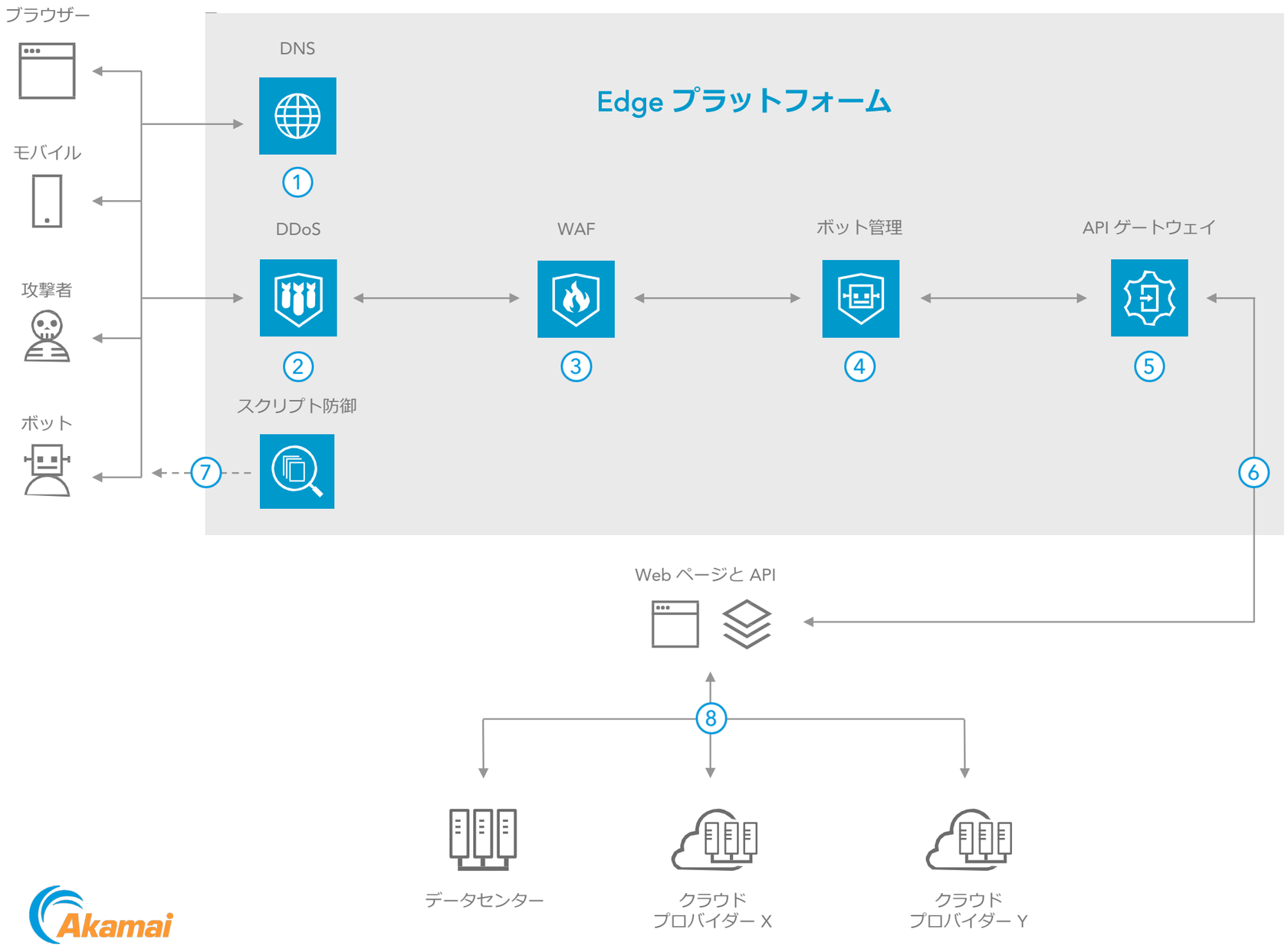
マルチクラウドのセキュリティ確保

リファレンスアーキテクチャ



概要

クラウドへの移行は、クラウドジャーニーという継続的な取り組みプロセスの最初のステップに過ぎません。次のステップでは、複数のクラウドプロバイダーを同時に採用し、ビジネス、アプリケーション、開発者チームにとって有効なさまざまな機能を活用します。

複数のクラウド環境に導入されたアプリケーションの保護を担当するセキュリティチームには、一貫したセキュリティ対策を維持する単一のセキュリティ制御セットが必要です。また、ビジネスのニーズに合うようにスタッフやリソースをスケーリングできることも要件になります。

1. 権威 DNS がクライアントのルックアップリクエストを解決し、最大規模の DDoS 攻撃を防御します。
2. 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。
3. Web Application Firewall が Web リクエストを検査し、SQL インジェクション、XSS、RFI のような脅威をブロックします。
4. 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。
5. 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。
6. Akamai Intelligent Edge Platform が、適切なブラウザーとモバイル（および許可されたボット）のトラフィックを Web アプリケーションに転送します。
7. スクリプト防御がサードパーティスクリプトのふるまいを監視して、Web スキミングと Magecart 型攻撃を特定し、緩和します。
8. Web アプリケーションは、プロバイダー数も単一でも複数でも可能、またデータセンターもオンプレミスでもクラウドでも可能と、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 ▶ Edge DNS
DDoS ▶ Kona Site Defender または Web Application Protector
WAF ▶ Kona Site Defender または Web Application Protector
API 防御 ▶ Kona Site Defender または Web Application Protector
Bot 管理 ▶ Bot Manager
API ゲートウェイ ▶ API Gateway
スクリプト保護 ▶ Page Integrity Manager

公開日：2020 年 8 月