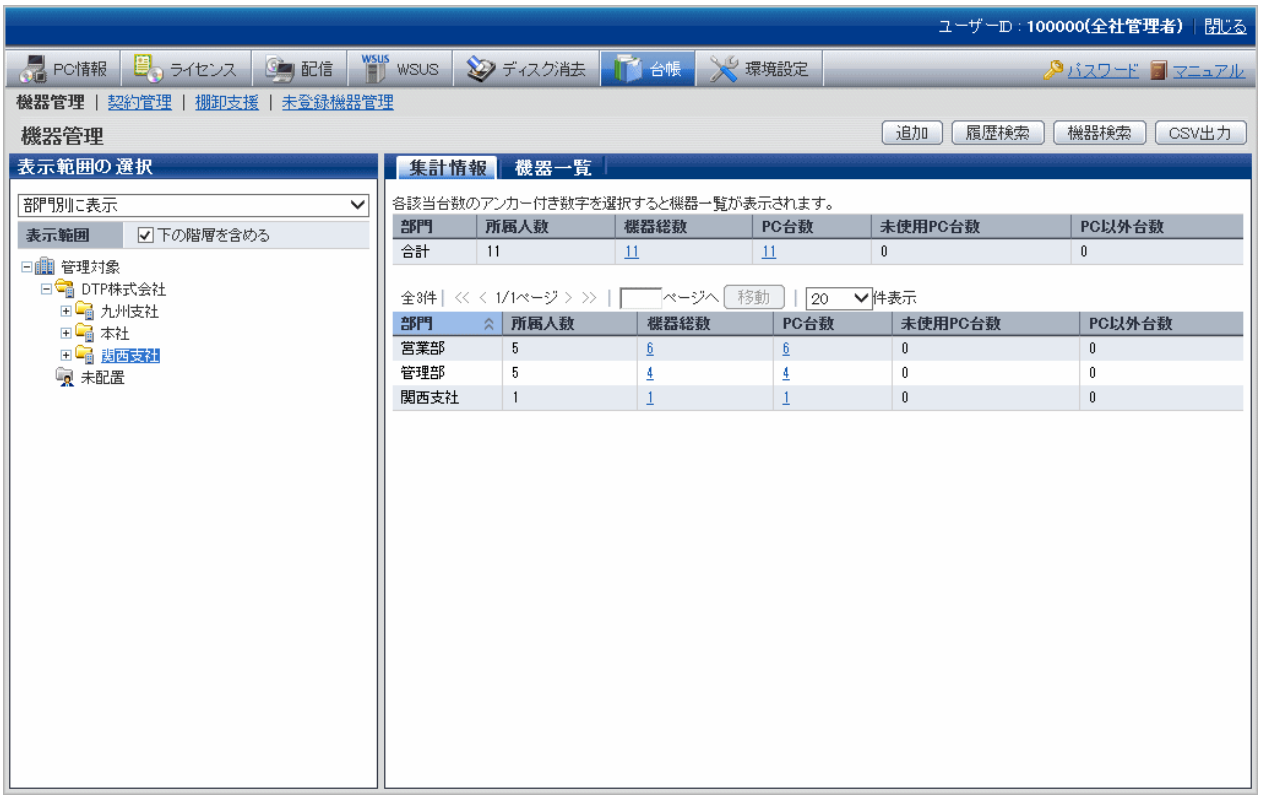
ユーザーの操作要件にあった機器情報を表示します。

機器情報の検索が簡単にでき、用途にあった検索結果を表示できます。

集計情報

管理対象機器の全体数やPC台数などを、部門別/分類別/場所別に表示します。

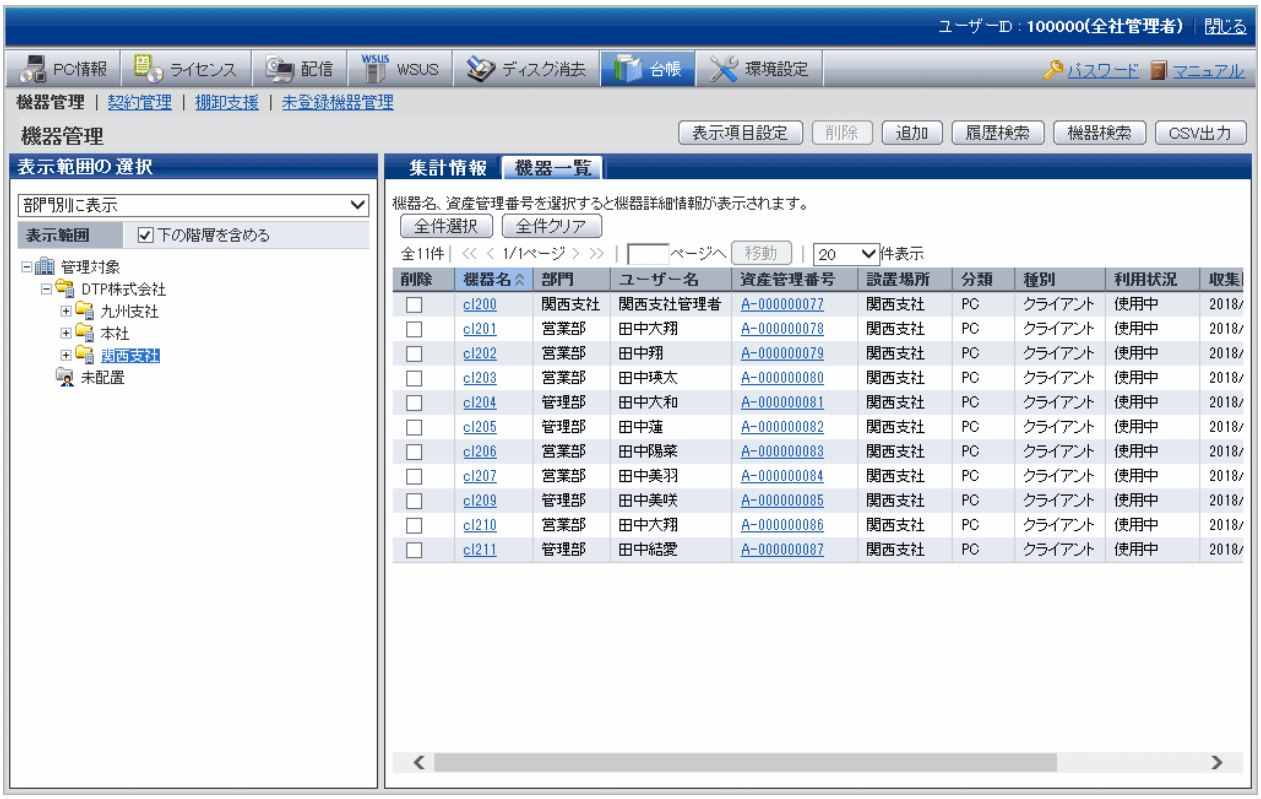
例えば、部門別に集計情報を表示した場合、以下のように表示されます。



機器一覧

管理対象機器の一覧を部門別/分類別/場所別に表示します。

例えば、部門別に一覧表示した場合、以下のように表示されます。



機器詳細

選択した管理対象機器の詳細情報を表示します。詳細情報とは、設置場所/メーカ名などの本体情報、利用者情報、契約情報、ハードウェア情報などです。

詳細情報は以下のように表示されます。

機器情報の登録/変更/削除

機器単位で機器情報を登録/変更/削除します。

現在の機器情報の内容を確認しながら、機器のデータを変更できます。

なお、機器情報を登録/変更/削除した結果は、履歴情報として保存されます。

注意

部門管理者は他部門の関連機器は削除できません

部門管理者の場合、機器情報を削除できるのは、自部門およびその配下の機器だけです。

自身が管理する機器の関連機器であっても、関連機器が他部門の管理機器である場合には、その関連機器は削除できません。
その場合、上記画面内の備考に、「他部門の機器のため、削除できません。」と表示されます。

機器情報の台帳保存

機器情報（集計情報、機器一覧、機器詳細）をそれぞれCSVファイルに保存します。

保存したデータは、ほかのドキュメントへの活用や、ほかのシステムとの情報連携やデータ比較などに利用できます。

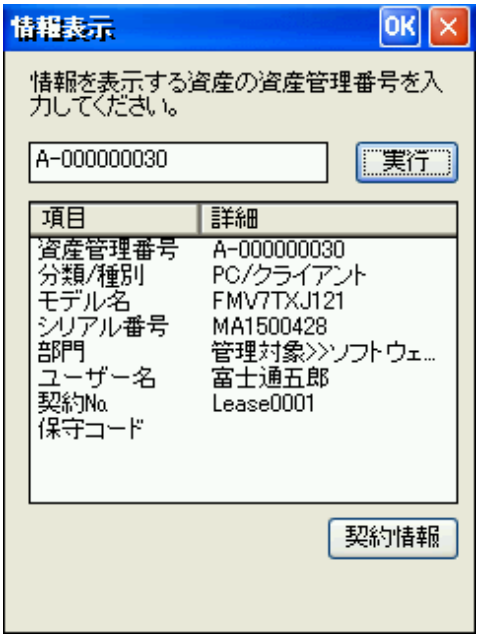
なお、機器情報の一覧表示の画面では、機器情報を資産情報の登録/変更ファイルとして使用できるCSVファイルに出力できます。この出力ファイルを編集し、資産情報の登録/変更機能で一括登録することにより、機器情報の一括変更ができます。

ATによる資産情報の確認

機器に貼ったバーコードラベルをATで読み込み、機器情報と契約情報を確認します。

ATで棚卸を行うときに、その場で機器情報と契約情報を参照できます。

機器情報は以下のように表示されます。



機器情報の変更履歴

機器の設置、移設/譲渡、棚卸、返却/廃棄までの状態変更を履歴情報として管理することで、過去に遡って機器の利用状況を確認できます。

運用方法

機器情報の変更履歴機能を利用する場合の運用方法を以下に示します。

- 大規模な組織変更/人事異動を実施した場合、システム管理者が機器の移設が漏れ/誤りなく行われているか確認したい。

  特定期間内に移動のあった機器一覧を表示し、移動前の設置場所から正しく移動できたか確認します。

- 新規追加したPCが、何台/どの部門に設置されたのか確認したい。

  特定期間内に新規追加された機器一覧を表示し、追加されたPCがどの部門に設置されたかを一覧から確認します。

- 部門管理者による棚卸時に、自部門内に知らない機器が追加されているが、どこからきたのか確認したい。

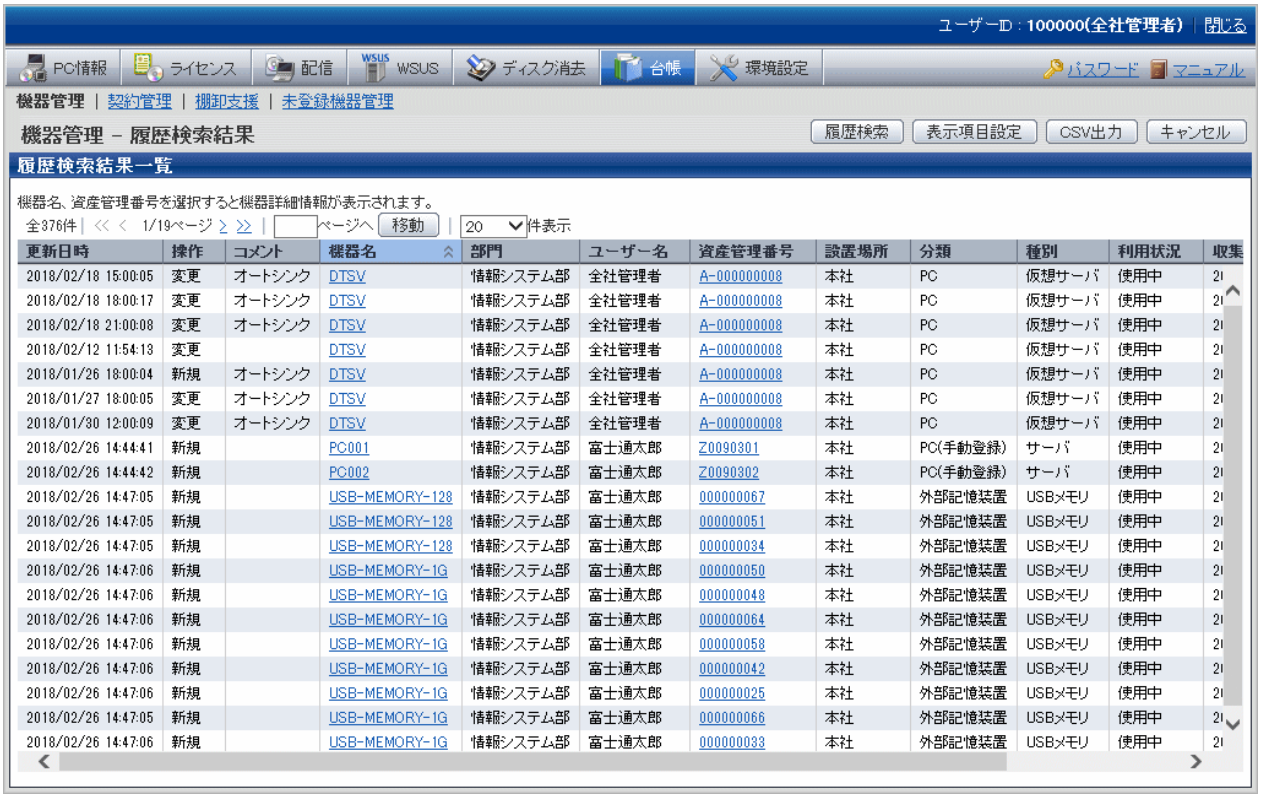
  追加機器のバーコードラベルに記されている機器の資産管理番号を元に、機器の履歴情報から前回の機器の利用者/設置場所を過去に遡って確認します。

- 機器の情報変更時に、誤って不必要な機器情報を変更してしまった場合、元の状態に戻したい。

  対象機器の変更履歴から変更前の情報を確認し、元の状態に戻します。

[更新履歴]画面

更新履歴は、[更新履歴]画面で確認します。



2.10.2 契約の管理

管理対象機器の契約情報を管理する機能で、操作として以下があります。

- 部門別/分類別による契約情報の確認
- 契約情報の登録/変更/削除
- 契約情報の割り当て
- 契約情報の台帳保存
- 契約期限のアラーム通知
- 契約の延長

さらに、ATと連携する場合には、以下の操作ができます。

- ATによる資産情報の確認

部門別/分類別による契約情報の確認

ユーザーの操作要件にあった契約情報を表示します。

契約情報の検索が簡単にでき、用途にあった検索結果を表示できます。

集計情報

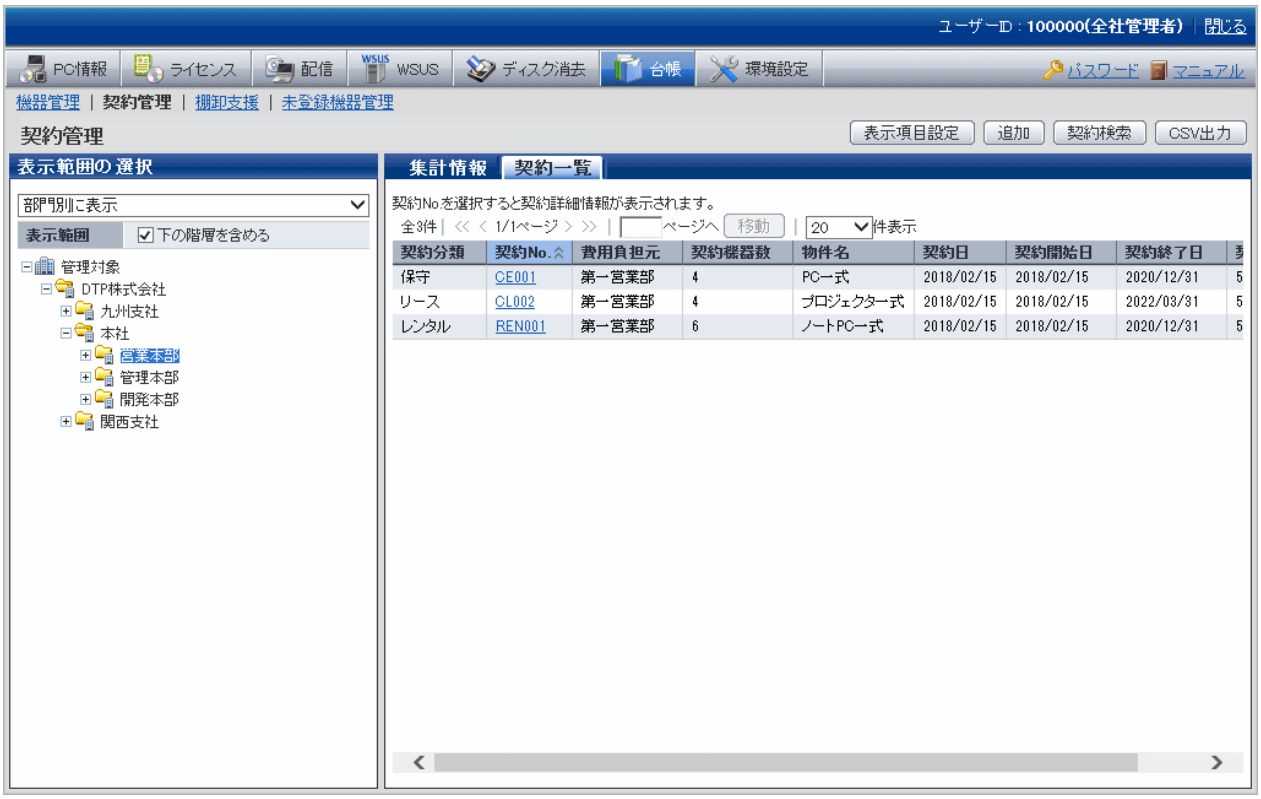
管理対象機器の契約数と契約機器数を、部門別/分類別に表示します。

例えば、部門別に集計表示した場合、以下のようになります。

契約一覧

管理対象機器の契約情報と契約機器数の一覧を、部門別/分類別に表示します。

例えば、部門別に一覧表示した場合、以下のようになります。



契約詳細

選択した管理対象機器の契約情報について、契約会社、契約期間、金額などの詳細情報や契約機器の一覧を表示します。

詳細情報は以下のように表示されます。

契約情報の登録/変更/削除

1契約単位で契約情報を登録/変更/削除します。

現在の契約情報の内容を確認しながら、契約のデータを変更できます。

- 契約情報の登録/変更
- 契約情報の削除

契約情報の割り当て

1契約単位に機器情報を割り当てます。

契約情報の管理をするためには、契約情報と機器情報を結びつける必要があります。契約情報に割り当てる機器を絞込検索することで、円滑かつ確実に機器情報の割り当てができます。

「割当機器の絞込」画面で絞り込む機器の条件を入力して検索します。検索結果の機器一覧から割り当てる機器を選択し、機器情報を割り当てます。

契約情報の台帳保存

契約情報（集計情報、契約一覧、契約詳細）をそれぞれCSVファイルに保存します。

保存したデータは、ほかのドキュメントへの活用や、ほかのシステムとの情報連携やデータ比較などに利用できます。

なお、契約情報の一覧表示の画面では、契約情報を資産情報の登録/変更ファイルとして使用できるCSVファイルに出力できます。この出力ファイルを編集し、資産情報の登録/変更機能で一括登録することにより、契約情報の一括変更ができます。

契約期限のアラーム通知

システム管理者に対し、リース/レンタル/保守の契約期限が近づいた場合と契約終了日になった場合に、契約情報をメールで通知します。

リース/レンタル/保守契約を結んでいる機器に対して契約を延長する場合、契約が切れる前に、契約を延長するか/新規契約とするかを機器の使用部署と調整し、契約会社と延長手続きを行う必要があります。しかし、契約期間は、例えばリース契約の場合では4年間と長いこともあり、システム管理者が各契約の契約期限切れを常時監視するのは、非常に手間がかかります。

そのため、契約切れとなる前と契約終了日にシステム管理者へ自動的にメールで通知することで、システム管理者の契約管理業務の負担を軽くできます。

アラーム通知の設定では、システム管理者に送付するメールのテンプレートを編集できます。

契約の延長

Systemwalker Desktop Patrolが管理する契約情報(リース／レンタル／保守)に対して、契約の延長を行います。

契約の延長を行うと、延長後の契約情報が作成され、元契約に割り当てられている機器情報も、延長後の契約情報に移行されます。

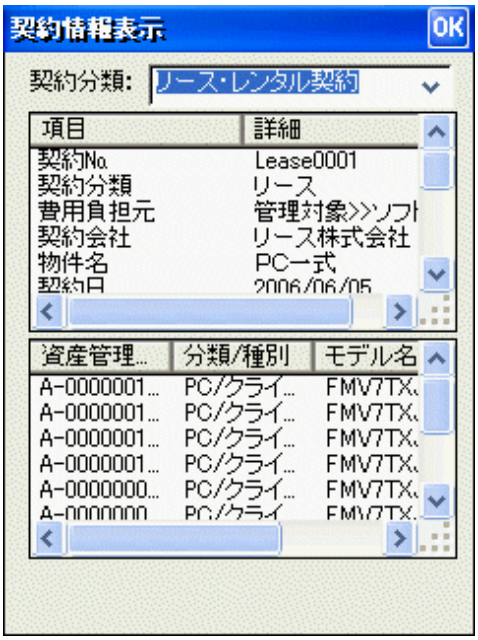
また、延長後の契約情報には、[元契約No.]も合わせて管理されます。この[元契約No.]は契約一覧画面でも確認することができるため、どの契約情報が再契約されたものか判別できます。

ATによる資産情報の確認

機器に貼ったバーコードラベルをATで読み込み、機器情報と契約情報を確認します。

ATで棚卸を行うときに、その場で機器情報と契約情報を参照できます。

契約情報は以下のように表示されます。



2.10.3 棚卸支援

管理対象機器の棚卸を支援するための機能で、操作として以下があります。

- 部門別/分類別/場所別による棚卸状況の確認
- 棚卸の状態変更
- 棚卸の運用設定
- 棚卸状況の台帳保存

・ 設置場所の補正

さらに、ATと連携する場合には、以下の操作ができます。

・ ATと連携した棚卸

部門別/分類別/場所別による棚卸状況の確認

ユーザーの操作要件にあった棚卸状況を表示します。

棚卸状況の検索が簡単にでき、用途にあった検索結果を表示できます。

集計情報

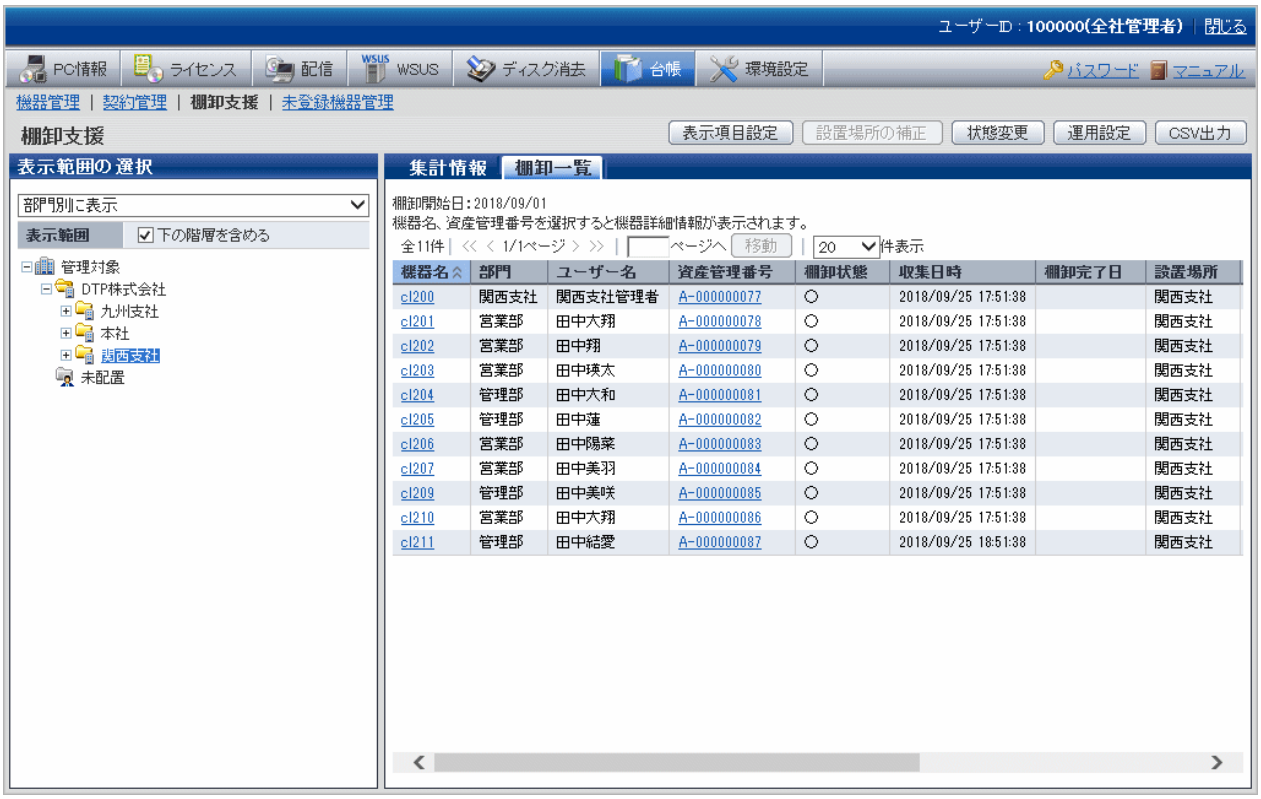
管理対象機器の棚卸対象台数や棚卸状況などを、部門別/分類別/場所別に表示します。

例えば、部門別に集計情報を表示した場合、以下のように表示されます。

棚卸一覧

管理対象機器の棚卸対象機器の一覧を、部門別/分類別/場所別に表示します。

例えば、部門別に一覧表示した場合、以下のように表示されます。



棚卸の状態変更

棚卸対象の機器に対して、管理者が手動により棚卸の状態を変更することができます。設定できる内容は以下のとおりです。

- 棚卸済みに設定
- 棚卸未完に設定
- 棚卸対象外に設定

棚卸実施済みかどうかの設定のほか、棚卸対象としない機器については、棚卸対象外に設定することができます。

棚卸の運用設定

棚卸対象の機器に対して、以下の運用設定を行います。

- 棚卸開始日の設定
- 棚卸状態の判定方法
- 設置場所の補正結果

棚卸対象の機器に棚卸開始日を設定すると、この設定日から現在日時の間に機器の存在を確認できた場合に、自動的に棚卸済みとなります。例えば、Systemwalker Desktop Patrolでインベントリ情報が収集された場合や、ATと連携した棚卸が行われた場合は、棚卸済みとなります。

棚卸開始日を設定することで、Systemwalker Desktop Patrolで収集されたインベントリ情報でPCの棚卸確認、また機器情報の自動検知による棚卸確認ができます。この結果、棚卸の確認作業を削減することができ、確実に管理を実施できます。

なお、Systemwalker Desktop Patrolでインベントリ情報が収集されたことを契機に棚卸済みとするには、棚卸状態の判定方法を設定する必要があります。

棚卸対象の機器が遠隔地にあるなどの理由で、Systemwalker Desktop Patrolによるインベントリ収集やATと連携した棚卸ができない場合には、棚卸状況の一覧表示の画面でシステム管理者が対象機器を棚卸済みと設定できます。逆に、棚卸済みとなった機器を棚卸未完に戻すことも可能です。

このように、棚卸済み/棚卸未完の設定をシステム管理者が変更でき、様々な運用要件に対応できます。

棚卸状況の台帳保存

棚卸状況（集計情報、棚卸一覧）をそれぞれCSVファイルに保存します。

保存したデータは、ほかのドキュメントへの活用や、ほかのシステムとの情報連携やデータ比較などに利用できます。

設置場所の補正

インベントリ収集や、ユーザー手動入力によって、資産台帳に登録された機器のIPアドレスと、管理者があらかじめ登録したセグメント管理情報を用いて、設置場所の補正を行います。機器の移設などにより、機器のIPアドレスが変更された場合は、棚卸時に設置場所の補正を行うことで、容易にかつ正確に設置場所を資産台帳に反映することができます。

ATと連携した棚卸

棚卸対象の機器に対してバーコードラベルを作成し、ATと連携して棚卸を行います。

Systemwalker Desktop Patrolで管理している資産情報からバーコードラベルを作成し、現地でATを使用してバーコードを読み込み、その結果を資産情報に反映する作業を体系化することで、棚卸業務を確実に行うことができ、管理作業を軽減できます。

棚卸用のバーコードラベルの作成

棚卸対象の機器に対して以下のようなバーコードラベルを作成します。対応するバーコードの規格は「Code-39」です。

バーコードラベルは棚卸対象の機器に貼り、ATで棚卸を行うときに使用します。

棚卸の対象機器情報のAT連携

棚卸対象の機器に貼ったバーコードラベルをATで読み込み、棚卸結果をSystemwalker Desktop Patrolで管理する資産情報へ反映します。この作業を行うために、棚卸を行う機器情報のATへの抽出と、ATで棚卸を実施した結果の取り込みを行います。

2.10.4 未登録機器管理

ネットワーク上に接続された機器を自動検知し、管理台帳に登録されていない機器を確認する機能です。機器情報を自動検知する方法として、以下の2つの検知方法があります。

- セグメント別検知

  セグメント単位にADTを導入し、機器情報を検知する方法

- ネットワーク一括検知

  CSサーバからICMP、SNMPに対応した機器の情報を検知する方法

注意

本機能は、IPv4のアドレスを持つ機器のみを自動検知し、IPv6の機器は検知の対象外となります。

未登録の機器については未登録機器管理の画面から機器情報を個々に登録します。または未登録機器一覧をファイルに出力して一括で登録することも可能です。

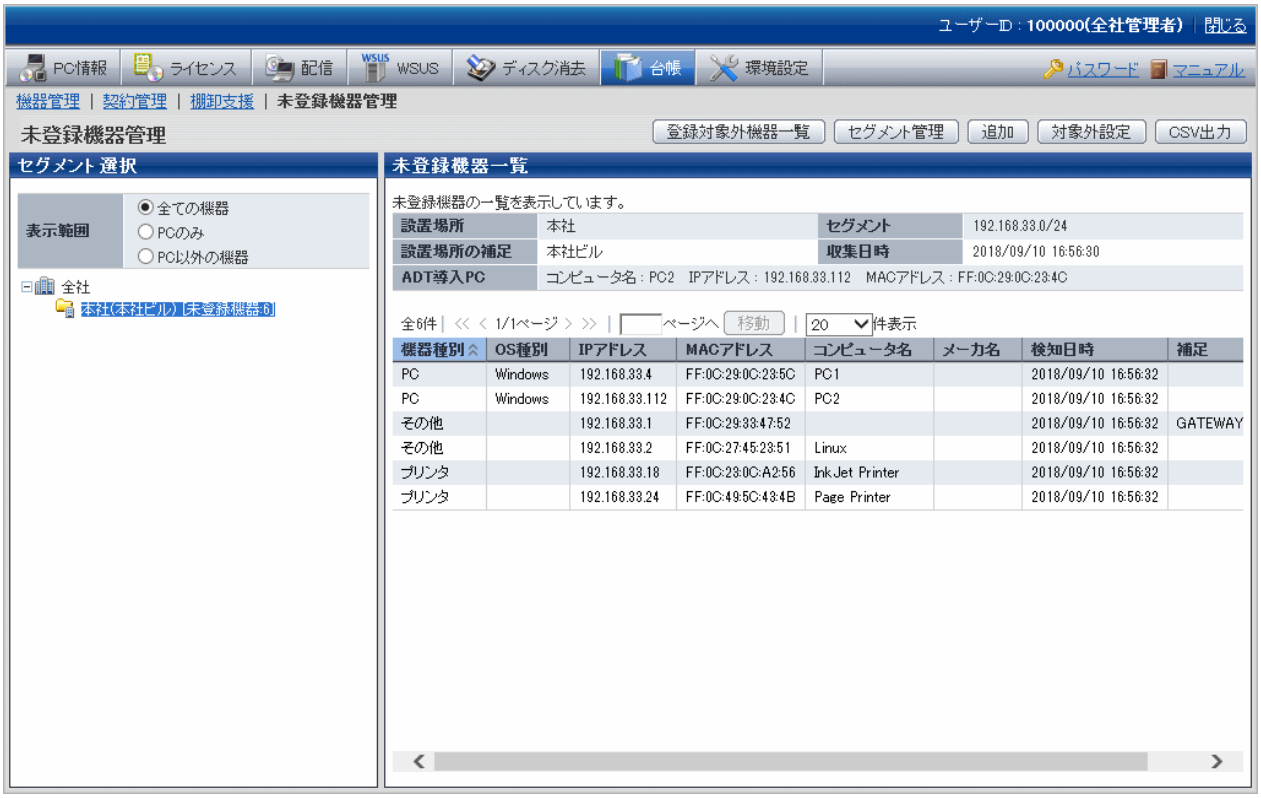
未登録機器管理の操作として以下があります。

- 未登録機器情報の確認
- 未登録機器情報の登録
- 対象外設定および登録対象外機器の一覧表示

- セグメント管理
- 未登録機器情報の台帳保存

未登録機器情報の確認

未登録機器の一覧を表示します。一覧表示は、セグメント単位で表示することができます。



未登録機器情報の登録

未登録機器一覧から管理対象とする機器を資産台帳に登録します。

対象外設定および登録対象外機器の一覧表示

未登録として検知された機器を、資産台帳の管理対象として扱わないように設定できます。また、対象外とした機器の一覧を表示することができます。

セグメント管理

未登録機器の表示／登録機能を利用する前に、セグメントと設置場所名称を関連付けるセグメント管理設定が必要となります。

未登録機器情報の台帳保存

未登録機器情報をCSVファイルに保存します。

保存したデータは、ほかのドキュメントへの活用や、ほかのシステムとの情報連携やデータ比較などに利用できます。

2.11 レポート出力機能

Systemwalker Desktop Patrolで管理する資産情報や、セキュリティ情報をレポートとして出力する機能です。大きく、4つのレポートがあります。

- 資産情報のレポート
- セキュリティ対策の監査レポート

- 省電力対策の監査レポート
- 複合機/プリンタの稼働状況レポート

2.11.1 資産情報のレポート

Systemwalker Desktop Patrolで管理する資産情報をレポート形式（Microsoft Excel形式）でファイルに出力したり、印刷したりする機能です。レポートを出力するときにグラフや表などを出力して、視覚的に現在の状況や問題点を把握できます。

資産情報のレポート形式の出力では、以下の操作ができます。

- レポート形式ファイルの出力
- レポートレイアウトの編集

レポート形式ファイルの出力

Systemwalker Desktop Patrolで管理する資産情報をレポート形式(Microsoft Excel形式)に変換し、印刷やファイル出力を行います。

資産情報をレポート形式で出力することで、以下の効果が期待できます。

- 資産情報の状況把握の効率化

  資産情報のサマリや一覧を出力することで、資産情報の状況を効率的に把握できます。

- 問題点の把握の効率化

  レポート内でグラフなどを使用することで、視覚的に問題点を把握できます。

- 資産管理実施内容の紙面化

  棚卸などの作業を行った結果を紙面として保管できます。

出力できるレポートは以下のとおりです。

- 資産稼働状況一覧

  資産の使用状況（使用/遊休）の一覧をレポート形式で出力します。

- 契約一覧

  資産の契約情報（リース/レンタル/保守）をレポート形式で出力します。

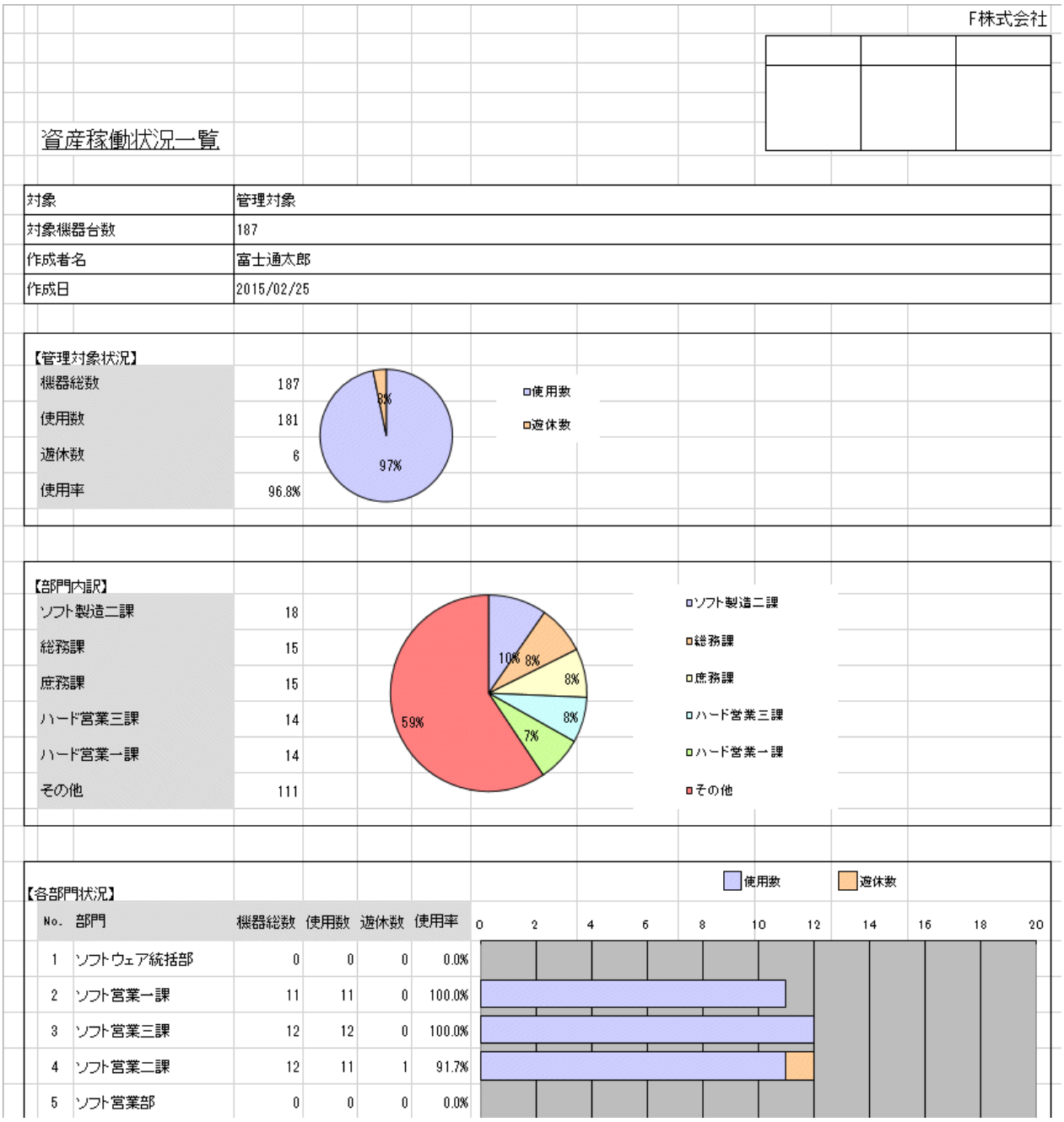
- 棚卸状況

  資産の棚卸の実施結果をレポート形式で出力します。

- ライセンス使用状況

  ソフトウェアのライセンス使用状況をレポート形式で出力します。

例えば、資産稼働状況一覧では以下のようなレポートを出力できます。



F株式会社

資産稼働状況一覧

対象	管理対象
対象機器台数	187
作成者名	富士通太郎
作成日	2015/02/25

【管理対象状況】

機器総数	187
使用数	181
遊休数	6
使用率	96.8%

【部門内訳】

ソフト製造二課	18
総務課	15
庶務課	15
ハード営業三課	14
ハード営業一課	14
その他	111

【各部門状況】

No.	部門	機器総数	使用数	遊休数	使用率
1	ソフトウェア統括部	0	0	0	0.0%
2	ソフト営業一課	11	11	0	100.0%
3	ソフト営業三課	12	12	0	100.0%
4	ソフト営業二課	12	11	1	91.7%
5	ソフト営業部	0	0	0	0.0%

レポートレイアウトの編集

Systemwalker Desktop Patrolで管理する資産情報のレポートのレイアウトを変更します。

レポート出力時にレポートタイトル、絞り込み条件、出力するレポートなどを変更します。

また、レポート形式(Microsoft Excel形式)で出力したデータを保存した後、Microsoft Excelの機能を使用してレイアウトを変更することもできます。

2.11.2 セキュリティ対策の監査レポート

ユーザーが決定した監査指針に基づきセキュリティ対策の運用状況を監査します。セキュリティ監査の結果は、セキュリティ対策の見直しに利用できます。

また、セキュリティ監査の結果は、レポートとして出力し、正しくセキュリティ対策が行われていることの証明書としても利用できます。

監査指針の設定

監査指針とは、セキュリティの監査を行う上で“何がセキュリティ対策として設定されていれば問題なしとするか”の評価基準です。セキュリティ監査は、監査指針に基づき実施されます。

監査指針では、以下の監査項目を組み合わせて、どの項目のチェックを行うかを設定します。

- ハードウェア
- OS(システム)
- OS(ユーザー)
- Internet Explorer
- セキュリティパッチ適用
- ウイルス対策ソフトウェア導入
- ウイルスパターン適用
- アクセス制御
- 暗号化状況
- 監査ソフト導入
- アプリケーション

Systemwalker Desktop Patrolでは推奨監査指針として、「情報漏洩対策」「脆弱性対策」の監査指針を提供しています。推奨監査指針は、ユーザーがカスタマイズできます。運用方法や環境に応じて、監査項目の設定を変更して使用します。

また、推奨監査指針以外にもユーザーが定義できる監査指針を利用し、セキュリティ監査を実施できます。

運用方法

Systemwalker Desktop Patrolでは、以下の2通りの運用があります。

- 是正期間を設ける運用

  PCの移動が多く、毎月確実なセキュリティ対策が実施されていることを保証する運用を行う場合に使用します。問題があれば是正期間中に対処を行うことができるため、厳密な運用を行うことができます。

- 是正期間を設けない運用

  セキュリティの実施状況の確認としてゆるやかな運用とする場合、是正期間を設けずに月単位で判断する場合に使用します。問題があっても翌月までに対処済みになればよいなどの指針で運用を行うことができます。

運用方法は変更可能です。Systemwalker Desktop Patrolを新規に導入し、セキュリティ監査の結果として達成率が低い間は、是正期間を設ける運用を実施し、安定期に入れば是正期間を設けない運用に変更することも可能です。

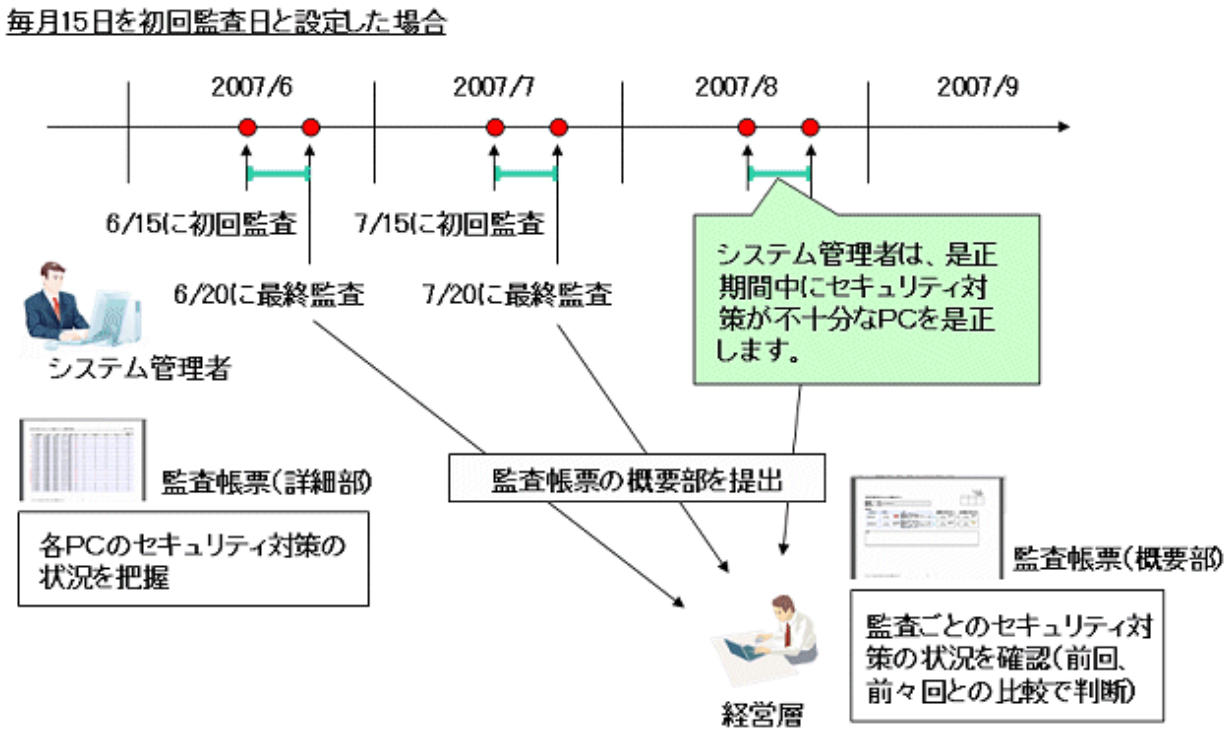
Systemwalker Desktop Patrolでは、セキュリティ対策を行う監査実施日、および是正期間を設け、定期的なセキュリティ監査を実施することを推奨します。

なお、セキュリティ監査をスケジュール実行し、夜間にセキュリティ監査を実施する運用も可能です。

運用パターン

是正期間を設ける運用

毎月15日を初回監査日、毎月20日を最終監査日とした場合の運用例を以下に示します。以下の例では、初回監査から最終監査までの是正期間にセキュリティ対策を実施し、セキュリティ対策状況を改善しています。



セキュリティ監査を行う流れは、以下のとおりです。

1. 初回監査日に、セキュリティ監査レポートを出力し、現状のセキュリティ対策状況を把握します。
2. 是正期間にセキュリティ対策状況として問題がなくなるまでセキュリティ対策を実施します。

   是正期間中は、毎日セキュリティ監査を実施し、監査結果からセキュリティ対策が不十分なPCに対してセキュリティ対策を実施します。

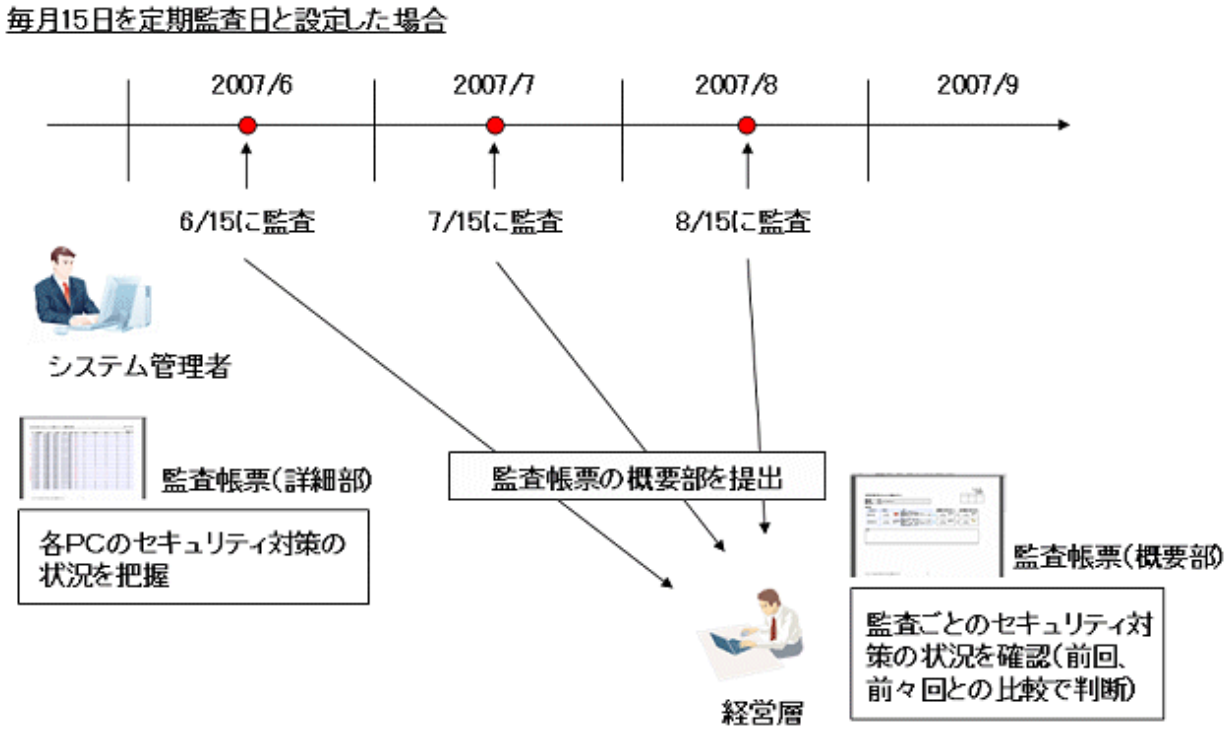
   セキュリティ対策を実施後、PCからインベントリ情報を収集し、セキュリティ監査レポートで問題がなくなったことを確認します。
3. 最終監査日に、セキュリティ監査の最終報告資料としてセキュリティ監査レポートを出力します。

システム管理者は、毎月15日に初回監査を実施します。出力されたセキュリティ監査の結果を確認し、セキュリティ対策が必要な機器の運用状況を20日までに是正します。毎月20日にシステム管理者から経営層の担当者にセキュリティ監査の結果を提出します。

是正期間を設ける運用では、監査結果として問題があっても、NGのPC利用者に対してセキュリティ対策の実施を促して、短期間にOKになるようにPC側の対処が終わるまでの猶予期間(是正期間)をもつことができます。

是正期間を設けない運用

毎月15日を監査日とした場合の運用例を以下に示します。以下の例では、是正期間を設けずに、セキュリティ監査レポートを出力し、長期的な観点でセキュリティ対策状況を確認しています。



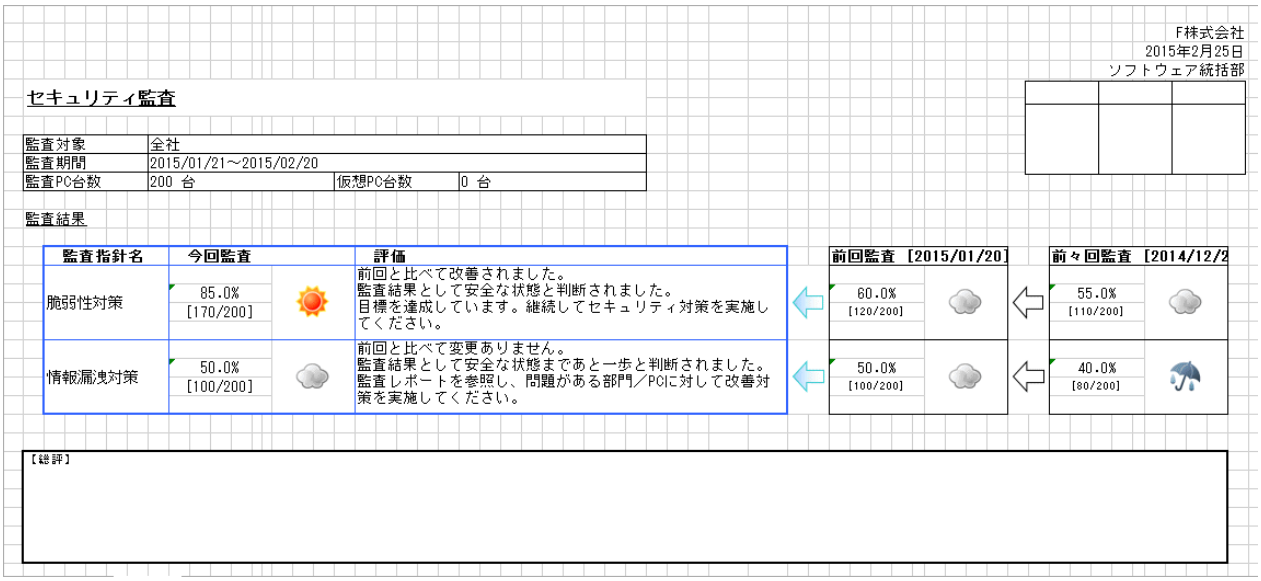
システム管理者は、毎月15日に定期監査を実施します。すでにセキュリティ対策が施されており、定期的にその状況を確認するだけでよい場合は、是正期間を設けない運用を利用します。

是正期間を設けない運用では、監査結果として既に安定している場合に、是正期間として時間を空けずに即時に判断することができます。

セキュリティ監査レポートの出力例

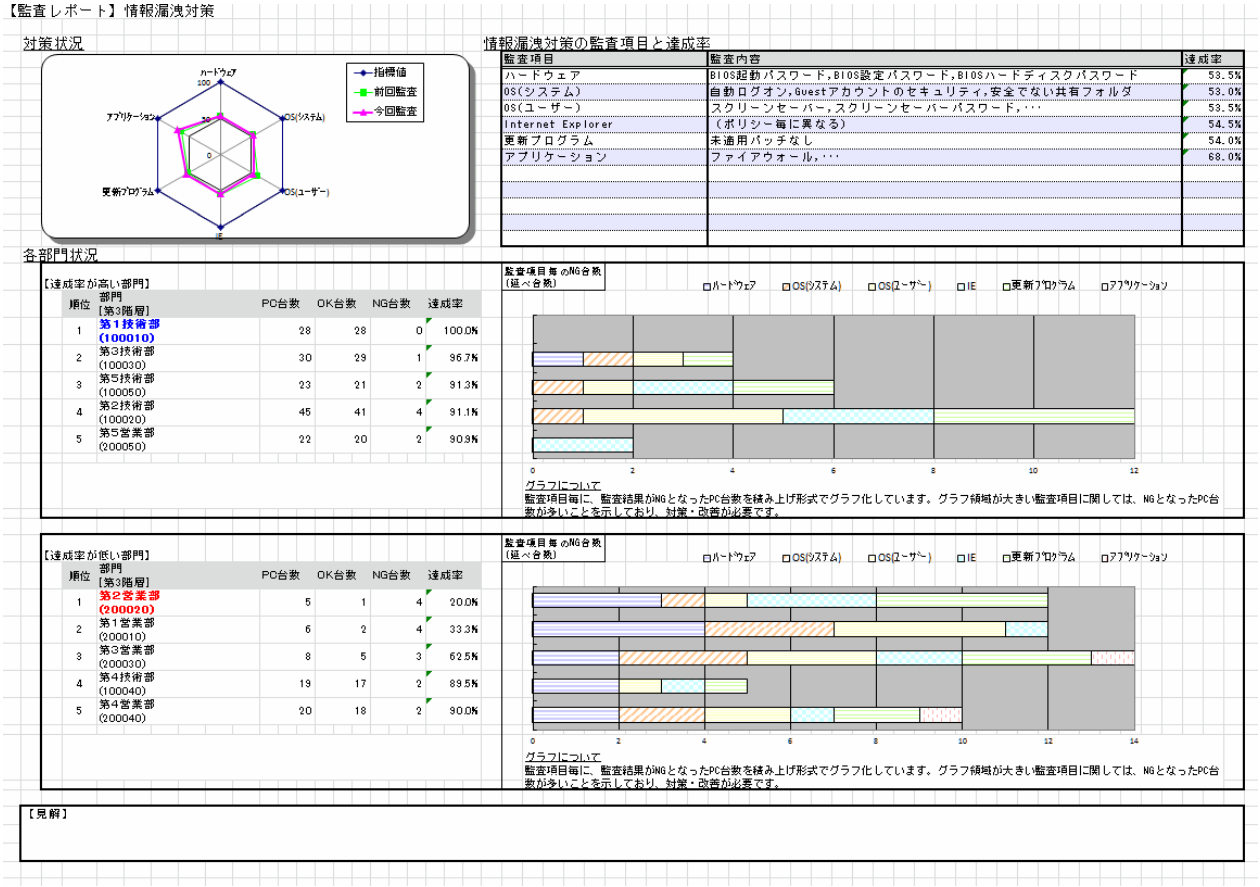
セキュリティ監査の結果として、セキュリティ監査レポートを出力します。セキュリティ監査レポートとは、Systemwalker Desktop Patrol、Systemwalker Desktop Keeper、Systemwalker Desktop Encryptionで実施しているセキュリティ対策について、運用状況やリスクのある部門/PCを把握・評価するために出力される監査/証明用レポートです。

以下は、セキュリティ監査レポートの[概要部]の出力例です。今回、前回、前々回のセキュリティ監査の結果が出力され、セキュリティ状況の推移が確認できます。



以下は、セキュリティ監査レポートの[監査レポート部]の出力例です。各監査内容や、監査項目ごとの達成率が表示されます。

また、集計結果でOK件数の割合が多い達成率の高いグループ、NG件数の割合が多い達成率の低いグループが表示されます。セキュリティ対策が不十分なグループに対し、セキュリティ対策の是正を促すことができます。



【監査レポート】情報漏洩対策

対策状況

情報漏洩対策の監査項目と達成率

監査項目	監査内容	達成率
ハードウェア	BIOS起動パスワード,BIOS設定パスワード,BIOSハードディスクパスワード	53.5%
OS(システム)	自動ログオン,Guestアカウントのセキュリティ,安全でない共有フォルダ	53.0%
OS(ユーザー)	スクリーンセーバー,スクリーンセーバーパスワード,･･･	53.5%
Internet Explorer	(ポリシー毎に異なる)	54.5%
更新プログラム	未適用パッチなし	54.0%
アプリケーション	ファイアウォール,･･･	68.0%

各部門状況

【達成率が高い部門】

順位	部門 [第3階層]	PC台数	OK台数	NG台数	達成率
1	第1技術部 (100010)	28	28	0	100.0%
2	第3技術部 (100030)	30	29	1	96.7%
3	第5技術部 (100050)	23	21	2	91.3%
4	第2技術部 (100020)	45	41	4	91.1%
5	第5営業部 (200050)	22	20	2	90.9%

監査項目毎のNG台数 (延べ台数)

グラフについて
監査項目毎に、監査結果がNGとなったPC台数を積み上げ形式でグラフ化しています。グラフ領域が大きい監査項目に関しては、NGとなったPC台数が多いことを示しており、対策・改善が必要です。

【達成率が低い部門】

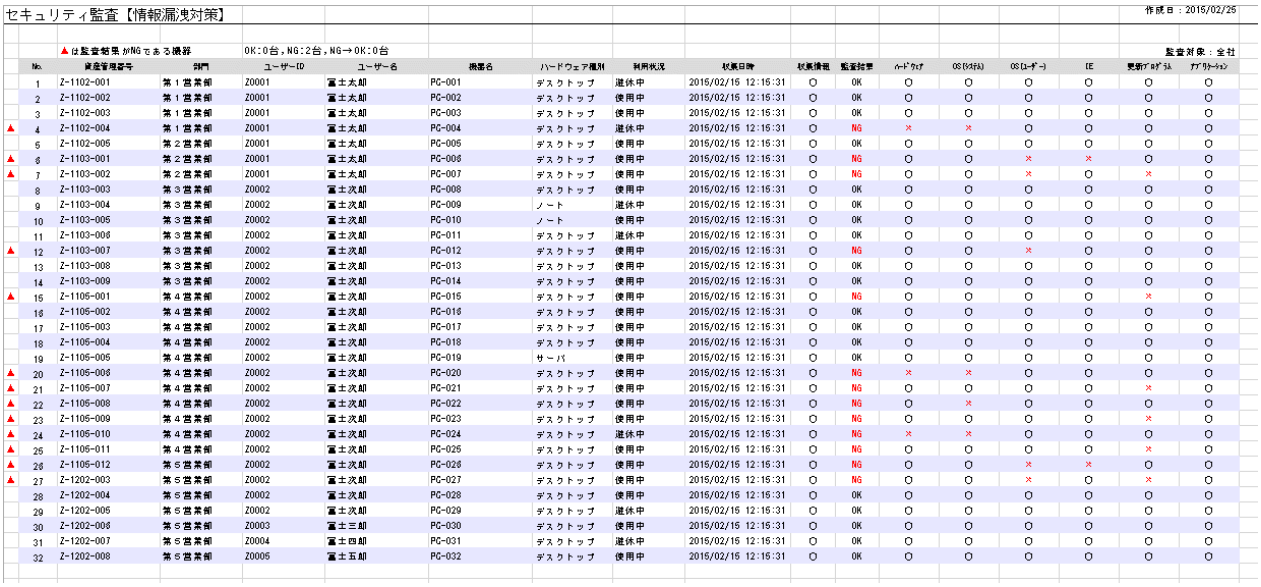
順位	部門 [第3階層]	PC台数	OK台数	NG台数	達成率
1	第2営業部 (200020)	5	1	4	20.0%
2	第1営業部 (200010)	6	2	4	33.3%
3	第3営業部 (200030)	8	5	3	62.5%
4	第4技術部 (100040)	19	17	2	89.5%
5	第4営業部 (200040)	20	18	2	90.0%

監査項目毎のNG台数 (延べ台数)

グラフについて
監査項目毎に、監査結果がNGとなったPC台数を積み上げ形式でグラフ化しています。グラフ領域が大きい監査項目に関しては、NGとなったPC台数が多いことを示しており、対策・改善が必要です。

【見解】

以下は、セキュリティ監査レポートの[詳細部]の出力例です。セキュリティ監査の結果が、機器ごとに表示されます。セキュリティ対策が不十分な機器を特定し、セキュリティ対策の是正を促すことができます。



セキュリティ監査【情報漏洩対策】

作成日：2016/02/25

▲は監査結果がNGである機器　OK:0台，NG:2台，NG→OK:0台　監査対象：全社

No.	資産管理番号	部門	ユーザーID	ユーザー名	機器名	ハードウェア種別	利用状況	収集日時	収集情報	監査結果	ハードウェア	OS(システム)	OS(ユーザー)	IE	更新プログラム	アプリケーション
1	Z-1102-001	第１営業部	Z0001	富士太郎	PC-001	デスクトップ	運休中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
2	Z-1102-002	第１営業部	Z0001	富士太郎	PC-002	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
3	Z-1102-003	第１営業部	Z0001	富士太郎	PC-003	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
▲ 4	Z-1102-004	第１営業部	Z0001	富士太郎	PC-004	デスクトップ	運休中	2015/02/15 12:15:31	○	NG	×	×	○	○	○	○
5	Z-1102-005	第２営業部	Z0001	富士太郎	PC-005	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
▲ 6	Z-1103-001	第２営業部	Z0001	富士太郎	PC-006	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	○	○	×	×	○	○
▲ 7	Z-1103-002	第２営業部	Z0001	富士太郎	PC-007	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	○	○	×	○	×	○
8	Z-1103-003	第３営業部	Z0002	富士次郎	PC-008	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
9	Z-1103-004	第３営業部	Z0002	富士次郎	PC-009	ノート	運休中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
10	Z-1103-005	第３営業部	Z0002	富士次郎	PC-010	ノート	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
11	Z-1103-006	第３営業部	Z0002	富士次郎	PC-011	デスクトップ	運休中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
▲ 12	Z-1103-007	第３営業部	Z0002	富士次郎	PC-012	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	○	○	×	○	○	○
13	Z-1103-008	第３営業部	Z0002	富士次郎	PC-013	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
14	Z-1103-009	第３営業部	Z0002	富士次郎	PC-014	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
▲ 15	Z-1105-001	第４営業部	Z0002	富士次郎	PC-015	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	○	○	○	○	×	○
16	Z-1105-002	第４営業部	Z0002	富士次郎	PC-016	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
17	Z-1105-003	第４営業部	Z0002	富士次郎	PC-017	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
18	Z-1105-004	第４営業部	Z0002	富士次郎	PC-018	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
19	Z-1105-005	第４営業部	Z0002	富士次郎	PC-019	サーバ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
▲ 20	Z-1105-006	第４営業部	Z0002	富士次郎	PC-020	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	×	×	○	○	○	○
▲ 21	Z-1105-007	第４営業部	Z0002	富士次郎	PC-021	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	○	○	○	○	×	○
▲ 22	Z-1105-008	第４営業部	Z0002	富士次郎	PC-022	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	○	×	○	○	○	○
▲ 23	Z-1105-009	第４営業部	Z0002	富士次郎	PC-023	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	○	○	○	○	×	○
▲ 24	Z-1105-010	第４営業部	Z0002	富士次郎	PC-024	デスクトップ	運休中	2015/02/15 12:15:31	○	NG	×	×	○	○	○	○
▲ 25	Z-1105-011	第４営業部	Z0002	富士次郎	PC-025	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	○	○	○	○	×	○
▲ 26	Z-1105-012	第５営業部	Z0002	富士次郎	PC-026	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	○	○	×	×	○	○
▲ 27	Z-1202-003	第５営業部	Z0002	富士次郎	PC-027	デスクトップ	使用中	2015/02/15 12:15:31	○	NG	○	○	×	○	×	○
28	Z-1202-004	第５営業部	Z0002	富士次郎	PC-028	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
29	Z-1202-005	第５営業部	Z0002	富士次郎	PC-029	デスクトップ	運休中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
30	Z-1202-006	第５営業部	Z0003	富士三郎	PC-030	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
31	Z-1202-007	第５営業部	Z0004	富士四郎	PC-031	デスクトップ	運休中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○
32	Z-1202-008	第５営業部	Z0005	富士五郎	PC-032	デスクトップ	使用中	2015/02/15 12:15:31	○	OK	○	○	○	○	○	○

2.11.3 省電力対策の監査レポート

ユーザーが決定した監査指針に基づき省電力対策の運用状況を監査します。省電力監査の結果は、グリーンICT対策の見直しに利用できます。

また、省電力監査の結果は、レポートとして出力し、正しく省電力対策が行われていることの証明書としても利用できます。

省電力監査レポートの出力例

省電力監査の結果として、省電力監査レポートを出力します。省電力監査レポートとは、省電力対策について運用状況やリスクのある部門/PCを把握・評価するために出力される監査/証明用レポートです。

以下は、省電力監査レポートの出力例です。

・ 省電力設定状況レポート

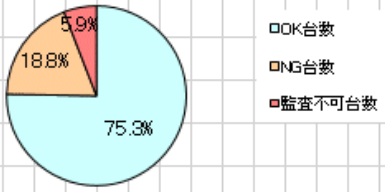
省電力設定状況レポート

F株式会社

対象	管理対象		
対象PC台数	170台	仮想PC台数	0台
作成者名	富士通太郎		
作成日	2015年02月25日		

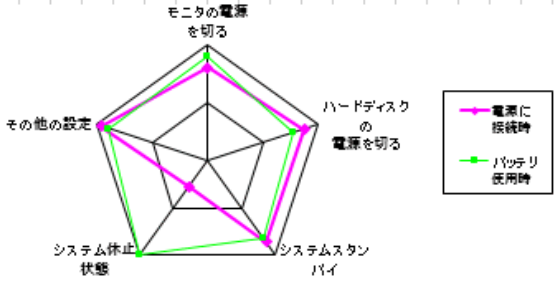
【省電力設定状況】

対象PC台数	170 台
OK台数	128台
NG台数	32 台
監査不可台数	10 台
達成率	81.2%



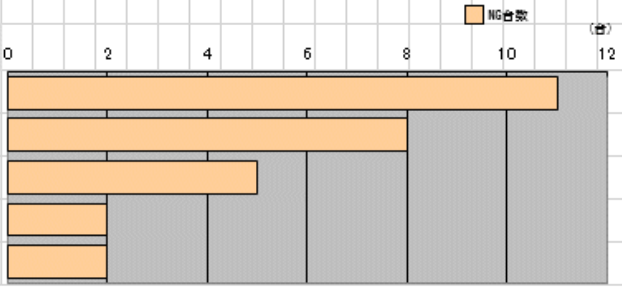
【省電力設定状況(達成率)の内訳】

	電源に接続時	バッテリ使用時
モニタの電源を切る	80.2%	90.2%
ハードディスクの電源を切る	87.5%	78.0%
システムスタンバイ	86.3%	82.0%
システム休止状態	27.5%	100.0%
その他の設定	96.3%	89.1%



【達成率の低いグループ】 (単位：台)

No.	部門	対象PC台数	OK台数	NG台数	監査不可台数	達成率
1	ソフトウェア統括部	20	9	11	0	45.0%
2	ソフト営業一課	28	20	8	0	71.4%
3	ソフト営業三課	22	17	5	0	77.3%
4	ソフト営業二課	8	6	2	0	75.0%
5	ソフト営業部	15	13	2	0	86.7%



【コメント】

・ 消費電力量の監査レポート

消費電力量の監査レポート

F株式会社

対象	管理対象
対象PC台数	170台
作成者名	富士通太郎
作成日	2015年02月25日
監査期間	2015年02月01日～2015年02月25日

【電気代の積算値と削減効果】

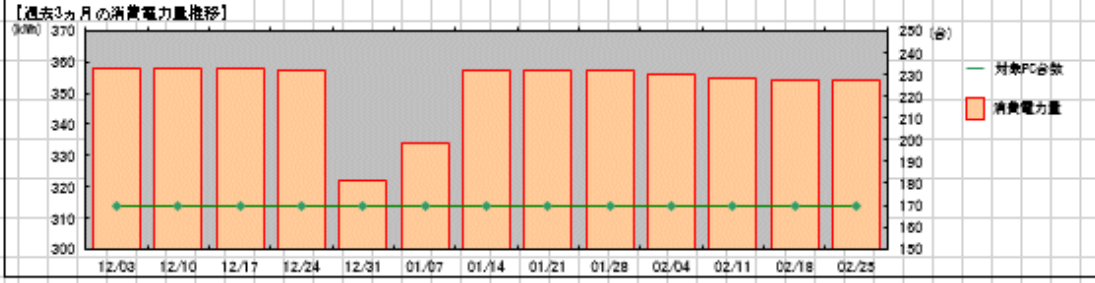
	当月の積算値	年度累計(※)
電気代	30,382円	143,411円
電力削減額	6,930円	35,112円
CO2削減量	174.8kg	885.8kg

(※)累計期間 2014年4月～2015年2月

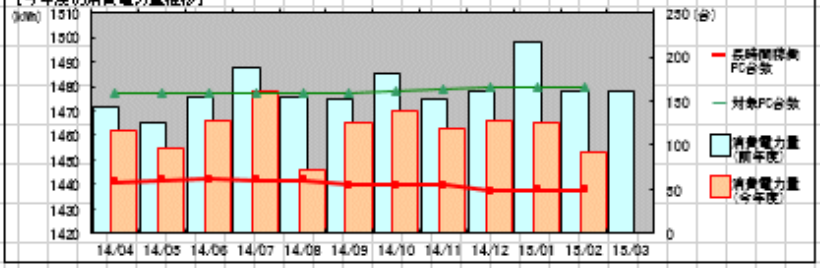
【消費電力量の参考情報】

	2015年02月	2015年01月
消費電力量	1,381kWh	1,401kWh
1台あたりの平均消費電力量	8.12kWh	8.24kWh
対象PC台数	170台	170台
長時間稼働PC台数	46台	50台
消費電力量の削減率	18.6%	17.4%

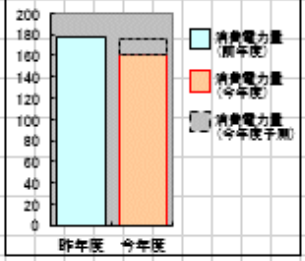
【過去3ヵ月の消費電力量推移】



【今年度の消費電力量推移】



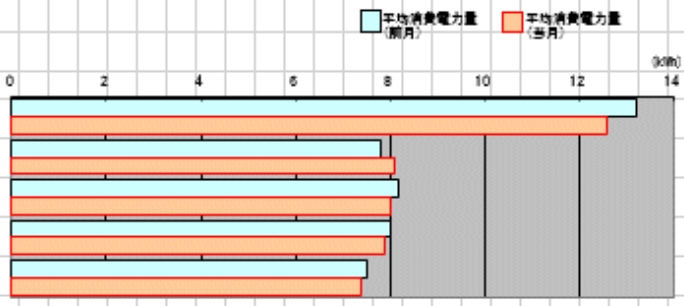
【昨年との比較】(単位:百kWh)



【達成率の低いグループ】

(単位:kWh)

順位	部門	1台あたりの平均消費電力量 前月	当月
1	ソフトウェア統括部	13.2	12.6
2	ソフト営業一課	7.8	8.1
3	ソフト営業三課	8.2	8.0
4	ソフト営業二課	8.0	7.9
5	ソフト営業部	7.5	7.4



【コメント】

2.11.4 複合機/プリンタの稼働状況レポート

複合機／プリンタと連携し、複合機／プリンタにおける消費電力量と稼働状況(スタンバイなどの稼働モード)を取得し、消費電力量・CO2排出量・費用や稼働時間の累計を見える化します。

これらの情報は、レポートとして出力します。

レポートの内容に基づき、定期的に公開／改善を実施することで、複合機／プリンタの省電力に役立てます。

なお、本機能は、システム管理者のみが使用できるものであり、部門管理者がログインした場合は選択できません。

また、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対応複合機／プリンタのみです。

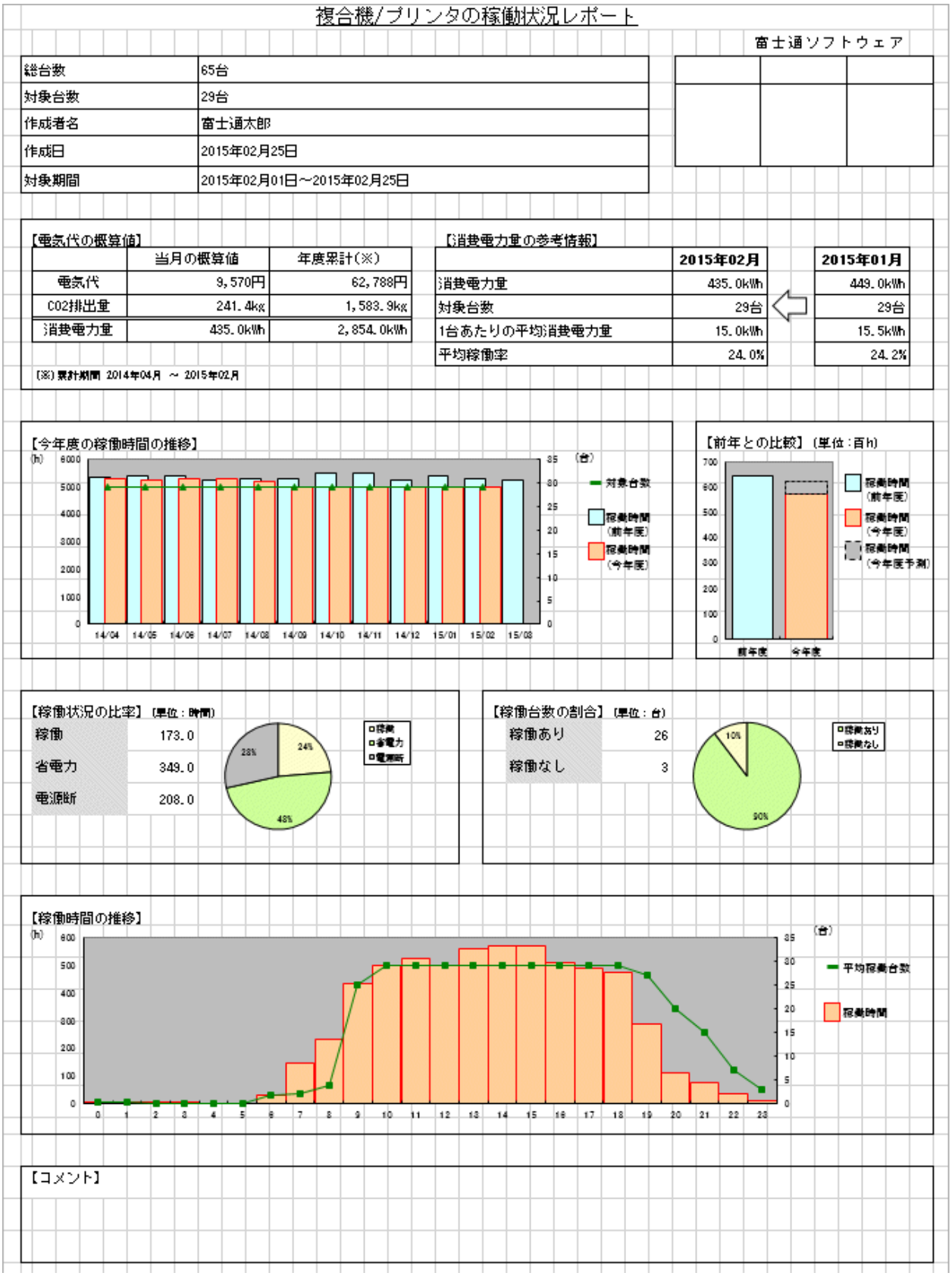
複合機/プリンタの稼働状況レポートの出力例

連携する複合機／プリンタの消費電力量・CO2排出量・費用や稼働時間を、複合機/プリンタの稼働状況レポートとして出力します。

複合機/プリンタの稼働状況レポートとは、現在の状況および削減施策の効果を把握するために出力される状況レポートです。

以下は、複合機/プリンタの稼働状況レポートの出力例です。

- 複合機/プリンタの稼働状況レポート

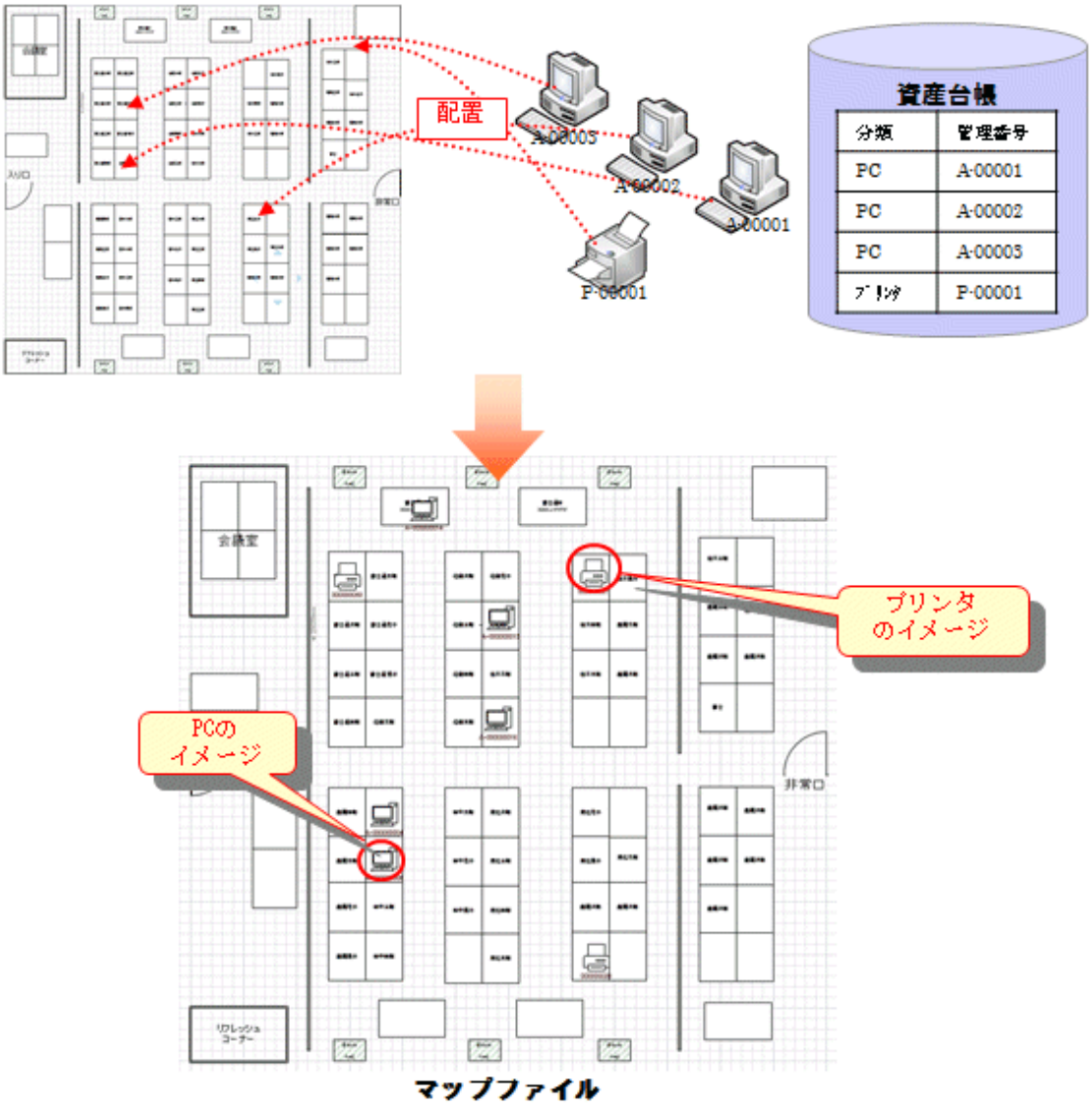


2.12 ロケーションマップ機能

フロアのイメージを示したレイアウト図に対して、資産台帳に管理されている機器を配置して管理できます。

機器の配置を視覚的に確認しながら、機器の資産情報を参照できます。

レイアウト図による機器管理を行う場合は、Microsoft Visioが必要です。



2.13 環境設定機能

ユーザー管理

CTの導入されたPCを利用・管理する人をユーザーと言い、このユーザーをCS上で一元管理するための機能です。ユーザーの登録、削除、およびユーザー権限の設定や変更を行います。

また、登録したユーザーをユーザー一覧として参照できます。

部門管理

事業部、部、課などのような企業の部門であり、PCを利用するユーザーは通常部門に所属します。部門の登録および削除を行います。

また、登録した部門を部門一覧として参照できます。

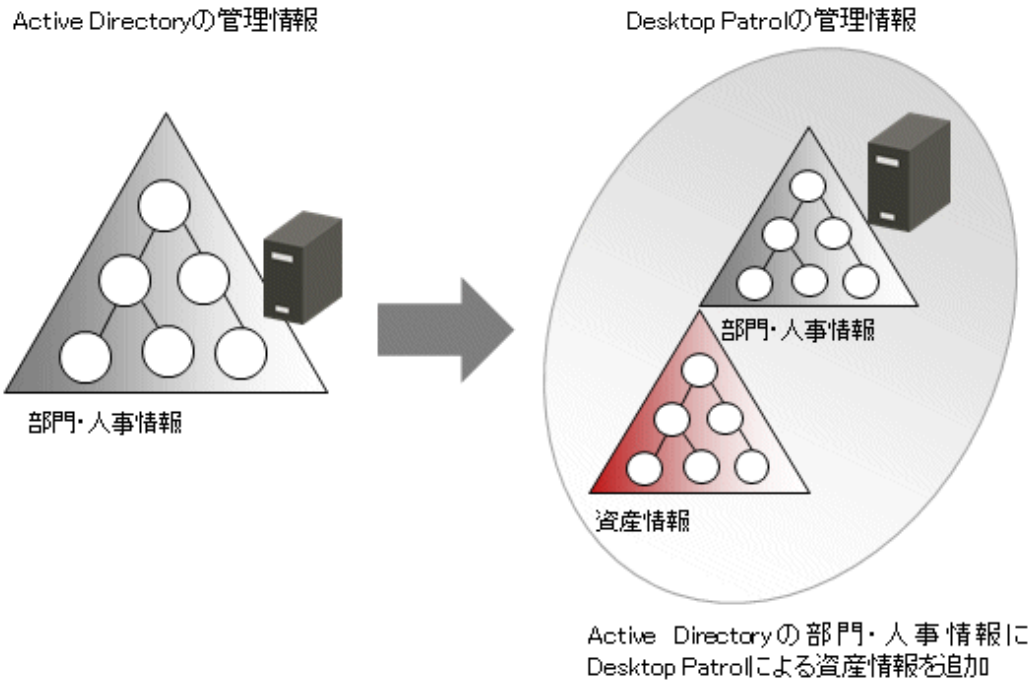
Active Directory連携機能

Active Directoryとは、ネットワーク上の各種資源（PCやプリンタ、ユーザー情報等）を効率よく管理するためのディレクトリサービスです。Desktop PatrolはActive Directoryと連携することにより、Active Directoryで管理している部門・人事情報に、Desktop Patrolによる資産情報を関連づけて管理できるようになります。また、Active Directoryの部門・人事情報からDesktop Patrolのマスタ管理情報を自動的に生成できるため、従来のように手作業によるDesktop Patrolのマスタ管理情報を作成する必要がなくなり、情報を一元管理する運用を行えます。

また、従来のActive Directoryと連携しない運用と併用することも可能であるため、Active Directoryと連携する部門や、連携しない部門を運用に応じて自由に選択でき、柔軟にユーザー業務へ対応できます。

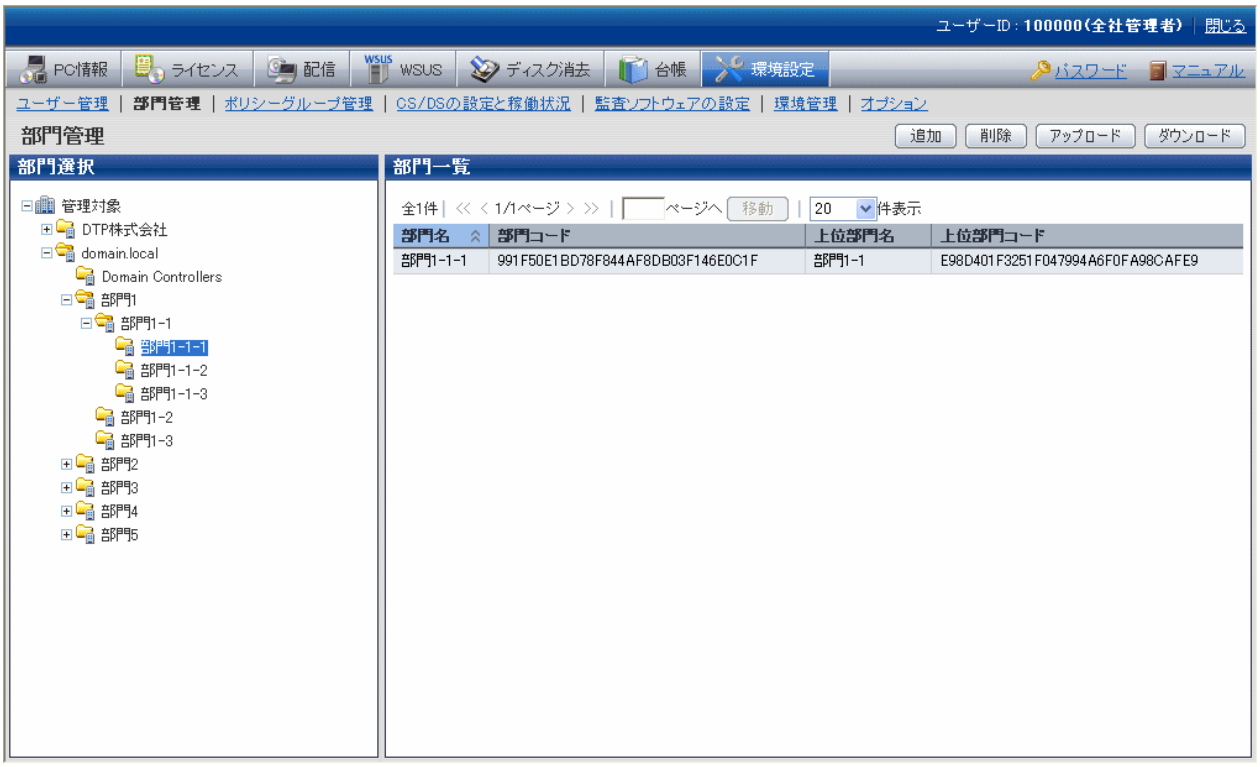
なお、Active Directoryと連携できるのは、シングルドメイン運用を行っている場合に限ります。マルチドメイン運用を行っている場合はDesktop Patrolと連携できません。

Active Directory連携機能の概要を以下に示します。



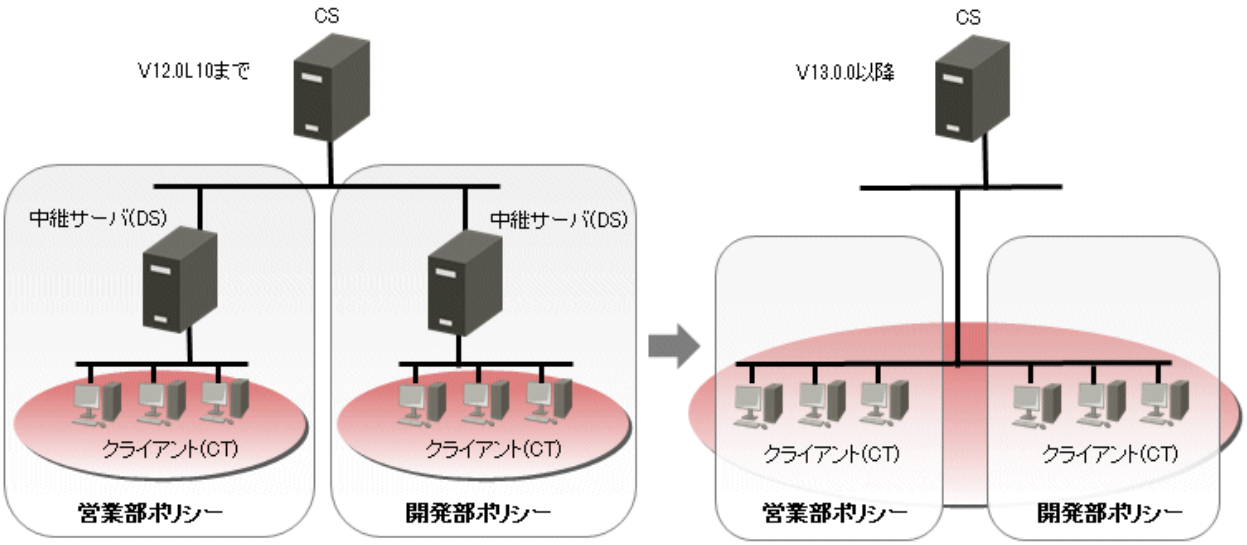
Active Directoryと連携した場合のメインメニューの例を以下に示します。

Active Directoryから取得した部門情報は、ドメイン名を最上位部門とした部門ツリー配下に表示されます。



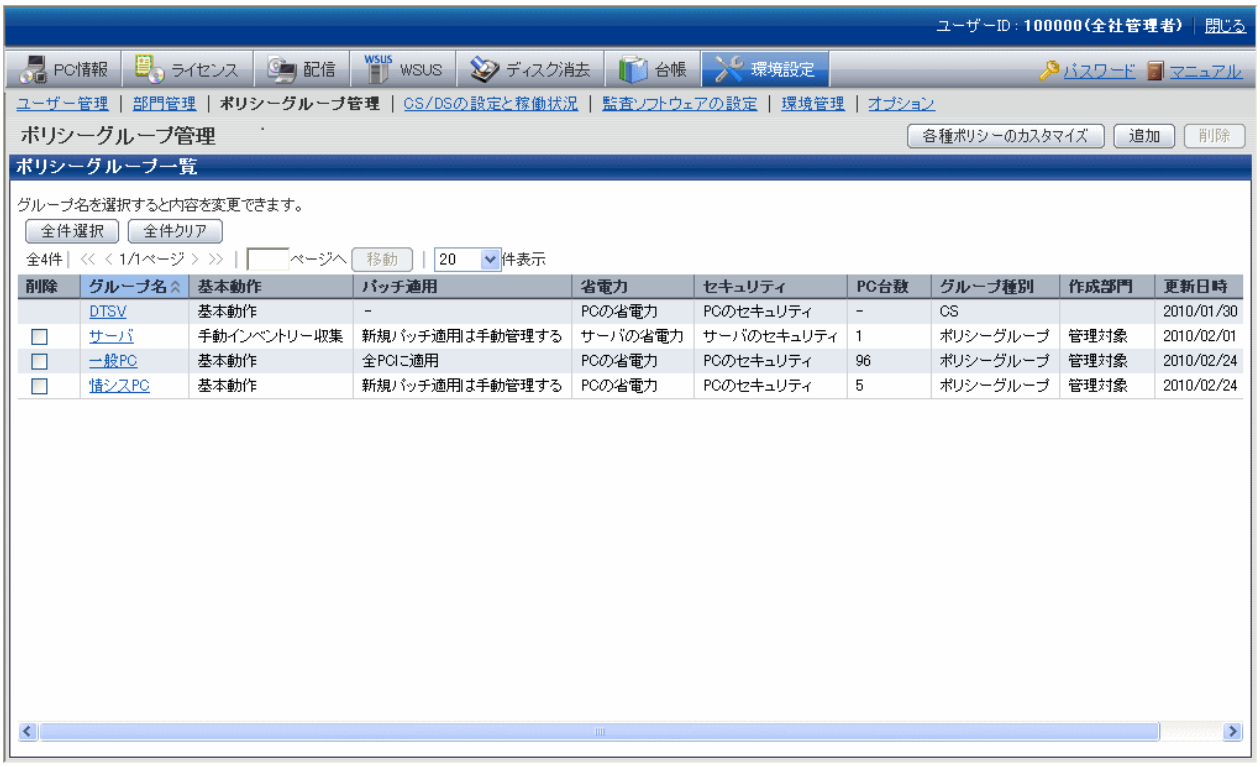
ポリシーグループ管理

ポリシーグループ管理機能とは、セキュリティパッチの適用スケジュールや適用動作、インベントリ収集スケジュール、またはソフトウェアの配信条件といった、クライアントの動作ポリシーを、論理的なグループ毎に設定可能とする機能です。



従来では動作ポリシーを変えるために、各拠点に複数の中継サーバを構築していましたが、PCを論理的なグループに所属させることにより、動作ポリシーを変えるための中継サーバは不要になります。

ポリシーグループは、メインメニューの以下の画面で作成します。



注意

V12以前のバージョン混在時の注意事項

ポリシーグループ機能はSystemwalker Desktop Patrol V13.0.0以降のCTで有効です。

V12以前のCTがインストールされているPCをポリシーグループに所属させた場合、ポリシーグループ単位ではなくDS単位のポリシーで動作します。

環境管理

Systemwalker Desktop PatrolとSystemwalker Desktop Keeperの間で、初期導入時に構成情報を連携できます。システム導入時に構成情報を流用して容易に環境を構築できます。

なお、Active Directoryと連携した運用を行う場合は、本機能を利用できません。

監査ソフトウェアの設定

ソフトウェア辞書の設定を行い、PCで監査対象とするソフトウェアを決定する機能です。

ソフトウェア辞書は、クライアントで使用されているソフトウェアのインベントリ情報を収集するためのポリシーです。ソフトウェア辞書には、以下の2種類があります。詳細は、“1.3.2 ソフトウェア辞書”を参照してください。

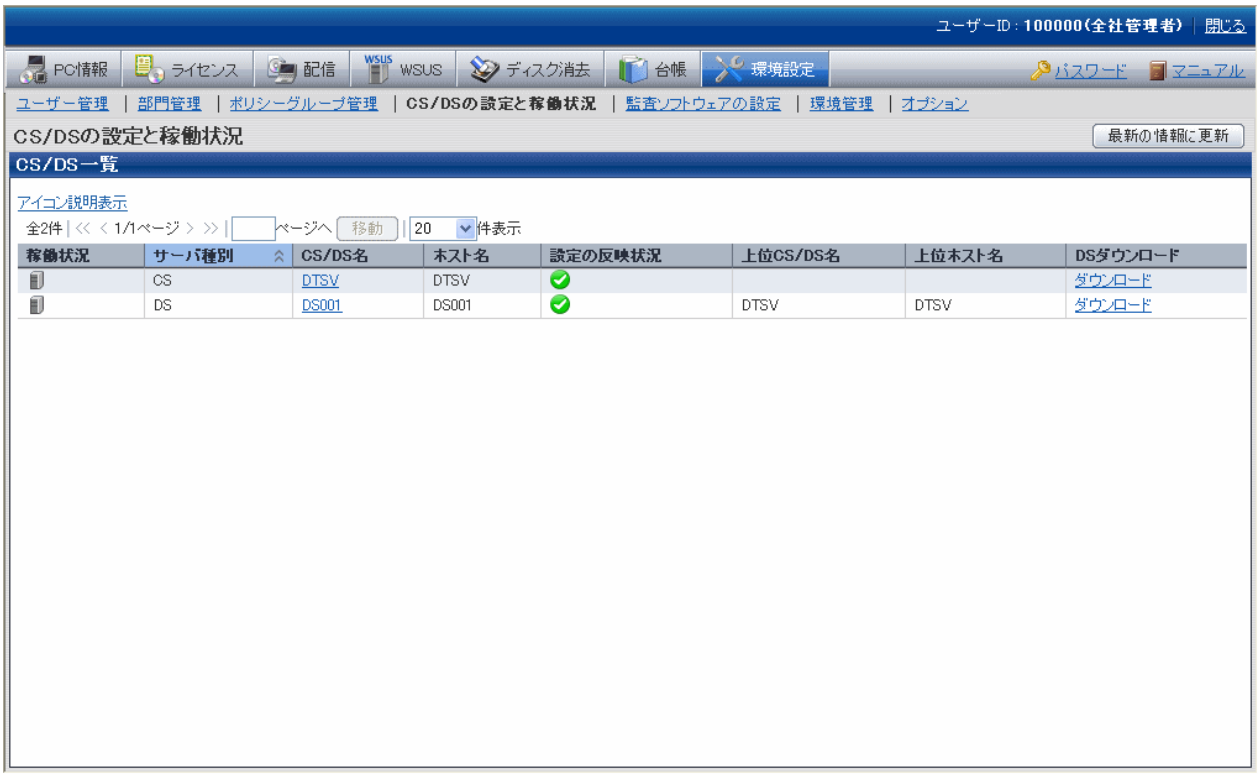
- サポートセンター定義
- ユーザー定義

編集した各ポリシーは、ソフトウェア配信のルートで、DSやCTに通知されます。

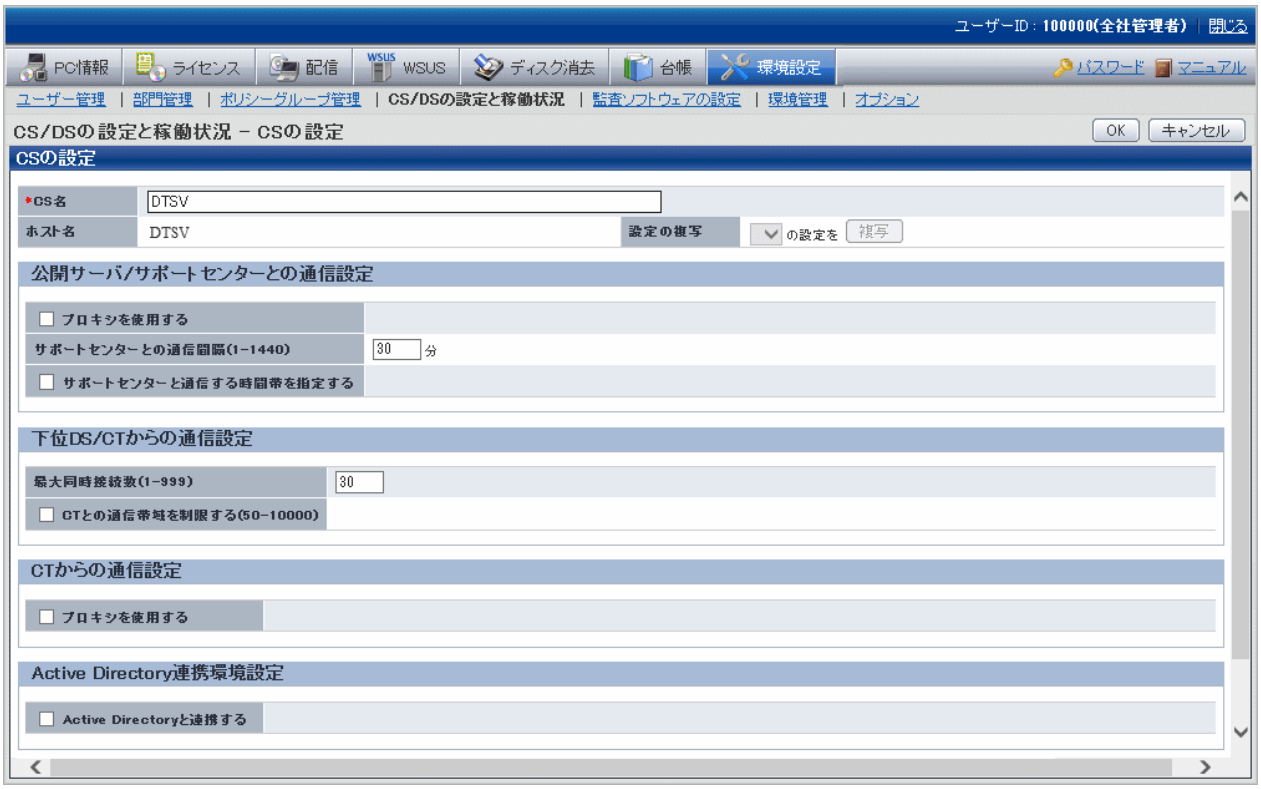
CS/DSの設定と稼働状況

CS/DSの稼働状況、およびCS/DSそれぞれの通信設定等を行う機能です。

稼働状況は以下の画面で確認できます。



設定画面は以下の画面で設定します。以下はCSの例です。



2.14 リモート操作機能

Systemwalker Desktop Patrolのリモート操作は、以下のような機能をサポートしています。

- リモート操作
- 双方向、複数画面受信
- 双方向ファイル転送、ファイルシステムの比較
- 双方向クリップボード転送

各機能の詳細は、Systemwalker Live Helpのマニュアルを参照してください。

リモート操作

管理者のキーボードとマウスでエンドユーザーのコンピュータを操作できます。特殊キーシーケンスも送信可能、リモートログオン、ログオフも可能です。

双方向、複数画面受信

画面やマウスの動きをリアルタイムで受信し表示(リモート操作)するだけでなく、自分の画面を送信して、エンドユーザーのトレーニングにも利用できます。さらに、同時に複数コンピュータの監視・リモート操作も行えます。受信画面はウィンドウに合わせて縮小表示が可能です。

双方向ファイル転送、ファイルシステムの比較

Windowsのエクスプローラと同様な操作感覚で双方向にファイル転送が行えます。

ローカルとリモートのコンピュータのファイルやフォルダの比較が可能なので、ファイルシステムの問題点の特定を効率化できます。

双方向クリップボード転送

クリップボードの内容を一括転送、問題発生時の画面取得やメモの転送が簡単に行えます。

2.15 アップデータ機能

DSおよびCTの修正を、簡易な操作でお客さまのシステムに修正適用できる機能です。

DSおよびCTの修正をアップデータ登録コマンドで登録することで、配信対象のDSおよびCTのマシンへ自動的に適用できます。適用は自動的に行われるため、DSおよびCTのマシンで管理者が適用操作を行う必要はありません。

修正を適用し、OSの再起動が必要となった場合に、再起動が必要であるとのメッセージを表示できます。詳細は、

“リファレンスマニュアル”の“CustomPolicy.exeコマンド”の“-cl.chkreboot.enabled”オプションを参照してください。

注意

修正を適用し、OSの再起動が必要となった場合、高速スタートアップ機能が有効な環境で修正の適用を完了させるためには、OSの「再起動」が必要です。

OSの「シャットダウン」では修正の適用が完了しない場合があります。

書き込み保護が「有効」なPCへの配信

書き込み保護が「有効」なPCに、CTアップデータを配信した場合、ファイル配信機能と同様に、書き込み保護のフィルター状態を変更して、修正適用します。

表示する画面などの情報は、“運用ガイド 管理者編”の“書き込み保護が「有効」なPCへの配信”を参照してください。

2.16 クライアント抑止機能

クライアント抑止機能とは、Systemwalker Desktop Patrolによるセキュリティの管理を確実に行うために、CTをインストールしたPCに対して、ユーザーが以下の操作を行うことを抑止する機能です。

- CTのサービス停止
- CTのアンインストール
- CTの接続サーバの変更

CTのサービス停止の抑止

ユーザーが、CTのサービス“ITBudgetMGR（INV）”を停止することを抑止します。

サービス停止の抑止には、以下の機能があります。

- サービスの即時停止を抑止
  - [コントロールパネル]-[管理ツール]-[サービス]のプロパティ画面の[サービスの状態]で[停止]ボタンを非活性化し、サービスが停止できないようにします。
  - Windows標準コマンドの“NET STOP”コマンドでサービスの停止を行うとコマンドが異常終了し、サービスが停止できないようにします。
- サービスが手動起動に変更されても自動起動に復旧

  [コントロールパネル]-[管理ツール]-[サービス]のプロパティ画面の[スタートアップの種類]を定期的に監視し、設定が[自動]以外に変更されていた場合は強制的に以下の設定に復旧します。
  - スタートアップの種類：自動

本機能は、CTだけが導入されている環境で有効になります。CS、DSでは本機能を使用できません。

CTのアンインストールの抑止

ユーザーが、CTのアンインストール操作を行うと、パスワード入力を要求し、アンインストールを抑止します。

[コントロールパネル]の[プログラムと機能]-[プログラムのアンインストール]からCTのアンインストール操作を行うと、パスワード入力を要求します。ユーザーがアンインストールを行う場合は、管理者へ連絡し、パスワードの確認を行う必要があります。

本機能は、CTだけが導入されている環境で有効になります。CS、DSでは本機能を使用できません。

CTの接続サーバ変更の抑止

ユーザーが、CTの環境設定画面から[接続サーバ]の変更を行うことを抑止します。

CTの環境設定画面の[サーバ切替え]タブの[接続サーバ]の入力域を非活性化し、初期値から変更できないようにします。

第3章 動作環境

本章では、Systemwalker Desktop Patrolを動作させるために必要な環境について説明します。

3.1 ハードウェア

Systemwalker Desktop Patrolを使用するために必要な、ハードウェア環境をコンポーネントごとに示します。

CS

- 必要CPUスペック

  インテル Xeon E5503(2GHz)以上

- 必要メモリ容量

  4.5GB以上(OSの使用量を含まず)

  WSUS連携機能を利用する場合、上記に追加で3.5GB以上

注意

SAMACのソフトウェア辞書に登録されているデータをCSに移入する場合は、配信サーバ機能のメモリサイズの拡張が必要です。メモリサイズの拡張方法は、“リファレンスマニュアル”の“ユーザー資産ソフトウェア辞書作成コマンドで出力するメッセージ”を参照してください。

- 必要ディスク容量

  1050MB(インストール先)＋135MB(システムドライブ:ランタイムライブラリを格納)＋登録ソフトウェアサイズ以上＋登録パッチサイズ(注1)＋CT稼働状況ログサイズ(注2)＋245MB(注3)+データベース容量

  注1)登録パッチサイズは、自動パッチ適用機能を使用する場合に必要です。35GB以上のディスク容量が必要です。

  注2)CT稼働状況ログを格納するための以下のディスク容量が必要です。
  また、CT動作状況チェックコマンドで表示する情報の一部(稼働状況)に、当ログファイルの情報を使用します。CSにCT稼働状況ログを格納していない環境では、“稼働状況”が表示されません。

  CT稼働状況ログサイズ = 30KB × ユーザー数 × 保存日数

  注3)ソフトウェアのインストールと管理に必要なディスク容量です。
  システムドライブ¥FujitsuF4CR 配下に確保します。

  ソフトウェアの登録/配信、またはセキュリティパッチの自動適用を行う場合、処理対象のソフトウェアのサイズに対して十分なディスク空き容量があることを確認してから実行してください。なお、ソフトウェアの登録/配信、またはセキュリティパッチの自動適用によるディスク領域不足を発生させないために、ソフトウェア格納ディレクトリは、OSがインストールされているディスク領域とは別の領域を指定してください。また、ソフトウェア格納ディレクトリ最大サイズを、必要に応じて設定してください。

  構築するデータベースサイズに応じて、以下のディスク容量が必要です。1台のCSで管理可能なPCの台数は、最大100,000台です。

PC台数	EXE情報の収集	ソフトウェア稼働状況の収集	データベース容量
500台	なし	なし	約34.1GB
	なし	あり	約34.6GB
	あり	なし	約38.0GB
	あり	あり	約38.4GB
1,000台	なし	なし	約52.1GB
	なし	あり	約53.2GB
	あり	なし	約59.6GB

PC台数	EXE情報の収集	ソフトウェア稼働状況の収集	データベース容量
	あり	あり	約60.7GB
3,000台	なし	なし	約114.3GB
	なし	あり	約117.3GB
	あり	なし	約133.9GB
	あり	あり	約136.8GB
10,000台	なし	なし	約134.5GB
	なし	あり	約144.4GB
	あり	なし	約199.7GB
	あり	あり	約209.6GB
20,000台	なし	なし	約163.3GB
	なし	あり	約183.1GB
	あり	なし	約293.8GB
	あり	あり	約313.5GB
50,000台	なし	なし	約213.1GB
	なし	あり	約254.8GB
	あり	なし	約489.0GB
	あり	あり	約530.8GB
80,000台	なし	なし	約286.3GB
	なし	あり	約353.1GB
	あり	なし	約727.8GB
	あり	あり	約794.6GB
100,000台	なし	なし	約335.1GB
	なし	あり	約418.6GB
	あり	なし	約887.0GB
	あり	あり	約970.5GB

機器（什器）の管理を行う場合

PC台数、PC以外の管理台数に応じて以下のデータベース容量が追加で必要です。

PC台数	データベース容量
100台～2,999台	PC以外の管理台数×0.39MB
3,000台～29,999台	PC以外の管理台数×0.34MB
30,000台以上	PC以外の管理台数×0.29MB

PC台数が20,000台を超える場合

CSのインストール先とは異なるドライブにデータベースを作成する必要があります。CPUのコア数は、8コア以上必要です。

また、データベース格納先には、以下の性能を満たすストレージが必要です。

シーケンシャルリード	300MB/秒 以上

シーケンシャルライト	300MB/秒 以上
ランダムリード(4KB)	10MB/秒 以上
ランダムライト(4KB)	10MB/秒 以上

WSUSの更新プログラムをダウンロードする場合

WSUSの動作のために必要ディスク容量として最低限40GB必要です。また、追加で更新プログラムのデータ容量が必要です。

例）Windows 10およびWindows 11の更新プログラム(Feature Update、Quality Update)を5年分保持する場合

ー 年に2回5GB以上必要

Feature Update：5GB×2×5=50GB

ー 月に1回以上、2GB以上必要

Quality Update：2GB×12×5=120GB

クイック実行形式のセキュリティパッチの配信を行う場合

以下のディスク容量が追加で必要です。

ー CSがインターネットに接続できる場合

配信する1チャネル、1ライセンスにつき、4.5GB以上必要。

- 例1）基本設定Microsoft 365(旧Office 365)の半期チャネル(特定セキュリティパッチを配信)を設定
  1（チャネル）× 4.5 ＝ 4.5GB以上
- 例2）基本設定でMicrosoft 365(旧Office 365)の半期チャネル(特定セキュリティパッチを配信)、先行検証用のポリシーグループでMicrosoft 365(旧Office 365)の半期チャネル(最新セキュリティパッチを配信)を設定
  2（チャネル）× 4.5 ＝ 9GB以上

ー CSがインターネットに接続できない場合（注）

- チャネルの概念の場合（例：Microsoft 365(旧Office 365)）
  月次チャネル（対象指定含む）：27GB以上
  半期チャネル（対象指定含む）：162GB以上
- ライセンスの概念の場合（例：Office2019）
  54GB以上

注）Office配信サーバにもCSと同様のディスク容量が必要です。

【Systemwalker標準データベースの拡張を行う場合について】

拡張前のデータベース割当量は、データベースの拡張の際「運用環境保守ウィザード」の「現在のデータベース使用状況です。」画面の「割当量」に表示されます。必要に応じて確認してください。

ディスクの空き容量として、退避データ格納先に必要となる容量と、データベース格納先に必要となる容量を合算した容量が必要です。

- 退避データ格納先のドライブには、拡張前のデータベース割当量と同じ容量が必要です。
- データベース格納先を別のドライブに変更する場合は、上記で見積もった必要ディスク容量が変更先のドライブに必要です。
  データベース格納先のドライブを変更しない場合は、上記で見積もった必要ディスク容量から拡張前のデータベース割当量を差し引いた容量が必要です。

DS

・ 必要CPUスペック

インテル Xeon E5503(2GHz)以上

・ 必要メモリ容量

850MB以上（OSの使用量を含まず）

WSUS連携機能を利用する場合、上記に追加で3.5GB以上

・ 必要ディスク容量

256MB（インストール先）＋12MB（システムドライブ：ランタイムライブラリを格納）＋ダウンロードソフトウェアサイズ＋ダウンロードパッチサイズ（注）以上

注）ダウンロードパッチサイズは、自動パッチ適用機能を使用する場合に必要です。35GB以上のディスク容量が必要です。

WSUSの更新プログラムをダウンロードする場合

WSUSの動作のために必要ディスク容量として最低限40GB必要です。また、追加で更新プログラムのデータ容量が必要です。

例）Windows 10およびWindows 11の更新プログラム(Feature Update、Quality Update)を5年分保持する場合

－ 年に2回5GB以上必要

Feature Update：5GB×2×5=50GB

－ 月に1回以上、2GB以上必要

Quality Update：2GB×12×5=120GB

クイック実行形式のセキュリティパッチの配信を行う場合

以下のディスク容量が追加で必要です。

配信する1チャネル、1ライセンスにつき、4.5GB以上必要。

－ 例1）基本設定でMicrosoft 365(旧Office 365)の半期チャネル(特定セキュリティパッチを配信)を設定
1（チャネル）× 4.5 ＝ 4.5GB以上

－ 例2）基本設定でMicrosoft 365(旧Office 365)の半期チャネル(特定セキュリティパッチを配信)、先行検証用のポリシーグループでMicrosoft 365(旧Office 365)の半期チャネル(最新セキュリティパッチを配信)を設定
2（チャネル）× 4.5 ＝ 9GB以上

AC

・ 必要CPUスペック

Pentium IV またはXeon 2GHz以上

・ 必要メモリ容量

256MB以上（OSの使用量を含まず）

・ 必要ディスク容量(注)

620MB以上

注) ファイルシステムは「NTFS（NT File System）」とする必要があります。

CT

Live Help Clientを導入した環境

・ 推奨CPUスペック

1GHz以上

・ 推奨メモリ容量

300MB以上（OSの使用量を含まず）

最小常駐使用メモリ

ー 通常時:32MB

ー ソフトウェア稼働状況収集時:300MB

ー コマンドモードCTは非常駐

・ 推奨ディスク容量

45MB以上(通常版:インストール先)+12MB(システムドライブ:ランタイムライブラリを格納)+パッチ適用時の作業ディスクサイズ(注)

注)パッチ適用時の作業ディスクサイズは自動パッチ適用機能を使用する場合に必要です。

ー セキュリティパッチを適用する場合
更新プログラムの場合(Windows 10およびWindows 11以外):約200MB以上
累積更新プログラムの場合(Windows 10およびWindows 11):約6GB以上

ー サービスパックを適用する場合:約9GB

Live Help Clientを導入していない環境

・ 推奨CPUスペック

1GHz以上

・ 推奨メモリ容量

300MB以上(OSの使用量を含まず)

最小常駐使用メモリ

ー 通常時:32MB

ー ソフトウェア稼働状況収集時:300MB

ー コマンドモードCTは非常駐

・ 推奨ディスク容量

20MB以上(通常版:インストール先)+12MB(システムドライブ:ランタイムライブラリを格納)+パッチ適用時の作業ディスクサイズ(注)

8MB以上(コマンドモードCT版)

注)パッチ適用時の作業ディスクサイズは自動パッチ適用機能を使用する場合に必要です。

ー セキュリティパッチ(Hotfix)を適用する場合:20MB以上

ー サービスパックを適用する場合:約9GB

セキュア版CTを導入した環境

・ 推奨CPUスペック

1GHz以上

・ 推奨メモリ容量

370MB以上(OSの使用量を含まず)

最小常駐使用メモリ

ー 通常時:102MB

ー ソフトウェア稼働状況収集時:370MB

・ 推奨ディスク容量

210MB以上(通常版:インストール先)+12MB(システムドライブ:ランタイムライブラリを格納)+パッチ適用時の作業ディスクサイズ(注)

注)パッチ適用時の作業ディスクサイズは自動パッチ適用機能を使用する場合に必要です。

ー セキュリティパッチ(Hotfix)を適用する場合:20MB以上

ー サービスパックを適用する場合：約9GB

ADT

- 必要CPUスペック

  Pentium IV 1GHz以上

- 必要メモリ容量

  512MB以上（OSの使用量を含まず）

- 必要ディスク容量(注)

  5MB以上

  注) ファイルシステムは「NTFS（NT File System）」とする必要があります。

AT

- 対象機器

  富士通株式会社「MultiPad V2」(型番：FHT451SC1、FHT451SC2)(注)

  注) 販売を終了しているため、新規に購入してご利用いただくことはできません。

  注) MultiPadとPCを接続するMultiPad USBドライバが、Windows 10およびWindows 11に対応していません。そのため、接続するACには、Windows 10およびWindows 11を使用できません。

- 必要インストール容量

  1MB

- microSDカード(注)

  8MB以上

  注) microSDカードがなくても動作します。ただし、バックアップ電池がなくなるとデータが消えることがあるため、microSDカードの使用を推奨します。

PC稼働管理機能の管理対象PC

PC稼働管理機能を使用する場合は、稼働管理対象のPCとしてインテル vProまたはインテル Centrino Proに対応したPCが必要です。AMT 2.0 ～ AMT 15.0 を搭載しているPCをサポートします。

プリンタ（棚卸/資産情報確認/レポート出力用）

プリンタは、ACで設定して、ATで読み込むためのバーコードラベルを作成する場合や、資産情報をレポートとして印刷する場合に使用します。

使用するプリンタには、以下の性能が必要です。

- A4印刷が可能
- 白黒印刷が可能
- 600dpi以上の解像度

資産情報をレポートとして印刷する場合には、カラープリンタの利用を推奨します。

また、バーコードラベルの印刷では、以下の市販のプリンタラベルに対応しています。

- エーワン株式会社「マルチプリンタラベル 紙ラベル A4判 18面 角丸」
- エーワン株式会社「レーザープリンタラベル 紙ラベル A4判 18面四辺余白付 角丸 」
- コクヨ株式会社「カラーLBP&コピー用紙ラベル<リラベル>はかどり18面角丸20枚」

なお、プリンタラベルは、一片の大きさ（またはラベルサイズ）が、「63.5×46.5mm」のものを使用してください。

SS

- 必要CPUスペック

  インテル Xeon E5503(2GHz)以上

- 必要メモリ容量

  2.5GB以上(OSの使用量を含まず)

- 必要ディスク容量

  2GB以上

ディスク消去実行する管理対象PC

BIOSで実行している。または、UEFIで動作している場合、旧BIOS向け互換モードであるCSM機能を有効にする必要があります。

3.2 ソフトウェア

Systemwalker Desktop Patrolを使用するために必要な、ソフトウェア環境をコンポーネントごとに示します。

3.2.1 動作OS

それぞれのコンポーネントが動作可能なOSを以下に示します。

注意

本書で説明する日本語版Systemwalker Desktop Patrolは、日本語OSにのみインストールできます。

日本語以外のOSまたはランゲージパックには、インストールできません。

また、日本語OSであっても、以下の場合のSystemwalker Desktop Patrolの動作はサポート対象外となりますので、ご注意ください。

- 日本語および英語以外のアプリケーションまたはドライバがインストールされている場合
- 「地域と言語のオプション」画面の「Unicode対応でないプログラムの言語」に、日本語以外を設定されている場合

CS

- Microsoft Windows Server 2012 Standard（注1）
- Microsoft Windows Server 2012 Essentials（注1）
- Microsoft Windows Server 2012 Foundation（注1）
- Microsoft Windows Server 2012 Datacenter（注1）
- Microsoft Windows Server 2012 R2 Standard（注1）
- Microsoft Windows Server 2012 R2 Essentials（注1）
- Microsoft Windows Server 2012 R2 Foundation（注1）
- Microsoft Windows Server 2012 R2 Datacenter（注1）
- Microsoft Windows Server 2016 Datacenter（注1）（注2）
- Microsoft Windows Server 2016 Standard（注1）（注2）
- Microsoft Windows Server 2016 Essentials（注1）（注2）
- Microsoft Windows Server 2019 Datacenter（注1）（注2）
- Microsoft Windows Server 2019 Standard（注1）（注2）

- Microsoft Windows Server 2019 Essentials（注1）（注2）

注1）Server Coreは使用できません。

注2）Nano Serverは使用できません。

注意

WSUS連携機能やクイック実行形式のセキュリティパッチの配信/適用機能を使用する場合

各機能の使用時には、以下の前提条件があります。

- 使用可能なCS
  - Systemwalker Desktop Patrol 64ビット版のCSのみ
- 各サーバが動作するOS
  - Windows Server 2012
    KB3095113が適用済みであること
  - Windows Server 2012 R2
    KB3095113が適用済みであること
  - Windows Server 2016
  - Windows Server 2019
- 適用不可のCT
  - CTがWindows 10 HomeおよびWindows 11 Homeの場合は、WSUS連携のパッチ適用はできません。

DS

- Microsoft Windows Server 2012 Standard（注1）
- Microsoft Windows Server 2012 Essentials（注1）
- Microsoft Windows Server 2012 Foundation（注1）
- Microsoft Windows Server 2012 Datacenter（注1）
- Microsoft Windows Server 2012 R2 Standard（注1）
- Microsoft Windows Server 2012 R2 Essentials（注1）
- Microsoft Windows Server 2012 R2 Foundation（注1）
- Microsoft Windows Server 2012 R2 Datacenter（注1）
- Microsoft Windows Server 2016 Datacenter（注1）（注2）
- Microsoft Windows Server 2016 Standard（注1）（注2）
- Microsoft Windows Server 2016 Essentials（注1）（注2）
- Microsoft Windows Server 2019 Datacenter（注1）（注2）
- Microsoft Windows Server 2019 Standard（注1）（注2）
- Microsoft Windows Server 2019 Essentials（注1）（注2）

注1）Server Coreは使用できません。

注2）Nano Serverは使用できません。

注意

64ビットOSでの注意事項を以下に示します。

- Systemwalker Desktop Patrol DSは、32ビット互換モードで動作します。

注意

WSUS連携機能やクイック実行形式のセキュリティパッチの配信/適用機能を使用する場合

各機能の使用時には、以下の前提条件があります。

- 各サーバが動作するOS(CSと同等か、それ以下のOS)
  - Windows Server 2012
    KB3095113が適用済みであること
  - Windows Server 2012 R2
    KB3095113が適用済みであること
  - Windows Server 2016
  - Windows Server 2019

なお、前提条件に合わず、各サーバ機能を構築できない環境にDSを導入する場合は、CTが接続するサーバを変更してください。詳細は、“リファレンスマニュアル”の“CustomPolicy.exeコマンド”の“-cl.wsus.connectServer”や “-cl.c2r.connectServer”オプションを参照してください。

ポイント

DSは、クライアントOSでも動作可能です。

ただし、以下はサポート対象外です。

- Windouws 11上での動作
- WSUS連携機能

なお、クライアントOSの利用可能ユーザー(接続可能数)については、Microsoft社のライセンスを確認してください。

クライアントOSでDSを導入したい場合は、サポート窓口までご相談ください。

AC

- Windows 8.1
- Windows 8.1 Pro
- Windows 8.1 Enterprise
- Windows 8.1 64ビット版
- Windows 8.1 Pro 64ビット版
- Windows 8.1 Enterprise 64ビット版
- Windows 10 Home
- Windows 10 Pro(注1)
- Windows 10 Enterprise
- Windows 10 Education
- Windows 10 Home 64ビット版
- Windows 10 Pro 64ビット版(注1)
- Windows 10 Enterprise 64ビット版

- Windows 10 Education 64ビット版
- Windows 11 Home
- Windows 11 Pro（注2）
- Windows 11 Enterprise
- Windows 11 Education

注1）Windows 10 Pro for Workstationsにも対応しています。

注2）Windows 11 Pro for Workstationsにも対応しています。

注意

ATとの連携機能について

棚卸端末AT（MultiPad）を使用する場合、接続するACには、32ビット版OSしか使用できません。MultiPadとPCを接続するMultiPad USBドライバが、32ビット版のみ対応しているためです。

注意

64ビットOSでの注意事項を以下に示します。

- Systemwalker Desktop Patrol ACは、32ビット互換モードで動作します。

CT

- Microsoft Windows Server 2012 Standard（注1）
- Microsoft Windows Server 2012 Essentials（注1）
- Microsoft Windows Server 2012 Foundation（注1）
- Microsoft Windows Server 2012 Datacenter（注1）
- Microsoft Windows Server 2012 R2 Standard（注1）
- Microsoft Windows Server 2012 R2 Essentials（注1）
- Microsoft Windows Server 2012 R2 Foundation（注1）
- Microsoft Windows Server 2012 R2 Datacenter（注1）
- Microsoft Windows Server 2016 Datacenter（注1）（注2）
- Microsoft Windows Server 2016 Standard（注1）（注2）
- Microsoft Windows Server 2016 Essentials（注1）（注2）
- Microsoft Windows Server 2019 Datacenter（注1）（注2）
- Microsoft Windows Server 2019 Standard（注1）（注2）
- Microsoft Windows Server 2019 Essentials（注1）（注2）
- Windows 8.1
- Windows 8.1 Pro
- Windows 8.1 Enterprise
- Windows 8.1 64ビット版
- Windows 8.1 Pro 64ビット版
- Windows 8.1 Enterprise 64ビット版

- Windows 10 Home
- Windows 10 Pro（注3）
- Windows 10 Enterprise
- Windows 10 Education
- Windows 10 Home 64ビット版
- Windows 10 Pro 64ビット版（注3）
- Windows 10 Enterprise 64ビット版
- Windows 10 Education 64ビット版
- Windows 11 Home
- Windows 11 Pro（注4）
- Windows 11 Enterprise
- Windows 11 Education

注1）Server Coreは使用できません。

注2）Nano Serverは使用できません。

注3）Windows 10 Pro for Workstationsにも対応しています。

注4）Windows 11 Pro for Workstationsにも対応しています。

注意

64ビットOSでの注意事項を以下に示します。

- Systemwalker Desktop Patrol CTは、32ビット互換モードで動作します。

ADT

- Microsoft Windows Server 2012 Standard（注1）
- Microsoft Windows Server 2012 Essentials（注1）
- Microsoft Windows Server 2012 Foundation（注1）
- Microsoft Windows Server 2012 Datacenter（注1）
- Microsoft Windows Server 2012 R2 Standard（注1）
- Microsoft Windows Server 2012 R2 Essentials（注1）
- Microsoft Windows Server 2012 R2 Foundation（注1）
- Microsoft Windows Server 2012 R2 Datacenter（注1）
- Microsoft Windows Server 2016 Datacenter（注1）（注2）
- Microsoft Windows Server 2016 Standard（注1）（注2）
- Microsoft Windows Server 2016 Essentials（注1）（注2）
- Microsoft Windows Server 2019 Datacenter（注1）（注2）
- Microsoft Windows Server 2019 Standard（注1）（注2）
- Microsoft Windows Server 2019 Essentials（注1）（注2）
- Windows 8.1
- Windows 8.1 Pro

- Windows 8.1 Enterprise
- Windows 8.1 64ビット版
- Windows 8.1 Pro 64ビット版
- Windows 8.1 Enterprise 64ビット版
- Windows 10 Home
- Windows 10 Pro（注3）
- Windows 10 Enterprise
- Windows 10 Education
- Windows 10 Home 64ビット版
- Windows 10 Pro 64ビット版（注3）
- Windows 10 Enterprise 64ビット版
- Windows 10 Education 64ビット版
- Windows 11 Home
- Windows 11 Pro（注4）
- Windows 11 Enterprise
- Windows 11 Education

注1）Server Coreは使用できません。

注2）Nano Serverは使用できません。

注3）Windows 10 Pro for Workstationsにも対応しています。

注4）Windows 11 Pro for Workstationsにも対応しています。

注意

64ビットOSでの注意事項を以下に示します。

- Systemwalker Desktop Patrol ADTは、32ビット互換モードで動作します。

AT

- Microsoft Windows CE 6.0

  Systemwalker Desktop Patrol ATを使用して、棚卸作業や資産情報の確認をする場合に必要です。

SS

- Microsoft Windows Server 2012 Standard（注1）
- Microsoft Windows Server 2012 Essentials（注1）
- Microsoft Windows Server 2012 Foundation（注1）
- Microsoft Windows Server 2012 Datacenter（注1）
- Microsoft Windows Server 2012 R2 Standard（注1）
- Microsoft Windows Server 2012 R2 Essentials（注1）
- Microsoft Windows Server 2012 R2 Foundation（注1）
- Microsoft Windows Server 2012 R2 Datacenter（注1）
- Microsoft Windows Server 2016 Datacenter（注1）（注2）

- Microsoft Windows Server 2016 Standard（注1）（注2）
- Microsoft Windows Server 2016 Essentials（注1）（注2）
- Microsoft Windows Server 2019 Datacenter（注1）（注2）
- Microsoft Windows Server 2019 Standard（注1）（注2）
- Microsoft Windows Server 2019 Essentials（注1）（注2）

注1）Server Coreは使用できません。

注2）Nano Serverは使用できません。

注意

64ビットOSでの注意事項を以下に示します。

- Systemwalker Desktop Patrol SSは、32ビット互換モードで動作します。

3.2.2 必要なソフトウェア

Systemwalker Desktop Patrolが機能するために必要なソフトウェアを以下に示します。

必須ソフトウェア

【CS】

CSを導入するサーバには以下のソフトウェアが必要です。

― **Webサーバ**

以下のどれか1つが必要です。

- Internet Information Services 8.0
- Internet Information Services 8.5
- Internet Information Services 10.0

CSVファイルを参照・編集する場合には、Systemwalker Desktop Patrolで入出力するファイルのエンコード形式に対応したエディタ、ソフトウェアが必要です。
入出力するファイルのエンコード形式については、“リファレンスマニュアル”の“SWDTP_config.exe(各種設定変更)”を参照してください。

Desktop Patrol 64ビット版のCSを導入するサーバには、以下のソフトウェアが必要です。

― **WSUS**

WSUS連携する場合は、以下のソフトウェアが必要です。OSに合わせて、以下のどれか1つが必要です。

- Windows Server 2012 WSUS
- Windows Server 2012 R2 WSUS
- Windows Server 2016 WSUS
- Windows Server 2019 WSUS

Desktop Patrol 64ビット版、かつ以下のOSの時にWSUSがインストールされていなかった場合、CSインストール時にWSUSを合わせてインストールします。

― Windows Server 2012

― Windows Server 2012 R2

― Windows Server 2016

― Windows Server 2019

IISがインストールされていなかった場合、CSインストール時にIISを合わせてインストールします。

【DS】

・ DSを導入するサーバには、以下のソフトウェアが必要です。

― **WSUS**

WSUS連携する場合は、以下のソフトウェアが必要です。OSに合わせて、以下のどれか1つが必要です。

- Windows Server 2012 WSUS
- Windows Server 2012 R2 WSUS
- Windows Server 2016 WSUS
- Windows Server 2019 WSUS

・ DSでWSUSがインストールされていなかった場合、DSインストール時にIISおよびWSUSを合わせてインストールします。

・ OSがWindows Server 2012以降の場合、DSインストール時にIISを合わせてインストールします。

【AC】

ACを導入するPCには以下のソフトウェアが必要です。

― **Microsoft Excel**

以下のどれか1つの製品が必要です。

- Microsoft Office Personal 2013（注1）
- Microsoft Office Home and Business 2013（注1）
- Microsoft Office Professional 2013（注1）
- Microsoft Office Personal 2016（注2）
- Microsoft Office Home and Business 2016（注2）
- Microsoft Office Professional 2016（注2）
- Microsoft Office Personal 2019（注3）
- Microsoft Office Home and Business 2019（注3）
- Microsoft Office Professional 2019（注3）
- Microsoft Office Professional Plus 2019（注3）
- Microsoft Office Standard 2019（注3）
- Microsoft 365 Apps for enterprise(旧Office 365 ProPlus)（注4）
- Microsoft 365 Apps for business(旧Office 365 Business)（注4）
- Microsoft Excel 2013
- Microsoft Excel 2016
- Microsoft Excel 2019
- Excel for Microsoft 365 Apps(旧Office 365)

注1）Microsoft Excel 2013(32ビット版)が必須です。

注2）Microsoft Excel 2016(32ビット版)が必須です。

注3）Microsoft Excel 2019が必須です。

注4）Excel for Microsoft 365 Apps(旧Office 365)が必須です。

ロケーションマップ機能を使用する場合には以下のソフトウェアが必要です。

－ **Microsoft Visio**

以下のどれか1つの製品が必要です。

- Microsoft Visio Standard 2013（注1）
- Microsoft Visio Professional 2013（注1）
- Microsoft Visio Standard 2016（注2）
- Microsoft Visio Professional 2016（注2）
- Microsoft Visio Standard 2019
- Microsoft Visio Professional 2019
- Visio Pro for Microsoft 365 Apps(旧Office 365)

注1）Microsoft Visio 2013(32ビット版)が必須です。

注2）Microsoft Visio 2016(32ビット版)が必須です。

【CT】

ディスク消去用CDを使用してディスク消去PCのハードディスクを消去する場合、ブータブルCDの作成が可能なCDライティングソフトウェアとして以下のソフトウェアが必要です。

－ **CDライティングソフトウェア**

例：Roxio Easy Media Creator

【ADT】

ADTを導入するPCに必要なソフトウェアはありません。

【AT】

ATを使用して、棚卸作業や資産情報の確認をする場合に、ACへ以下のソフトウェアのインストールが必要です。

－ Microsoft ActiveSync 4.0、4.2または4.5

－ Windows Mobile デバイスセンター 6.1

注)「MultiPad V2」は販売を終了しているため、新規に「MultiPad V2」を購入してご利用いただくことはできません。

【SS】

SSを導入するPCに必要なソフトウェアはありません。

【Webブラウザ】

Internet ExplorerおよびMicrosoft Edgeが使用できます。

Internet Explorerは、以下のバージョンを利用することを推奨します。

－ Windows Internet Explorer 11

注意

－ WindowsストアアプリのInternet Explorerはサポートしていません。

－ 新しいMicrosoft Edge(バージョン79以降)を使用してメインメニューを開いた場合、一部の画面でツリー表示と一覧表示の境界線を動かしての画面サイズ変更ができません 。

【クイック実行形式のOffice】

クイック実行形式のセキュリティパッチの配信/適用の対象となるクイック実行形式のOfficeは、以下のとおりです。

- Microsoft Office Professional 2019
- Microsoft Office Home and Business 2019
- Microsoft Office Personal 2019
- Microsoft Office Professional Plus 2019
- Microsoft Office Standard 2019
- Microsoft 365 Apps for enterprise(旧Office 365 ProPlus)
- Microsoft 365 Apps for business(旧Office 365 Business)

クイック実行形式のセキュリティパッチの配信/適用機能の利用時、以下の前提条件があります。

- 64ビット版のみサポートします。
- WindowsストアアプリのOfficeはサポートしていません。

関連ソフトウェア

仮想OS運用で使用できるソフトウェア

【CS/DS】

- VMware vSphere 6.0～7.0
- Microsoft Hyper-V
- KVM

【CT/AC/ADT】

- VMware vSphere 6.0～7.0
- VMware Horizon 7.11～7.13、8 2006～2016
- Citrix XenDesktop 7.15
- Citrix Virtual Apps and Desktops 1912 LTSR ,2003～2103
- Microsoft Hyper-V

メールソフト

システムアカウントユーザーまたは、部門管理アカウントユーザーで、アラーム通知によりメールを受信する場合に必要です。

Microsoft Outlook Express

Microsoft Outlook など

3.2.3 混在運用できない製品

共存できない製品

Systemwalker Desktop Patrolと以下の製品との共存はできません。

- Systemwalker IT BudgetMGR

・ FUJITSU ビジネスアプリケーション 瞬快

CSと共存できない製品

CSを導入する場合、以下の製品との共存はできません。

・ Systemwalker Desktop Keeper V15.0.0以降の管理サーバ・統合管理サーバ（注1）

・ Systemwalker Centric Manager V15.0.0以降の運用管理サーバ（注2）

・ Systemwalker Centric Manager V15.0.0以降の資産管理サーバ（注3）

・ Windows Server Update Services(WSUS)機能（注4）

注1）共存できない条件

以下の組み合わせは共存できません。

－ Windows(32bit)版 Systemwalker Desktop KeeperとWindows(64bit)版 Systemwalker Desktop Patrol

－ Windows(64bit)版 Systemwalker Desktop KeeperとWindows(32bit)版 Systemwalker Desktop Patrol

注2）共存できない条件

Systemwalker Centric Manager 運用管理サーバの「資産管理機能」をインストールしている場合は、以下の組み合わせは共存できません。

－ Windows(32bit)版 Systemwalker Centric ManagerとWindows(64bit)版 Systemwalker Desktop Patrol

－ Windows(64bit)版 Systemwalker Centric ManagerとWindows(32bit)版 Systemwalker Desktop Patrol

注3）共存できない条件

以下の組み合わせは共存できません。

－ Windows(32bit)版 Systemwalker Centric ManagerとWindows(64bit)版 Systemwalker Desktop Patrol

－ Windows(64bit)版 Systemwalker Centric ManagerとWindows(32bit)版 Systemwalker Desktop Patrol

注4）共存できる条件

Systemwalker Desktop Patrol CSのOSが、x64 Editionの場合は共存できます。

SSと共存できない製品

SSを導入する場合、CSを導入する場合に共存できない製品と同様の製品との共存ができません。

3.3 バージョンレベル混在運用について

Systemwalker Desktop Patrolの各コンポーネントで、バージョンレベルが異なる場合について説明します。

CT/ADTの場合

接続先サーバのバージョンレベルと異なるバージョンレベルでも接続可能です。

ただし、接続先サーバのバージョンレベルによって以下の制限があります。

・ 接続先サーバの方が古いバージョンの場合は、接続できません。

・ 接続先サーバの方が新しいバージョンの場合は、古いバージョンレベルの機能までしか使用できません。

CS/DS/SS/AC/ATの場合

すべて同じバージョンレベルで使用してください。

第4章 他製品との連携

他製品と組み合わせることで、より効果的な資産管理運用を行えます。

4.1 連携製品およびサービス一覧

Systemwalker Desktop Patrolと連携できる製品およびサービスを以下に示します。

種別	製品/サービス名	機能概要
自社製品	Systemwalker Desktop Keeper V13以降	・ Systemwalker Desktop Patrolの構成情報を移出し、Systemwalker Desktop Keeper側で、構成情報として移入できます。Systemwalker Desktop Patrol、Systemwalker Desktop Keeper共にV14.2.0以降の場合、Systemwalker Desktop PatrolからSystemwalker Desktop Keeperへの構成情報の取り込みは、自動で行われます。 ・ Systemwalker Desktop Keeperのポリシー設定状況をクライアントから収集し表示します。 ・ Systemwalker Desktop KeeperがV14.1.0以降の場合、Systemwalker Desktop Keeperの運用状況を状況画面に表示します。
	Systemwalker Desktop Inspection V13	・ Systemwalker Desktop Patrolが収集したインベントリ情報を利用して通信を許可するMACアドレスの一覧としてSystemwalker Desktop Inspection に移入することができます。 ・ Systemwalker Desktop Inspectionによって検疫ネットワークを構成する場合、セキュリティパッチ未適用の理由から検疫エラーとなったPCに対して、Systemwalker Desktop Patrolによってパッチ適用を行えます。
	Systemwalker Centric Manager V13以降	・ Systemwalker Centric Manager 運用管理サーバのデータベースに蓄積されたインベントリ情報をSystemwalker Desktop Patrolのデータベースに取込むことができます。 ・ Systemwalker Desktop PatrolのイベントログをSystemwalker Centric Managerの監視画面に表示し、Systemwalker Centric Managerで監視できます。
自社サービス	仮想デスクトップサービス FJDaaS-V	Systemwalker Desktop Patrolを仮想デスクトップサービス FJDaaS-Vのスタティックデスクトップ環境に導入できます。
他社製品	・ LanScope Cat6以降 ・ QAW ・ JP1	他製品のインベントリ情報(機器情報のみ)を資産管理台帳に取り込み、他製品で収集した機器をSystemwalker Desktop Patrolで管理できます。
CSV(テキストファイル)連携	CSVデータ連携インターフェース	上記以外の製品との連携のために、標準的なインターフェースとしてCSV形式ファイルでの連携を行うことができます。連携相手製品側の機能で出力したインベントリ情報のCSV形式ファイルを、本製品の連携用CSVファイルフォーマットに編集して、Systemwalker Desktop Patrolのデータベースに取込むことができます。

4.2 イベント連携

イベント連携とは、Systemwalker Desktop PatrolのイベントログをSystemwalker Centric Managerの監視画面に表示し、監視することです。

Systemwalker Desktop Patrolは、以下のイベント連携の運用を行えます。

・ アラーム通知によるイベント連携

・ イベントログ出力によるイベント連携

イベント連携が可能なSystemwalker Centric Managerのバージョンと、Systemwalker Desktop Patrolのアラームが表示される監視画面を以下の表に示します。

製品名	監視画面
Systemwalker CentricMGR SE/EE V10.0L20以降	Systemwalkerコンソール

アラーム通知によるイベント連携

Systemwalker Desktop Patrolのアラーム通知機能を使用し、Systemwalker Centric Managerの監視画面に、ライセンス違反やセキュリティパッチ未適用などのアラームを表示できます。

イベントログ出力によるイベント連携

Systemwalker Desktop Patrolで発生したイベントをイベントログに出力することにより、Systemwalker Centric Managerの監視画面に、CSまたはDSのイベントを表示できます。

以下の事象が発生した場合に、イベントログを出力します。

区分	説明
情報	・ サービスの起動と停止 ・ Systemwalkerサポートセンターからのソフトウェア辞書のダウンロードと適用 ・ Microsoft社の公開サイトからのセキュリティパッチのダウンロード
警告	自動リカバリや継続動作しても問題がない軽微なトラブルが発生した場合
エラー	CS,DSに、運用に影響のある異常が発生した場合

4.3 インベントリ情報の収集

Systemwalker Desktop Patrolでは、他製品の機能でインベントリ情報を収集できます。

インベントリ情報の収集として、以下の方法があります。

・ Systemwalker Centric Managerの機能を使用してインベントリ情報を収集する

・ CSV（テキストファイル）連携によってインベントリ情報を収集する

収集可能なインベントリ情報は以下のとおりです。

収集情報	収集方法		
	Centric Manager連携		CSV連携
	Windows	UNIX	
ハードウェア情報	○	○	○
ソフトウェア情報－ファイル検索	○	×	○
ソフトウェア情報－レジストリ検索（プログラム名の検索）	○	×	○
ソフトウェア情報－レジストリ検索（任意のキーと値の検索）	×	×	○
ユーザー情報	○（注）	○（注）	○
ソフトウェア稼働状況	×	×	○
レジストリ情報	×	×	×

収集情報	収集方法		
	Centric Manager連携		CSV連携
	Windows	UNIX	
EXE情報	×	×	×

○:収集可能 ×:収集不可

注)インストールレス型エージェント監視機能によるインベントリ収集を行っている場合は、収集できません。

Systemwalker Centric Managerの機能を使用してインベントリ情報を収集する

Systemwalker Centric Managerの機能で収集したインベントリ情報を、Systemwalker Desktop Patrolに取り込むことができます。これにより、UNIXなどのSystemwalker Desktop Patrolがサポートしないosのインベントリ情報についても、Systemwalker Desktop Patrolによる資産管理の対象にできます。

設定方法については、“運用ガイド 管理者編”を参照してください。

インベントリ収集の連携が可能なSystemwalker Centric Managerのバージョンを、以下の表に示します。

製品名	備考
Systemwalker Centric Manager V13.0.0以降	運用管理サーバまたは部門管理サーバと連携できます(注)。

注)

インストールレス型エージェント監視機能によるインベントリ収集を行っている場合は、運用管理サーバのみ連携できます。Centric Managerと同居する場合は運用管理サーバと同居できます。Centric Managerと同居しない場合は運用管理サーバからインベントリ情報を取り込みます。

CSV(テキストファイル)連携によってインベントリ情報を収集する

Systemwalker Desktop Patrolで規定されているCSVフォーマットに従って記入したインベントリ情報を取り込むことができます。

記入形式、および使用方法については、“運用ガイド 管理者編”を参照してください。

4.4 構成情報

Systemwalker Desktop Patrolでは、部門に基づく構成情報(ツリー構造)でPCを管理しています。この構成情報をSystemwalker Desktop Keeperが持つ構成情報と連携することにより、導入作業を省力化できます。

構成情報の連携が可能なSystemwalker Desktop Keeperのバージョンを、以下に示します。

- Systemwalker Desktop Keeper V13.0.0以降

なお、Active Directoryと連携した運用を行う場合は、本機能を利用できません。

Systemwalker Desktop Keeperの構成情報を移入する

Systemwalker Desktop Keeperで管理している構成情報(管理サーバおよび論理グループに基づく構成情報)をSystemwalker Desktop Keeperの機能により移出(CSV出力)し、Systemwalker Desktop Patrolの部門に基づく構成情報に移入できます。

使用方法については、“運用ガイド 管理者編”を参照してください。

Systemwalker Desktop Keeperに構成情報を移出する

Systemwalker Desktop Patrolで管理している構成情報(部門に基づく構成情報)をSystemwalker Desktop Patrolの機能により移出(CSV出力)し、Systemwalker Desktop keeperの管理サーバおよび論理グループに基づく構成情報に、Systemwalker Desktop Keeper側の機能で移入できます。

使用方法については、“運用ガイド 管理者編”を参照してください。

なお、Systemwalker Desktop Patrol、Systemwalker Desktop Keeper共にV14.2.0以降の場合、Systemwalker Desktop PatrolからSystemwalker Desktop Keeperへの構成情報の取り込みは、自動で行われます。

4.5 セキュリティ監査

Systemwalker Desktop Patrolでは、他製品で設定したセキュリティ設定情報をインベントリ情報として収集し、セキュリティ情報として監査できます。

セキュリティ監査が可能な他製品のバージョンを以下に示します。

- Systemwalker Desktop Keeper V13.0.0以降
- Systemwalker Desktop Encryption V13.0.0

Systemwalker Desktop Keeperのセキュリティ設定情報を監査する

クライアントにおけるSystemwalker Desktop Keeperのセキュリティ設定状況を監査できます。

Systemwalker Desktop Encryptionのセキュリティ設定情報を監査する

クライアントにおけるSystemwalker Desktop Encryptionのセキュリティ設定状況を監査できます。

4.6 MACアドレス連携

Systemwalker Desktop Patrolから、Systemwalker Desktop Inspectionに対してMACアドレス認証に用いる情報を移出できます。

Systemwalker Desktop Patrolのインベントリ情報の1つであるMACアドレスを移出することで、Systemwalker Desktop Inspectionの管理者の設定工数を省力化できます。

MACアドレス連携が可能なSystemwalker Desktop Inspectionのバージョンを、以下に示します。

- Systemwalker Desktop Inspection V13.0.0以降

4.7 検疫ネットワークとの連携

Systemwalker Desktop Inspectionによって検疫ネットワークを構成する場合、セキュリティパッチ未適用の理由から検疫エラーとなったPCに対して、Systemwalker Desktop Patrolによってパッチ適用を行えます。

検疫ネットワークにおいて、検疫エラーとなったPCのセキュリティレベルを自動更新する運用が行え、検疫エラー後のユーザーの対応負荷を軽減できると共に、システムのセキュリティ向上を図ることができます。

パッチ適用の連携が可能なSystemwalker Desktop Inspectionのバージョンを、以下に示します。

- Systemwalker Desktop Inspection V13.2.0以降

本連携でパッチ適用の対象となるのは、Systemwalker Desktop Patrolのソフトウェア辞書に定義された以下のパッチです。

- Microsoft Windows OS系の自動適用パッチ
- Microsoft製品の自動適用パッチ（適用条件あり、下記注意事項を参照）

注意

Microsoft製品の自動適用パッチの適用条件について

Microsoft製品の自動適用パッチの適用条件は、Windows OSがインストールされたドライブと同じドライブの“¥Program Files”配下に、Microsoft OfficeまたはMicrosoft 365がインストールされている場合のみです。

参照

検疫ネットワーク連携でのパッチ適用の方法については、“Systemwalker Desktop Inspection ユーザーズガイド”のマニュアルを参照してください。

4.8 他製品からの資産管理台帳の作成

他製品のインベントリ情報（機器情報のみ）を資産管理台帳に取り込み、他製品で収集した機器をSystemwalker Desktop Patrolで管理できます。

以下の製品のインベントリ情報を取り込むことができます。

- LanScope Cat6以降
- QAW
- JP1

用語集

AC

Systemwalker Desktop Patrol Asset Consoleの略称です。

システム管理者や部門管理者は、ACを起動してレポート出力や、資産情報の登録/変更の操作を行います。

ADT

Systemwalker Desktop Patrol Auto Detection Terminalの略称です。

セグメント毎に設置し、同一セグメント内のネットワークに接続されている機器を自動検知します。また、検知した機器の情報を、CSに通知します。

AT

Systemwalker Desktop Patrol Asset Terminalの略称です。

Systemwalker Desktop Patrolで作成したバーコードを読み込むことができる端末です。

CLEARSURE

コンピュータの盗難、紛失時にコンピュータのロック、ハードディスクのデータ消去または位置情報取得を行うことにより、情報漏えいのリスクを軽減する富士通のソリューションです。

なお、「CLEARSURE 3G/LTE」は対象外となります。

CS

Systemwalker Desktop Patrol CS（Corporate Server）の略称です。

CS操作ログ

CSに対して、以下の画面から行った操作のログ(定義変更、登録、削除)およびログイン/ログアウトのログのことです。

- メインメニュー
- ダウンロードメニュー

CT

Systemwalker Desktop Patrol CT（Client Terminal）の略称です。

CT稼働状況ログ

CTの稼働状況はログとしてCSに保存されます。管理者は、CT稼働状況ログによりCTの以下の稼働状況を確認できます。

- Systemwalker Desktop Patrolの稼働記録
  - Systemwalker Desktop Patrolサービス起動/停止
  - ポリシー受信
  - インベントリ収集
  - パッチ適用
  - ソフトウェア配信
  - アップデータ適用
- Windowsの稼働記録
  - Windowsへのログオン/ログオフ
  - Windowsのサスペンド状態/サスペンド復帰
  - バッテリ運用/AC運用

ー LAN接続有効/無効

Desktop Encryption情報

セキュリティ対策ソフトウェアであるSystemwalker Desktop Encryptionの導入状況および設定状況を、Systemwalker Desktop Encryptionが導入されているPCからセキュリティ情報として収集できます。

Desktop Keeper情報

セキュリティ対策ソフトウェアであるSystemwalker Desktop Keeperの導入状況および設定状況を、Systemwalker Desktop Keeperが導入されているPCからセキュリティ情報として収集できます。

DS

Systemwalker Desktop Patrol DS（Domain Server）の略称です。

DS単位

上位サーバの配下に配置されたCTを1つの管理単位とし、この管理単位ごとにクライアントポリシーの適用を行う運用です。

ハードウェア処理性能、回線速度など物理的な負荷分散を考慮してDSが設置されるため、このDSが設置される単位をDS単位と呼びます。

EXE情報

PCに存在する実行ファイル（拡張子が.exeのファイル)のプロパティ情報です。インベントリ収集により、CT上の実行ファイルのプロパティ情報が参照できます。

ICMP

Internet Control Message Protocolの略称で、TCP/IPで接続されたPCやネットワークの状態を、メッセージとして伝送するために使われるプロトコルです。

IPアドレス

IPv4アドレスとIPv6アドレスの総称です。

IPv6アドレスの種類

グローバルユニキャストアドレス、ユニークローカルアドレス、リンクローカルアドレス、マルチキャストアドレス、その他のアドレスに大別されるIPv6アドレスのビットに応じた分類を指します。

Live Help Client

支援を必要とするクライアントユーザーのPCや、リモート操作で運用するサーバに導入します。クライアント側は、「画面上のメッセージに対して、どう応えたらいいのかわからない」や、「アプリケーションの操作方法がわからない」などの場合に、「Live Help Expert」からの遠隔操作によって、支援を受けることができます。

Live Help Expert

「Live Help Client」をリモート操作するためのソフトウェアです。クライアントユーザーが、PCの操作に困っている場合などで、直接クライアントユーザーのPCに接続して、支援できます。

Office展開ツール (ODT)

Microsoft社が公開している、Office Deployment Tool(ODT) です。本書では、コマンドを指します。

Office配信サーバ

CSがインターネットに接続できない環境の場合、インターネットに接続できる環境にOffice Content Delivery Networkから更新プログラムを取得し、CSに更新プログラムを配信するサーバを指します。

PC情報

インベントリ情報、ユーザー情報を各PCから収集し、データベースに登録してCSで一元管理する機能です。

運用中資産のハードウェアの状況、ソフトウェアの導入状況、および、ソフトウェアの稼働状況を管理できます。

RA

IPv6アドレスの自動構成で用いられる手法の一つです。ルータ広告(Router Advertisement)の略称です。定期的にネットワーク内にルータのIPv6アドレスと利用可能なネットワークプレフィックスを通知します。通知するネットワークプレフィックスは、グローバルユニキャストアドレス、ユニークローカルアドレスのどちらであっても構いません。

SAMAC

一般社団法人 ソフトウェア資産管理評価認定協会(SAMAC)は、ソフトウェア資産管理の正しい普及促進を目的とした、非営利型一般社団法人です。

SNMP

Simple Network Management Protocolの略称で、サーバやネットワーク機器といった、TCP/IPで接続された機器をネットワーク越しに監視するための通信プロトコルです。

SS

Systemwalker Desktop Patrol SS（Secure server[ゲートウェイサーバ]）の略称です。

Systemwalkerサポートセンター

富士通が運営するシステムサポートセンターです。「ソフトウェア辞書」の配信や、それに伴う情報提供、Systemwalker Desktop Patrolの質問に対する回答を行っています。

Systemwalker Desktop Inspection

Systemwalker Desktop Inspectionは、クライアントの検疫結果に応じてネットワーク機器を制御し、検疫ネットワークを実現するソフトウェアです。

Systemwalker Desktop Keeper

Systemwalker Desktop Keeperは、「記録」、「禁止」、「管理」、「ログ分析」、および「レポート出力」を柱とした、内部情報漏洩対策ソフトウェアです。

Systemwalker Desktop Patrol CS（Corporate Server）

ソフトウェア配信の運用ポリシーやインベントリ情報の収集ポリシーを定義し、各PCに配信するサービスを受け持つサーバです。

ICT資産の情報(ICTリポジトリ)、人、部門などの部門情報を格納したデータベースにより、セキュリティパッチ配信、セキュリティ監査やライセンス管理をWebブラウザから行うサービスを提供します。通常は企業に1台導入されます。

「Desktop Patrol CS」、または「CS」と略す場合があります。

Systemwalker Desktop Patrol CT（Client Terminal）

インベントリ収集により資産を管理するPCに導入します。CTで配信ソフトウェアのダウンロード、セキュリティパッチの受信を行います。

「Desktop Patrol CT」、または「CT」と略す場合があります。

Systemwalker Desktop Patrol DS（Domain Server）

運用ポリシー、インベントリ情報、配信ソフトウェアなどの集配信の中継／格納をサービスするサーバです。

負荷分散するためなどの目的のために設置します。クライアントが遠隔地にあり、低速回線の場合、または配信するコンテンツの容量が大きい場合などに有効です。

「Desktop Patrol DS」、または「DS」と略す場合があります。

Systemwalker Desktop Patrol SS（Secure server[ゲートウェイサーバ]）

セキュア版CTの接続を受け付けるための中継サーバです。

セキュア版CTを管理する場合に、導入が必要なサーバです。

「SS」と略す場合があります。

Systemwalker Desktop Rights Master

Systemwalker Desktop Rights Masterは、機密情報、個人情報などが含まれるファイルを暗号化することで保護します。次に、ファイルにアクセス許可を設定することで、ファイルへの操作を制限して、情報の外部漏洩を防ぐソフトウェアです。

UNC（Universal Naming Convention）

Windowsのネットワーク環境上で、ネットワーク上にある資源を示すための表記法です。

アップストリームサーバ

WSUS連携を行う際に、Microsoft Updateと同期するWSUSサーバです。

アップデータ

CSからDS/CTに配信する修正モジュールです。管理者がメインメニューで適用処理をすると自動的にモジュールが最新のものになります。

アップデータ機能

DSおよびCTの修正を、簡易な操作でお客さまのシステムに修正適用できる機能です。

DSおよびCTの修正をCSに登録することで、自動的に適用できます。適用は自動的に行われるため、DSおよびCTのマシンで管理者が適用操作を行う必要はありません。

一時アドレス（匿名アドレス）

ステートレス自動構成(RA)を用いている時にノードに割り当てられる送信用のアドレスです。一定時間ごとに変更されます。詳細はRFC 3041を参照してください。

一括対処

省電力/セキュリティ設定の違反項目に対し、PCのユーザーによる画面操作により、設定の自動変更を行います。

インベントリ収集機能

CTで収集されたインベントリ情報を、CSまたはDSに送付する機能です。

インベントリ情報

PCの実態を管理する上で必要となる情報です。CPUやディスク容量などのハードウェアに関する情報、インストールされているソフトウェア製品名などのソフトウェア製品に関する情報、およびウイルス対策ソフトウェアのパターンファイルの版数管理、セキュリティパッチの適用状況などのセキュリティに関する情報に分類されます。

運用設定の診断結果画面

PCの省電力設定およびセキュリティ設定の診断結果を表示する画面です。

PCのユーザーはこの画面から診断結果を確認し、必要な設定変更を行います。

エージェントモード

CTをパソコンにインストールすることにより、自動的に最新の情報を収集し、ICT資産のデータベースを構築するモードです。

回復パスワード(数字パスワード)

TPMやUSBメモリの故障など、他のすべてのキーを紛失した場合やシステムに問題が生じた場合などに備えて用意しておく、ロックを解除するための10進数で表される48桁の数値列です。印刷、またはテキストファイルにしてUSBメモリなどに保存することができます。なお、この数字パスワードのことを画面上では「回復キー」と表示している部分があります。

書き込み保護

Windows 10およびWindows 11のPCにおいて、以下の項目が有効化されている状態を示します。

1. Windows 10およびWindows 11の[プログラムと機能]-[Windowsの機能の有効化または無効化]-[統合書き込みフィルター]機能がインストールされていること。
2. [統合書込みフィルター]機能の[フィルターの状態]が有効化（オン）されていること。

カスタムインストール

インストール時に設定する値をデフォルト値以外に設定可能なインストールです。

簡易操作ログファイル収集

CTがインストールされたPCで、ユーザーが行った操作をログとして保存し、そのログファイルを収集する機能です。

環境設定

「Systemwalker Desktop Patrol」の運用設定を行う機能です。

ユーザー管理、部門管理、ポリシーグループ設定、および「Systemwalker Desktop Keeper」間で構成情報を相互に利用するための環境設定を行います。

監査結果の保有期間

セキュリティ監査レポートの結果を保存しておく期間です。セキュリティ監査レポートの出力時に以前の結果情報として比較して判断できるように、3ヶ月、6ヶ月、1年のどれかを選択します。

監査指針

セキュリティ監査として、何がセキュリティ対策として設定されていれば問題なしとするかの評価基準を設定した定義です。

監査スケジュール

セキュリティ監査を実施する契機です。毎月の特定日と開始時間を設定します。

管理対象

システム管理者は未配置を含むすべての部門の参照および設定ができます。また、部門管理者およびユーザーは、操作者自身が所属する部門の参照および設定（部門管理者のみ）ができます。

このように各ユーザーが、参照および設定などの管理する部門の範囲を「管理対象」と呼びます。

メインメニューにログインした各ユーザーは、各機能画面の部門ツリーにおいて、管理対象から参照・設定対象となる部門を選択します。

機器

Systemwalker Desktop Patrolの管理台帳機能で管理するPCや什器です。

機器情報

管理台帳機能で管理する機器のモデル名、メーカー名、資産区分など、機器に関する情報です。

クイック実行形式

Officeをインストールする際の実行形式であり、Click to Run(C2R)を指します。

組み合わせ条件

複数のソフトウェアの定義を結合して、1つの辞書コードとして登録できます。この組み合わせにより、詳細なライセンス管理を行えます。

クライアントポリシー

CTの動作情報（ポリシー）を定義したものです。

グローバルユニキャストアドレス

2000::/3で定義されるIPv6アドレスです。GUAと略されることがあります。

契約情報

管理台帳機能で管理する機器の契約分類、契約会社、契約日など、契約に関する情報です。

コマンドモードCT

コマンド実行により、PC上のインベントリ情報をファイルに出力する機能です。ネットワークから切り離されたパソコンや回線速度の遅いネットワークなどでインベントリ収集を行う場合に使用します。

固有情報

機器に任意に設定できる情報です。

サポートセンター定義

「ソフトウェア辞書」にあらかじめ登録されているソフトウェアの検出条件です。代表的なソフトウェア、Microsoft社のセキュリティパッチ、ウイルス対策ソフトウェアのウイルス定義ファイルなどが登録されています。

資産情報

管理台帳機能で管理する機器情報や契約情報です。

辞書コード

ソフトウェアのバージョン、レベル、エディションなどの細かい製品単位や、それらをまとめた単位で、コードが割り当てられます。

サポートセンター定義、ユーザー定義の一要素です。

システムアカウント

メインメニューのすべてのメニュー項目について、設定および参照できる権限です。

システムセキュリティ

システムのセキュリティ情報として、BIOSの設定状況およびシステムのログオン状況を、各PCから収集できます。

自動対処

管理者は、省電力およびセキュリティ設定状況の監査項目に対して自動対処を指定できます。

省電力/セキュリティ設定の違反項目に対し、PCのユーザーの操作を必要とせずに自動で設定の変更を行います。

什器

CTをインストールできない機器（プリンタ、HUBなど）や、机や椅子などの設備を示します。

収集タイミング

インベントリ収集のタイミングを指定します。「時刻指定」、「電源投入時」、「ログオン時」が指定可能です。ただし、このタイミングで収集されるのは、CT上の前回収集時と差分があった場合です。最新の情報をインベントリ収集したい場合は、CTで、[スタート]-[プログラム]-[Systemwalker Desktop Patrol CT]-[インベントリ収集]、または[アプリ]-[Systemwalker Desktop Patrol CT]-[インベントリ収集]を選択するか、または「管理者」がメインメニューで再収集を指示することで再収集できます。

収集単位

CTのインベントリ収集の単位で、「毎週」、「毎日」、「収集しない」を選択可能です。

状況画面

メインメニューのトップ画面として、Systemwalker Desktop Patrolの運用状況を一覧表示する画面です。

この画面で、全体の状況が短時間で把握でき、状況に応じた対処を容易に行えます。

ステータスアイコン

状況画面の棒グラフ表示の左上に表示される、問題PCの比率を示すアイコンです。

製品情報

「プログラムと機能」にある「プログラムのアンインストール」や「インストールされた更新プログラムを表示」で表示されるソフトウェアの一覧を収集した情報です。

セキュア版CT

インターネット環境にあるPCに導入可能な、セキュア通信を行えるCTです。

セキュリティ監査

適用するべきセキュリティパッチやウイルス対策ソフトウェアのパターンが適用されていないPCを特定できます。これによりセキュリティホールやコンピュータウイルスの脅威に対するPCの防御能力を高めます。

セキュリティ監査機能

PCのセキュリティに関する様々な脅威対策を行うための、セキュリティ監査情報を管理する機能です。

セキュリティ監査レポート

Systemwalker Desktop Patrol、Systemwalker Desktop Keeper、Systemwalker Desktop Encryptionで実施しているセキュリティ対策について、運用状況やリスクのある部門/PCを把握・評価するために出力される監査/証明用レポートです。

セグメント別検知

ADTをセグメント毎に設置し、同一セグメント内のネットワークに接続されている機器を自動検知する方式です。また、検知した機器の情報を、CSに通知します。

是正期間

現状のセキュリティ状況を把握する日から、最終的にセキュリティ状況として承認するまでの期間です。本期間内にセキュリティ監査レポートを出力して、監査レベルがOKとなるようにセキュリティ対策を実施します。

ソフトウェア稼働状況

ソフトウェアが実際に稼働したかどうか（実行ファイルが動作したかどうか）の情報（ソフトウェア稼働状況）です。メインメニューでソフトウェア稼働状況を収集するようにした場合に確認可能となります。

ソフトウェア稼働状況では部門ごとの情報を参照できます。

ソフトウェア辞書

CTから収集するインベントリ情報を定義したものです。「サポートセンター定義」と「ユーザー定義」の2種類があります。

「ソフトウェア辞書」は、Systemwalkerサポートセンターから随時配信されます。

ソフトウェア情報

インベントリ情報の種類の1つです。コンピュータにインストールされているソフトウェア製品の製品名、バージョンなど、ソフトウェアの検索辞書により検索した結果を取得した情報です。ファイル名、ファイルサイズ、Windowsシステムのレジストリ情報の格納先などをもとに、ソフトウェア製品情報を特定できます。

ソフトウェア配信機能

CTなどに配信するソフトウェアを管理する機能です。新規登録、更新、削除、差分配信などができます。

ソフトウェアライセンス定義

ライセンス管理を行うには、そのソフトウェアが導入されているか判定するための検索条件を定義する必要があります。

Systemwalker Desktop Patrolでは、その検索条件の定義の集合を「ソフトウェア辞書」と呼びます。また、「ソフトウェア辞書」のソフトウェアに対するライセンスの定義を「ソフトウェアライセンス定義」と呼びます。

対処画面

メインメニューの状況画面の該当台数のリンクをクリックすることで表示される画面です。

この画面で、以下の運用対処が行えます。

- メッセージ送信
- インベントリ収集
- インベントリ削除
- セキュリティパッチの適用
- セキュリティ設定の変更
- 省電力設定の変更

ダウンロードメニュー

CTをインストールするためのセットアッププログラムのダウンロード、PCをディスク消去するためのディスク消去コマンドのダウンロード、およびディスク消去結果通知コマンドのアップロードを行うための入り口となる画面です。ブラウザから表示します。

ディスク消去管理機能

「ディスク消去計画」、「ディスク消去実行」、「ディスク消去情報管理」からなり、廃棄時期が近づいているPCを計画的に管理して、確実なディスク消去処理を実施できる機能です。

ディスク消去対象PCとしてディスク消去PCグループに登録されたPCに対して、ハードディスク情報を消去し、結果を管理者にアップロードします。ディスク消去情報は、CSで一元管理されます。

適用チェック

「ソフトウェア辞書」の辞書コードを、インベントリ収集する対象にしたい場合にチェックすることです。メインメニューでこの適用チェックをすることにより、インベントリ収集対象となります。

ネットワーク一括検知

CSサーバから、ADTをインストールせずにセグメントを越えて、ネットワークに接続されているICMPに対応した機器の情報を自動検知する方式です。

配信ソフトウェア

メインメニューで、CSまたはDSに登録した配信対象のソフトウェアです。Systemwalker Desktop Patrolでは、ファイル単位からソフトウェア単位までコンテンツとして登録できます。

配信用ソフトウェアグループ

ソフトウェアを配信する時に作成するグループです。配信するソフトウェアを種類ごとに分けるために使用します。

ハードウェア情報

インベントリ情報の種類の1つです。CPU種別、搭載物理メモリ量、ディスク容量などコンピュータのハードウェアに関する情報です。

パスワード ID

回復パスワード入力画面で表示されるIDです。

パスワード文字列

BitLockerで使用する10～20桁程度のパスワードです。BitLockerで暗号化されたドライブをシステムに接続後、パスワード文字列を入力するとロックを解除して、ファイルへアクセスできるようになります。

標準インストール

管理台数が300台までの環境で、デフォルト値で簡単に導入・構築が行えるインストールです。

ビル管理情報

活動している拠点（事業所）についてまとめた情報です。管理情報の構築時に必要な情報です。

ファイル配信機能

CSでの配信設定だけで、複数ファイルを複数CTに簡易な操作で配信する機能です。配信結果についても、CSで確認できます。

複数IPアドレス

IPv4アドレス、IPv6アドレスの個数を合計すると2以上となる状態です。

部門管理アカウント

メインメニューのメニュー項目について、ログインしたユーザーが所属している部門と、部門の配下の情報だけを設定および参照できる権限です。

部門管理情報

部門情報をまとめた部門についての情報です。管理情報の構築時に必要な情報です。

ポリシー

Systemwalker Desktop Patrolの各機能の動作を所定のルールで記述した情報の集まりをポリシーと呼びます。

ポリシーには、DSおよびCTに対するセキュリティパッチの適用スケジュールや適用動作、インベントリ収集スケジュール、またはソフトウェア配信スケジュールなどの動作設定情報などが含まれます。

ポリシーグループ

論理的なグループを作成し、そのグループ単位にクライアントポリシーの適用を行う運用です。ポリシーの設定を分けたい場合は、管理者がポリシーグループを作成し各クライアントPCをそのグループに登録します。

物理的なネットワーク構成にとらわれずに自由にグループを定義し、上位サーバをまたいだ任意のPCのポリシーを管理することが可能です。

ポリシーグループ単位の運用はメインメニューで設定します。

マスタ管理情報の構築

インベントリ情報、ライセンス情報を、ユーザー単位、部門単位ごとに参照するために使用するマスタ管理情報を登録することです。

マルチキャストアドレス

ff00::/8 で定義されるIPv6アドレスです。

メインメニュー

各PCから収集したインベントリ情報の参照、ライセンス管理やセキュリティ監査などのDesktop Patrol 業務を行うための入り口となる画面です。ブラウザから表示します。

ユーザーアカウント

メインメニューのメニュー項目について、ログインしたユーザーの情報だけを参照できる権限です。管理情報の構築時に登録するすべての「ユーザーID/パスワード」に割り当てられる権限です。

ユーザー管理情報

ユーザー情報をまとめた情報です。管理情報の構築時に必要な情報です。

ユーザー資産ソフトウェア辞書

ユーザーの資産管理情報をもとに作成されたソフトウェア辞書の定義を、ユーザー資産ソフトウェア辞書と呼びます。

ユーザー資産ソフトウェア辞書作成コマンド(dtplocaldic.exe)の実行により、メインメニューの[環境設定]-[監査ソフトウェアの設定]-[ユーザー定義]配下に定義が追加されます。

ユーザーセキュリティ

ユーザー設定のセキュリティ情報として、スクリーンセーバーの設定状況およびInternet Explorerのセキュリティレベル設定状況を、各PCから収集できます。

ユーザー定義

「ソフトウェア辞書」に登録されていないソフトウェアの検出条件を管理者が独自に作成したものです。企業内の独自のソフトウェアなどを定義する場合などに使用します。

ユニークローカルアドレス

fc00::/7で定義されるIPv6アドレスです。同一のサイト内で使用されます。ULAと略されることがあります。

ライセンス管理機能

管理者がメインメニューの[ライセンス]-[ライセンス割り当て]で、利用するソフトウェアごとにライセンスを割り当てることにより、ライセンス数を管理できます。

ライセンス管理を行うことで、ライセンス違反や遊休資産の発見が可能となります。

リモート操作機能

Systemwalker Desktop Patrolに同梱されているSystemwalker Live Helpの機能の1つです。対象のPCを、遠隔地から操作できます。また他にも、Systemwalker Live Helpでは、画像受信、ファイル転送、ファイル比較、クリップボード転送などの機能が使用できます。

リンクローカルアドレス

fe80::/10 で定義される IPv6 アドレスです。同一のL2ネットワーク内で使用されます。LLAと略されることがあります。

レジストリ情報

OSのレジストリに存在する情報です。メインメニューで収集したいレジストリ情報を設定した場合に確認可能です。