潜行するサイバー攻撃（第5回）

「史上最悪」の情報漏えい事件が残した教訓

2018.03.20

年々被害が深刻化するサイバー攻撃。2017年に米国の信用情報会社で発生した事件では1億人を超える顧客情報が流出、経営トップ辞任という事態に発展した。この事件は、サイバー攻撃の脅威に対する私たちの心構えを、あらためて考える契機になっている。

2017年9月、米国の大手信用情報会社エクイファックスから「サイバー攻撃により1億4000万件以上の個人情報が流出した可能性がある」との発表が行われた。流出が疑われたのは顧客の氏名・住所をはじめ、クレジットカード番号、社会保障番号、さらには運転免許証番号など極めて多岐にわたる。その規模と深刻さから「史上最悪レベル」と呼ばれるものとなった。

事件の引き金になったのは、同年3月に見つかった「Apache Struts2」の脆弱性だった。このソフトはWebアプリケーションを開発するためのフレームワーク（仕組み）だ。無償かつ自由に利用可能なことから広く使われる。半面、以前からたびたびセキュリティの脆弱性が指摘されていた

問題となった脆弱性（CVE-2017-5638）は、リモートで任意のコードが実行される恐れがあるというもの。3月7日に公開された後、わが国でもIPA（情報処理推進機構）が3月9日に注意喚起を行った。しかし、この脆弱性を悪用したサイバー攻撃は、数日間で一気に広がり、世界各国から不正アクセスの被害が報告される事態となる。日本でも東京都の都税支払いサイトやJETRO（日本貿易振興機構）、日本郵便のサイトなどが攻撃を受けた。

ところが、エクイファックスは脆弱性対策に必要なパッチ（修正プログラム）処理をすぐに行わなかった。7月末になってようやく対策に乗り出す。しかし、その時点ですでに膨大な個人情報が流出していた。同社の前CEOは、遅れの原因について「人為的、技術的ミスが重なった」と説明したものの、貴重な信用情報を扱う企業としてはあまりにずさんな対応だとして批判を浴びた。

被害の実態はさらに深刻？… 続きを読む