Penta SECURITY
TRUST FOR AN OPEN SOCIETY

Webアプリケーション脅威解析報告書

：2015年下半期

目次

はじめに

Web脅威の動向のサマリー

Web攻撃動向の解析

1. WAPPLESルールによる検知Top10
2. OWASP 2013基準Web攻撃類型Top10
3. Web攻撃発信国Top 5
4. Web攻撃の目的
5. WAPPLESルール別危険度
6. Web攻撃の月次推移

付録

1. WAPPLESルールによる対応
    1) OWASP 2013に対応するWAPPLESルール
    2) 危険度に対応するWAPPLESルール
    3) Web攻撃の目的に対応するWAPPLESルール
2. WAPPLESルールの紹介
3. Black List Top30

はじめに

本報告書では、ペンタセキュリティシステムズ株式会社(韓国本社)のWebアプリケーションファイアウォール(WAF : Web Application Firewall)であるWAPPLESより収集された検知ログの統計情報から、当社のICS(Intelligent Customer Support)のシステムを採用し解析した攻撃動向を記載しています。

本報告書の作成目的は、検知ログの統計データより解析されたWeb攻撃動向の情報を共有および提供することでWAPPLESを導入して頂いているお客様に、より高いレベルのセキュリティサービスを提供することにあります。

本報告書では、Web攻撃動向を次のように各カテゴリに分けて解析しており、WAPPLESの26の検知ルールとその危険度、OWASP2013の脆弱性TOP10、攻撃の発信国、攻撃を実行する目的、攻撃の月次推移等にあわせたデータおよび解析結果を提示しています。その他、WAPPLESの26の検知ルールに対し、OWSAP 2013脆弱性、危険度、Web攻撃を実行する目的にマッピングしたテーブルを提供することで、最近の攻撃の推移をより解りやすく理解して頂けるように致します。

本報告書で採用している検知ログの統計データは、官公署を除外した、検知ログの統計情報の収集および利用に同意したお客様、全1,064のWAPPLESに対し2015年7月1日から2015月12月31日までの期間のデータを基準とします。当該データには、検知ログの統計データのみであり、個人情報およびWAPPLESの保護対象の情報等は一切含まれていません。

Web脅威の動向のサマリー※

2015年上半期では、攻撃危険度は「緊急」であり、脆弱性スキャンを目的とした攻撃が最も多く見られていました。(WAPPLESルール別危険度の「緊急」の攻撃は35%、Web攻撃の目的の脆弱性スキャンの攻撃は、34%)
脆弱性スキャンを目的とした攻撃は、2015年上半期にも検知件数が約4億万件に達し、引き続き、同年下半期にも攻撃検知件数でトップとなりました。危険度の「緊急」レベルの攻撃は、データの消失、又は破壊、サーバの乗っ取り、管理者権限の奪取等の被害を及ぼす恐れがあります。サーバ管理者およびセキュリティ担当者は、定期的な脆弱性診断およびセキュリティポリシーの見直しを行い、2次被害を阻止することが求められます。

OWASP Top 10 (2013) 基準では、サーバサイドのスクリプト内のInclude関数を用いてWebサイト改ざんやサーバ運用妨害を引き起こすインジェクション(Injection)攻撃がトップとなりました。当該脆弱性を突いた攻撃は、攻撃難易度に比べて、その結果がシステムに非常に深刻な影響を与えるため、適切な対策を設けなければなりません。インジェクションの次に多かった脆弱性は、不適切なセキュリティ設定(Security Misconfiguration)です。当該脆弱性を突いた攻撃により、セキュリティ設定上のミスを悪用し、システムの管理者権限を奪取し、システム全体を乗っ取ることができます。

特に、機密データの流出と関連した攻撃の中ではWebサイトを介しdll、conf、ini等のファイルにアクセスを試み、システム構成情報を漏えいする攻撃があり、エクステンションフィルタリング(ExtensionFiltering)ルールにより最も多く検知されました。また、脆弱性スキャンの場合、自動化された攻撃ツールを採用し、不正なリクエストを発行し、そのレスポンスを以て脆弱性を把握するという試みがあり、インバリッドHTTP(InvalidHTTP)ルールにより最も多く検知されました。このような類の攻撃が成功した場合、Webサイトの脆弱性情報の露出、Webサーバの動作不能、機密情報漏えいに直結しますので、その対策に細心の注意を払うとともにWAPPLESポリシー設定を、(エクステンションフィルタリング(ExtensionFiltering)-「安全な形式のみアクセス可能」)にすることを推奨します。

< 2015年下半期（2015.07.01~2015.12.31）のWAPPLESの検知統計情報サマリー >

Web攻撃の目的	割合
1位　脆弱性スキャン	34%
2位　Webサイト改ざん	26%
3位　サーバ運用妨害	17%

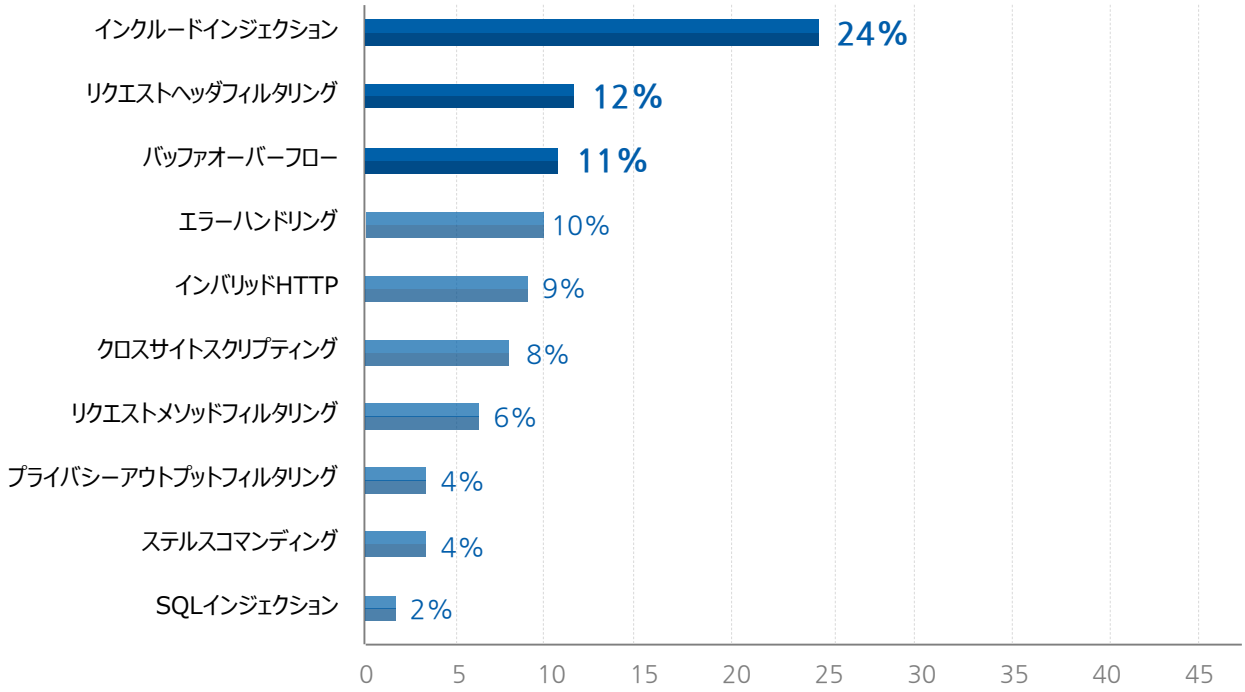
検知ルール	割合
1位 インクルードインジェクション	24%
2位 リクエスト ヘッダ フィルタリング	12%
3位 バッファ オーバーフロー	11%

危険度	割合
緊急	35%
高	29%
中	24%
脆弱性の下調べ	12%

※　詳細は、Web攻撃動向の解析を参考にしてください

Web攻撃動向の解析

1. WAPPLESルールによる検知Top10



本グラフは、WAPPLES検知ルール別に発生しているアラートの頻度を出力しています。2015年7月1日から2015年12月31日までの間、インクルードインジェクション(Include Injection)ルールにより最も多く検知され、その次がリクエストヘッダフィルタリング(Request Header Filtering)、バッファオーバーフロー(Buffer Overflow)の順となっています。当該攻撃は、危険度が「緊急」、「高」の攻撃であり、攻撃に成功した場合、ターゲットになるシステムに大きな被害を及ぼす恐れがあります。

▶ **インクルドインジェクション**(Include Injection)は、悪意のあるコードをアップロード後、Include関数を採用しコードを実行することにより、別なWebサイトや内部のファイルへ移動させる攻撃です。通常のテキスト形式のファイルに見せかけ、Webshellをアップロードし、管理者権限を奪取することができるため、非常に危険度の高い攻撃であり、必ず対策を講じなければなりません。

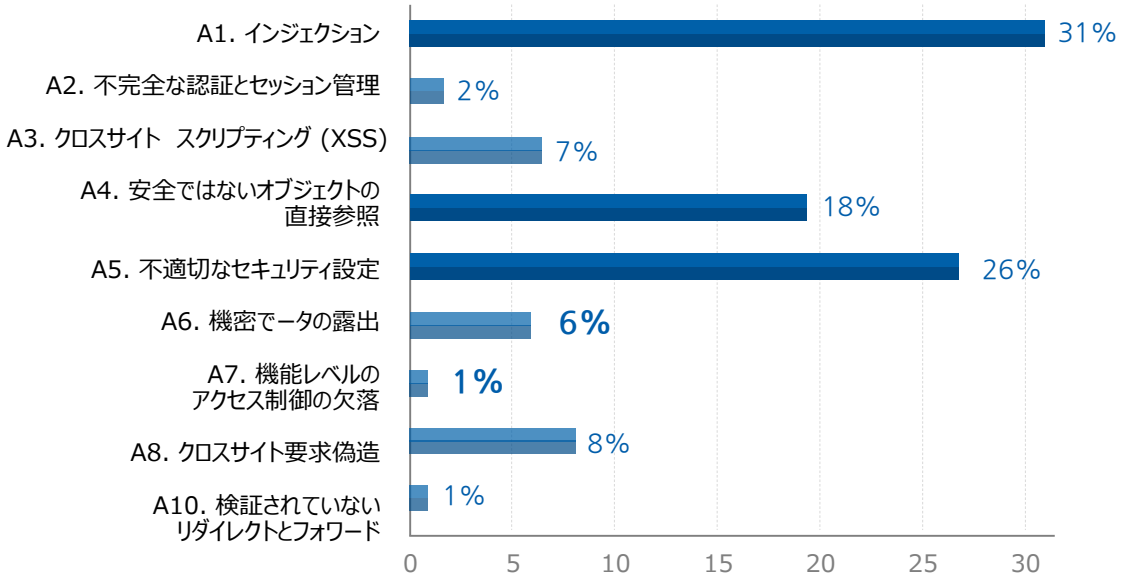
▶ **リクエストヘッダフィルタリング**(Request Header Filtering)は、Webブラウザからの正常なHTTPリクエストではないヘッダに必須要素が欠けており、不正なリクエスト(自動化された攻撃ツールからのリクエスト等)を検知します。

▶ **バッファオーバーフロー**(Buffer Overflow)は、ハッカーにより通常のメモリサイズを超える長い文字列がサーバに送り込まれ、遠隔コード実行やサービス拒否、メモリアクセスエラーなどを引き起こす試みです。プログラムの正常動作を妨げたり、特定のコマンドを行ったりするなどの危険な試みであるため、必ず対応が必要です。

WAPPLESルール	検知件数(件)
インクルードインジェクション(Include Injection)	400,159,339
リクエストヘッダフィルタリング(Request Header Filtering)	201,646,723
バッファオーバーフロー(Buffer Overflow)	178,920,781
エラーハンドリング(Error Handling)	172,610,037
インバリッドHTTP(Invalid HTTP)	147,768,779
クロスサイトスクリプティング(Cross Site Scripting)	124,988,607
リクエストメソッドフィルタリング(Request Method Filtering)	101,429,413
プライバシーアウトプットフィルタリング(Privacy Output Filtering)	72,687,079
ステルスコマンディング(Stealth Commanding)	70,687,268
SQLインジェクション(SQL Injection)	27,194,111

< 表1. WAPPLESルールによる検知Top 10 >

2. OWASP 2013基準Web攻撃類型Top10



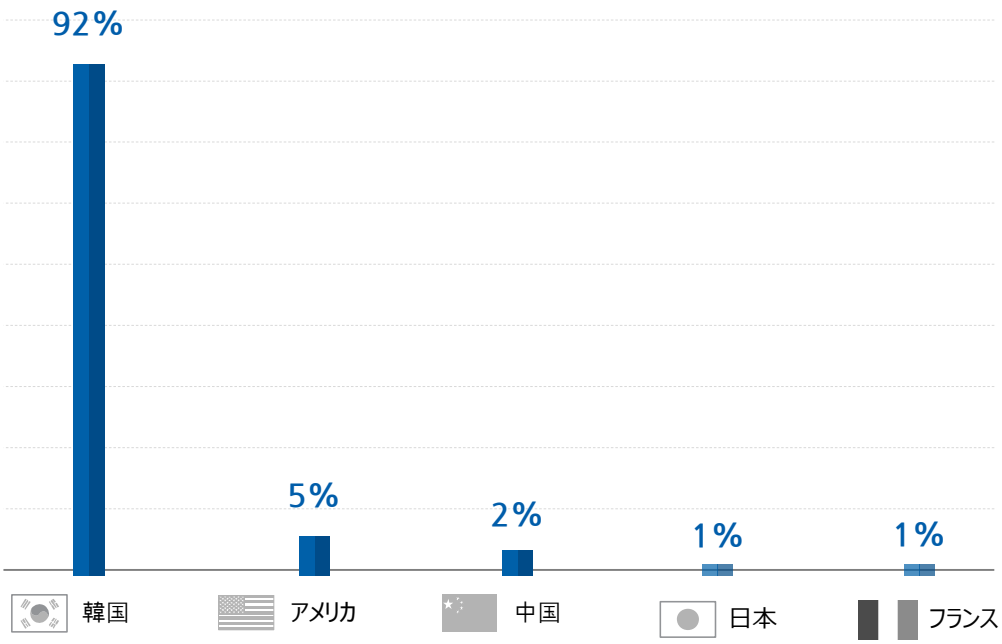
本グラフは、WAPPLES検知ルールにより発生したアラート情報を、OWASP Top 10に照らし合わせ、攻撃を類型化しています。2015年7月1日から2015年12月31日までの間、インジェクション(Injection)攻撃が最も多く発生し、その次に不適切なセキュリティ設定(Security Misconfiguration)の順となっています。

インジェクション(Injection)は、OWASP Top 10リスクのA1に該当するセキュリティ脅威です。テキスト基盤の試みが容易にでき、ほぼすべてのデータソースをインジェクションのパスとして活用できることから、比較的簡単に攻撃の試みが可能です。これらの攻撃は攻撃難易度は高くない反面、攻撃が成功した場合、データ消失や破壊、サービス拒否といった致命的な被害につながる恐れがあるため、適切なセキュリティ対策を設けることを推奨致します。

OWASP Top 10 Web Application Security Risks 2013	検知件数(件)
A1. インジェクション(Injection)	513,969,677
A2. 不完全な認証及びセッション管理(Broken Authentication and Session Management)	27,989,723
A3. クロスサイトスクリプティング(Cross Site Scripting : XSS)	124,988,607
A4. 安全ではないオブジェクトの直接参照(Insecure Direct Object References)	302,940,493
A5. 不適切なセキュリティ設定(Security Misconfiguration)	432,223,576
A6. 機密データの露出(Sensitive Data Exposure)	106,683,701
A7. 機能レベルのアクセス制御の欠落(Missing Function Level Access Control)	18,420,330
A8. クロスサイト要求偽造(Cross Site Request Forgery : CSRF)	140,917,566
A10. 未検証のリダイレクトとフォーワード(Unvalidated Redirects and Forwards)	16,654,996

< 表2. OWASP 2013基準Web攻撃類型Top10 >

3. Web攻撃発信国Top5



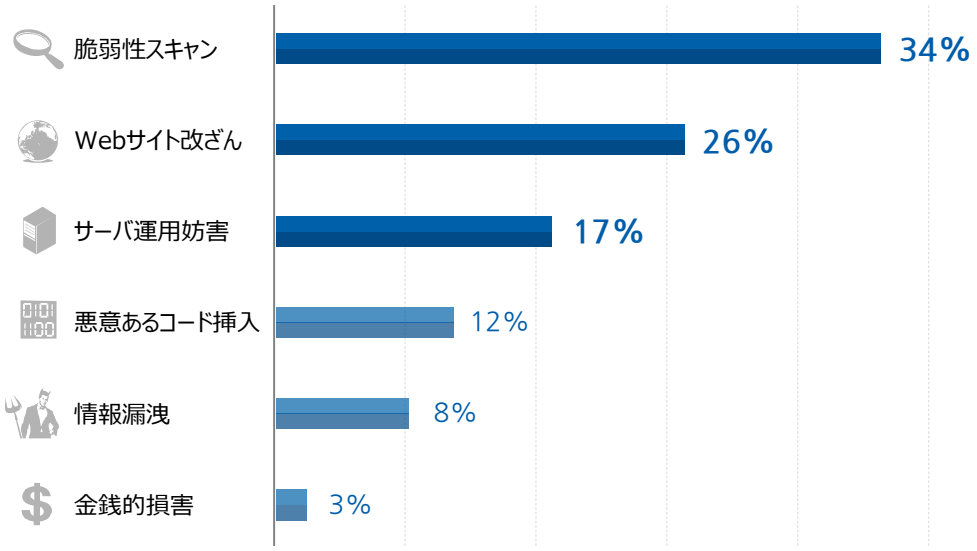
本グラフは、WAPPLES検知ルールにより発生したアラートを発信元アドレスに基づいて国別に分類し、頻度の高い攻撃発信国を出力しています。2015年7月1日から2015年12月31日までの間、韓国が最も頻度の高い攻撃発信国であり、その次が、アメリカ、中国の順となっています。

Web攻撃発信国Top5	検知件数(件)
韓国	861,671,567
アメリカ	96,831,598
中国	42,842,597
日本	22,394,306
フランス	11,625,407

< 表3. Web攻撃発信国Top 5 >

※　本報告書の解析対象としているデータは、韓国国内のサーバを保護対象としたWAPPLESに限定されているため、本攻撃発信国のランキングには全世界における攻撃の動向が反映されていることではありません。

4. Web攻撃の目的



本グラフは、WAPPLES検知ルールにより発生したアラートを、その実行の目的別に分類し、頻度を出力しています。2015年7月1日から2015年12月31までの間、脆弱性スキャンを目的とした攻撃が約5億5千万件（全体攻撃の34%）と最も多く検知されており、その次にWebサイト改ざん、サーバ運用妨害の順となっています。特に脆弱性スキャンの場合、前年同期比、約2億5千万件ほど増加したことが確認されました。インバリッドHTTP(Invalid HTTP)、ディレクトリ リスティング(Directory Listing)、エラーハンドリング(Error Handling)のような脆弱性スキャンを目的とした攻撃は、2次攻撃のための準備過程であるため、さらなる被害が引き起こされる前段階での対策が求められます。

▶ **脆弱性スキャン**は、自動化された攻撃ツールを用い、HTTP定義ではない不正なリクエスト(要求)およびレスポンス(応答)を返す(インバリッドHTTP)、RFC定義ではない不正なURIをリクエスト(要求)する(インバリッドURI)、Webサイトのディレクトリ構造を漏洩する(ディレクトリリスティング)、意図的にエラーメッセージを表示させる(エラーハンドリング)等を行い、Webサイトの脆弱性を洗い出す攻撃のための事前調査です。

▶ **Webサイト改ざん**は、特定のWebページを改ざんする(Webサイト改ざん)、SQLサーバにて実行されるコードに悪意あるコードを挿入して権限のないユーザが情報を取得するか操作する(SQLインジェクション)、Webサーバにて実行可能な.exe、.jsp、.phpなどのファイルをWebサーバにアップロードする(ファイルアップロード)、悪意あるスクリプト、ファイル、コードを挿入する(インクルードインジェクション)等、権限のないユーザが無断でWebサイトを修正・操作することです。

▶ **サーバ運用妨害**は、Webサーバの正常運用を妨害することであり、不正な実行コードにより内部のバッファを超えるようにする(バッファオーバープロー)、リクエスト(要求)にて必要以上のメソッドおよびヘッダを送り付ける等の攻撃があります。

▶ **悪意あるコード挿入**は、サーバの脆弱性を突いたTrojan、ウィルス等の不正なコードを挿入することであり、悪意あるスクリプトコードを挿入することによってユーザ情報を出力させる(クロスサイトスクリプティング)、サーバサイドスクリプトを挿入して悪意あるコマンドを実行し情報を取得する(ステルスコマンディング)、不正なアクセスにて悪意あるコードを送り付ける(不正アクセス)等の試みです。

▶ **情報漏洩**は、Webサイトに対し、住民登録番号(韓国)やクレジットカード番号のような個人情報を入力し漏洩する(プライバシーインプットフィルタリング、プライバシーアウトプットフィルタリング)または、個人情報の含まれているファイルをアップロードする(プライバシーファイルフィルタリング)等、ユーザの個人情報を不正に取得することです。

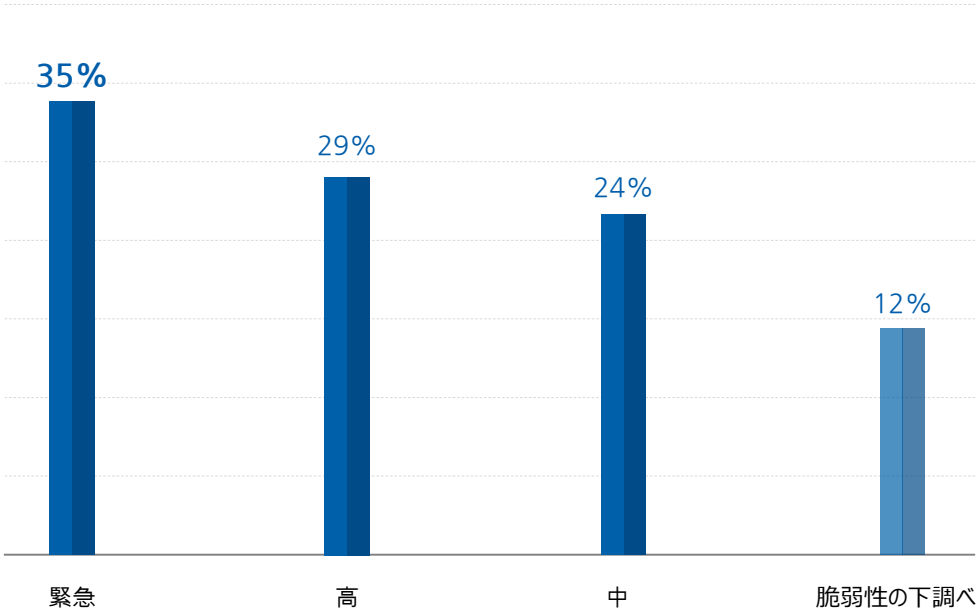
▶ **金銭的損害**は、認証プロセスを迂回するためにクッキー(ユーザの端末PCに保存されている個人情報)を改ざんし、攻撃を行うことにより、他のユーザ情報を取得し、そのユーザになりすます(クッキーポイズニング)、不正なパラメータを挿入しアプリケーション動作を妨害する(パラメータタンパリング)等、ユーザに対し金銭的損害を及ぼすことです。

Web攻撃の目的	検知件数(件)
脆弱性スキャン	557,082,024
Webサイト改ざん	430,875,510
サーバ運用妨害	282,142,686
悪意あるコード挿入	195,675,875
情報漏洩	131,376,995
金銭的損害	42,126,190

< 表4. Web攻撃の目的 >

※ Web攻撃の目的に対応するWAPPLESのルールについては、「WAPPLESルールによる対応 – 3. Web攻撃の目的に対応するWAPPLESルール」をご参考ください。

5. WAPPLESルール別危険度



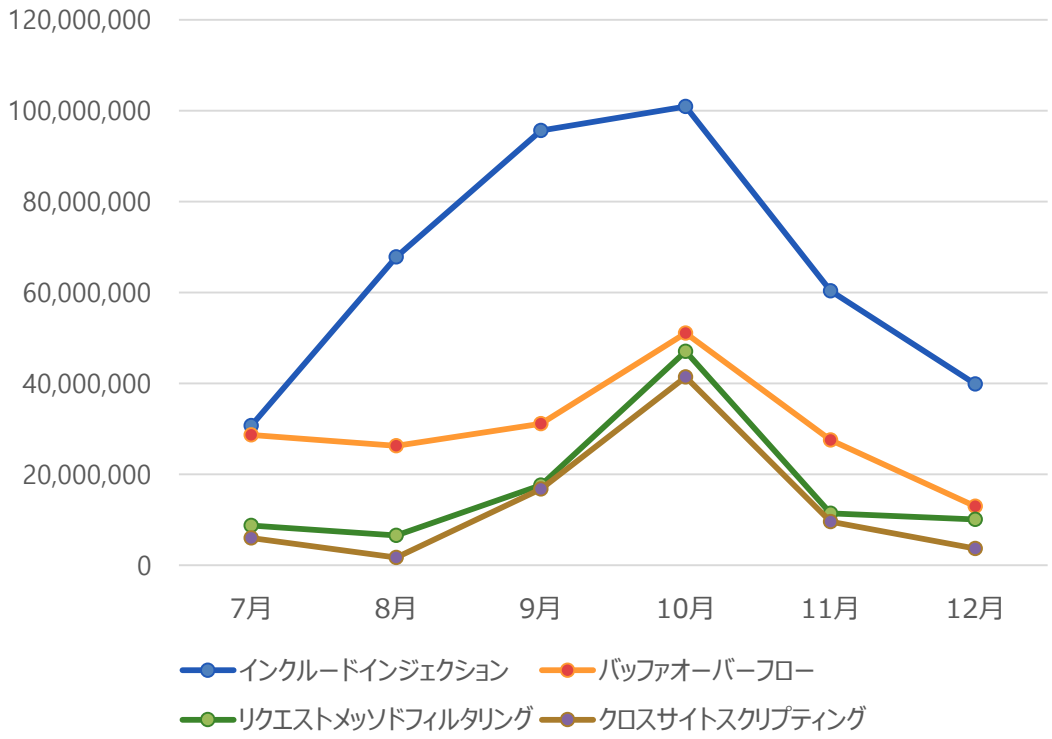
本グラフは、WAPPLESルールを対応への早急性に照らし合わせ、緊急、高、中、脆弱性の下調べといった危険度にて分類し、攻撃の発生頻度を出力しています。2015年7月1日から2015年12月31日までの間、緊急レベルが最も頻度が高く、その次が高、中の順となっています。

WAPPLESルール別危険度	検知件数(件)
緊急	570,727,797
高	462,256,179
中	388,423,218
脆弱性の下調べ	186,638,774

< 表5. WAPPLESルール別危険度 >

※　WAPPLESルールの危険度は、OWASP Top10を基準とし当社にて分類したレベルです。
　　詳細は、「WAPPLESルールによる対応－2. 危険度に対応するWAPPLESルール」をご参考ください。

6. Web攻撃の月次推移



本グラフは、対応への早急度の高い４つの攻撃に対しての月次の推移を出力しています。2015年下半期では、同年度上半期の分析結果で3位だったインクルードインジェクション(Include Injection、悪意のあるコードをアップロード後、Include関数を採用してコードを実行することにより、別なWebサイトや内部のファイルへ移動させる試み)が最も多く発生しました。その次にバッファオーバーフロー(Buffer Overflow、通常のメモリサイズを超える長い文字列をサーバに送り込み、遠隔コード実行やサービス拒否、メモリアクセスエラー等を引き起こす試み)の順となっています。これらの攻撃は攻撃難易度は高くない反面、攻撃が成功した場合、プログラム誤作動やWebサービス提供不能状態、機微情報の漏えい等致命的な被害につながる恐れがあるため、適切なセキュリティ対策を設けることを推奨致します。

危険度の高い攻撃	7月	8月	9月	10月	11月	12月
インクルードインジェクション (Include Injection)	30,677,045	67,778,168	95,643,805	100,891,097	60,358,430	39,888,637
					Total	**395,237,182**
バッファオーバーフロー (Buffer Overflow)	28,695,062	26,239,220	31,117,417	51,031,081	27,541,422	12,969,397
					Total	**177,593,599**
リクエストメソッドフィルタリング (Request Method Filtering)	8,753,751	6,556,798	17,603,864	47,013,642	11,429,200	10,103,742
					Total	**101,460,997**
クロスサイトスクリプティング (Cross Site Scripting)	6,003,376	1,690,993	16,769,684	41,400,916	9,556,080	3,666,566
					Total	**79,087,615**

< 表6.「 緊急」レベルの月次推移>

付録

1. WAPPLESルールによる対応

1) OWASP 2013に対応するWAPPLESルール

OWASP(Open Web Application Security Project)では、Webアプリケーションセキュリティ上で発生頻度が高く、他にも影響を及ぼす恐れのあるWeb脆弱性に関する報告書を作成しています。以下の表では2013年度OWASPが発表した10代脆弱性とこれに対応するWAPPLESルールを切り分けて表示しました。

NO.	OWASP 2013	WAPPLES Rules
1	インジェクション(Injection)	パラメータタンパリング（Parameter Tampering）
		SQLインジェクション（SQL Injection）
		ステルスコマンディング（Stealth Commanding）
		インクルードインジェクション（Include Injection）
2	不完全な認証およびセッション管理 (Broken Authentication and Session Management)	クッキーポイズニング（Cookie Poisoning）
		不正アクセス（Suspicious Access）
3	Cross Site Scripting(XSS)	クロスサイトスクリプティング（Cross Site Scripting）
4	安全ではないオブジェクトの直接参照 (Insecure Direct Object References)	URIアクセスコントロール（URI Access Control）
		インバリッドURI（Invalid URI）
		ユニコードディレクトリトラバーサル（Unicode Directory Traversal）
		エラーハンドリング（Error Handling）
		パラメータタンパリング（Parameter Tampering）
		ステルスコマンディング（Stealth Commanding）
5	不適切なセキュリティ設定 (Security Misconfiguration)	ディレクトリリスティング（Directory Listing）
		エラーハンドリング（Error Handling）
		リクエストメソッドフィルタリング(Request Method Filtering)
		インバリッドHTTP（Invalid HTTP）
		ファイルアップロード（File Upload）
6	機密データ露出(Sensitive Data Exposure)	プライバシーファイルフィルタリング（Privacy File Filtering）
		プライバシーインプットフィルタリング（Privacy Input Filtering）
		プライバシーアウトプットフィルタリング（Privacy Output Filtering）
		インプットコンテンツフィルタリング（Input Contents Filtering）
		エクステンションフィルタリング（Extension Filtering）
		Supported by transaction encryption function(e.g., TLS)
7	不安全な機能レベルのアクセス制御 (Missing Function Level Access Control)	URIアクセスコントロール（URI Access Control）
		ユニコードディレクトリトラバーサル（Unicode Directory Traversal）
		エクステンションフィルタリング（Extension Filtering）
8	クロスサイト要求偽造 (Cross Site Request Forgery)	クロスサイトスクリプティング（Cross Site Scripting）
		パラメータタンパリング（Parameter Tampering）
9	既知の脆弱なコンポーネントを使用 (アメリカing Components with Known Vulnerabilities)	ALL
10	未検証のリダイレクトとフォワード (Unvalidated Redirects and Forwards)	URIアクセスコントロール（URI Access Control）

2）危険度に対応するWAPPLESルール

レベル	説明	WAPPLESルール
緊急	Webサーバが完全にハッカーによって奪われ、操られているため、深刻な機密情報漏洩が懸念される	インクルードインジェクション (Include Injection)
		プライバシーアウトプットフィルタリング (Privacy Output Filtering)
		ステルスコマンディング (Stealth Commanding)
		SQLインジェクション (SQL Injection)
高	Webサーバを踏み台としハッキングが行われ、深刻な2次攻撃へと拡大される	プライバシーファイルフィルタリング (Privacy File Filtering)
		リクエストメソッドフィルタリング (Request Method Filtering)
		ファイルアップロード (File Upload)
		インバリッドURI (Invalid URI)
		バッファオーバーフロー (Buffer Overflow)
		クッキーポイズニング (Cookie Poisoning)
		クロスサイトスクリプティング (Cross Site Scripting)
中	Webサーバの情報が改ざんされ、深刻な障害までは陥っていないが、限定された範囲内のWebサーバ上被害が懸念される	リクエストヘッダフィルタリング (Request Header Filtering)
		URIアクセスコントロール (URI Access Control)
		エクステンションフィルタリング (Extension Filtering)
		Webサイト改ざん (Web Site Defacement)
		インバリッドHTTP (Invalid HTTP)
		不正アクセス (Sアメリカpicioアメリカ Access)
		ユニコードディレクトリトラバーサル (Unicode Directory Traversal)
		パラメータタンパリング (Parameter Tampering)
脆弱性の下調べ	本格的な攻撃のための準備の段階であり、脆弱性を洗い出し情報を収集する	ディレクトリリスティング (Directory Listing)
		インプットコンテンツフィルタリング (Input Content Filtering)
		エラーハンドリング (Error Handling)
		レスポンスヘッダフィルタリング (Response Header Filtering)

3）Web攻撃の目的に対応するWAPPLESルール

Web攻撃の目的は、

1. 攻撃を行うことによって、金銭的損害を及ぼすか、金銭的利益を得ることを狙っている
2. サーバーに負荷を与え、動作不能状態に陥るようにしてサーバー運用を妨害する
3. Web攻撃を実行するために、事前調査レベルで対象になるWebサーバの脆弱性をスキャンする
4. Webサイトを利用し、悪意あるコードを挿入しようとする
5. Webサイトの内容を任意で変更する（Webサイト改ざん）
6. 個人情報、サーバー情報、データベース情報などを漏洩させようとする

等が考えられます。

Web攻撃の目的	WAPPLESルール
金銭的損害	パラメータタンパリング (Parameter Tampering)
	クッキーポイズニング (Cookie Poisoning)
サーバ運用妨害	不正アクセス (Suspicious Access)
	リクエストメソッドフィルタリング (Request Method Filtering)
	バッファオーバーフロー (Buffer Overflow)
脆弱性スキャン	インバリッドURI (Invalid URI)
	インバリッドHTTP (Invalid HTTP)
	リクエストヘッダフィルタリング (Request Header Filtering)
	エラーハンドリング (Error Handling)
	ディレクトリスティング (Directory Listing)
	レスポンスヘッダフィルタリング (Response Header Filtering)
悪意あるコード挿入	ステルスコマンディング (Stealth Commanding)
	クロスサイトスクリプティング (Cross Site Scripting)
Webサイト改ざん	インクルードインジェクション (Include Injection)
	ファイルアップロード (File Upload)
	SQLインジェクション (SQL Injection)
	Webサイト改ざん (Web Site Defacement)
情報漏洩	SQLインジェクション (SQL Injection)
	ユニコードディレクトリトラバーサル (Unicode Directory Traversal)
	プライバシーアウトプットフィルタリング (Privacy Output Filtering)
	プライバシーファイルフィルタリング (Privacy File Filtering)
	プライバシーインプットフィルタリング (Privacy Input Filtering)

2. WAPPLESルールの紹介

WAPPLESルール	説明
バッファオーバーフロー (Buffer Overflow)	Webサーバに対しメモリ上Bufferをオーバーさせるような制限値より 大きなサイズのデータを遮断
クッキーポイズニング (Cookie Poisoning)	認証情報のような重要なデータが含まれているCookieの認証のためのMAC (Message Authenticity Code)より判断をし、改ざんを遮断
クロスサイトスクリプティング (Cross Site Scripting)	クライアント側にて実行可能な悪意あるスクリプトコードを挿入する 試みを遮断
ディレクトリリスティング (Directory Listing)	Webサーバのファイル、ディレクトリのトポロジー(構造)の外部漏洩 を遮断
エラーハンドリング (Error Handling)	Webサーバ、WAS、DBMSサーバなどの情報が含まれている エラーメッセージを遮断.
エクステンションフィルタリング (Extension Filtering)	悪意あるユーザより利用される恐れのある拡張子を持つファイルへの アクセスを遮断
ファイルアップロード (File Upload)	Webサーバ側にて実行可能なファイルのアップロードを遮断
インクルードインジェクション (Include Injection)	Webサーバにて実行可能なファイルの挿入を遮断
インプットコンテンツフィルタリング (Input Content Filtering)	Webサイトのような公開ページ上他人を不愉快にさせる言葉を遮断するか、 指定した言葉に変換
インバリッドHTTP (Invalid HTTP)	RFC 2068-HTTP/1.1基準プロトコルに準じていないアクセスを遮断
インバリッドURI (Invalid URI)	RFC 2068-HTTP/1.1基準プロトコルに準じ定義されている形式ではない URIへのアクセスを遮断
IP遮断 (IP Black)	同じ発信元より一定の時間内閾値以上の不正なアクセスが検知されると 発信元のアクセスを一時的に遮断
IPフィルタリング (IP Filtering)	指定した特定のIPのセグメントや国からのアクセスを遮断
パラメータタンパリング (Parameter Tampering)	Webサイトよりリクエストされていないパラメータを挿入し送り付けるか、 Webサーバから転送されたパラメータを改ざん
プライバシーファイルフィルタリング (Privacy File Filtering)	個人情報が含まれているファイルのアップロードおよびダウンロードを遮断

WAPPLESルール	説明
プライバシーインプットフィルタリング (Privacy Input Filtering)	掲示板やWebページのような公開ページ上個人情報 (クレジットカード番号、メールアドレス) の書き込みによる露出を遮断
プライバシーアウトプットフィルタリング (Privacy Output Filtering)	掲示板やWebページのような公開ページ上個人情報 (クレジットカード番号、メールアドレス) が漏洩される恐れのある場合、 遮断および一部に対しマスキング処理
リクエストヘッダフィルタリング (Request Header Filtering)	Webブラウザからの正常なHTTPリクエストではないヘッダに必須要素が欠けているか 間違っている場合、そのリクエストを不正なリスケストとして検知
リクエストメソッドフィルタリング (Request Method Filtering)	安全ではないHTTPリクエストのメソッドを遮断
レスポンスヘッダフィルタリング (Response Header Filtering)	HTTP レスポンスにてWebサーバおよびWASの情報を削除
SQLインジェクション (SQL Injection)	データベースに対しの不正なSQLクエリ文の試みを遮断
ステルスコマンディング (Stealth Commanding)	Webサーバ上特定のコマンドを実行するリクエストを遮断
不正アクセス (Suspicious Access)	Webブラウザからの正常なリクエストではない自動化されたツールによる アクセスを遮断
ユニコードディレクトリトラバーサル (Unicode Directory Traversal)	Webサーバのユニコード関連の脆弱性を利用するディレクトリおよび ファイルへのアクセスを遮断
URIアクセスコントロール (URI Access Control)	特定のURIやファイルへのアクセスを制御
Webサイト改ざん (Website Defacement)	Webページが改ざんされた場合、検知し復旧ページを出力

3. Black List Top 30

Black List Top 30は、WAPPLESの検知データから「スパム」と「ハッキング」で分類される攻撃を試みているソースIPを上位から30までをリストアップしたものです。

- **スパム**： 攻撃の第1レベルであり、攻撃のターゲットに対して意図していない行動を起こさせるための、Web掲示板にて許可されていない広告を掲示する、SQL Injectionのように広告の内容をDBに挿入する、等いったコメント スパム(Comment Spam)の試みが該当します。
  ✓ **該当するWAPPLESルール：SQLインジェクション (SQL Injection)**
- **ハッキング**：スパムのような第1レベルの試みにより得られた情報を以てシステムに対し直接的被害を及ぼすための本格的な試みが該当します。
  ✓ **該当するWAPPLESルール：クロスサイトスクリプティング (Cross Site Scripting)**
  ファイルアップロード (File Upload)
  ステルスコマンディング (Stealth Commanding)
  インバリッドURI (Invalid URI)

順位	ソース IP	発信国	危険度	区分
1	188.143.x.x	ロシア	98.17	スパム
2	14.63.x.x	韓国	96.2	ハッキング
3	117.21.x.x	中国	95.3	ハッキング
4	221.231.x.x	中国	94	ハッキング
5	37.187.x.x	匿名ネットワーク	93.9	ハッキング
6	188.138.x.x	匿名ネットワーク	93.9	ハッキング
7	185.65.x.x	匿名ネットワーク	93.7	ハッキング
8	180.97.x.x	中国	93.7	ハッキング
9	91.121.x.x	フランス	93.4	ハッキング
10	85.10.x.x	ドイツ	93.4	ハッキング
11	77.247.x.x	ノルウェー	92.2	ハッキング
12	62.210.x.x	フランス	92.1	ハッキング
13	85.25.x.x	匿名ネットワーク	91.75	ハッキング
14	194.150.x.x	匿名ネットワーク	91.5	ハッキング
15	64.79.x.x	アメリカ	91.3	スパム

順位	ソース IP	発信国	危険度	区分
16	176.10.x.x	匿名ネットワーク	91	ハッキング
17	210.102.x.x	韓国	90.8	ハッキング
17	178.217.x.x	ポーランド	90.8	ハッキング
19	5.79.x.x	アメリカ	90.2	ハッキング
20	62.210.x.x	フランス	89.8	ハッキング
21	46.4.x.x	ドイツ	89.8	ハッキング
21	94.242.x.x	グリス	89.7	ハッキング
23	192.42.x.x	匿名ネットワーク	89.6	ハッキング
24	195.154.x.x	フランス	89.5	ハッキング
25	176.126.x.x	アメリカ	88.9	ハッキング
26	158.85.x.x	アメリカ	88.8	スパム
27	66.96.x.x	アメリカ	88.6	ハッキング
28	98.19.x.x	アメリカ	88.5	スパム
29	66.76.x.x	アメリカ	88.1	スパム
30	64.251.x.x	アメリカ	88.1	ハッキング

Penta SECURITY
TRUST FOR AN OPEN SOCIETY

ペンタセキュリティシステムズ株式会社
東京都新宿区四谷四丁目3-20 いちご四谷四丁目ビル３F 〒160-0004
TEL. 03-5361-8201 FAX. 03-5361-8202 / www.pentasecurity.co.jp
お問い合わせ. japan@pentasecurity.com

Penta Security Systems Inc. [KOREA]
Yeouido, Seoul www.pentasecurity.com

Penta Security Systems Co. [U.S.A.]
Hoアメリカton, Texas www.pentasecurity.com/en