IPA Better Life with IT

情報セキュリティ10大脅威 2023

～ 組織編 ～

2023年9月13日
MCPC・情報セキュリティセミナー

独立行政法人情報処理推進機構（IPA）
セキュリティセンター
セキュリティ対策推進部

目次

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

● 情報セキュリティ対策の実現

・ウイルス、不正アクセス等の届出機関
・情報セキュリティの調査研究、普及啓発活動
・標的型サイバー攻撃の情報共有・初動対応の実施

● IT人材の育成

・国家試験「情報処理技術者試験」の実施機関
・IT人材の育成・発掘・スキル認定のとりくみ、若手人材育成

● IT社会の動向分析・基盤構築

・新たなIT社会の動向調査、新しい技術の安全性・信頼性の確保に向けた指針策定など

「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 2023
～組織編～

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

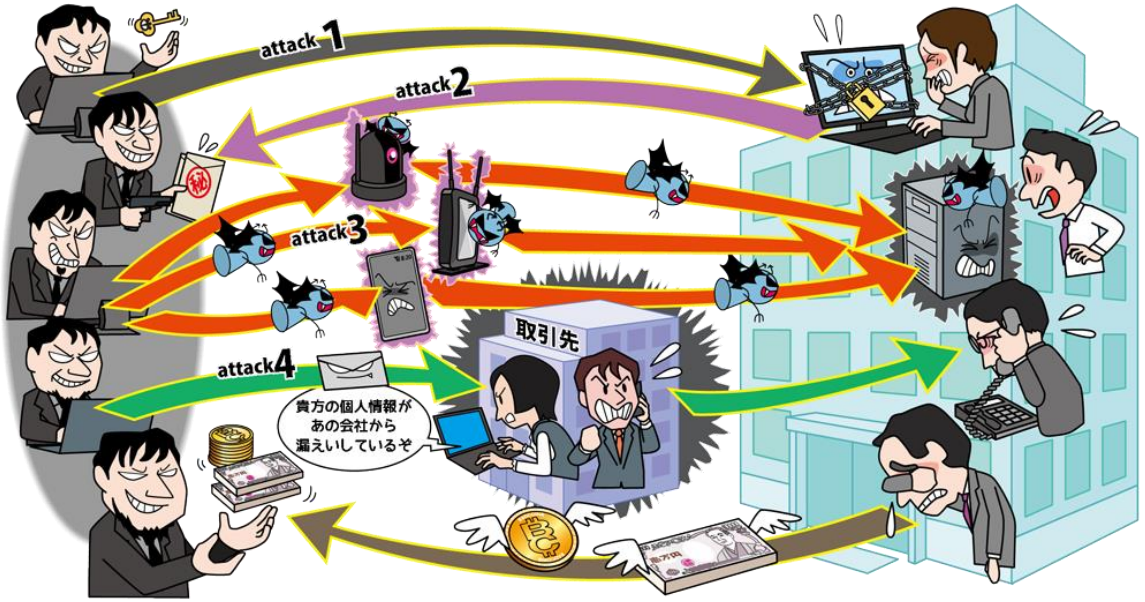
2. 脅威解説

- 1位　ランサムウェアによる被害
- 2位　サプライチェーンの弱点を悪用した攻撃
- 3位　標的型攻撃による機密情報の窃取
- 4位　内部不正による情報漏えい

1

ランサムウェアによる被害

【1位】ランサムウェアによる被害



- ランサムウェア攻撃でシステム停止や情報窃取等の被害を受ける
- 復旧や窃取された情報の削除等と引き換えに金銭を要求される
- システムへの被害が深刻な場合、事業継続が困難になるおそれも

【1位】ランサムウェアによる被害

● 攻撃手口①-1

・ランサムウェアに感染させる（組織内の個人を狙う）

- 業務に関するメールを装い不正なファイルを添付する

  →・実行ファイル（拡張子　.exe、.js 等）

  ・マクロを実行するとウイルスに感染するよう細工された Officeファイル（Word、Excel、PowerPoint 等）

  ・PDFファイル　　等が使われる

- 悪意あるウェブサイトにアクセスさせる

  →・標的組織がよく使うウェブサイトに脆弱性がある場合、ウイルスがダウンロードされるよう改ざんする

  ・メールで誘導する

【1位】ランサムウェアによる被害

● 攻撃手口①-2

・ランサムウェアに感染させる（機器やネットワークを狙う）

- 標的組織が利用しているソフトウェアや機器の**脆弱性**を悪用してウイルスに感染させる

  →OSの脆弱性を悪用し、同じ脆弱性を持つPCに**自動的に感染を拡大**させていく機能を持つランサムウェアも

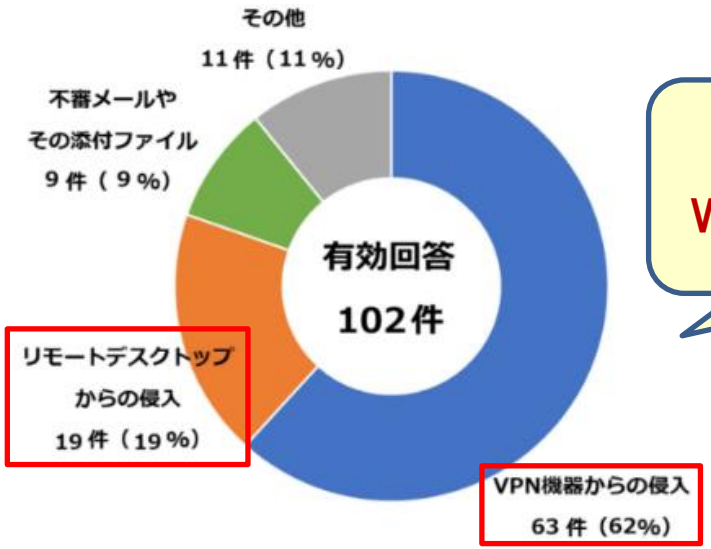
- 標的組織のネットワークに攻撃者が**不正アクセス**し、直接ウイルスに感染させる

  →・**VPN機器**の脆弱性を悪用する
  ・脆弱な設定の**RDP（リモートデスクトップ）**を経由する

【1位】ランサムウェアによる被害

- 攻撃手口①-2

・ランサムウェアに感染させる（機器やネットワークを狙う）



注　図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない。

（※1）
2022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

【出典】
※1　令和4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/R04_cyber_jousei.pdf

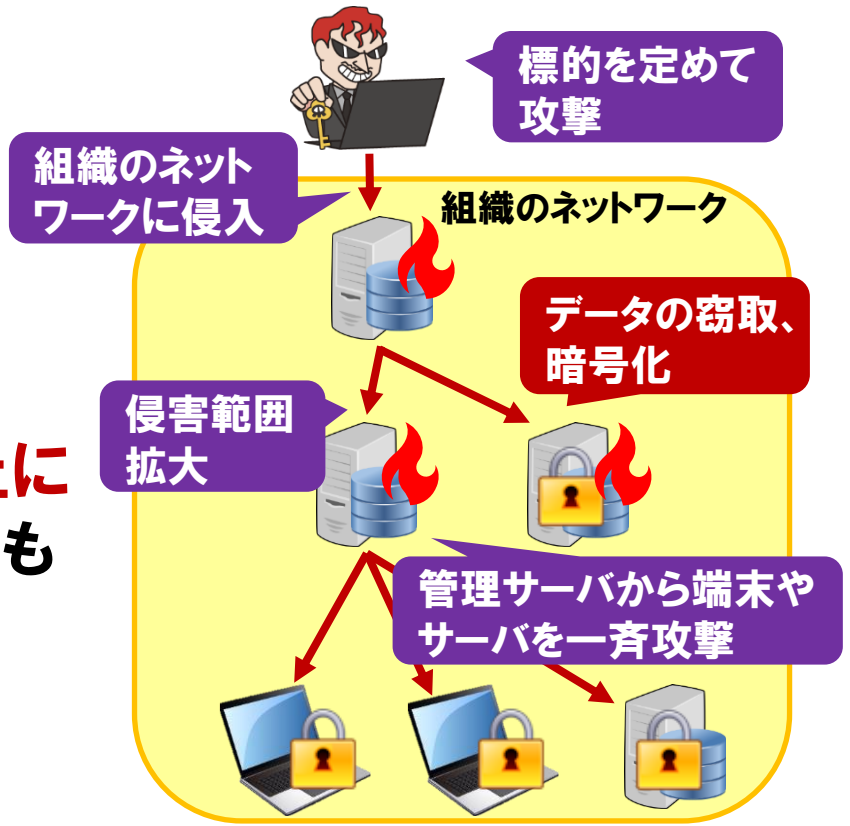
【1位】ランサムウェアによる被害

● 攻撃手口②-1

・重要情報を窃取する（二重脅迫） ※2020年頃から主流

- 標的組織に不正アクセスし、**重要情報を窃取**してから ランサムウェアに感染させて 機器、システムを暗号化

→暗号化からの復旧に加え、**窃取した重要情報をネット上に公開しないことと引き換え**にも 身代金を要求



（参考：IPA）事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/security/announce/2020-ransom.html

【1位】ランサムウェアによる被害

● 攻撃手口②-2

・二重脅迫にとどまらない四重脅迫(※1)

- DDoS攻撃を行うと脅迫して身代金を要求、または攻撃中止のための身代金を要求

  →さらなる混乱と金銭被害

  ※DDoS攻撃とは？
  多数の端末から標的のウェブサイトやサーバーに対して過剰なアクセスを行うことでシステムダウンさせるサイバー攻撃

- 顧客や取引先にランサムウェア攻撃を受けていることをリークすると脅迫し身代金を要求

  →リークされた場合、信用の失墜につながるおそれ

【出典】
※1「ランサムウェア攻撃 グローバル実態調査 2022年版」を発表
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220907-01.html

【1位】ランサムウェアによる被害

- 事例/傾向
  - 脆弱性を悪用されランサムウェア感染(※1)
    - 国内のIT企業が2021年末にサイバー攻撃の被害
    - 社員向けに提供されていた**ウェブサービスに脆弱性**があり、それを悪用されてサーバーに**繰り返し侵入**された
    - 社内管理情報や顧客情報等の**重要情報を窃取**され、**リークサイト上に公開**されていたことが判明
    - ウェブサービスの脆弱性をランサムウェア感染にも悪用され、社内の機器が**暗号化**の被害

【出典】
※1 サイバー攻撃による被害と復旧状況について(東京コンピュータサービス株式会社)
https://www.to-kon.co.jp/ja/topics/topics20220411103030.html

【1位】ランサムウェアによる被害

- 事例/傾向
  - ランサムウェア感染による長期のサービス停止（※1,2）
    - 2023年6月、人事労務サービスを展開するシステム会社がランサムウェア攻撃を受け、社労士業務に利用されるサービスやマイナンバー管理を行うサービス等**複数のクラウドサービスが停止**
    - サービスを利用している約2,800の社労士事務所と約57万の事業所が影響を受け、情報漏えいの可能性を公表する企業も
    - **約1ヶ月のサービス停止**により業績に甚大な影響

【出典】
※1 「社労夢」のエムケイシステム、ランサムウェア被害で個人情報漏洩の恐れ（朝日新聞デジタル）
https://smbiz.asahi.com/article/14930843
※2 社労士向けクラウド「社労夢」障害、発生からまもなく1カ月 6月料金請求なしで売上高予想32億円→未定に（ITmedia）
https://www.itmedia.co.jp/news/articles/2306/30/news164.html

【1位】ランサムウェアによる被害

- 対策
  - 経営者
    - 組織としての体制の確立
      - CISO (Chief Information Security Officer) 等、**専門知識を持つ責任者**を配置する
      - 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) を構築する
      - 継続的なセキュリティ対策を行うための**予算を確保**する
      - **情報セキュリティポリシー**の策定および従業員への周知

・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**

【1位】ランサムウェアによる被害

- 対策
  - システム管理者、従業員
    - 被害の予防（被害に備えた対策含む）
      - 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添付ファイルやURLを確認する
        - 不正なファイルやリンクではないという確証がない場合クリックしない
        - Officeファイルの場合マクロを実行しない

社内教育やメール訓練で従業員全体に浸透させる

【1位】ランサムウェアによる被害

- 対策
  - システム管理者、従業員
    - 被害の予防（被害に備えた対策含む）
      - –フィルタリングツールやセキュリティ製品を導入する
      - –脆弱性情報の収集および**セキュリティパッチの適用**を行う
      - –サポート切れのOSは利用しない
        →使用しているOSのサポート終了が告知された際には
        期限までに移行できるよう準備を行う
      - –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
      - –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
        →組織内に侵入された際に**被害を最小限に抑える**

【1位】ランサムウェアによる被害

- 対策
  - システム管理者、従業員
    - 被害の予防（被害に備えた対策含む）

－重要なファイルやシステムの**バックアップ**を準備する

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**オフラインで保管**

②バックアップに使用する**装置・媒体は複数用意**

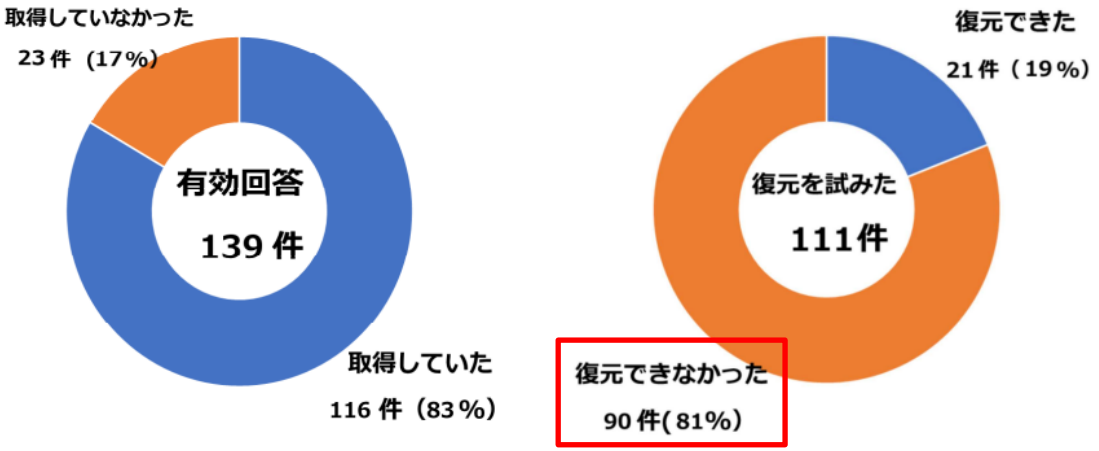
・**複数の媒体**でバックアップを取得し、さらに**コピー**も用意すると有事の際にどれか一つは利用可能な状態である可能性が高い
・災害にも備え少なくとも一つは**オフサイト**で保管する

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

【1位】ランサムウェアによる被害

- 対策
  - システム管理者、従業員
    - 被害の予防（被害に備えた対策含む）
      - –重要なファイルやシステムのバックアップを準備する



（※1）2022年に警察庁に報告があったランサムウェア被害における
バックアップの取得（左）・活用（右）状況

【出典】
※1　令和4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/R04_cyber_jousei.pdf

【1位】ランサムウェアによる被害

- 対策
  - システム管理者、従業員
    - 被害を受けた後の対応

–ウイルス感染が疑われる場合**ネットワーク接続を切断**し
組織の規定に従い**エスカレーション**、CSIRTに連絡

–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**

個人情報保護法の改正（2022年4月）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**

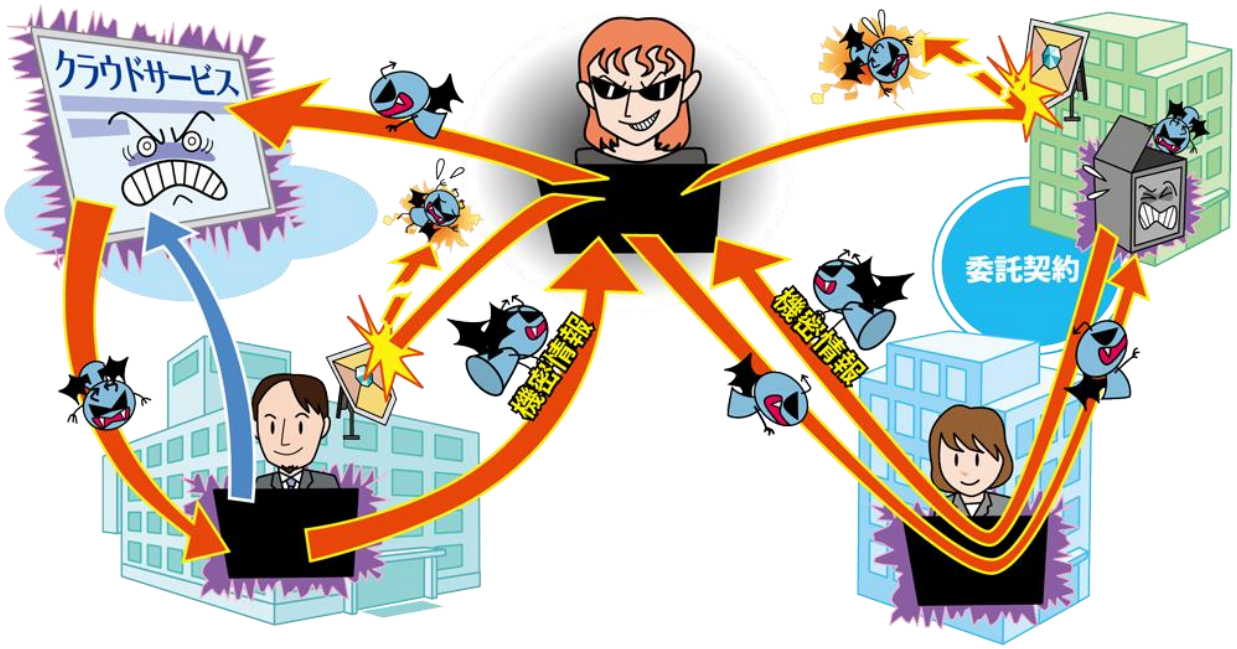
・身代金要求に応じる組織として**今後も標的に**
・復旧できる、情報が削除される保証はない

感染を防ぐ対策と万が一に備えた対策の両立を

2

サプライチェーンの弱点を悪用した攻撃

【2位】サプライチェーンの弱点を悪用した攻撃



- 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が狙われ、攻撃の足掛かりとされたり情報を窃取されたりする

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
- 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）

【2位】サプライチェーンの弱点を悪用した攻撃

● 攻撃手口①

・サプライチェーンの中でセキュリティが脆弱な組織を狙う

- 標的組織の取引先や委託先を攻撃し、保有されている標的組織の**重要情報を窃取**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**し、そこから標的組織に侵入する

【2位】サプライチェーンの弱点を悪用した攻撃

● 攻撃手口②

・ソフトウェアサプライチェーンを悪用する

- 標的組織が利用している**ソフトウェアの開発元**を攻撃してアップデートに**ウイルス**を仕込み、アップデートを適用した標的組織にウイルスを感染させる

  →ソフトウェアに組み込むOSSの脆弱性を悪用されたり
  OSSにウイルスが含まれていたりすることも

- MSP（企業システムの運用・監視等を請け負う事業者）を攻撃し、情報を窃取したり攻撃の足掛かりとする

【2位】サプライチェーンの弱点を悪用した攻撃

● 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

・契約における責任が不明確

- 専門知識、スキルが不足していることで、契約における情報セキュリティに関する責任範囲等を明確にできていない

【2位】サプライチェーンの弱点を悪用した攻撃

- 事例/傾向
  - 業務委託先経由でのランサムウェア感染(※1)
    - 2022年10月、大阪の総合病院がランサムウェア感染の被害を受けた
    - 給食サービスを委託していた**外部組織経由で感染**

      →①委託先が**VPN機器の脆弱性**を悪用され不正アクセスされる
      ②委託先⇔病院間の**ネットワーク経由**で不正アクセスされる
      ③病院の基幹システムやバックアップサーバー、電子カルテ等が暗号化される
    - 新規外来患者の受け入れや手術が一時停止する等の影響

【出典】
※1 情報セキュリティインシデント調査委員会報告書（大阪急性期・総合医療センター）
https://www.gh.opho.jp/pdf/report_v01.pdf

【2位】サプライチェーンの弱点を悪用した攻撃

- 事例/傾向
  - クラウドサービスからの情報漏えい(※1,2)
    - 2022年10月、ソフトウェア企業が提供するWebサイトの運営をサポートする複数のサービスが改ざんされていたことが明らかになった
    - 同社システムの**脆弱性を突かれ不正アクセス**をされ、サービスの**ソースコードが改ざん**された
    - 当該サービスをWebサイトの運営に利用していた10社以上の企業において、**サイトに入力された顧客の個人情報（クレジットカード情報含む）が漏えい**した可能性

【出典】
※1 不正アクセスに関するお知らせとお詫び（株式会社ショーケース）
https://www.showcase-tv.com/pressrelease/202210-fa-info/
※2 ショーケースが半年前にソースコード改ざん被害、利用企業のカード流出は10社超に（日経XTECH）
https://xtech.nikkei.com/atcl/nxt/column/18/00598/013000200/

【2位】サプライチェーンの弱点を悪用した攻撃

- 対策
  - 自組織
    - 被害の予防
      - 業務委託や情報管理における規則の整備と徹底
      - 外部組織も含めた報告体制等、問題発生時の運用規則整備
      - 納品物の検証を行う
        →組み込まれているソフトウェアも把握し脆弱性対策等を行う
      - 情報セキュリティの認証取得（ISMS、Pマーク、SOC2、ISMAP等）
        →顧客の信頼も得やすくなる
      - 公的機関が公開している資料の活用

        参考）・サイバーセキュリティ経営ガイドライン（経済産業省）
        https://www.meti.go.jp/policy/netsecurity/mng_guide.html
        ・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/keihatsu/sme/guideline/

【2位】サプライチェーンの弱点を悪用した攻撃

- 対策
  - 自組織
    - 被害を受けた後の対応
      - 組織の方針に従い各所へ**報告、相談**する
        →上司、CSIRT、関係組織、公的機関等
      - 影響調査および原因の追究
      - 契約に基づいた被害への補償

【2位】サプライチェーンの弱点を悪用した攻撃

- 対策
  - 自組織の商流に関わる組織に対して
    - 被害の予防

      –信頼性評価や品質基準に基づき、信頼できる委託先、取引先、サービスを選定する

      –**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

      –取引先や委託先組織の管理
      →情報セキュリティ対応の**定期的な確認、監査**

商流に関わる組織と情報セキュリティに対する意識を共有する

【2位】サプライチェーンの弱点を悪用した攻撃

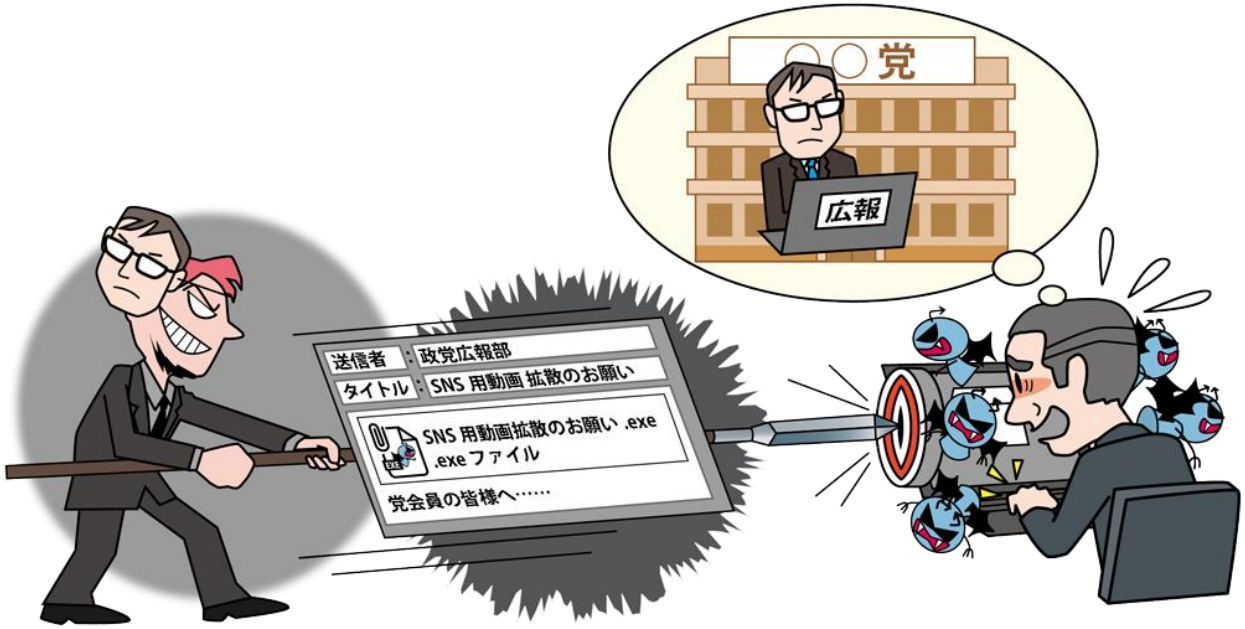
（参考）ソフトウェアサプライチェーン対策

- **SBOMによるコンポーネントの可視化**
  - SBOM（Software Bill Of Materials）とは、製品やシステムに含まれるソフトウェアを構成するコンポーネントや互いの依存関係、ライセンスデータ等をリスト化したもの
    →**リスク管理や脆弱性対策**に活用できる
  - 2021年5月に発令された**米国大統領令**（EO14028）において、ソフトウェアサプライチェーンセキュリティの向上の施策としてSBOM活用の検討指示が明記された
  - 日本国内においても経済産業省や総務省によりSBOM活用の議論や**実証実験が進められている**

3

標的型攻撃による機密情報の窃取

【3位】標的型攻撃による機密情報の窃取



- メール等を利用し標的組織の端末をウイルスに感染させる
- 組織内部に潜入し長期にわたり侵害範囲を徐々に広げる
- 組織の機密情報窃取やシステムの破壊を行う

【3位】標的型攻撃による機密情報の窃取

● 攻撃手口①

・初期侵入（組織内の個人を狙う）

- 業務に関するメールを装い不正なファイルを添付する

→・実行ファイル（拡張子　.exe、.js 等）

・マクロを実行するとウイルスに感染するよう細工された Officeファイル（Word、Excel、PowerPoint 等）

・ショートカットファイル（拡張子　.lnk）(※1)　　等が使われる

スピアフィッシング

不特定多数をターゲットとする通常のフィッシングに対し、特定の組織や個人を狙い情報の窃取やウイルス感染を試みるもの

【出典】

※1 サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 4 月～6 月］《 付録 》
～ショートカットファイルを悪用する攻撃の解析事例～（IPA）
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000100057.pdf

【3位】標的型攻撃による機密情報の窃取

● 攻撃手口①

・初期侵入（組織内の個人を狙う）

- **悪意あるウェブサイト**にアクセスさせる

  →標的組織がよく使うウェブサイトに脆弱性がある場合、ウイルスがダウンロードされるよう**改ざん**する

- **SNSのチャット機能**で不正なファイルを送信する

  →**標的組織の従業員にSNSで接触**し、チャットのやり取りで接近してウイルスが含まれるファイルを送る

ChatGPTに便乗したサイバー攻撃が増加中

ChatGPTや開発元を装ったメールや偽サイト、ChatGPTに関連すると装った偽のブラウザ拡張機能などの検出が急増
→ウイルス配布や情報窃取に利用されていると見られる

【3位】標的型攻撃による機密情報の窃取

● 攻撃手口②

・初期侵入（機器やネットワークを狙う）

- 標的組織が利用するクラウドサービス等へ不正ログインし、**認証情報を窃取**することで社内システムへ正規の経路から不正にアクセス
- 組織で利用されている機器の**脆弱性を悪用**し不正にアクセス

【3位】標的型攻撃による機密情報の窃取

● 攻撃手口③

・侵害範囲の拡大（ラテラルムーブメント）、情報窃取

- 初期侵入が成功すると遠隔操作ウイルス（RAT）と攻撃者側の**C&Cサーバー**との通信により遠隔操作が可能に
- 標的組織のネットワーク環境や機器の**探索**を行う
- 資格情報（ユーザーID・PW）の窃取や権限昇格
  →最終的に**管理者権限の取得**を目指す
- **セキュリティソフトの無効化**
- 端末やサーバー、共有フォルダ等から**機密情報をコピー、圧縮**し外部に送信

正規のツールを使われ不審な活動としての検出が困難な場合も

【3位】標的型攻撃による機密情報の窃取

- 事例/傾向
  - スピアフィッシングによる標的型攻撃（※1）
    - 2022年、参議院選挙の直前期間に自民党に対し**スピアフィッシングキャンペーン**が行われていたことが判明
    - **政党の広報**を装って選挙に関する依頼をしたり、**著名な政治家**を装ったりするメールが送られた
    - メールには不正にコマンドを実行し**情報窃取を行うウイルス**「LODEINFO」が含まれるファイルが添付されていた

【出典】
※1 APTグループ「MirrorFace」が日本の政治団体を標的に実行したLiberalFace作戦の詳細（ESETセキュリティニュース）
https://www.eset.com/jp/blog/welivesecurity/unmasking-mirrorface/

【3位】標的型攻撃による機密情報の窃取

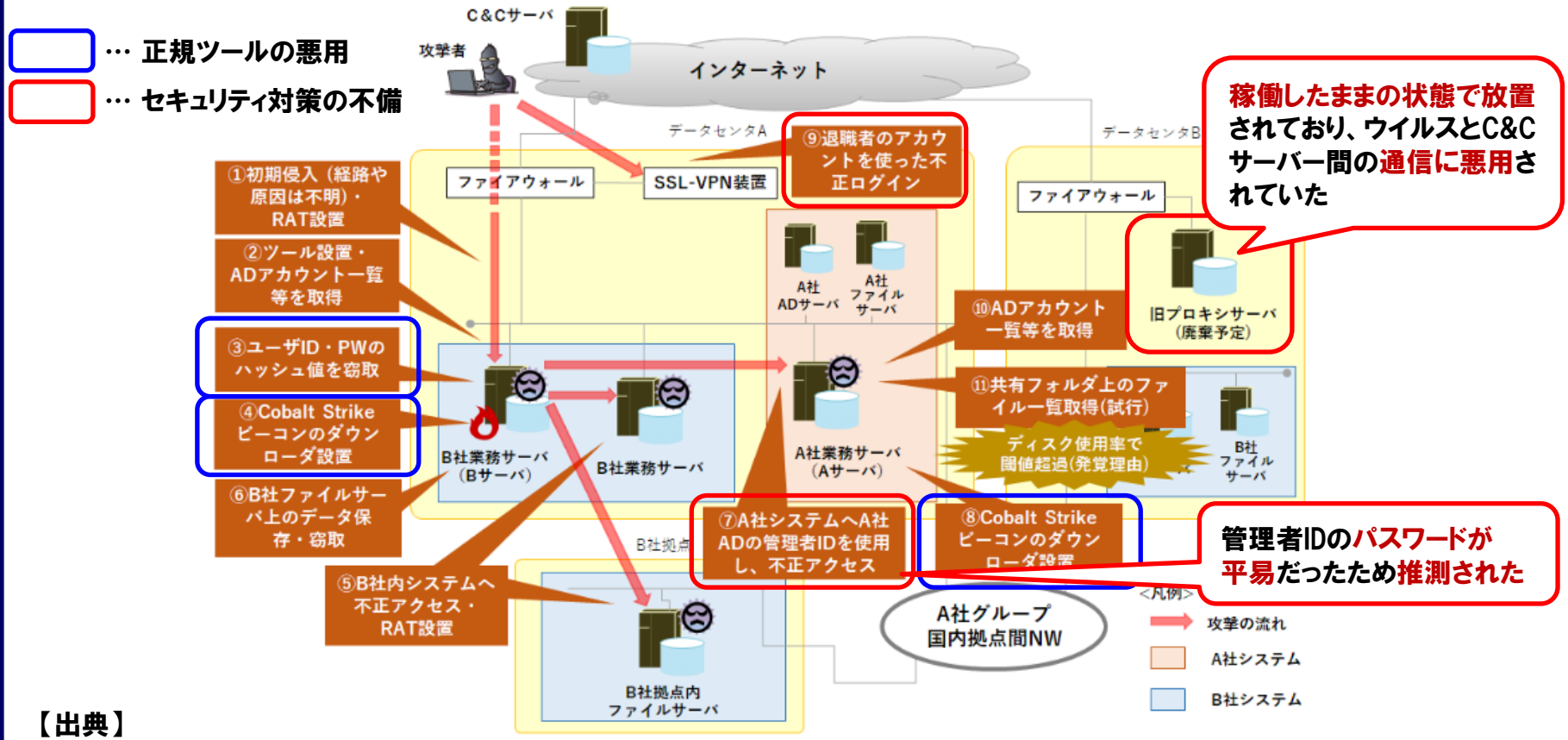
- 事例/傾向
  - 長期間の潜伏が確認された標的型攻撃（※1）
    - 2022年、国内の企業が**同じネットワーク内にあったグループ企業のサーバー**を介して標的型攻撃を受けた事例が報告された
    - 調査の結果、侵入経路となったグループ企業では攻撃が発覚する**1年半以上前から侵入**されていた痕跡があった
    - 攻撃には遠隔操作やファイルのダウンロードを行う2種のウイルスが使用された他、**WindowsOSの正規プログラム**や**商用のペネトレーションツール**の悪用が確認された

【出典】
※1 サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 7 月～9 月］（IPA）
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000103970.pdf

【3位】標的型攻撃による機密情報の窃取

● 事例/傾向

■ 長期間の潜伏が確認された標的型攻撃（※1）



【出典】
※1 サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 7 月～9 月］（IPA）
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000103970.pdf

【3位】標的型攻撃による機密情報の窃取

- 対策
  - 経営者
    - 組織としての体制の確立
      - CISO（Chief Information Security Officer）等、専門知識を持つ責任者を配置する
      - 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）を構築する
      - 継続的なセキュリティ対策を行うための予算を確保する
      - 情報セキュリティポリシーの策定および従業員への周知

【3位】標的型攻撃による機密情報の窃取

- 対策
  - システム管理者、従業員
    - 被害の予防（被害に備えた対策含む）
      - 情報の管理とルール策定
      - サイバー攻撃に関する継続的な情報収集と情報共有
      - セキュリティ教育・インシデント訓練を定期的に実施する
        →「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」等
      - フィルタリングツールやセキュリティ製品を導入する
      - 脆弱性情報の収集およびセキュリティパッチの適用を行う
      - セキュアなシステム設計やネットワーク分離を行う
      - 重要サーバーの要塞化（アクセス制御、暗号化等）

グループ企業や海外拠点等も含めた組織全体で実施する

【3位】標的型攻撃による機密情報の窃取

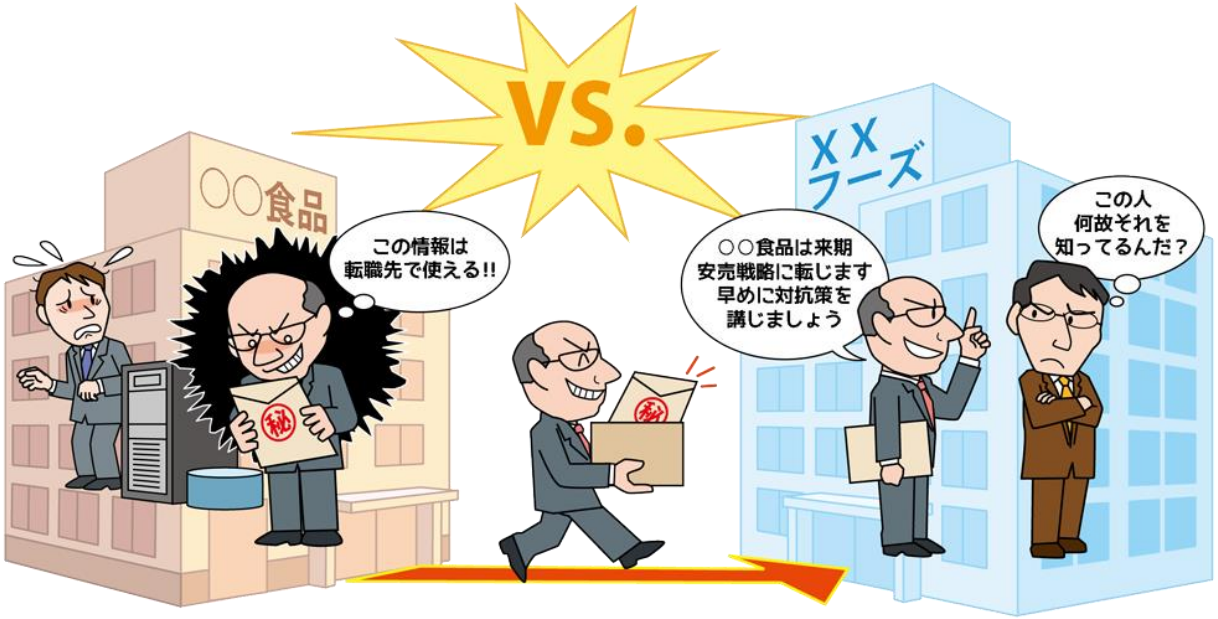
- 対策
  - システム管理者、従業員
    - 被害を受けた後の対応
      - –ウイルス感染が疑われる場合**ネットワーク接続を切断**し組織の規定に従い**エスカレーション**、CSIRTに連絡
      - –影響調査および原因の追究
      - –関係者、関係機関への連絡
        - →監督官庁、個人情報保護委員会、警察等

組織全員が危険性を認識し多角的な対策を

4

内部不正による情報漏えい

【4位】内部不正による情報漏えい



- 組織の職員や元職員による機密情報の漏えい
- 損害賠償による金銭被害や社会的信用の失墜を招く
- 不正に持ち出された情報を利用した組織も責任を問われる

【4位】内部不正による情報漏えい

● 攻撃手口①

・内部情報への不正なアクセス

- **付与されたパスワードを悪用**し、組織の重要情報を取得
  →必要以上のアクセス権限を付与していると、悪用された場合被害が大きくなる
- **在職中に使用していたアカウント**を悪用し、離職後も組織内部の情報にアクセス
  →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

【4位】内部不正による情報漏えい

● 攻撃手口②

・内部情報の不正な持ち出し

- 外部への持ち出しを許可されていない情報を、USBメモリー、HDD、メール、クラウドストレージ、スマホカメラ、紙媒体等で不正に持ち出す
- 組織内で使用していた機器を不正にフリーマーケット等に出品し、**機器の中に残っていた情報が流出**する

【4位】内部不正による情報漏えい

- 事例/傾向
  - 営業秘密を持ち出して競合他社に転職（※1）
    - 2022年9月、大手寿司チェーンの運営会社社長が**以前在籍していた競合他社の営業秘密を持ち出した**ことが判明した
    - 食材原価や使用料等のデータを自社データと比較する等して不正に利用
    - 転職前の元部下がパスワードを漏らす等して協力していた
    - 社長の他、データを不正利用した商品企画部長、協力した元部下が**不正競争防止法違反**の容疑で逮捕された

【出典】
※1 かっぱ寿司運営会社社長ら逮捕 不正競争防止法違反容疑 警視庁（NHK NEWS WEB）
https://www3.nhk.or.jp/news/html/20220930/k10013843141000.html

【4位】内部不正による情報漏えい

- 事例/傾向
  - 長期にわたる個人情報の漏えい(※1,2)
    - 2015年2月～2022年1月にかけて釜石市の職員2名が全市民の個人情報や業務上知り得た市民の滞納情報等を自宅PCに送信する等して漏えい
    - 個人情報を不正に入手するため、情報を入手できる部署の職員に依頼して送信させたことも
    - 立場を悪用し担当する業務を監査対象から外す行為も確認された

【出典】
※1 釜石市個人情報漏えい調査委員会報告書(釜石市)
https://www.city.kamaishi.iwate.jp/docs/2023041400057/file_contents/20272_.pdf
※2 市民の個人情報漏洩、女性主査「断った時の影響が不安で協力」と免職の元係長に渡す(讀賣新聞)
https://www.yomiuri.co.jp/national/20220826-OYT1T50237/

【4位】内部不正による情報漏えい

対策

・状況的犯罪予防の理論

- **犯行を難しくする**
  例）物理セキュリティやアクセス制御の強化
- **捕まるリスクを高める**
  例）アクセスログの監視
- **犯行の見返りを減らす**
  例）重要情報の暗号化
- **犯行の挑発を減らす**
  例）適切な人事や作業管理
- **犯罪を容認する言い訳を許さない**
  例）情報セキュリティポリシーの策定および掲示

【4位】内部不正による情報漏えい

- 対策
  - 経営者、管理者
    - 被害の予防

－基本方針の策定
→・情報取扱ポリシーの策定
・懲戒処分等を規定した就業規則の整備

－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

【4位】内部不正による情報漏えい

- 対策
  - 経営者、管理者
    - 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やアカウントの登録、変更、削除に関する**手順を定めて運用**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

・退職者と**秘密保持契約**を結ぶ

・**定期的な監査**を実施する

・DLP等セキュリティ製品を導入する

【4位】内部不正による情報漏えい

- 対策
  - 経営者、管理者
    - 被害の予防

      −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**

      ・記録媒体の廃棄時には適切な**データ消去**を実施する

      →**物理破壊**をするとより確実

      ・リース品を返却する際は必ずデータ消去と**初期化**が実施されていることを確認する

      −人的管理およびコンプライアンス教育の徹底

    - 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、証跡を記録し監視する

【4位】内部不正による情報漏えい

- 対策
  - 経営者、管理者
    - 被害を受けた後の対応
      - 組織の方針に従い各所へ**報告、相談**する
        →上司、CSIRT、関係組織、公的機関等
      - 影響調査および原因の追究、対策の強化
      - 内部不正者に対する**適切な処罰の実施**

外部の攻撃者だけでなく内部にも目を光らせることが必要

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

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

共通対策①
～パスワードを適切に運用する～

- **パスワードを初期設定のままにしない**
  - 特にIoT機器は初期設定のパスワードは共通して使われている場合もあり、危険性が高い
- **推測されにくいパスワードを使用する**

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

悪いパスワードの例

- **複数のサービスで同じID・パスワードを使い回さない**
  - パスワードリスト攻撃の被害を受けるおそれがある

共通対策②
～情報リテラシー、モラルを向上させる～

- **SNS、インターネットの利用について教育する**
  - －情報流出、炎上など様々なリスクがある
  - －AIチャットサービスに業務上の機密情報を入力してしまう事例も
- **コンプライアンス教育の徹底**
  - －就業規則や内部不正に対する懲戒処分の規定などの周知
  - －他人事として考えない、考えさせない
- **上記は継続的に取り組む**
  - －人の入れ替わりやイベント（長期休暇など）に対応
  - －運用状況や社会情勢に合わせ、内容をアップデートしていく

共通対策③

～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～

- **リンク、添付ファイル、QRコード、画像の開封や読込みを安易にしない**
  - –リンクの内容を確認したい場合は対象のサービスを検索して正規のWebページから確認する
  - –よく利用するWebサイトはブックマークをしてそこから開くようにする
- **不審な点があるメールへ直接返信したり、記載されている電話番号に連絡をしたりしない**
  - –相手に連絡したい場合は正規の連絡先や問い合わせ窓口を確認してから連絡する

共通対策④
～適切な報告/連絡/相談を行う～

- インシデントを隠蔽しない風土や関係性を築く
- エスカレーション先の周知
- 組織内の関連部署への横展開
- 外部の関連組織や公的機関への連絡
- 組織外への情報発信を検討

→ 判断基準/連絡先/連絡フロー の制定および周知

共通対策⑤
～インシデント体制を整備し、対応を行う～

- **専門知識を持つ責任者の配置**
- **専門部署（CSIRT）の設置**
  - インシデントの検知や連絡受付／情報収集／インシデント対応／関係各所への連絡 などを一元管理
- **有事の際の対応フローや運用手順の作成および周知**
- **定期的な訓練および手順の見直し（PDCAサイクル）**
- **外部の協力依頼先の用意**
  - 自組織で解決できない場合を想定する

→ 上記を継続的に行える体制の構築と予算の確保

共通対策⑥
～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～

- **脆弱性対策を適切に行う**
  - 自組織で利用しているハードウェア/ソフトウェアを把握管理する
  - 製品のサポート期限を把握し、サポートが切れる前に移行する
  - 脆弱性情報や攻撃情報を収集する体制の構築
  - 更新プログラム適用の手順の整備
- **適切なアクセス権限管理を行う**
- **セキュアなネットワーク環境を構築する**
  - ネットワーク分離/アクセス制御/プロキシサーバーの導入
- **セキュリティ製品を導入する**
  - アンチウイルス/フィルタリング/不審な挙動の検知/ネットワーク監視/データ持ち出し検知/Webサイトの保護 など
- **セキュリティ診断の実施**

共通対策⑦
～適切なバックアップ運用を行う～

- **バックアップを取得する**
- **バックアップを保管する**
- **バックアップからリカバリする**

→ 3-2-1-1-0 ルール

- 少なくとも3つのデータコピーを用意
- 少なくとも2つの異なるストレージメディアを使用
- 少なくとも1つはオフラインで保管
- 少なくとも1つはオフサイトで保管
- バックアップはエラー0で完了

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

情報処理推進機構（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**
- **経営者が認識すべき「3原則」、実行すべき「重要7項目の取組」を記載**
- **サンプルを参考に、自社のセキュリテイ規程を作成できる**

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
- 対策のヒントとなるQ＆A集や内部不正チェックシート等の付録付き

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 2023
https://www.ipa.go.jp/security/10threats/10threats2023.html

☆情報セキュリティ10大脅威 2023
→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 2023 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 2023 知っておきたい用語や仕組み

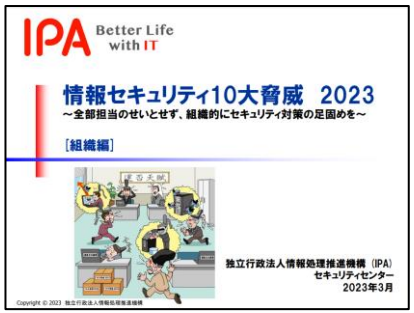
- 過去の全ての10大脅威はトップページから

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

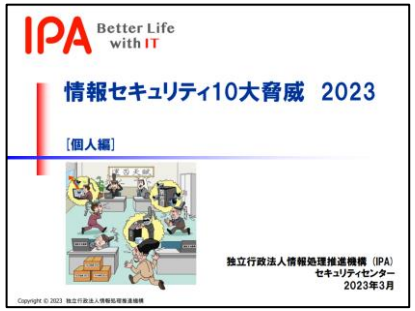
情報セキュリティ10大脅威 簡易説明資料

- **簡易説明資料（スライド形式）**

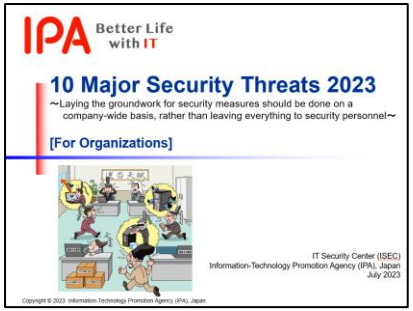
情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/security/10threats/10threats2023.html



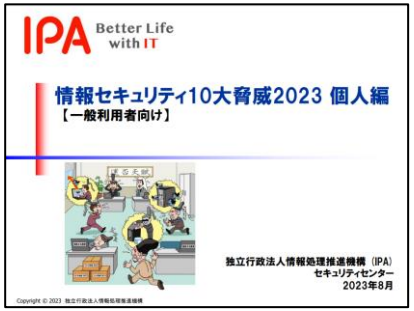
組織編



個人編



組織編
［英語版］



個人編
［一般利用者向け］

組織内やご家庭でのセキュリティ教育にご活用ください

IPA

IPA Better Life with IT

ありがとうございました