AKAMAI 製品概要

Edge DNS — 包括的な DNS セキュリティ

ドメイン・ネーム・システム（DNS）は、人間が判読可能なドメイン名を数値の IP アドレスに変換するシステムで、Web サイトへの訪問者やアプリケーションユーザーに質の高い Web 体験を提供するために必須の要素です。

DNS がダウンすると、オンラインプレゼンスも低下します。Akamai Edge DNS は、クラウド、オンプレミス、ハイブリッドのいずれの環境であっても、DNS インフラに対するさまざまな DNS 攻撃から包括的に保護します。また、高レベルの DNS パフォーマンス、回復力、可用性も提供します。

今日の DNS 分散型サービス妨害（DDoS）攻撃はかつてないほど大規模かつ高度になっており、DNS インフラの 24 時間 365 日の可用性に依存するグローバル企業にとって、こうした攻撃に対抗する保護が非常に大きな課題となっています。

Akamai Edge DNS は、以下を提供する外部の権威 DNS ソリューションです。

- **包括的なセキュリティ。**頻繁に発生する大規模で高度な攻撃から、クラウド、オンプレミス、ハイブリッドの DNS インフラを保護します
- **比類のないパフォーマンス。**世界で最も分散されたネットワークがオリジンの負荷を軽減し、24 時間 365 日の可用性を提供し、ページの読み込み時間を短縮します
- **直感的な管理。**DNS ゾーンを自己設定して管理し、独自の動的ポリシーをリアルタイムで適用できます

世界中に分散された Anycast ネットワーク上に構築されているため、Edge DNS をプライマリまたはセカンダリの DNS サービスとして実装し、必要に応じて既存の DNS インフラの代替とすることも、補助として追加することもできます。

主な機能

ノンストップの DNS 可用性

Akamai Connected Cloud は、世界中に数千台の DNS サーバーを擁しているため、ミッションクリティカルな DNS の可用性を確実に実現します。また、DNS の可用性はインターネット対応のセカンダリゾーンを使用することで強化できます。

Edge DNS には 100% アップタイムのサービスレベル契約（SLA）が付属しているため、顧客であっても社員であっても、お客様の Web サーバーやアプリケーションサーバーに確実に接続できます。

ビジネス上のメリット

DDoS 攻撃から DNS を保護します。
重要な DNS インフラを DNS 偽装から保護し、ブランドなりすましやフィッシングが発生しやすいゾーンを監視します。

DNS をノンストップで利用できるようにします。
グローバルに分散された Akamai の数千台の DNS サーバー、インターネット対応のセカンダリゾーン、100% アップタイム SLA により、DNS が常時利用できる状態に保たれます。

統合された DNS ソリューションでワークフローを簡素化します。
ゾーンおよびトラフィックの管理ポリシーと、ワークフローをプロビジョニングして設定できます。

迅速な応答により、ユーザー体験を向上させます。
高速で信頼性の高い DNS クエリーの解決ができます。

セキュリティチームを強化します。
DNS ゾーンを簡単にカスタマイズして、ワークフローを自動化し、ネットワークの変更を最小限に抑えます。

DNS DDoS 攻撃に対する包括的な防御

Edge DNS は、正当なユーザーリクエストに対応しながら最大規模の DNS DDoS 攻撃さえも吸収する、インテリジェントなアーキテクチャを備えた、拡張性の高い DNS プラットフォームを提供します。

オプションの DNSSEC 機能を使用すると、DNS 偽装による攻撃を防いで、ブランドなりすましやフィッシングドメイン名がないかゾーンを監視できます。

攻撃を受けても、ユーザーは快適なオンライン体験に引き続きアクセスできます。

DNS クエリーに対する高速かつ最適化された応答

Edge DNS は、ネットワークの状態に基づいて、最も近い高パフォーマンスの DNS サーバーからのユーザークエリーにインテリジェントに応答することで、DNS インフラの応答性を向上させ、最適化します。

世界各地に分散している Anycast ネットワークによって、世界のどこからお客様の Web サイトやアプリケーションに接続するユーザーであっても、DNS ソリューションが加速します。Zone Apex Mapping により、Akamai Connected Cloud のサイトでの DNS ルックアップ時間がさらに短縮し、パフォーマンスが向上します。

柔軟な設定と統合

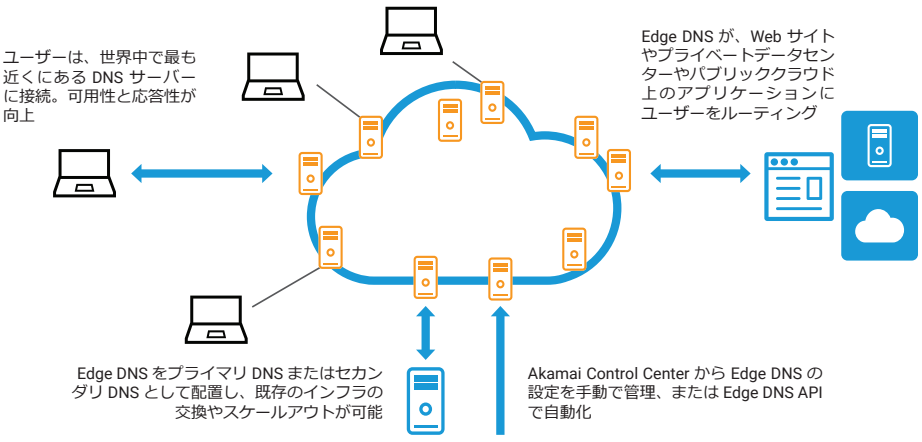
Edge DNS では、Akamai Control Center、API、Terraform などのツールを使用して、プライマリとセカンダリの DNS ゾーンをカスタマイズできます。

さらに、API を介して Edge DNS と標準の DevOps ツールキットおよびリソースを統合することで、お客様のネットワークインフラチームが DNS ワークフローをシンプル化および自動化できます。

動的な応答ポリシー

Akamai では、ゾーン管理とトラフィック管理の両方をプロビジョニングして設定するために、ソリューションを 1 つにすることの重要性を認識しています。Edge DNS には、Akamai Global Traffic Management の以下の機能が含まれています。

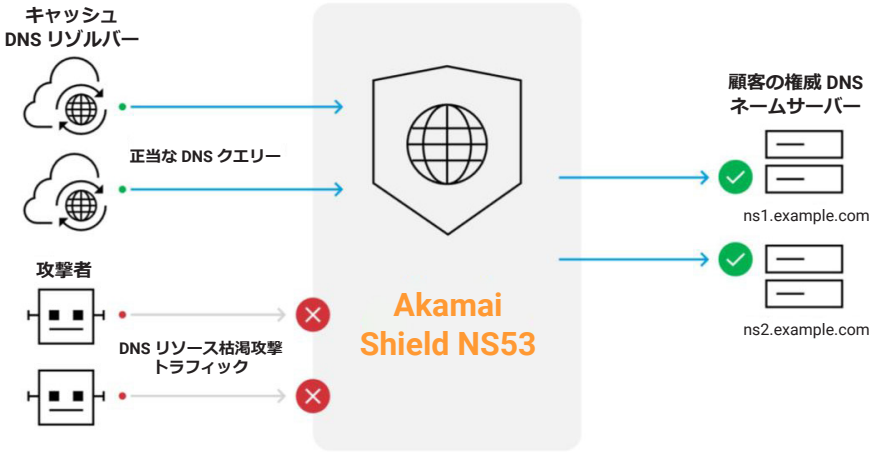
- 地域固有の応答などのポリシーを設定するためのシンプルなワークフロー
- DNS ワークフローの拡張性と柔軟性へのアクセス
- コンプライアンスなどの固有要件に低コストで対応



オンプレミスとハイブリッドの DNS インフラを保護

Akamai Shield NS53 は、双方向 DNS リバース・プロキシ・ソリューションです。オンプレミスとハイブリッドの DNS インフラ（Global Server Load Balancers ／ GSLB、ファイアウォール、ネームサーバーなど）をリソース枯渇攻撃（NXDOMAIN など）から守ります。独自の動的セキュリティポリシーの自己設定、管理、適用をリアルタイムで行えます。不正な DNS クエリーと DNS 攻撃フラッドはネットワークのエッジで阻止されるため、オンラインプレゼンスを支える重要な DNS インフラを保護できます。

Shield NS53 は、キャッシュからの正当なクエリーに応答し、必要な場合のみオリジン・ネーム・サーバーにクエリーを転送することによって、オンプレミスインフラの負荷軽減にも役立ちます。また、このソリューションは、Akamai の グローバルなサーバーの Anycast ネットワークにアクセスして、最も近い場所からユーザーのクエリーに応答することで、レイテンシーを低減し、ユーザー体験を向上させます。



DNS のセキュリティとパフォーマンスを強化

Akamai Edge DNS と Shield NS53 は、正当なユーザークエリーに確実かつ迅速に対応しながら、ネットワークのエッジで最大規模の DNS DDoS 攻撃をも阻止するように構築されています。

無料トライアルに登録するには、Akamai Edge DNS ページにアクセスするか、Akamai の営業担当チームまでお問い合わせください。

 | サポート | | 公開日：2025 年 4 月