IT Topics & News

「情報セキュリティ10大脅威 2021」を決定 「テレワーク等のニューノーマルな働き方を狙った攻撃」が3位に【IPA】

独立行政法人情報処理推進機構（略称＝IPA）は、2020年に発生した社会的に影響が大きかった情報セキュリティ上のトピックを「情報セキュリティ10大脅威2021」として1月27日に発表した。

情報セキュリティ分野の研究者、企業の実務担当者など約160名のメンバーからなる「10大脅威選考会」が、「個人」と「組織」向けの候補について審議・投票を行い決定される。

今回の発表では、「組織」の1位は昨年5位だった「ランサムウェアによる被害」となった。2020年8月にIPAは、ランサムウェアを用いた新たな攻撃の手口として「人手によるランサムウェア攻撃」と「二重の脅迫」について注意喚起を行っている。新たなランサムウェア攻撃は、標的型攻撃と同等の技術が駆使されるため、例えば、ウイルス対策、不正アクセス対策、脆弱性対策など、基本的な対策を、確実かつ多層的に適用することが重要となる。

「個人」の1位は昨年同様で「スマホ決済の不正利用」だった。近年のスマートフォンの普及に伴い、2018年頃よりキャッシュレス決済の一つであるスマートフォンを利用した決済（スマホ決済）が登場し、その後スマホ決

（図1）「情報セキュリティ10大脅威 2021」　NEW：初めてランクインした脅威

昨年順位	個　人	順位	組　織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗･中傷･デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫･詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

済を使った各社のサービスも登場し、その手軽さから普及が進んだ。一方、利便性の半面、第三者のなりすましによるサービスの不正利用や、連携する銀行口座からの不正な引き出し等も確認されている。

今回の結果で、「組織」にランクインした脅威を見ると、「テレワーク等のニューノーマルな働き方を狙った攻撃」が初登場で3位となった。2020年は新型コロナウイルス感染症の世界的な蔓延に伴い、感染症対策の一環として政府機関からテレワークが推奨されたが、テレワークへの移行に伴い、自宅などからVPN経由で社内システムにアクセスしたり、Web会議サービスを利用したりする機会が増加。また、私物PCや自宅ネットワークの利用、初めて使うソフトウェアの導入など、以前までは緊急用として使っていた仕組みを恒常的に使う必要性が出てきた。こうした業務環境の急激な変化を狙った攻撃が懸念されている。基本的な対策のほか、テレワークの規定や運用ルールの整備、セキュリティ教育の実施などが重要となる。

今回、10大脅威が発表されたが、上位の脅威だけ、または上位の脅威から優先して対策を行えばよいということではない。順位が高いか低いかに関わらず、自身または組織が置かれている立場や環境を考慮して優先度を付け、適切な対応を取る必要がある。また、かつてランクインしていた、「ワンクリック請求等の不当請求」や「ウェブサイトの改ざん」等は今回10大脅威に入っていないが、ランク外の脅威だから対策を行わなくて良いということではなく、継続しての対策が必要となる。とはいえ、これらが利用する「攻撃の糸口」は似通っており、脆弱性を悪用する、ウイルスを使う、ソーシャルエンジニアリングを使う等の古くからある基本的な手口が使われている。「ソフトウェアの更新」「セキュリティソフトの利用」などといった「情報セキュリティ対策の基本」（図2）を意識して、継続的に対策を行うことで、被害に遭う可能性を低減できるだろう。

（図2）情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する