中小企業のセキュリティー対策

—11—

組織を襲う10大脅威

人材不足がランクイン

独立行政法人情報処理推進機構（IPA）は、2017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100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。「情報セキュリティ10大脅威2018」として順位を決定し、IPAのホームページ（https://www.ipa.go.jp/security/vuln/10threats2018.html）で公表した。

今年の組織の脅威ランキングにはこれまでに一度もランクインしたことのない新たな脅威として「3位＝ビジネスメール詐欺」、「5位＝セキュリティー人材の不足」がランクインした。また、「4位＝脆弱（ぜいじゃく）性対策情報の公開に伴い公知となる脆弱性の悪用増加」は昨年のランク外（一昨年は6位）から復活ランクインしている。

「3位＝ビジネスメール詐欺」は、巧妙に細工したメールによるやりとりが行われ、その結果企業の担当者がだまされ、本来の振込口座とは異なる攻撃者の偽口座へ送金させる詐欺の手口である。昨年末に国内の大手企業の被害が大きく報道され、世間の耳目を集めた。この詐欺は、手口さえ知っていれば、だまされる前に気付ける可能性があった。

「5位＝セキュリティー人材の不足」は、以前から指摘されていた問題だ。他の脅威とはやや観点が異なるが、組織として取り組むべき課題の一つである。人材育成には時間がかかるため、数年先を見据えて計画的に進める必要があるだろう。

昨年、初めてランクインしたIoTに関する脅威は今年もランクインした。IoTはその利便性のみが注目されがちだが、Miraiを初めとしたウイルスがネットワークカメラなどのIoT機器を狙ったように、既に攻撃対象の一つになっているという認識を持ち、必要な対策を施した上で安全に利用していただきたい。

情報セキュリティ10大脅威2018

順位	組織の脅威	昨年順位
1位	標的型攻撃による情報流出	1位
2位	ランサムウエアによる被害	2位
3位	ビジネスメール詐欺	ランク外
4位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ランク外
5位	セキュリティー人材の不足	ランク外
6位	ウェブサービスからの個人情報の窃取	3位
7位	IoT機器の脆弱性の顕在化	8位
8位	内部不正による情報漏えい	5位
9位	サービス妨害攻撃によるサービスの停止	4位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	9位

手口を知り対策を怠らない

今年は「個人」と「組織」を合わせた20の脅威のうち、8割の16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。企業規模に係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-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）