

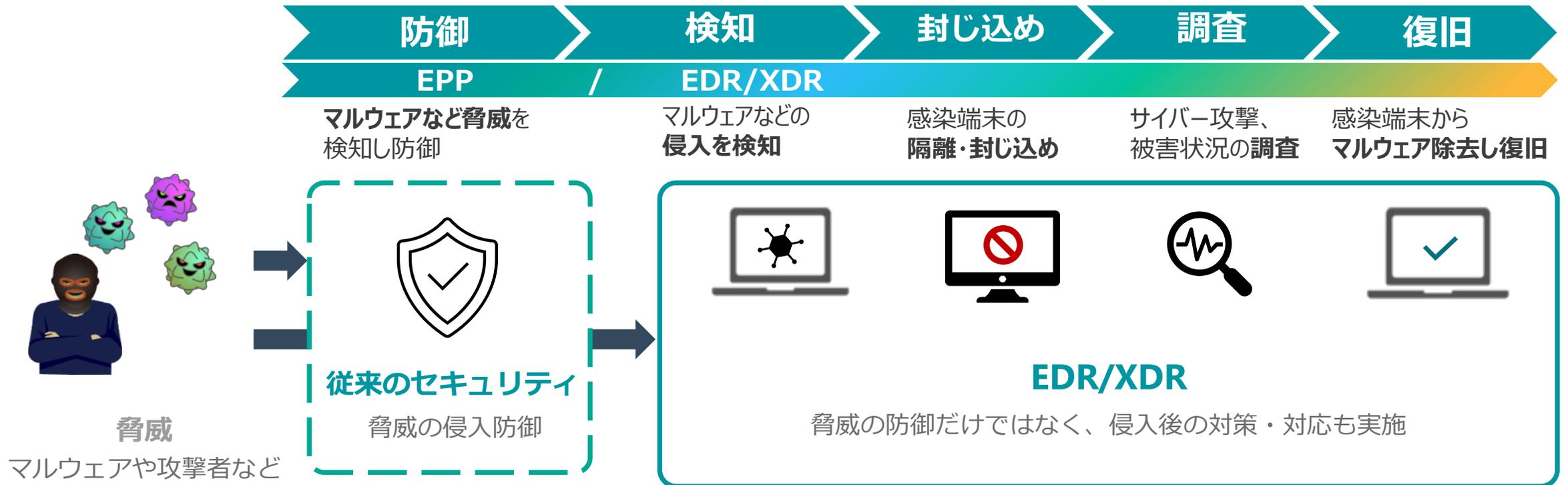
# ESET PROTECT MDR Lite ご紹介資料

# 企業を取り巻くセキュリティ事情



# EDR (Endpoint Detection & Response) /XDR (Extended Detection and Response)とは

EPPの防御をすり抜けた攻撃を検知して封じ込め、調査から復旧までを行うソリューション！  
「侵入を防ぐこと」を目的としたEPPとは異なり、「侵入後の素早い対応を行うこと」を主軸に、  
分析・調査などの事後対策を支援します。



Q.導入するだけでセキュリティは向上する？

A.いいえ、導入するだけでは**向上しません。**

適切な運用を行うことで最大限の効果を発揮します。

Q.従来のEPP製品のように検知からブロック（対処）まで全自動で行われる？

A.いいえ、自動で行われるのは基本的に**検知のみ**です。

最終的な判断は管理者に委ねられます。

EDR / XDRは

恒常的な  
**監視・運用**



セキュリティに対する  
**知識・知見**

を必要とするセキュリティツールです

# より効果的な事後対策を行うには...

## 短期間での運用開始

- 一般的なEDR/XDRは導入後のチューニングを行い、誤検知を減らすため運用開始まで時間がかかります。チューニング期間を**短期間で効果的に行う**ことで、契約開始からEDR/XDRを最大限にご活用いただけます。

## 24時間365日の監視体制

- サイバー攻撃はいつ発生するか分かりません。セキュリティ専任組織（SOCやCSIRT）などの**24時間365日継続監視ができる体制**を整えておくことで、突然発生した脅威にも備えることができます。

## 迅速かつ適切な初動対応

- 万が一、検知アラートが脅威によるものだった場合、対象端末のネットワーク隔離などの**初動対応を迅速かつ適切に行う**ことで、被害を最小限に食い止めることができます。

事後対策は事前防御とは大きく異なり  
**継続した運用体制で効果を発揮します！**



安い



早い



安心

低コストですぐに運用を開始でき、ESET社による運用と  
キヤノンマーケティングジャパングループによる国内サポートで  
**万が一の時は初動対応もおこなう  
安心なサービスです！**

# ESET PROTECT MDR Liteの特長

即時  
運用開始

ESET社による  
24時間365日  
体制の脅威監視

万が一の時には  
最短20分での  
初動対応

週次/月次での  
レポート提供

キヤノンによる  
日本語での  
サポート

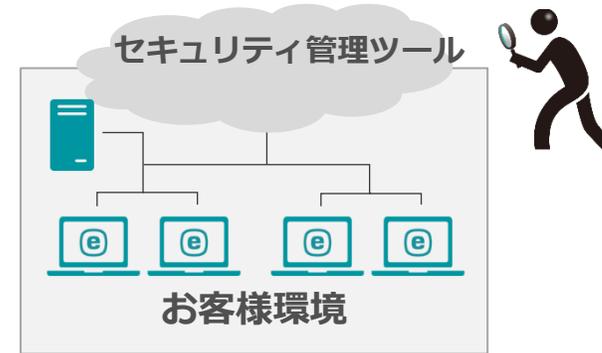
# サービスイメージ

## 最短20分での脅威への対応



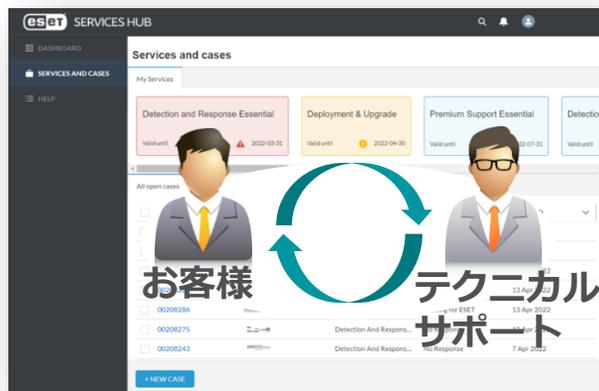
- 脅威が発生した場合、最短20分で初動対応  
例) NW隔離  
→クライアント上でアラートが表示されます
- 脅威の詳細(英語)の確認が可能

## 24時間365日体制の脅威監視



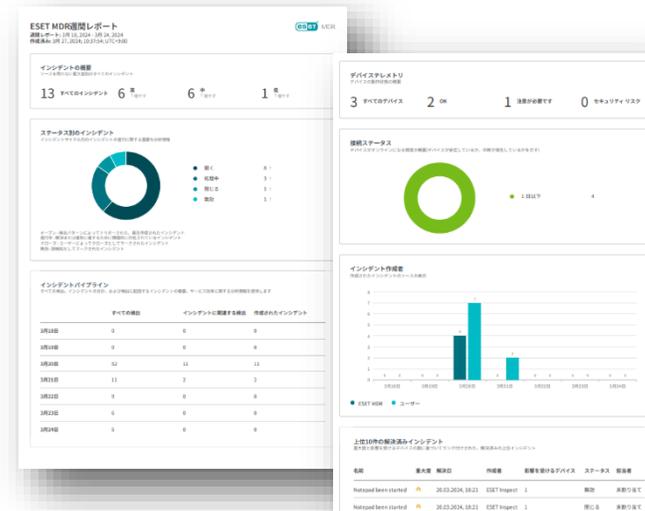
- 24時間365日お客様環境を監視、分析

## 日本語でのサポート



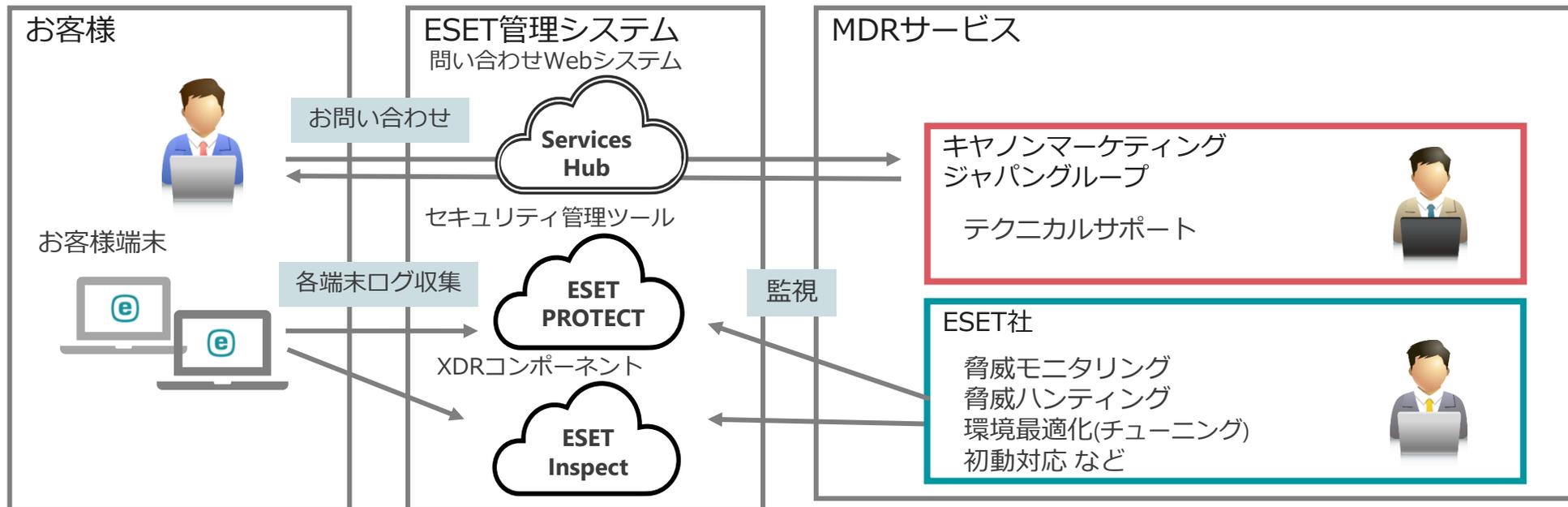
- Webシステムより24時間365日お問い合わせ可能

## 週次/月次でのレポート提供



- 環境内で発生したインシデントの状況やEPPの状態が把握可能
- セキュリティ管理ツールよりレポートダウンロード可能

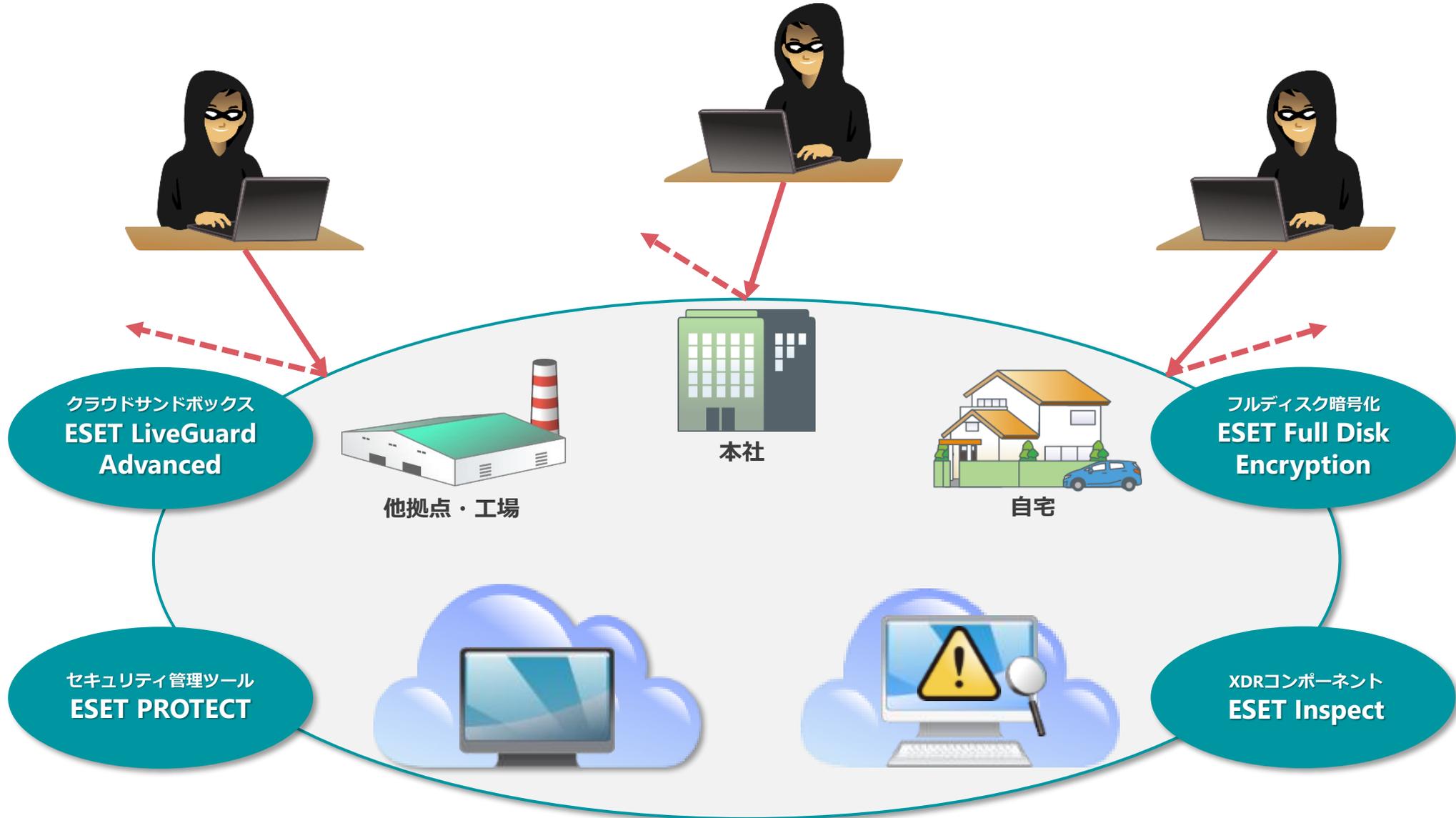
# ESET PROTECT MDR Lite提供サービス体制と一覽



サービス	サービス内容
脅威モニタリング	AIやIoC※に加え、高度な監視および検出技術を活用して、ESET社がお客様の環境を保護する24時間365日の継続的なサービスです。また、週次/月次のレポートにより、お客様にモニタリング情報を提供します。 ※IoC(Indicator of Compromise)：サイバー攻撃の痕跡を表す情報。 <a href="https://eset-info.canon-its.jp/malware_info/term/detail/00137.html">https://eset-info.canon-its.jp/malware_info/term/detail/00137.html</a>
脅威ハンティング	ESET社のセキュリティエンジニアが継続的に検出を確認・評価し、脅威が確認された場合はお客様のESET Inspectにインシデントを作成します。
初動対応	脅威モニタリングや脅威ハンティングで脅威が検出された場合、ESET Inspectを利用してネットワーク隔離やプロセス停止などの対応を行います。ESET Inspect上で詳細が確認できます。 XDRによって、インシデントの影響が広範囲におよぶと判断された場合には、被害拡大を未然に防ぐために、XDRの自動アクション機能で端末全体に対して初動対応(プロセスの停止やDLLの実行ブロック)が行われることがあります。
テクニカルサポート	24時間365日、本サービスやESETプログラムについてのお問い合わせに対応します。

# ESET PROTECT MDRに含まれる 防御機能のご紹介

# ESET PROTECT MDRなら事前防御・事後対策をまるごと強化！





防御

検知

封じ込め

調査

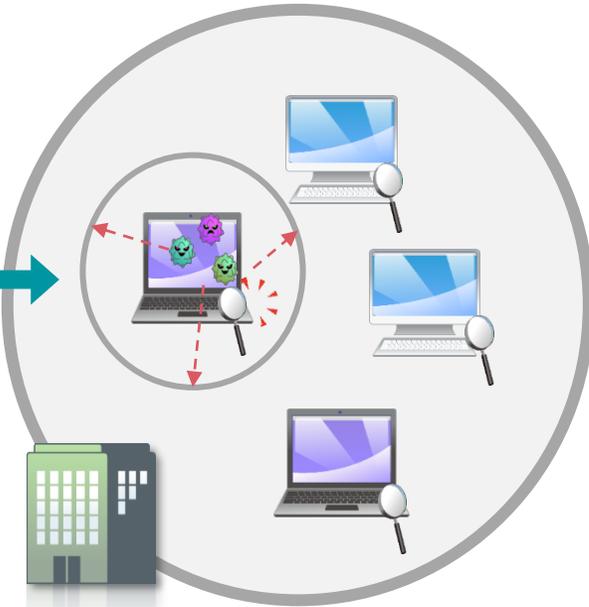
復旧

EPP

EDR/XDR



感染端末の  
ネットワーク隔離など



## 的確な状況把握

侵入経路や影響範囲、漏洩した情報など、被害状況の把握が容易。



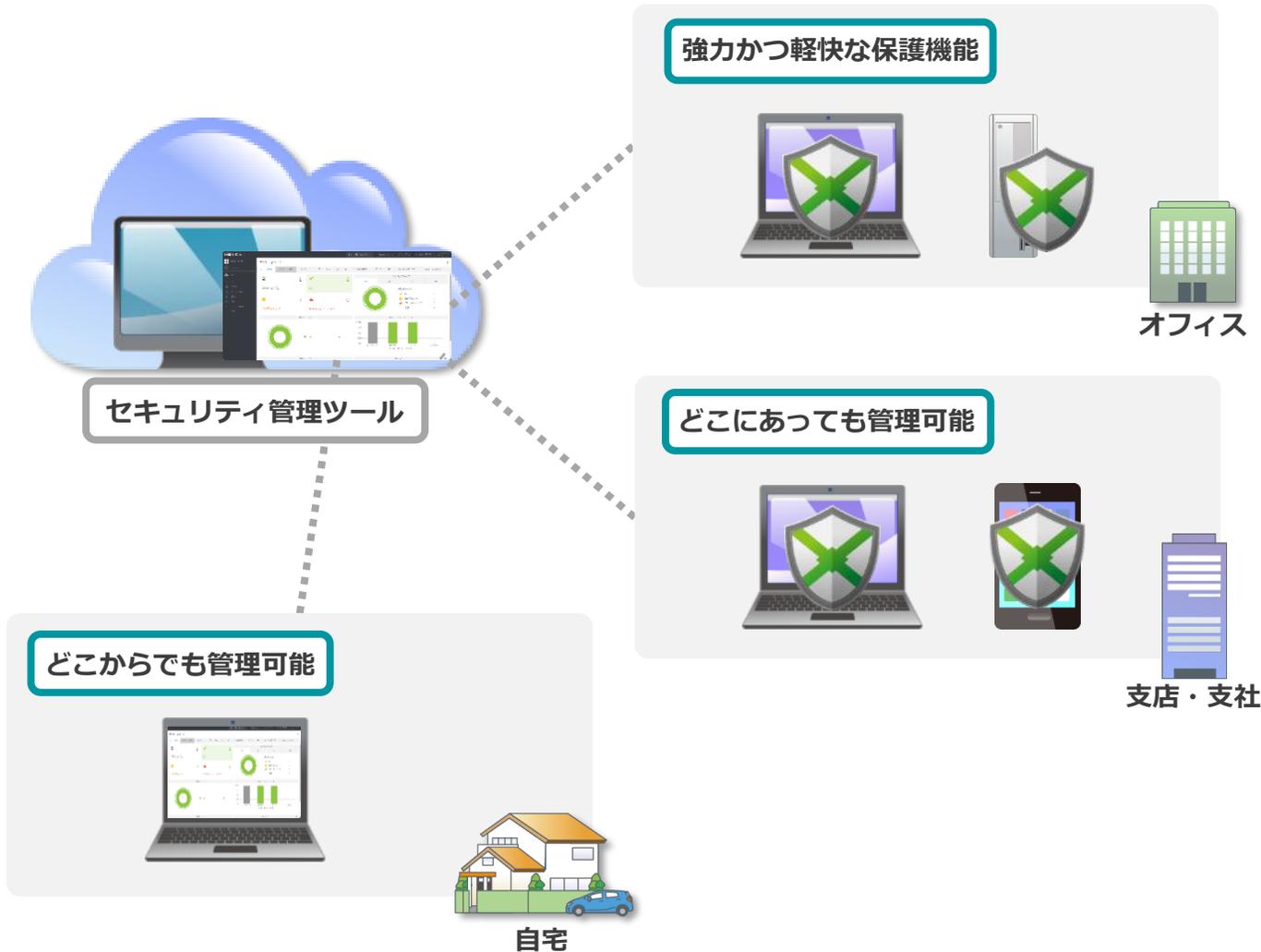
## スピーディーな対処

資産への脅威の侵害が深くなる前に対処を施すことが可能なため、感染拡大を抑え、業務停止時間を短くできる。



## 遠隔隔離・調査

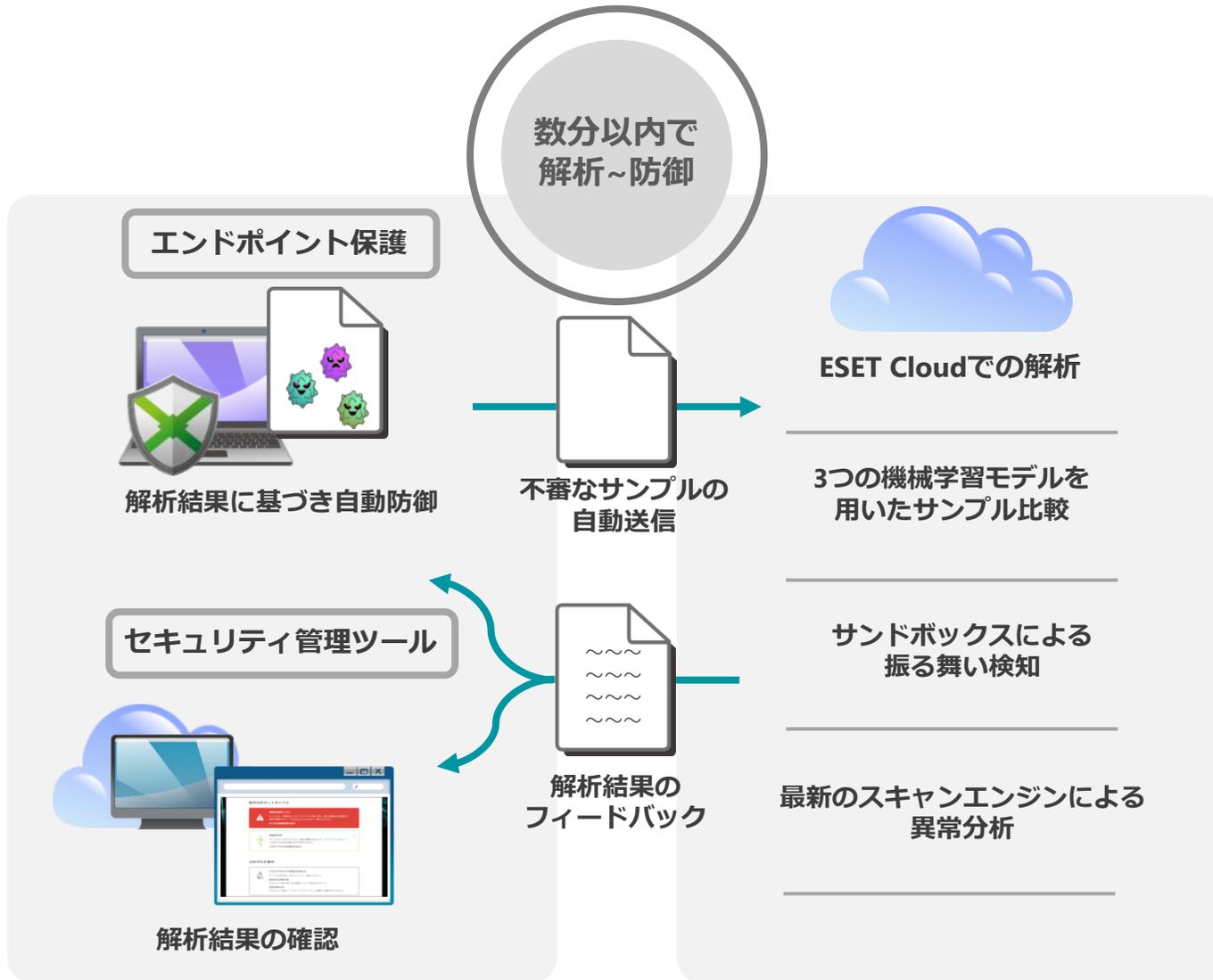
管理者が現地へ赴くことなく、侵害端末の隔離・調査を行うことが可能。



 **状況把握のしやすさ**  
クラウド上に管理ツールがあるため、社内外問わず端末がどこにあっても状況が把握可能。

 **サクサク軽快な動作**  
サイズの小さい検出エンジンと軽快な動作のエージェントにより、負荷を最小限におさえた、業務に影響を与えないウイルス対策が可能。

 **未知の脅威もおまかせ**  
20年以上実績のあるESET独自の検出技術を用いて、未知の脅威への防御も可能。



## 💡 カンタン導入

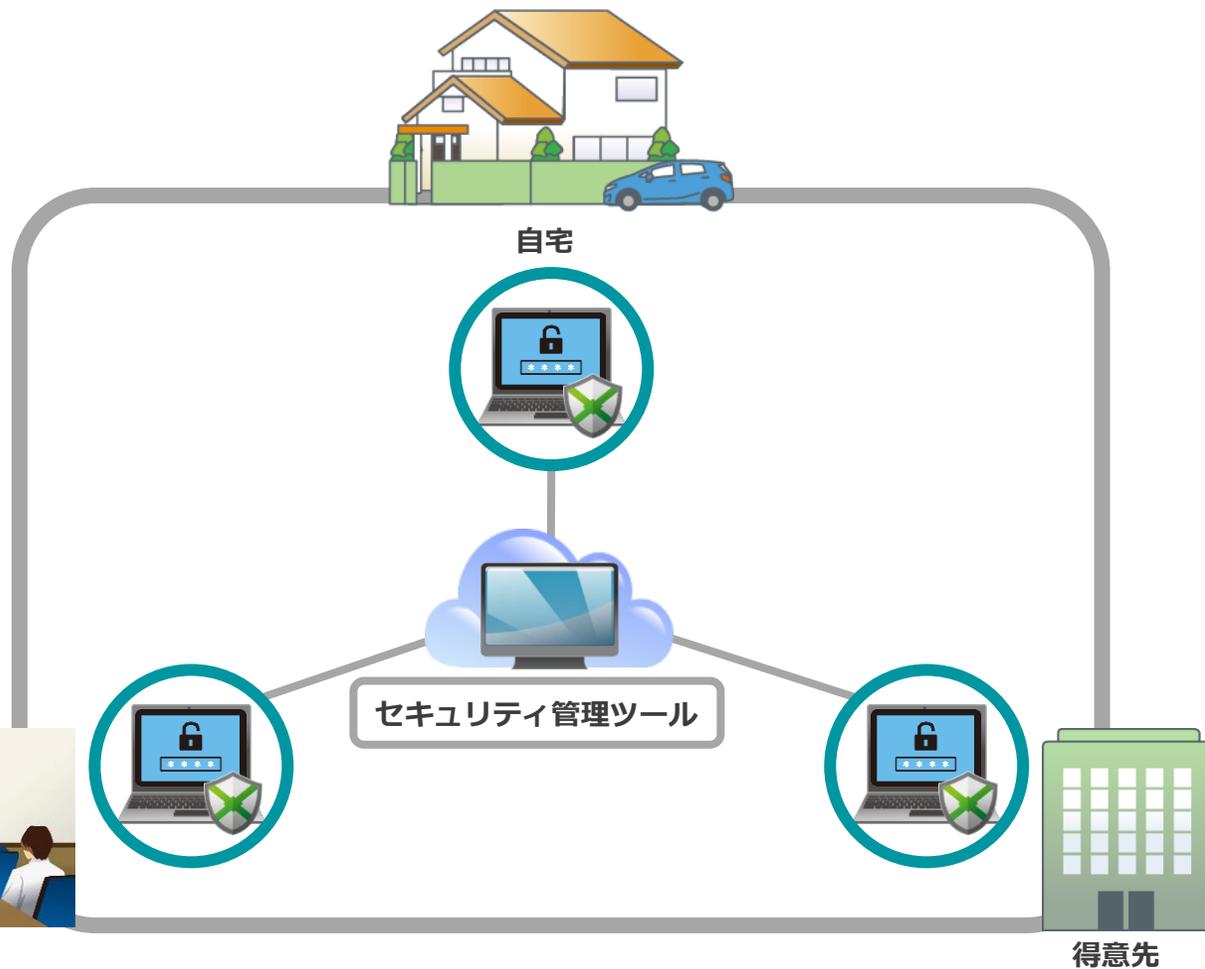
ライセンスを追加するだけで利用開始。  
少ない工数でセキュリティ対策を強化。

## 💡 解析結果レポート

管理ツールより確認可能。挙動はもちろん、  
攻撃手法や経路を確認できるので、  
セキュリティ対策の見直しに役立つ。

## 💡 自動解析/自動防御

未知の脅威を自動解析、結果に応じて即防御。  
導入後も運用負荷をかけずに利用可能。



## 💡 情報漏洩リスク減

PC紛失時に第三者がPCの中身を除くことができないため、リモートワークや外出でPCを持ち出しても安心。

## 💡 運用負荷の低減

エンドポイント保護とフルディスク暗号化を一元管理できるため、管理の手間が省ける。管理画面もエンドポイント保護と同じため迷うことなく使用可能。

**Canon**

キヤノンマーケティングジャパングループ