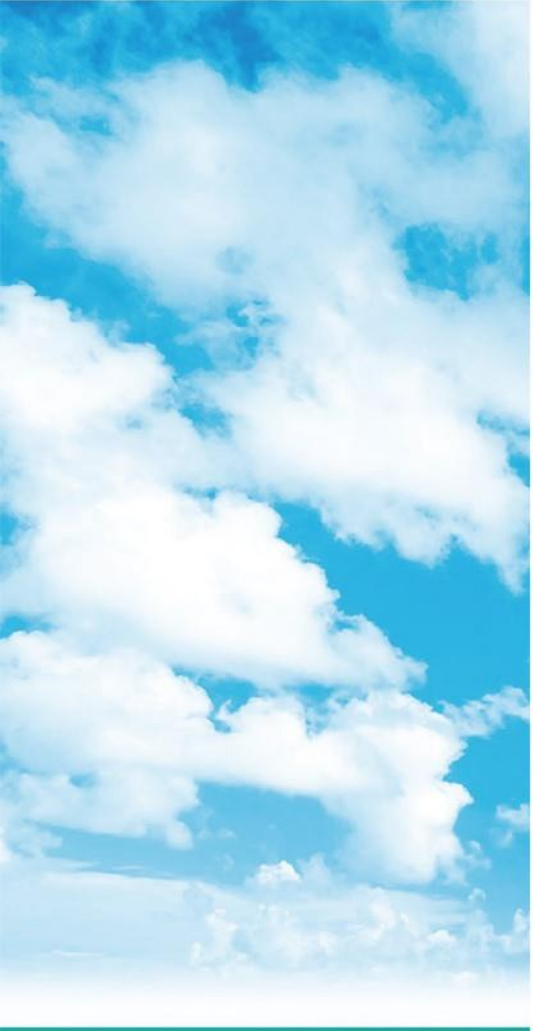


クライアント運用管理ソフトウェア

SKYSEA Client View

スカイシー クライアント ビュー

医療情報システムの安全管理に関するガイドラインから考える

システムを用いた情報セキュリティ対策

Sky

アジェンダ

1. 会社案内
2. システムを用いた院内の情報セキュリティ対策
   ~ 医療情報システムの安全管理に関するガイドラインを遵守するために ~

会社案内

Ｓｋｙ株式会社　会社概要

会社名	Ｓｋｙ株式会社		
設立	1985年3月2日	資本金	10億円
本社所在地	東京都港区港南2丁目18番1号 JR品川イーストビル9階	売上高	1,049.3億円（2024年3月期）
	大阪市淀川区宮原3丁目4番30号 ニッセイ新大阪ビル20階	従業員数	3,757名（2024年10月1日現在）
拠点所在地	札幌、仙台、大宮、東京、横浜、静岡、三島、 名古屋、大阪、神戸、広島、松山、福岡、沖縄	グループ 従業員数	3,824名（2024年10月1日現在）

事業内容

ICTソリューション事業
自社パッケージ商品開発 / 販売　システムインテグレーション

クライアント運用管理ソフトウェア	SKYSEA Client View
営業名刺管理	SKYPCE
学習活動端末支援Webシステム	SKYMENU Cloud
学習活動ソフトウェア	SkyMenu Class / SkyMenu Pro
シンクライアントシステム	SKYDIV Desktop Client
医療機関向け IT機器管理システム	SKYMEC IT Manager
システムインテグレーション	**提案から保守までシステム構築を一貫した体制で課題解決を支援**

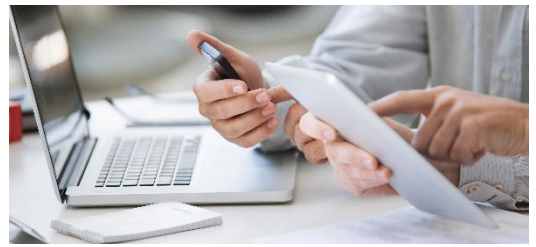
クライアント・システム開発事業
ソフトウェア開発・評価 / 検証

業務系システム開発

組込み / 制御 / アプリケーション開発

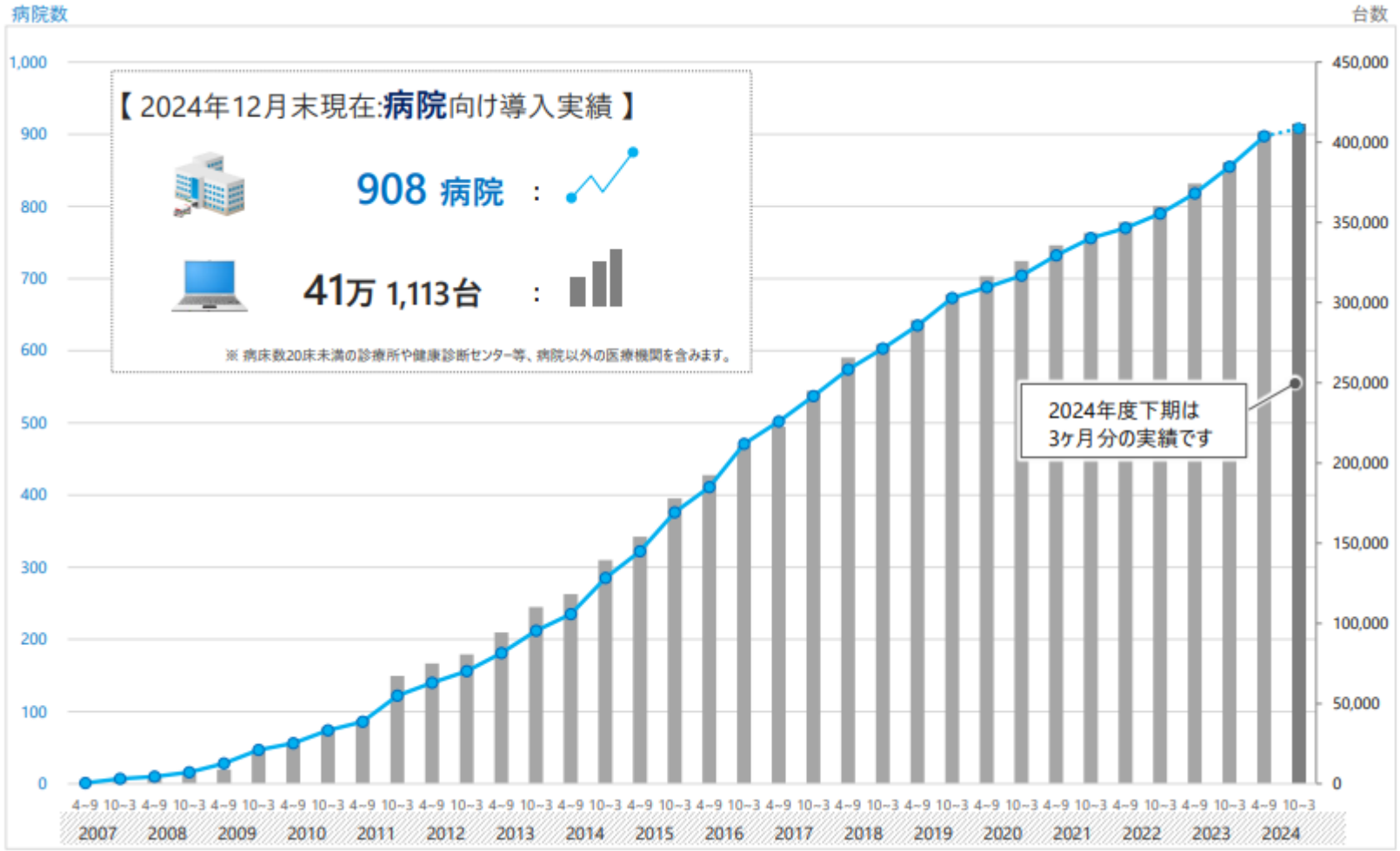
- カーエレクトロニクス開発
- モバイル開発
- デジタル複合機開発
- デジタルカメラ開発
- 社会インフラ
- 医療機器開発
- FA / その他開発

ソフトウェア評価 / 検証・サポート



医療機関向け：SKYSEA Client View導入実績

SKYSEA Client Viewは国内900を超える医療機関で導入されています。他業種を含む総ユーザー数は2万を超えており、様々な環境で安定して動作しているため、安心してご導入いただくことができます。



システムを用いた
院内の情報セキュリティ対策

~ 医療情報システムの安全管理に関するガイドラインを遵守するために ~

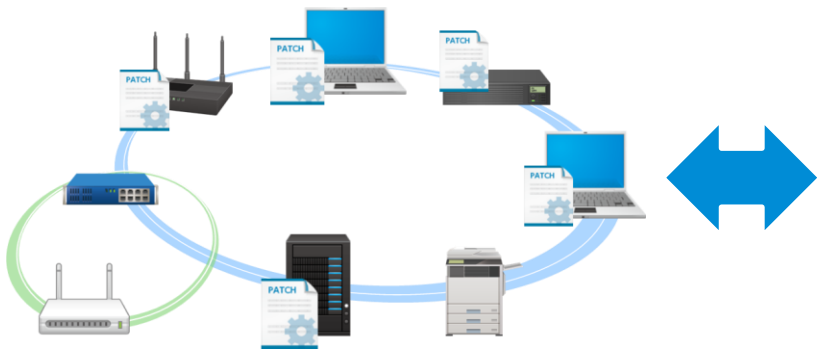
Sky株式会社

クライアント運用管理ソフトウェアSKYSEA Client Viewとは

IT運用管理と情報漏洩対策に役立つ各種機能と連携ソリューションを提供

ネットワーク経由でIT資産の情報や利用状況を自動で収集し、運用管理を行います。
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。

ネットワーク経由で自動収集・運用管理



運用管理と情報漏洩対策の機能を提供

2023年5月、医療情報システムの安全管理に関するガイドライン第6.0版の策定

2023年5月31日、厚生労働省よりガイドラインが改定され、別添、特集、Q&A等の参考資料と合わせて公表されました。第5.2版までと比較して、以下の変更が行われています。

第5.2版からの変更点

	①	②	③	④
目的	医療機関での **着実な実施**	オンライン資格確認の原則義務化に伴い、 **対象医療機関の拡大**に対応		**サイバー攻撃**の 多様化・巧妙化に対応
改定内容	対象者別の **4冊構成へ変更** 概説編 経営者 企画管理 システム運用	【新しい対象者へ】 **わかりやすい**よう、 特集や用語集などを提供  初めてでもわかる	【従来からの対象者へ】 第5.2版からの項目移行 対応表などを提供 従来の内容のどこが、どう変わったのかわかる 	・**ゼロトラスト思考**に即した考え方 ・**クラウドサービス**のリスクや対策 ・**新技術、新制度・規格**への対応

SKYSEA Client Viewは、多様化・巧妙化するサイバー攻撃対策を支援します

各対象者共通で前提となる項目：「概説編」より

情報セキュリティ対策は、守るべき情報資産を洗い出すことから始まります。

【概説編】　4.2 医療情報システムの安全管理に必要な要素

医療情報システムの安全管理において、情報セキュリティ対策は必須であり、医療機関等の特性を踏まえ、情報セキュリティの要素である「機密性（Confidentiality）」、「完全性（Integrity）」、「可用性（Availability）」のバランスを取りながら、リスクに対応することが求められる。

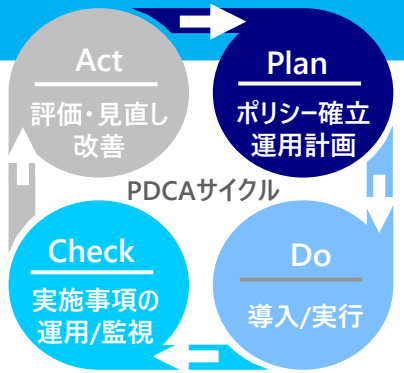
（中略）

これら3要素への対応を踏まえて講じた安全管理措置を的確かつ継続的に実施・改善するために、3要素を保護するための体系的な仕組みである**情報セキュリティマネジメントシステム（ISMS：Information Security Management System）を構築・運用することなどが求められる。**

※出典：「医療情報システムの安全管理に関するガイドライン 第6.0版 概説編（令和5年5月）」https://www.mhlw.go.jp/content/10808000/001102570.pdf

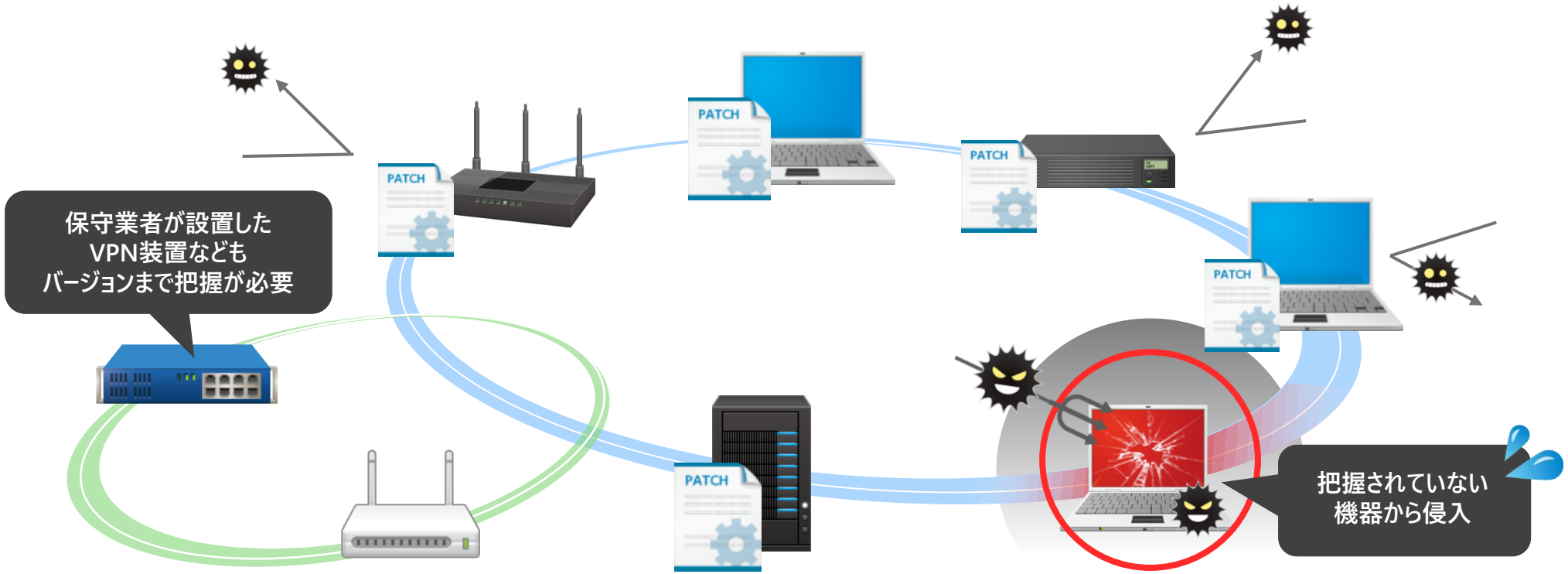
SKYSEA Client View では

情報資産の洗い出しや、変化のようすの
自動収集で、ISMSの構築・運用を支援します。



医療情報システムに接続する、全ての機器の把握が必要

ネットワークにつながっている全ての機器を漏れなく把握する必要があります。1台でも漏れがあると、侵入されたことに気付けずに感染が拡大する可能性があります。また、保守業者が設置したVPN装置、サブスクリプションで提供されるWi-Fi設備など、自身で設定を変更できない機器もバージョンまで把握する必要があります。



漏れなく・手作業で把握するのは、大きな負担がかかります。

ネットワーク経由で管理するシステムの利用が、効果的です

医療情報システムに用いる情報機器等の資産管理

【企画管理編】 9. 医療情報システムに用いる情報機器等の資産管理

【遵守事項】

② 医療機関等が管理する**情報機器等について、台帳管理等を行う**こと。台帳管理等の対象は、医療機関等内部の購入部署や購入形態に関わらず、**医療情報システムで利用する情報機器等全て**とすること。

③ 台帳管理されている医療情報システムに用いる**情報機器等の棚卸を定期的に行い、存在確認を行う**こと。また担当者と協働して、滅失状況などについても適宜確認すること。

④ 医療情報システムにおいて利用する情報機器等が、安全管理の観点から利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対して、**情報機器等における状況（ソフトウェアやファームウェアのアップデートの状況、脆弱性に関する対応状況等）を確認するよう指示**し、報告を受け、適宜必要な対応を行うこと。

9.1 情報機器等の台帳管理

医療情報システムで用いる情報機器等に関する安全性を確認するためには、医療情報システムで用いることを予定している情報機器等の所在が明らかになっているか、またそれらの情報機器等が使用できる状態なのか否か等を、適切に管理する必要がある。
そのため、企画管理者は、医療情報システムで用いる情報機器等について、台帳管理を行い、情報機器等が利用に適した状況にあることを確認できるようにしておく必要がある。
台帳で管理する内容としては、情報機器等の所在や利用者などが想定される。また、医療情報システムの適切な利用という観点では、**使用するソフトウェアやサービスのバージョン、ライセンスの状況なども管理対象として想定される。**

※出典：「医療情報システムの安全管理に関するガイドライン 第6.0版 企画管理編（令和5年5月）」https://www.mhlw.go.jp/content/10808000/001102575.pdf

SKYSEA Client View では

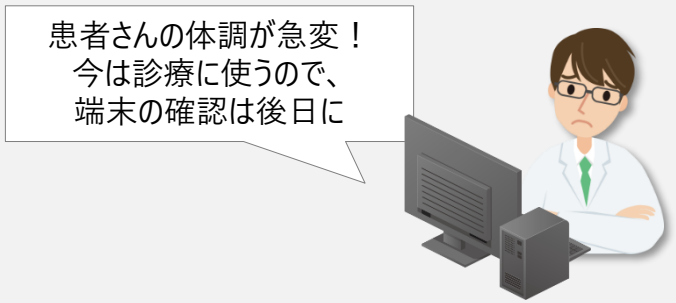
ネットワーク上の情報機器等の情報を台帳に収集し、定期的に自動更新します。

院内の情報機器を把握するには？

院内には、**病床数の約3倍のPC**があると言われており、IoT機器を含むとさらに大量の機器が存在します。
また、ファイルサーバーが無い病院の場合、**膨大な数の情報機器を使用している**ことが多いです。加えて、民間企業とは使用環境が異なるため、運用管理には大きな負担がかかります。

病棟のPCは24時間稼働。
PCが稼働しない時間はほぼない。

病棟のPCは24時間365日稼働しているので、
機器を確認するタイミングが難しい。



病院は敷地が広い。
また、入室に手間がかかる場所もある。

手術室は手術中でなくても、着替えて消毒・殺菌しないと
入室できません。

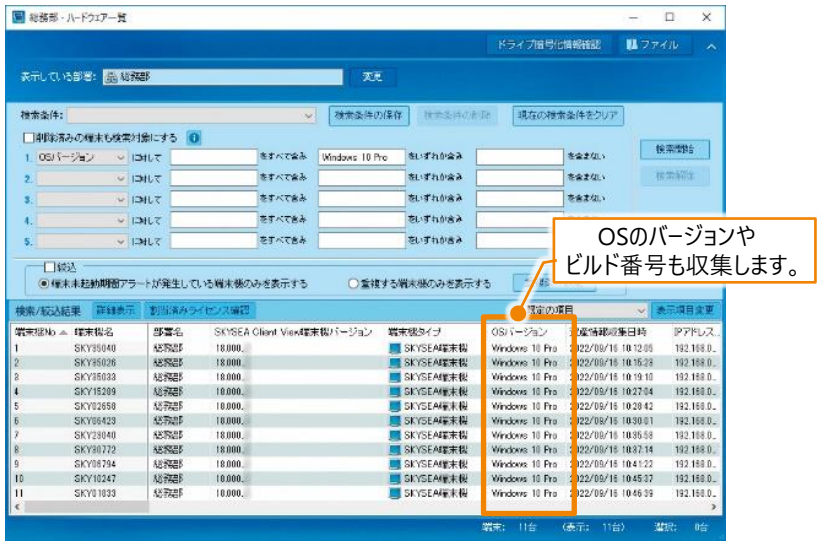
IT機器の保有状況を、常時手作業で管理するのは現実的ではありません。

ネットワーク上の最新のIT資産情報を把握

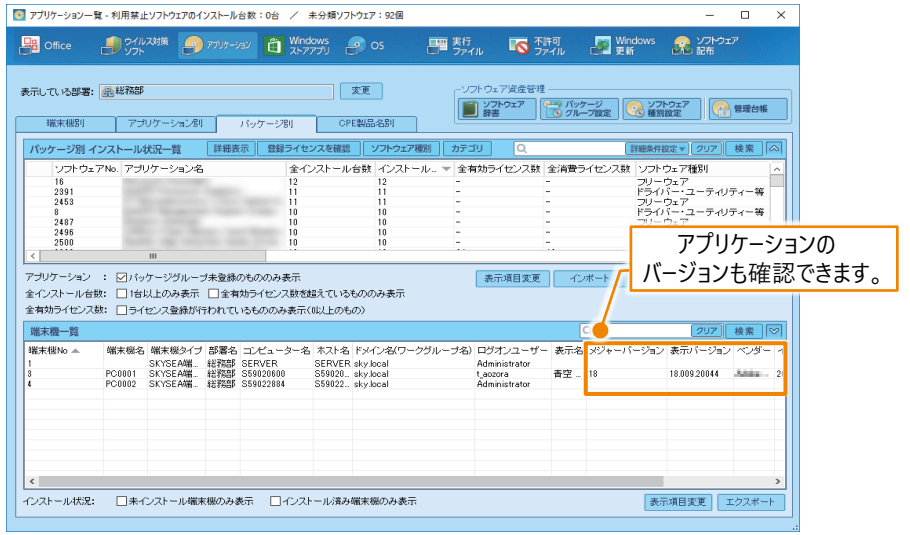
SKYSEA Client Viewは、ネットワーク上のIT機器のハードウェアやソフトウェア情報などを定期的に自動収集し、一覧で表示します。また、バージョン情報も収集するので、バージョンアップ状況を把握できます。

医療情報システムに接続されているクライアント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やソフトウェアの情報を一定時間ごとに自動収集し、台帳で管理できます。

ハードウェア一覧



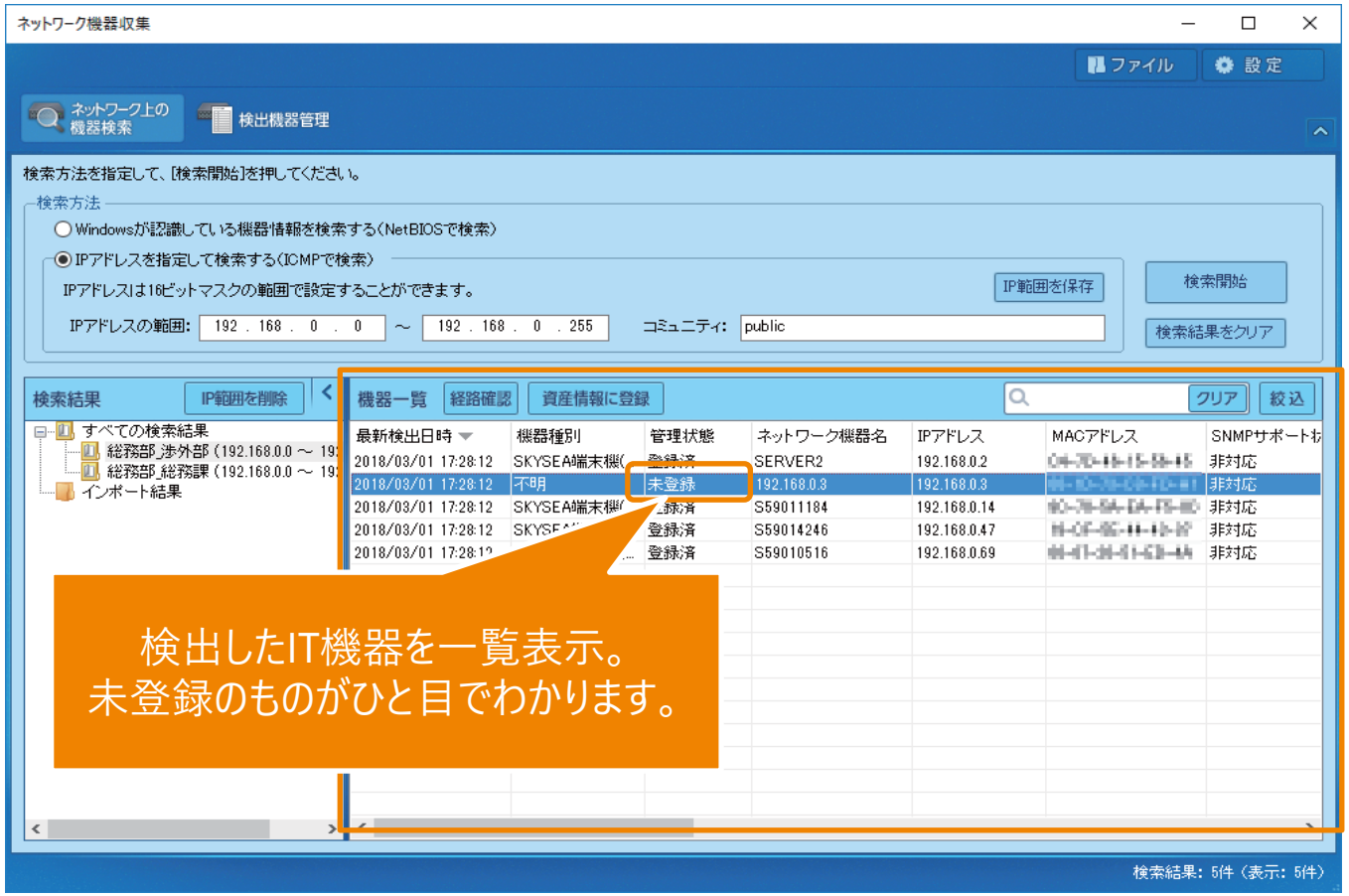
アプリケーション一覧



※ Microsoft Office for MacなどMac対象ソフトウェアでは一部取得できない項目があります。

IT機器の状況を確認

ネットワーク上のIT機器について、IPアドレス、製造元などを自動収集し、一覧で表示します。台帳に未登録の機器がひと目でわかり、存在確認も行えます。
また、製造元や機器名、型番等をもとに、脆弱性の公表時に対応の要否を検討できます。



脆弱性対策（利用機器・サービスに対する安全管理措置）

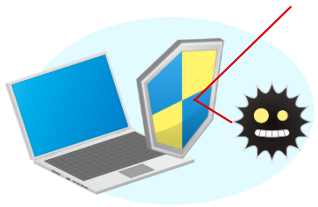
【システム運用編】8. 利用機器・サービスに対する安全管理措置

［遵守事項］
② **常時不正なソフトウェアの混入を防ぐ適切な措置**をとること。また、その対策の有効性・安全性の確認・維持（例えば**パターンファイルの更新の確認・維持**）を行うこと。

※出典：「医療情報システムの安全管理に関するガイドライン 第6.0版 システム運用編（令和5年5月）」https://www.mhlw.go.jp/content/10808000/001112044.pdf

SKYSEA Client View では

不正なソフトウェアの侵入口となる脆弱性対策として
ソフトウェアのアップデートや、ウイルス対策ソフトウェアのパターンファイル更新をご支援します。



「電子カルテはインターネットに繋がないので、マルウェアに感染しない」と思われがちですが、実際には多数の感染事例があります。また、毎日新しいマルウェアが発見され、パターンファイルは1日に複数回配布されています。病院のポリシーを確認しつつ、「常時」パターンファイルを更新できる仕組みが必要とされています。

インターネットに接続することのリスク

USBメモリなどのメディアは、最新のマルウェアに感染することはほとんどないため、パターンファイルの更新やウイルススキャンの回数は少なくても問題ありませんでした。ところが、VPN機器の脆弱性などからインターネットに接続されてしまうことによる、マルウェア感染が相次いでいます。

記録媒体：既存のマルウェア

外部からの紹介状に付属していた画像などのDVDにマルウェアが潜んでいて、感染してしまう。

ファイルサーバー代わりに利用。他院と研究用のデータを受け渡しして感染してしまう。

インターネット：新規のマルウェア

インターネットに接続していると、**最新のマルウェアに感染する可能性が高まります。**
未知のマルウェアに感染するリスクを前提とした脆弱性対策が、必要になります。

脆弱性対策には常にソフトウェアを最新版にアップデートすることが有効

脆弱性とは「プログラムの不具合や設計上のミスなどが原因となりOSやソフトウェアに発生したセキュリティ上の弱点」のことです。脆弱性を放置していると不正アクセスに利用されたり、マルウェアに感染する危険性があります。

公開されているNデイ脆弱性を
利用すれば効率的！

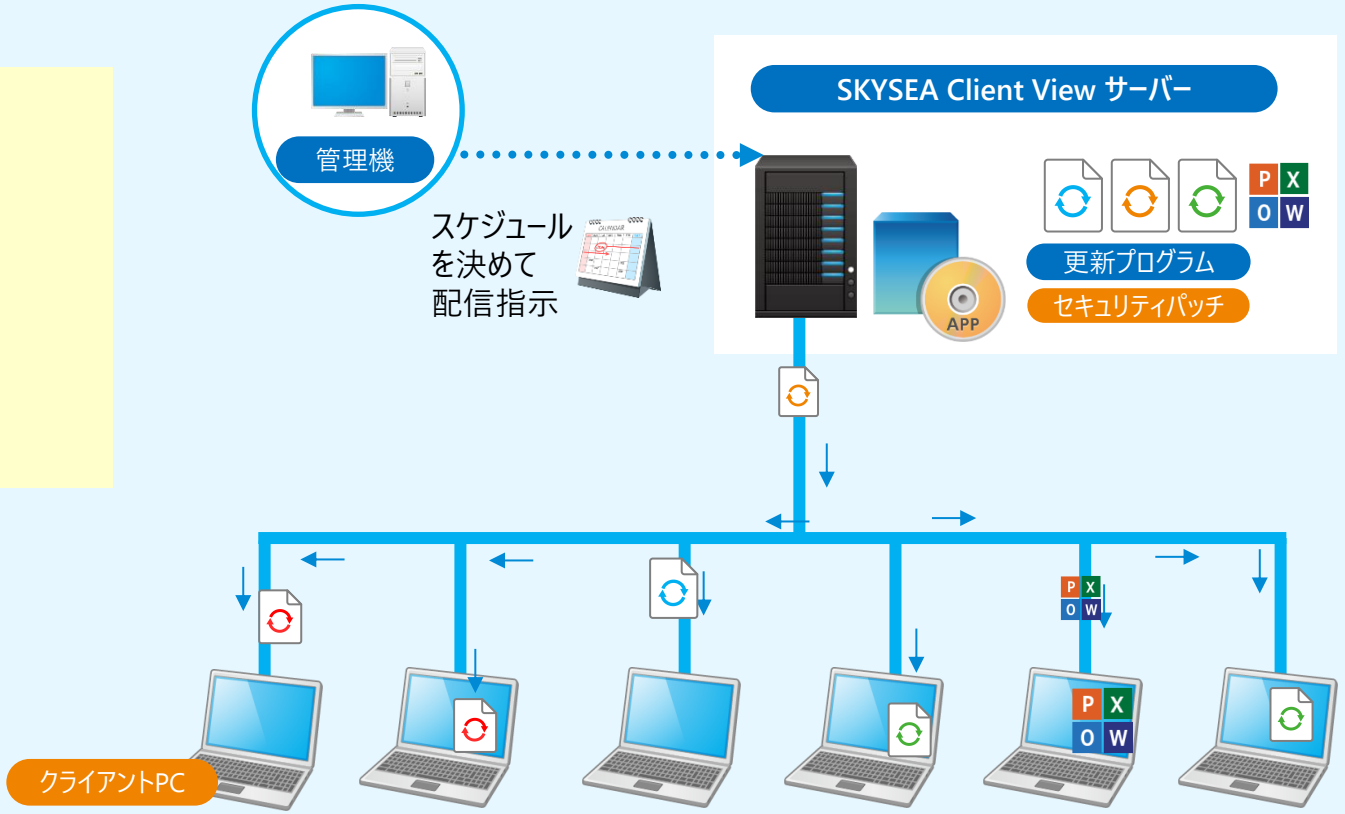
脆弱性を放置すること＝攻撃者の思うつぼ

公開されたセキュリティ更新プログラムはなるべく早く適用することが重要。

PCにWindows更新プログラムやセキュリティ更新プログラムを配布

脆弱性のあるアプリケーションを見つけたら、それらをインストールしているPCに対してセキュリティ更新プログラムや機能更新プログラムを配布。スケジュールを設定したり、指定したPCに対してセキュリティパッチを配布できます。

・セキュリティ更新プログラムの配布
・ソフトウェアインストール
・機能更新プログラムの配布
・WSUSと連携した配信
・Microsoft 365 Officeアプリアップデート



MicrosoftがWSUSの廃止を発表

引用：Microsoft公式ブログ（2024年9月20日付けのブログ「Windows Server Update Services (WSUS) deprecation」）
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-server-update-services-wsus-deprecation/ba-p/4250436

Microsoftは、クラウドを活用したWindows管理の一環として、Windows Server Update Services（WSUS）の廃止を発表しました。今後は新機能の開発を行わないものの、現行機能は維持され、更新プログラムの提供や既存コンテンツのサポートは継続されます。

Windows Server Update Services (WSUS) deprecation

By Nir Froimovici

Published Sep 20 2024 11:00 AM 57.3K Views

As part of our vision for simplified Windows management from the cloud, Microsoft has announced deprecation of Windows Server Update Services (WSUS). Specifically, this means that we are no longer investing in new capabilities, nor are we accepting new feature requests for WSUS. However, we are preserving current functionality and will continue to publish updates through the WSUS channel. We will also support any content already published through the WSUS channel.

Deprecation is the stage of the product lifecycle when a feature or service is no longer in active development. WSUS deprecation does not impact existing capabilities or support for Microsoft Configuration Manager. While the WSUS role remains available in Windows Server 2025, we recommend organizations transition to cloud tools, including Windows Autopatch and Microsoft Intune for client update management and Azure Update Manager

今後は新機能の開発を停止

当面は...

- 現在の機能は維持
- 更新プログラムは引き続き提供
- 公開されているコンテンツのサポート継続

今後は...

- クライアント更新管理用
  - Windows Autopatch
  - Microsoft Intune
- サーバー更新管理用
  - Azure Update Manager

➡ クラウドツールへの移行を推奨

更新プログラムをすぐに配布できるかを、予め分類

できるだけ最新の更新プログラムを適用することを推奨しますが、更新プログラムに電子カルテやシステムなどが対応していない場合、適用すると使用できなくなる可能性もあります。ベンダーに確認して、予め更新プログラムを適用できる端末 / できない端末などを把握して、分類しておくとスムーズに対応が行えます。

❶ システムごとに、利用端末のリストを用意

更新プログラムを適用できる端末 / できない端末を把握し、適用するための段取りをします。

- どのネットワークのどの端末が適用されていないのか。
- 適用できない理由は何なのか。
  (電子カルテ・医療用ソフトウェアが対応していない、ネットワークに接続されていない など)

❷ すぐにバージョンアップできない端末は、必要最低限の機能に限定

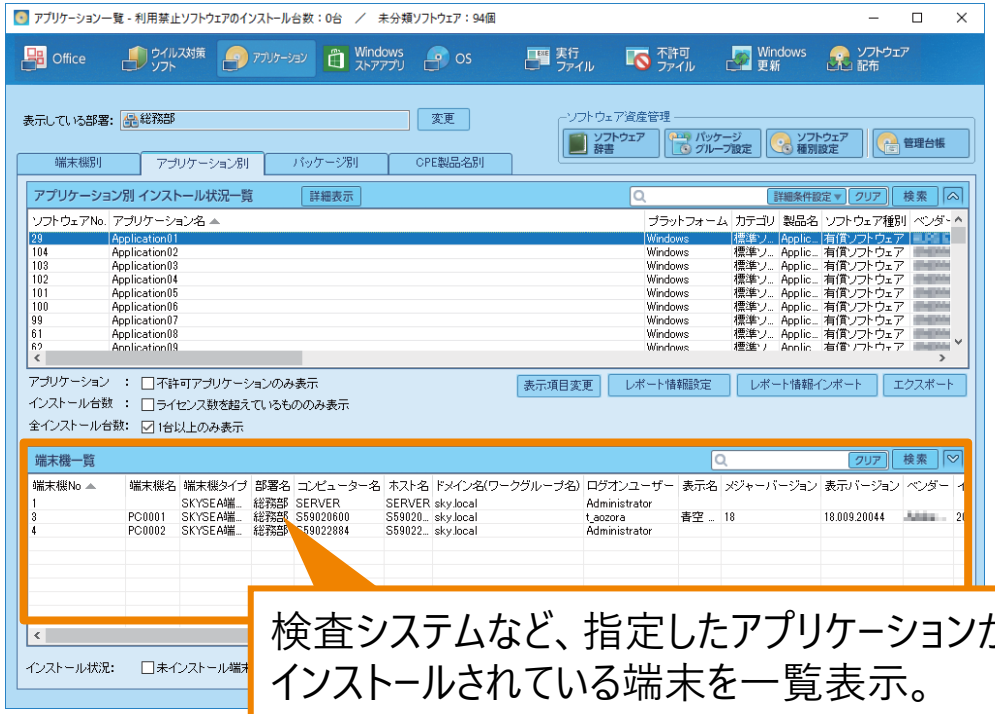
- 特定のサーバー以外は接続できないように、ポートやIPアドレスを制限する。
- USBメモリなどのデータ書き込みを禁止する。
- 使っていないアプリケーションを洗い出してアンインストールする。　　など

すぐ適用できない場合の代替策を用意し、管理することが重要です。

更新プログラムをすぐに配布できないPCを管理

特にHIS系では、診療に関わるシステムが最新のOS等に対応していないがために、アップデートできないPCがあります。
このようなPCを、SKYSEA Client Viewで管理できます。

▼インストール状況一覧（アプリケーション別）



検査システムなど、指定したアプリケーションがインストールされている端末を一覧表示。

任意項目に、アップデートできない理由を記載しておくことで、対策を検討できます！

情報システム管理者

アップデートできない場合の対策例

- スタンドアロン環境で運用する。
- UTMなどで、ネットワークから分離し、特定サーバーとの通信のみを許可する。

など

病院のHIS系で動作させるソフトウェアは、インターネットに接続しないことを前提としており、OSの更新プログラムの適用を想定した運用・開発体制になっていない場合があります。

ネットワークに関する安全管理措置 への対策

13. ネットワークに関する安全管理措置

13.2 不正な通信の検知や遮断、監視

外部からのサイバー攻撃の高度化・多様化に鑑みると、境界防御の対策を行っていたとしても、不正ソフトウェア等の攻撃や侵入があることから、このような場合を想定して、内部脅威監視や**EDRなどの措置を講じることも、有効な対策として挙げられる**。

※出典：「医療情報システムの安全管理に関するガイドライン 第6.0版 システム運用編（令和5年5月）」https://www.mhlw.go.jp/content/10808000/001112044.pdf

SKYSEA Client View では

インターネットに接続せずに使用でき、「EDR」と「振る舞い検知」の両方の特性を備えた「EDRプラスパック」をご提供しています。

特長① 発症する前に防御し、感染源を調査可能

＜オプション（ Ent / Pro / Tel / LT / 500cl Pack / ST ）＞

一般的なEDR製品は、情報の持ち出しなどを検知して対応を始めます。一方、SKYSEA Client ViewのEDRプラスパックは、不正プログラム特有のふるまいから検知し、防御します。

既知のマルウェアを検知

AV Antivirus。
EPP（Endpoint Protection Platform）とも呼ばれる

パターンファイルによるマルウェア検知

イメージ

未知のマルウェアも検知

NGAV Next Generation Antivirus

マルウェア特有の動作を基に検知

イメージ

端末の動きをもとに検知

一般的な **EDR** Endpoint Detection and Response

エンドポイントの動きを基に検知

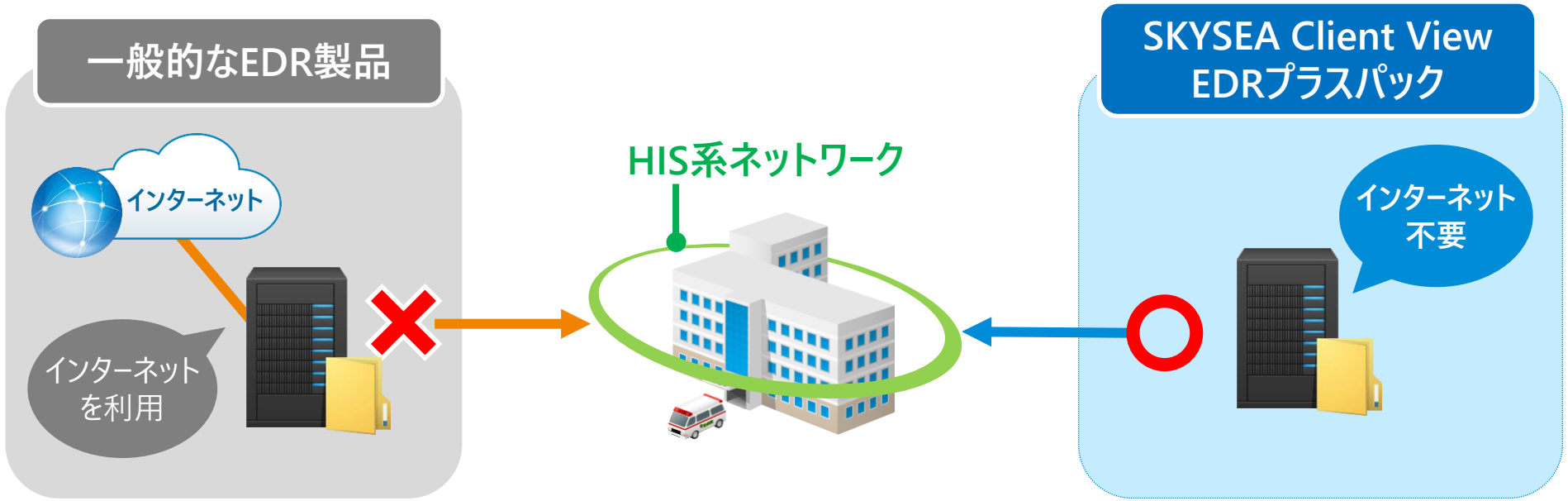
イメージ

SKYSEA Client View EDRプラスパックは
「ふるまい検知」で、発症前の防御を行いつつ、再感染の防止も支援します。

特長② HIS系でご利用可能

＜オプション（ Ent / Pro / Tel / LT / 500cl Pack / ST ）＞

一般的なEDR製品はインターネット接続が必要なため、HIS系ネットワークでのご利用が難しい場合が多いです。
SKYSEA Client ViewのEDRプラスパックでは、オンプレミス環境で運用できるのでインターネット接続が不要なため、
HIS系ネットワークでもご利用が可能です。



SKYSEA Client View EDRプラスパックは
HIS系でのご利用に最適なEDR機能をご提供いたします

ログの収集・管理（安全管理に必要な対策）

【経営管理編】 4.2 必要な措置

発見的措置は、仮にリスクとして想定する事象が発生しても、速やかに事象の発生を検知することで、具体的なリスクの発生を防止したり、被害拡大を防止したりするための措置であり、例えば**医療情報に対するアクセス状況をシステム操作ログ等を用いて監査**し、**不審なアクセスがないかどうかを確認の上**、必要に応じて措置を講じることなどが挙げられる。

※出典：「医療情報システムの安全管理に関するガイドライン 第6.0版 経営管理編（令和5年5月）」https://www.mhlw.go.jp/content/10808000/001102573.pdf

SKYSEA Client View では

ファイルサーバーやファイルごとに、アクセスの状況を記録し、分析することができます。

Active Directoryによるユーザー認証を行う環境の場合、誰がアクセスしたのかをログから把握することができるため、担当外の利用者による不審なアクセスを見分けやすくなります。

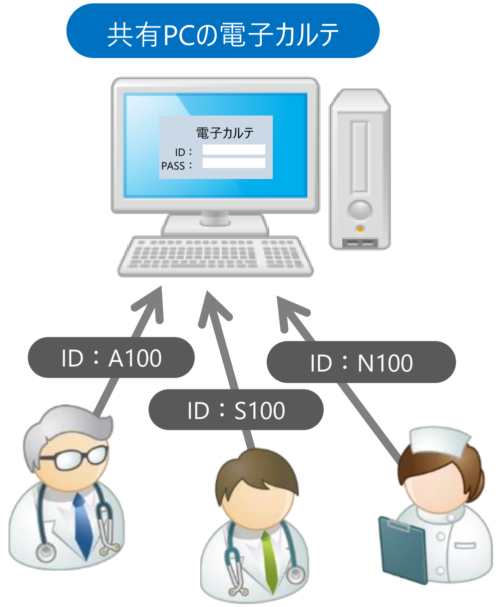
電子カルテシステム連携

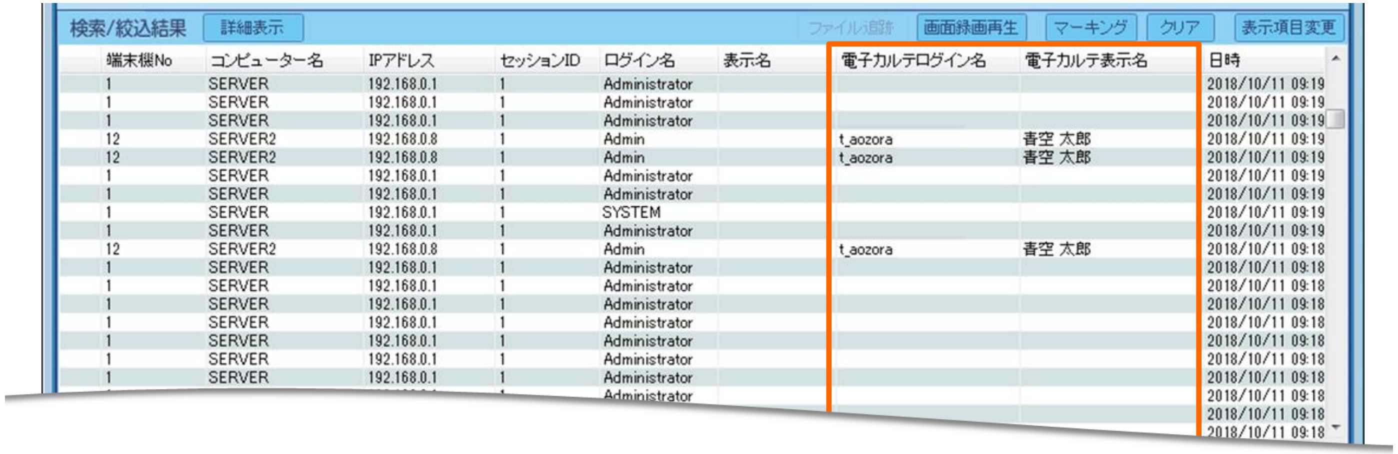
共有PCを使用する場合、共通のアカウントでログインすることが多いので、誰がPCを操作したのかがわからなくなります。PC操作ログ情報に電子カルテのユーザー情報を記録することで、共有PCでも利用者を特定でき、ユーザーごとに操作の確認ができます。また、電子カルテユーザーごとにUSBメモリの制限を設定したり、トラブル発生時には電子カルテ上からヘルプデスク依頼ができます。

※病院では、Windowsアカウントのログインなしでも電源を入れるとPCが使用状態になることが多く、Windowsからは、実質的に利用者を特定することはできません。

電子カルテユーザーの各種PC操作をログで確認

操作ログに電子カルテのログインID情報が含まれるため、共有PCでも利用者を特定でき、利用者ごとの操作確認がおこなえます。





端末機No	コンピューター名	IPアドレス	セッションID	ログイン名	表示名	電子カルテログイン名	電子カルテ表示名	日時
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:19
12	SERVER2	192.168.0.8	1	Admin		t_aozora	青空 太郎	2018/10/11 09:19
12	SERVER2	192.168.0.8	1	Admin		t_aozora	青空 太郎	2018/10/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:19
1	SERVER	192.168.0.1	1	SYSTEM				2018/10/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:19
12	SERVER2	192.168.0.8	1	Admin		t_aozora	青空 太郎	2018/10/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/10/11 09:18
				Administrator				2018/10/11 09:18
								2018/10/11 09:18
								2018/10/11 09:18

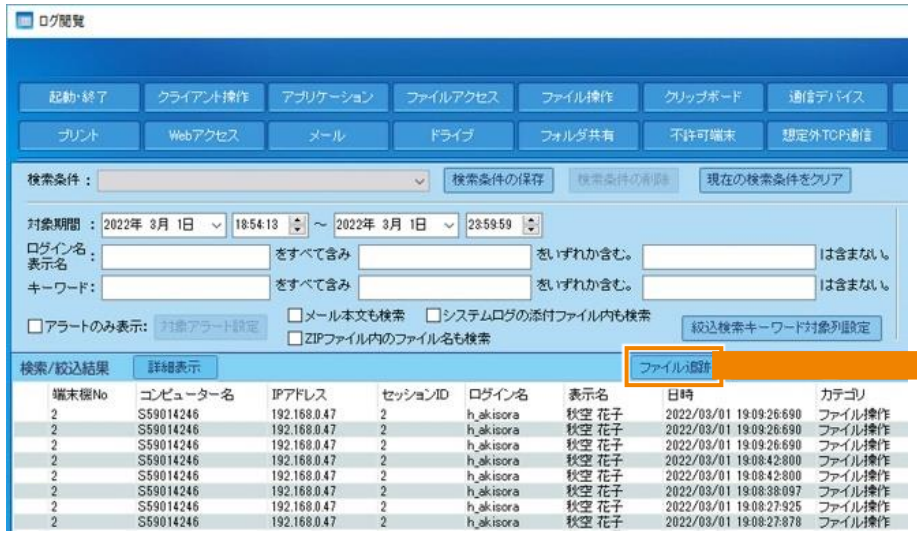
※ 電子カルテシステム連携機能はオプションです。＜オプション（ Ent / Pro / Tel / LT / 500cl Pack / ST ）＞
※連携可能な電子カルテシステムについては、SKYSEA Client View「協業・連携ソリューションのご案内」をご確認ください。＜ https://www.skyseaclientview.net/solution/ ＞

ファイル操作のログを追跡

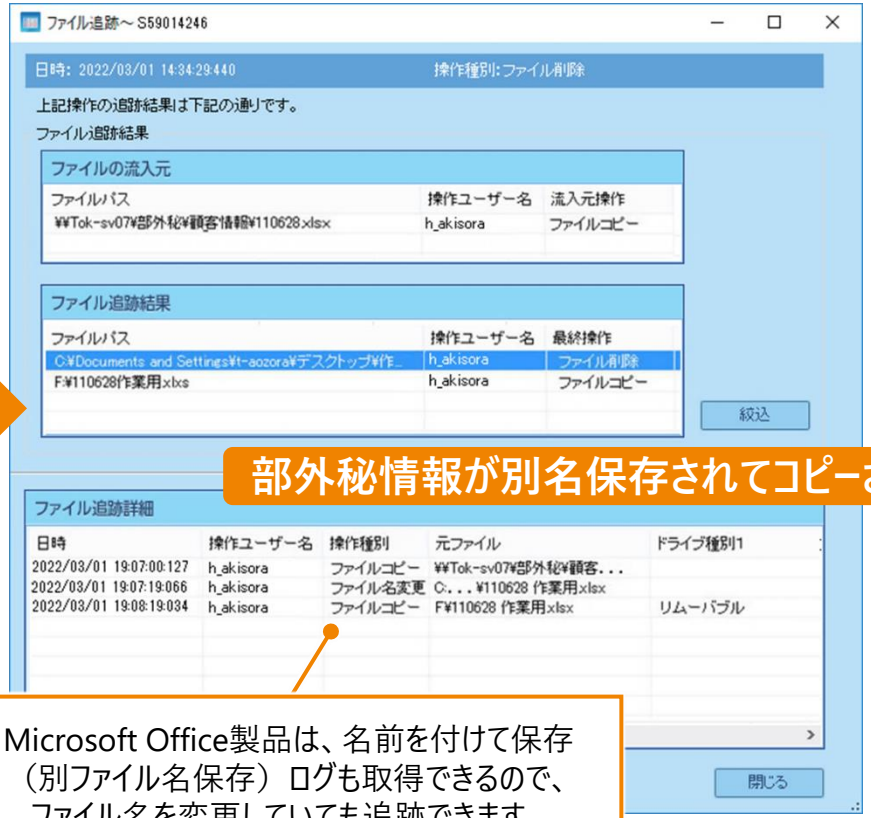
ファイル追跡

収集されたファイル操作ログから、1つのファイルに対して、どのような操作（コピー、ファイル名変更、新規作成、削除など）が行われたかを抽出することが可能です。状況の早期把握に役立ちます。

※Active Directoryによるユーザー認証を行う環境の場合、誰がアクセスしたのかをログから把握することができるため、担当外の利用者による不審なアクセスを見分けやすくなります。



指定ファイルの流入から流出までの操作ログを追跡します



部外秘情報が別名保存されてコピーされている！

Microsoft Office製品は、名前を付けて保存（別ファイル名保存）ログも取得できるので、ファイル名を変更していても追跡できます。

ログ解析レポート

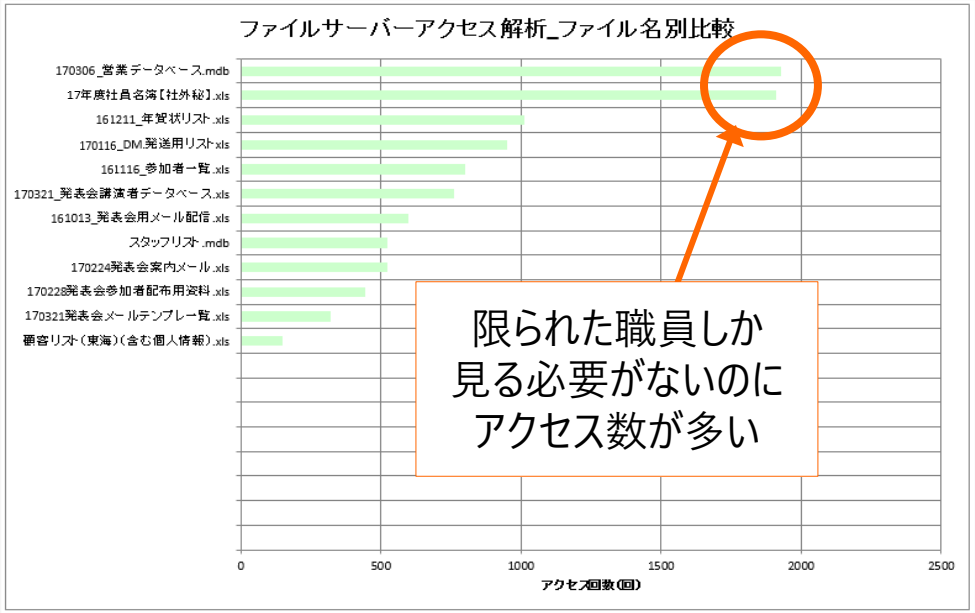
収集したログや資産情報をグラフ化する機能です。グラフで傾向を把握し、ログ検索やファイル追跡機能、画面録画※再生などを活用することで、規程に反した機密データの取り扱いが行われているなどといった問題点を特定し、今後の対策を立てることができます。
また、集計したデータはMicrosoft Excel形式のファイルとして出力できるので、集計データを使った報告書の作成にも活用できます。

※画面操作録画機能はオプションです。＜オプション（Ent / Pro / Tel / LT / 500cl Pack / ST）＞

ファイルサーバーアクセス解析

■ ファイル名別比較グラフ

ファイルアクセスのファイル名別比較グラフです。あらかじめ設定したフォルダ、もしくはファイルのアクセス状況を表示します。



利用例

不必要なファイルアクセスのチェック

例えば、患者ごとにファイルを作成している場合、特定の患者の情報だけ不自然にアクセス数が多い、といった状況を把握することができます。
不自然に多い場合は、ログを確認します。

SKYSEA Client Viewでご支援できる、その他の項目例

医療情報システムの安全管理に関するガイドライン第6.0版で求められる対応項目は多岐にわたります。限られた人員でも対応できるよう、さまざまな機能やサービスをご提供しています。

ガイドラインの項目		SKYSEA Client Viewの機能・サービス
経営管理	3.2.2. 情報セキュリティ対策を踏まえた訓練・教育	セキュリティ研修
企画管理	8. 情報管理（管理、持ち出し、破棄等）	デバイス管理（利用制限）、 不許可端末検知/遮断、ファイルアップロード制限
	9. 医療情報システムに用いる情報機器等の資産管理	持込端末管理
システム運用	7. 情報管理（管理・持出し・破棄等）	BitLocker管理、ウイルス対策ソフトウェア更新状況、インストール制限、USBデバイス棚卸、取り扱いファイル暗号化、MDM、紛失端末制御
	8. 利用機器・サービスに対する安全管理措置	接続時のウイルスチェック
	17. 証跡のレビュー・システム監査	電子カルテログイン情報連携、ログ収集・管理、画面操作録画
	18. 外部からの攻撃に対する安全管理措置	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、特定フォルダアクセスアラート設定

多様な機能とサービスでご支援いたします。ぜひご相談ください。

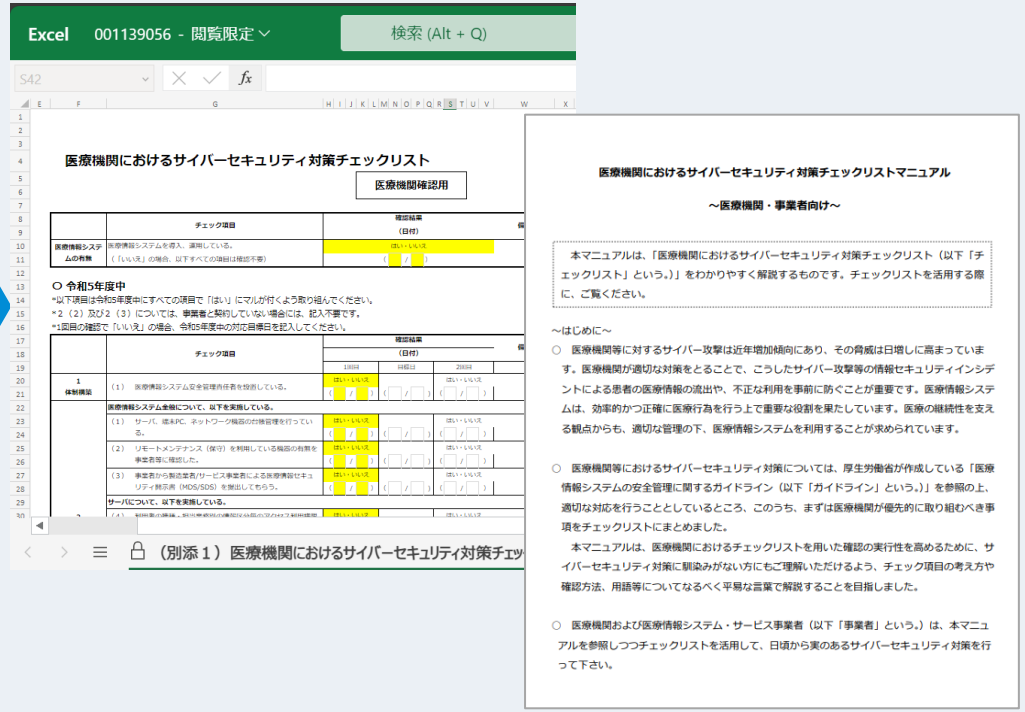
安全管理ガイドラインのうち、「優先的に取り組むべき事項」

医療機関のIT環境が多様になったため、「医療情報システムの安全管理に関するガイドライン第6.0版」では、「最低限」が示されていません。代わりに、医療機関が優先的に取り組むべき18項目を示したものがチェックリストです。

医療情報システムの安全管理に関する**ガイドライン**第6.0版

医療機関が
優先的に取り組む
べき18項目

医療機関におけるサイバーセキュリティ対策**チェックリスト**



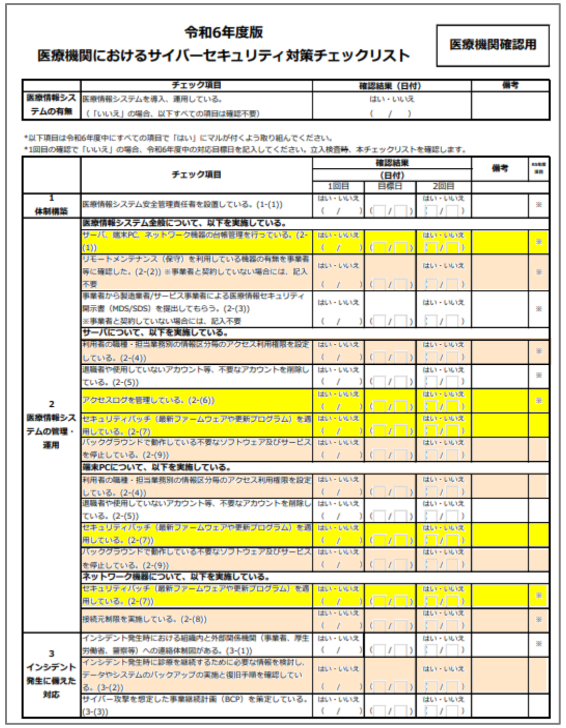
2023年6月より、医療法第25条の立入検査で、チェックリストへの対応が求められています

医療法第25条の立入検査で「チェックリストへの取り組み状況」を確認

令和5年6月より「医療法に基づく立入検査では、病院、診療所および助産所においてサイバーセキュリティ確保のために必要な取組を行っているかを確認すること」として、チェックリストへの取り組みが求められるようになりました。

▼ 医療機関におけるサイバーセキュリティ対策チェックリスト

※出典：厚生労働省Webサイト https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html



令和6年度版

医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。（「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ (/)	

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

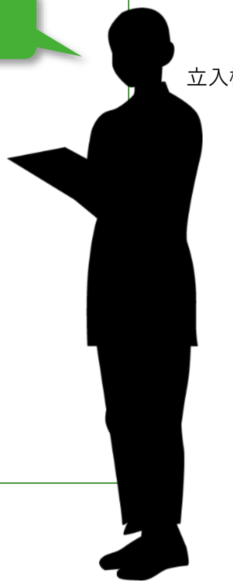
	チェック項目	確認結果（日付） 1回目	目標日	2回目	備考	[illegible]
1 体制構築	医療情報システム安全管理責任者を設置している。(1-(1))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**					
	サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-(1))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-(2)) ※事業者と契約していない場合には、記入不要	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。(2-(3)) ※事業者と契約していない場合には、記入不要	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	サーバについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	アクセスログを管理している。(2-(6))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7)	はい・いいえ (/)	(/)	はい・いいえ (/)		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	端末PCについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	ネットワーク機器について、以下を実施している。					
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	接続元制限を実施している。(2-(8))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
3 インシデント発生に備えた対応	インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。(3-(1))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-(2))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-(3))	はい・いいえ (/)	(/)	はい・いいえ (/)		

令和６年度中にすべての項目で「はい」にマルをつけてください。

【全般】（1）サーバ、端末PC、ネットワーク機器の台帳管理を行っている。

【サーバ】（6）アクセスログを管理している。
【サーバ】（7）セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
【サーバ】（9）バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。

【端末PC】（7）セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
【端末PC】（9）バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。



凡例： SKYSEA Client Viewでご支援可能　SKYSEA Client Viewで一部ご支援

SKYSEA Client Viewは、手作業では負担の大きい、チェックリストへの取り組みをご支援いたします

最後に

医療機関へのランサムウェア被害が頻繁に報道されています。

まずは基本的な対策を徹底することで、攻撃にかかる手間を増やし、攻撃を諦めさせることが大切です。そのためには、システムによる対応が有効です。

IT機器の見える化と
セキュリティ対策に
SKYSEA Client View

Ｓｋｙ株式会社では、お客様のお声やIT環境の変化をもとにバージョンアップを重ねつつ、
最新のサイバー攻撃に対応するための機能やサービスをご提供してまいります。

SKYSEA Client View は“企業・団体”のお客様向け商品です

SKYSEA Client View

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。

- 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。

東京 03-5860-2622　大阪 06-4807-6382

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 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