サイトガードシリーズ

SITEGUARD

ウェブサイトを取り巻く脅威と対策

リアルログから読み解く日本国内における WordPress セキュリティの現状

– JP-Secure Labs Report Vol.01 –

2018 年 2 月 23 日

株式会社ジェイピー・セキュア

JP-Secure Labs

JP-Secure

はじめに

本レポートは、国産ソフトウェア型 **WAF「SiteGuard シリーズ」**の開発・販売を行う**株式会社ジェイピー・セキュア**の「**サービスパートナー・プログラム**」に加入しているパートナー企業の協力のもと、不正アクセスの傾向を統計化したレポートです。

本レポートでは、世界的にシェアの高い**CMS**（Content Management System）である「**WordPress**」を対象にした情報を中心にまとめています。

「WordPress」は、企業規模を問わず、また SOHO や個人まで幅広く活用されている CMS であり、レンタルサーバーや VPS 等のサービスを利用するユーザーの多くが「WordPress」を活用していると言われています。

「WordPress」は、簡単にホームページを作成できるだけでなく、テーマ・プラグインを使用したデザインの変更や EC サイトの構築ができるなど、拡張性に優れ、ユーザーにとって様々な魅力がある実績豊富なオープンソースの CMS です。その一方で、改ざんや不正ログインなど、「WordPress」で作成されたウェブサイトへの攻撃は増加の一途を辿っており、「WordPress」のセキュリティ対策が重要な課題となっているのも事実です。これは「WordPress」が危険であるということではありません。どのようなウェブサイトであっても適切な運用管理が必要であり、サイト運営者の一つ一つの意識や対策が「安心・安全なウェブサイトの運用」につながります。

不正アクセスの傾向や発見された脆弱性のほか、攻撃の実例と対策をまとめた本レポートが皆様の「安心・安全なウェブサイトの運用」の一助となれば幸いです。

【集計期間】

2017 年 10 月 1 日 ～ 2017 年 12 月 31 日

【対象サービス】

GMO ペパボ株式会社「**ロリポップ！レンタルサーバー**」

GMO クラウド株式会社「**WADAX 共用サーバー**」

目　次

1. エグゼクティブサマリ 1

2. 検出統計（全体） 2

2.1 攻撃種別の分類（全体） 2

2.2 月別の統計 5

2.3 接続元（国別）の分類 6

3. WordPress に対する攻撃の検出傾向 7

3.1 WordPress に対する攻撃（攻撃種別） 7

3.2 WordPress に対する攻撃（検出箇所） 8

3.3 【トピックス①】ディレクトリトラバーサル（wp-config.php の読み取り） 10

3.4 【トピックス②】WordPress REST API の脆弱性 12

4. WordPress の脆弱性統計 14

5. WordPress のセキュリティ対策 18

6. おわりに 21

7. JP-Secure Labs 22

1. エグゼクティブサマリ

本レポートでは、集計期間中に確認された攻撃・検出に加えて、注目すべき脅威やインシデントの事例を取り上げます。

■検出総数 4,688 万／1 日あたり 50 万件を超える検出

ユーザー数 40 万超の「ロリポップ！レンタルサーバー」を含む対象サービスにおける攻撃の検出総数は、**46,883,944 件**となり、1 日あたりの検出数は平均で 50 万件を超えました。

集計期間中の対象サービスへの検出種別を分類するほか、レンタルサーバー、ホスティングというサービス、ウェブサイトの特性からみた検出傾向などについて解説します。

■WordPress のテーマ・プラグインに対する攻撃

WordPress のテーマ・プラグインで、クロスサイトスクリプティングや SQL インジェクションなどの脆弱性の報告が相次いでいます。

集計期間中の検出種別のほか、実際に行われている攻撃の一例をご紹介するとともに、テーマ・プラグインを含む WordPress のバージョン管理の重要性について解説します。

■WordPress のセキュリティ対策

豊富な実績・拡張機能というメリットがある反面、WordPress を使用しているとセキュリティの話題で「危険」と捉えられてしまうことがあります。実際には、WordPress だからということではなく、どのようなサイトであっても対策の基本的な考え方は変わりません。

本レポートの最後では、WordPress のセキュリティ対策のポイントについて解説します。

2. 検出統計（全体）

対象サービスのウェブサイトにおいて、集計期間中（2017 年 10 月～2017 年 12 月）に検出した攻撃の総数は、**46,883,944 件**でした。日によって変動はありますが、平均すると**毎日 50 万件**の攻撃を検出していることになります。

※ 対象サービスで稼働している **WAF**（ウェブアプリケーションファイアウォール）「**SiteGuard シリーズ**」の検出情報（検出ログ）をもとに集計しています。
（SQL インジェクションに代表されるウェブアプリケーションの脆弱性を悪用した攻撃や WordPress の脆弱性を悪用した攻撃等を検出・防御した総数です。）

※ 対象サービスの利用者によるセキュリティ診断等のアクセスが集計対象に含まれている場合があります。

※ 不正ログインの試行（ログインの失敗）のほか、ウェブ以外の不正アクセス（スパムメールやマルウェア等）の情報は含まれていません。

2.1 攻撃種別の分類（全体）

検出した攻撃を分類すると図 2.1-A のようになり、4 割近くを占める SQL インジェクションに次いで、OS コマンドインジェクション、バッファオーバーフロー、クロスサイトスクリプティングという順になりました。

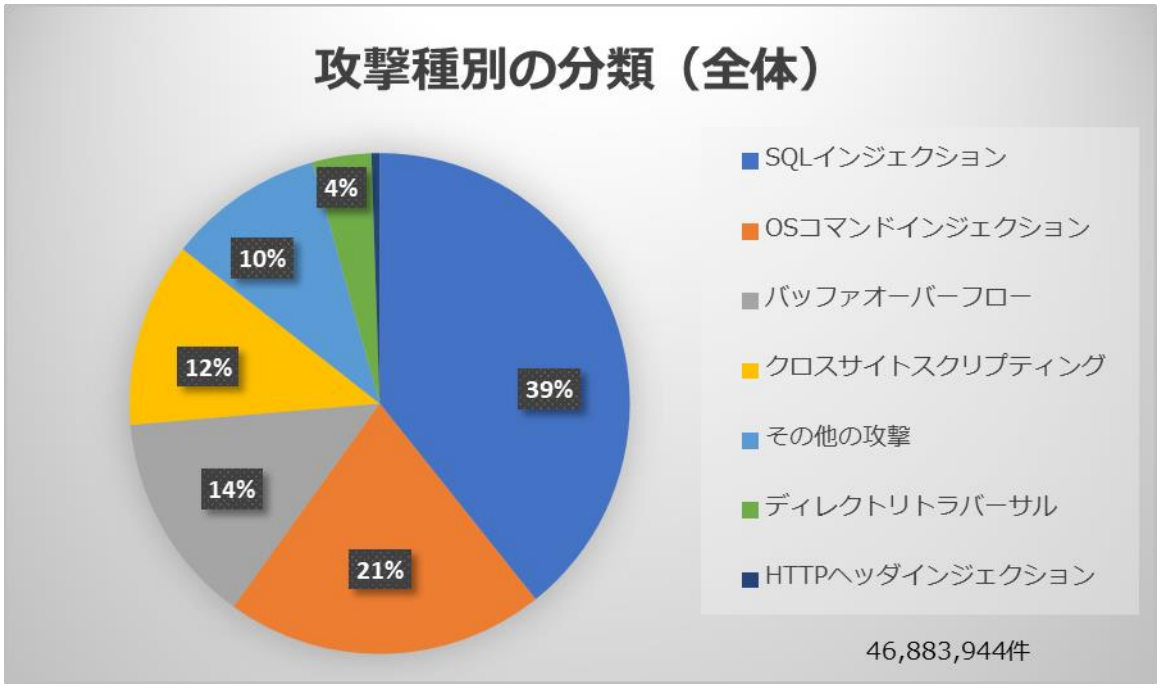


図 2.1-A 攻撃種別の分類（全体）

攻撃種別	検出した件数
SQL インジェクション	18,418,961
OS コマンドインジェクション	9,682,259
バッファオーバーフロー	6,425,395
クロスサイトスクリプティング	5,592,294
その他の攻撃	4,730,848
ディレクトリトラバーサル	1,785,787
改行コードインジェクション	248,400
合計	**46,883,944**

表 2.1-A 攻撃種別の分類（全体）

SQL インジェクションやクロスサイトスクリプティングに代表されるウェブアプリケーションの脆弱性を悪用する攻撃に対しては、以前からウェブサイトの運用において重点的な対策が求められており、検出傾向としても上位に入ることが多くなっています。

今回の統計において興味深かった点は、バッファオーバーフローに分類される攻撃が上位に入ったことです。詳細を確認したところ、一定期間の間、繰り返し、またはランダムな長い英数字を含む POST リクエストが大量に送信されていることが分かりました。

① 67777777788888888888999999999AAAAAAAAAAABBBBBBBBCCCCCCCCCCCDDDDDDDDDDEEEEEEEEE…

② xyyyyyyyyyyyyyzzzzzzzzzzzzzzz000000000000000111111111111111222222222222222233333333333333…

③ Oqlqu9DHLlqum2vA37048159DAa1GVZpFJYcgw04fvAaq5KOShaqumrYR92vosw0tx1imfNGyrjRK2jcKD6oV…

図 2.1-B バッファオーバーフローで検出されたリクエスト（要求本文）の例

該当のアクセスは、1 秒～10 秒の間に数回という頻度で、複数のサイトに対して継続的に行われていました。リクエストの内容からファジング（脆弱性検出手法の一つ）によるアクセスを検出したという可能性がありましたが、不特定多数の接続元（国）から繰り返し行われていたため、通常では用いられない形式・長さのリクエストを送信し続けることにより、システムの誤動作や負荷上昇を狙ったボットなどからのアクセスであったと推察されます。

※ バッファオーバーフロー攻撃の可能性について、「SiteGuard シリーズ」では、長い URL やパラメータの入力があった場合に検出します。

その他の攻撃の内訳は、図 2.1-C のように PHP-CGI リモートコード実行（CVE-2012-1823）の検出が最も多く、2 番目に多かったのは WordPress の設定ファイル（**wp-config.php**）の読み取りを試みる攻撃で、この 2 つで 8 割近くを占めるという結果になりました。

このほか、WordPress のプラグインなどで使用されている timthumb.php の脆弱性を悪用し、バックドアの設置やコード実行を試みる攻撃（2011 年）や Joomla! 3.4.5 までのバージョンに対するゼロデイ攻撃として話題になったリモートコード実行（原因は、PHP の脆弱性（CVE-2015-6835）の影響）などが検出されています。

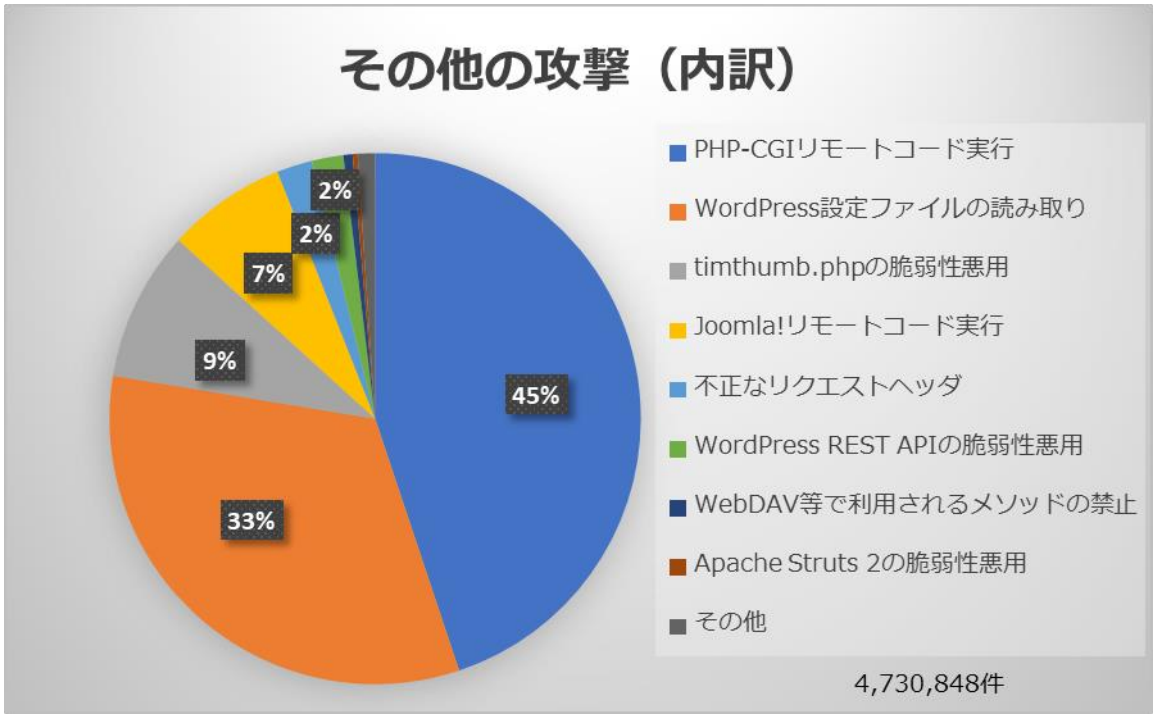


図 2.1-C その他の攻撃（内訳）

攻撃種別	検出した件数
PHP-CGI リモートコード実行	2,122,973
WordPress 設定ファイルの読み取り	1,547,866
timuthumb.php の脆弱性悪用	432,394
Joomla!リモートコード実行	343,941
不正なリクエストヘッダ	102,211
WordPress REST API 脆弱性の悪用	90,803
WebDAV 等で利用されるメソッドの禁止	26,699
Apache Struts 2 の脆弱性悪用	13,910
その他	50,051
合計	**4,730,848**

表 2.1-B その他の攻撃（内訳）

このように、PHP や CMS における過去の脆弱性悪用を試みる攻撃の検出が多い中、2017 年のウェブサイトのセキュリティにおいて、大きな話題となった **WordPress REST API の脆弱性**を悪用する攻撃を今現在も検出しています。また、度々、深刻な脆弱性が報告された **Apache Struts 2 の脆弱性悪用**を試みる攻撃も検出していますが、本レポートの集計対象であるサービスでは、Apache Struts 2 は利用されていないため、影響を受けることはなく、少数の機械的な攻撃を検出していたと考えられます。

2.2 月別の統計

集計期間の検出数について、月別にみると図 2.2-A のように、12 月の検出が多く、10 月と 11 月の検出数の合計に迫る結果となりました。

なお、「年末にかけて検出数が増加している」といった特徴はなく、後述する WordPress に対する不正アクセスの増加があり、全体的に 12 月の検出数が多かったという状況でした。

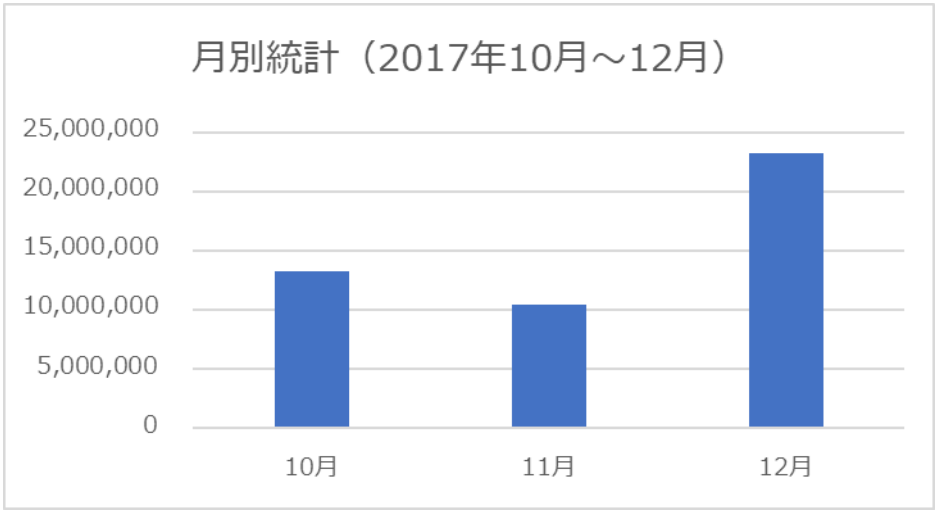


図 2.2-A 月別統計（グラフ）

集計対象（月）	検出した件数
2017 年 10 月	13,230,439
2017 年 11 月	10,421,047
2017 年 12 月	23,232,458
合計	**46,883,944**

表 2.2-A 月別統計（検出数）

2.3 接続元（国別）の分類

攻撃に使用された接続元 IP アドレスを国別で集計した結果が図 2.3 です。

接続元は、踏み台として経由されることが多いという前提はありますが、検出総数の 3 分の 1 を占めるアメリカ合衆国が最も多く、日本は 2 番目に多いという結果になりました。

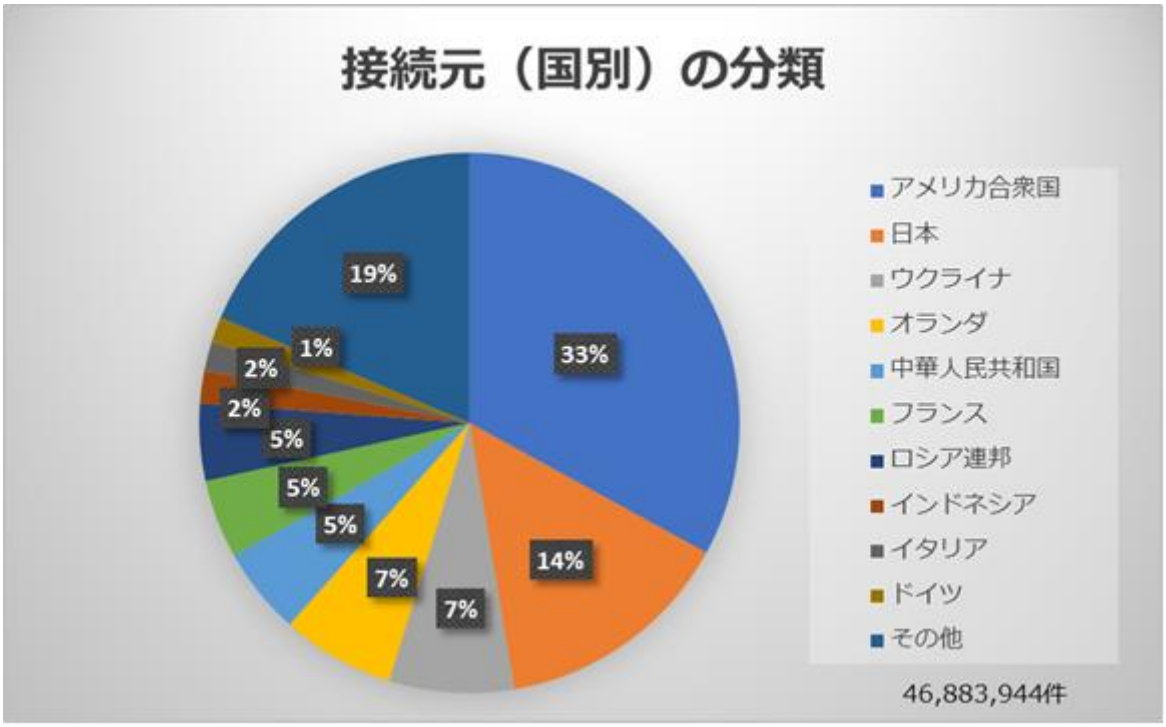


図 2.3 接続元の分類（国別）

	国名	検出した件数
1	アメリカ合衆国	15,462,052
2	日本	6,732,432
3	ウクライナ	3,503,358
4	オランダ	3,182,602
5	中華人民共和国	2,446,699
6	フランス	2,214,972
7	ロシア連邦	2,167,352
8	インドネシア	918,773
9	イタリア	809,804
10	ドイツ	717,684
—	その他の国	8,728,216
	合計	**46,883,944**

表 2.3 接続元（国別）の分類

3. WordPress に対する攻撃の検出傾向

攻撃の検出傾向（全体）**46,883,944** 件について、WordPress に対する攻撃を対象に集計すると、明らかに WordPress を対象にした検出、またはその可能性が高い検出が **15,031,521** 件ありました。
本レポートの集計対象のサービスでは、広く WordPress が有効活用されています。
世界的にみても有名な CMS であり、ユーザー数が多いという状況から、WordPress を対象とした攻撃の検出が多くなり、全体の約 3 分の 1 を占める結果になったと考えられます。

※ WordPress のコア（本体）に関するディレクトリである「**/wp-includes/**」やテーマ・プラグインがインストールされる「**/wp-content/**」、管理ページ「**/wp-admin/**」のほか、WordPress に関連するファイルへの検出など、WordPress への攻撃である、またはその可能性が高いと判定できる条件で集計しています。（WordPress のディレクトリ構成や機能を把握した攻撃と考えられる検出を対象に集計しています。）

3.1 WordPress に対する攻撃（攻撃種別）

検出した攻撃を分類すると図 3.1-A のようになり、SQL インジェクション、クロスサイトスクリプティングの検出で半数を占めています。このほか、OS コマンドインジェクション、WordPress の設定ファイル（wp-config.php）の読み取りを含むディレクトリトラバーサル系の攻撃が多いという結果になりました。

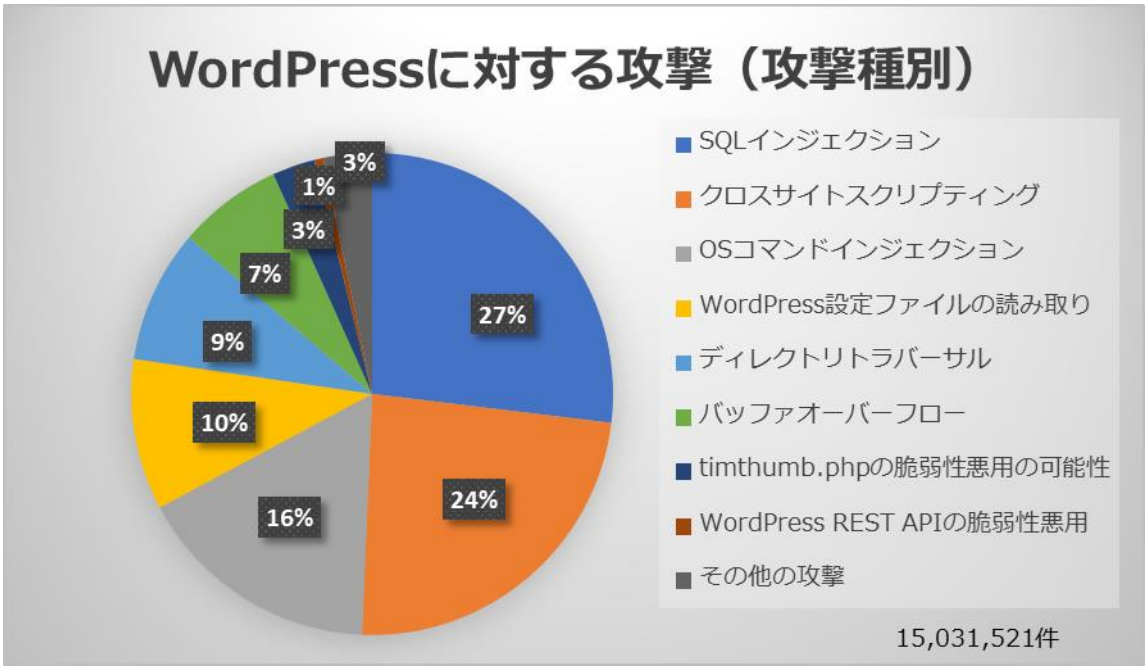


図 3.1-A WordPress に対する攻撃（攻撃種別）

攻撃種別	検出した件数
SQL インジェクション	4,046,307
クロスサイトスクリプティング	3,571,854
OS コマンドインジェクション	2,481,860
WordPress 設定ファイルの読み取り	1,522,406
ディレクトリトラバーサル	1,341,155
バッファオーバーフロー	1,055,097
timthumb.php の脆弱性悪用の可能性	432,079
WordPress REST API 脆弱性の悪用	90,785
その他	489,978
合計	**15,031,521**

表 3.1-A WordPress に対する攻撃（攻撃種別）

3.2 WordPress に対する攻撃（検出箇所）

検出箇所で分類すると図 3.2-A のようになり、「**xmlrpc.php**」での検出が最も多かったという結果になりました。このほか、プラグインやテーマがインストールされている「**/wp-content/plugins/**」「**/wp-content/themes/**」の検出が多く、テーマやプラグインで、Ajax を使用する場合にアクセスされる「**admin-ajax.php**」での検出を含めると、全体としてテーマやプラグインに関連した攻撃の検出が多いことも分かりました。

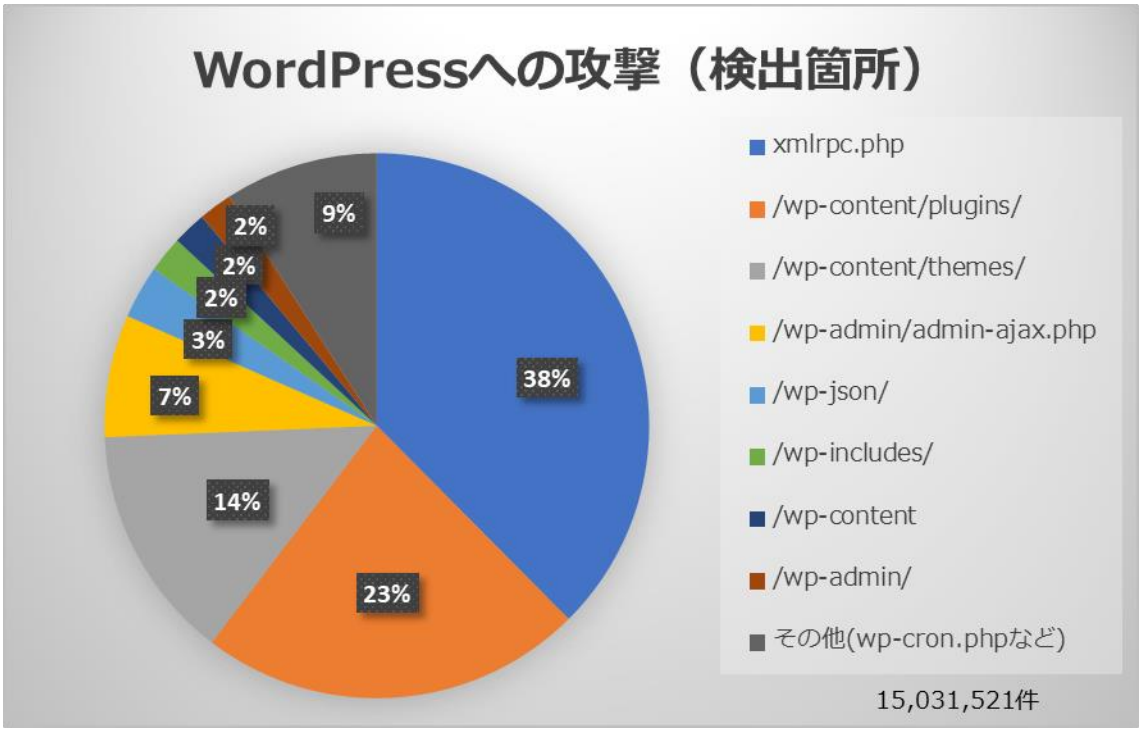


図 3.2-A WordPress に対する攻撃（検出箇所）

検出箇所	検出した件数
xmlrpc.php	5,645,473
/wp-content/plugins/	3,428,170
/wp-content/themes/	2,098,575
/wp-admin/admin-ajax.php	1,092,054
/wp-json/	474,766
/wp-includes/	322,834
/wp-content/	301,029
/wp-admin/	298,596
その他	1,370,024
合計	**15,031,521**

表 3.2-A WordPress に対する攻撃（検出箇所）

「xmlrpc.php」は、WordPress のスマートフォンアプリや外部からの投稿、ピンバックに対応するために用意されており、WordPress をインストールすると標準で使用できるようになっています。
WordPress によるウェブサイトの運用では、しばしば「xmlrpc.php」が DoS やブルートフォース攻撃に悪用され、本レポートの集計においても 12 月に「xmlrpc.php」へのアクセス急増と検出が発生していたことを確認しました。
WordPress のスマートフォンアプリを使用していない場合や「xmlrpc.php」によるアクセスが必要でない場合は、「xmlrpc.php」のアクセス制御などの対策を推奨いたします。

また、WordPress では、テーマ・プラグインの脆弱性を悪用する攻撃が多い傾向にあります。
本レポート執筆時点で、WordPress 公式に登録されているプラグインの数は、5 万 4 千を超えています。
テーマ・プラグインなどの拡張機能は、不特定多数のユーザーや有志によって、自由に開発・提供されており、豊富な機能と拡張性が WordPress の大きな魅力となっています。
その反面、開発者ごとの安全性の配慮にばらつきがあるほか、長い間更新されずに開発が終了してしまっている場合もあるなど、すべてがアクティブ且つ良質なものではありません。
残念ながら、これらの実情からテーマ・プラグインの脆弱性がターゲットとなってしまい、WordPress が「危険」と捉えられてしまう要因の一つになっています。
テーマ・プラグインを使用する際には、利用実績や更新情報などにも気を配るようにしてください。

3.3 【トピックス①】ディレクトリトラバーサル（wp-config.php の読み取り）

WordPress に対する攻撃では、ディレクトリトラバーサルの脆弱性があるテーマ・プラグインを狙って、wp-config.php を読み取ろうとする攻撃が多い傾向にあります。
実際の攻撃リクエストの例を図 3.3-A に示します。

```
/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php

/wp-content/plugins/dukapress/lib/dp_image.php?src=../../../../wp-config.php

/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp-config.php　など
```

図 3.3-A wp-config.php の読み取りを試みる攻撃リクエストの例

「../」を指定し、ディレクトリを遡ることで、本来アクセスが禁止されているディレクトリ、ファイルにアクセスを試みる攻撃で、WordPress のインストールディレクトリにある wp-config.php を不正に読み取ろうとしていることが分かります。
本レポートの執筆にあたり、攻撃・検出の対象となったいくつかのプラグインの古いバージョンにディレクトリトラバーサルの脆弱性が存在することを確認し、wp-config.php を読み取る攻撃が実行可能であることも確認しています。
wp-config.php には、データベースのホストやユーザー名、パスワードなどの情報も記録されているため、外部に漏れるようなことがないよう十分に注意する必要があります。

なお、wp-config.php の安全性を高める対策として、.htaccess ファイルで wp-config.php へのアクセスを禁止するという対策をよく見かけます。

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

図 3.3-B. wp-config.php へのアクセス禁止の設定例（.htaccess）

この設定により、リクエストのパスに直接 wp-config.php が指定された場合のアクセスを禁止することができますが、wp-config.php に直接アクセスしても実際は何も表示されません。
また、この設定では、図 3.3-A のようなアクセスを禁止することはできません。この対策自体に効果がないということではありませんが、別途、対策を講じる必要があります。

wp-config.php の読み取りを試みる攻撃は、WordPress を使用している（またはその可能性がある）サイトに対し、機械的に行われることが多くなっており、実際に脆弱性のあるプラグインがインストールされているかどうかに関係なく、バックドアのインストールや改ざんなどを含めて、常に攻撃が試行されている状況です。脆弱性の存在するテーマ・プラグインを使用していなければ、攻撃の影響を受けることはありませんが、ご利用の環境を把握し、古いプラグインやテーマがある場合はバージョンアップの実施を推奨いたします。

脆弱性の存在するテーマ・プラグインが停止された状態で残っている場合、脆弱性の影響を受ける可能性があります。使用していないテーマやプラグインは削除するようにし、必要となった場合に改めて最新版をインストールするようにしてください。

3.4 【トピックス②】WordPress REST API の脆弱性

2017 年のウェブサイトの脆弱性を悪用した大規模な攻撃の一つとして、WordPress REST API の脆弱性による大規模改ざんがありました。

【脆弱性の影響を受けるバージョン】

WordPress 4.7.0 - 4.7.1

【影響】

コンテンツの改ざん

一部プラグイン利用時には任意のコード実行も可能であるという報告あり

WordPress の 4.7 で標準化された REST API で、外部から認証なしで容易にコンテンツが改ざんされる脆弱性が発見され、深刻な問題として大きな話題となりました。
2017 年 1 月 26 日に WordPress 4.7.2 がリリースされ、この脆弱性が修正されていましたが、WordPress では「何百万という WordPress サイトの安全を保証するため」という意図で、脆弱性の存在を一週間遅れで公開するという対処をしました。

WordPress には自動更新の機能があり、マイナーバージョンは自動更新の対象となるため、自動更新による脆弱性の修正を進め、少しでも影響を低減するという意図であったと考えられますが、数週間後には 150 万ページ以上が改ざんされたという報道があり、広い範囲で被害が発生しました。

攻撃の方法は極めて容易であり、実際のリクエストの例を図 3.4-A に示します。

```
POST /wp-json/wp/v2/posts/20/?id=20A HTTP/1.1
Host: XXXXXXXXX
Content-Length: 92
Content-Type: application/json; charset=UTF-8

{"title": "You have been hacked", "content": "Hacked please update your WordPress version"}
```

図 3.4-A REST API 脆弱性を悪用する攻撃リクエストの例

id が 20 のコンテンツを更新するというリクエストですが、認証に関する情報はありません。
そのため、通常は「401 Unauthorized」となり、コンテンツを更新することはできません。

しかし、図 3.4-A のように id である 20 の後ろに **A** という文字列を追加し、「id=20**A**」としてリクエストを送信すると、認証なしでコンテンツが改ざんされます。
（abc や#など、数値以外を追加することで認証を回避した改ざんが可能となります。）

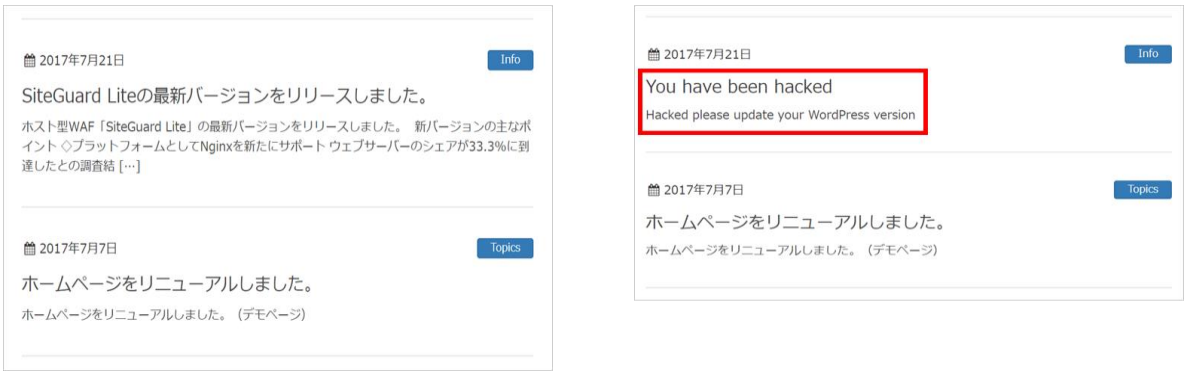


図 3.4-B REST API 脆弱性による改ざんの例

上記は、クエリストリングに細工した id を含んでいますが、要求本文（リクエストボディ）のパラメータに細工した id が含まれている場合も攻撃が成立します。

本レポートの執筆時点で、WordPress の最新バージョンは 4.9.4 であり、今現在では脆弱性の影響を受ける環境も少なく、すでに攻撃のピークは過ぎ去っていると判断して問題ない状況ですが、少数ながら継続して攻撃を検出しています。
WordPress をご利用の場合は、環境の把握とバージョン管理を徹底することを推奨いたします。

4. WordPress の脆弱性統計

2017 年 10 月 ～ 2017 年 12 月に確認された WordPress の脆弱性は、本体 5 件、テーマ 0 件、プラグイン 63 件 合計で 68 件でした。（**情報提供：株式会社レオンテクノロジー**）

図 4-A WordPress 脆弱性の内訳①

脆弱性の種別で見ると、ウェブアプリケーションの脆弱性を悪用した攻撃で代表的なクロスサイトスクリプティングと SQL インジェクションで大半を占めています。

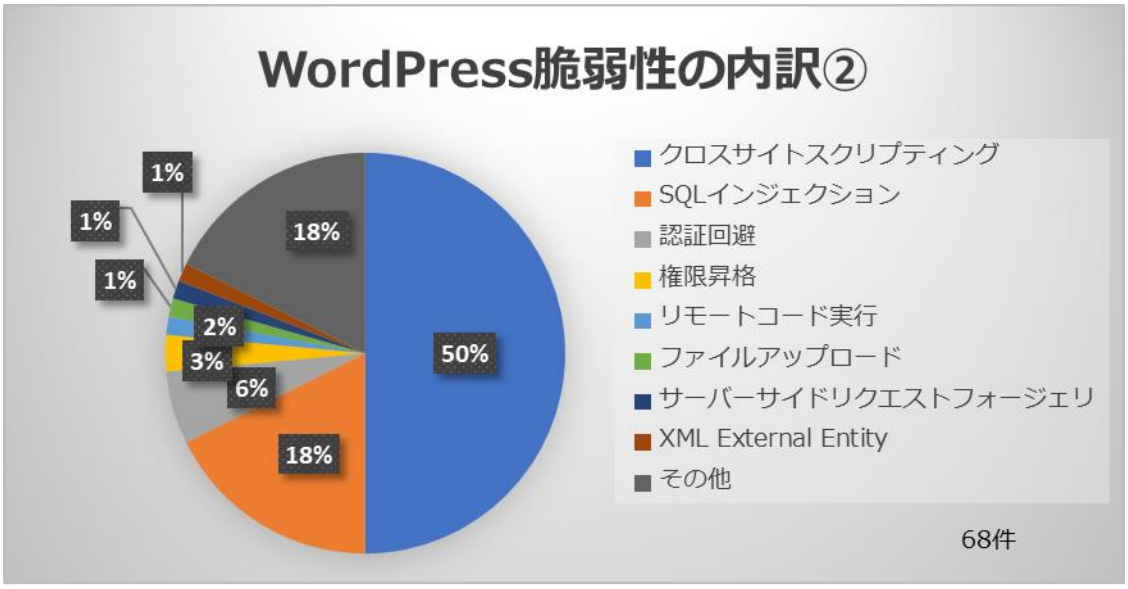


図 4-B WordPress 脆弱性の内訳②

WordPress を対象とした攻撃の検出では、トラバーサル系の攻撃も目立ちましたが、集計期間においてディレクトリトラバーサルの脆弱性に関する新たな報告はありませんでした。
ウェブアプリケーションの脆弱性では、クロスサイトスクリプティングと SQL インジェクションに関する報告が多い傾向にあり、WordPress の脆弱性においても同様です。この傾向は、当社で WordPress の脆弱性の情報収集を強化した 2015 年以降、現在も変わっておらず、今後も同様の傾向が続くと予想しています。

発見された脆弱性の一覧を表 4 にまとめています。
本体の脆弱性については、WordPress 4.8.2 以下のすべてのバージョンにおいて SQL インジェクションの脆弱性が見つかりました。この脆弱性に関して、WordPress の本体に対しては直接影響を受けないとされていますが、テーマやプラグインで SQL インジェクションが発生するおそれがあり、2017 年 10 月 31 日にセキュリティリリースとして WordPress 4.8.3 がリリースされました。
また、WordPress 4.9 リリース後にも XSS などの脆弱性が 4 件見つかり、2017 年 11 月 29 日にバグ修正を含んだ WordPress 4.9.1 がリリースされています。

プラグインの脆弱性では、アクティブインストール数が 500 万を超える SEO 対策プラグイン「Yoast SEO」やアクティブインストール数 100 万を超えるサイト複製用プラグイン「Duplicator」でクロスサイトスクリプティングの脆弱性が発見されています。このほか、「TablePress」 や「bbPress」 といった人気プラグインでも相次いで脆弱性が発見されています。
WordPress の公式ディレクトリから実績のあるプラグインやテーマを選別して使用することは、使用法だけでなく、様々な情報が数多く発信されるなどのメリットがありますが、実績の有無や人気に関係なく、脆弱性が発見されていますので、更新情報を把握するように心がけてください。

発見箇所	脆弱性の種別	脆弱性のある機能／テーマ・プラグインの名称	発見バージョン
本体	SQLi	$wpdb->prepare() Weakness	4.8.2 以下
本体	XSS	HTML Language Attribute Escaping	4.3.0-4.9
本体	Others	‘newbloguser’ Key Weak Hashing	3.7-4.9
本体	XSS	RSS and Atom Feed Escaping	1.5.0-4.9
本体	BYPASS	Authenticated JavaScript File Upload	2.8.6-4.9
プラグイン	Others	WordCamp Talks	21.0.0-beta2
プラグイン	SSRF	Qards	–
プラグイン	XSS	Qards	–
プラグイン	SQLi	WPHRM	1.0
プラグイン	SQLi	content_timeline	–
プラグイン	XSS	PopCash.Net Code Integration Tool	1.0
プラグイン	XSS	User Login History	1.5

プラグイン	XSS	pootle-button	1.1.1
プラグイン	MULTI	ultimate-form-builder-lite	1.3.6
プラグイン	XSS	easy-appointments	1.11.7
プラグイン	XSS	Post SMTP Mailer/Email Log	–
プラグイン	Others	Flickr Gallery	1.5.2
プラグイン	XSS	Caldera Forms	1.5.4
プラグイン	Others	Appointments	1.6.3
プラグイン	XSS	Shibboleth	1.7
プラグイン	XSS	Import any XML or CSV File to WordPress	3.4.5
プラグイン	Others	Invite Anyone	1.3.18
プラグイン	Others	RegistrationMagic-Custom Registration Forms	3.7.9.2
プラグイン	SQLi	Simple Login Log	1.1.0
プラグイン	SQLi	InLinks	1.0
プラグイン	BYPASS	UserPro	4.9.17
プラグイン	Others	WPML Translation Management	2.4.1
プラグイン	XSS	Emag Marketplace Connector	1.0
プラグイン	XSS	Ultimate Instagram Feed	1.3
プラグイン	XSS	Ultimate Instagram Feed	1.3.1
プラグイン	PRIVESC	Elementor Page Builder	1.7.12
プラグイン	SQLi	JTRT Responsive Tables	4.1
プラグイン	RCE	WP Support Plus Responsive Ticket System	8.0.7
プラグイン	XSS	WP Mail Logging	1.8.2
プラグイン	SQLi	Events	2.3.4
プラグイン	SQLi	Simple Events Calendar	1.3.5
プラグイン	XSS	Email Log	2.2.2
プラグイン	XSS	amtyThumb posts	8.1.3
プラグイン	XXE	TablePress	1.8
プラグイン	PRIVESC	Shortcodes Ultimate	5.0.0
プラグイン	SQLi	Active Directory Integration	1.1.8
プラグイン	XSS	Duplicator	1.2.28
プラグイン	XSS	Yoast SEO	5.7.1
プラグイン	MULTI	Formidable Forms	2.05.02
プラグイン	SQLi	bbPress	–
プラグイン	UPLOAD	AccessPress Anonymous Post Pro	3.2
プラグイン	XSS	WordPress Concours	1.1
プラグイン	XSS	WP Mailster	1.5.4
プラグイン	XSS	Smart Marketing SMS and Newsletters Forms	1.1.1
プラグイン	XSS	Custom Map	1.1
プラグイン	Others	Duplicate Page and Post	2.1.0-2.1.1
プラグイン	XSS	Content Cards	0.9.6

プラグイン	Others	No Follow All External Links	2.1.0-2.3.0
プラグイン	XSS	mediaburst-email-to-sms	3.0.0
プラグイン	XSS	mediaburst-ecommerce-sms-notifications	2.4.2
プラグイン	XSS	gravity-forms-sms-notifications	2.4.0
プラグイン	XSS	fscf-sms	2.4.0
プラグイン	XSS	formidable-sms	1.1.0
プラグイン	XSS	Csv Import-Export	1.1
プラグイン	XSS	contact-form-7-sms-addon	2.4.0
プラグイン	XSS	clockwork-two-factor-authentication	1.1.0
プラグイン	XSS	booking-sms	1.1.0
プラグイン	BYPASS	Apocalypse Meow	21.1.3-21.2.7
プラグイン	Others	WP No External Links	4.2.1-4.2.2
プラグイン	SQLi	RegistrationMagic – Custom Registration Forms	3.8.0.4
プラグイン	XSS	RegistrationMagic – Custom Registration Forms	3.8.0.4
プラグイン	BYPASS	Captcha	4.3.6–4.4.4
プラグイン	SQLi	Top 10	2.4.3

XSS：クロスサイトスクリプティング　SQLi：SQL インジェクション

SSRF：サーバーサイドリクエストフォージェリ　RCE：リモートコード実行

XXE：XML External Entity　UPLOAD：ファイルアップロード　BYPASS：認証回避

PRIVSEC：権限昇格　MULTI：複数の脆弱性　Others：その他、不明

表 4 WordPress 脆弱性一覧（2017 年 10 月～2017 年 12 月）

5. WordPress のセキュリティ対策

ここまで、WordPress を対象にした攻撃の内訳や発見された脆弱性、実際の攻撃例などを見てきましたが、WordPress にかぎらずウェブサイトのセキュリティ対策の基本は、

- 脆弱性対策
- ログインの保護

となります。

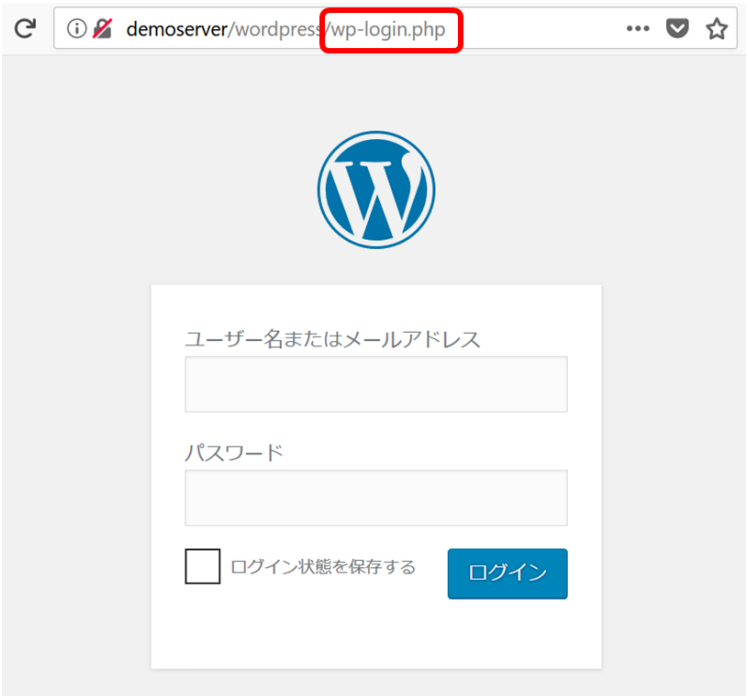
脆弱性対策：

ウェブアプリケーションを自社開発しているケースでは、SQL インジェクションなどの脆弱性がないようにセキュアな開発を徹底する必要がありますが、WordPress のようなソフトウェアを使用している場合は、本体だけでなく、プラグインやテーマといった拡張機能を含めてバージョン管理を徹底し、最新のバージョンを使用することが重要となります。
しかしながら、プラグインのバージョンアップによる誤動作や動作環境が最新バージョンに対応していないなど、運用上の理由ですぐにバージョンアップできないといったことも考えられます。
このようなケースに備えて、**ウェブアプリケーションファイアウォール**（WAF）の利用が効果的です。
WAF は、ウェブアプリケーションの脆弱性を悪用する攻撃の検出・防御に特化しており、SQL インジェクションやクロスサイトスクリプティング、ディレクトリトラバーサルなどの攻撃を検出・防御することができ、ご利用のサイトの安全性を高めます。

ログインの保護：

WordPress に対する攻撃で最も多いのは不正ログインであると言われています。
WordPress にかぎらず、ログインを保護する観点では、パスワード管理が重要な対策となります。
本レポートの集計対象となっているサービスにおいても、WordPress の不正ログインによる被害が多く、不正ログインの結果、サイトの改ざんや踏み台に悪用されるといったケースが確認されています。
その要因として、WordPress は、ディレクトリ・ファイル構成がはっきりしており、ログインページは **wp-login.php** であると知られているため、ログインページへの総当たり攻撃（※）の対象になっていることが挙げられます。

※総当たり攻撃
暗号やパスワードを解読、解析するための手法のひとつでブルートフォース攻撃とも呼ばれます。
（考えられるユーザー名・パスワードを自動化されたプログラムで全て試す手法などが該当します。）



また、WordPress の場合、「https://サイト URL/**?author=1**」のようにアクセスしていくことで、ユーザー名を確認することができます。設定により対処可能ですが、多くの環境でユーザー名が晒されている状態である可能性が高いことも一つの要因として考えられます。

そのため、推測しやすいパスワードを使用していると、ログインページから簡単に不正ログインを許してしまうことになります。

実際、不正ログインに関する相談を受けることは多く、複数のサイトでユーザー名とパスワードを使いまわしていた結果、管理対象サイトのすべてが改ざんされたというケースも確認しています。

仮に、admin や root といったユーザー名を使用していたり、ユーザー名が特定されたとしても強固なパスワードを使用していれば、不正ログインの被害を受ける可能性は極めて低くなります。

不正ログインの問題は、パスワードに対する利用者側の意識にも大きく左右されますが、機能面での対応として、ログインページ名の変更や繰り返しログインを試行する接続元をブロックする機能、画像認証（CAPTCHA）の機能を有するセキュリティプラグインを活用することが効果的です。

その他の対策：

管理ページ（/wp-admin）や xmlrpc.php へのアクセス制御も有効な対策となります。

管理者の操作を保護するという点では、WordPress のログインだけでなく、FTP や SSH の対策（アクセス制御や公開鍵認証の検討など）のほか、接続に利用するクライアント PC のマルウェア対策も重要です。

また、万一の事態に備えて、バックアップの取得を忘れないようにしてください。

WordPress のセキュリティ対策には、考慮すべき点が他にもありますが、これらの基本的な対策と考え方を意識するだけで、セキュリティレベルが大きく向上します。

是非、ご利用のサービスやサイトの環境をチェックし、必要な対策の追加や見直しを検討してください。

「SiteGuard シリーズ」による対策：

- ホスト型 WAF「**SiteGuard Lite**」

  ウェブサイトには外部からの不正アクセスによるコンテンツ改ざんや情報流出などの脅威が存在します。

  昨今の高度なサイバー攻撃からウェブサイトを保護するには WAF の活用が有効です。

  「SiteGuard Lite」は、Apache/Nginx/IIS のモジュールとして動作するホスト型の WAF で、ウェブアプリケーションの脆弱性を悪用する多様な攻撃を検出、防御します。

- WordPress 用セキュリティプラグイン「**SiteGuard WP Plugin**」

  WordPress の管理ページとログインページの保護を中心とした日本語対応のシンプル・簡単プラグインです。WordPress 本体やテーマ・プラグインの更新があったことを知らせる通知機能のほか、xmlrpc.php の悪用を防ぐ機能もあります。

管理ページアクセス制限	ログインしていない接続元から管理ディレクトリ（/wp-admin/）を守ります。
ログインページ変更	ログインページ名を変更します。
画像認証	ログインページ、コメント投稿に画像認証を追加します。
ログイン詳細エラーメッセージの無効化	ログインエラー時の詳細なエラーメッセージに変えて、単一のメッセージを返します。
ログインロック	ログイン失敗を繰り返す接続元を一定期間ロックします。
ログインアラート	ログインがあったことを、メールで通知します。
フェールワンス	正しい入力を行っても、ログインを一回失敗します。
XMLRPC防御	XMLRPCの悪用を防ぎます。
更新通知	WordPress、プラグイン、テーマの更新が必要になった場合に、管理者にメールで通知します。
WAFチューニングサポート	WAF (SiteGuard Lite)の除外ルールを作成します。

※ 本レポートの対象サービスでは、WAF「**SiteGuard シリーズ**」を標準または、オプション機能でご利用いただけます。このほか、各サービスにおいて WordPress 用セキュリティプラグイン「**SiteGuard WP Plugin**」が標準実装されています。詳しくは、**サービス紹介**をご確認ください。

6. おわりに

WordPress は、とても優れた CMS です。セキュリティに配慮しながら、その高い利便性を活かし、セキュアな WordPress ライフを送ってください。

JP-Secure Labs Report では、幅広い役割、年齢層の方々に情報をお届けしたいと考えています。
今後も協力会社との連携をさらに深めていき、インシデントの対応事例で分かったことや新たな脅威への対応にも焦点を当てた有益な情報提供に努めて参ります。

最後に、本レポートの作成にご協力いただいたパートナー企業・関係者の皆様にお礼を申し上げます。

7. JP-Secure Labs

JP-Secure Labs（ジェイピー・セキュア ラボ）では、企業理念である「誰にでも簡単に、安心して利用できる IT 社会の実現」に向けて、ウェブサイトのセキュリティを重点分野と位置づけ、脆弱性や攻撃手法、対策技術に関する調査・研究・開発を行っています。蓄積した技術や情報を自社製品・サービスの向上に生かすだけでなく、より多くの方のセキュリティ向上に貢献するべく、有益な情報発信にも取り組んでいます。

【主な活動内容】

- 独自アンテナシステムによる脆弱性情報の収集
- 攻撃手法の調査、検証
- ハニーポットを活用した攻撃状況の定点観測
- 協業パートナーとの連携によるセキュリティログの分析
- セキュリティ動向に関するレポート発信
- 自社製品・サービスの向上を目的とした技術開発
- 無償セキュリティツールの開発

サービス紹介

本レポートの作成にご協力いただいたパートナー企業のサービスを掲載します。

サービス名	GMO ペパボ株式会社「**ロリポップ！レンタルサーバー**」 LOLIPOP! レンタルサーバー by GMOペパボ **～やりたいことが、すぐできる｜ご利用実績 200 万サイト以上～**
URL	https://lolipop.jp/
SiteGuard シリーズのご利用について	WAF：全プラン標準実装 セキュリティプラグイン：WordPress 簡単インストール機能で標準実装

サービス名	GMO クラウド株式会社「**WADAX 共用サーバー**」 WADAX® by GMO **～サーバーなら WADAX｜No と言わないサポート体制～**
URL	https://www.wadax.ne.jp/service/shared/
SiteGuard シリーズのご利用について	WAF：オプション機能 セキュリティプラグイン：WordPress 簡単インストール機能で標準実装

用語集

- ウェブアプリケーション
  利用者に対して動的なページの提供を実現するウェブサイトで稼働するシステムのこと。（問い合わせフォーム、アンケートフォーム、会員ページ、掲示板など）
  Java や PHP、Perl などの言語で開発されるほか、データベースが活用されている。

- ウェブアプリケーションファイアウォール
  ウェブアプリケーションの脆弱性を悪用する攻撃から、ウェブアプリケーションを保護するソフトウェア、またはハードウェアのこと。
  Web Application Firewall という名称から WAF「ワフ」と呼ばれている。

- 脆弱性
  ウェブアプリケーション等のセキュリティ上の不備や弱点のこと。
  ウェブアプリケーションの脆弱性を悪用する攻撃として、想定しない SQL を実行することで、データベースシステムを不正に操作する SQL インジェクションや攻撃者の仕掛けた罠から不正にスクリプトなどを埋め込むクロスサイトスクリプティングなどがある。

- バッファオーバーフロー
  プログラムで用意しているバッファを超えるデータを送り込むなどの方法により、メモリ領域の破壊やシステムの誤動作が生じたり、悪意のあるコードが実行できてしまう状態のこと。

- ファジング
  ソフトウェアやシステムの不具合、脆弱性を検出する手法の一つで、ソフトウェアやシステムが予測不可能なデータ（ファズ）を入力し、例外処理の挙動などを確認すること。

- ワードプレス（WordPress）
  PHP で開発されているオープンソースの CMS（Content Management System）。
  テーマやプラグインによる拡張性に優れるため、ブログだけでなく、コーポレイトサイトや EC サイトなどにも広く活用されている。

【執筆者】

株式会社ジェイピー・セキュア　齊藤 和男

【協力者】

EG セキュアソリューションズ株式会社　徳丸 浩

GMO ペパボ株式会社　渕野 航介

【協力会社】

GMO ペパボ株式会社

GMO クラウド株式会社

株式会社レオンテクノロジー

ウェブサイトを取り巻く脅威と対策 – JP-Secure Labs Report Vol.01 –

JP-Secure

株式会社ジェイピー・セキュア

〒212-0013　神奈川県川崎市幸区堀川町 66-2　興和川崎西口ビル 2F

TEL：044-201-4036（代表）　FAX：044-201-4037

https://www.jp-secure.com/