最新セキュリティマネジメント（第1回）

サイバー空間潮流。サイバーセキュリティは経営問題

2021.06.22

年々深刻さを増すサイバー攻撃被害。新型コロナウイルス感染拡大によるテレワークの普及は、攻撃者にとって「絶好の機会」と捉えられているようだ。激化する脅威に対抗するため、経営者はどのような姿勢で臨めばよいのだろうか。本記事ではビジネスの未来を左右しかねないサイバーセキュリティに関する最新の潮流を紹介する。

高度化・巧妙化するサイバー攻撃の脅威

2020年12月、経済産業省から「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」が発表された。

標的となる組織や企業の情報システムに対し、ネットワークを介して侵入、破壊といった活動を行うサイバー攻撃は、コンピューターの普及とともに問題視されてきた。ここ数年で急速に手法の高度化・巧妙化が進み、私たちの社会に深刻な影響をもたらしている。

そして、2020年には、大規模な情報漏えいやランサムウェアによる身代金奪取事件が多数発生し、かつてないレベルで危険度が増している実態が明らかになった。その中で経産省が発表した注意喚起は、最近のサイバー攻撃に見られる特徴や攻撃の目的を検証するとともに、全関係者がセキュリティ対策に取り組む必要性を指摘している。

本連載ではこの注意喚起に加え、「サイバーセキュリティは“経営問題”として捉えるべき」との観点から、経営者が取るべき対策をまとめた情報処理推進機構（IPA）の「サイバーセキュリティ経営ガイドライン」を紹介し、ニューノーマル時代に知っておくべきポイントを解説する。

コロナ禍で「攻撃起点」拡大が加速

「テロ」とも称されるサイバー攻撃は、リアル世界と同様に「巧妙・卑劣な」手口で実行される。これはリスクの高い正面からの突破を避け、常に防御レベルの弱い部分を狙って攻撃を仕掛けるというものだ。今回の注意喚起では、攻撃者が使用するサプライチェーン上の「攻撃起点」が拡大していると指摘している。

具体的な攻撃起点としては、有効なセキュリティ対策を講じていない取引先企業、海外拠点、テレワーク拠点（自宅・外出先など）が挙げられている。取引先を装ったメールを使ってシステムに侵入し、ここ数年で大きな被害をもたらしているマルウェア「Emotet」をはじめ、さまざまな信頼関係を悪用した攻撃に十分注意を払うよう求めている。

攻撃起点の確保が終わると、攻撃者は情報の窃取やランサムウェアによる身代金要求といった二次的な攻撃に入る。また、経済のグローバル化やコロナ禍に伴うテレワーク拡大で導入が進むVPN（バーチャル・プライベート・ネットワーク）の脆弱性を悪用した攻撃の増加も指摘している。「自分のパソコンが攻撃起点になる」危険は確実に高まっているというのが現状だ。

狙いは「業務妨害」から「金銭要求」へ… 続きを読む