最新セキュリティマネジメント（第29回）

最新のサイバー攻撃の実態を知って被害を防ぐ

2023.10.23

2023年9月29日、独立行政法人情報処理振興機構（以下：IPA）が2023年上半期の「コンピュータウイルス・不正アクセスの届出事例」を公表した。2023年1月から6月の半年間にIPAに届けられ、IPAが受理したものの中から同様の被害の発生が想定される事例についてまとめたものだ。いま起きているサイバー攻撃の実態を伝えるとともに、被害の発生を防ぐために、最も注意すべきポイントを解説する。

2023年上半期の被害事例で見逃せない攻撃パターン

2023年上半期に届出があったうち、今後も同様の被害が発生すると判断してIPAが掲載した事例は58件あった。内訳は「コンピュータウイルスの検知・感染被害」9件、「身代金を要求するサイバー攻撃の被害」15件、「脆弱性や設定不備を悪用された不正アクセス」17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」9件、「その他」が8件となっている。

1つ目の「コンピュータウイルスの検知・感染被害」では、この連載コラムでも活動を再開したとお伝えしたEmotetが7件を占める。Emotetはメールアカウントやデータを盗み取ったり、他のウイルスへの二次感染を引き起こしたりするウイルスだが、依然として脅威を振るっているようだ。

Emotet対策としては、これまでのウイルス対策と同様、怪しいメールに対して「添付ファイルを開かない」「URLリンクにアクセスしない」「マクロを有効にしない」などを従業員に徹底するしかない。

今回注目したいのは、届出件数の多かった2番目と3番目の「身代金を要求するサイバー攻撃の被害」と「脆弱性や設定不備を悪用された不正アクセス」だ。いずれも大きな損失につながりかねない攻撃で、狙われている部分には共通点もある。

身代金を要求するサイバー攻撃、いわゆるランサムウエアによる脅威は常にIPAの「情報セキュリティ10大脅威」の上位にランクインし、今でも頻発していると見られる。気付かないうちにデスクトップ上やサーバー上のファイルが暗号化され、事業継続ができなくなった状態で、身代金を要求するメッセージが突きつけられる。

脆弱性などを悪用した不正アクセスの場合には、組織内部に侵入されてさまざまな被害が発生する。「サーバーとの通信が切断される」「パスワードの変更ができなくなる」「NASのファイルが開けなくなる」「業務で使っているパソコンが起動しなくなる」といった事態が発生して、業務に大きな支障を来す。

多様な働き方を支えるVPN装置が狙われている

今回の届出事例のリポートでは、こうした攻撃の多くがVPN装置の脆弱性に起因していると解説されている点に注目したい。VPN装置はテレワークなどハイブリッドな働き方を支える重要な役割を担うだけに、看過できないポイントだ。

ランサムウエア攻撃の解説では「感染・侵入の原因（推定も含む）として最も多く挙げていたのは、VPN装置の脆弱性を悪用

した不正アクセスであった」とあり、不正アクセスの解説では、「VPN装置の脆弱性を悪用された不正アクセス被害は、先期から引き続き、多数の届出があり、攻撃者から積極的に狙われている状況にある」とある。

問題は、脆弱性がさらされる原因として、既知の脆弱性を悪用された事例が多いことだ。VPN装置の脆弱性についてはベンダーから情報が通知され、修正プログラムが提供されるが、被害に遭った企業や組織は適切な対応を怠り、その結果被害が発生したケースも少なくないと考えられる。

このリポートでは脆弱性の管理体制の見直しを促すとともに、「自組織での対応が難しい場合には、契約している保守業者との契約内容を見直し、自社が対応可能な範囲を明確化する。あるいは、外部の専門業者に保守を委託することを勧める」と提案している。IPAが警告を発するほど事態は深刻なのだ。自社がどう対応するべきか真剣に考えてほしい。

IPAのホームページには被害に遭った際の届出様式が紹介されている。実際にサイバー攻撃を受けて被害に遭った場合には、同様の被害の発生を防ぐためにIPAに届け出るべきだ。こうした取り組みによって、社会全体でサイバー攻撃の被害を少しでも減らすことが求められている。