Cisco Customer Experience

やわらかいインフラ

ホワイトペーパー SP 版

---2030 年を見据えた SP インフラの理想像---

Version 1.0

Cisco Systems, Inc.
Corporate Headquarters

170 West Tasman Drive
San Jose, CA 95134-1706 USA

Phone: +1 408-526-4000
Toll Free: +1 800-553-NETS (6387)

目次

図目次

本書について

著者

Name	Title
Kazufumi Kosuge	Leader, Customer Delivery, Cisco Customer Experience
Takanori Matsui	Customer Delivery Engineering Technical Leader, Cisco Customer Experience
Yusuke Togashi	Customer Delivery Architect, Cisco Customer Experience
Toshiki Hayashi	Customer Delivery Architect, Cisco Customer Experience
Ryosuke Aoshika	High Touch Engineer, Cisco Customer Experience
Masato Sekiguchi	Customer Delivery Security Architect, Cisco Customer Experience
Ken Takashima	Security Consulting Engineer, Cisco Customer Experience

履歴

Version	Date	Status	Reason for Change
1.0	June 2024	Release Version	Initial Release

1 はじめに

このホワイトペーパーでは、シスコがビジネスや環境の変化に合わせて動的にインフラを拡張・運用できる「やわらかいインフラストラクチャ」（以下、やわらかいインフラ）について、その機能や特徴、利用方法などを解説します。やわらかいインフラとは、シスコのカスタマーエクスペリエンス部門（CX）のエンジニアが社内で使用してきた用語で、クラウド時代の DX プラットフォームを意味しており、ネットワーク業界だけでなく IT 全体において将来の課題に備え、リスクに対応可能な概念を表しています。

本ホワイトペーパーでは、技術部門の責任者やソリューション選定に携わる方々に向けて、やわらかいインフラという概念がどのような課題から必要とされ、どのような特長を持つのか、また具体的な活用例や導入する際の注意点、期待できる導入効果などを解説しています。

本ホワイトペーパーを通じて、やわらかいインフラについてより深く理解し、導入することで得られるメリットや効果について、共通のイメージを持てればと思います。

2 2030 年に向けた通信業界動向

現在の状況から見た 2030 年以降の要件

近年、通信業界に大きな革新をもたらしたものに 5G があります。5G は、IoT、AI、自動運転車、遠隔医療などの新しいテクノロジーの普及を可能にしてきました。しかし、5G の全面的な展開が進む中で、通信業界はすでに次のステップである Beyond 5G や 6G、 ITU-T Network 2030 等、2030 年の未来に向けた準備を始めています。

Beyond 5G の導入は、5G をさらに高度化させることで、通信インフラをあらゆる産業や社会活動の基盤へと進化させる可能性があり、新たな技術や規格の開発に向けた取り組みが進められています。これには、超高速・大容量通信、超低遅延、多数接続、自律性、超安全・信頼性をさらに向上させることが含まれます。これらの新しい通信技術は、AI や IoT がさらに普及し、自動運転車や遠隔医療、スマートシティなどのテクノロジーが一般化する未来を見据えたものです。

総務省が開催した「将来のネットワークインフラに関する研究会」の報告書によると、2030 年までに求められる主な要求条件は以下の通りです。

- 超高速・大容量

IoT デバイスやビッグデータ分析の増加、新たなサービス（VR、AR、自動運転車等）の需要増に対応するため、大量のデータを高速に伝送できるネットワークが必要になります。

- 低消費電力

環境負荷の軽減とデバイスのバッテリー寿命の延長のため、エネルギー効率の良い通信技術が求められます。

- 超低遅延

リアルタイム性が求められる遠隔操作や遠隔医療、自動運転車などのアプリケーションにおいて、遅延のない通信が必要となります。

- 多数接続

IoT が普及し、大量のデバイスがネットワークに接続する状況を想定し、それら全てのデバイスを同時に接続・管理できるネットワークが求められます。

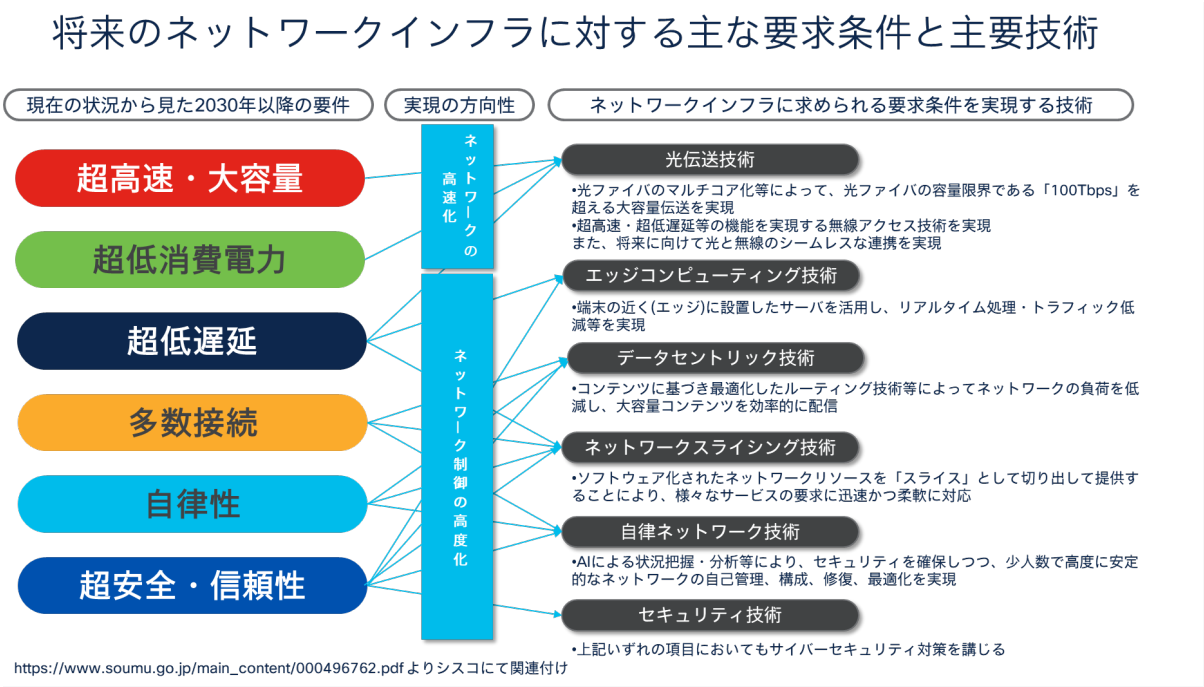
- 自律性

ネットワークが自己診断や自己修復を行い、ネットワークの適応性と効率性を高めていくことが求められます。これにより、通信品質の維持やトラフィックの最適化が可能となります。

- 超安全・信頼性

高度化する通信技術は新しいセキュリティリスクも生み出します。お客様のプライバシーやデータを保護するために、セキュリティの強化が必要になります。また、クリティカルな通信（例えば、遠隔医療や自動運転車）を支えるためには、ネットワークの信頼性が重要となります。

図 1 将来のネットワークインフラに対する主な要求条件と主要技術



ネットワークインフラ要件を実現する技術

次に新たなネットワークインフラ技術の開発に注目してみましょう。これには光伝送技術、エッジコンピューティング技術、データセントリック技術、ネットワークスライシング技術、自律ネットワーク技術、セキュリティ技術などが挙げられます。これらの技術は、将来の通信インフラをあらゆる産業や社会活動の基盤へと進化させるための重要な要素になります。

- 光伝送技術

光伝送技術は、光ファイバを通じて情報を高速に伝送する技術です。これにより、大容量データへの対応が可能になります。将来のインフラでは、超高速・大容量通信が求められるため、この技術が重要となります。

- エッジコンピューティング技術

エッジコンピューティング技術は、データをネットワークの末端（エッジ）で処理する技術です。これにより、データの遅延を減らし、リアルタイム処理やプライバシー保護を強化します。超低遅延や高度なセキュリティを要求する将来のインフラ環境では、この技術が必要となります。

- データセントリック技術

データセントリック技術は、データを中心にシステムを設計・運用する技術です。これにより、データの効率的な活用や管理が可能になると期待されています。大量のデータを効率的に処理・伝送する必要がある将来のインフラでは、この技術が重要となります。

- ネットワークスライシング技術

ネットワークスライシング技術は、1 つの物理的なネットワークを複数の仮想的なネットワークに分割する技術です。これにより、各仮想ネットワークがそれぞれ異なるサービスやアプリケーションに最適化され、多様な需要に対応できます。多数接続や自律性を求める将来のインフラでは、この技術はネットワークを考える上で重要となります。

- 自律ネットワーク技術

自律ネットワーク技術は、ネットワークが自己診断や自己修復を行う技術です。これにより、ネットワークの適応性と効率性を高め、通信品質を維持できます。自律性を求める将来のインフラ では、この技術をどう適応していくかが運用高度化の鍵となります。

- セキュリティ技術

セキュリティ技術は、ネットワークとデータの保護を目的とする技術です。これにより、顧客のプライバシー保護やデータの安全性が確保されます。超安全・信頼性を求める将来のインフラ では、この技術が重要です。

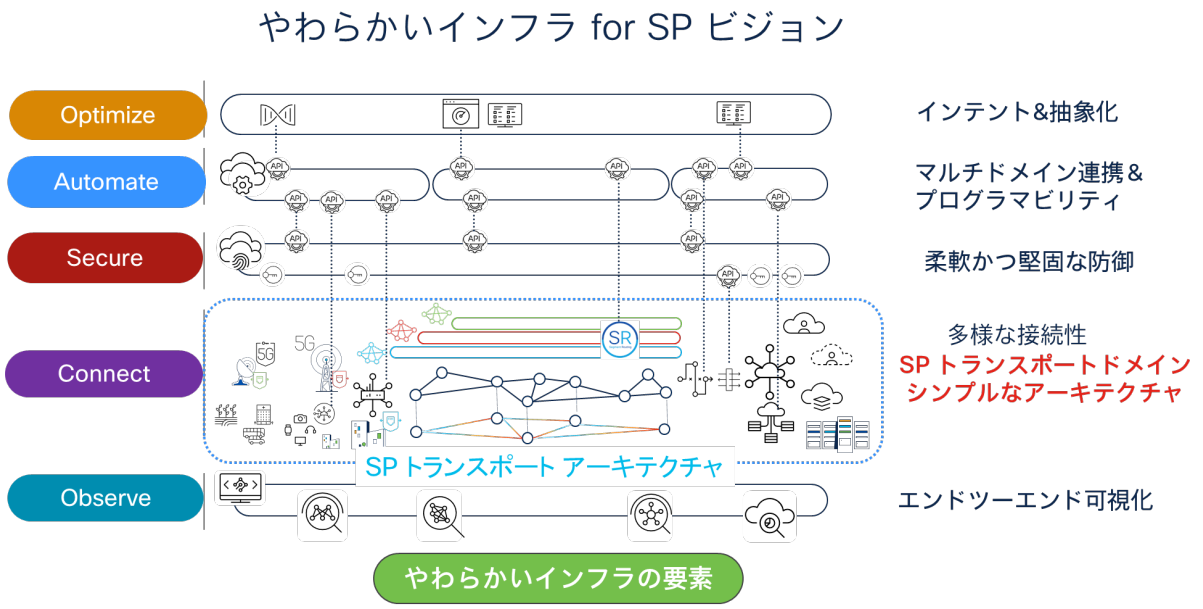
3 インフラの革新 – やわらかいインフラ

サービスプロバイダーのやわらかいインフラとは

サービスプロバイダーは現代社会において不可欠な役割を果たしていますが、急速な技術進化とお客様の通信要求の高まりが、信頼性のあるインフラの維持という重大な課題をもたらしています。この状況に対応するためには、サービスプロバイダーは避けられない高コストを負担する必要があります。しかし、インフラは単なるコストセンターというよりも、投資対象として捉えるべきです。新しいサービスを柔軟かつ迅速に展開できるインフラを最適な形で構築することが、ビジネス成功の鍵となります。

やわらかいインフラとは、従来のユースケースベースで作られた固いインフラに対して、ビジネスのデジタルプラットフォームとして将来のユースケースにも柔軟に対応し、変化し続けられるインフラです。やわらかいインフラの本質は、様々な外的要因の変化に柔軟に対応するため、従来のインフラの概念を拡張し、インフラ全体を統合制御することで個々のハードウェアによる固さを抽象化し、物理的な制約や依存関係を切り離すことだと言えます。

図 2 サービスプロバイダーにとってのやわらかいインフラ



やわらかいインフラでは、Connect、Secure、Optimize、Automate、Observe の 5 つの機能に分けてアーキテクチャを構築します。

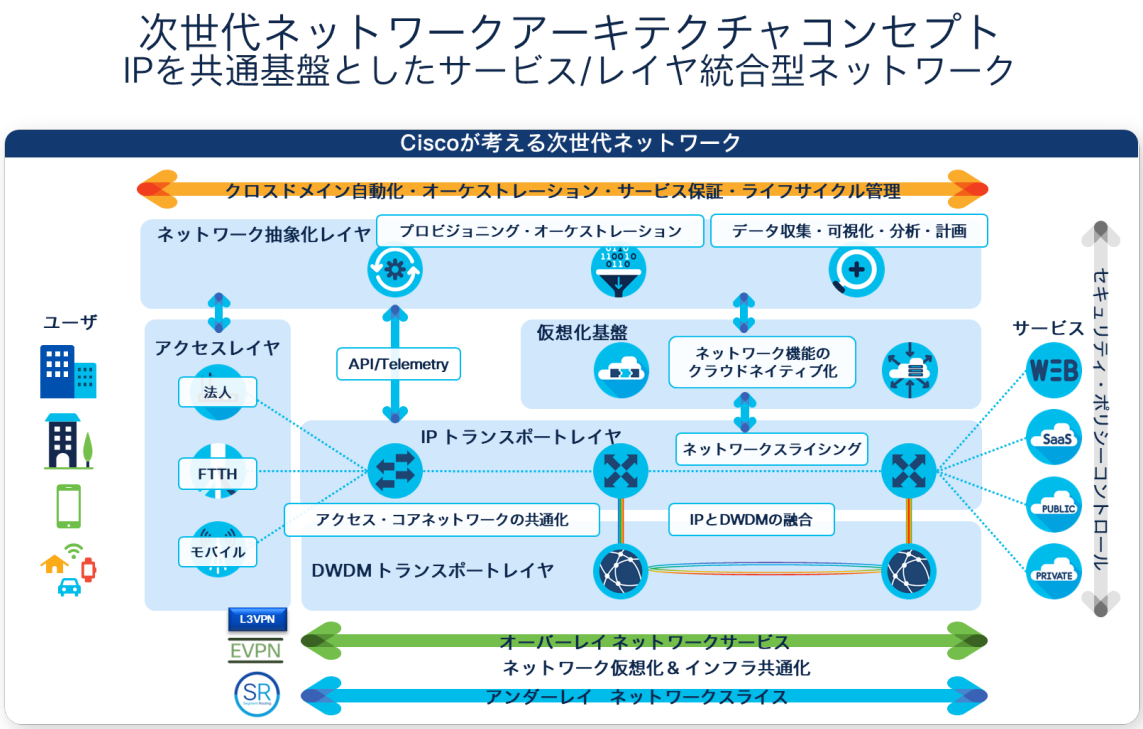
Connect では、多様なデバイスや回線をシンプルかつ柔軟に接続します。Secure では、物理的な境界にとらわれることなく、柔軟かつ堅固な防御を実現します。Optimize を通じて物理的な構成を抽象化することにより、リソースをより柔軟に活用できるようになります。Automate では、複数のドメインが横断的に連携し、ワンストップで迅速な運用が可能になります。そして Observe では、エ

ンドユーザからアプリケーションに至るまでのエンドツーエンドの可視化を実現し、その結果として顧客体験の向上を図ります。

これらの機能によって、やわらかいインフラは多様性、順応性、拡張性、セキュリティ、迅速性を特徴とし、幅広い要求に対応可能な柔軟なインフラへと変貌します。

次世代ネットワークアーキテクチャ コンセプト

図 3 IP を共通基盤としたサービス / レイヤ統合型ネットワーク



本ホワイトペーパーでは、サービスプロバイダーにおけるやわらかいインフラが目指す次世代ネットワークアーキテクチャのコンセプトのうち、特にトランスポートドメインのアーキテクチャに焦点を当てています。その範囲内で、トランスポートドメインを構成する要素として、必要とされる機能要件について解説します。

- 最適化につながる抽象化の重要性

抽象化は、ネットワークの複雑さを隠蔽し、管理者が重要なビジネス目標に集中できるようにするための重要な手段です。これにより、帯域の有効活用やシステムのシンプル化が可能となります。システムのシンプル化は、アーキテクチャを明確にし、拡張性を容易にします。これらの結果として、ネットワークの最適化と拡張性の向上が実現されます。

- ネットワークの仮想化

ネットワークの仮想化は、ネットワークの柔軟性と機敏性を向上させるために重要です。仮想化により、物理的なインフラストラクチャに依存せずにネットワークリソースを動的に割り当て、管理することが可能になります。これにより、低遅延、広帯域、省電力化といった要件を実現できます。

- インテントを反映する次世代のネットワークコントローラ

ビジネスの目標やポリシー（インテント）をネットワークに反映するためのインテリジェントなコントローラは必須になるでしょう。これにより、ネットワークの運用管理が大幅に簡素化され、トランスポートの効率化も可能になります。インテントベースド ネットワーキング（IBN）は、ネットワークの運用を自動化し、ネットワークのパフォーマンスとセキュリティを向上させるための新しいネットワークアーキテクチャのパラダイムです。ネットワークアーキテクチャの選定を進めるうえで、その効率性、柔軟性、自動化などの特長は大きなアドバンテージとなります。

- セキュリティ

ネットワークの重要性がますます高まるなか、常にセキュリティ脆弱性に晒されているという現実があります。したがって、新たなインフラストラクチャには、潜在的な脅威からネットワークを保護するため、必要になった際に速やかに対処できるような備えが必要がです。

これらの機能要件は、今後サービスプロバイダーのインフラストラクチャがビジネス環境の変化に迅速かつ効率的に対応できるようにするために不可欠です。

やわらかいインフラの導入

やわらかいインフラの導入は、不確実性が高まる現代のビジネス環境において、未来のトレンドに対する柔軟な対応力を持つために 重要です。このアプローチは、市場が求める新しいサービス要件に適応できる基盤を提供します。また、変化に合わせて最適化された調整を容易に行うことができます。さらに、既存のインフラを安全に運用し維持しながら、そのライフサイクルを効率的に管理することを可能にします。サービスプロバイダーとしての責任を全うするためには、将来に向けての明確なビジョンを定め、正しい戦略を適切なタイミングで展開することが求められます。このようなインフラの導入により、変動する市場ニーズへ迅速かつ柔軟に応じることが可能となります。

将来のネットワークインフラの導入戦略は、新規顧客獲得、既存顧客の定着率、顧客維持率の向上に直結します。新たな通信技術は、現行の 4G や 5G では提供できない新しいサービスやアプリケーションを可能にします。例えば、VR/AR、自動運転、遠隔医療、スマートシティといった先進技術の利用がより一層進化します。これらは、顧客に対して優れた体験を提供し、その結果、顧客のロイヤリティを高め、定着率と維持率を向上させます。

迅速にこれらの新しいサービスを展開する能力は、新規顧客を引きつけ、既存顧客の満足度を高める要因となります。また、やわらかいインフラを早期に導入するための戦略を進めることで、現在抱える課題に対処し、競合他社に対する優位性を確保できます。これにより、市場でのリーダーシップを維持し、新規顧客獲得のチャンスを増やすことが可能となります。

3.1 これまでのインフラからの脱却

これまで、サービスプロバイダーのインフラは多くの課題に直面してきました。組織内でサイロ化されたネットワーク設計は、情報共有を難しくし、全体としての効率性を低下させています。情報は特定の部署に閉じ込められ、他部署との協力が困難になっています。

既存のサービスプロバイダーのネットワークインフラには、最適化が進んでいない箇所がまだ多く存在しており、時代遅れの技術やソフトウェアの使用が継続されています。このような硬直化したインフラは、イノベーションの妨げとなり得るものです。

例えばコアネットワークにおいて、一部のインフラストラクチャでは静的なルーティングやスイッチングが採用されていますが、この方法はネットワークの柔軟性を低下させ、ビジネスニーズの変化への迅速な対応を困難にし、企業の成長を妨げる要因となっています。固定されたパスでは、必要に応じたリソースの動的な割り当てが不可能であり、ネットワークのパフォーマンスを最適化することが難しいため、ルーティングやパスを動的に設定できる仕組みが求められます。

また、様々なレイヤ（光、IP など）ごとに設計、構築、運用が行われるため、ネットワークの設計変更や障害発生時には、各レイヤにおける検討、導入、問題切り分けなどの作業が必要となります。これらの作業は時間を要するだけでなく、Capex および Opex を増大させる要因にもなります。

人手によるネットワーク管理も大きな課題になります。一つひとつのタスクを手動で行うことは非効率的でコストがかかり、エラーが発生しやすく、セキュリティリスクも増大します。また、サービスごとに異なるアンダーレイネットワークを構築する設計は、管理が複雑になり、コストが増大する問題もあります。古い機器を対象にした運用自動化を進めることで、短期的な課題は解決するかもしれません。しかし、部分的な最適化や個人依存の手法が固定化されることで、長期的な新たな課題を招いてしまうことがあります。

このように、従来のインフラストラクチャは、拡張性に欠けているのが実情です。サービスプロバイダーが所有するインフラは全国規模にわたるため、新規サービスを導入するたびに再構築するのには多大な困難が伴います。このため、予期せぬ新たな要求が生じた場合、既存のネットワークに機能を追加していく、いわばパッチワークのような手法を余儀なくされます。この結果、ネットワークはさらに複雑化し、管理が煩雑になってしまっています。

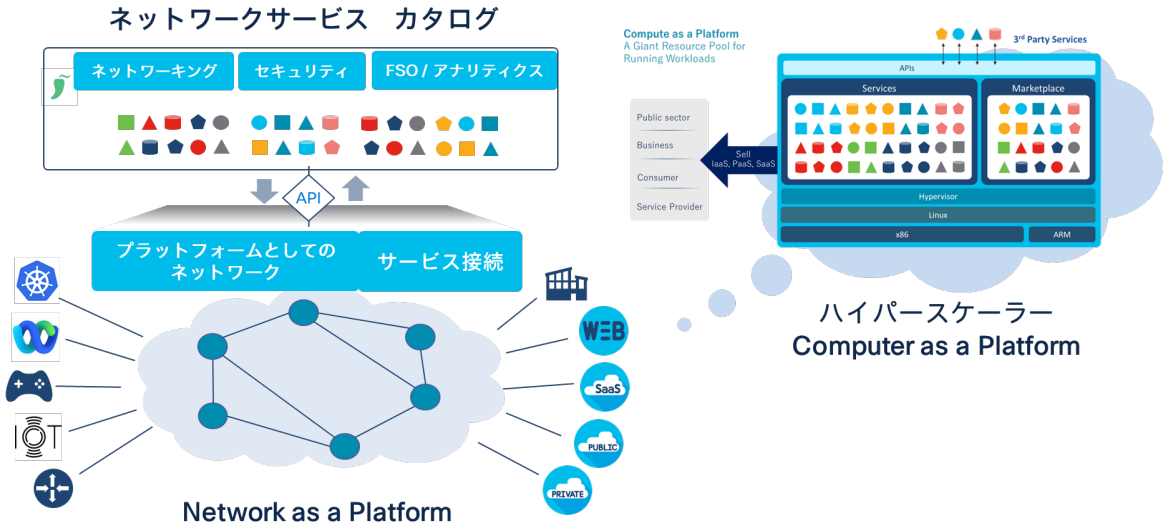
インフラの全国的な更新機会は極めて限られているのが実状であり、将来を見据えた明確なビジョンの下、適切なタイミングでの最新技術の採用を検討する正しい戦略が求められます。

ビジネスモデル変革

近年、クラウド事業者が提供するクラウドサービスの重要性と必要性が高まっています。その中で、クラウド事業者はインフラをサービス提供の核として位置付けています。同様に、ネットワークインフラも単なる技術的資産にとどまらず、収益を生み出す重要な基盤であると認識されています。これ

に基づき、サービスプロバイダーは新技術をネットワークインフラに導入し、古いインフラからの転換を図るべきです。この最適化は、市場への接続性を提供するだけでなく、付加価値の高いサービス創出のための基盤となります。データセンターやクラウドへの接続性要求が増大する状況で、サービスプロバイダーはネットワークアーキテクチャの改革にも力を入れる必要があります。

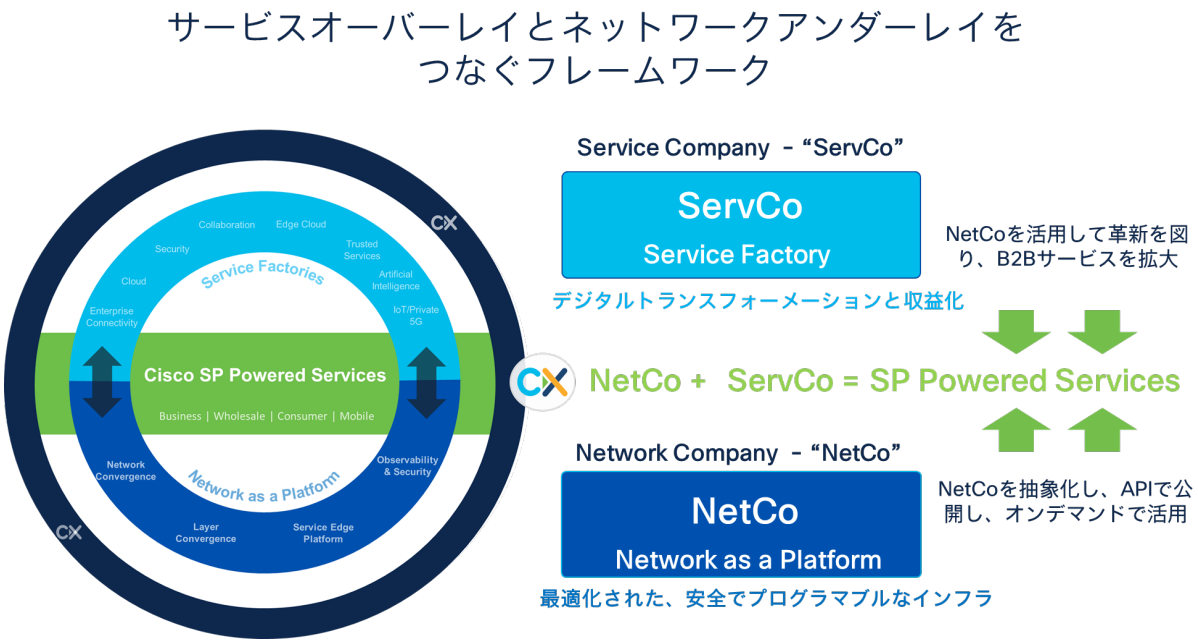
図 4 ビジネスモデル変革：クラウドライクなネットワークサービス



新規ビジネスチャンスを掴むためには、高い機敏性（アジリティ）を持って新規ビジネス開発に取り組むことが不可欠です。インフラの最適化は、このアジリティを支え、収益性の向上を実現します。加えて、安全で持続可能な運用の実現は、サービスプロバイダーの責務でもあります。最終的には、やわらかいインフラのコンセプトを考慮し、柔軟なエンドツーエンドのアーキテクチャを採用することで、これらの要求を満たすことができるでしょう。サービスプロバイダーはこうした変革を進めることで、将来にわたり競争力を保持することが可能になります。

シスコが提唱するサービスプロバイダーの新たなサービスフレームワークでは、ネットワークを競争力のあるサービスを生み出す基盤と捉え、それを「Network as a Platform」と定義します。サービスプロバイダーはこのプラットフォーム上に「Service Factory」を構築し、柔軟かつ効率的にサービスを開発・提供します。

図 5 収益を生み出すフレームワーク



サービスプロバイダーのビジネスモデル変革において、「Network as a Platform」は中核的な概念です。これは、ネットワークを単なる接続手段ではなく、さまざまなサービスが展開されるプラットフォームとして捉えるものです。このプラットフォームは、マルチクラウド接続やマルチアンダーレイ構成に対応する柔軟なアーキテクチャを必要とし、サービスエクスチェンジの役割を果たすハブとして消費者とクラウドサービスを繋ぎます。また、サービスの抽象化とアプリケーションプログラミングインターフェース（API）の公開、そして自動化は、このモデルにおいて不可欠な要素となります。これらによって、パフォーマンス、コスト、到達性、および課金に関して最適化された統合環境が提供されます。

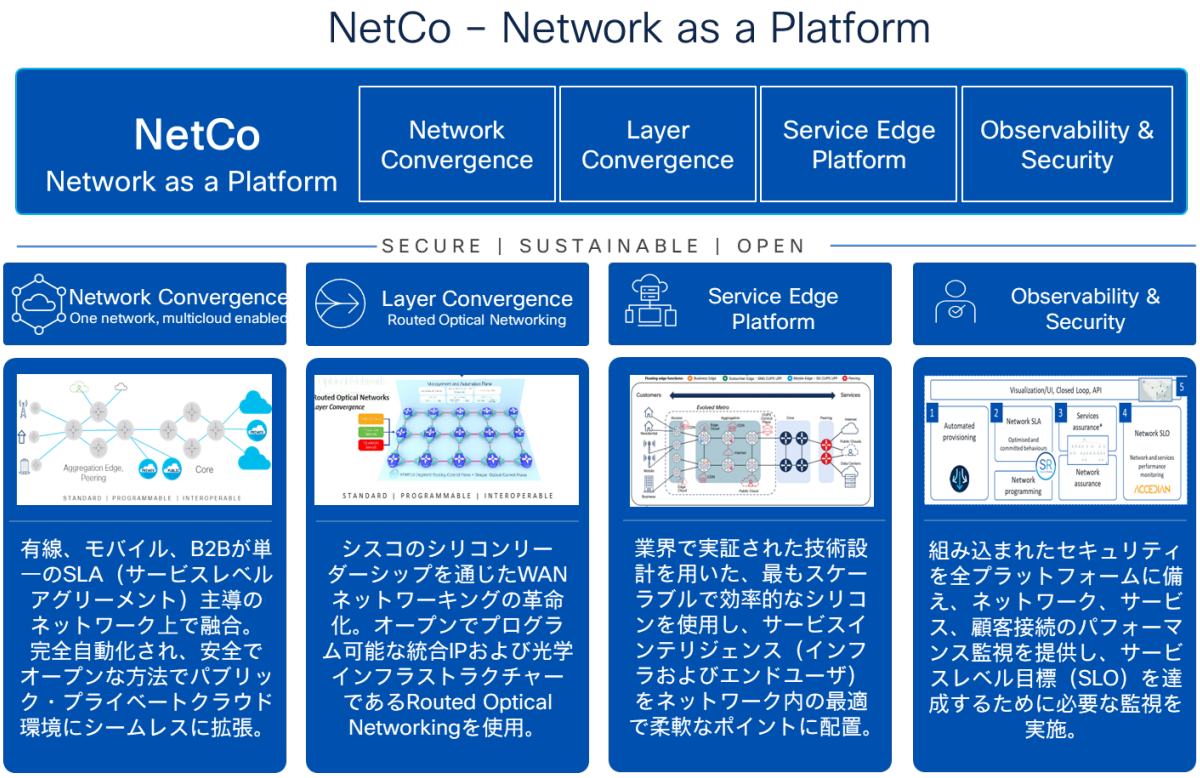
一方で、「Service Factory」は、このネットワークプラットフォーム上で展開されるビジネスモデルであり、エンタープライズ顧客のニーズに応えるために必要な要件を備えています。具体的には、エンドツーエンドで保証されたサービスレベルアグリーメント（SLA）の提供、顧客体験（QoE）を満たすサービス品質、そしてエンタープライズ顧客の接続要件に応じたクラウド接続の提供などが挙げられます。さらに、サービスは従来のプリペイドモデルからオンデマンドコンサンプションモデルへと移行し、顧客は使用した分だけ支払う柔軟性も享受できるようになります。

これら 2 つのビジネスモデルは相互に補完し合いながら、サービスプロバイダーにとって新たな収益源を創出します。「Network as a Platform」が革新的なネットワークアーキテクチャを提供する一方で、「Service Factory」はその上でユーザ指向のサービスを迅速に開発して提供することを可能にします。「Service Factory」におけるセルフサービスポータルの提供は、顧客にとって直感的な操作性をもたらし、サービスの自由度を高めます。この結果、サービスプロバイダーは顧客に対して価値ある体験を提供することができ、業界内での競争優位を獲得することが可能となります。

3.2 NetCo – Network as a Platform

本ホワイトペーパーでは、次世代ネットワークの展開にあたりサービスプロバイダーが直面する課題を取り上げ、「Network as a Platform」という解決策を提案しています。また、このアプローチを実現するために必要なネットワークインフラアーキテクチャの革新的なソリューションとその提供する価値について説明します。サービスプロバイダーは、各ソリューションの必要性と優先度を考慮し、最適なタイミングで適切な場所に展開することが推奨されます。

図 6 NetCo: Network as a Platform



Network Convergence：ネットワーク統合

Network Convergence は、統合されたインフラストラクチャを通じて、エンドツーエンドのトランスポートファブリックを形成することを目指しています。これにより、スライス技術やプログラマビリティに最適化されたインフラが構築されます。シンプルなプロトコルスタックを用いることで、よりシンプルなアーキテクチャを実装し、インフラの柔軟性を高めることができます。この柔軟性が「やわらかい」インフラを実現します。

Layer Convergence：レイヤ統合

Layer Convergence は、伝送と IP レイヤの完全なる統合を進めることにより、インフラをシンプル化することを目指しています。光伝送技術の革新は高いエネルギー効率を実現し、トランスポートのトポロジから運用に至るまで究極のシンプルさをもたらします。IP 技術の利点を維持しつつ、シンプル化されたアーキテクチャは、持続可能性の高いソリューションを提供します。また、セグメント

ルーティング（SR）との高い親和性は、ネットワークの柔軟性を向上させることに寄与し、その柔軟性は「やわらかい」と評価されます。

Service Edge Platform：サービスエッジプラットフォームの進化

Service Edge Platform は、集中配置から分散されたエッジ機能の実装が可能であり、エッジ機能をどこにでも配置できるアーキテクチャにより、ハイブリッドまたはマルチクラウドへ最適な接続性を提供することで、さらなる「やわらかさ」を提供します。ハードウェアの進化に伴い、最新のプラットフォームは、この分散アーキテクチャの特徴を活かすためにさらに適した重要な役割を果たすようになっています。

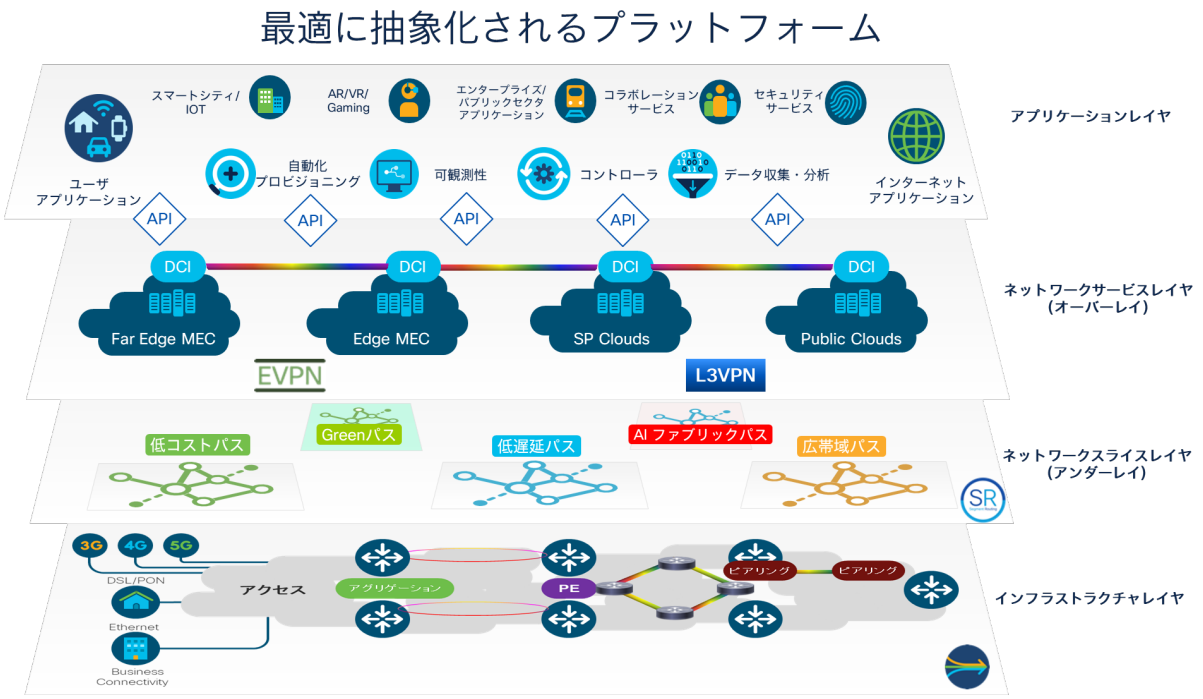
Observability & Security：オブザーバビリティ（可観測性）とセキュリティ

Observability & Security においては、ネットワークインサイトを用いた可視化や自動化を通じて効率化を図ることが可能です。これは、運用の複雑さを軽減し、セキュリティリスクへの対応を迅速化することに貢献します。また、インテントベースの SDN コントローラを活用することにより、将来的に AI 技術を組み込むことでさらなる進化が期待されます。安全なネットワーク運用を実現するためには、ネットワークの柔軟性と共に、セキュリティメカニズムが組み込まれた「やわらかい」アーキテクチャが不可欠です。このアプローチにより、サービスプロバイダーは複雑で変化するセキュリティ環境に対応し、顧客に対して信頼性の高いサービスを提供し続けることができます。

3.3 抽象化による最適化 - シンプルなアーキテクチャへ

サービスプロバイダーの将来のインフラストラクチャは、データセンターのサーバが仮想化されているように、ネットワークの物理的な構成からの脱却と、ネットワークレイヤとレイヤ間のインターフェイスの抽象化・標準化が今後さらに求められていくと考えられます。これは、不確実性の高い市場動向を見つつ、新規サービスの即時展開と既存サービスの維持を両立させ、業界の競争力を維持するためです。抽象化により、サービスの迅速な展開や変更が可能となり、事業の柔軟性とスピードを向上させることができます。また、外部環境の変化に対する耐性と最適化も実現し、運用の安定性と効率性を向上させることができます。

図 7 最適に抽象化されるプラットフォーム



ネットワークインフラの抽象化をすることで、新しいサービスやアプリケーションの開発を容易にします。例えば、サービス品質（QoS）を定義するだけで新規サービスを展開できるようになります。また、抽象化によって各ドメイン間のインターフェイスの標準化が可能となり、各ドメインと連携を必要とする開発プロセスの効率化を図ることができます。

ネットワークインフラの抽象化・標準化は効率的なネットワーク運用を可能にします。抽象化と標準化により、上位コントローラレイヤから標準的な API を使用し、共通化された下位のアンダーレイを制御することができます。これにより手作業中心のネットワーク運用で直面している運用の複雑さを軽減できます。さらに、サービスドメイン毎に異なるネットワークに対する、日々の変更工事やトラブルシューティングに対応するための知識や準備を統一化することができ、トランスポートドメインを一元的に管理することが可能となります。

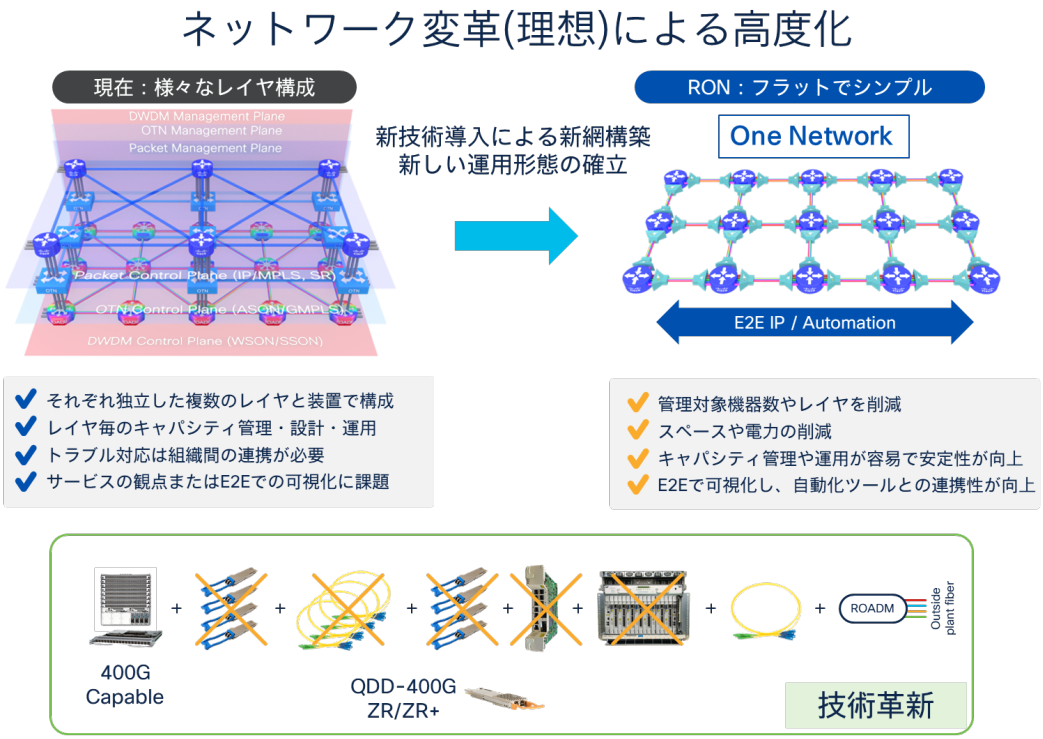
また、将来の完全自律化ネットワークへ向けては、ネットワークのプログラマビリティの基礎を整えることができ、ネットワーク技術部門全体で、業務を効率化しつつ新しいスキルアップの機会を得ることで、競争力のある組織を形成できます。

レイヤ統合 - IP と伝送の統合

Routed Optical Networking は、IP ネットワークと Optical 伝送を統合した先進的なネットワークアーキテクチャです。この統合により、ネットワークのアンダーレイが一階層化され、その上でオーバーレイによる抽象化が実現されます。これにより、従来の複数階層にわたるネットワーク構造と異なりフラットなネットワークアーキテクチャとなります。

ネットワーク全体としてハードウェアの必要性が減少し、消費電力の削減に直結します。さらに、統合されたネットワークアーキテクチャは、運用の単純化を実現し、運用コストの削減にも寄与します。 Routed Optical Networking により、サービスプロバイダーはより効率的で持続可能なネットワークを構築し、経済的な負担を軽減しながら、将来にわたって競争力を保つことができます。

図 8 Routed Optical Networking



3.4 ネットワーク仮想化 - エンドツーエンド SP ファブリック

ネットワークスライシングとは、物理的なネットワークを複数の仮想ネットワークに分割し、それぞれの仮想ネットワークが独立したネットワークとして動作することを可能にするネットワーク仮想化技術です。共通化されたインフラストラクチャを使って、サービスの要件ごとにネットワークパスのリソースを論理的に割り当てたものをスライスと呼びます。

サービスプロバイダーがネットワークスライシングを必要とする理由は、業界の競争力を維持し、新しいビジネスチャンスを掴むためです。デジタルトランスフォーメーションの進行に伴い、顧客のニーズは多様化し、高度化しています。これに対応するためには、物理ネットワークの制約を超えて、より柔軟でスピーディなサービス提供が求められています。ネットワークスライシングは、このニーズに対応するための最適な解決策となります。

ネットワークスライシングは、物理的なネットワークリソースを効率的に利用し、サービスプロバイダーが独自のサービスを提供するための独立したネットワーク環境を確保することを可能にします。それぞれのネットワークスライスは、サービス品質（QoS）、帯域幅、セキュリティなどの観点で設定や管理を行えます。これにより、サービスプロバイダーは顧客のニーズに対応したサービスを迅速

に提供することが可能となります。また、各ネットワークスライスが隔離されているため、セキュリティ面でも優れた特性を持っています。

サービスプロバイダーのトランスポートドメインで適用するネットワーク仮想化技術は、イーサネット VPN（EVPN）や既存のレイヤ 3 VPN（L3VPN）を用いた BGP ベースのネットワーク仮想化技術と SR 技術を組み合わせることで、最適な形で実現できます。SR は、ネットワークパスを単純化し、柔軟性を高め、運用の効率化を目指して開発されています。パケットヘッダに MPLS ラベルを使用する SR-MPLS と IPv6 拡張ヘッダを用いた SRv6 の方式があり、ユースケースを考慮した上で利用する方式等を選択します。

図 9 セグメントルーティングの特徴

ネットワークスライシングを作成する具体的な SR ソリューションとして、セグメントルーティングトラフィックエンジニアリング（SR-TE）やフレックスアルゴ（Flex-Algo）機能を検討できます。これらの技術を活用することにより、ネットワーク全体の効率を高めるだけでなく、ネットワークの信頼性と可用性も向上させます。これは、ネットワークの異常や混雑を検知し、パケットをそれらの問題から回避するための別のパスに自動的に誘導する能力を持っているからです。

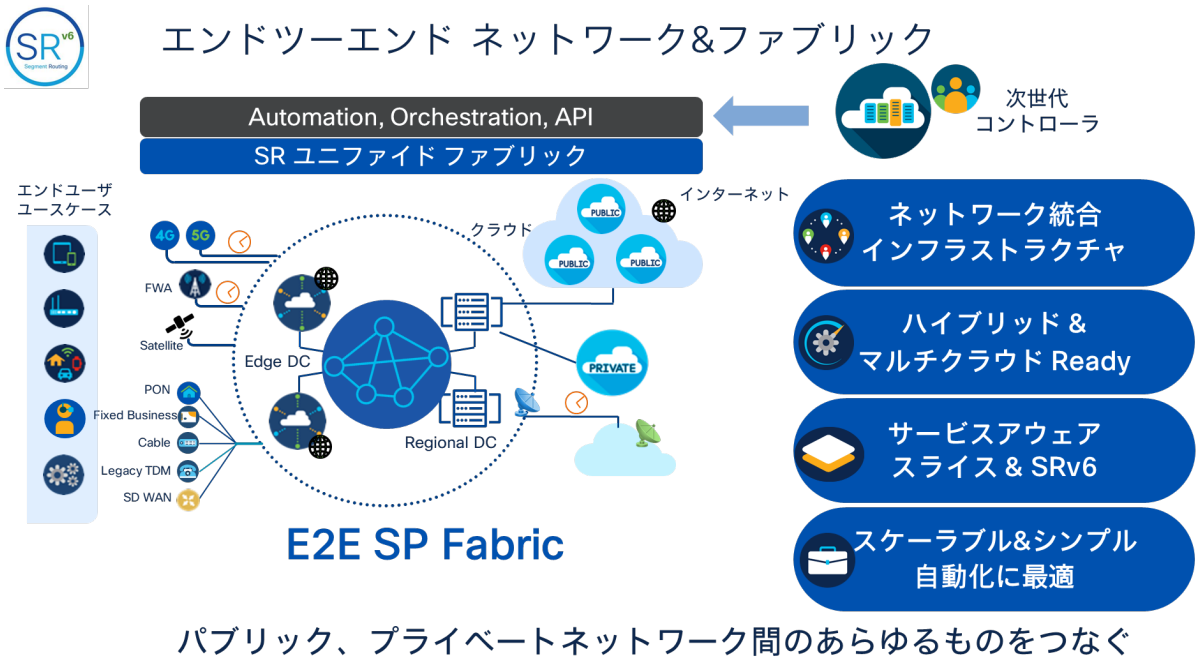
ネットワーク統合 - エンドツーエンド SP ファブリック

一般にネットワークファブリックとは、データを目的地に転送するために、アクセスポイント、スイッチ、ルータなどのネットワークデバイスを相互に接続するメッシュ状の構造を意味します。これは、すべてのノード（スイッチやエンドポイント）が他のノードと相互に接続されたネットワークトポロジの一形態であり、一般的には織物のようなマトリックスとして視覚化されることから「ファブリック」という名称が用いられます。「ファブリック」という用語は、接続を構成する物理配線を指す場合もありますが、ここでは物理トポロジ上に構築される仮想化された、かつ自動化されたオーバーレイ接続の格子を指しています。このファブリックは、ネットワークのアンダーレイを仮想化し、

複数のオーバーレイネットワークに分割して個別に最適化することで、異なるニーズに対応し、迅速な変更への対応が可能になります。

エンドツーエンド SP ファブリックとは、サービスプロバイダーの次世代インフラの目指すべきコンセプトであり、大量のデータ、複雑なネットワーク管理、顧客の要求増に対応し、柔軟性と効率的なリソース配分を実現します。ネットワークデバイスとネットワークコントローラの組み合わせにより、ファブリックの作成と管理が簡素化されます。コントローラによる集中管理型のシステムは、動的なトラフィックエンジニアリングを実現し、自動化ツールによってネットワークのノードの変更や再構成を容易にします。自動化された運用により、人的ミスの削減、コストの削減、一貫した高品質サービスの提供が可能となります。

図 10 エンドツーエンド SP ファブリック



さらにエンドツーエンド SP ファブリックは、サービスプロバイダーが 5G や IoT といった新たな技術の導入に伴う複雑さを管理する上での重要な役割を果たします。低遅延、高帯域幅、大規模接続性を要求するこれらの技術は、ネットワークの柔軟な調整と極めて高いスケーラビリティを必要とし、エンドツーエンド SP ファブリックはその要求に応える必要があります。

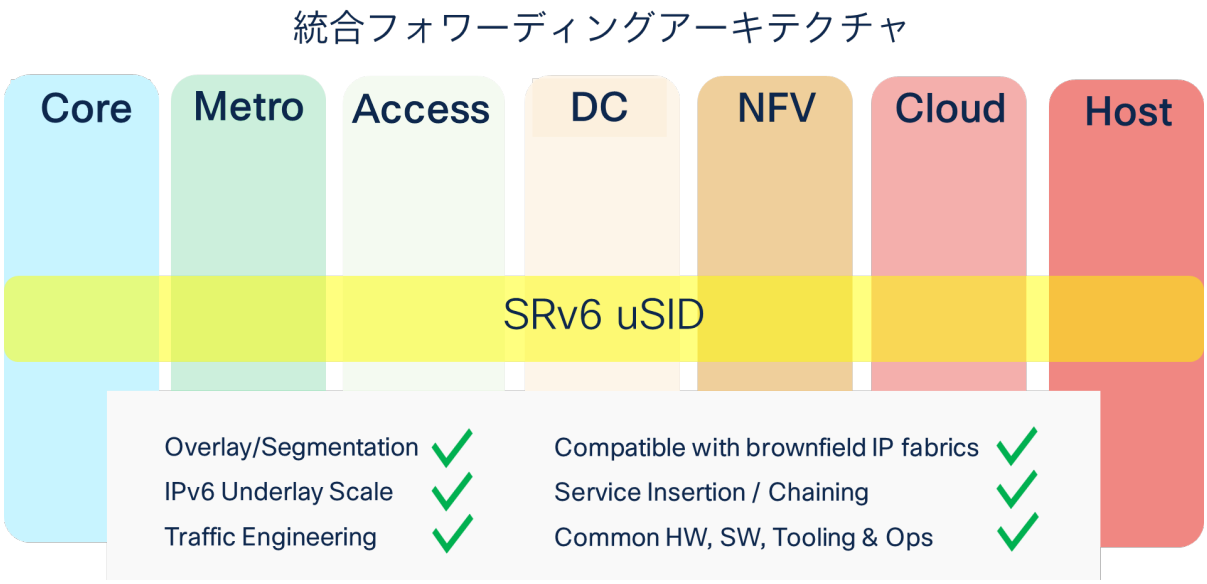
ファブリックアーキテクチャのトランスポートドメインへの適応については、地理的な制約により、伝送路を格子型に設計することが現実的ではない場合があります。実際にデータセンター内で使用されている CLOS アーキテクチャをトランスポートネットワークに直接適用することは困難であるため、トランスポートドメインにおいては、適切なトポロジを考慮に入れて、ネットワークスライシング技術を採用した仮想的なネットワークファブリックを形成することになります。

ファブリック対応のノードは、それらに直接接続されているエンドポイントによって生成されるすべてのトラフィックに適切なタグを追加します。ネットワークコントローラは、パケット内のタグに作用するポリシーをデバイスに設定し、ファブリックを作成します。各ノードは適切なタグをトラフィ

ックに追加し、受信したパケット内のタグを解釈して、割り当てられたポリシーに従って転送またはドロップする機能を有しています。これらのノードはプログラム可能であり、アクセス、サービス品質（QoS）、その他のポリシーが自動化されていることが求められます。

このタグに SRv6 技術を活用することで、柔軟な接続と効率的なトラフィック管理が実現できます。将来を見据えると、SRv6 が持つシンプルなネットワークスライシング技術と、ハイパースケールな要件に対応できる SRv6 ベースの仮想的なファブリックアーキテクチャが、柔軟性と拡張性を兼ね備えたインフラの構築と運用を可能にする有効な選択肢であることが期待できます。

図 11 SRv6 uSID 統合フォワーディングアーキテクチャ



SRv6 uSID（micro Segment ID）を用いることで、将来のハイパースケールネットワークへの対応が可能となります。ルート数の増大に対応するために、Prefix Summarization を活用することにより、フラットなネットワークトポロジを実現し、ネットワークのスケール拡張を容易にします。これにより、多数のデバイスやサービスが追加された際でも、ネットワークが大きくなることによる複雑性の増大を抑制し、効率的なルーティング情報の管理が行えるようになります。

SRv6 uSID は、データセントリックアプローチに基づいたネットワーク設計を可能にします。各ネットワークセグメントやサービス機能を細かな識別子である uSID に割り当てることで、データの流れとネットワークの動作を密接に連携させます。これにより、特定のデータやアプリケーションに応じた細やかなトラフィックエンジニアリングが実現し、ネットワークリソースの最適化が促進されます。

さらに、SRv6 uSID を採用することで、エンドツーエンドの統一されたフォワーディング機構が確立されます。これはネットワークの各ポイントで一貫した処理が可能となり、エッジからコア、データセンター間での一貫したポリシー適用や運用が実現します。このように SRv6 uSID 技術は、将来のネットワーク成長に伴う課題に対応するための鍵となる技術です。

サービスプロバイダーにおける SRv6 ベースのネットワークファブリックの採用は、インフラの運用効率の向上と顧客満足度の増大をもたらすだけでなく、将来の技術革新への対応力を高めるための重要な基盤を築くことにもつながります。

サービスエッジの柔軟な配置

- これまでのエッジルーティング設計

従来のエッジルーティング設計は、サービス要件を満たす目的で、使用可能なノードの性能をもとに大規模サービスエッジルータが導入されてきました。これには以下のような特徴があります。

✓ サービスリッチな設計：L2VPN、L3VPN、インターネット、ビジネス、マルチキャスト、サブスクライバーといった多様なニーズに対応します。
✓ ハイスケールな性能：数多くのサブスクライバー、キュー、カウンター、サービス、ルート数、ポリシー数に適応します。
✓ キャリアクラスの信頼性：全ての要素において冗長性を持ち、二重化されたルータを装備します。
✓ コスト：できるだけ少ない数のエッジロケーションに大型モジュラーシャーシを配置し、1 台のルータに多くの顧客やサービスを集約することで、コストを抑えます。

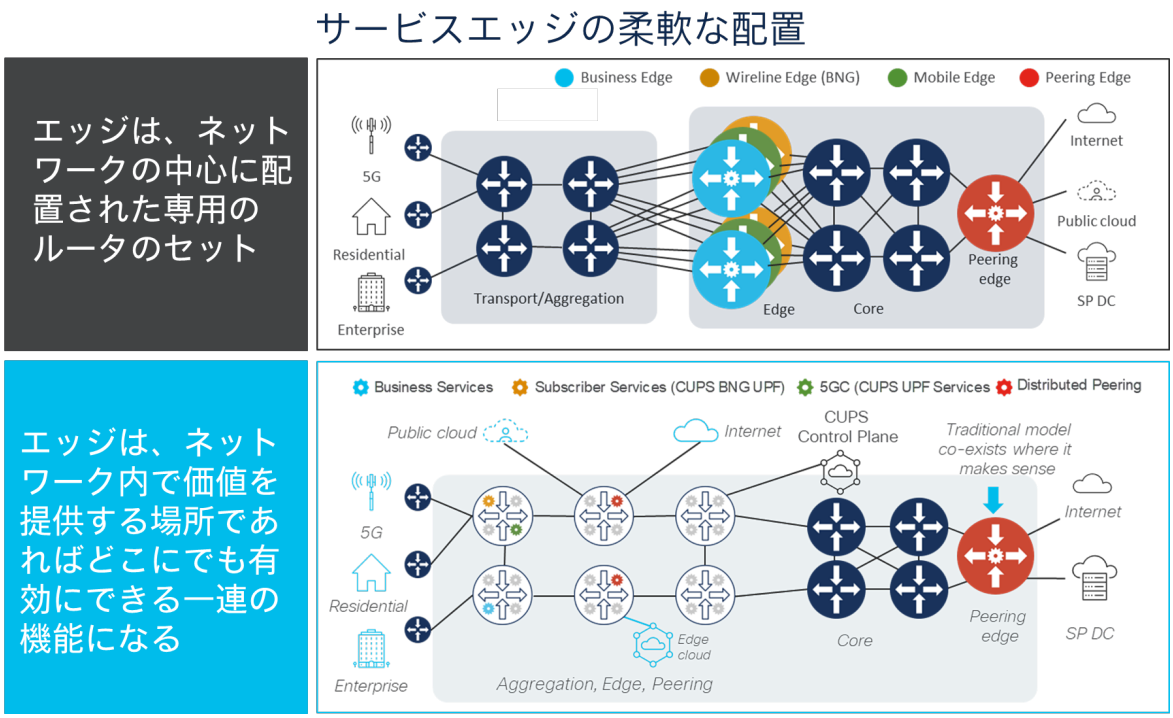
一方で、以下のような課題に直面しています。
✓ メジャーチェンジやアップグレードを可能な限り避ける、または遅らせる最小限のアプローチが求められます。技術世代間の互換性の問題により、多くの場合、ソフトウェアだけでなくハードウェアも含めたアップグレードが必要となります。
✓ イノベーションサイクルの遅れ、リスクの増加、技術利得の実現の遅さが見受けられます。
✓ 最も要件が厳しいサービスがすべての価格を決定する「最大公約数問題」に直面します。

- ビジネスモデル変革に伴うエッジルーティング設計の直面する課題

さらに従来のエッジルーティング設計は、増加するトラフィックとビジネスの変革という現実のために、新たな課題に立ち向かっている状況にあります。具体的には、以下の点が課題として挙げられます。

✓ 帯域幅の需要は増加の一途をたどる中で、顧客ごとの平均収益は停滞する傾向にあります。
✓ 集中型アーキテクチャのスケーリングに伴うコストと複雑性が増しています。
✓ コンテンツとアプリケーションは分散型アーキテクチャへと進化する流れにありますが、既存のエッジルーティング設計はこの流れに逆行する形となっています。

図 12 サービスエッジの柔軟な配置



- 共通のアンダーレイによりサービスエッジの柔軟な配置が可能に

共通のアンダーレイを用意することによって、サービスエッジを柔軟に配置することが可能です。サービスエッジは機能としてネットワーク内の任意の場所に配置することが可能となり、ネットワークはフラットな構成を実現します。ネットワークのエリアは統合され、シンプルなエンドツーエンドのファブリックアーキテクチャが現実のものとなります。

次世代サービスエッジルーティングの設計を検討する際には、革新的技術を備えた新しいサービスエッジプラットフォームの導入を適切な時期に考慮します。進化したシステムアーキテクチャを視野に入れ、将来の設計オプションとして検討することも重要です。サービスプロバイダーは展開する状況に応じて複数のオプションからアーキテクチャを検討できますが、それぞれ独自の利点とトレードオフを持ちつつも、組み合わせることでより優れた代替案を提供する可能性があります。

3.5 次世代ネットワークコントローラとインフラの進化 - AI の未来

やわらかいインフラのコンセプトにおいて、Optimize では抽象化を通じたリソースの制御を実現し、Automate では複数のドメインが連携するために、インテントを理解する統合コントローラによる集中制御のメカニズムが必要となります。

IBN では、ネットワーク運用者が「インテント」＝「意図」を定義し、その「意図」がネットワーク全体に自動的に適用されることを可能にします。一方でネットワークのアンダーレイは自律分散して

います。これにより、ネットワークのリソースやトラフィックフローをより効率的に管理し、ネットワークのパフォーマンスと安定性を向上させることが可能となります。また、ネットワークの動的な調整を可能にし、ネットワークの障害や混雑をより迅速に回避することができます。

SDN コントローラは、IBN の中心的な要素となります。SDN コントローラの主な役割は、ネットワークの「意図」を実装、検証、保証することです。SDN コントローラは、ネットワーク全体の状態を把握し、ネットワーク設定を自動的に適用・調整するための中心的な制御ポイントとして機能します。

このように SDN コントローラによって、ネットワークの運用を大幅に簡素化し、ネットワークのパフォーマンスとセキュリティを向上させることが可能になります。

SDN コントローラを導入すると、以下のような利点があります。

- 効率的なネットワーク管理
  ネットワークの設定や調整が自動化されるため、運用者は複雑なネットワーク設定タスクから解放され、他の重要な業務に集中することができます。

- 高いネットワークパフォーマンスと信頼性
  SDN コントローラは、ネットワークの状態をリアルタイムで把握し、必要に応じて設定を自動調整することで、ネットワークのパフォーマンスと信頼性を最適化します。

- 強固なセキュリティ
  SDN コントローラは、ネットワークの異常や脅威をリアルタイムで検知し、必要なセキュリティポリシーを自動的に適用します。

例えば、運用者がネットワークの「意図」について命令を出すことで、SDN コントローラからネットワークへ API を通じて SR Policy を設定できます。ネットワーク運用者は、特定のトラフィックが特定のパスを通過するように制御することで、複雑な設定操作を使うことなく、パフォーマンスの最適化、負荷分散、または特定のサービス品質（QoS）要件の達成を効率的かつ自動的に実装できます。

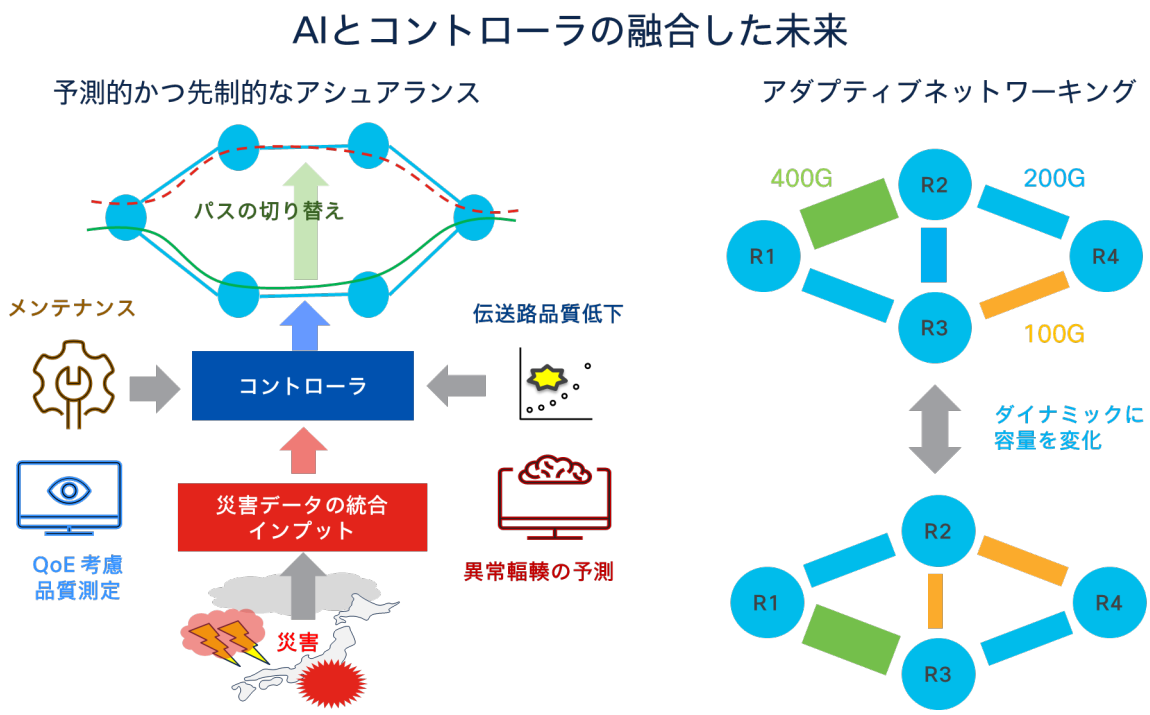
AI の未来と自律化ネットワーク

AIOps は「Artificial Intelligence for IT Operations」の略で、IT 運用管理に人工知能（AI）技術を適用することを指します。この技術はサービスプロバイダーの運用管理への適応が期待されている分野です。

AI を活用した予測ネットワーク技術は、自動化と組み合わせることで、自己修復能力を持つネットワークへの道を開く可能性を秘めています。ネットワークコントローラが AI と連携することにより、以下のような未来予測が可能になると考えられています。

- パフォーマンスモニタリング（PM）データを活用して、伝送路の劣化を予測します。具体的には、フォワードエラーコレクション（FEC）処理の前のビットエラーレート（BER）などを分析します。
- 自然災害や建設工事がファイバーケーブルのルートや伝送設備に与える影響を予測します。
- ネットワークのメンテナンスによるサービス中断を予測します。
- ネットワークコントローラなどを用いて、予防的なトラフィックの移動がネットワークに与える影響を分析します。
- 運用責任者の承認を得て、サービス停止が起こる前に、重要なトラフィックや全トラフィックを、中断なく別のルートに移動させます。
- 伝送路品質の良いリンクの容量を動的に変更し、サービストラフィックをコントロールします。

図 13 AI とコントローラの融合した未来



ただし、正確な予測を行うためには、まずネットワークのデータを十分に学習させる必要があります。現在の多くのネットワーク制御プレーン技術には、学習機能が組み込まれておらず、現在のテクノロジーやプロトコルは学習や予測機能を利用していません。既存の AI モデルでは不十分な場合、そのネットワーク構成と運用スタイルの特徴についての情報を加味して AI モデルをトレーニングするためには大量のデータを利用した学習が必要になる可能性があります。

オブザーバビリティ（可観測性）

オブザーバビリティは、システムの内部状態を外部から監視し理解する能力です。これには、メトリクス、ログ、トレースなど、システムの動作に関する豊富なデータが含まれます。オブザーバビリティは、システムの健全性をリアルタイムで理解するために不可欠であり、故障の原因分析やパフォーマンスの低下の識別に役立ちます。

AIOps ソリューションは、オブザーバビリティから得られるデータを活用して、機械学習アルゴリズムや自動化された分析を行い、システムの異常を迅速に検出し、予兆を認識して対処します。これにより、システム運用の効率が高まり、ダウンタイムの削減、問題解決の迅速化、運用コストの削減が実現可能になります。オブザーバビリティが提供する詳細なデータは、AIOps の分析プロセスにおいて非常に価値があり、より高度な運用インテリジェンスを生み出す基盤となります。

図 14 オブザーバビリティとアクティブモニタリング

ネットワークデータを充実させ、実用的な洞察を得る

5G の次のステージへと進むにあたり、サービスプロバイダーが直面する最大の課題の 1 つは、自社インフラに対する効果的なオブザーバビリティ戦略の策定と実装です。ビジネスの敏捷性を維持し、コストを増加させるネットワーク障害を未然に防ぐため、システムを全体的に観察し分析できる包括的なモニタリング体制が不可欠です。断片化されたモニタリング手法では、ネットワークの問題を迅速に検出し、深い洞察を提供する能力に欠けるため、最適な成果を得ることは困難です。したがって、エンドツーエンドの可視性を実現するオブザーバビリティ ソリューションを採用することにより、ネットワークの運用効率とビジネスの機動性が大幅に向上することになります。

サービスレベルアグリーメント（SLA）の遵守には、特にサービスプロバイダーにおける徹底したサービス監視が求められます。しばしば、機器は監視されていますが、サービス品質自体の監視がおろそかにされがちです。通信の単純な可否チェックに留まらず、レイテンシやジッターといった品質指

標の監視が必要です。これには、機器だけでなく、エンドツーエンドでのトラフィック、オーバーレイ、アプリケーションレベルでの監視が含まれ、アクティブ監視などの先進的な手法が効果的です。これらにより、トラフィックパフォーマンスのメトリックを測定し、サービス品質を総合的に評価することができます。

また、SLA は事業者とユーザ間の契約であり、ユーザがサービスの状況を確認できる透明性が不可欠です。特に企業ユーザにとっては、リアルタイムでのサービス品質の把握が業務において重要となります。情報は迅速かつ正確に提供されるべきであり、インフラのコントロールをユーザに部分的に委ねることで、ユーザの要求に対する迅速な対応が可能になります。この実現には、オブザーバビリティと自動化の統合が必要であり、SLA とユーザのニーズに応じてインフラの柔軟な制御が重要となります。

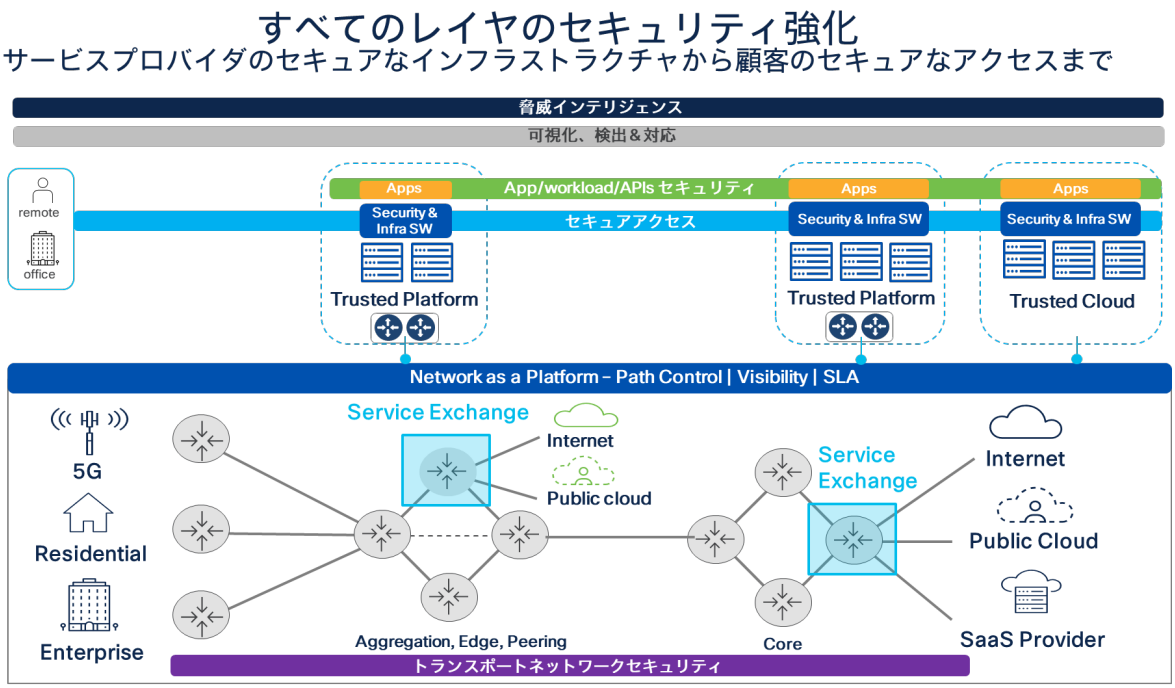
3.6 セキュアなやわらかいインフラ

サービスプロバイダーにおいてセキュリティが必要な背景

昨今、サービスプロバイダーのインフラには大きな変革が起こっており、サービスを提供する範囲は拡大し続けています。それに伴い、ネットワークインフラの分散化が進み、IoT やモバイル接続を通じて、従来想定していたユースケースを超えた用途での活用が増えてきています。

DX（デジタルトランスフォーメーション）が一般化する 2030 年に向け、サービスプロバイダーが提供するインフラは、現状の社会インフラという位置づけを超えて、さらに重要なものになっていくことが予想されます。そのような重要なインフラとして備えるべき大きな機能の 1 つに、セキュリティ機能が挙げられます。

図 15 セキュアインフラストラクチャ



Public Wi-Fi や Local 5G といった新たな接続ポイントに対して、IoT などさまざまなデバイスが接続されていくなかで、2030 年にはより多くのデバイスが現状では想像できない形で接続されることが想定されており、サービスプロバイダーのインフラに対するセキュリティはますます重要性を増していきます。顧客に提供するセキュリティの向上が期待されることを踏まえて、ここでは顧客にトランスポートドメインを提供するにあたり考慮すべきセキュリティ対策について概説します。

やわらかいインフラの実装を踏まえたセキュリティ対策の検討

サービスプロバイダーは、さまざまな顧客に対して、高速で高度な制御が可能なネットワークを提供していかなければなりません。これを実現するためには、ネットワークの仮想化、抽象化を行い、次世代ネットワークアーキテクチャを実装することが必要だと前述しました。

このような高度なネットワークを提供するにあたり、サービスプロバイダーがこれまでと同様に社会的な責任を果たし、ビジネスを継続していくために、法令の遵守、顧客情報の保護や継続的なサービスの提供を実践していく必要があります。

これらを実現するためには、従来のインフラの堅牢化や DDoS 対策、コントロールプレーンとデータプレーンの分離、信頼性の高いネットワークオペレーションシステムの採用などのセキュリティ対策や体制作りに加え、新たに実装される IBN とその運用に関連したセキュリティの検討も必要となります。一般的には、事業被害の想定、事業被害につながる脅威の想定、脅威に対応するためのセキュリティ対策の列挙と優先度付けの順に検討を行います。

- 事業被害につながる脅威の想定

今回は IBN の実装によって生じうる新たな脅威を想定し、どのような対策が必要かの一例を示します。

IBN の実現の中心要素となる SDN コントローラの導入により、SDN コントローラの脆弱性への攻撃による侵害や、コントローラへアクセスする際の認証情報の窃取などが新たな脅威として検討されます。これらによって情報資産やシステムの機密性、完全性、可用性が脅かされることになります。

- 脅威へ対応するためのセキュリティ対策

こうした IBN 実装上の脅威に対して、以下のようなセキュリティ対策を検討することが求められます。

✓ 脆弱性対策：インフラを構成する要素に関する脆弱性情報の収集、対策の検討、対策の実施といった一連のプロセスを適切に確立し、迅速な判断・対応を行います。パッチの適用にあたっては、その検証と展開を迅速に行うことが必要です。総務省にて推進される SBOM（Software Bill of Materials）のプロセスの熟成とプロセスの自動化が求められます。

✓ 管理者アクセスの強化：SDN コントローラへの管理者アクセスは特権管理による厳密なアクセ

ス管理や多要素認証を実施します。また、操作の痕跡の記録や証跡の確保も、二次災害の防止や原因究明のために、これまで以上に重要視されると考えられます。

✓ 継続的な堅牢性試験：セキュリティのライフサイクルを継続的にプロセス化する上で、侵入テストや脆弱性確認試験といった確認手法を確立し、定期的に実施していくことは、これまで同様に必要になると想定されます。

✓ IBN による変更時の強度確認：柔軟に管理できるインフラにおける柔軟なセキュリティのあり方を検討し、同様の考え方でセキュリティ管理ができるように同時に検討することが大切です。

このような脅威の想定と脅威への対応をまずはコアとなるトランスポート領域に適用し、最終的には、サービス全体、会社全体、サプライチェーン全体で策定・実践していくことで、統合的なセキュリティを実現することを目指し、顧客に対して安全で継続的なサービスを提供していく必要があります。

4 やわらかいインフラを活用したユースケース

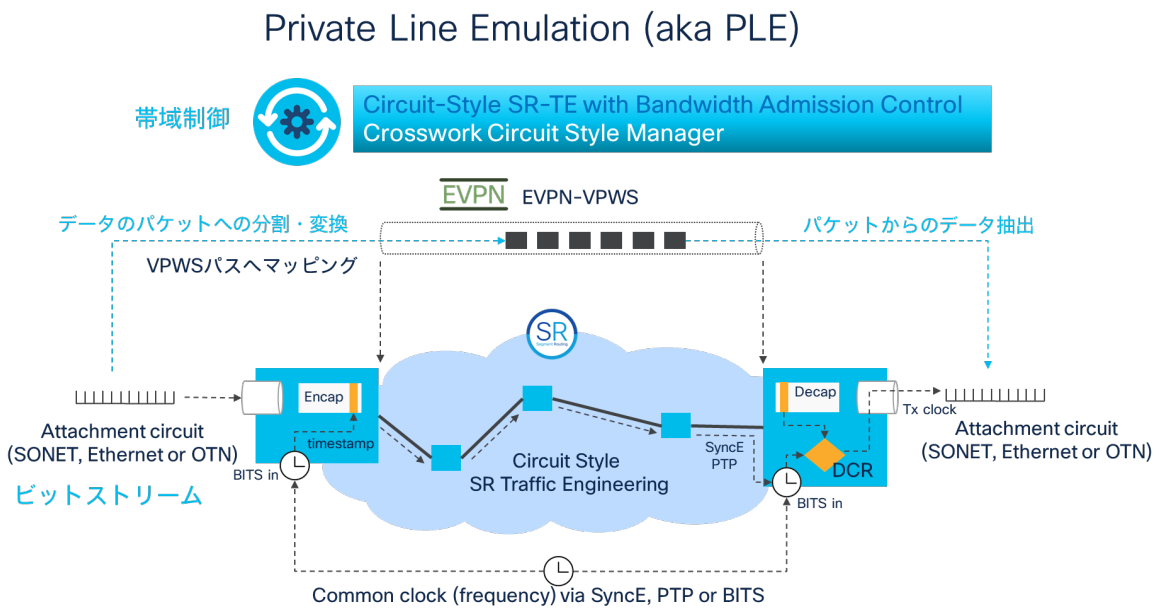
4.1 ユースケース 1： Routed Optical Networking Private Line Emulation

レイヤが統合されたアーキテクチャ上では、統合されたセグメントルーティング パケットネットワークを通じて、従来の TDM のような専用線サービスであるプライベートライン エミュレーション（PLE）が実現されます。この実現に関わる技術の中で、サーキットスタイル セグメントルーティング（CS-SR）は、基盤となる TDM に類似したトランスポートを提供し、従来の専用線イーサネットサービスおよび専用線エミュレーション ハードウェアを利用したビットトランスペアレントなイーサネット、OTN、SONET/SDH、ファイバチャネルサービスを提供するものです。

PLE は、EVPN 仮想プライベート ワイヤーサービス（EVPN-VPWS）回線上で動的にシグナリングされ、伝送されます。PLE サービスにおいては、Differential Clock Recovery（DCR）を用いて、2 つの PLE クライアント間の適切なフレームタイミングを確保します。クロック精度を維持するためには、各 PLE エンドポイントルータが共通のプライマリ基準クロック（PRC）に追跡可能な周波数ソースを必要とします。

加えて、帯域幅アドミッションコントローラーを用いることで、サーキットスタイルポリシーに基づく保証された帯域幅パスを提供する機能が備わっています。

図 16 Routed Optical Networking によるプライベートライン エミュレーション



Reference: XRDOCS Cisco Routed Optical Networking

https://xrdocs.io/design/blogs/latest-routed-optical-networking-hld

Reference: Cisco's Automation Solution for Routed Optical Networking White Paper

https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/automation-routed-optical-nw.html

4.2 ユースケース 2：データセンターとトランスポートドメインのシームレスな接続

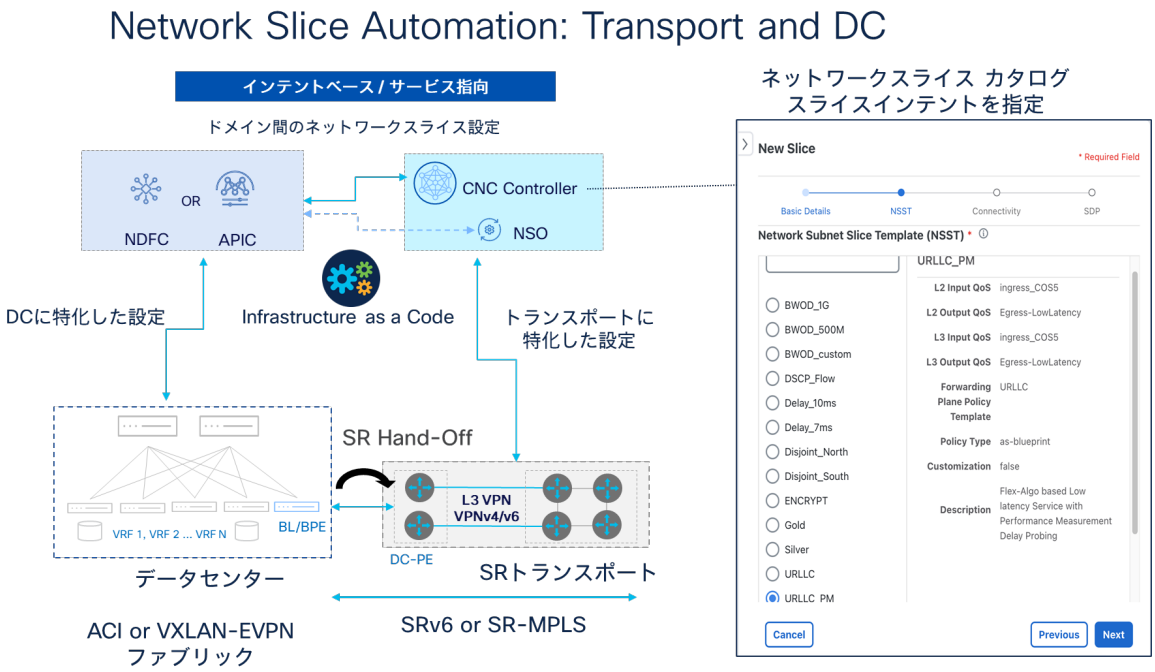
サービスプロバイダーは、5G に適応した分散型テレコムデータセンターの構築を進行中です。同時に、トランスポートドメインにおいてはセグメントルーティング（SR）やマルチプロトコル ラベルスイッチング（MPLS）の利用が進んでいます。これらのサービスプロバイダーは、データセンターからトランスポートドメインに至るまでの自動化とポリシーの一貫性を要求しています。そのため、データセンター技術と SR ベースのトランスポートネットワークとをシームレスに接続するために、双方の技術に適したハンドオフが必要です。

データセンターのテナントからトランスポートに展開される VPN へのサービス連携は、要求される仕様に基づき、自動化されたプロセスによって実現されます。このプロセスにおいては、適切なドメイン間のネットワークスライシングが重要な役割を果たします。

これを遂行するために、自動化コントローラには以下のような特性が不可欠です。まず、コントローラはインテントベースの機能を有していることが求められます。すなわち、システムやネットワークが顧客の意図を把握し、それに応じて自動的に最適な構成や動作を実施する能力が必要です。次に、

コントローラは宣言的な性質を備えていることが重要です。これはプログラムやコードが「何を成し遂げたいか」を表明し、具体的な手続きや手法ではなく、望む結果や状態を宣言するスタイルを採用することを意味します。最後に、サービス指向のアプローチが必須です。ソフトウェアは個々のサービスとして設計され、それぞれが特定のビジネス機能を提供する構造や設計手法を採ります。これらのサービスは相互に協働し、統合されたアプリケーションやシステム全体を構築します。

図 17 ネットワークスライス オートメーション (トランスポートとデータセンター)



Reference: Cisco ACI SR/MPLS Handoff Architecture White Paper

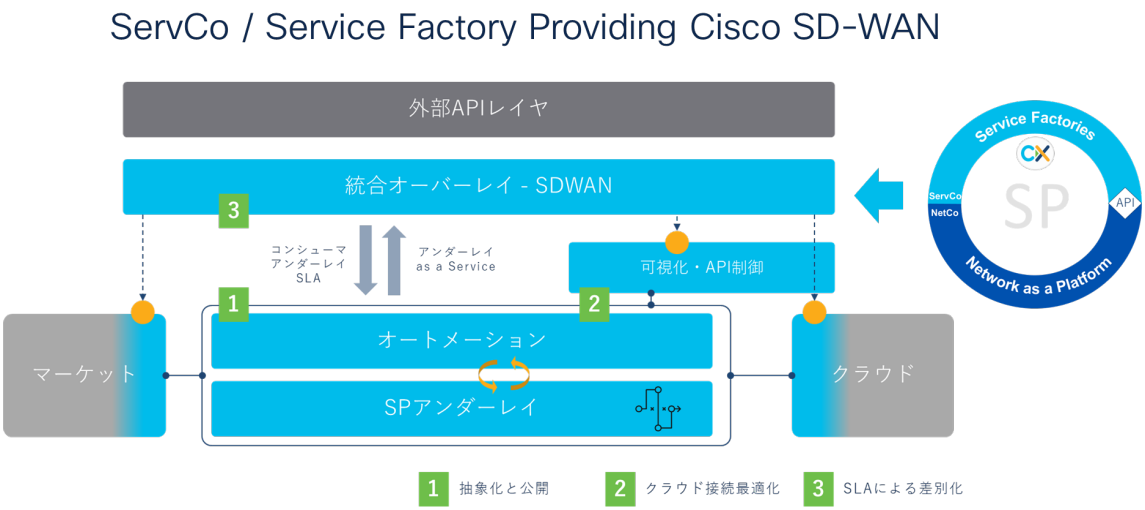
https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-744107.html

4.3 ユースケース 3：Service Factory Providing SD-WAN

Service Factory（ServCo）が提供するネットワークサービスは、Network as a Platform（NetCo）をアンダーレイとして利用する際に、API を介して SLA を指定して使用することになります。この抽象化されたインターフェイスにより、ServCo は NetCo の内部構造を意識することなく、サービスを開発・提供できるようになります。

SD-WAN は、ビジネスの要件に応じた高い柔軟性、信頼性、および顧客の特定のアプリケーションに合わせた品質保証を提供できます。サービスプロバイダーは、最優先事項およびハイタッチビジネス顧客のビジネス要件に対応するために、Service Factory は、SD-WAN とアンダーレイネットワーク間のシームレスな統合を 1 つのサービスとして提供できます。

図 18 ネットワークサービスとして Cisco SD-WAN を提供



ネットワークサービスとしてSD-WANを提供

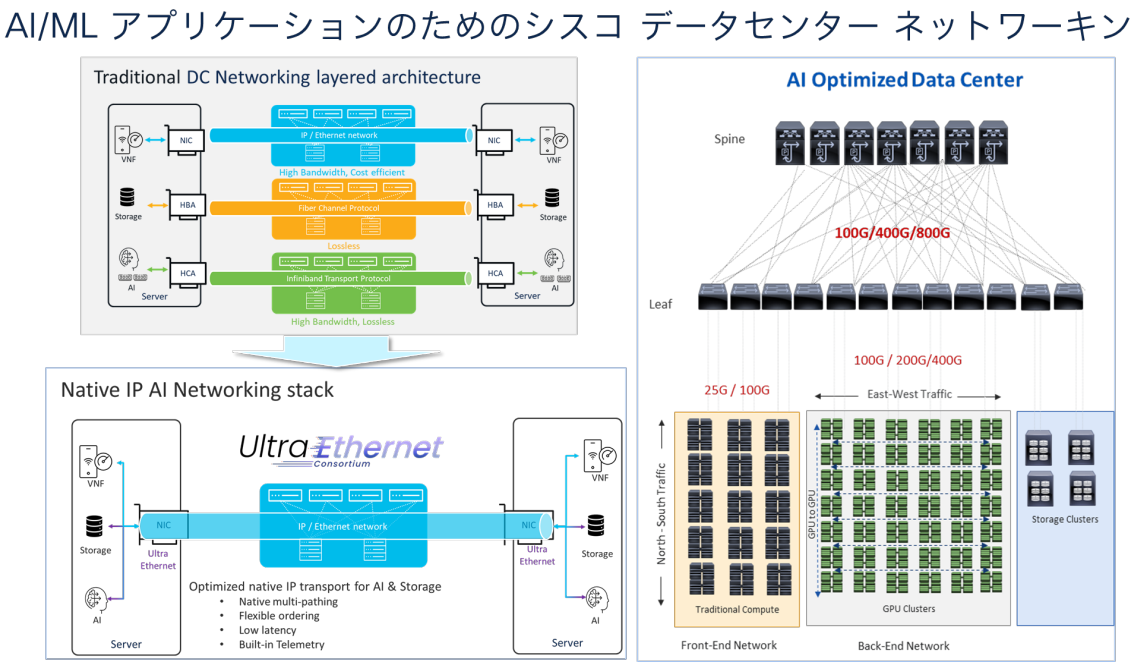
Reference: Cisco SD-WAN Solution White Paper
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/sd-wan/white-paper-listing.html

4.4 ユースケース 4：Native IP AI Network へ InfiniBand から Ultra Ethernet

AI 技術の進歩は、進化するネットワークインフラによってそのメリットが最大化されていきます。大規模な AI システムを運用する際には、単一の装置のみではなく、複数の装置を相互に連携させて計算を行うことが求められます。AI の計算プロセスでは高速性が要求されるため、複数の装置を用いたシステムでは、ストレージや GPU 間の通信速度が重要なファクターとなります。従来のデータセンターでは、IP、InfiniBand、ファイバチャネルなどの異なる技術の組み合わせが設計を複雑化し、システムの拡張性や柔軟性を損ねる課題が存在しました。

Ultra Ethernet 技術の採用により、AI とストレージシステムが必要とする低遅延のニーズを満たしながら、イーサネットベースの統一的なネットワークインフラを構築することが現実のものとなりつつあります。結果として、必要に応じて容易に拡張可能でありながら、柔軟性を維持したシステムが実現可能となります。将来的には、AI に特化したネットワークがイーサネットを基盤とした統合的なデータセンター内インフラと統合する可能性が高まっており、Ultra Ethernet 技術によって AI システムの通信インフラはシンプルでスケーラブル、かつ高い適応性を持つ「やわらかいインフラ」へと進化していくでしょう。

図 19 AI/ML のためのデータセンターネットワーキング



Reference: Enabling a new generation of AI with Ethernet

https://blogs.cisco.com/news/enabling-a-new-generation-of-ai-with-ethernet

Reference: Evolve your AI/ML Network with Cisco Silicon One White Paper

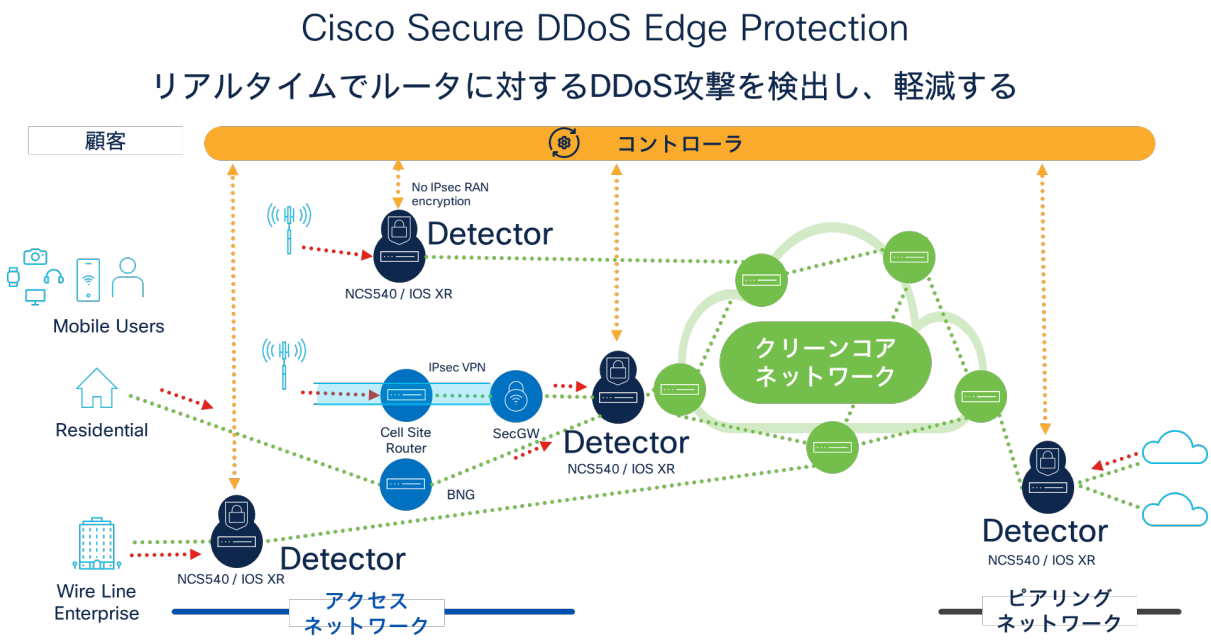
https://www.cisco.com/c/en/us/solutions/collateral/silicon-one/evolve-ai-ml-network-silicon-one.html

4.5 ユースケース 5：トランポートセキュリティ IOS XR DDoS エッジプロテクション

いくつかの 5G アプリケーションは、顧客にできるだけ近い場所に配置される必要があります。これにより、ネットワークオペレーターは、5G が求めるサブ 10 ミリ秒という厳しい遅延要件を達成します。しかし、5G に適したネットワークトポロジへの変更は、セキュリティの問題を引き起こし、ネットワークサービスの停止や、さらには顧客がアプリケーションを利用できなくなるような分散型サービス拒否（DDoS）攻撃のリスクを高める可能性があります。

シスコ セキュア DDoS エッジプロテクションは、サービスプロバイダーのネットワークエッジで発生するサイバー攻撃を防ぐための革新的なソフトウェアソリューションです。このエッジ保護ソリューションは、コントローラと 1 つあるいは複数のディテクターで構成されています。シスコ NCS ルータに展開されたエッジ保護は、セルサイトルータで DDoS 攻撃を検出し、対処する機能を持っています。DDoS 保護をネットワークのエッジに配置することで、サービスプロバイダーは 5G アプリケーションが要求するサブ 10 ミリ秒の遅延を満たすと同時に、顧客の品質体験（QoE）を保証することが可能となります。

図 20 シスコセキュア DDoS エッジプロテクション



Reference: Cisco Secure DDoS Edge Protection White Paper

https://www.cisco.com/site/jp/ja/products/security/ddos-edge-protection/index.html

Reference: Cisco DevNet Secure DDoS Edge Protection

https://developer.cisco.com/docs/secure-ddos-edge-protection/#!introduction

5 まとめ

本ホワイトペーパーでは、やわらかいインフラについて、その特徴や活用方法について解説してきました。やわらかいインフラとは、IT 業界においてこれまで IT 技術者の経験、知識、努力に支えられてきた課題に対し、今後予測される急激な変化に対応する永続的なアプローチを取り入れる概念です。これにより柔軟に対応しつつも、同時に堅牢性や高いセキュリティを維持することが可能です。

本ホワイトペーパーを通じて、やわらかいインフラの概要や主要機能、導入のポイント、またその効果についての理解が深まったと考えます。やわらかいインフラは、IT 業界でインフラ製品を提供するベンダーとしてユニークな戦略を持ち、ビジネスのアジリティが求められるインフラに必要な考え方を具備しています。この点において、多くの顧客から共感を得ています。

今後も、やわらかいインフラを含むシスコの CX サービスの拡充と品質向上に努め、顧客のニーズに応えるための努力を続ける予定です。やわらかいインフラの導入により、顧客のビジネス成功に貢献できることを願っています。

免責事項

IF THIS DOCUMENT IS PROVIDED AS A DELIVERABLE IN ACCORDANCE WITH THE CISCO TERMS AND CONDITIONS ASSOCIATED WITH A PURCHASED CISCO SERVICE (“TERMS”) THEN THIS DOCUMENT IS PRESENTED SUBJECT TO THOSE TERMS. IN ALL OTHER EVENTS, THIS DOCUMENT IS PROVIDED “AS-IS” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA 07/24