覚えておきたい情報セキュリティ&ネットワークのキホン（第18回）

EDRとは何か？従来の情報セキュリティシステムとの違いを解説

2022.09.20

サイバー攻撃の手口は、日々巧妙化しています。企業は悪意のある第三者から自社のデータを守るために、自社に設置されているパソコンはもちろん、テレワークで社外に持ち出して使用するパソコンやスマートフォンについても、サイバー攻撃を防ぐための情報セキュリティ対策を行う必要があります。

情報セキュリティ対策の手法にはさまざまなものがありますが、パソコンなどの端末上で不審な挙動を検知した際に、迅速な対応を行う手法として「EDR（Endpoint Detection and Response）」というものがあります。EDRを導入することで、未知のサイバー攻撃にも対応することが可能になります。

今回は、EDRが必要とされる背景やEDRの特徴、導入時のポイントを紹介します。

＜目次＞
・EDRとは
・EDRの主な情報セキュリティ機能
・EDRとEPPセキュリティシステムとの違い
・EDR導入で得られる効果
・EDR導入時の注意点
・まとめ

EDRとは

EDRとは、サイバー攻撃に対して「エンドポイント」で対応を行う情報セキュリティ対策です。エンドポイントとは「末端」「終点」という意味の言葉ですが、情報セキュリティの世界では、ネットワークに接続されている末端機器のパソコンやスマートフォン、タブレット、サーバーなどの端末を示す言葉です。

これらのパソコンやスマートフォン、タブレット、サーバーと、そこに保存されている情報をサイバー攻撃から守るのに役立つのが、EDRです。

EDRセキュリティが必要とされている背景

EDRは、サイバー攻撃に対抗するための情報セキュリティ対策として、さまざまな企業で活用されています。その背景には、従来の情報セキュリティ対策では防ぎづらい「未知の脅威」にも対応できる点があります。

従来の情報セキュリティ対策は、アンチウイルスソフトのように、既知のウイルス（マルウエア）の情報と突合して脅威を検知する手法が一般的でした。しかし最近では、新種のウイルスが次々登場しており、従来の情報セキュリティ対策ではこうした未知の危機に対処できなくなっています。

しかも従来の情報セキュリティ対策は、コロナ禍で普及しつつあるテレワークにも対応しづらくなっています。例えば、テレワーク中にパソコンやスマートフォン、タブレットといった端末を使用する場合、社外からの不正アクセスを監視する情報セキ

ュリティ対策の1つ「ファイアウォール」の保護外となる場合もあるため、ウイルス感染の危険性は高いといえます。

また、IT管理者の目が届きにくくなることから、ホームルーターの不備や機器のアップデート不足などが放置されて、これらのシステムの脆弱性を狙われる危険があります。

最近では、ランサムウエアに代表されるように、組織化された犯罪者集団による金銭目的でのサイバー攻撃が顕著になっています。バックアップデータを含む大量のデータが暗号化されて「身代金」を要求されたり、不正なマクロ機能を仕込んだファイルを請求書や履歴書等に見せかけて開かせ、悪意のあるプログラムを実行させたりするなど、さまざまな被害が報告されています。

サイバー攻撃の標的は、以前は大企業やグローバル企業が中心でしたが、最近は、情報セキュリティ対策が不十分な場合のある中小企業が狙われることも珍しくありません。中小企業を突破口として大企業への攻撃を仕掛ける攻撃者もいるため、情報セキュリティ対策は、企業の規模は関係なく、最重要課題と言えます。

このように、不正アクセスの複雑化や、社内外で業務を行うハイブリッドなワークスタイルの定着という現状を踏まえて、ネットワークの内外にとらわれず、すべての通信を信用せずに情報セキュリティ対策を行う「ゼロトラスト」という考え方が主流になってきています。

EDRであれば、たとえ未知のウイルスが端末内に侵入したとしても、端末上の各種操作ログを総合的に分析してウイルスの不審な挙動を検知し、感染したパソコンをネットワークから隔離することで、被害を最小限に抑えることが可能です。EDRは、ゼロトラストの観点からも有用な情報セキュリティ対策の1つとして注目されています。

EDRの主な情報セキュリティ機能… 続きを読む