LAC


# JSOC INSIGHT

## vol.2

2013年11月6日

JSOC Analysis Team

JAPAN SECURITY OPERATION CENTER

JAPAN SECURITY OPERATION CENTER

# JSOC INSIGHT

## 1　はじめに

JSOC（Japan Security Operation Center）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】**

2013 年 7 月 1 日 ～ 2013 年 9 月 30 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

本レポートでは、インシデント傾向の分析に加え、JSOC が観測した事例から、特に注目すべき脅威をピックアップしてご紹介します。

本レポート内にて取り上げている内容を含め、近年セキュリティインシデントが高度化しているとの報道がされる一方、JSOC では基本的な対策が行われていれば防ぐことができたインシデントも多く観測されています。ゼロデイ脆弱性のような新しい脅威への対策も重要ですが、アクセス制御や設定情報の管理といった基本的対策の徹底が、改めて最も重要な対策であると考えます。

### ➢ 「ミドルウェアの脆弱性を狙う攻撃」の一時的な急増および増加傾向の継続

ミドルウェアに対する攻撃が増加傾向にある中、とりわけ前回のレポート[1]において取り上げた Apache Struts2 の脆弱性「S2-016」を悪用した、不正なコード実行を目的とした通信を多く検知しました。JSOC では脆弱性公開直後からこの脆弱性を悪用した攻撃が発生していたことをいち早く確認しています。また脆弱性公開直後には、複数のお客様において実際に攻撃されていた事例も確認し、検知後には対処を促しています。

### ➢ 「Web サイト閲覧により感染するマルウェア」の被害拡大

ネットバンキングを悪用し不正送金を行うマルウェアとして昨年より大きな話題となっている「Zeus（Zbot）」や、感染ホスト内に保存されたアカウント情報を窃取する「PONY」といったマルウェアへの感染事例が増加しています。これらは、不正に改ざんされた Web サイトへアクセスした際にマルウェアを感染させる、「ドライブバイダウンロード」攻撃によって被害が拡大していると考えます。

### ➢ 日本国内における、ゼロデイ脆弱性を悪用した「水飲み場型攻撃」が発生

JSOC および緊急対応チーム「サイバー救急センター」は日本国内において、水飲み場型攻撃が行われたことを確認しました。また、この攻撃は Internet Explorer におけるゼロデイ脆弱性を悪用するものであることが判明したため、弊社から Microsoft 社へ非公開での情報提供を行いました。該当の脆弱性は 10 月に MS13-080 として修正が行われています。

### ➢ オープンリゾルバを悪用する「DNS アンプ攻撃」が行われる

９月上旬より、再帰問い合わせを許可しているDNSキャッシュサーバ（オープンリゾルバ）を悪用した 、DNSアンプ攻撃の通信を多数検知しています。JSOCでは以前よりDNSアンプ攻撃の準備行為と考えられる不審な DNS の通信を検知していましたが、9 月に入り、実際に多数の攻撃と被害事例を確認しています。

---

[1] JSOC INSIGHT vol.1
http://www.lac.co.jp/security/report/2013/08/08_jsoc_01.html

## 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

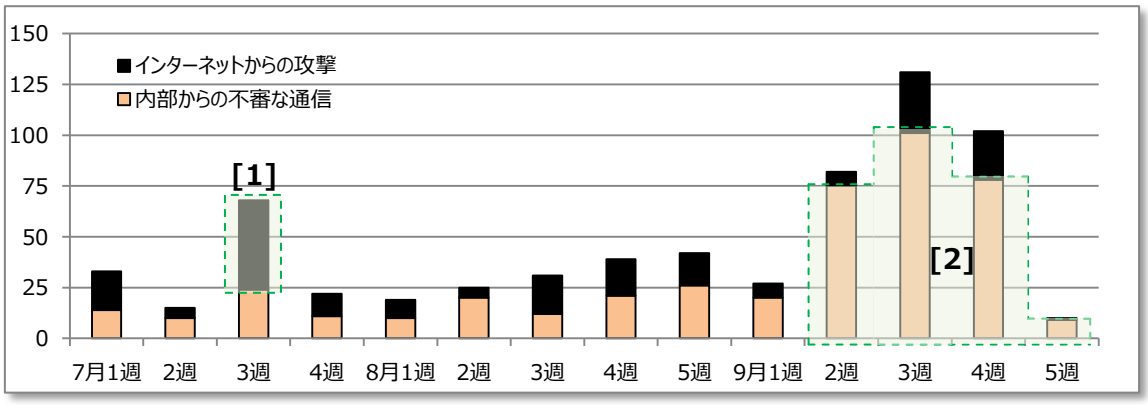
JSOC では、IDS/IPS、ファイアウォールで発生したログをセキュリティアナリストが分析し、検知した内容と監視対象への影響度に応じて 4 段階のインシデント重要度を決定しています。このうち、Emergency、Critical に該当するインシデントは、攻撃の成功や被害が発生している可能性が高いと判断される重要なインシデントです。

**表 1 インシデントの重要度と内容**

| 分類 | 重要度 | インシデント内容 |
|---|---|---|
| 重要インシデント | Emergency | 攻撃成功を確認したインシデント |
| | Critical | 攻撃成功の可能性が高いインシデント、攻撃失敗が確認できないインシデント<br>マルウェア感染を示すインシデント |
| 参考インシデント | Warning | 攻撃失敗を確認したインシデント |
| | 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、重要インシデント件数の推移と攻撃の種類の内訳を示したものです。

7 月 3 週に重要インシデントとして、外部からの攻撃（グラフ 1-[1]）、9 月 2～5 週には内部からの不審な通信を検知したインシデント件数（グラフ 1-[2]）が増加しました。

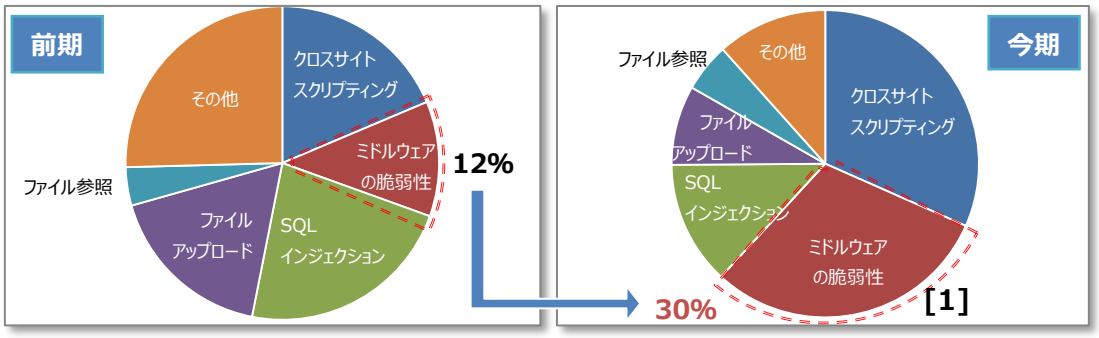



※ 9 月 5 週は 1 日分のデータです

**グラフ 1 重要インシデントの検知件数推移（2013 年 7 月～9 月）**

## 3.2　重要インシデントの検知傾向に関する分析

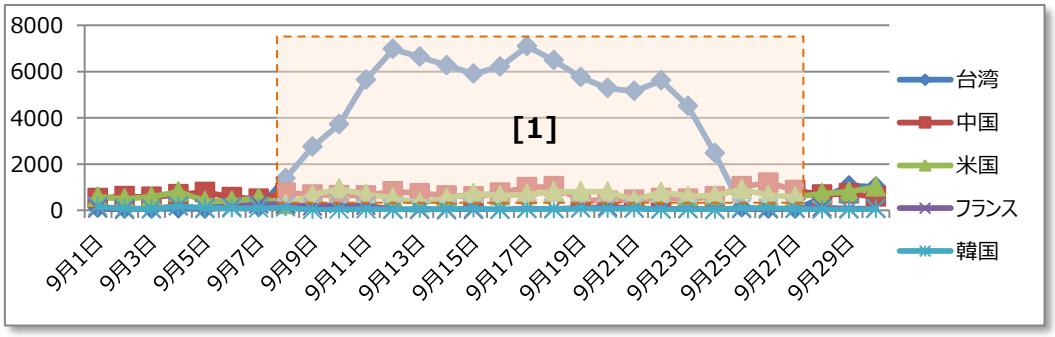
インターネットからの攻撃による重要インシデントでは、7 月 3 週にインターネットからの重要インシデント件数が増加しています。これはミドルウェアの脆弱性を狙った攻撃の増加によるものです。（グラフ 2.b - [1]）特に Apache Struts2 に存在するリモートコード実行の脆弱性（S02-016）の公開直後、本脆弱性を悪用した攻撃が急増しています。一部のお客様では実際に脆弱性が存在し、任意コード実行が可能であったことを確認しています。お客様側の対策が進んだこともあり、2013 年 10 月現在、重要インシデントの検知件数は減少しています。




**a. 2013 年 4～6 月**　　**b. 2013 年 7～9 月**

**グラフ 2　インターネットからの攻撃によるインシデントの内訳**

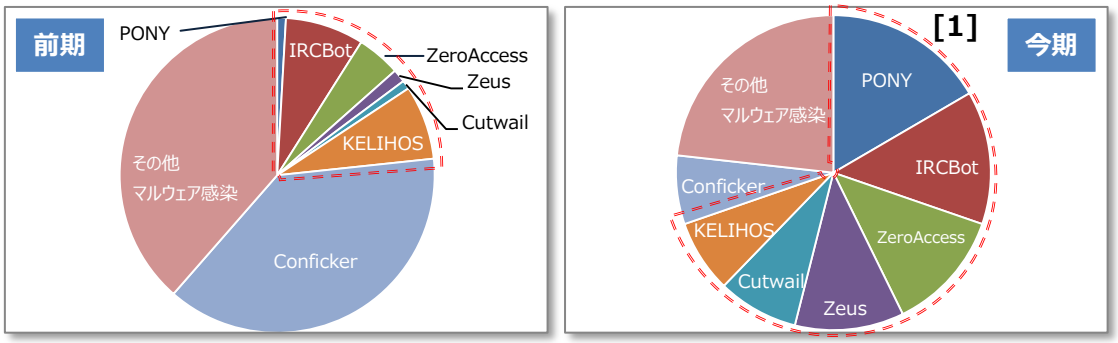
9 月 18 日は満州事変の発端となった柳条湖事件が起きた日であることから、例年その前後に主に中国からの攻撃通信が増加します[2]。本年は、9 月 9 日以降に台湾からの攻撃通信が増加しましたが、これは Web サーバに対して第三者中継を試み、特定プロバイダのメールアドレスに対してスパムメールを送信する攻撃（グラフ 3 - [1]）でした。JSOC の監視している範囲においては、この通信によるメール送信は全て失敗していることを確認しています。その他、中国を送信元とする攻撃の検知傾向に特筆すべき変化はありませんでした。




**グラフ 3　国別の攻撃通信の検知件数推移（2013 年 9 月）**

[2] 9 月 18 日に関連したサイバー攻撃に関しての注意喚起
http://www.lac.co.jp/security/alert/2013/09/12_alert_01.html

内部からの重要インシデントのうち、マルウェア感染の傾向については、昨年より大きな話題となっている不正送金を行うマルウェア、Zeus（Zbot）への感染通信の検知件数が増加しています。また、Zeusと同様に改ざんされたWebサイトを閲覧することによって感染するマルウェアであるPONY[3]やZeroAccessといったマルウェアへの感染通信の検知件数が増加しました。（グラフ4.b - [1]）

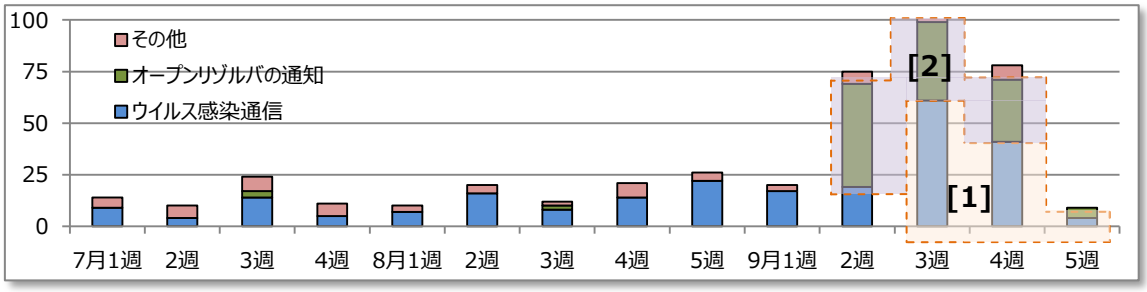



**a. 2013年4～6月**　　**b. 2013年7～9月**

**グラフ 4　マルウェア感染インシデントの内訳**

特に9月3週目以降、マルウェアに感染した通信による重要インシデントが増加しており、複数のお客様のホストにおいて、数種類のマルウェア感染インシデントが発生しています。（グラフ5 - [1]）

また、9月の2週目より内部のホストから多数の不審なDNS応答通信を検知したことによる重要インシデントが増加しています。これらの通信は、お客様のネットワーク内部に存在する、外部からの再帰問い合わせ可能なDNSサーバやネットワーク機器（オープンリゾルバ）がDNSアンプ攻撃に悪用されているものと考えます。（グラフ5 - [2]）本通信については4.2章にて詳細に解説をいたします。




**グラフ 5　内部から発生したCriticalインシデント検知件数推移**

[3] JSOC INSIGHT vol.1
http://www.lac.co.jp/security/report/2013/08/08_jsoc_01.html

## 4　今号のトピックス

### 4.1　日本における水飲み場型攻撃および攻撃に用いられた IE のゼロデイ脆弱性について

#### 4.1.1　ゼロデイ脆弱性を用いた攻撃の発見、脆弱性概要について

JSOC および、弊社緊急対応チーム「サイバー救急センター」は、8 月から 9 月にかけ、Internet Explorer（以下 IE）に存在するゼロデイ脆弱性[4]（Microsoft 社が 10 月 9 日に公開したセキュリティ更新プログラムにより修正済み）を悪用した攻撃、およびそれに関連したマルウェアによる被害が、実環境において発生していることを確認しました。

```
for (i=0;i<10000;i++) {
vault.push(document.createElement("div"));
vault[i].setAttribute("title",str);
}
for (i=5000;i<10000;i++) {
vault[i].setAttribute("title","");
}
CollectGarbage();
    var id_0 = document.createElement("sup");
    var id_1 = document.createElement("audio");
    document.body.appendChild(id_0);
    document.body.appendChild(id_1);
    id_1.applyElement(id_0);
    id_0.onlosecapture=function(e){document.write("");
initit();
var tile=new Array();
for (i=0;i<10000;i++) {
tile.push(document.createElement("div"));
tile[i].setAttribute("title",str);
}
}
    id_0['outerText']="";
    id_0.setCapture();
    id_1.setCapture();
    CollectGarbage();
    DisplayInfo(1);
    location.href=location.href;
}

    window.setTimeout("myonload()",3000);
```

**図 1　脆弱性を悪用する攻撃コードの一部**

この脆弱性は、IE バージョン 6 から 11 に至るまで多くのバージョンの IE が影響を受けるもので、ユーザが IE を使用して攻撃者が用意した不正なスクリプトなどを含む Web コンテンツへアクセスした際に、任意のコードが実行される危険な脆弱性です。このような脆弱性を悪用する攻撃手法は、以前日本国内で多数の感染が確認された Gumblar などと同じ、ドライブバイダウンロード攻撃として知られています。

[4] セキュリティパッチなどが存在しない、未修正の状態である脆弱性

**表 2 脆弱性概要**

| | |
|---|---|
| 脆弱性番号: | CVE-2013-3893 |
| 対象ソフトウェアバージョン: | Internet Explorer 6 から Internet Explorer 11 |
| 脆弱性を悪用された場合の影響: | Internet Explorer がメモリ内のオブジェクトに不適切にアクセスする場合に、リモートでコードが実行される |
| 脆弱性を解消する方法: | MS13-080 の適用 |
| 脆弱性の影響を回避する方法: | Fix it を適用する<br>http://support.microsoft.com/kb/2887505/ja<br>Enhanced Mitigation Experience Toolkit を使用する<br>http://support.microsoft.com/kb/2458544/ja |
| 参考 URL: | Internet Explorer 用の累積的なセキュリティ更新プログラム （2879017）<br>http://technet.microsoft.com/ja-jp/security/bulletin/ms13-080<br>CVE-2013-3893<br>http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3893 |

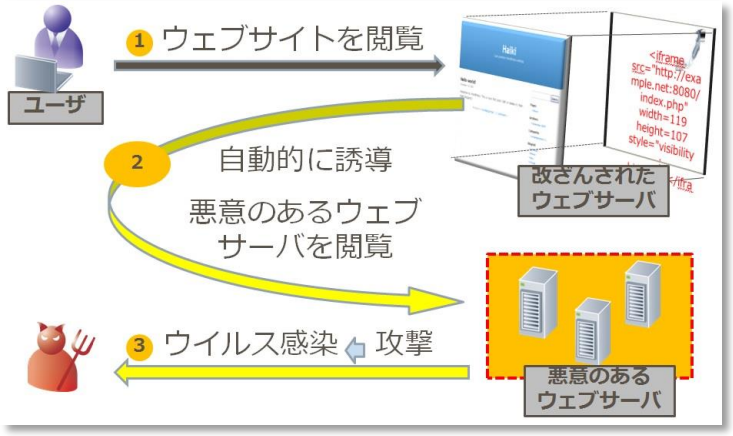


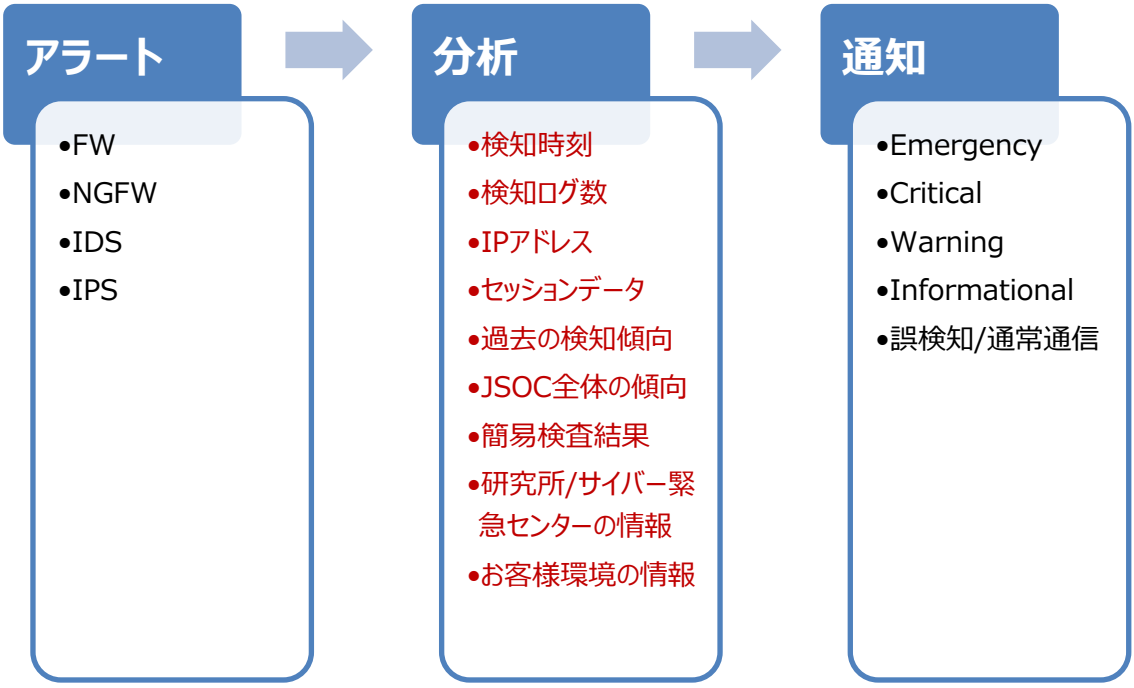

**図 2 ドライブバイダウンロード攻撃の例**

8 月から 9 月にかけてサイバー救急センターでは、Web 改ざんやマルウェア感染に関する複数の支援要請を受けました。これらの被害状況の調査・突合せが行われた結果、一連の攻撃は特定組織を標的としたドライブバイダウンロード攻撃であり、さらに IE に存在するゼロデイ脆弱性を悪用したものであることが判明しました。

また、JSOC では上記の脆弱性を用いた攻撃により生じたマルウェア感染によるものと考えられる通信を検知し、重要インシデントとしてお客様へ報告しています。

被害が生じた 8 月および 9 月当時において、該当の脆弱性は存在自体が未知であったため、JSOC が監視する IDS・IPS では該当の脆弱性を悪用する攻撃検知を目的としたシグネチャや、攻撃の被害によって生じるマルウェア感染通信を検知するシグネチャは存在しませんでした。

しかし、JSOC セキュリティアナリストが監視対象ネットワーク内で検知された通信を総合的に分析した結果、お客様のホストより通常とは異なる検知傾向の通信が発生していることを確認、送信元ホストが何らかのマルウェアに感染している可能性があると判断し、お客様へ緊急にて重要インシデントの連絡を行いました。




上記、分析の全ての要素を用いて、セキュリティアナリストが総合的に影響度判断を行う

**図 3 JSOC における分析の流れとその要素**

サイバー救急センターによる調査・解析、また JSOC によるマルウェア通信の検知・報告により、この脆弱性を悪用した攻撃の一連のシナリオが明らかになりました。また該当の脆弱性は当時 Microsoft 社によるセキュリティパッチや回避策が存在しない、ゼロデイ脆弱性であることが判明したことから、弊社より、Microsoft 社へ非公開にて情報提供を行いました。

該当の脆弱性は 2013 年 10 月、Microsoft 社のセキュリティアップデート MS13-080[5]において、修正が行われています。

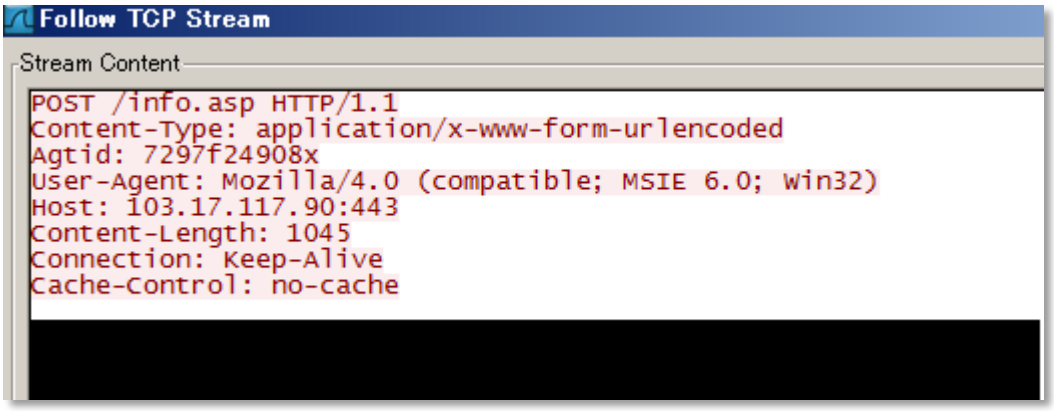
---

[5]マイクロソフト セキュリティ情報 MS13-080 - 緊急
Internet Explorer 用の累積的なセキュリティ更新プログラム（2879017）
http://technet.microsoft.com/ja-jp/security/bulletin/ms13-080

JSOC ではこの脆弱性を用いた攻撃が深刻な影響を及ぼすと判断し、該当の脆弱性を悪用した攻撃を検知するオリジナルシグネチャを早期に作成しました。該当のオリジナルシグネチャは、Microsoft 社によるセキュリティアップデートリリース前の 9 月中旬より、JSOC の監視サービスをご利用されているお客様の IDS・IPS へ順次適用を行っています。

**表 3 今回の攻撃に関連する JSOC オリジナルシグネチャ対応状況について**

| | |
|---|---|
| 対象デバイス: | McAfee Network Security Platform<br>Cisco IDS/IPS<br>Sourcefire 3D System |
| CVE-2013-3893 を悪用した攻撃を検知するシグネチャ | 計 4 パターンを適用 |
| 上記攻撃で感染するマルウェアによる通信を検知するシグネチャ | 1 パターンを適用 |




この通信は送信先ポートが 443/tcp（https）でありながら、通信は暗号化されていない

**図 4 攻撃によって感染するマルウェアが発生させる通信の例**

サイバー救急センターの調査および JSOC の検知事例より、攻撃成功後のマルウェア感染後の通信は図 4 の通信を含め複数種類の通信が発生することを確認しています。

また、通信の送信先は中国（香港）および韓国の複数の IP アドレスであることを確認しています。

**表 4 マルウェアによる通信の送信先の例**

| 中国（香港） | 韓国 |
|---|---|
| 111.118.21.105 | 103.17.117.90 |
| 180.150.228.10 | 210.176.3.130 |
| 211.47.206.113 | |
| 218.38.28.96 | |
| 218.38.28.99 | |

**※送信先はあくまで弊社が確認した限りのものとなります。送信先は攻撃者によって変更される可能性があります**

### 4.1.2　特定企業を対象とした Web 改ざん攻撃（水飲み場型攻撃）について

今回の攻撃は、攻撃対象が無差別である通常のドライブバイダウンロード攻撃とは異なり、改ざんされたサイトに対して一部の企業・組織からアクセスが行われた場合にのみ攻撃が実行されるよう、攻撃対象の制御が行われていました。

このような特定組織・企業を狙ったドライブバイダウンロード攻撃は**「水飲み場型攻撃」**という名称で呼ばれています。近年、同様の攻撃が世界的に行われていることが確認されていますが、今回のインシデントによって、日本においても水飲み場型攻撃が行われている事例が明確に確認された形となりました。

今回の水飲み場型攻撃の大きな特徴は以下のような点が挙げられます。

**【今回確認された水飲み場型攻撃の特徴】**

- 特定の企業・組織を狙った攻撃であり、標的企業・組織がアクセスする可能性の高い Web サイト（=水飲み場）を改ざんしたうえで、標的がアクセスするのを待つ
- 今回は、上記に加え改ざんしたサイトに埋め込まれる攻撃コードにゼロデイ脆弱性が悪用されていた

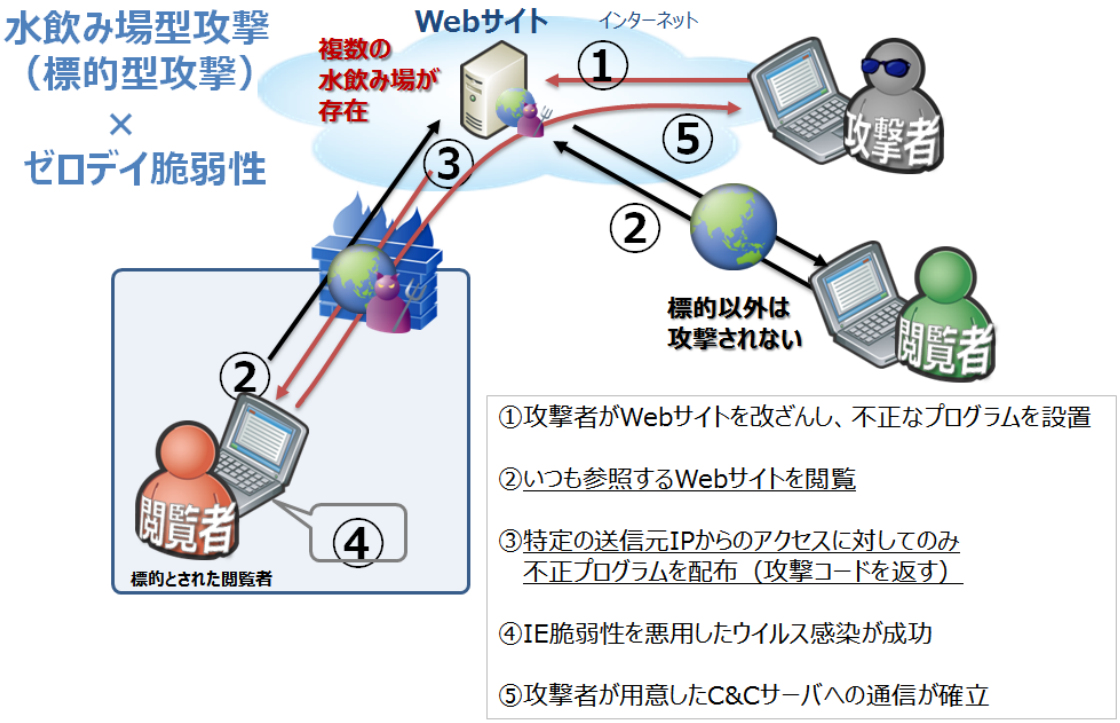



**図 5 今回確認された水飲み場型攻撃の仕組み**

**表 5 改ざんされた Web サイトおよび攻撃対象組織の特徴**

| | |
|---|---|
| 改ざん被害サイト: | 特定のユーザを対象とした情報提供サイト |
| 攻撃対象: | 官公庁、重要インフラ企業など |

今回の一連のインシデントにおいては、改ざん被害サイトは攻撃対象となった一部の組織から頻繁にアクセスされるサイトである、という情報がインターネット上で確認できる状態となっていました。そのため、攻撃者は、これらの情報から改ざん被害サイトを攻撃のための「水飲み場」として選定した可能性があります。

今回の攻撃では、以下のようなコードを用いて、特定組織・企業の IP アドレスからアクセスがあった場合にのみ攻撃が行われるようになっていたことを確認しています。

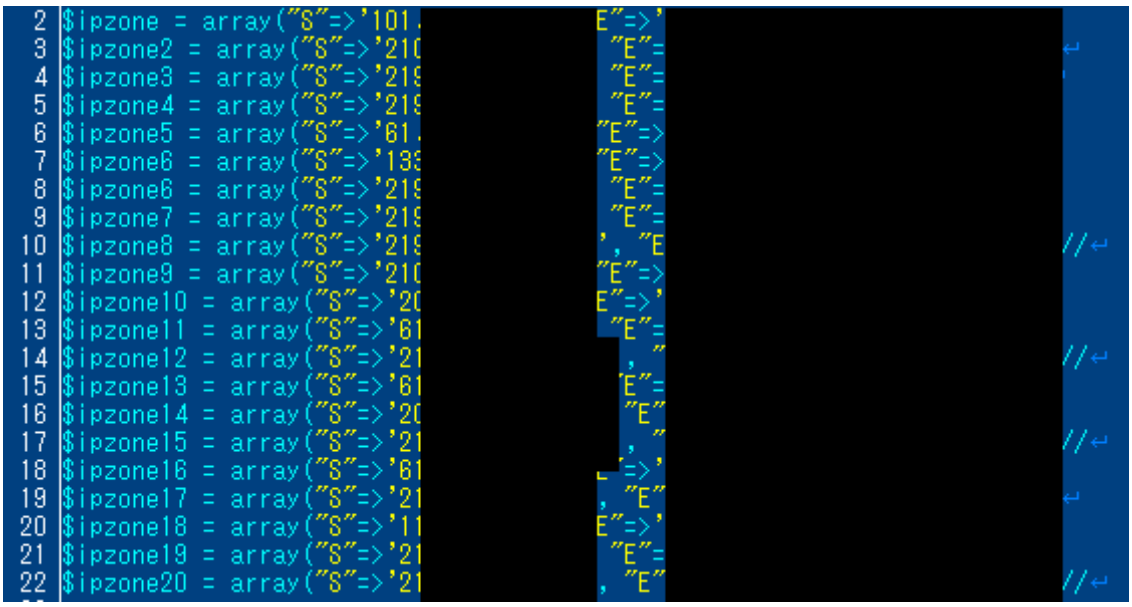


**図 6 攻撃対象が限定された攻撃コード**

図 6 の攻撃コードでは、実際に攻撃を行う前に、動作を以下のように分岐させています。

（1） 攻撃対象の IP アドレスからのアクセスである
→ ゼロデイの攻撃コードを実行
（2） 攻撃対象以外の IP アドレスからのアクセスである
→ 何もせず

このような仕組みを使用する理由は複数考えられますが、主に以下の理由が存在すると考えます。

**【攻撃対象を限定する理由】**

(1) 攻撃自体の発覚を遅れさせる

(2) セキュリティベンダなどに攻撃手法を出来るだけ解析されないようにする

（特に今回のようにゼロデイ脆弱性などを、可能な限り長期的に使用できるようにするため）

一部では今回のゼロデイ脆弱性を用いた水飲み場型攻撃は、完全に日本のみを標的としたものであるといった報道がなされています。しかし、JSOC およびサイバー救急センターでは上記の攻撃対象 IP アドレスの制御の他に、図 7 のようなコードを確認していることから、CVE-2013-3893 を用いたゼロデイ脆弱性による攻撃が、必ずしも日本企業・組織のみをターゲットとしたものではないと考えます。

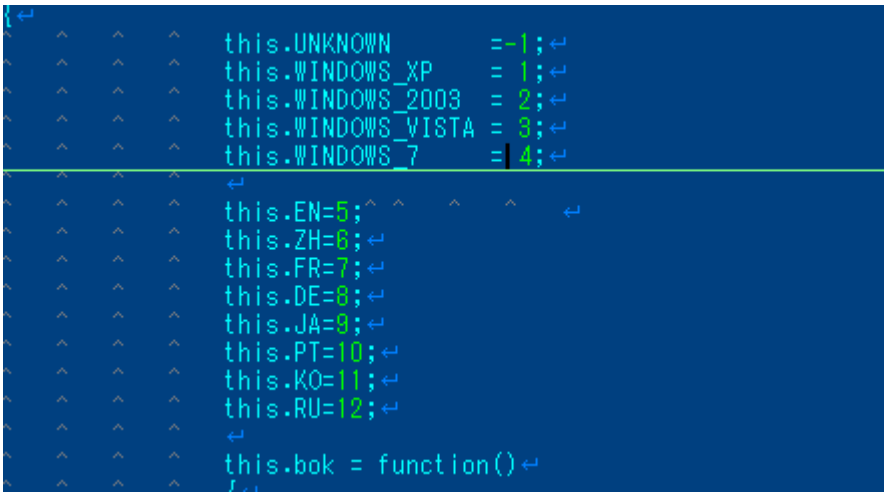



**図 7 OS バージョンおよび言語環境を特定するコード部分**

図 6 の攻撃対象の IP アドレスを限定している部分には、日本の企業・組織以外の IP アドレスは存在していないため、攻撃対象とする言語環境に関しては特定する必要性が低いと考えられます。しかし、実際の攻撃コードには図 7 の通り、アクセスしたユーザの言語環境を判別している部分が存在していました。そのため、攻撃対象 IP アドレスを指定している部分以外の攻撃コードについては、今回国内で確認されたケース以外にも流用されている可能性を示唆していると考えます。

実際に CVE-2013-3893 のゼロデイ脆弱性を悪用する攻撃コードが、台湾などの改ざんされたサイトでも悪用されている事例が報告されています[6]。また JSOC でも図 8 および図 9 のように今回国内で用いられた攻撃コードと国外にて用いられた攻撃コードがほぼ同様のものであることを確認しています。

---

[6] Latest Internet Explorer 0day used against Taiwan targets
http://www.alienvault.com/open-threat-exchange/blog/latest-internet-explorer-0day-used-against-taiwan-users

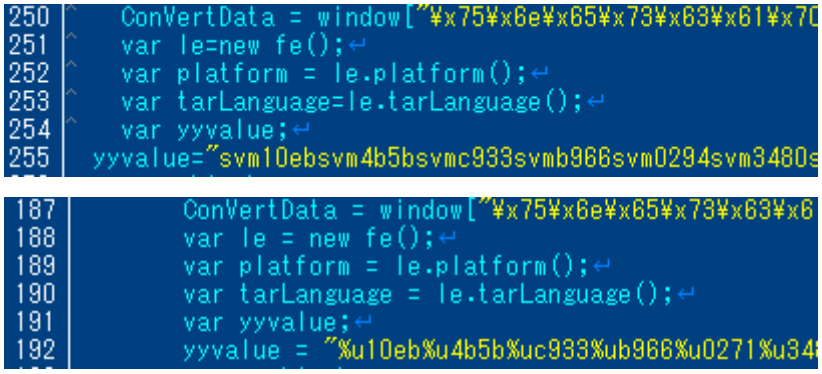



**図 8 国内および国外で用いられた攻撃コードの比較 1**

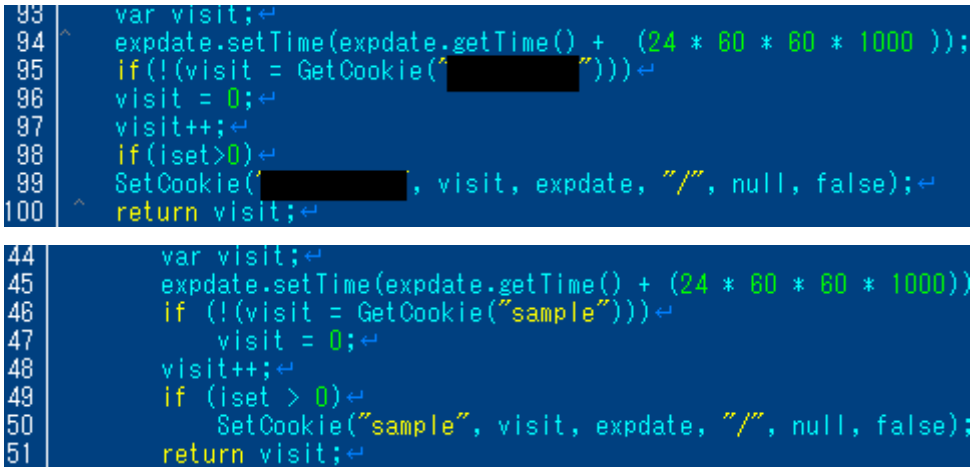



**図 9 国内および国外で用いられた攻撃コードの比較 2**

※図 8、9 とも、上が日本国内で用いられた攻撃コード、下が国外で用いられた攻撃コード

攻撃コードが流用されている場合、以下の 2 つの可能性が存在すると考えます。

**【攻撃コードが流用されている理由の推測】**

（1） 国内および国外の事例の攻撃者が同一である

（2） 攻撃コードが何らかの理由により、複数の個人もしくはグループ間で譲渡されている

特に（2）に関して、近年脆弱性に関する情報はアンダーグラウンドにおいて売買されていることが確認されているため、今回の攻撃コードも同様に売買されていた可能性があると考えます。

### 4.1.3　CVE-2013-3893 を悪用した攻撃・水飲み場型攻撃の対策

- **CVE-2013-3893 を悪用する攻撃への対策**

CVE-2013-3893 に関しては、脆弱性を修正するセキュリティアップデート（MS13-080）が既に Microsoft 社より公開されています。セキュリティアップデートが適用されているか早急にご確認ください。

- **水飲み場型攻撃全般への対策**

以下の対策を推奨いたします。

(1) 最新の製品やセキュリティアップデートを適用
(2) Enhanced Mitigation Experience Toolkit（EMET）[7]の使用
(3) 自組織におけるホストの状況の把握・ネットワーク監視
(4) インシデントレスポンス体制の構築
(5) JSOC セキュリティ監視サービスなどの活用

（1）に関して、水飲み場型攻撃では今回確認されたケースのようにゼロデイ脆弱性を悪用されるケースもありますが、多くの場合には既に修正されている脆弱性が用いられるため、非常に有効であると考えます。また、水飲み場型攻撃だけでなく、通常のドライブバイダウンロード攻撃や他のマルウェアについても同様に有効な対策となります。

（2）に関して、使用している場合には Windows のゼロデイ脆弱性を悪用する攻撃からも保護できる可能性があります。今回の脆弱性 CVE-2013-3893 を悪用した攻撃においても、セキュリティアップデート適用以前のホストであっても、EMET を使用している場合には影響がなかったことを確認しています。

更に詳細な対策については、弊社 Web サイトにおいても公開していますため、以下もご参照ください。

**水飲み場型攻撃に関する対策について**
http://www.lac.co.jp/security/alert/2013/10/09_alert_02.html

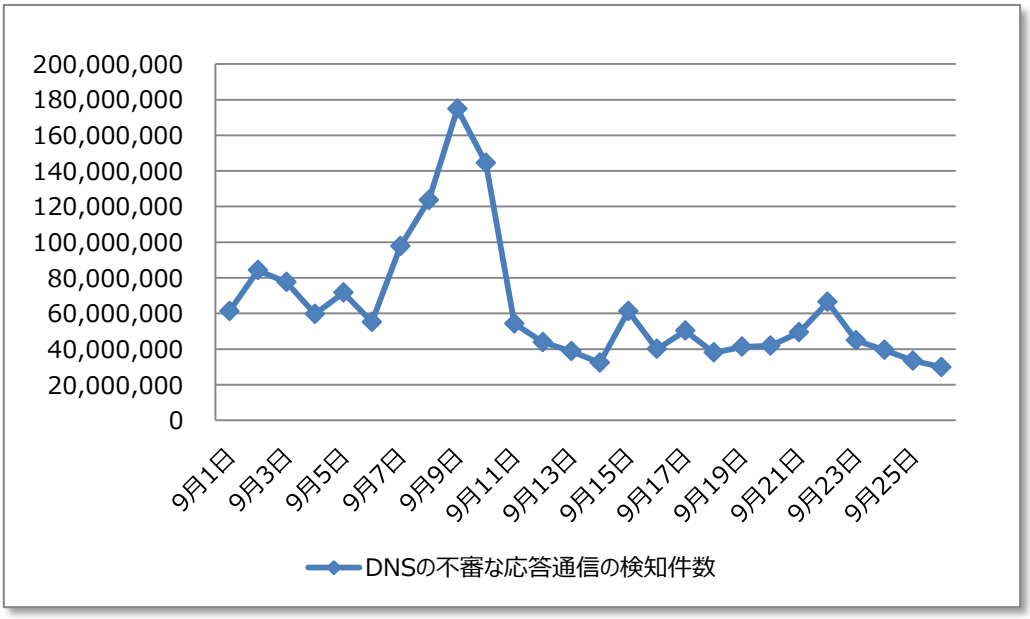
---

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

## 4.2　外部へ公開されている UDP サービスを悪用した通信の増加について

### 4.2.1　UDP サービスを悪用した攻撃の概要および件数の推移

2013 年 7 月以降、無制限に公開されている DNS や CHARGEN などの UDP サービスを悪用する DoS 攻撃に関連するインシデントが増加しています。特に、9 月上旬以降では、外部からの再帰問い合わせを許可している DNS キャッシュサーバ（オープンリゾルバ）を悪用する「DNS アンプ（リフレクター）攻撃」の通信を多数検知しました。



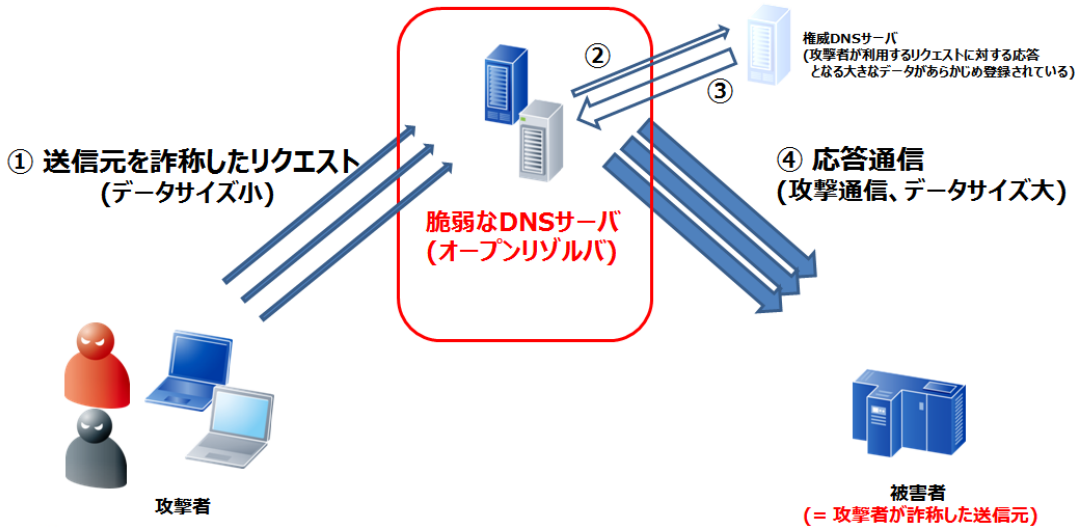

**グラフ 6 DNS アンプ攻撃に関する不審な応答通信件数の推移**

この攻撃については、中国を発信元とする再帰問い合わせ可能な DNS サーバの探索行為が増加しており、再帰問い合わせ可能な DNS キャッシュサーバ（オープンリゾルバ）を悪用する DDoS 攻撃である、「DNS アンプ（リフレクター）攻撃」の準備行為と考えられるとして、9 月 11 日に警察庁から注意喚起が行われていました。

一方 JSOC では、9 月以前より、この DNS アンプ攻撃の準備行為と考えられる不審な DNS の通信を既に検知していただけではなく、9 月に入って更に監視対象のホストから大量の通信が発生し、実際の攻撃から被害の発生にまで至っていることを確認しています。

具体的には、これらの通信の内容に DNS アンプ攻撃を意図していると考えられる不審なデータが含まれていることをきっかけに調査した結果、実際に外部からの再帰問い合わせが実行可能な環境であることなどを確認したため、お客様のホストが DNS アンプ攻撃に悪用されていると判断し、重要インシデントとして連絡を行いました。

DNS アンプ攻撃は、攻撃送信元からの比較的少ないデータの送信に対し、攻撃対象には大量のデータが送りつけられるという特徴があります。通信を中継するオープンリゾルバがデータ量を増幅させる役割を担うことから、オーディオ機器などのアンプになぞらえて、DNS アンプ攻撃と呼ばれています。




通信が②と③の過程で増幅されている

また、実際には多数の送信元から繰り返しリクエストが行われる

**図 10 DNS アンプ攻撃の概要**

UDP の通信は、セッションの確立（疎通や送信先の確認）を行いません。攻撃者は図 10 のように送信元を詐称したリクエストを行うことにより、オープンリゾルバを悪用して送信元を隠したまま効率的に攻撃を行うことが可能です。

CHARGEN サービスなどについても UDP で通信を行うため、DNS アンプ攻撃と同様に、リクエストの送信元を詐称すること可能です。CHARGEN は通信テストなどに用いられるサービスで、アクセスした送信元に文字列を送信するだけの単純な動作を行います。送信元を詐称することにより、詐称した送信元に対する大量の通信を発生させることが出来ます。

これは CHARGEN サービスに固有の問題ではなく、UDP でかつアクセス時に無差別に応答を返すサービスは全て同様に悪用される可能性があります。そのため、必要のない場合にはサービスを停止し、ファイアウォールなどのネットワーク機器によって、アクセス制御を行うことを推奨いたします。

**脆弱なサーバの応答**

(外部からのリクエストを受け付けている)

```
> server 192.168.1.1
DNS request timed out.
    timeout was 2 seconds.
既定のサーバー:  [192.168.1.1]
Address:  192.168.1.1

> a           .com
サーバー:  [192.168.1.1]
Address:  192.168.1.1

権限のない回答:
名前:    a.          .com
Addresses:        .53.114
                  53.115
                  53.116
                  53.117
                  53.118
                  53.119
                  53.120
                  53.121
                  53.122
                  53.123
                  52.128
                  52.129
                  52.130
```

**正しく設定されたサーバの応答例**

(外部からのリクエストを拒否している)

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights re
served.

C:¥Users¥Nacht>nslookup
DNS request timed out.
    timeout was 2 seconds.
既定のサーバー:  UnKnown
Address:

> server
DNS request timed out.
    timeout was 2 seconds.
既定のサーバー:
Address:

> a.          .com
サーバー:
Address:

***  [          ] が a.          com を見つけられません
: Query refused
>
```

**図 11 DNS サーバの再帰問い合わせに対する応答例**

なお、UDP のサービスを悪用する通信においては、実際にサービスが稼動しているか、あるいは悪用が可能であるかに関わらず、ポートがオープンであるように見受けられるホストに対して無差別に大量のリクエスト送信を行うケースがあることを確認しています。

その他、JSOC では、お客様のホストが DoS 攻撃に悪用された事例以外にも、悪用の対象となるポートがオープンであったために大量のリクエストを送信され、お客様自身のホストがサービス不能状態となってしまうといった被害事例も確認しました

**表 6 UDP でアクセス時に応答を返すサービスの例**

| サービス名 | 概要 |
|---|---|
| ECHO （7/tcp,udp） | 受け取ったデータを全てそのまま送信元に送り返す |
| DAYTIME （13/tcp,udp） | 現在の日付と時刻を文字列で出力する |
| CHARGEN （19/tcp,udp） | 文字列データを自動生成し、切断されるまで送り続ける |
| TIME （37/tcp,udp） | 西暦 1900 年 1 月 1 日午前 0 時 0 分 0 分 0 秒 からの秒数を 32bit の整数にして出力する |

### 4.2.2　最近の被害事例と対策

2013 年に入り、この DNS アンプ攻撃を用いた大規模な DDoS 攻撃の被害が報じられています。3 月には、欧州のスパム対策組織である Spamhaus がこの攻撃を受け、最大 300 Gbps もの通信が発生し、一時的な通信の遅延や障害が生じたと報じられました。[8]

DNS アンプ攻撃自体は以前から知られている攻撃手法ですが、トラフィック量そのものを増大させる DoS 攻撃であるため、攻撃対象となった場合には対策は難しく、最近でも大きな被害の生じる例が観測されています。

**表 7 近年の大規模な DNS アンプ攻撃の被害事例**

| 事例 | 概要 |
|---|---|
| PIE データセンター（２ちゃんねるなど）への攻撃 | 世界中のボットなど数万 IP によるアクセス |
| Spamhaus への攻撃 | 最大 300Gbps の通信が発生 |
| 金融機関システムへの攻撃 | 最大 167Gbps の通信が発生[9] |

また、通常の DNS サーバの設定ミスによりオープンリゾルバとなっているケース以外にも、一部のルータなどのネットワーク機器において意図せず DNS サーバが稼動しており、更にそれがオープンリゾルバであるため攻撃に悪用される事例が報告されています。[10]また、JSOC においても同様のケースによる被害事例を確認しています。

ネットワーク機器においてオープンリゾルバが稼動しているケースでは設定変更が不可能であることがあり、そのような場合には機器の交換を行う必要があります。それ以外の場合には、以下を参考にオープンリゾルバのチェックや設定変更を推奨いたします。

DNS アンプ攻撃などの DDoS 攻撃は、自組織が攻撃対象ではなくとも、管理する機器が攻撃に悪用された場合には社会的な責任を追及される可能性があります。可能な限り対策の実施を推奨いたします。

- **自組織のホストが DNS アンプ攻撃に悪用されないための対策**

(1) DNS の権威サーバとキャッシュサーバを分離し、ネットワーク機器にて適切なアクセス制御を実施する
(2) 権威 DNS サーバにおいては、再帰問い合わせを禁止する
(3) キャッシュ DNS サーバにおいては、DNS サーバの設定にて再帰問い合わせを受け付けるネットワーク範囲を限定する
(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

---

[8] The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)
http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho
[9] Prolexic Stops Largest-Ever DNS Reflection DDoS Attack
http://www.prolexic.com/news-events-pr-prolexic-stops-largest-ever-dns-reflection-ddos-attack-167-gbps.html
[10] JVN#62507275 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題
http://jvn.jp/jp/JVN62507275/

また、下記のサイトで DNS サーバがオープンリゾルバであるかのチェックが可能です。

**オープンリゾルバ確認サイト**
http://www.openresolver.jp/
**Open Resolver Project**
http://openresolverproject.org/
**The Measurement Factory: Open Resolver Test**
http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl

**※上記サイトによるテストは、自組織の DNS サーバにのみ行うようにしてください。**
**多数のサーバに対してオープンリゾルバを探す疑いのある行為が行われた場合には、セキュリティインシデントとして扱われる恐れがあります。**

オープンリゾルバが存在した場合には DNS サーバの設定の修正を行ってください。
下記のサイトに、詳細な設定変更の手順が紹介されています。

**■設定ガイド：オープンリゾルバ機能を停止するには【BIND 編】**
http://jprs.jp/tech/notice/2013-04-18-fixing-bind-openresolver.html

また、自組織への DNS アンプ攻撃など、リソースを枯渇させる DDoS 攻撃に対しては、以下のような対策を推奨いたします。

- **DNS アンプを含めた自組織への DoS 攻撃対策**

(1) 自組織のネットワーク状況をモニタリングできるようにしておく
(2) ネットワーク機器において、通信の帯域制限を行う
(3) ネットワーク機器において、不要なポートへのアクセスをブロックする
(4) ネットワーク機器に DDoS 攻撃に対する保護機能がある場合は、これを活用する
(5) サーバにおいて、同時接続数を制限する
(6) サーバにおいて、TCP の設定をチューニングする
(7) 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）
(8) 負荷分散装置を導入する
(9) CDN（コンテンツ配信網）サービスを利用する
(10) 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 DDoS 対策サービスを利用する

## 5　終わりに

2000 年に設立された JSOC は、19 号にわたり「侵入傾向分析レポート」を発行し、おかげさまで皆様より大きな反響を頂いてまいりました。通算 20 号目となった前号からは、株式会社ラックが発行する「ラックレポート（四半期に一度の発行）」の創刊に合わせ、最新の脅威にスポットを当て即時性を重視し、名称を「JSOC INSIGHT」と変え 3 ヶ月に一度の間隔で発行しています。

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、いち早く情報提供することを目指しています。

JSOC が、お客様と共に「安全・安心」を提供できるビジネスシーンの礎となれれば幸いです。

**JSOC INSIGHT vol.2**
**【執筆】**
天野　一輝 / 木村　諭紀雄 / 品川　亮太郎 / 庄子　正洋 / 三和　弘典