最新セキュリティマネジメント（第35回）

2023年、新種のランサムウエア攻撃が増加

2024.04.15

企業や組織に対するサイバー攻撃は依然として続いている。独立行政法人情報処理推進機構（以下、IPA）が2024年3月27日に発表した最新のリポート「コンピュータウイルス・不正アクセスの届出事例」によると、2023年下半期（7月～12月）に届出があった事例のうち4分の1以上がランサムウエア攻撃だった。このランサムウエア攻撃には新たな手法も登場している。

従来型攻撃に加えてノーウエアランサム攻撃が広がる

2023年7月から12月にIPAに届けられたサイバー攻撃は61件。このうち「脆弱性や設定不備を悪用された不正アクセス」が15件、「IDとパスワードによる認証を突破された不正アクセス」が13件あり、これらは基本的なセキュリティ対策を実施すれば未然に防ぐことが可能だったと分析されている。

届出があった事例の中で最も多かったのが「身代金を要求するサイバー攻撃の被害」で、17件に上る。この攻撃法は“ランサムウエア攻撃”と呼ばれている。一般的なランサムウエア攻撃は、企業や組織が保有するファイルを暗号化して利用できない状態にする。そして、暗号化を元に戻す処理である“復号”と引き換えに身代金を要求するというものだ。

しかし、今回届出のあった事例には、ファイルの暗号化ではなく窃取されたファイルの公開と引き換えに金銭を要求されたものがあったという。この攻撃手法は「ノーウエアランサム攻撃」といわれるもので、2023年9月21日に警察庁が発表したリポート「令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について」でも指摘している。

警察庁のリポートによればランサムウエアによる被害件数は103件あり、前年同期比で9.6％減少しているものの引き続き高い水準で推移しており、「ノーウエアランサム攻撃」が新たに6件確認されたという。新たな脅威ともいえる「ノーウエアランサム攻撃」はどのような攻撃で、被害を防ぐにはどんな対処方法が考えられるのだろうか。

ノーウエアランサム攻撃にどう向き合えば良いのか… 続きを読む