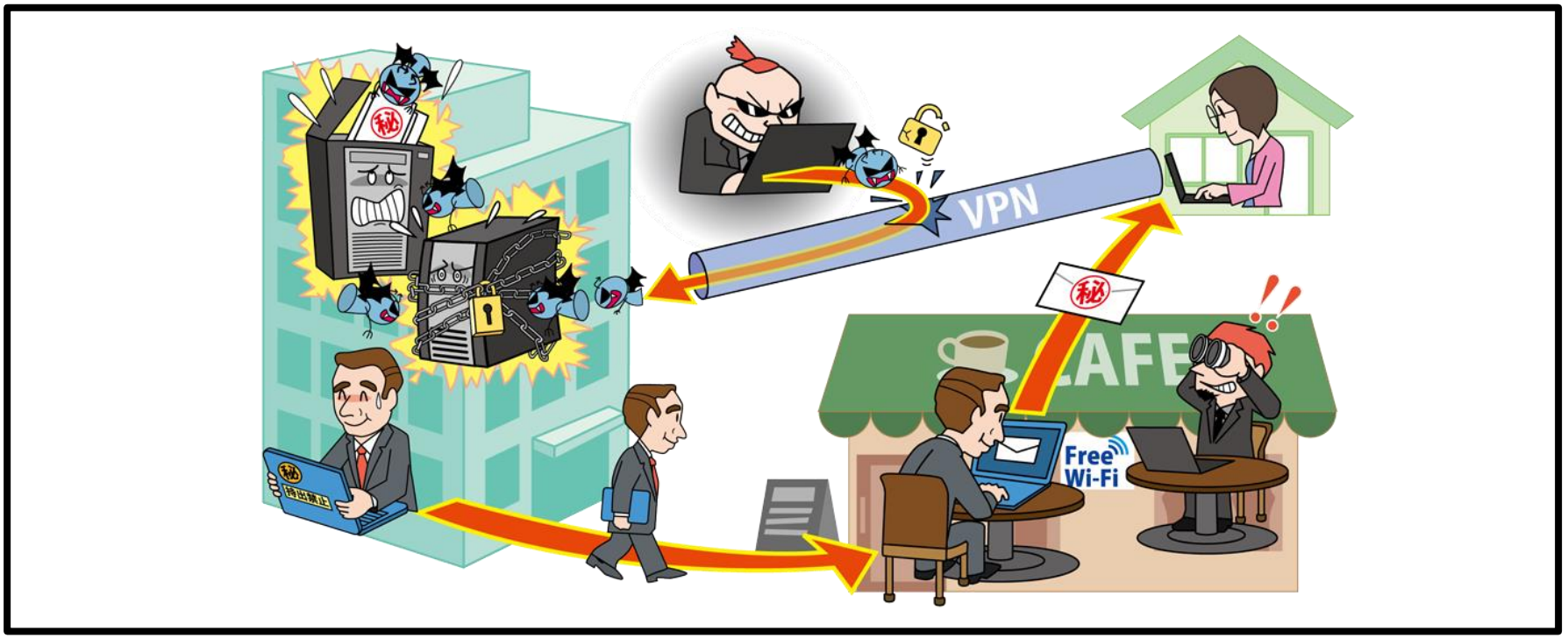
【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～



- 新型コロナウイルス対策の1つとして、テレワークが急速に普及
- ウェブ会議サービスやVPNの本格的な活用がされる中、それらを狙った攻撃が発生
- ウェブ会議の**のぞき見**やテレワーク用PCの**ウイルス感染**のおそれ

【5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

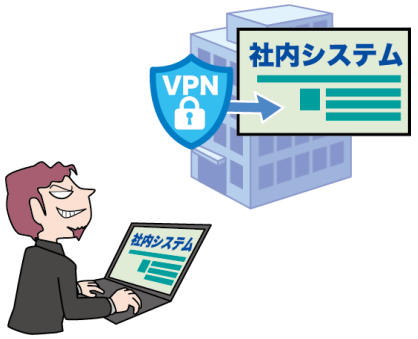
～未だ脆弱なテレワーク環境が狙われる～

● 攻撃手口/発生要因

・テレワーク環境や管理体制の不備

- テレワーク用ソフトの**脆弱性を悪用**した不正アクセス
- テレワーク移行時の、**セキュリティ対策が不十分な暫定状態のまま運用**、**管理体制の不備**
- 私物PCや自宅ネットワークの利用

※組織の**セキュリティ対策が適用されないところ**からの情報漏えいのおそれ



【5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

～未だ脆弱なテレワーク環境が狙われる～

- 2022年の事例/傾向①
  - リモート接続を狙ったランサムウェア攻撃 （※1）
    - 2022年6月、ニチリンの米国子会社がランサムウェア「mlock」に感染していたことを公表
    - 攻撃者は外部とのリモート接続における設定の脆弱性を悪用し、サーバーに侵入
    - 攻撃者は侵入後、別のサーバーにリモートアクセスツールなどをインストールし、ネットワークを偵察。その後ネットワーク全体にランサムウェアを配布していた。

【出典】
※1 ランサム被害、リモート接続の脆弱性が侵入口に - ニチリン（Security NEXT）
https://www.security-next.com/139557

【5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

～未だ脆弱なテレワーク環境が狙われる～

- 2022年の事例/傾向②

(※1,2)

- リモート接続の脆弱性やテレワークのセキュリティの実態
  - 警察庁によると、2022年上半期の国内におけるランサムウェア感染経路はVPN機器からの侵入が68％、リモートデスクトップからの侵入が15％と、**8割以上がリモート接続の脆弱性に起因**
  - IPAの調査結果では、テレワークのルール順守状況の確認については**改善傾向が見られる**ものの、ITユーザの35.5％、ITベンダの10.7％では**いまだに未確認**
  - 確認方法については、ITユーザは49.5％、ITベンダは40.8％の組織が**セルフチェックのみ**

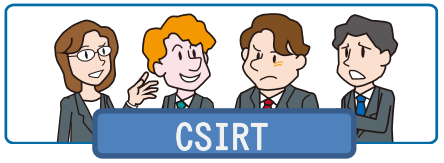
【出典】
※1 令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf
※2 2021年度 企業・組織におけるテレワークのセキュリティ実態調査（IPA）
https://www.ipa.go.jp/security/reports/economics/scrm/ug65p90000019dg8-att/000099573.pdf

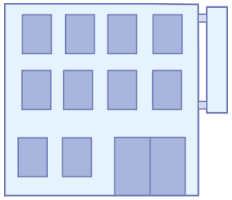
【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～

- **対策**
  - **組織（テレワーカー）**
    - ・被害の予防
      - －組織の**テレワークのルール**を順守
        （使用する端末、ネットワーク環境、作業場所等）

    - ・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

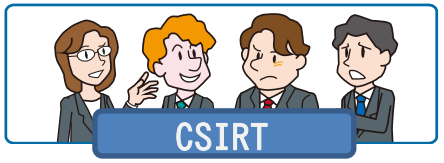


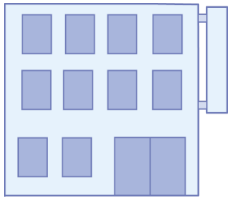


【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～

- **対策**
  - **組織（経営者層）**
    - ・組織としての体制の確立
      - –CSIRTの構築
      - –対策予算の確保と継続的な対策の実施
      - –テレワークのセキュリティポリシーの策定
      - –有事の際の連絡窓口やフローの確立

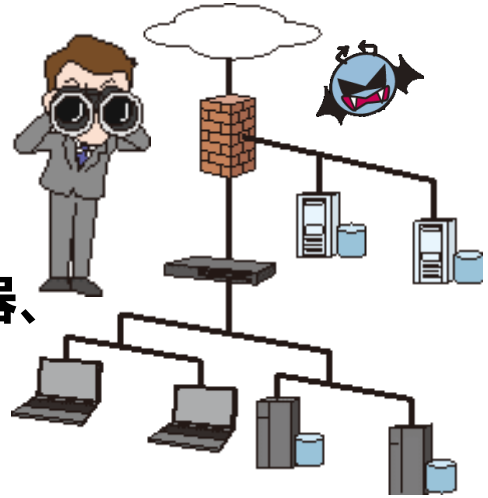




【5位】テレワーク等のニューノーマルな働き方を狙った攻撃

～未だ脆弱なテレワーク環境が狙われる～

- **対策**
  - **組織（セキュリティ担当者、システム担当者）**
    - ・被害の予防（被害に備えた対策含む）
      - －シンクライアント、VDI、VPN、ZTNA/SDP等の**セキュリティに強いテレワーク環境**の採用
      - －テレワークの**規程や運用ルール**の整備
        ※組織支給PCと私物PCの違いも考慮
      - －従業員に対する**セキュリティ教育**の実施
      - －利用するソフトウェアの**脆弱性情報の収集と周知、対策状況の管理**
      - －**セキュリティパッチ**の適用（VPN装置、ネットワーク機器、PC、スマートフォン等）
      - －ネットワークレベル認証（NLA）の実施
      - －多要素認証の設定を有効にする



【5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

～未だ脆弱なテレワーク環境が狙われる～

- **対策**
  - **組織（セキュリティ担当者、システム担当者）**
    - ・被害の早期検知
      - －適切なログの**取得と継続的な監視**
      - －ネットワーク**監視、防御**
      - －UTM・IDS/IPS、WAF、仮想パッチ等の**導入**
    - ・被害を受けた後の対応
      - －**CSIRTの運用**によるインシデント対応
        ※テレワーク環境をリモートから調査する
      - －影響調査および原因の追究、対策の強化