最新セキュリティマネジメント（第22回）

「情報セキュリティ10大脅威 2023」に学ぶ

2023.03.20

毎年恒例の「情報セキュリティ10大脅威」の最新版が、1月25日に独立行政法人情報処理推進機構（IPA）から発表された。これは、2022年に発生した脅威の中から約200名の研究者や企業の実務担当者の投票によってランク付けされたものだ。すべての脅威が含まれているわけではないが、ここから情報セキュリティの最新のトレンドを読み取れる。

10大脅威の変化から分かる最新トレンド

「情報セキュリティ10大脅威 2023」はいつものように「個人」と「組織」に分けて10大脅威を決定している。ここでは企業などを対象とした「組織」編を取り上げていく。

1位にランキングされたのは昨年、一昨年と同様に「ランサムウェアによる被害」だった。ランサムウエアと呼ばれるウイルスにパソコンやサーバーが感染すると、暗号化されて利用できなくなり、その復旧と引き換えに金銭を要求されるものだ。今、最も警戒すべき脅威と考えられている。

2位は「サプライチェーンの弱点を悪用した攻撃」だ。一昨年の4位、昨年の3位から毎年ランクアップしている。商品の企画開発から調達、製造、物流、販売といったサプライチェーン上で取引している企業などを狙った攻撃である。

強固なセキュリティ対策が講じられている大企業ではなく、ガードの甘い中小企業などの取引先に潜り込み、これを踏み台にして本命の企業を狙うという手口だけに、中小企業にとっては大きな脅威だといえる。

「情報セキュリティ10大脅威 2023」の解説書では、例として2022年3月に起きた攻撃が取り上げられている。トヨタ自動車の取引先のシステム障害により、国内の全工場が操業を停止した事件だ。実際に子会社の社内ネットワークへの侵入後に、同社の社内ネットワークにも侵入され、サーバーやパソコンへの攻撃の痕跡が確認されたという。

3位は特定の組織をターゲットとした「標的型攻撃による機密情報の窃取」、4位は「内部不正による情報漏えい」、5位は「テレワーク等のニューノーマルな働き方を狙った攻撃」と、ある意味いつもの顔ぶれが続く。注目すべきは2018年以来5年ぶりに圏外から10位にランクインした「犯罪のビジネス化（アンダーグランドサービス）」だろう。

ダークウェブまたはディープウェブと呼ばれる通常のブラウザーでは検索できないWebサイト上では、盗まれたIDやパスワードなどの情報が売り買いされているだけでなく、サイバー犯罪に使用するためのサービスやツールなどが取引されている。筆者も専門家からそうしたWebサイトを見せてもらったが、攻撃を請け負うサービスや誰でも簡単にウイルスが作れてしまうツールが、まるでECサイトのように取引されていて驚いた。こうした活動の活発化はサイバー攻撃の増加を意味する。

社内の啓発と体制づくりに解説書と活用法を役立てる… 続きを読む