株式会社ラック

# INSIGHT

**vol.8**

2015年7月13日

JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER

# JSOC INSIGHT Vol.8

JAPAN SECURITY OPERATION CENTER

## はじめに

JSOC(Japan Security Operation Center)とは、株式会社ラックが運営するセキュリティ監視センターであり、「JSOC マネージド・セキュリティ・サービス(MSS)」や「24+ シリーズ」などのセキュリティ監視サービスを提供しています。JSOC マネージド・セキュリティ・サービスでは、独自のシグネチャやチューニングによってセキュリティデバイスの性能を最大限に引き出し、そのセキュリティデバイスから出力されるログを、専門の知識を持った分析官(セキュリティアナリスト)が 24 時間 365 日リアルタイムで分析しています。このリアルタイム分析では、セキュリティアナリストが通信パケットの中身まで詳細に分析することに加えて、監視対象への影響有無、脆弱性やその他の潜在的なリスクが存在するか否かを都度診断することで、セキュリティデバイスによる誤報を極限まで排除しています。緊急で対応すべき重要なインシデントのみをリアルタイムにお客様へお知らせし、最短の時間で攻撃への対策を実施することで、お客様におけるセキュリティレベルの向上を支援しています。

本レポートは、JSOC のセキュリティアナリストによる日々の分析結果に基づき、日本における不正アクセスやマルウェア感染などのセキュリティインシデントの発生傾向を分析したレポートです。JSOC のお客様で実際に発生したインシデントのデータに基づき、攻撃の傾向について分析しているため、世界的なトレンドだけではなく、日本のユーザが直面している実際の脅威を把握することができる内容となっております。

本レポートが、皆様方のセキュリティ対策における有益な情報としてご活用いただけることを心より願っております。

*Japan Security Operation Center*
*Analysis Team*

**【集計期間】**

第一章 2015 年 1 月 1 日 ～ 2015 年 3 月 31 日

第二章 2014 年 4 月 1 日 ～ 2015 年 3 月 31 日

**【対象機器】**

本レポートは、ラックが提供する JSOC マネージド・セキュリティ・サービスが対象としているセキュリティデバイス（機器）のデータに基づいて作成されています。

## 第一章 2015 年 1 月から 3 月の傾向のまとめ

### 1 2015 年 1 月から 3 月のサマリ

第 1 章では、2015 年 1 月から 3 月に発生したインシデント傾向の分析に加え、特に注目すべき脅威をピックアップしてご紹介します。

- **JBoss Application Server の脆弱性を悪用する新たな攻撃を検知**

  2013 年に公開された JBossInvoker の脆弱性を悪用する新たな攻撃手法が複数公開されました。新たな攻撃手法は、これまでより容易にバックドアの作成や任意のコード実行ができ、一部の JBoss Application Server はすでにメーカサポートが終了していることから、未修正の状態の可能性があります。JSOC ではオリジナルシグネチャ(JSIG)でこれらの新しい攻撃を検知しました。

- **phpMoAdmin におけるコード実行の脆弱性(ゼロデイ)を悪用する攻撃を検知**

  オープンソースのデータベース MongoDB を管理する GUI ツールである phpMoAdmin に外部からコード実行可能な脆弱性が公開されました。phpMoAdmin は、2013 年 9 月以降、公式なアップデートが無く、2015 年 6 月時点においても本脆弱性は未修正の状態です。JSOC ではオリジナルシグネチャ(JSIG)でこれらの攻撃を検知しました。

- **マルウェアへの感染を引き起こすダウンローダの通信を検知**

  2015 年 1 月以降、JSOC で UPATRE/DYRE と呼ばれるダウンローダの感染通信を検知しました。UPATRE/DYRE はスパムメールに添付されて拡散されることが多く、感染すると外部からインターネットバンキングのお客様情報や利用情報を狙うマルウェアなど、複数のマルウェアをダウンロードします。JSOC では UPATRE/DYRE に感染したホストから、さらに多くのマルウェアに感染させるための端末情報を C&C サーバに送信することを確認しました。

## 2　JSOC における重要インシデント傾向

### 2.1　重要インシデントの傾向

JSOC では、IDS/IPS、マルウェア検出器、ファイアウォールで検知したログをセキュリティアナリストが分析し、検知した内容と監視対象への影響度に応じて 4 段階のインシデント重要度を決定しています。このうち、Emergency、Critical に該当するインシデントは、攻撃の成功や被害が発生している可能性が高いと判断される重要インシデントです。

**表 1 インシデントの重要度と内容**

| 分類 | 重要度 | インシデント内容 |
|---|---|---|
| 重要インシデント | Emergency | 攻撃成功を確認したインシデント |
| | Critical | 攻撃成功の可能性が高いインシデント、攻撃失敗が確認できないインシデント<br>マルウェア感染を示すインシデント |
| 参考インシデント | Warning | 攻撃失敗を確認したインシデント、攻撃内容に実害が無いことを確認したインシデント |
| | Informational | スキャンなど実害を及ぼす攻撃以外の影響の少ないインシデント |

図 1 に、2015 年 1 月から 3 月に発生した重要インシデントの件数推移を示します。

インターネットからの攻撃による重要インシデントに特筆すべき検知傾向変化は見られず、発生件数も大きな変化はありません。

ネットワーク内部から発生した重要インシデントの発生件数は、2015 年 3 月 12 日以降増加しました(図 1-[1])。これは、一部のお客様でマルウェア感染が継続して発生したためです。これ以外には特筆すべき傾向の変化は見られません。

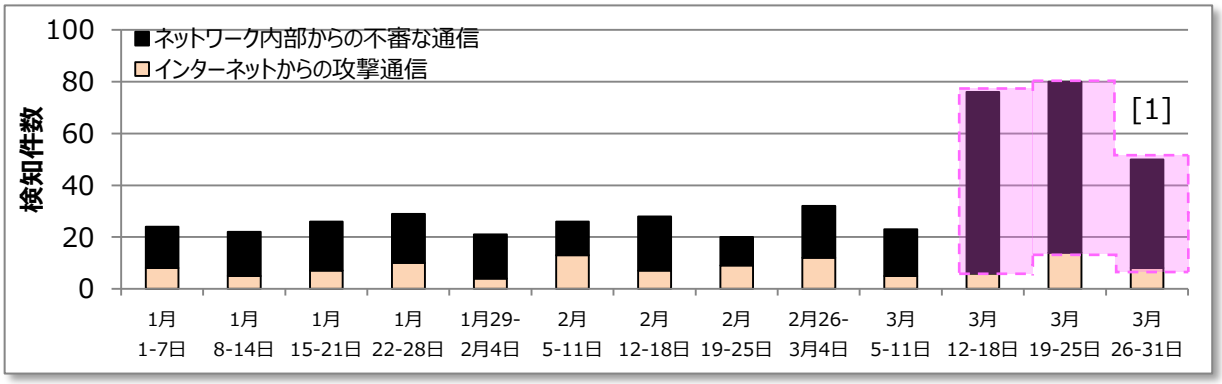



**図 1 重要インシデントの件数推移(2015 年 1 月～3 月)**

## 2.2　発生した重要インシデントに関する分析

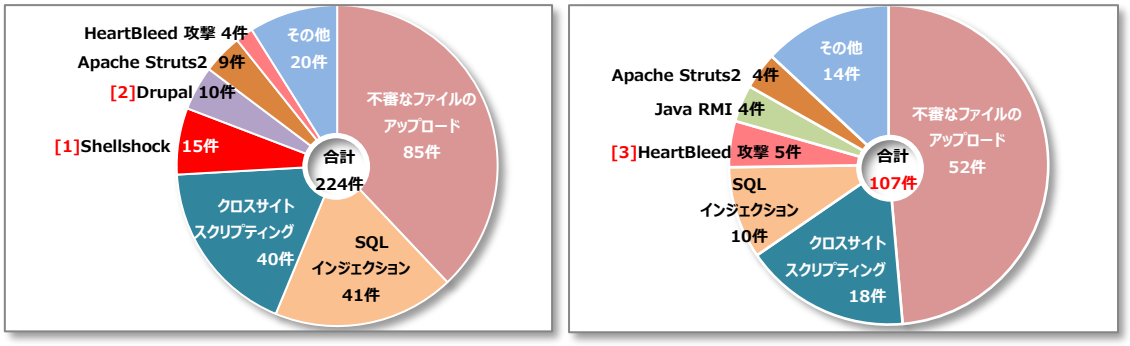
図 2 にインターネットからの攻撃による重要インシデントの内訳を示します。

2015 年 1 月から 3 月にインターネットからの攻撃により発生した重要インシデントの件数(107 件)は、2014 年 10 月から 12 月の件数 (224 件)より減少しました。これは、不審なファイルアップロードの試みや、SQL インジェクション、クロスサイトスクリプティングの重要インシデントの発生件数がそれぞれ減少したためです。

GNU bash のコード実行の脆弱性を悪用する攻撃(Shellshock)は、攻撃の検知件数が減少し、2014 年 12 月以降 Shellshock に起因する重要インシデントは発生していません(図 2-[1])。

2014 年 10 月、オープンソースのコンテンツ管理システム(CMS)である Drupal に対する SQL インジェクションの脆弱性(CVE-2014-3704)が公開されました。本脆弱性を悪用する攻撃[1]は、攻撃対象のホストに影響を与える攻撃の検知がなく、2015 年 1 月以降重要インシデントは発生しておりません(図 2-[2])。

また、2015 年 1 月から 3 月にかけて、OpenSSL の Heartbeat 機能の脆弱性を悪用した攻撃(Heartbleed)による重要インシデントが複数発生しました(図 2-[3])。これは攻撃に対して脆弱であることが認識されずに放置されたホストや、OpenSSL を組み込んだ製品など対策が困難なホストが依然として存在しているためと考えられます。




**a. 2014 年 10～12 月**　　**b. 2015 年 1～3 月**

**図 2 インターネットからの攻撃による重要インシデントの内訳**

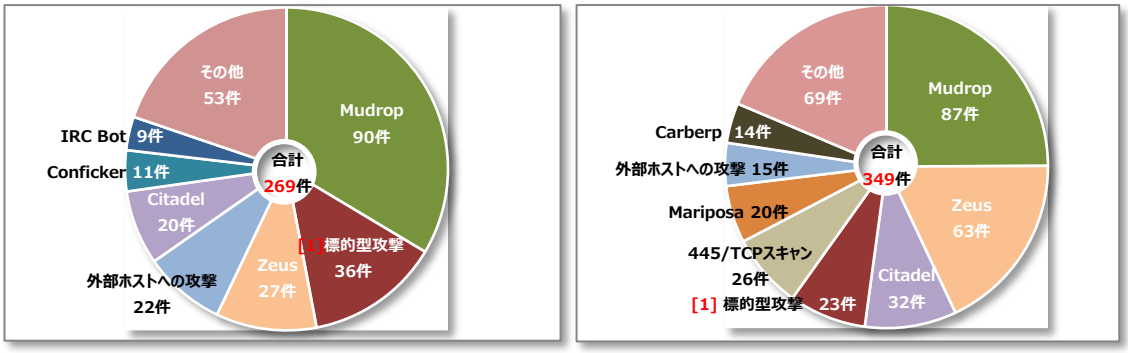
[1] JSOC INSIGHT vol.7
4.2 Drupal の SQL インジェクションの脆弱性を悪用する攻撃について
http://www.lac.co.jp/security/report/2015/05/19_jsoc_01.html

図 3 にネットワーク内部から発生した重要インシデントの内訳を示します。

2015 年 1 月から 3 月にネットワーク内部から発生した重要インシデントの件数(349 件)は、2014 年 10 月から 12 月の件数(269 件)より増加しました。これは、一部のお客様で、マルウェア感染が継続して発生したためです。その他のお客様では特筆すべき傾向の変化は見られません。

2014 年 11 月から 2015 年 3 月にかけて、標的型攻撃やマルウェア感染時に使用される、HTran と呼ばれる通信を中継するツールの通信を検知しました (図 3a.[1]、図 3b.[1])。HTran 自体は感染機能を持つマルウェアではありませんが、C&C サーバの隠蔽やホスト上の情報を転送するツールとして使用されることがあります。

HTran は 2011 年から 2012 年に複数のお客様で検知実績がありましたが、2013 年から 2014 年 10 月までは検知実績がなく、2015 年に入り複数の学術・研究機関において検知しました。また、調査の結果、感染通信を発生させたホストが iPhone であった疑いがあることから、公開されている HTran のソースコードを利用し、攻撃者が何かしらのモバイルアプリケーションの一部として組み込んだ可能性も考えられます。




**a. 2014 年 10～12 月　　b. 2015 年 1～3 月**

**図 3 ネットワーク内部から発生した重要インシデントの内訳**

## 2.3 大量に検知したインターネットからの攻撃通信例

表 2 に 2015 年 1 月から 3 月における、インターネットからの攻撃通信で特に検知件数が大量だった攻撃を示します。これらの攻撃通信の多くは、攻撃対象の使用状況にかかわらず無差別に発生しました。そのため、検知した攻撃通信が成功する事例を検知することは少なく、その試みはほぼ失敗を検知したものです。しかしながら、これらの通信が大量に発生することで分析コストが膨大になるため、リアルタイム監視を行う JSOC アナリストをしばしば苦しめました。

**表 2 大量に検知したインターネットからの攻撃通信**

| 概要 | JSOC の検知内容 | 検知時期 | 重要インシデントの有無 |
|---|---|---|---|
| SQL インジェクション | Web ページの改ざんを目的とした SQL インジェクション攻撃(図 4)を継続して検知しました。 | 2015 年 2 月末から 2015 年 3 月末まで | × |
| WordPress に対する内部ファイル参照攻撃 | WordPress のプラグインの脆弱性を悪用し、設定ファイルを閲覧する試みを継続して検知しました。 | 決まった時期は無く、定常的に検知 | × |
| Heartbleed 攻撃に脆弱なホストの探索 | Heartbleed 攻撃に脆弱なホストを調査する通信を継続して検知しました。 | 決まった時期は無く、定常的に検知 | ○ |
| Shellshock の検知 | Shellshock の影響有無を調査する通信や、ホストの悪用を試みる攻撃を継続して検知しました。攻撃に用いられるコマンドは多岐にわたりました。 | 決まった時期は無く、定常的に検知 | × |
| Apache Struts に対する攻撃 | Apache Struts の脆弱性(S2-016、S2-020)の有無を調査する通信を検知しました。 | 2015 年 3 月上旬から 2015 年 3 月末まで | ○ |


**図 4 改ざんを試みる(赤枠部分)SQL インジェクション攻撃**

## 3　今号のトピックス

### 3.1　JBoss Application Server におけるコード実行の脆弱性について

#### 3.1.1　JBoss Application Server に対する攻撃の検知事例

オープンソースとして提供されているアプリケーションサーバソフトウェアである JBoss Application Server(以下、JBoss AS)には、EJBInvokerServlet および JMXInvokerServlet にアクセス制御の不備があった場合、任意のコード実行が可能な脆弱性(CVE-2012-0874)が存在します[2]。特定バージョンの JBoss AS に含まれるコンポーネント EJBInvokerServlet および JMXInvokerServlet は、リモートから MarshalledInvocation クラスを介して他のアプリケーションの起動を行う役割をしますが、外部ネットワークから InvokerServlet に対してアクセスできる場合、任意のコードを実行される可能性があります。

2013 年、本脆弱性を悪用する手法として外部から悪意のあるファイルをダウンロードし、展開することで任意のファイルを設置する方法が公開されました。

図 5 に、本手法による攻撃通信を示します。


**図 5　JBoss AS に対し不正なファイルをアップロードし、展開する試み**

攻撃が成功すると、外部サイトに設置された圧縮ファイル(赤枠)が攻撃対象ホストにダウンロードされ、展開されます。ダウンロードしたファイルは、バックドアであり、攻撃者が設置したファイルを介して任意のコード実行が可能になり、ネットワーク内部の情報盗取されることや、攻撃対象ホストが他のホストに対する攻撃の起点となることが考えられます。

JSOC では本手法が公開された 2013 年 10 月より、定常的に InvokerServlet に対する不正なフ

[2]複数の JBoss Enterprise 製品における MBean メソッドを呼び出される脆弱性
http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001425.html

ァイルのアップロードを試みる通信を検知しておりますが、Web サーバに対する脆弱性スキャンの一部として検知することが多く、現在まで重要インシデントは発生していません。

2015 年 3 月、InvokerServlet にアクセス可能なホストに対し、より容易にファイルを作成する方法が公開されました。公開された情報には CVE 番号など明確に攻撃対象の脆弱性を特定できる情報はありませんでしたが、攻撃手法の特徴から、本攻撃は同じ脆弱性を悪用する攻撃であると考えられます。

図 6 に、本手法の公開後に JSOC で検知した攻撃通信を示します。

図 6 は攻撃通信の一部を検知したものです。検知した内容から、この攻撃は図 5 と同様に、InvokerServlet に対する攻撃であると判断できます。図 6 の攻撃通信を脆弱なサーバで受け取った場合、jsp コードを含んだバックドアが直接作成されます。このバックドアは、以下の HTTP 要求を受け取った場合、JBoss AS の実行権限で任意の操作を実行します。

- User-Agent ヘッダが「jexboss」である
- パラメータ「ppp」に実行したい外部プロセス名(OS コマンド、スクリプトファイル)が入っている

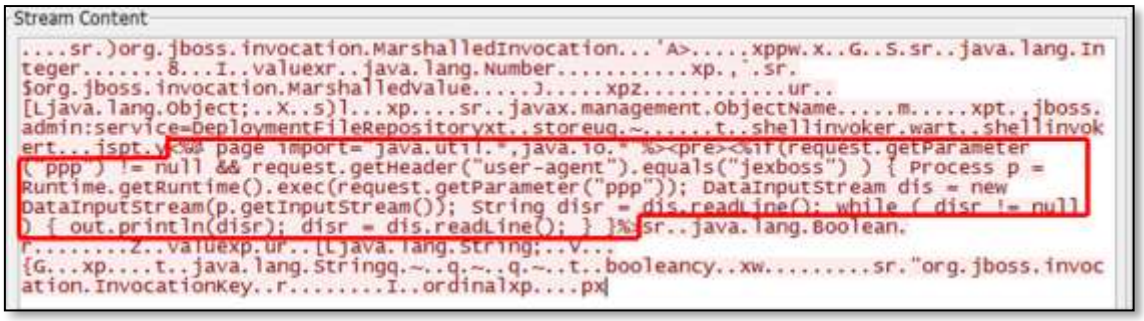



**図 6　JBoss AS に対しバックドアを作成する試み(一部)**

図 6に示す通信は、過去に作成したJSIGで検知しました。これは、JSOCで作るオリジナルシグネチャでは検知精度の向上を図るため、同じ脆弱性を悪用する様々な攻撃手法を想定し、検知できる様に工夫を凝らしているからです。過去に検知した攻撃通信から、今後発生する可能性のある攻撃通信を先読みしたシグネチャを作成していることも他にはない JSOC の強みの一つです。

### 3.1.2　JBoss Application Server の脆弱性を悪用する攻撃検証について

2015 年 3 月、3.1.1 に記載した攻撃手法と合わせて JBoss AS に対して任意のコード実行が可能な攻撃手法が公開されました。

図 7 に、この手法による攻撃通信を示します。

図 7の通信は、3.1.1 に記載したバックドアを作成する通信とは異なり、攻撃対象ホストで直接 OS コマンド(赤枠)を実行する試みです。JSOC では現在まで、本手法を悪用する通信を検知した実績はあり

ませんが、今後検知する可能性が考えられます。

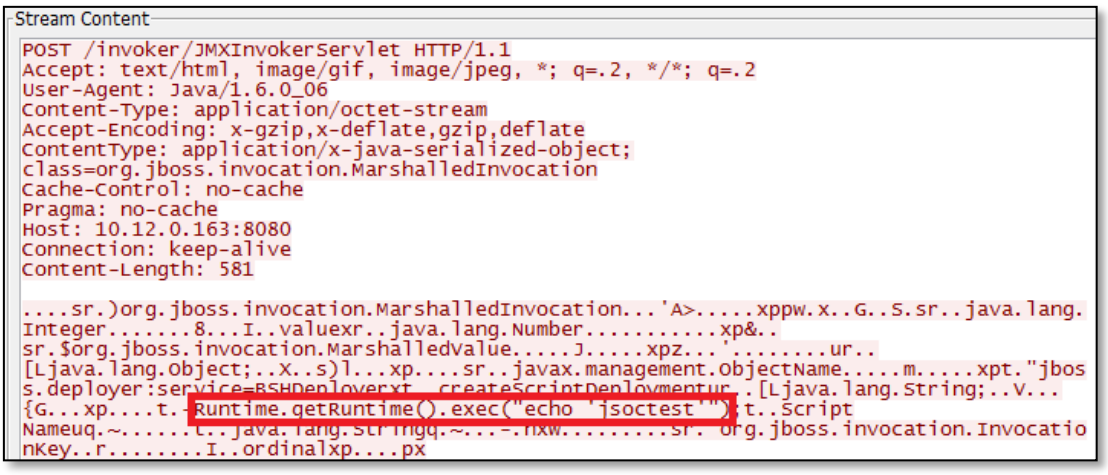



**図 7　JBoss AS に対しコード実行を試みる通信**

### 3.1.3　JBoss Application Server の脆弱性を悪用する攻撃への対策

新たに公開された攻撃コードは、対象とする脆弱性が明記されていません。JSOC では、バージョンの違う JBOSS AS の環境を準備し、本攻撃コードの検証を行いました。その結果、InvokerServlet に外部からアクセスできる環境下で、本攻撃の影響があることを確認できたバージョンは以下のとおりです。

- JBoss Application Server 3.2.x
- JBoss Application Server 4.x
- JBoss Application Server 5.x
- JBoss Application Server 6.x

一部の JBoss AS では過去に公開された脆弱性に対応し、InvokerServlet へのアクセス制御による対策を行ったバージョンも存在します。しかし、使用する OS や利用契約によっては、すでにサポートが終了しているバージョンの JBoss AS もあり、本攻撃手法の影響を受けるため、メーカの公開する回避策の適用か、影響を受けないバージョンへのアップデートが必要です。

本脆弱性の根本的な原因は InvokerServlet のアクセス制御の不備であるため、JBoss AS をご利用中の場合は、開発元が推奨する適切なアクセス制御[3]が行われているかを今一度ご確認ください。

[3] Securing JBoss Application Server
https://developer.jboss.org/wiki/SecureJboss/

## 3.2 phpMoAdmin におけるコード実行の脆弱性について

### 3.2.1 phpMoAdmin に対する攻撃の検知事例

オープンソースのデータベース MongoDB を管理する GUI ツールの phpMoAdmin には、細工されたパラメータにより任意のコードが実行可能な脆弱性が存在します。これは、phpMoAdmin で使われる eval 関数で適切に文字列処理が行われず、「system」や「exec」などの php の関数がそのまま解釈されるため、任意のコード実行が可能になるものです。phpMoAdmin は 2013 年 9 月の最新版公開以降、更新されておりません(2015 年 6 月 30 日現在)。そのため、本脆弱性は未修正の状態です。

JSOC では、本脆弱性を悪用する攻撃通信を 2 種類検知しました(図 8)。

図 8 a.は本脆弱性を悪用し php の関数「phpinfo」を実行する試み、b.は Linux の OS コマンド「id」を実行する試みです。phpMoAdmin の内部で使われるパラメータ「find」と「object」は、値の妥当性チェックを行わずに eval 関数の引数として利用されています(図 9 の赤線部)。そのため、攻撃者は悪意のあるリクエストを送信することで、任意のコード実行が可能です。

これまでに本攻撃を検知した対象ホストにて、phpMoAdmin を利用していると考えられるホストは確認していません。そのため、本攻撃は攻撃対象の脆弱性存在調査のため、phpMoAdmin の利用有無にかかわらず、無差別なホストに対して行われているように見受けられます。

Stream Content

```
GET /phpmoadmin/moadmin.php?collection=secpulse&action=listRows&find=array();phpinfo();exit;
HTTP/1.1
Host: [redacted]
Connection: Keep-Alive
```

**a. GET リクエストによるコード実行**

Stream Content

```
POST /moadmin.php HTTP/1.1
Host: [redacted]
Accept: */*
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; .NET CLR 1.1.4322)
Referer: [redacted]
Content-Type: application/x-www-form-urlencoded
Content-Length: 26

object=1;system('id');exit
```

**b. POST リクエストによるコード実行**

**図 8 phpMoAdmin におけるコード実行を試みる攻撃通信**

```
551         $find = array();
552         if (isset($_GET['find']) && $_GET['find']) {
553             $_GET['find'] = trim($_GET['find']);
554             if (strpos($_GET['find'], 'array') === 0) {
555                 eval('$find = ' . $_GET['find'] . ';');
556             } else if (is_string($_GET['find'])) {
557                 if ($findArr = json_decode($_GET['find'], true)) {
558                     $find = $findArr;
559                 }
560             }
561         }
```

**a. パラメータ「find」の処理部分**

```
685     /**
686      * Saves an object
687      *
688      * @param string $collection
689      * @param string $obj
690      * @return array
691      */
692     public function saveObject($collection, $obj) {
693         eval('$obj=' . $obj . ';'); //cast from string to array
694         return $this->mongo->selectCollection($collection)->save($obj);
695     }
```

**b. パラメータ「object」の処理部分**

**図 9 各パラメータの内部処理部分(ソースコードより抜粋)**

### 3.2.2 phpMoAdmin の脆弱性を悪用する攻撃への対策

脆弱性を修正したバージョンの phpMoAdmin がリリースされていないため、本脆弱性に対する根本的な対策はありません。本脆弱性の回避策は、phpMoAdmin に対して適切なアクセス制御設定を行うことです。しかしながら、今後、アクセス制御設定では回避できない他の脆弱性が見つかる可能性も捨て切れません。そのため、phpMoAdmin を現在ご利用の場合は、他の管理ツールへの移行をご検討ください。

また、このようなコード実行の脆弱性は、phpMyAdmin など他のデータベース管理ツールにも潜在している可能性が考えられます。他のツール、もしくは他のデータベースを利用している場合でも、最新のバージョンで運用し、管理ツールへのアクセス制御を適切に行うことが重要です。

## 3.3　マルウェアへの感染を引き起こすダウンローダの通信の検知について

### 3.3.1　UPATRE/DYRE 感染通信の検知事例

UPATRE/DYRE はスパムメールに添付されて拡散されることの多いダウンローダであり、感染すると複数のマルウェアをダウンロードします[4]。ダウンロードするマルウェアには一般的なワームやボットのほかに、GameoverZeus や ZBOT などのインターネットバンキングを狙うマルウェアが含まれているため、UPATRE/DYRE 感染によって端末上の情報を窃取されるだけでなく、金銭的な影響を受ける可能性があります。

JSOC では、2015 年 1 月、FireEye により複数のお客様にて UPATRE/DYRE に感染した通信を検知しました。

表 3 に JSOC で確認した UPATRE/DYRE 感染端末から発生した通信の接続先を示します。JSOC で検体解析を行った際、同一の検体を実行するたびに異なる送信先ホストに対してランダムなポート宛に対して HTTP 通信が発生することを確認しました。

**表 3 UPATRE/DYRE 感染端末から発生した通信の接続先**

| 接続先 IP アドレス | 接続先ポート | 所属国 | JSOC 検知有無 |
|---|---|---|---|
| 80.248.222.238 | 40266/TCP | フランス | |
| 177.124.228.4 | 46521/TCP | ブラジル | |
| 195.154.242.226 | 18208/TCP | フランス | ★ |
| 202.153.35.133 | 17211/TCP | インド | ★ |
| | 42886/TCP | | |
| | 44912/TCP | | |
| | 44951/TCP | | |
| | 45831/TCP | | |
| | 47773/TCP | | |
| | 40313/TCP | | |

★ は JSOC で検知実績のある接続先

その他は JSOC 検証による接続先

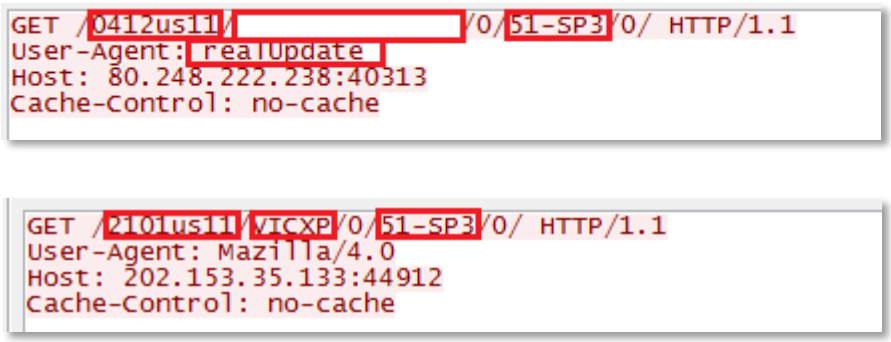
[4] 2013 年スパムメールに最も多く添付された UPATRE」ファミリ 巧妙化する添付手法
http://blog.trendmicro.co.jp/archives/8909

図 10 に UPATRE/DYRE 感染端末から発生した通信を示します。

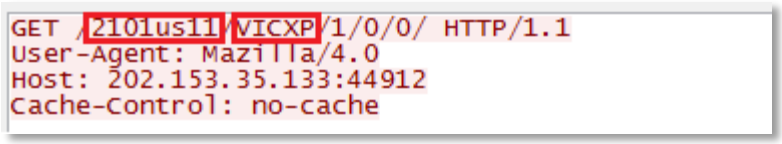
UPATRE/DYRE に感染した端末からは以下の特徴を持つ HTTP リクエストが発生します[5]。

① /感染日付と UPATRE/DYRE の作成情報/感染端末のホスト名/0/OS バージョン/0/

② /感染日付と UPATRE/DYRE の作成情報/感染端末のホスト名/1/0/0/




**a. ① の特徴を持つ HTTP リクエスト**




**b. ② の特徴を持つ HTTP リクエスト**

**図 10 UPATRE/DYRE 感染端末から発生した通信例**

また、端末が UPATRE/DYRE に感染する度、表 4 に示す異なる接続先に対して UDP 通信が発生する場合があることを確認しました。この通信は、接続先のホスト名から STUN(Simple Traversal of UDP through NATs)に関する通信であると考えられます。STUN は NAT を超えて双方向でリアルタイムの IP 通信をする技術であり、端末がグローバル IP アドレスを保有していなくとも、外部のホストと UDP を利用して音声、映像、文章などを双方向に通信することを可能にします。

UPATRE/DYRE 感染時に発生する通信の内容からその意図を明確に読み取ることはできませんでした。今後同様に STUN を用いたマルウェアの増加も考えられます[6]。利用する環境のポリシーを鑑みて STUN を利用した通信の必要性や、STUN を利用した通信のアクセス制御が適切か確認することが重要です。

---

[5] Threat Spotlight: Upatre – Say No to Drones, Say Yes to Malware
http://blogs.cisco.com/security/talos/upatre-ssl

[6] Malware Trending: STUN Awareness
http://researchcenter.paloaltonetworks.com/2014/09/malware-trending-stun-awareness/

**表 4 UPATRE/DYRE 感染時の STUN 通信の接続先**

| 接続先 |
|---|
| numb.viagenie.ca |
| stun.internetcalls.com |
| stun2.l.google.com |
| stun3.l.google.com |
| stunserver.org |

UPATRE/DYRE を検知した FireEye は、仮想環境においてファイルを実行した際の特徴的なふるまいを解析し、ファイルが疑わしい挙動を行うか調査しアラートをあげる機器です。

IDS/IPS はネットワーク通信のパターンマッチングにより検知するため、多種多様に存在するマルウェアやその亜種に対応するシグネチャが用意できず、検知できない可能性があります。JSOC ではファイアウォール、FireEye など様々な機器を監視しているため、それぞれの機器にて検知した情報や検証した結果を基に IDS/IPS に JSOC オリジナルシグネチャを作成し、検知精度を向上させることができることも JSOC の強みです。

### 3.3.2 UPATRE/DYRE などのインターネットバンキングを狙ったマルウェア感染への対策

マルウェアに感染しないよう、以下の基本的な対策を実施することが重要です。

□ ウイルス対策ソフトを最新の定義ファイルに更新する
□ オペレーティング・システムとアプリケーション・ソフトウェアを最新の状態に維持する
□ 不審なメールおよび添付ファイルは開かない

また、ウイルス対策ソフトでは検知できないようマルウェアや、ゼロデイ攻撃の影響を軽減するため、以下の対策を実施することが重要です。

□ Mircosoft 社が提供する EMET[7]を導入する

また、UPATRE/DYRE のように、副次的にインターネットバンキングを狙ったマルウェアに感染する場合、上記対策だけでなく、以下のインターネットバンキングを利用する上での対策も併せて実施されることが重要です。

[7] Enhanced Mitigation Experience Toolkit
https://technet.microsoft.com/ja-jp/security/jj653751.aspx

**端末の運用に関する対策**

□　利用するインターネットバンキングが提供する不正送金対策ソフトウェアを活用する

□　利用するインターネットバンキングが提供するワンタイムパスワードやトークンを活用する

**業務運用に関する対策**

□　複数のサイトで認証情報の使いまわしをしない。パスワード管理ソフトウェアを使用する

□　インターネットの閲覧やメールを送受信する端末と、インターネットバンキングや重要システムを利用する端末を分ける

□　被害にあった際に、迅速にアカウントやサービス利用の停止が出来るように通報・連絡先、手順を確認し、整備する

□　手口や被害事例について、常に最新の情報をセキュリティ情報サイトやニュースサイト、銀行サイトからの情報等で確認する

**その他被害の軽減方法**

□　振込限度額を必要最低額まで下げる

# 第二章 2014 年度の傾向のまとめ

## 1 2014 年度の年間サマリ

第二章では、2014 年 4 月から 2015 年 3 月までの 1 年間を振り返り、2014 年度通年のインシデント傾向をまとめます。

2014 年度はインターネットからの攻撃による重要インシデントが過去 3 年間で最多の件数となりました。

これは、2014 年度にミドルウェアの脆弱性が相次いで公開され、外部からその脆弱性を悪用する攻撃を継続して検知しためです。ミドルウェアの脆弱性は複数のサービスや製品で利用されているため影響範囲が広く攻撃対象が多岐にわたり、また対策が行き届きにくいことが特徴です。このような脆弱性の公開は 2015 年度以降も続くものと予想されます。これまではインターネットからの攻撃は Web アプリケーションに対する攻撃が中心でしたが、今後は Web アプリケーションのみならずこのようなミドルウェアを利用するネットワーク上の全ての機器が攻撃対象になると考えられます。

また、2014 年度、内部ホストがマルウェアに感染したことによって発生する重要インシデントは、Zeus、Citadel、Neverquest などインターネットバンキングを狙ったマルウェアの検知件数が増加する一方で、端末の設定情報を狙うマルウェアの検知件数は減少しました。攻撃者の狙いは、感染端末の設定情報からより直接的な金銭窃取に変わっていると考えられます。

## 2　インターネットからの攻撃による重要インシデントの検知傾向

### 2.1　検知傾向のまとめ

図 11 にインターネットからの攻撃によって発生した重要インシデントの件数推移を示します。

インターネットからの攻撃による重要インシデントは 2014 年度過去 3 年間で最多の件数が発生しました。

従来、毎年 9 月に柳条湖事件への抗議活動の一環として攻撃の検知件数が増加する事例がありましたが、近年 3 年間は特筆すべき傾向変化は見られませんでした(図 11-[1])。

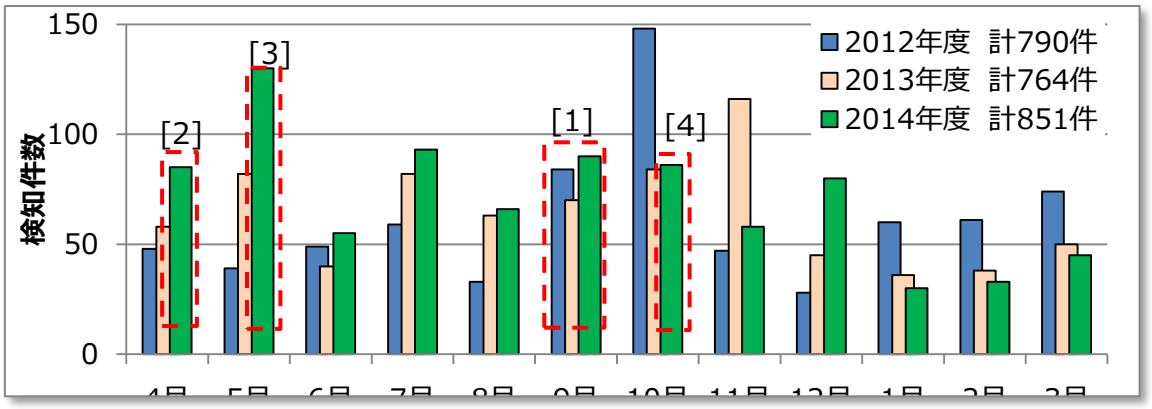


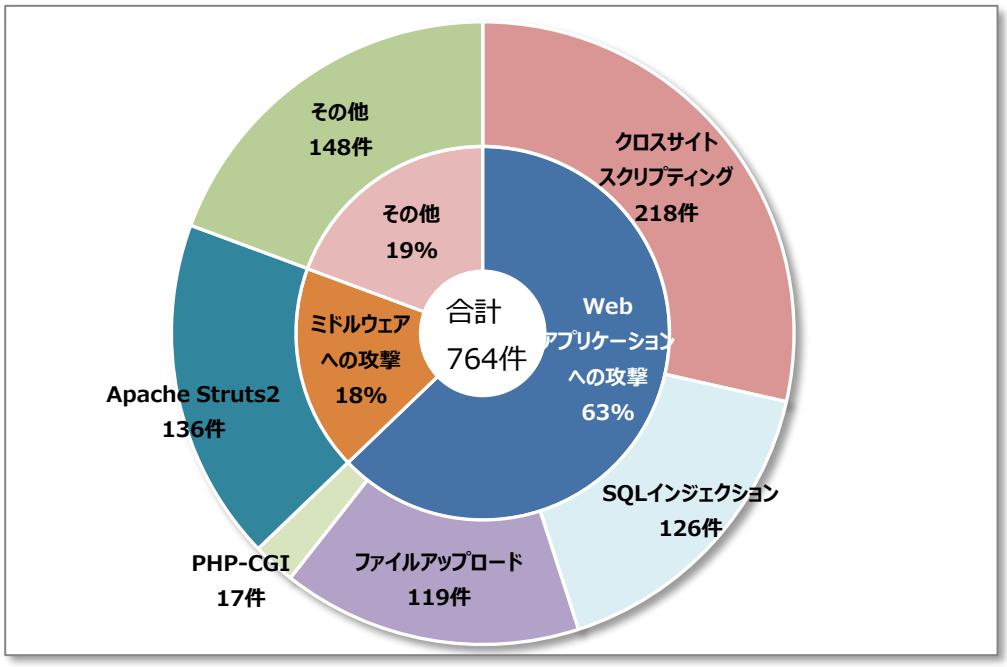

**図 11 インターネットからの攻撃による重要インシデントの件数推移**

図 12 にインターネットから発生した重要インシデントの内訳を、表 5 に 2014 年度に公開された外部公開ホストにおける主な脆弱性を示します。

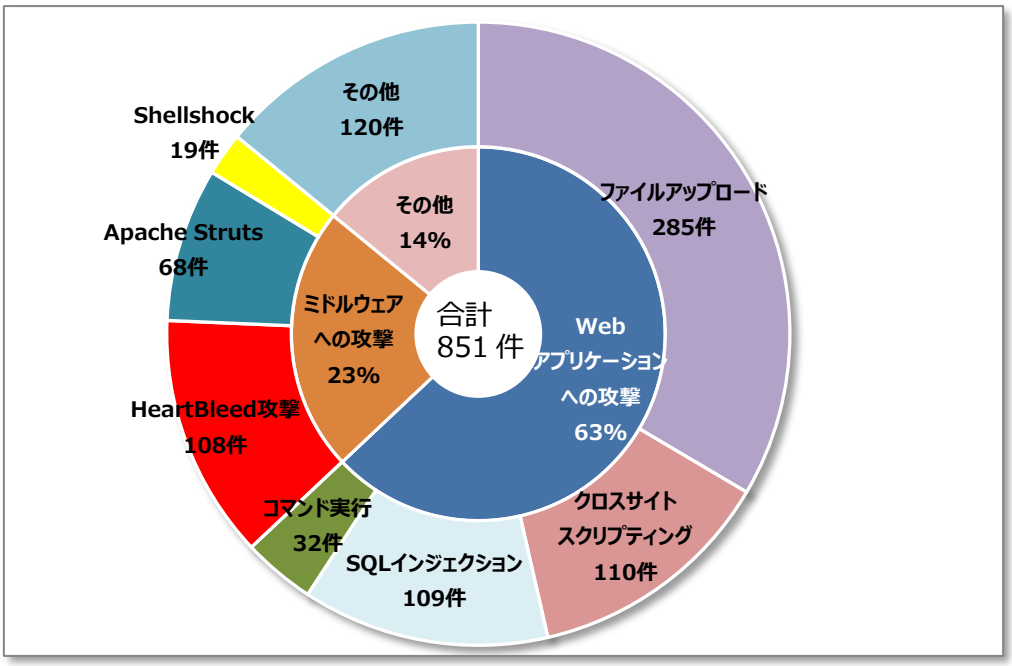
2014 年度は、ミドルウェアの脆弱性が相次いで公開(表 5 色つき)され、その脆弱性を悪用する攻撃を継続して検知しました。2013 年度までの攻撃対象は主に Web アプリケーションの脆弱性であり、ミドルウェアについては ApacheStruts など特定のミドルウェアが狙われるのみでした。

しかしながら、2014 年度脆弱性の存在が公開されたミドルウェアは、複数のサービスや製品で利用されていたため影響範囲が広く、攻撃対象が多岐にわたり、また対策が行き届きにくいことが特徴です。

このような脆弱性の公開は 2015 年度以降も続くものと予想されます。これまではインターネットからの攻撃は Web アプリケーションに対する攻撃が中心でしたが、今後は Web アプリケーションのみならず、このようなミドルウェアを利用するネットワーク上の全ての機器が攻撃対象になると考えられます。




a.　2013 年度




b.　2014 年度

**図 12　インターネットからの攻撃による重要インシデントの内訳**

**表 5 2014 年度に公開された外部公開ホストにおける主な脆弱性**

| 脆弱性の概要 | JSOC の検知概要 | 主な検知時期 |
|---|---|---|
| Apache Struts におけるコード実行の脆弱性[8] (S2-020、S2-021、S2-022) | 脆弱性の検証コード公開後、ホストを悪用する攻撃通信を検知しました。現在はほとんど攻撃通信および成功事例がありません。 | 2014 年 4 月～5 月 ※図 11-[2] |
| OpenSSL Heartbeat 拡張における情報漏えいの脆弱性[9](Heartbleed) | 脆弱性の公開後、脆弱性の有無を調査する攻撃通信を検知しました。現在も脆弱なホストの存在を確認しています。 | 2014 年 4 月～現在継続中 ※図 11-[3] |
| OpenSSL の ChangeCipherSpec(CCS) メッセージの処理の脆弱性[10] | 脆弱性の公開後、脆弱性の有無を調査する攻撃通信を検知しました。<br>脆弱性の公開当初は、攻撃に対して脆弱なホストの存在を確認しました。 | 2014 年 7 月 |
| SSLv3 プロトコルの暗号化データ解読の脆弱性[11](POODLE) | 攻撃と判断した検知実績はありません。 | |
| SSL/TLS の実装における脆弱性[12](FREAK ) | 攻撃と判断した検知実績はありません。 | |
| GNUBash におけるコード実行の脆弱性[13] (Shellshock) | 脆弱性の公開後、脆弱性の有無を調査する通信やホストを悪用する攻撃通信を検知し、現在も継続しています。<br>脆弱性の公開当初は、攻撃に対して脆弱なホストの存在を確認しました。 | 2014 年 9 月末～現在継続中 ※図 11-[4] |
| 各種コンテンツ管理システム (CMS)の脆弱性を悪用するファイルアップロードの試み | 公開から期間の経過した CMS やプラグインの脆弱性を悪用する攻撃通信を検知しています。攻撃の成功事例がありません。 | 2014 年度に増加～現在継続中 |

※ JSOC の検知事例の「現在」は 2015 年 3 月末の検知状況

---

[8] Apache Struts 2 の脆弱性が、サポート終了の Apache Struts 1 にも影響
http://www.lac.co.jp/security/alert/2014/04/24_alert_01.html

[9] TLS heartbeat read overrun (CVE-2014-0160)
https://www.openssl.org/news/secadv_20140407.txt

[10] JVN#61247051 OpenSSL における Change Cipher Spec メッセージの処理に脆弱性
https://jvn.jp/jp/JVN61247051/

[11] JVNVU#98283300 SSLv3 プロトコルに暗号化データを解読される脆弱性(POODLE 攻撃)
https://jvn.jp/vu/JVNVU98283300/

[12] JVNVU#99125992 SSL/TLS の実装が輸出グレードの RSA 鍵を受け入れる問題（FREAK 攻撃）
https://jvn.jp/vu/JVNVU99125992/

[13] JVNDB-2014-004410 GNU bash における任意のコードを実行される脆弱性
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-004410.html

## 2.2　OpenSSL の Heartbeat 拡張の脆弱性を悪用する攻撃(Heartbleed)

図 13 に Heartbleed 攻撃の検知件数および重要インシデントの件数推移を示します。

OpenSSL の Heartbeat 拡張の脆弱性の公開以来、JSOC では本脆弱性の有無を調査する通信や、本脆弱性を悪用する攻撃通信を多数検知しました。Heartbleed 攻撃の検知件数は、2014 年 4 月、脆弱性公開の直後から爆発的に増加したものの、2014 年 5 月以降徐々に減少傾向にあります。しかしながら、第 1 章 P.5 2.2 発生した重要インシデントに関する分析のとおり依然として脆弱なホストが見つかるケースが後を絶ちません。

Heartbleed 攻撃は SSL/TLS サービス（443/TCP）の通信以外にも IMAP over SSL/TLS(993/TCP)などの OpenSSL を使用する暗号化通信に対しても検知しています。実際に、一部のメールのアプライアンス製品内で脆弱性のある OpenSSL を使用していたために重要インシデントに繋がった事例も発生しました。

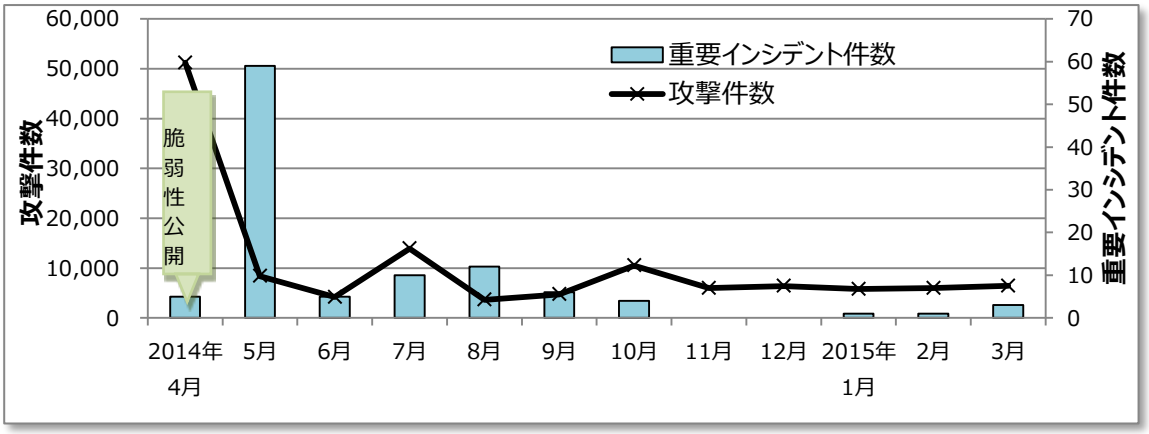



**図 13 Heartbleed 攻撃の攻撃件数および重要インシデントの件数推移**

## 2.3　GNU bash におけるコード実行の脆弱性を悪用する攻撃(Shellshock)

図 14 に Shellshock の検知件数および重要インシデントの検知件数推移を示します。

GNU bash におけるコード実行の脆弱性の公開以来、JSOC では本脆弱性の有無を調査する通信や、本脆弱性を悪用する攻撃通信を継続して高い頻度で検知しており、攻撃通信が収束する気配は見えません。また、本脆弱性の公開以来、攻撃対象のホストが Shellshock に対して脆弱な応答を確認した重要インシデントが複数発生しましたが 2014 年度末には収束しました。

Shellshock の検知傾向は日々変化しており、脆弱性の公開当初は、公開 Web サーバに対する攻撃が大半を占めましたが、対策が未実施になりがちな Web サーバ以外のサービスや、NAS 製品のようにネットワークに接続可能な製品(IoT)が徐々に狙われるようになりました。

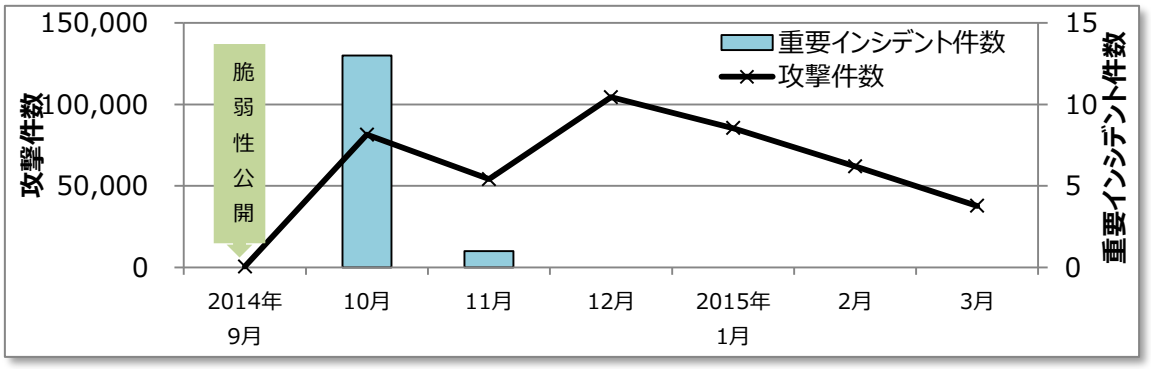



**図 14 Shellshock の検知件数および重要インシデントの件数推移**

## 2.4 不審なファイルアップロードの試みの検知について

2015 年 3 月、日本国内で複数の Web サイトが改ざんされイスラム国に関連すると考えられる画像ファイルが表示される事案が発生しました。本事案は日本国内でも広く利用される CMS である WordPress のプラグインの脆弱性が悪用されたことが報告されています[14](図 15)。


**図 15 改ざんされた Web サイトに掲載された画像の例**

2014 年度の JSOC 検知実績では、CMS やそのプラグインの脆弱性を悪用し、不審なファイルをアップロードする試みが増加しました(図 16)。JSOC で検知したファイルアップロードの試みの攻撃対象の一覧を表 6 に示します。これらの脆弱性はすでに公開から期間が経ったものが多く、JSOC では攻撃の成功事例の検知はありません。

最新の CMS を利用していても、プラグインに脆弱性が存在する場合はサーバを悪用される可能性があります。また、CMS で利用するプラグインは、テーマを使用すると自動的にインストールされる場合があり、管理者の意図しないプラグインが存在する可能性があります。なお、プラグインの修正は作成者に依存するため、プラグインの更新頻度によっては脆弱性が発見されても修正が行われない場合があります。

そのため、CMS 自体のバージョンアップや、以下の脆弱性公開時の対応を整備する必要があります。

[14] 「IslamicState(ISIS)」と称する者によるウェブサイト改ざんについて
http://www.npa.go.jp/keibi/biki/201503kaizan.pdf

### 脆弱性公開時の対策

□　脆弱性を修正したバージョンの適用や開発者が推奨する回避策の適用する

### 運用上の対策

□　プラグインの利用ポリシーを確認する

□　プラグイン利用状況を管理する

□　常に最新の情報を開発者のアナウンスやニュースサイト、セキュリティ情報サイト等で確認する

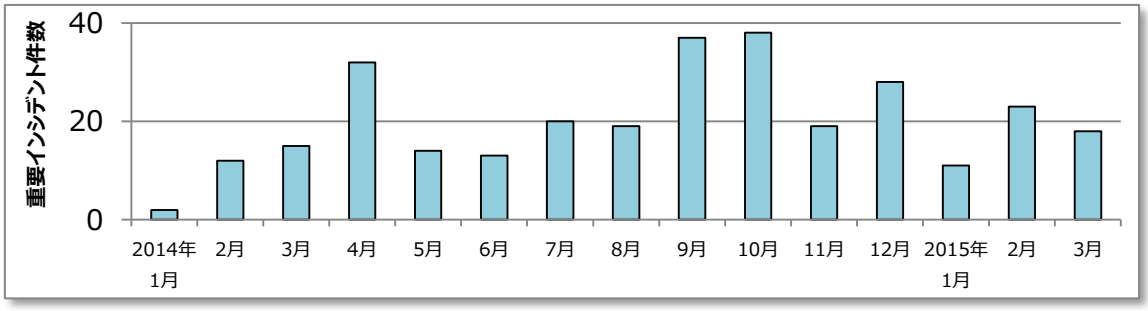



**図　16　ファイルアップロードの試みによる重要インシデント検知件数の推移**

**表　6　ファイルアップロードの試みを検知した攻撃対象**

| 対象 | プラグイン |
|---|---|
| FCK Editor | |
| Joomla ! | JCE |
| | jDownloads |
| WordPress | WP Symposium |
| | MailPoet Newsletters |
| | N-Media Website Contact Form with File Upload |
| | WP All Import |

```
POST /wp-content/plugins/wp-symposium/server/php/index.php HTTP/1.1
Host: [redacted]
Content-Length: 741
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:34.0) Gecko/20100101 Firefox/34.0
Connection: keep-alive
Content-Type: multipart/form-data; boundary=b66dcdf48ece45c5a331997deb666ae3

--b66dcdf48ece45c5a331997deb666ae3
Content-Disposition: form-data; name="uploader_url"
```

**図　17　不審なファイルアップロードの試みの検知例**

## 3　ネットワーク内部から発生した重要インシデントの検知傾向

図 18 に 2014 年度にネットワーク内部から発生した重要インシデントの件数推移を示します。

2014 年度にネットワーク内部から発生した重要インシデントの件数は 2013 年度より減少しました。

これは、2013 年度に多数発生した、DNS の設定不備を悪用した踏み台の試みによる重要インシデントの件数が減少したためです。

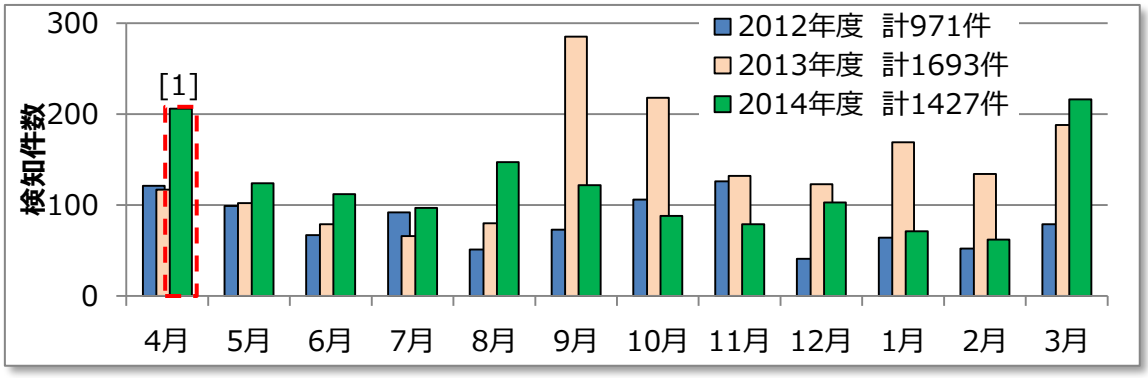
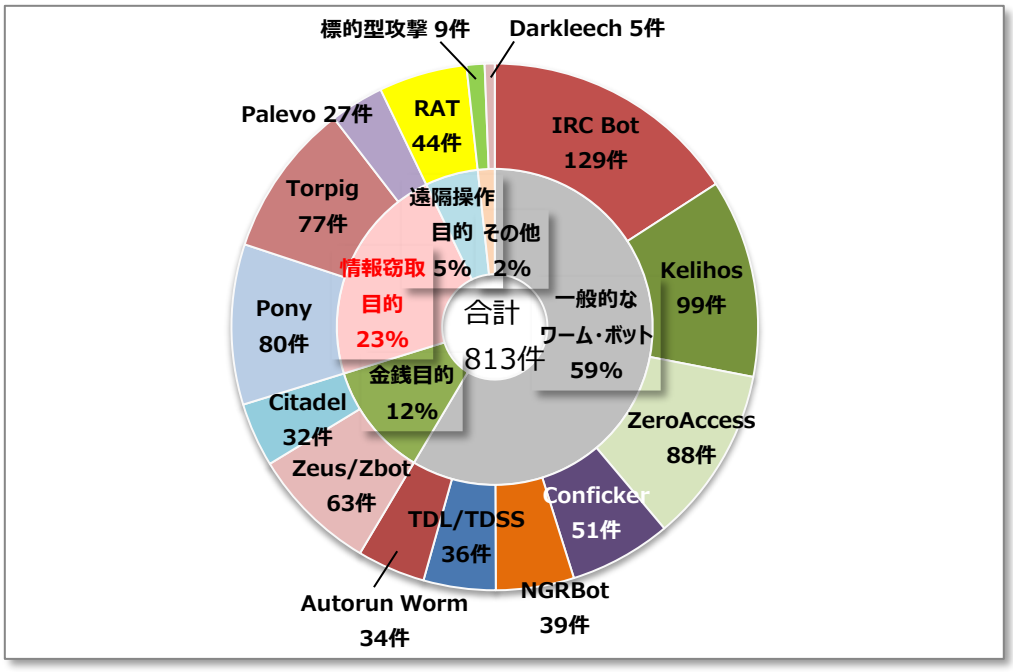


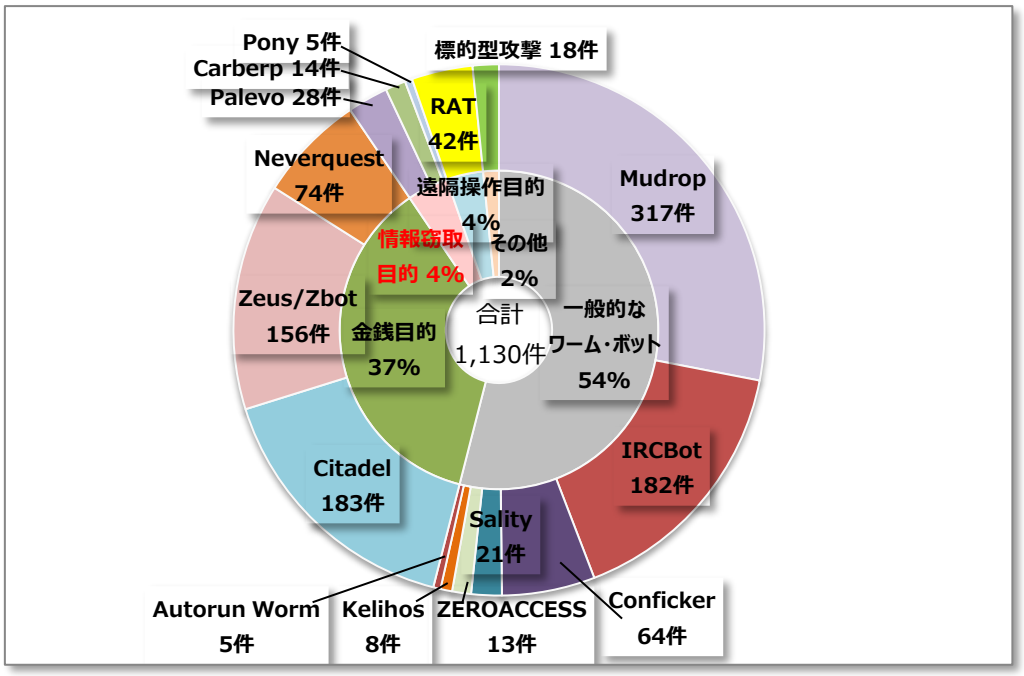

**図 18　ネットワーク内部から発生した重要インシデントの検知件数**

図 19 にネットワーク内部で発生したウイルス感染による重要インシデントの内訳を示します。

2014 年度は、Zeus、Citadel、Neverquest などインターネットバンキングを狙ったマルウェアの検知件数が増加しました(図 18-[1])。一方で端末の設定情報を狙うマルウェアの検知件数は減少しました。攻撃者の狙いは、感染端末の設定情報からより直接的な金銭窃取に変わっていると考えられます。




a. 2013 年度




b. 2014 年度

**図 19 ネットワーク内部から発生したウイルス感染による重要インシデントの内訳(件数上位 15 種)**

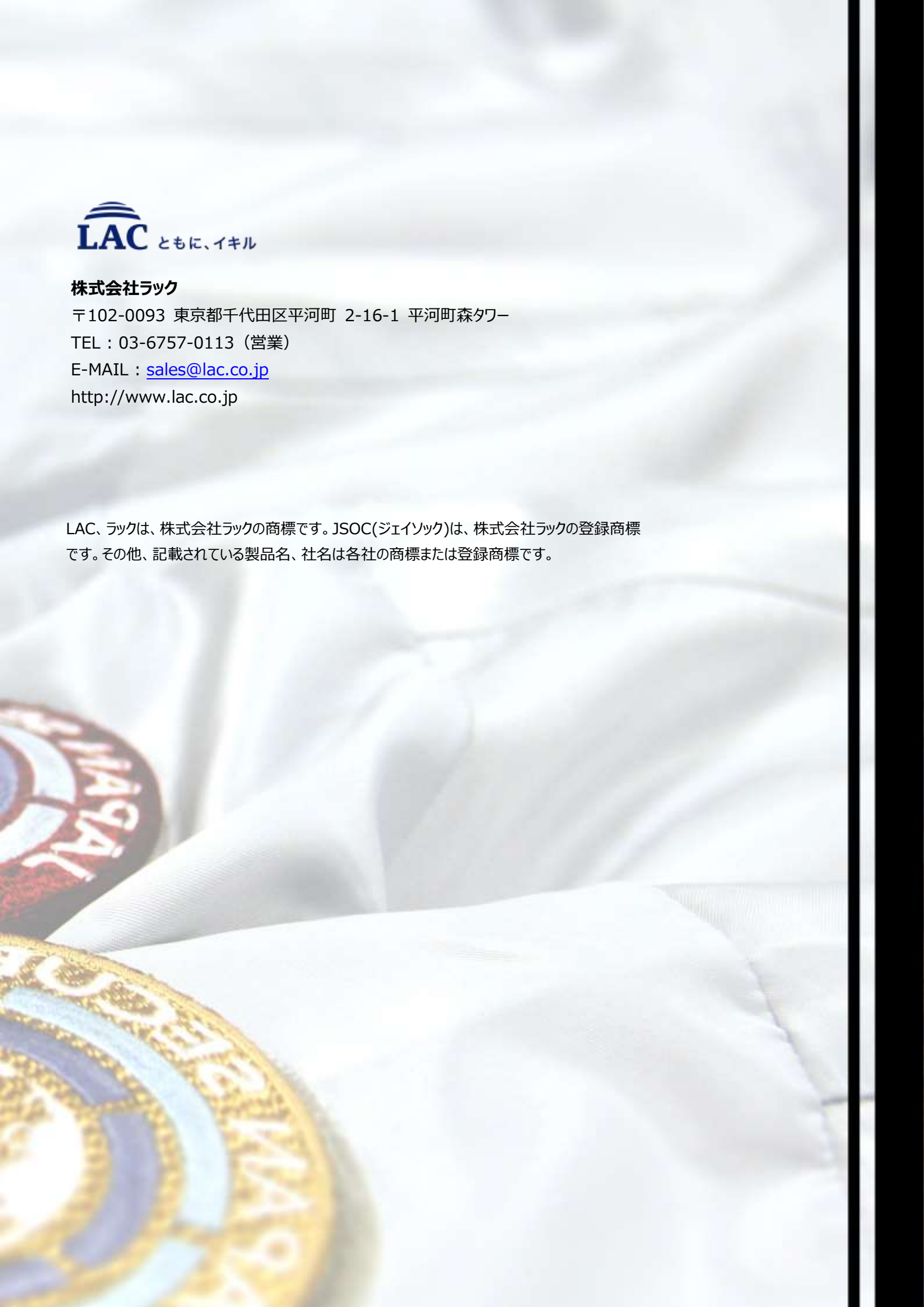
## 終わりに

JSOC INSIGHT は、「INSIGHT」が表す通り、その時々に JSOC のセキュリティアナリストが肌で感じた注目すべき脅威に関する情報提供を行うことを重視しています。

これまでもセキュリティアナリストは日々お客様の声に接しながら、より適切な情報をご提供できるよう努めてまいりました。この JSOC INSIGHT では多数の検知が行われた流行のインシデントに加え、現在、また将来において大きな脅威となりうるインシデントに焦点を当て、適時情報提供を目指しています。

JSOC が、「安全・安心」を提供できるビジネスシーンの支えとなることができれば幸いです。

**JSOC INSIGHT vol.8**
**【執筆】**
天野 一輝 / 三和 弘典 / 高井 悠輔 / 村上 正太郎
(五十音順)



**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（営業）
E-MAIL：sales@lac.co.jp
http://www.lac.co.jp