

クラウド環境で使える WAFサービス8選



JIG-SAW株式会社

電話

03-6269-9810

サービス問合せ

<https://ops.jig-saw.com/form/contact>

Webサイト

<https://ops.jig-saw.com>

システム運用代行
に関するお問合せはこちら



はじめに

クラウド全盛の時代ですが、クラウド環境におけるWebサイトのセキュリティ対策として、WAFの導入は一般的になっています。

各メーカーやベンダにてWAFのソリューションは幅広く展開されていますが、クラウド環境においては、製品・サービスをどのように選定すればよいかわからないという方も多いと思います。

本コンテンツではWAFの各ソリューションの比較、選定のポイントを交えてご説明します。

なぜWAFの導入が必要なのか？

Webサイトのクラウド運用が普及している昨今、サイトを運営していく中でのセキュリティ対策は必須となってきました。一口にセキュリティ対策といっても、Webアプリケーションのセキュリティ対策、Webサーバ自身のセキュリティ対策、ネットワークのセキュリティ対策、運営に関わる人のセキュリティ対策など、多岐に渡ります。しかしながら、サイバー攻撃による被害を食い止めたい、情報を盗み取られることが心配、といった重要なセキュリティの課題に対して、まずはWebアプリケーションの対策を優先すべきです。

Webアプリケーションの主な脆弱性

代表的なWebアプリケーションの脆弱性について以下に示します。（IPA「安全なウェブサイトの作り方_改訂第7版」1.ウェブアプリケーションのセキュリティ実装より抜粋*1）

- SQLインジェクション

データベースと連携したWebアプリケーション上でSQL文の組み立て方法に問題がある場合に、攻撃によって不正利用をまねく可能性があります。

- OSコマンドインジェクション

外部からの攻撃によりWebサーバのOSコマンドを不正に実行されてしまう問題を持つものがあります。

- ディレクトリトラバーサル

Webサーバ内のファイル名を指定するパラメータの実装に問題がある場合に、公開を想定していないファイルを参照されてしまう可能性があります。

- セッションハイジャック

セッションIDの発行や管理に不備がある場合に、悪意のある人にログイン中の利用者のセッションIDを盗聴され、不正なアクセスを許す可能性があります。

- クロスサイトスクリプティング

利用者からの入力内容やHTTPヘッダの情報の出力処理に問題がある場合に、利用者のブラウザ上で不正なスクリプトが実行されてしまう可能性があります。

- クロスサイトリクエストフォージェリ

ログイン済み利用者のリクエストが意図したものであるかどうかを識別する仕組みを持たず、外部サイトを経由した悪意のあるリクエストを受け入れてしまう場合に、利用者が予期しない処理を実行させられてしまう可能性があります。

*1 <https://www.ipa.go.jp/files/000017316.pdf>

- HTTPヘッダイネクション

任意のレスポンスヘッダフィールドやレスポンスボディを作成する罣が仕掛けられ、この罣を踏んだ利用者のブラウザで偽のページが表示されたり、スクリプトが実行されたり、任意のCookieを保存させられたりする可能性があります。

Webアプリケーションのセキュリティ対策

完璧なプログラミングにより、Webアプリケーションそのものに脆弱性がない環境以外、大抵の環境は上記のWebアプリケーション脆弱性に対するリスクを内包しています。

現在では、プログラミングによる対応には限界があることが共通認識になっており、Webアプリケーションの脆弱性対策を容易に実装できるWAFソリューションの導入がトレンドになっています。

WAF選定のポイント

各メーカーやベンダにて展開されているWAFソリューションは以下のとおり大別されます。

WAFソリューションの分類

各メーカーやベンダにて展開されているWAFソリューションは以下のとおり大別されます。

- 製品型

WAFパッケージとして展開されているソフトウェア、もしくはソフトウェアとハードウェアの一体型の製品群が分類されます。

- クラウド型

ソフトウェア、ハードウェア、ライセンス等の初期購入が不要で、クラウドサービスとして提供されるWAFソリューション全般が分類されます。

上記大分類は、さらに以下のWAFソリューションに分類されます。

- ソフトウェア型（製品型）

Webサーバ上にWAFパッケージをインストールし、専用のGUIもしくはCLIにて、セキュリティポリシーの設定を行います。シグネチャ更新、誤検知発生時のポリシーチューニングなど、導入後の運用管理が必要となります。

- アプライアンス型（製品型）

Webサーバの前に配置し、リバースプロキシもしくはブリッジとして動作するWAF専用機で、セキュリティ対策を行います。ソフトウェア型同様に、シグネチャ更新、誤検知発生時のポリシーチューニングなど、導入後の運用管理が必要となります。

- マネージドサービス提供型（クラウド型）

WAFセンターにおいて運用管理全般を行い、トラフィックをWAFセンター経由とする形態もしくは、Webサーバにエージェントを導入する形態でWAF機能を提供します。シグネチャ、セキュリティポリシーなどのWAF運用管理はWAFセンターが行います。

- クラウドメニュー提供型（クラウド型）

AWS、GCP、Azureなどのパブリッククラウドにおいて、クラウドのメニューとして提供されるWAF機能で、スピーディにデプロイすることが可能です。セキュリティルールの作成と適用、およびメンテナンスを自動化する機能も提供されています。

クラウド環境におけるWAF選定のポイント

各WAFソリューションにはそれぞれ特徴が存在しますが、Webサイトがクラウド環境にて構築されている場合は、クラウド型WAFソリューションが高い親和性を有し、導入が容易です。（表1）

また、主要なクラウドサービス（AWS、GCP、Azureなど）にはWAF機能がメニューとして用意されているため、それらの利用により迅速な導入が可能となります。なお、現在ではクラウドサービスのWAF機能の運用を支援するサービスがあり、運用負荷の少ない、安心な仕組みを提供することが可能になっています。

代表的なWAFソリューション

各メーカーやベンダにて展開されているWAFソリューションの代表的な製品、サービスを一部ご紹介します。

■ソフトウェア型

- SiteGuard Server Edition（JP-Secure）

Webサーバのモジュールとして動作するホスト型WAF（ソフトウェア）製品です。Webサーバ自体にインストールするため、専用ハードウェアが必要ありません。ネットワーク構成を変更せず、できるだけシンプルに導入したいお客様に最適な製品です。

[https://siteguard.jp-](https://siteguard.jp-secure.com/product/siteguard-server-edition)

[secure.com/product/siteguard-server-edition](https://siteguard.jp-secure.com/product/siteguard-server-edition)

■アプライアンス型

- Barracuda WAF（Barracuda Networks）

Barracuda WAFは、2007年よりWAFの国内販売台数シェアNo.1。一般企業はもちろん、ECサイト、xSP(*2)、金融機関、行政、大学など、幅広い業種にご提供しています。

<https://www.barracuda.co.jp/products/waf/>

*2 ISPやASP、MSPなど、ネットワークを介してサービスを提供する各種サービスプロバイダの総称

表1 WAFソリューションにおけるコスト・運用負荷の比較

WAFソリューション	コスト	運用負荷(運用実施項目)
ソフトウェア型	導入時：中 運用時：小	大（セキュリティポリシーの個別チューニング、検知・防御ログの定期解析、ホワイトリスト・ブラックリストの登録、SSL証明書の更新、シグネチャ・ソフトウェアのアップデート、WAF導入に伴うサーバ負荷影響の監視）
アプライアンス型	導入時：大 運用時：中	大（セキュリティポリシーの個別チューニング、検知・防御ログの定期解析、ホワイトリスト・ブラックリストの登録、SSL証明書の更新、シグネチャ・ファームウェアのアップデート、WAF導入に伴うネットワーク負荷影響の監視）
マネージドサービス提供型	導入時：小 運用時：中	小（ホワイトリスト・ブラックリストの登録、SSL証明書の更新、動作・仕様の問合せ）
クラウドメニュー提供型	導入時：小 運用時：小	中（クラウドネイティブのマネージドロールの選定、検知・防御ログの定期解析、ホワイトリスト・ブラックリストの登録、SSL証明書の更新、動作・仕様の問合せ）

注1 Webサーバ2台程度の中規模環境を想定

注2 コストは製品・ライセンス、サービスの料金のみで比較

注3 導入時コストは大:100万円、中:50万円、小:~10万円です

注4 運用時コスト(月額)は中:~5万円、小:~2万円です

注5 下線部の運用実施項目は、クラウドWAF機能の運用支援サービスの利用により運用負荷の軽減が可能

■マネージドサービス提供型

- 攻撃遮断くん（サイバーセキュリティクラウド）

攻撃遮断くんは、外部からのサイバー攻撃を遮断し、個人情報漏洩、改ざん、サービス停止などからWebサイトを守るクラウド型Webセキュリティサービスです。

https://www.shadan-kun.com/?utm_source=google&utm_medium=cpc&utm_campaign=ksk_site-top

- Scutum（セキュアスカイ・テクノロジー）

Webアプリケーションの脆弱性を狙った攻撃からWebサイトを守る、クラウド型WAFサービスです。

<https://www.scutum.jp/>

■クラウドメニュー提供型

- AWS WAF

AWS WAF は、可用性、セキュリティ侵害、リソースの過剰消費に影響を与えるような、ウェブの脆弱性を利用した一般的な攻撃やボットから、ウェブアプリケーションまたは API を保護するウェブアプリケーションファイアウォールです。

<https://aws.amazon.com/jp/waf/>

- Cloud Armor（GCP）

Google Cloud Armor は、Google のグローバルインフラストラクチャとセキュリティ システムを使用して、インフラストラクチャとアプリケーションを分散型サービス拒否（DDoS）攻撃から保護します。

<https://cloud.google.com/armor/docs?hl=ja>

- Azure WAF

悪意のある攻撃や一般的な Web 脆弱性（SQL インジェクション、クロスサイト スクリプティングなど）から Web アプリを保護できます。

クラウドネイティブな Azure Web アプリケーション ファイアウォール（WAF）サービスは数分でデプロイできます。

<https://azure.microsoft.com/ja-jp/services/web-application-firewall/>

■AWS WAF / Azure WAF 運用支援サービス

- WafCharm（サイバーセキュリティクラウド）

WafCharm(ワフチャーム) は、世界中のWebに対する攻撃パターンをAIによって学習し、AWS WAF / Azure WAFのルールを最適化させるWAF自動運用サービスです。

<https://www.wafcharm.com/service/>

おわりに

WAFソリューションについて、クラウド環境に導入するなら、という観点で比較を行いました。製品・サービスごとにそれぞれ特徴がありますが、クラウド環境との親和性、導入の容易さ、スピードを考慮して検討する必要があります。中小規模の環境においては、コスト面でも有利であることが多いため、Webサイトがパブリッククラウド環境にて構築されている場合は、クラウドメニュー提供型のWAFソリューションの選定をお勧めします。

あなたのシステムにひとつ上のサポートを

JIG-SAWは、これまでにないシステム管理・支援サービスを提供します。
クラウドをはじめとしたあらゆるシステムの「サポート」を科学し、企業の成長を後押しします。



あらゆるシステム管理とサポートを強化

「JIG-SAW OPS」

クラウドや自社で保有されているシステム環境を、管理者様に代わって24時間体制で管理し、企業のシステム管理体制を強化します。
JIG-SAWが開発した「puzzle」を使用した異常検知/自動通知の仕組みと、エンジニアによる技術サポートを組み合わせたサービスをご提供します。お客様が本来の業務に注力し、事業を最大化できるよう、システム管理の側面から全面的にサービスを支援します。

ひとつ上のマルチクラウド包括支援サービス

「JIG-SAW プライム」

Amazon Web Services、Google Cloud、Microsoft Azureを、高いコストパフォーマンスでご利用いただける、マルチクラウドの包括支援サービスです。企業やプロジェクト単位で複数のクラウド、複数のアカウントをお持ちの場合でも、円建ての請求書発行から問合せ窓口まで、一元的に支援します。お困りごとがあれば、クラウドエンジニアによるプロフェッショナルで高品質なサポートをご利用いただけます。

JIG-SAW

お問い合わせ

TEL 03-6269-9810

JIG-SAW株式会社 〒100-0005 東京都千代田区丸の内1丁目4-1 丸の内永楽ビルディング23F

WEB : <https://ops.jig-saw.com>

※本資料の記事・写真等の無断複製や転載を禁止します。

※本資料は2021年5月に作成されたものです。掲載されている各種情報は作成時点のものです。