特集記事
Web アプリケーションを守るための対策

FUJITSU Network IPCOM EX シリーズ　Web アプリケーション・ファイアーウォール

目次

目次

1	**Web アプリケーションの危険性**	3
2	**IPCOM EX シリーズの Web アプリケーション・ファイアーウォール**	7
2.1	WAF が提供するセキュリティ機能	7
2.2	導入・運用機能の特徴	9
3	**多重防御によるセキュリティ機能**	11

Web アプリケーションの危険性

1　Web アプリケーションの危険性

ＩＰＡ（独立法人情報処理推進機構）が発表している『情報セキュリティ　１０大脅威　２０１５』では、以下の脅威がランキングされています。

１位　インターネットバンキングやクレジットカード情報の不正利用　～個人口座だけではなく法人口座もターゲットに～
２位　内部不正による情報漏えい　～内部不正が事業に多大な悪影響を及ぼす～
３位　標的型攻撃による諜報活動　～標的組織への侵入手口が巧妙化～
４位　ウェブサービスへの不正ログイン　～利用者は適切なパスワード管理を～
５位　ウェブサービスからの顧客情報の窃取～脆弱性や設定の不備を突かれ顧客情報が盗まれる～
６位　ハッカー集団によるサイバーテロ　～破壊活動や内部情報の暴露を目的としたサイバー攻撃～
７位　ウェブサイトの改ざん　～知らぬ間に、ウイルス感染サイトに仕立てられる～
８位　インターネット基盤技術を悪用した攻撃　～インターネット事業者は厳重な警戒を～
９位　脆弱性公表に伴う攻撃　～求められる迅速な脆弱性対策～
１０位　悪意のあるスマートフォンアプリ～アプリのインストールで友人に被害が及ぶことも～

ウェブサイト関連の脅威として、「4 位　ウェブサービスへの不正ログイン」、「５位　ウェブサービスからの顧客情報の窃取」、「７位　ウェブサイトの改ざん」、「９位　脆弱性公表に伴う攻撃」の４つがランクインしており、依然、Ｗｅｂアプリケーションを狙った攻撃の対策とウェブサイトの防御の必要性が示されています。

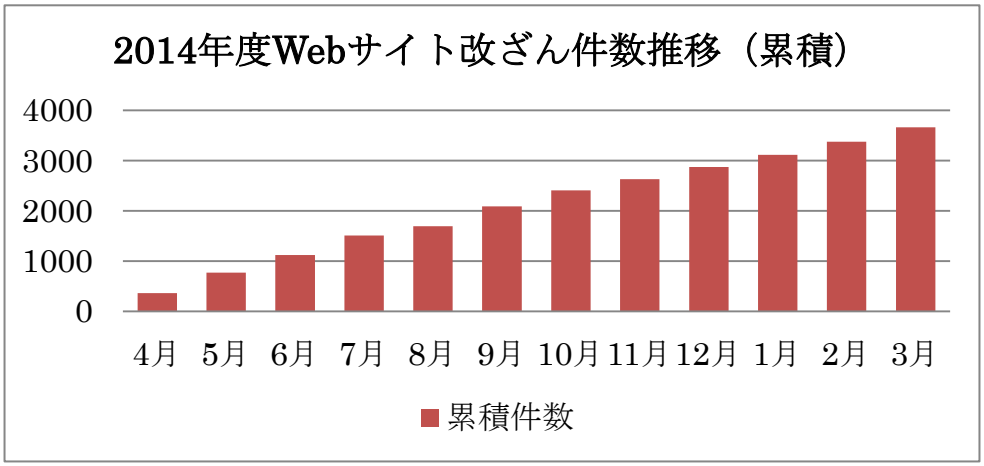
ウェブサービスへの不正ログインの攻撃手口は、パスワード推測やパスワードリスト攻撃などがあります。

ウェブサービスからの顧客情報の窃取やウェブサイトの改ざんの攻撃手口は、Web アプリケーションの脆弱性の悪用、ソフトウェア製品の脆弱性の悪用やリモートによる運用管理の悪用があります。特に、Web アプリケーションの脆弱性では、ＳＱＬインジェクションやディレクトリトラバーサルの脆弱性が悪用される危険性が高いです。

脆弱性公表に伴う攻撃では、2014 年は Apache Struts、OpenSSL、bash 等、広く利用されているソフトウェアの脆弱性対策情報の公表が相次ぎ、それらの脆弱性に対する攻撃が発生しました。

さらに、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（XSS）、クロスサイト・リクエスト・フォージェリ（CSRF）などの Web アプリケーションの脆弱性を狙った様々な攻撃がウェブサイトには継続的に行われています。

例えば、ウェブサイトの改ざんは、一般社団法人 JPCERT コーディネーションセンター（JPCER/CC）の報告では、2014 年度に年間３６００件以上発生しており、Ｗｅｂアプリケーションを狙った攻撃への対策が必要と考えられます。



出展:『JPCERT/CC インシデント報告対応レポート［2015 年 1 月 1 日～ 2015 年 3 月 31 日］』

図１．Web サイト改ざん件数の推移

このようなウェブサイトへの攻撃は、悪意ある攻撃者により金銭窃取などのために、個人情報やカード番号などの情報を窃取する目的で、ファイアーウォール（ＦＷ）や侵入検知防御（ＩＰＳ）を突き抜ける Web アプリケーションの脆弱性を狙った攻撃が多く仕掛けられます。このため、無防備なＷｅｂアプリケーションは危険です。

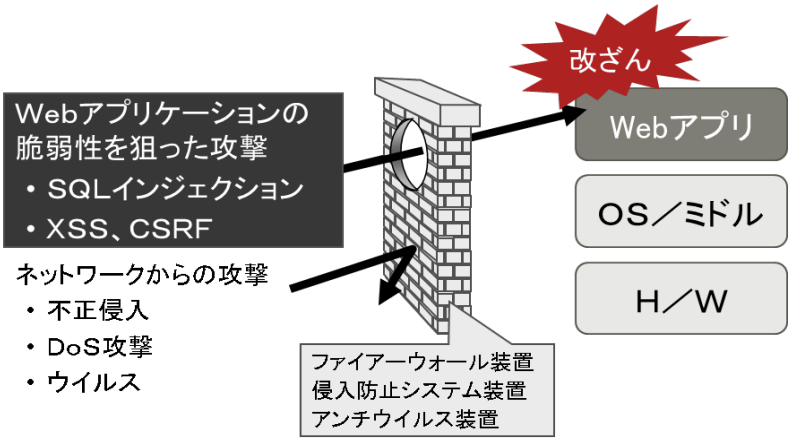


図２. Web アプリケーションの改ざん（イメージ）

具体的な攻撃手口の例を説明します。

・パスワードリスト攻撃は、悪意を持つ第三者が、何らかの手法によりあらかじめ入手してリスト化した ID・パスワードを利用してウェブサイトにアクセスを試み、結果として利用者のアカウントで不正にログインし、被害を与えます。

・SQL インジェクション攻撃は、データベースと連携している Web アプリケーションで、データベースの問い合わせ操作を行うプログラムのパラメーターに SQL 文などを挿入して不正侵入を行い、データベースに蓄積された情報の窃取や改ざんなどの被害を与えます。

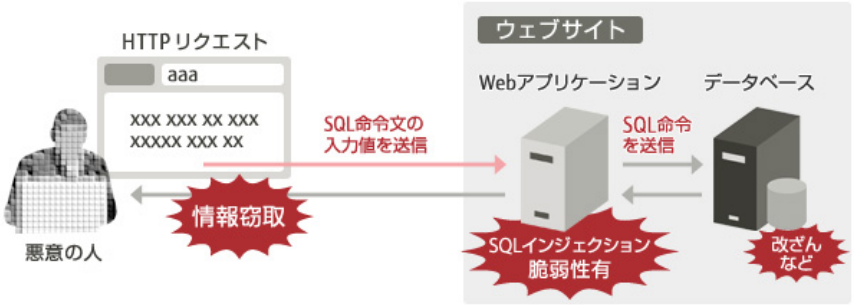


図２－１.SQL インジェクション攻撃例

・ディレクトリトラバーサル攻撃は、ファイル名を扱うようなプログラムに対して特殊な文字列を送信することで通常はアクセスができないファイルやディレクトリにアクセスし、情報窃取、ファイル削除や改ざんなどの被害を与えます。

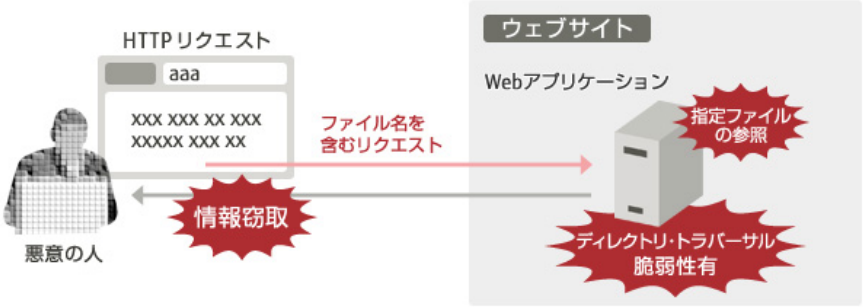


図２－２.ディレクトリトラバーサル攻撃例

・OS コマンドインジェクション攻撃は、閲覧者からのデータの入力や操作を受け付けるウェブサイトで、プログラムに与えるパラメーターに OS に対する命令文を紛れ込ませて不正に操作し、サーバ内の情報窃取、削除、改ざんやウイルス感染などの被害を与えます。

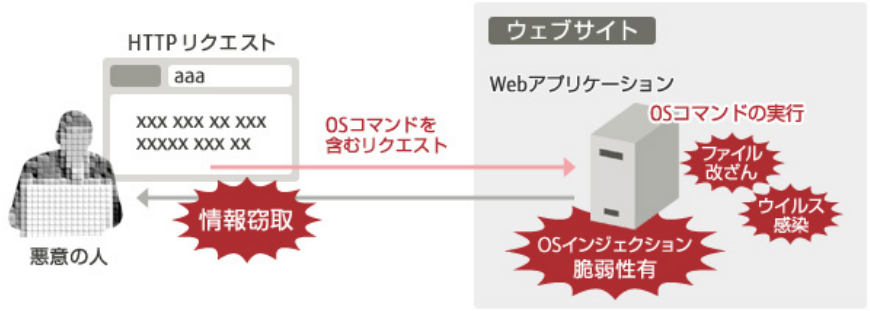


図２－３.OS コマンドインジェクション攻撃例

・クロスサイト・スクリプティング（ＸＳＳ）攻撃は、動的に Web ページを生成する Web アプリケーションに、外部から悪質なスクリプトコードなどを埋め込んでクライアントに送信させて悪意のあるスクリプトを実行させ、情報窃取やなりすましの被害を与えます。

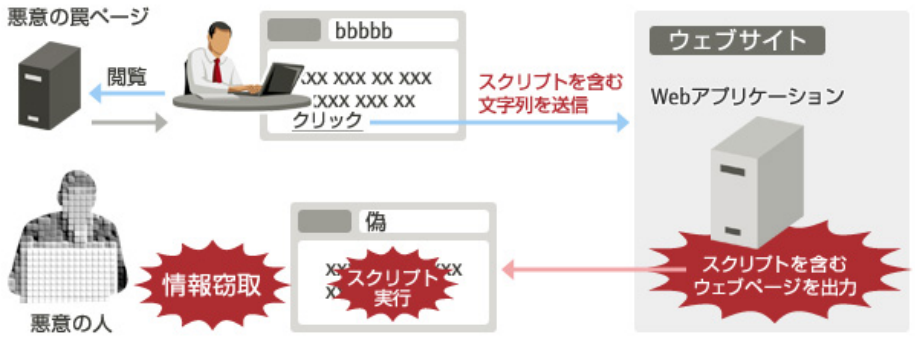


図２－４.クロスサイト・スクリプティング攻撃例

・クロスサイト・リクエスト・フォージェリ（ＣＳＲＦ）攻撃は、ウェブサイトにスクリプトや HTTP リダイレクトを仕込み、閲覧者に意図せず別のウェブサイト上で何らかの操作（掲示版への書き込みなど）を行わせ、被害を与えます。

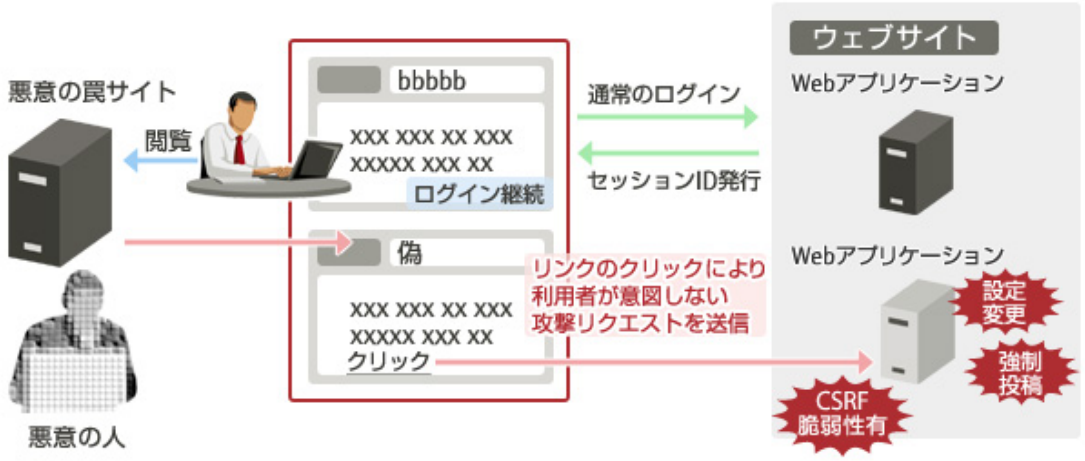


図２－５.クロスサイト・リクエスト・フォージェリ攻撃例

これらのＷｅｂアプリケーションの脆弱性を狙う攻撃から Web アプリケーションを守るためには、従来のファイアーウォール、侵入防止システムやアンチウィルスだけの防御対策では不十分です。

Ｗｅｂアプリケーションの脆弱性を狙う攻撃への理想的な解決策は、Ｗｅｂアプリケーションのプログラム修正ですが、ウェブシステムの改修は費用や時間など運用に与える影響が大きく、直ぐに解決することは困難です。例えば、プログラム修正は、修正のための開発者コストがかかり、対策実現までの期間が長く、修正した脆弱性の対策にしかならないことが考えられます。しかも、プログラム修正まで何の対策も行わなければ、様々な脆弱性を狙った攻撃を受け、ウェブサイトの改ざん、情報窃取や情報改ざん・削除やマルウェア感染の踏み台などにされ、被害者だけではなく、加害者にされてしまう可能性があります。さらに、ウェブサービスが停止すれば、ビジネスチャンスの喪失や信用失墜などの損失を与えます。

このため、Web アプリケーションを脆弱性の脅威から守り、ウェブサービスの運用を維持することが、重要と考え、直ちに、Web サーバの前にＷＡＦ装置を導入することを推奨します。

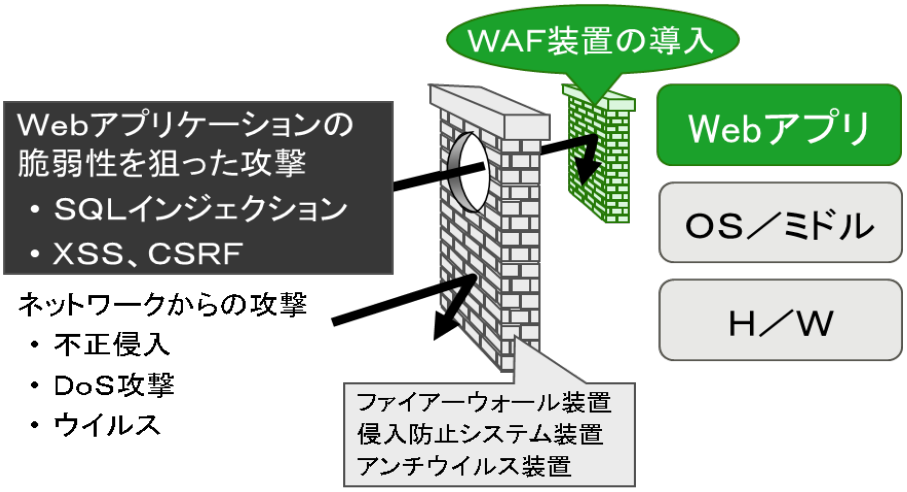


図３．WAF 装置を導入して Web アプリケーションを守る

IPCOM EX シリーズ Web アプリケーション・ファイアーウォール

2 IPCOM EX シリーズの Web アプリケーション・ファイアーウォール

IPCOM EX シリーズでサポートする Web アプリケーション・ファイアーウォール(以降 WAF と呼びます)では、絶えず進化、巧妙化している Web サーバや Web アプリケーションへの攻撃に対して、あらかじめ定義された「WAF ポリシー」に基づいて、HTTP リクエストやレスポンスのヘッダー、コンテンツの内容まで詳細な分析を行い、安全と判断したパケットだけを通過させる機能を提供します。

2.1 WAF が提供するセキュリティ機能

IPCOM EX シリーズの WAF は、シグネチャー（パターンマッチによる検索）を使用しない独自の高精度な攻撃検知および防御機能を搭載しています。

■ **アノマリ型のエンジンによる検知処理**

攻撃検知・防御機能として，高精度な検知エンジンを独自に開発し，多発する XSS 攻撃，SQL インジェクション攻撃，クッキー改ざんなどのクッキー操作攻撃，クロスサイトリクエストフォージェリ(CSRF)やセッションハイジャック／強制ブラウジングなどのセッション管理に関わる攻撃，HTTP プロトコル上の不正なパラメーター操作の攻撃などの脆弱性攻撃から Web システムを防御できます。既知の攻撃パターンだけでなく，未知の脆弱性攻撃（ゼロデイ攻撃）も防御できる高精度な検知エンジンを搭載しています。

■ **攻撃検知・防御機能**

脆弱性攻撃の検査処理として、URI のクエリ文字列，POST ボディ部のパラメーター文字列，および Cookie フィールドの文字列を対象とします。Cookie を使用した SQL インジェクション攻撃にも対応します。
IPCOM EX シリーズの WAF 機能は、以下の主な検知・防御機能を提供します。

●脆弱性攻撃防御機能

Web アプリケーションの脆弱性（セキュリティ上の不備）を利用して、悪意のあるコードの埋め込み、コマンドの注入を行うことで、サーバやクライアントに被害を与える攻撃から、Web アプリケーションを保護する機能として、以下の防御機能を提供します。

・クロスサイト・スクリプティング（XSS）攻撃防御
・SQL インジェクション攻撃防御
・OS コマンドインジェクション攻撃防御
・SSI(Server Side Include) インジェクション攻撃防御
・ディレクトリトラバーサル攻撃防御
・XML インジェクション攻撃防御
・XPath/Blind XPath インジェクション攻撃防御
・LDAP インジェクション攻撃防御

●改ざん防御機能

Web アプリケーションが Web ブラウザに送信する cookie や hidden 属性をもつフォームフィールドのパラメーターの内容がクライアント側で変更されることはありません。Web ブラウザが Web アプリケーションに送信する不正に操作（改ざん）された cookie の内容や hidden 属性をもつフォームフィールドのパラメーターを検出して防御する以下の機能をサポートします。

・cookie 改ざん防御
・hidden パラメーターの改ざん防御

●アクセス違反防御機能

HTTP プロトコルは、HTTP リクエストとレスポンスのペアにより 1 つの処理が完結します。しかし、複数の一連の Web ページで 1 つの処理を形成する場合などでは、この複数の一連の Web ページを 1 つのアクセス単位として管理するセッション機構が必要になります。このセッション管理機能を、cookie および hidden 属性をもつフォームフィールドのパラメーターを利用した独自のセッション管理機能を使用して、不正なアクセスを防御する機能として、以下の機能を提供します。

・セッションハイジャック攻撃防御
・強制ブラウジング攻撃防御
・クロスサイト・リクエスト・フォージェリ（CSRF: Cross Site Request Forgery）攻撃防御
・総当り（ブルートフォース）攻撃防御

●クローキング（情報隠蔽）機能

Web サーバや Web アプリケーションが送信する情報の中には、クレジットカード番号などの個人情報にあたる機密情報、Web サーバの種類やバージョン番号などの脆弱性攻撃の糸口になる情報など、本来、外部に出す必要のない情報を隠蔽する機能をサポートしています。本機能は、以下の情報を隠蔽する手段を提供します。

・HTTP レスポンスヘッダー
・HTTP レスポンスのステータスコード
・HTML コメント
・クレジットカード番号

●HTTP プロトコル要素の検証と規制機能

送受信される HTTP パケットが HTTP プロトコル標準に準拠しているかどうかの厳格な検証機能、および、HTTP プロトコル標準では規定されていない HTTP プロトコル要素(HTTP メソッド、cookie やパラメーターなどなど)の検証と規制、さらに、URL エンコード文字や非標準の %uXXYY エンコード文字の正当性検証と規制、HTTP メッセージボディの検証と規制、POST メソッドや PUT メソッドを使用したファイル転送の検証と規制など、Web サーバや Web アプリケーションに脅威を与える可能性のある様々な HTTP プロトコル要素の厳格な検証と規制機能をサポートしています。以下の HTTP プロトコル要素に対応します。

リクエストライン規制　HTTP ヘッダー規制　メッセージボディ規制
パラメーター規制　ファイル転送規制

本機能により、以下の防御機能を提供します。

・バッファオーバーフロー攻撃防御
・不正な HTTP パケット（HTTP プロトコル規約違反）を利用したサービス妨害攻撃の防御(悪意の攻撃)
・Web サーバや Web アプリケーションの未知の脆弱性に対する攻撃防御

■ 防御動作

攻撃検知時の防御動作（アクション）として，以下の機能を提供し，柔軟な運用が可能です。

1)通信の通過や遮断
2)任意のエラーページをクライアントへ通知
3)任意の URL へ通信をリダイレクト
4)サニタイズ（特定文字に変換）して通信を継続

2.2　導入・運用機能の特徴

WAF 機能の導入・運用を容易にするための機能を提供します。

■ **アノマリ型エンジンを搭載**

IPCOM EX シリーズの WAF に搭載される検知エンジンは、シグネチャーを必要としないアノマリ型のため、ゼロデイ攻撃に対応でき、運用や保守のコスト軽減が可能となります。

■ **簡単設定**

昨今増加傾向を示している防御優先度の高いセキュリティ脆弱性攻撃である SQL インジェクション攻撃、XSS 攻撃の防御設定については、日本語ウィザードの機能を提供し、少ない手順で導入・運用が開始できます。ハードウェア装置の導入が完了した後、例えば SQL インジェクション攻撃防御設定は、次の
五つの手順を実行することにより 約 5 分 で完了できます。

1)対象サイト選択
2)IP アドレス設定
3)フィルタ条件設定
4)対象外通信設定
5)SQL インジェクション防御設定

WAF 機能を導入後、Web サーバの公開サイトの変更に応じて、WAF ポリシー設定を学習機能の結果を元に編集し、段階的に防御設定を強化していくような運用も可能となります。

■ **テスト運用モード**

作成した WAF ポリシーが適切に機能するかどうかを検証するための運用モード「テスト運用モード」を実装しています。WAF ポリシーを作成、適用後、「テスト運用モード」で運用することで、通信を遮断することなく動作し、WAF ポリシーが意図した通りに機能していることを検証できます。また、実際の運用環境で、より安全な運用を維持するためのポリシーのチューニングにも活用でき、日々の運用管理業務の負荷を軽減できます。

■ **学習機能**

WAF 機能の運用開始にあたって、Web サーバの全コンテンツに対するポリシー（ ホワイトリストを含む WAF セキュリティポリシー）を一から定義することは、膨大な導入工数を伴います。そこで、Web アプリケーションの通信内容をキャプチャーして、WAF の定義項目（オブジェクトやオブジェクトタイプ一覧、ページのリンク関係、パラメーター一覧、入力フォーム変数など）を抽出、解析し、設定支援に使用できるようにデータベースとして保存する「学習機能」を提供します。
この機能により、WAF ポリシーの定義・編集の作業を実際の通信動作状況にもとづいて適切に実施できます。継続的にセキュリティポリシーの運用（追加、更新）行う上でも編集作業の負荷を軽減できます（図 4 参照）。

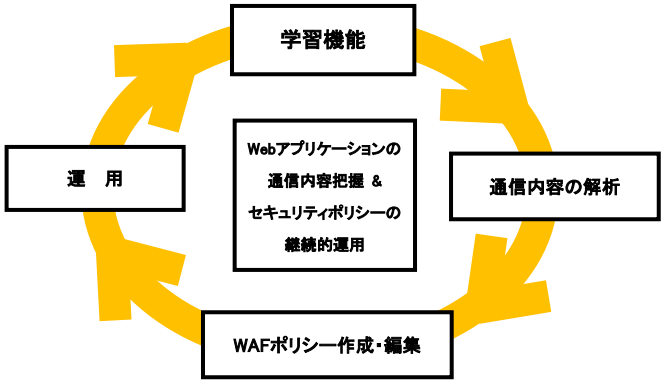


図4. セキュリティポリシーの運用

■ **統計機能**

WAF 機能導入後の運用状態を容易に把握するために、以下の運用管理機能を提供します。これらの運用管理機能により、WAF 機能を導入した Web サーバ環境の効率的な運用を支援することが可能となります。

a) WAF 統計情報集計

WAF 機能が検知した攻撃の状況を把握できます。検知カテゴリごとのポリシー違反（攻撃）と判定された回数の統計を、日ごと、週ごと、月ごとなど、期間条件で集計できます。

クロスサイト・スクリプティング攻撃カテゴリ、SQL インジェクション攻撃カテゴリ、OS コマンドインジェクション攻撃カテゴリなどの統計を継続的に採取することによって、Web サイトへの攻撃パターンの実状が把握できます。

b) トランザクション統計情報収集

WAF 機能が処理した HTTP パケットおよびトランザクションに関する統計情報を採取できます。これにより、ネットワーク環境における Web サーバへのアクセス状況が把握できます。

c) 学習統計情報収集

WAF の学習機能が採取・解析した Web サイトの統計情報を採取し、監視対象の特定のコンテンツへのアクセス状況などを把握できます。

d) クローキング（情報隠蔽）統計情報収集

クローキング（情報隠蔽）対象とした特定のコンテンツへのアクセス時のクレジットカード番号や、Web サイトからの応答レスポンス内容の隠蔽状況を採取するもので、隠蔽対象とした特定のコンテンツへの通信における情報隠蔽の状況を把握できます。

e) 通過・検知イベントログ

攻撃の種別、および攻撃元、接続先やサイト名などの情報を記録できます。ログの内容をシグネチャー型 IPS 機能と統一することで、Web サーバ管理者が、攻撃の詳細を特定できるようにしています。

また、検知イベント、通過イベントの通知手段として、Web コンソール画面表示、Syslog サーバへの転送、SNMP トラップ、メール転送機能を提供し、運用管理業務に柔軟に対応できるようにしました。

3　多重防御によるセキュリティ機能

IPCOM EX シリーズで WAF 機能をサポートすることで、従来からサポートする制御ブロックに加えて、5 階層の多重防御でのセキュリティ機能を構成します。
IPCOM EX 装置一台で，アプリケーション・ファイアーウォール機能，アノマリ型 IPS 機能，アンチウィルス／Web コンテンツ・フィルタリング機能，シグネチャー型 IPS 機能，さらに WAF 機能のサポートにより Web システムに対するネットワークの全レイヤーにわたるあらゆる攻撃からシステムを保護することができます。WAF 機能を加えた検知・防御により，攻撃による Web サーバの処理負荷を緩和でき，正常なトラフィックだけをサーバに処理させることで，サーバの安定稼動が可能となります。

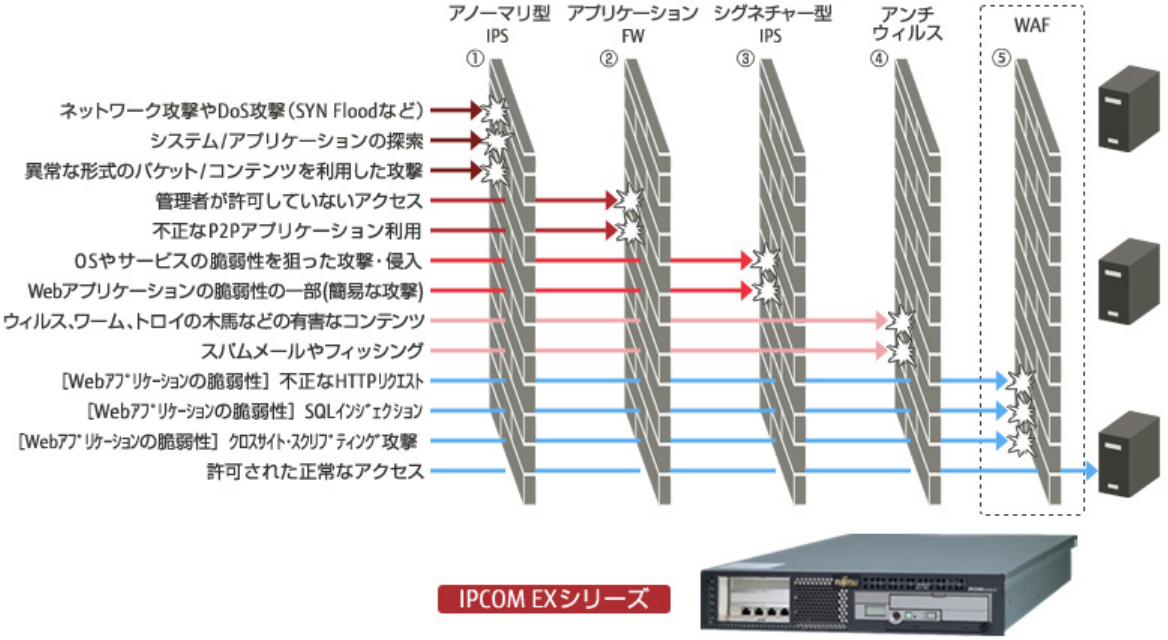


図５．セキュリティ管理機能の５階層制御ブロック

Web アプリケーション・ファイアーウォール（WAF）をサポートする装置は下記のとおりです(2015 年 5 月)。

FUJITSU Network IPCOM EX2700 IN
FUJITSU Network IPCOM EX2700 LB
FUJITSU Network IPCOM EX2700 SC

FUJITSU Network IPCOM EX2500 IN
FUJITSU Network IPCOM EX2500 LB
FUJITSU Network IPCOM EX2500 SC

FUJITSU Network IPCOM EX2300 IN
FUJITSU Network IPCOM EX2300 LB
FUJITSU Network IPCOM EX2300 SC

お問い合わせ
FUJITSU LIMITED
Web サイト: jp.fujitsu.com
2015 年 7 月

© Copyright Fujitsu Limited All rights reserved