最新セキュリティマネジメント（第15回）

「情報セキュリティ白書2022」に学ぶ（前編）

2022.08.23

独立行政法人情報処理推進機構（IPA）では、情報セキュリティに関する国内外の政策や脅威の動向、インシデントの発生、被害状況などをまとめた「情報セキュリティ白書」を2008年から毎年発行している。最新版が2022年7月15日に発行された。

本連載では、前編と後編に分けて同白書のトピックスの一部を紹介していく。全文はIPAのサイトで会員登録して簡単なアンケートに回答すれば無料で入手できるので、情報セキュリティ強化に役立ててほしい。

インシデントは件数、被害金額とも増加

IPAが発行した「情報セキュリティ白書2022」の序章では、2021年4月から2022年3月に発生した主な情報セキュリティインシデントや事件、情報セキュリティ政策やイベントが一覧表の形で提示されている。目を通すと1年間に起きた主な事件が分かるだろう。発生した事件の中で目につくのは、ランサムウエアによる被害や不正アクセス、国内工場の停止などだ。

続く第1章では「情報セキュリティインシデント・脆弱性の現状と対策」が約60ページにわたりまとめられている。2021年に注目されたのが、広範囲に影響を与えるサプライチェーンに関わるインシデントがいくつも起きたことだ。例えば、2021年5月には米国東海岸の燃料輸送が6日間にわたって停止し、社会的に大きな影響が出た。

サイバー犯罪の届出件数と被害額は毎年増加、2021年は約85万件で被害総額は69億ドルに上る。情報漏えいの手口として増加しているのがWebアプリケーションで、電子メールを10%ほど上回っている。最も注意が必要とされるランサムウエアの感染手口としては「フィッシング」と「脆弱性の悪用」が上位を占め、両方で全体の75%になる。

ランサムウエアは国内でも被害が拡大している。盗んだデータを暗号化するだけではなく、金銭を支払わなければデータを公開すると脅す「二重恐喝」が広がり、産業制御システムに影響を及ぼすウイルスが確認されているという。金銭が要求された被害のうち、85%が二重恐喝だったようだ。

ランサムウエアの感染経路として、VPNやリモートデスクトップが増えていることにも注目したい。白書には「新型コロナウイルス感染症拡大で定着したリモートワークにより顕在化した脅威である」と記されている。

被害防止策をインシデントごとに考えよう… 続きを読む