ゼロトラスト・ネットワーキングのための アリスタネットワークスの マルチドメイン・セグメンテーション・サービス（MSS）

マイクロセグメンテーション・ソリューションでデータセンターからキャンパス、ブランチまでの水平型（East-West）ラテラル・ネットワーク間の脅威を軽減

企業は、ハイブリッド・ワーカーやモバイル・ワーカー、管理対象および管理対象外の IT、OT、IoT デバイスの爆発的増加、分散型クラウド・アプリケーションなどのトレンドに推進されるデジタル変革に取り組んでおり、従来のネットワーク・セキュリティ境界の概念は崩れつつあります。

この急速な変化と、変わり続ける脅威の状況から、多くのセキュリティ上の課題が生じています。最大の課題は、ラテラル・ムーブメントを最小限に抑えてランサムウェアやその他のサイバー攻撃の水平展開を防ぐことです。このような増大する脅威を迅速に特定し、封じ込めなければ、収益と顧客の甚大な喪失につながる可能性があり、企業の評判も損なう危険があります。

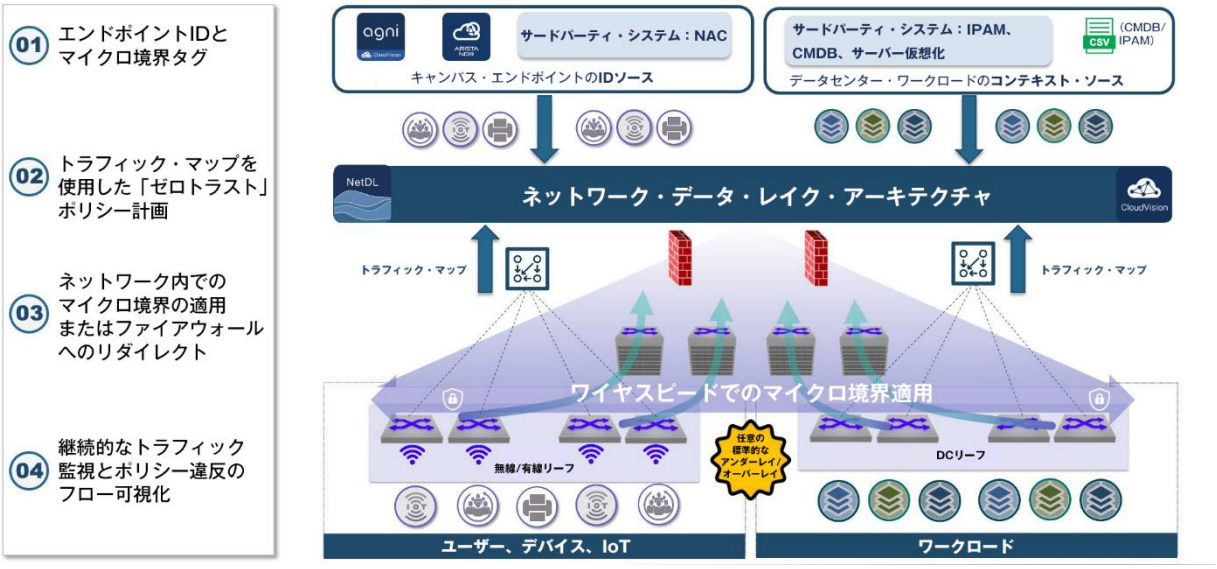
ゼロトラストとは、最新のデジタル変革を進めている企業を保護する枠組みです。

ゼロトラストでは、ネットワーク境界が存在しないことを前提とし、「Never Trust Always Verify（決して信頼せず、必ず検証せよ）」というアプローチに基づいて、すべてのユーザー、デバイス、アプリケーションを適切なアクセス権限とセキュリティ・ポリシーに照らして継続的に監視、検証し、信頼できるトラフィックのみを明示的に許可する必要があります。

アリスタのマルチドメイン・セグメンテーション・サービスは、米国のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）の「ゼロトラスト成熟度モデル」と同様の、以下のゼロトラスト・フレームワークの主要原則を実装します。

- **ラテラル・ムーブメントを抑制する**：ID 認識型マイクロ境界
- **何も信頼しない**：信頼できるトラフィックのみを明示的に許可するゼロトラスト・ポリシー
- **必ず検証する**：ポリシー違反および許可されたトラフィックの可視化、ゼロトラスト・ポリシーの更新と検証

Arista MSS は、データセンターからキャンパス、ブランチまで一貫した運用モデルでマイクロセグメンテーションを大規模に計画、展開、運用するための 4 つのコア・サービスを提供します。



1. エンドポイント ID とマイクロ境界タグ

マイクロセグメンテーション戦略を計画する最初のステップは、エンドポイント、ワークロード、さらにはネットワークを特定のマイクロ境界タグにバインドすることです。 Arista NetDL を搭載した CloudVision MSS は、外部ソースに接続してエンドポイントとワークロードを動的に識別してタグ付けすることで、マイクロ境界管理を自動化します。Arista MSS は、NAC システム、CMDB、IPAM、仮想化インフラストラクチャ管理ソリューションなど、さまざまな外部ソースに接続できます。

2. トラフィック・マップを使用した「ゼロトラスト」ポリシー計画

ゼロトラスト・アーキテクチャの原則では、ネットワーク上のすべてのトラフィックにセキュリティ・ポリシーによる明示的な許可が必要です。ゼロトラスト・ポリシーを作成するには、ネットワーク上の既存のトラフィック・フローを完全に可視化する必要があります。そうすることで、ポリシーで適切なリソースを保護すると同時に、正当な業務のフローを妨げないようにします。

Arista MSS は、ネットワークのさまざまな部分内および部分間のすべての通信をマッピングし、観測されたトラフィック・マップに基づいて信頼できる通信のみを許可する推奨ポリシー・セットを提供します。

3. ネットワーク内でのマイクロ境界の適用またはファイアウォールへのリダイレクト

次に、Arista MSS はゼロトラスト・ポリシーを EOS 搭載ネットワーク・スイッチに配布します。スイッチは、ワイヤスピードの分散適用を自ら実行するか、トラフィックをステートフル L4-7 インスペクション用にサードパーティ・ファイアウォールにリダイレクトすることができます。重要なのは、アリスタのスイッチベースの適用は、高度なタグ付けエンジンでハードウェア使用率を最適化し、スケーラビリティを最大化することにより、従来の ACL ベースのセグメンテーションに関連する TCAM 枯渇などの課題を克服できることです。また、タグはスイッチ内部にあり、ネットワーク・インフラストラクチャ全体で共有されないため、Arista MSS は任意のマルチベンダー・ネットワークにシームレスに挿入できます。このアプローチでは、組織を単一ベンダー・ネットワークに強制する独自プロトコルも回避できます。

4. 継続的なトラフィック監視とポリシー違反の可視化

ゼロトラスト・ポリシーが展開されると、MSS はポリシー違反を監視し、ネットワークでドロップされた特定のフローを報告できます。これにより、管理者は、有効だが新しいサービスが拒否されたときにゼロトラスト・ポリシーを更新したり、トラフィック・ルール違反を試みる特定のエンドポイントを監視したりするための重要な情報を得ることができます。

Arista MSS の主な利点

1. **キャンパス、ブランチ、データセンターのマイクロセグメンテーションに対応する単一の運用モデル**
   すべてのスイッチング・プラットフォームに共通の単一の EOS バイナリ、単一の Arista CloudVision® ポリシー・オーケストレーション・プラットフォーム、状態管理と監視のための集約されたネットワーク・データ・レイク（Arista NetDL™）インフラストラクチャに基づいています。

2. **カスタム・プロトコルやカスタム・ハードウェアを使用しない標準ベースのネットワーキング**
   Arista MSS は、他のスイッチベースのマイクロ境界セグメンテーション・ソリューションとは異なり、カスタム・プロトコルやカスタム・ハードウェアに依存しないため、標準的なブラウンフィールド・ネットワークやマルチベンダー・ネットワーク（有線および無線）に統合できます。

3. **カスタム・エージェントやカスタム・ソフトウェアを使用せず、あらゆるエンドポイントに柔軟に対応**
   MSS はエンドポイントやワークロードにソフトウェア・エージェントを必要としないため、マイクロ境界セグメンテーションをキャンパスからブランチ、工場、IoT エンドポイントや、データセンターの仮想ワークロードおよびベアメタル・ワークロードにまでシームレスに拡張できます。特定のオペレーティング・システムや仮想化プラットフォームの制限はありません。

4. **ゼロトラスト・マイクロ境界の管理の簡素化**
   CloudVision は、ネットワーク・アクセス制御ソリューション、IP アドレス管理製品、IT サービス管理ツール、仮想化プラットフォームなど、さまざまなキャンパス・エンドポイントおよびデータセンター・ワークロードの ID ソースと統合されます。このため、Arista MSS は、企業全体に ID 認識型マイクロ境界を動的に確立し、適用できます。

5. **「盲点」を排除したゼロトラスト・ポリシーの安全な展開**
   MSS は、Arista NetDL のデータを使用して、すべてのトラフィック・セッションのマップを生成し、観測されたトラフィック・マップに基づいてゼロトラスト・ポリシーの推奨セットを提供します。ポリシーが展開されると、MSS はポリシーに違反するトラフィックを継続的に監視し、監視とルール更新のためにフロー情報を CloudVision にストリーミングすることができます。重要なのは、MSS がネットワーク脅威検出・対応（NDR）やエンドポイント脅威検出・対応（EDR）など他のコンテキスト・ソースにも接続できることです。これにより、Arista MSS は、誤動作や侵害の可能性があるエンドポイントやワークロードに迅速に対応でき、必要に応じてそれらを分離して、侵害による組織への影響を最小限に抑えることができます。

Arista MSS を導入することによってメリットを得られる組織

既存のマイクロセグメンテーションを展開済みで、次のことを検討している組織：

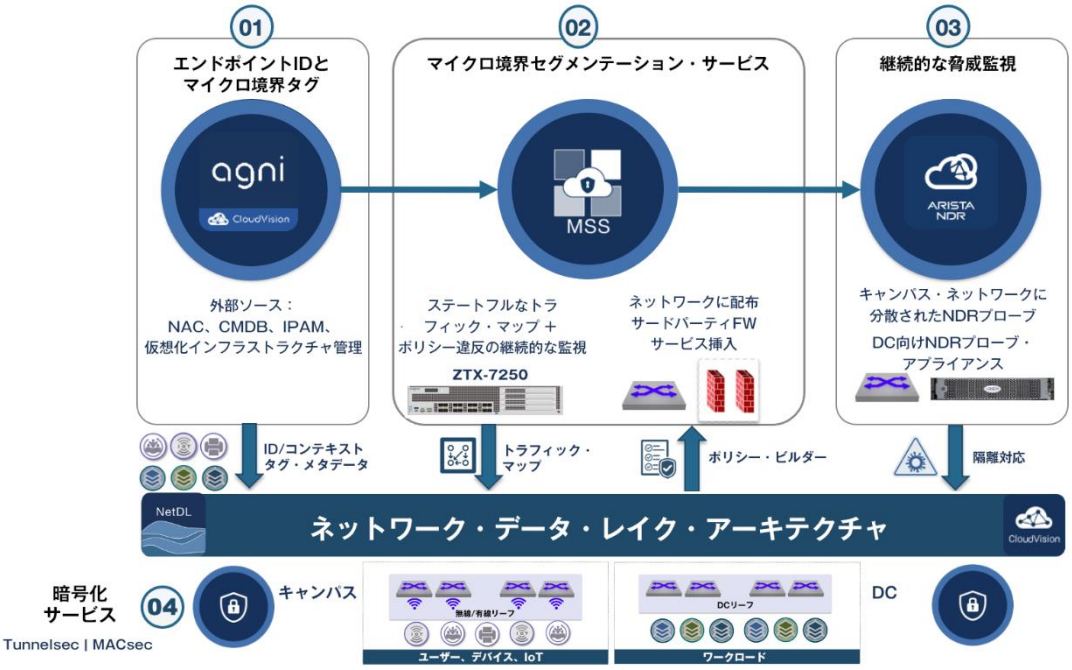
- **強化と拡張**：エージェント/ホストベースのマイクロセグメンテーションを強化して、ホスト・ファイアウォール/エージェントによって管理されていない残りのインフラストラクチャに拡張すること。
- **簡素化**：データセンターからキャンパス、ブランチまで、あらゆるネットワーク・オーバーレイおよびアンダーレイに適応する展開しやすい一貫したソリューションを採用して、既存のスイッチベースのマイクロセグメンテーション展開を簡素化すること。

マイクロセグメンテーションを導入するのは初めてで、次のことを検討している組織：

- **ファイアウォール費用の削減**：ファイアウォール費用を削減すると同時に、セグメンテーションをすべての内部トラフィックに拡張すること。
- **ゼロトラストの取り組みの加速**：既存のブラウンフィールド・ネットワーク・インフラストラクチャと有線および無線のエンドポイント、仮想化ワークロード、ベアメタル・ワークロードに簡単に組み込めるソリューションを採用して、ゼロトラストの取り組みを加速すること。

まとめ：アリスタのゼロトラスト・ネットワーキング（ZTN）サービス

Arista MSS は、アリスタの ZTN アーキテクチャの基盤の 1 つであり、企業全体にゼロトラストの取り組みをシンプルに導入するための一連のサービスを提供します。



詳しくは、www.arista.com/en/solutions/security/mss をご覧ください。

- Arista CloudVision AGNI：アクセス制御
- Arista MSS：ID 認識型マイクロ境界セグメンテーション
- Arista NDR：継続的な脅威監視と隔離対応

リファレンス：

https://www.arista.com/assets/data/pdf/Whitepapers/Zero-Trust-Maturity-Model-WP.pdf

https://www.arista.com/assets/data/pdf/Whitepapers/MSS-Segmentation-Technical-WP.pdf

アリスタネットワークスジャパン合同会社

〒100-0004　東京都千代田区大手町 1-7-2　東京サンケイビル　27F
Tel:03-3242-6401

西日本営業本部
〒530-0001　大阪市北区梅田 2-2　ヒルトンプラザウエストオフィスタワー　19F
Tel: 06-6133-5681

お問い合わせ先

Japan-sales@arista.com

www.arista.com/jp

Copyright © 2024 Arista Networks, Inc.
Arista のロゴ、および EOS は、Arista Networks の商標です。その他の製品名またはサービス名は、他社の商標またはサービス商標である可能性があります。

2024 年 4 月 23 日