

## 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

2023.10.25



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はメールアドレス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ェ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思われる。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… 続きを読む