情報セキュリティ10大脅威2024 組織編

MCPC　情報セキュリティセミナー

2024年6月12日

情報処理推進機構 (IPA)
セキュリティセンター
大友　更紗

IPA Better Life with IT

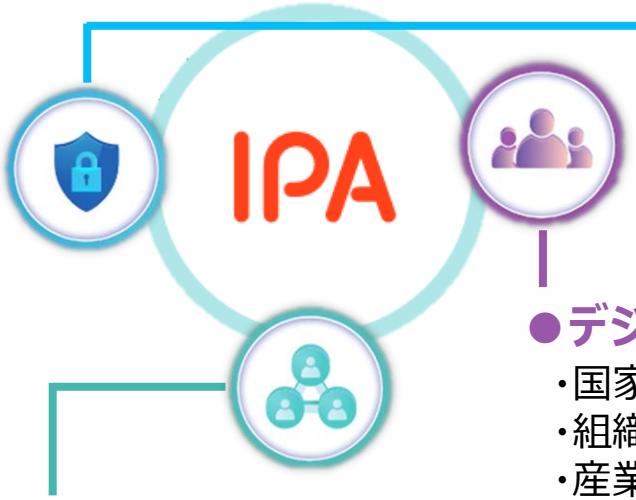
アジェンダ

１．情報セキュリティ10大脅威とは

IPA(情報処理推進機構)のご紹介

Information-technology Promotion Agency, Japan

- 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**」を目指しています



●サイバーセキュリティの確保
- ・セキュリティ啓発活動
- ・セキュリティ評価・認証
- ・標的型攻撃対応、脆弱性対策　etc.

●デジタル人材の育成
- ・国家試験 情報処理技術者試験
- ・組織・スキル変革の推進
- ・産業サイバーセキュリティ人材育成　etc.

●デジタル基盤の提供
- ・アーキテクチャ設計
- ・DX推進　etc.

「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資料
- 前年に発生したセキュリティ事故や攻撃の状況等から
  IPAが脅威候補を選出
- セキュリティ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」が投票
- TOP10入りした脅威を「10大脅威」として脅威の概要、
  被害事例、対策方法等を解説

２つの「10大脅威」

脅威に対して様々な立場の方が存在

立場ごとに注意すべき脅威も異なるはず

- 家庭等でパソコンやスマホを利用する人

「個人」

- 企業や政府機関などの組織
- 組織のシステム管理者や社員・職員

「組織」

「個人」と「組織」の２つの立場で脅威を解説

情報セキュリティ10大脅威 2024 個人編

「個人」向け脅威（五十音順）	初選出年	選出状況(2016年～)
インターネット上のサービスからの個人情報の窃取	2016年	5年連続8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	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6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	9年連続9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	6年連続6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	2年連続4回目

2024年から個人編では
「順位」を撤廃
→**順位に関わらず自身に関係のある脅威に対して対策を**

初選出の脅威は無く、常連の脅威ばかり
→よくある手口でも引っ掛かる人が後を絶たない
→**まずは手口を知り、基本的な対策をしっかり行うことが重要**

情報セキュリティ10大脅威 2024 組織編

順位	「組織」向け脅威	初選出年	選出状況(2016年～)
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

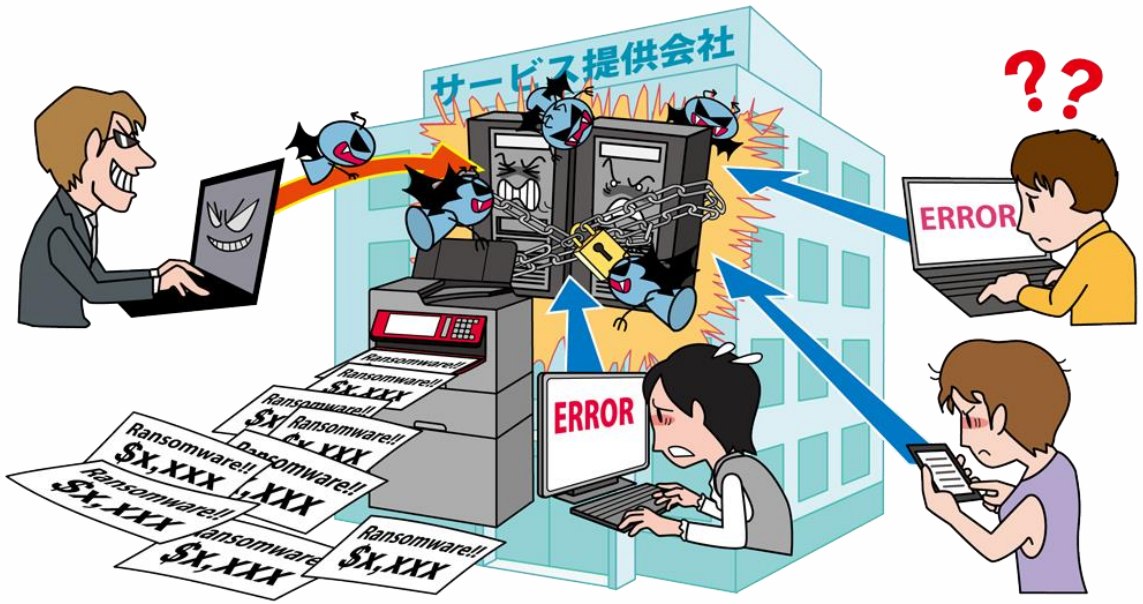
組織編はランキング形式だが…
→**順位に捕らわれず自組織に合わせた対策を**

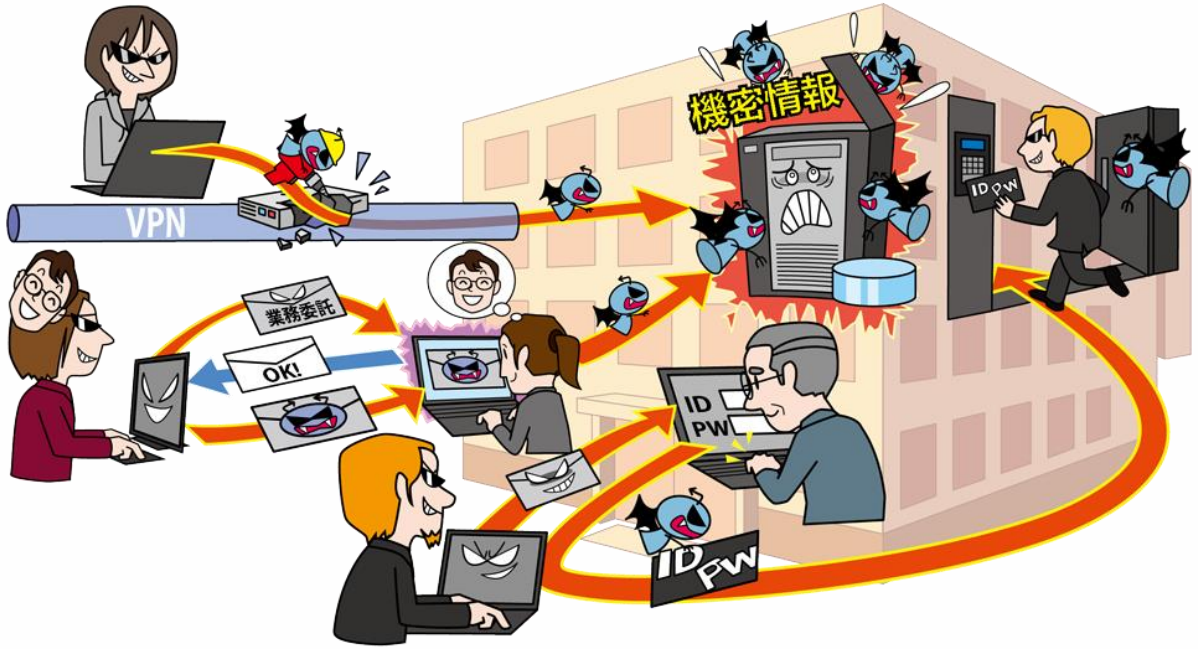
初選出の脅威は無く、常連の脅威ばかり
→攻撃者が有効と考える手口が長年変わっていない
→**まずは基本的な対策が重要**

2. 脅威解説

- ランサムウェアによる被害/標的型攻撃による機密情報の窃取
- サプライチェーンの弱点を悪用した攻撃
- 内部不正による情報漏えい等の被害

ランサムウェアによる被害/
標的型攻撃による機密情報の窃取





【概要】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

ランサムウェア攻撃とは？

- PCやサーバーに**データを暗号化するウイルス「ランサムウェア」**を感染させる攻撃
- **脅迫**により**身代金**を要求

→・データを**暗号化**する
  ・**情報を窃取**しリークサイト上に公開する
  ・**DDoS攻撃**(Webサイト等に過剰なアクセス)を行う
  ・攻撃を受けていることを取引先等に**リーク**する

復元したければ/やめてほしければ身代金を払え！

- 攻撃を受けるとシステムが動かなくなることも多く、**業務が停止**することも

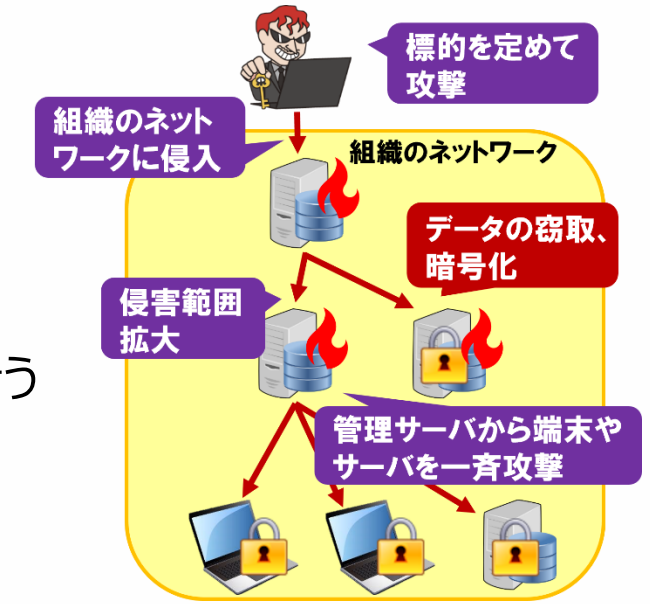
【概要】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

標的型攻撃とは？

- **ウイルス等**を使用して標的組織のシステムに侵入する攻撃
- 長期間にわたり**潜伏し侵害範囲を拡大**させていく傾向
- **機密情報等の窃取**やシステム破壊による**業務妨害**が目的

※標的型(侵入型)ランサムウェア攻撃

- 特定の組織に標的を定めシステムに侵入
- 侵害範囲を拡大して機密情報等を窃取
- 最終的にランサムウェアを展開して暗号化と脅迫を行う



【手口】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

ウイルスの感染経路

- 攻撃者から送られてきた添付ファイル

  →・**添付ファイルを開く**/Officeファイルの**マクロを実行する**ことでウイルスに感染

  ・主に**メール**が利用され**業務に関係する差出人や内容を装っている**ことが多い

  ・**SNS**で親密になりチャット機能で添付ファイルを送る標的型攻撃も確認されている

- 攻撃者が用意した悪意あるWebサイト

  →・アクセスしたりサイト上で何らかのアクションを起こすことでウイルスに感染

  ・**メール等で誘導**される

- 攻撃者からのシステムへの不正アクセス

  →・システムやネットワーク機器の**脆弱性**を悪用される

  ・ネットワークの**設定不備**を突かれる

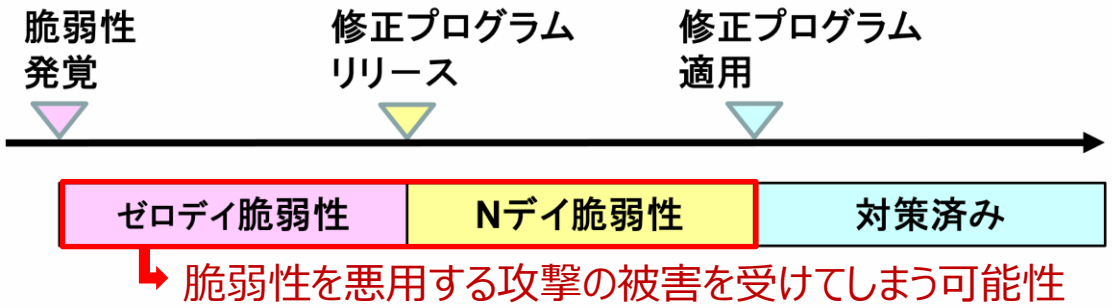
  ・システムにアクセスするための**認証情報を窃取/推測**される

近年のランサムウェア攻撃の主流

【手口】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

● 補足：狙われる脆弱性

5位 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7位 脆弱性対策情報の公開に伴う悪用増加



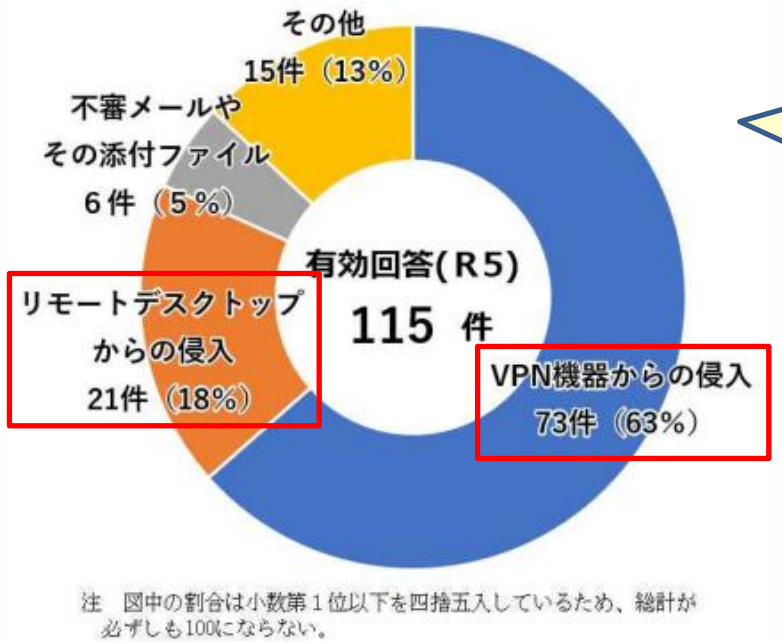
- **修正プログラムの公開前を狙う攻撃**
  →・知らぬ間にゼロデイ脆弱性を悪用されてしまう
- **脆弱性対策情報の公開に伴う悪用増加**
  →・脆弱性対策情報は攻撃者にとってのヒントでもある
  ・脆弱性対策情報が公開されてから攻撃が始まるまでの期間が短くなっている

Nデイ脆弱性の期間が
長いとリスク大
→**脆弱性の放置はNG**

【手口】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

● 補足：狙われるネットワークの入り口

9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



(※1)
2023年に警察庁に報告があったランサムウェア被害の感染経路

感染経路の約8割が
VPN機器・リモートデスクトップからの侵入
→・脆弱性
・平易な認証情報
・設定不備

・**テレワーク用のリモート接続経路**が狙われることも
・コロナ禍でテレワークを導入後オフィスワークに戻した場合、使わなくなったVPN機器を放置すると危険

【出典】
※1　令和５年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

【手口】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

- **侵入後の活動(横展開)**

①遠隔操作が可能な環境の確立

→・遠隔操作ウイルス(RAT)と攻撃者側の**C&Cサーバーとの通信**により実現

②ネットワーク環境や機器の探索

→・**セキュリティが脆弱な箇所**を探し侵害範囲を拡大

・機密情報や個人情報等の保管場所を確認

③管理者権限の取得

→・**資格情報の窃取**や**脆弱性の悪用**によって行われる

・より重要な情報へのアクセスや、セキュリティソフト無効化等の行為が可能に

④目的の達成

→・機密情報等をコピー、圧縮し外部に送信

・ランサムウェア展開による暗号化

【手口】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

補足：ビジネス化するサイバー攻撃

10位 犯罪のビジネス化（アンダーグラウンドサービス）

ダークウェブ等で行われているサイバー犯罪ビジネスの例

ウイルスの売買	脆弱性を悪用する攻撃ツールの売買	ボットネットの売買	認証情報の売買	サイバー犯罪組織の人材募集

- **サイバー犯罪の活発化**

  →・犯罪組織によるRaaS(Ransomware as a Service)等のビジネスモデルが確立したことでサイバー攻撃が活発化している

- **サイバー犯罪の高度化**

  →・完成されたウイルスや攻撃ツール等を購入できることで、本来高度な技術的知識を必要とするランサムウェア攻撃や標的型攻撃のハードルが下がっている

【事例1】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

(※1,2)

- **<u>脆弱性を悪用されたことによるランサムウェア感染</u>**
  - 名古屋港のコンテナターミナルで運用されているシステムがランサムウェアに感染(2023年7月)
  - 丸2日以上**システムが停止**し同港における**物流がストップ**
  - ランサムウェア感染に**VPN機器の脆弱性を悪用**された
  - 当該脆弱性は同年6月にVPN機器の開発元より**修正プログラムがリリースされていたが適用していなかった**

【出典】
※1　NUTS システム障害の経緯報告（名古屋港運協会）
https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf
※2　名古屋港システム停止、脆弱なＶＰＮ狙われたか…最新「修正プログラム」適用せず無防備状態　（讀賣新聞オンライン）
https://www.yomiuri.co.jp/national/20230727-OYT1T50215/

【事例2】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

- **横展開が行われたランサムウェア攻撃**(※1,2)
  - 国内の市民生活協同組合がランサムウェア攻撃を受けていたことを公表(2023年1月)
  - 攻撃者は**脆弱性を悪用してVPN経由で侵入**後、**内部を探索**し**複数のサーバーにおいてランサムウェアを展開**
  - 約49万人の個人情報を含むデータが暗号化された
  - **バックアップ**を取っていたデータベースは感染を逃れていたため、**データを復元することができた**

【出典】
※1 重大なシステムトラブルに伴う個人情報についてのお知らせ（市民生活協同組合ならコープ）
https://www.naracoop.or.jp/naranews/cat2/4628.html
※2 多数システムでランサム被害、復旧や事業継続に追われる - ならコープ（Security NEXT）
https://www.security-next.com/143034/

【事例3】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

- **<u>複数回のやり取りを伴う標的型メール攻撃</u>** (※1,2)
  - 国内の大学の教員の**PCがウイルスに感染し情報を窃取**された(2023年10月)
  - **実在する組織の担当者を騙った人物**から講演依頼のメールが届き、日程調整のため**複数回メールのやり取り**を行っていた
  - 数回目のメールに記載されていた**URLにアクセスしウイルスに感染**
  - 教職員や学生等の個人情報や過去の試験問題等、計4,341件が流出

【出典】
※1 東京大学大学院総合文化研究科・教養学部への不正アクセスによる情報流出について（東京大学）
https://www.u-tokyo.ac.jp/focus/ja/press/z0109_00952.html
※2 サイバー攻撃か 東大教員のパソコンに不正アクセス、個人情報4300件流出（TBS NEWS DIG）
https://newsdig.tbs.co.jp/articles/-/796546

【対策】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

● 組織としての体制の確立

- **専門知識を持つ責任者**(CISO等)を配置
- インシデントの防止や有事の際の対応を行う**専門チーム**(CSIRT)を構築
- 継続的なセキュリティ対策を行うための**予算の確保**
- **情報セキュリティポリシー**の策定および職員への周知

→・情報セキュリティに対する組織の**基本方針**
・基本方針を実現するための**対策基準**
・対策基準ごとの具体的なセキュリティ対策の**実施手順**、**運用規則**

【対策】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

● 被害の予防

- **メールの添付ファイルやリンクを安易にクリックしない**

①**電子署名**の有無や**メールアドレス**を確認する

②メール本文の内容を確認する

・**緊急性を強調**した内容、**添付ファイルやリンクに誘導**する内容は要注意

③少しでも**不審な点がある添付ファイルやURLは開かない**

・実行ファイル(.exe)等普段使わない種類のファイルはクリックしない

→PDF等よく使う種類のファイルが悪用されたり、ファイルの種類を偽装する手口もあるため
見慣れたファイルなら絶対安全というわけでもないので注意

・Officeファイルの場合**マクロを実行しない**

→「コンテンツの有効化」「マクロを有効にする」等のボタンを押さない

「設定」で機会を減らす対策も有効

→・業務で使用しない形式のファイルが添付されたメールは受信を拒否する
・業務でマクロ機能を使用しない場合は無効化する

少しでも不安な点があれば正規の窓口から相手に確認を

※疑いのあるメールに返信する、メールに記載されている番号に電話する、はNG

【対策】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

● 被害の予防

- **脆弱性対策**を行う

  ①**脆弱性情報の収集**および**修正プログラムの適用(アップデート)**を行う

  ②サポート切れのOSやソフトウェアは利用しない

  ・脆弱性が発見されても基本的にセキュリティパッチは公開されない

  ③セキュリティのサポートが充実しているソフトウェアやバージョンを使う

- フィルタリングソフトやセキュリティ製品を導入する

→・導入するだけでなく、**定期的なスキャン**や**パターンファイルの更新**が必要

・ウイルス検知によるブロックだけでなく、不審な通信や振る舞いを検知することで**迅速な対応を可能にする**ことも重要

【対策】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

被害の予防

- **認証を強化**する

  →・容易に推測できるパスワード(admin等)を使わない
  ・多要素認証の設定を有効にする

- **セキュリティ教育**を行う

  →・他人事として考えさせない
  ・人の入れ替わりやイベント(長期休暇前等)に合わせ**継続的に取り組む**

- ペネトレーションテストやインシデント訓練を行う

  →・定期的に行い**セキュリティ対策やインシデント対応手順をアップデート**する

【対策】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

被害の早期発見

- **ログを取得**し監視や解析を行う

  →・システムログ、アプリケーションログ、サーバーへのアクセスログ、
  　認証ログ、データベース操作ログ、通信ログ 等

- **ネットワークやエンドポイントの監視や防御**を行う

  →・セキュリティ製品を導入する

【対策】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

● 被害を最小限に抑える

- **ネットワーク分離**や共有サーバー等への**アクセス権の最小化**を行う

  →・組織のネットワーク内に侵入された際に侵害範囲を最小限に留める

- 重要なファイルやシステムの**バックアップ**を定期的に取得する

  ①バックアップ媒体とPCやサーバーとの**接続はバックアップ取得時のみ**

  ・ランサムウェア感染時に一緒に暗号化されないようバックアップデータは**オフラインで保管**

  ②バックアップに使用する媒体やバックアップデータは**複数用意**

  ・**複数の媒体**を用い、さらに**コピーも用意**することで有事の際に利用可能な状態である可能性が高まる

  ・一つは**オフサイトで保管**することで災害対策にも

  ③バックアップ方式の妥当性やバックアップデータの状態を**定期的に確認**

  ・必ず**エラーゼロ**でバックアップを完了させる

  ・バックアップからの**復旧手順を整備**し、実際に復旧できるか**テスト**する

【対策】ランサムウェアによる被害/標的型攻撃による機密情報の窃取

● 被害を受けた後の対応

- 発見者による適切な初動対応

  →・ウイルス感染が疑われる機器の**ネットワーク接続を切断**

  ・組織の規定に従い**エスカレーション**

- 担当部署や外部協力先によるインシデント対応、影響調査および原因の追究
- 復旧作業

  →・バックアップからの復旧

  ・復号ツールの活用

  [参考]No More Ransom(https://www.nomoreransom.org/ja/index.html)

- **身代金は支払わない**

個人情報保護法により、個人情報の漏えいが発生した場合は個人情報保護委員会への報告が義務付けられている

・身代金要求に応じる組織として今後も標的に
・復旧できたり流出した情報が削除されたりする保証はない

サプライチェーンの弱点を悪用した攻撃

【概要】サプライチェーンの弱点を悪用した攻撃

サプライチェーン攻撃とは？

- 商流(サプライチェーン)の中で**セキュリティ対策が甘い組織を狙う**攻撃
- セキュリティレベルが高い組織への攻撃の足掛かりとする

2種類のサプライチェーン

- 調達、製造、在庫管理、物流、販売、業務委託先等の一連の商流
  →・取引先、委託先、グループ企業
  　・利用している外部サービス
- ソフトウェア開発のライフサイクルにかかわる商流(**ソフトウェアサプライチェーン**)

【手口】サプライチェーンの弱点を悪用した攻撃

- **サプライチェーンから標的組織の重要情報を窃取する**
  - 標的組織の**重要情報を保有している取引先や委託先**を攻撃
  - 標的組織が利用している**サービス(の提供企業)**を攻撃

    →・サービスに不正アクセスする

    ・サービスを改ざんする

【手口】サプライチェーンの弱点を悪用した攻撃

- **サプライチェーンを足掛かりに標的組織を攻撃する**
  - 標的組織と**ネットワークが繋がっている子会社や委託先**に不正アクセス
    →認証情報を窃取する等して標的組織にも侵入する
  - **サービス事業者**を攻撃
    →MSP(企業システムの運用・監視等を請け負う事業者)を通じて
    標的組織への侵入やウイルス配布を行う
  - **ソフトウェアの開発元**を攻撃
    →開発元が提供するソフトウェアを改ざんしてウイルスを仕込み、
    当該製品の導入やアップデート適用を行った組織にウイルスを感染させる
  - **OSS**(オープンソースソフトウェア)を悪用
    →OSSに悪意あるコードや脆弱性を仕込み、当該OSSを含む製品を利用する
    標的組織への攻撃の足掛かりとする

【事例1】サプライチェーンの弱点を悪用した攻撃

- **業務委託先業者からの顧客情報漏えい**(※1,2)
  - 複数の保険会社が、**業務委託先から顧客の個人情報が流出**していたことを公表した(2023年1月)
  - **業務委託先のサーバーに不正アクセス**され、流出した個人情報が海外のウェブサイトに掲載されていた
  - 業務委託先が**委託元のセキュリティ管理のルールに基づいた情報管理を行っていなかった**ことが原因
  - 保険会社によっては130万件以上の顧客情報が流出した

【出典】
※1　個人情報流出に関する再発防止策について（アフラック生命保険株式会社）
https://www.aflac.co.jp/news_pdf/20230710.pdf
※2　個人情報漏えいに関するお詫びとご報告（チューリッヒ保険会社）
https://www.zurich.co.jp/customerdata/

【事例2】サプライチェーンの弱点を悪用した攻撃

- **ソフトウェアに脆弱性を仕込むサプライチェーン攻撃**(※1)
  - **広く利用されているオープンソースソフトウェア**「XZ Utils」に**深刻な脆弱性**が発見された(2024年3月)
  - 当該脆弱性は外部からの不正アクセスを可能にするもので、**バックドア**(攻撃者がシステム内に不正侵入するための入口)として悪用されるおそれがある
  - 数年間プロジェクトに関わり、2023年からXZ Utilsの**メンテナンスを任されていた人物が意図的に脆弱性を作り込んでいた**

【出典】
※1 「XZ Utils」にバックドア、オープンソースエコシステム全体の信頼を揺るがす事態に（Impress）
https://forest.watch.impress.co.jp/docs/news/1580604.html

【要因】サプライチェーンの弱点を悪用した攻撃

サプライチェーン攻撃を受けてしまう要因

- サプライチェーンを適切に選定、管理していない

  →情報セキュリティにおけるサプライチェーンリスクの認識が甘い

- 再委託先や再々委託先の管理が困難

  →再委託先、再々委託先組織の管理は委託先組織が行うため、
  委託元からのセキュリティ対策管理はさらに難しくなる

サプライチェーン攻撃を受けた後の対応が難しい要因

- 情報セキュリティに関する責任範囲が不明確

  →契約時に情報セキュリティに関する責任範囲を明確に定めていない場合、
  インシデント発生時の対応がスムーズにできない

【対策】サプライチェーンの弱点を悪用した攻撃

- **被害の予防(サプライチェーンの弱点にならない対策)**
  - ウイルス感染や不正アクセスを防ぐ対策を実施する
    →「ランサムウェアによる被害/標的型攻撃による機密情報の窃取」参照
  - 情報セキュリティの認証取得（ISMS、Pマーク、SOC2、ISMAP等）
    →要件を満たす運用を維持するよう定期的に見直す
  - 業務委託や情報管理における規則の整備と徹底
  - インシデント対応体制の整備
  - **商流に関わる組織への報告体制**の整備

【対策】サプライチェーンの弱点を悪用した攻撃

- **被害の予防(サプライチェーン攻撃の被害を受けない対策)**
  - 業務委託や情報管理における規則の整備と徹底
  - **セキュリティ面で信頼できる**委託先、取引先、サービスの選定
  - **契約時に**委託先、取引先における**情報管理等の規則を確認**する
  - 契約内容を確認する
    →・**情報セキュリティ上の責任範囲の明確化**
    ・問題発生時の対応や運用
    ・問題発生時の補償
  - 取引先や委託先との**連絡プロセスの確立**

環境の変化や情報セキュリティ情勢の変化等に対応できるよう、契約内容を見直す機会を持つ

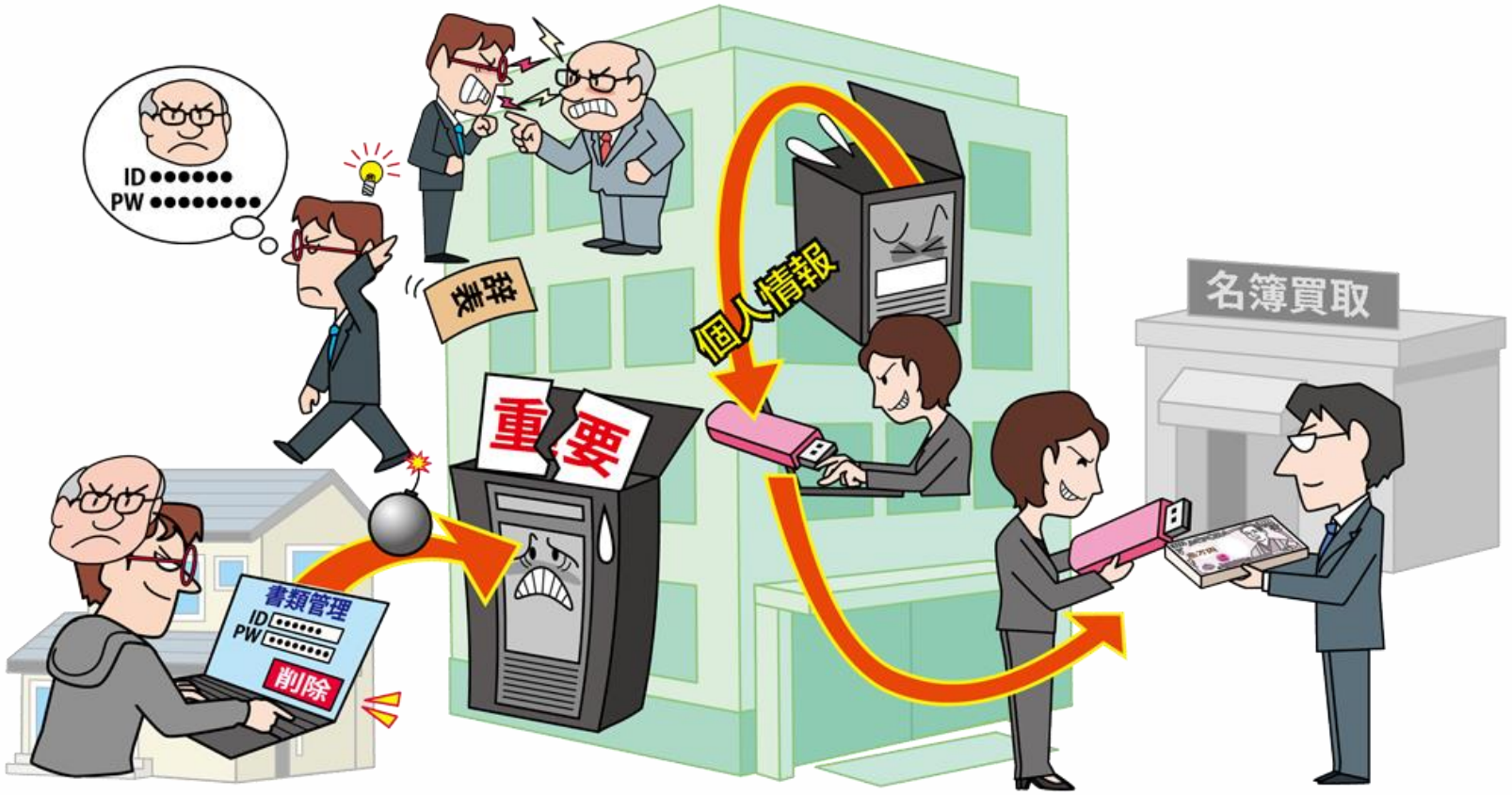
【対策】サプライチェーンの弱点を悪用した攻撃

- **被害の予防(サプライチェーン攻撃の被害を受けない対策)**
  - 委託先組織の管理
    →委託元組織が委託先組織の**セキュリティ対策状況や情報管理の実態を定期的に確認できる契約**とする
  - 納品物の検証を行う
    →**組み込まれているソフトウェアやOSSも把握**する
  - 公的機関が公開している資料の活用
    →・サイバーセキュリティ経営ガイドラインと支援ツール(経済産業省)
    https://www.meti.go.jp/policy/netsecurity/mng_guide.html

【対策】サプライチェーンの弱点を悪用した攻撃

- **被害を受けた後の対応**
  - 関係各所への報告、相談
  - 契約に基づいたインシデント対応
  - 契約に基づいた被害への補償対応
  - 影響調査および原因の追究

内部不正による情報漏えい等の被害



【概要】内部不正による情報漏えい等の被害

- **内部不正とは？**
  - 組織の従業員/元従業員による悪意ある不正行為
  - 組織の規則を守らなかったことによるインシデント

- **内部不正による情報漏えいの影響**
  - 社会的信用の失墜
  - 損害賠償等による経済的損失
  - 不正に取得された情報を利用した組織も責任を問われる

【手口】内部不正による情報漏えい等の被害

内部情報へのアクセス

- 従業員が**業務用に付与されたアカウント**を悪用

  →・必要以上のアクセス権限を付与していると、悪用された場合の被害が大きくなる

- **共用しているアカウント**を悪用
- **他の従業員のアカウント**を悪用

  →・規則性のあるID・パスワードを付与していると他人のアカウントの認証情報を推測できてしまう

  ・端末を複数人で共用している場合、ログイン情報が残っていると他人のアカウントを容易に悪用できてしまう

- 元従業員が**在職中に使用していたアカウント**を悪用

  →・離職者のアカウントを速やかに削除しないと被害を受けるおそれ

【手口】内部不正による情報漏えい等の被害

- **内部情報の不正な持ち出し**
  - **記録媒体を使用**して持ち出す

    →・USBメモリーやHDD等にコピー
    ・メールで外部に送信
    ・クラウドストレージにアップロード
    ・スマホで内部情報が表示された画面を撮影
    ・紙に印刷
  - 組織内で使用していた機器や記録媒体を**不正に販売**(ネットフリマ等)

    →・初期化されず残っていた情報が第三者に流出

【要因】内部不正による情報漏えい等の被害

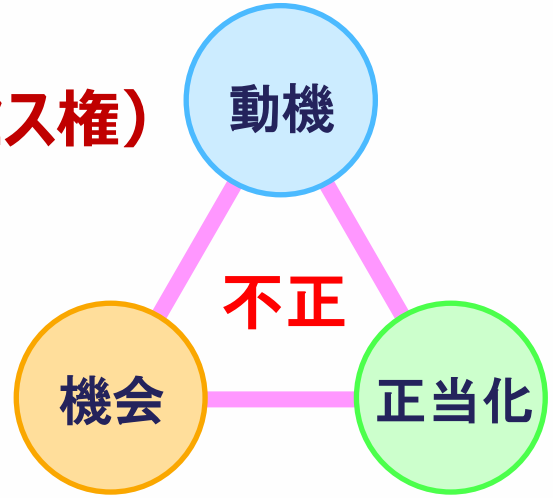
● 不正のトライアングル

- 動機
  - **・職場環境や処遇の不満**

    →処遇面（業務多忙、給料面）の不満、私怨による復讐、利益の享受等
- 機会
  - **・アクセス権限の不適切な付与（過剰なアクセス権）**
  - **・システム操作記録と監視の未実施**

    →不正に気づきにくく、不正の発覚が遅れる
- 正当化
  - **・自分勝手な理由づけ**

    →他の人もやっているから大丈夫、自分は正当に評価されていない



【事例1】内部不正による情報漏えい等の被害

- **派遣社員による顧客情報の持ち出し**(※1,2)
  - 情報通信事業者の元派遣社員が、運用に携わっていたシステムから**顧客情報約928万件を不正に持ち出し**ていたことが判明(2023年10月)
  - 不正が行われた期間は2013年7月～2023年1月の約10年間で、**顧客の少なくとも59組織が情報漏えいの被害**を受けた
  - 当該社員は**管理者用アカウントを悪用**してサーバーに接続しデータをコピー、**USBメモリーで持ち出し**を行っていた
  - 持ち出した情報は**名簿の買い取り業者に**渡されており、対価として1,000万円以上を受け取っていたとみられる

【出典】
※1 NTT西子会社、900万件の情報流出　USBに記録し第三者に渡す（朝日新聞）
https://www.asahi.com/articles/ASRBK4TB5RBKULFA00Q.html
※2 個人情報不正流出 元派遣社員に名簿業者から１０００万円超か（NHK）
https://www3.nhk.or.jp/kansai-news/20231107/2000079388.html

【事例2】内部不正による情報漏えい等の被害

元社員による社内情報の削除(※1)

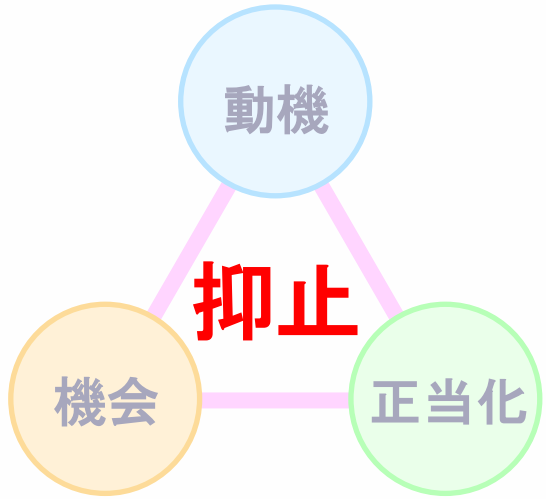
- 国内のメーカーの元社員が、電子計算機損壊等業務妨害罪等の疑いで警視庁に逮捕された。(2023年1月)
- 退職後に**元同僚や元上司のID/パスワードを悪用**して社内ネットワークやクラウドに不正アクセスし、人事や技術、顧客に関する**情報を削除**していた
- 人間関係を理由に退職しており、**嫌がらせが目的**だったとみられている
- データ復旧には約660万円を要した

【出典】
※1　元勤務先に不正アクセス、データ削除した疑い　退職していた男逮捕（朝日新聞）
https://www.asahi.com/articles/ASR1S4HC4R1SUTIL008.html

【対策】内部不正による情報漏えい等の被害

内部不正防止の基本原則(状況的犯罪予防)

- 犯行を難しくする　（やりにくくする）
  →対策を強化することで犯罪行為を難しくする
- 捕まるリスクを高める　（やると見つかる）
  →管理や監視を強化することで捕まるリスクを高める
- 犯行の見返りを減らす　（割に合わない）
  →標的を隠したり、排除したり、利益を得にくくすることで犯行を防ぐ
- 犯行の誘因を減らす　（その気にさせない）
  →犯罪を行う気持ちにさせないことで犯行を抑止する
- 犯罪の弁明をさせない　（言い訳させない）
  →犯行者による自らの行為の正当化理由を排除する



【対策】内部不正による情報漏えい等の被害

組織としての体制の確立

- 基本方針の策定

→・**情報取扱ポリシー**の策定

・懲戒処分等を含む**就業規則**の整備

- 資産の把握、対応体制の整備

→・**重要資産を把握**し、その**重要度をランク付け**する

・重要情報の**管理者を定める**

【対策】内部不正による情報漏えい等の被害

● 被害の予防

- 重要情報の管理、保護

→・重要情報への**アクセス権の管理**(アカウントの登録、変更、削除等)について
ルールを定めて運用する
・異動や離職に伴い**不要となったアカウントは直ちに削除**する
・ルールが守られているか**定期的に監査**を行う
・重要情報を監視、保護するセキュリティ製品(DLP等)を導入する

- 物理的管理の実施

→・重要情報の格納場所や執務室への**入退室管理**
・USBメモリー等**記録媒体の利用制限、持ち出し/持ち込みの管理**
・記録媒体や機器の廃棄時に**適切なデータ消去**を行う(物理破壊も検討)
・リース品返却時に初期化を行う

【対策】内部不正による情報漏えい等の被害

被害の予防

- 人的管理および**コンプライアンス教育**の徹底

→・職員/離職者と**秘密保持契約**を結ぶ
・他人事として考えさせない

被害の早期発見

- **システム操作履歴の監視およびその周知**

→・アクセス履歴や操作履歴等のログを記録、監視する
・監視していることを周知することで不正の抑止に繋がる

【対策】内部不正による情報漏えい等の被害

被害を受けた後の対応

- 発見者による適切な初動対応

  →・組織の規定に従い**エスカレーション**

- 担当部署や外部協力先による影響調査および原因の追究
- 内部不正者に対する**適切な処罰**の実施

  →不正の内容とそれに対する処罰を示すことでその後の不正の抑止に繋がる

- 関係各所や外部に対する**適切な公表**

３．対策のまとめ

- 情報セキュリティ対策の基本
- 共通対策

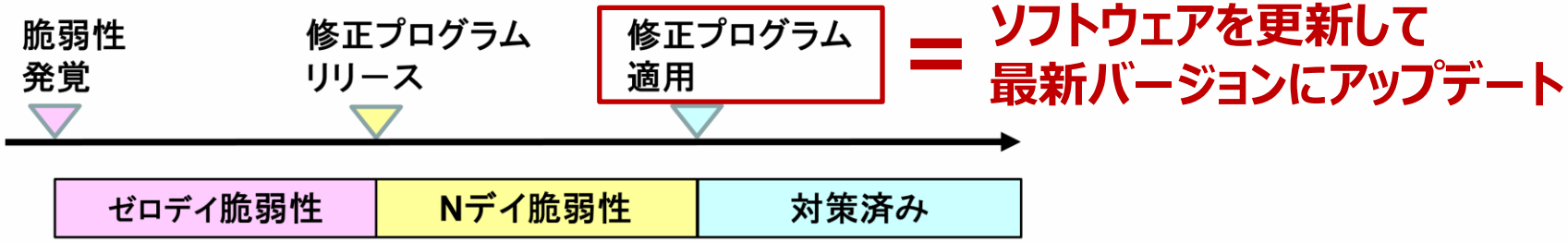
情報セキュリティ対策の基本

- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない
- 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

ソフトウェアの更新

- **ソフトウェアが持つ脆弱性は、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

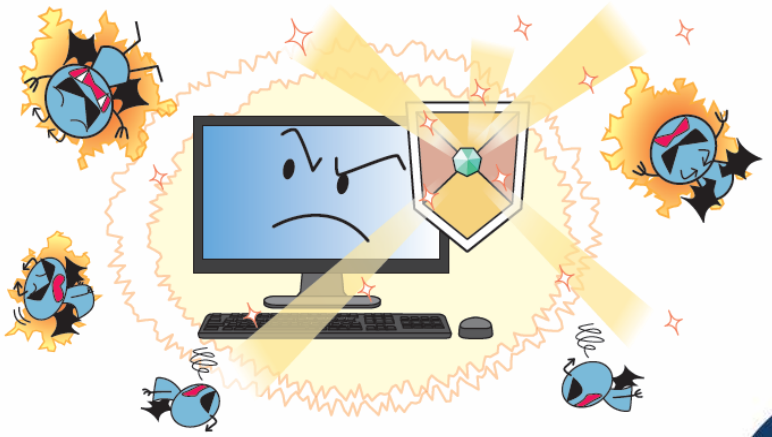
- 自動更新機能を活用する(Windows等)

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）
- その他市販のセキュリティソフトの利用も検討



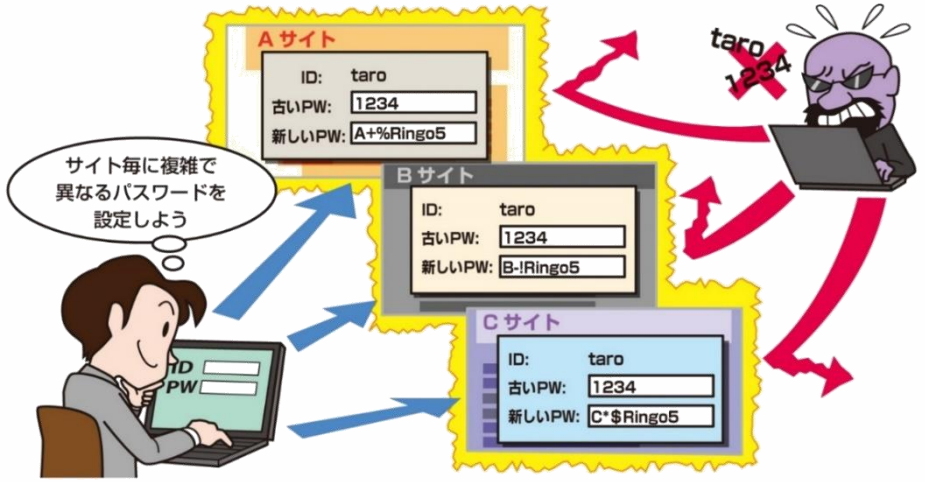
パスワードの管理・認証の強化

- **推測されにくいパスワードを設定　（長く複雑に）**
- **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

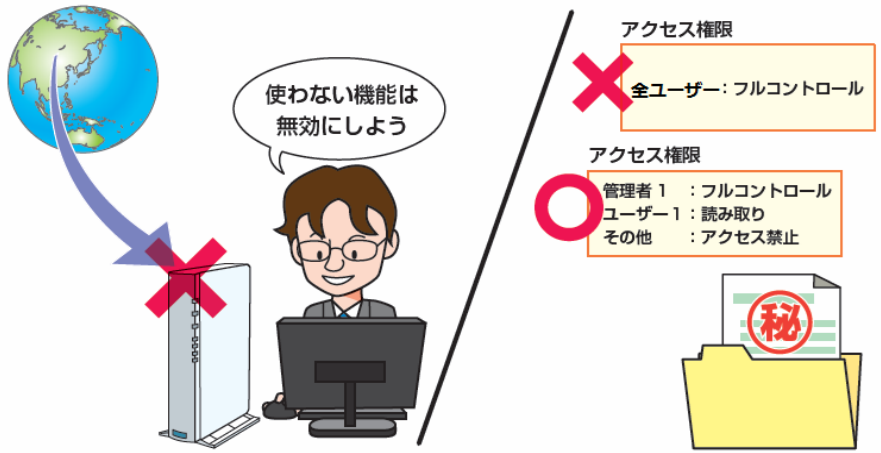
パスワード管理が大変…
→パスワード管理ソフトの利用も有効



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



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**
  - 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

情報セキュリティ対策の基本＋α

- 昨今はクラウドサービスの利用も一般的になってきている
- クラウドサービスの利用を想定した＋αの対策を行い備える必要がある

備える対象	情報セキュリティ対策の基本＋α	目的
インシデント全般	責任範囲の明確化（理解）	インシデント発生時に誰（どの組織）が対応する責任があるのかを明確化（理解）する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	仕様変更により意図せず変更された設定を適切な設定に直す（設定不備による情報漏えいや攻撃への悪用を防止する。）

共通対策

- 10大脅威で取り上げた脅威への対策の中で、複数の脅威に有効なものをピックアップ

複数の脅威に有効な対策
パスワードを適切に運用する
情報リテラシー、モラルを向上させる
メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
適切な報告/連絡/相談を行う
インシデント体制を整備し、対応を行う
サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う
適切なバックアップ運用を行う

4. 参考情報/資料紹介

中小企業の情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策ガイドライン(IPA)
https://www.ipa.go.jp/security/guide/sme/about.html

- 情報セキュリティ対策の必要性、情報を安全に管理する具体的な手順等を分かりやすい言葉で示したガイドライン
- 各種付録も充実

→・情報セキュリティ5か条
・情報セキュリティ基本方針（サンプル）
・5分でできる！情報セキュリティ自社診断
・情報セキュリティハンドブック（ひな形）
・情報セキュリティ関連規程（サンプル）
・中小企業のためのクラウドサービス安全利用の手引き
・リスク分析シート
・中小企業のためのセキュリティインシデント対応手引き

組織における内部不正防止ガイドライン

組織における内部不正防止ガイドライン(IPA)
https://www.ipa.go.jp/security/guide/insider.html

- 内部不正の防止および早期発見、被害拡大防止のためのガイドライン
- 状況的犯罪予防を応用した対策を提示
- 近年施行された法律およびテレワーク普及等の事業環境の変化を踏まえた改訂版(第5版)を2022年4月に公開
- 内部不正チェックシートや英語版も公開

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しています**

情報セキュリティ10大脅威 2024
https://www.ipa.go.jp/security/10threats/10threats2024.html

☆**情報セキュリティ10大脅威 2024**
→個人編、組織編、コラム、「情報セキュリティ対策の基本」と「共通対策」

☆**情報セキュリティ10大脅威の活用法**

☆**情報セキュリティ10大脅威 2024 セキュリティ対策の基本と共通対策**
→解説書から切り出したもの

☆**情報セキュリティ10大脅威 2024 知っておきたい用語や仕組み**（6月公開予定）

- **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

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)

情報セキュリティ10大脅威 2024
https://www.ipa.go.jp/security/10threats/10threats2024.html

組織編

個人編

個人編[一般利用者向け]は6月公開、組織編[英語版]は7月公開予定です