19年版「10大脅威」発表

1位は標的型攻撃による被害

独立行政法人情報処理推進機構（IPA）は、2018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ーに関するトピックについて、情報セキュリティー分野の研究者など約120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を選出した。「情報セキュリティ10大脅威2019」として順位を決定し、IPAのホームページ（https://www.ipa.go.jp/security/vuln/10threats2019.html）で公表している。

今年の組織の脅威ランキングの1位は18年に引き続き「標的型攻撃による被害」である。IPAに設置する「標的型サイバー攻撃特別相談窓口」に対して18年上期に寄せられた相談件数は155件。特定の攻撃グループによると思われる標的型メール攻撃が継続的に行われており注意が必要だ。

昨年3位だった「ビジネスメール詐欺による被害」はランクを一つ上げて2位となった。ビジネスメール詐欺は、巧妙に細工したメールのやりとりにより、企業の担当者をだまし、攻撃者の用意した口座へ送金させる詐欺の手口である。18年7月には、日本語のメールによる攻撃事例を確認した。あらゆる国内企業・組織が攻撃対象となり得る状況である。企業は、このような詐欺の手口があることを知るとともに、電信送金に関するチェック体制の整備が必要だ。

サプライチェーン全体の管理必要に

また、これまでの10大脅威に一度もランクインしたことのない新たな脅威として「サプライチェーンの弱点を悪用した攻撃の高まり」が4位にランクインした。今日、社内で利用するITシステムやお客に提供する製品・サービスにおいて設計・開発・製造、および運用・保守・廃棄に至るまでのプロセスの一部を外部委託することは一般的となっている。しかし、これら供給の連鎖（サプライチェーン）における情報セキュリティーリスクの把握やマネジメントは容易ではない。セキュリティー対策が不十分な企業が侵害の契機となる恐れがあるため、サプライチェーン全体のセキュリティーマネジメントが求められる。

順位	組織の脅威
1（1）	標的型攻撃による被害
2（3）	ビジネスメール詐欺による被害
3（2）	ランサムウエアによる被害
4（−）	サプライチェーンの弱点を悪用した攻撃の高まり
5（8）	内部不正による情報漏えい
6（9）	サービス妨害攻撃によるサービスの停止
7（6）	インターネットサービスからの個人情報の窃取
8（7）	IoT機器の脆弱（ぜいじゃく）性の顕在化
9（4）	脆弱性対策情報の公開に伴う悪用増加
10（12）	不注意による情報漏えい

※カッコ内は前回の順位

今年は「個人」と「組織」を合わせた20の脅威のうち、9割の18の脅威が昨年に引き続きランクインした。このように大半の脅威は急に出現したものではなく、また新しい手口でもない。よって手口を知り、常に対策を怠らないことが重要と考えられる。

IPAでは、情報セキュリティー対策の基本として、①ソフトウエアの更新、②セキュリティーソフトの導入、③パスワード管理・認証の強化、④設定の見直し、⑤脅威・手口を知ること推奨している。企業規模にかかわらず実行することが可能な基本的な対策だが、10大脅威のさまざまな脅威に対して有効な対策であるため確実に実行していただきたい。

また、これら基本的な対策に取り組むことを宣言することでセキュリティ対策自己宣言制度「SECURITY ACTION」のロゴマークを使用することができる。ロゴマークは、ウェブサイトや名刺などに表示することで、情報セキュリティーに自ら取り組んでいることをアピールすることが可能だ。利用手数料は無料。具体的な手続きはIPAのホームページ（https://www.ipa.go.jp/security/security-action/）を確認してほしい。

（独立行政法人情報処理推進機構・江島将和）