– JP-Secure Labs Report Vol.02 –

2018 年 9 月 5 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、当社パートナー企業のサービスを利用しているユーザー向けに、「**WordPress**」、「**Drupal**」といった **CMS**（Content Management System）のセキュリティに関する情報を中心にまとめています。
CMS は、簡単にホームページを作成できるだけでなく、テーマ・プラグインといった拡張機能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、ユーザーにとって様々な魅力があります。
その一方で、改ざんや不正ログインなど、CMS 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、CMS 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。しかし、CMS 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。

また、本レポートでは、当社の定点観測で収集された情報をもとにした不正アクセスの傾向についても取り上げます。

【集計期間】

2018 年 1 月 1 日 ～ 2018 年 6 月 30 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**」

【協力（定点観測）】

さくらインターネット株式会社
株式会社 KDDI ウェブコミュニケーションズ

※　本書は、情報提供を目的としています。

本書の記述を利用した結果に生じた損失等について、株式会社ジェイピー・セキュアは責任を負いかねます。

※　本書のデータをご利用いただく際には、出典元の明記をお願いいたします。

(例 出典：株式会社ジェイピー・セキュア『JP-Secure Labs Report Vol.02』)

目　次

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 1 億 1876 万件／1 日あたり 65 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、**118,759,291 件**となり、1 日あたりの検出数は平均で 65 万件を超えました。
これは、前回レポート（Vol.01）の 1 日あたりの検出数 50 万件を大きく上回っています。
レンタルサーバー、ホスティングサービスで収集された検出情報について、攻撃種別や接続元（国別）で分類し、検出傾向などについて解説します。

■WordPress に対する攻撃と脆弱性の傾向

集計期間中の WordPress に対する攻撃について、検出種別や検出箇所別にまとめたほか、WordPress の脆弱性情報の集計をもとに、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。

■定点観測レポート

当社の定点観測ポイントで収集した情報をもとに、不正アクセスの実態や傾向について解説します。
定点観測では、主にサイトスキャンや Tomcat Manager、WordPress へのブルートフォース攻撃を検出しましたが、「Drupalgeddon 2.0」と呼ばれ話題になった Drupal の深刻な脆弱性を悪用した攻撃などを検出したため、いくつかの脆弱性とその事例についても取り上げます。

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（2018 年 1 月～2018 年 6 月）に検出した攻撃の総数は、およそ **1 億 1876 万件**（**118,759,291**）でした。
サイトによる検出数の差異や日毎の変動はありますが、平均すると**毎日 65 万件**を超える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。）

※ 検出名や分類は、「SiteGuard シリーズ」による検出情報をもとにした表記になっています。

※ 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 割を超える SQL インジェクションに次いで、バッファオーバーフローや OS コマンドインジェクション、クロスサイトスクリプティングを多数検出しました。

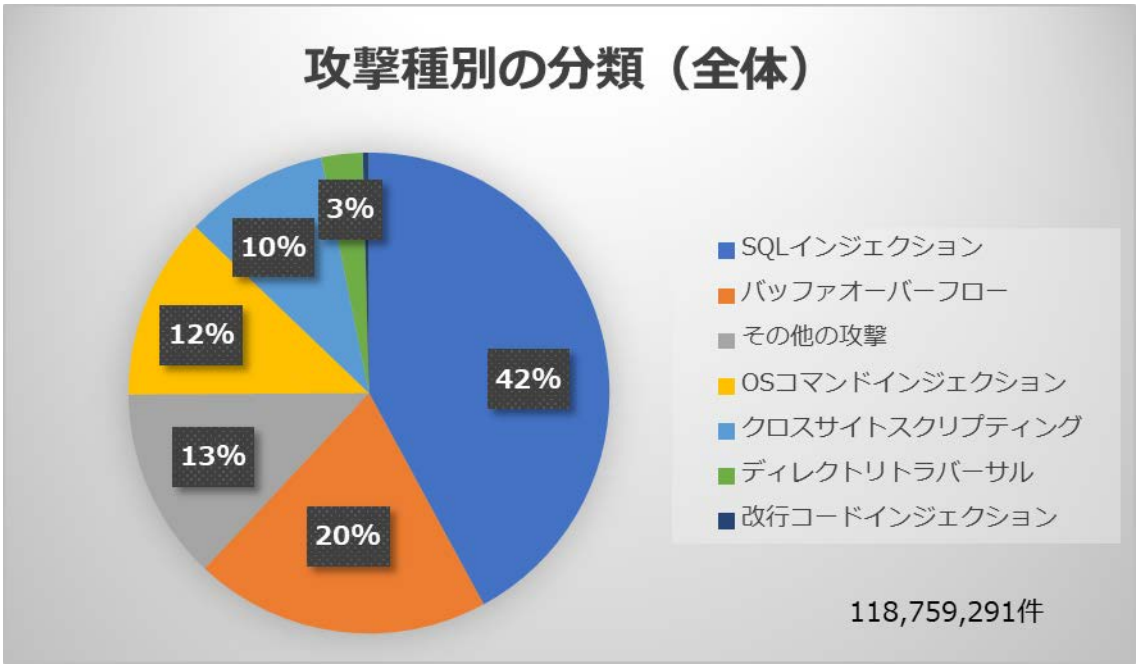

図 2.1-A 攻撃種別の分類（全体）

攻撃種別	検出した件数
SQL インジェクション	49,981,765
バッファオーバーフロー	23,618,352
その他の攻撃	15,354,265
OS コマンドインジェクション	14,558,662
クロスサイトスクリプティング	11,473,069
ディレクトリトラバーサル	3,285,114
改行コードインジェクション	488,064
合計	**118,759,291**

表 2.1-A 攻撃種別の分類（全体）

5000 万件に迫る検出数となった SQL インジェクション攻撃については、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います。SQL インジェクション攻撃のピークとされる 2008 年～2010 年頃に比べて被害事例は減少傾向にあると言われていますが、2018 年 5 月に経営コンサルティング会社の 57 万件の情報流出事故の原因が SQL インジェクションであったという報道があるなど、対策の重要性は今も変わりません。

前回レポート（Vol.01）に引き続き、全体の統計として、バッファオーバーフローに分類される攻撃が上位に入りました。詳細を確認したところ、前回同様に一定期間の間、繰り返し、またはランダムな長い英数字を含む URL へのアクセスや 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。
いずれも集計期間の 2018 年 1 月の 1 ヶ月間に集中しており、以降の検出数は大きく減少しました。

① 67777777788888888888999999999AAAAAAAAAAABBBBBBBBCCCCCCCCCCCDDDDDDDDDDEEEEEEEEE…

② xyyyyyyyyyyyyyzzzzzzzzzzzzzz0000000000000001111111111111112222222222222223333333333333…

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・URL）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、不特定多数の接続元（国）から複数のサイトに対して継続的に行われていました。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。

分類の対象外となった「その他の攻撃」も全体としては、3 番目の検出数になりました。
内訳は、図 2.1-C となり、WordPress の設定ファイル（**wp-config.php**）の読み取りを試みる攻撃が最も多いという結果になりました。WordPress のテーマやプラグインの脆弱性の悪用によるものが殆どで、攻撃の内容としてはディレクトリトラバーサルに分類されます。
その他、Joomla! リモートコード実行の可能性や PHP-CGI リモートコード実行（CVE-2012-1823）の検出が多く、これら 3 つの検出だけで 7 割以上を占めています。（※）
対象サービスでは、WordPress を中心とした CMS の利用者が多いため、WordPress のプラグインなどで使用されている timthumb.php の脆弱性悪用を含め、機械化された攻撃を多数検出していると推察されます。

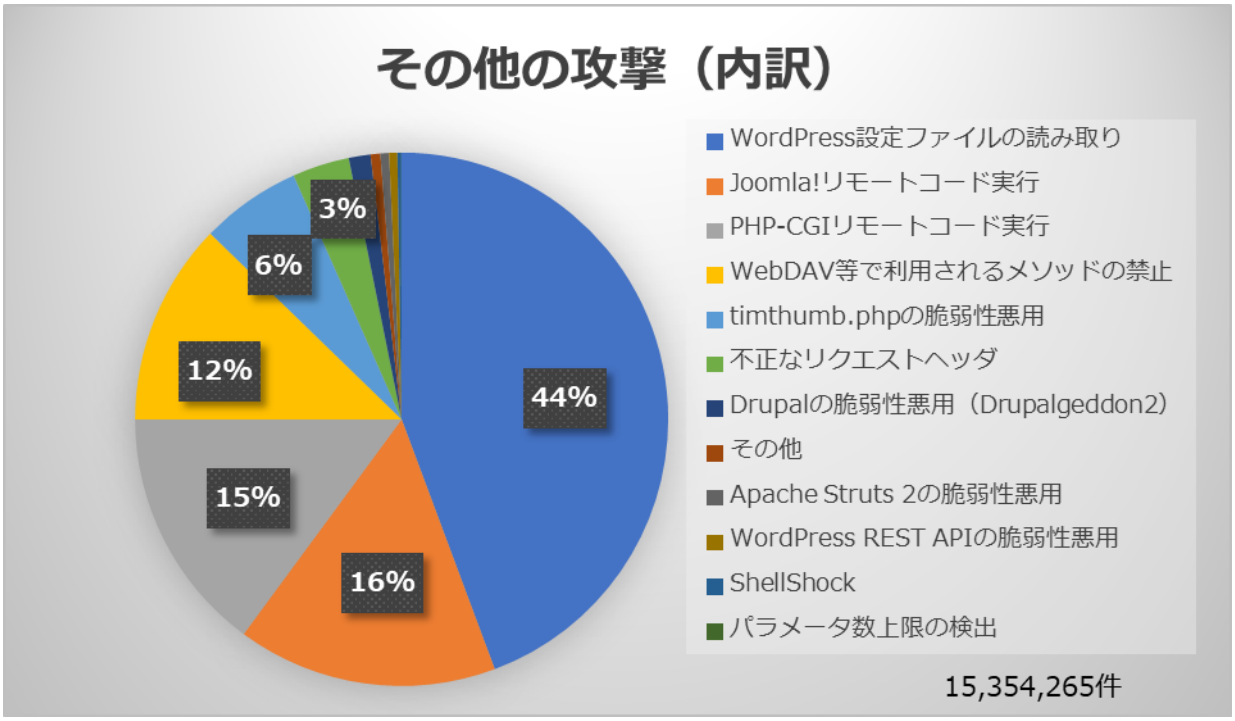

図 2.1-C その他の攻撃（内訳）

攻撃種別	検出した件数
WordPress 設定ファイルの読み取り	6,804,971
Joomla!リモートコード実行	2,423,300
PHP-CGI リモートコード実行	2,286,523
WebDAV 等で利用されるメソッドの禁止	1,883,740
timuthumb.php の脆弱性悪用	936,051
不正なリクエストヘッダ	530,635
Drupal の脆弱性悪用（Drupalgeddon 2.0）	202,541
その他	90,435
Apache Struts 2 の脆弱性悪用	80,501
WordPress REST API 脆弱性の悪用	76,807
ShellShock	35,957
パラメータ数上限の検出	2,804
合計	**15,354,265**

表 2.1-B その他の攻撃（内訳）

なお、CMS の **Drupal** の深刻な脆弱性として話題になった「Drupalgeddon 2.0」について、全体の割合から見ると少数であったものの、攻撃コードが公開された 4 月中旬以降の攻撃および検出の増加を確認しました。

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、1 月の検出が圧倒的に多く、2 月～6 月の検出数には大きな変化はありませんでした。

全体的に 1 月の検出数は多い傾向にありましたが、他の月と比べて倍以上の検出になったのは、「攻撃種別の分類（全体）」で述べたように、バッファオーバーフローに分類される攻撃が一定期間の間、大量に発生していたことが要因です。対象サービスにおいて実害はない状況でしたが、1 月だけで 1900 万件を超えるバッファオーバーフローの検出がありました。

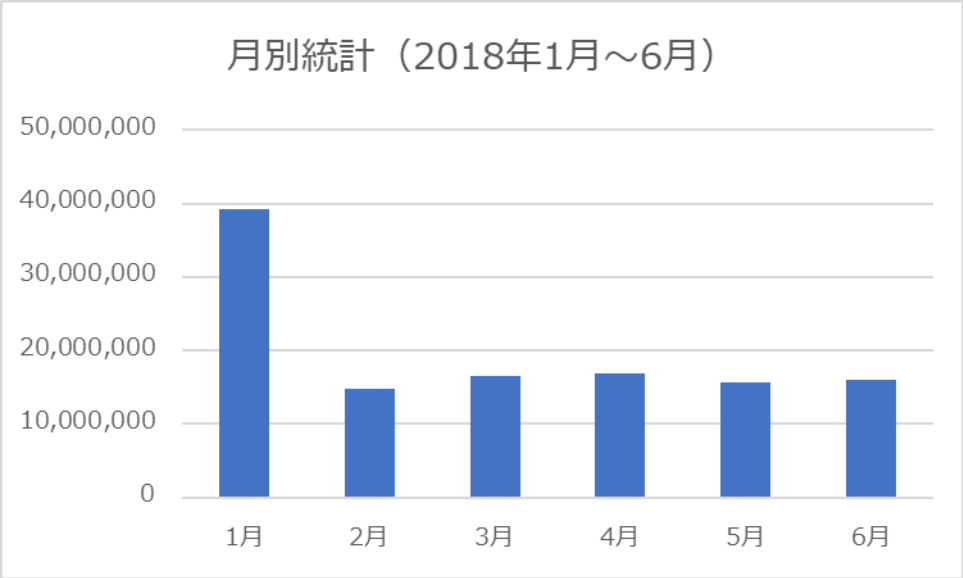

図 2.2-A 月別統計（グラフ）

集計対象（月）	検出した件数
2018 年 1 月	39,138,092
2018 年 2 月	14,764,284
2018 年 3 月	16,482,680
2018 年 4 月	16,819,621
2018 年 5 月	15,585,088
2018 年 6 月	15,969,526
合計	**118,759,291**

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、トップのアメリカ合衆国と２番目の日本で全体の３割を占めるという結果になりました。

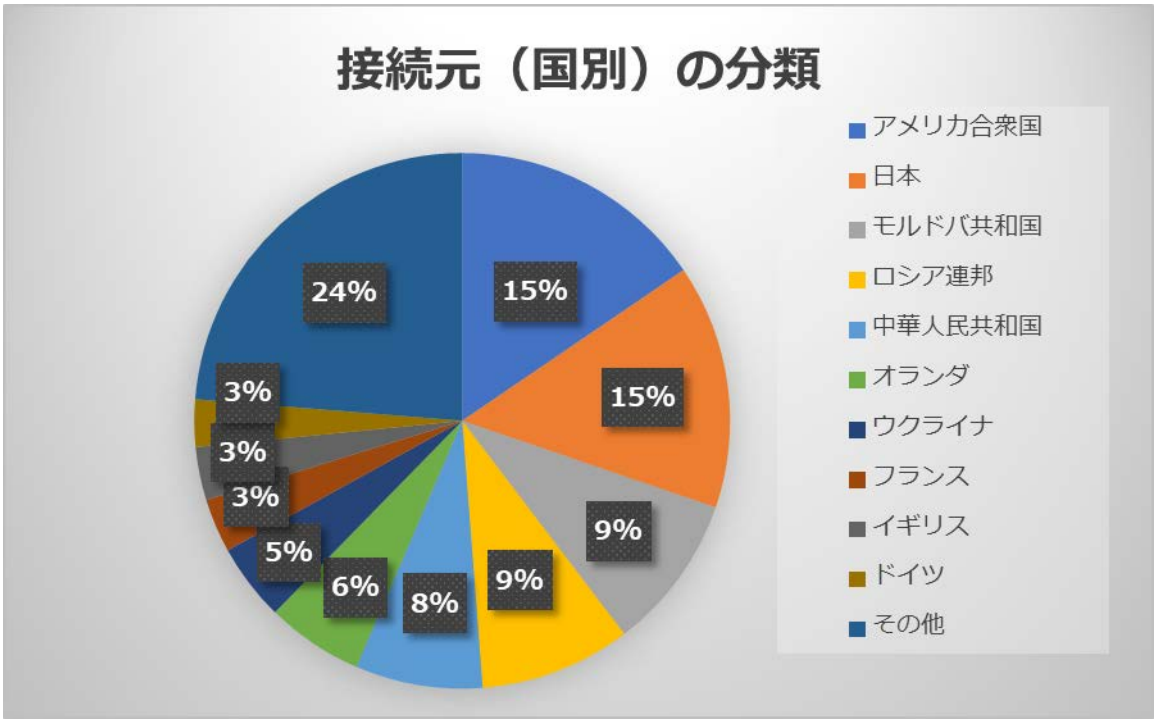

図 2.3 接続元（国別）の分類

	国名	検出した件数
1	アメリカ合衆国	18,389,925
2	日本	17,527,822
3	モルドバ共和国	11,174,984
4	ロシア連邦	10,841,525
5	中華人民共和国	9,127,587
6	オランダ	6,947,849
7	ウクライナ	5,523,645
8	フランス	3,869,755
9	イギリス	3,809,573
10	ドイツ	3,382,608
—	その他の国	28,164,018
	合計	**118,759,291**

表 2.3 接続元（国別）の分類

対象サービスのようなレンタルサーバーでは、CMS の管理画面など、攻撃を受けやすいページについて、海外 IP アドレスからのアクセスを禁止する機能が提供されていることがあります。前述の国別の分類のように、海外からの不正なアクセスは多いと考えられますので、有効活用すると良いでしょう。
（特定のページに対するセキュリティ強化策のため、海外からの通常アクセスに影響を及ぼすことはありません。）

3. WordPress に対する攻撃の検出傾向

攻撃の検出傾向（全体）**1 億 1876 万件（118,759,291）**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 **4 千万件以上（40,298,581）**ありました。

WordPress は、世界的に有名な CMS であり、CMS のシェアの大半を占めると言われています。

本レポートの集計対象のサービスでも、広く WordPress が有効活用されており、前回レポート（Vol.1）同様に、WordPress を対象とした攻撃の検出が多く、全体の約 3 分の 1 を占める結果になりました。

※ 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、全体の検出傾向と同様に SQL インジェクションが最も多く、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と合わせると 7 割を占めるという結果になりました。

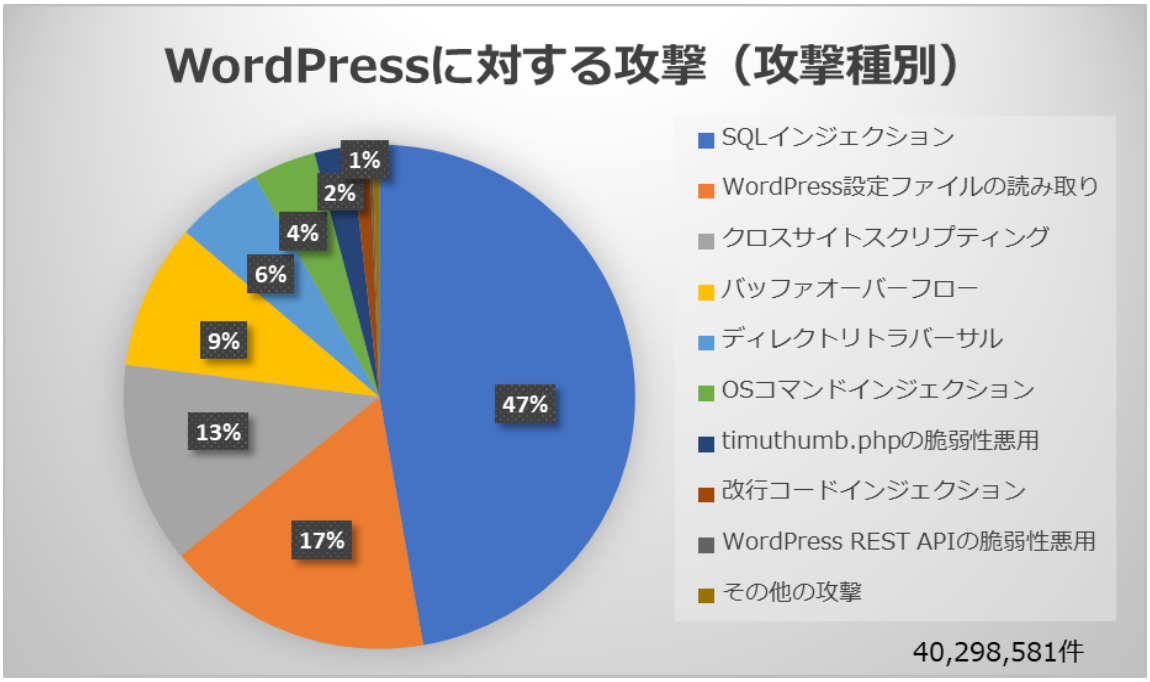

図 3.1-A WordPress に対する攻撃（攻撃種別）

攻撃種別	検出した件数
SQL インジェクション	19,043,060
WordPress 設定ファイルの読み取り	6,804,971
クロスサイトスクリプティング	5,193,242
バッファオーバーフロー	3,752,834
ディレクトリトラバーサル	2,241,196
OS コマンドインジェクション	1,612,352
timthumb.php の脆弱性悪用の可能性	432,079
改行コードインジェクション	471,240
WordPress REST API 脆弱性の悪用	76,807
その他	175,251
合計	**40,298,581**

表 3.1-A WordPress に対する攻撃（攻撃種別）

前回レポート（Vol.1）で取り上げた WordPress 4.7 / 4.7.1 の REST API 脆弱性を悪用した攻撃については、検出数が減少しています。外部から容易にコンテンツを改ざんできてしまうという深刻な脆弱性でしたが、特定バージョンの脆弱性であるほか、現状として該当するバージョンの WordPress が使用されるケースは少ないと思われますので、今後も検出数は減少していくと考えられます。

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、プラグインディレクトリの「**/wp-content/plugins/**」と「**xmlrpc.php**」での検出が多く、半数以上を占めています。このほか、テーマディレクトリの「**/wp-content/themes/**」、WordPress コア（本体）の「**/wp-includes/**」、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**」の順に検出数が多いという結果になりました。

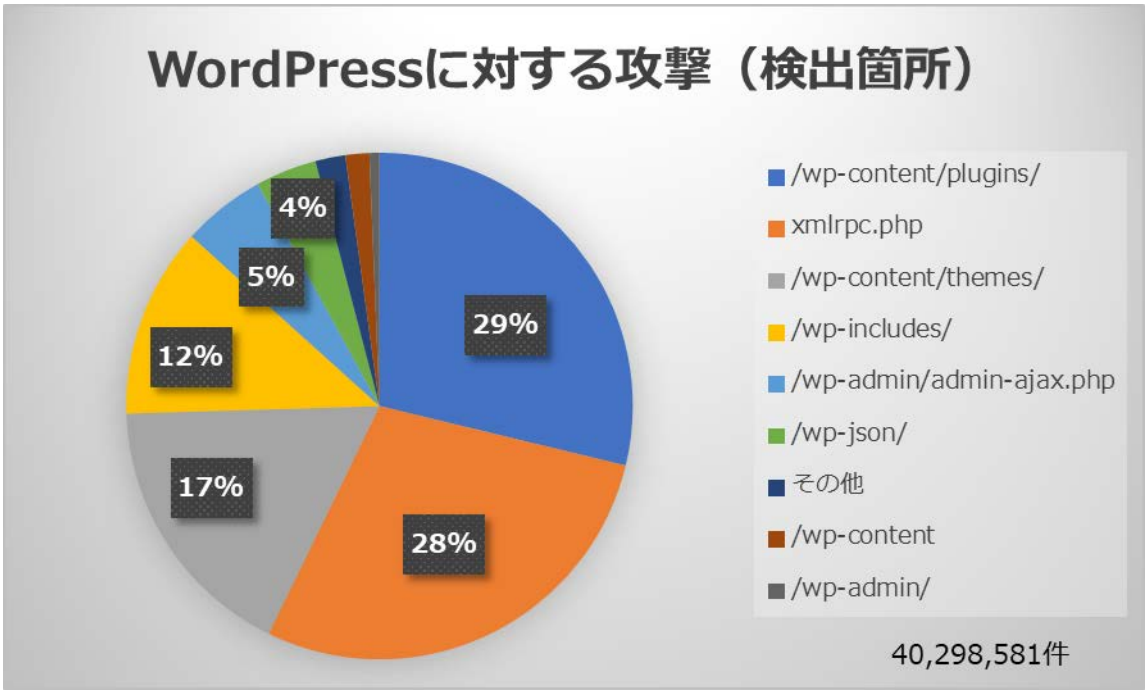

図 3.2-A WordPress に対する攻撃（検出箇所）

検出箇所	検出した件数
/wp-content/plugins/	11,594,027
xmlrpc.php	11,463,073
/wp-content/themes/	6,975,416
/wp-includes/	4,897,580
/wp-admin/admin-ajax.php	2,150,450
/wp-json/	1,573,074
その他	774,216
/wp-content/	611,788
/wp-admin/	258,957
合計	**40,298,581**

表 3.2-A WordPress に対する攻撃（検出箇所）

WordPress では、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、約 5 万 6 千となっています。
テーマ・プラグインなどの拡張機能は、WordPress の大きな魅力の一つですが、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。テーマ・プラグインを使用する際には、更新情報に気を配り、最新バージョンを使用するように心がけてください。

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標準で用意されていますが、DoS やブルートフォース攻撃に悪用されることがあり、本レポートの集計においても 1 月～3 月に xmlrpc.php での検出が増加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。
なお、xmlrpc.php を削除するという対策もありますが、WordPress のバージョンアップによって再度設置されてしまうため、継続的な対策ということを考えると、別の対策を実施した方が良いと考えられます。

WordPress のプラグインには、セキュリティ対策を目的としたプラグインもあります。
サーバーの設定ファイルや.htaccess によるアクセス制限に慣れていない場合は、xmlrpc.php のほか、管理ページ（/wp-admin/）のアクセス制限など、必要とする機能や運用方針に合ったセキュリティプラグインを有効活用することも検討してみてください。

図 3.2-B SiteGuard WP Plugin 設定例（XMLRPC 防御）

4. WordPress の脆弱性統計

2018 年 1 月 ～ 2018 年 6 月に確認された WordPress の脆弱性は、**本体 6 件**、**テーマ 4 件**、**プラグイン 100 件**で、**合計 110 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、発見される脆弱性の中でも比較的に多いとされるクロスサイトスクリプティングだけで半数を占める結果になりました。WordPress を対象とした攻撃の検出で多かったトラバーサル系については、1 件の脆弱性が見つかりました。

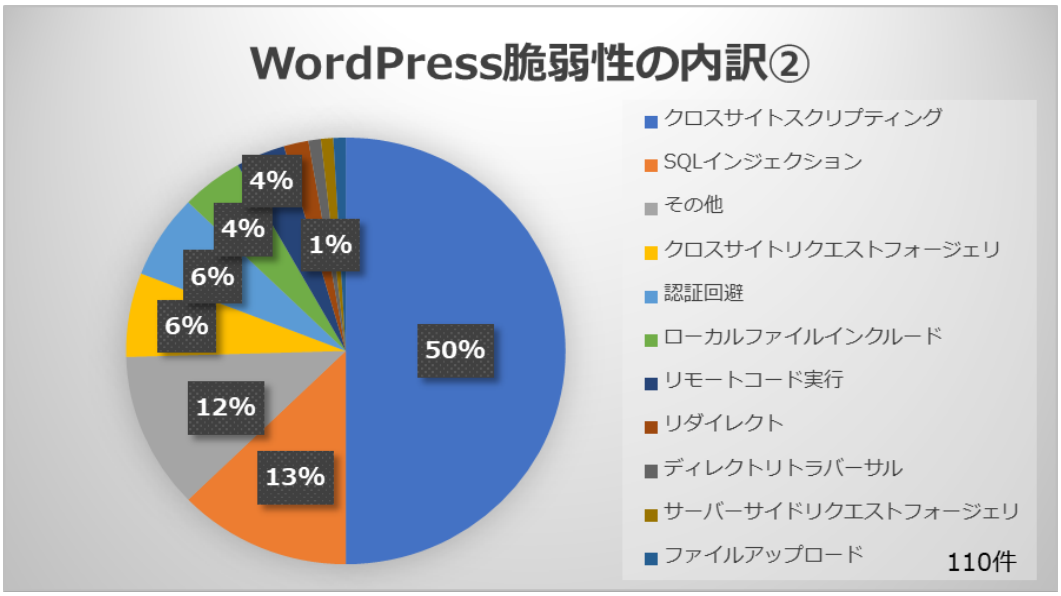

図 4-B WordPress 脆弱性の内訳②

脆弱性の種別	件数
クロスサイトスクリプティング	55
SQL インジェクション	14
その他	13
クロスサイトリクエストフォージェリ	7
認証回避	7
ローカルファイルインクルード	5
リモートコード実行	4
リダイレクト	2
ディレクトリトラバーサル	1
サーバーサイドリクエストフォージェリ	1
ファイルアップロード	1
合計	**110**

表 4-A WordPress 脆弱性の種別

当社で WordPress の脆弱性の情報収集を強化した 2015 年頃は、毎月 100 件ほどの脆弱性が発見されていた時期もありましたが、近年は減少傾向にあります。しかしながら、アクティブインストール数の多い人気プラグインで脆弱性が発見されることもあるため、ご利用の環境やプラグインの使用状況には十分な注意が必要です。本レポートの集計期間においても、アクティブインストール 300 万以上で、EC の機能を追加できる「WooCommerce」や写真や画像を使ったギャラリーを作成できる「NextGEN Gallery」、別の URL へのリダイレクト設定ができる「Redirection」など、利用者の多いプラグインで脆弱性が発見されています。また、高度なセキュリティ対策と DB バックアップの機能を持つ「iThemes Security」やブルートフォース対策の「Loginizer」といったセキュリティプラグインでも脆弱性が発見されました。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。

本体において発見された脆弱性では、下記の 2 点が話題となりました。

- /wp-admin/load-scripts.php に複数のパラメータ送信することで DoS が発生する問題
- 特定の権限を持つユーザーによって、任意のファイルを操作される脆弱性

いずれも目立った被害の報告はありませんが、攻撃コードが公開されており、注意が必要です。

/wp-admin/load-scripts.php に複数のパラメータ送信することで DoS が発生する問題：

「**load-scripts.php**」による DoS は、ネットワークやアクセス制御による対策の範囲であるという主旨の理由から、WordPress 側で脆弱性として認められなかったため、本件に関するセキュリティリリースはありませんでした。そのため、この問題については、今現在もその危険にさらされているサイトが存在している可能性が高いと考えられます。
load-scripts.php は、Javascript や css を読み込む機能で、実際には以下のようなリクエストで **load[]** パラメータを受け取ります。

```
https://ホスト名/wp-admin/load-scripts.php?c=1&load[]=common&ver=4.9.1
```

load[]パラメータには、カンマ区切りで複数のパラメータを指定することができるため、これを悪用して大量の読み込みを要求することで DoS が発生するという問題でした。（CVE-2018-6389）
前述のリクエスト例のように、load-scripts.php は、WordPress の管理ページ（/wp-admin/）の配下にあります。通常、管理ページのディレクトリ・ファイルには、ログインをしたユーザーでないとアクセスできませんが、load-scripts.php はログインページの認証なしでアクセスできる（外部からアクセスできる）点がこの問題のやっかいなところです。一つの有効な対策として、管理ページ（/wp-admin/）または、load-scripts.php のアクセス制限がありますので、セキュリティプラグインの有効活用などを含めて、WordPress のセキュリティ設定やアクセス制限を見直すことを推奨いたします。

図 4-C SiteGuard WP Plugin 設定例（管理ページアクセス制限）

特定の権限を持つユーザーによって、任意のファイルを操作される脆弱性：

外部から誰でも攻撃できる状態にはなく、特定の権限がないと攻撃を成立させることはできませんが、WordPress の設定ファイル（wp-config.php）の削除により、サイトを初期化されるなど、深刻な状態に陥る可能性があります。
この脆弱性については、2018 年 6 月末に公表され、WordPress 4.9.6 までのバージョンが対象となります。2018 年 7 月 5 日にリリースされた WordPress 4.9.7 で対策されています。

WordPress 本体の脆弱性の影響を受けないようにするためにも、最新バージョンを利用するように心がけてください。
更新情報の入手については、本体やテーマ・プラグインが更新されていることを通知する機能を活用することも有効です。WordPress 公式サイトの情報を参照することはもちろんですが、更新情報の入手を手助けするセキュリティプラグインがあります。

図 4-D SiteGuard WP Plugin 設定例（更新通知）

5. 定点観測

ここからは、当社のハニーポットによる定点観測ポイントのデータをもとに、不正アクセスの分類や攻撃の内容について見ていきます。

（協力：さくらインターネット株式会社、株式会社 KDDI ウェブコミュニケーションズ）

集計期間中（2018 年 1 月～2018 年 6 月）に定点観測ポイントで検出したアクセス数は、**99,303 件**でした。その多くはブルートフォースで、Tomcat Manager と WordPress のログインページで大半を占めています。このほか、/phpmyadmin、/PMA、/admin、/admin/assets/js/views/login.js などのディレクトリやファイルの存在を確認するサイトスキャンも多数検出しました。これらの不正アクセスは、ウェブサイトの運用において、よく見られる傾向ですが、中には D-Link や Linksys 製のルータ、QNAP Systems 製の NAS、Axis Communications 社のネットワークカメラといったネットワーク機器などの脆弱性悪用を目的とした調査・実行のアクセスもありました。

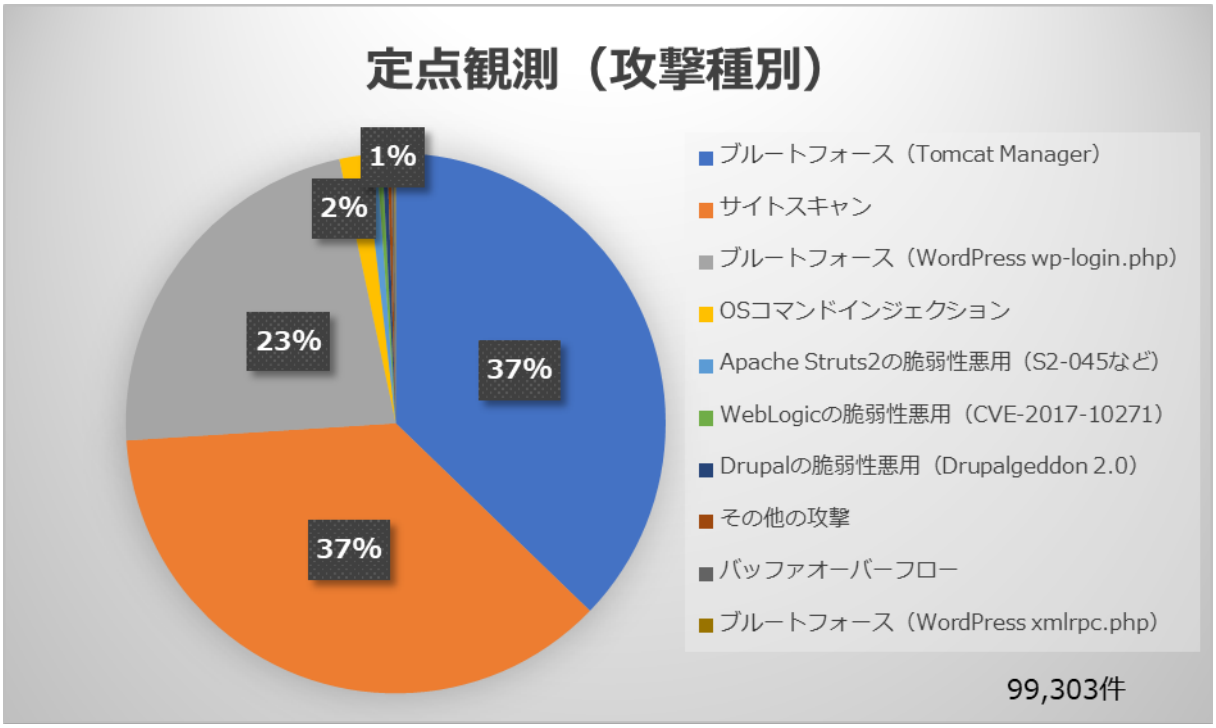

図 5-A 定点観測（攻撃種別）

攻撃種別	検出した件数
ブルートフォース（Tomcat Manager）	36,957
サイトスキャン	36,516
ブルートフォース（WordPress wp-login.php）	22,502
OS コマンドインジェクション	1,501
Apache Struts2 の脆弱性悪用（S2-045 など）	699
WebLogic の脆弱性悪用（CVE-2017-10271）	323
Drupal の脆弱性悪用（Drupalgeddon 2.0）	309
その他	225
バッファオーバーフロー	188
ブルートフォース（WordPress xmlrpc.php）	83
合計	**99,303**

表 5-A 定点観測（攻撃種別）

Apache Struts2 の脆弱性悪用については、2017 年 3 月に S2-045 による大規模な情報漏洩のインシデントが多発するなど、大きな話題になりました。全体の割合としては少ないものの、定点観測において今現在でも検出しています。
Oracle WebLogic Server の脆弱性悪用については、2017 年 10 月に報告された CVE-2017-10271 を悪用し、任意のコードを実行する攻撃の調査・実行のアクセスを検出しています。2018 年 1 月に入ってから該当の脆弱性を悪用する攻撃の増加があり、マイニングに悪用される事例が確認されるなど、多くの注意喚起や報道がありました。

集計期間中に観測した攻撃としては、Drupal の脆弱性悪用（Drupalgeddon 2.0）も大きな話題となりましたので、脆弱性の内容のほか、観測したデータをもとにまとめます。

Drupal リモートコード実行の脆弱性（Drupalgeddon 2.0）：

【脆弱性の影響を受けるバージョン】

Drupal 8.5.1 より前のバージョン

Drupal 7.58 より前のバージョン

※サポートが終了しているバージョン 6 系や 8.4 系にも影響あり

【影響】

外部からの任意のコード実行（リモートコード実行）

※非公開情報の搾取やシステムの改変などの被害を受ける可能性あり

本脆弱性については、「極めて重大な脆弱性」と位置付けられ、2018 年 3 月 21 日に Drupal からセキュリティアップデートに関する事前の予告がありました。ゼロデイの可能性や情報の公開から数時間、数日中には攻撃が発生するという見方もありましたが、2018 年 3 月 28 日のアップデートリリース直後は、攻撃コードの公開や攻撃発生に関する情報はありませんでした。しかし、2018 年 4 月 12 日に脆弱性に関する解析結果と攻撃コードが公開されたことをきっかけに、攻撃フェーズに入るという大きな動きがありました。（CVE-2018-7600）

本脆弱性は、2014 年の 10 月に同じく「極めて重大な脆弱性」として発見された Drupal の SQL インジェクションの脆弱性（CVE-2014-3704）Drupalgeddon に続き、Drupalgeddon 2.0 と呼ばれています。（極めて重大な脆弱性というインパクトから、ドルーパル（Drupal）とアルマゲドン（Armageddon）で、Drupalgeddon と呼ばれるようになったと言われています。）
さらに、ゴールデンウィーク直前の 2018 年 4 月 28 日には、本脆弱性と関連し、悪用されるリスクが高い脆弱性として Drupal から新たにセキュリティアップデートがありました。（CVE-2018-7602）
本レポートの執筆時点においても、一連の脆弱性を悪用した攻撃による仮想通過発掘を目的とした Drupal サイトのボット化などの情報が入っています。

日時	内容	備考
2018 年 3 月 21 日	Drupal より、セキュリティアップデートについて事前の告知があった。	
2018 年 3 月 28 日	セキュリティアドバイザリ(SA-CORE-2018-002) が公開され、対策済みのバージョンがリリースされる。	CVE-2018-7600
2018 年 4 月 12 日	脆弱性に関する解析結果と攻撃コードが公開され、攻撃フェーズに入る。 （以降、本レポート集計の対象サービスおよび定点観測においても攻撃を検出し始める。）	
2018 年 4 月 28 日	CVE-2018-7600 と関連し、悪用されるリスクの高い脆弱性として、新たにセキュリティアドバイザリ (SA-CORE-2018-004) が公開され、対策済みのバージョンがリリースされる。	CVE-2018-7602

表 5-B Drupalgeddon 2.0 に関するタイムライン

実際の攻撃リクエスト（Drupal 8 系）の例を見ていきます。
リクエストのパスは、**/user/register** となっており、標準で用意されているアカウント作成ページが対象になっています。

```
POST /user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax HTTP/1.1
Host:XXX.XXX.XXX.XXX:80
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) ・・・
Connection: close
Content-Length: 169
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

_drupal_ajax=1&_drupal_ajax=1&form_id=user_register_form&mail%5B%23markup%5D=echo+Name%3A+%24%28id+-u+-n%29+&mail%5B%23post_render%5D%5B%5D=exec&mail%5B%23type%5D=markup
```

要求本文をデコードした内容です。

```
_drupal_ajax=1&_drupal_ajax=1&form_id=user_register_form&mail[#markup]=echo Name: $(id -u -n) &mail[#post_render][]=exec&mail[#type]=markup
```

本脆弱性については、情報が公開された当初のパッチの内容から、**#**で始まるパラメータが影響を及ぼすということが予想されていました。（※1）
実際に、バリデーションの制限が緩いとされた mail パラメータを細工し、**#post_render** に実行する関数、**#markup** にコマンドを挿入することで、外部から任意のコードを実行する攻撃コードが公開されています。（※2）
この例では、id コマンドによってユーザー名を表示していますが、wget コマンドによってファイルをダウンロードしたり、ファイルを書き換えたりするパターンもあります。

※1
https://github.com/drupal/drupal/commit/19b69fe8af55d8fac34a50563a238911b75f08f7#diff-7bff52b3a152bd658c6b6ec3f48c13fdR87
※2
https://www.exploit-db.com/exploits/44448/

なお、攻撃リクエストは一例です。
前述のパターンは、アカウント作成の機能を無効にしていれば攻撃の影響を受けないと思われますが、攻撃経路は複数存在すると考えられますので、対策済みバージョンへのアップデートが必要となります。

本件にかぎらず、非公開情報の搾取やシステムの改変などの被害に遭う恐れのあるリモートコード実行の脆弱性については、十分な注意が必要です。
WordPress や Drupal といった CMS のほか、Apache Struts2 などのフレームワークをご利用の場合は、運用中のサイトのバージョン管理を徹底し、脆弱性に関する情報を収集するようにしてください。

これらの脆弱性への対応について、運用面での対策として **WAF**（ウェブアプリケーションファイアウォール）を活用するのも有効です。WAF により、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、防御することができます。

6. おわりに

前回レポート（Vol.1）に引き続き、CMS を中心とした検出傾向や攻撃事例について、報告させていただきました。本レポートの内容がセキュリティを身近なこととして捉えるきっかけとなり、また皆様のウェブサイトのセキュリティ対策の一助となれば幸いです。

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**」 **～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 海外アタックガード：全プラン標準実装

サービス名	GMO クラウド株式会社「**WADAX 共用サーバー**」 **～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。

- ハニーポット
  “おとり”として、攻撃者からの不正アクセスを受けることに意味を持つシステムのこと。
  あえて攻撃者からの不正アクセスを受けることによって、ウェブサイトへの攻撃手法や攻撃傾向を把握することが可能となる。マルウェアの検体入手等でも活用される。

- 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。

- Drupal（ドルーパル）
  PHP で開発されているオープンソースの CMS（Content Management System）。
  日本でのシェアはそれほど高くないと言われているが、WordPress や Joomla!と一緒に三大 CMS と呼ばれることがある。

- WordPress（ワードプレス）
  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

【データ分析】

株式会社ジェイピー・セキュア　佐藤 貴章

【協力者】

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

さくらインターネット株式会社

株式会社 KDDI ウェブコミュニケーションズ

株式会社レオンテクノロジー

JP-Secure Labs Report Vol.2

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 580 ソリッドスクエア 東館 6F

TEL：044-201-4036（代表）　FAX：044-201-4037

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

※　本レポートに記載されている製品・サービス名、社名は各社の商標または登録商標です。