JUNIPER NETWORKS | Engineering Simplicity

ホワイトペーパー

ゼロトラストの台頭

神話から現実を切り離す

目次

概要

企業は、サイバー攻撃から自社を保護して機密データの侵害を防ぐための適切な措置を講じていることを実証する必要があります。さらに、企業に対するその強いプレッシャーは高まり続けています。現在、企業のセキュリティに関して最も人気が高く、そしておそらく最も実現可能なアプローチは、ゼロトラストのコンセプトです。優れた防御を実現するセキュリティ戦略の策定において、ゼロトラストは不可欠です。ITおよびセキュリティのリーダー、エグゼクティブやエンジニアはその理由を理解する必要があります。

このホワイトペーパーでは、ゼロトラストセキュリティアーキテクチャの現実とこれまで信じられてきた神話や誤解とを切り離して説明します。そして、ゼロトラストネットワークアーキテクチャをサポートおよび実現するだけでなく、そのアーキテクチャの迅速かつ簡単な実装に役立つJuniper Connected Securityについて紹介します。

はじめに：より効果的なセキュリティモデル

ゼロトラストのコンセプトは急速に広がっており、セキュリティアプローチ全般、特にネットワークアーキテクチャに対するアプローチに大きな変革をもたらしています。データ侵害が絶えず発生していることからも、内部のユーザー、ネットワーク、システムを本質的に信じるべきという一般的な仮定はもはや有効ではないことが証明されており、ゼロトラストを考える時期が来ているといえます。

ゼロトラストアプローチの利点は明確で魅力的ですが、アーキテクチャの実装を担当するネットワークおよびセキュリティの専門家にとっては質問や課題がたくさんあります。ネットワークインフラストラクチャ全体を置き換える必要があるのか？ マイクロセグメンテーションは実現可能な目標か？ クラウドではゼロトラストアーキテクチャの可能性を享受できないのか？

このホワイトペーパーでは、ゼロトラストセキュリティアーキテクチャの現在の現実と古くから言われている神話とを切り離して説明します。そして、ゼロトラストネットワークアーキテクチャをサポートおよび実現するだけでなく、そのアーキテクチャの迅速かつ簡単な実装に役立つJuniper Connected Securityについて紹介します。

最新の環境を保護するより良い方法

*過去の状態：*エンドポイントは企業が所有、管理、保護するものでした。境界内のどのユーザーもデバイスも信頼できるものであると想定していました。企業アプリケーションは安全なデータセンター内で運用されており、お互いを信頼していました。

*そして現在：*ワークロードはクラウドへと移行され、管理されていないモバイルデバイスが例外ではなく標準となった今、ネットワーク境界は進化しています。アプリケーション、ユーザー、ユーザーのデバイスの場所は静的ではなくなっています。データはもはや企業のデータセンターの範囲内に留まってはいません。攻撃対象領域が拡大するにつれて可視性と保護の間のギャップが広がり続けており、企業はすべてを確認し保護するために、連携に欠ける複数のツールを追加する必要性に迫られています。

その一方、サイバー犯罪者は高度なセキュリティ対策を回避することにますます熟練してきており、ラテラルムーブメント（横方向への移動）を利用して侵害の標的に到達する攻撃者が増加しています。また、高度化するツールキットや、脆弱性の悪用方法の分かりやすい説明も利用できるようになっており、脆弱性の数は増え続けています。米国脆弱性情報データベースが2018年に公開した既知のセキュリティ脆弱性は14,760件であり、これは2016年に報告された数の2倍以上でした。

*結論：*より強力な境界を構築することは、ネットワーク、ユーザー、アプリケーション、データを保護するための適切なアプローチではなくなっています。

ゼロトラストの黎明期

新しいゼロトラスト情報セキュリティモデルは、2009年にForrester Researchによって紹介されました。その後、広く受け入れられるようになり、導入が進んでいます。企業は、ゼロトラストのコンセプトとそのアーキテクチャコンポーネントを導入することで、安全性を高めるとともに、コンプライアンスに関する負担を軽減し、最終的にはコストを削減できます。

出典：『No More Chewy Centers: The Zero Trust Model of Information Security』、Forrester Research, Inc.、2016年3月

新しいセキュリティパラダイム

ゼロトラストへと移行しましょう。これは、今日の脅威の状況に対して優れた保護を提供するために広く採用されつつある最新のセキュリティパラダイムです。「決して信頼せず、必ず確認せよ」というのがゼロトラストの基本理念です。つまり、ネットワークのすべての部分に悪意が潜んでいる（インターネット上に直接存在している）と仮定し、その仮定に従ってアクセス要求に対応するということです。

ゼロトラストアプローチでは、本質的に信頼するということ自体が重大な脆弱性であると捉えます。組織のネットワーク内のすべてが信頼できると仮定すると、攻撃者や悪意を持つ内部者は特権を悪用して簡単に横方向に移動し、ターゲットのデータにアクセスしたり、データを抜き取ったりすることが可能になってしまいます。

ますます高まるゼロトラストの重要性

最近のForbes Insightsの調査でサイバーセキュリティの先駆者と認められた複数の組織は、自社のセキュリティ戦略においてゼロトラストの取り組みは「極めて重要」と考えています。

出典：『Cybersecurity Trailblazers Make Security Intrinsic to Their Business』、Forbes Insights、2019年

そうではなく、重要なデータ、アプリケーション、サービスの周辺にマイクロペリメーターを作成して制御することで、保護対象のアセットに既知の許可されたトラフィックとアプリケーションのみがアクセスできるようにします。ゼロトラストアーキテクチャでは、誰がマイクロペリメーターを通過できるかを決定し、保護対象のアセットの近くに制御機能を設定することで、不正アクセスと機密データの流出を防ぎます。

このアプローチでは、すべての潜在的な攻撃から組織を保護することはできないものの、次のことが可能になります。

- 不正なラテラルムーブメントとアクセスを防ぐことで、高度な脅威と侵害のリスクを減らす
- 脅威の検出と対応を迅速化する
- 可視性のギャップを削減する
- HIPAA、PCI-DSS、FISMAなどのコンプライアンス要件をサポートする

ゼロトラストの柱の概要

ゼロトラストのコンセプトが登場して以来、業界のエキスパートやForresterのアナリストなどのオブザーバーはこのセキュリティアプローチについて検討してきました。Forresterの最新のレポートでは、これをZero Trust eXtended（ZTX）Ecosystem[1]と呼んでいます。

簡単に説明すると、ゼロトラストとは「セキュリティチームがネットワークを安全なマイクロペリメーターへと再設計し、難読化技術を使用してデータセキュリティを強化し、過剰なユーザー特権とアクセスに関連するリスクを制限し、分析と自動化によってセキュリティに関する検出と応答を劇的に改善する」ための概念およびアーキテクチャモデルです。

ZTX Ecosystemは、プロセスとテクノロジーを含む完全なアプローチを採用しており、図1に示すように、データ、ワークロード、ネットワーク、デバイス、人、可視性と分析、自動化とオーケストレーションを網羅しています。

ゼロトラストアプローチを採用する企業は増え続けており、現在、グローバル企業の60%はゼロトラスト戦略に取り組み、ゼロトラストの計画を策定しているか積極的に実行に移しています[2]。これらの企業がすでに認識しているのは、過去にゼロトラストの取り組みを妨げた誤解は、今日の現実を反映していないということです。そのような神話や誤解のいくつかを詳細に見ていきましょう。

ゼロトラストを支持する声

「ゼロトラストは今日、運用が複雑化したりアーキテクチャの大幅な変更が必要になったりすることのない成熟したソリューションを提供できます。実際のところ、運用を簡略化するとともにセキュリティを強化して高価値の重要なアセットを保護することが可能です」

出典：『Zero Trust Cybersecurity Current Trends』、American Council for Technology-Industry Advisory Council（ACT-IAC）、2019年4月

[1]『The Zero Trust eXtended (ZTX) Ecosystem; Strategic Plan: The Zero Trust Security Playbook』、Forrester Research, Inc.、2019年7月
[2]『The Digital Enterprise Report: How the World's Largest Organizations Are Evolving with Technology』、Okta、2019年

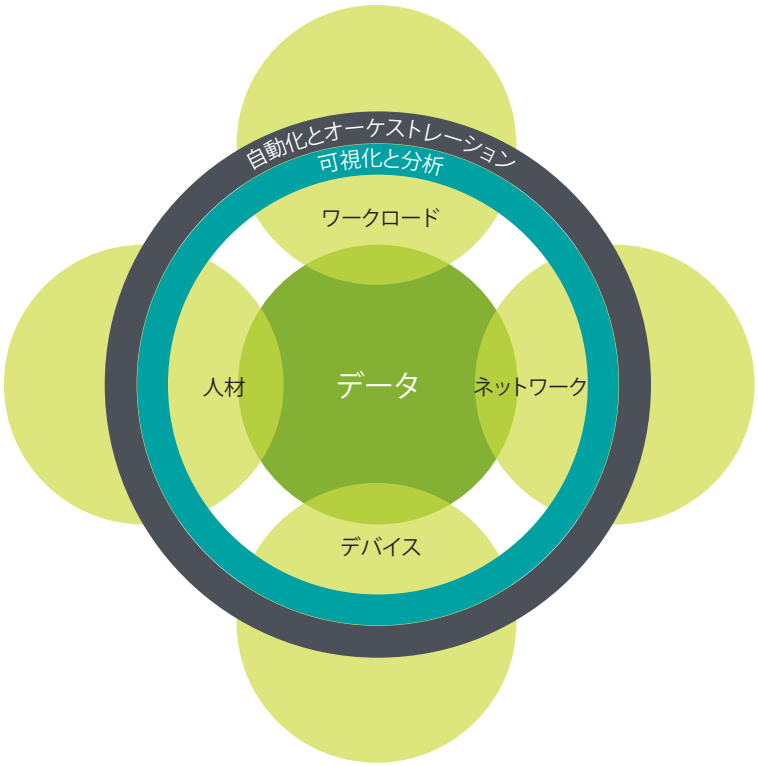

図1：Zero Trust eXtended（ZTX）Ecosystem、Forrester Research, Inc.

誤解その1：ほとんどの企業にとってゼロトラストへの移行はコストが高すぎる

ゼロトラストモデルの実装は、大企業を除き、コスト的に不可能であると多くの企業が誤解しています。ゼロトラストを実装している最も有名な企業として、GoogleやCoca-Colaなどが挙げられます。そのため、潤沢な資金を持つ企業でなければコスト面で慎重にならざるを得ないと考えてしまうことも理解できます。

しかし実際には、小規模な新興企業からグローバル企業まで、どのような規模の企業にとってもゼロトラストは適切で手頃なものです。その理由は次のとおりです。

1. ゼロトラストは道のりであって、プロジェクトではない。底なしの財源を保持し、大きな目標を背負っている企業は、ゼロトラストアーキテクチャを一から始めることを正当化できるかもしれませんが、大多数の組織は、より実用的で段階的なアプローチを採用するほうがよいでしょう。ゼロトラストは反復的なアプローチです。つまり、企業が前もってかなりのリソースと予算を投資する必要がなく、むしろ、それらのコストと労力を長期間にわたって分散させることができます。

2. ゼロトラストの実装により、運用効率の改善と複雑さの低減が実現するため、セキュリティコストが削減される。Forresterによると、「ゼロトラストではセキュリティ管理を一元化するため、支出も削減」[3]できます。

Juniper Connected Securityは、ゼロトラストアーキテクチャの実装を段階的に進めていくことをサポートします。すでに実施しているセキュリティを強化するとともに、「アラートの過負荷」に悩まされることなく可視性と脅威認識を高められます。たとえば、より安全なネットワークに向けたジュニパーの5段階のフレームワークは、自社のセキュリティがそのプロセスのどのあたりにいるのか、および今後の方向性について判断するのに役立ちます（図2を参照）。

[3]『The Eight Business and Security Benefits of Zero Trust』、Forrester Research、2019年9月

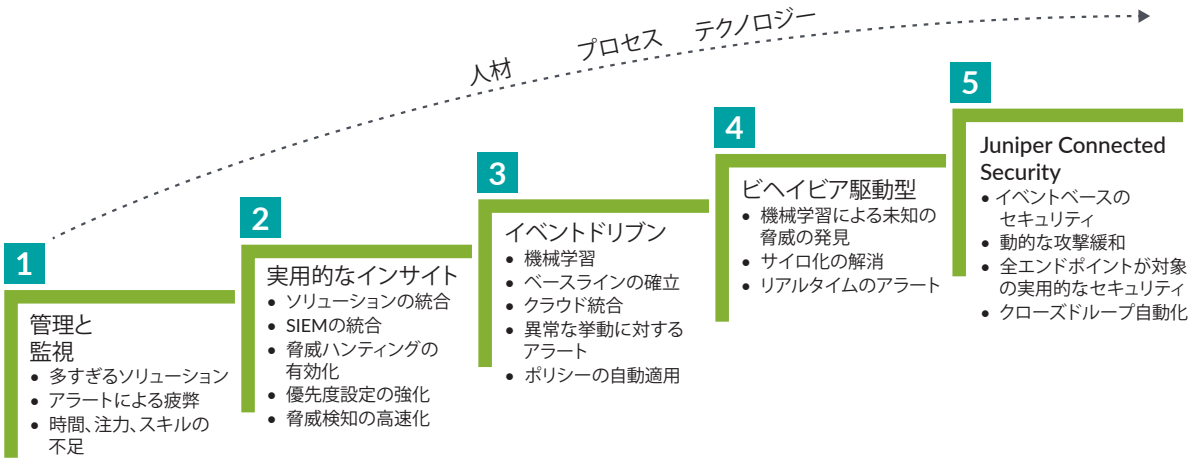

図2：Juniper Connected Securityへの5ステップのフレームワーク

誤解その2：マイクロセグメンテーションの実装は複雑すぎて現実的ではない

マイクロセグメンテーションは、ゼロトラストを念頭に置いた強力なネットワーク保護ツールです。モノリシックな境界を一連のマイクロ境界に分割してきめ細かいセキュリティ制御を実現し、攻撃を封じ込めます（図3を参照）。ではなぜ、セキュリティやネットワークの担当者はこのアプローチの採用を主張しないのでしょうか？

当初から、既存のアプリケーションや環境でマイクロセグメンテーションを実装するのは極めて時間がかかり、あまりにも複雑なものとして考えられていたからです。関係するアプリケーション、アプリケーション依存関係、サービス、ユーザーがあまりにも多いため、マイクロペリメーターを実装し維持することは単に実現不可能であると捉えられていました。その考えは、連携しない個別のセキュリティおよびネットワーキング製品を使用している企業には当てはまる場合もあります。そのような企業では、ネットワークや環境に対するエンドツーエンドの可視性を実現できません。

しかし、ゼロトラストを採用できるとともにゼロトラストネットワークのアーキテクチャコンポーネントを強力にサポートするテクノロジーなら、マイクロペリメーターの作成や維持のコストと複雑さを低減できます。これは、セキュリティ機能をデバイスに統合し、一元化されたセキュリティポリシーでそれらのデバイスを管理および制御することで可能になります。

たとえば、Juniper Connected Securityは、マイクロペリメーターを実現するゼロトラストアーキテクチャの主要なコンポーネントをサポートするのに必要な全機能を備えています。

- **ネットワークセグメンテーションゲートウェイ**：ネットワークの中核として機能するセグメンテーションゲートウェイは、従来のスタンドアロンのセキュリティサービスとデバイスを1つのゲートウェイに統合します。Juniper Connected Securityのセグメンテーションゲートウェイ機能により、次世代ファイアウォール、統合脅威管理（UTM）サービス、包括的な標準ベースのIPsec暗号化とルーティングおよびスイッチングを、ハイパフォーマンスでコスト効果の高い単一のプラットフォームに組み合わせることができます。
- **パラレルでセキュアなマイクロセグメンテーション**：高速インターフェイスにマッピングされたスイッチングゾーンで、セキュアなセグメントを作成します。Forresterはこのセグメントをマイクロコアと境界（MCAP）と呼んでいます。MCAPは複数のパラレルなマイクロセグメンテーションであり、統合セグメンテーションゲートウェイファブリックに集約されます。Juniper Connected Securityは、定義されたセキュリティ属性に基づいてネットワークのマイクロコアセグメンテーションを実行し、ネットワークアクティビティに対する可視性をアプリケーションにユーザーごとまたはロールベースで提供して、各MCAPの厳格なアクセスコントロールを実現します。そこからさらにジュニパーは、スイッチ、ルーター、Wi-Fiアクセスポイントを含むネットワークの各レイヤーまでセキュリティを拡張し、ジュニパーおよびサードパーティーのスイッチを含むネットワーク全体へと脅威が拡散するのを防ぎます。
- **一元管理**：効率的でスケーラブル、かつ簡単な管理機能を提供するJuniper Connected Securityにより、ITチームはネットワークバックプレーンとして機能する単一のシステムからすべてのMCAPを透過的に管理できます。セキュリティチームは、場所に関わらず、各MCAPのセキュリティを維持する包括的なポリシーセットを管理できます。これにより、必要なポリシー数やルール数を削減しながら、単一のセグメンテーションゲートウェイインスタンスの細かい管理をサポートできます。

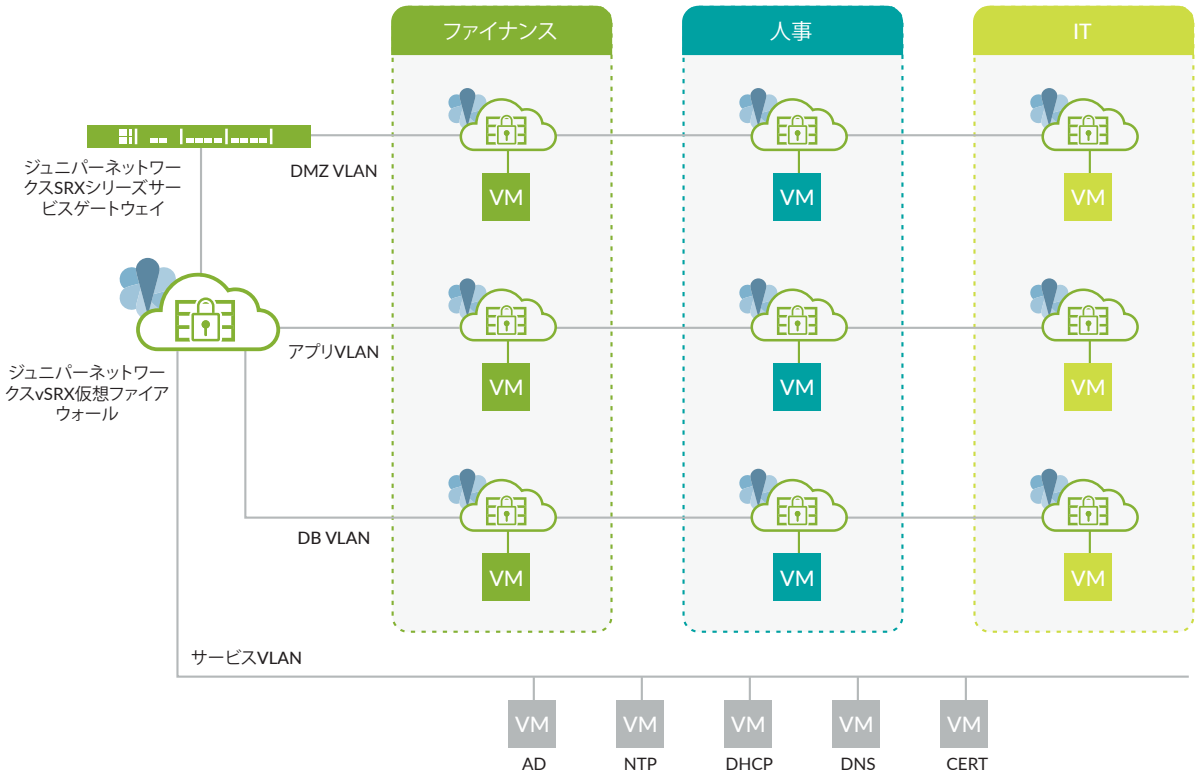

図3：データセンターのマイクロセグメンテーションの例

誤解その3：実装可能なのはグリーンフィールドの環境のみ

広く信じられている考え方の1つに、ゼロトラストはグリーンフィールドの場合のみ実装できるというのがあります。それ以外の環境では、すべてを置き換えて、単一のプラットフォームでやり直さなければならない、という考え方です。

一部の企業ではそのようにしている場合もありますが、ほとんどの企業はゼロトラストのためにすべてを置き換えるというアプローチは採用していません。幸いなことに、そうする必要はないのです。ゼロトラストアーキテクチャの実現には、ネットワーク全体の再構築は必要なく、また1回での大規模な作業も必要ありません。

今後の成熟度を高めながら段階的に着実に実装していくという、ゼロトラストへのロードマップを策定できます。この増分アプローチを成功させるカギとなるのが、企業がすでに保有しているものを簡単にサポートし統合できるソリューションの選択です。これにより、ゼロトラストをサポートする新しいセキュリティ機能を実装すると同時に、ネットワーク全体にセキュリティを拡張できます。

ジュニパーは、すべての企業にすべてのものを提供しようとするのではなく、オープンスタンダードと製品の相互運用性に注力しています。どのベンダーも1社だけで最新のエンタープライズネットワークの安全を確保することは不可能です。Juniper Connected Securityでは、複数のセキュリティソリューションを網羅する統合ビューにより、無駄に複雑化することなく、セキュリティインテリジェンスの活用、脅威の検出の向上、脅威の緩和が簡単に実現します。

誤解その4：ゼロトラストはオンプレミス環境でのみ可能

ゼロトラストの主な論拠は、企業がそのネットワーク内のすべてを信頼することはできなくなったということにあります。それを踏まえた一般的な誤解は、ゼロトラストは企業のデータセンター内でのみ適用可能であるという考え方です。企業環境内は信頼できるという仮定をサイバー犯罪者が悪用しているのは事実です。しかし、それら犯罪者の労力やテクニックはオンプレミス環境に限られているわけではありません。

また、ゼロトラストは主に企業のデータセンターに実装できる（または企業のデータセンターのみに実装できる）ものであると信じてしまう理由の1つとして、企業はセキュリティを担うのはクラウドサービスプロバイダだと考えがちであることが挙げられます。これはクラウドコンピューティングに関する最大の誤解の1つです。実際、クラウドの一般的なセキュリティモデルは責任共有モデルです。つまり、クラウドサービスプロバイダがクラウドインフラストラクチャの保護責任を担い、お客様がワークロード、データ、ユーザーの保護責任を担うというものです。ゼロトラストは、クラウドに適用できるというだけでなく、企業のアセットの保護をクラウド環境やマルチクラウド環境まで拡張するために不可欠です。

Juniper Connected Securityは、セキュリティポリシーとそれらの適用をクラウドにまで拡張し、新たなサービス提供モデルをサポートするとともに、エンドポイントからエッジ、およびその間にあるすべてのクラウドのワークロードやデータを保護します。これにより、企業はセキュリティ対策をオンプレミスからクラウドへと拡張できます。ジュニパーにより、コンテナ化されたワークロードまでゼロトラストセキュリティを拡張することも可能なため、可視性と適用をアプリケーション内の各マイクロサービス間の通信にまで拡張できます。

誤解その5：ゼロトラストには単一ベンダーのアプローチが必須

セキュリティ業界がゼロトラストの時流に乗るようになるにつれて、ベンダーの多くは単一ベンダーのソリューションの必要性に焦点を合わせて宣伝を行っています。ゼロトラストアーキテクチャですべてを確実に連携させるための唯一の方法は、必要なものすべてを提供する単一のベンダーを選択することであるという議論がなされてきました。

現実としては、ゼロトラストアーキテクチャ内でネットワーキングの保護に必要なすべてのものを1社で提供できるベンダーはありません。Forresterは、さまざまなセキュリティドメインの機能を統合することが不可欠であると報告し、「ゼロトラストでは、異なるデータシステム、ネットワーク、インフラストラクチャ全体のアセットの使いやすさと、コマンドおよびコントロールが重要」と述べています。

そのため、Juniper Connected Securityはグローバルなパートナーエコシステムを築いています。これは、お客様組織のすべてのレベルにおいて実際のビジネス価値を促進するネットワークの提供と実装を専門とするエコシステムです。このようなパートナーシップで、ジュニパー独自の製品およびサービスを補完するクラス最高のソリューションと業界専門知識を活用し、幅広いお客様のニーズに対応しています。

ゼロトラストの導入とJuniper Connected Security

ゼロトラストアーキテクチャに関する事実とフィクションを分けて説明してきました。ここで、企業がゼロトラストを可能な限り最も有利な方法で導入するのに役立つJuniper Connected Securityの独自の位置付けについて見ていきましょう。

何よりもまず、安全でハイパフォーマンスなネットワークにおけるリーダーシップが挙げられます。ジュニパーがサポートしているのは、極めて高度なネットワークを構築するお客様です。Fortune Global 100のうちの97社、ソーシャルメディアの世界トップ5社、米国のスマートフォンのトラフィックの86%以上を含む、世界最大級のネットワークをジュニパーはサポートしています。

研究開発に多大な投資を行うことで、ジュニパーネットワークスは、ネットワーキングテクノロジーのすべての側面、つまりシリコン、システム、ソフトウェア、セキュリティなどにわたり業界で最も画期的なイノベーションを生み出しています。次世代ファイアウォール、スイッチング、高度なマルウェア防御、インテリジェントなポリシー、柔軟な導入モデルにJuniper Connected Securityを組み合わせることで、ジュニパーは世界中の企業のゼロトラストのニーズに効果的に対応できるという優れた地位を確立しています（図4を参照）。

[4]『The Zero Trust eXtended (ZTX) Ecosystem; Strategic Plan: The Zero Trust Security Playbook』、Forrester Research, Inc.、2019年7月

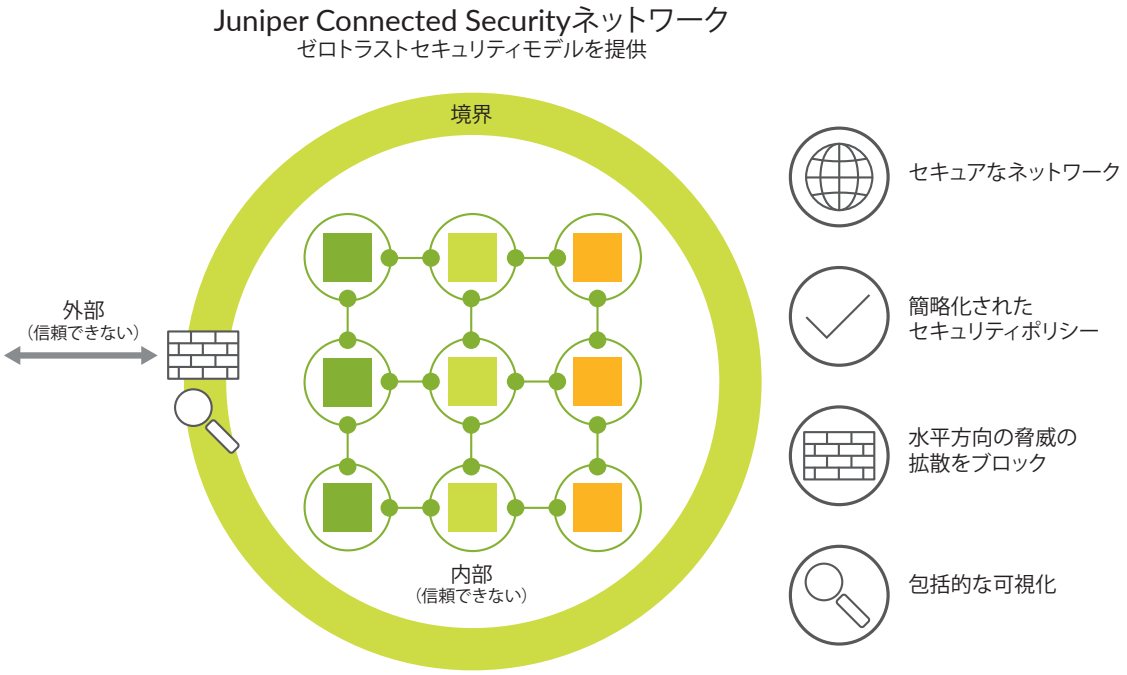

図4：Juniper Connected Securityによるゼロトラストアーキテクチャ

表1：ゼロトラストモデルの各柱をサポートするJuniper Connected Security

柱	ジュニパーの機能
データ	• ビジネスデータをネットワーク全体に安全に転送できるスタンダードベースの包括的なIPsec暗号化を提供 • マイクロセグメンテーションをサポート
ネットワーク	• ネットワークを単一のエンティティとして表示、保護、自動化 • サードパーティー製品を含むネットワークのすべてのポイントにセキュリティを拡張 • 堅牢なセグメンテーションゲートウェイ機能でマイクロセグメンテーションをサポート
ユーザー	• ユーザーアクセスの制御とポリシーの適用を非常にきめ細かく実行 • ユーザーインタラクションを保護
デバイス	• ユーザーのインテントベースのポリシーをサポートすることで、ネットワークデバイス（スイッチ、ルーター、ファイアウォール、およびその他のセキュリティデバイス）で情報やリソースを共有できるようにするとともに、脅威が検出された場合にネットワーク内で修復アクションを実行できるようにする
ワークロード	• 境界の奥深く、パブリッククラウド、およびその他の場所（最新のサービス提供モデルが組織のワークロードを処理する場所）で高度な防御を提供 • きめ細かいポリシー制御を可能にする
分析と可視性	• ユーザーおよびアプリケーション認識を含む、ネットワークトラフィックに対する可視性を提供 • セッション情報をリアルタイムに分析し、SPANポートを通じて、一元化されたリポジトリにパケットキャプチャを送信
自動化とオーケストレーション	• 自動化、機械学習、リアルタイムの脅威インテリジェンスを活用した統合型の防御を提供 • 共通のセキュリティポリシーを作成、導入、複製するためのプラットフォームで管理を簡略化し、新しいアプリケーションやサービスの実装を簡素化

まとめ

今日の脅威環境と最新のコンピューティング環境を考慮すると、あらゆる規模の企業と組織は今こそゼロトラストをその情報セキュリティ戦略の中心的な信条とするべきです。境界セキュリティの強化のみに依存し続ければ、企業やクラウド環境の両方でサイバー攻撃を受ける回数が増え続けることになります。

Juniper Connected Securityのメリットについて詳しくは、www.juniper.net/jp/ja/solutions/security/をご覧ください。

ジュニパーネットワークスについて

ジュニパーネットワークスは、世界をつなぐ製品、ソリューション、サービスを通じて、ネットワークを簡素化します。エンジニアリングのイノベーションにより、クラウド時代のネットワークの制約や複雑さを解消し、お客様およびパートナーの皆様が日々直面している困難な課題を解決します。ジュニパーネットワークスは、世界に変革をもたらす知識の共有や人類の進歩のリソースとなるのはネットワークであると考えています。私たちは、ビジネスニーズにあわせた、拡張性の高い、自動化されたセキュアなネットワークを提供するための革新的な方法の創造に取り組んでいます。

米国本社
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話番号：888. JUNIPER (888.586.4737)
または+1.408.745.2000
FAX：+1.408.745.2100
www.juniper.net

アジアパシフィック、ヨーロッパ、中東、アフリカ
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話番号：+31.0.207.125.700
FAX：+31.0.207.125.701

日本
東京本社ジュニパーネットワークス株式会社
〒163-1445 東京都新宿区西新宿3-20-2
東京オペラシティタワー45階
電話番号：03-5333-7400
FAX：03-5333-7401
西日本事務所
〒530-0001 大阪府大阪市北区梅田2-2-2
ヒルトンプラザウエストオフィスタワー18階
www.juniper.net/jp

Juniper Networks | Engineering Simplicity