ゼロトラストの成熟度を高めるには、まずネットワークから

はじめに

ゼロトラストの概念はかなり前から存在しましたが[1]、ここ 10 年間で、多くの組織がゼロトラスト・アーキテクチャの構築と維持に乗り出すようになりました。この取り組みが加速した原因は、内部脅威や、ランサムウェア、国家機関による攻撃などがハード境界をたやすく突破し、ネットワークの「脆弱な内側」を自由に移動する例が増えたことにあります。特に注意すべきなのは、最近の攻撃はマルウェアを使わず、内部の人間の認証情報や、環境内に展開済みの正規のアプリケーションを利用することが多いという点です。つまり、組織を標的とする攻撃のほとんどは、それが内部の正規ユーザーが手引きしたり、意図的に仕掛けたりしたものでなくとも、実態としては「内部攻撃」になります。

ゼロトラスト化については多くの労力や資金が投じられていますが、この取り組みの現状について疑念を持つ人もいます。見込み客、顧客、パートナー、業界アナリストと話してみると、進展していることは明らかです。たとえば、この 2～3 年で、ゼロトラストはゴールではなく、終わりのない戦略であるという理解が広がりました。さらに、多くの組織がこの戦略に着手し、セキュリティを強化する多要素認証やシングル・サインオンなどのメカニズムを導入して、ひとまずの成果を上げています。しかし、どれほど熱心な組織でも、ID、アプリケーション、デバイス、ネットワーク、データのすべての領域でゼロトラストを実現しようとすると、たちまち壁にぶつかっています。

本ホワイトペーパーでは、ゼロトラスト戦略に立ちふさがる障害について説明します。また、先進的な組織が採用している、ゼロトラストを段階的に成熟させるアプローチについて触れ、この考え方を念頭に置いて、米国のサイバーセキュリティおよびインフラストラクチャ・セキュリティ庁（CISA）とアナリスト会社 Forrester が提唱する成熟度モデルの詳細を見ていきます。そして、これらのモデルに基づき、広範囲にわたるネットワーク戦略で他の領域の成熟度不足をどのように補えるかを説明します。最後に、アリスタのセキュリティ・ソリューションと CISA モデルとの対応を示し、これらのソリューションがゼロトラスト戦略をどう進展させるかを解説します。

ゼロトラスト・セキュリティの現状を知る

ゼロトラスト・セキュリティでは、明示的な信頼性という前提に基づき、エンタープライズ・ネットワーク上のあらゆる活動を、どのデバイス、アプリケーション、ユーザーがどのリソースにアクセスするときでも完全に可視化し、制御します。このアプローチでは、ネットワーク・ロケーションに対する暗黙的な信頼を排除し、その代わりに、リソースへのアクセスを許可する前に必ず要求者のセキュリティ・ポスチャを継続的に監視および評価します。このプロセス中に悪意ある行為が検出された場合は、安全を守るために、迅速な対応を行います。

ゼロトラストはきわめて合理的な考え方ですが、いざ実装しようとすると難しい課題があります。初期の頃は、「ゼロトラスト」と名の付く製品やソリューションを購入するのが主流でした。そうなったのは主に、「ゼロトラストのワンストップ・ソリューション」をうたう各ベンダーのマーケティングの結果です。最近では、ゼロトラストはむしろ ID、データ、ワークロード、デバイス、ネットワークなど複数の領域に関わる戦略であることが広く理解されるようになっています。取り扱う範囲の広さから、ゼロトラストは非常に難しいものという印象がありますが、この 2～3 年で次のような進展が見られています。

- 従業員と関係者のトレーニング。多くの組織が、従業員向けの基本的なセキュリティ意識向上トレーニングを導入しています。これにはたとえば、フィッシング詐欺やソーシャル・エンジニアリングの手口を見分ける方法や、従業員のパスワードの「衛生状態」を守る方法、機密データを扱う際は暗号化を用いる、といった基本ルールが含まれます。
- 多要素認証（MFA）の実装。業界の統計[2]によれば、80%を超える組織が何らかの形で MFA を実装しています。MFA がリスク軽減に役立つことが明らかになるにつれ、この数字は年々増え続けています。
- 最小アクセス権の原則の適用。MFA とも密に関係しますが、この原則はまだそれほど多くの組織で実装されていません。最小アクセス権の原則を適用すると、従来のアプリケーションやデータ・アクセスのニーズに応えられなくなる場合が多いためです。
- 重要なアセットの特定（デバイスやデータ・ストアなど）。多くの組織は、保護すべき対象を認識しています。ただ、キャンパス、データセンター、クラウドにまたがる今日の複雑な IT 環境の中で、保護すべきデータがどこにあるかを詳しく把握することは困難です。

[1] https://en.wikipedia.org/wiki/Zero_trust_security_model
[2] https://www.watchguard.com/wgrd-resource-center/infographic/state-password-security

- セキュリティ・ポスチャの定期的な評価。さまざまな組織が、侵入テストや侵害評価を定期的に実施しています。ただ、攻撃対象領域全体のセキュリティを理解し、評価することには苦戦しています。IoT、サプライチェーン、契約業者、クラウドベースのインフラを利用している組織では、特に難易度が高まります。
- エンドポイントとネットワークに対するセキュリティ・コントロールの導入。エンドポイント脅威検知・対応（EDR）が一般化し、基本レベル以上のアンチウイルス機能を含むエンドポイント保護プラットフォーム（EPP）と統合される例が増えています。同様に、多くの組織はネットワーク上に境界ファイアウォールや IDS/IPS を導入しています。さらに進んで、ネットワーク脅威検知・対応（NDR）ソリューションを展開する組織も現れています。

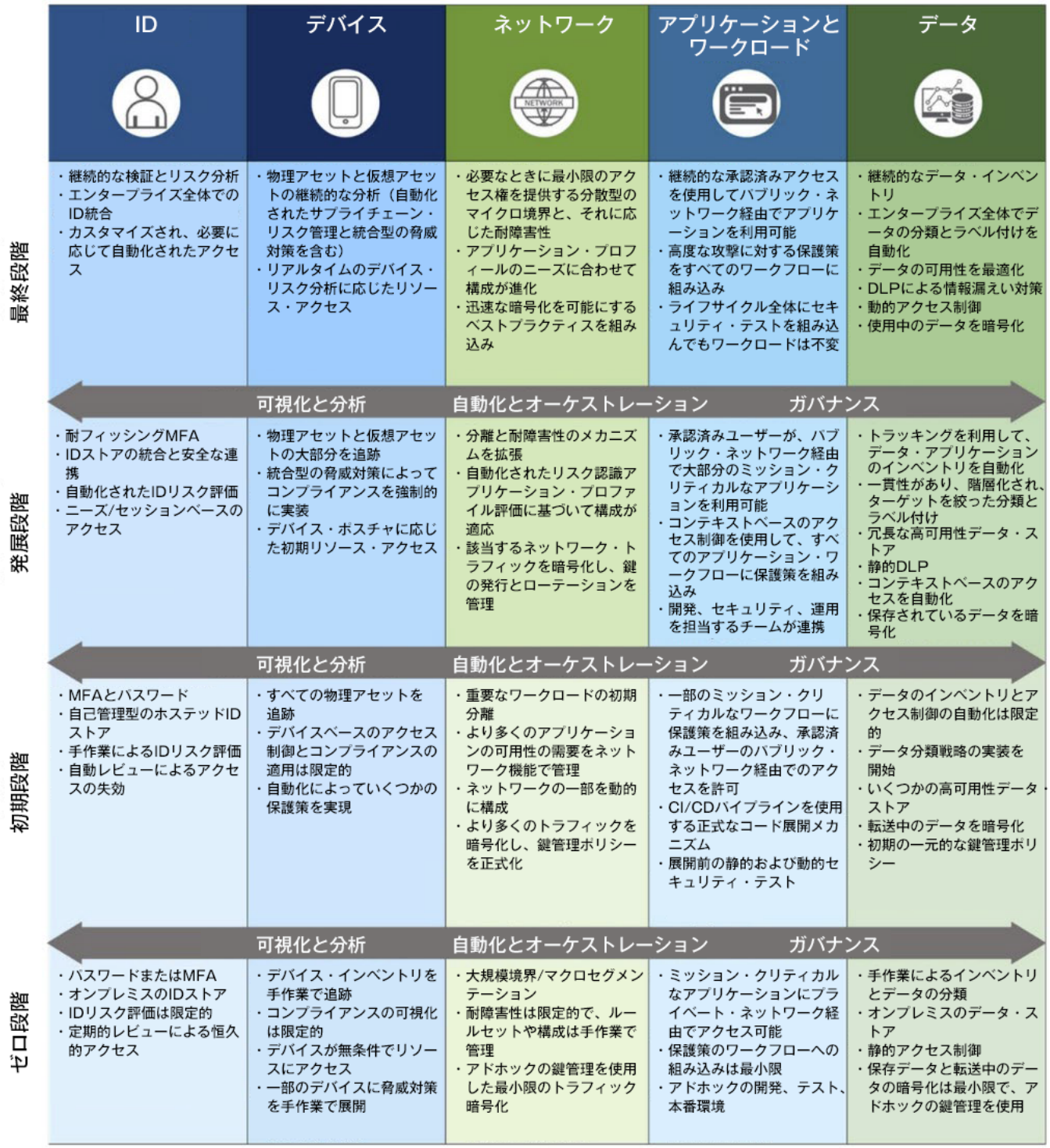
しかし、それで十分でしょうか。上記のことに取り組んでいれば、ゼロトラストを達成したと本当に主張できるでしょうか。ご想像のとおり、そうとは言い切れません。ここで理解に役立つのが、ゼロトラスト戦略の成熟度という考え方です。

ゼロトラスト成熟度モデル

米国のサイバーセキュリティおよびインフラストラクチャ・セキュリティ庁（CISA）[3]は、自らを「米連邦のサイバーセキュリティに関する作戦指揮官であり、重要なインフラのセキュリティと耐障害性に関する国家調整官」と定義しています。2018 年に設立されたこの機関は、民間の組織と公的な組織を結び付ける一方で、サイバーセキュリティと物理セキュリティ、および耐障害性プログラムの策定を支援する情報やツールを提供しています。

2021 年に起きた Colonial Pipeline へのランサムウェア攻撃[4]をはじめ、世間を騒がせるセキュリティ侵害がいくつも発生したことで、サイバーセキュリティが改めて注目され、CISA がこのような攻撃のリスク軽減の舵取りをすることになりました。その結果生み出された素晴らしいツールの 1 つが、CISA のゼロトラスト成熟度モデルで、最新版が 2023 年 4 月に公開されています[5]。このドキュメントは、ゼロトラストへの移行に関する処方型ガイダンスを提供するもので、NIST などの組織が以前に作成したモデルを基盤としています。CISA のモデルは、最適なゼロトラストというゴールに向けて、徐々に前進していくことに重点を置いています。このモデルでは、「ID」、「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」の 5 つを基本の柱とし、それぞれについて、「可視化と分析」、「自動化とオーケストレーション」、「ガバナンス」に関する考慮事項を示しています（図 1）。

[3] https://www.cisa.gov/
[4] https://en.wikipedia.org/wiki/Colonial_Pipeline_cyberattack
[5] https://www.cisa.gov/sites/default/files/publications/CISA%2520Zero%2520Trust%2520Maturity%2520Model_Draft.pdf



アナリスト会社 Forrester も同様のアプローチを採用し、レポート「Gauge Your Zero Trust Maturity」[6]の中で、図 2 のようなモデルを提示しています。Forrester のモデルは 5 つのフェーズから成り[7]、それぞれ次のように定義されています。

[6] https://www.forrester.com/report/gauge-your-zero-trust-maturity/RES179008
[7] https://www.forrester.com/report/chart-your-course-to-zero-trust-intermediate/RES178999

- フェーズ 0：検出、分類、インベントリ化を行う
- フェーズ 1A：ID や宛先を管理する
- フェーズ 1B：あらゆるものを保護する
- フェーズ 2：アプリケーションへのゼロトラスト・アクセスを提供する
- フェーズ 3：侵害を想定して、可視性を向上させる
- フェーズ 4：自動化とオーケストレーションを行う
- フェーズ 5：ネットワークにゼロトラストを実装する

これらのフェーズの進捗状況に基づき、Forrester は成熟度レベルを初級、中級、上級と定義しています。このモデルでは、初級の成熟度レベルはゼロトラストではなく、「従来の標準的なサイバーセキュリティ・アーキテクチャを反映」しているにすぎません。Forrester の中級レベルに達した組織のみが、ゼロトラストに向かっていると見なされます。

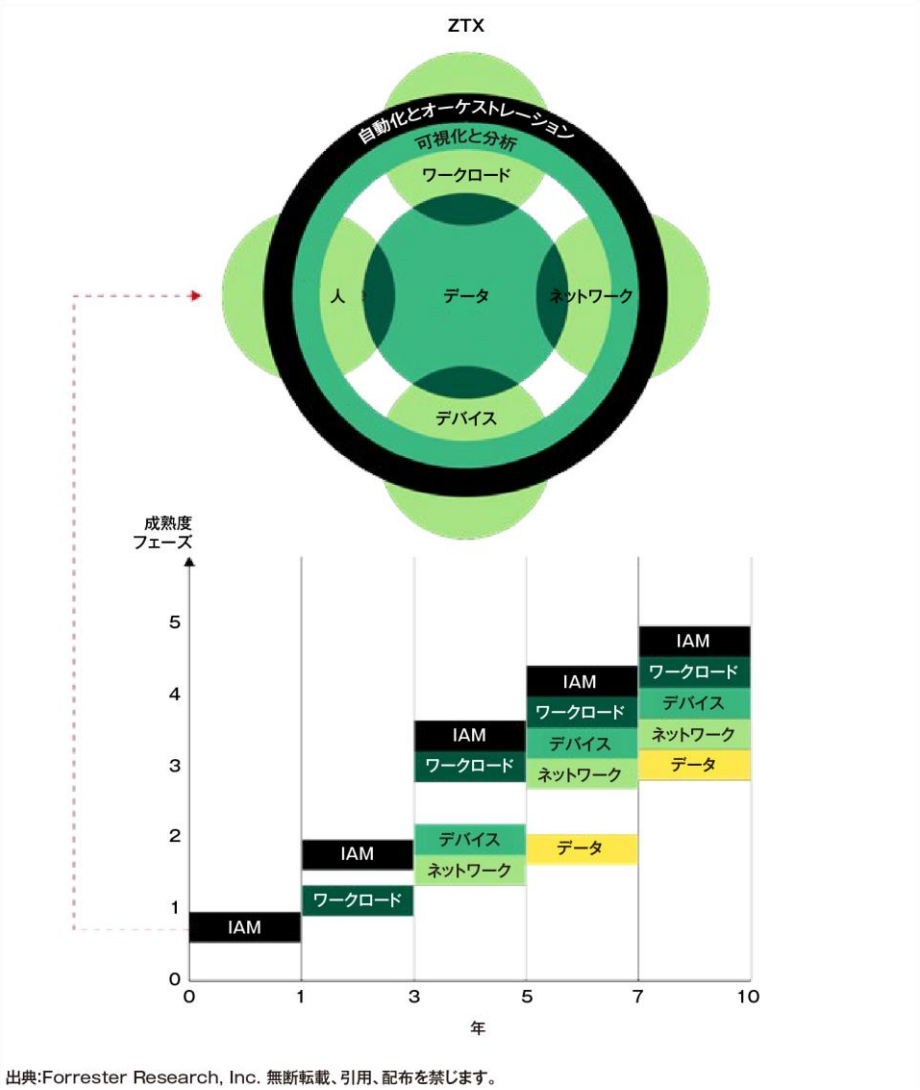


図 2：Forrester のゼロトラスト成熟度フェーズ

図 1 と図 2 からわかるとおり、Forrester のアプローチでは、CISA のモデル（図 3）とは異なり、それぞれの柱に取り組む順番が決まっていて、完成までに約 10 年を要します。実際に、Forrester は、ネットワークにゼロトラストを適用するのは最後にすることを推奨しており、その理由として、ネットワークのゼロトラスト化は複雑で、セキュリティ以外のビジネス・メリットがわかりにくい点を挙げています。さらに、ネットワークが組織の端まで広がっている状況では、ネットワークのゼロトラスト化を実現した後に、物事がうまくいかなくなるリスクが大いにあります。そしてもちろん、物事がうまくいかない場合には、すべてのゼロトラスト化の取り組みが大きく後退する可能性があります。

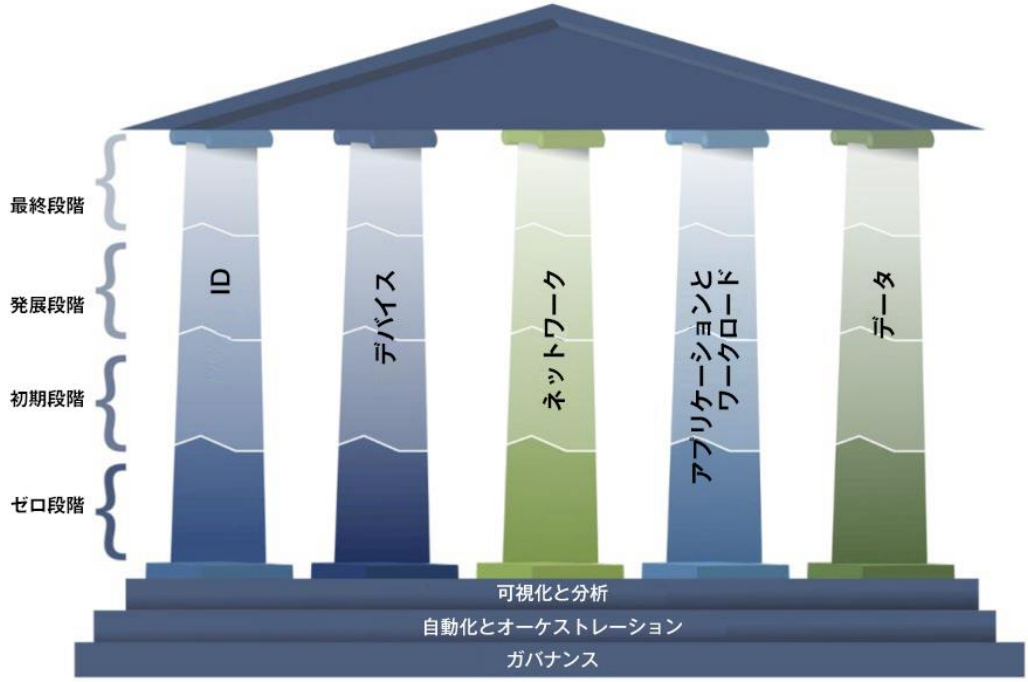


図 3：CISA のゼロトラスト成熟度の進み方

ゼロトラスト成熟度の課題

本ホワイトペーパーで説明するフレームワークは、ゼロトラスト戦略の進み具合を評価するのに役立ちます。お客様や業界の専門家と話をするなかで判明したのは、残念ながら、いまだ多くの組織が成熟度モデルの「ゼロ段階」または「初級」レベルにあるという点です。これはなぜでしょうか。

ゼロトラスト・セキュリティの実装はときに難しく、特にハード面での困難があります。多くの組織が以下のような障害にぶつかり、行き詰まっています。

- 既存のネットワーク、システム、アプリケーションの多くがビジネスに不可欠で、簡単には置き換えできません。さらに、最新の ID、データ保護、その他のセキュリティ・ソリューションとの統合が困難です。実際、こうしたアプリケーションの多くは「暗黙の信頼」という考えに基づいて設計、構築されたもので、ゼロトラストの原則とは相容れません。
- デバイス、アプリケーション、データ、ユーザーのインベントリ化は簡単そうに思われますが、IoT、BYOD、DevOps、シャドーIT が普及している現代では、多くの場合、これらのエンティティのうち構成管理データベースで追跡されているものは 50%以下にとどまります。しかも、これらを可視化するツールやプロセスがないため、「ベストエフォート型の検出」にならざるを得ません。
- データの保護と暗号化によって鍵管理が複雑化し、あらゆる場所で暗号化を行うことでパフォーマンスに影響が生じます。SMBv1 や HTTP のようなセキュアでない平文のプロトコルが広く普及している事実を見れば、強度が低い平文のプロトコルを組織環境から取り除くのがどれほど難しいことかがわかります。
- 人間の行動や抵抗がゼロトラスト化の障害になる場合もあります。考えてみれば、「そのままでは信頼しない」という方針を組織の従業員や関係者に適用するのは失礼な話に思われます。そのため、ゼロトラスト化を達成、成熟させるには企業文化を変える必要がありますが、これは簡単なことではありません。

ネットワークはゼロトラストのターゲットにしやすいと思われるかもしれませんが、前述のとおり、専門家はむしろ最後にネットワークに取り組むことを推奨しています。一体なぜでしょうか。その一因は、ネットワークの定義そのものが変化し、単にスイッチとルーターの集まりではなくなっている点にあります。現在では、大部分の組織のネットワークは、キャンパスやデータセンターからクラウド、オペレーショナル・テクノロジー（OT）や IoT まで、複数の領域にまたがっています。そして、ファイアウォール、セグメンテーション、ネットワーク・アクセス制御（NAC）、ネットワーク侵入検知などのネットワーク・セキュリティ・コントロールが出現してから数十年が経過しますが、これらの技術には次のような重大な欠点があります。

- セグメンテーションと NAC は、運用オーバーヘッドの増大や、独自のパケット形式の使用とベンダー・ロックインにつながることから、しばしば否定的に語られます。また、ベンダー・ソフトウェアの品質やオペレーターのミスにより、これらの技術が機能停止の原因になる場合もあります。
- ファイアウォールは高額で、管理のオーバーヘッドが大きいため、境界付近や DMZ 内など、特に価値が大きい場所でのみ使用されています。つまり、各所にマイクロ境界を構築するやり方には不適切です。
- ネットワークから収集したデータを一元的に分析することは、独自のデータ形式や、複数のコンソール、不十分な可視化といった要因により、引き続き課題となっています。
- ネットワーク脅威検知の中心技術は今でもパターン・マッチングや異常検知です。どちらも偽陽性や偽陰性を生じる可能性が高く、運用上のオーバーヘッドや、表に現れない、軽減できないリスクを組織にもたらします。

ゼロトラストの成熟を早めるには

そうは言っても、10 年かけてゼロトラストを成熟させるやり方に素直に従ってよいものかという疑問は生じます。もっと他に良い方法はないのでしょうか。アリスタは、あると考えています。ポイントは、まずネットワークを中心に据えてゼロトラスト戦略を進めることです。

まずはネットワークから

ネットワークのゼロトラスト化にリスクがあることは前述のとおりです。それなのに、なぜネットワークから始めるのでしょうか。ネットワーク中心のアプローチには、以下のメリットがあります。

- ネットワークは広範囲をカバーします。すべての通信がどこかの時点でネットワークに達するので、可観測性、脅威検知、アクセス制御を透過的に実現できます。これにより、簡単には「ゼロトラスト化」できない従来のデバイス、ワークロード、データ・ストアのリスクを軽減できます。ネットワークのゼロトラスト化を実現すれば、全体的なゼロトラストの取り組みをスピードアップさせ、データやワークロードといった他の領域のより困難な課題に対処するための時間を稼ぐことができます。
- ネットワークは、デバイスが管理対象か、管理対象外かを区別しません。その代わりに、個々のデバイスを特定し、どのような種類のどこにあるデバイスにも認証と承認のポリシーを適用できます。
- ネットワークは、デバイス、ワークロード、ユーザー、データなどよりはるかに同質です。TCP/IP などのプロトコルは汎用的であり、複雑さを伴う各種オペレーティング・システムやアプリケーション・サーバー・ソフトウェアとは異なります。

もちろん、ネットワークの盲点を指摘して反論する人もいるでしょう。たとえば、ネットワーク・トラフィックをバックホールせず、インターネットに直接ルーティングするリモート・エンドポイントやブランチなどの存在です。これらの仕組みは組織の従来のネットワークに達しない場合があるので、組織のゼロトラスト・コントロールで検出できない可能性があります。そのため、ゼロトラスト・ネットワーキング・アーキテクチャを実装する際には、エンドポイント脅威検知・対応やゼロトラスト・ネットワーク・アクセス・テクノロジーのような補完ソリューションとの密な連携を含めることが必要です。

マイクロ境界の活用

ネットワークのゼロトラスト化とは、具体的にはどのような状態を指すのでしょうか。CISA はその成熟度モデル（図 1）の中で、数多くの処方型ガイダンスを提供しています。さらに CISA は、特に重要なネットワーク・コントロールについて説明するとともに、可視化と分析、自動化とオーケストレーション、ガバナンスに関する主なネットワーク機能についても触れています（図 4）。

機能	ゼロ段階	初期段階	発展段階	最終段階
ネットワーク・セグメンテーション	大規模境界 / マクロセグメンテーションを使用してネットワーク・アーキテクチャを定義。ネットワーク・セグメント内での到達可能性に対する制約は最小限。 マルチサービス相互接続（一括トラフィックの VPN トンネルなど）を利用することもできる。	ネットワーク・アーキテクチャの展開を開始。重要なワークロードを分離し、最小機能の原則に従って接続を制約し、サービス固有の相互接続に移行する。	エンドポイントとアプリケーション・プロファイルの分離メカニズムの展開をさらに多くのネットワーク・アーキテクチャに拡張。イングレス/イグレス・マイクロ境界とサービス固有の相互接続を利用する。	ネットワーク・アーキテクチャは、完全分散型のイングレス/イグレス・マイクロ境界と、アプリケーション・プロファイルに基づく広範なマイクロセグメンテーションで構成されている。サービス固有の相互接続に対し、必要最低限の接続を必要なときに動的に提供する。
ネットワーク・トラフィック管理（新機能）	静的なネットワーク・ルールと構成を手作業で実装し、サービス・プロビジョニング時にトラフィックを管理する。監視機能（アプリケーション・パフォーマンス監視や異常検知など）は限定的で、ミッション・クリティカルなアプリケーションのプロファイル変更の監査とレビューは手作業。	独自のトラフィック管理機能でアプリケーション・プロファイルを作成。すべてのアプリケーションとプロファイルのマッピングを開始する。 静的ルールの適用をすべてのアプリケーションに拡張。アプリケーション・プロファイル評価の監査を手作業で定期的に実行する。	リソース最適化のために、動的なネットワーク・ルールと構成を実装。自動的にリスクを認識し、対応するアプリケーション・プロファイルの評価と監視に基づいて、定期的に適応させる。	動的なネットワーク・ルールと構成を実装し、継続的に変化させて、アプリケーション・プロファイルのニーズを満たし、ミッション・クリティカリティやリスクなどに基づいてアプリケーションの優先順位を付け直す。
トラフィック暗号化（旧称は暗号化）	最小限のトラフィックを暗号化し、手作業またはアドホックのプロセスを利用して暗号化鍵を管理し、保護する。	内部アプリケーション宛てのすべてのトラフィックの暗号化、外部アプリケーション[27]宛てのトラフィックの選択的な暗号化、鍵管理ポリシーの正式な承認、サーバー / サービス暗号化鍵の保護を開始する。	該当するすべての内部 / 外部トラフィック・プロトコル[28]を暗号化し、鍵と証明書の発行とローテーションを管理し、暗号アジリティのベストプラクティスの組み込みを開始する。[29]	必要に応じてトラフィックの暗号化を継続し、セキュアな鍵管理に関する最小権限の原則をエンタープライズ全体に適用し、できる限り広範に暗号アジリティのベストプラクティスを組み込む。
ネットワーク耐障害性（新機能）	個々のアプリケーションの可用性の需要にのみ合わせて、ケースバイケースでネットワーク機能を構成する。ミッション・クリティカルと見なされないワークロードの耐障害性メカニズムは限定的。	その他のアプリケーションの可用性の需要を管理するネットワーク機能の構成や、ミッション・クリティカルと見なされないワークロードの耐障害性メカニズムの拡張を開始する。	大半のアプリケーションについて、可用性の需要と耐障害性のメカニズムを動的に管理するよう、ネットワーク機能を構成。	包括的なデリバリと認識を組み込んで、すべてのワークロードの可用性の需要の変化に適応し、それに応じた耐障害性を提供する。
可視化および分析機能	境界に重点を置いた限定的なネットワーク監視機能と最小限の分析を組み合わせ、一元的な状況認識の開発を始める。	既知の侵害インジケーターに基づくネットワーク監視機能（ネットワーク列挙を含む）を使用して、環境ごとの状況認識を開発する。分析や脅威ハンティング活動のために、さまざまなトラフィック・タイプと環境にまたがるテレメトリの相関付けを開始する。	異常ベースのネットワーク脅威検出機能を展開して、すべての環境にまたがる状況認識を開発する。分析のため、複数ソースからのテレメトリの相関付けを開始。強力な脅威ハンティング活動のための自動化プロセスを組み込む。	組織のすべてのネットワークと環境の通信を可視化すると同時に、エンタープライズ全体での状況認識と高度な監視機能を実現し、すべての検出ソースにまたがるテレメトリの相関付けを自動化する。
自動化およびオーケストレーション機能	手作業のプロセスで、組織のネットワークと環境の構成とリソースのライフサイクルを管理する。ポリシー要件と状況認識を定期的に統合する。	自動化手法を利用して、組織のネットワークまたは環境の一部の構成とリソースのライフサイクルの管理を開始する。すべてのリソースの使用期間がポリシーとテレメトリに基づいて定義されていることを保証する。	自動化された変更管理手法（CI/CD など）を利用して、組織のネットワークと環境のすべての構成とリソースのライフサイクルを管理し、認識されたリスクに対応して、ポリシーや保護策を適用する。	変化するニーズに合わせた自動開始や失効など、自動化された変更管理手法で管理する Infrastructure as Code を使用して、ネットワークと環境を定義する。
ガバナンス機能	境界の保護に重点を置いたアプローチで、静的ネットワーク・ポリシー（アクセス、プロトコル、セグメンテーション、アラート、修復）を実装する。	個々のネットワーク・セグメントとリソースに合わせてカスタマイズされたポリシーを定義し、実装を開始すると同時に、必要に応じて全社規模のルールも継承する。	カスタマイズされたポリシーの実装に自動化を組み込み、境界に重点を置いた保護策からの移行を促進する。	エンタープライズ全体にネットワーク・ポリシーを実装し、カスタマイズされたローカルなコントロール、動的なアップデート、アプリケーションとユーザー・ワークフローに基づくセキュアな外部接続を実現する。

図 4：CISA のゼロトラスト成熟度モデル（ネットワーク機能）

このセクションでは、図 4 の各機能について検討し、利用可能なアプローチと関連する課題について取り上げます。

ネットワーク・セグメンテーション

現代の組織の多くは、セグメント化の際に、VLAN やファイアウォールなどに基づく大まかなマクロセグメンテーションを用います。この手法では、ネットワークをビジネス・ニーズに基づいて分割します。よくある例としては、DMZ、開発環境と本番環境の分離、異なる機能ユニットの分離（財務ネットワークから人事部門を切り離すなど）が挙げられます。CISA のガイダンスでは、各組織に対し、マイクロ境界に移行してゼロトラスト・ポスチャを強化し、セグメンテーションをできる限りワークロードやデータ・ストアに近づけることを推奨しています。さらに、このアプローチでは、アプリケーションのワークフロー内で逸脱を自動的に学習、適用、検出する必要があります。

マイクロセグメンテーション・ソリューションは近年人気を博しており、仮想ホスト型環境で効果的に利用されています。ベアメタル・ワークロードの場合は、サーバーにエージェントをインストールする必要があり、オペレーティング・システムとアプリケーションの互換性、潜在的なパフォーマンスの問題、エージェントの保守の負担といった課題が出てきます。

ネットワーク・トラフィック管理

CISA の成熟度モデルにおけるこの機能の要点は、ネットワーク・トラフィックを監視し、異常を特定し、トラフィック・パターンが変化した場合に監査する能力です。組織の成熟度レベルがゼロ段階から最終段階に上がると、これらの機能の多くは、監視に対するリスク認識アプローチをもとに自動化され、自己学習型になります。多くの組織は、これらの機能を実行するのにネットワークまたはアプリケーション・パフォーマンス管理ツールを使用していましたが、ほとんどの場合、この取り組みにはミッション・クリティカリティ、リスク、組織への影響についてのコンテキストが不足しています。さらに、アラートが依存する異常検知はかなりの量のノイズを生み出す可能性があるので、結果としてフィルターで除外されたり、完全に無視されたりすることもあります。

トラフィック暗号化

ゼロトラスト成熟度の最終段階の目標は、組織と外部を結ぶ垂直方向のトラフィックと、組織内部の水平方向のトラフィックの両方で、転送中のすべてのデータを暗号化することです。現在、ほとんどの組織は、この機能を Web アプリケーションに組み込む際に TLS を使用しています。SSH などのプロトコルも一般的です。しかし、前述のとおり、従来のアプリケーション、特にカスタムのポートとプロトコルを使用するアプリケーションに暗号化を組み込むことは困難です。また、多くの場合、組織が利用できる補完コントロールも、こうしたアプリケーションでやり取りされるトラフィックをセグメント内に分離し、平文のトラフィックを閲覧できる人を最小限に抑えることくらいです。それでも、平文のシークレットとパスワードは、あらゆる組織で広範に利用されてきました。さらに、暗号化を広く採用している組織でさえ、鍵管理や暗号化のベストプラクティスなど、いくつかの根本的な要素に悩まされています。

ネットワーク耐障害性

ネットワーク耐障害性とは、その名前が示すとおり、組織のビジネスクリティカルなネットワーク機能に対するアクセスを提供および保守するための機能です。組織の成熟度が高まるにつれて、このプロセスの大部分は自動化され、変化する可用性の需要に自動で適応するようになります。また、耐障害性のあるネットワークは、脅威や、可用性に影響を与えるその他のイベントから自動的に回復できます。最後に、本セクションで説明する他の機能と同様に、この機能はコンテキスト対応でなければならず、アプリケーションやワークロードの重要性に応じて調整可能です。

可視化および分析機能

可視化と分析について、CISA はまず境界センサーからアグリゲーションと分析を一元化することを推奨しています。ただし、最終的な目標は、ネットワーク全体の境界センサーが状態の変化や脅威の可能性をオペレーターに自動的に警告できるようにすることです。現在の多様化したネットワークでは、組織はネットワーク・センサーからのテレメトリについて自動分析や脅威分析を行えるようになるどころか、「ネットワーク上に何があるか」といった簡単な質問に答えるのにも四苦八苦しています。　そのため、大部分の組織はやむをえず、限られたセンサーからの SNMP ポーリングやネットワーク・ログ監視、あるいは複数のコンソールからデータを取得してアナリストが手作業で分析する古い手法を利用しています。こうした可視化の難しさが、ネットワークのゼロトラスト化の先延ばしを専門家が推奨する唯一最大の理由であるとアリスタは考えています。

脅威対策の観点から言うと、CISA の成熟度は、既知の脅威を特定する純粋な境界ベースの、昔ながらのシグネチャ型アプローチから、非マルウェア攻撃やネットワーク深部の内部脅威を検出する機械学習ベースのソリューションへと進んでいきます。このような新しい AI ベースのサービスは、ネットワーク経由でやり取りする各エンティティの背後にあるコンテキストとアクティビティを理解して、エンティティをクラスタ化し、異常値を特定することができます。これらのソリューションは、コンテキストや説明性を提供し、リスク軽減に大きな影響をもたらします。これにより、アナリストの生産性が向上し、セキュリティ・チームとネットワーク・チームの運用オーバーヘッドが減少します。

自動化およびオーケストレーション機能

現在、ネットワークの変更の自動化とオーケストレーションがあまり実装されていないのは、基盤となるインフラが脆弱なためです。成熟した組織の多くは、明示的な変更管理のワークフローを備えていますが、ほとんどは手動でトリガーする必要があります。一方で、CISA は IaC（Infrastructure as Code）のパラダイムで機能する広範な自動化を推奨し、ソフトウェア開発者の間で人気の CI/CD（Continuous Integration/Continuous Deployment）プロセスを利用しています。

ガバナンス機能

ガバナンスでは、誰にネットワーク接続を許可するかと、接続にどのような行動を許可するかが重要です。攻撃対象領域は拡大する一方で、組織の対応はますます難しくなっています。そのため、この領域における成熟度は、許可されたネットワーク、デバイス、サービスを手動で認識するプロセスから、これらのエンティティの検出やポリシー適用を完全に自動化する方向へと進みます。同様に、このプロセス中に発見された不正エンティティに対し、必要に応じて隔離または分離措置を行うネットワーク・ポリシーを定義して、修復処理を自動化する必要があります。多くの組織は、IP 利用デバイスを発見するためにネットワークの定期的な自動スキャンを実行していますが、この方法では、リアルタイムのビューや、修復の自動化に必要なコンテキストは得られません。そのため、IP の「向こう側」についての調査は人間のオペレーターが行うことになります。この調査は通常、数日から数週間かかり、組織のさまざまな部門の関与が必要になります。

アリスタがゼロトラストの成熟を後押し

アリスタは、ネットワーク上に既に展開されている基盤インフラを利用して、あらゆる規模の組織をゼロトラスト成熟度の最終段階へと迅速に誘導します。Arista Extensible Operating System（EOS®）は、アリスタのネットワーキング・ソリューションの中核をなすもので、次世代のデータセンター、キャンパス、クラウド・ネットワークを支えます。Arista EOS を利用して構築されたネットワークは、数十万ノードへと拡張可能で、大規模に動作する管理機能とプロビジョニング機能を備えています。EOS の優れたプログラマビリティを通じてさまざまなソフトウェア・アプリケーションを利用し、ワークフローの自動化、高可用性、これまでにないネットワーク可視化、セキュリティ、分析を可能にしたり、仮想化、管理、自動化、オーケストレーションのサービスを提供する幅広いサードパーティ・アプリケーションとのスピーディな連携を実現したりできます。

EOS Network Data Lake（NetDL）は、EOS のコアであるパブリッシュ/サブスクライブ状態機能を基盤として構築されたデータ・レイクで、ネットワーク・データソース向けのデータ・ストアと分析機能（アラート、フロー、フル・パケット・キャプチャ、コントロール・プレーン・トラフィック、デバイス状態ストリーミングなど）に加え、サードパーティ・データや外部データとの連携機能を備えています。このため、さまざまなアプリケーションがこのデータセットを使って処理や分析を行い、運用に関するインサイトや予測を導き出すことができます（図 5）。

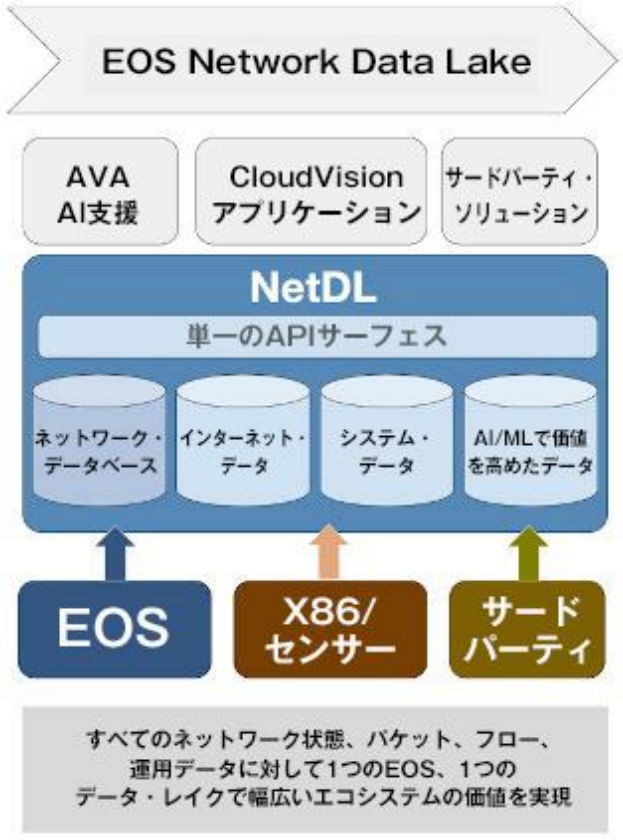


図 5：アリスタの EOS と NetDL のアーキテクチャ

NetDL は、信頼できる唯一のネットワーク・データソースと共通のセンサー/コレクター・アーキテクチャを提供し、脅威ハンティング、ネットワーク・パケット・ブローカー、ネットワーク脅威検出・対応、アプリケーション・パフォーマンス監視に必要なフォレンジックと分析を可能にします。さまざまな業界リーダーと協力することで、アリスタは本番環境において顧客に大きなメリットを提供できます。これらのデータ・ドリブン型ネットワーク・モデルは、アクションにつながる運用成果をもたらすインサイトに変換することができます。

Arista Autonomous Virtual Assist（Arista AVA™）は、機械学習や他の AI テクノロジーを利用して、広範な可視化、継続的な脅威検知、セグメンテーション、アクセス制御のあらゆる要素を強化します。AVA は多種多様な運用ユースケースに拡張可能です。たとえば、ネットワーク脅威検出・対応、エクスペリエンス品質管理、プロアクティブな NetOps、ネットワーク・アクセス制御の課題に対処できます。NetDL 内にある分散ネットワーク全体の状態およびテレメトリ・データ、分散センサー・ネットワーク、サードパーティのデータ・ソースと組み合わせることで、ネットワーク・デザインの自動化と拡張性をこれまでにない新たなレベルに向上させるとともに、手動で行われるネットワークの保護とサポートの負担を大幅に削減できます。

これらのコア・テクノロジーで構成される基盤が、一連の機能の相互連携を可能にし、アリスタのゼロトラスト・ネットワーキング・ソリューションを形成します（図 6）。

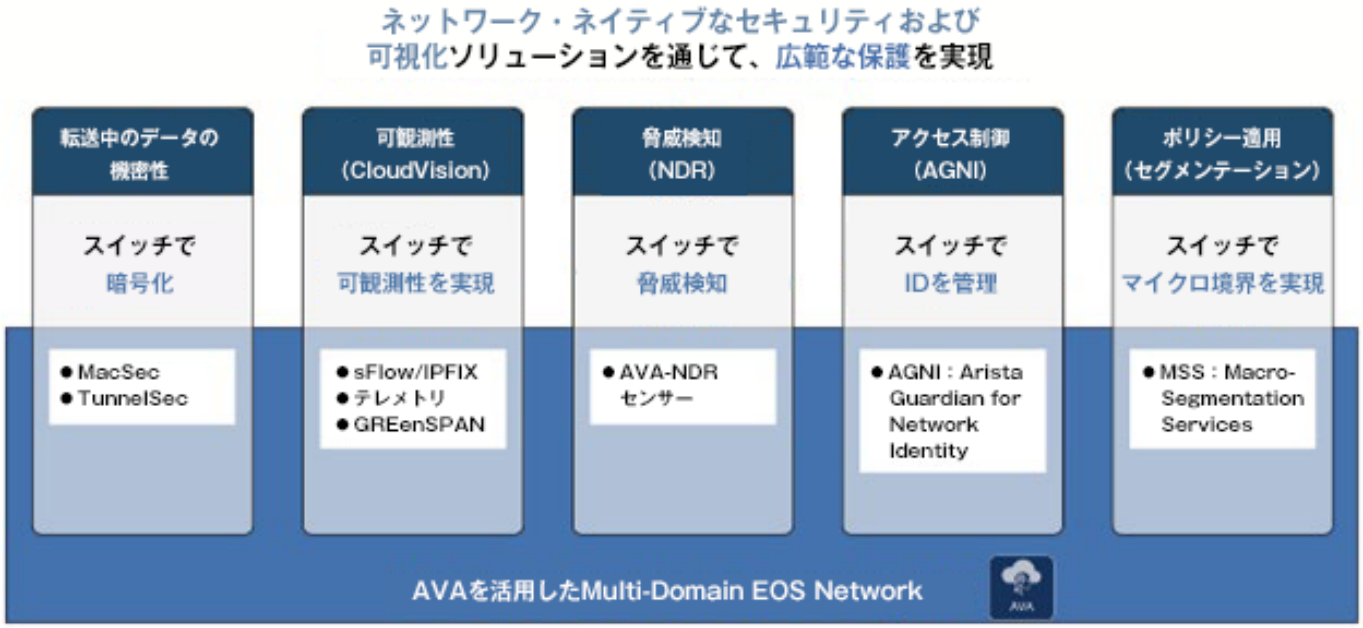


図 6：アリスタのゼロトラスト・ネットワーキング・ソリューション

以下のセクションでは、アリスタのサービスと CISA のゼロトラスト成熟度モデルのネットワーク機能がどのように対応しているかと、そのサービスが組織を成熟度の最終段階にどのように推し進めるかを説明します。

ネットワーク・セグメンテーション

機能	ゼロ段階	初期段階	発展段階	最終段階
ネットワーク・セグメンテーション	大規模境界 / マクロセグメンテーションを使用してネットワーク・アーキテクチャを定義。ネットワーク・セグメント内での到達可能性に対する制約は最小限。 マルチサービス相互接続（一括トラフィックの VPN トンネルなど）を利用することもできる。	ネットワーク・アーキテクチャの展開を開始。重要なワークロードを分離し、最小機能の原則に従って接続を制約し、サービス固有の相互接続に移行する。	エンドポイントとアプリケーション・プロファイルの分離メカニズムの展開をさらに多くのネットワーク・アーキテクチャに拡張。イングレス/イグレス・マイクロ境界とサービス固有の相互接続を利用する。	ネットワーク・アーキテクチャは、完全分散型のイングレス/イグレス・マイクロ境界と、アプリケーション・プロファイルに基づく広範なマイクロセグメンテーションで構成されている。サービス固有の相互接続に対し、必要最低限の接続を必要なときに動的に提供する。

図 7：CISA のゼロトラスト成熟度（ネットワーク・セグメンテーション機能）

アリスタの Macro-Segmentation Services（MSS）を利用すると、エッジ・スイッチを通じてマイクロ境界を作成し、キャンパス・ネットワークに追加のファイアウォールを展開することなく、各アセットを個別に保護または分離できます。Arista MSS は、VRF、VXLAN、PACL など従来のモデルを引き続きサポートしつつ、最先端のセグメンテーション・オプションを提供します。MSS-Group は、認証ポリシーをインターフェイスやサブネット、物理ポートではなく、セキュリティ・セグメント・グループに適用します。これらのグループはアプリケーション・ワークフローを中心に作成され、管理者が CloudVision 内で定義したポリシーを使用して、セグメント間およびセグメント内のグループの通信を制御できます。

またアリスタは、DMZ エッジ、データセンター、キャンパスのネットワークをまたぐ柔軟なファイアウォール・ポリシーの配置を通じて、セグメンテーションをサポートします。さらに、ステートフル・インスペクション・メカニズムと論理ゾーン分類を利用して、セキュリティ・ポリシーを仮想ワークロードやクラウド・ワークロードに広げることもできます。特に強調したいのは、この機能が特定のクラウドに依存せず、Amazon Web Services、Microsoft Azure、Google Cloud Platform などのあらゆるクラウド・ネットワークで一貫性をもって動作することです。

ネットワーク・トラフィック管理

機能	ゼロ段階	初期段階	発展段階	最終段階
ネットワーク・トラフィック管理（新機能）	静的なネットワーク・ルールと構成を手作業で実装し、サービス・プロビジョニング時にトラフィックを管理する。監視機能（アプリケーション・パフォーマンス監視や異常検知など）は限定的で、ミッション・クリティカルなアプリケーションのプロファイル変更の監査とレビューは手作業。	独自のトラフィック管理機能でアプリケーション・プロファイルを作成。すべてのアプリケーションとプロファイルのマッピングを開始する。 静的ルールの適用をすべてのアプリケーションに拡張。 アプリケーション・プロファイル評価の監査を手作業で定期的に実行する。	リソース最適化のために、動的なネットワーク・ルールと構成を実装。自動的にリスクを認識し、対応するアプリケーション・プロファイルの評価と監視に基づいて、定期的に適応させる。	動的なネットワーク・ルールと構成を実装し、継続的に変化させて、アプリケーション・プロファイルのニーズを満たし、ミッション・クリティカリティやリスクなどに基づいてアプリケーションの優先順位を付け直す。

図 8：CISA のゼロトラスト成熟度（ネットワーク・トラフィック管理機能）

ネットワーク・トラフィック管理機能に求められるのは、まずアプリケーションを特定してから、最適なユーザー・エクスペリエンスに合わせて分類する能力です。この機能は、サービス品質や帯域幅の予約と、きめ細かな監視ポリシーを通じて実現されます。Arista EOS は、強力なサービス品質機能に加えて、他のアプリケーションとの比較で、ネットワーク内の適切な優先度に合わせてトラフィックを分類する機能を提供します。Arista DANZ Monitoring Fabric（DMF）[8]を利用することで、IT オペレーターは物理環境、仮想環境、コンテナ環境の完全な可視化を実現し、すべてのユーザー、デバイス/IOT、アプリケーションのトラフィック（垂直型および水平型）を広範囲にわたって監視できます。ホップ・バイ・ホップの詳細な可視化、予測分析、スケールアウト型のパケット・キャプチャが 1 つのダッシュボードに統合されているため、これまでに類を見ない可観測性を実現し、ネットワークとアプリケーションのパフォーマンスの問題を監視、検出、トラブルシューティングできるだけでなく、セキュリティ侵害や他の障害の根本原因の検出をスピードアップできます。

トラフィック暗号化

機能	ゼロ段階	初期段階	発展段階	最終段階
トラフィック暗号化（旧称は暗号化）	最小限のトラフィックを暗号化し、手作業またはアドホックのプロセスを利用して暗号化鍵を管理し、保護する。	内部アプリケーション宛てのすべてのトラフィックの暗号化、外部アプリケーション[27]宛てのトラフィックの選択的な暗号化、鍵管理ポリシーの正式な承認、サーバー / サービス暗号化鍵の保護を開始する。	該当するすべての内部 / 外部トラフィック・プロトコル[28]を暗号化し、鍵と証明書の発行とローテーションを管理し、暗号アジリティのベストプラクティスの組み込みを開始する。[29]	必要に応じてトラフィックの暗号化を継続し、セキュアな鍵管理に関する最小権限の原則をエンタープライズ全体に適用し、できる限り広範に暗号アジリティのベストプラクティスを組み込む。

図 9：CISA のゼロトラスト成熟度（トラフィック暗号化機能）

[8] https://www.arista.com/en/products/danz-monitoring-fabric

アリスタのネットワーク・インフラは、MACsec や TunnelSec などの暗号化機能をネイティブにサポートします。スイッチに実装されているこれらの機能を利用して、従来のアプリケーションやワークロードとの間でやり取りされるデータを暗号化できます。従来のシステムを変更する必要はなく、代わりにネットワークを利用して、不正アクセス、傍受、改ざんからデータを保護します。

TunnelSec は、IPSec や SSL/TLS など業界標準のプロトコルを使用して、パブリック・インターネットを含む、あらゆるネットワークでセキュアなトンネルを確立し、リモート・ロケーション間のセキュアな通信やデータ交換を実現できます。支店やデータセンターが複数あり、パブリック・ネットワーク経由でセキュアに通信する必要がある組織にとって、この機能は特に有効です。

MACsec はネットワーク・スタックのリンク・レイヤで動作し、キャンパスまたはデータセンターのネットワーク・デバイス間でのデータ暗号化を提供します。MACsec は、データセンター内など同じ物理ネットワーク上にあるデバイス間のセキュアな通信に使用されます。

ネットワーク耐障害性

機能	ゼロ段階	初期段階	発展段階	最終段階
ネットワーク耐障害性（新機能）	個々のアプリケーションの可用性の需要にのみ合わせて、ケースバイケースでネットワーク機能を構成する。ミッション・クリティカルと見なされないワークロードの耐障害性メカニズムは限定的。	その他のアプリケーションの可用性の需要を管理するネットワーク機能の構成や、ミッション・クリティカルと見なされないワークロードの耐障害性メカニズムの拡張を開始する。	大半のアプリケーションについて、可用性の需要と耐障害性のメカニズムを動的に管理するよう、ネットワーク機能を構成。	包括的なデリバリと認識を組み込んで、すべてのワークロードの可用性の需要の変化に適応し、それに応じた耐障害性を提供する。

図 10：CISA のゼロトラスト成熟度（ネットワーク耐障害性機能）

Arista EOS と CloudVision[9]は、継続的なアプリケーション・デリバリと優れたパフォーマンスを実現するための最新のアプローチです。ゼロトラストのコンテキストで耐障害性の鍵となるのは、ネットワークの需要に応じて動的に拡張または縮小する機能です。これはたとえば、需要が増えているときや、可用性が脅かされているときに、ユーティリティ・クラウドの枠を広げて利用することを指します。同様に、ネットワーク運用で障害復旧サイトやバックアップ・データセンターのキャパシティを利用することもできます。アリスタの Cloud Vision と EOS は連携して、あらゆるパブリック・ユーティリティ・クラウドに動的なオンボーディングと接続をセキュアに提供し、パフォーマンスを最適化します。多くの場合、この機能のゼロトラスト成熟度を高めようとする組織は、EVPN などの強力な EOS 機能を利用して、アクティブ/アクティブ構成のデータセンターを展開します。これにより、キャパシティ全体を単一の仮想データセンターとして提供しながら、地域固有のフォールト・トレランスを実現します。そして CloudVision は、従来のデータセンターとハイブリッド・クラウドの両方に一元的な管理機能を提供します。

可視化および分析機能

機能	ゼロ段階	初期段階	発展段階	最終段階
可視化および分析機能	境界に重点を置いた限定的なネットワーク監視機能と最小限の分析を組み合わせ、一元的な状況認識の開発を始める。	既知の侵害インジケーターに基づくネットワーク監視機能（ネットワーク列挙を含む）を使用して、環境ごとの状況認識を開発する。分析や脅威ハンティング活動のために、さまざまなトラフィック・タイプと環境にまたがるテレメトリの相関付けを開始する。	異常ベースのネットワーク脅威検出機能を展開して、すべての環境にまたがる状況認識を開発する。分析のため、複数ソースからのテレメトリの相関付けを開始。強力な脅威ハンティング活動のための自動化プロセスを組み込む。	組織のすべてのネットワークと環境の通信を可視化すると同時に、エンタープライズ全体での状況認識と高度な監視機能を実現し、すべての検出ソースにまたがるテレメトリの相関付けを自動化する。

図 11：CISA のゼロトラスト成熟度（可視化および分析機能）

[9] https://www.arista.com/en/solutions/telemetry-analytics

Arista NDR[10]は AI 対応のプラットフォームで、数十億のネットワーク通信を分析して、新しいネットワーク（境界、コア、IoT、およびクラウドのネットワーク）に存在するすべてのデバイス、ユーザー、アプリケーションを自律的に検出し、プロファイル化と分類を行います。この攻撃対象領域に関する深い理解に基づいて、これらのエンティティを出入りする脅威を検出し、迅速な対応をするために必要なコンテキストを提供します。

Arista NDR は、既存の展開済みスイッチをネットワーク・セキュリティ・センサーとして利用し、エンタープライズ全体に可視化と分析機能を提供します。その結果、追加のネットワーク・タッピング・インフラやネットワーク可視化ソリューションを展開しなくても、既に展開済みのインフラを利用して、幅広い状況認識機能からメリットを得ることができます。これは、キャンパスまたはブランチ・ロケーションで特に重要です。このようなコンポーネントの展開や保守は、専用のラック・スペースやローカル IT に関する専門知識なしでは難しいことがあるからです。

自動化およびオーケストレーション機能

機能	ゼロ段階	初期段階	発展段階	最終段階
自動化および オーケストレーション機能	手作業のプロセスで、組織のネットワークと環境の構成とリソースのライフサイクルを管理する。ポリシー要件と状況認識を定期的に統合する。	自動化手法を利用して、組織のネットワークまたは環境の一部の構成とリソースのライフサイクルの管理を開始する。すべてのリソースの使用期間がポリシーとテレメトリに基づいて定義されていることを保証する。	自動化された変更管理手法（CI/CD など）を利用して、組織のネットワークと環境のすべての構成とリソースのライフサイクルを管理し、認識されたリスクに対応して、ポリシーや保護策を適用する。	変化するニーズに合わせた自動開始や失効など、自動化された変更管理手法で管理する Infrastructure as Code を使用して、ネットワークと環境を定義する。

図 12：CISA のゼロトラスト成熟度（自動化およびオーケストレーション機能）

Arista CI パイプライン[11]は、Arista CloudVision プラットフォームが提供する可視化を基盤として構築され、ネットワークとセキュリティの運用を管理する高度な CI 環境を提供します。この機能と、Arista Validated Designs（AVD）や、他の追加機能や連携を組み合わせることで、ネットワークおよびセキュリティ運用ワークフローの自動化を大幅に簡素化、強化できます。

ガバナンス機能

機能	ゼロ段階	初期段階	発展段階	最終段階
ガバナンス機能	境界の保護に重点を置いたアプローチで、静的ネットワーク・ポリシー（アクセス、プロトコル、セグメンテーション、アラート、修復）を実装する。	個々のネットワーク・セグメントとリソースに合わせてカスタマイズされたポリシーを定義し、実装を開始すると同時に、必要に応じて全社規模のルールも継承する。	カスタマイズされたポリシーの実装に自動化を組み込み、境界に重点を置いた保護策からの移行を促進する。	エンタープライズ全体にネットワーク・ポリシーを実装し、カスタマイズされたローカルなコントロール、動的なアップデート、アプリケーションとユーザー・ワークフローに基づくセキュアな外部接続を実現する。

図 13：CISA のゼロトラスト成熟度（ガバナンス機能）

CloudVision Arista Guardian for Network Identity™[12]（CV AGNI）は、SaaS 型のネットワーク・アクセス制御（NAC）ソリューションであり、有線および無線ネットワークのユーザー、関連デバイス、IoT のネットワーク ID に関するオンボーディングと継続的なガバナンスを簡素化します。CV AGNI は、Microsoft Azure AD や Okta といった既存の ID プロバイダーを利用して、効果的なゼロトラスト・アーキテクチャに不可欠な Policy Decision Point（PDP）と Policy Enforcement Point（PEP）の役割を果たします。CV AGNI は、Arista NDR のデータと、エンドポイント脅威検出・対応ソリューションなどのサードパーティ・テクノロジーに基づいたリアルタイムのポスチャ評価を利用して、動的な承認を実行します。この評価と組織が定義したポリシーに基づいて、承認されなかったエンティティやセキュリティ・ポリシーに違反するエンティティを自動的に隔離できます。

10 https://www.arista.com/jp/products/network-detection-and-response
11 https://www.arista.com/assets/data/pdf/Arista-CI-Pipeline-Tech-Brief.pdf
12 https://www.arista.com/en/products/network-access-control

ゼロトラストを支えるアリスタの統合ソリューション

以上の機能を併せ持つ一元化された統合ソリューション（図 14）が、旧来のアプローチから、ゼロトラスト成熟度モデルの最終段階への移行を後押しします。しかも、基盤となるネットワーク・インフラを利用し、展開を簡素化して、運用オーバーヘッドを削減します。

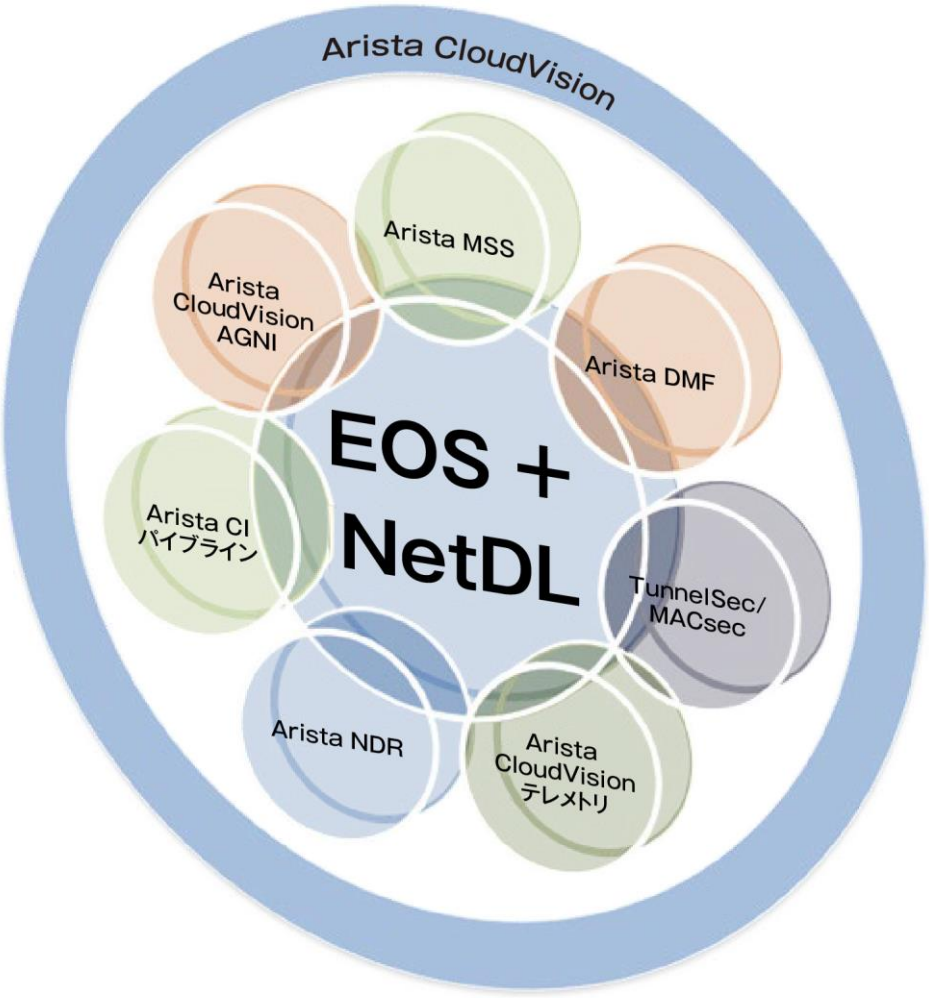


図 14：ゼロトラストを加速化するアリスタのソリューション群

まとめ

ゼロトラスト・アーキテクチャは、内部ネットワーク上のデバイスを暗黙的に信頼するのをやめることで、サイバー脅威に関連するリスクを軽減しようとする考え方です。しかし、キャンパス、データセンター、クラウドなどに広がる現代のネットワークでは、これは言うほど簡単なことではありません。ファイアウォール、ネットワーク・アクセス制御、脅威検知などを含むネットワーク・セキュリティ・レイヤを追加するアプローチは、多額のコストがかかり、複雑で、脆弱性を伴う上に、メリットの数値化が困難です。その結果、多くの組織は、特に重要資産が置かれていることが多いネットワーク深部において、いちかばちかのリスク管理をすることになります。

アリスタは、EOS 内の統合オペレーティング・システムの基盤と CloudVision の共通管理プレーンの上に構築されたセキュリティ・ソリューション・スイートを提供します。このソリューションは、CISA のゼロトラスト成熟度モデルに対応し、成熟度の最終段階を目指す組織の取り組みを加速させます。さらに、これらのネットワーク・セキュリティ・コントロールは、ID、デバイス、ワークロード、データなどの領域で生じているゼロトラスト・ポスチャのギャップを相殺するのに役立ちます。最も重要な点は、この統合セキュリティ・ツールセットが、スイッチから WAN ルーターまでのネットワーク・インフラを通じて重要なセキュリティ機能を提供し、組織内の既存のセキュリティ・プログラムやツールとシームレスに連携することです。アリスタのアプローチは、セキュリティをただの題目から実効力のあるものに転換し、後付けのネットワーク・セキュリティではなく、ネットワークの中に組み込まれたセキュリティを実現します。

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

ARISTA
2023 年 4 月 24 日