LAC

JSOC INSIGHT

vol.4

2014 年 7 月 22 日

JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER

JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT

1　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。緊急で対応する必要のある重要なインシデント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】

2014 年 1 月 1 日 ～ 2014 年 3 月 31 日

※2013 年度傾向のまとめは 2013 年 4 月から 2014 年 3 月までを対象としています。

2　エグゼクティブサマリ

本レポートは、2013 年度第 4 四半期である 2014 年 1 月～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。また 2013 年度を振り返り、通年での傾向をまとめています。

2.1　第 4 四半期のサマリ

この四半期の特徴としては、自組織のサイトがインターネットからどのように見えているか、どのようなサービスや情報にアクセスできるか、つまり、外からの見た目を意識することが重要であるということが挙げられます。

本来アクセスできてはならない場所にアクセスされたり、公開する必要の無いサービスを公開していたり、問題が無いと判断して公開しているサービスが脆弱なままであったりと、見た目に気をつけることで回避できたのではないかというインシデントが多数ありました。そのため、アクセス制御を適切に行い、脆弱性を修正し続けるという今までにも言われてきたごくごく当たり前のことを丁寧に運用し続けることが、やはり重要であると考えます。

➢　手口が多様化した DDoS 攻撃の検知

時刻同期に使用される NTP の機能を悪用した DoS 攻撃[1]を JSOC にて確認しました。これはリフレクター攻撃と呼ばれる攻撃の一種ですが、近年、主に攻撃に使われてきた DNS とは異なり NTP サービスが利用されました。この原因は、外部の第三者に対して不必要なアクセスを許可している点にあります。外部に公開しているサービスを確認し、アクセス制御の見直しなどを定期的に実施する必要があります。

➢　インターネットバンキングを狙うマルウェアの流行

インターネットバンキングに使用されるアカウントを狙うマルウェアによる脅威が顕在化しています。マルウェアの感染により、不正送金された結果、ある日突然会社の口座残高がゼロになり、倒産に繋がるような懸念も出ています。今まで主流であった Zeus/Zbot、SpyEye だけでなく Citadel や Neverquest と呼ばれる新しいマルウェアの感染が複数のお客様で観測しました。

➢　IoT(Internet of Things)のセキュリティ

パソコンやスマートフォンのような情報通信機器だけではなく、家電製品や自動車などもインターネットに接続され、相互に通信できるようになってきており、このような技術や概念は IoT(Internet of Things)と呼ばれています。JSOC では、情報通信機器ではなく、IoT 組み込み機器と考えられる送信元からの攻撃通信を確認しており、今後さらに悪用されていくことは明らかです。ネットワークに機器を接続する際は、すべての機器が悪用される可能性があることを考え、アクセス制御などの対策を行う必要が

[1] ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起
http://www.jpcert.or.jp/at/2014/at140001.html

あります。

➢ 再び Apache Struts

2013 年 7 月に影響度の大きな脆弱性の公開後、多数の攻撃が観測された Apache Struts 2 に、再び影響度の大きな脆弱性が公開され、実際に攻撃を確認しています。また現行の 2.x 系だけではなく、すでにサポートが終了した 1.x 系にも同種の脆弱性が存在しており、Windows XP と同じくサポートが終了した製品を使用し続けることのリスクについて考え直すいい機会となりました。Apache Struts に限らず Web サービスを支えるフレームワークについては、製品のライフサイクルを考慮し、サポートが終了した製品を使い続けるような状況になることがないように運用設計すること、基幹の入れ替えが困難な場合には WAF や IPS による緩和策の導入や有償のサポートを受けることが望ましいと考えます。

2.2 2013 年度の年間サマリ

2013 年度は、インターネットからのインシデントとして Web サービスに対する攻撃が増加しました。特に、Web サーバのミドルウェアの脆弱性を狙った攻撃では、昨年同様に、脆弱性情報が公開された直後から攻撃通信の検知が増加しはじめ、実際に攻撃が成功した事例も確認しています。

内部からのインシデントとしては、不正送金に使用されるマルウェアの検知が増加しました。昨年まで検知された Zeus や SpyEye だけでなく Citadel や Neverquest といった新たなマルウェアや、機能が拡張された亜種を検知していることから、本格的に日本が標的として狙われ始めたことが読み取れます。また、国内企業や組織を狙った水飲み場型攻撃や正規のソフトウェアアップデートを悪用した標的型攻撃を確認しました。さらに、DNS や NTP、Chargen といった UDP を使用するサービスを悪用したリフレクター攻撃の検知も増加しています。

このように 2013 年度も新しい脅威や脆弱性が多数公開され、それに伴うインシデントが発生しております。今後も新たな脅威や脆弱性はなくなることはありません。対策としては、ソフトウェアのライフサイクルまで考えた運用を行い続けることが大原則であり、緩和策として各種セキュリティ対策製品の補完的な導入と運用を行い、単一の製品で十分と考えるのではなく複数の製品を多層的に組み合わせると言う運用を継続することしかないと考えます。

3　JSOC における重要インシデント傾向

3.1　重要インシデントの傾向

JSOC では、IDS/IPS、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なインシデントです。

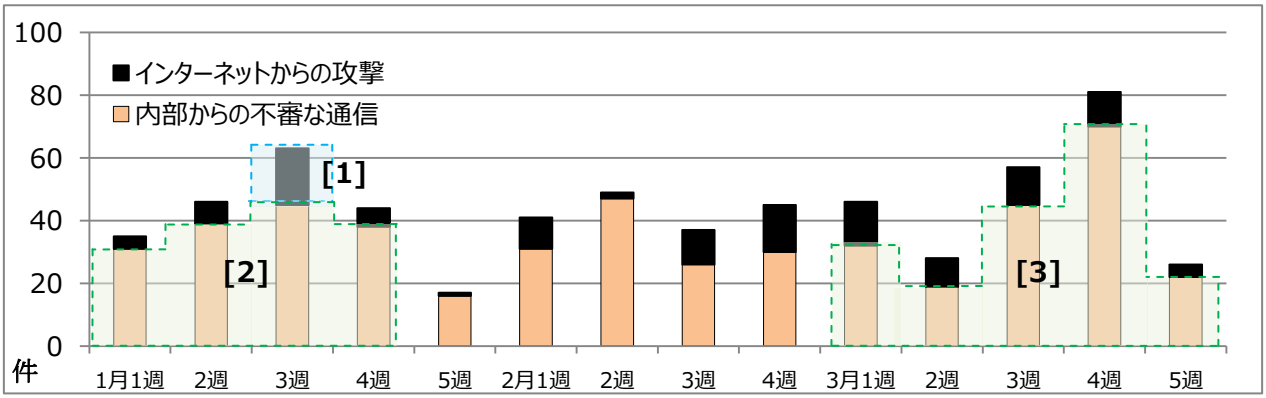
表 1 インシデントの重要度と内容

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 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
	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

グラフ 1 は、2014 年 1 月～3 月の重要インシデントの件数推移を示したものです。

インターネットからの攻撃による重要インシデントの発生件数については、一時的に 1 月 3 週に増加しました(グラフ 1-[1])。これは、クロスサイトスクリプティングの試みが増加したこと、NTP サービス(時刻同期に使われる UDP のサービス)や Chargen サービス(接続すると一定の文字列を生成し応答する UDP のサービス)を悪用した攻撃を検知していることが原因です。

内部から発生した重要インシデントの発生件数については、12 月から 1 月 4 週にかけて増加しました(グラフ 1-[2])。これは、主に 12 月 4 週より増加傾向にあった Citadel の感染通信によるものです。2 月に入り Citadel による感染通信は減少に転じましたが、3 月に入り Neverquest の感染通信による重要インシデントが増加しました(グラフ 1-[3])。なお、この二つのマルウェアに関連があるかどうかは不明です。



グラフ 1 重要インシデントの件数推移(2014 年 1 月～3 月)

※ 1 月 5 週および 3 月 5 週は 3 日分のデータです

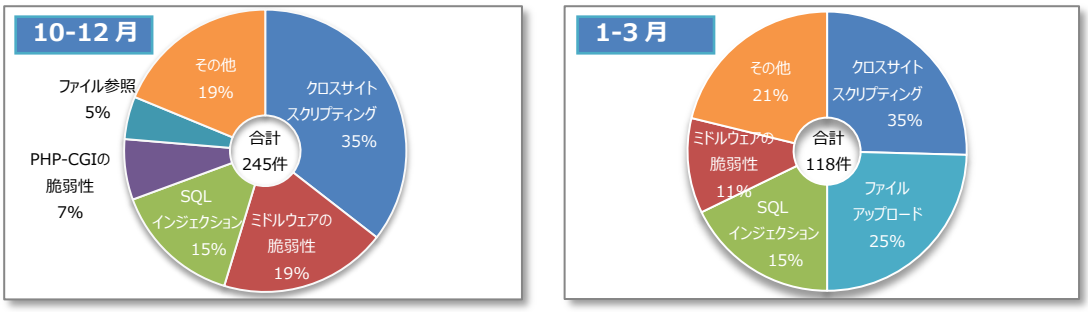
3.2　発生した重要インシデントに関する分析

グラフ 2 は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内訳です。

第 3 四半期(10-12 月)のインシデント 245 件と比較して、第 4 四半期(1-3 月)は 118 件と重要インシデント件数が減少しています。これには複数の要因がありますが、理由の一つとして第 3 四半期で多発していた CGI 環境で動作する PHP の脆弱性を悪用した攻撃が減少していることが挙げられ、お客様が本脆弱性への対応を実施された結果が大きく影響していると考えます。

また、1 月 3 週から 4 週にかけては、NTP サービス(時刻同期に使われる UDP のサービス)や Chargen サービス(接続すると一定の文字列を生成し応答する UDP のサービス)を悪用した攻撃による重要インシデントが発生しています。ともに、不正な UDP パケットを大量に送信することにより攻撃対象ホストをサービス不能にする DoS 攻撃に使われています。こうした攻撃の場合、外部からの不要なアクセスを許容していることが原因であるため、適切なアクセス制御の実施およびアクセス制御の定期的な見直しを推奨いたします。さらに、ファイルアップロードの試みによる重要インシデントの発生件数が前期と比較し大幅に増加しました。これは複数のお客様で、バックドア(PHP ファイル)をアップロードする試みを検知したためです。

3 月に、HTTP の PUT メソッドを悪用したファイルアップロードの試みが成功し Emergency インシデントが発生しました。本攻撃は、新たな手法を用いた攻撃ではなく、JSOC で日常的に検知している攻撃です。このようなインシデントは、Web サーバの新規公開時や置き換え時における設定不備が原因で発生していると考えられ、同様の攻撃による Emergency インシデントが 1 年に数件程度発生しております。公開前や置き換え後には必ずセキュリティ診断を実施し、サーバの設定に不備がないことを確認してから公開する運用の徹底を推奨いたします。



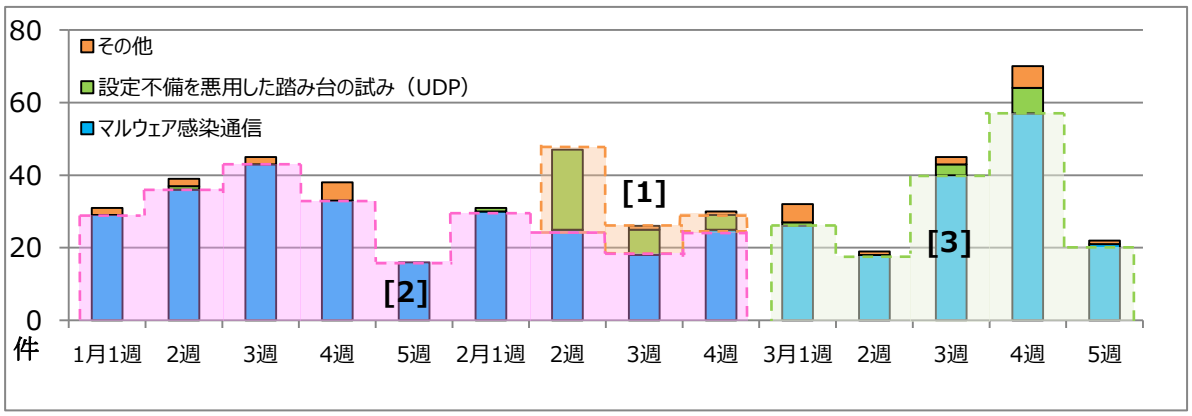
a. 2013 年 10～12 月　　**b. 2014 年 1～3 月**

グラフ 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

グラフ 3 は内部から発生した重要インシデントの検知件数推移です。内部から発生した重要インシデントは、お客様サイトの UDP サービスを悪用し踏み台とした DoS 攻撃とマルウェアの感染に大別できます。

お客様サイトの UDP サービスを悪用し踏み台とした DoS 攻撃は、2013 年 9 月に DNS サーバを

踏み台とする攻撃の検知件数が増加し[2]、それ以降減少傾向にあったものの、2 月 2 週から 4 週にかけて NTP サーバを踏み台とし外部の別のホストを攻撃する試みを多数検知したため、重要インシデントが増加しました(グラフ 3-[1])。NTP サーバを踏み台として悪用されたことによる重要インシデント件数の割合は、UDP を使用するサービスを悪用した攻撃のうち約 65%を占めました。



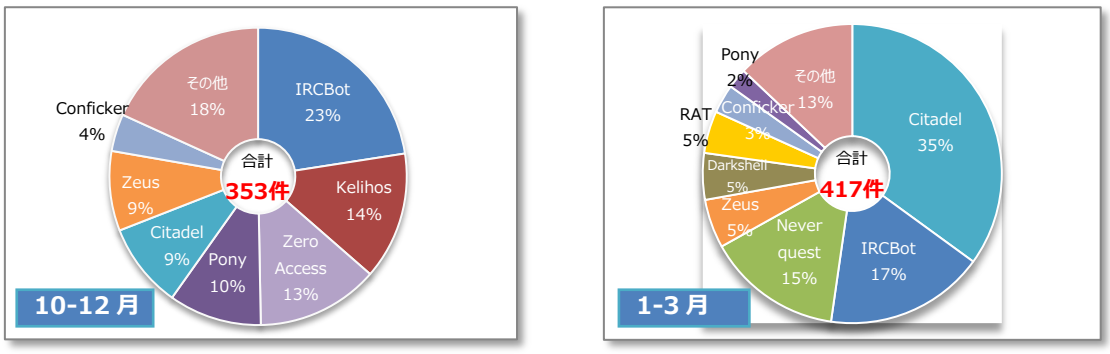
グラフ 3 内部から発生した重要インシデントの件数推移(2014 年 1 月～3 月)

※1 月 5 週および 3 月 5 週は 3 日分のデータです

グラフ 4 にマルウェア感染による重要インシデントの件数内訳を示します。

内部ホストのマルウェア感染による重要インシデントは、第 3 四半期の 353 件と比較して第 4 四半期は 417 件へと増加しました。

第 3 四半期の 12 月 4 週以降に増加した認証情報の窃取を行うマルウェア Citadel による感染通信は、第 4 四半期の 1 月から 2 月にかけて検知しています(グラフ 3-[2])。さらに 2 月 4 週以降、Citadel とは異なる種類で、同じく認証情報の窃取を行うマルウェア Neverquest による重要インシデントが徐々に増加し、3 月 3 週および 4 週では 15 件以上のインシデントが発生しています(グラフ 3-[3])。今後も、Citadel や Neverquest といったマルウェアによる重要インシデントは、継続して発生するものと予測しています。



a. 2013 年 10～12 月　　b. 2014 年 1～3 月

グラフ 4 マルウェア感染による重要インシデントの内訳

[2] JSOC INSIGHT Vol.3
http://www.lac.co.jp/security/report/2014/03/11_jsoc_01.html

4　今号のトピックス

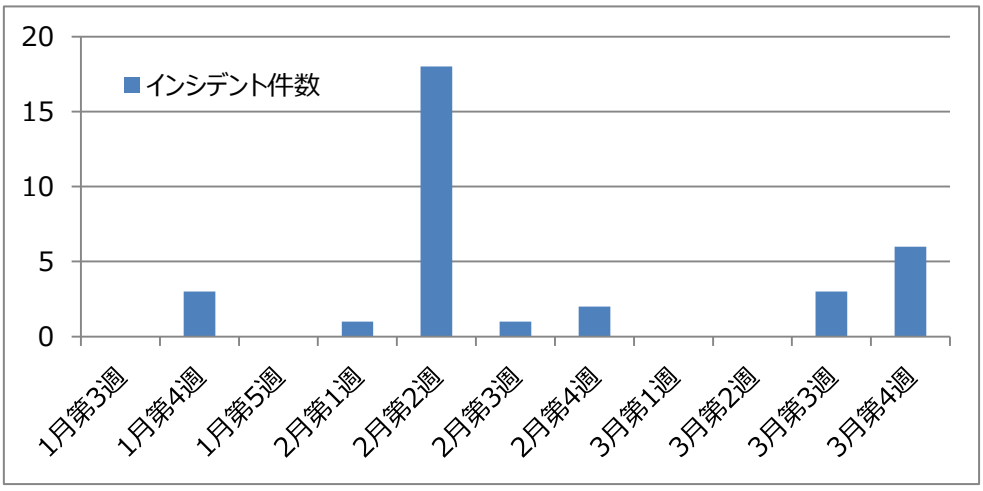
4.1　外部へ公開しているサービスを悪用した DoS 攻撃の増加について

2013 年 7 月以降、UDP サービスを悪用する DoS 攻撃のインシデントが増加しました。これらのインシデントにはリフレクター攻撃と呼ばれるサービスの応答を悪用する手法が用いられています。この手法では、以前は DNS が主に悪用されていましたが、DNS 以外のサービスが悪用されていることを確認しています。今回、2014 年 1 月から 3 月にかけて新しく発生した NTP を使用した事例と WordPress の Pingback 機能を使用した事例を紹介します。

4.1.1　NTP を悪用した DoS 攻撃

2013 年 12 月には、多くのお客様に「DNS リフレクター攻撃」の攻撃対象となったホストの対策が講じられたため、DoS 攻撃に関する通信は減少傾向にありました。しかし、1 月後半から NTP サービスを悪用したリフレクター攻撃の通信を多数検知しております。なお NTP サービスは時刻同期に使用される、DNS と同じく UDP を用いたサービスです。NTP サービスに関する不審な通信を検知したことをきっかけに JSOC での調査の結果、お客様のホストが脆弱であることを確認できたため、NTP リフレクター攻撃に悪用されていると判断し、重要インシデントとしました。

また警察庁から 2014 年 1 月に NTP サービスに関する注意喚起が公開[3]されております。



グラフ 5 NTP サービスを悪用したインシデント件数の推移

NTP リフレクター攻撃は、ntpd に実装されているサーバの状態を確認する monlist と呼ばれる機能を悪用します。monlist は、NTP サーバが過去に通信したマシンの IP アドレスの履歴リストを返す機能で、問い合わせのリクエストがあるとリスト上の IP アドレスを最大 600 件応答します。monlist の問い合わせ

[3] NTP サーバを踏み台としたリフレクター攻撃（NTP リフレクター攻撃）に対する注意喚起について
http://www.npa.go.jp/cyberpolice/topics/?seq=12892

方と応答の例を図 1 に示します。

```
# ntpdc -c monlist 10.12.0.163
remote address          port local address      count m ver code avgint  lstint
===============================================================================
10.12.0.254               123 10.12.0.163          5139 4 4     180     71      44
10.12.0.102             33024 10.12.0.163             8 3 4     180  45999    6248
10.12.0.170               123 10.12.0.163             1 1 3     180  40689   40689
10.12.0.180               123 10.12.0.163             1 1 3     180 367375  367375
10.12.0.103               123 10.12.0.163            12 3 4     180  30618  367421
10.12.0.165               123 10.12.0.163            12 3 4     180  30619  367434
10.12.0.151               123 10.12.0.163            12 3 4     180  30623  367479
10.12.0.158               123 10.12.0.163            12 3 4     180  30626  367510
10.12.0.110               123 10.12.0.163             1 1 3     180 367558  367558
```

図 1 monlist の応答例

次に DDoS 攻撃を実現させる NTP リフレクター攻撃の概要を図 2 に示します。monlist 機能の性質上、応答パケットのほうがリクエストのパケットよりもサイズが大きくなります。そのため、攻撃者からの比較的少ないデータ量の送信に対し、被害者側では大量のデータ量を受信することになります。

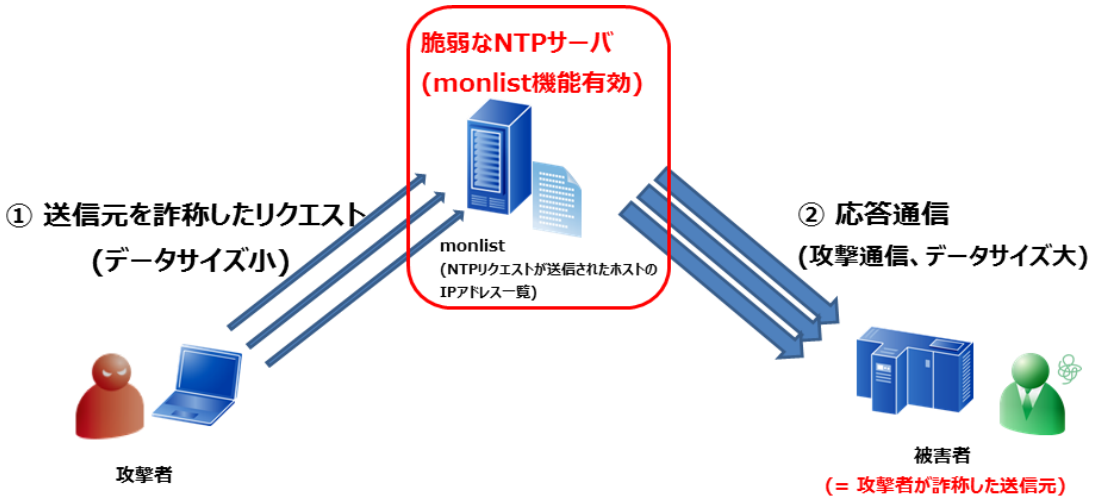


図 2 NTP リフレクター攻撃の概要

さらに、UDP は接続を確立する必要が無く、攻撃者は NTP サーバにリクエストを送信する際、図 2 のように送信元を偽装することができることから、容易に効率的な攻撃を行うことが可能です。

なお、この攻撃が増加したことについては、次の要因が考えられます。

1. DNS リフレクター攻撃の対策が進み、DDoS 攻撃の踏み台となりうるホストが減少した
2. DNS と比較して monlist 機能を悪用したほうが、攻撃パケットの容量が大きくなる可能性が高い
3. 攻撃用スクリプトやツールが 2014 年 1 月頃に公開された (図 3 参照)

```
use threads;
use Socket;

my $num_of_threads = $ARGV[5];
my $target = $ARGV[0];
my $udp_src_port = $ARGV[1];
my $time = $ARGV[2];
#Open Input List.
my $openme = $ARGV[3];

open my $handle, '<', $openme;
chomp(my @servers = <$handle>);
close $handle;

my $ppr = $ARGV[4];
my @threads = initThreads();
print "I guess im attacking $target for $time seconds with $num_of_threads threads¥n";

#Does the list exist?
if (-e $openme) {
print "Using $openme as list.¥n";
}
unless (-e $openme) {
print "List does not exist.¥n";
```

図 3 公開されている攻撃スクリプト

2014 年 2 月には、CDN サービスの CloudFlare を使用しているサイトに向けて、最大 400Gbps ものNTPリフレクター攻撃を検知し、通信遅延や通信障害が生じたと報じられています[4]。また、2013 年の Spamhaus に対する DNS リフレクター攻撃は 30,956 台の DNS サーバを悪用し、最大 300Gbps の通信を発生させたことに対し、今回の攻撃は僅か 4,592 台の NTP サーバで実現していると言われています。

NTP リフレクター攻撃などの DDoS 攻撃は、自身の組織が攻撃対象ではなくとも、管理下にあるサーバや機器が攻撃に悪用された場合、社会的な責任を追及される可能性があります。そうならないためにも、本攻撃に関しては、次の対策を実施することを推奨いたします。

1. NTP サーバを外部へ公開する必要がない場合、ネットワーク機器にて適切にアクセス制御を行う
2. 本脆弱性が修正済みであるバージョン以降の ntpd を適用させる
   2014 年 6 月 28 日時点での修正済みバージョン：ntpd 4.2.7p446(開発版)
3. ntpd の設定を変更し、monlist 機能を無効化する、もしくは monlist 機能が使用できるホストを制限する
4. 組織内から組織外に対し、送信元アドレスを変更したパケットを出さないように制限する[5]

---

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

[5]イングレスフィルタリングとは
https://www.nic.ad.jp/ja/basics/terms/ingress-filtering.html

4.1.2　WordPress サイトにおける Pingback 機能を悪用した DDoS 攻撃ついて

リフレクター攻撃では UDP サービスの悪用以外にも、Web アプリケーションの通常機能が悪用された DDoS 攻撃[6]が行われたことが特徴的でした。2014 年 3 月に、ブログソフトウェア「WordPress」の Pingback 機能が有効となっていた 16 万以上のサイトが DDoS 攻撃の踏み台として悪用されていた、と米セキュリティ会社の Sucuri 社から発表されました。

本攻撃には、WordPress にて利用されている XML-RPC API の 1 つである Pingback 機能が悪用されました。Pingback 機能は、ブログ記事などにリンクを設置したときに、リンク先の Web サイトへリンクしたことを通知し、通知を受けた Web サイトが通知元にリンクが設置されているか確認する仕組みを提供します(図 4 参照)。

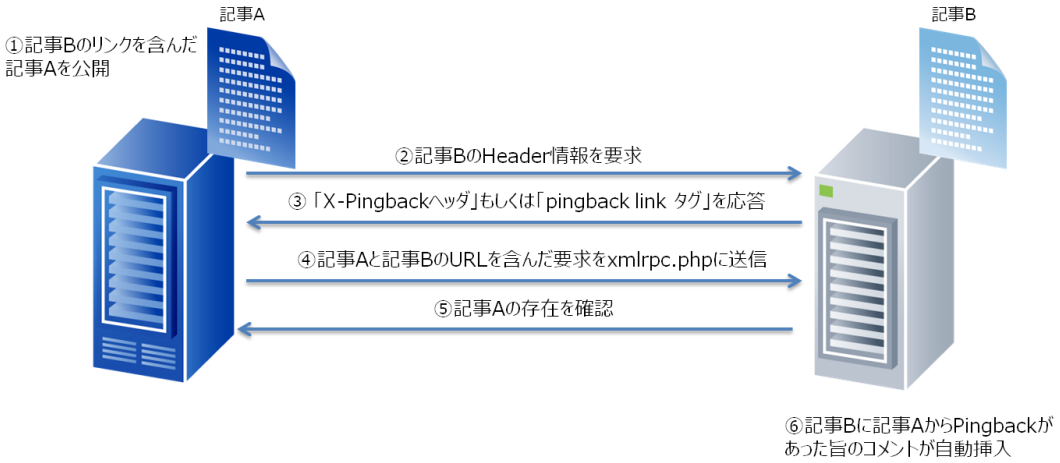


図 4　Pingback 機能が有効なサーバでの通常通信

攻撃者は、本機能が有効な WordPress が動作するホスト上の XML-RPC API(xmlrpc.php)に対して、攻撃対象の URL をリンク元に設定した Pingback のリクエスト(図 5 参照)を送信することで、WordPress を踏み台にした DDoS 攻撃を仕掛けていました。

---

[6] More Than 162,000 WordPress Sites Used for Distributed Denial of Service Attack
http://blog.sucuri.net/2014/03/more-than-162000-wordpress-sites-used-for-distributed-denial-of-service-attack.html

図 5 攻撃者が送信する Pingback リクエスト例

すでに本機能を悪用され、Sucuri 社への攻撃の踏み台となってしまったサイトについては、Sucuri 社が公開しています[7]。ただし、このサイトは最新情報が反映される仕組みではないため、現在でも踏み台となった WordPress が Pingback 機能を有効にしているかどうかを確認できるものではありません。

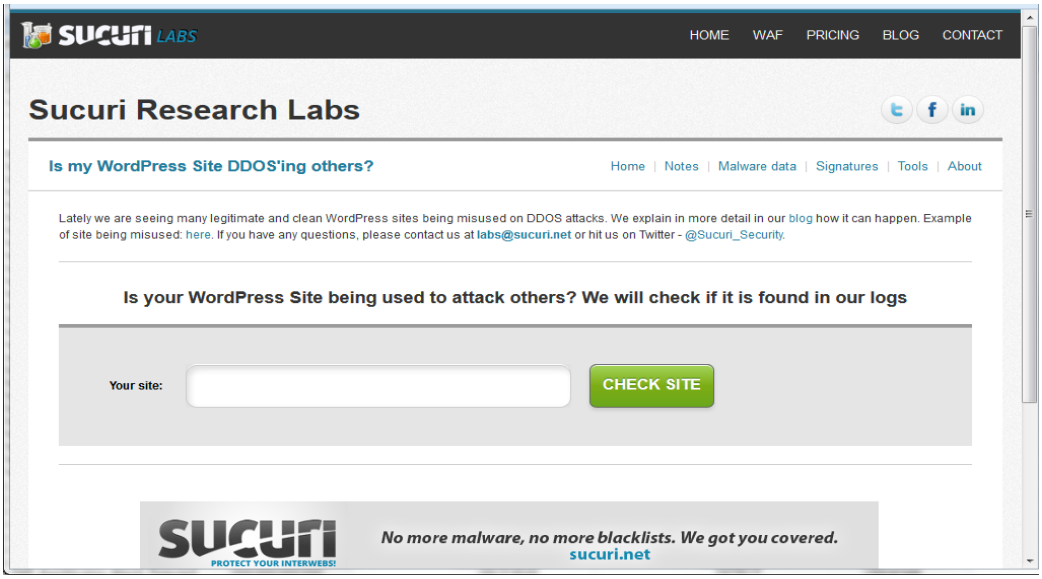


図 6 Sucuri 社に対する攻撃の踏み台となったかを確認できるサイト

[7] Is my WordPress Site DDOS'ing others?
http://labs.sucuri.net/?is-my-wordpress-ddosing

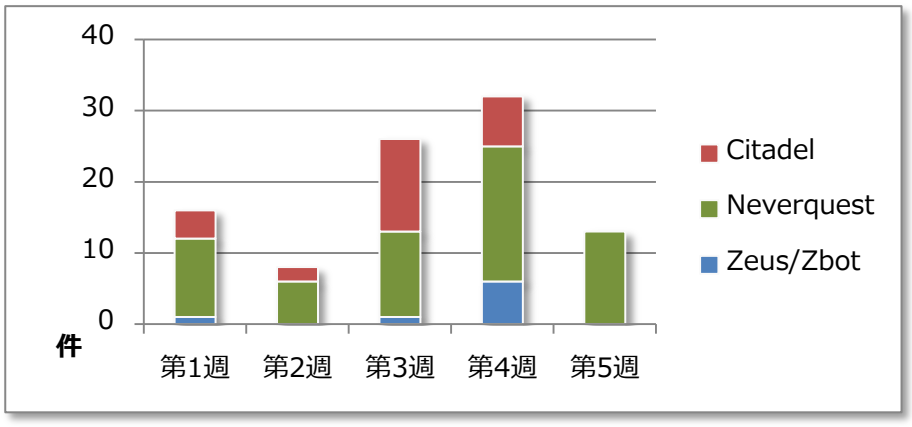
また、ここで取り上げた攻撃手法は、正規の機能を悪用しているため、通常のソフトウェアのアップデートだけでは防ぐことができません。自組織が運用している WordPress が踏み台とならないためにも、以下の対策を実施してください。

1. Pingback 機能が不要である場合、本機能を無効化する、もしくは Pingback 機能を無効化するプラグインを導入する
2. 外部からの不必要な XML-RPC API へのアクセスを制限する
3. 攻撃を行っている送信元からの通信をファイアウィールなどのネットワーク機器で遮断する

4.2 インターネットバンキングのアカウント情報を狙うマルウェアについて

昨年より、銀行口座から預金情報（現金）を窃取する、不正送金被害が急増しています。不正送金被害は、預金者が利用しているパソコンがマルウェアに感染し、パスワードなどを含む口座情報がパソコンから盗み出されることにより発生しています。

そのようなマルウェアとしては、「Zeus/Zbot」、「SpyEye」、「Citadel」 などが代表的ですが、2013 年 11 月末頃から新種として「Neverquest」が、セキュリティ情報サイトやメディアで見られるようになりました。JSOC でも 2 月末より、学術系機関を中心とした複数のお客様にてマルウェアの感染通信を検知しております。グラフ 6 に 2 月末以降に検知した、不正送金に使用されるマルウェアに感染したことによる重要インシデントの件数を示します。



グラフ 6 不正送金に使用されるマルウェア別インシデントの件数推移（2014 年 3 月）

※ 2/28 からのデータです。

4.2.1 Neverquest について

Neverquest に感染すると、利用者がインターネットバンキングサイトにアクセスした際、Web ブラウザに表示されるサイトページを改ざんし、不正なコードを挿入することでログイン情報が盗み出されてしまいます。攻撃者は、VNC（Virtual Network Computing）サーバを利用して感染したホストをリモート制御し、取得したログイン情報を用いることで正規利用者を装って感染ホストからインターネットバンキングサ

イトにログインします。

また、カスペルスキー社とシマンテック社により、Neverquest には、スパムメールやツールキットによって自己複製をする機能がある他、Google、Yahoo、Amazon AWS、Facebook、Twitter、Skype 等のインターネットバンキング以外のサイトにアクセスした際にも、アカウント情報を窃取する機能があると報告されています。[8] [9]

4.2.2 Neverquest の検知事例

JSOC では Neverquest から制御ホスト(C&C サーバ)への通信においては、表 2 に示す 3 つの接続先に集中していることを確認しました。

表 2 Neverquest の制御ホスト（C&C サーバ）接続先

送信先 IP アドレス	所属国
146.185.233.38	ロシア
146.185.233.80	ロシア
185.13.32.80	ロシア

図 7 に Neverquest から制御ホスト（C&C サーバ）に接続するリクエスト例を示します。掲示板サイトへの投稿を模しています。

```
POST /forumdisplay.php?fid=XXXXXXXXX　（省略）
POST /post.aspx?forumID=XXXXXXXXX　（省略）
                                        ※XXXXXXXXX は数字
```

図 7 Neverquest から制御ホスト（C&C サーバ）に接続するリクエスト例

プロキシなどのログで、表 2 の宛先 IP アドレスや図 7 のリクエスト内容のログが見られないかご確認ください。同じ送信元ホストからこれらの IP アドレスや図 7 の 2 つのリクエストの通信が発生している場合は感染の可能性が考えられますため、送信元ホストの詳しい調査を推奨します。

4.2.3 不正送金に使用されるマルウェアの対策について

不正送金の手口は日々巧妙化しております。不正送金に使用されるマルウェアに限らず情報窃取するマルウェアやその他マルウェアへの対策としても、感染防止対策だけに重点を置くのではなく、感染時の対策や対応手順なども併せて事前に準備しておくことが必要です。また、現在実施しているセキュリティ対策について、確認・見直しを継続的に行ってください。

以下に、JSOC が推奨する不正送金に使用されるマルウェア対策のポイントを示します。

---

[8] トロイの木馬 Neverquest：多数の銀行がターゲットに
http://blog.kaspersky.co.jp/neverquest-trojan-built-to-steal-from-hundreds-of-blanks/

[9] オンラインバンキングを狙うトロイの木馬、危険な新種の Neverquest は古い同族の進化形
http://www.symantec.com/connect/ja/blogs/neverquest

■端末の運用

1) OS、アプリケーション、アンチウィルスソフトウェアを最新状態に保つ。
2) EMET[10] 等を導入することにより、ゼロデイ攻撃によるウィルス感染の危険を緩和する。
3) PhishWall のような不正送金対策ソフトを活用する。

■業務運用・心がけ

4) 複数サイトでアカウント情報の使いまわしをしない。パスワード管理ソフトの利用。
5) インターネットの閲覧やメールを受信する端末と、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。
6) 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、手順について確認しておく。
7) 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しておく。

■その他

8) 振込限度額を下げる。

4.3 IoT (Internet of Things) のセキュリティについて

IoT (Internet of Things) は、情報通信機器だけでなく、様々な機器に通信機能を持たせ、インターネットに接続したり相互に通信ができるようになる技術や概念などの総称です。特に近年、家電製品や自動車など多種多様な機器がインターネットにつながるようになってきています。

しかし、その一方でセキュリティの観点で言えば、セキュリティが十分考慮されていない、あるいは不十分で脆弱な機器が多いと考えられます。組み込み機器に関する情報は、メーカ以外には非公開であることも多いため、脆弱性が発見された場合にも、対応が遅れたり、サポートされていなかったりする場合もあります。また、利用者にとっては、使用中の機器がインターネットに接続していることは気付けても脆弱性が存在しているサービスが稼動していたり、悪用されていたりすることに気付くことは困難です。

4.3.1 JSOC におけるインシデント事例

■事例 1

お客様のネットワークより、外部のホストに対して CGI 環境で動作する PHP の脆弱性を悪用する攻撃が発生しました。 該当ホストは Linux 組み込み型の IP カメラが稼動し、PHP の脆弱性が存在していたため、攻撃が成功してワームに感染し、外部への攻撃通信が発生していました。また、IP カメラのメーカ様においても脆弱性や悪用方法について把握されていないようであり、認知度の低さが伺える状況でした。

■事例 2

[10] Enhanced Mitigation Experience Toolkit
http://support.microsoft.com/kb/2458544/ja

お客様環境にて NTP に関する不審な通信を検知し、NTP リフレクター攻撃の踏み台となった可能性があったため調査を依頼したところ、該当のホストはネットワーク機器であり、時刻同期機能を有効にすると、 monlist 機能が有効となった ntpd が起動することが判明しました。さらにそのネットワーク機器がファイアウォールの管理外にあったため、適切なアクセス制御ができず外部から NTP の monlist 機能の参照が可能であり、踏み台となっていました。

4.3.2 組み込み機器のセキュリティ対策について

組み込み機器に対しても脆弱性診断を実施し、脆弱性が存在しないかを確認する必要があります。

IPA (独立行政法人情報処理推進機構) から、「SHODAN」(図 8) という、インターネットに接続する機器を検索できる Web サービスを活用して、自組織のインターネット接続機器を検査する方法と実施すべき対策が公開されています。[11]

図 8 インターネットに接続する機器を検索できるサイト「SHODAN」

一方、攻撃者もログイン等の認証設定が不適切な機器や、脆弱性が残る古いバージョンの機器などを発見するために悪用していると言われています。「SHODAN」の検索キーワードでも、カメラ関連のキーワードが上位を占めており、この中には攻撃者による調査行動も含まれているものと推測しています。

[11] IPA テクニカルウォッチ 「増加するインターネット接続機器の不適切な情報公開とその対策」の公開
https://www.ipa.go.jp/about/technicalwatch/20140227.html

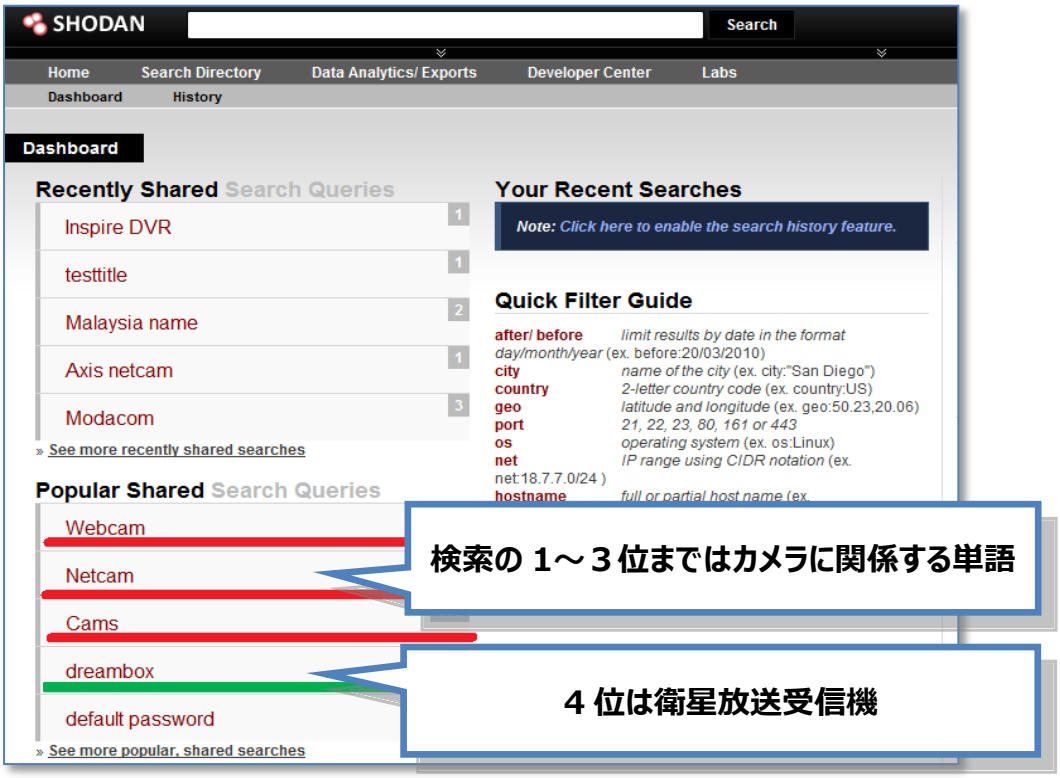


図 9「SHODAN」で多く検索されているキーワード

JSOC においても以前より「SHODAN」を送信元としたポートスキャン通信を日常的に検知しています (表 3)。また、OpenSSL Heartbeat 等の脆弱性をスキャンする通信も確認しています。

表 3「SHODAN」の送信元 IP アドレス

ドメイン名	IP アドレス	割当国
census1.shodan.io	198.20.69.74	米国
census2.shodan.io	198.20.69.98	米国
census3.shodan.io	198.20.70.114	米国
census4.shodan.io	198.20.99.130	米国
census5.shodan.io	93.120.27.62	ルーマニア
census6.shodan.io	66.240.236.119	米国
census7.shodan.io	71.6.135.131	米国
census8.shodan.io	66.240.192.138	米国
census9.shodan.io	71.6.167.142	米国
census10.shodan.io	82.221.105.6	アイスランド
census11.shodan.io	82.221.105.7	アイスランド
census12.shodan.io	71.6.165.200	米国
census13.shodan.io	24.73.251.74	米国

SHODAN を使えば誰にでも容易に情報が得られてしまうため、自組織のインターネット接続機器を意図せず公開していないか早急に調査し、万が一存在した場合は、設定変更や通信制御など適切な対処を取ることを推奨します。

4.4 Apache Struts の脆弱性を悪用した攻撃について

2014 年 4 月 17 日に IPA より、Apache Struts 2 の脆弱性についての注意喚起が公開されました。Apache Struts 2.3.16.1 以前のバージョンに対して、ClassLoader をリモートから操作できるという脆弱性です。

その後、Apache Struts 2.3.16.2 に対策漏れ[12]や CookieInterceptor を利用して ClassLoader が操作できる脆弱性が指摘され、最終的に Apache Struts 2.3.16.3 で脆弱性が修正されています。

また、2013 年 4 月 5 日でサポートが終了している Struts 1 においても同様の脆弱性が存在することが確認されています[13]。JSOC では過去にも Apache Struts 2 に対する脆弱性についてレポートを公開[14]していますが、今回の脆弱性も以前のレポートで取り上げた脆弱性(S2-016)と同様に影響が大きいと考えています。

表 4 Apache Struts の脆弱性(S2-020～S2-022)の概要

脆弱性を悪用された場合の影響	➢ Web アプリケーションの動作権限内で情報の窃取や特定ファイルの操作 ➢ DoS ➢ 攻撃者が操作したファイルに Java コードが含まれている場合、任意のコードが実行される可能性
対象バージョン	Struts 2.0.0 – Struts 2.3.16.2
脆弱性の解消バージョン	Struts 2.3.16.3
該当する脆弱性の Apache Struts Advisory および共通脆弱性識別子(CVE)	S2-020 - CVE-2014-0094 S2-021 - CVE-2014-0112, CVE-2014-0113 S2-022 - CVE-2014-0116
参考 URL	Apache Struts 2 Documentation http://struts.apache.org/release/2.3.x/docs/s2-020.html http://struts.apache.org/release/2.3.x/docs/s2-021.html http://struts.apache.org/release/2.3.x/docs/s2-022.html

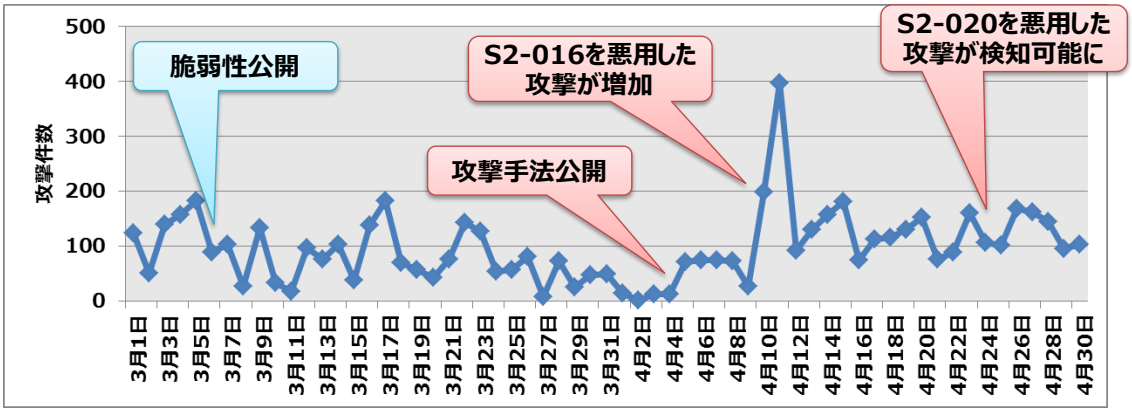
Apache Strutsの脆弱性を悪用した攻撃は増減はあるものの定常的に行われていることから、既にターゲットとして定着していることが伺えます。実際に、S2-20 の脆弱性を悪用した攻撃の検知に対応した

[12] Apache Struts2（2.3.16、S2-020 の修正版）に対するゼロディを弊社エンジニアが発見いたしました。
http://www.mbsd.jp/news20140422.html

[13] 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

[14] 【JSOC 侵入傾向分析レポート vol.19】および【JSOC INSIGHT vol.3】

オリジナルシグネチャを適用したところ、S2-20 の脆弱性を悪用した攻撃の増加を確認しました。



グラフ 7 Apache Struts の脆弱性を悪用した攻撃件数の推移

今回の脆弱性の情報は IPA による注意喚起が発表された 4 月 17 日より以前から、中国では脆弱性実証コードを含めて情報が公開(図 10)されていました。

図 10 中国の S2-020 に対する脆弱性情報

S2-020 の脆弱性が存在する Apache Struts2 が稼働しているサーバに対し、以下の文字列を送信することで、任意の ClassLoader を操作することができます。

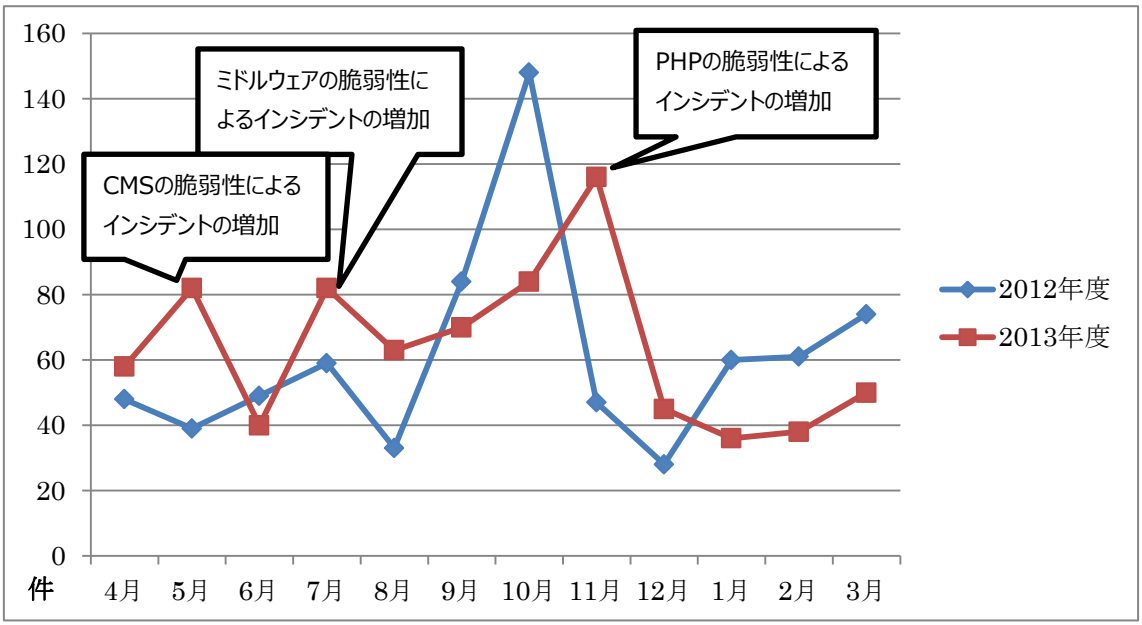
http://(Struts2 が稼働するサーバ)/example.action?class.classLoader.(操作したい属性)

根本的な対策として、当該脆弱性が修正された Apache Struts 2.3.16.3(2014 年 5 月 14 日現在最新)以降のバージョンにアップデートすることを推奨いたします。また、Apache Struts 1.x 系に関しましては、サポートが終了していることから公式サイトからの修正バージョンの公開は未定ですので、1.x 系の保守サービスを提供しているベンダによる個別サポートを利用するか、以下に挙げる緩和策の実施をご検討ください。

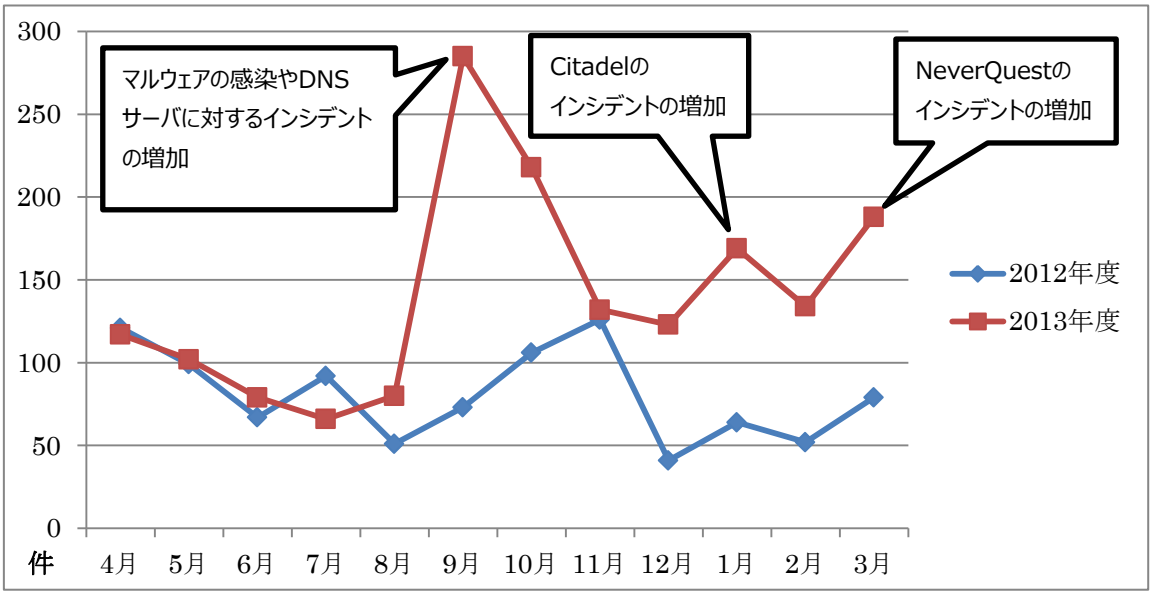
- リクエストを拒否するフィルタ機能を実装する。なお、設定する内容については利用しているアプリケーションによりますので保守ベンダにお問い合わせください。
- WAF、IPS などネットワーク側で当該攻撃を遮断する。

5.1　2013 年度を振り返って

2013 年度に発生した主なインシデントは以下のグラフ 8、9 のとおりです。これらのインシデントについて JSOC で観測した内容を元に振り返ります。



グラフ 8 インターネットからのインシデント推移



グラフ 9 内部からのインシデント推移

※DNS サーバや NTP サーバを踏み台とし、お客様の内部ネットワークから通信が発生したインシデントは内部に分類しています。

5.2 Web サイトへの攻撃

JSOC で 2013 年度に観測した特徴的な Web への攻撃を表 5 にまとめました。脆弱性や脅威は攻撃者がいる限り決してなくなることはありません。そのため、インターネットを使う限りは継続して対応していく必要があります。

Apache Struts 2 のような Web アプリケーションフレームワークは、フレームワーク上で動作している既存の Web アプリケーションとの互換性の問題があり、容易にバージョンアップができないこと、オープンソースであり未知の脆弱性が発見された際に応用がされやすいことから、今後も攻撃者に狙われる可能性が高いと考えます。

表 5 Web サイトへの攻撃インシデントまとめ

No.	検知内容	概要	時期
1	Darkleech Apache Module に感染した Web サーバからの不正なサイトへ誘導するコードが埋め込まれたレスポンス	Blackhole Exploit Kit が仕掛けられた不正なサイトへ誘導しマルウェアをダウンロードさせ感染させる。	2013 年 4 月から
2	Joomla!などの CMS の脆弱性を利用した改ざん	HTML や PHP を改ざんし Javascript を埋め込む	年間を通して
3	Apache Struts 2.x 系の脆弱性を利用した任意のコマンド実行の試み	S2-016 の脆弱性情報公開翌日から攻撃件数、重要インシデント件数が増加。バックドアの設置。	2013 年 7 月から
4	CGI 環境で動作する PHP の脆弱性を利用した情報の閲覧、任意のコマンド実行の試み	Bitcoin を得るために IRC Bot 化および Bitcoin Miner が実行される。	2013 年 10 月から
5	Apache Struts 2.x 系、Apache Struts 1.x 系の脆弱性を利用した任意のコマンド実行の試み	サポートが終了している Struts1 にも影響が確認される。	2014 年 4 月から
6	PUT メソッドを悪用したファイルのアップロード	PUT メソッドが有効になっていたため、攻撃者が攻撃準備として txt ファイルのアップロード実施。	年間を通して

5.3　標的型攻撃

標的型攻撃については新たに 2 種類の特徴的な手法を確認しました。

ひとつは、2012 年に国外で話題になった水飲み場型攻撃が、日本国内においても明示的に行われている事例[15]が確認されたことです。水飲み場型攻撃とは、水飲み場に集まる動物を狙う猛獣の攻撃になぞらえ、攻撃対象とするユーザーが普段アクセスする Web サイト（水飲み場）に罠をしかけ、サイトを閲覧しただけでマルウェアに感染させる攻撃手法です。

改ざんされた Web サイトにアクセスしたユーザーを事前に設定したアクセスリストに基づいて選別を行い、特定の IP アドレス帯からアクセスしたユーザーのみに攻撃を行っていました。また、攻撃コードとして IE のゼロデイ(CVE-2013-3893、MS13-080 にて修正)が使用されていました。これらの点から攻撃者は計画的に攻撃準備を行っていたものと考えます。

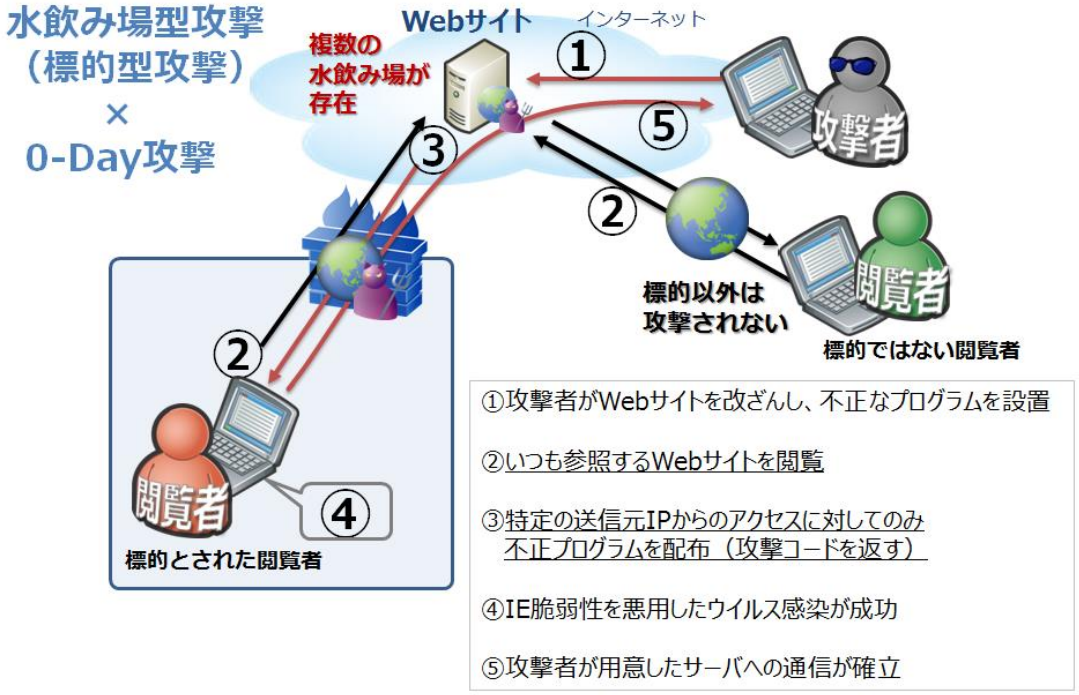


図 11 水飲み場型攻撃の仕組み

もうひとつは、正規のソフトウェアのアップデートを装いマルウェアに感染させる事例[16]が確認されたことです。これは、正規のアップデートサーバのコンテンツが改ざんされた事により、ソフトウェアアップデートのプロセスが

[15] 日本における水飲み場型攻撃に関する注意喚起
http://www.lac.co.jp/security/alert/2013/10/09_alert_01.html

[16] 正規のソフトウェアのアップデートで、不正なプログラムが実行される事案について
http://www.lac.co.jp/security/alert/2014/01/23_alert_01.html

実行されたときに本来のアップデートサーバではなく、攻撃者が用意した別のサーバへ転送され、マルウェアをダウンロードし、感染させられてしまうという手法でした。

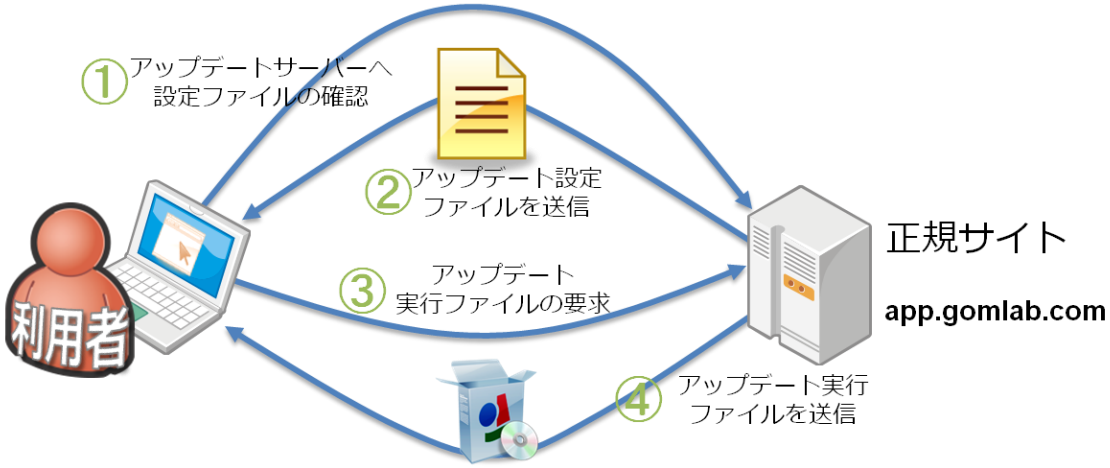


図 12 正常なアップデートの流れ

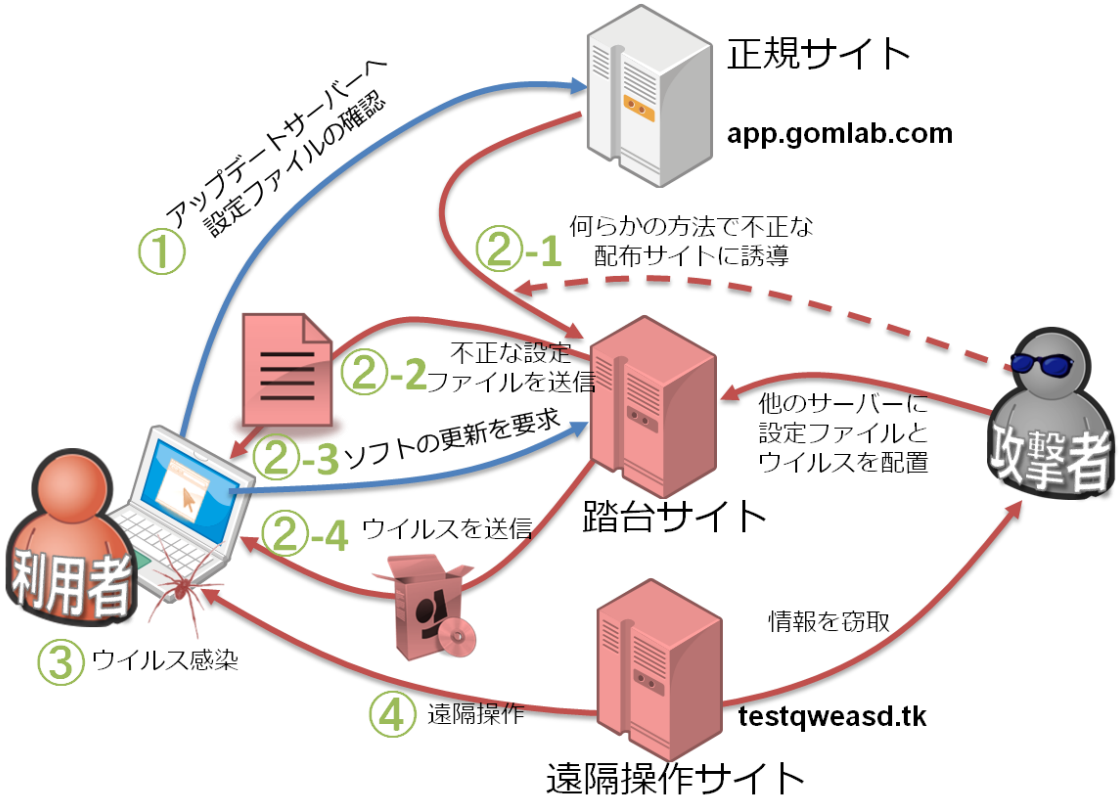


図 13 正常ではないアップデートによるマルウェア感染の流れ

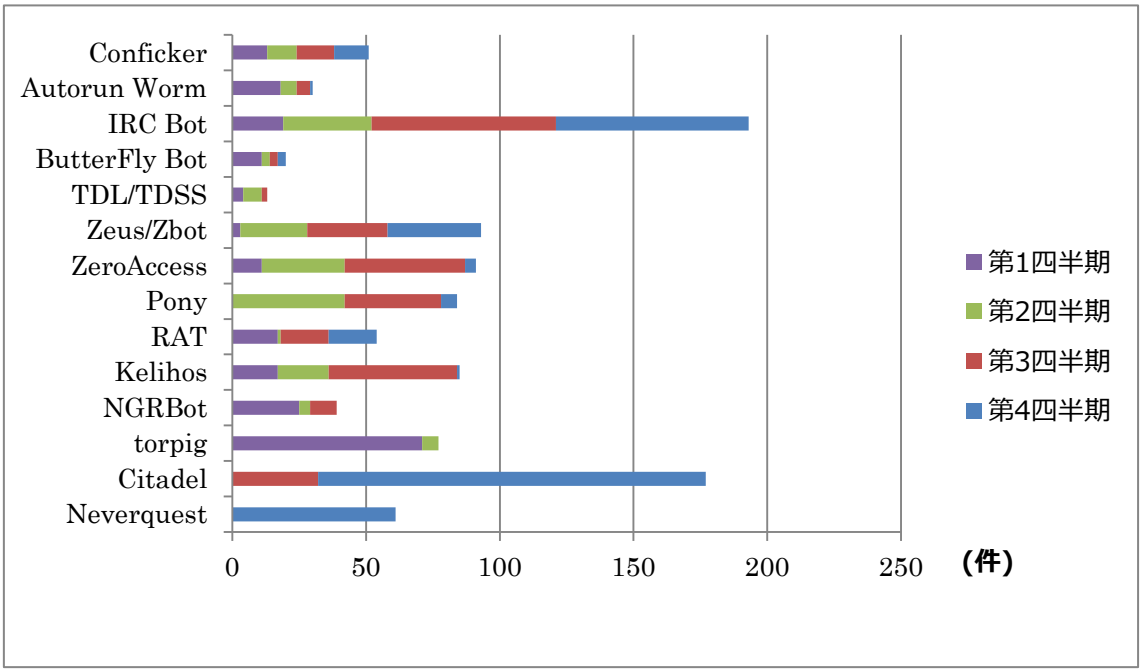
脆弱性情報は一般に公開されていないもの(ゼロデイ)を含め、闇サイトなどで売買されていることを確認していますが、ここで取り上げた水飲み場型攻撃で使用された攻撃コードについても、国外の事例で使用された攻撃コードと非常に似通っているため、同一の製作者から販売された攻撃コードであると推測しています。また、攻撃者は改ざんした Web サイトにてアクセス制御を行い、標的の絞込みを行っていることが確認していますが、これは攻撃自体の発覚を遅らせ、セキュリティベンダなどに攻撃手法を解析されないようにし、より長く攻撃コードを使用し続けることを目的としているためであると考えます。

水飲み場への罠の設置、攻撃を確実に成功させるためにゼロデイを使用、標的を限定するためのアクセス制御といった水飲み場型攻撃の手法は 2014 年も継続して注視する必要があると考えます。

5.4 マルウェアの動向

年間を通して torpig、ZeroAccess、Kelihos、IRCBot 等のボットネットの通信を多数確認しました。Darkleech Apache Module により、Blackhole Exploit Kit が仕掛けられた不正なサイトに誘導された結果、アカウント情報を搾取するマルウェアである Pony に感染させられた事例を確認しました。さらに、不正送金ウイルスである Zeus/Zbot、Citadel、Neverquest の検知数も増加しております。

日本は、消費者保護が行き届いていることから、消費者サイドの警戒心が薄い反面、経済水準が高く取引額も多いことから、市場としても魅力が高いため国内外の犯罪者から狙われているようです。2014 年度もこのような傾向は続くと考えられ、警戒が必要であると考えます。



グラフ 10 主なマルウェア感染の四半期別インシデント件数

5.5 UDP サービスを悪用した攻撃の増加

2013 年 7 月頃より DNS リフレクター攻撃の準備行為として、再帰問い合わせを許可している DNS サーバの探索行為を確認しておりました。9 月頃より、DNS リフレクター攻撃の検知が増加しはじめ、実際に監視対象ホストが踏み台として悪用された事例を確認しました。さらに、監視対象ホストへ大量のリクエストを送信された事が原因で監視対象ホスト自体がサービス不能状態になった事例も確認しました。また、同じ UDP を使用する NTP の monlist 機能を悪用した新たなリフレクター攻撃についての情報が公開され、実際に悪用された事例が確認しました。その他、Chargen を悪用するケースも見られています。お客様による対応が進んだことにより攻撃の成功割合は徐々に減少しましたが、今後、DNS や NTP、Chargen 以外の UDP のサービスを悪用した同様の攻撃が発生する可能性があります。

6　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.4

【執筆】

影山 徹哉 / 髙井 悠輔 / 内藤 伊里 / 松本 隆志 / 門田 昌也

(五十音順)