2025年5月26日

三重県自治体情報セキュリティクラウド接続団体様

追加セキュリティ対策（EDR）概要

アジェンダ

1. 追加セキュリティ対策（EDR）とは
2. 提案概要
3. SOC運用

1. 追加セキュリティ対策（EDR）とは

EDRとは、エンドポイント（PCなどの端末）を監視し、不審な振る舞いを検知して対処するためのツール・サービスです。

ネットワーク上のエンドポイント端末からログデータを収集し、不審な挙動やサイバー攻撃を検知してセキュリティ管理者に通知します。通知を受けたセキュリティ管理者は、EDR管理画面でリモートからエンドポイント端末の復旧対応が可能です。

EPP（Endpoint Protection Platform）

目的：マルウェア感染の防止

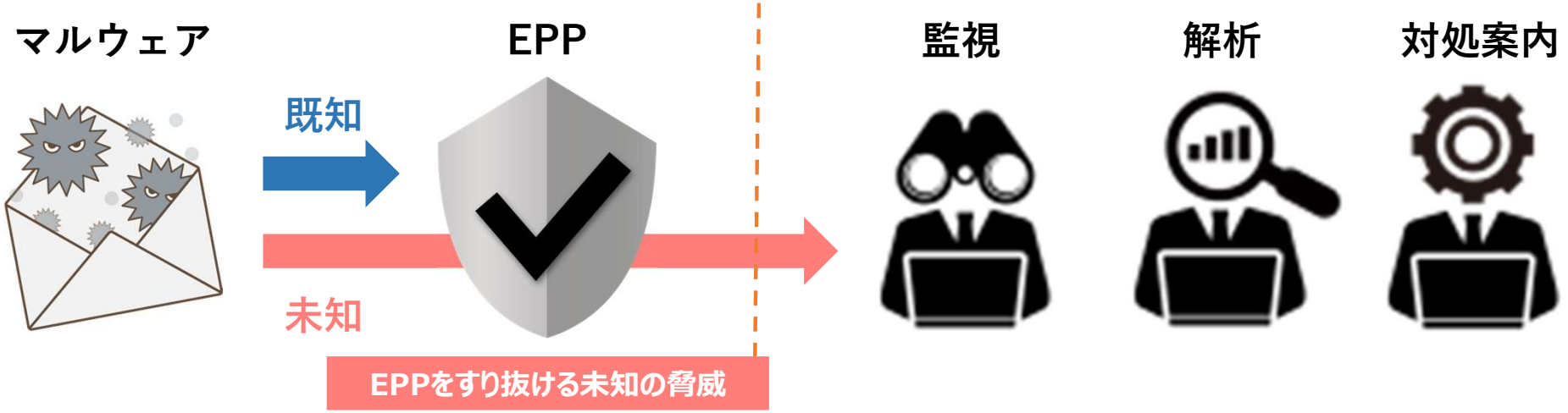
役割：**既知のマルウェア**を自動検知・ブロックする

（パターンマッチングによる検出）

EDR（Endpoint Detection and Response）

目的：**未知の脅威**の迅速な検知や対処

役割：エンドポイントのアクティビティを記録し続け、侵害後の調査や対処を可能にする



EPP・EDR を併用して、既知および未知の侵害に備える

政府動向

地方公共団体における 情報セキュリティポリシーに関する ガイドライン（令和 5 年 3 月版）**より抜粋。**

βモデル、β‘モデルにおいて、「未知の不正プログラム対策（エンドポイント対策）」が必須

項目		No.	必須	監査項目
3.情報システム全体の強靭性の向上	技術的対策	3	○	iii）未知の不正プログラム対策（エンドポイント対策）統括情報セキュリティ責任者及び情報システム管理者により、**パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。** ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。

β モデル、 β‘モデルにおける**必須の**セキュリティ対策について （技術的対策部分のみ抜粋）

2．提案概要

追加セキュリティ対策（EDR）として、以下をご提供いたします。

・ソフトウェア「製品名のため非公開」によるエンドポイント端末のログ収集
・専門家によるマネージドサービス「SOC」

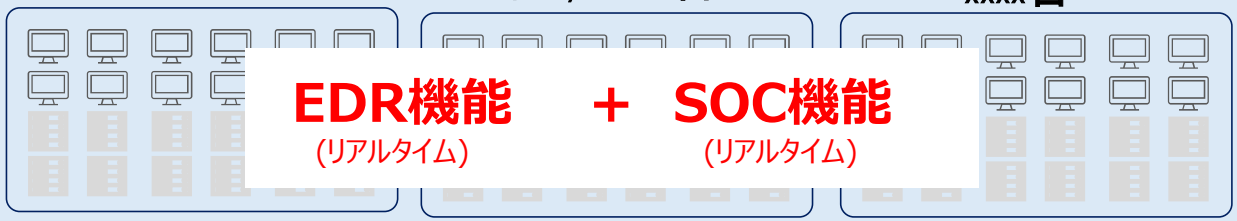
三重県自治体情報セキュリティクラウド　プラットフォーム

IT資産から情報取得、調査をご提供

約9,000台

約3,000台（※）

xxxx台



EDR機能（リアルタイム）　＋　**SOC機能**（リアルタイム）

- 24時間365日対応
- 国内最高峰のSOC事業サービス
- 全自治体の窓口対応

- 公開脆弱性の排除
- 他団体事案リスク報告
- 数分-数十分での調査
- ガイドライン改定に対応

- IT資産の可視化
- ポリシー違反の可視化
- 脆弱な資産の可視化

※ 2022年1月時点での想定台数。

追加セキュリティ対策

「製品名のため非公開」＋「SOC」＝「ガイドライン準拠のサービス提供」

3. SOC運用

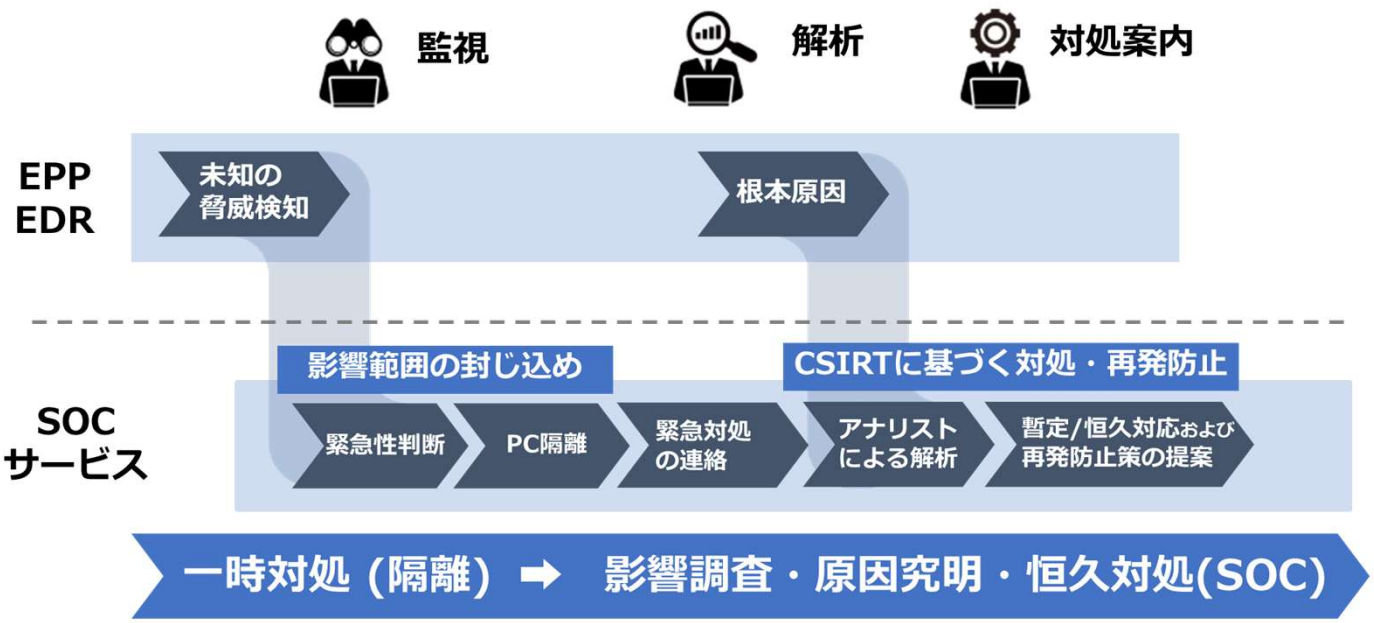
CEC SOCサービス ３つのポイント

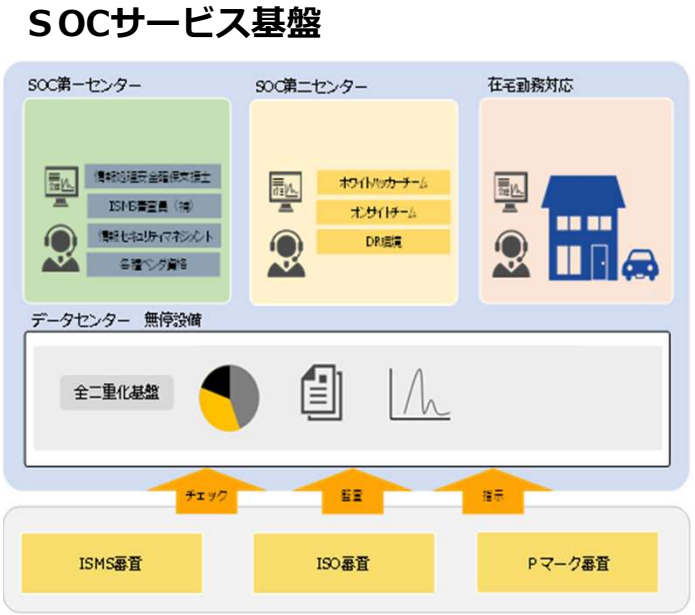
SOCサービス提供における基本方針

Point1: 影響範囲を最小限に留めること　インシデント発生時にお客様がなにをすべきか　迅速・的確な一次通報（目標30分以内）

Point2: 同一インシデント発生を防ぐこと　周辺ログの解析まで含めた、二度と感染しないための「恒久対処」と月次報告

Point3: 高品質なサービスの継続的に提供できること　ISMSなど各種認証取得に裏打ちされたサービスの継続性





SOCポータルによる接続団体様との情報連携

ポータル構成は下記になります。