JUNIPER NETWORKS | Driven by Experience™

AIドリブンキャンパスネットワーク

次の10年のキャンパスネットワークに人工知能を活用する

ホワイトペーパー

目次

概要

次の10年間のネットワークで重要となるのは、より良いユーザーエクスペリエンスを提供し、IT運用を簡略化することです。従来の有線/無線LANソリューションでは、今日の課題と多様な企業のニーズに対応するために必要な拡張性、信頼性、俊敏性が不足しています。

AIドリブンキャンパスネットワークは、クラウド、モバイル、IoTの時代においてAI（人工知能）を活用します。ジュニパーのキャンパスソリューションは、堅牢なハードウェアポートフォリオとMist AI™の優れた機能を組み合わせて、ネットワーク運用を合理化し、ユーザーエクスペリエンスを高め、ITチームが戦略上重要な取り組みに集中できるようにします。このホワイトペーパーでは、Mist AIが推進するエンドツーエンドのAIドリブンキャンパスネットワークのコンポーネントについて説明します。

はじめに

エンタープライズネットワークは、クラウドレディネットワークのニーズの増大や、多数のモバイルデバイスやIoTデバイスに対応するために、大きく変化しています。残念なことに、デバイスが増加するにつれ、複雑さも増大しています。クラウドベースのアプリケーションは、新しいビジネスモデルを可能にし、ビジネスの俊敏性を提供し、ユニファイドコミュニケーション、ビデオ、その他の遅延の影響を受けやすいアプリケーションなどの重要な技術の導入をサポートします。技術が進歩し、ML（機械学習）とAIが普及したことも、ITチームとエンドユーザー双方にとっての運用とエクスペリエンスの大幅な向上を可能にします。

ネットワークアーキテクトは、データ、音声、ビデオのクラウドレディアプリケーションの最新のビジネス要件に対応するために、オープンスタンダードとソフトウェア主導型管理プラットフォームを使用しながら、ネットワークの設計を変更して、運用コストを削減しています。自動化、テレメトリ、AIの機能を簡単な方法で活用して、今後10年のネットワークを構築することが、最終目標です。

ジュニパーAIドリブンキャンパスネットワーク

ジュニパーネットワークスのクラウドサービス、ソフトウェア製品、ハードウェア製品のポートフォリオは、エンドツーエンドのキャンパスネットワークソリューションを提供します。このソリューションは、WAN、LAN、Wi-Fi、セキュリティの分野に及びながらも、EVPN-VXLAN（イーサネットVPN-仮想拡張LAN）などのオープンスタンダードをサポートして、アーキテクチャの簡素性、拡張性、パフォーマンスを推進します。

ジュニパーのAIドリブンキャンパスネットワークは、以下で構成されています。

- 最新のマイクロサービスクラウドAIOpsプラットフォーム
- AIを活用したWi-Fi/有線スイッチング
- EVPN-VXLANを実行するキャンパスファブリック
- クラウドレディキャンパスイーサネットスイッチ
- Wi-Fi、Bluetooth LE、IoTを使用するエンタープライズグレードのアクセスポイント
- Juniper Connected Securityとネットワークセグメンテーション
- Junos®オペレーティングシステム
- Junos Telemetry

最新のマイクロサービスクラウドAIOpsプラットフォーム

Juniper® Mistクラウドアーキテクチャは、マイクロサービスを中心に構築されており、優れた俊敏性、拡張性、耐障害性を実現します。クラウドサービスは、必要に応じて柔軟にスケールアップおよびスケールダウンして、モノリシックなハードウェアのコストを削減して複雑さを解消します。ネットワークを中断することなく、新しい拡張機能やバグ修正をほぼ毎週提供できます。オープンAPIを利用し、100%プログラム可能で、完全に自動化して、サードパーティの補完的製品とシームレスに統合できます。Juniper Mistクラウドアーキテクチャは、AI、ML、データサイエンスを最新のマイクロサービステクノロジーと組み合わせてエンタープライズネットワークに革新的なアプローチをもたらし、他に類を見ないソリューションを提供します。

AIを活用したWi-Fi/有線スイッチング

ジュニパーはMist AIをキャンパスネットワークに適用して、有線/無線の統合ソリューション全体でユーザーエクスペリエンスを最適化し、IT運用を簡略化します。従来のソリューションは15年以上前のものであり、拡張にコストがかかり、バグが発生しやすく、管理がしにくいモノリシックなコードベースを利用しています。ユーザーエクスペリエンスは、かつての稼働時間に代わり、ネットワークインフラストラクチャの成否を測るうえで最も重要な指標となっています。ジュニパーはどう対処しているのでしょうか。

Juniper Mist Wi-Fi Assuranceは、手動のトラブルシューティング作業を自動化された無線操作に置き換えることで、Wi-Fiの予測、信頼性、測定を可能にし、ユーザーのサービスレベルを可視化します。異常が検知されると、イベントの関連付けを目的としたパケットのキャプチャが自動的に開始します。クライアントレベルのRRM（無線リソース管理）でネットワークのインテリジェンスを構築しながら、無線ネットワークによるユーザーエクスペリエンスの可視性を従来よりも向上させます。

Juniper Mist Wired Assurance（図1を参照）は、有線デバイスについてもAIを活用して自動化します。Juniper Networks® EXシリーズイーサネットスイッチから収集した豊富なJunos Telemetryデータを活用して、運用の簡略化、MTTR（平均修復時間）の短縮、IoTデバイス、サーバー、プリンターなどのエンドユーザーエクスペリエンスの可視性向上を実現します。Juniper Mist Wired Assuranceは、Juniper Mistクラウドアーキテクチャからのオンボーディング、プロビジョニング、管理まで、EXシリーズのスイッチングのあらゆる面を簡略化します。

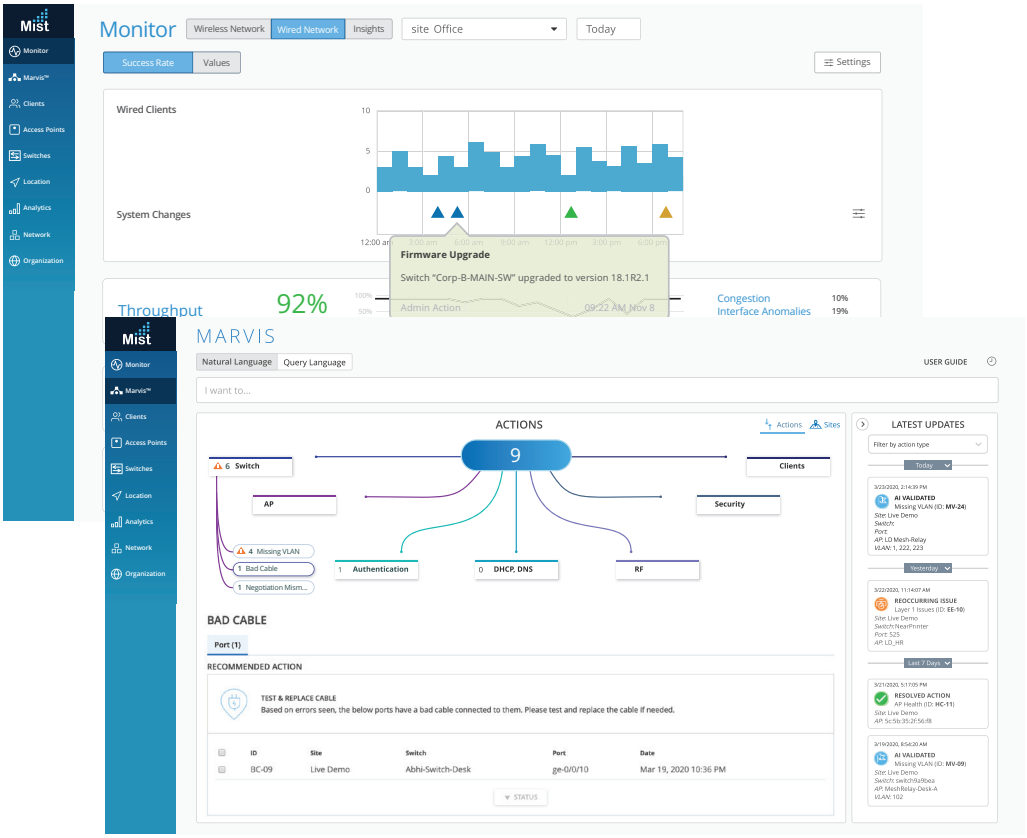

図1：Wired Assuranceと仮想ネットワークアシスタントMarvis

仮想ネットワークアシスタントMarvis（図1）は、WLAN、LAN、WANの各エンタープライズネットワーク専用にMist AIを使用して構築されています。自然言語を適用しているため、ユーザーがMist AIと直接対話できます。これにより、ネットワーク運用は事後対応型のトラブルシューティングから自動運転のアクションによる事前対応型の修復へと変化します。Marvisは、IT部門の効率性を高め、サポートチケット数を最小化し、解決までの時間を短縮します。AIOps（AI for IT Operations）の導入が加速し続ける中、Marvisは、企業が効率的かつ正確に大規模なIT管理を行うのをサポートします。

キャンパスファブリック

キャンパスでIoTデバイスの使用が増加するということは、これ以上複雑にせずに、ネットワークを迅速に拡張する必要があるということです。IoTデバイスの多くは、ネットワーキング機能に限界があり、建物あるいはキャンパス間でL2隣接関係を必要とします。ただしL2は、ループ、障害後のコンバージェンス速度の低下、データプレーンのフラッディングによるセキュリティの懸念事項の原因となります。セキュリティ上の問題は従来独自のプライベートVLANによって解決していましたが、ループやコンバージェンスが遅いという他の問題がL2ネットワークに残っていました。しかし、このアプローチは、ネットワーク帯域幅の過剰な消費のため、非効率で管理が困難です。また、VLANを新しいネットワークポートまで拡張する必要があるため、管理が難しくなっています。

EVPN-VXLAN

AIドリブンキャンパスアーキテクチャは、オープンスタンダードであるEVPN（イーサネットVPN）とVXLAN（仮想拡張LAN）などのテクノロジーを使用して、オーバーレイネットワークをアンダーレイから分離します。したがって、ネットワークのループがなくなってコンバージェンスが速くなります。また、ネットワーク管理者は異なるL3ネットワーク間に論理L2ネットワークを作成してエンタープライズネットワークの最新ニーズに対処できます。EVPN-VXLANでは、IoTデバイス間のトラフィックを分離してマイクロセグメンテーションを可能にし、セキュリティを強化することもできます。ジュニパーは、以下の検証済みEVPN-VXLANキャンパスファブリックに対応しています。

- **EVPNマルチホーミング（折り畳んだコアまたはディストリビューション）：**ネットワークのディストリビューションにおけるEVPNマルチホーミングにより、スイッチからディストリビューションのデバイスペア間のLAGにアクセスできるようになります。アクセスレイヤーからディストリビューションレイヤーまでマルチホーミング機能を提供することで、キャンパスネットワーク全体でSTPY（スパニングツリープロトコル）が不要になります。このため、ディストリビューションレイヤーと折り畳んだ状態のコアレイヤーが可能になります。
- **キャンパスファブリックコアディストリビューション：**2台のEXシリーズにおけるコアスイッチまたはディストリビューションスイッチを相互に接続することで、L2 EVPNとL3 VXLANゲートウェイをサポートします。ディストリビューション層とコア層の間のIP Closネットワークには、2つのモードがあります。中央部または端面でルーティングされたブリッジングオーバーレイです。
- **キャンパスファブリックIP Clos：**キャンパスファブリックIP Closアーキテクチャは、VXLAN L2ゲートウェイ機能をアクセスレイヤーまで延長し、標準に基づいたグループベースのポリシーを使用したマイクロセグメンテーションを実現します。

エンドツーエンドのEVPN-VXLANアーキテクチャでは、キャンパスとデータセンターを単一のIPファブリックとして管理し、ジュニパーが提供するOTT（Over-the-Top）ポリシーおよびコントロールを利用することが可能です。また、ネットワーク全体でグループベースのポリシーを使用してポリシー適用を簡略化します。スイッチは何台でもClosネットワークやIPファブリックに接続することができます。EVPN-VLANがファブリックを拡張して企業の建物を複数接続し、VXLANはネットワーク全体にL2を拡張します。

詳細については、www.juniper.net/assets/us/en/local/pdf/solutionbriefs/3510643-en.pdf（英語）をご覧ください。

ジュニパーは、EVPN-VXLANベースのアーキテクチャ以外にバーチャルシャーシテクノロジーもサポートし、最大10台の相互接続したスイッチを、1つのIPアドレスを持つ1台の論理デバイスとして運用できます。バーチャルシャーシテクノロジーを使用すると、エンドポイントの論理グループから物理トポロジーを分離して、リソースを効率的に利用できます。

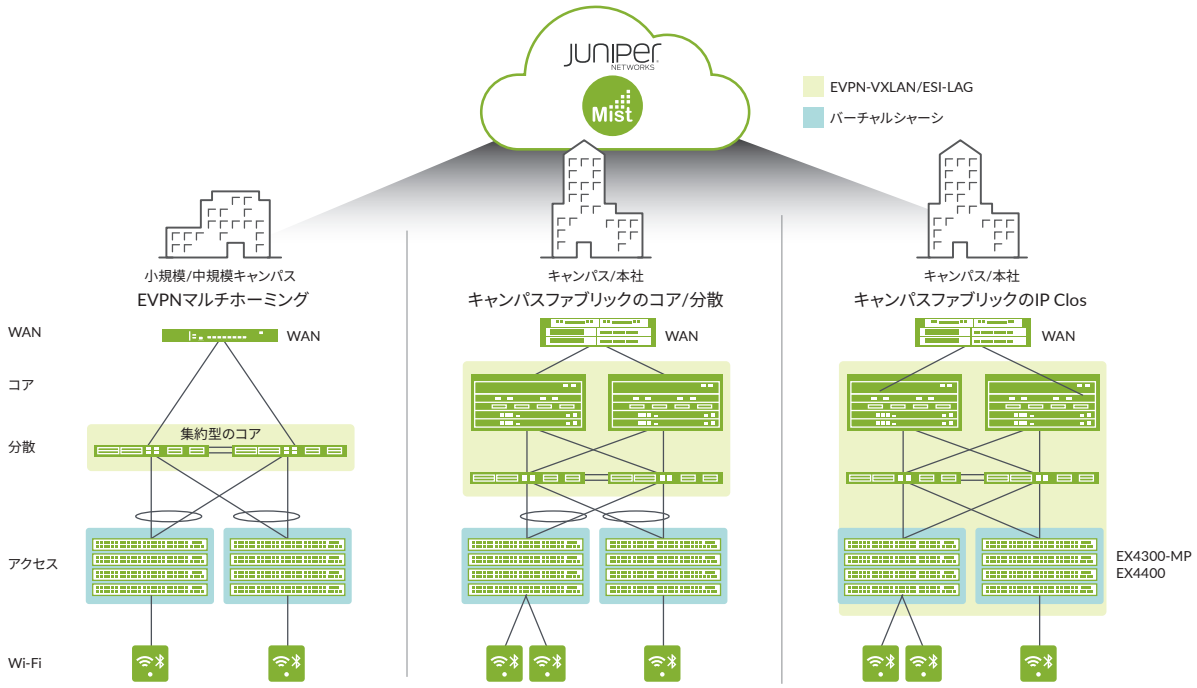

図2：バーチャルシャーシやEVPN-VXLANベースのアーキテクチャを採用したキャンパスファブリック

クラウドレディキャンパスイーサネットスイッチ

ジュニパーは、エンタープライズキャンパスネットワーク向けのコア/ディストリビューションスイッチのAIドリブン、プログラム可能、オープンのポートフォリオを提供しています。アクセススイッチはクラウドに対応し、Juniper Mist Wired Assuranceをサポートし、アクセスレイヤースイッチングのAIOpsを可能にします。スイッチは以下のさまざまなキャンパス要件を満たします。

- クラウドレディ、Juniper Mistクラウドアーキテクチャによる管理
- マルチギガビットのサポート
- MACsec（Media Access Control Security）AES256
- パワーオーバーイーサネット（PoE/PoE+/PoE++）
- バーチャルシャーシおよびEVPN-VXLANによる拡張性のあるファブリックアーキテクチャ
- マルチベンダーサポート
- GBP（グループベースのポリシー）を使用した標準に基づくマイクロセグメンテーション
- フローベーステレメトリ

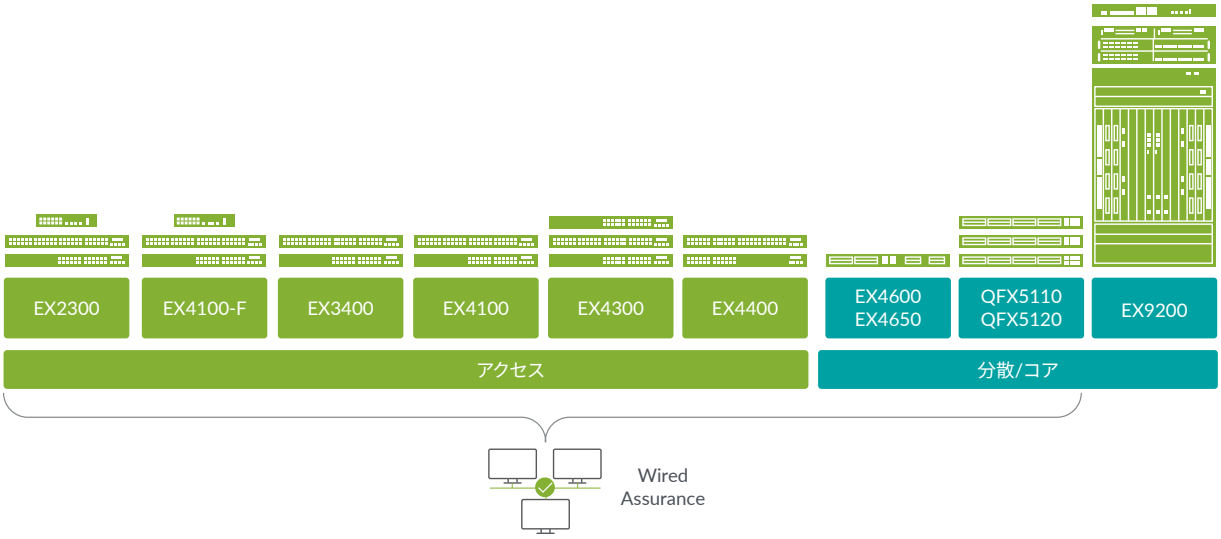

図3：EXシリーズとQFXシリーズスイッチのキャンパスポートフォリオ

AIドリブンキャンパスファブリックの導入

キャンパスファブリックを手動で構成すると、導入の一貫性が失われたり、凡ミスが発生したりすることがあります。ジュニパーは、Juniper Mistクラウドによって EVPN-VXLANキャンパスファブリックの管理を簡単にすることで、この運用上の負荷を解消します。具体的には、管理者はトポロジーを選択し（EVPNマルチホーミング、分散-コア、IP CLOS）、それ以外の操作をソフトウェアに実行させることができます（図4を参照）。このAIドリブンアプローチは、キャンパスと支社/拠点におけるLAN、WLAN、WAN環境間の管理を統合しながら、有線/無線キャンパスネットワークの優れたユーザーエクスペリエンスを確保します。

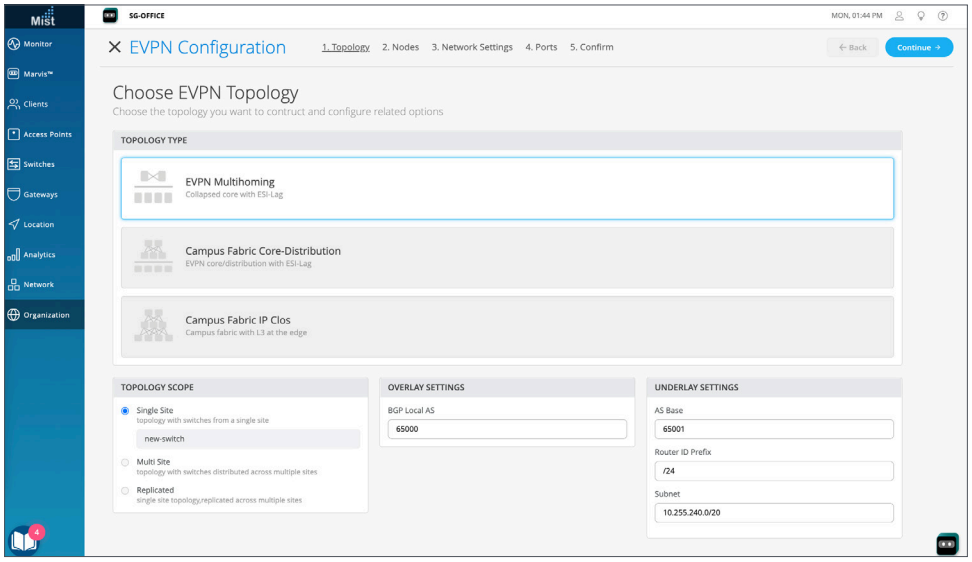

図4：Juniper Mist Wired Assuranceキャンパスファブリック設計

*当初はEVPNマルチホーミングがサポートされ、追加のアーキテクチャは将来のリリースでサポートされます。

AIドリブンキャンパスファブリックの運用

Juniper Mist™ Wired Assuranceは、クラウドで管理されるEXシリーズイーサネットスイッチの請求、構成、管理、トラブルシューティングを実行します。このクラウドベースのサービスは、AIを活用した自動化とサービスレベルにより、接続デバイスのエクスペリエンスを確実に向上させます。Juniper Mist Wired Assuranceは、Junos®オペレーティングシステムの豊富なスイッチテレメトリデータを活用して、運用の簡略化、平均修復時間の短縮、可視性の向上を実現します。Day 0からDay 2までのオペレーションの主要な特徴は、以下のとおりです。

- **Day 0のオペレーション**ーグリーンフィールドスイッチを請求したり、ブラウンフィールドスイッチを1つのアクティベーションコードで導入したりすることで、スイッチをシームレスにオンボーディングし、本当の意味でプラグアンドプレイのシンプルさを実現します。
- **Day 1のオペレーション**ーテンプレートベースの構成モデルを実装し、従来のファブリックやキャンパスファブリックの展開を一括して行うことができます。一方で、サイトあるいはスイッチ固有のカスタム属性を適用するために必要な柔軟性と制御性も維持されます。ダイナミックポートプロファイルによるポートのプロビジョニングを自動化します。
- **Day 2のオペレーション**ーJuniper Mist Wired AssuranceのAIを活用し、接続前と接続後の主要な指標を使用しながら、スループット、接続の成功、スイッチの健全性などのサービスレベルの期待事項を満たします（図5を参照）。Marvis Actionsの自動運転機能を追加すると、ループの検出、不足しているVLANの追加、設定ミスのポートの修正、不良ケーブルの特定、フラッピングポートの隔離、および持続的に欠落しているクライアントの発見などが可能になります（図6を参照）。また、Juniper Mistクラウドを利用して、ソフトウェアのアップグレードを簡単に行うことができます。

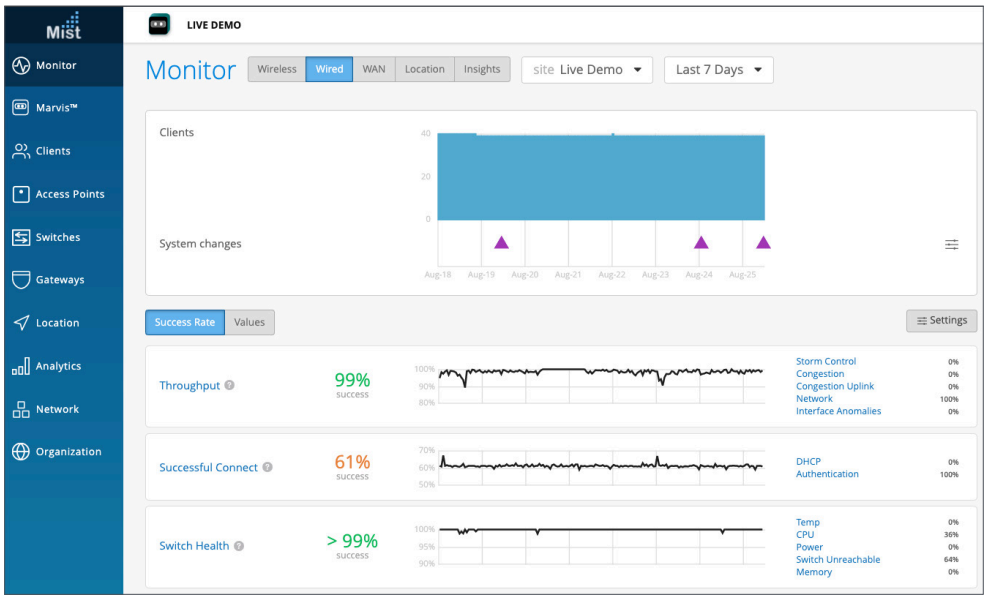

図 5：Juniper Mistのサービスレベル期待値（SLE）

図 6：有線スイッチに対応したMarvisアクション

詳細については、Juniper Mist™ Wired Assuranceをご覧ください。

エンタープライズグレードのWi-Fiアクセスポイント

ジュニパーは、エンタープライズグレードのアクセスポイントで、Wi-Fi、BLE（Bluetooth Low Energy）、IoTのコンバージェンスをリードしています。これらの製品は、機械学習とイベントの関連付けを活用して、データ収集、分析、ポリシー適用の機能を提供します。Juniper AP 43/AP 45シリーズ高パフォーマンスアクセスポイントは、特許取得済みの動的vBLE 16エレメントアンテナアレイを備えており、業界をリードする精度と拡張性のロケーションサービスを可能にします。ジュニパーアクセスポイントは、Mist AIに流入する150を超える状態に関するメタデータを収集する目的で構築されています。

特長	AP45	AP34	AP43	AP63	AP33	AP32	AP12
Wi-Fi規格	Wi-Fi 6E 802.11ax（Wi-Fi 6）4x4：4SS	Wi-Fi 6E 802.11ax（Wi-Fi 6）2x2：2SS	802.11ax（Wi-Fi 6）4x4：4SS	802.11ax（Wi-Fi 6）4x4：4SS	802.11ax（Wi-Fi 6）5GHz：4x4：4SS 2.4GHz：2x2：2SS	802.11ax（Wi-Fi 6）5GHz：4x4：4SS 2.4GHz: 2x2：2SS	802.11ax（Wi-Fi 6）2x2: 2SS
アンテナオプション	内部/外部	内部	内部/外部	内部/外部	内部	内部/外部	内部
仮想BLE	✓	—	✓	✓	✓	—	—

Juniper Connected Security

ZDNetのレポートによると、2020年にFBIに報告された攻撃件数は前年と比較して69%増加しました。今では、規模に関係なくどの企業にとっても、効果的なセキュリティ戦略を立てることの重要性が従来よりも増しています。ネットワークの防御態勢を維持するためには、全体像を把握する必要があります。何を保護するか、何から保護するかの両方の点において、可視化するうえで大きなギャップが存在することは許容できません。業界は、過去10年間にネットワークセキュリティのイノベーションを数々実現してきましたが、攻撃の成功件数は減少していません。キャンパスのすべての接続ポイントでセキュリティを確保するために何が必要であるかは明白です。AIを活用した防御態勢を取ると、迅速かつ効果的にネットワークが自己防衛できるようになります。

Juniper® Connected Securityは、セキュリティの可視性、インテリジェンス、ポリシー適用を、クライアントからワークロードにいたるまで、ネットワーク上のあらゆる接続ポイントに拡張します。すべての接続ポイントでキャンパスネットワークに誰が、あるいは何がアクセスしているかを把握し、AIを活用してその瞬間のリスクを見極めます。これにより、リスクを緩和できるとともに、キャンパスの保護とキャンパスリソースへの確実なアクセスとの間でバランスを取ることができます。

データセキュリティでは、次の2点を対象にする必要があります。データセンターのデータと、エッジのデータへのアクセスです。ゼロトラストの他の要素はすべてデータとデータへのアクセスを保護するように設計されていますが、データを保護するためには、転送中の暗号化、保存時の暗号化、セキュアな接続が必要です。

- Secure Vector Routingは、ルーティングベクトルに基づいたセグメンテーションを可能にするため、攻撃者による転送中のデータ傍受が著しく困難になります。
- Secure Connectは、どこからの接続に対してもZTNA（Zero Trust Network Access）を実行し、接続をプライベートトンネル内でカプセル化します。
- インテントベースのセキュリティコントロールは、Junos自動化によりパブリッククラウド環境内のデータセキュリティポリシー適用を自動化します。たとえば、新しく作成したAmazon S3バケット内のデータはすべて、保存時に暗号化され、承認済みデータアクセス権が適用されます。ルールを手動で作成する必要はありません。

ネットワーク

ネットワークのポイント間を移動するパケットは、合法的なこと、エクスプロイトやマルウェアを含まないこと、ポイントAからポイントBへの移動を承認されていることが必要です。悪意のあるコンテンツがないか、トラフィックのインスペクションやプロファイリングが実行される必要があります。

次世代ファイアウォール（NGFW）は、トラフィックのインスペクションに最適なソリューションに進化しました。トラフィックに悪意があるかどうかを判断するために、パケットのヘッダーと本文やパケットのグループには通常シグネチャが適用されますが、AIならば未知のファイル、システム、動作、トラフィックパターンを迅速に評価して、攻撃が試行されているかどうかを判別できます。

ジュニパーネットワークスのSRXシリーズサービスゲートウェイは、ネットワークトラフィックを可視化してコントロールする以外にも、以下のようなAIドリブンセキュリティサービスを活用して既知や未知の脅威と戦うセキュリティ機能を装備しています。

- 新しいマルウェアに対する脅威防御。Juniper ATP Cloudは、機械学習を使用して実行時のファイルの動作を把握することで、未知のファイルを迅速に評価し、マルウェアやグレイウェアかどうかを判別します。
- 復号化を必要としない可視性とコントロール。ATP Cloudはまた、使用されている証明書の重要なコンポーネントやトラフィックの動作を把握することで、暗号化されたネットワークトラフィックや、IoTなどの接続デバイスのリスクを評価します。

人/ユーザー

キャンパスのユーザーは、内部リソースとインターネット上のリソースにアクセスします。ユーザーは攻撃ベクトルになる可能性があり、リスクを抑えるためには、ユーザーのアクセスをコントロールし、認証する必要があります。

SRXシリーズゲートウェイでユーザーベースのポリシーを使用すると、内部または外部のあらゆるリソースを対象に、アクセスをきめ細かくコントロールできます。SRXシリーズは、IDプロバイダと連携し、ユーザーがどこにいてもセキュアなアクセスとセキュリティポリシーが適用されるようにします。さらにATP Cloudが、ユーザーのアカウントが侵害されているかどうかを評価し、適切なセキュリティポリシーやVLANになるように動的に調整を実行して、必要な場合は認証を強化します。

ワークロード

ワークロードは、一時的な場合もありますが、アプリケーションを構成するコンポーネントです。ワークロードをアプリケーションのエクスプロイトから保護することと、他のワークロードから分離してセグメント化することは、データセンター内の貴重なデータを守るうえでの最終防衛線として、適切な方法です。

- Cloud Workload Protectionは、あらゆるクラウド環境やオンプレミス環境において、またゼロデイエクスプロイトの発生時において、アプリケーションワークロードを自動的に保護します。これにより、本番環境のアプリケーションは常に脆弱性の悪用に対するセーフティネットを確保できるようになり、ビジネスクリティカルなサービスは接続を維持され、耐障害性が確保されます。手動で介入する必要はなく、ランタイムアプリケーション保護などの機能で、マイクロセグメンテーションを活用して、個々のデータベース、データコレクター、個々のリソースのすべてが保護されます。
- ジュニパーネットワークスのcSRXコンテナファイアウォールは、個々のアプリケーションに出入りするトラフィックをセグメント化してコントロールするという方法で、コンテナ化されたファイアウォールによりアプリケーションを保護します。

デバイス

キャンパスからネットワークに接続するデバイスは、可視性に課題があります。ユーザーのデバイス、一時的なサーバー、IoTデバイスなどが対象になるためです。IoTデバイスは、キャンパスのいたるところにあります。インターネットに接続している自動販売機、コーヒーポット、プリンターなどです。IoTデバイスの場合、ユーザーベースのデバイスとは異なり、適切なレベルのネットワークアクセス権や現在のデバイスの状況を特定することは困難です。IoTデバイスはエンドポイントエージェントを装備していない場合があるためです。

- ATP Cloudは、ネットワークに関するジュニパーの脅威インテリジェンスの中心的存在です。接続デバイスのリスク評価、デバイスのタイプ（IoTを含む）の特定、そして接続デバイスのセキュリティが侵害された場合には適切なアクションのオーケストレーションを実行します。

ATP Cloudは、ゼロトラストネットワーク内のデバイス保護に役立つ以下の機能を装備しています。

Mist AIによるリスクプロファイリング

分散型アクセスネットワークのエッジにネットワークセキュリティを提供します。ネットワークを詳細に可視化し、ネットワーク上のすべての接続ポイントでポリシーの適用を可能にすることで、ITチームがインフラストラクチャを防御できるようにします。キャンパスネットワークは、脅威を認識するネットワークの一部として、防御に積極的に対応します。

Mistに対応したセキュリティインテリジェンス

SRXシリーズとATP Cloudによって検知された脅威アラートが、ユーザーやデバイスが無線ネットワークに接続したときにセキュリティリスクを迅速に評価し、適切なアクション（隔離やポリシーの適用など）を実行します。

EXシリーズ向けSecIntel

ATP Cloudは、デバイスのセキュリティ侵害情報をEXスイッチに送信します。このため、感染したデバイスのブロックまたは隔離をスイッチにおいて実行できます。エンドポイントエージェントが存在しなくても、デバイスをコントロールできるようになっています。

分析と自動化

ネットワークで起こっていることを可視化できれば、半分戦いに勝ったようなものです。可視化してインテリジェンスを収集し、それでゼロトラストポリシーを強化すると、リスクをさらに緩和しつつ、ネットワークチームとセキュリティチーム内部での拡張性も実現します。可視性は以下の手段で得ることができます。

- Security Director Cloud - オンプレミス、クラウドベースのセキュリティコントロール、クラウドで提供されるセキュリティコントロールを、1つのユーザーインターフェイスから管理します。Security Director Cloudを使用すると、ユーザー、デバイス、アプリケーションが場所を移動しても、セキュリティポリシーを確実に適用できます。可視性や脅威に対する保護手段を失うことはありません。セキュリティポリシーは、一度作成したら、場所が変わってもあらゆるユーザー、デバイス、アプリケーションに拡張できます。
- Security Director Insights - 進行中の攻撃を強調表示し、検知内容をMitre ATT&CKフレームワークにマッピングするSecurity Directorの機能です。サードパーティのあらゆるセキュリティツールのインテリジェンスと検知情報を取り込みます。その後、Security Directorで直接、またはAnsible自動化を介して適切なアクションを定義し、ネットワーク内の他のツールにオーケストレーションを提供できます。
- Junos自動化 - 堅牢なAPI群やその他のネイティブの自動化要素を搭載したジュニパーのJunosオペレーティングシステムによって、自動化が強化されています。企業は、ジュニパーのプラットフォーム全体に及ぶほぼすべてのプロセスや機能のパフォーマンスについて、独自の方法でコントロールと構成ができ、また監査もできるようになります。この場合、プログラムによってJunosを活用し、運用を簡素化します。プロセスのチケット要求や顧客の変更要求を自動化すると同時に、アーキテクチャ全体の健全性を確保することで、CapExとOpExの両方を削減できます。

キャンパスネットワークのセグメンテーション

ネットワークアーキテクトは、データと資産を保護するために、マイクロセグメンテーションやマクロセグメンテーションなどの手法を組み合わせることができます。普遍的なEVPN-VXLANアーキテクチャをキャンパスとデータセンターにわたって拡張して、エンドポイントとアプリケーションの一貫したエンドツーエンドのネットワークセグメンテーションを構築できます。このため、レイヤー2フラッディングを最小限に抑えて、セキュリティの脅威を低減し、ネットワークを簡略化することもできます。

- マイクロセグメンテーションとは、共有ネットワークデバイス内のネットワークと共有リンク間のネットワークの論理的な分離のことです。これをEVPN-VXLANネットワーク内で実現するためには、レイヤー2でVLANを使用し、レイヤー3でVRF（仮想ルーティング/転送）を使用します。VRFは互いに分離された2台のVRFデバイス間のIPトラフィックを維持することで、分離を実行します。
- マイクロセグメンテーションでは、リスクを緩和し、セキュリティニーズに対処することで、ネットワーク保護の重大な問題に対応します。ジュニパーは、ACL（アクセスコントロールリスト）またはファイアウォールフィルターに基づいてマイクロセグメンテーションを実装し、仮想化ネットワーク間のトラフィックをコントロールします。

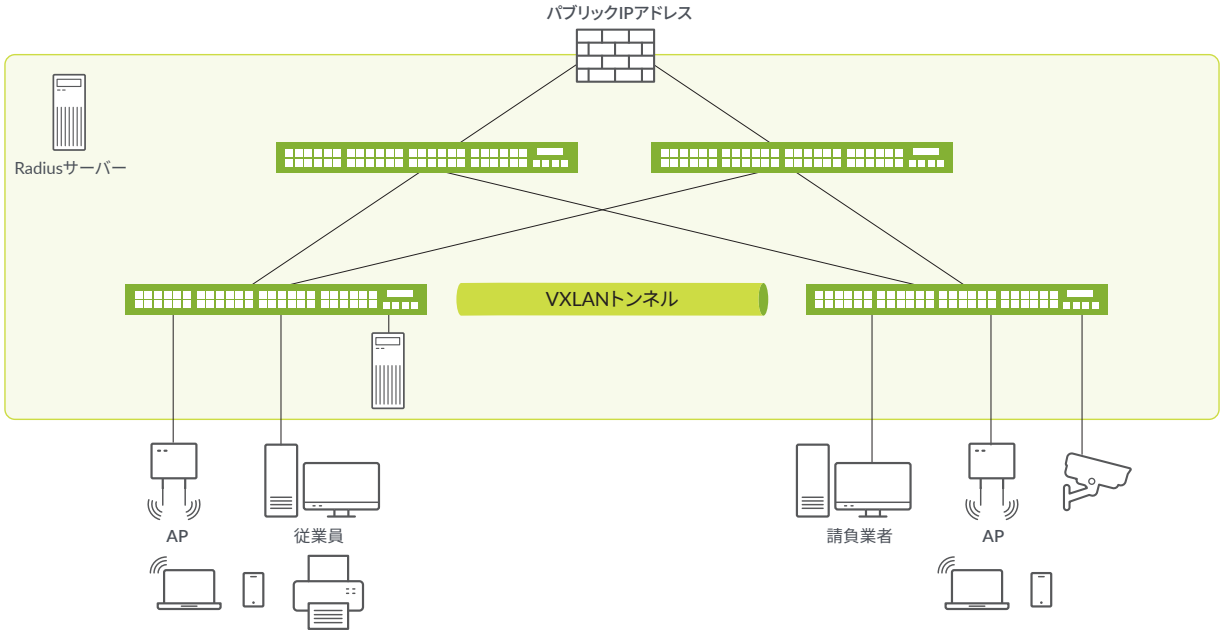

図7：従業員またはIoTデバイスに基づくネットワークセグメンテーション

Junos OS: 高パフォーマンスネットワークの基盤

Junos®オペレーティングシステムは、ジュニパーのルーティング、スイッチング、セキュリティのデバイス間に共通する言語のようなものです。Junos OSだけで、高パフォーマンスネットワークの複雑さを解消して、可用性を高め、サービスを迅速に導入しながら、TCOを削減できます。ユーザーエクスペリエンスが一貫し、Junos OSのツールセットが自動化されるため、計画策定とトレーニングが簡単になるとともに、日常の運用効率が向上し、ネットワーク全体にすべての変更を迅速に実装できます。

Junos OSは、他のネットワークオペレーティングシステムとは異なり、1つのオペレーティングシステムが1つのモジュラー式アーキテクチャで構築され、1回のソフトウェアリリースで提供されます。主なメリットは以下のとおりです。

- 1つのオペレーティングシステムがあらゆるタイプと規模のプラットフォームにおいて、ネットワークとセキュリティのインフラストラクチャの計画、導入、運用に伴う時間を短縮し、手間を軽減します。
- 1つのリリーストラックで、新機能を実績ある一定の間隔で安定的に提供して、ソフトウェアニーズの変化に対応します。
- 1つのモジュール式ソフトウェアアーキテクチャが、高可用性、セキュア、拡張可能で、自動化とパートナーのイノベーションを妨げないソフトウェアを提供します。

Junos Telemetry

運用の健全性に関する統計を収集する従来のデータモデルでは、ネットワークの拡張性と効率性が限界に達しています。Junos Telemetry Interfaceは、プッシュモデルによりデータを非同期的に提供することで、ポーリングをなくし、限界を克服します。その結果、拡張性が高く、ネットワーク内の数千のオブジェクトを監視できます。

Junos Telemetry Interfaceを利用すると、物理インターフェイスやファイアウォールフィルターなど、さまざまなシステムリソースのデータの収集やエクスポートのために、センサーをプロビジョニングできます。以下の2つのデータモデルがサポートされます。

- ジュニパーネットワークスが定義したオープンで拡張可能なデータモデル。このモデルは分散型のアーキテクチャを特長とし、簡単に拡張できます。
- ユニバーサルキー/値形式のGPB（Google Protocol Buffer）構造化メッセージとしてデータを生成するOpenConfigデータモデル。gRPCリモートプロシージャーコールはTCPをベースにしており、SSL暗号化をサポートするため、セキュアかつ信頼性が高いと見なされています。

まとめ

ジュニパーのAIドリブンキャンパスは、柔軟性が高く、スタンダードベースの将来のクラウドに対応した最新アーキテクチャをお客様に提供するように設計されています。信頼性、セキュリティ、俊敏性を損なうことなく、現在の厳格な要件を満たします。共通の構成要素、パッケージ済みの自動化ワークフロー、カスタムの自動化ツールキットが、予測分析のメリットをデータセンターからキャンパス、さらにその先にまで広げます。

追加資料

- キャンパス設計センター（英語）
- EXシリーズファミリーのWebページ
- Juniper Mistクラウドサービス
- Juniper Connected Security
- ライブデモ：Wired WednesdayとWireless Wednesday（英語）
- ライブデモ：AIドリブンエンタープライズ
- Juniper Connected Security

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、ネットワーク運用を劇的に簡素化し、エンドユーザーに最上のエクスペリエンスを提供することに注力しています。業界をリードするインサイト、自動化、セキュリティ、AIを提供する当社のソリューションは、ビジネスで真の成果をもたらします。つながりを強めることにより、人々の絆がより深まり、幸福、持続可能性、平等という世界最大の課題を解決できるとジュニパーは確信しています。

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：+31.207.125.700
FAX：+31.207.125.701

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

日本
ジュニパーネットワークス株式会社
東京本社
〒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
https://www.juniper.net/jp/jp/

2000752-006-JP 2022年7月