TLP：CLEAR

ゼロトラストへの道のり

ゼロトラストにおけるマイクロセグメンテーション

第 1 部：序論と計画

バージョン：1.0

公開日: 2025 年 7 月 29 日

サイバーセキュリティ・インフラセキュリティ庁

この文書は *TLP:CLEAR* とマークされている。取得者は、この情報を制限なく共有することができます。情報は、標準的な著作権規則の対象となります。トラフィックライトプロトコルに関する詳細については、*https://www.cisa.gov/tlp* 。をご覧ください

改訂履歴

バージョン	改訂の概要	
	初回リリース – 全ページ	2025 年 7 月 29 日

序文

「ゼロトラストへの道のり」シリーズは、組織が最新のゼロトラスト (ZT) 原則を採用するためのサイバーセキュリティ機能とアーキテクチャについて取り上げている。決して信頼せず、常に検証するという ZT のコアコンセプトは、これまでのサイバーセキュリティモデルから発展したものである。現在の ZT シリーズは、組織の ZT への移行を支援し、他のリソースを補完するものである。

「ZTA の実装は、インフラストラクチャやプロセスの全面的な置き換えではなく、長い道のりだ。組織は、最も価値の高いデータ資産を保護するゼロトラストの原則、プロセスの変更、およびテクノロジーソリューションを段階的に実装するよう努めるべきである」[1]

マイクロセグメンテーションは、ゾーンまたはセグメントへの接続を制限するネットワーク制御だ。従来、組織は、インターネットプロトコル（IP）アドレス範囲、仮想ローカルエリアネットワーク（VLAN）、および静的ルールに基づいて接続を許可または拒否できるデバイスやサービスを使用して、ネットワーク制御を実現していた。この文脈では、マイクロセグメントは、より細粒度で手動で作成・管理されるアクセスルールを持つ、より小さなゾーンまたはアドレス範囲を指す。このアプローチは、ネットワークデバイス、仮想化ネットワーク、またはファイアウォール、ルーター、スイッチなどの境界防御装置に適用される静的ルールとルーティングを通じて実現されるのが一般的だ。

このドキュメントでは、従来のネットワークマイクロセグメンテーションの原則を、ゼロトラストアーキテクチャ（ZTA）および動的ポリシー実施に関連する課題に適用するための、背景、参考資料、および初期計画に関するガイダンスを提供する。動的ポリシー実施および ZT のコンテキストでは、マイクロセグメンテーションは、ネットワークに関する議論や機能以上のものとなる。これは、現在の最先端のネットワーク機能と制御だけでなく、ホストやワークフロー認識型ポリシー適用メカニズム（一般的にポリシー適用ポイント（PEP）と呼ばれる）に実装された機能も含まれる。[2] これは、ZT のためのマイクロセグメンテーションの目的を達成するために、ホスト、アプリケーション、データベース、オペレーティングシステム、仮想化プラットフォーム、または専用デバイスに適用可能な、進化する機能のセットだ。ZT におけるマイクロセグメンテーションを PEP で適用する場合、アクセスルールのパラメーターは IP アドレスを超えて、接続に関する文脈情報を含むようになる。[3] この追加の文脈情報は、 属性[4] と呼ばれ、初期アクセスと継続アクセス両方の動的ポリシー決定を支援するために、幅広い情報を包含することができる。

---

[1]米国商務省国立標準技術研究所、「ゼロトラストアーキテクチャ - NIST テクニカルシリーズ出版物」、ゼロトラストアーキテクチャ、セクション 7、2020 年 8 月、https://doi.org/10.6028/NIST.SP.800-207。

[2]米国商務省国立標準技術研究所、「ゼロトラストアーキテクチャ - NIST テクニカルシリーズ出版物」、ゼロトラストアーキテクチャ、セクション 7、2020 年 8 月、https://doi.org/10.6028/NIST.SP.800-207。

[3]米国商務省国立標準技術研究所、「Guide to a Secure Enterprise Network Landscape（セキュアなエンタープライズネットワーク環境ガイド）」、コンピュータセキュリティリソースセンター、2022 年 11 月 17 日、https://doi.org/10.6028/NIST.SP.800-215。

[4]米国商務省国立標準技術研究所、「ゼロトラストアーキテクチャ - NIST テクニカルシリーズ出版物」、ゼロトラストアーキテクチャ、セクション 2.1-4、3.3、6.3、2020 年 8 月、https://doi.org/10.6028/NIST.SP.800-207。

目次

1. 序論 6
1.1 エグゼクティブサマリー 6
図 1：ZTMM - ネットワーク 6
1.2 背景 7
図 2：ゼロトラスト成熟度旅路 7
図 3：脅威の影響とセグメンテーション 8
2. セグメンテーションとは何であるか？ 11
2.1 主要な概念 11
図 4：ポリシーによるアクセス制御 13
図 5：TIC の推移 14
図 6：伝統的なネットワークセグメンテーション 14
図 7：マイクロセグメンテーション 15
図 8: ワークフローベースのマイクロセグメンテーション 16
2.2 セグメンテーションの種類 16
表 1：セグメンテーションの種類と機能 16
3. 段階的なアプローチ 19
3.1 フェーズ 1：セグメンテーションの候補リソースの識別 19
3.2 フェーズ 2：選択した候補リソースの依存関係を識別する 19
3.3 フェーズ 3：適切なセグメンテーションポリシーの決定 20
3.4 フェーズ 4：更新されたセグメンテーションポリシーの展開 20
4. 計画上の考慮事項 21
4.1 ユーザーと組織のサポート 21
4.2 セグメンテーションの対象となるリソースの識別 21
4.3 依存リソースの識別 21
4.4 適切なセグメンテーションポリシーの決定 22
4.5 更新されたセグメンテーションポリシーの展開 22
4.6 ユーザーデバイスの取り扱い 22
4.7 OT、IoT、レガシー環境およびデバイスの取り扱い 22
4.8 制御と可視化の集中化 23
4.9 継続的な保守と進化 23
5. マイクロセグメンテーションの例 24
5.1 シナリオ 1：既存のオンプレミスエンタープライズの再構築 24
5.2 シナリオ #2: 環境移行の一部としてのマイクロセグメンテーション 24
5.3 シナリオ 3：分散型エンタープライズのマイクロセグメンテーション 25
6. 結論 26

附属書 A：連邦ガイドライン 27
附属書 B：頭字語 28

1. 序論

1.1 エグゼクティブサマリー

従来の境界重視のアーキテクチャでは、サイバー侵入や侵害からエンタープライズリソースを保護することはもはや困難である。マイクロセグメンテーションは、より小規模なリソースグループを保護することで、攻撃対象領域を縮小し、横方向の移動を制限し、可視性を高めて、マイクロセグメント化された環境の監視を強化する。マイクロセグメンテーションは、さまざまな制御やサイバーセキュリティツールによる多層防御や、データ、資産、構成、脆弱性の適切な管理に代わるものではない。むしろ、マイクロセグメンテーションは、既存の機能と組み合わせて使用することで、リスクや脅威に応じた保護を的を絞って適用する組織の能力を強化する。

システムセキュリティとアーキテクチャにおけるこの文化的および技術的な変化の採用は、組織のリーダーシップに依存する。このゼロトラストへの道のりは、リーダーにマイクロセグメンテーションの概念と段階的な実装アプローチの概要をわかりやすく説明する。このドキュメントには、連邦文民行政機関（FCEB）に関する具体的な参照情報があるが、あらゆる組織が、ここで提供される情報を活用してネットワークを最新化し、ゼロトラストアーキテクチャへの移行を進めることができる。

マイクロセグメンテーションは、情報技術（IT）、運用技術（OT）、産業用制御システム（ICS）、モノのインターネット（IoT）などのあらゆるテクノロジー環境、およびクラウド、オンプレミス、ハイブリッドなどのあらゆる実装モデルに適用できる。マイクロセグメンテーションにより、マイクロセグメント内の特定のシステムやデータに、リスクと脅威に応じた保護機能と可視化機能を適用することができる。マイクロセグメンテーションは、システムやデータのセキュリティを大幅に強化し、侵害されたリソースが影響を与える範囲を縮小するのに役立つ。

ZTAs の一部として実装された場合、マイクロセグメンテーションソリューションは、ネットワークの場所に基づく暗黙の信頼に依存するのではなく、アクセス時に追加の特性を利用して、ターゲットリソースを保護する。PEP は、これらの特性を使用して、初期アクセスを認可し、リソースへの接続が存在する間、継続的なアクセスが必要かつ認可されていることを妥当性確認する。サイバーセキュリティ・インフラセキュリティ庁（CISA）は、ネットワークの柱におけるゼロトラスト成熟度モデル（ZTMM）でマイクロセグメンテーションについて取り上げている。[5)]

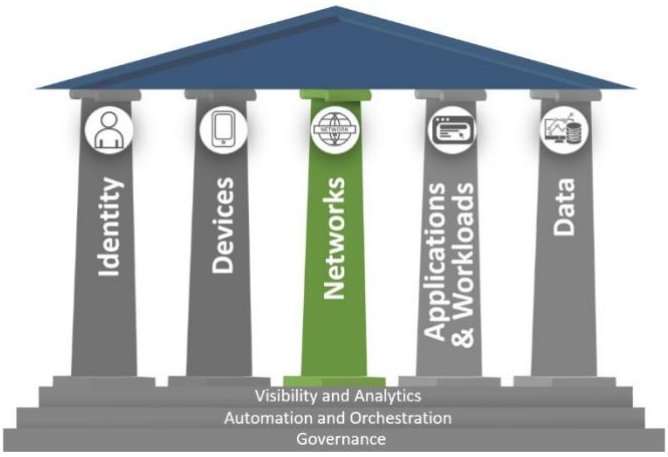


図 *1*：*ZTMM* - ネットワーク

[5] サイバーセキュリティ・インフラセキュリティ庁「ゼロトラスト成熟度モデル第 2.0 版」、ゼロトラスト成熟度モデル第 2.0 版、第 4 節、ZTMM の柱, 2023 年 4 月, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

この文書では、マイクロセグメンテーションはネットワークのセグメンテーション以上のものとして扱われている。マイクロセグメンテーションの実装に使用されるソリューションは、複数の技術的能力にまたがり、開放型システム間相互接続 (OSI) モデルの複数の層で実装される。[6]

技術的能力が限られた大規模な境界に依存していた従来のセグメンテーションから、微調整されたマイクロセグメンテーションに移行するには、リーダーが主導するパラダイムシフトが必要だ。マイクロセグメンテーションの導入に成功すると、エンタープライズのサイバーセキュリティと可用性が向上する。

この文書では、マイクロセグメンテーションへの移行に関する概念、課題、およびメリットに焦点を当て、ZT の推進を支援するこのアーキテクチャイニシアチブを成功裏に導入するための、高レベルのアクションを推奨する。参照した連邦ガイドラインおよび頭字語は、それぞれ附属書 A および附属書 B に記載している。

技術リーダーおよび実装チーム向けに、技術ガイドが別途作成される予定だ。この技術ガイドでは、この移行に関する技術的な考慮事項、推奨事項、および課題について、実装シナリオを用いて説明する。

1.2 背景

大統領令 (EO) 14028、「国のサイバーセキュリティの向上」(2021 年 5 月 12 日)[7] は、各機関に対して、ZT サイバーセキュリティの原則を採用し、それに応じてネットワークアーキテクチャを調整するよう指示している。この取り組みを支援するため、CISA は、政府機関が ZTA を実装する際に使用するための「ZTMM7」[8] を策定した。この成熟度モデルには、5 つの技術的柱が挙げられている。組織は、時間をかけて各柱を進め、システム、アプリケーション、データ、資産を ZTA に向けて保護することができる。 ZT の旅は決して終わりがなく、技術の進歩とともに進化し続ける。図 2 (右) に示すように、組織の目標は ZT 成熟度の頂点に到達し、すべてのコンポーネントを最適に運用することかもしれないが、現実には、組織は ZTA を維持し、現在および予想される脅威に対処し、識別した脅威とリスク許容度に合わせて調整するために、ZT のニーズを継続的に評価する必要がある。

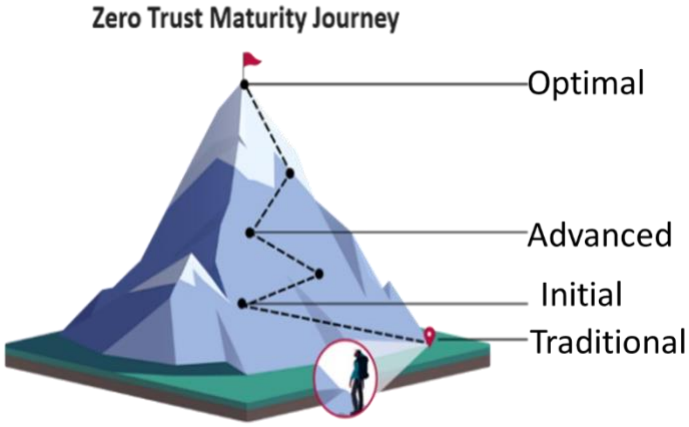


図 2：ゼロトラスト成熟度旅路

[6]国際標準化機構/国際電気標準会議、「情報技術 - 開放型システム間相互接続 - 基本参照モデル、7498-1:1994」、1996 年 6 月 1 日、https://www.iso.org/standard/20269.html。

[7]国際標準化機構/国際電気標準会議、「情報技術 - 開放型システム間相互接続 - 基本参照モデル、7498-1:1994」、1996 年 6 月 1 日、https://www.iso.org/standard/20269.html。

[8]サイバーセキュリティ・インフラセキュリティ庁、「ゼロトラスト成熟度モデルバージョン 2.0」、ゼロトラスト成熟度モデルバージョン 2.0、セクション 4 および ZTMM の柱、2023 年 4 月、https://www.cisa.gov/sites/default/files/202304/zero_trust_maturity_model_v2_508.pdf。

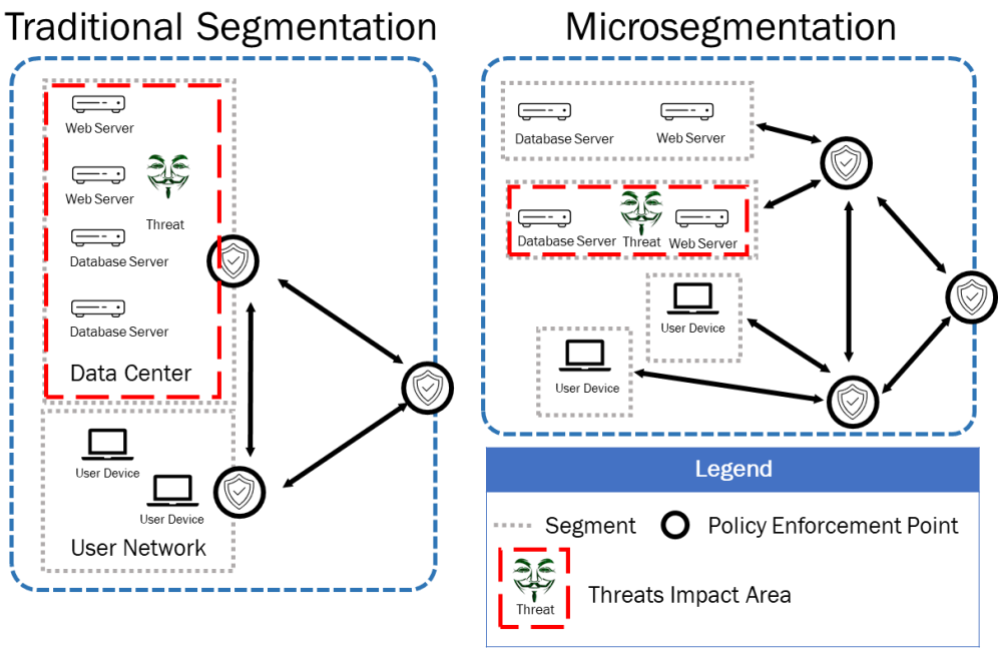


図 3：脅威の影響とセグメンテーション

2022 年 1 月 26 日、行政管理予算局（OMB）は、大統領令 14028「米国のサイバーセキュリティの改善」を支援し、民間機関のエンタープライズセキュリティアーキテクチャを ZTA 原則に整合させ、その基盤とするため、覚書 M-22-09「米国政府のゼロトラストサイバーセキュリティ原則への移行」[9] 発表した[10] この覚書では、各機関は ZTA 構造への移行を義務付けられている。OMB のこの要件を支援するため、CISA は ZTMM をバージョン 2 に更新した。ZTMM は、ZTA を構成する主要なセキュリティ機能を定義し、機能の実装を、厳格さのレベルを高めながら管理しやすい段階に分割するための枠組みを定めている。

ZT の設計哲学は、アクセス認証や認可など、暗黙の信頼（デフォルトで許可）を排除し、明示的な検証（デフォルトで拒否）に置き換えることに重点を置いている。ZT アーキテクチャは、境界に防御構造を構築してセキュリティ侵害の防止を図るのではなく、侵害は発生すると想定し、ネットワークはすでに侵害されていると想定して、現在および将来の侵害による被害を最小限に抑える設計となっている。

M-22-09 は、機関に対し「環境を意味のある形で隔離し、攻撃者が 1 つのアプリケーションやコンポーネントを侵害しても、組織内を横方向に移動して他の独立した環境を侵害できないようにすること」を要求している。[11] これに沿って、ZTMM はネットワーク境界の伝統的なアプローチから、組織ネットワークを細粒度でセグメント化するアプローチへの移行に焦点を当てている。図 3（前ページ）に示すように、マイクロセグメンテーションは、脆弱性やその他の弱

[9]行政管理予算局、「M-22-09 連邦ゼロトラスト戦略」、米国政府をゼロトラストのサイバーセキュリティ原則へと移行、2022 年 1 月 26 日、https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf。

[10]大統領執行事務局、「国のサイバーセキュリティの改善に関する大統領令」、ホワイトハウス、2021 年 5 月 12 日、https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nationscybersecurity。

[11]行政管理予算局、「M-22-09 連邦ゼロトラスト戦略」、米国政府をゼロトラストのサイバーセキュリティ原則へと移行、2022 年 1 月 26 日、https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf。

点を悪用してネットワークに隣接するシステムやデータを攻撃する脅威の機会を制限する。その結果、マイクロセグメントは、悪用された場合の組織への影響を制限する。

従来は組織とインターネットの境界に焦点を当てていた CISA は、現代のネットワークアーキテクチャに対応するため、Trusted Internet Connections（TIC）プログラムを更新した（*TIC 3.0* プログラムガイドブックを参照）。信頼できるインターネット接続（[12] マイクロセグメンテーションは、ネットワークセキュリティグループにおける TIC セキュリティ機能として次のように定義されている。「マイクロセグメンテーションは、アプリケーションおよびデータワークフローの通信ニーズに応じて、ネットワークを物理的または仮想的に分割し、データを保護するためのセキュリティ制御を容易にする。マイクロセグメンテーションは、組織が従来の境界中心のアーキテクチャ（TIC 2.0）から離れ、セキュリティとパフォーマンスの現代化の一環としてマイクロ境界に基づくアーキテクチャを採用する際に不可欠である。これには、TIC 3.0 のユースケースで説明されているものも含まれる。例えば、TIC 3.0 クラウドユースケースなどである

TIC 参照アーキテクチャのセクション 4.3 では、信頼ゾーンとそれに関連する信頼レベルについて説明している。[13]「セキュリティ機能保護を共有する単一の要素または要素のグループは、信頼ゾーンを構成する。これらのゾーンは、ネットワークの場所 に基づいており、組織の境界の内部または外部に定義することができる。前述のように、この信頼ゾーンおよび信頼レベルの概念は、組織が自社の環境をどのように理解および記述するのが最適かによって、よりきめ細かなアプローチ（ZT の概念との整合など）も可能にする。信頼ゾーンは、隣接する信頼ゾーンから信頼やセキュリティを必ずしも継承するわけではなく、信頼やそれに続くセキュリティ機能は、隣接するゾーンの信頼に依存するわけでもない。信頼のレベルは、サービスやデータの展開オプションにも影響する可能性がある。セキュリティ機能を展開し、ゾーンに指定された信頼レベルに見合った厳格な実装を確保することで、機関は、信頼性の向上を、そのゾーンにサービスやより機密性の高いデータを展開する機会として活用することができる。

ZT をサポートするためにマイクロセグメンテーションを使用することは、このアプローチを基盤としている。ZT へ移行する組織は、適切かつ認可されていることが証明されるまでは、すべてのコミュニケーションは悪意のあるものであると想定して作業を行うべきである。ZTA の「決して信頼せず、常に検証する」という基本概念[14] は、PEP による信頼ゾーンと信頼レベルの概念と組み合わせて活用することができる。

ZT の原則との整合性に加え、マイクロセグメンテーションには、次のような追加のメリットがある。

- ネットワークに侵入した攻撃者の横方向の移動範囲を縮小する
- マルウェア、悪意のあるコード、バグ、設定ミスのあるシステム、および内部脅威の封じ込めを改善する
- ネットワークおよびシステムの可視性を向上する

---

[12]サイバーセキュリティ・インフラセキュリティ庁、「CISA TIC 3.0 プログラムガイドブック v1.1」、サイバーセキュリティインシデントおよび脆弱性対応プレイブック、2021 年 11 月、https://www.cisa.gov/sites/default/files/publications/CISA%2520TIC%25203.0%2520Program%2520Guidebook%2520v1.1.pdf。

[13]サイバーセキュリティ・インフラセキュリティ庁、「CISA TIC 3.0 プログラムガイドブック v1.1」、サイバーセキュリティインシデントおよび脆弱性対応プレイブック、2021 年 11 月、https://www.cisa.gov/sites/default/files/publications/CISA%2520TIC%25203.0%2520Program%2520Guidebook%2520v1.1.pdf。

[14]Alper Kerman、「ゼロトラストサイバーセキュリティ：『決して信頼せず、常に検証する』」、国立標準技術研究所：Taking Measure：Just a standard blog、2024 年 4 月 26 日、https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify。

- ポリシーの実施機会の改善、リソース固有のリスク許容度および保護ニーズに対応するきめ細かなポリシーを実現する
- 特定の脆弱性やエクスプロイト、特別なリソースクラスなど、標的を絞った緩和策のサポートを強化する

2. セグメンテーションとは何であるか？

序論

物理的または仮想的なアーキテクチャアプローチとして、ネットワークセグメンテーションは、ネットワークを複数の個別の部分（セグメント）に分割する。これらのセグメントは、通常、インフラストラクチャ、アプリケーション、データ、サービスなどの関連リソースをグループ化する。各セグメントは、独自のネットワークまたはサブネットワークとして機能し、追加のセキュリティと制御を提供する。セグメンテーションは、デバイス、データ、およびアプリケーションへのアクセスを制限し、ネットワーク間のコミュニケーションを制限するために使用される。ZTA では、セグメント境界の PEP が、ポリシー決定機能の一部として、セグメントのリソースへのアクセスを管理する。PEP を使用して、これらのセグメントに出入りするトラフィックを分離、妥当性確認、および監視することができる。セグメンテーションは、論理機能、オペレーティングシステム、またはアプリケーション自体を通じて、物理インフラストラクチャに実装することができる。セグメンテーションの実装方法を選択する際の重要な考慮点は、攻撃者がセグメンテーションを迂回する方法を理解し、その迂回方法を完全にブロックできない場合でも監視できるようにすることである。

2.1 主要な概念

ZT への移行全般、特にマイクロセグメンテーションの実装は、テクノロジー、ポリシー、セキュリティ文化の大きな変化を意味する。そのため、この移行を成功させるには、サイバーセキュリティおよび IT 技術スタッフによる広範なサポートと、組織全体での効果的なコミュニケーションが不可欠だ。影響を受けるすべてのチームは、この移行の背景にある重要な概念、および活動や期待される成果を説明するために使用される用語を理解しておく必要がある。

マクロセグメンテーション：従来のネットワーク管理は、プライベート（内部）ネットワーク空間のマクロセグメンテーションに基づいている。ネットワークセグメンテーション戦略として、マクロセグメンテーションはネットワークを複数の独立したチャンクに分割し、さまざまなビジネス要件に対応する。マクロセグメントの一般的な使用例としては、開発環境と生産環境の分離、非武装地帯（DMZ）、可視性と制御の強化、ユーザーセグメンテーション、アプリケーションセグメンテーションなどが挙げられる。要約すると、マクロセグメンテーションは、組織のネットワーク内の異なる領域間で移動するトラフィックを高度に制御し、セキュリティ、分離、可視性を向上させる。

マイクロセグメンテーション：マイクロセグメンテーションは、プライベート（内部）ネットワーク空間のマクロセグメンテーションの概念を基盤としている。これらは、ビジネス要件に基づく境界または境界線をさらに分割し、プライベート内部ネットワーク空間からビジネス要件をサポートするすべての内部および外部ネットワークに拡張する。これらのマイクロセグメントは、動的または静的に定義でき、従来のネットワーク層の制御や機能を超える機能を活用して、実施と監視を行いる。

信頼ゾーン：従来のネットワークでは、「信頼ゾーン」が使われていて、これはほとんどの場合、ファイアウォールの設定に明示的に表れてる。ファイアウォールのインターフェースの一部は「信頼された」ゾーンに接続され、その他のゾーンは「信頼されていない」ゾーンに接続されてる。一部の事業体は、さまざまな信頼度を導入することで、この概念をさらに強化する場合がある。これらの信頼度は、さまざまな用語で識別される場合がある。多くの場合、管理ネットワークは、特に信頼性の高い位置を占め、厳格な制御と監視の対象となるのが理想的だ。

「ゼロトラスト」という用語が示唆するように、信頼をネットワークの場所（ゾーン）に関連付けるという概念は更新する必要がある。既存の信頼ゾーンおよび機能を利用することは、ソリューションアーキテクチャにおいて依然として有効だが、ZT をサポートするマイクロセグメンテーションでは、リスク、可視性、および制御を考慮してマイクロセグメントを実

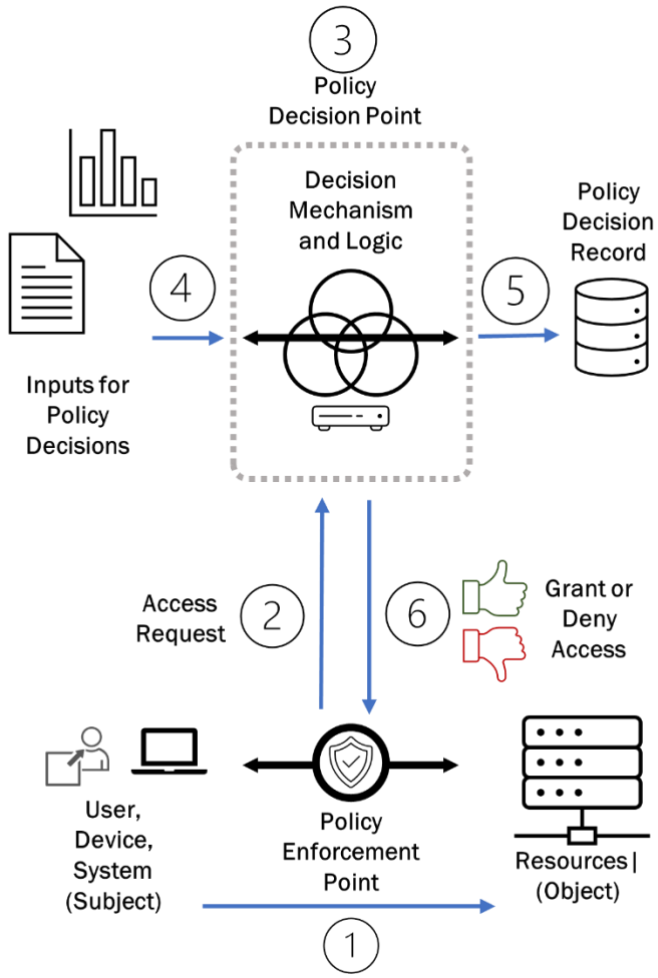
装する必要がある。伝統的な信頼ゾーンは、一般的なネットワークセグメンテーションを支援するために引き続き存在するが、伝統的なネットワーク境界を強化するマイクロセグメントと常に密接に関連しているわけではない。つまり、マイクロセグメントは従来の信頼ゾーンを分割したり、跨いだりする可能性がある。マイクロセグメントゾーンは、設計と実装において伝統的なネットワーク機能を超える機能を活用する。

ポリシー制御アクセス：ポリシーによる動的なアクセス制御では、PEP および関連するポリシー決定ポイント (PDP) を使用して、保護されたリソースおよびネットワークセグメントへのアクセスを決定する。この決定には、従来のネットワークアクセス制御ソリューションなど、さまざまなソースからの情報を活用することができる。通常、ポリシーエンジン (PE) には、PDP に統合された ID 情報、デバイス情報、接続メタデータ、および認可ルールが含まれており、これに基づいてアクセスを決定する。このアクセス決定は、適切な制御プレーンを介して PEP に伝達される。PEP は、この決定を利用して、保護されたリソースへのアクセスを許可または拒否する決定を実行する。このプロセスフローは、図 4：ポリシー制御アクセス（次のページ）に示されている。アクセス決定を行うために使用されるデータソースは、ポリシールールで定義されている。ポリシー制御アクセスは、ZTMM で定義されている ZT の成熟度を最適化するために不可欠である。アクセス決定に使用されるポリシールールは、組織のリスク許容度および保護対象リソースに対する脅威に合わせて調整される。PEP は、OSI モデルの任意の層で動作し、ネットワークまたはシステムで使用されるエンドポイントまたはデバイスに配置することができます。PDP は、アーキテクチャの設計および組織の要件に応じて、複数の PEP をサポートすることができます。アクセス強制の決定には、複数の PEP が関与する場合がある。

サーフェイス管理：これまで、攻撃対象領域はセキュリティモデリングにおいて重要な考慮事項だった。この概念は単純で、攻撃対象領域とは、敵がアクセスできる組織のリソースの一部だ。しかし、マクロセグメンテーションを使用している複雑なエンタープライズ環境では、攻撃対象領域を正確に文書化することは困難だ。マクロセグメンテーションは、マイクロセグメンテーションよりも管理は簡単だが、最新の脅威に対処するために必要なきめ細かな制御ができない。

マイクロセグメンテーションは、攻撃対象領域をより管理しやすいコンポーネントに分割する。各セグメントは、それぞれ独自の攻撃対象領域を持つと考えることができる。そして、セグメントはリソースを防御するために存在するため、各セグメントは「防御対象領域」と考えることができる。これらの保護 面は、組織全体のより小さく、より明確に定義された部分をカバーしているため、管理が容易だ。その結果、このようなサーフェイスは、保護サーフェイス内で実行されるリソースや活動に対するリスクや脅威に焦点を当てた、より適切かつ効果的な保護ポリシーをサポートする。

ポリシーによるアクセス制御：最新のネットワーク設計では、ポリシーを有効にして、リソースへのアクセスを動的に制御することが重視されている。図 4 は、ポリシーによるアクセス制御の主な構成要素と、この動的な決定プロセスがどのように行われるかを示した例だ。



1. ユーザー（サブジェクト）は、PEP を通じて保護されたリソース（オブジェクト）へのアクセスを要求する。

2. PEP は PDP と通信し、アクセス決定を要求する。この要求には、ユーザーに関する情報に加え、デバイス情報や接続特性など、その他の多くの属性が含まれる場合がある。

3. PDP は、確立されたポリシールールを利用してアクセス決定を行う。これには、他のデータソースへのクエリーが含まれる場合もある。

4. 決定ロジックで利用されるポリシールールに基づき、PDP は複数の入力データソース（デバイス状態、ユーザートレーニングステータス、脅威インテリジェンス、ログなど）を利用できる。

5. ポリシーに基づくアクセス決定は記録され、PEP（複数可）に送信され、実行される。

6. PEP はアクセスを許可または拒否し、対象接続をオブジェクトに適切に誘導する。

図 4：ポリシーによるアクセス制御

これらの概念はマイクロセグメンテーションや ZT に限定されたものではないが、マイクロセグメンテーションと ZT のメリットを完全に実現するために必要な、自動化され、動的で条件付きなアクセス決定を可能にする。これらの条件付きアクセス決定には、ユーザーや接続デバイス属性、接続特性など、多様な要素が含まれる可能性がある。通常の営業時間中に、既知の組織デバイスからリソースに接続するユーザーは、営業時間外に、外国にある未知のデバイスから接続する場合とは、、異なるアクセス権限を持つ場合がある。初期アクセス権限を条件に応じて自動的に決定し、セッション中に継続的なアクセス必要性を定期的に妥当性確認するこの機能により、リソースのセキュリティが大幅に向上し、組織とその資産に対するリスクが軽減される。

TIC およびマイクロセグメンテーション：連邦政府内の TIC プログラムでは、政府機関との接続のセキュリティと可視性を向上するために必要な機能とアーキテクチャについて記載している。[15] 連邦政府以外の組織は機能とアーキテクチャの意図する成果を確認し、それらを組織固有の要件およびリスクマネジメントにマッピングすることで、文書および成果物に記載されている原則および設計概念を適用することができる。TIC 3.0 は、TIC 2.0 の境界アーキテク

[15]サイバーセキュリティ・インフラセキュリティ庁、「信頼できるインターネット接続（TIC）：CISA」、サイバーセキュリティ・インフラセキュリティ庁 CISA、2025 年 1 月 13 日アクセス、https://www.cisa.gov/resources-tools/programs/trusted-internet-connections-tic。

チャを進化させ、保護および可視化機能を改善し、プログラムの意図を満たす方法を文書化したものであることにご留意すること。

図 5（以下）は、TIC が組織の境界（マクロセグメンテーション）から、より小さな信頼ゾーン（マイクロセグメンテーション）および PEP へと進化した様子を示している。この変更により、文書に特定のユースケースが追加され、TIC プログラムがクラウドコンピューティング、モバイルユーザー、リモートユーザーへの支援を強化した。この移行に伴い、信頼ゾーンもネットワークの場所に基づくものから属性に基づくものへと進化し、組織が ZTA への移行を可能にした。

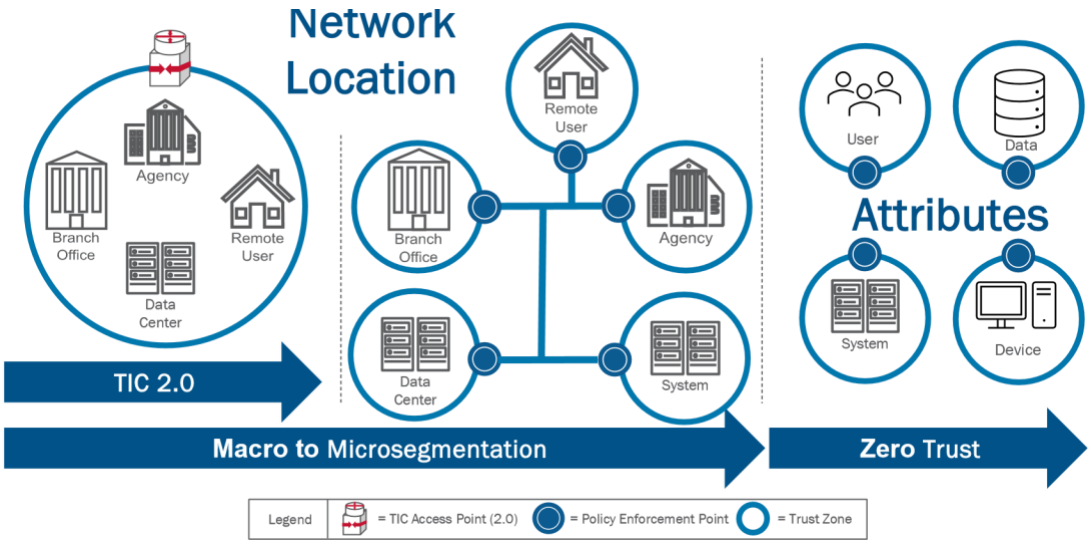


図 5：*TIC* の推移

従来のネットワークのセグメンテーション従来のネットワークは、多くの場合、物理的なネットワークのレイアウトを忠実に反映し、特定のビジネスニーズや機能をサポートする、粗い粒度のネットワークセグメントを中心に構築されている。このようなアーキテクチャのセキュリティ保護は、多くの場合、組織の内部ネットワークとインターネットなどの他のネットワークとの境界の保護に重点が置かれている。このようなシナリオでは、侵害されたエンドポイントは、攻撃者が環境全体を探索し、横方向に移動するための出発点となる。図 6（右）は、このようなネットワークの例を示している。図示されたセグメントは例であり、マクロセグメンテーションの下に開発、科学、研究、バックアップ、管理などの他のセグメントが存在する場合もある。

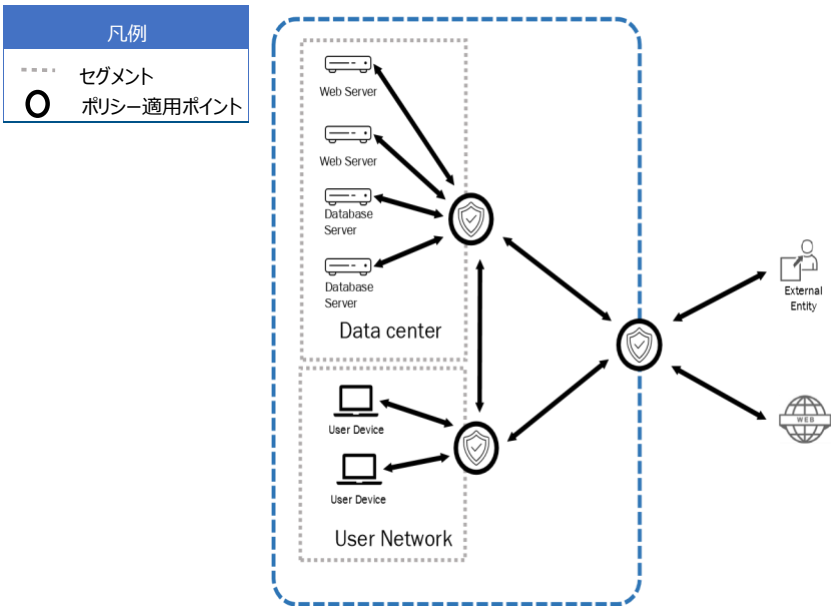


図 6：伝統的なネットワークセグメンテーション

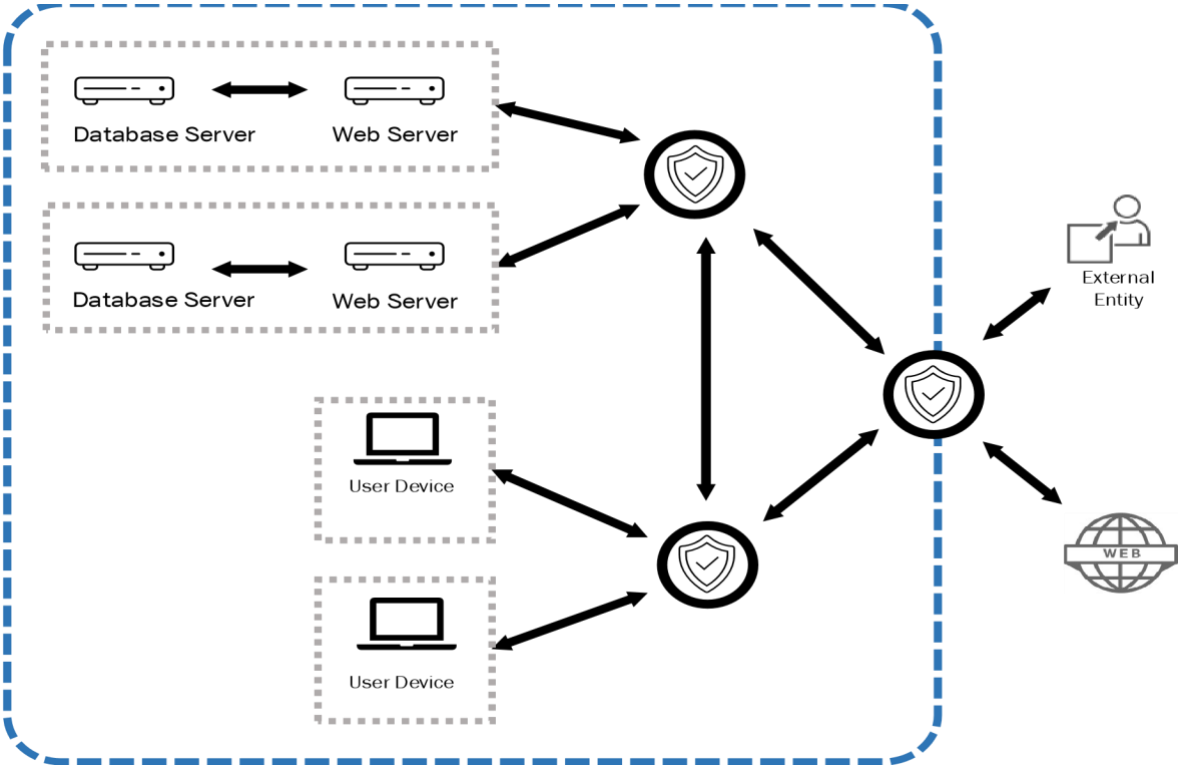


図 7：マイクロセグメンテーション

マイクロセグメンテーション

マイクロセグメンテーションは、ネットワークセグメントのサイズを最小限に抑え、発見の機会を増やし、侵害されたエンドポイントからの横方向の移動を制限することに重点を置いた設計哲学で、図 3.に示されている[16] たとえば、従来のネットワークでは、データセンター内のすべてのサーバーを単一のネットワークセグメントに配置するため、侵害された組織のエンドポイントからアクセスされる可能性がある。図 7（上）に示すマイクロセグメンテーションアプローチを使用すると、組織は、サーバーが業務機能を実行するために必要な他のサーバーとのみ通信できるようにセグメントを作成し、横移動の機会を制限することができる。

より高度なマイクロセグメンテーションの実装では、アプリケーションワークフローとの統合を強化することでネットワークセグメンテーションを強化し、物理的なネットワークレイアウトではなくアプリケーションワークフローに基づいて論理的なネットワークセグメントを作成する。このより高度なアプローチの例は、図 8（次ページ）を参照。ZTA のコンテキストでは、マイクロセグメンテーションは他のポリシー制御メカニズムと連携して、より詳細な認可ポリシーを実現する。このようなモデルでは、マイクロセグメントは動的なシステムコンポーネントやリアルタイムのアクセスニーズを含む場合があるた

[16]ナノセグメンテーションは、ネットワークセグメントのサイズを最小限に抑えることをより重視するために、マイクロセグメンテーションの代わりに使用されることがある。

め、マイクロセグメントの正確な境界は刻一刻と変化する可能性がある。これらの動的なコンポーネントや変動するアクセスニーズは、PEP によって実施されるポリシーによって管理する必要がある。

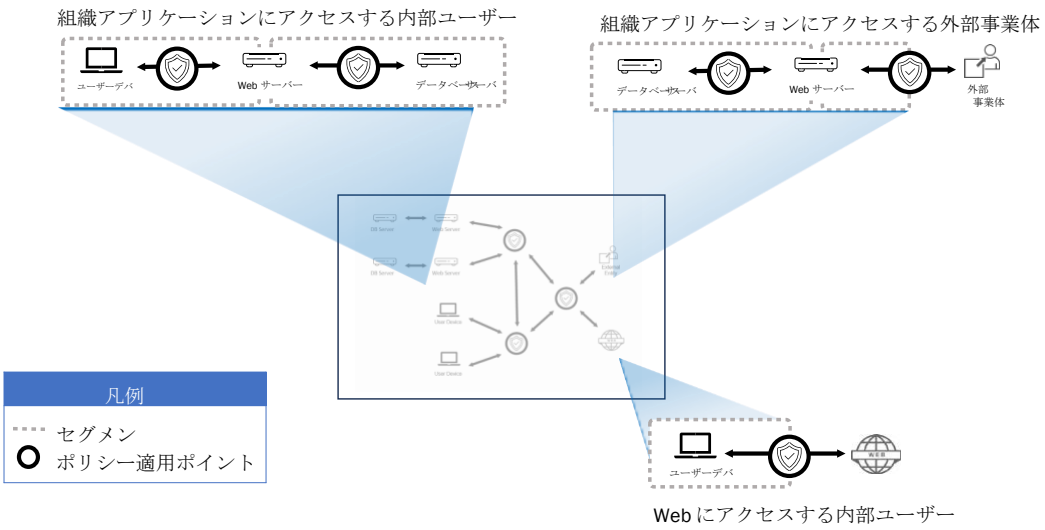


図 *8:* ワークフローベースのマイクロセグメンテーション

2.2 セグメンテーションの種類

組織のエンタープライズアーキテクチャを構成する環境は多様であるため、単一のソリューションを使用してエンタープライズ全体にマイクロセグメンテーションを実装することは現実的ではないか、あるいは望ましくない場合もある。ほとんどのエンタープライズアーキテクチャでは、組織は、既存の機能と 1 つ以上のベンダー製品を組み合わせるなどして、複数のマイクロセグメンテーション機能を組み合わせ、識別されたユースケース、ニーズ、および目標に合わせてそれぞれを適切に適用する必要がある。組織は、利用可能なオプションと、それらを自社の環境に最適に適用する方法を理解する必要がある。

組織は、利用可能なソリューションの種類を調査し、ミッション要件を満たす実装を計画する必要がある。

次の表は、一般的に利用可能なセグメンテーションのタイプについて、概要をまとめたものである。これらは明確な高レベルのタイプであるが、ベンダーのソリューションは複数のタイプで構成される場合がある。

表 *1*：セグメンテーションの種類と機能

タイプ	説明
ネットワーク	ネットワークベースのデバイスおよびアプライアンスは、デバイス経由でルーティングされるネットワークトラフィックに対してセグメンテーションポリシーを適用する。 概要

タイプ	説明
	• 既存のネットワークインフラストラクチャの熟知と再利用により、移行が容易になる可能性がある • レガシーインフラストラクチャがマイクロセグメンテーションをサポートしない状況にも対応可能 • マイクロセグメンテーションへの環境の完全移行と維持が難しい場合がある • エンドポイント、アイデンティティ、アプリケーションワークフローに関する可視性が制限される可能性がある 適用性 • オンプレミス環境 • IaaS（Infrastructure as a Service）/PaaS（Platform as a Service）クラウド展開 例 • ルーター • ソフトウェア定義広域ネットワーク (SD-WAN) • 次世代ファイアウォール • ウェブアプリケーションファイアウォール（WAF）
エンドポイント	ホストやその他のデバイスに展開された機能により、エンドポイントのセグメンテーションポリシーを適用する。 概要 • アプリケーションのワークフロー、アイデンティティ、エンドポイントとのより良い統合を可能にする可能性がある。 • 通常、エンドポイントの場所に関係なく動作し、移動型やリモートエンドポイントにも対応する • すべてのエンドポイントにエージェントを展開する必要があり、追加の保守が必要になる場合があり、アプライアンス、IoT、OT、レガシーインフラストラクチャでは動作しない場合がある。 適用範囲 • オンプレミスおよびリモートユーザーデバイス • サーバー • IaaS クラウド展開 例 • セキュアアクセスサービスエッジ (SASE) エージェント • ホストベースのファイアウォール
コンテナ	アプリケーション仮想化環境内でアプリケーションをパッケージ化し、安全に実行する方法。これらの機能は、コンテナの展開に対するセグメンテーションポリシーを適用する。16F[17] 概要

[17]国立標準技術研究所、「アプリケーション・コンテナのセキュリティ・ガイド NIST SP 800-190」、コンピュータ・セキュリティ・リソース・センター、2017 年 9 月、https://doi.org/10.6028/NIST.SP.800-190。

タイプ	説明
	• 継続的インテグレーション/継続的デリバリー (CI/CD) 展開モデルと容易に統合できる可能性がある • 既存のコンテナ展開と連携できる可能性がある • ソリューションは、特定のコンテナオーケストレーション枠組みに固有のものになる場合があり、移植性が制限される 適用性 • コンテナの展開 例 • コンテナオーケストレーションフレームワークのセグメンテーション サービスメッシュ
ハイパーバイザー	仮想マシンをホストするエンドポイントに展開される機能で、展開された仮想マシンのセグメンテーションポリシーを適用する。 概要 • 既存の仮想マシン (VM) 展開で動作する可能性がある • よく理解されているネットワークベースのセグメンテーションと類似している • ソリューションは特定のハイパーバイザーに依存するため、移植性が制限される 適用範囲 • VM が展開されているハードウェアを組織が管理している VM 展開
クラウド	クラウドネイティブ機能により、クラウドに展開されたインフラストラクチャのセグメンテーションポリシーが強制される。 概要 • アプリケーションワークフロー、ID、クラウドに展開されたリソースとの強力な統合の可能性 • ソリューションは特定のクラウドベンダーに依存するため、ポータビリティが制限される可能性がある。 適用可能性 • クラウドサービスの展開 例 • クラウドネイティブ • クラウドワークロード保護プラットフォーム (CWPP) • クラウドセキュリティポスチャ管理 (CSPM) • クラウドネイティブアプリケーション保護プラットフォーム (CNAPP)

3. 段階的なアプローチ

序論

米国国立標準技術研究所（NIST）の「ゼロトラストアーキテクチャの計画」[18] に準拠して、組織は ZT 機能への投資を行う前に、現在のエンタープライズシステム、リソース、インフラストラクチャ、人員、およびプロセスを評価する必要がある。既存の組織エンタープライズを従来のネットワークセグメンテーションからマイクロセグメンテーションアプローチに移行するには複雑な作業が伴うため、組織は段階的なアプローチを採用し、エンタープライズの一部を時間をかけて移行すべきである。この文書は、組織のアプローチの参考となる高レベルの概要を紹介しているが、各組織は、自社のニーズに最も適したアプローチを決定する必要がある。

組織は、よりスムーズで容易な移行を確保するために、段階的なアプローチを計画し、企業全体の一部を徐々にマイクロセグメンテーションに移行すべきである。

例えば、組織は、組織固有のさまざまな規準（重要度、移行の容易さなど）に基づいて優先順位付けを行い、1 回に 1 つのアプリケーション、ワークフロー、資産、または環境をセグメント化し、時間をかけてエンタープライズを繰り返しセグメント化することができます。以下に概説する段階は 1 回限りの作業ではなく、移行期間中に組織が繰り返し実施する必要がある。これらは、従来のセグメンテーションアプローチが引き続き使用されている場合、およびより高度なセグメンテーションが採用されている場合にも繰り返すことができる。繰り返し実施することで、組織は、組織内のアプリケーションや環境、テクノロジー環境、脅威、攻撃者の手法の変更により、更新が必要な部分に関する経験と洞察を得ることができる。この知識は、すでに展開されているマイクロセグメントの改善に役立てることができる。

この文書では、マイクロセグメンテーションの対象となるシステム、サービス、コンポーネント、およびデータのグループを「候補リソース」と呼ぶ。これらのリソースをグループ化することで、組織はセキュリティ目標を達成するための潜在的かつ適切なマイクロセグメンテーションの選択肢を識別することができる。

3.1 フェーズ 1：セグメンテーションの候補リソースの識別

組織は、アプリケーション、ワークフロー、データ、資産、および環境を確認し、マイクロセグメンテーションへの移行の候補となるリソースを識別する。組織は、組織固有の規準（重要度、セキュリティ、移行の容易さなど）を使用して、候補の優先順位を決定する。たとえば、マイクロセグメンテーションの初期導入段階では、移行の容易さを優先し、その後、 組織がマイクロセグメンテーションの経験を積んだ段階で、重要な資産（高価値資産など）を候補として優先する。

3.2 フェーズ 2：選択した候補リソースの依存関係を識別する

候補リソースについて、組織は、ビジネス機能を実行するために必要なその他のアプリケーション、ワークフロー、データ、資産、および環境を識別する。この識別プロセスには、関係者を参加させる必要がある。

---

[18]国立標準技術研究所、「ゼロトラストアーキテクチャの計画：連邦政府管理者向け計画ガイド」、コンピュータセキュリティリソースセンター、2022 年 5 月 6 日、https://csrc.nist.gov/publications/detail/whitepaper/2022/05/06/planning-for-a-zero-trust-architecture/final。

3.3 フェーズ 3：適切なセグメンテーションポリシーの決定

組織は、候補リソースがビジネス機能を実行できるようにするさまざまなセグメンテーションの選択肢を検討する。次に、組織固有の規準（セキュリティ、実装の容易さ、長期的な保守の容易さなど）を用いて、適切なポリシーを選択する。このプロセスには、さまざまなワークフローへの影響を適切に評価し、関連するリスクを理解するために、ユーザーも参加させるべきである。

3.4 フェーズ 4：更新されたセグメンテーションポリシーの展開

組織は、セグメンテーションポリシーをテストして、その正確性を妥当性確認する。たとえば、ポリシー違反にフラグを立てて、見落とされている可能性のある依存関係を検知する、許容モードでポリシーを実装することができる。次に、ポリシーを展開し、ポリシーの展開を妥当性確認するための適切な可視性が確保されていることを確認する。組織は、変更内容と現在の実施レベルに関する公開文書、およびユーザーがフィードバックを提供したり支援を受けたりするための明確に定義されたチャネルを用意すべきである。

4. 計画上の考慮事項

従来のネットワークセグメンテーションからマイクロセグメンテーションへの移行および既存のエンタープライズは複雑な作業であり、この文書で概説する段階的なアプローチが有効だ。グリーンフィールドアプローチ（以前のプロジェクトの制約のない、白紙の状態のプロジェクトなど）を活用できる組織でも、段階的なアプローチを採用することでメリットを得ることができる。段階的な移行を実行することで、組織は未知の課題や矛盾を識別し、それらを解決するための戦略を立てることができるため、業務ミッションのリスクを最小限に抑えながら、ZT の目標を達成することができる。この文書は、組織の計画立案に役立つハイレベルなアプローチを紹介している。ただし、各組織は、そのニーズに最も適したアプローチを決定する必要がある。

マイクロセグメンテーションへの移行に関する組織の計画では、展開されているさまざまなアプリケーション、ワークフロー、資産、環境、および組織全体での移行を最適にサポートする方法を考慮する必要がある。

4.1 ユーザーと組織のサポート

マイクロセグメンテーションへの移行前および移行中は、ユーザー要件を理解し、ユーザーの賛同を得るとともに、ユーザーやミッションへの悪影響を回避する必要がある。組織は、移行計画の段階で、ユーザーやシステム所有者のニーズを理解するために時間とリソースを割くべきである。

この移行の目的とメリットをユーザーやシステム所有者に伝えることで、彼らの賛同を得るために必要な知識を提供することができ、このようなコミュニケーションは成功に不可欠だ。

4.2 セグメンテーションの対象となるリソースの識別

移行の候補を効果的に識別するには、組織は自社のアプリケーション、ワークフロー、環境、および資産を理解する必要がある。次に、組織はこれらの候補に優先順位を付ける必要がある。その際には、重要度に関する懸念（セキュリティ、ビジネス機能への重要度など）や移行に関する懸念（移行の容易さなど）を考慮する必要がある。

組織が新しいアプリケーションや資産を採用したり、新しい環境（クラウド移行など）に移行したりすることは、マイクロセグメンテーションの原則を適用するチャンスとなります。たとえば、既存のアプリケーションや環境をそのままクラウドに移行するリフティング＆シフトモデルではなく、マイクロセグメンテーションを完全に統合したクラウドネイティブのアプローチを検討すべきである。

4.3 依存リソースの識別

組織は、移行候補がビジネス機能の実行に使用するリソース（移行候補が依存するリソース、および移行候補に依存するリソース（ ）を含む）を把握する必要がある。移行候補が既存の展開済みリソースである場合は、移行候補のコミュニケーションを追跡することで、依存リソースの初期リストを作成することができる。組織は、依存リソースリストの包括性を妥当性確認する必要がある。

4.4 適切なセグメンテーションポリシーの決定

組織は、必要なビジネス機能を可能にしつつ、ネットワーク内での横方向の敵対的な移動の可能性を制限するセグメンテーションポリシーを確立する必要がある。組織は、さまざまなセグメンテーションポリシー間のトレードオフを理解し、そのポリシーが目標を達成できるかどうかを判断すべきである。たとえば、きめ細かいセグメントは横方向の移動の機会を制限することができるが、そのようなきめ細かいセグメントの開発、展開、および保守は困難な場合がある。粗粒度のセグメントは管理が容易であるが、横方向の移動の増加の可能性を考慮して、追加のセキュリティ保護と可視性が必要になる場合がある。あるいは、組織の既存のマイクロセグメンテーションインフラストラクチャを使用すると、ネットワークアーキテクチャに基づいたセグメンテーションアプローチの開発と維持が容易になる場合がある。一方、その組織のアプリケーションワークフローに基づいたセグメンテーションアプローチは、セキュリティとアプリケーションの整合性を高めることができる場合がある。

4.5 更新されたセグメンテーションポリシーの展開

組織は、更新されたマイクロセグメンテーションポリシーを展開する際に、潜在的な問題について考慮し、これらの更新されたポリシーを元に戻す機会を含めることを検討すべきである。ポリシーを更新する前に、組織は、セキュリティ要件を満たしながらビジネス機能を継続するために、展開プロセス全体を通じて適切なモニタリング、テスト、およびアセスメントの手順を実施すべきである。

4.6 ユーザーデバイスの取り扱い

ユーザーデバイスは、ほとんどの組織のワークフローの中核を成している。リモートワークの増加に伴い、多くのユーザーデバイスはオンプレミスとオフプレミスの両方の場所で動作し（つまり、ローミングデバイス）、定期的に両者の間を移動している。これらのデバイスのローミング特性は、マイクロセグメンテーションの考慮事項を複雑にする可能性がある。同時に、これらのデバイスは、信頼できないリソース（例：インターネット、メール）へのアクセスや、潜在的に信頼できない場所での動作により、追加のセキュリティ上の懸念を引き起こす可能性がある。オンプレミスのエンドポイントについては、従来のネットワークベースのマイクロセグメンテーションアプローチをユーザーエンドポイントに採用することができます。ただし、リモートで動作するユーザーエンドポイントについては、ユーザーエンドポイントに適切なセグメンテーションを提供するために、エージェントベースまたはアプリケーションベースのアプローチを検討する必要があるかもしれません。また、ユーザーデバイスに対する多層防御戦略の一環として、追加のセキュリティ保護と可視化も検討すべきである。

4.7 OT、IoT、レガシー環境およびデバイスの取り扱い

OT、IoT、およびレガシー環境、デバイス、アプリケーションは、マイクロセグメンテーションソリューションの展開にはあまり適していない場合がある。たとえば、これらのデバイスではエージェントベースのセグメンテーションソリューションを使用できない場合があり、ネットワークベースのセグメンテーションソリューションの展開が必要になります。同時に、これらのリソースはセキュリティ保護が限定的である可能性があり、これらのリソースを保護し、侵害された場合の悪用を制限するためのセグメンテーションの必要性が高まっている。組織は、利用可能な代替ソリューションを検討すべきであるが、セグメンテーションポリシーを定義する際には、これらのリソースも考慮に入れる必要がある。これには、これらのリソースへのアクセス、およびこれらのリソースからのアクセスを可能な限り制限することが含まれる。

たとえば、組織は OT 環境を IT 環境からセグメント化し、OT 環境でのビジネス機能の実行に必要なトラフィックのみ許可するポリシーを定義することができる。可能であれば、組織は、多層防御戦略の一環として、このセグメント化に追加のセキュリティ保護と可視性を補完することができる。

4.8 制御と可視化の集中化

組織のエンタープライズは、さまざまな環境、アプリケーション、エンドポイント、ユーザー、その他のリソースで構成されている。たとえば、組織には、オンプレミスの拠点、クラウドベースのインフラストラクチャ・アズ・ア・サービス（IaaS）およびソフトウェア・アズ・ア・サービス（SaaS）の展開、およびオンプレミスとリモートの両方で動作するユーザーがいる場合がある。エンタープライズ全体でマイクロセグメンテーションポリシーを維持および妥当性確認を行うことは困難である。組織は、ポリシーが実装されている場所に関係なく、これらのポリシーの管理を一元化する方法を検討し、ポリシーの適切な適用を理解および妥当性確認するために必要な可視性を確保する必要がある。

4.9 継続的な保守と進化

マイクロセグメンテーションアーキテクチャへの移行は、単一の移行ではない。組織のアプリケーションや環境、テクノロジー環境、脅威、攻撃者の手法の変化により、既存のセグメンテーションアプローチの妥当性を確認し、これらの変化に対応するための更新が必要になる場合がある。組織全体の ZTA 実装の一部としての変更により、組織のマイクロセグメンテーションアーキテクチャに追加の変更が必要になる場合がある。組織アプリケーションおよびインフラストラクチャの展開プロセスの一環として、これらのネットワークセグメンテーションポリシーを定義、妥当性確認、およびテストすることで、アプリケーションおよびインフラストラクチャの変更に合わせてマイクロセグメンテーションポリシーを確実に進化させることができる。さらに、組織は、セグメンテーションアプローチを定期的に評価し、現在の脅威ランドスケープに対してその有効性を妥当性確認する必要がある。

5. マイクロセグメンテーションの例

CISA は、ZTA への移行を進めるさまざまな機関と協力してきた。以下の例示シナリオは、各機関がマイクロセグメンテーションの導入における初期アプローチをどのように扱ったかを示している。これらのシナリオでは、マイクロセグメンテーションへの移行は、組織の ZT 戦略全体の一部として扱われている。これらの例は、特定のハイレベルな初期アプローチを強調したものだが、各組織は、ZTA の全体的な実装を進めていく中で、特定のアプリケーション、環境、またはミッションのニーズに応じて、追加の方法を採用している場合もある。

5.1 シナリオ #1：既存のオンプレミスエンタープライズの再構築

この組織は、主にオンプレミス環境に展開されたインフラストラクチャ、サービス、およびアプリケーションで構成されていた。既存の展開規模が大きかったため、この組織は、最初の取り組みとして、既存のインフラストラクチャのセグメンテーションの強化に重点を置くことにした。この取り組みは、主に、既存のネットワークインフラストラクチャを使用し、必要な場合にのみコンポーネントを更新して、ネットワークベースのマイクロセグメンテーションモデルを導入するという形で行われた。

この組織は、セグメンテーションの対象となるリソースと関連する依存関係を識別するための十分なデータを提供するために、アプリケーション、ワークフロー、データ、ハードウェア資産、および環境の詳細なインベントリを作成した。最初の移行候補については、アーキテクチャの目標を定義するポリシーを作成して、データセンター、サーバー、ユーザーなどの高レベルの環境を適切にセグメント化することに重点を置いた。これらのポリシーは、目標の要件を満たす技術的ソリューションによって実装される。これらの高レベルのセグメンテーション機能が整った後、組織は、より微調整されたマイクロセグメンテーションの候補を探し始めた。組織は、マイクロセグメンテーションの原則を実際に適用する方法を学ぶために、移行の容易さに重点を置いて、移行の最初の候補を選定した。

各候補について、組織は新しいポリシーを開発し、ポリシー違反が発生した場合にアラートを発する許可モードで適用した。これにより、ポリシーを時間をかけて磨き上げ、最終的に本番環境に移行することができた。組織は、移行対象のリソースがミッション要件を満たし続けることを確認するため、パイロットユーザーグループと協力して各リソースのテストを実施した。

5.2 シナリオ #2: 環境移行の一部としてのマイクロセグメンテーション

この組織は、組織環境とアプリケーションが主にオンプレミス環境に展開されていたモデルから、ほとんどのインフラストラクチャがクラウド環境に展開されるモデルへの移行を目指していました。これらの新しい展開はグリーンフィールドであることから、 のマイクロセグメンテーションの原則を最初から組み込む機会となりました。レガシー環境とサービスをクラウドに移行するにあたり、この組織はクラウドネイティブのセグメンテーション機能を使用してマイクロセグメンテーションを実装した。

組織は、アプリケーション、ワークフロー、データ、エンドポイント、ユーザー、環境の詳細なインベントリを作成し、これらをクラウド環境に移行する最適な方法を決定した。組織は、クラウドへの「リフトアンドシフト」ではなく、クラウドネイティブ技術を使用して移行対象を実装することを選択した。このアプローチにより、クラウド環境内で利用可能な機能を使用してマイクロセグメンテーションを統合することができた。

この組織は、移行候補リソースごとに、パイロットユーザーグループと協力して、クラウド環境への再実装を行った。これは、同等の SaaS ソリューションを採用するか、Platform as a Service (PaaS) または IaaS を使用して機能を再実装する形になる。この組織は、展開方法に固有の機能を使用して、適切なセグメンテーションを実施した。たと

えば、コンテナベースの PaaS 展開では、サービスメッシュアーキテクチャを使用し、SaaS 展開では、ネイティブの CASB (Cloud Access Security Broker) 展開を使用した。パイロットユーザーグループがパイロット展開をテストして妥当性を確認した後、組織はパイロットを本番環境に移行し、全ユーザーベースを新しい展開に移行した。このアプローチにより、組織は、レガシーのセグメンテーションを含め、オンプレミスインフラストラクチャを徐々に縮小することができました。

5.3 シナリオ #3：分散型エンタープライズのマイクロセグメンテーション

この組織は、さまざまな支店や多数の遠隔地勤務者を含む分散型ワークフォースを有している。支店からのすべてのトラフィックはメインロケーションを経由してルーティングされ、オンプレミスアプリケーションへのアクセスを可能にし、組織のトラフィックに中央集約型のセキュリティポリシーを適用できるようにしていた。遠隔地ユーザーは、仮想プライベートネットワークを使用してオンプレミスロケーションに接続し、オンプレミスアプリケーションにアクセスしていた。この組織は当初、ネットワークベースとエージェントベースの展開を組み合わせたマイクロセグメンテーションの実装に SASE ソリューションの利用に重点を置いていました。これにより、ポリシーの一元化と、組織内のエンドポイントおよび支社と組織およびリモートリソースとの接続の可視化を実現することができました。目標は、SASE ソリューションが提供する一元化された制御を使用して、マイクロセグメンテーションを実装することであった。

この組織は、パイロットセットの支店と、オンプレミスおよびリモートのユーザーからなるパイロットグループと協力した。この組織は、ネットワークベースの展開方法を使用して支店のトラフィックを SASE プロバイダに送信し、エージェントベースの展開方法を使用してユーザーのエンドポイントから SASE プロバイダへのアクセスを可能にした。当初、SASE の展開は、インターネットへのアクセスを仲介するために使用され、支店やリモートユーザーがメインのロケーション経由でインターネットにアクセスする必要がなくなった。その後、組織は、 を使用して、パイロットグループが直接アクセスする代わりに、SASE プロバイダ経由で組織の内部アプリケーションにアクセスできるようにする SASE プロバイダの機能を利用できるようになりました。アプローチの成功を妥当性確認した後、組織は残りの支店に移行し、SASE エージェントを組織のユーザーエンドポイントにさらに広く展開した。

このモデルにより、組織は SASE ソリューションを、組織のエンドポイントと展開されたサービス間のすべての接続を仲介する、中央のポリシー実施ポイントとすることができた。組織は、組織内の各アプリケーションについて、まず SASE ソリューションを通じてパイロットグループに提供した。その後、テストを経て、組織は SASE ソリューションをエンタープライズ全体に提供した。サービスへのすべてのアクセスが SASE ソリューションに移行した後、組織はサービスへの直接アクセスを無効にした。ただし、サービスへのアクセスが必要なレガシーリソースについては例外とする。

6. 結論

マイクロセグメンテーションの実装を通じて ZTA をサポートするには、組織のテクノロジー、ポリシー、セキュリティ文化の大幅な変革が必要だ。組織は、テクノロジーの更新とクラウドへの移行を活用して、マクロセグメンテーションからマイクロセグメンテーションに移行すべきである。

この文書は、ZTA の一環としてマイクロセグメンテーションへの移行の計画と範囲の決定を開始する組織向けに、概要的なガイダンスと推奨事項を提供するものだ。CISA は、この移行期間中に実装チームをサポートするための技術ガイドを後日公開する予定だ。

附属書 A：連邦ガイドライン

以下の文書リストには、公開時点で入手可能なガイダンス文書の最新バージョン（ドラフトを含む）が記載されている。

- サイバーセキュリティ・インフラセキュリティ庁、*CISA* のゼロトラスト成熟度モデル、バージョン *2.0*、2023 年 4 月。
- サイバーセキュリティ・インフラセキュリティ庁、信頼できるインターネット接続 *3.0* クラウド使用事例、バージョン *1.1*、2023 年 12 月。
- サイバーセキュリティ・インフラセキュリティ庁、信頼できるインターネット接続 *3.0* プログラムガイドブック、バージョン *1.1*、2021 年 7 月。
- サイバーセキュリティ・インフラセキュリティ庁、信頼できるインターネット接続 *3.0* リファレンスアーキテクチャ、バージョン *1.1*、2021 年 7 月。
- サイバーセキュリティ・インフラセキュリティ庁、*Trusted Internet Connections 3.0 Security Capabilities Catalog*、バージョン *3.2*、2024 年 11 月。
- 国際標準化機構/国際電気標準会議 (ISO/IEC)、*7498-1:1994*、情報技術 – 開放型システム間相互接続 – 基本参照モデルセクション 3.1 *(1996* 年更新*)*。
- 国立標準技術研究所、ゼロトラストアーキテクチャの計画：連邦政府管理者向け計画ガイド、2022 年 5 月。
- 国立標準技術研究所、*NIST* 特別刊行物、*800-190*：アプリケーション・コンテナ・セキュリティ・ガイド、2017 年 9 月。
- 国立標準技術研究所、*NIST* 特別刊行物、*800-207*：ゼロトラストアーキテクチャ、2020 年 8 月。
- 国立標準技術研究所、*NIST* 特別刊行物、*800-215*：エンタープライズネットワークのセキュリティ確保に関するガイド、2022 年 11 月。
- 行政管理予算局、大統領令 *14028*「国のサイバーセキュリティの改善について」、2021 年 5 月。
- 行政管理予算局、覚書 *22-09*：連邦ゼロトラスト戦略、2022 年 1 月。

附属書 B：頭字語

略語	Meaning	意味
CASB	Cloud Access Security Broker	クラウドアクセスセキュリティブローカー
CI/CD	Continuous Integration/Continuous Delivery	継続的インテグレーション/継続的デリバリー
CISA	Cybersecurity and Infrastructure Security Agency	サイバーセキュリティ・インフラセキュリティ庁
CNAPP	Cloud-Native Application Protection Platform	クラウドネイティブアプリケーション保護プラットフォーム
CSPM	Cloud Security Posture Management	クラウドセキュリティポスチャ管理
CWPP	Cloud Workload Protection Platform	クラウドワークロード保護プラットフォーム
DMZ	Demilitarized Zones	非武装地帯
EO	Executive Order	大統領令
FCEB	Federal Civilian Executive Branch	連邦文民行政機関
IaaS	Infrastructure as a Service	サービスとしてのインフラストラクチャ
ICS	Industrial Control System	産業用制御システム
IOT	Internet of Things	モノのインターネット
IP	Internet Protocol	インターネットプロトコル
ISO/IEC	International Organization for Standardization/International ElectroTechnical Commission	国際標準化機構/国際電気標準会議
IT	Information Technology	情報技術
M	Memorandum	覚書
NIST	National Institute of Standards and Technology	国立標準技術研究所
OMB	Office of Management and Budget	行政管理予算局

OSI	Open Systems Interconnection	開放型システム間相互接続
OT	Operational Technology	オペレーショナルテクノロジー
PaaS	Platform as a Service	サービスとしてのプラットフォーム
PDP	Policy Decision Point	ポリシー決定ポイント
PEP	Policy Enforcement Point	ポリシー実施ポイント
SASE	Secure Access Service Edge	セキュアアクセスサービスエッジ
SaaS	Software as a Service	サービスとしてのソフトウェア
SD-WAN	Software-Defined Wide Area Network	ソフトウェア定義広域ネットワーク
TIC	Trusted Internet Connections	信頼されたインターネット接続
VM	Virtual Machine	仮想マシン
VLAN	Virtual Local Area Network	仮想ローカルエリアネットワーク
WAF	Web Application Firewall	Web アプリケーションファイアウォール
ZT	Zero Trust	ゼロトラスト
ZTA	Zero Trust Architecture	ゼロトラストアーキテクチャ
ZTMM	Zero Trust Maturity Model	ゼロトラスト成熟度モデル