WordPress に対する攻撃の実態調査

四半期レポート(2016 年 7 月～9 月)

株式会社神戸デジタル・ラボ

WP PORTAL チーム

内容

エグゼクティブサマリー

WP PORTAL チームでは、WordPress への攻撃情報を分析するために、国内のサーバに攻撃を収集するシステムを設置して攻撃情報を収集しました。分析の結果、以下の攻撃情報が得られました。

アカウントに対する攻撃が行われています。

WordPress のログイン画面に対し、総当たり攻撃を行い、アカウントを乗っ取るような攻撃が観測されました。

ID パスワードの傾向から、比較的単純なパスワード（123456 や password といった推測されやすいもの、ID と同一のもの）などが影響を受ける可能性があります。設定されているパスワードが複雑なものかご確認されることをお勧めします。

また、必要に応じて二要素認証など、安全を強化する仕組みの追加もご検討ください。

テーマ・プラグインに対する攻撃が行われています。

テーマやプラグインに対し、ディレクトリトラバーサルや任意ファイルアップロードの脆弱性を使用したと考えられる攻撃が観測されました。

使用中のテーマやプラグインが脆弱性をもっている場合、不正なファイルが設置されるなどして、サイトの情報が乗っ取られる可能性があります。また、不正なファイルにより、別の攻撃に使用される可能性があります。

観測されている攻撃は既知のものが多かったため、使用しているテーマやプラグインが最新のものかを確認して、最新のものでない場合はアップデートされることをお勧めします。

1 攻撃状況の概況

1.1 観測手法

WP PORTAL チームでは、独自の観測システムを使用し、WordPress への攻撃と考えられるアクセスの収集を行いました。本書では国内のサーバに設置した 3 つの観測点を使用して、攻撃を収集したものを解説しています。

また、これらのシステムでの観測は 2016 年 2 月ごろから行っており、本書は 2016 年 7 月 1 日～同年 9 月 30 日の間のものを解説しています。

1.2 収集結果

同期間に収集したアクセス数を集計した結果、表 1 のようになりました。

アカウントに対する攻撃は、多量のパスワードを総当たりで試行するため多くのアクセスを観測しました。

テーマに対する攻撃、プラグインに対する攻撃は、アカウントに対する攻撃と比較してアクセスは少ないものの、既知の脆弱性を使用した攻撃などを観測しました。

表 1 収集結果概要

攻撃種別	アクセス数
アカウントに対する攻撃（2 章で解説）	278,457
テーマに対する攻撃（3 章で解説）	271
プラグインに対する攻撃（4 章で解説）	959

2 アカウントに対する攻撃

ユーザ ID パスワードを狙った攻撃が継続的に行われています。

2.1 攻撃概要

WordPress は専用のログイン画面を持っており、処理は wp-login.php で行われます。ログイン試行のリクエストは通常 1 つの POST リクエストで構成されており、このリクエストを機械的に試行するようなアクセスが観測されています。

ログインの際に行われる POST リクエストのボディ部分は以下の通りです。パラメータ「log」の部分に ID、パラメータ「pwd」の部分にパスワードが記載されます。このリクエストを wp-login.php に送信することでログインの試行を行うことができます。

レスポンスとしてステータスコード「200」がサーバから送信される場合、ログインが失敗と判断されます。ステータスコードが「302」の場合、ログインが成功し、wp-admin 以下の WordPress 管理者専用ページにリダイレクトされます。

```
log={USERNAME}&pwd={PASSWORD}&testcookie=1
```

一方で、WordPress サイトを XML で操作する際に使用する xmlrpc.php ファイルに対するアクセスも観測されており、これらのアクセスの中にはアカウントに対する攻撃も見られています。

以下に xmlrpc.php に対するリクエスト例を記載しています。これは、WordPress が用意している API のうち「wp.getUsersBlogs」を使用して、サイトの情報を取得しようとしているものです [1]。このリクエストでは、ユーザ名が「admin」、パスワードが「1qaz2wsx」のアカウントに対して試行しています。

```
<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
  <methodName>wp.getUsersBlogs</methodName>
  <params>
    <param><value>admin</value></param>
    <param><value>1qaz2wsx</value></param>
  </params>
</methodCall>
```

2.2　攻撃状況

図 1 ではアカウントに対する攻撃とみられるアクセスの総数を記載しています。短期間で多くのログイン試行が行われていることがわかります。

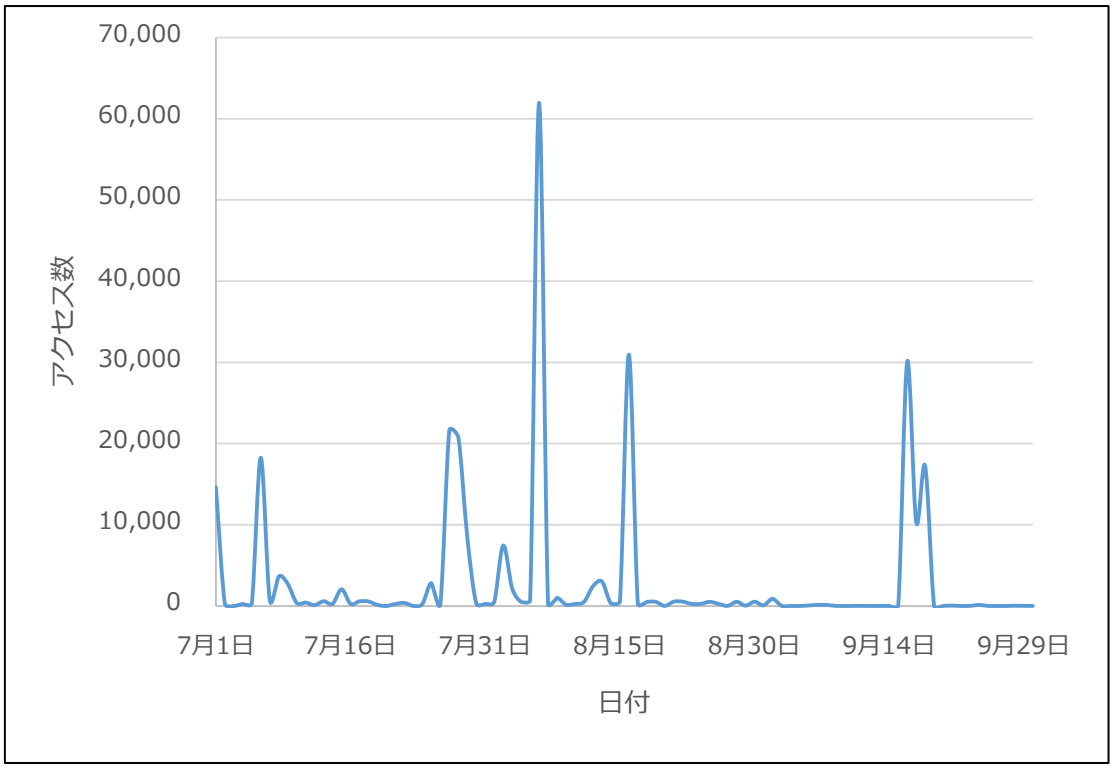

図 1 アカウントに対する攻撃の総数

図 2 では、5,000 件以内のものを拡大して表示されています。短期間で大量のアクセスが来ている中で、数 100 件程度のログイン試行も継続的に行われています。

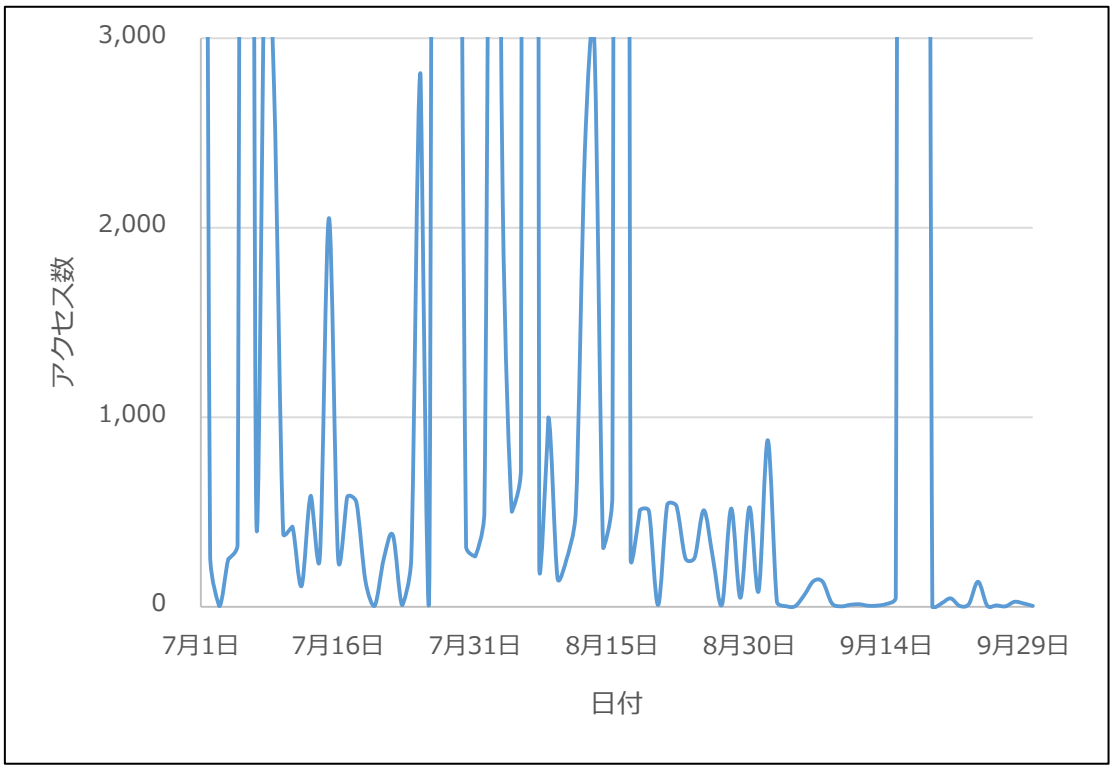

図 2 アカウントに対する攻撃の総数（部分拡大）

図 3 ではアカウント攻撃に多く使用されたパスワードを示しています。試行が多かったパスワードでは、主に「admin」や「123456」などの推測可能なパスワードが多く狙われていることがわかります。

図 3 内の「account」と呼ばれるものは攻撃者がサイトごとに推測したものになります。例えば、WordPress の設定によっては URL 末尾に「?author=1」などを入力すると、レスポンスの内容からアカウント名が推測できる場合があり、この機能を使用してサイトごとのアカウント名を推測したと考えられます。

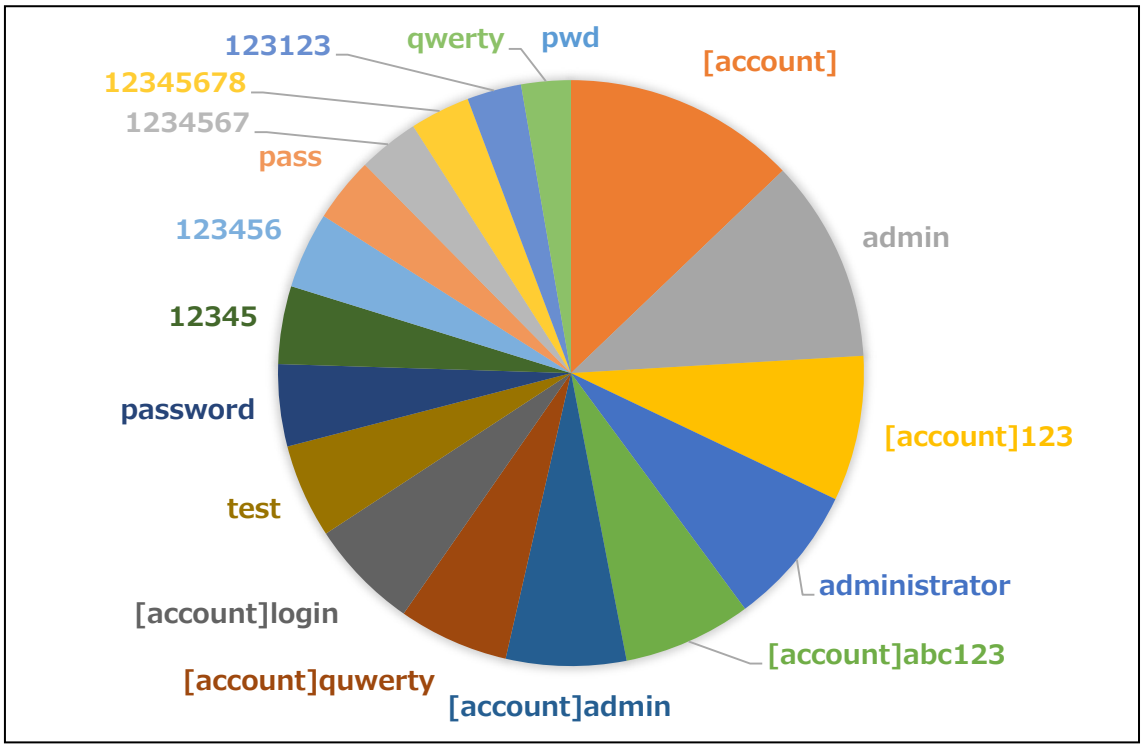

図 3 試行された回数の多いパスワード

2.3 対策

ID パスワードの傾向から、比較的単純なパスワード（123456 や password といった推測されやすいもの、ID と同一のもの）などが影響を受ける可能性があります。設定されているパスワードが複雑なものかご確認されることをお勧めします。

また、必要に応じて二要素認証など、安全を強化する仕組みの追加もご検討ください。

3 テーマに対する攻撃

WordPress のテーマの脆弱性を狙った攻撃が観測されました。

3.1 攻撃概要

WordPress で使用されているテーマは wp-content/themes 配下にテーマごとにディレクトリが分けられて配置されています。通常、WordPress の管理画面にあるインストール機能を使用するか、ディレクトリを配置するなどの方法でインストールを行います。

テーマごとの設定変更などは WordPress の管理画面で行うことが多いため、通常は WordPress の管理画面にログインが必要になります。しかし、テーマが配置されている wp-content/themes ディレクトリ自体には認証がなく、攻撃者により直接アクセスされることにより攻撃が行われる場合があります。

本システムでは、本来外部からのアクセスを想定していないのにも関わらずアクセスがあったテーマを収集して、それらのアクセスを分析しました。

3.2 攻撃状況

テーマに対する攻撃もしくは探索数は図 4 に示しています。一部短期間でアクセスが集中した時もありましたが、全体として継続的にアクセスが行われていました。

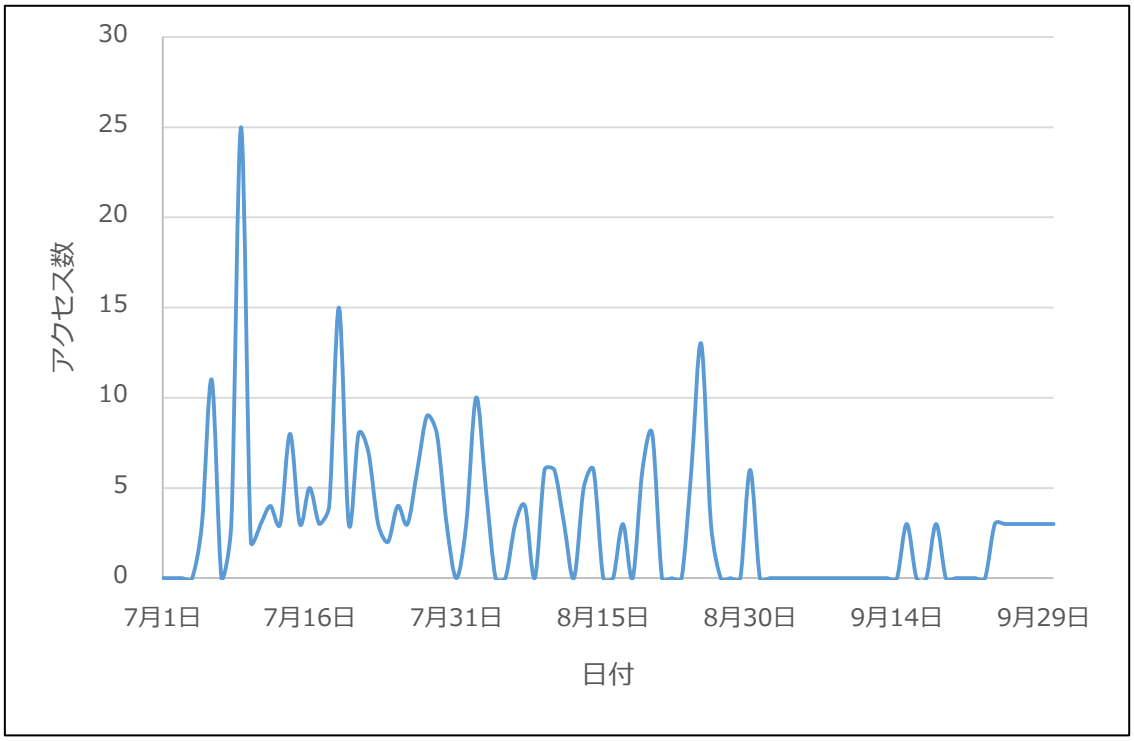

図 4 テーマに対する攻撃傾向

図 5 にどのテーマにアクセスがあったかを示しています。アクセスがあったテーマのうち、アクセス回数が少数であったものはグラフから除外して表示しています。グラフから攻撃されるテーマに偏りはなく、攻撃者がリストのようなものを使用し様々なテーマに対しアクセスを試みていることが分かります。

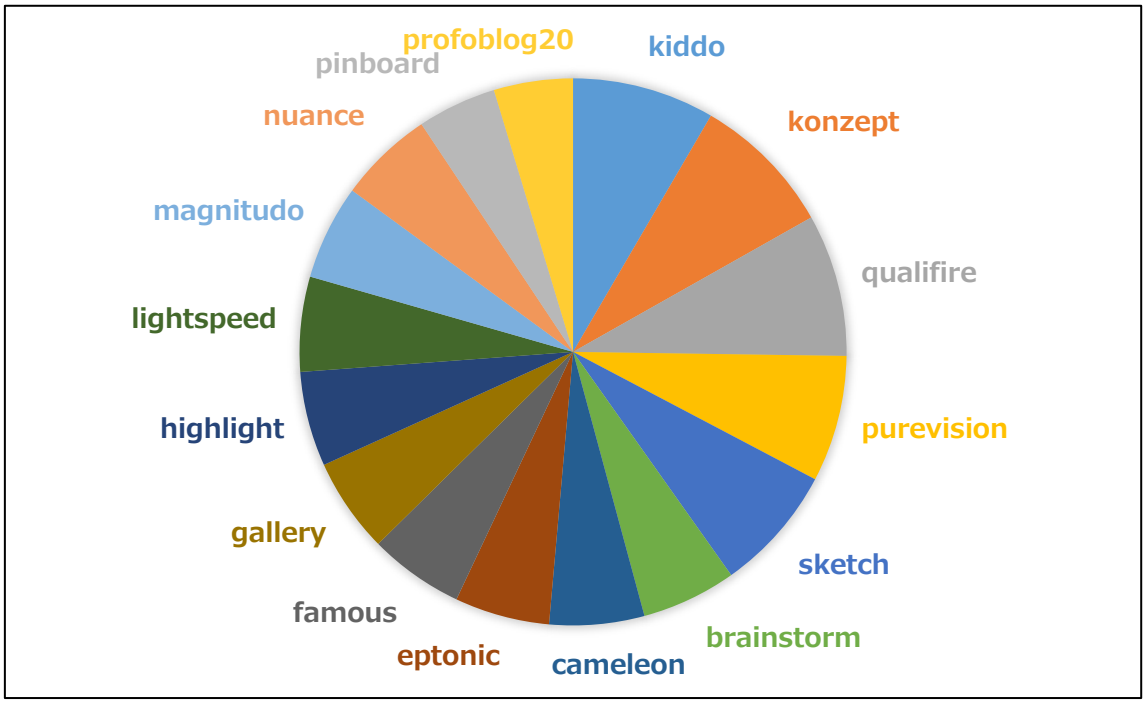

図 5 アクセスがあったテーマ名

3.3 脆弱性を狙った攻撃

攻撃の中にはテーマの脆弱性を狙ってファイルをアップロードするものも確認されました。

以下にリクエスト例を示します。これは攻撃者がアップロードを試行している GET リクエストボディの一部分です。一部を安全のため加工しています。

このリクエストから、攻撃者はテーマ内の download.php に対してアクセスを行い、download.php 内にある処理を悪用して、上位ディレクトリにある wp-config.php を取得しようとしていると考えられます。

wp-config.php を取得されると、WordPress が使用しているデータベースのアクセス情報（ホスト名、ID、パスワード）などの重要な情報が漏えいする可能性があります。

通常、wp-config.php ファイルは外部から取得できないようになっていますが、download.php にディレクトリトラバーサルの脆弱性がありパラメータにあるファイルを読もうとしている場合は、以下のようなパラメータから攻撃者に wp-config.php の内容が取得される可能性があります。

本システムでは、同様のアクセスが複数のテーマに対して行われましたが、WordPress の公式ディレクトリに無く現在は配布が終了しているものもあり、脆弱性の有無は確認できていません。

```
GET /wp-content/themes/

(テーマ名)/lib/scripts/download.php?file=../../../../../wp-config.php
```

3.4　対策

自身のサイトが使用しているテーマに対するアクセスログを確認し、「../../../../../」が含まれるリクエストが行われていないかどうか確認してください。また、発見した場合は、当該のファイルを確認し、上位ディレクトリに対するアクセスを禁止できているかどうか確認してください。

使用していないテーマに対してのアクセスは問題ありません。但し、停止したままでテーマのディレクトリを削除していない場合は影響を受ける場合があります。

また、これらの脆弱性情報の多くはインターネット上に公開されています。インターネット上に公開されているものは、攻撃者のツールなどに搭載される場合が多く、すぐに攻撃に使用される可能性があります。

これらの攻撃を防ぐ方法の 1 つとして、使用しているテーマが最新のものかを確認して、最新のものでない場合はアップデートされることをお勧めします。

4 プラグインに対する攻撃

WordPress のプラグインの脆弱性を狙った攻撃が観測されました。

4.1 攻撃概要

WordPress で使用されているプラグインは wp-content/plugins 配下にプラグインごとにディレクトリが分けられて配置されています。先述のテーマと同様、WordPress の管理画面にあるインストール機能を使用するか、ディレクトリを配置するなどの方法でインストールを行います。

プラグインごとの設定変更などは WordPress の管理画面で行うことが多いため、通常は WordPress の管理画面にログインが必要になります。しかし、プラグインが配置されている wp-content/plugins ディレクトリ自体には認証がなく、攻撃者により直接アクセスされることにより攻撃が行われる場合があります。

本システムでは、本来外部からのアクセスを想定していないのにも関わらずアクセスがあったプラグインを収集して、それらのアクセスを分析しました。

4.2 攻撃状況

プラグインに対する攻撃もしくは探索数は図 6 に示しています。一部短期間でアクセスが集中した時もありましたが、全体として継続的にアクセスが行われていました。

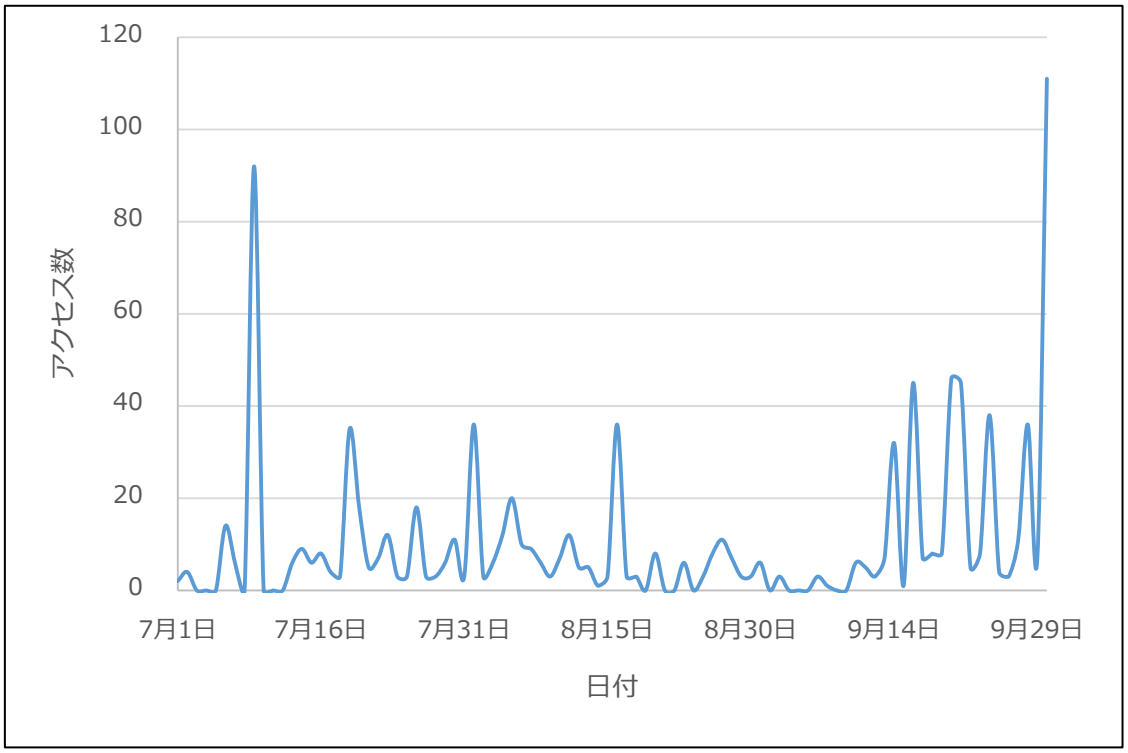

図 6 プラグインに対する攻撃傾向

図 7 にどのプラグインにアクセスがあったかを示しています。アクセスがあったプラグインのうち、アクセス回数が少数であったものはグラフから除外して表示しています。グラフから攻撃されるプラグインに偏りはなく、攻撃者がリストのようなものを使用し様々なプラグインに対しアクセスを試みていることが分かります。

このグラフから EC 機能をもったプラグインに対するアクセスが多くみられましたが、どのアクセスも静的ファイルへのアクセスのため、このアクセスで攻撃の内容は特定できず、プラグインの使用の有無を確認していると考えられます。

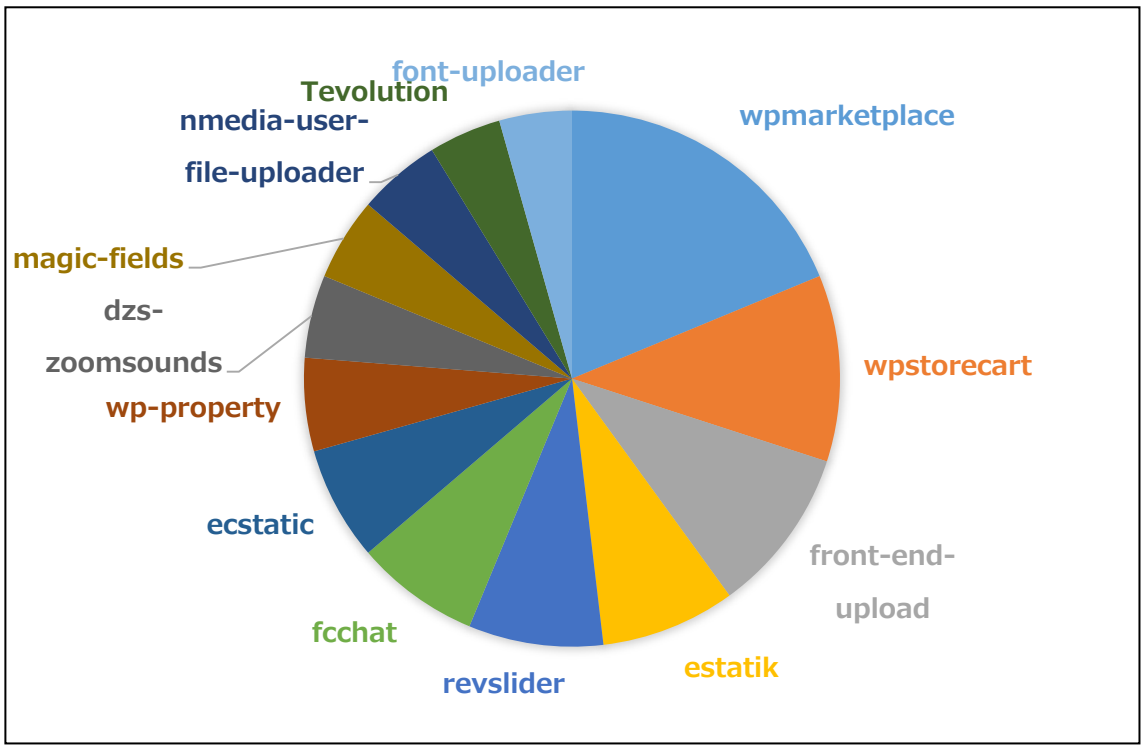

図 7 アクセスがあったプラグイン名

4.3 脆弱性を狙った攻撃

攻撃の中にはプラグインの脆弱性を狙ってファイルをアップロードするものも確認されました。

以下にリクエスト例を示します。これは攻撃者がアップロードを試行している POST リクエストボディの一部分です。一部を安全のため加工しています。

リクエストから内容から、「123」と記載されたファイルをアップロードしようとしていることがわかります。これは
「WordPress 用 ReFlexGallery プラグインの admin/scripts/FileUploader/php.php における任意の PHP コードを実行される脆弱性」 [2]
を使用しているものとみられ、既知の脆弱性を使用しているものであると考えられます。

アップロードされるファイルは「123」と記載されたファイルであり、このリクエストのみでサイトに大きな影響を与えるわけではありませんが、レスポンスからアップロードが成功したと分かると、別のファイルをアップロードされ、バックドアの設置やマルウェアの配布など二次攻撃が行われる可能性があります。

またこれらの攻撃は当該プラグインを最新版にアップデートを行うことで防ぐことができます。

```
--aa877db0cb1aac55c69f7c7289d10282

Content-Disposition: form-data; name="_________"; filename="cap.txt"

Content-Type: application/octet-stream
123
--aa877db0cb1aac55c69f7c7289d10282--
```

4.4　対策

観測されている攻撃は既知のものが多くみられました。また、これらの脆弱性情報の多くはインターネット上に公開されています。インターネット上に公開されているものは、攻撃者のツールなどに搭載される場合が多く、すぐに攻撃に使用される可能性があります。

このため、使用しているプラグインが最新のものかを確認して、最新のものでない場合はアップデートされることをお勧めします。

また、使用しないプラグインは、停止したままであれば攻撃の影響を受ける可能性があります。使用しないものは、プラグインのディレクトリを削除するようにしてください。

5 終わりに

本書では、「アカウントに対する攻撃」、「テーマに対する攻撃」、「プラグインに対する攻撃」について解説しました。

「アカウントに対する攻撃」はパスワードを複雑なものにすることが有用であると考えられます。

「テーマに対する攻撃」、および「プラグインに対する攻撃」は、自身の使用しているテーマおよびプラグインが最新版かどうかを確認し、最新版がある場合はアップデートすることで、攻撃の影響を回避することができると考えられます。

どちらの対策も、日々の運用で心がけておくことが必要になります。定期的にメンテナンスを行う担当者がいるかどうか、メンテナンス日が決まっているかどうか、重要なセキュリティアップデートが行われた場合に対応する計画が決まっているかどうかをご確認ください。

6 参照文献

1. XML-RPC wp. Codex. (オンライン) https://codex.wordpress.org/XML-RPC_wp.
2. WordPress 用 ReFlex Gallery プラグインの admin/scripts/FileUploader/php.php における任意の PHP コードを実行される脆弱性. JVN iPedia.（オンライン）http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-002851.html.

WordPress に対する攻撃の実態調査
四半期レポート(2016 年 7 月～9 月)

【執筆】
松本 悦宜、寺岡 良真

（注意事項）
本書で記載しているデータは 2016 年 11 月 1 日時点のものです。
内容は予告なく変更する場合があります。

株式会社 神戸デジタル・ラボ
本社
〒650-0034　神戸市中央区京町 72 番 新クレセントビル
TEL：078-327-2280　FAX：078-327-2278
担当窓口：
セキュリティソリューション事業部
三木 剛<miki@kdl.co.jp>
松本 悦宜<y-matsumoto@kdl.co.jp>

東京支社
〒150-0022 東京都渋谷区恵比寿南 1-1-1 ヒューマックス恵比寿ビル
TEL： 03-6871-9400

ホームページ
弊社サイト：http://www.kdl.co.jp/
Proactive Defense 専用サイト：http://www.proactivedefense.jp/