情報セキュリティ10大脅威とその対策

モバイルコンピューティング推進コンソーシアム様
MCPC　情報セキュリティセミナー

2025年06月11日

情報処理推進機構 (IPA)
セキュリティセンター
小山　明美

IPA Better Life with IT

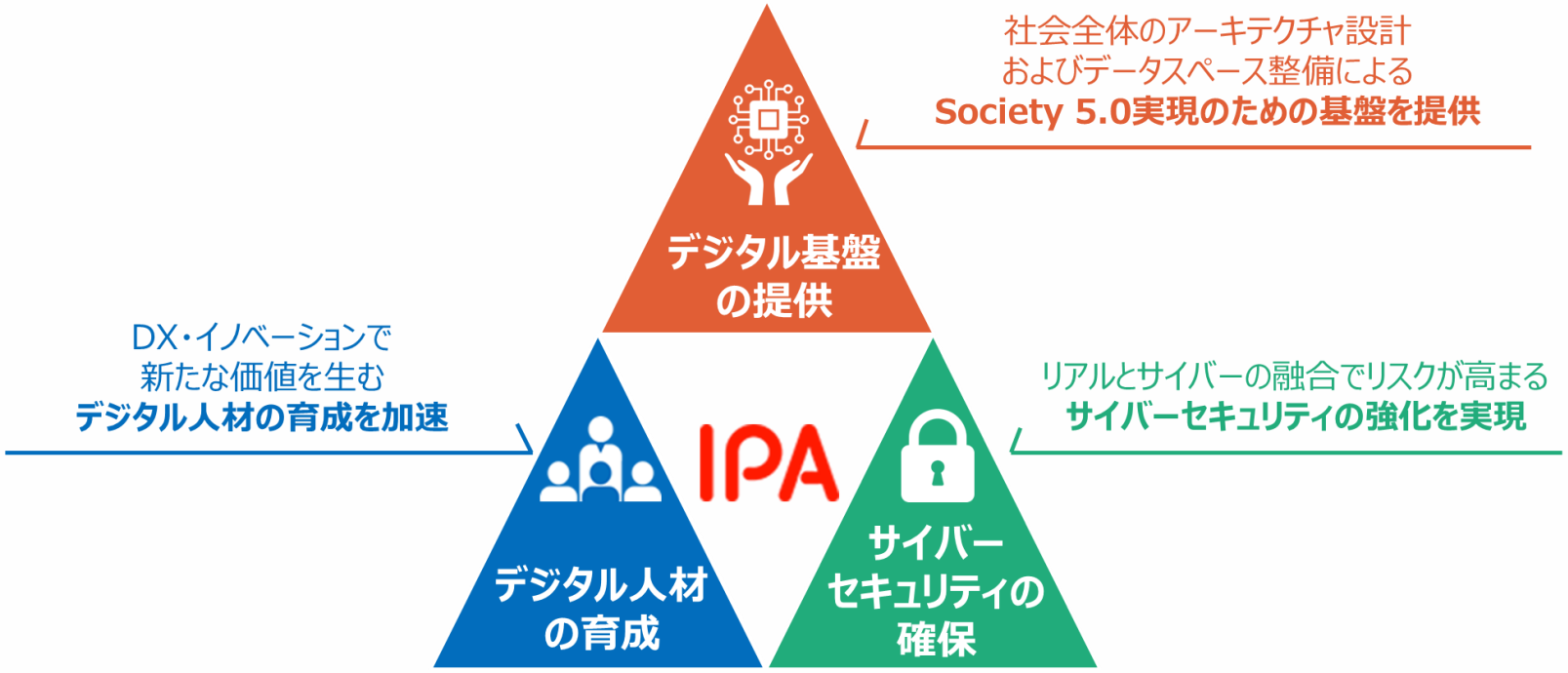
アジェンダ

1. 情報セキュリティ10大脅威とは
2. 脅威の紹介
3. 対策のまとめ
4. 参考情報/資料紹介

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。

普及啓発／地域・中小企業支援

- 地域・中小企業支援
  - セキュリティ自己宣言制度
  - サイバーセキュリティお助け隊
  - セキュリティ相談窓口
- 普及啓蒙コンテンツの発信
  - セキュリティ10大脅威
  - 情報セキュリティ白書
  - AIセキュリティ調査

相談受付件数12,787件（2024年）

SECURITY ACTION
セキュリティ対策自己宣言
累計宣言数 約39万件
（2024年12月）

サイバーセキュリティ お助け隊

サイバー攻撃の検知分析／対処支援

- サイバー情勢の地政学分析
- 標的型サイバー攻撃の対策支援
- 情報共有（攻撃対策情報、脆弱性情報、マルウェア・不正アクセス届出）
- 不正通信監視（独法等）
- サイバー事故原因究明

J-CRAT
初動対応支援
366件
（2023年）

JVN iPedia
脆弱性データベース
約22万件登録（2024年12月）

J-CSIP
情報共有枠組
業界数13（組織数279）
（2023年12月現在）

ガイドライン策定／セキュリティ評価・認証

- セキュリティガイドライン（中小企業向け、内部不正対策等）
- 情報セキュリティ監査・評価
  - 情報セキュリティ監査（独法等）、政府システム監査
  - クラウドセキュリティ評価（ISMAP）
  - 制御システムリスクアセスメント支援
- 評価認証・暗号
  - IoT製品セキュリティラベリング（JC-STAR）、JISEC
  - 暗号動向調査

JC-STAR

CRYPTREC
Cryptography Research and Evaluation Committees

セキュリティ人材育成

- 国家資格「情報処理安全確保支援士」
  登録者数22,845名（2024年10月1日時点）
- 中核人材育成プログラム
  累計435名修了（2017年～）
- 若手人材発掘（セキュリティ・キャンプ）
  累計1,232名受講（2004年度～）
- 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)
- マルウェア・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

- 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つの立場から脅威を解説

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～)
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	6年連続9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
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	2020年	6年連続6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
ネット上の誹謗・中傷・デマ	2016年	10年連続10回目
フィッシングによる個人情報等の詐取	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
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
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

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 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

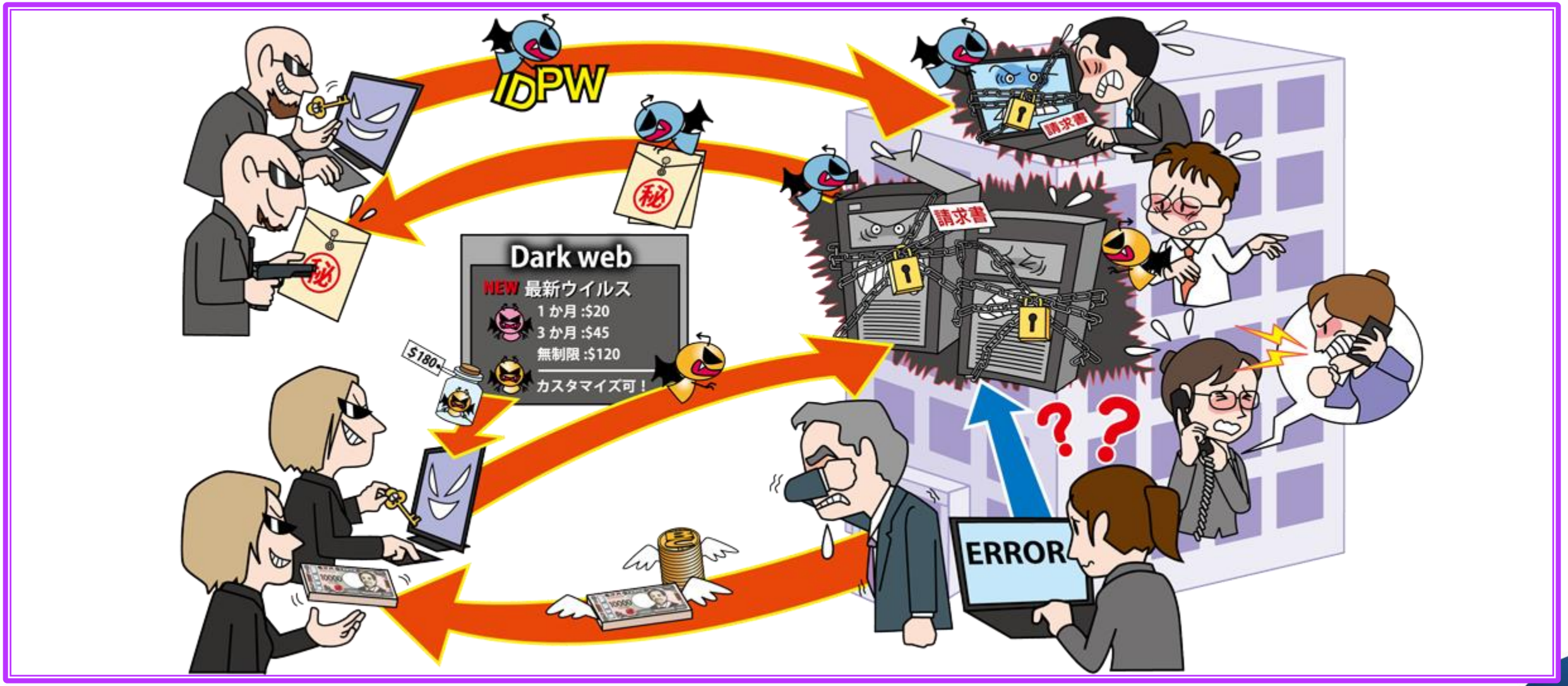
常連の脅威ばかり。
つまり、脅威に対して組織的な対策ができていない。
手口を知り、基本的な対策を行うことが重要

海外からの脅威・攻撃に
注目が集まっている

2．脅威の紹介

- ランサム攻撃による被害
- サプライチェーンや委託先を狙った攻撃
- 内部不正による情報漏えい等

ランサム攻撃による被害



【概要】ランサム攻撃による被害

- **ランサムウェアとは？**
  - **Ransom(身代金)**と**Software**を組み合わせた造語
  - マルウェアの一種
  - PCやサーバ上のデータを**暗号化**する

暗号化：データを一定の規則で変換すること
例：アルファベットの一つ隣の文字に変換する

暗号化前：ransomware

暗号化後：sbotpnxbsf

- **ランサムウェア攻撃とは？**
  - 攻撃者がPCやサーバを**ランサムウェア**に感染させる
    → データ**暗号化** → システム停止 → **業務停止**
  - **データの復旧等を条件に**身代金を支払うように**脅迫する**

【概要】ランサム攻撃による被害

● 最近のランサム攻撃の傾向

	攻撃内容	身代金を支払わせる際の脅迫内容
従来型	データ暗号化	データを復元したければ・・・
二重脅迫	機密情報の窃取	機密情報を公開されたくなければ・・・
三重脅迫	DDoS攻撃準備	DDoS攻撃をされたくなければ・・・
四重脅迫	取引先情報の窃取	情報漏えいを取引先に知られたくなければ・・・

・攻撃者は、**身代金が支払われるまで**何重にも脅迫する。
・ランサムウェアを用いずに脅迫をする攻撃
(No Where Ransom)が流行っている。

【手口】ランサム攻撃による被害

ランサムウェアに感染させる手口

- 不正アクセス
  - ・**OSやアプリケーションなどの脆弱性**
  - ・**サーバ等の設定不備**
  - ・**パスワード設定の不備**

悪用 → 攻撃者がPCやサーバに侵入し、ランサムウェアに感染させる

- Webサイトの悪用
  - ・インターネット上に**不正なWebサイト**を用意
  - ・脆弱性があるWebサイトを**改ざん**

ユーザがWebサイトにアクセス → Webサイトからランサムウェアをダウンロードして実行すると、感染する。

- メールの悪用
  - ・メール本文の**不正なWebサイトへのリンク**を開かせる
  - ・**添付ファイルを開かせる**ことでPCをランサムウェアに感染させる

【事例１】ランサム攻撃による被害

- **システムが停止し、情報が漏えいしたケース**
  - 2024年6月、大手出版社及びその関連会社のサーバがランサムウェアに感染
  - **データ暗号化**によりクラウドサービスを**提供できなくなり、復旧に約2ヶ月かかった**
  - **254,241件**の**個人情報**が**漏えい**
  - フィッシング※により流出した従業員アカウントを使った**不正アクセス**が原因

    ※本物のWebページにそっくりな偽サイトを作り、そこにID/PW等を入力させて詐取する詐欺行為

【出典】
ランサムウェア攻撃による情報漏洩に関するお知らせ（株式会社KADOKAWA）
https://group.kadokawa.co.jp/information/media-download/1356/d3f77b589c58d083/
漏洩情報の拡散行為に対する措置ならびに刑事告訴等について（株式会社KADOKAWA）
https://www.kadokawa.co.jp/topics/12010/
KADOKAWAグループへのサイバー攻撃や悪質な情報拡散についてまとめてみた(piyolog)
https://piyolog.hatenadiary.jp/entry/2024/08/19/074417#f-897d5d27

【事例２】ランサム攻撃による被害

- **RaaS(Ransomware as a Service)が利用されたケース**
  - 2024年6月、IT企業の社内システムの複数のサーバがランサムウェアに感染し、データが暗号化されてしまった
  - 被害を受けたサーバに個人情報が保存されていたため、情報流出の可能性は完全には否定できなかった
  - **VPNルータの設定不備**及び**サーバの脆弱性の悪用**が原因
  - ”Phobos”という**RaaS**で用いられるランサムウェアが使われた

【出典】
弊社内ネットワークへの外部からの不正アクセス被害の発生について（第一報）（株式会社ヒロケイ）
https://www.hirokei.co.jp/news/646/
弊社内ネットワークへの外部からの不正アクセス被害の発生について（第二報）（株式会社ヒロケイ）
https://www.hirokei.co.jp/news/649/
弊社内ネットワークへの外部からの不正アクセス被害の発生について（第三報）（株式会社ヒロケイ）
https://www.hirokei.co.jp/news/668/

【補足】ランサム攻撃による被害

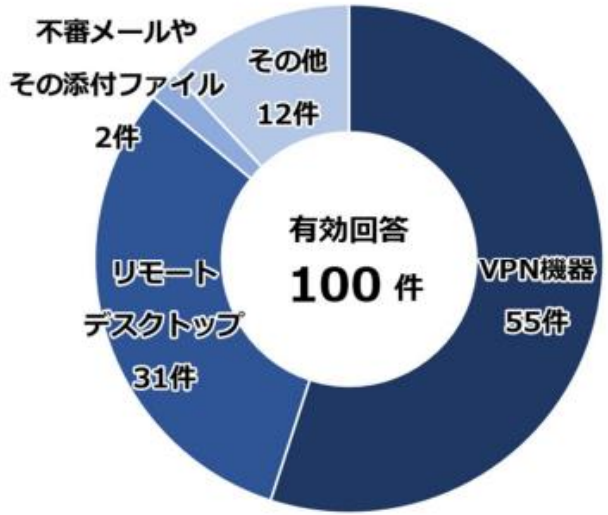
- **ダークウェブ**
  - 通常のブラウザでは検索できないWebサイト
  - サイバー攻撃をするためのツールや個人情報等が売買される。
    また、サイバー攻撃の代行サービスも提供される。具体例を以下に示す。

攻撃手段	売買や提供されるもの
フィッシング	フィッシングサイト作成ツール、フィッシングサイトの作成代行サービス
マルウェア	ボットネット、ランサムウェア、ランサムウェア攻撃代行サービス(RaaS)
不正アクセス	不正アクセスができたアカウント情報、不正アクセス代行サービス(AaaS)
DDoS	DDoS代行サービス(DaaS)
その他	脆弱性悪用ツール、犯罪集団募集サービス

【傾向】ランサム攻撃による被害

狙われ続けるリモートワーク環境

- 2024年の国内の**ランサムウェア被害**における感染経路は、VPN機器からの侵入が55%、リモートデスクトップからの侵入が31%と**8割以上がリモートワーク環境の脆弱性に起因**



【出典】
令和6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/R6/R06_cyber_jousei.pdf

【対策】ランサム攻撃による被害

被害の予防(不正アクセス対策、Webサイトへの対策)

- **脆弱性対策**を行う
  - ・**ソフトウェア資産を把握**し、**脆弱性情報の収集**及び**修正プログラムの適用(アップデート)**を行う
  - ・**サポート切れ**のOSやアプリケーションは利用しない
    ※脆弱性が発見されても基本的に修正プログラムは公開されない
- **認証を強化**する
  - ・容易に推測できるパスワード(“password”等)を使わない
  - ・ネットワークレベル認証(NLA)
  - ・多要素認証
- **フィルタリングソフト**や**セキュリティ製品**を導入する
  - ・社外の不審なWebサイトへの、社内からのアクセスをブロックする

【対策】ランサム攻撃による被害

被害の予防(メールへの対策)

- **不審なメールのリンクや添付ファイルを安易にクリックしない**

①メールの送信元の確認
- 送信元の**メールアドレス**のドメインの確認
- **電子署名**の有無

②メール本文の内容の確認
- **緊急性を強調**しているものには要注意
- 本文に書かれた**リンク**には要注意

③不審な**添付ファイルの有無**の確認
- 拡張子がexeのファイルなど、少しでも不審な点がある添付ファイルは開かない
- もし、Officeファイルを開いてしまった場合でも、**マクロは実行しない**
  →「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

- **メールに返信しない。**
- **メールに記載されている電話番号**に電話しない。

「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

少しでも不審な点があれば**正規の窓口から確認を**

【対策】ランサム攻撃による被害

被害を最小限に抑えるための予防策

- 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
  - ・**ネットワーク分離**
  - ・共有サーバ等への**アクセス権の最小化**
- 重要なファイルを含むシステム全体の**バックアップ**を定期的に取得
  - ・暗号化されたデータの**復旧**が可能
  - ・**ログ**をバックアップしておけば、障害調査が進みやすくなる。
  - ・バックアップデータは**複数用意**
    ※災害対策のため、**複数の媒体**でバックアップを取り、一つは**オフサイトで保管**
  - ・バックアップデータの状態を**定期的に確認**
    ※バックアップからの**復旧手順を整備**して**リハーサル**をし、データを復旧できることを確認しておく

【出典】
令和6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/R6/R06_cyber_jousei.pdf

【対策】ランサム攻撃による被害

被害を受けた後の対応

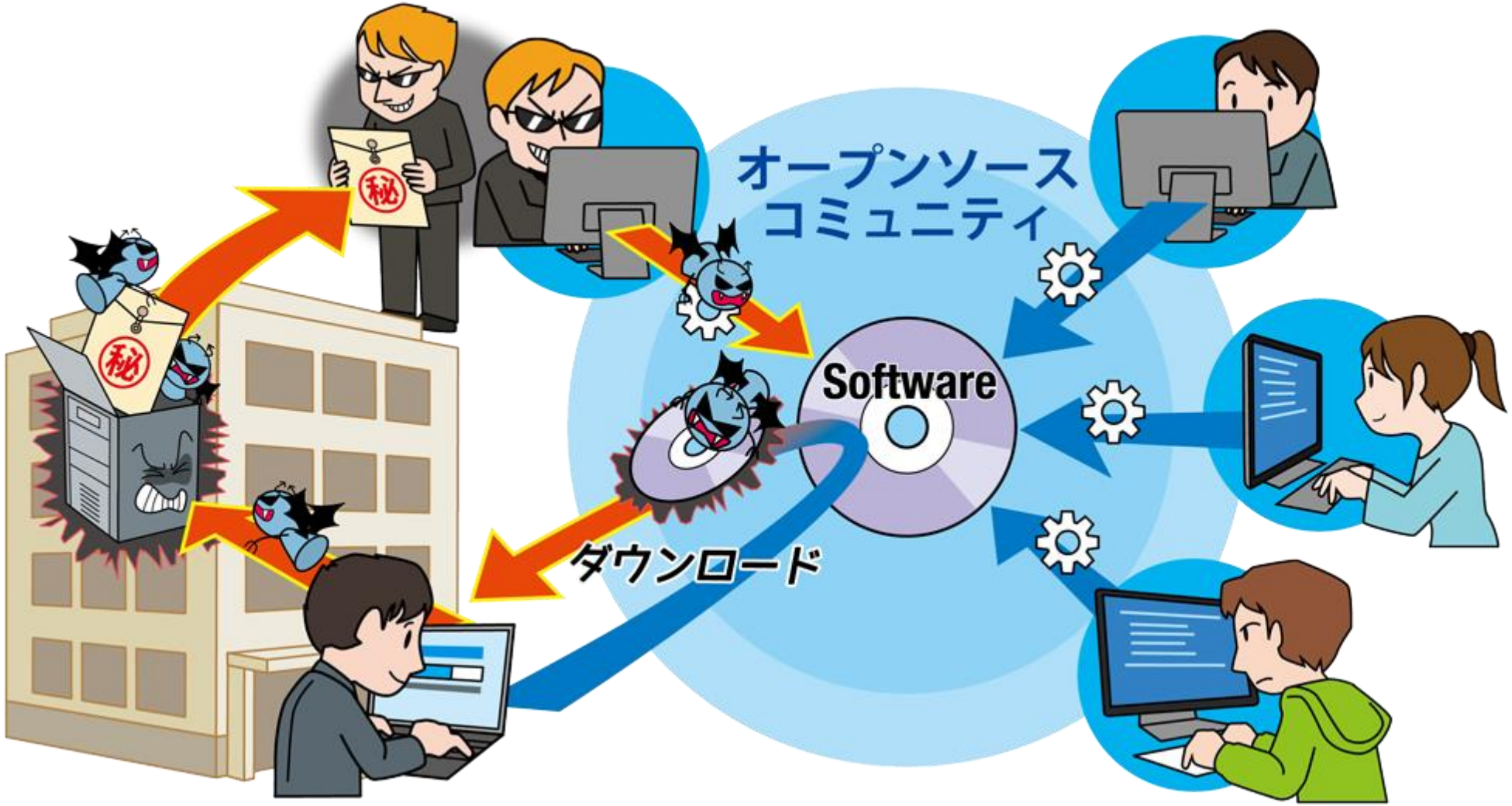
- 発見者による適切な初動対応
  - ・マルウェア感染が疑われる機器を**ネットワークから切断**
  - ・組織の規定に従い**エスカレーション**
- 担当部署や外部協力先による影響調査および原因の追究
- 復旧作業
  - ・バックアップからの復旧
  - ・復号ツールの活用

  [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

・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
・身代金要求に応じる組織として今後も標的に

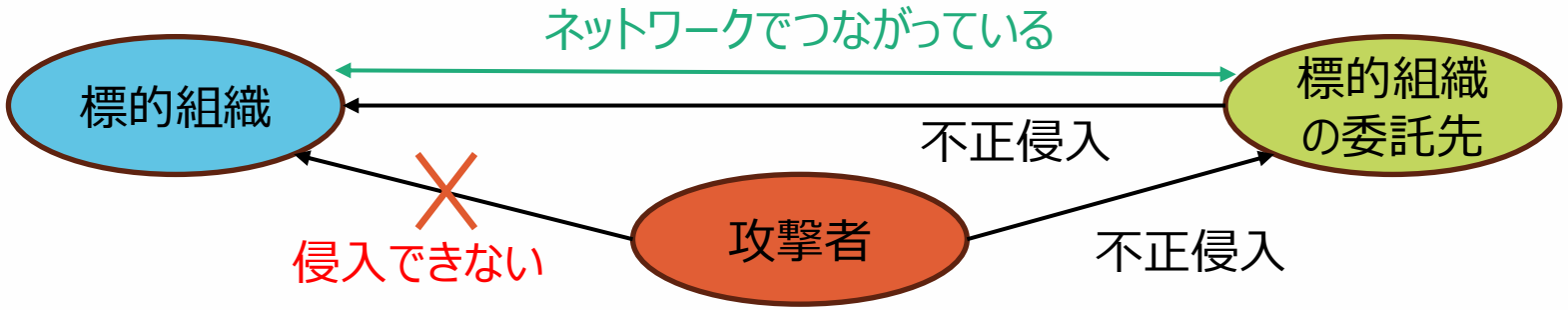
サプライチェーンや委託先を狙った攻撃



【概要】サプライチェーンや委託先を狙った攻撃

サプライチェーン攻撃とは？

サプライチェーンの中で**セキュリティ対策が甘いところを狙った攻撃**



2種類のサプライチェーン

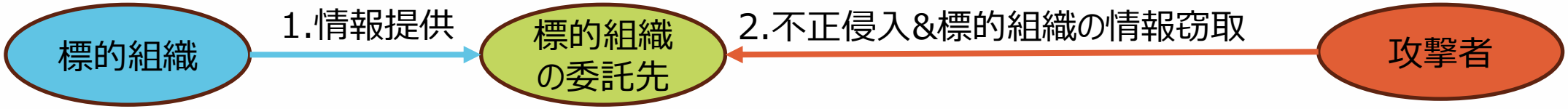
- 調達、製造、在庫管理、物流、販売、業務委託先等の一連の商流
  - ・取引先、委託先、グループ企業
  - ・利用している外部サービス
- ソフトウェア開発のライフサイクルに関わるサプライチェーン(**ソフトウェアサプライチェーン**)

【手口】サプライチェーンや委託先を狙った攻撃

● 企業間のつながりを利用した標的組織への攻撃

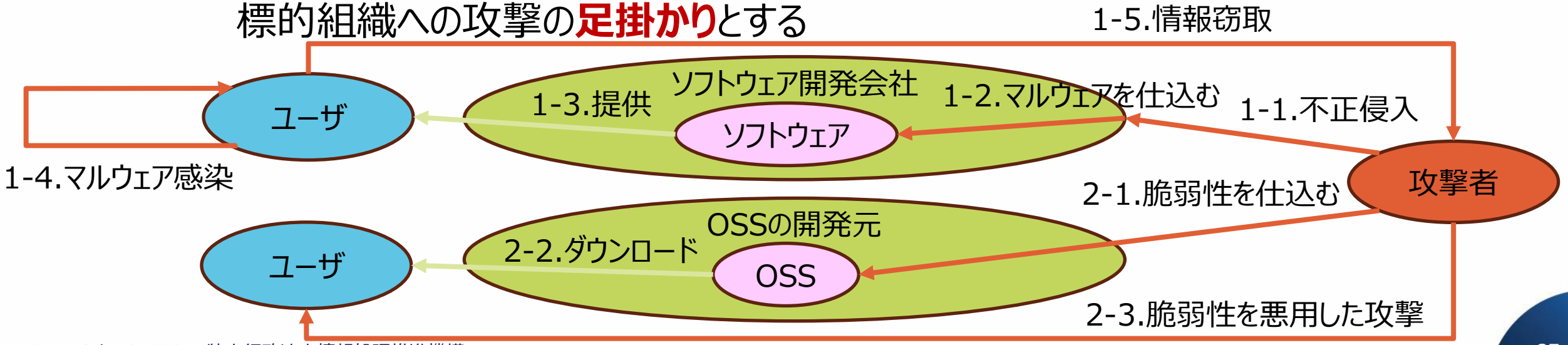
- 標的組織と**ネットワークが繋がっているグループ会社や委託先**に不正アクセス
  →・**標的組織の認証情報を委託先で窃取**して標的組織に侵入

・標的組織が**委託先に提供している情報を窃取**する



【手口】サプライチェーンや委託先を狙った攻撃

- **ソフトウェアサプライチェーンを足掛かりにした標的組織への攻撃**
  - **ソフトウェアの開発会社等**を攻撃
    →ソフトウェアの開発会社が提供する**ソフトウェアを改ざんしてマルウェアを仕込み**、**ソフトウェアの導入やアップデート適用**を行った組織をマルウェアに感染させる
  - **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】サプライチェーンや委託先を狙った攻撃

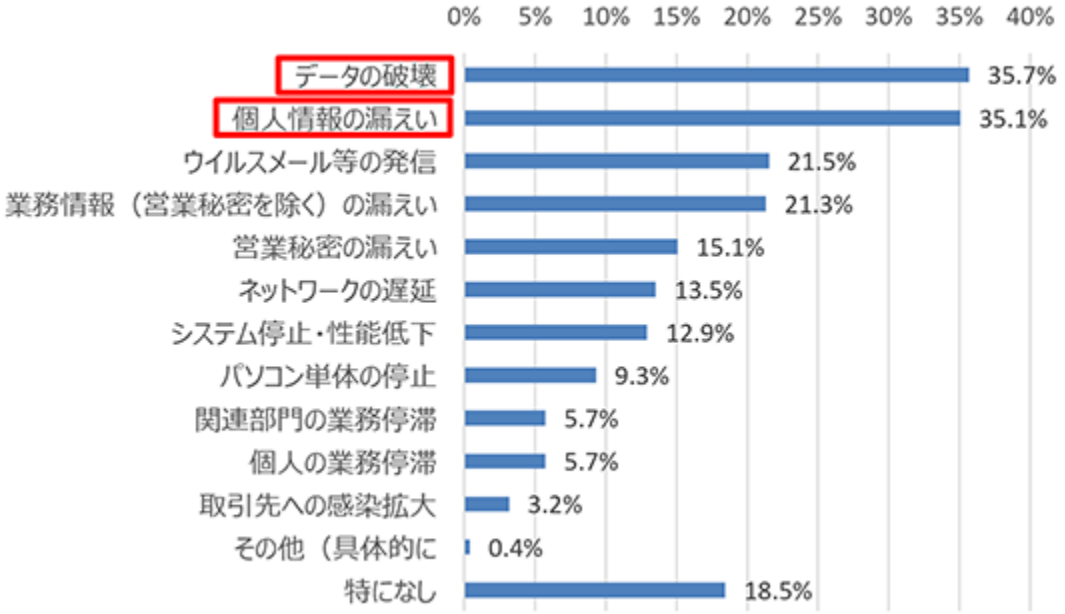
業務委託先業者からの顧客情報漏えい

- 2024年5月、複数の自治体等から印刷業務を委託された企業が**顧客から預かっている個人情報**を社外流出させていた
- 2024年6月、攻撃者グループのリークサイトに、流出した個人情報をダウンロードするためのURLが記載されたことで事件が発覚
- 原因は**業務委託先のVPN機器の不正アクセス**にあった
- 自治体だけでも**50万件以上**もの個人情報が流出していた

【出典】
不正アクセスによる個人情報漏えいに関するお詫びとご報告（株式会社イセトー）
https://www.iseto.co.jp/news/news_202410.html
報道発表資料「委託業者のランサムウェア被害に伴う個人情報漏えい事案」に係る市民への対応について（豊田市）
https://www.city.toyota.aichi.jp/pressrelease/1060027/1060257.html
印刷業務委託先のランサムウェア被害について（第3報）（徳島県）
https://www.pref.tokushima.lg.jp/ippannokata/kurashi/zeikin/7242743/
委託業者におけるコンピューターウイルス感染について（和歌山市）
https://www.city.wakayama.wakayama.jp/kurashi/zeikin/1001083/1058780.html

サイバーインシデントによる被害

- 過去3期内で、サイバーインシデントが発生した企業における被害額の平均は**73万円**（うち9.4%は100万円以上）、
  復旧までに要した期間の平均は**5.8日**（うち2.1%は50日以上）

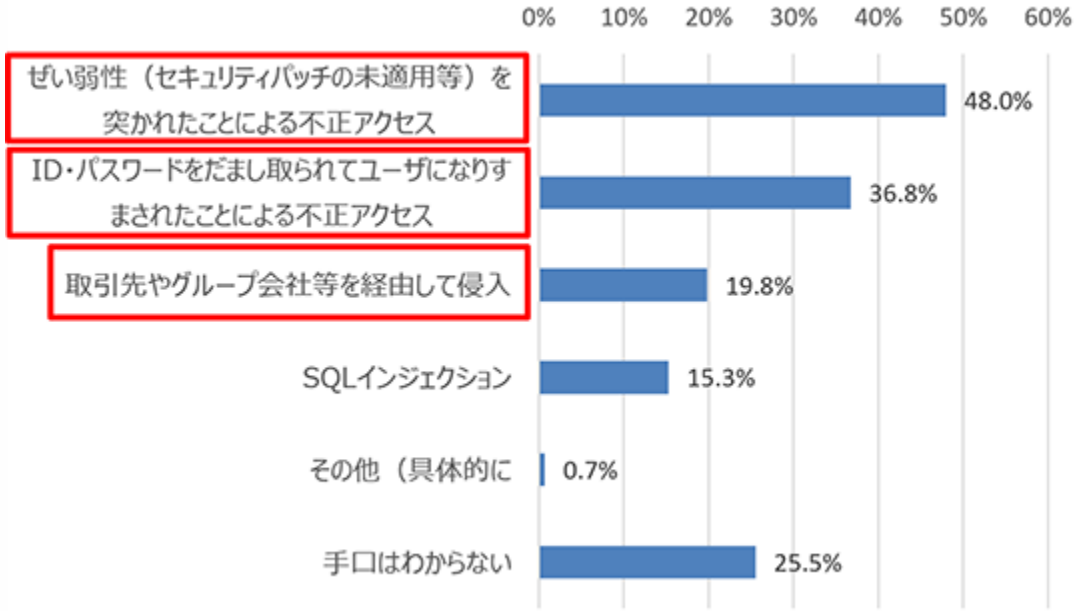


質問：貴社でサイバーインシデントによる影響で、生じた被害について教えてください。（MA）(n=975)

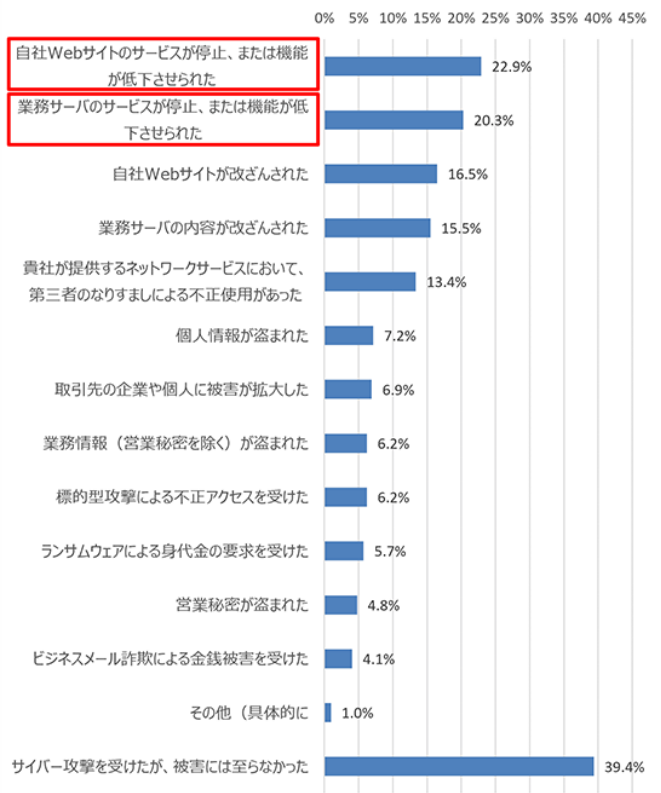
IPA「2024年度 中小企業における情報セキュリティ対策に関する実態調査」
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html

不正アクセスの手口・被害の内容

- 不正アクセスされた企業の**約５割**が脆弱性を突かれ、他社経由での侵入も**約２割**



質問：貴社が受けたサイバー攻撃の手口について教えてください。（MA）(n=419)

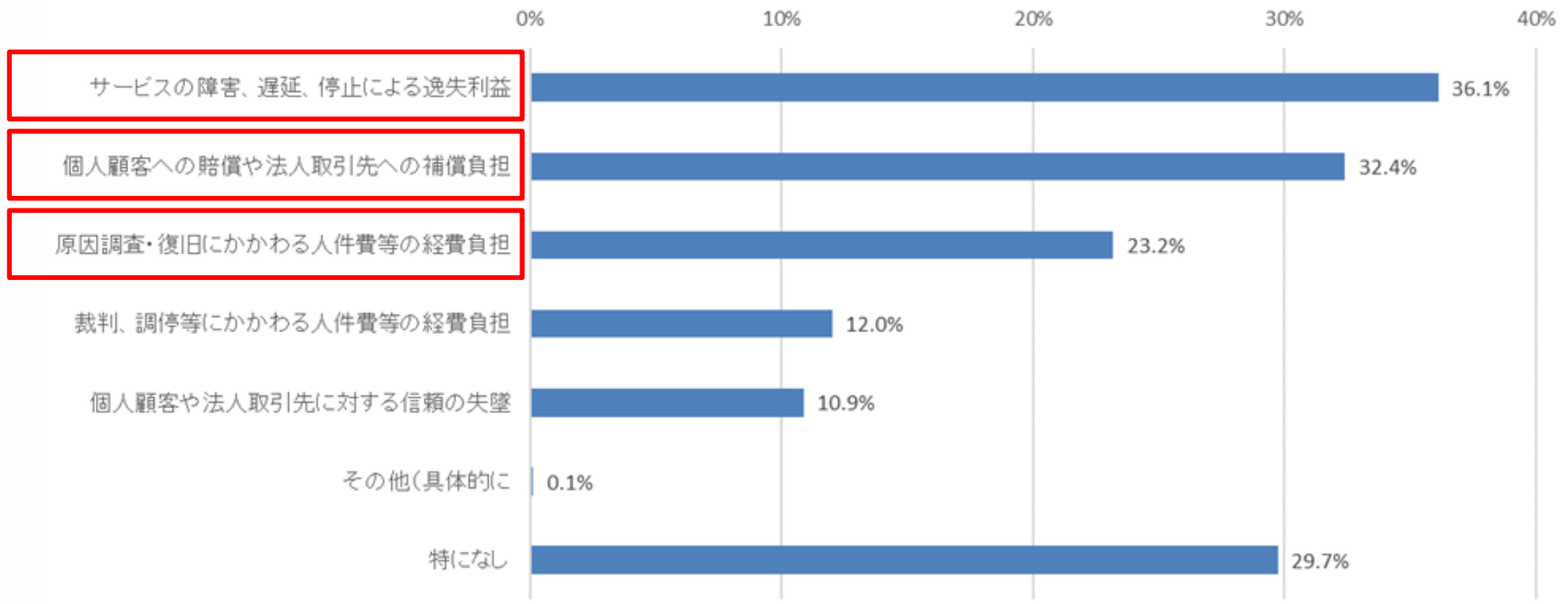


質問：貴社が受けたサイバー攻撃の被害について教えてください。（MA）(n=419)

IPA「2024年度 中小企業における情報セキュリティ対策に関する実態調査」
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html

サイバーインシデントによる取引先への影響

- サイバーインシデントにより取引先に影響があった企業は**約７割**



質問：サイバーインシデントにより貴社の取引先（サプライチェーン）に影響はありましたか。影響が及んだ場合はその内容について教えてください。（MA）（n=975）

IPA「2024年度 中小企業における情報セキュリティ対策に関する実態調査」
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html

【要因】サプライチェーンや委託先を狙った攻撃

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、管理できていない
  →そもそも**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、
  委託元から再委託先などのセキュリティ対策管理は難しい

サプライチェーン攻撃を受けた後の対応が難しい要因

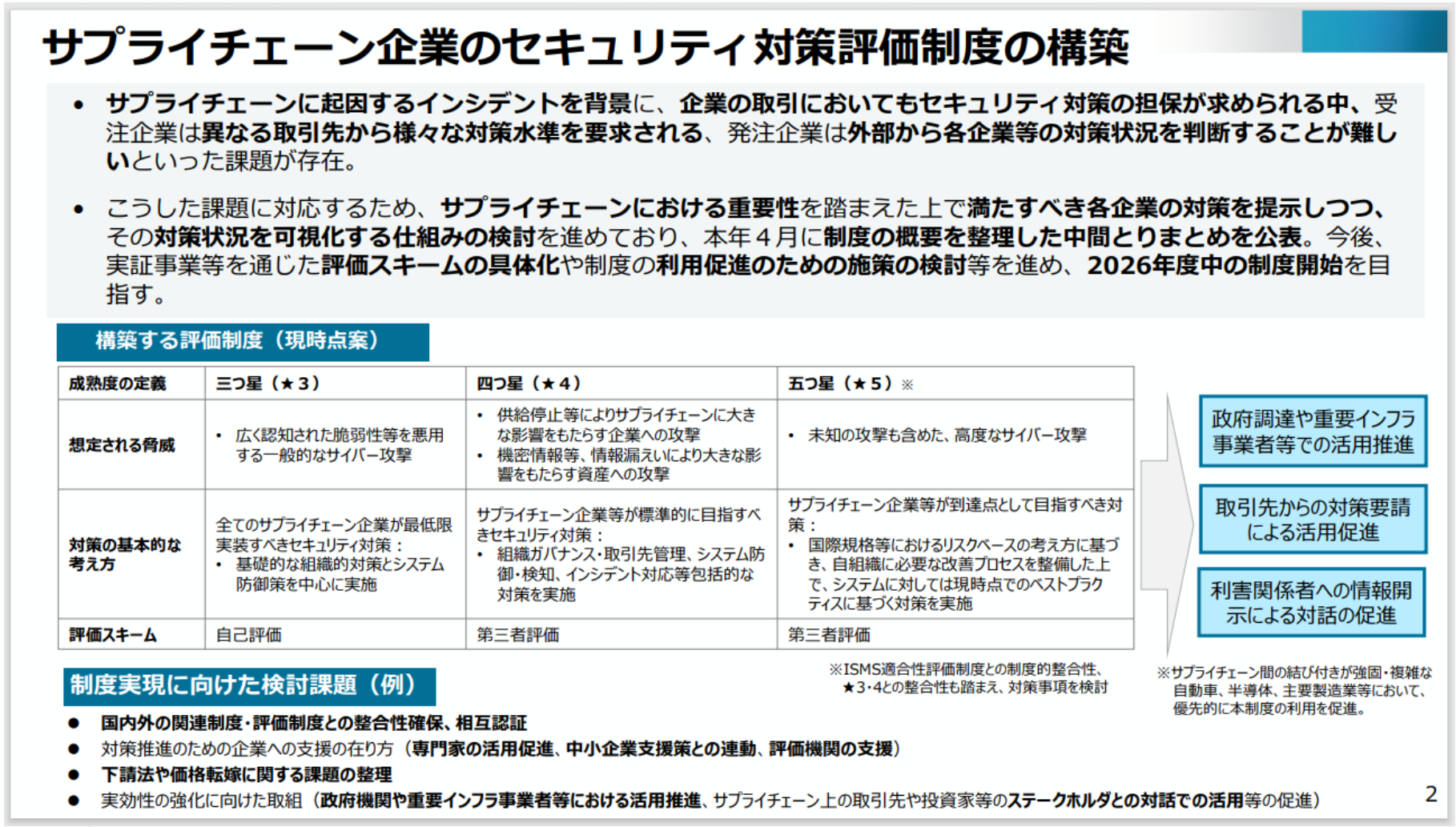
- 情報セキュリティに関する**責任範囲が不明確**
  →契約時に情報セキュリティに関する**責任範囲を明確に定めていない**場合、
  インシデント発生時の対応がスムーズにできない

【対策】サプライチェーンや委託先を狙った攻撃

- **被害の予防(サプライチェーン攻撃の被害を受けないための対策)**
  - 自組織における情報セキュリティ対策を実施する。
    →ISMS、Pマーク、SOC2、ISMAP等に**適合した運用**をする。また、運用を定期的に見直す。
  - **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
    →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**
    - インシデント発生時の対応や運用方法、補償内容
    - 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

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

検討中のサプライチェーン企業評価制度



サプライチェーン企業のセキュリティ対策評価制度の構築

- **サプライチェーンに起因するインシデントを背景**に、**企業の取引においてもセキュリティ対策の担保が求められる中**、受注企業は**異なる取引先から様々な対策水準を要求される**、発注企業は**外部から各企業等の対策状況を判断することが難しい**といった課題が存在。
- こうした課題に対応するため、**サプライチェーンにおける重要性**を踏まえた上で**満たすべき各企業の対策を提示しつつ、その対策状況を可視化する仕組みの検討**を進めており、本年４月に**制度の概要を整理した中間とりまとめを公表**。今後、実証事業等を通じた**評価スキームの具体化**や制度の**利用促進のための施策の検討**等を進め、**2026年度中の制度開始**を目指す。

構築する評価制度（現時点案）

成熟度の定義	三つ星（★３）	四つ星（★４）	五つ星（★５）※
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が標準的に目指すべきセキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等が到達点として目指すべき対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施
評価スキーム	自己評価	第三者評価	第三者評価

※ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

政府調達や重要インフラ事業者等での活用推進
取引先からの対策要請による活用促進
利害関係者への情報開示による対話の促進

※サプライチェーン間の結び付きが強固・複雑な自動車、半導体、主要製造業等において、優先的に本制度の利用を促進。

制度実現に向けた検討課題（例）

- **国内外の関連制度・評価制度との整合性確保、相互認証**
- 対策推進のための企業への支援の在り方（**専門家の活用促進、中小企業支援策との連動、評価機関の支援**）
- **下請法や価格転嫁に関する課題の整理**
- 実効性の強化に向けた取組（**政府機関や重要インフラ事業者等における活用推進**、サプライチェーン上の取引先や投資家等の**ステークホルダとの対話での活用**等の促進）

2

自己評価の仕組みである「SECURITY ACTION」（一つ星及び二つ星）、「JAMA・JAPIA自工会/部工会サイバーセキュリティガイドライン」や国際標準である「ISMS適合性評価制度」等とは相互補完的な制度として発展することを目指す。

2026年度中
制度開始予定

サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（概要）
https://www.meti.go.jp/press/2025/04/20250414002/20250414002-1.pdf

【対策】サプライチェーンや委託先を狙った攻撃

- **被害の予防(サプライチェーン攻撃の被害を受けないための対策)**
  - 取引先や委託先との**連絡プロセスの確立**
  - 委託先組織の管理
    →セキュリティ対策状況や情報管理の実態を確認する
  - 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
    - **OSSの脆弱性情報を収集**し、問題がないかを確認する。
  - 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】サプライチェーンや委託先を狙った攻撃

- **被害を受けた後の対応**
  - 関係各所への報告・連絡・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、原因特定、および再発防止策の策定

内部不正による情報漏えい等

【概要】内部不正による情報漏えい等

- **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
    →・**個人情報の窃取**
    ・機密情報の**改ざん**
    ・**ミスの隠蔽**のための情報削除
- **内部不正による情報漏えい等の影響**
  - **社会的信用の失墜**
  - 損害賠償等による**経済的損失**

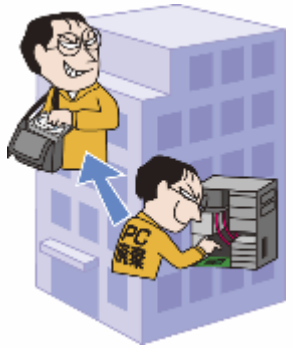
【手口】内部不正による情報漏えい等

内部不正による情報漏えいの手口

- アクセス権限を悪用した重要情報の窃取
  - 付与された**管理者権限**を悪用
  - **必要以上に割り当てられたアクセス権限**を悪用
- 不正にアカウントを使って情報を窃取
  - **共用しているアカウント**を悪用
  - **在職中に使用していたアカウント**を悪用

※**不正に取得された情報と知りながら情報を使用した組織**は、
刑事罰の対象になるおそれがあるので、注意が必要

- 情報の持ち出し方法
  - USBメモリー、HDD、スマホカメラ、紙媒体、メール、クラウドストレージ等



【事例】内部不正による情報漏えい等

- **顧客情報を転職先に持ち出し、営業活動に使用したケース**
  - 2024年8月、不動産会社にて、同社に勤務した元社員が退職時に**顧客情報を不正に持ち出し**てしていたことが発覚
  - 顧客情報には、不動産登記簿に記載されていた氏名、マンション名、部屋番号等の25,406件があった
  - これらの顧客情報は、**転職先のDM(ダイレクトメール)の送付時**に利用されていた
  - 同社は刑事告訴を視野に管轄警察署に相談をしていた

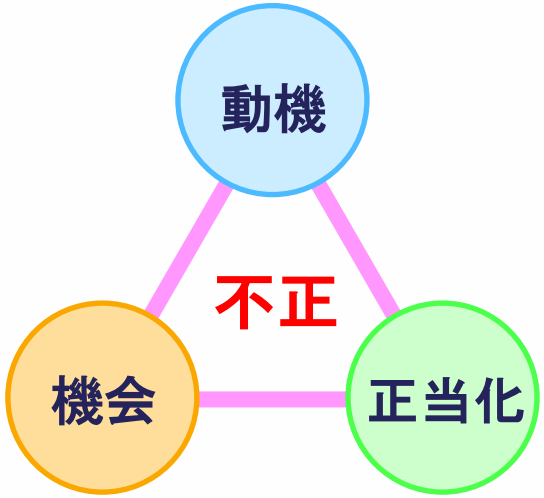
【出典】
従業員による個人情報の不正な持ち出しに関するご報告とお詫び（東急リバブル株式会社）
https://www.livable.co.jp/assets/files/3972

【要因】内部不正による情報漏えい等

- **人が不正行為を働くメカニズム(不正のトライアングル)**

三つの要素がそろうと、人は不正を働く可能性が高まる

- 動機やプレッシャー(不正を働くに至る**背景**がある)
  - お金が必要 / 自分を評価してくれない / 厳しいノルマの達成 / ミスの隠蔽
- 機会(不正を**実行できる環境**がある)
  - 重要情報を閲覧できる / 不正を行っても発覚しにくい
- 正当化(**自分だけ**が悪いわけではない)
  - みんなやっている / 自分を評価してくれない組織が悪い / 転職先の会社のため



【対策】内部不正による情報漏えい等

- **被害の予防(経営者、管理者)**

不正を「やりにくい」、「やると見つかる」、「割に合わない」ようにすることが基本

  - システムやデータへのアクセス権限の管理
    - **最小限の権限付与**、利用者IDの**共用禁止**等の処置、**古いアカウントの削除**などの定期的な棚卸
  - システム操作履歴の監視
    - アクセス履歴や操作履歴等の**ログ、証跡を記録し、監視**する
    - **DLP（情報漏えい対策）等のツール**を導入する
    - **監視していることを従業員に周知**する
  - **物理的管理**の実施(保管場所、入退室管理、持ち出しや持ち込みの管理)
  - 内部不正者に対する**懲戒処分**等を規定した就業規則を整備し**従業員を教育**

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
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
マルウェア感染	**セキュリティソフトの利用**	攻撃をブロックする
設定不備の悪用	**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

パスワードの管理・認証の強化

推測されやすいパスワードを設定するとどうなるのか？

- **悪意のある攻撃者が本人になりすまして、不正アクセスする**

攻撃内容	攻撃詳細	影響
機密情報の窃取	クレジットカード情報の窃取	金銭の不正利用
	住所や電話番号等の窃取	個人情報の売買
	メールアドレスの窃取	詐欺メールの送信
システム情報の改ざん	システムファイルの改ざん	システムの停止
	社内のサーバの改ざん	社外の不正なサイトへアクセスさせる
		不正アプリをダウンロードさせる
		マルウェアをダウンロードさせる
マルウェア感染	ランサムウェア感染	身代金要求
	ボットネットへの感染	DDoS攻撃
その他	関連組織への不正アクセスの足掛かりにする	さらなる不正アクセスの実行
	同一アカウントのシステムへの不正アクセス	さらなる不正アクセスの実行

推測されにくいパスワードの設定が非常に重要

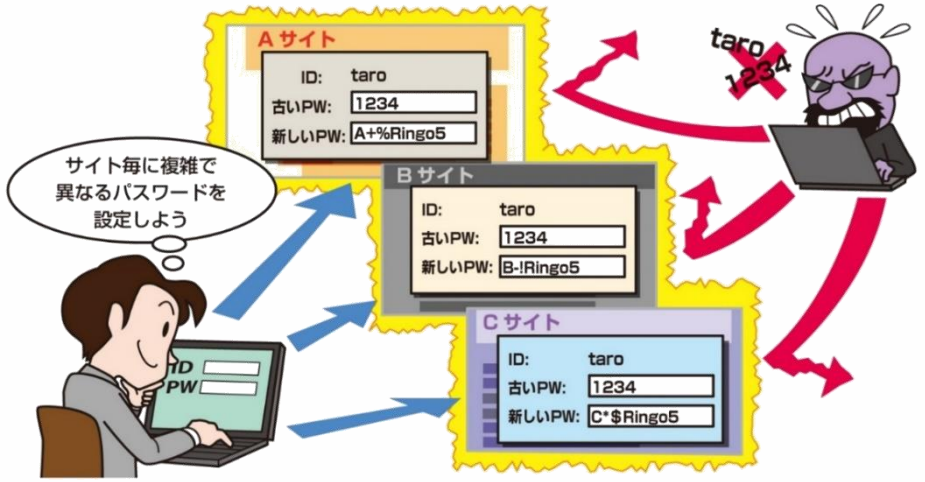
パスワードの管理・認証の強化

- **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**

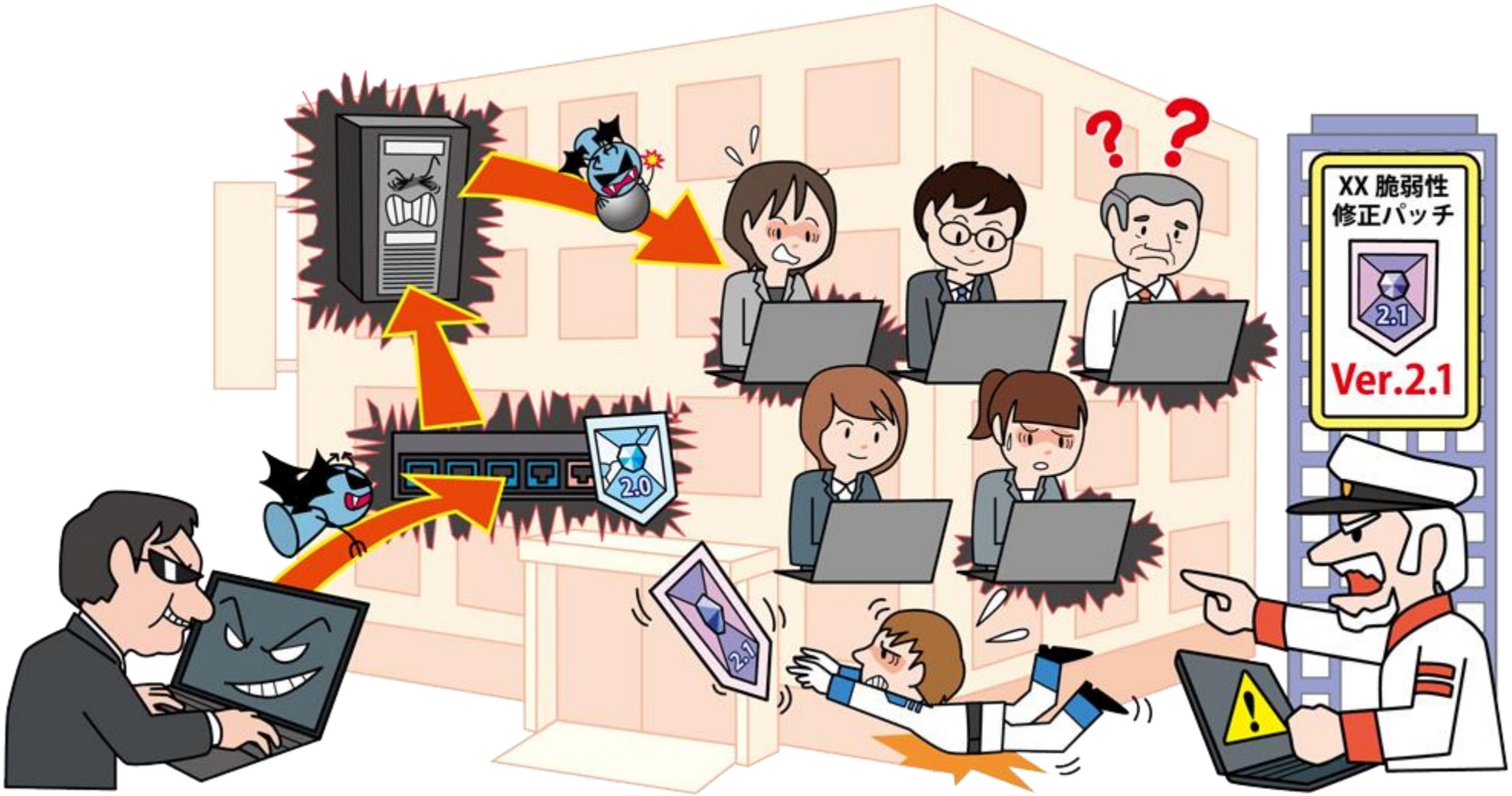
パスワード	悪い点
123456	連続した数字
Password p@ssw0rd	単純な単語や その類似系
taro1202	名前や誕生日
1qaz2wsx	キーボードの縦配列
qwerty	キーボードの横配列

脆弱なパスワードの例

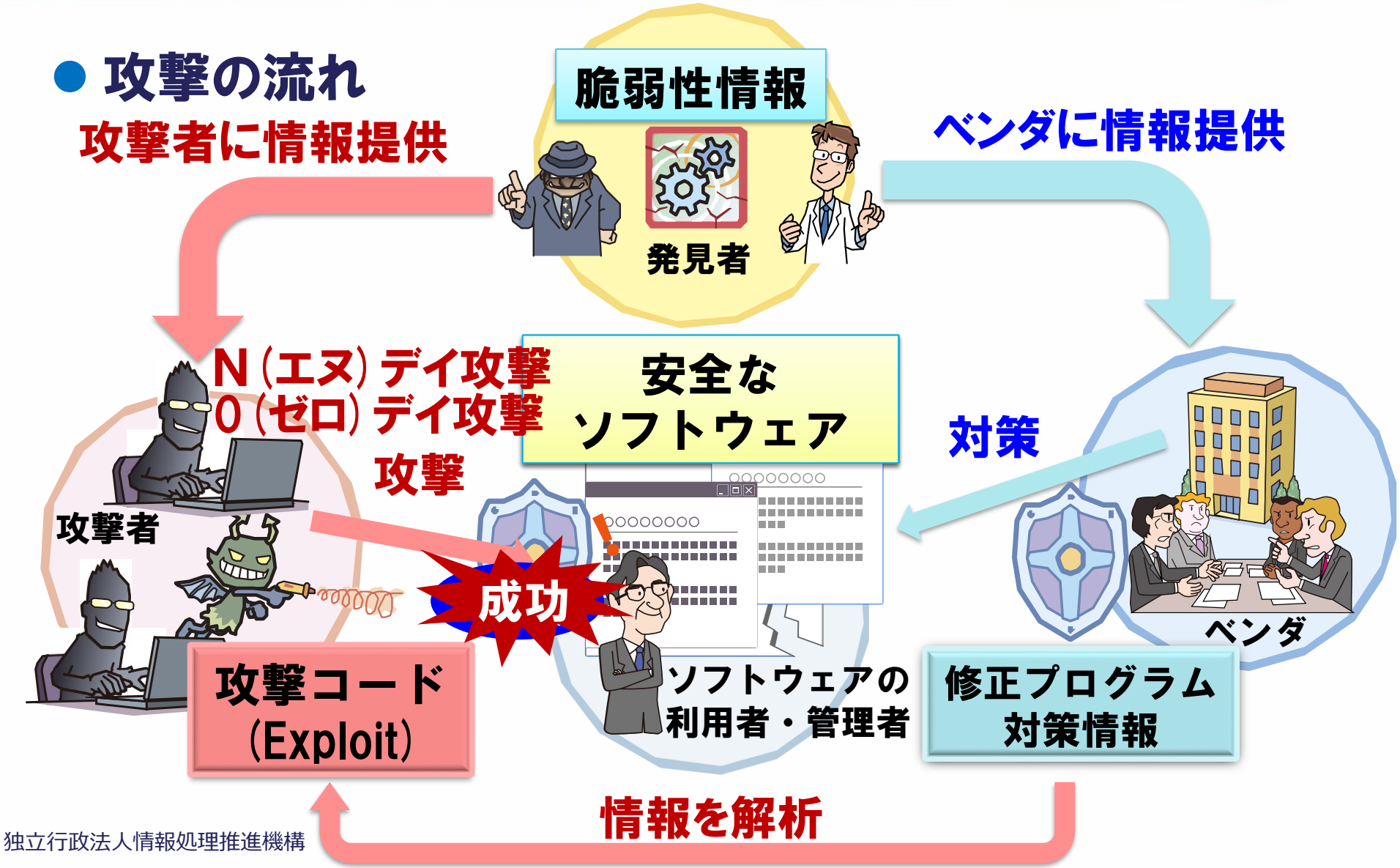
パスワード管理が大変…
→**パスキー**の導入も有効



ソフトウェアの更新

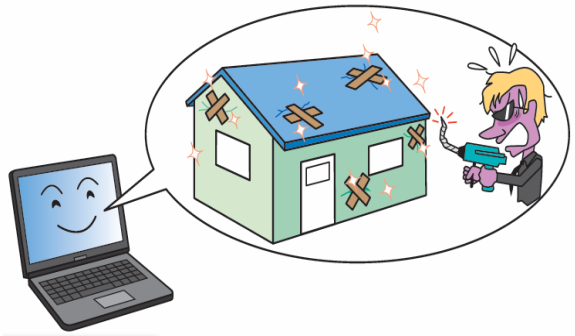


脆弱性を放置するとどうなるのか？



ソフトウェアの更新

- **<u>ソフトウェアの脆弱性の解消には、ソフトウェアのアップデートが必要</u>**
  - 修正プログラムがリリースされて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)

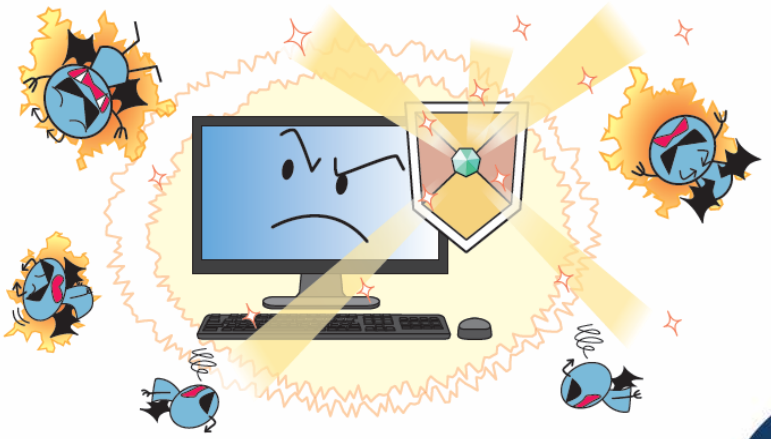


セキュリティソフトの利用

- **マルウェア対策機能でマルウェア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…

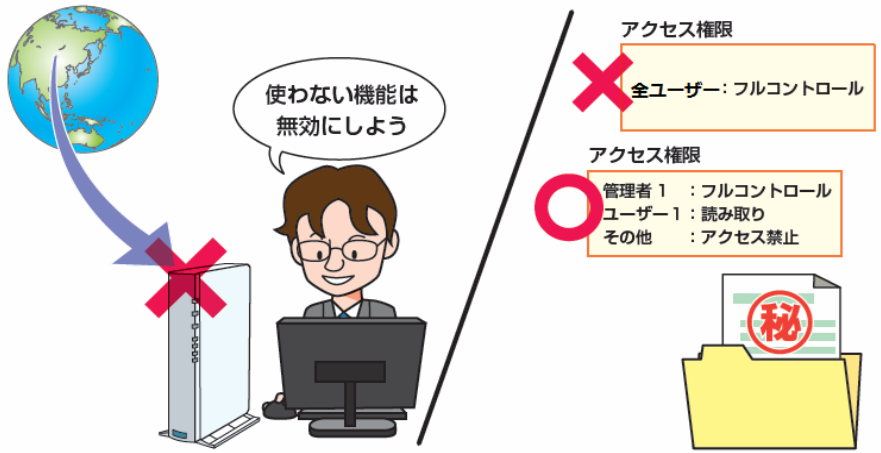
- 最低限、**Windows標準のセキュリティ機能は有効にする（Microsoft Defender）**
- その他**市販のセキュリティソフトの利用**も検討



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**
  - 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

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 (IPA)

- 内部不正防止の重要性や対策の体制、関連する法律などの概要を**易しい文章で説明**
- 「基本方針」「資産管理」「技術的管理」「職場環境」「事後対策」等の10の観点のもと、合計33項目からなる**具体的な対策**
- 自組織の内部不正**対策の状況を把握するためのチェックシート**

IPAサイバーセキュリティ相談窓口

IPAサイバーセキュリティ相談窓口（企業組織向け）
URL　：https://www.ipa.go.jp/security/support/soudan.html
E-Mail: cs-support@ipa.go.jp

- IPAでは企業組織向けに、セキュリティインシデントに関する相談や、マルウェア・不正アクセス・脆弱性情報に関する届出を受け付ける窓口を設けております。セキュリティインシデント等が発生した際などにご活用いただくことができます。

情報セキュリティ10大脅威

- **下記Webページに解説書・簡易説明資料を公開しています**

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　解説書
→「情報セキュリティ対策の基本」、「組織編」、「コラム」、「共通対策」、「個人編(6月公開予定) 」

☆情報セキュリティ10大脅威の活用法
→「組織編」、「個人編(7月公開予定) 」

☆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
→7月公開予定

☆情報セキュリティ10大脅威 2025
簡易説明資料

→ 組織編　公開済み
　個人編　7月末公開予定