# 【4位】標的型攻撃による機密情報の窃取

## ～攻撃手口は様々、隙を作らない対策を～


- 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を破壊する

# 【4位】標的型攻撃による機密情報の窃取

## ～攻撃手口は様々、隙を作らない対策を～

IPA

- **攻撃手口**

**・メールを使って標的組織を攻撃する**

- **メールからウイルスに感染させる**
  - 添付ファイルを開封させる
  - メール本文のリンクにアクセスさせる
- **標的組織の従業員や職員を油断させ、不信感を抱かれにくいようにする**
  - メール本文や件名、添付ファイル名は業務や取引に関連するように偽装する
  - 実在する組織の差出人名が使われる
  - メールのやり取りを複数回行う(やり取り型攻撃)

# 【4位】標的型攻撃による機密情報の窃取

## ～攻撃手口は様々、隙を作らない対策を～

- **攻撃手口**

**・Web サイトの改ざん**

- 標的組織が**頻繁に利用する Web サイト**を攻撃者が**改ざん**し、標的組織の従業員や職員がその Web サイトにアクセスした際に、PCが**ウイルスに感染**する(水飲み場型攻撃)

# 【4位】標的型攻撃による機密情報の窃取

## ～攻撃手口は様々、隙を作らない対策を～

- **攻撃手口**

**・不正アクセス**

- **標的組織が利用するものの脆弱性を悪用して不正アクセスをし、組織内部に侵入する**
  - クラウドサービス
  - Webサーバー
  - VPN装置
- **認証情報等を窃取し、組織のシステムへ再侵入する**

# 【4位】標的型攻撃による機密情報の窃取

## ～攻撃手口は様々、隙を作らない対策を～

- **2023年の事例/傾向①**
  - **複数回のやり取りを伴う標的型メール攻撃**
    - 2023年10月、東京大学は標的型攻撃メールにより教員のPCがウイルスに感染し、情報を窃取されたことを公表した
    - 2022年7月に実在する組織の担当者を騙った人物からメールが届き、教員がやりとりをしている中でメールに記載されたURLをクリックしたところ、ウイルスに感染した
    - 最終的に教員は被害に気付かなかった
    - 教職員や学生等の個人情報や過去の試験問題等の計4,341 件が流出したおそれがある

【出典】 東京大学大学院総合文化研究科・教養学部への不正アクセスによる情報流出について(東京大学)
https://www.u-tokyo.ac.jp/focus/ja/press/z0109_00952.html
サイバー攻撃か 東大教員のパソコンに不正アクセス、個人情報4300件流出(TBS NEWS DIG)
https://newsdig.tbs.co.jp/articles/-/796546

# 【4位】標的型攻撃による機密情報の窃取

## ～攻撃手口は様々、隙を作らない対策を～

- **2023年の事例/傾向②**
  - **JAXAに不正アクセスがあったが情報は取られず**
    - 2023年11月、宇宙航空研究開発機構(JAXA)が<u>サイバー攻撃</u>を受け、内部ネットワークに<u>不正アクセス</u>された
    - 不正アクセスを受けたのは一般業務用の管理サーバーであり、<u>機微情報は含まれていなかった</u>
    - 不正アクセスはネットワーク機器の<u>脆弱性を悪用</u>されたものとみられる
    - 外部機関から通報を受けたJAXAは<u>文部科学省に報告</u>し、<u>一部のネットワークを切り離した</u>上で、調査をしている

【出典】 JAXAにサイバー攻撃＝不正アクセス、機微情報含まず(時事通信社)
https://sp.m.jiji.com/article/show/3109334
JAXAへの不正アクセスについてまとめてみた(piyolog)
https://piyolog.hatenadiary.jp/entry/2023/11/29/123934

# 【4位】標的型攻撃による機密情報の窃取

## ～攻撃手口は様々、隙を作らない対策を～

- **2023年の事例/傾向③**
  - **ネットワーク貫通型攻撃に注意**
    - 2023年8月、IPAは企業や組織のネットワークとインターネットとの境界に設置されるセキュリティ製品の脆弱性が狙われ、ネットワーク貫通型攻撃としてAPT攻撃に利用されていると注意喚起を行った
    - ネットワーク内部へ不正アクセスされた場合、保有情報の漏えいや改ざん、他組織への攻撃の踏み台になるおそれがあるため、日々の確認や平時の備えが大切である
    - 同年5月に経済産業省が公開した「ASM(Attack Surface Management)導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」の活用も有効である

【出典】 インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～(IPA)
https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html
「ASM(Attack Surface Management)導入ガイダンス
～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめました(経済産業省)
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

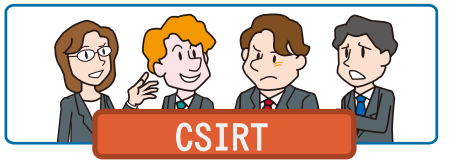
# 【4位】標的型攻撃による機密情報の窃取

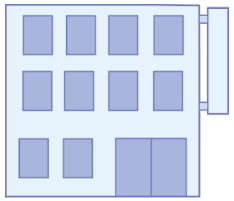
## ～攻撃手口は様々、隙を作らない対策を～

- **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



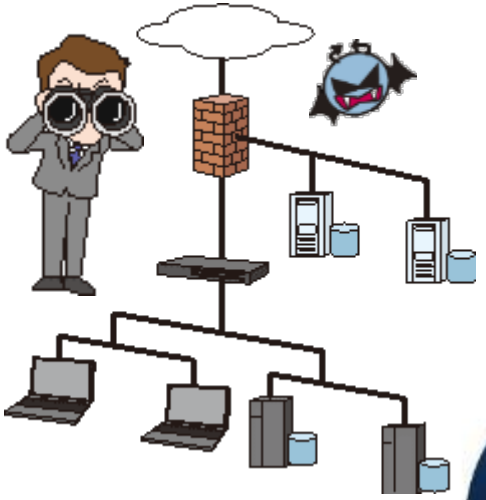
# 【4位】標的型攻撃による機密情報の窃取

## ～攻撃手口は様々、隙を作らない対策を～

- **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／対応力の向上】**

- 情報の管理と運用規則策定
- サイバー攻撃に関する継続的な情報収集
- 情報リテラシー、モラルを向上させる
- インシデント対応の定期的な訓練を実施
- 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
- アプリケーション許可リストの整備
- 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



# 【4位】標的型攻撃による機密情報の窃取

## ～攻撃手口は様々、隙を作らない対策を～

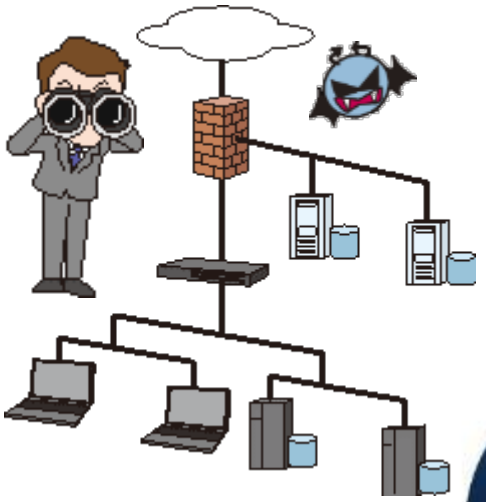
- **対策**
  - **組織(セキュリティ担当者、システム管理者)**

**【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



# 【4位】標的型攻撃による機密情報の窃取

## ～攻撃手口は様々、隙を作らない対策を～

- **対策**
  - **組織(従業員、職員)**

**【被害の予防(通常、組織全体で実施)】**

- 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

**【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