フォーティネットの AWS WAF 向け マネージドルール

AWS（Amazon Web Services）で Web アプリケーションの セキュリティを簡素化および強化する方法

目次

はじめに

消費者は、あらゆるデバイスで高品質なアプリケーションエクスペリエンスを求めていますが、革新的で最先端の開発により、あらゆる規模の企業にとって、その実現がかつてないほど容易になりました。今では、開発者は猛スピードで並外れた素晴らしいWebアプリケーションを構築できるようになっています。

同時に、セキュリティで保護されていないWebアプリケーションは攻撃者にとって容易な侵入経路となり、セキュリティ侵害の主流となっています[1]。企業としては、Webアプリケーションのセキュリティを確保し、規制基準に準拠するために、包括的なアプローチが不可欠となっています。しかし、高品質なアプリケーションの構築と配布に重要なリソースを割くことなく、これを実現する必要があります。

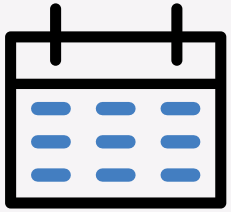
このeBookでは、現在の脅威の状況を説明し、最新の脅威からWebアプリケーションを保護するためのソリューションを提案しつつ、取り組みを達成できるようにガイドします。

脅威の状況

全体のうち
60%
の Web サイトで
重大な脆弱性が
少なくとも 1 つは存在 [2]

セキュリティ侵害の
86%
が金銭目的 [3]

データ侵害の
平均総費用は
約 424 万ドル [4]



平均
287 日
で侵害を特定 [5]

AWS を利用しても、Web ベースのアプリケーションやクラウドのデータを保護する責任は顧客自身にあります（AWS 共同責任モデルに準拠）。これはデータセンターの場合と同じです。アプリケーションレイヤーに対する攻撃と、規制圧力が日々ますます高まる中、Web アプリケーションを保護し、規制要件を遵守していくことが重要になります。

セキュリティ制御の管理に負担をかけずに、潜在的な脆弱性の数と多様性に対応していくには、アプリケーション環境全体で効率的なセキュリティプロセスを確立することが不可欠です。その最初のステップは、現在の環境に存在する脅威を理解することです。

一般的な Web アプリケーションの脅威

インジェクション攻撃

悪意ある攻撃者が不正な入力データを Web アプリケーションに注入する攻撃です。このデータをアプリケーションがコマンドの一部として処理することにより、プログラムの実行内容が変更されてしまいます。

例

SQL インジェクション：データ駆動型アプリケーションを攻撃するために使用されるのが一般的です。このインジェクションにより、悪意のある SQL クエリが Web アプリケーションの入力フィールドに挿入され、データベースを操って機密情報を公開します。

クロスサイトスクリプティング（XSS）：インジェクションの一種です。攻撃者は Web アプリケーションの入力フィールドから悪意のあるコードを埋め込み、第三者がアクセスしたときにスクリプトを実行させて不正サイトに誘導し、個人情報を盗んだり、マルウェアをダウンロードさせます。

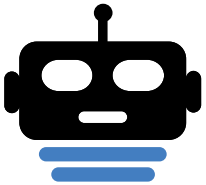
インクルード攻撃

Web アプリケーションを操作して悪意のあるファイルをプログラムに含めることを目的とした攻撃です。多くの場合、Web アプリケーションのファイルやスクリプトを動的に含める機能が利用されています。攻撃が成功すると、情報の漏えいやリモートでコードが実行されるのが一般的です。

例

リモートファイルインクルード（RFI）：外部ファイルやスクリプトを動的に受け入れる Web アプリケーションに対する攻撃で、攻撃者は悪意のあるリモートファイルを挿入します。

ローカルファイルインクルード（LFI）：悪意のあるユーザーが、Web アプリケーションを操り、Web サーバー上のファイルを読み込ませる攻撃です。ローカルファイルやスクリプトを動的に読み込む機能が利用されています。



悪意のあるボット

検索エンジンのインデックス作成など、反復作業を実行するときに使用される場合もありますが、多くの場合、マルウェアの形式で用いられます。このボットを使用すると、ハッカーが悪用できる Web ベースのアプリケーションの脆弱性を継続的に検索することができます。

例

脆弱性を探す Spider：悪意のあるデータマイニングツールです。Web サイトをスキャンして脆弱性のある領域を検出し、Web アプリケーションの悪用可能箇所を攻撃者に通知することができます。

コンテンツスクレイパー:スクリプトを実行すると、ユーザーの許可なく独自の用途のために元のコンテンツを盗むことができるボットです。ほとんどの場合、自動化ソフトウェアにより実行され、RSS フィードからコンテンツを盗み出し、それらを自分のサイトに投稿できるようになっています。

OWASP トップ 10

OWASP（Open Web Application Security Project）は、ソフトウェアのセキュリティ向上に焦点を当てた非営利の慈善団体です。OWASP では、さまざまなアプリケーションのセキュリティ脅威やこれらの解決方法の提案に関する記事を定期的に公開しています。

OWASP トップ 10 は、世界中のセキュリティ専門家たちによって作成された Web アプリケーションセキュリティの知識文書です。OWASP トップ 10 に掲載されているナレッジは、アプリケーションの保護を強化するのに役立ちます。さらに、クレジットカード決済を処理するアプリケーションに必要な PCI DSS（ペイメントカード業界データセキュリティ基準）など、多くの業界や規制基準の基盤ともなっています。

Web アプリケーションファイアウォール（WAF）

WAF は、特に規制対象のアプリケーション（PCI、HIPAA など）や個人を特定できる情報（PII）で処理するアプリケーションをはじめ、ビジネスクリティカルな Web アプリケーションを保護するための事実上の業界標準です。WAF には不正な Web トラフィックを防御するルール（シグネチャ）が多数用意されています。これにより、クロスサイトスクリプティングや SQL インジェクションなどの一般的な攻撃や、OWASP トップ 10 で説明されている他の脅威からアプリケーションを保護することができるようになっています。

Web アプリケーションのセキュリティを簡素化および強化

AWS WAF

AWS WAF は、導入しやすいソリューションで、多くの組織の基本的なニーズを素早く満たすことができます。また、Web アプリケーションセキュリティの管理を簡素化するために、Web セキュリティルールの作成、展開、管理を自動化できるフル機能の API（アプリケーションプログラミングインタフェース）を提供します。これらのルールにより、アプリケーションのトラフィックフローを制御したり、特有のニーズに合わせたルールを作成したりすることができるようになります。

AWS WAF のパートナールールを活用することで、管理をさらに簡素化することができます。このソリューションにより、セキュリティルールの作成をサードパーティの専門家に任せることができ、Web アプリケーションの開発に注力しやすくなります。

フォーティネットの AWS WAF 向けマネージドルール

フォーティネットのマネージド WAF ルールのパッケージを使用することにより、インフラストラクチャを管理することなく、AWS WAF 上でより堅牢なセキュリティ制御を高速かつ容易に確立できます。脆弱性や不正な攻撃者が新たに見つかると、ルールが自動的に更新されるため、セキュリティポリシーが最新の状態に保たれます。これにより、WAF の管理負荷が解消され、アプリケーションの開発に時間をかけることができるようになります。

選択肢は多様で、エントリーレベルの SQL インジェクションルールやクロスサイトスクリプティングルールから、OWASP トップ 10 パッケージ全体まで選択できます。

フォーティネット FortiWeb

FortiWeb は Web アプリケーションと API の堅牢な保護、ボット減災、高度なインサイトなど多数の機能を備えています。
AWS WAF では利用できない OWASP トップ 10 を包括した保護機能や機械学習による高度な検知レベルを可能にします。
AWS Marketplace にて FortiWeb Cloud の 14 日間の無料トライアルをぜひご利用ください。
詳細については、aws.fortiweb-cloud.com を参照してください。

フォーティネットの AWS WAF 向けマネージドルールオプション

OWASP トップ 10 を包括したルールグループ

このルールグループは、フォーティネットが管理する AWS WAF（SQLi/XSS、一般および既知のエクスプロイト、悪意のあるボットルールセット）のルールにすべて対応した包括的なパッケージとして機能し、OWASP トップ 10 の Web アプリケーションの脅威から保護します。

SQLi/XSS のルールグループ

SQLi/XSS ルールセットは、OWASP トップ 10 で特定された 2 大アプリケーション脅威である SQL インジェクションおよびクロスサイトスクリプティングに対する保護を提供します。

一般および既知のエクスプロイトのルールグループ

このルールセットは、OWASP トップ 10 で強調されている最も一般的で高度な脅威を検知します。これには、多くのインジェクション攻撃、リモートファイルインクルード（RFI）、ローカルファイルインクルード（LFI）、HTTP レスポンス分割、データベース漏えいの脆弱性、その他の共通脆弱性識別子（CVE）が挙げられます。

悪意のあるボットのルールグループ

悪意のあるボットルールグループは、OWASP によって識別されたコンテンツスクレイパー、Spider、および他の不要な自動化ツールを、Web アプリケーションにリスクをもたらすボットとして分析、リクエスト、ブロックします。

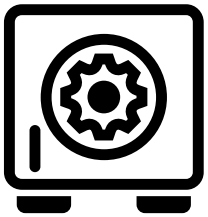
API ゲートウェイのルールグループ

このルールグループは、OWASP トップ 10 を包括したルールグループと同一の保護を提供しますが、AWS API ゲートウェイのセキュリティを確保するようにカスタマイズされています。

フォーティネットの AWS 向けマネージド WAF ルールのメリット

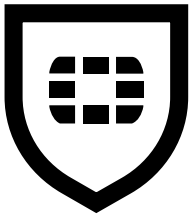
導入および管理の簡素化

AWS Marketplace で数回クリックするだけで利用開始できます。ルールセットをサブスクリプションで利用することで、AWS WAF コンソールで容易に構成できるようになります。また、トラフィックログを表示したり、必要に応じたアクションを実行したりすることができます。



高度なセキュリティ保護

フォーティネットでは、既存の AWS WAF を補完し、基本的なアプリケーションセキュリティのニーズを維持し、高度な機能でさらに複雑な脅威にも対応することで、OWASP トップ 10 の脅威からも保護できるようになります。



最新ルールを自動適用

フォーティネットの受賞歴を誇る FortiGuard Labs がバックボーンとなって、フォーティネット特有のルールグループを実現しています。また、利用している間は、ルールグループが自動的に更新されるため、フォーティネットが管理するルール保護が常に適用されます。

フォーティネットのパートナールールセット

フォーティネットのパートナールールセットにより、導入が簡素化され、WAF 管理が事実上不要になります。必要なのは、AWS WAF とフォーティネットのルールセットを導入することだけであり、Web アプリケーションを包括的に保護します。

4 つの簡単なステップで利用開始

AWS Marketplace でフォーティネットの AWS WAF 向けマネージドルールを導入する方法を紹介します。

1. **Web ACL に名前を付ける：**Web アクセスコントロールリスト（Web ACL）の名前を選択し、配置する地域と AWS リソースを指定します。

2. **条件を作成：**フォーティネットで定義した、Web アプリケーションを保護する AWS WAF 条件を 1 つ選択します。

3. **ルールを作成：**Web ACL にルールを追加して、環境内のルールを確立します。

4. **確認および作成：**導入を完了させます。

OWASP トップ 10 にも対応する、フォーティネットの AWS WAF 向けマネージドルールを
是非テストしてみてください。

今すぐ始める

[1]「2021 Data Breach Investigations Report」、Verizon、2021 年 8 月（英語）：https://www.verizon.com/business/resources/reports/dbir/

[2]「ESG Master Survey Results: Modern Application Development Security」、ESG、2020 年 11 月 19 日（英語）：https://www.esg-global.com/research/esg-master-survey-results-modern-application-development-security

[3]「2020 Data Breach Investigations Report」、Verizon、2020 年 5 月（英語）：https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report

[4]「Cost of a Data Breach Report 2021」、IBM、2021 年 7 月（英語）：https://www.ibm.com/security/data-breach

[5] 同上

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

EB-Managed-Rules-AWS-202203-R1