SITEGUARD

WAFとは

～ WAF選定・導入のポイントと SiteGuardが選ばれる理由～

EG Secure Solutions

はじめに

ウェブはいまやインターネット社会における重要なインフラとなり、その活用範囲は広がり続けています。単なる情報発信の場にかぎらず、ショッピングやゲーム、メールや SNS をはじめとするコミュニケーションツールなど、その用途は多様化し、日々多くの新しいウェブサイトが公開されています。
その利便性の反面、ウェブサイトがサイバー攻撃のターゲットとなり、ウェブサイトを経由してデータベースを不正に操作され、個人情報をはじめとする機密情報が窃取される被害やウェブコンテンツ（ページ）の改ざんなど、様々な被害が発生しているのも事実です。

サイバー攻撃はシステムの脆弱な部分を狙ってきます。ウェブサイトにおいては、近年ウェブアプリケーションの脆弱性が悪用されるケースが増加傾向にあり、単に攻撃の被害を受けるということだけでなく、攻撃者に踏み台として悪用されることで、加害者とみられてしまう恐れもあります。
ウェブサイトの管理者は、現時点で被害はなくともウェブアプリケーションの脆弱性を悪用する攻撃、その脅威が身近に存在する、この実態を認識して適切な対策を実施するとともに、万が一に備えて被害の性質や影響を理解しておくことが必要です。

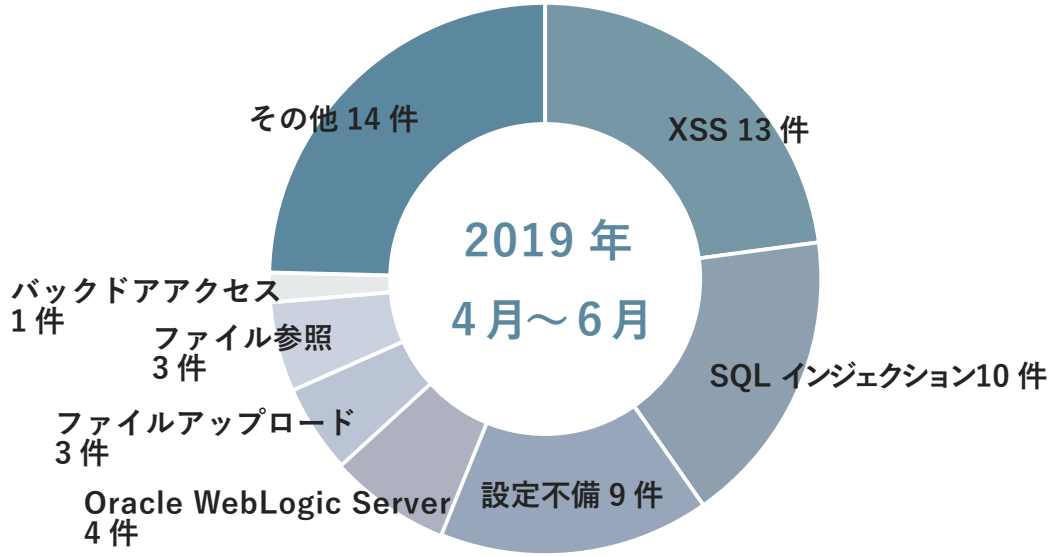
本書では、EG セキュアソリューションズが提供するソリューションである WAF（Web Application Firewall）に関連する技術情報のほか、WAF の選定や導入のポイントについて解説しています。

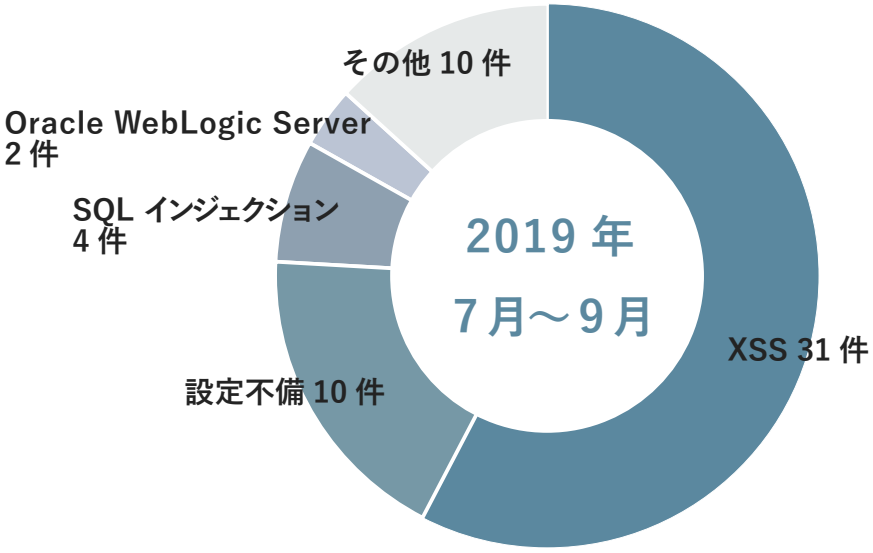
狙われるウェブアプリケーションの脆弱性

個人情報の窃取やサイト改ざんなど、ウェブサイトを狙った攻撃による事件・事故が後を絶たず、ウェブサイトのセキュリティ対策が求められています。これらの事件・事故の原因は、SQL インジェクションやクロスサイトスクリプティングといったウェブアプリケーションの脆弱性を悪用した攻撃によるものが代表的であり、その脅威はウェブサイトの規模や企業・個人に関係なく、身近なこととして意識する必要があります。

重要インシデントの傾向

インターネットからの攻撃により発生した重要インシデントの内訳
※出典：株式会社ラック「JSOC INSIGHT vol.26」





被害の一例

情報漏洩

ウェブサイトを経由してデータベースサーバー等へ不正にアクセスされ、個人情報をはじめとする機密情報が窃取される被害です。
EC サイトなど、クレジットカード情報を含む個人情報を大量に扱うサイトにとっては特に深刻であり、信用の低下やサイト停止による機会損失、顧客への補償といった様々な損害を被る恐れがあります。
脆弱なウェブアプリケーションを介して不正にデータベースを操作する SQL インジェクション攻撃による被害が代表的ですが、Apache Struts2 のリモートコード実行（RCE）など、フレームワークやソフトウェアの脆弱性が悪用されるケースも増えています。

改ざん

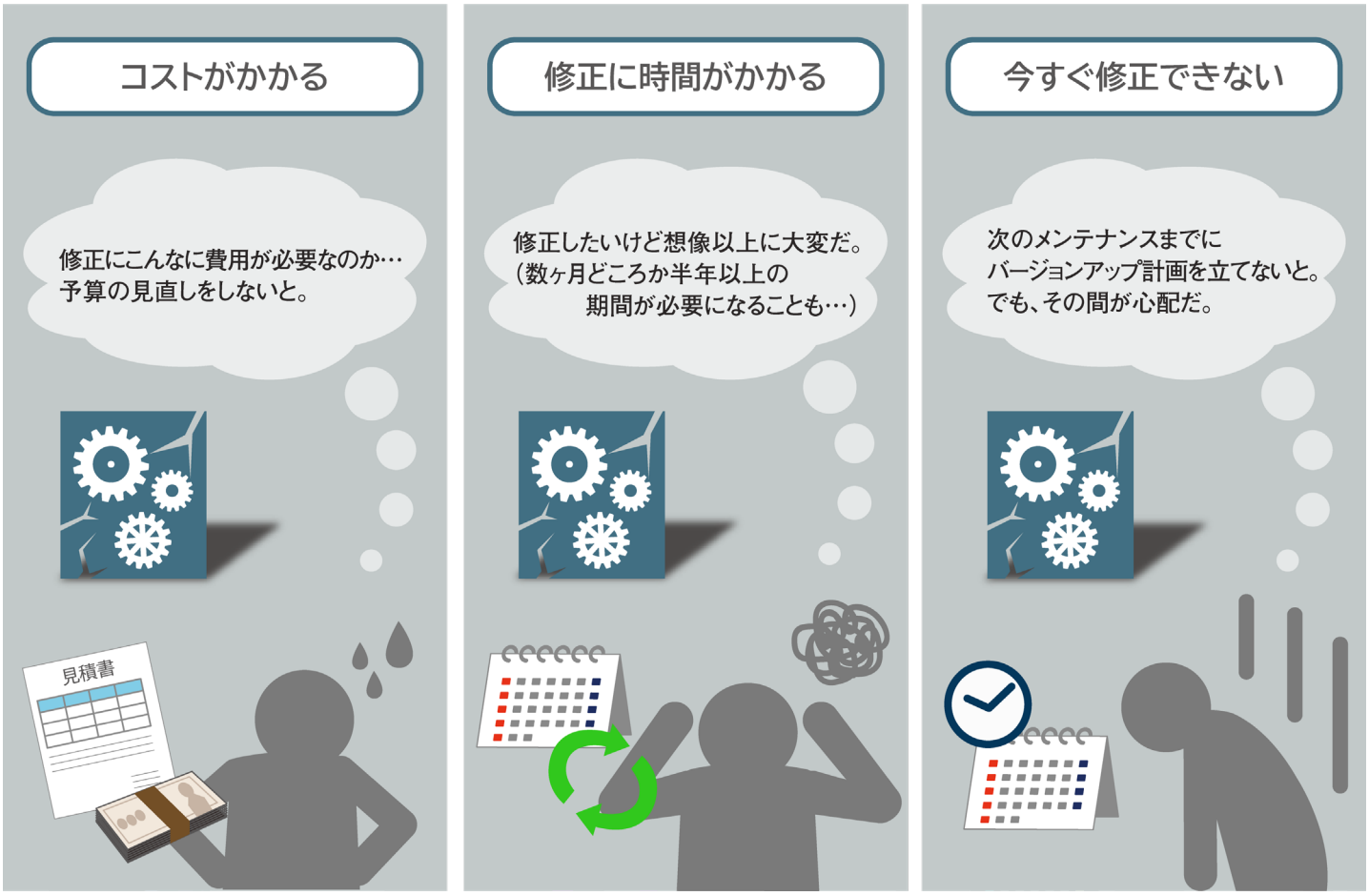
ウェブサイトのコンテンツが不正に書き換えられてしまう被害です。
近年の改ざん被害では、主義主張などのメッセージ性のある画像を挿入するといった目に見えてわかりやすい改ざんだけでなく、スクリプトを埋め込んでウェブサイトを訪れたユーザーを不正なサイトへ誘導し、マルウェア感染させたりするなどの手法も用いられています。
このほか、偽の決済ページを表示させることでクレジットカード情報を詐取するなど、ユーザーへの影響が大きい被害も報告されています。ひとたび改ざんが発生すると、そのサイトの信用は著しく低下するだけでなく、加害者として見られてしまう恐れもあります。
実際の攻撃には、ウェブアプリケーションの脆弱性を悪用する SQL インジェクション攻撃により、データベースに格納されたデータを不正に改ざんする方法や CMS（Content Management System）などのソフトウェアの脆弱性悪用などがあります。

Apache Struts2 などのフレームワークや CMS の脆弱性を悪用する攻撃では、脆弱性に関する情報が公開されてから短期間で攻撃が開始されるというケースも増えてきており、ウェブサイトの運営者は脆弱性に関する情報の収集に努めるほか、迅速に対策を講じることが求められています。

難しい「脆弱性ゼロ」

安全なウェブサイト・ウェブアプリケーションの構築は、セキュア設計・セキュアプログラミングが基本であり、それを完璧に行うことができれば何の心配もありません。しかしながら、常にセキュアプログラミングのノウハウを持つ自社スタッフや開発委託先を確保できるとはかぎらず、また人が関わる作業であるため、対策漏れなどが生じることも考えられます。Apache Struts2 などのフレームワークや CMS を使用してウェブサイトを構築している場合、通常自ら脆弱性を修正するといったことは困難です。

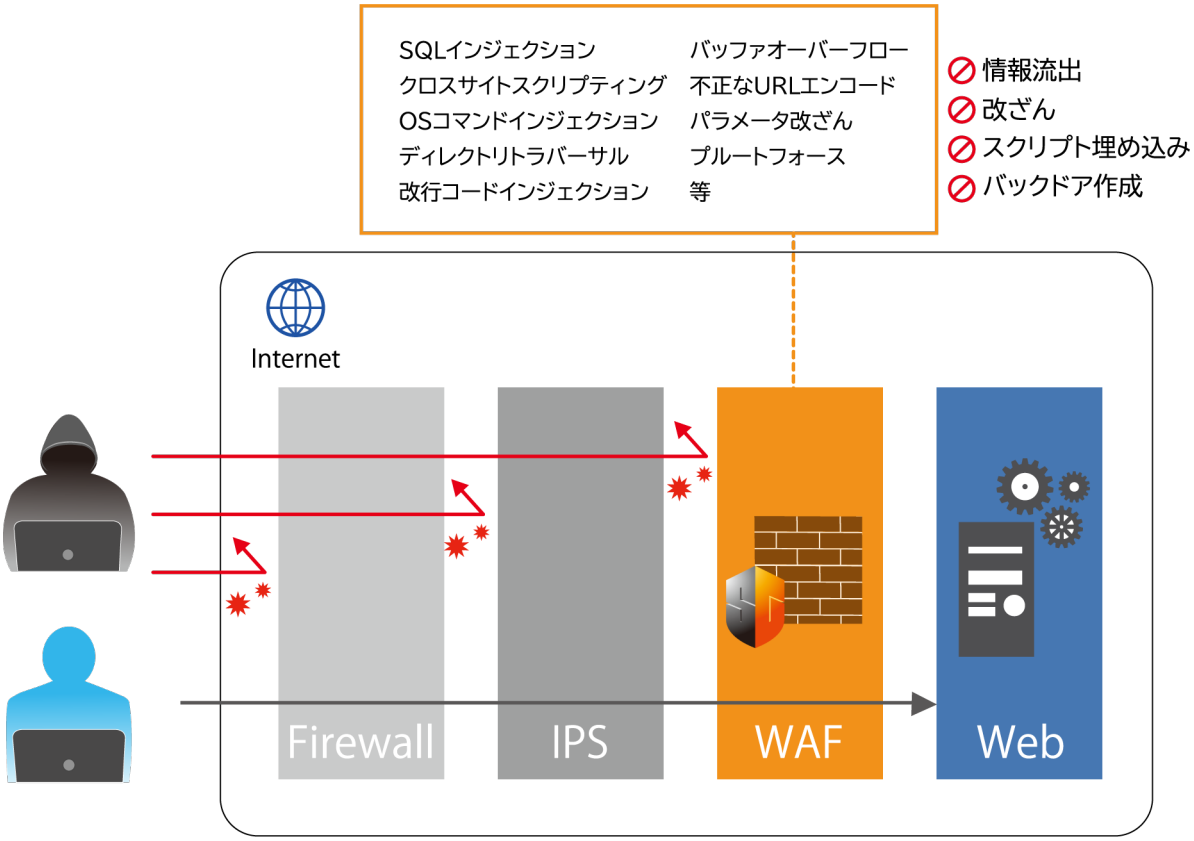
内部的な自主検査はもちろんのこと、運用開始前に第三者による脆弱性診断を受ける取り組みは一般化していますが、脆弱性が見つかった場合の対応については、運用上の理由（サイトを停止できない、バージョンアップできないなど）により修正が困難であったり、修正までに長い時間が必要になることもあります。



このような実情から根本的な対策を基本としつつ、別のアプローチでの対策が求められるようになり、ウェブアプリケーションの脆弱性の有無とは独立したかたちで攻撃を防御できる WAF の活用が急速に進んでいます。

WAF（Web Application Firewall）

Web Application Firewall は、ウェブアプリケーションの脆弱性を悪用する攻撃を検出・防御し、ウェブサイトを保護するためのセキュリティ製品です。それぞれの単語の頭文字から WAF（ワフ）と呼ばれています。



被害の防止

現実的な対策で、
ウェブアプリケーションを
取り巻く脅威に対抗。

攻撃の可視化

脅威は身近に存在する。
攻撃の実情を
把握して備える。

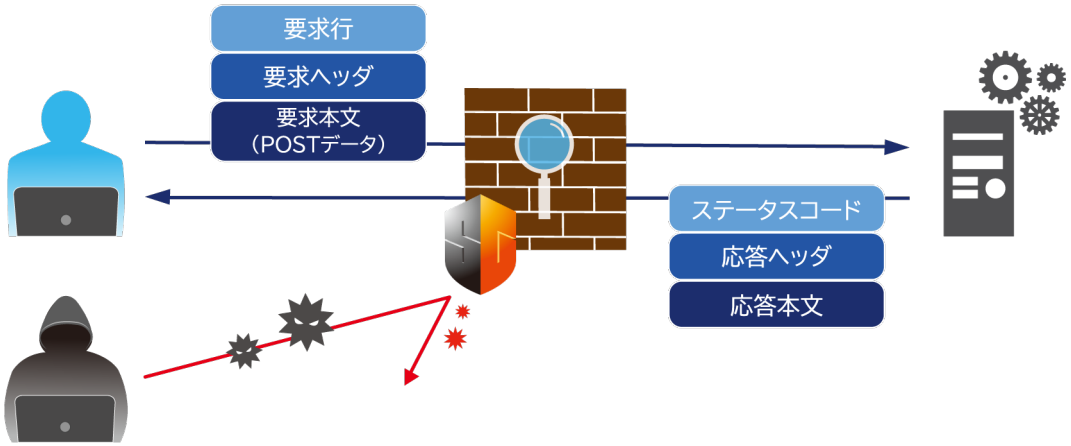
対策の一元化

ウェブアクセスを
一元的に検査して、
ウェブサイトを保護。

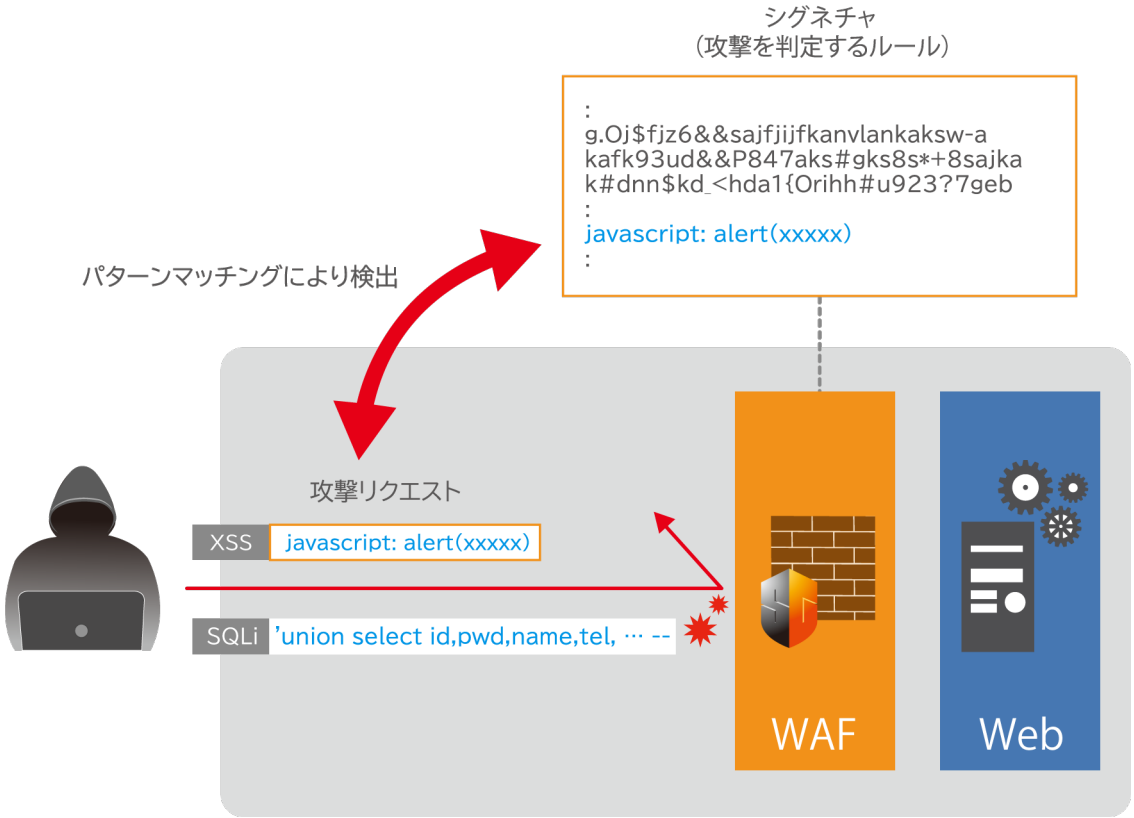
コストダウン

WAF を有効活用して
改修にかかるコストや
負担を下げる。

WAF による防御の基本は、シグネチャ検査です。検出パターン（シグネチャ）に基づき、HTTP リクエスト（リクエストライン、リクエストヘッダ、要求本文）および HTTP レスポンス（ステータスコード、レスポンスヘッダ、応答本文）に含まれる各種データを検査して攻撃を検出します。



シグネチャには、定義方法により不正なパターンを定義する「ブラックリスト」と、安全なパターンを定義する「ホワイトリスト」の二種類があります。通常、単にシグネチャと呼ぶ場合はブラックリストを指すことが多く、製品が標準搭載するシグネチャを活用することで、利用者は一から防御ルールを作成する必要なく、全サイトに対して均一の防御ルールを適用することができます。



ウェブアプリケーションを守る WAF

WAF を導入することで、以下のような様々な脅威からウェブサイトを保護することができます。

代表的な脅威・攻撃手法

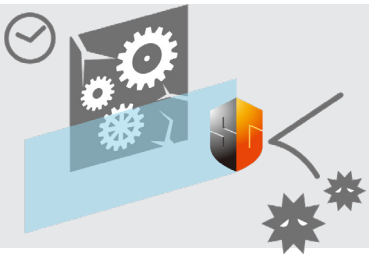
SQL インジェクション	SQL 文を含んだ入力データを送信してデータベースに不正にアクセスする。データベース内の機密情報の漏洩やデータ改ざんにより、大きな被害を受ける恐れがある。
クロスサイト スクリプティング	脆弱な標的サイトにアクセスするように仕向けることで、ウェブサイトが本来想定していない機能（スクリプト実行など）をブラウザ側で実行させる。Cookie のセッション情報が盗まれるなどの恐れがある。
クロスサイト リクエストフォージェリ	対象ウェブサイトの投稿や登録といった重要な機能について、他のサイトから本来の手順を経ずにクライアントに実行させる。なりすまし投稿などに悪用される恐れがある。
ディレクトリトラバーサル	ディレクトリパスを遡ってサーバー上のファイルに不正にアクセスする。本来公開を意図していないファイルの参照・実行の恐れがある。
OS コマンド インジェクション	OS コマンドを含んだ入力データを送信してサーバー上のリソースに不正にアクセスする。サーバー上で任意のコマンドが実行された結果、大きな被害を受ける恐れがある。
改行コード インジェクション (HTTP ヘッダ・メールヘッダ)	改行コードを含んだ入力データを送信して、HTTP レスポンスヘッダやHTTP レスポンスを改ざんする。クライアントは偽りの Cookie やページ内容による影響を受ける可能性がある。任意のメールヘッダの挿入や本文の改変、不正なメール送信に悪用される可能性もある。

WAF の活用が有効なケース

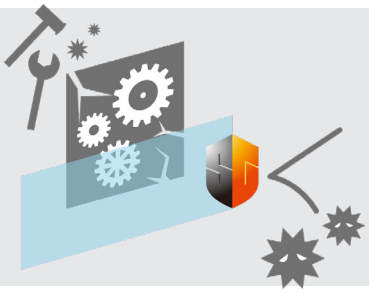
ウェブアプリケーションの脆弱性を悪用する攻撃、脅威への対策として、以下のようなケースで WAF が有効です。

脆弱性を修正できない

脆弱性の存在を把握しながらも運用上の理由からアプリケーションを修正できない場合があります。脆弱性の修正と WAF を併用することで現実的かつ効果的な対策が可能です。



Apache Struts2 などのフレームワークや CMS を使用している場合、バージョンアップの計画やテストの実施に時間を要することがあります。このようなケースにおいて、WAF で防御しながらバージョンアップ作業を進めるといった対策が可能となります。



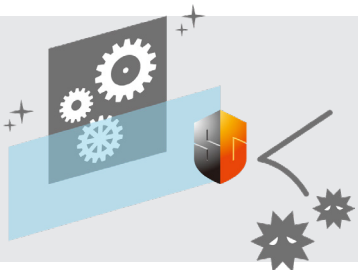
いますぐ攻撃を防ぎたい

不正アクセスにより、ウェブサイトが実害を被ると対策完了までサービスの再開は困難です。ダウンタイムは機会損失に直結します。緊急対応的な WAF の活用は迅速なサイト復旧の大きな助けとなります。

SQL インジェクションによる被害が多発していた 2010 年頃まで、緊急対応として WAF で攻撃を防御しながら、脆弱性の修正を進めるというケースも多くみられました。

保険的対策をしたい

情報流出等の事故が起きてしまうと、直接・間接的に莫大なコストが発生します。事前対策として WAF を利用することで、万が一のリスクを低減することができます。

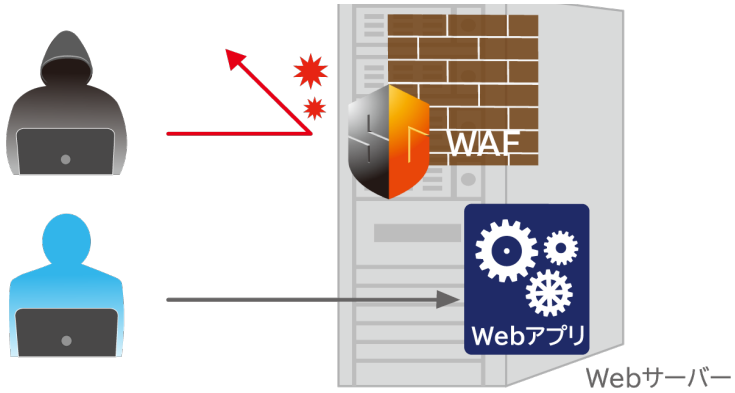


現在は、脆弱性診断やセキュアな開発という根本的な対策を基本としつつ、セーフティネットとしての WAF 活用が一般化してきています。

WAF の種類

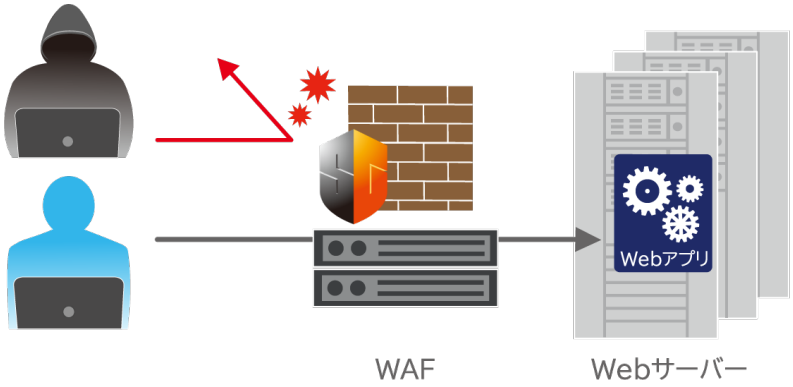
ホスト型

ウェブサーバーにインストールして利用する WAF です。
ソフトウェアで提供され、ウェブサーバーのモジュールとして動作するタイプを指すことが一般的です。
ウェブサーバーごとに WAF をインストールする必要があり、導入要件はウェブサーバーの環境に依存しますが、最もシンプルな構成であり、専用ハードウェアを必要とせず、ネットワーク構成に影響を与えないことが主な利点となります。以前はウェブサーバーの負荷が課題になることもありましたが、昨今のハードウェア性能の向上もあり、現在の影響は少なくなっています。



ゲートウェイ型

ウェブサーバーの前段で独立した機器として利用する WAF です。
リバースプロキシのほか、インライン構成で設置されることが多く、複数のウェブサーバーを一元的に保護することができます。リバースプロキシはサイトの成長に合わせて拡張しやすく、インライン構成は導入しやすい点が特長です。
ソフトウェアもしくはアプライアンスがあり、アプライアンスの場合は仮想アプライアンスとして提供されることもあります。専用機としてのハードウェア購入費が高くなったり、ネットワークの構成変更が必要となる場合があります。リバースプロキシの場合は、ウェブサーバーからみた接続元 IP アドレスがプロキシの IP アドレスになるため、クライアントの接続元 IP アドレスの取得についても考慮する必要があります。



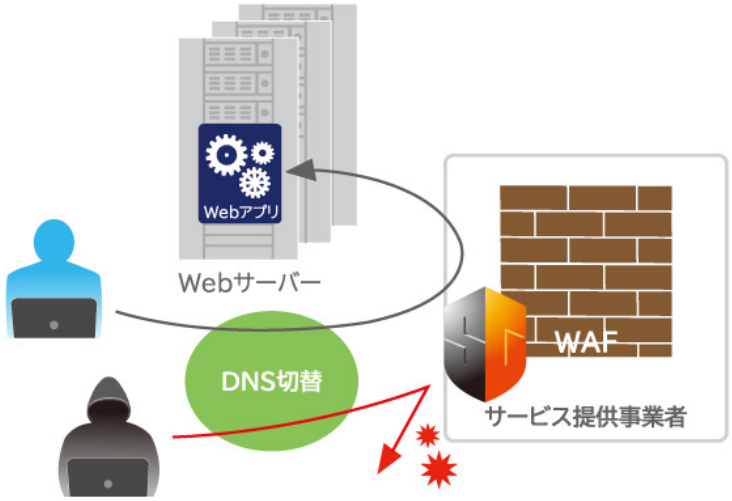
※通常、プロキシが付与する X-Forwarded-For 等のヘッダからクライアントの接続元 IP アドレスを判定できるように配慮されています。

クラウド型

DNS 切替型

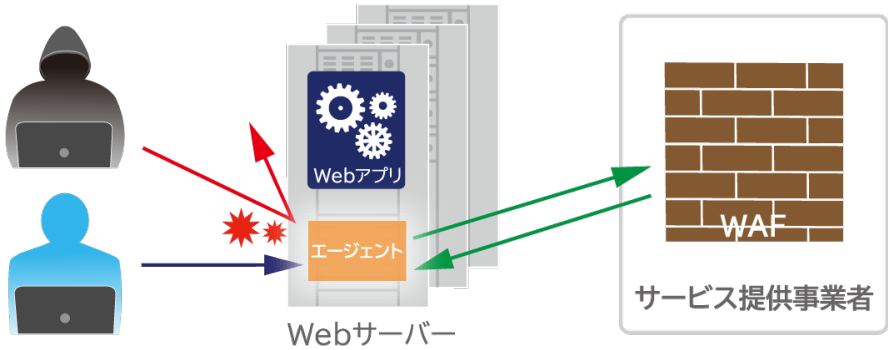
DNS の設定変更により、クライアントからウェブサーバーへの通信を WAF サービス提供事業者のネットワーク経由にする方式が代表的です。組織外の通信経路を経由しますが、前述のゲートウェイ型のリバースプロキシと同等の動作イメージになります。

※前述のゲートウェイ型の構成と同様、ウェブサーバーからみた接続元 IP アドレスはサービス提供事業者の IP アドレスに変換されます。



エージェント型

前述のホスト型との組み合わせに近い形態として、ウェブサーバーにエージェントをインストールし、エージェントとサービス提供事業者の WAF がネットワーク経由で連携する形態もあります。



クラウドサービスとして提供される WAF の場合、専用ハードウェアを用意したり、物理的なネットワークを変更する必要がなく、サービスの提供事業者に WAF の運用を任せることができるという利点があります。一般的に FQDN の数や通信量によってサービス料金が上がることのほか、組織外（自社環境以外）の通信障害などの影響を受ける可能性があるといった課題もあります。

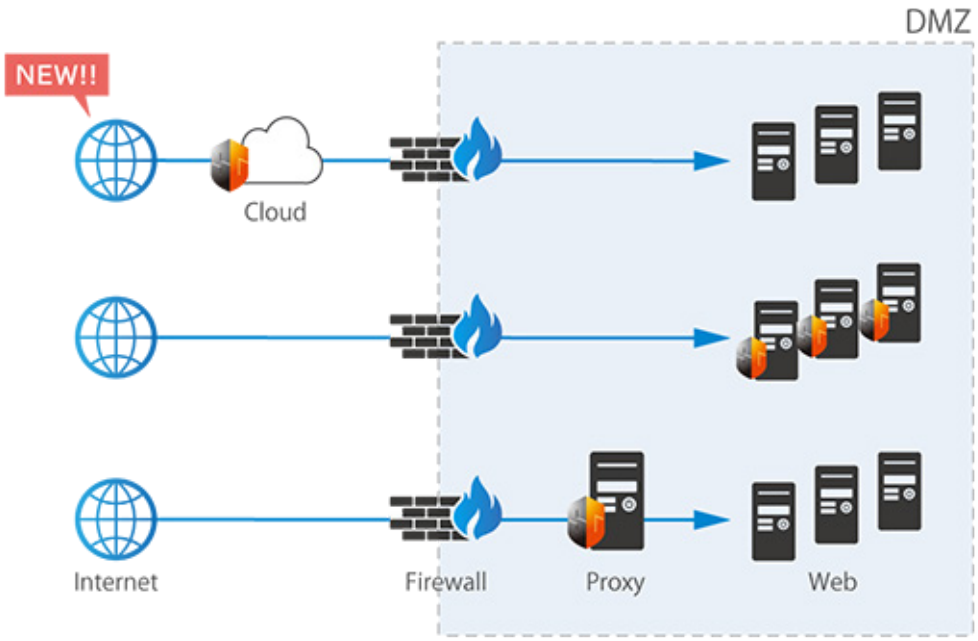
おすすめの WAF「SiteGuard シリーズ」

WAF 選定・導入のポイントは、稼働しているウェブサイトの環境や特性、運用方針に合わせて適切な WAF を選定することです。重要なポイントではありますが、単純に「インストールが簡単そうだから」「費用が安いから」という理由だけで決めてしまうと、

ウェブサイトの環境と製品・サービスの仕様が合っていなかった…
ウェブサイトの拡張でドメイン数が増えたら想定以上のコストがかかるようになってしまった…

など、運用開始後に困ってしまうことも少なくありません。
提供形態や構成、検討ポイントをもとに正しく選定することが大切です。

そこで…



「SiteGuardシリーズ」は、シンプルかつ高性能な国産ソフトウェア WAF です。
特に以下のような要件、課題のあるウェブサイトへの導入に適しています。

ドメイン毎に詳細かつ柔軟な設定をしたい

「SiteGuard シリーズ」は、URL や IP アドレスによるホワイトリストの登録だけでなく、要求メソッドやパラメータの名前・パラメータの値など、様々な条件を組み合わせた検査ポリシーを作成することができます。特定の入力値に限定したい場合や URL・パラメータの値が変動するときも詳細な設定ができます。「SiteGuardシリーズ」であれば、ウェブサイトの特性に合った柔軟な設定が可能です。

保護対象の FQDN の数や通信量を気にしたくない

「SiteGuard シリーズ」は、インストールする OS の数でライセンスをカウントします。そのため、バーチャルホストで多数のサイトを運用している場合であっても必要なライセンス数が増えることはありません。「SiteGuardシリーズ」であれば、ウェブサイトの拡張により FQDN 数の増加が見込まれる場合であっても安心してご利用いただけます。また、通信量による課金や制限もありませんので、ピーク時だけでなく大きなサイズのファイルダウンロードやアップロードが必要な環境でも安心です。

リクエストの情報（ログ）などを外部に出すことができない

「SiteGuardシリーズ」は、ウェブサイトへのアクセス情報や検出情報をインストールしたサーバー上にログとして記録します。ログにはアクセスした URL や接続元の IP アドレス、パラメータの内容など、様々な情報が記録されます。WAF によるセキュリティ対策では様々な情報が必要となり、検査の結果が記録されていきます。要件によっては、これらの情報が組織外に蓄積されることがセキュリティポリシー違反となり、クラウド型の利用が適さない場合があります。「SiteGuardシリーズ」であれば、ログ管理を含めて自社内でコントロールすることができます。

おすすめの WAF「SiteGuard シリーズ」

NEW!!

クラウド型

マネージドによる運用お任せ、クラウドサービスで
WAF を利用したいお客様に最適な製品です。

ホスト型

サーバーインストール型で、シンプルな構成で
WAF を導入したいお客様に最適な製品です。

ゲートウェイ型

WAF をリバースプロキシ構成で構築したい
お客様に最適な製品です。

SiteGuard が選ばれる理由

- WAF 市場初期より国産専業メーカーとして販売期間 14 年
- IPA 発行「WAF 読本」へ監修協力するなど公的機関からの信用を獲得
- 官公庁や金融機関をはじめ規模・業種問わず幅広い環境での導入実績
- ウェブサーバー数百台や数万 VM など大規模環境で安定稼働する品質
- 高い運用性が求められる大手レンタルサーバーの多くで標準採用

「SiteGuardシリーズ」は、信頼と実績の純国産 WAF です。
それぞれ以下のような要件、課題のあるウェブサイトへの導入に適しています。

クラウド型

WAF の運用管理をサービス事業者に任せたい

クラウド型 WAF「SiteGuard Cloud Edition」は、マネージドサービスとして提供され、当社が WAF の運用管理を行います。国内メーカーとして、「SiteGuard シリーズ」の開発・販売・サポートのすべてを自社対応しており、日々の運用はエンジニアの伴走によりサポートします。
かんたん導入・かんたん運用を実現します。

新しい機器の設置や製品のインストールができない

クラウド型 WAF「SiteGuard Cloud Edition」は、DNS の設定変更により WAF を導入できるため、の新たな機器の設置やインストール作業は不要です。

ソフトウェア型

ドメイン毎に詳細かつ柔軟な設定をしたい

ホスト型 WAF「SiteGuard Server Edition」とゲートウェイ型 WAF「SiteGuard Proxy Edition」は、URL や IP アドレスによるホワイトリストの登録だけでなく、要求メソッドやパラメータ名・値など、様々な条件を組み合わせた検査ポリシーを作成することができます。ウェブサイトの特性にあった柔軟な設定が可能です。

保護対象の FQDN の数や通信量を気にしたくない

ホスト型 WAF「SiteGuard Server Edition」とゲートウェイ型 WAF「SiteGuard Proxy Edition」は、製品をインストールする OS の数でライセンス数をカウントし、保護対象となる FQDN の数や通信量による課金はありません。そのため、バーチャルホストで多数のサイトを運用している場合やアクセス数の多いサイト、大きなサイズのファイルダウンロードやアップロードが必要な環境でも定額で、安心してご利用いただけます。

信頼と実績の純国産 WAF「SiteGuard シリーズ」に関するお問い合わせは、こちら
https://siteguard.jp-secure.com/

EG セキュアソリューションズ株式会社
〒 105-0001
東京都港区虎ノ門 1-2-8 虎ノ門琴平タワー 8F
TEL: 03-6257-3927　FAX: 03-6257-3928
E-Mail: sg-sales@eg-secure.co.jp
SiteGuard シリーズ製品サイト : https://siteguard.jp-secure.com/