ローカル５Ｇ交換設備等共用のための
技術的手引

2023 年 3 月

目次

第１部：ローカル５Ｇ導入を検討するユーザ企業に向けた手引

第１章　ローカル５Ｇの動向とコア共用

第２章　コア共用の効果について

第３章　コア共用の実用モデル例

第２部：導入企業等を支援する SIer 等に向けた手引

第４章　ネットワーク類型

第５章　類型別の性能要件

第６章　類型別の機能要件

第７章　類型別のセキュリティ要件

第８章　類型別の運用要件

第９章　類型別のコスト評価

1. 背景及び目的

- 第５世代移動通信システム（５Ｇ）は、超高速・超低遅延・多数同時接続といった特長を有しており、我が国の経済成長に不可欠な Society 5.0 を支える基幹インフラとして、様々な産業分野での活用が期待されています。

- ５Ｇの中でも、令和元年 12 月 24 日に制度化されたローカル５Ｇは、企業や自治体等の様々な主体が自らの建物や敷地内で柔軟にネットワークを構築できることから、様々な分野における課題の解決や新たな価値の創造への活用、デジタルトランスフォーメーションの推進等にも寄与することが期待されています。

- 全国の様々な業界・団体でローカル５Ｇへの期待や導入希望が高まる中、ローカル５Ｇシステム構築に係る設備の低廉化は市場原理に基づき進むものの、中小企業等をはじめとする民間企業や自治体等の各団体が個別で導入するには依然、導入・運用のための費用等が課題になっており、これらの状況の打破に向けては、ローカル５Ｇシステムの異ベンダー組合せによる柔軟な機器構成の実現（以下、「相互接続」）とローカル５Ｇ交換設備を共用できる仕組みの確立（以下、「コア共用」）が望まれます。

- このような仕組みは、同一ユーザ内の他、産業集積エリアなど複数の異なるユーザ間や、特定の業種においてサプライチェーンを構成する企業グループ間で共用形態を運用するなど、柔軟なネットワークを実現し、ローカル５Ｇの最適な活用に寄与すると考えられます。

2. 本技術的手引の位置づけ・意義

- コアを共用する仕組みに関しては、ローカル５Ｇの無線設備を運用する上での課題やそのノウハウを導入検討事業主体が取り入れ、システム構築をしやすい環境を整備することが肝要です。

- 加えて、地域の拠点や本社等の中央管理拠点へのコア機能の配置や、その他既存の IT システム・通信ネットワーク（企業 WAN・LAN 等）と連携し、一体的に管理することで全体最適化を図り、経済合理性を高める必要性があります。コアの共用は、こうした最適化の一環で必然性の高い運用方法としてニーズが高まっています。

- 例えば、工場でのローカル５Ｇの導入など、複雑かつ高い要件が求められるユースケースにおいては、ネットワーク構成のみならず、ネットワークの心臓部を担う交換設備（コアネットワーク）の個々の機能群においてより高度な実装が求められます。具体的には、監視や認証といった管理機能の在り方、アプリケーション毎に柔軟なネットワーク構成を実現するためのポリシー制御など、より高度なコア共用形態の実装を目指す必要があります。

- さらに、今後コア共用形態が浸透するにつれて、同一ユーザ内の他、産業集積エリアなど、複数の異なるユーザ間や、特定の業種におけるサプライチェーンを構成する企業グループ間で、共用形態を運用するニーズが顕在化することが予想されます。

- 上記の点から、本技術的手引は、設備面・技術面・運用面等からコア共用の実現に向けて、今後ローカル５Ｇシステムの導入を検討する企業やそれを支援する SIer 向けに参照頂くことを目的としています。

- なお、異なるユーザ間でコアを共用することで生じる相互接続性を担保するための技術的手引については「相互接続のための技術的手引」を参照ください。

3. 本手引書の概要

本技術的手引は 2 部構成となっており、第 1 部はローカル５Ｇ導入を検討するユーザ企業等向けの手引、第 2 部はユーザ企業等を支援する SIer 等向けの手引となります。それぞれの概要は、以下のとおりです。

第１部：ローカル５Ｇ導入を検討するユーザ企業等に向けた手引

ローカル５Ｇの導入を検討されているユーザ企業等向けに、コア共用の位置づけ等について説明します。各章の概要は以下のとおりです。

- 第 1 章「ローカル５Ｇの動向とコア共用」では、ローカル５Ｇの特徴、ローカル５Ｇネットワークを構成する各要素や各要素間のインターフェース、国際標準化動向との関係等について説明します。
- 第 2 章「コア共用の効果について」では、コア共用の定義及び目的と狙いについて説明し、コア共用の具体的な効果等について説明します。
- 第 3 章「コア共用の実装モデル例」では、コア共用の主な目的やユースケースの類型・モデル、目的やユースケースの類型・モデル毎の例示、各実装モデルのメリット・デメリット、コア共用の費用感等について説明します。

第２部：ユーザ企業等を支援する SIer 等に向けた手引

ローカル５Ｇの導入企業等を支援する SIer 等がコア共用のシステム構築を実現するための具体的な要件等について説明します。各章の概要は以下のとおりです。

- 第 4 章「ネットワーク類型」では、コア共用のネットワーク類型の概要について説明します。
- 第 5 章「類型別の性能要件」では、共用構成において各種伝送性能や性能比較検証結果を整理し、満たす性能要件等について説明します。
- 第 6 章「類型別の機能要件」では、共用構成において機能検証結果を整理し、満たす機能要件等について説明します。
- 第 7 章「類型別のセキュリティ要件」では、共用構成においてセキュリティ検証結果を整理し、満たす機能要件等について説明します。
- 第 8 章「類型別の運用要件」では、共用構成におけるローカル５Ｇシステム運用時の留意点、改善方策の取り方など実例等について説明します。

1. ローカル５Ｇの整備・運用の特徴、公衆網との違い

- ローカル５Ｇは、企業や自治体等の様々な主体が自らの建物や敷地内で柔軟にネットワークを構築できることから、様々な分野における課題の解決や新たな価値の創造への活用、デジタルトランスフォーメーションの推進等にも寄与することが期待されています。ローカル５Ｇは、28GHz 帯（ミリ波）に加えて 4.6GHz-4.9GHz 帯（Sub6）においても利用が可能となる等、ローカル５Ｇの導入・利活用が更に活発化していくことが見込まれています。

- ローカル５Ｇは、自らの建物や敷地内で、柔軟にネットワークを構築できる５Ｇネットワークです。特に、高速・大容量、低遅延、多数同時接続といった５Ｇの特徴を活かし、高精細映像を活用したソリューション（リアルタイム映像伝送による遠隔監視・巡視点検、遠隔作業支援・指導、AI による画像解析）やモビリティの遠隔制御等で活用が期待されています。

- ローカル５Ｇは、キャリア網と比較して、規模を確保し経済合理性を高めることが期待できないため、普及展開に向けては、需要と供給のバランスが成立するモデルを先行的に打ち出していくことが肝要です。

- キャリア５Ｇでは、携帯電話事業者がエリア整備を行いますが、ローカル５Ｇでは建物や土地の所有者または所有者より依頼を受けた者が独自に５Ｇ環境を構築することができます。したがって、実現したい時期やユースケース・要件等にあわせて、柔軟にネットワークを構築できます。

表 1-1-1　キャリア５Ｇとローカル５Ｇの比較

	キャリア５Ｇ	ローカル５Ｇ
使用エリア	日本全国	地方自治体や企業、団体などの建物または土地内といった限定エリア
サービス提供者	携帯電話事業者	建物や土地の所有者 また、所有者より依頼を受けた者
主な用途	全国向けの通信サービス	限定エリア向けの通信サービス
周波数帯	3.7GHz帯、4.5GHz帯 28GHz帯	4.7GHz帯（4.6～4.9GHz） 28GHz帯（28.2～29.1GHz）

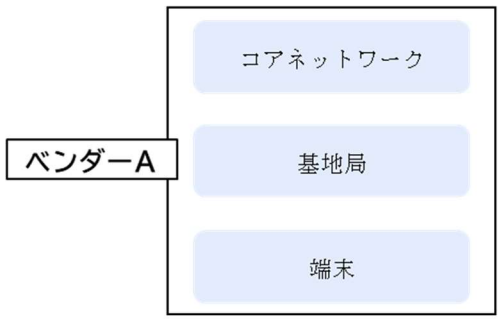
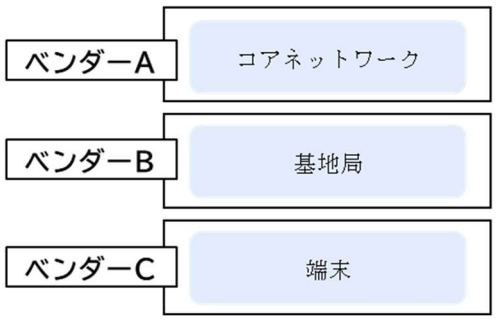
- ローカル５Ｇの特長の１つに、準同期運用があります。これは、キャリア５Ｇなどの同期運用しているシステムと基本的な無線通信のタイミングを揃えつつ、同期システムがダウンリンク通信に使用している時間帯の一部をアップリンク通信に使用することで、同期運用への影響を最小限に抑えてアップリンク通信の割合を増やす方式です。アップリンク通信の割合を増やすことは、アップリンク通信の速度が増すことにつながります。これにより、ローカル５Ｇでは、より多様なユースケースに対応できることが期待されています。

- ローカル５Ｇには、大手通信機器ベンダー等による垂直統合（以下「垂直統合」：１つのベンダー等がネットワーク装置の各機能をすべて提供するケース）と、マルチベンダーによる相互

接続（以下「相互接続：複数のベンダー等がネットワーク装置の各機能をそれぞれ提供するケース）の２つのケースがあります。垂直統合は、接続が保証された機器をシステムもしくはサービスとしてベンダー等から提供を受けるものです。これに対し相互接続は、ユーザ企業がユースケースや要件に合わせてカスタマイズする必要がありますが、より柔軟かつ拡張性の高いネットワークを構築することができます。

- 相互接続性を担保するための技術的手引については「相互接続のための技術的手引」に示していますが、コア共用にあたっても前提となる考え方であるため、こちらでも概要を説明しています。

表 1-1-2　ローカル５Ｇの提供形態例

	垂直統合	相互接続
概要	1つのベンダー等が各機能をすべて提供	複数のベンダー等が各機能をそれぞれ提供
イメージ図		

2. 異ベンダーの機器毎の性能特性、ユーザニーズ・要件に応じた構築の重要性

５Ｇ／ローカル５Ｇの製品は、多様なベンダーが独自の技術等で製品の差別化を図っていることから機器毎に特徴がありますが、留意しなければならない点として以下が挙げられます。

① ５Ｇは製品によって性能が異なる

- ５Ｇは、高速大容量、低遅延、多数同時接続を満たす移動体通信システムとして性能要件がグローバル標準として定められています。具体的には、携帯電話システムの国際標準団体である3GPP[1]が、ITU-R（国際電気通信連合　無線通信部門）が定める５Ｇの技術性能要件を満たすための技術仕様について標準化を実施しています。
- 世界中のベンダー等が、この標準化された性能要件を満たす５Ｇ機器を開発・生産しています。しかしながら、各ベンダーは、５Ｇ製品の市場への投入にあたって 3GPP 標準の策定を待つ必要はなく、独自の規格で製品を開発し、それを売り出すこともあります。3GPP の標準化に沿う場合は、仕様策定後に技術検証等を経て、一般的に 1～2 年後に製品が市場へ投入されます。どの時点(リリース)の仕様に沿うかによって、製品の性能も異なるため、同じ５Ｇ製品でも規格が異なるものが併存している状態になります。
- また、重要なのは、3GPP が国際標準化した規格であっても、ベンダー独自の規格であっても、ITU-R が定める５Ｇの技術性能要件（高速大容量・超低遅延・多数同時接続のいずれか）を満たしていれば「５Ｇ」と呼ばれる点です。そのため、５Ｇであっても、異なる規格や性能を具備した機器が存在します。こうしたベンダーの製品化方針や技術力の違い等に起因して、実際にはベンダーや製品ごとに性能は大きく異なります。

② 異なる５Ｇは製品同士がつながらない場合がある

- 上述した国際標準においては、異なるベンダーの製品間で相互運用を可能とするための統一規格として、製品間で通信を確立するためのインターフェースが標準化されています。そのため、５Ｇ技術を具備したローカル５Ｇシステムを構成する各機器については、異なるベンダー間においても相互接続で利用できる仕様となっています。これにより、ユーザ企業や SIer（システムインテグレータ）等はそれぞれの要件に適した性能の機器を組み合わせてローカル５Ｇシステムを構築することが可能となります。
- しかしながら、国際標準規格に準拠した機器同士であっても、相互接続が不能となる、あるいは接続が安定しないといった組み合わせが存在することが確認されています。このように、現時点では異なるベンダーを組み合わせたローカル５Ｇシステムの構築にはリスクが伴います。これにより、ローカル５Ｇ機器は結果的にベンダーロックインの構図となっているのが実情です。
- ユーザの所要性能や予算に応じた最適なローカル５Ｇ環境を導入するためには、コア設備や基地局等を異なるベンダーから選定できることが極めて重要です。そのため、ユーザ企業から、機器の標準化やマルチベンダー環境の構築に対する期待が高まっています。

[1] 3rd Generation Partnership Project の略。移動体通信システムの仕様の規格策定を行う国際的な標準化団体であり、３Ｇの規格策定以降、４Ｇ(LTE)、５Ｇの標準化も行っています。

3. ローカル 5G ネットワークを構成する各要素の定義

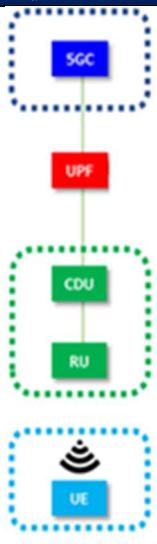
- ローカル５Ｇのネットワークは下表のとおり、コアネットワーク、基地局、端末の３つの要素に分けることができます。

- コアネットワークとは、交換機及び加入者情報管理装置などで構成されるネットワークの総称です。基地局及び端末を収容する装置として、ユーザセッションの確立やユーザデータの転送処理などを行います。

- 基地局は、その役割によって３つに分けることができます。
  ・CU：主にデータ処理を行います。
  ・DU：主に無線信号処理を行います。
  ・RU：送受信されるデジタル信号の無線周波数変換や電力の増幅を担います。

- 端末は、ローカル５Ｇと直接通信を行う専用端末（ルータやスマートフォン等）です。

表 1-3-1　ローカル５Ｇネットワークの通信機器の概要と接続イメージ

分類	名称	説明	接続イメージ
コアネットワーク	5GC	5th Generation Core network の略。 UE 認証・制御処理やユーザデータのルーティング（通信経路設定）等の基幹統制を行う設備	
	UPF	User Plane Function の略。 ローカル５Ｇと外部ネットワークの間でユーザデータの送受信を行うゲートウェイ機能	
基地局	CU/DU	CU：Central Unit、DU：Distributed Unit の略。 無線信号処理機能。無線アクセスネットワークにおける集約ノード機能（CU）と分散ノード機能（DU）。	
	RU	Radio Unit の略。 無線装置（無線送受信機）	
端末	UE	User Equipment の略。 ローカル５Ｇと直接通信を行う専用端末。	

- ５Ｇのコアネットワークの主要な機能群は C-Plane と U-Plane に分かれます。C-Plane は通信の確立などに係る一連の制御機能、U-Plane とはユーザデータの送受信処理を指します。５Ｇでは、この C-Plane と U-Plane を分離し、後者を担う装置である UPF を例えば基地局側やユーザ側に物理的に設置することができます。

- これにより、C-Plane に接続せずに、U-Plane のデータ伝送をインターネット回線などデータ通信網へ接続することができます。ユーザにとっては、その分の回線コストを抑えることができます。

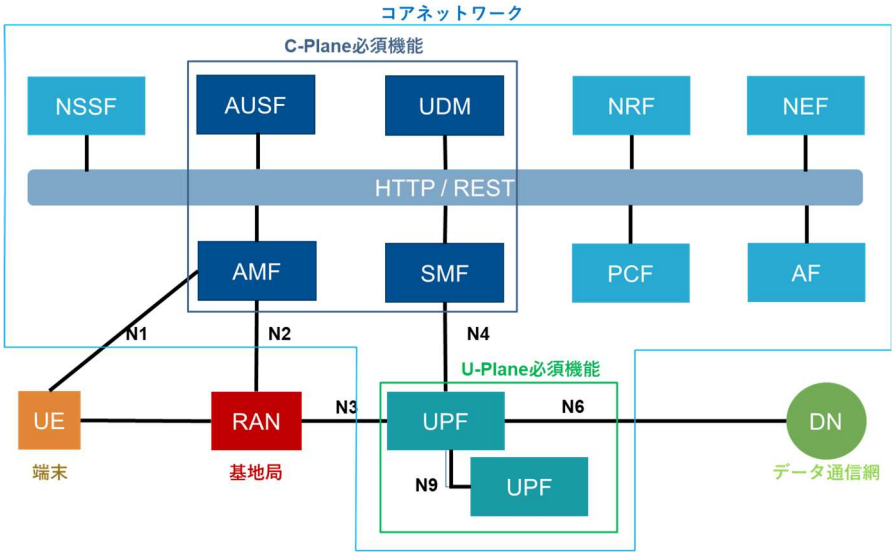


図 1-3-1　５Ｇのネットワークの構成

表 1-3-2　５Ｇのネットワークの構成要素の説明

種別	略	機能概要
AMF	Access and Mobility management Function	モビリティ管理機能（無線の制御、ハンドオーバなどの移動制御等)
SMF	Session Management Function	セッション管理機能（端末のアドレス管理等）
UDM	Unified Data Management	加入者情報データ管理・処理機能（加入者の管理、SIM の制御等）
AUSF	AUthentication Sever Function	認証処理機能（SIM の認証等）
UPF	User Plane Function	ユーザデータ処理機能（データトラヒックの制御等）
PCF	Policy Control Function	QoS および課金のためのポリシー制御機能（ポリシーの管理、QoS や課金管理等）
NSSF	Network Slice Selection Function	ネットワークスライスの選択機能
NRF	Network Repository Function	ネットワークサービス管理・検索機能
NEF	Network Exposure Function	各 NF のサービスを公開する機能（コアの外部向け API 等）
AF	Application Function	外部アプリケーション機能、トラヒック制御や監視・解析機能等

- ５Ｇでは 1 台の端末が複数の UPF に同時に接続することができます。例えば、大容量が求められるアプリケーションと低遅延が求められるアプリケーションのように、性能要件が異なる複数のアプリケーションごとに UPF を分けることが可能になります。このように、異なる性能要件に対応してネットワークを分ける技術を「ネットワークスライシング」と称し、各要件に対応したネットワークの断面を「ネットワークスライス」と呼びます。

- 前述の例では、低遅延アプリケーション用のネットワークスライスは、基地局に地理的に近い位置に UPF を配置し、他のアプリケーションによる輻輳状況などに影響されないように設計することも可能になります。

- このように、コアの上位の機能を共用しながら複数の UPF を分散配置することで、異なる要件のアプリケーションを同一の端末に対して提供することが可能になります。これがコア共用を実現する技術的な特徴です。

- 従来のハードウェアベースの監視運用から、ソフトウェアベースの性能面も加味した監視運用が求められています。相互接続性等は 3GPP などの国際標準において規定されている部分はあるものの、ベンダー実装に依存することは明らかであることから、複数のコアネットワークや基地局のシェアリング等、いわゆる共用を実現するアーキテクチャを考えるうえで、実現すべき機能の優先順位付けが重要となっています。

4. 3GPP/O-RAN などの標準化動向

５Ｇに係る標準化の動向と前項で説明したネットワーク要素やインターフェースとの対応関係について概説します。

①　５Ｇの標準化の特徴

- 移動体システムの標準化においては、周波数、無線技術、通信手順や信号インターフェースなどを統一化する取組みが行われています。５Ｇにおいては基地局をはじめとするネットワークの構成等について、４Ｇから大きく進化させるための標準化がなされています。

- ４Ｇでは、基地局は「電波を制御する装置(RRH)」と「信号を処理する装置(BBU)」に物理的に分けた構成となっており、その間の通信路を規定するインターフェース(CPRI)が規定されていました。しかしながら同インターフェースが十分に標準化されていなかったことから、各ベンダーが独自に規定していました。そのため、異なるベンダーが提供する RRH や BBU を相互に接続することが困難でした。また、CRPI はアンテナの数に比例して必要帯域が増加するという特性があったため、４Ｇ と比較してアンテナの数が大幅に増加する５Ｇでは対処が難しいという課題が生じました。

- このような背景の下、５Ｇでは国際標準化機関 3GPP において大幅な見直しが行われ、伝送速度や遅延時間等に係る要件を満たすために工夫がなされました。具体的には、BBU の機能を DU と CU に配置し、RRH の機能を RU に配置する構成へ変更されました。つまり、RRH/BBU の 2 段構成から、RU/DU/CU の 3 段構成へ、配置と機能の分離へ再定義されました。

- 上記のネットワークを構成する要素の分離をどこで実施するかについては、分離する位置で処理する通信容量とその複雑性のトレードオフの関係にあります。RU では電波というアナログ信号とデジタル信号を変換する機能を備えるため技術が複雑化します。また、アンテナなど末端の装置を束ねている上位の装置である CU や DU は処理する通信容量が大きい一方で、処理するための技術は末端に比べると容易になります。特に CU については、必要となる処理能力は比較的軽く、仮想化技術を使った汎用サーバ上で十分な性能を発揮することが可能ですが、DU では５Ｇのアンテナ技術である MIMO の信号分離演算や復号演算の処理が大規模になると言われています。そのため、CU 寄りで分離する方が複雑性を軽減でき、異なるベンダーの機器を相互接続しやすくなる特徴を有しています。

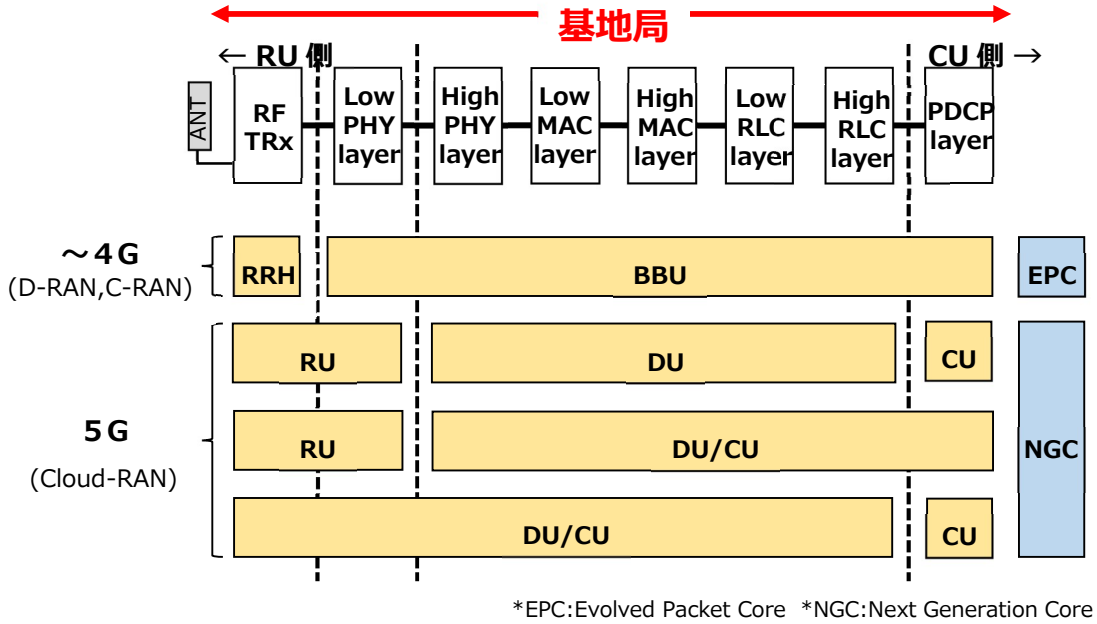


図 1-4-1　５Ｇの基地局に係る標準化

② O-RAN におけるオープン標準

- 上述の５Ｇの標準規定に基づき、DU と CU の間のインターフェースについて、グローバルの業界団体 Open RAN Alliance(O-RAN)において規定されています。O-RAN は、2018 年 2 月に NTT ドコモを含む世界の携帯電話会社 5 社によって設立された団体です。無線アクセスネットワーク（RAN）[2]におけるオープンで標準化されたインターフェースの実現や AI 技術等を活用することでインテリジェントなものに進化することを目的とした活動を行っています。
- 世界の主要な携帯電話事業者が O-RAN で規定されたインターフェースを採用していくことを宣言しています。これにより、５Ｇを構成するネットワークの標準化やマルチベンダー環境が整いつつあります。

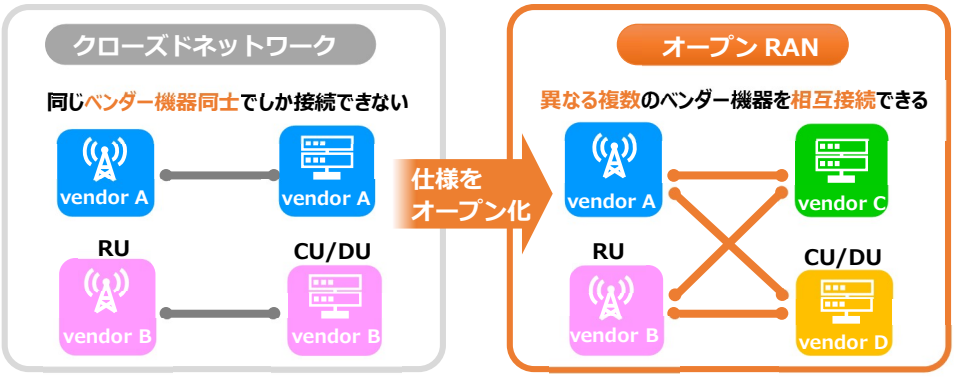


図 1-4-2　O-RAN の概要

- このように、４Ｇまでは各ベンダーが独自のインターフェースを規定していたことから、RAN は 1 つのベンダーに閉じることが通例でした。５Ｇにおいてはインターフェースの標準化と O-RAN におけるベンダー独自の設定を排除した規定により、仮想化技術の活用とともに「マルチベンダー」による構成が可能となり、ネットワークのオープン化が進展しています。

[2] コア装置と端末の間に位置する基地局などで構成される領域を指します

1. コア共用の概要

ローカル５Ｇの今後の発展と、それに伴い必要とされるコア共用について概説します。

① ローカル５Ｇの発展

- ローカル５Ｇは多様な分野・業態においてユースケースの具現化が進んでおり、今後は屋内に加え屋外利用、同一ユーザによる複数拠点でのシームレスな利用、災害時に強いインフラとしての活用など、利便性や強靭性等を追求した様々なユーザニーズを起点としてユースケースが拡大していくことが想定されます。これに伴い、ローカル５Ｇのネットワーク・システムの構成や利用形態は多様化していくことが予想されます。
- 全国の様々な業界・団体でローカル５Ｇへの期待や導入希望が高まる中、ローカル５Ｇシステム構築に係る設備の低廉化は市場原理に基づき一定程度進むものの、中小企業等をはじめとする民間企業や自治体等の各団体が個別で導入するには依然、導入・運用のための費用等が課題になっています。
- これらの状況の打破に向けては、ローカル５Ｇシステムの異ベンダーの製品の組合せによる柔軟な機器構成の実現とコアネットワークやCU等を共用できる仕組みを確立することで、ローカル５Ｇの導入にあたって多様な選択肢を用意することが肝要です。

② コア共用の概要

- 現在、ローカル５Ｇのネットワークは、実証段階の取り組みも多いことから、コアをユーザ拠点の施設に導入して運用する「オンプレ型」が主流となっています。
- 「オンプレ型」とは、各ユーザ拠点にコア及び基地局などを設置します。アプリケーションに応じて、データ処理用の MEC サーバ（例：高速な映像解析等）などの周辺装置の併設や、当該拠点から通信事業者の回線等を経由してクラウドアプリケーションと連携するケースも想定されます。こうしたオンプレ型の場合、ユーザ側でシステムやネットワークを専有することができ、各種要求水準に応じたカスタマイズも可能になります。
- 「オンプレ型」に対して「コア共用型」とは、コアの一部または全てを、ユーザ・拠点より上位の位置に配置し、下位のユーザ・拠点間で共用する構成です。例えば、同一ユーザ（企業等）内の複数拠点で導入・運用する場合の他、例えば同一地域内で異なるユーザの拠点でそれぞれ導入・運用するケースが想定されます。また、「拠点より上位の位置」とは、例えばユーザ企業の本社や産業集積等の地域拠点（例：県単位等）の施設内が想定されます。その他に、ユーザに近いエリアで局舎等施設を保有し、地域の IP ネットワーク等を提供する固定系通信事業者などの回線提供事業者、クラウド事業者やデータセンタ事業者などが挙げられます。クラウドでコアを実装する形態（クラウドコア）も「コア共用型」の一種とみなすことができます。

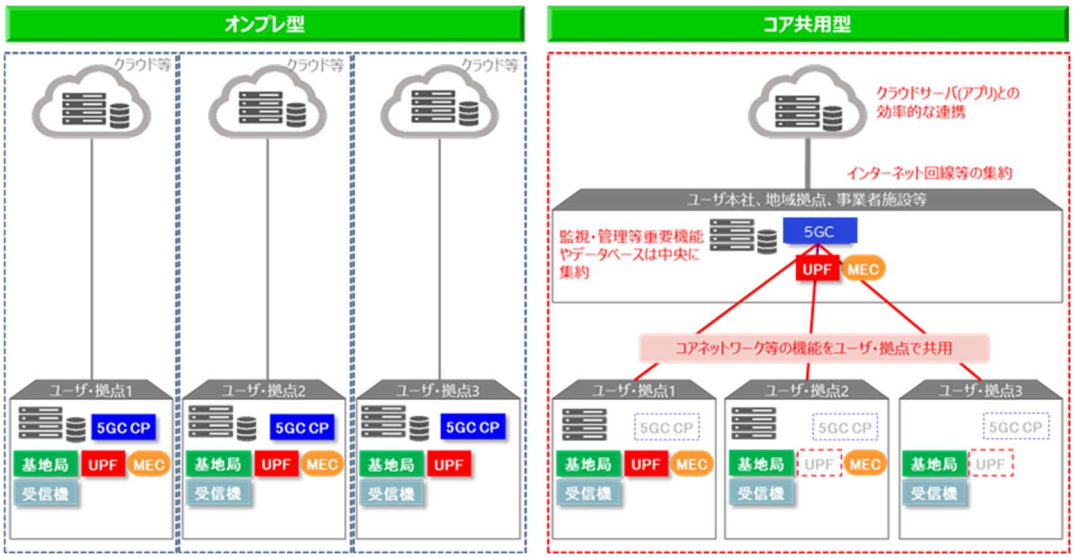


図 2-1-1　コア共用の概念図

- クラウド～端末までのネットワークを構成する要素のどこまでを「ユーザ施設等の拠点側」に設置するか、どこから「拠点より上位の位置」に設置するか、によって共用形態を実現するネットワーク構成をより詳細に類型化することができます。
- 「ユーザ施設等の拠点側」とは、例えば工場内などユーザが実際に５Ｇプリケーションを利用している環境を指します。「共用」とは、「拠点より上位の位置」を複数の拠点やユーザ間で共用している状態です。ユーザ側からみると、他のユーザ（同一企業・異なる企業、同一地域・異なる地域等）とコア等の設備・機能を共用している状態である一方、コアを含むローカル５Ｇのネットワーク・システムを提供する事業者側からみると、自身や連携している事業者のインフラをユーザ間で共用している状態になります。

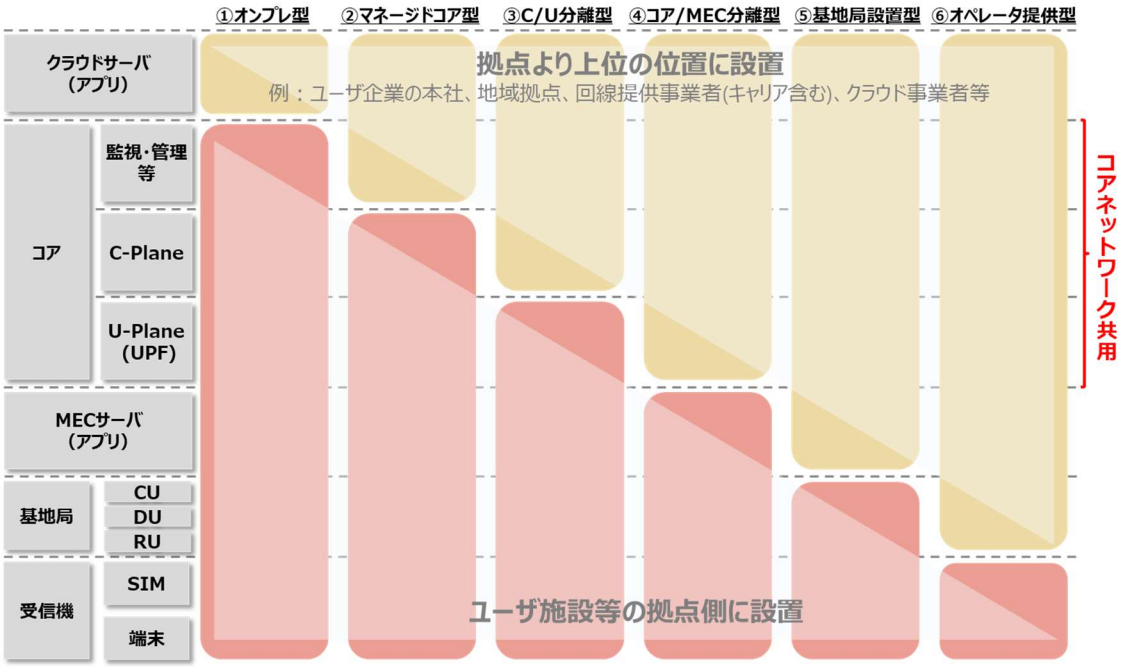


図 2-1-2　共用モデル

2. コア共用の狙い

コア共用の必要性やニーズは、今後のローカル５Ｇの広がりにおいて顕在化することが想定されます。ここでは、その前提となる３つの観点から説明します。

① ローカル５Ｇを導入するユーザ拠点の広がり

- 現在のローカル５Ｇの導入は、主として特定の単一拠点で構築するケースです（例：Ａ社の○○工場にオンプレ型で構築する）。
- 今後は、ユーザ企業が複数の拠点でローカル５Ｇの構築を進めることが想定されます。さらには、サプライチェーンの最適化等の観点から異なる企業同士でシステム統合等を図ることが期待されます。この場合、拠点毎に構築するのではなく、企業内や企業間でコアを共用することで全体最適化を図りたいというニーズが顕在化すると考えられます。
- ユーザ内でコアを共用することで、システムの最適化・一元化等によるコスト低減が期待されます。また、システムを一元化することで、他のプラットフォームやシステムとの接続・連携の実現性も高まるものと想定されます。

② ローカル５Ｇのユースケースの広がり

- 現在のローカル５Ｇは主に特定のユースケースや性能要件に応じて最適なネットワーク構成で構築するケースです（例：低遅延が求められるため、コア(UPF)をユーザ設備内にオンプレで構築する）
- 今後は、ローカル５Ｇのユースケースはユーザ個別で多様化していくことが想定されます。例えば、低遅延が求められるユースケースで構築した設備を活用しつつ拡張したいなどといったニーズが顕在化することが考えられます。
- ユーザがユースケース毎にローカル５Ｇネットワークを構築するのではなく、コアを共用してネットワークの拡張を図りつつ、複数のユースケースやそれを体現するソリューションを実装して投資・費用対効果を高めていくことが想定されます。

③ 同一地域内におけるローカル５Ｇのエリアの広がり

- 現在のローカル５Ｇは主に特定のエリアや拠点で構築するケースです（例：○○敷地内に基地局を設置）。
- 今後は、より多くのエリアや拠点でローカル５Ｇの構築が進むことが想定されます。その際に例えば同一の地域内で様々なローカル５Ｇユーザやネットワークの構築が進むと、各ユーザの導入・運用のコストを抑えるため地域内でローカル５Ｇネットワークやその設備を共用したいというニーズが顕在化するでしょう。
- 地域内でコアを共用することで、例えば地域内中心にトラヒックが流通し、地域外へ流れるトラヒックとその伝送に係るコストを低減させることができます。また、共用が広がれば、同地域の通信基盤の強化にもつながります。

3. コア共用の具体的な効果

前節にて説明したコア共用の位置づけを踏まえ、ここではコア共用による具体的な効果について、経済面、性能面、運用面の３つの観点から説明します。

① 経済面

- 「オンプレ型」の場合、設置する拠点毎にコアを導入するためのインテグレーションや検証に係る初期費用の他、保守・運用費用も生じます。コア装置の費用の他、利用するコアネットワークの機能拡張等に応じて生じる費用や、監視・管理、SIM 認証など共通基盤に係る費用が拠点毎に生じます。これらの費用は一般的には導入するユーザの負担となり、オンプレ型によって構築する拠点毎に発生することになります。そのため、ユーザにとって投資や費用に対する効果が見出せなければ、導入拠点数を増やすといった投資判断が難しくなります。

- 「コア共用型」ではオンプレ型のようにコアを拠点毎に設置せず、コアのコストを複数のユーザで分割することで導入費用を低減することができます。また、拠点毎で要する事前の接続検証等の工程やその検証費用も低減することができます。これらの導入に係る工程が削減されるため、導入までの期間の短縮化にもつながります。コアの運用についてもユーザ間で共用しているため、ユーザあたりの運用経費も低減することができます。

- このように、ユーザ・拠点側毎に全てのコアネットワークの機能を導入・運用せずに、必要な機能のみ配置することで拠点単位の導入・運用コストを下げることができます。拠点数が多い程コア共用による経済合理性が高まると言えます。

② 性能面・拡張性

- コア共用型の場合、オンプレ型では費用が課題となるような高機能なコアを安価に使用できます。また、1 つの場所に設備を設置する、分散された（距離的に離れた）場所に設備を配置するといったネットワークの柔軟な構築形態の選択が可能になるとともに、ユーザが利用するアプリケーション要件等に応じて柔軟で効率的なネットワークスライスを実現することができます。さらに、ネットワーク機能間の一連のやりとりをサービスとして定義し、それらをいつでも再利用できるため開発・構築のプロセスを圧縮しサービスの早期提供につながります。

- 上位側に MEC サーバを配置することで、各ユーザ・拠点から当該サーバへアクセスして、５Ｇと連動したアプリケーションを利用することができます。共用領域から上位に位置するインターネット回線等をまとめたり、ユーザのアプリケーションを実装するクラウドサーバと効率的かつ効果的に連携することが可能になります。

- オンプレ型のように自社施設等に全ての設備や機能を導入しなくても、各ユーザ・拠点での５Ｇの用途やニーズに応じた柔軟な構成が可能になるため、多様なユースケースについて導入しやすくなります。例えば、以下のようなケースが想定されます。

- ✓ ユーザ・拠点 1：コアネットワークのデータ通信処理部（UPF）をユーザ・拠点側に具備し、工場におけるキズ検知向けのリアルタイムな映像 AI 解析など、超低遅延が求められるアプリケーションを利用する。
- ✓ ユーザ・拠点 2：MEC サーバのみ拠点側に置くことで、必要なデータ処理を行い、中央側へのアップリンク回線の帯域を圧縮する。
- ✓ ユーザ・拠点 3：コアネットワークや MEC は上位側に委ねながら、大容量のダウンロードを中心とした利用のため５Ｇ回線を活用する。

③ 運用面

- 監視・管理等の重要機能やデータベース等は中央に集約するような構成を取ることで、運用監視もサービスとして提供されるため、運用監視に掛かる負荷を軽減するとともに、ユーザの BCP（事業継続計画）に係る IT システムの設計と連携することが可能になります。

- ソリューションとの組み合わせを含む選択肢の多様化、運用の一元化、既存設備・システムとの整合や拡張性の確保、責任分解点の明確化、冗長性確保（BCP の観点）、効果的かつ経済合理性の高い運用体制の構築につながります

- 他方、デメリットとしては、クラウドの機能を利用する費用が掛かることや、共用にかかわる各種課題（セキュリティ、データ管理等）や５Ｇ性能（超低遅延等）とのトレードオフの関係が挙げられます。（これらの留意事項や解決策については 3 章を参照）

4. コア共用の普及シナリオ

- コア共用型の運用により、ユーザ企業の本社等の中央管理拠点へのコア機能の配置や、ユーザ企業における既存の IT システムや通信ネットワーク（企業 WAN・LAN 等）と連携し、一体的な管理による全体最適化が進み、ローカル５Ｇを利用するユーザの経済合理性が高まることが期待されます。
- 例えば、工場での運用など複雑かつ厳しい要件が求められる５Ｇのユースケースへ対応するため、コアの機能を拡張することで、コアを共用するユーザがそのメリットを享受できます。例えば、監視や認証といった管理機能の在り方、BCP に資するコアネットワーク自体の冗長化（中央管理拠点におけるコアネットワーク機能のバックアップ等）など、より高度なコア共用の運用形態も想定されます。
- また、ローカル５Ｇユーザが具体的なニーズや要望をローカル５Ｇ提供する事業者（キャリア、ベンダ、クラウド事業者等）へ伝えることで、コア共用の機能や運用等へと反映され、ユーザにとって最適なネットワーク・システム構築や全体的な品質向上にもつながると考えられます。
- こうしたユーザ及び事業者側の双方の取り組みを通じて多用な共用形態が具現化し、中堅・中小企業などのローカル５Ｇ導入意向ユーザにおける導入ハードルが低減化していくことが期待されます。
- コア共用が浸透するにつれ、同一ユーザ企業内の他、産業集積エリアなど、複数の異なる企業間や、特定の業種におけるサプライチェーンを構成する企業グループ間で、共用形態を運用するニーズが顕在化することが予想されます。全国各地で多様な共用形態の構築が進むことで、拠点・エリアを超えた利用やコアネットワークの統合・集約など、ユーザの利便性をさらに高めるローカル５Ｇの運用につながることが期待されます。
- 将来的には、基地局を共用して、キャリアの５ＧコアネットワークとローカルＧコアネットワークが接続するなど、キャリア５Ｇとローカル５Ｇ同士のコアネットワークが連携することで、さらに多様なユースケースの実現につながることが期待されます。

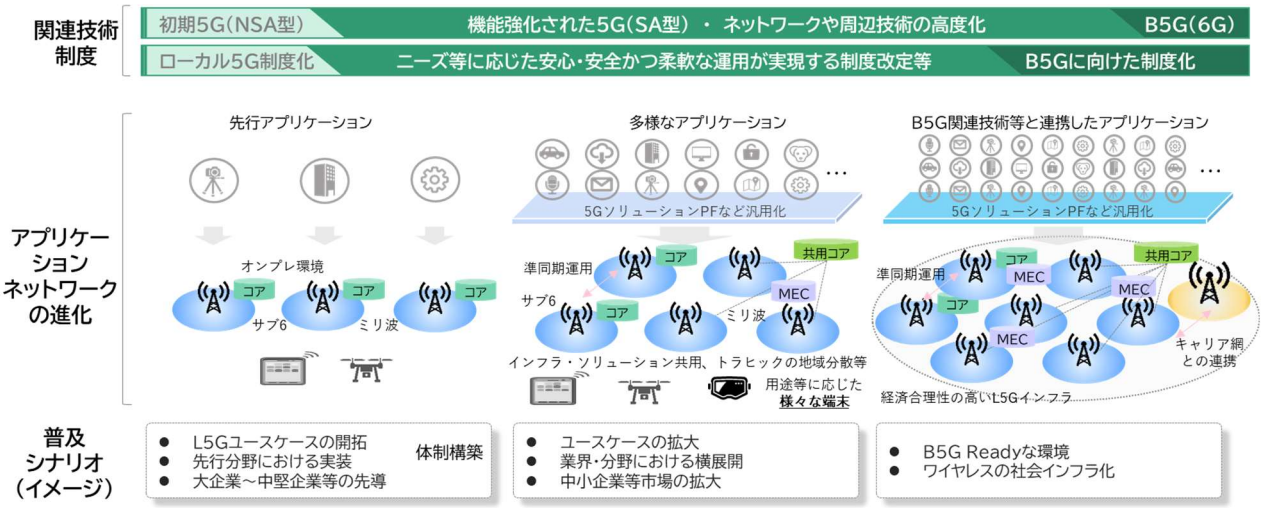


図 2-4-1　コア共用のロードマップ

1. コア共用の主なユースケースの類型・モデル

「２．コア共用の狙い」にて挙げたユーザの観点から、コア共用の類型として以下の①・②のパターンが挙げられます。

① 複数のユーザでコアを共用する

- あるエリア（県・地域ブロック等）内の複数のユーザの間でコアを共用する形態です。具体的には、地域における産業集積地区（例：工業区域）や港湾などの一定のエリアに、複数の異なるユーザや、特定の業種におけるサプライチェーンを構成する企業グループ間で共用形態を構成します。
- コア設備等については、特定のユーザの施設または地域内の中立的な組織（地方自治体が所掌する産業センタ等）の施設に設置します。必要に応じてネットワークを監視・管理する機能等も配置します。
- 各ユーザで異なる５Ｇアプリケーションの利用要望や固有の要件を有していることから、それぞれを満たすための共用形態を構成します。
- 各ユーザ拠点間を閉域網で構成することで、例えば同じアプリケーションやデータを複数のユーザ拠点間で共用して利用することが可能になります。一方で、インターネット網へ接続する構成の場合は、セキュリティ確保の観点からユーザ拠点間でアプリケーションやデータは共用しないことも想定されます。
- 例えば、中小企業においてオンプレミスの構築はコスト面で導入障壁がある一方、複数の異なる中小企業等の間でローカル５Ｇの交換設備を共用することで、各企業が共用効果を享受することができます。

＜複数企業パターンのユースケース例（製造分野の例）＞

- **解決したい課題及びソリューション：**
  製造業における安全確保、コロナ禍における密集の対策に人的リソースを投入することの企業負担といった課題に対し 4K 監視カメラと AI 技術を活用することで、現場に専用の人員を配置することなく、危険エリアへの立ち入り検知・管理者への通知/遠隔地からの現場映像の確認や作業エリアにおける人数検知・密検知を行うことが可能になります。
- **ローカル５Ｇの活用方法：**
  ローカル５Ｇ性能(大容量、低遅延)を活かし、高精細映像の伝送およびリアルタイム性を実現します。4K 画質の AI カメラによって人侵入検知および混雑度検知を行い、スマートフォン型端末を利用して、有事の通知の受け取りや映像確認をスマートフォン型端末で行い、遠隔地の管理者が現場の作業員の安全管理を行います。
- **ネットワーク構成：**
  この例では、地域等のデータセンター内にコア設備を設置し、WAN 回線を経由して複数のユーザ施設へ接続することで、コアを共用します。
  ここでは、ユーザ拠点内に、工場内の作業エリアと管理者が待機する事務室の二箇所に一台ずつ基地局を設置しています。工場の基地局には人侵入検知用と混雑度検知用の AI カメラを接続しています。事務室の基地局には遠隔からカメラ映像を確認する用途のスマートフォン型端末

を接続しています。AI カメラのリアルタイムの映像はインターネットを介さずにスマートフォン型端末から直接確認することができます。また、AI カメラの各検知 AI が取得した統計データ(例：人侵入を検知した時間、リアルタイムの混雑度レベル 等)は、インターネット経由でクラウドへ蓄積され、スマートフォンからクラウドへアクセスすることで確認が可能です。

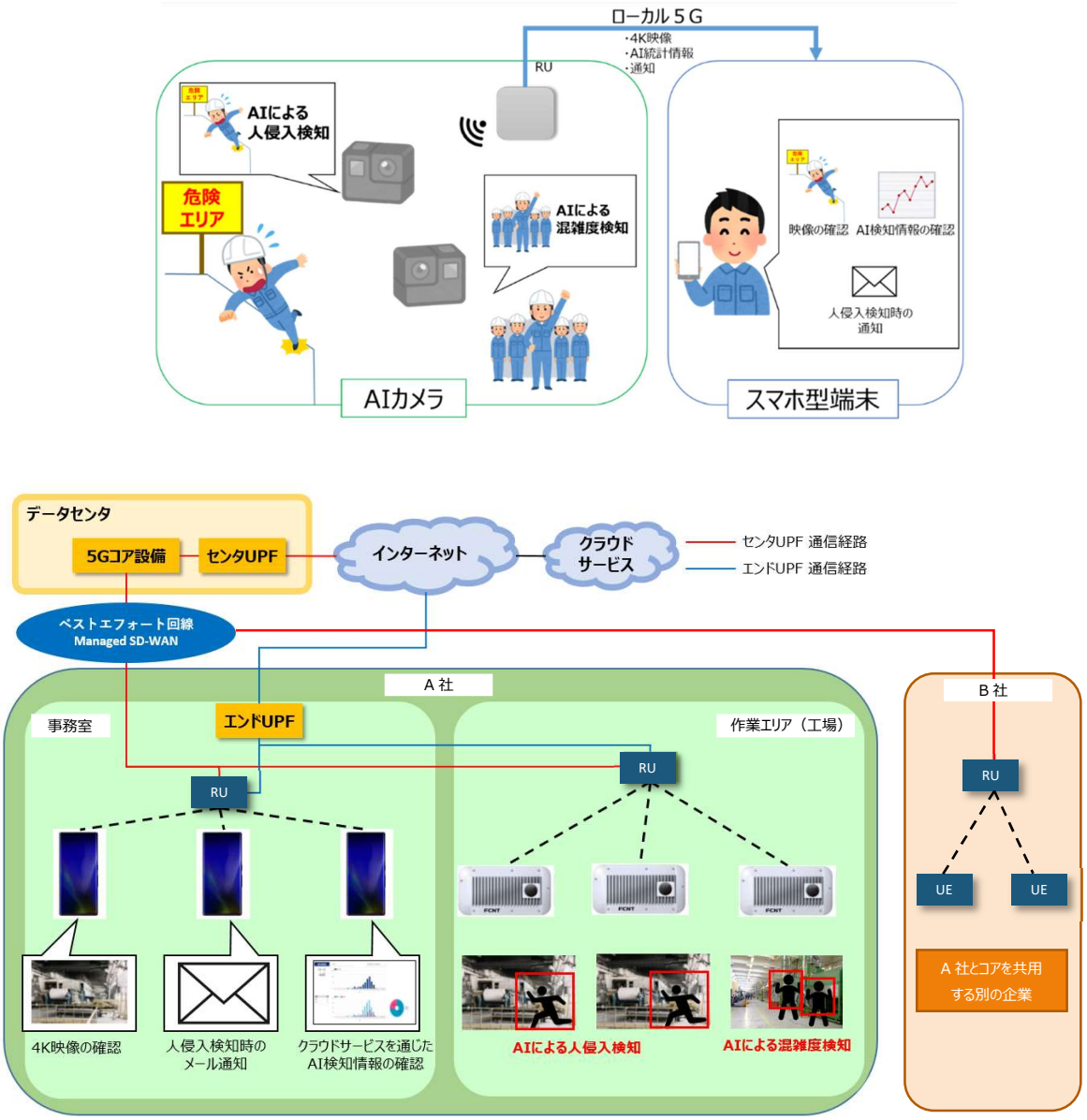


図 3-1-1　複数企業パターンのユースケース例

② 同一のユーザや業界でコアを共用する

- 同一のユーザ企業や同一業界（産業界や官公庁等）内で、全国複数拠点でコア共用形態を構成します。具体的には、拠点内または各拠点でローカル５Ｇのアプリケーションを利用するため、各アプリケーションの要件を満たすためのネットワーク構成や運用形態を構築します。特に同一業界内では、ネットワーク構成や利活用アプリケーションは類似しているケースが多いといえます。
- 一般に大手企業はユーザ拠点配置や自社運用の割合が高く、中堅・中小企業は事業者側配置率やアウトソース運用の割合が高いことから、ユーザの企業規模や拠点構成等によって様々なコア共用形態が想定されます。
- この場合、ローカル５Ｇのコア等の設備や機能を、ユーザ企業のエンド拠点と、上位の位置（事業者拠点等）に配置することになります。MEC やクラウドサーバ等でアプリケーションを

実装し、拠点間でアプリケーションやデータ等を共用する使い方が想定されます。

- 例えば業界共用の高速バックボーンネットワーク※を有する業界では、同業界の異なる団体間が当該既存のネットワークを活用したコア共用に係る効果が期待されます。
  ※団体が業界共用ネットワーク に接続するための接続点（POI）間を繋ぐネットワーク

＜業界共用パターンのユースケース例（教育分野の例）＞

- **解決したい課題及びソリューション：**
  専門性の高い大学の教育においては、工学部や医学部の高額な精密機器・農学部や獣医学部の研究対象のように、研究に必要な設備や環境や専門家が有するスキルについて距離的な制約といった課題があります。（例：熟練医師の手術は限られた人数しか間近で見ることが出来ない）。この課題に対し、例えば 8K カメラを活用した高精細な Web 会議システムを構築することで遠隔拠点へのリアルタイムの情報共有および双方向コミュニケーションが可能となります。
- **ローカル５Ｇの活用方法：**
  遠隔教育は多様性のある学習環境や専門性の高い授業の実現等、最新かつ専門的な知識や技能に触れることのできる質の高い学習の実現に資するとして注目されています。ローカル５Ｇの性能(大容量、低遅延)を活かし、高精細な映像をリアルタイムに配信することで、遠隔地からも精密機器の細かな箇所や有スキル者の繊細な作業を見ることが出来ます。
- **ネットワーク構成：**
  この例では、センタ拠点にコア設備を設置し、WAN 回線を経由して複数の大学拠点へ接続することで、コアを共用します。
  業界共用ネットワークを活用し、8K 画質のカメラを利用して、大学間のリアルタイム 8K 映像伝送を実現します。

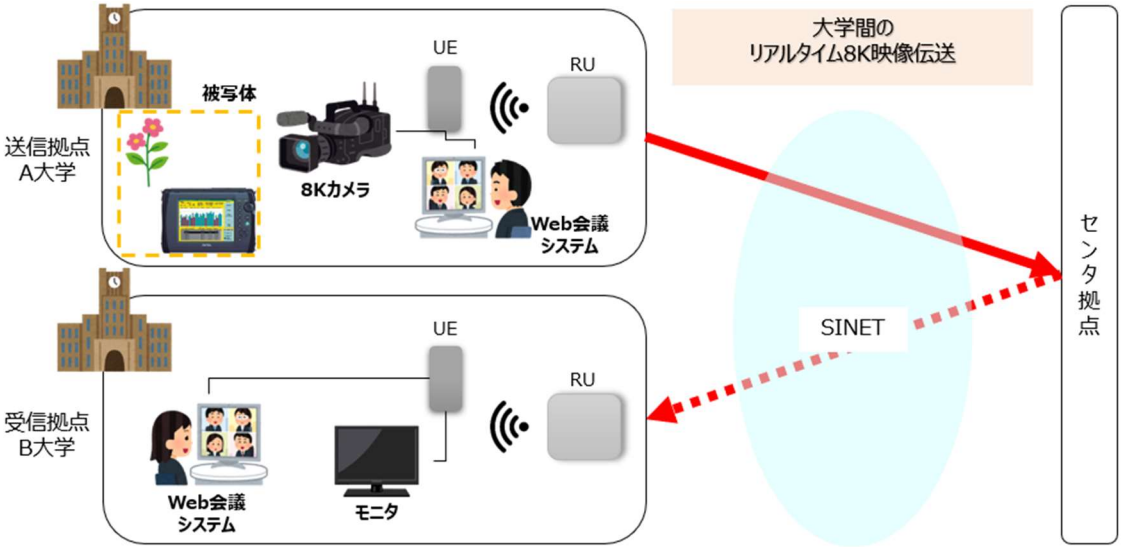


図 3-1-2　業界共用パターンのユースケース例

2. コア共用のネットワーク構成

コア共用において想定されるネットワーク構成について説明します。

ネットワーク構成のパターン

- ローカル５Ｇのネットワーク構成の形態は、下図の①から⑥まで類型化することができます。この中で、③～⑥がコア共用の形態に該当します。コア共用により、システム全体での総機器数が減少し、エンド拠点における導入の容易化やコスト低廉が見込まれます。

- ローカル５Ｇを導入する際は利用用途やユーザ・拠点配置・アプリケーション等によって最適な形態を選択する必要があります。③は 5GC のみ共有して UPF は共用しない形態です。④～⑥は UPF を共用する形態であり、物理的な距離による遅延を改善するために、④・⑤(右)のようにエンド拠点に UPF を設置することも可能です。

- ⑤(右)は 5GC と UPF に加えて CU を共用する形態であり、更なる導入の容易化やコスト低廉化が望めます。

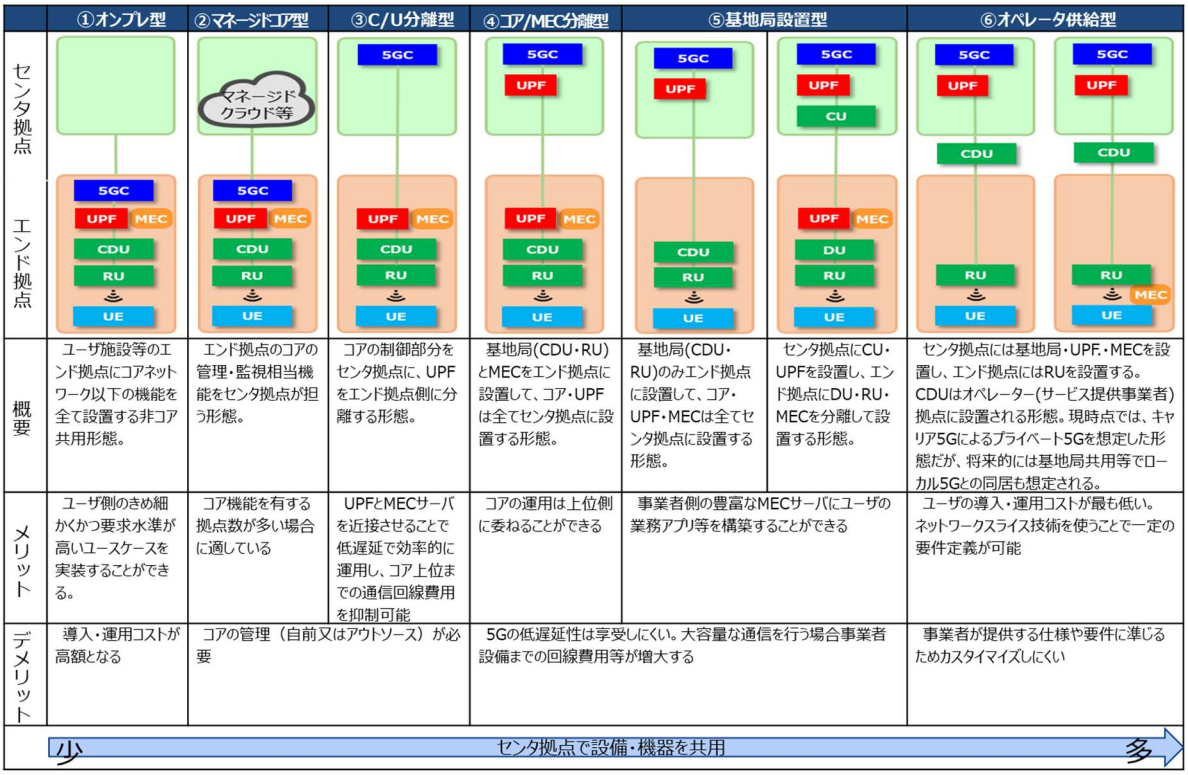


図 3-2-1　コア共用におけるネットワーク構成

共用の範囲

- 共用する機器の範囲については、5GC を共用する形態、5GC/UPF を共用する形態、5GC/UPF/CU を共用する形態が挙げられます。
- CU は、無線アクセスネットワークにおける集約基地局であり、主にデータ処理を行うネットワーク要素です。５Ｇでは、４Ｇにおける BBU の機能を DU と CU に分離することで、一つの CU に対して複数の DU を配置する構成が可能となりました。そのため、センタ拠点に配置した CU 共用する形態で、複数ユーザ DU を接続することが可能です。
- また、DU と CU の間のインターフェースについて、グローバルの業界団体 Open RAN Alliance(O-RAN)において規定されています。そのため、共用する CU と DU で異ベンダーの製品を組み合わせることも可能になります。
- このように、UPF と CU を共用することで、ユーザ側の構築や物品調達、運用コストを減らせるメリットがあります。

UPF の設置位置

- UPF の設置位置はセンタ拠点に共用する場合(センタ UPF)とエンド拠点に設置する場合(エンド UPF)が考えられます。UPF の設置場所を変えることで基地局やアプリケーションを利用する場所との距離も変わるため、スループットや遅延時間等の伝送性能に影響します。
- センタ UPF の場合、設置位置がユーザから遠くなるため、遅延時間は長くなります。
  費用や運用面についてみると、UPF をユーザ間で共用することから、ユーザ当たりの費用逓減効果が期待できます。他方で、大容量通信に利用する場合、ユーザ拠点からセンタ UPF までの伝送回線（WAN 回線等）については相応の帯域を用意する必要があるため、伝送回線費用は高くなります。
- エンド UPF の場合、設置位置が末端（ユーザ側）に近い程、その分遅延時間を短くすることができます。しかしながら、UPF の構築や物品調達、運用コストがかかります。
- このように、UPF の設置位置と伝送性能はトレードオフの関係にあります。

3. 各実装モデルにおける費用感

- ①のオンプレ型に比べ、コア設備を共用するモデル③⑤の場合、機器数の削減により費用の低廉化が見込めます。例えば、5 拠点での共用の場合は、オンプレ型と比較して構成により約 1～5 割のコスト削減効果があります。

- ③UPF をエンド拠点に設置する場合、広帯域な拠点間回線は必要がないため機器の集約によるコストメリットが見込めます。

- ⑤UPF をセンタ集約した場合、1 拠点あたりの削減が見込めます。ただし、低遅延が必要なユースケースには広帯域回線（ギャランティ回線）が必要であり費用が増大するため、既設の広帯域回線が利用できない場合は UPF をエンド拠点に設置する構成③が望ましいといえます。

- さらに⑤（右）のように CU もセンタ集約した場合、さらに費用の削減が見込めます。

	①オンプレ型	③C/U分離型(コア設備のみ共有)	⑤基地局設置型(コア設備＋UPF共用、CU/DU分離)	
センタ拠点		5GC セキュリティ	5GC UPF セキュリティ	5GC UPF セキュリティ CU
拠点間回線				
エンド拠点	5GC UPF セキュリティ CDU RU UE	UPF MEC CDU RU UE	CDU RU UE	UPF MEC DU RU UE
特徴	拠点間の回線不要であり完全閉域NWである	コア設備/セキュリティ装置の共用により安価であり、UPFがエンド拠点に配置されることで低遅延通信が可能	コア設備/セキュリティ装置に加えUPFも共用する安価な構成。ユーザ通信が拠点間回線を通るため、要件に応じて拠点間回線の選定が必要	コア設備/セキュリティ装置/UPFに加えCUも共用するさらに安価な構成。低遅延を要する場合はエンド拠点にUPFを設置することも可能
	低遅延性能かつユーザのセキュリティ要件により閉域NWが求められる等の用途であり、他拠点と共用しないモデル	複数企業や同一企業等の複数の拠点間で共用する場合で、工場の遠隔操縦等の低遅延性能を要する用途で採用するモデル	③と同様に複数の拠点間で共用する場合で、比較的低遅延を要しない用途で採用するモデル	低コストでありながら低遅延を求められるアプリケーションにも柔軟に対応可能な共用モデル

図 3-3-1　各実装モデルの特徴

第 2 部
ユーザ企業を支援する
SIer 等に向けた手引

1. 本手引書の対象

本手引書では、コア共用の形態について、UPF の設置位置及び共用の範囲の 2 つの軸を組み合わせた、4 つのネットワーク類型を対象に、検証結果等に基づく要件や課題等についてご説明します。

本手引書の検証内容の詳細については「ローカル５Ｇの交換設備の接続・共用の在り方に関する調査研究の請負」の報告書（令和 3 年度/令和 4 年度）を参照ください。

① 共用の範囲

- 共用の範囲は、5GC を共用する形態、5GC/UPF を共用する形態、5GC/UPF/CU を共用する形態が挙げられます。

② UPF の設置位置

- UPF の設置位置は、基地局やアプリケーションを利用する場所との距離とも関係するため、スループットや遅延時間等の伝送性能に影響します。UPF の設置位置と伝送性能はトレードオフの関係にあります。

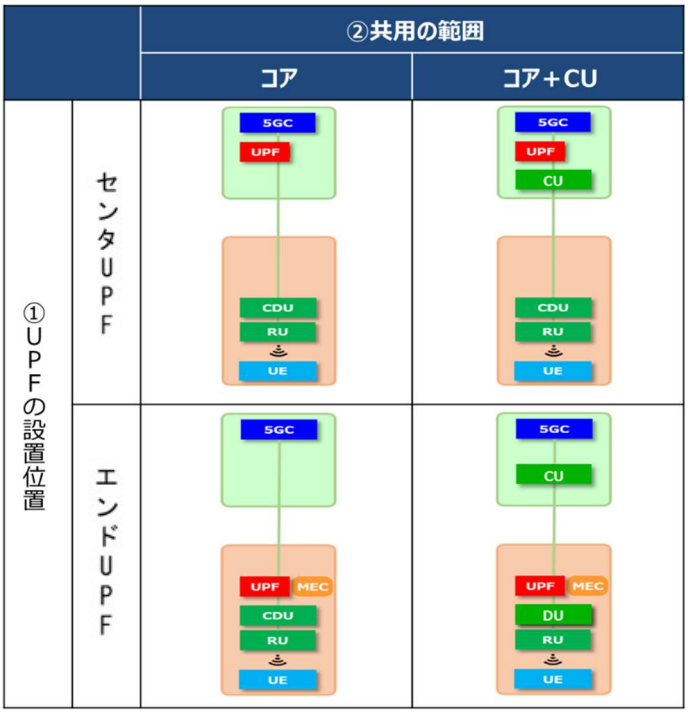


図 4-1-1　対象となるネットワーク類型

③ 共用の対象（ユースケース）

- あるエリア（県・地域ブロック等）内で、複数のユーザの間でコアを共用する形態「複数企業共用パターン」と、同一のユーザ企業や同一業界（産業界や官公庁等）内で、全国複数拠点でコア共用形態「業界共用パターン」を構成します。

2. コア共用のパターンとメリット・デメリット

共用の範囲

- 共用する機器の範囲については、UPF のみを共用する形態（同図左）と、UPF と CU を共用する形態が挙げられます。
- CU は無線アクセスネットワークにおける集約基地局であり、主にデータ処理を行うネットワーク要素です。５Ｇでは、４Ｇにおける BBU の機能を、DU と CU に分離することで、一つの CU に対して複数の DU を配置する構成が可能となりました。そのため、CU をセンタ拠点側に配置して複数の DU で共用も可能です。
- また、DU と CU の間のインターフェースについて、グローバルの業界団体 Open RAN Alliance(O-RAN)において規定されています。そのため、共用する CU と DU で異ベンダーの製品を組み合わせることも可能になります。
- このように、UPF と CU を共用することで、ユーザ側の構築や物品調達、運用コストを減らせるメリットがあります。

UPF の設置位置

- 分散配置する UPF の設置位置はセンタ拠点に置く場合(センタ UPF)とエンド拠点(エンド UPF)が考えられます。UPF の設置場所を変えることで基地局やアプリケーションを利用する場所との距離も変わるため、スループットや遅延時間等の伝送性能に影響します。
- センタ UPF の場合、設置位置がユーザから遠くなるため、遅延時間は長くなります。
  費用や運用面についてみると、UPF をユーザ間で共用することから、ユーザ当たりの費用逓減効果が期待できます。他方で、大容量通信に利用する場合、ユーザ拠点からセンタ UPF までの伝送回線（WAN 回線等）については相応の帯域を用意する必要があるため、伝送回線費用は高くなります。
- エンド UPF の場合、設置位置が末端（ユーザ側）に近い程、その分遅延時間を短くすることができます。しかしながら、UPF の構築や物品調達、運用コストがかかります。
- このように、UPF の設置位置と伝送性能はトレードオフの関係にあります。

3. 3GPP/O-RAN の標準化仕様の内容と上記整理との関係及び必要性

- ローカル５Ｇシステムは、下図に記載する 14 の要素によって分類可能であり、各要素は主に 7 つのインターフェースによって接続されます。早期環境整備の点からは、SIM の認証、ユーザ情報の整理・運用を担うコア、無線部の制御を行い通信性能の要となる基地局、そしてユーザとのインターフェースを取り持つ端末という 3 つの機器において、異ベンダー間の相互接続を整備することで、各企業、SIer 等はそれぞれの要件に適したベンダーの機器を用いてローカル５Ｇシステムを構築することが可能となります。

- 赤枠で示している部分が、本技術的手引の主な対象となります。

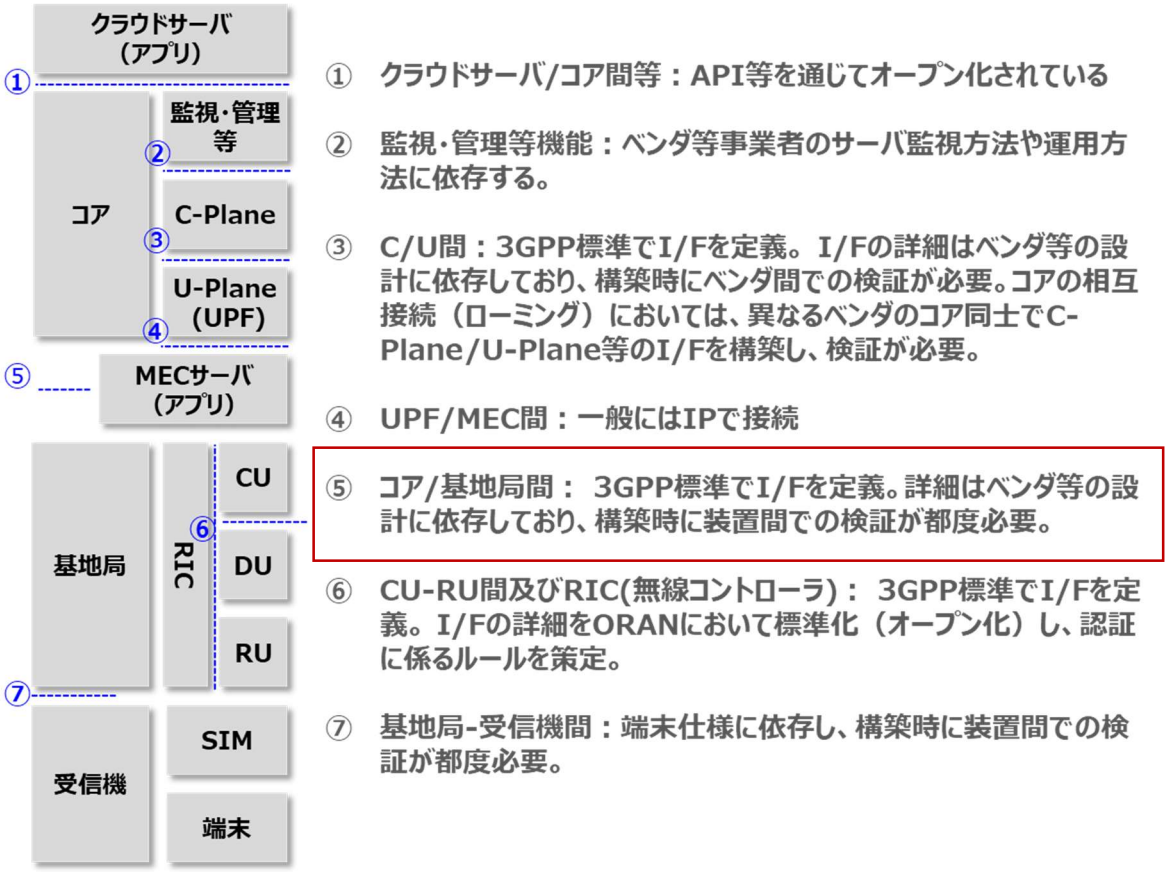


図 4-3-1　インターフェースの整理

1. 性能要件に関する概要

コア共用に係る性能要件について説明します。ローカル５Ｇの特性を活かしながら、性能要件を設定するためには、以下の 5 つの観点が重要と考えられます。

本手引書では、ローカル５Ｇのシステム構成や環境の違いによる伝送性能への影響や相関性に係る検証結果を踏まえて、性能要件において参考となるデータや留意事項について概説します。

検証は、前述の 4 つのネットワーク類型のパターン毎に、伝送性能、UE 多接続及び TDD 方式等を測定し、比較しています。

① ネットワーク要素の設置場所・接続形態

- 現在ローカル５Ｇの構築事例の多くは設備ユーザ拠点の設置するオンプレ型が主流ですが、共用の選択肢として 5GC（C-Plane/U-Plane）をデータセンタ等の地域の拠点に設置する地域共有型や、クラウドを活用するクラウド型が考えられます。それら共用形態において 5GC（C-Plane/U-Plane）・基地局（CU/DU/RU）・UE の各設備の設置場所や接続形態は、性能と費用対効果のトレードオフとなります。
- 5GC をセントラルコアとして保有し、各ユーザ拠点に UPF と基地局を設置し、それらを一括で集中的に監視・管理する構成について、特に大学や自治体、港湾といった場所での活用が進んでいます。例えば大学において、複数のキャンパスに跨ったネットワークを構築するといったケースが想定されます。（本手引書では「業界共用パターン」として掲載）
- また、工業団地のようなエリアで、複数のユーザ企業がローカル５Ｇを使うユースケースにおいて、工業団地を管理している事業者が 5GC/UPF/CU を保有して各ユーザ企業で共有し、DU/RU は各ユーザ企業が保有するというケースも想定されます（本手引書では「複数企業共用パターン」として掲載）。
- こうしたユースケースにおいて、コアと離れた拠点の基地局等について、低遅延や大容量を担保する為の通信回線の性能や距離の限界値等への考慮が必要となります。

② UPF の設置場所

- ユーザ企業等のＤＸを実現するためには、データハンドリングが重要なポイントとなります。そのため、ローカル５Ｇのネットワークアーキテクチャを考える上では、特に５Ｇのドメインからデータを切り出す出口である UPF をどこに置くかが重要となります。
- UPF の設置場所については、遅延時間に係る性能要件や考え方、ユーザがデータをどのように扱いたいか等に応じて考える必要があります。
- 例えば、UPF を地域のデータセンタ等に設置して共用するケースが想定されます。この場合同地域内のユーザ間でのコスト面の共用効果が期待できますが、個々のユーザのエンド拠点においてデータ処理ができない点やエンド拠点から地域のデータセンタまでの VPN 等の別回線が必要になる点に留意が必要となります。
- そのため、ユーザのローカル拠点においてデータハンドリングを重視する場合、UPF をローカル拠点に置くニーズが強いと考えられます。また、データ処理等を行う MEC についても、UPF と隣接してデータ処理を行うため、UPF と同様に、ユーザのローカル拠点に設置するのが望ましいと考えられます。

- コア設備と離れた拠点の基地局について、通信制御はコアが行い、ユーザトラヒックはコア設備を経由せずネットワーク負担を軽減する仕組みの検討が必要となります。

③ 遅延性能の確保

- 上述の設置場所・接続形態について、性能要件の観点からは遅延が重要な指標となります。共用形態を取ることでセンタ拠点に設置した UPF を使用する場合、エンド拠点からセンタ拠点への拠点間通信が発生するため、遅延性能の劣化が懸念されます。
- 特に、製造業等において遅延時間に対する要求水準が高い場合があります。例えば、遠隔作業支援の際に支持者と作業者間のコミュニケーションにおいて、遅延が発生することによりリアルタイムでの支援が困難となる事象が想定されます。
- これらの解決手法として、U-Plane を拠点内で処理するべくエンド拠点に UPF を設置すること(MEC)が効果的であると考えられます。ただし、その際にはエンド拠点の UPF の導入費用に留意が必要です。
- このように、ユースケースの要件と生じる費用を考慮した構成設計が肝要となります。

④ 多数同時接続性の確保

- 伝送容量及び低遅延性に加えて、５Ｇの重要な性能要件が端末(UE)の多数同時接続性です。
- コア共用において、UE が多数同時接続する場合に、発生するスループットが増大することから、コアが各端末を制御するための帯域や処理能力を確保することが必要となります。具体的には、UE 台数に応じて DU 装置等にメモリの増強が必要となる場合があります。ただし、CPU はコア共用による影響は少ないことが検証から明らかになっております。
- また、UE 数の増大に応じて、コア～基地局の回線は、一定の帯域を確保することが重要となります。
- エンド拠点に UPF を設置する場合は、センタ拠点とエンド拠点間の回線には C-Plane 通信しか流れず、UE 台数が増えても帯域の占有量は小さい(例 30 台でも数 10kbps 程度)ため、一般的な 100Mbps のベストエフォート回線等を用いても問題ありません。
- センタ拠点に UPF を設置し同じ回線内で C-Plane と U-Plane 通信を流す場合、U-Plane の通信は C-Plane と比較して大きな帯域を必要とするため、UE の接続台数と必要な C-Plane/U-Plane の総スループットを満たす回線の選定が必要となります。

⑤ 準同期 TDD 方式の採用

- 安定性の高い低遅延性の実現はローカル５Ｇを活用する重要なメリットとなります。加えて、アップリンクのトラヒックを大きく確保ができることもメリットです。例えば、リアルタイムの映像伝送や、高精細画像を取り込んで AI で解析するソリューションにおいては、アップリンクのトラヒックを大きくすることが求められます。
- これらのニーズに応え、ダウンリック・アップリンクの比率の可変を実現する「準同期 TDD 方式」は、キャリア５Ｇに対するローカル５Ｇのメリットになります。

2. 共用環境毎の基本的な性能（伝送スループット、遅延時間等）

本項では、4 つのネットワーク類型のパターン毎に、ローカル５Ｇのユースケースに応じた性能要件を満たすことができるか、コア共用構成における伝送スループットや遅延時間等の性能について、実測を行った検証結果を基に、満たすべき性能要件について説明します。

＜検証概要＞

- ローカル５Ｇのコアと CU を共用する構成において、環境の違いによる伝送性能への影響や相関性について検証しました。
- UPF の設置位置については中央に設置して共用する「センタ UPF」とユーザのローカル拠点に設置する「エンド UPF」について比較検証しました。また、共用の対象（ユースケース）については「複数企業共用パターン」及び「業界共用パターン」）２つのパターンについて比較検証しています。
- これらの環境の違い及びローカル５Ｇのシステム構成による伝送性能への影響や相関性について比較・考察しました。

＜検証環境＞

- 複数企業共用パターン及び業界共用パターン（いずれもコア＋CU 共用型）といった環境の違いについて計測結果を比較検証しました。
- 遅延時間の測定に関してはエンド拠点それぞれで実施することでセンタ拠点からエンド拠点までの距離による影響を分析しました。

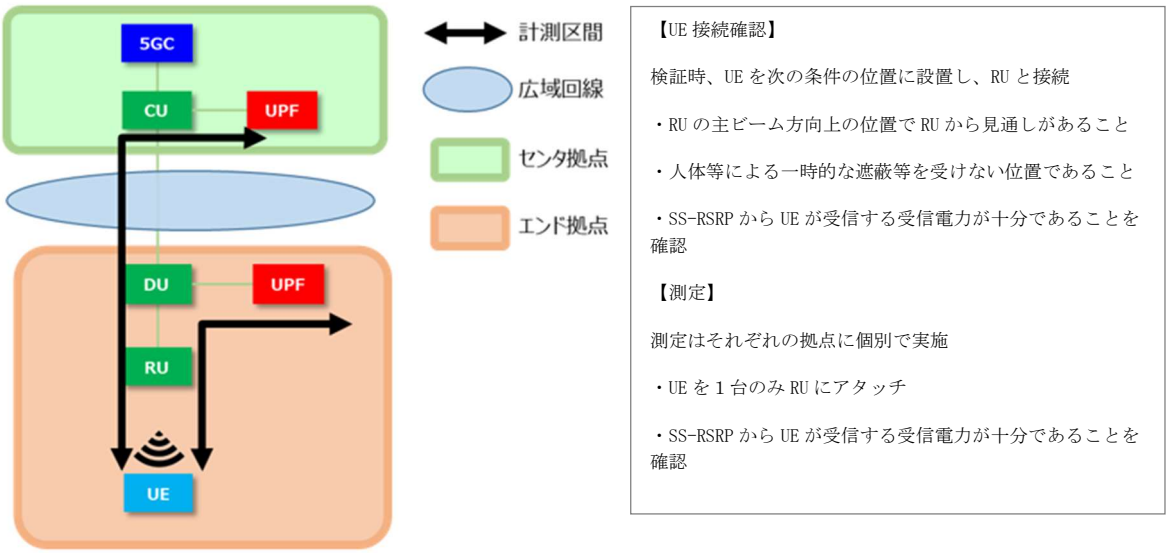


図 5-2-1　検証環境及び計測の前提条件

＜検証結果＞

① スループット

- TCP/UDP の DL スループットについて測定結果を比較すると、エンド UPF 構成の場合には複数企業共用パターンで TCP/UDP：658Mbps/698Mbps、業界共用パターンで TCP/UDP：643Mbps/700Mbps と、双方で高い DL スループットを実測することができました。
- 一方、センタ UPF 構成の場合には業界共用パターンでは TCP/UDP：159Mbps/686Mbps と TCP の DL スループットが低下し、複数企業共用パターンでは TCP/UDP：47Mbps/224Mbps であり TCP/UDP 両方の DL スループットが大きく低下しています。
- エンド UPF 構成の場合は UE～RU～DU～エンド UPF という比較的シンプルな構成であるため、スループットを低下させる要素が最小限であることで、複数企業共用パターン及び業界共用パターンの双方で高い DL スループットを実測できたと考えられます。
- 業界共用パターンのセンタ UPF の場合は UE～RU～DU～ギャランティ回線～CU～センタ UPF という構成であり、エンド UPF と比較して拠点間通信が発生することによって TCP の DL スループットが影響を受け、エンド UPF よりも DL スループットが低下したものと考えられます。
- 複数企業共用パターンのセンタ UPF の場合は UE～RU～DU～ベストエフォート回線～CU～センタ UPF という構成であり、業界共用パターンと同様に拠点間通信が発生することに加えてベストエフォート回線の区間は通信の伝送帯域・速度が保証されないことから、TCP/UDP の両方の DL スループットが大きく制限され、比較的低い DL スループットという結果になったものと考えられます。

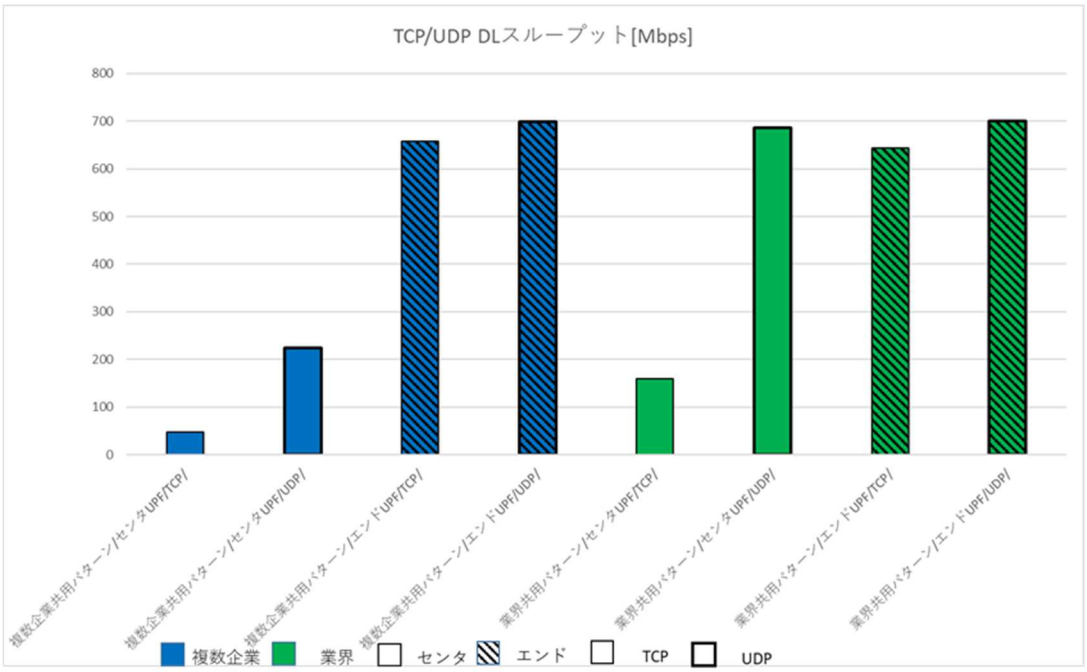


図 5-2-2　ＤＬスループット

- TCP/UDP の UL スループットについて測定結果を比較すると、複数企業共用パターンのセンタ UPF 構成で TCP/UDP：63.8Mbps/65.2Mbps、複数企業共用パターンのエンド UPF 構成で TCP/UDP：63.5Mbps/65.0Mbps、業界共用パターンのセンタ UPF 構成で TCP/UDP：63.9Mbps/65.1Mbps、業界共用パターンのエンド UPF 構成で TCP/UDP：62.3Mbps/65.1Mbps と、どの組み合わせもほぼ同程度の UL スループットを実測できました。

- ただし、複数企業共用パターンのセンタ UPF 構成の場合は通信の伝送帯域・速度が保証されないベストエフォート回線を経由するため、タイミング次第で UL スループットが大きく低下する可能性があると考えられます。

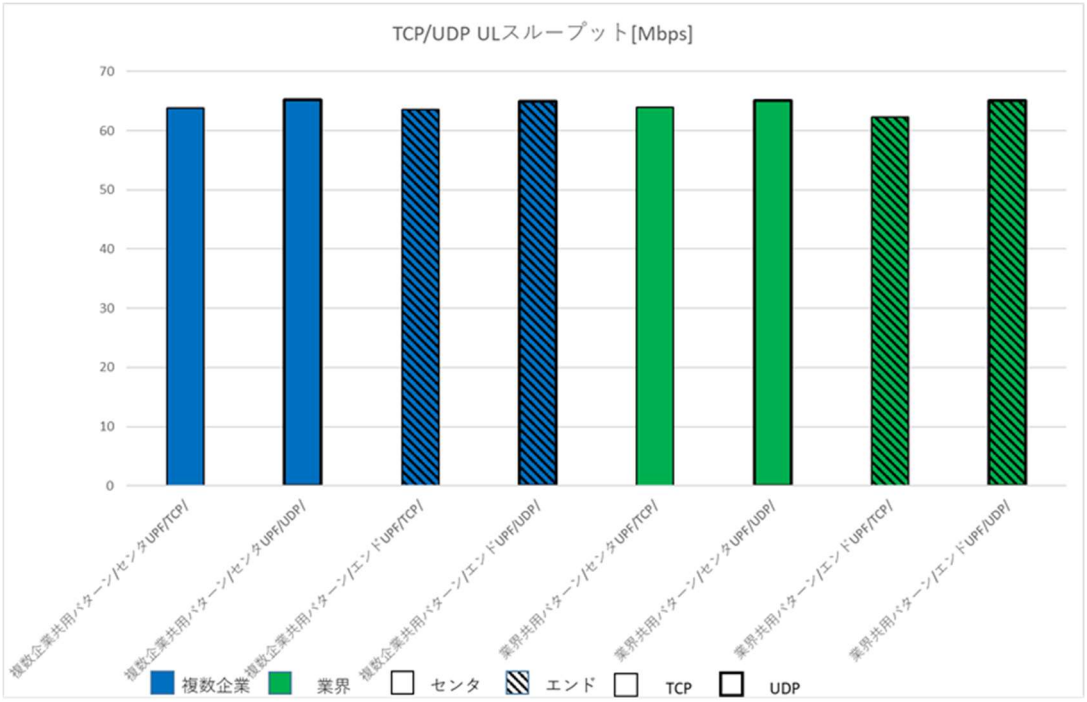


図 5-2-3　ＵＬスループット

② 遅延時間

- UE からセンタ UPF またはエンド UPF に対して ping を送信し、遅延測定を行った結果を以下に示します。
- 測定した遅延時間の平均値は 39.3ms であり、ユーザ拠点からセンタ拠点の距離による伝送遅延によるものと考えられます。

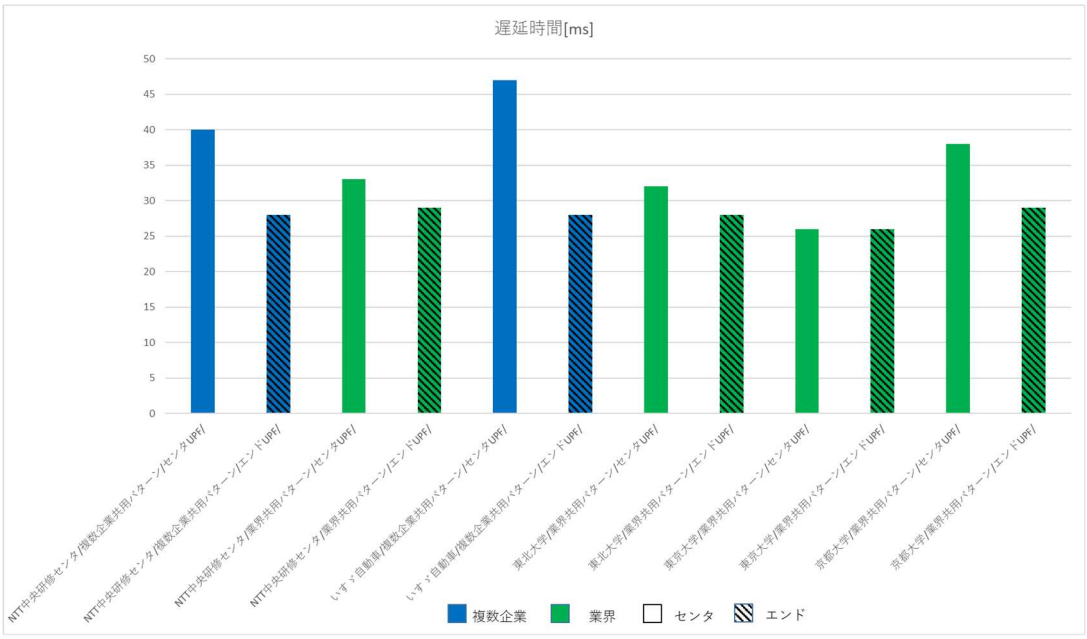


図 5-2-4　遅延時間

＜スループットおよび遅延時間に関するまとめ＞

	共用の範囲	UPF の設置場所
スループット	● コアとコア＋CU では性能において顕著な差は見られません。	● エンド UPF ではシステムの実力値を十分に発揮できるといえます。 ● センタ UPF では、WAN 回線の影響を受けます。特に、ベストエフォート回線を使用する場合は他のユーザの影響を受けるため、スループットが大きく制限される可能性があります。
遅延時間	● コアとコア＋CU では性能において顕著な差は見られません。	● エンド UPF ではシステムの実力値を十分に発揮できるといえます。 ● センタ UPF では、WAN 回線の影響及びセンタ拠点～エンド拠点の距離の影響を受けます。特にベストエフォート回線を使用する場合は、遅延時間が大きく劣化する可能性があります。

3. 端末数に応じた性能への影響

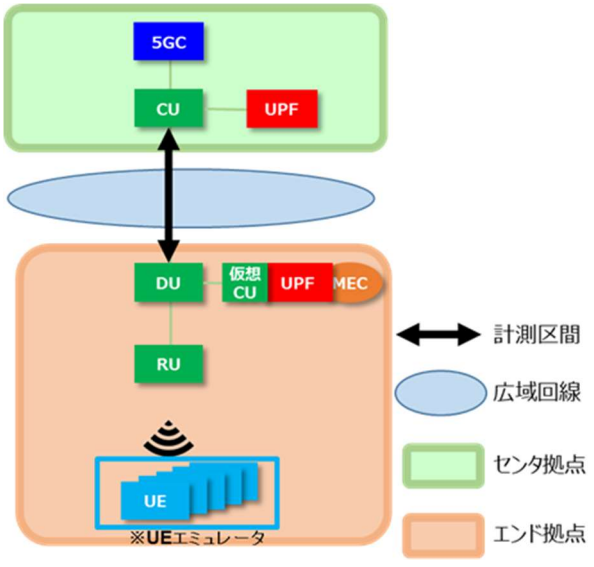
本項ではコア共用において UE の同時接続数を増やした場合の影響等について説明します。

＜検証概要＞

- 複数の UE を同時に接続した場合に、基地局及び WAN 回線を経由してコアに確実に接続できること、また WAN 回線の必要帯域を確保できるかという観点で検証を実施しました。
- また、ローカル５Ｇのコアと CU を共用する構成において、UE の同時接続を増大させながら、WAN 回線で必要となる帯域について検証しました。
- 具体的には、UE 同時接続数を 1 台・10 台・20 台・30 台と変更しながら拠点間を流れる通信への影響を確認しました。これらの環境の違い及びローカル５Ｇのシステム構成による伝送性能への影響について検証を行っています。また、共用の対象（ユースケース）については「複数企業共用パターン」及び「業界共用パターン」）2 つのパターンについて比較検証しています。

＜検証環境＞

- UE が多数接続した場合に C-plane にどれだけの通信が発生するかを測定しました。
- UE エミュレータを用いて数十台分の UE 接続状態を再現し、Linux コマンドを用いて 5GC の通信ポートのパケットキャプチャを行い、Wireshark を用いてスループットを計測しました。
- 複数企業共用パターン及び業界共用パターン（いずれもコア＋CU 共用型）といった環境の違いについて計測結果を比較検証しました。



【UE エミュレータ接続】

・RU を停波状態としアンテナ取り外し

・同軸ケーブルを用いて RU アンテナポートに UE エミュレータを接続（減衰器により電力を調整）

・RU から電波発射

【測定】

測定はそれぞれの拠点に個別で実施

UE 接続数は 1 台・10 台・20 台・30 台

測定手順は次のとおり

・想定する UE 接続数が全てアタッチしたことを確認

・WAN 回線上の使用帯域を測定

図 5-3-1　検証環境及び計測の前提条件

＜検証結果＞

- 複数企業共用パターンにおいて計測した結果について説明します。
- UE1 台の場合、ピークとして 12kbps 程度のスループットが確認できました。これは UE アタッチ時に発生した C-plane 通信です。またアタッチの処理以外で一定の間隔で 1.6kbps 程度のスループットが発生していました。
- UE30 台の場合、ピークとして 20kbps 程度のスループットが確認できたほか、5kbps～18kbps の間で散逸的にスループットが発生しています。それぞれが 30 台の UE が順次アタッチした時に発生した C-plane 通信です。アタッチするタイミングが重なったことでピークの値はやや増えたものの、使用する帯域としてはそれほど変動していないと考えられます。

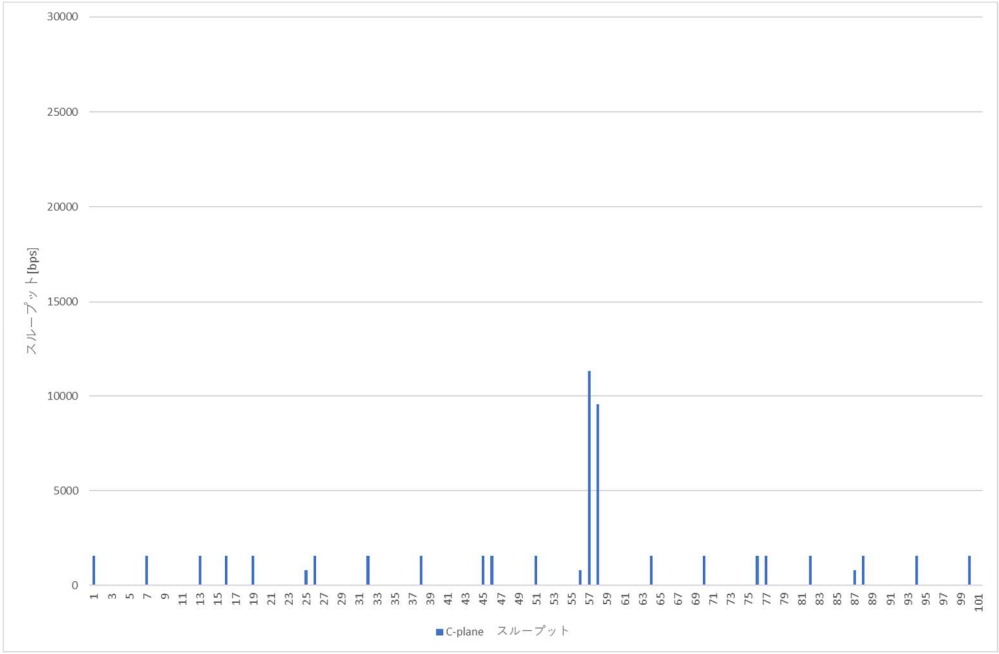


図 5-3-2　C-Plane スループット（UE1 台）

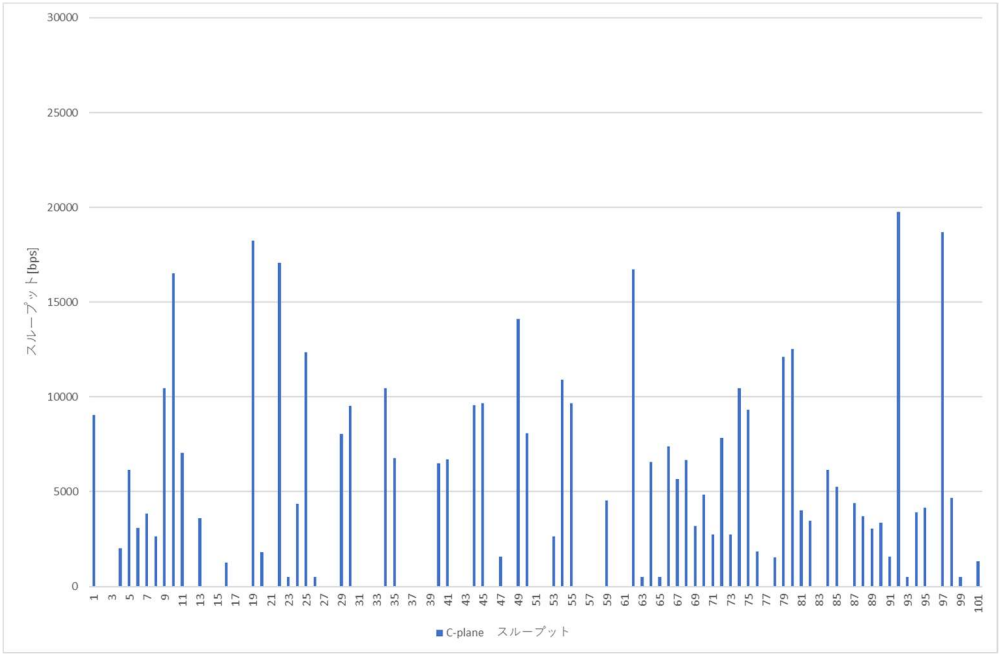


図 5-3-3　C-Plane スループット（UE30 台）

- アタッチのタイミングが重なることでピーク値に変動がみられるものの、最大ピーク値は30kbps に満たない数値でした。このことから本検証の環境下では複数企業共用パターンと業界共用パターンの別並びに接続する UE 数の変動は、C-plane に使用する帯域に大きな影響を与えないものと考えられます。
- 「業界共用パターン」において計測したところ、同様の傾向・結果が得られたため違いはありませんでした。

表 5-3-1　C-Plane スループット（全パターンの比較）

環境	UE 数	WAN 回線上の 使用帯域(ピーク)
複数企業共用パターン （コア＋CU 共用）	1 台	11,296bps
	10 台	17,040bps
	20 台	17,584bps
	30 台	19,776bps
業界共用パターン （コア＋CU 共用）	1 台	14,480bps
	10 台	28,528bps
	20 台	17,920bps
	30 台	22,224bps

4. 同期方式/準同期方式による影響

本項では、コア共用において同期方式/準同期方式の場合の影響等について説明します。

＜検証概要＞

- コア共用構成においても TDD の準同期方式のパフォーマンスが発揮できるか、伝送性能の変動等について検証しました。
- 本検証では、ローカル５Ｇのコアと CU を共用する構成において、TDD の準同期方式(総務省告示第 23 号別図第一号に規定された準同期方式のフレーム構成)を適用した場合の伝送性能について検証しました。
- 具体的には、コア共用モデルおよび無線フレームの同期タイミングの違いによるスループットや遅延時間への影響を確認しました。コア共用モデルは「複数企業共用パターン」及び「業界共用パターン」）２つのパターンについて比較検証しました。これらの環境の違い及び同期制御による伝送性能への影響について検証を行いました。

＜検証環境＞

- DL 方向（RU→UE）と UL 方向（UE→RU）の 2 方向について TCP/UDP スループット、遅延時間、ジッタ、パケットロスについて測定しました。
- 本手引書では、スループット及び遅延時間について説明します。

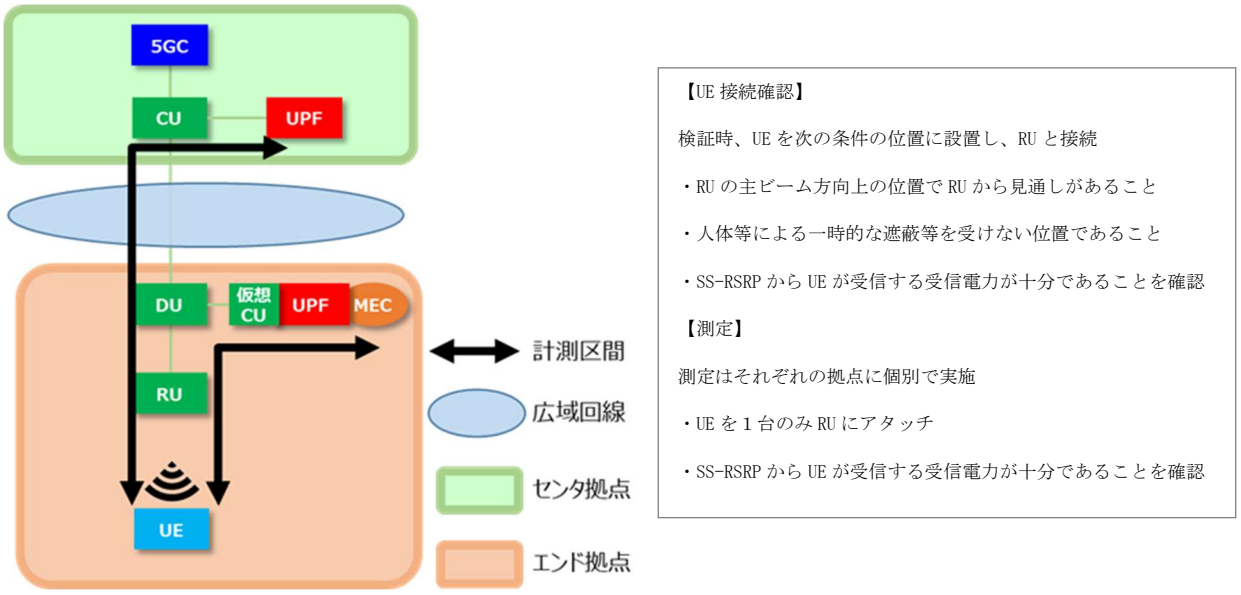


図 5-4-1　検証環境及び計測の前提条件

＜検証結果＞

① スループット

- TCP/UDP の UL スループットについて測定結果を比較します。平均値を算出すると同期方式の場合の TCP/UDP の UL スループット平均値は 64.2Mbps であったのに対し、準同期方式の場合は 123.5Mbps であり、準同期方式によって UL スループットが上昇していることが確認できました。特に UDP の UL スループットの平均値で比較すると、同期/準同期：65.1Mbps/130.0Mbps とほぼ 2 倍に上昇しています。

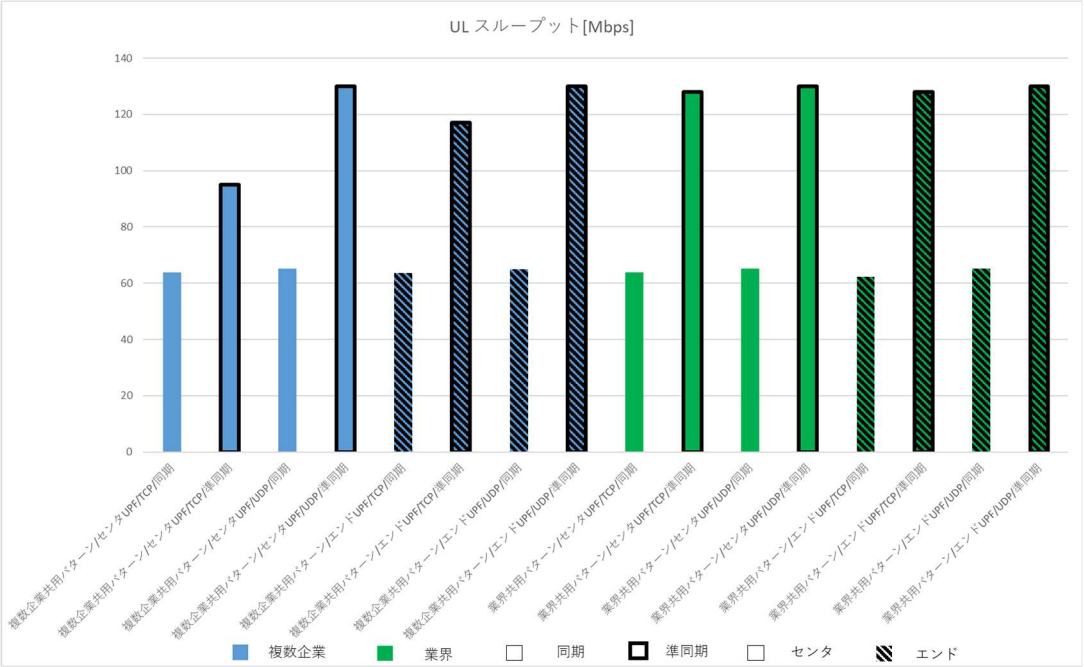


図 5-4-2　UL スループット比較

② 遅延時間

- 遅延時間について測定結果を比較します。複数企業共用パターン及び業界共用パターンの違い、センタ UPF 及びエンド UPF の違い、並びに同期方式及び準同期方式の違いに関係なく平均値の 31ms に対する差分が 4ms 以内であり、ほぼ差が見られない結果といえます。
- ジッタも同様にすべての結果が 1ms 程度であるため、環境及び同期方式/準同期方式の違いはネットワークのゆらぎに影響していないと考えられます。

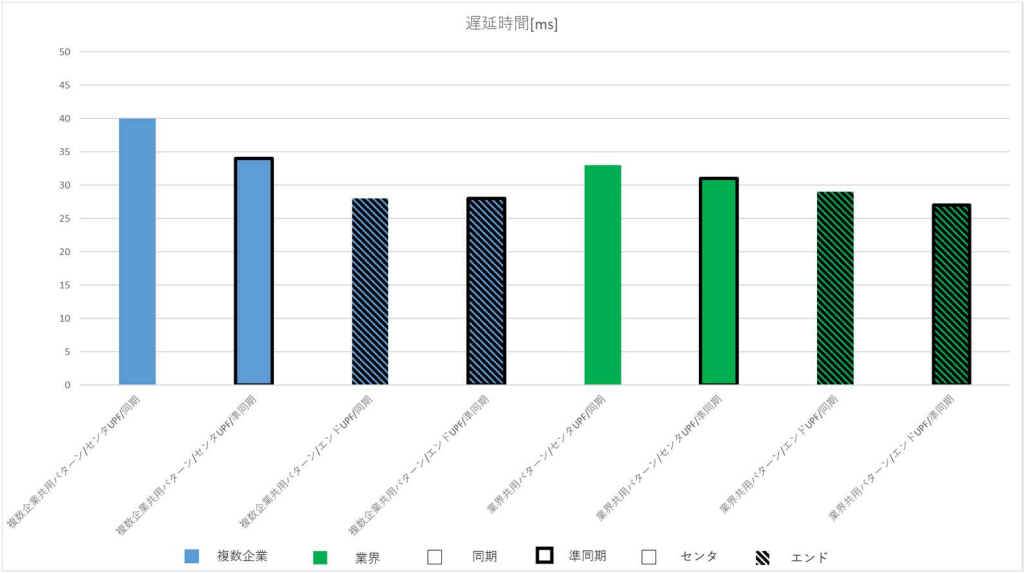


図 5-4-3　遅延時間比較

5. 性能要件に関するまとめ

本項ではコア共用に関する性能要件についてまとめます。SIer 等においては、ユーザと要件等について詳細に協議し、事前に必要な性能を確認した上で導入を行うことが肝要です。

① スループット

- 検証の結果から、コア共用形態における伝送性能はオンプレ型と比べて遜色ないものであることが確認できました。
- スループットについてはユーザの使用したいアプリケーションに応じて目標値を設定した上で目標値を満たすような機器選定、共用形態の選定、回線設計を行うことが重要です。
- アップリンクの比率を高めたい場合等、必要に応じて準同期 TDD 方式の選択を実施することが有効です。
- 大容量通信を目的とするユースケースでは、エンド拠点に UPF を設置して回線を圧迫しないようにすることが有効です。エンド拠点に UPF を設置できずセンタ拠点に UPF を設置する必要がある場合は、センタ拠点とエンド拠点を接続する拠点間回線にギャランティ回線を採用するといった回線設計への考慮が必要です。その際には、センタ拠点とエンド拠点の物理的な距離に応じて遅延時間が長くなる場合があることに留意する必要があります。
- 高いスループットが求められないユースケースにおいては、センタ拠点に UPF を設置する共用形態を取り、拠点間回線にベストエフォート回線を選択することでコストを抑えた実装が可能です。

② 遅延時間

- 遅延時間について、ユーザの使用したいアプリケーションに応じて目標値を設定し、目標に応じた共用形態の選定、回線設計を行うことが重要です。
- 遅延時間への要求が高く低遅延が求められるユースケースにおいては、エンド拠点へ UPF を設置することが推奨されます。エンド拠点に UPF を設置できずセンタ拠点に UPF を設置する必要がある場合は、センタ拠点とエンド拠点を接続する拠点間回線にギャランティ回線を採用するといった回線設計への考慮が必要です。その際には、センタ拠点とエンド拠点の物理的な距離に応じて遅延時間が長くなる場合があることに留意する必要があります。
- 低遅延性が求められないユースケースにおいては、センタ拠点に UPF を設置する共用形態を取り、拠点間回線にベストエフォート回線を選択することでコストを抑えた実装が可能です。

③ UE の同時接続台数と回線設計

- UE の同時接続台数について、予めユーザニーズを確認した上で台数と総スループットの目標値を設定し、目標値に合わせた機器選定、共用形態の選定、回線設計を行うことが重要です。
- エンド拠点に UPF を設置する場合は、センタ拠点とエンド拠点間の回線には C-Plane 通信しか流れず、UE 台数が増えても帯域の占有量は小さい(例 30 台でも数 10kbps 程度)ため、一般的な 100Mbps のベストエフォート回線等を用いても問題ありません。
- センタ拠点に UPF を設置し同じ回線内で C-Plane と U-Plane 通信を流す場合、U-Plane の通信は C-Plane と比較して大きな帯域を必要とするため、UE の接続台数と必要な C-Plane/U-Plane の総スループットを満たす回線の選定が必要となります。

1. 機能要件に関する概要

コア共用に係る機能要件について説明します。コア共用環境下における機能として必要と考えられる項目は下表のとおりです。

表 6-1-1　コア共用に係る機能要件

必要機能		用途
管理機能	SIM 認証の管理（SIM の登録/変更/閲覧(拠点毎に権限範囲を分ける等)）	新規端末の登録、既設端末の変更、通信端末の管理
	端末認証の管理（端末情報の閲覧等）	接続状態と通信状態の把握
	ポリシーの管理（登録/閲覧等）	端末に対するポリシーの設定及び管理
	セッションの管理	C-Planeの通信状況、認証判定結果等の確認
	ログの蓄積・管理（閲覧等）	システム状態の把握、トラブルシュート
トラフィックモニタリング		トラフィックモニタ、累積通信量の把握
在圏情報		接続先RU（PCI）の把握
ネットワークスライス		eMBB/URLLCをUE毎に指定しNW柔軟性を高める

① 各機能要素の共用

- 5GC は数多くの機能が定義されています。具体的には、登録・接続・移動管理（AMF）、セッション管理（SMF）、端末認証機能（AUSF）、SIM 番号管理（UDM）、ポリシー管理（PCF）等が挙げられます。

  - 登録・接続・移動管理（AMF：Access and Mobility Management Function）

    N2 インターフェースを終端し、登録管理 RM（Registration Management）、接続管理 CM（Connection Management）、移動管理 MM（Mobility Management）の機能を担います。AUSF 選択を行い、UE 認証手順を中継しセキュリティ・キーを管理します。セッション管理 SM のために SMF 選択を行い UE-SMF 間の SM メッセージを中継します。

  - セッション管理（SMF：Session Management Function）

    セッション管理 SM の機能を担い、UE への IP アドレス割当管理や UPF の選択・制御を行います。

  - 端末認証機能（AUSF：Authentication Server Function）

    UE 認証の機能を担います。

  - ポリシー管理（PCF：Policy Control Function）

    各種のポリシー・ルールを保持しポリシー実施のために C-Plane 機能を提供します。

- ローカル５Ｇのコア共用においては、これらの各要素の機能をどこまで共用可能か、共用するのかについても検討する必要があります。例えば、ネットワークスライス毎に構築する（共有しない）方法もあれば、企業内の SD-WAN と連携させる構成においては、UPF と SMF は 1 セットにする（スライスの中に構築する）など多様な構成が想定されます。

- ユーザから見た場合、コアを複数ユーザで共用する際は、システム運用や管理をユーザ毎に実施できる必要があります。特に求められる機能としてはSIM認証や端末情報管理等が挙げられます。
- また、コア共用下では、異なるユースケースが混在することが想定されるため、UEごとに異なるUPFを選択する等の自由度及び柔軟性の高い構成が望ましいと考えられます。
- マルチテナント型においては在圏情報やトラヒックモニタリング等の管理機能も求められます。

② ネットワークスライシング

- さらに、先進的なコア活用として、コアで異なる品質等の要件を有するサービスを共存させるため、アプリケーションによって大容量伝送や低遅延通信等、柔軟なネットワーク設計が可能なネットワークスライシング機能も有効と考えられます。
- ネットワークスライシングを用いる際は多様なユースケースに応じた通信品質の区分け等における有効性の確認が重要となります。
- そのため、ネットワークスライシングを導入することで、ローカル５Ｇシステムの共用環境下における柔軟性が高まります。アプリケーションによって所要性能が異なるUE端末を共用環境下で利用する場合、スライシング技術を用いて柔軟なネットワークを構成することが可能となりますので、今後の実装が期待されています。

2. 管理機能

本項では、実際の製品例を用いて、ローカル５Ｇシステムに関する管理機能の実用性について確認するとともに、管理機能の在り方等について説明します。

＜検証概要＞

- 監視や認証といった管理機能の在り方、アプリケーション毎に柔軟なネットワーク構成を実現するためのポリシー制御など、より高度なコア共用形態の実装を目指す必要があります。
- 本検証では、接続企業等の利用ユーザに関する顧客管理機能の実用性の検証を行い、コア装置の製品による顧客管理機能の違いを比較考察しました。

＜検証環境＞

- 以下の機能を本検証環境において利用可能であることを確認しました。特に、拠点ごとに区切られて情報の閲覧登録が出来ることを確認しました。

  ・SIM 認証の管理状況: Web GUI 上のメニュー上での SIM の登録・変更・削除を実施

  ・端末認証の管理状況：5GC との接続状況に基づき、基地局と端末の通信状態を確認

  ・ポリシーの管理状況：Web GUI 上のメニュー上での 5GC のポリシーに基づく 5QI[3]を設定

  ・セッション管理の管理状況：Web GUI 上のメニュー上でのセッション状態を確認

  ・ログの蓄積・管理状況：Web GUI 上のメニュー上でのログやアラーム等の確認

  ・管理権限の設定状況：SIM 情報等の操作・閲覧管理ができることを確認

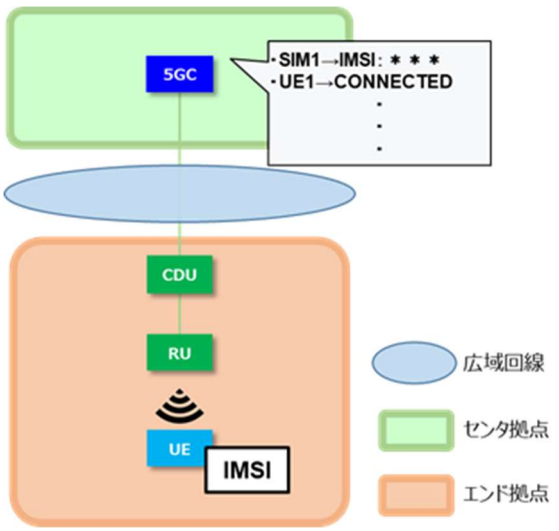


図 6-2-1　検証環境及び計測の前提条件

[3] 5G QoS Identifier

＜検証結果＞

① SIM 認証の管理

- SIM 認証の管理状況は Web GUI 上のメニューから編集し、SIM 固有の IMSI、OPc 値及び K 値並びに AMBR 値(最大可能ビットレート)、DNN、割当 IP アドレスを追記し、SIM 登録・変更・削除等が可能です。下図は例です。

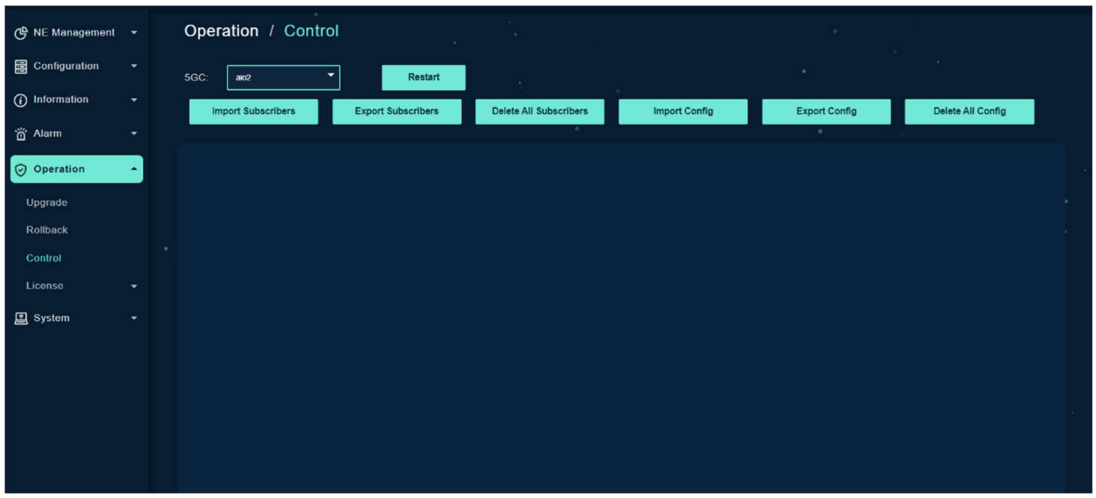


図 6-2-2　SIM 認証の管理（例）

② 端末認証の管理

- 端末認証の管理状況は、端末が 5GC に接続している状態を表す情報であり、WebGUI 上のメニューから確認できます。基地局と通信状態の場合は「CONNECTED」、通信がない状態は「IDLE」と表示されます。5GC にアタッチしていない端末は表示されません。この機能によって現在利用中の端末を確認することが可能です。下図は例です。

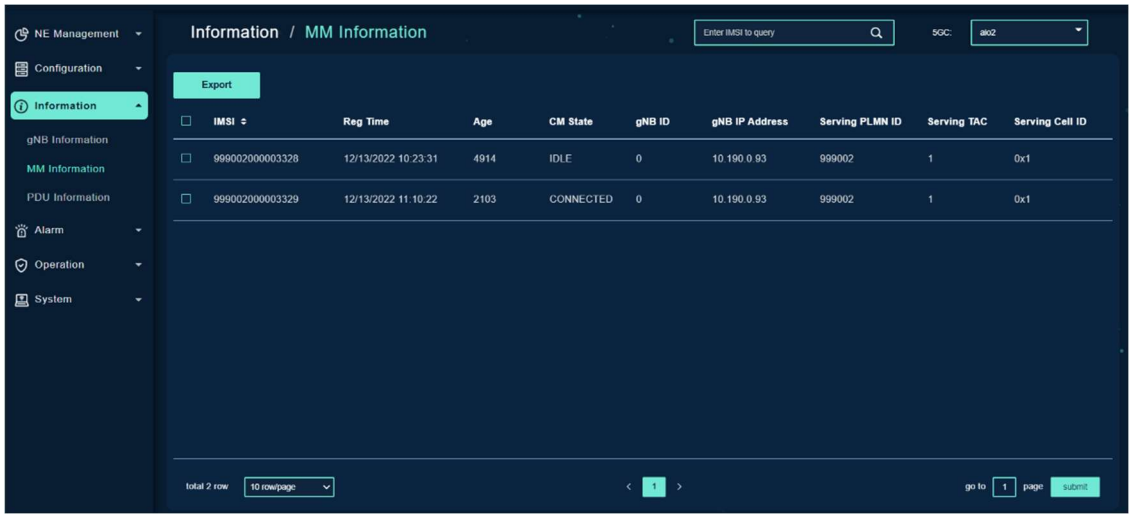


図 6-2-3　端末認証の管理（例）

③ ポリシーの管理状況

- ポリシーの管理状況は、WebGUI 上のメニューから QoS Profile を選ぶことで確認できます。5GC のポリシーとして 5QI を設定することが可能です。下図は例です。

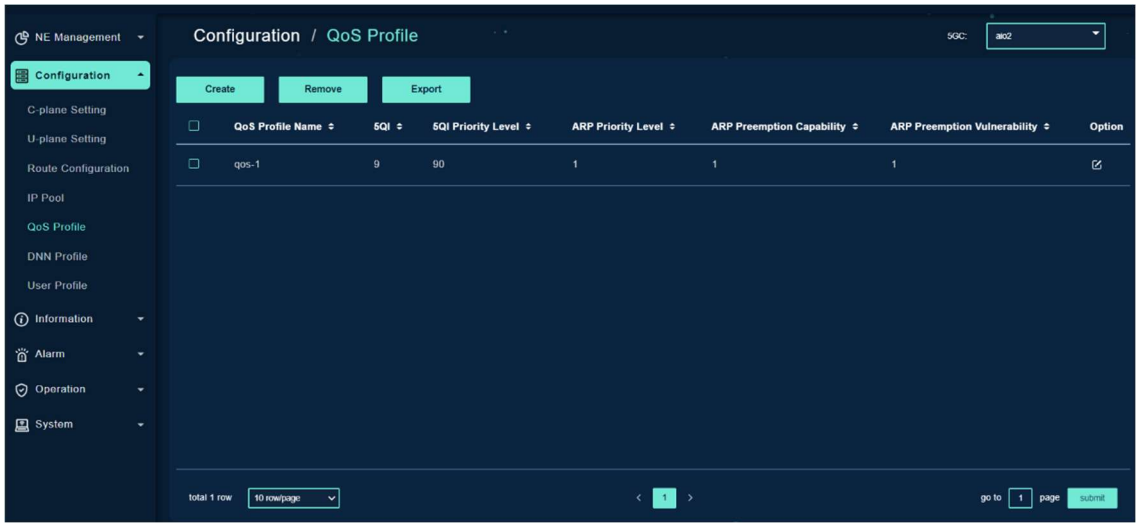


図 6-2-4　ポリシーの管理状況（例）

④ セッション管理の管理状況

- セッションの管理状況は、WebGUI 上のメニューから確認でき、セッションの状態として ACTIVE あるいは INACTIVE を表示されます。セッションで N3 の接続相手の CU を Remote N3 Address から確認できます。下図は例です。

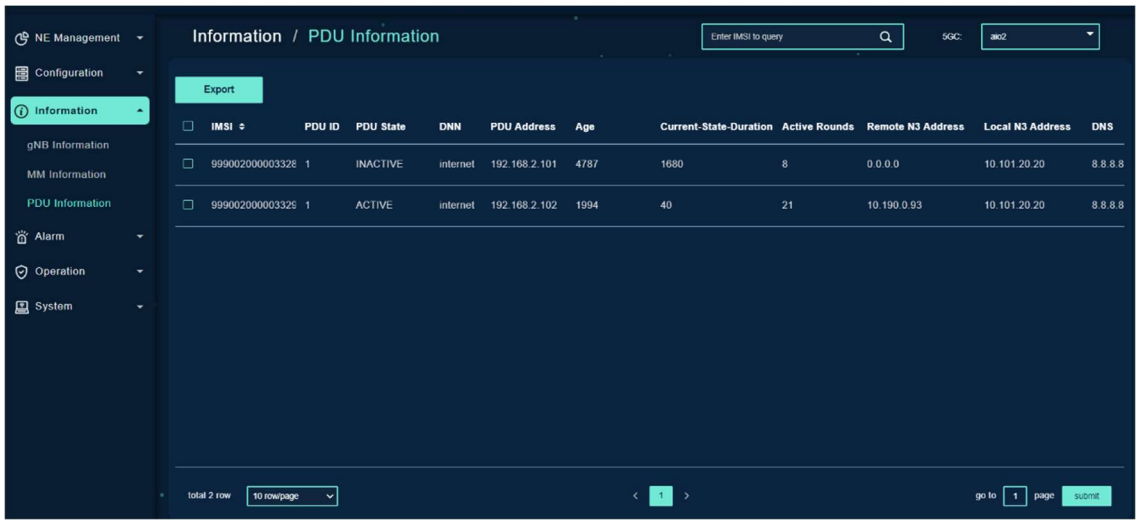


図 6-2-5　セッション管理の管理状況（例）

⑤ ログの蓄積、管理状況

- ログの管理状況は、WebGUI 上のメニューから、ユーザが行った操作のログを確認できます。また Alarm を選ぶことで 5GC が検知したアラームや、故意に CDU を停止し、警報を表示させることもできます。下図は例です。

図 6-2-5　ログの蓄積、管理状況（例）

⑥ 管理権限の設定状況

- 前段までの操作・閲覧を行う際は、Web ブラウザに指定の URL を入力し、UserName と Password を入力しログインします。URL、UserName 及び Password によって拠点ごとに SIM 情報等の操作・閲覧管理が可能であることを確認しました。

3. トラヒックモニタリング

本項では、複数の UE のトラヒックモニタリングについて確認するとともに、同機能の在り方等について説明します。

＜検証概要＞

- マルチテナント型等におけるローカル５Ｇネットワークの運用においては、トラヒックモニタリングに係る管理機能が求められます。
- 本検証では、ローカル５Ｇ通信状況を把握・管理する機能について検証として、複数の UE での通信状況やアップリンク/ダウンリンクの互いの通信への影響等について検証しました。
- 具体的には、UPF の設置位置、製品の違いに着目しました。「センタ UPF」と「エンド UPF」について比較検証しました。また、共用の対象（ユースケース）については「複数企業共用パターン」及び「業界共用パターン」）２つのパターンについて比較検証しています。これらの環境の違い及びローカル５Ｇのシステム構成による比較・考察しました。

＜検証環境＞

- 本検証では、通信状況の把握・管理機能確認の検証を行いました。
- 以下の手順で通信状況管理機能を確認しました。

  ・UE1 台での通信状況

  ・UE2 台での通信状況

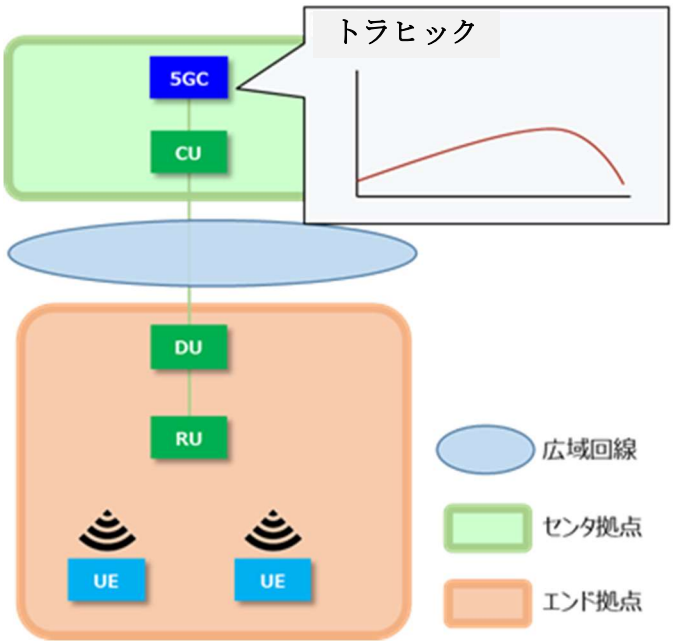


図 6-3-1　検証環境及び計測の前提条件

＜検証結果＞

- UE２台を接続しセンタ UPF と UDP での通信を発生させたときのトラヒックモニタリング画面で確認しました。一方の UE でセンタ UPF→UE 方向の DL の通信を発生させ、他方の UE で UE→センタ UPF 方向の UL の通信を発生させました。各グラフの下には各 UE の IMSI が表示され、グラフの色によってどちらの UE で通信が発生しているかを確認できます。
- TCP の場合には UDP と比べると DL を発生させたときにも UL 方向の通信が発生し、UL を発生させたときにも DL 方向の通信が発生していることが確認できます。

図 6-3-2　複数企業共用パターン　UE２台(センタ UPF　UDP)

図 6-3-3　複数企業共用パターン　UE２台(センタ UPF　TCP)

- UE とエンド UPF とで通信を発生させたときも、センタ UPF と同様にトラヒックモニタリング機能によって通信状態を確認することができました。
- TCP の場合には UDP と比べると DL を発生させたときにも UL 方向の通信が発生し、UL を発生させたときにも DL 方向の通信が発生していることが確認できました。

4. 在圏管理

本項では、DU 管轄内の端末情報の閲覧等（在圏管理）の機能についてについて確認するとともに、同機能の在り方等について説明します。

＜検証概要＞

- コア共用において、端末の接続状態等の在圏管理が求められます。
- 本検証では、DU の管轄内の端末情報の閲覧等の機能について検証しました。

＜検証環境＞

- 本検証では、DU 管轄内の端末情報の閲覧等の機能について検証しました。
  - ・１台の RU に 1 台の UE を接続して在圏情報を確認
  - ・１台の RU に 2 台の UE を接続して在圏情報を確認
  - ・2 拠点の RU にそれぞれ UE を接続し、在圏情報を確認

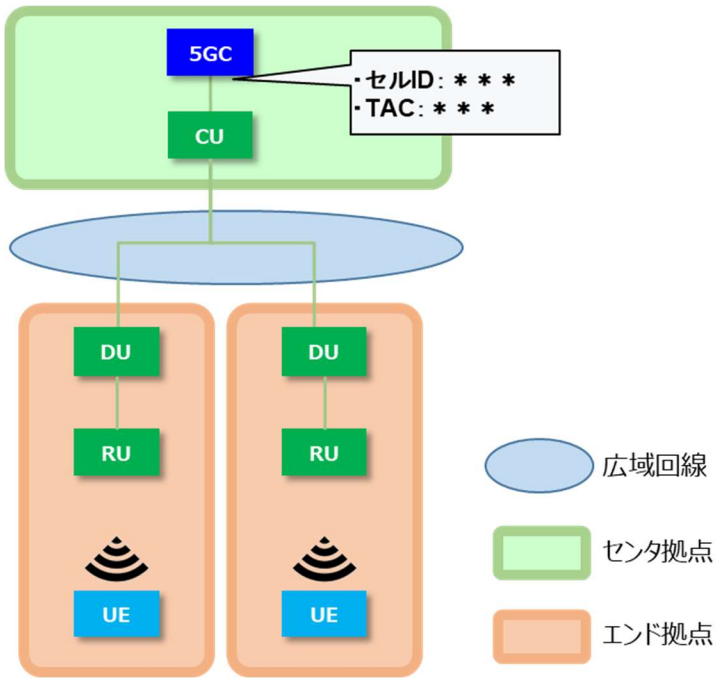


図 6-4-1　検証環境及び計測の前提条件

＜検証結果＞

- 在圏機能が WebGUI によって閲覧できることを検証しました。WebGUI 上のメニューから、端末が接続している gNB は gNB ID 及び gNB IP Address によって判別することができ、gNB に対する在圏確認機能として使用することができます。
- 在圏機能は拠点に応じて表示する画面を切り替えます。そのため拠点ごとに UE の在圏を確認することができます。

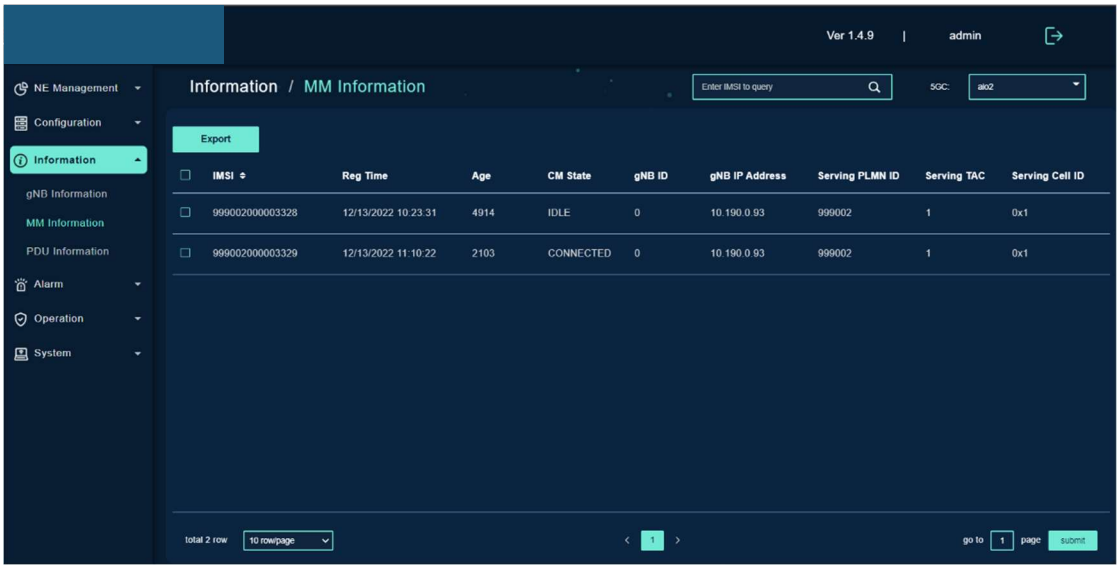


図 6-4-2　在圏機能の閲覧（例）

5. ネットワークスライス

＜検証概要＞

- ネットワークスライスの実現に向けて、ネットワークスライシングの特性評価として、UPF 配置の影響、アプリ要件毎の影響等に配慮した設定や通信品質の検証を行う必要があります。
- 本検証では、ネットワークスライスの設定（eMBB/URLLC）、ネットワークスライスを設定した状態での通信品質確認、各スライスの同時通信に関する検証を行いました。
- 具体的には、コア共用モデルと UPF の設置位置の違いに着目しました。コア共用モデルは「複数企業共用パターン」及び「業界共用パターン」）2 つのパターンについて比較検証しました。UPF の設置位置については中央に設置して共用する「センタ UPF」とユーザのローカル拠点に設置する「エンド UPF」について比較検証しました。これらの環境の違い及びローカル５Ｇのシステム構成による通信性能について比較・考察しました。

＜検証環境＞

- 本検証では、以下を確認しました。
  - ・eMBB と URLLC の設定
  - ・eMBB と URLLC の通信品質：スループット、遅延時間、パケット損失率、ジッタ
  - ・2UE の同時通信による通信品質：スループット、遅延時間、パケット損失率、ジッタ

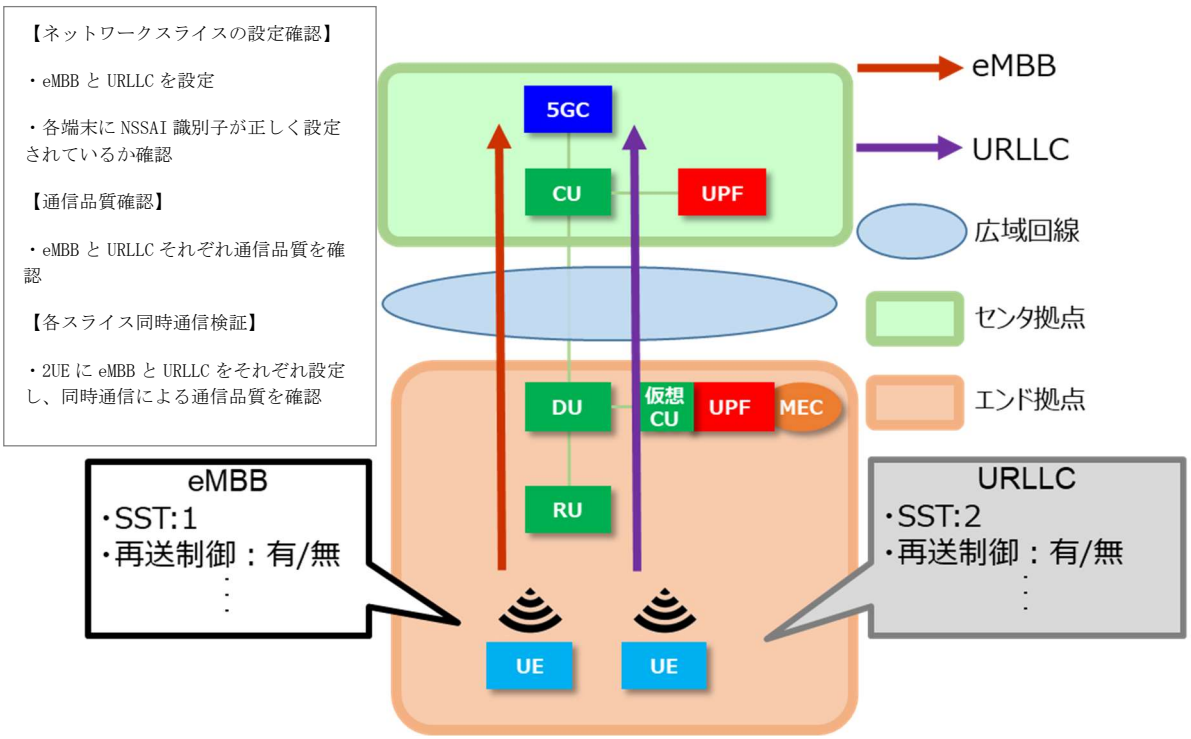


図 6-5-1　検証環境及び計測の前提条件

＜検証結果＞

① eMBB 機能

- eMBB に設定した UE１台を接続し、スループットを検証しました。eMBB のスループットは DL で 700Mbps 程度でした。
- eMBB に設定した UE１台を接続し、遅延時間を検証しました。複数企業共用パターン及び業界共用パターンの別並びにセンタ UPF 及びエンド UPF の別に関係なく、ほぼ同程度という結果でした。

② URLLC 機能

- URLLC に設定した UE１台を接続し、スループットを検証しました。
- URLLC のスループットは eMBB のスループットとほぼ同様の結果でした。

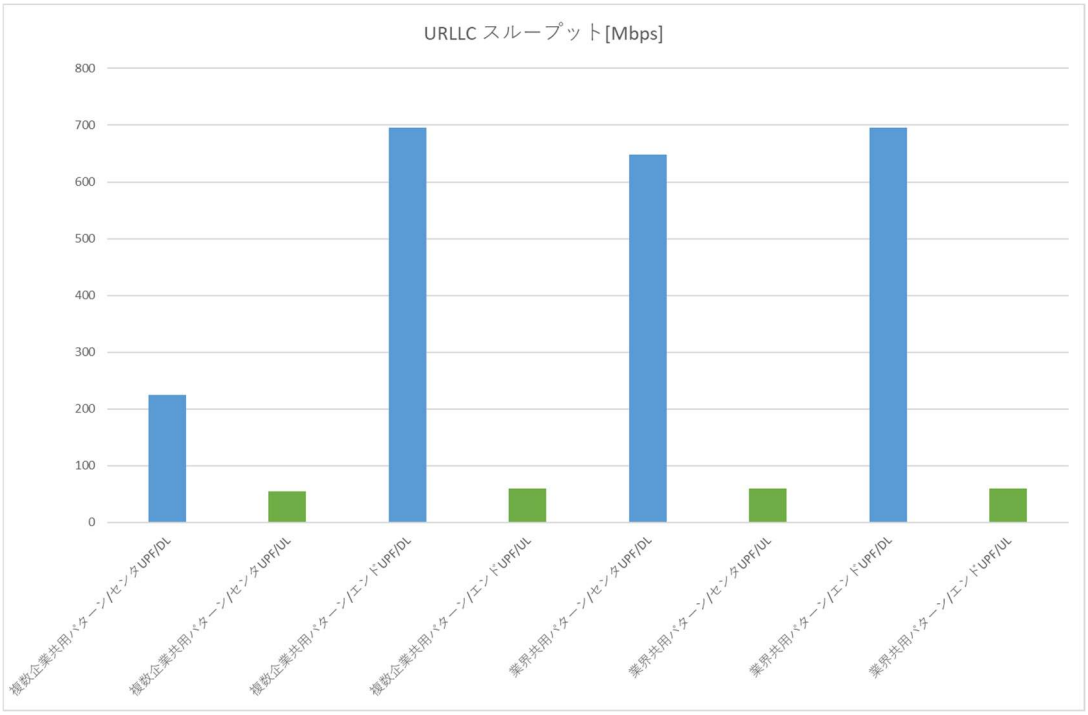


図 6-5-2　URLLC スループット検証結果

- URLLC に設定した UE１台を接続し、遅延時間を検証しました。
- 複数企業共用パターン及び業界共用パターンの別並びにセンタ UPF 及びエンド UPF の別に関係なく、ほぼ同程度という結果でした。

③ eMBB/URLLC 同時接続

- eMBB に設定した UE 1 台及び URLLC に設定した UE 1 台を同時に接続し、スループットを検証しました。
- スループットの数値は性能検証等と比べて低い値となりました。検証時点ではネットワークスライス機能において eMBB/URLLC 同時接続の設定は開発段階であり、使用可能なリソースブロック数及び変調方式に制限があるためです。本検証では eMBB のリソースブロック数を 200、URLLC のリソースブロック数を 73 に設定し、変調方式は QPSK を用いました。そのため性能検証時と比べて eMBB では 3 割程度、URLLC では 1 割程度までスループットが低下し合計で 300Mbps 弱という結果でした。
- また複数企業共用パターンのセンタ UPF 環境では合計のスループットが他の環境を下回っています。これはベストエフォート回線によって通信帯域に制限を受けたためと考えます。

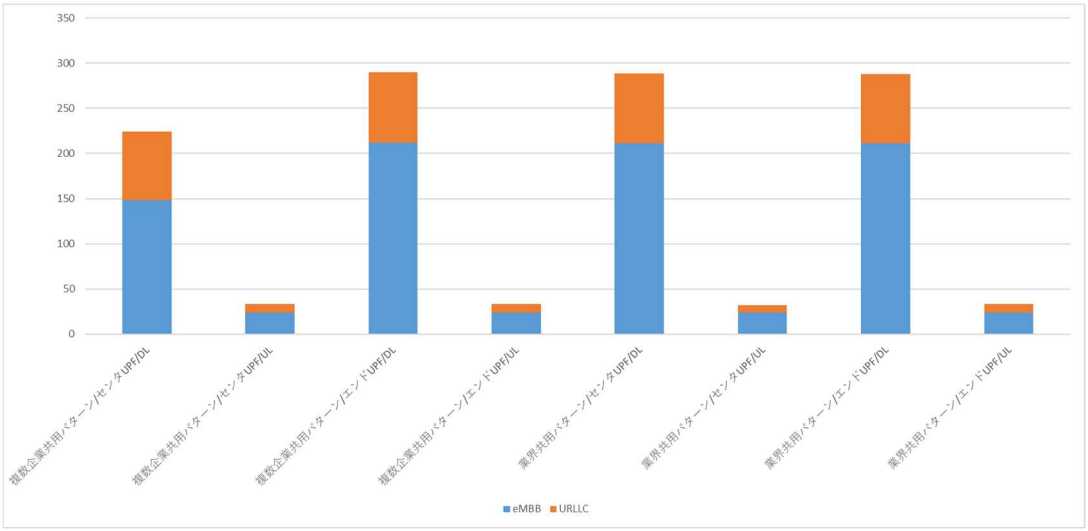


図 6-5-3　eMBB/URLLC 同時接続検証結果（スループット）

- eMBB に設定した UE 1 台及び URLLC に設定した UE 1 台を同時に接続し、遅延時間を検証しました。
- 遅延時間の平均値は 27ms であり、複数企業共用パターン及び業界共用パターンの別、センタ UPF 及びエンド UPF の別並びに eMBB 及び URLLC の別に関係なく、ほぼ同程度という結果でした。

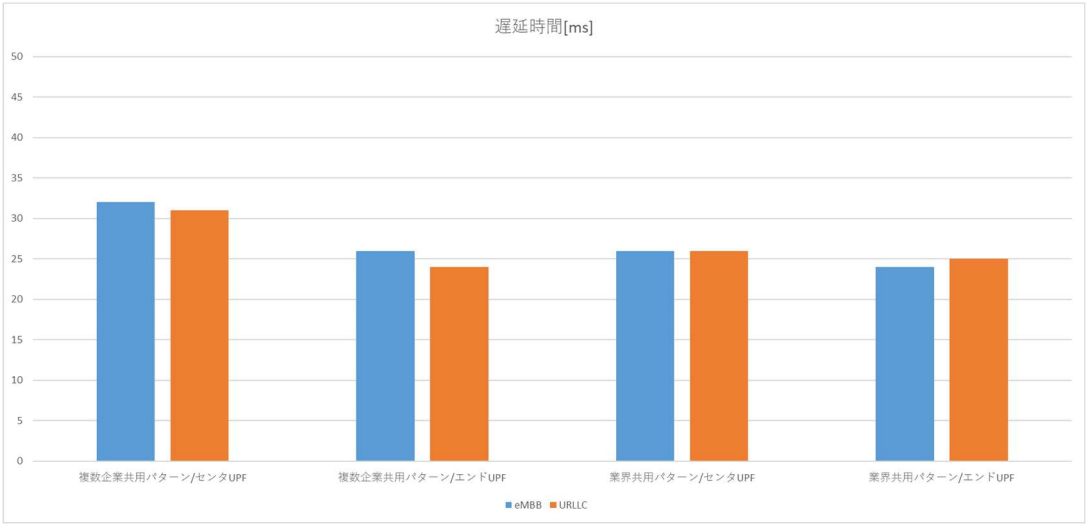


図 6-5-4　eMBB/URLLC 同時接続検証結果（遅延時間）

4. 機能要件に関するまとめ

本項ではコア共用環境下におけるローカル５Ｇシステムの各機能に求められる要件についてまとめます。SIer 等においては、ユーザと要件等について詳細に協議し、事前に必要なセキュリティ対策を決めることが肝要です。

① 管理機能等

- コア共用の環境下でローカル５Ｇシステムを管理運営するにあたり、必要な機能が 2 社の機器の双方で実装されていることを確認しました。
- SIM 認証管理は、IMSI 番号などの SIM 情報、暗号化情報等の登録及び閲覧を行うための機能です。コアへ UE の追加登録、登録変更、登録削除を行い、UE をローカル５Ｇシステムで利用可能とするために不可欠な機能です。SIM 認証管理をコア共用サービスとして提供する SIer が担う想定の場合、例えば UE の接続可否を利用シーンに応じて柔軟に変更するといったユースケースでは、ユーザ企業等自身が直接 SIM 認証を管理することを望むケースも考えられます。今後の開発によって、SIM 認証機能のみを分離してユーザ企業がエンド拠点で利用することで、ユースケースに対する更なる柔軟性の向上が期待できます。また、操作性の向上が実現することで運用時の利便性がさらに増すものと期待できます。
- 端末情報管理及びセッション管理は、SIM 認証管理機能によって登録された SIM を実装した UE について、接続状態であるか否か、通信中であるか否かを表示することで UE の運用実態を確認できる機能です。例えば監視カメラのように、特定の UE に対して定常的に接続中及び通信中であることを要求するユースケースでは、本機能を元に監視体制を構築することで、システムの正常性確認に有効であると考えられます。また、本検証では IMSI 番号によってどの UE であるかを識別しています。UE が多種類存在するユースケースでは、UE の型名や外観等を登録したデータベースと連携することで、どの UE に関する端末情報及びセッション情報であるかが、視覚的に区別できると考えられます。このように監視体制等との連携や GUI のデザインをユースケースに応じて工夫することで、将来的に運用時の利便性がさらに増すものと期待できます。
- ポリシー管理は、エンド拠点ごとまたは UE ごとにネットワーク上の挙動を制御するためのポリシー設定を行う機能です。例えば、単信音声のようなユースケースでは、リアルタイム性が要求されますが小容量の通信が主となります。対してセンサ類に蓄積したログを一括で送出するようなユースケースでは大容量の通信が主となります。これらの多様なユースケースに対し、適切なポリシーを設定することで柔軟なネットワーク構築でのユーザニーズへの対応が期待できるものと考えます。また本検証で確認できたポリシー設定は限定的であったため、今後の開発・検証によって多様なポリシーに対応した高機能化の実現が望ましいと考えられます。
- 管理権限は、コア等を共用した環境下において複数のエンド拠点を個別に管理するため、コアの各機能へのアクセス権限をエンド拠点ごとに分離する機能です。本検証ではコアへのログイン画面、Username、Password によって実現しています。ユーザによってはユーザ自らによるコアの操作を最小限とし、例えばポリシー管理などは SIer に委任することを望むことが考えられます。そういったユーザニーズに対応するため、ユーザ向け管理画面と SIer 向け管理画面をそれぞれ用意するなど、今後の高機能化が望ましいと考えられます。

② トラヒックモニタリング

- 2 社の機器では、トラヒックモニタリングについて、機能上の差がありますが、それぞれ特徴があるため、用途や運用方法等に応じて選択することが有用です。
  - ✓ 機器例１：スループット及びパケットダイヤグラムを UE(IMSI 番号)ごとに色分けされたグラフによって表示することが可能です。またグラフのピークに応じて縦軸のスケールが自動的に追従します。そのため UE ごとの時単位や分単位といった短期的な通信量の変動を確認することに適しています。
  - ✓ 機器例２：エンド拠点(CU)におけるスループットの総量をグラフによって表示することが可能です。縦軸スケールが固定であり、拠点における日単位や月単位といった長期的な通信量の変動の確認に適しているといえます。
  - ✓ 両機器とも UPF の通信ポートにおけるスループットに相当する数値をグラフ化しています。そのため、DL ではトラヒックモニタ機能でグラフ表示されたスループットと実際に UE へ到達しているスループットが乖離している可能性があることに注意が必要です。
- トラヒックモニタリング機能は、コア等を共用した環境をサービスとしてユーザへ提供する SIer にとっては、ユーザごとの通信量に応じた従量課金システムの構築において必要になると考えられます。また、エンド拠点で端末を運用するユーザにとっても UE またはローカル５G システムの運用実態を確認するために有効な機能です。
- このように、トラヒックモニタリング機能は、ユーザニーズ及び SIer のニーズが高いと考えられることから、グラフ表示のデザイン工夫や通信量の統計といった機能の追加によってさらに実用性が向上することを期待されます。

③ 在圏機能検証

- 在圏機能は、接続中のある UE がどの拠点のどの基地局と接続しているか確認する機能です。
- 実際に、2 社の機器の双方で接続中の UE（IMSI 番号）がどの基地局 ID と接続しているか表示する機能が実装されていることを確認できました。
- 本機能は、拠点ごとに UE 接続数を把握することで、コア等を共用した環境をサービスとしてユーザへ提供する SIer は利用者数に応じた従量課金システムの構築に必要であると考えられます。
- また、基地局と UE の通信の正常性確認や複数の基地局がある拠点ではハンドオーバー機能の確認及び管理をすることができます。さらに基地局の利用率について統計を取ることによって、基地局の再配置検討に有効な情報を取得できます。UE の大まかな位置を取得することにも利用できるなど、今後、ユースケースに応じて柔軟に高機能化されていくことが望ましいと考えます。

④ ネットワークスライシング

- ネットワークスライス機能は、物理的なネットワークを仮想的に複数のネットワークに分割し、それぞれのスライスに必要な通信機能を提供することで、異なるアプリケーションに対して必要な通信品質を実現する機能です。
- 検証では、eMBB(Enhanced Mobile Broadband：大容量・広帯域通信)及び URLLC(Ultra-Reliable Low-Latency Communications：超高信頼性・低遅延通信)の機能が実装されていることを確認しました。
- 遅延時間を重要視するユースケースにあっては、ネットワーク高負荷下でも遅延時間を保持できる URLLC が有効であることを確認できました。ただし、WAN 回線を経由するセンタ UPF ではバースト的に増加するスループットを再現できない可能性があることについても確認しました。

1. セキュリティ要件に関する概要

本項では、コア共用に係るセキュリティ要件および効果的な対策について説明します。

ネットワークセキュリティについて

- 拠点内で全ての通信が完了するオンプレの構成と異なり、コア共用下においては拠点間通信が発生するため、外部からの侵入や不正な通信に対するセキュリティ上のリスクが生じます。また、多くのユーザを共通のコアに収容することから、メンテナンス時のシステム停止などが全ユーザに波及することの認識、対策が必要となります。
- セキュリティの在り方は、例えば UPF や MEC を設置する場所にも依存します。エンド UPF を設置する場合、特にエンド UPF からインターネットに接続する場合はインターネットからの攻撃を防ぐために FW装置等を実装する等が想定されます。また、MEC をユーザで用意する場合、ユーザ施設内の MEC のセキュリティは、ユーザの範疇の対応が必要となります。
- 一方で、こうしたケースにおいては、ユーザにセキュリティリスクをお伝えした上で、セキュリティソリューションも含めてご提案する、またはセキュリティが担保できる状態でサービスをご提供する必要があります。接続（通信サービス）の観点では、セキュリティも含めてトータルで考えることが肝要であるため、セキュリティをどちらが担保するかが課題となります。
- また、5GC を保有した場合には、マルチテナントで提供する形では UDM を共用する形態が想定されます。つまり、基地局で報知される PLMN は同じ情報になり、A 企業/B 企業といった別の企業が 5GC を共有して利用する場合、SIM の情報として同じ PLMN が見えてしまえば、基地局にアタッチしようとする動作はするため、そのような点に対する IMSI のトラッキングや暗号化も含めて考える必要があります。

デバイス側のセキュリティについて

- デバイス側のセキュリティも重要です。例えばローカル５Ｇでは人手がないところで、無人化施工等のユースケースが想定されます。デバイス抜き差し等されるリスクも考えられます。加えて、システム構築や運用時には、通信情報の漏洩、登録ユーザや端末情報の漏洩、異常トラヒックや悪意ユーザトラヒックによるシステムへの影響等について考慮する必要があります。
- 端末からの攻撃を監視するには、センタ UPF/エンド UPF それぞれの N3 インターフェースにトラフィック監視装置を設置し、不正通信発生時には必要に応じて端末へのペナルティ(５Ｇからの切断)を適用する等の対策が想定されます。

コア共用環境において想定される具体的な攻撃の種類

- 上記内容から、コア共用環境下におけるセキュリティ攻撃は以下の 4 つに大別されます。

  ①　エンド拠点とセンタ拠点間に拠点が分かれることに起因する攻撃

  ②　攻撃者に乗っ取られたローカル５Ｇ構成要素から他の機器への攻撃

  ③　端末および SIM を悪用する攻撃

  ④　インターネットからの攻撃

- このうち「④インターネットからの攻撃」については一般的なインターネットに接続されるLAN ネットワークのセキュリティと同様、UTM 等によるセキュリティ対策が有効です。コア共用環境特有ではないため本技術的手引書では割愛いたします。

- 「①センタ拠点とエンド拠点に拠点が分かれることに起因する攻撃」について、拠点内で全ての通信が完了するオンプレの構成と異なり、コア共用下においては拠点間通信が発生するため、外部からの侵入や不正な通信に対するセキュリティ上の懸念が生じます。具体的にはコアへの侵入/通信の傍受、コアを共用する異なる拠点への不正通信攻撃が想定されます。
- これらの攻撃に対する対策としては IPsec による拠点間通信の暗号化が効果的であり、IPsec を構成するための鍵交換手法として広く用いられている Diffie-Hellman 方式の他に量子暗号鍵交換方式がコア共用環境下で利用可能であることが検証により確認されています。

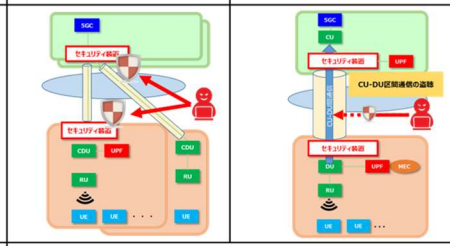
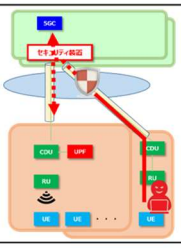
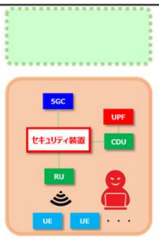
	センタ拠点とエンド拠点に拠点が分かれることに起因する 外部からの攻撃に対するセキュリティ			(参考)オンプレ構成
攻撃の種類	ローカル５Gシステム外部からの攻撃			-
想定攻撃例	コアへの侵入/通信の盗聴 (コア共用)	CU-DU区間通信の盗聴 (コア+CU共用)	コア共用する異なる拠点への攻撃	コア共用構成をとることによる新たなセキュリティホールは想定されない
攻撃のイメージ				
攻撃によって もたらされる影響	コアからの攻撃への踏み台として利用される 端末情報やSIM情報の漏洩/ユーザ通信の漏洩		異なる拠点への攻撃や通信の傍受	-
対策方法	Diffie-Hellman方式(DH方式)/量子暗号鍵交換方式で構成されたIPsecによる暗号化			
結果	IPsecの認証機能/暗号化機能により拠点間通信の傍受と不正な接続が防げた			
考察	・センタ拠点のセキュリティ装置として仮想アプライアンス製品１台を複数ユーザで共用することでコストが抑えられる ・エンド拠点にはIPsec機能を有するセキュリティ機器のみを設置することでコストを抑えられる			

図 7-1-1　①センタ拠点とエンド拠点に拠点が分かれることに起因する攻撃の概要

- 「②攻撃者に乗っ取られたローカル５Ｇ構成機器から他の機器への攻撃」については以下の攻撃が考えられます。

  ・AMF を操作する N2 通信に対する DoS 攻撃 / 不正パケットの送信(N2)

  ・不正な GTP-U によるフレームを送信することで不正なデータ通信を行う攻撃(N3)

  ・SMF＋UPF に対するセッション情報の書き換え攻撃 / 不正パケットの送信(N4)

  ・データベースエントリの操作または流出を目的とした攻撃(SBA)

- これらの攻撃について、各インターフェース(N2/N3/N4/SBA)に適切な Firewall 機能を具備することにより防げることが検証で確認されています。

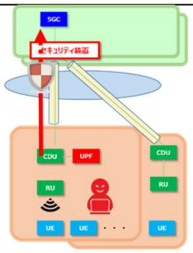
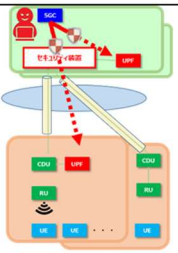
	攻撃者によって乗っ取られたローカル５Gシステム内部からの 不正通信等の攻撃に対するセキュリティ	
攻撃の種類	ローカル５Gシステム内部からの攻撃	
想定攻撃例	コアへのDoS攻撃/不正なデータ通信 等	セッション情報の書き換え・削除 等
攻撃のイメージ IPsecトンネル 広域回線 センタ拠点 エンド拠点 検証する攻撃 攻撃者		
攻撃によって もたらされる影響	サービスの停止/通信の傍受	セッションの乗っ取り(中間者攻撃)
対策方法	Firewallによる遮断	
結果	各ファンクション通信に対応したFirewall機能によって各攻撃が検知・遮断できた	
考察	・センタ拠点のセキュリティ装置として仮想アプライアンス製品１台を複数ユーザで共用することでコストが抑えられる ・エンド拠点にはIPsec機能を有するセキュリティ機器のみを設置することでコストを抑えられる	

図 7-1-2　②攻撃者に乗っ取られたローカル５Ｇ構成機器から他の機器への攻撃の概要

- 「③端末を悪用した攻撃」は端末からのコアネットワーク装置の乗っ取り、不正な URL アクセス等の不正な U-Plane 通信、SIM の差し替え等が想定されます。このうちコアネットワーク装置の乗っ取りについては②の Firewall での対策が有効です。その他 U-Plane の通信および SIM の差し替えについては、以下図のとおり、セキュリティ機能付き SIM/監視装置/端末管理装置を用いて不正通信発生時に端末をネットワークから分断する等の対策をとることの有効性が確認されています。
- また、数多くの端末の接続が想定されるローカル５Ｇにおいては、不正な通信を行った端末への対応稼働の負荷が想定されるため、それら管理稼働削減のための接続端末の可視化方法の検証も必要となります。こちらについては端末を用途に合わせて分類し、分類ごとにセキュリティポリシーを定めた運用を行うことで効率的な管理が可能と言えます。この課題についても、セキュリティ機能付き SIM/監視装置/端末管理装置を用いることの有効性が検証により示されています。

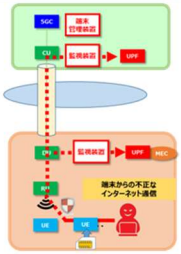
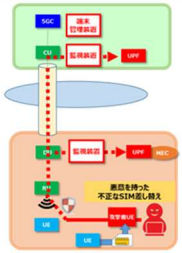
	端末の不正利用やSIMの不正利用に対するセキュリティ	
攻撃の種類	端末からの攻撃	
想定攻撃例	端末からの不正なインターネット通信	悪意を持った不正なSIM差し替え
攻撃のイメージ IPsecトンネル 広域回線 センタ拠点 エンド拠点 検証する攻撃 攻撃者		
攻撃によって もたらされる影響	端末のウイルス感染/セキュリティインシデント発生による社会的影響	エンド拠点ネットワークへの不正な侵入による情報漏洩やネットワークの他の端末への攻撃
対策方法	セキュリティ機能付きSIM、監視装置、端末管理装置による通信の検知	
結果	・セキュリティ機能付きSIMの機能で拠点毎/端末毎に通信を監視し、不正な通信やSIMの不正入れ替えの発生時にはそれを検知・遮断し、セキュリティポリシーに応じて端末の隔離ができることを確認	
考察	・コア/CU共用環境下において監視装置および端末管理装置を複数ユーザで共用することが可能だが、エンドUPFを使う場合はエンド拠点にも監視装置を設置する必要がある ・役割の重要性や通信の特性に応じて端末を分類し、分類ごとに適切なセキュリティポリシーを設定することで柔軟に多数の端末の管理が可能	

図 7-1-2　③端末を悪用した攻撃の概要

2. CU-DU 区間通信の暗号化

本項では拠点間通信の暗号化の参考として、Diffie-Hellman および量子暗号鍵交換方式を用いた CU-DU 区間通信の暗号化に関する検証結果を記載します。

＜検証概要＞

- オンプレミス構成においては CU-DU 区間の通信は暗号化されないことが一般的です。しかし、本調査検証においては CU を複数ユーザで共有し異なる拠点に設置する構成をとるため、CU-DU 区間が遠隔での通信となり経路上での盗聴のリスクがあります。
- CU-DU 区間を流れる通信には、端末認証情報等の重要情報が含まれているため、3GPP では CU-DU 区間には認証・権限付与、完全性保護、機密保持が必須であると定義されています。（文書番号：ETSI TS 133 501 V15.2.0 (2018-10)）
- 本調査研究では CU-DU 区間の通信に IPsec を用い、その効果を確認しました。IPsec の鍵交換においては Diffie-Hellman 方式（以下、DH 方式)を採用しました。また、さらに高度なセキュリティを求めるユーザを想定して、量子暗号鍵交換方式の有効性についても検証を行いました。
- 通常、量子暗号鍵交換方式を用いる際は各拠点のオンプレミス環境にセキュリティ製品を導入し、拠点間を光ファイバーで直接接続することが必要ですが、本検証では検証用に準備されたパブリッククラウド上で交換・生成した量子暗号鍵をインターネット経由で ETSI で標準化された API を用いて各拠点のセキュリティ装置に配布し、拠点間通信の暗号化を行いました。（文書番号：ETSI GS QKD 014 V1.1.1 (2019-02)）

＜検証環境＞

- 本検証ではセンタ拠点とエンド拠点を IPsec で接続し、IPsec の構成の際には DH 方式および量子暗号鍵方式をそれぞれ採用し暗号化の効果のおよび CU-DU 区間の遅延に関する検証を行いました。

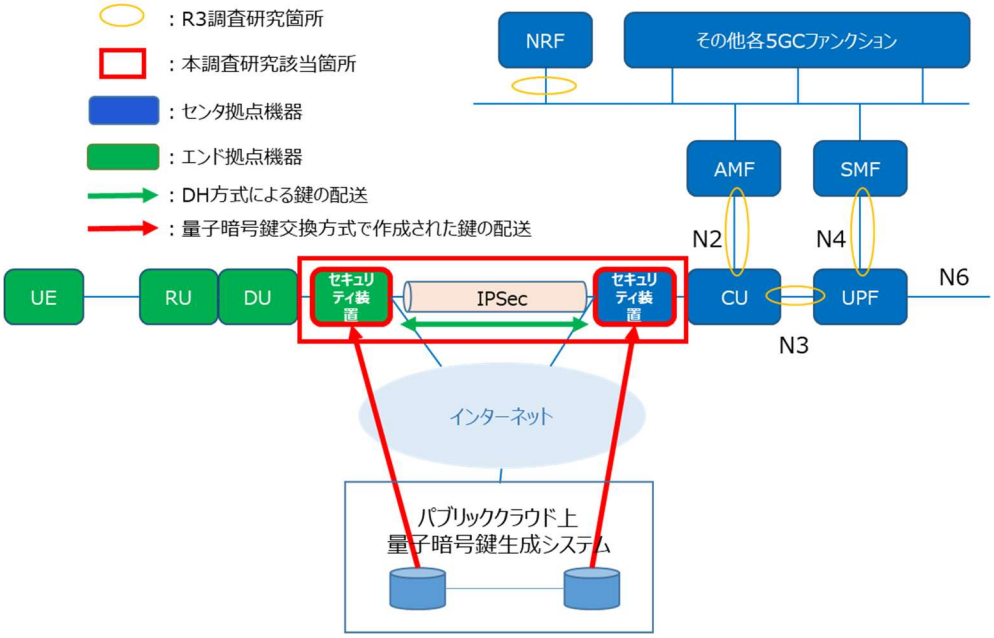
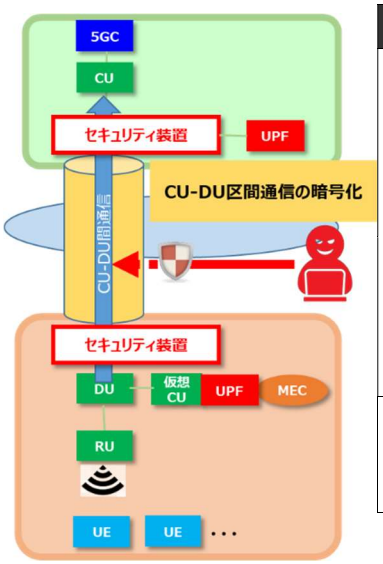


図 7-2-1　検証環境



検証概要	評価項目	検証手順
IPsec 通信の確立	IPsec の成立確認	DH 方式、量子暗号鍵交換方式のそれぞれ以下を実施 ・両拠点の鍵を用いて IPsec トンネルを ・C-plane および U-plane の通信がともにえることを確認
	暗号化の確認	DH 方式、量子暗号鍵交換方式のそれぞれ以下を実施 ・C-plane の通信のみ暗号化を施す設定の ・CU-DU 区間で暗号化されることを確認
CU-DU 区間の遅延測定	遅延値の確認	DH 方式、量子暗号鍵交換方式のそれぞれ以下を実施 ・CU-DU 区間の通信遅延値を測定

図 7-2-2　検証イメージ

＜検証結果＞

① IPsec 通信の確立 > IPsec の成立確認

DH 方式および量子暗号鍵交換方式のそれぞれについてセンタ拠点とエンド拠点間に IPsec トンネルを構築し、CU-DU 区間の暗号化を行ったところ、いずれの方式においても問題なく IPsec の確立が確認できました。

② IPsec 通信の確立 > 暗号化の確認

DH 方式および量子暗号鍵交換方式のそれぞれについて構築した IPsec が適切に動作することを確認しました。具体的には、IPsec トンネルに入る前後のパケットの違いについてパケットキャプチャを実施し比較しました。その結果 IPsec に入る前は SCTP(C-Plane)、GTP(U-Plane)とそれぞれのプロトコルが見えている一方、IPsec 内では ESP として暗号化されていることが確認できました。

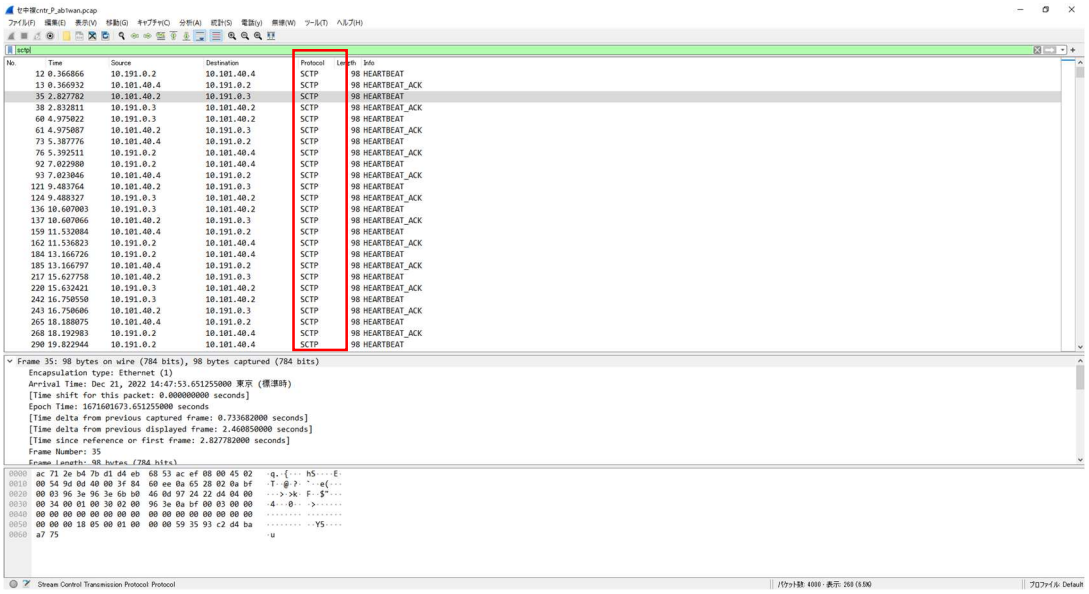


図 7-2-3　IPsec トンネルに入る前の C-Plane パケット例

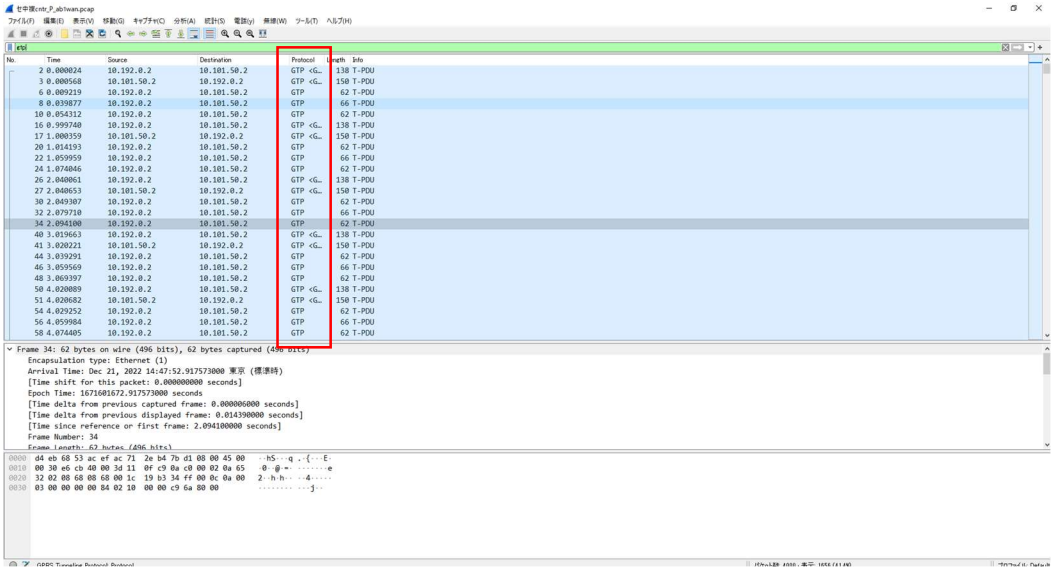


図 7-2-4　IPsec トンネルに入る前の U-Plane パケット例

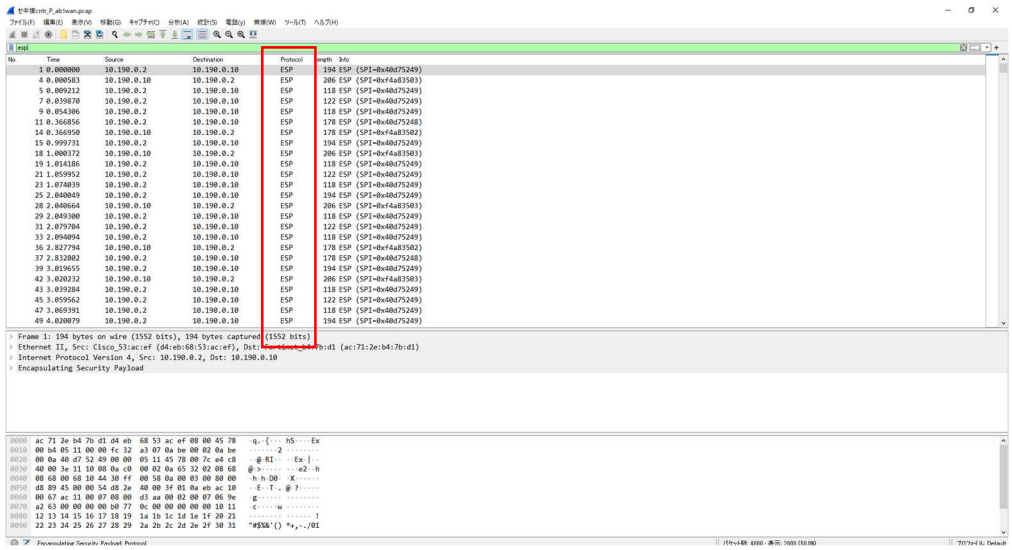


図 7-2-5　IPsec トンネル内のパケット例

③　CU-DU 区間の遅延測定 > 遅延値の確認

- 各拠点において、DH 方式および量子暗号鍵方式のそれぞれで C-Plane / U-Plane それぞれの IPsec トンネルについて CU-DU 区間の遅延値を測定した結果例（測定には DU から CU への ping を用いました）を下表に示します。
- この結果から、CU-DU 区間の遅延は地理的な距離や回線種別による影響は受ける一方で、鍵交換の方式による影響はないことが確認できました。これは、鍵交換の種別は、IPsec の通信を始めるための IKE フェーズ 1 にのみ関わり、実際の C-Plane/U-Plane の通信パケットが送られる IKE フェーズ 2 には関わらないためと考えられます。
- このことから鍵交換方式の採用においては通信性能には影響がないことが言えます。

表 7-2-1　CU-DU 区間遅延測定結果

拠点名	鍵交換方式	C-Plane 遅延(msec)	U-Plane 遅延(msec)
拠点 A (業界共用)	DH 方式	1.363	1.370
	量子暗号鍵方式	1.405	1.410
拠点 B (複数企業共用)	DH 方式	4.697	4.603
	量子暗号鍵方式	4.631	4.650
拠点 C (複数企業共用)	DH 方式	6.411	6.343
	量子暗号鍵方式	6.349	6.440
拠点 D (業界共用)	DH 方式	5.869	5.855
	量子暗号鍵方式	5.921	5.874
拠点 E (業界共用)	DH 方式	0.382	0.353
	量子暗号鍵方式	0.402	0.375
拠点 F (業界共用)	DH 方式	7.931	7.946
	量子暗号鍵方式	7.926	7.957

3. セキュリティ機能付き SIM

本項では端末に関するセキュリティの参考として、セキュリティ機能付き SIM を用いた検証結果を記載します。

＜検証概要＞

- 無線及び端末側のセキュリティについては、認証情報の登録されていない不正な SIM を用いた端末からの攻撃や、SIM スワッピング等の SIM の不正な利用のようなセキュリティリスクに対し、当該 SIM からの通信を検知・遮断できることを確認する必要があります。
- また、数多くの端末の接続が想定されるローカル５Ｇにおいては、不正な通信を行った端末への対応稼働の負荷が想定されるため、それら管理稼働削減のための接続端末の可視化方法の検証も必要です。
- これらを踏まえて、コアを共用した環境において、ユーザ環境や通信の内容に応じたセキュリティの推奨設定、端末のセキュリティレベルのモデル化を行いました。

＜検証環境＞

- 各拠点の端末にセキュリティ機能付き SIM を挿入し、センタ拠点に端末通信の監視装置と端末管理システムを設置しました。エンド UPF を使用した際の検知を行うためエンド拠点にも監視装置を設置しました。監視装置にて検知した不正な通信に対し、端末管理システムから SIM 隔離等の措置を行いました。また、端末管理システムでは通信の可視化も行いました。
- 本検証にあたり、端末管理のモデルとして端末の用途別に表 7-3-1 に記載の 3 種類の端末分類を行い、各モデルに応じた適切なセキュリティ設定を実施した上で検証を行い、セキュリティ機能付き SIM システムの有効性を確認しました。

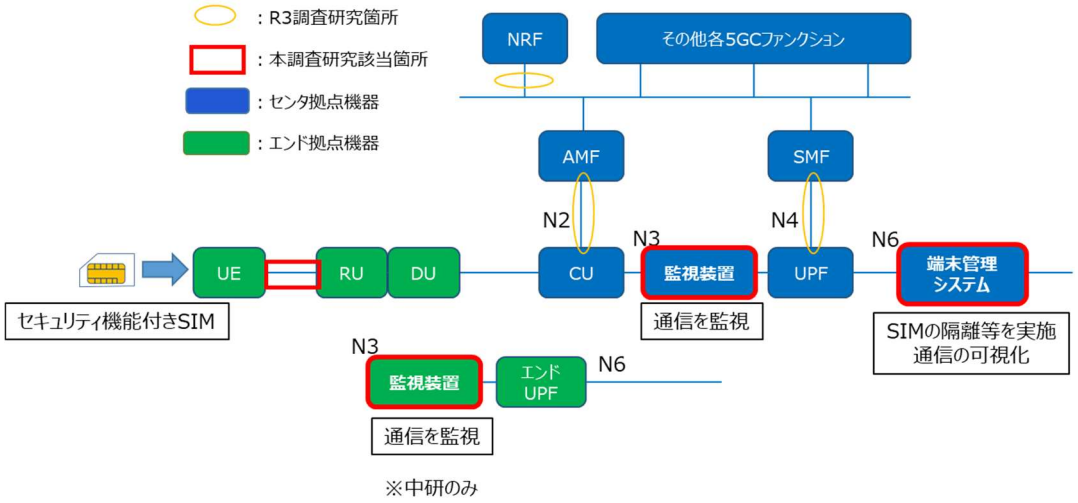


図 7-3-1 検証環境

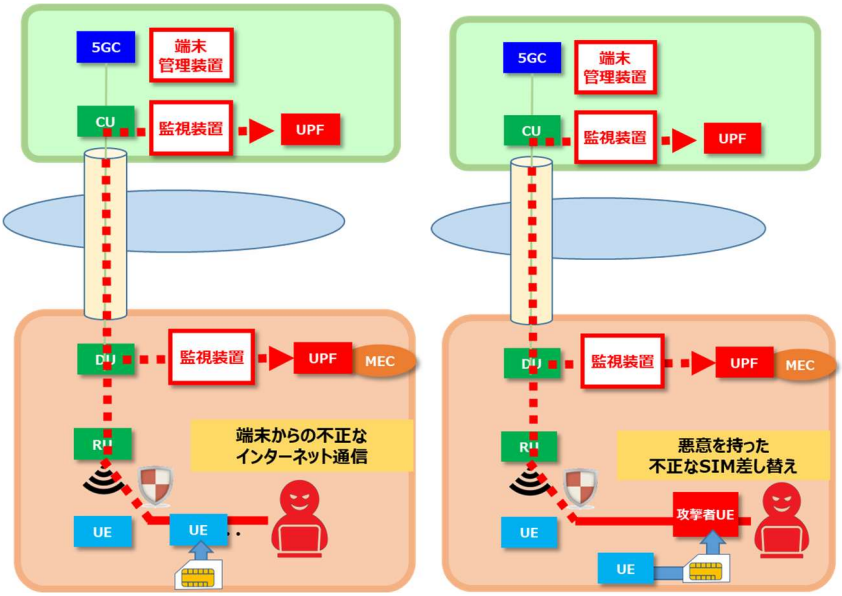


図 7-3-2　検証イメージ

表 7-3-1 デバイス種別の定義

デバイス種別	概要	例	P2P 通信	不正通信時の挙動
Critical Device	インシデント発生時に自動隔離を行うと可用性や人命にかかわる機器	産業機器/医療機器	行う	検知はするが、自動隔離は行わない
Monitoring Device	映像による監視や稼働管理を行う機器	監視カメラや独立したセンサ	行わない	検知次第、自動隔離する
Communication Device	人間やセンサ同士でのコミュニケーションを行う機器	スマートフォンや連携動作するセンサ	行う	検知次第、自動隔離する

＜検証結果＞

- 各デバイスモデル別に端末からの不正通信や SIM スワッピング等の各攻撃について、端末管理システムから適切なペナルティを設定できること、またコア共用環境下においてそれらペナルティを各ユーザ個別に独立して設定できることを確認しました。
- インシデント発生時に人名や可用性に大きな影響のある Critical Device については、検知は行うが即座の自動隔離は行わない設定を行い正常な動作を確認しました。その際に、必要に応じて検知を確認した管理者が手動で端末の隔離を行えることも確認しました。
- 映像による監視や稼働管理を行う Monitoring Device については、検知次第自動で隔離可能なことを確認しました。また、Monitoring Device 同士の通信は想定されないため、最小特権の原則から端末同士の通信を遮断できることも確認しました。
- スマートフォンのように人やセンサ同士が互いに通信する Communication Device についても、検知次第自動で隔離可能なことを確認しました。Monitorin Device とは異なり、端末間通信を許可できることも確認しました。

4. コア共用に係るセキュリティリスク及び対策（利便性や運用要件とのバランス等）

本項ではコア共用に関するセキュリティリスクおよび対策についてまとめます。SIer 等においては、ユーザと要件等について詳細に協議し、事前に必要なセキュリティ対策を決めることが肝要です。要件に合わせて以下のセキュリティ対策を組み合わせることが有効と考えられます。

① 拠点間通信の暗号化

＜概要＞

- コアまたはコアと CU を共用することによる拠点間通信の盗聴への対策として拠点間通信の暗号化が有効です。拠点間通信の盗聴がなされると、端末情報や SIM 情報を含むユーザ情報の流出や共用する他拠点への不正アクセス等に利用されかねないため本設定については全ての共用形態において採用することが推奨されます。
- コアを共用し CDU-5GC 区間が分離することにより WAN 区間を流れる通信は N2/N4(C-Plane)と N3(U-Plane)の 2 種類があり、いずれも暗号化の実施が有効です。
- CU を共用し CU-DU 区間が分離することにより、WAN 区間を流れる通信は F1-C(C-Plane)と F1-U(U-Plane)の 2 種類があり、以下のような暗号化の対応が考えられます。

  ・F1-C はユーザの認証情報等の重要情報を含む通信であり、その通信は SCTP を用いた平文で行われるため、拠点間通信時には暗号化を施すことが有効です。

  ・F1-U は無線区間で PDCP を用いてすでに暗号化されたパケットが送信されるため、拠点間通信時に改めての暗号化は不要と考えられます。

＜IPsec の活用＞

- 検証結果から拠点間通信の暗号化に IPsec を用いることが有効であると考えられます。
- IPsec は Phase 1 と Phase 2 に分かれます。Phase 1 で暗号化に使う鍵を交換し、Phase 2 で Phase 1 で交換した鍵を用いて実際の暗号化通信を行うための VPN を構築します。本調査研究では Phase 1 の鍵交換について、DH 方式と量子暗号鍵交換方式の二種類の方式を検証しました。F1-C や F1-U の通信は Phase 2 で行われるため、ローカル５Ｇシステムに必要なそれらの通信において、遅延や IPsec の強固性に DH 方式と量子暗号鍵交換方式の間に差分はないことが確認できました。検証結果から、コア共用の構成における拠点間の暗号化には DH 方式および量子暗号鍵交換方式がいずれも使用可能であると言えます。
- DH 方式および量子暗号鍵交換方式の違いについて、量子暗号鍵交換方式は Phase 1 の鍵交換の際に CU-DU 区間で盗聴された場合でも量子(光子)レベルでそれを検知することができるため、鍵をすぐさま変更することが可能であり、DH 方式のように盗聴されて量子コンピューティングで解読される心配はありません。金融業や OT 機器の使用等の従来の IPsec よりもさらに厳重なセキュリティを求める場合に、量子暗号鍵交換方式の採用が有効であると考えられます。
- また、検証においては ETSI 標準 API を使用して量子暗号鍵の受け渡しの確認を行いました。将来的なマルチベンダ化を考慮した際には、ベンダ独自の実装ではなく ETSI 標準 API を使用することが望ましいと考えられます。

② 各５Ｇインターフェースを狙う攻撃の遮断

＜概要＞

- N2/N3/N4 インターフェースの通信および各 5GC ファンクションの管理を行う NRF 向けインターフェースに対する通信を用いたセッションハイジャックや DoS 攻撃に対しては、各インターフェースに Firewall を設置し攻撃を遮断することが有効です。5GC ファンクションへの攻撃は共用する全ユーザに対するローカル５Ｇシステムの停止のような広範囲へのセキュリティ被害が懸念されるため、本設定については全ての共用形態において採用することが推奨されます。

＜IPsec および Firewall の実装について＞

- ①IPsec および②Firewall の実装に際しては、センタ拠点に複数ユーザで共用可能な IPsec/Firewall 装置を設置することで、コストを抑えながら複数ユーザのセキュリティを守ることが可能です。その際に両方の機能を具備する装置を採用することでさらに導入・運用コストの低減が期待できます。

③ セキュリティ機能付き SIM の活用

＜概要＞

- 多目的かつ多種類の端末が接続されるローカル５Ｇシステムにおいて、端末からの不正な通信を適切に防ぎ、システムの可用性と機密性を守ることは重要です。また、コア共用構成のように複数のテナントが同じローカル５Ｇシステムに接続する環境の運用にあたっては、テナント毎に求められる適切なポリシーが設定できること、およびテナント毎の端末の可視化・管理機能を有することが効果的と考えます。本検証おいては端末を SIM 単位で管理し、不正な通信を監視装置で検知し遮断できること、また必要に応じて端末からローカル５Ｇシステムへの接続を拒否できることを確認しました。
- 端末からの不正な通信の監視においては、CU-UPF 間の通信を監視し、端末からのすべての通信を監視することが効果的と言えます。このとき、エンド UPF からユーザ通信が行われ、その通信も監視したい場合には、エンド拠点にも監視装置を入れることが必要となります。

＜端末種別毎のセキュリティ要件の在り方＞

- 本検証結果を以て、ローカル５Ｇシステムに接続する端末の種類を以下の三つに分けて、それぞれ異なるセキュリティポリシーで運用することが考えられます。
  - Critical Device（P2P 通信あり / 不正通信の検知はするが自動での隔離はしない）
  - Monitoring Device（P2P 通信なし / 不正通信を検知次第自動隔離する）
  - Communication Device（P2P 通信あり / 不正通信を検知次第自動隔離する）
- 上記のような端末分類を採用し、各種攻撃に対してのセキュリティ対策および可視化を行うことを考えた際、多種多様な特性を持ち OS にて動作している端末本体に管理エージェントのようなソフトウェアを一律で導入することは現実的ではないため、セキュリティ機能付き SIM を用いることが有効です。セキュリティ機能付き SIM を用いることで、端末の種類によらず不正通信発見時に端末の隔離を即座に、かつ他の端末やネットワークに影響を与えず行うことが可能です。
- Critical Device は医療機器や OT 機器のように、不正通信時に即座にローカル５Ｇから隔離してしまうと人命や可用性に大きな影響を及ぼす端末と定義します。これらの端末から不正通信が発生した際には前述の理由から検知にとどめ、即時の隔離は行わないことが求められます。実際の運用にあたっては、検知を確認したあと不正通信の内容をログで確認し、必要に応じて

手動で隔離を行えるシステムが望ましいと考えます。またその際には手動で隔離したこともログに残ることが運用上有効であると考えられます。

- Monitoring Device は監視カメラや独立したセンサのように、端末間の通信を行わない端末と定義します。これらの端末から不正通信が発生した際には被害を最小限に防ぐために、即座に隔離を行うことが有効と考えます。また、端末間の通信を行わないことが予めわかっているため、端末から端末への通信はあらかじめネットワークの設定で禁止しておくことが最小特権の原則から有効であると考えられます。

- Communication Device は人が持ち歩く携帯型端末や互いに情報を送りあい連携をとるセンサ端末のように、端末間の通信を行う端末と定義します。Monitoring Device と同様、これらの端末から不正通信が発生した際には被害を最小限に防ぐために、即座に隔離を行うことが有効と考えます。Monitoring Device との違いとして、端末同士の通信が想定されるため、端末間の通信は禁止しません。

- これらの端末分類を採用するため、SIM ごとに端末を分類し、その端末分類毎に異なるセキュリティポリシーを適用できるシステムが有効と考えます。また、コアを共用するシステムにおいては、テナント毎に必要とする端末の分類が異なる場合や、さらに細かな設定が求められる場合が想定されるため、テナント毎にも異なるセキュリティポリシーを適用できることが望ましいと考えられます。

＜不正な通信の種類＞

- 端末へ直接攻撃者の PC を接続することによる乗っ取りや、端末から不正な Web サイトを閲覧する等によりウイルスに感染するといった、正規の端末が攻撃の踏み台にされるケースについて考えます。このケースにおいては、上記の端末の分類に応じて検知または隔離を行うことが効果的と考えます。また、その不正通信の判別においては、セキュリティベンダが定義する不正通信パターンを採用し、最新化し続けることが望ましいと考えられます。

- 次に SIM の入れ替えについて、倉庫等に放置していたあるいは手の届く位置に常設されていた等の理由で、攻撃者が正規端末から SIM を抜いて攻撃者自身の端末または放置されていた別の正規端末に差し替えて社内ネットワーク等に不正に接続しようとするケースについて考えます。このケースについて、ローカル５Ｇシステムの一般利用において、SIM が抜かれること自体が正常な運用ではないと考えられるため、いずれの端末分類においても検知と同時に隔離を実施することが有効です。例外として、検証や研究利用等 SIM を頻繁に抜き差しすることが想定される場合においては、検知のみを行うように設定できることが望ましいと考えられます。

- Monitoring Device における端末から端末への通信について考察します。監視カメラやセンサは場合によっては手に届きやすい場所に常設されることが想定されるため、三つの端末分類の中で最も乗っ取りの被害に遭いやすいと考えます。Monitoring Device の端末間通信を禁止することは、万が一の乗っ取りの際に、ほかの端末への攻撃やウイルス感染を広げることに効果的であると考えられます。

- また、上記以外のセキュリティリスクについては以下のガイドラインを参考に適切な対応を取ることが有効です。

  「ローカル５Ｇセキュリティガイドライン」
  https://www.ict-isac.jp/news/news20220331.html

＜端末通信の可視化による管理稼働削減効果について＞

- コアやCU共用の環境においては、複数の拠点に多様な種類かつ多数の端末が接続されるため、それら端末のセキュリティ管理を一台ずつ行うことには人的、時間的に多くのリソースが必要となります。単一のサービス提供者が複数拠点に対するセキュリティ環境を提供する形態を考える場合、ユーザ毎に端末のオンライン/オフラインの状況、IPアドレスやIMSI番号等のステータス情報、不正通信やSIMスワッピング等の不正操作が行われた端末の状態やそのログ等を簡単なGUI操作で確認できることが肝要です。

- この点に関してもセキュリティ機能付きSIM、監視装置および端末管理システムを用いることで、不正通信が行われた際の拠点や端末の特定、不正通信の内容や現在のステータスを確認し、Critical Deviceにおける手動での隔離や、不正通信によりネットワークから自動で隔離された端末の再接続等、適切な対応をとることが可能となります。

＜セキュリティ機能付きSIMの採用について＞

- 上記のような端末分類を採用し、各種攻撃に対してのセキュリティ対策および可視化を行うことを考えた際、多種多様な特性を持ちOSにて動作している端末本体に管理エージェントのようなソフトウェアを一律で導入することは現実的ではないため、セキュリティ機能付きSIMを用いることが有効です。セキュリティ機能付きSIMを用いることで、端末の種類によらず不正通信発見時に端末の隔離を即座に、かつ他の端末やネットワークに影響を与えず行うことが可能です。

1. 運用要件に関する概要

- コア共用では、自治体や業界団体での共用ケースなど、ローカル５Ｇシステムに対して電気通信事業者等による運用監視が行われないケースが想定されます。
- この場合、一般的な通信サービス事業と同様に、コア共用を行う場合にも必ずシステム構築、運用、1 次保守を行う、通信事業者相当の能力を備えた運用管理者または相当の体制が必要となります。その運用管理者が、不具合発生時の要因特定、対策・復旧等について担保する必要があります。
- 広範囲に渡るため障害時の要因特定に向けた切り分け手順、責任分界点、なるべく他のユーザや拠点に影響を及ぼさないような復旧方法を入念な検討・検証を繰り返したうえで整備する必要があると考えられます。
- 本手引書では、システムの維持・運用においては、正常性等の監視や障害等が発生した場合の原因切り分け等が必要であるため、ローカル５Ｇシステムに起こりうる障害事例について実際の環境下で再現し、有効な監視体系について説明します。
- 具体的には、障害の発生から原因の切り分け、復旧、復旧後の正常性確認について検証し、システム正常性等の監視に有効となる指標 KPI 及び障害等の原因切り分けに有効となる指標（サブ KPI）の設定、またこれらの KPI 及びサブ KPI の有効性及び妥当性を評価することで、ローカル５Ｇシステムの監視体制モデルについて説明します。

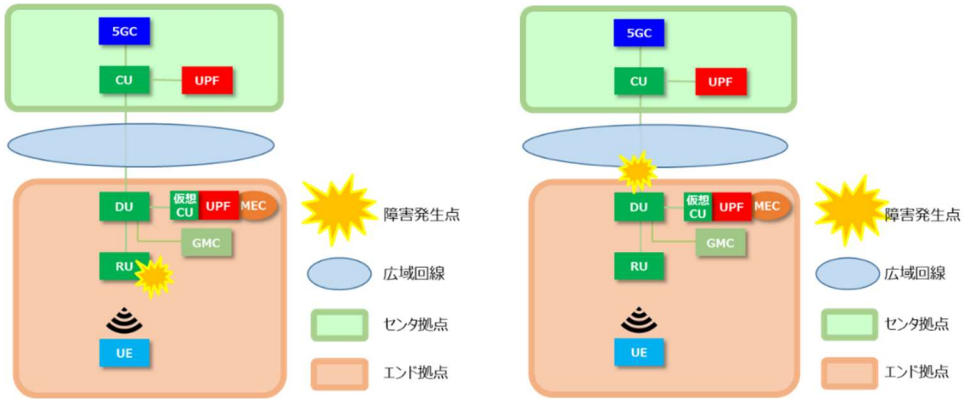
2.　監視運用検証

＜検証概要＞

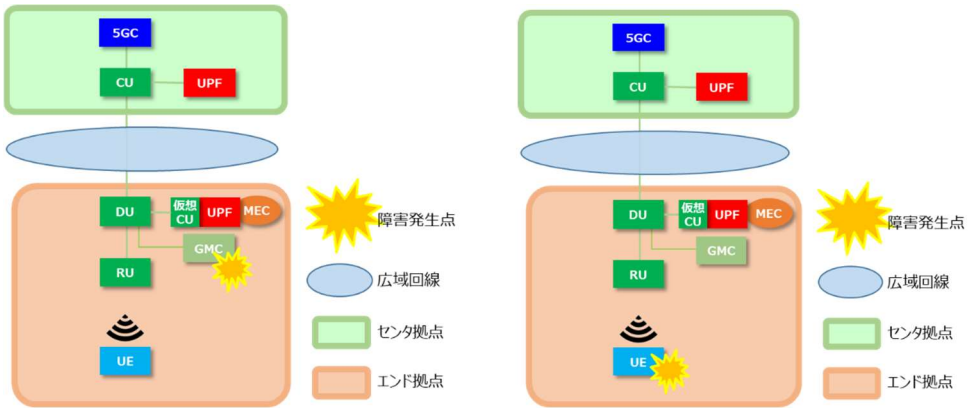
- システムの維持・運用においては、正常性等の監視や障害等が発生した場合の原因切り分け等が必要であるため、ローカル５Ｇシステムに起こりうる障害事例について実際の環境下で再現し、有効な監視体系について検証します。
- 具体的には、障害の発生から原因の切り分け、復旧、復旧後の正常性確認について検証し、システム正常性等の監視に有効となる指標 KPI 及び障害等の原因切り分けに有効となる指標（サブ KPI）について考察します。これらの KPI 及びサブ KPI の有効性及び妥当性を評価することで、ローカル５Ｇシステムの監視体制モデルについて整理します。

＜検証環境＞

- 本検証では、過去に移動通信システムで発生した障害事例を参考に、ローカル５Ｇシステムにおいても発生が見込まれる次の４つの障害事例について再現し検証しました。
  - ・RU 装置故障による電波送出停止
  - ・設備故障による WAN 回線のエンド拠点側通信断
  - ・GMC 故障による同期外れ
  - ・SIM カード破損による SIM 認証エラー



RU 装置故障による電波送出停止　　設備故障による WAN 回線のエンド拠点側通信断



GMC 故障による同期外れ　　SIM カード破損による SIM 認証エラー

図 8-2-1　監視運用検証に係る検証環境

＜検証結果＞

- システム正常性等の監視に有効となる指標を KPI とサブ KPI として設定して、実際に監視した場合の効果を検証した評価と難易度について説明します。

表 8-2-1　監視運用検証の検証結果

仮説 KPI 項目	RU	WAN	GMC	SIM	評価と難易度
5GC の機器死活監視	－	－	－	－	本検証では Alert を出す対象ではなかったため、障害が 5GC を原因としないものである判断材料として有効でした。もし、5GC の機器死活監視について Alert が発生した場合は、他に優先して対応すべき重大な障害であるため、KPI として必須と考えられます。 また、ICMP トラップによる監視であれば比較的に容易に実現できると考えられます。
呼処理の異常検知	－	－	－	○	SIM 障害において異常検知した項目であり、KPI として有効であると考えます。ただし、UE の運用形態によってはユーザが現地で認知可能な異常であり、常時監視・遠隔監視の必要性についてはユースケースに応じて検討すべきであると考えられます。 また、監視するには 5GC ベンダーの技術的な協力が必要となるため、実装の難易度は高いと考えられます。
RU の機器死活監視	－	－	－	－	本検証では Alert を出す対象ではなかったため、RU 障害や SIM 障害が 5GC から RU までの区間を原因としないものである判断材料として有効でした。もし、RU の機器死活監視について Alert が発生した場合は、途中区間の通信区間断や電源障害などが疑われるため、KPI として必須と考えられます。 また、ICMP トラップによる監視であれば比較的に容易に実現できると考えられます。
RU 電波送信レベル	○	－	－	－	RU 障害において異常検知した項目であり、KPI として有効であると考えます。RU 障害を再現性が低いものと設定する場合は常時監視の必要性は低くなりますが、遠隔監視は必要であると考えられます。 また、監視するには RU ベンダーの技術的な協力が必要となるため、実装の難易度は高いと考えられます。
RU 電波受信レベル	－	－	－	－	本検証では Alert を出す対象ではなかったものの、RU 電波送信レベルと同様に KPI として有効であると考えられます。 監視の難易度についても RU 電波送信レベルと同様に高いと考えられます。
RU の GPS 同期状態	－	－	－	－	本検証では Alert を出す対象ではなかったため、GMC 障害が 5GC から RU までの区間を原因としないものである判断材料として有効でした。もし、RU の GPS 同期状態について Alert が発生した場合は、途中区間の通信区間断や RU 装置故障などが疑われる

					ため、KPI として必須と考えます。 　また、監視するには RU ベンダーの技術的な協力が必要となるため、実装の難易度は高いと考えられます。
VPN セッション状態	－	○	－	－	コア共用において WAN 回線は不可欠であり、WAN 回線の障害は重大な影響を発生させるものであるため、WAN 障害を検知する項目として KPI として有効であると考えられます。 　ネットワーク機器のベンダーの技術的な協力が必要となるため、実装の難易度は高いと考えます。 　WAN 回線事業者と SLA を取り交わすことで、ローカル５Ｇシステム内で監視せずに、WAN 回線事業者に監視体制を求めることも選択できると考えられます。
GMC の機器死活監視	－	－	－	－	GMC はエンド拠点の機器がセンタ拠点と同期するために必要なクロック信号の供給元となる機器です。直接的にローカル５Ｇの通信が通過する機器ではないため、GMC に対しては積極的な監視をしなければならないため、KPI として必須と考えられます。 　また、監視するには GMC ベンダーの技術的な協力が必要となるため、実装の難易度は高いと考えられます。
GMC の GPS 捕捉状態	－	－	○	－	GMC 障害において異常検知した項目であり、KPI として有効であると考えられます。 　また、監視するには GMC ベンダーの技術的な協力が必要となるため、実装の難易度は高いと考えられます。

3. コア共用に係る運用体制及び対策（要因特定、責任分界点、復旧方法等）

本項では、コア共用環境下における監視運用に関する要件についてまとめます。SIer 等においては、ユーザと要件等について詳細に協議し、事前に必要な監視運用体制（SLA）を決めるべきことが肝要です。

① 監視要件

- 本検証では Alert の監視及び通知の機能を有する Zabbix サーバをセンタ拠点に設置し、コア共用での監視運用体制の基本形として SIer がシステム監視者となる想定で実施しました。そして本検証を通して、この体制に置いて KPI 及びサブ KPI を設定し監視することが、障害の原因箇所のリモート切り分け及び現地駆け付けまでの時間を短縮し、障害復旧の迅速化に資するという結果を得たものと考えられます。
- 特に機器死活監視は、単に対象の機器の状態を通知するだけでなく、その機器までのネットワークの正常性を判別するためにも有効な情報でした。KPI またはサブ KPI として重要であると考えます。ただし、ユースケースによっては本検証以外の項目が KPI として適切である場合も想定されます。そのため、ユーザが重要視する Alert についてシステム監視者と事前に取り決めることが有効であると考えられます。
- しかし、KPI 等の Alert から適切に切り分けを実施するためには、システムの構成・系統を正確に把握することが求められます。そのため、システム監視者の元には 5GC が設置されたセンタ拠点に限らず、主としてユーザが管理するエンド拠点及び拠点間を接続する WAN 回線まで含めた系統図等を事前に整備することが必要であると考えられます。
- 本検証では機器故障を原因とし、機器交換による復旧を想定しました。そのため予備の機器が必要であり、障害復旧までの時間を短くするため、予備品を事前に確保しておくことが有効です。また RU 及び UE を予備品に交換する場合、無線局免許についても手続きが必要であることに注意すべきと考えられます。

② ユーザとの連携体制

- さらにシステム監視者とユーザの連携によって、より監視運用をスムーズに進められるといえます。障害発生時の連絡方法、連絡窓口、連絡可能な時間帯や現地駆け付け対応のための現地入場手続きなど、ユーザとシステム監視者が事前に協議することでスムーズに対応が進められると考えられます。

③ WAN 回線の監視運用

- センタ拠点とエンド拠点を接続する WAN 回線についても、事前に体制を構築することが監視運用に求められるといえます。本検証ではサービス用の WAN 回線と別に保守用の WAN 回線が存在しており、サービス用 WAN 回線が断となった場合もエンド拠点の機器監視が可能でしたが、サービス用の WAN 回線のみで構成されるシステムの場合にはエンド拠点の Alert が一切通知されず、リモートによる切り分けは非常に困難となります。
- そうした場合には、現場駆け付け班による現地点検だけでなく、ユーザによるエンド拠点内の機器点検など様々な対応が考えられます。ユースケースに応じて WAN 回線に対する SLA など、WAN 回線障害発生時の体制を整備することが監視運用に有効であると考えられます。