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）

Sky株式会社の取り組みや、商品・イベントなどの情報を発信しています。

企業アカウント
sky_it_corporate
Instagram

企業アカウント
@Sky_corporate
X（旧Twitter）

公式YouTube™チャンネル
@Sky_Inc.
YouTube™

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 ソリューションパートナー」の認定を受けています。

Microsoft Solutions Partner

Sky株式会社　— https://www.skygroup.jp/ —

東京本社　〒108-0075
東京都港区港南2丁目18番1号 JR品川イーストビル9F
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　大宮支社　横浜支社　静岡支社　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。

Sky / 25･02･26

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

概要
カタログ

ITリスク対策が、企業を進化させる。

Sky

SKYSEA Client Viewの特長

20,000社を超える導入実績

※SKYSEA Client Viewの実績は、オンプレミス版とクラウド版の合計値となっています。

累計導入実績
（2025年1月末現在）

22,926社

12,079,851クライアント

毎年のバージョンアップで常に進化

Ver.14（2019） Ver.15（2020） Ver.16（2021） Ver.17（2022） Ver.18（2023） Ver.19（2024） Ver.20（2025）

各分野で高い評価を獲得

顧客満足度調査 2024-2025 日経コンピュータ 運用管理・仮想化ソフト／サービス（クライアント）部門

日経コンピュータ 2024年9月5日号
顧客満足度調査 2024-2025
運用管理・仮想化ソフト/サービス（クライアント）部門 1位

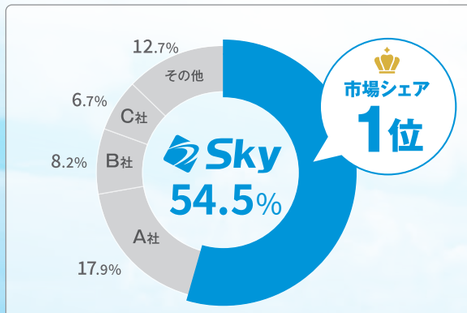
自治体ITシステム満足度調査 2024-2025 日経ガバメントテクノロジー

日経BPガバメントテクノロジー 2024年秋号
自治体ITシステム満足度調査 2024-2025
運用管理・仮想化ソフト/サービス（クライアント）部門 5年連続1位

パートナー満足度調査 2025 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 2025年3月6日号
パートナー満足度調査 2025
クライアント管理・統合運用管理ソフト／サービス部門 3年連続1位

※上記調査は、製品ではなく企業を対象にしたものです。



「端末管理・セキュリティツール（ソフトウェア）」2023年度

市場シェア1位を獲得！

富士キメラ総研「2024 ネットワークセキュリティビジネス調査総覧 市場編」

組織の安全なIT運用を支援する各種機能

資産管理
- IT資産情報の自動収集
- アップデート状況の管理
- ソフトウェアの配布

ログ管理
- 操作ログの自動収集
- ログを検索・解析
- PC画面の録画

セキュリティ管理
- 不正操作を検知し管理者に通知
- 利用者にもポップアップ通知
- 使用不許可PCの検知

デバイス管理
- 管理台帳の作成
- 使用の制限
- 棚卸による所在確認

ITセキュリティ対策強化
- 他社製品との連携による多層防御
- マルウェア感染時のネットワーク遮断
- 共有フォルダへのアクセス制限

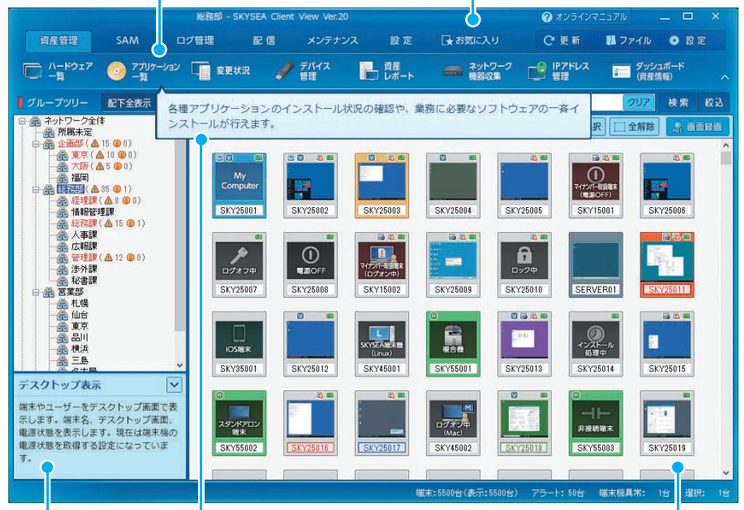
メンテナンス
- リモート操作
- 電源の制御
- メッセージの配信

モバイル機器管理（MDM）
- 機器情報の自動収集
- 不要な機能・操作の制限
- 紛失・盗難時のリモート制御

直感的に使いやすい管理画面を搭載

カテゴリ分けされた
わかりやすい機能メニュー

よく使う機能を登録できる
「お気に入り」タブ



各機能について説明する
「機能ガイド」

初めてでも操作に迷わない
「ふきだしヒント」

各PCの稼働状況が確認できる
デスクトップ画面表示

運用形態

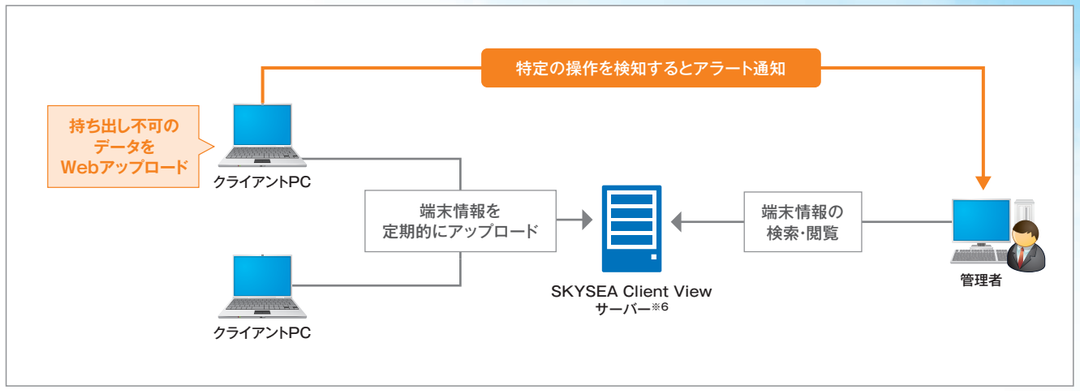
	オンプレミス		クラウド	
	オンプレミス版※1	アプライアンス版（NAS版）	M1 Cloud Edition	S1H / S3H Cloud Edition
特長	すべての機能と連携ソリューションが利用可能 すべての搭載機能と各連携ソリューションが利用できるほか、PCは50,000台まで管理可能。パブリッククラウドにも対応します。	バンドル済みの専用機器で手間なく導入、小規模環境に最適 SKYSEA Client Viewがバンドルされた専用機器でご提供。汎用サーバーと比べて導入の手間やコストを削減できます。	手軽に導入でき、専門知識がなくても簡単運用 インターネット接続環境さえあれば利用でき、アップデートもすべて自動。専門的な知識がなくても手軽に導入・運用が可能です。	サーバー管理の負担を軽減しつつ多くの機能が使える オンプレミス版と遜色ない使いやすさと豊富な機能を搭載。サーバー管理の負担も軽減でき、導入コストも抑えられます。
サーバー導入	必要	不要※2	不要	不要
アップデート	お客様の任意で実施	お客様の任意で実施	弊社が対応	お客様の任意で実施※3
ログについて	自社で保管	自社で保管	クラウド上で保管（2年間）※4	クラウド上で保管（3か月間）※5
PCの管理台数	1～50,000台	1～20台	1～20,000台	50～20,000台
主な導入コスト	● サーバーライセンス ● クライアントライセンス ● サーバー調達費　など	● サーバーライセンス ● クライアントライセンス ● アプライアンス機器調達費　など	なし	なし
主な運用コスト	● 保守ライセンス ● メンテナンスコスト など	● 保守ライセンス ● メンテナンスコスト など	● サービス利用料	● サービス利用料

- オンプレミス版やM1 Cloud Edition、S1H / S3H Cloud Editionの搭載機能については、P.05～06をご覧ください。
- アプライアンス版（NAS版）については、「機能一覧」ページ（https://www.skyseaclientview.net/ver20/feature/）の「アプライアンス版（NAS版）」をご覧ください。

※1 搭載機能が異なる各種エディションから必要に応じてお選びいただけます。※2 アプライアンス機器の導入が必要です。※3 サーバーOSのアップデートは弊社が行います。※4 Web管理コンソールからすべてのPCのログを月単位でダウンロードいただけます。 ※5　PC1台あたりの規定保管容量を設定しています。保管容量を1TB単位で追加でき、保管期間が無期限になるオプションもご用意しています。そのほか、ローカル環境にログを定期的に自動ダウンロードすることも可能です。

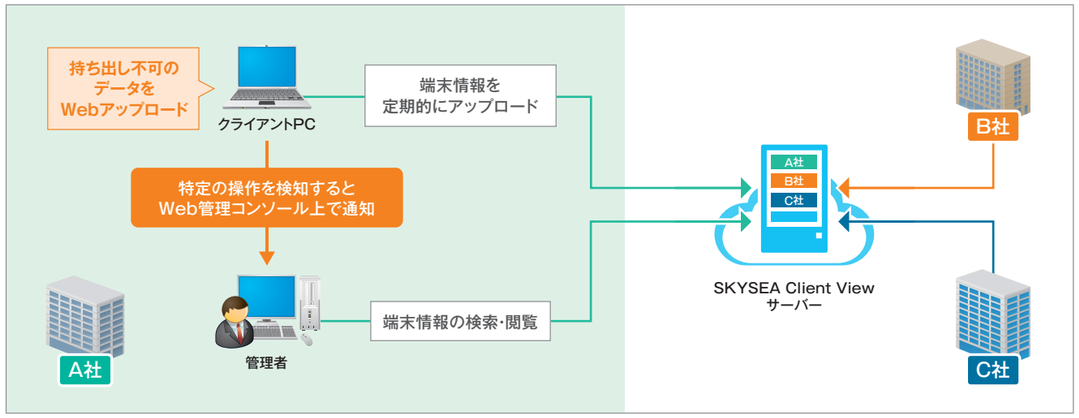
運用イメージ

■ オンプレミス版　■ アプライアンス版（NAS版）

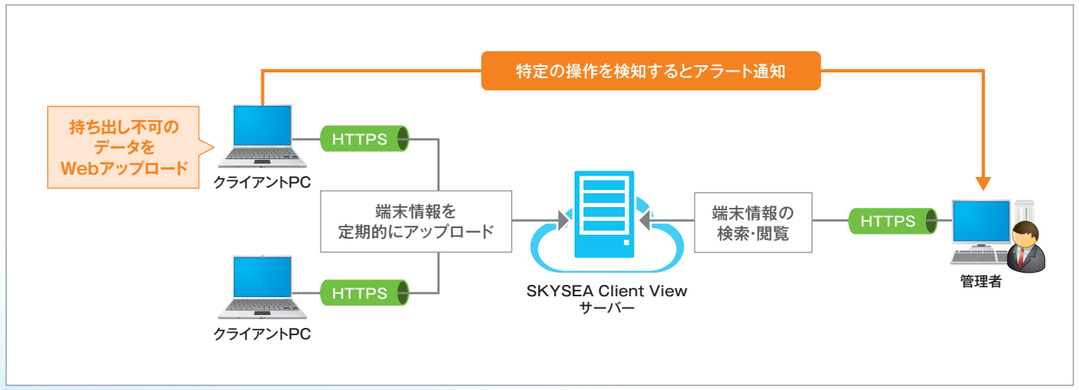


※6 アプライアンス版（NAS版）は、汎用サーバーの代わりにアプライアンス機器を利用します。

■ M1 Cloud Edition



■ S1H / S3H Cloud Edition



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　M1＝M1 Cloud Edition
S1H＝S1H Cloud Edition※1　S3H＝S3H Cloud Edition※1　　OP＝オプション

資産管理	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
ハードウェア一覧 / アプリケーション一覧※2	●	●	●	●	●	●	●	●（※3）	●（※3）
ソフトウェア配布	●	●	●	●	●	●	●	●（※3）	●（※3）
インターネット経由での資産情報収集	●	●	●	●	●	●	●	●	●
ネットワーク機器情報収集※2	●	●	●	●	●	●	—	●（※3）	●（※3）
不許可端末情報収集	●	●	●	●	●	●	—	●（※4）	●（※4）
ダッシュボード	●	●	●	●	●	●	●	●	●

ログ管理	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
ログ収集 / 閲覧※2※5	●	●	●	●	●	●	●	●	●
画面操作録画	OP	OP	OP	OP	OP	OP	—	—	—
想定外TCP通信ログ	●	●	●	●	●	●	—	●	●
送信メールログ	●	OP	OP	OP	OP	●	—	—	—
Web利用状況	●	●	●	●	●	●	—	●（※4）	●（※4）
スタンドアロン端末機ログ収集	●	●	●	●	●	●	—	●	●

セキュリティ管理	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
注意表示（アラート）※6	●	●	●	●	●	●	●	●	●
不許可端末遮断	●	●	OP（※7）	OP（※7）	OP（※7）	●	—	OP（※4）（※7）	●（※4）
端末機異常通知	●	●	OP	OP	OP	OP	—	—	●
ログオフし忘れ防止	●	OP	OP	OP	OP	OP	—	—	—
電子メール送信宛先フィルタ	●	OP	OP	OP	OP	●	—	—	—

セキュリティ管理	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
メール送信時の添付ファイル自動削除	●	OP	OP	OP	OP	●	—	—	—
PC環境診断	OP	OP	OP	OP	OP	OP	—	—	—
CPE製品名管理	●	●	●	●	●	●	—	●	●
紛失端末制御	OP	OP	OP	OP	OP	OP	OP	OP	OP
ブラウザ環境分離	OP	OP	OP	OP	OP	OP	—	—	—
更新プログラム配布管理	●	●	●	●	●	●	—	—	—
Windows 10以降更新制御	●	●	●	●	●	●	—	●	●
EDRプラスパック	OP	OP	OP	OP	OP	OP	—	OP	OP
マイナンバー取扱端末設定・管理	●	●	●	●	●	●	—	●	●
残業時間お知らせメッセージ	●	●	●	●	●	●	—	●	●
画面キャプチャー防止	●	—	●	—	—	—	—	—	—
ファイル受渡しシステム※8	OP	OP	OP	OP	OP	OP	—	—	—

デバイス管理	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
USBデバイス / メディア 台帳管理・使用制限※2※9※10	●	●	●	●	●	●	●（※11）	●	●
USBデバイスの棚卸	●	●	●	●	●	●	—	●	●
申請・承認ワークフローシステム（デバイス利用申請など）	OP	OP	OP	OP	OP	OP	—	—	—
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	—	—	—
USBデバイス不正ファイル検出※12	●	●	●	●	●	●	—	●	●

ITセキュリティ対策強化	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
UTM / 次世代ファイアウォール連携	●	●	●	OP	OP	OP	—	—	●（※4）
特定フォルダアクセスアラート	●	●	●	OP	OP	OP	—	—	●
組織外ネットワーク接続制御	●	●	●	OP	OP	OP	—	—	●
syslog送信	●	●	●	OP	OP	OP	—	—	●（※4）
アプリケーションログ	●	●	●	OP	OP	OP	—	—	●
ソフトウェアの緊急配布	●	OP	OP	OP	OP	OP	—	—	●（※3）
検疫ソフトウェア連携	●	●	●	OP	OP	OP	—	—	●
Microsoft Office更新制御	●	●	●	OP	OP	OP	—	—	●（※3）
セキュリティ基準を満たさない 共有フォルダアクセス制御	●	●	●	OP	OP	OP	—	—	●
ZIPファイル内のファイル情報収集	●	●	●	OP	OP	OP	—	—	●

レポート	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
ログ解析レポート	●	●	●	●	●	●	—	OP（※4）	OP（※4）
資産レポート	●	●	●	●	●	●	—	OP（※4）	OP（※4）
PC活用状況分析	●	●	●	●	●	●	●	●	●
資産・ログ利活用レポートライブラリ	●	●	●	●	●	●	—	OP（※4）（※13）	OP（※4）（※13）

メンテナンス	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
リモート操作※2	●	●	●	OP	●	●	OP	OP（※3）	●（※3）
リモート操作（インターネット経由）※2	OP	OP	OP	OP	OP	OP	OP	OP	OP
キーボード・マウス転送	●	●	●	OP	●	●	—	OP（※3）	●（※3）

メンテナンス	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
電源制御	●	●	●	●	●	●	—	●（※3）	●（※3）
定期再起動	●	OP	OP	OP	OP	OP	—	—	—
メッセージ配信	●	●	●	●	●	●	—	●（※3）	●（※3）

ソフトウェア資産管理（SAM）	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
導入ソフトウェア台帳	●	●	●	●	●	●	—	●	●
申請・承認ワークフローシステム（ソフトウェア利用申請など）	OP	OP	OP	OP	OP	OP	—	—	—

サーバー監査	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
OSログ閲覧	OP	OP	OP	OP	OP	OP	—	—	—
データベースログ収集	OP（※14）	OP（※14）	OP（※14）	OP（※14）	OP（※14）	OP（※14）	—	—	—

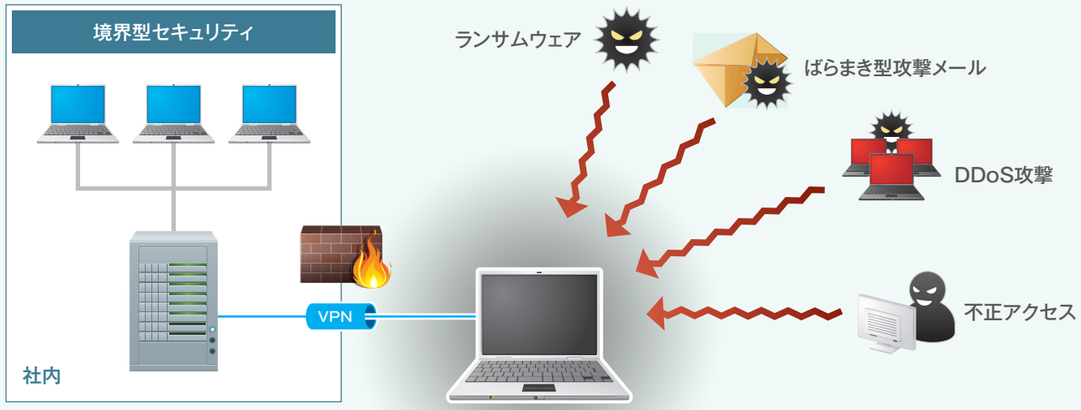
モバイル機器管理（MDM）※15	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
資産管理 / セキュリティ管理	OP	OP	OP	OP	OP	OP	OP	OP	OP
モバイルデバイス応急対策ツール	OP	OP	OP	OP	OP	OP	—	OP	OP

その他	オンプレミス						クラウド		
	Ent	Pro	Tel	LT	500	ST	M1	S1H	S3H
在席確認・インスタントメッセージ	OP	OP	OP	OP	OP	OP	—	—	—
Remote Access Services	OP	OP	OP	OP	OP	OP	OP	OP	OP
管理者向けコミュニティサイト	●（※16）	●（※16）	●（※16）	●（※16）	●（※16）	●（※16）	●（※16）	●（※16）	●（※16）

※1　クラウド上のサーバーとクライアントPCとの接続にはHTTPSを利用します。また、VPN接続を利用いただくことも可能です。
※2　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。※3　管理機とクライアントPCが直接通信できない環境では一部利用できない機能があります。※4　VPN接続環境下においてのみ利用いただけます。※5　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。※6　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。※7　不許可端末の接続を検知する機能は標準搭載です。※8「申請・承認ワークフローシステム」オプションでご利用いただけます。※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　メディアには対応しておりません。※12 SKYSEA Client Viewがインストールされていないパソコン上で保存、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「アプリケーション利用 / Webシステム用グループ集計」「プリンター印刷 / Webシステム用グループ集計」「Webアクセス（ドメイン毎） / Webシステム用グループ集計」「外部記憶書き出し / Webシステム用グループ集計」は利用いただけません。※14　本機能は「サーバー監査」機能＜オプション（Ent/Pro/Tel/LT/500/ST）＞のオプションとしてご購入いただけます。※15 ログ収集などのログ管理機能は搭載しておりません。※16 ご契約内容等により、一部のお客様はご利用いただけない場合がございます。

サイバー攻撃のリスク対策を エンドポイントセキュリティで実現

ランサムウェアなどのサイバー攻撃が激化するなか、リモートワークの導入によってPCを組織外に持ち出す機会は増え、情報漏洩リスクも高まっています。組織内のネットワークを堅牢にする「境界型セキュリティ」ではこれらリスクに対処しきれない今、末端のIT機器を強固に守る「エンドポイントセキュリティ」が求められています。「SKYSEA Client View」では、エンドポイントへの対策に特化したさまざまな機能を搭載しています。



PC（エンドポイント）は常に情報漏洩リスクにさらされている!

リスク1

把握していない端末経由で マルウェアに感染

対策1
組織内のエンドポイントを 全数把握

リスク2

更新プログラム未適用で 脆弱性が狙われる

対策2
OSやソフトウェアの アップデートを徹底

リスク3

未知のサイバー攻撃に 対処できない

対策3
EDR製品などを 活用して脅威に対応

「SKYSEA Client View」がエンドポイント対策を支援!

対策1 組織内のすべてのIT機器を把握し、管理漏れをなくす

管理者が把握できていないIT機器が1台でもあると脆弱性は放置され、マルウェア感染につながる可能性も。「資産管理」機能※1で、組織内のIT機器情報を自動収集し、新たに持ち込まれる機器についても素早く把握することができます。

VPN機器などのデバイス情報も網羅

ネットワーク機器情報収集

標準搭載 Ent/Pro/Tel/LT/500/ST/S1H/S3H

IPアドレスの範囲などを指定し、資産情報が登録されていないIT機器を洗い出し。VPN機器、Webカメラ、IoTデバイスなど、ネットワーク接続されるものはすべて管理できます。

※1「資産管理」機能については、P.13をご覧ください。

新たなIT機器の接続をアラートで通知

不許可端末検知

標準搭載 Ent/Pro/Tel/LT/500/ST/S1H/S3H

組織で購入したPCや持ち込みPCなど、新たなIT機器がネットワークに接続された際に、管理者にアラートで通知。MACアドレスなどの機器情報が確認でき、資産情報として登録できます。

対策2 迅速なアップデートで脆弱性に対策、ソフトウェアを常に最新に

OSやソフトウェアの更新プログラムが適用されず、脆弱性が残された状態では、攻撃者に不正アクセスに利用されたり、マルウェア感染のリスクも高まります。組織で利用するソフトウェアなどの脆弱性情報を的確に把握し、手間なくスピーディにアップデートを行えるように支援します。

一斉配布で素早いアップデートを実施

ソフトウェア配布

標準搭載

管理機から各PCに一斉に更新プログラムを配布・インストールし、脆弱性に素早く対応。配布スケジュールを設定し、業務に支障が出にくい時間帯に実行することも可能です。

最新の脆弱性情報を効率的に取得

CPE製品名管理

標準搭載 Ent/Pro/Tel/LT/500/ST/S1H/S3H

SKYSEA Client Viewで管理するソフトウェアと、JVN※2が提供する脆弱性情報をひもづけ、まとめて表示。各ベンダーのWebサイトなどで情報収集する手間を減らし、速やかな修正プログラム適用につなげていただけます。

※2　JVN（Japan Vulnerability Notes）。日本で利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ポータルサイト。

対策 3

EDR製品と連携し、未知の脅威への対策を万全に

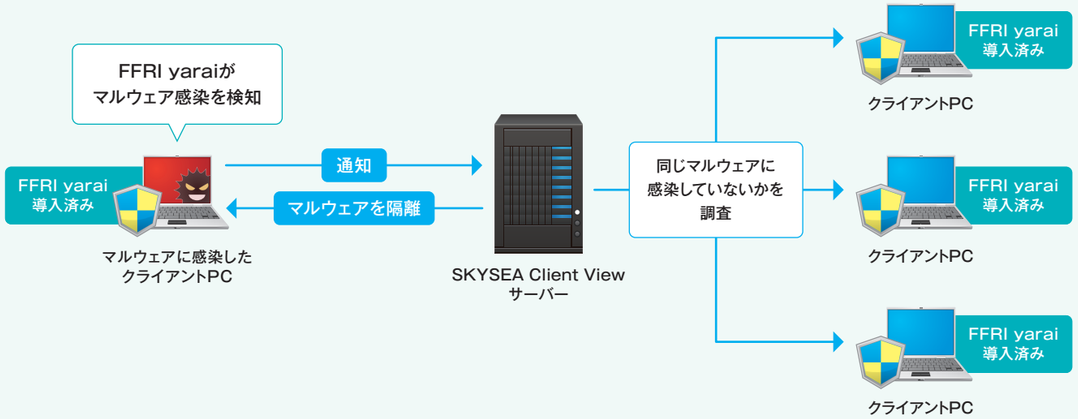
進化するサイバー攻撃の脅威に対しては、パターンファイルに依存したマルウェア検知では不十分です。未知の脅威を検知し、素早い調査・駆除を可能にするEDR製品との連携機能をご提供しています。

未知のマルウェアをふるまい検知で素早く発見、隔離して調査

EDRプラスパック

オプション Ent/Pro/Tel/LT/500/ST/S1H/S3H

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

標的型攻撃対策に特化し、未知の脅威・脆弱性攻撃からクライアントPCを防御する次世代エンドポイントセキュリティです。

先読み技術
パターンファイルに依存しないふるまい検知で、未知の脅威を防御

豊富な導入実績
中央省庁や金融機関、ライフラインを支える重要システムに多くの導入実績

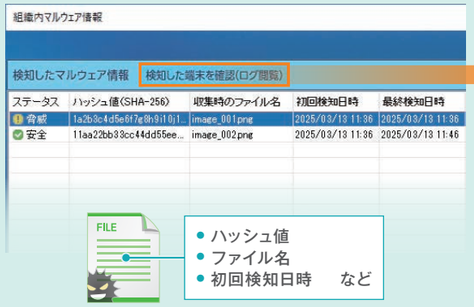
多層防御
5つのエンジンと一般的なウイルス対策ソフトウェアとの同居による多層防御

安心の純国産
基礎技術研究から開発・保守に至る全行程を日本国内で実施

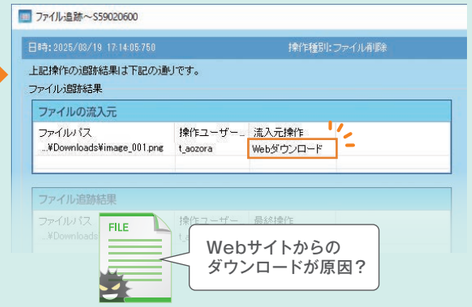
PCの操作ログから感染原因を調査

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。

1 検知されたマルウェアの情報が一覧で表示

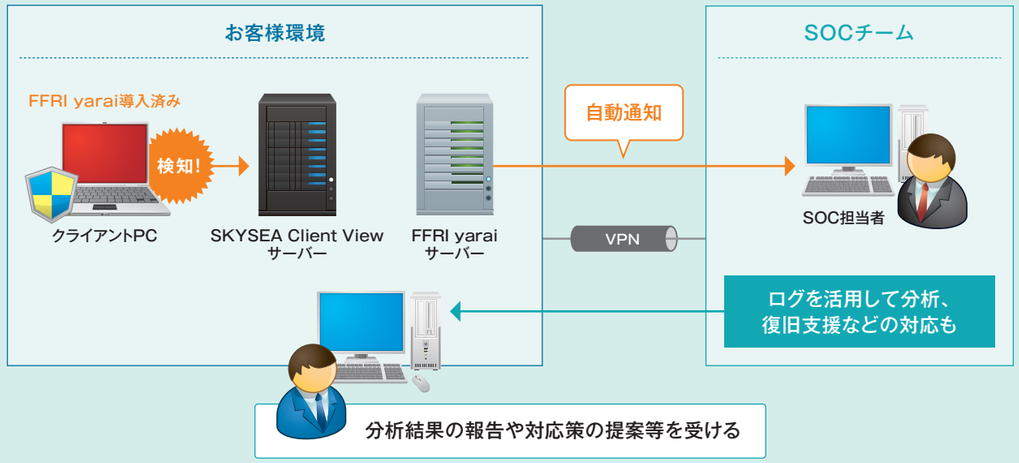


2 マルウェアのファイル名を基に流入元を調査



「EDRプラスパック」の効果をより高めるSOCサービスをご提供

情報セキュリティの専門チームが「EDRプラスパック」の運用・監視を行い、サイバー攻撃検知時の分析や対応策の提案、復旧支援などを行うサービスをご用意しています。「EDRプラスパックを導入したいけど、専門的なノウハウを持つ人材がいない」「迅速に対応できるリソースの確保が難しい」といった組織でお役立ていただけます。



「EDRプラスパック」の運用・監視を行うSOCサービス

エヌ・ティ・ティ・アドバンステクノロジ株式会社様
- EDR端末監視ソリューション(SKYSEA&yarai SOC)

サービス&セキュリティ株式会社様
- セキュリティ運用監視サービス

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の操作履歴（ログ）を活用することで、日々の業務でPCを使用する従業員の労働時間の見える化を支援します。また、業務時間外のPC操作を制限する機能なども搭載しており、組織の過重労働対策への取り組みをサポートします。

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

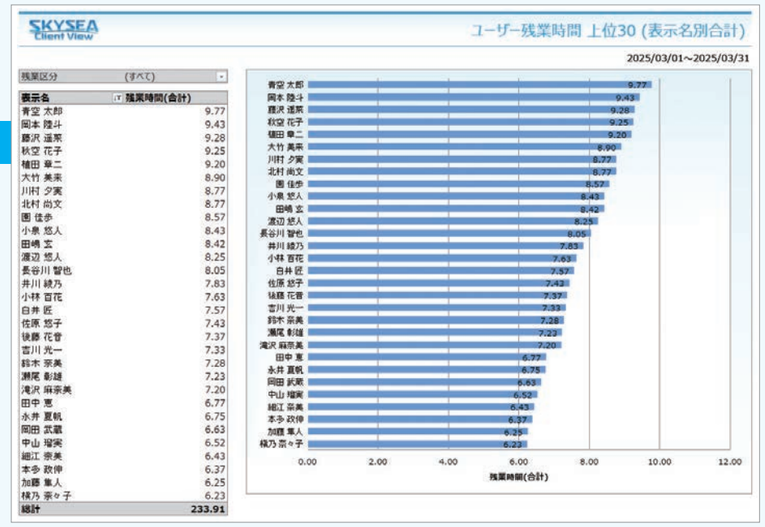
標準搭載 Ent/Pro/Tel/LT/500/ST　オプション S1H/S3H

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

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。



PCの操作時間を集計・分析し、従業員の頑張りを定量的に見える化

PC活用状況分析

標準搭載

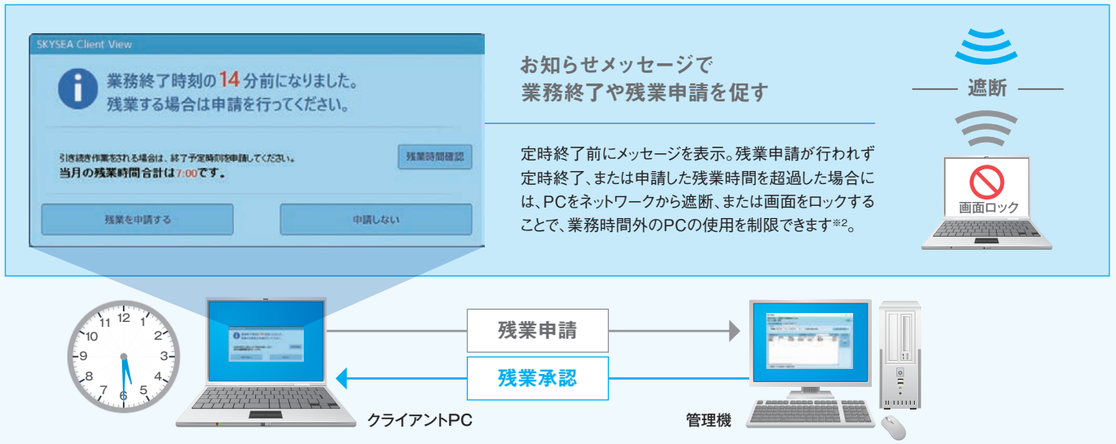
業務時間内におけるPCの操作時間の割合を、ユーザーごとに集計・分析してグラフ化。従業員の頑張りや負荷状況を把握する際の、定量的な参考データとしてご活用いただけます。

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】

標準搭載 Ent/Pro/Tel/LT/500/ST/S1H/S3H

定時終了前や業務時間外に従業員に業務終了や残業申請を促すことができます。申請された残業は、管理機から承認 / 拒否が行えるほか、当月の累計残業時間を一覧で確認することもできます。PCの操作ログから残業時間を日々適切に把握することで、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。



※1 本機能は、お客様の営業日と業務時間を設定いただくことでご利用いただけます。ただし、残業の申請・管理は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対応ください。※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。

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、台帳で管理。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。

必要な情報を素早く検索、管理業務を効率化

ハードウェア一覧　標準搭載

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

標準搭載　Ent/Pro/Tel/LT/500/ST/S1H/S3H

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。

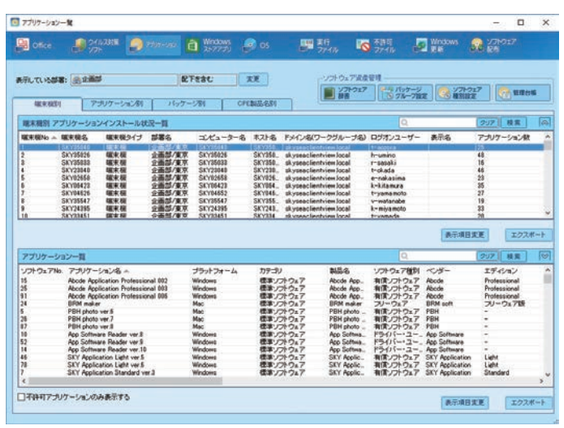
インストール状況を把握し、ライセンスの最適化を図る

アプリケーション一覧　標準搭載

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で、適切な管理を支援します。

管理できるソフトウェア種別

- Microsoft Office
- ウイルス対策ソフトウェア
- アプリケーション / Windows ストアアプリ
- OSライセンス情報
- Windows更新プログラム
- 実行ファイル



ログ管理

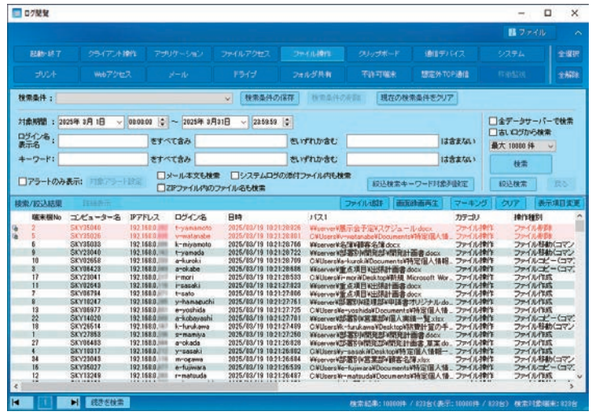
日々のPCの挙動をログに記録、情報漏洩リスクの早期発見などに活躍

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　標準搭載

ログの種別や期間などを指定して、重要データの取り扱いやアプリケーションの起動状況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

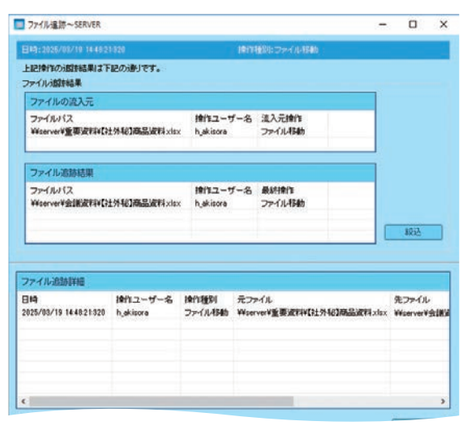
標準搭載　Ent/Pro/Tel/LT/500/ST/S1H/S3H

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　標準搭載　Ent/Pro/Tel/LT/500/ST/S1H/S3H

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

標準搭載　Ent/Pro/Tel/LT/500/ST/S1H/S3H

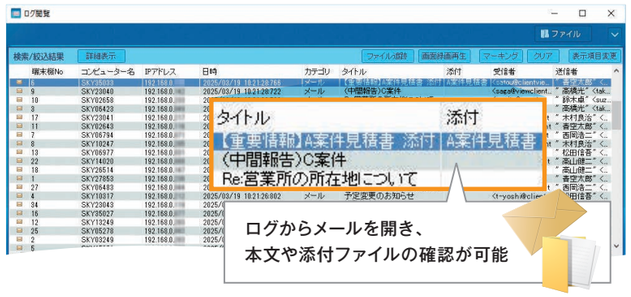
サーバーの共有ファイルへのアクセスログから、アクセス前後5分のクライアントPCでどんな操作が行われていたか、ファイルがどのように使われていたのかを確認できます。

メール経由での情報漏洩の防止に活用

送信メールログ

標準搭載 Ent/ST　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※1

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	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	送信メールの宛先(CC / BCCを含む)、件名、本文(一部)、添付ファイル名など。
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等の通信デバイスによる接続に関するログなど。通信状況を基に、社内か社外どちらで操作していたかの参考情報となるログも記録。
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。

※1 M1 Cloud Editionでは一部のログのみ対応しています。詳しくはSKYSEA Client View Webサイト(https://www.skyseaclientview.net/ver20/feature/)の機能一覧表をご覧ください。※2 実行コマンドや起動元アプリに関する情報の収集は、「ITセキュリティ対策強化」機能<標準搭載(Ent/Pro/Tel/S3H)、オプション(LT/500/ST)>が必要です。※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、Safariでの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、情報セキュリティ意識の向上に

業務と関係ないアプリケーションの使用など、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。

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

標準搭載

ファイルのWebアップロードやダウンロードなどの操作を、クライアントPC単位で制限できます。一方的に操作を禁止するだけでなく、メッセージで注意を促すなど、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※6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。

■ 主なアラート項目※7

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	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。
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※8【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※9	「Print Screen」キーによる画面キャプチャーを禁止します。

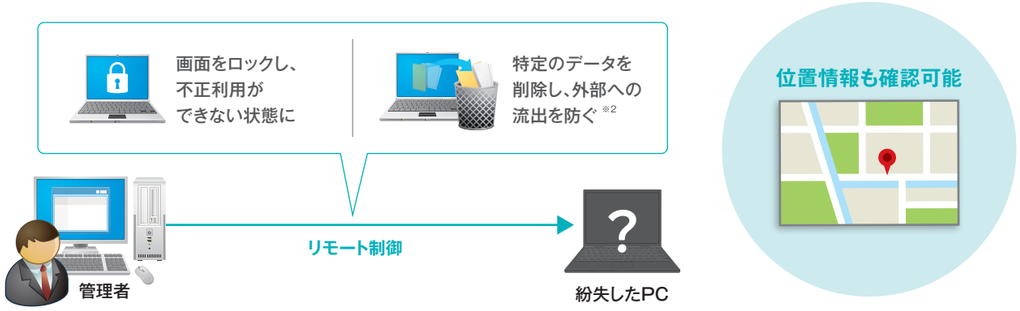
※6「画面操作録画」機能<オプション(Ent/Pro/Tel/LT/500/ST)>が必要です。※7 M1 Cloud Editionでは一部のアラート項目のみ対応しています。詳しくはSKYSEA Client View Webサイト(https://www.skyseaclientview.net/ver20/feature/)の機能一覧表をご覧ください。※8「送信メールログ」機能<標準搭載(Ent/ST)、オプション(Pro/Tel/LT/500)>が必要です。※9 Enterprise Editionとテレワーク Editionでのみご利用いただけます。

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

リモートワークなどで社外に持ち出したPCが紛失・盗難に遭った際、画面ロックやデータ削除をインターネット経由で実行でき、第三者の利用を防ぐことができます。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。

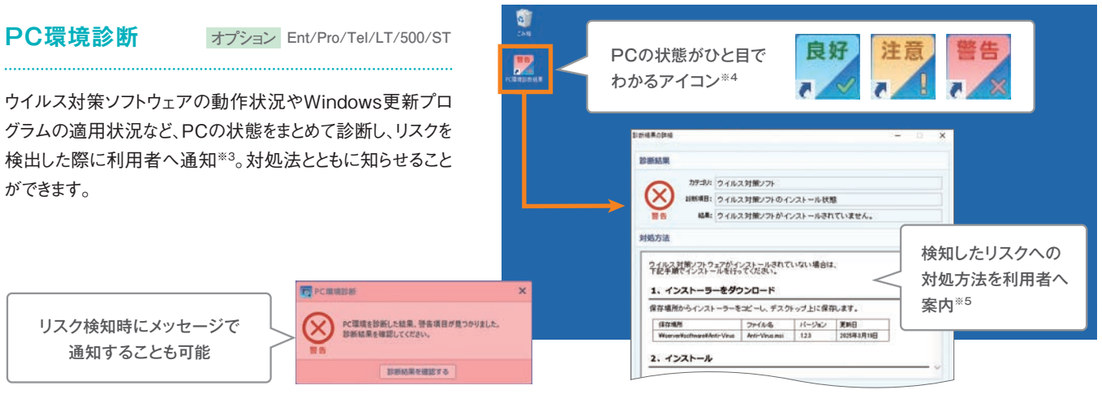


PCを自動診断、情報漏洩リスクを伴う状態を素早く通知

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利用者へ通知※3。対処法とともに知らせることができます。



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
	• ウイルス対策ソフトウェアの定義ファイル更新状態
	• Windows更新プログラムの適用状況 / 再起動待ち状況
	• Windowsへのログオンパスワード設定状態
	• 不許可アプリケーションのインストール状態
	• WSUSサーバーの設定状況　など

※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 管理者にもアラートで通知します。※4 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。※5 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。

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・盗難などによる情報漏洩リスクもはらんでいます。デバイスを1台ずつ適切に管理し、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。

「使用不可能」「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

標準搭載

デバイスやメディア1つずつに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」、それ以外は「使用不可能」にするなど、組織の運用に沿って管理できます※6。

□ デバイス種別制御

各デバイスのイラストをクリックするだけで、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。

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

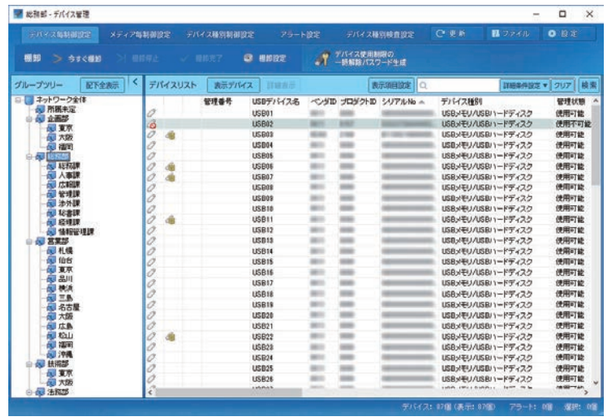
標準搭載 Ent/Pro/Tel/LT/500/ST/S1H/S3H

指定日時に棚卸依頼メッセージを各PCに送信。デバイスを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】

標準搭載 Ent/Pro/Tel/LT/500/ST/S1H/S3H

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。



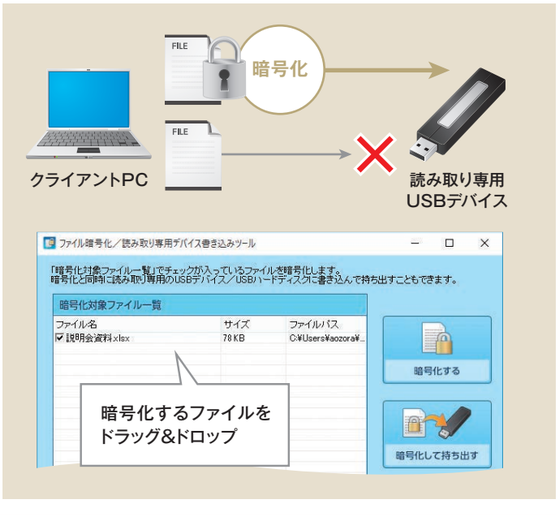
※6 M1 Cloud Editionではデバイスの管理のみ対応しています。

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

標準搭載 Ent/Pro/S3H　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。※1



□ 暗号化ファイルの復号を組織内に限定　特許取得

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）

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。

※1 CRYPTREC暗号リスト（電子政府推奨暗号リスト）」で定義されている暗号技術を採用しています。

ITセキュリティ対策強化

標準搭載 Ent/Pro/Tel/S3H　オプション LT/500/ST

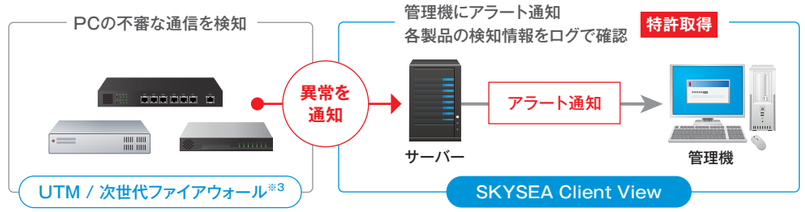
猛威を振るうサイバー攻撃に 多層防御による情報漏洩対策を

UTM※2などの製品と連携してマルウェア侵入を早期に把握したり、重要データを保存した共有フォルダへのアクセスを監視・制御するなど、サイバー攻撃対策を支援する各種機能をまとめて搭載。階層的な防御でリスクの最小化を行います。

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 / 次世代ファイアウォール連携

UTMや次世代ファイアウォールなど他社メーカー様の製品と連携。各製品がマルウェア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、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ことも可能です。



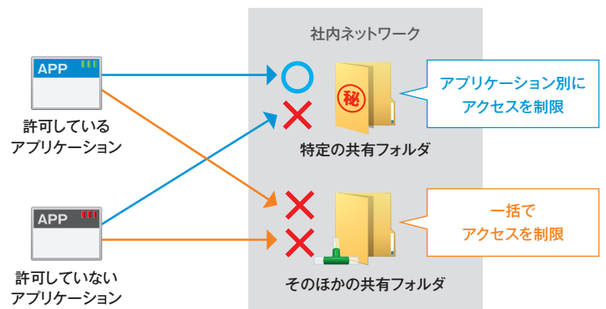
不審な通信の例

- 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、そのほかの共有フォルダへのアクセスを一括で制限できます。意図しないアプリケーションによる共有フォルダへのアクセスを抑止し、情報漏洩を防ぎます。



※2 UTM（Unified Threat Management）：統合脅威管理。※3 連携する各メーカー様の製品については、SKYSEA Client ViewのWebサイト（https://www.skyseaclientview.net/solution/）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セキュリティ対策強化」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。

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。

メンテナンス作業に欠かせない、PC間のデータ転送も可能

リモート操作

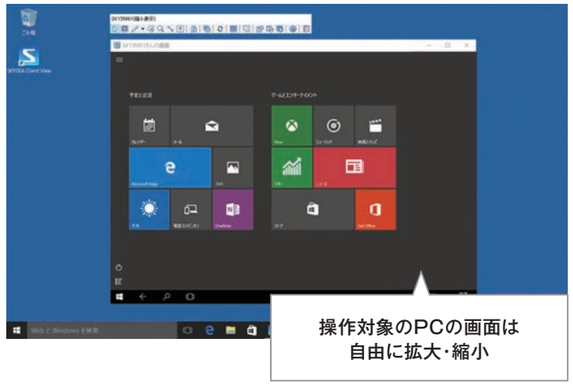
標準搭載 Ent/Pro/Tel/500/ST/S3H　オプション LT/M1/S1H

管理機のデスクトップにクライアントPCの画面を表示。リモート操作やファイル・テキスト・画像などの転送が行えます。

□ キーボード・マウス転送【関連特許取得】

標準搭載 Ent/Pro/Tel/500/ST/S3H　オプション LT/S1H

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。

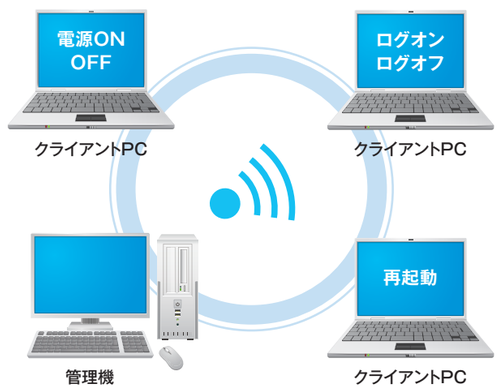


メンテナンス中の再起動や、電源切り忘れ時の対応に

電源制御

標準搭載 Ent/Pro/Tel/LT/500/ST/S1H/S3H

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、電源の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。



モバイル機器管理（MDM）　オプション

スマートフォン、タブレット端末のビジネス活用を支援

スマートフォンやタブレット端末※1を安全に運用管理するために、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。

資産情報を収集・管理、業務に不要な操作の制限も可能

資産管理

デバイス名や電話番号など、モバイル端末の各種資産情報を自動で収集。一覧画面で管理できます。

セキュリティ管理※3

組織での使用ルールに沿って、日々の業務で必要のない機能や操作などを制限できます。

紛失・盗難に備えて、リモートで画面ロック・データ削除

モバイル端末制御

モバイル端末に対して、リモートで画面ロックやデータ削除が行えます。紛失・盗難に遭った際の、第三者の不正利用や機密データの流出を防ぎます。

□ モバイル端末位置情報管理

端末の位置情報を地図上で確認できます。紛失してしまった際の捜索の手掛かりなどにお役立ていただけます。

※1 対応する機種情報は、SKYSEA Client View Webサイト（https://www.skyseaclientview.net/ver20/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、スマートフォン / タブレット端末では行えないものがあります。