【セキュリティ対策最前線】

デジタル時代に求められるグローバルセキュリティガバナンス

デジタル時代の到来により企業システムが変化するなか、セキュリティはどうあるべきか。新たなセキュリティマネジメントの鍵となるエンドポイントの攻略について講演より探る。

エンドポイント対策がセキュリティマネジメントの鍵

企業を支える ICT 環境は絶えることなく変革を続けている。クラウドサービスの普及、働き方改革に伴うモバイルデバイスの活用、グローバルでのコミュニケーションの増加――。これらがもたらすセキュリティへのインパクトは、防御ポイントの多様化だ。

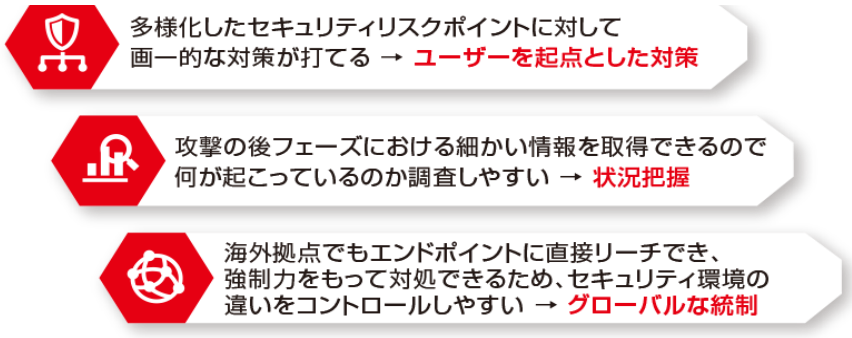
従来は国内の事業所に堅牢なゲートウェイ対策を施すことで一定のセキュリティを担保できていたが、現在の状況は異なる。自宅やカフェ、海外の事業所など異なるプラットフォームからのアクセス増加により、新たなリスクが生まれているのだ。

「デジタル時代におけるセキュリティマネジメントの鍵を握るのは、エンドポイント対策」。こう語るのは、富士通の森玄理氏だ。なぜエンドポイント対策が重要なのか。

「理由は 3 点あります。1 点目は、個々のユーザーを起点とした対策であること。多様化したセキュリティリスクポイントに対し、画一的な対策が打てます。2 点目は、状況把握がしやすいこと。攻撃後の行動解析により詳細な情報を取得することが可能です。3 点目は、グローバルな統制に資すること。海外拠点でも直接リーチできることから、セキュリティ環境の違いをコントロールしやすくなります」（森氏）

富士通株式会社
サイバーセキュリティ事業戦略本部
本部長代理
森 玄理氏

なぜエンドポイントがセキュリティ対策の鍵か？



マスクだけではウイルスは防ぎきれない

従来、セキュリティサービスプロバイダーは防御・検知にフォーカスした MSS（監視・運用）サービスを提供してきた。しかし、リスクが多様化するにつれてウイルスの侵入を完全に防ぐことは困難になってきている。

富士通の勝田圭介氏は、「これまで多くの企業・団体が力を入れてきた入口対策は、マスクを付けて風邪を予防するようなものです。ただ、どれほど気を付けていても体内に入り込んでしまうウイルスは存在します。今後は侵入を前提とした対策にも注力していかなければなりません」と指摘する。

サイバー攻撃の最初の標的にされやすいのは、パソコンなどのクライアント端末。その中に入っている情報には限りがあり、侵入された瞬間に莫大な被害が生じるケースは稀だ。攻撃者にとって有益なコア情報にたどり着くには、数週間から数カ月程度かかるのが一般的だという。

「ウイルスに侵入されても、重症化させない。そのためには、侵入後の的確な状況把握と対応強化が重要です。攻撃者の人手による潜伏活動に着目し、不審な動きや特有の痕跡を検知・対処するソリューションとして、EDR（Endpoint Detection & Response）が注目されています」（勝田氏）

現在、国内には約 10 の EDR 製品があり、基本的な機能は「データ収集」「攻撃検知」「遠隔対処」の 3 点に集約される。このうち、「端末に直接乗り込んで遠隔対処できる第 3 の機能が EDR の醍醐味」と勝田氏は強調する。

「攻撃のターゲットとなった端末を切り離す場合、従来は現地で LAN ケーブルを抜く必要がありました。それに対し、EDR は端末ごとにリモートで対処でき、業務への影響を最小限に抑えることが可能です」（勝田氏）

富士通株式会社
サイバーセキュリティ事業戦略本部
GMSS 事業部サービス企画開発部
アシスタントマネージャー
勝田 圭介氏

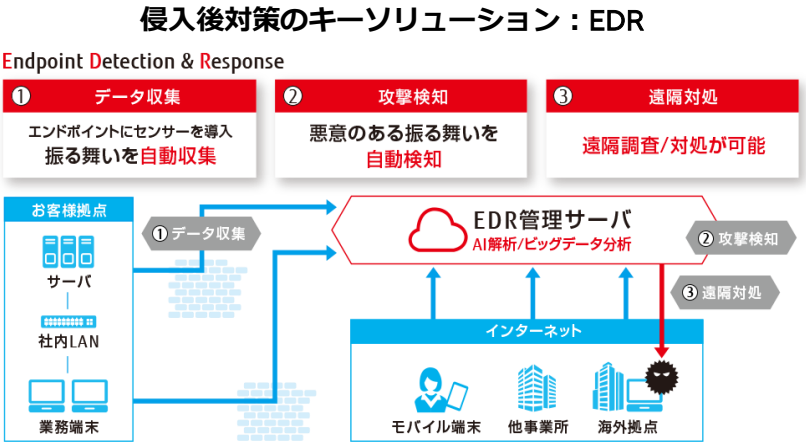
MSS から EDR 運用までセキュリティには総合力が必要

問題は、EDR の運用を自社でできるかどうかだ。日々発生するアラートに対し、「本当に悪意があるか」「遮断しないといけないか」といった判断を個別に行う負荷は小さくなく、人的リソースの課題もある。勝田氏は、EDR 運用には 3 つのポイントがあると指摘する。

「まず、高度セキュリティアナリストの存在。日々の対処に終始するのでなく、攻撃者の心理や手口を把握し、根本原因を突きとめてセキュリティ体制を強化できるアナリストが欠かせません。次に、24 時間 365 日の対応。サイバー攻撃はいつ訪れるか知れず、早期対処による被害の極小化が重要になります。最後に、統合的な運用です。侵入を防ぐための既存対策も引き続き重要であり、EDR と組み合わせた運用により、より効果的なセキュリティマネジメントを実現できます」（勝田氏）

富士通は現在リリースされている各社の EDR を評価・検証しており、顧客の環境や運用体制を踏まえた選定サポート、導入支援が可能だ。加えて、EDR アラートに対する 24 時間 365 日の監視・分析、緊急対処まで実施する包括的な運用サービスも提供している。

森氏は、「EDR は対応力の向上が期待できるソリューションのひとつです。しかし、それだけですべてが解決するわけではありません。従来型の MSS から EDR 運用まで、トータルにサポートする富士通の総合力にぜひご期待ください」と話し、講演を締めくくった。



（注）本特集は日本経済新聞出版社の許可を得て、「日経 MOOK」3 月 12 日号『まるわかり！サイバーセキュリティ』（日本経済新聞出版社刊）に掲載された内容より転載したものです。記事作成時点の情報のため、その後予告なしに変更されることがあります。あらかじめご了承ください。

関連リンク
Managed Security Services

[2019 年 3 月掲載]

お問い合わせ先
製品・サービスについてのお問い合わせはコチラ
富士通株式会社　〒211-8588　神奈川県川崎市中原区上小田中 4-1-1

