2022年6月30日

第26回日本医療情報学会春季学術大会　シンポジウム2022 in せとうち
チュートリアル3

医療機関におけるサイバーセキュリティへの課題と対応

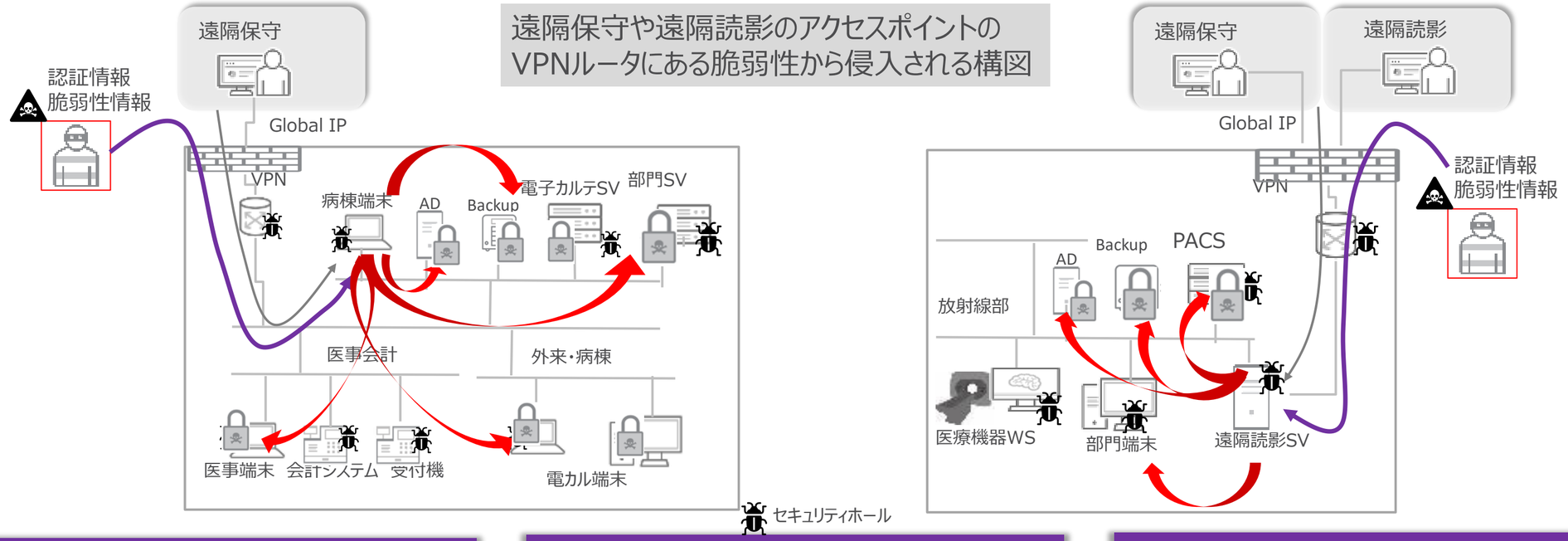
トレンドマイクロ株式会社
松山　征嗣

目次

医療機関のサイバーセキュリティ被害考察

病院機能停止に至るシステム障害

遠隔保守や遠隔読影のアクセスポイントの
VPNルータにある脆弱性から侵入される構図



VPNルータの脆弱性放置

VPNルータの認証強度低い
１要素（パスワード）

VPN利用者のアクセス制御
ユーザーIDのみ、ホスト識別無し

ネットワークセグメントでの
アクセス制限なし

リモートデスクトップ、
PowerShellの悪用

セキュリティ対策ソフトが
更新されていない・停止されている

内部の端末、サーバの
OS・アプリケーション脆弱性放置

認証情報の窃取・権限昇格
セキュリティ対策の強制停止

重要情報へのアクセス
外部流出の可能性、データ暗号化

各社報道からの参考情報及び当社ナレッジから推測される構図です。

医療情報システムの安全管理に関するガイドライン第5.2版

6.5 技術的安全対策

抜粋

インシデント対応の経験を踏まえ重要と考える

5.2版で追加

C項（最低限のガイドライン）

- 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。

D項（推奨されるガイドライン）

- **外部のネットワークとの接続点やDB サーバ等の安全管理上の重要部分には、ファイアウォール（ステートフルインスペクションやそれと同等の機能を含む。）を設置し、ACL（アクセス制御リスト）等を適切に設定すること。**

B項（考え方） 不正ソフトウェア対策

- **検出するためのパターンファイルや検索エンジンを常に最新のものに更新しておく**
- **システム側の脆弱性を可能な限り小さくしておくこと**
  - **セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのパッチ適用**
  - **利用していないサービスや通信ポートの非活性化**
  - マクロ等の利用停止
  - メールやファイルの無害化
  - EDR（Endpoint Detection and Response）や「振る舞い検知」

対策を実施した際の業務への影響や、対策処理の速度や可用性、網羅性について、十分な検討が必要

B項（考え方） ネットワーク上からの不正アクセス

- 医療情報システムと外部ネットワークとの関係に応じて、**IDS、IPS** の採用も検討すべき
- システムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的に実施し、**パッチ適用等の対策**を講じておく
- 不正ソフトウェアが侵入した場合を想定した内部脅威監視などのモニタリング

費用対効果を鑑みて、リスクの高いところについて重点的に行うなども考えられる

戦術的に考えるサイバーセキュリティ対策

サイバーセキュリティフレームワーク

サイバーセキュリティ対策を考える上での考え方
NISTが提唱

NIST：National Institute of Standards and Technology
米国国立標準技術研究所

侵入前提の視点　　**事後対応の視点**

技術的視点　　**組織・プロセスの視点**

サイバーセキュリティはマルチ・リスクで考える
防御だけでなく、全体的な見直しが必要となる

参考）サイバーセキュリティフレームワーク

機能	カテゴリ	要旨
識別力	資産管理	管理対象の把握、ポリシーやマニュアルの整備、リスク想定とリスクマネジメント体制など組織的な準備が問われます。
	ガバナンス	
	リスクアセスメント	
	リスクマネジメント戦略	
防御力	アイデンティティ管理、認証／アクセス制御	システムや情報を保護するための技術対策や運用手順、関係者へのトレーニングなど技術的、人的な準備が問われます。
	意識向上およびトレーニング	
	データセキュリティ	
	情報を保護するためのプロセスおよび手順	
	保守	
	保護技術	
検知力	検知とイベント	主に技術的対策において検知したイベントへの注意力が問われます。
	セキュリティの継続的なモニタリング	
	検知プロセス	
事故対応力	対応計画	セキュリティインシデント発生時対応の準備、実際に発生した際の対応をもとに改善へ生かす仕組みが整っているかが問われます。
	コミュニケーション	
	分析	
	低減	
	改善	
復旧力	復旧計画	復旧プロセスの検証も含めた準備、プロセスの見直しが行われているかが問われます。
	復旧	
	コミュニケーション	

参考　重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1版
https://www.ipa.go.jp/security/publications/nist/index.html
独立行政法人情報処理推進機構（IPA）

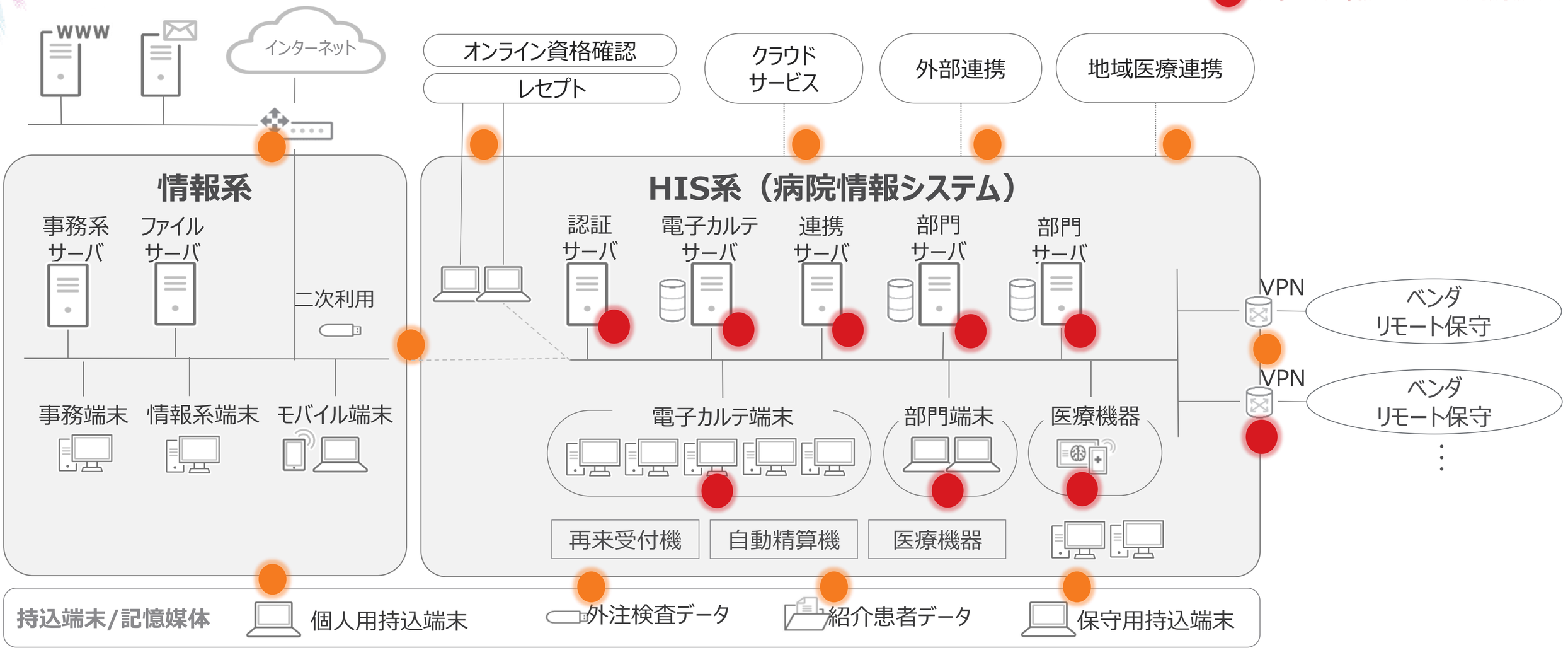
特定＝守る対象が明確でなければ守れない

何がどこにあるのか

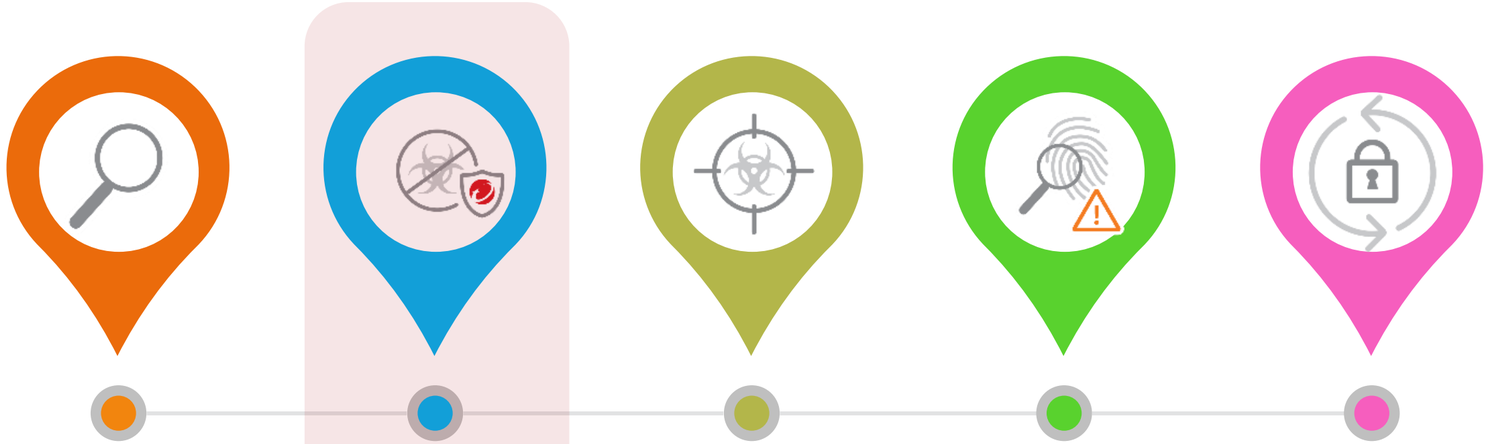
想定するリスクと脅威

組織としての方針・情報のアップデート

ネットワーク内の機器、外部との接点の整理



防御＝最もROIの高い領域

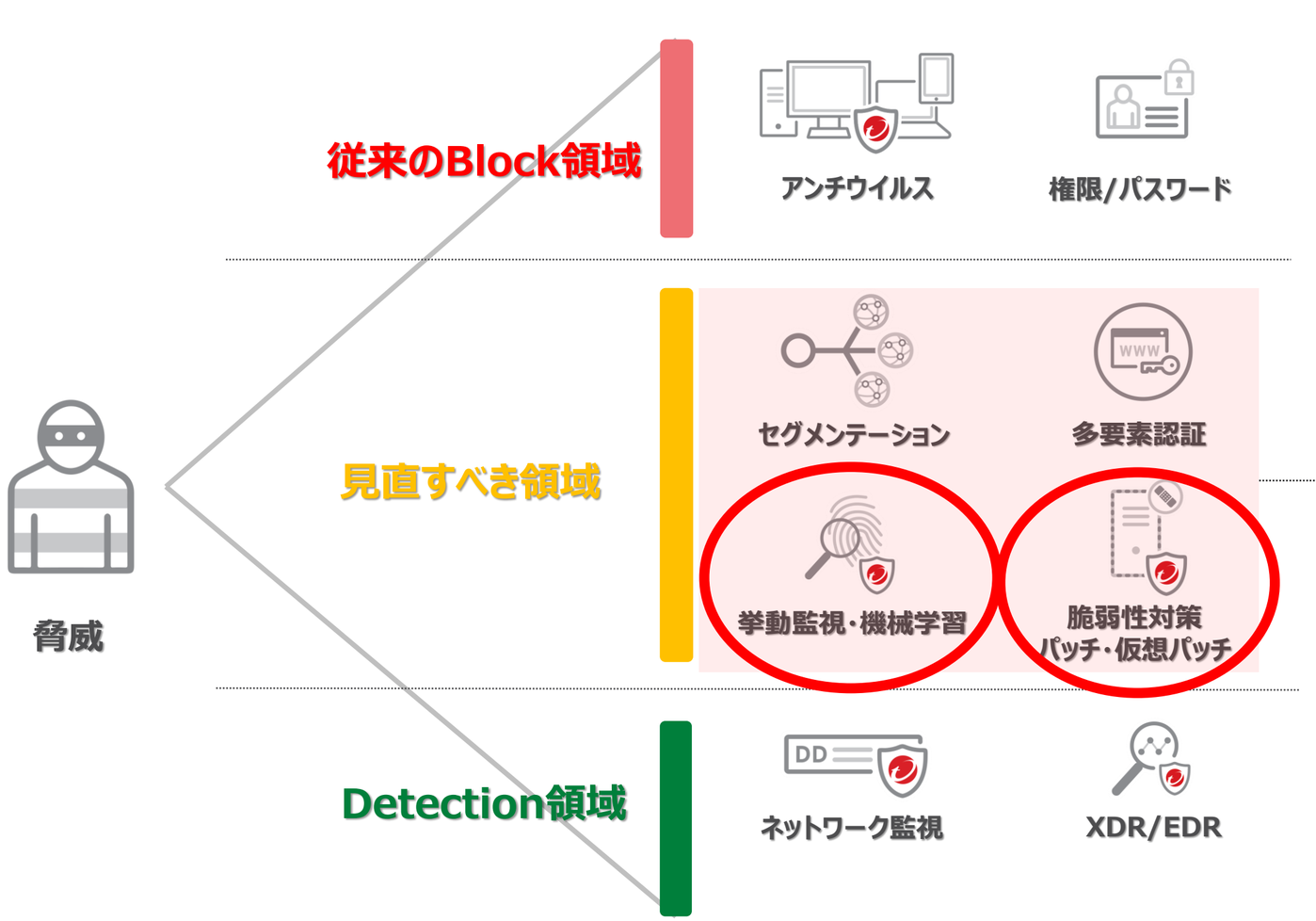


自動的に守られる領域

検知＋対応のセットで、はじめて守られる領域

防御＝自動で事業被害を食い止められる最も強力な盾

実際のインシデント事例から防御策を見直す



インシデント対応時に遭遇する問題

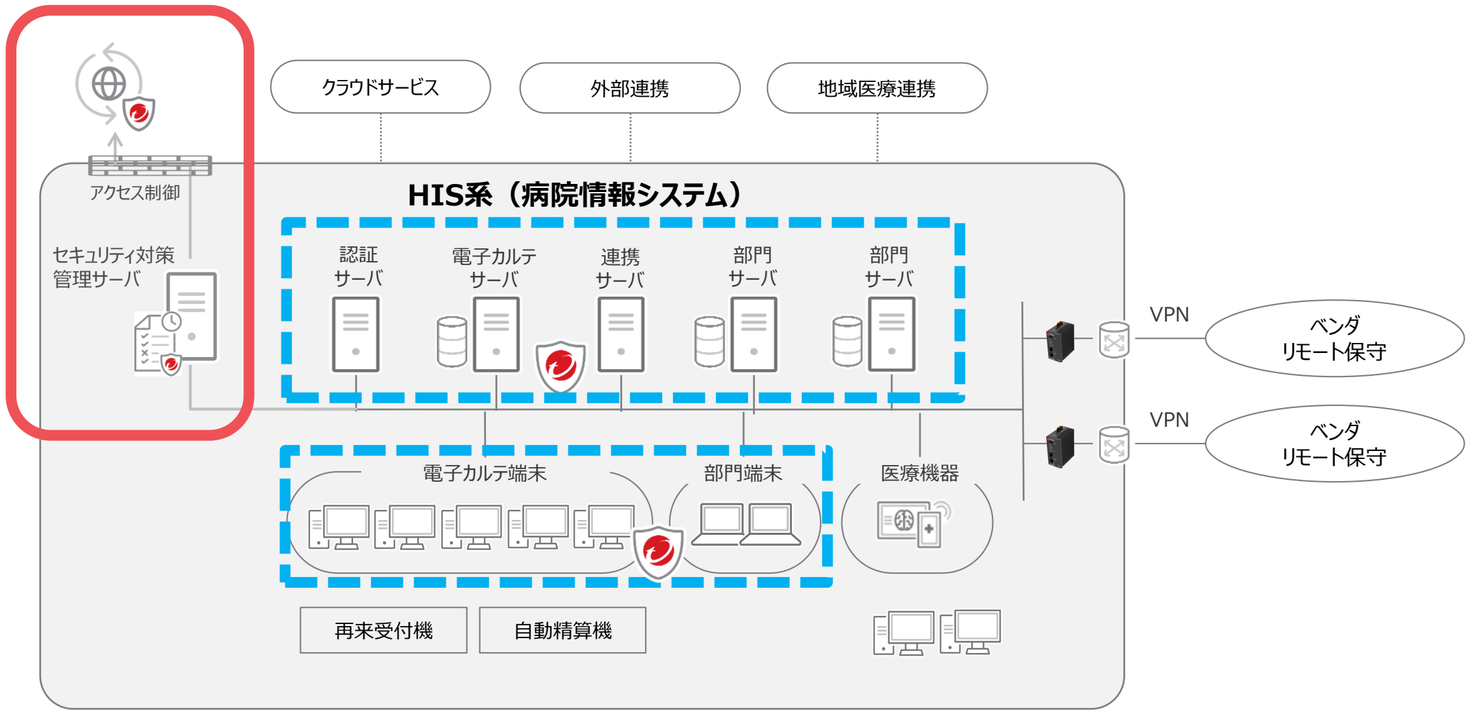
- **パターンファイル更新**がされていなかった
- **パターンファイルによるスキャンのみ**有効化していたため発見できなかった

- 脆弱性が原因で権限昇格、**アンチウイルスソフトが停止**されていた
- **RDPサービスの脆弱性があり、接続制限が無かったため**、攻撃に悪用された

費用対効果が非常に高い防御策

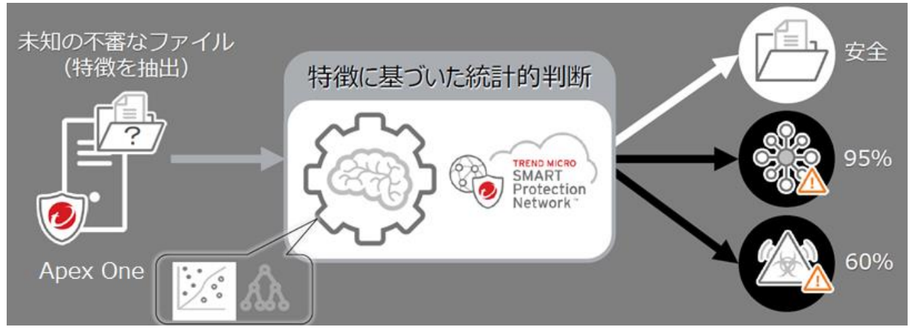
マルウェア対策ソフト運用の見直し

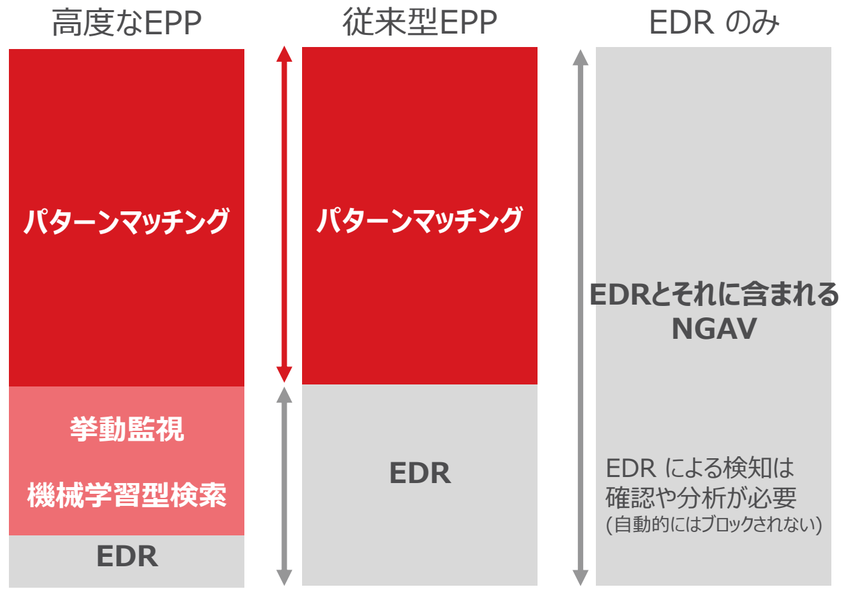
安全なアップデート環境の構成



マルウェアの引込み、情報流出をさせないためのアクセス制御

高度な検知機能の有効活用





パフォーマンス、運用の負荷、責任分界点に注意

脆弱性対策の必要性　仮想パッチ

クライアントへ流れるネットワークパケットから、OSやアプリケーションの脆弱性を悪用する攻撃コードを検出し、当該パケットをブロックすることで、脆弱性のリスクを低減します。

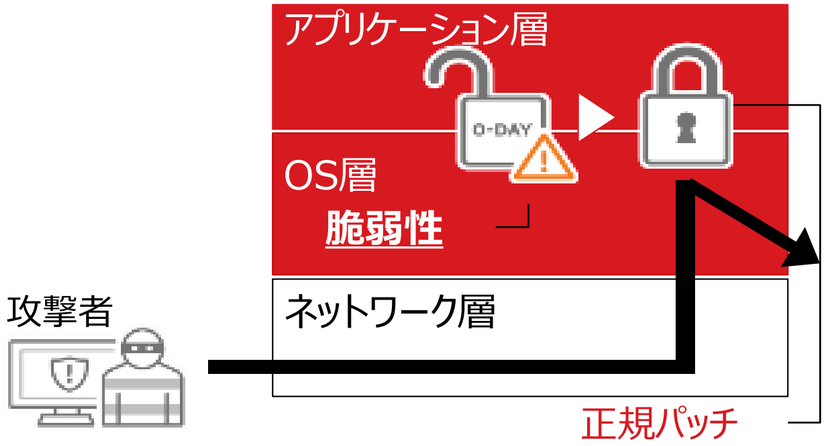
課題例①
OSやアプリケーションのパッチ適用に時間がかかり、全台への適用を徹底できない。

仮想パッチはOSやアプリケーションそのものを修正するわけではないため、迅速に脆弱性への攻撃リスクを緩和することが可能

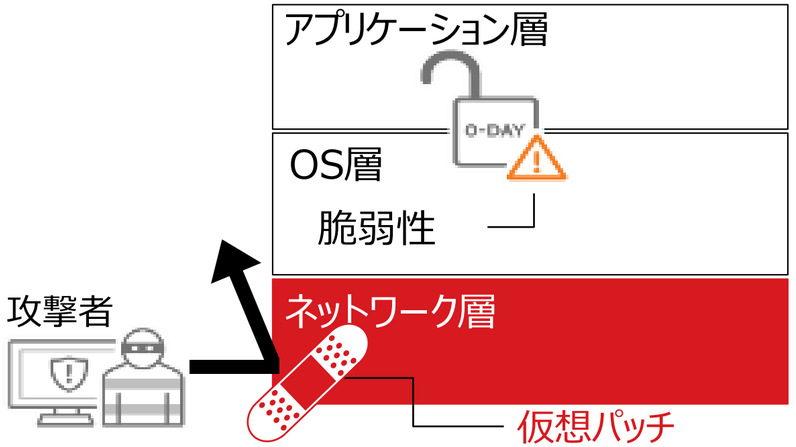
課題例②
内部ネットワークにおけるクライアント間の横感染のリスクを軽減したい。

ホスト型のIPSとして動作するため、ネットワークの境界を通らない Lateral Movement (横感染) を検知することが可能

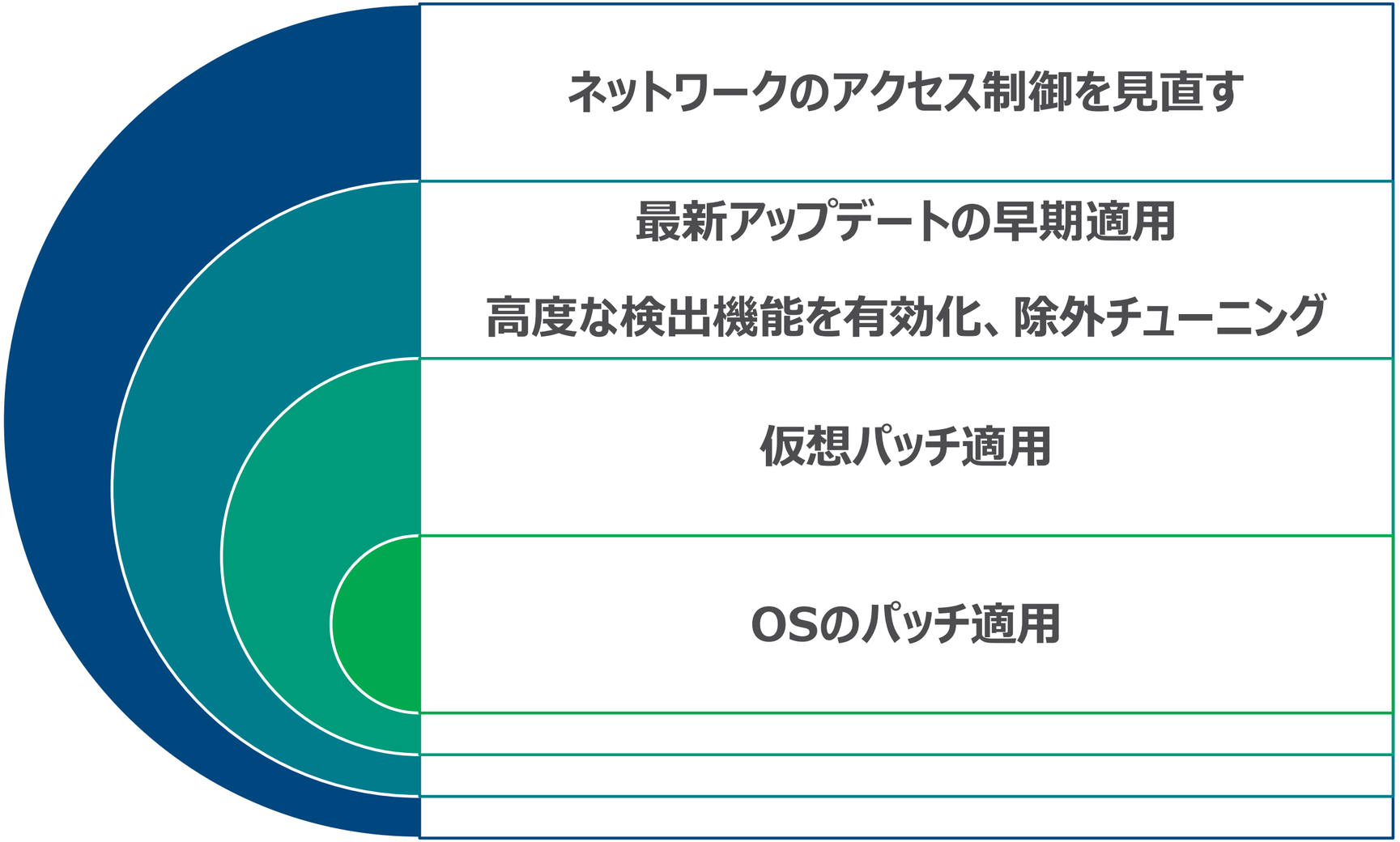
i) 正規パッチによる防御



ii) 仮想パッチによる防御



防御フェーズの強化案のサマリ



- ネットワークのアクセス制御を見直す
  - Trend Micro Apex One
  - Trend Micro Deep Security
- 最新アップデートの早期適用
  - 高度な検出機能を有効化、除外チューニング
  - Trend Micro Apex One
  - Trend Micro Deep Security
- 仮想パッチ適用
  - Trend Micro Apex One
  - Trend Micro Deep Security
  - Edge IPS
- OSのパッチ適用

実績No.1エンドポイントセキュリティ

Trend Micro Apex One™

Trend Micro Apex One™（以下、Apex One）は、ひとつのエージェントにエンドポイントに必要なセキュリティを集約。統合管理による一元的な可視化と制御が可能です。

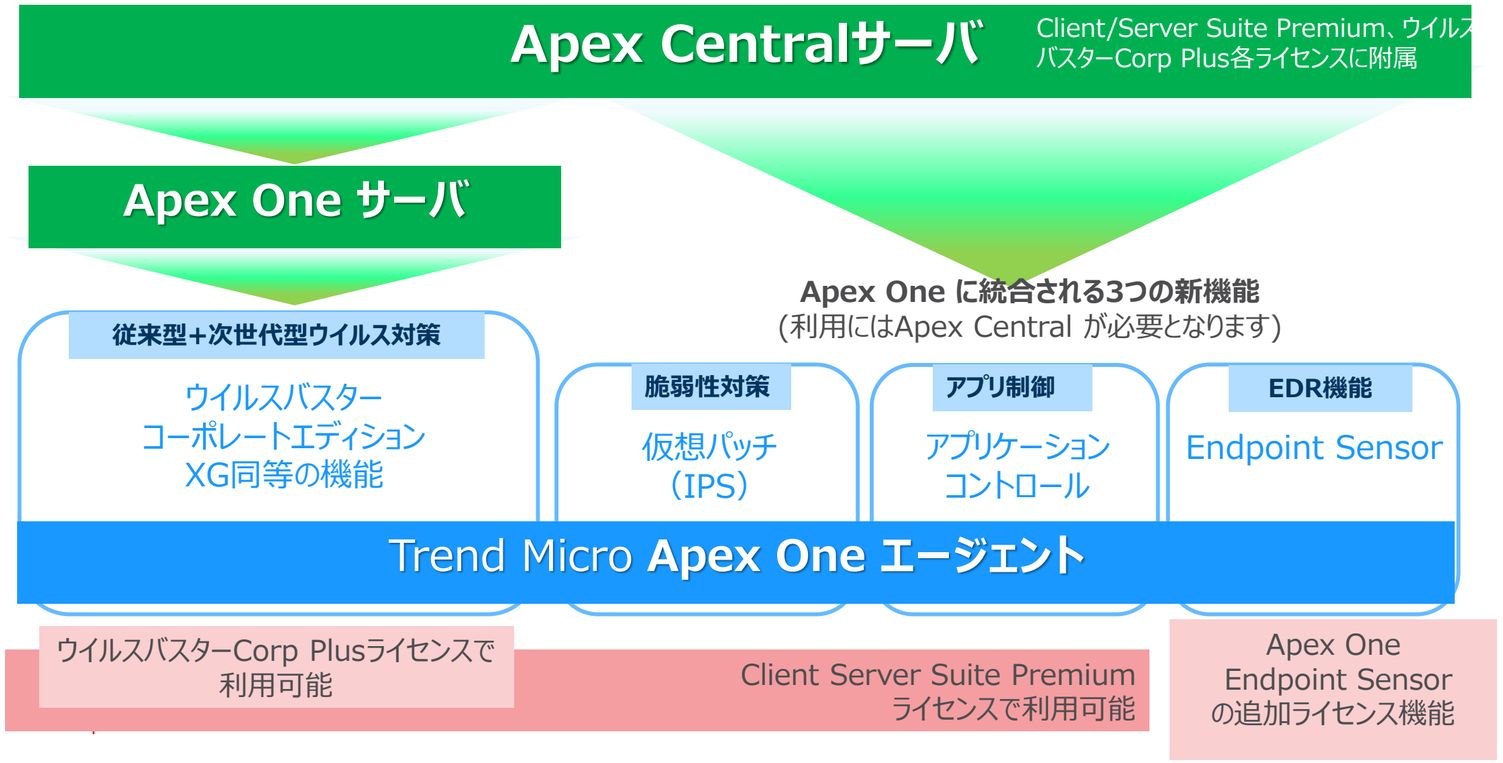
先進的な技術と実績ある技術の融合

- パターンマッチング
- 挙動監視によるファイルレス検出
- 機械学習型検索

エンドポイントに必要な更なる対策

- 脆弱性対策（仮想パッチ）
- アプリケーションコントロール

シングルエージェントで複数技術を組み合わせ、多層防御を提供します



Apex One が提供する機能	
通信制御	ファイアウォール
	Webレピュテーション
	仮想パッチ(IPS)
未然防止	デバイスコントロール
	アプリケーションコントロール
既知の脅威対策	パターンマッチング・スマートスキャン
	スパイウェア対策
未知の脅威対策 ・ファイル特性 ・ふるまい検知	機械学習型検索(ファイル)
	挙動監視・イベント監視・ランサムウェア対策
	機械学習型検索(プロセス)
	サンドボックス(Deep Discovery)連携
通信検知	クライアントファイアウォール
	Webレピュテーション
	不審接続監視
横感染防止	仮想パッチ(IPS)
EDR	Endpoint Sensor: Attack Discovery による痕跡の検出(EDR※)
	Endpoint Sensor: データレコーディングによる侵害調査(EDR※)
復旧	ダメージクリーンナップエンジン

※EDR = Endpoint Detection and Response

TREND MICRO

サーバにはマルウェア対策以上に、脆弱性対策の重要性が増しています

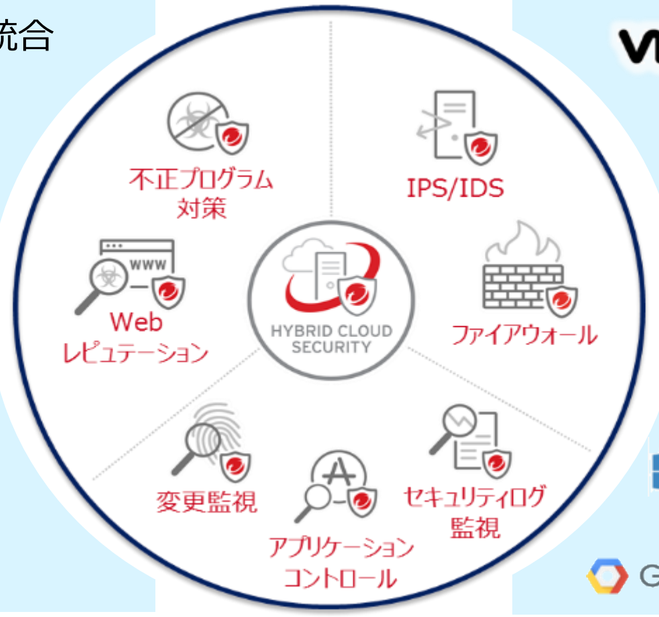
Trend Micro Deep Security

Deep Securityは複数のセキュリティ機能を統合的に提供します。（右図）

複数のセキュリティ製品を組み合わせる必要がなく、コストと運用負荷を最小化しつつ、サーバのセキュリティポリシーの統一化を図ります。

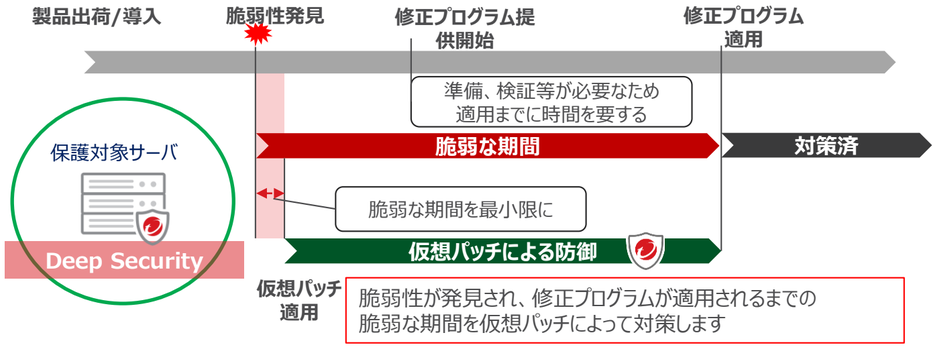
Deep Securityは多様なサーバ環境や標的型サイバー攻撃対策といったセキュリティ課題をシンプルに解決します。

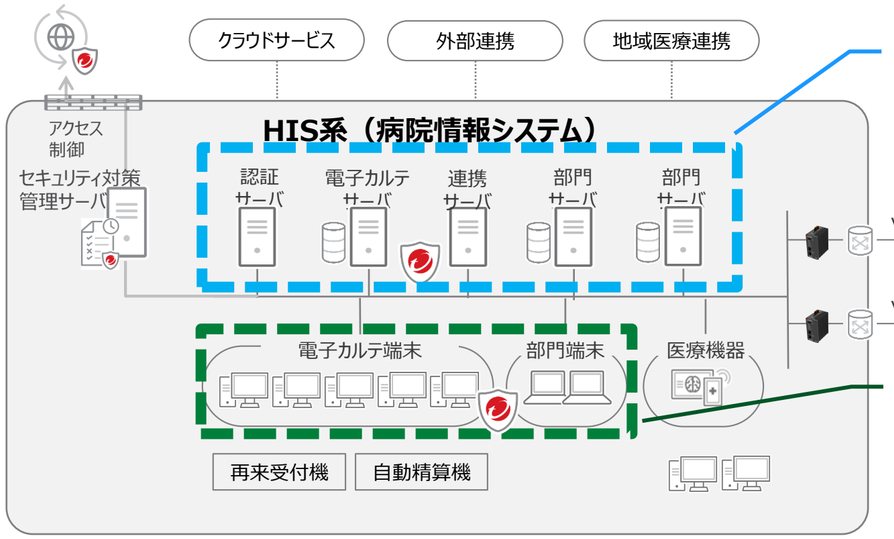
- クラウド環境のセキュリティ対策
- サーバ仮想環境のセキュリティ対策
- VDI環境のセキュリティ対策
- コンテナ環境のセキュリティ対策
- レガシーOS延命利用対策
- PCI DSS準拠支援



クラウドとの連携
- Auto Scaling対応
- コンソール連携

vmware
aws
Microsoft Azure
Google Cloud Platform





Trend Micro Deep Security

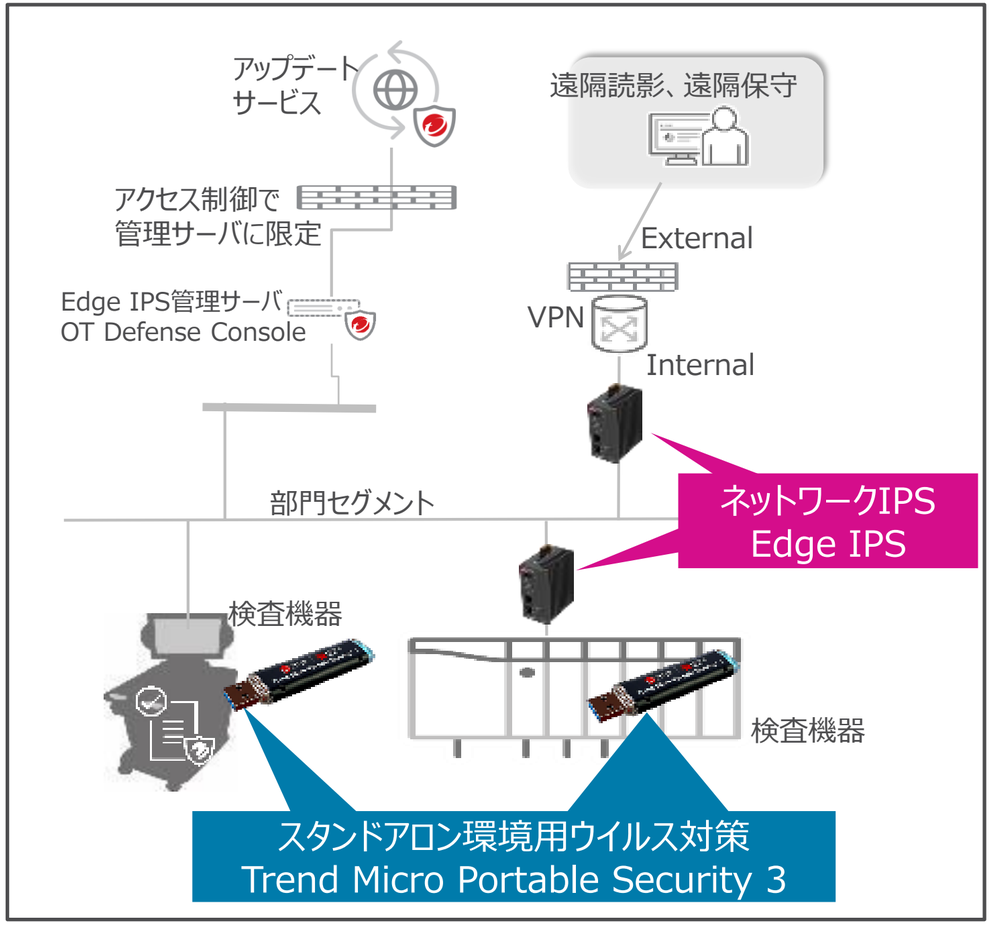
Trend Micro Apex One

医療機器等の脆弱性対策、リモートアクセス経路の侵入防御

Edge IPS

医療機器や保守アクセスポイントなどにインライン設置することで、
医療機器のOS脆弱性への攻撃や、アクセスポイントから展開されるネットワーク攻撃を検知、保護

重要資産の保護・可視化	• FW/IPS/Protocol Filter/DoS Preventionによる保護 • ZDIの知見を活用した産業向け高精度IPSフィルタの提供 • 資産情報、利用されているプロトコル情報の可視化
かんたん運用	• 透過型IPSにより既存設備のNW設定を変えることなく導入可能 • Web Consoleによる単独管理 • OT Defense Console(ODC)を利用した統合管理・監視
高信頼性ハードウェア	• スループット 200Mbps　ハードウェアバイパス有 • 入力電源2重化対応 • 動作温度範囲：-40 to +75℃　ファンレス設計



検知＝侵入を許しても早く気づいて実害を減らす

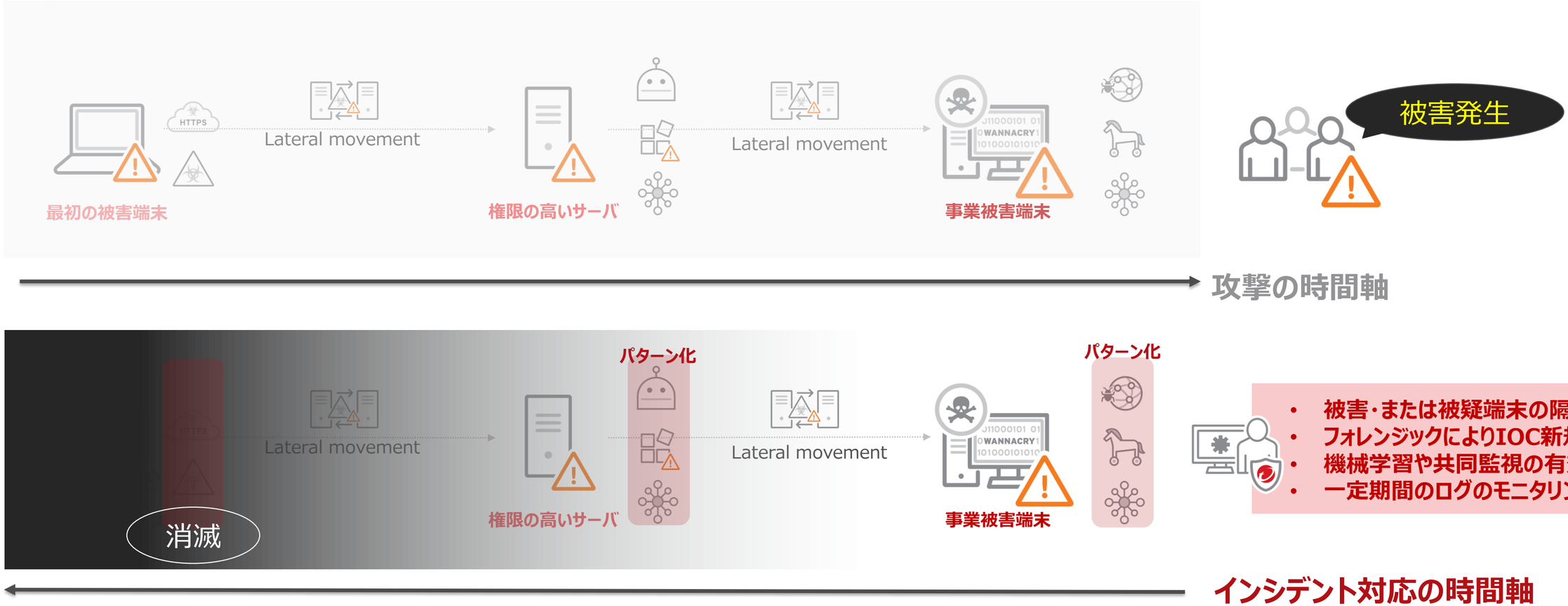
インシデント対応からわかる現実

- 大多数のユーザがパターンのみの運用
- 重大被害が発生してから対応を開始
- 調査に必要なログがローテートされている
- インシデント対応時に重要端末を初期化済
- 収束後に原因究明を求める

現実的な強化ポイント

- **エンドポイントでの活動を記録できるEDR**
- **ネットワークレイヤーでの挙動監視NDR**

ランサムウェア感染に対する実際のインシデント対応



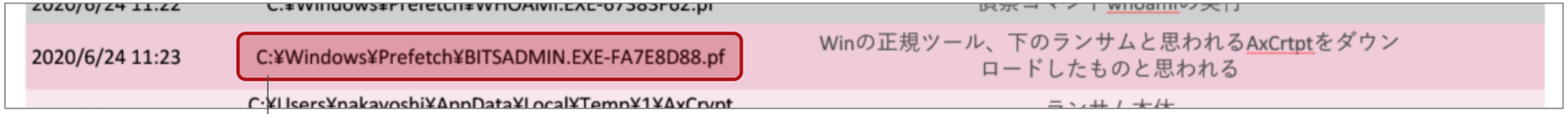
- 被害・または被疑端末の隔離
- フォレンジックによりIOC新規パターン化
- 機械学習や共同監視の有効化
- 一定期間のログのモニタリング

早期に攻撃に気づけず痕跡が消滅し、IOC情報や起点が途絶える

IoC (Indicators of Compromise)→侵害の痕跡

EDRはどのような粒度の情報を提供できるか？

MFT



正規ツールbitsadmin.exeを実行したことがわかる

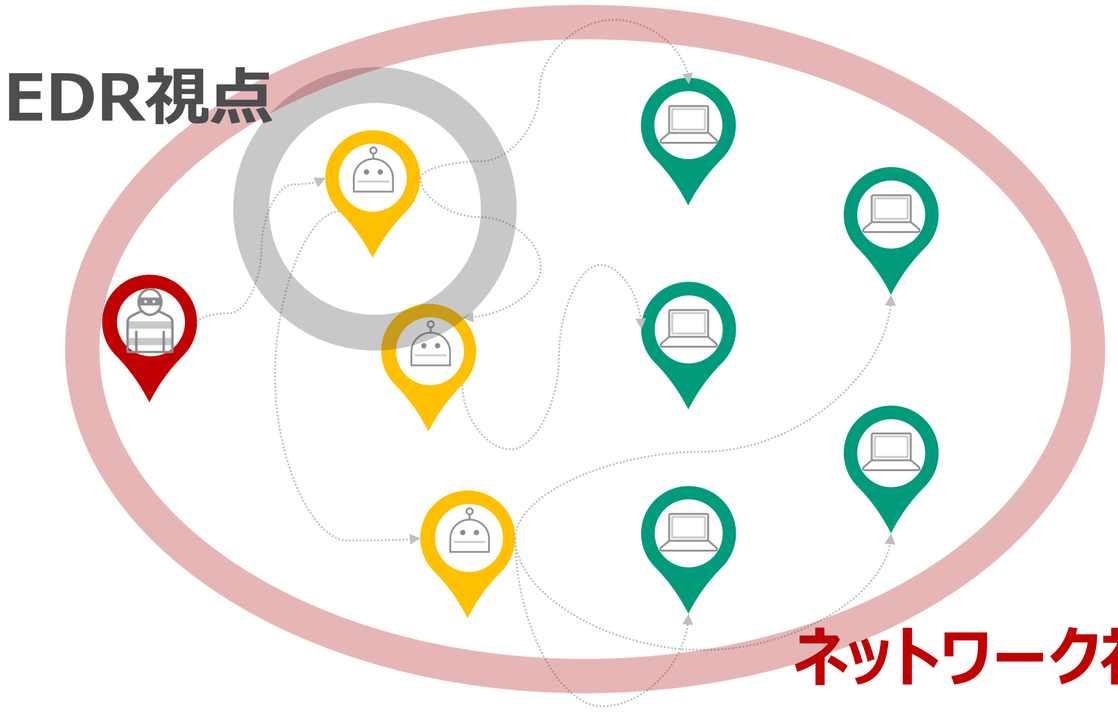
EDR

bitsadmin.exeを実行し、**不審サイトから不審な1.zipをダウンロード**

EDRにより調査において非常に有用な情報が記録される

ネットワーク領域での検知（NDR視点）

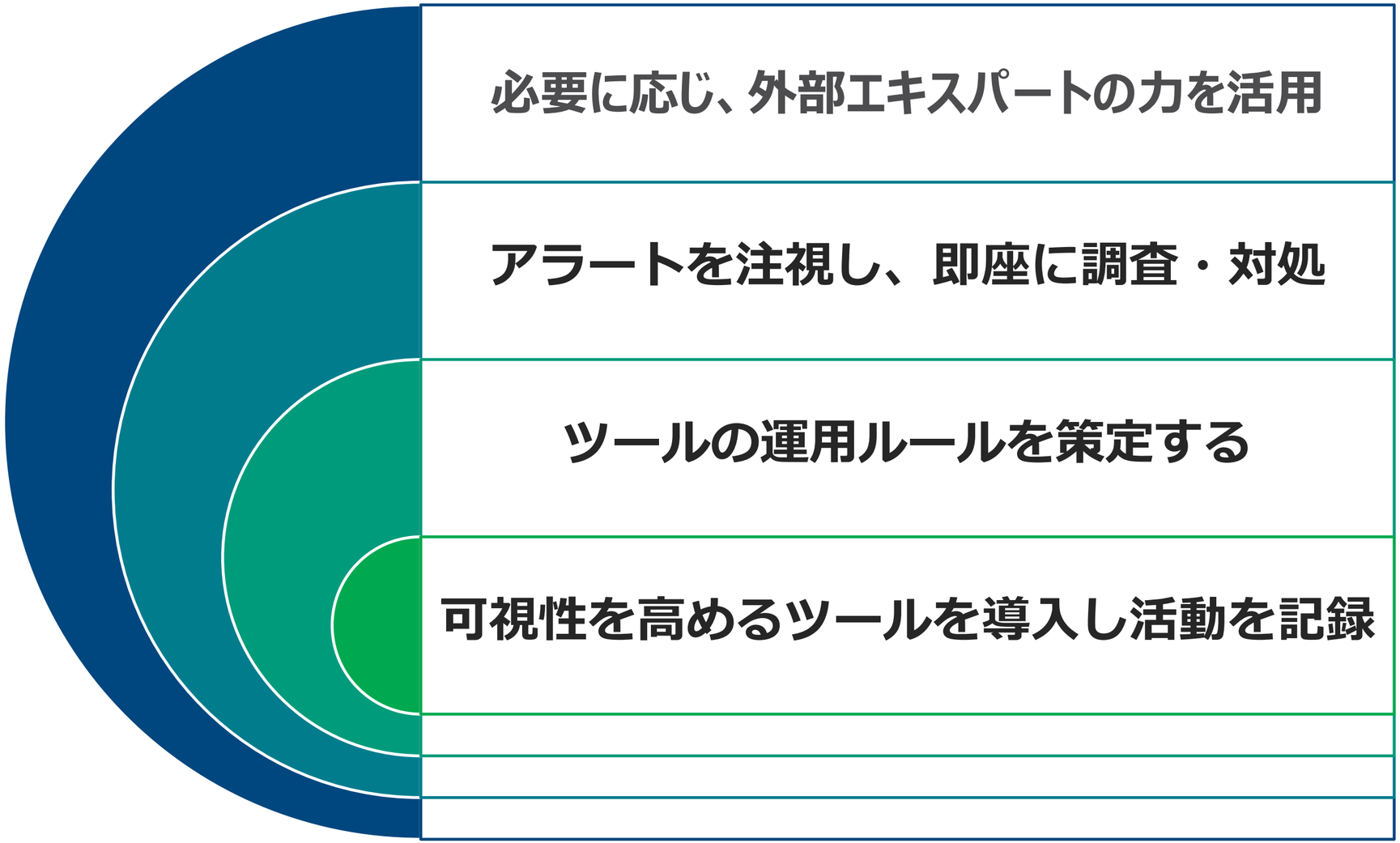
脅威の詳細	送信元IP	送信先IP	プロトコル
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request) - V			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request) - V			SMB
RADMIN - SMB2			SMB2
MPACKET - SMB2			SMB2
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
RADMIN - SMB2			SMB2
MPACKET - SMB2			SMB2
MS17-010 - Remote Code Execution - SMB (Request)			SMB
RADMIN - SMB2			SMB2
MPACKET - SMB2			SMB2
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request) - V			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request) - V			SMB
RADMIN - SMB2			SMB2
MPACKET - SMB2			SMB2
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request) - V			SMB
MS17-010 - Remote Code Execution - SMB (Request) - V			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request) - V			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB
MS17-010 - Remote Code Execution - SMB (Request) - V			SMB
MS17-010 - Remote Code Execution - SMB (Request)			SMB



WannaCry等でも悪用された脆弱性MS17-010を用いた拡散手法の実例。
不正ファイルのハッシュ値もアクセス先も数が多く、頻度も高いため、EDRの領域よりもネットワーク領域での可視化が適している。

Endpoint対策の導入が出来ないシステム、機器とのGAP
ネットワーク領域での可視化が有効

検知フェーズの強化案のサマリ



Trend Micro Apex One

Trend Micro Deep Security

Trend Micro Deep Discovery

トレンドマイクロの EDR ソリューション

完全 SaaS 型と、オンプレミス EPP と SaaS 型 EDR の2パターンがあります

従来型 アンチウィルス	次世代型 アンチウィルス (NGAV)	EDR	リスクの可視化/ ゼロトラスト*
・既知の脅威の検出 ・パターンマッチング	・未知の脅威の検出 ・挙動監視	・エンドポイントの活動ログの記録 ・インシデント対応	・環境のリスク可視化 ・アクセス制御

エンドポイントセキュリティを**オンプレミス**で運用する場合

Trend Micro Apex One (オンプレミス)	EDR: Endpoint Sensor

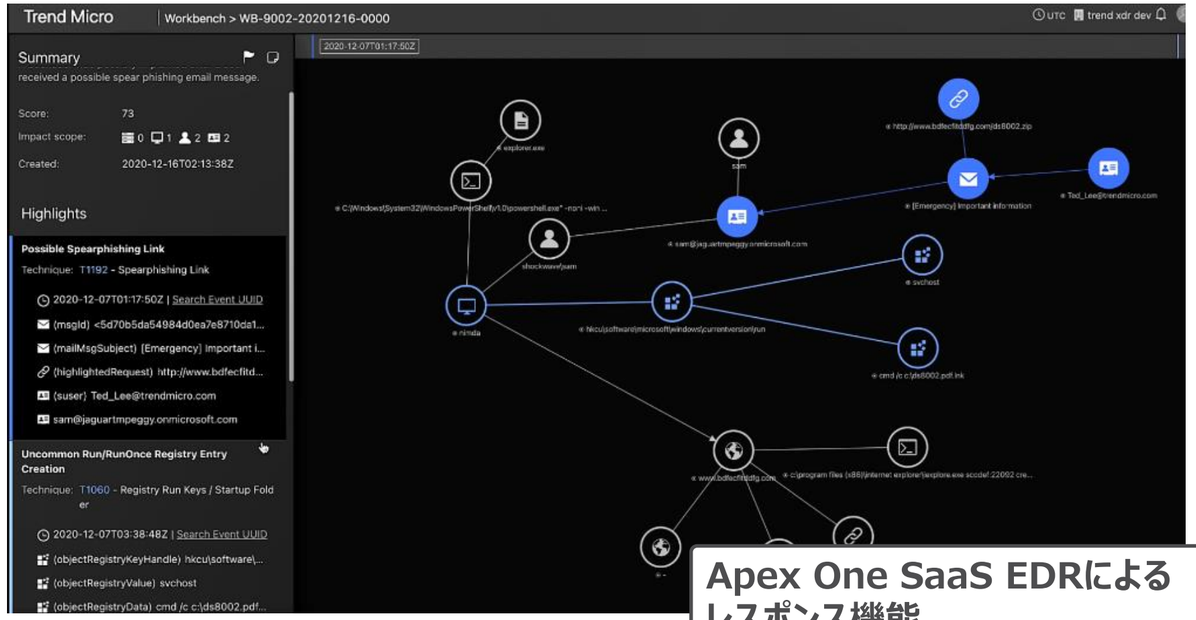
SaaS 型エンドポイントセキュリティと EDR のセットソリューション

Trend Micro Apex One SaaS with XDR(SaaS)

*リスクの可視化およびゼロトラストの機能はプラットフォーム Trend Micro Vision One 上で提供されます
（XDR ライセンスで利用可能です）

Endpoint対策/EDR　Apex One

- 不正プログラム対策、EDRの両機能を１エージェントで実装可能。
- バージョンアップ、パッチ適用不要で持ち出し端末にも対応可能。
- EPPでの検知→EDRへのシームレスな運用が可能。
- 相関分析によりEPPのみでは気づけないインシデントの予兆をとらえることが可能。
- 検体登録から2時間でのパターンファイル作成が可能であり、迅速なIRが可能。(有償サポート要)



EPP検知状況の確認

EDRでの証跡確認

相関分析による予兆検知

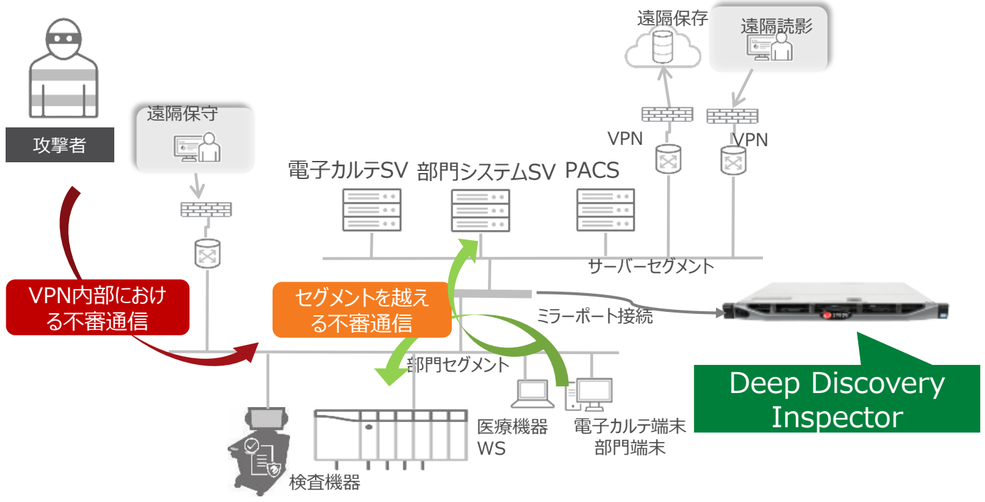
Apex One SaaS EDRによるレスポンス機能

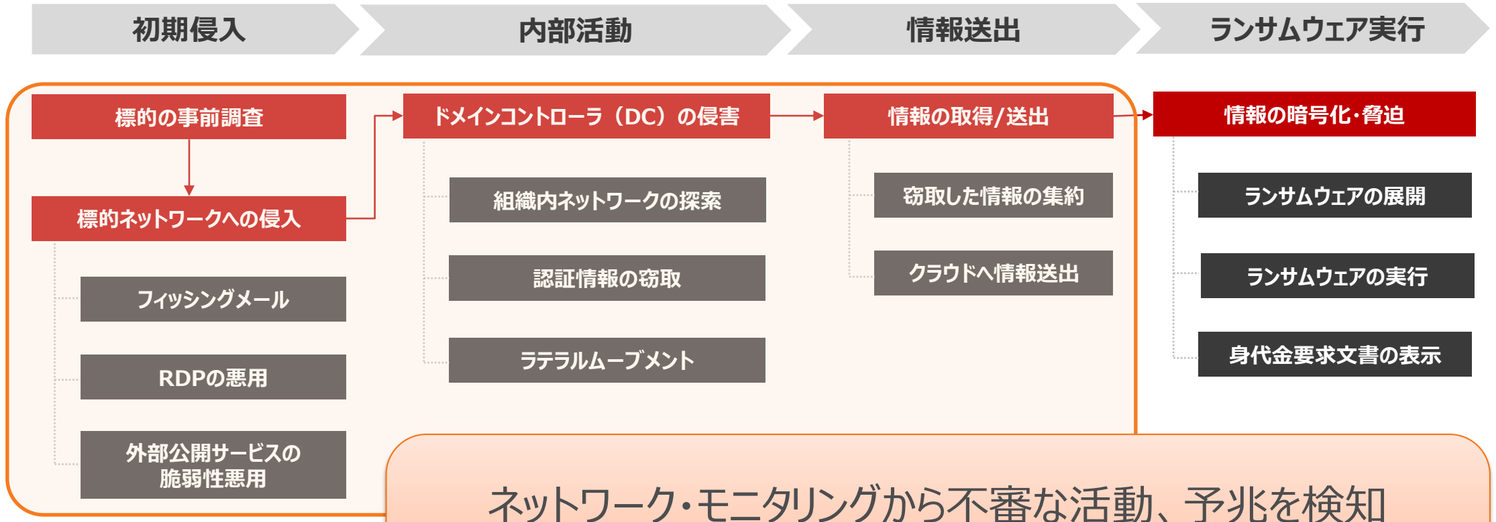
- **エンドポイントの隔離**
- **エンドポイントの復旧**
- **プロセスの終了**
- **ブロックリストへの登録**
- **ブロックリストの解除**

内部ネットワーク脅威監視・不審な活動のモニタリング

Deep Discovery Inspector

- 攻撃者は安全とされたはずのネットワーク内で攻撃活動を展開する
- 内部での攻撃活動は正規ツールによる隠ぺいが巧妙化している
- ネットワークを通じて展開される最新の攻撃を分析、知見をルール化することで早期に攻撃活動を検知し、早期対処に繋げる





内部ネットワーク脅威監視
Deep Discovery Inspector

複数レイヤを統合した分析、対処～Zero Trustへ

Vision One

各所に配置されたセンサーからテレメトリを収集、相関分析して…

脅威を可視化、レスポンス
XDR（eXtended Detection & Response）

MITRE TTPsベースの精密なアラート化	アラート一覧チェックと詳細分析（RCA）
ログクエリ検索	レスポンス（リモート操作等）
セキュリティ分析エンジン	ユーザIOCによる検索

リスクを可視化、予防
Zero Trust Risk Insight

ID / ユーザベースのリスク可視化	クラウドアプリ利用のリスク可視化
デバイスのリスク可視化（ハイリスク脆弱性情報含）	リスク要因の提示

Zero Trust Secure Access

（開発中）ポリシー、リスクに基づいた動的なアクセス制御

データレイク (各製品、機能からのデータ)

SIEM (Splunk)

(開発中) Access Control (3rd party/ TM)

Apex One

Cloud One

Cloud App Security

Deep Discovery

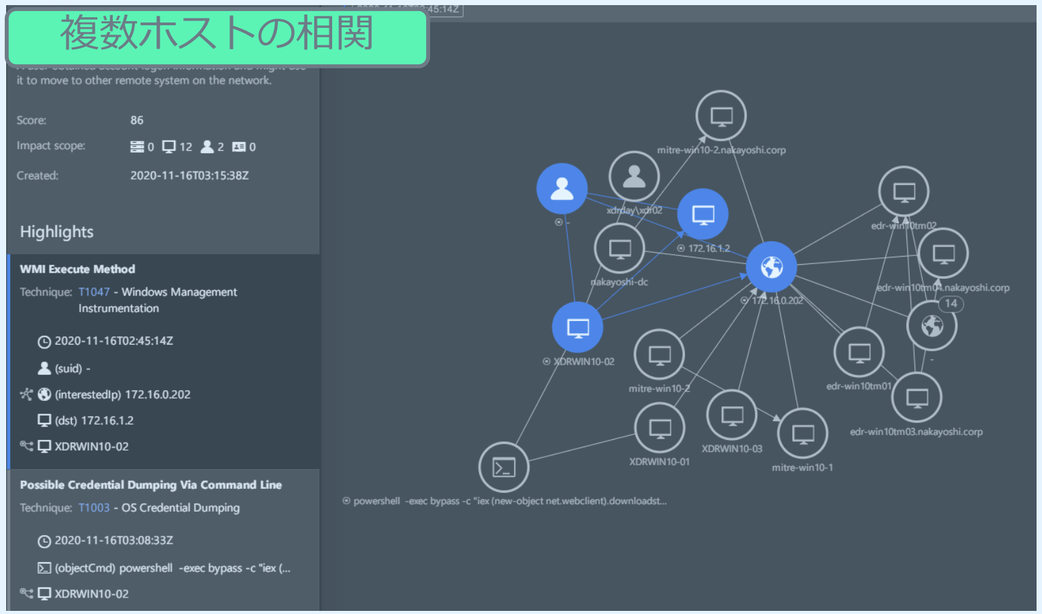
TM Web Security

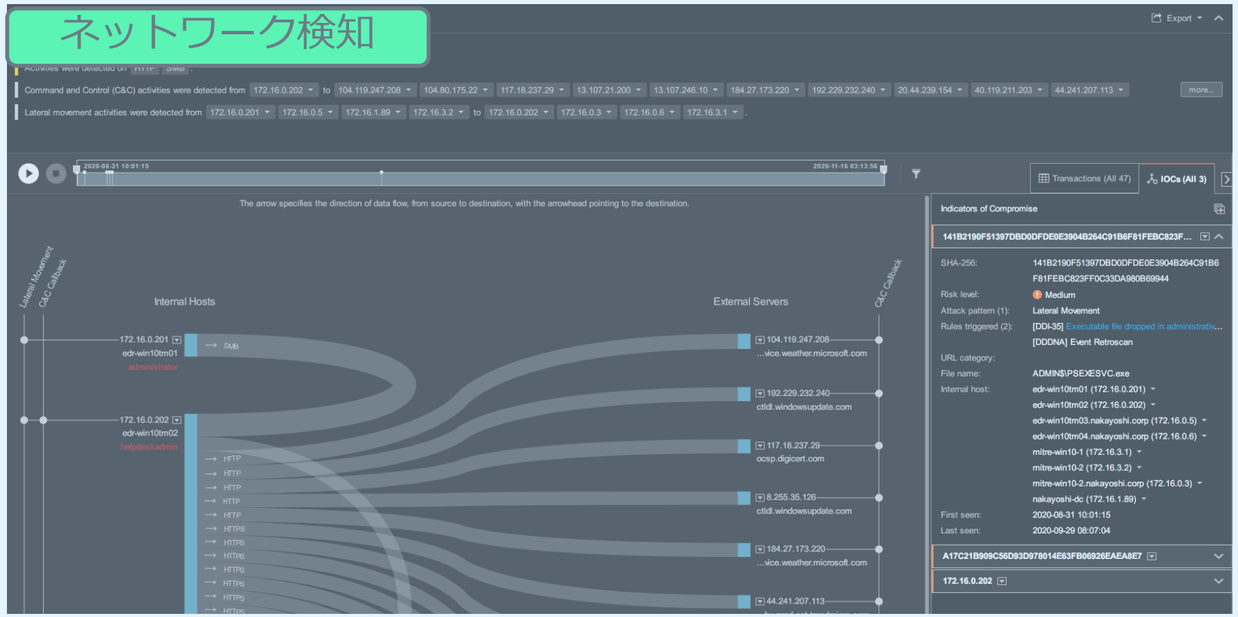
Azure AD, Okta

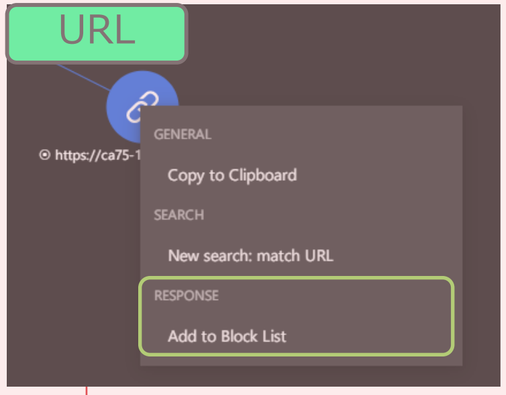
他のWeb Gateway

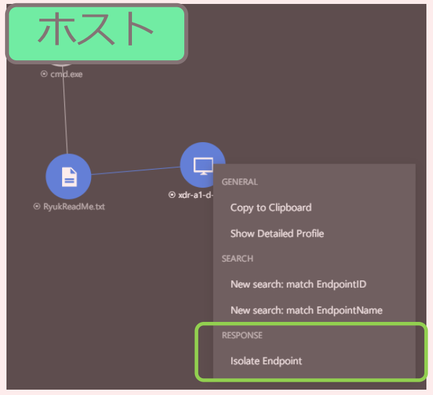
他3rd party (開発中)

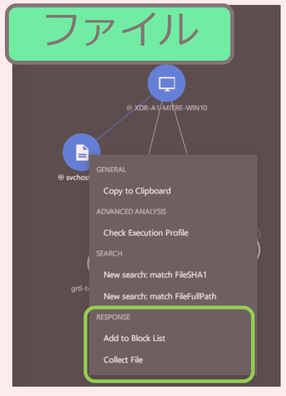
Vision One:サイバーセキュリティのトータルプラットフォーム











複数レイヤーでの相関検知

複数レイヤーでの対応機能

対応＝復旧の前に原因究明

原因究明、問題解決をしない復旧は再発リスク

災害モードでの業務継続と、組織内、サプライヤーとのチームワークが求められる

サイバーセキュリティは災害対策同様インシデント対応の訓練が重要

インシデント対応ボードゲーム

インシデント対応ボードゲームとは

セキュリティインシデント対応の机上訓練をボードゲーム形式で行うことで、有事発生時の自組織の対応力を事前に理解するためのツール
PDFデータはホームページからダウンロード可能

対象者

インシデント対応に携わるステークホルダー
情報システム部門責任者、システム管理者、経営責任者、事務部門責任者、医療部門責任者、本部担当者など

プレイ人数、プレイ時間

4～7名、1ラウンド40～50分（通常2ラウンドで実施）

厚生労働省・医療情報システムの安全管理に関するガイドライン第5.2版
6章　6.10　B項（考え方）
・非常時に備えたセキュリティ体制の整備
一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、そのために情報セキュリティ責任者(CISO)等の設置や、緊急対応体制（CSIRT 等）を整備するなどが強く求められる。
6章　6.10　C項（最低限のガイドライン）
・非常時における対応に関する教育及び訓練を従業者に対して行うこと。なお、医療情報システムの障害時の対応についても同様に行うこと。

診療録管理体制加算 施設基準（様式17）
- 専任の医療情報システム安全管理責任者の配置の有無（ 有 ・ 無 ）
- 職員を対象とした情報セキュリティに関する研修の実施

ある日、医療情報部にこのような報告、問い合わせがばらばらと・・・

電子カルテサーバのレスポンスが低下

ファイルサーバのファイルが開けない

さて、どうしたものか・・・

情シス部門責任者　経営責任者　医療部門責任者
システム管理者　事務部門責任者

トレンドマイクロ　ボードゲーム　医療

検索

まとめ

- ネットワークアクセス制御で到達範囲を必要最小限にする
- OS、アプリケーションの脆弱性を早期に修正する
- マルウェア対策は常に最新に・高度な検知設定を活用する
- 脅威活動のモニタリングにより未知の攻撃を早期に検知する

TREND MICRO™

THE ART OF CYBERSECURITY

An Innovative Approach to Cybersecurity

トレンドマイクロのクラウドセキュリティプラットフォームによる、日本におけるハイブリッドクラウドワークロードの自動保護。**実際のデータを使用し、トレンドマイクロの脅威リサーチャーでアーティストでもあるJindrich Karasekによって作成されました。**