最新セキュリティマネジメント（第46回）

「情報セキュリティ10大脅威2025」決定

2025.02.13

2025年1月30日、独立行政法人情報処理推進機構（以下、IPA）が「情報セキュリティ10大脅威2025（以下、10大脅威）」を決定したと発表した。詳細な解説は2月下旬以降順次公開されるが、今回は速報版の内容を紹介する。

依然として変わらない中小企業が狙われる現実

10大脅威は情報セキュリティ対策の普及を後押しするために、2006年以降IPAが毎年公表しているものだ。前年発生した情報セキュリティ事故やサイバー攻撃の中からIPAが候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200人から構成された「10大脅威選考会」の投票を経て決定される。

組織部門の第1位、第2位は前年と同じ脅威だった。第1位は社会問題としてニュースなどでも度々取り上げられる「ランサム攻撃による被害」で、2016年に初めて選出されてから10年連続10回目のランクインとなった。企業などが保有するデータを暗号化して利用できない状態にした上で、そのデータを復号する対価として金銭を要求する目的があり、身代金を意味する「Ransom（ランサム）」という言葉が使われている。

ランサムウエアによる被害で肝に銘じておきたいのは、中小企業にとって人ごとではないという点だ。実に被害の約6割が中小企業で占められている。ニュースなどの報道は知名度の高い大企業が目立つが、中小企業も大きな被害に遭っている。

関連する脅威が、第2位の「サプライチェーンや委託先を狙った攻撃」だ。サイバー攻撃者には効率的に金銭を稼ぎたいという目的がある。できれば大企業を攻撃したいが、強固なセキュリティ対策を講じている企業も多く、それは効率的ではない。そこで、セキュリティ対策が不十分で比較的規模の小さいサプライチェーン企業や委託先を攻撃し、大企業への足掛かりにするケースが増えている。一昨年話題になった関西の中核病院のケースでは、委託している給食業者のサーバー経由で攻撃したと見られている。

世界情勢の不安定化にも注意… 続きを読む