

— 企業・団体向け クライアント運用管理ソフトウェア —



毎年 お客様の声を取り入れ、 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～

もくじ

1. 医療機関での情報漏洩事故とサイバー攻撃
2. SKYSEA Client Viewで実施するセキュリティ対策
3. 内部からの情報漏洩対策
4. 医療機関における改正個人情報保護法

会社案内

S k y 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
Sky Menu Pro



SKYMEC
IT Manager



スカイメニュークラス
Sky Menu 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

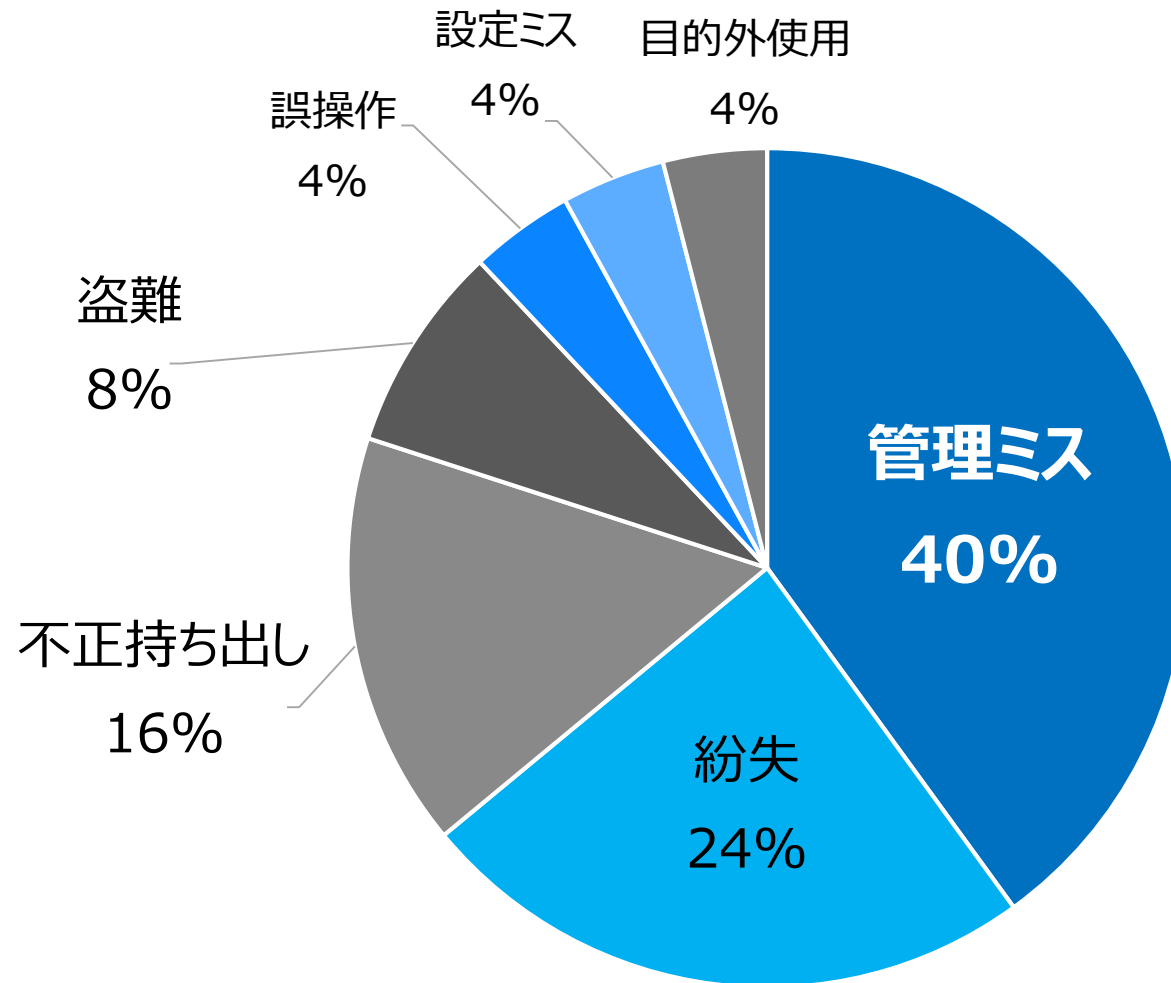


ソフトウェア
評価/検証

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）

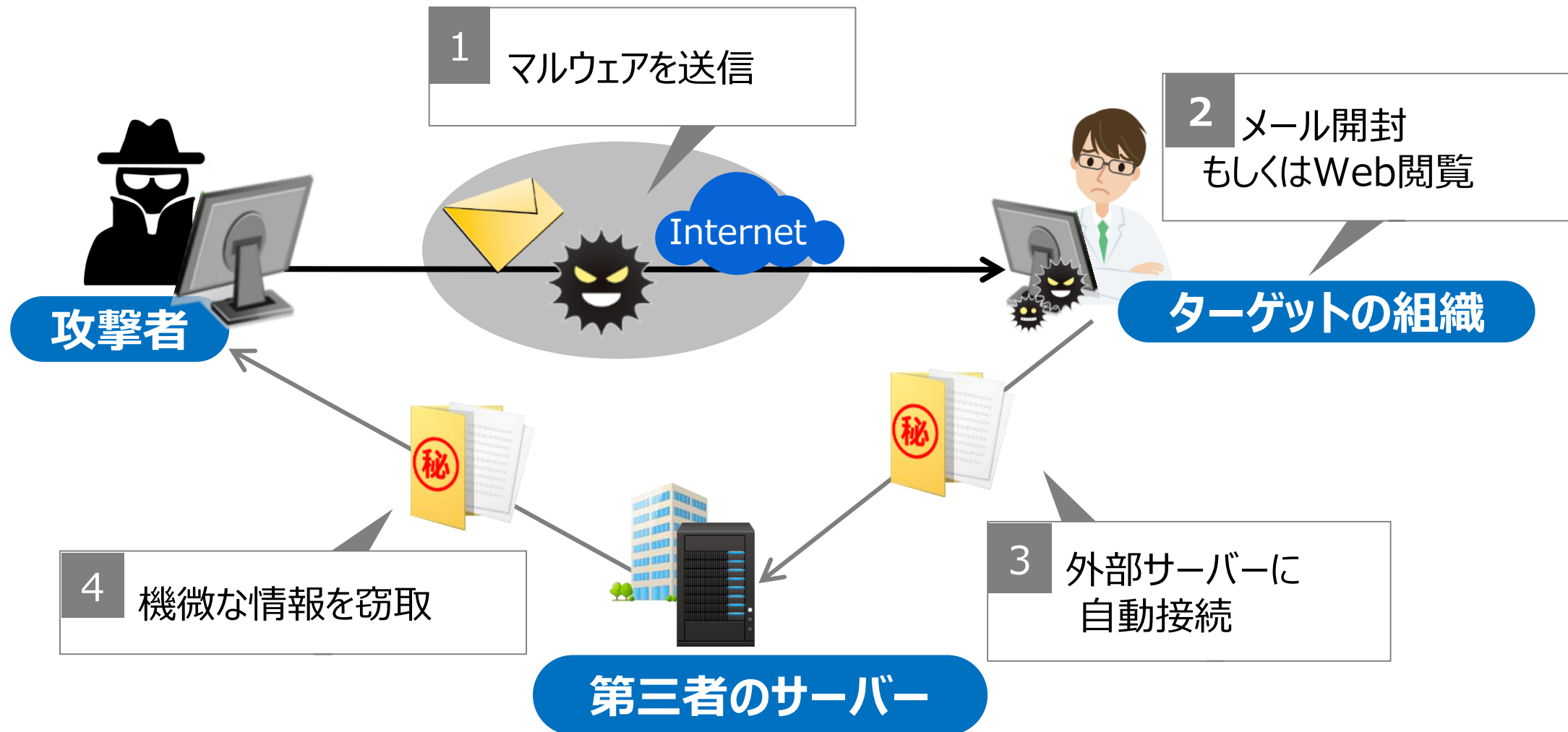


情報漏洩事故のうち
約7割が悪意のない
ミスが原因。



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。

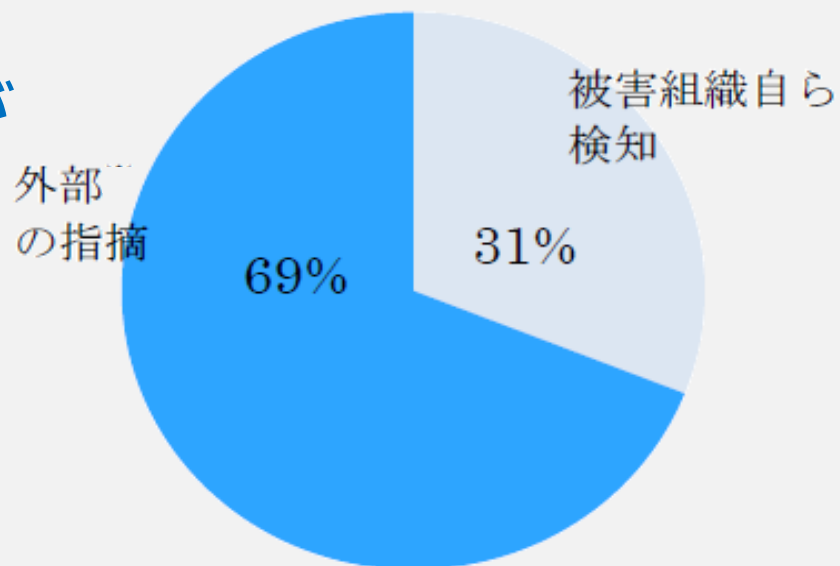


気づきにくい標的型攻撃

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

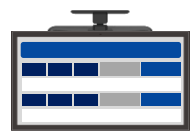


院内システム概要例

※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



インターネット
接続端末

- ・病院HP管理
- ・メール
- ・インターネット



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

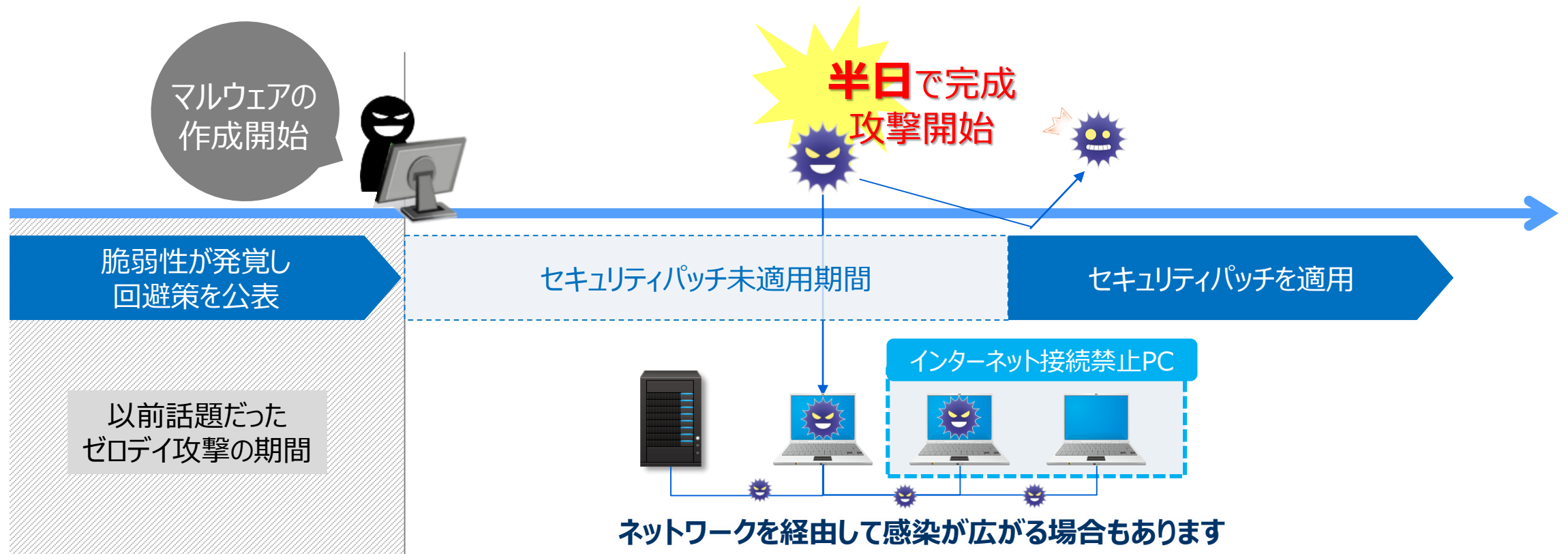
OSやソフトウェアのバージョンを常に最新の状態に保ち、脆弱性を解消することで感染リスクを低減します。

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。

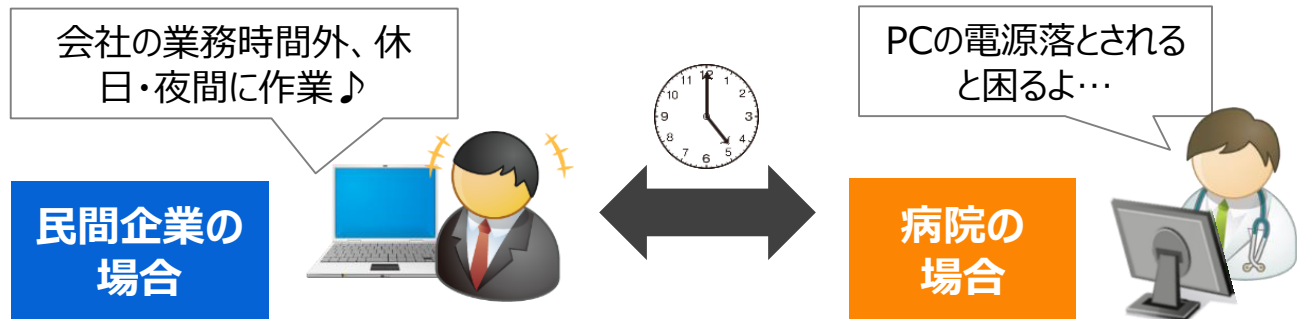


ソフトウェアメーカーが公開しているパッチをできるだけ早く
適用するだけでも標的型攻撃の多くを防ぐことは可能です。

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。

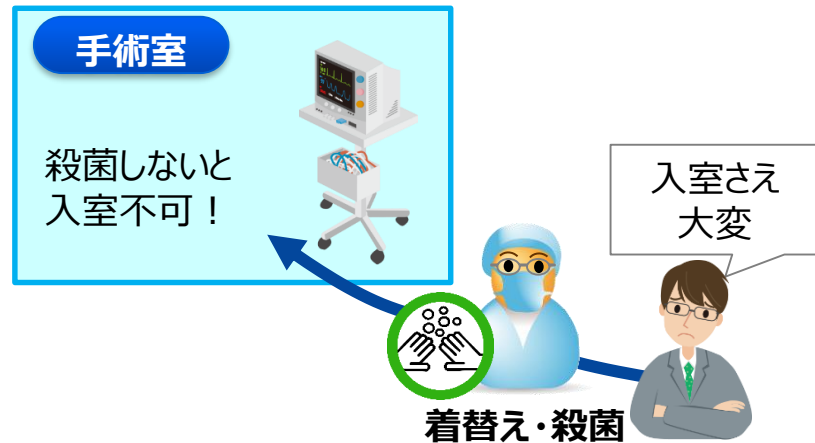


システム担当者が病院内をまわってアップデートしようとしても...

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。



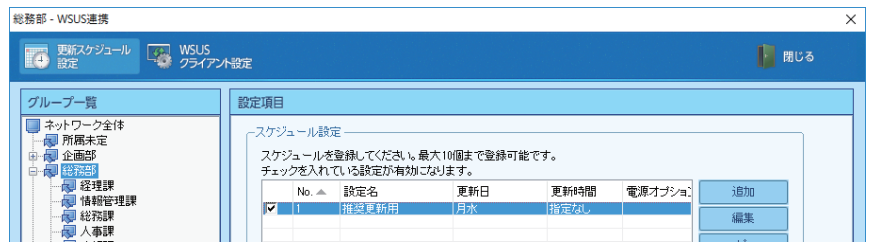
WSUS連携で更新プログラムを一斉配布

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。



クライアントPC

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

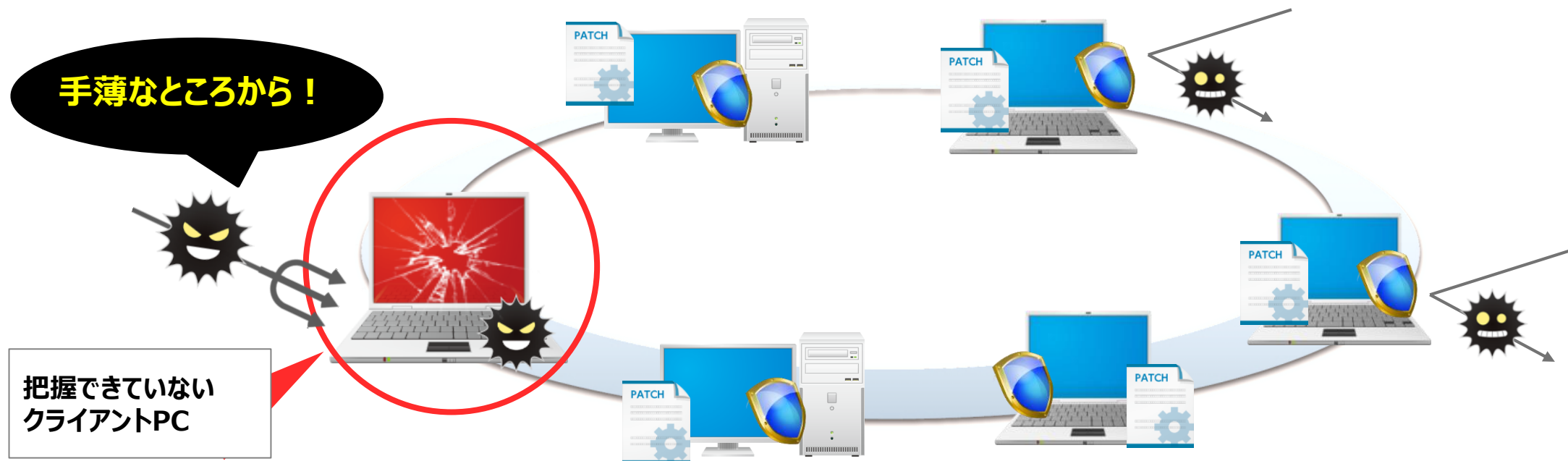


更新プログラムの適用ができれば、サイバー攻撃に対するクライアントPCのセキュリティリスクは大幅に下がります。

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。

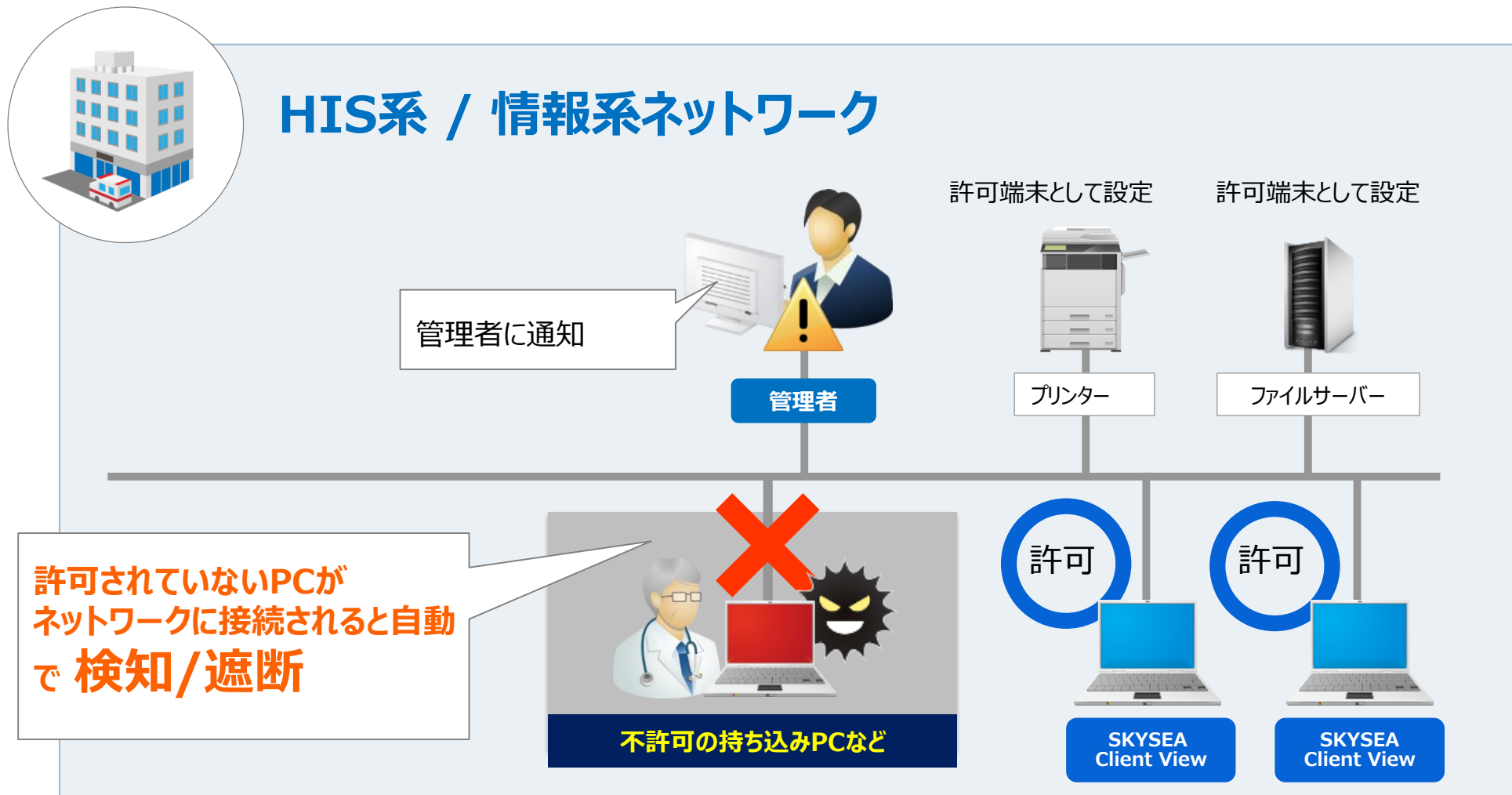
セキュリティ対策を行うために、まずは院内のネットワークに接続されている機器を把握しておくことが大切です。特にインターネットに接続しているPCの場合、1台でも対策に漏れがあるとそのPCからマルウェアに感染し、被害が拡大する可能性があります。



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PCがHIS系や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。



「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

システムが最新の
セキュリティパッチに未対応の場合
(サポートが終了、検証されていないなど)



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

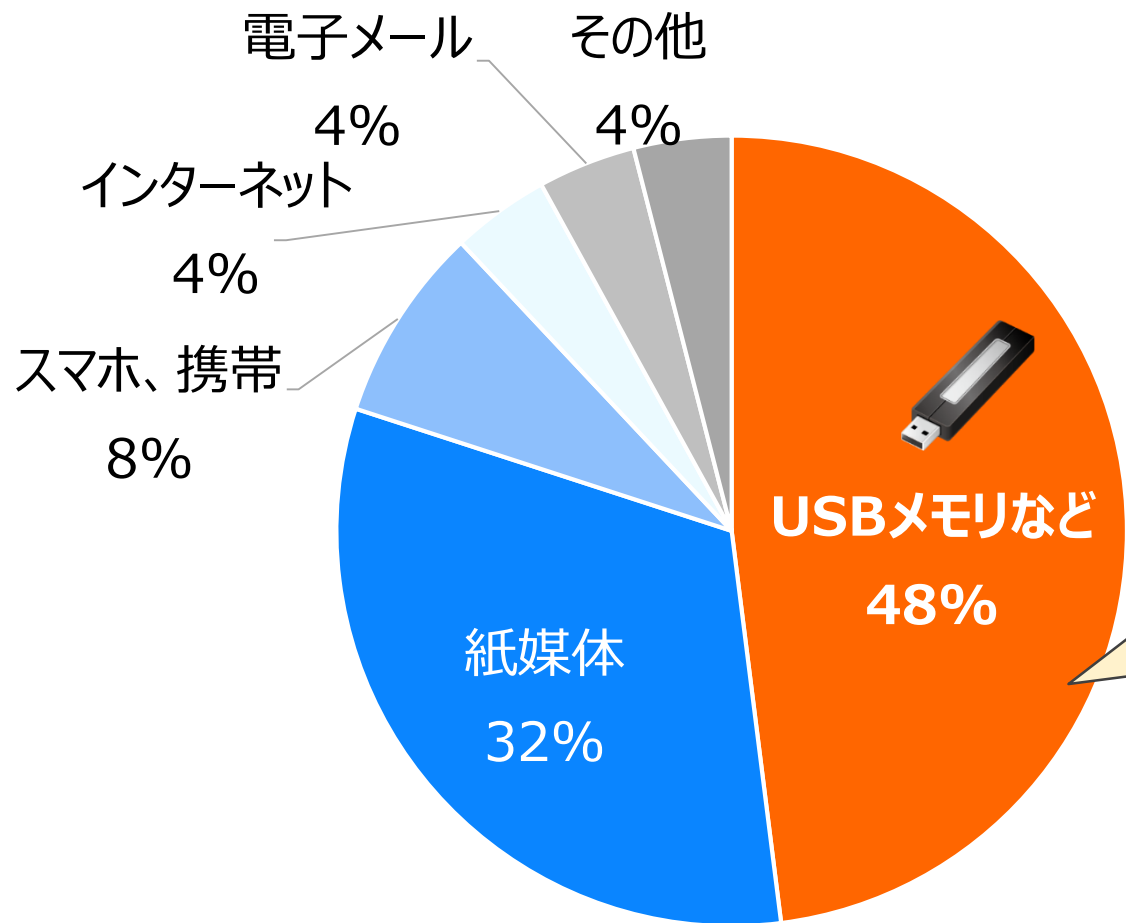
インストールされているシステムについて、OSやOffice製品に更新プログラムを適用しても問題ないかを確認しておきます。パッチ適用に左右されるシステムは今後も使用していくのか検討が必要です。



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…。

対策しようにも
どうしたら…



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※。

内科 A先生 技師 Bさん



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。

SKYSEA Client View

登録済みのUSBメモリ/USBハードディスクです。
デバイス情報を表示します。

管理情報
管理番号 dev_52
管理部署 ネットワーク全体/情報システム部
管理状態 使用不可能
ステータス -
管理ユーザー Administrator
表示名

登録情報
デバイス種別 USBメモリ/USBハードディスク
登録日 2014/12/24
登録先 MASTER
デバイス名
ベンダID
プロダクトID
シリアルNo
説明

登録したら、識別シールを貼って返却
●●病院管理部

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。

グループツリー	デバイスリスト	表示デバイス	詳細表示
ネットワーク全体	管理番号	管理状態	使用制限
外科	dev_86	使用不可能	部署別(全部署)
内科	dev_81	使用不可能	部署別(全部署)
看護部	dev_89	使用不可能	部署別(全部署)
薬務部	dev_95	使用不可能	部署別(全部署)
事務部	dev_80	使用不可能	部署別(全部署)
所属未定	dev_87	使用不可能	部署別(全部署)
検索グループ	dev_108	読み取り専用	部署別(全部署)(期間制限)
	dev_84	使用不可能	部署別(全部署)(期間制限)
	dev_74	使用可能	部署別(全部署)(期間制限)
	dev_98	使用可能	部署別(全部署)(期間制限)
	dev_85	使用不可能	部署別(全部署)
	dev_67	-	部署別(全部署)
	dev_109	読み取り専用	部署別(全部署)(期間制限)
	dev_94	使用不可能	部署別(全部署)
	dev_96	使用不可能	部署別(全部署)
	dev_99	使用不可能	部署別(全部署)
	dev_134	読み取り専用	部署別(全部署)
	dev_6	使用可能	部署別(全部署)
	dev_73	使用可能	部署別(全部署)
	dev_70	使用可能	部署別(全部署)
	dev_132	読み取り専用	部署別(全部署)
	dev_88	使用不可能	部署別(全部署)

※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

管理番号	管理状態	使用制限	ステータス	棚卸実施ユーザ	管理部署	管理ユーザー	管理
USB30	使用不可能	部署別(全部署)	-		所属未定	sky15	sky
USB31	使用不可能	部署別(全部署)	-		所属未定	sky22	sky
USB33	使用不可能	部署別(全部署)	-		広報部	sky07	sky
USB36	使用可能	部署別(全部署)	-		総務部	sky04	sky
USB38	使用不可能	部署別(全部署)	棚卸完了(2012/1... sky19		カスタマーサポー...	sky19	sky
USB41	使用可能	部署別(全部署)	-		営業部	sky01	sky
USB42	使用可能	部署別(全部署)	棚卸未完了		管理部	sky13	sky
USB43	使用可能	部署別(管理部署)	-		所属未定	sky16	sky
USB44	使用可能	部署別(全部署)	-		所属未定	sky12	sky
USB47	使用可能	部署別(全部署)	棚卸完了(2012/1... sky17		所属未定	sky17	sky
USB48	使用不可能	部署別(全部署)	-		経理部	sky03	sky
USB49	使用不可能	部署別(全部署)	-		広報部	sky08	sky

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。

デバイスリスト				表示デバイス	詳細表示	ウイルススキャン結果
		管理番号	USBデバイス名	ベンダID		
		USB43		056E		
		USB77		04BB		
		USB42		056E		
		USB53		0411		
		USB73		04BB		
		USB44		0A6B		
		USB51		0A6B		
		USB57		9EC		

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。

ファイル一覧			
USBデバイス内に残っている可能性があるファイルの一覧を表示しています。			
USBデバイス名: USB01			
USBデバイス最終ファイル情報 47734			
ファイルパス	更新日時	作成日時	ファイルサイズ
※会議資料.xlsx	2018/03/01 10:21:25:938	2018/03/01 10:25:04:854	23.28KB
入院患者一覧.xlsx	2018/03/01 09:53:23:330	2018/03/01 10:25:04:854	15.51KB
※給与支払明細.xlsx	2018/03/01 18:53:07:697	2018/03/01 10:25:04:854	16.80KB

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。

エクスポート

ログ閲覧

閉じる

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、従業員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

検索条件: 検索条件の保存 検索条件の削除 現在の検索条件をクリア

対象期間: 2017年 3月 1日 0:00:00 ~ 2017年 9月19日 23:59:59

ログイン名: をすべて含む をいずれか含む は含まない

表示名: をすべて含む をいずれか含む は含まない

キーワード: 個人情報 をすべて含む をいずれか含む は含まない

☐ アラートのみ表示: ☐ メール本文も検索 ☐ システムログの添付ファイル内も検索

☐ 全データサーバーで検索 最大 200000 件

検索/絞込結果 詳細表示

ログイン名	表示名	日時	カテゴリ	個別情報1	個別情報詳細1	個別情報2	個別情報詳細2	個別情報3
Administrator		2017/03/22 13:04:28:651	ファイル操作	操作種別	ファイル削除	パス1	C:\Users\administrator SKYSEA\Desktop\1703_21個人情報ログ.csv	パス2
		2017/03/21 17:25:18:768	ファイルアクセス	アクセスPC	192.168.0.50	アクセスユーザー	Administrator	操作種別
		2017/03/21 17:25:18:768	ファイルアクセス	アクセスPC	192.168.0.50	アクセスユーザー	Administrator	操作種別
Administrator		2017/03/17 19:55:51:044	プリント	プリンター名	SKY PRINTER 101	印刷枚数	30	ホスト名 / IPア
Administrator		2017/03/17 19:43:44:020	ファイル操作	操作種別	ファイル名変更	パス1	C:\Users\aozora\Desktop\【特定個人情報あり】従業員一覧.xls	パス2
Administrator		2017/03/17 19:42:45:018	ファイル操作	操作種別	ファイルコピー	パス1	\\sv-files\管理部\個人情報_【特定個人情報あり】従業員一覧.xls	パス2
Administrator		2017/03/11 20:43:57:569	ファイル操作	操作種別	ファイル名変更	パス1	C:\Users\eiyou02\Desktop\社外秘-個人情報.xls	パス2
Administrator		2017/03/11 20:43:44:912	ファイル操作	操作種別	ファイルコピー	パス1	\\master\ファイルサーバー\社外秘-個人情報一覧.xls	パス2
Administrator		2017/03/10 12:55:38:329	Webアクセス	操作種別	メール送信	書き込み内容 / ...	商品購入者の顧客情報リスト.xlsx	アカウント監査
Administrator		2017/03/08 10:14:14:988	ファイル操作	操作種別	ファイル上書き保存	パス1	C:\Users\administrator SKYSEA\D...社外秘-個人情報一覧.xls	パス2
Administrator		2017/03/08 10:14:14:988	ファイル操作	操作種別	ファイル上書き保存	パス1	C:\Users\administrator SKYSEA\D...社外秘-個人情報一覧.xls	パス2
Administrator		2017/03/08 10:14:14:988	ファイル操作	操作種別	ファイル上書き保存	パス1	C:\Users\administrator SKYSEA\D...社外秘-個人情報一覧.xls	パス2
Administrator		2017/03/08 10:13:52:879	クライアント操作	説明	Microsoft Excel	アプリケーション...		パッケージID(\\
Administrator		2017/03/08 10:13:52:879	クライアント操作	説明	Microsoft Excel	アプリケーション...		パッケージID(\\

検索結果: 608件 / 8台 (表示: 605件 / 8台) 検索対象端末: 23台



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。

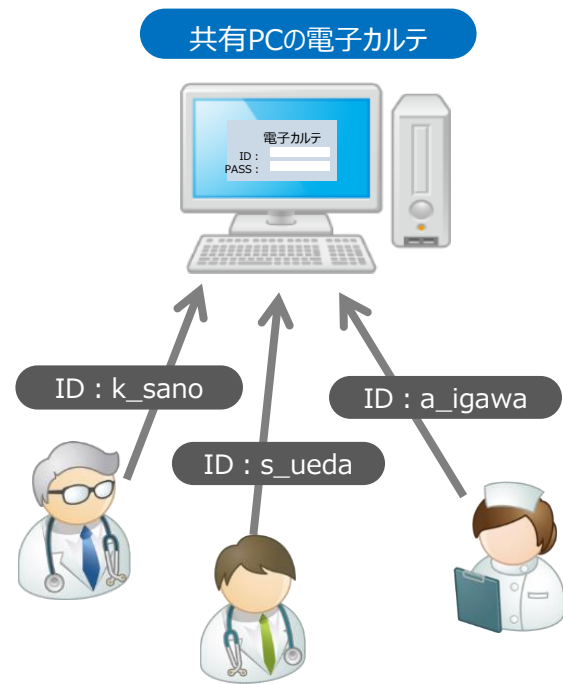
電子カルテ連携

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。

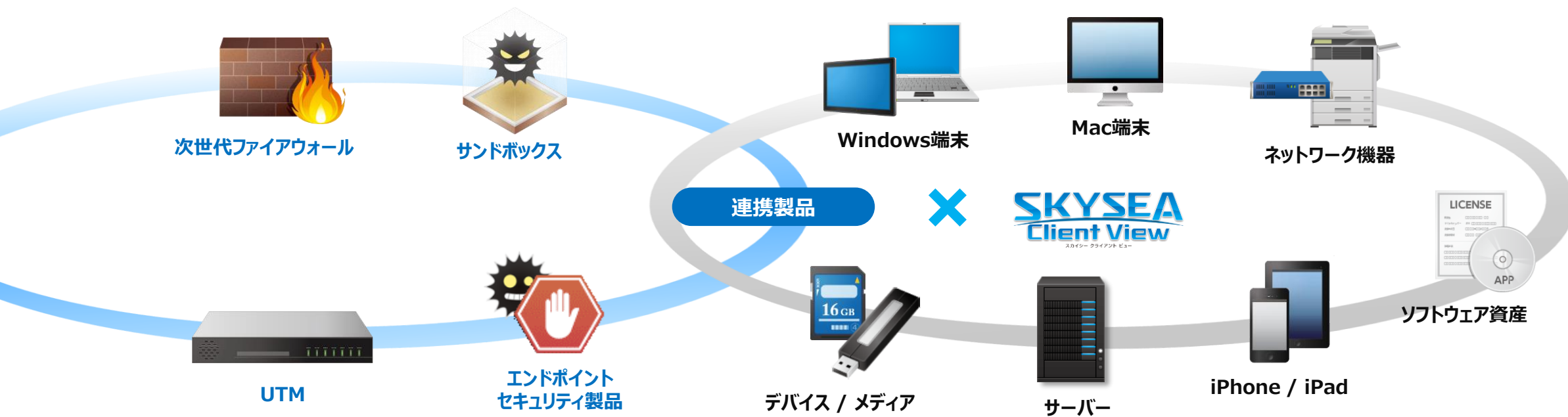


検索/絞り込み結果		詳細表示	ファイルの操作 画面録画再生 マーキング クリア 表示項目変更					
端末機No	コンピューター名	IPアドレス	セッションID	ログイン名	表示名	電子カルテログイン名	電子カルテ表示名	日時
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:19
1	SERVER	192.168.0.1	1	Administrator				2018/ 2/11 09:19
12	SERVER2	192.168.0.8	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
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

※ 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



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

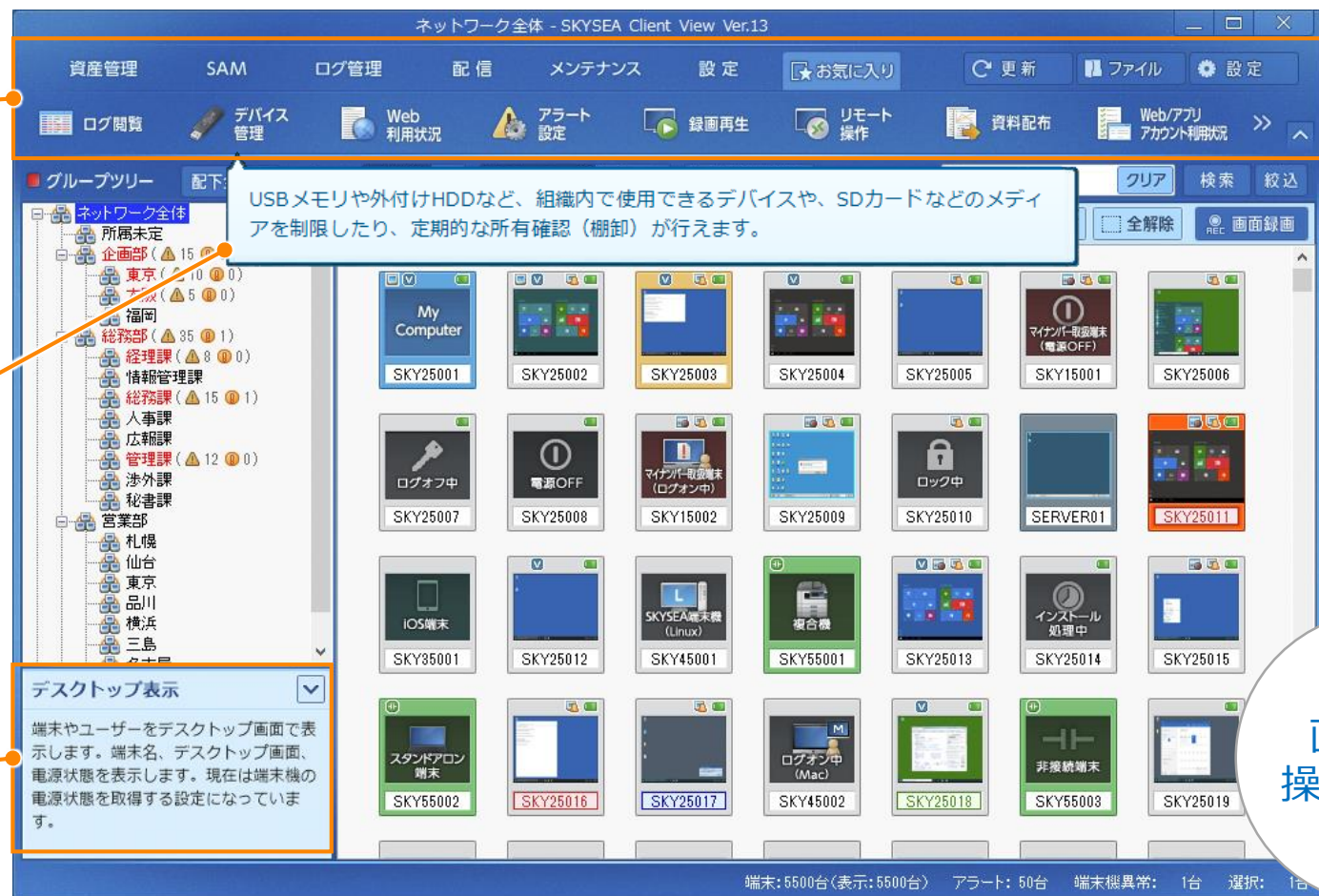
操作内容をイメージ
しやすい用語を表記。

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。

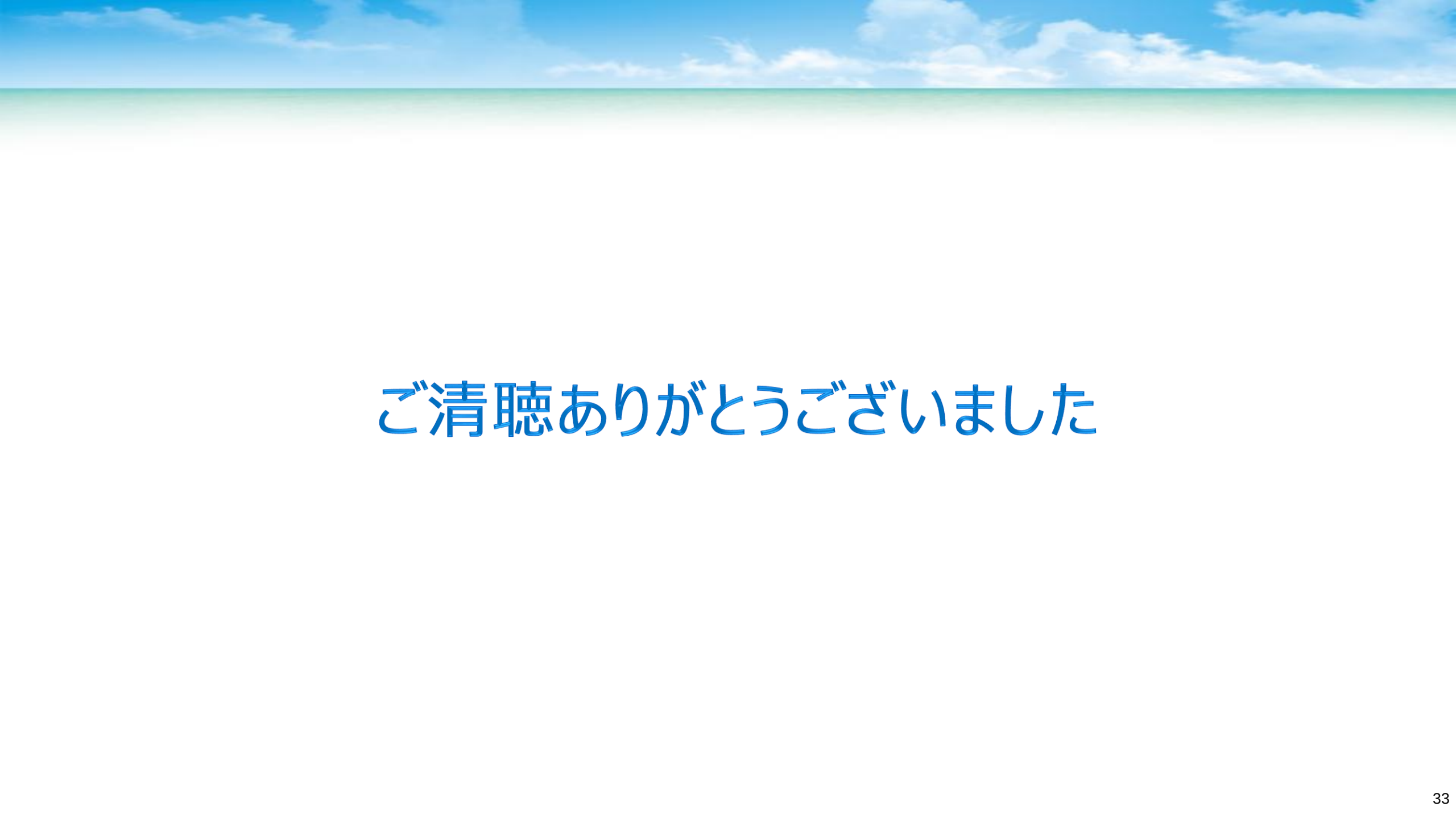


直感的に
操作できます

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。

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。

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

●SKYSEA および SKYSEA Client View は、Sky株式会社の登録商標です。●その他記載されている会社名、商品名は、各社の登録商標または商標です。●本文中に記載されている事項の一部または全部を複写、改変、転載することは、いかなる理由、形態を問わず禁じます。●本文中に記載されている事項は予告なく変更することがあります。