AKAMAI ソリューション概要

# エンドツーエンドのゼロトラストで シンプル化とセキュリティ確保を実現

ゼロトラストは、ユーザー、デバイス、ネットワーク、データ、アプリケーション全体にわたって暗黙的な信頼を排除することで組織の安全を確保する、サイバーセキュリティに対する戦略的アプローチです。ゼロトラスト・アプローチは、企業ファイアウォールの内側にあるものがすべて安全であると想定するのではなく、常に侵入を受けることを警戒し、要求の発信元がどこかに関係なく、最小限のアクセス権限を適用します。

## ゼロトラストがいま注目されている理由

ゼロトラストは、常に変化する最近の環境に対してより効果的に適応する必要がある組織にとって、最優先事項となっています。これらの組織は、ハイブリッドな働き方を受け入れ、場所を問わずユーザー、デバイス、アプリを保護できる新しいセキュリティモデルを求めています。

## 最新のゼロトラスト・アーキテクチャの原則

- 明示的に、常にコンテキストに沿って検証する
- 明示的に最小権限を適用する
- 継続的に監視する

## 統合が不可欠

### 統合型のエンドツーエンドアプローチ

ゼロトラストに対して総合的なアプローチを採る場合は、アイデンティティ、ネットワーク、アプリケーションなど、組織のすべてのエンティティをカバーする必要があります。ゼロトラストは、エンドツーエンドの戦略として機能するため、すべての要素を統合する必要があります。複数のポイントソリューションを緩やかに統合するやり方は、この戦略的アプローチには適しません。

Akamai は、現代の組織にとって不可欠なゼロトラスト・ソリューションをすべて揃えた、包括的で堅牢なポートフォリオを構築しました。複数のセキュリティ製品をインストール、実行、およびパッチ更新する代わりに、必要なすべてのテクノロジーを単一ベンダーに任せることができるため、コストを削減し、運用効率を向上させることができます。

### ソリューション間でのシグナルの共有

Akamai はゼロトラスト・ポートフォリオに自動化を組み込んでいるため、複雑さやカスタマイズに伴う負担が大幅に軽減されています。そのため、ポートフォリオ製品はすべての製品で脅威に関する知識を共有できるようになり、各製品のセキュリティを高めています。ある製品が脅威を特定した場合、その脅威を緩和するために別の製品にアラートを送信します。

## 利点

- **従業員の分散**
  ユーザーは時間、場所、デバイスを選ばずに安全に仕事ができる
- **クラウド移行**
  クラウド環境やハイブリッドクラウド環境全体を通してセキュアなアクセス制御を提供する
- **リスク緩和**
  ランサムウェアなどのマルウェアのラテラルムーブメント（横方向の移動）を最小限に抑える
- **コンプライアンス**
  機微な情報をマイクロ境界で囲み、コンプライアンス確保をサポート

Akamai

# ユーザー、アプリケーション、ネットワークをカバーする包括的なエンドツーエンドのポートフォリオ

## ワークロードのセキュリティ確保
**Akamai Guardicore Segmentation：アプリケーションのためのゼロトラスト**

Akamai Segmentation は、ランサムウェアなどのマルウェアの拡散を制限するように設計された、業界をリードするマイクロセグメンテーションソリューションを提供します。この製品は、ワークロード、プロセス、アプリケーションを可視化、確認できるようにし、アクセスポリシーを実現します。

## ネットワークのセキュリティ確保
**Enterprise Application Access：ゼロトラスト・ネットワーク・アクセス（ZTNA）**

Akamai のゼロトラスト・ネットワーク・アクセス・テクノロジーは、従来の VPN テクノロジーに代わる強力なユーザーアイデンティティを実現するように設計されています。Enterprise Application Access は、ネットワーク全体を危険にさらすことなく、ユーザーが役割を担う上でそのアプリケーションにアクセスする必要があるかどうかに基づいてユーザーアクセスを許可します。Enterprise Application Access により、ユーザーのアイデンティティが可視化され、識別と認証の強度が高まります。

## ユーザーのセキュリティ確保
**Secure Internet Access：ゼロトラストのインターネットアクセス**

Secure Internet Access は、クラウドベースのセキュア Web ゲートウェイソリューションです。Secure Internet Access はユーザーのすべての Web リクエストを検査し、リアルタイムの脅威インテリジェンスと高度なマルウェア分析テクニックを適用して、安全なコンテンツのみが配信されるようにします。悪性のリクエストやコンテンツは事前にブロックされます。

**多要素認証：強力なゼロトラスト・アイデンティティ**

Akamai MFA は、従業員アカウントをフィッシングなどの中間マシン攻撃から保護します。これにより、強力な認証に成功した従業員のみが自分が所有するアカウントにアクセスでき、それ以外のアクセスは拒否され、従業員アカウントの乗っ取りが防止されます。

## 追跡と監視
**脅威ハンティング：セキュリティサービス**

Akamai の脅威ハンターの精鋭チームは、「常に侵害を受ける可能性があることを前提とする」アプローチを採用することで、標準的なセキュリティソリューションでは検知が困難な異常な攻撃のふるまいや高度な脅威がないかどうかに常に目を光らせています。当社の脅威ハンターは、お客様のネットワークで重大なインシデントを検知すると直ちにお客様に通知し、お客様のチームと密接に連携を取りながら状況を改善します。

# Akamai の優位性

Akamai には、他のゼロトラスト・ベンダーとは異なる利点がいくつかあります。従来型と最新型、Windows 対応と Linux 対応、オンプレミスと仮想化、コンテナなど、幅広いサービスを提供しています。当社の優れた可視化機能により、ユーザーは各ワークロードがどのように動作しているかを完全に把握することができます。社内の優秀な脅威ハンティングサービスがセキュリティチームの能力を向上させているため、脅威の先を行くことができます。

**ゼロトラストの詳細と開始方法については、akamai.com をご覧ください。**

 | サポート | 公開日 2022 年 6 月