

情報セキュリティ10大脅威

順位	「組織」向け脅威
1	ランサム攻撃による被害
2	サプライチェーンや委託先を狙った攻撃
3	システムの脆弱性を突いた攻撃
4	内部不正による情報漏えい等
5	機密情報を狙った標的型攻撃
6	リモートワーク等の環境や仕組みを狙った攻撃
7	地政学リスクに起因するサイバー攻撃
8	分散型サービス妨害攻撃（DDoS攻撃）
9	ビジネスメール詐欺
10	不注意による情報漏えい等

- IPA（独立行政法人 情報処理推進機構）では毎年、前年度に発生した社会的に影響が大きかった事案から、「**情報セキュリティ10大脅威**」を決定し、発表しています。
- 2025年に発表された「組織」に対する10大脅威は、左表の通りです。
- 今回は、このうち大半をしめる黄色に塗った項目に関連する「**サイバー攻撃**」について説明します。

IPA（独立行政法人 情報処理推進機構）の「情報セキュリティ10大脅威 2025」

<https://www.ipa.go.jp/security/10threats/10threats2025.html>

情報セキュリティ教材動画「華麗なる情報セキュリティ対策」も参考にしてください。

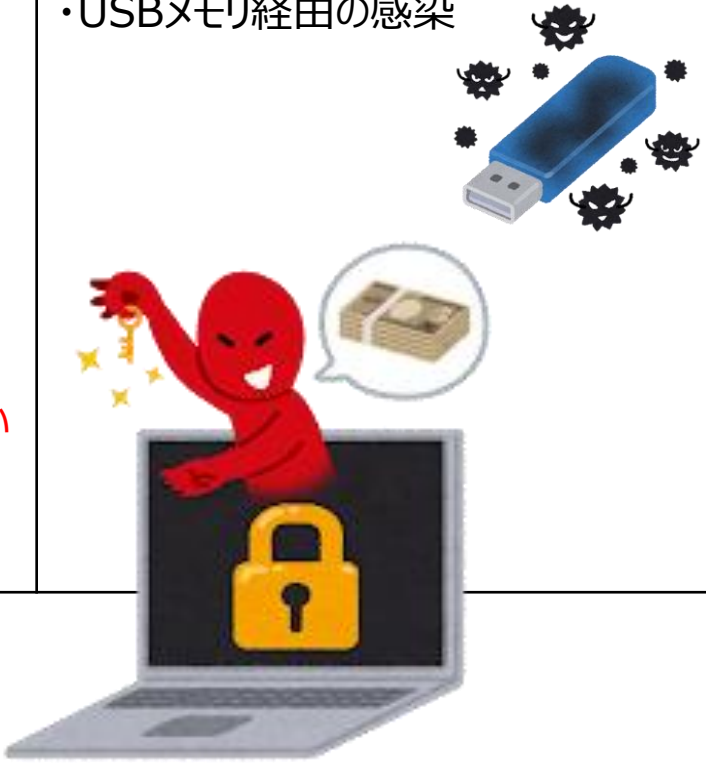
https://www.youtube.com/playlist?list=PLi57U_f9scIJJPYjMPHEFq7swlnhwOFsb

サイバー攻撃とは？

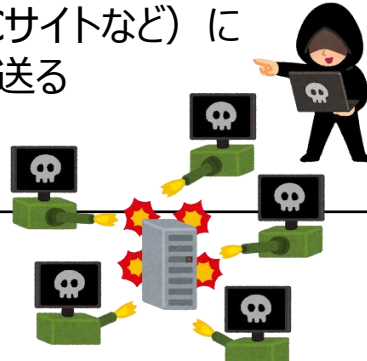
- 「サイバー攻撃」とは、インターネットやネットワークを通じて、企業や個人の情報を盗んだり、業務を妨害したりする行為です。
 - 印刷業界は、顧客情報や製版・印刷データなど、大量の重要情報を扱うため、サイバー攻撃のターゲットになっています。
 - また印刷会社は、多くの顧客と取引があるため、攻撃を受けるとその影響範囲が大きいです。
 - サイバー攻撃の代表的なものは、a) マルウェア/ランサムウェア、b) フィッシング、c) DDoS攻撃 です。
- これらについて、簡単に説明します。



サイバー攻撃とは？

	種類	説明	攻撃の手口
a	マルウェア/ ランサムウェア	・ウイルスやランサムウェアなど、悪意のあるソフトウェアを使って、PC、サーバー、保存されているデータを攻撃する ・ランサムウェアは、データを暗号化したり、公開すると脅して身代金を要求する 【実例】 ・名古屋港のコンテナターミナルシステム停止 ⇒システムの一部が、最新のセキュリティアップデートを適用していなかったことが一因とされている ・大阪の総合医療センターの電子カルテシステム停止 ⇒給食事業者のパスワードが推測されやすいものだったことが、被害拡大の一因とされている ※詳しくは、以下のページを参照 https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf	・メールの添付ファイルから ・偽サイトからの自動ダウンロード ・ネットワークおよび接続されている機器のセキュリティが弱い部分から侵入 ・USBメモリ経由の感染 

サイバー攻撃とは？

	種類	説明	攻撃の手口
b	フィッシング	・偽のメールやサイトで、IDやパスワードを盗んで悪用する 【実例】 ・証券会社に登録してあるID・パスワードを盗んで勝手に取引 ⇒不審なメールやサイトを見抜けなかった、多要素認証を採用していなかった等が要因とされている	・正規の会社や団体を装った偽メールや偽サイト ・正規のサービスを装った偽サービス 
c	DDoS攻撃 (ディードスこうげき)	・複数のPCやネットワーク機器から、標的のシステムやネットワークに対して大量のアクセスを送り、サービスを停止させる ・あなたの会社のインターネットサービスが狙われる可能性も ・あなたの会社のネットワーク機器が操作されて、攻撃に使われる可能性も 【実例】 ・航空会社、銀行、携帯電話会社のシステム障害によるサービス停止	・マルウェアを使って多数のPCを感染させる ・ID・パスワードが初期設定のネットワーク機器を乗っ取る ・これらのPCや機器を遠隔操作可能にして、標的のシステム（サービス、ホームページ、ECサイトなど）に大量のアクセスを送る 

一人ひとりができる対策

- ・メールやウェブサイトのURLを安易にクリックしない

⇒「[フィッシングメールに注意！](#)」※（※ 詳細は、[青字タイトルのコンテンツを参照](#)）

- ・パスワードを適切に管理する：初期設定のままにしない、

推測可能なパスワードを使わない、使いまわさない

⇒「[パスワードは長く複雑に](#)」

- ・PCのOSやソフトを常に最新にしておく

⇒「[ソフトウェアは最新に！](#)」

- ・常日頃、セキュリティ意識を持った行動をする：

出所が信頼できないソフトはインストールしない ⇒「[アプリは公式サイトから](#)」

管理していないUSBメモリはPCにつながない ⇒「[そのUSBメモリは大丈夫？](#)」

業務でフリーWi-Fiを使用しない ⇒「[危険なフリーWi-Fi](#)」

- ・困ったときは、すぐに上司や情報システム部門に相談する

