ESET XDR ソリューションのご紹介

イーセットジャパン株式会社

2024/03

Digital Security
Progress. Protected.

はじめに

本資料は、2024年3月現在の情報に基づき作成されています。

最新脅威に対応するため、 ESETでは随時新機能のリリースを行っています。
新機能の搭載や既存機能の改修などにより、本資料の記載内容と異なる場合があります。

日々変化する脅威やサイバー攻撃手法に対応し、顧客を脅威から最大限に保護するため、
ESETでは最新テクノロジーを逸早く搭載するESETのSaaSソリューションのご利用を推奨しています。
このため、本資料はESETのSaaSソリューションのご利用を前提に用意しています。

日本を取り巻くサイバー空間の状況

高度化する攻撃手法	標的型攻撃	脆弱性を突く攻撃	ランサムウェア
• ファイルレス攻撃 • 署名付きモジュールを悪用した攻撃 • 正規なプログラムを悪用した攻撃	• 取引先に装った標的型メール • 外部公開された情報を悪用した攻撃 • サプライチェーンの弱点を狙った攻撃	• Apatch Struts 2 • Log4j • SMB	• Wannacry • LockerGoga • MegaCortex • LockBit

約**2,684**億円/年

日本におけるインシデント
損害賠償額の総額

約**6**億円/件

日本におけるインシデント
あたりの損害賠償額

約**3**万円/人

個人情報流出時１件あた
りの平均想定損害賠償額

Source: https://www.jnsa.org/result/incident/2018.html

インシデント発生に伴うビジネス影響

事業の停止

企業機密の漏えい

企業価値の低下

企業ブランド力の低下

等々

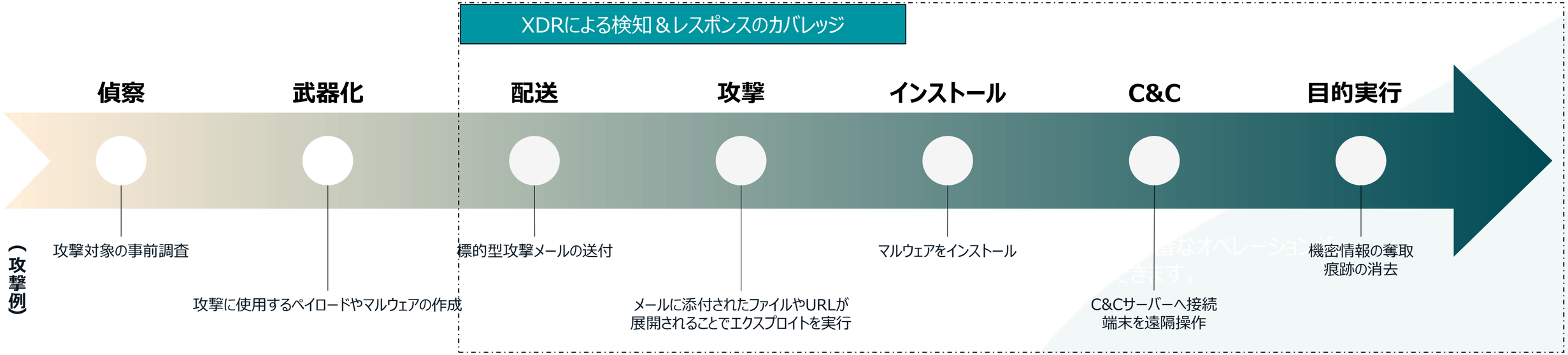
多様化するサイバー攻撃に必要なセキュリティ対策

情報セキュリティ10大脅威 2024 [組織]	
順位	「組織」向け脅威
1	**ランサムウェア**による被害
2	**サプライチェーンの弱点**を悪用した攻撃
3	**内部不正**による情報漏えい等の被害
4	**標的型攻撃**による機密情報の窃取
5	**修正プログラムの公開前**を狙う攻撃 （**ゼロデイ攻撃**）

昨今のサイバー攻撃は、脆弱性や、サプライチェーン上の弱点、内部不正など企業の**「弱点」**を狙う攻撃が増えています。

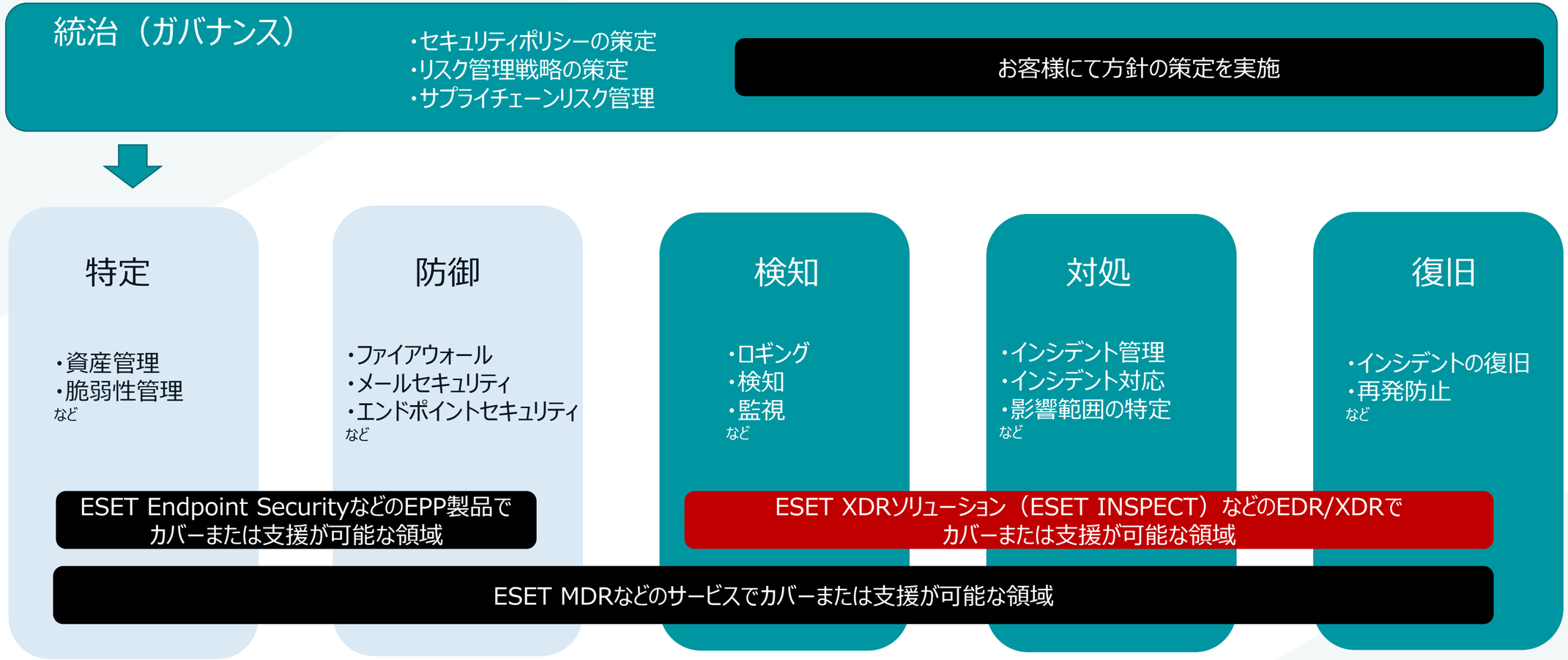
OSや、ネットワーク機器の脆弱性を突いて秘匿性の高い手段を用いられることが多く、インシデントに**早期に気づく**手段として、XDR（Extended detection and response）が有効です。

Source: https://www.ipa.go.jp/security/10threats/10threats2024.html



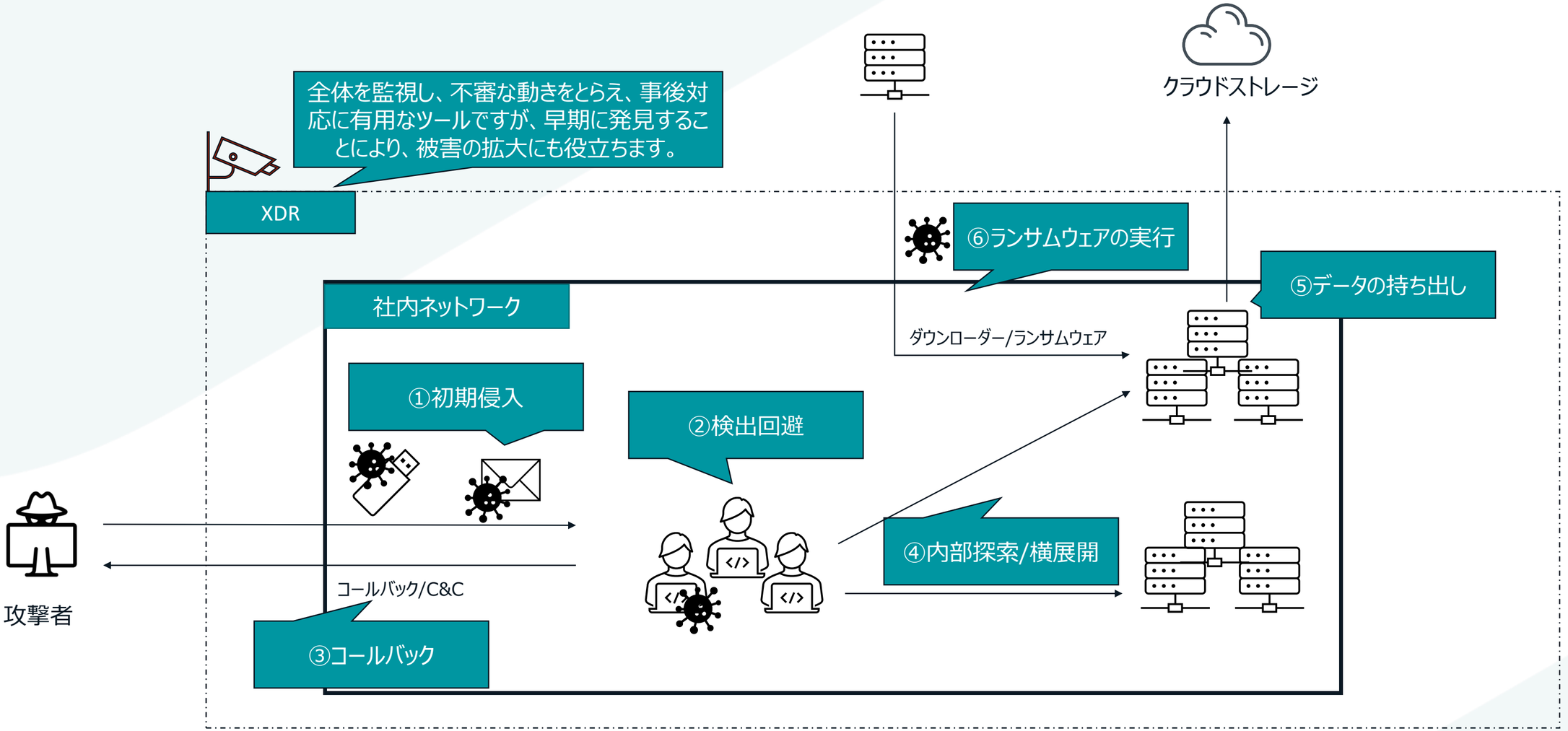
グローバルサイバーセキュリティ基準から見る必要なセキュリティ対策

米国NISTのサイバーセキュリティ技術レベル基準(ver2)から見る必要なセキュリティ対策



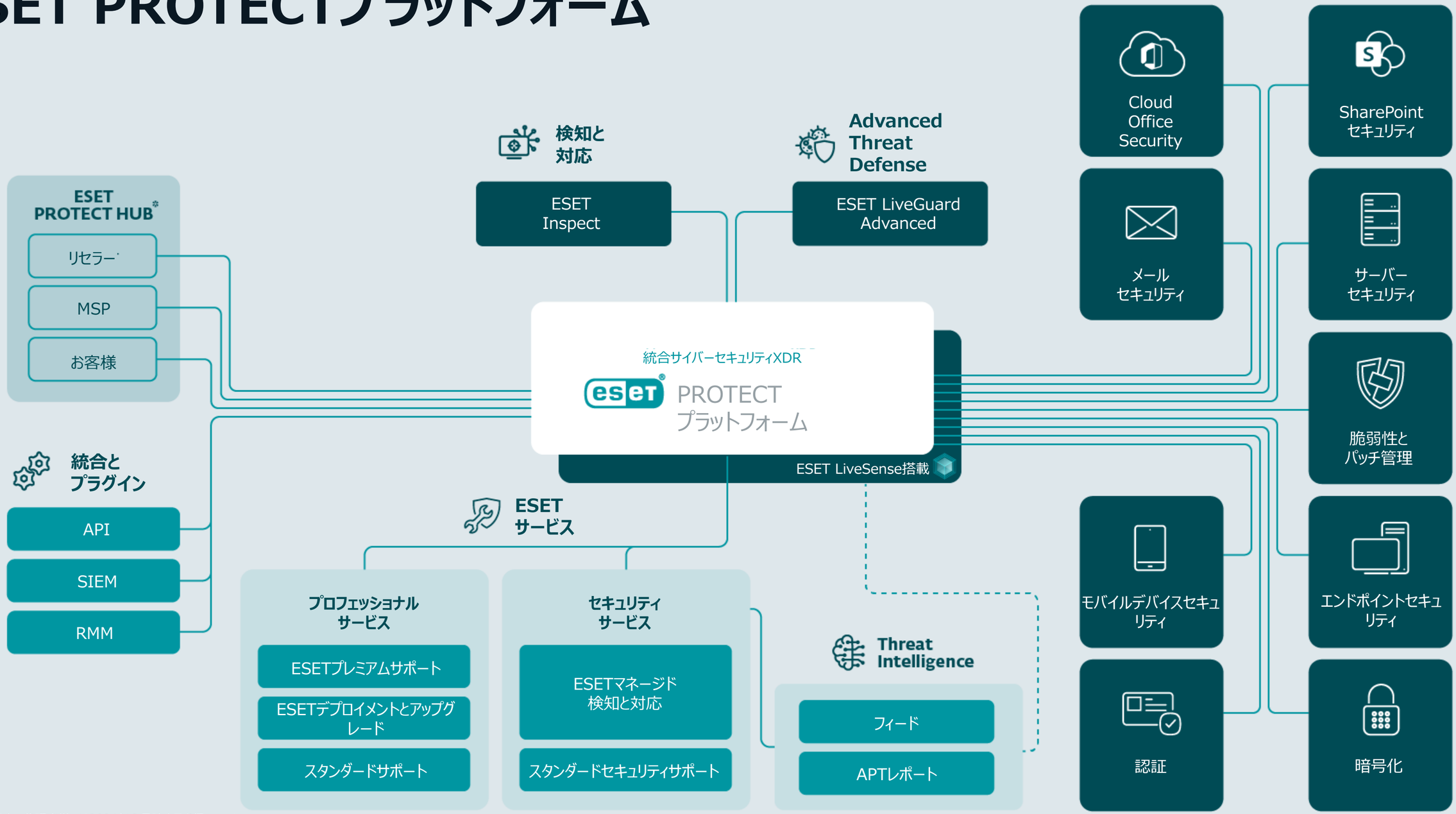
Source: https://www.nist.gov/cyberframework

実際の攻撃事例から見るXDRの必要性



昨今のサイバー攻撃は最終目的を達成するため、一連の攻撃フェーズを経て攻撃を展開。
XDRでは常に各端末のログに対してAIモデルを用いて解析を行い、感染拡大を防ぎインシデントに対して
プロアクティブな対応を実現可能。

ESET PROTECTプラットフォーム

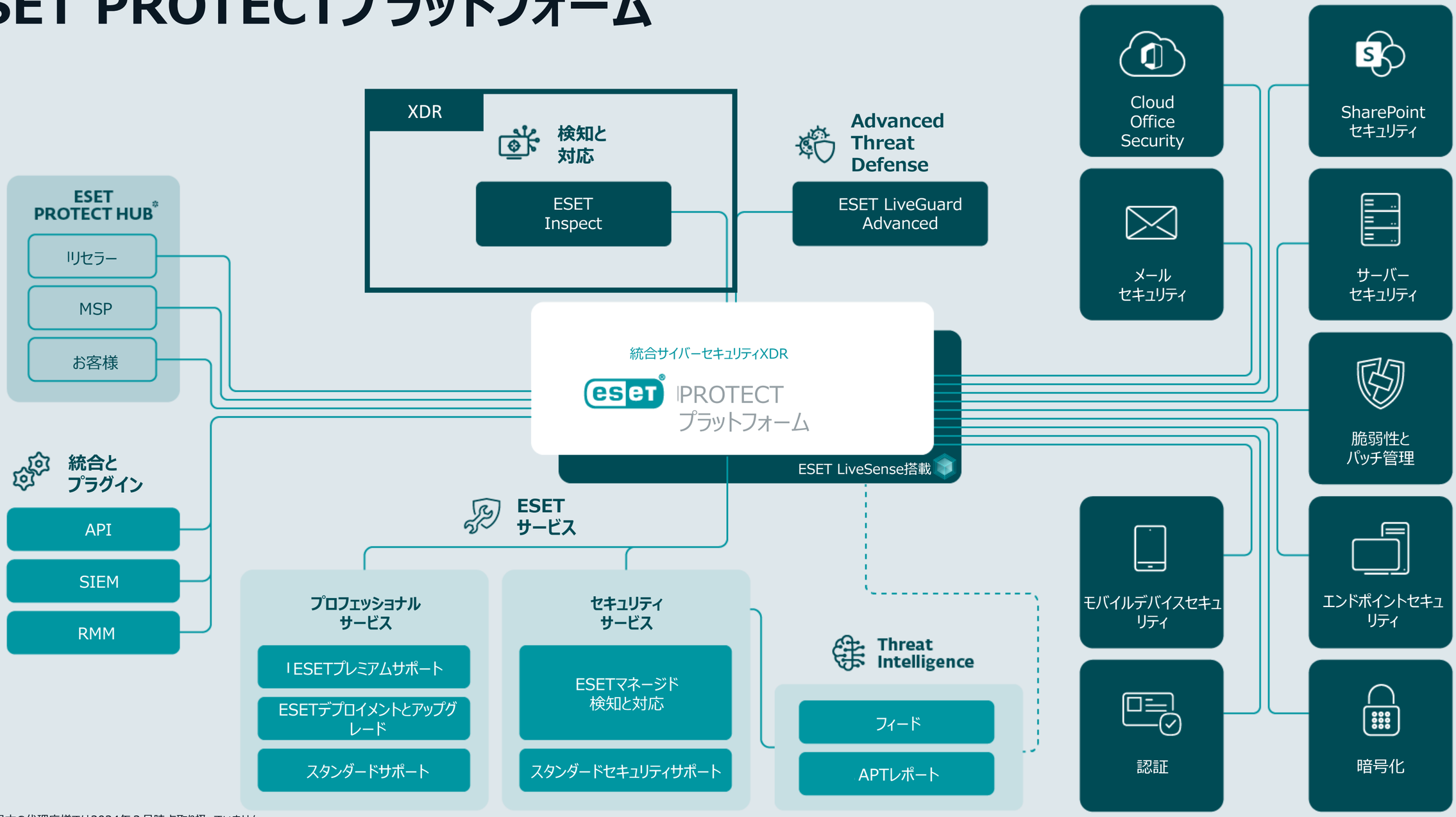


※メールセキュリティは日本の代理店様では2024年３月時点取り扱っていません
※クラウド版のSecure Authenticator（認証）は2024年中のリリース予定です

ESET PROTECTプラットフォームの特徴

シングルプラットフォーム	防御から検知、レスポンスまで単一のセキュリティプラットフォームで実現。 EPPの強い防御力とXDRの強い検知力のシナジーを生み出す。
AI搭載	EPPもXDRもAIエンジンを搭載。 長年培った脅威ナレッジを用いたAIモデルを使用し、予測能力と検知能力が大きく向上。
簡単導入	SaaSソリューションで管理サーバの構築は不要。 XDRもEPPも一回のインストールで完了。 事前定義済みのルールやセキュリティポリシーをそのまま利用可能でセキュリティはわずかの数クリックで向上。

ESET PROTECTプラットフォーム



※メールセキュリティは日本の代理店様では2024年３月時点取り扱っていません
※クラウド版のSecure Authenticator（認証）は2024年中のリリース予定です

ESET XDRソリューションの特徴

ESET XDRソリューション ５つのポイント

※IDCが提唱するEDRを選定する際に考慮すべき5つのポイントです。

先進性 — **AIを活用**し、日々進化する攻撃に対応

信頼性 — EPP機能を取り入れ、**防御力を損なわず**に検知力が大きく向上

直感性 — AIによる相関分析で事象の全体像を把握しやすく、**直感的にわかりやすい**UIを実装

保守性 — 自社でSOC体制の構築が困難な場合もMDRサービスは別途契約可能で、**24時365日の監視サービス**を提供

運用性 — SaaSソリューションで**メンテナンスフリー**

ESET XDRソリューションの特徴

シングルプラットフォーム ESET PROTECTでXDRとEPPをまとめて管理

在宅ワーク、複数の拠点をまとめて
単一のプラットフォームで管理

ダッシュボードはカスタマイズ可能で
企業のセキュリティポリシーに合わせて柔軟に編集可能

企業全体のセキュリティリスクを可視化

脆弱性を継続的にモニタリングし、パッチ適用の自動化が可能

ポリシーを指定し、企業全体に単一のポリシーを適用し、**ガバナンスが向上**

エンドポイント、サーバー、EDRを単一のプラットフォームで一元管理

ESET XDRソリューションの機能

AIモデルやESET独自の技術を搭載したESETのXDRソリューション

ESET INSPECTの提供機能

検知

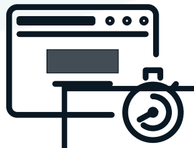
不審なアクティビティの検知

可視化

機械学習アルゴリズムを用いた相関分析

対応

インシデント対応機能の自動化、スレッドハンティング



スレッドハンティングやRoot Causeアナリシスに必要な情報や痕跡（IoC）を記録。

ESET事前定義のルールを使用可能。
環境に応じてカスタマイズルールにも対応し、環境に特化したインシデントの検知も可能。

AI技術を活用し、特定のインシデントに対し、相関分析でインシデントの全体像を把握。

ESET独自のレピュテーションサービス（LiveGrid）を用いてプロセスに対してスコアリングを行い、プロセスの危険度を可視化。

管理コンソールからワンクリックで端末を隔離可能

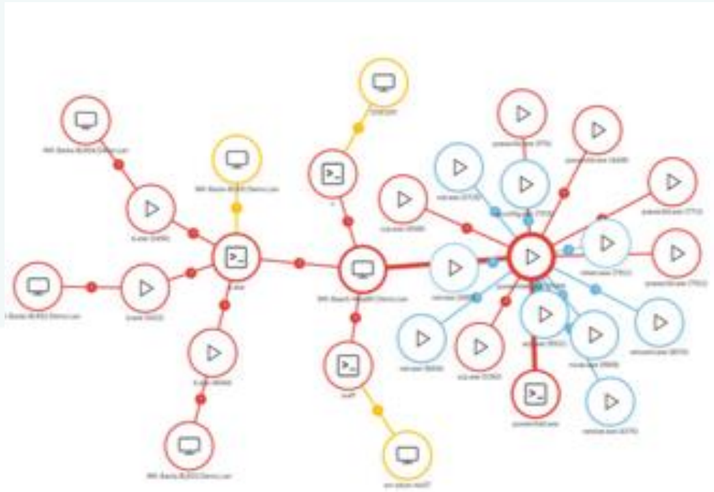
特定のイベントに対してトリガー（隔離、インシデントの発令など）を設定することが可能で、オペレーションの自動化を実現。

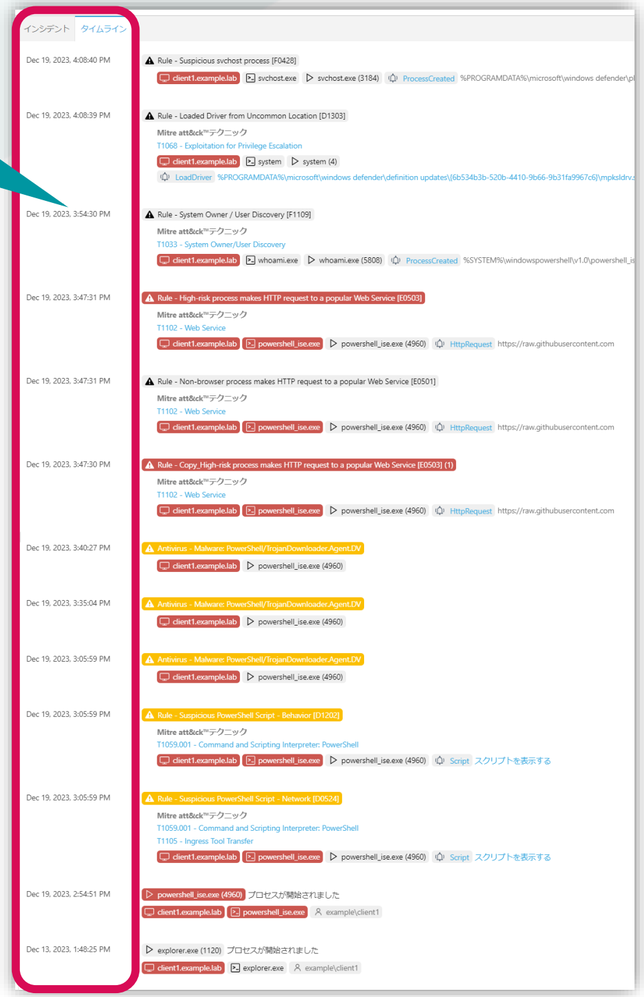
ESETのマルウェアリサーチャーが作成した1,000個以上の検知ルール（ルールは不定期に追加）を用意しており、
MiTRE ATT&CKフレームワークとの高い親和性を持つ。

ESET INSPECT – 相関分析

AI技術を活用し、相関分析でインシデントの全体像を把握

対象端末でインシデントに関係する不審な可能性のあるビヘイビアを時系列で表示





■機能概要

AIモデルを活用し、独自の機械学習アルゴリズムを用いて、インシデントの全体像を可視化。

インシデント対応に有用な情報を抽出し、**AIによる相関分析**を行いインシデントの全体像を把握しやすくなり、調査時間の短縮を実現。

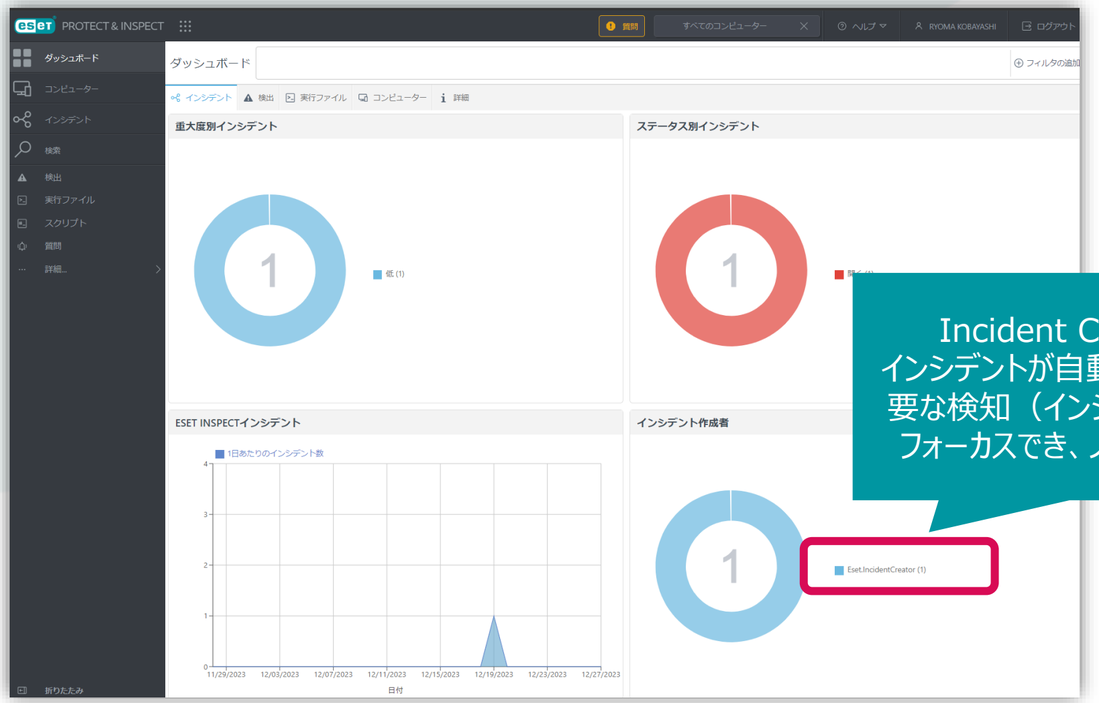
■特徴

インシデントが上がった際に、時系列、タイムラインなどを確認し、相関分析が自動的に行われ、**調査スコープを限定し、**迅速な初動対応、事後インシデント対応の効率化が向上されます。

相関図が表示され、インシデントに関与するオブジェクトの可視性が大きく向上。
タイムラインが表示され、インシデントの時系列を追うことでインシデントの全体像を把握可能。

ESET INSPECT – インシデント自動作成機能

ノイズを減らし、オペレーションの最適化を実現



Incident Creatorにより、インシデントが自動的に生成され、重要な検知（インシデント）の対処にフォーカスでき、ノイズが軽減される

■機能概要

EDRによる検知の中から重要度の高いものを「インシデント」として検知し、インシデント（重要度の高いもの）を優先的に対応することにより、**オペレーションが最適化される**

■特徴

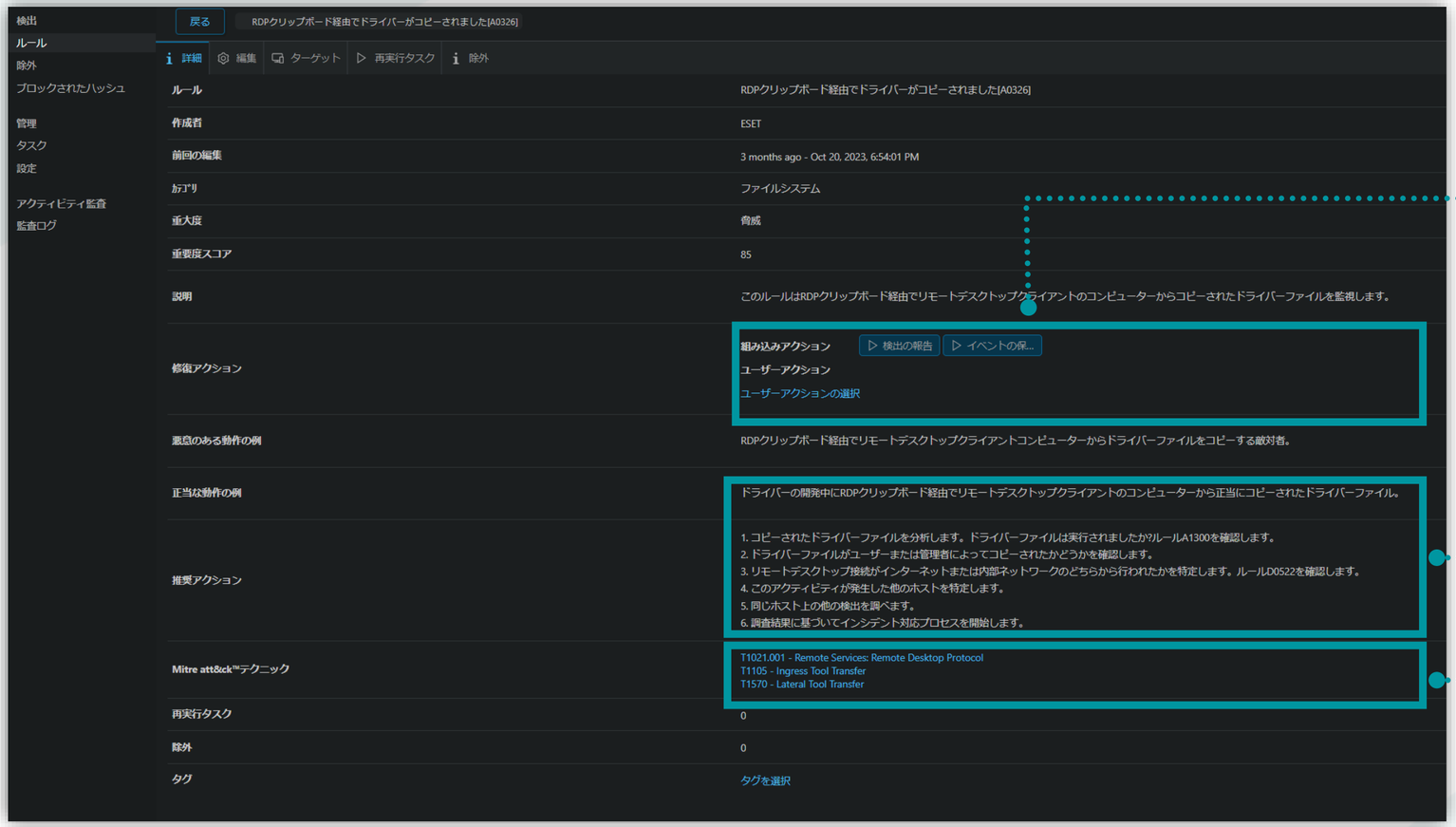
利用環境で確実に不審な動きだと判断できる検知に対してインシデントのフラグを付けることによって、インシデント報告の自動化を実現。

※例：
EPPによるランサムウェアの検知時
EIでPowershellによるマルウェアダウンロードの試行時

ESET INSPECT – 視覚的にわかりやすいコンソール

日本語対応済みで、検知時の推奨アクションも確認可能

コンソール（検知ルール、検知時のアクションを含む）は日本語化されており、検知時に推奨アクションを参考に
検知内容への対処が可能



検知時のアクションを指定し、
検知時の対応（端末の隔離や
インシデントの発令）を自動化

推奨アクションの一例：
RDP（リモートデスクトップ）経
由でドライバーファイルのコピーが
行われた際に取るべき行動

MiTRE ATT&CKとの
マッピング

XDRにもEPPが必要な理由

ESETはランサムウェアを含んだマルウェア対策に**NGAV（機械学習、振る舞い検知）とパターンマッチング方式**の両方を実装。

検出技術	強み	弱み
NGAV	実行前のファイル特徴や、実行後の挙動で判定するため 未知の脅威へも対応可能	実際の振る舞いや学習データに基づく判断となるため、 精度は低い
パターンマッチング	既知脅威の検出率が高く、誤検出率が低い	未知の脅威への対応は発見後のパターン更新が必要

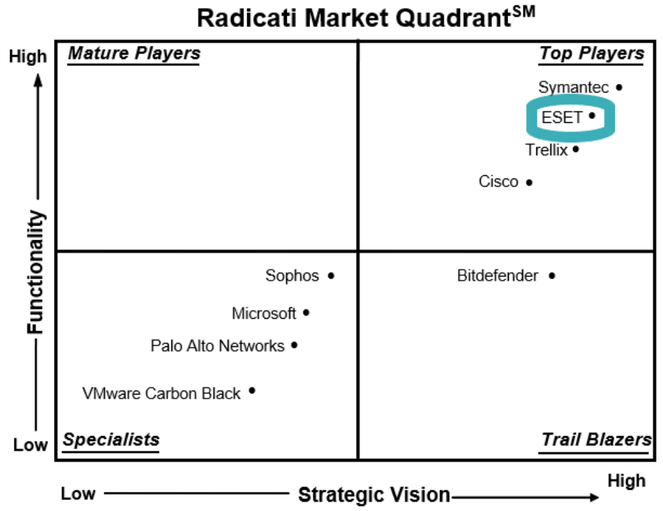
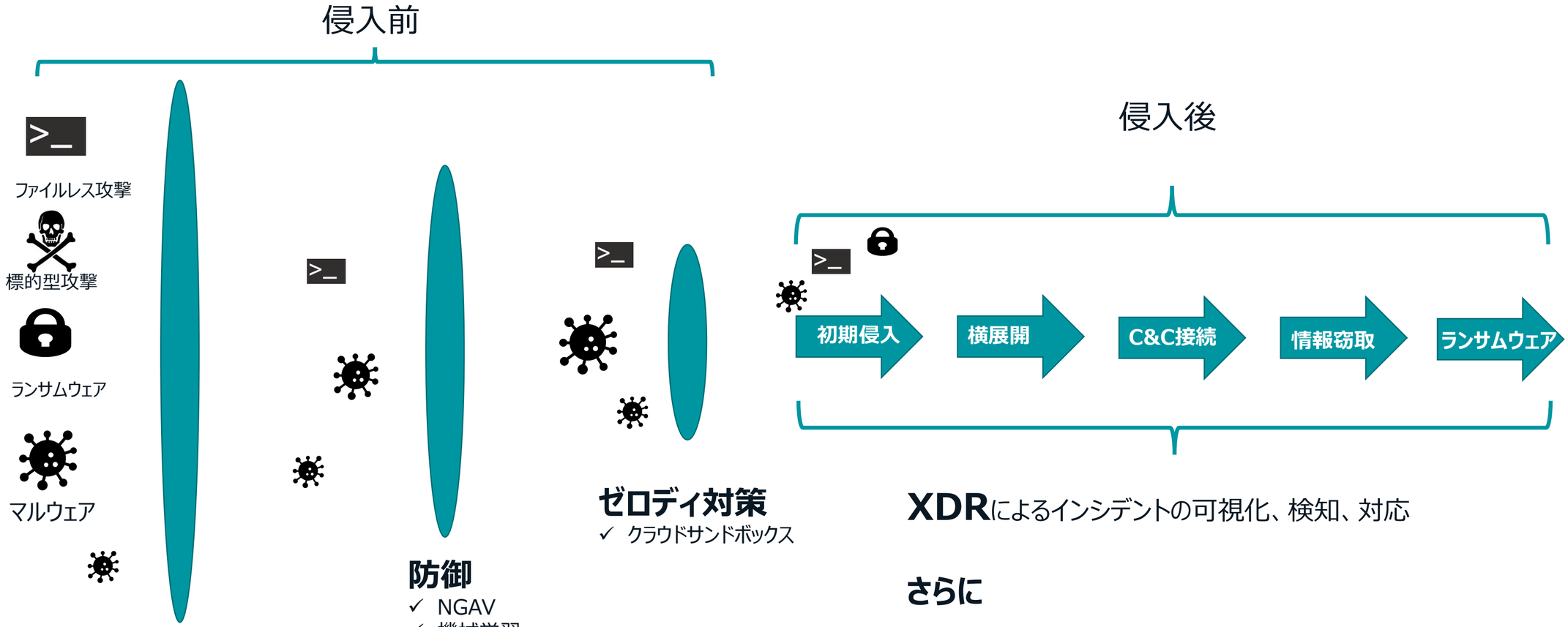


Figure 3: APT Protection Market Quadrant, 2023*

ESETのソリューションはNGAV、パターンマッチングそれぞれの強みを生かしています。EPPの検知内容をXDR相関分析の一部として取り入れて、**高い防御力を維持し、XDRとの相乗効果**を生み出す。

※EPPの定義：NGAV、パターンマッチングの両方を搭載したエンドポイントプロテクションです。

ESETソリューションの優位性



侵入経路対策
- ✓ デバイスコントロール
- ✓ ファイアウォール
- ✓ メールクライアント機能
- ✓ クラウドオフィスセキュリティ
- ✓ 脆弱性管理

防御
- ✓ NGAV
- ✓ 機械学習
- ✓ パターン対応
- ✓ In-product Sandbox

ゼロディ対策
- ✓ クラウドサンドボックス

XDRによるインシデントの可視化、検知、対応

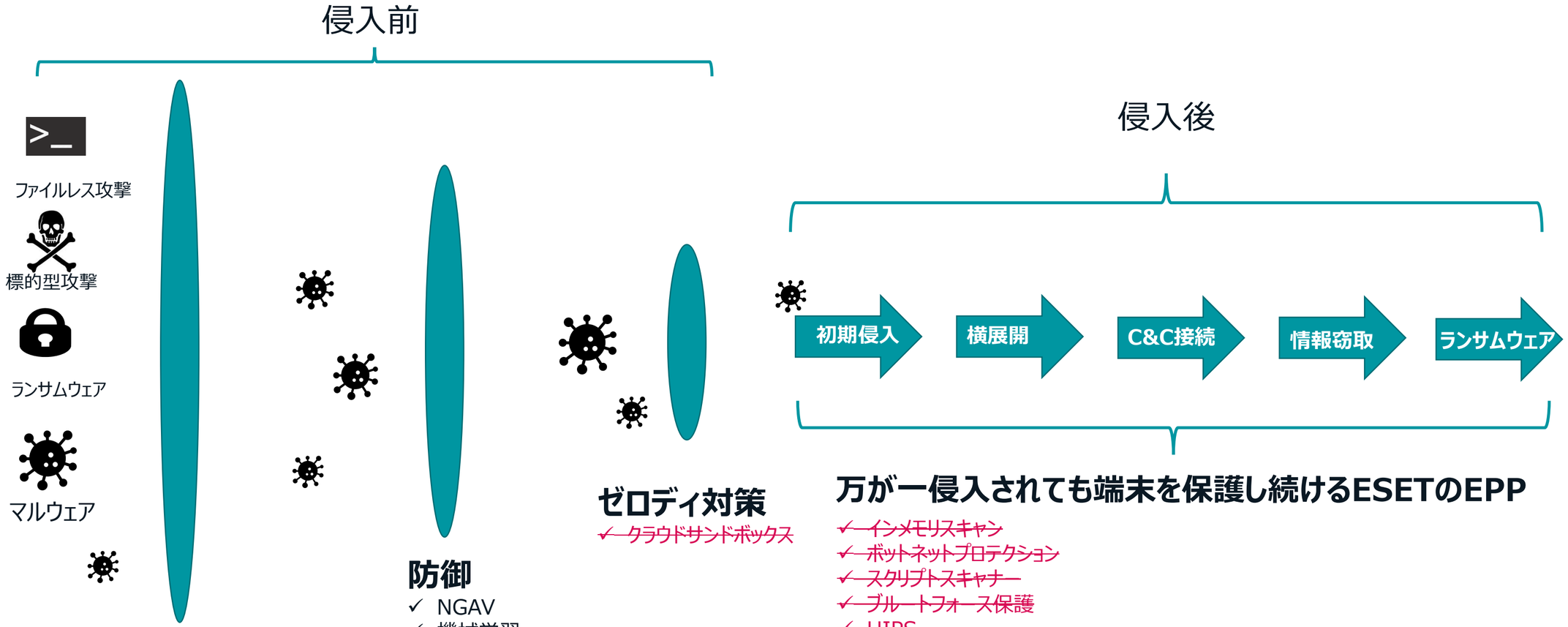
さらに

万が一侵入されても端末を保護し続けるESETのEPP

- ✓ インメモリスキャン
- ✓ ボットネットプロテクション
- ✓ スクリプトスキャナー
- ✓ ブルートフォース保護
- ✓ HIPS
- ✓ ランサムウェアシールド

ESETのシングルプラットフォームでEPP～XDRをすべてカバー可能です

ESETソリューションをXDR/NGAV専業ベンダーに置き換えた場合



侵入経路対策
- ✓ デバイスコントロール
- ✓ ファイアウォール
- ~~✓ メールクライアント機能~~
- ~~✓ クラウドオフィスセキュリティ~~
- ✓ 脆弱性管理

防御
- ✓ NGAV
- ✓ 機械学習
- ~~✓ パターン対応~~
- ~~✓ In-product Sandbox~~

ゼロディ対策
- ~~✓ クラウドサンドボックス~~

万が一侵入されても端末を保護し続けるESETのEPP
- ~~✓ インメモリスキャン~~
- ~~✓ ボットネットプロテクション~~
- ~~✓ スクリプトスキャナー~~
- ~~✓ ブルートフォース保護~~
- ~~✓ HIPS~~
- ~~✓ ランサムウェアシールド~~
- ✓ XDR

侵入前提で設計されていて、**事後対応に特化**するソリューションに置き換えることにより、**多くの防御機能が喪失**します。

よくあるご質問

No	質問	回答
1	ESETはNGAVや機械学習を搭載していますか。	はい、NGAVも機械学習機能を搭載しています。 NGAVや機械学習はヒューリスティック技術を用いており、ESETは20数年以上前から搭載した機能です。
2	XDRのNGAVソリューションはESETのEPPの代替えになりますか。	いいえ、なりません。ESETのEPPはNGAVだけではなく侵入経路を遮断したり、ゼロディ対策機能や多層防御を搭載しており、XDRベンダーに置き換えることにより、防御の部分が大きく弱くなり、セキュリティレベルが低下してしまいます。
	NGAVがあればパターンマッチングは不要でしょうか	いいえ、NGAVとパターンマッチングは向きと不向きがありますので、異なる検出技術でお互いに置き換えられません。弱みの部分、それぞれの技術で補い合えるため、それぞれの強みと弱みを理解し、両方の技術を取りいれることを強く推奨しています。
3	ESETのXDRを使うメリットは？	シングルプラットフォームでEPPもXDRを一元管理できて、防御力を維持しつつ、可視性の向上、検知能力の向上、事後対応のキャパシティが追加されます。管理も単一のプラットフォームでできますので、運用もセキュリティも向上されます
4	導入は簡単でしょうか？	インストーラーを作成し、一回のインストールでEPPもXDRも簡単にインストールされます。 ４か月で数万台導入し、運用開始の実績もあります。
5	パターン更新の負荷は？	タスクを組み、自動的に行われますので、運用負荷はなしです。

Digital Security
Progress. Protected.

イーセットジャパン株式会社
https://www.eset.com/jp/