23年版の10大脅威を公表

ランサムウエアによる被害が3年連続1位

独立行政法人情報処理推進機構（IPA）は、2022年に発生した社会的に影響が大きかったと考えられる情報セキュリティに関する事案について、情報セキュリティ分野の研究者など約200人のメンバーからなる「10大脅威選考会」の審議・投票によりトップ10を選出し、「情報セキュリティ10大脅威2023」として順位を決定し、IPAのホームページで公表した。

組織の順位では、3年連続で「ランサムウエアによる被害」が1位となった。22年も脆弱（ぜいじゃく）性を悪用した事例やリモートデスクトップ経由での不正アクセスによる事例が発生している。

また、情報の暗号化のみならず窃取した情報を公開すると脅す「二重脅迫」に加え、DDoS攻撃（分散型サービス妨害攻撃）を仕掛ける、被害者の顧客や利害関係者へ連絡するとさらに脅す「四重脅迫」が新たな手口として挙げられている。ランサムウエアの感染経路は多岐にわたるため、ウイルス対策、不正アクセス対策、脆弱性対策などの基本的な対策を、確実かつ多層的に適用することが重要である。また、バックアップの取得や復旧計画を策定するといった、攻撃を受けることを想定した事前の準備が重要である。

個人の順位では、「フィッシングによる個人情報などの詐取」が2年連続で1位となった。フィッシング詐欺は、実在の公的機関、有名企業をかたるメールやショートメッセージサービス（SMS）を送信し、正規のウェブサイトを模倣したフィッシングサイトへ誘導することで認証情報や個人情報などを入力させ詐取する手口である。フィッシング対策協議会のフィッシング報告状況によると22年の報告件数は約97万件と、21年の約53万件から大幅に増加しており、一層の注意が必要である。詐取された認証情報による不正ログインを予防するために多要素認証を有効にする、被害を早期に発見するために利用サービスのログイン履歴やクレジットカードなどの利用明細を日常的に確認するといった取り組みが大切である。

「共通対策」で効率化支援

23年版は組織、個人共に10位の脅威が入れ替わるのみで、9位までの脅威の種類は22年版と同じであった。しかし、組織10位に他の脅威を誘発しかねない「犯罪のビジネス化（アンダーグラウンドサービス）」がランクインしたように、各脅威に対して適切な対策を取ることが引き続き求められる。

IPAでは今年新たに、多岐にわたる脅威に対して共通する対策をまとめて具体的に解説する「共通対策」を作成する。パスワードの適切な運用方法や、適切なインシデント対応方法などを七つの項目に分類して記載し、効率的な対策を支援する。「共通対策」は「情報セキュリティ10大脅威2023」にランクインした各脅威の詳しい解説とともに、2月下旬にIPAのウェブサイトで公開する予定である。対策の検討や社内教育の参考にしてほしい。

（独立行政法人情報処理推進機構・江島将和）

10大脅威2023の脅威順位

個人	順位	組織
フィッシングによる個人情報などの詐取	1位	ランサムウエアによる被害
ネット上の誹謗（ひぼう）・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃
メールやSMSなどを使った脅迫詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取
クレジットカード情報の不正利用	4位	内部不正による情報漏えい
スマホ決済の不正利用	5位	テレワークなどのニューノーマルな働き方を狙った攻撃
不正アプリによるスマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの個人情報の窃取	8位	脆弱性対策情報の公開に伴う悪用増加
インターネット上のサービスへの不正ログイン	9位	不注意による情報漏えいなどの被害
ワンクリック請求などの不当請求による金銭被害	10位	犯罪のビジネス化（アンダーグラウンドサービス）

「情報セキュリティ10大脅威2023」はこちらを参照