ホワイトペーパー

Akamai で ゼロトラスト成熟度を達成

連邦政府機関に対する CISA の 横断的機能サポート

概要

ゼロトラスト・セキュリティは、機密性の高い政府データ、重要なインフラ、および国家安全保障システムを保護するためのゴールドスタンダードとなっています。連邦政府機関は、従来の境界ベースのセキュリティモデルに頼っていては、現代の脅威に対抗できなくなりました。サイバー犯罪者は、認証情報の盗難、ランサムウェア、内部ユーザーによる攻撃などの巧妙な手口を使い、ますます進化しています。これに伴い、連邦政府組織はセキュリティポスチャのゼロトラスト・フレームワークへの移行を進めています。しかし、この移行は断片化されており、連邦システムのセキュリティを確保するためにはさらに多くの対策を講じる必要があります。

Cybersecurity and Infrastructure Security Agency（サイバーセキュリティ社会基盤安全保障庁、CISA）のゼロトラスト成熟度モデルは、連邦政府機関が暗黙的な信頼を排除し、厳格な検証メカニズムを実施するセキュリティ原則を実装するのに役立ちます。このモデルは、次の 5 つの基本的な柱に基づいて構築されます：アイデンティティ、デバイス、ネットワーク、アプリケーションとワークロード、データ。さらに、可視性と分析、自動化とオーケストレーション、ガバナンスの 3 つの横断的機能により、サイバーセキュリティに対する包括的で一貫したアプローチを確保できます。

これらの目標を達成するためには、マイクロセグメンテーションをゼロトラスト・セキュリティの中核と考え、内部（水平方向）のネットワーク防御の基本的な構成要素として捉える必要があります。ワークロードをセグメント化し、ラテラルムーブメント（横方向の移動）を制限することで、連邦政府組織は潜在的な侵害を阻止し、ゼロトラスト・ポリシーを適用できます。さらに、外部（垂直方向）の通信を保護し、承認された組織のみが政府のアプリケーションにアクセスできるようにするために、包括的なアプリケーション・プログラミング・インターフェース（API）セキュリティソリューションを実装する必要があります。

このホワイトペーパーでは、ゼロトラスト成熟度を達成するための重要なステップについて説明します。Akamai Guardicore Segmentation、Akamai API Security、Akamai Enterprise Application Access などの Akamai の高度なセキュリティソリューションによって、連邦政府機関が CISA のガイドラインを満たし、サイバーセキュリティポスチャの強化を支援する仕組みに焦点を当てています。

境界ベースのセキュリティからゼロトラストへのシフト

従来のサイバーセキュリティは、境界ベースの防御を重視しており、いったんネットワーク内に入ったエンティティは信頼できるものとされていました。しかし、現代のサイバー脅威に直面し、このモデルは失敗を繰り返してきました。攻撃者は、脆弱な認証情報や誤って構成されたセキュリティ設定を悪用し、ラテラルムーブメントの手法を使って従来の防御を回避し、機密情報にアクセスします。

ゼロトラストでは、ユーザー、デバイス、アプリケーション、ネットワークトラフィックの継続的な検証を求めることで、暗黙的な信頼を排除します。すべてのアクセス要求は、リアルタイムのリスク評価に基づいて認証、承認、継続監視されます。この手法により、アタックサーフェスが大幅に削減され、攻撃者がネットワークの一部に侵入した場合でも、不正なアクセスを防止できます。

CISA のゼロトラスト成熟度モデル

CISA のゼロトラスト成熟度モデルは、連邦政府機関がセキュリティフレームワークを徐々に強化するためのロードマップを提供します（図）。このモデルは、次の 5 つの主な柱で構成されています：

- **アイデンティティ：**強力な認証、認可、およびアクセス制御を適用して、正規ユーザーのみが機密リソースを操作できるようにします
- **デバイス:**エンドポイントデバイスを監視、保護、検証して、政府機関のネットワークにアクセスする前にセキュリティポリシーに準拠していることを確認します
- **ネットワーク：**マイクロセグメンテーションと高度なアクセス制御ポリシーを実装して、不正なラテラルムーブメントを防止します
- **アプリケーションとワークロード：**厳格なアイデンティティベースのアクセスポリシー、ランタイムセキュリティ、および API セキュリティ制御により、アプリケーションとワークロードを保護します
- **データ：**機密性の高い政府データを暗号化し、監視し、不正なアクセスや窃取から保護します

CISA のゼロトラスト成熟度モデルの柱（出典：CISA）

これらの柱に加えて、このモデルには、ゼロトラストのすべての構成要素にわたって適用される 3 つの重要な横断的機能が統合されています。

- **可視性と分析：**継続的に監視、ロギング、異常検知を行って、脅威をリアルタイムで特定して緩和します
- **自動化とオーケストレーション：**AI 主導のセキュリティ自動化により、ポリシーを適用し、脅威に対応し、アクセス制御を合理化します
- **ガバナンス：**一元的なポリシー適用により、Federal Information Security Modernization Act（連邦情報セキュリティ近代化法、FISMA）や National Institute of Standards and Technology（米国国立標準技術研究所、NIST）の Special Publication 800-207 など、連邦指令へのコンプライアンスを維持します

マイクロセグメンテーションと API セキュリティの重要性

従来のネットワーク・セキュリティ・モデルでは、ネットワークは通常、ネットワークベースのファイアウォールを使用して広範なセグメントに分割されていました。このアプローチは一定レベルのセキュリティを提供しますが、現代の分散環境を完全に保護するために必要な細分性が欠けています。連邦政府の環境では、ネットワークベースのセグメンテーションは通常、オーバープロビジョニングにつながります。つまり、ユーザーやアプリケーションは、実際に必要な量よりも多くのリソースにアクセスできるようになります。これにより、意図せずラテラルムーブメントの機会が生じてしまいます。攻撃者はネットワークの一部を侵害すると、ほとんど抵抗を受けずに、更に機密性の高い領域に進出できます。

マイクロセグメンテーションの概念は、ネットワーク内の水平方向（East ／ West）のトラフィックをきめ細かく制御することで、この課題に対処します。マイクロセグメント化された環境では、各アプリケーション、ワークロード、サービスは他から分離され、アクセスは特定のポリシーに基づいて制限されます。これにより、ユーザー、デバイス、およびアプリケーションは、アクセスが明示的に許可されているリソースとのみ通信できるようになります。マイクロセグメンテーションは、アイデンティティベースのアプリケーション対応セグメンテーションを実装することで、サイバー攻撃による潜在的な損害を制限し、アタックサーフェスを縮小し、ゼロトラストの原則を適用します。

垂直方向（North ／ South）のネットワークトラフィックに関しては、連邦ネットワークでは、システム間の通信を容易にするために API を利用することが増えてきています。その結果、API エンドポイントの保護が最優先事項になります。近年、API 攻撃（インジェクション攻撃、クレデンシャルスタッフィング、不正なデータアクセスなど）が激増しています。連邦政府機関は、セキュリティ担当者が API トラフィックをリアルタイムで探索、監視、保護できるように、API のライフサイクル全体を保護する包括的な API セキュリティソリューションを必要としています。API の探索は特に重要です。誰も把握していない API が存在することは珍しくありません。

Akamai ゼロトラスト・ソリューションの概要

アイデンティティ

Akamai MFA は、フィッシングや中間者攻撃などから従業員アカウントを保護する、キーレス FIDO2 アイデンティティソリューションです。強力なアイデンティティベースの認証を受け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るようになります。その他のアクセスは拒否され、従業員アカウントの乗っ取りが阻止されます。

デバイス

Akamai Guardicore Segmentation は、ランサムウェアやその他のマルウェアの水平方向へ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です。Akamai Guardicore Segmentation は、継続的にデバイスを監視しポリシーを適用することで、デバイスの設定、ソフトウェアのインストール、および潜在的な脆弱性を検証し、準拠したデバイスのみがネットワークにアクセスできるようにします。さらに、このソリューションでは、IoT デバイスのセキュリティを確保するために、エージェントレスなアプローチをサポートしています。

Akamai Enterprise Application Access は、認証されたユーザーとデバイスのみがアプリケーションにアクセスできるようにする、包括的なゼロトラスト・ネットワーク・アクセス・ソリューションです。Enterprise Application Access は、デバイスのアイデンティティとポスチャを検証することで、Akamai Guardicore Segmentation の機能を補完します。デバイスが非準拠であることが判明した場合や、セキュリティリスクがある場合、Enterprise Application Access によって機密性の高いアプリケーションへのアクセスを制限できます。

ネットワーク

Akamai API Security は、垂直方向のトラフィックの継続的な探索とリアルタイム分析を通じて、連邦のセキュリティ専門家に API 資産全体の包括的な可視性を提供します。このソリューションは、未知の API を検知し、脆弱性を特定し、API のふるまいを分析します。これによりセキュリティチームは、急速に拡大するこのアタックサーフェスで、攻撃を検知し、リスクを修復できるようになります。

Akamai App & API Protector は、Web アプリケーションファイアウォール、ボット緩和、API セキュリティ、レイヤー 7 分散型サービス妨害（DDoS）防御を 1 つのソリューションに統合します。これは、脆弱性を迅速に特定し、ネットワーク全体および API 資産全体で脅威を緩和します。

Akamai Secure Internet Access Enterprise は、他のセキュリティソリューションに伴う複雑さや管理のオーバーヘッドをなくし、ユーザーやデバイスがどこからでも安全にインターネット接続できるようにする、クラウドベースのセキュアなドメイン・ネーム・サービス（DNS）です。

Akamai Guardicore Segmentation は、ネットワークトラフィックをきめ細かく制御し、正当なトラフィックのみが許可されるようにします。

Akamai ゼロトラスト・ソリューションの概要

アプリケーションとワークロード

Akamai Enterprise Application Access は、場所に関係なく、従業員、サードパーティの請負業者、パートナー、モバイルユーザーにゼロトラスト・アクセスを提供します。

Akamai Guardicore Segmentation は、アプリケーションとワークロードの可視性と理解を提供します。

データ

Akamai Secure Internet Access Enterprise は、コンテンツフィルタリング、高度な脅威防御、データ損失防止などの機能により、データへの安全なアクセスを提供します。不正アクセスやデータ漏洩を防止することで、データインベントリ管理をサポートします。

Akamai Guardicore Segmentation：水平方向の保護の鍵

Akamai Guardicore Segmentation は、組織、特に連邦政府機関がオンプレミス環境とクラウド環境全体にきめ細かなセキュリティ制御を実装できるようにするために設計された、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です

ワークロードとアプリケーションの細分化されたセグメンテーション

ネットワークレベルでアクセスを制御する従来のセグメンテーションとは異なり、Akamai Guardicore Segmentation はアプリケーションレベルとワークロードレベルでセキュリティポリシーを適用します。これにより、アクセスが厳密に制限されます。たとえば、連邦政府機関では、人事（HR）アプリケーションが、指定された HR データベースとのみ通信するように制限できるため、侵害が発生した場合に攻撃者が横方向に移動するのを防ぐことができます。

アイデンティティベースのマイクロセグメンテーション

Akamai Guardicore Segmentation は、IP アドレスだけでなく、ユーザーとデバイスのアイデンティティに基づいてセグメンテーションを実施します。これにより、役職、信頼レベル、およびリアルタイム検証に基づいてアクセスが動的に許可されるようになります。たとえば、請負業者やサードパーティのパートナーを、必要なシステムのみに制限することで、不正アクセスのリスクを軽減できます。

動的なポリシー適用

Akamai Guardicore Segmentation は、ユーザーの行動、デバイスの健全性、ネットワークアクティビティなどのリアルタイムの要因に基づいて、セキュリティポリシーを継続的に調整します。異常な量のデータ転送など、疑わしいアクティビティが検知された場合、Akamai Guardicore Segmentation は自動的にアクセスを制限し、トラフィックをブロックし、セキュリティチームにアラートを送信します。このプロアクティブなアプローチにより、セキュリティポリシーが進化し、新たに出現する脅威に対抗できるようになります。

Akamai Guardicore Segmentation のマイクロセグメンテーションを統合することで、ゼロトラスト・アーキテクチャを強化し、リスクを最小限に抑え、ネットワーク上で厳格なアクセス制御を維持できます。

ケーススタディ

連邦政府の環境における Akamai Guardicore Segmentation

ある連邦政府機関は最近、ラテラルムーブメント攻撃から内部システムを保護するために、Akamai のマイクロセグメンテーションソリューションを導入しました。Akamai Guardicore セグメンテーションを採用する前は、従来のネットワークベースのセグメンテーションを使用していましたが、これは細分性が限定的であり、さまざまなネットワークセグメントで広範なアクセスを可能にしていました。そのため、ネットワークの一部が侵害された場合に、ラテラルムーブメントの危険性が大きくなっていました。

Akamai Guardicore Segmentation を使用することにより、以下を行うことができるようになりました。

- 細分化されたセグメンテーションの実装：アプリケーションレベルでワークロードをセグメント化することで、ラテラルムーブメントのリスクを軽減し、各アプリケーションが必要なリソースとのみ通信できるようにしました。
- 可視性の向上：このソリューションの可視化ツールにより、内部トラフィックを詳細に把握でき、セキュリティチームは潜在的な脅威をリアルタイムで特定して緩和できるようになりました。
- セキュリティの強化：Akamai Guardicore セグメンテーションを既存のアイデンティティ管理システムおよびアクセス制御システムと統合することで、ネットワーク全体でゼロトラストを適用し、継続的にアクセスを監視し、リアルタイムのリスク評価に基づいて動的に調整することができるようになりました。

この例は、Akamai Guardicore セグメンテーションの機能によって、ネットワークセキュリティが向上し、ラテラルムーブメントのリスクが軽減し、常に必要最小限の権限が維持されることを示しています。

API セキュリティ：垂直方向のトラフィックの保護

Akamai は、API セキュリティを確保するためのソリューションをいくつか提供しています Akamai の API セキュリティプラットフォームは、API インタラクションを包括的に可視化し、垂直方向の脅威をリアルタイムで自動的に検知して緩和します。高度なふるまい分析により、連邦政府機関は次のことを実現できます：

- **シャドウ API の特定**。シャドウ API は攻撃者に悪用される可能性があります
- **API トラフィックパターンの監視**。不正なアクセス試行を検知します
- **API レート制限の実装**。不正利用やサービス拒否攻撃を防止します
- **忘れられた API、放置された API、未知の API の特定**。潜在的な攻撃経路を明らかにします
- **すべての API のインベントリを作成**。構成やタイプ（RESTful、GraphQL、SOAP、XML-RPC、JSON-RPC、gRPC など）に関係なく作成します

Akamai Secure Internet Access Enterprise は、セキュリティチームがネットワーク内外の両方において、すべてのユーザーやデバイスがインターネットに安全に接続できるようにするために設計された、クラウドベースの DNS ファイアウォールです。マルウェア、ランサムウェア、フィッシング、低スループットの DNS データ窃取などの悪性の DNS リクエストをプロアクティブにブロックします。Secure Internet Access Enterprise は、アプライアンスを導入、管理、アップグレードする必要がないため、セキュリティの複雑さを軽減します。このソリューションはシンプルで直感的に使用できます。

Akamai App & API Protector では、Akamai Cloud を介して実行されるアプリや API に対する API 脅威を探索して緩和できます。また、Akamai API Security が突き止めた潜在的な脅威が含まれるトラフィックをすべて阻止できます。Akamai の API 保護ソリューションを組み合わせて展開することで、API を包括的かつ継続的に可視化でき、セキュリティ担当者はアプリケーション資産全体において API セキュリティの問題を探索、監査、検知、対応できます。

ゼロトラストによる横断的機能の実現

ゼロトラスト・アーキテクチャの主な課題の 1 つは、テクノロジーのサイロ化リスクです。各サイロは独立して動作することが多く、セキュリティ制御、ポリシーの適用、脅威検知の断片化につながります。したがって、すべてのセキュリティレイヤーにわたる統合が最も重要であると考えられます。

機密性の高いデータや複雑なインフラを管理する連邦政府機関にとって、このような断片化されたアプローチは、重大なセキュリティリスクをもたらす可能性があります。攻撃者は、サイロ（柱）間の可視性の欠如を悪用したり、異なるシステム間で一貫性のないポリシー適用を利用したりする場合があります。これらのリスクを緩和するために、連邦政府組織は、すべての柱に可視性、ガバナンス、自動化を統合した、統一された柱横断のセキュリティモデルを採用して、一貫したポリシー適用を確保し、攻撃者が悪用できるギャップを減らす必要があります。

統一されたセキュリティモデルを実現するためには、柱横断の統合で、CISA のゼロトラスト成熟度モデルにおける、3 つの横断領域に重点を置く必要があります。それは、可視性と分析、自動化とオーケストレーション、ガバナンスです。これらの要素は、リアルタイムのリスク評価に基づいて、すべての柱でアクセスと権限が動的に調整されるゼロトラスト・アーキテクチャを実現するためには不可欠です。

可視性と分析

可視性は、脅威を検知し、ユーザーのふるまいを理解し、すべての柱に動的なセキュリティポリシーを適用する上で重要です。アイデンティティ、デバイス、アプリケーション、データの相互作用を完全に把握できないと、セキュリティチームは状況を把握できず、異常なふるまいや不正なアクセス試行を検知することが困難になります。Akamai のソリューションは、包括的な柱横断の可視性を提供します。

- Akamai Guardicore Segmentation は、セグメント化されたワークロード間のネットワークトラフィックを監視し、水平方向のトラフィックを可視化し、ネットワーク内でのラテラルムーブメントの試行を検知します。
- Enterprise Application Access では、アプリケーションのアクセスパターンを把握し、機密性の高いアプリケーションとのやり取りを追跡し、コンテキストデータに基づいてアクセスを動的に調整できます。

これらの機能を統合することで、連邦政府機関はすべての柱にわたってデータを関連付け、セキュリティイベントを統一的に把握できるようになります。ユーザーがアプリケーションへのアクセスを要求すると、Akamai のソリューションは、ユーザーのアイデンティティだけでなく、デバイスのセキュリティ、使用しているネットワーク、アプリケーションのリアルタイムの動作もチェックできます。これにより、セキュリティチームは潜在的な脅威を迅速に検知し、権限昇格のリスクを最小限に抑え、リアルタイムのリスク評価に応じて権限を動的に調整できます。

自動化とオーケストレーション

インシデントへの対応や、複数のシステムにわたるポリシーの適用は、時間のかかる手作業のプロセスになる場合があります。ゼロトラストでは、セキュリティポリシーをすべての柱に動的に適用する必要があり、高度な自動化とオーケストレーションが求められます。これにより、リスクレベルの変更に応じて、権限が必要最小限のレベルに直ちに調整され、人的ミスや応答遅延の可能性が低減されます。Akamai のソリューションは、アイデンティティ、ネットワーク、アプリケーションのセキュリティにまたがる、自動化されたワークフローを提供します。

- Akamai Guardicore Segmentation は、自動マイクロセグメンテーションを提供し、リアルタイムのトラフィックパターンと検知された異常に基づいてネットワーク・セグメンテーション・ポリシーを動的に調整します。これにより、ネットワーク内の疑わしいアクティビティを迅速に分離し、ラテラルムーブメントを防止できます。

- Enterprise Application Access は、アプリケーションアクセスのセキュリティを確保するプロセスを自動化します。これにより、ユーザーはセキュアなプロキシを介してのみアプリケーションにアクセスでき、変化するリスク要因に基づいて権限が継続的に更新されます。

これらのプロセスを自動化することで、連邦政府機関はセキュリティポリシーを一貫して迅速に適用でき、攻撃者にとっての攻撃のチャンスを削減できます。

ガバナンス

ガバナンスはあらゆるセキュリティ戦略の基盤であり、ポリシーが一貫して適用され、コンプライアンス要件が満たされていることを保証します。柱横断モデルでは、ガバナンスは、すべてのセキュリティ制御がゼロトラストの原則に合致していることを保証する必要があります。Akamai のソリューションを使用することで、すべての柱を網羅するガバナンスポリシーを実装できます。

- アイデンティティガバナンス：アイデンティティベースのアクセス制御が、デバイス、アプリケーション、およびネットワーク全体で一貫して適用され、アクセス許可がリアルタイムのリスク評価に基づいて定期的に確認および更新されるようにします
- ネットワークガバナンス：オンプレミス、クラウド、ハイブリッドインフラを含む環境全体でネットワークセグメンテーションとトラフィック監視ポリシーを適用します。Akamai Guardicore Segmentation により、ネットワーク・セグメンテーション・ポリシーを定義し、インフラ全体に一貫して適用できます
- データガバナンス：アクセスが最小権限に基づいて制限され、すべてのデータ転送で不正アクセスや疑わしいアクティビティが継続的に監視されるようにすることで、機微な情報を保護します

Akamai のテクノロジーは、シームレスに連携するように設計されており、ゼロトラストをサポートする完全統合された柱横断のセキュリティアーキテクチャを連邦政府機関に提供します。

ケーススタディ

連邦政府機関における柱横断の統合

大規模な連邦政府機関は、アイデンティティ、ネットワーク、およびアプリケーション層全体にわたってセキュリティポリシーが断片化され、大きな課題に直面していました。異なるシステムがアイデンティティ検証、アプリケーションアクセス、ネットワークセグメンテーションを管理しているため、セキュリティポリシーの適用に一貫性がなく、可視性にギャップが生じていました。

Akamai の統合ソリューションを採用することで、次のことが可能になりました。

- **アイデンティティとアプリケーションセキュリティを統一：**Akamai のアイデンティティ、認証情報、およびアクセス管理（ICAM）ソリューションである Enterprise Application Access が統合され、アプリケーションアクセスが常にリアルタイムのアイデンティティデータに基づいて認証されるようになりました。これにより、ユーザーのふるまいとデバイスの健全性に基づいてアプリケーションの権限を動的に調整できるようになりました。
- **動的なネットワークセグメンテーションの適用：**Akamai Guardicore Segmentation が導入されたことにより、アイデンティティとアプリケーションアクセスに基づいてネットワークトラフィックをセグメント化し、機密性の高いシステム間のラテラルムーブメントを防止し、リアルタイムのリスク評価に基づいて権限が継続的に更新されるようになりました。
- **可視性と自動化の向上：**Akamai の統合された分析と自動化のツールを使用して、セキュリティポスチャを完全に可視化し、すべての柱にわたってポリシーの適用を自動化しました。

その結果、アタックサーフェスが縮小し、インシデント対応時間が短縮され、連邦のセキュリティ規制に完全に準拠するようになりました。この事例は、断片化されたセキュリティアーキテクチャを、ゼロトラストをサポートする一貫性のある動的なセキュリティモデルに変換する、柱横断の統合の力を示しています。

結論

ゼロトラスト・セキュリティはもはや任意のセキュリティではありません。高度なサイバー脅威から連邦政府機関を保護するためには不可欠です。マイクロセグメンテーション、API セキュリティ、強力なアイデンティティ制御を実装することで、連邦政府機関は、連邦政府のサイバーセキュリティ要件へのコンプライアンスを維持しながら、リスクを大幅に削減できます。

Akamai は、Akamai Guardicore Segmentation、Akamai API Security、Akamai Secure Internet Access Enterprise など、ゼロトラスト・ソリューションの包括的なスイートを提供しており、プロアクティブな適応型セキュリティポスチャの実現を支援します。Akamai の専門知識を活用することで、連邦政府機関はゼロトラストへの取り組みを加速し、セキュリティの長期的な回復力を確保できます。

今こそ連邦政府機関が行動を起こす時です。Akamai のセキュリティソリューションを統合することで、ゼロトラスト成熟度を達成し、サイバーリスクを緩和し、国家の最も重要なデジタル資産を保護できます。

今すぐ Akamai にお問い合わせいただき、包括的なセキュリティソリューションの詳細をご確認ください。