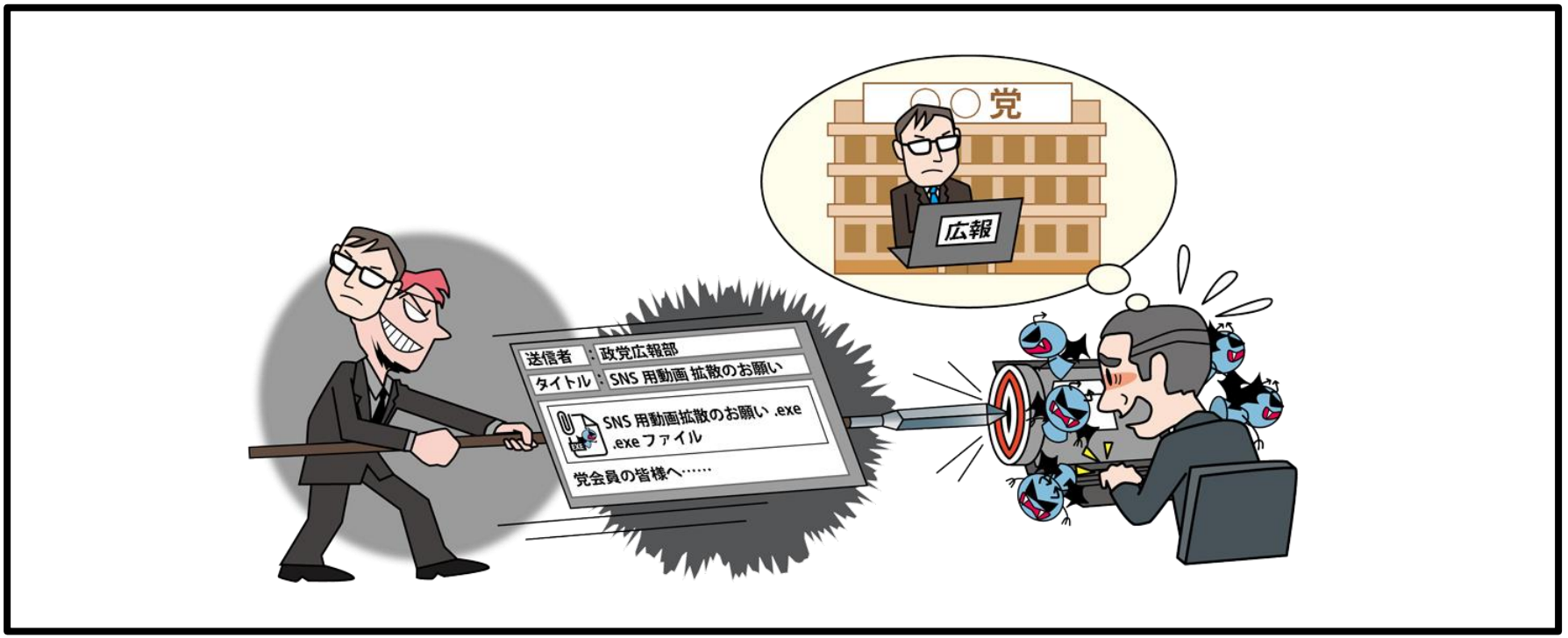
【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～



- メール等を利用し特定組織のPC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

～メールが来たらまずは疑え！？意識は常に高く～

● 攻撃手口

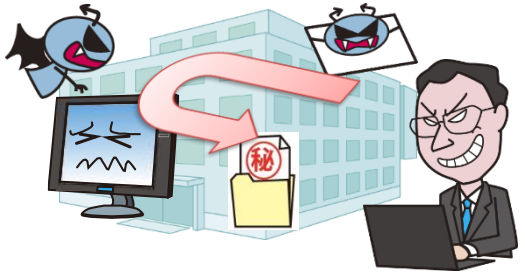
・メールやウェブサイトからウイルスに感染させる

■ メールを利用した手口（標的型攻撃メール）

- 不正な添付ファイルを**開かせる**
- 不正なウェブサイトへのリンクを**クリックさせる**

■ ウェブサイトを利用した手口

- 標的組織が頻繁に利用するウェブサイトを調査し、
  当該サイトを**閲覧する**とウイルスに感染するように改ざん
  （水飲み場型攻撃）



【3位】標的型攻撃による機密情報の窃取

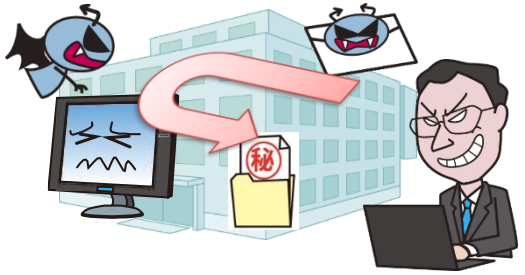
～メールが来たらまずは疑え！？意識は常に高く～

● 攻撃手口

・不正アクセスして認証情報を窃取
・社内システムへ侵入しウイルスを感染させる

■ 不正アクセスによる手口

- 組織が利用するクラウドサービスやウェブサーバー、VPNの**脆弱性を悪用**して不正アクセスし、**認証情報等を窃取**
- 窃取した認証情報等を悪用して正規の経路で社内システムへ侵入し、PCやサーバーを**ウイルスに感染させる**



【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

● 2022年の事例/傾向①

■ シンクタンクへの標的型メール攻撃 (※1,2,3)

・2022年6月に**シンクタンクへの標的型メール攻撃**があったことを警察庁が公開

・メールには個人情報の圧縮ファイルが添付されており、データの代行登録を依頼するという、**業務に関連した内容**であった

・シンクタンクを狙った攻撃は**NISCが注意喚起**しており、IPAも**政府関係機関とよく連携して対応**するよう求めている

【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 学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について(注意喚起)(内閣サイバーセキュリティセンター)
https://www.nisc.go.jp/pdf/press/20221130NISC_press.pdf

※3 サイバーレスキュー隊(J-CRAT)活動状況[2022年度上半期](IPA)
https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000106897.pdf

【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

● 2022年の事例/傾向②

■ 日本の政治団体を狙ったスピアフィッシング（※1）

・2022年、**参議院選挙の直前期間**にスピアフィッシングキャンペーンが行われていたことをESET Researchが公開

・**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ていた

・メールには**悪意のあるファイルが添付**されており、実行すると「LODEINFO」と呼ばれる**ウイルスに感染する**

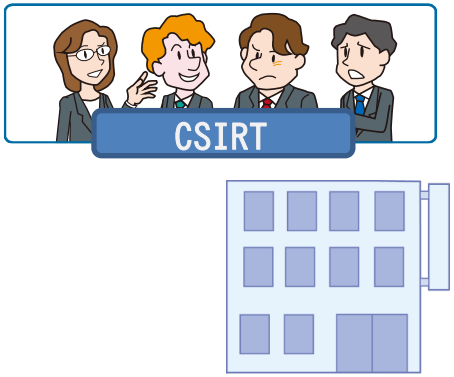
・感染すると不正にコマンドを実行され、情報窃取等の被害にあう

【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

～メールが来たらまずは疑え！？意識は常に高く～

- 対策
  - 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
      - –セキュリティポリシーの策定



【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

● 対策

■ セキュリティ担当者、システム担当者

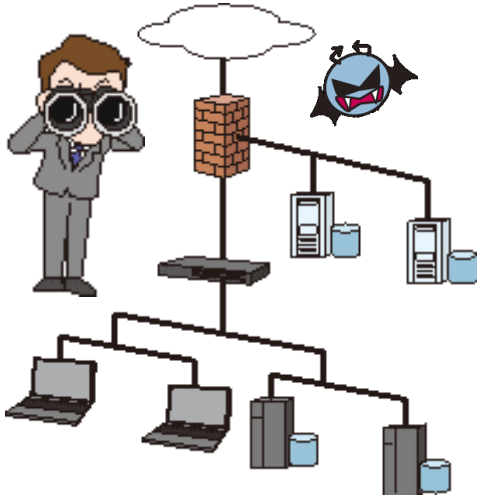
・被害の予防/対応力の向上

- 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
- 従業員に対するセキュリティ教育の実施
- インシデント対応の**定期的**な訓練を実施

※関係者やセキュリティ業者、専門家と迅速に連携できる対応方法や連絡方法を整備する

- 管理端末への**継続的**セキュリティパッチ適用
- 総合運用管理ツール等によるセキュリティ対策状況の**把握**

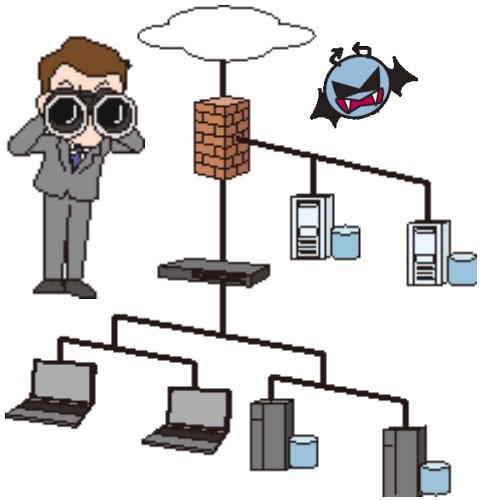
※従業員や職員が利用するPCのソフトウェア更新状況を管理し、リスクの可視化を行う



【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

- 対策
  - セキュリティ担当者、システム担当者
    - ・被害の予防/対応力の向上
      - –アプリケーション許可リストの整備
      - –アクセス権の**最小化**と管理の強化
      - –ネットワーク分離
      - –重要サーバーの**要塞化**（アクセス制御、暗号化等）
      - –**取引先**のセキュリティ対策実施状況の確認
      - –**海外拠点**等も含めたセキュリティ対策の向上
      - –**セキュリティ診断**を行う
      - –**ペネトレーションテスト**を行う

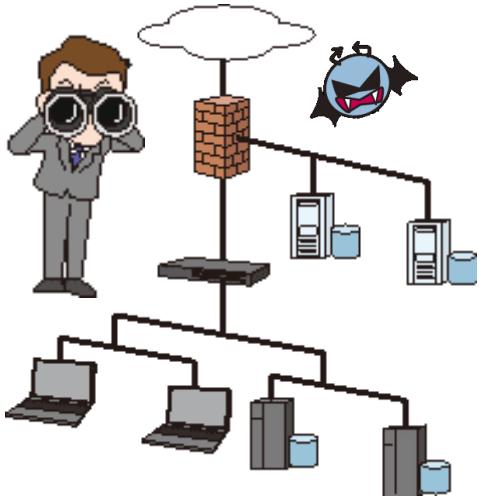


【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

- 対策
  - セキュリティ担当者、システム担当者
    - ・被害の早期検知
      - –UTM、IDS/IPS、WAF、仮想パッチ等の導入
      - –EDR,NDR等を用いたエンドポイントやネットワークの**監視、防御**
      - –ログを取得し**監視や解析**する

        システムログ、アプリケーションログ、サーバーへのアクセスログ、認証ログ、データベース操作ログ、通信ログ等
    - ・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
      - –影響調査および原因の追究、対策の強化



【3位】標的型攻撃による機密情報の窃取

～メールが来たらまずは疑え！？意識は常に高く～

- **対策**
  - **従業員、職員**
    - ・被害の予防（通常、組織全体で実施）
      - －添付ファイルやリンクを**安易にクリックしない**
    - ・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