ITで働き方を変える（第13回）

サイバー攻撃の被害を最小化する「初動対応」と「調査・分析」

2024.01.22

サイバー攻撃が巧妙化、高度化する中で中小企業が攻撃の対象として狙われるケースが増えてきている。確固としたセキュリティ対策を講じている大企業をいきなり狙うより、サプライチェーンの構成員である中小企業を攻撃し、そこを踏み台に攻撃対象を拡大する方が効率が良いからだ。規模が小さく、専任のIT管理者もいない中小企業はこの状況にどう対応すれば良いのだろうか。

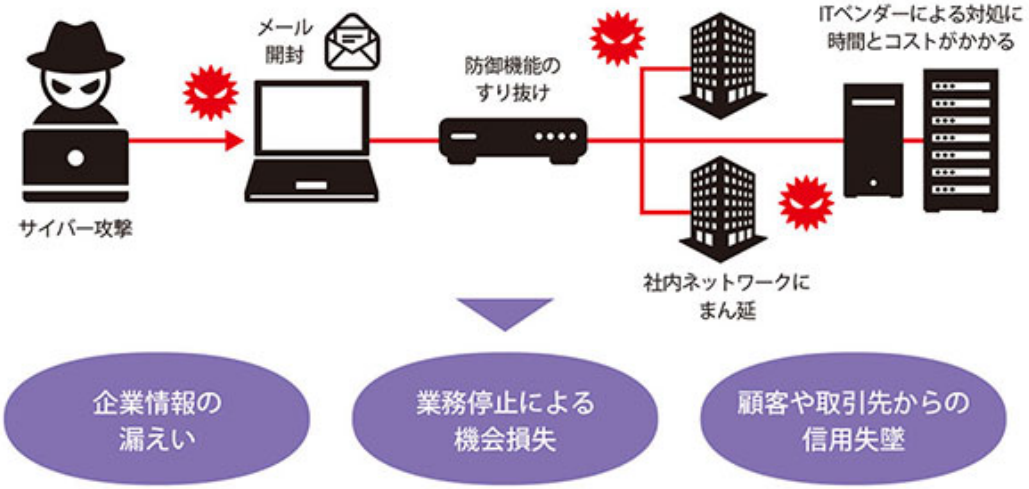
どの中小企業にも求められるセキュリティ対策の強化

昨年から急増しているサイバー攻撃として注目されているランサムウエア攻撃は、不正なプログラムを使って企業が持つデータを暗号化し、使えなくしたところで身代金を要求する攻撃手法だ。サプライチェーンを狙った攻撃の多くがこの攻撃である。

このサプライチェーンへの攻撃で狙われるのが中小企業だ。大企業に比べてセキュリティが脆弱で攻撃しやすく、それを踏み台としてランサムウエア攻撃を広げるケースが増えている。日本でも製造業や医療サービス業などでサプライチェーンを構成する中小企業がサイバー攻撃を受けて被害が拡大したケースが発生した。中小企業も例外ではなく、セキュリティの対策と体制の強化が求められている。

一方、日々進化するサイバー攻撃は高度なセキュリティ機能を導入していても100％防御することはできない。そこで求められるのは、いくつものセキュリティ対策を組み合わせた多層防御である。いかにインシデントの発生を早期検知するのかが問われ、被害拡大を抑止する封じ込めや早期復旧、関連する取引先などへの迅速な報告なども求められる。

●ランサムウエアの感染例



しかし、規模が小さく専任のIT管理者もいない中小企業にとってはこうした仕組みや体制を整えるのは難しい。そこでNTT西日本ではこれまでの多層防御のセキュリティ機能にEDRセキュリティ機能とチャット連携機能を加えてパワーアップした「セキュリティおまかせプラン プライム plus」の提供を開始した。

NTT西日本に任せて安心のセキュリティ対策サービス… 続きを読む