CLOUDFLARE

Webアプリケーションファイアウォール

SQLインジェクションやクロスサイトスクリプティングなどの攻撃からWebサイトを保護

CloudflareのWebアプリケーションファイアウォール（WAF）は、SQLインジェクション、クロスサイトスクリプティング（XSS）、ゼロデイ攻撃（OWASPが特定した脆弱性や、アプリケーションレイヤーを標的とする脅威など）からWebサイトを保護します。WAFは、Alexaの上位50のサイト、金融機関、Eコマース企業、大手企業など多数のお客様に利用されています。CloudflareのDDoS保護と完全に統合されており、毎日無数の攻撃をブロックしながら、新しい脅威が発生するたびにそれを自動的に学習します。

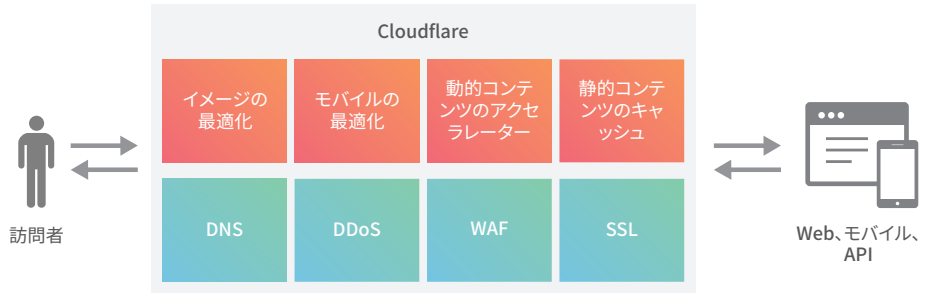
ニーズに合わせてカスタマイズできる強力なルールエンジン

WAFではModSecurityルールセットを追加設定なしで実行し、OWASPが特定した最も重大な欠陥からWebアプリケーションを保護できます。また、既存のルールセットやカスタムルールを実行できます。各ルールは30秒以内に有効になります。

クラウド展開とDDos軽減およびCDN

CloudflareのWAFはクラウドベースのサービスであるため、ハードウェアやソフトウェアをインストールして維持する必要はありません。1回のクリックで展開でき、ニーズに合わせてカスタマイズできます。

また、Cloudflareサービス全体と統合されているため、追加機能を無料で利用できます。WebサイトをDDoS攻撃から保護すると同時に、Cloudflareのグローバルコンテンツ配信ネットワークを活用してWebサイトを高速化できます。



要点：

- **自動保護**：DDoS軽減と完全に統合されたレイヤー7保護を提供する強力なデフォルトルールセットと、広範なカスタマイズ機能により、さまざまな脅威から保護します
- **0.3ミリ秒の非常に高速な処理時間**：即座のグローバル更新
- **PCI DSS要件6.6への準拠**：CloudflareのWAFを利用すれば、PCIコンプライアンスをコスト効率的に満たすことができます
- **リアルタイムのレポート作成**：強力なロギングにより、現在起こっていることを即座に把握できます
- **クラウド展開**：ハードウェア、ソフトウェア、調整は必要ありません

主な機能	メリット
セキュリティ	
アプリケーション／レイヤー7を対象とするディープパケットインスペクション	標準およびカスタムのWebアプリケーションがSQLインジェクションやクロスサイトスクリプティングなどのさまざまな攻撃から常に保護されます。
SSL	オーバーヘッドや追加のレイテンシーなしでSSL接続を終了します。SSLで暗号化されたトラフィックにWAFポリシーを適用します。証明書をアップロードしたり、高価なハードウェアソリューションを購入したりする必要はありません。
GETおよびPOST HTTP/HTTPS要求に対応	広範なHTTP/HTTPSトラフィックに対応します。
URLごとのカスタムルールセット	特定のURLやサブドメインをWAF保護の対象に含めたり対象から除外してドメインをテストすることも、特定のサブドメインを含めたり除外することもできます。
DDoS軽減との統合	DDoSに対するフルスタックの保護が可能です。追加の実装は必要ありません
IPレピュテーションデータベースとの統合	10億以上のIPに関するリアルタイムのインテリジェンスを活用して悪意のあるトラフィックをブロックします。追加の実装は必要ありません
仮想パッチ処理	お客様がサーバーにパッチを適用したりコードを更新したりする前に脆弱性を修正し、お客様が余裕を持ってパッチの適用や更新のテストを行えるようにします。
IPまたは地域別の制限	特定のIPアドレスや国からのトラフィックをブラックリストやホワイトリストに登録し、特定のIPアドレスや国のハッカーから保護できます。
低い誤検出率	全体的な誤検出率が5,000万分の1と非常に低いため、サイトへのトラフィックが適正であることが保証されます。
CDNサービスとの完全な統合によるアウトバウンドのコンテンツトランスフォーメーション	サイト訪問者のWebレイテンシーを削減します。追加の実装は必要ありません。
ルールセット	
自動学習とセキュリティ主導の調査	Cloudflareのセキュリティチームによって自動的に展開されるパッチにより、ゼロデイ脆弱性や新しい脅威から保護します。
ModSecurityロジックおよび形式との互換性	既存のルールセットを簡単にインポートして既存の保護を保持できます。
OWASP ModSecurityのコアルールセット	Open Web Application Security Project（OWASP）によって特定された最も重大な欠陥であるOWASP脆弱性から保護します。この機能はデフォルトとして含まれており、追加料金なしで使用できます。
ゼロデイCloudflareルールセット	Cloudflareのセキュリティチームが、Cloudflareの顧客ベースで特定した脅威からお客様を保護します。この機能はデフォルトとして含まれており、追加料金なしで使用できます。
主要なCMSおよびEコマースプラットフォーム向けのプラットフォーム固有のルールセット	WordPress、Joomla、Plone、Drupal、Magneto、IISなどのプラットフォームを追加設定なしで保護できます。追加料金はかかりません。
カスタムルール	お客様のWebアプリケーションに固有の状況に対応します。BusinessプランおよびEnterpriseプランでご契約のお客様については、この機能はデフォルトとして含まれており、追加料金なしで使用できます。
WAF設定	
ブロック	攻撃をブロックし、Webサイトに対するアクションを未然に防ぎます。
シミュレート	誤検出をテストするには、WAFをシミュレートモードに設定します。このモードでは、攻撃の可能性があるトラフィックに対する応答が、チャレンジやブロックなしで記録されます。
チャレンジ	チャレンジページでは、Webサイトへのアクセスを続行する訪問者にCAPTCHAを送信するよう要求します。
しきい値／感度設定	ルールのトリガー感度を設定します。
カスタマイズ可能なブロックページ	訪問者がブロックされたときに表示されるページをカスタマイズします（「詳細については、こちらの電話番号までお問い合わせください」など）。この機能は、Enterpriseのお客様が利用できます。
レポート作成	
リアルタイムロギング	WAFの微調整に役立つj情報を可視化できます。
未加工ログファイルへのアクセス	Enterpriseのお客様は、すべてのWAFリクエストを対象に詳細な分析を実行できます。
管理	
高可用性（SLAを提供するサービスを基盤に構築）	BusinessおよびEnterpriseのプランでは100%の稼働時間が保証され、100%の稼働時間が達成できなかった場合には、違約金が支払われます。
ハードウェア、ソフトウェア、調整が不要	DNSを少し変更するだけで利用できます。
PCI認定	Cloudflareのサービスは、レベル1サービスプロバイダー認定を受けています。