

「Web Application Firewall 読本」を公開

～WAF の概要、機能の詳細、導入におけるポイント等をまとめた手引書～

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、ウェブサイトの脆弱性の修正作業が長期化している事例が少ないことから、ウェブサイト運営者が Web Application Firewall（ウェブ・アプリケーション・ファイアウォール、WAF）を導入する際の参考となる解説資料「Web Application Firewall 読本」を 2010 年 2 月 16 日（火）から IPA のウェブサイトで公開しました。

URL : <http://www.ipa.go.jp/security/vuln/waf.html>

Web Application Firewall（WAF）は、ウェブアプリケーション¹の脆弱性²を悪用した攻撃など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です。WAF は脆弱性を修正するといったウェブアプリケーションの実装面での根本的な対策ではなく、攻撃による影響を低減する対策となります。WAF は、WAF を導入したウェブサイト運営者が設定する検出パターンに基づいて、ウェブサイトと利用者間の通信の中身を機械的に検査します（図 1）。WAF を使用することで以下の効果を期待できます。

- ・ 脆弱性を悪用した攻撃からウェブアプリケーションを防御する
- ・ 脆弱性を悪用した攻撃を検出する
- ・ 複数のウェブアプリケーションへの攻撃をまとめて防御する

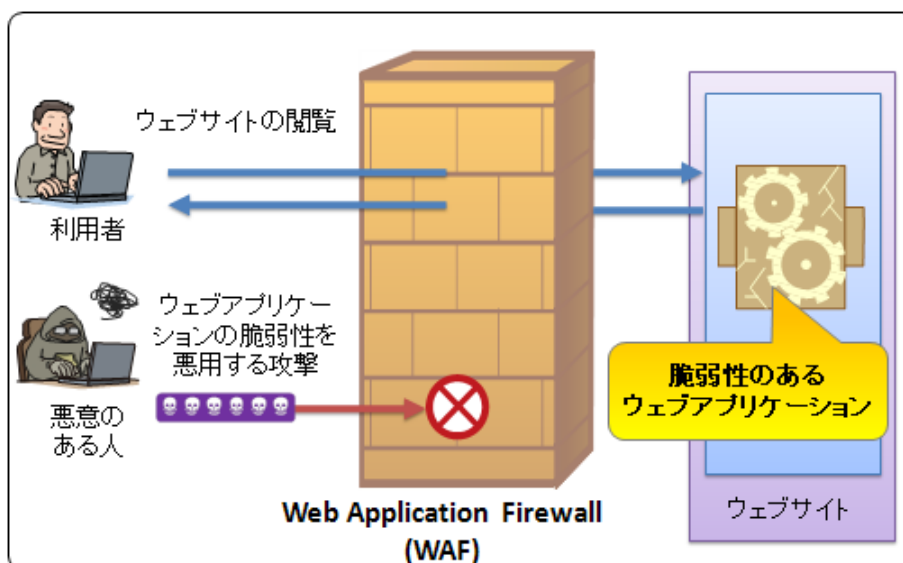


図1 WAFの動作概要図

「Web Application Firewall 読本」は、ウェブサイト運営者がWAFの導入を検討する際に、WAFの理解を手助けするための資料です。本資料では、KISA³やOWASP⁴、WASC⁵などにおけるWAFに関する取り組み、WAFの概要、機能の詳細、導入におけるポイント等をまとめました。

近年、SQLインジェクション攻撃⁶などウェブサイトを狙った攻撃が継続⁷しています。既に作り込んでしまったウェブサイトの脆弱性については、「原因を作らない実装」へ修正する根本的解決が必要です。しかし、IPAが届出⁸を受けたウェブサイトの脆弱性に関しては、IPAがそれぞれのウェブサイト運営者へ脆弱性対策実施を促していますが、脆弱性の修正作業が長期化している事例が少なくありません⁹。このため、IPAでは、ウェブサイトを保護する運用面での方策の一つであるWAFの導入促進を目的として本解説資料の編さんを実施しました。

韓国では KISA が、WAF の普及に取り組んでおり、ウェブサイトのセキュリティ対策として効果を挙げている事例もあります。また、クレジット業界における国際的なセキュリティ基準 PCI-DSS¹⁰では、2008 年 7 月から「定期的なアプリケーションコードの見直し」または「WAF の導入」のどちらかが必須要件となりました。また、ISO/IEC 15408¹¹に基づいて評価・認証された WAF が中小企業等基盤強化税制の対象になることが検討される¹²など注目を集めています。

本資料が、WAF の検討や導入の一助となることを期待します。

「Web Application Firewall 読本」各章の内容：

第 1 章では、「WAF によるウェブアプリケーションの脆弱性対策」として、ウェブアプリケーションへの攻撃および脆弱性対策の実情、各機関における WAF に関する取り組みを紹介しています。

第 2 章では、「WAF の概要」として、WAF に関する概要をまとめています。この章では、WAF とはどのようなものであるかを解説しています。

第 3 章では、「WAF の詳細」として、WAF の機能をまとめています。この章では、WAF にはどのような機能があり、その機能にどのような留意点があるかを解説しています。

第 4 章では、「WAF 導入におけるポイント」として、WAF を導入する際の「事前検討」・「導入」・「運用」の各フェーズにおける検討すべきポイントをまとめています。

付録では、オープンソースソフトウェアの WAF、および商用製品の WAF を紹介しています。

本資料（全 50 ページ）は、次の URL よりダウンロードの上、ご参照ください。

<http://www.ipa.go.jp/security/vuln/waf.html>

なお、内閣官房をはじめとして、関係省庁及び政府関係機関では 2010 年 2 月を「情報セキュリティ月間」として、情報セキュリティに関する普及啓発活動を官民連携の下に行っています。IPA はこの活動に協力しています。（<http://www.ipa.go.jp/security/event/2009/security-month.html>）

■ 本件に関するお問い合わせ先

IPA セキュリティセンター 山岸／勝海

Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp

■ 報道関係からのお問い合わせ先

IPA 戦略企画部広報グループ 横山／大海

Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

脚注：

¹ ウェブサイトで稼動するシステムです。一般に、Java, PHP, Perl などの言語を利用して開発され、サイトを訪れた利用者に対して動的なページの提供を実現しています。

² ウェブアプリケーション等におけるセキュリティ上の弱点。コンピュータ不正アクセスやコンピュータウイルス等により、この弱点が攻撃されることで、そのウェブアプリケーションの本来の機能や性能を損なう原因となり得るもの。また、個人情報等が適切なアクセス制御の下に管理されていないなど、ウェブサイト運営者の不適切な運用により、ウェブアプリケーションのセキュリティが維持できなくなっている状態も含まれます。

³ Korea Internet & Security Agency. 韓国において情報セキュリティの促進を担う政府機関「韓国インターネット振興院」。

⁴ Open Web Application Security Project. <http://www.owasp.org/>

⁵ Web Application Security Consortium. <http://www.webappsec.org/>

⁶ SQL インジェクションとは、データベースと連携したウェブアプリケーションに、データベースへの命令文の組み立て方法に問題があるとき、データベースを不正に操作されてしまう問題です。これにより、ウェブサイトから重要情報が漏洩したり、ウェブサイトの情報が書き換えられたりといった被害を受ける場合があります。詳細は「知っていますか？脆弱性（ぜいじゃくせい）」を参照下さい。http://www.ipa.go.jp/security/vuln/vuln_contents/sql.html

⁷ ウェブサイトを狙った攻撃に関する注意喚起。

http://www.ipa.go.jp/security/vuln/documents/2009/200908_attack.html

ソフトウェア等の脆弱性関連情報に関する届出状況の 2.3 節「ウェブサイトを狙った攻撃に関する注意喚起」。

<http://www.ipa.go.jp/security/vuln/report/vuln2009q4.html#L23>

⁸ IPA セキュリティセンターでは、経済産業省の告示に基づき、脆弱性情報に関する届出を受け付けています。「脆弱性関連情報の届出」を参照下さい。<http://www.ipa.go.jp/security/vuln/report/index.html>

⁹ ソフトウェア等の脆弱性関連情報に関する届出状況の 2.2 節「ウェブサイトの脆弱性で 90 日以上対策が未完了のもの」は 551 件。 <http://www.ipa.go.jp/security/vuln/report/vuln2009q4.html#L22>

¹⁰ Payment Card Industry Data Security Standard. <https://www.pcisecuritystandards.org/>

¹¹ IT セキュリティ評価及び認証制度（JISEC）。<http://www.ipa.go.jp/security/jisec/index.html>

¹² 平成 22 年度税制改正要望の結果概要。http://www.soumu.go.jp/main_content/000048760.pdf