働き方再考（第17回）

多様な働き方に安心を！エンドポイントセキュリティ強化のコツ

2024.01.22

コロナ禍でテレワークなどが導入されたことで、私たちの働き方は大きく変わった。感染拡大が収束した今ではクラウド環境でオフィスワークとテレワークを併用するハイブリッドワークも普及しつつある。いわば「働き方のいいとこどり」が可能となり、それ自体が企業の競争力強化につながっている。しかし、落とし穴もある。どこでも業務が遂行できるようになった反面、エンドポイントの拡大によるセキュリティリスクの高まりだ。規模の小さな企業もその例外ではない。

ビジネス的にも社会的にも求められるセキュリティの強化

企業のシステムを狙うサイバー攻撃はますます巧妙になり、高度化している。攻撃者はセキュリティ対策が脆弱なところに攻撃をかけ、効率良く成果を挙げようとしている。特に狙われているのがサプライチェーンの構成員でもある中小企業だということはご存じだろうか。

サプライチェーンでは企業同士が円滑に取引するために、ネットワークでつながっている。中心的な役割を果たしているのは大企業だが、大企業はしっかりしたセキュリティ対策を講じてる場合が多く攻撃者が攻撃を成功させるには時間も手間もかかる。そこでネットワークにつながっているセキュリティの脆弱な可能性の高い中小企業を狙っているのだ。

攻撃者はまず中小企業のシステムに侵入してIDやパスワードを盗み出し、不正なプログラムを送り込んで攻撃を広げる。近年流行しているランサムウエア攻撃でも同様の手口が使われている。実際にサプライチェーン経由でランサムウエア攻撃を受けて、事業がストップして被害を受けたケースが発生している。

取引先に迷惑をかけないというサプライチェーンの構成員としての責任を果たすために、中小企業にもセキュリティ対策の強化が求められているのである。

インシデント対応に求められる仕組みや体制をどう用意するのか… 続きを読む