最新セキュリティマネジメント（第16回）

「情報セキュリティ白書2022」に学ぶ（後編）

2022.09.22

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。2022年版は7月15日に発行された。先月の前編では第1章の「情報セキュリティインシデント・脆弱性の現状と対策」を中心に紹介したが、今回は情報セキュリティ政策の変化や企業におけるセキュリティ対策の状況などについてのトピックスを紹介する。

情報セキュリティ政策を活用する

IPAが発行した「情報セキュリティ白書2022」の第2章は「情報セキュリティを支える基盤の動向」というタイトルで、幅広い情報が網羅されている。ここでは一般企業にとって参考になる情報について取り上げる。

最初の「国内の情報セキュリティ政策の状況」では、政府が推進する情報セキュリティ政策の状況について解説されている。政府は経済社会のデジタル化やDX推進の動きに併せてサイバーセキュリティ確保に向けた取り組みを同時に推進する「DX with Cybersecurity」が重要だとしている。

現在、経済産業省のもとでIPAがさまざまな施策に取り組んでいるが、基本となるのが2019年4月に策定された「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」である。CPSFを軸に「サイバーセキュリティ経営ガイドライン」「中小企業の情報セキュリティガイドライン」など、さまざまな支援ツールが提供されている。

これらのツールの中には、サイバーセキュリティ経営を実践するためのプラクティス集や実践をサポートする事例の検索ツール、サイバーセキュリティ経営を可視化するツールなどが記載されており、具体的な対策を進める上でも活用できるだろう。

また、中小企業が利用しやすいセキュリティ対策サービスを「サイバーセキュリティお助け隊」として認定する取り組みも紹介されている。一定の基準に従ってIPAが認定したマークの使用権を付与するもので、サービスを選ぶ際の参考になる。

さらに、近年不足しているセキュリティ人材を育成する取り組みとして、以前も取り上げた若年層向けのセキュリティ・キャンプや産業サイバーセキュリティセンターにおける中核人材育成プログラムや情報セキュリティマネジメント試験、情報処理安全確保支援士が紹介されている。自社のセキュリティ人材の育成目標に組み込むのもよいだろう。

脅威は認識しつつも具体的対策は遅れている… 続きを読む