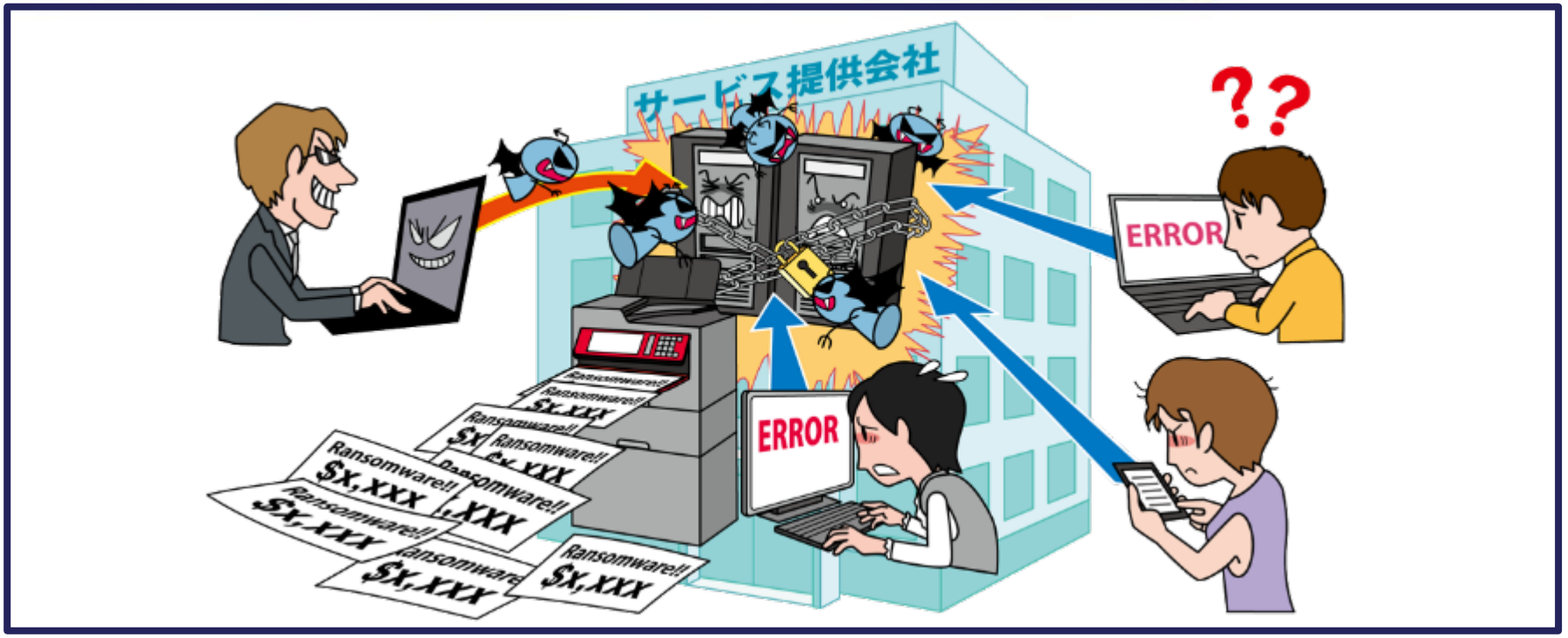
【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～



- PC等に保存されているファイルが暗号化され、使用不可にされる
- 復旧と引き換えに金銭を要求される
- 情報が窃取されて、公開され、さらに攻撃を受けている事を
  ビジネスパートナー等に公表すると脅迫されるケースもある
- 組織の規模や業種に関係なく攻撃される

【出典】 令和５年上半期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/R05_kami_cyber_jousei.pdf

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

IPA

- **攻撃手口**

・ウイルス(ランサムウェア)に感染させて金銭を要求

- **脆弱性を悪用した手口**
  - ソフトウェアの脆弱性を悪用し
    ウイルスを実行(感染させる)
  - 攻撃ツール等を利用して
    ネットワーク越しに次々と感染させる

- **不正アクセスによる手口**
  - 意図せず公開されているポート(リモートデスクトップ等)から
    サーバーに不正アクセスさせる
  - サーバー上で攻撃者がウイルスを実行させる(感染させる)

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

IPA

- **攻撃手口**

・ウイルス(ランサムウェア)に感染させて金銭を要求

- **メールを悪用した手口**
  - 不正な添付ファイルを開かせる
  - メール内のリンクをクリックさせる
- **Web サイトを悪用した手口**
  - ランサムウェアをダウンロードさせるようにWebサイトを改ざんした
  - 当該サイトを閲覧するようにメールなどで誘導した

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

- **2023年の事例/傾向①**
  - **ランサムウェア感染による業務停止**
    - 2023年7月、名古屋港統一ターミナルシステムがランサムウェアに感染した
    - リモート接続機器の脆弱性を悪用した不正アクセスが原因であった
    - 物理サーバー基盤および全仮想サーバーが暗号化されていることが判明した
    - 約2日半、ターミナルでの作業停止を余儀なくされた

【出典】 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
コンテナターミナルにおける情報セキュリティ対策等検討委員会について(国土交通省)
https://www.mlit.go.jp/kowan/kowan_mn2_000006.html

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

- **2023年の事例/傾向②**
  - **ランサムウェア感染によるサービス提供停止**
    - 2023年6月、エムケイシステムのデータセンターのサーバーが不正アクセスされ、ランサムウェアに感染した
    - データが暗号化され、社会保険労務士向けクラウドサービス「社労夢」をサービス提供できなくなった
    - 約3,400人のユーザーに影響があり、オンプレミスで動作するパッケージ版が代替として提供された
    - インフラ設備の再構築費用などがかかったため、エムケイシステムは業績予想を下方修正した

【出典】 第三者によるランサムウェア感染被害への対応状況のお知らせ(第２報)(株式会社エムケイシステム)
https://contents.xj-storage.jp/xcontents/AS97180/fd524344/99b9/470f/90e6/a580932b7962/140120230620507046.pdf
当社サーバへの不正アクセスに関する調査結果のご報告(第３報)(株式会社エムケイシステ ム)
https://contents.xj-storage.jp/xcontents/AS97180/813d570f/5138/4bc7/a113/f4837598df38/140120230719524126.pdf

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

- **2023年の事例/傾向③**
  - **VPN経由で侵入、ランサムウェアを横展開**
    - 2023年1月、ならコープがランサムウェアによる攻撃を受けていたことを公表
    - 原因は、攻撃者が脆弱性を悪用してVPN経由で侵入後、内部情報を収集し、ランサムウェアを横展開したことにある
    - サーバー11台で約49万人の個人情報を含むデータが暗号化されたが、それらの外部への流出は確認されていない
    - 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】 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
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/

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？ ～

- **対策**
  - **組織(経営者層)**

【組織としての体制確立】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？ ～

- **対策**
  - **組織(システム管理者、従業員)**

【被害の予防】

- インシデント対応体制を整備し、対応する
- 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
- 多要素認証の設定を有効にする
- 提供元が不明のソフトウェアを実行しない
- 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
- 共有サーバー等へのアクセス権の最小化と管理強化
- 公開サーバーへの不正アクセス対策
- 適切なバックアップ運用(取得、保管、復旧訓練)を行う

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？ ～

- **対策**
  - **組織(システム管理者、従業員)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- 適切なバックアップ運用(復旧作業)を行う
- 復号ツール※1の活用
- インシデント対応体制を整備し、対応する

【出典】 ※1 The No More Ransom Project(No More Ransomプロジェクト)
https://www.nomoreransom.org/

【1位】ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？ ～

- **身代金の支払いと復旧業者の選定について**
  - 原則、身代金を支払わずに復旧を行う
  - 身代金を支払ってもデータの復元や情報の流出を防げるとは限らない
  - 対応を依頼した業者が攻撃者との裏取引で身代金を支払うことで復旧した場合、事実上、自組織が攻撃者に資金提供をしたとみなされるおそれもある
  - 対応を依頼する業者の選定※1にも注意が必要

【出典】 ※1 データ被害時のベンダー選定チェックシート Ver.1.0(特定非営利活動法人デジタル・フォレンジック研究会)
https://digitalforensic.jp/higai-checksheet/