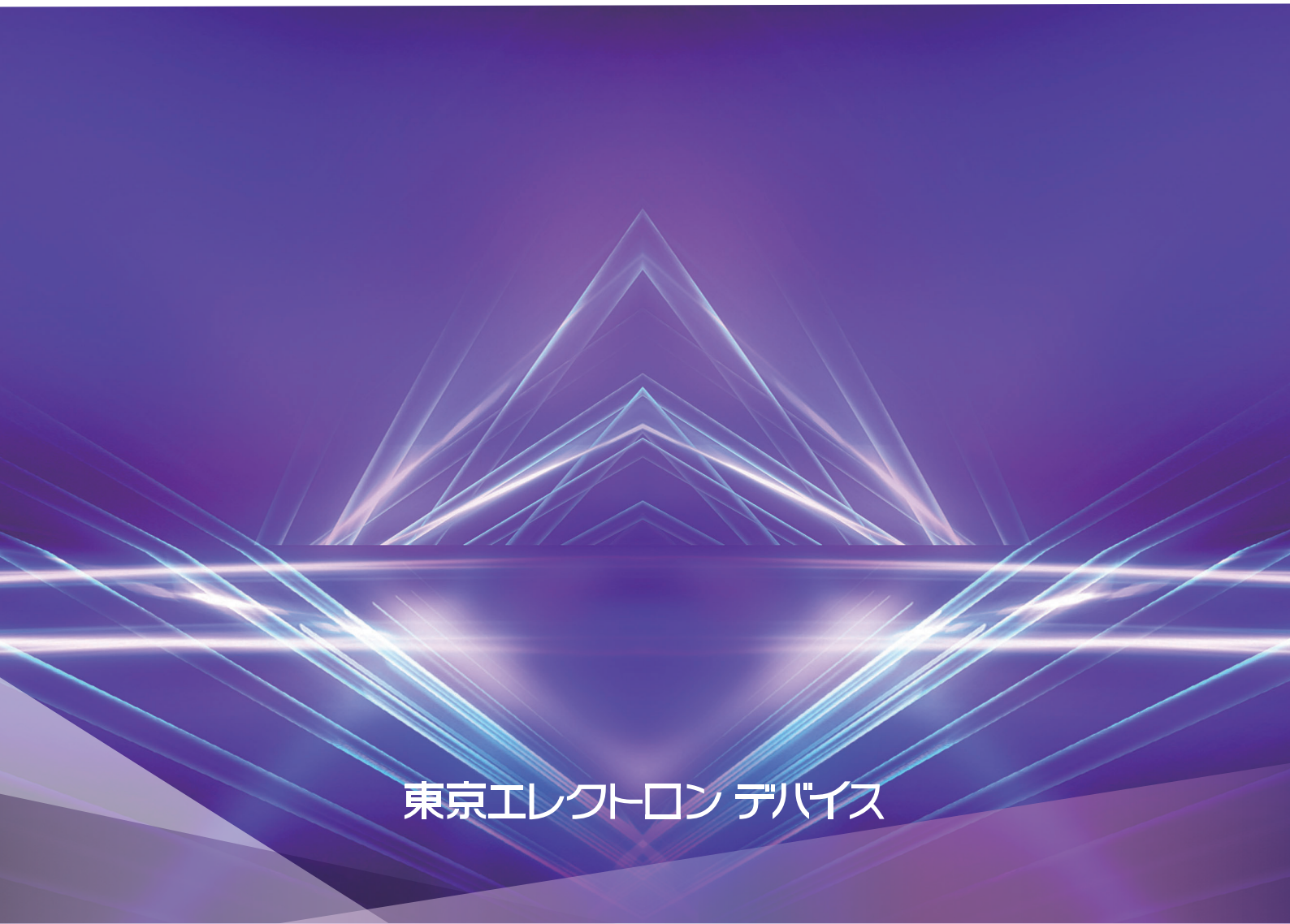
未知の脅威をアクティブに封じ込める
次世代型 EDR ソリューション

SentinelOne

サイバー攻撃の手口が日々刻々と高度化・複雑化し続ける現在、エンドポイントを保護するための新しいソリューションとしてEDR（Endpoint Detection & Response）が注目されています。東京エレクトロンデバイスが提供する「SentinelOne Endpoint Protection Platform」は、脅威の検知から対応・修復までを可能な限り自動実行する「Active EDR」というコンセプトに基づいた、次世代エンドポイントセキュリティソリューションです。



東京エレクトロン デバイス

従来のセキュリティ対策が抱える課題とは？

近年、サイバー攻撃の手口が急速に高度化・複雑化し、機密情報の窃取や重要データの毀損といった被害に遭うインシデントが後を絶ちません。多くの企業はインターネットと内部ネットワークの境界にファイアウォールやIDS／IPS（不正侵入検知／防御システム）を設置し、エンドポイントにはアンチウイルス製品を導入するといったセキュリティ対策を講じているはずです。それにもかかわらず、インシデントが発生してしまうのは、従来のセキュリティ対策だけでは次々に出現する未知の脅威に対抗し切れないからです（図1）。

従来のエンドポイントセキュリティの対策は、既知の攻撃パターンを記録したデータベースに照らし合わせて脅威を検知・防御するシグネチャマッチング型が主流でした。その後も、仮想環境（サンドボックス）での検知や機械学習によるファイル解析といった、さまざまなアプローチが出てきています。

しかしこれらの方法では、爆発的に増え続ける脅威をもれなく検知することは難しいのです。未知の脅威を推測・発見する過程では誤検知も多く、なかでもOSの正規ツールを不正操作して攻撃を仕掛けるファイルレス攻撃には、無力とも言える状況なのです。

こうした状況を打破するために、最終的な攻撃のターゲットになっているエンドポイントでは、より一層強化した検知・防御の仕組みを導入する必要性が高まっています。そんな新しいエンドポイントセキュリティソリューションとして注目されているのが、EDR（Endpoint Detection & Response）です。

図 1●従来のセキュリティ対策では高度化・複雑化する攻撃を守り切れない

新たなソリューションとして注目を集めるEDR

EDRは、従来のセキュリティ対策のように脅威の侵入を未然に防ごうとするものではありません。たとえ侵入を許したとしても、感染の初期段階で素早く検知（Detection）・対応（Response）することで、情報漏えいなどの最悪の事態を避けるというコンセプトのソリューションです。エンドポイントの一挙手一投足をモニタリングし、ログとして常時記録をとりながら脅威を検知するという働きをします。「侵入を前提とした」という表現がよく使われますが、厳密には「感染を前提とした」ものなのです。

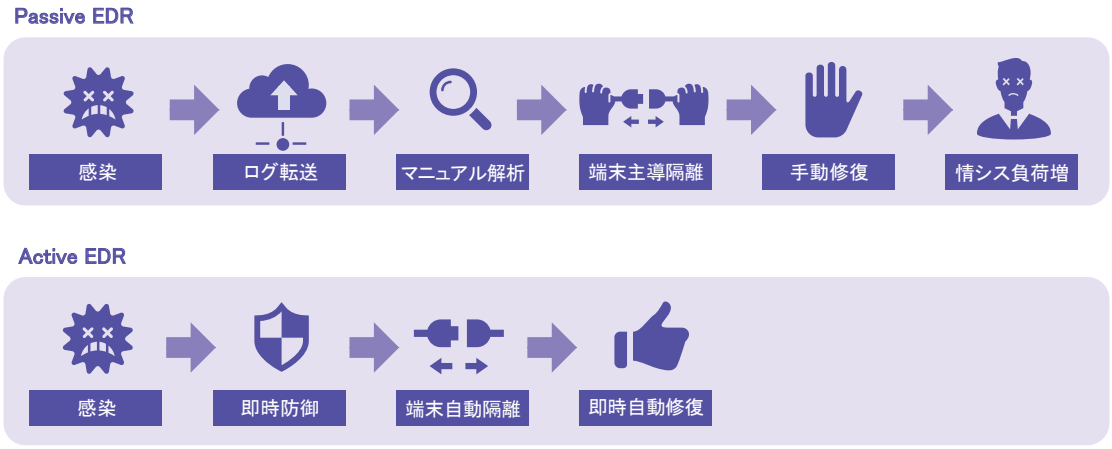
米国の調査会社ガートナーによると、現在は全世界の約15%の企業がEDRを導入しています。2021年には大企業の80%、中規模企業の25%、小規模企業の10%がEDRを導入し、数年内には確実にEDRが標準的に導入されると見ています。実際、多くのセキュリティベンダーが続々とEDR市場に参入し、すでに激しい競争が始まっています。

しかしながら、現時点のEDRには課題も指摘されています。EDRは本来、企業のセキュリティ監視・運用管理を代行するセキュリティオペレーションセンター（以下SOC）向けのツールとして誕生したという経緯があります。そのため、ツールを使いこなすには専門知識が必要であり、一般企業にとって運用管理のオペレーションは難しいものです。また検知してから対応するまでにタイムロスが発生してしまうと、想定以上のスピードで感染が広がってしまうという懸念もあります。

Active EDR のコンセプトに基づいた SentinelOne

さらに大きな課題と言えるのが、各セキュリティベンダーのEDR製品には機能差があるということです。なかにはEDRという名称でありながら検知も対応もせず、検知は既存のエンドポイント保護（EPP）ツールが担当し、対応はアラートを受け取った担当者が手作業で行わなければならない製品もあるほどです。

図 2●Passive EDR と Active EDR の違い



最も一般的なEDR製品は検知・対応の機能を備えているものの、上述したようにSOCがインシデント発生時の対応を受動的に行う目的で作られています。そのため、実際のインシデント発生時におけるオペレーションや対応の判断には、どうしても高度な専門知識とスキルが必要になります。また分析処理をクラウド側で実行するEDR製品も多く、そうした製品の場合はクラウドへの接続が必須であり、検知するのに時間がかかるという課題もあります。

こうした一般的なEDR製品の課題を解決するには、検知・対応の機能をできる限り自動実行し、高度な専門知識やスキルがなくてもインシデント対応が可能な製品が求められます。また分析処理をエンドポイント内部で実行し、オンラインでもオフラインでも素早い検知・対応を行えることが望ましいと言えます。

こうした機能を備えた EDR 製品が、東京エレクトロンデバイスが提供する「SentinelOne Endpoint Protection Platform（以下 SentinelOne EPP）」です。SentinelOne EPP は検知・対応を自動実行するだけでなく、攻撃に関与したすべてのプロセスを可視化し、感染前の状態に戻す修復機能も搭載しているという特長があります。もちろん、高度な専門知識やスキルがなくてもインシデント対応が可能です。

SentinelOne EPP ではインシデント発生時に受動的に対応する一般的な EDR 製品を「Passive EDR」、インシデント対応を自律的・能動的に実行する EDR 製品を「Active EDR」と呼んでいます（図 2）。その Active EDR のコンセプトに基づいた唯一の製品が、SentinelOne EPP なのです。

検知・対応だけでなく「修復処理」も実現

Active EDR の機能を提供する SentinelOne EPP は、外部から脅威がエンドポイントに侵入したときに、そのインシデントを自動的に検知し、自律的に防御機能が働く仕組みになっています。例えば Microsoft Word を隠れ蓑にしたあるファイルレス攻撃はエンドポイントに侵入すると、数分以内に約 10,000 以上ものイベントが発生して攻撃者が遠隔から不正操作を行う C&C（Command & Control）サーバーとの通信が成立してしまいました。このような場合、ネットワーク全体に感染が広がるのは時間の問題であり、他社の EDR 製品では情報漏えいの実害に遭うことになります。

それに対して、SentinelOne EPPをエンドポイントに導入しておくと、このようなファイルレス攻撃が侵入したとしても、わずか数十イベント足らずで攻撃を検知・ブロックします。まさに感染の初期段階で素早く対応します。さらに修復機能によって、感染前の元の状態に戻すことも可能になっています（図3）。

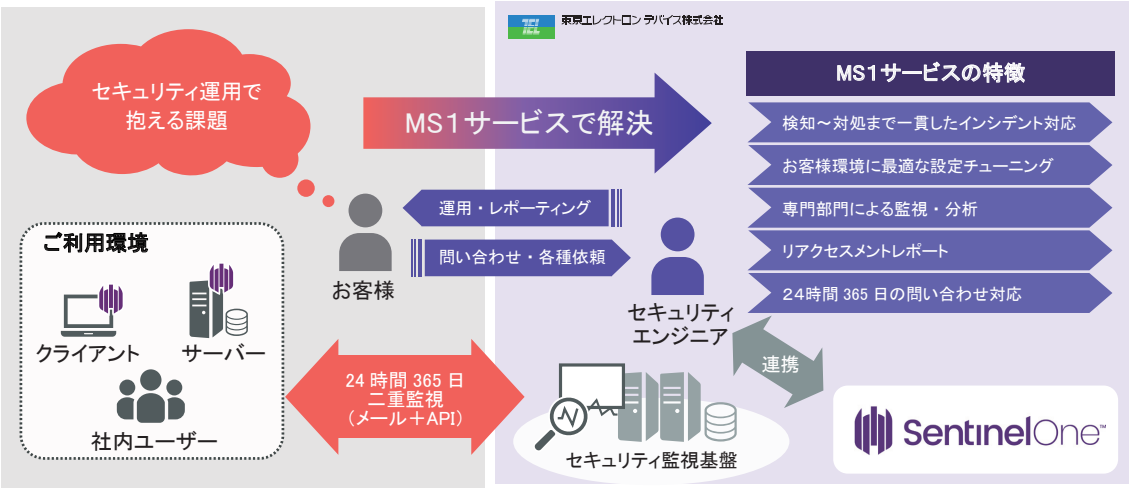
Active EDRは従来のEDR製品のように検知・調査目的に留まらず、より積極的に防御し、修復を行う、まさにこれからのデジタルトランスフォーメーション（DX）時代の安全を担うセキュリティ製品です。

東京エレクトロンデバイスでは、この SentinelOne EPP を“一押し”の EDR 製品として推奨しています。開発元の米 SentinelOne 社との間にも、技術サポートの太いパイプラインが存在しており、日本国内で安心して導入することができます。さらに東京エレクトロンデバイスでは、SentinelOne EPP を導入した後のインシデント対応への迅速化、セキュリティ運用の最適化を支援するマネージドサービス「Managed SentinelOne（MS1）サービス」も提供しています（図 4）。

すでにSentinelOne　EPPを導入し、運用負荷とコストを抑制しながら高度な脅威検知と防御を実現した導入事例が多数存在しています。これからEDR製品を導入しようという企業は、ぜひ東京エレクトロンデバイスにお問い合わせください。

図 3●高度な攻撃も即時検知・ブロックし、修復も実行可能

図 4●東京エレクトロンデバイス「Managed SentinelOne（MS1）サービス」



東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp

新宿：〒163-1034 東京都新宿区西新宿 3-7-1 新宿パークタワー S34 階
Tel.03-5908-1990 Fax.03-5908-1991

大阪：〒540-6033 大阪府大阪市中央区城見 1-2-27 クリスタルタワー 33 階
Tel.06-4792-1908 Fax.06-6945-8581

名古屋：〒451-0045 愛知県名古屋市西区名駅 2-27-8 名古屋プライムセントラルタワー 8 階
Tel.052-562-0826 Fax.052-561-5382

つくば：〒305-0033 茨城県つくば市東新井 15-4 関友つくばビル 7 階
Tel.029-848-6030 Fax.029-848-6035

お問い合わせは、Web サイトの下記フォームよりお願いします。
https://cn.teldevice.co.jp/product/sentinelone/form.html