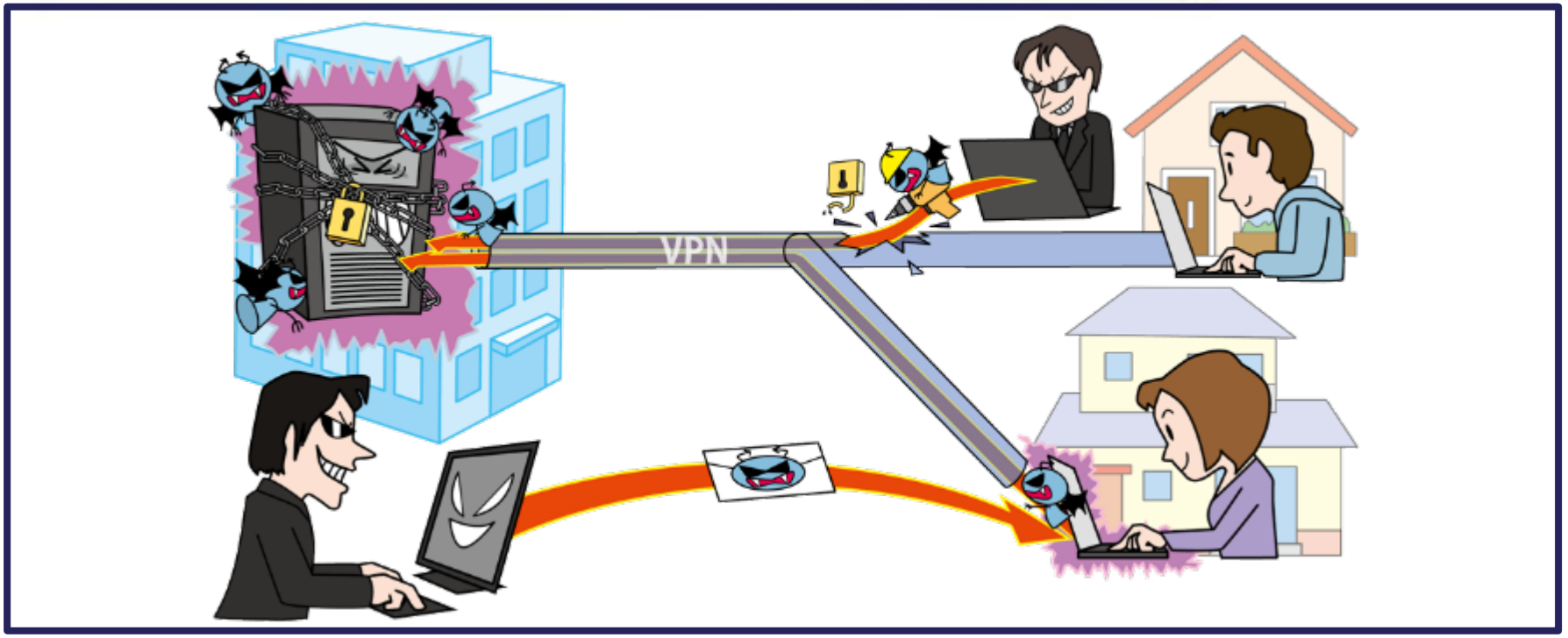
【9位】テレワーク等のニューノーマルな働き方を狙った攻撃

～狙われ続けるテレワーク環境、セキュリティ対策を～



- 2020年以降、感染症対策の一環として政府機関がニューノーマルな働き方の1つであるテレワークを推奨している
- VPN等の本格的な活用がされる中、それらを狙った攻撃が発生
- 業務環境に脆弱性があると、Web会議をのぞき見されるリスクが高まる

【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

～狙われ続けるテレワーク環境、セキュリティ対策を～

IPA

♦ 攻撃手口/発生要因

・テレワーク環境や管理体制の不備

- **テレワーク用製品の脆弱性を悪用して不正アクセスする**
  - VPN等のテレワーク用に導入している製品の脆弱性や設定ミス等を悪用する
    - 社内システムに不正アクセスしたり、PC内の業務情報等を窃取したりする
    - Web会議サービスの脆弱な設定を悪用してWeb会議をのぞき見する
- **テレワーク移行時のまま運用している脆弱なテレワーク環境を攻撃する**
- **脆弱な私物PCや自宅ネットワークの利用を狙う**
  - 適切なセキュリティ対策が施されていない私有端末および自宅のネットワーク環境でテレワークを行うと情報を盗聴されるおそれがある

【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

～狙われ続けるテレワーク環境、セキュリティ対策を～

- **2023年の事例/傾向①**
  - **在宅勤務のために用意したリモートアクセス経路より侵入の疑い**
    - 2023年10月、セイコーグループは顧客や取引先担当者等の個人情報約60,000件が流出したことを公表した
    - 原因は在宅勤務のために用意したリモートアクセス経路より侵入されたものとみられている
    - ランサムウェアに感染し、データセンターや国内拠点の一部サーバー内部に保存されていたデータの暗号化もされた

【出典】 ランサムウェアによる個人情報流出を確認、リモートアクセス経路より侵害か - セイコー(Security NEXT)
https://www.security-next.com/150579
当社サーバに対する不正アクセスに関するお知らせ(第３報)(セイコーグループ株式会社)
https://www.seiko.co.jp/information/202310251000.html

【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

～狙われ続けるテレワーク環境、セキュリティ対策を～

- **2023年の事例/傾向②**
  - **Web会議サービスの脆弱性**
    - Microsoftは2023年10月に、Teamsに影響する脆弱性(CVE-2023-4863)を、Zoomは2023年11月に、Zoom Roomsに影響する脆弱性(CVE-2023-43590)を対策し、最新版リリースした
    - セキュリティ対策は定期的に行われており、最新版の製品を利用していない場合、攻撃を受けるリスクが高くなるため、利用者には迅速なアップデートが求められている

【出典】 ビデオ会議サービスの「Zoom」、脆弱性9件を修正(Security NEXT)
https://www.security-next.com/151283
WebPのゼロデイ脆弱性は「Teams」や「Skype」にも ～Microsoftが影響製品を公表【10月10日追記】(窓の社)
https://forest.watch.impress.co.jp/docs/news/1536304.html

【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

～狙われ続けるテレワーク環境、セキュリティ対策を～

- **2023年の事例/傾向③**
  - **狙われ続けるテレワーク環境**
    - 警察庁によると、令和5年上半期におけるランサムウェア被害の感染経路としてVPN機器経由のものが35件で最も多く、全体の約71%を占めていた
    - リモートデスクトップから侵入したものは5件で全体の約10%を占めていた
    - テレワークに利用される機器等の脆弱性や強度の低い認証情報を悪用されたものが全体の約82%を占めていた

【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

【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

～狙われ続けるテレワーク環境、セキュリティ対策を～

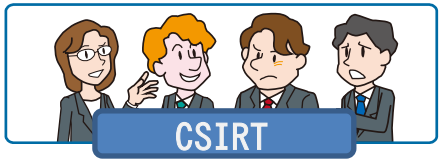
- **対策**
  - **個人(テレワーカー)**

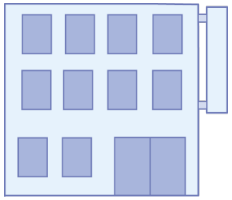
【被害の予防】

- 組織のテレワークのルールを順守する
  (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】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等





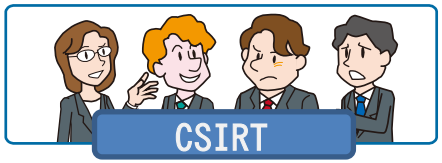
【9位】テレワーク等のニューノーマルな働き方を狙った攻撃

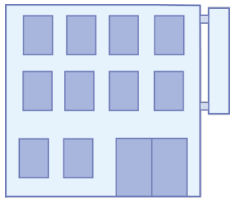
～狙われ続けるテレワーク環境、セキュリティ対策を～

- **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
  - テレワーク環境ならではの連絡方法や対応手順の作成
- テレワークのセキュリティポリシーを策定する



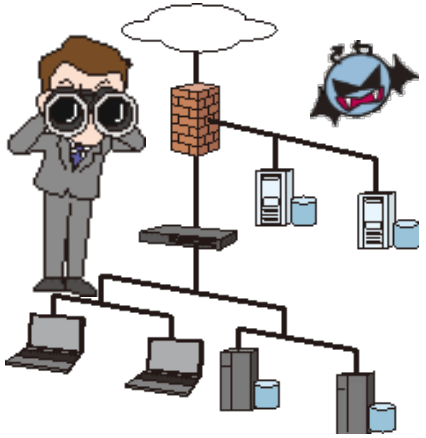


【参考】 テレワークを行う際のセキュリティ上の注意事項(IPA)
https://www.ipa.go.jp/security/anshin/measures/telework.html

【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
～狙われ続けるテレワーク環境、セキュリティ対策を～

- **対策**
  - **組織(セキュリティ担当者、システム管理者)**

【被害の予防】



- シンクライアント、VDI、VPN、ZTNA/SDP等の<u>セキュリティに強いテレワーク環境</u>を採用する
- テレワークの<u>規程や運用規則を整備</u>する
  - 組織支給PCと私物PCの違いも考慮する
- <u>情報リテラシー、モラルを向上</u>させる
- サーバーやクライアント、ネットワークに<u>適切なセキュリティ対策</u>を行う
- ネットワークレベル認証(NLA)を行う
- 多要素認証の設定を有効にする

【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

～狙われ続けるテレワーク環境、セキュリティ対策を～

- **対策**
  - **組織(セキュリティ担当者、システム管理者)**

【被害の早期検知】

- 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

【被害を受けた後の対応】

- インシデント対応体制を整備し、対応する