DARKTRACE

医療機関向け_Darktrace ご提案資料

AIを活用したNDR（ネットワーク検知・対応）

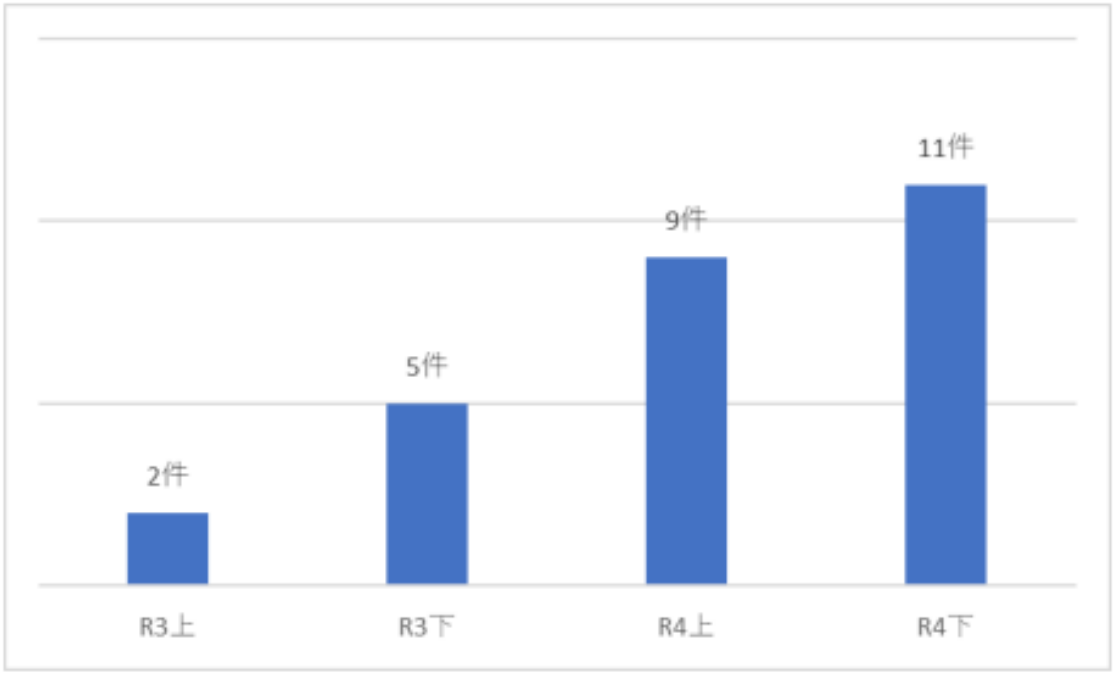
株式会社 アイ・アイ・エム

2024年8月

医療業界のセキュリティ脅威

サイバー攻撃脅威と医療業界のセキュリティ課題とは

電子カルテが閲覧できなくなり、医療活動ができなくなる被害が続発しています



医療・福祉分野におけるランサムウェア被害件数

※参照元：サイバー事案の 被害の潜在化防止に向けた検討会 報告書 2023

2018年10月「奈良県の病院でランサムウェア被害」

電子カルテシステムが使用不可に。復旧まで紙カルテの運用を余儀なくされた。
職員が私物PCでネットワーク機器に接続したことが原因とみられる。

2021年10月「徳島県の病院がランサムウェア被害」

8万5000人分の電子カルテや院内LANが使用不能に。会計システムで診察費の請求ができず、一部の診療科を除き新規患者の受け入れを中止。復旧に2か月を要した。

2022年6月「東京都の病院で院内サーバーがウイルス感染」

電子カルテが閲覧不能に。会計システムも停止したため診療を一部停止し、診療費を後日請求する事態に。

2022年10月「大阪の医療センターでランサムウェア被害」

電子カルテなどが暗号化され、外来診療や各種検査が停止し、復旧に2か月を要した。ランサムウェアの侵入口は給食委託事業者のVPN装置とされる。

医療機関が狙われる理由

セキュリティホールが発生しやすい状況に置かれており、人命を優先で攻撃成功の可能性が高いと想定

高価値な情報

●機密情報の豊富さ

患者の個人情報や医療記録など機微な情報を保有しているため、攻撃者にとって魅力的なターゲットになり得る

●業務停止の影響の大きさ

病院の業務停止は人命に関わるため、解決を急ぐために身代金支払いの可能性が高い

環境の複雑さと医療ICT化

●複雑なネットワーク

多くのデバイスやシステムが相互接続されており、管理が難しく脆弱性が発生しやすくなりがち

●医療機器のセキュリティ

ICT化により多くの医療機器がネットワークに接続されているがシステムの安定稼働のためにセキュリティツールを入れづらい環境である

人的要因

●外部ベンダーの管理

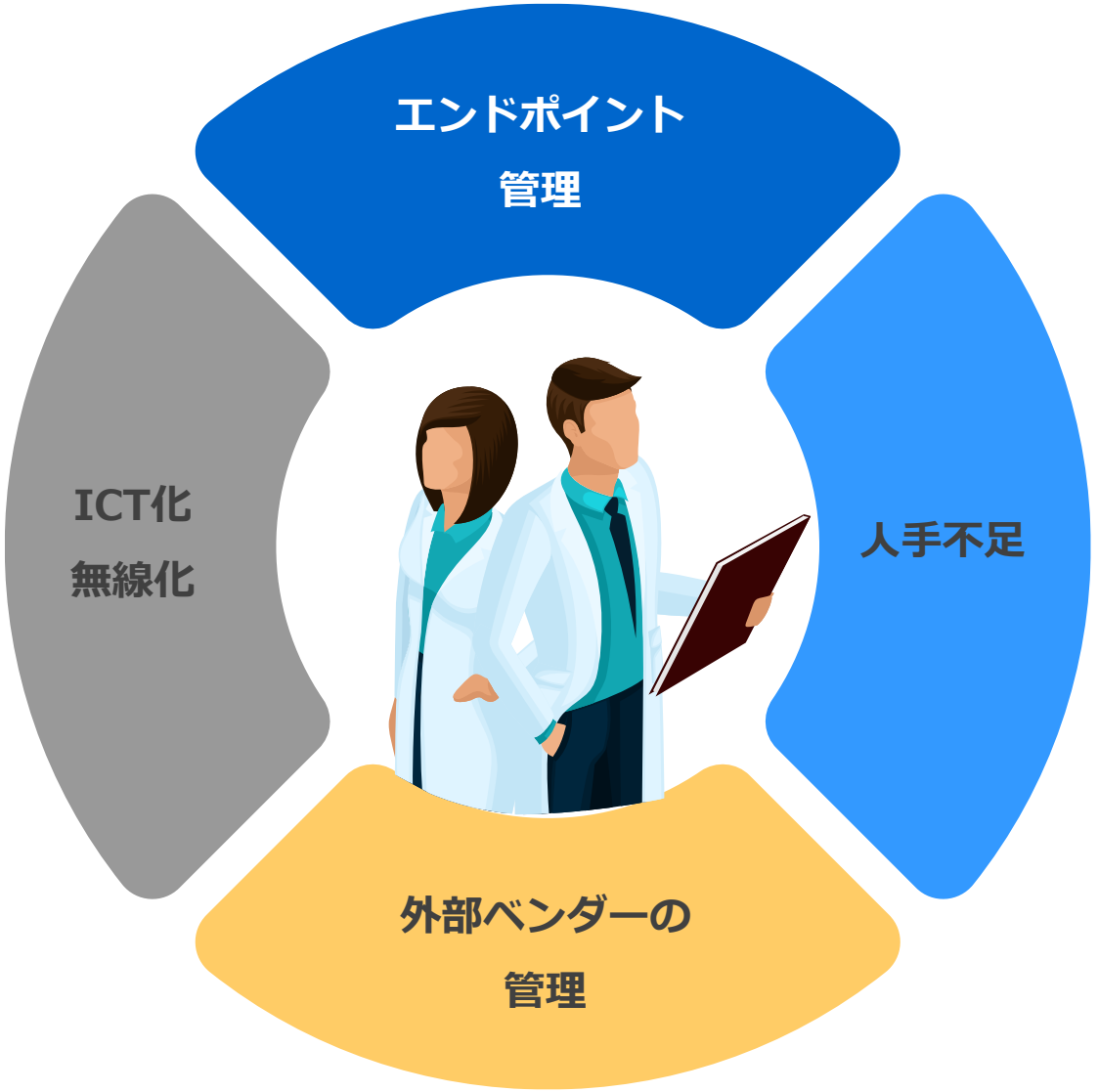
診療業務に関わる多くの外部ベンダーの管理まで手が回らない。セキュリティにおける責任範囲も不明瞭になる場合がある

●セキュリティリテラシーのばらつき

人命救急が最優先で多忙なため、情報セキュリティにまで配慮しづらく、セキュリティリテラシーにばらつきがある

医療機関が抱えるセキュリティ課題

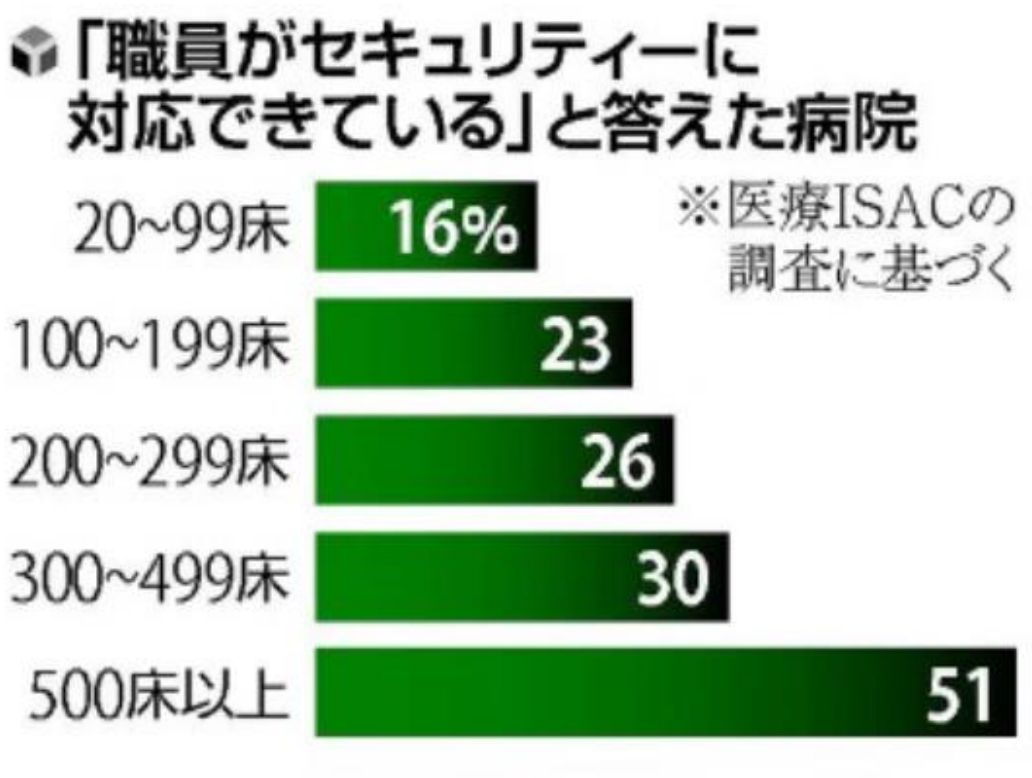
医療機関特有の課題が、セキュリティ課題に繋がっています



人材不足がセキュリティ対策にも影響！医療機関において攻撃者から情報を守る人材は不足しています

セキュリティ対応済と言える病院は
500床以上で約50%程度

医療分野のセキュリティーに取り組む一般社団法人「医療ＩＳＡＣ」が全国の５８６病院から回答を得たアンケートによると、職員がセキュリティーに「対応できている」と答えたのは、５００床以上でも５１％にとどまっていた。



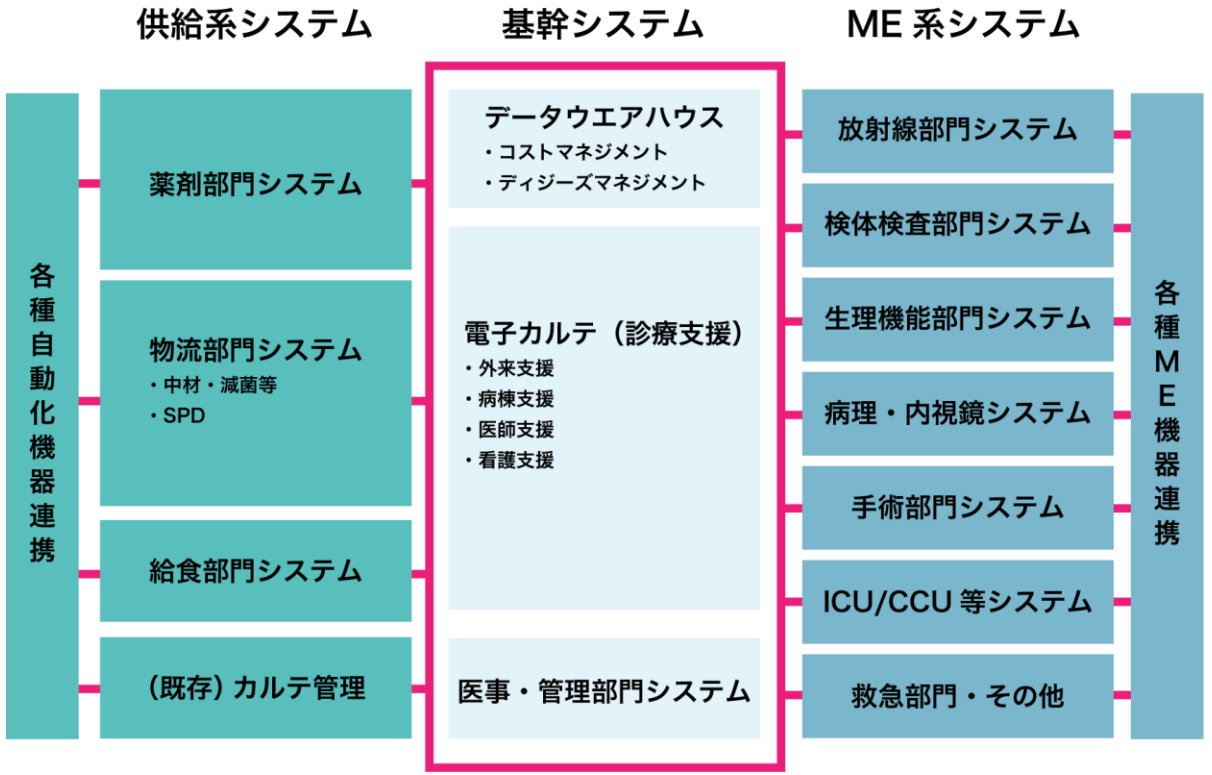
※参照元：医療ISAC調査

ランサム被害対応を任され、慣れない業務と責任の重さに疲弊してしまう担当者も続出しています

診療業務はさまざまな外部ベンダーと連携！外からの接続やベンダー側のセキュリティも重要です

外部ベンダーのセキュリティも重要
外部ネットワーク接続を注視

医療業務は多くの外部ベンダーの連携によって成り立っています。さらに医療のICTにより、外部ベンダーが保守回線を使用し院内ネットワークに入ってくることが増えており、外部接続の状況の把握はもちろん、外部ベンダー側の環境にも注意を払う必要があります。



大阪の医療センターでは、侵害された外部ベンダーの回線から、院内ネットワークに侵入されたことが原因でした

※参考資料

大阪急性期・総合医療センター 情報セキュリティインシデント調査報告書 概要　2023.3.28 調査委員会

本書は、2022年10月31日(月)に大阪急性期・総合医療センターにてサイバー攻撃による大規模システム障害が発生した
ントについて、調査委員会として調査した結果をまとめた報告書の概要である。電子カルテシステムが暗号化された影響
るを得なかったが、同年12月12日に電子カルテサーバーが再稼動し、翌年1月11日に診療機能が完全復旧した。

医療インシデントに多く見られる外部ベンダーからの侵入例

◆調査結果から推定される攻撃者の手順　（調査報告書11～12頁）

No	項目	攻撃者の手順
1	給食事業者に侵入	給食事業者が設置・運営する給食システムに、情報基盤構築事業者がリモート保 器の脆弱性を用いて侵入（漏洩され公開されていたID・パスワード情報を用いて侵
2	給食事業者内探索・情報窃取	給食事業者内データセンターのID・パスワードが脆弱だったことから、攻撃者に容易に不正アクセス その後、システム情報（IPアドレスやパスワード情報など）を窃取されたため給食事業者内での攻撃拡大。
3	病院給食サーバー侵入	給食事業者の端末から窃取した病院のサーバーの認証情報により、RDP通信を用いて、病院給食サーバーに侵入。ウイルス対策ソフトのアンインストールも実施。
4	病院内のシステム情報の窃取	病院給食サーバーを踏み台に、病院内の他サーバーの認証情報をツールを用いて窃取。 なお、病院給食サーバーと他サーバーのID・パスワードは共通で窃取は容易。
5	他サーバー侵入	病院給食サーバーで窃取した他サーバー認証情報により、電子カルテシステムなどの基幹システムや他のシステムのサーバーに侵入。
6	クライアントへのログオン試行	侵入されたサーバー等を経由して、クライアントにログオン試行した可能性。
7	ランサムウェア感染	各サーバーでランサムウェア感染、永続化を行い、ランサムノート（身代金要求文書）を表示

◆被害状況　（調査報告書11頁、21頁、28頁、40～41頁）

No	項目	被害内容
1	電子カルテを含む総合情報システム	基幹システムサーバーの大部分がランサムウェアにより暗号化。PC端末（院内に約2,200台）も不正アクセスの痕跡あり。 ⇒全てのサーバ、端末をクリーンインストール 基幹システムサーバ再稼働に43日間、部門システム含めた全体の診療システム復旧に73日間を要す
2	診療制限	2022年11月の診療実績　（前年同月対比）　※2022年12月は現在計算中 新入院患者数：558人（前年同月比33.3%）、延入院患者数：10,191人（前年同月比52.9%） 初診患者数　：465人（前年同月比17.9%）、延外来患者数：15,744人（前年同月比61.6%）
3	被害額	現在精査中　調査・復旧費用で数億円以上 診療制限に伴う逸失利益として十数億円以上を見込んでいる

※転載：大阪急性期・総合医療センター 情報セキュリティインシデント調査報告書 概要 2023.3.28 調査委員会

電子カルテなどの稼働を邪魔しないようにセキュリティツールの導入が後手になり攻撃を受けるケースも

医療システムの稼働を妨げないように
エンドポイントセキュリティが後手に

電子カルテシステムや業界特有の辞書アプリなどが端末にインストールされていますが、医療行為を妨げないように不要なアプリケーションのインストールやセキュリティツールで重たくなる製品は避ける必要があります。

導入済でも、アップデートで端末が重たくなるため、アップデートを行っておらず攻撃を防げないトラブルも･･･

※参考資料

エンドポイント管理をしなかったケース

逸失利益は数十億円規模！サイバー攻撃で診療停止の大阪の病院、復旧まで2カ月

電子カルテシステムを稼働させていた基幹システムサーバがランサムウェアで暗号化。診療制限となり、完全復旧したのは約2か月後。被害額は調査～復旧で数億円、診療制限で十数億円に及ぶと想定される。
原因はさまざまで、VPNの脆弱性を放置していたり、アンチウイスが未導入だったり、ID・パスコードの使いまわしなどが後に発覚している。

エンドポイント管理をしたケース

大規模システム障害で全世界で大混乱
アンチウイルスのバグでブルースクリーン

アンチウイスのWindows版に提供されたアップデートファイルにバグが発生。このバグにより世界中のWindows搭載PCがブルースクリーンに。世界で850万台のWindows端末が影響を受けたと発表。米国では金融や医療、外食、製造など主要業界が軒並み影響を受けた。

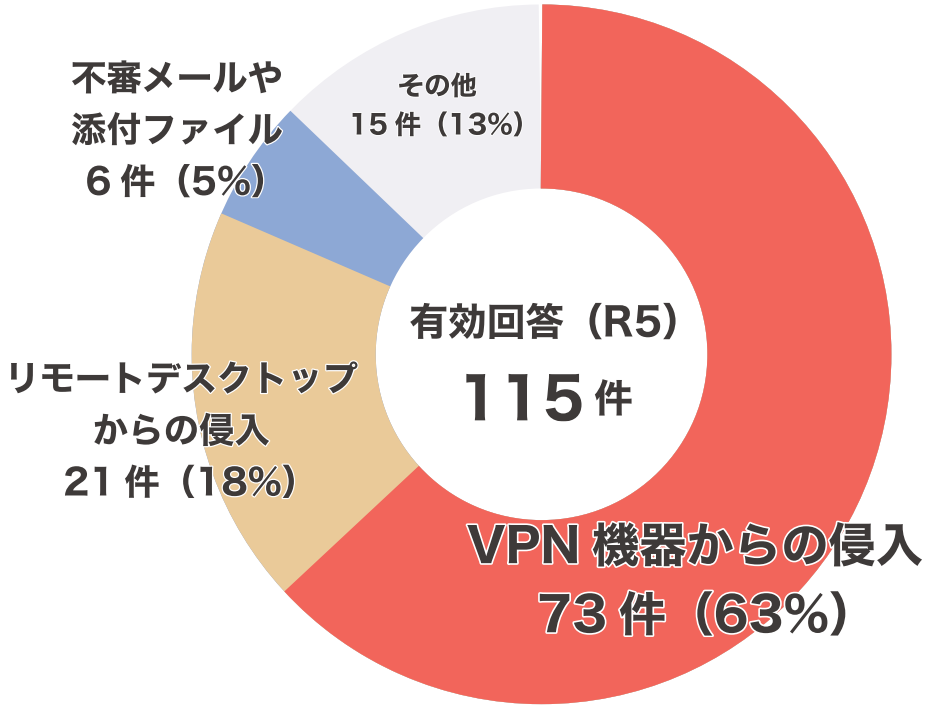
エンドポイント管理は必要だが、影響を受けないセキュリティ製品選定が重要

さまざまな機器が電子カルテに無線でデータ転送！
セキュリティツールが入らない機器の監視も重要です

ICT化・無線化によりセキュリティが必要な機器も多様化

電子カルテ端末の無線化やPC・タブレットで問診することが増加。バイタル機器なども無線に繋がり、検知結果をHISに飛ばすなどICT化が進展。これら繋がっている機器にもセキュリティが必要ですが、端末自体にアンチウイルスなどのセキュリティ対応が施せない機器も多くあり、対策が必要です

企業・団体等における感染経路



参照：警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」

バイタル機器などアンチウイルスなどがインストールできない機器は、セキュリティホールになる可能性が･･･

国も医療機関にサイバーセキュリティを義務化

立入検査を実施！医療機関で「サイバーセキュリティ対策」が義務化（医療法施行規則改定）

医療法施行規則第 14 条第２項（新設）

病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティを確保するために必要な措置を講じなければならない。

検査の基準となる必要な措置は「最新の医療情報システムの安全管理に関するガイドライン」

立入検査でセキュリティ対応も検査対象となります（医療法第２５条第１項・医療法第２５条第３項）

厚労省側

- 都道府県
  保健所設置市 等
- 地方構成（支）局

- 病院（毎年）
  有償診療所（3年に1回）
  無償診療所・助産所（随時）
- 特定機能病院（毎年）
  臨床研究中核病院（毎年）

医療機関側

※引用：昭和二十三年厚生省令第五十号　医療法施行規則 ／ 医療法施行規則の一部を改正する省令の施行等について　／医療法第25 条第1 項の規定に基づく立入検査要綱の改正

攻撃者は攻撃成功のためにさまざまな手段を尽くします。貴院は対策できていますか？！

落とし穴 1

時間外や夜間・休日が狙われる

IT運用管理者の監視が手薄になる深夜や祝日、連休などのタイミングを狙ってきます。

攻撃された際に
すぐに対策できますか？

落とし穴 2

バックアップファイルも消される

先ずバックアップファイルを削除してきます。

後で復旧すればいい
と思っていませんか？

落とし穴 3

思わぬところから侵入される

まずは院外の環境から侵入し、その後に病院ネットワークへ侵入します。

すべての侵入経路を監視できていますか？

落とし穴 4

展開のスピードが非常に早い

手作業の対処では到底間に合わない「マシンスピード」で展開・目的実行します。

手作業で対応できると
思っていませんか？

医療業界のサイバーセキュリティに最適解

AIネットワーク脅威検知「Darktrace」

AI型ネットワークセキュリティ

内部へ侵入してくる脅威をAIがネットワークで網羅的に監視・検知・対処

DARKTRACE

NDR 国内市場シェア No.1※

Darktraceはネットワーク機器に流れるトラフィックを基に、AI（機械学習）を活用して、ネットワークに接続した様々なデバイスやユーザーの行動パターンを学習・分析することで、未知のサイバー攻撃や内部不正の兆候を検知します。

- AIアナリスト
- 未知の攻撃検知
- 内部不正検知
- エージェントレス
- ネットワーク可視化
- 不正通信の自動遮断

https://www.lanscope.jp/professional-service/service/product/darktrace/

Darktrace開発企業「Darktrace社」とは

生物の免疫(immune)が、外的や環境変化に対抗するような仕組みをITセキュリティシステムに適用

AIネットワーク脅威検知

DARKTRACE

ケンブリッジ大学の数学者と、英国の国家サイバーセキュリティに携わったメンバーで2013年に設立

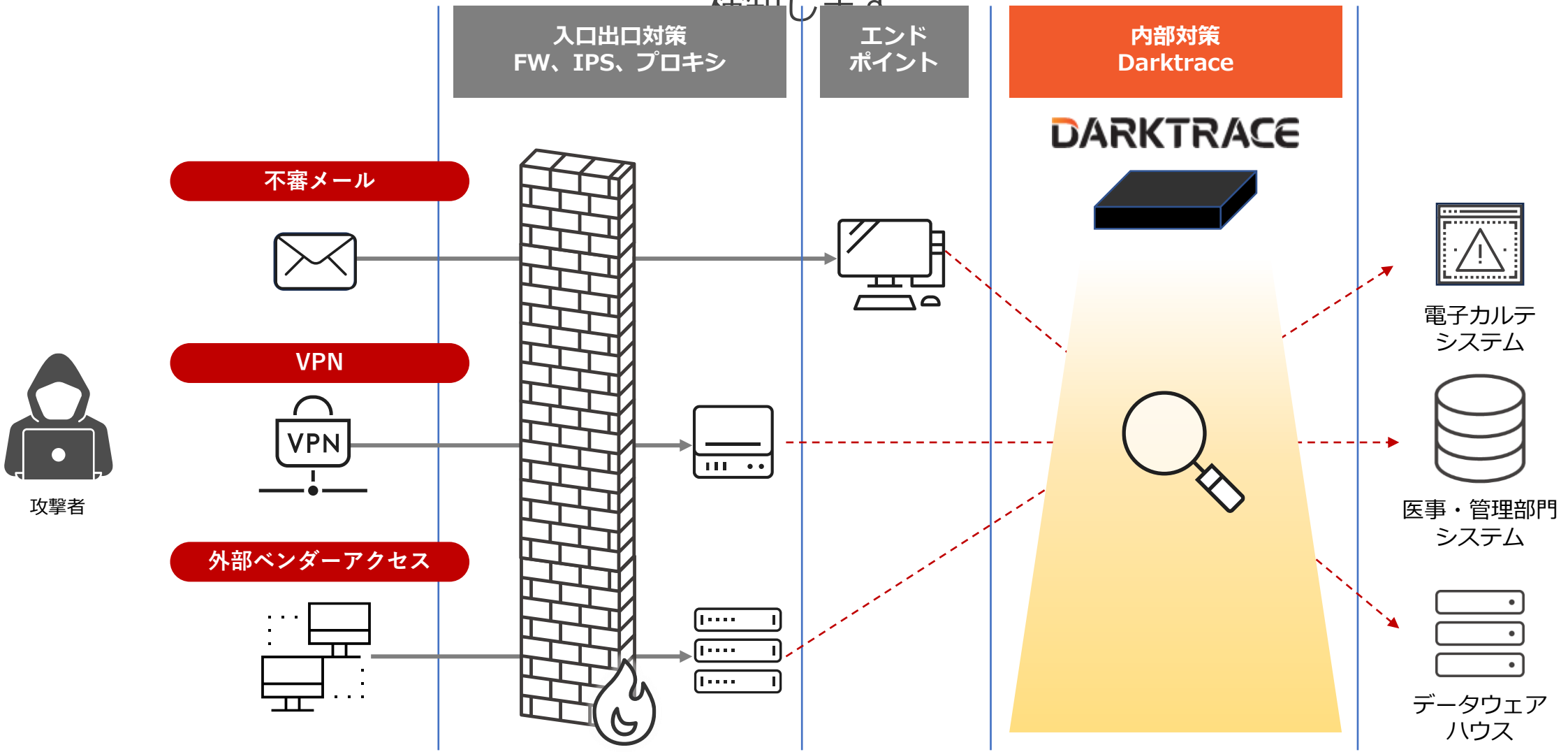
英国ニュース紙「TIME」において、世界で最も影響力のある100社に選ばれる

英国政府主催「AI安全サミット」にサイバーセキュリティ専業企業として唯一招待（2023年）

https://darktrace.com/ja

Darktraceの監視領域

ネットワーク機器に流れるトラフィックを分析し、外部からの攻撃や内部不正などの兆候を可視化・検知します



医療業界を狙うセキュリティインシデントを検知・対策

対応が難しいゼロデイ・標的型攻撃などの外部脅威に加え、内部脅威(不正)にも幅広く手を打つことが可能

医療機関が抱えるセキュリティ課題を解決

IIM

院内全体が監視範囲

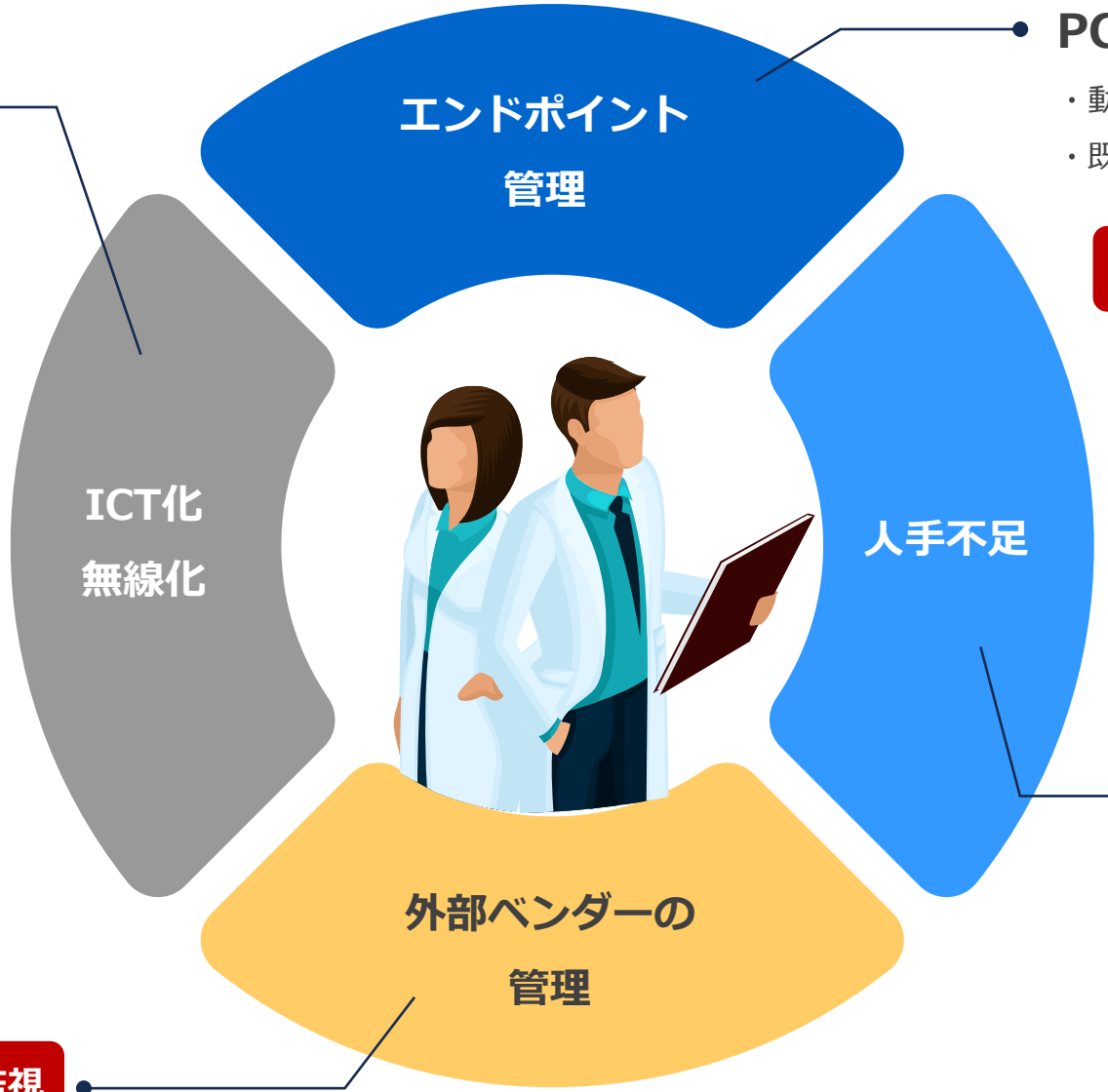
・ネットワークから情報収集
・デバイス種別に関係なく監視分析

医療機器・IoT機器も監視

PCへのインストールが不要

・動作遅延は一切発生しません。
・既存環境やシステムと一切干渉しません

医療業務への影響・負荷ナシ



不正な挙動も監視

・外部ベンダーの挙動も監視
・通常業務とは違う挙動を即座に警告
・接続遮断も可能

外部からの脅威もリアルタイム監視

AIがセキュリティ担当者

・AIが各病院の特徴を自律的に学ぶ
・24時間365日休まず院内を監視
・攻撃をマシンスピードで遮断

高度なセキュリティ人材に

SEIKO GROUP

IPA「情報セキュリティ10大脅威」にも対応

Darktraceはサイバー攻撃などの外部脅威以外の、内部不正・院内リスクにも対応できます

情報セキュリティ10大脅威2024

順位	組織	Darktraceの対処
1位	ランサムウェアによる被害	さまざまなランサムウェアの予兆を検知、自動対処
2位	サプライチェーンの弱点を悪用した攻撃	取引業者、保守業者や海外拠点などからの通信でも、普段とは異なる不審な通信を検知・対処可能
3位	内部不正による情報漏えい等の被害	珍しい外部宛先へのデータアップロードや、普段とは異なるファイルサーバへの不審なアクセスなどを検知・対処可能
4位	標的型攻撃による機密情報の窃取	稀な宛先からのリモートアクセスや、ポートスキャン、管理者権限の行使など、通常と異なる行動を検知・対処可能
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	ルール・シグネチャでは対策できないゼロデイ攻撃でも脅威性のある珍しい挙動として検知・対処可能
6位	不注意による情報漏えい等の被害	標的型攻撃メールのURL（添付ファイル）から派生する不審な宛先への通信、不審なExeファイルのダウンロードを検知・対処可能
7位	脆弱性対策情報の公開に伴う悪用増加	ランサムウェアで標的とされやすい脆弱性のあるプロトコルの残存などの通信も検知可能
8位	ビジネスメール詐欺による金銭被害	攻撃と疑われるメールの検知、ブロックが可能（オプション：Darktrace/Email）
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	遠隔地や在宅勤務などの環境も検知・対処可能（オプション：Darktraceクラウド）
10位	犯罪のビジネス化（アンダーグラウンドサービス）	RaaS (Ransomware as a Service)でも1位と同様検知・対処可能

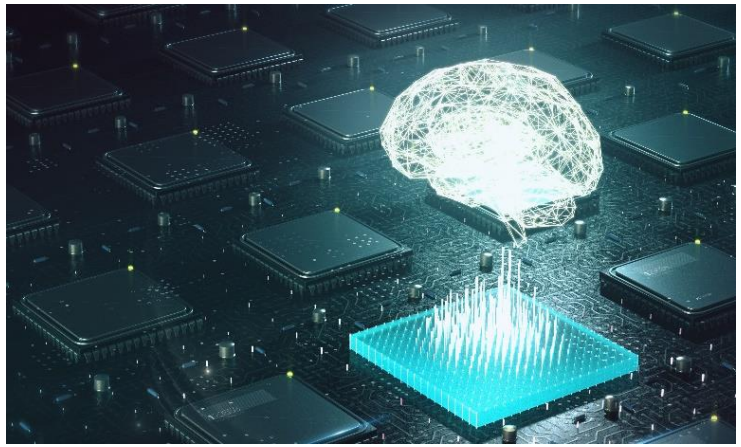
※IPA 情報セキュリティ10大脅威 2024を元に作成

Darktraceの特長

ネットワークに接続するだけで簡単に導入可能！AIがネットワーク全体を可視化し未知の脅威を検知

AIによる脅威検知・遮断

AIによる「教師なし機械学習」で検知
問題抽出から対策提案や自動遮断を実施



通常の業務パターンに外れた挙動をスコアリングして検出（ホワイトリスト型検知）
AIが**関連脅威単位で自動トリアージ・対応策を提示・自動遮断**

監視領域が広い

監視ツールが未導入な機器も可視化
外部脅威・内部不正・怪しい挙動も検知

エンドポイント管理ツールが導入できないIoT機器やレガシーOSなどもエージェントレスで監視可能。外部からの攻撃に加え、**内部の不正も検知時可能。**

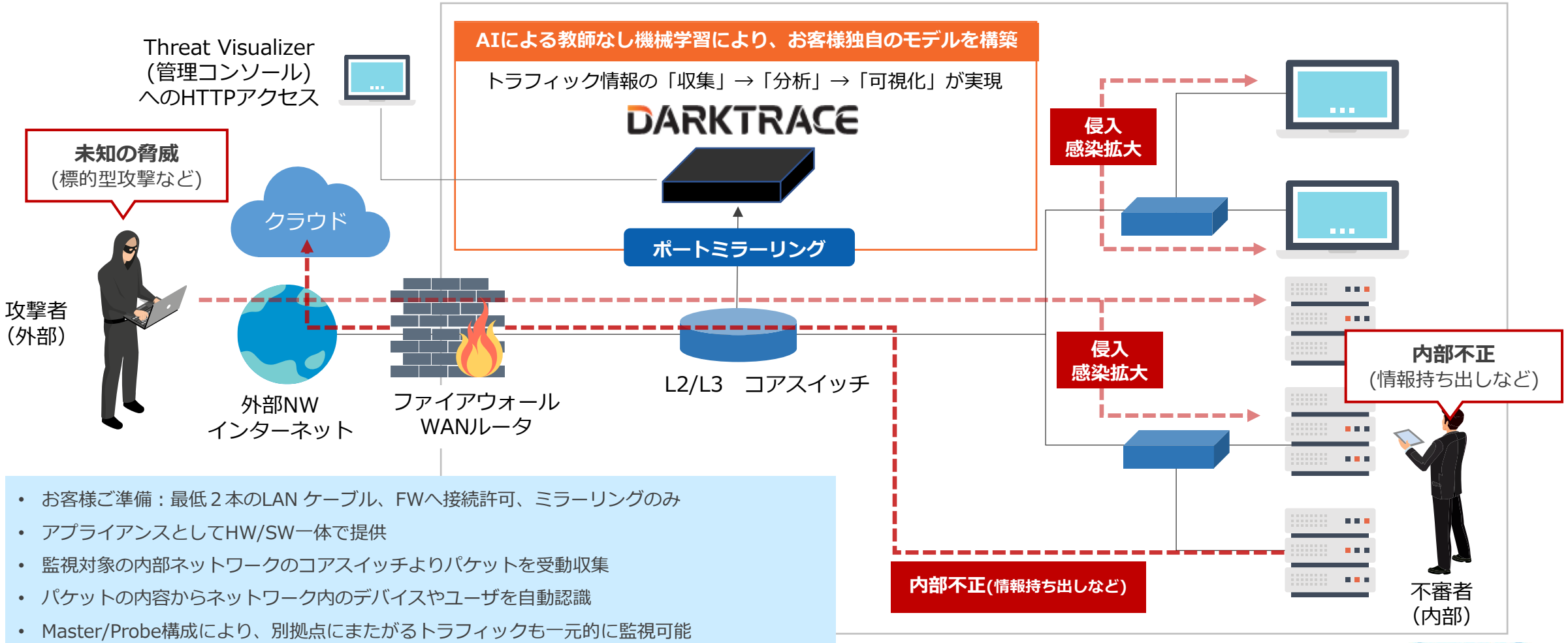
管理者・環境負荷が少ない

既存ネットワークに影響を与えず
アップデートチューニングが不要

今の環境を変えず、**他システムに影響を与えない。**導入後もAIの自律的学習により自動でチューニングするため、**アップデートの手間がなく管理者負担が少ない**

トラフィックをポートミラーリングで流すだけ！ルール定義・詳細設定不要で他システムへの影響はなし

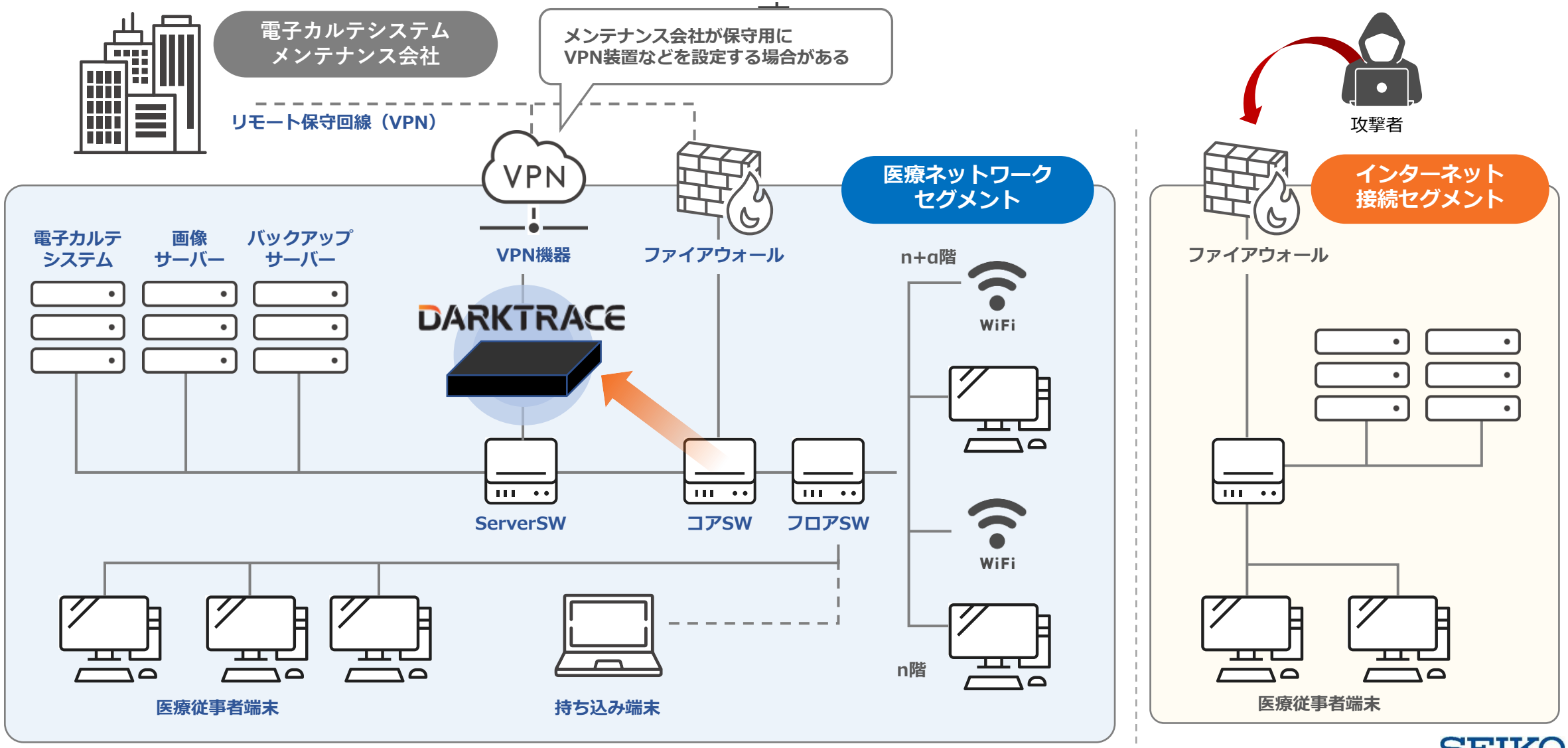
ネットワーク機器に流れるトラフィックを基にAIを活用しサイバー攻撃や内部不正の兆候を検知
ネットワークに接続した様々なデバイスやユーザーの行動パターンを学習・分析します



- お客様ご準備：最低２本のLAN ケーブル、FWへ接続許可、ミラーリングのみ
- アプライアンスとしてHW/SW一体で提供
- 監視対象の内部ネットワークのコアスイッチよりパケットを受動収集
- パケットの内容からネットワーク内のデバイスやユーザを自動認識
- Master/Probe構成により、別拠点にまたがるトラフィックも一元的に監視可能

Darktrace構成図（医療機関の最小構成イメージ）

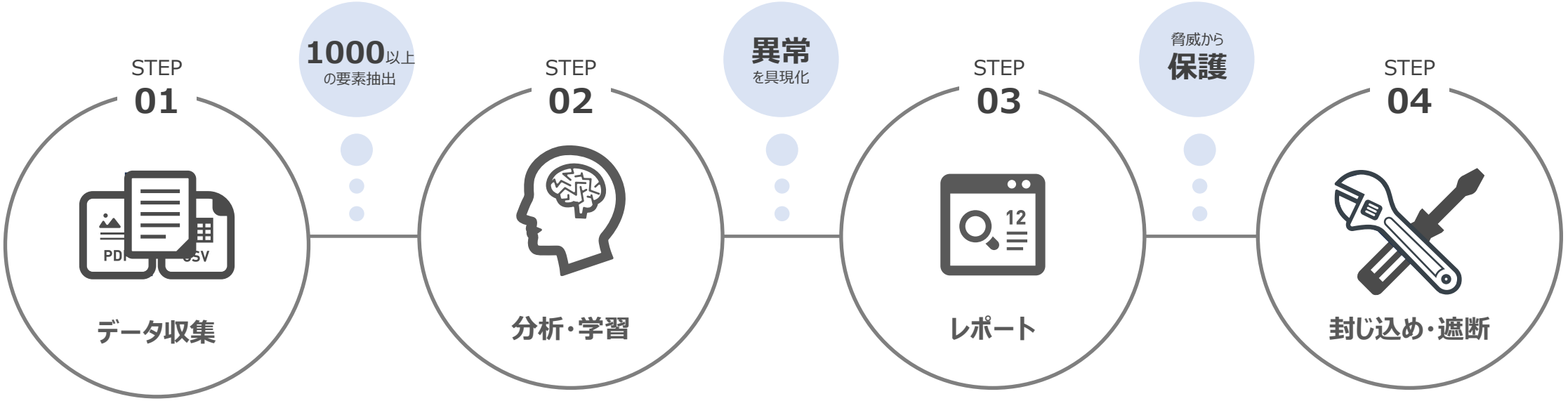
クローズドの環境でも保守などで外部ベンダーの接続が発生するため、医療でよく用いられる構成で



※ServerSWへ接続しているルータ等がある場合でコアSWを通過しない通信は把握できません

Darktraceの脅威検知

AI（機械学習）によって、平時（モニタリング）と有事（インシデント対応）を強力にサポート



あらゆる通信をキャプチャ

リアルタイムに
ネットワーク全体解析

AIによる分析・検出

ルールや事前設計に依存せず、
移動分析・学習を自立して継続。
通常の挙動を学習し、
通常と異なる挙動を検出

インシデントレポート

不審な挙動・攻撃の時系列を
トラッキングし
関連する挙動を自動で紐づけ
対応策を提案

リアルタイムに対処

数秒以内に攻撃を封じ込め
リアルタイムに遮断
スマホで再接続指示が可能

DETECT（検知）

RESPOND（自動対処）

※オプション機能です

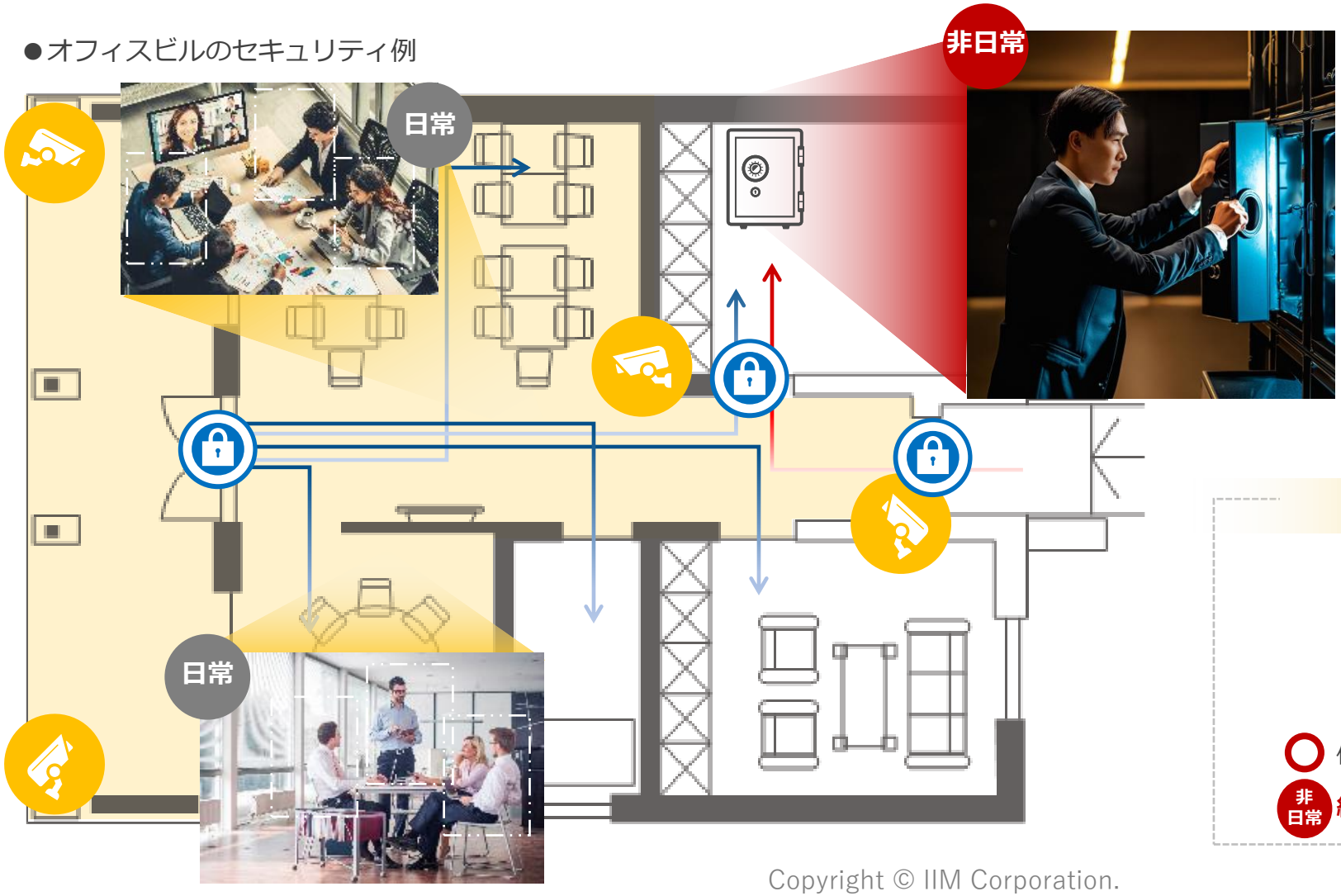
DarktraceのDETECT（検知）とは

DETECT

24時間365日、常時AIが院内環境を継続的に学習・監視！普段と異なる挙動に対して検知します

自己学習型AIを搭載した「院内ネットワーク内の監視カメラ」のような存在です

●オフィスビルのセキュリティ例



内部の悪意ある人間が巧妙に侵入、ドアや金庫の鍵や暗証番号が漏洩した場合、気づける？

DARKTRACE の検知方式

・普段より口数が少ない、もしくはよく喋る
・業務上、金庫には月1回しか入らないのに今日は5回も入っている
・知っているはずのことを周りに聞いている
・今日だけなぜか裏口から入っている等々を捉える

医療現場に当てはめると・・・

○ 伊藤先生は院内で画像管理サーバへアクセスする

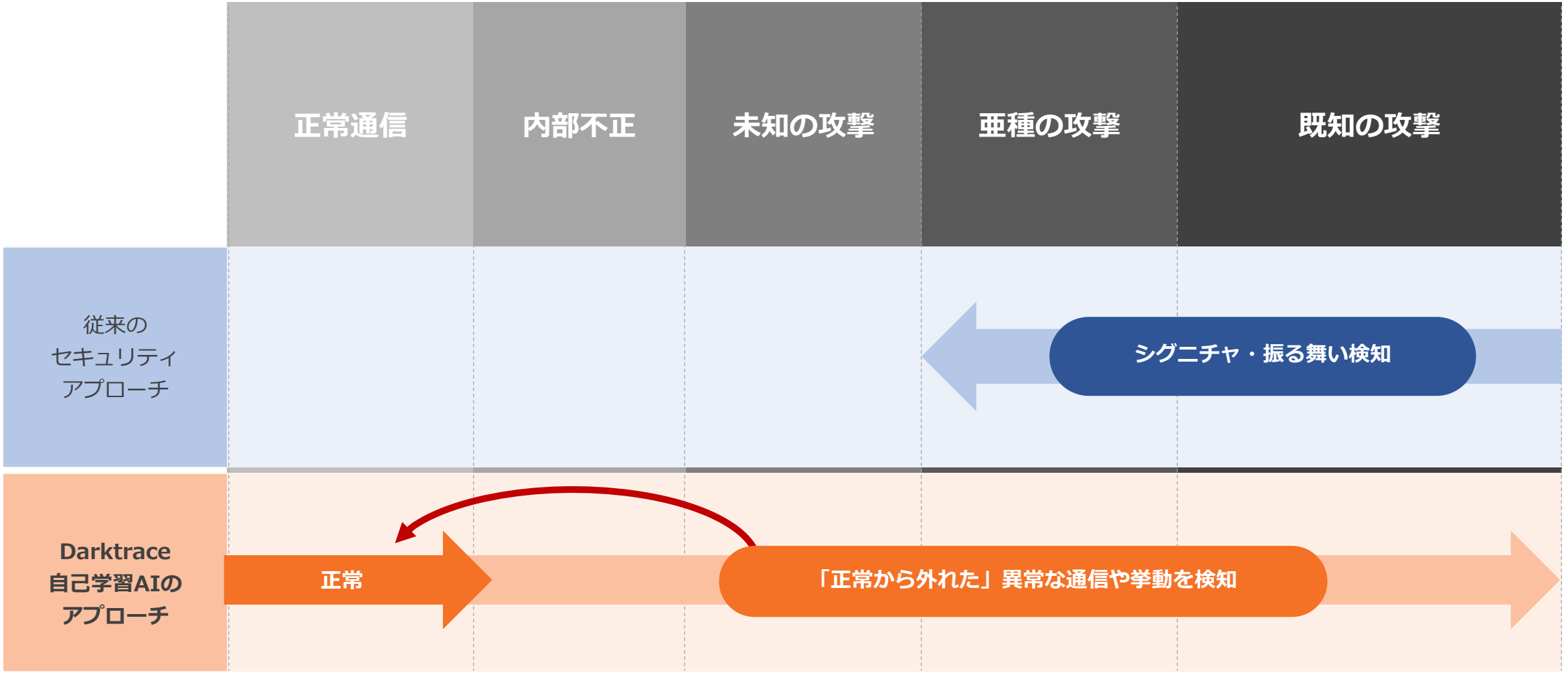
非日常 **給食管理サーバーから画像管理サーバーへアクセスする**

DarktraceのDETECT（検知）　従来型との違い

DETECT

Darktraceはシグニチャではなく普段を正常として脅威検知を行うため、未知やゼロデイ攻撃にも有効です

●脅威種別に対対するアプローチMAP



DarktraceのDETECT（検知）大変なアラート管理もAIが効率化

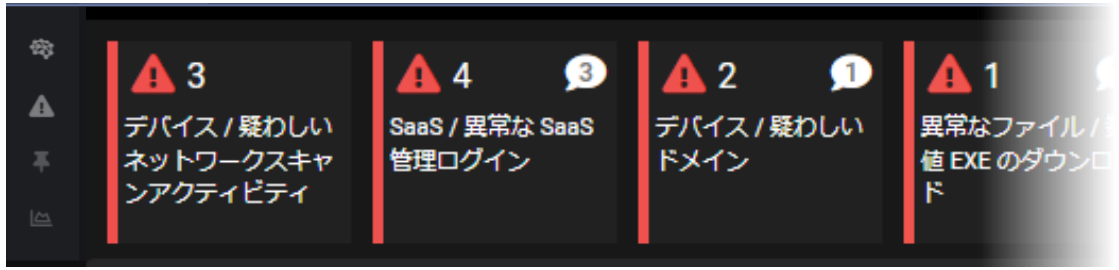
DETECT

膨大なアラートをAIが自動で脅威分析・トリアージ！「多種多様な脅威の検知」と「運用の省力化」が可能

1）教師なし機械学習で異常を検知

院内ネットワークすべてにおける

さまざまな起点の脅威検知が可能な検知アプローチ

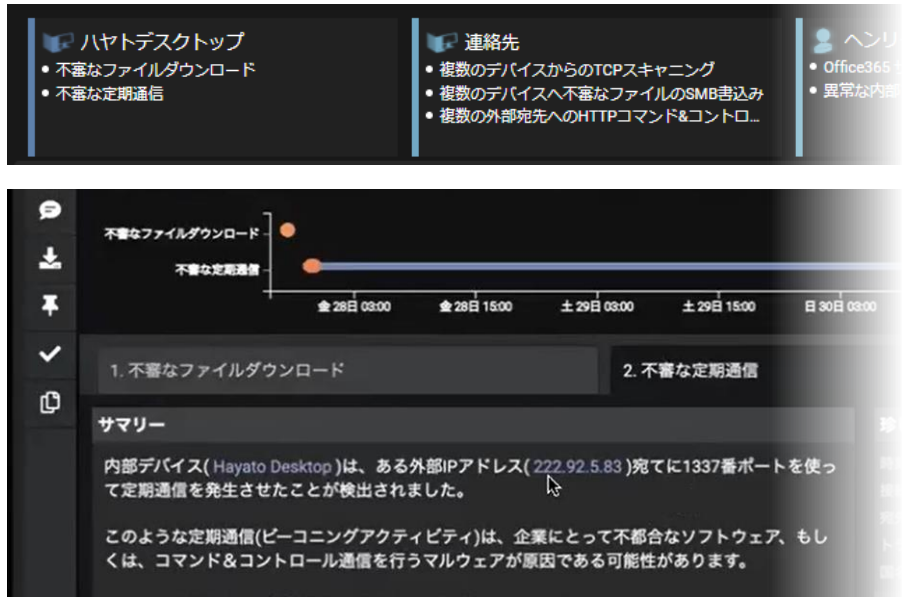


- 異常 ＝「いつもと異なる」「周りと異なる」挙動を検知
- 攻撃を受けると「必ず**「いつもと違う挙動」が発生**
- 外部や内部からの脅威を見逃さない

2）検知した異常を自律的にトリアージ

重要なインシデント対応に**専念できる**

運用の省力化が可能



- セキュリティアナリストの分析手法を学んだ独自AIが**関連する脅威単位に自律的にトリアージ**
- AI作成の日本語レポートをもとに**素早く**判断、効率的に対処可能へ

SEIKO GROUP

AIが自動で脅威を分析、トリアージ「 サイバーAIアナリスト」

DETECT

大変なアラートの脅威判定や影響調査をAIが脅威レベルを自動で判別・自動的に詳細レポートを生成します

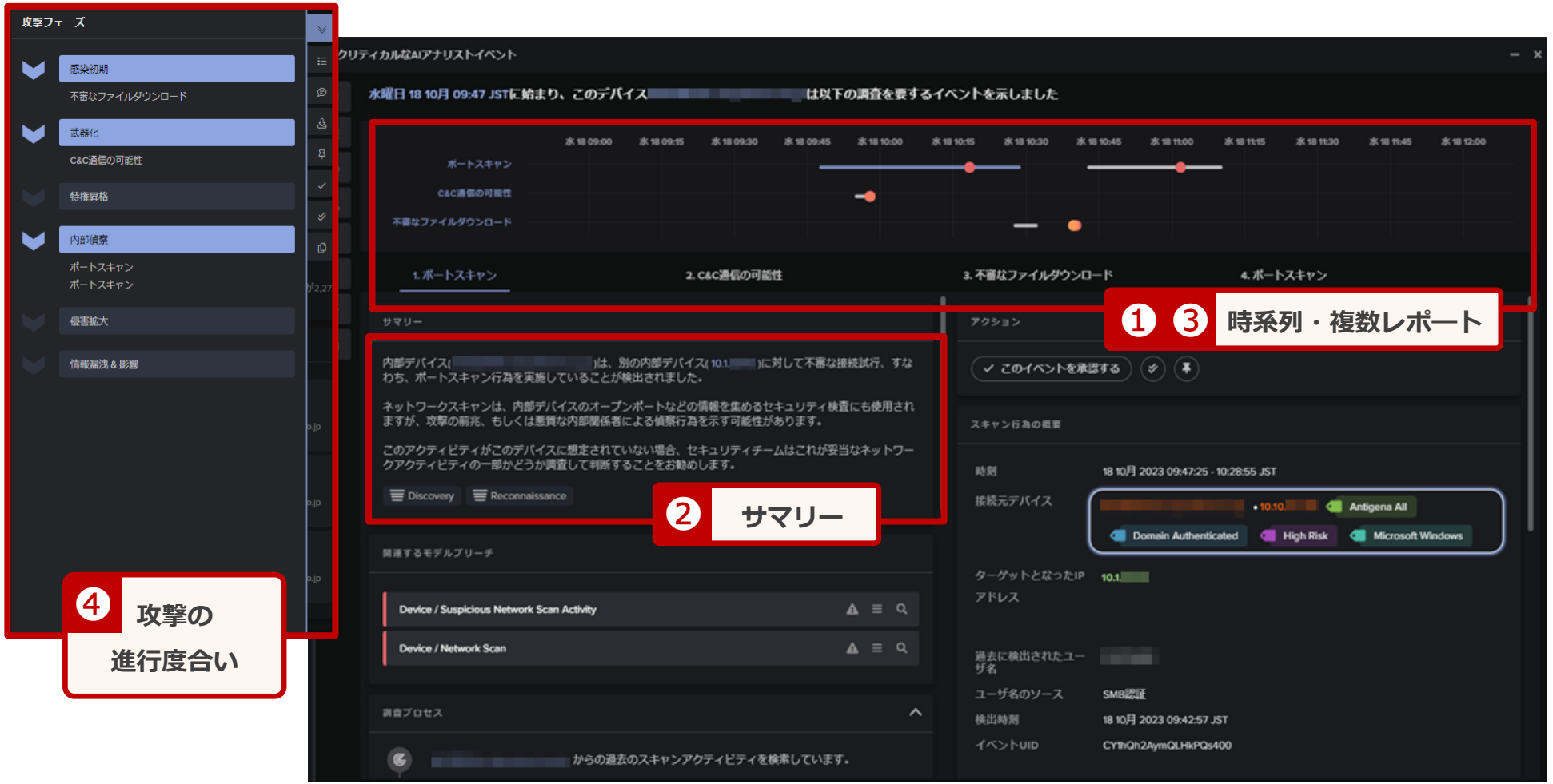
内部ネットワーク内で過去に発生していない珍しい通信として検知、このような未知の通信も、Darktraceは予兆レベルで検知可能

①イベントフローの可視化
関連性の高いイベントを
攻撃フェーズ毎に自動的に
関連付け

②自動的にレポートが生成
生成されたレポートを元に
関連部門と容易に連携可能
日本語対応済

③対応時間の削減
複数アラートを
1つのレポートで対応

④攻撃度侵攻度を可視化
Cyber Kill Chain FWに沿っ
てわかりやすく表示



SEIKO GROUP

LockBitが侵入！2日目・3日目の深夜時間帯にファイルの暗号化が実行を検知

攻撃の詳細を把握し、侵入状況を把握し、2次被害の抑制に活躍

さまざまなランサムウェア関連のモデルブリーチが発生

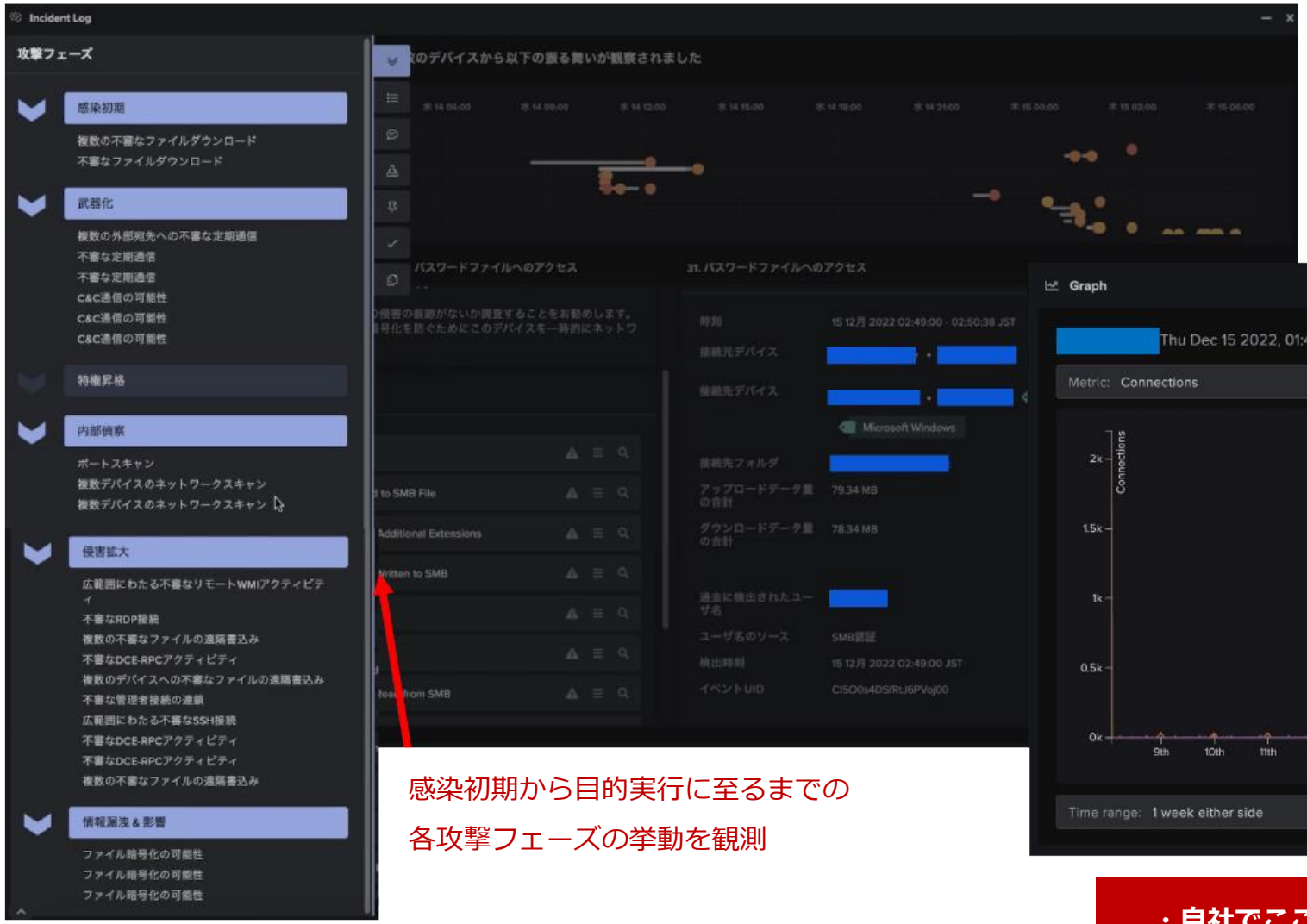
❶大量のレポートが生成。表示は21～24件目だが、さらに右側には表示されていないレポートがある

❷AIの調査結果として、ファイル拡張子に「.lockbit」が付加されて名前が変更されていることが報告されている

❸[Restore-My-Files.txt]というタイトルの脅迫状が、影響を受けた各ディレクトリにドロップされている

- **一目で脅威の状況が分かる**
- **RESPONDがあれば、ここまで侵入される前に遮断できる**

DETECT検知例「LockBit感染」



感染初期から目的実行に至るまでの
各攻撃フェーズの挙動を観測

短時間で多くのアラートが生成されている

・自社でここまでできるためコンサル費用の大幅削減
・2次被害の抑制に成功

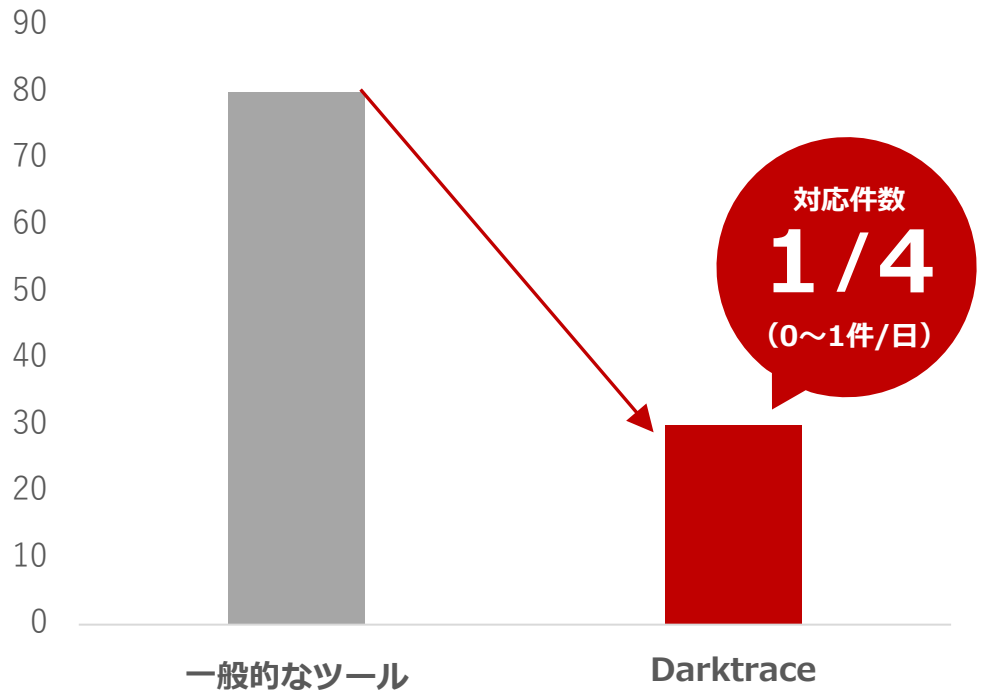
DarktraceのDETECT（検知）　DarktraceAIがセキュリティ工数を削減

DETECT

ネットワーク全体と監視範囲が広いにも関わらず、調査工数は大幅に削減できます

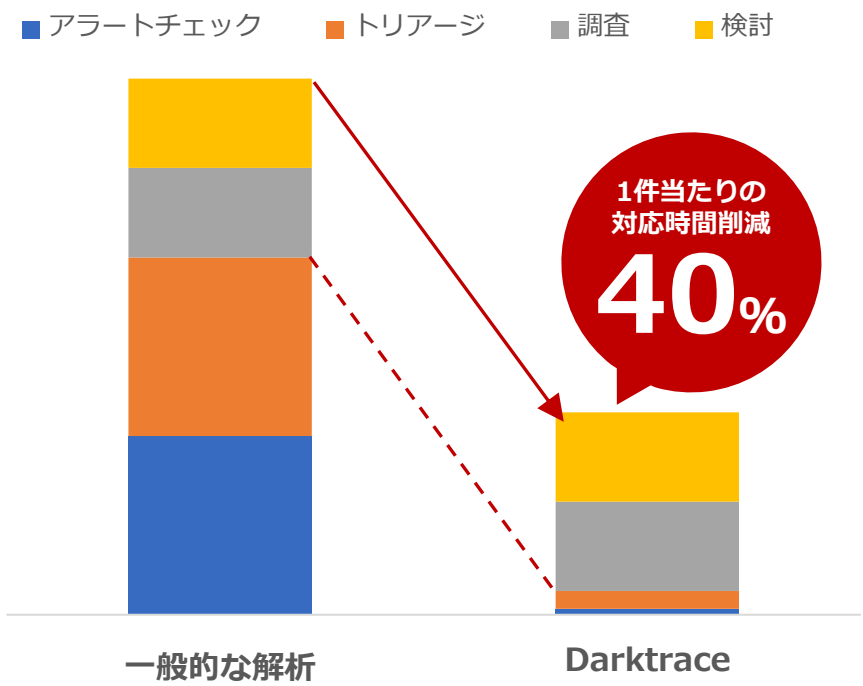
アラート対応件数が大幅縮小

1日あたりのアラート対応件数比較
※1,000台環境



調査時間の大幅削減

1件あたりの調査時間比較



※Darktrace社調査結果より

SEIKO GROUP

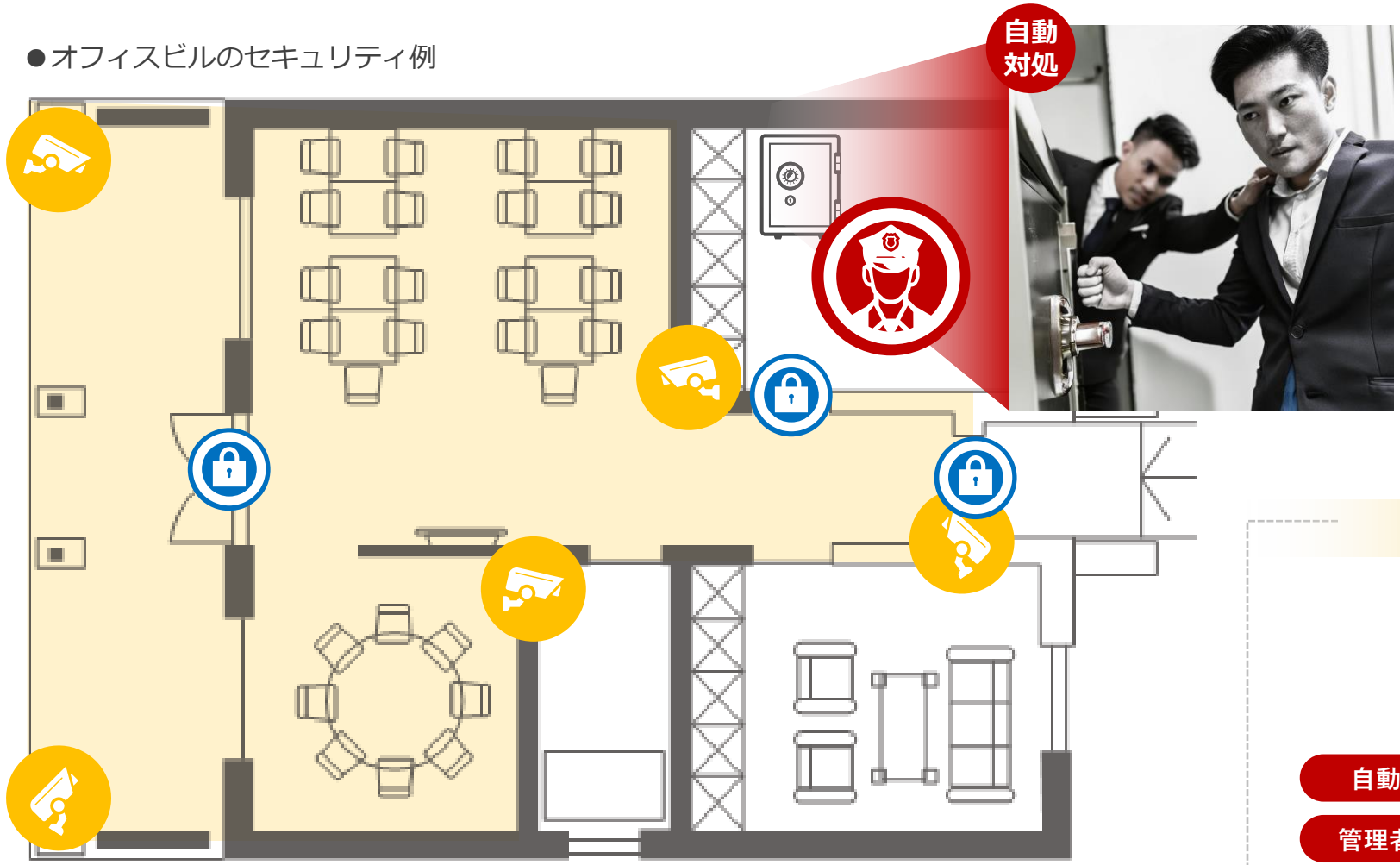
DarktraceのRESPOND（自動対処）とは

RESPOND

24時間365日常時待機するAI警備員！脅威性の高い挙動を即時に止めることができます

24時間365日、常時AIが「貴院」環境を継続的に学習・更新し、個々の病院にとって最適なサイバーセキュリティ体制を自律的に実現します

●オフィスビルのセキュリティ例

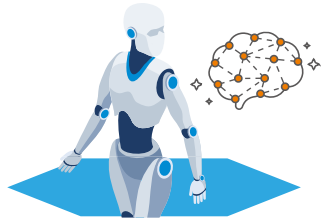


違法が行われた際に
すぐに駆け付けて防ぐ事ができますか

DARKTRACE の検知自動対処

・金庫室の侵入は24時間365日監視・通知される
・ホームセキュリティが5分以内に駆け付ける
・犯人を逮捕して警察に突き出す

医療現場に当てはめると・・・



自動遮断 外部から今まで接続のないIPが接続してきた

管理者通知 深夜に外部ベンダーがアクセスしてきた

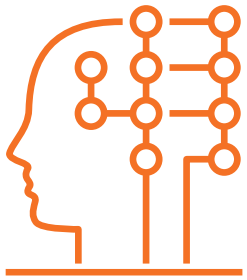
SEIKO GROUP

DarktraceのRESPOND（自動対処）とは

RESPOND

24時間365日監視・遮断対応が可能！遮断後は、どこにいても・いつでも再接続指示ができます

24時間365日
自律遮断

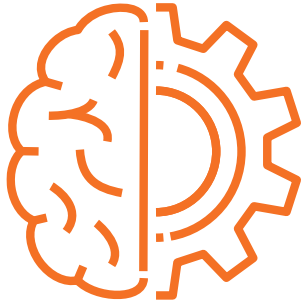


AIが院内ネットワークを

24時間365日監視

自律的に自動遮断

遮断設定の
カスタマイズ



特定の時間・デバイス・

イベントに対してなど

柔軟に設定可能

モバイルアプリから
遠隔管理可能

自律遮断発生時も

モバイルアプリ経由で

確認・**再接続を指示**も可能

RESPOND

自動遮断の設定は2タイプ！普段通りの動きを維持強制させるだけなので業務影響はでません

不審通信の疑いがある通信先のみ通信を自動遮断するため、通常業務に影響を与えない設計思想です

（１）DarktraceのRSTパケット※による自動遮断

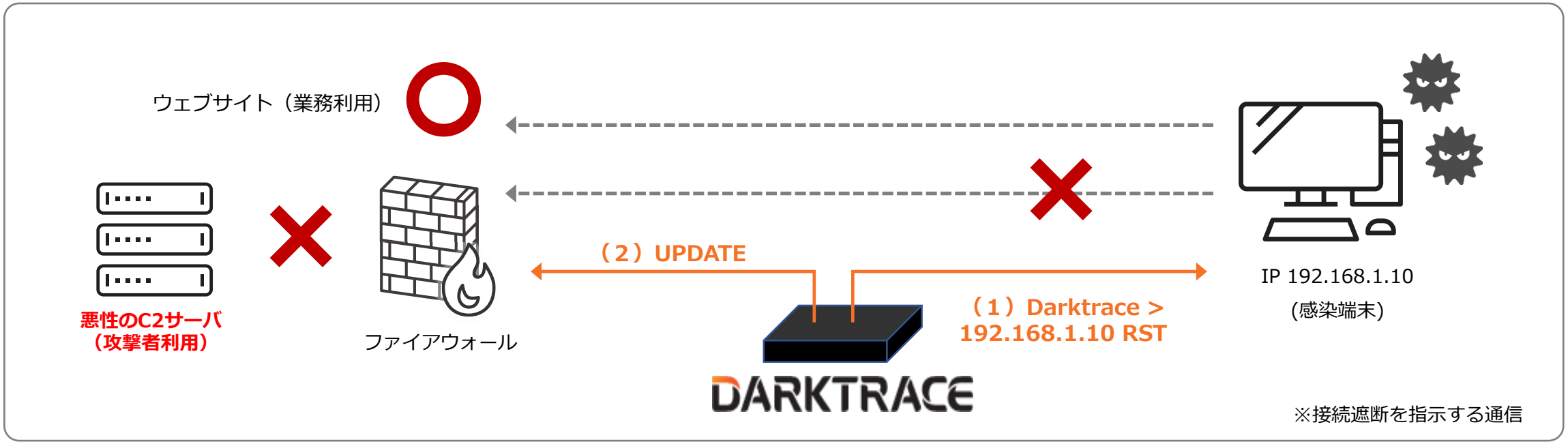
脅威の対象となる通信”のみ”を遮断することで

診療業務に影響・中断させることなく脅威を阻止

（２）Firewall と連携して自動遮断

既存のセキュリティ防御との統合で

連携を取りながら自動対処も可能

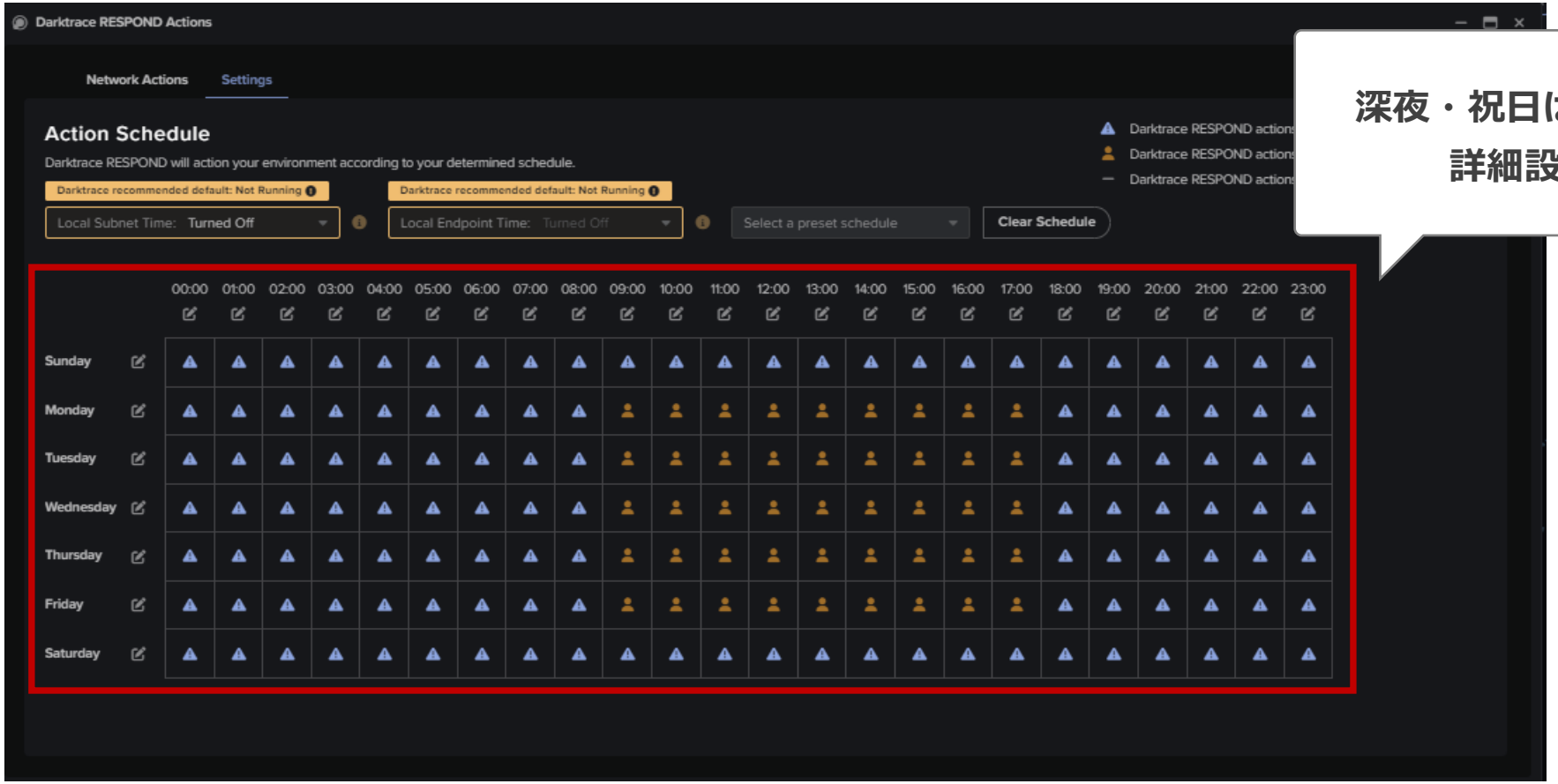


DarktraceのRESPOND（自動対処）カレンダー形式で効率管理

RESPOND

IIM

自動対処はカレンダー形式でいつ・どんなモードにするかを細かく設定可能です



深夜・祝日は自動対処など詳細設定が可能

Autonomousモード
AIによる自動対処

Human confirmationモード
人が判断して対処

SEIKO GROUP

DarktraceのRESPOND（自動対処）運用フローイメージ

RESPOND

メールやモバイルアプリから遠隔で内容確認し、遮断・再接続の指示が出せます

（１）Darktraceから通知受信（メール、モバイルアプリ等）

▼

（２）管理画面（Threat Visualizer）から確認

Autonomousモード運用時

(AIによる自動対処のため既に遮断済)

- 問題あり
  - そのまま遮断しておく
  - 調査／対処の実施
    - ・ユーザーへの確認 ・ログ調査
    - ・端末の隔離など
- 問題なし
  - 遮断を解除

Human confirmationモード運用時

(人が判断して対処するためこの時点では未対処)

- 問題あり
  - 遮断を実施する
  - 調査／対処の実施
    - ・ユーザーへの確認 ・ログ調査
    - ・端末の隔離など
- 問題なし
  - アクションクリア

もし大阪の某病院でDarktrace（RESPOND）を導入していたら

RESPOND IIM

	時系列での事柄	RESPOND（通信遮断オプション）
1	外部委託会社がマルウェア感染	監視外の環境なので対象外
2	外部委託会社から病院へリモートサーバへアクセス	通常のログインと変わらないためこの時点では判別不可
3	院内ネットワークでスキャニング行為	スキャニングの動きを阻止
4	他の端末へのSMB接続	ファイルのダウンロード等の挙動を阻止
5	他の端末へのリモートアクセス	通常業務と関連性が乏しい場合は、リモートアクセスを阻止
6	バックアップファイルの削除	バックアップファイルへのアクセスならびに削除の動きを阻止
7	ファイルの暗号化	暗号化の動きを阻止
8	脅迫文書の格納	感染端末を隔離するアクションにて阻止

活動初期

通信遮断で**活動初期の段階での封じ込め**が可能！ファイル暗号化にまで至らないため**実害の発生防止**に寄与

SEIKO GROUP

※参考

今やサイバー攻撃を完全に防ぐのは困難！いかに早く検知・対処し被害を最小限に抑えるかが重要です

利益損害のイメージ　※全業界が調査対象

項目	平時	事業中断時	差額
売上高	10億円	6億円	▲4億円
固定費 人件費、賃料等	2億円	2億円	—
変動費 材料費、電気代等	7億円	4.2億円	2.8億円
営業利益（損失）	1億円	▲0.2億円	▲1.2億円

◇事業中断による売上が4割減
◇事業が中断していても
　固定費は定額必要
◇通常1億円稼げるのに、
　営業損益▲0.2億円
◇結果として、
　▲0.2億円－1億円＝▲1.2億円
　の損失が発生

対応例	概要	想定コスト
事故原因・ 被害範囲調査費用	その後の対策を進めるためにも原因や被害範囲等各種調査が必要 サイバー攻撃等の場合、フォレンジック調査が必要	300～400万
法律相談費用	リーガル面（個人情報保護法等）を踏まえた対応が必要 法律事務所へ依頼するのが通例	数十万
広告宣伝費用	お詫び分の作成・ホームページへの掲載、DM送付などが必要 新聞出稿等の検討も必要	DM系封書130円/一通　　新聞全国紙240万、地方紙50万
コールセンター	問合せ対応のため、電話受付体制の整備が必要、コールセンター事業者への委託が一般的	1ヶ月140万/1オペレーター 初月：３OP、次月以降は1OPで700～1000万
システム復旧費用・ 再発防止費用	システム消失・改ざんがあった場合、データ復旧が必要、データ復旧は主にバックアップされたデータの復旧。セキュリティベンダーなど、対策規模によってケースバイケース	システム構築したITベンダーなどでコストは対応規模次第

※引用：JNSA「サイバー攻撃を受けるとお金がかかる」

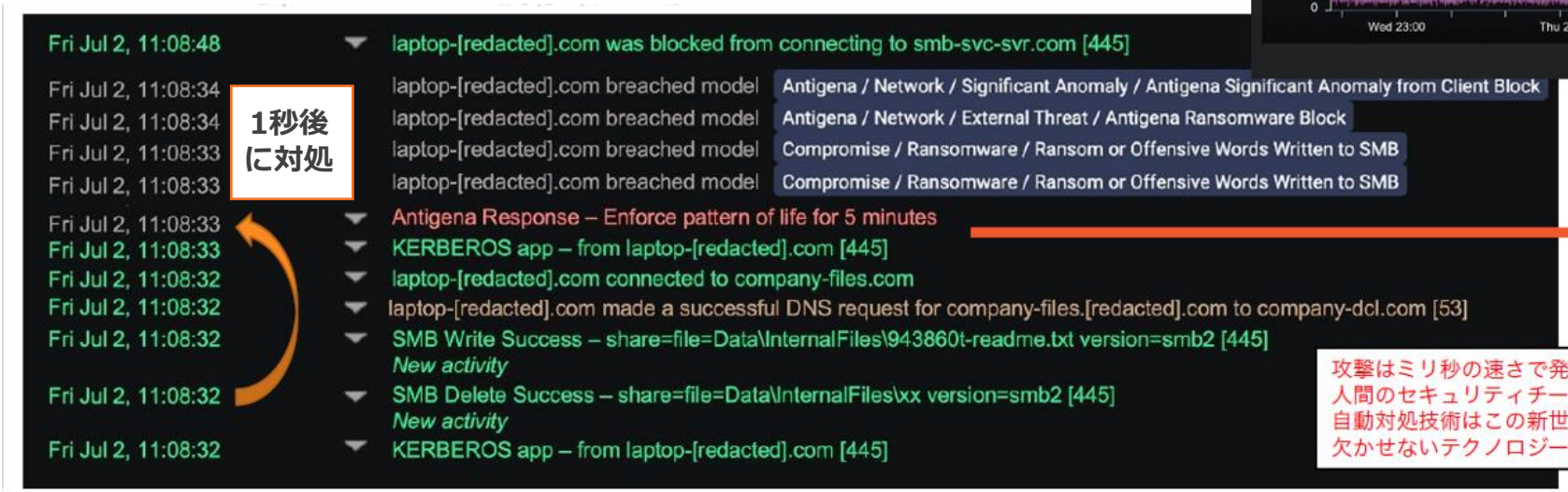
Revilランサムウェアから攻撃を受けるも、Darktraceが早期に検知
人では対応できないマシンスピードで遮断を行い1秒後には安全な環境へ

ランサムウェアグループであるREvilはKaseyaのソフトウェアの脆弱性を悪用してMSP（Managed Service Providers）およびそれらの顧客に対する攻撃をしかけました。少なくとも1,500社が影響を受け、その中にはKaseyaと直接関係のない企業も含まれていました。

DarktraceのRESPONDを導入していたこの企業は
1秒のうちに検知・自動対処で事なきを得た

感染したラップトップからのネットワーク接続

Darktrace RESPONDにより
コネクションが確立されなくなったことが
グラフから読み取れる。



攻撃はミリ秒の速さで発生し、
人間のセキュリティチームが対応できるレベルを超えていました。
自動対処技術はこの新世代のマシンスピード攻撃に対抗する上で
欠かせないテクノロジーであることが実証されています。

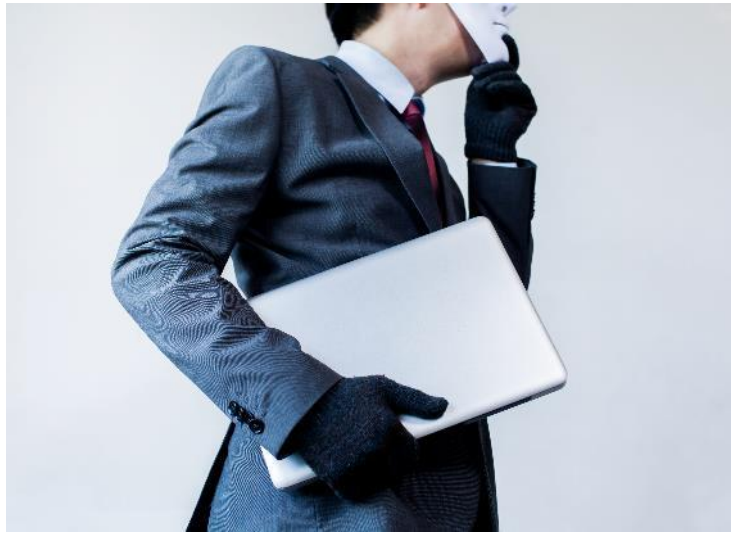
Darktrace運用監視サービス

セキュリティ監視をプロに任せたい「運用監視サービス」

現場経験が豊富な専任アナリストが、常時監視・調査・対応支援を行います

あらゆる脅威を監視

内部不正やポリシー違反も監視

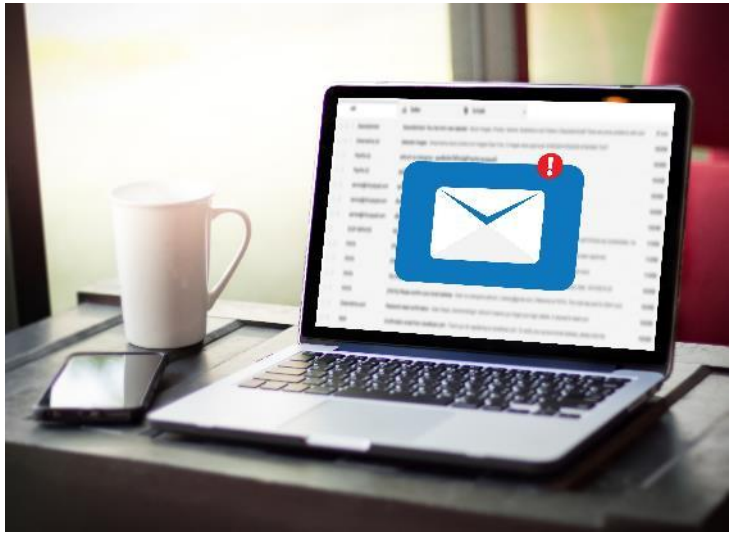


サイバー攻撃や怪しい挙動などの外部脅威以外にも、内部不正やポリシー違反も併せてチェックします。

スタンダード　アドバンスド

アナリストによる詳細報告

詳細で分かりやすい報告メール



現場経験豊富なアナリストが高危険度アラートに対して通知。事象だけでなく、影響範囲やリスク予測などを踏まえた推奨対処まで示したメールをお送りします。

スタンダード　アドバンスド

LANSCOPE連携

LANSCOPEを活用した調査

IT資産管理・ログ管理「LANSCOPEエンドポイントマネジャー」や、EPP・EDR「LANSCOPEサイバープロテクション」の情報も活用して、エンドポイントの詳細調査解析まで実施が可能です。

アドバンスド

運用監視サービスイメージ

監視運用サービスで、自社運用によるあらゆる 「不足」の解決をサポートします

自社運用の場合

日々発生する
セキュリティアラートに対し・・・

- ◆常時監視が出来ない（**リソース不足**）
- ◆最新の攻撃に気づけない（**情報不足**）
- ◆マルウェア感染か正常な通信か分からない（**スキル不足**）
- ◆どのアラートを報告すべきか分からない（**経験不足**）

検知 → 調査分析 → 報告

運用監視サービスの場合

検知 → 調査分析 → 報告

監視工数が大幅に削減

検知

- ・セキュリティアナリストによる定期監視
- ・情報による一次切り分け
  - ※ アラート内容、検知条件、想定される脅威
- ・最新の脅威インテリジェンス情報による一次切り分け
  - ※ 脆弱性情報、攻撃手法、マルウェア解析情報

調査・分析

- ・該当端末の特定、攻撃サーバーの調査・特定
- ・発生時系列の分析、影響範囲（感染）の調査
- ・発生前後の挙動及び操作情報の調査（原因特定）
- ・外部の脅威情報を踏まえた分析（接続先、ハッシュ値など）

報告

- ・適切な対処（NW隔離、AVスキャンなど）及び対策を支援
- ・自社・他社の監視実績を基にした報告アラートの選別

2種類の運用監視サービスをご用意

スタンダード

Darktrace社のサイバーアナリストが
脅威を検知・サポートします

Darktraceのアナリストがアラートを調査します。早急に調査が必要な事象と判断した場合、24時間365日、メールやSMSなどで管理者へ通知を行います。

こんな方におすすめ

- 24時間365日監視をしてほしい
- とにかくまず注意すべきアラートが出たことを把握したい
- コストを抑え必要最低限の監視支援を受けたい

アドバンスド

エムオーテックスのアナリストが分析調査
日本語でサポートします

エムオーテックスのアナリストが分析調査した結果を1日に2回、定期連絡します。調査分析レポートは日本語対応で、通信内容に加えて原因・経緯までを報告します。
アラートに関してQ&A対応も可能で、安心してご利用いただけます。

こんな方におすすめ

- 24時間365日、日本語で細やかな支援を行ってほしい
- セキュリティ監視をお任せしたい
- 専門知識や管理人数が少なく、行うべき対策まで相談したい

運用監視サービスの概要

	スタンダード	アドバンスド
提供元	Darktrace	エムオーテックス（MOTEX）
サービス特徴	・メーカーのアナリストによる標準サービス ・高危険度のアラートを調査 ・通知内容は発生した通信の情報のみ	・MOTEXのアナリストによる高付加価値なサービス ・高危険度で発生したアラートが調査対象 ・通知内容は通信内容に加え、原因・経緯まで含まれる ・顧客の環境に合わせた調査範囲のカスタマイズ提案可能
対応言語	英語	日本語
対応時間	24時間365日	24時間365日 ※弊社営業日 9:30-17:30はMOTEXアナリストによる詳細解析/分析/通知を提供 それ以外の時間帯はDarktrace機器からのアラート自動メール通知とし、 MOTEXアナリストによる詳細解析/分析/通知は翌稼働日での対応となります。
報告タイミング	随時 Darktrace社アナリストによる分析調査した結果、早急に調査が必要な事象と判断した時点で連絡します。	定期 MOTEX社アナリストによる分析調査した結果を1日に2回、弊社営業日にて定期連絡します。 ① 9:30-15:00の発生アラート ⇒ 当日17:30までに報告 ② 15:00-翌9:30の発生アラート ⇒ 翌日12:00までに報告
検知後のアクション	・ Darktrace社アナリストによる分析調査 ・ 早急に調査が必要な事象と判断したものを報告 ・ 問題がなければ、報告せずクローズ	・ 弊社アナリストによる分析調査 ・ 弊社アナリストからお客様セキュリティ担当者にメール報告 ・ 問題がなければ、報告せずクローズ
カスタマイズ性	不可 ※アラートの調査・分析はDarktrace機能で可能なもののみとし、他機器のログ調査などは含みません。	可能 ※MOTEX提供のセキュリティ対策製品(エンドポイントマネージャー、Cylance、Deep Instinct)のログ調査
対象アラート数	上限なし	詳細調査は15件/月を想定 ※調査対象のアラート件数を超える場合、翌月に超過分をご発注いただきます。
報告内容の問い合わせ	問い合わせ対応なし ※別途有償サービスを契約する必要あり	Eメール

エムオーテックスによる運用監視（アドバンスド）のアラート報告イメージ

運用監視（アドバンスド）

アナリストが、脅威度が高いアラートと判断した場合、日次レポート（メール）にてご連絡します

報告内容

- 検知日時
- 検出脅威（アラート名、アラートレベル等）
- 検知内容（対象端末、通信先）
- 調査内容（OSINTでの調査結果）
- 確認事項（推奨対処）

● 日次レポート例 ~マルウェア感染事例~

【検知日時】 ： 20XX年▲▲月◆◆日 16:35:12
【検出脅威】 ： Unusual Incoming Data Volume（73%）
【検知内容】
対象端末より、普段接続しない通信先に対して繰り返し行われる通信が検知されました。
C&C サーバとの通信である可能性があります。
- 対象端末 ： 10.150.120.XX
- 通信先 ： panisdar[.]com（5[.]188.60.XX）
【調査内容】
通信を確認したところ、通信先のポート番号443（SSL）に対して9:29～10:01、
13:05～17:06の時間帯に通信が発生していました。通信先は C&C サーバとして報告されています。
また、以下のファイルをダウンロードすることが報告されており、対象端末は16:07:00にアクセスを行っていました。
・http://XXXXXXXXX [.]org/img/sm/story.rar
※アクセスすると、マルウェアに感染する恐れがあります。
VirusTotal上では複数ベンダーが脅威ファイルであると判定しています。
VirusTotalの結果:https://www.virustotal.com/gui/file/xxxxx（ハッシュ値）
【確認事項】
マルウェア感染などの被害が拡大する恐れがあるため、該当する端末をネットワークから至急隔離してください。なお、通信先情報より、最近確認されている不審メールを開封した可能性があります。
以下、参考URLとなります。
・https://www.jc3.or.jp/topics/v_log/201902.html#d20190218b
※情報窃取型不正プログラム「URSNIF」に関連

該当する端末を確認し、不審なメールに添付されたファイルを開いていないか、
不審ファイルが検知されていないかを確認してください。
また、ウイルス対策ソフトによるスキャンを実施することを推奨します。

運用監視（アドバンスド）

事前に報告基準を取り決めた上で、脅威度の高い通信を検知した場合のみ、ご報告します

例えば「Level2」 以上を報告対象とし、Level 1以下は対象外となります

緊急度高

緊急度低

レベル	報告	定義	具体例
Level 3	日次メール (詳細報告) 及び 月次レポート	**【緊急対応】** 被害が確認でき、 セキュリティインシデントが 発生している可能性が極めて高い	**【攻撃関連】** ・ウイルス感染による通信が発生していると判断した場合（C＆C通信、内部NWからの攻撃通信） ・ウイルス感染によって、データ転送など、情報漏洩の可能性があると判断した場合
Level 2	日次メール (詳細報告) 及び 月次レポート	**【詳細調査】** 被害は確認できず、 セキュリティインシデントが 発生している可能性が高い	**【攻撃関連】** ・ウイルス/スパイウェアのダウンロードを検知したが、端末に影響があると判断できた場合 ・スパイウェア感染による通信が発生していると判断した場合 【内部不正】 ・ポリシー違反によって、データ転送など、情報漏洩の可能性があると判断した場合
Level 1	日次メール (簡易報告) 及び 月次レポート	**【経過観察】** 被害は確認できず、 セキュリティインシデントが 発生している可能性が低い	**【攻撃関連】** ・ウイルス/スパイウェアのダウンロードを検知したが、ウイルス対策ソフトなどによって、端末に影響がないと判断した場合 **【内部不正】** ・ポリシー違反によって、クラウド利用を検知した場合
Level 0	日次メール (簡易報告) 及び 月次レポート	**【通常通信】** 通常通信を過検知している 可能性が高い	**【攻撃関連 / 内部不正】** ・マルウェアの影響や攻撃通信、ポリシー違反に該当する通信でない場合 ・業務利用や軽微な私的利用

報告対象

運用監視（アドバンスド）におけるカスタマイズ例：
LANSCOPE / Cylance/ Deep Instinct ログの活用

運用監視（アドバンスド）

Darktraceで取得可能な情報に加え、エムオーテックスのセキュリティ製品のログ情報も踏まえた深堀調査を提供

検知

<検知フェーズ>

・外部への不審なデータ送信を検知
↓
・検知情報から普段アクセスのない宛先であることを確認

詳細調査・影響確認

<絞り込みフェーズ>

・アラート検知前に外部へ送信したデータとほぼ同量のデータを内部ファイルサーバーからダウンロードしていることを確認
↓
・不審なEXEをダウンロードしており、ファイル名からデータ転送ツールであることを確認

追加調査 エンドポイント

<詳細調査フェーズ>

・操作ログから以下を確認。
-ファイルサーバーからデータをダウンロードしリネーム
-データ転送ツールをインターネットからダウンロードし実行

・検知/隔離情報から脅威を確認
- 不審ファイルの詳細/脅威度 など

DARKTRACE

<検知フェーズ>

・アラート検知

・検知内容確認（通信先、データ量、時間、ユーザー等）

<絞り込みフェーズ>

・影響範囲絞り込み（アラート前後の通信内容、関連する端末、ユーザー）

LANSCOPE Endpoint Manager

<詳細調査フェーズ>

・該当時間の操作内容確認
（操作ログ）

CylancePROTECT　deep instinct

<詳細調査フェーズ>

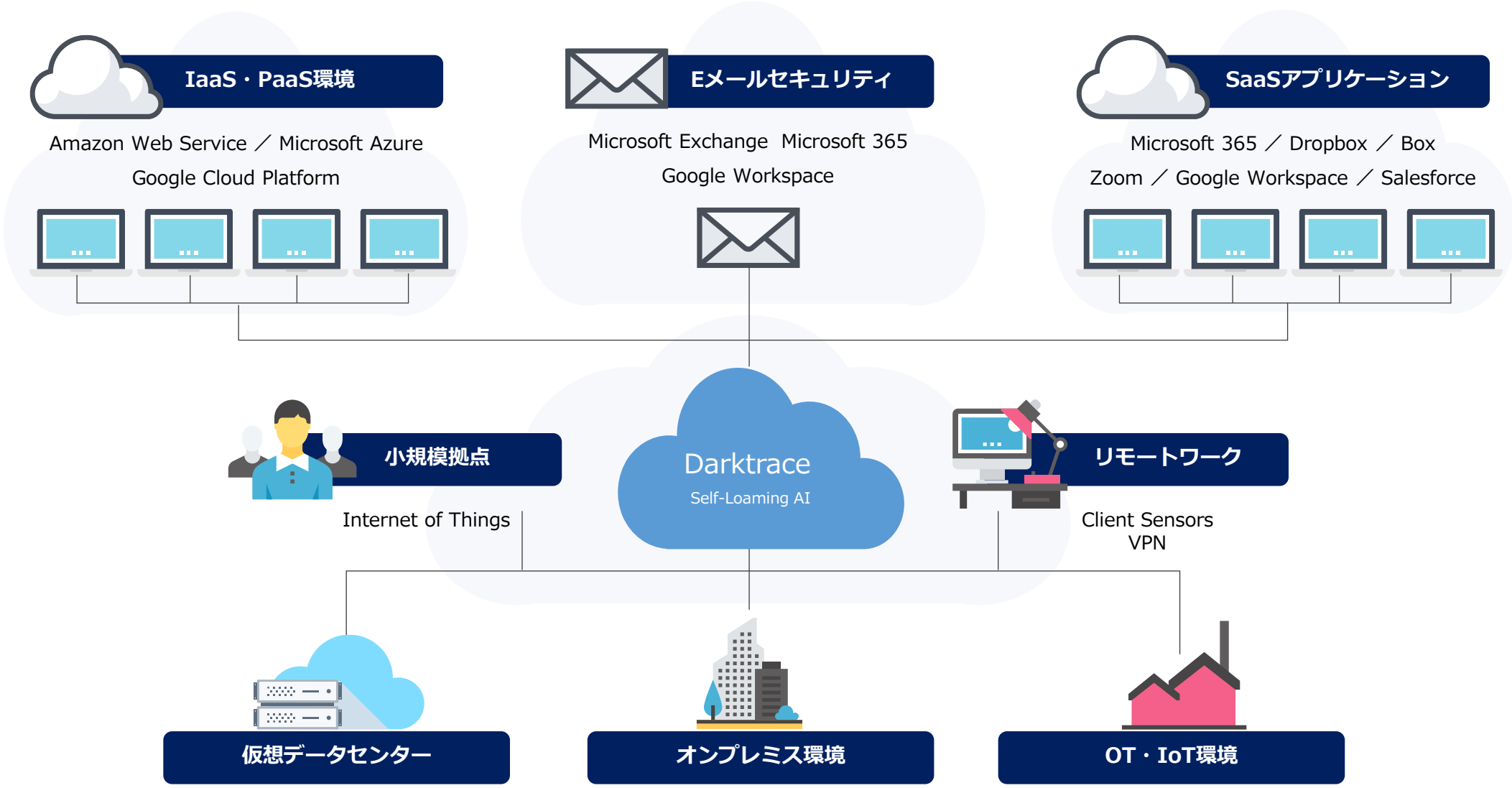
・導入端末の情報確認※
（カテゴリ、検知状況、脅威スコア）

※マルウェア感染が疑われる挙動が確認された場合や、その他インシデントの可能性がある場合、アナリストにて Cylance/Deep Instinct上での検知状況を確認

SEIKO GROUP

テレワークやクラウド環境の監視も対応（オプション）

院内ネットワークに加え、クラウドなども含めた包括的なセキュリティ対策へ拡張可能



Darktrace事例

医療業界導入事例

Darktrace導入事例（１）

医療法人錦秀会 様

ITコンサル・導入支援・運用保守
アスクラピウス株式会社 様

業　種	医療・福祉
病床数	グループ全体で6,000床

導入経緯・課題

近隣の大阪急性期・総合医療センターにおいてインシデントが発生、自分たちにも同様のことが起こり得ると実感。

他病院で立て続けに発生したインシデントはもはや他人事ではない。

サイバーセキュリティ対策計画はDarktraceでフィナーレ

導入時のポイント

電子カルテ環境にインストールが不要だった点と、医療従事者に負担を掛けず、業務に影響を与えない構成が好印象。内部対策としてNDR（Darktrace）を導入

運用時のポイント

必要に応じてモバイルアプリで遮断を解除

・Teamsにアラート通知がくるようにし、必要に応じてモバイルアプリで通信遮断を解除する運用とすることで工数を削減。

医療従事者が安心してITを利用できる仕組みを確立

・エージェントレスで医療業務やシステムに悪影響を与えない
・PCなどの端末を経由しない攻撃も察知できるという安心感
・管理者2名でも24時間365日異常を検知・自動対応できる体制を確立

医療法人A

業　種	医療・福祉
病床数	200未満

予測レベルでの脅威をAIが自動検知・分析
ネットワークの完全可視化・保全をたった1名で実現

導入経緯・課題

・増加する医療機関へのサイバー攻撃に対し**自社の境界型防御に危機感**

・**万が一に備えた**電子カルテなどの患者の機微な医療情報の適切な保護

導入効果（１） **「予測検知と精度の高さ」**

通信の定常状態学習とネットワーク完全可視化で、

従来対策をすり抜ける脅威に対しても予兆レベルで検知できました。

導入効果（２） **「通信異常の自動調査による運用工数削減」**

各アラートの異常度や因果関係まで**AI が自動的に調査分析**してくれるため、

少人数運用でも漏れなく対処できる体制がとれました。

Darktrace導入事例（３）

地方中核病院B

業　種	医療・福祉
病床数	250未満

ランサムウェア攻撃への不安と
エンドポイント防御依存の限界、全IP端末の通信監視界

導入経緯・課題

・国内の他病院に被害をもたらしているランサムウェア等**未知のサイバー攻撃への対策が急務。**
電子カルテメーカー指定のセキュリティ対策ソフトへの不安あり

・**メディカルIoTデバイス**への対策が講じられていない

導入効果（１）　**「エンドポイントに依存せずネットワークで網羅的に対策」**

院内通信の完全可視化とあらゆる異常の自律検知・遮断を
AIが24時間365日体制で実現

導入効果（２）　**「少人数体制ながら死角なきランサムウェア対策を実現」**

ルールベースの境界型製品が見逃す通信も検知し、セキュリティレベルを飛躍的に向上。

LockBit等へのランサムウェア自動対処

医療法人C

業　種	医療・福祉
病床数	200未満

病院のセキュリティ担当者でも低負荷で安心に運用
内部の不正も洗い出せ
「まさに防衛費用として最適な投資でした」

導入経緯・課題

サイバーセキュリティ対策として、全ての端末にアンチウイルスソフトとURLフィルタリングツール、ファイアウォール製品も導入して境界における基本的な対策を実施済みであったが、入口出口対策だけでは本質的にネットワーク内部の脅威に対する対策が難しかった。

Google Driveの個人アカウントにログインしてデータをダウンロードする職員の行為が見受けられたため、あらゆる院内端末とその通信の状況をおしなべて一元的に可視化し、ネットワークの出入口やその内部で発生するトラフィックを常に監視できるような体制構築を考えたい。

導入効果

「少人数体制でも漏れのない対策を実現」

500台強の院内端末（各種医療機器も含む）の挙動や通信を情報管理課の2名体制で、1日に3-4回の頻度で確認しており、特に異常度の高いアラートについては当該当端末のIPアドレスを絞り込んだ上で端末ログの深掘調査を3D可視化ツール上でワンストップで進めています。

また、**一定のセキュリティに関する知識があれば誰でも使えるのも魅力**です。

Darktrace ライセンス形態

標準ライセンス	オプション
筐体課金：モデル　S、M、X2	**追加モジュール課金** ・テレワーク（エンドポイント対策） ・クラウド（各種SaaS） ・メール環境　他
＋	
デバイス課金：デバイス数	

※標準ライセンスのモデルのスペックの詳細は「Darktrace スペック表」をご確認ください

※標準ライセンスのデバイス課金のデバイス数は、Darktrace機器で観測、計測したデバイス数を指します

Darktraceサービスのメニュー 一覧

	名称	付帯サービス	概要
1	**Darktrace 3年間ライセンス**	製品保守	Darktrace製品 のご利用に必要なアプライアンス・デバイスライセンス/保守サービスをご提供いたします。
2	**Darktrace 運用監視付(スタンダード) 3年間ライセンス**	製品保守 運用監視（スタンダード）	Darktrace製品 のご利用に必要なアプライアンス・デバイスライセンス/保守サービスに加え、Darktrace 社提供の監視サービスをご提供いたします。
3	**Darktrace 運用監視付(アドバンスド) 3年間ライセンス**	製品保守 運用監視（アドバンスド）	Darktrace製品 のご利用に必要なアプライアンス・デバイスライセンス/保守サービスに加え、エムオーテックス提供の監視サービスをご提供いたします。

Darktrace スペック表

機種	DCIP-S	DCIP-M	DCIP-X2
寸法(縦幅)	1ユニット	1ユニット	2ユニット
容積（cm）	W44×D37×H4.4	W44×D74.5×H4.4	W44×D74.5×H8.8
重量	6kg	15kg	23kg
搭載可能ラック	19インチ	19インチ	19インチ
インターフェイス※①	10/100/1000　BASE-T　1つ	10/100/1000　BASE-T　1つ	10/100/1000　BASE-T　1つ
収集用ポート	10/100/1000　BASE-T　3つ	10/100/1000　BASE-T　3つ	10/100/1000　BASE-T　1つ 10　GBASE-T　2つ
SFP +ポート	該当なし	10Gbe/1Gbe SFP+2つ	10Gbe/1Gbe SFP+2つ
ピーク時のスループット	300Mbps	2Gbps	5Gbps
最大監視デバイス数	1.000	8.000	36.000
最大コネクション数	2.000	50.000	100.000
電源	260W IEC 13C 120/240V(1本)	750W IEC 13C 120/240V(2本)	1110W IEC 13C 120/240V(2本)
電力消費量 （1時間あたり）	Idle時:26W 稼働率85%時:89W 最大：105W	Idle時:120W 稼働率85%時:359W 最大：418W	Idle時:128W 稼働率85%時:365W 最大：426W
拡張可能モジュール※②	以下のうち、最大1つ利用可能 ・2-port 1G/10G SFP+ ・2-port 1G RJ45 1000 BASE-T ・4-port 1G RJ45 1000 BASE-T	以下のうち、最大1つ利用可能 ・2-port 1G/10G SFP+ ・2-port 10G RJ45 10000 BASE-T ・2-port 1G RJ45 1000 BASE-T ・4-port 1G RJ45 1000 BASE-T	以下のうち、最大3つ利用可能 ・2-port 1G/10G SFP+ ・2-port 10G RJ45 10000 BASE-T ・2-port 1G RJ45 1000 BASE-T ・4-port 1G RJ45 1000 BASE-T

※①インターフェイスは「admin port」「Remote management port」の2種となります。
※②拡張可能モジュールは別売りとなります。

サービス導入までの流れ

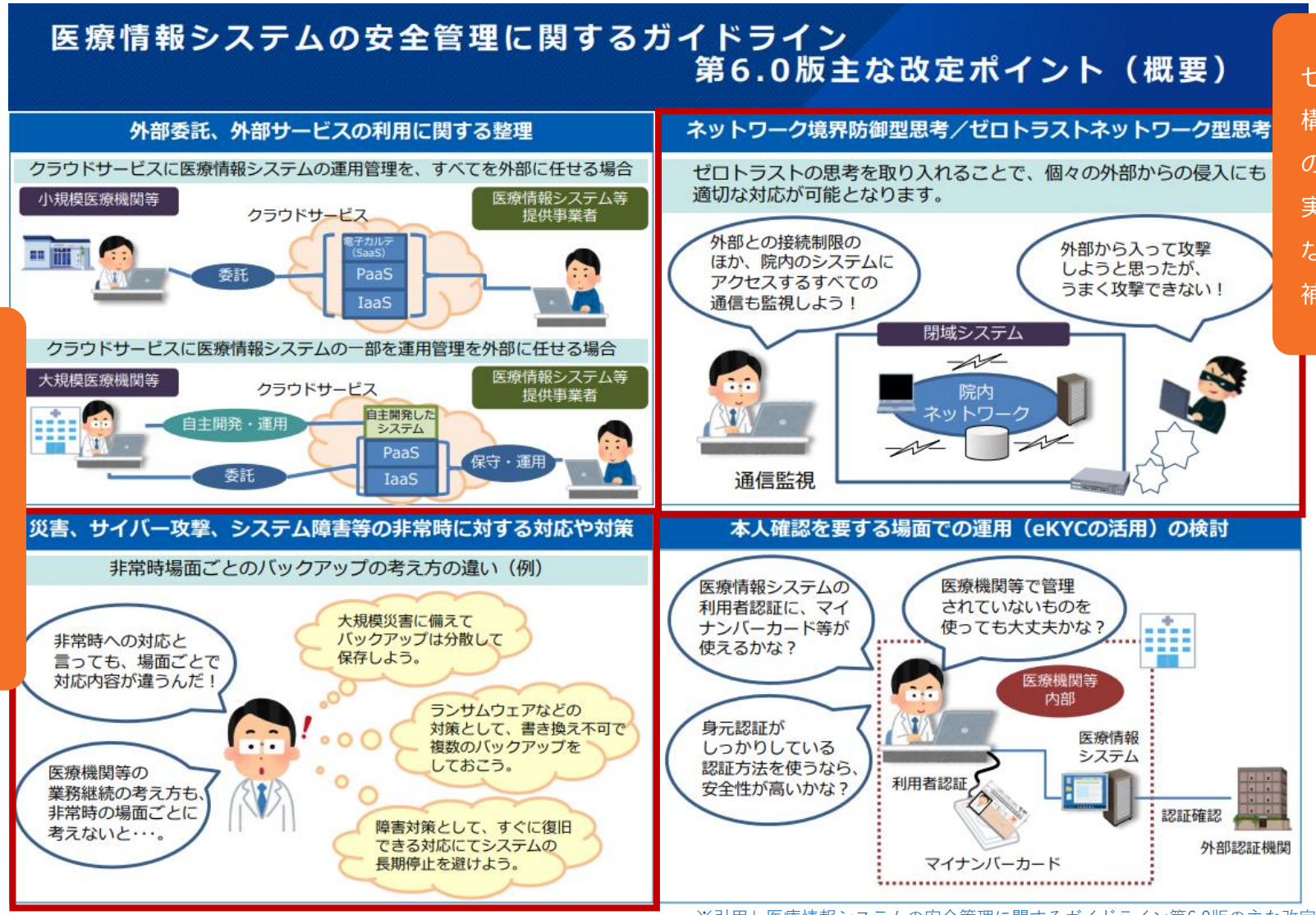
	導入フェーズ			設計・構築フェーズ			運用フェーズ
イベント				★Darktrace 機器発注及び導入作業ご発注		★Darktrace サービス契約開始	★運用監視サービス 開始
期間		4週間		12週間			
内容	**Step1** **PoV** Darktraceの評価を行います	**Step2** **監視対象検討** PoVの結果を踏まえて監視対象とするネットワークセグメントを検討します	**Step3** **設置場所検討** 監視対象のトラフィックを収集できる設置場所を検討します	**Step4** **運用設計** 運用に関する取り決め(アラート報告件数やタイミング等)を検討します	**Step5** **設定・構築** 機器の設定と設置作業を行いトラフィックの収集を開始します	**Step6** **チューニング** トラフィックの学習が進行しますアラートの検知状況を確認してチューニングを行います	**Step7** **運用開始** 正式に運用を開始します
ライセンスのみ	○	○	○		○	○	○
ライセンス Darktrace監視	○	○	○		○	○	○
ライセンス MOTEX監視	○	○	○	○	○	○	○

Appendix

医療情報システムの安全管理に関するガイドライン6.0対応

最新の医療情報システムの安全管理に関するガイドライン対応

検査の基準となる「医療情報システムの安全管理に関するガイドライン6.0」にも対応



※引用」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版の主な改定ポイント（概要）

ゼロトラストネットワークを構築するにあたりDarktraceのような通信監視が必須！現実的に人的工数は多くかけれないのでAIにより通信監視を補う必要がある。

サイバー攻撃があった際に何が起きていたか把握するためには常時パケットキャプチャをしているDarktraceのアラートもしくはログが役立つ。自動対処で実被害の抑え込みも可能

医療情報システムの安全管理に関するガイドライン対応表

要求事項				Darktrace対応
8	利用機器・サービスに対する安全管理措置 [Ⅰ～Ⅳ]	8．1	不正ソフトウェア対策	○
		8．3	端末やサーバの安全な利用の管理	○
		8．4	情報機器等の棚卸	○
10	医療情報システム・サービス事業者による保守対応等に対する安全管理措置[Ⅰ、Ⅲ]	10．1	保守時の安全管理対策	△
13	ネットワークに関する安全管理措置 [Ⅰ、Ⅲ]	13．2	不正な通信の検知や遮断、監視	○
		13．3	通信の暗号化・盗聴等の防止	△
18	外部からの攻撃に対する安全管理措置[Ⅰ～Ⅳ]	18．1	サイバーセキュリティ対応	○

PICKUP！　医療情報システムの安全管理に関するガイドライン対応

8．利用機器・サービスに対する安全管理措置［Ⅰ～Ⅳ］
8．1　不正ソフトウェア対策
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。 ④メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。
8．3　端末やサーバの安全な利用の管理
⑥ IoT 機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様である。 (1) IoT 機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。 (2) IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用すること。 (3) 使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。
8．4　情報機器等の棚卸
⑦企画管理者と協働して、医療情報システムで用いる 情報機器 等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、 情報機器 等の滅失状況なども併せて確認すること。

※Darktraceの対応についての詳細は、お問い合わせください

PICKUP！　医療情報システムの安全管理に関するガイドライン対応

10. 医療情報システム・サービス事業者による保守対応等に対する安全管理措置[Ⅰ、Ⅲ]

10．1　保守時の安全管理対策

③ 保守を実施するためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。

④ リモートメンテナンス（保守）によるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集し、保守に関する作業計画書と照合するなどにより確認し、当該作業の終了後速やかに企画管理者に報告し、確認を求めること。

13. ネットワークに関する安全管理措置［Ⅰ、Ⅲ］

13．2　不正な通信の検知や遮断、監視

⑤ルータ等のネットワーク機器について、安全性が確認できる機器を利用 し、不正な機器の接続 や不正なデータやソフトウェア の混入 が 生じないよう、セキュリティ対策を実施 すること。特に VPN 接続による場合は、施設内のルータを経由して異なる施設間を結ぶ通信経路の間で送受信ができないように経路を設定すること。

⑧ 医療機関等で用いる通信において、ネットワーク上で「改ざん」されていないことを保 証す ること。またネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。なお、可逆的な情報の圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにはあたらない。

⑨ ネットワーク経路でのメッセージ挿入、不正ソフトウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。

18．外部からの攻撃に対する安全管理措置[Ⅰ～Ⅳ]

18．1　サイバーセキュリティ対応

① 医療情報システムに対する不正ソフトウェアの混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。

- 攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時切断
- 他の情報機器への混入拡大の防止や情報漏洩の抑止のための当該混入機器の隔離
- 他の情報機器への波及の調査等被害の確認のための業務システムの停止

※Darktraceの対応についての詳細は、お問い合わせください