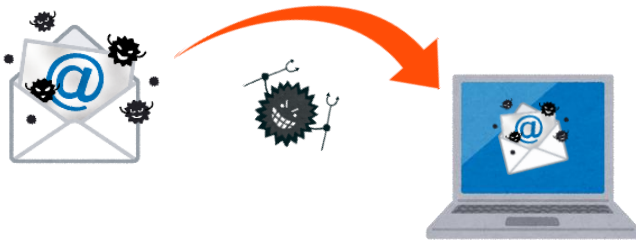


「情報セキュリティ10大脅威2020」 (組織) 1位 標的型攻撃による機密情報の窃取

IPA（情報処理推進機構）が公開している「情報セキュリティ10大脅威2020」の中で、「組織」の視点からは、2016年から5年連続で、

「**標的型攻撃による機密情報の窃取**」が脅威の1位として選出されています。

攻撃者（犯人）はメールの添付ファイルや悪意のあるウェブサイトを利用し、組織のPCをウイルスに感染させた後、組織内部のネットワーク等に侵害範囲を拡大しながら機密情報を窃取します。



順位	組織	昨年順位
1位	標的型攻撃による機密情報の窃取	1位
2位	内部不正による情報漏えい	5位
3位	ビジネスメール詐欺による金銭被害	2位
4位	サプライチェーンの弱点を悪用した攻撃	4位
5位	ランサムウェアによる被害	3位
6位	予期せぬIT基盤の障害に伴う業務停止	16位
7位	不注意による情報漏えい(規則は遵守)	10位
8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
9位	IoT機器の不正利用	8位
10位	サービス妨害攻撃によるサービスの停止	6位

【 攻撃手口 】

ウイルスに感染させて 機密情報を窃取

- メールを利用した手口
 - ・ 不正な添付ファイルを開かせる
 - ・ 不正なウェブサイトへのリンクをクリックさせる
 - ・ 多くはOffice文書ファイルを悪用
本文や件名、添付ファイル名は業務に関連するような内容に偽装され、実在する組織の差出人名が使われる場合もあります。

- ウェブサイトを利用した手口
 - ・ 標的組織が頻繁に利用するウェブサイトを調査し、当該サイトを閲覧するとウイルスに感染するように改ざんする。

不正アクセスによって 機密情報を窃取

組織が利用するメールのクラウドサービスやウェブサーバーへ不正アクセスし、認証情報等を窃取します。そして窃取した情報を利用し、社内システムの利用等に用いる正規のアクセス経路で組織内部へ潜入し、組織内部のPCやサーバーをウイルスに感染させます。



(IPA「情報セキュリティ10大脅威2020」を基に作成)

「情報セキュリティ10大脅威 2020」の詳細については、下記ウェブサイトで開催されています。

<https://www.ipa.go.jp/security/vuln/10threats2020.html>

対策／対応

【経営者層】

- **組織としての体制の確立**
 - ①迅速かつ継続的に対応できる体制の構築
 - ②対策予算の確保と継続的な対策の実施
 - ③セキュリティポリシーの策定

【セキュリティ担当者】

- **被害の予防／対応力の向上**
 - ①情報の管理とルール策定
 - ②サイバー攻撃に関する継続的な情報収集と情報共有
 - ③セキュリティ教育の実施
 - ④インシデント発生時の訓練の実施
 - ⑤統合運用管理ツール等によるセキュリティ対策状況の把握
 - ⑥取引先のセキュリティ対策実施状況の確認
- **被害を受けた後の対応**
 - ①組織内の体制（CSIRT（※1）等）の運用
 - ②影響調査および原因の追究,対策の強化



【システム管理者】

- **被害の予防（BCP（※2）対策含む）**
 - ①セキュアなシステム設計
 - ②重要サーバーの要塞化（アクセス制御、データの暗号化等）
 - ③ネットワーク分離
 - ④バックアップの取得
- **被害の早期検知**
 - ①ネットワーク監視、防御
 - ②エンドポイントの監視、防御
- **被害を受けた後の対応**
 - ①バックアップから復旧



【従業員・職員】

- **情報リテラシーの向上**
 - ①セキュリティ教育の受講
- **被害の予防**
 - ①「情報セキュリティ対策の基本」（※3）を実施
- **被害を受けた後の対応**
 - ①CSIRTへの連絡



CSIRT（※1）…企業や行政機関などの組織内に設置され、コンピュータシステムやインターネットなどのネットワークに保安上の問題や事故が生じた際に対応する専門チームのこと。

BCP（※2）…企業が自然災害などの緊急事態に遭遇した場合において、業務中断に伴うリスクを最低限にするために、平素から事業継続について戦略的に準備しておく計画のこと。

「情報セキュリティ対策の基本」（※3）

攻撃の系口	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（畏にはめる）	脅威・手口を知る	手口から重要視すべき対策を理解する