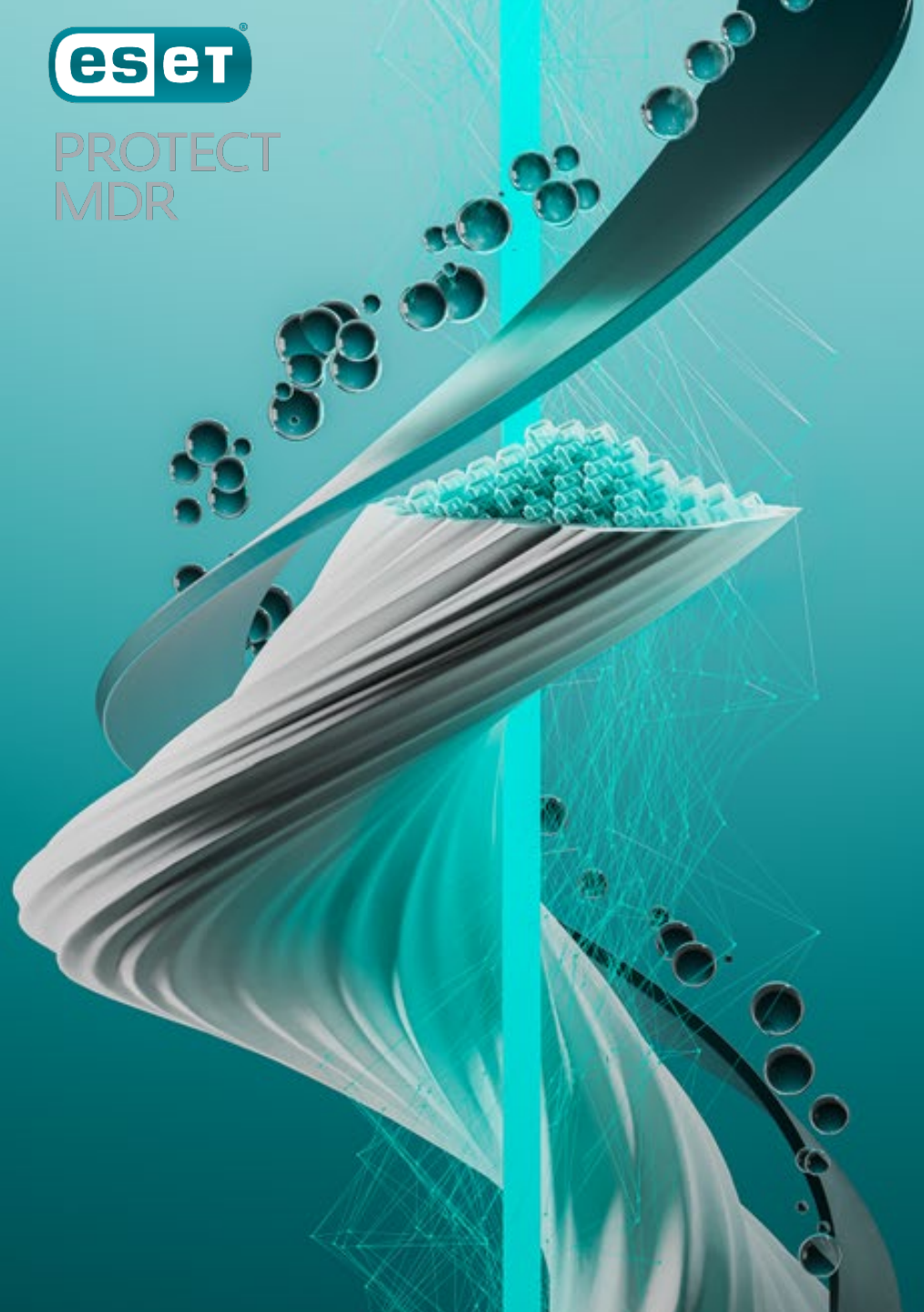


ESETのXDRソリューション「ESET PROTECT MDR」のご紹介

キヤノンマーケティングジャパン株式会社
セキュリティソリューション企画本部

Ver. 1.0

この動画でお伝えしたいこと

- 最近のセキュリティ動向
- 侵入前の「防御」に加え、事後対処を含めた「防衛」の必要性
- ESETのXDRソリューション「ESET PROTECT MDR」

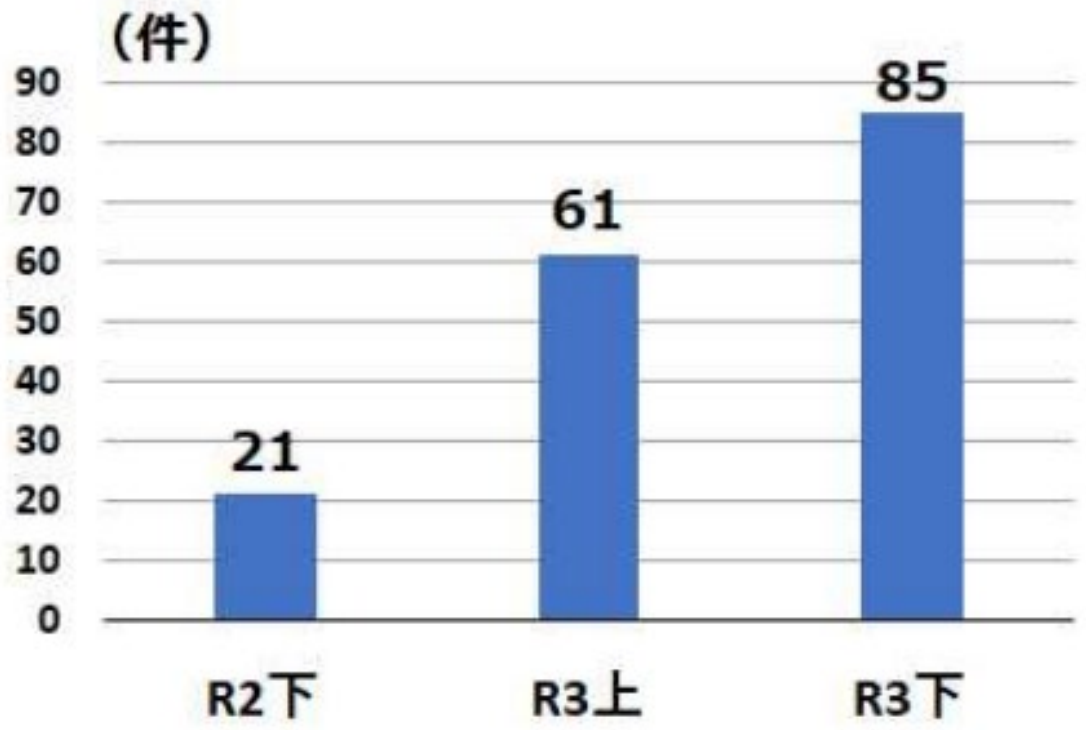
最近のセキュリティ動向

最近のセキュリティ動向について

ランサムウェア被害の報告件数の推移

- 直近一年間で被害は4倍に

【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】



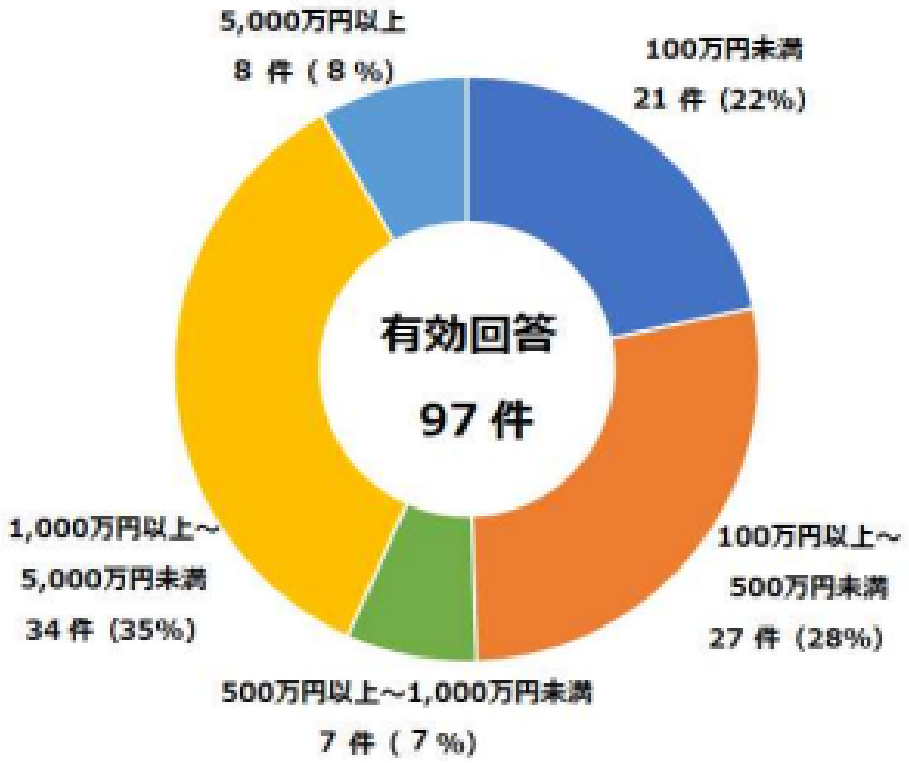
出典：警察庁 令和３年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

最近のセキュリティ動向について

ランサムウェア被害時における、調査・復旧費用の総額

- 1,000万円以上、5,000万円未満が最多

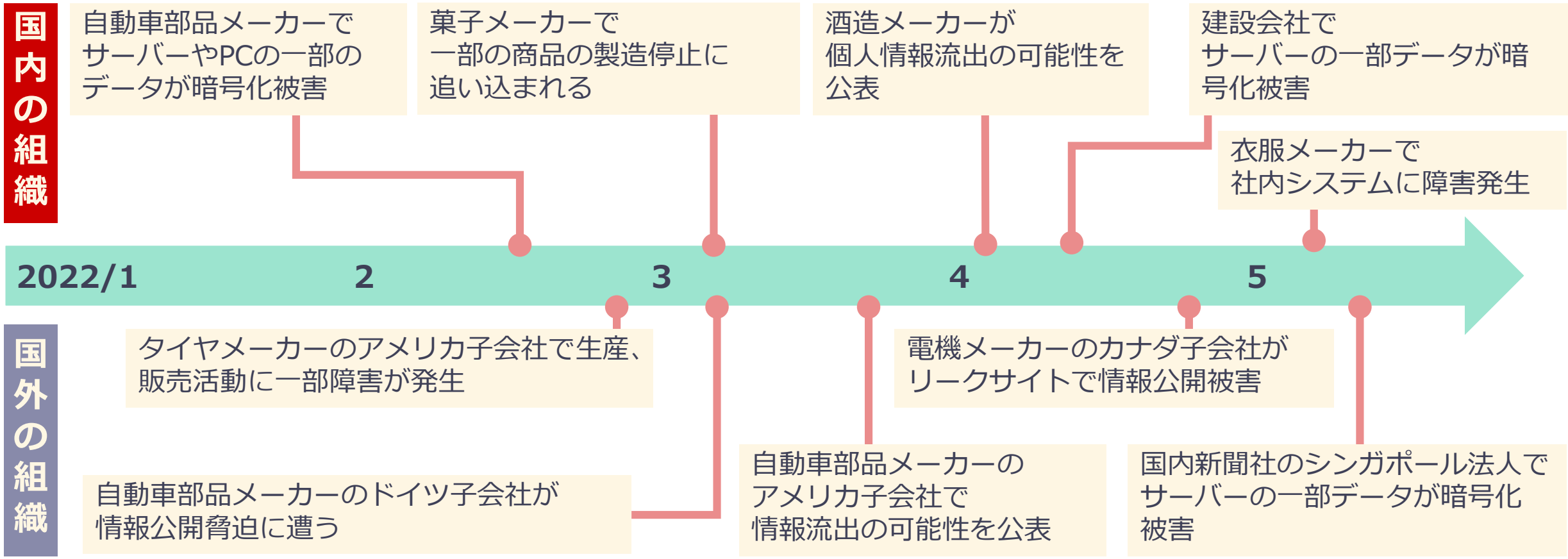
【図表６：調査・復旧費用の総額】



出典：警察庁 令和３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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

最近のセキュリティ動向について

国内外の主なランサムウェア被害事例（2022年1月～5月）



最近のセキュリティ動向について

浮彫りになってきた課題

- 防御に加え、侵入後の対処にも備える必要がでてきた
- 対処するためのツールの検討が必要

侵入後の対処を含めた「防衛」の必要性

侵入後の対処を含めた「防衛」の必要性

防衛とは…

侵入を防ぐ「防御」、ツールでいうとEPP（既にご利用のセキュリティソフトウェア）

＋

侵入後の「対処」、ツールでいうとXDR

ESETのXDRソリューション「ESET PROTECT MDR」について

用語の確認

- EPP とは
- EDRとは
- XDRとは

ESETのXDRソリューション「ESET PROTECT MDR」について

EPP とは

- ウイルス対策ソフトに代表される、ウイルスなどのマルウェアを検出して「侵入を未然に防ぐ」ことを基本思想とする仕組み。

ESETのXDRソリューション「ESET PROTECT MDR」について

EDRとは

- エンドポイントで不審な動きがないかどうか常時監視を行い、ログを取得する仕組み。ログデータはサーバー上に集められ、まとめて分析処理が行われる。ここで疑わしい挙動の痕跡が検出されると、すぐに管理者に通知し、対象物を速やかに隔離などの対応をする。システムに侵入されることを前提に、その後の対応・復旧を中心にサポートすることが特徴。

XDRとは

- EDRのセキュリティレイヤーを増やして、統合して集中管理する機能をもった仕組み。

ESETのXDRソリューション「ESET PROTECT MDR」について

XDRによる防衛のながれ

防御	検知	封じ込め	調査	復旧
パターンマッチング・**機械学習・サンドボックス**なども利用した防御	**マルウェア感染・外部からの不正アクセス**などを検知	攻撃を受けた端末の**隔離**・マルウェア感染拡大の**抑え込み**	サイバー攻撃**内容・被害状況の把握**	感染端末からの**マルウェア除去**
侵入される前提の対策が必要	**早期に攻撃を発見し、被害を抑えられる**	**感染拡大を抑え、業務停止時間を短くできる**	**侵入経路や影響範囲、漏えいした情報の把握が容易になる**	**復旧にかかる時間と手間を抑えられる**

XDRを導入した場合…

侵入後の対処を含めた「防衛」の必要性

XDR導入にむけての課題

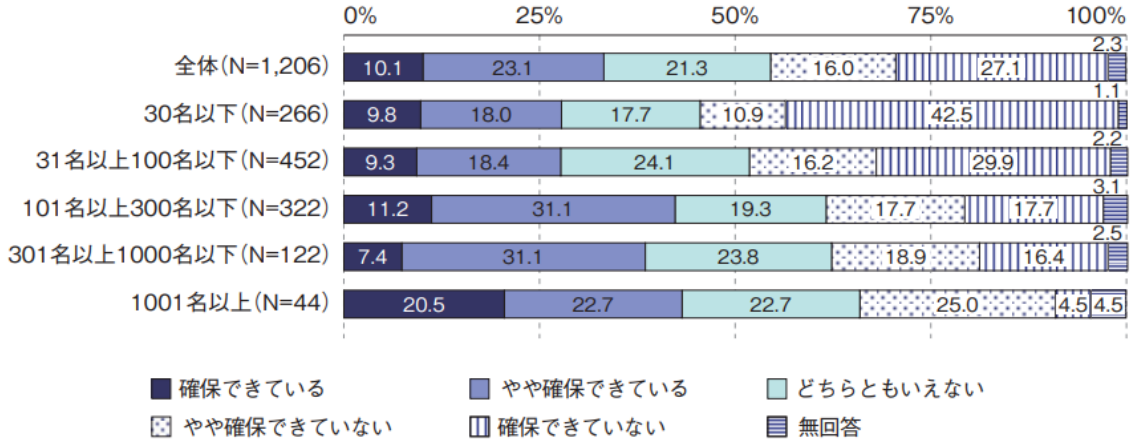
- 常時監視する人的リソースが必要
- 適切に運用するノウハウが必要

侵入後の対処を含めた「防衛」の必要性

セキュリティ人材の不足

- 「確保できていない」IT企業は27.1%
- 約90%の企業で情報セキュリティ専門技術者の不足している

IT企業の情報セキュリティ専門技術者の確保状況【従業員規模別】



出典：IPA IT人材白書
https://www.ipa.go.jp/files/000073566.pdf

侵入後の対処を含めた「防衛」の必要性

そこでもとめられるもの

- XDRの導入に加え、それを外部から常時監視し、ノウハウを提供するセキュリティーサービス

侵入後の対処を含めた「防衛」の必要性

それらすべてを解決するもの

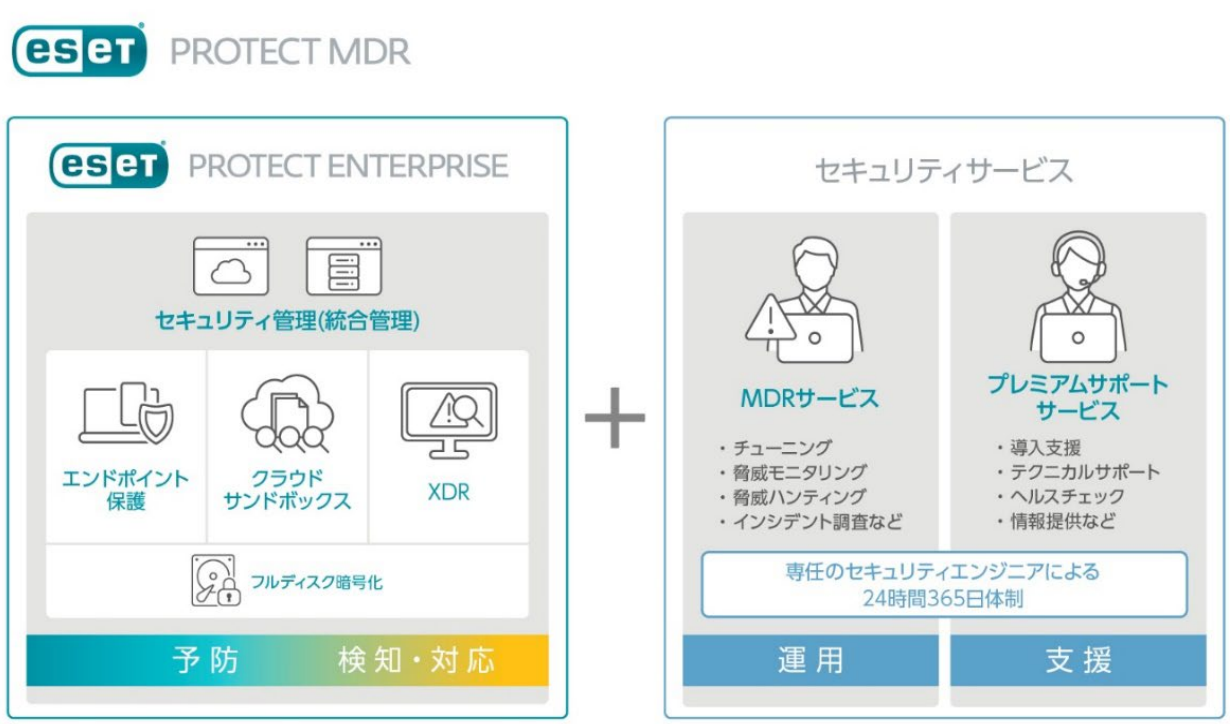
- ESETのXDRソリューション「ESET PROTECT MDR」

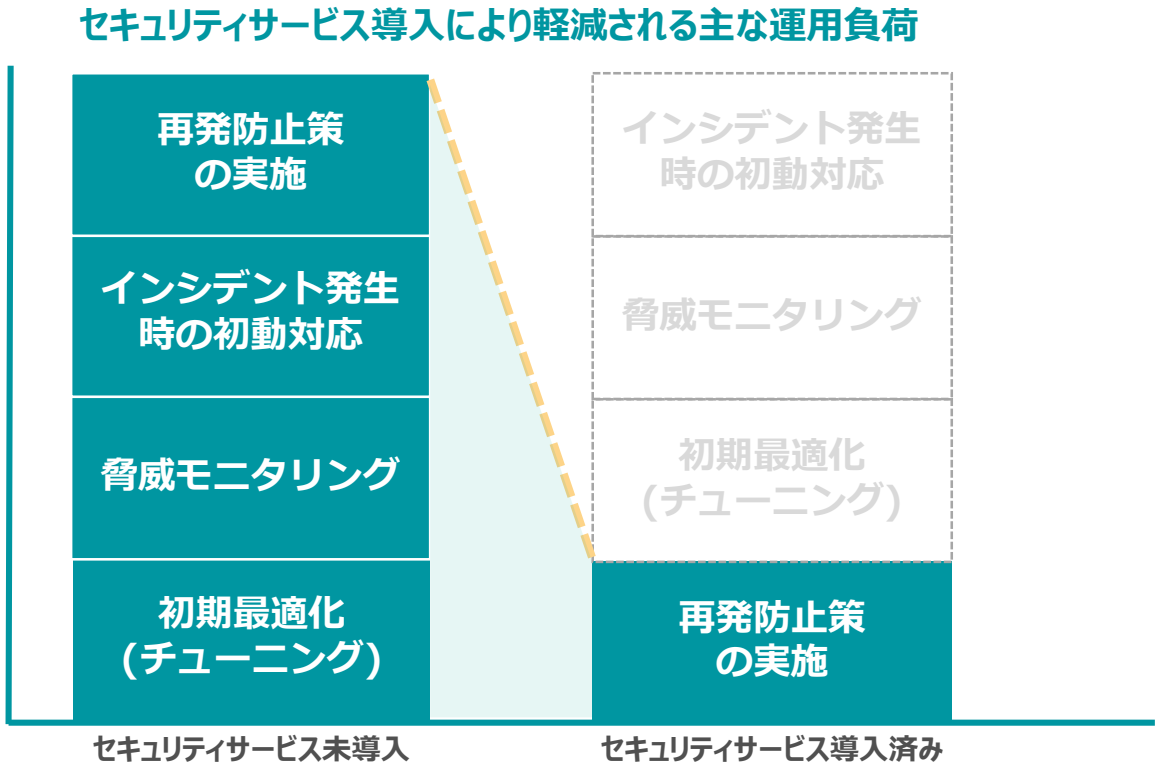
ESETのXDRソリューション「ESET PROTECT MDR」について

ESETのXDRソリューション「ESET PROTECT MDR」について

ESET PROTECT MDRとは

「ESET PROTECT MDR」は、XDRに加え、複雑化するセキュリティ製品の運用を代行する「MDRサービス」と導入支援やテクニカルサポートなどの「プレミアムサポートサービス」を併せた「セキュリティサービス」をご提供します。専任のセキュリティエンジニアによるサポートのもと、脅威モニタリングやインシデント発生時の初動対応などのセキュリティ運用をアウトソーシングすることで、お客様は本来のビジネスに集中することができます。

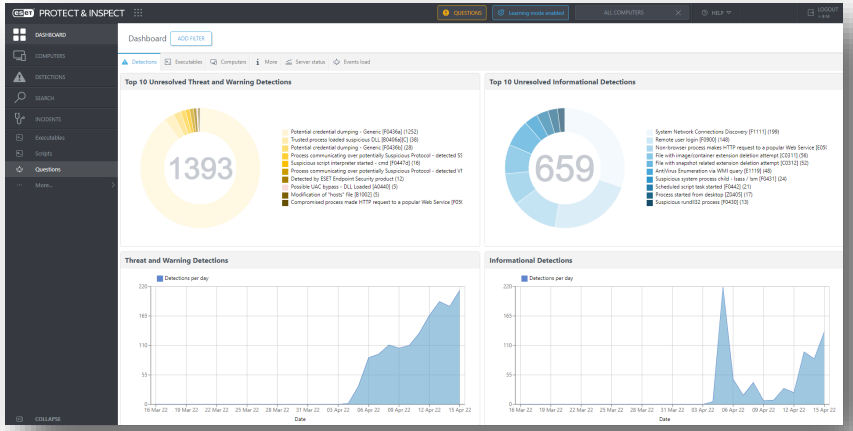




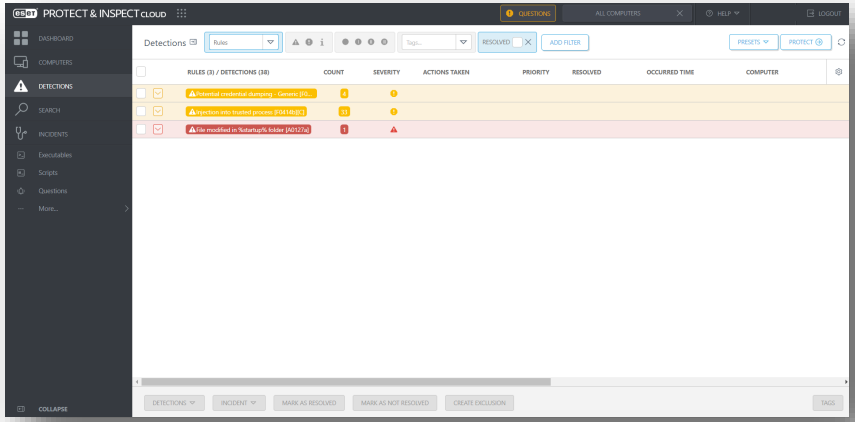
ESETのXDRソリューション「ESET PROTECT MDR」について

Webコンソール

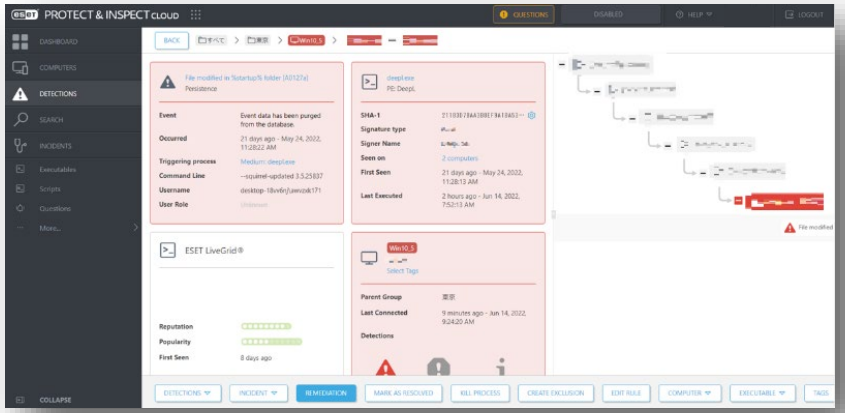
ダッシュボード



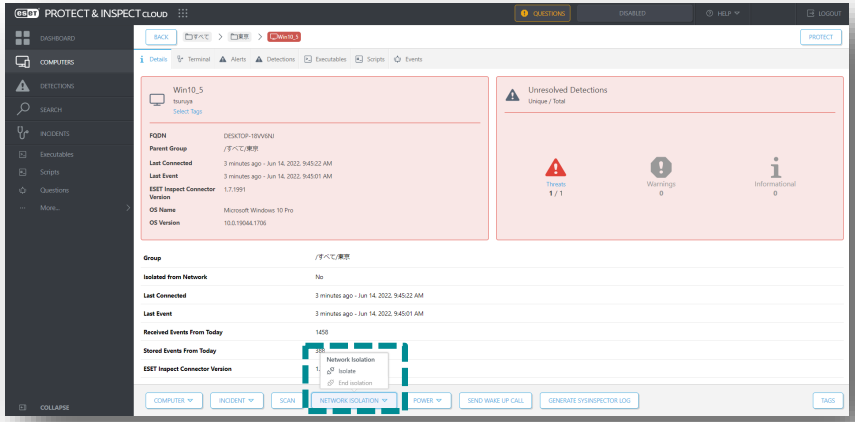
検出アラート一覧



プロセス詳細情報画面



実行ファイル詳細画面



ESETのXDRソリューション「ESET PROTECT MDR」について

予防・検知・対応から運用までワンベンダーで実現する最上位のXDRソリューション

	クラウド型セキュリティ管理ツール	オンプレミス型セキュリティ管理ツール	基本的なエンドポイント保護	総合的なエンドポイント保護	クラウドサンドボックス	フルディスク暗号化	クラウドアプリケーションセキュリティ	XDR	MDRサービス	プレミアムサポートサービス
PROTECT MDR	●*1	（●）*1	●	●	●	●	-	●*1	●	●

- **高度化するサイバー攻撃に一気通貫で対応**
  EPPを中心とした「予防」からXDRによる「検知・対応」まで一気通貫で対応。EDR専業ベンダーでは提供できない、事前・事後両対策を統合したソリューションが簡単で迅速なインシデント対応を実現します。

- **専門スタッフにまるごとお任せ**
  XDRの導入において課題となるチューニングや脅威監視は専門スタッフがお客さまに代わって実施。24/365体制でEPPからXDR領域まで広範囲にサポートするため、お客さまの負荷を軽減できます。

- **早期の環境導入と運用コスト低減を実現**
  セキュリティ管理ツール、XDRともクラウドを選択すれば短時間でセットアップ完了。インフラのメンテナンスが不要なため、管理者は監視や制御に集中できます。クラウド側で随時バージョンアップされるため常に最新の環境を利用できます。

- **実態のない環境依存型攻撃も検知**
  昨今増えているWindowsの標準機能を悪用して攻撃の痕跡を残さない、ファイルレスマルウェアや標的型ランサムウェアなどの環境依存型攻撃も高い精度で検知し削除します。

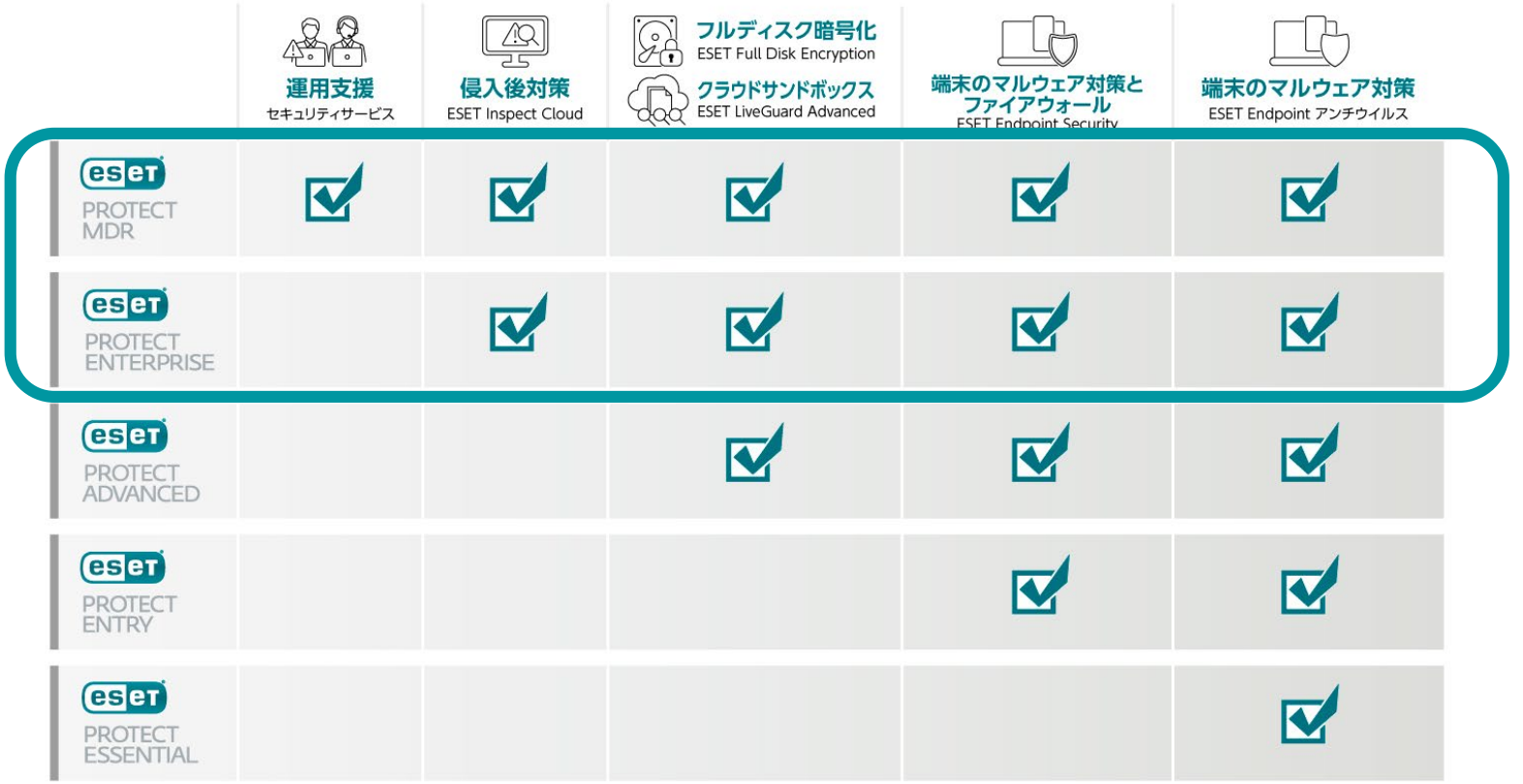
- **ランサムウェアやゼロデイ攻撃からエンドポイントを保護**
  クラウドサンドボックステクノロジーが未知の攻撃であっても自動解析・自動防御。境界型防御が手薄になる社外環境であってもプラスアルファの防御でエンドポイントを守ります。

- **PC紛失盗難時の情報漏洩を防ぐ**
  持ち出しが増える業務端末PCのディスクをまるごと暗号化。インストールや暗号化状態の管理もセキュリティ管理ツールからリモートで一元管理でき、テレワークや在宅勤務中もPC上のデータをしっかりと保護します。

*1　MDRサービスおよびプレミアムサポートサービスを利用される際はセキュリティ管理ツールおよびXDRともクラウド利用が前提となります。

ESETのXDRソリューション「ESET PROTECT MDR」について

ESETプログラムとその機能



※Windows向けプログラム、クラウドソリューションに絞って簡略化して記載しています。

Canon

キヤノンマーケティングジャパングループ