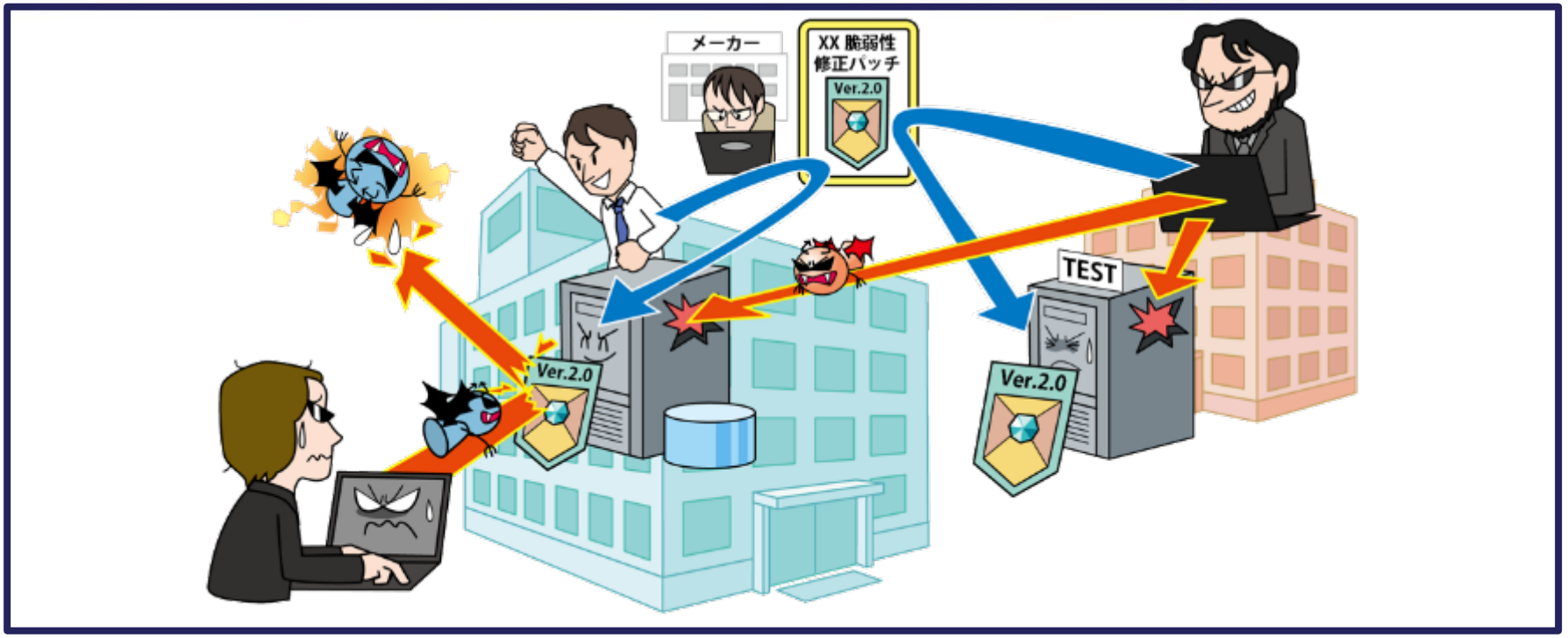
【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～



- 脆弱性の修正プログラム(パッチ)や回避策が公開される前に脆弱性を悪用した攻撃が行われる
- 事業やサービスの停止など、多くのシステムやユーザーに被害が及ぶ
- 脆弱性対策情報が公開された場合は、早急な対応が求められる

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

IPA

- **攻撃手口**

・開発ベンダ―等が脆弱性を認識しないとその脆弱性に対する修正プログラムは作成されない
・その修正プログラムが公開される前の脆弱性を悪用

- **修正プログラムが公開される前に発見した(された)脆弱性を悪用**
- **悪用の手口は脆弱性毎に様々なものがある**
  - DDoS攻撃(分散型サービス妨害攻撃)
  - 簡易プログラム(スクリプト)の実行
  - 特権アカウントの作成

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **2023年の事例/傾向①**
  - **HTTP/2の脆弱性を悪用したゼロデイ攻撃**
    - 2023年8月、HTTP/2プロトコルの脆弱性を狙った大規模なDDoS攻撃が確認される
    - 一連の攻撃で1秒間に3億9,800万件を超えるリクエストが発生しており、過去最大規模の4,600万件のリクエストが発生したケースをはるかに上回る規模の攻撃である
    - この攻撃は、HTTP/2ラピッドリセット攻撃と呼ばれており、HTTP/2 をサポートする多くのソフトウェアに影響を与える
    - 影響を受けるソフトウェアの開発ベンダー間で情報共有が進められて、パッチやアップデートが提供された

【出典】 ラピッドリセット攻撃」が発生 - 1秒間で約4億リクエスト(Security NEXT)
https://www.security-next.com/150165

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **2023年の事例/傾向②**
  - **「WinRAR」の脆弱性を悪用したゼロデイ攻撃**
    - 2023年4月、ファイル圧縮ソフトの「WinRAR」に複数の脆弱性が存在しており、一部の脆弱性がゼロデイ攻撃に悪用されていることが分かった
    - 圧縮ファイル内のファイルのプレビューを行おうとすると、同名のフォルダ内に配置されたスクリプトを実行させることが可能になるという脆弱性であった
    - 2023年8月2日、開発元である「RARLAB」は、脆弱性の修正をしたバージョンアップ版「WinRAR 6.23」をリリースしている

【出典】 4月以降「WinRAR」狙うゼロデイ攻撃が発生 - 最新版に更新を(Security NEXT)
https://www.security-next.com/148924

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **2023年の事例/傾向③**
  - **Cisco Systems製品へのゼロデイ攻撃**
    - 2023年10月、Cisco Systems は「Cisco IOS XE」に、リモートから認証がなくとも特権アカウントを作成できる脆弱性があることを公表した
    - 2023年9月中旬よりゼロデイ攻撃が行われていることも公表した
    - 同社は、顧客のサポート中に脆弱性を確認した
    - 同製品の利用者に対して、開発ベンダー等が推奨する対策を講じるとともに、侵害を受けていないか確認するように呼びかけている

【出典】「IOS XE」の深刻なゼロデイ脆弱性 - JPCERT/CCも攻撃被害を確認(Security NEXT)
https://www.security-next.com/150345

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **参考情報（2024年の最新事例）**
  - **Ivanti VPN製品へのゼロデイ攻撃**
    - 現地時間2024年1月10日にIvantiからIvanti Connect Secure および Ivanti Policy Secure Gatewaysに関する脆弱性情報が公開された
    - 本脆弱性（CVE-2024-21887,CVE-2023-46805）を悪用されると、認証を回避されて第三者にコマンドを実行されるおそれがあった
    - 日本時間1月11日にIPAにおいても注意喚起を行っており、1月15日には国内での悪用も確認され、侵害の調査などの対応を推奨した
    - その後さらに、CVE-2024-21888,CVE-2024-21893,CVE-2024-22024などの脆弱性も確認され、2月16日までに修正パッチが順次公開された

【出典】CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways (Ivanti)
https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
KB CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways (Ivanti)
https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
Ivanti Connect Secure（旧Pulse Connect Secure）および Ivanti Policy Secure Gateways の脆弱性対策について(CVE-2023-46805 等) (IPA)
https://www.ipa.go.jp/security/security-alert/2023/20240111.html
Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）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/2024/at240002.html

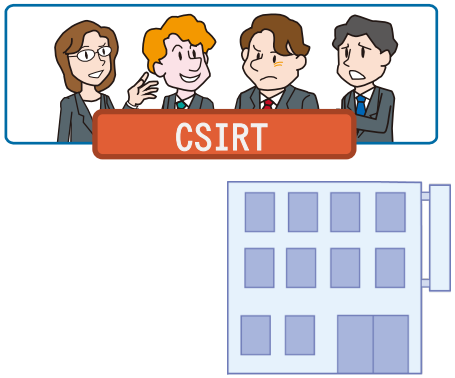
【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

- **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



【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

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

【被害の予防】

- 資産の把握、対応体制の整備
- セキュリティのサポートが充実しているソフトウェアやバージョンを使う
- 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
- 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

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

～脆弱性対策情報が公開されたら即時対応を～

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

【修正プログラムのリリース前の対応】

- 回避策や緩和策の適用
- 当該ソフトウェアの一時的な使用停止、場合によってはサービスの停止も検討する

【修正プログラムリリース後の対応】

- 修正プログラムの適用

【被害を受けた後の対応】

- 影響調査、原因の追究、対策の強化
- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等