シスコが考える 5G 時代の エンドツーエンド アーキテクチャ

第 2 版

第 2 版刊行にあたって

高橋 寛嗣

2019 年の暮れに、本 5G アーキテクチャホワイトペーパーを発行してから、早くも 1 年が経過しようとしています。変化の激しい、通信、IT 業界において 1 年という時間はとてつもなく長く、その間に起こる変化は膨大なものとなります。シスコシステムズ合同会社としては、そうした変化を的確に捉え、最新の情報を公開すべく、ホワイトペーパー第 2 版の刊行を行うことにしました。

前回の初版を刊行後、様々な反響をいただき、本ホワイトペーパーに対する注目度の高さとその責任の大きさを感じております。そうした期待に答えることができるよう、第 2 版では内容を見直し、下記の通り最新情報を加筆しました。

- 第 1 章：RAN の構成要素である RU、DU、CU に関して、より詳細な記述を追記しました
- 第 2 章：時刻同期に関して追記をしました
- 第 3 章：4G CUPS から 5G へのシームレス移行に関して、よりわかりやすい図を含めて追記しました
- 第 5 章：一部の図を入れ替え、また新しく 5.10 を追記しました
- 用語集をソートするなど、より読みやすくなるよう修正しました

本ホワイトペーパーが、皆様の 5G 戦略立案・検討の一助になることを願います。

はじめに

山田 欣樹

5G は私たちの生活のあらゆるところに進化と革新をもたらすと言われています。一般ユーザにとっては超高速通信の実現によるこれまでにはない体験が提供され、非常にスケーラブルで低遅延対応のアプリケーションによって、様々な業界の企業にとっても新しいビジネス モデルを創造する機会となるでしょう。また、5G サービスを提供する サービスプロバイダーにとっても、これまでにはないサービスを一般ユーザや企業に提供することによって新たな収益源を確保する機会となるため、世界中のあらゆる業界で 5G の商用サービスに向けた取り組みが始まっているのです。

サービスプロバイダーにとっては、5G サービスを実現するためには課題があります。今後トラフィック需要が爆発的に増加することが予測されており、eMBB (超高速)、URLLC (低遅延・高信頼)、mMTC (多数同時接続)　といった 5G の厳しいサービス要件も満たす必要があるので、ネットワーク設備を大幅に増強する必要があります。また、接続されるデバイスが増大するとともにネットワーク上の脅威の対象も増大するため、サイバー セキュリティへの対策もこれまで以上に考慮する必要があります。一方で、収益性の観点から、設備投資と運用コストを抑制しつつ、サービス検討から収益化までの時間を短縮する必要性にも迫られています。従来のネットワーク アーキテクチャと運用方法では、これらの相反するニーズを同時に実現することはできません。そのため、これまでにはない技術革新が必要不可欠です。 サービスプロバイダーの通信インフラは、無線アクセス、トランスポート ネットワーク、分散データ センターなど、複数のドメインがあります。各ドメインで革新的なテクノロジーを採用することはもちろん必要ですが、それだけではドメイン毎に異なるテクノロジーが採用されて、全体として効率的で一貫性のあるサービス提供ができなくなってしまいます。 サービスプロバイダーが 5G サービスを実現するためには、ドメインを跨ったエンドツーエンドでのネットワーク アーキテクチャに基づいた通信インフラを構築することが重要なのです。

このブログでは、シスコが考えるエンドツーエンドでの サービスプロバイダー ネットワーク アーキテクチャと、それを支える 5G を中心としたテクノロジーについて、テーマごとに 9 章に分けてご紹介していきます。

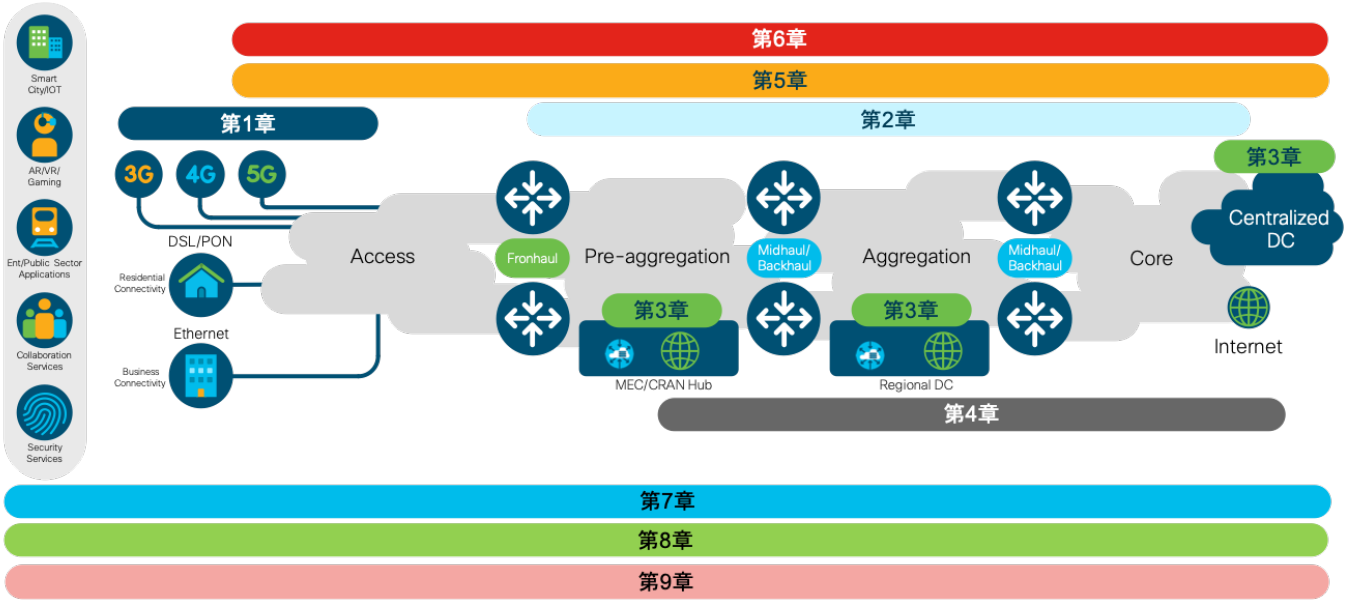


図 0-1 エンドツーエンド ネットワークと各章のマッピング図

目次

5G 時代の無線アクセス

大槻 暢朗

シスコが考えるサービスプロバイダー エンドツーエンドアーキテクチャ 第 1 章は、「5G 時代の無線アクセス」についてです。

5G とは、正確には 3GPP において定義された 5G New Radio (NR) を用いる第 5 世代移動体通信システム（モバイルコア、基地局、端末から構成されます）のことを意味します。日本においては免許認可有りの周波数帯で運用されます。

しかしながら 5G という言葉はすでに移動通信システムに留まらずアンライセンス帯無線通信システムや、Multi-access Edge Computing (MEC)、トランスポートを巻き込んだエコシステムを形成し始めています。

本章においてはその中でも無線アクセス技術に注目し、5G RAN を中心に 5G RAN とのインターワークが想定される無線アクセス技術（Wi-Fi、LoRaWAN）の特徴をご紹介し、最後にそれら無線アクセス技術の適用領域について考察します。

1.1 5G Mobile

ここでは 5G 時代における最も代表的な無線アクセス技術である 5G モバイルに関して、無線伝送技術ではなく RAN (Radio Access Network) の構成やトランスポートに焦点をあててご紹介します。

1.1.1 Virtualized RAN

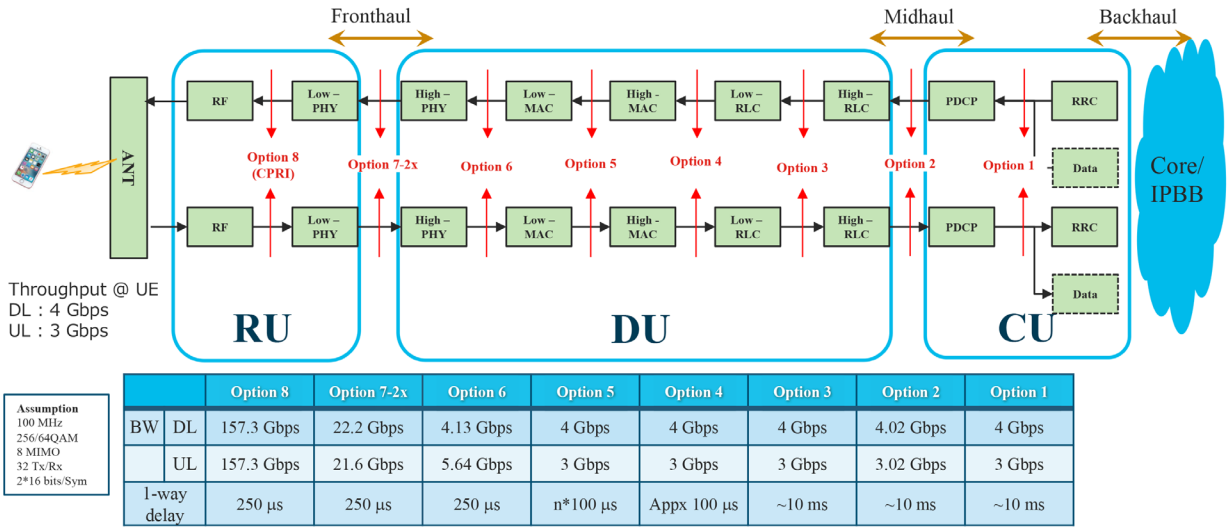
5G（第 5 世代移動通信システム）は 10 Gbps の最高伝送速度、無線区間で 1 msec 程度の遅延、100 万台/㎢ の端末収容数を特長としており [1-1]、これらを活かした新たなビジネスやサービスの実現が期待されています。しかし、5G を実現するための投資は莫大な金額となることが予想され、サービスプロバイダー (SP) の 5G に関する設備投資の効率化は喫緊の課題となっています。

その課題に対する対処の 1 つとして、5G ではアーキテクチャ全体が仮想化を想定した作りになっており、安価な汎用サーバの活用による投資効率化が期待できます。また、すべてのネットワークファンクション（NF）間のインターフェイス（IF）は 3GPP [1-2] において標準化されており、サービスプロバイダーは各ベンダーの製品ロードマップに縛られることなく最適なタイミングでさまざまなベンダーの最新かつ最適な機能を選択して、ソフトウェアという形で投資することが可能となっています。

この仮想化の取り組みは 4G の時代からコア ノードを中心に進められてきましたが、SP の CAPEX の 7~8 割が基地局機器・工事に由来するという状況を背景に、5G では同様の検討が Radio Access Network (RAN) の領域にも踏み込まれ、virtualized RAN (vRAN) の検討が進められました。

vRAN はその名のとおり仮想化技術によって RAN のファンクションを汎用サーバ上にソフトウェアで実装することが目的ですが、仮想化が実現できたとしてもその実装がベンダー独自となってしまうとベンダロックインの状態に陥るため、本来の目的である投資の削減効果が薄れてしまいます。そのため仮想化の過程として、ベンダロックインを回避するため RAN のファンクション間の IF やアーキテクチャを標準化することが重要になります。ここでは特に RAN の物理的な配置に大きな影響を与える IF の標準化に焦点を当てます。

図 1-1 に RAN のファンクション一覧とファンクションの分割方法 Option、ならびに要求条件を示します [1-2]。4G の Centralized-RAN [1-3] においては Option 8 (RF と Low-PHY の間) でファンクションが 2 つに分けられ、Radio Frequency (RF) は Remote Radio Head (RRH)、RF ファンクション以外のファンクションは Base Band Unit (BBU) という形で筐体を物理的に分けて実装されました。RRH と BBU の間の通信路はフロントホールと呼ばれ、Common Public Radio Interface (CPRI) [1-4] がデファクト スタンダードとなっています。



		Option 8	Option 7-2x	Option 6	Option 5	Option 4	Option 3	Option 2	Option 1
BW	DL	157.3 Gbps	22.2 Gbps	4.13 Gbps	4 Gbps	4 Gbps	4 Gbps	4.02 Gbps	4 Gbps
	UL	157.3 Gbps	21.6 Gbps	5.64 Gbps	3 Gbps	3 Gbps	3 Gbps	3.02 Gbps	3 Gbps
1-way delay		250 µs	250 µs	250 µs	n*100 µs	Appx 100 µs	~10 ms	~10 ms	~10 ms

図 1-1 RAN のファンクション

しかし CPRI は送信アンテナ数に比例して必要帯域が増加するという特性があり、4G と比較して送信アンテナ数が数倍に増加する 5G においては CPRI では対処が難しいという問題がありました。

そこで 5G では機能分割の仕方が再考され、3GPP において Option 2 での分割が規定されました。Option 2 で分割された際の RF 側のファンクション群を Distributed Unit (DU)、コア側のファンクション群を Centralized Unit (CU) と呼びます。しかし Option 2 ではキャリア アグリゲーション (CA)、Coordinated Multiple Point (CoMP) や enhanced Inter-Cell Interference Coordination (eICIC) のような DU 同士の同期要件が厳しい無線方式の実装が難しいという課題もあり、それらの機能が比較的容易に実装可能で、且つ CPRI の課題であった膨大な必要帯域を削減することが可能な Option 7 の検討が進められました。

Option 7 で区切られたファンクション群は RF 側を Radio Unit (RU)、コア側を Distributed Unit (DU) と呼びます。Option 7 はさまざまな方式が提案されていますが [1-5] [1-6]、世界のモバイル オペレータを中心に RAN のオープン化を議論している業界団体である Open RAN Alliance (ORAN) において Option 7-2x (ORAN split) が規定され [1-7]、世界の主要オペレータは今後 ORAN split を採用していくことを宣言しています。

これまでの RAN の世界ではベンダー独自の IF の実装方法等がネックとなり、RAN は 1 つのベンダーに閉じることが通例でしたが、インターフェイスの標準化と ORAN におけるベンダー独自の設定を排除した詳細プロファイルの規定により、仮想化とともにマルチベンダ構成が可能となり、RAN のオープン化が進展しています。

1.1.2 RAN の M-plane のオープン化

RAN はその性質上非常に細かく膨大な量のパラメータを持ちます。これらパラメータのチューニングがユーザ体感に大きな差を与えますが、チューニング作業は測定と調整の繰り返しでありオペレータは多大な作業量を強いられます。これを解決する手段として 3GPP においても Self Optimization Network (SON) の標準化が進められていますが、SON は各ベンダー独自の Element Management Systems (EMS) において実装されていることが通例であったため、同一エリアにてマルチベンダの基地局を運用することが難しいという問題がありました。また、オペレータの運用作業者にとっても複数 EMS のユーザインターフェースや機能を学習する必要があり、Opex 削減に向けた課題となっていました。

ORAN ではフロントホールのオープン化に加えて M-Plane (管理プレーン) の標準化が検討されてい

ます［1-8］。フロントホールと同様にこれまでの基地局はベンダー独自の仕様で閉じられており、上記で述べたようなベンダロックインの課題がありました。

そのような現状を打破するべく ORAN では RAN の機能部を定義し、それを標準化されたモデル言語である YANG 言語で記述する機構とインターフェイスを標準化しました。YANG によるモデル化はルータのドメインにおいては近年実装がデファクト スタンダードとなり、それを活かしたベンダー共通 Operation Support System (OSS) やさまざまなソリューションによるプロビジョニング等のネットワーク自動化が急速に進められています。今後は RAN のプロビジョニング と SON を含めたエンドツーエンドのネットワーク自動化が推進されると期待されています。エンドツーエンドのネットワーク自動化については別章で取り上げます。

1.1.3 RAN 仮想化の現状

1.1.1 項において RAN の仮想化とインターフェイスの標準化の動きについて紹介しました。本項では RAN 仮想化の現状について述べます。

5G では RAN の構成要素として大きく RU、DU、CU があることを前節で述べました。RU はデジタル処理が可能な部分もありますが、デジタル信号を電波というアナログ信号に変換する機能部を備えているため、仮想化は困難です。そのため仮想化が進められている機能は DU と CU となります。CU については必要となる計算規模は比較的軽く、汎用サーバ上で十分な性能を発揮することが可能です。一方 DU については、 PHY 部、特に Multiple Input Multiple Output (MIMO) の信号分離演算や Forward Error Correction (FEC) の復号演算の処理が大規模になってしまうため、現状の CPU 性能では処理速度が追いつかないことがわかっています。

そこで、DU を汎用サーバ上で動作させるために Field Programmable Gate Array (FPGA) 等のハードウェア アクセラレーターを追加し、処理の一部をハードウェアにオフロードさせる手法を用いることが多くなっています。 このようにハードウェアアクセラレーター を追加することにより DU についても専用筐体は不要となり、 vDU を汎用サーバ上で実装することが可能となりますが、ハードウェア オフロードは他の Virtual Network Function (VNF ; 仮想化ネットワーク機能) とのハードウェア共通化やオートヒーリング等の仮想化ならではの運用を難しくするなど、一定の制限が加わることになります。しかしそれでも汎用サーバで RAN を実現することによる装置設置スペースや消費電力の削減は、RAN の構築・運用に関わるコストの削減に大きく貢献することが期待され、多くのモバイルオペレータで導入の検討が進められています。

1.1.4 5G RAN を収容するトランスポート

1.1.1 項において、ORAN split と Option 2 という 2 つの代表的な RAN のファンクションスプリットをご紹介しました。本項ではそれぞれのスプリットの間に入る伝送路の要求条件を満たすトランスポートの観点から RAN の形態について考察します。

図 1-2 に 5G で想定される代表的な RAN の形態について示します。ORAN split は Lower Layer Split (LLS) とも呼ばれます。ORAN split ではそのアーキテクチャ上の理由から RU - DU 間 (フロントホール) の遅延を 250 µsec 以内に抑える必要があります［1-2］。装置の実装にも依りますが、250 µsec の内、RU/CU/DU 内での処理遅延等を考慮すると伝送遅延のマージンとされるのは 100 µsec 程度と一般的に考えられており、ファイバ内の光の速度を 2.0×10^{8} m/s と仮定すると、RU - DU 間の距離は 20 km 以内という制約が出ることを意味します。これらの遅延の制約は無線区間の再送制御である Hybrid Automatic Repeat reQuest (HARQ) の制約に起因します。5G ではこの制約を緩める検討もされていますが、5G の特長の 1 つである超低遅延を実現するためには劇的な緩和は期待できないため、この程度のマージンがリーズナブルと考えられます。

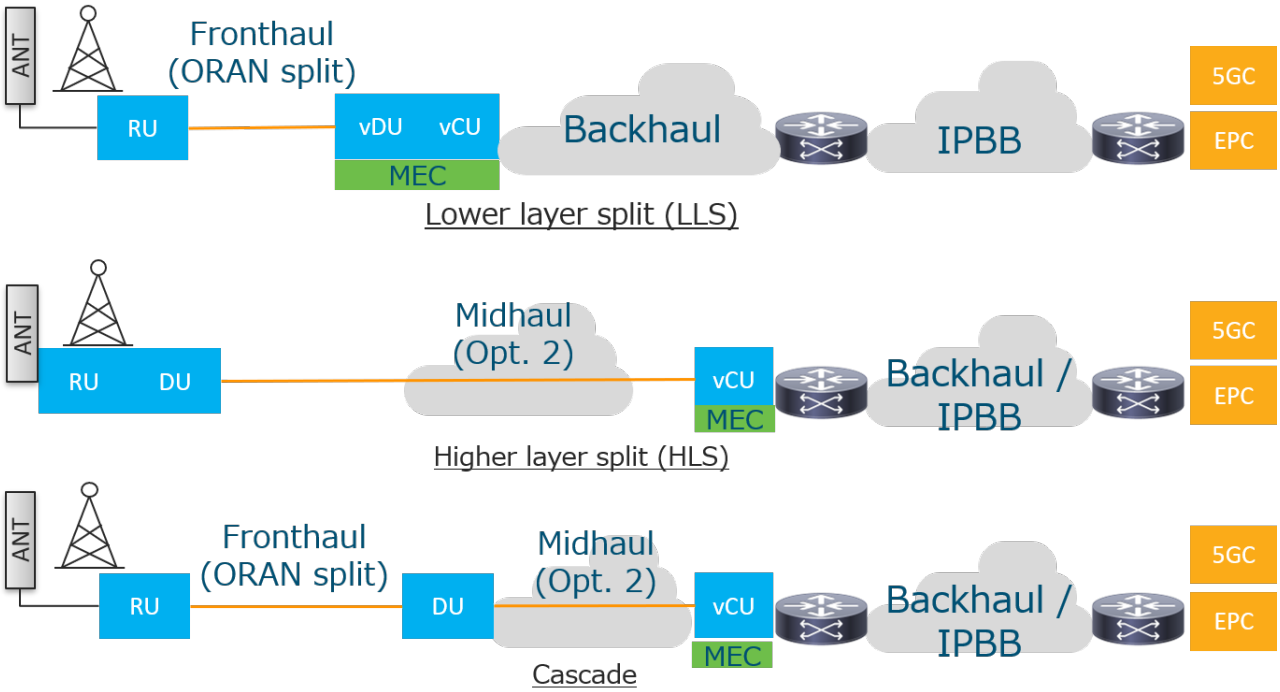


図 1-2 代表的な RAN の形態

Split 2 は Higher Layer Split (HLS) とも呼ばれます。HLS における DU - CU 間のネットワークはミッドホールと呼ばれます。ミッドホールはフロントホールと比較して、必要帯域、遅延、双方の面から大幅に要求条件が緩和されます。遅延の面については 250 µsec から 10 msec へと緩和されます。こちらも伝送遅延のためのマージンは装置実装に依存しますが、仮に 10 msec のほぼ全てを伝送遅延のマージンと考えると、約 2,000 km まで DU - CU 間の配置を離すことができるため、ほぼ制限はないと考えることができます。HLS ではこの特徴を活かし、地理的により NW の上位の方に CU を集約することで仮想化のメリットを享受しようとする検討が増えています。

また、フロントホールは必要帯域がミッドホール及びバックホールと比べて格段に多く、ユーザ スループットを改善する際のボトルネックになりやすいため、特に高スループットを期待されている mmW の (ミリ波を利用する) 基地局は RU と DU を 1 つの筐体に収めてサイト側に設置する Option 2 が選択されるケースが多くなると考えられています。一方で 1.1.1 項でも述べましたがセルエッジのスループット改善のために CoMP や eICIC 等 Advanced 機能を使用する場合は ORAN split の形が有効となります。

このような現状を踏まえると、ORAN split と Option 2 はどちらがよいという議論ではなく、各サイトの状況と各 SP のエリア展開戦略に応じて使い分けつつ共存していくことになると考えられます。当然 2 つの方式が 1 つのサイトに重畳されるパターン (例えばマクロセルは ORAN split でスモールセルは Option 2) も増加すると考えられます。このような状況において効率的にネットワークを構築するためには、フロントホールとミッドホールという要求条件の異なる 2 つのネットワークを 1 つのトランスポートで構築することが重要となります。ORAN split、Option 2 共にパケットベースのインターフェースとなっているため、フロントホールとミッドホールはパケットベースのネットワークに重畳可能です。4G のフロントホールのデファクトスタンダードである CPRI は Time Division Multiplexing (TDM) をベースとした各ベンダー独自の仕様であり、パケット多重が不可能でした。そのため 4G のフロントホールでは WDM を用いてファイバを集約することが一般的でしたが、5G の世界では、スイッチやルータといったネットワーク機器を用いることで、より安価かつ柔軟なパケットベースのネットワークでフロントホールとミッドホールを重畳する検討が盛んになってきています。フロントホールのパケ

ットネットワーク化により、(1) フロントホール回線の冗長性、(2) 複数基地局のフロントホール回線を物理的に 1 つに集約、(3) 他の通常 LAN 回線 (ビル内 LAN 等) との NW 共用、の実現が可能となります。これも RAN のオープン化の効果ということができます。

1.1.5 Time Sensitive Network (TSN)

では、フロントホール、ミッドホール、通常 LAN 回線を 1 つのネットワークに重畳するにはどのようなトランスポート技術が必要になるかを考えてみたいと思います。

ネットワーク化のためにルータ等の装置を挿入すると、その装置における処理遅延が発生するため、1.1.4 項で述べた ORAN split 時におけるフロントホールの距離制限 20 km が、装置での処理遅延に応じてさらに短くなってしまうという課題が発生します。装置内遅延は主に、低優先なジャンボ パケットが入ってきた際に伝送自体に時間がかかってしまい、その間に高優先な ORAN split パケットがキューイングされることで発生します。

一方でミッドホールの距離制限は 2,000 km と長いため装置の処理遅延は問題になりません。そのためフロントホールとミッドホールを 1 つのパケットネットワークに重畳するには、いかに遅延要件の厳しい ORAN split のフロントホールのトラフィックを、遅延要件のゆるい Option 2 のトラフィックや、その他のベスト エフォート トラフィックよりも優先することができるか、が重要となります。Time Sensitive Network (TSN) はこの装置遅延の問題を緩和することができるイーサネット技術です [1-9] 。TSN では、そのようなキューイング状況が発生した際に低優先のジャンボパケットの送出が終わるのを待つことなく中断し、高優先パケットを優先的に送出することができるようになります。TSN により、ORAN split においても NW 機器の処理遅延を抑制し、ジッタも低く抑えることが可能となります。フロントホールとミッドホールを重畳する際に TSN は必須の技術といえるでしょう。

1.2 Wi-Fi 6

従来の「Wi-Fi」という言葉は IEEE802.11 で規定された無線 LAN 規格 のベンダー相互接続性を担保するための団体である Wi-Fi Alliance から取られた無線 LAN 機器の通称でした。そのため、技術の進歩は規格名で表されており、主だった規格に注目すると IEEE 802.11b/a/g/n/ac と呼称されてきました。

しかし Wi-Fi という名称が一般に十分浸透したという背景と、規格名では技術の進歩が一般ユーザにわかりづらいというマーケティングの観点から、最新の規格である IEEE 802.11 ax からは Wi-Fi 6 という名称が用いられることになり、技術の進歩が番号で分かるようになりました。IEEE 802.11 ac は Wi-Fi 5 と呼ばれます。

これまでの Wi-Fi の進化は、個々の端末のピークスループットを向上させることを主に考えられてきましたが、Wi-Fi 6 ではシステム全体のスループットの向上に向けて舵が切られています。Wi-Fi 6 のシステムスループット向上に資する主な特長を次に示します [1-10] 。

1.2.1 OFDMA

Wi-Fi 6 の最も大きな特徴は、多元接続の方式が、これまでの分散制御である Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA; 搬送波感知多重アクセス/衝突回避) から、集中制御の Orthogonal Frequency Division Multiple Access (OFDMA; 直交周波数分割多元接続) ベースに変更となったことです。

図 1-3 に従来の CSMA/CA ベース OFDM と OFDMA ベースのリソース割当の概念図を示します。これまでは、送信権を持った端末が全ての周波数リソースを使って送信し、多元接続は時間的に分割することで実現されていました。そのため特に音声等のショートパケットでは周波数リソースを使い切れず、無駄が生じていました。

Wi-Fi 6 では、 OFDMA の採用により、周波数リソースを細分化して必要な分だけを複数端末に割り当てることができるようになったため、無駄が削減されシステムスループット・遅延の改善が期待できます。また、これまでの時間軸方向のリソース制御だけではなく、その端末にとって最も適切な周波数のみを用いて通信を行う等の、時間/周波数軸の両方にわたる細かな無線リソースの制御も可能となり、通信品質の改善も期待できます。

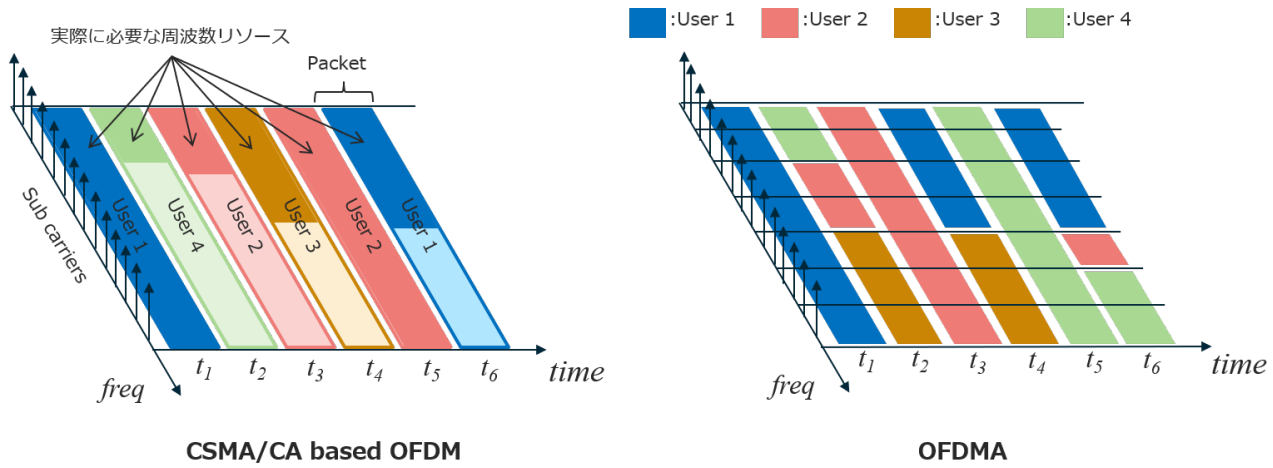


図 1-3 多元接続方式

1.2.2 MU-MIMO

集中制御型となったことにより可能となる技術に Multi-User Multiple-Input Multiple-Output (MU-MIMO) があります。MIMO 技術はアンテナの数に応じて送信するデータストリーム数を増加させることが可能な技術ですが、従来の規格でも対応していた Single-User MMO (SU-MIMO) の場合、送受信のアンテナ数の内、少ない方のアンテナ数が限界となります。

筐体の大きさから、一般的にアクセスポイント (AP) の方が端末よりもアンテナの数が多く、1 対 1 で通信を行う場合は AP のアンテナ数を全て活かすことができませんでした。しかし MU-MIMO では、同じ周波数・同じタイムスロットで、ビームフォーミング技術を用いて端末が空間的に棲み分けることにより、複数の端末が AP と同時に通信を行うことが可能となります (図 1-4)。すなわち、AP で備えるアンテナを限界まで活用し、システム スループットの向上が可能となります。MU-MIMO はダウンリンクのみ Wi-Fi 5 でも対応しましたが、アップリンクは端末同士の同期が必要であり技術的な難易度が高いため Wi-Fi 5 での導入は見送られました。しかし Wi-Fi 6 では集中制御となったため端末同士の同期が比較的容易となり、アップリンクの MU-MIMO に対応可能となりました。

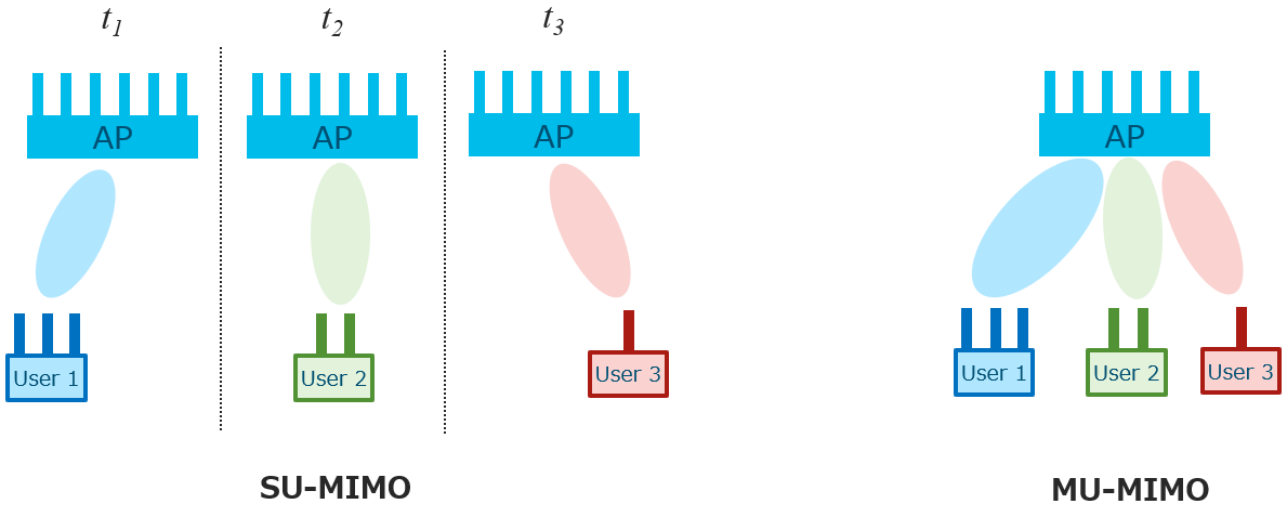


図 1-4 SU-MIMO と MU-MIMO の比較

1.2.3 BSS color

Wi-Fi 6 で OFDMA が導入されたものの、OFDMA による集中制御が可能となるのは Basic Service Set (BSS) に所属する (同一 AP 配下の同一グループ) 端末のみであり、異なる BSS を持つ AP や STA との空間棲み分けを実現する手段は listen-before-talk 方式の CSMA/CA が基本です。そのため複数の BSS が狭隘な空間にまとまって存在するような高密度環境においてチャネル間干渉が発生しスループットが劣化してしまうという課題は解決されません。

しかし、実際には隣接 BSS からの信号は微弱であり、検出はされるものの、同時に自分が送信したとしても問題なく受信可能となる場合が多く、現状の CSMA/CA による保護は過剰な保護と言える状態でした。

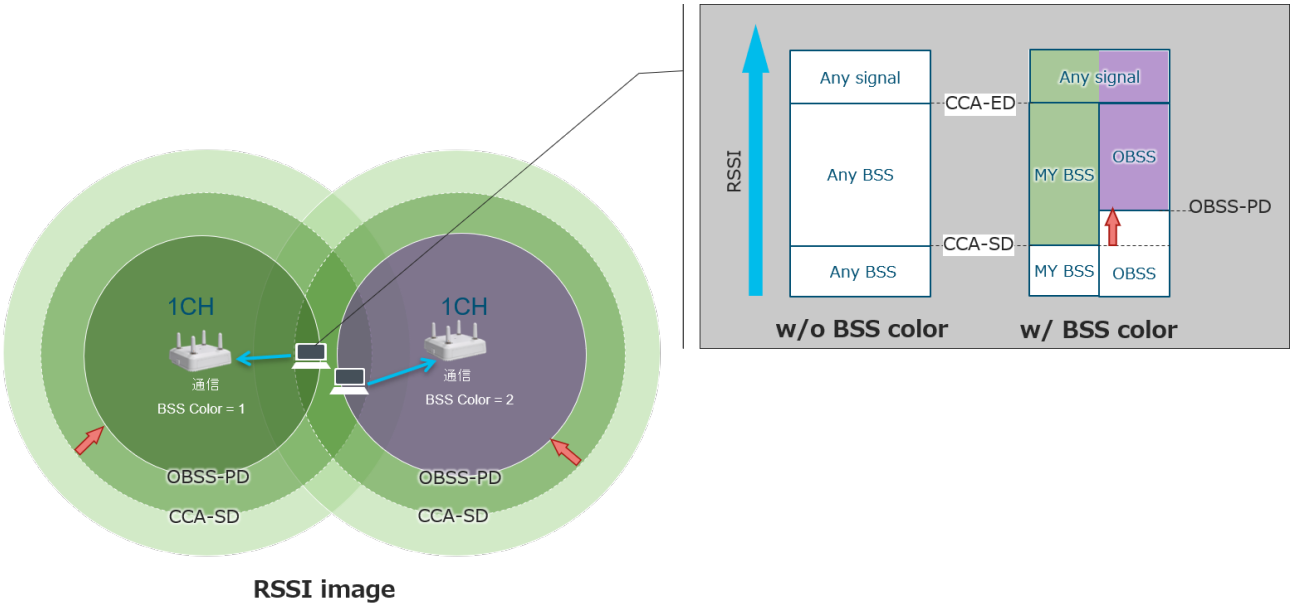


図 1-5 BSS coloring のイメージ

そこで Wi-Fi 6 では、BSS color と呼ばれる、BSS を識別するための ID を物理層の Preamble に入れることによって、MAC 層ではなく物理層のレベルで BSS を識別する方式が導入されました。また、自 BSS (MYBSS) 用のシグナル検出の閾値と、他 BSS (Overlapping BSS; OBSS) 用のシグナル検出の閾値 (OBSS_PD) を個別に設け、OBSS_PD を動的に調整することが可能となりました (Dynamic Sensitivity Control; DSC)。

これらを組み合わせ、かつ OBSS_PD を MYBSS より高く設定する (感度を鈍くする) ことで、どこかから信号が届いた際に、自 BSS の信号は受信するが、他 BSS (OBSS) からの信号は無視をして、当該チャネルは使用されていないと判断するという動作が可能となりました。これにより、周波数チャネルの繰り返し利用の効率が向上し、システム全体の効率を改善することが可能となりました。

1.3 LPWA

これまでの項では、ブロードバンド無線アクセス技術として 5G、Wi-Fi 6 をご紹介しましたが、本項では、主に Internet of Things (IoT) での利用を主眼に開発されたナローバンド無線アクセス技術である Low Power Wide Area (LPWA) についてご紹介します。

1.3.1 LPWA 概要

多様なアプリケーションの通信ニーズを満たすため、ブロードバンド化とは逆に、通信速度を落とすことでより低消費電力で広いカバー エリアを低コストで実現する LPWA が期待されています。LPWA には上記のニーズを満たすアクセス方式が複数提唱されています (表 1-1)。

表 1-1 主な LPWA のアクセス方式

System	LoRaWAN	Sigfox	LTE-M	NB-IoT
推進団体	LoRa Alliance	SIGFOWX	3GPP	3GPP
使用周波数	920 Mhz	920 Mhz	セルラと同一	セルラと同一
通信速度	290 bps ~ 50 kbps	上り：100 bps 下り：600 bps	上り/下り 300 kbps ~ 1 Mbps	上り：62 kbps 下り：21 kbps
カバレッジ	数 km ~ 十数 km	数 km ~ 十数 km	数 km ~ 十数 km	数 km ~ 十数 km

代表的なものとしては、非セルラー系の LoRaWAN、Sigfox、セルラー系の LTE-M、NB-IoT が挙げられます。特に LoRaWAN は非セルラー系では現時点で最も活用されている方式です。次の項で LoRaWAN の概要を述べます。

1.3.2 LoRa/LoRaWAN

図 1-6 に LoRaWAN のプロトコルスタックを示します。LoRaWAN ネットワークシステムは、正確には、LoRa という物理層の方式を規定した規格と LoRaWAN という Media Access (MAC) 層の方式を規定した規格で構成されています。LoRa は、端末の低消費電力化と端末価格低減のため受信機の構成を単純にしつつ、長距離伝送を実現するためチャープ スペクトラム拡散方式を採用しています。

LoRaWAN は、LoRa alliance によって定義されている MAC 層プロトコルです。スループットを犠牲にする代わりに低消費電力通信に特化した Aloha 方式を採用しており、同期型のセルラー系のシステムと比べて 3 倍以上のバッテリーのもちを実現可能です。基地局をゲートウェイとしたスター型のネットワーク構成を採用していますが、端末は特定の基地局ではなく複数の基地局に接続することが可能となっており冗長性を実現しています。

LoRa alliance は非営利標準化団体であり、世界中から多くの SP、インテグレーター、アプリケーション開発会社、センサー チップセット ベンダーが参加しています。アンライセンス帯で運用可能であるため、セルラー系と比較して比較的容易に運用可能であり、様々なアプリケーションへの適用が期待されています。

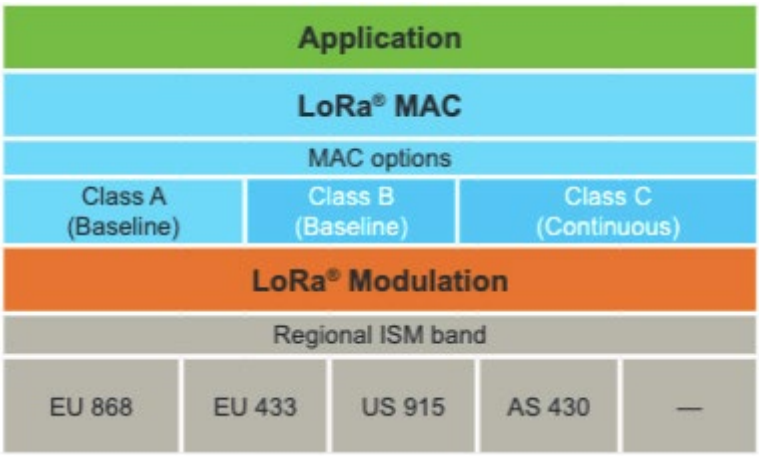


図 1-6 LoRaWAN プロトコルスタック

1.4 Multi access

先の項では 5G 時代における代表的な 3 つの無線アクセス技術のカテゴリについてご紹介してきました。ここでは、それら無線アクセス技術のすみわけについて考察します。

4G は、2010 年に日本で初めて NTT ドコモがサービスを開始しました。Wi-Fi は IEEE 802.11 n (Wi-Fi 4) が 2009 年に策定されました。同時期からモバイル端末にも Wi-Fi が実装されることが当たり前になり、同じ端末で 2 つの無線アクセス方式を使用できるようになると、モバイルと Wi-Fi はそれぞれ、通信料はかかるもののライセンス帯におけるマネージド サービスで屋外でもどこでも使える 4G と、使用場所が制限されアンライセンス帯であるため通信品質が不安定なものの 4G と比較して格安の Wi-Fi という棲み分けがされるようになりました。

Wi-Fi は当時の 4G と比較してスループットが高く、4G のトラフィックが爆発的に伸び始めると、4G のトラフィックをオフロードさせるための技術としても注目されました。

一方で、IoT の観点では、センサー ネットワーク等を中心に当初の 4G ではターゲットになっていなかった、「通信速度は低いものの低消費電力かつ安価な端末で広いカバレッジエリア」というニーズを満たすために各種 LPWA の検討も進みました。

しかし、モバイル技術の世代が 5G になると、使用される周波数として mmW (ミリ波) が追加され周波数幅が Wi-Fi と比べても格段に広く、5G が Wi-Fi のスループットを上回るようになります。ミリ波は電波伝搬による電力の減衰量がこれまでのモバイル用の周波数帯と比較して大きいため、高スループットが期待できるエリアは小さく (スモールセル) なる傾向があります。

また、同じモバイルの設備を用いて低速回線・低消費電力に特化した NB-IoT の検討が進み、5G 時代のモバイル技術は LPWA としても活用できるようになります。一方で Wi-Fi も Wi-Fi 6 ではモバイルと同様の OFDMA を採用し、アンライセンス帯でありながら、モバイルのような集中制御を取り入れて品質が安定しました。

ブロードバンドの観点から見ると、5G と Wi-Fi 6 は技術的に歩み寄りを見せており、特にミリ波の 5G と Wi-Fi 6 は、どちらの方式も狭いエリアで高スループットが期待できるという意味で近しいものとなってきました。

日本では、ローカル 5G と呼ばれる制度が新設されたことで、特定の市区町村、特定の敷地内といった地域限定で既存のモバイル オペレータ設備に頼らずに独自のモバイル サービスを提供できる下地が整い、多くの企業が参入を目指す状況になっています。この結果、 5G の通信料金が下がり、さまざまなサービスが創出されることが期待されています。

それでは、スループットは Wi-Fi を上回り、エリアの観点から運用方法も Wi-Fi に近づき、 Wi-Fi よりも安定した品質を持ち、広カバレッジで低消費電力 LPWA 通信もできる 5G モバイル技術があれば、 Wi-Fi も LoRaWAN も不要になるのでしょうか。いえ、そうではありません。

まず、ブロードバンド観点で Wi-Fi と 5G の比較を考えてみます。5G のサービスをユーザが受けるためには、基地局インフラが整備されることは当然として、併せて端末も 5G に対応した端末に替える必要があります。

現時点で Wi-Fi は、多くの企業内 LAN 等で使用されていますが、これを 5G に置き換えるためには、インフラの整備に加えて端末をすべてリプレースする必要があるため、現実的とは言えないでしょう。

一方、Wi-Fi であれば常に下位互換性を持つため、AP を Wi-Fi 6 に置き換えたとしても端末を取り替える必要はなく、端末の緩やかな入れ替えを待つというマイグレーション方法が可能です。また、モバイルと比較して品質が求められない代わりに、安価に実装できる Wi-Fi は、常にモバイルよりもサービス料金そのものが安価となるため、金額面での関係性もこれまでと変わりありません。

ミリ波の 5G と Wi-Fi 6 を比較すると、 どちらもスモールセルで運用されるという点では同じであるものの、Wi-Fi 6 は周波数帯が 2.4GHz 帯および 5GHz 帯であるため、壁の多いオフィス内等でのサービス エリア化を想定した場合、ミリ波よりもエリアの構築が容易となると考えられます。そ

して Wi-Fi は、アンライセンス帯であるため、周波数免許の取得が不要であり、特殊技能を持つ技術者を備える必要がなく難しい申請をすることもなく誰でも構築運用が可能です。

しかし、Wi-Fi は下位互換性を保つために従来の規格で使用されていたランダムアクセスの基本思想を受け継いでいます。そのため、全ての端末及び AP が Wi-Fi 6 に対応している場合には、安定した通信が可能となりますが、1 つでも未対応の端末がエリア内に存在する場合に効率は劣化してしまいます。また、アンライセンス帯であるため、干渉波を受けて通信に支障を来す場合も考えられます。5G はその逆で、インフラ構築運用は手間が掛かるものの、通信は安定しており、他システムからの干渉を受ける心配もありません。

次に、 LoRaWAN と 5G の比較を考えます。Wi-Fi と同様ですが LoRaWAN はアンライセンス帯で運用を想定されている無線アクセスシステムです。そのため誰でも 5G と比べて容易に無線設備を構築運用することが可能です。センサー ネットワークの需要があるエリアで NB-IoT に対応した 5G 基地局がタイムリーに構築されるかどうかは、サービスプロバイダーの設備計画次第になってしまうため、NB-IoT に頼ったセンサー ネットワークは、迅速なサービス展開に支障を来すことが考えられます。また、バッテリー寿命の観点から見ると LoRaWAN は セルラー系 LPWA と比較して 3 倍以上の寿命を実現できるとされているため、センサ端末のメンテナンスが大幅に楽になります。

一方で、 NB-IoT 等のセルラー系 LPWA は、 サービスプロバイダーが所望の地域のサービス エリア化を完了させてしまえば、ユーザは、面倒なインフラ構築やメンテナンスを行うことなくセンサー ネットワークを利用できるため、そのような場合においてはセルラー系 LPWA が適していると考えられます。

表 1 - 2 に 5G、Wi-Fi 6、LoRaWAN の特性をまとめます。

特に Wi-Fi は、 5G が普及すると不要になると考えられがちですが、上記の表のように、モバイルと Wi-Fi の根本的な特性は 5G/Wi-Fi 6 の時代においても変わらず一長一短があるため、ユーザとしてはユース ケースに応じて適切なアクセスを使い分けることが重要となります (図 1-7) 。

表 1-2 各無線アクセス技術の特徴

Technology	5G	Wi-Fi 6	LoRaWAN
Range	Short (mmW) / Long (Sub 6)	Short	Long
Spectrum	Licensed	Unlicensed	Unlicensed
Max Throughput	Up to 10 Gbps	> 1Gbps	Up to 20 Kbps
Delay	1-10 ms	Variable	100 ms
Qulity	High	Low	Low
Cost	High	Low	Low

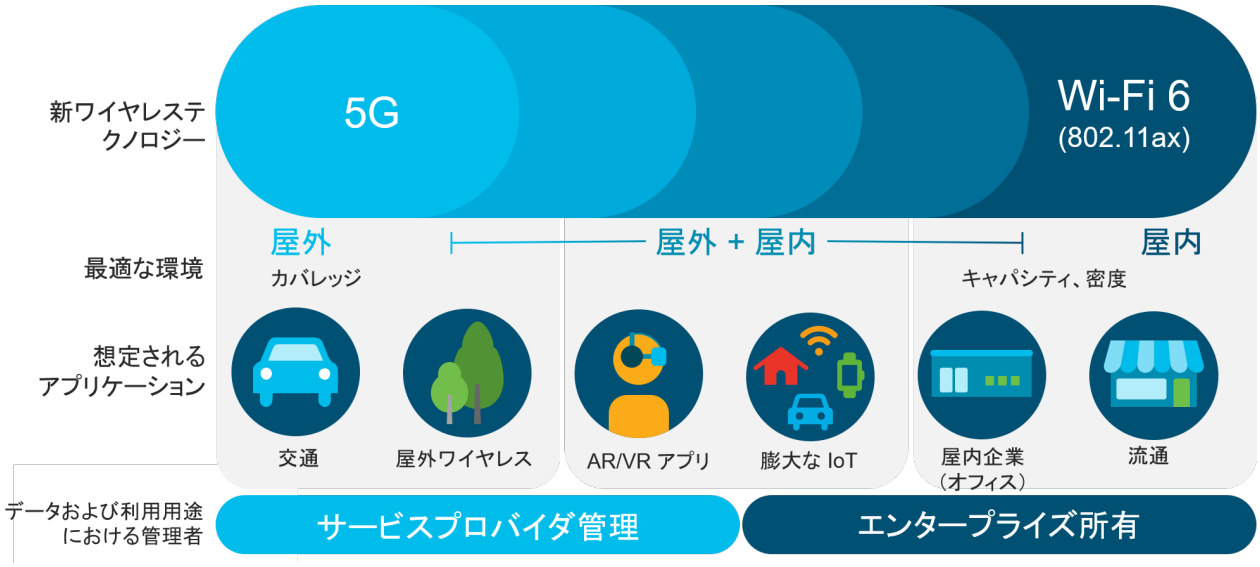


図 1-7 各種無線アクセス技術の使い分け

広範なサービス エリアを求められる場合には、当然 sub 6 (6GHz 以下の周波数帯) を用いた 5G と 4G LTE が必須となります。周波数の特性上、より周波数帯域の低い方が電波が遠くまで飛びやすく障害物にも耐性を持つためです。また、スモール セルの観点からも、安定した通信、低遅延/低ジッタが求められる交通システム、Factory Automation (FA) 、Virtual Reality (VR) /Augmented Reality (AR) システム等には 5G が適しています。

反対に、モバイル程の高品質は不要だがブロードバンド アクセスが求められるオフィス用アクセス回線としては、安価にインフラを整えられる Wi-Fi 6 が適していると考えられます。どちらか一方だけというものではなく、両方のアクセスを跨って、使い常に適切な回線を使い分けたいというユース ケースも出てくると思われます。

5G 時代における通信インフラはよりアプリケーション セントリックなものとなるため、ユーザからはアクセス回線を意識させないことが重要です。今後は、複数のアクセス回線を同じポリシーの下で運用可能とするコントローラが非常に重要な位置を占めることになるでしょう。

用語集

3GPP (3rd Generation Partnership Project): 3G (第 3 世代移動体通信システム) から発足したモバイル技術の標準化プロジェクト

AP (Access Point): 無線 LAN の親局

AR (Augmented Reality): 仮想空間を重ね合わせることで人間が知覚する現実環境を拡張する技術

BBU (Base-Band Unit): 4G の C-RAN 構成における集中制御部兼パケット-無線信号変換 (ベースバンド機能) 部

BSS color: BSS を物理層で識別するための ID

BSS (Business Service Set): 1 つの AP とその配下の無線 LAN 端末とで構成されるネットワーク

C-RAN (Centralized RAN): 無線基地局機能の内、無線機能の一部を張り出し、複数の無線機能部を 1 つの共通機能部を持つ RAN の形態の 1 つ。

CA (Carrier Aggregation): 複数の周波数チャネルを組み合わせてスループットを向上させる無線方式

CCA-ED (Clear Channel Assessment Signal Detection): 無線信号を検出するための受信電力の閾値

CCA-SD (Clear Channel Assessment Energy Detection): 無線 LAN 信号を検出するための受信電力の閾値

CSMA/CA (Carrier sense Multiplexing Access/Collision Avoidance): 通信前に干渉波の状況を確認してから送信する通信プロトコル

CoMP (Coordinated Multi-Point): 複数サイトから同時に同一の信号を送受信することで通信品質を向上させる無線方式

D-RAN (Distributed RAN): RRH と BBU が同一ロケーションに設置される、もしくは同一筐体となっている RAN の形態

EMS (Element Management System): 各装置の管理システム

FA (Factory Automation): 工場における生産工程の自動化を図るシステム。

FEC (Forward Error Correction): 誤り訂正符号

FPGA (Field Programable Gate Array): プログラムで再構成可能な集積回路

HLS (Higher Layer Split): 5G のファンクションスプリットにおける Option 2 の別称

IoT (Internet of Things): あらゆる物がインターネットに接続されるネットワークの仕組み

LLS (lower layer split): 5G のファンクションスプリットにおける Option 7 の総称

LTE-M: LTE 方式で低価格低消費電力に特化した IoT 向けモバイル通信技術。ハンドオーバが可能であり端末が移動する場合に適している

LoRaWAN: LoRa alliance によって策定された MAC プロトコル、およびそれをサポートする機器・システムの総称

MAC (Media Access Control): OSI 参照モデルにおける第 2 層

MEC (Multi-access Edge Computing): ネットワーク内のエッジ（物理的に UE [User Equipment] 寄りの位置）に計算機リソースを用意して各種処理を行うシステム、概念のこと

MIMO (Multi-Input Multi-Output): 複数アンテナを用いて送受信する無線通信方式

MU-MIMO (Multi-User MIMO): 同一時間同一周波数において複数端末と同時にデータを送受信する MIMO 通信方式

MY BSS: 当該端末が属する BSS

NB-IoT (Narrow Band IoT): LTE 方式で低価格低消費電力に特化した IoT 向けモバイル通信技術。端末が固定されている場合に適している

OBSS (Overlap BSS): 隣接する BSS

OBSS_PD (OBSS Packet Detection): OBSS の電波を検出するための受信電力の閾値

OFDM (Orthogonal Frequency Division Multiplexing): 直交周波数を利用して周波数利用効率を高めるデジタル変調方式

OFDMA (Orthogonal Frequency Division Multiplexing Access): 直交周波数を用いて多元接続を実現する通信方式

OSS (Operation Support System): サービスプロバイダーのシステム管理・運用を支援するシステムの総称

PHY (Physical): OSI 参照モデルの第 1 層 (物理層) 。物理信号の処理機能部

RAN (Radio Access Network): ユーザ端末をコアネットワークへ接続する無線アクセスネットワーク

RRH (Remote Radio Head): 4G の C-RAN 構成における張り出し無線機能部

RSSI (Received Signal Strength Indicator): 受信電力

SU-MIMO (Single-User MIMO): 同一時間同一周波数において単一端末と複数データストリームを同時に送受信する MIMO 通信方式

Sigfox: SIGFOX 社が提唱する IoT 向け無線通信方式

Sub 6: 6G Hz 未満の周波数帯の電波

TSN (Time Sensitive Network): 標準のイーサネットを拡張し、遅延に敏感な通信と通常通信の融合を図った方式

VNF (Virtual Network Function): 仮想化されたネットワーク機能部

VR (Virtual Reality): 仮想現実、ユーザの五感を刺激することで仮想的に物事を知覚させる技術

Wi-Fi: Wi-Fi alliance の相互接続試験に合格した機器の総称および無線通信システム

YANG (Yet Another Next Generation): データモデル言語の一種。NETCONF 等のネットワーク管理プロトコルと一緒に運用される。

eICIC (enhanced Inter-Cell Interference Coordination): 隣接サイトで連携しサイト間の干渉を低減させる無線スケジューラ

mmW (milli meter Wave): 30 ~ 300GHz の周波数の電波を指すが、5G では 28GHz 帯を指して使われる。

5G におけるトランスポート テクノロジー

鎌田 徹平

2.1 はじめに

本章では、5G におけるトランスポート ネットワークについて考えます。

5G のネットワークでは、Edge computing への対応や遅延に敏感なトラフィックへ対応するためにエンドツーエンドでの IP による接続性が必要だと言われています。これは、 Any-to-Any での接続を考慮した際に柔軟なサービス提供を行うための経路制御に必須のものであり、ネットワークを構成する要素を減らし、フラットな IP ネットワークで構築することによってネットワークがシンプルに構成でき、オペレーションの簡素化、さらには迅速なサービス展開につながります。

また、エンドツーエンド IP での構成により、アクセス ネットワークの統合による効率化を進めることができます。従来はさまざまなサービス タイプに応じて個別のアクセス ネットワークを持つことが必要とされてきましたが、IP で統合することによって物理的にも一本の Fiber 上に重畳できるようになります。これをシスコでは、 IP over Ethernet over Fiber と呼んでいます。

しかし、5G の要件も含めさまざまな要件が重畳されるネットワークではネットワークをスライシングする技術が必要になるケースがあります。シスコでは従来、IP ネットワークの簡素化に対してセグメント ルーティングと呼ばれる技術を提唱してきました。セグメント ルーティングは、ネットワーク スライシングとも親和性の高い技術です。次項ではこのセグメント ルーティングについて解説します。

2.2 セグメント・ルーティング

現在の IP ネットワークには、多くの構成技術/プロトコルが存在しており、複雑化の一途をたどっています。セグメント ルーティングは、このようなネットワークの複雑性の解決、これまでと同様の SLA 要件の提供、次世代のトランスポート基盤となりうる柔軟性の実現といった特徴を兼ね備えた IP ネットワークの基盤技術です。この技術は多くのネットワーク ベンダーとキャリアの参画により Internet Engineering Task Force (IETF) で標準化が進められ、ベースとなるアーキテクチャは RFC8402 [2-1] として公開されています。

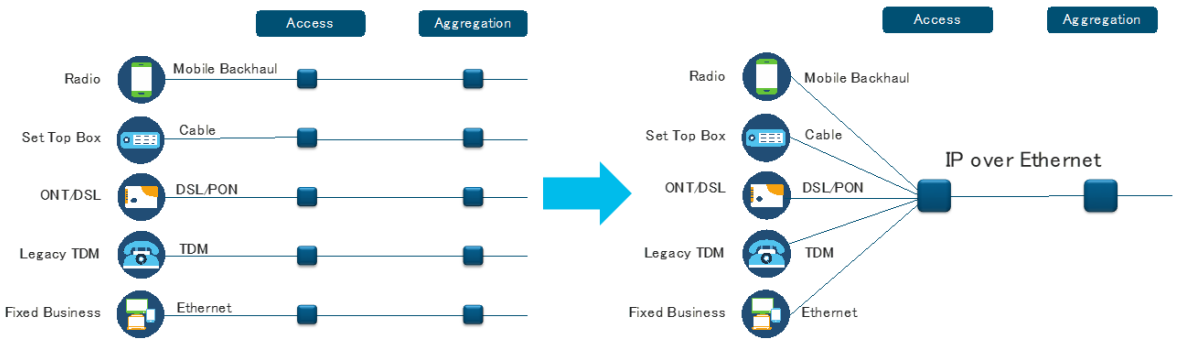


図 2-1 IP over Ethernet over Fiber 概要図

セグメント ルーティングでは、ネットワークの転送情報やサービス情報をセグメントと呼ばれる単位で表現し、シンプルかつ柔軟なルーティング制御を実現します。この概念をもとにさまざまな付加機能を提供できるため、キャリア網に代表される高可用性 (高 SLA) が求められる大規模 VPN ネットワーク基盤としての適用が可能です。セグメント ルーティングでは、IGP (OSPF/IS-IS) のみで、これまでの LDP、RSVP-TE といったプロコトルやそのステート情報を排除したステートレスなネットワークを実現できます。またセグメント ルーティングにより実現される Topology Independent Loop Free Alternative (TI-LFA) [2-2] では、IGP のみで障害時の迂回路を自動計算して高可用性ネットワークが構築可能となり、運用負荷を大幅に低減できます。

Software Defined Network (SDN) との高い親和性も大きな特徴です。送信元ノードがパスを選択し宛先までの経路を規定できるソース ルーティング アーキテクチャを用い、PCEP といったプロトコルへの対応により、オーケストレータからのパス制御やサービス追加も容易になります。

迅速なサービス提供、ネットワークの運用コスト低減などの観点から、これらのプログラマビリティ特性は次世代のネットワークには必須の要件と考えられています。

2.3 Label & IPv6 データ プレーン

セグメント ルーティング (SR) は、データプレーン非依存の技術です。現在 2 つのデータ プレーンに対応し、最初に実装が進んできたのは、多くのキャリア網で展開されている MPLS ベースの SR-MPLS [2-3] です。さらに、 Label 環境以外への適用が可能となる、現在まさに実装が進んでいるのが、 IPv6 ベースの Segment Routing IPv6 (SRv6) [2-4] です。これは多くの既存ネットワーク インフラを有効活用しつつ同じネットワーク上にセグメント ルーティングが展開できることを意味します。セグメントルーティング未対応機器との後方互換性を持つため、セグメント ルーティング ベースの次世代ネットワークにシームレスに移行できます。

セグメント ルーティングは、ソース ルーティングのため、送信元のルータがパケットの転送経路情報、パケットへ適用するサービス情報を付与します。この情報はセグメント ID (SID) と呼ばれ、SR-MPLS の場合は 20 ビットの Label として、SRv6 の場合は 128 ビットの IPv6 アドレスとして定義されています [2-5] 。

SR-MPLS では、1 Label に 1 つの情報を持ちます。転送情報とサービス情報を付与する場合、複数の Label をスタックすることでこれが表現されます。一方で、SRv6 では、1 つの 128 ビット SRv6 SID に宛先ノード情報を示す「Locator」、サービス情報を示す「Function」、オプション情報を示す「Argument」の 3 つの情報を埋め込むことが可能です。

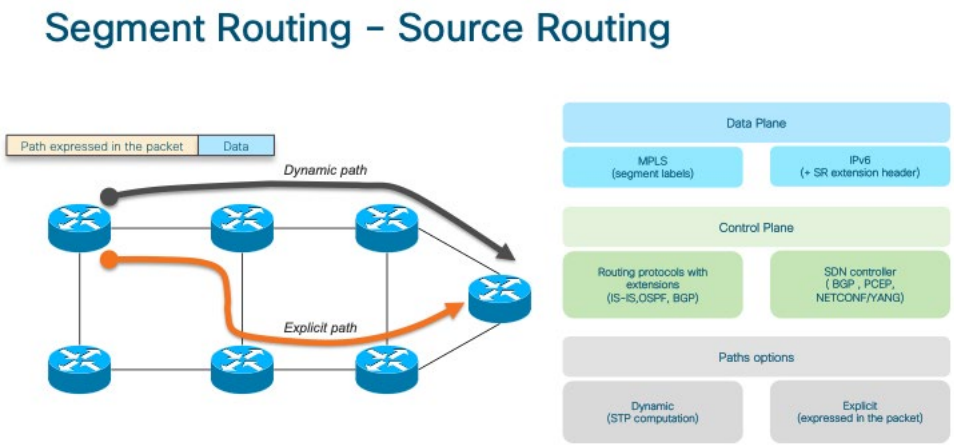


図 2-2 セグメント ルーティング構成要素

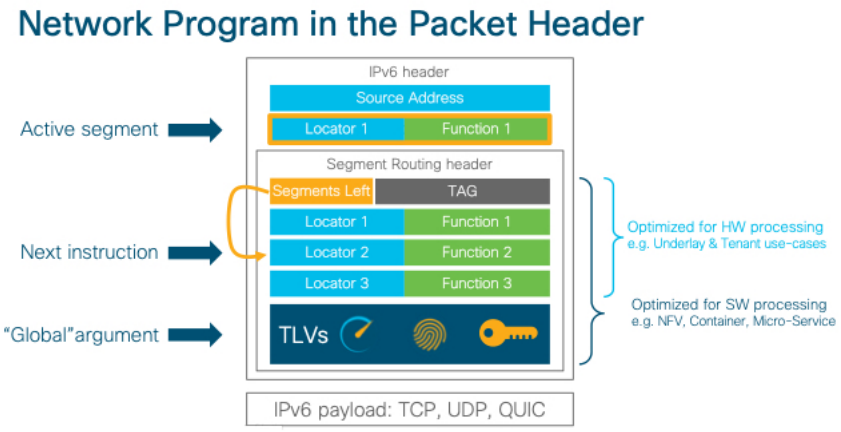


図 2-3 SRv6 パケットの構成

これら 3 つのビット長を選択可能にすることで、適用するネットワークのユース ケースに合わせて柔軟に SID を選択できます。また 1 SID の空間サイズ自体が大きくなるため、たとえばモバイル 5G ネットワークに求められる多数同時接続要件等へも十分な対応が可能です。

前述したとおり、セグメント ルーティングは SDN との親和性も高く、サービス チェイニング要件にも対応します。SR-MPLS では、サービス識別子を Label として積み重ねることで、SRv6 では SID の「Function」にサービス識別子を埋め込み Segment Routing Header (SRH) と呼ばれる IPv6 拡張ヘッダーに SID をスタックすることで (図 2-3)、適用するサービス群を送信元ノードから定義します。SDN コントローラにより送信元ノードへチェイニング情報を書き込むことにより、ユーザごとのサービスチェイニングもセグメント ルーティング ネットワーク上で実現が可能です。

2.4 ネットワークスライシング

ネットワーク スライシングは、次世代ネットワークに期待される機能要件の 1 つとして VPN や QoS、トラフィックエンジニアリングなどさまざまな手法による実現が議論されています [2-6]。セグメント ルーティングでは、トラフィック エンジニアリングの技術を活用し、ネットワーク リソースを最大限有効化したスライシングが実現できます。 2 種類の技術がネットワーク スライシング実現に適用可能であり、1 つは SR-TE [2-7]、もう 1 つが Flexible Algorithm (Flex-Algo) [2-8] と呼ばれるセグメント ルーティングとともに開発が進む新たな提案です (図 2-4)。

SR-TE は、従来の MPLS-TE と同様のコンセプトで、SID の積み重ねにより任意の経路でパケット転送を行うことができます。適用例としては、ユーザ単位でのパス制御などが想定されます (例：ユーザ 1: 高品質回線、ユーザ 2: 低遅延回線)。

Flex-Algo は、 IGP の拡張機能により実現されるマルチトポロジ ルーティング技術です。各ルータはアルゴリズムごとの IGP トポロジ データベースを持ち、それぞれのアルゴリズムで IGP パス計算が行われます。適用例としては、サービス単位でのパス制御などが想定されます (例：Algo-0: ベスト エフォート トポロジ、Algo-128: 低遅延トポロジ)。

SR-TE と Flex-Algo を柔軟に組み合わせることで、さまざまな要件に対応するネットワーク スライシングが実現できます。

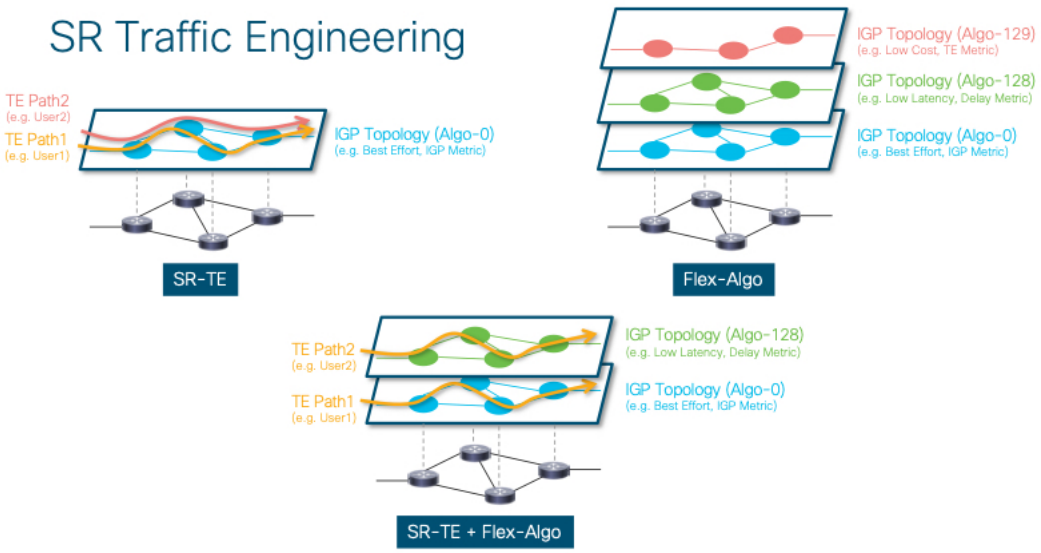


図 2-4 セグメント ルーティングによるネットワーク スライス

2.5 時刻同期

5G のトランスポートに対する重要な要件の 1 つに時刻同期があります。同期は、主に周波数同期と時刻/位相同期に分類されますが、LTE や 5G で提供する時分割多重通信にこの時刻/位相同期が利用されており、基地局において時刻同期を実現することで周波数帯域の利用効率を向上させることができます。

特に 5G ではさらなる帯域利用効率の向上や通信品質の向上のための高度な通信方式が求められており、非常に高精度の時刻同期が要求されます。時刻同期の精度は、Coordinated Universal Time (UTC) に対するエンドポイント (LTE/5G における基地局に相当) の時刻誤差を表す絶対時刻誤差と、エンドポイント同士の誤差を表す相対時刻誤差に分類されます。絶対時刻誤差は、LTE/5G 共に 1.5 μsec 以内と定義されています。相対時刻誤差については、どのような無線伝送方式 (アプリケーション) を適用するかにより異なります。表 2-1 に各アプリケーションにおける時刻同期精度の要件を記します。 [2-9]

表 2-1 各アプリケーションと時刻同期精度要件

Level of Accuracy	Typical Application (for information)	Maximum Relative Time error requirement
6A	Intra-band non-contiguous carrier aggregation, with or without MIMO or TX diversity, and Inter-band carrier aggregation, with or without MIMO or TX diversity	260 ns
6B	Intra-band contiguous carrier aggregation, with or without MIMO or TX diversity	130 ns
6C	MIMO or TX diversity transmissions, at each carrier frequency	65 ns

これらの要件を満たすために、従来、Global Navigation Satellite System (GNSS; 主に GPS) から受信する時刻情報に同期することで対応してきましたが、GPS では屋内や信号が弱い場所などでは利用が困難である、設置するのにコストがかかるといった物理環境に由来する問題点がありました。

そこで、Precision Time Protocol (PTP) [2-10] を始めとしたパケットを通して同期を行う技術に注目が集まっています。PTP では、Grand Master Clock (GMC) となる装置が GNSS と時刻同期を行ったあと、配下の装置である Boundary Clock (BC) や Slave に対して PTP によりパケットを通して時刻同期を行うことで、ネットワーク全体に対して単一の GPS ソースから IP を用いて同期を行うことができます。また、表 2-1 に記した精度を達成するために各構成要素に関してもさまざまな提案がなされています。

GMC について G.8272 [2-11] では最大時刻誤差 100ns を定義しており、高精度なレシーバを搭載することが求められます。また、GNSS と時刻同期ができなくなった際に、高精度な時刻を維持するために周波数同期を利用する手法として G.8272.1 が策定されています。

周波数同期技術としては Sync-E があり、PTP と並行して動作させるという検討も必要と考えられます。物理要件によっては GNSS 信号を受信できない、または品質を担保することができない可能性もあるため、いかに高精度な時刻情報を取得するかについては、今後も非常に重要なトピックの 1 つとして検討を重ねていく必要があります。

次に、 BC についても時刻誤差を低減するための要件があります。BC において時刻誤差を起こす要因としては主に 2 つあります。

1 つ目は装置内の処理遅延です。PTP ではパケットに対してタイムスタンプを打刻して隣の装置に対して時刻情報を広告し、隣の装置も時刻情報を打刻した PTP パケットを戻すことで双方向の伝送遅延を考慮した時刻同期を行います。

このタイムスタンプを打刻する際の処理遅延は、PTP の時刻同期精度に非常に大きな影響を与えるため、高精度なハードウェア タイムスタンプを打刻できる装置が必須となります。

また、装置内で打刻したあと PTP パケットを送信するまでの処理遅延についても検討が必要です。この処理遅延は装置の実装に依存し、標準化された方法での対処が困難であるため、あらかじめ注意が必要です。

2 つ目の要因としては装置間の伝送遅延です。特に双方向の伝送遅延が非対称となる場合には注意が必要であり、遅延変動を除去するための手法も議論されています。

上記のように時刻同期に関する要件は、ハードウェアに依存する要素が非常に大きいですが、5G のネットワーク要件としては必須要件となるため、念頭においてネットワーク設計を行う必要があります。

2.6 まとめ

2 章では、5G におけるトランスポートテクノロジーについて解説しました。5G のネットワークでは Edge computing への対応や遅延に敏感なトラフィックへ対応するためにエンドツーエンドでの IP による柔軟な制御が必須の要件となり、様々なサービスを重畳するケースも検討する必要があります。本章ではこの要件を満たす技術としてセグメントルーティングの紹介を行い、また、もうひとつ重要な要件となる時刻同期についても解説いたしました。

5G コアのクラウドネイティブ アーキテクチャ

尚 軍

5G 時代には、通信事業者はサービスの迅速化、高度化、多様化が求められる一方、加入者に投資コストを転嫁することは厳しく制限されます。そのため、無線ネットワークだけではなく、サービス提供の柔軟性にかかわる 5G パケット コアにも斬新なアーキテクチャが求められます。

2018 年以降実装された 5G トライアルと商用ネットワークのパケットコアは、基本的には 4G EPC をベースとした 5G NSA (ノンスタンドアロン) の実装です。

本章では、5G SA (スタンドアロン) パケットコアの 3GPP の標準化における定義を解説します。また、それを実現するためにクラウドネイティブアーキテクチャを追求したシスコ 5G SA パケットコア製品のアプローチと、そのアーキテクチャの応用および汎用化について考察します。

3.1 5G パケットコアの 3GPP の標準化定義

2G/3G/4G と進化してきたパケットコア ネットワークには、次のような課題があります。

- Control Plane (CP) と User Plane (UP) の完全分離がされていない。3GPP の Release 14 で Control/User Plane Separation (CUPS : CU 分離) の取り組みがありましたが、幅広く実装されていません。このようなモノリシック的なパケットコアのアーキテクチャでは、5G に期待されている高速大容量、超低遅延、多数同時接続などのユース ケースで必要とされる UP の柔軟な配置や、新サービスの迅速な立ち上げに求められる高度な自動化、CP/UP のそれぞれ独立したスケールアウトなどを実現することは不可能です。
- 障害時の復旧、新サービスの導入が困難。パケット コア内のネットワーク機能 (NF) 間では、1 対 1 のインターフェイス (Diameter、GTP-C) とコールフローが定義され、それぞれの NF が個別に複雑なステートを持っているため、新機能や NF の追加/変更の際に慎重な設計とテストが必要です。このため、スケールアウトや障害時の復旧、新サービスの導入に非常に時間を要します。
- アクセス ネットワークへの依存性。現在のパケット コア ネットワークは、アクセス ネットワークに依存する部分が多く、非 3GPP アクセス (Wi-Fi 等) への対応に大きな変更が必要になります。将来、衛星回線や固定ブロードバンドなど多様なアクセスの取り組みも視野に入れている 5G においては、アクセス非依存のアーキテクチャにする必要があります。
- ネットワーク スライシングへの対応。5G が多様なサービスを共通の基盤で実現するためには、パケット コアにもネットワーク スライシングの実現が必要です。しかし、4G EPC がモノリシックかつ密結合の構造であるため、自動化や、効率的で柔軟なスライシングの実現が非常に困難です。

以上の課題から、5G で要求される高速大容量、超高信頼・低遅延、多数同時接続などの多様なユース ケースを効率的なネットワーク スライスにより自動化プロセスで実現するためには、より柔軟なアーキテクチャを持つパケットコアが求められています。

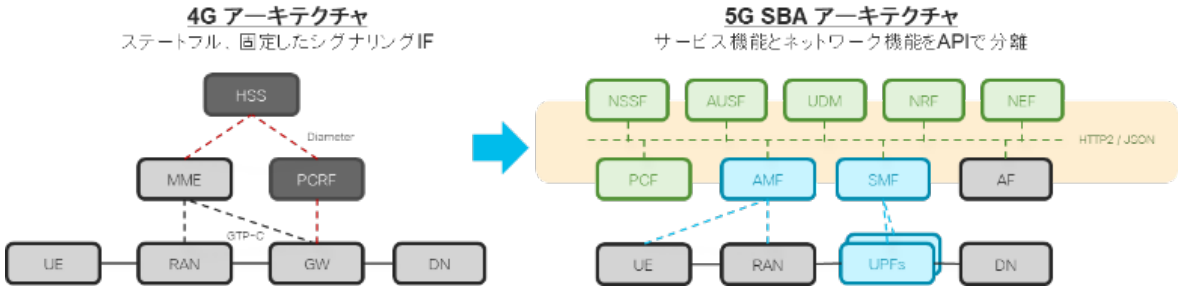


図 3-1 3GPP における 4G と 5G コア ネットワークの違い

2018 年 6 月に完成し、「5G Phase 1」と位置づけられた 3GPP Release 15 から、 5GC (5G コア ネットワーク) の主な特徴を次に規定しています [3-1] [3-2] [3-3] :

- CU の完全分離
- クラウド化と Service Based Architecture (SBA; サービス ベース アーキテクチャ) の導入
- ネットワーク スライスに対応するためのコア ネットワーク内の NF 機能分担を再定義
- アクセス非依存

図 3-1 は 4G から 5G へのアーキテクチャの変化を示しています。SBA はコアの NF 機能をサービスとして捉え、インターフェイス (Service based Interface; SBI) を軽量な Web アプリケーション ベースに統一することで効率化を実現します。

従来のポイントツーポイントの Diameter や GTP-C 採用せず、 Web 世界で容易な自動化を実現できる HTTP2/JSON の RESTful API を採用しました。また、BUS 型のアーキテクチャを採用し、NF 間を互いに「サービス」としてリクエスト/レスポンス等の形で制御します。

3.2 クラウド ネイティブ アーキテクチャで実現するシスコの 5GC ソリューション

5G における迅速な新サービスの投入をコントロール可能なコストで実現するために、シスコは、5G コア ネットワークの実装に次の要素が必須と考えています :

- CUPS (CU 分離)
- クラウド ネイティブ (CN) 化: クラウド化と高度な自動化が可能な仮想化基盤
- CP (Control Plane) の SBA
- 仮想化環境の UP (User Plane) 性能改善
- ネットワーク スライスの効率的な実現
- エッジ コンピューティングの実現
- 4G EPC から 5GC へのシームレスな移行と共存

上記の要素を順に見ていきましょう。

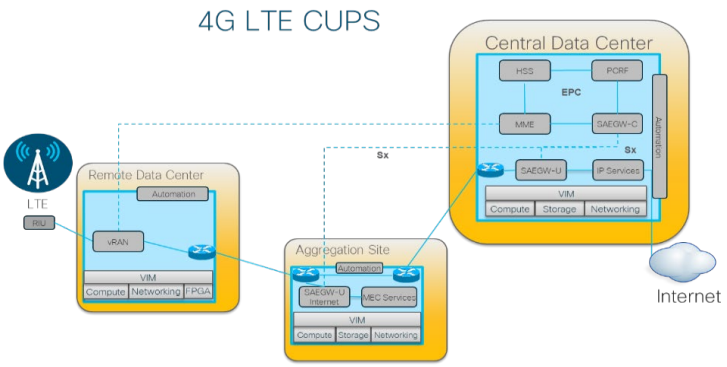


図 3-2 CUPS (Control/User Plane Separation)

3.2.1 CUPS (CU 分離)

シスコは、CUPS を 4G EPC から実装しており、5GC の CU 分離の基礎になりました (図 3-2) 。

CUPS の実装には次のメリットがあります。

- ユーザ機器において数 ~ 数十 Gbps のスループットを実現
- 処理能力拡張や保守運用作業を CP と UP で独立に行える
- CP を DC に集約したオペレーションが可能
- UP を VoLTE や IoT などのユース ケースごとに分離可能
- UP の物理的な配置が柔軟にでき、Remote CUPS による低遅延の MEC ユース ケースに対応可能
- 障害時の切り離しが容易 (UP 障害時も CP はサービス継続可能)

3.2.2 クラウド ネイティブ: クラウド化と高度な自動化が可能な仮想化基盤

数年前に、European Telecommunications Standards Institute (ETSI; 欧州電気通信標準化機構) の Management and Orchestration (MANO) Network Function Virtualization (NFV; ネットワーク仮想化) フレームワークが制定されて以来、パケット コアの NFV 化が進んでいます。しかし、多くの仮想化実装は、交換機時代の設計を踏襲し、元の機能を Virtual Network Function (VNF; 仮想化ネットワーク機能) で再ポーティングする仮想化アプライアンス化にとどまっているのが実情です。

本来 NFV で実現したいインフラとの分離、機能間の疎結合化、運用の完全自動化は、必ずしも実現できていません。逆に、仮想化基盤の導入と頻繁な変更への対応に多くの時間とコストがかかってしまうケースも見られます。

こうした経験を踏まえ、業界と多くのお客様が次に必要と考えているのが、クラウド ネイティブのアーキテクチャです。

シスコは、クラウド ネイティブのアーキテクチャを実現するために、4 つの重要な要素があると考えています (図 3-3) [3-4] 。

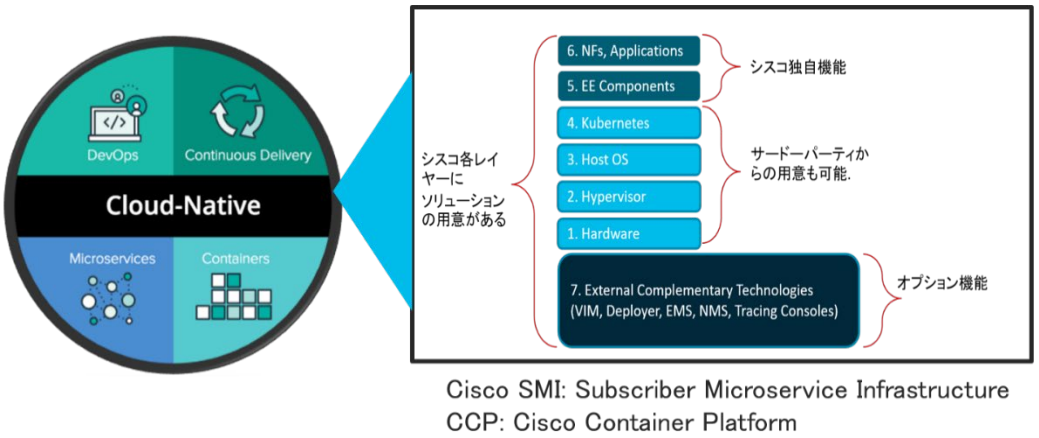


図 3-3 シスコが考えるクラウド ネイティブの 4 要素

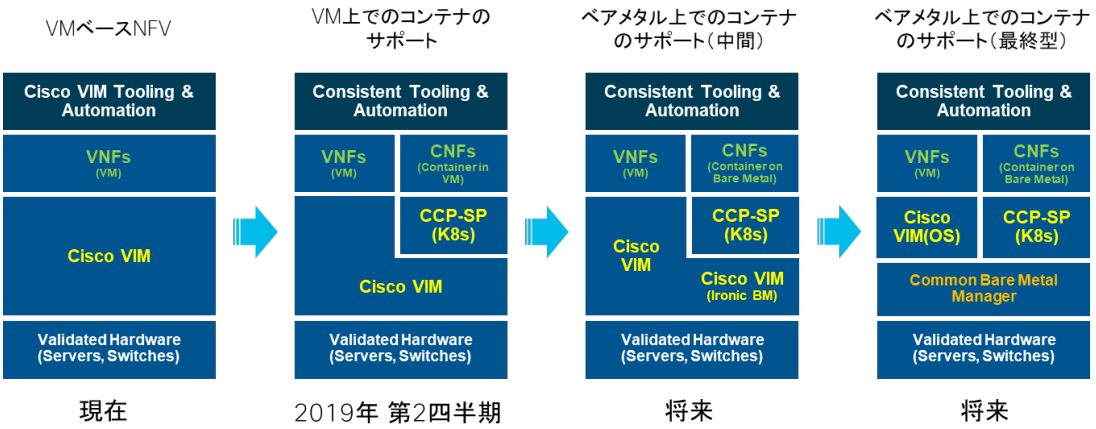


図 3-4 CVIM 仮想化基盤のクラウド ネイティブへの進化

- Microservices (マイクロサービス)
  - モジュラー、疎結合のソフトウェア サービス
  - 個々にデプロイ可能で、それぞれライフサイクルの管理が可能
  - ステートフルとステートレス アプリケーションの分離
- Containers (コンテナ)
  - マイクロサービスの仮想化と管理
  - マルチ環境への非常に高いポータビリティ
- Continuous Delivery (継続デリバリ)
  - 自動的に CI/CD (Continuous Integration/Continuous Deployment)
  - カナリア (Canary) イン・サービス アップグレードを可能
- DevOps
  - 迅速なデプロイの自動化管理
  - 検証環境と商用環境のギャップをできるだけ縮小し、商用への導入をスムーズにする

シスコのクラウド ネイティブ対応アーキテクチャは、今まで取り込んだ仮想化基盤 (CVIM; Cisco Virtual Infrastructure Management) の経験を踏まえて進化してきました (図 3-4) 。CVIM が 5GC のみのためではなく、より汎用的な仮想基盤を目指しています。

シスコは 5GC を実装するにあたり、クラウド ネイティブ時代の初期段階でお客様が導入しやすいよう、より統合され、かつオープンなアーキテク

チャを取ることが重要と考え、SMI (Subscriber Microservice Infrastructure) を 5GC の共通クラウド ネイティブサービスインフラとして開発しています。このアーキテクチャの実現には、業界のオープンソースを含めたさまざまなエコシステムと Web スケールの技術の取り入れが重要です。

シスコは、業界に幅広く採用されている Docker コンテナと自動化ツールの Kubernetes を採用し、CN プラットフォームの柱として、アプリケーションの自動化ライフサイクル管理を実現しています。図 3-5 にそのアーキテクチャを示しています。

- Infrastructure as a Service: VM、プライベート クラウド、パブリック クラウド、またはエッジ クラウドにも対応可能、将来ベアメタルへ移行
- Docker、Kubernetes、Istio 等が Service Mesh でアプリケーションのライフサイクル自動化を管理
- VPP (FD.io)、Contiv、また将来 NSM (Network Service Mesh) で高度化コンテナネットワークを実現
- アプリケーションのマイクロサービス化
- 共通サービスインフラ (SMI: Subscriber Microservice Infrastructure): アプリケーション間で共通な初期化、デプロイ、監視と可視化、パッケージ管理、memif (Shared Memory Packet Interface)、ステート データベースなどを効率的に管理
- 上位レイヤへの API 提供
- 各ドメイン内とドメインにまたがる自動化ツール (NSO、ESC、Matrix、Situation Manager など)

このクラウド ネイティブ アーキテクチャに基づき、シスコ 5GC がパブリッククラウドへの導入が可能になりました。現在 5G as a Service の開発を鋭意取り込み中です。

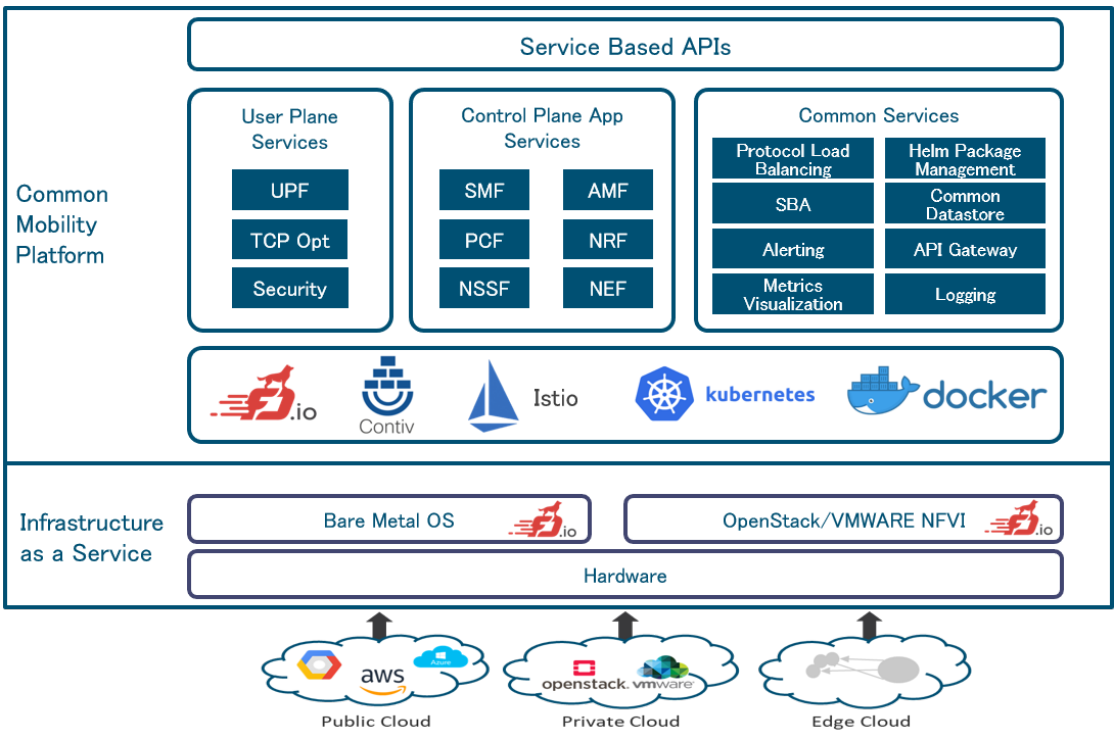
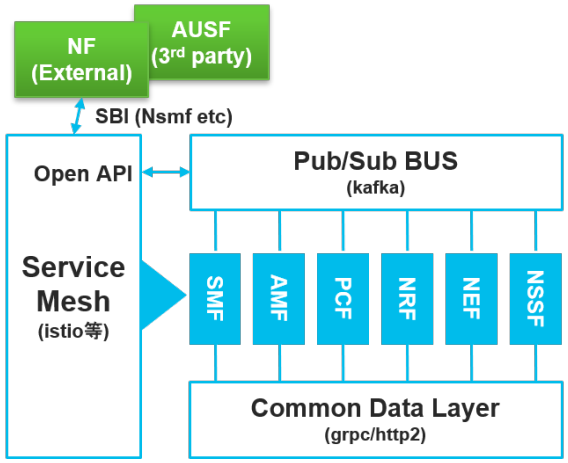


図 3-5 シスコのクラウド ネイティブ 5GC アーキテクチャ

3.2.3 5GC Control Plane の Service Based Architecture

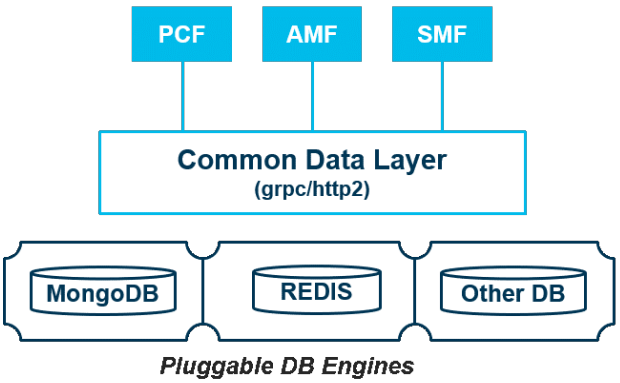
具体的にシスコの実装を見てみましょう。 シスコは、3GPP の SBA に準拠し、 Pub/Sub 通信用のメッセージバス (Kafka) を介し、オープン API を使ったネットワーク機能 (NF; Network Function) を開発しました。外部ネットワーク機能との通信は 3GPP 標準が規定する HTTP2/JSON ベースの SBI (Service Based Interface) を経由して行い、内部の通信は gRPC (google RPC) でパフォーマンスの最適化を図っています（図 3-6）。また、Istio 等 [3-5] を使ったサービスメッシュにより、マイクロサービス化されたネットワークファンクションのディスカバリー、トラフィックの制御、耐障害性とセキュリティーなどを実現しました。シスコでは、この SBA 共通実行環境を SMI (Subscriber Microservice Infrastructure) と呼んでいます。

セッションステート情報を保持するデータストアは、ネットワーク機能から分離されます（図 3-7）。データストアの高可用性と柔軟性を実現するために、共通データ層としてシスコが開発したのが、CDL (Common Data Layer) です。CDL は、高速キャッシュ、地理的冗長化などの特徴を持っています。



- オープンAPIを介したSBAサービスの公開
- 単一または複数NFをサポート
- 認証とセキュリティの強化
- 動的なサービス発見とポリシーベースルーティング
- 内部gRPCでパフォーマンス最適化
- Pub/Sub通信用のメッセージバス

図 3-6 SMI: シスコが提供する SBA 共通実行環境



- NFに公開されている共通データ層API
  - セッション状態情報は必要に応じて共有
- Pluggable DBエンジン – MongoDBとREDIS
  - パフォーマンス向上やデータ統合など要望により選択
  - 適切な場所に適切な量の状態を保存
- セントラル対ローカル展開
- 個別ライフサイクル管理
- 高可用性や地理的冗長構成の提供
  - 最高の可用性を実現するために、データベースを地域を分散して配置可能

図 3-7 ネットワーク機能から分離したデータストアの構造

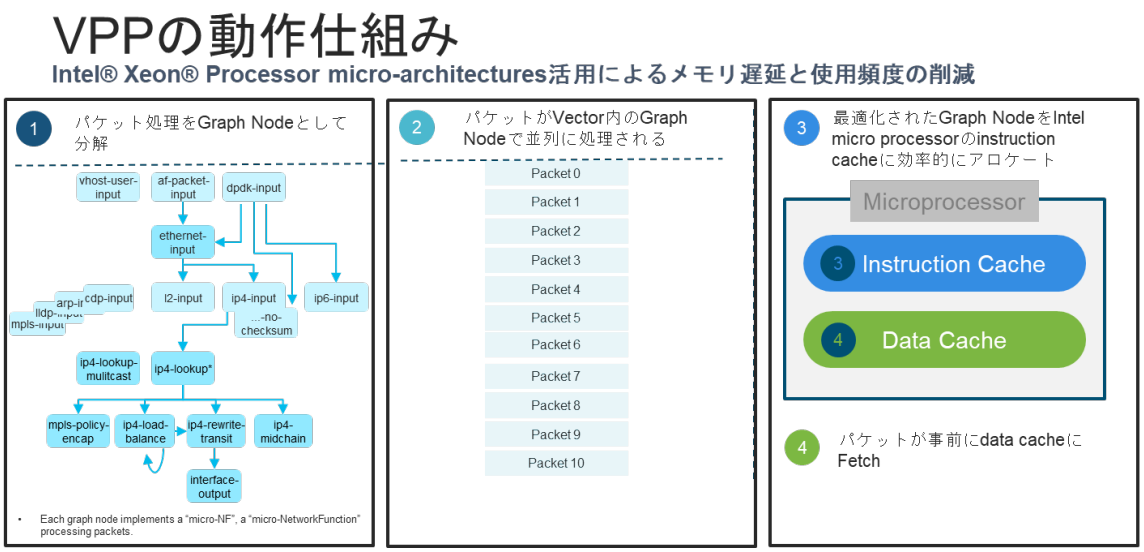


図 3-8 3GPP ネットワーク スライスのコンセプト

3.2.4 仮想化環境の User Plane 性能改善

マイクロサービス等によるクラウド ネイティブ化は、 Web アプリケーション分野で成熟した技術で、5GC Control Plane にあたるネットワーク機能には比較的容易に適用できます。しかし、複雑かつ高性能が要求される User Plane でのパケット処理に適用するには、アーキテクチャの最適化が必要です。User Plane のクラウドネイティブ化にあたっては、コンテナ間通信が行われるたびに起こるカーネルや、Virtual I/O への過度なアクセスを避ける工夫が必要です。

シスコは、パケットを処理する機能をカーネルではなくユーザ空間に構成し、共有メモリで通信を行うことでカーネルや Virtual I/O をバイパスし、User Plane を最適化しています。

シスコは、これを実現する User Plane として、VPP (Vector Packet Processing) 技術 (図 3-8) を開発しました。VPP は COTS (商用既製品) の CPU と Linux のユーザ空間で動作し、モジュール化されたアーキテクチャで、高性能、また、柔軟性と豊富な機能を持つ仮想化環境のパケット処理プラットフォームです。 VPP は、広く活用してもらうために、Fast Data input/output (FD.io) [3-6] としてオープンソース化しています。

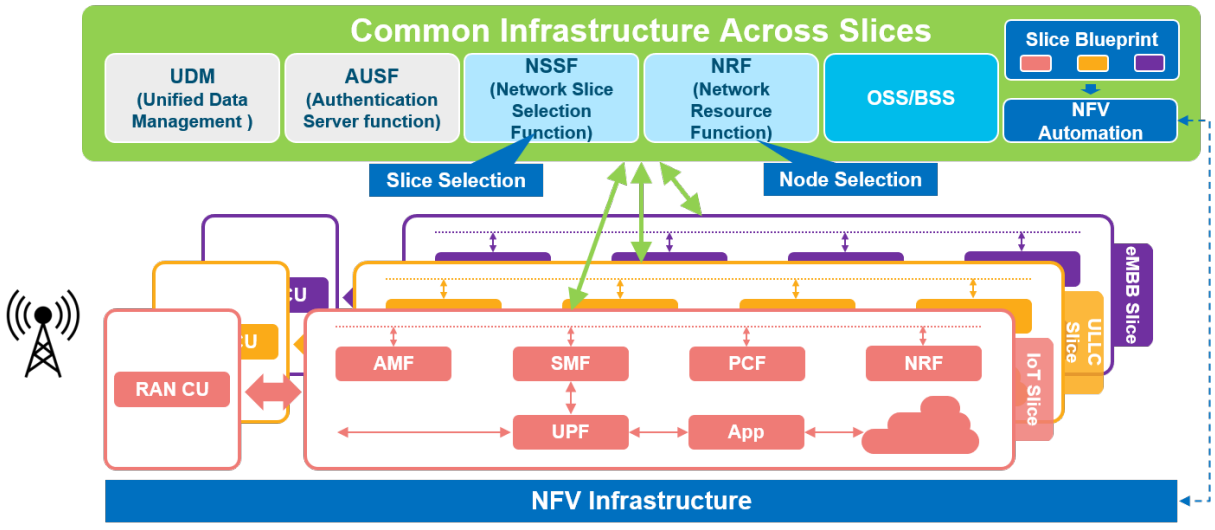


図 3-9 3GPP ネットワーク スライスのコンセプト

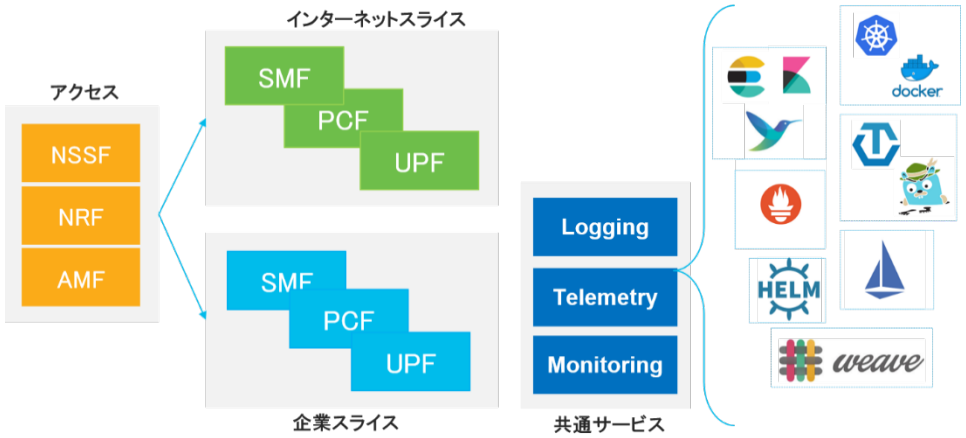


図 3-10 Cisco 5GC ネットワーク スライス実装コンセプト

3.2.5 ネットワーク スライスの効率的な実現

3GPP Release15 から 5GC における柔軟なネットワーク スライスの実現方法が規定されました (図 3-9) 。

Cisco 5GC も、ネットワーク スライスの実現だけではなく、そのマネジメントを含めたソリューションを提供する予定です (図 3-10) 。スライスを構成する NF を柔軟に配置するマネジメント機能や、スライスの SLA 監視・保証するソリューションを提供します。またユーザ端末からサービスデータセンターまでのエンドツーエンドスライスを実現するため、RAN、トランスポート、データセンター間の連携も検討しています。

3.2.6 エッジ コンピューティングの実現

5G の高速大容量、超低遅延とクリティカル IoT の一部のユース ケースには、よりユーザに近いロケーションでアプリケーションを実行するニーズがあります。たとえば、コネクテッド カーのように大量データアップロードが必要なケースや、リモート操縦や手術で超低遅延が要求されるようなケースが想定されます。現在、通信事業者とサービス提供者の間でビジネスモデルが模索されています。技術的には、CP と UP の分離により、モバイル ネットワークのエッジ コンピューティングが実現しやすくなりました。ポリシー、課金、デバイス管理や複雑なデータ処理、蓄積をセンター側で行いながら、データ転送と処理などはエッジに UP を配置することで、MEC ホストで処理することができます (図 3-11) 。

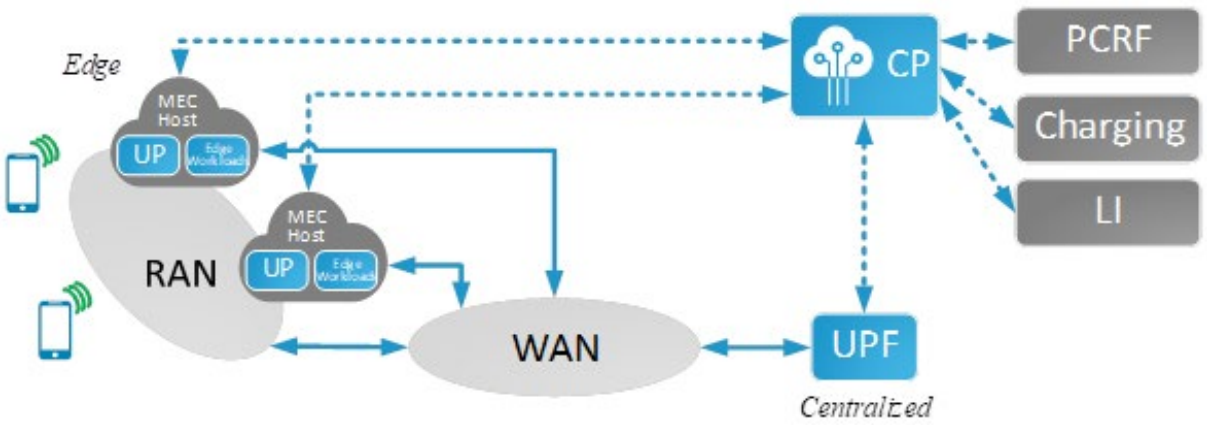


図 3-11 CU 分離とエッジ コンピューティング

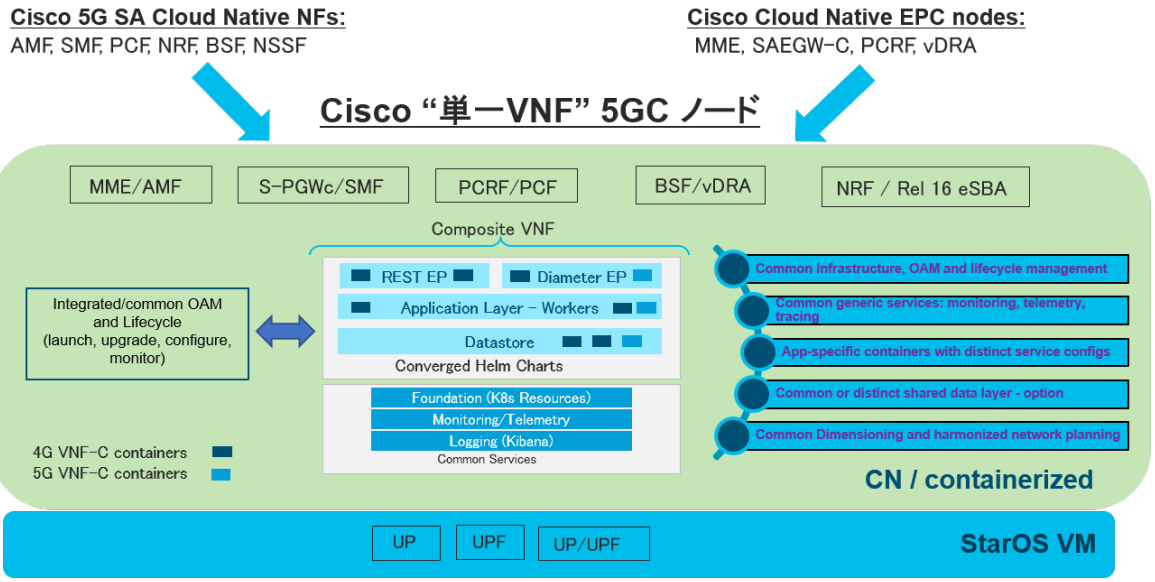


図 3-12 Cisco Mobility 共通 4G/5G Core

UP をエッジに配置することにより、エッジでのサービスが可能になりましたが、ここで課題となるのが端末のローミング処理です。3GPP では、モビリティ管理について 3 タイプの SSC Mode を定義しています。シスコも順次 SSC Mode1/2/3 [7] をサポートしていく予定です。

3.2.7 4G EPC から 5GC へのシームレスな移行

現在 5GC の導入を検討しているお客様においては、まず、既存の 4G EPC を 5G ノンスタンドアロン (5G NSA) に対応させ、次に 5G SA (5GC) を導入するケースが多いと予想されます。しかし、4G と 5G の共存場面は、長期間続くと考えられます。シスコは、 5GC のアーキテクチャを 4G から 5GC へスムーズに移行できるよう、Common Core を実装する予定です (図 3-12)。そのために、EPC のコントロールプレーンも、この SMI の上に 5GC と共存できるよう、マイクロサービス化の開発をしています。

さらに User Plane も 4G PGW-U/SGW-U と 5G の UPF を単一 VNF になるように開発し、よりシームレスな移行が可能になりました。[図 3-13]

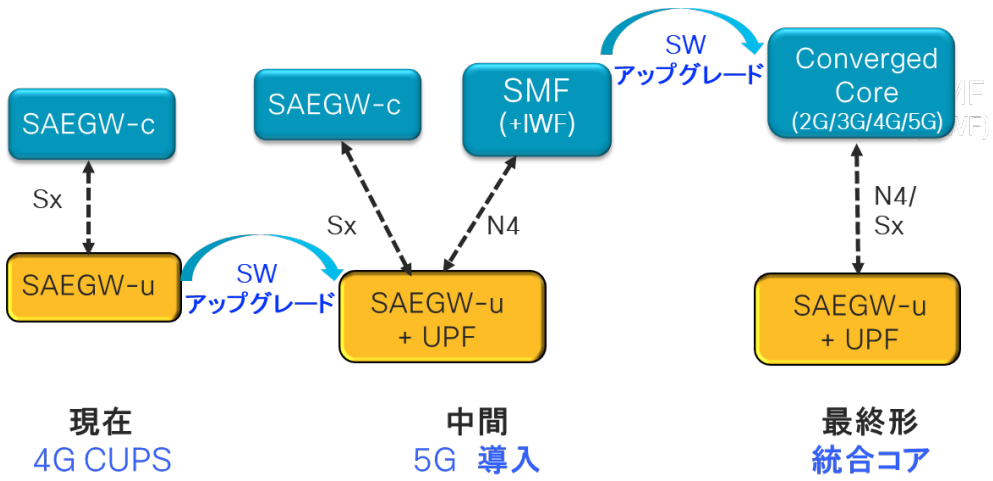


図 3-13 4G CUPS から 5G へのシームレス移行

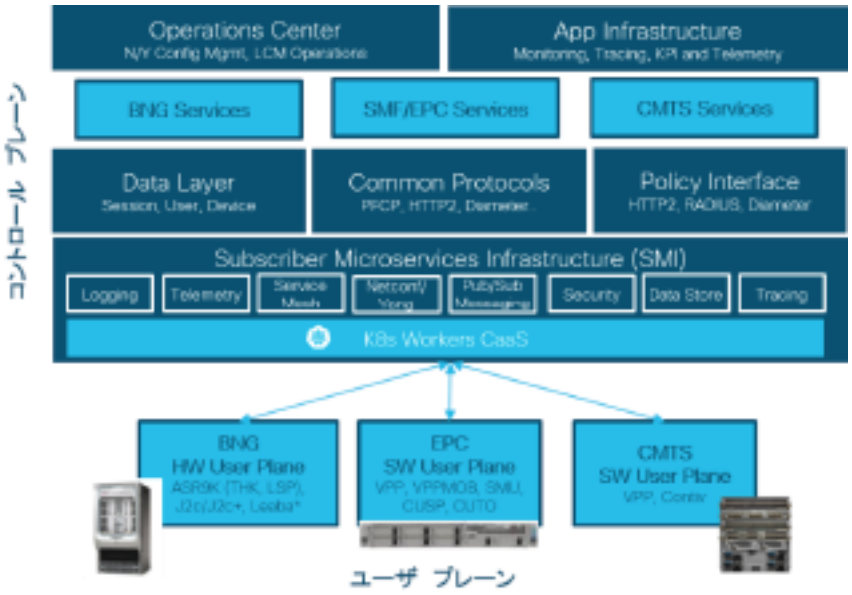


図 3-14 5GC/CMTS/BNG の共通クラウド ネイティブ アーキテクチャ

3.3 モバイルサービス以外のサービスのクラウド ネイティブ化

ケーブルブロードバンド サービスを提供している MSO (ケーブル オペレータ) も、ハードウェアとのディスアグリゲーションを推進しています。今までの ATCA ベースの CCAP (Converged Cable Access Platform) システムから、CMTS (Cable Modem Termination System) コアと Remote Phy Deployment (RPD) に進化し、さらに、クラウド ネイティブ アーキテクチャ ベースの Cloud CMTS と SmartPhy に変身しています。シスコでは、これらの加入者管理機能も、5GC で開発したクラウド ネイティブ基盤を活用する予定です。このように、Cloud CMTS チームが、クラウド ネイティブ基盤の汎用化により、マイクロサービスの機能開発にフォーカスし、より早く顧客に機能を提供できるようになります。シスコは、他にも Cloud Native Broadband Router (cnBR) を開発し、クラウド ネイティブのアドバンテージを生かせる MSO 向けソリューションを提供する予定です。また、より広義的なブロードバンド加入者制御の BNG (Broadband Network Gateway) 機能も同様に、この基盤を利用する計画です。 (図 3-14) 。

このようなアーキテクチャが将来 FMC (Fixed Mobile Convergence) の実現につながる基盤になります。

3.4 まとめ

- 5G 時代の加入者向けサービスに柔軟に対応するためには、マイクロサービス化が不可欠です。
- 固定、モバイルとケーブル通信に共通する加入者管理のコア ネットワークには、斬新なクラウド ネイティブ ベースのアーキテクチャが必要です。
- クラウド ネイティブの実装は、オープンソースベースが多く、コード開発そのものが少なくなる一方、ベンダー間の差別化が難しくなります。製品化のためのアーキテクチャの設計、インテグレーション、可視化とオーケストレーションのツール開発が非常に重要になり、お客様が採用する際の重要な評価ポイントになるでしょう。
- インテグレーション、サービスの移植をよりシンプルにするために、実績が多く、市場に広範囲に受け入れられる基盤選びが大切です。シスコは、Docker コンテナと Kubernetes の

自動化ツールを共通したツールとして採用し、製品化していきます。

- クラウドネイティブ時代の技術を CP に多く適用しつつ、UP の性能向上と最適化も非常に重要と考えます。
- シスコがオンプレミス、プライベートクラウド、パブリッククラウド (As a Service)、ベアメタル等のあらゆる形態のプラットフォーム上で動作する 5G 時代のクラウド ネイティブベースのパケットコアを提供いたします。

用語集

5GC: 5G Core Network

BNG: Broadband Network Gateway

CCAP: Converged Cable Access Platform

CCP-SP: Cisco Container Platform for SP

CEE: Cisco Execution Environment

CMTS: Cable Modem Termination System

CN: Cloud Native

CP: Control Plane

CUPS (Control and User Plane Separation): コントロールプレーンとユーザプレーンの機能的分離

CVIM: Cisco Virtual Infrastructure Management

EPC: Evolved Packet Core

MEC (Multi-access Edge Computing): ネットワーク内のエッジ（物理的に UE [User Equipment] 寄りの位置）に計算機リソースを用意して各種処理を行うシステム、概念のこと

NFV: Network Function Virtualization

RPD: Remote Phy Deployment

SBA: Service Based Architecture

SMI: Cisco Subscriber Microservice Infrastructure

SSC: Session and Service Continuity

UP: User Plane

VPP: Vector Packet Processing

cnBR: Cisco 開発のケーブル事業者向けの Cloud Native Broadband Router

5G 時代のデータセンター ファブリック アーキテクチャ

佐々木 俊輔

4.1 はじめに ― 5G におけるテレコム クラウド基盤

ここまでの章では、5G において、 4G 以前と比べてアーキテクチャが大きく進化を遂げる点を見てきました。

第 1 章では vRAN のコンセプトが RAN に導入され、従来一体型だった DU と CU の分離および仮想化が可能となることを見ました [4-1] 。続いて第 3 章では、5G Core ではコントロール プレーンとユーザ プレーンの分離 (CUPS) が可能になり、それぞれのネットワークファンクション (Network Function; NF) が分離してデプロイされるようになることを見ました [4-3] 。こうしたモバイル ソフトウェア アーキテクチャの進化により、5G では、提供するサービスに応じて、RAN や 5G コア NF およびサービス用アプリケーションを仮想基盤上に柔軟に配置できるようになりました。

こうしたアーキテクチャの進化に対応して、モバイル通信事業者は、 NF を配置するための仮想基盤をネットワークの各所に用意し始めています。ここでは、この基盤をテレコム クラウド基盤と呼びます。テレコム クラウド基盤には、パブリッククラウドと同様に拡張性と柔軟性、コスト最適化が期待されます。一方で、NF に一定の性能が求められることや、モバイルネットワーク上に配置されるといったモバイル通信事業者独自の要件も考慮にいれる必要があります。

本章では、このテレコム クラウド基盤、特にデータセンターファブリック (DC ファブリック) について、そのアーキテクチャや要件を考えていきます。

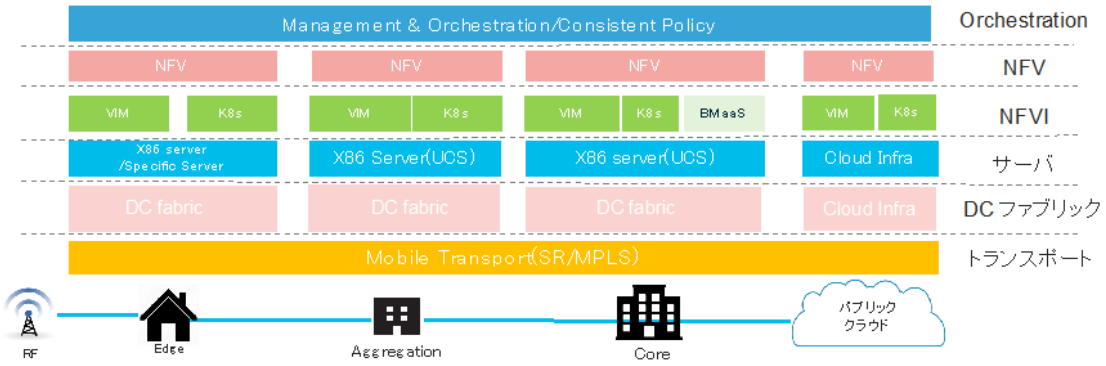
4.2 モバイル通信事業者のテレコム クラウド環境の展開 (コア/アグリゲーション/エッジ)

ここでは、全国規模でサービスを展開するモバイル通信事業者のネットワークを考えます。テレコム クラウド基盤が必要となる場所は多岐にわたります。本章では、それぞれの場所の特性に応じて以下のように呼び分けることにします。バックボーン ネットワークの中央拠点にあたる「コア」、地域単位でネットワークを集約する「アグリゲーション」、無線基地局に物理的に近い場所にある「エッジ」です。それぞれについてテレコム クラウド基盤としての要件を考えてみましょう。

図 4-1 の下の表に、コア・アグリゲーション・エッジのそれぞれについて、ロケーションの数、サーバを設置するファシリティの環境、サーバ/NFVI (Network Function Virtualization Infrastructure: ネットワークファンクション仮想化インフラ) /NFV [4-2] の制約条件についての指標を示します。なお、これらの数値は国や事業者により大きく差があるため、ここでは日本における平均的な目安として考えていただければと思います。

コアに配置されるデータセンターは、具体的には北海道・東北・関東といったエリア拠点が想定されます。集約拠点であるため数は 10 以下です。一方で、テレコム クラウド環境の構築にあたってファシリティやリソースの制約はありません。ワークロードが集中するため、サーバ環境/NFVI/NFV の性能と拡張性が求められます。コンピューティングとしては、ベアメタル・仮想化基盤・コンテナ基盤といった多様な実行環境が求められること

になります。いわゆるパブリック クラウド環境のアーキテクチャに近いと考えてよいでしょう。



ロケーション定義	Edge / エッジ	Aggregation / アグリゲーション	Core / コア
ロケーション数	• 1,000 以上 • Small Cellを含めると10,000以上 • 地域の通信局舎を含む小規模拠点	• 100 以下 • 各都道府県の拠点	• 10 以下 • 北海道・東北・関東・中部・関西・九州などエリア拠点
サーバ設置環境	• 他事業者の設備共用も想定され • スペース電源などに大きな制約	• スペース電源などに多少の制約	• 制約無し
サーバ・NFVI・NFV	• 19インチラックサーバ以外に小型の専用サーバ • VM数10以下 • コンテナ環境の比率が高くなると想定される	• 19インチラックサーバ • VM数100以下 • コアと同様だがサーバ設置環境からリソースの制約を受ける	• 19インチラックサーバ • VM数100以上 • 稼働するネットワーク機能・アプリケーションに合わせてベアメタル・仮想基盤・コンテナ基盤を組み合わせ

図 4-1 モバイル通信事業者のテレコム クラウド基盤の配置場所 [4-4]

アグリゲーションは、具体的には都道府県単位で設置される拠点のデータセンターが想定されます。設置数は 100 が目安となるでしょう。コアに比べて数が多い半面、拠点の規模やファシリティなどの充実度は下がることが想定されます。テレコム クラウド基盤としては、サーバ/NFVI/NFV については拠点のリソース制約に合わせて柔軟な構築が求められます。

エッジのデータセンターの場所は無線基地局に近い場所が想定されます。設置数としては 1,000 以上を想定としていますが、もしも将来、スモールセル (1 章を参照) の展開が増えた場合には、エッジの数はさらに増えることも考えられます [4-3] 。テレコム クラウド基盤としては、他社設備を借用して利用する可能性もあり、コストの観点から電源や物理スペースの制約が大きくなると想定されます。サーバについて言えば、一般的な 19 インチ ラック収容のサイズではなく、より小型でかつ耐環境性が高いものが求められるでしょう。NFVI/NFV については、サーバのリソースに合わせてスケール可能なコンテナ環境が主流になると考えられます。

コア・アグリゲーション・エッジでの、それぞれのテレコム クラウド基盤の展開イメージを図 4-1 の上図に示しました。各データセンターに共通して言えることは、5G サービスの展開に合わせて多数の物理サーバが配備されることになり、それらを収容するために 「DC ファブリック」 が必要になると見込まれることです。この DC ファブリックの要件については、次のセクションで深堀りします。

図 4-1 に示す、サーバ、NFV、NFVI、Orchestration についても考えてみます。前述の通り、テレコム クラウドでは物理サーバ上に仮想・コンテナ基盤が構成され、その上に NF やアプリケーションが動作します。各データセンターは地理的には分散して配置される一方で、サーバ・NFVI・NFV/NF およびアプリケーションのライフサイクル管理は、モバイル通信事業者が所有するインフラ全体で一元的・統一的に行われる必要があります。これを担うのが、図中のエンドツーエンド オーケストレーションのレイヤです。このレイヤでは、モバイル ネットワークサービスに対する共通のポリシーの下に、サービス展開の自動化や統一的なライフサイクル管理を実現することが求められます。オーケストレーション レイヤについては第 6 章でより詳しく取り上げます。

4.3 DC ファブリック に求められる機能

テレコム クラウド基盤における DC ファブリックは、サーバを収容する多数のポートに対し、低遅延・広帯域接続を提供する CLOS 構成 [4-5] のネットワークです。 CLOS 構成は、Spine スイッチと Leaf スイッチの 2 種類のスイッチを水平スケールさせていく構成です。ポート数と高帯域を確保しやすく、メンテナンス性と拡張性が高いことがメリットの 1 つで、大型の Web 企業を中心に採用が広がりました。

テレコム クラウド基盤の視点で、DC ファブリックに求められる一般的な機能や特性を以下にまとめました。

- 拡張性、柔軟性、統合運用
- 仮想化基盤との連携
- 分析・可視化機能
- トランスポート ネットワークとの連携

それぞれについて以下で詳しく見ていきます。

拡張性、柔軟性、統合運用

テレコム クラウド基盤では、5G ネットワーク ファンクションやアプリケーションのワークロードを柔軟にスケールさせることが期待されるため、それを支える x86 サーバは膨大な数になります。サーバを収容するためのポートを提供する ToR (Top of Rack) スイッチも大量に必要となり、ネットワーク管理者による個別の設定・管理が難しくなることが想定されます。そのため DC ファブリックを構成するスイッチ群を、いわゆる SDN (Software Defined Network) 技術によって統合運用する仕組みが求められています。

SDN で構築される多くの DC ファブリックは、アンダーレイ ネットワークとオーバーレイ ネットワークを分離したアーキテクチャを採用しています。アンダーレイには L2 ではなく、マルチパスが可能で経路制御が容易な L3 の IP ルーティング プロトコル (IS-IS, OSPF, BGP) が採用されます。論理的なオーバーレイには、代表的なプロトコルとしては VXLAN EVPN (RFC 8365) が用いられています [4-6] 。さらに、ファブリックスイッチへの設定を SDN コントローラが一元的に行うことが一般的です。

運用面で必要になる機能としては、ToR スイッチ増設時のディスカバリーや初期設定がゼロタッチで行える機能、故障機器の交換やメンテナンス時に安全にトラフィックを迂回できる機能、交換後に元のスイッチの設定が自動的に復元できる機能等が要件として挙げられるでしょう。これらを実現するための機能を提供するのも SDN コントローラの役割となります。

また、基本的なこととして、サーバ側の多様なポート要件を満たすためには、1G/10G/25G/40G/100G/400G といった幅広い通信レート、光・メタルといった多様なインターフェイス種別をサポートするスイッチのラインナップが必要となるでしょう。

仮想化基盤との連携

DC ファブリックの基本的で最も大事な機能は、テレコム クラウド上で稼働するモバイル ネットワーク ファンクションやアプリケーションに対してネットワーク接続性を提供することです。5G においてはそうしたアプリケーションの多くが仮想基盤やコンテナ基盤上で動作するため、DC ファブリックは仮想ネットワーク・コンテナネットワークと適切に連携する必要があります。

一例として、アプリケーション インスタンスに割り当てる IP アドレスや、所属させる VLAN などの基本的な情報は、アプリケーションのデプロイ時に仮想・コンテナ基盤によって設定が行われます。アプリケーションのデプロイと同時に、それと整合的な設定を DC ファブリックに対しても行う必要があります。

これを実現する方法は複数考えられます。一般的には 1) アプリケーションのデプロイを行うオーケストレータが仮想・コンテナ基盤と DC ファブリックの両方に適切な設定を投入する方法、または 2) 仮想・コンテナネットワークが設定されると同時に、DC ファブリック側に自動的に設定が入るプラグインの仕組みを使う方法 のどちらかが採用されるケースが多いようです。運用の主体や設定ポリシーによってどういった方式が望ましいかを検討する必要があります。

分析・可視化機能

モバイル通信事業者にとって、ユーザ通信品質の監視および維持は 5G になっても変わらず運用上の最重要課題です。4G 以前のモバイルネットワークでは、物理的なモバイルネットワーク機器の処理の負荷や外部ポート・内部バスのカウンタ等を SNMP や CLI で監視することで、通信品質について一定の監視が行えていました。ところが 5G では、ネットワーク機能が DC ファブリック配下に分散配置されることになるため、DC ファブリック上の通信状況をいかに把握して可視化するかが重要となります。また、大量の DC ファブリックスイッチに対するデータ収集方法として、SNMP や CLI ではコレクターの負荷が大きすぎてスケールしないという問題があります。

ここで近年活用され始めているのが、Telemetry (テレメトリ) 技術です。SNMP や CLI がプル型のデータ収集であるのに対してプッシュ型が利用可能で、スイッチ側からコレクター装置に対して従来よりも高頻度で統計データを送信します。対象となるデータには「ソフトウェアテレメトリ」と呼ばれる装置自体の CPU 利用率やルーティングプロトコル情報、インターフェイスカウンタ、温度などのセンサー情報に加えて、「ハードウェアテレメトリ」と呼ばれるデータプレーンレベルの統計情報があります。後者には、通信フローの情報や ASIC 内部のカウンタ情報などが含まれ、フローの可視化に活用できるほか、通信品質の問題が発生した場合の重要な情報源となります。

テレメトリデータは GPB (Google Protocol Buffer) [4-7] や JSON 形式の構造化データとしてエンコードされ、それぞれ gRPC (Google Remote Procedure Call) と HTTP(S) プロトコルで運ばれるのが一般的です。収集されたデータはコレクター装置でデコードされたのち、集約・分析・可視化されます。この領域には機械学習 (ML, Machine Learning) や AI (Artificial Intelligence) など最新のテクノロジを活用することが期待されています。

近い将来、5G で、産業機械や医療・交通などミッション クリティカルなサービスが提供されるようになると、DC ファブリックにおける通信の分析・可視化はさらに重要性を増すと想定されます。スイッチへのテレメトリの設定投入や、ファブリックのトポロジ情報の管理などが DC ファブリックの設定を行う SDN コントローラから一元的に行えることも重要なポイントになると考えられます。

トランスポート ネットワークとの連携

データセンター上で動作するネットワーク ファンクションやアプリケーションは、当然ながらモバイル ユーザやインターネットなどの外部ネットワークと通信する必要があります。そのため DC ファブリックは、トランスポート ネットワークとの間で、データプレーン レベルおよびルーティング プロトコル レベルの両方で適切に連携する必要があります。

ここでは例を使って説明します。図 4-2 は、DC ファブリックとトランスポートネットワークの連携の一例を示したものです。DC ファブリックは図の赤い枠で囲まれた部分にあたります。DC ファブリックはアプリケーションを論理ネットワーク (VRF) で収容し、その経路を、 BL (Border Leaf) スイッチがトランスポートの PE (Provider Edge) に対して eBGP で広報しています。トランスポート側では、第 2 章で見たセグメント ルーティングをアンダーレイとして L3VPN オーバーレイが構成されており、アプリケーションへの到達性を VPNv4 経路としてエンドツーエンドで広報します。

BL と PE の接続方式としては多様な方式が考えられますが、この例では Inter-AS Option A または B (RFC4364) が考えられます [4-8] 。どの方式が望ましいかは通信事業者の接続ポリシーに依存するため一概には言えませんが、Option B であればトランスポートから DC ファブリックまで切れ目なく Segment Routing MPLS でデータプレーンが延伸されることになります。PE では VLAN インターフェイスが必要なく、ラベルだけを見て転送できるようになるため、PE のスケール面で利点があると言えます。

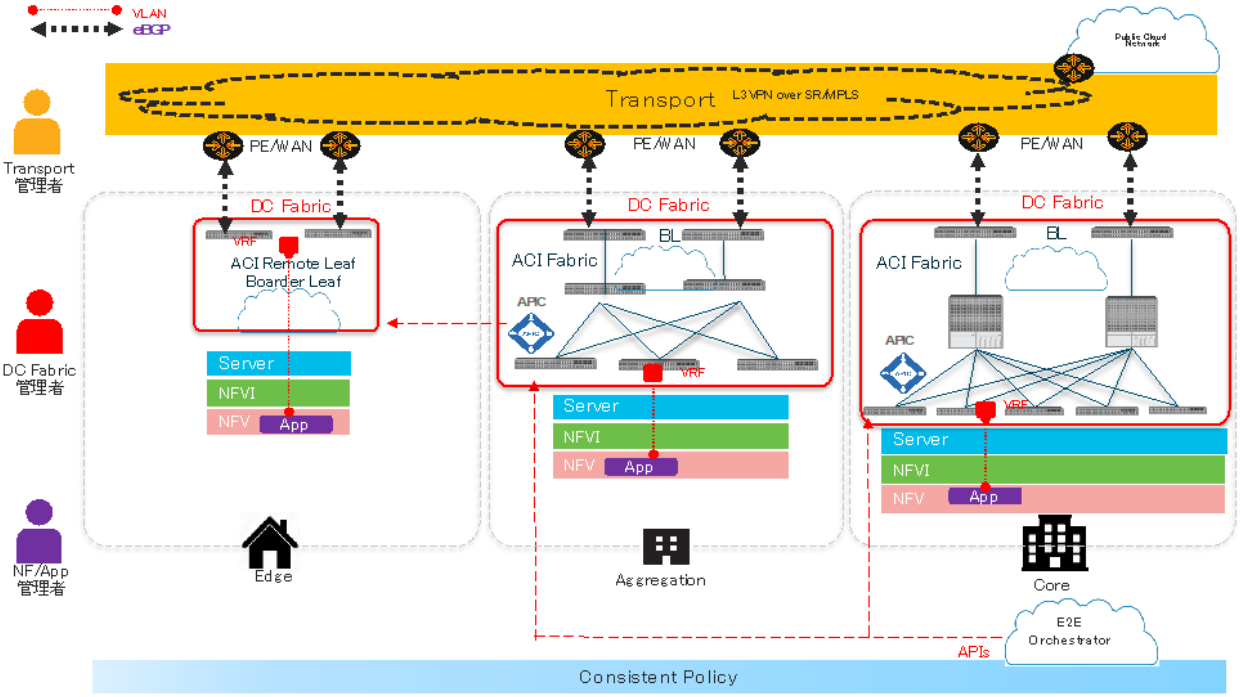


図 4-2 DC ファブリックとトランスポートの連携の例

4.4 エッジにおける DC ファブリックの要件

エッジにおける DC ファブリックについては、前節の議論に加えて、ファシリティ面の制約を考慮にいれて要件を考える必要があります。図 4-1 でも見たように、エッジ データセンターはスペースや電力容量が少ない場合があり、コアやアグリゲーションのような規模の DC ファブリックやサーバを配置できるとは限りません。小規模なファブリックの場合、専用の Spine スイッチや SDN コントローラを配置すると非経済的になってしまう可能性もあります。

図 4-2 の例では、コアとアグリゲーションのデータセンターには SDN コントローラが管理する DC ファブリックが配置している一方、エッジについてはリモートリーフ (Remote Leaf) を配置した例を記載しています。

リモートリーフとは、センター側の DC ファブリックの Spine スイッチからエッジに対して、Leaf スイッチを仮想的に延伸するような形で配置し、リモート制御できる機能です。リモートリーフのライフサイクル管理や設定の投入などのオペレーションは、コアやアグリゲーションに配置した SDN コントローラから行う仕組みです。こうした機能により、小規模なエッジ DC 拠点にもコスト的に有利な形で DC ファブリックが展開可能となります。

4.5 シスコの DC ファブリック ソリューション

ここまでは、5G のアーキテクチャ変遷をとらえながら、テレコム クラウド環境におけるデータセンター ファブリック (以下 DC ファブリック) に求められる要件を考えてきました。このセクションでは、そうした要件に対応した具体的なシスコのソリューションをご紹介します。

シスコでは、業界ごと・お客様ごとに異なるニーズに応えるため、複数の DC ファブリック ソリューションを展開しています (図 4-3) 。その中でも、今回は、テレコム クラウド向けに急速に採用が広がっている Cisco ACI (Application Centric Infrastructure) を取り上げ、その利点をご紹介します。

図 4-3 シスコの DC ファブリック ソリューション

テレコム クラウドに限らずデータセンターでのファブリックの需要は Web 企業を中心に引き続き旺盛で、次々と新しいテクノロジへの開発投資が行われています。近年では Segment Routing IPv6 (SRv6) を DC ファブリックに活用する事例も出てきています [4-9]。

今回ご紹介する Cisco ACI も、進化途上にある多様な DC ファブリックの実装の一例としてご理解いただけたら幸いです。

4.6 Cisco ACI (Application Centric Infrastructure)

このセクションでは、Cisco ACI の概要をご紹介するとともに、セクション 4.3 で見てきたコア、アグリゲーション、エッジのそれぞれのデータセンターの諸々の要件に、ACI がどのように応えることができるかを考察します。

ACI の構成要素を図 4-4 に示しました。ACI は Nexus 9000 シリーズスイッチがつくる ACI ファブリックと、ファブリックを制御するコントローラである APIC (Application Policy Infrastructure Controller) から構成されます。

ACI ファブリックは CLOS トポロジを採用しており、ToR スイッチである Leaf とコア スイッチである Spine からなります。Leaf のうち、WAN トランスポートと接続するものを Border Leaf (BL) と呼びます。これらの Leaf、Spine、Border Leaf は、APIC または APIC に接続済みのスイッチに接続すると自動的にディスカバリーされ、集中管理下に置かれます。普段のすべてのオペレーションは APIC から実施され、スイッチを個別に設定する必要はありません。

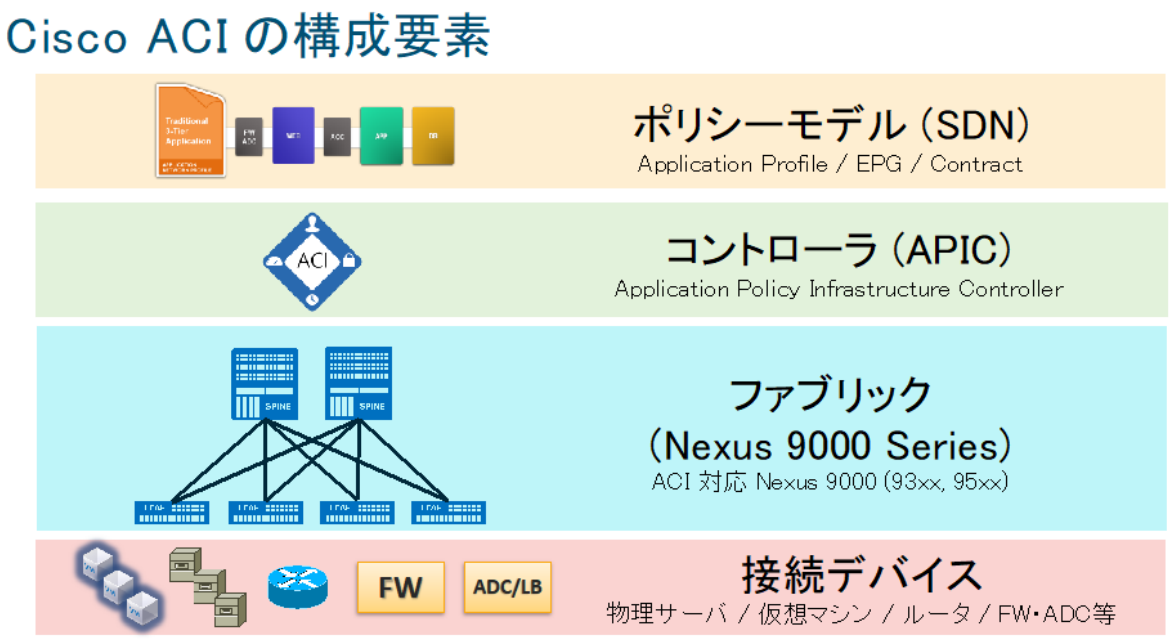


図 4-4 Cisco ACI の構成要素

ACI の大きな特徴のひとつに、APIC による物理ネットワークの抽象化があります。 APIC は、「ポリシーモデル」という考え方をもとに、従来の DC ファブリックの設定を抽象化しました。従来の DC ネットワークの設計手法では、DC ファブリックにアプリケーションやそれを動かすサーバデバイス（以下ではまとめてアプリケーションと呼びます）を収容する場合、アプリケーションが想定する論理ネットワーク構成を、物理ネットワーク上の設定項目に「翻訳」する必要がありました。

論理的なネットワーク構成の例：

・フロントエンド Web サーバ ←→ (Layer 3 ネットワーク) ←→ アプリケーション サーバ ←→ (Layer 2 ネットワーク) ←→ データベース サーバ

物理ネットワークの設定項目の例（一部）：

・フロントエンドサーバの IP アドレス、接続された Leaf ポート、アプリケーションの利用する TCP/UDP ポート
・Layer 3 ネットワークの VLAN とゲートウェイ設定、ポートへの VLAN 設定、通信フィルタ用の ACL の設定
・フロントエンドサーバへのロードバランス用の仮想 IP (VIP) の設定
・アプリケーションサーバの IP アドレス、VLAN、接続された Leaf ポート、アプリケーションの利用する TCP/UDP ポート
・Layer 2 ネットワークの VLAN 設定、ポートへの VLAN 設定
・データベースサーバの IP アドレス、VLAN、接続された Leaf ポート、アプリケーションの利用する TCP/UDP ポート

こうした「翻訳」作業は、アプリケーション開発者から見ると、アプリケーションの動作にとって本質的な作業ではないため、複雑なネットワーク要件をインプットしなければならないことが煩雑に感じられていました。また、アプリケーション側で増設・移設などがあった際にはその度に同様の設計と設定変更が必要で、大規模なデータセンター環境ではネットワーク運用者の負担が大きくなっていました。

こうした課題に根本的にアプローチするため、ACI では、アプリケーションが意図する論理的なネットワークの構成を「ポリシー」として APIC 上に記述することで、ネットワーク設定項目への翻訳が自動的に行われるという仕組みを採用しました。これが「Application Centric」 の言葉の由来です。

本章では、ACI のポリシーモデルの考え方については深入りすることは避け、別稿に譲りたいと思います [4-10]。ここでは、ACI が従来のファブリックと異なるアプローチを取っていること、それによって様々なメリットを享受できるようになることを感じていただけたら幸いです。

4.7 テレコムクラウド DC ファブリックとしての ACI

ACI が前節で見たテレコム クラウド基盤における DC ファブリック要件をどのように満たすことができるかを表 4-1 にまとめました。

このように、ACI はテレコム クラウド基盤における DC ファブリック要件に十二分に応えることができるソリューションです。特に、説明の中でも触れたように、エンドツーエンド スライシングや MEC、サービスチェイニング、トランスポート スライスとの連携など、5G 時代に求められる機能をカバーしている点に、ぜひ着目いただきたいと思います。

テレコム クラウド基盤における Cisco ACI のご提案について、シスコでは、より詳しい内容をホワイトペーパー [4-15] に解説していますので、ぜひ合わせて参照いただけたら幸いです。

4.8 MEC で広がる 5G の可能性

DC ファブリックの話題からやや離れますが、本章の最後に MEC について触れたいと思います。

5G で実現が期待されているサービスの 1 つが MEC (Multi-access Edge Computing) です。第 3 章で見たように 5G では CUPS アーキテクチャが採用され CU 分離が実装されたことで、エッジコンピューティングが実現できると期待されています。MEC の目的は大きく 2 つあります。1 つはエッジに低遅延のアプリケーション実行環境を提供すること、もう 1 つはユーザトラフィックのオフロードによるトランスポート ネットワークへの影響を緩和することです。

当然ながら、すべてのサービスをエッジに配置すればよいわけではなく、サービスが求める遅延とその効果、それにかかる費用などを考慮して最適なバランスを判断する必要があります。

表 4-1 ACI による DC ファブリック要件への対応

テレコム クラウドにおける要件	サブ項目	説明
拡張性、柔軟性、統合運用	ACI ファブリックの拡張性	ACI は水平スケールアウトが可能な CLOS ファブリックを提供します。Leaf スイッチの選択肢は多岐にわたり、100/1000 Base-T ポートから 1G/10G/25G/100G/400G ポートまで、多様なインターフェイスを持つサーバ等のデバイスを収容可能です ［4-11］。 ACI では、ファブリックを構成するためのアンダーレイ ネットワークは自動的に構成されます。内部的には MP-BGP と VXLAN を始めとする標準的なプロトコルをベースに構築が行われますが、スイッチ ID の指定以外は、ユーザが手動で設定したり、状態を意識したりする必要は一切ありません。 ACI では、複数の拠点にまたがる構成もサポートしています (Multi-Pod および Multi-Site) 。Multi-Site 構成では、執筆時点で最大 1,600 台の Leaf スイッチがサポートされており、今後さらに拡張予定です。
	インテントベース ファブリック	APIC では、論理ネットワーク設定をポリシーとして抽象化しています。エンドポイントの識別子として End Point Group (EPG) と Contract の概念を導入しており、アプリケーション視点でネットワークを提供できる業界唯一のソリューションです。 DC ファブリックの設定を、従来のように「何をどういう順番で設定するか (How) 」 という概念から、「アプリケーションやユーザは何がほしいか (What) 」 という概念に切り替えたという意味で、ACI はインテント (意図) ベース ファブリックと呼ぶことができます。シスコでは、データセンターにおける ACI を始めとしてあらゆる領域でインテントベースのコンセプトを展開しています。
	APIC の運用性	APIC はファブリック スイッチの完全なライフサイクル管理を実現しています。ACI ファブリックに接続されたスイッチは自動的にディスカバリーされ、ファブリックに組み込むことができます。ファームウェアのアップグレードや故障機器の交換のための作業も APIC から一元的に行うことが可能です。 APIC はファブリック上のネットワークの設定・監視および可視化を提供します。ファブリックのすべての設定とステートに対応した情報にアクセスする GUI と API を備えており、上位のオーケストレータや OSS/BSS と連携して監視・運用の自動化を実現します。
	ACI ファブリックの柔軟性： サービスチェイニング	ACI では、ファブリックに接続された複数のサービスノードにトラフィックを転送するサービスチェイニングが簡単に設定できます。 従来のサービスチェイニングは、ルータ機器上での Policy-Based Routing (PBR) と Access Control List (ACL) による複雑な設定を使って、サービスノード単位でトラフィックを曲げることが必要でした。 ACI では、上で説明した抽象化ポリシーによってこれらの設定を簡素化することが可能となっています。複数のサービスノードがある場合の負荷分散やヘルスチェック、ノードの追加・削除を柔軟に行うことができます。 モバイル通信事業者のテレコム クラウド基盤では、主に GiLAN ネットワークでサービスチェイニングが多く使われており、ACI によりオペレーションの簡素化が可能です。
	ACI ファブリックの柔軟性： リモートリーフへの対応	ACI は Remote Leaf 機能をサポートしています。Leaf スイッチをトランスポート越しに配置して、集中管理することができます。エッジなどの小規模拠点まで DC ファブリックを延伸する場合に利用できます。 Remote Leaf に収容されるトラフィックはローカルオフロードすることが可能です。通信を拠点内やローカルな地域内で直接行うことができるため、例えば MEC (Multi-access Edge Computing) の展開時にも活用できます。
仮想・コンテナ基盤との連携	APIC の連携機能	APIC は 仮想基盤 (OpenStack および VMware vCenter)、コンテナ基盤 (kubernetes) との連携機能を備えています。 例えば、EPG 設定に合わせて仮想スイッチの VLAN 設定を APIC から自動的にプッシュすることで論理ネットワークを仮想レイヤまでシームレスに拡張することができます。一方で、仮想マシンに関するオペレーションは従来どおり仮想レイヤ側のツール (例： vCenter) で行うことで、ファブリック管理と仮想基盤管理の適切な連携と分担が実現できます。 さらに、仮想マシンやコンテナを ACI ファブリックに収容されるエンドポイントとして認識することができます。従来のように IP アドレス・サブネット単位だけではない細やかな通信の可視化とフィルタリングが可能になります。

テレコム クラウドにおける要件	サブ項目	説明
分析・可視化機能	ACI ファブリックのテレメトリ機能	ACI を構成するスイッチは、ソフトウェア テレメトリに加えて、ハードウェア テレメトリに対応しています。データプレーン パケットをラインレートで分析する機能を備えており、SNMP など従来の手法では難しかった粒度でフロー情報やネットワーク デバイスの各種情報を取り出すことができます。これらは ASIC レベルで実装されており、スイッチ負荷を最小に抑えながら実行が可能です。 テレメトリの情報は、 ACI と連携するコレクター製品である Cisco Network Insights for Resouces ［4-12］ や、ビッグデータ分析基盤である Cisco Tetration Analytics ［4-13］ により収集・分析が可能です。
トランスポート ネットワークとの連携	ACI とセグメント ルーティングの連携機能	第 1 回で触れた DC ファブリックとトランスポート ネットワークの連携について、シスコでは 5G で求められるエンドツーエンド スライシングの視点から重要と考えています。 ACI でもこの機能に積極的に投資を行っており、特に第 2 章で解説したセグメント ルーティングとの連携に力を入れています。 ACI の Border Leaf は、データプレーン レベルでの連携 (802.1q, MPLS Label) とコントロールプレーン レベルでの連携 (BGP Labelled Unicast ［4-14］) が可能となる機能を具備します。これにより、ACI ファブリックに収容されるアプリケーションのポリシーに基づいたトランスポート スライスの選択が可能になります。

ユースケース.	遅延許容時間	概要
モバイルビデオ	~75 ミリ秒	~25 ミリ秒のバファを含む
Virtual Reality 双方向ゲーム	20 ミリ秒 50 ミリ秒	ヘッドセットでの Virtual Reality や双方向ゲームを想定。遅延があると「VR 酔い」が発生し体感品質の低下に繋がる
VoIP	200 ミリ秒	従来のユースケースに近い
URLLC のユースケース（将来に実現されるものを含む）		
モバイル Augmented Reality	~100 ミリ秒	リモートでの重機操作など遠隔からを想定(100 ミリ秒は画像処理含む)。遅延許容時間は想定作業に依存。
ファクトリーオートメーション	0.25 ~ 1 ミリ秒	生産ラインにおける機械やシステムのリアルタイム制御。Industry IoT で議論中。
コネクテッドカー・自動運転	0 ~ 1ミリ秒	遅延許容時間は、自動運転にかかる想定作業に依存
スマートグリッド	1 ~ 100 ミリ秒	スマートグリッドの周波数を維持するためには小さい遅延での電力系統での同期が望まれる

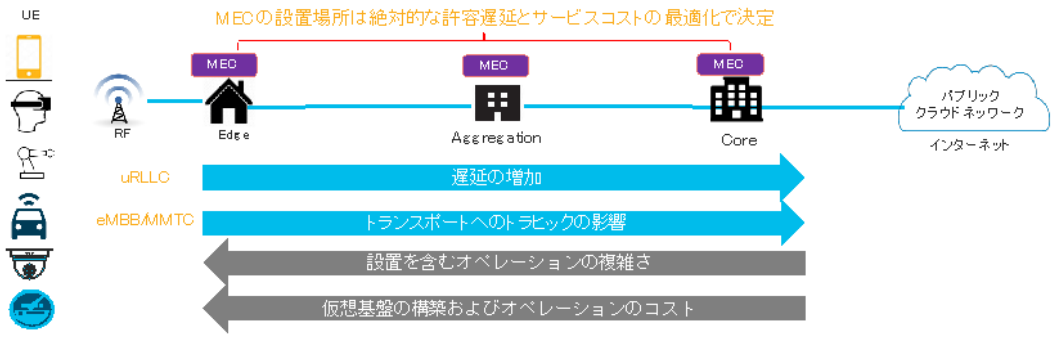


図 4-5 MEC のアプリケーション特性と配置についての考察 ［4-4］

図 4-5 に、MEC として想定されるユース ケースと、各ユースケースで使われるアプリケーションが許容する遅延時間についてまとめました。なお、遅延の値は一般的なサービスが求める参考値を記載したもので、アプリケーションによって大きく異なることにご注意ください。また、遅延はトランスポート遅延に加えて MEC サーバや仮想基盤で追加される遅延、アプリケーション処理にかかる遅延も含まれることにもご注意ください。

図 4-5 の表をみると、既存のスマートフォンを活用したモバイルビデオ配信や、 Virtual Reality (VR; 仮想現実) に関しては許容遅延が比較的大きいことがわかります。このようなサービスは、トランスポートに流れるトラフィック量の抑制によるコスト削減効果が得られ、かつ QoE（ユーザ体

感品質) を損わずに MEC に配置することが可能と考えられます。配置場所としては、アグリゲーションやコアが候補となるでしょう。

一方で、MEC をよりユーザに近いエッジに設置することで、4G 以前では実現できなかった 10ms 以下、場合によっては 1ms 以下の超低遅延サービスが実現できると期待されています。こうしたサービスの候補を示したのが、表の中の下段です。5G の超低遅延サービス (URLLC) では、MEC の低遅延特性を活かした多くのサービスが実現に向けて議論されています。すでにトライアルが実施されているサービスもあります。

実証実験の例として、モバイル Augmented Reality (AR; 拡張現実) では、5G を利用して、重機と距離を置いた安全な操作室から重機を操作する実証実験があります [4-16]。この実験では重機操作における遅延の許容が 100ms まで可能です (重機備え付けのカメラ映像処理を含む)。重機の操作室を、県を代表するアグリゲータの近くの企業オフィスに置けば、その県の配下の重機を操作することも可能になると期待されています。

4.9 まとめ

本章では、5G のアーキテクチャ変化に対応したテレコムクラウドの展開と、DC ファブリックのアーキテクチャについて議論しました。Web 企業で採用が広がっている DC ファブリックの最新アーキテクチャに加えて、モバイル通信事業者が構築するテレコム クラウドでは、ネットワーク内の配置場所に応じて制約事項や求められる要件が異なることを見てきました。

その上で、テレコム クラウド環境での DC ファブリック ソリューションの一例として、 Cisco ACI とその特徴をご説明しました。MEC のユースケースについても触れ、将来的に可能になると期待されるユースケースについて具体例を紹介しました。

本章の内容が 5G に向けたテレコム クラウド基盤の構築や、エッジ コンピューティングを含む様々なサービスの開発を検討されている皆様のお役に立てたら幸いです。

用語集

ACI: Application Centric Infrastructure

AC (Access Control List): ルータ等でフィルタや IP サブネット特定に用いる設定

AR (Augmented Reality): 仮想空間を重ね合わせることで人間が知覚する現実環境を拡張する技術

ASIC (Application Specific Integrated Circuit): 特定用途向け、ここでは特にパケット処理用の集積回路

BL (Border Leaf): DC ファブリックのうち外部ネットワークと接続するリーフスイッチ

BSS (Business Support System): サービス事業者の運用システムの 1 つ

CLOS: マルチステージの回路交換ネットワーク、最近では特にスパイン・リーフによる DC ファブリックネットワークのトポロジを指す

CUPS (Control and User Plane Separation): コントロールプレーンとユーザプレーンの機能的分離

EPG (End Point Group): ACI のコンセプトの 1 つ

GPB (Google Protocol Buffers): Google が開発した高速データ交換用のインターフェイス記述言語

GiLAN: 3GPP で定義された SGi インターフェイスに置かれる LAN

JSON (JavaScript Object Notation): JavaScript 言語をベースに開発された軽量のデータフォーマット

L3VPN (Layer 3 Virtual Private Network): 通信事業者が仮想的な専用レイヤ 3 網を提供するサービス

MEC (Multi-access Edge Computing): ネットワーク内のエッジ（物理的に UE [User Equipment] 寄りの位置）に計算機リソースを用意して各種処理を行うシステム、概念のこと

NF (Network Function): ルータやモバイルコアなどネットワーク機能を提供するソフトウェア実装を指す

OSS (Operation Support System): サービスプロバイダーのシステム管理・運用を支援するシステムの総称

PBR (Policy-Based Routing): 特別なポリシーに基づいたルーティングを強制したい場合に用いる技術

PE (Provider Edge): 通信事業者のトランスポートネットワークの機器のうちユーザ拠点を収容するルータ

SDN: Software Defined Network

SRv6: Segment Routing IPv6. IPv6 をデータプレーンに使ったセグメントルーティングの実装

Telemetry: 遠隔測定法. ネットワーク機器から主にプッシュ型でデータを送信する技術を指す

URLLC (Ultra Reliable and Low Latency Communications): 5G 要件の 1 つで、超高信頼かつ低遅延な無線通信を実現

VPNv4 (Virtual Private Network for IPv4): L3VPN インフラで利用される VPN 用プレフィクス

VRF (Virtual Routing and Forwarding): ルータ内に独立した仮想ルーティングテーブルを保持するシステム

VR (Virtual Reality): 仮想現実、ユーザの五感を刺激することで仮想的に物事を知覚させる技術

gRPC (Google Remote Procedure Call): GPB 用のリモートプロシージャコールシステム

5G 時代のエンドツーエンドネットワークスライシング

丸山 和宏/河野 美也

ここまでの章では、5G 時代の RAN/トランスポート/パケットコア/データセンターファブリックについて述べてきました。いずれの章でも「スライシング」というキーワードが出てきています。この章では、5G において注目されているトピックの 1 つであるスライシングについてさらに考察していきたいと思います。

5.1 ネットワークスライシングとは

4G までは、通信の主な対象が「人」でした。これに対して、5G では超広帯域、超低遅延・高信頼性、多接続という特徴を活かし、これまでの「人」から「あらゆるモノ」にまで、通信の対象が広がろうとしています。これに伴い、様々なビジネスユースケースへの 5G の展開が期待されています。そして、その実現にあたってはネットワークスライシングが重要な役割を担うことになります。

ネットワークスライシングは、各サービスの要件に応じて差別化された処理を提供する論理ネットワークの作成を目的としています。ネットワーク上の様々なファクター (遅延や帯域、可用性など) を考慮しながら、サービスに求められる SLA (Service Level Agreement) を満たす最適な論理ネットワーク (スライス) を構成します。一旦作成された後も継続して SLA を監視し、必要に応じてスライスを作成し直すことも可能です。 SDN コントローラ、オーケストレータと組み合わせることにより、スライスの迅速なプロビジョニング、継続的な監視、再構成のクローズド・ループを自動で回すことができます。

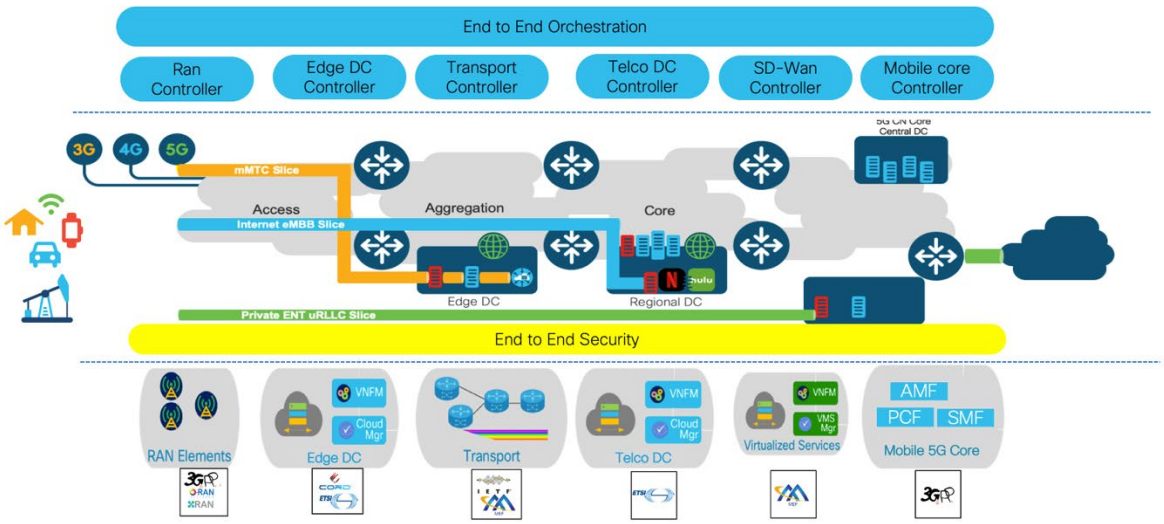


図 5-1 ネットワーク・スライシング- カスタマイズド・ネットワーク・インスタンス

ネットワークスライシングでは、キャリア網内の各ドメインを跨ぐ一気通貫なスライスを提供することが重要になります。エンドツーエンドで真にサービス要件を満たすには、 RAN/トランスポート/パケットコア/データセンターの全てのドメインが、一貫したポリシー・制御のもとでスライスを作成していくことが求められます。エンドツーエンドスライシングは、文字通りユーザ端末からデータセンター内の宛先アプリケーション・サーバ、もしくは企業向け通信であれば企業設備との接続ポイントまで一気通貫で繋ぐ専用ネットワークを、ビジネスニーズに応じて迅速、かつ柔軟に提供するものです。

5.2 スライスの求められる背景

5G 時代のいま、ネットワークスライシングが求められる背景を以下に挙げます。

URLLC (Ultra-Reliable and Low Latency Communications) などを活用した新サービスへの対応

5G において注目されているユースケースの 1 つが、ゲーミングや AR/VR などの超低遅延 (URLLC) の特徴を活用したサービスです。エンドツーエンドで数 10ms 以下（場合によっては 10ms 以下）の遅延要件が求められるこれらサービスの通信においては、刻々と変化するネットワーク環境の中で、要求される通信品質を常に安定して担保できることがサービス提供の鍵となります。ネットワークスライシングは、他のサービス (大容量通信サービスなど) と区別した低遅延専用スライス（低遅延に最適化された論理ネットワーク）を作成・展開することにより、求められるサービス品質を提供することができます。また、伝送路の遅延が大きくなった場合などは、迅速に検知し、必要に応じて経路変更などスライスの構成を自律的に組み替えることにより、求められる遅延要件を遵守しながら安定したサービスを維持します。このようにネットワークスライシングは、5G 時代の新サービス要件に応える、最適化された専用論理ネットワークを提供します。

セキュリティ

5G では、莫大な数の「モノ」が接続されてくることが想定されます。これに伴い、今まで以上にセキュリティリスクの増大が懸念されます。このため、企業からはキャリア網内においても他社の通信から自社の通信を隔離したいとの要望が増えています。ネットワークスライシングは、このような通信の隔離、セキュアなネットワーク提供の手段としても用いることができます。

所有からシェアへ

これからのキャリア網は、自社の通信だけではなく MVNO (Mobile Virtual Network Operator) や ISP とシェアしながら様々な通信を重畳させていくシェアリングエコノミーの形態を取るケースが増えてくると考えられます。ネットワークスライシングは、このような他社サービスネットワークの閉域性を保ちながら、1 つの物理ネットワーク上へ展開するケースにおいても有効な手段となり得ます。

企業ユーザによるキャリアネットワーク・リソースの活用

ロボットや HD カメラなど企業の IoT デバイスが 5G で接続される環境においては、これら IoT デバイスの通信に対しても、その企業独自のポリシー（QoS ポリシー、セキュリティポリシー、等）の適用を望むケースがでてくると考えられます。この場合、キャリア網内にその企業専用のスライスを作成することで、企業はそのスライスを企業ネットワークの延長と捉えることができ、提供された API を通じて独自のポリシーを適用し自社ネットワークと同様の運用を行うことができるようになります。

5.3 各業界団体、標準化団体におけるネットワークスライシングの検討

ネットワークシステムにおいて、ネットワークに関するリソース（QoS キュー、Routing Table、Traffic Engineering Path など）を分離し、ネットワーク品質の差別化や運用管理の分離を行うことは、従来から行われていました。また、近年モバイルゲートウェイが仮想化され、論理的インスタンスを柔軟に生成および配置することが可能になりました。5G を取り巻く環境では、それらの論理分割をより柔軟かつ迅速で魅力あるサービス提

供に結びつけるために、様々な業界団体や標準化団体がネットワークスライシングを定義し検討を進めています。本章の Appendix にて、各団体での検討状況を記載いたします。

5.3.1 各標準化団体・業界団体の検討状況まとめ

現在、多くの標準化団体・業界団体でネットワークスライシングの検討を行っており、それらを概観すると、いくつかの検討の側面が浮き彫りにされます。次の表に、検討の側面、主要な標準化団体・業界団体、検討のポイントを整理します。

表 5-1 標準化団体・業界団体のネットワークスライシング検討状況

検討の側面	標準化団体・	検討の側面
Architecture	NGMN、GSMA、etc.	価値、アーキテクチャ設計、全体ポリシー
Management、Orchestration	ITU-T、IETF、ETSI ISG NFV、etc.	抽象化、自動化、サービス提供、サービス保証
Transport Slice	IETF、MEF、IEEE、etc.	リソースの共有と分離、Multitenant/VPN、QoS、ポリシー、トポロジー分割 SLA モニタリングとアシュアランス
Packet Core Network Slice	3GPP	CN Slice の共有と分離、ノード/スライス選択、Décor
RAN Slice + UE	3GPP	DL/UL スケジューリング、ハンドオーバー管理、呼制御ポリシー、電波利用管理、Dual Carrier ポリシー、リンク多重ポリシー、SON ポリシー

5.4 エンドツーエンドスライスの実現手法の一例

上記のとおり、現在各標準化団体・業界団体において各々のドメインを中心にネットワークスライシングの検討が行われています。そして、今後はエンドツーエンドスライスを見据えたクロスドメインでのネットワークスライシングの在り方が議論されていくことになると考えますが、現時点では、エンドツーエンドでの検討はまだ活発には行われておらず、各事業者が個別に手法を模索しているのが実情です。

このような状況で、エンドツーエンドスライシングを具体的に考える一助となるべく、低遅延サービス向けエンドツーエンドスライス実現手法の一例を以下に示します。

マネジメント・プレーン

下記例では、各ドメイン（RAN/トランスポート/ファブリック/モバイルネットワーク）に配置されたドメインコントローラと中央に配置された E2E (エンドツーエンド) オーケストレータが連携しながら、オペレータもしくはユーザの要求に沿ってエンドツーエンドでスライスのプロビジョニング、運用・監視を行っています。

フォワーディング・プレーン

RAN ドメインでは、無線のリソースブロック割当や波形をスライス毎に適切に選択することで無線区間における低遅延要求条件を満たし、IEEE802.1q (VLAN) 等でトランスポートとの橋渡しと区分けを行います。トランスポートドメインでは Flexible Algorithm (Flex-Algo) [5-1] を用いて低遅延に最適化されたトポロジーを用意しています。ファブリックドメインでは IEEE802.1q によりスライスを区分しています。モバイルドメインでは低遅延サービス専用 UPF を立て、他のサービスから分離して低遅延処理を提供しています。

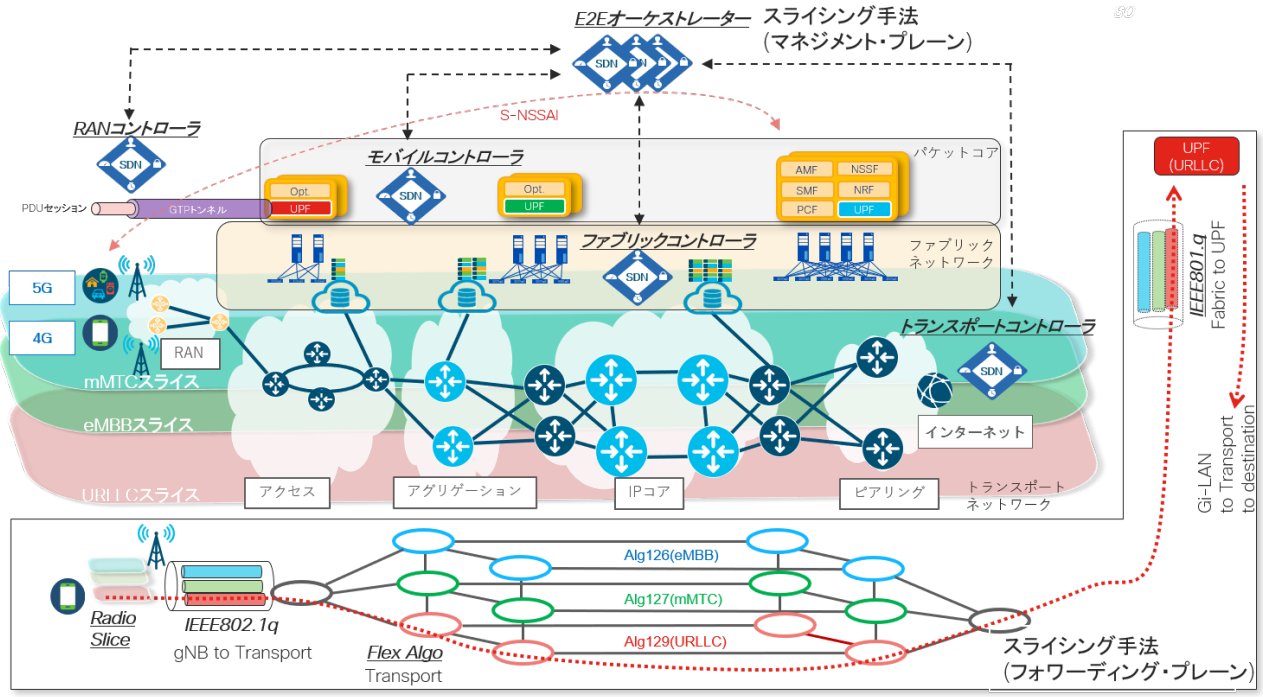


図 5-2 エンドツーエンドスライスにおけるスライシング実現手法の一例

エンドツーエンドスライス上でのパケット転送

ユーザ端末は自身が属するスライス情報（S-NSSAI [5-2] 等）をコアノード（AMF、SMF 等）とやりとりし、スライスに紐付いた PDU セッションをターゲットの UPF（この例では低遅延専用 UPF）との間で確立します。ユーザ端末からの PDU セッションを基地局（gNB 等）は GTP エンキャップ後、該当スライスに紐づく IEEE802.1q VLAN に転送します。トランスポートドメインでは Flexible Algorithm にて用意された低遅延スライス専用トポロジー上で転送され、ファブリックドメインでは該当 IEEE802.1q VLAN 上を渡り、モバイルドメインでは低遅延専用 UPF に到達します。その後、 GiLAN 側に転送され同様に低遅延スライス専用トポロジー上で宛先まで転送されます。この例では、ユーザ端末から RAN/トランスポート/ファブリック/モバイル（パケットコア）、そしてデータセンターもしくは企業設備の接続点まで、同一ポリシー（低遅延）にてエンドツーエンドで低遅延に最適化されたスライスを実現している一例を示しています。

5.5 今なぜネットワークスライシングなのか

共通の物理ネットワーク上に複数の論理ネットワークを実現するという考え方は旧来より存在します。VPN で仮想の専用ネットワークを実現することができ、QoS やトラフィック エンジニアリング技術によって SLA 特性の差別化が可能です（今では、セグメントルーティング技術、および Flex Algo や TE Policy を使って、よりシンプルに VPN や異なる SLA を提供することができます）。また、セルラーネットワークでは、APN でサービスを分けることも可能です。

では、今なぜネットワークスライシングが注目されているのでしょうか。それは、5G というモバイルネットワークにおける世代進化は、単なる Radio 技術の進化ではなく、ネットワークシステムアーキテクチャ全体に関わる大きな変遷契機であるからです。「モバイルファースト」と言われるように、現代のほとんどのシステムは、スマートフォン、 タブレットなどモバイルでの使用を前提としています。つまり、モバイルは今や普遍的にほとんどのシステムに組み込まれており、もはや特殊なシステムではありません。そして何よりも、現代の、着目すべきより大きな潮流は、デジタル トランスフォーメーションとデジタル ディ

スラプションです。このデジタル ディスラプション (非連続的、破壊的な変化) は、様々な市場の勢力図を塗り替え再定義する可能性を秘めており、デジタル ボルテックスによると、それぞれの業界の市場シェア上位 10 社のうち平均 4 社がデジタル ディスラプションによってその地位を失うと考えられています [5-3]。

そのような中、ネットワークシステムは、より利便性と提供価値を高める必要があります。これまでのやり方で、これまでのドメイン毎に、帯域増強や信頼性向上などの改善を行うのでは立ち往きません。例えば 5G の 1 つの要件とされる URLLC は、 Radio 部分だけが超低遅延を実現しても、システム全体として超低遅延性・高信頼性を実現しないとあまり意味がありません。デジタル時代の進展を念頭に、時期を同じくして起こっている技術進化 – SDN・プログラマビリティ、仮想化・クラウドネイティブ、自動化、機械学習、IoT プラットフォーム、エッジコンピューティング、オープン・ディスアグリゲーション – なども併せて、アーキテクチャ全体を俯瞰してシステムを再定義する必要があります。その再定義の 1 つがネットワークスライシングであると考えます。

現在多く業界団体や標準化団体において、ネットワークスライシングの検討が行われています。本章の Appendix として、スナップショット的ではありますが、業界団体や標準化団体においてどのような議論が行われているかを示します（2019 年中盤時点）。当然のことかもしれませんが、エンドツーエンドの検討は概念的なものに留まり、詳細の検討は専らドメイン毎に個別に行われているのが現状です。

5.6 ドメイン間の検討

多様な SLA やこれまでとは全く異なるユーザ体験を提供するためには、システム全体の検討が必要です。モバイルネットワークシステムは、3GPP 用語で言う所の RAN、CN、TN、DN などのドメインから構成され、現在それぞれのドメイン毎にネットワークスライシングの検討が進んでいますので、それらを統合することが求められます。まずは、ドメインを統合するオーケストレータが、それぞれのドメインのオーケストレータと連携し、エンドツーエンド オーケストレーションを実現することが考えられます（図 5-3）。エンドツーエンドオーケストレーションの具体的方法論については、第 6 章で記述します。

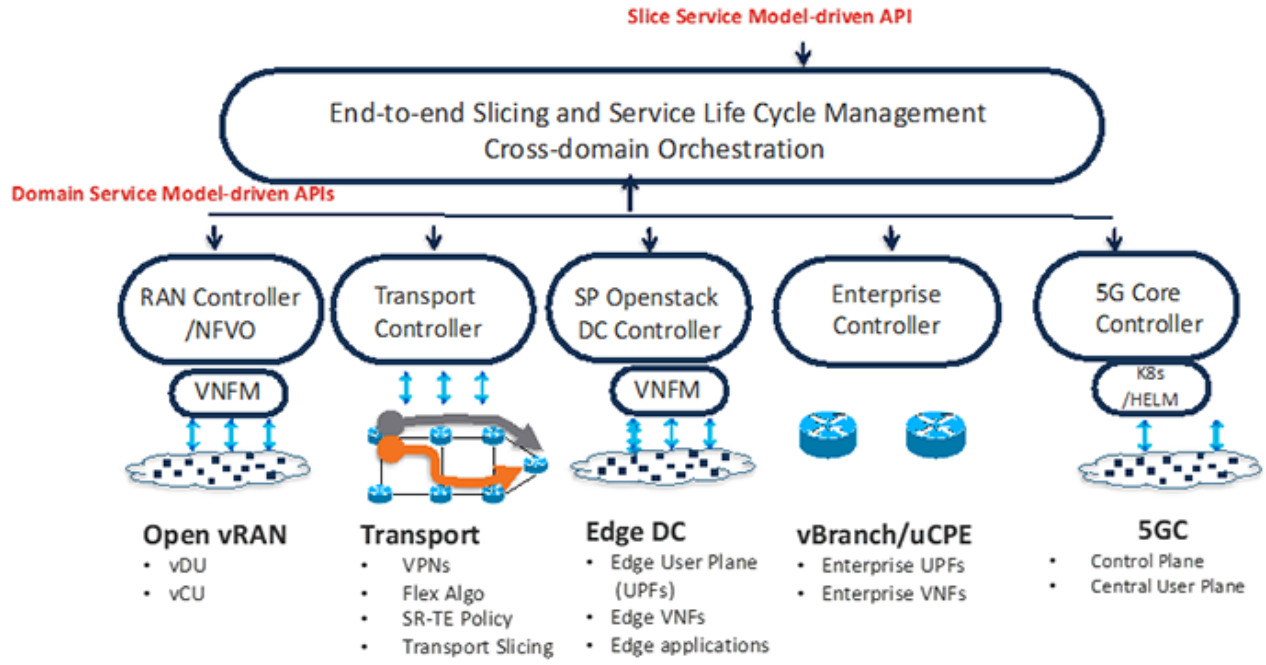


図 5-3 エンドツーエンド ネットワークスライシングとサービス ライフサイクル向けの
クロスドメイン オーケストレーション (Source: John Mullooly)

また、実際のトラフィックを適切なネットワーク側スライスにマッピングするために、データプレーンのマッピング方式も必要になります。前回述べたように既存の VLAN ID を使うことが考えられますが、新たな ID (MNTC-ID; Mobile Network Transport Context ID、SLID; Slice ID) を導入する提案も出てきています draft-clt-dmm-tn-aware-mobility [5-4] 、 draft-filsfils-spring-srv6-stateless-slice-id [5-5]) 。

5.7 ドメインを超えた検討と今後の展望

より革新的に考えると、ドメイン間連携の検討だけでは不十分で、必ずしも既存アーキテクチャを踏襲するのでなく、新たなドメイン境界を定義することも含めてドメインを超えて検討することが必要になります。前述例の URLLC サービスでは、システム全体で超低遅延を実現するために、コンピューティングやストレージをどう分散配置するかも重要な要素になります。さらに、これからのデジタル時代のサービスを考えると、これまでのコネクション中心ネットワークアーキテクチャ (どのように接続性を提供するか) ではなく、データ中心アーキテクチャ (どのようなデータをどう収集・蓄積・分析するか) にシフトする必要があると考えます。今までの慣習にとらわれていたら、ネットワークシステムの価値を高めることはできません。

これは 1 つの例ですが、例えばモバイルパケットコアは、CUPS (図 5-4) により、コントロールプレーンとユーザ プレーンが完全に分離され、UPF はデータ転送に特化するように進化しました。このことにより、モビリティを支えるためのアンカーポイントをコントロール プレーンとは独立して偏在させることができるため、より柔軟なコンピューティングやストレージの配置や、ローカル 5G のような、企業システムとの新たな形態での融合が可能になります。そうであれば、もう一歩論を進めて、gNB や UPF などデータプレーンを司るエンティティを、モバイル側でなく TN 側もしくは DC ファブリックやエンタープライズ スイッチ ファブリック 側に属させる方が、アーキテクチャがシンプルになる可能性があります。現状では、これらが別ドメインであるため、まず、データプレーンとしてトラフィックを識別し、適切なスライスにマッピングするための VLAN-ID 等の余計な ID を割り当て・管理する必要があります。また、ネットワーク側との接続点が Single Point of Failure/Bottleneck になるため、それを避けるために MC-LAG や制御プロトコルを駆使して冗長化する必要があります (図 5-5) 。これらは、スライスの数が増えた時にそのまま複雑化とコスト増大の要因になり得るため、アーキテクチャ見直しによる効果は大きいと考えます。そこで筆者を含めたグループは、ドメイン境界見直しの必要性について、IETF DMM WG で議論を開始しました (draft-kohno-srv6mob-arch [5-6]) 。

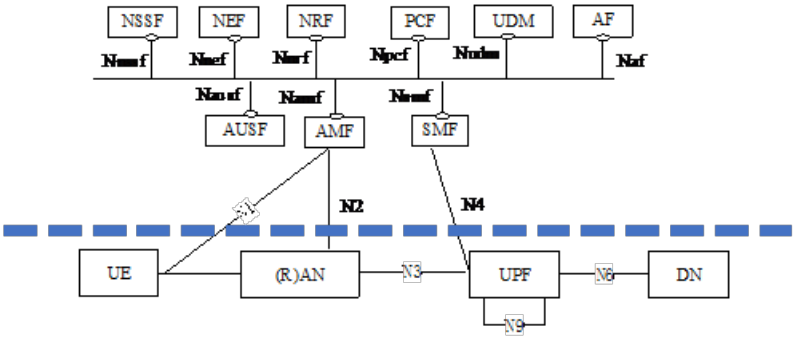


図 5-4 CUPS (Reference – 3GPP TS23.501)

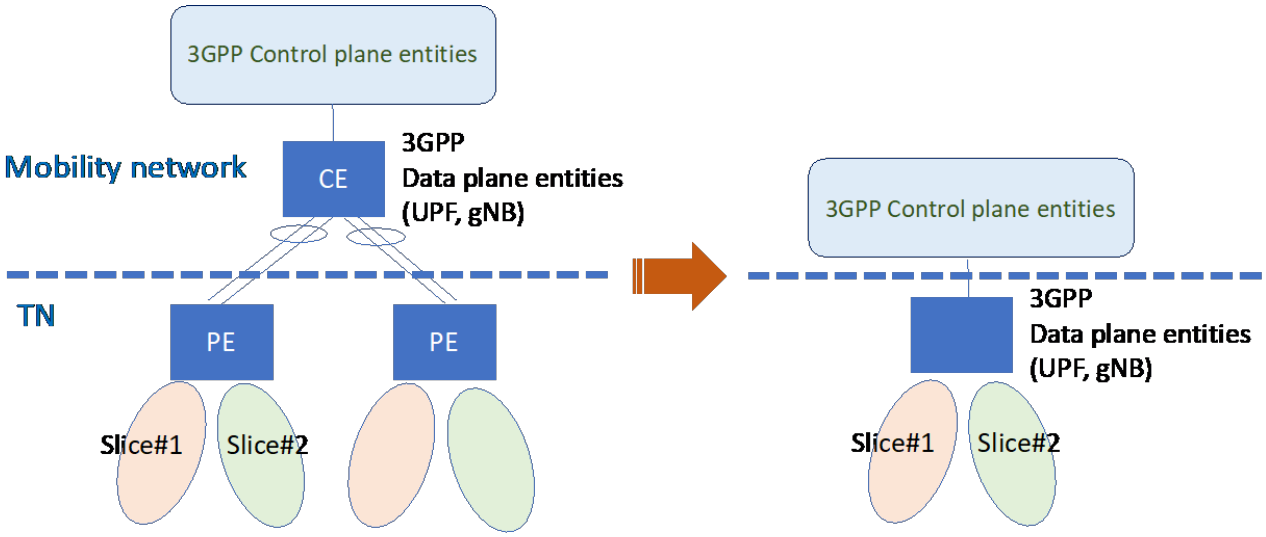


図 5-5 ドメインを超えたアーキテクチャ見直しの例： UPF、 gNB をネットワーク側のエンティティとする

このように、デジタル時代の新たなアプリケーションやサービスを効率的に提供するためには、ドメイン間連携のみならず、ドメインを超えたアーキテクチャの見直しも必要であると考えます。既存のドメインを踏襲するだけでは、Distributed/Edge Computing の有効活用や、データ中心アーキテクチャ（どのようなデータをどう収集・蓄積・分析するか）へのシフトは困難です。

5.8 まとめ

本章では、ネットワークスライシングというテーマを中心に、現在の検討状況と今後のアーキテクチャ展望について議論しました。ネットワークスライシングを、デジタル時代に真に有用なプラットフォームサービスにするためには、ドメイン間の検討のみならず、システムを俯瞰し、ドメイン境界を見直す必要があります。そしてさらに重要なのは、このネットワークスライシングを使っていかに優れたシステムを構築できるか、ということです。そのためには、接続対象となるシステムに対し良い抽象化と API を提供すること、ポリシーや ID の連携ができることなどが必要になります。この辺に関しては、第 7 章「5G/Hetnet の企業向け活用」でも少し触れます。

5.9 Appendix

第 5 章の Appendix として、ネットワークスライシングについて、業界団体や各標準化団体において、どのような議論が行われているかの概略をまとめました (2019 年中盤時点) 。ネットワークスライシングというトピックについて、いかに多くの業界団体・標準化団体がその策定に取り組んでいるか、ということがわかります。ただし、これは一時点の非網羅的なスナップショットに過ぎず、正確な検討内容については、各団体の出版物をご参照ください。

5.9.1 NGMN

NGMN (Next Generation Mobile Networks [5-7]) は、次世代モバイルネットワークに関する標準化、実用化を策定するアライアンスであり、日本からも NTT ドコモが参画しています。NGMN は、5G white paper [5-8]を発行し、その中でネットワークスライシング を「共通の物理インフラ上で，仮想的に独立した事業として複数の論理ネットワークを運用する概念」と定義しています。また、「ひとつのネットワーク スライスは，仮想的に独立したエンドツーエンドネットワークと捉えられる」と、RAN、パケットコアなどのドメインを越えてエンドツーエンドで検討することの重要性を強調しています (図 5-6) 。

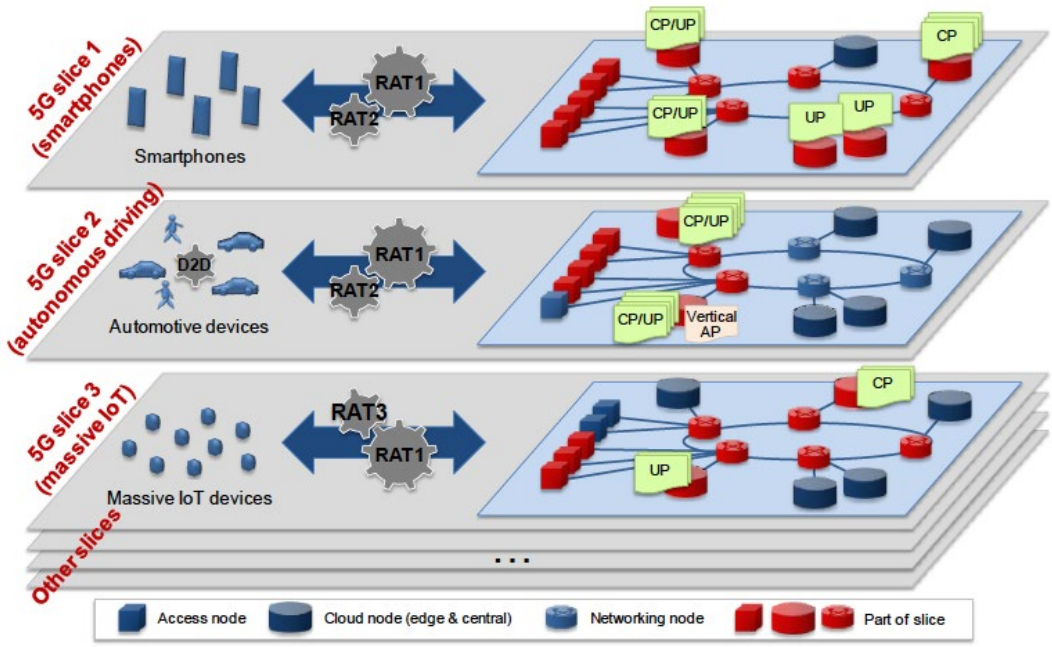


図 5-6 共通基板上に実現されるネットワークスライス (NGMN)

5.9.2 GSMA

GSMA (GSM Association [5-9]) は、800 社近くの移動体通信事業者や端末製造メーカー、ソフトウェア企業が加盟する世界最大の携帯通信事業者の業界団体で、Mobile World Congress の主催でも有名です。GSMA では Future Network Program の一環としてネットワークスライシングへの手引き[5-10]を発行しており、その中で、ネットワークスライシングはモバイル通信事業者が SLA に準拠した特定のビジネス要件に合わせた接続性とデータ処理を提供するために必要と述べています（図 5-7）。スライシングにより、データ速度、品質、待ち時間、信頼性、セキュリティ、およびサービスなどを、顧客要望に合わせてカスタマイズ可能であるとしています。

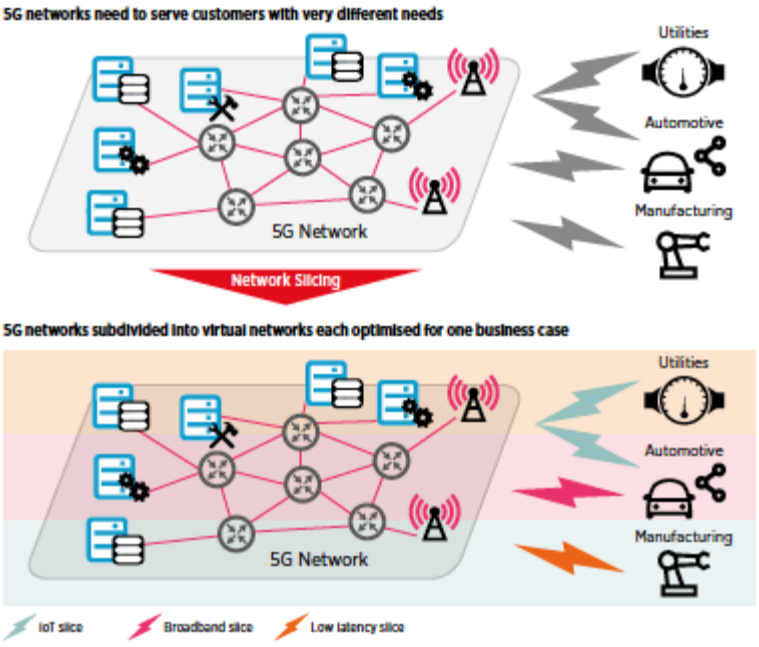


図 5-7 各ビジネス要求に最適化された仮想ネットワーク (GSMA)

5.9.3 ITU-T

ITU-T (International Telecommunication Union-Telecommunication Standardization Sector [5-11]) は、国際電気通信連合の部門の 1 つで、通信分野の標準策定を担当しています。ITU-T は将来のネットワークのあり方を検討する FG-IMT2020 (Focus Group on IMT-2020) を設置し、そこでネットワークスライシングについても議論されました。実際の技術標準化は 3GPP 等で行われるため、ITU-T では主にアーキテクチャ概念が整理され、スライスの階層化とマネジメント、オーケストレーションとの関係が重視されています (図 5-8) 。

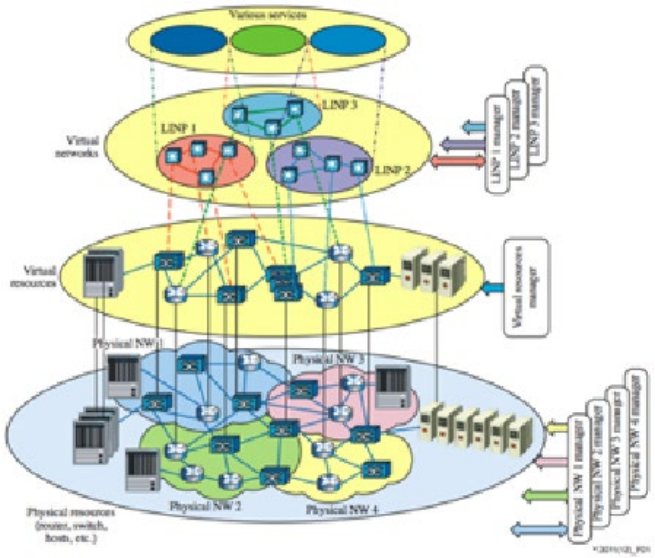


図 5-8 ネットワーク仮想化のフレームワーク (ITU-T Y.3011)

5.9.4 IEEE

IEEE は米国に籍を置く、世界最大の電気工学、電子工学に関する学会かつ標準化組織です。IEEE 自体ではネットワークスライシングに関する標準化を行っていませんが、IEEE 主催カンファレンスである Netsoft (International Conference on Network Softwarization [5-12]) において、スライシングに関する特集を行っています。図 5-9 は、Netsoft で行われたネットワークスライシング Tutorial によるもので、ネットワーク スライスのタイプと、それぞれの管理責任主体について整理しています。

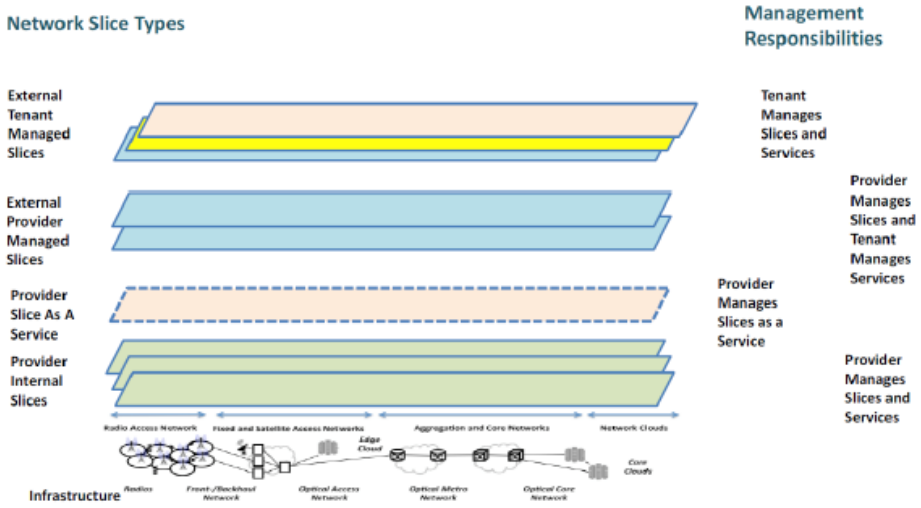


図 5-9 ネットワークスライシング Landscape (IEEE Netsoft Tutorial)

5.9.5 ONF

ONF (Open Networking Foundation) [5-13]は、あらゆるネットワークをソフトウェアで定義可能にする SDN (Software Defined Network) を推進する非営利団体です。ONF では、5G スライシングも SDN の 1 つのアプリケーションとして定義しています [5-14]。図 5-10 は SDN をベースにしたスライスの抽象化を示しています。

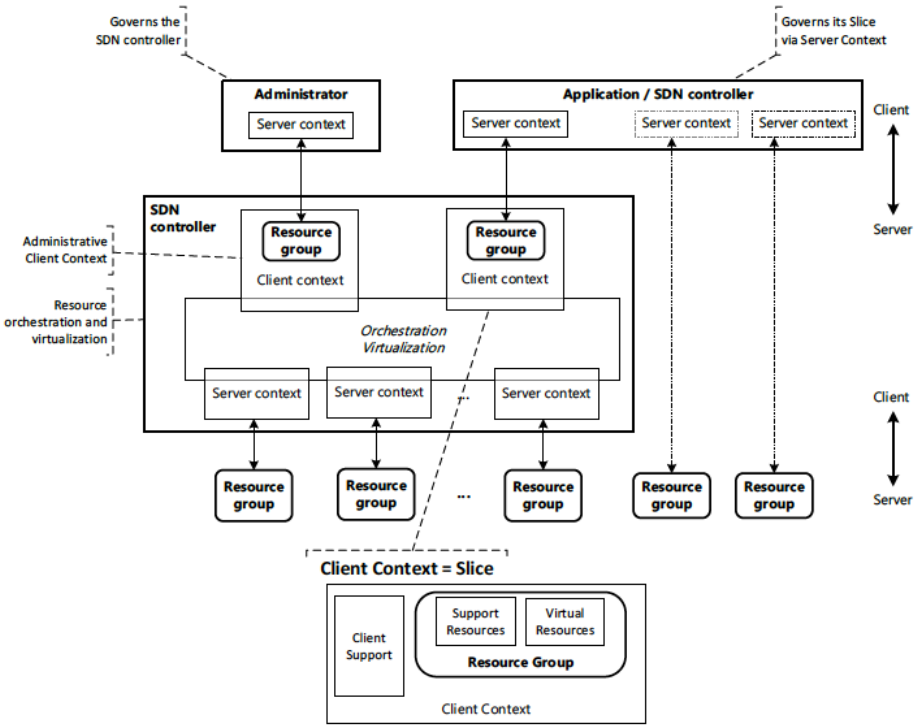


図 5-10 SDN based Slice Abstraction

5.9.6 IETF

IETF (Internet Engineering Task Force) は、インターネットや IP に関わるプロトコルの標準化を行う団体です。いくつかの BoF や Working Group においてネットワークスライシングに関連する議論が行われています。

ACTN (Abstraction and Control of Transport Networks) [5-15] BoF では、トランスポートネットワークの制御および抽象化をどのように行うかを議論しました。図 5-11 は、トラフィックエンジニアパスをどのように抽象化し、また仮想ネットワーク (VN) をどのように定義するかを示しています。

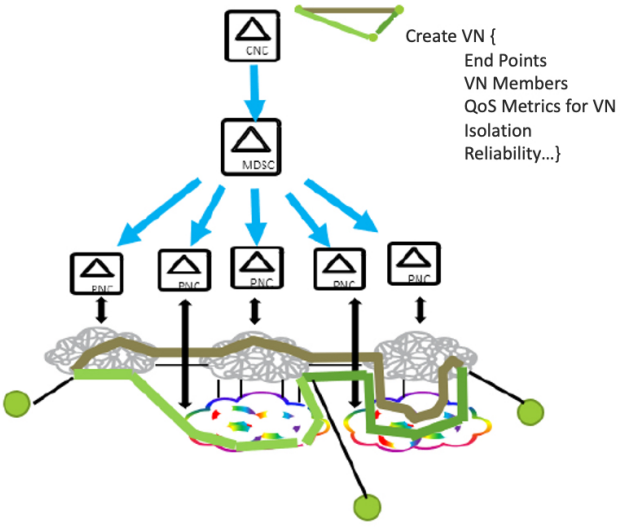


図 5-11 ACTN framework for ネットワークスライシング

さらに、複数のドメインにまたがるエンドツーエンドスライスをどのようにモデル化してどのようにサービス定義するか、などを議論するため、COMS (Common Operation and Management on network Slices) [5-16]が、BoF として設定されました。しかし、議論のポイントを絞るのが難しく、また IETF で議論すべきなのか、という根源的な問いも提起され、一旦この BoF も終結しています。しかし、IETF で議論すべきかは別として、このような検討は必要と思われます。図 5-12 は、COMS が検討しようとしたサービス デリバリー インターフェイス、カスタマー サービス インターフェイスおよびフレームワークを示しています。

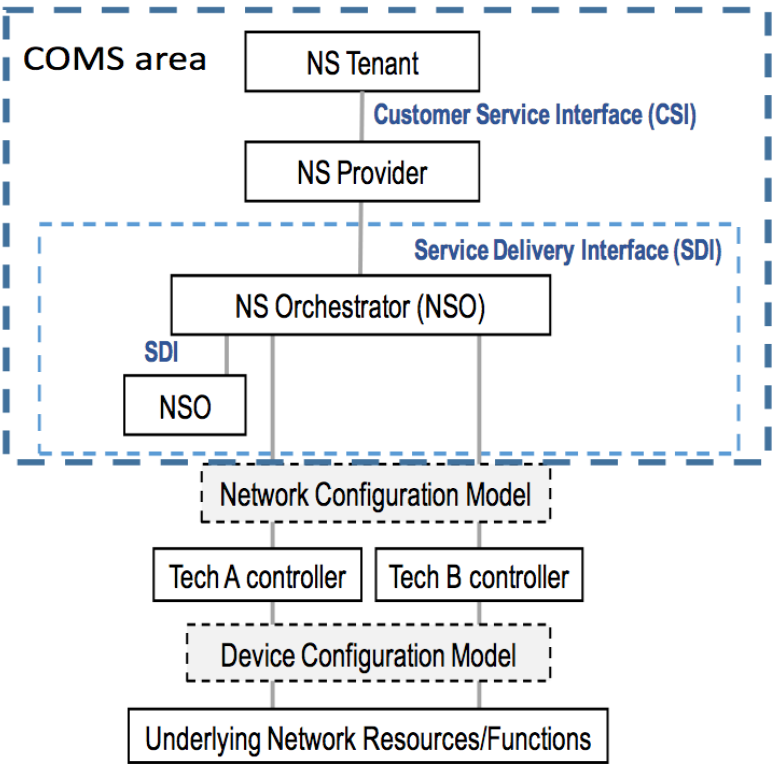


図 5-12 “COMS motivation” IETF101 COMS BOF

IETF の本領は IP プロトコル周辺であり、ネットワークスライシングを構成する要素技術の多くが (L2/L3VPN、セグメントルーティング、トラフィック エンジニアリングなど) IETF で検討・標準化されています。ここではその中でも、現在セグメントルーティングを標準化する SPRING WG で議論されている Flex Algo によるネットワークスライシングの実装可能性について紹介します。

IGP Flex Algo [5-17] は、IGP extension により、各ノードは、そのノードが属するアルゴリズム番号、およびそのノードが持つ prefix をアルゴリズム番号に紐づけて広報します。アルゴリズムに持たせる意味はネットワークオペレータが任意に定義できますが、これをネットワークスライシングに適用することにより、ネットワークオペレータは、 Slice ごとに異なるトポロジーを生成可能です。このことにより、ポリシーの適用を完全自動的に行うことができ、またパスを指定するための SID 段数も最小化することができます。

なお、セグメントルーティング関連技術を利用したネットワークスライシングについては、“Building blocks for Slicing in Segment Routing Network [5-18] ” に記述しています。

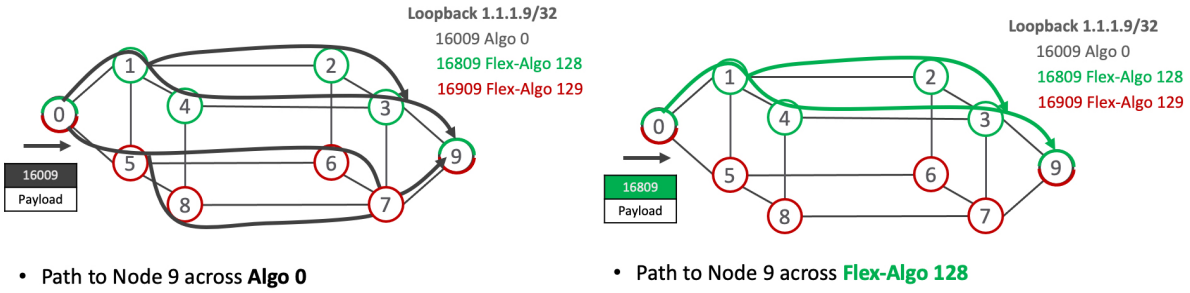


図 5-13 IGP Flex アルゴリズムによる Multi Plane の実現

5.9.7 MEF

MEF (旧称; Metro Ethernet Forum) は、元々 EFM (Ethernet in the First Mile) / Carrier Ethernet に関する標準化を行っていた非営利のコンソーシアムですが、 現在は MEF と改名し、Optical, IP, SD-WAN, Cloud Service, LSO (Life Cycle Orchestration) などにも領域を広げています。 MEF で行われたセミナー [5-19] では、トランスポート スライスにおいてスライシングをどのように表現するかについて記述しています (図 5-14) 。

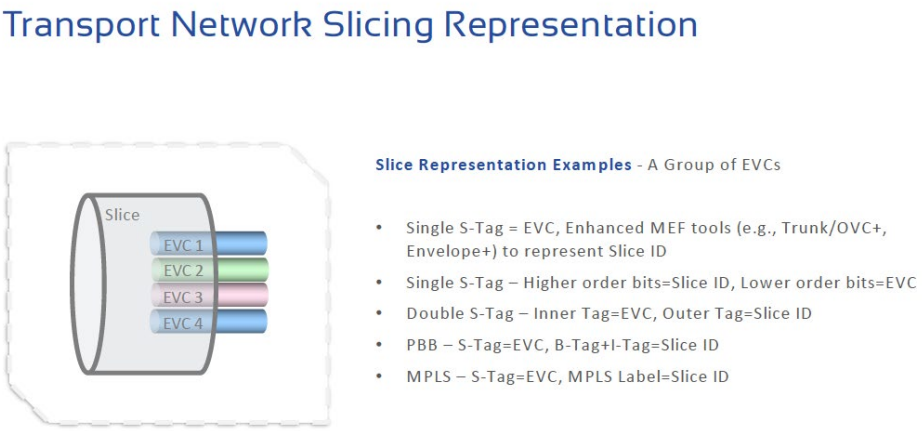


図 5-14 Network Slice Representation

5.9.8 3GPP

3GPP (3rd Generation Partnership Program) は、モバイルブロードバンドの標準化を司る標準化団体です。団体名称は 3GPP ですが、3G だけでなく 4G、5G の標準化も行っています。3GPP では、5GC Architecture (TS 23.501) を中心に、ネットワークスライシングの定義を行っています。3GPP における検討の対象は AMF, SMF, UPF, PCF などの Mobile Gateway Node であり、スライスの定義をまとめると下記のようになります。

- 動的に作成される論理的なエンドツーエンド ネットワークである
- ネットワークスライスは、RAN 部分と CN 部分から構成される
- UE は複数のスライスにアクセスすることができる
- 各スライスは、SLA で合意したサービスタイプを提供する

図 5-15 に示すように、Mobile Gateway は共有または分離され、どのように Gateway Node もしくはスライスを選択するか、ということが検討の中心です。

また、3GPP ではスライス識別子を定義しています。スライス識別子 (S-NSSAI, Sub Network Slice Selection Assist Information) は、スライスサービスタイプ (SST) およびスライス区別 (SD) から構成され、ネットワークスライスの識別・選択は、S-NSSAI を介して行われます。 UE は最大で 8 つまでの S-NSSAI を持つことができます。代表的な SST 値として下記が定義されています。

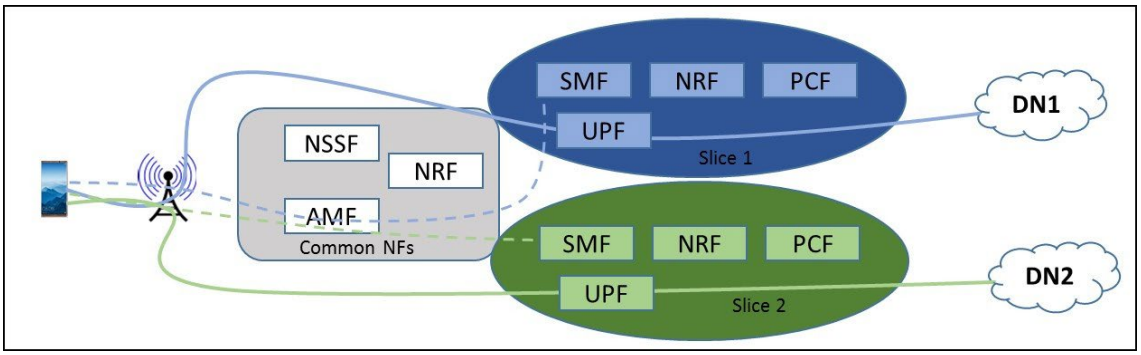


図 5-15 3GPP におけるスライス [5-20]

Slice/Service type	SST 値	特徴
eMBB (enhanced Mobile Broadband)	1	高データレート、高トラフィックデンシティのサポート
URLLC (Ultra Reliable and Low Latency Communications)	2	高信頼性と超低遅延のサポート
• MIoT (Massive IoT)	3	多数で高密度の IoT デバイスのサポート

RAN においても、スライシングの議論が行われています。UE からどのようにスライスを選択するかが主なポイントです。UE からダイナミックに指定する、予め UE を特定のスライスに登録しておくなど、いくつかの方法が検討されています。

特に無線区間は、リソース (Spectrum) が限られており、また Handover などのケアが必要なため、効果のあるスライス範囲を吟味し、複雑化させないための検討が必要です。

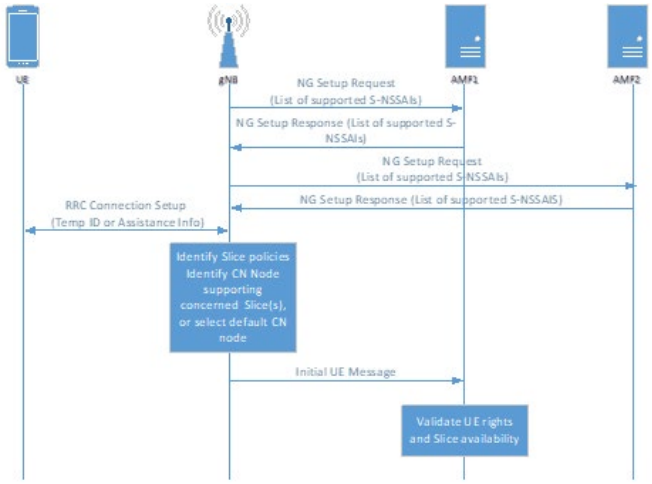


図 5-16 Radio Access Network におけるスライス選択例 (TS 38.300)

5.9.9 ETSI ISG NFV

ETSI ISG NFV は、ETSI (欧州電気通信標準化機構) においてネットワーク機能仮想化に関する、特にオーケストレーション周りの標準化を行うために発足されたグループです。 NFV Framework においてネットワークスライシングをどのようにサポートするかが主要テーマですが、NFV release 3.0 にて、エンドツーエンド ネットワークスライシングに必要となる「NFV におけるネットワークスライシングのサポート」、「複数の管理ドメインのサポート」、「複数サイト間のネットワーク接続性」をカバーすることを発表しました [5-21] [5-22]。

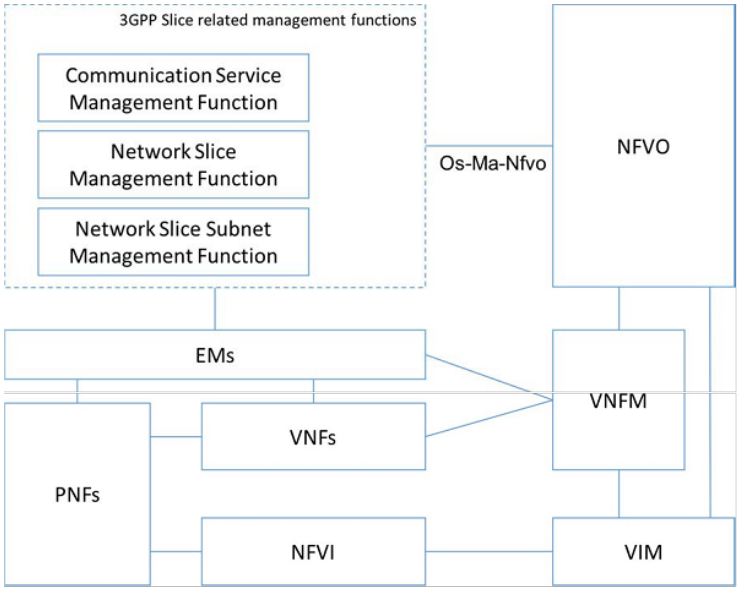


図 5-17 ETSI NFV フレームワークにおけるネットワーク スライス マネジメント (ETSI GR NFV-EVE 012)

5.10 追記 (2020 年 9 月)

5.10.1 追記にあたり

本稿執筆時点から少し時間が経ち、日本でも「beyond 5G」の議論が始まりました [5-23]。いかにリソースを共有もしくは配分しながら、効果的に、異なる品質要請を持つアプリケーションをサポートするために、エンドツーエンドネットワークスライシングの方式検討はこれまで以上に重要になります。特に、単なる接続性でなく、超高信頼低遅延などのシステム要件を実現するためには、ドメインを超え、レイヤを超えた方式検討が必要です。無線区間がどんなに速くなっても、パケットロスが避けられなかったり、遅延を縮減できなかったりすれば、アプリケーションのスループットは向上しません。

なお、本稿公開後にフィードバックやお問合せを戴きました。大変有難く感謝しております。1 つ重要なご質問がありましたので、それにお応えしたいと思います。それは、「本稿の出発点となる文書または定義は何か。NGMN ホワイトペーパー、3GPP TS23.501 か TS28.530 辺りと想定されるが如何」というものです。確かにそれらの文書は非常に重要で参考にしましたが、実際はより一般的な、「Multi-Tenant 分離」、「QoS/SLA 差別化」、「リスク分散や封じ込め」などのアーキテクチャ概念を出発点としています。そして各標準化団体や業界団体の活動や文書についてはなるべく偏らずに俯瞰的にサーベイすることを試みました。「ドメインを超えたアーキテクチャの見直し」のために、ある程度自由な視点が必要と考えるからです。一方、依拠不明と捉えられても反論の余地なく、今後改善して行きたいと思います。貴重なコメント、感謝いたします。

5.10.2 Appendix (5.9 業界団体・標準化団体動向) のアップデート

今回は固定網 (トランスポート) スライス関連を中心に簡潔にアップデートします。

2020 年 4 月に、MEF が “Slicing for Shared 5G fronthaul and backhaul” と題したホワイトペーパー[5-24] を発行しました。日本からも NTT が貢献され、事業者共通の共有 xHaul の要件や xHaul トランスポートのスライシング・共有化アーキテクチャを議論しています。

また Broadband Forum (BBF) では Fixed Mobile Convergence (FMC) を検討しており、そのコンテクストにおいて、サービス管理とネットワークスライスのオーケストレーション、ライフサイクル管理の運用、モバイルネットワークとの連携などについて検討しています [5-25]。

IETF においては、Network Slicing に関する Design Team が発足しました。TEAS WG (Traffic Engineering Architecture and Signaling Working Group) 配下に発足したため、トラフィックエンジニアリングのための論理的なネットワークトポロジーについての議論が中心です。トランスポートスライスおよび SLO (Service Level Objective) の定義 [5-26]、アーキテクチャフレームワークのモデリング [5-27] が策定されつつあります。

このように、標準化団体、業界団体における検討は進んでいます。また、組織間の交流もより活発になってきています。しかしそれでもまだ、ドメインを超える検討は不足しています。分散コンピューティング、エッジコンピューティングとの相互作用、データ中心アーキテクチャの実践など、現状からのフィードバックを重要視しながらも、抜本的なアーキテクチャ見直しを視野に入れて検討したいと考えます。

用語集

AMF (Access and Mobility management Function): 登録管理、アクセス制御、モビリティ管理機能を提供

APN: Access Point Name

AR (Augmented Reality): 仮想空間を重ね合わせることで人間が知覚する現実環境を拡張する技術

CN (Core Network): Mobile Packet Core

CUPS (Control and User Plane Separation): コントロールプレーンとユーザプレーンの機能的分離

DN (Data Network): インターネット、データセンタなどのネットワーク

GTP (GPRS Tunneling Protocol): 基地局とモバイルゲートウェイ間のトンネル

GiLAN: 3GPP で定義された SGi インターフェイスに置かれる LAN

IETF DMM WG: Internet Engineering Task Force Distributed Mobility Management Working Group

MVNO (Mobile Virtual Network Operator): 無線通信回線設備を開設・運用せずに、自社ブランドで携帯電話などの移動体通信サービスを行う事業者のこと

PDU (Packet Data Unit) セッション: ユーザ端末とデータネットワークが接続されている UPF との間で張られるトンネル

RAN (Radio Access Network): ユーザ端末をコアネットワークへ接続する無線アクセスネットワーク

S-NSSAI (Single Network Slice Selection Assistance Information): スライス識別子

SMF (Session Management Function): セッション管理機能を提供

TN (Transport Network): RAN と CN、CN 同士を接続するためのネットワーク

UPF (User Plane Function): 5G モバイル コアネットワークにおいてユーザプレーン処理に特化した機能を提供

URLLC (Ultra Reliable and Low Latency Communications): 5G 要件の 1 つで、超高信頼かつ低遅延な無線通信を実現

VPN: Virtual Private Network

VR (Virtual Reality): 仮想現実、ユーザの五感を刺激することで仮想的に物事を知覚させる技術

gNB (Next generation Node B): 5G 無線基地局

5G 時代に考える エンドツーエンド オートメーション

佐々木 俊輔

これまでの章では、主に 5G におけるネットワークインフラの技術やアーキテクチャの変遷について見てきました。それを踏まえて、本章のテーマである「エンドツーエンド オートメーション (自動化) 」について考えます。そもそも自動化とは何でしょうか。なぜ 5G では自動化が必要と考えられているのでしょうか。あらためて 5G のアーキテクチャの変革を振り返りながら、その理由を考えてみましょう。

なお、本章ではオートメーション、自動化、オーケストレーションの用語を同じ意味で用います。

6.1 5G システム アーキテクチャの変革のおさらい

図 6-1 に、これまでの章で見てきた 5G でのシステム アーキテクチャの変革の全体像を示しました。各セクションで見たポイントを整理してみます。

- 仮想ネットワークファンクション (VNF) やクラウド ネイティブ ファンクション (CNF) の登場により、ネットワークのコアからエッジまで様々な場所にテレコムクラウド基盤が構築されます (第 4 章) 。仮想・コンテナのフォーマットでデプロイされる VNF や CNF を動作させるための x86 サーバが多数配備されることになり、それを効率的に収容し管理するための広帯域・低遅延なデータセンター ファブリックが必要となります。
- エッジは特に大きく変革します。基地局のソフトウェア機能が分解 (ディスアグリゲーション) され仮想化した vRAN がエッジ DC で動作します (第 1 章) 。また、モバイル エッジ コンピューティング (Mobile Edge Computing; MEC) のユースケースでは、モバイルのユーザプレーン ファンクション (User Plane Function; UPF) や低遅延を要求する仮想・コンテナアプリケーションが展開されるようになります (第 3 章、第 4 章) 。
- エッジ DC の数の増大に伴って、エッジ DC 同士、およびエッジ DC とセンター DC をつなぐトランスポート ネットワークの重要性が増すことになります。さまざまなサービスが拠点をまたがって分散配置されるようになり、一貫した SLA や通信ポリシーの提供のためにエンドツーエンド ネットワーク スライスの提供が求められます (第 5 章) 。
- エンドツーエンド ネットワーク スライスで一貫した SLA を実現するためには、5G のコアおよび無線区間の通信ポリシーとトランスポート ネットワーク上での通信ポリシー、データセンター ファブリック上の通信ポリシーが一貫したものになる必要があります。これは、コントロールプレーン、データプレーン、マネジメントプレーンのすべての設定を統一的に制御しなければ実現できません。

こうしたポイントを踏まえて、本章のテーマであるエンドツーエンド オーケストレーションの必要性を考えてみましょう。

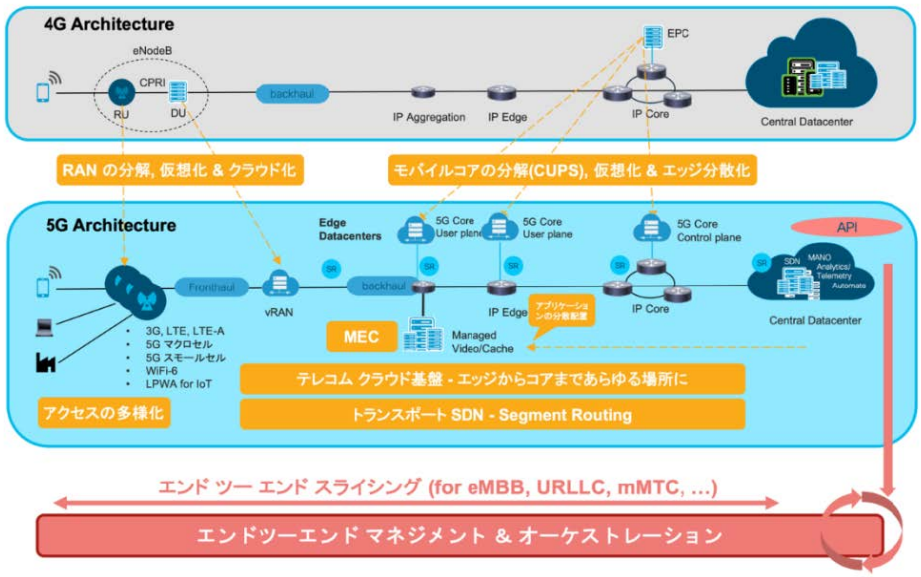


図 6-1 5G システム アーキテクチャの変革の全体像

6.2 変革から浮かび上がる運用上の課題

上で述べたようなインフラ側の変化から、次に挙げるように、従来のネットワーク インフラ運用になかった課題が浮かび上がってきます。

- システム管理者が扱うレイヤの数とコンポーネントの数が激増します。ネットワーク ファンクション本体の管理に加え、VNF が動く仮想レイヤ、CNF が動くコンテナ レイヤ、コンテナ OS を載せる物理サーバ レイヤ、それを収容する DC ファブリック レイヤ、さらにトランスポート ネットワークまでを、一貫したポリシーで管理しなければなりません。
- それぞれのレイヤの技術を理解し構築・運用・トラブルシュートできる人材が必要になります。運用コストを急に増やせない場合、従来よりもはるかに多くのコンポーネントを少人数で管理することになります。
- レイヤが増えることから、複数のレイヤ間で一貫した通信の設定を行うことが重要になります。例えば、仮想レイヤと物理ファブリック、トランスポートの間での整合的な VLAN 設定や VRF 設定、ルーティング設定などが挙げられます。
- ネットワーク ファンクションがディスアグリゲーションされ、マイクロサービスとして展開されるということは、従来は専用ハードウェア内部で行われていた通信がイーサネットや IP の通信として外部化されることを意味します。その通信を運ぶファブリックの設計や、通信の信頼性を担保、監視する仕組みが必要とされるでしょう。

これらの課題には個別にアプローチする必要がありますが、共通しているのは、人には扱いきれない複雑性の増加とデバイス数の増大、それに起因する運用上のヒューマン エラーのリスクだと言えるでしょう。そこで、5G では自動化によってこうした課題にアプローチすることが不可欠と考えられているわけです。

6.3 自動化のゴールは「クローズド ループ」

では、自動化を実現するために何が必要なのでしょうか。

自動化の究極的なゴールは、これまで人が行ってきた作業を人の手を経ずに行うことと言えるでしょう。従来のネットワーク オペレーションでは、人がネットワーク機器からさまざまなログやデータを取得して蓄積し、ツールを使って分析・可視化していました。そこから人が問題の兆候を見つけ出し、対処法を判断します。そして、人がサービスや機器に対して必要な変更を施します。データの収集から始まるこうした一連の作業を「クローズド ループ」と呼んでいます [6-1]。図 6-2 に、クローズド ループを構成する 4 つの大きな機能コンポーネントを示します。

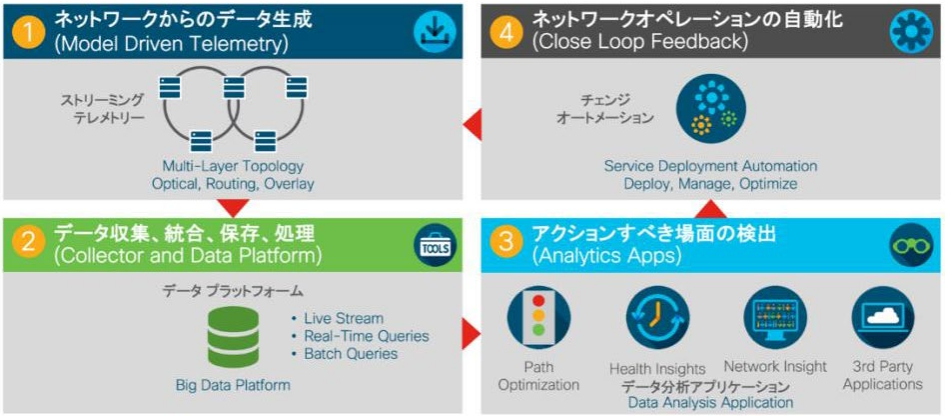


図 6-2 ネットワーク自動化のクローズド ループ

自動化とは、人間ではなくプログラム（ソフトウェアや AI と読み替えてもいいでしょう）に、このクローズド ループの各機能を実行させることと言えるでしょう。これを実現するためには、既存のネットワーク管理基盤にどのような要素を追加する必要があるでしょうか。図 6-2 をもとに、データを収集・分析する視点（図の 1、2、3）と、サービスおよびデバイスのライフサイクル管理（図の 4）の視点のそれぞれから考えてみましょう。

- データの収集・統合・保存・分析 (Assurance; アシュアランス)
  - ネットワークの各レイヤごとに、統計データやログを収集する仕組みが必要です。従来と異なるのは、人と違いプログラムが理解できる構造化データが出力されることが求められる点です。また、各レイヤの正確な状態を判定するためには、従来よりも高精度のデータを収集する必要もあります。これにはストリーミング テレメトリ[6-2] と呼ばれる技術が用いられます。
  - 大量のデータを処理し、必要なアプリケーションにフィードするためのコレクターおよびデータ プラットフォームが必要になります。
  - 複数のレイヤから収集されるデータを関連付け (コリレーション) して、問題の原因を推定する分析エンジンが必要になります。データが膨大な量になるため、こうした関連づけを人が行うことは困難です。そこで、近年の機械学習 (Machine Learning; ML) や人工知能 (Artificial Intelligence; AI) の助けを借りて、データから有意義な情報の抽出を行うことが必要になってきます [6-3]。
- サービス デバイスの設定とライフサイクル管理 (Provisioning; プロビジョニング)
  - 5G のシステムではネットワーク ファンクションは仮想化・コンテナ化されています。そのため、VNF・CNF の配置・起動・停止・削除等のライフサイクルを管理する仕組みが必要になります。ETSI (欧州電気通信標準化機構) [6-4] で定義された MANO スタックでは NFVO/VNFM のコンポーネントがこれにあたります
  - プログラムが設定を投入・変更・削除できるようにするために、各デバイスは自身のデバイスモデルを公開し API 経由で制御できることが求められるでしょう。また、管理コンポーネント同士が API 経由で連携できる仕組みも実装される必要があります。たとえば分析アプリケーションが問題を検知したら、プロビジョニングを担うオーケストレーションの API を叩いてネットワークの変更を行うことなどが考えられます。
  - エンドツーエンドでサービスを展開する場合、複数のドメインの複数のレイヤにまたがって整合的な設定を投入する必要があります。こうしたサービス単位の設定の抽象化を実現するためのオーケストレーション エンジンが必要になります

このようにプログラムにクローズド ループを実現させるという大きなゴールから検討を始めることで、必要となるアシュアランスおよびプロビジョニング用の管理コンポーネントをもれなく整理し、その要件を適切に特定していくことができます。ここに挙げたのは一般的な例に過ぎませんが、ユーザの事情に合わせた最適な自動化ソフトウェアスタックを選定するにあたっても参考となれば幸いです。

6.4 エンドツーエンド での オーケストレーションへ

第 5 章「5G 時代のエンドツーエンド ネットワークスライシング」で触れたように、エンドツーエンド スライシングは、ネットワークの各ドメイン(RAN、トランスポート、DC ファブリック、モバイルコア) ごとに配置されたドメイン コントローラと、中央に配置されたエンドツーエンド オーケストレータが連携しながらプロビジョニングおよび運用・監視を行うことが想定されています。

ところが、通信事業者のすべてのネットワーク ドメインに、一斉に自動化を導入できるかというと、実際には困難と言えるでしょう。そもそもドメインごとに対象となるテクノロジーが大きく異なります。また、ドメインごとに開発・運用・建設といった役割が分かれているという組織上の課題も挙げられます。他方、ドメインを分割しておくことで影響の局所化が可能であったり、ビジネスの動向に合わせて投資メリットのあるドメインから徐々に自動化を実装するスモールスタートが可能であったりといった利点もあります。

そこで、まずはドメインごとに自動化のクローズド ループの実現に取り組み、クロス ドメインのオーケストレーションを行う仕組みをその上に重ねるという階層的オーケストレーションが、現実的なアプローチと考えられています。これを表したのが図 6-3 です。

ここで大事なことは、各ドメイン内の自動化にあたっても、ゴールであるエンドツーエンド オーケストレーションを見据えた設計を採用することです。それぞれのドメインが自由に自動化を設計してしまうと、ドメイン間の連携時に多大な開発コストがかかるおそれがあります。そこで、各ネットワーク ドメイン内でそれぞれ完結したクローズド ループを構築しつつも、各ドメインのオーケストレータが外部向けには抽象化したサービス モデルを提供することが重要です。これにより、ドメイン間を疎結合の API で相互連携させることが可能になります。

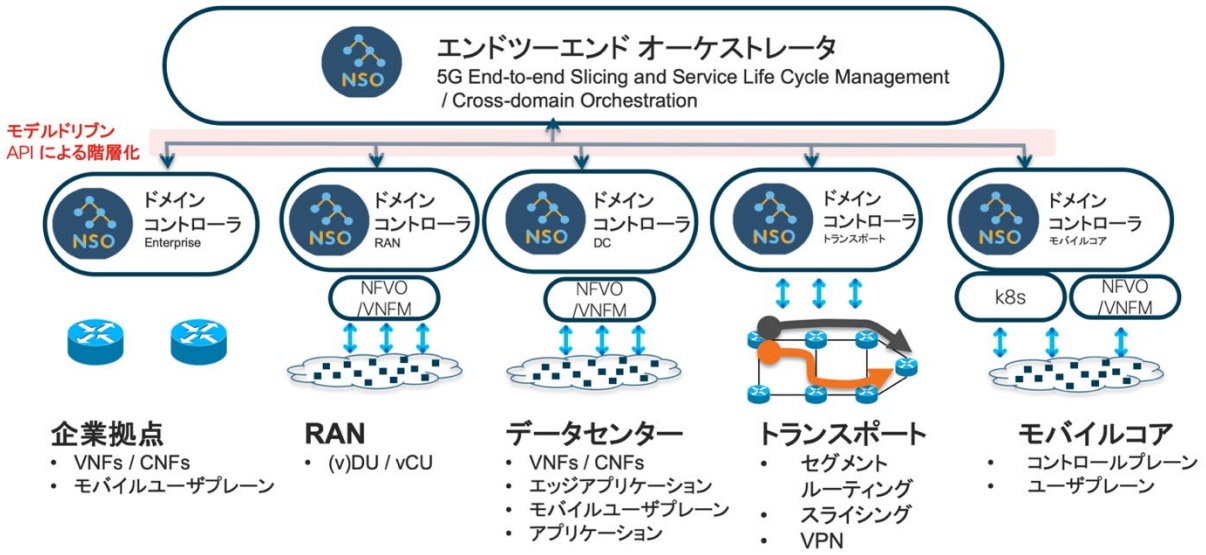


図 6-3 5G における エンドツーエンド オーケストレーション

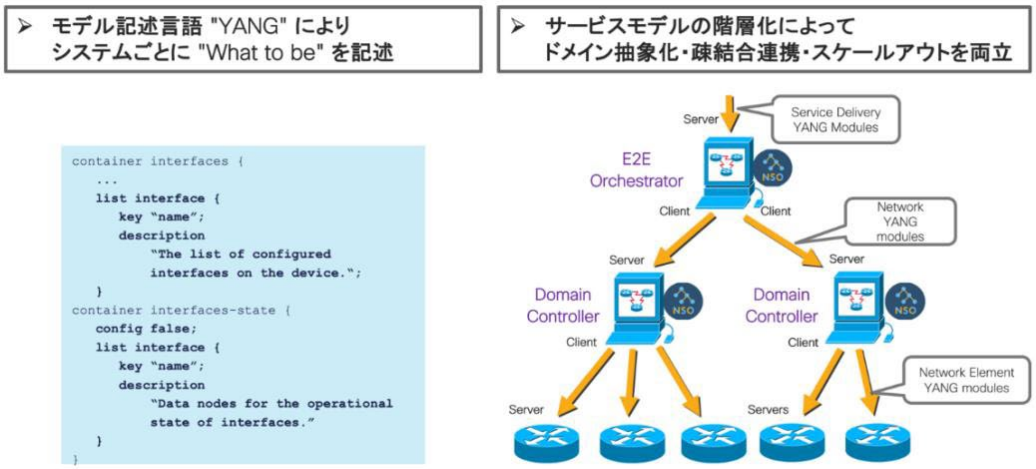


図 6-4 モデル駆動形オーケストレータと階層化アーキテクチャ

こうしたネットワーク ドメインの抽象化の考え方は、近年、IETF [6-5] や OpenConfig [6-6] などの標準化団体で積極的に議論され、具体的な標準モデルの策定が行われています。ここで登場したネットワークの「抽象化」と「モデル化」という考え方は大変重要ですが、長くなるため Appendix-A にて説明します。

図 6-4 に、モデル駆動形のオーケストレーションの概念図を示しました。

モデル化の考え方をもとにした自動化の考え方は「モデル駆動形」、「モデル ベース」などと呼ばれています。モデル化のメリットとしては次が挙げられます。

- 外部連携のための API が標準的なモデル言語 (YANG 言語) で定義されることで、システム間連携のためのインターフェイスを明確化し、個別開発する労力を削減可能
- モデルが同じならば、ソフトウェア アップグレードなどで内部の構成が変わっても外部には影響を与えないため、システムの疎結合性・メンテナンス性が向上する
- 下位のオーケストレータのサービス モデルを上位のオーケストレータが取り込むことが容易なため、オーケストレータの階層化によりクロス ドメインの自動化を実現するのに適している

これらのポイントは、いずれもエンドツーエンド オーケストレーションを構築するうえで重要と言えます。ドメインごとの自動化を検討する場合、オーケストレータにモデル ベースのものを採用することで、エンドツーエンドの自動化にも容易に対応できます。スモール スタートが可能で、かつエンドツーエンドを見据えたアーキテクチャとして、モデル ベースの自動化は有力な選択肢と言えるでしょう。

6.5 まとめ: エンドツーエンドでの自動化がもたらすメリット

本章では、5G に向けてのインフラ アーキテクチャの変革トレンドから、運用上の課題を浮かび上がり、その解決には自動化が必要であることを見てきました。そして、自動化にあたって必要なソフトウェア スタック、そして重要な抽象化とモデル化の考え方について述べてきました。

ここまで読んでいただいた方は、もしかしたら、自動化は必要となるコンポーネントも、考慮すべき要件も非常に多く、大変な取り組みになると感じられたかもしれません。そこで、こうした自動化の取り組みに、労力とコストに見合う価値があるかどうかを最後に考えてみましょう。

エンドツーエンドでのネットワーク自動化が実現したあかつきには、通信事業者に次のようなメリットをもたらすと考えられます。

- API が各レイヤ・各ドメインでオープンになることにより：
  - プログラム的な手法による運用の進化、API の公開による柔軟な新サービスが創出できる可能性 (NaaS; Network as a Service)
  - API 連携の企業ユースケースの発掘により新たな収益源を創出できる可能性
- 最先端のアプリケーション開発・運用手法を取り込むことにより：
  - CI/CD (Continuous Integration/Continuous Deployment) の手法、デプロイ自動化ツール群の取り入れによる開発・運用の進化、進化したソフトウェア テスト手法の採用による省人化・品質向上および信頼性向上
  - 生産性の向上、技術部門の働き方改革を実現
- 大量のデータの分析により：
  - ML/AI 手法を用いた分析により経験知や人手に頼らない分析と運用が可能に
- ソフトウェア スキルの活用により:
  - ネットワーク業界においてもソフトウェア スキルで可能な開発やオペレーションが増加し、高度な IT 人材をひきつけることで企業および業界全体の価値の向上、さらなる投資やブレークスルーへの期待

これらは想像できる多くのメリットの一部にすぎませんが、このような理想とするアーキテクチャや自動化の姿をネットワーク業界全体で共有して議論していくことが、いま求められていると言えないでしょうか。昨今、通信業界では、ユーザが低コスト・高品質・迅速なサービスを求め、競合が次々と参入する厳しいビジネス環境が続いています。そうした中で、本章で議論したような 5G によるシステム アーキテクチャの変革に伴う自動化の実現が必要になる日がすでに訪れています。本章の内容が皆様の取り組みの一助になれば幸いです。

Appendix A: ネットワークの抽象化とモデル化

抽象化とは、あるドメインを外から見たときに、ドメイン内部の不要な情報がきちんと隠蔽され、必要な情報にアクセスするインターフェイス (API; Application Programming Interface) のみが公開されていることを意味します。これは、ドメインが独立して正常に動作することを担保し、外部からドメインに対する不当な変更や情報取得を防ぐために重要な考え方です。

一方で、モデル化とは、ドメインが持つ機能をわかりやすい設計図にすることを意味します。身近な喩えとして車のプラモデルを考えてみてください。本物の車が持つ細かい性質、たとえばエンジンの内部構造や配線等は捨象して、特徴がわかるような外見や骨格、色合い等を取り出したものになっています。それと同じように、ネットワーク ドメインでは物理配線や機器の種別、ルーティングのパラメータなどの細かい部分は無視し、外から見て意味がある情報 (顧客識別 ID や拠点のネットワーク情報、SLA など) を切り出すことを指します。

モデル化には、モデルを記述するための適切な言語が必要です。モデル化のための言語として IETF で定義されたのが YANG [6-7] (RFC 7950) です。

モデルは、抽象化する対象に応じて oo モデルという形で呼ばれます。

サービス モデルという場合、たとえば VPN サービスのように外部の法人顧客から見たときに、意味がある情報を記述することになります。物理配線や機器の種別、ルーティングの内部パラメータは、法人顧客にとっては意味がないので捨象されます。一方、顧客識別 ID や拠点のネットワーク情報は重要なのでサービス モデルに含まれ、外部からのプロビジョニング対象として公開されることになります。

デバイス モデルという言葉もあります。これはネットワーク デバイスの OS 設定項目を構造化・パラメータ化したものです。たとえばルータで BGP を設定するコマンドは、OS によって、

router bgp 65000

だったり、ブラケット付きの

{ routing { protocol bgp { as-number id 65000 } } }

だったりと違いがあります。デバイス モデルは、こうした文法上の構造の違いも含めて、そのデバ

イスの設定情報を構造化された形で記述したものと言うことができます。

一方で、上記のような文法の違いは、ユーザからしてみれば意味のある違いではありません。そこで、サービス モデルでは設定として重要な情報である“bgp”と“65000”のみをパラメータとし、デバイス モデルの差分は自動的に吸収・変換されるような仕組みがモデル ベースのオーケストレータには実装されています。

用語集

CI/CD (Continuous Integration/Continuous Deployment): 継続的なソフトウェアの開発とデプロイメントのサイクル

CNF: Cloud Native Function または Container Network Function の略、コンテナ化された NF

MANO (Management and Orchestration): ETSI NFV で定義された管理ソフトウェア群

ML/AI (Machine Learning/Artificial Intelligence): 機械学習とそれを利用して自動的な判断・処理を行う人工知能に相当する機能を指す

NF (Network Function): ルータやモバイルコアなどネットワーク装置

NFVO (NFV Orchestrator): ETSI NFV で定義された管理ソフトウェアコンポーネントの 1 つ

OpenConfig: ベンダー非依存なネットワーク管理手法を志向しテレメトリを始めとするさまざまな手法やモデルを定義するワーキンググループ

SLA Service Level Agreement): ここではユーザ企業と通信事業者の間で交わされるサービスレベルを合意した契約

UPF (User Plane Function): 5G モバイルコアネットワークにおいてユーザプレーン処理に特化した機能を提供

VNF (Virtual Network Function): 仮想化されたネットワーク機能部

VNFM (Virtual Network Function Manager): ETSI NFV で定義された管理ソフトウェアコンポーネントの 1 つ

VRF (Virtual Routing and Forwarding): ルータ内に独立した仮想ルーティングテーブルを保持するシステム

5G/Hetnet の企業向け活用

河野 美也

7.1 背景

企業や公共団体などの産業界は、デジタル時代に向けて、高性能高品質でセキュアな新たなアクセス方式に大きく期待しています。通信事業者としても、コンシューマーサービスにおいてはユーザ数/ARPU に大きな増加が見込まれないため、企業や、スマートヘルス、スマートシティ、コネクテッドカー、その他 IoT システムなどの新たなサービス需要に対して真に価値のあるサービスを提供することが、5G 投資への論拠となります。

また、最近日本においても、全国用の周波数帯域に加えてローカル用の周波数帯域を割り付けるローカル 5G/プライベート LTE の導入が決定されました。これにより、通信事業者以外の企業や第三者機関がモバイルサービスを運営可能になります。一方、Wi-Fi も進化を遂げました。新規格 Wi-Fi6 (IEEE 802.1ax) により、従来の EDCA/CSMA との後方互換性を持たせながらも OFDMA を導入し、衝突や非決定性の問題を回避することが可能になります (第 1 章参照) 。

さらに、用途によっては、低スループットではあるが安価・省電力でライセンス不必要の LPWA が適する場合もあるでしょう。つまり、利用する企業側からすると、表 7-1 のように、アクセス手段やサービス形態が多様化し、多様な可能性と選択肢が提供されることになります。このため、本章のタイトルを「5G の企業向け活用」でなく、アクセス手段の多様化という意味を込めて「5G/Hetnet の企業向け活用」にしました。

企業の情報システム環境も大きく変わっています。複数のクラウドサービスの利用が当然となり、また、固定の配線を最少化するのは勿論、場所にかかわらず、移動中であっても、システムを効率よく安全に利用できることが必須になっています (図 7-1-1) 。

表 7-1 アクセス手段とサービス形態の多様化

ライセンス形態	Licensed/Unlicensed
カバレージ	Indoor/Outdoor、 Macro/Micro
通信方式	Cellular/Wi-Fi/LPWA
サービス種別	Public/Private
システムの運営 (所有と管理)	SP-Managed/3rd party Managed/Enterprise Managed

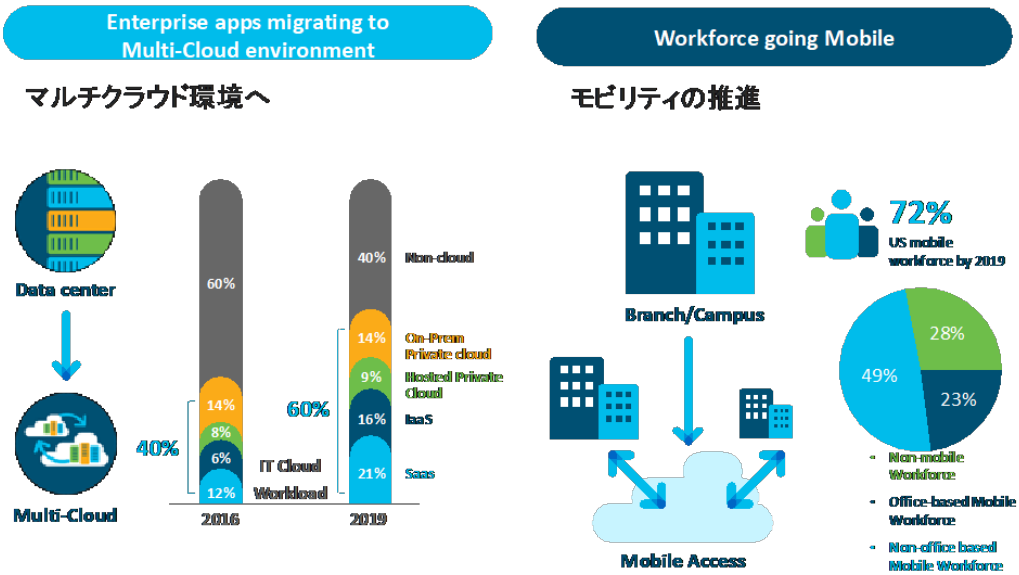


図 7-1-1 企業環境の変化

そのために企業は、通信事業者が提供するモバイルサービスを利用しますが、これまでのサービスは接続性の提供に留まり、企業のポリシーやセキュリティ指針を統合し活用するようなモバイルサービスの提供はできていませんでした（図 7-1-2）。

シスコでは、これまで多くの企業ネットワークシステムを手がけてきた経験から、これからの時代における、価値の高いモバイルサービスを模索しています。いかに簡単に、シンプルに、セキュアに、ポリシー一貫性やプライバシーを保ちながら、魅力的なサービスを提供するか。本章では、Cisco が提供しようとしている、5G/Hetnet 時代の企業向けソリューションのいくつかを紹介します。

7.2 多様なサービス形態の融合

アプリケーションシステムにおいては、すでにパブリック システムとプライベート システムの融合が進みつつあります。社内システムを使っているつもりでも、機能によって複数のパブリック クラウドの IaaS や SaaS が組み合わされ、企業のクレデンシャルでそのままシステムが使えるようになっていることも多いと思います。しかしネットワークシステムにおいては、パブリック システム である通信事業者のモバイルサービスは単なるコネクティヴィティの 1 つに過ぎず、認証もポリシーも全く別であることが殆どです。

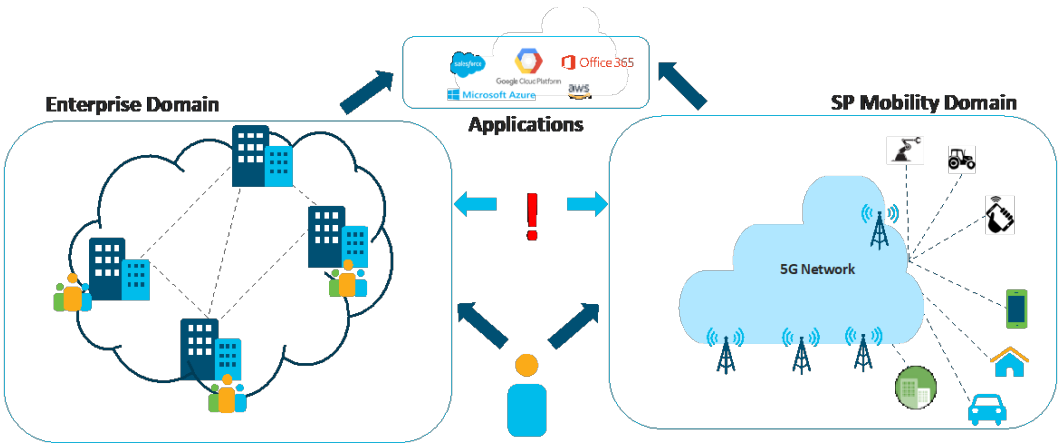


図 7-1-2 現状：企業システムと通信事業者のシステムは別物

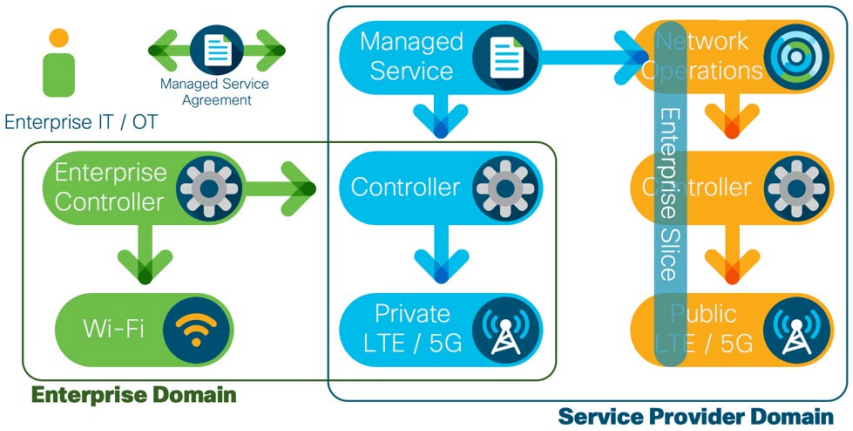


図 7-2-1 企業システムと通信事業者システム融合の例

今後のネットワークシステムは、単にパブリック システムとプライベート システムだけでなく、前項で見たような多様なサービス形態が融合するものと考えられます。図 7-2-1 に一例を示します。

この図では、オレンジが通信事業者システム、グリーンが企業側システム、ブルーは通信事業者が Local 5G システムをマネージメント サービスとして企業に提供している例を示しています。通信事業者設備は、ネットワーク スライシングとして仮想専用網的に提供されています（ネットワーク スライシングに関しては、第 5 章もご参照ください）。勿論これは一例であり、「ローカル 5G は導入せず通信事業者の提供するネットワーク スライシングのみを利用する」、「ローカル 5G システムを、通信事業者ではなく、企業または第三者機関が所有・提供する」などの可能性もあります。

28 GHz 帯のローカル 5G を利用して CATV における放送配信のラストワンマイルを代替するという取り組みも報道され[7-1]、5G FWA (Fixed Wireless Access) の可能性も高まります。このように、多様なサービス形態が融合するため、これまでとは異なる、新たなセキュリティやポリシーに対する考え方、新たな責任分界の考え方が必要になります。

図 7-2-2 に、セキュリティ・ポリシー融合の例について概念図を示します。

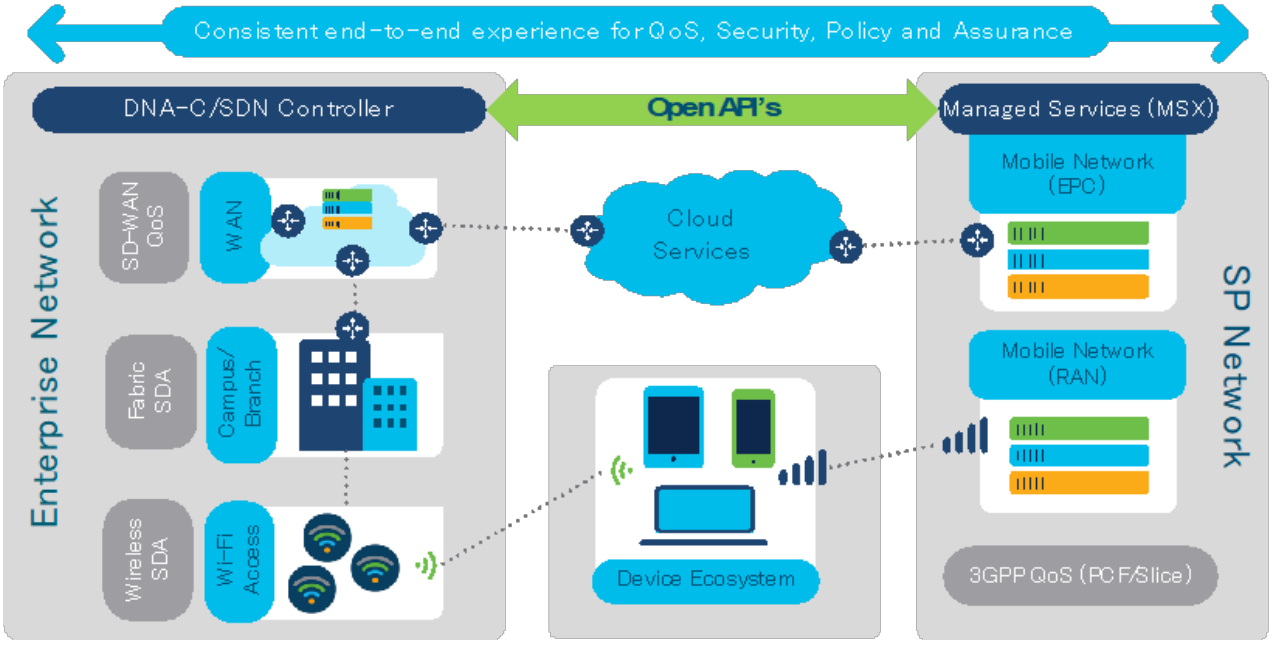


図 7-2-2 企業システムと通信事業者システムにおけるセキュリティ・ポリシーの一貫性

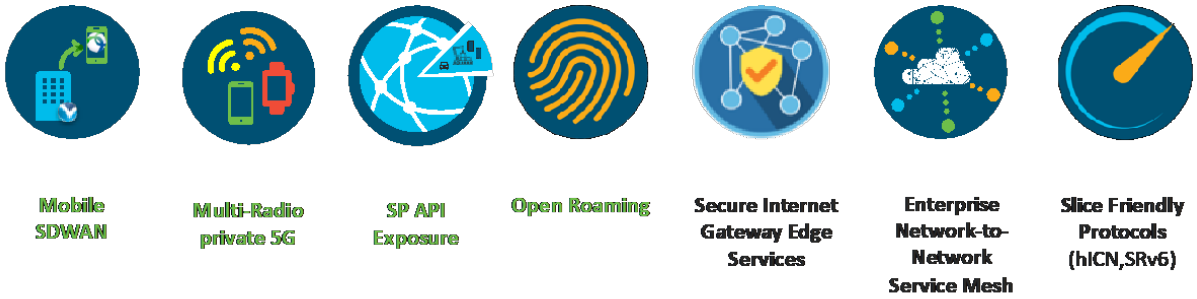


図 7-3-1 Hetnet/5G for Enterprise – Seven Technology Pillars

これまでは、企業ネットワークシステムと通信事業者のシステムはそれぞれ別物であることが殆どでした。しかし、企業や産業システムにおいてモバイルが主流になり、Private LTE/Local 5G のようなサービスが登場し、また通信事業者の方でも、企業・産業システム向けの Managed Service や Network Slicing を提供するようになります。

5G を始めとする多様なアクセス技術とサービスの組み合わせにより、企業や IoT など産業向けネットワークシステムの、新たな可能性が広がります。

7.3 Seven pillars

5G/Hetnet 時代の企業・産業界向けソリューションは、多くの様々な可能性があり、まだ技術も発展途上であるため、現時点で完成的で網羅的なソリューションを提示することはできません。そこでここでは、シスコが重要と考えている要素技術の可能性を Seven pillars (7 つの柱) として示します。この Seven Pillars は、社内外のカンファレンス等で限定的に発表されているものであり、開発途上の技術も含みますので、現時点 (2020 年 1 月現在) でリリース計画が保証されているものではないことをご了承ください。

7.3.1 Mobile SD-WAN

企業システムがマルチクラウド前提・モバイル前提になると、必ず企業のゲートウェイにログインし、そこからインターネットやクラウドサービスを使用する、というこれまでの方式は、効率的とは言えなくなります。アプリケーションはパブリック クラウドやエッジ クラウドに偏在しているのに、常に企業ネットワークにログインさせることは、ゲートウェイへの投資効果の面でも、遅延などユーザ経験の面でも、最適とは言えません。

しかし企業は、モバイルユーザに対しても、ポリシーの一貫性やセキュリティを提供する必要があります。モバイル SD-WAN は、この問題を解決します。

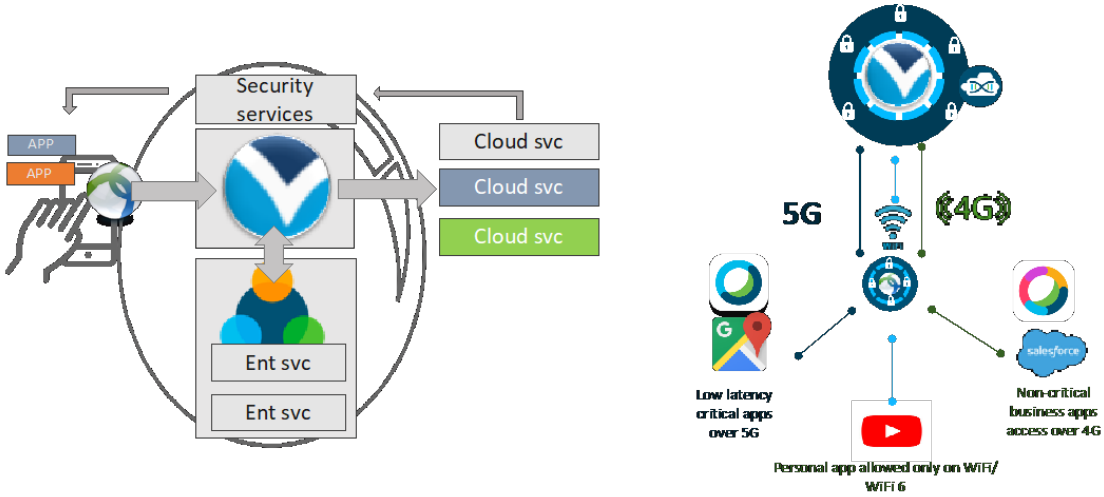


図 7-3-1-1 Mobile SD-WAN

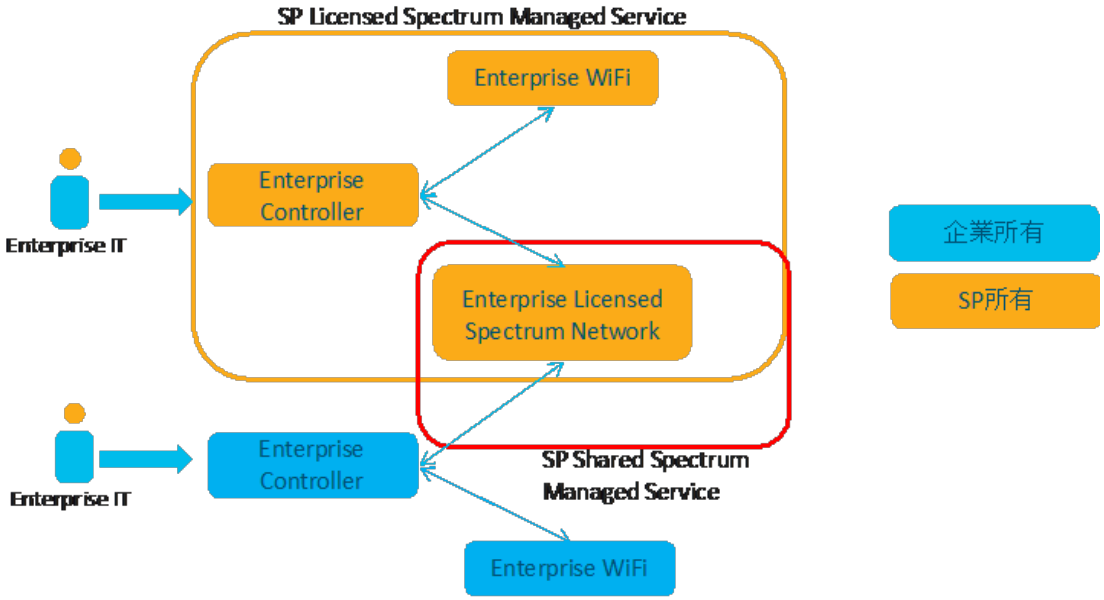


図 7-3-2-1 Multi-radio Private 5G

企業の IT 部門は、アプリケーションがサービスにアクセスするためにどのネットワークパスを使用するかを規定することが可能になります。この制御は、モバイルデバイス上に PBR エージェントを実装することにより実現します。さらに、SD-WAN Edge により、トラフィックをセグメント化します。

7.3.2 Multi-Radio Private 5G

前項で見たとおり、アクセス手段やサービス形態は多様化します。企業が所有する Wi-Fi システムと、通信事業者がマネージドサービスとして提供する Local 5G を組み合わせる、ということも考えられます（図 7-3-2-1）。シスコではこのような混在環境におけるセキュリティやポリシー連携などについて取り組んでいます。

7.3.3 SP API Exposure

第 5 章に記述したとおり、通信事業者が ネットワーク スライシングをサービスとして提供する場合、そのサービスを使っていかに優れた企業システムを構築できるかが問題です。その方法の 1 つとして、API を企業システム側に提供することが考えられます。

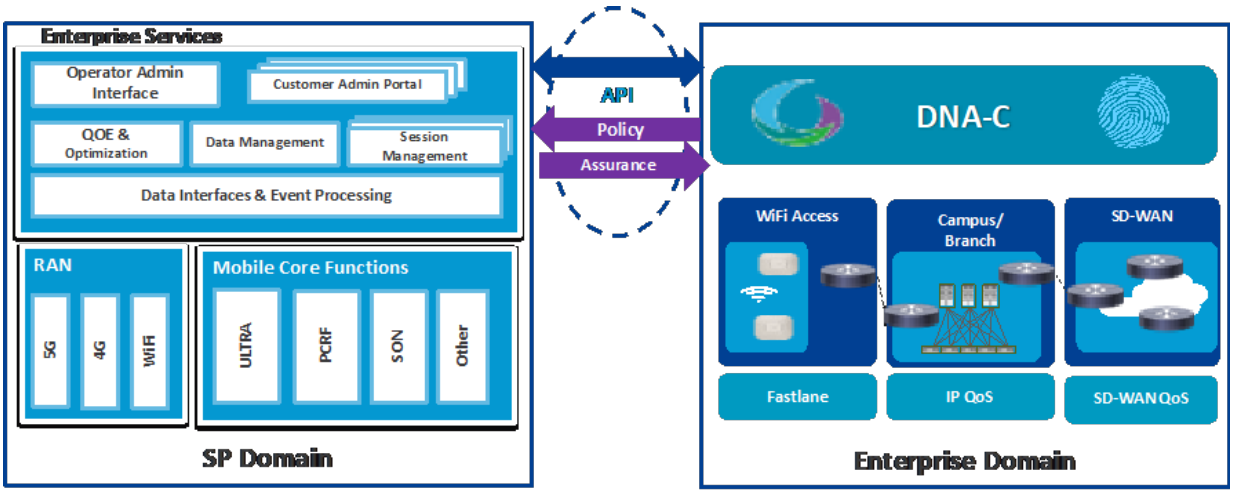


図 7-3-3-1 API による企業システムからの通信事業者システムの利用

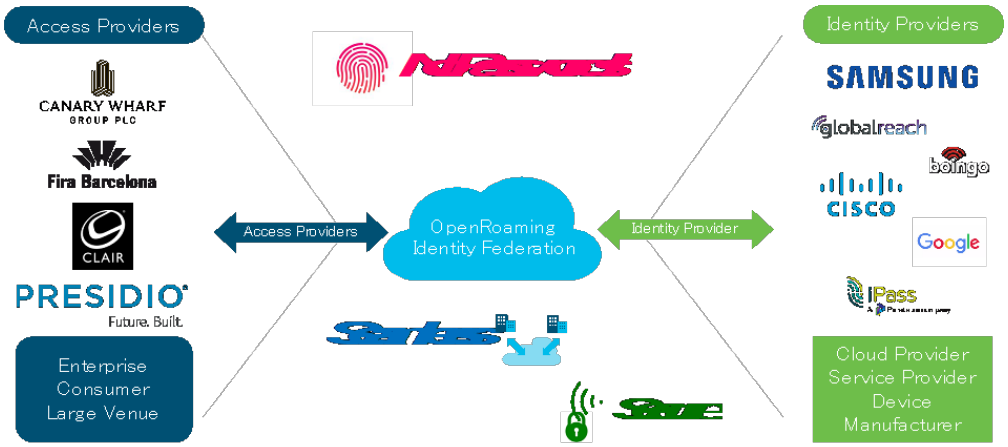


図 7-3-4-1 オープン ローミングによる ID 連携

企業は、例えば工場の自動化に際し、グループ毎に、通信品質、セキュリティ、プライバシー、信頼性の制御を求めます。その場合、通信事業者が企業向けに API を提供し、企業側から必要に応じた QoE や SLA の制御を行わせることが考えられます。それら API によって、企業向けオーケストレーション製品である DNA Center のポリシー適用と組み合わせることができれば、企業は、DNA Center が提供する IBN (Intent Based Networking) を、通信事業者ネットワークに拡張させることができるようになります。

7.3.4 Open Roaming

オープンローミングは、IEEE 802.11u に基づいた Hotspot 2.0 技術 [7-2] を拡張し、 ID 連携を実現します。オープン ローミング連合 (Federation) が成立すると、ユーザはあらゆる場所で、5G および Wi-Fi 6 ネットワークを介して、自動でシームレスかつ安全に接続できます。 オープン ローミング 連合は、通信事業者、デバイス、クラウドプロバイダーなどの ID プロバイダーと、小売業者、ホテル、大規模会場、企業キャンパスなどの Wi-Fi アクセスプロバイダーで構成され、ユーザが自動的に接続できるようにします。

オープン ローミングにより、例えば企業は従業員に場所に依存しないアクセスを提供できることになります。また通信事業者としては、5G で使用される EAP/AAA 基盤上に構築することにより、5G/private 5G 展開と整合させ、5G 価値提供の一環とすることが可能になります。

7.3.5 Secure Internet Gateway

Secure Internet Gateway (SIG) は、ユーザがどこにいても、VPN の外であっても、安全なインターネットアクセスを提供します。通常の Web Security と異なり、Open DNS (Umbrella) を活用しているため、基礎となる IP レイヤと連携させ、予見的なインテリジェンスに結びつけることができます。図 7-3-5-1 に、通常の Web Security と Secure Internet Gateway の比較を示します。

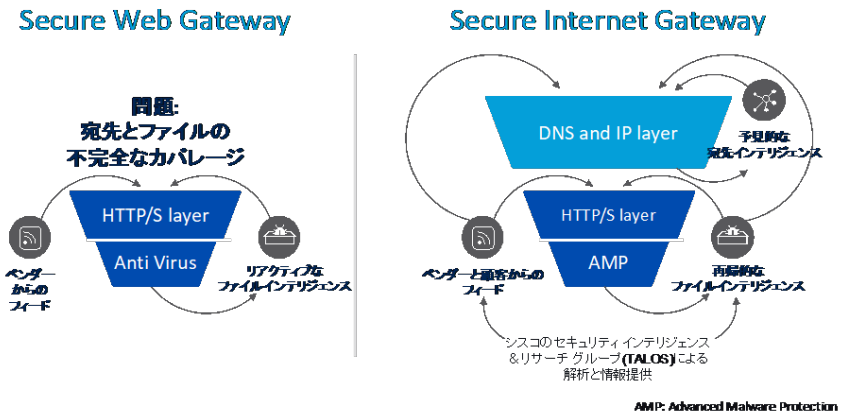


図 7-3-5-1 Secure Web Gateway vs Secure Internet Gateway

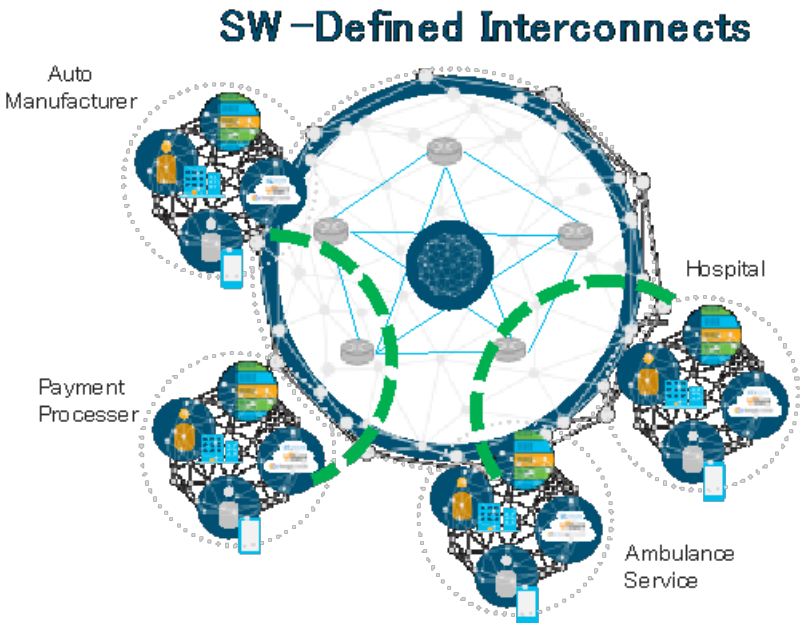


図 7-3-6-1 E-NNI: Software Defined Interconnects

7.3.6 E-NNI

E-NNI (Enterprise Network and Network Interconnection) とは、クラウドベースにフォーカスした、事業者間ネットワーク接続を意味します。現状では、SD-WAN や企業独自の VPN が個別に存在していますが、これらを相互接続させることにより、あらたな価値を提供できる可能性があります。E-NNI とは SD-WAN を相互接続させるための SD-Exchange と言えるかもしれません。

E-NNI により、高い信頼性と ID 管理性をもたせながら、さまざまなネットワークタイプ、クラウド、エンドポイントへの柔軟な接続し、異種ネットワークタイプ間の自動相互接続を可能にします (図 7-3-6-1) 。

7.3.7 Slice Friendly Protocols SRv6 and hICN

セグメント ルーティングの data plane option として MPLS と IPv6 が定義されていますが、SRv6 (Segment Routing IPv6) は、IPv6 data plane を採用したセグメント ルーティング技術です。SRv6 は、セグメント ルーティングの持つ、Fast Protection、Micro loop avoidance、SR Policy、Flex Algo、VPN 等のすべての機能 (第 2 章参照) をサポートする上に、MPLS とは異なり Native IPv6 であるため、下記の特徴を持ちます。

- アドレス空間が大きく集約もしやすいためスケールする
- サーバなどコンピュートにも実装し易い
- Network Programmability [7-3] により In Networking Computing などあらゆる用途に活用できる

hICN (Hybrid Information Centric Networking) は、IPv6 dataplane を採用した ICN 技術です。ICN は、これまでの、宛先 IP アドレスのロケーション (Where) に基づいてルーティングを行っていたパラダイムではなく、コンテント名 (What) に基づいてルーティングを行うパラダイムに変更させる、というパラダイム変革提案です。Cisco VNI の調査結果 [7-4] も示すとおり、現在のトラフィックの 8 割近くは動画転送であるにも関わらず、現在のネットワークシステムはコネクション中心であり、データやコンテンツに最適化されているとは言えない状況です。ICN は分散された Named Data をロケーションによらず pull するモデルであり、データやコンテンツに最適化されたアーキテクチャです。またコネクション非依存であるため、Anchorless Mobility、Multi Path Transport をネイティヴにサポートすることができます。

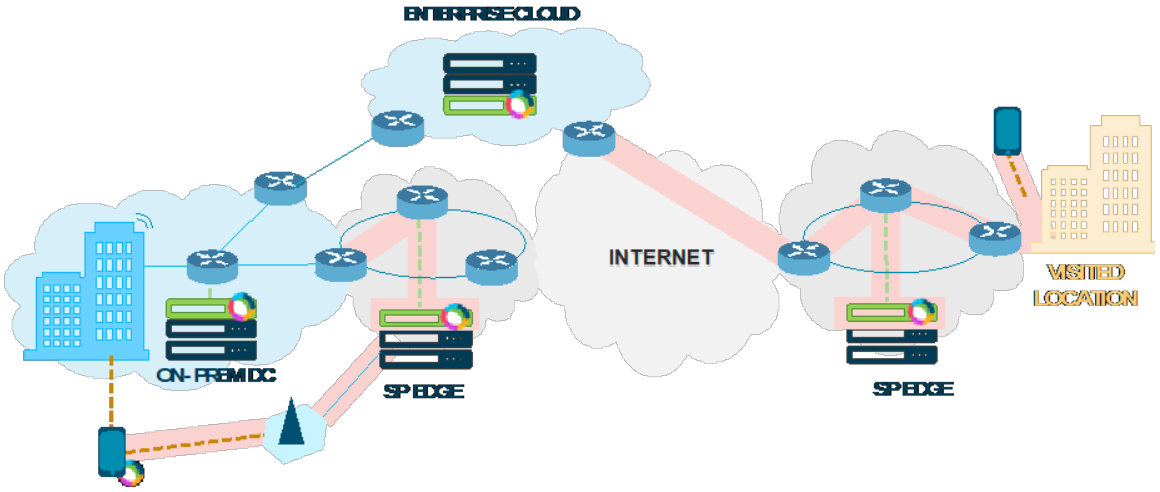


図 7-3-7-1 End-to-End Slice としての SRv6, hICN の実装

しかし、ICN のようなパラダイム変革提案を現実的に普及させることは大変困難です。そこで提案されたのが hICN [7-5] です。hICN は、Content 名の Semantics を IPv6 パケットに埋め込むことにより、ICN を実現します。ICN 非対応ノードは単に IPv6 転送するだけでよいので、共存も容易になります。また、前述の SRv6 を組み合わせることにより、SRv6 の Traffic Steering や Ti-LFA による Fast Protection などを併せて実現することも可能です。

それでも SRv6 や hICN は、既存システムからの移行が困難、と言われるかもしれません。そこで登場するのがエンドツーエンド ネットワーク スライシングのコンセプトです。第 5 章で述べたように、ネットワーク スライシングは、5G 時代のアーキテクチャ変遷可能性と捉えられます。そして、例えば hICN を 1 つのエンドツーエンド スライスとして実装する、ということにより、十分に実装の可能性が高まると考えられます。

勿論これは可能性のひとつに過ぎませんが、5G というアーキテクチャ変遷契機に、データ中心アーキテクチャ（どのようなデータをどう収集・蓄積・分析するか）にどのようにシフトするかを検討する必要があると考えます。また、いずれにせよ、少なくともこれから設計するインフラは IPv6 ベースに考えておいた方が効率は良いです（そして SRv6 は、“Slice Friendly“ というよりネットワーク スライシングの実装を可能にする技術でもあります）。

7.4 まとめ

本章では、アクセス手段やサービス形態が多様化し、多様な可能性と選択肢が提供されることになる 5G/Hetnet 時代に、どのような技術が必要になるか、どのようなシステムが実現可能になるか、という観点から、現在検討されている技術可能性について記述しました。勿論これが全てではなく、また開発途上のものも含むため、実際の展開にあたってはより深い議論が必要です。この記事が、アクセス手段やサービス形態が多様化し、データが偏在するデジタル時代に向けて、これまでとは異なるセキュリティやポリシーに対する考え方や、データ中心アーキテクチャへの検討の一助になることを願っています。

5G のサービス ユース ケース

山田 欣樹

これまでの章では、5G におけるアクセス、トランスポート、コア ネットワークおよび仮想化基盤ならびに DC ファブリックのアーキテクチャについて見てきました。同時にエンド ツー エンドのサービス基盤構築手法と自動化、5G のエンタープライズにおける可能性とそれを実現するスライシングについて見てきました。それらを踏まえて、本章では 5G における具体的なサービスのユース ケースについて紹介します。

8.1 具体的な 5G のユース ケース

日本においても 2020 年の商用サービス開始に向けて、モバイル事業者に対する周波数割り当てがすでに決まっており、モバイル事業者は 5G トライアル環境の提供を行い、パートナー（企業、団体）の参加を広く呼びかけています [8-1]。5G のトライアルにおけるユース ケースとしては、地方の人口減少や過疎化などの課題を考慮した、5G による遠隔重機操作や遠隔医療といった地域創生に関わるものが挙げられます。また、政府が推進するコンパクト シティや、Society 5.0 で掲げた第 4 次産業革命の次に来るべき超スマート社会実現に向けて、5G を活用したセンシングによる安心・安全な街づくりや、自動運転、スマート ファクトリーといった次世代の先端技術に関連するソリューションが注目されています [8-2]。

8.2 スマート シティ

現在、世界の多くの都市が人口増加、渋滞、治安悪化等の多くの課題を抱えています。一方、国連気候変動枠組条約締約国会議（COP）での環境意識の高まりにより、環境負荷を抑制しつつ成長を目指す持続的な発展が求められています。シスコでは、京都府のほか、世界の多くの都市と包括提携を結び、都市のスマート化により持続的な発展を可能にする取り組みを支援しています[8-3]。具体的には、それらの都市でセンサーを収容するための Wi-Fi/LoRaWAN/ZigBee/Cellular といったマルチアクセスの整備と、センサー デバイスから得られる情報を統合する IoT プラットフォームにより、センサーからの情報を一元的に管理し、エネルギーの効率的利用や安心・安全な街づくりといった具体的なソリューションを提案しています。

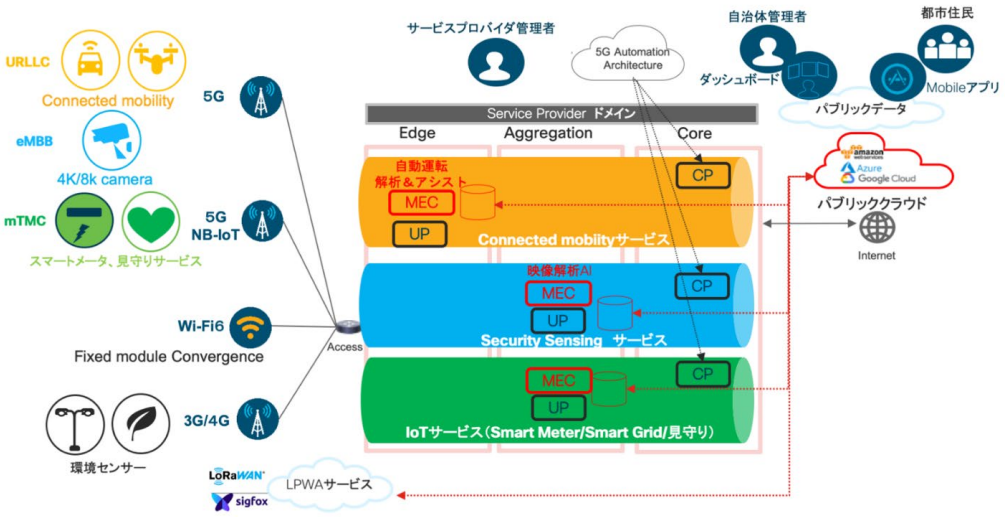


図 8-1 スマート シティのユース ケース

図 8-1 はスマート シティにおいて、都市を管理する自治体管理者がモバイル事業者と連携して、既存のアクセスと 5G を組み合わせ、都市に必要な各種 IoT サービスを実現する具体的な方法について示したものです。自治体としてのゴールは都市で得られるさまざまなセンサー情報を一元的にダッシュボードで管理運用し、分析することで、都市がよりスマートになることです。さらに、住民に有益なデータを開放し、都市生活の満足度向上や MaaS (Mobility as a Service) といった、次世代のスマート シティのコンセプトを実現していくことも視野に入れられています。

まず、都市においては通信事業者から、FTTH に代表される有線回線や Wi-Fi 無線サービス、および 3G/4G といったモバイル サービスが提供されています。都市ではモバイル端末の密度が非常に高くなるため、モバイル事業者は不感地帯の解消に向け、Wi-Fi AP と連携する Fixed Mobile Convergence を実現しているケースが多く見られます。

同時に Wi-Fi AP を外国人観光客にも開放し、観光情報を発信する代わりに、その導線分析情報を自治体に提供するサービスも多く見られます。シスコは、モバイル端末と Wi-Fi の自動的なローミング方法として OpenRoaming を提唱しています。この技術により、海外から訪日した 5G ユーザのスムーズなローミングを提供することが可能になります[8-4] 。

一方、機器、IoT サービスはすでに 3G/4G で提供されています。しかし IoT 向けの低い通信速度で、低コストなサービスが揃っていない点や、通信デバイスの消費電力が大きく駆動時間が短い点が指摘されており、用途が限定的なのが現状です。その制約を解消する手段として、LPWA (Low Power Wide Area)、LoRaWAN や Sigfox が注目されています。

LPWA は通信速度が非常に遅い一方、基地局がカバーする通信エリアが比較的広く、通信モジュールの消費電力が非常に小さいため、センサー デバイスの充電を想定することなく低コストのサービス展開が可能です。しかし、データの通信速度があまりに遅い点やデバイスの収容密度が小さい点、通信の信頼性が比較的低くベスト エフォートな面がある点が課題です。

それでは、次に 5G を活用したスマート シティに期待されるユース ケースを見ていきます。図 8-1 にあるように、5G サービスを提供するモバイル事業者により仮想化基盤が構築され、コネクテッド モビリティに適した超低遅延サービスを想定した URLLC スライス、4K/8K のセキュリティ カメラ向けの eMBB スライス、IoT サービスを想定した mMTC スライスなどが構築されてスマート シティ向けのサービスを展開することを想定しています。これらのサービスは MEC を具備しており、パブリック クラウドと連携し、サービスの最適化が実施されることも想定しています。

8.2.1 コネクテッド モビリティ

都市で人口が集中した結果、車に代表されるモビリティ サービスは慢性的に渋滞が発生しており、経済的な損失は計り知れません。一方、バス等の都市の公共交通機関は人材不足によりサービス維持が難しく、自治体でもコネクテッド モビリティに対する関心が高まっています。また大規模災害時には、遠隔操作または自立稼動の無人航空機ドローンを活用した被災者支援の活動が期待されています。図 8-1 はコネクテッド モビリティの実現方法を示しています。モバイル事業者のコネクテッド モビリティ スライスでは MEC がエッジに設置されており、低遅延での処理が可能です。自治体はコネクテッド モビリティの開発が目的ではないため、自動運転ノウハウを持つベンダーとの提携が現実的であり、パブリック クラウドとの連携で速やかなサービス展開と柔軟な運用が可能になります。

8.2.2 eMBB: 4K/8K カメラと MEC の画像解析 AI が実現する安心・安全な社会

都市では、より快適で安心・安全な環境が求められます。その実現方法として、4K/8K 監視カメラを 5G で接続し、モバイル事業者の MEC により AI 画像解析を利用して異常な振る舞いを迅速に検知し、社会の安心・安全の維持に貢献することが期待されています。

光回線の普及した日本では、すでに FTTH と 4K カメラで MEC を活用した AI 画像分析の試みが行われていますが、より俯瞰できる場所にカメラを設置する場合、5G の利便性は欠かせません。また、最新の画像圧縮技術である H.265 により、高解像度映像をより低い速度で転送することが可

能になりつつありますが、AI 画像分析の精度を上げるために、より高密度の送信フレーム レートにおいては 4G では帯域が足りず、5G が必要になります。

図 8-1 で示すように、MEC では、パブリック クラウドのコンテナ環境で事前に構築された AI 学習データとアプリケーションが、そのままモバイル事業者の環境にクラウド ネイティブでアプリケーションを展開できることは、 サービスプロバイダーにとっては管理コストの削減、自治体管理者にとってはセキュリティ コストの削減および治安維持の効果が見込めます。

また、自治体管理者にとっては、カメラの映像のプライバシーをどのようにセキュアにするかという問題も重要です。仮に 5G で大容量のストリームをクラウドまで送信できたとしても、パブリック スペースにプライバシー情報が含まれる映像をアーカイブすることが課題でした。その点、モバイル事業者の MEC の環境ではパブリック クラウドにデータをアップロードする必要がないため、コンプライアンス的にも問題ありません。

8.2.3 mTMC (5G NB IoT) が実現するスマート メーターや見守り等の IoT サービス

5G では、すでに規定され商用化されている NB-IoT (Narrow Band-IoT; 3GPP Release13 で規定) を継続して利用（Release16 で拡張）し、高密度で IoT デバイス接続が実現可能と言われています。NB-IoT は上り下りの転送速度が 100kbps 程度ですが、他の LPWA より十分大容量であるため、スマート メーターの情報も伝送可能です。加えて、他の LPWA と同様に省電力技術を導入し、単 4 電池 2 本で 10 年以上動作することが想定されています。通信モジュールのコストは他のデバイスより多少高いと考えられますが、用途によっては他の LPWA に十分対抗可能であり、IoT 通信に適した規格と言えます（注：日本国内において割り当てられている周波数帯は 3.7 GHz、4.5 GHz および 28 GHz であり、将来 IoT 接続に最適なサブ GHz 帯の導入が求められます）。

図 8-1 にあるように、5G NB-IoT のユース ケースとしては、水道、ガス、電気の各種スマート メーターの管理が挙げられます。スマート メーターは膨大な数が設置されており、上り下りの通信速度、広いカバー エリア、低コストで効率的に収容する手法として期待されています。これらの膨大なスマート メーターを収容する際には、アプリケーションの負荷集中とトランスポートへのトラフィック負荷を抑制するために、MEC で処理分散するのが望ましいでしょう。一部メーターは震災対策用として、下り通信によるメーター制御が考慮されているものの、処理速度は求められないため、MEC はアグリゲーションもしくはコアに配置されても十分と思われます。

8.2.4 過疎地域でのユース ケース

ここまで都市部を想定した 5G のユース ケースを見てきましたが、過疎地域での 5G のユース ケースもあります。シスコは英国において「Rural First」という過疎地域での 5G トライアル サービスを提供する取り組みのメイン スポンサーとして、5G Core と仮想化基盤でサービス スライシングを提供しています。また、パートナーとともに過疎地域での無線アクセス手法の確立、農業や牧畜 IoT センサーの活用に関するユース ケースを支援しています [8-5]。

8.3 スマート ファクトリーと製造業に対するデジタル トランスフォーメーション

日本は、製造業が国の基幹産業であり、政府が進める Society 5.0 でも工場のスマート化は大きなテーマとして議論されています。単に高度なモノ作りにとどまらず、部品メーカーを結ぶサプライチェーンや、5G モジュールを組み込んで出荷した製品のライフ サイクル全般を統括的に管理・運用することが考えられています。その結果、今後、サプライチェーンで利用が進むと考えられているブロックチェーンなど、さらなるデジタル トランスフォーメーションの進化に 5G のインフラを活用し、より柔軟に対応することが期待されています。本項ではスマート ファクトリーにおける 5G のメリットを述べるだけではなく、製造業、ここでは自動車製造企業にとって、5G がどれだけ企業のデジタル トランスフォーメーションに貢献できるかを見ていきます。

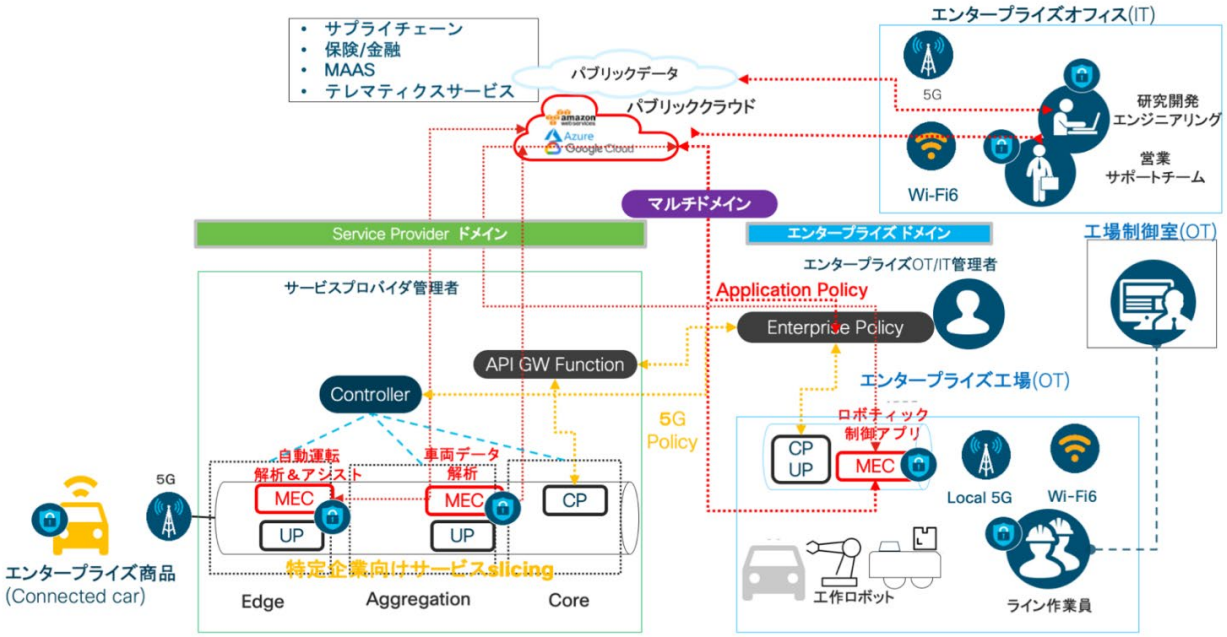


図 8-2 5G のスマート ファクトリーへの活用と製造業へのデジタル トランスフォーメーション推進

図 8-2 は、スマート ファクトリーへの活用および製造業へのデジタル トランスフォーメーション推進について示しています。右側が対象となる自動車製造ベンダーの企業ドメインになっており、一般的な IT 部署が管理するオフィスと OT (Operational Technology) 部署が管理する工場のフィールドを示しています。また、左側がモバイル サービス事業者のドメインです。ここでは協業する自動車製造ベンダー向けのスライスを作成しており、5G では商品であるコネクテッド カーや従業員の接続サービスを提供しています。これら 2 つのドメインがどのように連携し、企業側のトランスフォーメーションが推進されるかを見ていきたいと思います。

8.3.1 エンタープライズ ドメイン

工場において 5G を活用したスマート ファクトリーの事例について見ていきましょう（総務省ではローカル 5G という形で、土地所有者もしくは委託事業者による工場内限定でのサービスが議論されています。本項ではローカル 5G により工場のスマート化を実施するケースを想定しています）。

工場における情報化は、OT と呼ばれ、オフィスにおける情報化である IT とは技術やオペレーションが異なる部分もあります。たとえば OT では通信の遅延の許容時間が非常に小さく、TSN (Time Sensitive Networking) といったミッション クリティカルな通信品質が求められます。また、機器のライフ サイクルも IT 製品に比べると非常に長く、インフラの停止を極力行わないオペレーションが求められます。現在、工場内の生産ラインの工作機器は有線回線で固定されています。仮に、生産ラインを変更する場合は、工場の生産ラインをいったん停止させたあと工作機器を移動し、再度セットアップする必要がありました。工場内の無線化については以前から検討されていましたが、無線通信の遅延と信頼性が課題でした。アンライセンス帯域 (2.4/5 Ghz) の Wi-Fi では妨害電波に弱く、混信、ノイズによる干渉などが発生する可能性があるため、なかなか導入に踏み切れないのが現状でした。

一方、ライセンス帯域の 5G ではその課題は解消されます。工作機器に 5G モジュールを搭載し、複数の 5G 対応の高解像度位置センサーと連携した場合、工作機器の移動が容易で、遠隔操作で設置場所も制御できるため、生産ライン変更の際も停止時間を極力短くできる可能性があります。また、工場作業員のウェアラブル端末や、4K/8K の高解像度カメラの映像は、工場内で低遅延用にスライシングされた MEC の画像解析 AI により即座にフィードバックを送ることが可能になります。たとえば工場作業員が誤った作業をした場合、ウェアラブル端末が即座にアシスト メッセージを出して作業員の生産性を高める支援を行い、一方、

工作機器は逐一正確な部品の状態を把握することで生産ラインの不良品率の低下が期待できます。

8.3.2 マルチ ドメイン

次に、サービスプロバイダ ドメインとエンタープライズ ドメインの連携を実現するためにシスコが提唱する マルチ ドメインの役割について見ていきます (図 8-2 参照) 。シスコは製造業も含む一般的なエンタープライズ向けに、直感的なオペレーションを可能にする DNA-C (Digital Network Architecture-Center) のコンセプトを発表しました。これは、 IT 部署および OT 部署で利用する有線、および Wi-Fi から接続される PC、モバイル端末、および、すべての IoT デバイスに対して、端末レベルで認証を行い、ポリシー コントロール機能を提供します。これにより、ネットワークのセキュリティは高いレベルを保証される一方、直感的なポリシー適用を可能にし、IT 部署および OT 部署の運用コストの低減を実現しています。

シスコは、エンタープライズ事業者がモバイル サービス事業者に対して、自社のネットワーク同様、5G 環境においてもモバイル端末の一貫したセキュリティ ポリシーの適用を求めている点を考慮し、API 連携を提唱しています。例えば、5G Core のポリシー制御機能と DNA-C を API を介して連携させることにより、モバイル端末の位置情報と DNA-C からのポリシー情報を参照して、モバイル端末のコントロールを行うようなことが可能になります (詳細は第 7 章参照) 。

企業では、 IT 部署および OT 部署が業務用モバイル端末に関するガイドラインを設定しているものの、厳格な適用は難しいのが実情です。DNA-C を活用すれば、工場内では業務用モバイル端末に通話のみのアプリを許可するといったガイドライン遵守も可能になります。また、IT 部署では、製品稼動時に想定した場所 (国) 以外での利用を制限したり、完成品のセンサーの設置場所や製品のアクチュエータの状態を、セキュリティを高めた状態でサポート部署にレポートすることにより、予兆交換をしたり、修理部品を事前に手配し円滑に修理を行うといった顧客満足度の向上にも貢献できる可能性があります。

8.4 まとめ

本章では 5G サービスのユース ケースについて、スマート シティとスマート ファクトリーについて具体的な事例を紹介しました。5G のアーキテクチャはモバイルサービス事業者にネットワーク インフラの柔軟性を提供すると同時に、MEC による低遅延通信やデータの分散処理を実現し、スマート シティを推進する自治体や、工場のスマート化を進める企業のデジタル トランスフォーメーションの推進をもたらすことが期待されています。

一方、5G がすべての IT および OT の問題を解決できるわけではないため、モバイル サービス事業者は、ユース ケースの検討、導入を進める際に、顧客の既存ビジネスとネットワークを理解したうえで 5G の有効性を具体的なソリューションとして提案する必要性があります。

これを実現するには、多くの IT および OT、またデジタル トランスフォーメーションを熟知するソリューション パートナーが必要であり、シスコとソリューション パートナーはその一角として参加し、活躍できることを期待しています。

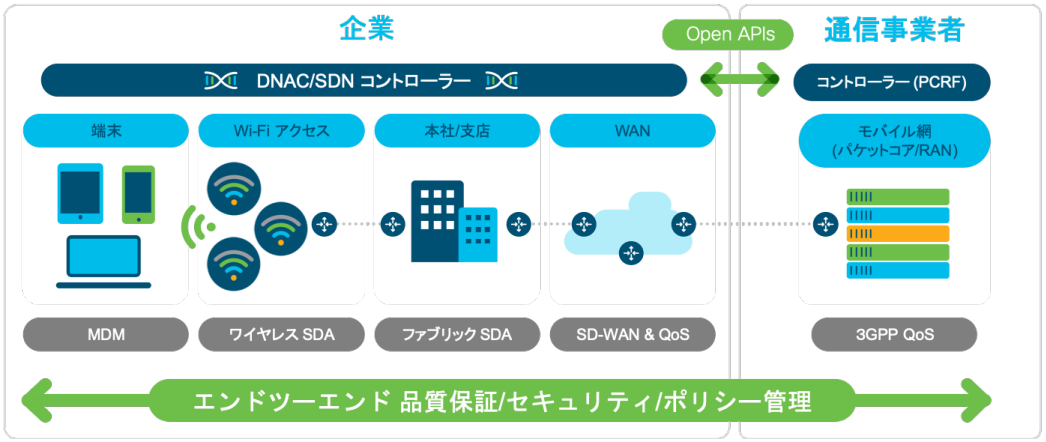


図 8-3 企業ネットワークとモバイル網の融合

用語集

CP: Control Plane

IT: Information Technology

IoT (Internet of Things): あらゆる物がインターネットに接続されるネットワークの仕組み

MDM: Mobile Device Management

MEC (Multi-access Edge Computing): ネットワーク内のエッジ（物理的に UE [User Equipment] 寄りの位置）に計算機リソースを用意して各種処理を行うシステム、概念のこと

OT: Operational Technology

SDA: Software-Defined Access

UP: User Plane

5G 時代のトラスト サイバーセキュリティ

河野 美也

9.1 背景

5G 時代、我々はサイバーセキュリティへの考え方を変えるべきでしょうか。5G に限らず、新しい技術を導入するときは、必ず新たなセキュリティリスクを想定すべきです。したがって、否、5G といえども特別ではない、という考えも一理あります。

一方、日本を始めとする各国政府や EU は、5G をデジタル社会および経済のバックボーンと捉え、セキュリティリスクに備えるための声明を出しています［9-1］［9-2］。また、第 5 章でも述べたとおり、5G というモバイルネットワークにおける世代進化は、単なる Radio 技術の進化ではなく、ネットワークシステムアーキテクチャ全体に関わる大きな変遷契機であり、時期を同じくして、SDN・プログラマビリティ、仮想化・クラウドネイティブ、自動化、機械学習、IoT Platform、エッジコンピューティング、オープン・ディスアグリゲーションなどの技術進化が起こっています。

各所で取り上げられる「トラスト」という言葉の意味自体も変化しています。

デジタルトランスフォーメーション渦中の今こそ、5G インフラを構築する通信事業者は勿論のこと、5G 時代のネットワークシステムを活用するすべての関係者が、サイバーリスクの特性を見直し、来たるべき課題に備える必要があるのではないでしょうか。本章では、5G 時代に必要なトラストサイバーセキュリティに関する考慮点をいくつかの観点から記述します。

9.2 「トラスト」を保証する

まず、ネットワークシステムを構成するハードウェアや OS、ソフトウェアそれぞれ自体が信頼できるものでないと、トラストの根底がゆらぎます。システムが第三者によって改ざんされたり、不正使用や誤用されることのないよう、また、万が一そのようなことが起こった場合にも直ちに検出・回復できるような仕組みが必要です。ここではそのための基礎となる概念を記述します（参考資料［9-3］）。

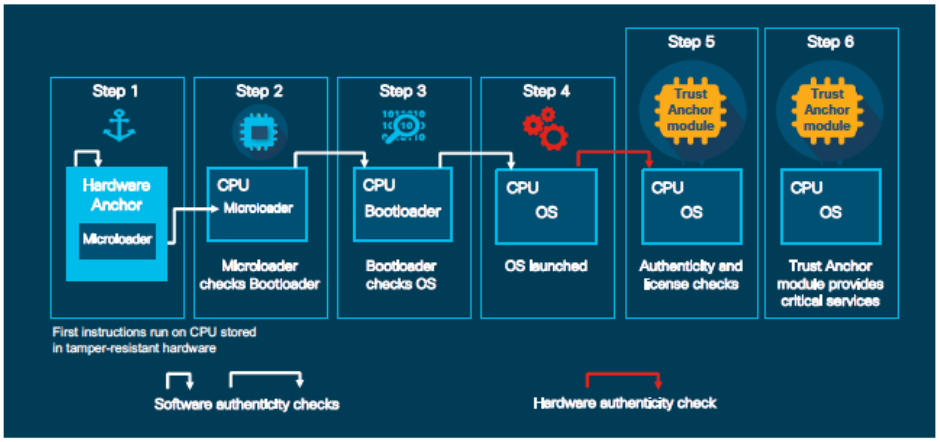


図 9-1-1 トラストのチェーン：ハードウェアとソフトウェアの整合性確認

Image Signing: イメージ署名

イメージ署名は、特定のコードブロックに対して一意のデジタル署名を作成するための 2 段階のプロセスです。最初に、チェックサムに類似したハッシュアルゴリズムを使用して、コードブロックのハッシュ値を計算します。次に、ハッシュは秘密キーで暗号化され、デジタル署名が画像に添付されて配信されます。署名されたイメージは実行時にチェックされ、ソフトウェアが変更されていないことを確認できます。

Secure Boot: セキュアブート

セキュアブートは、改ざん防止ハードウェアのマイクロローダー (ブートする最初のコード) を保護し、そのハードウェアプラットフォームで実行されるコードが本物であり、変更されていないことを確認します。

Chain of Trust: トラストのチェーン

システム上のコードが実行される前に各要素の整合性が検証されると、トラストのチェーンが生成されます。トラストのチェーンは、トラスト要素のルート (根) から始まります。トラストの根は、チェーン内の次の要素 (通常はファームウェア) を開始する前に検証します。署名および信頼された要素を使用することで、システムを安全に起動し、ソフトウェアの整合性を検証するトラストのチェーンを生成します (図 9-1-1) 。

Trust Anchor module (TAm): トラストアンカーモジュール (TAm)

TAm はシスコ独自の改ざん防止チップであり、多くのシスコ製品に内蔵されています。不揮発性セキュアストレージ、セキュアユニークデバイス識別子 (SUDI)、乱数生成 (RNG)、セキュアストレージ、キー管理などの暗号サービス、そして実行中の OS およびアプリケーションへの暗号化サービスなどを備えています。

Run-time Defences (RTD): ランタイム防御 (RTD)

ランタイム防御は、実行中のソフトウェアへの悪意のあるコードのインジェクション攻撃を標的にします。シスコのランタイム防御には、アドレス空間レイアウトランダム化 (Address Space Layout Randomization; ASLR)、組み込みオブジェクトサイズチェック (Built-in Object Size Check; BOSC)、および X スペースが含まれます。

これらは、ハードウェア、BIOS、OS、Network OS に適切に実装されます。図 9-2-1 に IOS-XR の例を示します。

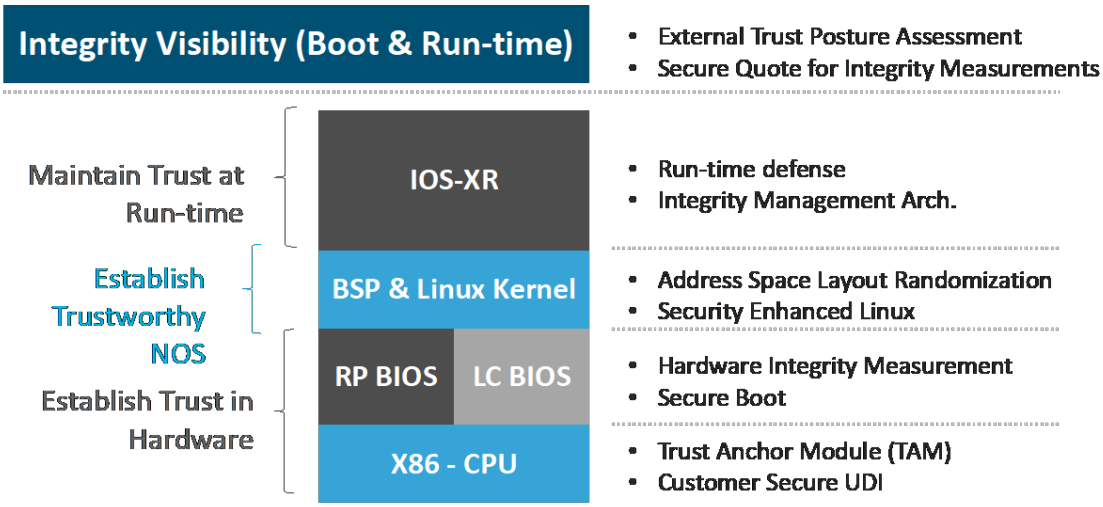


図 9-2-1 Trust Worthy Lifecycle

9.3 5G アーキテクチャとセキュリティ考慮点

本項では、5G アーキテクチャ特性に関わるセキュリティ考慮点を記述します。

9.3.1 5G インフラストラクチャへのセキュリティリスク

米業界団体である 5G Americas では、5G ネットワークに対する脅威を次のように整理しました［9-4］（2018 年 10 月）。

- 5G に関連する IoT への脅威
- Massive IoT への脅威
- UE（ユーザ端末）への脅威
- RAN への脅威（不正なベースステーション含む）
- 加入者プライバシーに関わる脅威
- コアネットワークへの脅威
- ネットワークスライシングへの脅威
- NFV と SDN への脅威
- 相互接続およびローミングに関わる脅威

また、欧州ネットワーク情報セキュリティ機関［ENISA］では、5G ネットワークに対する脅威を次のようにまとめています［9-5］（2019 年 11 月）。

- コアネットワークへの脅威
- アクセス無線ネットワークへの脅威
- エッジコンピューティングへの脅威
- 仮想システムへの脅威
- 物理インフラへの脅威
- 一般的な脅威
- SDN への脅威

このように、複数の観点からリスクを洗い出すことに加え、特に 5G インフラストラクチャのアーキテクチャ特徴である、下記のような柔軟性、オープン性、ダイナミック性に留意して、リスクを分析する必要があります。

- コアネットワークがクラウドネイティブに実装される
- サービスベースド アーキテクチャにより API が解放される
- CUPS によりコントロールプレーンとユーザプレーンが分離され、モバイルアンカーが分散配置される
- Virtual RAN、Cloud RAN により無線アクセスもフロントホール / バックホールに分離される
- ネットワークスライシングにより仮想的に複数の論理ネットワークが（自動的に）構成および実行される

これらを加味し、5G インフラストラクチャへのセキュリティリスクの可能性をまとめたものを図 9-3-1 に示します。

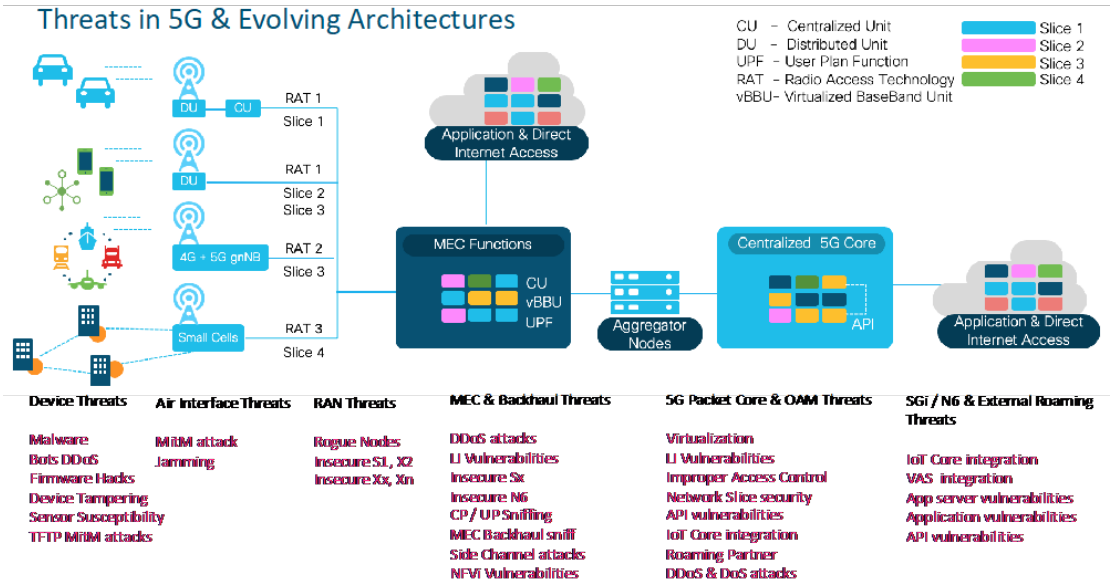


図 9-3-1 5G インフラストラクチャとセキュリティリスク（出典 ［9-6］）

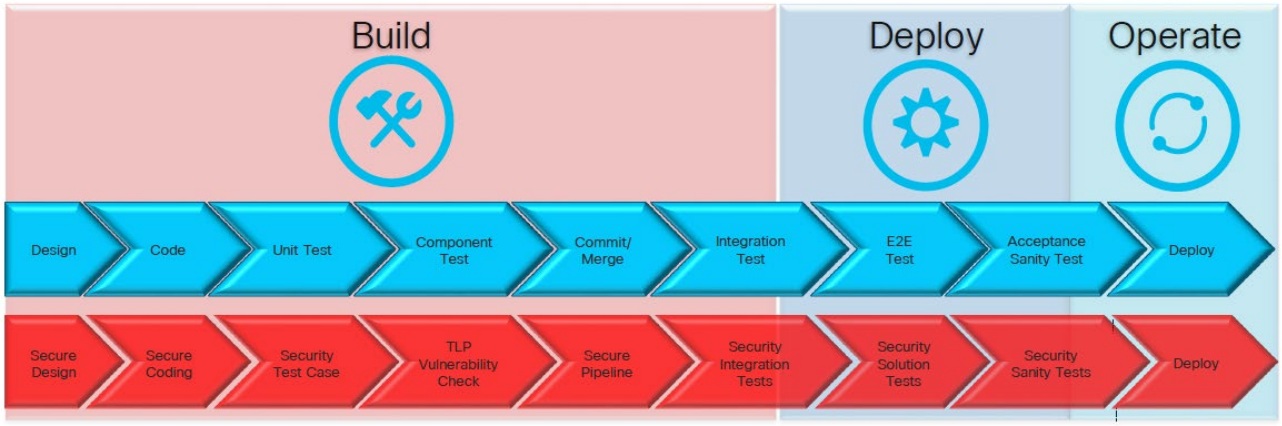


図 9-3-2 SecDevOps アプローチ (出典 [9-7])

9.3.2 Security by Design

一方、新しい実践をセキュリティ向上につなげる検討も重要です。例えば、ネットワークスライシングについては、不具合や悪意のある攻撃が発生した場合に、脆弱性をスライス内に閉じ込める、という活用方法も考えられます。また、クラウドネイティブの実践である DevOps モデルを、この機に SecDevOps モデルに発展させたり、CI/CD により、セキュリティリスクのあるソフトウェアを直ちにアップグレードして脆弱性を回避したりすることなども考えられます。最も重要なのは、セキュリティ ポリシーをシステム設計に組み込む ”Security by Design” を定着させることです。図 9-3-2 に SecDevOps のライフサイクルを示します。

9.3.3 企業システムとの融合

第 7 章、第 8 章で議論したとおり、5G 時代にはアクセス手段やサービス形態が多様化し、多様な可能性と選択肢が提供されます。企業の構内に通信事業者の管理するモバイルアンカーが分散配置されたり、企業システム側から通信事業者の提供するネットワークスライシングを制御するなど、様々な形態による、企業ネットワークシステムと通信事業者システムの相互運用・相互乗り入れが考えられます。このため、セキュリティ ポリシー統合の検討に加え、これまでとは異なる責任分界点の考え方が必要になります。

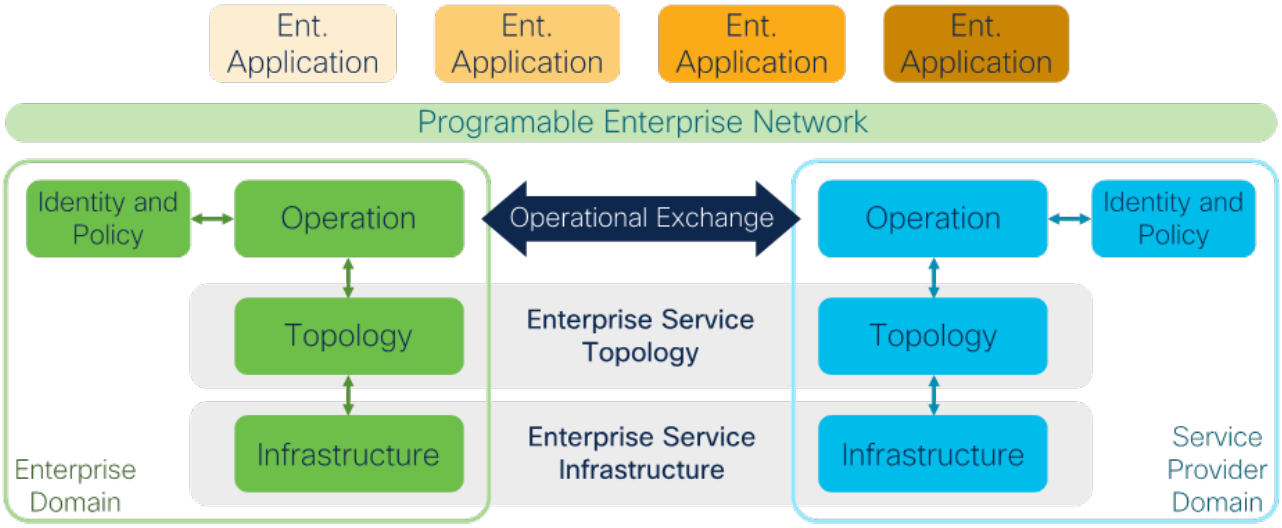


図 9-3-3 企業システムと通信事業者システムの融合

9.4 セグメンテーションと可視化

9.3 項では、考えられるセキュリティリスクを挙げました。それらのリスクに対しどのように対策するかは、それぞれの技術実装や条件により異なりますが、共通して重要なのは、セグメンテーション（適切なポリシーの設定とアクセス制御を含む)、そして可視性の提供です。

9.4.1 セグメンテーション

テナントや、そのユーザの属するグループにより、アクセスできる対象やリソースを制限するのがセグメンテーションであり、具体的には VPN/VRF、VXLAN VNI、 ACI EPG (End Point Group)、コンセプト的にはネットワークスライシングなども、このセグメンテーションに相当します。ここでは TrustSec 技術 ［9-8］ をご紹介したいと思います。

TrustSec とは、IP アドレスや VLAN ID に基づくアクセス制御ではなく、SGT (Scalable Group Tag、Security Group Tag) と呼ばれる識別子を用いることによってユーザグループや端末の属性に応じたアクセス制御を行う技術です。これにより、物理トポロジーや VLAN にかかわらず、ポリシーに基づいた柔軟なセグメンテーションを行うことができます。SGT を伝搬するプロトコルは現在 IETF において公開・標準化を行っており ［9-9］、Open Daylight などのオープンソースとの使用も可能です ［9-10］。また、ACI との統合も可能になっています ［9-11］。

さらに ISE (Identity Services Engine) により、TrustSec セキュリティ グループ タグを管理し、ネットワーク全体に一貫したポリシーを適用できるようになります。図 9-4-1 に TrustSec と ISE の動作例、図 9-4-2 に ISE の概要を示します。

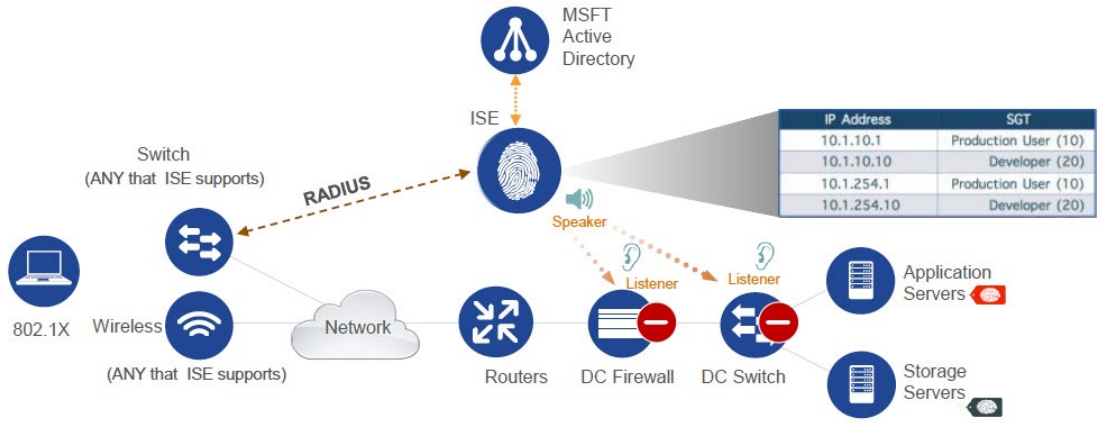


図 9-4-1 TrustSec 動作

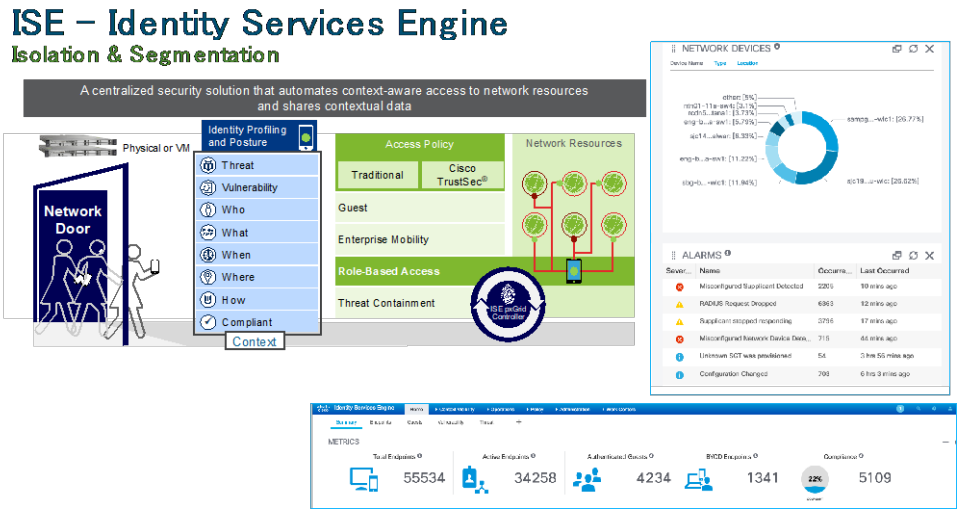


図 9-4-2 ISE 概要

TrustSec および ISE は主にエンタープライズシステムに使用されていたため、通信事業者にとってはあまり馴染みがなかったかもしれません。しかし、第 7 章で述べたとおり、5G の提供価値可能性として、企業システムと様々な形態の通信事業者サービスとの統合が挙げられます。例えば、ISE によるポリシー管理と通信事業者サービスであるネットワークスライシングを接続し、ポリシー一貫性を実現することにより、さらに価値を高めることが可能になります。

9.4.2 可視化

ネットワークシステムに何が起こっているかを把握するために、可視化が重要です。現在は暗号化されるトラフィックが増えており、Let's Encrypt の統計 [9-12] によると、2019 年には Firefox で読み込まれたページの約 80% が HTTPS となっています。このため Packet Inspection でトラフィックを解析することは無意味となり、Flow base の解析が重要視されるようになりました。ここでは Flow base の可視化・分析ツールとして、ETA (Encrypted Traffic Analysis) を紹介します。ETA はトラフィックが暗号されていても、フローの振る舞いを検知することにより、異常性を検出します。

Flow Analytic のソリューション例としては、Stealthwatch (図 9-4-4)、Tetration (図 9-4-5) などがあります。

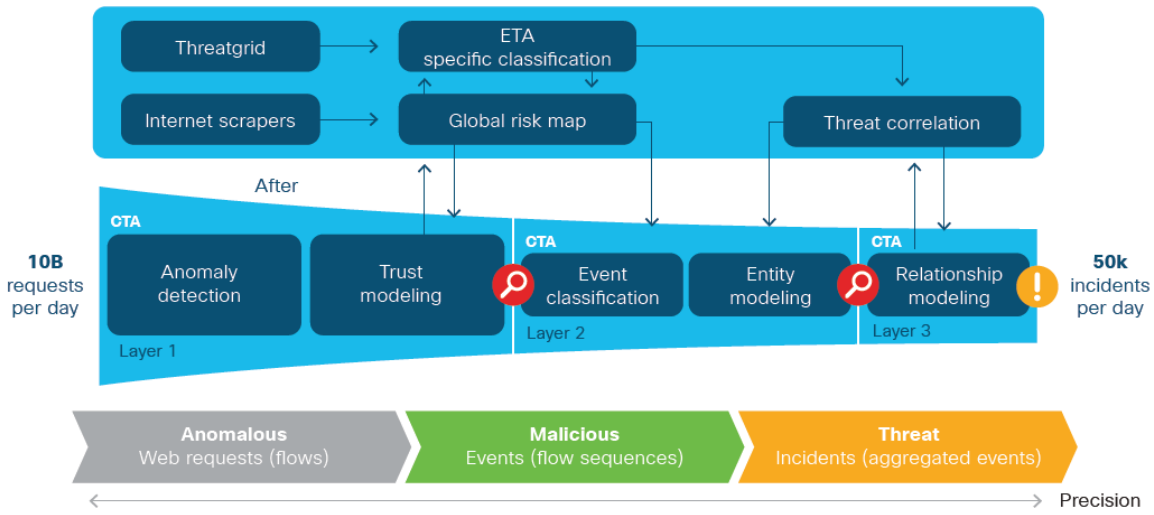


図 9-4-3 ETA (Encrypted Traffic Analysis) による異常検出

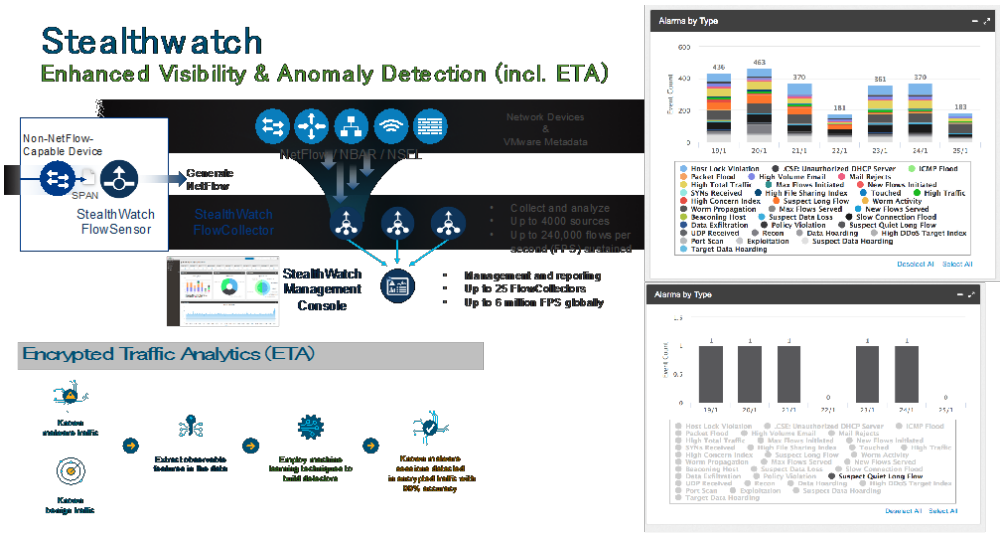


図 9-4-4 Stealthwatch

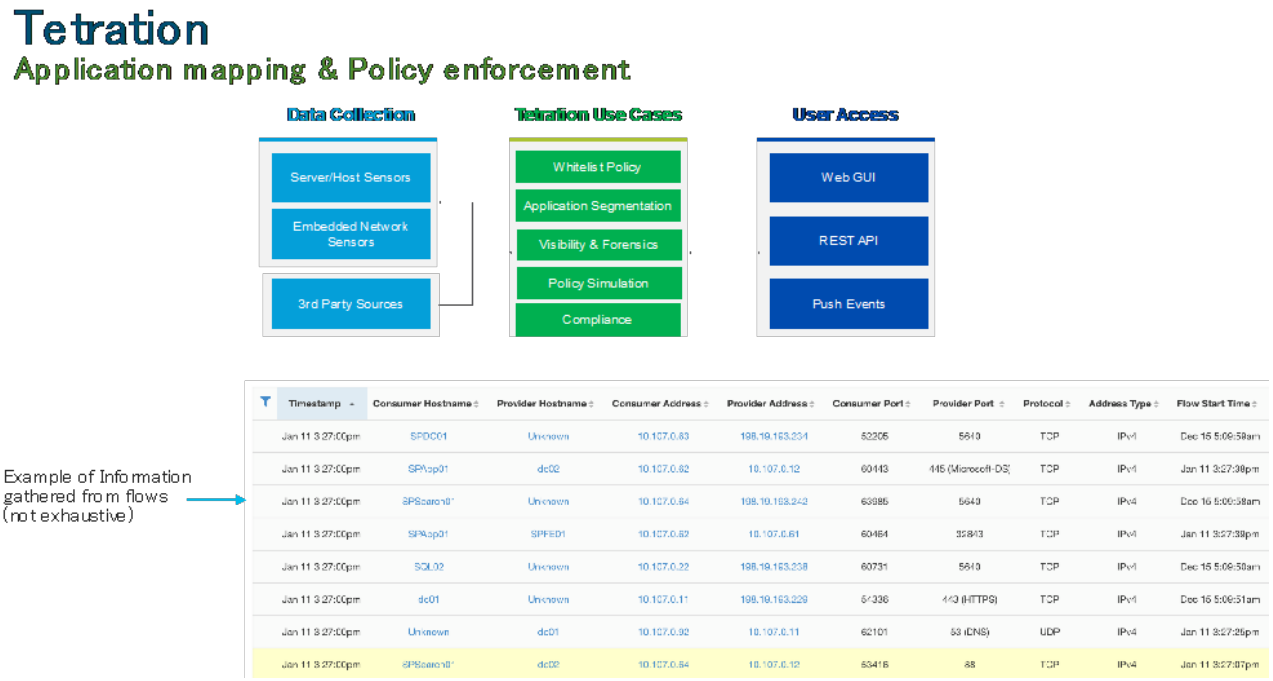


図 9-4-5 Tetration

なお、トラフィックの可視化だけでなく、9.2 項で述べたようなネットワークシステムを構成するコンポーネントの整合性についても可視化し、何らかの異常が検出されたときにアラート通知する仕組みも必要になります。

Trust Insight [9-13] は、ネットワークデバイスからハードウェアおよびソフトウェアの署名情報を集約し、ハードウェアが本物であり、実行中のソフトウェアが公開済みの既知の良好な値 (KGV; Known Good Value) にマップされているかどうかを検証するためのエビデンスを収集します。このサービスにより、シスコプラットフォームに組み込まれた信頼できるテクノロジーを最大限に活用し、運用上のベストプラクティスを実装して、システムの整合性情報の変更を収集および検証できます。

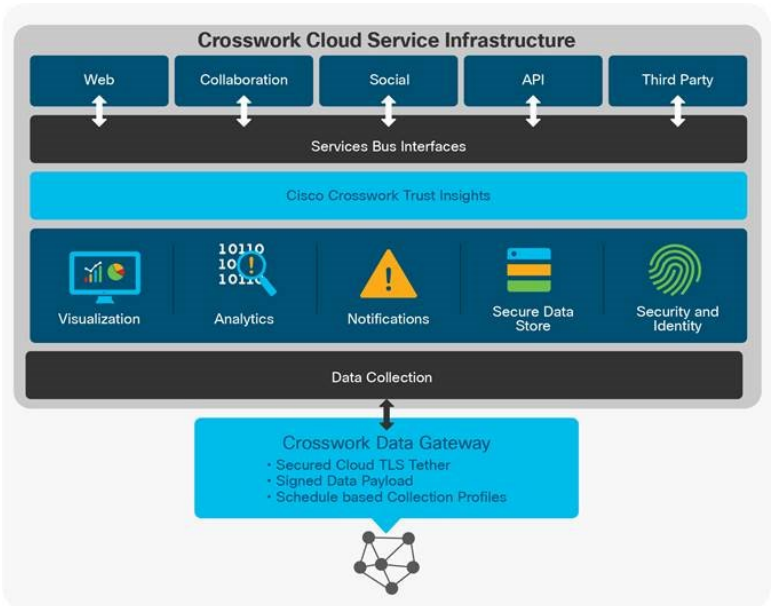


図 9-4-6 Trust Insight

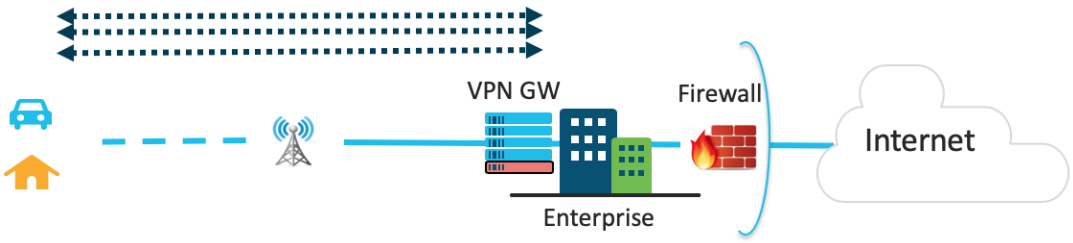


図 9-5-1 境界型セキュリティモデル

9.5 「ゼロトラスト」

ここまで、ネットワークシステムがいかに「トラスト」を保証するか、という観点で議論して来ました。しかし時代は「ゼロトラスト」です。Forrester 社のレポート「2019 年 Q4 最重要ゼロトラスト extended ecosystem プロバイダー」[9-14] で、シスコはリーダーとしてトップにランキングされています。あるときは「トラストを保証することが重要」とし、あるときは「ゼロトラスト」を標榜するのは、大いなる矛盾ではないでしょうか。

ここで注意すべきなのは、「ゼロトラスト」はセキュリティモデルを表していることです。そしてそのモデルには対の概念であるモデルが存在します。それは「境界型（perimeter）」モデルです。境界型モデルでは、ファイアウォールなどで防御壁をつくり、その防御壁で囲われた内側は安全と考えます。

現在ではモバイルが普及していますが、ユーザがどこにいても、移動中でも、企業システムにアクセスできるようにするために、境界型モデルでは、IP Sec や SSL で VPN に接続します。VPN に入ってしまえば安全、という考え方に基づいており、インターネット等外部に出る場合は、ファイアウォールを介します (図 9-5-1)。

しかし、そのモデルでは立ち往かなくなってきました。まず、”Mobile First”と言われるようにモバイルが主流になり、モバイル接続が急速に増加しているため、VPN Gateway がボトルネックになり、スケール性やコストを圧迫します。次に、マルチクラウド、分散クラウドが普及し、企業システムであっても企業内 DC に Workload があるとは限りません。SaaS の利用も増えています。その場合、必ず VPN に入るのは、トラフィックパスの観点からも非最適となります（図 9-5-2）。

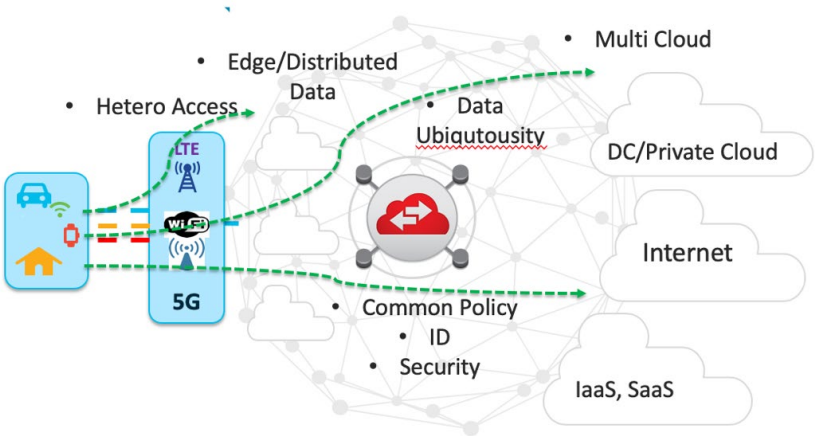


図 9-5-2 データの遍在性

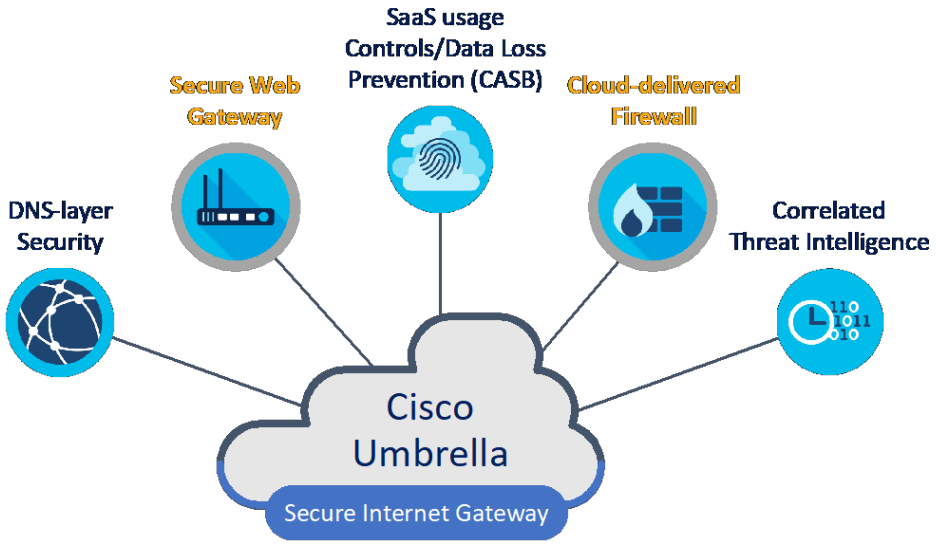


図 9-5-3 Secure Internet Gateway (SIG)

しかし、VPN に入らずにインターネットに直接接続させる、ということは、ユーザをマルウェアやランサムウェアに容易に感染させる可能性に晒すことになります。そこで、ユーザがどこにいようと VPN に入っていなくても、何も信用しない「ゼロトラスト」セキュリティモデルを適用する必要があります。

ここでは、ゼロトラストモデルを実現する代表的ソリューションとして、Secure Internet Gateway と Duo Security を紹介します。他のソリューションに関しては [9-15] もご参照ください。

Secure Internet Gateway (SIG) は、セキュア Web ゲートウェイ、DNS レイヤーセキュリティ、クラウド配信ファイアウォール、クラウドアクセスセキュリティブローカー機能、および脅威インテリジェンスを統合します [9-16] (図 9-5-3) 。SIG の Web ゲートウェイに比べた利点については、第 7 章で述べています。

Duo Security は、多要素認証 (Multi Factor Authentication; MFA) でユーザ ID を検証するソリューションです。クレデンシャルの盗難、フィッシング、およびその他の ID ベースの攻撃からユーザとそのデバイスを保護するのに役立ちます。アプリケーションへのアクセスを許可する前にユーザの ID を検証してデバイスの信頼を確立します。

図 9-5-4 Duo Security

「ゼロトラスト」モデルに基づくソリューションは、下記のメリットも提供します。

- ポリシーベースの制御を一貫して適用できる
- 環境全体のユーザ、デバイス、コンポーネントなどを可視化できる
- 詳細なログ、レポート、アラートを取得し、より的確に脅威を検出して対応できる

ネットワークシステムを構築する場合はトラストを保証することが重要ですが、一方、企業システムとユーザを保護する、という観点からは、これまでの「境界型」セキュリティモデルから、「ゼロトラスト」セキュリティモデルに移行する必要があります。

ゼロトラストは、ネットワーク、アプリケーション、および環境全体のすべてのアクセスを保護する包括的なアプローチです。ユーザ、エンドユーザデバイス、API、IoT、マイクロサービス、コンテナなどからのアクセスのセキュリティを確保し、ワークフォース、ワークロード、ワークプレイスを保護します。

9.6 まとめと謝辞

本章では 5G 時代のトラスト サイバーセキュリティに関する考慮点ついて、「トラストを保証する」、「5G アーキテクチャとセキュリティ考慮点」（前半）、「セグメンテーションと可視化」、「ゼロトラスト」（後半）という観点から記述しました。セキュリティの話題は多岐に渡り、ともすれば対症療法的になってしまいがちですが、セキュリティは奥深く、またシステムアーキテクチャと密接に関係します。5G やそれと同時に起こっている技術変化を的確に捉えて、セキュリティを設計に組み込む ”Security by Design” を実践して行きたいと考えます。

筆者はシステムアーキテクチャを専門にしていますが、セキュリティに関しては初学者です。本章の執筆にあたって Security SEVT team のメンバーの有志（瓜倉 格さん、岡本 真樹さん、大野 由貴さん、川端 奈津子さん）に貴重な助言を戴きました。この場を借りてお礼申し上げます。

参考文献

[1-1] 総務省, “第５世代移動通信システム（５Ｇ）の今と将来展望,” [online]
http://www.soumu.go.jp/main_content/000633132.pdf

[1-2] 3GPP TR 38.801: “Study on new radio access technology: Radio access architecture and interfaces”

[1-3] 安部田 貞行，新 博行:“超高速ブロードバンドサービ スを実現する無線アクセスネットワーク,” 信学会総合 大会論文集，Mar. 2012.

[1-4] Common Public Radio Interface (CPRI); Interface Specification v7.0 [Online]. Available: http://www.cpri.info/

[1-5] Common Public Radio Interface: ECPRI Interface Specification v2.0. [Online]. Available: http://www.cpri.info/

[1-6] IEEE Standard for Radio over Ethernet Encapsulations and Mappings IEEE Std 1914.3TM-2018.

[1-7] O-RAN Alliance, “O-RAN Fronthaul Control, User and Synchronization Plane Specification Version 1.0,” Mar. 2019.

[1-8] ORAN-WG4., “O-RAN Alliance Working Group 4 Management Plane Specification Version 1.0,” Mar. 2019.

[1-9] IEEE Standard 802.1CM-2018, “Time-Sensitive Networking for Fronthaul,” June 2018.

[1-10] E Khorov et al., “A Tutorial on IEEE 802.11ax High Efficiency WLANs,”
IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 1, FIRST QUARTER 2019.

[2-1] RFC 8402: “Segment Routing Architecture”

[2-2] Internet draft: “draft ietf rtgwg segment routing ti lfa”

[2-3] Internet draft: “draft ietf spring segment routing mpls

[2-4] Internet draft: “draft ietf spring srv6 network programming

[2-5] Internet draft: “draft ietf 6man segment routing header”

[2-6] Internet draft: “draft ali spring network slicing building blocks”

[2-7] Internet draft: “draft ietf spring segment routing policy”

[2-8] Internet draft: “draft ietf lsr flex algo”

[2-9] ITU T Q13/15: “Network synchronization and time distribution performance Supporting 5G mobile transport and fronthaul”

[2-10] IEEE Std 1588 2008: “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems”

[2-11] ITU T G.8272: “Timing characteristics of primary reference time clocks”

[3-1] 3GPP TS 23.501-System Architecture for the 5G System; Stage 2

[3-2] 3GPP TS 23.502-Procedures for the 5G System; Stage 2

[3-3] NTT Docomo Technical Journal-Vol25_3_003jp

[3-4] Cisco: Evolving the Mobile Core to Being Cloud Native White Paper

[3-5] Istio Community: https://istio.io

[3-6] VPP と fd.io オープンソースプロジェクト: https://wiki.fd.io

[3-7] 3GPP TS 23.501 – System Architecture for the 5G System; Stage 2

[4-1] Cisco Japan Blog, 5G - シスコが考えるサービスプロバイダー エンドツーエンド アーキテクチャ, 第 1 章: https://gblogs.cisco.com/jp/2019/11/service-provider-end-to-end-architecture-1-radio-access-in-5g-era-1/

[4-2] ETSI NFV: https://www.etsi.org/technologies/nfv

[4-3] Cisco Japan Blog, 5G - シスコが考えるサービスプロバイダー エンドツーエンド アーキテクチャ、 第 3 章: https://gblogs.cisco.com/jp/2019/12/service-provider-end-to-end-architecture-3-5g-core-cloud-native-arch-1/

[4-4] Santanu Dasgupta, Cisco Live 2019 Melbourne: https://www.ciscolive.com/global/on-demand-library.html?#/session/15482030363300015p2j

[4-5] Facebook: https://engineering.fb.com/production-engineering/introducing-data-center-fabric-the-next-generation-facebook-data-center-network/

[4-6] IETF RFC8365: https://tools.ietf.org/html/rfc8365

[4-7] Google, Google Protocol Buffers: https://developers.google.com/protocol-buffers

[4-8] IETF RFC4364: https://tools.ietf.org/html/rfc4364

[4-9] “Next Data Center Networking with SRv6,” LINE 株式会社, JANOG44 発表: https://www.janog.gr.jp/meeting/janog44/program/srv6

[4-10] ACI ポリシー理論: https://www.cisco.com/c/ja_jp/products/collateral/cloud-systems-management/aci-fabric-controller/white-paper-c11-729906.html

[4-11] ACI-mode Switches Hardware Support Matrix: https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/acihwsupport/index.html

[4-12] Cisco Network Insights for Data Center: https://www.cisco.com/c/ja_jp/support/data-center-analytics/network-insights-data-center/tsd-products-support-series-home.html

[4-13] Cisco Tetration: https://www.cisco.com/c/ja_jp/products/data-center-analytics/tetration-analytics/index.html

[4-14] IETF, RFC 3107

[4-15] Cisco ACI in Telecom Data Centers White Paper: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-740717.html

[4-16] 総務省，２０２０年の５Ｇ実現に向けた取組: https://www.soumu.go.jp/main_content/000593247.pdf

[5-1] Internet draft: “draft-ietf-lsr-flex-algo”

[5-2] 3GPP TS 23.501: “System architecture for the 5G System (5GS)”

[5-3] Digital Vortex – デジタル・ディスラプションによる諸業界の再定義: https://www.cisco.com/c/dam/m/ja_jp/offers/164/never-better/core-networking/digital_vortex.pdf

[5-4] U. Chundri et al, “Transport Network aware Mobility for 5G,” draft-clt-dmm-tn-aware-mobility

[5-5] C. Filsfils et al. “Stateless and Scalable Network Slice Identification for SRv6,” draft-filsfils-spring-srv6-stateless-slice-id

[5-6] M. Kohno et al, “Architecture Discussion on SRv6 Mobile User plane,” draft-kohno-dmm-srv6mob-arch

[5-7] https://www.ngmn.org/

[5-8] NGMN 5G whitepaper v1.0

[5-9] https://www.gsma.com/

[5-10] GSMA “An Introduction to ネットワークスライシング”

[5-11] https://www.itu.int/en/ITU-T/Pages/default.aspx

[5-12] http://netsoft2019.ieee-netsoft.org/

[5-13] https://www.opennetworking.org/

[5-14] ONF TR-526: “Applying SDN architecture to 5G slicing”

[5-15] https://datatracker.ietf.org/wg/actn/about/

[5-16] https://datatracker.ietf.org/wg/coms/about/

[5-17] draft-ietf-lsr-flex-algo

[5-18] draft-ali-spring-ネットワークスライシング-building-blocks

[5-19] MEF 3.0 & The Road to 5G

[5-20] https://sdn.ieee.org/newsletter/december-2017/ネットワークスライシング-and-3gpp-service-and-systems-aspects-sa-standard

[5-21] Report on ネットワークスライシング Support with ETSI NFV Architecture Framework

[5-22] https://www.etsi.org/newsroom/press-releases/1622-2019-07-etsi-nfv-announces-new-features-to-its-architecture-to-support-5g

[5-23] Beyond 5G 推進戦略懇談会: https://www.soumu.go.jp/main_sosiki/kenkyu/Beyond-5G/

[5-24] MEF Whitepaper “Slicing for Shared 5G fronthaul and backhaul,”: http://www.mef.net/resources/download?id=54&fileid=file1

[5-25] Broadband Forum SD-406 “End to End Network Slicing”

[5-26] “IETF Definition of Transport Slice,” draft-nsdt-teas-transport-slice-definition-03

[5-27] “Framework for Transport Network Slices,” draft-nsdt-teas-ns-framework-04

[6-1] Cisco Crosswork Network Automation: https://www.cisco.com/c/en/us/products/cloud-systems-management/crosswork-network-automation/index.html

[6-2] Telemetry: http://www.openconfig.net/projects/telemetry/

[6-3] Cisco Crosswork Situation Manager: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/datasheet-c78-740229.html

[6-4] ETSI: https://www.etsi.org/

[6-5] IETF: https://www.ietf.org/

[6-6] OpenConfig: http://openconfig.net/

[6-7] RFC7950 The YANG 1.1 Data Modeling Language: https://tools.ietf.org/html/rfc7950

[7-1] https://www.nikkei.com/article/DGXMZO47469980Y9A710C1X13000/

[7-2] Wi-Fi Alliance, Hotspot 2.0 specification: https://www.wi-fi.org/ja/discover-wi-fi/specifications

[7-3] Clarence Filsfils et al, “SRv6 Network Programming,”draft-ietf-spring-srv6-network-programming

[7-4] Cisco Visual Networking Index: https://www.cisco.com/c/ja_jp/solutions/service-provider/visual-networking-index-vni/index.html

[7-5] L. Muscariello et al, “Hybrid Information-Centric Networking,” draft-muscariello-intarea-hicn

[8-1] NTT ドコモ 5G オープンクラウド: https://www.nttdocomo.co.jp/info/news_release/2018/07/05_00.html

[8-2] Society 5.0 を支える基盤 5G: http://www.soumu.go.jp/main_sosiki/singi/chiiki_honbu/daijin_maill_03_00001.html

[8-3] 京都府とシスコの「スマートシティへの挑戦」: https://gblogs.cisco.com/jp/2016/10/cisco-dispatched-06-challenge-to-smart-city/

[8-4] OpenRoaming: Automatic and Seamless Roaming Across Wi-Fi 6 and 5G: https://blogs.cisco.com/wireless/openroaming-seamless-across-wi-fi-6-and-5g?oid=psten016624

[8-5] Rural First -Connecting the UK beyond the city: https://www.cisco.com/c/m/en_uk/innovation/projects/5g-rural-first.html

[9-1] EU 「5G ネットワークセキュリティ」: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

[9-2] 総務省「IoT/5G セキュリティ総合対策」: https://www.soumu.go.jp/main_content/000630364.pdf

[9-3] Cisco Trustworthy Technology Data Sheet: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trustworthy-technologies-datasheet.pdf

[9-4] 5G Americas, “5G Americas 5G Security Whitepaper”: https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_5G_Security_White_Paper_Final.pdf

[9-5] 欧州ネットワーク情報セキュリティ機関 「5G ネットワークへの脅威」: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[9-6] Michael Gellar and Pramod Nair, “5G Security Innovation with Cisco”

[9-7] Scott Ryan Cisco Live 2019, “Secure your enterprise apps,” BRKCLD-2431

[9-8] Cisco Trust Sec 「ソフトウェア定義型セグメンテーション」：
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/trustsec/index.html?dtid=osoblg000513

[9-9] draft-smith-kandula-sxp-09

[9-10] https://docs.opendaylight.org/en/stable-oxygen/user-guide/sxp-user-guide.html

[9-11] Cisco TrustSec and ACI Integration:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-16-7/sec-usr-cts-xe-16-7-book/cts-aci-intgn.html

[9-12] https://letsencrypt.org/ja/stats/#percent-pageloads

[9-13] https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/datasheet-c78-741972.html

[9-14] Forrester “Zero Trust eXtended Ecosystem Platform Providers, Q4 2019“:
https://www.forrester.com/report/The+Forrester+Wave+Zero+Trust+eXtended+Ecosystem+Platform+Providers+Q4+2019/-/E-RES146875

[9-15] Cisco ゼロトラストセキュリティ: https://www.cisco.com/c/ja_jp/products/security/zero-trust.html

[9-16] https://learn-umbrella.cisco.com/technical-papers/sig-white-paper

執筆者一覧

第 2 版刊行にあたって	高橋 寛嗣
はじめに	山田 欣樹
第 1 章 5G 時代の無線アクセス	大槻 暢朗
第 2 章 5G におけるトランスポートテクノロジー	鎌田 徹平
第 3 章 5G コアのクラウドネイティブアーキテクチャ	尚 軍
第 4 章 5G 時代のデータセンターファブリックアーキテクチャ	佐々木 俊輔
第 5 章 5G 時代のエンドツーエンド ネットワークスライシング	丸山 和宏/河野 美也
第 6 章 5G 時代のエンドツーエンド オーケストレーション	佐々木 俊輔
第 7 章 5G/Hetnet の企業向け活用	河野 美也
第 8 章 5G のサービスユースケース	山田 欣樹
第 9 章 5G 時代のトラスト サイバーセキュリティ	河野 美也

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

2155-2010-000-A