重要情報の扱いを考え直す（第2回）

情シスに求められるものが多過ぎる

2017.12.20

悪質なサイバー攻撃の被害が相次ぐ中、企業における情報システム部門（以下、情シス）の仕事に変化が表れている。それがセキュリティ管理の外注化だ。日々、高度化、巧妙化するサイバー攻撃による情報流出を防ぐため、「自前」でのセキュリティ管理にこだわることが難しくなりつつある。情シスの未来像とは、どのような姿なのだろうか。

2017年5月に発生した、身代金を要求するランサムウエア「WannaCry」による世界的なサイバー攻撃。わが国でも数社の大企業が感染被害を受けて問題となった。メールなどに添付されて送りつけられる、こうしたマルウエアを検知するにはウイルス対策ソフトのデータベースを常に最新にしておく必要がある。しかし、1日に100万以上出現するといわれるウイルスの新種、亜種をすべて駆除するのは、もはや不可能な状況に陥りつつある。

サイバー攻撃の手口も一段と巧妙化している。特定のターゲットに対して行われる標的型攻撃メール、システムをダウンさせることによる業務妨害など、コンピューターを使うすべての業務が攻撃対象だ。

脅威が増すサイバー攻撃に対して、情報を守る側のセキュリティ対策も高度化を重ねている。具体的にはウイルス対策ソフトに代表される、侵入防止を目的とした水際対策に加え、攻撃者の動きを把握して攻撃実行を未然に防ぐ対策や、たとえ侵入を許しても被害を最小限に抑える事後対策などが開発されている。

セキュリティに関する高度なスキルを持つ人材の育成に加え、AI（人工知能）の活用も進む。AIはウイルス対策ソフトでも使われているほか、最近ではプログラムの脆弱（ぜいじゃく）性を見つけ出したり、機械学習によって攻撃内容を判定したりする利用法も本格化してきた。

セキュリティ関連技術は急ピッチで進化を遂げつつあるが、同時に困った問題も表面化してきた。それは「情シスが対応し切れない」という悩みだ。システムの開発、運用、保守など、企業におけるITの担い手である彼らに、いったい何が起こっているのだろうか。

セキュリティ対策の負担増と情報シスの業務範囲拡大… 続きを読む