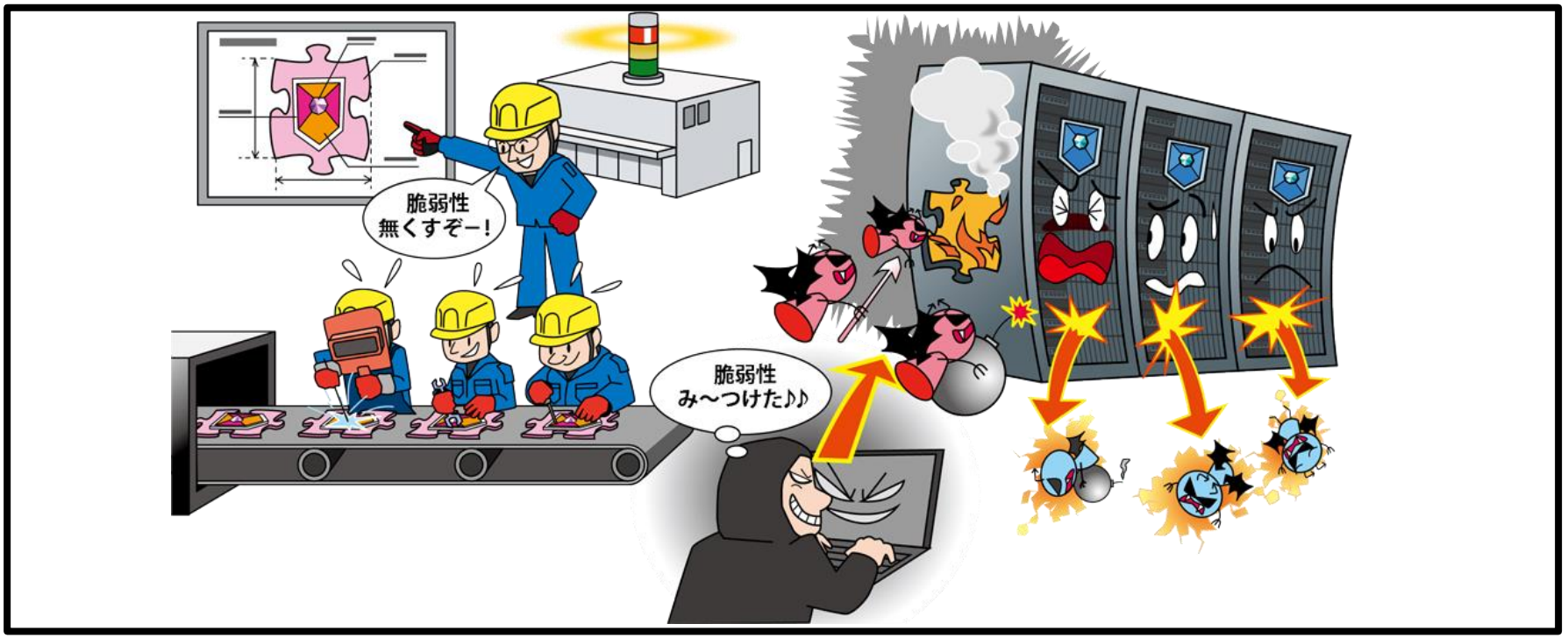
【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表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
- 攻撃を確実に防ぐ事前の対策は難しく、**いつのまにか被害に遭うおそれ**がある

【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～

● 攻撃手口

・開発ベンダー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

・確実な事前の対策は難しく、無防備な状態の組織を狙う

【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～

- 2022年の事例/傾向①
  - Fortinet製品 へのゼロデイ攻撃（※3,4,5）
    - 2022年12月、FortiGate等のセキュリティアプライアンス製品にOSとして搭載されている**FortiOSの脆弱性を公表**
    - 遠隔の第三者に認証を回避され、任意のコードやコマンドを実行されるおそれ
    - 影響する製品には**サポート終了バージョンも含まれていた**
    - 対策や緩和策だけでなく、脆弱性を悪用した**攻撃のログや痕跡等の調査も推奨**された

【出典】

※1 FortiOS - heap-based buffer overflow in sslvpnd（Fortinet, Inc.）
https://www.fortiguard.com/psirt/FG-IR-22-398

※2 Fortinet製品のSSL VPN機能に脆弱性 - すでに悪用、侵害調査を（Security NEXT）
https://www.security-next.com/142121

※3 FortiOSのヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）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/2022/at220032.html

【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～

● 2022年の事例/傾向②

(※1,※2)

■ Microsoft Exchange Serverでゼロデイ攻撃が発生

・ベトナムのセキュリティ企業が、Microsoft Exchange Serverの**未修正の脆弱性を悪用する攻撃発生**を2022年9月に公表

・マイクロソフトは**脆弱性に関する情報と緩和策**を同月に公開

・マイクロソフトは、脆弱性を悪用してユーザーのシステムに侵入する限定的な標的型攻撃を確認しているとし、11月に**修正プログラムをリリースするまで、暫定的な緩和策を案内**

【出典】

※1　Microsoft Exchange Serverでゼロデイ攻撃が発生（トレンドマイクロ株式会社）
https://www.trendmicro.com/ja_jp/research/22/i/ms-exchange-zero-day.html

※2　Microsoft Exchange サーバーのゼロデイ脆弱性報告に関するお客様向けガイダンス（Microsoft Security Response Center）
https://msrc-blog.microsoft.com/2022/09/30/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server-ja/

【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～

● 対策

■ 組織（システム管理者）

・被害の予防

- 資産の把握、対応体制の整備
- NDR等を用いたネットワークの監視および攻撃通信の遮断
- EDR等を用いたエンドポイントの監視、防御
- 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
- セキュリティ診断やペネトレーションテストを行う

・攻撃の予兆／被害の早期検知

- UTM、IDS/IPS、WAF、仮想パッチ等の導入

【6位】修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～事前に防ぐことは困難。悪用の情報が公表されたら即時対応を～

● 対策

■ 組織（システム管理者）

・修正プログラムリリース前の対応

－**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**

・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

必要に応じて回避策、緩和策を**無効化**する。

・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

－影響調査および原因の追究、対策の強化