強い会社の着眼点（第20回）

「サイバーセキュリティ月間」に改めて考える！対策のポイント

2025.02.03

日本政府は、重点的かつ効果的にサイバーセキュリティに対する取り組みを推進するため、毎年2月1日から3月18日までを「サイバーセキュリティ月間」と定めている。大上段に構えた情報からお伝えすることになってしまうが、この期間中に政府は団体や企業などと連携し、サイバーセキュリティに関する普及啓発活動を集中的に実施する。

「サイバーセキュリティ月間」とは？どのような取り組みなのか

どこかの営利団体がセキュリティ商材を売り込むために企画したイベントではなく、10年以上にわたる国を挙げての取り組みであり、それだけサイバーセキュリティが国や社会を守るために重要だとわかる。その対象は、一般人に向けたICTリテラシー向上のためのセミナーから、学生、子ども向けの講習会、ビジネスパーソン向けの実践的な注意喚起セミナーまで幅広いものになる。内閣サイバーセキュリティセンター（NISC）では、「みんなで使おうサイバーセキュリティ・ポータルサイト」で情報を提供し、参加を呼びかけている。

重要度増すサイバーセキュリティ対策。現在はどのような被害が増加？

このような国を挙げての取り組みがあって、大企業から情報が流出したといったニュースに触れることがあっても、多くのビジネスパーソンや中小企業経営者にとってセキュリティ脅威はなかなか自分ごととして捉えられないのも事実だろう。

まず、どんなセキュリティ脅威が企業に襲いかかっているかを整理してみよう。こうしたときに役立つのが、情報処理推進機構（IPA）が毎年発表している「情報セキュリティ10大脅威」だ。原稿執筆時点で最新の2024年版をひもといてみる。

1位：ランサムウェアによる被害

2位：サプライチェーンの弱点を悪用した攻撃

3位：内部不正による情報漏えい等の被害

4位：標的型攻撃による機密情報の窃取

5位：修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

※IPA「情報セキュリティ10大脅威2024」（組織）を基にBiz Clip作成

上位5番目までの脅威は、このような状況になっている。このうち、1位のランサムウェアと、3位の内部不正、4位の標的型攻撃は、2016年から9年連続して9回目の選出となっており、脅威として常連化していることがわかる。一方で、「サプライチェーン攻撃」は、2019年から6年連続6回目、ゼロデイ攻撃は2022年から3年連続3回目の選出で、比較的新しく脅威の度合いが高まっていることがわかる。

そうした中で、IPAでは「多数の脅威があるが『攻撃の糸口』は似通っている」「基本的な対策の重要性は長年変わらない」と分析する。さらにIPAは情報セキュリティ対策の基本として、「ソフトウェアの更新」「セキュリティソフトの利用」「パスワードの管理・認証の強化」「設定の見直し」「脅威・手口を知る」の5つを常に意識することを推奨する。この基本からもわかるように、一度セキュリティ対策をすればOKではなく、常に情報を入手し、対策を強化していく日常的な取り組みが求められているのだ。

具体的な対策は？IT人材が不足する場合の対応策は？… 続きを読む