

## AKAMAI ソリューション概要

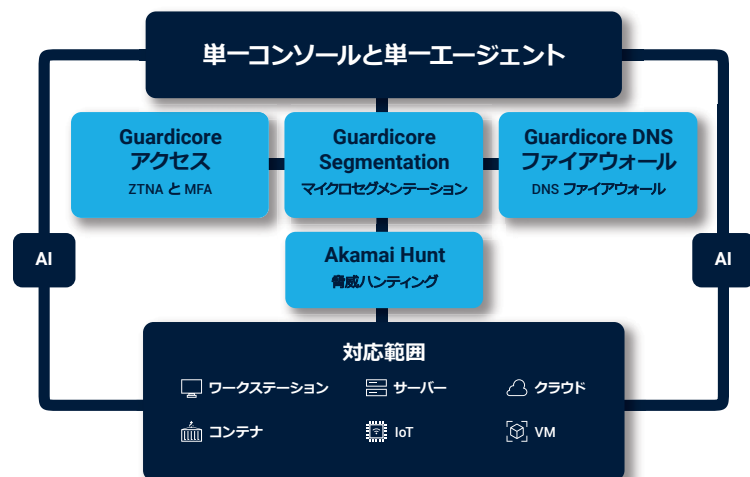
# Akamai Guardicore Platform : ゼロトラスト・セキュリティ

ゼロトラストの導入は、ほとんどの企業にとって非常に複雑でコストがかかります。特に、オンプレミスやクラウドのアセット、リモートまたはオフィス内の従業員を保護対象とする場合に、これが当てはまります。そのため、Akamai Guardicore Platform は、ゼロトラストのあらゆる側面に単一のコンソールと単一のエージェントで効率的に対応できるように構築されています。

サイバー脅威がますます巧妙化し、規制要件が厳しくなり続けているため、組織は運用効率を維持しながらネットワークを保護するという大きなプレッシャーに直面しています。Akamai Guardicore Platform は、堅牢なゼロトラスト・セキュリティ・モデルを効果的に導入するために必要なツールと機能を組織に提供することでこれらの課題に対処する、包括的なゼロトラスト・ソリューションです。

このプラットフォームは、トップクラスのマイクロセグメンテーション、ゼロトラスト・ネットワーク・アクセス (ZTNA)、DNS ファイアウォール、脅威ハンティングを1つのプラットフォームに統合することで、ゼロトラスト・プロジェクトを実現するように構築されています。これらのコンポーネントが連携することで、ゼロトラストの取り組みが合理化され、アタックサーフェスが大幅に削減され、エンタープライズ全体のセキュリティ体制が強化されます。

## Akamai Guardicore Platform



## マイクロセグメンテーション

Akamai Guardicore Platform の主要コンポーネントの1つは、マイクロセグメンテーションです。従来、ネットワークセキュリティは、ネットワークの外部境界のセキュリティ確保に重点を置いた境界ベースの防御に依存してきました。しかし、サイバー脅威が進化するにつれて、境界防御はもはや高度な攻撃の阻止には不十分であることがますます明白になっています。

## メリット



### 統合型インフラ

パフォーマンスへの影響を最小限に抑えながら、迅速に展開し、容易にスケーリング。



### 幅広く豊かな可視性

ネットワークアセットと通信に関する包括的な知見を獲得。



### 統一されたポリシーエンジン

単一のUIからさまざまな環境でのポリシー適用をシンプル化。



### モジュール式による柔軟性

お客様のビジネス要件に合わせたモジュール式コンポーネントを活用。



### 完全なカバー範囲

オンプレミスとクラウドのすべてのアセット、および在宅とオフィスのユーザーを保護。



### トップクラスのソリューション

業界をリードするマイクロセグメンテーションとZTNAを組み合わせて、セキュリティ体制を強化。



マイクロセグメンテーションは、ネットワークをより小さく管理しやすいセグメントに分割し、最小権限の原則に基づいて各セグメントにセキュリティポリシーを適用するという、異なるアプローチを取ります。このようにきめ細かいセキュリティアプローチにより、1 つのセグメントが侵害されても、残りのネットワークは保護されたままになります。Akamai Guardicore Segmentation を利用すれば、オンプレミスのデータセンター、クラウドインスタンス、レガシー OS、IoT デバイス、Kubernetes クラスターなど、あらゆる資産が保護されます。しかも、コンソールを変更する必要はありません。

## ゼロトラスト・ネットワーク・アクセス (ZTNA)

Akamai Guardicore Platform は、マイクロセグメンテーションに加え、ゼロトラスト・ネットワーク・アクセス (ZTNA) 機能も提供します。ZTNA はゼロトラストを前提としたセキュリティモデルです。つまり、企業ネットワーク内に存在しているからといって、デフォルトでユーザーやデバイスが信頼されることはありません。その代わりに、アイデンティティ、デバイスポスチャー、その他のコンテキスト要素の厳密な検証に基づいて、リソースへのアクセスが許可されます。このアプローチは、不正アクセスのリスクを最小限に抑え、組織がデータ漏えいや内部ユーザーによる脅威を防止するうえで役立ちます。

## DNS ファイアウォール

Akamai Guardicore プラットフォームのもう 1 つの重要なコンポーネントが、DNS ファイアウォールです。DNS (ドメイン・ネーム・システム) は、人間が読めるドメイン名を IP アドレスに変換する、インターネットの基本コンポーネントです。しかし、多くのマルウェアバリエーションが DNS を利用してコマンド & コントロールサーバーと通信したりデータを流出させたりするため、DNS はサイバー攻撃の一般的なターゲットとなっています。DNS ファイアウォールを展開することで、組織は悪性の DNS クエリーをブロックし、マルウェアが悪性ドメインと通信できないようにして、データ漏えいやその他のサイバー脅威のリスクを軽減できます。

## 脅威ハンティング

最後に、Akamai Guardicore Platform には、セキュリティ脅威が本格的なインシデントにエスカレートする前に組織がそれをプロアクティブに特定して緩和できるようにする、適応型セグメンテーションサービスが含まれています。脅威ハンティングでは、異常なふるまいや脅威の痕跡情報 (IOC) など、ネットワーク内の侵害の兆候を積極的に探します。脅威ハンティングのツールや手法を活用することで、サイバー攻撃者の一歩先を行き、貴重な資産を損害から守ることができます。

Akamai Guardicore Platform には、コア機能以外にも、市場の他のセキュリティソリューションとは異なるいくつかの重要な利点があります。このプラットフォームは、エージェントの肥大化とコンソール疲れを最小限に抑える、軽量の統合型インフラを提供し、組織がセキュリティスタックをより効率的に展開および管理できるようにします。さらに、このプラットフォームは、ネットワークアセットと通信に対する幅広く豊かな可視性をもたらし、セキュリティ専門家がネットワーク環境に関する包括的な知見を得て、脅威に迅速かつ効果的に対応できるようにします。



Gartner は、ゼロトラスト・ネットワークング (ZTN) に移行するためにマイクロセグメンテーションや ZTNA を導入することを提案しています。

– Gartner®, Quick Answer :  
What Is Zero Trust Networking?  
Andrew Lerner 氏、John Watts 氏、2023 年 9 月 13 日\*

詳しくは、[Akamai ゼロトラスト・セキュリティの Web ページ](#)をご覧ください。

\*GARTNER は、Gartner, Inc. またはその関連会社の米国およびその他の国における登録商標およびサービスマークであり、同社の許可に基づいて使用しています。All rights reserved.