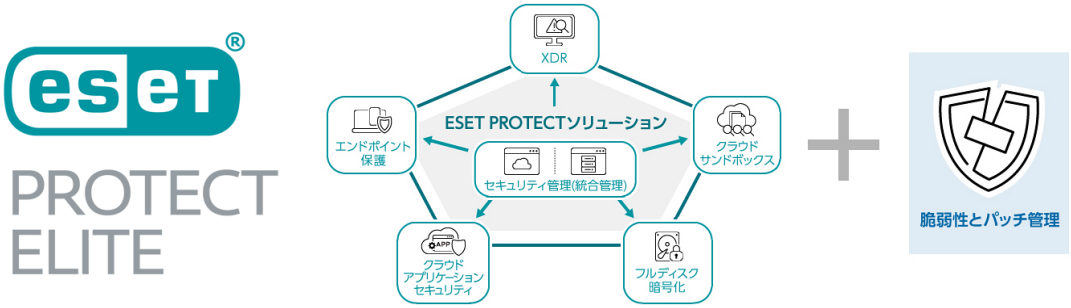
2023 年 8 月 28 日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

脆弱性の診断と自動的な修正対応を可能にした XDRソリューション“ESET PROTECT Elite”の販売を開始

キヤノンマーケティングジャパン株式会社（代表取締役社長：足立正親、以下キヤノンMJ）は、サイバー攻撃に対する防御・検知・対応に加え、予防対策として脆弱性診断と自動的な修正対応を実施するXDRソリューション“ESET PROTECT Elite”を2023年9月20日より販売を開始します。常に最新の修正プログラムが適用されたソフトウェアの状態を保つことで、昨今増加する脆弱性をついたサイバー攻撃によるリスク低減を実現します。



サイバーセキュリティ上の脆弱性は、悪意のある第三者によって不正アクセスやウイルス感染などの攻撃を受けることで、情報漏えいや改ざん、システム停止などの被害を引き起こす可能性があります。昨今では、大手製造業が脆弱性を悪用したサプライチェーン（供給網）攻撃を受け一時生産停止となったり、医療機関において外部委託事業者の脆弱性から基幹システムがランサムウェアに感染することで、一部の診療が制限されたりする被害が報告されています。
こうした報道により、脆弱性のリスクに対する認識が高まっている一方で、予防対策として日々発見されるOS（オペレーティングシステム）やソフトウェアの脆弱性情報を人の手により確認し、企業や組織が使用しているすべてのシステムにセキュリティパッチ※1を適用することは大きな負荷となっています。

キヤノンMJはこのたび、OSやソフトウェアの脆弱性の診断と自動的な修正対応を実現する新機能※2「ESET Vulnerability and Patch Management」※3を搭載したXDR※4ソリューション“ESET PROTECT Elite（イーセット プロテクト エリート）”の販売を開始します。“ESET PROTECT Elite”はサイバー攻撃への予防、防御並びに、万が一企業のシステム内に侵入を許した際、脅威の検知と封じ込めなどの事後対応まで幅広く対応するESETの最上位ソリューションです。

1. 脆弱性評価と自動パッチ対応する「ESET Vulnerability and Patch Management」※3

OSやソフトウェアを定期的に自動スキャンすることにより、脆弱性を即座に可視化することが可能な機能をESET PROTECTソリューションシリーズで初めて※2搭載しました。深刻度に合わせ優先順位付けする脆弱性評価や、セキュリティポリシーに合わせて自動または手動でのセキュリティパッチ適応設定が可能で、脆弱性を悪用した攻撃を未然に防ぎます。

2. 脅威に対する防御から、万が一の侵入に対する検知・対応を行う包括的なXDRソリューション

脅威の侵入に対し、クラウドサンドボックスやエンドポイント保護など、ESETの多層防御機構を用いてマルウェアなどの脅威から迅速かつ精度高く端末を守ります。また万が一侵入を許した際の事後対応として、XDRを用いて組織内のログデータを収集し、脅威の検知・可視化をすることで、セキュリティ管理者が状況を確認し、速やかに対処できるよう支援します。

3. 多重化した対策を1つのコンソールで統合管理。

巧妙化・多様化したサイバー攻撃に対し、“ESET PROTECT Elite”は予防、防御、検知、対応までの対策を1コンソールで集中管理することで、より高度な脅威検知や迅速な対応を実現します。また運用管理の効率化によるコストの削減や、セキュリティ対策効果の最大化などを実現します。

製品名	提供開始日	ライセンス数	希望小売価格（税別） ※1ライセンス当たり
ESET PROTECT Elite	2023年9月20日（水） 予定	100 ～ 249	9,720円
		250 ～ 499	8,940円
		500 ～ 999	8,190円
		1,000 ～ 1,999	7,410円
		2,000 ～ 4,999	6,720円
		5,000 ～ 9,999	5,970円

※1. OSやソフトウェアに存在する脆弱性やバグを修正するプログラム
※2. 2023年8月28日時点。
※3. 提供開始日時点での対応OSはWindowsのみ。Windows Sever OSやmacOSは2024年に順次対応予定。
※4. XDR（Extended Detection and Response）異なるセキュリティ製品・セキュリティ階層で収集した、異なる種類のイベントデータを統合して、エンドポイントでの調査、対応を適切に行うソリューション。

＊ ESETは、ESET, spol. s r.o.の登録商標です。

●報道関係者のお問い合わせ先　：キヤノンマーケティングジャパン株式会社　広報部　03-6719-9093（直通）
●セキュリティソリューションホームページ：https://cweb.canon.jp/it-sec/
●ニュースリリースホームページ　：canon.jp/newsrelease

＜“ESET PROTECT Elite”の主な特長＞

サイバー攻撃による脅威の侵入防御から、万が一組織内に脅威が侵入した場合の事後対応として脅威検知と対処およびその運用までを支援します。

予防対策として、新たに※搭載した脆弱性とパッチ管理により脆弱性を悪用した攻撃を未然に防ぎ、クラウドサンドボックスやエンドポイント保護などESETの多層防御機構を用いてマルウェアなどから迅速かつ精度高く端末を守ります。事後対応として、XDRを用いて組織内のログデータを収集し、脅威の検知・可視化をすることで、セキュリティ管理者が状況を確認し、速やかに対処できるよう支援します。

※2023年8月28日時点。

＜“ESET PROTECT Elite”の主な機能概要＞

1.脆弱性とパッチ管理（ESET Vulnerability & Patch Management）

クライアント端末のOS及び、アプリケーションを自動スキャンし、セキュリティパッチを適用することで脆弱性のタイムリーな検出と修復が可能です。セキュリティパッチはユーザーの設定するポリシーに基づき自動または手動で適用できます。
脆弱性とセキュリティパッチ管理の状態確認は、ESET PROTECT Eliteで利用できるESET PROTECT Cloudのコンソールから、エンドポイントの状態と共に一元管理が可能で、社内外どこにいても状態を確認できます。また、スケジュール設定による自動スキャン、脆弱性の重大度ベースの優先順位付け、影響を受けるデバイスの一覧と脆弱性データベース、特定の脆弱性の例外を作成する機能、カスタマイズ可能なセキュリティパッチ適用ポリシーなどの機能により、ユーザーの環境やニーズに合わせた設定が可能です。

＊ 提供開始日時点での対応OSはWindowsのみ。Windows Sever OSやmacOSは2024年に順次対応予定。

2.XDR（ESET Inspect / ESET Inspect Cloud）

組織内の端末のログ情報を記録し、端末上の疑わしい動きを検出します。検出結果を分析、調査することで、組織内に潜む脅威をいち早く割り出し、封じ込めることが可能となります。悪質なファイルや不審なプロセスを発見した場合、管理者はプロセス終了や端末のシャットダウン、ネットワーク隔離などの処置を速やかに実施できます。クラウド型／オンプレミス型、どちらも選択可能です。

3.セキュリティ管理ツール

端末の検出エンジンのアップデートやウイルス検査の実施、端末ログやレポート情報の取得、ユーザー管理、設定変更や、各種セキュリティ対策の運用管理などを一元的に行い、個々の端末を適正な状態に保つことができます。

4.エンドポイント保護

ウイルス・スパイウェアなどのマルウェア対策、フィッシング対策やネットワーク保護、迷惑メール対策などによりエンドポイントを保護します。

5.クラウドサンドボックス（ESET LiveGuard Advanced）

ランサムウェアやゼロデイ攻撃などで使用される未知の高度なマルウェアを検出し、端末を防御します。端末で見つけた不審なサンプルをクラウド上の解析環境に自動で送信、解析し、悪質と判断されたファイルは全社レベルで自動的にブロックします。

6. フルディスク暗号化（ESET Full Disk Encryption）

PC のディスク全体の暗号化とプリブート認証※を行います。万が一 PC が紛失・盗難にあった際の情報漏洩を防ぎます。

※ OSの起動前に行うユーザー認証。

7. クラウドアプリケーションセキュリティ（ESET Cloud Office Security）

Microsoft 365のセキュリティを強化するクラウドサービスです。Exchange Online / OneDrive / Microsoft Teams / SharePoint Online に対するマルウェア対策と、スパムメール対策、フィッシング対策、またクラウドサンドボックステクノロジーによるランサムウェアやゼロデイ攻撃への対策が統合され、脅威から重要データとユーザーを保護します。