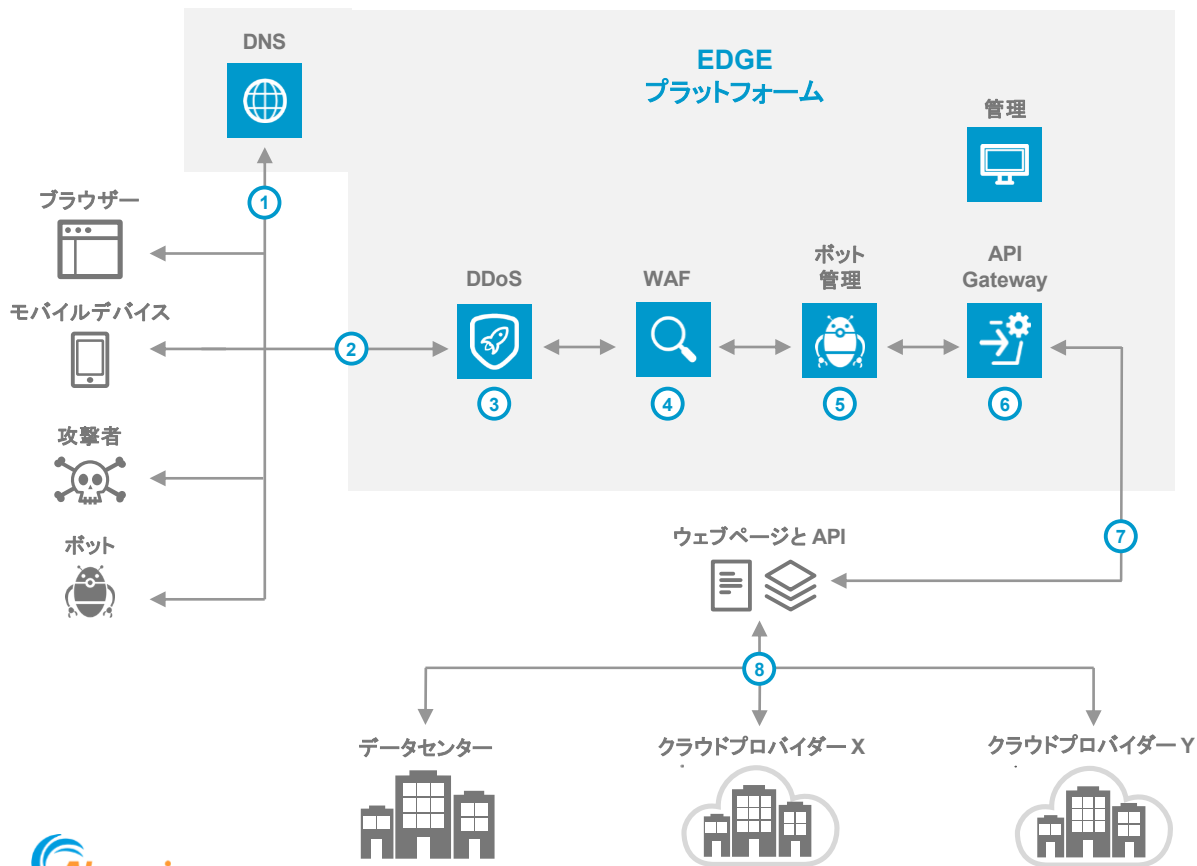


マルチクラウドのセキュリティ確保

リファレンスアーキテクチャ



概要

Akamai Intelligent Edge Platform を導入すると、複数のクラウドを利用している環境で、ユーザー体験のセキュリティと一貫性が大幅に向上します。セキュリティの制御を一元化できるため、現在のセキュリティ対策を維持しながら、ビジネス上のニーズに合わせてスタッフやリソースを拡充できます。

- 1 クライアントは、最大規模の DDoS 攻撃に対処できる規模を誇る Akamai の DNS サービスに対して DNS ルックアップを実行します。
- 2 ユーザーは、Akamai Intelligent Edge Platform を介してウェブアプリケーションにアクセスします。
- 3 エッジサーバーが、ネットワークレイヤーに対する DDoS 攻撃を自動的に破棄し、アプリケーションレイヤーへの DDoS 攻撃にも数秒で対応します。
- 4 Web Application Firewall がウェブリクエストを検査し、SQL インジェクション、XSS、RFI のような悪意のある脅威をブロックします。
- 5 ボット管理によりボットトラフィックを識別して管理し、さまざまな高度な条件付きアクションにより制御します。
- 6 API Gateway が、モバイルアプリのような API 利用者からのリクエストを認証、承認、制御して API トラフィックを管理します。
- 7 Akamai Intelligent Edge Platform が、適切なブラウザとモバイル（および許可されたボット）のトラフィックをウェブアプリケーションに転送します。
- 8 ウェブアプリケーションは、単一または複数のプロバイダーによるオンプレミスまたはクラウドのデータセンターを任意に組み合わせた環境に展開できます。

キープロダクト

DNS • Fast DNS

DDoS • Kona Site Defender または Web Application Protector

WAF • Kona Site Defender または Web Application Protector

API 保護 • Kona Site Defender または Web Application Protector

ボット管理 • Bot Manager

API ガバナンス • API Gateway