Akamai

ホワイトペーパー

ワールドクラスのセキュリティポスチャへのロードマップ

ゼロトラストを中心にカスタマイズされた変革プランをご覧ください

進化し続けるセキュリティ環境、私たち Akamai がセキュリティを確保し続け、また現状に安住しないよう、先頃、Zero Trust Maturity Model（ゼロトラスト成熟度モデル、ZTMM）を使用したセキュリティパフォーマンスの可視化を実現しました。ここでは、皆様の組織が同様の作業を行うことで、改善すべき重要な領域を明らかにし、ワールドクラスのセキュリティポスチャを実現するための明確なロードマップを作成する方法をご紹介します。

ゼロトラストへの道のりをシンプル化

エンタープライズアクセスとセキュリティは複雑で、常に変化しています。そのような状況においては、ゼロトラストのセキュリティポスチャに移行する際に、どこに注力すべきかを特定するのが難しい場合があります。

当社が、現在のセキュリティポスチャを評価し、可視化するためのツールとして ZTMM を使用することをお勧めするのはそのためです。当社はこれまで、このツールを使用して、Akamai での自社のセキュリティポスチャを評価するとともに、複数のお客様のセキュリティポスチャも評価してきました。この過程を完了すると、ゼロトラストアーキテクチャに近づくための実践的なアクションのロードマップが手に入ることと思います。（ゼロトラストの概念の詳細については、付録 A を参照してください。）

ZTMM が重要な理由

当社では、さらに強固なセキュリティポスチャを導入する過程において最も重要なステップは、「始めること」だと考えています。しかし、サイバーセキュリティの複雑で絶え間なく変化するトピックに関して言えば、「始めること」は言葉で言うほど簡単なことではありません。当社は、多くの組織が、ゼロトラストを実現するために何を実施するべきか、どの程度実施するべきか、変更の順序はどうするべきかを判断する際に苦労していることを知っています。

そこで威力を発揮するのが ZTMM です。ZTMM はゼロトラストを中心としたフレームワークを作り、直線的で一貫した感覚を提供し、実施を容易にします。組織による、変更計画や更新予算の策定を支援します。また、IT スペシャリストではない意思決定者にゼロトラストの概念を説明し、IT チームが必要とする合意形成を支援します。

ZTMM は試行錯誤の上に完成したものです。米国サイバーセキュリティ・社会基盤安全保障庁（CISA）によって開発され、米国の各連邦政府機関で広く利用されています。

ゼロトラスト成熟度モデルの 5 本の柱と 3 つの機能

ZTMM は、5 本の柱に関わる実装の進捗状況を示すものであり、時間の経過とともに発展していきます。5 本の柱とは、考慮すべきアイデンティティ、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、そしてデータのことです（図 1）。また ZTMM では、5 本の柱のすべてに共通する 3 つの機能についても考慮する必要があります。

- 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

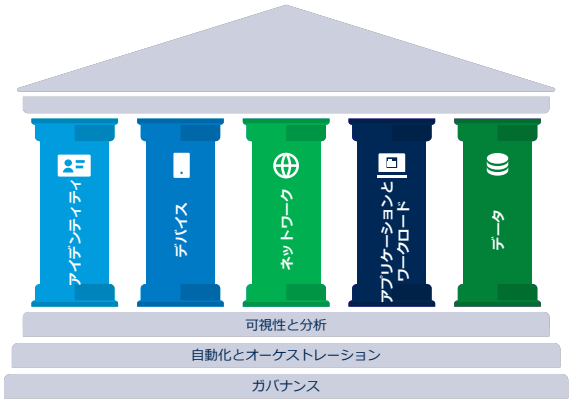


図 *1*：*CISA* の *ZTMM* は、ゼロトラストへの移行をサポートするパスの *1* つです（出典：*CISA*）

この対象分野それぞれに、組織がゼロトラストアプローチの達成にどれだけ近づいているかを示す成熟度が割り当てられます。4 つの成熟度ステージ（従来型、初期、高度、最適）は、手動設定と VPN から理想的な「境界のないセキュリティ」セットアップまでの段階を表しています（図 2）。成熟度の最終段階である「最適」では、組織はアプリケーションに最小限の権限を付与し、脆弱なデバイスへの認証とアクセスを拒否し、内部の脅威の拡散を防止し、セキュリティインシデントを即座に検知して対応します。（ZTMM フレームワークの詳細については、付録 B を参照してください。）

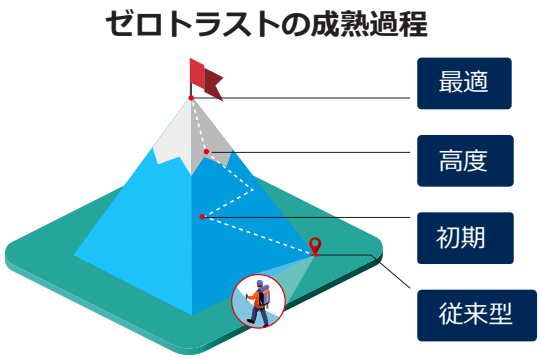


図 *2*：ゼロトラストの成熟過程（出典：*CISA*）

ZTMM は、成熟度が低い領域を明らかにすることで、組織がよりバランスの取れたセキュリティ環境を構築するのに役立ちます。Akamai の業界をリードするセキュリティ・ソリューション・スイートと専門知識を組み合わせることにより、成熟したセキュリティポスチャへの移行がこれまで以上に簡単に行えるようになりました。

お客様の社内チームはゼロトラストの実現に苦労していますか？それは他の企業も同じです。

ゼロトラストアーキテクチャを構築する責任は、1 つの部署が負うべきものではありません。組織のあらゆるレベルのさまざまな関係者の同意、柔軟な対応、承認を必要とします。

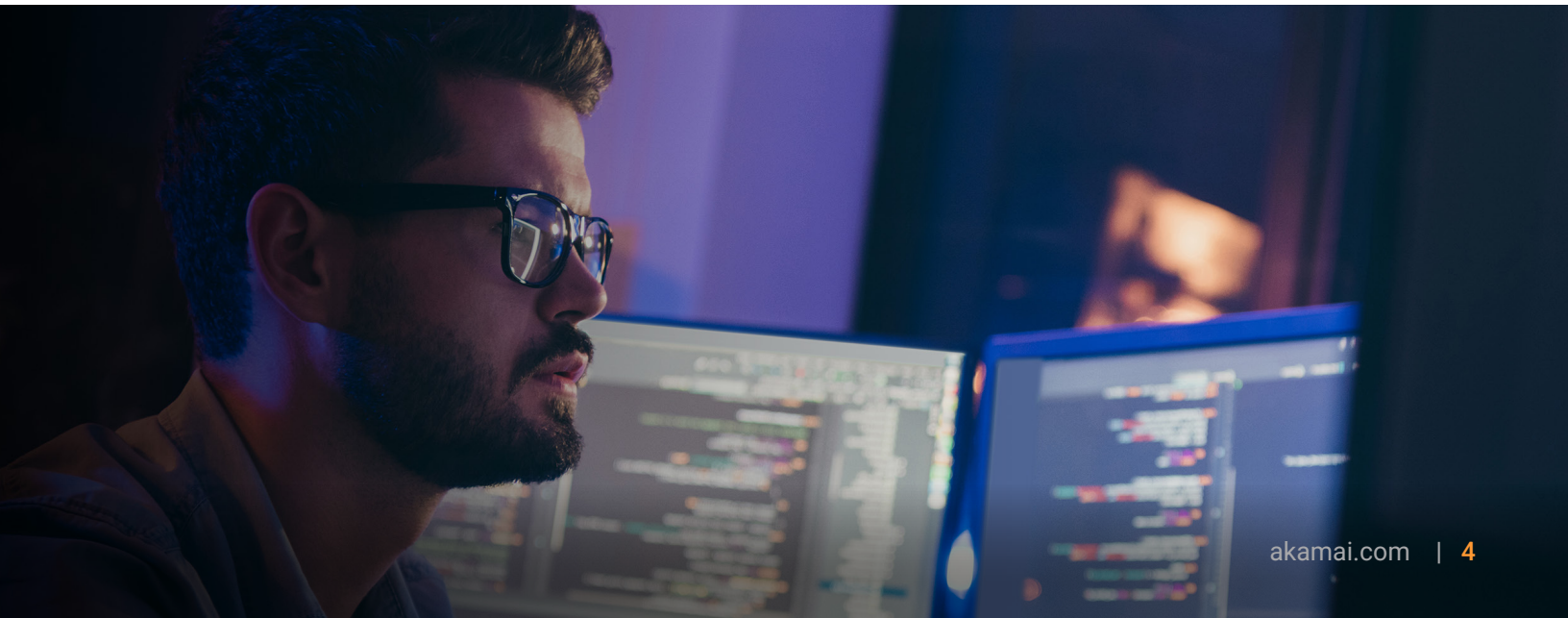
Akamai はオンラインビジネスの力となり、守るサイバーセキュリティおよびクラウドコンピューティング企業です。当社の市場トップクラスのセキュリティソリューション、優れた脅威インテリジェンス、グローバル運用チームが、世界中のあらゆるタッチポイントで重要なデータとアプリケーションを保護しています。このように全体を見渡せるということは、当社が、ゼロトラスト・セキュリティポスチャへの移行において最も一般的な課題を理解しており、ソリューションの発見をお手伝いできることを意味します。

ゼロトラストに関する 3 つの一般的な課題

1. **どこから始めるべきかを理解する。**通常は、ワークロードの可視化から始めて、サイバー回復力を高めるためにアタックサーフェスを減らすことをお勧めしていますが、これはその組織の現在のセキュリティポスチャによって異なります。

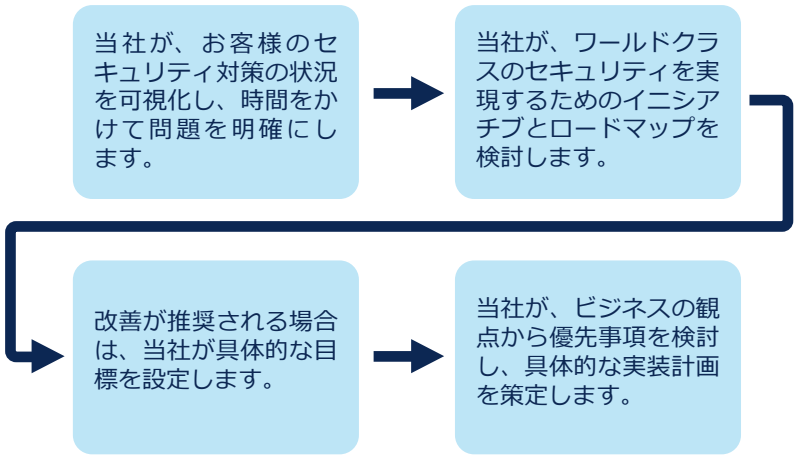
2. **迅速に成功を達成する。**ゼロトラストの達成は、チームが 1 つのことに集中したり、目標に向けた小さなステップを実行したりすることが困難な、非常に大きな取り組みのように思えることがあります。

3. **ROI を実証する。**ゼロトラストプロジェクトは安価ではありません。そして通常、組織内での文化的変化や技術的変化が必要になります。投資利益率を（アタックサーフェスの削減、侵害の緩和、脆弱性に対するセキュリティの確保、金銭的利益などにより）実証する能力は、特に意思決定者やセキュリティリーダーにとって極めて重要です。



ゼロトラストへの行程を開始し、セキュリティポスチャを可視化する準備はできていますか？

当社が行ったように、お客様も ZTMM を使用して、現在のセキュリティ対策の成熟度ステータスを可視化できます。これにより、自社のプロセスと、ゼロトラストアーキテクチャを実現するために変更すべきこととのバランスを向上させる方法が明確になります。



Akamai がお客様をゼロトラスト・セキュリティポスチャに導く方法

ゼロトラストアーキテクチャが実現すると、さまざまな制御と原則を用いて、セキュリティの課題に対処することができます。

当社は、イニシアチブとロードマップを検討して、お客様がワールドクラスのセキュリティを実現するために、事業全体と各目標を考慮した実装計画を作成する支援をします。このようなアプローチにより、当社はお客様と協力して、長期的で効果的かつ持続可能なセキュリティシステムとプロセスを構築することができます。

Akamai Cloud に加えて、高度な分散型 ZTNA ソリューションや、業界をリードするマイクロセグメンテーション、フィッシング対抗型多要素認証（MFA）、プロアクティブ DNS ファイアウォールなど当社のセキュリティ製品スイートが、お客様のセキュリティポスチャを、ゼロトラスト成熟度の最終段階である「最適」へと導きます。さらに、1 台のコンソールから、単一のエージェントだけで、システム全体を運用することができます（図 3）。

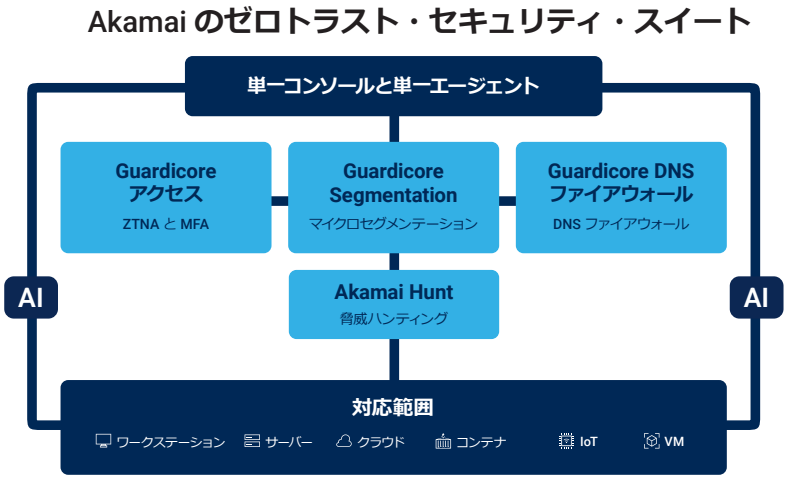


図 *3*：*Akamai* のセキュリティ製品スイートは、*1* 台のコンソールから、単一のエージェントによって実行できます

ケーススタディ

ゼロトラスト成熟度モデルを使用した、多国籍小売企業の e コマースのセキュリティポスチャの可視化

最近当社は、ある多国籍小売企業の e コマースのセキュリティポスチャを分析し、それをワールドクラスのセキュリティポスチャに近づけるために、そのセキュリティステータスを可視化し、そのセキュリティ状況を可視化し、ワールドクラスのセキュリティポスチャに近づくための対応するロードマップを策定し提供しました。当社の専門家チームは、ZTMM 全体で改善すべき領域を特定し、重要性の高いものから低いものへとランク付けを行いました。ここでその結果をお伝えします。

実装にばらつきがある、バランスがとれていないシステム

それぞれの柱において、モバイルデバイス管理やアプリケーション展開の自動化など、一部の機能は最高レベル（「最適」）の成熟度で実装されていることがわかりました。しかし、それぞれの柱の一部の機能は「従来型」レベルにとどまっており、深刻なリスクをもたらしていました。

特に、アイデンティティとネットワークという 2 本の柱の重要機能が強化されていませんでした。この 2 本の柱はゼロトラストアーキテクチャの基盤です。そのような機能には、MFA、アイデンティティインフラストラクチャの統合管理、コンテキストベースのアクセス制御、マイクロセグメンテーションなどが含まれます。

リスクの高い ID インフラストラクチャ

当社のアナリストは、ID とパスワードによる認証がその小売企業の標準であることを確認しました。MFA の使用は少数のシステムに限られていました。そのため、認証情報が悪用されるリスクが高くなっていました。さらに、Microsoft Entra ID、オンプレミスの Active Directory（AD）、Lightweight Directory Access Protocol（LDAP）などの複数の ID インフラストラクチャが存在していました。その小売企業の管理が統合されていないため、LDAP などのセキュリティ対策が不十分な ID インフラから侵害が発生するリスクがありました。

統合されていない認可管理

認可管理が統合されていないため、各アプリケーションは個別に処理されていました。脆弱なデバイスからのアクセスや疑わしいアクセスをブロックすることはできませんでした。その小売企業のネットワークにアクセスする従業員またはパートナーの PC がマルウェアに感染した場合、ラテラルムーブメント（横方向の移動）によってシステムやリソースへの不正アクセスが行われるリスクが高まっていました。

不十分なセグメンテーション

小売企業のセキュリティ対策は外部からの脅威に重点を置いたものであり、すでにネットワークに侵入した攻撃者がもたらすリスクが見過ごされていることが判明しました。堅牢な内部セグメンテーションがなければ、倉庫の Wi-Fi ネットワークや VPN の脆弱性を突いた侵入によって、ラテラルムーブメントが野放しになる可能性があります。このような内部障壁の欠如により、広範なシステム侵害、データ漏洩、運用停止のリスクが大幅に高まっていました。拡散防止の手段が用意されていないネットワークでは、攻撃が何の抵抗も受けず広がっていく可能性があるからです。

不十分な脆弱性管理と対応

この小売企業には、ソフトウェア部品表（SBOM）を脆弱性情報にリンクする管理システムがありませんでした。つまり、アプリケーションの脆弱性を迅速に特定して対応することができず、リスクが高まっていました。

当社の推奨事項

私たちはこの小売企業に、セキュリティポスチャを強化するために、次の 5 つのステップを実行することを、推奨しました。

1. 現行の設定における不正侵入やラテラルムーブメントのリスクを低減するため、予防的な対策を講じる
2. アイデンティティインフラストラクチャと既存の技術スタックの統合を継続する
3. ゼロトラスト・ネットワーク・アクセスと連動させて認証および認可機能を拡張する計画を立てる
4. きめ細かなワークロードおよびアプリケーション保護を実装する最も効果的な方法を決定する
5. 未知の将来の脅威に対する対応システムとプロセスを構築し、脆弱性管理と対応を強化するシステムとプロセスを開発し、計画を策定する

ゼロトラストに関心をお持ちでしたら、当社にお問い合わせください。無料のセキュリティ評価をご案内します。

付録 A：ゼロトラストという概念について

ゼロトラストとは、ユーザー、デバイス、システムを、それが組織のネットワーク境界の内側にあるものであれ、外側にあるものであれ、一切信頼するべきではないという考え方に基づいた、セキュリティ概念です。

信頼しない代わりに、リスクを最小限に抑えるために検証プロセスと監視を使用します。これには、厳格なアイデンティティおよびアクセス管理（IAM）ポリシーの適用、多要素認証（MFA）の使用、役割ベースのアクセス制御（RBAC）の優先順位付けなどのアプローチが含まれます。

ゼロトラストの概念は約 15 年前から存在していましたが、組織がリモートアクセス要件の増加に直面した COVID-19 パンデミック時に重要視されるようになりました。多くの企業は、ユーザーとデバイスが集中管理ではなく分散管理されている場合、既存のセキュリティ対策が有効に機能しないことに気づきました。

今日、ゼロトラストアーキテクチャ、ゼロトラスト・ネットワーク・アクセス（ZTNA）、ゼロトラストセキュア Web ゲートウェイ（SWG）、マイクロセグメンテーションなど、ゼロトラスト原則に基づく実装が数多く行われています。

ゼロトラストの詳細についてはこちらをお読みください

付録 B：ZTMM 2.0 フレームワーク

5 本の柱

それぞれの柱は、独自のペースで進めることができ、柱相互の調整が必要になるまで、他の柱よりも早く進行させてもかまいません。

柱	説明
アイデンティティ	エージェンシーユーザーまたは（非人格エンティティを含む）エンティティを一意に記述する属性または属性セット
デバイス	サーバー、デスクトップおよびノートパソコン、プリンター、携帯電話、モノのインターネット（IoT）デバイス、ネットワーキング機器など、ネットワークに接続できるあらゆる資産
ネットワーク	エージェンシー内部ネットワーク、ワイヤレスネットワーク、インターネットなどの一般的なチャネル、およびメッセージの転送に使用されるその他の潜在的なチャネルを含む、オープン通信メディア
アプリケーションとワークロード	オンプレミス、モバイルデバイス、クラウド環境で実行されるエージェンシーシステム、コンピュータープログラム、サービス
データ	システム、デバイス、ネットワーク、アプリケーション、データベース、インフラ、バックアップに存在している構造化ファイル、非構造化ファイル、フラグメント、および関連メタデータ

柱間機能

この 3 つの機能はゼロトラストフレームワーク全体をサポートし、セキュリティ対策を統合し、応答性を高め、一貫性あるものにします。

機能	説明
可視性と分析	組織は、すべてのユーザーアクティビティ、デバイスの状態、およびネットワークインタラクションを、明確かつリアルタイムに把握する必要があります。脅威が検知され、迅速に対処されることで、リスクが軽減されます。組織は、情報に基づいた予防的なセキュリティ意思決定を行います。
自動化とオーケストレーション	人的ミスは、セキュリティ課題によく見られる原因です。自動化とオーケストレーションが最適化されると、人的ミスの可能性が最小限に抑えられます。自動化によって日常的なタスクがシンプル化され、オーケストレーションによってさまざまなシステム間でセキュリティ活動が整理されます。その結果、脅威への対応をより迅速化し、かつ統合するための適切な条件が生まれます。
ガバナンス	優れたセキュリティガバナンスにより説明責任が生まれ、誰もが同じセキュリティ慣行と規制に従うようになります。その結果、安全な運用のための強力な基盤が構築されます。また、ゼロトラストの明確なガイドラインが設定され、組織はコンプライアンス基準を満たすことが可能になります。

ゼロトラスト成熟度モデルにおける成熟度

ZTMM 2.0 は、各機能の成熟度レベルを 4 段階で定義します。その目標は、5 本柱と 3 つの機能の現在の成熟度レベルを判定し、それぞれを最高成熟度レベルに移行する計画を作成することです。

成熟度レベル	説明
従来型	主導による設定、応答、および緩和。静的でサイロ化されたポリシーとソリューション
初期	自動化の開始、初期の柱間ソリューション。最小限の権限に対する柔軟な変更、内部システムの集約された可視性
高度	自動制御（該当する場合）、柱間ポリシーの適用、リスク／ポスチャに基づく最小権限の変更、事前定義された緩和策への対応
最適	自動制御（該当する場合）、柱間ポリシーの適用、リスク／ポスチャに基づく最小権限の変更、事前定義された緩和策への対応