— 企業・団体向け クライアント運用管理ソフトウェア —

SKYSEA Client View

スカイシー クライアント ビュー

Ver.17

テレワークの「見える化」で、
社員の隠れた努力も見えてくる。

Sky

組織の重要データを守るために

SKYSEA Client Viewが
リスク対策を支援します

標的型攻撃やランサムウェアなどのサイバー攻撃、
PCの誤操作やデバイスの紛失といった人為的なミスなど、
組織は情報漏洩リスクと常に隣り合わせです。

SKYSEA Client Viewは組織の重要なデータを守るため、
情報セキュリティ対策の強化とIT資産の安全な運用管理を支援する
各種機能・ソリューションを提供いたします。

SKYSEA Client Viewは——

毎年のバージョンアップで お客様の声を取り入れ、進化を続けます

お客様の声に磨かれ、常に改善を図るため、SKYSEA Client Viewは発売以来、毎年定期的なバージョンアップを重ねています。
IT環境の変化にいち早く対応し、さらに使いやすい商品を目指して、今後もバージョンアップ・進化を続けます。

Ver.1~3
- ポップアップ通知
- 不許可端末検知

Ver.4
- コスト削減支援

Ver.5.1~6.1
- ソフトウェア資産管理（SAM）
- サーバー監査

Ver.8.1~8.2
- Macログ管理

Ver.10~10.2
- マイナンバー運用管理支援
- データベース監査
- 外部との通信ログ取得強化

Ver.11.4~12.3
- サイバー攻撃への多層防御
- UTMなど他社製品と連携
- 過重労働対策強化

Ver.14~15.1
- 更新プログラム配布管理
- Microsoft Office アップデート支援
- ソフトウェアの脆弱性管理支援

Ver.16.2~17
- PC環境の自動診断
- 紛失PCのリモート制御
- EDR製品連携によるマルウェア対策強化
- SKYSEA Client View Cloud Editionリリース
- テレワーク支援機能強化

2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 **2021**

Ver.3.1~3.4
- ログ自動バックアップ
- ポリシー違反チェック
- 省電力支援

Ver.4.1~5
- デバイス管理
- エンタープライズモード
- パフォーマンス・性能向上

Ver.7~8
- ユーザーインタフェース刷新
- Mac、Linux対応
- iPhone / iPad対応

Ver.9~9.2
- ログデータ圧縮、検索高速化
- メディア管理対応

Ver.11~11.3
- 標的型攻撃対策強化
- 持ち出しファイルの暗号化

Ver.13~13.2
- 残業管理機能強化
- Windows 10 自動アップデート制御

Ver.15.2~16.1
- 各アプリケーションの操作時間見える化
- 共有フォルダのファイル自動暗号化
- メールの添付ファイル自動暗号化

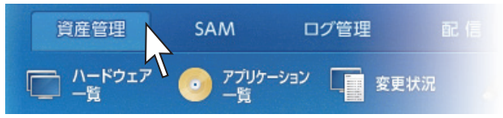
初めてでも使えるソフトウェアを目指して

直感的に使いやすい管理画面を搭載

どんなに多機能でも、操作に手間取れば運用には役立ちません。
SKYSEA Client Viewの機能メニューは、「使いやすさ」にこだわった設計を大切にしています。

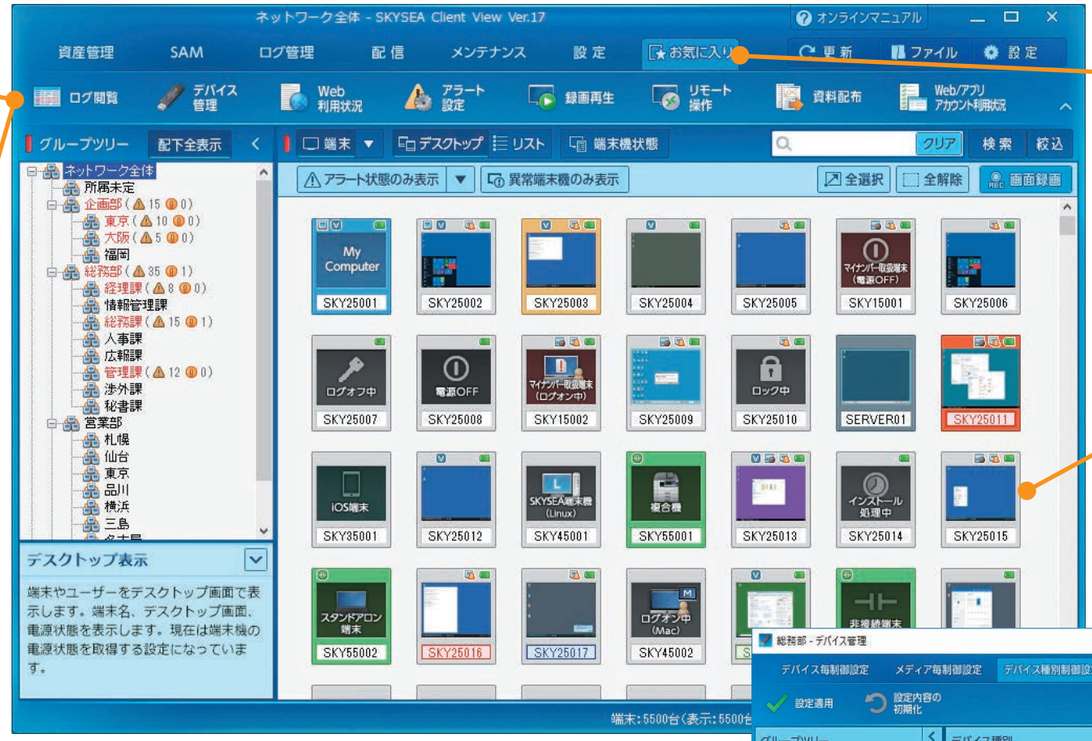
カテゴリ分けされた わかりやすい機能メニュー

機能ごとにわかりやすく整理されたアイコンを用意。必要な機能（操作）がすぐに見つかるように、操作のカテゴリで分類されています。



初めてでも操作に迷わない 「ふきだしヒント」

ボタンや項目にポインターを合わせると、操作のヒントを表示する「ふきだしヒント」を搭載。機能説明を載せた「機能ガイド」（画面左下）と併せて、管理画面の操作を支援します。



よく使う機能を登録できる 「お気に入り」タブ

よく使う機能ボタンを1つのタブにまとめて登録できます。機能メニューをカスタマイズすることで、日々の管理業務の利便性向上にお役立ていただけます。

各PCの稼働状況が確認できる デスクトップ画面表示

各PCのデスクトップ画面の様子や各種設定、アラート発生の状況を部署ごとに一覧で確認できます。アラートを種別ごとに色分けして表示し、分類しやすくすることも可能です。

使用制限の設定が簡単な デバイス管理画面

デバイスの使用制限など、アイコンをクリックして切り替えるだけで簡単に制御設定が行え、複雑な操作なしで運用を開始できます。

機能概要

Ent＝Enterprise Edition　Pro＝Professional Edition　Tel＝テレワーク Edition　LT＝Light Edition
500＝500 Clients Pack　ST＝Standard Edition　標準＝標準環境（VPN環境）※1
HTTPS＝HTTPSゲートウェイ環境※2　S1=S1 Cloud Edition　S3=S3 Cloud Edition　OP＝オプション

資産管理	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
PCのハードウェア・ソフトウェア情報を自動収集して管理※3	●	●	●	●	●	●	●	●	●	●
SKYSEA未導入のPCの情報も検出・管理	●	●	●	●	●	●	●	●	—	—
インターネット経由で資産情報を収集	●	●	●	●	●	●	OP	OP	●	●
プリンターなどのIT機器情報を定期収集※3	●	●	●	●	●	●	●	●	—	—
ソフトウェアを一斉配布、インストール	●	●	●	●	●	●	●	●	●	●

ログ管理	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
PCの操作ログを記録、データを素早く抽出して確認※3※4	●	●	●	●	●	●	●	●	●	●
ネットワーク非接続PCのログを収集	●	●	●	●	●	●	●	●	●	●
組織内PCの外部との通信状況を把握	●	●	●	●	●	●	●	●	●	●
クライアントPCの操作画面を録画	OP	OP	OP	OP	OP	OP	—	—	—	—
送信メールをログとして記録	●	OP	OP	OP	OP	●	—	—	—	—
Webサイトのアクセス状況を集計・管理	●	●	●	●	●	●	●	●	—	—

セキュリティ管理	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
組織のセキュリティポリシーに沿って不適切な操作を制限※5	●	●	●	●	●	●	●	●	●	●
宛先指定でメール送信を制限	●	OP	OP	OP	OP	●	—	—	—	—
メール送信時の添付ファイル自動削除	●	OP	OP	OP	OP	●	—	—	—	—
マイナンバー取り扱いPCへの各種操作を制限	●	●	●	●	●	●	●	●	●	●

	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
更新プログラムの配布・適用を管理	●	●	●	●	●	●	—	—	—	—
Windows 10の自動アップデートを制御	●	●	●	●	●	●	●	●	●	●
ソフトウェアの脆弱性情報を取得・管理	●	●	●	●	●	●	●	●	●	●
未登録の持ち込みPCからのアクセスを遮断	●	●	OP（※6）	OP（※6）	OP（※6）	●	—	●	—	—
残業申請や帰宅を促すメッセージをPCに表示	●（※7）	●（※7）	●（※7）	●（※7）	●（※7）	●（※7）	●	●	●	●
残業未申請PCの画面をロック、ネットワーク遮断	●（※7）	●（※7）	●（※7）	●（※7）	●（※7）	●（※7）	●	●	—	—
画面キャプチャーによる情報の持ち出しを禁止	●	—（※8）	●	—（※8）	—（※8）	—（※8）	—	—	—	—
PC環境を自動で診断	OP	OP	OP	OP	OP	OP	—	—	—	—
紛失したPCをリモートロック・データ削除	OP	OP	OP	OP	OP	OP	—	—	—	—
EDR製品と連携し、マルウェア感染対策を強化	OP	OP	OP	OP	OP	OP	OP	OP	OP	OP

デバイス管理	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
USBデバイスやメディアの台帳管理、使用制限※3※9※10	●	●	●	●	●	●	●	●	●	●
紛失したデバイスの保存データをログ追跡※11	●	●	●	●	●	●	●	●	●	●
持ち込みデータを含むデバイスを接続禁止※11※12	●	●	●	●	●	●	●	●	●	●
取り扱いファイル暗号化	●	●	OP	OP	OP	OP	—	●	—	●
外付けデバイス&ファイル暗号化	OP	OP	OP	OP	OP	OP	—	—	—	—
利用申請・承認をWebシステム上で管理	OP	OP	OP	OP	OP	OP	—	—	—	—

「SKYSEA Client View Cloud Edition」を新たにご用意しました

クラウドサービスとしてのご提供のため、ライセンスの初期費用や新規でサーバーを調達する必要がなく、導入コストを抑えることが可能です。また、オンプレミス版と同様に豊富な機能をご利用いただけます。詳しくはP.15をご覧ください。

ITセキュリティ対策強化	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
各種操作ログをsyslogとして他社製品へ送信	●	●	●	OP	OP	OP	—	●	—	—
UTMと連携し、サイバー攻撃を早期把握	●	●	●	OP	OP	OP	—	●	—	—
ウイルス検知したPCをネットワーク遮断	●	●	●	OP	OP	OP	—	●	—	●
特定（共有）フォルダへのアクセスを制限	●	●	●	OP	OP	OP	—	●	—	●
暗号化通信時のみ共有フォルダアクセスを許可	●	●	●	OP	OP	OP	—	●	—	●
社外でのインターネット利用を制限	●	●	●	OP	OP	OP	—	●	—	●
社外からVPN経由でインターネット接続	●	●	●	OP	OP	OP	—	●	—	●
ログから起動元プロセスを特定	●	●	●	OP	OP	OP	—	●	—	●
ZIPファイルの中身をログで記録	●	●	●	OP	OP	OP	—	●	—	●
Microsoft Officeの更新プログラム適用管理	●	●	●	OP	OP	OP	—	●	—	●
緊急性の高い更新プログラムを強制配布	●	OP	OP	OP	OP	OP	—	●	—	●

レポート	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
ログ解析レポート	●	●	●	●	●	●	OP	OP	OP	OP
資産レポート	●	●	●	●	●	●	OP	OP	—	—
資産・ログ利活用レポートライブラリ	●	●	●	●	●	●	OP	OP	OP	OP

メンテナンス	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
離れた場所にあるPCを管理機からリモート操作※3	●	●	●	OP	●	●	OP	●	OP	OP
複数PCへ管理機の操作を一斉転送	●	●	●	OP	●	●	OP	●	OP	OP
PCを遠隔制御（資料配布、電源制御など）	●	●	●	●	●	●	●	●	—	—
インターネット経由で管理機からリモート操作※3	OP	OP	OP	OP	OP	OP	OP	OP	OP	OP

ソフトウェア資産管理（SAM）	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
各種管理台帳を用意し、ソフトウェア資産を複合的に管理	●	●	●	●	●	●	●	●	●	●
Webシステムによる利用申請、承認に対応	OP	OP	OP	OP	OP	OP	OP	OP	OP	OP

サーバー監査	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
サーバーのイベントログを集積、アクセス状況などを把握	OP	OP	OP	OP	OP	OP	—	—	—	—
データベース上の操作をログとして収集	OP（※13）	OP（※13）	OP（※13）	OP（※13）	OP（※13）	OP（※13）	—	—	—	—

モバイル機器管理（MDM）※14	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
モバイル端末の資産情報を収集・管理、機能制限設定も可能	OP	OP	OP	OP	OP	OP	—	—	—	—

その他	Edition						Cloud Edition			
							標準		HTTPS	
	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
在席確認・インスタントメッセージ	OP	OP	OP	OP	OP	OP	—	—	—	—

※1 クラウド上のサーバーと管理機・クライアントPCとの接続には、VPNを利用します。※2 社外でのクライアントPC利用時にVPN接続が行えない場合は、HTTPS接続（オプション）でご利用いただけます。Linuxは非対応です。※3 Mac端末やLinux端末には、一部対応していない機能があります。※4 エディションによっては一部のログが対応しておりません。※5 エディションによっては一部のアラートが対応しておりません。※6 未登録の持ち込みPCからのアクセス検知は、標準機能です。※7 他社メーカー様の勤怠/就業管理システムと連携したメッセージ通知、画面ロックは、「勤怠情報取り込み」機能＜オプション（Tel/LT/500/ST）＞で提供しています。※8 オプションとしてもご購入いただけません。※9 メディア登録時は別途、管理番号を個別に付与する必要があります。※10 エディションによっては一部の機能が対応しておりません。※11 iPhone / iPad / iPod touchや、Android端末などのWPD（Windows Portable Devices）、デジタルカメラなどのWIA（Windows Image Acquisition）をご利用の場合は、非対応となります。※12 SKYSEA Client Viewがインストールされていないと PC上で保存、編集されたファイルを含むデバイスの使用を禁止できます。※13 本機能はサーバー監査機能（オプション）のオプションとしてご購入いただける機能です。※14 ログ収集などのログ管理機能は搭載しておりません。

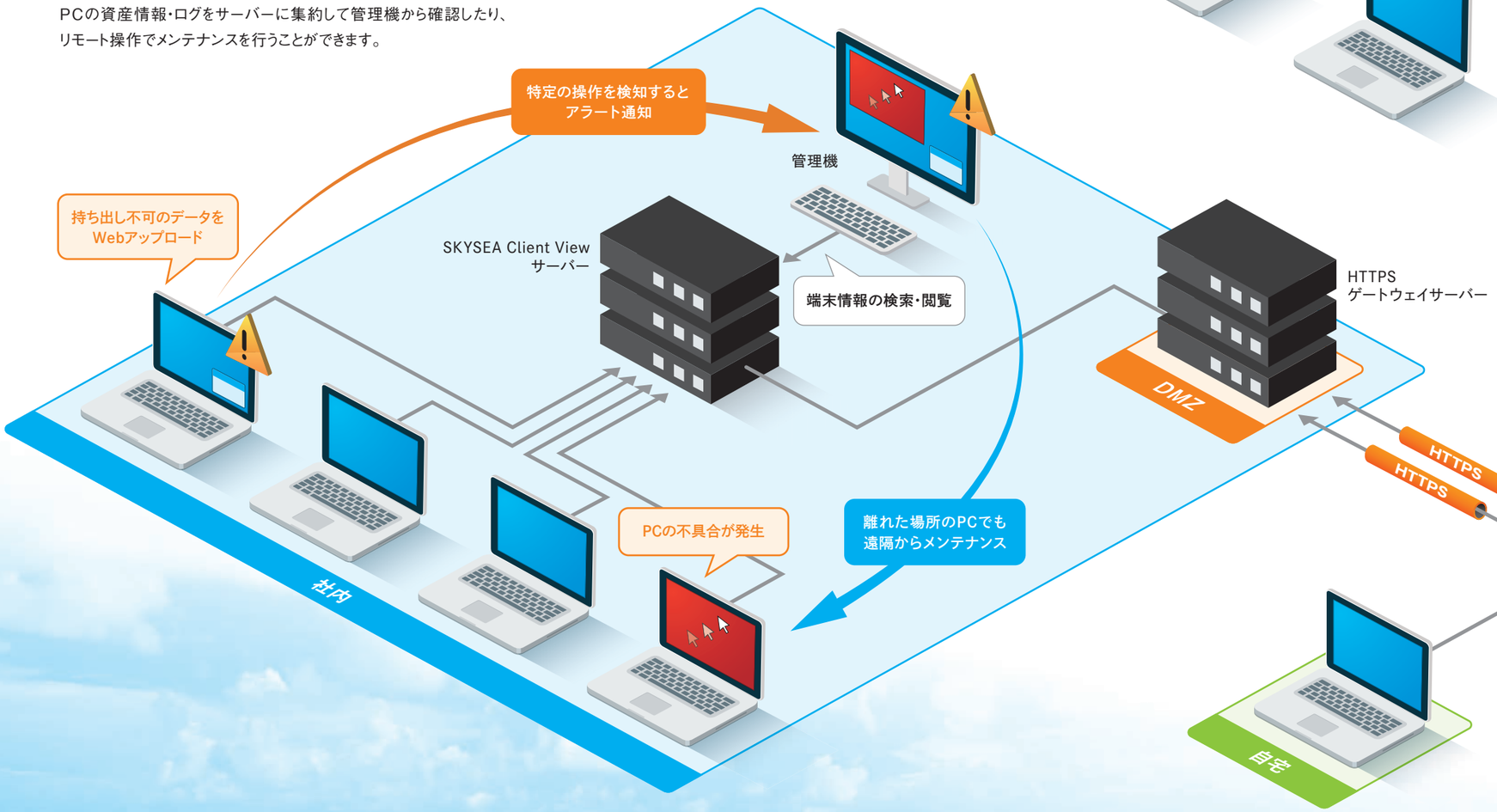
SKYSEA Client View

運用イメージ

SKYSEA Client Viewでは、システム管理者が組織内で管理されているPCの資産情報や操作状況を把握できるほか、
組織のポリシーに反する操作を制限するなど、IT資産の運用管理や情報セキュリティ対策の強化が行えます。
インターネットやクラウドなどを活用した幅広い運用に対応できる柔軟性も特長です。

組織内のPC情報を集約して運用管理

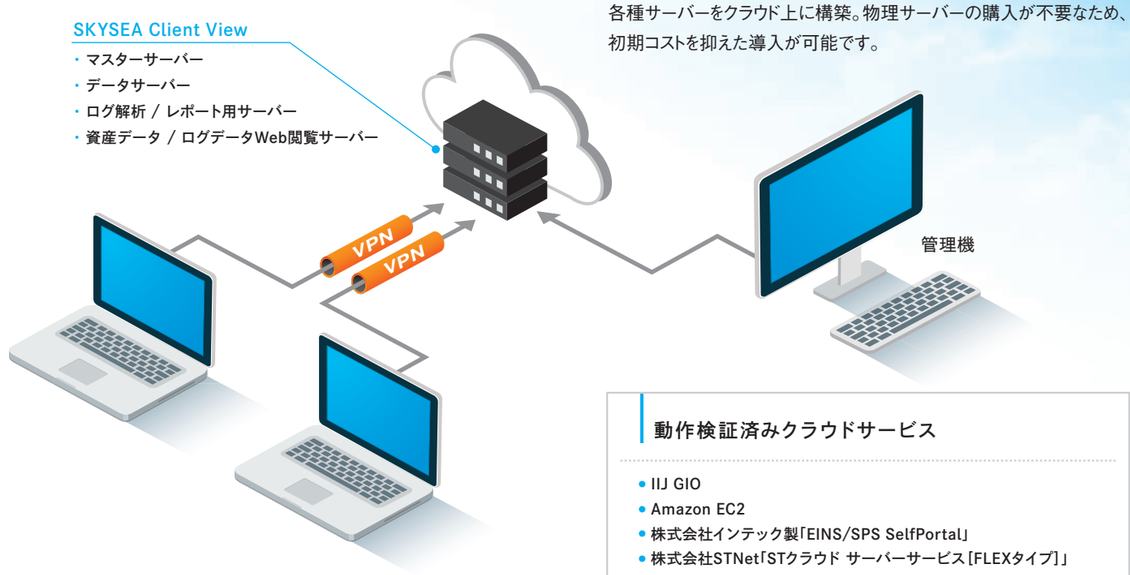
PCの資産情報・ログをサーバーに集約して管理機から確認したり、
リモート操作でメンテナンスを行うことができます。



SKYSEA Client View Cloud Editionについては P.15へ

パブリッククラウドにも対応

各種サーバーをクラウド上に構築。物理サーバーの購入が不要なため、
初期コストを抑えた導入が可能です。

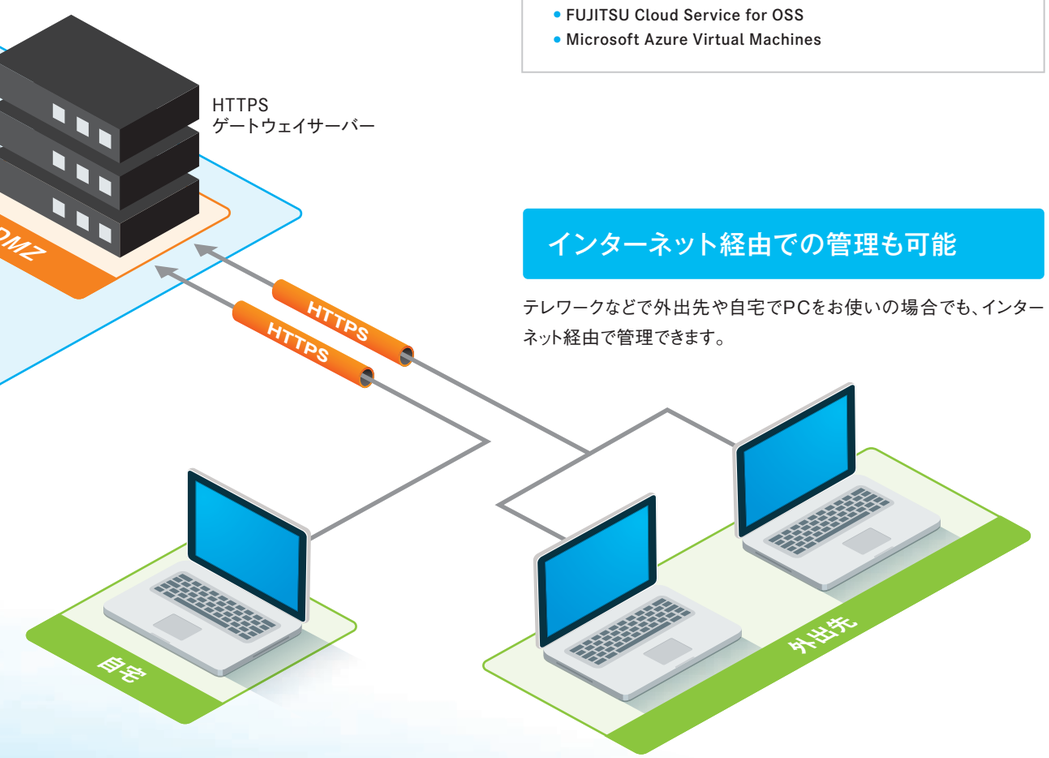


動作検証済みクラウドサービス

- IIJ GIO
- Amazon EC2
- 株式会社インテック製「EINS/SPS SelfPortal」
- 株式会社STNet「STクラウド サーバーサービス[FLEXタイプ]」
- NTT Com Enterprise Cloud
- ニフクラ
- FUJITSU Cloud Service for OSS
- Microsoft Azure Virtual Machines

インターネット経由での管理も可能

テレワークなどで外出先や自宅でPCをお使いの場合でも、インター
ネット経由で管理できます。



■ 他社製品との連携ソリューションで各種対策をさらに強化

SKYSEA Client Viewでは、セキュリティ製品をはじめとする各メーカー様の製品と連携することで、情報セキュリティ対策やIT資産管理、ITシステム運用、勤怠管理などをさらに強化していただける各種ソリューションをご用意しています。

暗号化

暗号化製品によるハードディスクやデータの暗号化状況をSKYSEA Client Viewの管理画面上で管理・確認できます。

個人情報利用状況確認

クライアントPCに保存されている個人情報を含む機密ファイルなどを検索。検索結果をSKYSEA Client Viewで管理できます。

ファイル無害化

ファイル無害化サーバーへのファイルのアップロード / ダウンロード状況をログとして収集できます。

USBデバイス管理・利用制限

USBデバイスの利用を制限したり、PCに接続するだけで管理台帳への登録が行えます。

USB装置連携

スタンドアロンPCに接続すると、ウイルススキャン結果と資産情報がUSBメモリに保存され、SKYSEA Client Viewに取り込めます。

アクセス制御

SKYSEA Client ViewのIT資産情報を基に、SDNによるアクセス制御設定を自動化し、ネットワーク管理の負荷軽減を支援。

シンクライアント対応

シンクライアント環境で利用した操作ログを、SKYSEA Client Viewで収集・管理できます。

SKYSEA Client View インストール対応NAS

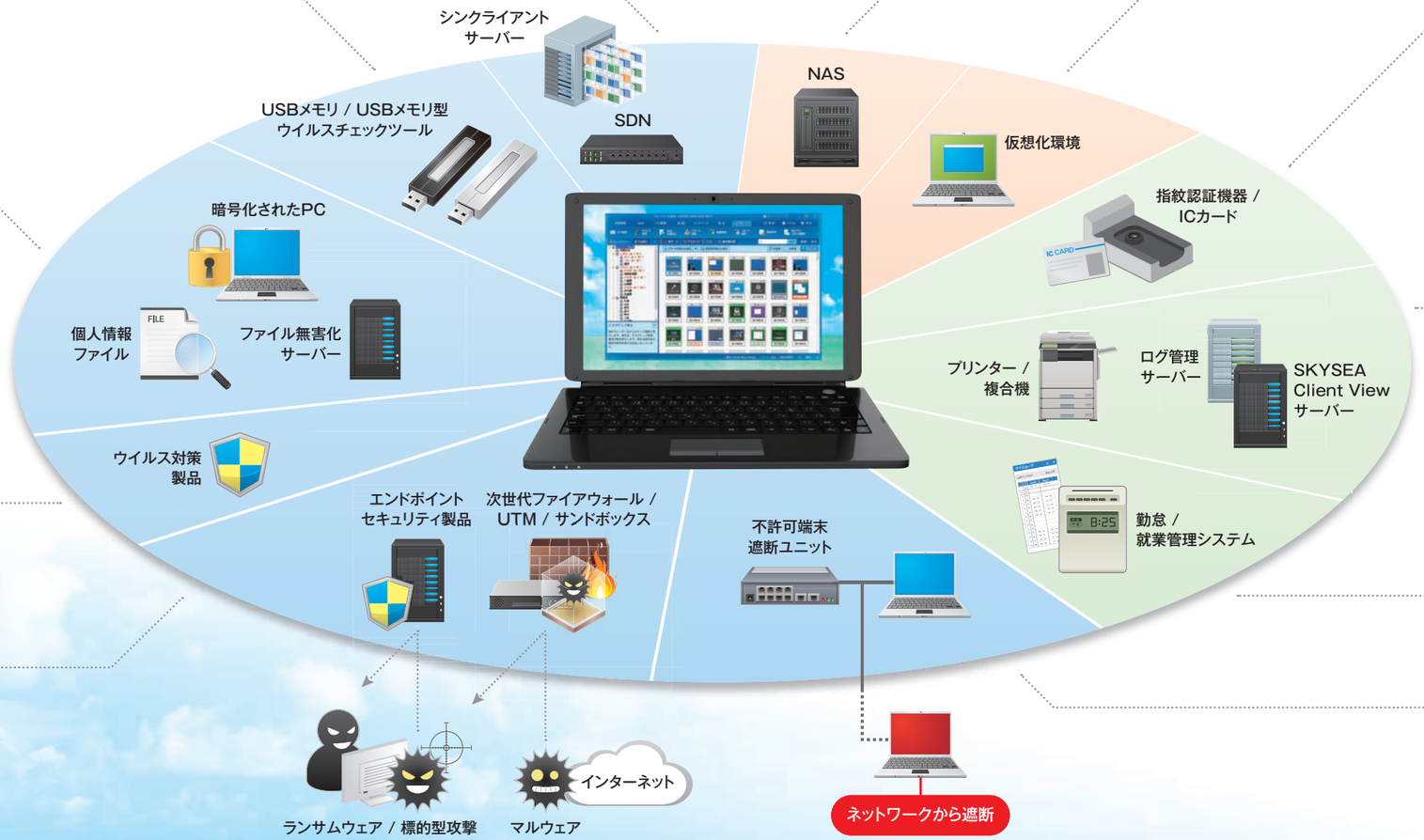
対象のNAS製品に、SKYSEA Client Viewのサーバー機能をインストールできます。

仮想化環境

各メーカー様が提供する仮想化環境で、SKYSEA Client Viewが運用できます。

認証

生体認証やICカードなどを使用してログインしたユーザーの操作状況を、ログとして記録・管理できます。



統合ログ管理

SKYSEA Client Viewの操作ログを連携製品に取り込み、他社システムのログとまとめて管理。総合的な状況把握を支援します。

SKYSEA Client Viewのデータと各種IT機器のマシンデータを合わせて相関分析が行える連携ソリューションもご用意しています。

プリンター連携

印刷物のスキャン・保存状況や、印刷イメージをログで記録。MIB情報を自動収集し、資産情報として管理できます。

ウイルス対策製品 インストール状況

インストール状況やパターンファイルのバージョンなどを資産情報として収集・管理できます。

勤怠 / 就業管理システム連携

SKYSEA Client Viewの操作ログを勤怠管理システムなどに取り込み、システムの出退勤時刻とPCの使用時間を照合し、差異を確認できます。

サイバー攻撃対策

PCや通信の異常を検知した連携製品から出力されたログをSKYSEA Client Viewが検知。対象PCをネットワークから自動遮断し、管理者にアラート通知します。

不許可端末検知・遮断

SKYSEA Client Viewをインストールしていないが接続されると、ネットワークから遮断し、管理者に通知します。

多様化するビジネススタイルを柔軟なIT運用管理でサポート

SKYSEA Client View Ver.17では、資産管理やログ管理などの機能を
クラウドサービスとして提供する「SKYSEA Client View Cloud Edition」をご用意。
そのほか、テレワーク運用やサイバー攻撃対策、ヘルプデスク対応など日々の管理業務を支援する新たな機能を搭載しました。
多様化する組織のビジネススタイルを、さまざまな機能とサービスで柔軟にサポートします。

SKYSEA Client View Cloud Edition

SKYSEA Client Viewが
SaaSで利用可能に

ログ利活用連携

他社製品へ出力できるログを拡張、
より幅広いログ分析が可能に

テレワーク運用支援

「Web会議時間」を見える化し、
業務プロセス改善を支援

ソフトウェア更新管理

キャッシュ配布対象を細かくグループ分けし、
PC間の通信負荷を軽減

テレワーク運用支援

社内・社外のどちらで働いていたか、
ログから判断が可能に

運用管理支援

資産情報やログが
アップロードされていないPCをアラート通知

サイバー攻撃対策

マルウェア対策を強化する連携機能が
新たな製品に対応

運用管理支援

リモート操作画面を自由に拡大できるようにし、
操作性を改善

デバイス使用制限

USBデバイスの使用期限設定を拡張、
組織の運用に沿った管理が可能に

その他 新機能

- Exchange接続によるメール送信ログを
  より正確に取得できるように改善
- Exchange Onlineの先進認証を利用した
  メール送受信に対応
- クライアント用インストールランチャーの
  起動時間を高速化
- リモート操作を行ったPCの情報を
  ログで正確に取得できるように改善
- Amazon AppStreamに対応

SKYSEA Client View Cloud Edition

SKYSEA Client View が SaaSで利用可能に

SKYSEA Client ViewをSaaSで利用できるエディション
「SKYSEA Client View Cloud Edition」を新たにリリースしました。
オンプレミス版とほぼ同じ豊富な機能をクラウドサービスとして提供し、
組織のIT資産管理や情報漏洩対策、テレワーク運用をサポートします。

SKYSEA Client View Cloud Editionの特長

導入コストを抑えることが可能

ライセンスの初期費用やサーバーの新規調達が不要なため、導入コストを抑えて運用を開始いただけます。また、利用に伴う継続的なサーバーメンテナンスも不要です。

オンプレミス版と同等の豊富な機能

資産管理やログ管理、セキュリティ管理やデバイス管理など、オンプレミス版とほぼ同じ豊富な機能をご利用いただけます。

機能が異なる2つのエディションと、各種オプションをご用意

S1 Cloud Edition

資産管理やログ管理、セキュリティ管理など、IT資産運用や情報漏洩対策に必要な基本機能を搭載しています。※1

S3 Cloud Edition

S1 Cloud Editionの機能に加えて、サイバー攻撃対策にお役立ていただける各種機能を搭載しています。※1

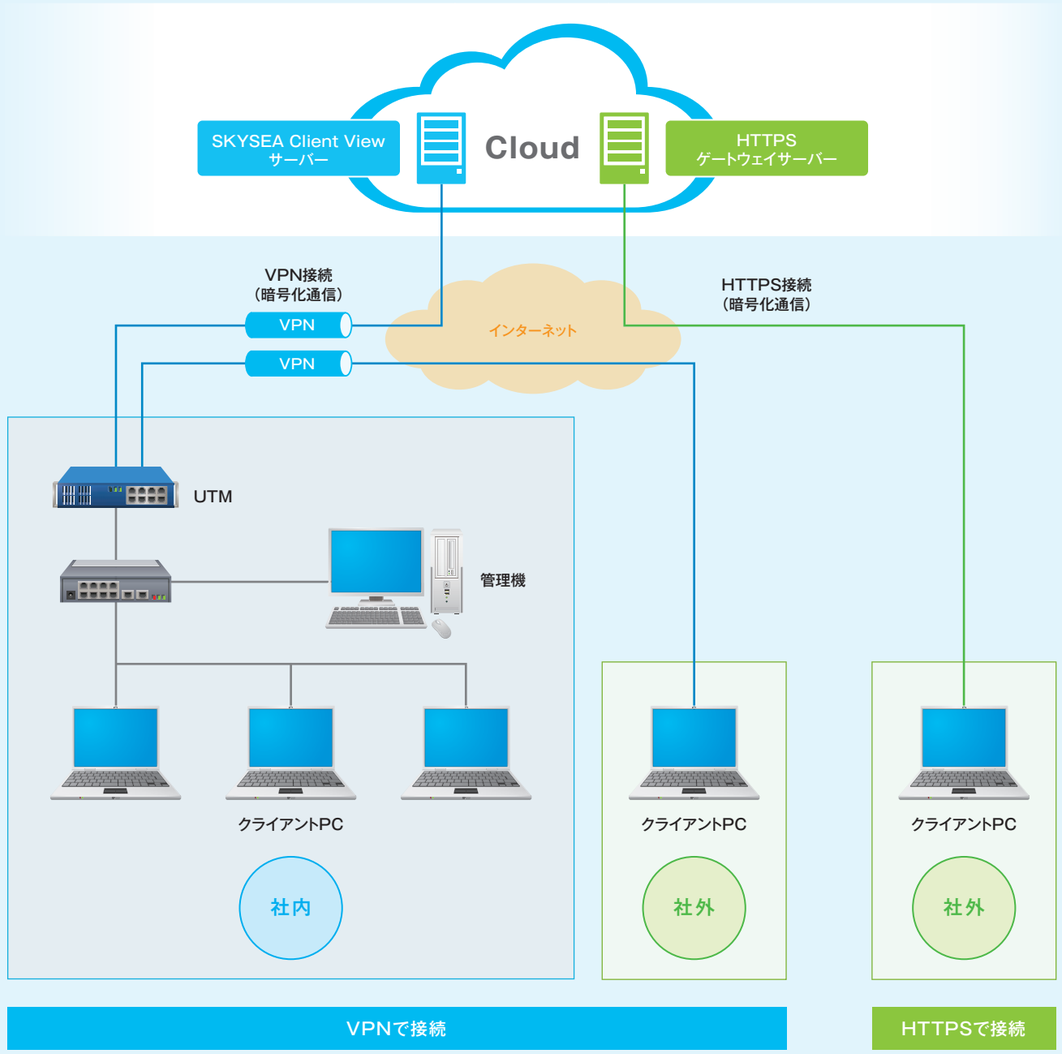
オプション

- httpsゲートウェイオプション※1
- シンクライアントオプション
- ログ保管容量追加オプション（1TB単位）
- ログ解析オプション※2
- リモート操作オプション
- httpsゲートウェイ経由リモート操作オプション
- EDR プラスパック Cloud（FFRI yarai Cloud版のみ）

※1 詳細はP.57の機能一覧をご覧ください。※2 オンプレミス版と異なり、本機能はオプションとなります

クラウドとのVPN接続で利用

クラウド上のサーバーと管理機・クライアントPCとの接続には、VPNを利用します。社外でのクライアントPC利用時にVPN接続が行えない場合は、HTTPS接続※3でご利用いただけます。



■ 収集したログは3か月間保管

クライアントPCから収集したログは、クラウド上に3か月間保管されます。また、PC1台あたりの規定保管容量は、S1 Cloud Editionが93MB、S3 Cloud Editionが558MBとなります。※4

■ 本サービスの提供について

最低契約台数50台、1年以上の利用契約が必要です。月額もしくは年額の利用料でご契約ください。最新バージョンのSKYSEA Client Viewを提供します。

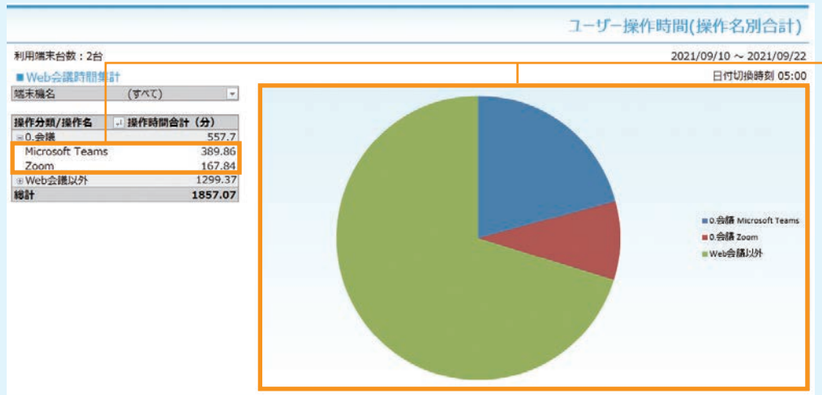
※3「httpsゲートウェイオプション」が必要です。※4 保管期間を過ぎると日付の古いログから消去されます。「ログ保管容量追加オプション」をご利用いただくと、保管期間の延長や規定容量を超えるログを保存いただけます。

テレワーク運用支援

「Web会議時間」を見える化し、業務プロセス改善を支援

「ユーザー操作時間レポート」拡張

テレワークの普及に伴い増加したWeb会議時間を、ユーザーごとにレポート集計。日々の業務のなかでWeb会議が占める割合を見える化することで、業務プロセスの改善などを検討する際の参考情報としてご活用いただけます。



Web会議時間を
集計・グラフ化

対応システム

- Cisco Webex
- Microsoft Teams※1
- Zoom

※1 Mac版のMicrosoft Teamsは非対応です。

テレワーク運用支援

社内・社外のどちらで働いていたか、ログから判断が可能に

「ログ管理」機能拡張

PCと社内にあるSKYSEA Client Viewサーバー※2との通信状況に関する情報を、ログとして取得できるように強化。各種操作ログをチェックする際、それが社内での操作なのか、テレワーク時など社外での操作なのかを判断する際の参考情報としてご活用いただけます。

※2 マスターサーバー、もしくはデータサーバー。

社内勤務か、テレワークかの判断材料に

社内勤務、またはテレワークで社内環境へVPN接続している可能性

- SKYSEAサーバー通信成功（ローカル通信）

テレワークの可能性

- SKYSEAサーバー通信成功（インターネット経由）
- SKYSEAサーバー通信失敗

サイバー攻撃対策

マルウェア対策を強化する連携機能が新たな製品に対応

「syslogによる異常端末監視」アラート拡張

連携するUTMなどのセキュリティ製品が不審な通信を検知した際、管理者にアラート通知をしたり、該当PCをネットワークから遮断する機能※3を拡張。新たに、機械学習エンジンを搭載した次世代ファイアウォール※4に対応しました。パターンマッチングでは難しい未知の脅威を検知し、速やかな状況把握と安全性の確保を支援します。

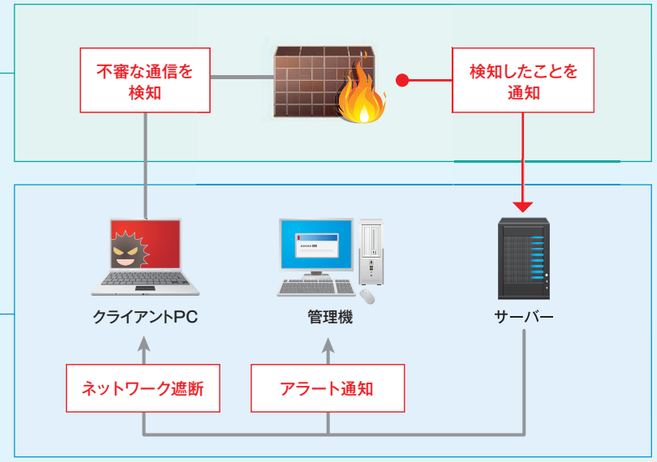
※3 詳しくはP.46をご覧ください。※4 連携するセキュリティ製品については、SKYSEA Client ViewのWebサイトをご覧ください。

次世代ファイアウォール

- パターンマッチングでは難しい未知の脅威を検知

SKYSEA Client View

- 検知情報をログで確認
- 脅威の拡散等を抑止

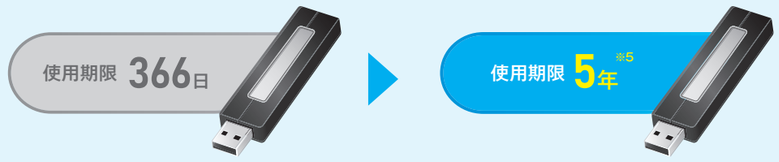


デバイス使用制限

USBデバイスの使用期限設定を拡張、組織の運用に沿った管理が可能に

「デバイス管理」機能改善

指定したUSBデバイスの使用期限を、従来の366日よりも長く設定できるように改善。例えば、年単位のライセンス期限があるウイルス対策ソフトウェア搭載のセキュリティUSBメモリを、ライセンス期限切れと同時に使用できなくなるように設定することができます。



※5 使用期限は2037年12月31日までの間で設定いただけます。

ログ利活用連携

他社製品へ出力できるログを拡張、より幅広いログ分析が可能に

「syslog送信設定」機能拡張

SKYSEA Client Viewが検知したアラートログを他社製品へsyslog出力し、情報漏洩対策などに活用できる機能※1を強化。アラートログだけでなく、そのほかのログも出力できるようにしました。例えば、Webアクセスに関するログを他社のログ統合管理システムへ出力し、アクセス状況の分析を行うなど、さまざまなログを対象にご活用いただけます。

※1 詳しくはP.48をご覧ください。

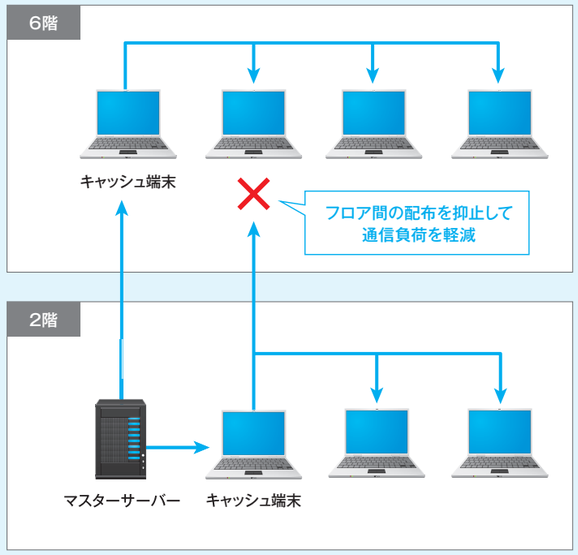
ソフトウェア更新管理

キャッシュ配布対象を細かくグループ分けし、PC間の通信負荷を軽減

「ソフトウェア配布」機能拡張

PCへのソフトウェア配布がセグメントごとに効率的に行える、キャッシュ配布機能※2を強化。配布対象のPCを、IPアドレス単位で柔軟にグループ分けできるようになりました。例えば、セグメント内に複数フロアのPCがまとまって存在する場合に、配布対象をフロアごとにグループ分けすることで、フロアをまたいだ通信を起こさずに配布でき、通信負荷の軽減につなげていただけます。

※2 マスターサーバーから配布されたソフトウェアを受け取ったPC（キャッシュ端末）が、同じセグメント内のPCへソフトウェアを配布する機能。キャッシュ端末からソフトウェアを受け取ったPCは新たにキャッシュ端末となり、未配布のPCへソフトウェアを配布します。

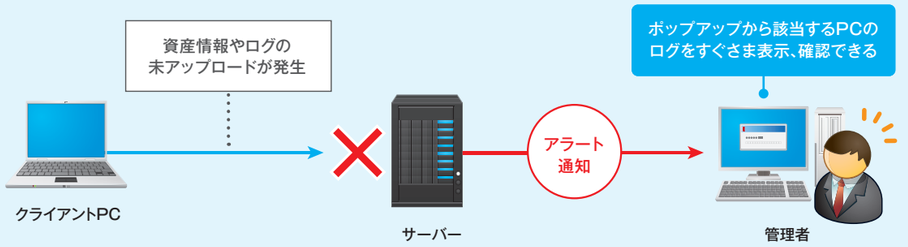


運用管理支援

資産情報やログがアップロードされていないPCをアラート通知

SKYSEA端末アップロード異常検知

何らかの原因で、クライアントPCから資産情報やログがサーバーにアップロードされなかった場合に、異常を検知して管理者にアラート通知。該当するPCの状況をログですぐに確認でき、原因の把握と素早い復旧にお役立ていただけます。



運用管理支援

リモート操作画面を自由に拡大できるようにし、操作性を改善

「リモート操作」機能改善

リモート操作中に、接続先PCのデスクトップ画面を自由に拡大・縮小できるように改善。接続先PCの画面解像度が管理機より低い場合でも拡大して表示でき、メンテナンスや問い合わせ対応がより作業しやすくなりました。

テレワークの労働時間や業務状況の見える化を支援

SKYSEA Client Viewで記録されたPCの操作ログを活用することで、従業員の労働時間や業務状況の見える化を支援します。テレワーク中の従業員の状況把握や、過重労働対策の取り組みにもお役立ていただけます。

勤怠管理やセキュリティ面におけるテレワークの課題を解決

課題 労働時間が見えにくい

解決

- PCの使用時間を集計して、労働時間を見える化
- 業務時間外のPC使用を制限し、サービス残業を抑止

課題 仕事中の様子がわからない

解決

- PCの操作ログをまとめた各種レポートから業務状況を把握
- メッセージの送信・受信で従業員間の情報共有を支援

私物のPCは危険？ テレワークでは会社貸与のPCが有効

私物PCをテレワークで利用する場合は、OSや各ソフトウェアが最新の状態でなかったり、セキュリティ対策が不十分であることも考えられます。また、PCの所有者によってITスキルなどに違いがあり、システム管理者が依頼する各種対策が十分に行えない場合があることも想定できます。加えて、プライベートでも利用する私物PCに、SKYSEA Client Viewなどのログ収集ツールを導入することは現実的ではありません。そのため、シンクライアントシステムの利用（弊社商品では「SKYDIV Desktop Client」）や、リモートデスクトップ方式の利用、また管理が行き届いた会社貸与のノートPCを持ち帰って利用する方法が、安全かつ効率的だといえます。

ログを集計・グラフ化し、労働時間や業務状況の把握を支援

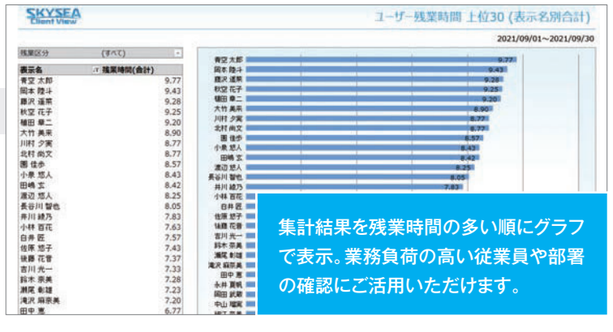
ログ解析レポート / 資産・ログ利活用レポートライブラリ

日々蓄積されるPCの操作ログを集計・グラフ化し、労働時間の視覚的な把握を支援します。これら集計結果と、勤怠 / 就業管理システムやタイムカードなどの記録とを照らし合わせ、勤務実態の調査に活用いただけます。

業務時間外のPCの使用時間から従業員の残業時間を把握

残業時間レポート

指定した期間における、業務時間外でのPCの使用時間を、残業時間として算出。ユーザー別・部署別での合計残業時間や、部署別の平均残業時間を集計、確認することができます。また、残業時間は始業前と定時後で分けて表示することも可能です。

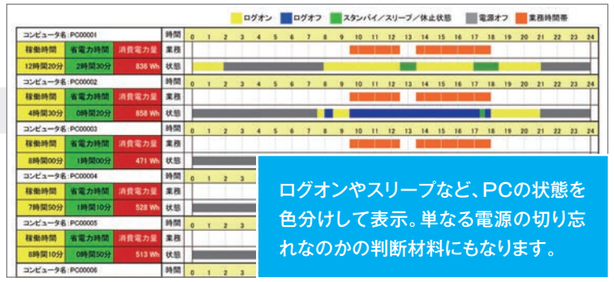


集計結果を残業時間の多い順にグラフで表示。業務負荷の高い従業員や部署の確認にご活用いただけます。

PCごとに24時間の使用状況を表示、テレワーク中の業務状況の把握に

時間帯別使用状況解析レポート

業務時間内にログオフが続いているPCがないか、早朝・深夜にPCが使用されていないかなど、テレワーク中の状況の把握を支援します。

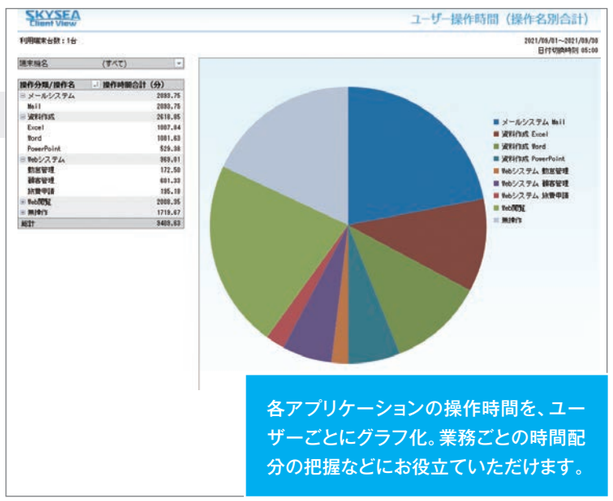


ログオンやスリープなど、PCの状態を色分けして表示。単なる電源の切り忘れなのかの判断材料にもなります。

各アプリケーションの操作時間を見える化、働き方の傾向把握をサポート

ユーザー操作時間レポート

アプリケーションやWebシステムごとの操作時間を集計して見える化。それぞれの操作時間を確認することで、どの業務にどれくらいの時間をかけていたかなど、従業員の働き方を把握するための参考情報として活用いただけます。



各アプリケーションの操作時間を、ユーザーごとにグラフ化。業務ごとの時間配分の把握などにお役立ていただけます。

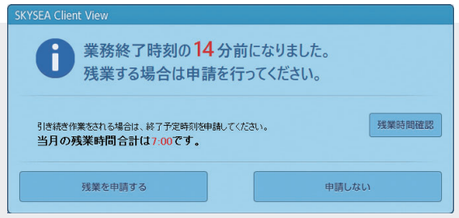
日々の残業状況を適切に把握、状況の早期改善を支援

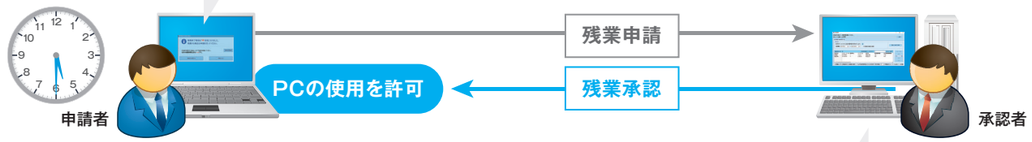
残業時間お知らせメッセージ / 残業管理 【関連特許取得】

定時終了前や業務時間外に、PCの画面にメッセージを表示し、従業員に業務終了や残業申請を促すことができます。管理機では残業申請の承認 / 拒否が行えるほか、当月の累計残業時間なども確認できます。タイムカードなどでの月ごとの集計ではなく、PCの操作ログから残業時間をリアルタイムに把握でき、業務負荷の偏りといった状況の早期改善にお役立ていただけます※1。

お知らせメッセージで業務終了や残業申請を促す

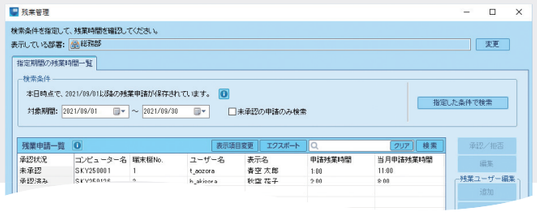
定時終了前などにメッセージを表示。残業申請が行われないまま定時終了時刻が過ぎたり、申請した残業時間を超過した場合には、PCをネットワークから遮断したり、画面をロックすることで、業務時間外のPC使用を制限できます※2※3。





残業申請の承認や拒否、残業状況の確認を行う

残業申請の承認 / 拒否、および当月の累計残業時間を確認できます。スマートフォンからでも申請内容の確認や承認操作ができ、外出先でPCが手元にない場合でも承認処理が行えます※4。



※1 残業の申請・管理を必ずこの機能で行っていただく必要があるものではありません。お客様の運用ルールに沿ってご利用ください。※2 システム管理者が事前に設定した解除コードをPC上で入力することで、ネットワーク遮断や画面ロックの解除が行えます。※3 他社メーカー様の勤怠 / 就業管理システムと連携したメッセージ通知、画面ロックは、「勤怠情報取り込み」機能<オプション(Tel/LT/500/ST)>で提供しています。
※4 DMZ内にリバースプロキシサーバーまたはロードバランサーの設置が必要です。加えて、専用のデータベースサーバー、またはWebサーバーを設置する必要があります。

出退勤時刻とPC使用時間の差異をチェック

勤怠 / 就業管理システム連携

SKYSEA Client Viewで収集したログオン・ログオフや操作開始・終了ログを、各メーカー様の勤怠 / 就業管理システムへエクスポートし、システムで管理している出退勤時刻との差異を確認。労働時間の適正な把握を支援します。

深夜や休日のPC起動を制限し、長時間労働を抑止

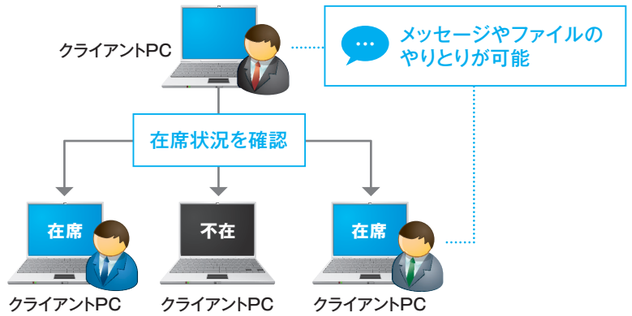
定期電源OFF設定

時間や曜日を指定し、その間のPCの電源を強制的にOFFにすることができます。電源OFFを実行することを、事前に従業員へメッセージ通知することも可能です。いつでもPCを起動させやすいテレワーク環境において、深夜や休日の起動を制限することで、サービス残業や長時間労働を抑止します。

PC操作から在席状況を把握、メッセージで手軽に情報共有

在席確認・インスタントメッセージ　オプション(Ent/Pro/Tel/LT/500/ST)

PCへのログオンやキーボード・マウスの操作状態から、ほかの従業員の在席状況を自分のPCで確認することができ、メッセージを送り合うこともできます。コミュニケーションや情報共有が不足しがちなテレワークにおいて、在席状況を確認した上で、メッセージで手軽にやりとりすることができます。



Web会議システムのバージョン情報を管理し、脆弱性対策を徹底

「アプリケーション一覧」機能改善

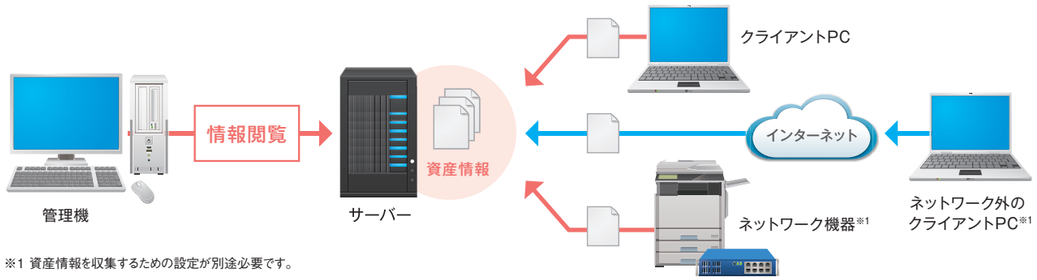
テレワークに欠かせないWeb会議システムを安全に利用し続けるには、常に最新バージョンへの更新を行い、脆弱性を放置しないことが重要です。Ver.16.2では、クライアントPCごとのWeb会議システムのインストール状況やバージョンを資産情報として収集可能に。未更新のPCを素早く確認できるようにすることで、脆弱性対策の徹底をサポートします。※5

※5 対応するWeb会議システムについては、P.75「Web会議システムについて」をご覧ください。

資産管理

日々変動する資産情報を自動収集、IT資産運用の最適化を支援

クライアントPCやサーバーのハードウェア情報、ソフトウェア情報、プリンターやルーターなどのネットワーク機器情報などを24時間ごとに自動収集し、1つの台帳で管理。組織内のIT資産の活用状況を的確に把握することで、各部署での運用の最適化やコストダウンなどに活用いただけます。



※1 資産情報を収集するための設定が別途必要です。

必要な情報を素早く検索、管理業務を効率化

ハードウェアー覧

検索条件を細かく指定し、条件にあった端末だけを表示できます。特定のOSを搭載したPCを抽出し、バージョンアップの検討に活用するなど、日々の管理の効率化にお役立ていただけます。

資産変更状況

事前に設定した資産情報の項目が変更されると、画面上に赤字で強調表示されます。気づきにくい、資産情報の小さな変化も適時把握できます。

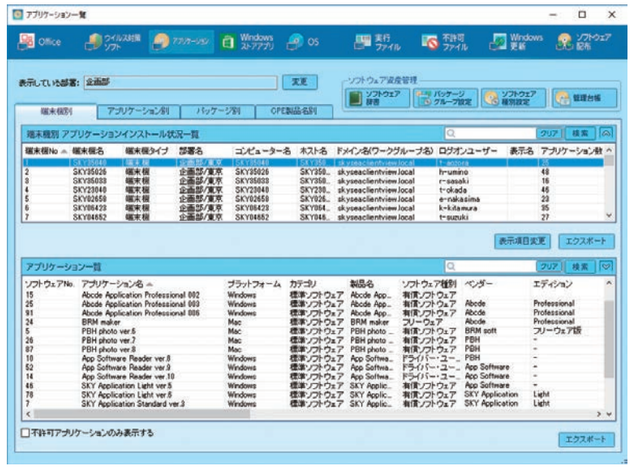
インストール状況を把握し、ライセンスの最適化を図る

アプリケーション一覧

ソフトウェアごとのインストール台数や、プロダクトIDなどの情報を表示。必要なソフトウェアが導入されているか、ライセンスが正しく使用されているかなどを確認することができます。そのほか、WindowsやMicrosoft Officeの更新プログラムの適用状況も、一覧で確認することが可能です。

ウイルス対策ソフトウェア更新状況

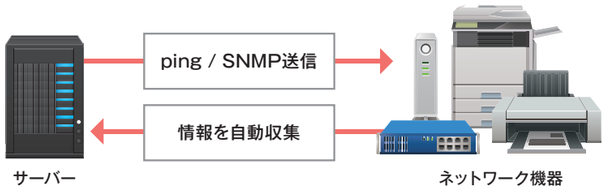
クライアントPCごとにウイルス対策ソフトウェアのインストール状況を確認できます。複数メーカー様のウイルス対策ソフトウェアに対応しています。



オフィス機器情報を収集して一元管理

ネットワーク機器情報収集

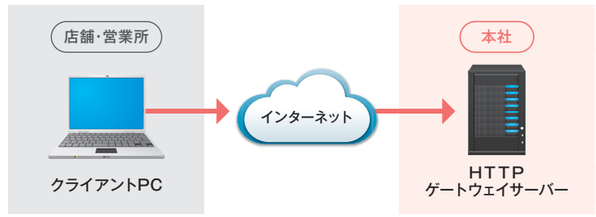
プリンターやHUBなどのネットワーク機器の情報を収集し、台帳管理できます。SNMP対応機器であれば、詳細な情報も収集でき、オフィス内の機器の状況が細やかに確認できます。



社内ネットワークへの接続が困難なPCの運用管理に

インターネット経由での資産情報収集

本社のネットワークとの接続が難しい他拠点のクライアントPCなどから、HTTP(S)通信による資産情報やログの収集が行えます。デバイス管理やリモート操作※2、各種セキュリティポリシーの設定も行えます。

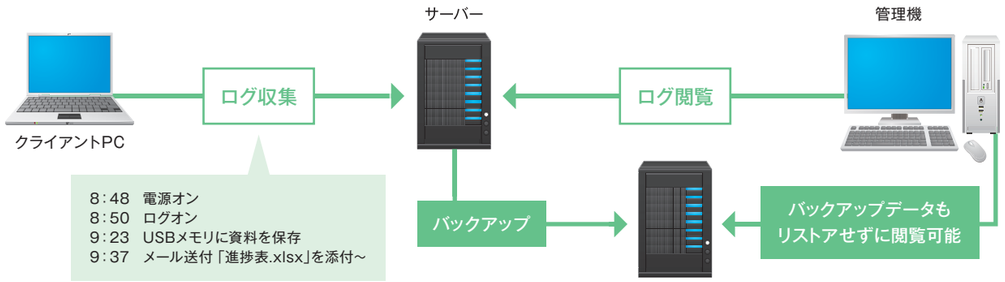


※2 リモート操作する側、操作される側の両方のPCで、別途ツールのインストールや起動が必要です。

ログ管理

日々のPCの挙動をログとして管理
情報漏洩リスクの早期発見などに活躍

クライアントPC上でのユーザーの操作や、外部との通信、ファイルへのアクセス状況など、PCのさまざまな挙動をログとして記録。膨大なデータから必要な情報を抽出することで、「いつ」「誰が」「何をしたのか」を正確に把握し、情報漏洩リスクの素早い発見を支援します。



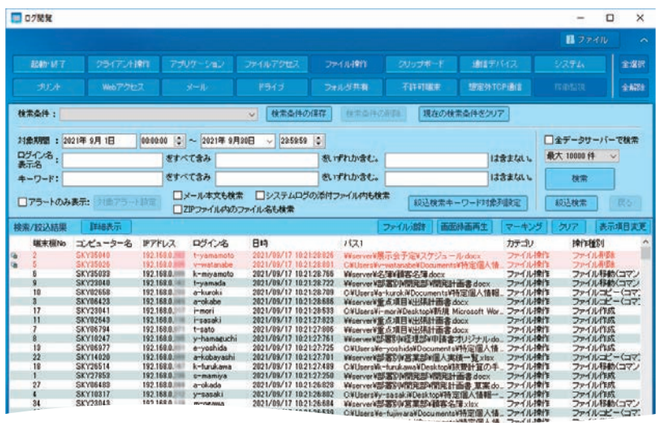
特定のファイル操作などをログで確認、状況把握を支援

ログ閲覧

ログの種別、キーワードや期間などの条件を指定することで、重要データの取り扱いやアプリケーションの起動状況などを一連のログとして表示。PCの不審な挙動がないかを確認でき、状況の早期把握に役立ちます。

全データサーバー一括ログ出力

複数のデータサーバーでログを管理している場合でも、すべてのデータサーバーを検索範囲に指定して、一度にログ検索することができます。



別名保存されても、ファイル操作を徹底追跡

ファイル追跡

外部への情報流出が疑われる操作など、不審なファイル操作について、流出経路の特定が行えます。ファイルコピー、別名保存によって分岐したファイル操作の追跡も可能です。

アクセスログから不審な操作を確認

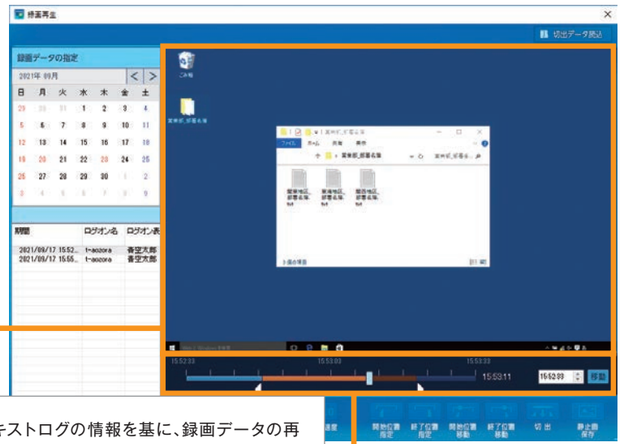
サーバーの共有ファイルへのアクセスログから、アクセス前後5分のクライアントPCでどんな操作が行われていたか、ファイルがどのように使われていたのかを確認できます。

重要データの取り扱い状況を視覚的に把握

画面操作録画

オプション（Ent/Pro/Tel/LT/500/ST）

重要データを取り扱う担当者にとっては、これらデータを管理するシステム（データベース）にアクセスすることが業務上必要であり、その操作を制限するのは現実的ではありません。画面操作を録画しておくことで、操作の正当性の確認や、不注意による誤操作の早期発見にお役立ていただけます。



テキストログでは把握できないマウス操作や、アプリケーション上での文字入力など、詳細な操作内容を視覚的に把握できます。

テキストログの情報を基に、録画データの再生位置をピンポイントで指定し、チェックしたい操作を素早く表示できます。

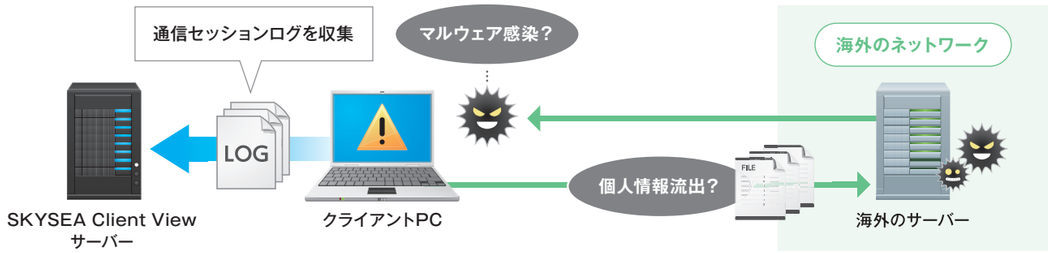
注意すべき操作が行われると、自動で録画を開始

重要データを取り扱うシステムの起動時など、指定した操作が行われると自動的にPC画面の録画が開始されるように設定することもできます。

組織内にあるPCの外部との通信状況を把握

想定外TCP通信ログ

各サーバー、クライアントPCの通信セッションをログとして収集、管理。ログの詳細を確認することで、普段通信することのない海外の外部サーバーへのアクセス状況などをいち早く把握し、マルウェア感染などによる不正なデータ送信がないか察知することにお役立ていただけます。マルウェアの攻撃対象になりやすいInternet Explorerによるバックグラウンド通信を記録することも可能です。



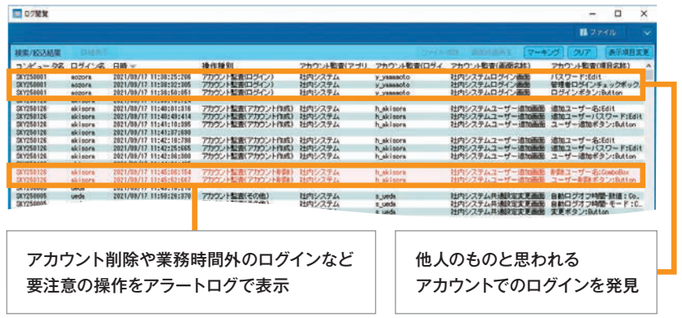
サイバー攻撃の被害発覚時の調査に備え、ログの長期保存・バックアップを

標的型攻撃では、マルウェアがPCに侵入してから、数か月後に情報漏洩の被害が発生しているケースもみられます。そのため、被害の発覚後にマルウェアの侵入経路などの調査を行うためには、ログを長期間保存しておくことが望まれます。SKYSEA Client Viewでは、ログを最大10年間保存するように設定できます。また、バックアップしたログデータをリストア（復元）せずに閲覧・利用でき、過去のログを調査する際もすぐに作業に取り掛かることができます。

業務基幹システムなどのアカウント利用状況を把握

Webアプリケーションアカウント監査

指定したWindowsアプリケーションやWebシステムごとに、アカウントの取り扱いに関するログを記録※1。不審なアカウントの追加や削除がないか、他人のアカウントを利用した「なりすましログイン」がないかなどの状況把握にご活用いただけます。

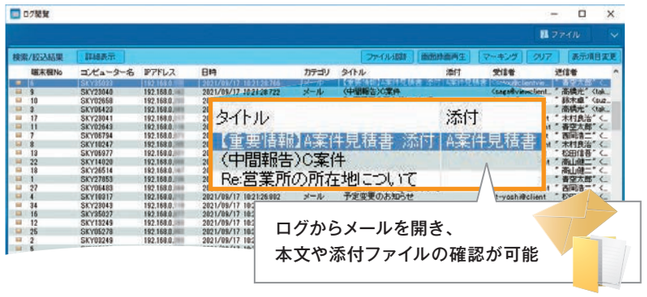


※1 事前にログ取得の対象画面、および対象操作（アカウントの入力、ログイン処理を行うためのボタン操作など）を登録する必要があります。登録できていない場合は、ログ取得が行えません。

メール経由での情報漏洩の防止に活用

送信メールログ
オプション（Pro/Tel/LT/500）

送信メールとその添付ファイルをログとして記録します。また、メールの件名や本文も対象に含めたキーワード検索ができ、確認したい送信メールログを手間なく絞り込むことができます。



収集できる操作ログ一覧 ……… SKYSEA Client Viewでは、種別ごとにカテゴリ分けしてログを管理しています。

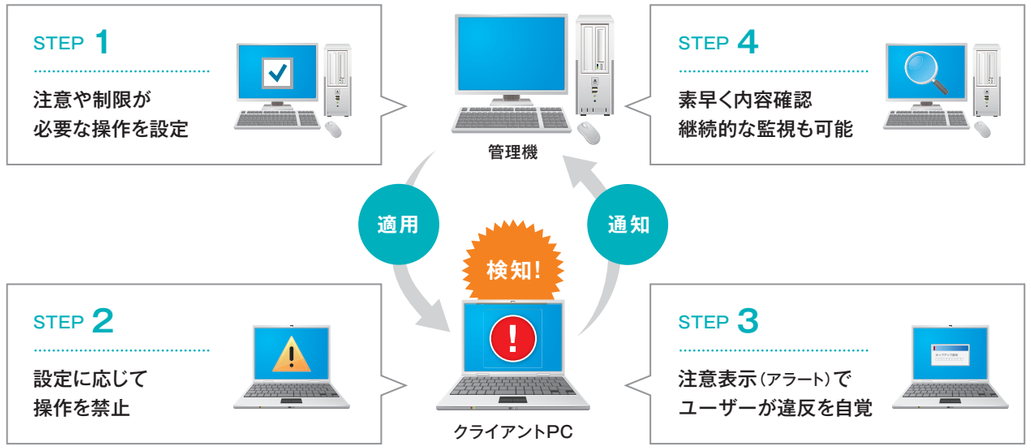
起動・終了ログ	ユーザーごとのログオン / ログオフや電源ON / OFF、操作開始 / 終了時刻など。
クライアント操作ログ	アクティブ状態のウィンドウタイトルと稼働時間、業務で使用するアプリケーションのログイン状況など。
アプリケーションログ※2	ユーザーが利用したアプリケーションの実行ファイル名や稼働時間、ファイルパス、ハッシュ値、実行コマンド、ファイルパス（起動元アプリ）、ハッシュ値（起動元アプリ）、プロセスIDなど。
ファイルアクセスログ	ローカルの共有フォルダへのアクセス、アクセスユーザー、操作種別など。
ファイル操作ログ	ファイルの作成、上書き保存、削除、コピー、名前変更、ライティングソフトウェアを用いたCD-R / DVD-Rへの書き込みなど、ファイル・フォルダ操作の履歴（MTP / PTP接続デバイスでファイルコピーしたログも取得）※3。
クリップボードログ	コピー&ペーストしたときのクリップボードの内容※4など。
システムログ	アラート設定変更を行った部署・変更内容、ログ未回収期間に達したクライアントPCのログ、リモート操作のログ（PC操作時、管理機操作時両方）など。
プリントログ	印刷したドキュメントのプリンター名、プリントタイトル、印刷枚数、印刷対象のファイルパス、IPアドレス、ポート名など。
Webアクセスログ※5	Internet Explorer、Mozilla Firefox、Google Chrome、Microsoft Edge（Chromium版）でアクセスしたURL、ウィンドウタイトル、稼働時間、Gmail送信ログ、WindowsアプリケーションやWebシステムへのログイン状況など。 ● Webファイルアップロード：対応するWebブラウザでアクセスしたURL、Dropbox等のWebサイトにアップロードしたファイル名などを記録。 ● Web書き込み：対応するWebブラウザでアクセスしたURL、Webメール・掲示板への書き込みログ、書き込んだ内容、Microsoft 365でのファイル作成ログなどを収集。 ● FTPアップロード：FTPへのファイルアップロードログなどを収集。
送信メールログ オプション（Pro/Tel/LT/500）	メールを送信した宛先（CC / BCCを含む）、件名、添付ファイルの送信履歴など。
ドライブ追加・削除ログ	USBデバイスなどのドライブの追加・削除、ドライブ種別などを記録。
フォルダ共有ログ	共有フォルダの作成・削除、共有元アドレス、共有名など。
不許可端末ログ （Windowsのみ）	登録されていないクライアントPCのMACアドレス・IPアドレスなどを検知。デフォルトゲートウェイを新規で利用、または変更されたログなどを収集。
通信デバイスログ	ネットワークカードやBluetoothなどの通信デバイスによる接続に関するログなど。
想定外TCP通信ログ	実行ファイルのTCPによる通信に関するログなど。

※2 起動元アプリケーション、コマンドプロンプト情報のアプリケーションログはオプション（LT/500/ST）です。 ※3 Mac端末の場合、ファイルコピー、ファイル上書き保存、フォルダコピーは対象外です。
※4 Mac端末の場合、Print Screenは対象外です。※5 Mac端末の場合、書き込みログは対象外です。

セキュリティ管理

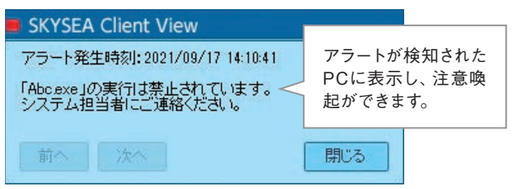
社内ポリシーに沿って不適切な操作を制限、ユーザーの情報セキュリティ意識向上に

業務と関係ないアプリケーションの使用や、Webサイトへの書き込みなど、組織のセキュリティポリシーに違反する行為に対して、注意表示（アラート）メッセージを通知したり、操作そのものを禁止するように設定できます。ポリシーに反する行為が行われたPCの画面を、自動的に録画することも可能です。



▶ アラート検知時の通知（禁止）方法

ポップアップ通知
アラートが検知されたPC、管理機の画面にメッセージを表示。



メール
アラート発生時に管理者のPCにメールを送信。

画面録画
アラートが検知されたPCの画面を録画※1。

禁止
アラート対象の操作が行われた場合に、その操作を禁止。

アラートログ
アラート対象となった操作を「アラートログ」として記録。

※1「画面操作録画」はオプション（Ent/Pro/Tel/LT/500/ST）です。

重要データの漏洩を防ぐため、各種操作を制限

注意表示（アラート）設定

ファイルのWebアップロード、メール送信、印刷出力など、クライアントPC単位での制限設定が行え、情報漏洩の防止にお役立ていただけます。一方的に操作を禁止するだけでなく、メッセージでユーザーに注意を促すなど、柔軟な設定が可能です。

操作前後の様子をログでも確認

管理画面上で、ポリシーに反する操作が行われたときの画面の様子や、操作前後のログを確認することで、適切に状況を把握することが可能です。

設定可能なポリシー（例）

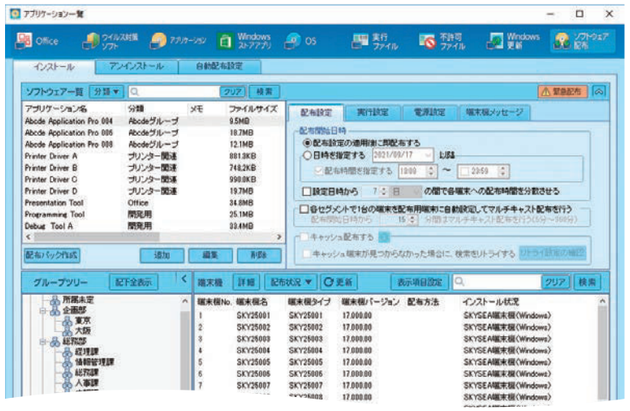
許可 / 不許可アプリケーション	● 許可していないアプリケーションのインストールを検知します。
アプリケーション実行	● 事前に指定したアプリケーション（またはそれ以外）の実行を禁止します。
業務外アプリケーション実行	● ゲームや動画など音声を出力するアプリケーションの実行を禁止します。
特定フォルダアクセス※2	● 指定したフォルダへのアクセスがあった場合に検知します。
禁止ファイル持ち込み	● 指定したキーワードを含むファイルやフォルダに対する操作を検知します。
記憶媒体 / メディア使用	● 指定したUSBデバイス、メディアの使用を禁止します。
USBデバイスによる不正ファイル持ち込み	● SKYSEA Client Viewがインストールされていないパソコン上で保存されたファイルを含むUSBデバイスの接続を禁止します。
印刷枚数	● 指定した枚数以上の印刷が一度に行われた場合に検知します。
電子メール送信宛先フィルタ オプション（Pro/Tel/LT/500）【関連特許取得】	● 指定したアドレス以外へのメール送信を禁止します。
Web閲覧	● 指定したURLのWebサイトの閲覧を禁止したり、指定URLのみ閲覧を許可します。
Print Screenキーによる画面コピー※3	● 「PrintScreen」キーによる画面キャプチャーを禁止します。

※2「ITセキュリティ対策強化」機能をご導入いただくことで、特定フォルダへのアクセスを許可するアプリケーションが指定できます。詳しくは、P.45をご覧ください。 ※3 Enterprise Editionとテレワーク Editionでのみご利用いただけます。その他のエディションではご利用いただくことはできません。また、オプションとしてもご購入いただけません。

脆弱性対策を迅速に行うため更新プログラムを一斉配布

ソフトウェア配布

情報漏洩リスクを考慮して、更新プログラムの適用が必要な場合などに、管理機から各部署のクライアントPCに一斉にソフトウェアを配布、インストールできます。スケジュールを設定し、業務に支障が出にくい時間帯に処理を実行することも可能です。

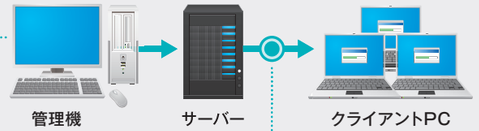


■ 作業をまとめて一括処理も可能

複数のインストール、アンインストール処理をグループにまとめて一括で実行することも可能。業務ソフトウェアの入れ替え時などに役立ちます。

配布用スクリプトもご用意

保守契約ユーザー用Webサイトにて、ソフトウェア配布を簡素化する各種スクリプトをご用意。また、専用ツールで操作を録画し、スクリプトファイルを自動生成することも可能です。



端末を中継させ、配布負荷を軽減

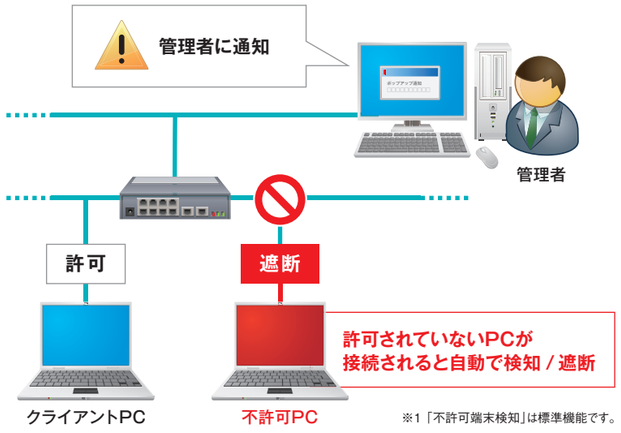
セグメントごとに自動選択された端末からクライアントPCにマルチキャスト方式で一斉配布を行うことで、配布を高速化。サーバーとの通信量を軽減します。

社内ネットワークへの不許可PCの接続を遮断

不許可端末検知※1 / 不許可端末遮断

オプション（Tel/LT/500）

使用が許可されていない、社外からの持ち込みPCが社内ネットワークに接続されると、接続を自動的に検知。管理者へメール通知し、ログを出力します。自動的に接続を遮断することもでき、ウイルス感染対策としてもご活用いただけます。



■ 接続PCの機器情報を自動で検出

ネットワーク接続された不許可PCの機器情報を自動で検出し、端末の特定に役立てることもできます。

※1「不許可端末検知」は標準機能です。

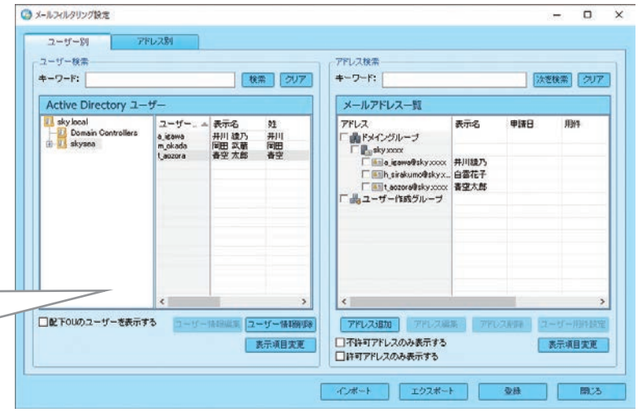
指定した宛先以外へのメール送信を制限

電子メール送信宛先フィルタ

オプション（Pro/Tel/LT/500）

事前に指定したメールアドレス以外への送信を検知し、禁止します。管理者が把握していないアドレスに、重要データが送信されてしまうことによる情報漏洩リスクを軽減します。

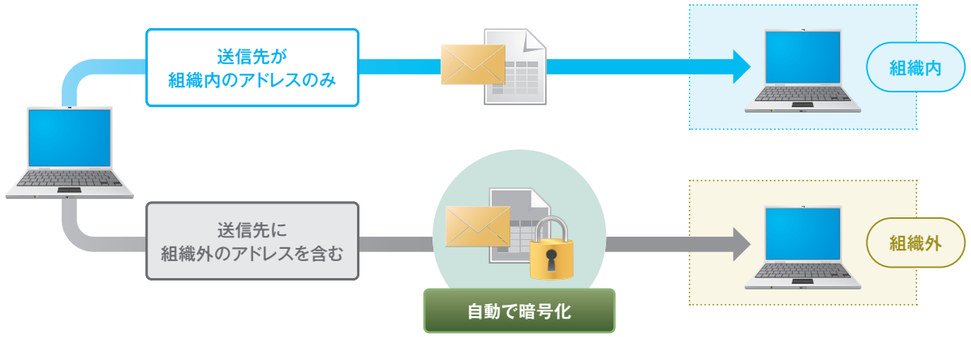
Active Directoryに登録されたユーザーごとに送信を許可するアドレスを指定したり、アドレスごとに送信を許可するユーザーの指定が可能。



組織外へ送信するメールの添付ファイルを自動で暗号化

電子メール送信時の添付ファイル自動暗号化※2

組織内で使用しているメールアドレスやドメインを登録しておき、未登録の宛先を含むメールが送信される際に、添付ファイルを自動で暗号化します。組織外へ送信する添付ファイルの暗号化し忘れなどを防ぎます。



添付ファイルの自動削除も可能

■ 電子メール送信（添付ファイル付き）アラート※3
オプション（Pro/Tel/LT/500）

未登録の宛先を含むメールが送信される際に、添付ファイルを自動で削除することも可能です。組織内の重要データを添付ファイルとして外部に持ち出す行為などを制限できます。

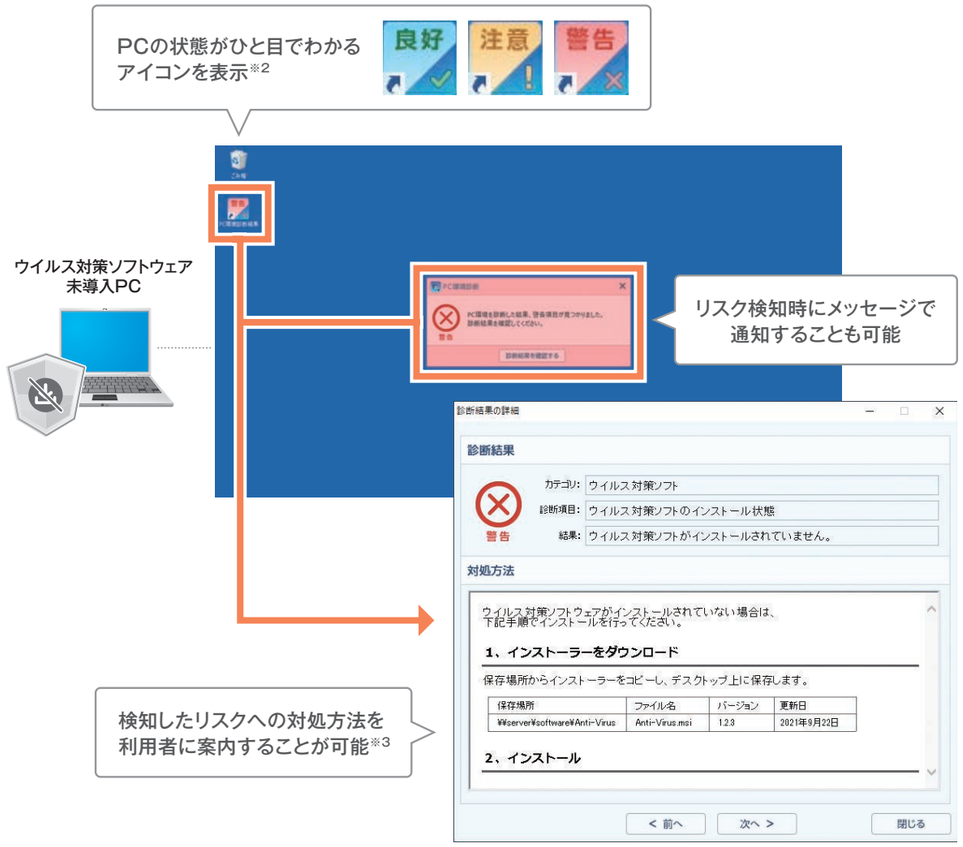
※2 本機能をご利用いただくには、「送信メールログ」機能＜オプション（Pro/Tel/LT/500）＞と、「外付けデバイス&ファイル暗号化」機能＜オプション（Ent/Pro/Tel/LT/500/ST）＞が必要です。また、本機能は「Microsoft Outlook」にのみ対応しています。その他のメールクライアントや、「Outlook.com」などのWebメールには対応しておりません。※3 本機能は「Microsoft Outlook」の2003以降のバージョンにのみ対応しています。

PCを自動診断、情報漏洩リスクを伴う状態を素早く通知

PC環境診断

オプション（Ent/Pro/Tel/LT/500/ST）

ウイルス対策ソフトウェアの動作状況やWindows更新プログラムの適用状況など、PCの状態をまとめて診断し、リスクを検出した際にアイコンやメッセージで通知※1。対処法とともに利用者へ知らせることができます。ウイルス感染や脆弱性の放置につながるPCの状態を素早く把握し、対処につなげることで情報漏洩対策を徹底いただけます。



診断できる内容

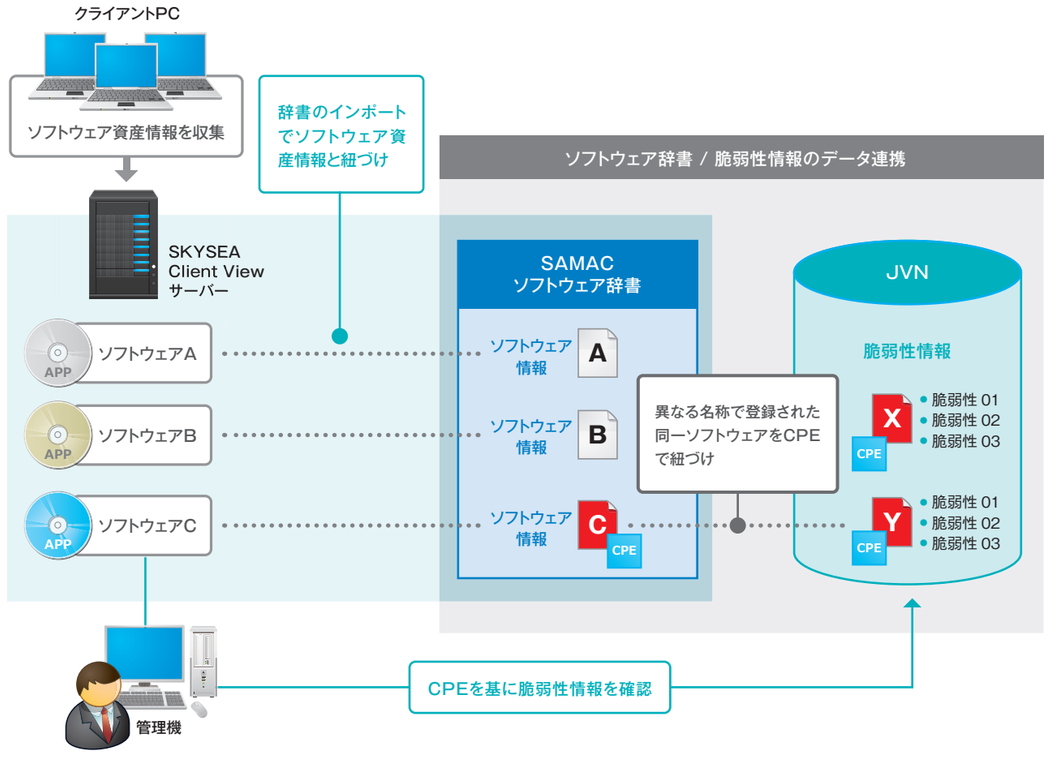
• ウイルス対策ソフトウェアのインストール状況 / 有効化状況	• Windows更新プログラムの適用状況 / 再起動待ち状況	• Windows Updateの更新プログラムのチェック状況
• WSUSサーバーの設定状況	• Windows Defenderのスキャン状況 / リアルタイム保護状況	• 指定したアプリケーションのインストール状況

※1 管理者にもアラートで通知します。※2 ログオン時に自動で診断し、事前に設定したレベルに応じて診断結果が表示されます。※3 管理者があらかじめ設定した診断項目ごとの対処方法を表示させることができます。

脆弱性情報を効率的に取得、迅速なアップデート対応をサポート

CPE製品名管理

多くの組織では、利用しているソフトウェアの脆弱性を管理する際、ソフトウェアと脆弱性情報との紐づけを人手をかけて行っています。そのような手間を軽減するため、SAMACとIPAは共同で、SAMACソフトウェア辞書※4とJVN※5の脆弱性情報を製品識別子CPE※6で紐づけ、データ連携を行うことで脆弱性管理の効率化を支援する仕組みを用意しています。SKYSEA Client Viewでは、この仕組みを活用。SAMACソフトウェア辞書をインポートすることで、CPEを含む辞書のソフトウェア情報と、SKYSEA Client Viewのソフトウェア資産情報が自動で紐づき、CPEを基に組織で利用しているソフトウェアの脆弱性情報をJVNから確認することができます。



最新の脆弱性情報が必要な場合は……
JVNから直接情報を取得し確認

SAMACソフトウェア辞書は数か月ごとに更新されるため、本辞書をインポートするだけでは、最新の脆弱性情報を把握することが困難な場合もあります。そこで、JVNから最新の脆弱性情報を取得できる機能も搭載。任意のソフトウェアを検索し、最新の情報を確認することができます。また、新たな脆弱性情報を取得した際に、管理機に通知することも可能です。

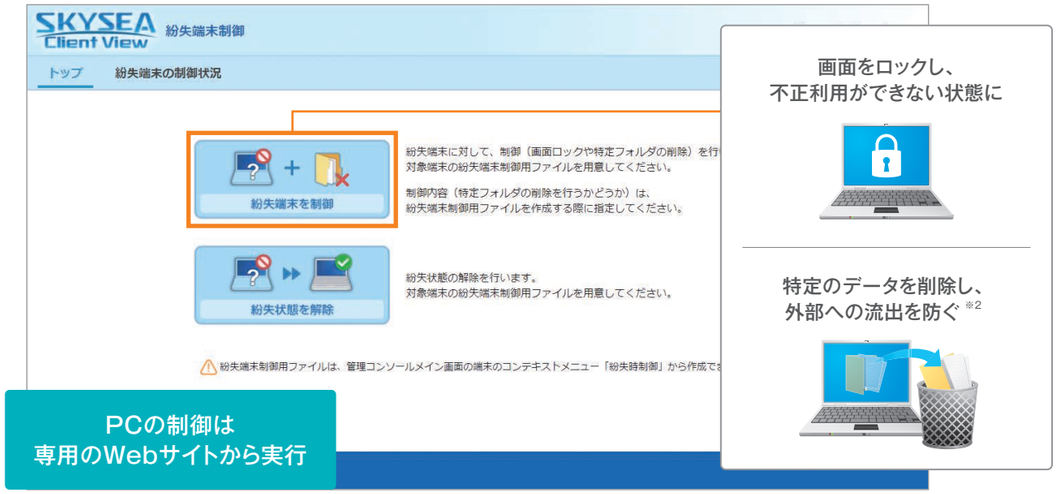
※4 一般社団法人IT資産管理評価認定協会（SAMAC）が提供する、国内外で一般公開されているソフトウェアに関する情報を収録したマスターデータ。保守契約をいただいているユーザー様に向けて、保守契約ユーザー用Webサイトでご提供しています。 ※5 日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイト。正式名称は「Japan Vulnerability Notes」。※6 情報システムを構成するハードウェアやソフトウェアなどを識別するための名称の基準。

紛失したPCをリモートロックし、情報漏洩を防ぐ

紛失端末制御※1

オプション（Ent/Pro/Tel/LT/500/ST）

テレワークなどで会社貸与のPCを社外に持ち出す場合は、万が一の紛失・盗難への対策が重要です。「紛失端末制御」機能は、紛失・盗難に遭ったPCに対して、画面ロックやデータ削除をインターネット経由でリモート実行でき、PC内のデータを第三者が扱えないようにすることで情報漏洩を防ぎます。また、PCが接続しているWi-Fi機器などを基に、大まかな位置情報を確認することも可能です。



PCの位置情報の確認も可能

専用のWebサイトでは、紛失したクライアントPCの位置情報も確認できます。地図上で視覚的に把握し、捜索に役立てることができます。※3

地図データ©2021 Google

発見したPCはマルウェア感染を考慮し、オフラインでロックを解除

紛失したPCには、マルウェアなどが第三者に仕込まれている可能性があり、感染拡大を防ぐためにも発見時にオフラインでPCを調査する必要があります。本機能では、管理機で発行した解除用パスワードをPCに入力することで、オフラインのまま画面ロックを解除することができます。

閉域網の環境にも対応※4

インターネットから分離された閉域網の環境でも、本機能をご利用いただけます。その場合、紛失したPCの制御等は閉域網内にあるマスターサーバーを通じて行われます。

※1 紛失したPCがインターネットに接続できる状態であることが必要です。※2 削除対象はあらかじめ、フォルダ単位で指定します。※3 PCの位置情報は主に、使用しているWi-Fi機器やIPアドレスを基に取得します。Wi-Fi機器と位置情報が紐づけられたGoogleのデータベースの情報から位置を特定したり、IPアドレスを割り振るプロバイダの所在地情報から推定します。そのほか、携帯電話基地局からの取得も行えるため、SIMカードを利用したモバイル通信を行うPCの位置情報も取得可能です。加えてGPS機能を搭載したPCに限り、GPSを利用した位置情報も取得できます。 ※4 閉域網の環境で利用する場合は、紛失したPCに専用のSIMカードなどが挿入されており、閉域網内のマスターサーバーと接続できる状態であることが必要です。

EDR製品と連携し、マルウェア対策のさらなる強化を支援

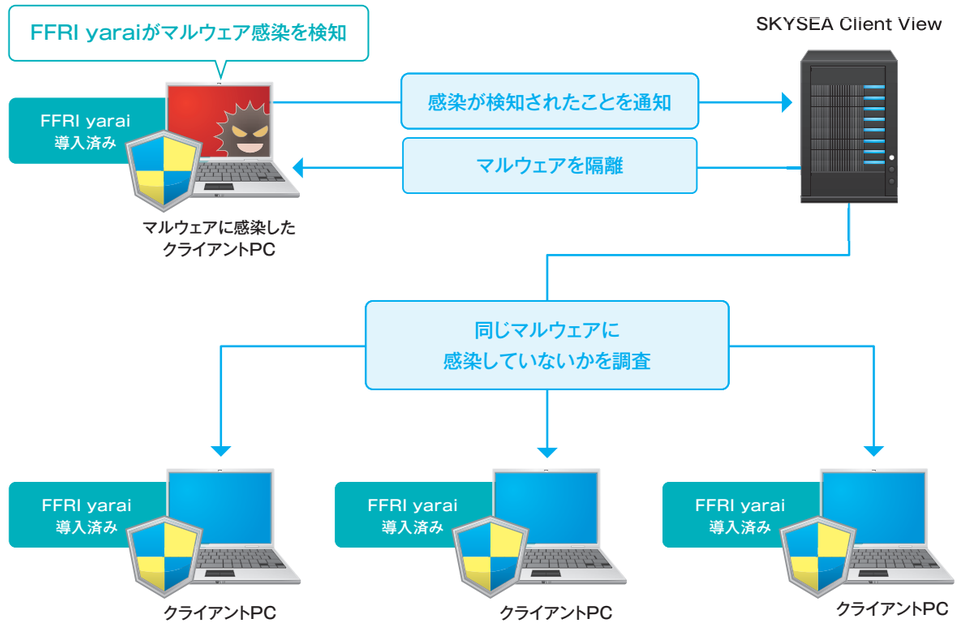
組織内マルウェア情報

オプション※5（Ent/Pro/Tel/LT/500/ST）

FFRIセキュリティ社製「FFRI yarai」がクライアントPCのマルウェア感染を検知した際、「SKYSEA Client View」がPC上のマルウェアを隔離します。また、検知したマルウェアの情報を基に、ほかのクライアントPCが同じマルウェアに感染していないかを自動で調査し、マルウェアが確認された場合は同様に自動で隔離します。

「FFRI yarai」とは……

パターンファイルを基にした従来の手法では検知が難しいゼロデイ攻撃などに対して、マルウェア特有の振る舞いを検知することで未知の脅威の早期発見をサポートする、次世代エンドポイントセキュリティ製品です。



PCの操作ログから感染原因を調査

検知したマルウェアに関する情報や感染したPCの操作ログは、専用の管理画面からすぐに確認できます。感染原因の調査など、事後の対応にお役立ていただけます。

※5「EDRプラスパック」オプション、または「EDRプラスパックCloud」オプションが必要です。

Windows 10の継続した更新管理を支援

定期的に公開されるWindows 10の更新プログラムの、管理・配布を支援する機能もご用意。PCを常に最適な状態に保ち、安全にご利用いただけるようスムーズな更新管理をサポートします。

品質更新プログラムのスムーズな取得・適用を支援

■ 更新プログラム配布管理

保守契約ユーザー用WebサイトからWindows 10などの更新プログラム情報を一覧で取得・インポートすることで、マイクロソフト社（Microsoft Corporation）が公開する更新プログラムのダウンロードから、PCへの配布・適用までを管理画面上で一括管理することができます※1。

※1 Windows 10の更新プログラムについては、品質更新プログラムに対応しています（2021年9月現在）。また、更新プログラム情報の一覧を取得する際は、初回のみWebサイトにて利用者情報の登録が必要です。

デバイス管理

デバイスやメディアの適正管理で、個人 / 機密情報の漏洩防止を支援

USBメモリなどの記憶媒体は大量のデータを手軽に持ち運ぶことができる反面、紛失などによって重要情報が漏洩し、企業の信用を失う危険性もはらんでいます。本機能を活用し、USBデバイスやメディアを1台ずつ適切に管理、細やかに使用制限を設定することで、組織の大切な情報を守るお手伝いをいたします。

※2 PCに内蔵されているカードリーダーや、CD / DVD / ブルーレイディスクドライブを含みます。※3 メディア登録時は別途、管理番号やメディア種別などの登録が必要です。また、台帳登録済みのメディアをフォーマットすると、未登録のメディアと判断され、再度登録する必要があります。

使用不可、読み取り専用など実運用に合わせて柔軟に設定

USBデバイス / メディア使用制限

デバイスやメディア1台ずつに対して使用制限を設定できます。データのやりとりが多い部署は「読み取り専用」、それ以外の部署は「使用不可能」にするなど、組織の運用に沿った管理が可能です。

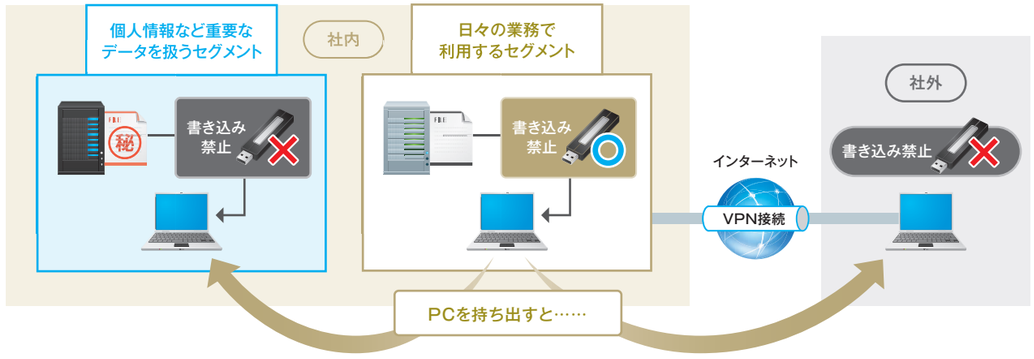
デバイス種別制御

各イラストをクリックするだけで、デバイス種別ごとの使用制限が切り替えられます。個別のデバイスの設定と組み合わせることもできます。

セグメントごとにデバイス使用を制限、データの持ち出しを抑止

セグメントごとのデバイス制御 / 印刷禁止

ネットワークのセグメントごとに、USBデバイスやメディアの使用を制限できます。例えば、日々の業務で利用するセグメントではデバイスの使用を許可し、個人情報など重要なデータを扱う別セグメントでの使用を禁止することで、使用範囲を限定。データの不要な持ち出しを抑止します。また、社外からのVPN接続による社内データの書き込みも禁止できます。



セグメントごとに印刷の制限も可能

セグメントごとに印刷も制限できます。社外でPCを利用する場合などに、誤って社内のプリンターを指定して印刷してしまうことがないようにし、印刷物を放置することによる情報漏洩リスクを抑止します。

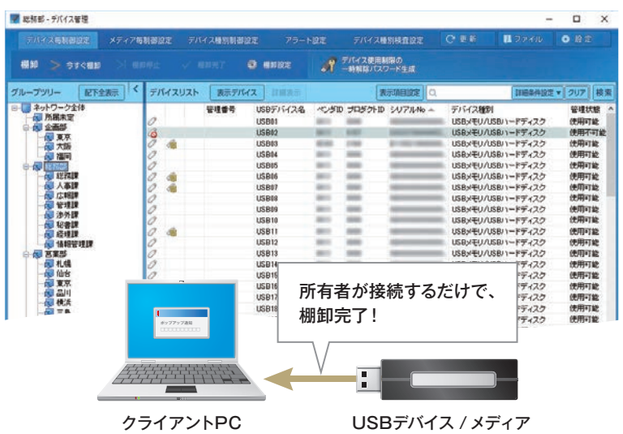
接続すると棚卸が完了、所有確認を効率的に

USBデバイス / メディア棚卸 特許取得

指定日時に棚卸依頼メッセージを各PCに送信。デバイス(メディア)をPCに接続するだけで所有確認が完了します。管理対象デバイス(メディア)の数が膨大な場合などに、棚卸の負担を軽減します。

USBデバイスファイル確認 【関連特許取得】

USBメモリなどの紛失時に、USBメモリ内に重要なデータが記載されていなかったかを素早く確認でき、初動対応を迅速に行えます。



USBデバイスの利用申請・承認をWebシステムで管理

申請・承認ワークフローシステム

オプション(Ent/Pro/Tel/LT/500/ST)

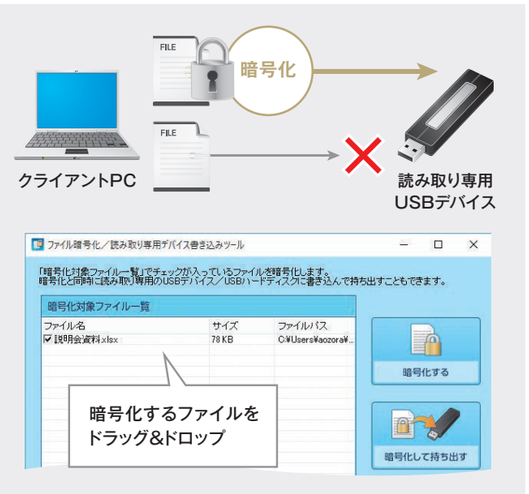
USBデバイスの利用申請、承認がWebブラウザ上で管理できます。事前に設定したフローに沿って申請、承認を行うことで、煩雑になりがちな申請の流れを明確にし、日々の申請業務の効率化を支援します。

USBメモリによるデータの持ち出しをより安全に

取り扱いファイル暗号化

オプション(Tel/LT/500/ST)

USBデバイスによる重要データの持ち出し時に、クライアントPC上でファイルを暗号化できます。読み取り専用デバイスに対しても、暗号化したファイルのみ保存できるように設定でき、持ち出し時のセキュリティ強化につながります。



暗号化ファイルの復号を組織内に限定 特許出願中

暗号化ファイルの復号を、組織内のPCでしか行えないように設定し、使用範囲を限定することで、セキュリティをさらに強化していただけます。

本機能はUSBメモリなどでのファイル持ち出しにご利用いただくことを想定したファイル暗号化機能であるため、ご利用を検討される際には、お客様の使用用途に適合しているかのご確認をお願いいたします。暗号化によるセキュリティをさらに重視される場合には、日本電気株式会社製「InfoCage ファイル暗号」や、富士通株式会社製「FENCE」シリーズなどの製品をお使いいただきますようお願いいたします。なお、「InfoCage ファイル暗号」および「FENCE」シリーズについては、SKYSEA Client Viewと共存してご利用いただくことが可能です。(メーカー様は五十音順にて記載しております)

デバイスの書き込みやアップロードするファイルの暗号化を徹底

外付けデバイス&ファイル暗号化

オプション（Ent/Pro/Tel/LT/500/ST）

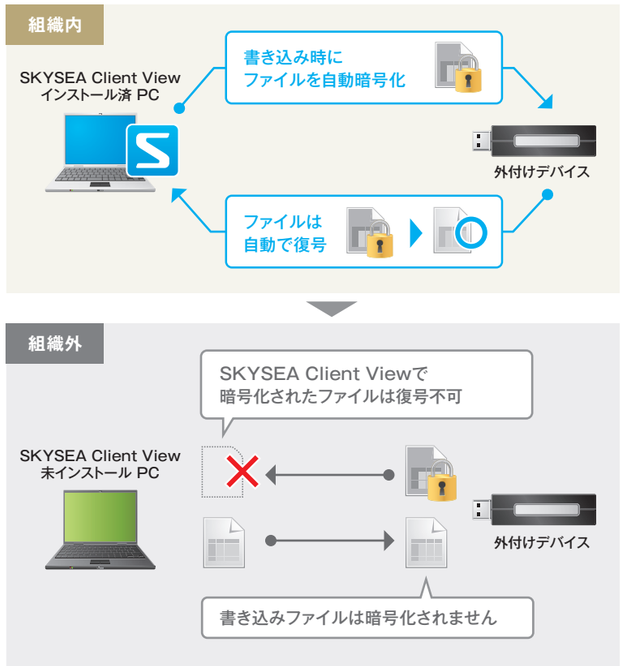
外付けデバイスに書き込むファイルや、Webアップロードを行うファイルの暗号化を徹底し、万が一の情報漏洩に備えた対策を支援します。

紛失・盗難などのリスク対策に、外付けデバイス内のファイルを自動で暗号化※1

外付けデバイスを使って組織内でファイルをやりとりする際に、書き込んだファイルを自動で暗号化します※2。暗号化されたファイルは、組織外のPCでは復号できないため、セキュリティを強化していただけるほか、暗号化 / 復号は組織内のPC※3接続時に自動で行われるため、ユーザーは意識することなくデバイスを利用することができます。

本機能のような暗号化に限らず、データの取り扱いに際しては、ソフトウェアのバグなどがなくてもハードディスクの破損などでデータを損失するリスクがあります。お客様の環境に合わせて、データのバックアップを取るなどの運用を行っていただくことをお勧めします。

※1 外付けデバイス本体を暗号化するものではございません。
※2 事前に暗号化対象となる外付けデバイスを指定しておく必要があります。
※3 外付けデバイスのドライブを暗号化したPCと同一のマスターサーバーに所属するPCを指します。



外付けデバイス利用時に、ユーザーへ各種メッセージを通知

組織外へのファイル持ち出しに利用できないことを通知

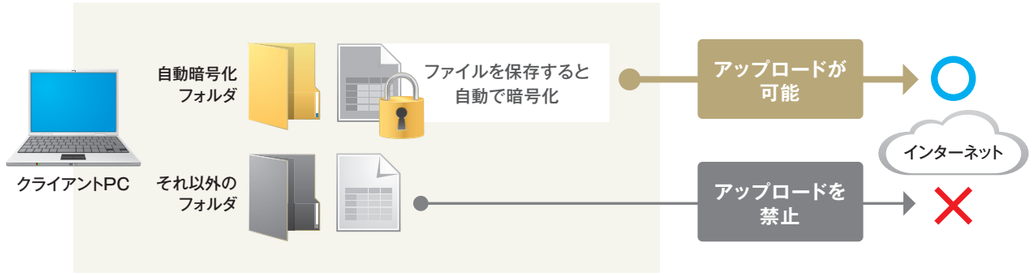
暗号化設定を行った外付けデバイスに「取り扱いファイル暗号化」機能（P.42）などでファイルを保存しようとした際、組織外で利用できないデバイスであることを事前に通知できます。

暗号化が無効な状態であることを通知

フォーマットなどで暗号化が無効となった外付けデバイスがPCに接続された際、暗号化が必要な状態であることを通知できます。暗号化が有効なデバイスのみ利用を許可している場合に、ユーザーへの注意喚起にお役立ていただけます。

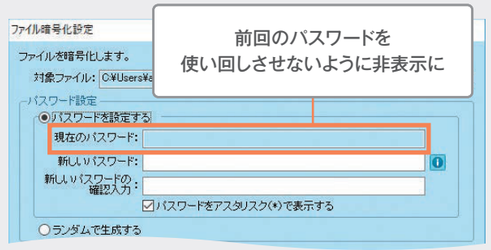
暗号化されたファイルのみWebアップロードを許可し、セキュリティを強化

ファイルを保存すると自動的に暗号化が行われる「自動暗号化フォルダ」をPC上に作成し、フォルダ内の暗号化ファイルのみWeb上へのアップロードを許可することができます。Webメールでファイルを送信する場合などに添付ファイルの暗号化を強制させることで、安全なデータ共有を支援します。



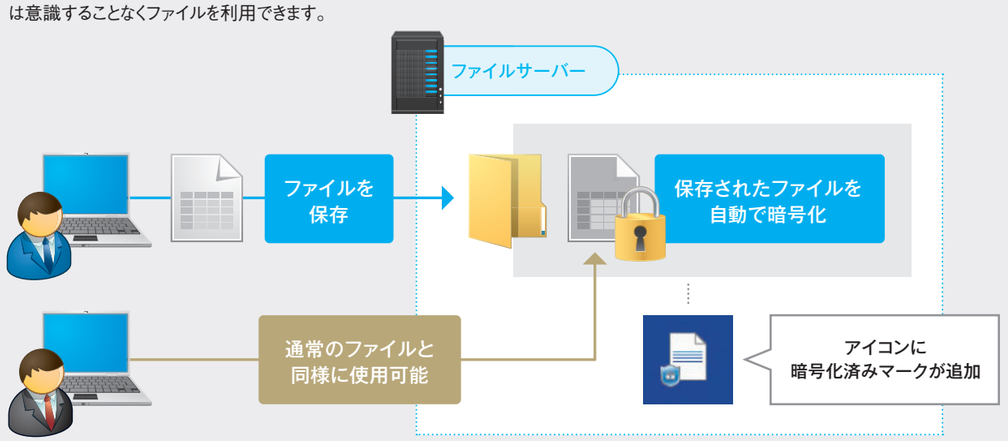
復号用のパスワードの使い回しを禁止

ファイルを暗号化する各PCのユーザーが復号用パスワードを設定するように運用している場合に、前回設定したパスワードを非表示にすることができます。パスワードを使い回せないようにし、暗号化ファイルのセキュリティを強化します。



共有フォルダ上のファイルを自動で暗号化、ファイル流出時の被害を最小限に

ファイルサーバー上の特定の共有フォルダを「自動暗号化フォルダ」として設定し、個人情報など重要データをやりとりするフォルダでの暗号化を徹底できます。組織内のPCからフォルダ内のファイルを利用する場合は暗号化 / 復号が自動で行われるため、ユーザーは意識することなくファイルを利用できます。

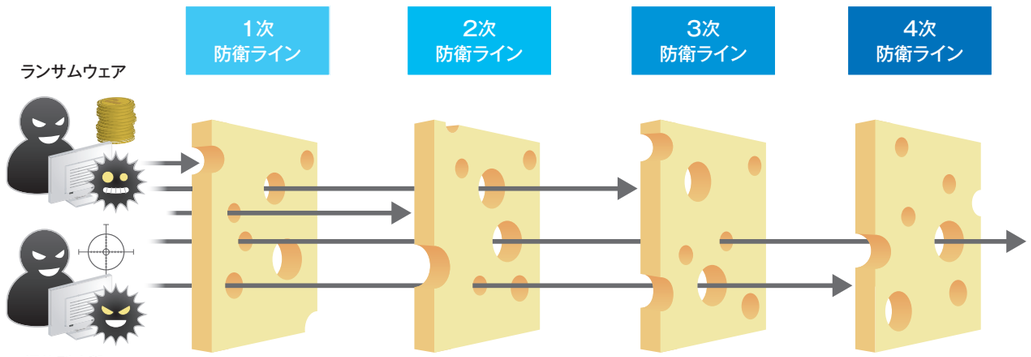


ITセキュリティ対策強化

オプション（LT/500/ST）

猛威を振るうサイバー攻撃に
多層防御による情報漏洩対策を

日々進化し、悪質化が進む標的型攻撃やランサムウェアなどのサイバー攻撃。SKYSEA Client Viewでは、UTM※1製品などと連携してサイバー攻撃の早期把握を支援する機能や、共有フォルダへのアクセスを監視・制御する機能などの各種機能をまとめた「ITセキュリティ対策強化」機能をご用意。階層的な防御でサイバー攻撃のリスク最小化を支援します。



ファイアウォール / IPS / サンドボックスなど / UTM

SKYSEA Client View

エンドポイントセキュリティ（ウイルス対策ソフトウェアなど）

連携

- UTM製品と連携し、サイバー攻撃を早期把握

連携

- エンドポイントセキュリティ製品と連携、ウイルスなどを検知したPCを遮断

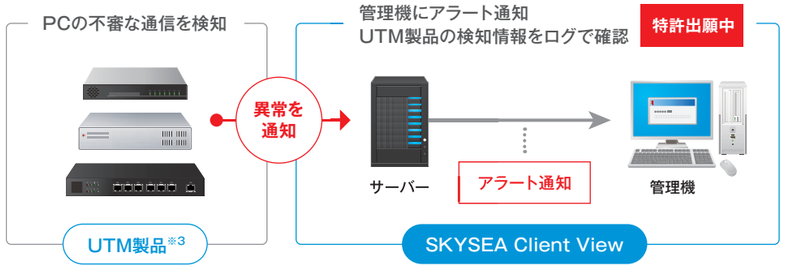
- 共有フォルダへのアクセスを検知・制御
- 社外での通信制限 / 手動でのネットワーク遮断
- アラート情報をsyslog出力し、他社製品で活用
- ZIPファイル内の各ファイル名をログとして記録
- アプリケーションログで起動元プロセスを特定
- ソフトウェア配布で更新プログラムを強制実行※2

※1 UTM（Unified Threat Management）：統合脅威管理。※2 本機能は、Professional Editionやテレワーク Editionにおいてはオプションとなります。

UTMが検知した異常をアラート通知、マルウェア侵入を早期把握

UTM連携

不正侵入検知・防止機能（IPS）などを搭載した各メーカー様のUTM製品と連携。UTM製品がマルウェア侵入などによる不審な通信を検知した際に出力する「syslog」や「SNMPトラップ」を基に、素早くアラートで通知します。これらの通信が検知されたPCは、組織内ネットワークから自動的に遮断するように設定することもできます。



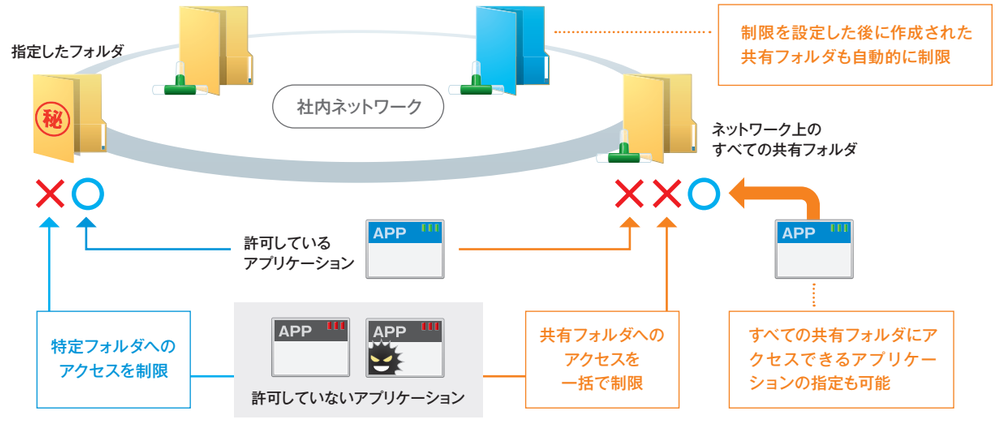
不審な通信の例

- ウイルスなどのマルウェアを拡散しようとする通信
- マルウェア感染などの可能性がある危険なWebサイトへのアクセス
- ボットネット※4やC&Cサーバー※5への通信 など

社内の共有フォルダへのマルウェアのアクセスを抑止

特定フォルダアクセス アラート設定※6

許可したアプリケーション以外による特定フォルダへのアクセスを制限したり、ネットワーク上に作成された共有フォルダへのアクセスを一括で制限できます。クライアントPC上に作成された共有フォルダに対するアクセスも制限でき、管理者が把握できていない共有フォルダからの情報漏洩の防止にお役立ていただけます。



※3 連携する各メーカー様の製品については、P.71「協業・連携ソリューション」をご覧ください。※4 ボットネット：ウイルスなどにより攻撃用プログラム（ボット）を送り込まれ、悪意ある攻撃者に遠隔操作されている多数のPC / サーバー群で構成されたネットワーク。※5 C&C（Command and Control）サーバー：サイバー攻撃において、攻撃者がインターネットからPC上のマルウェアに対して不正コマンドを送信し、PCを遠隔操作するために用いられる指令サーバー。※6 「ITセキュリティ強化」機能を導入していない場合は、指定したフォルダへのアクセス検知のみ行えます。

社内外でのPCのネットワーク接続を制御

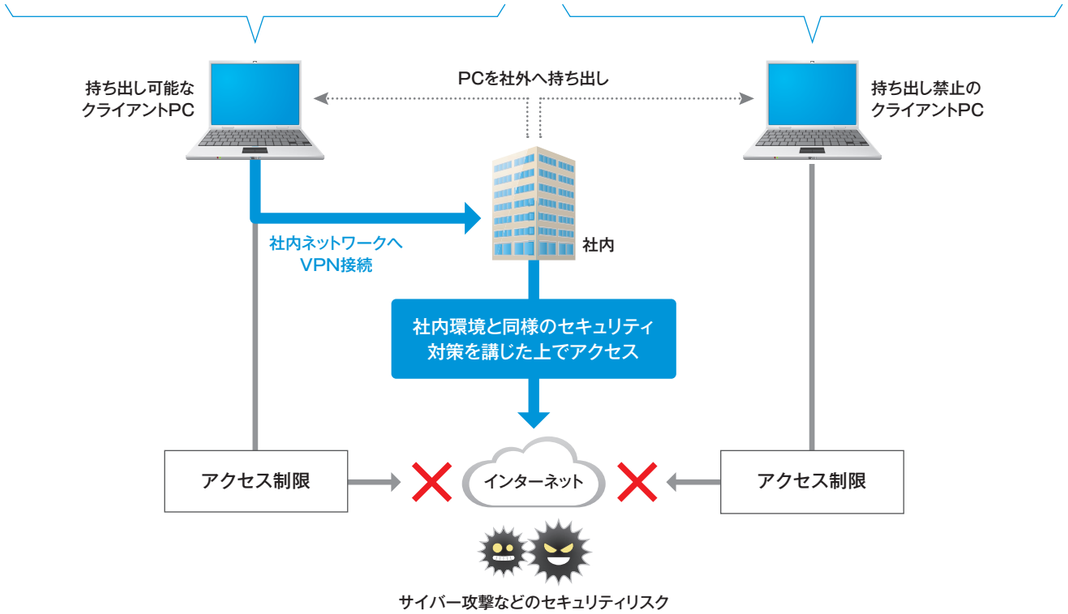
組織外ネットワーク接続（デフォルトゲートウェイ / VPN・プロキシサーバー）

社内ネットワークへ強制的にVPN接続、社外からのインターネット利用をよりセキュアに

公衆無線LANや出張先のホテルの有線LANなどを利用して、社外から直接インターネットにアクセスする場合は、社内に比べてマルウェア感染などのセキュリティリスクが高まります。社外からインターネットにアクセスする際に、強制的に社内ネットワークを経由させることで、社内でPCを使用する場合と同様のセキュリティ対策を講じることができます。

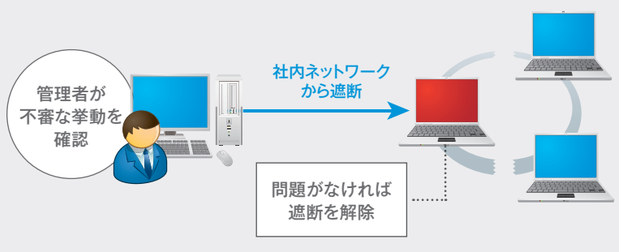
持ち出し禁止のPCに対して、社外でのインターネット利用を制限

PCが事前に指定したネットワーク外に持ち出された際に、自動的にインターネットへのアクセスを制限することができます。例えば、社外への持ち出しを禁止しているPCが万が一持ち出された場合でも、インターネットへのアクセスを制限することで、セキュリティリスクの軽減を支援します。



挙動が不審なPCに対し、管理者が手動でネットワークを遮断

負荷がかかる作業をしていないのにPCの通信速度が遅い、処理速度が遅いといった場合、何らかの問題が発生している可能性があります。そういったときに、まずは管理者が管理コンソール上で対象PCのネットワークを手動で遮断し、安全を確認した上で遮断を解除することができます。

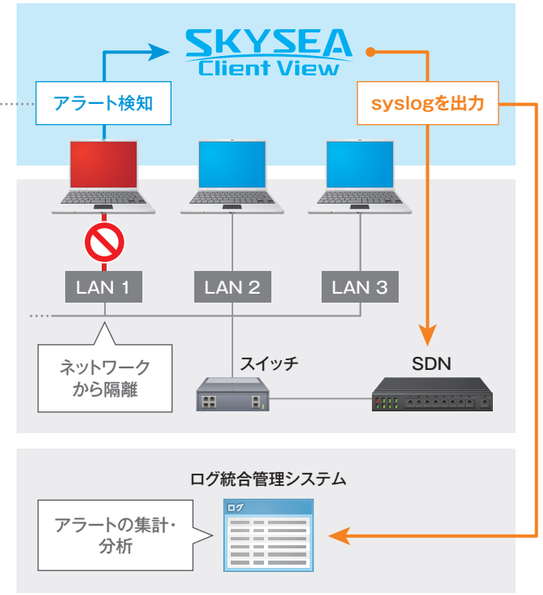


アラートをsyslog出力し、他社製品で情報漏洩対策などに活用

SKYSEA Client Viewアラート syslog出力

SKYSEA Client Viewが検知したアラート情報をsyslogとして出力し、他社製品で活用することができます。例えば、SKYSEA Client Viewが情報漏洩リスクを伴う操作を検知した際、SDN製品がsyslogを受信することでアラート端末をネットワークから自動で隔離したり、ログ統合管理システムがsyslogを基にアラートの集計や分析を行うことができます。

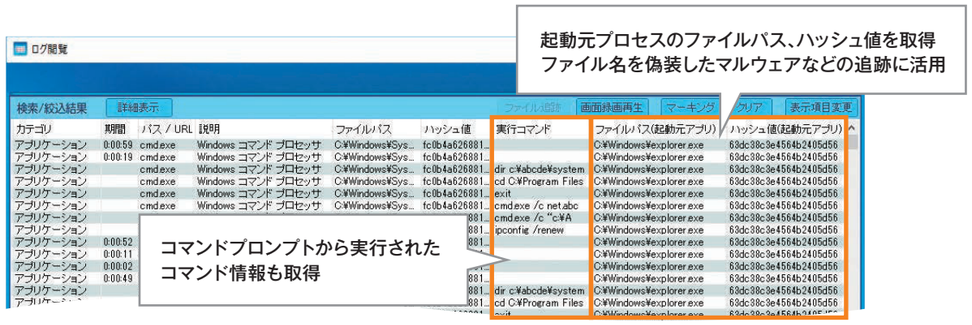
（UTMやウイルス対策ソフトウェアなどの連携製品が検知したアラートにも対応）



起動元プロセスを特定しマルウェアの追跡に活用

アプリケーションログの取得

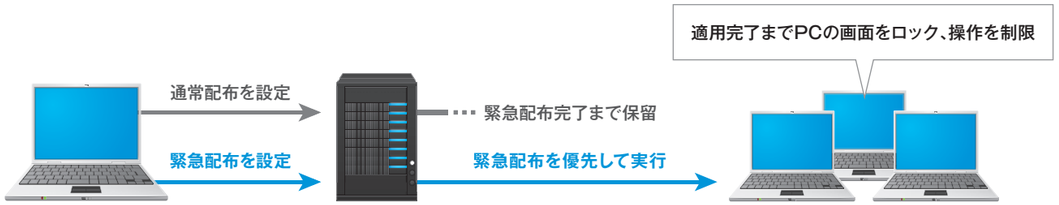
標的型攻撃で使われるマルウェアは、侵入したPC内のアプリケーションを利用して情報を抜き出すことが多いため、起動されたアプリケーションだけでなく、起動元まで特定できなければ、マルウェアによるものなのかを判断できません。アプリケーションログとして起動元プロセスに関する情報（ファイルパス、ハッシュ値など）や、コマンドプロンプトから実行されたコマンドに関する情報を取得することで、マルウェアの追跡にお役立ていただけます。



緊急性の高い更新プログラムを優先的に強制配布

ソフトウェアの緊急配布※1

事前に予約したソフトウェア配布を保留にし、更新プログラムなどを最優先で配布。脆弱性を突いた外部からの攻撃やマルウェア感染のリスクを最小限にするために、ベンダーから提供された更新プログラムを速やかに適用するお手伝いをいたします。

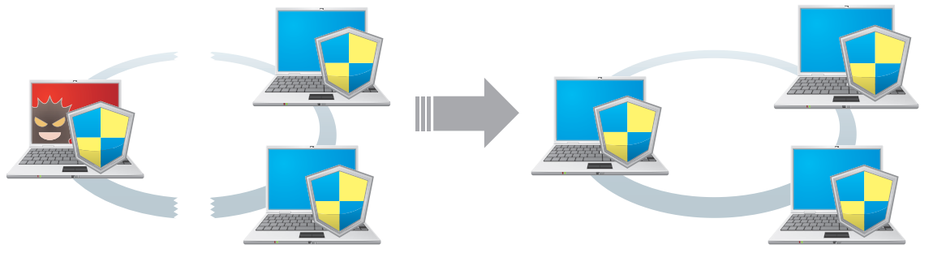


※1 本機能は、Professional Editionやテレワーク Editionにおいてはオプションとなります。

ウイルスを検知したPCを遮断、速やかな調査の実施を支援

検疫ソフトウェアイベントログ監視 / 検疫ソフトウェアレジストリ監視

ウイルス対策ソフトウェアなどの各種エンドポイントセキュリティ製品と連携し※2、ウイルス感染などの異常を検知したPCをネットワークから自動的に遮断※3。速やかな調査と安全性の確保を支援します。PCに問題がないことを確認できれば、ネットワークへ再接続することも可能です。



特定の通信先のみ接続も可能

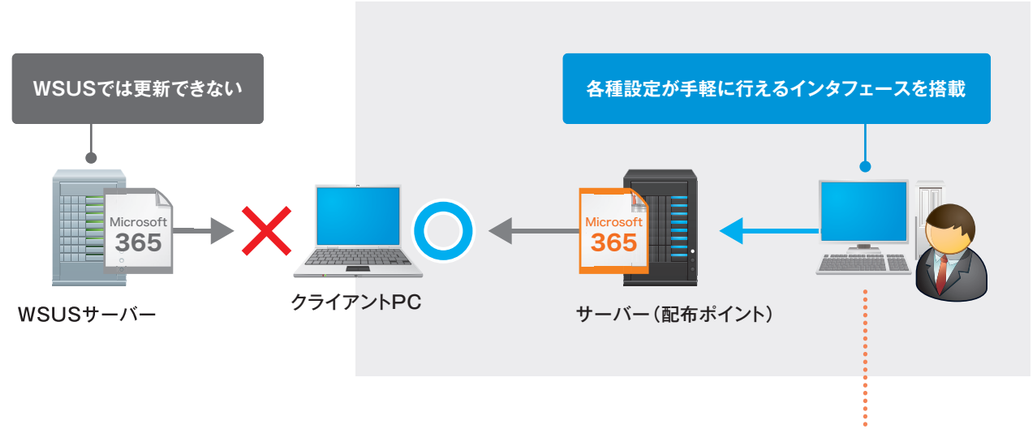
ネットワークから遮断する際に、SKYSEA Client Viewのサーバーなど、特定の通信先との接続のみを維持させることで、ログを活用してウイルスの侵入、感染原因の調査などを行っていただけます。

※2 連携する各メーカー様の製品については、P.71「協業・連携ソリューション」をご覧ください。※3 ネットワークから遮断せず、アラート通知のみ行うように設定することもできます。

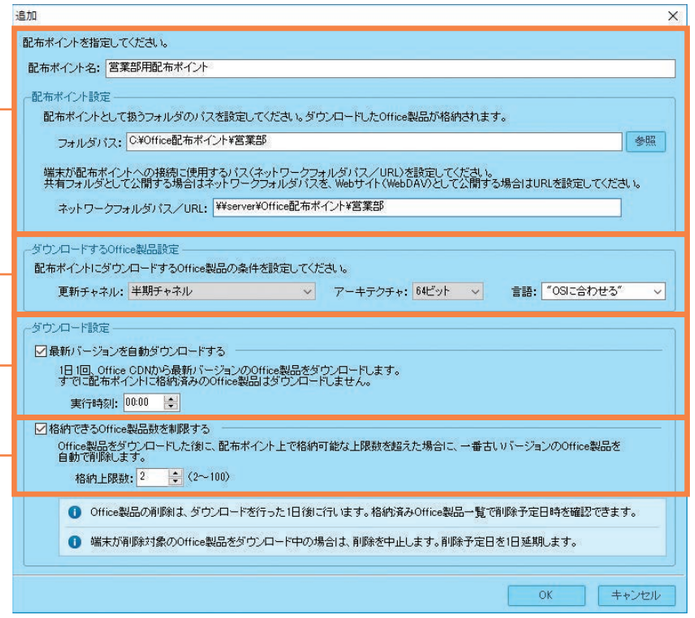
Microsoft 365 / Office 2019のアップデートをよりスムーズに

Microsoft Office更新制御

Microsoft 365 / Office 2019は、Windows OSと違い、WSUSサーバーからの更新プログラムの配布は行えません。代わりに、「配布ポイント」に指定されたサーバーから配布する方法が用意されていますが、この方法は複雑で設定にある程度のIT知識を要します。SKYSEA Client Viewは、配布に関するこれら設定が手軽に行えるインタフェースを搭載。部署ごとに複数の配布ポイントを設けることで、大規模環境でのアクセス負荷を分散させる運用も可能です。



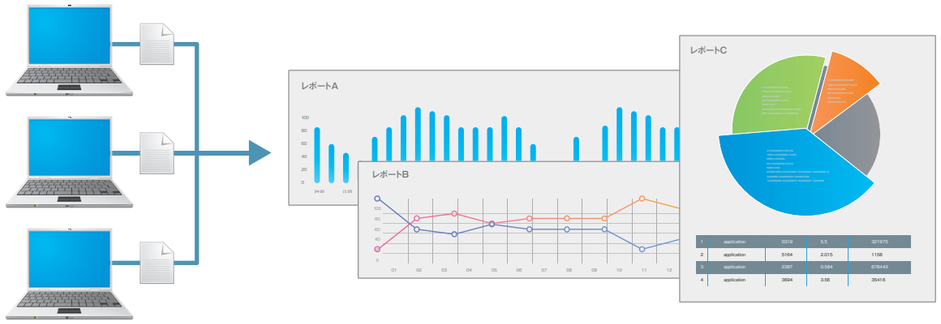
- アクセス負荷の分散のために、部署ごとなどに配布ポイントが指定可能
- ダウンロードする更新プログラムの種類を選択可能
- 最新バージョンの更新プログラムは自動でダウンロード
- 配布ポイントにある古いバージョンの更新プログラムは自動で削除



レポート

日々蓄積されるデータを活用し、IT資産運用の傾向を適切に把握

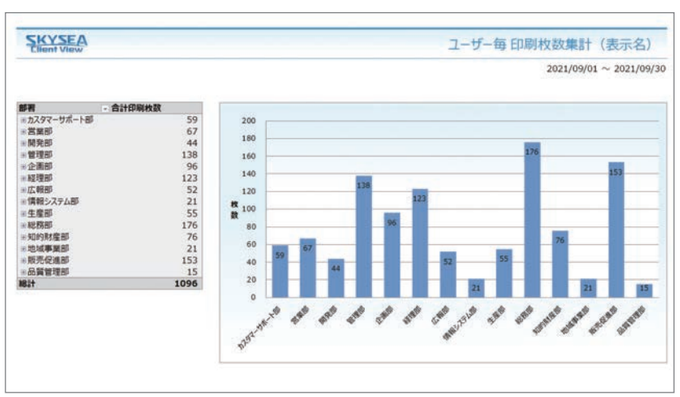
資産情報やログデータは、トラブルの原因特定や個別の操作の監視だけでなく、具体的な目的に応じてレポートとして集計することで、傾向を把握しながら変化を察知するツールとしても活用できます。各種レポートを分析することで、コスト削減やセキュリティポリシーの改善などにお役立ていただけます。



必要なレポートをダウンロードして活用

資産・ログ利活用レポートライブラリ

保守契約ユーザー用Webサイトから、必要な情報を含む最適なテンプレートをダウンロードし、レポートに集計。IT資産運用の傾向把握に活用いただけます。

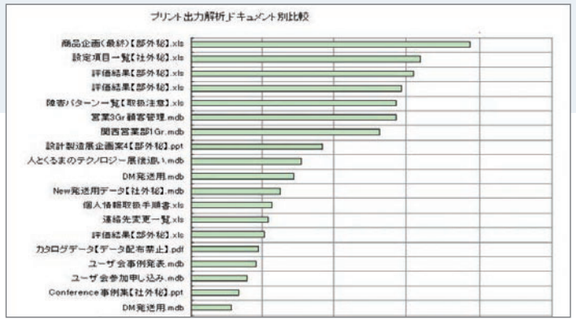


組織のさまざまなニーズに対応する各種レポートをご提供

社外秘、部外秘ファイルなどの出力状況の確認に

ドキュメント別プリント出力比較レポート

ドキュメントごとに、印刷枚数をグラフ表示。「社外秘」など、あらかじめ設定したキーワードを含むドキュメントに絞り込んで集計することも可能です。



長期間利用されていないPCの洗い出しに活用

末稼働端末一覧

1週間、1か月といった期間を指定して稼働していないPCをリストアップ。不要なPCの洗い出し、IT資産の有効活用にお役立ていただけます。

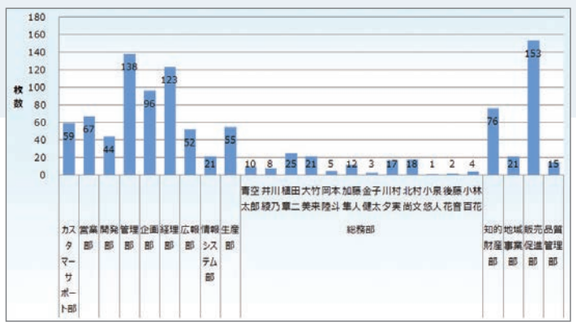
端末機稼働状況 未稼働端末一覧

No.	コンピューター名	部署名	前回起動日時
1	SkyPC00001	企画部	2021/09/17
2	SkyPC00002	企画部	2021/09/10
3	SkyPC00003	企画部	2021/09/09
4	SkyPC00004	企画部	2021/09/15
5	SkyPC00005	企画部	2021/09/22
6	SkyPC00006	企画部	2021/09/22
7	SkyPC00007	企画部	2021/09/22
8	SkyPC00008	企画部	2021/09/15
9	SkyPC00009	企画部	2021/09/16
10	SkyPC00010	企画部	2021/09/09
11	SkyPC00011	企画部	2021/09/08
12	SkyPC00012	企画部	2021/09/08
13	SkyPC00013	企画部	2021/09/15
14	SkyPC00014	企画部	2021/09/17
15	SkyPC00015	企画部	2021/09/17

指定した期間内のユーザーの印刷枚数を集計

プリンター印刷状況レポート

大量に印刷を行っているユーザー（PC）を確認することで、コスト削減の検討などにお役立ていただけます。



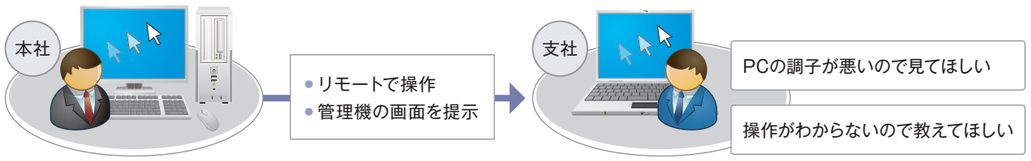
レポート一覧

集計・出力できるレポートの一覧は、SKYSEA Client View Webサイト（https://www.skyseaclientview.net/product/function/rep/）をご覧ください。

メンテナンス

離れた拠点のPCをリモート操作、メンテナンスや問い合わせ対応を効率的に

オフィスの各フロアに部署が点在する場合や、事業所が複数存在する場合などに、PCのメンテナンスや問い合わせ対応を行う際、自席の管理機から対象PCをリモート操作でき、作業の効率化にお役立ていただけます。



複数のPCを同時接続し、切り替えながら操作も可能

リモート操作

オプション（LT）

管理機の画面をクライアントPCのデスクトップに表示させたり、ファイル・テキスト・画像などを端末間で共有（転送）できます。

キーボード・マウス転送【関連特許取得】

オプション（LT）

同じ作業を複数のPCで繰り返し行う場合に、管理機のキーボード、マウス操作を各PCで一斉に実行できます。

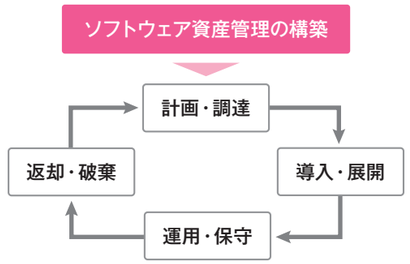
電源制御

管理機から、電源のON / OFFや、ログオン / ログオフ、再起動がリモートで行えます。管理機から各クライアントPCの電源状況を確認した上で、切り忘れ対応に活用したり、メンテナンスで再起動が必要な場合などに役立ちます。

ソフトウェア資産管理（SAM）

管理台帳でソフトウェア資産を複合的に管理し、導入・運用などの各フェーズでの業務を支援

「ソフトウェア資産管理（SAM）」に必要な管理台帳を用意し、ソフトウェア資産の適切な管理を支援。ソフトウェアメーカー様による監査への対応など、国際規格（ISO/IEC 19770-1:2006）などに準拠した適切なSAM計画に活用いただけます。



SKYSEA Client View が支援できること

- 資産対象範囲の特定
- 情報収集、調査（管理台帳の整備）
- リリース（配布、インストール）
- ソフトウェア情報（管理台帳）の更新
- ライセンス情報の登録
- ライセンスの割り当て
- 定期的な棚卸
- 廃棄PCのライセンス情報（台帳）の更新
- 不要ソフトウェアの廃棄（アンインストール）

ソフトウェアの導入状況を端末ごとに詳しく管理

導入ソフトウェア台帳

ハードウェア、ソフトウェア、ライセンス（部材）情報を紐づけることで、ソフトウェアがどの端末（ユーザー）でインストールされ、各端末（ユーザー）にどのライセンスが割り当てられているかを記録、管理します。

突合（とつごう）による齟齬（そご）の確認

台帳上の記録と、自動収集されたIT資産情報を突合※1し、齟齬※2を抽出して表示。棚卸などに活用でき、適切なソフトウェアライセンスの割り当てに役立ちます。

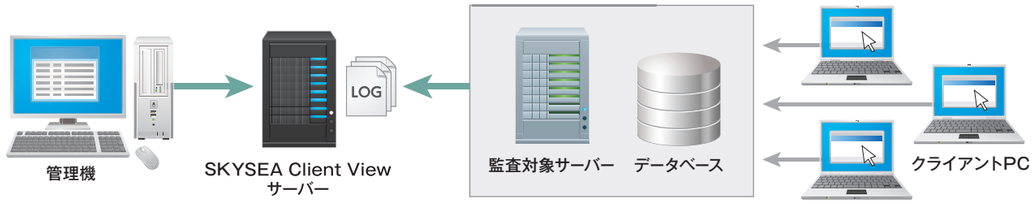
※1 突合（とつごう）：SAMにおいて、ソフトウェア利用状況や保有ライセンス数と、台帳の記録を照合すること。※2 齟齬（そご）：SAMにおいて、突合（※1）によって明確になった相違点。

サーバー監査

オプション（Ent/Pro/Tel/LT/500/ST）

重要データが集まるサーバーのアクセス状況の把握を支援

サーバーには個人情報や社外秘ファイルなど、重要なデータが集約されており、万全の情報漏洩対策が必要です。本機能では、各サーバーのイベントログを集積し、一括管理。権限のないユーザーからのアクセス状況や、データベースの取り扱い状況などの把握にもお役立ていただけます。



複数サーバーのログを1つの管理画面で検索・閲覧

OSログ閲覧

複数サーバーのイベントログをデータサーバーに集約。監査ログと併せて管理できます。操作の種類ごとに条件を絞って検索ができるため、必要なログが見つけやすく、調査がスムーズに行えます。

監査ログとは?

Windowsイベントログの一種で、主にセキュリティに関するログです。管理者が設定した監査ポリシーに従って書き出されます。

管理できるイベントログ種別
- アプリケーション
- セキュリティ
- システム など

管理できる監査ログ種別

▶ 管理者操作
- アカウント操作
- パスワード操作
- グループ操作
- 監査ポリシー操作 など

▶ クライアント操作
- ログオン
- ログオフ など

モバイル機器管理（MDM）

「SKYSEA Client View for MDM」オプション（Ent/Pro/Tel/LT/500/ST）としてご利用いただけます。

スマートフォン、タブレット端末のビジネス活用を支援

iPhone / iPad / iPod touch※1の資産情報などを管理するために、一般的なモバイルデバイスマネジメント（MDM）の一部である資産管理機能をご用意。BYOD※2の今後の普及を考え、また、プライバシーにも配慮し、ログ管理機能は搭載しておりません。また、同様の理由から、Apple社のMDM機能を活用したセキュリティ管理以外の機能は搭載しておりません。


iPhone / iPad など

資産管理	セキュリティ管理※3
モバイル端末の各種資産情報を一覧画面で適切に管理	業務に不要なアプリなどを使用不可に設定

ログ収集などのログ管理機能は搭載しておりません。

業務での必要性を考慮し、カメラなどの機能を制限

iPhone / iPad運用管理

組織での使用ルールを考慮し、日々の業務で必要がない、情報漏洩のリスクがある機能などを、あらかじめ使用禁止に設定できます。

制限できる機能例
- カメラ
- iTunes Store
- Safari
- iCloud
- Siri
- スクリーンショットの保存
- マルチプレーヤーゲーム
- アプリ内での購入 など

※1 iPhone / iPad / iPod touchの対応機種情報は、SKYSEA Client View Webサイト（https://www.skyseaclientview.net/ver17/mobile/）をご覧ください。※2 BYOD（Bring Your Own Device）：個人保有のモバイル端末を職場に持ち込み、業務で使用すること。※3 Windows端末に対して行えるセキュリティ管理でも、iPhone / iPad / iPod touchでは行えないものがあります。

機能一覧

Win＝Windows 端末　Mac＝Mac 端末　Lin＝Linux 端末　iOS＝iPhone / iPad / iPod touch　Ent＝Enterprise Edition
Pro＝Professional Edition　Tel＝テレワーク Edition　LT＝Light Edition　500＝500 Clients Pack　ST＝Standard Edition
標準＝標準環境（VPN環境）※1　HTTPS＝HTTPSゲートウェイ環境※2　S1=S1 Cloud Edition　S3=S3 Cloud Edition　OP=オプション

資産管理 ｜ 収集できる資産情報については、P.62をご覧ください。			対応OS			Edition						Cloud Edition 標準		Cloud Edition HTTPS	
			Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
資産情報収集	収集方法	● 資産情報インポート	○	○	○	●	●	●	●	●	●	●	●	●	●
		● スタンドアロン端末資産情報収集　● アンケート	○	—	—										
ネットワーク機器情報収集	収集方法	● IPアドレス指定によるネットワーク機器情報収集（手動、または定期自動収集） ● NetBIOS検索によるネットワーク機器情報収集（手動での収集） ● 不許可端末情報収集（ネットワーク接続時に自動収集） ● MIB情報更新（定期的に自動更新、または手動更新）	○	○	○	●	●	●	●	●	●	●	●	—	—
		● 収集した機器情報を資産情報として登録										●	●	●	●
	自動判別できる機器種別	・機器（Windows）　・サーバー（Windows Server）　・HUB ・機器（非Windows）　・サーバー（Windows AD Server） ・機器（Mac）　・プリンター ・機器（Linux）　・複合機				●	●	●	●	●	●	●	●	—	—
	手動設定できる機器種別	・ネットワーク機器　・Firewall　・CDメディア ・機器（Intel vPro テクノロジー対応）　・周辺機器　・DVDメディア ・サーバー（非Windows Server）　・その他　・Blu-rayメディア ・ソフトウェアインストールメディア ・ルーター　・プロジェクター ・IP電話	○	—	—							●	●	●	●
資産情報管理	ハードウェア一覧	● ハードウェア情報の一覧表示（※3）（ネットワーク機器情報、レジストリ情報を含む）　● 資産情報の検索グループ作成 ● 重複条件設定 ● 資産情報の表示設定　● CSVファイル入力（インポート） ● 資産情報の詳細表示 / 編集　● CSVファイル出力（エクスポート） ● 資産情報の検索 / 検索条件保存	○	○	○	●	●	●	●	●	●	●	●	●	●
		● ネットワーク機器の死活監視設定　● MIB情報を手動で更新 ● MIB情報更新設定	○	○	○							●	●	—	—
		● BitLockerやその他サードパーティ製品によるドライブ暗号化情報を収集 / 確認 / 出力	○	—	—	●	●	●	●	●	●				
	資産変更状況	● 変更状況の表示設定　● CSVファイル出力（エクスポート） ● 絞り込み表示設定													
	アプリケーション一覧	● ウイルス対策ソフトウェアインストール状況　● OSインストール状況 ● アプリケーションインストール状況　● CSVファイル出力（エクスポート）	○	○	○							●	●	●	●
		● Officeインストール状況	○	○	—										
		● Office展開 / 更新設定適用状況　● 実行ファイルインストール状況 ● Windows ストアアプリインストール状況　● 不許可ファイル検出状況 ● Windows更新プログラムインストール状況	○	—	—										
資産情報運用	省電力支援	● 省電力設定状況表示　● 電源切り忘れプリンター検索 ● 省電力設定を強制配布	○	○	○	●	●	●	●	●	●	●	●	●	●
	定期電源ON	● 電源ONスケジュールの設定（部署ごと、または端末機ごと） ● 電源ONスケジュール除外設定										●	●	—	—
	定期電源OFF	● 電源OFFスケジュールの設定（部署ごと、または端末機ごと）										●	●	●	●
	ソフトウェア配布・インストール（※4）	● ソフトウェア配布										● ※5	● ※5	● ※5	● ※5
		● ソフトウェア配布（即時配布）										● ※5	● ※5	—	—
		● ソフトウェア配布スケジュール設定　● ソフトウェア配布スクリプト自動生成ツール ● 配布したソフトウェアのインストール状況確認　● ソフトウェア配布中継 ● 配布するソフトウェアの分類登録　● ソフトウェア配布バック ● ソフトウェア配布自動実行設定										●	●	●	●
		● マルチキャスト配布										●	●	—	—
		● キャッシュ配布										●	●	●	●
		● キャッシュ配布（キャッシュ端末検索期間中のダウンロード開始）	○	—	—	●	●	●	●	●	●	●	●	—	—
		● 端末機側での配布ソフトウェア優先実行										●	●	●	●
		● 配布 / 実行状況の確認　● 配布 / 実行前後の電源ON / OFF / スリープ状態の切り替え										●	●	—	—
		● 実行ファイル / Windows更新プログラム配布										●	●	●	●
		● 実行ファイル / Windows更新プログラム配布（即時配布）										●	●	—	—
	Windows更新プログラム配布実行	● 配布実行										●	●	●	●
		● 配布実行（即時配布）										●	●	—	—
		● 配布状況の確認										●	●	●	●
	Intel vPro テクノロジー対応	● 電源制御（強制シャットダウン / 強制再起動 / 無線LANでの電源ON） ● ブルースクリーン状態のリモート操作 ● リモート操作中のBIOS設定										●	●	—	—
	その他	● Webブラウザ上での資産情報閲覧（※6）										—	—	—	—
		● 部署インポート	○	○	○							●	●	●	●

資産管理 ｜ 収集できる資産情報については、P.62をご覧ください。			対応OS			Edition						Cloud Edition 標準		Cloud Edition HTTPS	
			Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
資産情報運用	その他	● 資産情報の自動定期バックアップ	○	○	○	●	●	●	●	●	●	—	—	—	—
		● 端末機振り分け　● IPアドレスの使用状況管理 ● 端末機No.の重複検知　● 廃棄済み端末機の資産情報を個別管理	○	○	○							●	●	●	●
		● インターネット経由での資産情報収集・管理	○	○	—							OP	OP	●	●

ログ管理※7 ｜ 収集できるログについては、P.63をご覧ください。			対応OS			Edition						Cloud Edition 標準		Cloud Edition HTTPS	
			Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
ログ収集	収集方法	● 時間指定ログ収集　● リアルタイムログ収集　● ネットワーク接続端末ログ収集	○	○	—	●	●	●	●	●	●	●	●	●	●
		● スタンドアロン端末機ログ収集	○	—	—										
	ログ閲覧（ビューアー）	● 検索　● CSVファイル出力（エクスポート）　● ログ情報の詳細表示 ● 検索条件保存　● 操作ログ追跡（※8） ● ファイル追跡　● 全データサーバーからログを検索	○	○	—										
ログデータ保存		● ログデータのバックアップ	○	○	—	●	●	●	●	●	●	● ※9	● ※9	● ※9	● ※9
		● バックアップデータ閲覧　● バックアップ時のデータ圧縮										●	●	●	●
		● ログデータの自動定期バックアップ										● ※9	● ※9	● ※9	● ※9
		● 削除された端末機のログを閲覧（※10）　● ログデータ保存先を端末機ごとに設定する ● ログデータを圧縮して保存　● ログデータの再回収 ● 保存済みのログ、バックアップログを圧縮										●	●	●	●
画面操作録画	録画方法	● スケジュール録画　● 検知録画　● ワンタッチ録画	○	—	—	OP	OP	OP	OP	OP	OP	—	—	—	—
	再生・保存	● 順再生 / 逆再生　● マルチディスプレイ録画データの保存・再生（最大4画面まで） ● 等速・2倍速・4倍速 ● 録画画像の切り出し / 静止画保存　● マイナンバー取扱端末の録画データを個別に保存 ● 録画データとログデータの個別保存、保存期間を別々に設定　● スタンドアロン端末機の録画データ収集													
	検索	● テキストログとの連動													
送信メールログ	送信メールログ	● 送信メール保存　● 添付ファイル保存	○	○	—	●	OP	OP	OP	OP	●	—	—	—	—
	一覧表示	● メール件名 / 送信者アドレス / 受信者アドレス / 添付ファイル有無													
	注意表示	● 管理機の画面にメッセージを表示（ポップアップ通知）　● 管理者へのメール通知 ● 許可ドメイン以外への送信を検知	○	—	—										
	設定	● メールサイズにより添付ファイルの保存、破棄を選択	○	○	—										
	検索	● 送信メールログ本文検索													
その他		● Web利用状況	○	○	—	●	●	●	●	●	●	●	●	—	—
		● インターネット経由でのログ収集・管理	○	○	—							OP	OP	●	●
		● 残業管理	○	—	—							●	●	●	●
		● 残業管理（残業申請Web承認（※11））　● 残業時間アラート	○	—	—	●	●	●	●	●	●	—	—	—	—
		● Web / アプリケーションアカウント利用状況	○	—	—							●	●	●	●
		● Webブラウザ上でのログ閲覧（※12）	○	—	—							—	—	—	—
		● 端末機の電源状態を操作し、ログを強制アップロード	○	—	—							●	●	●	●

セキュリティ管理 ｜ 設定できるアラート（注意表示）項目については、P.63をご覧ください。			対応OS			Edition						Cloud Edition 標準		Cloud Edition HTTPS	
			Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
注意表示通知	通知方法	● 管理機の画面にメッセージを表示（ポップアップ通知）　● アラート端末の自動解除設定 ● キーワードごとにアラート通知のON / OFFを設定	○	—	—	●	●	●	●	●	●	●	●	●	●
		● 端末機の画面にメッセージを表示（ポップアップ通知）（※7※13）　● 注意表示ログ出力（※7※13） ● メールによる通知（※7※13）　● 一定時間内のアラート / メールの集約（※7※13） ● アラート優先順位別表示設定	○	○	—										
注意表示設定	設定	● 端末機 / ユーザーごとの個別設定（※7※14）　● 設定内容の一覧表示 ● グループごとの設定（※7※14）	○	○	—	●	●	●	●	●	●	●	●	●	●
		● アラート項目別優先順位設定　● アラート優先順位別表示設定	○	○	○										
		● アラート項目別定期検知設定　● 検知時に実行するファイル（コマンド）の設定 ● スタンドアロン端末機の設定	○	—	—										
不許可端末検知 / 遮断	注意表示	● 不許可端末を一覧表示　● 管理者へのメール通知 ● 管理機の画面にメッセージを表示（ポップアップ通知）	○	—	—	●	●	●	●	●	●	●	●	—	—
	遮断（※15）	● 検知した不許可端末をネットワークから遮断				●	●	OP	OP	OP	●	—	●	—	—
WSUS連携		● Windows Updateの実行スケジュール設定（部署ごと、または端末機ごと）　● WSUSクライアント設定	○	—	—	●	●	●	●	●	●	●	●	●	●
Windows 10 更新制御		● 機能更新プログラムの自動適用を制御　● 通信カード（モデム）/ Wi-Fi接続 / テザリングによるWindows Update 制御設定	○	—	—	●	●	●	●	●	●	●	●	●	●
更新プログラム配布管理		● Windows更新情報ファイルの取得　● 指定したPCへの手動配布・適用 ● PC全台への自動配布・適用	○	—	—	●	●	●	●	●	●	—	—	—	—
CPE製品名管理		● CPE製品名の登録　● CPE製品名ごとの脆弱性情報の確認	○	○	○	●	●	●	●	●	●	●	●	●	●
紛失端末制御		● 画面ロック　● 特定フォルダ削除　● 位置情報表示	○	—	—	OP	OP	OP	OP	OP	OP	—	—	—	—
組織内マルウェア情報（EDRプラスパック）		● 検知ファイルの隔離・収集　● 他端末の感染有無の調査	○	—	—							OP	OP	OP	OP
		● 他端末の感染有無の調査（他端末への即時反映）				OP	OP	OP	OP	OP	OP	OP	OP	—	—
		● 隔離ファイルの復旧										OP	OP	OP	OP
その他		● SKYSEA Client Viewの通信セキュリティ設定（電子証明書発行 / 登録）　● SKYSEA Client Viewの通信受け付けネットワーク設定 ● Windowsファイアウォールの例外設定　● SKYSEA Client Viewの不正停止監視	○	—	—	●	●	●	●	●	●	●	●	●	●
		● PC環境を自動で診断	○	—	—	OP	OP	OP	OP	OP	OP	—	—	—	—

デバイス管理※7※16 ｜ 設定できるアラート（注意表示）項目については、P.63をご覧ください。

			対応OS			Edition						Cloud Edition			
												標準		HTTPS	
			Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
デバイス管理	登録・管理・棚卸	● USBデバイスの台帳自動登録 ● USBデバイス棚卸	○	○	—	●	●	●	●	●	●	●	●	●	●
		● USBデバイス台帳管理 ● USBデバイスファイル確認（※16※17）	○	—	—							●	●	●	●
		● Webブラウザ上での情報閲覧（※12）	○	—	—							—	—	—	—
		● スタンドアロン端末への管理情報設定 ● 接続時のウイルスチェック	○	—	—							●	●	●	●
	管理者設定	● USBデバイス登録設定 ● USBデバイス管理者承認	○	—	—							●	●	●	●
	使用制限（※7）	● 部署別使用制限 ● ユーザー / 権限グループ / 端末機別使用制限 ● USBデバイスの複数部署管理設定 ● デバイス種別制御	○	○	—							●	●	●	●
		● USBデバイスのパスワード設定解除検知 ● 使用制限の一時解除	○	—	—							●	●	●	●
	PCログオン認証	● USBメモリによるコンピューター使用制限	○	—	—							●	●	●	●
メディア管理（※18）	登録・管理・棚卸	● メディア棚卸 ● メディア台帳管理 ● メディアの台帳登録（※19）	○	—	—	●	●	●	●	●	●	●	●	●	●
		● Webブラウザ上での情報閲覧（※12）										—	—	—	—
		● スタンドアロン端末への管理情報設定 ● 接続時のウイルスチェック										●	●	●	●
	管理者設定	● メディア登録設定										●	●	●	●
	使用制限	● 部署別使用制限 ● メディア種別制御 ● ユーザー / 権限グループ / 端末機別使用制限										●	●	●	●
申請・承認ワークフローシステム		● デバイス利用申請（デバイスのみ）	○	○	—	OP	OP	OP	OP	OP	OP	—	—	—	—
		● ファイル持ち出し申請	○	—	—							—	—	—	—
取り扱いファイル暗号化		● ファイルの暗号化、読み取り専用デバイス / 光学メディアへの書き込み ● ファイルの復号	○	—	—	●	●	OP	OP	OP	OP	—	●	—	●
外付けデバイス暗号化（※20）		● デバイス内のデータの暗号化 / 復号 ● 特定フォルダ内のデータの暗号化 / 復号	○	—	—	OP	OP	OP	OP	OP	OP	—	—	—	—

ITセキュリティ対策強化 ｜ 設定できるアラート（注意表示）項目については、P.63をご覧ください。

			対応OS			Edition						Cloud Edition			
												標準		HTTPS	
			Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
セキュリティ管理		● 端末機ごとに手動でネットワーク遮断	○	—	—	●	●	●	OP	OP	OP	—	●	—	—
		● 各種操作ログのsyslog出力	○	○※21	○※21							—	●	—	—
	Microsoft Office更新制御	● 配布ポイントの管理	○	—	—							—	●	—	●
		● 配布ポイントの管理（管理機からの即時ダウンロード）										—	●	—	—
		● Microsoft Officeの更新（アップデート）設定の適用 ● Microsoft Officeの展開（インストール）設定										—	●	—	●
資産管理	資産情報運用	ソフトウェア配布・インストール（※4） ● ソフトウェアの緊急配布	○	—	—	●	OP	OP	OP	OP	OP	—	●	—	●
		● ソフトウェアの緊急配布（即時反映）	○	—	—							—	●	—	—

メンテナンス※7

		対応OS			Edition						Cloud Edition			
											標準		HTTPS	
		Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
リモート操作	● リモート操作 ● 全画面表示 ● 端末機画面を管理機で表示 ● 全画面表示（拡大表示） ● 複数同時リモート接続 ● 縮小表示（ズーム 0～100%） ● マルチディスプレイ時の操作画面の切り替え ● 等倍表示（自動スクロール / 手動スクロール） ● 操作対象の端末機上に、操作中である旨のメッセージを表示 ● 画面確認・リモート操作開始時、端末機側に許可を要求 ● リモート操作時の画面転送設定（※24） ● リモート操作中のカーテン機能	○	○	—	●	●	●	OP	●	●	OP	●	OP	OP
	● 管理機画面を端末機で表示 ● 端末機側のデスクトップへ描画 ● 特定アプリケーションの画面をマスクして表示 ● ミラードライバー設定 ● リモート操作中のファイル転送 ● リモート操作中のクリップボード連携	○	—	—	●	●	●	OP	●	●	OP	●	OP	OP
	● リモート操作時の自動画面録画（※25）										—	—	—	—
	● 複数端末機画面を管理機で巡回表示				●	●	●	●	●	●	●	●	—	—
	● リモート操作（インターネット経由）				OP	OP	OP	OP	OP	OP	OP	OP	OP	OP

メンテナンス※7

		対応OS			Edition						Cloud Edition			
											標準		HTTPS	
		Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
キーボード・マウス転送	● 複数端末機を一斉操作 ● 複数端末機のウィンドウ画面を代表画面にそろえる ● 一斉操作 / 単体操作の切り替え ● 操作中の端末機ロック ● 複数端末機のウィンドウ画面をセンタリング / 左上にそろえる	○	—	—	●	●	●	OP	●	●	OP	●	OP	OP
端末機制御	● 電源制御（電源ON・OFF / ログオン / ログオフ / 再起動） ● 電源ON・OFFスケジュール設定	○	—	—							●	●	—	—
	● アンケート配信 ● メッセージ配信	○	—	—							●	●	●	●
	● アンケート配信（即時配信） ● メッセージ配信（即時配信）	○	—	—	●	●	●	●	●	●	●	●	—	—
	● 資料配布 ● マクロ実行 ● 実行ファイルの配布と実行	○	—	—							●	●	—	—
	● クライアントPC環境保護	○	—	—							●	●	●	●
	● クライアントPCドライブ保護 ● ディスクイメージ配信 ● ディスクメンテナンス	○	—	—	OP	OP	OP	OP	OP	OP	—	—	—	—

ソフトウェア資産管理（SAM）

			対応OS			Edition						Cloud Edition			
												標準		HTTPS	
			Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
ソフトウェア資産管理（SAM）	運用ルール策定	● ソフトウェア資産管理台帳 ● 管理対象ソフトウェアの策定 ● ソフトウェア情報登録支援	○	○	○	●	●	●	●	●	●	●	●	●	●
	ライセンスの記録・管理	● 保有ライセンスの記録・割当 ● 突合を自動で実行（※26） ● ライセンス部材の記録 ● 台帳と実際のライセンス利用状況を照合（突合）													
	台帳の更新	● 台帳更新履歴の保存・閲覧													
	登録可能なライセンス形態	● 対応ライセンス種別 ・パッケージライセンス ・同時接続ライセンス ・プリインストール ・監視対象マシン数ライセンス ・ユーザー固定ライセンス ・サイトライセンス ・プロセッサライセンス ・規模ライセンス ・サーバーライセンス ・クライアントアクセスライセンス（デバイス / ユーザー） ● ライセンスに付帯される契約・権利 ・アップグレード版 ・重複インストール権 ・使用期限契約ライセンス ・セカンドライセンス ・ダウングレード使用権 ・アップグレード使用権													
申請・承認ワークフローシステム		● ソフトウェア利用申請 ● 管理ソフトウェア追加申請 ● 利用中ソフトウェア移動申請 ● 任意定義申請 ● 利用中ソフトウェア廃棄申請 ● コンピューター移動申請 ● コンピューター廃棄申請	○	○	—	OP	OP	OP	OP	OP	OP	—	—	—	—

サーバー監査 ｜ 収集できるログについては、P.63をご覧ください。

			対応OS			Edition						Cloud Edition			
												標準		HTTPS	
			Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
アクセスレポート	サーバーアクセス状況	● サーバー別アクセス比較 ● 端末別アクセス一覧 ● フォルダ別アクセス比較 ● 時間帯別アクセスグラフ ● ファイル別アクセス比較 ● ユーザー別アクセス一覧	○	—	—	OP	OP	OP	OP	OP	OP	—	—	—	—
OSログ閲覧	サーバー監査ログ閲覧 / Windowsイベントログ閲覧	● イベントログ蓄積 ● イベントログバックアップリストア ● 取得対象イベントログ設定	○	—	—	OP	OP	OP	OP	OP	OP	—	—	—	—
		● 監査対象サーバーごとに条件を指定してアラート検知	○	—	—	OP	OP	OP	OP	OP	OP	—	—	—	—

モバイル機器管理（MDM）※27 ｜ 収集できる資産情報については、P.62をご覧ください。

			対応OS	Edition						Cloud Edition			
										標準		HTTPS	
			iOS	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
セキュリティ管理	デバイス制限	● アプリケーションのインストール禁止 ● 音声ダイヤルの利用禁止 ● カメラの利用禁止 ● アプリケーション内での購入（課金）禁止 ● FaceTimeの禁止 ● 購入した全項目のiTunes Storeパスワードの入力をユーザーに強制 ● スクリーンショットの保存禁止 ● マルチプレーヤーゲームの利用禁止 ● ローミング中の自動同期の禁止 ● Game Centerへの友達の追加禁止 ● Siriの利用禁止	○	OP	OP	OP	OP	OP	OP	—	—	—	—
	アプリケーション制限	● iTunes Storeの利用禁止 ● Safariの利用の禁止											
	iCloud制限	● バックアップの禁止 ● フォトストリームの禁止 ● 書類の同期の禁止											
	セキュリティとプライバシーの設定	● Appleへの診断データの送信を禁止 ● 暗号化バックアップの強制 ● 信頼されていないTLS証明書の受け入れ禁止											
	コンテンツレーティング設定	● 不適切な内容のミュージックとPodcastの禁止											
	パスコード設定	● パスコード設定を構成する											
運用支援・紛失対策	無線LAN設定	● SSID ● セキュリティの種類 ● 自動接続 ● プロキシ設定 ● 非公開ネットワーク	○	OP	OP	OP	OP	OP	OP	—	—	—	—
	証明書設定	● 証明書のインストール											
	リモート制御	● ロック ● ワイプ ● パスコード消去											
	検知・アラート	● アンインストール検知 ● デバイストークン無効検知											

レポート※22

			対応OS			Edition						Cloud Edition			
												標準		HTTPS	
			Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
ログ解析レポート	● ユーザー作業状況 ● ファイルサーバーアクセス解析 ● セキュリティ ・ユーザー別作業時間解析 ・時間帯別推移 ・ファイル名別比較 ・端末別アラート比較 ・部署別作業時間解析 ・端末別比較 ・日別アラート件数推移	○	—	—	●	●	●	●	●	●	OP	OP	OP	OP
	● 端末機稼働状況 ● プリント出力解析 ● アプリケーション解析 ● Webアクセス解析 ・稼働時間比較 ・ドキュメント別比較 ・端末別比較 ・時間帯別推移 ・時間帯別使用状況解析 ・端末別比較 ・日別比較 ・端末別比較 ・日別稼働台数推移 ・プリンター別比較 ・Web別利用時間推移 ・未稼働端末一覧 ・IPアドレス別比較 ・端末別デバイス書き込み比較	○	○	—										
資産レポート	● ライセンス利用状況 ● 不許可アプリケーションインストール状況（Windows ストアアプリ） ● 不許可アプリケーションインストール状況 ● 必須アプリケーション未インストール状況	○	—	—	●	●	●	●	●	●	OP	OP	—	—
	● 端末利用状況	○	○	○										
その他	● 資産・ログ利活用レポートライブラリ（※23）	○	○	—	●	●	●	●	●	●	OP	OP	OP	OP

インストーラー	対応OS			Edition						Cloud Edition			
										標準		HTTPS	
	Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
● 部署情報付きインストーラー作成	○	○	○※28	●	●	●	●	●	●	●	●	●	●
● リモートインストールツール	○	—	—	●	●	●	●	●	●	●	●	—	—

操作画面				対応OS			Edition							Cloud Edition			
														標準		HTTPS	
				Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
端末機閲覧画面	● 端末表示			○	—	—	●	●	●	●	●	●	●	●	●	●
	● ユーザー表示	● デスクトップ表示 / リスト表示											●	●	—	—
	● 操作画面の折りたたみ表示 ● お気に入りタブ ● 機能ガイド	● アラート端末表示 （アラート端末のデスクトップ画像のみ表示） ● ふきだしヒント	● 端末機閲覧画面検索機能 ● 重要なお知らせ ● オンラインマニュアル										●	●	●	●
エンタープライズモード	● 端末選択時資産情報詳細表示 ● ソフトウェア一覧のマトリックス表示	● 端末検索 ● 各画面設定の保存復帰	● ドッキングウィンドウ	○	—	—	●	●	●	●	●	●	●	●	●	●

その他	対応OS			Edition						Cloud Edition			
										標準		HTTPS	
	Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
● 通信帯域制限	○	○	○	●	●	●	●	●	●	●	●	●	●
● 通信帯域制限（端末間）	○	○	○							●	●	—	—
● 管理サーバー切り替え　● サーバー間の端末機移動	○	—	—							●	●	—	—
● SKYSEA Client Viewリモートアップデート	○	○	○							●	●	●	●
● 管理機のパスワード認証 ● 管理機ごとの使用機能の利用設定 ● 管理機ごとの管理権限部署設定 ● 管理機の起動抑止設定 ● マイナンバー取扱端末設定 ● マイナンバー取扱管理機設定（専用のパスワード認証）	○	—	—							●	●	●	●
● データサーバーの中継構成	○	—	—							—	—	—	—
● 複数マスターサーバー連携による一元管理	○	—	—							●	●	●	●
● Active Directoryユーザー連携	○	—	—							●※29	●※29	●※29	●※29
● アンインストーラー用期限付きパスワード発行 ● 管理コンソールの各種設定情報バックアップ / リストア ● 通信に使用しないネットワークカードを設定	○	—	—							●	●	●	●
● 端末機インストール時に所属先マスターサーバーを自動で設定	○	○	○							●	●	●	●
● 端末機インストール時に保存先データサーバーを自動で設定	○	○	—							●	●	●	●
● シンクライアントライセンス数設定	○	—	—							●	●	●	●
● メール添付ファイルの自動暗号化	○	—	—	※30	※30	※30	※30	※30	※30	—	—	—	—
● 在席状況を確認しメッセージで情報共有	○	—	—	OP	OP	OP	OP	OP	OP	—	—	—	—

・医療機関向けオプション機能も別途ご用意しております。詳しくは、SKYMEC IT Managerのカタログをご参照ください。

※1 クラウド上のサーバーと管理機・クライアントPCとの接続には、VPNを利用します。※2 社外でのクライアントPC利用時にVPN接続が行えない場合は、HTTPS接続（オプション）でご利用いただけます。Linuxは非対応です。※3 Mac端末、Linux端末の場合、レジストリ情報の表示はできません。※4 Mac端末、Linux端末ではアップデーターの配布・実行のみ対応しています。※5 配布できるソフトウェアの合計サイズの上限は20GBです。※6 Windows端末上でのみ閲覧できます。対象となる資産情報は、Mac端末、Linux端末からも収集できます。※7 Mac端末の対応OSは、Mac OS X 10.5以降のバージョンとなります。※8「アクセスPCの前後の操作ログを追跡」は、端末機（Mac）で共有フォルダにアクセスした場合には追跡できません。※9 収集したログはクラウド上に3か月間保管されます。また、クライアントPC1台あたりの規定保管容量は、S1 Cloud Editionが93MB、S3 Cloud Editionが558MBです。保存期間の延長や規定保存容量を超過される場合は「ログ保管容量追加オプション（1TB単位）」が必要です。※10 データサーバーに保存されたログを閲覧できます。※11 残業申請Web承認における承認処理は、iOSではSafari、AndroidではGoogle Chromeで行えます。※12 Windows端末上でのみ閲覧できます。対象となる資産およびログ情報は、Windows端末、Mac端末からも収集できます。※13 Mac端末には、「記憶媒体 / メディア使用」アラート、「記憶媒体 / メディア使用（棚卸期間超過）」アラートの場合のみ対応します。※14 Mac端末に対しては、端末機デバイスアラートのみ設定できます（ユーザーごとの設定はできません）。※15 Windows Vista / Windows Server 2008以降のOSのみ遮断できます。※16 eSATA接続ハードディスクの管理は、端末機（Windows）に接続されたものに対してのみ行われます（ただし、Windows 2000は除く）。端末機（Linux）は非対応です。※17 eSATA接続ハードディスクは管理対象外です。※18 Windows端末では、Windows 2000は管理対象外です。※19 メディア登録時は別途、管理番号やメディア種別などの登録が必要です。※20「外付けデバイス&ファイル暗号化」機能＜オプション（Ent/Pro/Tel/LT/500/ST）＞として提供します。※21 Mac端末、Linux端末で検知できないアラートについては、syslogが出力できません。※22 各レポートへのアクセスはWindows端末のみ対応しています。※23 ダウンロードしたテンプレートによっては、Mac端末のログ集計が行えないものもあります。※24 Mac端末では、滅色設定ができないなど、一部適用されない設定項目があります。※25「画面操作録画」機能＜オプション（Ent/Pro/Tel/LT/500/ST）＞が必要です。※26 事前に専用ツールをWindowsのタスクスケジューラなどのジョブ管理システムで定期的に実行するように登録しておく必要があります。※27 ログ収集などのログ管理機能は搭載しておりません。※28 対応するLinuxディストリビューションについてはP.67「動作環境」をご覧ください。※29 マスターサーバーはActive Directoryドメインに参加しないため、マスターサーバー上の管理機では利用できません（組織内にある役職レベル1の管理機は利用可能）。※30「送信メールログ」機能＜オプション（Pro/Tel/LT/500）＞と「外付けデバイス&ファイル暗号化」機能＜オプション（Ent/Pro/Tel/LT/500/ST）＞が必要です。

収集できる資産情報（PC）				対応OS			Edition							Cloud Edition			
														標準		HTTPS	
				Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
自動収集項目	・端末機No. ・コンピューター名 ・部署名 ・ログオンユーザー ・SKYSEA Client View端末機バージョン ・資産情報収集日時 ・最終起動日時 ・ホスト名 ・ドメイン名（ワークグループ名） ・通常使うプリンター（※1） ・プリンター名（※2） ・ポート名 / デバイスURI（※2） ・死活監視状態 ・システムモデル ・システムシリアル	・マザーボードUUID ・OSバージョン ・ネットワークカード数 ・ドライブ数 ・MACアドレス ・ネットワークカード ・IPアドレス割り当て方式 ・IPアドレス ・サブネットマスク ・デフォルトゲートウェイ ・デフォルトゲートウェイ（MACアドレス） ・DNSサーバー ・CPUタイプ ・CPU周波数	・CPU数 ・CPUコア数 ・メモリサイズ ・ドライブタイプ ・ドライブ名 ・全容量 ・空き容量 ・所属マスターサーバー ・通信用マスターサーバー ・データサーバー指定方法 ・データサーバー ・画面操作ログ用データサーバー ・個別画面操作録画ライセンス ・役職レベル	○	○	○	●	●	●	●	●	●	●	●	●	●
	・システム製造元			○	—	○										
	・最新ポリシー設定適用済み ・ポリシー設定適用日時 ・使用中のディスプレイ数 ・ディスプレイアダプター名称 ・現在の解像度 ・ディスプレイ色数 ・ディスプレイアダプター情報（※2※3）	・モニター情報（※2※3） ・モニター名称 ・モニターシリアル（※4） ・スクリーンセーバーのパスワードによる保護 ・HTTPゲートウェイ利用 ・通信方法設定	・最終利用HTTPゲートウェイURL ・最終利用プロキシサーバー ・グローバルIPアドレス ・Google Chrome（SKYSEA Client Viewアドオン） ・端末利用者	○	○	—										
	・表示名 ・SKYSEA Client Viewインストール状況 ・SNMPサポート状況 ・BIOSバージョン ・AMTプロビジョニングモード ・AMTプロビジョニングステート ・AMTバージョン ・Windowsプロダクト ID ・OSサービスパック ・OSバージョン（ビルド番号） ・Windows準備レベル ・OS言語 ・日本語言語パック ・IEバージョン ・IEサービスパック ・ESU（2020年） ・ESU（2021年） ・ESU（2022年） ・モデム数 ・SCSI数 ・SCSI	・IPv6グローバルアドレス割り当て方式 ・IPv6グローバルアドレス ・IPv6ユニークローカルアドレス割り当て方式 ・IPv6ユニークローカルアドレス ・IPv6一時アドレス割り当て方式 ・IPv6一時アドレス ・IPv6リンクローカルアドレス割り当て方式 ・IPv6リンクローカルアドレス ・IPv6デフォルトゲートウェイ ・IPv6デフォルトゲートウェイ（MACアドレス） ・IPv6DNSサーバー ・Credential Provider ・Firefox（SKYSEA Client Viewアドオン） ・省電力設定 ・WSUS連携設定 ・Windows Update更新結果（WSUS連携） ・Windows Updateダウンロード元 ・Windows 10更新制御設定 ・Windows 10大型アップデートの延期 ・定期電源ON設定 ・定期電源OFF設定	・接続デバイス最終検査日時 ・接続デバイス最終不正プログラム検出日時 ・管理機制限設定 ・暗号化状態（※2） ・暗号化方式（※2） ・暗号化リカバリファイル収集日時（※2） ・プリンタードライバー名（※2） ・（プリンターの）IPアドレス（※2※5） ・PC保護状態 ・PC環境保護 ・アクセス共有フォルダ数 ・共有フォルダパス（※2） ・最終アクセス日時（※2） ・ネットワークドライブ割り当て数 ・共有フォルダパス（※2） ・ドライブ名（※2） ・最終検出日時（※2） ・設定したレジストリ情報数	○	—	—										
	・紛失時制御端末	・紛失端末制御用サーバーとの最終通信結果	・位置情報取得結果				OP	OP	OP	OP	OP	OP	—	—	—	—
	・Safari（SKYSEA Client Viewアドオン）	・Mac標準メーラー「メール」（SKYSEA Client Viewアドオン）		—	○	—	●	●	●	●	●	●	●	●	●	●
任意設定項目	・AMTホスト名 / IPアドレス	・管理コンソール起動抑止	・マイナンバー取扱端末	○	—	—										
	・端末機名 ・資産No. ・端末機タイプ ・セキュリティグループ ・所有ADユーザー ・メールアドレス	・ネットワーク機器の死活監視設定 ・MIB情報自動更新間隔設定 ・種別（デスクトップ / ノート） ・OSライセンス種別 ・OSライセンス形態 ・状態区分	・導入責任者 ・管理部署 ・管理者 ・使用部署	○	○	○	●	●	●	●	●	●	●	●	●	●
	・前管理者 ・前利用者 ・設置場所 ・導入形式 ・登録日	・導入日 ・購入日 ・購入先 ・購入金額（円） ・リース / レンタル期限	・経費（円） ・メモ ・通常時の消費電力（W） ・省電力時の消費電力（W） ・任意項目01～50													
	・Mac端末カーネル拡張 / システム拡張			—	○	—										

収集できる資産情報（ネットワーク機器）					対応OS	Edition							Cloud Edition			
													標準		HTTPS	
					iOS	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
収集可能な資産項目	・最新検出日時 ・機器種別 ・管理状態 ・ネットワーク機器名	・IPアドレス ・MACアドレス ・SNMPサポート状況	・コミュニティ ・ドメイングループ（ワークグループ名）	・システム製造元 ・初回検出日時 ・システムシリアル	○	●	●	●	●	●	●	●	●	●	●

収集できる資産情報（モバイル端末）

		対応OS	Edition						Cloud Edition			
									標準		HTTPS	
		iOS	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
収集可能な資産項目	・端末機No. ・端末機名 ・端末機タイプ ・所属 ・初期登録キー ・個体識別情報 ・システムモデル ・システム製造元 ・OSバージョン ・OSサービスパック ・ポリシー適用状況 ・電話番号 ・キャリア名 ・デバイス容量 ・パスコード / パスワード ・Wi-Fi MACアドレス ・Bluetooth MACアドレス ・証明書 ・プロファイル ・プロビジョニングプロファイル ・アプリケーション名 ・パッケージ名 / 識別子 ・バージョン ・アプリケーションの追加 ・SIMの差し替え	○	OP	OP	OP	OP	OP	OP	—	—	—	—

収集できるログ

			対応OS			Edition							Cloud Edition			
													標準		HTTPS	
			Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST		S1	S3	S1	S3
ログ管理	ログ収集	・起動･終了ログ ・クライアント操作ログ ・アプリケーションログ ・ファイル操作ログ（※6） ・クリップボードログ ・システムログ ・プリントログ（※6） ・Webアクセスログ（※6） ・ドライブ追加･削除ログ ・フォルダ共有ログ	○	○	—	●	●	●	●	●	●		●	●	●	●
		・送信メールログ	○	○	—	●	OP	OP	OP	OP	●		—	—	—	—
		・ファイルアクセスログ	○	—	—	●	●	●	●	●	●		●	●	●	●
		・不許可端末検知ログ	○	—	—	●	●	●	●	●	●		●	●	—	—
		・通信デバイスログ ・想定外TCP通信ログ	○	—	—	●	●	●	●	●	●		●	●	●	●
	ログ収集（ITセキュリティ対策強化）	・アプリケーションログ（起動元アプリケーション、コマンドプロンプト情報） ・ファイル操作ログ（ZIPファイル内のファイル名）	○	—	—	●	●	●	OP	OP	OP		—	●	—	●
不許可端末検知 / 遮断	不許可端末ログ	・IPアドレス / MACアドレス ・許可設定状況	○	—	—	●	●	●	●	●	●		●	●	—	—
サーバー監査	アクセスレポート	・成功 / 失敗ファイルアクセスログ	○	—	—	OP	OP	OP	OP	OP	OP		—	—	—	—
	OSログ閲覧	● イベントログ ・アプリケーションログ ・セキュリティログ ・システムログ ・セットアップログ ・転送されたイベントログ				OP	OP	OP	OP	OP	OP					
		● 監査ログ ・アカウント操作ログ ・グループ操作ログ ・パスワード操作ログ ・監査ポリシー操作ログ ・ロックアウトログ ・ログオンログ ・ログオフログ ・ファイルアクセスログ ・印刷ログ				OP	OP	OP	OP	OP	OP					
	データベース監査ログ閲覧	・アカウント操作 ・パスワード操作 ・データベース操作 ・バックアップ / リストア ・ログイン / ログアウト ・SELECT ・INSERT ・UPDATE ・DELETE				OP ※7	OP ※7	OP ※7	OP ※7	OP ※7	OP ※7					

設定できるアラート（注意表示）項目一覧

		画面操作録画※8	端末アラート	ユーザーアラート	対応OS			Edition						Cloud Edition			
														標準		HTTPS	
					Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
資産	資産情報の変更	—	○	—	○	—	—										
	HDD容量不足	—	○	—													
	リース / レンタル切れ	—	○	—													
	許可 / 不許可アプリケーション（デスクトップアプリケーション / Windows ストアアプリ）	—	○	—										●	●	●	●
	インストール必須アプリケーション	—	○	—				●	●	●	●	●	●				
	インストール必須アプリケーション（遮断）	—	○	—										●	●	—	—
	SKYSEA未対応OSバージョン	—	○	—										●	●	●	●
	ネットワーク機器の死活監視	—	○	—	○	○	○							●	●	—	—
	端末未起動期間設定	—	○	—										●	●	●	●
	SKYSEA端末アップロード異常検知	—	○	—	○	○	—							●	●	●	●
アプリケーション	ウィンドウタイトル	○	○	○	○	—	—										
	不許可ファイル検索	—	○	—													
	アプリケーション実行（デスクトップアプリケーション / アプリケーション実行中の特定操作 /Windows ストアアプリ）	○	○	○ ※9													
	禁止アプリケーションの名前変更	○	○	○													
	業務外アプリケーション実行	○	○	○				●	●	●	●	●	●	●	●	●	●
	レジストリ変更	○	○	○													
	インストール	○	○	○													
	システム構成変更	○	○	○													
	Windows ストアの利用	○	○	○													
	Windows ストアアプリの自動更新	—	○	—													
ファイル操作	CSVファイル出力	○	○	○	○	—	—										
	規定時間外端末機操作	○	○	○													
	Autorun（自動実行）	—	○	—													
	特定フォルダアクセス	○	○	○													
	ドライブ追加	○	○	—													
	共有フォルダ書き込み	○	○	○				●	●	●	●	●	●	●	●	●	●
	ローカル共有フォルダ作成	○	○	—													
	ローカル共有フォルダアクセス	○	○	—													
	カスタマイズ	○	○	○													
	禁止ファイル持ち込み	○	○	○													
	実行ファイル不正操作	○	○	○													
	ファイル自動暗号化（※10）	—	○	—				OP	OP	OP	OP	OP	OP	—	—	—	—

設定できるアラート（注意表示）項目一覧

		画面操作録画※8	端末アラート	ユーザーアラート	対応OS			Edition						Cloud Edition			
														標準		HTTPS	
					Win	Mac	Lin	Ent	Pro	Tel	LT	500	ST	S1	S3	S1	S3
デバイス	記憶媒体 / メディア使用	○	○	○	○	○	—										
	記憶媒体 / メディア使用（棚卸期間超過）	○	○	○													
	記憶媒体 / メディア書き込み（※11※12）	○	○	○													
	BitLocker To Goで保護されていない記憶媒体使用	○	○	—	○	—	—	●	●	●	●	●	●	●	●	●	●
	USBデバイスによる不正ファイル持ち込み（※13）	—	○	○													
	USBメモリによるコンピューター使用制限	—	○	○													
	セーフモードで起動時（Windows）の記憶媒体 / メディア使用	—	○	—													
ITセキュリティ対策強化（ファイル操作）	特定フォルダアクセス（アプリケーション指定）	○	○	○	○	—	—							—	●	—	●
	ローカル共有フォルダへのアクセス（通信）を暗号化（ファイルサーバー用）	—	○	—				●	●	●	OP	OP	OP	—	●	—	●
	セキュリティ基準を満たさない共有フォルダへのアクセス（端末用）	○	○	—										—	●	—	●
	想定外共有フォルダアクセス	○	○	—				●	●	●	●	●	●	●	●	●	●
ITセキュリティ対策強化（その他）	検疫ソフトウェアイベントログ監視（※14）	—	○	—	○	—	—							●	●	●	●
	検疫ソフトウェアレジストリ監視（※14）	—	○	—										●	●	●	●
	検疫ソフトウェアログファイル監視（※14）	—	○	—										●	●	●	●
	syslogによる異常端末監視（※14）	—	○	—				●	●	●	OP	OP	OP	—	●	—	—
	SNMPトラップによる異常端末監視（※14）	—	○	—										—	●	—	—
	組織外ネットワーク接続（デフォルトゲートウェイ）（※14）	—	○	—										—	●	—	●
	組織外ネットワーク接続（VPN･プロキシサーバー）（※14）	—	○	—										—	●	—	●
その他	Web / アプリケーションアカウント監査	○	○	—	○	—	—										
	通信デバイス使用	○	○	—													
	想定外TCP通信	○	○	—													
	Webダウンロード	○	○	○													
	FTPダウンロード	○	○	○				●	●	●	●	●	●	●	●	●	●
	Webアップロード	○	○	○													
	FTPアップロード	○	○	○													
	Web閲覧	○	○	○													
	掲示板 / Webメール書き込み	○	○	○													
	電子メール送信	○	○	—													
	電子メール送信（添付ファイル付き）	○	○	—				●	OP	OP	OP	OP	●	—	—	—	—
	電子メール送信宛先フィルタ	○	○	—													
	電子メール送信時の添付ファイル自動暗号化	—	○	—				※15	※15	※15	※15	※15	※15				
	印刷枚数	—	○	—													
	印刷ドキュメント名	○	○	—													
	印刷ファイルパス	○	○	—				●	●	●	●	●	●	●	●	●	●
	印刷禁止	—	○	—													
	印刷物取り忘れ	—	○	—													
	不許可端末検知	—	○	—										●	●	—	—
	不許可端末遮断	—	○	—				●	●	●	OP	OP	●	—	●	—	—
	残業時間お知らせメッセージ	—	○	—				●	●	●	●	●	●	●	●	●	●
	残業時間お知らせメッセージ（遮断）	—	○	—				●	●	●	●	●	●	●	●	—	—
	残業時間お知らせメッセージ（勤怠情報取り込み）	—	○	—				●	●	OP	OP	OP	OP	—	●	—	—
	管理者権限ログイン抑止	—	○	—				●	●	●	●	●	●	●	●	●	●
	Print Screenキーによる画面コピー	—	○	○				●	—	●	—	—	—	—	—	—	—
	アプリケーションによる画面キャプチャー	—	○	○				●	—	●	—	—	—	—	—	—	—
	共有エクスペリエンス（近距離共有･デバイス間の共有）	—	○	—													
	アクティビティ（タイムライン）履歴の保存	—	○	—													
	デバイス間でのアクティビティ（タイムライン）の同期	—	○	—													
	クリップボードの履歴の保存	—	○	—													
	デバイス間でのクリップボードの同期	—	○	—													
	Windowsサンドボックスの利用	○	○	○													
	OneDriveの利用	○	○	○													
	OneDriveの同期設定	—	○	—													
	OneDrive for Businessの利用	○	○	○				●	●	●	●	●	●	●	●	●	●
	Dropboxの利用（※16）	○	○	○													
	BitLockerドライブ暗号化でスマートカードを使用した認証	—	○	—													
	レジストリ操作	○	○	—													
	圧縮ファイル生成	○	○	—													
	Windowsを「セーフモードとネットワーク」で起動	—	○	—													
	任意定義アラート	○	○	○													
	ユーザーアラートを優先する	—	○	—													
アラート設定	許可 / 不許可アプリケーションインストール検知、モバイル端末情報末アップロード検知				iOS			OP	OP	OP	OP	OP	OP	—	—	—	—

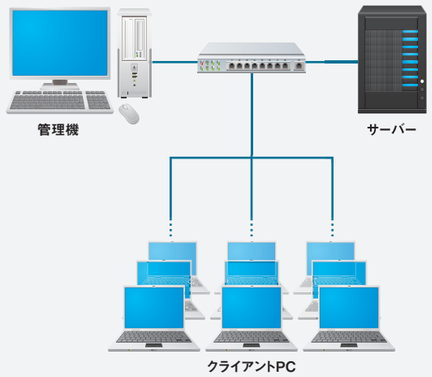
※1 Mac端末、Linux端末の場合、印刷システムとして「CUPS」が使用されている必要があります。※2 ハードウェア情報の詳細表示画面でのみ表示されます。※3 製造元、ドライバー、ドライバーの説明、ドライバーファイル、デバイスIDの情報が取得できます。ただし、モニタードライバー情報は、Windows XP / Windows Server 2003以前のOSでは取得できません。※4「モニターシリアル」は、仮想マシンでは取得できません。また、機種によっては取得できない場合があります。※5 取得できるのは、PCと直接接続しているネットワークプリンターかつ、レジストリにIPアドレスが存在する場合のみです。※6 Mac端末では一部収集できない項目があります。詳しくは、「Mac端末運用管理について(P.79)」をご覧ください。※7「サーバー監査」(オプション)のオプション機能として提供します。※8 画面操作録画はすべてオプションです。※9「アプリケーション実行中の特定操作」のみユーザーアラートは設定できません。※10「外付けデバイス&ファイル暗号化」機能(オプション)として提供します。※11 Mac端末の場合、OSデバイスへの書き込みは禁止されますが、管理機上では対象のMac端末に対するアラートは発生しません。※12 Mac端末では、CD / DVD / ブルーレイドライブへの記憶媒体書き込み制限はできません。またブランクディスクを挿入した場合は、記憶媒体使用制限もできません。※13 eSATA接続ハードディスクは設定対象外です。※14 Windows Vista / Windows Server 2008以降のOSに対応しています。※15 本アラート項目を利用するには、「送信メールログ」機能<オプション(Pro/Tel/LT/500)>と、「外付けデバイス&ファイル暗号化」機能<オプション(Ent/Pro/Tel/LT/500/ST)>が必要です。※16 DropboxおよびDropbox Pro / Business / Enterpriseに対応しています。

システム構成

2021年9月8日時点の情報です。システム構成の最新情報は、Webサイト（https://www.skyseaclientview.net/ver17/system/）でご覧いただけます。
詳しい構成・スペックの最新情報は、Webサイト（https://www.skyseaclientview.net/ver17/technicalsheet/）の「システム構成」をご覧ください。

サーバー構成例 ❶ ＜管理対象PC1,000台まで＞

クライアントPCを管理する基本的なサーバー構成※1



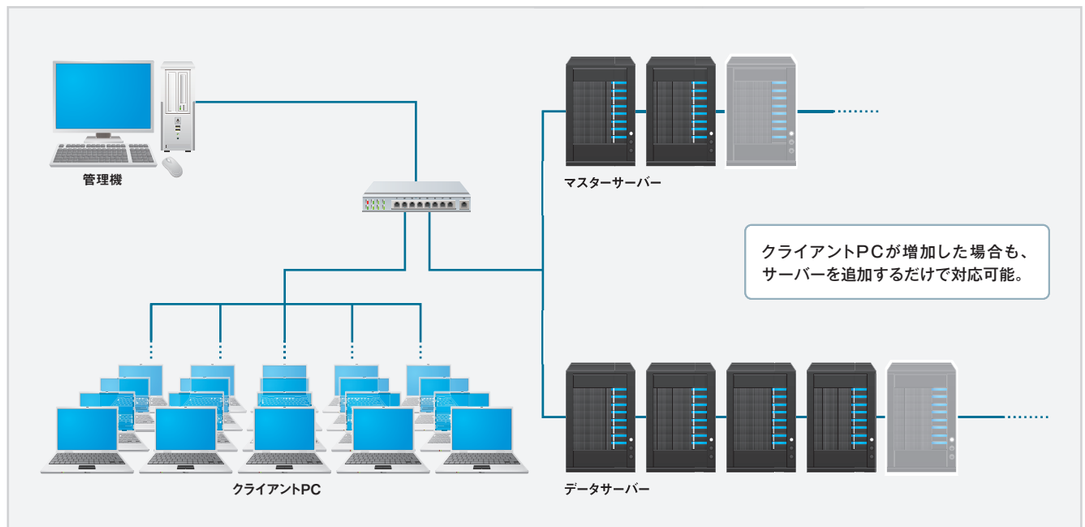
以下のサーバー機能を1台のサーバーにインストールして運用いただけます。	
マスターサーバー機能	資産情報を蓄積するためのサーバー機能です。
データサーバー機能	ログを蓄積するためのサーバー機能です。※2
ログ解析 / レポート用サーバー機能	収集したログ情報を集計・解析し、グラフ化して表示したり、収集したログ情報から各種レポートを出力するサーバー機能です。

※1 基本的な構成例です。詳しいサーバー構成については、Webサイトの「システム構成」の技術資料をご覧ください。 ※2 画面操作録画機能＜オプション（Ent/Pro/Tel/LT/500/ST）＞をご利用の場合は、録画データをログデータとは別のサーバーに保存可能です。それぞれ別々に保存することで、サーバーの負荷を分散することができます。

サーバー構成例 ❷ ＜管理対象PC1,001台から＞

マスターサーバー、データサーバーを分離して大規模環境に適応※3

大規模環境で運用する際に、複数台のマスターサーバー、データサーバーを設置した場合でも、各サーバーの情報が統合され、管理機から一元管理できます※4。



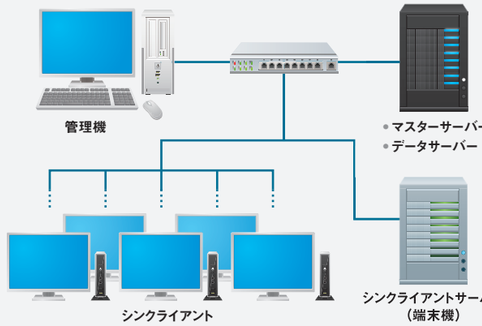
※3 詳しいサーバー構成については、Webサイトの「システム構成」の技術資料をご覧ください。 ※4 マスターサーバー、データサーバーともに、1台あたり5,000クライアントまで管理できます。画面操作録画機能＜オプション（Ent/Pro/Tel/LT/500/ST）＞でクライアントの常時録画を行う場合は、データサーバー1台あたり150クライアントまでとなります。

サーバー構成例 ❸

サーバーベース方式・仮想PC方式のシンクライアント環境の運用管理にも対応

シンクライアント環境でも、操作ログの収集やセキュリティポリシーに沿った注意表示（アラート）が設定できます。また、仮想PC方式の場合は資産管理にも対応し、物理PCと仮想PCが混在する環境でもクライアントに関する情報が一元管理できます。

「サーバーベース方式」のシンクライアント環境で
SKYSEA Client Viewを運用するための構成図



サーバーベース方式

- VMware社製 VMware Horizon
- Citrix社製 Virtual Apps and Desktops
- Microsoft社製 リモートデスクトップサービス（ターミナルサービス）
- Sky株式会社製 SKYDIV Desktop Client

使用できる機能：ログ管理 / セキュリティ管理 / デバイス管理※5 / メンテナンス※6

仮想PC方式

- VMware社製 VMware Horizon
- Citrix社製 Virtual Apps and Desktops
- HP社製 CCI
- 日本電気株式会社製 VirtualPCCenter
- Microsoft社製 Hyper-V
- Sky株式会社製 SKYDIV Desktop Client

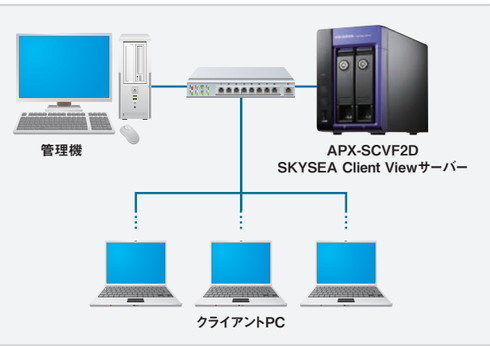
使用できる機能：ログ管理 / セキュリティ管理 / デバイス管理※7 / 資産管理 / メンテナンス

※5 サーバーベース方式における「デバイス管理」機能は、VMware社製 VMware Horizonに対応しています。※6 Citrix社製 Virtual Apps and DesktopsとVMware社製 VMware Horizonのアプリケーション配信では、「メンテナンス」機能をご利用いただけません。※7 仮想PC方式における「デバイス管理」機能は、Citrix社製 Virtual Apps and DesktopsとVMware社製 VMware Horizonに対応しています。

サーバー構成例 ❹ ＜管理対象PC20台まで※8＞

アプライアンスプラットフォーム装置を利用した構成
「アイ・オー・データ機器社製 APX-SCVF2D」※9

「APX-SCVF2D」を使用することで、サーバー機を導入せずに、クライアントPCの制限や操作ログ収集、USBデバイス、ソフトウェア資産の管理が可能となり、小規模な環境でも情報漏洩対策やIT資産の有効活用が容易に行えます。



※8 アイ・オー・データ機器社製「APX-SCVF2D」以外のNASをご利用の場合、SKYSEA Client Viewの専用サーバーとしてだけでなく、NASとしても利用するときは、50台以下でNASの推奨台数を上限とします。※9 「APX-SCVF2D」は受注生産となっているため、場合によって納品までに2～3か月を要することがあります。ご購入を希望される場合は、事前にSky株式会社までご連絡ください。

サーバー構成例 ❺

物理サーバーを使わない環境でも
情報漏洩対策、IT資産管理が可能に

SKYSEA Client Viewのマスターサーバー、データサーバーの動作確認が取れているクラウドサービス

- IIJ GIO
- Amazon EC2
- 株式会社インテック製「EINS/SPS SelfPortal」
- 株式会社STNet「STクラウド サーバーサービス［FLEXタイプ］」
- NTT Com Enterprise Cloud
- ニフクラ
- FUJITSU Cloud Service for OSS
- Microsoft Azure Virtual Machines

SKYSEA Client Viewの各種サーバーをクラウド上に構築できます。物理サーバーの購入が不要なため、初期コストを抑えて導入できます。インターネット経由でのIT資産管理、ログ収集、ソフトウェア配布が可能です。

SKYSEA Client Viewをサービスとして提供いただいているクラウド事業者様

株式会社STNet	STクラウドサーバーサービス［FLEXタイプ］
NECネッツエスアイ株式会社	エンドポイント統合管理サービス With SKYSEA Client View
NECフィールディング株式会社	iQQsam powered by SKYSEA Client View
CTCシステムマネジメント株式会社	SKYSEA on Cloud
JBCC株式会社	PC運用管理月額サービス for SKYSEA
株式会社ソフトクリエイト	SKYSEA Client View SaaS on SCCloud
東京日産コンピュータシステム株式会社	SKYSEA クラウド on ITte

動作環境

2021年9月8日時点の情報です。最新情報は、Webサイト（https://www.skyseaclientview.net/ver17/operation/）でご覧いただけます。
記載の数値は最低スペックです。システム構成や管理対象となる端末の数によって動作環境が異なる場合があります。
OSやその他のプログラムによっては、サポートが終了しているものがあります。サポート対象のOSやプログラムをご利用ください。
詳しくは、Webサイトの技術資料（https://www.skyseaclientview.net/ver17/technicalsheet/）をご確認ください。

管理機（Windows）・端末機（Windows）

CPU	Intel® Pentium® Ⅲ　866MHz 以上（x86アーキテクチャまたはx64アーキテクチャ）	メモリ	256MB以上※1
ハードディスク	600MB以上の空きがあること※2		
OS	● Windows 2000 Server SP4 ● Windows 2000 Professional SP3※3 / SP4 ● Windows Server 2003 Standard Edition SP1/SP2、Standard Edition x64 SP2、Enterprise Edition SP1/SP2、Enterprise Edition x64 SP2、R2 Standard Edition SPなし/SP2、R2 Standard Edition x64 SP2、R2 Enterprise Edition SPなし/SP2、R2 Enterprise Edition x64 SP2 ● Windows Server 2008 Standard Edition SPなし/SP2、Standard Edition x64 SPなし/SP2、Enterprise Edition SPなし/SP2、Enterprise Edition x64 SPなし/SP2、R2 Standard Edition SPなし/SP1、R2 Enterprise Edition SPなし/SP1 ● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter ● Windows Server 2016 Standard、Datacenter ● Windows Server 2019 Standard、Datacenter ● Windows XP Professional SP1/SP2/SP3、Professional x64 Edition SP2 ● Windows Vista Business SPなし/SP1/SP2、Business x64 Edition SPなし/SP1/SP2、Enterprise SPなし/SP1/SP2、Enterprise x64 Edition SPなし/SP1/SP2、Ultimate SPなし/SP1/SP2、Ultimate x64 Edition SPなし/SP1/SP2 ● Windows 7 Professional SPなし/SP1、Professional x64 Edition SPなし/SP1、Enterprise SPなし/SP1、Enterprise x64 Edition SPなし/SP1、Ultimate SPなし/SP1、Ultimate x64 Edition SPなし/SP1 ● Windows 8 Windows 8、Windows 8 x64 Edition、Pro、Pro x64 Edition、Pro with Media Center、Pro with Media Center x64 Edition、Enterprise、Enterprise x64 Edition ● Windows 8.1 Updateなし/Update 1 Windows 8.1、Windows 8.1 x64 Edition、with Bing、with Bing x64 Edition、Pro、Pro x64 Edition、Pro with Media Center、Pro with Media Center x64 Edition、Enterprise、Enterprise x64 Edition ● Windows 10 Home、Home x64 Edition、Pro、Pro x64 Edition、Pro Education、Pro Education x64 Edition、Pro for WorkStations、Pro for WorkStation x64 Edition、Enterprise、Enterprise x64 Edition、Enterprise LTSC※4、Enterprise x64 Edition LTSC※4、Enterprise for Virtual Desktop、Education、Education x64 Edition ● Windows Embedded 8.1 Industry Pro（x86 Edition, x64 Edition）※5 ● Windows Embedded 8.1 Industry Enterprise（x86 Edition, x64 Edition）※5 ● Windows 10 IoT Enterprise（x86 Edition, x64 Edition）※5		
ブラウザ	● Internet Explorer 5.5 SP2/6/7/8/9/10/11 ログ解析クライアントのご利用には、Internet Explorer 6/7/8/9/10/11（Windows ストアアプリ版は非対応）が必要です※6。中でも、資産・ログ利活用レポートライブラリの利用には、Internet Explorer 8/9/10/11（Windows ストアアプリ版は非対応）が必要です※6。申請・承認ワークフローシステムのご利用には、Internet Explorer 6/7/8/9/10/11（Windows ストアアプリ版を含む）が必要です※6。資産データ / ログデータWeb閲覧機能のご利用には、Internet Explorer 6/7/8/9/10/11（Windows ストアアプリ版を含む）が必要です※6。		
ディスプレイ	1024×768 16bit Color以上	ハードウェア環境	Intel® vPro™ Technologyに対応※7
ネットワーク	TCP/IP通信ができるネットワークであること		

※1 端末機の台数増加に伴い、管理機で必要なメモリも増加します。端末機が300台以上の場合、管理機には512MB以上のメモリが必要です。512MB未満の場合、ログの最大表示件数を20,000件以下に設定する必要があります。それ以上の件数は、表示時間が非常に遅くなります。※2 運用状況により異なります。※3 不許可端末遮断ユニット一括設定ツールは動作いたしません。※4 LTSB（Long Term Service Branch）も含みます。※5 端末機でのみご利用いただけます。※6 セキュリティ設定の変更が必要です。※7 SKYSEA Client Viewのインテル vProテクノロジー AMT対応機能をご利用の際は、お客様の環境がインテル vProテクノロジー AMTが動作する環境か、ご確認いただきますようお願いいたします。一例として、インテル vProテクノロジー AMTでは、無線LAN環境において固定IPアドレスをサポートしていないため、DHCP環境でしか動作しないことが確認されております。また、KVMリモート・コントロールのみ対応していない機種もございます。

端末機（Mac）※1※2

CPU	Intel製CPU、Apple Silicon	メモリ	512MB以上	ハードディスク	空き容量600MB以上				
OS	● Mac OS X 10.4 Tiger x86 Tiger x64	● Mac OS X 10.6 Snow Leopard x86 Snow Leopard x64	● OS X 10.8 Mountain Lion x64	● OS X 10.11 El Capitan x64	● macOS 10.14 Mojave x64
	● Mac OS X 10.5 Leopard x86 Leopard x64	● OS X 10.7 Lion x86 Lion x64	● OS X 10.9 Mavericks x64	● macOS 10.12 Sierra x64	● macOS 10.15 Catalina x64
			● OS X 10.10 Yosemite x64	● macOS 10.13 High Sierra x64	● macOS 11 Big Sur x64

※1 J2SE Runtime Environment 5.0 以上をインストールする必要があります。※2 Apple Siliconを搭載しているMac端末の場合、SKYSEA Client Viewをインストールする前にRosettaをインストールする必要があります。

端末機（Linux®）※1※2

OS	● Red Hat®			
	Enterprise Linux® 4 x86 Enterprise Linux® 4 x64	Enterprise Linux® 5 x86 Enterprise Linux® 5 x64	Enterprise Linux® 6 x86 Enterprise Linux® 6 x64	Enterprise Linux® 7 x64 Enterprise Linux® 8 x64
	● Ubuntu			
	18.04 LTS x64	20.04 LTS x64		

※1 CPU、メモリ、ハードディスクの動作環境は、端末機（Windows）に準じます。※2 Microsoftストアで公開されているUbuntuには対応しておりません。

マスターサーバー

CPU	Intel® Pentium® 4　3GHz以上	メモリ	1GB以上
ハードディスク	管理対象PCが300台の場合、120GB以上の空きがあること		
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter ● Windows Server 2016 Standard、Datacenter ● Windows Server 2019 Standard、Datacenter		
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること
その他	Internet Explorer 6.0 SP1/7/8/9/10/11、Microsoft .NET Framework 4 / 4（日本語言語パック）、Microsoft SQL Server 2014 Express Edition SP3 / 2019 Express Edition※1		

※1 Microsoft SQL Server 2019に対応するOSはWindows Server 2016 / 2019です。

データサーバー

CPU	Intel® Pentium® 4　3GHz以上	メモリ	1GB以上
ハードディスク	管理対象PCが300台の場合、120GB以上の空きがあること		
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter ● Windows Server 2016 Standard、Datacenter ● Windows Server 2019 Standard、Datacenter		
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP / IP通信ができるネットワークであること

ログ解析用サーバー / レポート用サーバー※1

CPU	Intel® Pentium® 4　3GHz以上	メモリ	1GB以上
ハードディスク	管理対象PCが300台の場合、40GB以上の空きがあること		
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter ● Windows Server 2016 Standard、Datacenter ● Windows Server 2019 Standard、Datacenter		
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること
その他	Internet Information Services 8.0/8.5/10、Microsoft SQL Server 2014 Express Edition SP3 / 2019 Express with Advanced Services※2※3、Microsoft .NET Framework 3.5 SP1 / 4 / 4（日本語言語パック）が必要）		

※1 サーバーシミュレーション機能および、ファイルサーバー利用状況レポート機能をご利用の場合、レポート対象とする各サーバーに情報収集のため、モジュールのインストールが必要になります。情報収集のためのモジュールについての動作環境は「管理機・端末機」に準じます。※2 レポートの印刷機能を使う場合のみログ解析サーバーへのインストールが必要です。※3 Microsoft SQL Server 2019に対応するOSはWindows Server 2016 / 2019です。

資産データ / ログデータ Web閲覧機能サーバー※1

CPU	資産データ:デュアルコア Intel® Xeon®　2.0GHz以上 ログデータ:Intel® Xeon®　1.8GHz（4コア/4スレッド）以上	メモリ	資産データ:2GB以上 ログデータ:4GB以上
ハードディスク※2	資産データ:10GB以上の空きがあること ログデータ:30GB以上の空きがあること※3		
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter ● Windows Server 2016 Standard、Datacenter ● Windows Server 2019 Standard、Datacenter		
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること
その他	Apache Tomcat 9.0.50、Java SE Runtime Environment 6 / 7 / 8 / 10、OpenJDK 11 / 12 / 13 / 14 / 15 / 16、Play Framework 1.2.7.2		
その他（ログデータのみ）	Microsoft SQL Server 2014 Express Edition SP3 / 2019 Express Edition※4（Windows PowerShell 2.0、Microsoft .NET Framework 3.5 SP1 / 4 / 4（日本語言語パック）が必要）		

※1 次の条件でのみマスターサーバー・データサーバー・ログ解析サーバーと同居可能です。端末台数1,000台以下、ログデータWeb閲覧機能へのログオンは同時に1ユーザーまで（ログ検索件数の上限は50,000件に制限されます）、スペックは、Webサイトの技術資料「システム構成」に準じます。これら以外の場合は、マスターサーバーのほか、SKYSEA Client Viewのほかのサーバー機能との同居不可のため、専用のサーバー機が必要です。※2 資産データWeb閲覧サーバーとログデータWeb閲覧サーバーを同一のサーバーにインストールする場合も、ログデータWeb閲覧サーバー単体の場合と同じく、Webサーバーとして10GB、データベースサーバーとして20GBの空きが必要です。※3 Webサーバーとして10GB、データベースサーバーとして20GBの空きが必要です。※4 Microsoft SQL Server 2019に対応するOSはWindows Server 2016 / 2019です。

HTTPゲートウェイサーバー※1

CPU	Intel® Xeon®　1.8GHz（2コア/4スレッド）以上		メモリ	4GB以上
ハードディスク	10GB以上の空きがあること			
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter ● Windows Server 2016 Standard Edition x64、Datacenter x64		● Windows Server 2019 Standard Edition x64、Datacenter x64 ● Red Hat® Enterprise Linux® Server x64 6.3/6.4/6.5/6.6/7.0/7.1/7.2/7.3/7.4/7.5/7.6/8.0/8.1/8.2	
ディスプレイ	1024×768 16bit Color以上		ネットワーク	TCP/IP通信ができるネットワークであること
その他	Windows	Java SE Runtime Environment 7 / 8 / 10、OpenJDK 11 / 12 / 13 / 14 / 15 / 16、Internet Information Services 8.0/8.5/10.0、Play Framework 1.2.7.2		
	Linux®	Apache 2.2 / 2.4、OSにバンドルされたjava-1.7.0-openjdk / java-1.8.0-openjdk、Play Framework 1.2.7.2		

※1 端末台数1,000台以上のスペックは、技術資料の「システム構成」に準じます。

サーバー監査用モジュール <オプション(Ent/Pro/Tel/LT/500/ST)>

CPU	Intel® Pentium® 4　3GHz以上	メモリ	1GB以上
ハードディスク	15GB以上の空きがあること		
OS	● Windows 2000 Server SP4 ● Windows Server 2003 Standard Edition SP1/SP2、Standard Edition x64 SP2、Enterprise Edition SP1/SP2、Enterprise Edition x64 SP2、R2 Standard Edition SPなし/SP2、R2 Standard Edition x64 SP2、R2 Enterprise Edition SPなし/SP2、R2 Enterprise Edition x64 SP2 ● Windows Server 2008 Standard Edition SPなし/SP2、Standard Edition x64 SPなし/SP2、Enterprise Edition SPなし/SP2、Enterprise Edition x64 SPなし/SP2、R2 Standard Edition SPなし/SP1、R2 Enterprise Edition SPなし/SP1 ● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter　● Windows Server 2016 Standard、Datacenter　● Windows Server 2019 Standard、Datacenter		
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること
その他	データベース監査ログ閲覧※1に対応しているデータベースは、次のとおりです。 Microsoft SQL Server 2005 / 2008 / 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019※2 各エディションおよび Oracle® Database 12c Release 1※3 / Release 2※3		

※1「サーバー監査」<オプション(Ent/Pro/Tel/LT/500/ST)>のオプション機能としてご購入いただける機能です。※2 Microsoft SQL Server 2019に対応するOSはWindows Server 2016 / 2019です。※3 監査対象のOracle Databaseサーバーの対応OSは、Red Hat Enterprise Linux Server x64 5.6以降 / 6 / 7 / 8、Windows Server x64 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019です。

申請・承認ワークフローシステムWebサーバー <オプション(Ent/Pro/Tel/LT/500/ST)>

CPU	デュアルコア Intel® Xeon®　2.0GHz以上	メモリ	2GB以上
ハードディスク	10GB以上の空きがあること		
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter　● Windows Server 2016 Standard、Datacenter　● Windows Server 2019 Standard、Datacenter		
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること
その他	Apache Tomcat 9.0.50、Java SE Runtime Environment 6 / 7 / 8 / 10、OpenJDK 11 / 12 / 13 / 14 / 15 / 16、Play Framework 1.2.7.2		

申請・承認ワークフローシステムデータベースサーバー <オプション(Ent/Pro/Tel/LT/500/ST)>

CPU	デュアルコア Intel® Xeon®　2.0GHz以上	メモリ	2GB以上
ハードディスク	20GB以上の空きがあること		
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter　● Windows Server 2016 Standard、Datacenter　● Windows Server 2019 Standard、Datacenter		
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること
その他	Microsoft SQL Server 2014 Express Edition SP3 / 2019 Express Edition※1(Microsoft .NET Framework 3.5 SP1 / 4 / 4(日本語言語パック)が必要)		

※1 Microsoft SQL Server 2019に対応するOSはWindows Server 2016 / 2019です。

残業申請Web承認システムWebサーバー※1

CPU	Intel® Xeon®　1.8GHz(2コア/4スレッド)以上	メモリ	4GB以上
ハードディスク	10GB以上の空きがあること		
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter　● Windows Server 2016 Standard、Datacenter　● Windows Server 2019 Standard、Datacenter		
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること
その他	Internet Information Services 8.0 / 8.5 / 10.0、Microsoft .NET Framework 4.6.2以降		

※1 残業申請Web承認機能を使用するには、リバースプロキシサーバー、またはロードバランサーが必要です。

残業申請Web承認システムデータベースサーバー

CPU	Intel® Xeon®　1.8GHz(2コア/4スレッド)以上	メモリ	4GB以上	ハードディスク	20GB以上の空きがあること
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter　● Windows Server 2016 Standard、Datacenter　● Windows Server 2019 Standard、Datacenter				
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること		
その他	Microsoft SQL Server 2014 Express Edition SP3 / 2019 Express Edition※1(Microsoft .NET Framework 3.5 SP1 / 4 / 4(日本語言語パック)が必要)				

※1 Microsoft SQL Server 2019に対応するOSはWindows Server 2016 / 2019です。

在席確認・インスタントメッセージ機能サーバー <オプション(Ent/Pro/Tel/LT/500/ST)>

CPU	Intel® Xeon®　1.8GHz(2コア/4スレッド)以上	メモリ	4GB以上	ハードディスク	20GB以上の空きがあること
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter　● Windows Server 2016 Standard、Datacenter　● Windows Server 2019 Standard、Datacenter				
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること		
その他	Microsoft SQL Server 2014 Express Edition SP3 / 2019 Express Edition※1				

※1 Microsoft SQL Server 2019に対応するOSはWindows Server 2016 / 2019です。

モバイル情報収集サーバー※1 <オプション(Ent/Pro/Tel/LT/500/ST)>

CPU	Intel® Xeon® E5405　2GHz以上	メモリ	4GB以上	ハードディスク	20GB以上の空きがあること
OS	● Windows Server 2016 Standard、Datacenter　● Windows Server 2019 Standard、Datacenter				
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること		
その他	Internet Information Services 8.0/8.5/10、Microsoft .NET Framework 3.5 SP1				

※1 iOS対応の場合、インターネットに公開する必要があります。また、モバイル情報収集サーバーに対してはSSL(HTTPS)によって通信が行える必要があります。SSLの証明書には自己署名証明書もご利用いただけますが、商用のSSL電子証明書(有償)のご利用を推奨いたします。

モバイル情報中継サーバー <オプション(Ent/Pro/Tel/LT/500/ST)>

CPU	Intel® Xeon® 5130　2GHz以上※1	メモリ	2GB以上※2	ハードディスク	20GB以上の空きがあること※3
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter　● Windows Server 2016 Standard、Datacenter　● Windows Server 2019 Standard、Datacenter				
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること		
その他	XmlLite ランタイム				

※1 モバイル端末が1,000台以上の場合は、Xeon X3230 2.66GHz、Xeon E5540 2.53GHz以上が必要です。※2 モバイル端末が1,000台以上の場合は、8GB以上のメモリが必要です。※3 モバイル端末が1,000台以上の場合は、40GB以上の空きが必要です。また、運用状況により異なります。

グローバルマスターサーバー※1

CPU	16コア32スレッド以上	メモリ	32GB以上	ハードディスク	350GB以上の空きがあること
OS	● Windows Server 2012 Standard、Datacenter、R2 Standard、R2 Datacenter　● Windows Server 2016 Standard、Datacenter　● Windows Server 2019 Standard、Datacenter				
ディスプレイ	1024×768 16bit Color以上	ネットワーク	TCP/IP通信ができるネットワークであること		
その他	Microsoft .NET Framework 4 / 4(日本語言語パック)、Microsoft SQL Server 2014 Standard Edition SP3 x64※2 / 2019 Standard Edition※3				

※1 グローバルマスターサーバー環境で使用する管理機には、3GB以上のメモリが必要です。※2「Standard Edition」以上のエディションに対応しています。詳しくは、Webサイトの技術資料(https://www.skyseaclientview.net/ver17/technicalsheet/)をご確認ください。※3 Microsoft SQL Server 2019に対応するOSはWindows Server 2016 / 2019です。

クラウド対応について※1※2※3

対応サービス(IaaS)	● IIJ GIO　● Amazon EC2　● 株式会社インテック製「EINS/SPS SelfPortal」　● 株式会社STNet「STクラウド サーバーサービス [FLEXタイプ]」 ● NTT Com Enterprise Cloud　● ニフクラ　● FUJITSU Cloud Service for OSS　● Microsoft Azure Virtual Machines
以下のシステムについて、対応サービス(IaaS)上での動作をサポートいたします。 ● 管理機・端末機　● マスターサーバー・データサーバー　● ログ解析用サーバー / レポート用サーバー　● HTTPゲートウェイサーバー ● サーバー監査用モジュール / データベース監査用モジュール　● 申請・承認ワークフローシステムWebサーバー ● 申請・承認ワークフローシステムデータベースサーバー　● モバイル情報収集サーバー　● モバイル情報中継サーバー	
対応サービス(DaaS)	● Amazon WorkSpaces※4　● Amazon AppStream　● Azure Virtual Desktop
以下のシステムについて、対応サービス(DaaS)上での動作をサポートいたします。 ● 端末機	

※1 必要なインスタンスは、それぞれカタログに記載のハードウェアスペックに準じます。また、クライアント接続台数が同数であっても実際のシステムの負荷は大きく異なりますので、実際の負荷に合わせて適切なインスタンスを選択してご利用ください。※2 クラウド上と組織内のクライアントPCなどとの通信・ネットワークについては、カタログに記載の制限事項「利用するネットワークについて(P.72)」の条件に沿った構成での構築をお願いいたします。
※3 クラウド利用時には、各クラウドサービス事業者が推奨する可用性の確保やデータバックアップの実施を強くお勧めいたします。※4 SKYSEA Client View Ver.16.0をご利用の場合、「管理機設定」画面に表示されるクライアントライセンス数の内訳において、Amazon WorkSpaces上の端末が、VDI方式ではなく物理PCとして判定されます。VDI方式の端末として判定させる手順については、弊社までお問い合わせください。

ハードディスク空き容量について

画面操作録画のデータ容量 (1台1fpsの場合1時間で約20MB)	【常時録画】1日 8時間　約160MB(例. 端末機100台に対して3か月間ログを取った場合 … 約1,440GB) 【検知録画】1日(約2時間※1) 約40MB(例. 端末機100台に対して3か月間ログを取った場合 … 約360GB)
ログデータ容量※2	1日 約1MB※3

※1 検知録画の設定によっては、常時録画に近い容量が必要になる場合があります。※2 ログデータを圧縮していない場合の参考値です。※3 事務作業など一般的な業務利用の場合です。ご利用環境によっては、1日約5MB以上になる場合があります。メール送信ログ、クリップボードログは、この参考値の範囲に含みません。

協業・連携ソリューション※1※2※3

サイバー攻撃対策	次世代ファイアウォール・UTM・サンドボックス	● 日本電気株式会社　Aterm SA3500G、UNIVERGE IXシリーズ ● パロアルトネットワークス株式会社 次世代ファイアウォール WildFire 脅威分析および防御サービス※4	● FireEye, Inc.　FireEye ● フォーティネットジャパン株式会社　FortiGate
	エンドポイントセキュリティ製品（アラート）	● ウェブルート株式会社　Webroot SecureAnywhere Business エンドポイント プロテクション ● 株式会社FFRI　FFRI yarai ● 株式会社カスペルスキー Kaspersky Endpoint Security for Windows ● ヴイエムウェア株式会社　VMware Carbon Black	● キヤノンマーケティングジャパン株式会社 ESETセキュリティ ソフトウェア シリーズ ● Symantec Endpoint Protection ● トレンドマイクロ株式会社 ウイルスバスター™ Corp. 11.0 SP1 / XG、Trend Micro Apex One™ ● パロアルトネットワークス株式会社　Traps ● BlackBerry Japan株式会社　BlackBerry® Protect
	設定ファイルの適用・配布 / インストール・アンインストール / ログ収集		● 株式会社Blue Planet-works AppGuard® Enterprise、AppGuard® Solo
ウイルス対策※5	ウイルス対策製品インストール状況	● エフセキュア株式会社 ● 株式会社カスペルスキー ● ヴイエムウェア株式会社　VMware Carbon Black ● キヤノンマーケティングジャパン株式会社 ESETセキュリティ ソフトウェア シリーズ ● サイバーリーズン・ジャパン株式会社　Cybereason NGAV	● ノートンアンチウイルス※6 ● トレンドマイクロ株式会社 ● 日本マイクロソフト株式会社 ● BlackBerry Japan株式会社　BlackBerry® Protect ● マカフィー株式会社
統合ログ管理		● 株式会社インテック　LogRevi	● インフォサイエンス株式会社　Logstorage
不許可端末検知・遮断（不許可端末遮断ユニット）		● 株式会社ソフトクリエイト　L2Blocker ● 日本シー・エー・ディー株式会社 IntraGuardian2+ for SKYSEA、IntraGuardianSmart for SKYSEA	● 日本電気株式会社　InfoCage 不正接続防止 ● 株式会社PFU　iNetSec Smart Finder、iNetSec SF
USBデバイス管理・利用制限※7	USBデバイス管理	● 株式会社アイ・オー・データ機器　EasyDiskシリーズ ● ITGマーケティング株式会社 Samsung Portable SSD T7、Samsung Portable SSD T7 Touch ● イーディーコントライブ株式会社　Traventy 3 ● NECソリューションイノベータ株式会社　NonCopy for USB	● エレコム株式会社 ● 株式会社グリーンハウス　GH-UF3VCシリーズ、GH-UF3SRシリーズ ● ハギワラソリューションズ株式会社 ● 株式会社バッファロー
	USBメモリ型ウイルスチェックツール	● エレコム株式会社　USBメモリ型ウイルスチェックツール	● ハギワラソリューションズ株式会社　USBメモリ型ウイルスチェックツール
個人情報利用状況確認	個人情報利用状況確認	● アララ株式会社　P-Pointer File Security	● 三菱スペース・ソフトウエア株式会社　すみずみ君
	個人情報利用状況確認と暗号化		● 東芝情報システム株式会社　Secure Protection
暗号化		● チェック・ポイント・ソフトウェア・テクノロジーズ株式会社 Check Point Full Disk Encryption ● 株式会社日立製作所　JP1 / 秘文 Data Encryption	● 株式会社日立ソリューションズ　秘文 Data Encryption ● 株式会社富士通ビー・エス・シー　FENCE-Works、FENCE-Pro
プリンター連携	印刷ログ	● サイオステクノロジー株式会社　Quickスキャン、Speedoc	● ドロシーワークス株式会社　PRINT EYE※8
	プリンター MIB情報	● キヤノン株式会社 ● コニカミノルタ株式会社 ● シャープ株式会社	● セイコーエプソン株式会社 ● 富士フイルムビジネスイノベーション株式会社 ● 株式会社リコー
勤怠 / 就業管理システム連携		● アマノ株式会社　TimePro-VG、TimePro-NX ● 株式会社オービックビジネスコンサルタント 奉行Edge 勤怠管理クラウド ● クロノス株式会社　就業管理システム クロノスPerformance ● 京葉システム株式会社　タイム・ワークス	● 日通システム株式会社　勤次郎 Enterprise 就業ソリューション※9 ● 株式会社日立ソリューションズ　人事総合ソリューション リシテア ● 富士通株式会社　FUJITSU Enterprise Application GLOVIA iZ 就業 ● 三菱電機ITソリューションズ株式会社　ALIVE SOLUTION TA ● 株式会社両備システムズ 公開羅針盤
SDN / ネットワーク機器連携		● アライドテレシス株式会社　AT-SESC	● パナソニックLSネットワークス株式会社 PPS（Power to Progress SDN）
仮想化・シンクライアント		● ヴイエムウェア株式会社 サーバー仮想化　：VMware ESXi™ デスクトップ仮想化　：VMware Horizon® View™ アプリケーション仮想化：VMware Horizon® View™ ● システムインテリジェント株式会社　Fogos PRO ● シトリックス・システムズ・ジャパン株式会社 サーバー仮想化　：Citrix® Hypervisor デスクトップ仮想化　：Citrix® Virtual Apps and Desktops アプリケーション仮想化：Citrix® Virtual Apps and Desktops	● Ｓｋｙ株式会社　SKYDIV Desktop Client ● 日本電気株式会社　デスクトップ仮想化：VirtualPCCenter ● 日本ヒューレット・パッカード株式会社　デスクトップ仮想化：CCI ● 日本マイクロソフト株式会社 サーバー仮想化　：Microsoft Hyper-V アプリケーション仮想化：Microsoft Remote Desktop Service
認証		● 日本情報システム株式会社　Yubi Plus ● 富士通株式会社　AuthConductor※10、SMARTACCESS/Premium、PalmSecure LOGONDIRECTOR	● 株式会社ローレルインテリジェントシステムズ　FSS® スマートシリーズ
ファイル無害化		● 株式会社ブロット　Smooth File® ネットワーク分離モデル	
SKYSEA Client View インストール対応NAS		● 株式会社アイ・オー・データ機器 ● エレコム株式会社	● 株式会社バッファロー
	SKYSEA Client View プリインストールモデル		● 株式会社アイ・オー・データ機器　APX-SCVF2D

連携ソリューションのご利用には、Sky株式会社の商品および各メーカー様の製品のバージョンなど、条件がある場合があります。詳細についてはSky株式会社までお問い合わせください。

※1 一部、連携対応予定の製品もございます。※2 メーカー様は五十音順にて記載しています。※3 製品が多数ある場合は、メーカー様名のみ記載しています。※4「パロアルトネットワークス次世代ファイアウォール」のサブスクリプションサービスとなります。※5 各メーカー様の詳しい対応製品については、Webサイトの技術資料「ウイルス対策ソフトウェア対応表」をご覧ください。※6 そのほかにも対応商品がございます。※7 各メーカー様の詳しい対応情報については、Webサイトの「動作検証済みUSBメモリ（各種USBデバイス含む）」に関する情報をご覧ください。※8 Ver.3.1.251.0 Early 2021 Update以降に対応しています。※9 連携メーカー様にてSKYSEA Client Viewとの連携機能を開発・検証・ご提供いただいています。※10 連携対象となる AuthConductor は、サーバー型のAC SE/EE です。

制限事項

2021年9月8日時点の情報です。最新情報は、Webサイト（https://www.skyseaclientview.net/ver17/limit/）でご覧いただけます。
SKYSEA Client Viewの技術資料については、Webサイト（https://www.skyseaclientview.net/ver17/technicalsheet）でご覧いただけます。

動作環境について

OSについて	● 英語版OSには、端末機のみ対応となります。アンケート・注意表示等の各種表示は日本語になります。インストールにあたっては、別途日本語ランゲージパックのインストールが必要です。 ● 64bit版OSおよび英語版OSの対応ソフトウェアは、記載されている製品の中で、64bit版OSおよび英語版OSそれぞれに対応しているソフトウェアのみとなります。 ● 英語版Windowsに関して、CD-R / DVD-Rへの書き込み、Webアクセス等への注意表示設定および操作ログは、OSの標準機能、または日本語版の対応ソフトウェアのみ対応となります。アンケート、注意表示等の端末機側UIの英語対応は行っておりません。文字化けへの対応には、別途日本語ランゲージパックのインストールが必要になります。端末機以外は対応をしておりません。 ● 動作環境（P.67～71）に記載のOSは、サービスパックまで指定されたもののみ対応となります。その他のエディションについては、別途お問い合わせください。 ● SKYSEA Client View端末機（Windows）がインストールされたサーバーにおいて、「サーバーの役割と機能」から追加可能なすべての役割や機能に対して正常動作を保証することはできません。現状、フェールオーバークラスタリング機能ではフェールオーバーが正しく行われない場合があります。詳しくは、弊社までお問い合わせください。 ● Windows標準動作のターミナルサービスを停止している場合、SKYSEA Client Viewの一部機能が利用できません。Sky株式会社（以下、弊社）までお問い合わせください。 ● Windows 2000環境でウイルスバスターコーポレートエディション10.0と併用する場合、SKYSEA Client Viewが正常に動作しない場合があります。詳しくは、弊社までお問い合わせください。 ● Windows RTには対応していません。　● Mac端末対応に関する制限事項については、「Mac端末運用管理について（P.79）」をご覧ください。 ● Windows 8.1における、「Assigned Access Mode」での動作およびNFC（Near Field Communication）による印刷はサポートしておりません。 ● Windows 10のタブレットモードでは、SKYSEA Client Viewの管理機は非対応です。 ● Windows 10の場合、SKYSEA Client Viewがインストールされた状態でのプロビジョニング パッケージ（.ppkg）の利用、デバイスガード、企業データの保護（EDP）には非対応です。 ● Windows 10の大型アップデートへの対応は、Semi-Annual Channelでの大型アップデートの配信開始までに、サポート中の最新バージョンに対する更新プログラムまたは対応バージョンへのアップデーターのリリースにて対応します。Windows 10の大型アップデートがSemi-Annual Channel（Targeted）に配信が開始され、適用されると動作保証外となりますのでSemi-Annual Channelでの運用を推奨します。SKYSEA Client Viewの更新プログラムの適用または対応バージョンへアップデート後、Windows 10大型アップデートの実施を行ってください。 ● SKYSEA Client View端末機（Windows）がインストールされた端末の、Windows 10未満からWindows 10へのアップデートについては、元のOSがWindows 7以降の場合にのみ対応しています。それ以前のOSの場合は、SKYSEA Client Viewをアンインストールした上で、OSのアップデートを行ってください。 ● SKYSEA Client View端末機（Mac）がインストールされている端末の、macOS Sierraへのアップデートについては、元のOSが、OS X El Capitanの場合のみに対応しています。それ以外のOSの場合は、SKYSEA Client Viewをアンインストールした上で、OSのアップデートを行ってください。 ● Windowsコンテナには非対応です。　● Windowsサンドボックスには、SKYSEA Client Viewを構築できません。 ● SHA-2形式のコード署名がサポートされていない環境では、一部の機能をご利用いただけません。
利用するネットワークについて	● ほかの通信により、SKYSEA Client Viewが利用可能な帯域幅が確保できない場合には、本ソフトウェアを正常にご利用いただけない場合があります。 ● ネットワークについては、TCP / IPによって、クライアント同士およびクライアントとサーバー間が相互に通信できる必要があります（NAT環境については、お客様のネットワークによってご利用いただける場合がございます。詳しくは、弊社までお問い合わせください）。 ● ネットワークについては、HUBやルーター、クライアントファイアウォールなどにおいて、SKYSEA Client Viewが使用する通信ポートは相互に通信できるように設定していただく場合があります。
メモリについて	● 本ソフトウェアをクライアントPCに導入される場合には、本ソフトウェアが動作するために十分なメモリ容量が必要です（業務で利用するアプリケーションなどで搭載されているメモリが使われてしまっている場合には、動作しない、動作が極端に遅くなるなどの可能性があります）。
サーバーについて	● サーバーについては、SKYSEA Client Viewのみが動作するサーバーをご用意ください。Active Directoryの管理、ファイル・プリンターの共有なども含め、ほかの用途で利用されるサーバーとの共存利用は行わないようにしてください。サーバーの増設が難しい場合は仮想化も可能ですのでご検討ください。 ● サーバーが複数台設置される環境下ではSKYSEA Client Viewのバージョンは同一のバージョンでご利用ください。また、アップデートを行う際はバージョンを統一してからご利用ください。 ● クライアントの台数分のCAL（クライアントアクセスライセンス）が必要です。
データサーバーの台数について	● クライアントの利用状況により、負荷は大幅に異なります。 ● 適正台数については、クライアント側の使用頻度などについて、十分な調査の上、適切な台数算出と配置をお願いいたします。
各種収集したログのディスク使用量について	● クライアントの利用状況により、収集されるログサイズは大幅に異なります。 ● ログを収納するディスク容量を算出する際には、クライアント側の使用頻度などについて、十分な調査の上、必要なログのディスク容量を算出していただきますようお願いいたします。
管理機について	● エンタープライズモードおよびソフトウェア資産管理（SAM）機能は、Windows 2000 SP3ではご利用いただけません。 ● Windows 2000 SP4でご利用の場合は、「Windows 2000 SP4用の更新プログラムロールアップ 1」の適用が必要です。 ● 送信メールログの添付ファイル追跡をWindows 2000の管理機で行う場合は、Windows 2000 Professional SP4とWindows 2000 SP4用の更新プログラムロールアップ 1を適用してください。また、Windows XPの管理機で行う場合は、Professional SP2以降を適用してください。
本商品とその他ソフトウェアとの動作について	● 再起動ごとにハードディスクの内容を復元する環境修復ソフトウェアをお使いの場合は、本ソフトウェアが正しく動作しない場合があります。 ● OS（ファイルシステム）を経由しないファイル操作や特殊な処理を行っているアプリケーションによるファイル操作など、操作ログの取得が行えないため、アラート設定や記憶媒体の制御などSKYSEA Client Viewが正常に動作しない場合があります（暗号化ソフトウェアやデバイス制御ソフトウェア（秘文AE/IC・IF等）が該当します）。
Windows To Go について	● デバイス管理、セキュリティ管理、ログ管理などの一部機能は、Windows To Go導入済みのデバイスに対応していません。
その他	● TOE（TCP / IP Offload Engine）を無効にしてご利用ください。 ● ビデオカードの種類によりリモート操作や管理機の利用が正常に行えない場合があります。 ● Windowsのフォントサイズを標準と異なる値に設定されている場合には、GUI画面が正しく表示されない場合があります。 ● Windows XPモードの仮想マシン上にインストールされたSKYSEA Client Viewはクライアントライセンスを消費しませんが、そのためにはWindows Virtual PCの「統合機能」を有効にしておく必要があります。 ● HTTPゲートウェイサーバーや資産データ / ログデータ Web閲覧機能サーバー、申請承認ワークフローシステムなどの環境を構築するにはJavaが必要です。対応するJavaは無償版の「OpenJDK 11」です。

Microsoft Office製品用のアドイン（Officeアドイン）について

- 次の機能はOfficeアドインによって提供されます。
  - ○ Microsoft Exchange接続による送信メールログ取得
  - ○ Microsoft Exchange Online接続による送信メールログ取得
  - ○ SMTP over SSL / TLSによる送信メールログ取得
  - ○ Microsoft Word / Excel / PowerPointの「名前を付けて保存」時のログ取得
  - ○ Microsoft Word / Excel / PowerPointのプリントログの印刷ファイルパス取得
  - ○ メール送信宛先フィルタリング
  - ○ メール添付ファイルの自動暗号化
  - ○ メール添付ファイルの自動削除
- OfficeアドインにはSKYSEA Client View Ver.9で追加されたアドインと、Ver.8.2以前のアドインがあります。
- SKYSEA Client View Ver.9以降のアドイン、Ver.8.2以前のアドイン共通
  - ○ Windows XP Professional SP1には対応していません。
  - ○ Microsoft Office製品のセキュリティ設定のレベルによっては、SKYSEA Client Viewのアドインが読み込まれず、アドインによって提供される機能がお使いになれない場合があります。
  - ○ Windows ストアアプリ版のMicrosoft Office 2016 / 2019には対応していません。
  - ○ SMTP over SSL/TLSによる送信メールログは、SMTP接続による送信メールログと合わせて重複して取得されます。
- SKYSEA Client View Ver.8.2以前のアドインについて
  - ○ ログを収集するには「Microsoft .NET Framework 2.0」のインストールが必要です。端末機のOSがWindows 2000の場合は「Microsoft .NET Framework 1.1」も必要です。Microsoft Office 2010の64bit版を利用する場合には、「Microsoft .NET Framework 3.5」のインストールが必要です。Microsoft Office 2013を利用する場合は、「Microsoft .NET Framework 3.5」または「Microsoft .NET Framework 4.0」が必要です。
  - ○ インターネット接続ができない環境では、Microsoft .NET Frameworkの挙動により、Microsoft Office製品の起動に時間がかかる場合があります。

Microsoft Office製品用のアドイン（Officeアドイン）について

○ インターネット接続ができない環境では、Microsoft Wordの起動に時間がかかる場合があります。詳細については、Microsoft社のサポートページをご確認ください。
○ Microsoft Outlook 2003をご利用の場合、「KB2293428」の更新プログラムが適用されていると送信メールログの収集が行えません。回避方法に関しては、弊社までお問い合わせください。
○ Officeアドイン設定で、Ver.8.2以前のアドインが選択されている場合でも、Microsoft Office 2016がインストールされている端末では、Ver.9.0以降のアドインが使用されます。

資産管理について

ウイルス対策ソフトウェアについて	● ウイルス対策ソフトウェアの情報が収集できる製品は、以下の製品のみです。 ○ エフセキュア社製 F-Secure Client Security 12、F-Secure Client Security Premium 12、F-Secure Server Security 12、F-Secure Server Security Premium 12、F-Secure Email and Server Security 12、F-Secure Email and Server Security Premium 12、F-Secure PSB Workstation Security 12、F-Secure PSB Server Security 12、F-Secure PSB Email and Server Security 12 ○ トレンドマイクロ社製 ウイルスバスター 2008 / 2009 / 2010、ウイルスバスター コーポレートエディション 7.3 / 8.0 / 10.0 / 10.0 SP1 / 10.5 / 10.6 / 10.6 SP2 / 10.6 SP3 / 11.0 / 11.0 SP1 / XG、Trend Micro Apex One（オンプレミス版 / SaaS版）、Trend Micro ビジネスセキュリティ 6.0、ウイルスバスタービジネスセキュリティ 7.0 / 9.0 / 9.5 /10.0、ServerProtect for Linux 3 ○ ノートンライフロック社製 ノートン アンチウイルス 2006 / 2007 / 2008 / 2009 / 2010 / 2011 / 2012 ○ ブロードコム社製 Symantec AntiVirus Corporate Edition 10.0.x / 10.1.x / 10.2.x、Symantec Endpoint Protection 11.0 / 12.1 ○ マカフィー社製 McAfee VirusScan Enterprise Ver.8.7i / 8.8、McAfee SaaS Endpoint Protection、McAfee Total Protection Service v5.0、McAfee Endpoint Security 10（ただし、McAfee Endpoint Security 10に関しては、インストール時に「Threat Prevention:脅威対策」項目のチェックボックスをオフにした場合、プログラムバージョンのみが収集されます。） ○ Cybereason社製 Cybereason NGAV ○ ESET社製 ESET NOD32 アンチウイルス 3.0 / 4.0 / 4.2 / 5.0 / 6.0 / 7.0 / 8.0 / 9.0 / 10.0 / 11.0 / 12.0 / 13.0 / 14.0、ESET Smart Security V3.0 / V4.0 / V4.2 / V5.0 / V6.0 / V7.0 / V8.0 / V9.0、ESET Internet Security 10.0 / 11.0 / 12.0 / 13.0 / 14.0、ESET Endpoint Security、ESET Endpoint アンチウイルス ○ Microsoft社製 System Center 2012 / 2012 R2 / 2016 / 2019、Forefront Endpoint Protection 2010、Security Essentials ● 検索エンジンバージョン、プログラムバージョン、パターンファイルバージョンのみ収集できる製品は、以下の製品のみです。 ○ F-Secure Linux Security 11　○ F-Secure PSB Linux Security 11 ● 検索エンジンバージョン、パターンファイルバージョン、パターンファイル更新日時のみ収集できる製品は、以下の製品のみです。 ○ Microsoft社製 Microsoft Defender ● プログラムバージョン、パターンファイルバージョン、パターンファイル更新日時のみ収集できる製品は、以下の製品のみです。 ○ F-Secure Client Security 13 / 14 / 15　○ F-Secure Email and Server Security Premium 14 / 15　○ ノートン アンチウイルス ○ F-Secure Client Security Premium 13 / 14 / 15　○ ヴイエムウェア株式会社 VMware Carbon Black　○ ノートン アンチウイルス プラス ○ F-Secure Server Security 14 / 15　○ Symantec Endpoint Protection 14 / 14.1 / 14.2 / 14.3　○ ノートン インターネット セキュリティ ○ F-Secure Server Security Premium 14 / 15　○ ノートン セキュリティ ○ F-Secure Email and Server Security 14 / 15　○ ノートン 360 ● プログラムバージョンとパターンファイル更新日時のみ収集できる製品は、以下の製品のみです。 ○ カスペルスキー社製 カスペルスキー アンチウイルス 2012 / 2013 / 2014 / 2015、カスペルスキー インターネットセキュリティ 2012 / 2013 / 2014 / 2015 / 2016 / 2017 / 2018 / 2019 / 2020 / 2021、Kaspersky Endpoint Security for Windows 8 / 10 / 11 ○ ウイルスバスター 2011 / 2012、ウイルスバスタークラウド ● プログラムバージョンのみ収集できる製品は、以下の製品のみです。 ○ Kaspersky Endpoint Security for Linux 8 / 10 / 11 ○ BlackBerry Japan社製 BlackBerry Protect ○ Symantec Endpoint Protection Linux版 12.1 / 14 / 14.1 / 14.2 / 14.3 ○ McAfee VirusScan Enterprise for Linux 1.6.0 / 1.7.1 / 1.9 / 2.0、McAfee Endpoint Security Linux版 10 ※詳しい対応状況については、Webサイトの技術資料をご覧ください。
Microsoft Officeについて（Windows版）	● Microsoft Office状況として、ソフトウェア情報が収集できるWindows版のバージョンは、以下のバージョンのみです。 ○ 対応オフィスソフトウェア Microsoft Office 2000 / XP / 2003 / 2007 / 2010 / 2013 / 2016 / 2019 ※ただし、プロダクトキーの収集は、Microsoft Office 2010以降に対応しています。また、Windows端末のみ対応しています。 ● 以下のバージョンは、Microsoft Office状況として、ソフトウェア情報が収集できません。通常のアプリケーションとしてのソフトウェア情報の収集となります。 ○ クイック実行でインストールされたMicrosoft Office 2013 / 2016のAccess以外の単体製品　○ Microsoft Office Visio製品 ○ クイック実行でインストールされたMicrosoft Office 2019の単体製品　○ Microsoft Office Project製品 ○ Windows ストアアプリ版のMicrosoft Office 2016 / 2019　○ Microsoft Office SharePoint Design ● SKYSEA Client Viewで収集可能なMicrosoft Office 2010 / 2013 / 2016のプロダクトIDは、Microsoft Officeの画面上で表示されるプロダクトIDとは異なります。 ● インストール日の日付は、Microsoft Update等によって、初回インストール以後に更新される場合があります。 ● Microsoft Office（2013 / 2016 / 2019）のクイック実行によるインストールでは、プロダクトID、GUID、プリインストールの項目について、収集可能な情報がないため収集できません。
Autodesk社製ソフトウェアについて	● シリアル番号が取得できる製品は以下のとおりです。なお、2017以降の製品については、シリアル番号は取得できません。 ○ AutoCAD 2010 / 2011 / 2012 / 2013 / 2014 / 2015 / 2016　○ AutoCAD Civil 3D 2010 / 2011 / 2012 / 2013 / 2014 / 2015 / 2016 ○ AutoCAD Electrical 2010 / 2011 / 2012 / 2013 / 2014 / 2015 / 2016　○ AutoCAD LT 2010 / 2011 / 2012 / 2015 / 2016 ○ AutoCAD Mechanical 2010 / 2011 / 2012 / 2013 / 2014 / 2015 / 2016　○ Autodesk Inventor 2010 / 2011 / 2012 / 2013 / 2014 / 2015 / 2016 ○ AutoCAD Map 3D 2010 / 2011 / 2012 / 2013 / 2014 / 2015 / 2016
Web会議システムについて	● Web会議システムの情報が収集できる製品は以下のとおりです。 ○ Amazon Chime　○ Cisco Webex　○ Microsoft Teams　○ Slack ○ Zoom
ネットワーク機器情報収集について	● 情報が収集できるのは、収集を行う管理機から「net view」コマンドによって探索できるドメイン / ワークグループ内の端末のみです。ネットワーク探索とファイル共有が無効になっている場合など、「net view」コマンドで探索できない端末の情報は収集できません。 ● SKYSEA Client View以外の不許可端末検知ソフトウェア / 機器で検知した端末の情報は収集されません。 ● MACアドレスが収集できない端末の情報は収集されません。 ● ネットワーク機器の自動収集設定と不許可端末検知の両方が有効な場合において、以下の端末の情報は収集されません。 ○ 「不許可端末検知設定」で「許可ハードウェア」として登録されている端末 ○ 「許可 / 不許可ハードウェアー覧」への自動登録の除外対象に設定されているIPアドレスの端末 ● ネットワーク経路情報を収集するには、経路上の機器の各種MIB情報をSNMPで取得できる必要があります。 ● 本機能は、組織外の機器の情報収集を目的としたものではありません。
プリンターについて	● プリンターのIPアドレスが取得できるのは、Windows端末に直接接続されているネットワークプリンターで、レジストリにIPアドレス情報が存在する場合のみです。 ● Linux端末では、CUPSと呼ばれる印刷システムより情報を取得します。そのため、CUPS以外の印刷システムが使用されている場合は、プリンター情報は収集できません。
ソフトウェア配布について	● 配布 / インストールできるアプリケーションは、弊社にて「ソフトウェア情報」をご提供しているアプリケーションに限ります。 ● ソフトウェア配布中継機能をご利用にあたり中継のためのクライアントPCに別途、ソフトウェア配布中継用モジュールのインストールが必要です。 ● Windows ストアアプリは配布できません。 ● Windows XPモードや仮想環境上の端末機、Windows 8 / Windows 8.1で高速シャットダウンした（ハイブリッドブートが有効な）端末機については、電源オプションを設定しても、配布時に電源をONにできません。 ● 配布時にマスターサーバーとは異なるセグメントの端末機の電源をONするには、各セグメントに少なくとも1台のソフトウェア配布用中継端末があり、マスターサーバーと通信できる必要があります。中継端末とマスターサーバーがHTTP（S）接続の場合は、ご利用いただけません。 ● マルチキャスト配布を利用する場合、ネットワーク環境によっては、警告が発生したり、通信に影響を与えたりする恐れがあります。必ず事前にご利用のネットワーク環境についてご確認ください。 ● スリープ（またはInstant Go）状態のPCに対してソフトウェア配布を行うには、配布対象のPCで次の設定が行われている必要があります。 ○ ソフトウェア配布設定で、スリープから復帰する時刻を設定されていること。 ○ 「Instant Go」が搭載されているPCの場合、「Instant Go」機能が有効になっていること。搭載されていないPCの場合、「スリープ解除タイマーの許可」が有効になっていること。 ○ 「ハイブリッドスリープを許可する」が有効になっている場合に、休止状態に移行していないこと。

資産管理について

省電力設定について	● Windows Server 2003 / Windows Server 2008 / Windows Server 2012などのサーバーOSは、省電力設定の対象外となります。
電源OFFスケジュール機能について	● マスターサーバーおよび、サーバーOS上の端末機は、本機能の対象外です。
資産データWeb閲覧機能について	● 資産データWeb閲覧機能は、Internet Explorer 6 / 7 / 8 / 9 / 10 / 11（Windows ストアアプリ版を含む）に対応しています。
その他	● Windows ストアアプリのInternet Explorerは、資産情報として収集されません。 ● Windows更新プログラム適用状況は、スタンドアロン端末は非対応です。 ● 実行ファイル情報を収集する「実行ファイル情報設定」は、Mac、Linux非対応です。また、電子証明書による収集設定は、Windows 2000でご利用いただけません。 ● macOS 10.13（High Sierra）以降のOSでは、資産情報の「スクリーンセーバーのパスワードによる保護」が収集できません。

ログ管理について

Webアクセスログについて	● Web閲覧（ダウンロード）ログは、Internet Explorer 5.5 SP2 / 6 / 7 / 8 / 9 / 10 / 11、Mozilla Firefox 3.0 / 3.5 / 3.6 / 4.0 / 5.0 / 6.0 / 7.0 / 8.0 / 9.0 / 10.0 / 11.0 / 12.0 / 13.0 / 14.0 / 15.0 / 16.0/ 17.0 / 18.0 / 19.0 / 20.0 / 21.0 / 22.0 / 23.0 / 24.0 / 25.0 / 26.0 / 27.0 / 28.0 / 29.0 / 30.0 / 31.0 / 32.0 / 33.0 / 34.0 / 35.0 / 36.0 / 37.0 / 38.0 / 39.0 / 40.0 / 41.0 / 42.0 / 43.0 / 44.0 / 45.0 / 46.0 / 47.0 / 48.0 / 49.0 / 50.0 / 51.0 / 52.0 / 53.0 / 54.0 / 55.0 / 56.0 / 57.0 / 58.0 / 59.0 / 60.0 / 61.0 / 62.0 / 63.0 / 64.0 / 65.0 / 66.0 / 67.0 / 68.0 / 69.0 / 70.0 / 71.0 / 72.0 / 73.0 / 74.0 / 75.0 / 76.0 / 77.0 / 78.0 / 79.0 / 80.0 / 81.0 / 82.0 / 83.0 / 84.0 / 85.0 / 86.0 / 87.0 / 88.0 / 89.0 / 90.0 / 91.0、Google Chromeの弊社製品リリース時の安定版に対応しています。Windows ストアアプリのGoogle Chromeには対応していません。 ● Mozilla FirefoxやGoogle Chrome、Microsoft Edge（Chromium版）を使用したWebアクセスログ収集を行う場合、Webブラウザのバージョンや環境によっては、SKYSEA Client Viewの拡張機能（アドオン）をユーザーが有効にする必要があります。Webブラウザの仕様が変更された場合は、ログ収集機能をご利用いただくことができなくなる恐れもあります。 ● ご利用のSKYSEA Client ViewおよびMozilla Firefoxのバージョンによっては、アドオン一覧画面に「未検証」の警告が表示されることがあります。 ● Mozilla FirefoxやGoogle Chrome、Microsoft Edge（Chromium版）は、FTPアップロードログには対応していません。 ● Google Chromeを使用したWebアクセスログ収集を有効にしている環境では、Google Chromeの設定を次のように固定するよう制御します。 ○ 「ダウンロード時に各ファイルの保存場所を確認する」→有効 ○ 「ネットワーク動作を予測してページの表示速度を向上させる」→無効 ● Google ChromeやMicrosoft Edge（Chromium版）を使用したシークレットモードでのWebアクセスログ収集を行う場合、非ドメイン環境では拡張機能（アドオン）をユーザーが有効にする必要があります。 ● 「localhost」に対してhttp通信が行えない環境で、Google Chromeを使用したWebアクセスログ収集を有効にすると、ログ収集や使用制限が正しく行われない場合があるため、書き込みやファイルアップロード / ダウンロード操作を一律で禁止するよう制御します。SKYSEA Client Viewでも「localhost」の除外設定を追加しますが、グループポリシーや自動プロキシ構成スクリプトなどで上書きされる場合があるため、ご利用環境に応じて「localhost」を除外してください。 ● Internet Explorerの「Webダウンロード」アラートログの収集を有効にしている環境では、アドオンなしのInternet Explorerの起動を禁止します。ピン留めサイト / 固定サイトのショートカット（*.website）からの起動もできなくなります。 ● Adobe Flash Playerを利用するWebアップロードのログは取得できません。 ● Microsoft Edge（EdgeHTML版）は、20.10240.16384.0 / 25.10586.0.0 / 38.14393.0.0 / 39.15002.1001.0 / 40.15025.1000.0 / 40.15063.0.0 / 41.16299.15 / 42.17134.1.0 / 44.17763.1.0 / 44.18356.1.0 / 44.18362.1.0 / 44.18362.387.0 / 44.18362.449.0 / 44.19041.0.0 / 44.19041.1.0 / 44.19041.423.0のバージョンのみ対応しています。 ● Microsoft Edge（EdgeHTML版）では、操作種別が「Webアクセス」以外のWebアクセスログは取得できません。 ● Microsoft Defender Application Guardを使用した場合、Microsoft Edge（EdgeHTML版）のログは取得できません。
Gmail ウェブメール サービス（以下略称）送信ログについて	● 「Gmail送信」ログは、「Webアクセス」ログとして収集します。そのため「送信メール」ログ関連の機能には対応していません（「電子メール送信」アラート、「電子メール送信宛先フィルタ」アラート、「添付ファイル保存」、「送信メール本文検索」など）。 ● 対応しているGmail送信画面は「標準HTML形式」および「簡易HTML形式」です。 ● 対応しているWebブラウザは、「Webアクセスログについて」の「Web閲覧（ダウンロード）ログ」の対応ブラウザをご覧ください（ただしInternet Explorer 5.5 SP2を除く）。 ● Internet Explorer 11（デスクトップアプリ）のエンタープライズモードは、送信メールログの取得に対応していません。 ● Google ChromeではJavaScriptを有効にしてください。Google Chromeの仕様が変更された場合は、ログ収集機能をご利用いただくことができなくなる場合があります。 ● ログ取得対象となるGmailの言語は、日本語のみです。
Microsoft 365 / Office Onlineのログ収集について	● Word Online / Excel Online / PowerPoint Onlineのファイル作成ログとOutlook Web App / Outlook.comのメール送信ログが、「Webアクセス」ログとして収集できます。 ● Outlook Web App / Outlook.comのメール送信ログは、「Webアクセス」ログとして収集します。そのため「送信メール」ログ関連の機能には対応していません（「電子メール送信」アラート、「電子メール送信宛先フィルタ」アラート、「添付ファイル保存」、「送信メール本文検索」など）。 ● Internet Explorer 11（デスクトップアプリ）のエンタープライズモードは、送信メールログの取得に対応していません。 ● Outlook Web App / Outlook.comのメール送信ログを取得するには、JavaScriptの設定を有効にしてください。 ● WebアクセスのFTPダウンロードログは非対応です。 ● OneDriveの同期によるMicrosoft 365のWebダウンロードについては、ログが複数出力される場合があります。 ● OneDriveへのファイル保存は、ログとして記録されない場合があります。 ● Microsoft 365 / Office Onlineの仕様が変更された場合は、ログ収集機能をご利用いただくことができなくなる場合があります。 ● 「Windows 10 1903」以降のスタートメニューから起動可能な「Word」や「Excel」は、Microsoft Edge（EdgeHTML版）により起動されるため、ログ収集の対象外です。
FTPアップロードログについて	● FTPアップロードログを取得できるのは、以下の条件となります。 ○ 利用クライアントが、FFFTP 1.96 / 1.97 / 1.98 / 1.99 / 2.0 / 3.0 / 3.1 / 3.2 / 3.3 / 3.4 / 3.5 / 3.6 / 3.7 / 3.8 / 3.9 / 4.0 / 4.1 / 4.2 / 4.3 / 4.4 / 4.5 / 4.6 / 4.7 / 4.8 / 4.9 / 4.9.1 / 4.9.2 / 5.0 / 5.1 / 5.2、NextFTP 4、Internet Explorer 5.5 SP2 / 6 / 7 / 8 / 9 / 10 / 11であること。 ○ Socksプロトコルを経由しないFTP接続であること。Socksプロトコルを経由するとアップロード自体が行えません。 ○ FTPS（File Transfer Protocol over SSL/TLS）には対応していません。
送信メールログについて	● Windows ストアアプリによるメール送信ログは、SMTPにのみ対応しています。SMTP over SSL / TLS、およびExchange接続には対応していません。 ● SMTP接続による送信メールで取得できるのは、以下の条件となります。 ○ 利用クライアントが、Microsoft Outlook 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365、Microsoft Outlook Express 6、Windowsメール、Becky! Internet Mail Ver.2、Mozilla Thunderbird 2 / 3.0 / 3.1 / 5.0 / 6.0 / 7.0 / 8.0 / 9.0 / 10.0 / 11.0 / 12.0 / 13.0 / 14.0 / 15.0 / 16.0 / 17.0 / 24.0 / 31.0 / 38.0 / 45.0 / 52.0 / 60.0 / 68.0 / 78.0 / 91.0、Windows Live メール、メール（Windows 8 / Windows 8.1 / Windows 10の標準Windows ストアアプリ）、Mail（Mac OS Xの標準アプリ）であること。 ○ 暗号化されていないSMTPによりメール送信が行われていること。 ● SMTP over SSL / TLS、またはExchange接続による送信メールで取得できるのは、以下の条件となります。 ○ 利用クライアントが、Microsoft Outlook 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365であること。 ○ 本機能では専用のアドインを使用します。アドインに関する制限事項は「Microsoft Office製品用のアドイン（Officeアドイン）について（P.72）」をご覧ください。 ○ 送信済みアイテムに保存されるメッセージがログ取得の対象となります。 ○ Outlookの機能「会議」「タスク」「フィードの共有」に関するログを取得するには、ログ設定で使用するOfficeアドインをVer.9.0以降に設定する必要があります。 ● Webメール、グループウェアメールなどの接続方法は送信メールログとして取得することはできません（Webメールは、Webアクセスログとして、取得することができます）。 ● Microsoft Word、Microsoft Excelなど、メールソフトウェア以外からのメール送信は、送信メールログとして取得することができません。

ログ管理について

ファイル操作ログについて

- OSを経由しないファイル操作や特殊な処理を行っているアプリケーションによるファイル操作など、ファイル操作ログが取得できない場合があります。
- 暗号化ソフトウェアをご利用の場合、暗号化ソフトウェアが暗号化や復号処理を行うため、ファイル操作ログを取得できない場合があります。
- コマンドプロンプト上でのログ収集に対応しているコマンドは、次のとおりとなります。COPY/DEL/ERASE/MD/MKDIR/MOVE/RD/REN/RENAME/REPLACE/RMDIR/SORT/XCOPY/EXPAND/ECHO/FSUTIL/リダイレクト(DIR > DIR.TXTなど)
- Windows PowerShellでのログ収集に対応しているコマンドは、次のとおりとなります。Copy-Item/MkDir/Move-Item/New-Item/Remove-Item/Rename-Item/リダイレクト(DIR > DIR.TXTなど) ※その他の動作についてはお問い合わせください。
- 上書き保存ログは、ファイルの更新が行われ、ファイルを閉じたときに生成されます。
- 上書き保存ログは、OSやアプリケーションが自動的に行ったファイルの更新処理についても生成されます。
- 操作上は上書きであっても、実際の動作としてはファイルの生成およびファイル名変更である場合、上書き保存ログは生成されません(ただし、Microsoft Word / Excel / PowerPointについては、上書きとしてのログも記録されます)。
- ファイル参照ログは、Windows の「最近使ったファイル」/「最近使った項目」に登録されるファイルのみが対象です。また「最近使ったファイル」/「最近使った項目」が更新されない場合はログが取得できません。
- Microsoft OneDriveの同期処理によるファイル操作ログは取得できません。
- Microsoft OneDrive、Microsoft OneDrive for Business、Dropboxの仕様が変更された場合は、「Webストレージ」などのログ項目が収集できなくなる可能性があります。
- Windows 8 / 8.1の「ファイル履歴」機能によるファイル操作ログは取得できません。
- Windows XP以前のクライアントOS、Windows Server 2008以前のサーバーOSでは、Windowsポータブルデバイス(MTP / PTP接続のデバイス)に対するファイル操作ログが取得できません。
- Windows Vistaでも、次の条件を満たしていない場合は、上記の制限事項が適用されます。
  - ○ Service Pack 2と「KB2761494」に加え、「KB971514」または「KB971644」のWindows更新プログラムがインストールされていること。
- Windowsポータブルデバイス上のファイルの「ファイル参照」ログ、およびファイルサイズは取得できません。また、操作によってログの出力内容が特殊になる場合があります。
- ZIPファイル内のファイル情報の収集設定は、Windows端末、スタンドアロン端末のみ対応しています。対応OSは、Windows XP SP2以降のOS、Windows 2000 SP4 + Update Rollup 1、Windows Server 2003 SP1以降のOSとなります。また、利用する圧縮ソフトウェアや指定した形式によっては、ログが取得できないことがあります。

ファイルアクセスログについて

- ネットワークやOSの負荷状況によっては、ファイルアクセスログが取れない場合があります。
- ウイルス対策ソフトウェアとの相性により、ファイルアクセスログが取れない場合があります。
- TOE(TCP / IP Offload Engine)を無効にしてご利用ください。ファイルアクセスログが取れない場合があります。
- マルチセッション環境下からのアクセスによるファイルアクセスログは、アクセスユーザーの情報が正しく取得できない場合があります。
- 共有フォルダに対するファイル操作の通信が、NICチーミングされた仮想ネットワークアダプタを流れない場合は、ファイルアクセスログが取得できません。

ファイル操作ログ / ファイルアクセスログについて

- ファイルサイズ情報は、操作種別やタイミングによっては取得できない場合があります。

「名前を付けて保存」時のログについて

- 「名前を付けて保存」時のログ収集に対応したMicrosoft Office製品のバージョンは、次のとおりです。
  - ○ Microsoft Word 2002 / 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365
  - ○ Microsoft Excel 2000 / 2002 / 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365
  - ○ Microsoft PowerPoint 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365
- 本機能では専用のアドインを使用します。アドインに関する制限事項は「Microsoft Office製品用のアドイン(Officeアドイン)について(P.72)」をご覧ください。

プリントログについて

- 印刷ファイルパス取得に対応したMicrosoft Office製品のバージョンは、次のとおりです。
  - ○ Microsoft Word 2002 / 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365
  - ○ Microsoft Excel 2000 / 2002 / 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365
  - ○ Microsoft PowerPoint 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365
- 対応しているMicrosoft Office製品の印刷ファイルパス取得では専用のアドインを使用します。アドインに関する制限事項は「Microsoft Office製品用のアドイン(Officeアドイン)について(P.72)」をご覧ください。
- ログ収集設定によっては、Windows ストアアプリによるプリントログが取得できなかったり、一部の項目が取得できない場合があります。Windows ストアアプリ以外では、Microsoft EdgeやInternet Explorer 10でも同様の制限があります。
- プリンターにデータが送られた時点で、プリントログとして記録されるため、実際にプリンターで印刷が完了されたかどうかは、ログから確認することはできません。
- プリンターのIPアドレスが取得できるのは、Windows端末に直接接続されているネットワークプリンターで、レジストリにIPアドレス情報が存在する場合のみです。
- ファイルの種類やアプリケーションによっては、印刷ファイルパスが正確に取得できない場合があります。
- Windows ストアアプリは印刷ファイルパス取得に対応していません。

アプリケーションログについて

- 仮想DOSマシンで実行されるアプリケーションは、アプリケーションログとして取得することができません。
- Windows 2000では、アプリケーションログの起動元プロセス情報は取得できません。
- Windows PowerShell ISEで実行したコマンドのログは取得できません。
- command.comで実行したコマンドのログは取得できません。
- コマンド実行で起動したアプリケーションとの対話によるサブコマンドの実行は取得できません。
- バッチファイル内でさらに別のバッチファイルを呼び出した場合、呼び出されたバッチファイルのコマンドのログは取得できません。

スタンドアロン端末機ログ収集について

- スタンドアロン端末機ログ収集をご利用の場合、データサーバーが必要です。
- 対象のクライアントPC(Windows のみ)に別途、スタンドアロン端末機用モジュールのインストールが必要です。

通信デバイス接続ログについて

- Bluetoothデバイスのログ取得(およびデバイスの使用禁止)を行うには、Microsoft標準のBluetoothドライバーが必要です。
- Microsoft標準のBluetoothドライバーの場合でも、OSのバージョンによっては、以下の制限があります。
  - ○ Windows XP SP1以前のOSでは、Bluetoothデバイスの接続ログが出力できません。
  - ○ Windows XP SP3以前のOSでは、Bluetoothデバイス種別ごとの禁止は行えません(Bluetoothアダプタの無効化により、すべてのBluetoothデバイスが使用禁止になります)。
  - ○ Bluetooth LE(Bluetooth Low Energy)デバイスには対応していません。

Web / アプリケーションアカウント監査について

- Windows端末のみ対応しています。ただし、スタンドアロン端末は非対応です。
- 次のOSではMicrosoft .NET Frameworkアプリケーションのログが取得できません。
  - ○ Windows 2000の場合、Windows XP SP2以前またはSP3で「KB971513」が適用されていない場合、Windows Vista SP1以前またはSP2で「KB971513」が適用されていない場合
- 対応しているWebブラウザは、「Webアクセスログについて(P.74)」に記載されているブラウザのうち、Internet Explorer 5.5 SP2、Mozilla Firefox 3.0 / 3.5以外です。
- Windows ストアアプリ、Windows Presentation Foundation (WPF)アプリ、ブラウザのWindowsネイティブ認証(基本認証)はログが取得できません。また、その他アプリケーションの画面やWebサイトのページの構成によっては、ログが取得できない可能性があります。

ログ解析について

- インストール時には、IIS6.0または、IIS7.0 / IIS7.5 / IIS8.0および、Microsoft .NET Framework 3.5 SP1が必要となります。

CD / DVD / ブルーレイライティングソフトウェアについて

- Windows XP / Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10のエクスプローラによるライティングに対応しています。Windows Vista以降のOSでは、マスターディスク形式にのみ対応しており、ライブファイルシステム形式には対応していません。また、Windows XPのブルーレイは非対応です。
- CD書き込みログは、ISOファイルなどのディスクイメージの書き込みには対応しておりません。ライティングソフトウェア製品のディスクイメージ書き込み機能などを使用してメディアに書き込まれたファイルは、ログに残りません。ただし、「Windows ディスク イメージ書き込みツール」については、利用したイメージファイル名が記録されます。
- ライティングソフトウェアの対応製品は以下のとおりです。(※ブルーレイにも対応)
  - ○ BlindWrite 5
  - ○ B's Recorder GOLD 5/7/9(※)/11(※)/13(※)/16
  - ○ CD Manipulator 2.70 Final
  - ○ Clone CD 5.3.0.1
  - ○ Clone DVD 2.9.0.9
  - ○ CopyToDVD 3.1.3.137
  - ○ Corel VideoStudio Pro X5(※) / X9(※)
  - ○ CyberLink Power2Go 6(※) / 10(※) / 13
  - ○ Easy Media Creator 9 / 10(※)
  - ○ Inter Video DVD Copy 5 Platinum / Gold
  - ○ Nero 7 / 8
  - ○ PowerProducer 5 Ultra(※)
  - ○ Sonic RecordNow 9(※)
  - ○ WinCDR 9.0
  - ○ WinCDR Lite Ver.2
  - ○ Windows DVD メーカー
  - ○ Windows ディスク イメージ書き込みツール

ログ管理について

CD / DVD / ブルーレイライティングソフトウェアについて

- ライティングソフトウェア(パケットライト方式)の対応製品は以下のとおりです。ただし、書き込み制限には対応していますが、CD書き込みログの取得には対応していません。(※ブルーレイにも対応)
  - ○ B's CLiP 5/7
  - ○ CyberLink InstantBurn 5(※)
  - ○ Easy Media Creator 9(Drag-to-Disc)(※)
  - ○ RecordNow 9(Drag-to-Disc)(※)
  - ○ Nero InCD 5
- Corel Video Studio Pro X5 / X9によるCD書き込みログの書き込み元ファイルパスはすべてCorel Video Studio Pro X5 / X9の作業フォルダとなります。

ログデータWeb閲覧機能について

- 本機能はデータサーバーが必須です。
- 画面操作録画の再生には対応していません。
- ログデータWeb閲覧機能は、Internet Explorer 6 / 7 / 8 / 9 / 10 / 11(Windows ストアアプリ版を含む)に対応しています。
- ログのWeb閲覧に関する操作ログを取得するには、Webシステムサーバーに端末機プログラムをインストールする必要があります。

画面録画再生について

- ゲームやビデオ再生画面など、ウィンドウ内が録画されない(黒くなり表示されない)場合があります。
- クライアントOSでの常時録画は、単一のユーザーでログオンしている場合のみお使いいただけます。
- 「個別画面操作録画」のライセンスはSKYSEA Client View Ver.10.2以降で有効なライセンスです。Ver.10.2より前の端末機で画面操作録画を行うには、通常の画面操作録画ライセンスが必要です。
- マルチディスプレイ環境でディスプレイ毎に異なるスケーリングが設定されていると、画面が見切れて録画される場合があります。

高速ログ検索について

- 弊社製品「SKYSEA Client View High Speed Log Search」の販売は終了いたしました。すでに販売いたしました本製品に関するサポート、ならびに保守契約の更新につきましては、従来どおり対応いたします。また、今後ログの高速検索をご希望のお客様につきましては、株式会社インテック様の統合ログ管理ソフトウェア「LogRevi(ログレビ)」をご検討いただきますようお願いいたします。
  <LogRevi(ログレビ)に関するお問い合わせ>株式会社インテック ビジネスソリューション企画推進部　TEL：03-5665-5140　e-mail：itps_info@intec.co.jp

起動・終了ログについて

- すでに存在するセッションに対してリモート操作を行った場合、接続元IPアドレスおよび接続元コンピューター名は、接続PCのものではなく、セッション生成時のコンピューターのものが表示される場合があります。

セキュリティ管理について

- 「ファイル操作」注意表示について、ユーザーのオペレーションにより、これらの注意表示が発生し、メール送信または、端末機のポップアップ通知が行われた後、一定時間(2分)内に発生した同一種別の注意表示に対する、メール送信および、端末機の画面にメッセージを表示(ポップアップ通知)は行われません。
- FTPアップロード・ダウンロードを禁止できるのは、以下が条件となります。
  - ○ 利用クライアントが、FFFTP 1.96 / 1.97 / 1.98 / 1.99 / 2.0 / 3.0 / 3.1 / 3.2 / 3.3 / 3.4 / 3.5 / 3.6 / 3.7 / 3.8 / 3.9 / 4.0 / 4.1 / 4.2 / 4.3 / 4.4 / 4.5 / 4.6 / 4.7、NextFTP 4、Internet Explorer 5.5 SP2 / 6 / 7 / 8 / 9 / 10 / 11であること。
- 通信デバイス使用制限機能は、Windowsのデバイスマネージャー上に表示されている通信デバイスが対象になります。
- 指定した無線アクセスポイントのみ通信を許可する機能はWindows XP SP2以前のOSではお使いいただけません。
- 次のGUIDのデバイスをBluetoothデバイスと判定します。
  - ○ Broadcom「95c7a0a0-3094-11d7-a202-00508b9d7d5a」
  - ○ Cambridge Silicon Radio Limited「473a6b1d-3407-400e-b91a-f991c5a39dc3」
  - ○ IVT Corporation「9b21fd3a-b1ab-4eb9-956fe56acfe78bce」
  - ○ Microsoft標準「e0cbf06c-cd8b-4647-bb8a-263b43f0f974」
  - ○ Motorola Solutions「a173b237-6a34-4bb5-aa63-2561160fa200」
  - ○ Toshiba「7240100f-6512-4548-8418-9ebb5c6a1a94」
- Bluetooth LE(Bluetooth Low Energy)デバイスには対応していません。
- 業務外アプリケーション実行アラートは、Windows 8 / Windows 8.1 / Windows 10 / Windows Server 2012 / Windows Server 2012 R2の端末機では検知されません。
- 印刷物取り忘れアラートは、Windows ストアアプリからの印刷に対応していません。
- OneDriveアプリ(デスクトップアプリ)を利用する端末機に対して、OneDriveの利用アラートを有効にするには、設定適用後に端末機をログオンし直す必要があります。
- OneDrive、OneDrive for Businessの利用を禁止しても、禁止前にローカルフォルダに同期したファイルは削除されません。また、同期されたファイルへのアクセスも禁止されず、アラートも検知されません。
- Windows 10のExcel Mobile、PowerPoint Mobile、Word Mobileは、OneDriveの利用またはOneDrive for Businessの利用を禁止している場合には起動自体が禁止されます。また、ユーザーが起動していない場合でも、バックグラウンドで起動されることがあり、この場合もアラート検知されます。
- OneDrive、OneDrive for Businessのブラウザの利用禁止については、今後Microsoft社のサイト構成変更によっては利用を検知できなくなったり、両者を区別して検知できなくなる可能性があります。
- Webアップロード / ダウンロードを禁止に設定している場合でも、OneDrive同期時のMicrosoft 365のWebアップロード、ダウンロードは禁止できません。
- アプリケーション実行中の特定操作アラートで、指定アプリケーション起動時に印刷をアラート対象としており、かつ指定のプリンターへの印刷を除外している場合、指定アプリケーションが実行されている間は、指定アプリケーション以外からの印刷も指定プリンターに限定されます。
- 複数のPCから同時に印刷を行った場合、印刷禁止アラートまたはアプリケーション実行中の特定操作アラートによる印刷の禁止が行われない場合があります。
- プリンターサーバー経由での印刷を印刷禁止アラートまたはアプリケーション実行中の特定操作アラートで検知する場合は、プリンターサーバーにSKYSEA Client Viewの端末機プログラムをインストールし、アラート設定もプリンターサーバーに対して行う必要があります。また、アラート対象の端末機とプリンターサーバーとが双方向に通信ができる必要があります。
- 印刷ファイルパスアラートでは、Microsoft PowerPointからの印刷は禁止できません。
- Windows ストアアプリは印刷ファイルパスアラートに対応していません。
- 印刷禁止アラートで印刷を禁止するには、アラート検知するコンピューター上で「Print Spooler」サービスが実行されている必要があります。また、Windows 2000の端末機の場合、特定のアプリケーションでの印刷をアラート対象から除外する設定に対応していません。
- ログ収集設定によっては、Microsoft Edge(EdgeHTML版)によるMicrosoft Print to PDFなどの印刷操作を、印刷禁止アラートで禁止することができません。
- Internet Explorerのバージョンや状態、ダウンロードの方法によっては、Webダウンロード禁止の除外設定が正しく動作しない場合があります。
- 許可フォルダへのファイル操作禁止を行うドライバーを実行する場合や、想定外共有フォルダアクセスアラートを使用する場合、特定フォルダアクセスアラートの禁止とアクセス許可設定を使用する場合、圧縮ファイル生成アラートを使用する場合には、Windows 2000 / Windows XP / Windows Server 2003では以下のサービスパック、アップデートプログラムの適用が必要です。適用されていない場合は、アラート検知および禁止が動作しません。
  - ○ Windows 2000 SP4 + Update Rollup 1
  - ○ Windows XP SP2以降
  - ○ Windows Server 2003 SP1以降
- 圧縮ファイル生成アラートは、圧縮に使用したソフトウェアや指定した圧縮形式によっては、操作ログの取得やアラート検知ができない場合があります。
- 想定外共有フォルダアクセスアラートで、アラート判定に利用する「ファイルの読み込みバイト数」「ファイルへの書き込みバイト数」は、実際のファイルサイズは異なることがあります。
- アプリケーション実行アラートで、アプリケーションの起動そのものを禁止するドライバーには、以下のOS、サービスパックが必要です。これら以外のOSでは、ドライバーを使用する設定になっていてもアプリケーション起動の即時禁止は行われず、アプリケーションが起動してからプロセスが強制終了する禁止処理が行われます。
  - ○ Windows Vista SP1以降
  - ○ Windows Server 2008 以降
- アプリケーション実行アラート、特定フォルダアクセスアラート、想定外共有フォルダアクセスアラートなどでのアプリケーションのホワイトリスト設定で、ドライバーによる許可フォルダへのファイル操作禁止を行う場合、アラート対象となるのはコマンドプロンプトによるファイル操作のうち、エクスプローラとコマンドラインの内部コマンドのみとなります。
- レジストリ操作アラートは、Windows 2000の端末機では検知されません。
- アラート発生時のメール通知機能設定で対応しているSMTP認証方式は、「LOGIN」または「CRAM-MD5」です。
- 一度ユーザーアラート設定が適用されたユーザーでも、ログオンしたコンピューターをオフラインで使用するなど、30日を超えてマスターサーバーと通信できない状態が続くと、そのユーザーに対するユーザーアラート設定が解除されます。
- 任意定義アラートをユーザーアラートとして設定した場合、意図したとおりに検知されない場合があります。
- SKYSEA 未対応OSバージョンアラートは、Windows 10にのみ対応しています。
- 組織外ネットワーク接続(VPN・プロキシサーバー)アラートで検知対象となるブラウザは、Internet Explorer、Microsoft Edge(Chromium版 / EdgeHTML版)、Google Chrome、Mozilla Firefoxです。また、本機能はWindows Vista以降のクライアントOSでのみご利用可能です。
- 通信カード(モデム) / Wi-Fi接続 / テザリングによる大型アップデート制御設定アラートは、Windows 10の従量制課金接続設定を利用して、機能更新プログラムを含むすべての更新プログラムのダウンロードを制限します。有効にした場合、OneDrive / Microsoft Office Outlookの同期が行われなくなる場合があります。

不許可端末検知 / 遮断について

- 不許可端末の遮断を行うには、許可端末にSKYSEA Client Viewをインストールするか、許可端末リストに正しく登録する必要があります(ネットワークプリンターなどを含む)。
- 認証VLANや検疫ネットワークなど、通常のIPネットワークではない環境においては、不許可端末遮断機能を使用できない場合があります。
- 不許可端末検知 / 遮断機能については、必要なときのみ該当機能を有効・無効、ON / OFFすることはできません。お使いになる際には、本機能を常時有効、ONにしていただけますようにお願いいたします。ネットワーク上に、すでに不許可になる端末が存在している場合において、不許可端末検知・遮断機能を設置して有効にしてから、動作を開始するまでの時間は環境により変化します。
- SKYSEA Client Viewの管理機・端末機をインストールしたクライアントPC(Windows XP / Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10)では、ネットワークカードのチーミング設定を行わないでください。

セキュリティ管理について

不許可端末検知 / 遮断について	● ルーター等により、パケットの内容を変更するような動作が行われる環境、およびパケットを検疫するような環境では遮断機能がご利用いただけないことがあります。 ● ネットワーク上の機器から頻繁にARPリクエストが送信される環境では、遮断機能が効果的に動作しない可能性があります。 ● 無線LAN接続の端末機では遮断機能がご利用いただけません。また無線LAN接続の端末機で遮断機能を有効にした場合、無線アクセスポイントが高負荷になる可能性があります。 ● 不許可端末検知 / 遮断をご利用の環境では、バージョン混在でお使いにならないようお願いいたします。不許可端末検知 / 遮断の動作に問題が生じることがあります。必ずサーバーおよび全クライアントPCをアップデートし、同一バージョンに合わせていただきますようお願いいたします。 ● 不許可対象となる端末が多数ある状態で、不許可端末検知 / 遮断を有効にすると、ネットワークが不安定になる可能性があります。	
	端末機による検知 / 遮断について	● 不許可端末を検知するには、そのセグメントにSKYSEA Client Viewをインストールしたクライアントが起動している必要があります。 ● サーバーOSでのご利用の場合は、別途お問い合わせください。
メール送信宛先フィルタリングについて	● メール送信宛先フィルタリングに対応したメールクライアントは、Microsoft Outlook 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365です。 ● 本機能では専用のアドインを使用します。アドインに関する制限事項は「Microsoft Office製品用のアドイン（Officeアドイン）について（P.72）」をご覧ください。 ● Active Directory環境が必要です。	
WSUS連携について	● WSUS連携で対応しているWSUSのバージョンは下記のバージョンです。 ○ WSUS 3.0 SP2 ○ Windows Server 2012 WSUS ○ Windows Server 2012 R2 WSUS ○ Windows Server 2016 WSUS ○ Windows Server 2019 WSUS ● Windows XPモードや仮想環境上の端末機、Windows 8 / Windows 8.1で高速シャットダウンした（ハイブリッドブートが有効な）端末機については、電源オプションを設定しても、実行時に電源をONにできません。 ● マスターサーバーおよび、サーバーOS上の端末機は、更新完了後に電源をOFFにできません。 ● WSUSサーバーへの接続にHTTPプロキシを利用する環境では、WinHTTP proxyの設定が適切に構成されている必要があります。 ● ユーザーによる操作が必要な更新プログラムの適用はできません。 ● 配布時にマスターサーバーとは異なるセグメントの端末機の電源をONするには、各セグメントに少なくとも1台のソフトウェア配布用中継端末があり、マスターサーバーと通信できる必要があります。中継端末とマスターサーバーがインターネット経由（HTTP（S））で接続する場合は電源をONにできません。	
更新プログラム配布管理について	● 端末機上で個別に更新プログラムを配布・適用するツールは、クライアントPCドライブ保護が有効な環境では実行できません。	
Windows 10更新制御について	● 対応OSは、Windows 10 Pro（バージョン1703以上）のみとなります。	
CPE製品名管理について	● 本機能をご利用いただくには、インターネットへのアクセスが可能な、Windows 7 / Windows Server 2008 R2以降の管理機が必要です。	
Microsoft Office更新制御について	● 管理対象のMicrosoft 365 / Office 2019のバージョンによっては、適用状況の一覧画面において、製品名や更新チャネルなどの情報が正しく取得できない場合があります。	
SKYSEA Client View アラートsyslog出力について	● 本機能を利用される場合は、データサーバー1台あたりのクライアント管理台数が3,000台までとなります。	
紛失端末制御について	● 紛失端末制御用Webサイトを経由して端末機の制御を行う場合は、制御対象の端末機がインターネットに接続できる必要があります。 ● マザーボードのUUIDが、起動するたびに変更される端末機の場合、本機能は利用できません。 ● 本機能を有効化した端末機の位置情報は、SKYSEA Client View以外のあらゆるデスクトップアプリから取得可能になります。	

デバイス管理について

● デバイスマネージャー上で「SCSI、RAIDコントローラ、ATA、SATA（Serial ATA）」と認識している機器は、「内蔵デバイス」の扱いとなります。ただし、CD/DVDドライブは、すべて「外付けデバイス」の扱いとなります。また、バスタイプがATAまたはSATAの、ホットプラグ対応ハードディスク（OSの認識として）は「eSATA接続ハードディスク」として「外付けデバイス」の扱いとなります。
● 「eSATA接続ハードディスク」としてデバイス管理機能をご利用いただけるのは、バスタイプがATAまたはSATAの、ホットプラグ対応ハードディスクに限ります（OSの認識として）。
● 記憶媒体 / メディア使用禁止機能は、特殊な方法で記憶媒体を制御しているシステムをお使いの場合には、禁止にできないときがあります。
● セキュリティグループごとのデバイス使用制限を設定する場合に、「Builtinコンテナ」内のセキュリティグループを指定すると、Mac端末で正しく動作しないことがあります。
● CD / DVD / ブルーレイライティングソフトウェアの中には、特殊な書き込み処理を行っているものがあります。そのため、ドライブへの書き込み禁止設定がされている場合、特殊な書き込み処理をするソフトウェアの一部製品に対しては、実行ファイルの起動を禁止することでデータ書き込みを制限しています。起動を禁止しているライティングソフトウェアは、以下の製品です。B's Recorder GOLD 7
　○ BlindWrite 5
　○ Clone CD 5.3.0.1
　○ Clone DVD 2.9.0.9
　○ CopyToDVD 3.1.3.137
　○ Easy Media Creator 9 / 10
　○ Inter Video DVD Copy 5 Platinum / Gold
　※起動を禁止している実行ファイルについては弊社までお問い合わせください。
● Windows Server 2003 SP1 / SP2、Windows Server 2003 R2 / SP2 では、記憶媒体使用禁止機能を解除しても、OSの再起動を行わないと解除されない場合があります。
● ネットワークドライブの使用制限に対応するOSは、Windows 7以降およびWindows Server 2008 R2以降です。
● シリアルナンバー等の機器情報が認識できないデバイスの管理には、以下の制限があります。
　○ デバイス名が同じ場合、個体識別ができないため、デバイス管理台帳では、1つのデバイスとして登録されます。　○ 棚卸等、一部の機能をご利用いただけません。
　※安心してお使いいただけるUSBメモリの推奨メーカー様の一覧は、動作環境（P.71）をご覧ください。
● 大量にファイルを保存したデバイスでは、「USBデバイスファイル確認」機能をご利用いただけない場合があります。
● デバイスに大量のファイルをコピーしてすぐ削除を行った場合、ファイルコピーログとファイル削除ログが出力されますが、ファイルコピーログに対してアラートが発生しない場合があります。
● Thunderboltで接続するデバイスの管理は、Mac端末に接続された場合のみ行えます（Windows OSは対象外です）。
● 「USBでもeSATAでも接続可能」「USBでもFireWire / Thunderboltでも接続可能」というように、1つのデバイスで複数のインタフェースに対応する場合は、それぞれのインタフェースによって別々のデバイスとして登録されます。
● スマートフォンやタブレット端末のように、PCとの接続モードによってプロダクトID（PID）が変化するデバイスは、プロダクトIDごとにデバイス情報が登録されます。
● Windows XP以前のクライアントOS、Windows Server 2008以前のサーバーOSでは、Windowsポータブルデバイス（MTP / PTP接続のデバイス）など、OS上でドライブレターが割り当てられない（ボリュームとしてマウントされない）デバイスについては、「記憶媒体 / メディア書き込み」アラートによる書き込み禁止設定がされている場合、使用禁止設定として動作します。ただし、WIA（Windows Imaging Acquisition）として認識した場合は、OSによって書き込みが制限されるため、SKYSEA Client Viewでは前述の制御を行いません。また、これらのデバイスに対するファイル操作ログも取得できません。
● Windows Vistaでも、次の条件を満たしていない場合は、上記の制限事項が適用されます。
　○ Service Pack 2と「KB2761494」に加え、「KB971514」または「KB971644」のWindows更新プログラムがインストールされていること。
● 「iTunes」や「ドコモケータイdatalink」などを利用して、アプリケーション経由でスマートフォン / フィーチャーフォンとデータをやりとりするような環境では、そのアプリケーションの実行を禁止してください。デバイスの使用制限（使用禁止 / 書き込み禁止）が正しく動作しない可能性があります。
● 端末機に接続中のWindowsポータブルデバイスに対して、「記憶媒体 / メディア書き込み」アラートによる書き込み禁止設定を有効にするには、設定適用後にデバイスを接続し直す必要があります。
● 使用禁止処理が行われたWindowsポータブルデバイスを再度使用可能にするには、使用可能設定に変更するだけでなく、クライアントPCを再起動する必要があります。
● iPhone / iPad / iPod touchなどのiOS搭載デバイスは、iTunesをインストールしていることにより、1つのデバイスに対して2つのデバイス情報が登録されます。またこれらのデバイスにエクスプローラからデータを書き込むことはできませんが、iTunesからは音楽・画像ファイルの書き込みができるため、iTunesの実行を禁止するなどの対策が必要です。
● メディア管理で対応している光ディスクは、DVD-RAMです。
● 申請・承認ワークフローシステムをご利用の場合、インストール・設定前に、Active Directoryのセットアップが必要です。
● 申請・承認ワークフローについては、有効期間外のデバイス使用設定は未対応です。
● 申請・承認ワークフローシステムのファイル持ち出し申請で許可されたファイルの書き出しを行う場合、次の制限があります。
　○ 光学メディアへの書き出しを行う場合は、OS標準のパケットライト方式でフォーマットされているメディアでのみ行えます。また、Windows Vista以降のOSのみ対応しています。
　※Windows Vista / Windows Vista SP1ではさらに、Windows Feature Pack for Storage 1.0 が適用されている必要があります。
　○ 光学ドライブが複数存在する環境では、光学ドライブへの書き出しは行えません。
　○ 持ち出せるファイルサイズの上限は4,352MBですが、暗号化して書き出す場合やファイルシステムの仕様によっては、4,352MBを下回ることがあります。
　○ Windowsポータブルデバイス（MTP / PTP接続のデバイス）への書き出しは非対応です。
　○ ファイル名に「Shift_JIS」以外の文字が含まれるファイルは非対応です。
● 申請・承認ワークフローシステムでJRE 7をインストールしている環境の場合、SSLを用いたメール送信でサポートするプロトコルはTLSv1.0のみで、TLSv1.1 / 1.2はサポートしていません。

デバイス管理について

接続時のウイルスチェックについて	● ウイルス対策ソフトウェアの対応状況については、Webサイトの技術資料をご覧ください。 ● 本機能を使ってUSBデバイスおよびメディアをウイルススキャン中に、別のUSBデバイスおよびメディアを接続した場合、ウイルス対策ソフトウェアによっては、後から接続したUSBデバイスおよびメディアのウイルスチェックが起動しない場合があります。 ● Windows 2000ではご利用いただけません。 ● USBデバイスおよびメディアの接続時にドライブが追加されない場合は、スキャンできません。 ● ウイルス対策ソフトウェアで、すでにUSBデバイスおよびメディア接続時にウイルスチェックが行われるよう設定されている場合は、本機能が動作しないことがあります。	
外付けデバイス&ファイル暗号化について	外付けデバイスの暗号化について	● 対応OSは、Windows 7以降、およびWindows Server 2008 R2以降です。　● 暗号化に対応しているファイルシステムは、FAT32、NTFS、exFATです。 ● マルチカードリーダーなど、複数のドライブを認識できるデバイスを介した暗号化には対応していません。 ● スタンドアロン端末では、デバイス暗号化ツールはインストールできません。また、スタンドアロン端末上で暗号化されたデバイスを使用しても、デバイス暗号化情報の「最終使用日時」、および「最終使用端末ID」は更新されません。 ● ほかの暗号化機能を利用されている場合は、本機能が利用できない場合があります。 ● パスワードロック機能を搭載しているUSBデバイスは、本機能のサポート対象外です。 ● メディアとして台帳登録されているデバイスは、本機能で暗号化できません。また、本機能で暗号化されているデバイスは、メディアとして台帳登録できません。
	Webアップロードファイルの強制暗号化について	● 対応OSは、Windows 7以降、およびWindows Server 2008 R2以降です。また対応ブラウザは、Internet Explorer 11（ただし、Windows 8.1のストアアプリ版は非対応）、Mozilla Firefox 64以降（延長サポート版はMozilla Firefox 60以降）、Google Chrome 71以降です。Microsoft Edge（EdgeHTML版）には対応していません。また、これら対応ブラウザ以外の非対応のブラウザにおいては、Webアップロードが禁止されます。 ● 自動暗号化フォルダでファイル暗号化を行った際、ファイル操作ログが正しく収集されない場合があります。 ● 自動暗号化フォルダ内のファイルのみWebアップロードを許可するように設定しているとき、ブラウザの画面上にフォルダ外のファイルがドラッグ&ドロップされた場合は、アップロードの目的外であってもアラートとして検知されます。 ● 自動暗号化フォルダ内のファイルのみWebアップロードを許可するように設定していても、Google ChromeやMozilla FirefoxではWebアップロードが禁止されることがあります。
	メール添付ファイルの自動暗号化について	● 端末機（Windows）とスタンドアロン端末機に対応しています。端末機（Mac）と端末機（Linux）には対応していません。また、対応するメールクライアントは、Microsoft Outlook 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365です。 ● 「Officeアドイン設定」で「Ver.9.0以降のアドイン」を選択し、かつ「ログ収集時に電子証明書を使用する」にチェックを入れている場合、以下の環境では本機能は対応していません。 　○ Windows 7 / Windows Server 2008 R2（SP未適用）以前のOS　○ Microsoft Office 2010 SP1以前のMicrosoft Office ● メールへファイルを添付してから一定時間（60分）経過した後に送信するなど、操作の内容によっては添付ファイルのファイルパスが正しくログ取得できないことがあります。 ● 本機能では専用のアドインを使用します。アドインに関する制限事項は「Microsoft Office製品用のアドイン（Officeアドイン）について（P.72）」をご覧ください。

レポートについて

● 「ユーザー操作時間レポート」において、Web会議を行った時間を集計できる対象システムは以下の通りです。
　○ Cisco Webex　○ Microsoft Teams　○ Zoom
● レポートで印刷表示を行う場合は、Adobe Reader 9 / 10 / 11が必要です。
● レポートを閲覧する端末機、管理機およびログ解析サーバー / レポート用サーバーには、JIS2004対応フォント（KB927489）の適用が必要です（Windows Vista以降、Windows Server 2008以降のOSには、標準搭載されています）。JIS2004対応フォントについては、Microsoft社のサポートページをご確認ください。
● 解析結果の表示には、Microsoft Excel 2000 / 2002 / 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 365が必要です。中でも、「資産・ログ利活用レポートライブラリ」の解析結果の表示には、Microsoft Excel 2007 / 2010 / 2013 / 2016 / 2019が必要です。
● Windows ストアアプリのInternet Explorerは、ログ解析レポートに対応していません。

ログ解析用サーバー / レポート用サーバーについて	● ログ解析レポート / Web利用状況レポート / ユーザー作業状況レポートをご利用の場合、データサーバーが必要です。 ● ログ解析機能をHTTPS通信で利用する場合、対応するログ解析用サーバーのOSはWindows Server 2008R2以降となります。

メンテナンスについて

● キーボード・マウス操作が同時に行えるのは、最大50台までです。
● Windows XPならびにWindows Server 2003以前のOSの場合、リモートデスクトップ接続と併用すると、リモート操作の接続に失敗する場合があります。
● リモート操作中のファイル転送は、Windows 8 / Windows 8.1のスタート画面やWindows ストアアプリの画面に対しては行えません。
● アプリケーション実行中の特定操作アラートで、リモート操作時に特定アプリケーションの画面をマスクして表示させないように設定している場合でも、Windows 10のタスクビュー下部に表示されるデスクトッププレビュー内のウィンドウはマスクされません。
● マルチディスプレイで使用しているMac端末のリモート操作（画面提示）を行う場合、リモート操作カーテンを実行した状態でディスプレイを切り替えると、デスクトップの内容が一瞬表示されます。
● Windows XP以前、またはAeroが無効に設定されているWindows 7 / Windows Vistaのリモート操作（画面提示）を行う場合、リモート操作カーテンの実行中はレイヤードウィンドウが表示されなくなります。
● タッチ操作が可能な端末に対してリモート操作を行う場合、端末機側でもタッチ操作が可能な場合があります。
● タッチパッド搭載の端末に対してリモート操作を行う場合、機種によってはタッチパッド操作が可能な場合があります。
● 電源制御機能によるMicrosoftアカウントでのリモートログオンは行えません。　● マクロ機能、実行機能によるWindows ストアアプリの実行はできません。
● 電源制御 / 定期電源ON機能は、Windows 8以降の高速スタートアップ（ハイブリッドブート）には対応していません。高速スタートアップが有効な状態で、手動でシャットダウンを行った場合は、リモート電源ONができません。
● 電源制御 / 定期電源ON機能では、スリープ状態の端末機を復帰させることはできません。
● SKYSEA Client View端末機（Mac）上で、FileVaultを有効にすると、ユーザーがログインするまでは、「リモート操作」や「電源状態の取得」が動作しません。

クライアントPC 環境保護について	● 本機能は、Windows 8.1以降のOS（サーバーOSを除く）でのみご利用可能です。　● アプリケーションごとの設定は、ユーザープロファイルに依存する設定のみ修復できます。 ● 同居するアプリケーションによっては、プロファイルの修復に失敗する場合があります。 ● 本機能は、ローカルグループポリシーを利用しています。ドメインポリシーなど優先されるポリシーが適用されている場合は、保護設定が適用されない場合があります。 ● スタンドアロン端末機に対しては保護を行うことはできません。 ● 本機能の一部設定は、移動ユーザープロファイル機構を利用して実現しています。Windows ストアアプリなどの、移動ユーザープロファイルに対応していないアプリケーションはご利用いただけません。また、移動ユーザープロファイルを利用しているアカウントに対する「インストール / アンインストール」に対応していないアプリケーションを「ソフトウェア配布」機能で配布する場合は、環境保護設定を解除してください。 ● 本機能は、管理機とクライアントPC間で双方向の通信が確立されている必要があります。NAT環境や、HTTPゲートウェイを利用している環境も該当します。 ● 他ソフトウェアの環境復元機能を有効にしている場合は、本機能で保護設定を行っても、端末の再起動時に保護設定前の状態に戻ります。 ● Microsoftアカウントでのログオンや、OneDriveには対応していません。OneDriveで同期するファイルがある場合、プロファイルの保護が失敗します。
クライアントPC ドライブ保護について	● 本機能を使用する場合は、次の点にご注意ください。 　○ ドライブ保護に必要な容量は64GB以上です。 　○ 端末イメージの保存場所となるドライブは、NTFSでフォーマットされている必要があります。 　○ 導入時、初期化処理には1時間程度かかる場合があります。 　○ 初期化処理を行うと、ドライブの総容量や、利用可能な空き容量が減少します。 　○ 保護対象となるドライブはシステムドライブのみです。 　○ 休止（Hibernation）には対応していません。 　○ 保護対象外に指定できるファイルは最大で30個です。フォルダには、制限はありません。 ● 本機能は、Windows 8.1以降のOSでのみご利用可能です。 ● 本機能は、管理機とクライアントPC間で双方向の通信が確立されている必要があります。NAT環境や、HTTPゲートウェイを利用している環境も該当します。 ● 初期化した場合、Windowsの「システムの復元」機能で作成された復元ポイントはすべて削除されます。また、初期化後は「システムの復元」機能は使用できません。 ● トレンドマイクロ社製ウイルスバスターと同居している場合は、不正変更防止サービスを無効にしてください。

メンテナンスについて

ディスクメンテナンスについて	● 本機能は、物理ディスク（ハードディスク / SSD）を複数台搭載しているコンピューターのバックアップ / リストアには対応していません。 ● Sysprepを実行する場合は、事前にバックアップを行うことを推奨します。 ● NTFSの次の機能が利用されているボリュームのバックアップ / リストアはサポート対象外です。 〇 拡張属性　〇 シンボリックリンクでもジャンクションでもない解析ポイント 〇 オブジェクトID ● 「Windowsシステムリストア用起動USBデバイス作成ツール」の起動には、Windows ADK 8.1が必要です。 ● バックアップしたデータを別の端末にリストアする場合、リストア先のディスクサイズは、バックアップ元と同じか、それ以上の容量が必要です。 ● ネットワーク設定できるIPアドレスは、IPv4形式のみです。 ● 本機能は、次の環境ではご使用になれません。 〇 Windows To Goで起動している状態　〇 デュアルブート環境 ● マルチログオンされている状態では、バックアップ / リストアできません。 ● 無線LANアダプタしか搭載されていない機種（タブレット端末など）にリストアする場合、MACアドレスを指定して、コンピューター名、IPアドレスの自動設定はできません。 ● タブレット端末でバックアップ / リストア時に、タッチパネルでの操作ができない場合は、キーボードやマウスをご用意ください。

ソフトウェア資産管理（SAM）について

● Microsoft Office 2000 / 2010 / 2013 / 2016 / 2019の場合は、Microsoft Office製品がプリインストール版か判定する情報が取得できません。
● Microsoft Office 2000の場合は、リリース種別（製品版、ダウンロード版など）の情報が取得できません。
● Windows 2000 / XPは、SQL ServerのCPUコア数の取得をサポートしていません。
● Windows Server 2003でSQL ServerのCPUコア数を取得する場合は、「KB932370」がインストールされている必要があります。
● SQL Server 2000以前のエディション情報は取得できません。
● Windows ストアアプリは、ソフトウェア資産管理（SAM）機能の管理対象外です。
● Windows ストアアプリのInternet Explorerでは、申請・承認ワークフローシステムをお使いいただけません。
● 申請・承認ワークフローシステムをご利用の場合、インストール・設定前に、Active Directoryのセットアップが必要です。
● 申請・承認ワークフローシステムでJRE 7をインストールしている環境の場合、SSLを用いたメール送信でサポートするプロトコルはTLSv1.0のみで、TLSv1.1 / 1.2はサポートしていません。

リモートインストールツールについて

● リモートインストールツールをご利用の場合は、事前設定が必要となります。
● ツールを実行する管理機としては、Windows 2000ではご利用いただけません（データの配布先クライアントPCとしてはご利用いただけます）。

インターネット経由での資産情報・ログ収集機能について

● 管理コンソールからインターネットの向こう側にある端末機に対しては、次の機能がご利用になれません（ただし、リモート操作については「リモート操作（インターネット経由）」オプションを追加することでご利用いただけます）。
〇 電源状態の取得　〇 キーボード・マウス転送　〇 実行
〇 データ取得　〇 電源制御　〇 マクロ
〇 リモート操作　〇 資料配布　〇 ソフトウェア配布の配布 / 実行状況出力
● 管理コンソールからインターネットの向こう側にある端末機へは設定が即座に反映されません。コンピューターの起動時など、端末機から設定を取得するタイミングに反映されます。
● マスターサーバーから直接実行する次の機能も、インターネットの向こう側にある端末機に対してはご利用になれません。
〇 ネットワーク機器の死活監視　〇 MIB情報更新
● HTTP（S）経由でソフトウェア配布の中継機能をご利用になる場合は、ソフトウェア配布中継端末プログラムに加え、端末機プログラムもインストールする必要があります。
● インターネット経由の資産情報・ログ収集が有効の管理機・端末機では次の機能がご利用になれません。
〇 不許可端末検知 / 遮断　〇 残業管理（前日までの作業時間一覧）
〇 アラート項目「インストール必須アプリケーション」「残業時間お知らせメッセージ」による検疫　〇 資産レポート
〇 Web利用状況　〇 ソフトウェア配布のマルチキャスト配布（マルチキャスト配布用端末として自動選択されません）
● Webブラウザを使用する機能はHTTP（S）経由での使用をサポートしていません。
〇 ログ解析レポート
● 監査対象サーバーからデータサーバーへのデータアップロードはHTTP（S）経由では行えません。
● HTTPゲートウェイサーバーから接続するマスターサーバー、データサーバーは、HTTPゲートウェイサーバーからコンピューター名でアクセスできる必要があります。従って、IPアドレスを指定してマスターサーバー、データサーバーを構築した環境ではご利用いただけません。
● HTTPゲートウェイサーバーまでの通信経路で、HTTPリクエスト数で制限するファイアウォール機能を持つセキュリティ製品を利用される場合には、ご利用環境に応じて設定が必要になります。

Mac端末運用管理について

※ここでは、Mac端末運用管理の各種制限事項について説明しています。Mac端末の対応機能については、機能一覧（P.57～64）の「対応OS-Mac」の列をご覧ください。
● OSのバージョンによっては、SKYSEA Client Viewの部署別インストーラーに同梱しているJavaが対応していないことがあります。その場合、対応するバージョンへOSをアップグレードするか、OSのバージョンに合わせて同梱しているJavaを差し替える必要があります。
● 電源状態の取得、部署別インストーラー作成、デバイス管理、ログ管理、リモート操作をご利用いただけるOSのバージョンは、Mac OS X 10.5以降となります。ただし、macOS 10.14のMac端末からリモート操作権限を取得するには、端末のシステム環境設定で、SKYSEA Client Viewの「アクセシビリティ」を許可する必要があります。
● 端末機No.重複の検知をご利用いただけるOSのバージョンは、Mac OS X 10.6以降となります。
● Mac OS X 10.5 / 10.6では、SSLを用いたメール送信でサポートするプロトコルはTLSv1.0のみで、TLSv1.1 / TLSv1.2はサポートしていません。
● macOS 10.15のMac端末に対して、リモート操作、管理コンソールの項目「最前面ウィンドウキャプション」の表示、クライアント操作ログの収集を行う場合は、端末のシステム環境設定「セキュリティとプライバシー」で、SKYSEA Client Viewの「画面収録」を許可する必要があります。
● ファイアウォール設定を有効にする場合、SKYSEA Client Viewが外部からの接続を受け入れるのを許可する必要があります。

資産管理について		● Apple Siliconを搭載しているMac端末の場合、資産情報「CPUタイプ」が正しく取得されない場合があります。
	ウイルス対策ソフトウェアについて（Mac版）	● プログラムバージョン、検索エンジンバージョン、パターンファイルバージョンのみ収集できる製品は、以下の製品のみです。 〇 エフセキュア社製 F-Secure Client Security for Mac 12 / 13 / 14 / 15、F-Secure Elements EPP Computer Protection for Mac 17 〇 マカフィー社製 McAfee VirusScan for Mac 9.1 / 9.2 / 9.5 / 9.6 / 9.7 / 9.8 ● プログラムバージョンのみ収集できる製品は、以下の製品のみです。 〇 ESET社製 ESET Cyber Security V6.0 〇 カスペルスキー社製 カスペルスキー セキュリティ for Mac、カスペルスキー インターネット セキュリティ for Mac、Kaspersky Endpoint Security for Mac 8 / 10 / 11 〇 ヴイエムウェア株式会社 VMware Carbon Black 〇 トレンドマイクロ社製 ウイルスバスター for Mac プログラムバージョン 1.5 / 1.6 / 2.0 / 3.0 / 5.0 / 6.0 / 7.0 / 8.0 / 9.0 / 10 / 11.0、Trend Micro ビジネスセキュリティ 6.0、ウイルスバスター ビジネスセキュリティ 7.0 / 9.0 / 9.5 / 10、Trend Micro Apex One（オンプレミス版 / SaaS版） 〇 ノートンライフロック社製 ノートン アンチウイルス Mac版 11.1 / 12.0、ノートン アンチウイルス プラス、ノートン インターネットセキュリティ Mac版、ノートン セキュリティ、ノートン 360 〇 ブロードコム社製 Symantec Endpoint Protection 12.1 / 14 / 14.1 / 14.2 / 14.3 〇 McAfee Endpoint Protection for Mac 1.0 / 1.1 / 1.2 / 2.1 / 2.2 / 2.3、McAfee Endpoint Security 10 ※詳しい対応状況については、Webサイトの技術資料をご覧ください。

Mac端末運用管理について

資産管理について	Microsoft Officeについて（Mac版）	● Microsoft Office状況として、ソフトウェア情報が収集できるMac版のバージョンは、以下のバージョンのみです。 〇 対応オフィスソフトウェア Microsoft Office for Mac 2011 / 2016 / 2019（取得できる情報はインストール状況のみとなります）
	プリンターについて	● Mac端末では、CUPSと呼ばれる印刷システムより情報を取得します。そのため、CUPS以外の印刷システムが使用されている場合は、プリンター情報は収集できません。
申請・承認ワークフローシステムについて		● Mac端末でご利用の場合、対応ブラウザはSafari 5.1 / 6.0 / 6.1 / 6.2 / 7.0 / 7.1 / 8.0 / 9.0 / 10.0 / 11.0 / 12.0 / 13.0 / 14.0となります。
デバイス管理について		● Mac端末にMTP（メディア転送プロトコル） / PTP（画像転送プロトコル）で接続されたデバイスは、「記憶媒体 / メディア使用」アラートによる使用禁止、および「記憶媒体 / メディア書き込み」アラートによる書き込み禁止に対応していません。 ※MTP / PTPで接続されたデバイスはドライブとして認識されないため、データの書き込みはできませんが、デバイスによっては、「イメージキャプチャ」（Mac OS X標準アプリケーション）によって画像ファイルの読み取りができる場合があります。 ● Mac端末に接続されたiPhone / iPad / iPod touchなどのiOS搭載デバイスは、「記憶媒体 / メディア使用」アラートによる使用禁止、および「記憶媒体 / メディア書き込み」アラートによる書き込み禁止に対応していません。 ● Mac端末における「Android File Transfer」を利用したデータ送信の制限には対応していません。 ● CD / DVD / ブルーレイドライブへの記憶媒体書き込み制限はできません。またブランクディスクを挿入した場合は、記憶媒体使用制限もできません。 ● OS X El Capitan（10.11）以降のMacでデバイスを新規登録すると、WindowsやOS X Yosemite（10.10）以前のMacから登録したときと異なるデバイス名が登録されることがあります。 ● デバイスの使用禁止、書き込み禁止を設定していて、端末機にデバイスを接続したときに「使用可能」で登録する設定の場合でも、OS X El Capitan（10.11）以降のMacでデバイスを新規登録した場合のみ、使用禁止、または書き込み禁止の制御が行われます。
ログ管理について		● アプリケーションログの起動元プロセス情報、コマンドプロンプト実行ログは取得できません。 ● ファイルアクセスログ、不許可端末検知ログには対応していません。 ● ファイル操作ログの「ファイル上書き保存」には対応していません。 ● ファイル操作ログの「フォルダコピー」には対応していません（コピー操作が含まれるログの追跡も途切れます）。「ファイルコピー」のログ収集対象となる操作は、Finderとcpコマンドによる同一ファイル名でのコピー操作のみです。 ● ファイル操作ログおよびファイルアクセスログのファイルサイズ情報は、操作種別やタイミングによっては取得できない場合があります。 ● Webアクセスログの対応ブラウザは、Safari 5.1 / 6.0 / 6.1 / 6.2 / 7.0 / 7.1 / 8.0 / 9.0 / 10.0 / 11.0 / 12.0 / 13.0 / 14.0、Google Chromeです。Safari 6.2 / 7.1 / 8.0では、SKYSEA Client Viewの機能拡張（アドオン）をユーザーが有効にする必要があります。 ● Safariは、Web書き込みログ、Webアップロードログ、FTPアップロードログ、Gmail送信ログには対応していません。また、プロキシサーバーを利用する環境で、SafariによるWebアクセスログを収集するには、「プロキシ設定を使用しないホストとドメイン」の設定で「localhost」に対して通信可能な設定にする必要があります。 ● Google Chromeは、FTPアップロードログには対応していません。Google ChromeによるWebアクセスログ収集をご利用いただけるOSのバージョンは、Mac OS X 10.6以降です。また、Google Chromeの仕様が変更された場合、ログ収集機能の利用ができなくなる恐れがあります。 ● SMTP接続による送信メールで取得できるのは、利用クライアントがMail（Mac OS X標準）である場合となります。 ● 資産管理同様、CUPS以外の印刷システムが使用されている場合は、プリントログの印刷枚数およびデバイスURI情報は収集できません。 ● ログデータWeb閲覧機能でログ検索を行う場合、送信メールログの本文データは「Shift_JIS」で検索するため、「Shift_JIS」で表現できない文字は検索できません。 ● アラート発生通知メールの内容に、「Shift_JIS」で表現できない文字列が存在する場合は、「?」に変換されます。 ● macOS 10.14のMac端末から送信メールログを収集するには、端末のシステム環境設定で、SKYSEA Client Viewの「フルディスクアクセス」を許可した上で、メールプラグインを有効化する必要があります。 ● プリントログの印刷ファイルパス取得には対応していません。 ● Microsoft 365 / Office Onlineのログ取得には対応していません。
ログ解析について		● 資産・ログ利活用レポートライブラリのレポート集計処理を行う場合、Mac端末のUTF-8形式のログは「Shift_JIS」に変換して集計されるため、「Shift_JIS」で表現できない文字は「?」に変換されます。
インターネット経由での資産情報・ログ収集機能について		● Mac OS X 10.4には対応していません。 ● OS X 10.10をご利用の場合、一部の資産情報が正常に収集されないことがあります。

シンクライアント対応について

● 動作確認を行ったバージョンについては以下のとおりです。
〇 ヴイエムウェア株式会社製 VMware View 4.6 / 5.0 / 5.1 / 5.2 / 5.3
〇 ヴイエムウェア株式会社製 VMware Horizon 5.2 / 5.3 / 6.0 / 6.1 / 7.0 / 7.0.1 / 7.0.2 / 7.0.3 / 7.1.0 / 7.3.2 / 7.4 / 7.10 / 7.12 / 8.0
〇 システムインテリジェント株式会社製 Fogos PRO
〇 シトリックス・システムズ・ジャパン株式会社製 XenApp 5.0 / 6.0 / 6.5 / 7.6 / 7.8
〇 シトリックス・システムズ・ジャパン株式会社製 XenDesktop 5.0 / 5.5 / 7.0 / 7.6 / 7.8
〇 シトリックス・システムズ・ジャパン株式会社製 XenApp and XenDesktop 7.9 / 7.12 / 7.14 / 7.16
〇 シトリックス・システムズ・ジャパン株式会社製 Citrix Virtual Apps and Desktops 7 1909
〇 Sky株式会社製 SKYDIV Desktop Client 2.1
〇 日本電気株式会社製 VirtualPCCenter 2.1 / 4.0
〇 日本ヒューレット・パッカード株式会社製 CCI 4.0
〇 Microsoft社製 Windows Server 2008 Standard Edition Terminal Services
〇 Microsoft社製 Windows Server 2008 Standard x64 Edition Terminal Services
〇 Microsoft社製 Windows Server 2008 R2 Remote Desktop Services（Terminal Services）
〇 Microsoft社製 Windows Server 2012 Remote Desktop Service
〇 Microsoft社製 Windows Server 2012 R2 Remote Desktop Service
〇 Microsoft社製 Windows Server 2016 Remote Desktop Service
〇 Microsoft社製 Windows Server 2019 Remote Desktop Service
〇 株式会社ワッセイ・ソフトウェア・テクノロジー製 Phantosys 5LV
※SKYSEA Client View Ver.16シリーズにおいては、上記の各シンクライアント製品の動作確認バージョンおよび、それより新しいシンクライアント製品のバージョンをサポートいたします（ただし、各シンクライアント製品の修正プログラム、マイナーバージョンアップ、メジャーバージョンアップが行われた際には、事前の動作検証をお願いいたします）。
● ターミナルサービス、XenApp等の環境でご利用の場合、シンクライアントサーバーに1アクセスユーザーあたり約25MBのメモリをSKYSEA Client Viewにて利用します。
● シンクライアント環境（サーバーベース方式）で各種操作ログを収集する場合は、別途設定が必要です。
● VDI環境の仮想PCは、起動してから終了するまでの間、マスターサーバー・データサーバーと通信可能な状態であることが必要です。
● インスタントクローン環境など、利用するごとに仮想イメージが破棄される環境の場合、収集した仮想PC上の操作ログの一部がデータサーバーに保存されないことがあります。

仮想化について	● SKYSEA Client Viewでは仮想環境上での動作もサポートしております。Webサイトの技術資料をご覧の上、物理環境と同等の性能を有する環境をご用意ください（高速なストレージ装置やファイバーチャネルなどの高速なインタフェースを用いたり、ネットワークインタフェースを仮想マシンごとに割り当てるなど）。 ● 動作確認を行った仮想化環境は下記のとおりです。 〇 ヴイエムウェア株式会社製 VMware ESX/ESXi 3.5 / 4.0 / 5.0 / 5.1 / 5.5 / 6.0 / 6.5 / 7.0 〇 シトリックス・システムズ・ジャパン株式会社製 XenServer 5.6 SP2 / 6.2 / 7.0 / 7.2 〇 シトリックス・システムズ・ジャパン株式会社製 Citrix Hypervisor 8.0 〇 Microsoft社製 Windows Server 2012 Hyper-V 〇 Microsoft社製 Windows Server 2012 R2 Hyper-V 〇 Microsoft社製 Windows Server 2016 Hyper-V ※SKYSEA Client View Ver.16シリーズにおいては、上記の各仮想化環境製品の動作確認バージョンおよび、それより新しい仮想化環境製品のバージョンをサポートいたします（ただし、各仮想化環境製品の修正プログラム、マイナーバージョンアップ、メジャーバージョンアップが行われた際には、事前の動作検証をお願いいたします）。

在席確認・インスタントメッセージ機能について

- 端末機（Windows）のみ対応しています。ただし、スタンドアロン端末は非対応です。
- インターネット経由（HTTP(S)）ではご利用いただけません。
- サーバーから端末機に対する通信ができない場合は、ほかの端末機から送信されたインスタントメッセージが表示されるまでに時間がかかることがあります。

サーバー監査について

- サーバーOSで監査ログを出力するための設定が必要です。ご利用いただけるサーバーに関する詳細は、動作環境（P.69）をご覧ください。
- サーバー監査機能をご利用の場合、データサーバーが必要です。
- サーバー監査機能は、OSの監査ログからファイルアクセスログを出力しております。出力するために必要なグループポリシー、監査ログの設定が必要となります。また、出力されるログの内容は監査ログの内容に依存します。
- SQL Serverのデータベース監査ログを収集するには、SQL Serverに「共有メモリ」プロトコル、「SQL Server認証」でアクセスできる必要があります。
- Oracle Databaseのデータベース監査ログを収集するには、Oracle DatabaseとInstant Clientを使用してTCP / IP接続ができ、監査対象サーバーにOracle Database用のODBCドライバーがインストールされており、監査モードが「Unified Auditing」になっている必要があります。
- SKYSEA Client ViewからOracle Databaseへのログオンには、パスワード・ファイル認証を使用します。オペレーティング・システム認証は使用できません。

SKYSEA Client View for MDMのご利用について

共通事項	● モバイル端末の台数分にCAL（クライアントアクセスライセンス）が必要です。
iPhone / iPad対応について	● SKYSEA Client View for MDM（iPhone / iPad対応）を運用するには、データサーバーが必須となります。 ● 本機能では、Appleプッシュ通知サービス（APNS）を利用しており、モバイル端末機（iOS）およびモバイル情報収集サーバーからAPNSサーバーに対して、所定の通信ポートで通信可能なネットワーク環境が必要になります。詳しくは、Webサイトの技術資料をご覧ください。 ● Appleプッシュ通知サービスを利用する上で必要となる証明書には、1年の有効期限があります。有効期限が切れる前に必ず証明書を更新してください。証明書を更新しない場合、SKYSEA Client View for MDMの機能が使用できなくなります。 ● 資産情報の電話番号はSIMカードが挿入されている場合のみ収集できます。 ● 機能制限設定の「Appleへの診断データの送信を禁止する」機能は、iOS 5.1以上でのみお使いいただけます。 ● iPhone / iPad / iPod touchのMDMプロファイルを利用するほかのMDMツールとの共存はできません。 ● 一部の機能制限設定は、利用するためにApple Configuratorで「監視対象」に設定しておく必要があります。

SKYSEA Client View for MDMの管理コンソール・サーバー側について

共通事項	● SKYSEA Client ViewはUnicodeに対応していないため、管理コンソール上で、モバイル端末機の資産情報に「?」が表示される場合があります。 ● モバイル端末機は、資産レポートの対象外です。
iPhone / iPad対応について	● 「モバイル設定」の「無線LAN設定」で「SSID」を設定する場合に、「=」は使用できません。 ● アラート設定の「アクセスポイント接続設定」で、同名の「SSID」は設定できません。

「重要なお知らせ」機能について

- 本機能をご利用いただくには、Windows 7 / Windows Server 2008 R2以降の管理機が1台以上必要です。
- PCの時刻設定が1週間以上進んでいる管理機では、重要なお知らせがダウンロードできません。
- Ver.12.2より前の端末機については、セキュリティ更新プログラムの適用状況を収集できません。そのため、適用が完了しても対応状況は「未対応」のままになります。
- 脆弱性に対するSKYSEA Client View更新プログラムの自動適用は、SKYSEA Client Viewがインストールされており、かつマスターサーバーとの通信が可能な端末のみ対応しています。ただし、iOSなどのMDM端末は非対応です。

シリアル番号の登録について

- SKYSEA Client Viewのシリアル番号は「発行日の時点で公開されている最新のバージョン」に合わせて発行しています。
- 発行したシリアル番号を登録する際、ご使用のSKYSEA Client Viewのバージョンによっては、登録に失敗します。登録に失敗した場合は、ご使用いただいているバージョンに合わせたシリアル番号を発行いたしますので、弊社までお問い合わせください。また、最新バージョンにアップデートしていただくことでも、シリアル番号の登録が可能になります。
- バージョンアップや機能の改善に伴い、シリアル番号の仕様が変更になる場合があります。

海外での利用について

- SKYSEA Client Viewは、海外での販売、サポートには対応いたしません。

個人情報の適切な取り扱いについて

- SKYSEA Client Viewを使用して得られる情報の中に、個人情報の保護に関する法律等に規定する個人情報（以下、「個人情報」と言います）が含まれる場合があります。使用により取得する情報の中に個人情報が含まれる可能性に留意し、個人情報が含まれる場合は、個人情報の保護に関する法律等を遵守してご利用ください。

電子納品について

- ソフトウェア本体、マニュアル、ライセンス証書などは、専用のWebサイトからダウンロードいただく形となります。

医療機関向けオプション機能について

※医療機関向けオプションに搭載されている機能の制限事項の詳細については、SKYMEC IT ManagerのWebサイト（https://www.skymec.net/）の「制限事項」をご参照ください。

（お客様に安心してご利用いただくために）脆弱性対策への取り組みについて

脆弱性情報などの緊急案内を「重要なお知らせ」機能で通知

SKYSEA Client Viewは、本製品の脆弱性情報など弊社からの緊急案内を管理コンソール上で通知する「重要なお知らせ」機能を搭載しています。緊急時の更新プログラムの適用を速やかに行っていただくためにも、本機能のご利用を強く推奨します。

脆弱性などの重要情報をデスクトップ画面に表示

- 本機能は管理コンソールの起動時に弊社が公開しているWebサーバーにアクセスし、最新の重要なお知らせをダウンロードします。そのため、インターネットに接続できる管理機をご用意ください。
- 本製品では、適切なお知らせの実施とサービス向上のために、次の情報を収集・送信します。第三者がお客様の団体名や所属する個人を特定できるような情報の収集・送信および保存はいたしません。 ●「シリアル番号のハッシュ値」 ●「更新プログラムの未適用台数」

専用のWebページにて最新の脆弱性情報を公開

脆弱性情報の詳細や対策方法、また弊社における製品脆弱性情報の公開の流れについて、専用のWebページ「セキュリティ・脆弱性について」で公開しています。

https://www.skygroup.jp/security-info/

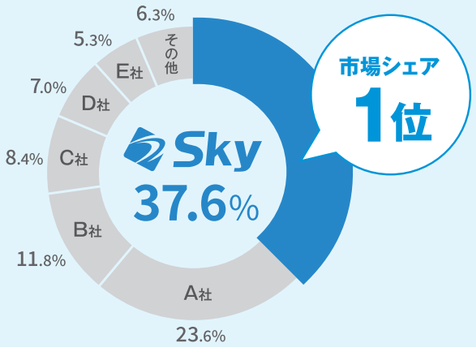
サポートサービス

顧客満足度調査 2021-2022 日経コンピュータ 運用管理・仮想化ソフト（クライアント）部門
日経コンピュータ 2021年9月2日号
顧客満足度調査 2021-2022
運用管理・仮想化ソフト/サービス（クライアント）部門
2年連続1位

自治体ITシステム満足度調査 2021-2022 日経BPガバメントテクノロジー
日経BPガバメントテクノロジー 2021年秋号
自治体ITシステム満足度調査 2021-2022
運用管理・仮想化ソフト/サービス（クライアント）部門
2年連続1位

パートナー満足度調査 2021 日経コンピュータ クライアント管理・統合運用管理ソフト／サービス
日経コンピュータ 2021年2月18日号
パートナー満足度調査 2021
クライアント管理・統合運用管理ソフト／サービス部門
1位

※上記の調査は、製品ではなく企業を対象にしたものです。



「統合エンドポイント管理ツール」2020年度

市場シェア1位を獲得！

富士キメラ総研「2021 ネットワークセキュリティビジネス調査総覧 市場編」

クライアント運用管理ソフトウェア「SKYSEA Client View」は、株式会社富士キメラ総研の「2021 ネットワークセキュリティビジネス調査総覧 市場編」において、「統合エンドポイント管理ツール」2020年度市場シェア1位を獲得しました。今後もお客様により高いご満足を提供すべく、商品およびサービスのさらなる品質向上に取り組んでまいります。

最高の情報漏洩対策のために最新版をご提供

常に高いセキュリティレベルを維持していただくために、機能改善を主としたマイナーバージョンアップだけではなく、新機能を搭載するメジャーバージョンアップもご提供しています。アップデートモジュールは「保守契約ユーザー用Webサイト」より、ダウンロードいただけます。また、バージョンアップによる機能強化ポイントや、アップデート手順書をご紹介しています。

最新情報と共に、運用を支えるさまざまなツールを公開

保守契約ユーザー用Webサイト

SKYSEA Client Viewの最新版アップデーターのほか、運用にお役立ていただける情報や各種ツールをご提供しています。

- よくあるご質問（FAQ）、トラブルシューティング
- ソフトウェアダウンロード
- ドキュメントダウンロード
- オンラインマニュアル
- 障害情報、技術情報 など

最新のソフトウェア辞書情報をご提供

国内外で一般公開されているソフトウェアの情報を収録した、一般社団法人IT資産管理評価認定協会（SAMAC）の「SAMACソフトウェア辞書」をご提供しています。ダウンロードしてSKYSEA Client Viewに登録すれば、SKYSEA Client Viewで収集したソフトウェア情報を、「有償ソフトウェア」や「フリーソフトウェア」といった種別ごとに分類できます。また、ソフトウェア管理台帳に登録したソフトウェア情報に、ソフトウェア辞書のベンダー、エディションなどの情報を反映することができます。

専門のスタッフが、お客様の日々の運用をサポート

ヘルプデスクサービス

お困りのときは電話・メール・FAXなどでお気軽にお問い合わせいただければ、専門スキルを持ったサポートスタッフがトラブルの内容、お客様の環境などを確認し、全力で対応いたします。

5つのお約束

01 お問い合わせには翌営業日までに回答いたします。
02 いつでも品質の高いサポートを提供いたします。
03 どこまでもサポート品質の向上を追求いたします。
04 サービスの改善もリスク管理を行った上で実施いたします。
05 問題点は徹底して再発防止に取り組みます。

ITサービスマネジメント国際規格

『ISO/IEC 20000』を取得

自社開発したソフトウェアの保守サポートサービスにおいて、ITサービスマネージメントのグローバルスタンダードである国際規格「ISO/IEC 20000」を取得しています。

bsi. ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY
ITMS 512306 / ISO/IEC 20000-1:2018

定期的に、“お困りごと”がないかをお伺いします

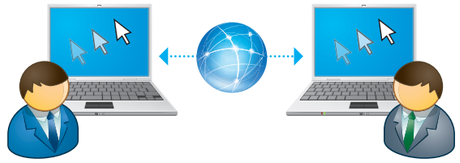
ご導入いただいた後も一定期間、Sky株式会社（以下、弊社）のスタッフより定期的にご連絡し、運用方法やソフトウェアの操作について、ご不明な点やお困りごとがないかを伺い、お客様の快適な運用を支援いたします。

※お客様よりお問い合わせをいただいた直後など、状況に応じてお電話を控える場合や、メールにてご連絡を差し上げる場合がございます。

リモート操作で、より早く的確にトラブルを解決

リモートサポートサービス

お問い合わせ内容やトラブルの状況に合わせて、弊社スタッフが、インターネットを通じてお客様のPCをリモートコントロール。操作のご案内やトラブル解決に対応いたします。簡単な操作で安全に接続できるので、電話だけのサポートに比べてお客様のご負担を減らすことができ、早期のトラブル解決にお役立ていただけます。



運用に役立つ情報を定期的にお届け

情報誌『SKYSEA Client View NEWS』

IT、情報セキュリティ分野の有識者の寄稿やインタビューのほか、導入事例やワンポイントアドバイスなど、組織のIT運用管理に役立つ情報を掲載した情報誌「SKYSEA Client View NEWS」を定期的に発行しています。

メールマガジン

SKYSEA Client Viewに関する最新情報や各種セミナーのご案内、導入事例や話題のニュースなど、お役立ていただける情報をお届けします。

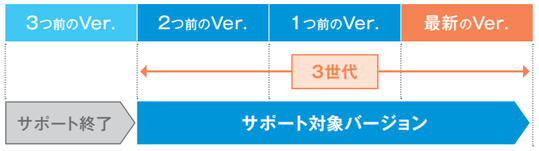
保守契約ユーザー向けサポートニュース

SKYSEA Client Viewの運用や情報漏洩対策にお役立ていただける情報をご提供します。 ※保守契約ユーザー用Webサイトよりお申し込みいただく必要がございます。

ライフサイクルポリシーについて

サポートの対象は最新のバージョンを含め、3世代までです

サポートの対象となるSKYSEA Client Viewのバージョンは、最新のメジャーバージョンを含め、3世代までです。メジャーバージョンアップが行われた時点で、3世代より前となるバージョンはサポート終了となります。



サポートが終了したバージョンのお問い合わせについて

サポートが終了したバージョンの基本的な操作方法についてはサポートいたしますが、不具合・トラブルなどで調査が必要な場合には、まずご利用のSKYSEA Client Viewをサポート対象のバージョンにバージョンアップいただきますようお願いいたします。バージョンアップ後に、調査等を継続いたします。

Ver.14を含む場合のサポート期間について

通常、SKYSEA Client Viewではメジャーバージョンを約12か月ごとにリリースしていますが、Ver.15については、Ver.14のリリース後、約7か月でのリリースとなりました。そのため、これら2バージョンを合わせて1世代として取り扱うことで、他バージョンと比べてサポート期間が短くならないようにしています。

Column

上原 哲太郎 氏

立命館大学 情報理工学部 セキュリティ・ネットワークコース 教授 京都大学博士（工学）

1995年　京都大学大学院工学研究科博士後期課程研究指導認定退学。京都大学大学院工学研究科助手、和歌山大学システム工学部講師、京都大学大学院工学研究科助教授、京都大学学術情報メディアセンター准教授を経て、2011年総務省技官。通信規格と情報セキュリティ施策に従事。2013年より現職。NPO情報セキュリティ研究所理事、NPOデジタル・フォレンジック研究会会長、（一財）情報法制研究所理事、京都府警察サイバーセキュリティ戦略アドバイザー、和歌山県警察サイバー犯罪対策アドバイザー、滋賀県警察サイバーセキュリティ対策委員会アドバイザー、芦屋市CIO補佐官。

DX（デジタル・トランスフォーメーション）への対応は、まずITリテラシーの底上げから

コロナ禍に見舞われた日本社会は、これまでいかに保守的で非効率な業務形態にしがみついてきたか、その不都合な現実と嫌というほど向き合わされました。進まないテレワーク、なくならない押印とFAX、特別定額給付金給付やワクチン配送・接種予約のデジタル化の遅れ、これらのトラブルは我々がいかにデジタル時代に対応できていなかったかの証明になってしまいました。

この事態を打破するためには、各業務の現場が「仕事のやり方を変える」という痛みを受け入れ、デジタルに最適化された業務手続きを確立する必要があります。コロナ禍を無事乗り越えたとしても次に私たちが直面するのは急速な社会の高齢化であり、今まで先送りされてきた生産性向上という課題に取り組まずしてこの社会を維持することは困難です。

DXによる生産性向上は、現場の意識改革とITリテラシー向上のための従業員教育から始める必要があります。ローコード・ノーコードツールやRPAの導入のためには、各現場に業務とITの双方に通じた人材の配置を必要とします。GIGAスクール構想の効果が出てくるまではまだ間があり、現状では社会人のリカレント教育に頼らざるを得ません。データ構造とアルゴリズムの考え方が少し身につくだけで、多くの現場で業務効率の劇的な改善策が見いだせるようになるでしょう。

一方、デジタル化はその効率化と引き換えのリスクを呼び込むことも忘れてはいけません。ITリテラシー教育と平行してセキュリティ教育にも取り組み、従業員のセキュリティへの理解を底上げすることで、日々高度化するサイバー攻撃への対応力を上げ、安心して全力でDXに取り組むことができるようになるのです。

監修 上原 哲太郎 氏　セキュリティ研修について

本研修は上原 哲太郎 氏監修のもと、セキュリティご担当者様が知っておくべき、インシデント発生時の対応等、組織的・体系的に情報セキュリティを確保するために必要な情報をご紹介します。また、一般職員の方向けに、一般的な情報セキュリティ対策が学べる研修もご用意しています。組織としてのセキュリティリテラシーの向上に、ぜひご検討ください。

■ 管理者向けセキュリティ研修

組織として取り組むべき情報セキュリティ対策についてご紹介します。情報セキュリティを担保しながら、生産性を向上していくための心得を知ることができます。

費用 150,000円／回　所要時間 約1時間30分

■ 一般職員向けセキュリティ研修

従業員が日ごろから意識すべき情報セキュリティ対策についてご紹介します。業務でPCを使用するにあたっての情報資産の取り扱い方や、習得すべきセキュリティリテラシーを学んでいただけます。

費用 150,000円／回　所要時間 約1時間30分

※1回200名様までご参加いただけます。201名様以上ご参加いただく場合は複数回の実施で対応いたしますので、回数分をご購入ください。※ご要望に応じてZoomによる実施も承っております。※記載している事項は2021年9月8日時点の情報です。最新情報は、Webサイト（https://www.skyseaclientview.net/support/guide/guide005.html#service10）をご覧ください。

品質向上への取り組み

専用テスティングルームを設置・自社PC約8,000台以上に導入

社内に専用のテスティングルームを設置し、あらゆる環境を想定した評価 / 検証を行っています。また全事業部約8,000台以上のクライアントPCにSKYSEA Client Viewを導入し、実際の業務で活用しています。継続的な運用の中で浮き彫りになる、細かな課題も見逃さずに商品開発にフィードバックを行っており、お客様と同じ「利用者の視点」でソフトウェアの機能向上に取り組んでいます。

情報セキュリティマネジメント国際規格『ISO/IEC 27001』

Sky株式会社（以下、弊社）は、情報セキュリティ対策の管理の仕組みについて規定した国際規格である「ISO/IEC 27001」を取得。SKYSEA Client Viewを自社活用しながら、第三者機関による定期的な監査を受けて継続審査に合格しており、高い情報セキュリティレベルを維持しています。

IS 80703 / ISO/IEC 27001:2013

IS 80703 / JIS Q 27001:2014

個人情報保護規格『プライバシーマーク』

弊社は、保有する個人情報の取り扱いおよび管理体制について、第三者機関に認証を受け「プライバシーマーク」を取得。お客様の情報はもちろん、あらゆる個人情報を適切に管理・保護しております。高い情報セキュリティレベルを実現するために、商品の品質管理を徹底しています。

品質管理規格『CMMI® レベル3』

ICTソリューション事業部開発部開発課では、ソフトウェアの品質管理向上に取り組み、2007年2月～2010年2月の期間、国際的な品質管理規格CMMIレベル3達成の認定を受けました。今後も改善を積み重ね、より高品質で使いやすいソフトウェアを目指した開発を行います。

特許への取り組み

Sky株式会社（以下、弊社）は、お客様に便利で使いやすい機能を提供し続けるために、先進の技術を駆使してさまざまな研究・開発に取り組んでいます。その成果として、特許出願・取得を行うとともに、新機能として商品に搭載しています。

SKYSEA Client View 関連 特許取得実績（2021年9月現在）

分類項目	特許取得	分類項目	特許取得	分類項目	特許取得
資産管理	14	ログ管理	15	セキュリティ管理	22
メンテナンス	5	操作画面	11	その他	6

「知的財産活用支援奨励賞」受賞

日本弁理士会が主催する第3回知的財産活用表彰において、「知的財産活用支援奨励賞（事業支援サポート部門）」を受賞いたしました。SKYSEA Client Viewが、企業の営業秘密保護を支援する機能を多数搭載していること、さらに、これら機能に関して積極的に特許出願・取得に取り組んでいることが評価され、本賞を受賞することとなりました。

有償開放特許 現在の有償開放特許数【131件】

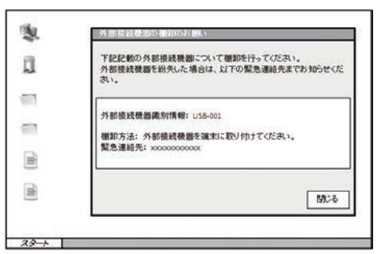
弊社の保有している特許技術は、有償開放（ライセンス提供）しております。その特許技術のいくつかを紹介いたします。このほかにも、弊社の所有する特許を有償にてライセンス提供いたします。詳しくは、Webサイト（https://www.skyseaclientview.net/patent/）をご覧ください。

発明の名称　棚卸支援システム及び棚卸支援プログラム

特許番号：特許第5208879号　　**出 願 日**：2009年8月6日

登 録 日：2013年3月1日

概　　要：外部接続機器の利用時に、端末とその外部接続機器を関連付けた使用情報を生成する。棚卸の際には、その使用情報を用いて、外部接続機器を所持している可能性の高い端末を特定する。



商品搭載実績

SKYSEA Client View USBデバイス棚卸

棚卸の際に、USBデバイスの所持者や最終使用端末を特定して通知することができる。

Column

情報セキュリティ対策の徹底は個人情報を扱う組織の責務

岡村 久道 氏

弁護士 / 博士（情報学） / 京都大学大学院医学研究科講師（非常勤）

京都大学法学部卒業。弁護士。博士（情報学）。京都大学大学院医学研究科講師（非常勤）。元国立情報学研究所客員教授。専門分野は情報ネットワーク法、知的財産権法など。主著は「情報セキュリティの法律」「これだけは知っておきたい個人情報保護」「個人情報保護法」「迷宮のインターネット事件」「番号利用法――マイナンバー制度の実務」など多数。

悪質なサイバー攻撃による大量漏えいやランサムロック被害が頻発している。現に被害を受けた日本企業も多い。

そうしたなか個人情報保護法の2020年改正で、「重大な漏えい等」発生のおそれが判明した企業に対し、個人情報保護委員会に報告し、本人に通知する義務が新たに課された。2021年改正で義務の対象が自治体や国公立学校、その他の公的機関にも拡大された。

報告・通知事項は【表】のとおりであり、本人全員に連絡が取れないときは、代替措置が必要だ。自社サイトでの公表や相談窓口の設置が想定されている。

委員会への報告時期は、事実関係を十分に把握できていない段階の「速報」と、原因や再発防止策も含めて報告を求める「確報」の二段階としている。「確報」は当該事態を知った日から30日（不正アクセスなど故意によるものは60日）以内とされている。事故発覚後から対処すべき事柄は尽きないから、「確報」期限など、あっという間に過ぎてしまう。

これら改正は2022年度初頭に施行される。まさに「待ったなし」である。さらにプライバシー侵害として集団訴訟を提起される事態も懸念される。他社から預かったデータなら取引打ち切りになりかねない。

こうした事故発生を防止するための「転ばぬ先の杖」として、また不幸にして事故が発生したときでも原因を迅速にトレースできるように、日頃から十分なセキュリティ対策を講じることこそが最も大切だ。だから操作ログ情報収集ツールの重要性は高い。

そうした従業員・職員向けモニタリングツールを導入する際の条件として、委員会は、①モニタリングの目的を事前に特定して内部規程化し、従業員などに明示、②モニタリング実施の責任者・権限を定め、③その実施ルールを設けて内容を運用者に徹底、④当該ルール遵守状況の確認を求めている。勤務先貸与端末の場合を含め、それを使う従業員などにとって、モニタリング自体が自身の個人情報やプライバシー保護に関わるからだ。そのため、こうした条件を守り、対象となる従業員などに事前告知して同意を取得しておけば安心だ。導入で職場全体のセキュリティ意識も高まる。以上の点は学校の場合も変わらない。

いまや「管理策が不十分でした」と謝罪するだけでは済まされない時代が到来したことを、改めて我々は肝に銘じる必要があるはずだ。

事項	委員会への報告	本人への通知
(1) 概要	○	○
(2) 漏えい等が発生（おそれを含む）した個人データの項目	○	–
(3) 漏えい等が発生（おそれを含む）した個人データの頭数	○	–
(4) 原因	○	○
(5) 二次被害又はそのおそれの有無と内容	○	○
(6) 本人への対応の実施状況	○	–
(7) 公表の実施状況	○	–
(8) 再発防止措置	○	–
(9) その他参考事項	○	○

Column

「新しい働き方」に向けて、より重要となる労務実態の見える化

宮川 弘之 氏

株式会社Ｈ＆Ｉコンサルティング 代表取締役
社会保険労務士事務所Ｈ＆Ｉ 所長 / 特定社会保険労務士

証券会社勤務を経て、平成14年社会保険労務士として開業登録。日ごろは中小企業から大企業まで幅広く就業規則作成、人事制度構築（賃金制度・退職金制度・人事考課制度）、人事労務リスクマネジメント（労使トラブル対策、労働組合対策、労働時間管理適正化の支援等）、企業研修を主に行っている。また大学、自治体においても「ハラスメント」・「メンタルヘルス」等の研修・客員講師の実績も多数あり。

「過重労働の防止」「ワーク・ライフ・バランス」「多様で柔軟な働き方」の実現を目的とした「働き方改革関連法」が2019年4月より順次施行され、その中の一つの施策として「労働時間法制の改正」が行われました。

法改正後は、残業時間の上限規制とともに、健康管理の観点からタイムカードやPCのログ等の客観的な記録に基づいて、すべての従業員（管理監督者を含む）の労働時間を把握することが企業に義務づけられました。長時間労働を抑制するためにも、「業務の見える化」により、その業務プロセスを検証し、生産性の向上を図ることが不可欠となります。

また、2020年に入り、新型コロナウイルス感染症の拡大防止のために多くの企業が時差出勤やテレワークを実施するなど、今までと違った「新しい働き方」の導入が進んでいます。ただ、テレワークには、「在宅勤務者の正確な労働時間が把握しづらい（勤務時間とプライベート時間の区分が困難）」「在宅勤務者の管理や評価がしづらい（業務内容の把握が困難）」「情報セキュリティの管理が難しい」など、労務管理上の課題が数多くあります。

SKYSEA Client Viewは、従業員のPC利用時間や作業内容（操作ログ情報）を企業が把握することを支援し、従業員の「業務の見える化」および「情報セキュリティの管理」に役立てることができます。

このようなソフトウェアを活用し、“Withコロナ時代の新しい働き方”という労働環境の変化に対応することが望まれます。

公式YouTube™チャンネル

新しい動画を
随時公開中！

Sky株式会社 公式チャンネルのご案内

最新技術への取り組みや自社パッケージ商品の特長などを、動画で幅広くご紹介しています。
SKYSEA Client Viewの機能についてまとめた動画なども公開していますので、ぜひご覧ください。

公式チャンネルのご視聴は
検索もしくはQRコードから

Sky株式会社 公式チャンネル

SKYSEA Client View は“企業・団体”のお客様向け商品です

商品に関するお問い合わせや最新情報は

Webサイト

SKYSEA　検索

https://www.skyseaclientview.net/

商品に関するお問い合わせは、Webサイトよりお受けしております。

インフォメーションダイヤル

- 企業名、本社代表電話番号などをお答えいただけない場合、ご利用いただけません。
- 法人以外の方からのお問い合わせには対応いたしかねます。
- サービス・品質の向上とお問い合わせ内容などの確認のために、通話を録音させていただいております。

03-5860-2622（東京） **06-4807-6382**（大阪）

受付時間 9:30～17:30（土・日・祝、ならびに弊社の定める休業日を除く平日）

弊社は、Microsoft社の製品やテクノロジーをベースとしたサービスの開発や販売を行うIT関連企業に対するパートナープログラム制度において、「マイクロソフトGoldコンピテンシーパートナー」の認定を受けています。

Gold
Microsoft Partner
Microsoft

Sky株式会社 — https://www.skygroup.jp/ —

東京本社　〒108-0075
東京都港区港南二丁目16番1号 品川イーストワンタワー15F
TEL.03-5796-2752　FAX.03-5796-2977

大阪本社　〒532-0003
大阪市淀川区宮原3丁目4番30号 ニッセイ新大阪ビル20F
TEL.06-4807-6374　FAX.06-4807-6376

札幌支社　仙台支社　横浜支社　三島支社　名古屋支社　神戸支社
広島支社　松山支社　福岡支社　沖縄支社

※本カタログに掲載している画面はすべて開発中のものです。※各機能のご紹介は、Windows端末の管理を基本として掲載しております。

KO-20000-11 / 21·09·24