

## 情報セキュリティ10大脅威2022

### 組織編

#### 1位 ランサムウェアによる被害 (昨年順位1位)

ランサムウェアとはウイルスの一種である。PCやサーバが感染すると、端末のロックや、データの暗号化が行われ、その復旧と引き換えに金銭を要求される。また、重要な情報が窃取されることもあり、社会的信用を失うおそれがある。さらに、復旧に時間がかかる場合、更なる経済的損失につながるおそれもある。

#### 2位 標的型攻撃による機密情報の窃取 (昨年順位2位)

標的型攻撃とは、特定の組織(官公庁、民間団体、企業等)を狙う攻撃のことであり、機密情報等を窃取することや業務妨害を目的としている。攻撃者は社会の変化や、働き方の変化に便乗し、状況に応じた巧みな攻撃手法で機密情報等を窃取しようとする。

#### 3位 サプライチェーンの弱点を悪用した攻撃 (昨年順位4位)

商品の企画・開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群をサプライチェーンと呼ぶ。このサプライチェーンの関係性を悪用し、セキュリティ対策の強固な企業を直接攻撃せずに、その企業が構成するサプライチェーンの中でセキュリティ対策が手薄な関連組織や利用サービスの脆弱性等を最初の標的とし、そこを踏み台として本命の標的である組織を攻撃する手口がある。関連組織に預けた情報が漏えいしたり、本来の標的である企業が攻撃を受けたりすることで被害が発生する。

#### 4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 (昨年順位3位)

2020年から続く新型コロナウイルス感染症(COVID-19)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がニューノーマルな働き方の1つであるテレワークを推奨している。勤労形態としてテレワークが活用され、ウェブ会議サービスやVPN等の本格的な活用がされる中、それらを狙った攻撃が行われている。

#### 5位 内部不正による情報漏えい (昨年順位6位)

組織に勤務する従業員や元従業員等の組織関係者による機密情報の持ち出しや悪用等の不正行為が発生している。また、組織内における情報管理のルールを守らずに情報を持ち出し、紛失や情報漏えいにつながるケースも散見される。組織関係者による不正行為は、組織の社会的信用の失墜、損害賠償による経済的損失により、組織に多大な損害を与える。また、不正に取得した情報を他組織に持ち込んだ場合、その組織も損害賠償等の対象になるおそれがある。

#### 6位 脆弱性対策情報の公開に伴う悪用増加 (昨年順位10位)

ソフトウェアや機器類の脆弱性対策情報の公開は、脆弱性の脅威や対策情報を製品の利用者に広く呼び掛けられるメリットがある。一方で、その情報を攻撃者に悪用され、当該製品に対する脆弱性対策を講じていないシステムを狙う攻撃が行われている。近年では脆弱性関連情報の公開後に攻撃コードが流通し、攻撃が本格化するまでの時間もますます短くなっている。

#### 7位 修正プログラムの公開前を狙う攻撃 (ゼロデイ攻撃) (初ランクイン)

ソフトウェアの脆弱性が発見され、脆弱性の修正プログラム(パッチ)や回避策が公開される前に脆弱性を悪用したサイバー攻撃が行われることがある。これをゼロデイ攻撃と呼ぶ。多くのシステムで利用されているソフトウェアに対してゼロデイ攻撃が行われると、社会が混乱に陥るおそれがある。

#### 8位 ビジネスメール詐欺による金銭被害 (昨年順位5位)

ビジネスメール詐欺(Business E-mail Compromise:BEC)は、巧妙な騙しの手口を駆使した偽のメールを組織・企業に送り付け、従業員を騙して送金取引に関わる資金を詐取する等の金銭被害をもたらすサイバー攻撃である。2021年も経営者になりました手口が引き続き確認されている。

#### 9位 予期せぬIT基盤の障害に伴う業務停止 (昨年順位7位)

組織が利用するサーバやインターネット上のサービス、業務システム等で使用しているネットワークやクラウドサービス等のIT基盤に予期せぬ障害が発生し、長時間にわたり利用者や従業員に対するサービスを提供できなくなるケースがある。こうしたIT基盤の停止はシステムの可用性を侵害する情報セキュリティリスクであり、IT基盤を利用している組織の事業に大きな影響を与えるおそれがある。

#### 10位 不注意による情報漏えい等の被害 (昨年順位9位)

組織で取り扱う重要情報について、組織の規定の不備や情報を扱う従業員に対する情報リテラシー教育の不足、不注意・ミスによって引き起こされる情報漏えいが後を絶たない。漏えいした情報が悪用され、他の脅威を誘発してしまうおそれがある。また、組織の社会的信用の失墜や、経済的な損失につながる可能性がある。

出典：IPA(独立行政法人情報処理推進機構)「情報セキュリティ10大脅威2022」<https://www.ipa.go.jp/security/vuln/10threats2022.html>

異常を検知すれば、警察へ速報をお願いします

京都府中京警察署警備課

TEL:075-823-0110(内線483)



千年を守る 未来を創る