NIST 800-207 と Arista NDR を活用したゼロトラスト戦略の構築

新型コロナウイルス感染症（COVID-19）の世界的流行の影響により、組織におけるデジタル変革への取り組みが加速した結果、ゼロトラストはバズワードから急速に現実的なものとなりました。ただし、ゼロトラストは目的地ではなく、道のりです。残念ながら、多くの企業において、この道のりに明確な終わりはありません。そこで、NIST は、組織のサイバーセキュリティ態勢向上の取り組みと道筋を測定できるようにするゼロトラスト戦略の枠組みを文書にまとめました[1]。NIST の文書はおもしろい読み物というわけではありませんが、ゼロトラストの取り組みに着手した多くのお客様からアリスタが耳にした内容と合致しています。

この文書のポイントについて説明する前に、NIST 800-207 ガイダンスの読み進め方として、記載順どおりではない順序で読むことをお勧めします。NIST の文書の第 2 節で、ゼロトラスト・アーキテクチャの初心者向け基礎知識を読んだ後、次に第 7 節を読めば、今後の進め方の理解に役立ちます。次に第 5 節を読むと、移行後の脅威モデルの進化について見通しを把握できます。NIST の文書では明示的に示されていませんが、アリスタのお客様との作業において、この新しい脅威モデルが現在の脅威モデルと比較してどうなるかをベンチマークで測定することは有益です。

先にお伝えしますが、ゼロトラストを導入したからといって、脅威がなくなるわけではありません。第 5 節では、ゼロトラスト・アーキテクチャの安全性確保のために導入すべき一連の制御について説明しています。最後に、この文書全体を読むことができない場合は、前述の節のほかに第 3 節も必ず読むことをお勧めします。皆様の環境においては、どのようになるでしょうか。

[1] https://csrc.nist.gov/publications/detail/sp/800-207/final

ゼロトラスト・アーキテクチャ（ZTA）への移行

お客様のチームでは、ゼロトラストは明確に定義された比較的短いタイムラインの単発のプロジェクトであるかのように想定されていることが多々あります。ネットワークを最初から作り直す場合や、比較的単純なネットワークである場合を除き、ゼロトラスト・アーキテクチャ（ZTA）の構築と維持に必要な継続的プロセスの理解に第 7 節が役立ちます。

7 Migrating to a Zero Trust Architecture 35
7.1 Pure Zero Trust Architecture 35
7.2 Hybrid ZTA and Perimeter-Based Architecture 35
7.3 Steps to Introducing ZTA to a Perimeter-Based Architected Network 36
7.3.1 Identify Actors on the Enterprise 37
7.3.2 Identify Assets Owned by the Enterprise 37
7.3.3 Identify Key Processes and Evaluate Risks Associated with Executing Process 38
7.3.4 Formulating Policies for the ZTA Candidate 38
7.3.5 Identifying Candidate Solutions 38
7.3.6 Initial Deployment and Monitoring 39
7.3.7 Expanding the ZTA 39

図 1：ゼロトラスト・アーキテクチャへの移行に関する NIST のガイダンス

目次（図 1）からわかるように、第 7 節では、ZTA を展開する際の考慮事項と手順について詳しく説明しています。ご想像のとおり、これをゼロから始めたり、一挙にネットワーク・トポロジを大幅に変更したりする余裕はないため、この種の取り組みが「1 回で終わる」ことはほとんどありません。

図 2 のように、このプロセスはフィードバック・ループで継続的に行う取り組みです。

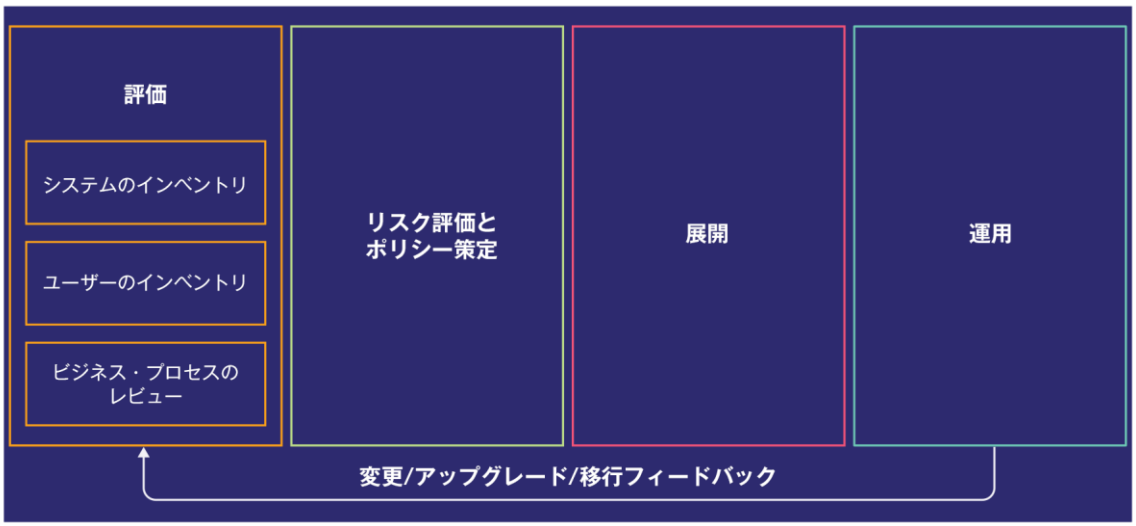

図 2：ゼロトラスト・アーキテクチャへの移行プロセス[2]

ZTA に移行する前に、どのリソース/アセットを保護する必要があり、誰がそれらにアクセスするかを把握する必要があります。Active Directory または CMDB から始めるのは確かに良い方法の 1 つですが、それらは確実に正確でしょうか。Arista NDR の導入に際し、平均的なお客様が「管理対象」としているネットワーク上のリソースやデバイスは実際の 50%未満にすぎず、管理対象外のインフラストラクチャの多くを可視化できていないことが明らかになりました。第 7.3.1 節と第 7.3.2 節で説明しているように、それを把握することが効果的な ZTA 戦略の基礎となります。

[2] Adapted from NIST 800-207

ZTA 戦略構築の良い出発点は、ネットワーク・レベルでの可視化と制御を確保することです。シャドーIT、クラウド IoT、BYOD、サードパーティ・デバイスが企業ネットワーク上で増加しているため、従来のエージェントベースのソリューションに加えて、エージェントレスのアプローチも必要になっています。

Arista NDR で展開される AI ベースのセキュリティ・ナレッジ・グラフ、EntityIQ™は、1 つのネットワーク接続だけで、エンタープライズ・ネットワーク上のすべてのデバイス、ユーザー、アプリケーションの識別、プロファイリング、追跡を行うことができるため、アナリストは、新しい統合やエージェントを必要とすることなく、ネットワーク上の状況を即座に把握できます。

また、Arista NDR の Adversarial Modeling 言語（AML）を使用して、ビジネス・プロセスを可視化および監視し、それらのプロセスが損なわれた場合にそれを検出することができます。たとえば、ある小売業のアリスタのお客様は、PCI[3] エンクレーブに関して ZTA を運用しています。Arista NDR は、不正デバイスや不正ユーザーがこの環境にアクセスしようとする試みがないか、監視します。この機能を ZTA 移行前に使用して、アクセスの必要なすべてのデバイスとユーザー、および統合可能なデバイスとユーザーのインベントリを行うことにより、このお客様は絞り込まれた許可リストを定義できました。移行後は、Arista NDR の機能によって、悪意の有無にかかわらず、この許可リストに反する試みを監視できるようになりました。

最後に、SP 800-207 が指摘するように、ZTA への移行は平坦な道のりではありません。第 7.3.6 節で強調しているように、継続的なモニタリングと調整が必要です。そのためには、ネットワークからの適切なテレメトリが必要であり、人間が大量のデータを処理したり効果的なルールを手動で構築したりすることなく、そのテレメトリを大規模に分析できる必要があります。AML はそのための柔軟性を提供します。移行後と過去のアクセス・パターンを比較できるため、管理者はネットワークの中断を迅速に特定し、修正することができます。

ZTA 移行前後の脅威モデル

今日の攻撃的な脅威の状況下では、セキュリティ・チームは常に組織の脅威モデルを明確に理解しておく必要があります。この脅威モデルがゼロトラスト移行時に果たすもう 1 つの目的は、どのプロセスが組織にとって最もリスクが高く、そのため最初に ZTA に移行すべきかを特定することです。Arista NDR は、社内のデバイス、ユーザー、アプリケーションだけでなく、ドメイン、ASN、IP アドレスなどの社外の宛先まで、あらゆるエンティティのリスクを自動的にスコア付けします。企業はこの機能により、リスクの高いエンティティを使用するビジネス・プロセスを優先的に ZTA に移行できるようになりました。

ZTA 移行後の脅威モデルはどうでしょうか。ゼロトラストによってすべての脅威がなくなるわけではありませんが、セキュリティと耐障害性は向上します。SP 800-207 は、ゼロトラストの原則に従ってネットワークを設計したからといって、安全なネットワークを確保できるわけではないと主張しています。

5 Threats Associated with Zero Trust Architecture 28
5.1 Subversion of ZTA Decision Process 28
5.2 Denial-of-Service or Network Disruption 28
5.3 Stolen Credentials/Insider Threat 29
5.4 Visibility on the Network 29
5.5 Storage of System and Network Information 30
5.6 Reliance on Proprietary Data Formats or Solutions 30
5.7 Use of Non-person Entities (NPE) in ZTA Administration 30

図 3：ゼロトラスト・アーキテクチャへの脅威に関する NIST のガイダンス

では、どうすれば「適切に行う」ことができるのでしょうか。組織が現在懸念している脅威から着手するとよいでしょう。たとえば、従来の「ファイアウォールの内側」のアプリケーションが減少し、SaaS やその他のクラウドベースのプラットフォーム上のアプリケーションが増加してはいないでしょうか。監視されているセキュリティ指標は、脅威がマルウェア以外（環境寄生型）の脅威へ進化し

[3] https://www.pcisecuritystandards.org/

ていることを示してはいないでしょうか。業界の統計によると、現在の多くの侵害案件にマルウェアの痕跡はありません。代わりに、攻撃者は環境内のツールを使用したり、内部の人間の認証情報を悪用したり、Twitter や Google Drive のような広く利用されているサイトをコマンド・アンド・コントロールに使用したりしています。セキュリティ・チームは今、通常のビジネス活動と同じように見える活動の中から悪意を検出することが必要になっています。脅威モデルを構築すれば、組織は安全なゼロトラストを実装するための基本的な制御を探すことができます。

その例を次に示します。

第 5.3 節は、実行時のゼロトラストの判断時におけるコンテキストの重要性を強調しています。たとえば、財務部門のユーザー「Bob」が会社のデバイスからログインし、通常アクセスしているリソースにアクセスする場合、それは許容されます。しかし、個人のデバイス、携帯電話、クラウド上のワークロードからアクセスする場合は、許容されないでしょう。同様に、「Bob」がソース・コード管理システムにアクセスしようと試みる場合、それが明示的に禁止されていなかったとしても、悪意を示すものである可能性があります。現在、このような脅威を発見するためには、手動の脅威ハンティングに多大な投資を必要とすることが多く、それは煩雑かつ反復不可能なプロセスになっています。Arista NDR の自律的なハンティング機能は、このような行動上の脅威を検出し、お客様のインフラストラクチャの他の部分（オーケストレーション、チケッティング・システム、ネットワーク適用ソリューション、エンドポイント・エージェントなど）と統合することにより、アナリストの代わりに自動対応アクションを始動させます。

第 5.4 節では、Web トラフィックの 90%以上が暗号化されるようになったことによるネットワーク・セキュリティのもう 1 つの課題について説明しています。アリスタの独自のデータによると、いわゆる水平方向のトラフィックの 50%以上が、ネットワーク境界内でも暗号化されています。さらに、ポリシー違反やプライバシー侵害の可能性があるという理由から、復号化を避けようとする組織が増えています。技術的な観点からは、エンドツーエンドの暗号化と TLS 1.3 を使用するアプリケーションは、さらなる障害となります。この傾向を悪用し、ネットワーク脅威検出を回避する手段として暗号化トラフィックを使う攻撃者が出現してきています。Gartner の最近の報告によると、現在、悪意のあるトラフィックの 70%以上が暗号化されています。NIST SP 800-207 で指示されているように、Arista NDR は、データ・サイエンスに基づく暗号化トラフィック分析を行い、技術、プライバシー、ポリシーの制約の範囲内で、セキュリティ・チームに有益な情報を提供します。このようなユースケースには、アプリケーション固有のプロトコルや通信、回線を通過する暗号化されたトラフィックの性質を特定することなどがあります。たとえば、暗号化されたファイルが Zoom 会議セッションで転送されるのは問題ないかもしれませんが、そのファイルが PowerShell スクリプトから Dropbox アカウントに転送されていたら調査する必要があります。

ZTA の実践

NIST の文書の第 3 節は、ZTA の構成要素を非常に適格に説明しています（図 4）。特に第 3.4 節は、ZTA を効果的に実装するための重要なネットワーク要件を概説しています。これには、管理対象デバイスと管理対象外デバイスを効果的に区別できることや、暗号化されたトラフィック（前述）を含むすべてのネットワーク・トラフィックをキャプチャして分析できることなどがあります。

[4] https://www.crowdstrike.com/blog/global-threat-report-foreword-2020/
[5] https://www.bondcap.com/report/itr19/

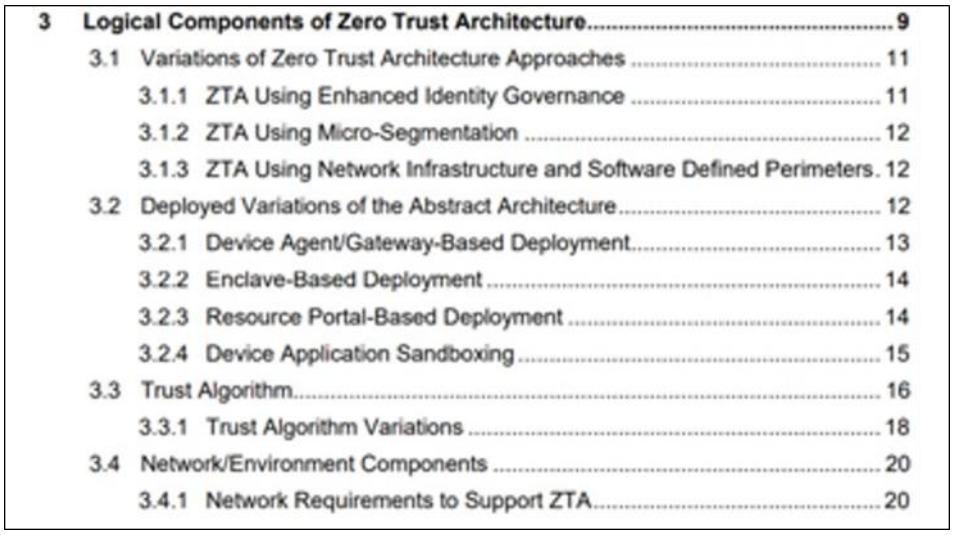
3 Logical Components of Zero Trust Architecture 9
3.1 Variations of Zero Trust Architecture Approaches 11
3.1.1 ZTA Using Enhanced Identity Governance 11
3.1.2 ZTA Using Micro-Segmentation 12
3.1.3 ZTA Using Network Infrastructure and Software Defined Perimeters. 12
3.2 Deployed Variations of the Abstract Architecture 12
3.2.1 Device Agent/Gateway-Based Deployment 13
3.2.2 Enclave-Based Deployment 14
3.2.3 Resource Portal-Based Deployment 14
3.2.4 Device Application Sandboxing 15
3.3 Trust Algorithm 16
3.3.1 Trust Algorithm Variations 18
3.4 Network/Environment Components 20
3.4.1 Network Requirements to Support ZTA 20

図 4：ゼロトラスト・アーキテクチャの構成要素に関する NIST のガイダンス

ZTA の基本理念はシンプルですが、戦略を計画する際には実装上の現実的課題への対応を計画することが不可欠です。たとえば、第 3.3 節で説明している信頼性アルゴリズムは、アクセスを要求しているユーザーまたは ID、要求されているアクセスのタイプ、アクセスを許可するための最小セキュリティ要件（多要素認証、更新されたパッチ・レベルなど）、内外両方の脅威インテリジェンスからのデータなどの情報を考慮して、判断を下す必要があります。このような制御を導入すると、「このアクセスは、この特定のアクセスを要求するピア・グループから外れているデバイスから行われていないか」、「問題のユーザーまたはデバイスは、比較的まれなドメインへの接続を繰り返すなどの弱いシグナルで侵害を示していないか」など、ネットワークに関する非常に具体的な質問ができるようになる可能性があります。

Arista NDR は、機械学習アプローチの組み合わせを用いてこの分析を自動化します。従来のソリューションは、主に教師なしの学習を使用して、「正常」の基準から外れた異常を検出します。悪意のない異常を検知する誤検知や、逆に、以前から存在する侵害を「正常」と想定して見逃す検知漏れがよく発生します。リスクと隣り合わせのまま気付かない状況が続くという意味では、検知漏れの方がより危険です。Arista NDR プラットフォームは、エンティティの動作を、過去に観測された動作と比較するだけでなく、ピア・グループや組織の他の部分から観測された動作とも比較します。ベースライン設定に依存しないことにより、価値創出までの時間も短縮でき、継続的な運用コストも削減できます。特に、1～3 か月の「トレーニング」と、環境が変わるたびに行う再トレーニングを必要とするソリューションと比べてスピードアップされます。

まとめ：アリスタがゼロトラスト戦略を可能に

図 5：アリスタがゼロトラスト・アーキテクチャ戦略を可能に

ユーザーや必要なリソースの場所に関係なく、組織の生産性を高めることが IT チームに求められる現在、ゼロトラスト・アーキテクチャの構築は崇高な目標です。しかし、NIST 800-207 が指摘するように、ボタンを 1 つ押すだけで魔法のように組織を変革できるわけではありません。ゼロトラスト戦略を進めるには、組織の生産性とセキュリティの強化を確保できるように、慎重に考える必要があります。

図 5 が示すように、アリスタは、ゼロトラスト・アーキテクチャの効果的な移行と運用に必要なツールを数多く提供しています。

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

2022 年 3 月 29 日　02-0099-01