Information-technology Promotion Agency, Japan

ISOG-J 主催セミナー

「事例から学ぶ！ウェブ改ざんの実態と対策」

ウェブ改ざんによる被害とその対策

2013年12月12日

独立行政法人情報処理推進機構
技術本部　セキュリティセンター
岡野　裕樹

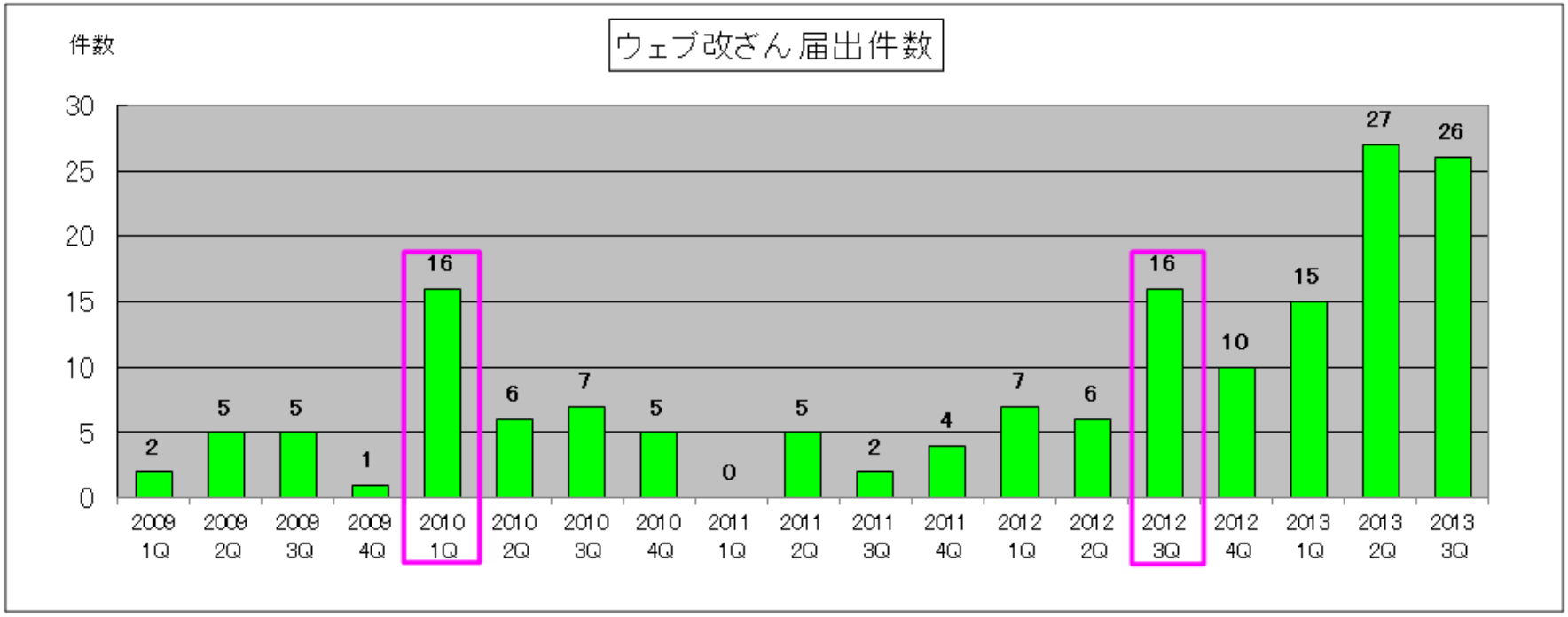
本日の講演内容

- ウェブ改ざんの事例
- 改ざんの原因（サーバ側、ftpクライアント側）
- 防ぐための管理（サーバ側、ftpクライアント側）
- 気づくための管理
- 改ざん被害発生時の対処

本日の講演内容

- ウェブ改ざんの事例
- 改ざんの原因（サーバ側、ftpクライアント側）
- 防ぐための管理（サーバ側、ftpクライアント側）
- 気づくための管理
- 改ざん被害発生時の対処

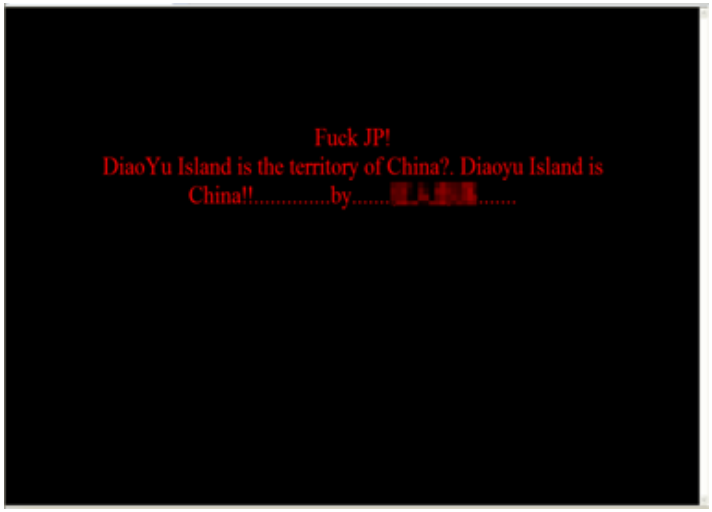
ウェブ改ざん届出件数の推移



- これまでにウェブ改ざん届出の多かった時期
  - 2010年第1四半期：ガンブラーの流行
  - 2012年第3四半期：一部島しょの領有権に関する近隣国からの抗議行動の一環によるものと推測される改ざん

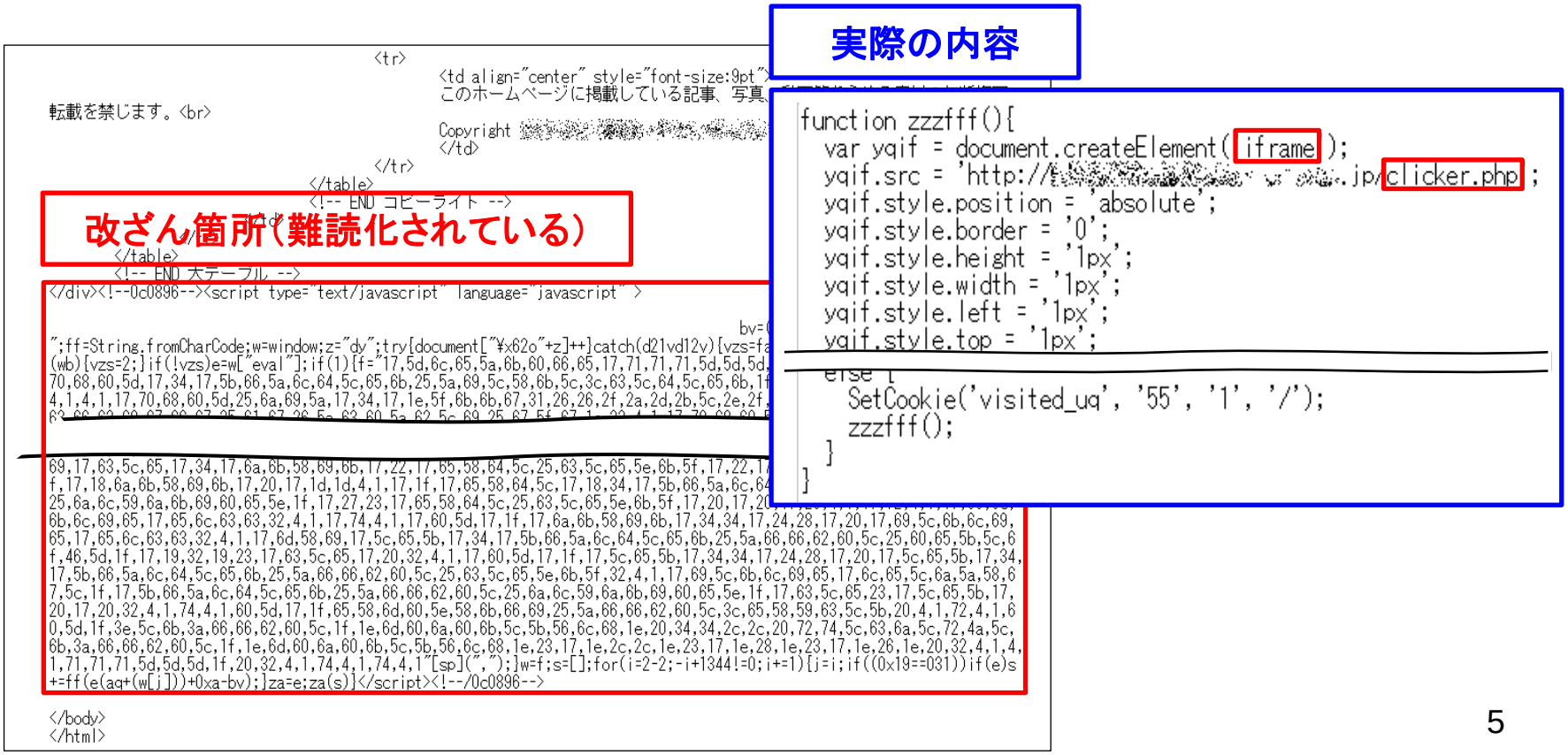
改ざん事例（いわゆる「主義主張」）

- 特徴など
  - ウェブ改ざんを行い、何かしらの考えや主義などを主張することが目的である。
  - 文章や国旗などの画像が挿入され、アクセスすると明らかに正常な状態ではないことがわかる。

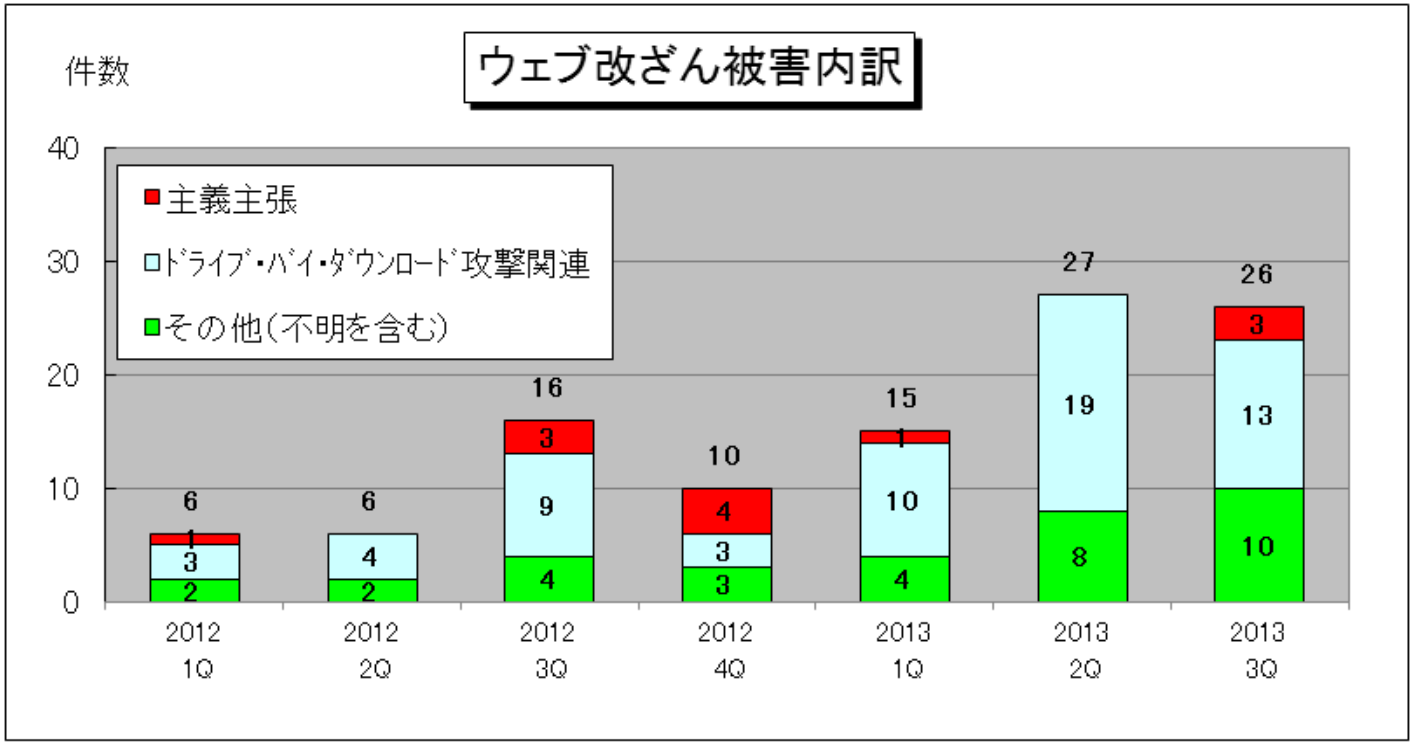


改ざん事例（閲覧者へのウイルス感染を狙ったもの）

- 特徴など
  - 閲覧者のパソコンをウイルス感染させ、何かしらの利益を得ることが目的である。
  - ブラウザ上での表示を見ただけでは、改ざんされていることに気づけない。
  - 挿入されるコードが難読化されていることもある。



ウェブ改ざん被害の内訳



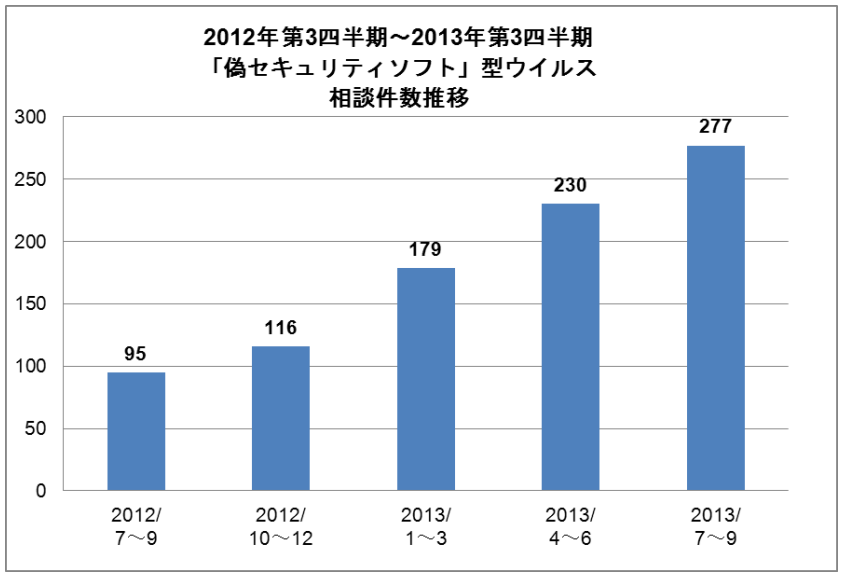
- ウェブ改ざん被害の特徴
  - 閲覧者のウイルス感染を目的とした改ざんが目立っている。
  - 2012年第3四半期には、一部島しょの領有権に関する近隣国からの抗議行動の一環によるものと推測される主義主張を目的とした改ざんが多く報告された。

閲覧者にとっての脅威

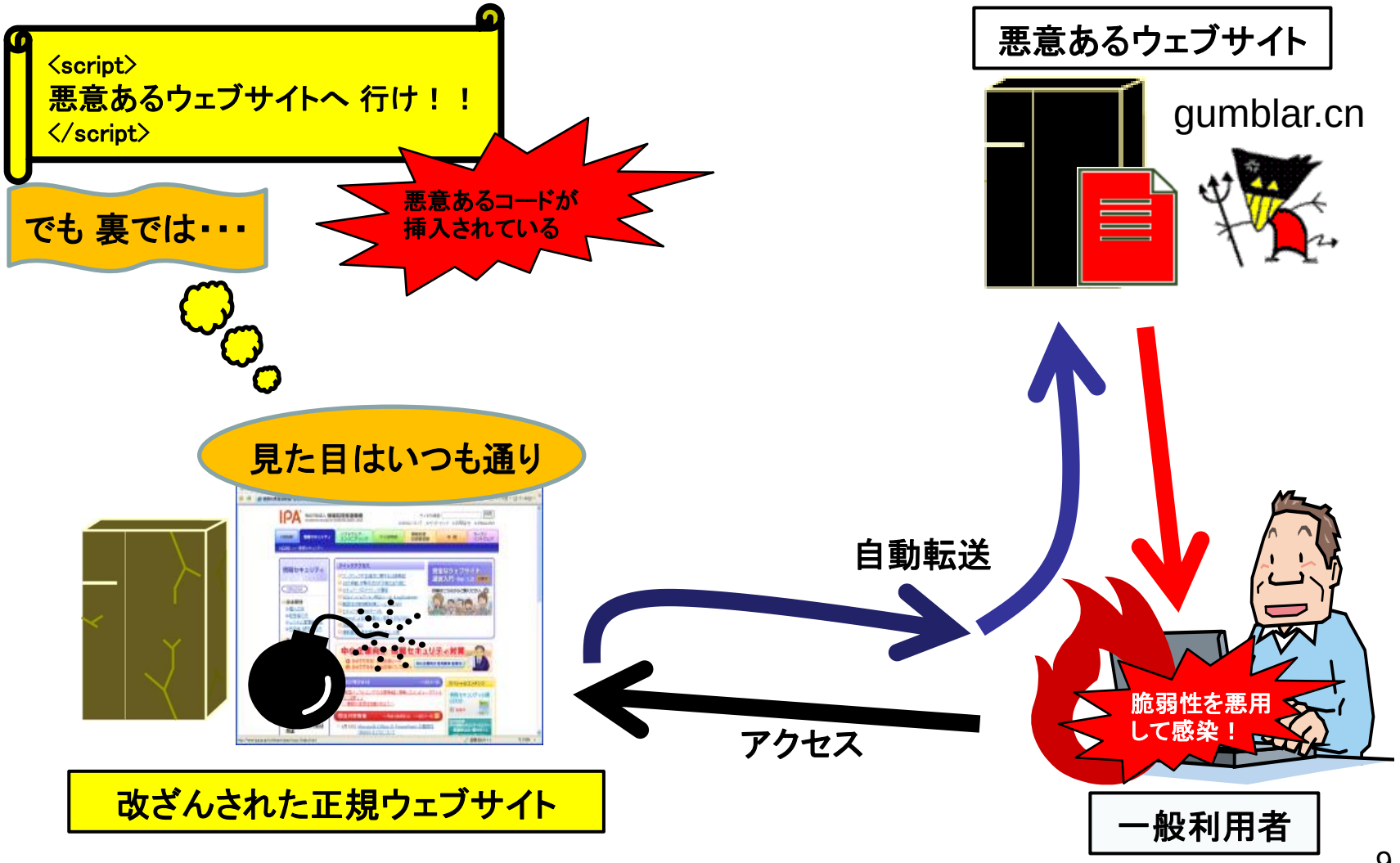
- ウイルス感染の危険性（drive-by download）
  - セキュリティ対策が不十分なパソコンでは、サイトを閲覧しただけでウイルスに感染させられてしまい、かつ、ウイルスに感染したことが見た目には全く分からない場合がある。
- 怪しいサイトを見なくても感染
  - 有名企業のサイトが攻撃に使われる場合があるため、「不審なサイトを閲覧しない」といった回避策が有効とならず、日常的に利用しているサイトが突然危険なサイトとなる可能性もある。
- 様々なウイルスへの感染
  - 悪意あるサイトに仕掛けられるウイルスは攻撃者が任意にコントロールできるため、閲覧者はどのようなウイルスに感染させられるのか予測できない。

閲覧者の被害事例

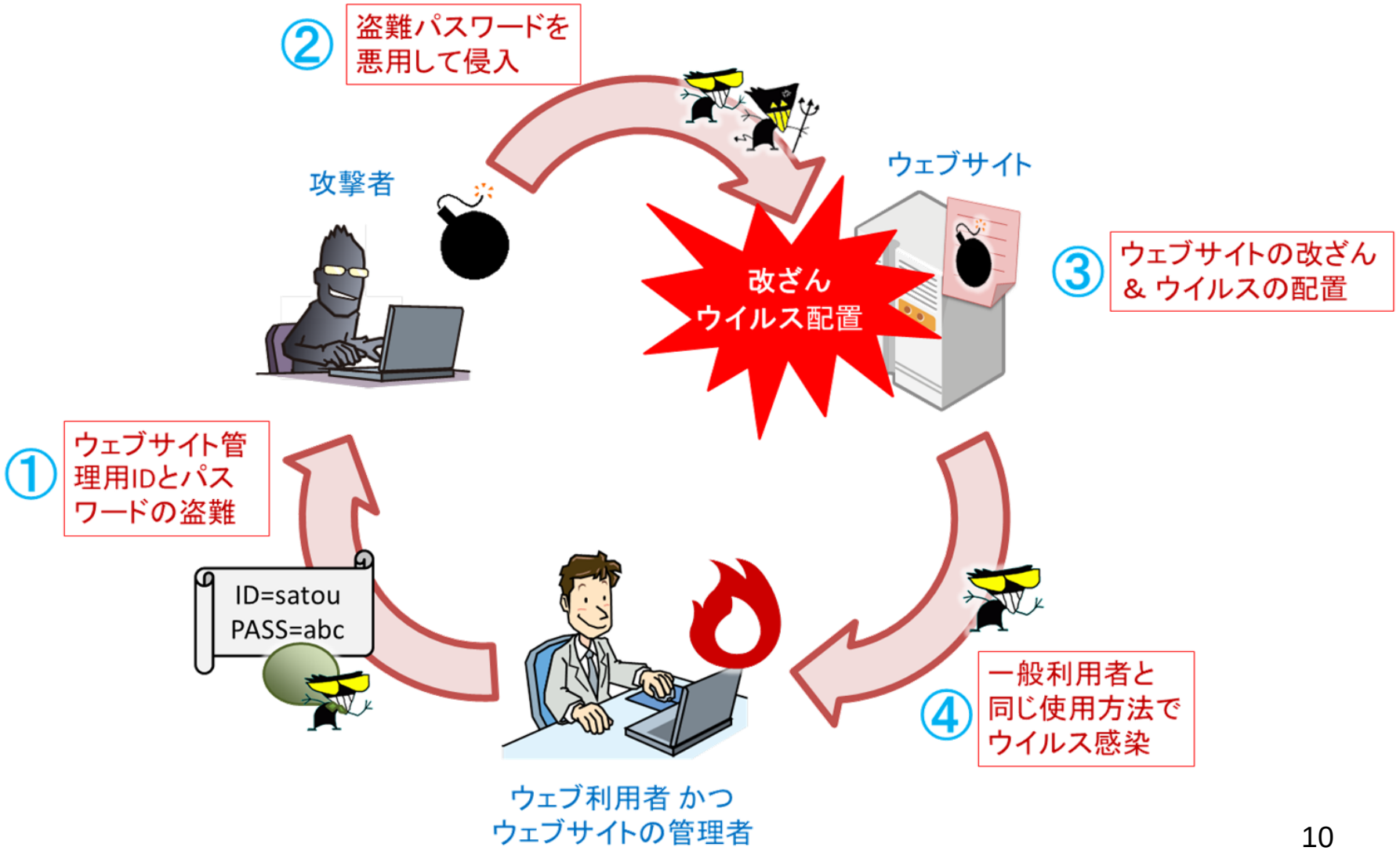
- drive-by downloadによる多種多様なウイルスへの感染
  - 偽セキュリティ対策ソフト型ウイルス
    - ウイルスが発見されたという偽の表示を行い、駆除するために偽のセキュリティ対策ソフトの「有償版」の購入を迫るウイルス
  - ftpのID/パスワードを盗むウイルス（更なるウェブ改ざんの被害）
  - その他のサービスのID/パスワード情報を盗むウイルス
  - 攻撃者の目的に合わせた様々なウイルスへの感染の危険性



ガンブラーでのウイルス感染の仕組み

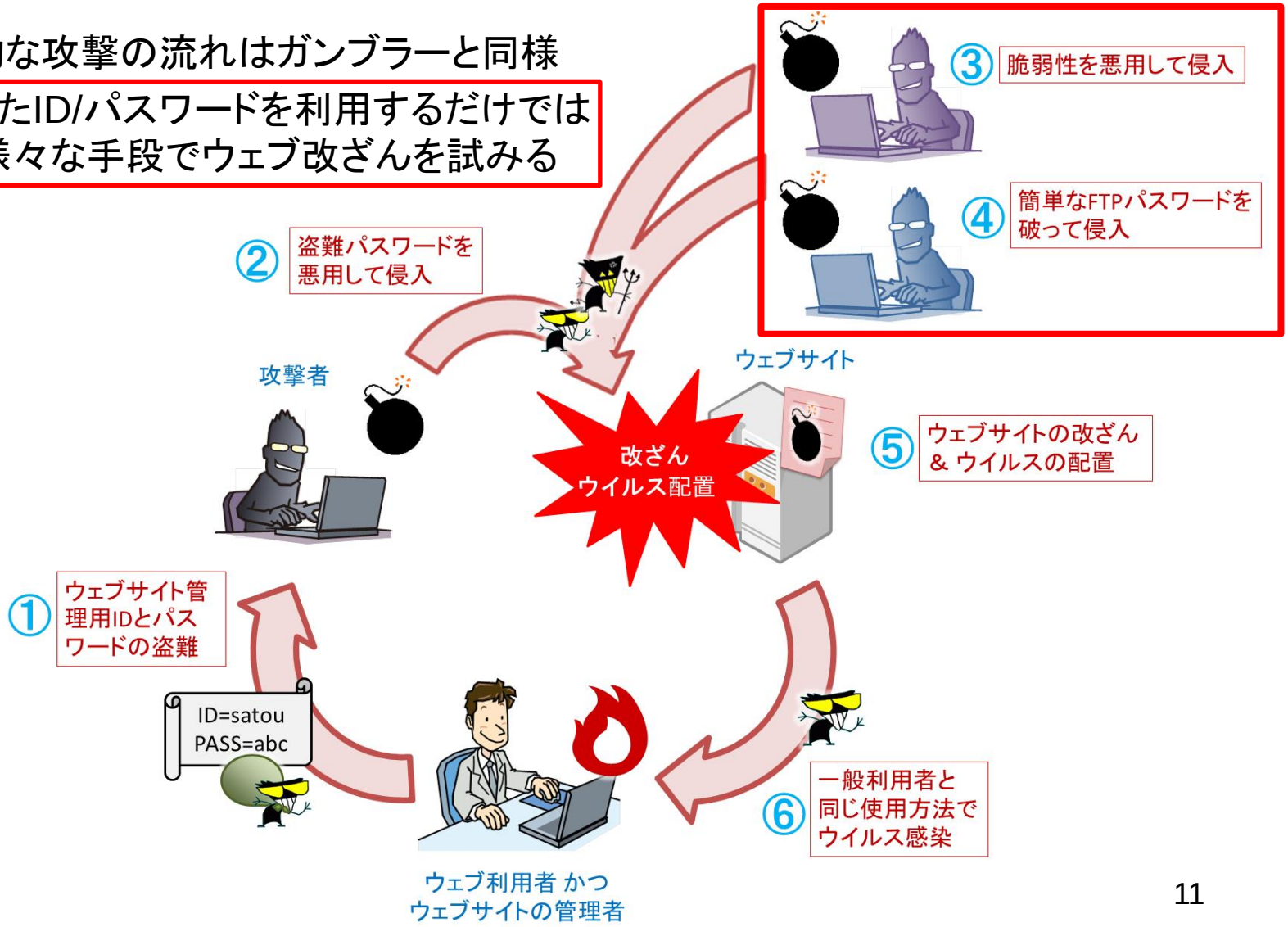


ガンブラーの典型的な手口



最近の手口

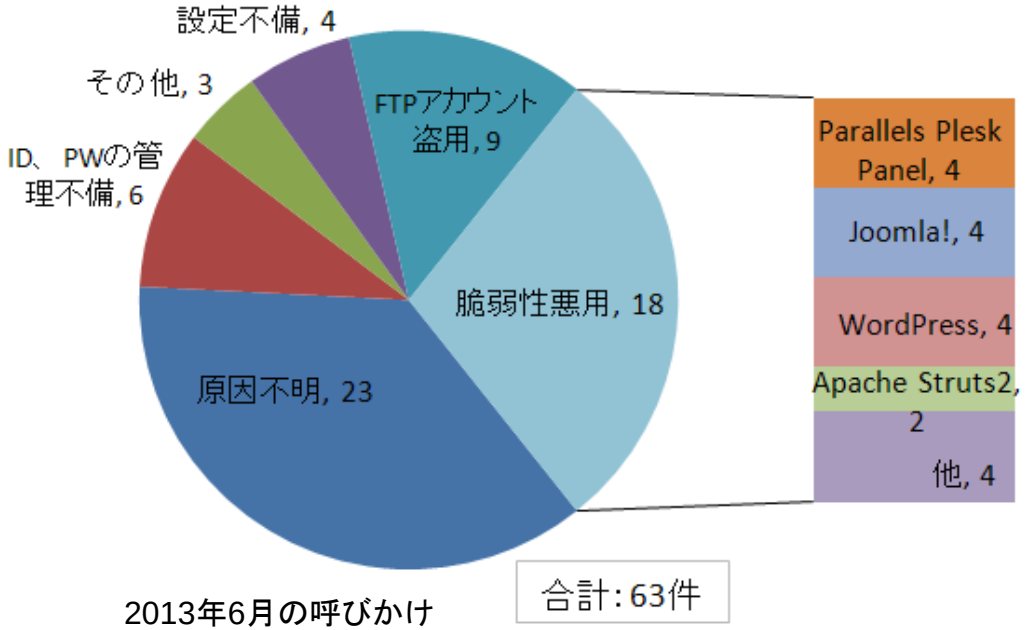
- 基本的な攻撃の流れはガンブラーと同様
- 盗難したID/パスワードを利用するだけではなく、様々な手段でウェブ改ざんを試みる



本日の講演内容

- ウェブページ改ざんの事例
- 改ざんの原因（サーバ側、ftpクライアント側）
- 防ぐための管理（サーバ側、ftpクライアント側）
- 気づくための管理
- 改ざん被害発生時の対処

改ざんの原因（サーバ側）

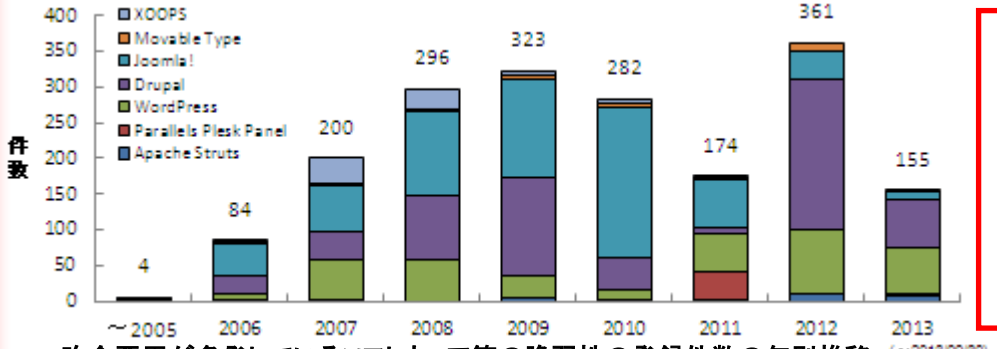


2013年6月の呼びかけ
ウェブ改ざんの「原因」による分類（2012年1月～2013年5月）

- 脆弱性悪用
  - サーバ上のミドルウェア、CMS（プラグインを含む）の脆弱性を悪用
  - Apache Struts 2、Parallels Plesk Panel、WordPress、Movable Type、Drupal、Joomla!、JCE（Joomla! プラグイン）・・・
- ID、パスワードの管理不備
  - ftp、サイト管理画面などの推測され易いパスワード

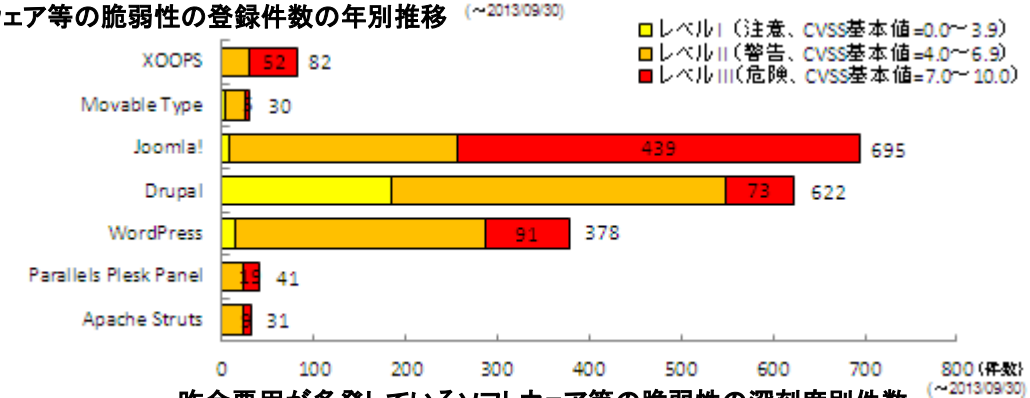
改ざんの原因（サーバ側）

- サーバ上のソフトウェア等の脆弱性に関する注意喚起等
  - 2013.10.18（IPA）
    脆弱性対策情報データベースJVN iPediaの登録状況 [2013年第3四半期（7月～9月）]
    http://www.ipa.go.jp/security/vuln/report/JVNiPedia2013q3.html



昨今悪用が多発しているソフトウェア等の脆弱性の登録件数の年別推移

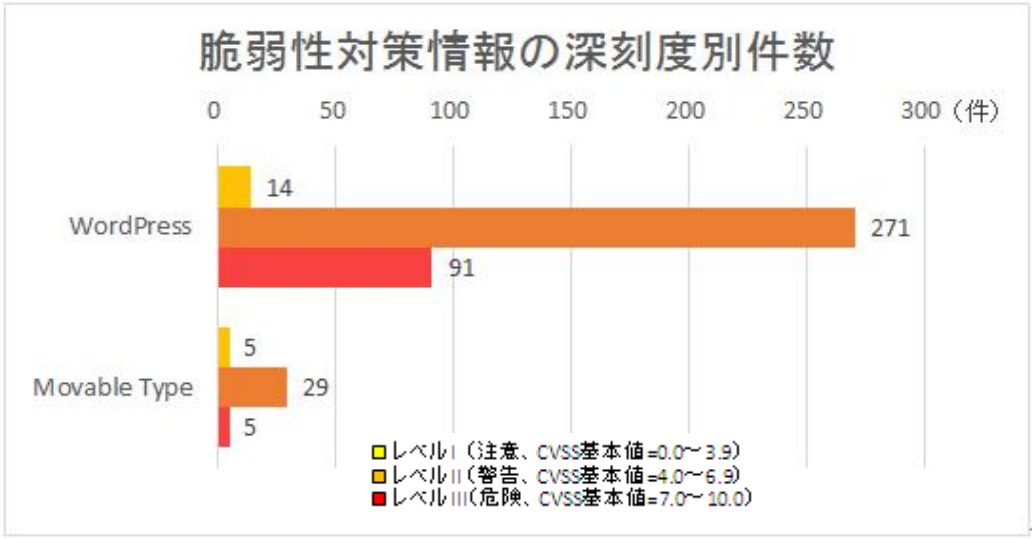
- 絶えず脆弱性が発見されている。
- CVSS基本値による脆弱性の深刻度のレベル分けにおいて「危険」に分類されている脆弱性も発見されており、対策は必須と言える。



昨今悪用が多発しているソフトウェア等の脆弱性の深刻度別件数

改ざんの原因（サーバ側）

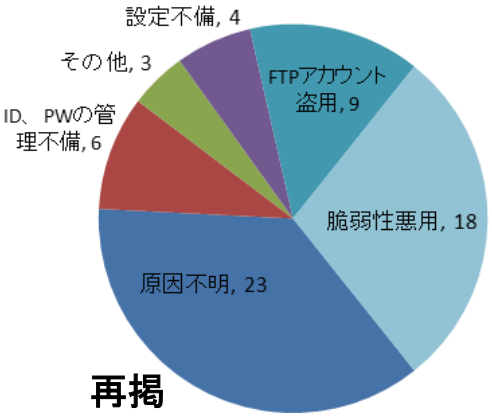
- サーバ上のソフトウェア等の脆弱性に関する注意喚起等
  - 2013.04.08（JPCERT/CC）
    旧バージョンの Parallels Plesk Panel の利用に関する注意喚起
    http://www.jpcert.or.jp/at/2013/at130018.html
  - 2013.09.13（IPA）
    WordPressやMovable Typeの古いバージョンを利用しているウェブサイトへの注意喚起
    http://www.ipa.go.jp/security/topics/alert20130913.html



- 特に改ざんの原因につながるなどの深刻な脆弱性が存在するソフトウェアについては、個別の注意喚起などが発せられている。

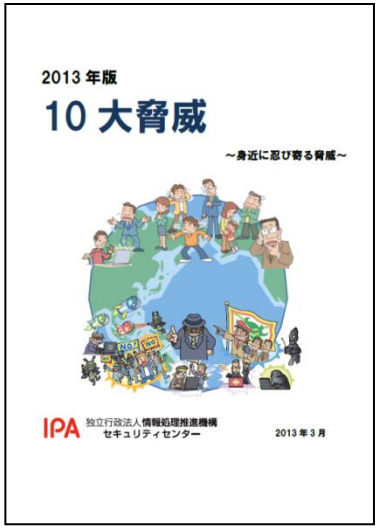
改ざんの原因（ftpクライアント側）

- ftpアカウント盗用
  - 原因はわからないが、ftpアカウントを不正に利用され、改ざんが行われた
  - ftpクライアント端末のウイルス感染によりftpのアカウントが盗用された
- 10大脅威では・・・
  - クライアントソフトの脆弱性を突いた攻撃が上位



再掲

2013年6月の呼びかけ
ウェブ改ざんの「原因」による分類
（2012年1月～2013年5月）



2008 年	2009 年	2010 年	2011 年	2012 年	2013 年	10 大脅威
8 位	—	2 位	3 位	4 位	1 位	クライアントソフトの脆弱性を突いた攻撃
4 位	3 位	6 位	8 位	1 位	2 位	標的型諜報攻撃
—	—	—	4 位	6 位	3 位	スマートデバイスを狙った悪意あるアプリの横行
—	—	—	—	—	4 位	ウイルスを使った遠隔操作
—	—	3 位	—	—	5 位	金銭窃取を目的としたウイルスの横行
—	—	—	—	2 位	6 位	予期せぬ業務停止
2 位	2 位	1 位	2 位	5 位	7 位	ウェブサイトを狙った攻撃
—	—	8 位	—	9 位	8 位	パスワード流出の脅威
3 位	5 位	5 位	1 位	8 位	9 位	内部犯行
7 位	—	—	—	—	10 位	フィッシング詐欺

http://www.ipa.go.jp/security/vuln/10threats2013.html

本日の講演内容

- ウェブページ改ざんの事例
- 改ざんの原因（サーバ側、ftpクライアント側）
- 防ぐための管理（サーバ側、ftpクライアント側）
- 気づくための管理
- 改ざん被害発生時の対処

改ざんを防ぐための管理（サーバ側）

- 推測されにくいパスワードの設定
  - ftpやその他サイト管理画面などのパスワードは、推測されにくいパスワードを設定する
- アクセス制限
  - ftpなどへの接続制限を行う（接続元IPアドレス、VPN）。万が一、ID/パスワードが盗み取られてしまっても、外部からのアクセスを防ぐ。
- サーバ上のソフトウェア等の脆弱性への対応
  - 最新版にアップデートを行う
  - プラグインも忘れずに
- 脆弱性情報の収集
  - JVN iPedia、セキュリティベンダーなど
- 有事の際の対応を事前に検討
  - 連絡体制、対応手順

改ざんを防ぐための管理（サーバ側）

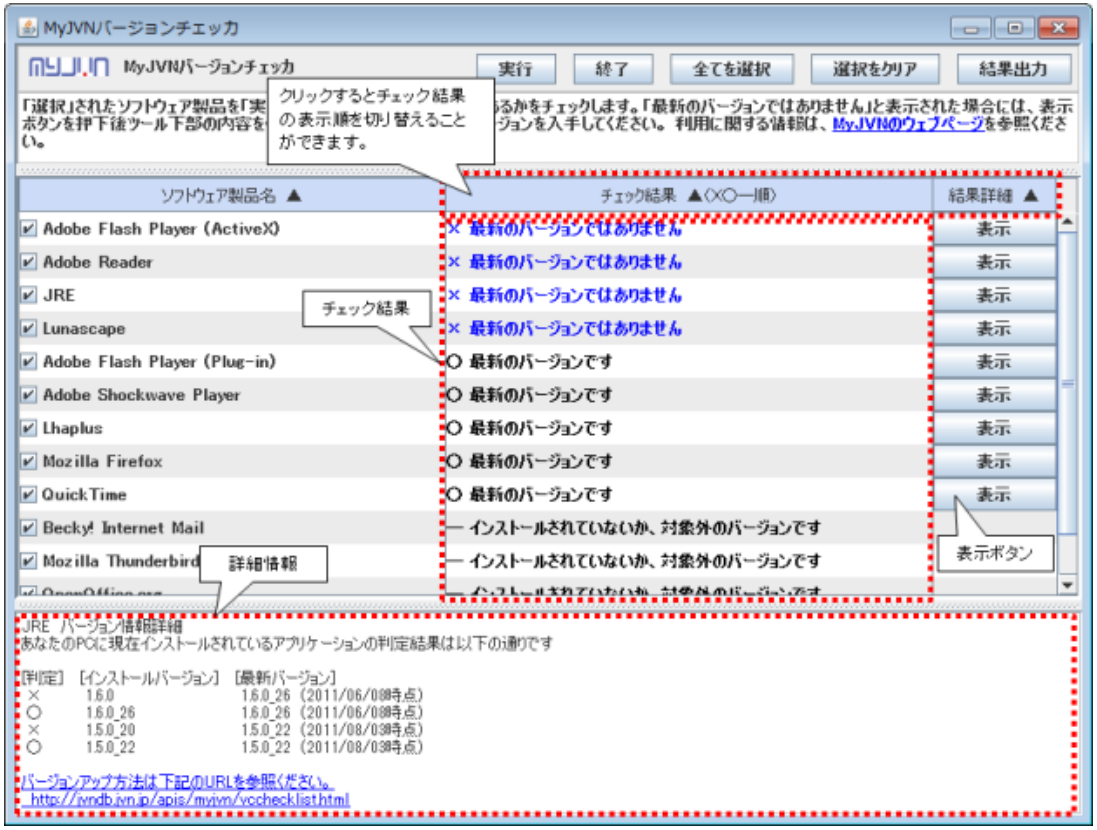
- JVN iPedia（http://jvndb.jvn.jp）
  - 国内外問わず日々公開される脆弱性対策情報を収集、蓄積することを目的とした脆弱性対策情報データベース

改ざんを防ぐための管理（ftpクライアント側）

- アップデートを行う
  - ウイルスによるftpのアカウント情報等の漏えいを防ぐ（drive-by downloadによるウイルス感染を防ぐ）。Windows Update、各種ソフトウェア（特にAdobe Flash Player、Adobe Reader、Javaなど）のアップデート、ウイルス対策ソフトを最新の状態で利用する。MyJVNバージョンチェッカの利用、自動アップデートの設定。
- 更新専用パソコンの導入
  - ftpクライアント専用の端末を用意する。ウェブやメールの閲覧などを原因とするウイルスの感染を防ぐことが可能。
- アカウントを共有しない
  - 万が一、インシデントが発生してしまった際の原因の特定に有効。

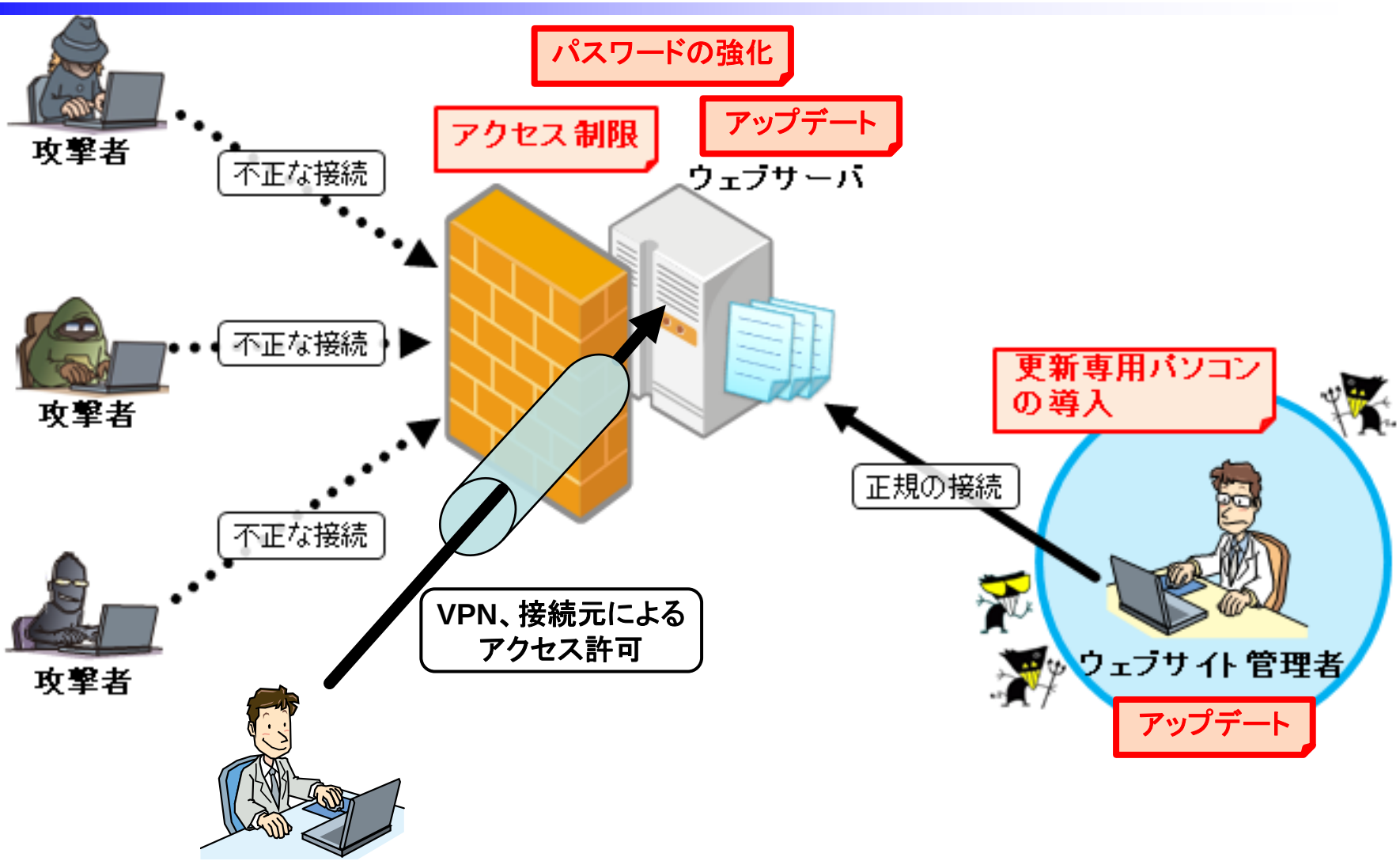
改ざんを防ぐための管理（ftpクライアント側）

- MyJVNバージョンチェッカ（http://jvndb.jvn.jp/apis/myjvn/）
  - 利用者のコンピュータにインストールされているソフトウェア製品のバージョンが最新であるか、簡単な操作で確認するツールです。



- Adobe Flash Player
- Adobe Reader
- Adobe Shockwave Player
- JRE
- Lhaplus
- Mozilla Firefox
- Mozilla Thunderbird
- QuickTime
- Lunascape
- Becky! Internet Mail
- OpenOffice.org
- VMware Player

改ざんを防ぐための管理（まとめ）



本日の講演内容

- ウェブページ改ざんの事例
- 改ざんの原因（サーバ側、ftpクライアント側）
- 防ぐための管理（サーバ側、ftpクライアント側）
- 気づくための管理
- 改ざん被害発生時の対処

改ざんに気づくための運用・管理

- バックアップデータとサーバ上のデータの比較
  - サーバにコンテンツ（.htaccess等を含む）をアップロードする際には、そのコピーを保管しておき、定期的にサーバ上のファイルと比較を行う。
- アクセスログの定期的な確認
  - （万が一、インターネットへ公開するのであれば、）ftp、サイト管理画面等へのアクセスログを定期的に確認する。
    - 認証試行のログはないか？
    - 不審なIPアドレスの認証成功のログはないか？
- 問い合わせ先の掲載
  - ウェブサイト上にメールアドレスなどの連絡先を掲載し、外部からの連絡を受けられる体制を整える。
- ウェブサイト改ざん検知サービスなどを利用する

改ざんに気づくための運用・管理

- sshへの大量の認証試行のログ
  - この後、sshのパスワードが破られ、ウェブ改ざんの被害に

```
May 18 21:41:40 www sshd[28839]: input_userauth_request: invalid user audrey
May 18 21:41:40 www sshd[28839]: Received disconnect from [redacted]: 11: Bye Bye
May 18 21:41:42 www sshd[28840]: Invalid user molly from [redacted]
May 18 21:41:42 www sshd[28843]: input_userauth_request: invalid user molly
May 18 21:41:42 www sshd[28843]: Received disconnect from [redacted]: 11: Bye Bye
May 18 21:41:45 www sshd[28844]: Invalid user sophie from [redacted]
May 18 21:41:45 www sshd[28847]: input_userauth_request: invalid user sophie
May 18 21:41:45 www sshd[28847]: Received disconnect from [redacted]: 11: Bye Bye
May 18 21:41:47 www sshd[28848]: Invalid user alexa from [redacted]
May 18 21:41:47 www sshd[28851]: input_userauth_request: invalid user alexa
May 18 21:41:47 www sshd[28851]: Received disconnect from [redacted]: 11: Bye Bye
May 18 21:41:49 www sshd[28852]: Invalid user claire from [redacted]
May 18 21:41:49 www sshd[28855]: input_userauth_request: invalid user claire
May 18 21:41:49 www sshd[28855]: Received disconnect from [redacted]: 11: Bye Bye
May 18 21:41:51 www sshd[28856]: Invalid user aaliyah from [redacted]
May 18 21:41:51 www sshd[28859]: input_userauth_request: invalid user aaliyah
May 18 21:41:51 www sshd[28859]: Received disconnect from [redacted]: 11: Bye Bye
May 18 21:41:54 www sshd[28860]: Invalid user leah from [redacted]
May 18 21:41:54 www sshd[28863]: input_userauth_request: invalid user leah
May 18 21:41:54 www sshd[28863]: Received disconnect from [redacted]: 11: Bye Bye
```

本日の講演内容

- ウェブページ改ざんの事例
- 改ざんの原因（サーバ側、ftpクライアント側）
- 防ぐための管理（サーバ側、ftpクライアント側）
- 気づくための管理
- 改ざん被害発生時の対処

改ざん被害発生時の対処

- 早急なウェブサイトの公開停止
  - 加害者にならないために・・・
  - 安全なマシンからftp等のパスワードの変更

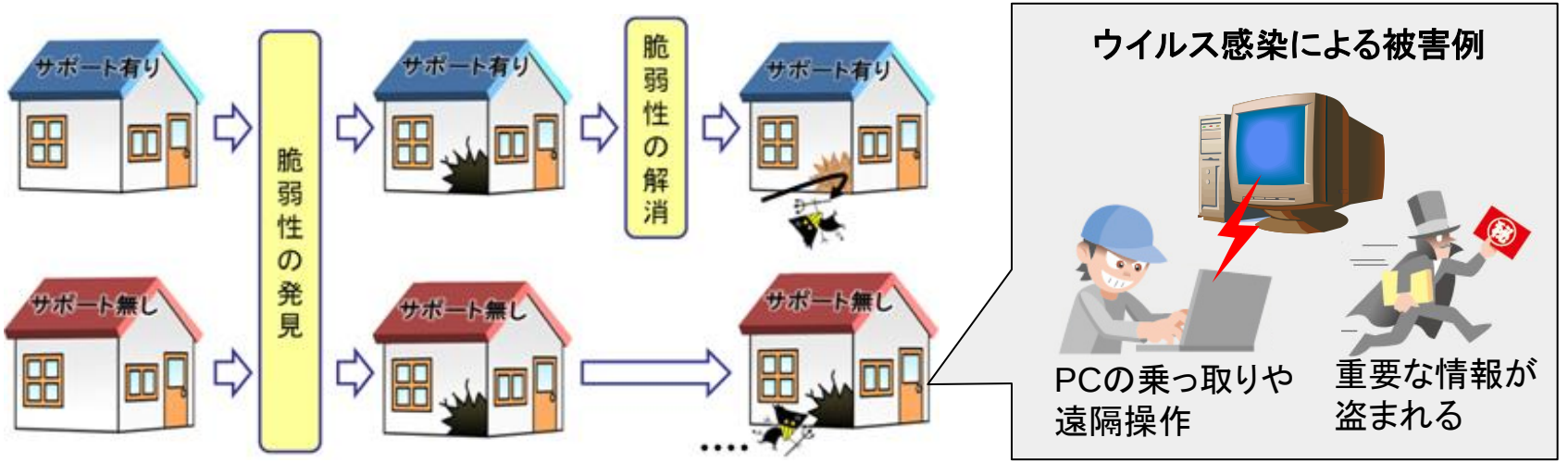
- 改ざん箇所の洗い出し、原因の特定等の調査
  - バックアップデータとの比較
  - 公開ディレクトリ内ファイル群の再アップロード
  - 各種サービスの関連ログの確認
  - ウェブコンテンツのソースファイルのウイルススキャン

改ざん被害発生時の対処

- ウェブサイトを再公開する場合の注意点
  - サイト閲覧者へ向けた事実告知が重要
    a. 改ざんの事実の説明
    b. 改ざんされていた箇所
    c. 改ざんされていた期間
    d. ウェブサイト利用者が改ざんされていた箇所を閲覧した場合に想定される被害（ウイルス感染など）の説明
    e. ウイルスのチェック方法の説明（必要に応じてオンラインスキャンサイトの紹介など）
    f. 問い合わせ窓口の連絡先

Windows XP サポート終了について

2014年4月9日(日本時間) にWindows XPのサポートが終了します。
これにより、新たな脆弱性が発見されてもセキュリティ更新プログラムが提供されなくなり、ウイルスや不正アクセスの脅威にさらされたままの状態になる可能性が高まります。



サポート終了 OS を家にたとえた場合のイメージ図

詳しくは・・・ ■Windows XPのサポート終了について（IPA）
http://www.ipa.go.jp/security/announce/winxp_eos.html

ITパスポート試験

IPA

<PR>

http://www.jitec.ipa.go.jp/ip/

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

セキュリティセンター（IPA/ISEC）
http://www.ipa.go.jp/security/

★情報セキュリティ安心相談窓口：
TEL：03（5978）7509 (平日10:00-12:00、13:30-17:00)
FAX ：03（5978）7518
E-mail： anshin@ipa.go.jp