情報セキュリティ10大脅威とその対策

サイバーセキュリティセミナー 2025

2025年02月18日

情報処理推進機構 (IPA)
セキュリティセンター
篠塚　耕一

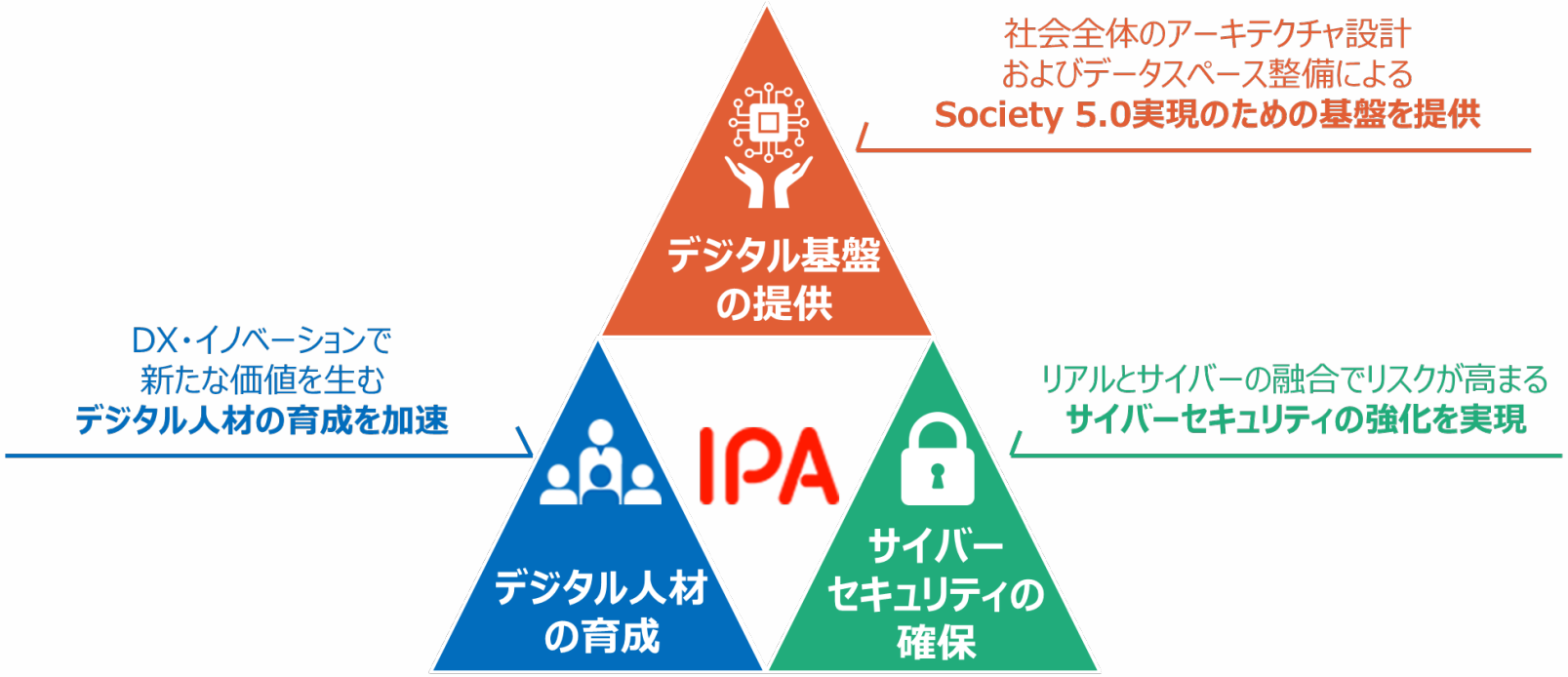
IPA Better Life with IT

アジェンダ

独立行政法人情報処理推進機構（IPA）について

日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人。
誰もが安心してITのメリットを実感できる「**頼れるIT社会**」の実現を目指しています。

「**人材**」、「**セキュリティ**」、「**デジタル基盤**」の3つの中核事業



■ **名称: 独立行政法人情報処理推進機構**
(Information-technology Promotion Agency, Japan)
■ **設立: 2004年1月5日**
（前身母体の設立は1970年10月1日）
■ **理事長: 齊藤 裕**

IPAの組織の紹介

情報処理推進機構(IPA)

- 理事長
- 理事【２名】
- 監事

セキュリティセンター（ISEC）
設立：1997年1月
サイバーセキュリティ全般

産業サイバーセキュリティセンター（ICSCoE）
設立：2017年4月
産業サイバーセキュリティ人材育成、サイバー事故原因究明、サイバー技術研究の調査・分析　など

デジタル人材センター（DHRC）
設立：2008年11月
情報処理安全確保支援士、情報セキュリティマネジメント試験　など

サイバーセキュリティに関わる事業

デジタルアーキテクチャ・デザインセンター（DADC）
設立：2020年５月
セキュリティアーキテクチャで連携

デジタル基盤センター（DISC）
設立：2023年７月

AIセーフティ・インスティテュート（J-AISI）※
設立：2024年２月
※デジタル基盤センターが事務を行う特別の組織
AIセキュリティで連携

サイバーセキュリティに関する業務概要

■ 平時からインシデント発生時まで、サイバーセキュリティのマネジメントからオペレーションまでトータルな施策・対応を実施。

リテラシー向上

- 情報セキュリティ10大脅威、情報セキュリティ白書
- 経営者向け、社内セキュリティ担当者向けの各種ガイドライン
- 従業員教育コンテンツ（動画教材など）
- 地域・中小企業支援
- 情報セキュリティ安心相談窓口
  10,923件（2023年）

サイバーセキュリティCSお助け隊

SECURITY ACTION ★ セキュリティ対策自己宣言

累計宣言数
約30万者
（2023年10月）

オペレーション（検知・分析・対処調整）

- 情報共有枠組
  （サイバー攻撃情報・脆弱性）
- 国家支援型サイバー攻撃対策
- サイバー事故原因究明
- サイバー情勢分析
- セキュリティ監視（独法等）

JVN iPedia
脆弱性データベース
約20万件登録（2024年3月）

J-CSIP Initiative for Cyber Security Information sharing Partnership of Japan

IPA J-CRAT
2011年創立　341件支援（2023年）

セキュリティ基準・評価認証

＜製品・サービスのセキュリティ評価・認証＞

- IoT製品セキュリティラベリング（JC-STAR）
- クラウドサービスセキュリティ評価（ISMAP）

JC-STAR

＜セキュリティ基準・分析・監査等＞

- 制御システムセキュリティリスク分析
- サプライチェーンセキュリティ評価
- 独法等情報セキュリティ監査、政府システム監査

人材育成

- 中核人材育成プログラム
  累計435名受講（2017年～）
- 若手人材発掘（セキュリティ・キャンプ）
  累計1,073名受講（2004年度～）
- 国家資格「情報処理安全確保支援士」
  登録者数21,727名（2023年10月1日時点）
- 情報セキュリティコンクール
  応募約５万点（2023年度）

サイバーセキュリティ関連業務の全体像（対策フロー別）

- サイバーセキュリティのマネジメントからオペレーションまでトータルな施策・対応を実施※

①国家・経済の安全保障に貢献し、②誰も取り残さず、③組織・個人自らのサイバーセキュリティ対策をサポート

識別

- 自社診断ツール
- リスク分析シート
- 制御システム・リスクアセスメント
- ウェブ簡易チェック（自治体や重要イベント関係先等）

防御

- IT製品セキュリティ評価・認証(JISEC)
- IoT製品セキュリティラベリング(JC-STAR)
- 暗号モジュール試験・認証(JCMVP)
- CRYPTREC(電子政府推奨)暗号リスト
- 脆弱性対策情報DB(JVN iPedia)
- 安全なウェブサイトの作り方
- セキュリティ啓発コンクール
- セキュリティ・キャンプ
- 中核人材育成プログラム / 短期プログラム
- インド太平洋地域向け日米EU産業制御システムサイバーセキュリティウィーク
- 脆弱性情報届出制度
- 脆弱性情報優先提供

検知

- 標的型攻撃特定・分析(J-CRAT)
- 情報共有枠組(J-CSIP)
- ウイルス・不正アクセス届出
- 注意喚起発信(各種メディア活用)
- お助け隊サービス制度
- セキュリティ監視(独法等)
- ウェブ脆弱性監視（政府要請主体）

対応

- 初動対応支援(J-CRAT)
- サイバーインシデントに関する原因究明調査
- 情報セキュリティ安心相談窓口
- お助け隊サービス制度（駆付支援、サイバー保険）
- 重要イベント対処調整支援
- 重大事象の原因究明調査

復旧

統治

- 経営/中小ガイドライン
- 内部不正防止ガイドライン
- ECサイト構築・運用セキュリティガイドライン
- セキュリティ自己宣言制度
- クラウドサービスセキュリティ評価 (ISMAP)
- 独法等情報セキュリティ監査
- 政府機関システム監査

サイバー情勢研究・分析
情報セキュリティ10大脅威、情報セキュリティ白書
情報処理安全確保支援士制度、セキュリティプレゼンター制度
シン・テレワークシステム/自治体テレワークシステム for LGWAN

※ 世界で利用されている米国国立標準技術研究所(NIST)のセキュリティ対策検討・推進フレームワーク、「サイバーセキュリティフレームワーク2.0」の考え方を参考にしたサイバーセキュリティ支援サービスを提供

１．情報セキュリティ10大脅威とは

「情報セキュリティ10大脅威」とは？

- IPAが2006年から毎年発行している情報セキュリティについての啓発資料
- 前年に発生したセキュリティ事故やサイバー攻撃の状況等から
  IPAが10大脅威の候補になる脅威を選出
- セキュリティの専門家や企業のシステム担当者等から構成される
  「10大脅威選考会」が脅威の候補に投票
- **TOP10入りした脅威を「10大脅威」**として
  脅威の概要、脅威の手口、被害事例、対策方法等を解説

２つの「10大脅威」

様々な脅威が存在する

情報を扱う立場によって注意するべき脅威も異なる

- 企業や政府機関等の組織
- 組織のシステム管理者や社員・職員

「組織」

- 家庭等でパソコンやスマホを利用する人

「個人」

「組織」と「個人」の２つの立場から脅威を解説

情報セキュリティ10大脅威 2025 組織編

順位	「組織」向け脅威	初選出年	選出状況(2016年～)
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

組織編はランキング形式だが…
順位に囚われずに自組織に合わせた対策の実施を

近隣諸国から攻撃等の影響を考えて**新設**

年末の**DDoS攻撃**の**影響**等もあるためランクイン

情報セキュリティ10大脅威 2025 個人編

「個人」向け脅威（五十音順）	初選出年	選出状況(2016年～)
フィッシングによる個人情報等の窃取	2019年	7年連続7回目
ワンクリック請求等の不当請求による金銭被害	2016年	3年連続5回目
偽警告によるインターネット詐欺	2020年	6年連続6回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	7年連続7回目
不正アプリによるスマートフォン利用者への被害	2016年	10年連続10回目
インターネット上のサービスへの不正ログイン	2016年	10年連続10回目
インターネット上のサービスからの個人情報の窃取	2020年	6年連続9回目
クレジットカード情報の不正利用	2016年	10年連続10回目
スマホ決済の不正利用	2016年	6年連続6回目
ネット上の誹謗・中傷・デマ	2016年	10年連続10回目

2024年から個人編では「順位」を撤廃
※順位に囚われず、
自身に関係のある脅威に
対して対策の実施を

常連の脅威ばかり。
つまり、よくある手口に
引っ掛かる人が後を絶たない。
手口を知り、基本的な対策を行うことが重要

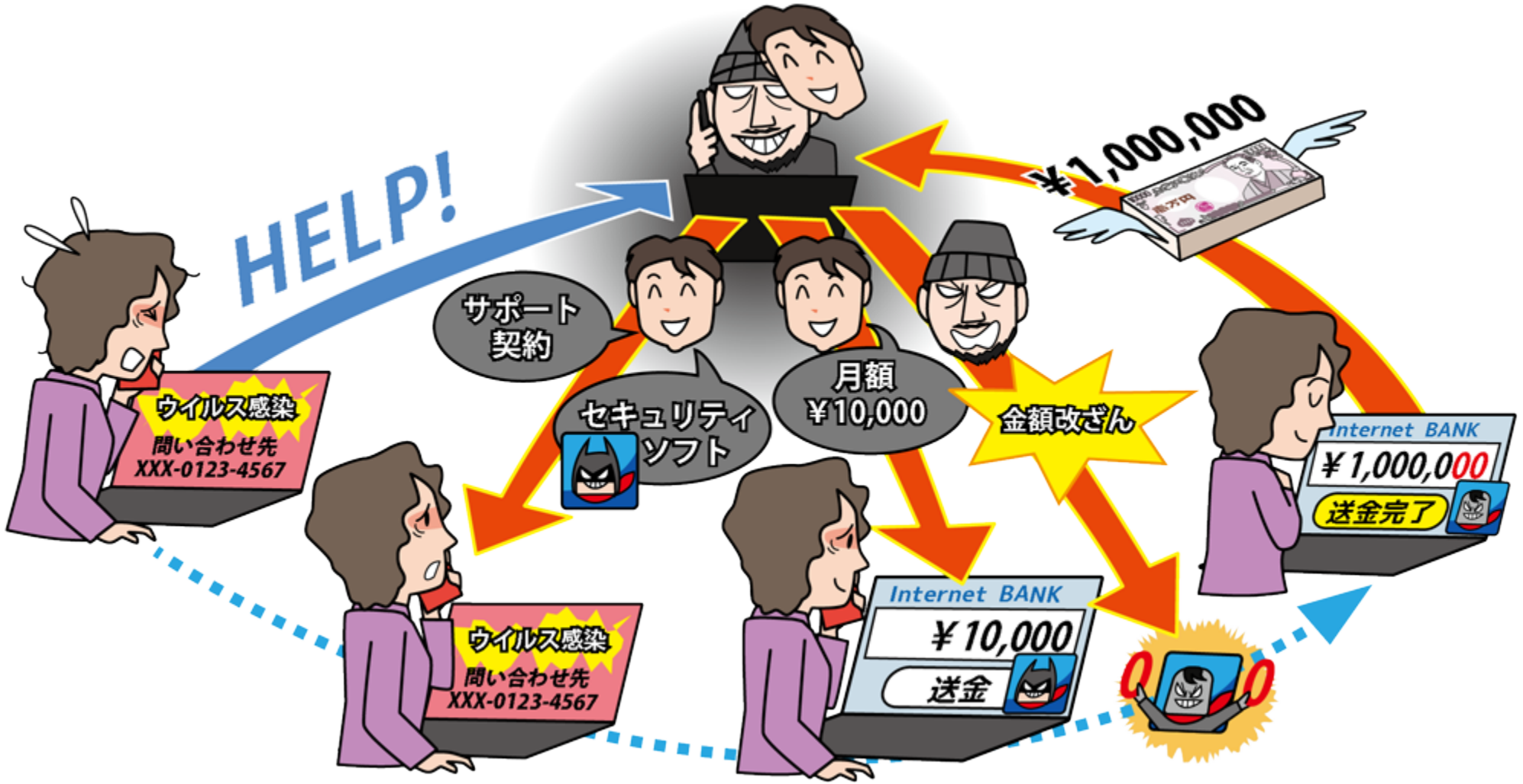
情報セキュリティ10大脅威 2025 個人編

脅威名	脅威の特徴１ 悪意のある人間に騙されてしまう	脅威の特徴２ システムの弱点が突かれてしまう	脅威の特徴３ 自分が加害者になるおそれもある
フィッシングによる個人情報等の詐取	○	×	×
ワンクリック請求等の不当請求による金銭被害	○	×	×
偽警告によるインターネット詐欺	○	×	×
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	○	×	×
不正アプリによるスマートフォン利用者への被害	○	×	×
インターネット上のサービスへの不正ログイン	△	○	×
インターネット上のサービスからの個人情報の窃取	△	○	×
クレジットカード情報の不正利用	△	○	×
スマホ決済の不正利用	△	○	×
ネット上の誹謗・中傷・デマ	△	×	○

2．脅威の紹介

- 悪意のある人間に騙されてしまう脅威
- システムの弱点が突かれてしまう脅威
- 自分が加害者になるおそれもある脅威

悪意のある人間に騙されてしまう脅威



【概要】悪意のある人間に騙されてしまう脅威

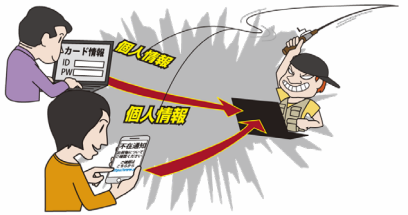
- **どんな脅威があるのか？**
  - **Webサイト**を利用した詐欺
    - **フィッシング詐欺**
    - **ワンクリック詐欺**
    - **偽警告(サポート詐欺)**
  - **メール**や**電話**や**SNS**を利用した脅迫・詐欺
  - **不正アプリ**を利用した情報や金銭の窃取

※騙されないために、まずは**手口を知ること。**
その上で**必要な対策**を打つ。

- **どんな問題が起きるの？**
  - **クレジットカード情報**などを含む**個人情報**を**窃取**されてしまう
  - **不正送金**や**物品の購入**をされたり、**脅迫**されて**金銭**を支払ってしまったりする

【手口】フィッシング詐欺

- **フィッシング(Phishing)詐欺とは？**
  - **正規のWebサイトに似せた偽のWebサイト(フィッシングサイト)**を使い、ユーザに**個人情報等**を**入力**させ、その情報を**窃取**する行為
  - 「洗練された(so**phi**sticated)」と「魚釣り(fi**shing**)」を組み合わせた造語
    ※犯罪者が**個人情報**を**釣り上げる**イメージ



- **フィッシング詐欺に引っかかるとどうなるのか？**
  - 利用しているインターネットサービスの**IDとパスワード**が**盗まれ**、**不正アクセス**される
- **フィッシングサイトへ誘導する手口には、どんなものがあるのか？**
  - **Web広告**にフィッシングサイトへのリンクを埋め込む
  - フィッシングサイトへのリンクが記載されたメール(**フィッシングメール**)やSMSを送付する
  - **SNSで交流**し、**チャット等**でリンクをクリックさせる

【事例】フィッシング詐欺

どんな事例があるの？

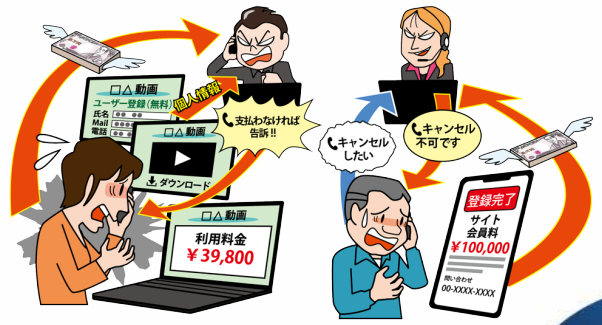
- 2024年5月、フィッシング対策協議会は**国税庁を騙るフィッシング**が増えているため、注意喚起を行った
- 手口としては、「**税務署からのお知らせ**」等のタイトルのメールが届き、メールには、本文に書かれた**リンク**を**クリック**させるようになっていた
- そのリンクをクリックしてしまうと、**フィッシングサイト**が表示され、名前や住所などの個人情報や、クレジットカード情報等の入力を要求される
- フィッシング対策協議会は、フィッシングサイトに**情報**を**入力しない**ように呼び掛けている

【出典】
国税庁をかたるフィッシング （2024/05/22）（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/nta_20240522.html

【手口】ワンクリック詐欺

- **ワンクリック詐欺とは？**
  - Webサイトを閲覧しているユーザが**リンクをクリックする等**のことをした際に、**有料サービス**の**会員登録完了画面**等が表示される。その画面(**ワンクリックサイト**)には会員料金等の振込先と**問い合わせ電話番号**が書かれている。
  - その電話番号に連絡すると、**「契約は解除できない」**と言われ、**金銭**の**支払い**を**迫られる**という詐欺である

- **ワンクリックサイトへ誘導する手口には、どんなものがあるのか？**
  - **アダルトサイト**や**出会い系サイト等**の**広告**をクリックさせる
  - **メール**や**SMS**にワンクリックサイトの**リンクを記載**しクリックさせる
  - **SNSで交流**し、**チャット等**でリンクをクリックさせる



【事例】ワンクリック詐欺

どんな事例があるの？

- 2024年2月、東京都の青少年がスマートフォンでゲーム関連サイトを見ていた時に**広告**を**タップ**してしまい、**アダルトサイト**を開いてしまった
- そのアダルトサイトで18歳以上か年齢確認をされた際には「はい」を選んだ
- 「**登録ありがとうございます**」という**金銭**を**請求**される画面が表示された
- 青少年は**ワンクリックサイト**のことを**知っていた**ため、そのまま**画面**を**閉じた**
- サイト側にはメールも電話もしていないが個人情報が漏れていないか心配になったため、東京都都民安全推進部に相談したことで、問題が発覚した

【出典】
相談事例「架空請求」 | こどものネット・スマホのトラブル相談！こたエール（東京都都民安全推進部）
https://www.tokyohelpdesk.metro.tokyo.lg.jp/consult/jirei/kakuu.html

【手口】偽警告(サポート詐欺)(1/2)

- **偽警告とサポート詐欺とは？**

偽警告の特徴の例

画面を閉じるための
×ボタンが無くて閉じれない

ウィルス検知画面

慌てさせる文言

心配になるような
色や演出

以下のWebサイトからご自身のPCで、体験できます
【出典】偽セキュリティ警告（サポート詐欺）対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

偽のサポート窓口
への誘導

他にも・・・
警告音がなったり、
するケースもある

【手口】偽警告(サポート詐欺)(2/2)

- **電話番号に連絡するとどうなるのか？**
  - ウイルス駆除の**サポートをすると持ち掛けられ**(**サポート詐欺**)、**リモート操作アプリ**を**インストール**させられる
- **サポート詐欺を受けるとどうなるのか？**
  - 攻撃者は電話をしながら被害者のPCに**リモートログイン**して、以下のことをする
    - **個人情報**を**窃取**する
    - インターネットバンキング等の**暗証番号**を聞き出し、そのサイトに**ログイン**し、**金銭を振り込む**
  - サポート作業が完了すると以下のことを要求する
    - **法外**な**サポート費用**
    - **セキュリティソフトウェア**の**購入**

【事例】偽警告(サポート詐欺)

どんな事例があるの？

- 2024年3月、Y市の施設の管理業務を委託している組織の職員がPCを操作した際に、**ウイルス感染した**という内容の表示があった
- この職員は表示された電話番号に**電話**をして**指示通り**に**対応**し、電話対応している際に**約32万円**を支払ってしまった
- 翌日の朝に別の職員が当該PCの電源を入れた後に、**遠隔操作**が行われていると思われる画面が表示されたことで異常が発覚した
- 当該PCには深層水脱塩施設利用者の**登録情報約1万5000件**が保存されており、それらが**流出**したおそれがあるため、調査をしているとのことである

【出典】
委託先がサポート詐欺被害、個人情報流出のおそれも - 焼津市（Security NEXT）
https://www.security-next.com/155008
焼津市、深層水の購入者1万5000人の個人情報漏えいか　原因は「サポート詐欺」（ITMedia NEWS）
https://www.itmedia.co.jp/news/articles/2403/21/news164.html

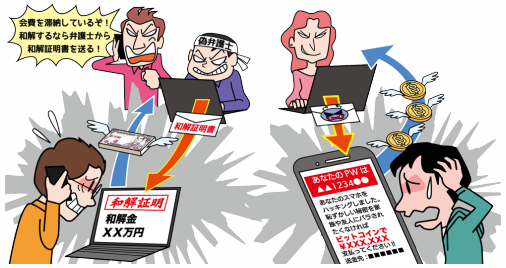
【対策】Webサイトを利用した詐欺

どんな対策があるのか？

- 所持している端末に**Webフィルタリングソフト**を**導入**する
  ※フィッシングサイト等の**不正なWebサイト**に**アクセスできない**ようにする
- ワンクリックサイトや偽警告画面が表示された場合は全て**無視**、または**画面を閉じる**
- ワンクリックサイトや偽警告画面に記載された電話番号には**電話しない**
  ※誤って電話をしても、**詐欺**に**気付いたならば**、そのタイミングで**電話**を**切る**
- 偽警告画面が**全画面表示**で×ボタンが押せない場合は、**ESCキー長押し**で**解除**する
- メールやSNSを利用した詐欺への対策は、P26を参照すること
- サポート詐欺をされている際にリモート操作アプリのダウンロードを
  させられそうになった場合の対策は、P30を参照すること

【手口】メールや電話やSNS等を使った脅迫・詐欺

- **どんな手口があるのか？**
  - メールやSMSや電話で、未払いの料金がある等と**嘘の請求**(**架空請求**)をする
    ※こちらが電話をすると、**社会的**な**信用**のある**公的機関**や**弁護士**等を名乗って**脅す**
  - あらかじめ標的の人のIDとパスワードをを入手しておき、**IDとパスワード**を**記載**した**メール**を**送信**することで、**PC**を**ハッキングした**と**思わせて脅迫**する
  - **SNS**で**親交**を**深める**
    - **恋愛感情**に**付け込んで**金銭の振り込みや投資の勧誘をする(**ロマンス詐欺**)
    - チャット等で**性的**な**ビデオ動画**を**撮影する**等した後に、
      その**動画を公開**する等と脅迫する(**セクストーション**)
    - **チャット**にフィッシングサイトやワンクリックサイトの**リンク**を記載してクリックさせる
  - フィッシングサイト等の**リンク**を記載した**メール**や**SMS**を送信する



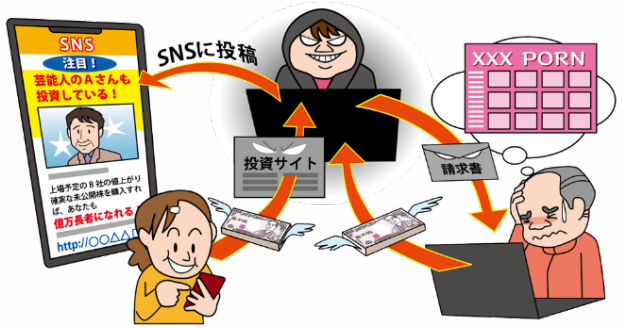
【事例】メールや電話やSNS等を使った脅迫・詐欺

- **どんな事例があるの？**
  - 2024年7月、小松市の60代の男性が**SNS**の通信アプリで女性を名乗る人物から、**金(ゴールド)**の**投資話**を持ち掛けられた
  - 8月からは指示されたアプリで投資を始め、**2か月間**で**26回**にわたり**合計約2億2400万円**を指定の口座に**送金**した。
  - その後、相手から「アカウントが疑われて**現金**の**引き出し**が**停止**されました。**解除**するには**3000万円**が**必要**です」というメッセージが届いたため、男性は**警察**に**相談**して詐欺に気付いた
  - 警察はSNSでやり取りを重ねる中で、**親近感**や**恋愛感情**を抱かせて**金銭**をだまし取る「**SNS型ロマンス詐欺**」とみて捜査している

【出典】
SNS型ロマンス詐欺か 石川 小松 60代男性 約2億2400万円の被害（NHK NEWS）
https://www3.nhk.or.jp/news/html/20241025/k10014619421000.html

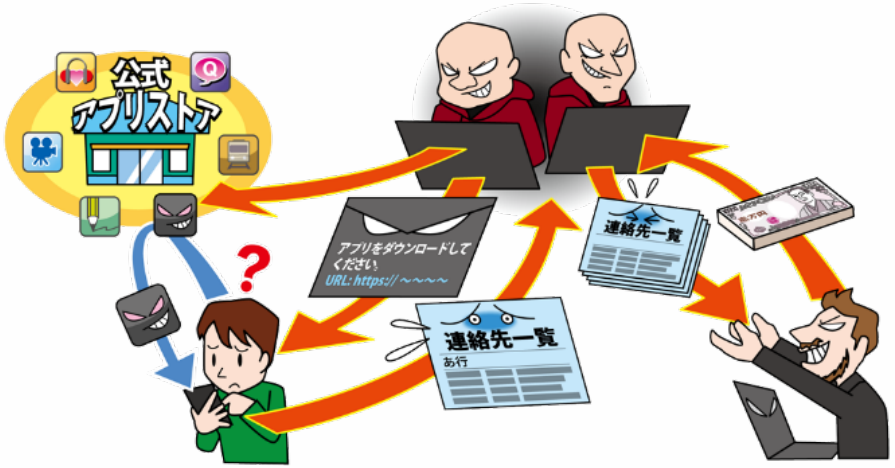
【対策】メールや電話やSNS等を使った脅迫・詐欺

- **どんな対策があるのか？**
  - 迷惑メールフィルターを利用する
  - 基本的に詐欺まがいのメールやSMSや電話は**全て無視**する
  - **メール**や**SNS**の**チャット**に記載されている**リンク**は**安易**に**クリックしない**
  - **メール**に記載されている**電話番号**には**直接電話しない**
  - **メール**の**送信元**の**アドレス**や**電話番号**は、**Web検索**して**問題がないか**を確認する
  - 自分が利用しているサービスのIDとパスワードが記載されたメール等を受信した場合、そのサービスの**IDとパスワードを変更**する　※少なくとも**パスワード**は**必ず変更する**
  - **SNS**の交流相手が金銭や投資の話を始めた場合、**それ以降**の**連絡**を**絶つ**



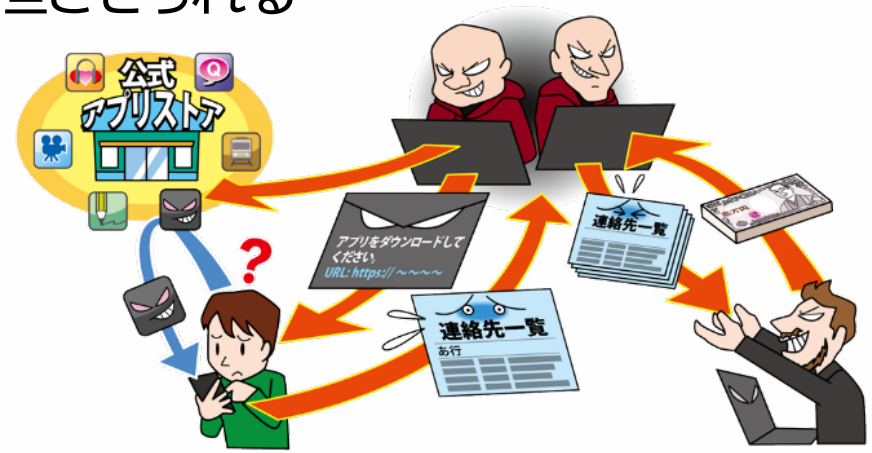
【手口】不正アプリを利用した攻撃(1/2)

- **どんな手口があるのか？**
  - **不正アプリ**の**ダウンロードサイト**に誘導する
    - **Webサイトの広告**や**偽警告**の**リンク**をクリックさせる
    - 送信した**メール**や**SMS**に記載されたダウンロードサイトの**リンク**をクリックさせる
    - **SNS**で**交流**し、**チャット**に記載したダウンロードサイトの**リンク**をクリックさせる
  - **公式マーケット**に**不正アプリ**を**紛れ込ませて**、**ダウンロード**させる



【手口】不正アプリを利用した攻撃(2/2)

- **不正アプリをインストールするとどうなるのか？**
  - **インストール時**に**個人情報窃取**や**金銭振り込み**を行う
  - インストール時は何もしないが、**アプリ**の**アップデート後**に**不正行為**を行う
  - **ワンクリックサイトのような画面**をPCやスマートフォンに**表示**して金銭を振り込ませようとする
  - PCやスマートフォンが以下のサイバー攻撃に加担させられる
    - **フィッシングメール**の送信
    - **仮想通貨**の**マイニング**
    - **DDoS攻撃**



【事例】不正アプリを利用した攻撃

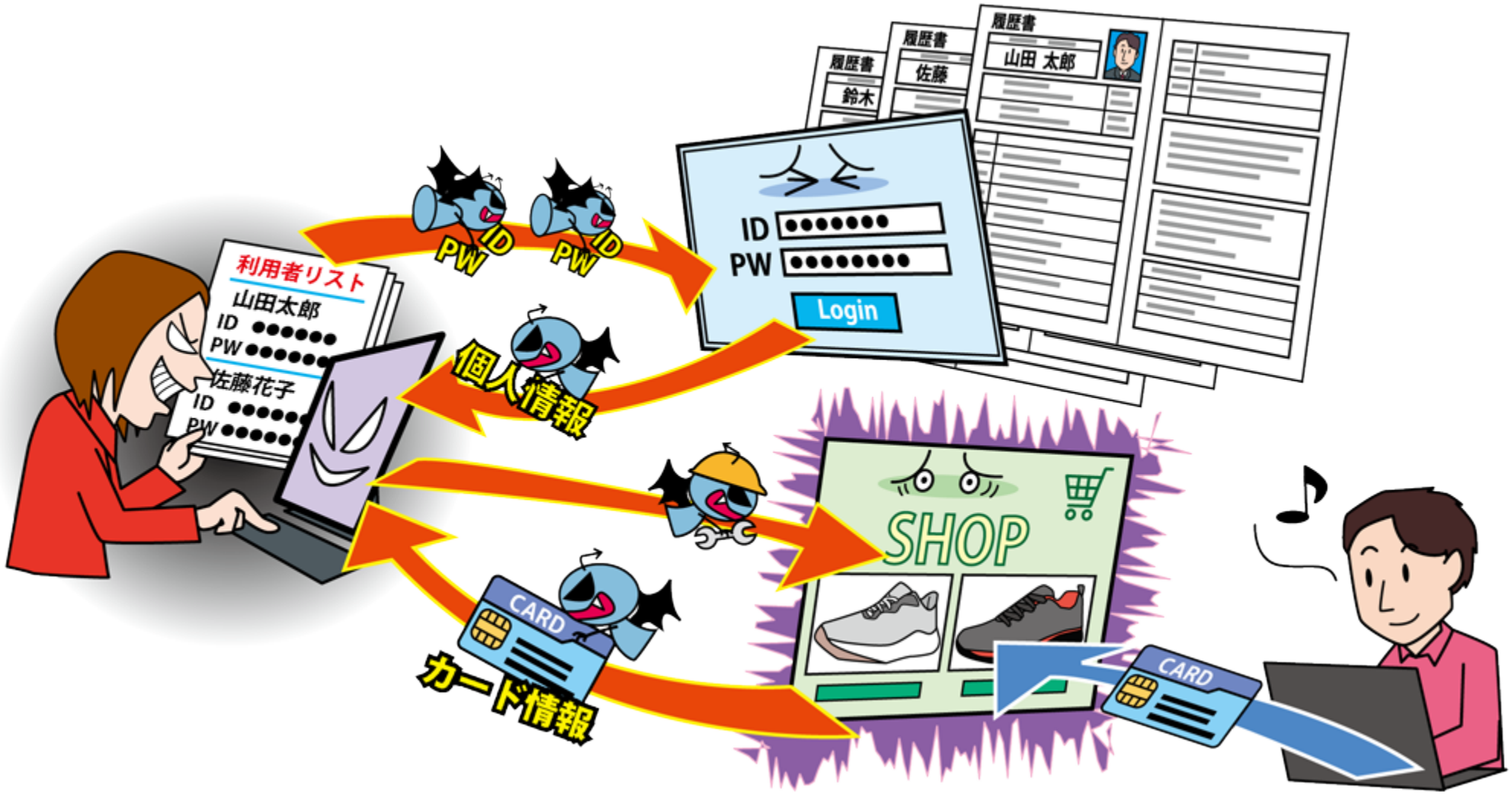
- **どんな事例があるの？**
  - 通信事業者を装った**SMS**により**不正アプリ**を**インストール**させて、**ネットワーク暗証番号**等を**詐取**する手口をJC3が確認した
  - SMSのリンクをクリックすると、不正アプリをインストールするよう誘導される
  - Android 版アプリ、iPhone版アプリの両方が確認されている
  - JC3は、**正規のアプリサイト以外のサイト**からアプリケーションを**インストールしない**ように注意を呼び掛けている

【出典】
通信事業者を装ったフィッシング（不正アプリに注意）（JC3）
https://www.jc3.or.jp/threats/examples/article-409.html

【対策】不正アプリを利用した攻撃

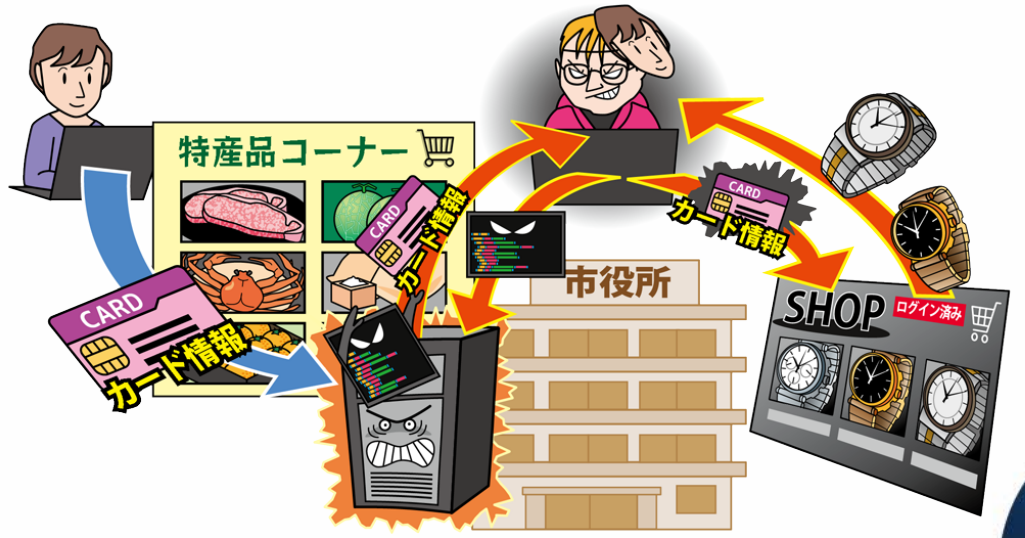
- **どんな対策があるのか？**
  - アプリは**公式マーケット**からのみ**ダウンロード**する
    ※公式マーケットに**不正アプリ**が**紛れている**こともあるので、以下を確認する
    - アプリの**レビュー**を読んで評判が悪くないか
    - **アプリ**及び**アプリ開発者**の**情報**を**Web検索**して問題がないか
  - アプリインストール時等に要求される**アクセス権限**を確認し、
    以下のように**必要以上**の**権限**を**要求**された場合は、**アンインストール**する
    - **デバイス管理者**の権限
    - **使わないはず**の**個人情報**(**電話帳**や**メール等**)を利用する権限
  - **不要**な**アプリ**はそもそも**インストールしない**。インストール済みなら**アンインストール**する。
  - スマートフォン用の**セキュリティソフト**をインストールする

システムの弱点が突かれてしまう脅威



【概要】システムの弱点が突かれてしまう脅威

- **どんな脅威があるの？**
  - インターネットサービスへの**不正ログイン**
  - インターネットサービスからの**情報窃取**
  - **クレジットカード情報**の**不正利用**
  - **スマホ決済**の**不正利用**
- **どんな問題が起きるの？**
  - **個人情報**を**窃取**されてしまう
  - **不正送金等**により**金銭窃取**をされてしまう



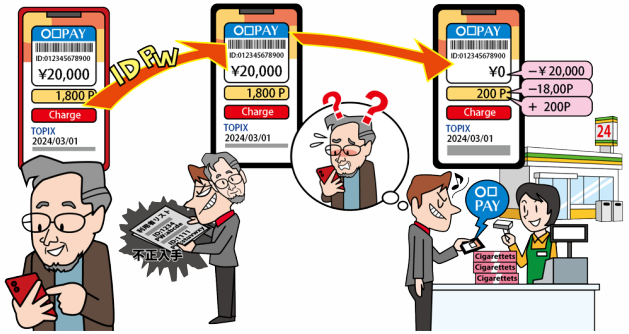
【手口】システムの弱点が突かれてしまう脅威

- **攻撃者は、どんな手口でシステムの弱点を突くの？**
  - パスワードの不備を突いて、インターネットサービスに**不正ログイン**する
    - あらかじめ盗んだ**大量**の**IDとパスワード**を**片っ端から**入力する(**パスワードリスト攻撃**)
    - 以下のパスワードを入力する(**パスワード類推攻撃**)
      - » あらかじめ盗んだ個人情報に含まれる**名前**や**生年月日等**の**組み合わせ**
      - » **適当な単語**の**組み合わせ**
  - **パスワード認証のみ**で**振り込み**ができるインターネットサービスで、本人に**なりすまして**振込を行う
  - **所有端末**を**ウイルス**に**感染**させ、ウイルスに**個人情報**を**窃取**させる
  - 所有端末で利用している**ソフトウェア**の**脆弱性**を**悪用**したり**設定**の**不備**を**悪用**したりして、所有端末を**乗っ取り**、**個人情報**を**窃取**する

【事例】システムの弱点が突かれてしまう脅威

どんな事例があるの？

- 2024年の8月から9月にかけて複数の端末からの、**ユーザーIDとパスワードの組み合わせ**を用いた**不正ログイン**が大量にあったとスポーツ関連事業者が公表した
- この期間にあった不正ログインは**4,274件**であった

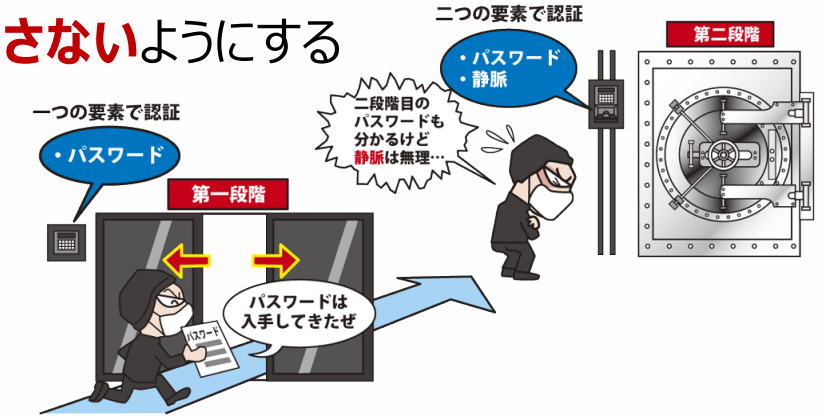


- ただし、顧客の個人情報を閲覧できるページへの**アクセス履歴が無かった**ため、**個人情報の漏えい**や、**データの改ざん**等は**無かった**としている
- また、他にも不正なアクセス履歴は無かったことが確認できたため、**クレジットカード情報**を利用した**不正送金**等が起きた可能性は**非常に低い**としている

【出典】
※1　弊社オンラインサイトへの不正ログインの発生とパスワード変更のお願いについて（Golf Digest Online Inc.）
https://company.golfdigest.co.jp/brand/news/post.html

【対策】システムの弱点が突かれてしまう脅威(1/2)

- **どうすれば良いの？**
  - パスワードを含めた**認証管理**を**徹底**する
    - パスワードは**10文字以上**で、**規則性がない**ものにする
    - 他のインターネットサービスで利用する**IDとパスワードを使い回さない**ようにする
    - パスワード以外の認証も利用した**多要素認証**もお薦め
    - そもそもパスワードを利用しない**パスキー**はさらにお薦め
  - 悪意のある攻撃者に端末を乗っ取られないようにする
    - 所有端末に**セキュリティソフトを導入**する
      - » **ウイルスの検知・駆除**をするためにウイルス対策機能を有効化する
      - » **所有端末への不正な通信をブロック**するためにファイアウォール機能を有効化する
    - 所有端末で利用しているソフトウェアの**脆弱性**を**解消**するために、**最新版**に**アップデート**する
    - 所有端末の**利用していない設定**を**無効化**する



【対策】システムの弱点が突かれてしまう脅威(2/2)

- **どうすれば良いの？**
  - クレジットカードの不正利用対策
    - **利用限度額**を設定する
    - **プリペイドカード**を利用する
    - **利用頻度が低いサービス**にはクレジットカード情報は**登録しない**
    - **利用していないクレジットカード**は**破棄**する
    - **利用時**に**逐次通知**する設定にし、**利用明細**を**定期的に確認**する
  - スマホ決済の不正利用対策
    - **決済時**に**逐次通知**する設定にし、**利用明細**を**定期的に確認**する
    - 紛失対策
      - » スマートフォンの**画面ロック**の有効化
      - » **リモート**からの**データの遠隔消去**／**初期化**機能の有効化

自分が加害者になるおそれもある脅威

【概要】自分が加害者になるおそれもある脅威

- **どんな脅威があるの？**
  - インターネット上の**誹謗・中傷・デマ**

- **どんな問題が起きるの？**
  - SNSや掲示板等で**他人**を**誹謗・中傷**したり、**脅迫**や**犯罪予告**と考えられる書き込みをしたりすると、**事件**に**発展**してしまう
  - **デマ**を**発信**したり**拡散**したりすることで、**世間**を**混乱**させてしまう

- **なぜこんなことをするの？**
  - 日頃の**不満**や**ストレス**の**捌け口**としてしまう
  - 面白い書き込みをして**目立ちたい**と考える
  - 災害対策情報等を**デマ**と**分からず拡散**する等の**親切心**が**裏目**に出る

【事例】自分が加害者になるおそれもある脅威

- **どんな事例があるの？**
  - 2024年1月1日に発生した能登地震に乗じて、X等のSNSで**偽**の**救援**を**求める投稿**が確認されている
  - その投稿後に、救援は完了したため**寄付金**を**募る**旨の投稿もされていた
  - この時に、実際に**寄付**を**してしまった**ユーザがいることも確認されている
  - 首相はSNS事業者には投稿の削除等の対応を要請し、SNSのユーザには寄付をしないことを呼び掛けている

【出典】
※1　令和6年能登半島地震の偽情報関連の報道についてまとめてみた（piyolog）
https://piyolog.hatenadiary.jp/entry/2024/01/06/020106
※2　善意につけ込む偽情報　震災時に…なぜ投稿？　SNSで「悲劇の現金化」が…　記者も実践！　ウソを見極める方法とは【#みんなのギモン】（日テレNEWS）
https://news.ntv.co.jp/category/society/5bba32008d98452d885d76f06a0d2a7e

【対策】自分が加害者になるおそれもある脅威

- **どうすれば良いの？**
  - インターネット上の**情報**を**鵜呑みにしない**ようにする
    - **複数**の**情報源**から情報を得る
    - 投稿者の情報をWeb検索し、**投稿者**の**評判**を**確認**する
  - 投稿をする前に**影響範囲**を**考える**
    - **「他人も書いているから問題にならない」**とは思わないようにする
    - **情報の拡散**も**問題になる**ことを**認識**する
  - 被害を受けたら、**サイト管理者**や**プロバイダ**に**投稿の削除**を**依頼**する。
    または、以下の組織に相談する。
    - セーファーインターネット協会：https://www.saferinternet.or.jp/bullying/
    - 弁護士、日本司法支援センター法テラス：https://www.houterasu.or.jp/
    - サイバー犯罪相談窓口：https://www.npa.go.jp/bureau/cyber/countermeasures/defamation.html

３．対策のまとめ

- **情報セキュリティ対策の基本**

情報セキュリティ対策の基本

- 多数の脅威があるが「攻撃の手口」は似ている
- 基本的な対策方法は年月が経っても変わらない
- 下記の「情報セキュリティ対策の基本」は常に意識

攻撃の手口	情報セキュリティ対策の基本	目的
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
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
ソフトウェアの脆弱性の悪用	**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
設定不備の悪用	**設定の見直し**	誤った設定を攻撃に悪用されないようにする

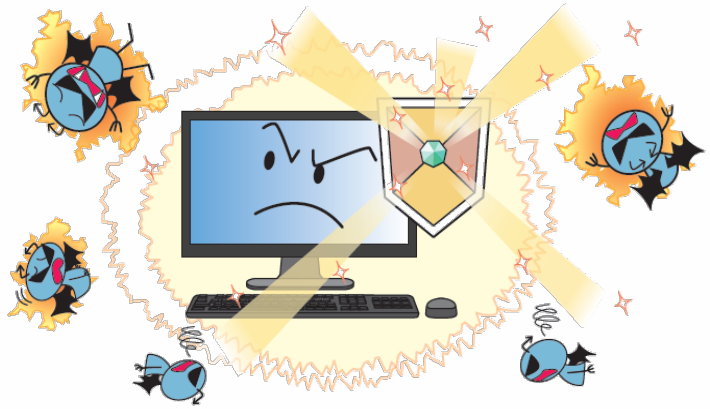
脅威・手口を知る

- **公的機関の注意喚起やニュース等から脅威の手口に関する情報を収集**
- **変化する手口を理解して適切な対策を実践**
  - ソフトウェア開発ベンダや、注意喚起や情報発信を行っている公的機関の**SNSアカウントをフォロー**する
  - 公的機関やニュースサイトの**メールマガジンを利用**する

→[参考] IPAメールニュース
https://www.ipa.go.jp/mailnews.html

セキュリティソフトの利用

- **ウイルス対策機能でウイルスの感染を未然に防ぐ**
- **ファイアウォール機能で不正な通信をブロックする**



※通常のPC(Windows)であれば…

- 最低限、**Windows標準のセキュリティ機能は有効にする（Microsoft Defender）**
- Macintoshやスマホ等には、**市販のセキュリティソフトの利用**を検討する

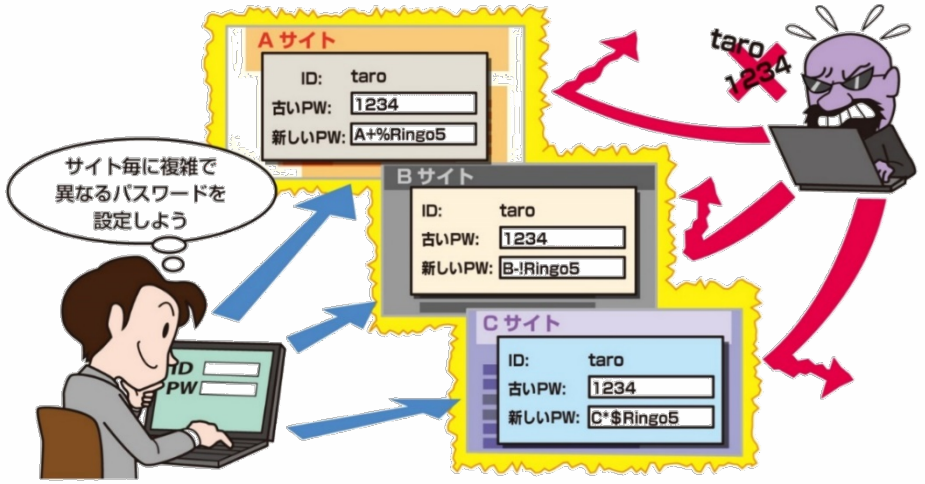
パスワードの管理・認証の強化

- **文字数が多く、規則性のないパスワードを設定**
- **複数のインターネットサービスでパスワードを使い回さない**
- **多要素認証等、強い認証方式が利用できれば利用する**

パスワード	悪い点
123456	連続した数字
Password p@ssw0rd	単純な単語や その類似系
taro1202	名前や誕生日
1qaz2wsx	キーボードの縦配列
qwerty	キーボードの横配列

脆弱なパスワードの例

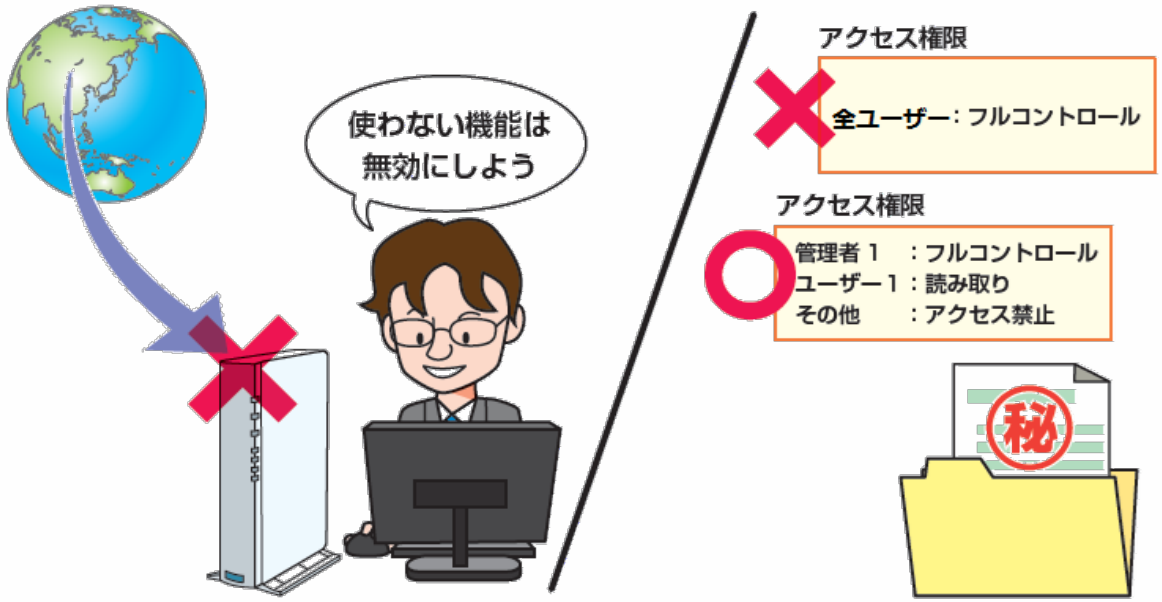
パスワード管理が大変…
→パスワード管理ソフトの利用や
パスキーも有効



設定の見直し

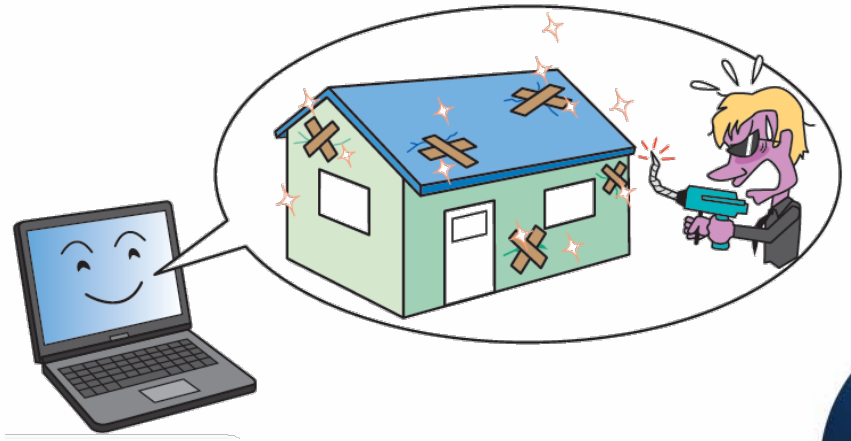
- **利用する機器やソフトの仕様を理解して適切に運用する**
  - **初期パスワードからパスワードを変更する**(IoT機器等)
  - サーバーやクラウドサービスの**公開設定を確認**する

    →バージョンアップや仕様変更によって意図しない設定変更がされる場合があるため注意
  - **アクセス制限**の設定を確認する
  - **不要な機能は無効化**する



ソフトウェアの更新

- **ソフトウェアの脆弱性は、ソフトウェアを更新して解消する**
  - 修正プログラムのリリースから適用するまでの**期間が長期化**すると、脆弱性を悪用した**攻撃をされる可能性が非常に高くなる**
  - 修正プログラムを迅速に適用する
    →**利用しているソフトウェアの把握**と**継続的な情報収集**が必要
    [参考]MyJVNバージョンチェッカ(IPA)
    https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html
  - 自動更新機能を活用する(Windows等)



4. 参考情報/資料紹介

安心相談窓口

- **安心相談窓口（IPAの相談窓口）**
  - Webサイト：https://www.ipa.go.jp/security/anshin/about.html
  - メールでの相談：anshin@ipa.go.jp
  - 電話での相談：03-5978-7509
    ※土日祝日・年末年始は除く、10:00～12:00、13:30～17:00 に受付

Check!!
安心相談窓口だより（IPA）
https://www.ipa.go.jp/security/anshin/attention/index.html
※よくある手口や対策を紹介しているので是非ご覧ください

情報セキュリティ10大脅威 解説書

- **下記Webページに解説書を公開する予定です**

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10大脅威 2025**
→個人編、組織編、コラム

☆**情報セキュリティ10大脅威の活用法**
→個人編、組織編

☆**情報セキュリティ10大脅威 2025 セキュリティ対策の基本と共通対策**
→解説書から「共通対策」を切り出したもの

☆**情報セキュリティ10大脅威 2025 知っておきたい用語や仕組み**

情報セキュリティ10大脅威 簡易説明資料

- 簡易説明資料(スライド形式)

組織編

個人編[一般利用者向け]

- **過去の10大脅威はトップページから**

情報セキュリティ10大脅威 トップページ
https://www.ipa.go.jp/security/10threats/index.html