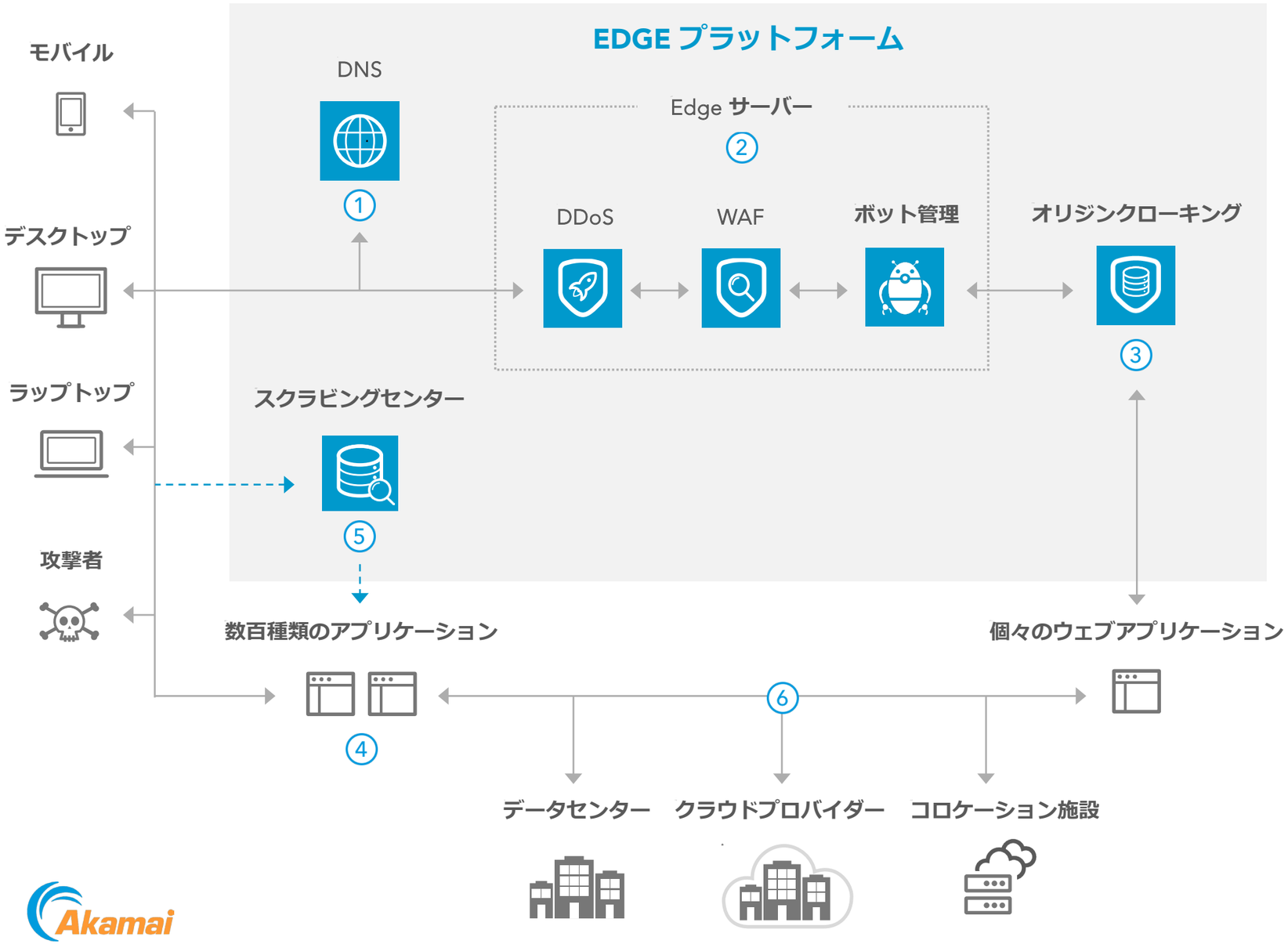
DDoS 防御

リファレンスアーキテクチャ



概要

Akamai は、迅速かつ効果的な防御により DDoS 攻撃のリスクを緩和します。この防御機能は、最大規模かつ最も巧妙な DDoS 攻撃に対抗できるように設計されており、データセンターやパブリック・クラウド・インフラストラクチャ、コロケーション施設など、展開場所にかかわらずアプリケーションを保護します。

1. クライアントは、最大規模の DDoS 攻撃も吸収した 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. Edge サーバーは、DDoS 攻撃、ウェブアプリケーション攻撃、ボット攻撃を検知するために CDN トラフィックを自動的に検査し、悪性の脅威を阻止します。
3. Akamai は、指定された Edge サーバー経由で CDN トラフィックをルーティングし、他のソースから発生したトラフィックをドロップして、攻撃がエッジベースの防御をバイパスするのを防ぎます。
4. 通常、非 CDN トラフィックは、お客様の BGP ルート広告に基づき、オリジンに直接ルーティングされます。
5. お客様は、Akamai スクラビングセンター（常時稼働またはオンデマンド）を経由してトラフィックをルーティングできます。スクラビングセンターでは、事前対応型の緩和制御またはアクティブ SOC 緩和で DDoS 攻撃をブロックします。
6. Akamai の CDN ベースサービスと DDoS スクラビングサービスは、お客様のデータセンター、パブリック・クラウド・インフラストラクチャ、コロケーション施設に展開されたアプリケーションをいずれも防御できます。

キープロダクト

DNS ▶ Edge DNS
DDoS／WAF ▶ Kona Site Defender または Web Application Protector
ボット ▶ Bot Manager
スクラビングセンター ▶ Prolexic Routed

公開日：2020 年 3 月