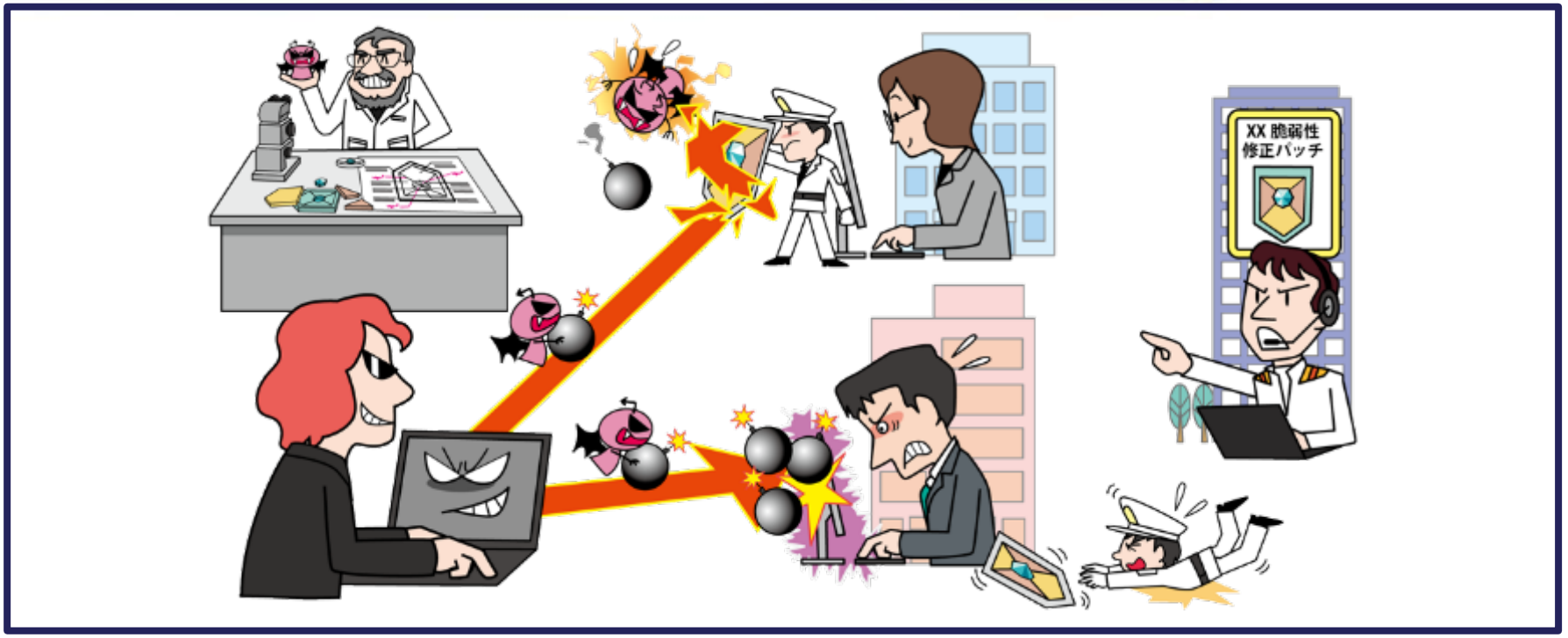
【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～



- 脆弱性対策のために公開された脆弱性情報を攻撃者が悪用する
- 広く利用されている製品の脆弱性の場合は被害が広範囲に及ぶ
- 脆弱性情報の公開後、それらを悪用した攻撃が発生するまでの時間が近年は短くなっている傾向がある

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **攻撃手口**

・対策前の脆弱性(Nデイ脆弱性)を悪用

- **公開されたパッチの適用や回避策を講じるまでの期間(N日)の脆弱性をNデイ脆弱性と呼ぶ**
  - ソフトウェアの管理が不適切な企業は、未対応の時間(N 日)が長くなるため、被害に遭うリスクが大きくなる
  - 脆弱性が攻撃可能であることを実証するPoC(実証コード)が公開され、攻撃に悪用されることもある

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

♦ 攻撃手口

・公開されている攻撃ツールを使用

- 公開された脆弱性に対する攻撃ツールは**短期間で作成される**
- **ダークウェブ上**のWebサイト等での**販売**や、**攻撃サービスとして提供**されたりする
- 誰でも利用可能なオープンソースのツールに**脆弱性を利用する機能が実装**され、それを**悪用**される

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **2023年の事例/傾向①**
  - **ソフトウェアの修正版公開後に攻撃活動の増加**
    - 2023年10月25日、Apache Software Foundationは Apache ActiveMQ等で、リモートからコード実行が可能な脆弱性を対策したバージョンを公表した
    - 本脆弱性は技術情報や実証コードが公開されており、Rapid7によると10月27日に脆弱性を悪用したと見られるランサムウェアの活動を同社の複数の顧客で確認していた
    - NICTのダークネット観測網では、同脆弱性に関連した通信を10月27日頃 から観測し、11月26日頃には更なる通信の増加が確認されてボットとみられる感染活動を観測した

【出典】「Apache ActiveMQ」の脆弱性が標的に - ランサム攻撃にも悪用か(Security NEXT)
https://www.security-next.com/150846
CVE-2023-46604: Apache ActiveMQ の悪用の疑い(ラピッドセブン・ジャパン株式会社)
https://www.rapid7.com/ja/about/japan-blog-and-news/etr-suspected-exploitation-of-apache-activemq-cve-2023-46604/
ActiveMQの脆弱性(CVE-2023-46604)を悪用したボットの感染活動について(NICTER Blog)
https://blog.nicter.jp/2023/12/cve-2023-46604/

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **2023年の事例/傾向②**
  - **VPN機器の脆弱性が断続的な攻撃の対象に**
    - 2023年5月、Array Networksが提供する「Array AG シリーズ」の脆弱性を悪用した標的型攻撃が観測されていることをJPCERTコーディネーションセンターが注意喚起した
    - 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が行われているとして、 IPAにおいても2023年8月に注意喚起を行った
    - 本脆弱性は２つあり、それぞれ2022年の9月、2023年3月に修正されているが、海外拠点も標的となっており、自組織の海外拠点における対策や侵害調査を行うことも推奨されている

【出典】 Array Networks Array AGシリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起
(一般社団法人JPCERTコーディネーションセンター)
https://www.jpcert.or.jp/at/2023/at230020.html
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
Array Networks製VPN機器、標的型攻撃の対象に - 侵害状況の確認を(Security NEXT)
https://www.security-next.com/149480

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **2023年の事例/傾向③**
  - **脆弱性を修正した機器へ継続的な攻撃**
    - 2023年5月19日、Barracuda Networksは同社の製品のESGにリモートからシステムコマンドが実行可能となる脆弱性があることを特定し、翌日に修正パッチを公開した
    - 本脆弱性の修正対応後も、特定の組織では攻撃者による継続的な攻撃活動が確認されている
    - 同社では脆弱性の最初の悪用は2022年10月とし、侵害された組織にアプライアンスの交換を推奨している
    - FBI、IPA、JPCERTコーディネーションセンターにおいても注意喚起を行っており、修正パッチを済ませた組織でも追加の侵害調査を行う事を推奨した

【出典】 Barracuda製メールセキュリティ製品に脆弱性 - すでに悪用も(Security NEXT)
https://www.security-next.com/146475
Barracuda、「ESGアプライアンス」の交換を呼びかけ(Security NEXT)
https://www.security-next.com/146896
Barracuda 製 Email Security Gateway Appliance (ESG) の脆弱性について(CVE-2023-7102)(CVE-2023-7101)(IPA)
https://www.ipa.go.jp/security/security-alert/2023/alert20231225.html
Barracuda Email Security Gateway(ESG)の脆弱性(CVE-2023-2868)を悪用する継続的な攻撃活動に関する注意喚起
(一般社団法人JPCERTコーディネーションセンター)
https://www.jpcert.or.jp/at/2023/at230017.html

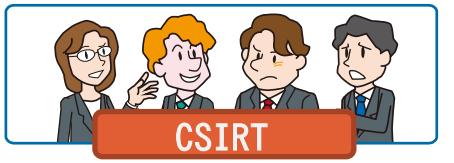
【7位】脆弱性対策情報の公開に伴う悪用増加

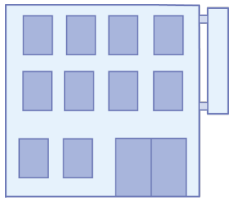
～放置せず、傷口が広がる前に速やかな処置を～

- **対策**
  - **組織(経営者層)**

【被害の予防】

- 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





【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **対策**
  - **個人、組織(システム管理者/ソフトウェア利用者)**

【被害の予防】

- 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
- 脆弱性関連情報の収集と対応
- 一時的なサーバー停止等

【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】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- インシデント対応体制を整備し、対応する

【7位】脆弱性対策情報の公開に伴う悪用増加

～放置せず、傷口が広がる前に速やかな処置を～

- **対策**
  - **組織(開発ベンダー)**

【製品セキュリティの管理、対応体制の整備】

- 製品に組み込まれているソフトウェアの把握、管理の徹底
- 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
- 脆弱性発見時の対応手順の作成
- 脆弱性情報を迅速に発信する仕組みの整備