―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.13.2

お客様の声を取り入れ、毎年バージョンアップ

いま求められるセキュリティ対策とは？

～SKYSEA Client Viewを活用した資産管理、情報漏えい対策～

Sky株式会社

もくじ

会社案内

Ｓｋｙ株式会社　会社概要

東京本社 大阪本社	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　15階 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
設立	1985年3月2日
資本金	4億5千万円
売上高	542.7億円（2018年3月期）
従業員数	2,484名（2018年9月末現在）
グループ 従業員数	2,602名（2018年9月末現在）
拠点所在地	札幌、仙台、東京、横浜、三島、名古屋、 大阪、神戸、広島、松山、福岡、沖縄
グループ会社	株式会社エッグ

事業内容

● パッケージ商品の開発・販売

SKYSEA Client View

スカイメニュープロ SkyMenu Pro

SKYMEC IT Manager

スカイメニュークラス SkyMenu Class

● 各種ソフトウェアの設計・開発・評価

業務系システム

カーエレクトロニクス

モバイル

デジタル複合機

デジタルカメラ

エネルギー

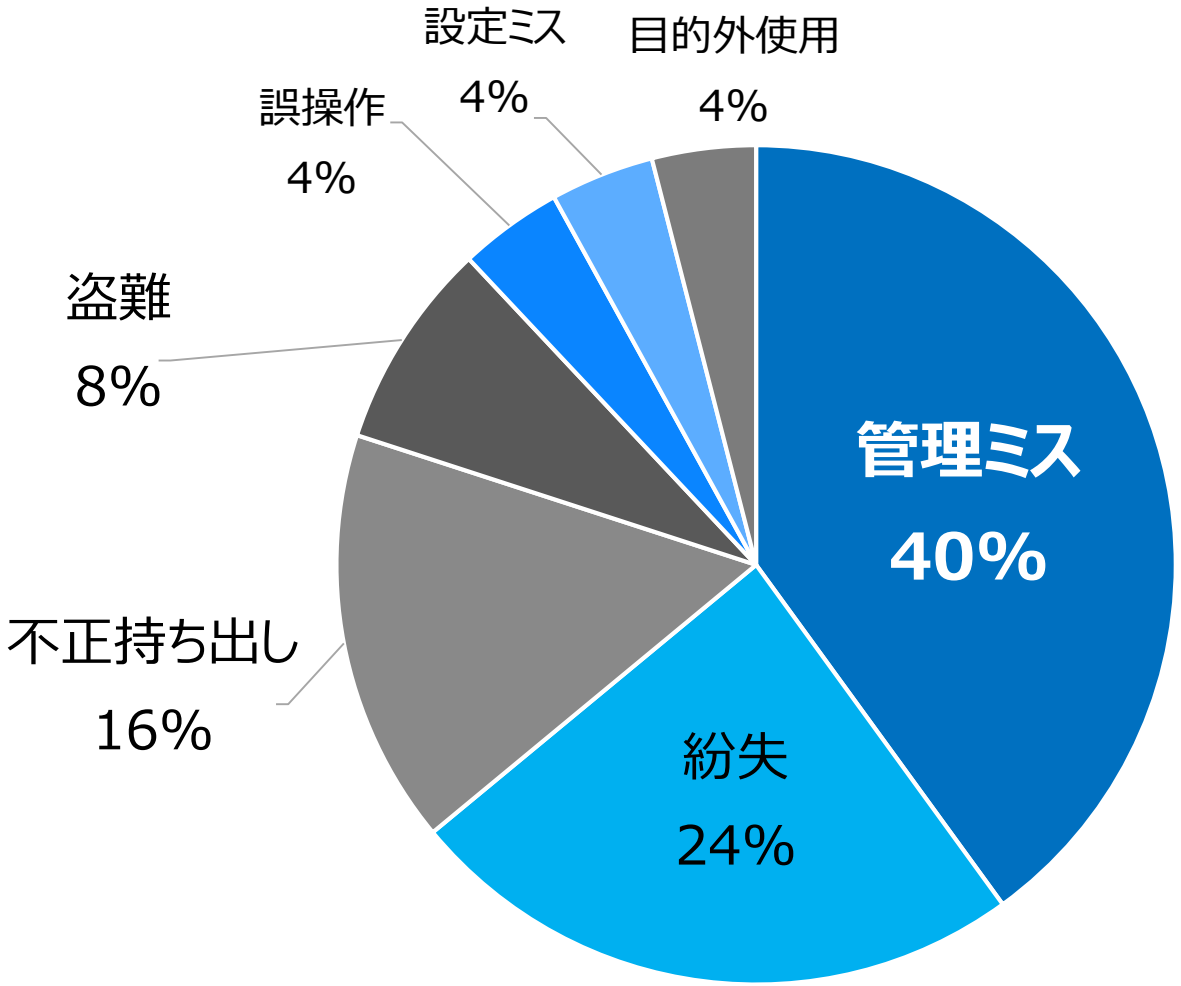
医療機器・その他

ソフトウェア評価/検証

医療機関での
情報漏洩事故とサイバー攻撃

医療機関での個人情報漏洩事故は？

医療・福祉業での漏洩原因別事故件数（2016年）

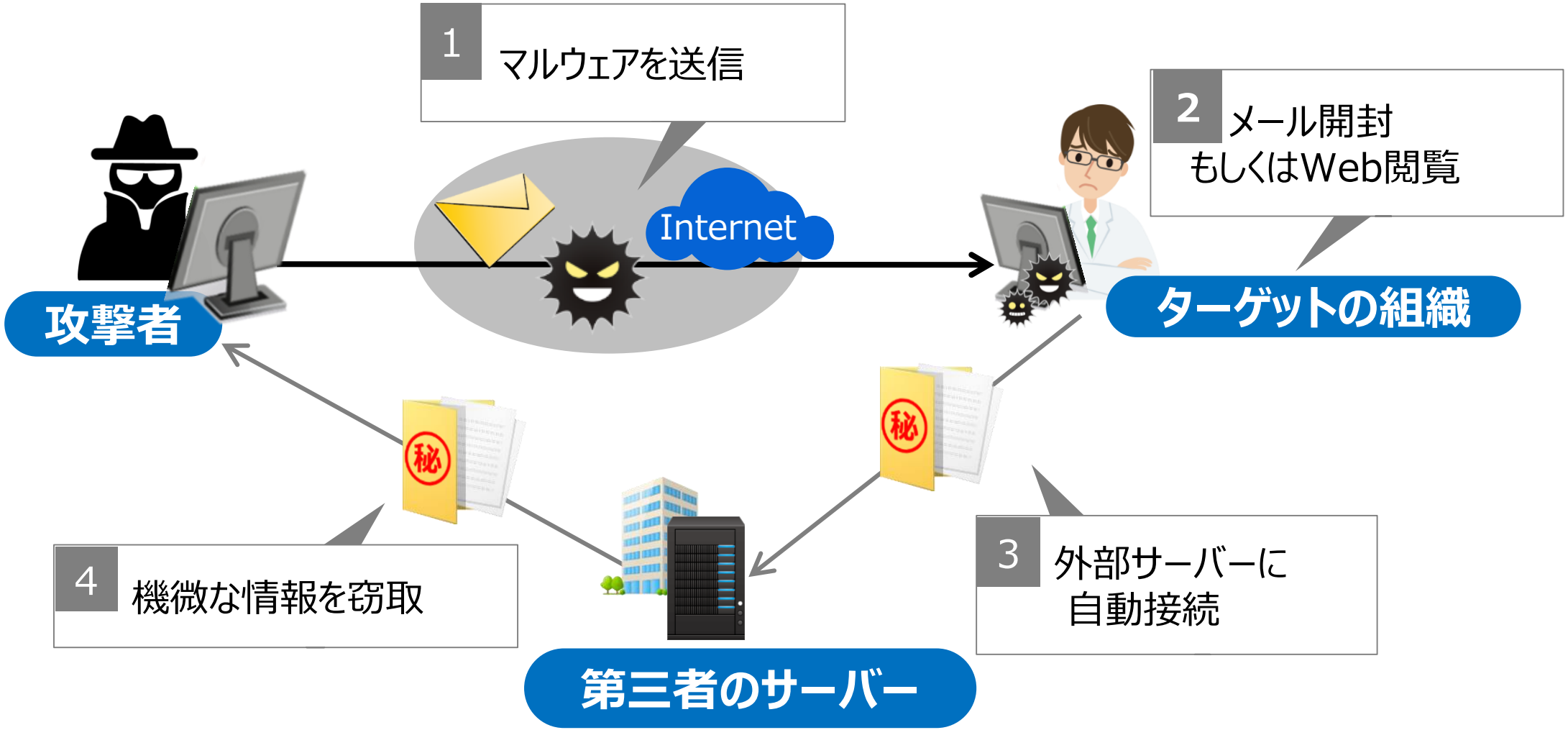


情報漏洩事故のうち
約7割が悪意のないミスが原因。

参考：『2016年 情報セキュリティインシデントに関する調査報告書』より引用　NPO 日本ネットワークセキュリティ協会調査

標的型攻撃とは？

金銭や知的財産（個人情報、新製品のデータなど）の重要情報の不正な取得を目的として、特定の標的（ターゲットになる企業や組織）に対して行われるサイバー攻撃のこと。

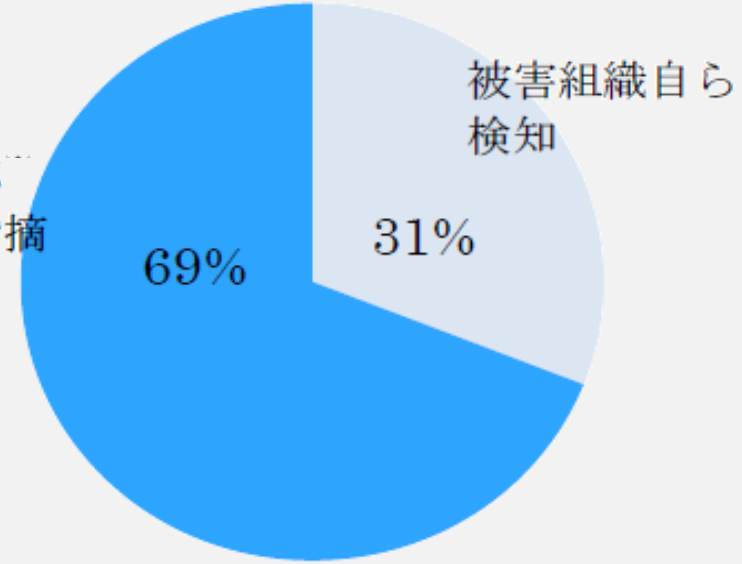


気づきにくい標的型攻撃

引用：経済産業省「サイバーセキュリティ経営ガイドライン」より

標的型攻撃は外部の指摘で気付くのが7割。発覚まで時間がかかる。

セキュリティ侵害が発覚した経緯は？



攻撃されていることに気づいたり、攻撃されているとわかってからマルウェアを見つけ出すことも困難。

侵入してから３ヶ月動かないマルウェアも。

PCに感染しても一定期間動かないなど、サンドボックスでも検出されないようにプログラムされているマルウェア。

３ヶ月くらいでログが消える組織が多い。

時間が経ってから気付いたときのために、操作ログの長期保存、マルウェアの痕跡を追うための詳細なログと検索が必要です。

SKYSEA Client Viewで
実施するセキュリティ対策

SKYSEA Client View 支援範囲

院内システム概要例

※代表的なシステムを記載

SKYSEA Client Viewの支援範囲

基幹システム

患者呼出システム　医事会計システム

事務管理システム

・病院HP管理
・メール
・インターネット

インターネット接続端末

人事給与システム

勤怠管理システム

情報系ネットワーク

電子カルテシステム

HIS系ネットワーク

部門システム

- 病理検査システム
- 放射線情報システム
- 手術管理システム
- 麻酔記録システム
- ナースコールシステム
- リハビリシステム
- 健診システム
- リネンシステム
- 給食管理システム

※部門システムにも導入いただけます

「医療機器におけるサイバーセキュリティの確保について」（薬食機参発0428 第１号 / 薬食安発0428 第1号 / 平成27年4月28日）にて、機器の機能に影響がない範囲で、IT資産管理ソフトウェアのインストールは法律上問題がない、との見解が出されています。各システムにインストールされる際は、事前に製造販売業者にご相談ください。

脆弱性にはセキュリティパッチの適用が必須

脆弱性とは？

「セキュリティの問題を引き起こす、ソフトウェアの設計・実装上の弱点」のこと。攻撃者が自由に操作できれば、ユーザーに被害を及ぼせるようになります。

脆弱性を突かれると…

ファイルを開いただけでマルウェアが活動するよう、脆弱性を利用したファイルを送りつけ。

①文書ファイルを開くだけで

マルウェアが仕込まれた文書ファイル

②マルウェアが活動・感染

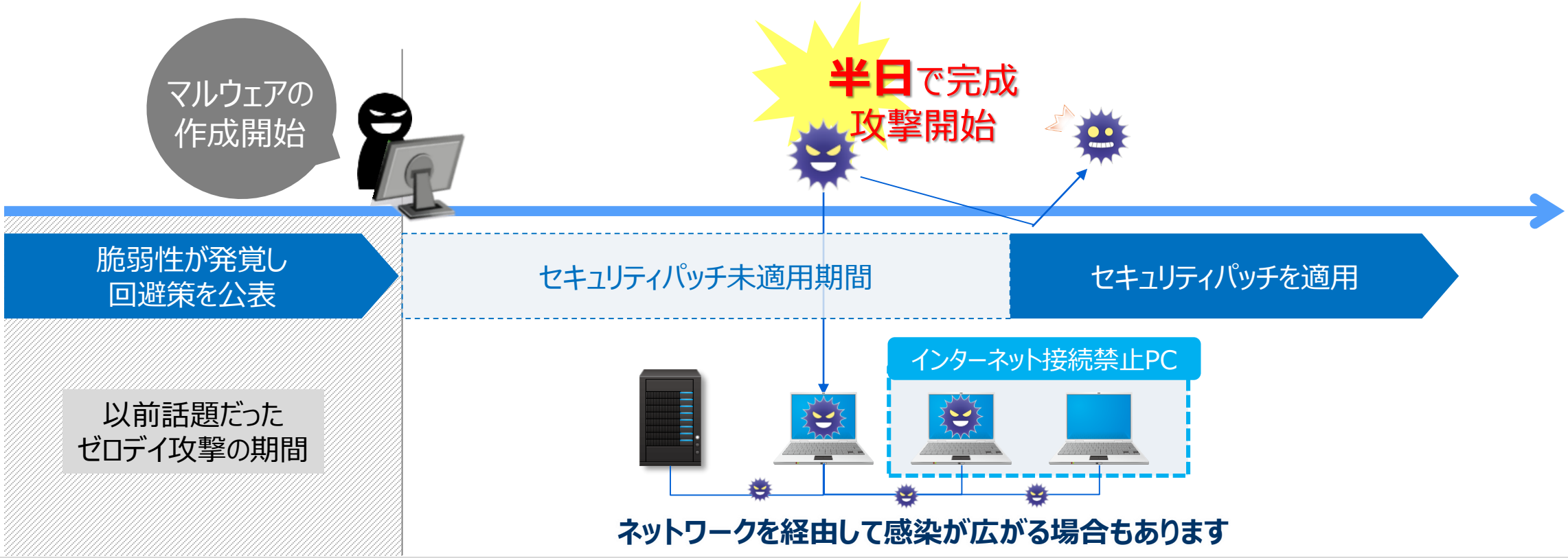
対策はOSやソフトウェアを常に最新の状態に保つこと

OSやソフトウェアのバージョンを常に最新の状態に保ち、脆弱性を解消することで感染リスクを低減します。

企業と比べると、病院はパッチの適用が遅め。

公開されたセキュリティパッチは早急に適用を

以前はセキュリティパッチが未公表の脆弱性を悪用した**ゼロデイ攻撃**が話題でした。
最近は効率化を考えて、**公開されてすぐの脆弱性**が攻撃されることが多いです。

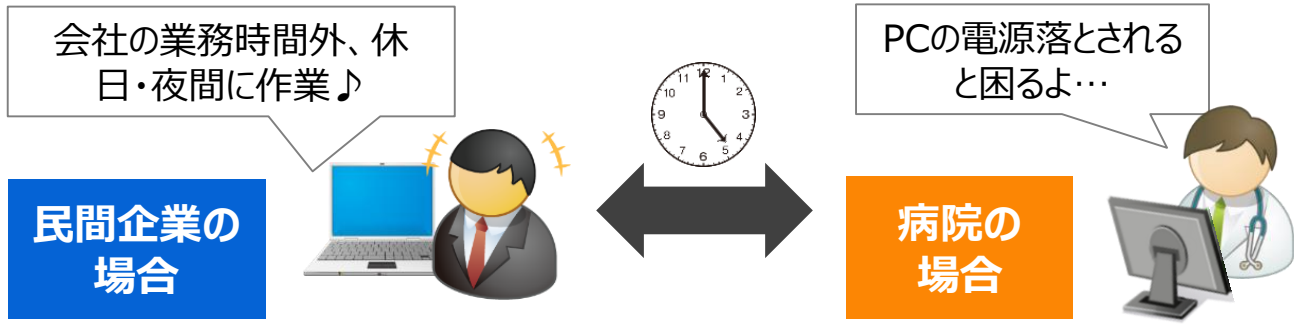


ソフトウェアメーカーが公開しているパッチをできるだけ早く
適用するだけでも標的型攻撃の多くを防ぐことは可能です。

病院ではセキュリティパッチの適用も大変

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、
セキュリティパッチを適用するタイミングが難しいです。



システム担当者が病院内をまわってアップデートしようとしても・・・

敷地が広く、病棟や外来のPC1台ずつにパッチを当てていくのは大変です。

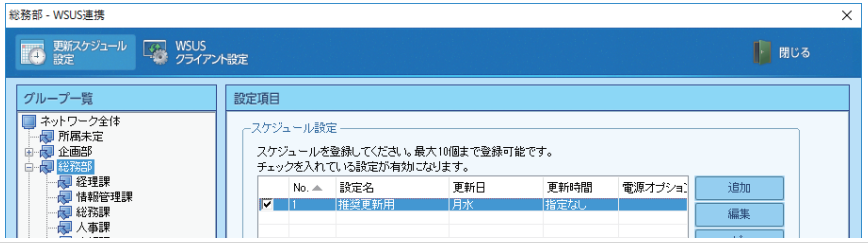
手術室は手術中でなくても、着替えて、
消毒・殺菌しないと入室できません。

WSUS連携で更新プログラムを一斉配布

ネットワーク上のPCへ更新プログラムの一斉配布・実行が可能です。
外来のPCは夜にまとめて配布・実行する、入室しにくい手術室は使っていない時間帯を調べて１台ずつ遠隔で更新プログラムを当てるなど、適用作業を効率化できます。

1 更新プログラムの更新を実行

業務に支障の少ない時間帯に定期的な適用を行うなど、
更新プログラムの適用スケジュールを管理できます。



WSUSは、ネットワーク管理者の負担と、ネットワークの負荷の軽減に有効

2 WSUSから更新プログラムを適用

SKYSEA Client View サーバー

クライアントPC

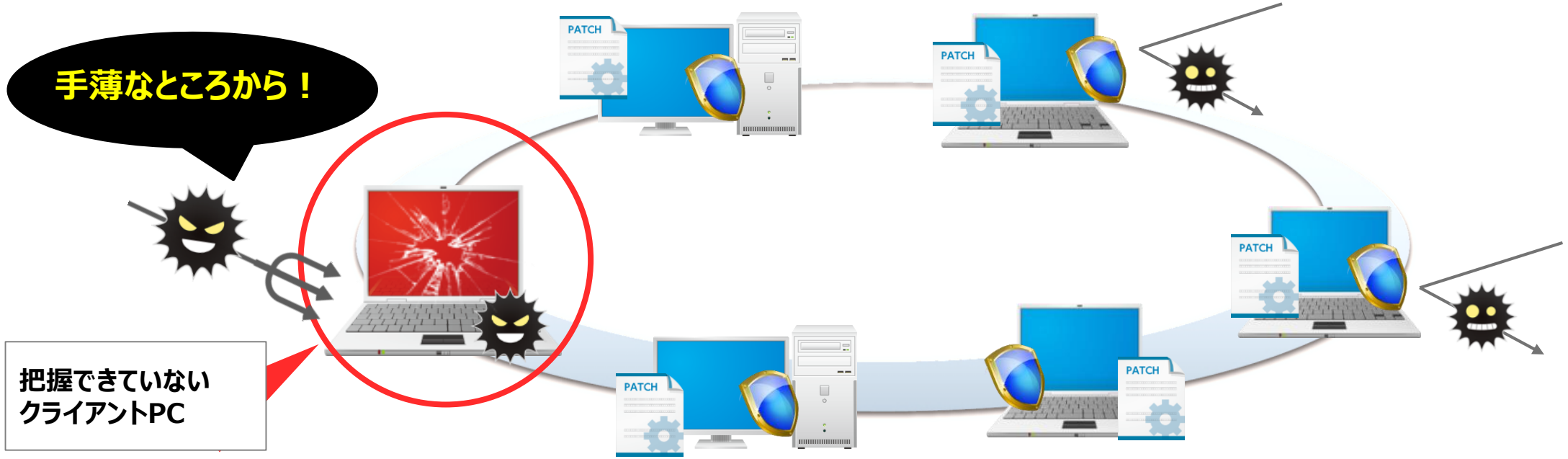
WSUSサーバー

更新プログラムの適用ができれば、サイバー攻撃に対するクライアントPCのセキュリティリスクは大幅に下がります。

まずはクライアントPCの管理から

すべてのPCをもれなく把握することが必要です。

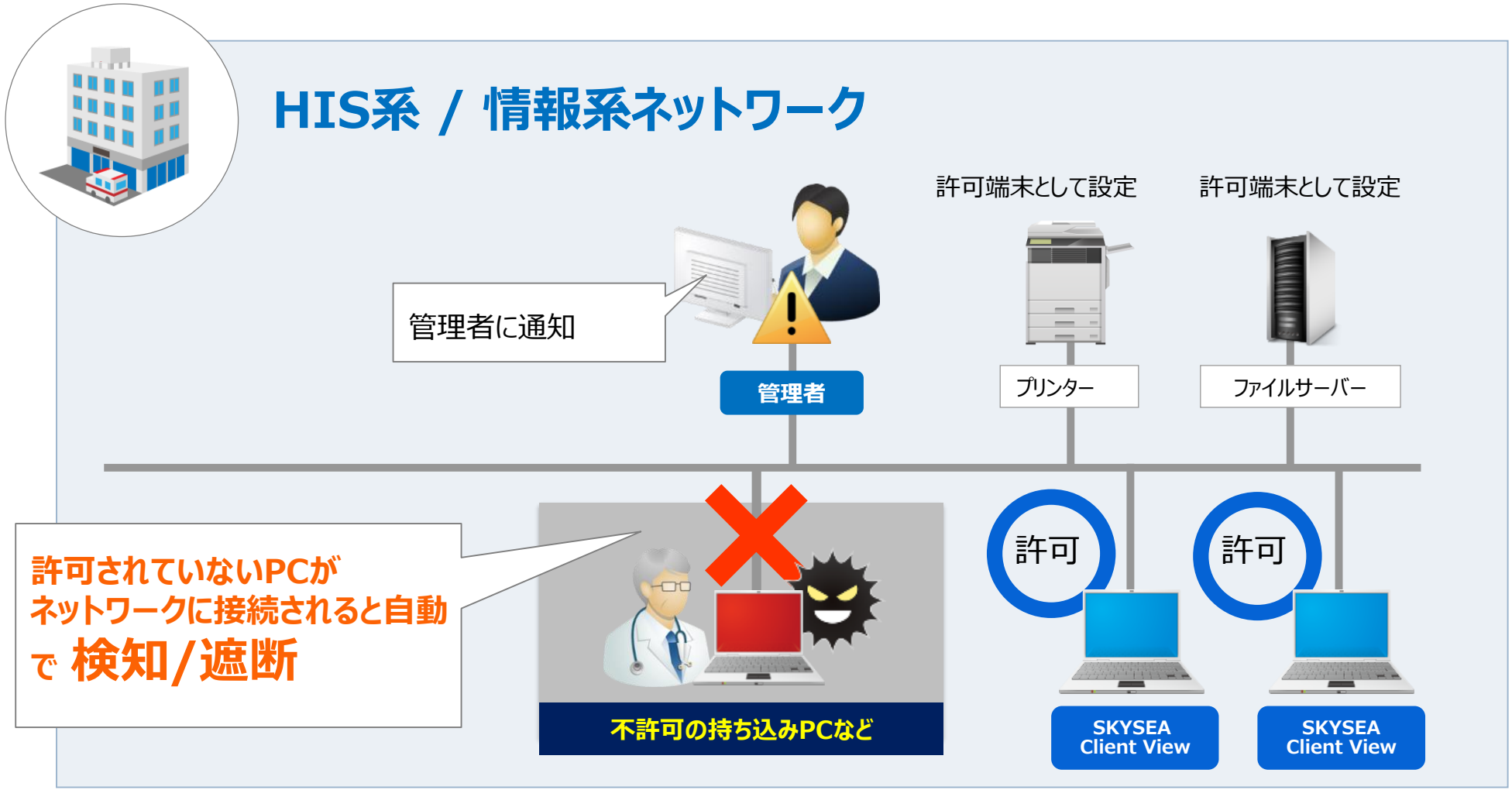
セキュリティ対策を行うために、まずは院内のネットワークに接続されている機器を把握しておくことが大切です。特にインターネットに接続しているPCの場合、1台でも対策に漏れがあるとそのPCからマルウェアに感染し、被害が拡大する可能性があります。



1台でも把握できていないクライアントPCや持ち込まれたPCがあると、そこからマルウェアが侵入する恐れがあります

許可されていないPCの接続を発見・遮断

SKYSEA Client Viewがインストールされていないが情報系ネットワークに接続されると、許可されていない端末としてネットワークから遮断します。非常勤医師の持ち込みPCなど許可していないPCを検知し、遮断できます。



※ 不許可端末遮断はオプションです。<500cl Pack/LT>

「すぐ」の適用が難しい場合は、代わりの方法を

電子カルテ系（HIS系）など

日頃からインストールされているシステムなどの情報をまとめた台帳を管理

①各システムが入っている端末のリストを用意

パッチの適用ができる端末/できない端末がわかる

②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する

・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　など

インターネット系など

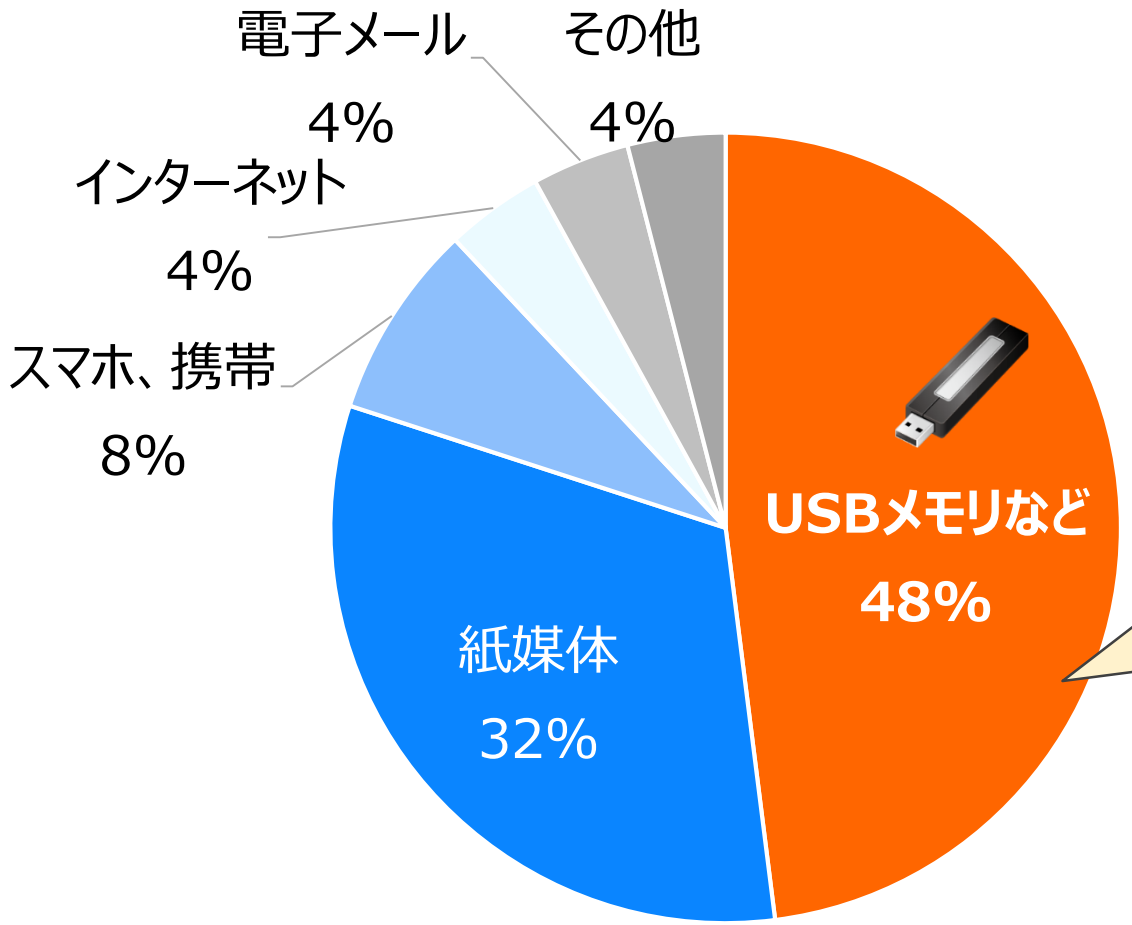
できるだけ早くアップデート

インストールされているシステムについて、OSやOffice製品に更新プログラムを適用しても問題ないかを確認しておきます。パッチ適用に左右されるシステムは今後も使用していくのか検討が必要です。

内部からの情報漏洩対策

医療機関での情報漏洩事故は？

医療・福祉業での漏洩媒体別事故件数（2016年）



情報漏洩事故のうち
約半数がUSBメモリなどの
可搬媒体から漏洩。

どんな情報が
どれだけ含まれていたか
わからないケースも…。

参考：『2016年 情報セキュリティインシデントに関する調査報告書』より引用　NPO 日本ネットワークセキュリティ協会調査

ネットワーク分離とUSBメモリ

インターネットに繋がっていないデータは安全？

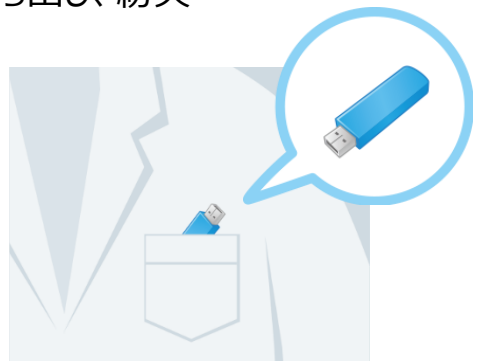
ネットワークを分離しても、異なるセグメント間でUSBメモリでやり取りする際に、USBメモリに侵入していたマルウェアに感染したり、持ち込み・持ち出しによる情報漏洩事故が発生することもあります。

デバイスによる情報漏洩のリスクが潜んでいます！

マルウェアが潜んでいる私物USBを持ち込み、病院内の端末に挿す

患者のデータを保存したUSBメモリやデジタルカメラを紛失

学会用に患者のデータをUSBで持ち出し、紛失

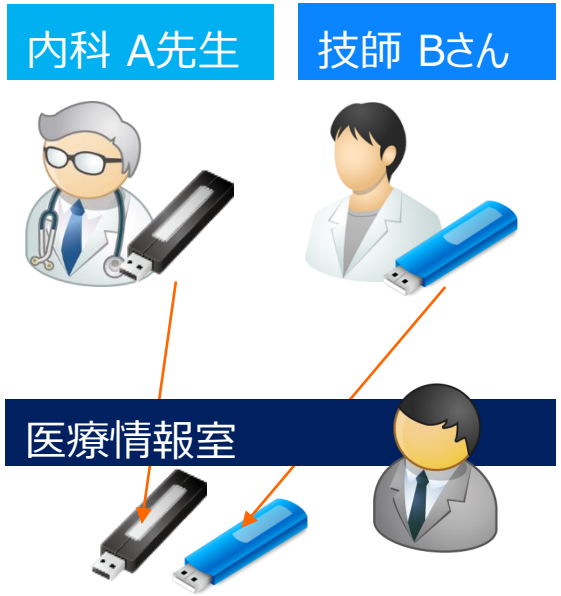


白衣のポケットにUSBメモリをいれたまま、クリーニングに出してしまった！

USBメモリの台帳登録までの流れ

1 利用者からUSBメモリを回収

院内で使用するUSBメモリを、利用者から回収※。

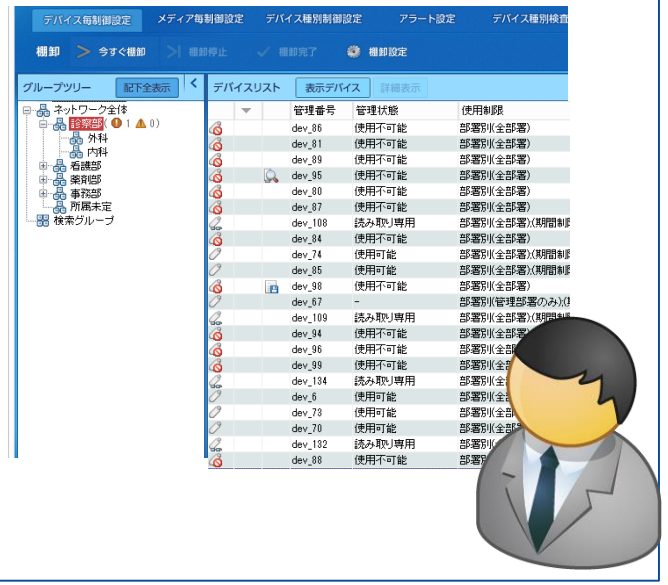


2 USBメモリを登録

挿入すると、USBメモリの情報が登録画面に表示。

3 利用状況を台帳で確認

一定期間後、USBメモリ管理台帳で、利用されているUSBメモリの本数を確認。



※使用中のUSBメモリに代えて、暗号化機能などを搭載した登録済みUSBメモリを渡す病院もあります。

運用ポリシーに合わせたUSBメモリの個別制御

SKYSEA Client Viewでは、USBメモリのベンダーID、プロダクトID、シリアルナンバーで個別に管理でき、台帳に登録されたデータは個別に編集できます。電子カルテシステムと連携※し、電子カルテのログインユーザー単位で、使用制限を設定することも可能です。

個別に使用可能などを設定

使用可能、読み取り専用、使用不可などを個別に設定できます。

病院で配布されたUSBメモリ

私物のUSBメモリ

電子カルテのログインID単位でUSBメモリの使用を制限できます

電子カルテログインID：D001
デバイス使用可

電子カルテログインID：D021
デバイス使用不可

※ 電子カルテシステム連携はオプションです。<Pro/Ent/500cl Pack/ LT/ ST>
※ 連携可能な電子カルテシステムについては、弊社までお問い合わせください。

USBメモリ以外のデバイス制御も可能

操作に迷わないシンプルなデバイス制御設定画面で、CD/DVDドライブやスキャナーなど、USBメモリ以外のデバイス制御も簡単に行えます。

デバイス種別制御設定

青枠は使用可能

黒枠は読み取り専用

赤枠は使用不可能

特定のグループのみ使用制限が可能
すべてのグループでUSBメモリの使用を禁止した上で、USBメモリでのデータのやりとりが欠かせないグループでのみ使用を許可するなど、柔軟な管理が可能です。

※ Mac端末では、CD / DVD / Blu-ray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。

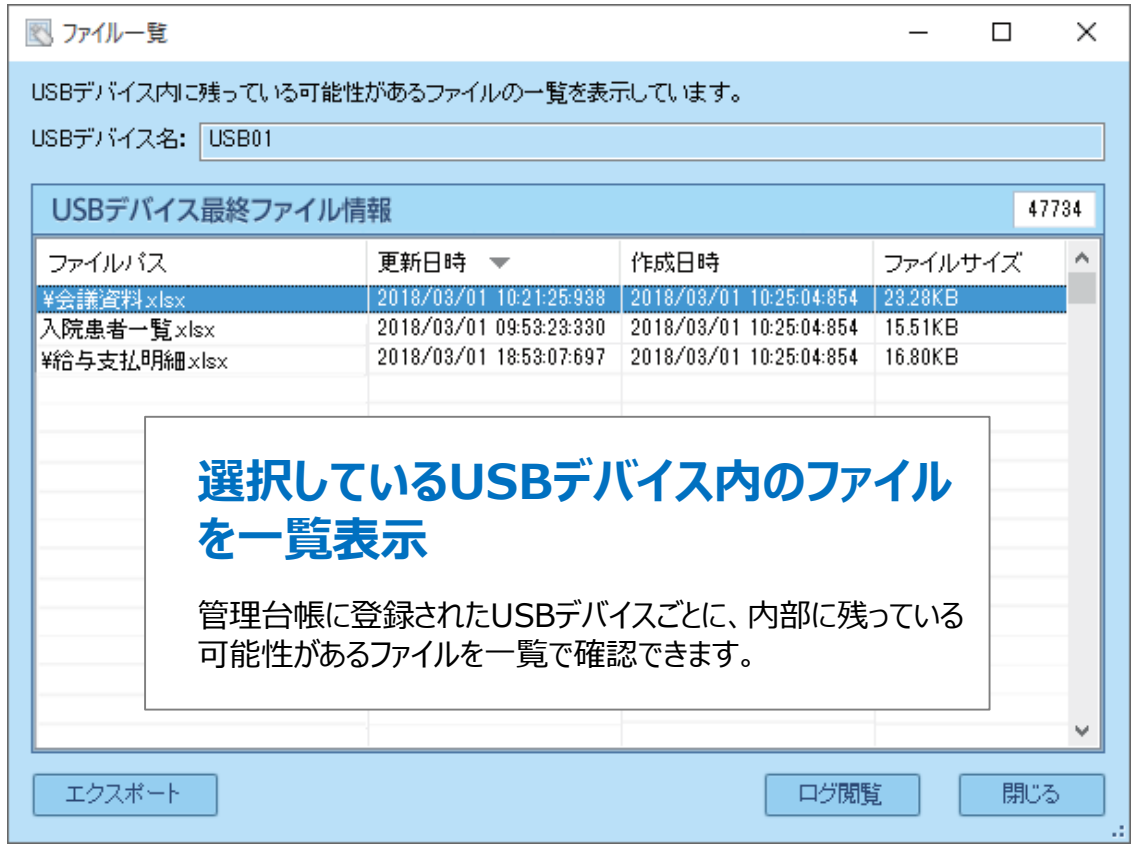
病院でよく使われるデジタルカメラにも、データを保存できてしまいます。
カメラやカードリーダーは原則禁止し、許可したときだけの利用をお勧めします。

USBメモリなどの紛失時に初動対応を迅速化

USBメモリなどを万が一紛失してしまった場合にも、重要データが含まれていないかを確認でき、初動対応が迅速に行えます。また、USBデバイスに保存されているファイルの操作ログを表示できます。

ファイルが記載されているUSBデバイスをアイコンで表示

ファイルが残っている可能性があるUSBデバイスをアイコンで表示するため、わかりやすく把握できます。



選択しているUSBデバイス内のファイルを一覧表示

管理台帳に登録されたUSBデバイスごとに、内部に残っている可能性があるファイルを一覧で確認できます。

医療機関における
改正個人情報保護法

医療機関における個人情報保護法のポイント

個人情報の取り扱いについて

個人情報保護法 20条：安全管理措置

個人情報取り扱い事業者は、その取り扱う個人データの漏洩、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンスより

４．安全管理措置、従業者の監督及び委託先の管理

(2)⑦ 技術的安全管理措置：

個人データの盗難・紛失等を防止するため、個人データを取り扱う情報システムについて以下のような技術的安全管理措置を行う。

- 個人データに関するアクセス管理
- 個人データに対するアクセス記録の保存
- 不正が疑われる異常な記録の存否の定期的な確認

電子カルテ系以外のインターネット系向けのガイドライン

医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス

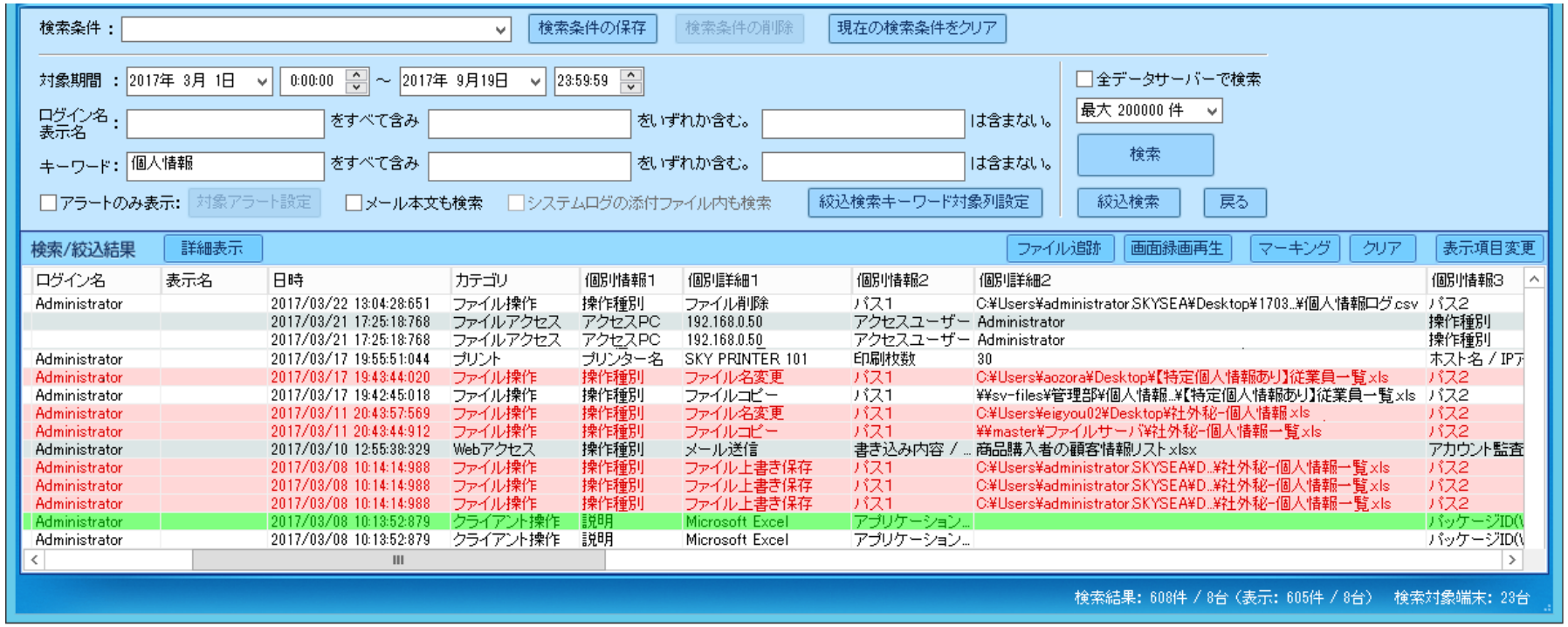
平成２９年４月14日

厚生労働省

http://www.mhlw.go.jp/file/06-Seisakujouhou-12600000-Seisakutoukatsukan/0000144825.pdf

個人データへのアクセス記録

個人情報ファイルへのファイル操作ログ例



院内では共有PCで利用しているので、ログをとっても、
WindowsのログインIDと紐付かず、誰が操作したかわからない…

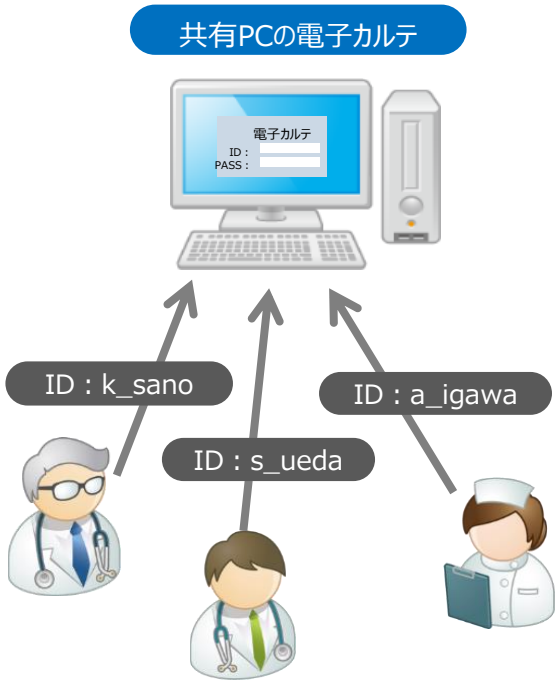
PCを使用する場合、共通のアカウントでログインすることが多いので、誰がPCを操作したのかがわかりません。Windowsアカウントのログインなしでも電源を入れるとPCが使用状態になることが多く、Windowsからは、実質的に利用者を特定することはできません。

電子カルテ連携

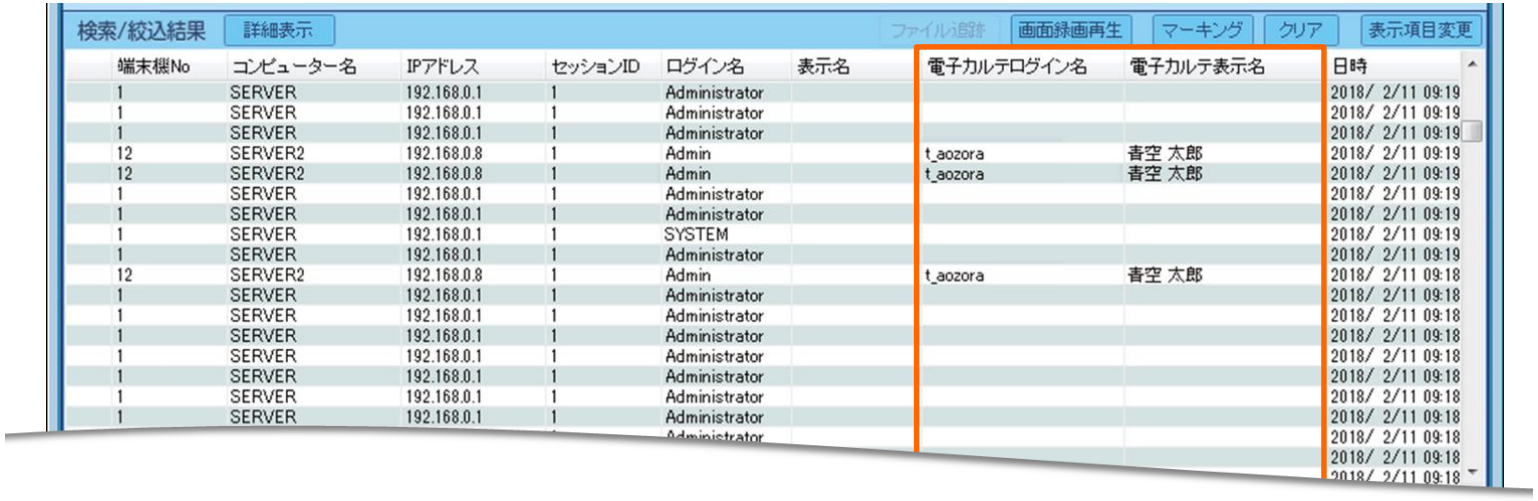
電子カルテのログイン情報からユーザーごとの操作を特定

PC操作ログ情報に電子カルテのログインIDを含めてログを収集します。
共有PCでも利用者を特定、ユーザーごとに操作の確認ができます。

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/ 2/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:19
12	SERVER2	192.168.0.8	1	Admin		t_aozora	青空 太郎	2018/ 2/11 09:19
12	SERVER2	192.168.0.8	1	Admin		t_aozora	青空 太郎	2018/ 2/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:19
1	SERVER	192.168.0.1	1	SYSTEM				2018/ 2/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:19
12	SERVER2	192.168.0.8	1	Admin		t_aozora	青空 太郎	2018/ 2/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:18
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:18
				Administrator				2018/ 2/11 09:18
								2018/ 2/11 09:18
								2018/ 2/11 09:18

※ 電子カルテシステム連携はオプションです。<Pro/Ent/500cl Pack/ LT/ ST>
※ 連携可能な電子カルテシステムについては、弊社までお問い合わせください。

SKYSEA Client Viewで情報漏洩対策を支援

クライアントPCをはじめとして、組織内のサーバー、ソフトウェア、ネットワーク機器など、さまざまなIT資産を一元管理し、より安全な情報漏洩対策の実現をお手伝いします。また、各メーカー様の製品と連携し、対策のさらなる強化を支援します。

企業の安全なIT運用を支援する各種機能を搭載

ログ管理	セキュリティ管理	デバイス管理	レポート
IT資産管理	ソフトウェア資産管理(SAM)	メンテナンス	サーバー監査	モバイル機器管理(MDM)

SKYSEA Client Viewの特長

さらに『使いやすい』操作画面をめざしてデザイン変更

アイコンや機能ガイドで、多数の機能から使いたい機能がひと目でわかるよう構成しています。

**利用シーンを
イメージしたアイコン**

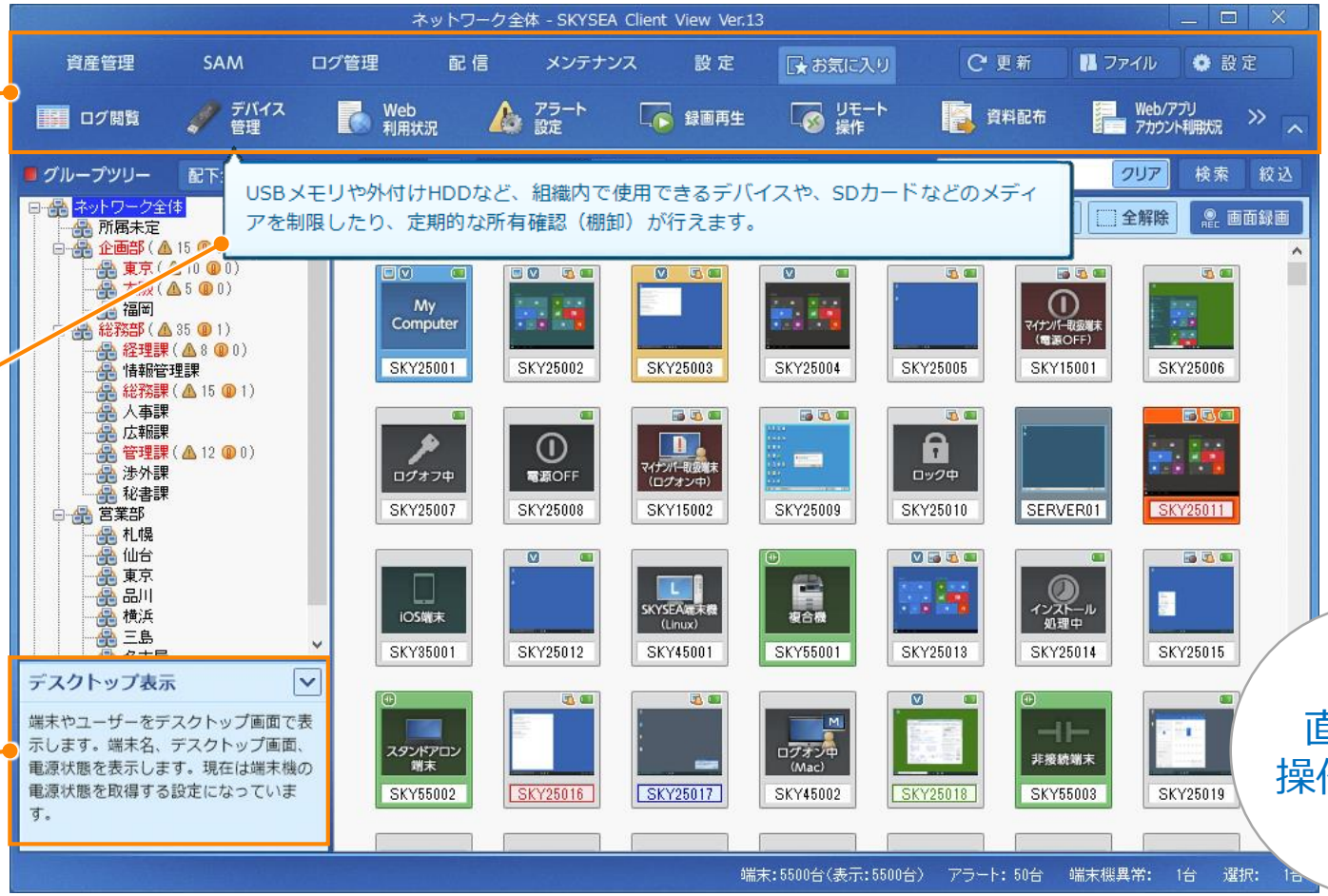
操作内容をイメージ
しやすい用語を表記。

ふきだしヒントを表示

初めてでも
操作に迷いません。

機能ガイド

アイコンにマウスを合わせると
各機能の解説を表示。



直感的に
操作できます

お客様のワークスタイルに合った「安全・安心」なIT活用を

SKYSEA Client Viewで

情報漏洩対策と

IT運用管理を

ご支援いたします

ご清聴ありがとうございました

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。

- 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。

インフォメーションダイヤル

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　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