脆弱性対策の効果的な進め方

2024年03月19日

独立行政法人情報処理推進機構
セキュリティセンター

IPA Better Life with IT

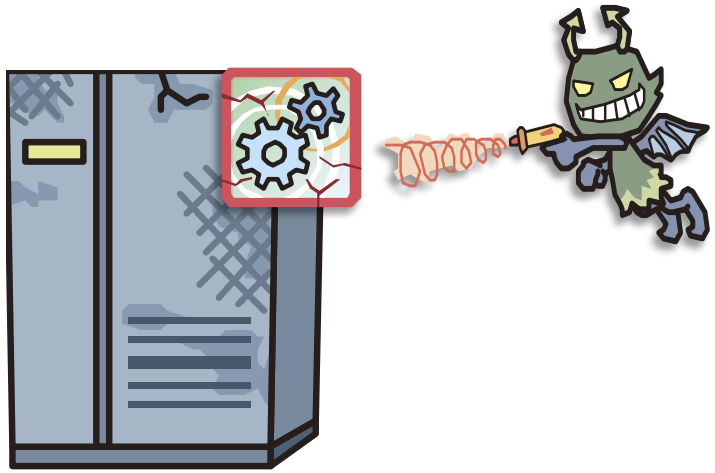
セミナーの内容

1. 脆弱性とは
2. 脆弱性関連情報の収集
3. 共通脆弱性評価システムCVSSとは
4. CVSSを使った評価事例
5. IPAの脆弱性対策支援ツール紹介

1. 脆弱性とは

脆弱性とは

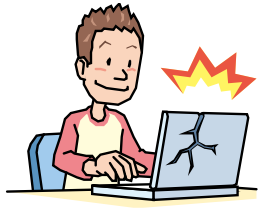
- **コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した<u>セキュリティ上の欠陥</u>**



✓ウイルスに感染させられる
✓ウェブページを改ざんされる
✓クレジットカードなどの個人情報が窃取される

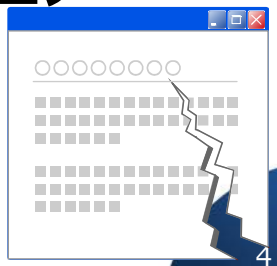
脆弱性は様々なソフトウェアに存在する（1）

- **PCにインストールされているソフトウェア**
  - ✓OS(Windows)
  - ✓ソフトウェア(Adobe Reader)
  - ✓ソフトウェア(Oracle Java)

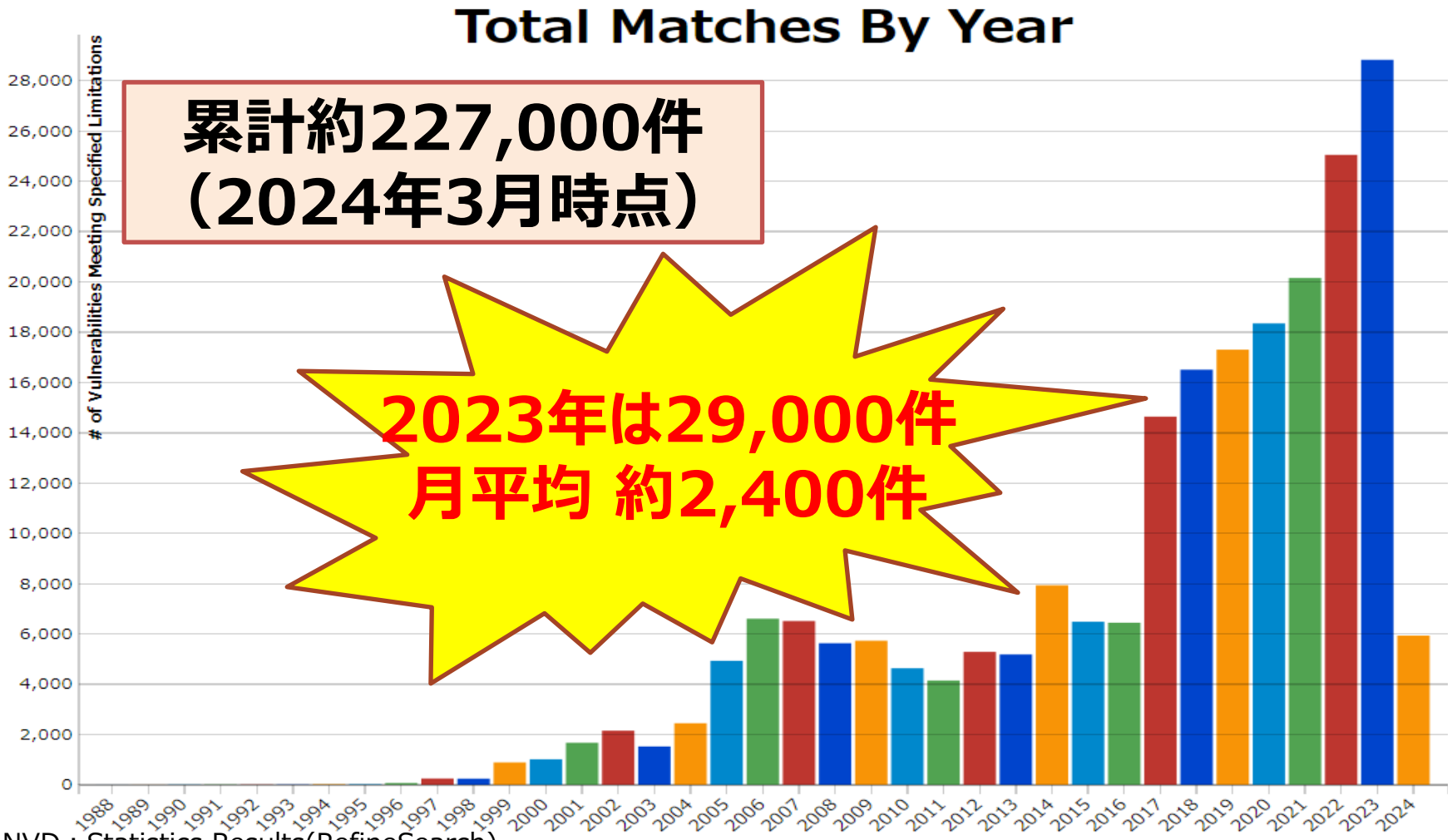


- **組織で公開しているウェブサイト**
  - ✓ミドルウェア(Apache HTTP Server)
  - ✓コンテンツ管理システム(WordPress)

- **国内政府機関から提供されているソフトウェア**
  - ✓ソフトウェア(e-Gov電子申請アプリケーション)



脆弱性は様々なソフトウェアに存在する（2）
～日々公表される膨大な数の脆弱性～



NVD：Statistics Results(RefineSearch)
https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false

脆弱性は様々なソフトウェアに存在する（3）
～時にはインフラにかかわる製品にも～

■テレワークで使用するツール

✓VPN接続機器の脆弱性

→脆弱性が悪用されると、遠隔の第三者によって、
任意のコードやコマンドを実行されるおそれがある。（2022年12月）

IPA ： https://www.ipa.go.jp/security/security-alert/2022/alert20221213.html

■社会インフラを支えるツール

✓数百万個のIoT機器が影響を受ける脆弱性群

→医療、電力、石油、製造などのインフラ業界の機器も影響を受けるとされている。脆弱性が悪用されると、リモートコードの実行によって機器を制御され、大きな被害に繋がるおそれがある。（2020年6月）

トレンドマイクロ ： https://blog.trendmicro.co.jp/archives/25346

脆弱性は様々なソフトウェアに存在する（4）
～脆弱性をねらう攻撃～

Exchange Server の脆弱性を狙った攻撃

→Microsoft より Exchange Server の脆弱性に関する情報が公開された。
脆弱性を組み合わせることで、攻撃者により任意のコードを実行される
おそれがあり、悪用も確認された。（2022年11月）

Security NEXT： https://www.security-next.com/141302

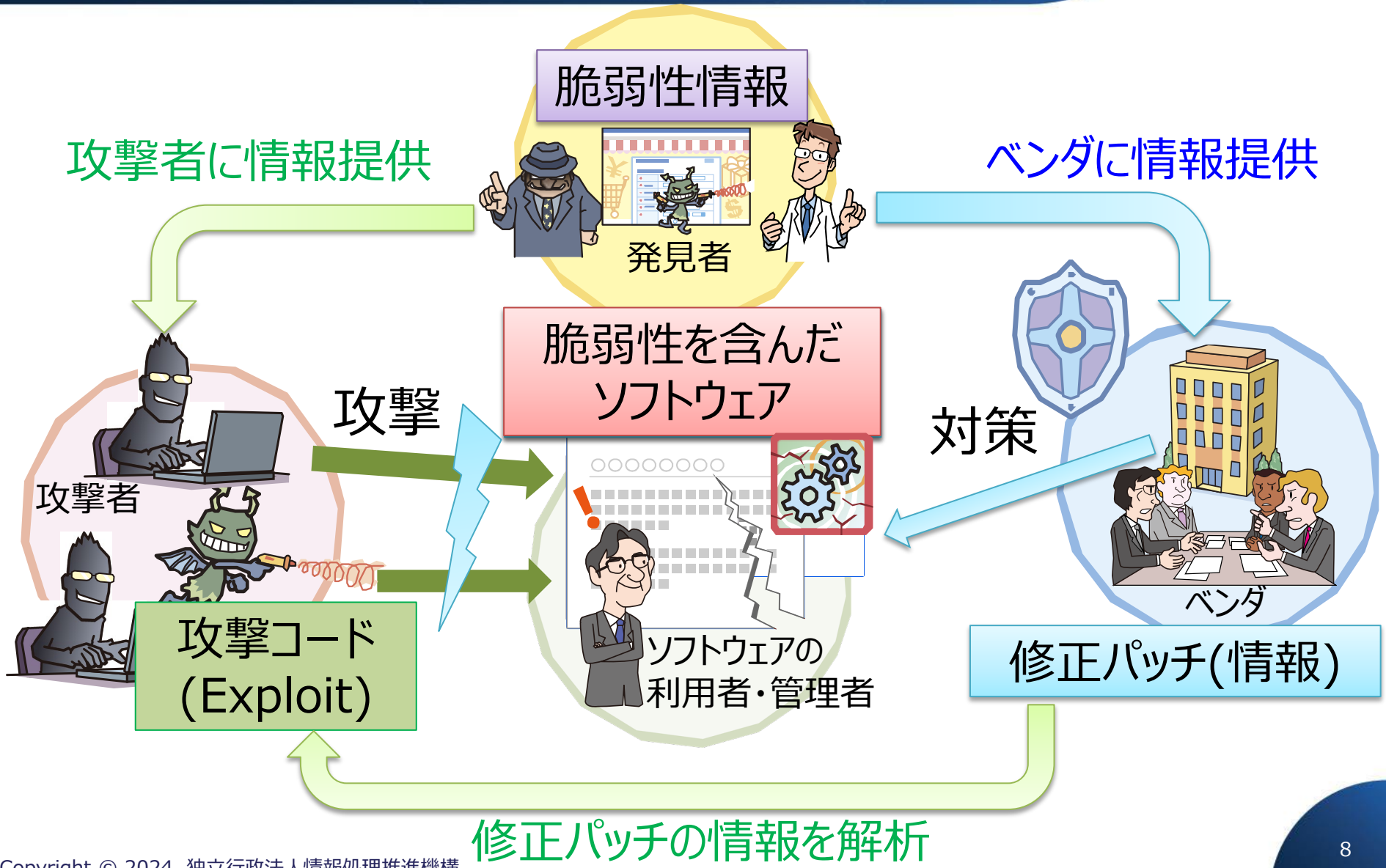
広く普及している製品の脆弱性が狙われる

→Apache Software Foundation から、Apache Log4j にリモートから
任意のコードが実行可能な脆弱性が発表され、翌日に脆弱性を悪用した
攻撃が確認された。（2021年12月）

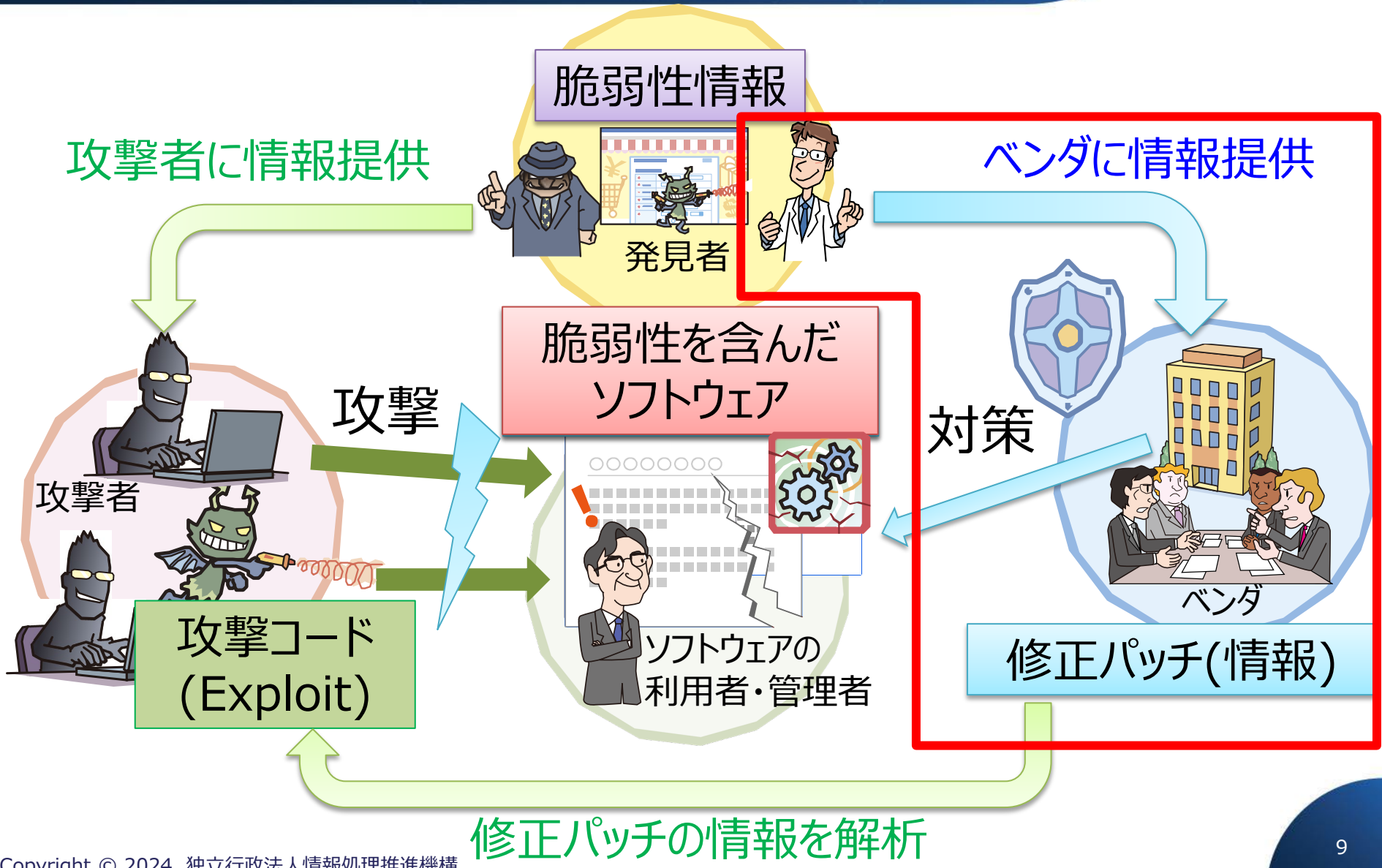
株式会社ラック：
https://www.lac.co.jp/lacwatch/alert/20211213_002820.html

様々なソフトウェアで脆弱性が確認され、攻撃を受けている。

脆弱性が発見された際の流通経路（1）



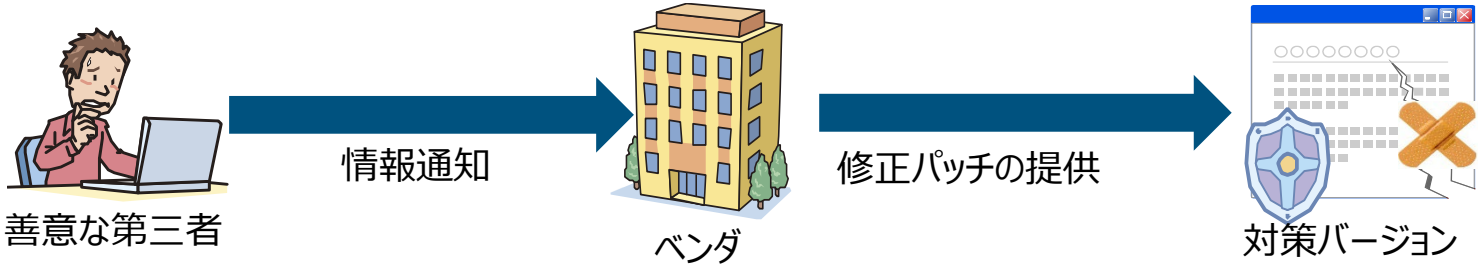
脆弱性が発見された際の流通経路（2）
～脆弱性と攻撃の関係（平時）～



脆弱性が発見された際の流通経路（2）
～脆弱性と攻撃の関係（平時）～

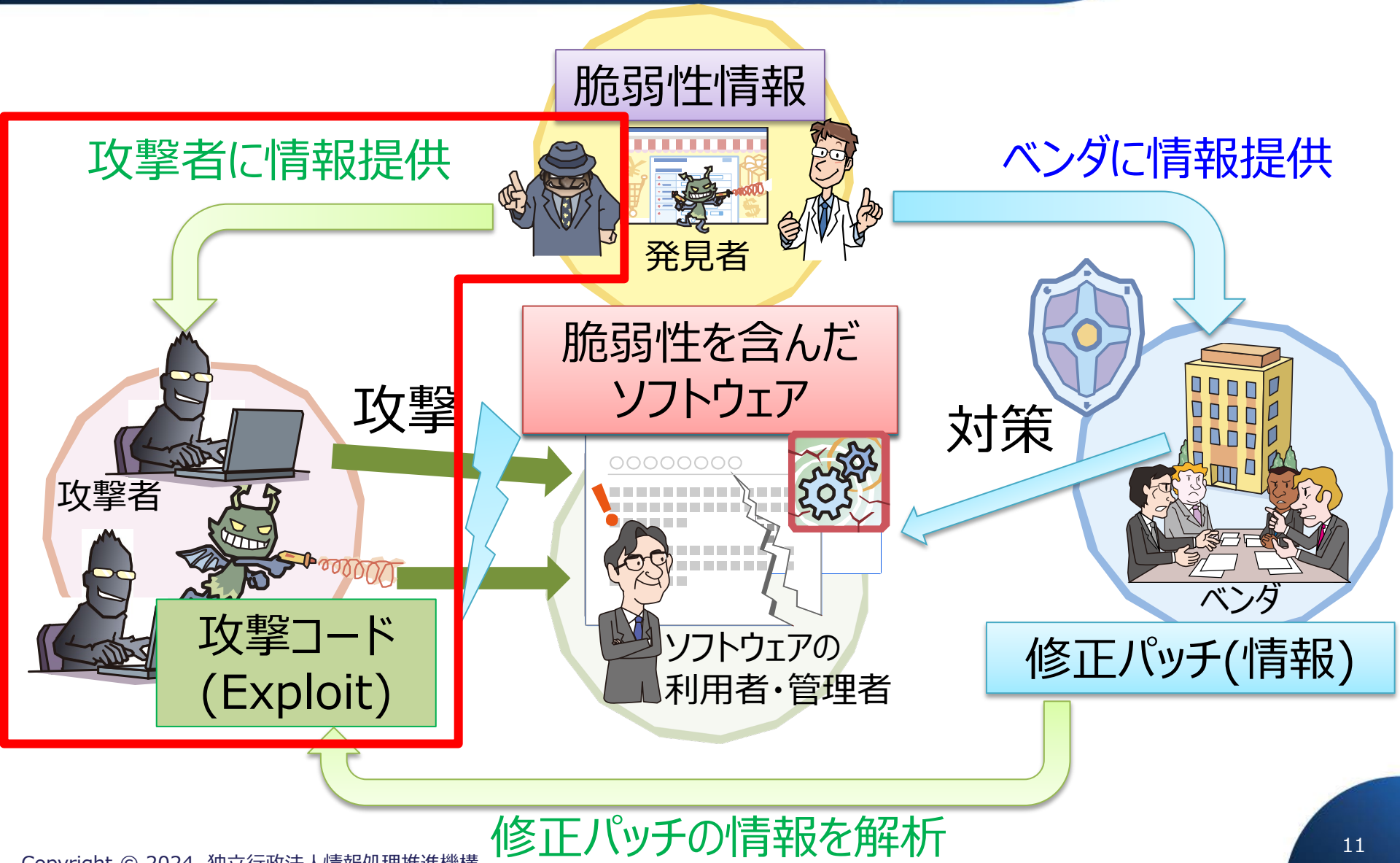
発見者が製品ベンダ

発見者が善意な第三者



- ✓ 脆弱性情報が安全に流通されたケース（危険度低）
- ✓ 攻撃を受ける前に修正パッチを入手することが可能
- ✓ 修正パッチが未適用の場合、攻撃の被害に遭う可能性がある

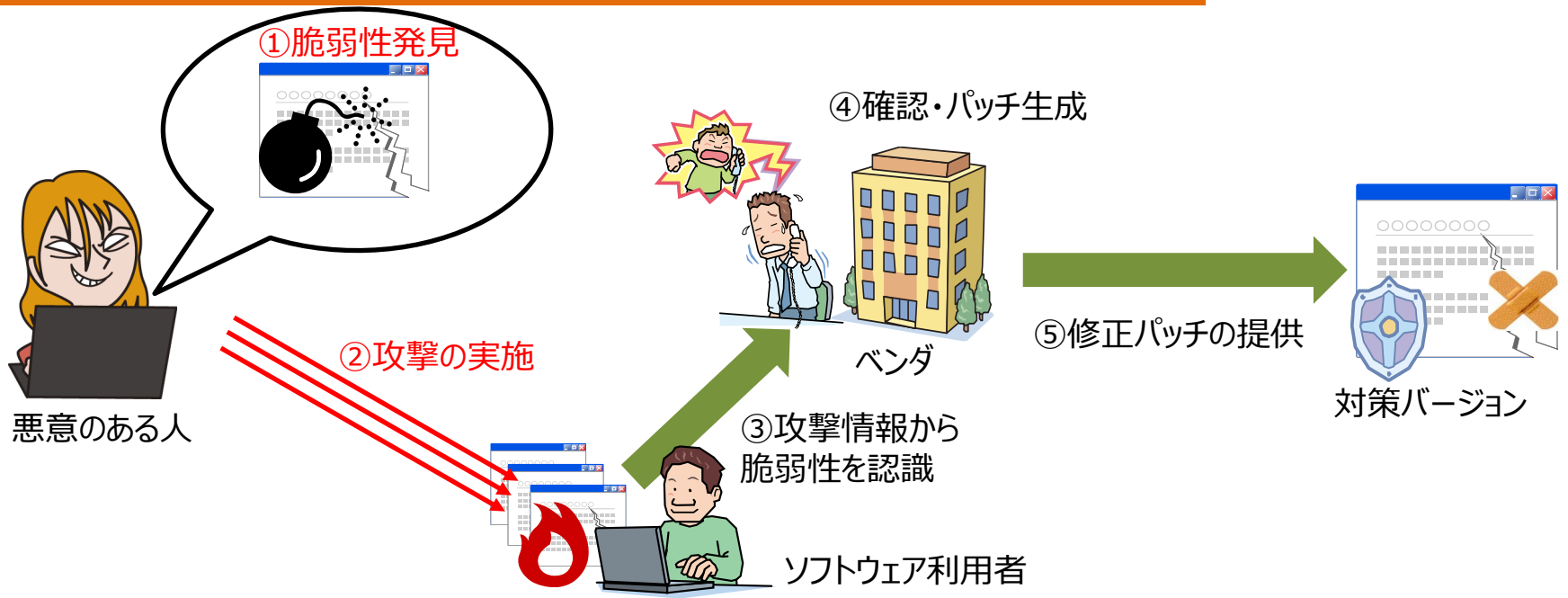
脆弱性が発見された際の流通経路（3）
～脆弱性と攻撃の関係（ゼロデイ攻撃）～



脆弱性が発見された際の流通経路（3）
～脆弱性と攻撃の関係（ゼロデイ攻撃）～

IPA

発見者が攻撃者または悪意ある第三者



- ✓ 攻撃により脆弱性の存在を認識するケース(危険度大)
- ✓ 攻撃が実際に行われ、被害が発生しているおそれがある
- ✓ ベンダの対応を待つため、修正パッチの適用に時間がかかる
- ✓ 利用者はパッチ提供まで、暫定の対応策を検討する必要がある

脆弱性が発見された際の流通経路（4）
～修正パッチを放置しない～

発見者が脆弱性情報を公開したら

攻撃者に攻撃される前に

ベンダから提供される修正パッチを

ソフトウェアの利用者・管理者が適用する

脆弱性を悪用する攻撃とは？

脆弱性が攻撃されると怖いことはわかったけど、実感がわかない

それでは、実際にどのように脆弱性を悪用して攻撃するのか、見てみましょう

脆弱性への攻撃例

クロスサイトスクリプティング（XSS）

- ✓Webサイトに書かれているスクリプトが、別のWebサイトへとまたがって（クロスして）実行されることから、クロスサイトスクリプティングと呼ばれる。
- ✓Webサイトを閲覧する、またはリンクをクリックすると、
  - →偽ページが表示される
  - →他の不正サイトへ誘導させられる

クロスサイトスクリプティングの脆弱性

攻撃の流れ

掲示板

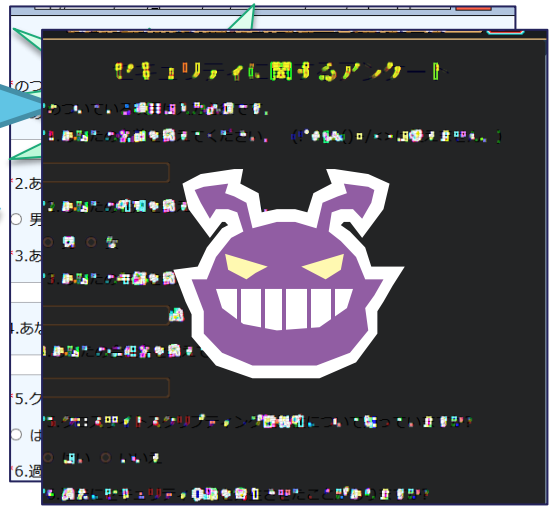
③． 閲覧・クリック

②． リンク表示

④． 偽ページが表示

掲示板利用者

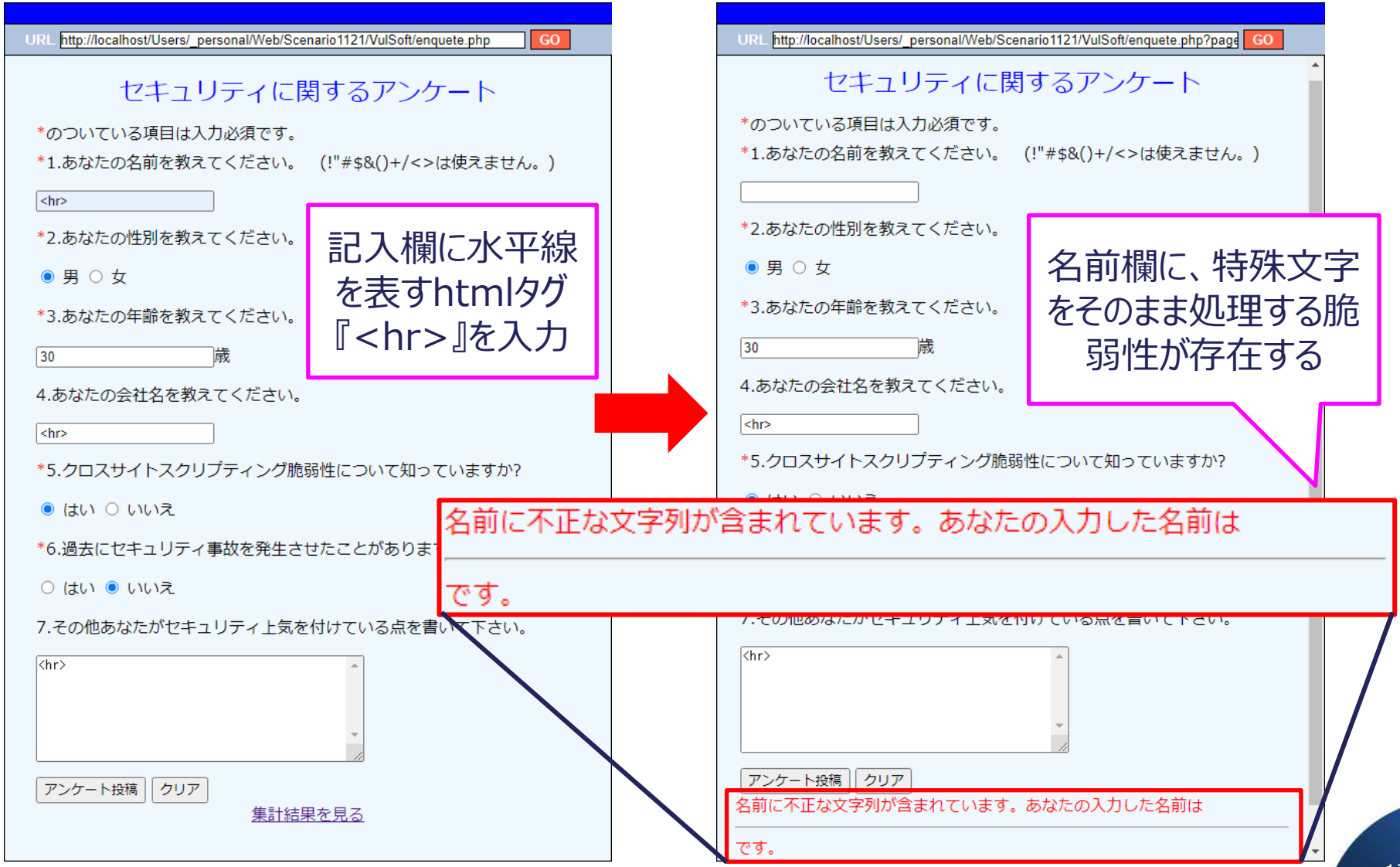
脆弱性を含むアンケートページ



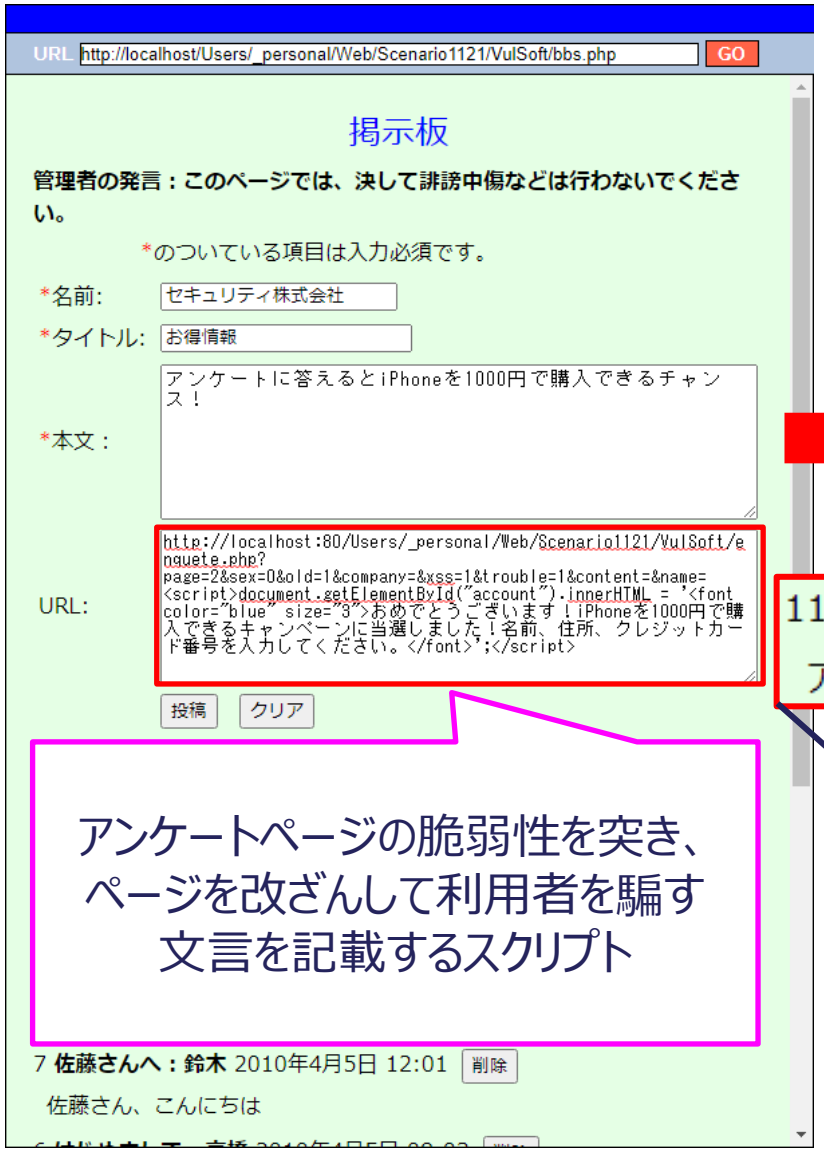
①.細工したスクリプト

攻撃者

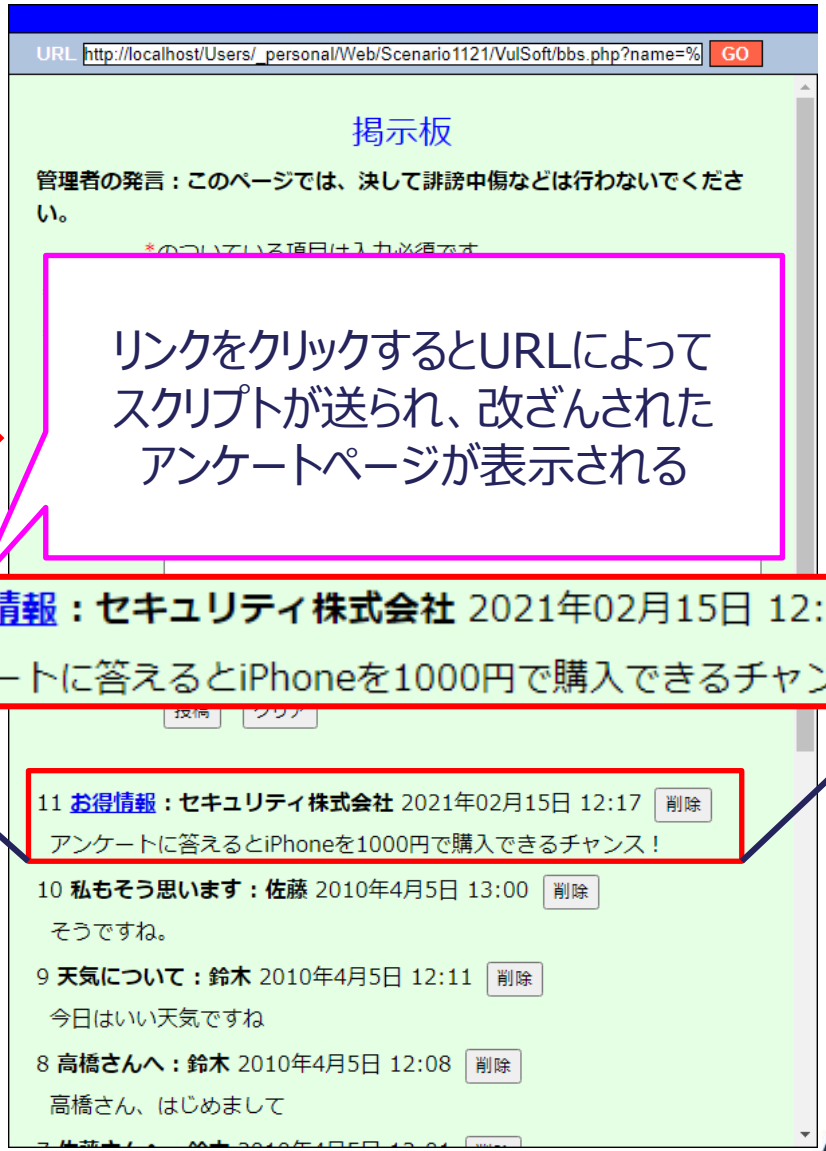
クロスサイトスクリプティング　攻撃例
～攻撃者目線～



クロスサイトスクリプティング　攻撃例
～攻撃者目線～

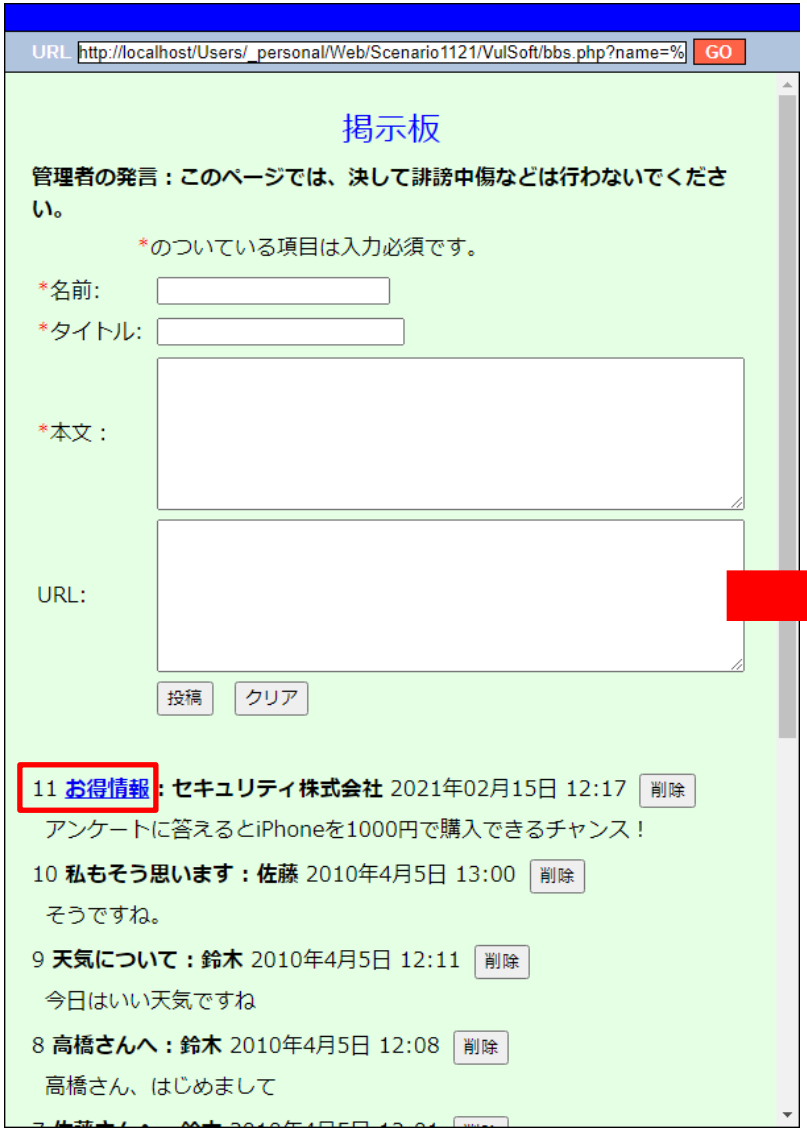


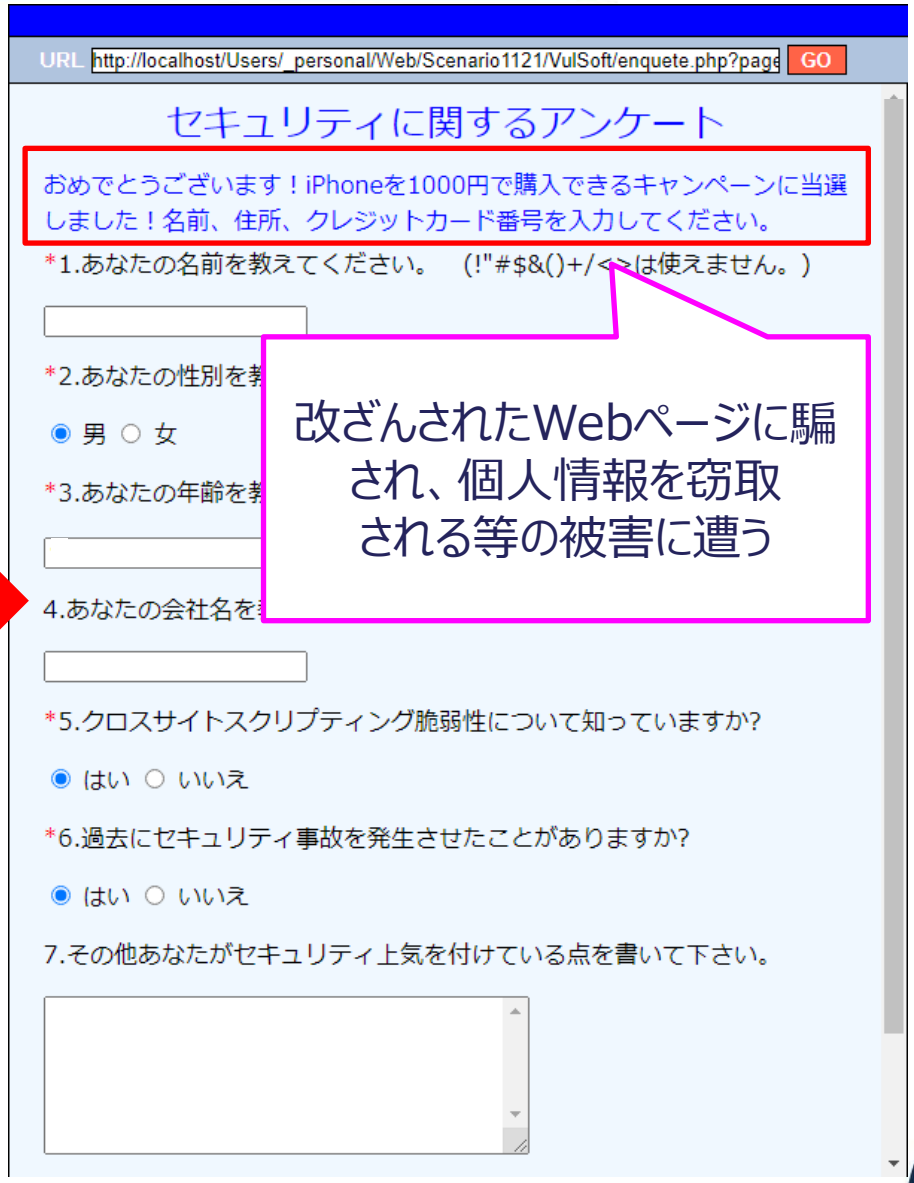
アンケートページの脆弱性を突き、ページを改ざんして利用者を騙す文言を記載するスクリプト



リンクをクリックするとURLによってスクリプトが送られ、改ざんされたアンケートページが表示される

クロスサイトスクリプティング　攻撃例
～利用者目線～





クロスサイトスクリプティングの脆弱性

■想定される被害

✓個人情報を窃取される（フィッシング）

→口座番号やクレジットカード情報を詐取された場合、**金銭被害**も

✓ウイルスに感染させられる

→**脆弱性対策を怠った企業が被害の責任を負わされることも**

まとめ（1章）

■ ここまでお伝えしたこと

✓脆弱性は様々なソフトウェアに存在している
✓迅速な修正パッチ適用の重要性
✓脆弱性を悪用されると、様々な被害にあう

→脆弱性の危険性を理解し、適切な脆弱性対策を行う意識を持つことが重要