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

（調達番号：0049-0259）

成果報告書

令和 4 年 3 月

東日本電信電話株式会社

目次

1. 実証概要

1.1 背景・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。特にローカル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解決や新たな価値の創造への活用、ポストコロナにおける「新たな日常」の構築、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の普及に向けては技術の発展・ユースケースの創出が必須になります。総務省「課題解決型ローカル５Ｇ等の実現に向けた開発実証」においては技術実証及び課題実証にて検討を進めてきましたが、さらなる普及に向け、技術の発展や費用の低廉化を目指したローカル５Ｇ設備の共用、相互接続の在り方に関する検討や、中小企業をはじめとする様々な団体の利用促進に向けたプラットフォームの検討が必要です。

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、特に高コストであるローカル５Ｇ交換設備（以下「コア」という。）を各団体が共用できる仕組みを検討するとともに、ローカル５Ｇの無線設備を運用する上での諸課題やそのノウハウを導入検討事業主体に周知し、システムを構築しやすい環境を早急に整備し、導入を促進する必要があります。

ユーザー企業等は、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顕在化していきます。

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 5G のユースケースにおいては、ネットワーク構成のみならず、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、BCP に資するコア自体の冗長化（中央管理拠点におけるコア機能のバックアップ等）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。

コア共用形態が浸透するにつれ、同一ユーザー企業内の他、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します。この場合、各ユーザーの運用ポリシーや要件が異なることから、共用のための運用ルール等（セキュリティ、運用主体、責任分解等）が必要になります。

全国各地で、多様なコア共用形態の構築が進むことで、拠点・エリアを超えたシームレスな利用や、コアの統合・集約など、ユーザーの利便性をさらに高めるニーズが顕在化します。この場合、多様な接続の形態を実現するために、ベンダーロックインを回避し、マルチベンダー環境の確保をしていく必要があります。

本検証事業は、企業や各団体等へのローカル５Ｇ導入促進を目指し、異なる企業や団体間

でコアを共用することで生じる、異なるメーカ間での相互接続性の検証を行うとともに、性能・機能・セキュリティ等からコア共用の実現性を検証しました。特に、今後、ローカル５Ｇが普及していく際に想定されるケースである、「商工会議所等の地域団体や自治体等が中心となったコア共用パターン（複数企業共用パターン）」及び「多数の団体が参加している業界におけるコア共用パターン（業界共用パターン）」について検証を行い、今後のローカル５Ｇの普及促進に効果的な方策等を検討しました。

1.2　実施事項及び検証目標

(1) 検証実施の概要

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の普及に向けては技術の発展・ユースケースの創出が必須です。総務省「課題解決型ローカル５Ｇ等の実現に向けた開発実証」においては技術実証及び課題実証にて検討を進めてきましたが、さらなる普及に向け、異ベンダ間での相互接続及び導入の容易化・費用の低廉化を目指したコア設備の共用や、中小企業をはじめとする様々な団体の利用促進に向けたプラットフォームの検討が必要になります。

本実証ではローカル５Ｇの更なる普及に向け「図 1-2-1-1　本検証イメージ」に示す複数企業共用パターンと業界共用パターンの共有形態を構築し、ローカル５Ｇ設備の共用、相互接続の在り方に関する検討を実施しました。

パターン	考え方	ローカル5G設備の在り方	ユースケース
複数企業共用パターン	・同一地域等での異なる企業間でコア設備を共用	・複数企業共用パターン、業界共用パターン双方の最適な構成を検証	・新たな働き方の創出や技術の伝承に資する遠隔指導(VR・AR)で実証
業界共用パターン	・全国に点在している同一業界の異なる団体でコア設備を共用		・4K高精細映像のAI解析による人物の顔認証、属性検知の実証

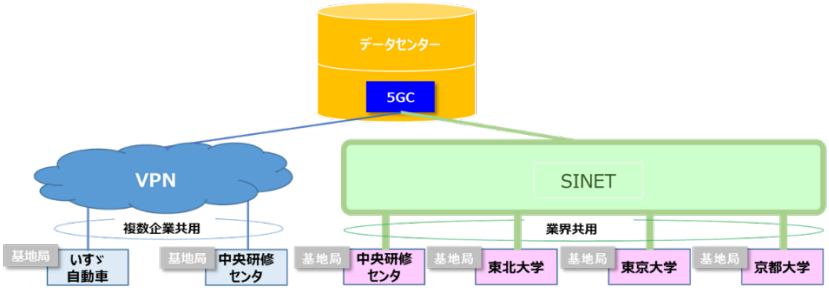


図 1-2-1-1 本検証イメージ

(2) 共用パターン

①　複数企業共用パターン（異ユーザー間の共用）

中小企業はローカル５Ｇの導入に際してコスト面で障壁がある一方、工場の無線化・製造ラインの遠隔監視等、利活用場面の展開が見込まれることから、商工会議所等の地域団体や自治体等を中心として、同一地域等の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形態を想定したコア共用パターンの検証を行いました。なお、中小企業で実行的な共用範囲として接続拠点(コアと通信する基地局を設置する拠点)は、「いすゞ自動車株式会社」(以下、いすゞ自動車) 所有の藤沢工場 (所在：神奈川県藤沢市土棚8) 及び、当社、東日本電信電話株式会社(以下、NTT 東日本) 所有の「NTT 中央研修センタ」(所在：東京都調布市入間町 1-44) に構築しました。

表 1-2-2-1 複数企業共用パターンにおける拠点と選定理由

拠点	選定理由
いすゞ自動車	接続拠点はコア装置設置都道府県の隣接県として選定 複数企業共用パターンにて製造業におけるグループ内での共同利用可能性も含め検証を行うことが可能なため選定
NTT 中央研修センタ	接続拠点はコア装置設置都道府県内の拠点として選定 本拠点は「ローカル５Ｇオープンラボ」の設置拠点であり、ローカル５Ｇを活用した新規商品・サービス開発に取り組む中小製造業を含む各種企業が集う拠点であるため選定

【ユースケース概要】

日本の製造業は、生産年齢人口の減少に伴い技術伝承や人材不足が大きな課題であり、技術力や暗黙知の形式知化が求められています。特に中小製造業においては顕著な課題です。そこで、ウェアラブルカメラを活用することで遠隔指導による高度な技術の伝承や、離れた現場と現場における技術指導が可能になり、製造業等の中堅中小企業への活用効果が見込まれます。本活用シーンは、ローカル５Ｇの高速広帯域性との親和性が高いため、複数企業共用パターンの検証に適したユースケースとして選定しました。

本検証では、ウェアラブルカメラ・360 度カメラを利用し、遠隔地の熟練作業員が現場の未熟練作業員の作業をサポートしました。

ウェアラブルカメラは遠隔地での現場作業支援、現場作業映像の録画、ハンズフリーでの作業者とのコミュニケーションなどを実現できます。また、360 度カメラを活用することで熟練作業員は作業者目線だけではなく、環境全体の確認ができるため、安全確認をしつつ、的確な指示を出すことが可能になります。複数の拠点からリアルタイムでの指示だしやコミュニケーションを取ることが可能なため、遠隔地での作業支援の効率化が見込めます。

具体的には、ウェアラブルカメラと 360 度カメラを装着した作業者に対し、離れた場所にいる熟練者が指示・指導を実施し作業者が作業を実施します。状況に応じた必要スペックの検証及び複数拠点での同時接続・利用時の他拠点への影響を検証しました。

本検証で実施する作業内容及び指示・指導内容については参画企業にヒアリングを実施し、経験値の必要な業務であり、視覚情報で知覚、思考、行動に伴う作業がある業務を選定し実施しました。

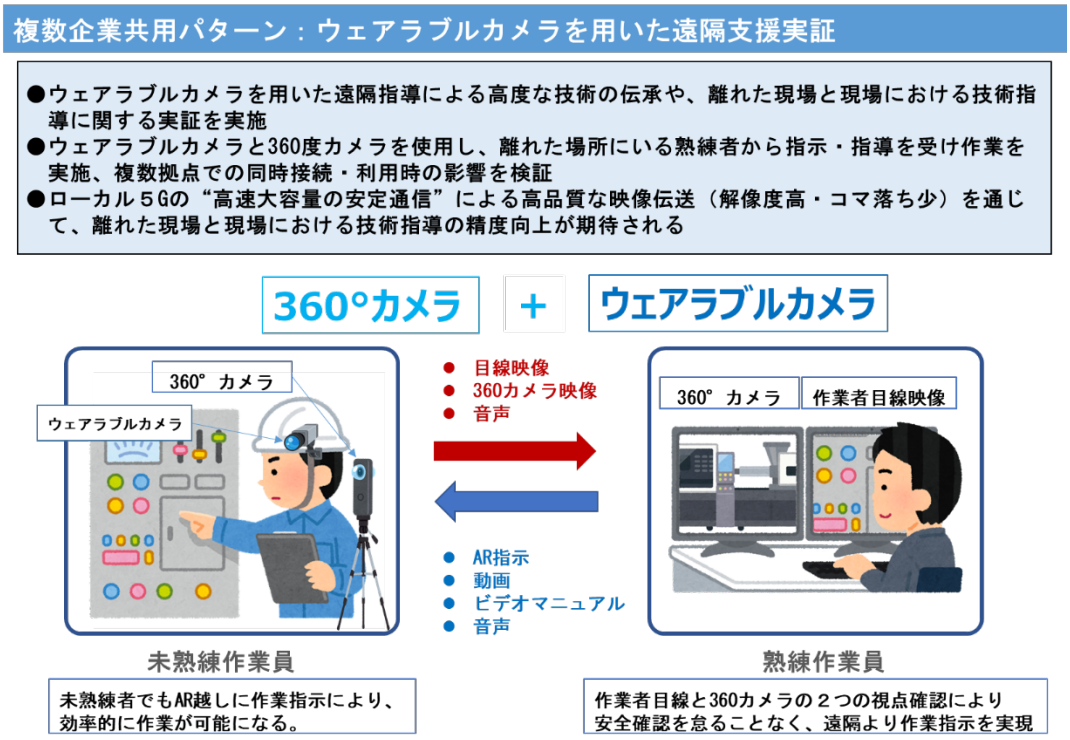


図 1-2-2-1 複数企業共用パターン　ユースケース概要図

② 業界共用パターン（同一業界内の共用）

業界共用高速バックボーン NW を有する業界では、当該既存の NW を活用した交換設備共用に係る効果が期待されることから、全国に点在している同一業界の異なる団体間でローカル５Ｇの交換設備を共用する形態を想定したコア共用パターンの検証を行いました。なお、本検証では距離に応じたコア共用の実現性を検証するため、日本における 8 地方区分(北海道、東北、関東、中部、近畿、中国、四国、九州)にもとづき、隣接する地方区分及び隣接しない地方区分として、宮城県仙台市青葉区片平二丁目 1 番 1 号に所在する「東北大学」、東京都文京区本郷七丁目 3 番 1 号に所在する「東京大学」、京都府京都市左京区吉田本町に所在する「京都大学」に検証環境を構築しました。また、本検証では業界共用パターンにおいて有望なユースケースと想定される AI 解析を用いた検証を実施しました。解析状況をモニタリングするため、NTT 東日本所有の「NTT 中央研修センタ」(所在：東京都調布市入間町 1-44)に環境を構築しました。

表 1-2-2-2 業界共用パターンにおける拠点と選定理由

拠点	選定理由
東京大学	コア装置が設置される東京都の地方区分である「関東」の拠点として選定 教育分野におけるバックボーン NW である「SINET」に接続する拠点として選定
東北大学	コア装置が設置され、かつ上記接続拠点である「関東」の隣接地方区分である「東北」の拠点として選定 教育分野におけるバックボーン NW である「SINET」に接続する拠点として選定
京都大学	上記の「関東」「東北」と隣接しない地方区分である「近畿」の拠点として選定 教育分野におけるバックボーン NW である「SINET」に接続する拠点として選定
NTT 中央研修センタ	接続拠点はコア装置設置都道府県内の拠点として選定 本拠点は、教育施設等を有する環境を活かしユースケースの映像解析を実施する拠点 各大学同様にバックボーン NW である「SINET」に接続する拠点として選定

【ユースケース概要】

前項の製造業のみならず、全業界においても、人口減少・人手不足は大きな課題となっています。加えて新型コロナウィルスの影響で、現地の作業をより効率化していく事は急務となっており、全業界において DX の推進は喫緊の課題となっています。

その様な中「AI を活用した高精細な現場映像の即時解析」は、製造業・物流業における検品や行動解析、小売業・まちづくりにおける人流の把握、鉄道・交通や金融業界等における異常行動の検知・警備への活用、大学・教育領域での生徒反応の解析・授業改善等、幅広い業界・分野での活用が想定されており、これらの AI 解析機能を現地（オンプレミス）に置かず NW 側に設けて全国拠点をカバーし業界単位等、複数企業で利用する形態が実現できれば、DX の推進に大きく寄与しうると考えられるため、業界共用パターンの検証に適したユースケースとして選定しました。

また、本ユースケースは、ローカル５Ｇの備える高速広帯域の利点との親和性が高く、高精細映像解析の継続的な安定利用、無線による機器設置場所の自由度向上、等の点と合わせて、ローカル５Ｇの大規模 NW である本検証に適したユースケースであると考えます。本検証においては、そうした映像解析の、最も基本的な実践的活用シーンの具体例として工場や小売店舗等における警備・勤怠管理等利用を想定した顔認証機能、マーケティングに活用できる人流・属性解析機能を実現する AI 顔認証システムを用いた検証を実施しました。

具体的にはローカル５Ｇ基地局+4K カメラを設置し、複数の基地局拠点からの AI 顔認証システムの同時利用の可否の検証を実施しました。

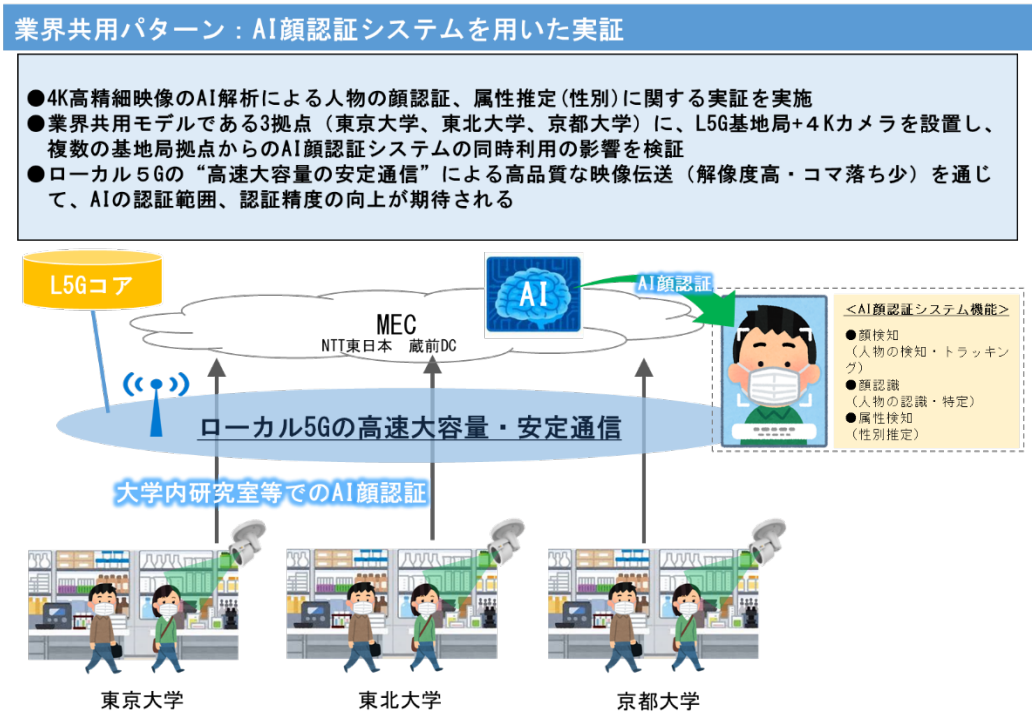


図 1-2-2-2 業界共用パターン　ユースケース概要図

(3) 相互接続検証

3GPP では、第５世代移動通信システム（5G）のサービス要求実現に向けて、新しいコアネットワークの策定検討を行われています。3GPP での標準化は、各国及び各ベンダー間の仕様の指標となっており、3GPP に準拠した製品間での相互接続が今後期待されています。一方でコア・基地局・端末に関して、フィールドの要件やアプリケーションを使用する上での所要性能に応じて、柔軟に組み合わせて設計することが望まれています。

本実証では 3GPP に準拠した複数の製品について、マルチベンダー構成での接続可否を実証し、性能の検証や課題の洗い出しを実施し、令和 4 年度における調査研究テーマを提言します。

マルチベンダー構成での相互接続検証は「図 1-2-3-1　マルチベンダー構成での相互接続検証」の構成で実施し、相互接続の組合せは計８つのパターンで実施しました。

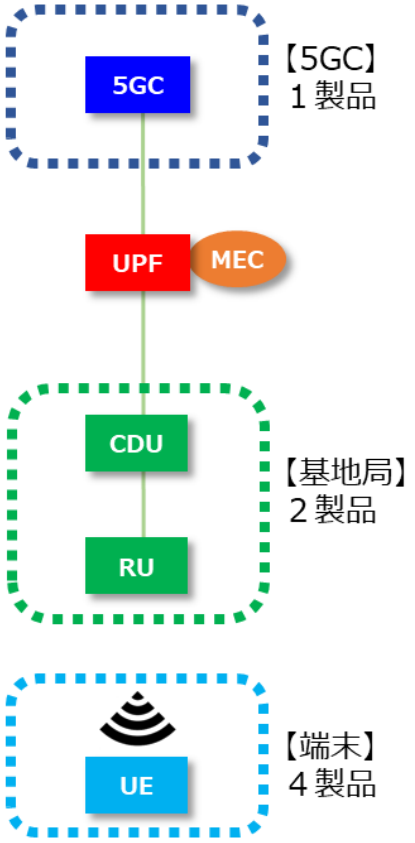


図 1-2-3-1 マルチベンダー構成での相互接続検証

具体的な検証項目は以下のとおりとなります。

表 1-2-3-1　異メーカ基地局との相互接続　検証項目

大項目	中項目	検証概要	検証項目
相互接続検証	基地局（異メーカー）との相互接続確認	電源 OFF/ON 動作時の挙動確認	基地局（CU／DU／RU）の電源をそれぞれ OFF/ON させ、再度起動した際、コア装置や端末と正常に接続できること
		電波 OFF/ON 動作時の挙動確認	停波後、発波させた際、コア装置や端末と正常に接続できること
		通信品質の確認	Ping による疎通試験、および iperf による伝送スループット試験を実施
		長期安定化試験	無操作状態とした環境においてエラーログの出力が無く、疎通試験上異常が無いこと

表 1-2-3-2　異メーカ端末との相互接続　検証項目

大項目	中項目	検証概要	検証項目
相互接続検証	端末（異メーカー）との相互接続確認	機内モードの ON/OFF の挙動確認	端末の機内モード ON/OFF させ、再度通常モードで起動した際、基地局やコア装置と正常に接続できること
		電源 OFF/ON 動作時の挙動確認	端末の電源を OFF/ON させ、再度起動した際、基地局やコア装置と正常に接続できること
		通信品質の確認	Ping による疎通試験、および iperf による伝送スループット試験を実施
		準同期の動作確認	準同期 TDD 方式において正常に接続できること
			トラフィック負荷を印加した際、理論値と比較し妥当なトラフィック値（DL／UL）が出力されること
		長期安定化試験	無操作状態とした環境においてエラーログの出力が無く、疎通試験上異常が無いこと

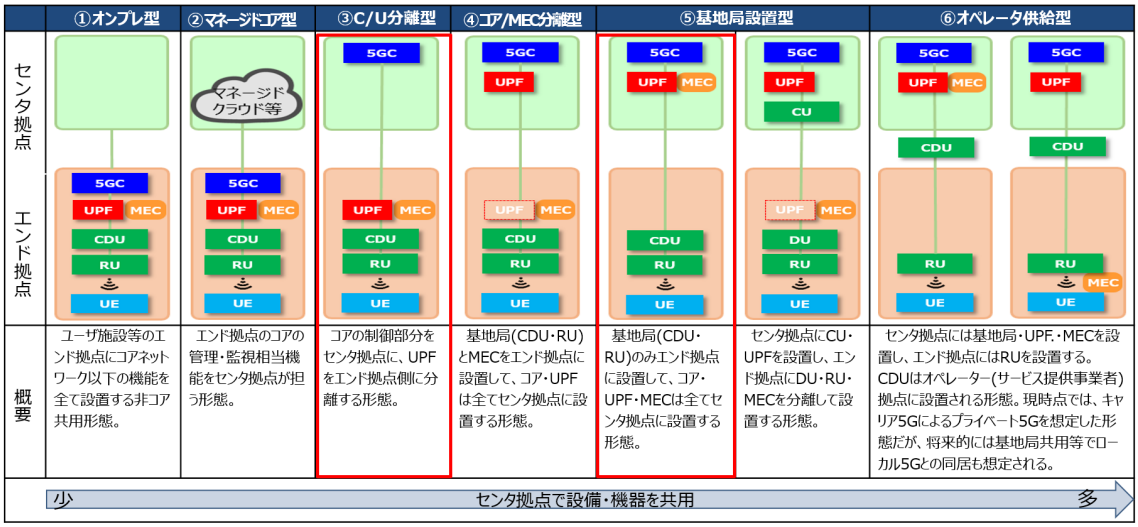
(4) コアの共用におけるローカル５Ｇシステム検証

コアの共用環境においては、以下のような課題が挙げられます。

・複数のエンド拠点が NW 上で統合運営されるため、大規模な設計において必要となる各種リソース、通信性能、遅延時間等を検証する必要がある。
・複数の異なる企業や団体において共用するシステムとなるため、運用における管理機能について、登録や閲覧をユーザーが実行できる環境を実装し、様々な共用形態において必要と考えられる機能を洗い出す必要がある。
・複数の異なる企業や団体において共用するシステムとなるため、１のユーザー拠点内にローカル５Ｇシステム全てが実装されるケースと異なり、セキュリティの観点での措置や施策を検証し、推奨されるセキュリティ対策や構成を明らかにする必要がある。
・上記３点に加えて、コアの共用システムを運用するうえでの課題等について実証結果をもとに考察し、今後検討すべき課題を見出すことが必要。

本実証では、上記の項目について複数企業共用パターン及び業界共用パターンのそれぞれの環境において検証しました。

また、「図 1-2-4-1　UPF の設置位置」による性能差分を評価・分析し、本モデルにおける課題の洗い出しを実施しました。



本実証で使用する構成

図 1-2-4-1　UPF の設置位置

具体的な検証内容は下記①～④となります。

①　性能検証

コア装置と基地局装置が異なった拠点に設置される特殊な構成において、ローカル５Ｇのシステムを維持運営する際の各システムのリソースや end-end の通信性能について検証を行いました。また、2 つの共用パターンでは異なる広域回線を用いてその差分を分析し、UPF の配置による通信性能の比較検証を実施し、遅延時間等の性能を明確にしたうえで UPF の共用形態について考察を実施しました。

また、物理的に地上の広域回線の距離が異なる各拠点において、UE の接続に要する時間と UPF までの遅延時間を検証し、回線の種別や距離に伴う性能差分について考察しました。

表 1-2-4-1　性能検証項目概要

項番	項目	概要
(1)-1	消費リソースの検証	コアの共用環境では、複数の拠点でローカル５Ｇのネットワークが構築されるため、各拠点では端末（UE）がそれぞれ共用しているコアに接続される形態であり、コアを共用しない形態と比較すると端末数が多くなることが推定されます。 コアの共用環境を設計構築するうえでは、各拠点の端末が同時接続されるとき、各機器（5GC、UPF、CDU、RU）の UE の接続時の消費リソースを把握する必要があるため、UE1 台が接続した際の消費リソースと複数台 UE が接続した際の消費リソースを検証しました。また、UL 方向のデータ通信（5Mbps/1UE）の状況を模擬し、複数台接続時の消費リソースの変化を考察しました。 消費リソースは、メモリ消費量と CPU 使用率の 2 点を対象に確認しました。
(1)-2	UE 接続台数の最大数検証	端末の最大接続数は、5GC や CDU の性能によって異なります。コア共用環境下において、複数の拠点でローカル５Ｇシステムが稼働している状況で、RU-UE 区間の伝送性能が共用環境によって劣化するのか検証することを目的に、最大接続端末数を検証するとともに、(1)-4 における伝送スループットの結果と比較し、コアの共用における影響を検証しました。
(1)-3	UE 接続時間の検証	センタ拠点（5GC 設置拠点）に対して、異なる地方等で地上の広域回線の距離や回線種別が異なる各実証フィールドにおいて、UE が 5GC システムにアクセスし認証完了するまでの接続時間を計測することで、その差分を比較するとともに、コア装置を共用するうえで実用的な回線種別や範囲について考察しました。
(1)-4	UE～UPF 間の通信性能の検証	コアの共用環境では、ローカル５Ｇシステムの通信はエンド拠点の UE 端末からセンタ拠点まで物理的に長い距離を介することが想定されます。この地上の広域回線区間について、ギャランティ型とベストエフォート型の回線を用意し、この回線の種別による伝送スループット及び遅延時間への影響を検証しました。 また、地上の広域回線の区間が特に長いロケーションの場合、低遅延が要求されるアプリケーションでは実用が困難となることが考えられるため、エンド拠点に UPF を設置したケースにおける遅延時間を検証しました。

		本検証における結果を分析し、センタ拠点で UPF を共用するモデルの実用可否を考察しました。

UE の接続時及び U-Plane 通信時のそれぞれにおいて、5GC、UPF（エンド拠点及びセンタ拠点それぞれ）、CDU、RU の消費リソースを確認しました。また、UE 接続台数が増やした状況での消費リソースの変動状況を確認しました。

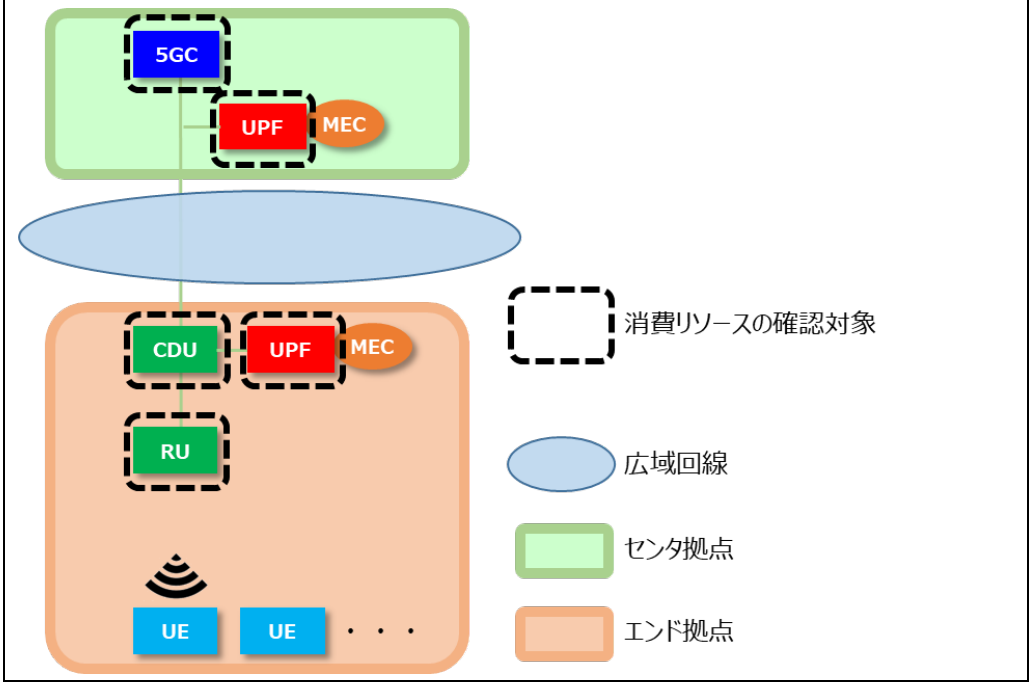


図 1-2-4-2　検証イメージ　消費リソースの検証

エンド拠点において、1 台の RU 及び CDU に接続できる端末数の限界数について確認を行いました。また、1 台の UE で最大伝送スループット（UE）を計測し、複数台接続時の Total 伝送スループットの差分比較を実施しました。

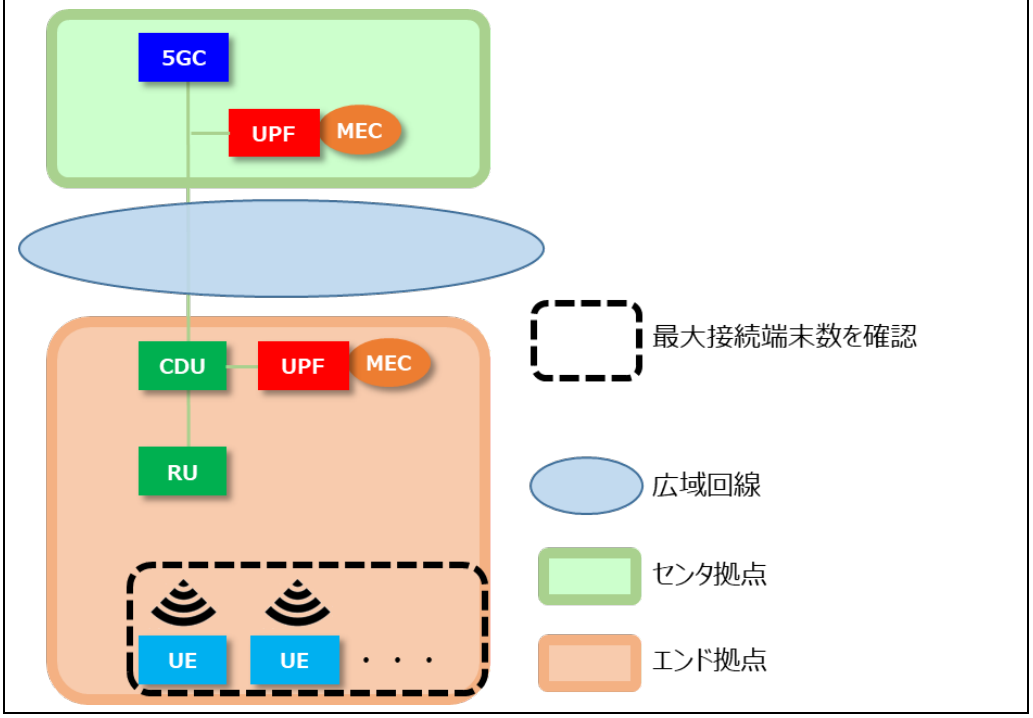


図 1-2-4-3　検証イメージ　UE 接続台数の最大数検証

本実証フィールドのすべてのエンド拠点において、UE 端末が接続に要する時間を確認しました。加えて、UE からセンタ拠点 UPF とエンド拠点 UPF の双方へ pingRTT による遅延影響を確認しました。

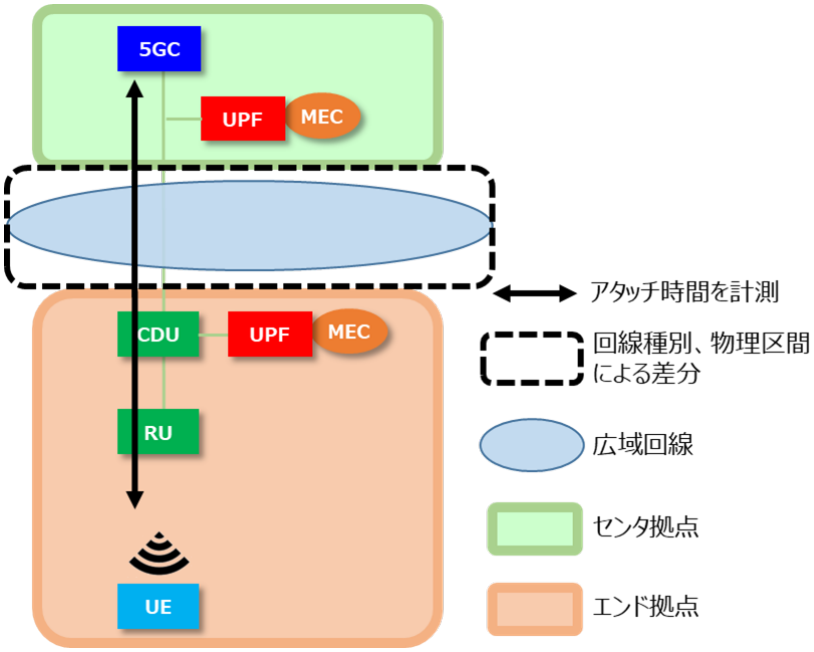


図 1-2-4-4　UE 接続時間の検証

伝送スループット及び遅延時間を検証。広域回線による差分と UPF 設置位置による性能への影響を検証しました。

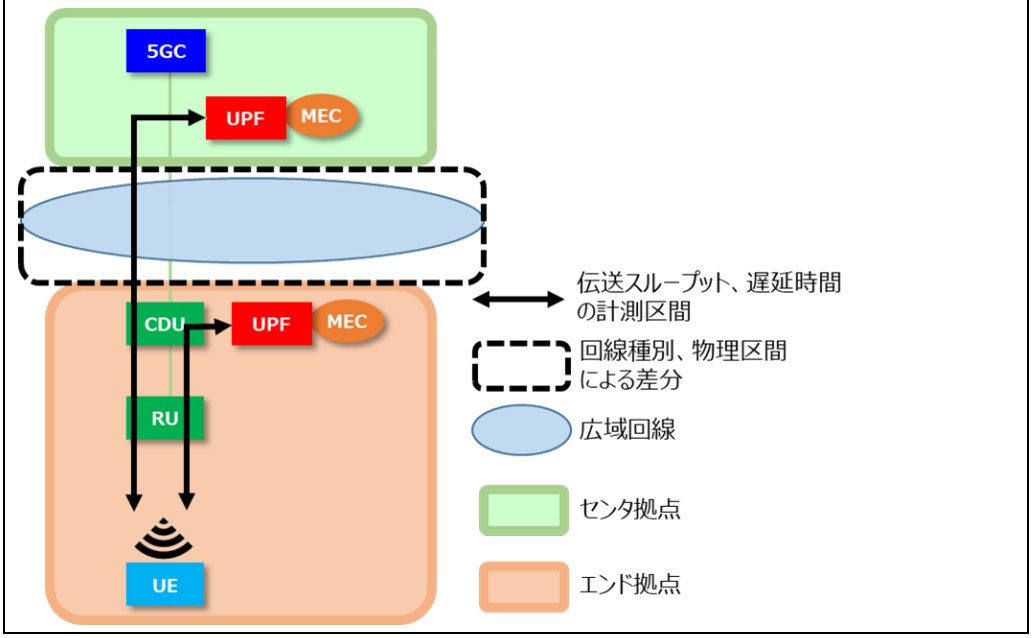


図 1-2-4-5　検証イメージ　UE～UPF 間の通信性能の検証

② 機能検証

ローカル５Ｇシステムの管理機能について、コアの共用環境下において複数の拠点で異なる企業や団体が利用する状況において、管理・運営に関する各機能の実装状況を確認し、必要と考えられる機能を考察しました。

また、ユーザーやUE端末単位でのUPFの指定制御の実用性について検証しました。対象とした管理機能と説明は以下となります。

- 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。

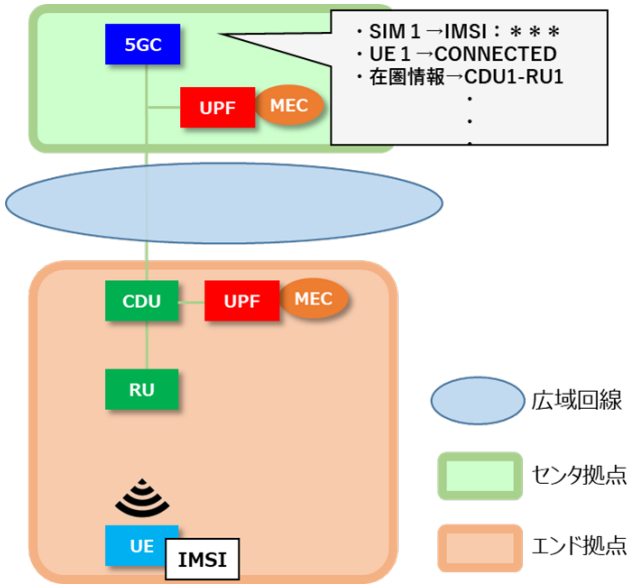


図 1-2-4-6　コア内の管理機能やログ情報の実装状況の確認検証

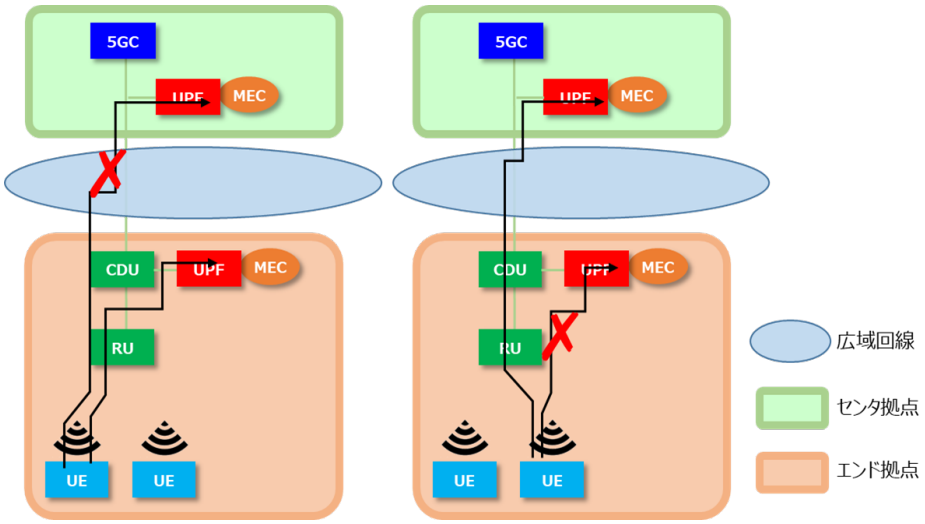


図 1-2-4-7　UE ごとの UPF 指定・制御の検証

③　セキュリティ検証

コア共用下においてはオンプレの構成と異なり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あります。本検証ではコア-基地局間におけるネットワークファンクション間通信に着目し、それら通信に対するセキュリティを評価し、セキュリティ向上させる手段を見出すため検証を行いました。

想定する攻撃は外部ネットワークからの攻撃と内部ネットワークからの攻撃に分類されます。

まず外部からの攻撃については、コアを共用している異なる拠点やコア共用と関係ない外部ネットワークからの侵入や通信の傍受が考えられ、これらの攻撃を IPsec によって防げることを確認しました。複数企業共用パターンにおいては回線サービス(SDN)によって安全性が確保されていると判断し、業界共用パターンのみ検証を行いました。その際はセンタ拠点とエンド拠点に設置したセキュリティ装置による IPsec を検証しました。

次に内部からの攻撃については、エンド拠点からコアに対する攻撃、侵入されたコアから UPF に対する攻撃が考えられ、これらの攻撃をファンクション別のファイアウォールで防げることを確認しました。ファイアウォール機能を持つセキュリティ装置には複数のユーザーで共用可能な仮想アプライアンス製品を導入し、各ファンクション通信について N2 Firewall / N3 Firewall / N4 Firewall / SBA Firewall の機能を用いて検証しました。

表 1-2-4-2 想定される攻撃

攻撃の種類	外部からの攻撃		内部からの攻撃	
	不正な外部からコアへの接続	マルチテナント間の攻撃	エンド拠点からコアに対する攻撃	侵入されたコアからUPFに対する攻撃
想定される攻撃の例	コアへの侵入	コア共用する異なる拠点への攻撃	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
攻撃によってもたらされる影響	コアからの攻撃への踏み台	異なる拠点への攻撃や通信の傍受	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	ネットワーク仮想化 (本構成ではセキュリティ装置が持つ機能を採用)		セキュリティ装置の各機能 (N2 Firewall / N3Firewall / N4 Firewall / SBA Firewall)	

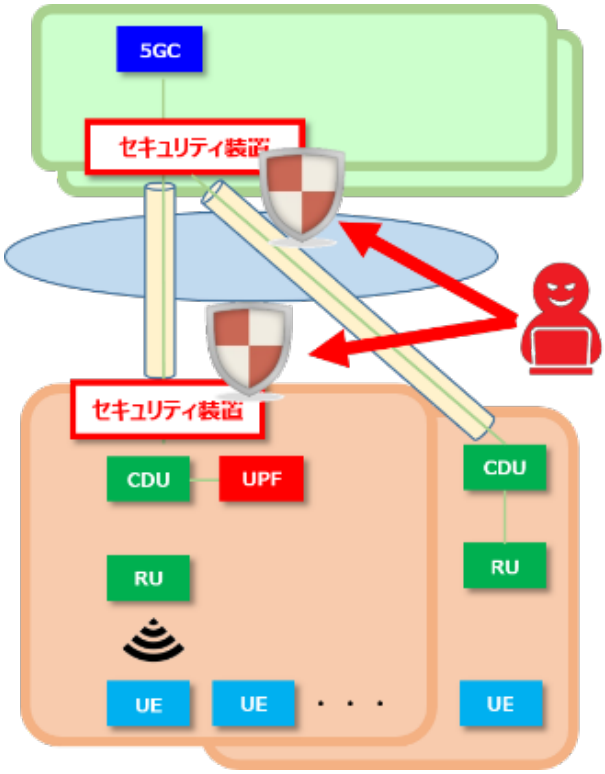


図 1-2-4-8　不正な外部からの攻撃

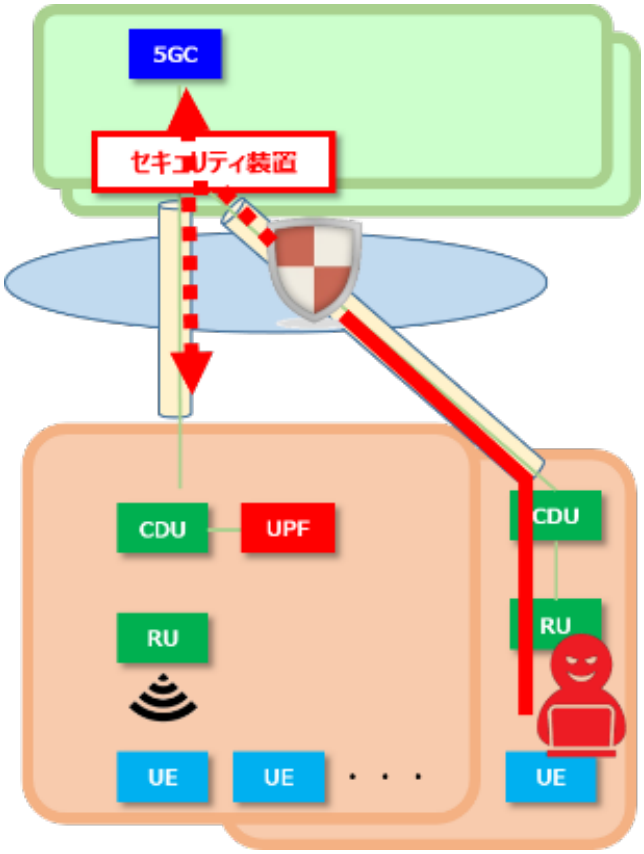


図 1-2-4-9　マルチテナント間の攻撃

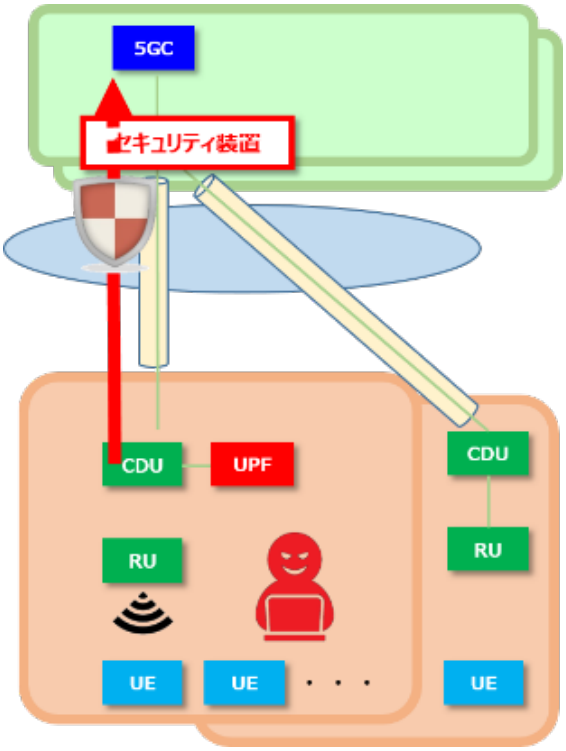


図 1-2-4-10　エンド拠点からコアに対する攻撃

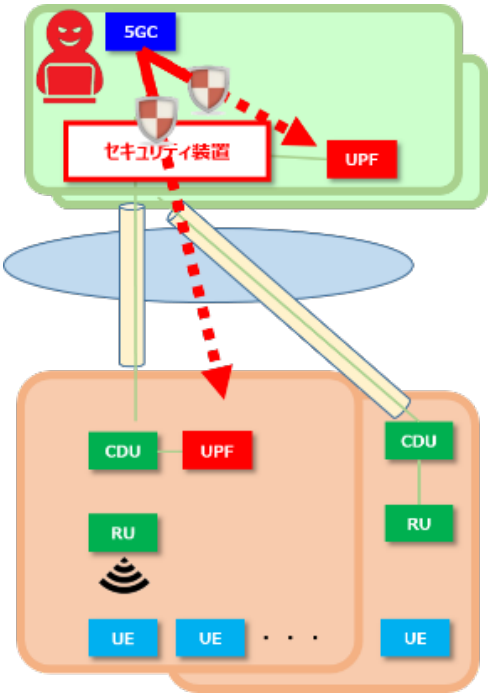


図 1-2-4-11　侵入されたコアから UPF に対する攻撃

表 1-2-4-3　セキュリティ検証対象箇所

共用パターン	UPF配置	N6 Firewall	SecGW	N2 Firewall	N3 Firewall	N4 Firewall	SBA Firewall	マルチテナント
		ユーザー通信	拠点間	ファンクション間	ファンクション間	ファンクション間	ファンクション間	閉域性
		外部からの攻撃	外部からの攻撃	内部からの攻撃	内部からの攻撃	内部からの攻撃	内部からの攻撃	外部からの攻撃
複数企業共用ﾊﾟﾀｰﾝ	ｾﾝﾀ拠点	対象外※1	対象外※2	セセ複 1	セセ複 2	セセ複 3	セセ複 4	セセ複 5
	ｴﾝﾄﾞ拠点	対象外※1	対象外※2	セエ複 1	対象外※3	セエ複 2	セエ複 3	セエ複 4
業界共用ﾊﾟﾀｰﾝ	ｾﾝﾀ拠点	対象外※1	セセ業 1	セセ業 2	セセ業 3	セセ業 4	セセ業 5	セセ業 6
	ｴﾝﾄﾞ拠点	対象外※1	セエ業 1	セエ業 2	対象外※3	セエ業 3	セエ業 4	セエ業 5

※1：一般的な IP ネットワークのセキュリティ確保の問題であるため対象外とする

※2：回線サービス（SDN）により WAN 区間の安全性を確保するため対象外とする

※3：拠点内の有線ケーブル区間通信のため安全確保済という考えで対象外とする

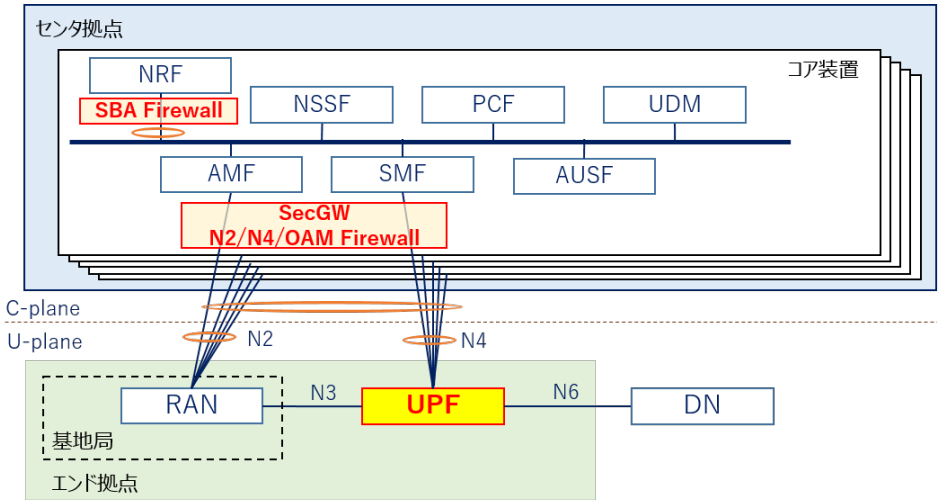


図 1-2-4-12　検証イメージ（エンド拠点の UPF を使用）

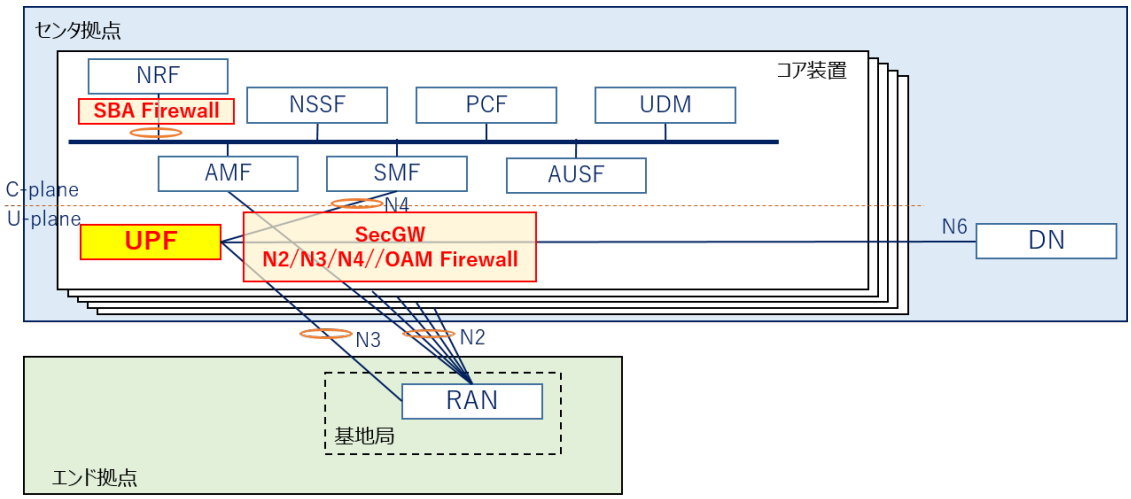


図 1-2-4-13　検証イメージ（センタ拠点の UPF を使用）

④　運用課題の洗い出し

コア共用の実現に向けて、①～③の性能・機能・セキュリティの検証結果をふまえて、運用面での課題について検討及び考察しました。また、3GPP 標準化の動向に着目し、マルチベンダー構成の最新技術をふまえた今後の実用化に向けた課題を検討しました。

1.3　実施体制

（1）共同検証機関

共同検証機関の各役割を明確にし、課題に対して取組みました。共同検証機関の実施体制は、「表 1-3-1 共同検証機関の役割」のとおりです。

表 1-3-1 共同検証機関の役割

	機関名	役割
共同検証機関	東日本電信電話株式会社	本検証の調査研究者。 代表機関として全体企画・管理を実施。 また、東日本エリアにおけるローカル５Ｇ検証環境の構築・技術検証を担当。
	国立情報学研究所	本検証の調査研究分担者。 コア共用の実現に向け技術サポート及び助言を担当する。 本検証では、業界共同パターンの各大学からコア間のネットワーク回線を SINET で提供。
	東北大学	本検証の調査研究分担者。 コア共用の実現に向け技術サポート及び助言を担当する。 業界共同パターンの検証フィールドの提供。
	東京大学	本検証の調査研究分担者。 コア共用の実現に向け技術サポート及び助言を担当する。 業界共同パターンの検証フィールドの提供。
	京都大学	本検証の調査研究分担者。 コア共用の実現に向け技術サポート及び助言を担当する。 業界共同パターンの検証フィールドの提供。
	広島大学	本検証の調査研究分担者。 コア共用の実現に向け技術サポート及び助言を担当する。
	いすゞ自動車株式会社	複数企業共同パターンの検証フィールドの提供。 複数企業共同パターンでの検証サポートを担当する。
	三菱総合研究所	本検証では、コア共用の実現に向け、課題の分析や提言の検討を担当する。
	NTT ブロードバンドプラットフォーム株式会社	西日本エリアにおける検証環境の構築。

（2）プロジェクト体制

ローカル５Ｇのコアをはじめとした無線通信等の技術者、課題解決に必要な機器開発・検証環境の構築を行うベンダー等、本事業の遂行に必要な専門知識・経験を有する要員が確保され、関係者の協力のもと、本事業を遂行しました。代表機関である NTT 東日本の実施体制は「図 1-3-1 プロジェクト体制図」のとおりです。

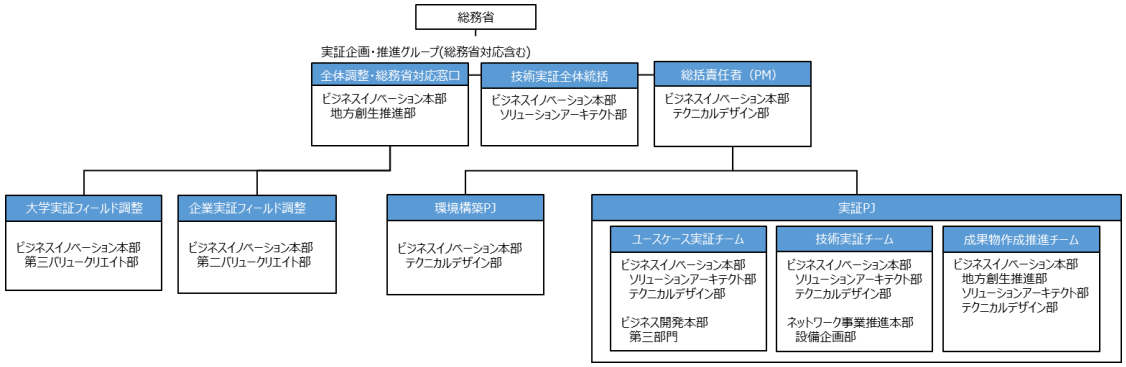


図 1-3-1 プロジェクト体制図

（3）プロジェクトマネージャ

本調査検討を円滑に進めるため、検証全体を統括した実績のあるプロジェクトマネージャを配置しました。

（4）全体調整・総務省対応窓口

主管課及び関係課並びに検証全体調整事業者及び分野別検証調整、貴省と調整・連携する連絡調整窓口等を整備しました。具体的には、実証企画・推進グループを窓口としました。

（5）技術検証全体統括

技術検証担当者は適切かつ生産性の高いアウトプットを実現するため、高い技術力を有する技術検証担当者配置しました。

（6）再委託

再委託をしようとする第三者の住所又は所在地、氏名又は名称、再委託する業務の範囲、その必要性、再委託の業務に従事する者の適格性及び情報保全のための履行体制については以下の「表 1-3-2　再委託内容一覧」のとおりです。

表 1-3-2　再委託内容一覧

名称	所在地	再委託する業務の範囲と必要性	再委託の業務に従事する者の適格性及び情報保全のための履行体制等
伊藤忠テクノソリューションズ株式会社	東京都港区虎ノ門4-1-1　神谷町トラストタワー	・ローカル５Ｇ機器調達にあたり必要な会社。 ・ローカル５Ｇ機器設定支援あたり必要な会社。	・ローカル５Ｇ機器を熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
株式会社ミライト	東京都江東区豊洲5-6-36	・ローカル５Ｇシステム構築作業支援にあたり必要な会社。	・ローカル５Ｇ機器のネットワーク環境構築を熟知。 ・東日本電信電話株式会社との

名称	所在地	再委託する業務の範囲と必要性	再委託の業務に従事する者の適格性及び情報保全のための履行体制等
		・映像解析アプリケーション機器調達にあたり必要な会社。	委託契約中に機密保持に関する条項を明確化し情報保全を実施。
ネットワンシステムズ株式会社	東京都千代田区丸の内二丁目 7 番 2 号 JP タワー	・映像解析アプリケーションライセンス調達にあたり必要な会社。	・映像解析アプリケーションのライセンス提供会社。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
エヌ・ティ・ティラーニングシステムズ株式会社	東京都港区南麻布 1-6-15	・遠隔調教アプリケーションシステム構築にあたり必要な会社。	・遠隔調教アプリケーションのライセンス提供会社。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
日本コムシス株式会社	東京都品川区東五反田 2-17-1	・ローカル５Ｇ環境構築・ケーブル敷設にあたり必要な会社。	・配線作業・機器設置に熟知 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
大和電設工業株式会社	仙台市青葉区大町二丁目５番１号	・ローカル５Ｇ環境構築・ケーブル敷設にあたり必要な会社。	・配線作業・機器設置に熟知 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
株式会社エヌ・ティ・ティ エムイー	東京都豊島区東池袋三丁目 21 番 14 号 NTT 新池袋ビル	・サーバ機器構築にあたり必要な会社。	・サーバ構築に熟知 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
三菱総合研究所	東京都千代田区永田町二丁目 10 番 3 号	コア共用の実現に向け、課題の分析や提言の検討及び報告書作成支援にあたり必要な会社。	・ローカル５Ｇの動向・普及への課題に熟知 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
エヌ・ティ・ティ・ブロードバンドプラットフォーム株式会社	東京都千代田区内神田 3 丁目 6 番 2 号 アーバンネット神田ビル	・京都大学でのローカル５Ｇ環境構築に必要な会社。	・配線作業・機器設置に熟知 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
SG ムービング株式会社	東京都江東区新砂 3-2-9 X フロンティア EAST 6F	・ローカル５Ｇ機器の各拠点への運搬スケジュール管理を行うにあたり必要な会	・全国のシステム機器運搬管理に多数の実績があり、情報通信インフラ構築に伴う機器運搬

名称	所在地	再委託する業務の範囲と必要性	再委託の業務に従事する者の適格性及び情報保全のための履行体制等
		社。	管理に熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
コムシスネット株式会社	東京都品川区東五反田 1-25-13　神野商事ビル８階	・ローカル５Ｇ機器の構築を行う。本実証では日本コムシス株式会社の元で NTT 中央研修センタでの施工管理業務を実施するにあたり必要な会社。	・ローカル５Ｇ機器構築に熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
エクシオ・エンジニアリング東北株式会社	宮城県仙台市青葉区大町 2-１5-28	・東北大学でのメタル配線・光配線業務を実施するにあたり必要な会社。	・東北大学における配線業務に熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
エヌ・ティ・ティ・ビズリンク株式会社	東京都文京区小石川１丁目４番１号住友不動産後楽園ビル	・遠隔調教システムのサービス提供・設定を実施するにあたり必要な会社。	・特殊技術であるウェアラブルカメラによる遠隔協調システムに熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
APRESIA System 株式会社	東京都中央区築地 2-3-4　築地第一長岡ビル８階	・ローカル５Ｇ交換設備共用パターンの技術実証、相互接続検証、５Ｇシステムの検証の技術支援に必要な会社。	・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
フォーティーネットジャパン株式会社	東京都港区六本木 7-7-7　Tri-Seven Roppongi ９階	・相互接続検証及び共用パターンの技術実証におけるローカル５Ｇセキュリティ機器の技術支援に必要な会社。	・ローカル５Ｇセキュリティ機器に熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
CTC テクノロジー株式会社	東京都港区虎ノ門 4-1-1　神谷町トラストタワー	・ローカル５Ｇ機器の保守に必要な会社。	・ローカル５Ｇ機器の代理店保守専門子会社であり機器保守について熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
愛和電気	神奈川県藤沢市石川 2-26-21	・いすゞ藤沢工場での電気工事を実施するにあたり必	・いすゞ自動車工場における情報通信インフラ構築の電気工

名称	所在地	再委託する業務の範囲と必要性	再委託の業務に従事する者の適格性及び情報保全のための履行体制等
		要な会社。	事を熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
アイ情報設備	東京都文京区本駒込 6-5-3 ビューネ本駒込 9 階	・いすゞ藤沢工場での配線業務を実施するにあたり必要な会社。	・情報通信インフラ構築の配線業務を熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
ナイスキャリーサービス関東	埼玉県草加市青柳 3-22-1	・ローカル５Ｇ機器移設作業管理を行う。機器運搬作業管理に関する知見・技術に長けておりネットワーク機器運搬にあたり必要な会社。	・ネットワーク機器運搬において、機器運搬作業管理を熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
JESCO 株式会社	東京都中野区中央 4-3-4	・NTT 中央研修センタでの機器設置業務にあたり必要な会社。	・機器設置作業を熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
有限会社デジテック	東京都中央区勝どき 2-18-1 黎明スカイレジテル 1303	・東京大学における機器設置にあたり必要な会社。	・東京大学での工事をはじめとするネットワーク機器設置に関する知見・経験を有する。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
みなと通信株式会社	宮城県亘理町荒浜字西木倉 108-3	・東北大学での電気配線業務にあたり必要な会社。	・東北大学内の天井内配線及び端末処理や無線技術などを含む現場での工事について熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
新光電機株式会社	大阪府豊中市蛍池南町 3-9-1	・京都大学にローカル５Ｇ環境ケーブルに必要な会社。	・配線作業を熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
いすゞシステムサービス株式会社	東京都品川区南大井 6-26-1 大森ベルポート A 館	・いすゞ藤沢工場での施工管理及び安全管理を実施にあたり必要な会社。	・情報通信インフラ構築の施工管理及びそれに伴う安全管理を熟知。

名称	所在地	再委託する業務の範囲と必要性	再委託の業務に従事する者の適格性及び情報保全のための履行体制等
			・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
エス・イー・サービス	宮城県仙台市泉区松森字陣が原 8-1	東日本地域への機器運搬を行うにあたり必要な会社。	・システム機器運搬管理に多数の実績があり、情報通信インフラ構築に伴う機器運搬を熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。
髙吉輸送	大阪府寝屋川市池田北町 25-10	・京都大学への機器運搬を行うにあたり必要な会社。	・システム機器運搬管理に多数の実績があり、情報通信インフラ構築に伴う機器運搬を熟知。 ・東日本電信電話株式会社との委託契約中に機密保持に関する条項を明確化し情報保全を実施。

1.4 検証のスケジュール

検証は「図 1-4-1 検証のスケジュール」のとおり実施しました。

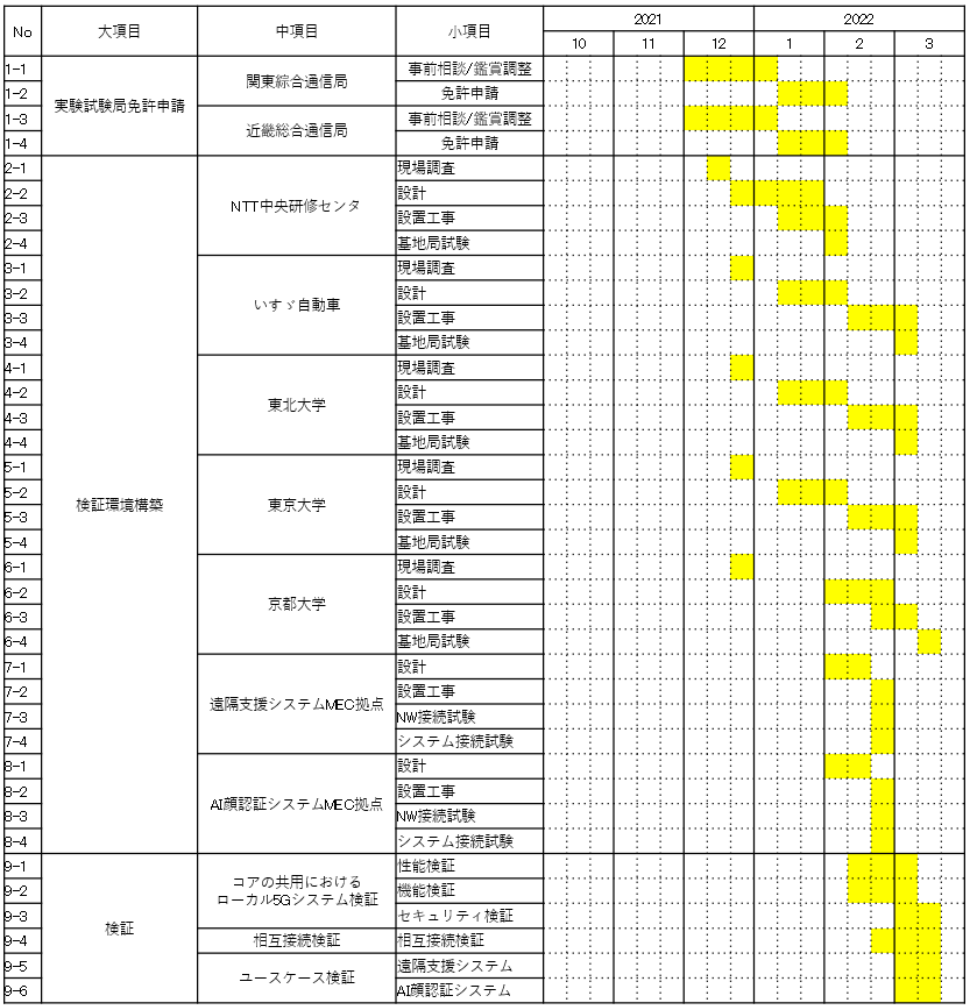


図 1-4-1　検証のスケジュール

1.5　免許申請の概要

(1) 申請者、申請先、申請概要

東日本電信電話株式会社及び京都大学を申請者として、関東総合通信局ならびに近畿総合通信局へ申請しました。

免許の種別は実験試験局であり、希望期間は免許の日より令和 4 年 3 月 31 日までとしています。

申請時のスケジュールについては「図 1-5-1-1　免許申請スケジュール」のとおりです。

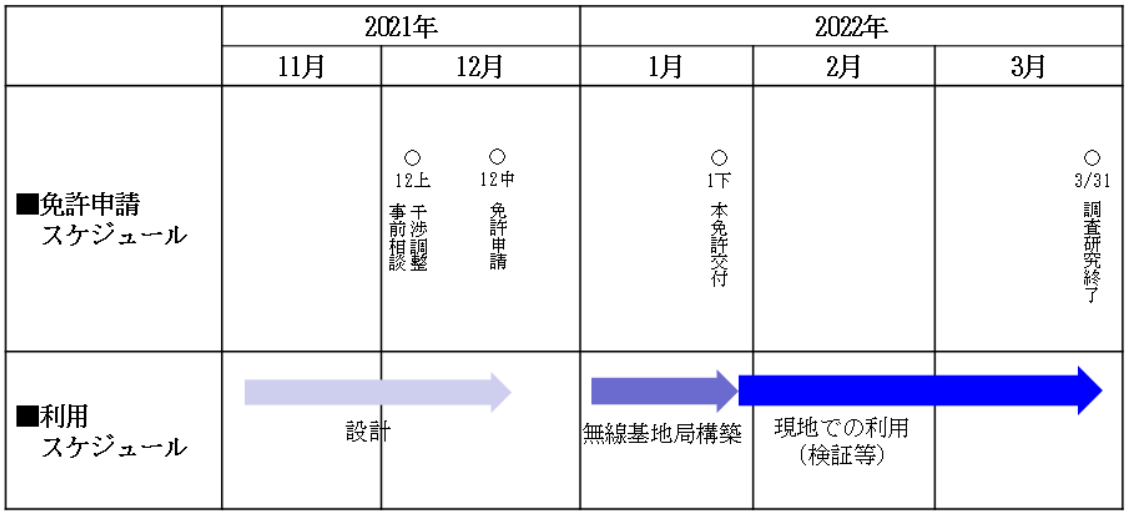


図 1-5-1-1　免許申請スケジュール

本実証では、複数の地方に跨って実験エリアを設けるため、以下のとおり、免許人及び申請先（総合通信局）を分けてそれぞれ対応しました。

・NTT 中央研修センタ、いすゞ自動車、東北大学、東京大学

免許人：東日本電信電話株式会社

申請先：関東総合通信局

・京都大学

免許人：京都大学

申請先：近畿総合通信局

周波数は 4.8-4.9GHz 帯を使用し、上り・下りリンクで時分割共用する TDD(Time Division Duplex)方式を用います。実験エリア内に基地局相当装置と陸上移動局相当装置を設置し双方向間で通信を行うものとしました。

・基地局相当：10 局（関東総合通信局：8 局、近畿総合通信局：2 局）

・陸上移動局相当：20 局（関東総合通信局：18 局、近畿総合通信局：2 局）

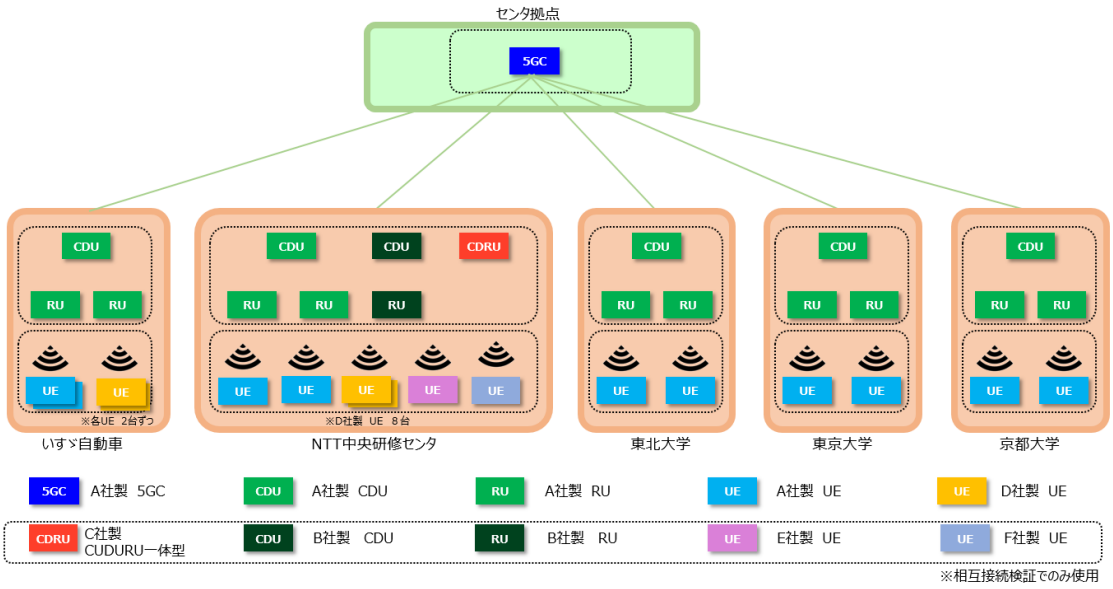


図 1-5-1-2　基地局配置イメージ図

なお、本検証において構築するローカル５Ｇシステムは本調査研究に資する検証にて使用し、電気通信事業には該当しないことから、本件に係る電気通信事業の届出は不要です。

IMSI は、「自らコアネットワークを構築して 運用する場合」かつ「自らの通信の利用のみ」に指定されている「999-002」から始まる番号を使用します。

無線局免許については、以下の点に留意し免許申請を行いました。

I.　無線局開設に係る免許関係諸経費は本実証の免許申請者の負担としました。

II.　本件契約締結後、速やかに周辺の携帯電話事業者等と周波数調整を開始し、合意を取った上で、総務省総合通信局等に無線局免許申請を行い、実証実験開始までに無線局免許を取得しました。また、干渉調整や登録点検で要する期間も考慮し、本実証契約後速やかに事前相談を行い、免許申請手続きを開始しました。

①　東日本電信電話株式会社が免許人となる無線局の諸元

表 1-5-1-1～表 1-5-1-5 の実験試験局について、関東総合通信局より免許を交付いただきました。

表 1-5-1-1　A 社製機器　実験試験局（基地局相当装置）

項目	実験試験局（基地局相当装置）
無線局数	8　局
識別信号	ひがしでんでんちゅうけんじっけんきち１～８
機器ベンダ	A社
中心周波数	4849.86MHz
占有帯域幅	99.72MHz
空中線構成	4T1R
電波の型式	99M7 X7W
変調方式	DL:OFDMA(QPSK,16QAM,64QAM,256QAM) UL:OFDMA(QPSK,16QAM,64QAM)
送信出力[W(dBm)](※)	16dBm(40mW)
空中線指向性(※)	無指向性
アンテナ利得(※)	5.0dBi/port
備考	適合表示無線設備
キャリアとの同期条件	同期TDD、準同期TDD1
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ内
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ内 ・宮城県仙台市青葉区片平二丁目1番1号　東北大学　片平キャンパス　電気通信研究所内 ・東京都文京区本郷七丁目3番1号　東京大学　本郷キャンパス内 ・神奈川県藤沢市土棚8　いすゞ自動車　藤沢第二工場内

表 1-5-1-2　A 社製機器　実験試験局（移動局相当装置）

項目	実験試験局（移動局相当装置）
無線局数	8　局
識別信号	ひがしでんでんちゅうけんじっけんたんまつ1～8
機器ベンダ	A社
中心周波数	4849.86MHz
占有帯域幅	100MHz
空中線構成	1T4R
電波の型式	100M D1A,D1B,D1C,D1D,D1F,D1X,D7W, G1A,G1B,G1C,G1D,G1F,G1X,G7W
変調方式	DL:OFDMA(QPSK,16QAM,64QAM,256QAM) UL:OFDMA(QPSK,16QAM,64QAM)
送信出力[W(dBm)]（※）	23dBm(200mW)
空中線指向性（※）	無指向性
アンテナ利得（※）	アンテナ1　TRx：2.3dBi アンテナ2　Rx：2.0dBi アンテナ3　Rx：1.1dBi アンテナ4　Rx：1.6dBi
備考	適合表示無線設備
キャリアとの同期条件	同期TDD、準同期TDD1
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ内
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ内 ・宮城県仙台市青葉区片平二丁目1番1号　東北大学 片平キャンパス 電気通信研究所内 ・東京都文京区本郷七丁目3番1号 東京大学 本郷 キャンパス内 ・神奈川県藤沢市土棚8　いすゞ自動車 藤沢第二工 場内

表 1-5-1-3　D 社製機器　実験試験局（移動局相当装置）

項目	実験試験局（移動局相当装置）
無線局数	8 局
識別信号	ひがしでんでんちゅうけんじっけんたんまつ9～16
機器ベンダ	D社
中心周波数	4849.86MHz
占有帯域幅	100MHz
空中線構成	1T4R
電波の型式	100M D1A,D1B,D1C,D1D,D1F,D1X,D7W,G1A,G1B,G1C,G1D,G1F,G1X,G7W
変調方式	OFDM (QPSK/16QAM/64QAM/256QAM)
送信出力[W(dBm)]（※）	23dBm(200mW)
空中線指向性（※）	無指向性
アンテナ利得（※）	2.4dBi
備考	適合表示無線設備
キャリアとの同期条件	同期TDD、準同期TDD1
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ内
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ内 ・神奈川県藤沢市土棚8　いすゞ自動車　藤沢第二工場内

表 1-5-1-4　E 社製機器　実験試験局（移動局相当装置）

項目	実験試験局（移動局相当装置）
無線局数	1　局
識別信号	ひがしでんでんちゅうけんじっけんたんまつ17
機器ベンダ	E社
中心周波数	4849.86MHz
占有帯域幅	100MHz
空中線構成	2T4R
電波の型式	100M D1A,D1B,D1C,D1D,D1F,D1X,D7W,G1A,G1B,G1C,G1D, G1F,G1X,G7W
変調方式	(CP-OFDM) QPSK, 16QAM, 64QAM (DFT-s-OFDM) Pi/2_BPSK, QPSK, 16QAM, 64QAM
送信出力[W(dBm)](※)	23dBm(200mW)
空中線指向性(※)	無指向性
アンテナ利得(※)	アンテナ1　TRx：0.4dBi アンテナ2　TRx：0.1dBi アンテナ3　RX：-3.1dBi アンテナ4　RX：-1.5dBi
備考	適合表示無線設備
キャリアとの同期条件	同期、準同期TDD1
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ内
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ内

表 1-5-1-5　F 社製機器　実験試験局（移動局相当装置）

項目	実験試験局（移動局相当装置）
無線局数	1　局
識別信号	ひがしでんでんちゅうけんじっけんたんまつ18
機器ベンダ	F社
中心周波数	4849.86MHz
占有帯域幅	100MHz
空中線構成	1T4R
電波の型式	100M D1A,D1B,D1C,D1D,D1F,D1X,D7W,G1A,G1B,G1C,G1D,G1F,G1X,G7W
変調方式	(CP-OFDM)QPSK, 16QAM, 64QAM, 256QAM (DFT-s-OFDM)QPSK, 16QAM, 64QAM, 256QAM
送信出力[W(dBm)]（※）	23dBm(200mW)
空中線指向性（※）	無指向性
アンテナ利得（※）	アンテナ1　TRx：0.4dBi アンテナ2　Rx：-0.1dBi アンテナ3　Rx：1.0dBi アンテナ4　Rx：0dBi
備考	適合表示無線設備
キャリアとの同期条件	同期、準同期TDD1
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ内
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ内

② 京都大学が免許人となる無線局の諸元

表 1-5-1-6～表 1-5-1-7 のとおり、実験試験局について近畿総合通信局より免許を交付いただきました。

表 1-5-1-6 A 社製機器 実験試験局（基地局相当装置） 京都大学

項目	実験試験局(基地局相当装置)
無線局数	2 局
機器ベンダ	A社
中心周波数	4849.86MHz
占有帯域幅	99.72MHz
空中線構成	4T1R
電波の型式	99M7 X7W
変調方式	DL:OFDMA(QPSK,16QAM,64QAM,256QAM) UL:OFDMA(QPSK,16QAM,64QAM)
送信出力[W(dBm)](※)	16dBm(40mW)
空中線指向性(※)	無指向性
アンテナ利得(※)	5.0dBi/port
備考	適合表示無線設備
キャリアとの同期条件	同期、準同期TDD1
常置場所	・京都府京都市左京区吉田本町 京都大学 吉田キャンパス 総合研究9号館内
移動範囲	・京都府京都市左京区吉田本町 京都大学 吉田キャンパス 総合研究9号館内

表 1-5-1-7　A 社製機器　実験試験局（移動局相当装置）　京都大学

項目	実験試験局(基地局相当装置)
無線局数	2　局
機器ベンダ	A社
中心周波数	4849.86MHz
占有帯域幅	99.72MHz
空中線構成	4T1R
電波の型式	99M7 X7W
変調方式	DL:OFDMA(QPSK,16QAM,64QAM,256QAM) UL:OFDMA(QPSK,16QAM,64QAM)
送信出力[W(dBm)](※)	16dBm(40mW)
空中線指向性(※)	無指向性
アンテナ利得(※)	5.0dBi/port
備考	適合表示無線設備
キャリアとの同期条件	同期、準同期TDD1
常置場所	・京都府京都市左京区吉田本町　京都大学　吉田キャンパス　総合研究9号館内
移動範囲	・京都府京都市左京区吉田本町　京都大学　吉田キャンパス　総合研究9号館内

干渉調整については、「表 1-5-1-8　　干渉調整先事業者」のとおり各事業者に対し実施しました。

表 1-5-1-8　　干渉調整先事業者

	事業者名
キャリア	NTT ドコモ
基地局	東京大学（コンソーシアムメンバ）
実験試験局	東京大学（コンソーシアムメンバ） 東京ケーブルネットワーク株式会社 日本電信電話株式会社

干渉調整の結果、共用利用に伴う運用制限又は技術制限は生じないことが確認でき、希望する申請内容で合意をいただくことができました。

またセキュリティ対策については下記の点を考慮し、構築を行いました。

・ ローカル５Ｇシステムとインターネット接続用回線の境界にはファイアウォール機能を具備したネットワーク装置を設置し適切な設定を行いました。
・ 拠点間のローカル５Ｇシステムの接続にあたっては、IPsec による暗号化方式を用いて接続しました。
・ 今回使用するローカル５Ｇ装置にはパスワード等の設定を行い、第三者による不正な設定変更等が行われないよう適切に管理しました。

(2) 次年度以降の申請対応

本実証検証は 2022/3/31 迄の調査研究となりますが、継続してコア共用に関連する検証及び相互接続検証を実施するため、一部の無線設備のみ無線局免許の有効期限を延伸する再免許申請を実施しました。

(3) 申請者を免許人とした理由

関東総合通信局管轄の無線局は、無線機器の常置場所を NTT 中央研修センタとしていることから、東日本電信電話株式会社を免許人としました。

近畿総合通信局管轄の無線局は、京都大学構内のみを使用するため、京都大学を免許人としました。

無線設備を常置する場所の保有者が免許人となることで、無線設備の管理・運用を適切に実施することを目的としています。

2.　実証環境

本検証の構築について、各検証パターン「複数企業共用パターン」、「業界共用パターン」と「相互接続検証」の３つに分けて以下で説明します。

2.1　複数企業共用パターン

複数企業共用パターンの検証では、「いすゞ自動車」と「NTT 中央研修センタ」に検証環境を構築しました。屋内にローカル５Ｇ基地局を設置して検証を行いました。詳細は「3.1 章　ネットワーク構成」にて示します。

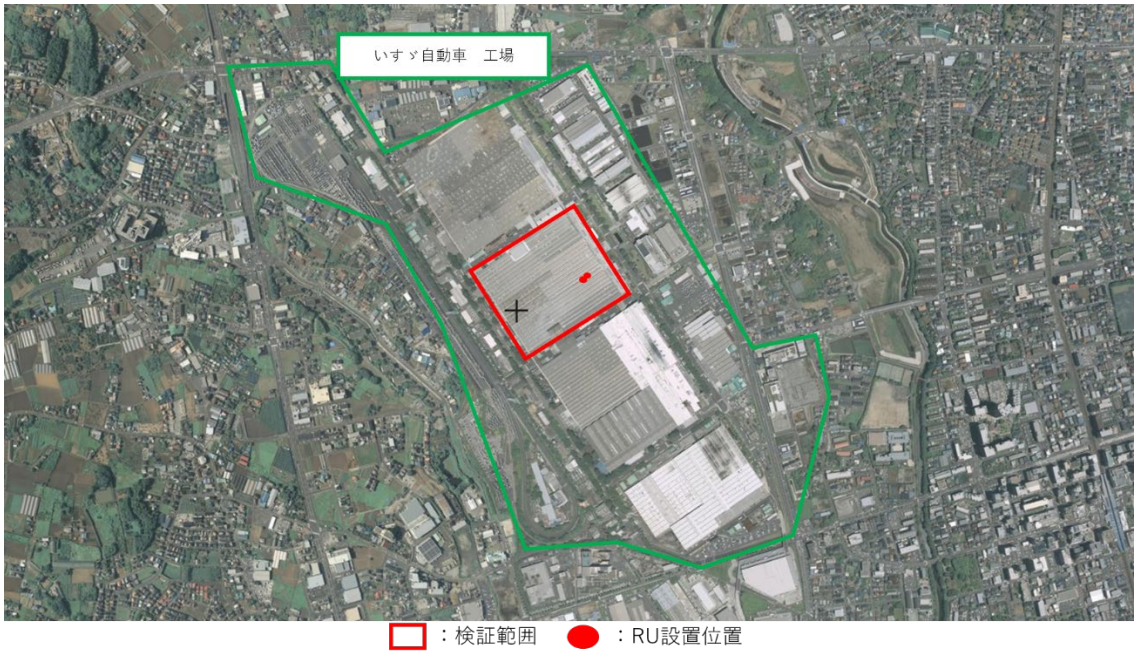


図 2-1-1　いすゞ自動車検証エリア　全体
（国土地理院地理院地図を加工。以後、航空写真については特記無い場合同じ）

図 2-1-2　いすゞ自動車検証エリア

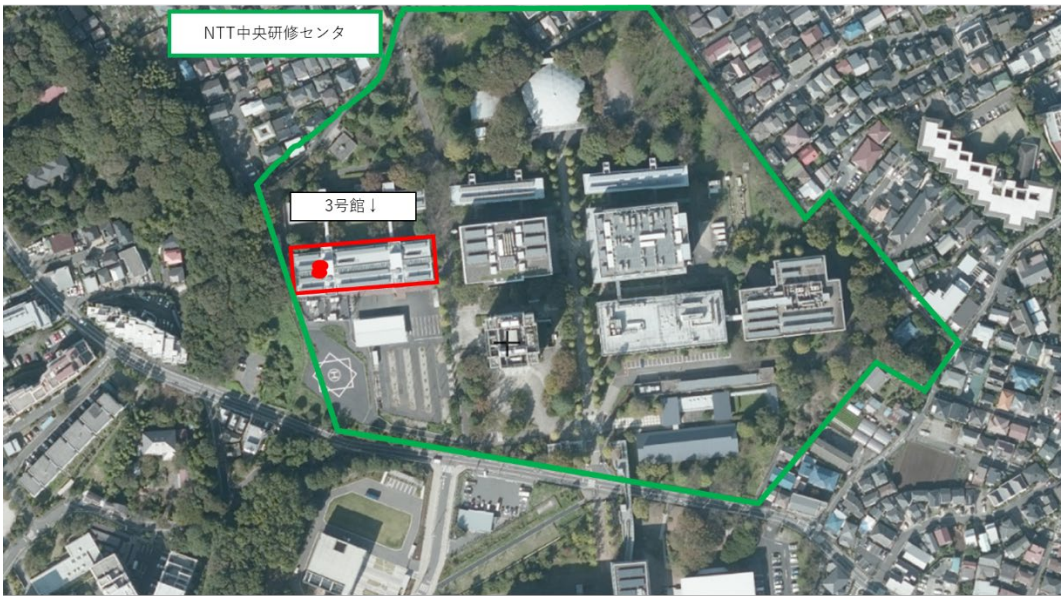


図 2-1-3　　NTT 中央研修センタ 検証エリア　全体

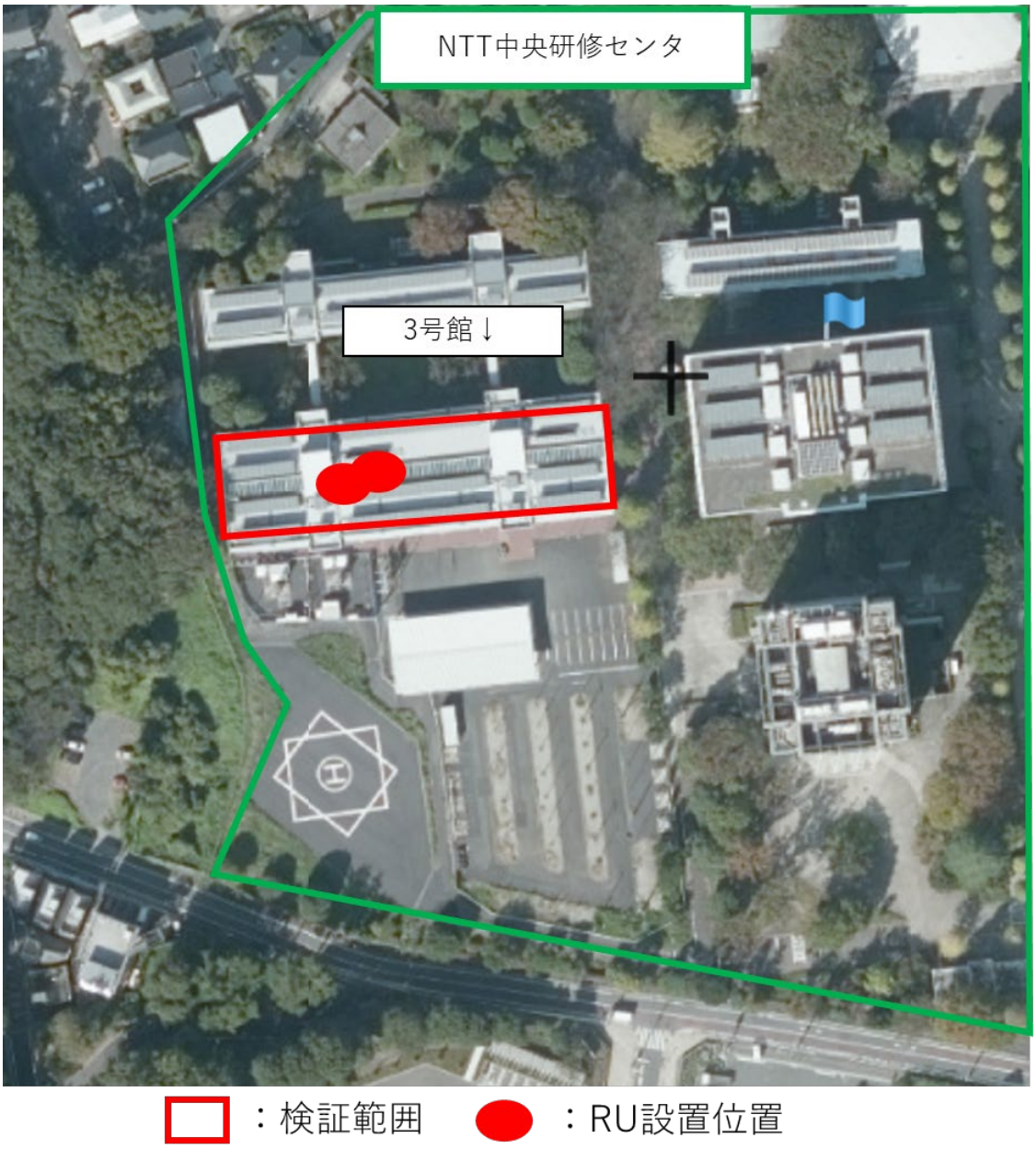


図 2-1-4　NTT 中央研修センタ 検証エリア　3 号館

2.2 業界共用パターン

業界共用パターンの検証では、「東北大学」、「東京大学」、「京都大学」に検証環境を構築しました。屋内にローカル５Ｇ基地局、RU と UE を設置して検証を行いました。詳細は「3.1 章　ネットワーク構成」にて示します。

図 2-2-1 東北大学　検証エリア全体

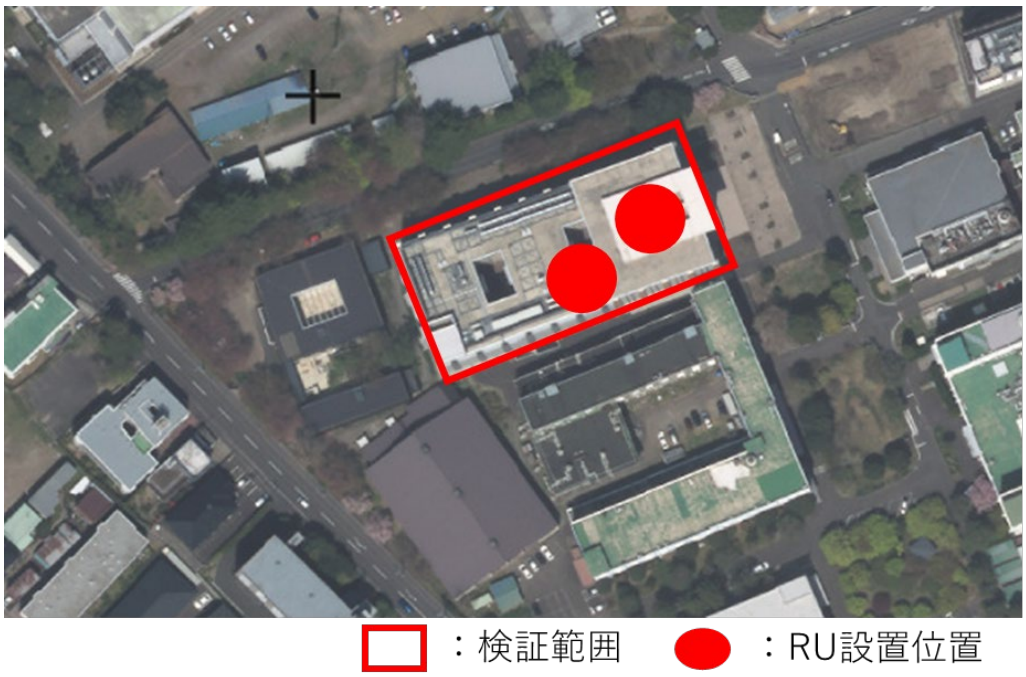


図 2-2-2 東北大学　検証エリア　電気通信研究所

図 2-2-3 東京大学　検証エリア全体

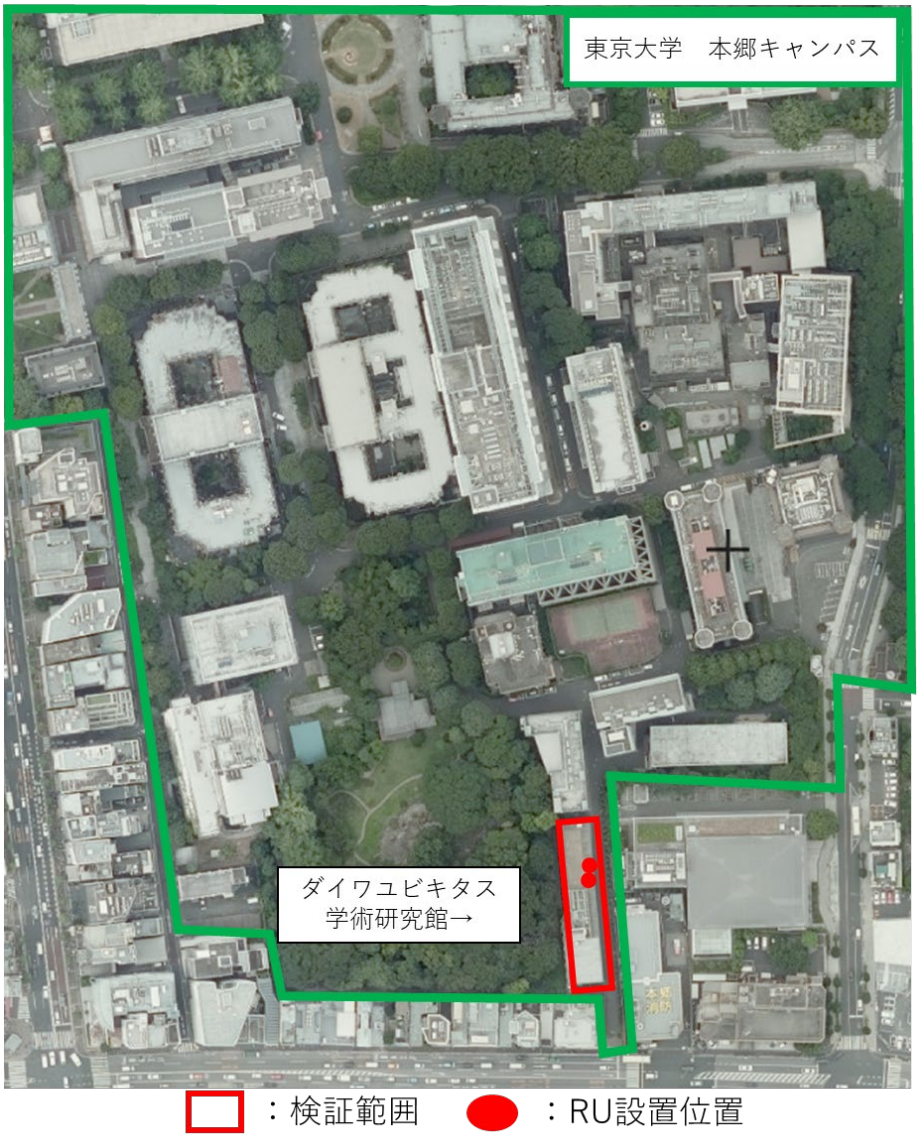


図 2-2-4 東京大学　検証エリア　ダイワユビキタス学術研究館

図 2-2-5 京都大学　検証エリア　全体

図 2-2-6 京都大学　検証エリア　総合研究 9 号館

2.3 相互接続検証

相互接続検証では、「NTT 中央研修センタ」に検証環境を構築しました。屋内にローカル５Ｇ基地局を設置して検証を行いました。詳細は「3.1 章　ネットワーク構成」にて示します。

3. 検証環境の構築

3.1 ネットワーク構成

(1) ネットワーク・システム構成図（全体像）

本検証において構築したシステムの構成図を図 3-1-1-1～図 3-1-1-5 に示します。

センタ拠点（SINET DC）に設置した 5G コア用基盤サーバのハードウェア 1 台にローカル５Ｇ基地局 5 拠点を拠点毎に異なる仮想マシン（5G コア VM）に収容しました。5G コア VM は、ローカル５Ｇのコアシステムの UPF 以外の C-Plane 機能と UPF の U-Plane 機能を分割配備することを可能としました。また、UTM 用基盤サーバ上でセキュリティ機能を提供する仮想マシンである UTM VM 及び WAF VM は、仮想マシン内で更に基地局 5 拠点を仮想化収容することで 5 拠点間での共有を実現しています。DNS 用基盤サーバには、検証環境を構成する上で必要となる DNS や疎通確認等をするための検証で必要となる仮想マシンを配置しています。各基盤サーバは、通信帯域の輻輳を回避するために、予め複数の回線でネットワークに接続、必要に応じて帯域を追加することが可能な構成としています。

センタ拠点には基地局 5 拠点を接続するための回線として、複数企業共用パターン用のベストエフォート回線、業界共用パターン用のギャランティ回線、ユースケースを提供するベストエフォート回線を配置しています。

他、センタ拠点では、AI 顔認証システムと通信するために必要となるカメラゲートウェイ（カメラ GW）、遠隔でシステム運用を行うためのオペレータ拠点とセンタ拠点を接続するベストエフォート回線、コンソールサーバも配置しています。システムの遠隔運用は、センタ拠点だけでなく、ローカル５Ｇ基地局が配置された 5 拠点もセンタ拠点を介すことで可能です。

ローカル５Ｇ基地局の 5 拠点には、基地局（CDU-A、CDU-C、RU-A）や高精度な時刻同期を RU に提供するグランドマスタークロック（GMC）、PTP 対応 L2SW を配置することに加え、ローカル５ＧコアシステムのU-Plane 機能のみを具備した仮想マシン（UPF VM）が稼働する拠点 UPF サーバを配置しています。また、業界共用パターンの拠点には、SINET を介したセンタ拠点との接続でセキュリティ機能を提供する UTM、拠点 UPF サーバ上の UPF VM を利用しての AI 顔認証システムとの通信に必要なカメラ GW も配置しています。

複数企業共用パターン、業界共用パターン共に、遠隔運用のコンソールサーバをセンタ拠点同様に配置しました。NTT 中央研修センタは、複数企業共用パターンと業界共用パターンを兼ねる拠点のため、両パターンの機器、回線が配置されています。

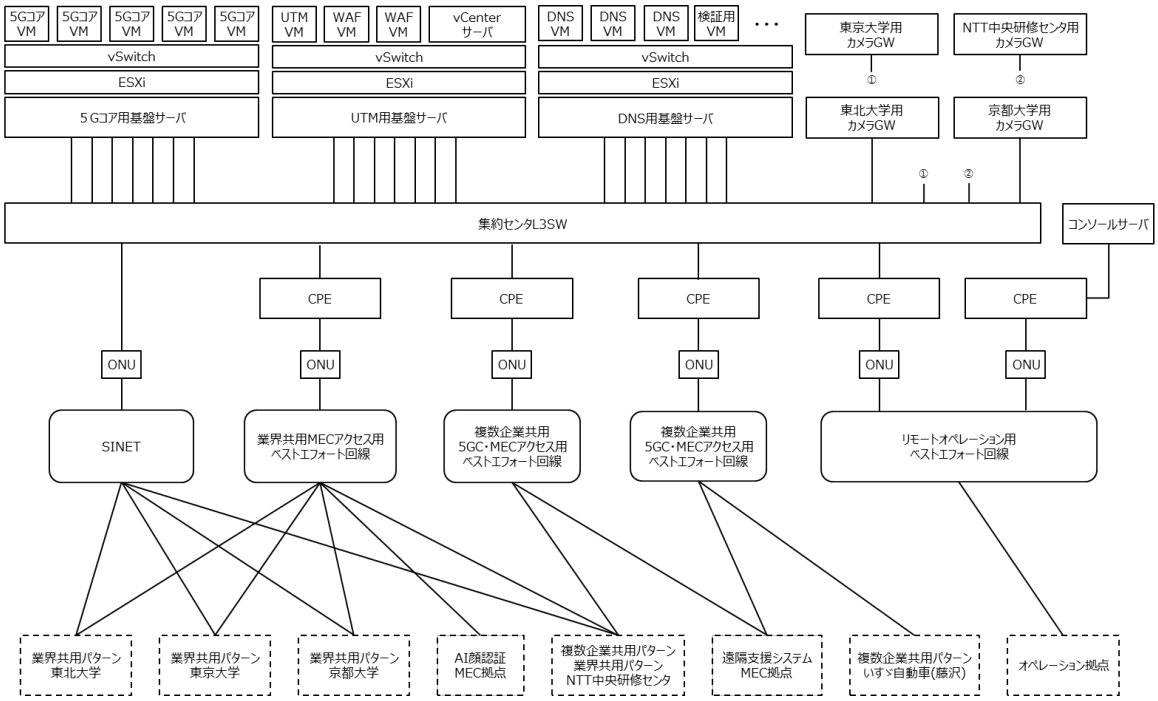


図 3-1-1-1 センタ拠点（SINET DC） ネットワーク構成図

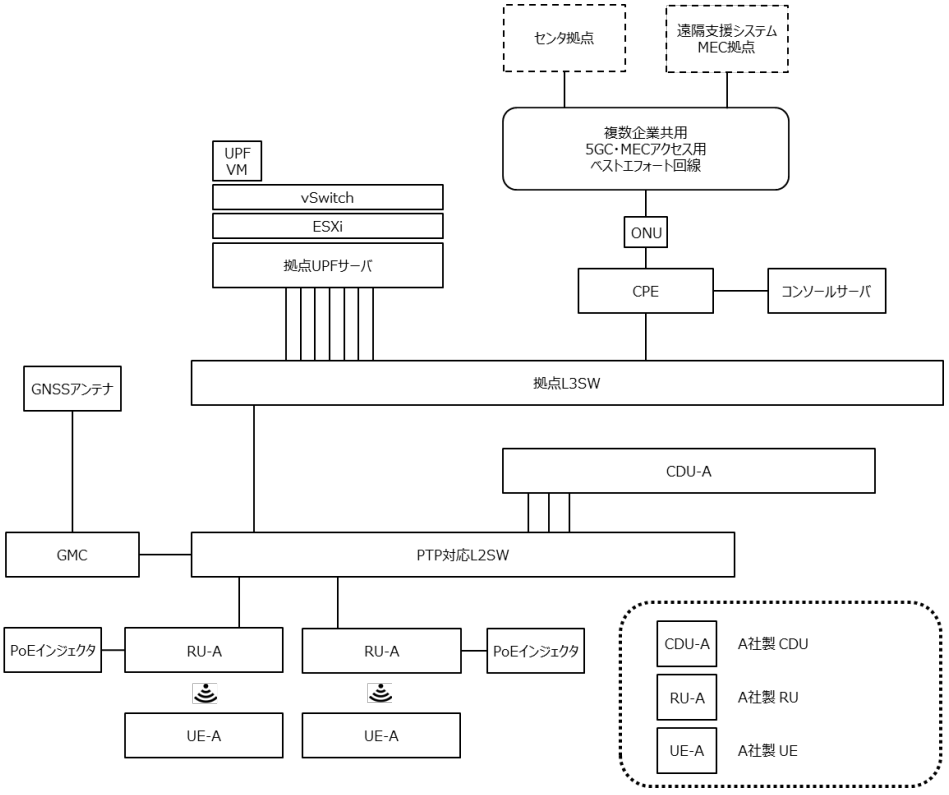


図 3-1-1-2 いすゞ自動車 ネットワーク構成図

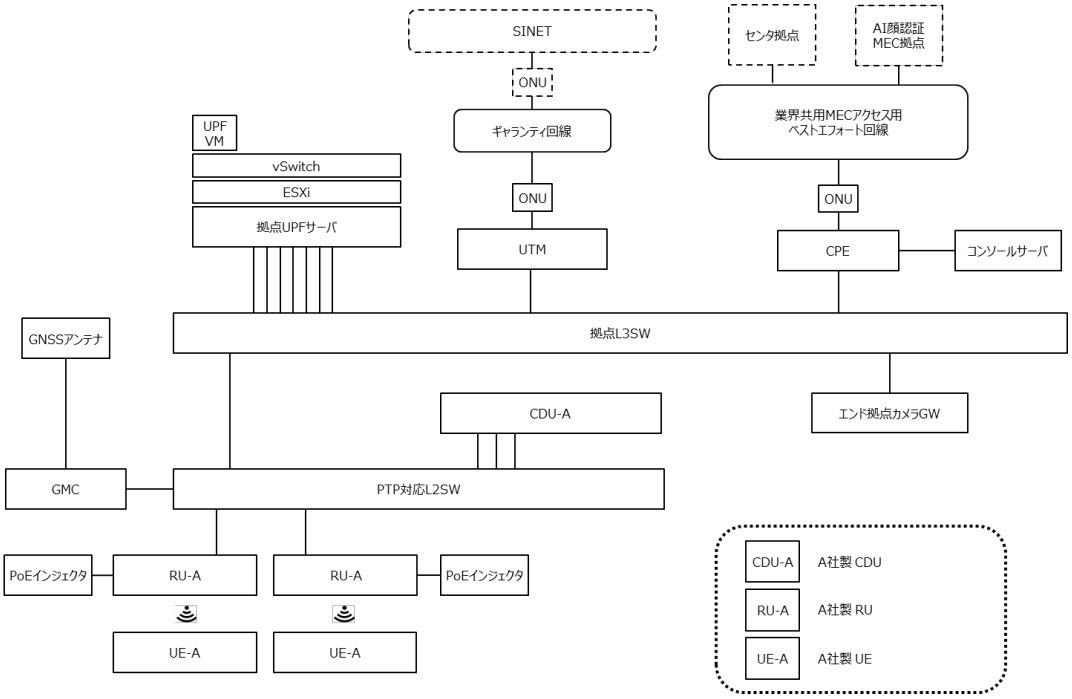


図 3-1-1-3 東北大学、東京大学、京都大学 ネットワーク構成図

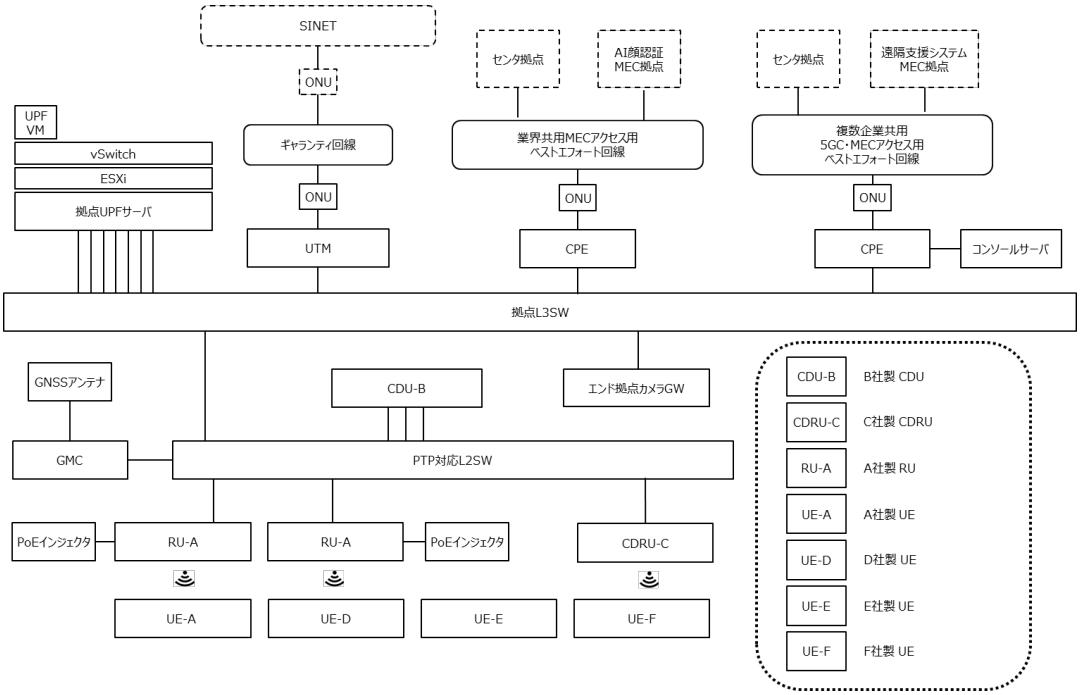


図 3-1-1-4 NTT 中央研修センタ ネットワーク構成図

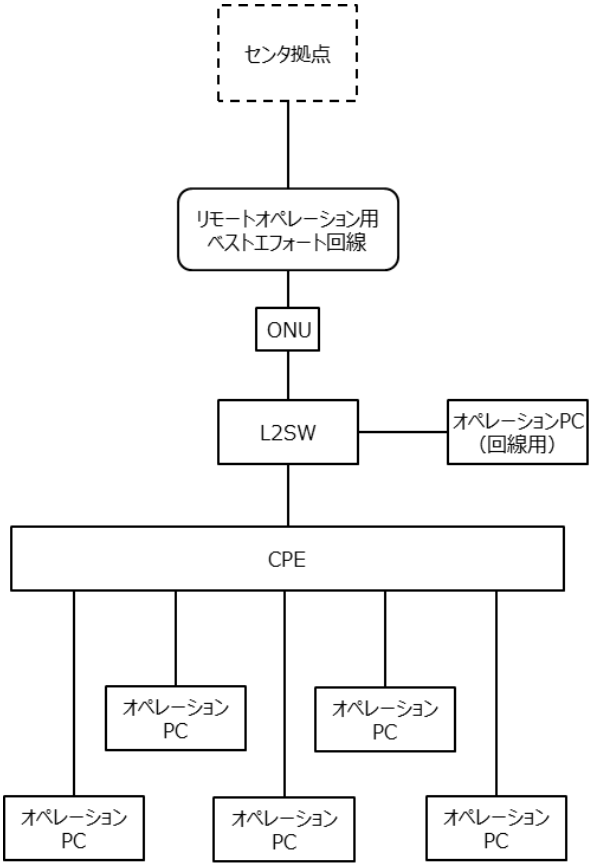


図 3-1-1-5 オペレータ拠点 ネットワーク構成図

(2) センタ拠点・エンド拠点間ネットワーク

拠点間ネットワークを図 3-1-2-1 に示します。拠点間ネットワークは、センタ拠点(SINET DC)、複数企業共用パターン拠点(いすゞ自動車、NTT 中央研修センタ)、業界共用パターン拠点(東北大学、東京大学、京都大学)、AI 顔認証システム拠点、遠隔支援システム拠点を結ぶネットワークから構成されます。

センタ拠点(SINET DC)と複数企業共用パターン拠点であるいすゞ自動車と NTT 中央研修センタ、AI 顔認証システム拠点、遠隔支援システム拠点を結ぶネットワークには、VPN 機能が提供可能な Software Defined Network (SDN) の 1Gbps のベストエフォート回線を使用しました。SDN では、将来的に複数企業共用パターン拠点でインターネットアクセスを必要とした場合には、ローカルブレークアウトやセキュアなインターネットアクセスのオプションサービスが利用可能です。また、センタ拠点(SINET DC)と業界共用パターン拠点である東北大学、東京大学、京都大学、NTT 中央研修センタを結ぶネットワークには、1Gbp もしくは 100Mbps のギャランティ回線、および国立情報学研究所が提供する学術情報ネットワーク SINET を使用しています。

複数企業共用パターン(ベストエフォート)と業界共用パターン(ギャランティ)で異なる回線を用意し、回線種別によるそれぞれのユースケースへの影響の比較、遅延等性能への比較を行います。

複数企業共用パターンでは、ローカル５ＧのC-Plane通信及びU-Plane通信、遠隔支援システムとの通信は、複数企業共用パターンSDN上で行われます。回線を統合することでセンタ拠点及びユースケースを提供する拠点への安価な接続を提供しています。なお、異なる企業間の通信は、SDNのVPN機能により制限されています。

業界共用パターンでは、ローカル５ＧのC-Plane通信及びU-Plane通信は、学術用ネットワークのSINETを介したギャランティ回線上で行われ、AI顔認証システムとの通信は業界共用パターン SDN を介して行われます。将来的に業界共用パターン拠点で特定のユースケースをギャランティ回線で安定して利用すると同時に、SDNを介して多様なユースケースを利用することも可能な構成となっています。

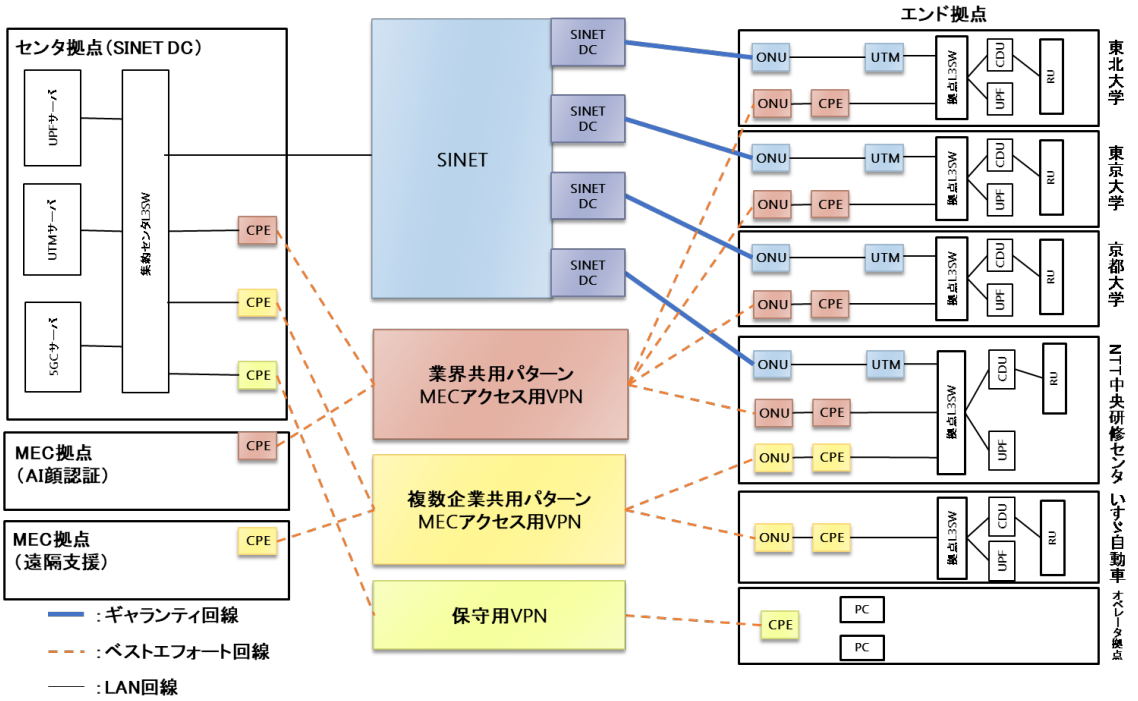


図 3-1-2-1 拠点間ネットワーク

表 3-1-2-1 各拠点での用途と回線

拠点	用途	回線
センタ拠点	5GC 設置	・SINET ・1Gbps ギャランティ回線 ・1Gbps ベストエフォート回線
いすゞ自動車	複数企業共用パターン検証	・1Gbps ベストエフォート回線
NTT 中央研修センタ	複数企業共用パターン検証	・1Gbps ベストエフォート回線
	業界共用パターン検証	・1Gbps ギャランティ回線
	相互接続検証	・1Gbps ギャランティ回線 ・1Gbps ベストエフォート回線
東北大学	業界共用パターン検証	・1Gbps ギャランティ回線 ・1Gbps ベストエフォート回線
東京大学	業界共用パターン検証	・1Gbps ギャランティ回線 ・1Gbps ベストエフォート回線

京都大学	業界共用パターン検証	・100Mbps ギャランティ回線 ・1Gbps ベストエフォート回線
オペレータ拠点	センタ拠点の機器運用	・1Gbps ベストエフォート回線

RU と UE の距離と角度は各拠点の周辺環境によって、「図 3-1-2-2　RU-UE の距離/方向の考え方」、「表 3-1-2-2　RU-UE の距離/方向」のように UE の設置位置を調整しました。

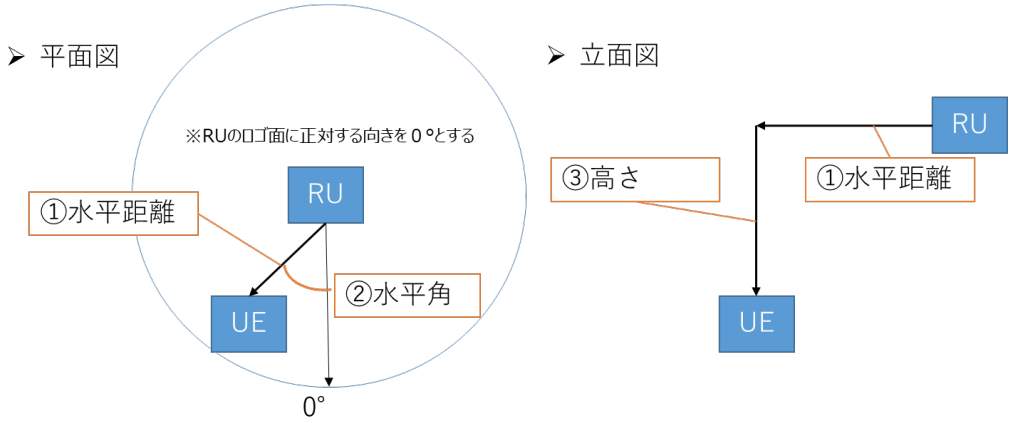


図 3-1-2-2　RU-UE の距離/方向の考え方

表 3-1-2-2　RU-UE の距離/方向

設置拠点	水平距離[m]	水平角[°]	高さ[m]	備考
NTT 中央研修センタ	2	≒45	2.0	
東北大学	5	≒180	1.5	間に壁あり
東京大学	5	≒0	1.5	
京都大学	3	≒0	1.5	
いすゞ自動車 (360° カメラ)	2	≒45	2.0	
いすゞ自動車 (ウェアラブルカメラ)	0～20	0～360	1.0	UE を持ち歩いた

(3) 遠隔支援システム

複数企業共用パターンのユースケース検証で利用した遠隔支援システムについて、全体構成を「図 3-1-3-1　遠隔支援システム全体構成」に示します。ローカル５Ｇシステム上で利用する本システムは、遠隔支援システムサーバ、ウェアラブルカメラと 360 度カメラ、コックピット PC で構成されます。サーバは、「図 3-1-2-1　拠点間ネットワーク」に示す遠隔支援システム拠点に設置、ウェアラブルカメラと 360 度カメラ、コックピット PC のセットはエンド拠点で利用します。いすゞ自動車と NTT 中央研修センタに、それぞれ 2 セットずつ計 4 セットを配置し、同時利用が可能な構成となっています。

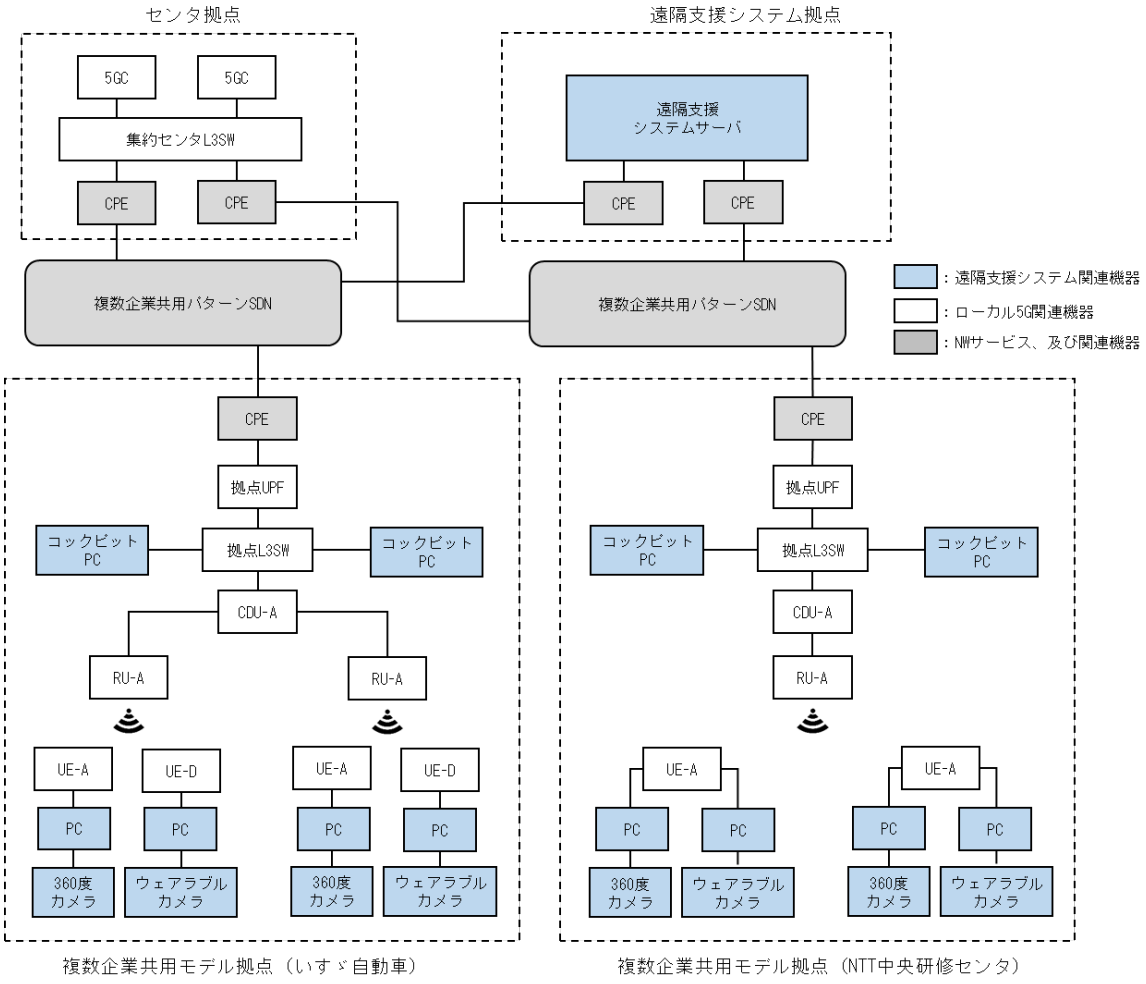


図 3-1-3-1　遠隔支援システム全体構成

(4) AI 顔認証システム

業界共用パターンのユースケース検証で利用した AI 顔認証システムについて、全体構成を「図 3-1-4-1 AI 顔認証システム全体構成」に示します。ローカル５Ｇシステム上で利用する本システムは、AI 顔認証サーバ、カメラとカメラゲートウェイ（カメラ GW）、閲覧用 PC で構成されます。

AI 顔認証サーバは、「図 3-1-2-1 拠点間ネットワーク」に示す AI 顔認証システム拠点に、カメラとカメラ GW は東北大学、東京大学、京都大学、NTT 中央研修センタに配置しました。カメラ GW については、センタ拠点に配置されたローカル５Ｇコアシステムの U-Plane 機能を利用するためにセンタ拠点にも設置しています。AI 顔認証システムの認証結果の閲覧は、閲覧用 PC が設置された NTT 中央研修センタで行いました。

なお、遠隔支援システム同様に業界共用パターン全拠点での同時利用も可能な構成になっています。

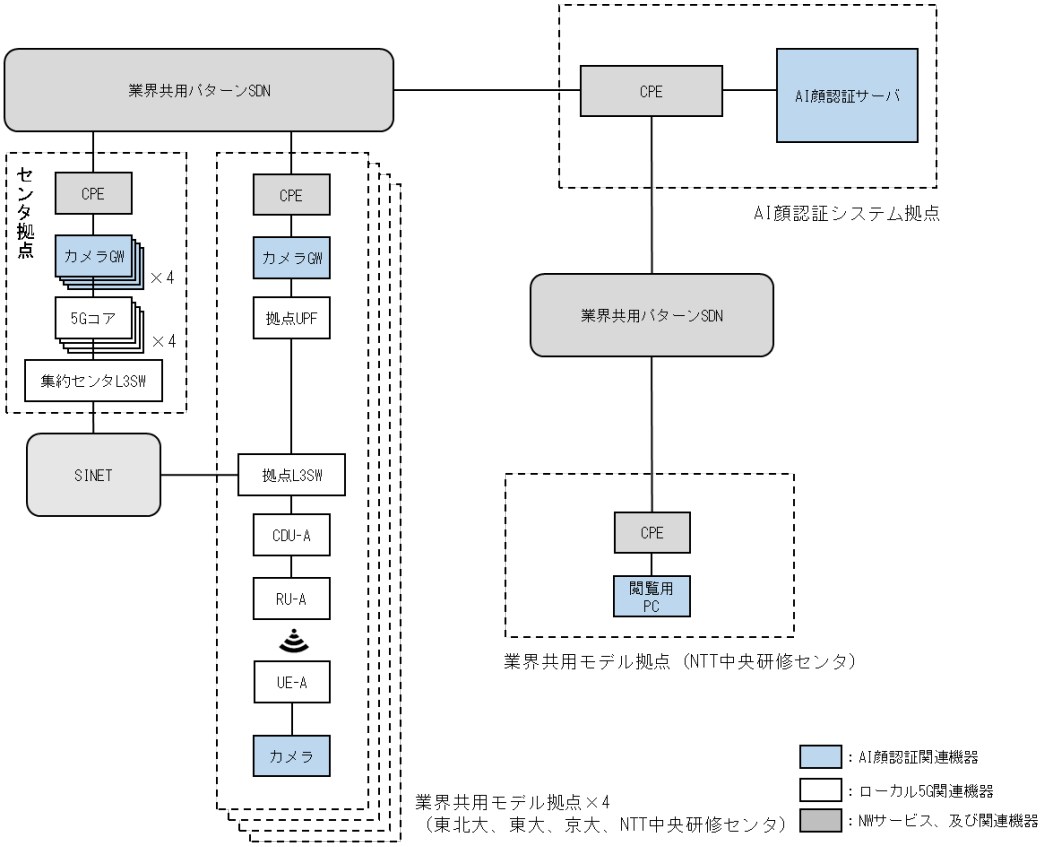


図 3-1-4-1　AI 顔認証システム全体構成

3.2 ネットワーク・システム構成機器

本検証において構築したシステムを構成する機器類を表 3-2-1～表 3-2-9 に示します。

表 3-2-1　ローカル５Ｇネットワーク機器一覧　センタ拠点（SINET DC）

No.	物品	メーカ	型番	数量	備考
1	5G コア用基盤サーバ	J 社	XXXXXXXXXX	1	CPU：Intel Xeon 32 コア メモリ：288GB DISK：1.6TB
		A 社	XXXXXXXXXX	5	5G コア C-Plane 機能
		A 社	XXXXXXXXXX	5	5G コア U-Plane 機能
		K 社	XXXXXXXXXX	2	仮想基盤ソフト
2	UTM 用基盤サーバ	J 社	XXXXXXXXXX	1	CPU：Intel Xeon 32 コア メモリ：288GB DISK：1.6TB
		L 社	XXXXXXXXXX	1	UTM VM 仮想アプライアンス
		L 社	XXXXXXXXXX	1	UTM VM Upgrade License
		L 社	XXXXXXXXXX	1	IPS ライセンス
		L 社	XXXXXXXXXX	1	UTM VM 製品保守
		L 社	XXXXXXXXXX	2	Web Application Firewall 仮想アプライアンス
		L 社	XXXXXXXXXX	2	WAF VM 製品保守
		K 社	XXXXXXXXXX	2	仮想基盤ソフト
		K 社	XXXXXXXXXX	1	仮想基盤管理ソフト
3	DNS 用基盤サーバ	J 社	XXXXXXXXXX	1	CPU：Intel Xeon 32 コア メモリ：288GB DISK：1.6TB
		M 社	XXXXXXXXXX	3	DNS VM 試験用 VM
		K 社	XXXXXXXXXX	2	仮想基盤ソフト
5	センタ拠点 L3SW	N 社	XXXXXXXXXX	1	
6	コンソールサーバ	O 社	XXXXXXXXXX	1	

表 3-2-2　ローカル５Ｇネットワーク機器一覧　複数企業共用パターン拠点（いすゞ自動車）

No.	物品	メーカ	型番	数量	備考
1	拠点 L3SW	N 社	XXXXXXXXXX	1	
2	コンソールサーバ	O 社	XXXXXXXXXX	1	
3	拠点 UPF サーバ	J 社	XXXXXXXXXX	1	CPU：Intel Xeon 16 コア メモリ：32GB DISK：800G
		A 社	XXXXXXXXXX	1	5G コア U-Plane 機能
		K 社	XXXXXXXXXX	2	仮想基盤ソフト
4	PTP 対応 L2SW	A 社	XXXXXXXXXX	1	
5	CDU-A	A 社	XXXXXXXXXX	1	
6	RU-A	A 社	XXXXXXXXXX	2	
7	UE-A	A 社	XXXXXXXXXX	2	
8	GMC	O 社	XXXXXXXXXX	1	

表 3-2-3　ローカル５Ｇネットワーク機器一覧　業界共用パターン拠点（東北大学）

No.	物品	メーカ	型番	数量	備考
1	拠点 L3SW	N 社	XXXXXXXXXX	1	
2	コンソールサーバ	O 社	XXXXXXXXXX	1	
3	UTM	L 社	XXXXXXXXXX	1	
		L 社	XXXXXXXXXX	1	ライセンス + 製品保守
4	拠点 UPF サーバ	J 社	XXXXXXXXXX	1	CPU：Intel Xeon 16 コア メモリ：32GB DISK：800G
		A 社	XXXXXXXXXX	1	5G コア U-Plane 機能
		K 社	XXXXXXXXXX	2	仮想基盤ソフト
5	PTP 対応 L2SW	A 社	XXXXXXXXXX	1	
6	CDU-A	A 社	XXXXXXXXXX	1	
7	RU-A	A 社	XXXXXXXXXX	2	
8	UE-A	A 社	XXXXXXXXXX	2	
9	GMC	O 社	XXXXXXXXXX	1	

表 3-2-4　ローカル５Ｇネットワーク機器一覧　業界共用パターン拠点（東京大学）

No.	物品	メーカ	型番	数量	備考
1	拠点 L3SW	N 社	XXXXXXXXXX	1	
2	コンソールサーバ	O 社	XXXXXXXXXX	1	
3	UTM	L 社	XXXXXXXXXX	1	
		L 社	XXXXXXXXXX	1	ライセンス + 製品保守
4	拠点 UPF サーバ	J 社	XXXXXXXXXX	1	CPU：Intel Xeon 16 コア メモリ：32GB DISK：800G
		A 社	XXXXXXXXXX	1	5G コア U-Plane 機能
		K 社	XXXXXXXXXX	2	仮想基盤ソフト
5	PTP 対応 L2SW	A 社	XXXXXXXXXX	1	
6	CDU-A	A 社	XXXXXXXXXX	1	
7	RU-A	A 社	XXXXXXXXXX	2	
8	UE-A	A 社	XXXXXXXXXX	2	
9	GMC	O 社	XXXXXXXXXX	1	

表 3-2-5　ローカル５Ｇネットワーク機器一覧　業界共用パターン拠点（京都大学）

No.	物品	メーカ	型番	数量	備考
1	拠点 L3SW	N 社	XXXXXXXXXX	1	
2	コンソールサーバ	O 社	XXXXXXXXXX	1	
3	UTM	L 社	XXXXXXXXXX	1	
		L 社	XXXXXXXXXX	1	ライセンス + 製品保守
4	拠点 UPF サーバ	J 社	XXXXXXXXXX	1	CPU：Intel Xeon 16 コア メモリ：32GB DISK：800G
		A 社	XXXXXXXXXX	1	5G コア U-Plane 機能
		K 社	XXXXXXXXXX	2	仮想基盤ソフト
5	PTP 対応 L2SW	A 社	XXXXXXXXXX	1	
6	CDU-A	A 社	XXXXXXXXXX	1	
7	RU-A	A 社	XXXXXXXXXX	2	
8	UE-A	A 社	XXXXXXXXXX	2	
9	GMC	O 社	XXXXXXXXXX	1	

表 3-2-6　ローカル５Ｇネットワーク機器一覧　複数企業共用パターン・相互接続検証拠点（NTT 中央研修センタ）

No.	物品	メーカ	型番	数量	備考
1	拠点 L3SW	N 社	XXXXXXXXXX	1	
2	コンソールサーバ	O 社	XXXXXXXXXX	1	
3	UTM	L 社	XXXXXXXXXX	1	
		L 社	XXXXXXXXXX	1	ライセンス + 製品保守
4	拠点 UPF サーバ	J 社	XXXXXXXXXX	1	CPU：Intel Xeon 16 コア メモリ：32GB DISK：800G
		A 社	XXXXXXXXXX	1	5G コア U-Plane 機能
		K 社	XXXXXXXXXX	2	仮想基盤ソフト
5	PTP 対応 L2SW	A 社	XXXXXXXXXX	1	
6	CDU-B	B 社	XXXXXXXXXX	1	
7	CDRU-C	C 社	XXXXXXXXXX	1	
8	CDRU-C 用暗箱	P 社	XXXXXXXXXX	1	
9	RU-A	A 社	XXXXXXXXXX	2	
10	RU-B	B 社	XXXXXXXXXX	1	
11	UE-A	A 社	XXXXXXXXXX	2	
12	UE-D	D 社	XXXXXXXXXX	8	
13	UE-E	E 社	XXXXXXXXXX	1	
14	UE-F	F 社	XXXXXXXXXX	1	
15	GMC	O 社	XXXXXXXXXX	1	

表 3-2-7　ローカル５Ｇネットワーク機器一覧　運用拠点（オペレータ拠点）

No.	物品	メーカ	型番	数量	備考
1	オペレーション PC	Q 社	XXXXXXXXXX	6	

表 3-2-8　遠隔支援システム機器一覧

No.	物品	メーカ	型番	数量	備考
1	ウェアラブルカメラ	R 社	XXXXXXXXXX	4	
2	360 度カメラ	S 社	XXXXXXXXXX	4	
3	ウェアラブルカメラ接続用 PC	T 社	XXXXXXXXXX	4	
4	360 度カメラ接続用 PC	T 社	XXXXXXXXXX	4	

表 3-2-9　AI 顔認証システム機器一覧

No.	物品	メーカ	型番・品名	数量	備考
1	ネットワークカメラ	U 社	XXXXXXXXXX	一式	
2	カメラ GW	V 社	XXXXXXXXXX	一式	
3	GPU サーバ	J 社	XXXXXXXXXX	一式	
4	AI 顔認証ソフトウェア	W 社	XXXXXXXXXX	一式	

3.3 ネットワーク・システム構成機器仕様

本検証において構築したシステムを構成する機器類の仕様を示します。

(ア) 5G コア用基盤サーバ

本ローカル５Ｇシステムのコア装置は、5G コア用基盤サーバにて構成されます。5G コア用基盤サーバはローカル５Ｇシステムのソフトウェアを仮想化搭載します。ハードウェアはサーバ 1 台をセンタ拠点（SINET DC）内のラックに設置しています。

表 3-3-1 5G コア用基盤サーバ仕様

項目	仕様	備考
電源	100-120/200-240VAC	
消費電力	800W パワーサプライ(80PLUS Platinum モデル)×2、最大 2 基、リダンダント構成	
CPU	Intel® Xeon® Gold (16 コア 32 スレッド)×2	
メモリ容量	288GB	
DISK 容量	1.6TB	
概算質量	16.27kg（最大）	
外形寸法	4346×7498×429 mm、1U ラックマウント型	

（イ） UTM 用基盤サーバ

UTM 用基盤サーバを 1 台、センタ拠点（SINET DC）内のラックに設置しています。

表 3-3-2 UTM 用基盤サーバ仕様

項目	仕様	備考
電源	100-120/200-240VAC	
消費電力	800W パワーサプライ(80PLUS Platinum モデル)×2、最大 2 基、リダンダント構成	
CPU	Intel® Xeon® Gold (16 コア 32 スレッド)×2	
メモリ容量	288GB	
DISK 容量	1.6TB	
概算質量	16.27kg（最大）	
外形寸法	4346×7498×429 mm、1U ラックマウント型	

（ウ） DNS 用基盤サーバ

DNS 用基盤サーバを 1 台、センタ拠点（SINET DC）内のラックに設置しています。

表 3-3-3 UPF 用基盤サーバ仕様

項目	仕様	備考
電源	100-120/200-240VAC	
消費電力	800W パワーサプライ(80PLUS Platinum モデル)×2、最大 2 基、リダンダント構成	
CPU	Intel® Xeon® Gold（16 コア 32 スレッド)×2	
メモリ容量	288GB	
DISK 容量	1.6TB	
概算質量	16.27kg（最大）	
外形寸法	4346×7498×429 mm、1U ラックマウント型	

（エ） L3SW

センタ拠点（SINET DC）では 5G コア用基盤サーバ、UTM 用基盤サーバ、DNS 用基盤サーバを接続する機器として L3 スイッチを 1 台構築しました。また、複数企業共用パターン拠点、業界共用パターン拠点では PTP 対応 L2SW、拠点 UPF サーバ、WAN 回線を収容する機器類を接続する機器として L3 スイッチを各拠点 1 台（計 5 台）構築しています。各 L3 スイッチは各拠点内のラックに設置しました。

表 3-3-4 L3SW 仕様

項目	仕様	備考
スイッチング容量	最大 480Gbps	
外形寸法	444.5（W）×44（H）×547（D）（mm）	
重量	10.7 kg	
最大定格電力	950W	

（オ） コンソールサーバ

5G コア用基盤サーバ、UTM 用基盤サーバ、DNS 用基盤サーバ、センタ拠点 L3SW、拠点 L3SW、GMC、拠点 UPF サーバを遠隔から運用保守するために、コンソールサーバを全拠点に 1 台ずつ合計 6 台構築しました。コンソールサーバは各拠点内のラックに設置しています。

表 3-3-5 コンソールサーバ仕様

項目	仕様	備考
電源	AC100V～240V	
消費電力	17W	
LAN ポート	10Base-T/100Base-TX / 1000Base-T 対応 2 ポート Auto Negotiation 対応・Auto-MDI/MDI-X 対応 ボンディング機能（アクティブ-スタンバイ方式） IPv4/IPv6	
シリアルポート数	RJ45×32port	
シリアルポート 設定可能速度	2400、4800、9600、19200、38400、57600、115200(bps)	
概算質量	約 3.4kg	
外形寸法	426(W)×262(D)×44(H)mm	

（カ） UTM

業界共用パターン拠点では、WAN 回線を介するローカル５Ｇトラフィックを暗号化する機器として UTM を各拠点 1 台（計 4 台）構築しました。各 UTM は各拠点内のラックに設置しています。

表 3-3-6 UTM 仕様

項目	仕様	備考
ファイアウォール スループット	1518 バイト UDP パケット：10 Gbps 512 バイト UDP パケット：10 Gbps 64 バイト UDP パケット：6 Gbps	
ファイアウォール 同時セッション（TCP）	700,000	
ファイアウォールポリシー	5,000	
外形寸法	216（W）×38.5（H）× 160（D） mm	
重量	1.01kg	
消費電力（平均/電圧）	17.0 W / 18.5 W	

（キ） 拠点 UPF サーバ

複数企業共用パターン拠点、業界共用パターン拠点では、センタ拠点を介せずにローカル５Ｇのトラフィックを転送するために、UPF サーバを各拠点 1 台（計 5 台）構築しました。拠点 UPF サーバは各拠点内のラックに設置しています。

表 3-3-7 UPF サーバ仕様

項目	仕様	備考
電源	100-120/200-240VAC	
消費電力	800W パワーサプライ(80PLUS Platinum モデル)×2、最大 2 基、リダンダント構成	
CPU	Intel® Xeon® Silver(8 コア 16 スレッド)×2	
メモリ容量	32GB	
DISK 容量	800GB	
概算質量	16.27kg（最大）	
外形寸法	4346×7498×429 mm、1U ラックマウント型	

（ク） PTP 対応 L2SW

PTP 対応 L2 スイッチは GMC(Grand Master Clock)と接続し、GPS アンテナから得た時刻等を接続される機器に同期させるためのスイッチです。L3SW、CDU、RU と接続しています。PTP 対応 L2 スイッチはセンタ拠点を除く各拠点に設置するラックに収容しました。

表 3-3-8 PTP 対応 L2SW 仕様

項目	仕様	備考
LAN ポート数	4 (10,100,1000BASE-T) 8(SFP/SFP+) (1000BASE-X/10GBASE-R)	
SFP＋スロット数	8	
スイッチング容量	168Gbps	
外形寸法	210 (W) ×43.8 (H) ×220 (D) (mm)	
重量	2.3kg 以下	
消費電力	33W 以下	

（ケ） CDU-A

CDU-A サーバは、5G システムの無線アクセスネットワークにおける集約ノード機能を担う CU(Central Unit)と分散ノード機能を担う DU(Distributed Unit)を実装する仮想サーバです。CDU-A サーバは時刻同期対応スイッチした PTP 対応 L2SW に接続しました。CDU-A サーバはセンタ拠点・NTT 中央研修センタ・オペレータ拠点を除く各拠点に設置するラックに収容しています。

表 3-3-9 CDU-A 仕様

項目	仕様	備考
電源	100-120/200-240VAC	
消費電力	800W 以下	
CPU	Intel® Xeon® Gold (20 コア 40 スレッド)	
メモリ容量	256GB	
ストレージ容量	512GB	
概算質量	25kg 以下 ※装置本体のみの質量(アクセサリーを含まない)	
外形寸法	440(W) x 710(D) x 88(H) mm	

（コ） CDU-B

CDU-B サーバは、5G システムの無線アクセスネットワークにおける集約ノード機能を担う CU(Central Unit)と DU(Distributed Unit)を実装する仮想サーバです。CDU-B サーバは、時刻同期対応スイッチした PTP 対応 L2SW を接続します。本検証では NTT 中央研修センタに 1 台用意しました。

表 3-3-10 CDU-B 仕様

項目	仕様	備考
電源	100-120/200-240VAC	
消費電力	800W 以下	
CPU	Intel® Xeon® Gold (20 コア 40 スレッド)	
メモリ容量	256GB	
ストレージ容量	512GB	
概算質量	25kg 以下 ※装置本体のみの質量(アクセサリーを含まない)	
外形寸法	440(W) x 710(D) x 88(H) mm	

（サ） CDRU-C

CDRU-C サーバは、5G システムの無線アクセスネットワークにおける集約ノード機能を担う CU(Central Unit)と分散ノード機能を担う DU(Distributed Unit)と無線装置の RU(Radio Unit)を実装する仮想サーバです。本検証では NTT 中央研修センタに 1 台用意しました。

表 3-3-11 CDRU-C 仕様

項目	仕様	備考
対応周波数帯	4.7～4.8GHz/4.8～4.9GHz 2 つのパターンから選択	
最大出力	+23dBm(200mw)	
アンテナ利得	指向性アンテナ　12dBi	
最大チャネル帯域幅	100MHz	
MIMO レイヤー数 DL/UL	DL：2×2 MIMO UL：2×2 MIMO	
NW インターフェース	Ethernet 1Gbps ×1（保守用） Ethernet 1Gbps ×1(データネットワーク接続点)	
時刻同期	GPS	
対応電源	AC100V	
概算質量	20kg 程度	
外形寸法	(W)285mm ×(H) 513mm ×(D) 471mm	
動作温度	0℃～40℃	

（シ） CDRU-C 用暗箱

CDRU-C 用暗箱は、CDRU-C が技術適合証明を未取得のため使用しました。

表 3-3-12 CDRU-C 用暗箱

項目	仕様	備考
シールド周波数範囲	・Sub6 帯（600MHz～6GHz） ・ミリ波帯（28GHz 帯）	
シールド特性値	60dB 以上（Sub6 帯、ミリ波帯）	
電波吸収特性	40dB 以上（25～40GHz） t=50mm	
外形寸法	1274(W) x 759(D) x 1475(H) mm	
排熱用 FAN（天井）	4 個（消費電力　AC100V/36W）	
質量	約 160kg	

（ス） RU-A

RU-A は A 社製のローカル５Ｇの RU で、センタ拠点を除く各拠点に 2 台ずつ合計 10 台設置しています。

表 3-3-13 RU-A

項目	仕様	備考
電源	PoE++給電	
消費電力	60W 以下	
概算質量	3.5kg 以下(装置本体のみ)	
外形寸法	218(W) x 218(D) x 64(H) mm	
動作温度	-5～40℃(屋内用)	
対応周波数	5G NR 4.8～4.9GHz 100MHz 幅	
最大送信電力	23dBm(200mW)	
本体同梱品	・壁面取付金具 x 1 ・PoE インジェクター x 1 ・AC 電源コード（AC100V 対応） × 1	

(セ) RU-B

RU-B は B 社製のローカル５ G の RU で、本検証では NTT 中央研修センタに 1 台設置しました。

表 3-3-14 RU-B

項目	仕様	備考
電源	PoE++給電	
消費電力	60W 以下	
概算質量	3.5kg 以下(装置本体のみ)	
外形寸法	218(W) x 218(D) x 64(H) mm	
動作温度	-5～40℃(屋内用)	
対応周波数	5G NR 4.8～4.9GHz 100MHz 幅	
最大送信電力	23dBm(200mW)	
本体同梱品	・壁面取付金具 x 1 ・PoE インジェクター x 1 ・AC 電源コード (AC100V 対応) ×１	

（ソ） UE-A

UE-A は A 社製のローカル５Ｇ端末（UE）で、本検証ではセンタ拠点を除く各拠点に 2 台ずつ合計 10 台用意しました。

表 3-3-15 UE-A 仕様

項目	仕様	備考
電源	AC 給電	
消費電力	最大 40W 以下	
概算質量	1.6kg 以下	
外形寸法	105(W) x 154(D) x 233(H) mm	
動作温度	0℃～+40℃	
対応周波数	5G NR 4.8～4.9GHz 100MHz 幅	
最大空中線電力	23dBm(200mW)	
本体同梱品	AC 電源アダプター x 1	

（タ） UE-D

UE-D は D 社製のローカル５Ｇ端末（UE）で、本検証では NTT 中央研修センタに 8 台用意しました。

表 3-3-16 UE-D 仕様

項目	仕様	備考
バッテリー	5300mAh(typ)	
バンド	Sub6 n79,mmWave n257,4G B38,B41	
概算質量	228g	
外形寸法	119(W) x 72(D) x 23.5(H) mm	
ディスプレイ	2.4’ タッチパネル付き	
無線	Dual band WiFi(16 端末接続) MIMO 802.11 a/b/g/n/ac/ax	
I/O	USB3.1 Gen2, Type C, Nano-SIM, RJ45	

（チ） UE-E

UE-E は E 社製のローカル５Ｇ端末（UE）で、本検証では NTT 中央研修センタに 1 台用意しました。

表 3-3-17 UE-E 仕様

項目	仕様	備考
電池容量	4070mAh	
消費電力	最大 40W 以下	
概算質量	約 171g	
外形寸法	164.1(W) x 75.7(D) x 7.7(H) mm	
温湿度条件	5℃～35℃ / 45%～85%RH	
対応周波数	NR （ Sub6 local5G:n79, mmWave local5G:n257）	
外部 I/O	USB TypeC （USB 3.1 Gen2, Displayport サポート）	
コネクティビティ	WLAN （802.11a,b,g,n,ac,ax 2x2MIMO） / Bluetoth 5.1	
ディスプレイ	6.7 インチ（3120 x 1440） フレキシブル有機 EL	
CPU/モデム	SM8250+SDX55M	
OS	Android 10	
カメラ	フロント：32M, リア：48M+16M（広角）+8M（光学 3 倍ズーム）	

（ツ） UE-F

UE-F は F 社製のローカル５Ｇ端末（UE）で、本検証では NTT 中央研修センタに 1 台用意しました。

表 3-3-18 UE-F 仕様

項目	仕様	備考
電池/充電端子	リチウムイオン電池(6000mAh)/USB Type-C(PD3.0)	
位置測位	GPS/GLONASS/BeiDou/Galileo/みちびき/A-GPS	
概算質量	約 326g	
外形寸法	165(W) x 27(D) x 78(H) mm	
ディスプレイ	約 2.6 インチ	
CPU	Qualcomm® Snapdragon™ 865 5G Mobile Platform, Snapdragon™ X55 5G Modem-RF System	
メモリ	RAM：8GB / ROM：128GB	
通信方式	5G NR(Sub6/mmW)、Local5G(Sub6/mmW)、4G LTE™(マルチバンド)	
ネットワークタイプ	NSA/SA ※SA はローカル５Ｇでのみ使用可能です。	

(テ)　GMC(Grand Master Clock)

GMC は GPS アンテナから受信した時刻情報を元に高精度な時刻同期を RU(5G システム無線基地局)に対して行います。センタ拠点を除く各拠点に 1 台ずつ合計 5 台設置しました。

表 3-3-19　GMC 仕様

項目	仕様	備考
定格電圧	AC100V～AC240V±10% (50/60Hz)	
定格電流	0.48A	
消費電力	39W	
発熱量	141.8kJ/h	
設置方式	ラックマウント (取付金具付属)	
外形寸法	430(W) x 500(D) x 44(H) mm (突起部を除く)	
質量	約 10kg	

（ト） ウェアラブルカメラ

ウェアラブルカメラには、R 社の機器を使用しました。

表 3-3-20　ウェアラブルカメラ　仕様

項目	仕様	備考
OS	Windows、Android	
イメージセンサ	1/2.3 型 CMOS イメージセンタ	
総画素数	約 1230 万画素	
レンズ	185 度広角レンズ	
マイク	モノラル、無指向性	
動画フォーマット	Motion JPEG	
音声フォーマット	PCM(mono)	
解像度/フレームレート	Full HD,HD,VGA/30p,10p,5p	
映像出力	UVC1.1 準拠	
音声出力	UAC1.0 準拠	
外部出力端子	USB2.0 TypeA ケーブル直出し(1.5m)	
電源電圧	DC5V±5%(USB より給電)	
消費電力	最大 2.5W	
外形寸法	37×69×92(mm)	
重量	約 140g	
堅牢性	防水・防塵(IP65)	

（ナ） 360 度カメラ

360 度カメラには、S 社の機器を使用しました。

表 3-3-21　360 度カメラ　仕様

項目	仕様	備考
静止画性能	6720×3360 ピクセル	
動画性能	・4K　3840×1920 ピクセル/29.97fps/56Mbps ・2K　1920×960 ピクセル/29.97fps/16Mbps ・最大連続記録時間　25 分	
ライブストリーミング性能	・4K　3840×1920 ピクセル/29.97fps ・2K　1920×960 ピクセル/29.97fps	
外形寸法	48×132.5×29.7（mm）	
重量	約 182g	

（ニ） ウェアラブルカメラ接続用 PC

ウェアラブルカメラを接続する PC には、T 社の PC を仕様しました。

表 3-3-22　ウェアラブルカメラ接続用 PC

項目	仕様	備考
CPU	クアッドコア第 11 世代　Intel Core i3-1115G4 プロセッサ	
MEM	8 GB または 16 GB LPDDR4x	
グラフィックス	Intel UHD グラフィックス	

（ヌ） 360 度カメラ接続用 PC

360 度カメラを接続する PC には、T 社の PC を使用しました。

表 3-3-23　360 度カメラ接続用 PC 仕様

項目	仕様	備考
CPU	クアッドコア第 10 世代　Intel Corei7-1065G7 プロセッサ	
MEM	16GB または 32GB 3733Mhz LPDDR4x	
グラフィックス	6GB　GDDR6 グラフィックメモリ付き　NVIDIA GeForce GTX 1660, Max-Q Design	

（ネ） ネットワークカメラ

ネットワークカメラには、U 社の機器を使用しました。

表 3-3-24　ネットワークカメラ　仕様

項目	仕様	備考
ビデオ圧縮	H.265、H.264 ・配信モード 固定ビットレート、可変ビットレート、フレームレート指定、 ベストエフォート配信 ・画質選択 3 段階（可変ビットレート選択時は 10 段階） ・配信方式 ユニキャスト、マルチキャスト	
解像度	3840×2160、2560×1440、1920×1080、1280×720、640×360、320×180	
フレームレート	25/30 フレーム/秒	
対応プロトコル	・IPv4 TCP／IP、UDP／IP、HTTP、HTTPS、RTSP、RTP、 RTP／RTCP、ICMP、ARP	
寸法	幅×高さ×奥行き：130 ×130×337（mm）	
重量	約 1.7kg	
電源	DC12V、PoE（IEEE802.3af 準拠）	
消費電力	DC12 V ： 930 mA／約 11.2 W、 PoE DC 48 V ： 240 mA／約 11.5 W（クラス 0 機器）	

（ノ） カメラ GW

カメラ GW には、V 社の製品を使用しました。

表 3-3-25　カメラ GW　仕様

項目	仕様	備考
電源	・定格入力電圧 AC100-240V ・入力電圧範囲 AC90-264V	
消費電力	最大 14W	
WAN ポート	・10/100/1000BASE-T（RJ-45 コネクター）×1 オートネゴシエーション 10M/100M Full/Half 固定設定、1000M Full 固定設定、 MDI/MDI-X 自動認識、MDI/MDI-X 固定設定 ・バイパスポート（RJ-45 コネクター）×1	
LAN ポート	・10/100/1000BASE-T（RJ-45 コネクター）×4 オートネゴシエーション 10M/100M Full/Half 固定設定、1000M Full 固定設定、 MDI/MDI-X 自動認識、MDI/MDI-X 固定設定	
その他インターフェース	・コンソール：RS-232（RJ-45 コネクター）×1 ・USB：USB2.0、タイプ A（メス）コネクター、最大給電電流 700mA×1	
概算質量	1.5kg	
外形寸法	210（W）×220（D）×42.5（H）mm（突起部含まず）	

（ハ） GPU サーバ

GPU サーバには、J 社の GPU サーバを使用しています。

表 3-3-26　GPU サーバ　仕様

項目	仕様	備考
CPU	16 コア Intel Xeon Gold	
GPU	NVIDIA Tesla T4	
RAM	60GB	
SSD	160GB	
OS	CentOS 7.5	

（ヒ） AI 顔認証ソフトウェア

AI 顔認証ソフトウェアには業界最高水準の認識精度と認識スピードを誇る AI 顔認証ソフトウェアを採用しました。ディープラーニングにより 1,000 万を超える顔データを学習しており顔認証のほかに、映像から個人を特定せずに属性の推定を行うことも可能です。

3.4　システム機能・性能・要件

構築したネットワーク・システムは、本検証の実施及び検証目標の達成に必要となる以下の機能、性能および要件を満たしています。

(1) ローカル５Ｇネットワーク

表 3-4-1-1　ローカル５Ｇネットワーク機能・性能・要件

システム機能	・ Sub6 帯のスタンドアローン（SA）構成に対応した各コンポ―ネント機能（コアネットワーク装置、基地局（CU＋DU＋RU）、端末（UE））を有する
性能	・ 同期パターンでのスループットが理論値 DL:約 283Mbps、UL：約 43Mbps ・ 準同期 TDD 方式でのスループット理論値 DL:約 121Mbps、UL：約 108Mbps
要件	・ 複数拠点の基地局も同一コアにて収容することが可能であること ・ 複数メーカのコア、基地局、UE を用いた相互接続検証が可能であること ・ サプライチェーンリスクへの対応の機器であること

(2) 拠点間ネットワーク

(ア)複数企業共用パターン

表 3-4-2-1　複数企業共用パターン拠点間ネットワーク機能・性能・要件

システム機能	・ 各システムにおけるデータ通信、およびコア～CDU 間のデータ通信を可能とする
性能	・ 拠点間 VPN 回線　上り下り最大 1Gbps ・ 拠点内有線 LAN 接続　1000BASE-T 以上
要件	・ 中小企業での実行的な共用範囲として接続拠点（コアと通信する基地局を設置する拠点）で都道府県内もしくは隣接都道府県で複数拠点が接続できること

(イ)業界共用パターン

表 3-4-2-2　業界共用パターン拠点間ネットワーク機能・性能・要件

システム機能	・ 各システムにおけるデータ通信、およびコア～CDU 間のデータ通信を可能とする
性能	・ 拠点間 VPN 回線　上り下り最大 1Gbps ・ 拠点内有線 LAN 接続　1000BASE-T 以上
要件	・ 日本における 8 地方区分（北海道、東北、関東、中部、近畿、中国、四国、九州）に基づいた、隣接する地方区分及び隣接しない地方区分で 3 拠点以上（近・中・遠距離）接続できること ・ 団体が業界共用 NW に接続する接続点（POI）間をつなぐ、バックボーン NW に接続可能であること

(3) 遠隔支援システム

表 3-4-3-1　遠隔支援システム機能・性能・要件

システム機能	・　ウェアラブルカメラ（フル HD）と 360 度カメラ（フル HD）を装着した４名の見習い社員が離れた場所に位置する熟練者から指示、指導を受けつつ作業を実施可能
性能	(ウェアラブルカメラ) ・　配信解像度　フル HD(1920×1080) (360 度カメラ) ・　配信解像度　フル HD(1920×1080)
要件	・　外部ストレージに映像の記録、保存が可能であること ・　低遅延での配信が可能であること ・　ウェアラブルカメラ着用者へ図面の共有が可能であること ・　本部から現場のウェアラブルカメラ着用者へ指示が出せること

(4) AI 顔認証システム

表 3-4-4-1　AI 顔認証システム機能・性能・要件

システム機能	・　顔検知（人物の検知・トラッキング） ・　顔認識（人物の認識・特定） ・　属性検知（性別推定・年齢推定） ・　感情推定、笑顔の検知
性能	(ネットワークカメラ) ・　映像解像度：4K(3840×2160) ・　ビデオ圧縮：H.264 および H.265 に対応 (GPU サーバ) ・　CPU：16 コア Intel Xeon Gold ・　GPU：NVIDIA Tesla T4 ・　RAM：60GB ・　SSD：160GB ・　OS：CentOS 7.5
要件	・　複数台の 4K カメラ映像(15fps／15Mbps)の伝送が可能であること ・　低遅延で AI 解析（顔検知、顔認識、属性推定）が可能であること ・　映像データの記録、保存の有無について設定が可能であること ・　解析結果の閲覧が可能であること

4.　相互接続検証

4.1　検証概要

本検証では、異なるメーカ間におけるローカル５Ｇのコア・基地局・端末の相互接続について現状分析を行い、相互接続を実現するための仕組みを整理します。

4.2　検証環境

本検証で使用する構成は以下の「図 4-2-1 構成イメージ」のとおりで、相互接続の組合せは「表 4-2-1　異メーカの組合せパターン」のとおり 8 パターンについて検証します。コアは A 社製の装置を使用し、異なるメーカの基地局及び端末の接続を検証します。

また、本検証は相互接続検証拠点である NTT 中央研修センタにて行います。

なお、基地局と端末間は電界強度による検証への影響を避けるため、遮蔽物の無い見通し環境で検証を行います。

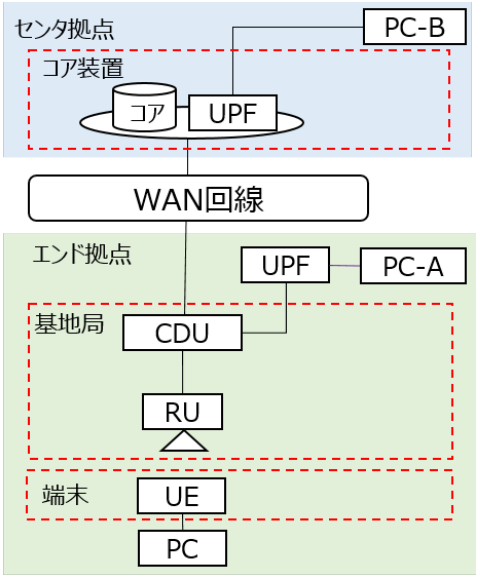


図 4-2-1　構成イメージ

表 4-2-1　異メーカの組合せパターン

組合せパターン	コア装置	基地局	端末
相コ基端-1	5GC-A	CDU-B	UE-A
相コ基端-2	5GC-A	CDU-B	UE-D
相コ基端-3	5GC-A	CDU-B	UE-E
相コ基端-4	5GC-A	CDU-B	UE-F
相コ基端-5	5GC-A	CDRU-C	UE-A
相コ基端-6	5GC-A	CDRU-C	UE-D
相コ基端-7	5GC-A	CDRU-C	UE-E
相コ基端-8	5GC-A	CDRU-C	UE-F

5GC-A：A 社製 5GC
CDU-B：B 社製 CDU
CDRU-C：C 社製 CDU,RU
UE-A：A 社製 UE
UE-D：D 社製 UE
UE-E：E 社製 UE
UE-F：F 社製 UE

4.3 検証内容

(1) 検証目標

異なるメーカのコア装置・基地局・端末の接続については、コア装置内のログ及び「表 4-3-1-1　検証目標」に記載の検証目標を確認することで正常に接続できているか否かを判断します。

表 4-3-1-1　検証目標

項目	性能目標
電源 OFF/ON 操作時の正常性	基地局、端末のそれぞれの電源 OFF/ON 操作した際、異常なく復帰すること
機内モード ON/OFF 操作時の正常性	端末の機内モードの ON/OFF 操作した際、異常なく復帰すること
同期パターンの正常性	同期／準同期設定において接続性、システム性能（トラフィック）に異常が無いこと
長期安定化試験における正常性	無操作状態において接続性、システム性能（トラフィック）に異常が無いこと

(2) 評価・検証項目

（ア）異メーカ基地局との接続評価・検証方法

本検証での評価・検証項目は、以下の「表 4-3-2-1　評価・検証項目」のとおりです。

表 4-3-2-1　評価・検証項目

大項目	中項目	検証概要	検証項目
相互接続検証	基地局（異メーカー）との相互接続確認	電源 OFF/ON 動作時の挙動確認	基地局（CU／DU／RU）の電源をそれぞれ OFF/ON させ、再度起動した際、コア装置や端末と正常に接続できること
		電波 OFF/ON 動作時の挙動確認	停波後、発波させた際、コア装置や端末と正常に接続できること
		通信品質の確認	Ping による疎通試験、および iperf による伝送スループット試験を実施
		長期安定化試験	無操作状態とした環境においてエラーログの出力が無く、疎通試験上異常が無いこと

（イ）異メーカ端末との接続評価・検証方法

本検証での評価・検証項目は、以下の「表 4-3-2-2　評価・検証項目」のとおりです。

表 4-3-2-2　評価・検証項目

大項目	中項目	検証概要	検証項目
相互接続検証	端末（異メーカー）との相互接続確認	機内モードの ON/OFF の挙動確認	端末の機内モード ON/OFF させ、再度通常モードで起動した際、基地局やコア装置と正常に接続できること
		電源 OFF/ON 動作時の挙動確認	端末の電源を OFF/ON させ、再度起動した際、基地局やコア装置と正常に接続できること
		通信品質の確認	Ping による疎通試験、および iperf による伝送スループット試験を実施
		準同期の動作確認	準同期 TDD 方式において正常に接続できること
			トラフィック負荷を印加した際、理論値と比較し妥当なトラフィック値（DL／UL）が出力されること
		長期安定化試験	無操作状態とした環境においてエラーログの出力が無く、疎通試験上異常が無いこと

(3) 評価・検証方法

本検証で用いる測定ツールは、以下の「表 4-3-3-1　測定ツール」のとおりです。

表 4-3-3-1　測定ツール

項目	測定内容および具体的なツール
測定ツール	伝送スループット：iperf 等の測定ツール
	伝送疎通試験：ping 試験

（ア）異メーカ基地局との接続評価・検証方法

本検証の手順及び検証イメージは、以下の「表 4-3-3-2 検証手順」及び「図 4-3-3-1　検証イメージ」のとおりです。

表 4-3-3-2 検証手順

工程	実施内容	対応図表
相基-1	5GC-A（コア装置）と CDU-B（基地局）を接続	図 4-3-3-1
相基-2	メーカ独自に解釈しているパラメータや、接続のために調整しているパラメータの存在や調整状況などを分析	図 4-3-3-1
相基-3	表 4-3-2-1 の評価・検証項目を確認	図 4-3-3-1
相基-4	5GC-A と CDRU-C（基地局）を接続	図 4-3-3-1
相基-5	パラメータ等をコア装置に反映し、パラメータのチューニングを行いつつ正常に接続できるか検証	図 4-3-3-1
相基-6	表 4-3-2-1 の評価・検証項目を確認	図 4-3-3-1

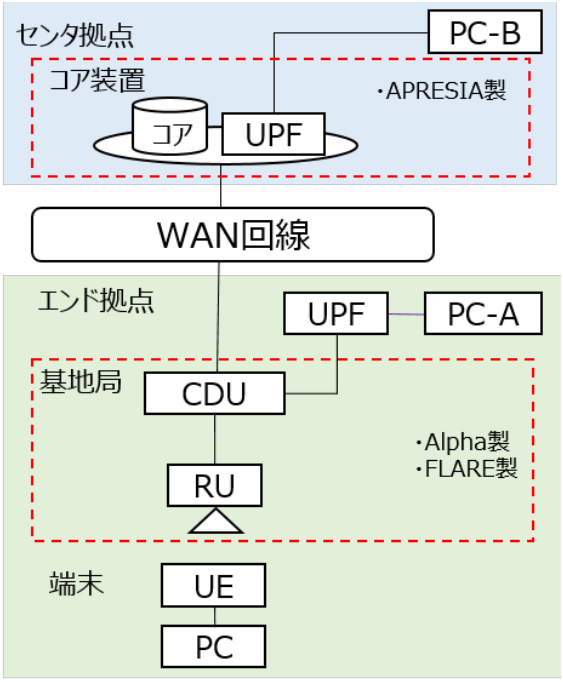


図 4-3-3-1　検証イメージ

（イ）異メーカ端末との接続評価・検証方法

本検証の手順及び検証イメージは、以下の「表 4-3-3-3 検証手順」及び「図 4-3-3-2　検証イメージ」のとおりです。

表 4-3-3-3 検証手順

工程	実施内容	対応図表
相端-1	5GC-A に CDU-B を接続（同期設定）	図 4-3-3-2
相端-2	UE-A を接続	図 4-3-3-2
相端-3	表 4-3-2-2 の評価・検証項目を確認	表 4-3-2-2
相端-4	UE-A を切り離し、UE-D を接続	図 4-3-3-2
相端-5	表 4-3-2-2 の評価・検証項目を確認	表 4-3-2-2
相端-6	UE-D を切り離し、UE-E を接続	図 4-3-3-2
相端-7	表 4-3-2-2 の評価・検証項目を確認	表 4-3-2-2
相端-8	UE-E を切り離し、UE-F を接続	図 4-3-3-2
相端-9	表 4-3-2-2 の評価・検証項目を確認	表 4-3-2-2
相端-10	準同期 TDD 方式に変更し、相端-2 から 9 を実施	―
相端-11	表 4-3-2-2 の評価・検証項目の準同期を確認	―
相端-12	5GC-A に CDRU-C を接続（同期設定）	図 4-3-3-2
相端-13	UE-A を接続	図 4-3-3-2
相端-14	表 4-3-2-2 の評価・検証項目を確認	表 4-3-2-2
相端-15	UE-A を切り離し、UE-D を接続	図 4-3-3-2

相端-16	表 4-3-2-2 の評価・検証項目を確認	表 4-3-2-2
相端-17	UE-D を切り離し、UE-E を接続	図 4-3-3-2
相端-18	表 4-3-2-2 の評価・検証項目を確認	表 4-3-2-2
相端-19	UE-E を切り離し、UE-F を接続	図 4-3-3-2
相端-20	表 4-3-2-2 の評価・検証項目を確認	表 4-3-2-2
相端-21	準同期 TDD 方式に変更し、相端-13 から 20 を実施	―
相端-22	表 4-3-2-2 の評価・検証項目の準同期を確認	―

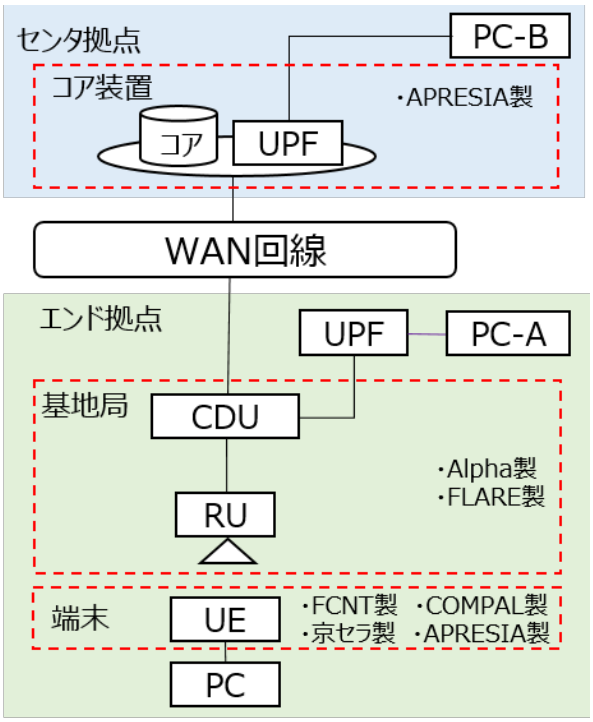


図 4-3-3-2　検証イメージ

4.4 検証結果及び評価・分析

(1) 相互接続試験の検証結果

相互接続の実現に向けて、コア装置の製作者である A 社と弊社で事前に準備及び検証を実施し、標準規格の整合及び不定なパラメータや処理に関して相互接続に適応できるよう措置を施しました。本内容に関しては、次章「4.5 ケーススタディ (2)相互接続に関連する項目、パラメータ等」に詳細を記載しています。

上記の措置を施したうえで実施した相互接続試験の検証結果は以下のとおりです。

（ア）異なるメーカ基地局との相互接続結果

コア装置「5GC-A」に対して 2 つの異なるメーカ基地局を接続する試験を実施しました。

－CDU-B　(B 社製 CDU)
－CDRU-C　(C 社製 CUDURU 一体型)

検証結果は以下の「表 4-4-1-1 異なるメーカ基地局との相互接続結果」のとおり、いずれの異なるメーカ基地局とも相互接続は問題ないことを確認しました。

表 4-4-1-1　異なるメーカ基地局との相互接続結果

組合せパターン	コア装置	基地局	接続可否
相コ基-1	5GC-A	CDU-B	○
相コ基-2	5GC-A	CDRU-C	○

（イ） 異なるメーカ端末との相互接続結果

基地局「CDU-B」及び「CDRU-C」に対して、それぞれ異なるメーカ端末を接続する試験を実施しました。

－UE-A　(A 社製 UE)
－UE-D　(D 社製 UE)
－UE-E　(E 社製 UE)
－UE-F　(F 社製 UE)

検証結果は以下の「表 4-4-1-2　異なるメーカ端末との相互接続結果」のとおりです。

コア「5GC-A」、基地局「CDRU-C」、端末「UE-A」の 1 の組合せのみ接続不可という結果となり、その他の 7 つの組合せでは問題なく相互接続可能であることを確認しました。しかし、「5GC-A」、基地局「CDRU-C」、端末「UE-F」に関しては、接続良好であることを確認し、性能及び品質についても問題ないことを確認していましたが、最後に実施を予定して

いた検証テーマである長期安定化試験の準備をしていたところ、接続不可という事象が生じました。

本検証において、接続不可となった上記 2 つの組合せに関しては、原因究明及び解決方策を検討し、各種視点でのアプローチを行いましたが、事象の解決には至りませんでした。本件に関しては、次項の（２）及び（３）にて詳細を記載します。なお、接続可能時に計測した性能及び品質のデータに関しては、他の製品と同様に評価しコメントします。

表 4-4-1-2　異なるメーカ端末との相互接続結果

組合せパターン	コア装置	基地局	端末	接続可否
相コ基端-1	5GC-A	CDU-B	UE-A	○
相コ基端-2	5GC-A	CDU-B	UE-D	○
相コ基端-3	5GC-A	CDU-B	UE-E	○
相コ基端-4	5GC-A	CDU-B	UE-F	○
相コ基端-5	5GC-A	CDRU-C	UE-A	×
相コ基端-6	5GC-A	CDRU-C	UE-D	○
相コ基端-7	5GC-A	CDRU-C	UE-E	○
相コ基端-8	5GC-A	CDRU-C	UE-F	○（※）

※「5GC-A」、基地局「CDRU-C」、端末「UE-F」は当初は接続良好であるも、その後に接続不可の事象が発生し解決に至っていない

（ウ）　組合せパターン毎の性能、品質

組合せパターンにおける DL/UL 毎の性能及び品質を検証しました。伝送スループットは「表 4-4-1-3　組合せパターンごとの性能 伝送スループット」にまとめ、基地局ごとに同期・準同期それぞれ図で示します。また、遅延時間は「表 4-4-1-4　組合せパターンごとの性能 遅延時間」、その他の品質については「表 4-4-1-5　組合せパターンごとの品質」にて結果を示します。

表 4-4-1-3　組合せパターンごとの性能 伝送スループット

組合せ	同期			準同期 TDD		
パターン	DL	UL	Total	DL	UL	Total
相コ基端-1	300Mbps	28Mbps	328Mbps	170Mbps	60Mbps	230Mbps
相コ基端-2	200Mbps	28Mbps	228Mbps	100Mbps	58Mbps	158Mbps
相コ基端-3	150Mbps	30Mbps	180Mbps	150Mbps	60Mbps	210Mbps
相コ基端-4	250Mbps	30Mbps	280Mbps	115Mbps	60Mbps	175Mbps
相コ基端-5	接続不可	接続不可	-	接続不可	接続不可	-
相コ基端-6	300Mbps	65Mbps	365Mbps	200Mbps	150Mbps	350Mbps
相コ基端-7	180Mbps	77Mbps	257Mbps	180Mbps	135Mbps	315Mbps
相コ基端-8	250Mbps	30Mbps	280Mbps	280Mbps	80Mbps	360Mbps

B 社製（CDU-B）は DL 及び UL の MCS 値を「9」に設定し測定

C 社製（CDRU-C）は DMCS に設定し測定

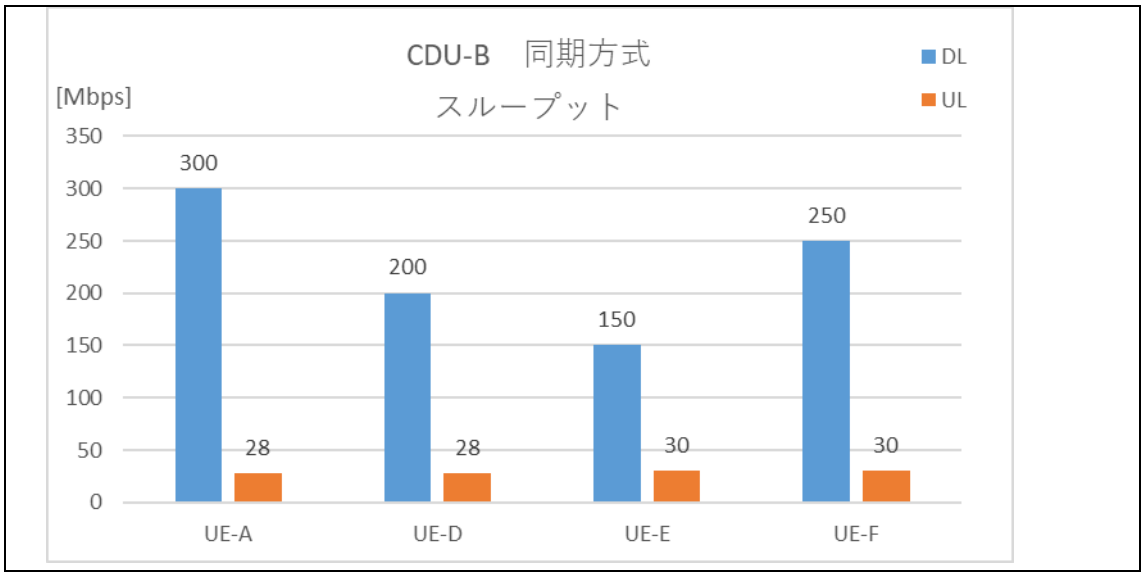


図 4-4-1-1 CDU-B　同期方式スループット

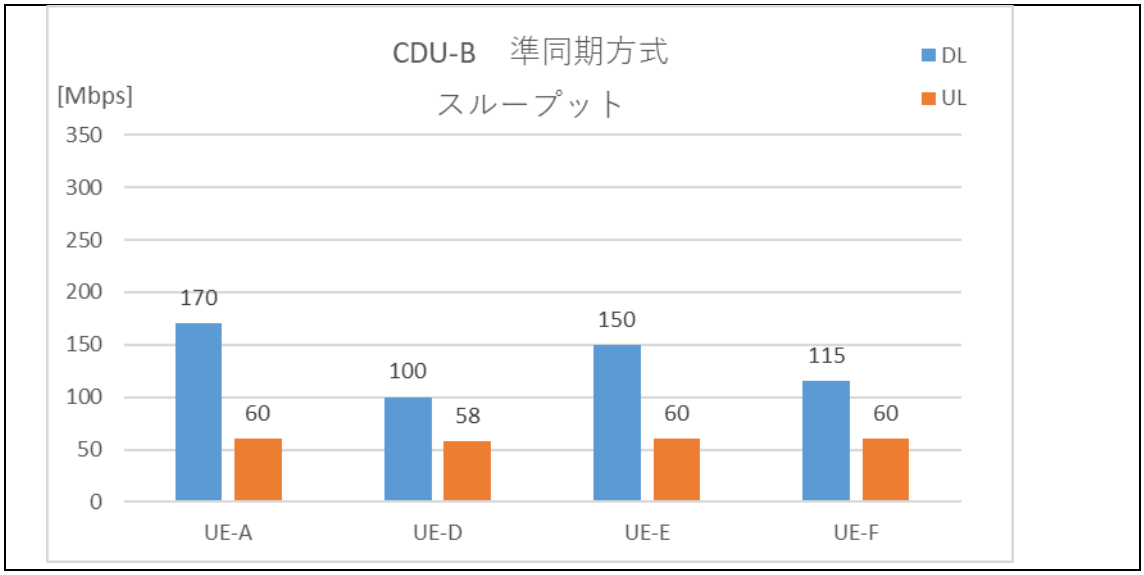


図 4-4-1-2 CDU-B　準同期方式スループット

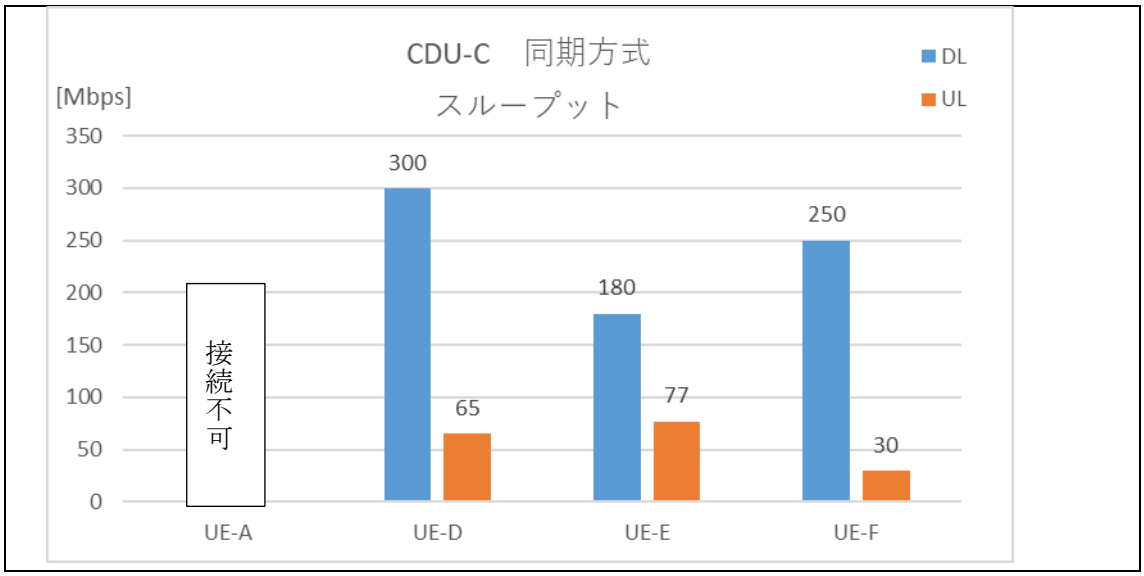


図 4-4-1-3 CDU-C　同期方式スループット

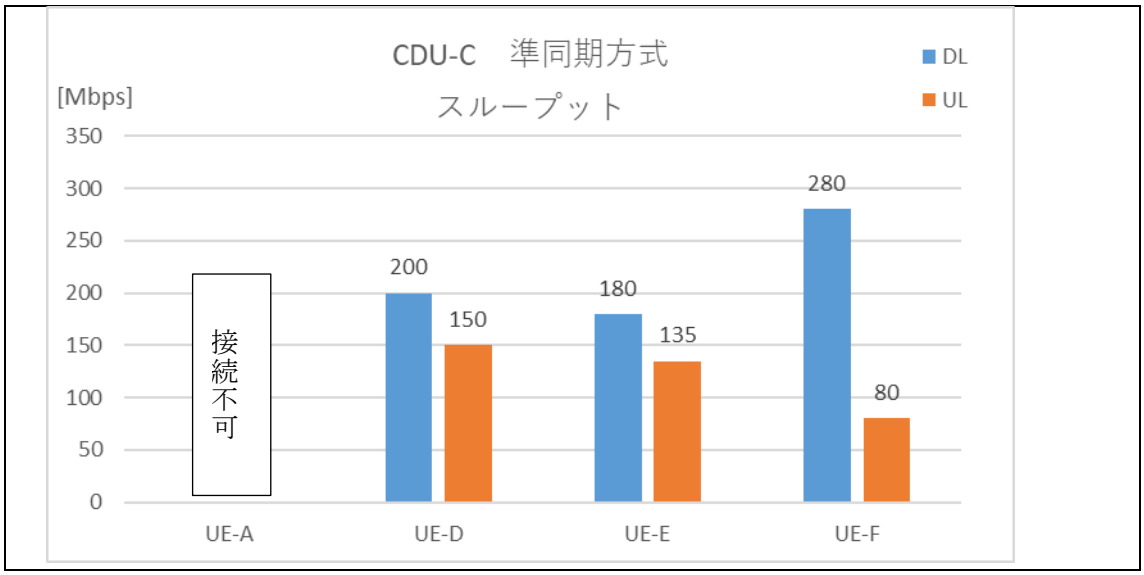


図 4-4-1-4 CDU-C　準同期方式スループット

表 4-4-1-4　組合せパターンごとの性能 遅延時間

組合せパターン	遅延時間	
	同期［msec］	準同期［msec］
相コ基端-1	35	36
相コ基端-2	40	36
相コ基端-3	39	40
相コ基端-4	39	40
相コ基端-5	-	-
相コ基端-6	32	28
相コ基端-7	30	29
相コ基端-8	27	30

表 4-4-1-5　組合せパターンごとの品質

組合せパターン	電源の OFF/ON 時の挙動		機内モード ON/OFF 時の挙動	長期安定化試験の結果
	基地局	端末		
相コ基端-1	問題なし	問題なし	問題なし	問題なし
相コ基端-2		問題なし	問題なし	問題なし
相コ基端-3		問題なし	問題なし	問題なし
相コ基端-4		問題なし	問題なし	問題なし
相コ基端-5	問題なし	―	―	―
相コ基端-6		問題なし	問題なし	問題なし
相コ基端-7		問題なし	問題なし	問題なし
相コ基端-8		問題なし	問題なし	接続不可の事象が発生したため未実施

伝送スループットに関して、同期 TDD 方式については、どの組合せにおいても「Total スループット約 300Mbps」の結果が得られています。今回の組合せの中で、それぞれの基地局に対して最も Total スループットが良かったのは以下となります。

・同期 TDD 方式において Total スループットが最良結果となった組合せ
　CDU-B ：UE-A　　Total スループット：328Mbps
　CDRU-C：UE-D　　Total スループット：365Mbps

※UE-E（相コ基端-3,7）はスマートデバイスとなりますが本検証環境では、USB テザリング機能を用いて測定しているため、スマートデバイス上にインストールしたアプリケーション等を動作させる場合は、本結果と異なる可能性があります

いずれの基地局の組合せにおいても、同期 TDD 方式における通信性能は良好であると評価できます。一方で、準同期 TDD 方式については、「Total スループット 150Mbps～350Mbps

程度」であり、端末による差が大きい結果となりました。Total スループットが最良となる組合せは以下となります。

・準同期 TDD 方式において Total スループットが最良結果となった組合せ
CDU-B ：UE-A　　Total スループット：230Mbps
CDRU-C：UE-F　　Total スループット：360Mbps

※UE-E（相コ基端-3,7）はスマートデバイスとなりますが本検証環境では、USB テザリング機能を用いて測定しているため、スマートデバイス上にインストールしたアプリケーション等を動作させる場合は、本結果と異なる可能性があります

同期 TDD 方式と比べると、Total スループットが低下する組合せが多い結果となりましたが、準同期 TDD 方式で期待される UL スループットは、全ての組合せにおいて 2 倍以上に向上する結果を得られました。この結果をふまえ、相互接続組合せにおいても問題なく準同期方式を適用することが可能であると考えられます。

遅延時間に関しては、組合せによって 27msec～40msec のバラつきが発生していることを確認しました。全体的に CDRU-C より CDU-B の遅延時間が多い結果となっているため、gNB での処理速度に依存してこのような結果がでていると推察されます。

基地局 CDU-B での遅延時間平均 ： 同期 38.3ms 、 準同期 38ms
基地局 CDRU-C での遅延時間平均： 同期 29.6ms 、 準同期 29ms

電源 OFF/ON 時の挙動に関しては、全組合せにおいて電源 ON 時に自動的に接続が開始されることを確認しました。機内モード時の挙動は、全端末が問題なく起動し利用できることを確認しました。長期安定化試験は 48 時間連続状態での検証を実施しました。結果、CDRU-C と UE-F の組合せにおいて通信断及びデタッチが発生し、その他の組合せにおいてはエラーログの発生はなく、デタッチの事象も生じず連続通信が安定して実行される結果を得ました。

また、検証結果に対する組合せパターン毎の考察は以下の「表 4-4-1-6 考察」のとおりです。

表 4-4-1-6 考察

組合せパターン	考察
相コ基端-1	・問題なく相互接続し利用が可能 ・CDRU-C との接続不可であるが CDU-B とは接続可能
相コ基端-2	・問題なく相互接続し利用が可能 ・UE-D として CDRU-C と接続した性能と比較し CDU-B は性能が下がる
相コ基端-3	・問題なく相互接続し利用が可能 ・同期 DL スループットが低いが、準同期でも同等の DL スループットを確認
相コ基端-4	・問題なく相互接続し利用が可能 ・同期 DL スループットは良好だが、準同期 DL スループットは大きく低下
相コ基端-5	接続不可
相コ基端-6	・問題なく相互接続し利用が可能 ・DL/UL ともに全パターンで最良のスループットを確認
相コ基端-7	・問題なく相互接続し利用が可能 ・UL 2 レイヤーのため UL スループットが良好
相コ基端-8	・問題なく相互接続し利用が可能 ・準同期 DL スループットが良好 ・接続不可の事象が発生し、改善できず （接続不可のため長期安定試験を実行できなかった）

(2) 相互接続の実現に向けた要因分析

D 社、E 社、F 社の端末が認証成功したことに対して、A 社の端末のみが C 社 CDU を経由した接続が不可となりました。また、F 社の端末は当初問題なく接続され通信を行えていましたが、検証の途中から接続不可が発生しました。

A 社及び F 社の端末に共通していることとして、CDU(UE)から送付された特定のメッセージ、 “PDU session establishment reqeust”に対して、本来 5GC が応答すべきメッセージ、”PDU session establishment accept”を返していないことが観測されており、これらが接続不可となる要因であると考察されます。

対象機器のパラメータ等を確認しましたが、その他の要因と思わしき設定の差異（接続 OK 端末と NG 端末の差異）は見られませんでした。
その他に、環境要件やバグ等の影響を検証するために以下の対応を実施しましたが、原因究明及び解決には至りませんでした。

・CDU-5GC 区間の広域回線の種別を変更
ベストエフォート型「SDN」とギャランティ型「ビジネスイーサワイド」の 2 つの種別を切り替えてそれぞれ相互接続を試みたが、状況に変化はみられず。

・SecGW の設定変更、パケットドロップのモニタ
本実証で実装しているセキュリティ装置「SecGW」において、CDU-5GC 区間の各種設定を全通り試してみたが、状況は変わらず接続不可であった。
また、接続不可が生じた際のパケットドロップをモニタしたが、特にパケットドロップは発生していなかった。

・UPF の変更
エンド拠点 UPF の構成とし、センタ拠点 UPF は機能をオフの状態にて接続確認するも、改善は見られなかった。

・MTU（Maximum Transmission Unit）サイズの変更
各システムにおける MTU 値を変更し、複数の MTU サイズでの接続を試みるも改善されず。

・電波チューニング等
端末及び基地局の無線区間に関して、物理的距離を変えて受信電力の強弱それぞれの状態で検証、また TDD 方式を同期・準同期のそれぞれのパターンで実施するが改善は見られなかった。

・各システムリセット
以下のシステムに関して、初期化及びリセット等を実施するも改善は見られなかった。

-5GC との接続に関連するファンクション（AUSF 等やデータベース等）
-UPF
-CDU
-RU 及び UE

(3) 相互接続の実現方策の検討

5GC 側から応答不能となるまでのメッセージ上で、端末の SIM 情報は正常に認証されていました。その後、PDU session の認証リクエストに対して 5GC が応答不能となっています。

特定メッセージの応答不能の原因究明として、応答不能となるまでの認証メッセージ群の差分検証、UE-5GC 間において特定条件でのパケットドロップの可能性検証、5GC に内在する潜在不具合の確認を実施し、要因に対して解決方策を施すことで相互接続を実現できる見込みです。

上記の原因究明に関して、今後、各機器ベンダーの支援を受けて解決方策を施し改善する予定です。

また、本事象に関しては令和 4 年度の同調査研究においても原因究明と実現方策が明らかにされることを希望します。

(4) 相互接続検証の結果を踏まえたコアの共用における考察

全８つの組合せの相互接続検証を実施した結果、6 つの組合せで問題ないことが確認できました。3GPP に準拠した製品同士の場合は、異なるベンダー間の相互接続が実現可能であることが分かりました。しかし、今回の検証で接続不可となった 2 つの組合せのように、標準規格に準じていても接続不可となるケースも確認されたため、今回実証した構成以外の新たな組合せ等で継続して実証を行い、その他の要件や課題を洗い出し、相互接続を実現するための方策を導出することが有益であると考えられます。

本対応に関しては、令和 4 年度の調査研究においても重要なテーマと考えられ、受注企業コンソーシアムのみでは全容を解明することが困難と考えられるため、各システムベンダーやモバイルシステム業界企業、技術評価団体等の協力を得る専門委員会等を設け、有識者間での議論及び検証を行うことが必要であると考えます。

このような専門委員会に国内企業や団体がより多く参加することで、本調査研究の結果の共有と、相互接続実現に向けた製品改善等の動きも飛躍的に向上し、ひいては相互接続構成によるローカル５Ｇシステムの普及に繋がることが期待されます。

また、本実証では相互接続構成におけるコアの共用は実施しておりませんが、相互接続試験の単体の結果として、5GC の設定パラメータ等を変更せずに 2 つの異なる基地局（CDU-B、CDRU-C）へ接続可能であることから、コアを共用した環境下での相互接続も実現可能であることが推定されます。

4.5　ケーススタディ

本ケーススタディは、ローカル５Ｇシステムとして将来的に期待されているマルチベンダー構成に焦点をあて、コアネットワーク（5GC)、基地局（gNB)、端末（UE）の相互接続実現に向けた検証結果についてまとめたものとなります。

※本実証で選定した各製品は、3GPP 規格に準じた製品です
※令和 4 年現在、各ベンダーでは製品のバージョンアップ等が積極的に進められているため、今後は本検証と異なった結果になる可能性があります

(1) はじめに

昨今、モバイル通信システムの新世代として 5G NR が登場し、各無線機ベンダー、MNO 事業者等が率先して技術検証及び実用化が行われています。さらに、日本ではローカル５Ｇ制度が導入され、一般企業や自治体等が独自に 5G 網を構築することが可能になりました。一方で、ローカル５Ｇを導入促進、普及を目指すものの、既存の MNO 事業用途の 5G システムは大規模かつ高価な製品が多いことが課題として挙げられています。

5G システムは 3GPP による標準化が進められています。各システムやファンクションの標準化に伴い、マルチベンダー構成によるローカル５Ｇシステムの設計と利用が期待されています。ローカル５Ｇでは用途に応じて必要な機能や規模が異なるため、見合ったシステム構成に近づけるべくマルチベンダー構成とすることで、余分な性能等を削り、費用の低廉化につなげることが可能であると考えられます。

(2) 相互接続に関連する項目、パラメータ等

相互接続の実現に向けて、5GC、gNB、UE のパラメータを合わせる必要があります。現時点で必要と考えられる項目及び内容は以下の「表 4-5-2-1　5GC-gNB 間の相互接続に関係するパラメータ」のとおりです。

表 4-5-2-1　5GC-gNB 間の相互接続に関係するパラメータ

パラメータ	パラメータ概要	3GPP原文　記載内容（抜粋）
IPアドレス	N2,N3通信用IFのIPアドレス(5GC/CDU)	ー
PLMNID	ネットワークの事業者識別番号。 ローカル5G向けのPLMNは総務省様ガイドラインにて規定。	**TS23.003, 12.1 PLMN Identifier** A Public Land Mobile Network is uniquely identified by its PLMN identifier. PLMN-Id consists of Mobile Country Code (MCC) and Mobile Network Code (MNC)
TAI TAC	単体～複数のセルで構成されるセル単位。5GC側からUEの位置情報管理に用いられる。	**TS23.003, 19.4.2.3 Tracking Area Identity (TAI)** Tracking Area Code (TAC) is a fixed length code (of 2 octets) identifying a Tracking Area within a PLMN.
SST	ネットワークスライシングのサービスタイプ。サービスタイプ毎にNW特性を設定。	**TS23.501, 5.15.2.1 General, 5.15.2.2 Standardised SST values** A Slice/Service type (SST), which refers to the expected Network Slice behaviour in terms of features and services
SD	同タイプのネットワークスライシングを識別するための情報。	**TS23.501, 5.15.2.1 General** A Slice Differentiator (SD), which is optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.

表 4-5-2-2　　5GC-UE 間の相互接続に関係するパラメータ

パラメータ	パラメータ概要	3GPP原文　記載内容（抜粋）
OPc値	UE認証で使用するパラメータ。	**TS33.834 5.3 OP / Opc / TOP / TOPc** OP, OPc, TOP and TOPc are used to provide separation between the functionality of the algorithms when the same algorithm (e.g. MILENAGE or TUAK) is used by different operators. **TS35.205 8.3 Analysis of the role of OP and OPc** The 128-bit value OP is the Operator Variant Algorithm Configuration Field, which the Task Force was asked to include to provide separation between the functionality of the algorithms when used by　different operators.
K値	UE認証で使用するパラメータ。	**TS33.834 5.2 K / Ki** The K (sometimes referred to as the Ki) is the permanent key securely stored on the USIM on a UICC and in the Authentication Centre AuC / HSS.
PLMNID	ネットワークの事業者識別番号。 ローカル5G向けのPLMNは総務省様ガイドラインにて規定。	**TS23.003, 12.1 PLMN Identifier** A Public Land Mobile Network is uniquely identified by its PLMN identifier. PLMN-Id consists of Mobile Country Code (MCC) and Mobile Network Code (MNC)
TAI TAC	単体～複数のセルで構成されるセル単位。5GC側からUEの位置情報管理に用いられる。	**TS23.003, 19.4.2.3 Tracking Area Identity (TAI)** Tracking Area Code (TAC) is a fixed length code (of 2 octets) identifying a Tracking Area within a PLMN.
SST	ネットワークスライシングのサービスタイプ。サービスタイプ毎にNW特性を設定。	**TS23.501, 5.15.2.1 General, 5.15.2.2 Standardised SST values** A Slice/Service type (SST), which refers to the expected Network Slice behaviour in terms of features and services
SD	同タイプのネットワークスライシングを識別するための情報。	**TS23.501, 5.15.2.1 General** A Slice Differentiator (SD), which is optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.
APN	アクセスポイントの名称。	**TS23.003, 9.1 Structure of APN** The APN Network Identifier; this defines to which external network the GGSN/PGW is connected and optionally a requested service by the MS. This part of the APN is mandatory
AMF	コアネットワークノードとUEとの間の通信を処理する非アクセス層。 TS 33.102のAnnex HにAMFの各ビットの記述有り。	**TS 33.102, Annex H (normative): Usage of the AMF** The 16 bits in the AMF are numbered from "0" to "15" where bit "0" is the most significant bit and bit "15" is the least significant bit (see subclause 3.4) Bit "0" is called the "AMF separation bit". It is used for the purposes of EPS (Evolved Packet System) and is specified in -　TS 33.401 [28] for E-UTRAN access to EPS; -　TS 33.402 [29] for non-3GPP access to EPS; -　TS 33.501 [42] for 5G-RAN access to 5G System. Bits "1" to "7" are reserved for future standardization use. Bits "1" to "7" shall be set to 0 while not yet specified for a particular use. Bits "8" to "15" can be used for proprietary purposes. See Annex F for examples usages. Annex F (informative): Example uses of the proprietary part of the AMF F.1　Support multiple authentication algorithms and keys F.2　Changing sequence number verification parameters F.3　Setting threshold values to restrict the lifetime of cipher and integrity keys
CK,IK生成アルゴリズム	SIMカードの認証に用いられるハッシュ値の計算アルゴリズム。	**TS 35.205 [8]** MILENAGE = authentication and key generation algorithm as specified in 3GPP TS 35.205 [8]
秘匿・インテグリティアルゴリズム	NULLは暗号化、インテグリティなしを意味する。 SNOW3Gは3GPP特有のブロック暗号方式。 AESは一般的な共通鍵暗号方式。	**TS33.401 5.1.3.2 Algorithm Identifier Values** All algorithms specified in this subclause are algorithms with a 128-bit input key except Null ciphering algorithm. NOTE: Deviations from the above requirement have to be indicated explicitly in the algorithm identifier list below. Each EPS Encryption Algorithm (EEA) will be assigned a 4-bit identifier. Currently, the following values have been defined for NAS, RRC and UP ciphering: "00002" EEA0 Null ciphering algorithm "00012" 128-EEA1 SNOW 3G based algorithm "00102" 128-EEA2 AES based algorithm **TS33.401, 5.1.4.2 Algorithm Identifier Values** All algorithms specified in this subclause are algorithms with a 128-bit input key. NOTE: Deviations from the above requirement have to be indicated explicitly in the algorithm identifier list below. Each EPS Integrity Algorithm (EIA) will be assigned a 4-bit identifier. Currently, the following values have been defined: "00002" EIA0 Null Integrity Protection algorithm "00012" 128-EIA1 SNOW 3G "00102" 128-EIA2 AES

本実証で使用する各製品は、上記のパラメータを合わせて相互接続検証を行いました。しかし、下記 3 点に関しては、規定上は合わせる必要がないとされているものの、実際には相互接続不可となったため、改善措置を施し検証しました。

① Masked IMEISV の IE が存在していても支障がないはずだが接続不可

IE/Group Name	Presence	Range	IE type and reference	Semantics description	Criticality	Assigned Criticality
Message Type	M		9.3.1.1		YES	reject
AMF UE NGAP ID	M		9.3.3.1		YES	reject
RAN UE NGAP ID	M		9.3.3.2		YES	reject
Old AMF	O		AMF Name 9.3.3.21		YES	reject
UE Aggregate Maximum Bit Rate	C-ifPDUsessionResourceSetup		9.3.1.58		YES	reject
Core Network Assistance Information for RRC INACTIVE	O		9.3.1.15		YES	ignore
GUAMI	M		9.3.3.3		YES	reject
PDU Session Resource Setup Request List		*0..1*			YES	reject
>PDU Session Resource Setup Request Item		*1..<maxnoofPDUSessions>*			-	
>>PDU Session ID	M		9.3.1.50		-	
>>PDU Session NAS-PDU	O		NAS-PDU 9.3.3.4		-	
>>S-NSSAI	M		9.3.1.24		-	
>>PDU Session Resource Setup Request Transfer	M		OCTET STRING	Containing the *PDU Session Resource Setup Request Transfer* IE specified in subclause 9.3.4.1.	-	
Allowed NSSAI	M		9.3.1.31	Indicates the S-NSSAIs permitted by the network	YES	reject
UE Security Capabilities	M		9.3.1.86		YES	reject
Security Key	M		9.3.1.87		YES	reject
Trace Activation	O		9.3.1.14		YES	ignore
Mobility Restriction List	O		9.3.1.85		YES	ignore
UE Radio Capability	O		9.3.1.74		YES	ignore
Index to RAT/Frequency Selection Priority	O		9.3.1.61		YES	ignore
Masked IMEISV	O		9.3.1.54		YES	ignore
NAS-PDU	O		9.3.3.4		YES	ignore

図 4-5-2-1　Masked IMEISV

（出典　3GPP 文書：TS 38.413　9.2.2.1 INITIAL CONTEXT SETUP REQUEST）

Masked IMEISV の Presence 列は“O”となっておりオプショナルであることが確認できます。また、Assigned Criticality は“ignore”となっており、仮に UE 側がサポートしていない場合にはこのフィールドは無視してよいと考えられます。

しかし、5GC-UE 間の相互接続では、当該フィールドを UE 側がサポートしていないと相互接続できないことが判明したため、5GC 側で“InitialContextSetupRequest”メッセージ内の当該フィールドを削除する措置を施し問題を解決しました。

② DNS の IE が規格上オプショナルなのに NAS のメッセージに存在しないと接続不可

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION ESTABLISHMENT ACCEPT message identity	Message type 9.7	M	V	1
	Selected PDU session type	PDU session type 9.11.4.11	M	V	1/2
	Selected SSC mode	SSC mode 9.11.4.16	M	V	1/2
	Authorized QoS rules	QoS rules 9.11.4.13	M	LV-E	6-65538
	Session AMBR	Session-AMBR 9.11.4.14	M	LV	7
59	5GSM cause	5GSM cause 9.11.4.2	O	TV	2
29	PDU address	PDU address 9.11.4.10	O	TLV	7, 11 or 15
56	RQ timer value	GPRS timer 9.11.2.3	O	TV	2
22	S-NSSAI	S-NSSAI 9.11.2.8	O	TLV	3-10
8-	Always-on PDU session indication	Always-on PDU session indication 9.11.4.3	O	TV	1
75	Mapped EPS bearer contexts	Mapped EPS bearer contexts 9.11.4.8	O	TLV-E	7-65538
78	EAP message	EAP message 9.11.2.2	O	TLV-E	7-1503
79	Authorized QoS flow descriptions	QoS flow descriptions 9.11.4.12	O	TLV-E	6-65538
7B	Extended protocol configuration options	Extended protocol configuration options 9.11.4.6	O	TLV-E	4-65538
25	DNN	DNN 9.11.2.1B	O	TLV	3-102

図 4-5-2-2　DNS IE

（出典　3GPP 文書：TS 24.501　8.3.2 PDU session establishment accept）

Extended protocol configuration options の Presence 列は“O”となっておりオプショナルであることが確認できます。このフィールドの値が設定されていなくても問題ないはずですが、実際にはこのフィールドが設定されていないと PDU セッションの確立に失敗する事象が発生したため、5GC 側で“PDU session establishment accespt”メッセージ内へ当該フィールドを追加する措置を施し問題を解決しました。

※Extended protocol configuration options の詳細は、TS 24.008 に記載があります。

9.11.4.6 Extended protocol configuration options See subclause 10.5.6.3A in 3GPP TS 24.008 [12].

TS 24.008

10.5.6.3A Extended protocol configuration options
10.5.6.3 Protocol configuration options
10.5.6.3.1 General
Table 10.5.154/3GPP TS 24.008: Protocol configuration options information element Network to MS direction:
- 000DH (DNS Server IPv4 Address);

図 4-5-2-3　Extended protocol configuration options の詳細
（出典　3GPP 文書：TS 24.008　）

③ UE と AMF のプロトコルがリビジョン（15.2 と 15.3）によって異なる

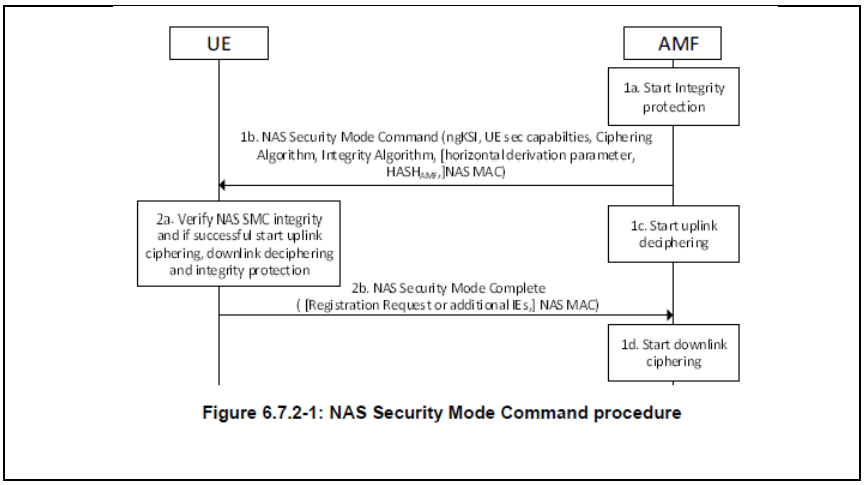


図 4-5-2-4　　V15.2 のシーケンス

（出典　3GPP 文書：TS 24.501　Figure 6.7.2-1: NAS Security Mode Command procedure）

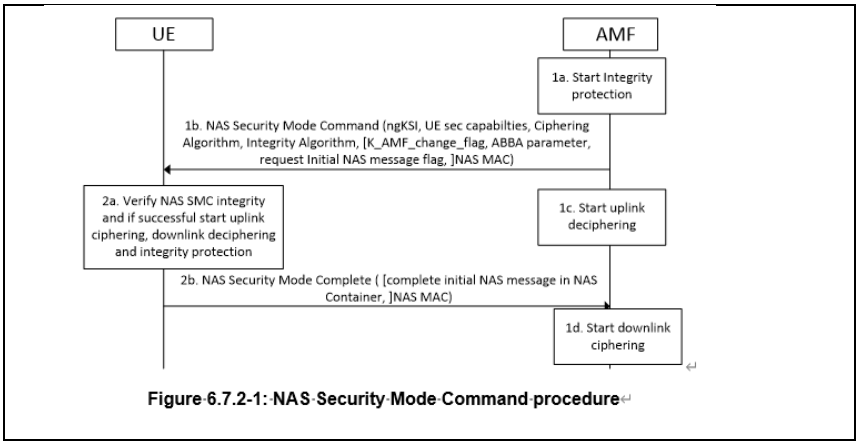


図 4-5-2-5　　V15.3.1 以降のシーケンス

（出典　3GPP 文書：TS 24.501　Figure 6.7.2-1: NAS Security Mode Command procedure）

NAS の Security Mode Command procedure が V15.3.1 から仕様が変わっており、以前のシーケンスと互換性がなく、再接続に失敗するケースがあります。また、CR0488 によって AMF から UE に送信している horizontal derivation parameter が、K_AMF_change_flag に変わりました。

本事象解決のため、5GC 側の“NAS Security mode command”内のフィールド構成を V15.3.1 以降のシーケンスへ対応させる措置を施しました。

(3) 相互接続試験に使用した製品一覧

（ア）5GC コア

本実証では、Free5GC をベースに制作された A 社の 5GC（5GC-A）を採用しました。Free5GC 準拠であり価格も比較的安い国内ベンダー製品という点が選定理由です。

5GC-A を「表 3-3-1　5G コア用基盤サーバ仕様」のコア用基板サーバに仮想化搭載しました。

表 3-3-1 5G コア用基盤サーバ仕様（再掲）

項目	仕様	備考
電源	100-120/200-240VAC	
消費電力	800W パワーサプライ(80PLUS Platinum モデル)×2、最大 2 基、リダンダント構成	
CPU	Intel® Xeon® Gold（16 コア 32 スレッド)×2	
メモリ容量	288GB	
DISK 容量	1.6TB	
概算質量	16.27kg（最大）	
外形寸法	4346×7498×429 mm、1U ラックマウント型	

（イ）CDU/RU

本実証では、3GPP に準拠した B 社製の CDU（CDU-B）と C 社製の CDRU（CDRU-C）を採用しました。CDU-B は集約ノード機能を担う CU(Central Unit)と DU(Distributed Unit)を実装する仮想サーバです。海外ベンダー製品ですが、価格が低い点や多種の UE との接続実績があることから選定しました。CDRU-C はソフトウェア基地局の製品です。

表 3-3-10 CDU-B 仕様（再掲）

項目	仕様	備考
電源	100-120/200-240VAC	
消費電力	800W 以下	
CPU	Intel® Xeon® Gold（20 コア 40 スレッド）	
メモリ容量	256GB	
ストレージ容量	512GB	
概算質量	25kg 以下 ※装置本体のみの質量(アクセサリーを含まない)	
外形寸法	440(W) x 710(D) x 88(H) mm	

表 3-3-11 CDRU-C 仕様（再掲）

項目	仕様	備考
対応周波数帯	4.7～4.8GHz/4.8～4.9GHz 2 つのパターンから選択	
最大出力	+23dBm(200mw)	
アンテナ利得	指向性アンテナ　12dBi	
最大チャネル帯域幅	100MHz	
MIMO レイヤー数 DL/UL	DL：2×2 MIMO UL：2×2 MIMO	
NW インターフェース	Ethernet 1Gbps ×1（保守用） Ethernet 1Gbps ×1（データネットワーク接続点）	
時刻同期	GPS	
対応電源	AC100V	
概算質量	20kg 程度	
外形寸法	(W)285mm ×(H) 513mm ×(D) 471mm	
動作温度	0℃～40℃	

（ウ）UE

UE は令和 3 年現在に商用利用されている製品から 4 機種を選定しました。固定 CPE タイプの A 社製 UE（UE-A)、モバイルルータタイプの D 社製 UE（UE-D）及び、F 社 UE（UE-F)、スマートデバイスの E 社製 UE（UE-E）です。アプリケーションや用途、環境によって使用する UE タイプが異なるため、各 UE タイプより選定しました。

表 3-3-15 UE-A 仕様（再掲）

項目	仕様	備考
電源	AC 給電	
消費電力	最大 40W 以下	
概算質量	1.6kg 以下	
外形寸法	105(W) x 154(D) x 233(H) mm	
動作温度	0℃～+40℃	
対応周波数	5G NR 4.8～4.9GHz 100MHz 幅	
最大空中線電力	23dBm(200mW)	
本体同梱品	AC 電源アダプター x 1	

表 3-3-16 UE-D 仕様（再掲）

項目	仕様	備考
バッテリー	5300mAh(typ)	
バンド	Sub6 n79,mmWave n257,4G B38,B41	
概算質量	228g	
外形寸法	119(W) x 72(D) x 23.5(H) mm	
ディスプレイ	2.4’ タッチパネル付き	
無線	Dual band WiFi(16 端末接続) MIMO 802.11 a/b/g/n/ac/ax	
I/O	USB3.1 Gen2, Type C, Nano-SIM, RJ45	

表 3-3-17 UE-E 仕様（再掲）

項目	仕様	備考
電池容量	4070mAh	
消費電力	最大 40W 以下	
概算質量	約 171g	
外形寸法	164.1(W) x 75.7(D) x 7.7(H) mm	
温湿度条件	5℃～35℃ / 45%～85%RH	
対応周波数	NR （ Sub6 local5G:n79, mmWave local5G:n257）	
外部 I/O	USB TypeC （USB 3.1 Gen2, Displayport サポート）	
コネクティビティ	WLAN（802.11a,b,g,n,ac,ax 2x2MIMO） / Bluetoth 5.1	
ディスプレイ	6.7 インチ（3120 x 1440） フレキシブル有機 EL	
CPU/モデム	SM8250+SDX55M	
OS	Android 10	
カメラ	フロント：32M, リア：48M+16M（広角）+8M（光学 3 倍ズーム）	

表 3-3-18 UE-F 仕様（再掲）

項目	仕様	備考
電池/充電端子	リチウムイオン電池(6000mAh)/USB Type-C(PD3.0)	
位置測位	GPS/GLONASS/BeiDou/Galileo/みちびき/A-GPS	
概算質量	約 326g	
外形寸法	165(W) x 27(D) x 78(H) mm	
ディスプレイ	約 2.6 インチ	
CPU	Qualcomm® Snapdragon™ 865 5G Mobile Platform, Snapdragon™ X55 5G Modem-RF System	
メモリ	RAM：8GB / ROM：128GB	
通信方式	5G NR(Sub6/mmW)、Local5G(Sub6/mmW)、4G LTE™(マルチバンド)	
ネットワークタイプ	NSA/SA ※SA はローカル５Ｇでのみ使用可能です。	

(4) 相互接続組合せ結果

相互接続組合せによる実証結果は「表 4-5-4-1 相互接続組合せ」のとおりです。

表 4-5-4-1 相互接続組合せ

組合せパターン	コア装置	基地局	端末	接続可否
相コ基端-1	5GC-A	CDU-B	UE-A	○
相コ基端-2	5GC-A	CDU-B	UE-D	○
相コ基端-3	5GC-A	CDU-B	UE-E	○
相コ基端-4	5GC-A	CDU-B	UE-F	○
相コ基端-5	5GC-A	CDRU-C	UE-A	×
相コ基端-6	5GC-A	CDRU-C	UE-D	○
相コ基端-7	5GC-A	CDRU-C	UE-E	○
相コ基端-8	5GC-A	CDRU-C	UE-F	○（※）

※「5GC-A」、基地局「CDRU-C」、端末「UE-F」は当初は接続良好であるも、その後に接続不可の事象が発生し解決に至っていない

（ア）5GC-A/CDU-B/UE-A

B 社製 CDU と A 社製 UE を接続検証した結果を「表 4-5-4-2 B 社製 CDU と A 社製 UE 接続結果」に示します。

表 4-5-4-2 B 社製 CDU と A 社製 UE 接続結果

項目	検証結果
相互接続可否	接続可能
UEの電源ON/OFF時の挙動	「（２）相互接続に関連する項目、パラメータ等」を予め設定し基地局の電波が到達している環境下において、UEの電源をONにすることで自動的に基地局にアタッチすることを確認。
機内モードON/OFF	基地局にアタッチしている状況下において、UEに搭載している機内モードをONにすることで、基地局からデタッチされ、機内モードをOFFに戻すと自動的に基地局にアタッチすることを確認。
伝送スループット（DL/UL）	【同期TDD方式】 DL：300Mbps　　UL：28Mbps 【準同期TDD方式】 DL：170Mbps　　UL：60Mbps ※MCS値はDL/ULともに「9」を設定し測定 ※DLは4Layer、ULは1Layer ※UE配下のPCよりiPerfによるスループット計測（1分）の中央値であり、パケットロスが5%以下となる最大伝送スループット
遅延時間	同期TDD：35ms 準同期TDD：36ms ※UE配下のPCからUPFへのPing応答時間（20回）の中央値
長時間安定試験	48時間の連続Ping疎通：応答率99.8%
考察	総合的に問題なく相互接続が可能と考えられる ・電波環境の良いフィールドの場合、MCSをより多値な設定にすることで、伝送スループットの向上が見込める ・UL：1Layerでの結果であるため、今後2Layer以上にシステム改善が進むことでULスループットの向上が期待できる ・準同期TDDによるULスループットの向上が確認でき、遅延時間も正常であることを確認

（イ）5GC-A/CDU-B/UE-D

B 社製 CDU と D 社製 UE を接続検証した結果を「表 4-5-4-3 B 社製 CDU と D 社製 UE 接続結果」に示します。

表 4-5-4-3 B 社製 CDU と D 社製 UE 接続結果

項目	検証結果
相互接続可否	接続可能
UEの電源ON/OFF時の挙動	「（２）相互接続に関連する項目、パラメータ等」を予め設定し基地局の電波が到達している環境下において、UEの電源をONにすることで自動的に基地局にアタッチすることを確認。
機内モードON/OFF	基地局にアタッチしている状況下において、UEに搭載している機内モードをONにすることで、基地局からデタッチされ、機内モードをOFFに戻すと自動的に基地局にアタッチすることを確認。
伝送スループット（DL/UL）	【同期TDD方式】 DL：200Mbps　　UL：28Mbps 【準同期TDD方式】 DL：100Mbps　　UL：58Mbps ※MCS値はDL/ULともに「9」を設定し測定 ※DLは4Layer、ULは1Layer ※UE配下のPCよりiPerfによるスループット計測（1分）の中央値であり、パケットロスが5%以下となる最大伝送スループット
遅延時間	同期TDD：40ms 準同期TDD：36ms ※UE配下のPCからUPFへのPing応答時間（20回）の中央値
長時間安定試験	48時間の連続Ping疎通：応答率100％
考察	総合的に問題なく相互接続が可能と考えられる ・電波環境の良いフィールドの場合、MCSをより多値な設定にすることで、伝送スループットの向上が見込める ・UL：1Layerでの結果であるため、今後2Layer以上にシステム改善が進むことでULスループットの向上が期待できる ・準同期TDDによるULスループットの向上が確認でき、遅延時間も正常であることを確認

（ウ）5GC-A/CDU-B/UE-E

B 社製 CDU と E 社製 UE を接続検証した結果を「表 4-5-4-4 B 社製 CDU と E 社製 UE 接続結果」に示します。

表 4-5-4-4 B 社製 CDU と E 社製 UE 接続結果

項目	検証結果
相互接続可否	接続可能
UEの電源ON/OFF時の挙動	「（２）相互接続に関連する項目、パラメータ等」を予め設定し基地局の電波が到達している環境下において、UEの電源をONにすることで自動的に基地局にアタッチすることを確認。
機内モードON/OFF	基地局にアタッチしている状況下において、UEに搭載している機内モードをONにすることで、基地局からデタッチされ、機内モードをOFFに戻すと自動的に基地局にアタッチすることを確認。
伝送スループット（DL/UL） （※1）	【同期TDD方式】 DL：150Mbps　UL：30Mbps 【準同期TDD方式】 DL：150Mbps　UL：60Mbps ※MCS値はDL/ULともに「9」を設定し測定 ※DLは4Layer、ULは1Layer ※UE配下のPCよりiPerfによるスループット計測（1分）の中央値であり、パケットロスが5%以下となる最大伝送スループット
遅延時間	同期TDD：39ms 準同期TDD：40ms ※UE配下のPCからUPFへのPing応答時間（20回）の中央値
長時間安定試験	48時間の連続Ping疎通：応答率100％
考察	総合的に問題なく相互接続が可能と考えられる ・電波環境の良いフィールドの場合、MCSをより多値な設定にすることで、伝送スループットの向上が見込める ・UL：2Layerを搭載しているが、基地局側が2Layerの受信に対応していないため、2Layer受信が可能となればULスループットの向上が期待できる ・準同期TDDによるULスループットの改善が確認でき、遅延時間も正常であることを確認

（エ）5GC-A/CDU-B/UE-F

B 社製 CDU と F 社製 UE を接続検証した結果を「表 4-5-4-5 B 社製 CDU と F 社製 UE 接続結果」に示します。

表 4-5-4-5 B 社製 CDU と F 社製 UE 接続結果

項目	検証結果
相互接続可否	接続可能
UEの電源ON/OFF時の挙動	「（２）相互接続に関連する項目、パラメータ等」を予め設定し基地局の電波が到達している環境下において、UEの電源をONにすることで自動的に基地局にアタッチすることを確認。
機内モードON/OFF	基地局にアタッチしている状況下において、UEに搭載している機内モードをONにすることで、基地局からデタッチされ、機内モードをOFFに戻すと自動的に基地局にアタッチすることを確認。
伝送スループット（DL/UL）	【同期TDD方式】 DL：250Mbps　　UL：30Mbps 【準同期TDD方式】 DL：115Mbps　　UL：60Mbps ※MCS値はDL/ULともに「9」を設定し測定 ※DLは4Layer、ULは1Layer ※UE配下のPCよりiPerfによるスループット計測（1分）の中央値であり、パケットロスが5%以下となる最大伝送スループット
遅延時間	同期TDD：39ms 準同期TDD：40ms ※UE配下のPCからUPFへのPing応答時間（20回）の中央値
長時間安定試験	48時間の連続Ping疎通：応答率99.6%
考察	総合的に問題なく相互接続が可能と考えられる ・電波環境の良いフィールドの場合、MCSをより多値な設定にすることで、伝送スループットの向上が見込める ・UL：1Layerでの結果であるため、今後2Layer以上にシステム改善が進むことでULスループットの向上が期待できる ・準同期TDDによるULスループットの向上が確認できるが、DLスループットは大きな低下を確認した

（オ）5GC-A/CDRU-C/UE-A

C 社製 CDU と A 社製 UE を接続検証した結果を「表 4-5-4-6 C 社製 CDU と A 社製 UE」に示します。

表 4-5-4-6 C 社製 CDU と A 社製 UE

項目	検証結果
相互接続可否	接続不可
UEの電源ON/OFF時の挙動	「（２）相互接続に関連する項目、パラメータ等」を予め設定したが、基地局とのアタッチが不可であることを確認。
機内モードON/OFF	―
伝送スループット（DL/UL）	―
遅延時間	―
長時間安定試験	―
考察	接続が不可となる原因として、CDU(UE)から送付された特定のメッセージ、“PDU session establishment reqeust”に対して、本来5GCが応答すべきメッセージ、”PDU session establishment accept”を返していないことが判明した。端末のSIM情報は正常に認証されており、その後のPDU session(End-to-Endの通信を繋ぐU-planeの接続性を確保するセッション)の認証リクエストに対して5GCが応答不能となっていた。 特定メッセージの応答不能の原因究明として、応答不能となるまでの認証メッセージ群の差分検証、UE-5GC間に於いて特定条件でのパケットドロップの可能性検証、5GCに内在する潜在不具合の確認を実施し、要因に対して解決方策を施すことで相互接続を実現できる見込み。

（カ）5GC-A/CDRU-C/UE-D

C 社製 CDU と D 社製 UE を接続検証した結果を「表 4-5-4-7 C 社製 CDU と D 社製 UE 接続結果」に示します。

表 4-5-4-7 C 社製 CDU と D 社製 UE 接続結果

項目	検証結果
相互接続可否	接続可能
UEの電源ON/OFF時の挙動	「（２）相互接続に関連する項目、パラメータ等」を予め設定し基地局の電波が到達している環境下において、UEの電源をONにすることで自動的に基地局にアタッチすることを確認。
機内モードON/OFF	基地局にアタッチしている状況下において、UEに搭載している機内モードをONにすることで、基地局からデタッチされ、機内モードをOFFに戻すと自動的に基地局にアタッチすることを確認。
伝送スループット（DL/UL）	【同期TDD方式】 DL：300Mbps　UL：65Mbps 【準同期TDD方式】 DL：200Mbps　UL：150Mbps ※DMCSを有効にし測定 ※DLは4Layer、ULは1Layer ※UE配下のPCよりiPerfによるスループット計測（1分）の中央値であり、パケットロスが5%以下となる最大伝送スループット
遅延時間	同期TDD：32ms 準同期TDD：28ms ※UE配下のPCからUPFへのPing応答時間（20回）の中央値
長時間安定試験	48時間の連続Ping疎通：応答率100％
考察	総合的に問題なく相互接続が可能と考えられる ・DL/UL Total伝送スループットに関して、全8つの組合せの中で最も性能が良い結果を得ている ・準同期TDDによるULスループットの向上が確認でき、遅延時間も正常であることを確認

（キ）5GC-A/CDRU-C/UE-E

C 社製 CDU と E 社製 UE を接続検証した結果を「表 4-5-4-8 C 社製 CDU と E 社製 UE 接続結果」に示します。

表 4-5-4-8 C 社製 CDU と E 社製 UE 接続結果

項目	検証結果
相互接続可否	接続可能
UEの電源ON/OFF時の挙動	「（２）相互接続に関連する項目、パラメータ等」を予め設定し基地局の電波が到達している環境下において、UEの電源をONにすることで自動的に基地局にアタッチすることを確認。
機内モードON/OFF	基地局にアタッチしている状況下において、UEに搭載している機内モードをONにすることで、基地局からデタッチされ、機内モードをOFFに戻すと自動的に基地局にアタッチすることを確認。
伝送スループット（DL/UL） （※1）	【同期TDD方式】 DL：180Mbps　UL：77Mbps 【準同期TDD方式】 DL：180Mbps　UL：135Mbps ※DMCSを有効にし測定 ※DLは4Layer、ULは2Layer ※UE配下のPCよりiPerfによるスループット計測（1分）の中央値であり、パケットロスが5%以下となる最大伝送スループット
遅延時間	同期TDD：30ms 準同期TDD：29ms ※UE配下のPCからUPFへのPing応答時間（20回）の中央値
長時間安定試験	48時間の連続Ping疎通：応答率100％
考察	総合的に問題なく相互接続が可能と考えられる ・DL/UL Total伝送スループットに関して、全8つの組合せの中で最も性能が良い結果を得ている ・準同期TDDによるULスループットの向上が確認でき、遅延時間も正常であることを確認

（ク）5GC-A/CDRU-C/UE-F

C 社製 CDU と E 社製 UE を接続検証した結果を「表 4-5-4-9 C 社製 CDU と E 社製 UE 接続結果」に示します。

表 4-5-4-9 C 社製 CDU と E 社製 UE 接続結果

項目	検証結果
相互接続可否	接続可能
UEの電源ON/OFF時の挙動	「（２）相互接続に関連する項目、パラメータ等」を予め設定し基地局の電波が到達している環境下において、UEの電源をONにすることで自動的に基地局にアタッチすることを確認。
機内モードON/OFF	基地局にアタッチしている状況下において、UEに搭載している機内モードをONにすることで、基地局からデタッチされ、機内モードをOFFに戻すと自動的に基地局にアタッチすることを確認。
伝送スループット（DL/UL）	【同期TDD方式】 DL：250Mbps　UL：30Mbps 【準同期TDD方式】 DL：280Mbps　UL：80Mbps ※DMCSを有効にし測定 ※DLは4Layer、ULは1Layer ※UE配下のPCよりiPerfによるスループット計測（1分）の中央値であり、パケットロスが5%以下となる最大伝送スループット
遅延時間	同期TDD：27ms 準同期TDD：30ms ※UE配下のPCからUPFへのPing応答時間（20回）の中央値
長時間安定試験	未実施
考察	当初問題なく接続できていたが、その後に接続不可となる事象が発生し、原因究明に至らなかった ※以下は接続可能時に計測した性能に関するコメント ・UL：1Layerでの結果であるため、今後2Layer以上にシステム改善が進むことでULスループットの向上が期待できる ・準同期TDDによるULスループットの向上が確認でき、遅延時間も正常であることを確認

基地局毎の伝送スループットの結果は表 4-5-4-10～表 4-5-4-11 にまとめます。

表 4-5-4-10　CDU-B との相互接続における DL/UL 伝送スループット

組合せパターン	同期			準同期 TDD		
	DL	UL	Total	DL	UL	Total
ア	300Mbps	28Mbps	328Mbps	170Mbps	60Mbps	230Mbps
イ	200Mbps	28Mbps	228Mbps	100Mbps	58Mbps	158Mbps
ウ	150Mbps	30Mbps	180Mbps	150Mbps	60Mbps	210Mbps
エ	300Mbps	28Mbps	328Mbps	115Mbps	60Mbps	175Mbps

表 4-5-4-11　CDRU-C との相互接続における DL/UL スループット

組合せパターン	同期			準同期 TDD		
	DL	UL	Total	DL	UL	Total
オ	接続不可	接続不可	-	接続不可	接続不可	-
カ	300Mbps	65Mbps	365Mbps	200Mbps	150Mbps	350Mbps
キ	180Mbps	77Mbps	257Mbps	180Mbps	135Mbps	315Mbps
ク	280Mbps	30Mbps	310Mbps	250Mbps	80Mbps	330Mbps

(5)　相互接続に関する考察

現在、3GPP では第５世代移動通信システム(5G)のサービス要求実現に向けて、新しいコアネットワークの策定検討を行われています。3GPP での標準化は、各国及び各ベンダー間の仕様の指標となっており、3GPP に準拠した製品間での相互接続が今後期待されています。一方でコア・基地局・端末に関して、フィールドの要件やアプリケーションを使用する上での所要性能に応じて、柔軟に組み合わせて設計することが望まれています。

相互接続を実現するには、3GPP に準拠したインターフェースとすることが必要であり、特に、（２）で挙げている項目に関しては、不整合時に相互接続が実現できないことが推定されます。

本実証では、当該標準規格に準拠した製品の８つの組合せにおいて検証し、7 つの組合せにおいて相互接続を実現に成功し、伝送速度や遅延時間等も含めた各性能を明らかにしました。

しかし、接続不可となった１つの組合せ（5GC-A×CDRU-C×UE-A）及び当初は問題なく接続できたがその後に接続不可となった１つの組合せ（5GC-A×CDRU-C×UE-F）に関しては、原因究明に至っていないため今後改善を図ります。この結果をふまえると、今回実証していない他の製品の組合せ等において、別に整合を取る必要があるパラメータ等が存在すると推定されるため、相互接続に必要な要件を明らかにするためには、今後も継続して検討及び解析が必要であると考えられます。

これらの結果をふまえ、令和４年度における相互接続に関する調査研究では、以下４点のテーマの実行を推奨します。

・令和３年度の相互接続試験において接続不可及び通信断が生じた組合せに関する原因究明及び改善措置の実行
・相互接続の実現方策のブラッシュアップ及び独自解釈パラメータ等の分析
・新たな組合せによる相互接続検証
・上記をふまえた相互接続ガイドライン（本ケーススタディの更新含む）の検討、作成

5. ローカル５Ｇシステムの検証

5.1 検証概要

本検証では、複数企業共用パターン及び業界共用パターンそれぞれの構成におけるローカル５Ｇシステムの性能、機能、セキュリティの検証を行うことで、各種課題を洗い出し、令和 4 年以降のコアの共用実現に向けて実装が必要な機能等を報告書にまとめます。

5.2 検証環境

検証環境については以下のとおりです。

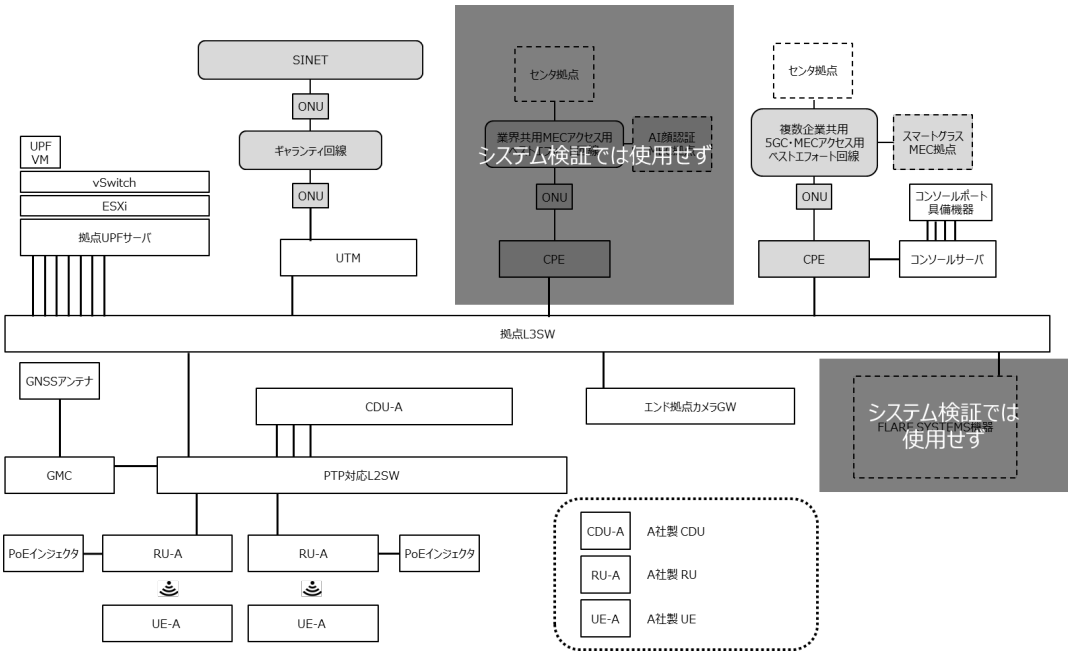


図 5-2-1 システム検証におけるネットワーク構成図 NTT 中央研修センタ

RU 設置については以下の「図 5-2-2　RU 設置の様子（NTT 中央研修センタ）」のとおりです。

図 5-2-2 RU 設置の様子（NTT 中央研修センタ）

また 5.3 章の（１）コアの共用における性能検証の検証項目において、UE の接続台数を検証する項目について「図 5-2-3　接続可能台数検証の様子（NTT 中央研修センタ）」に示す構成で行いました。

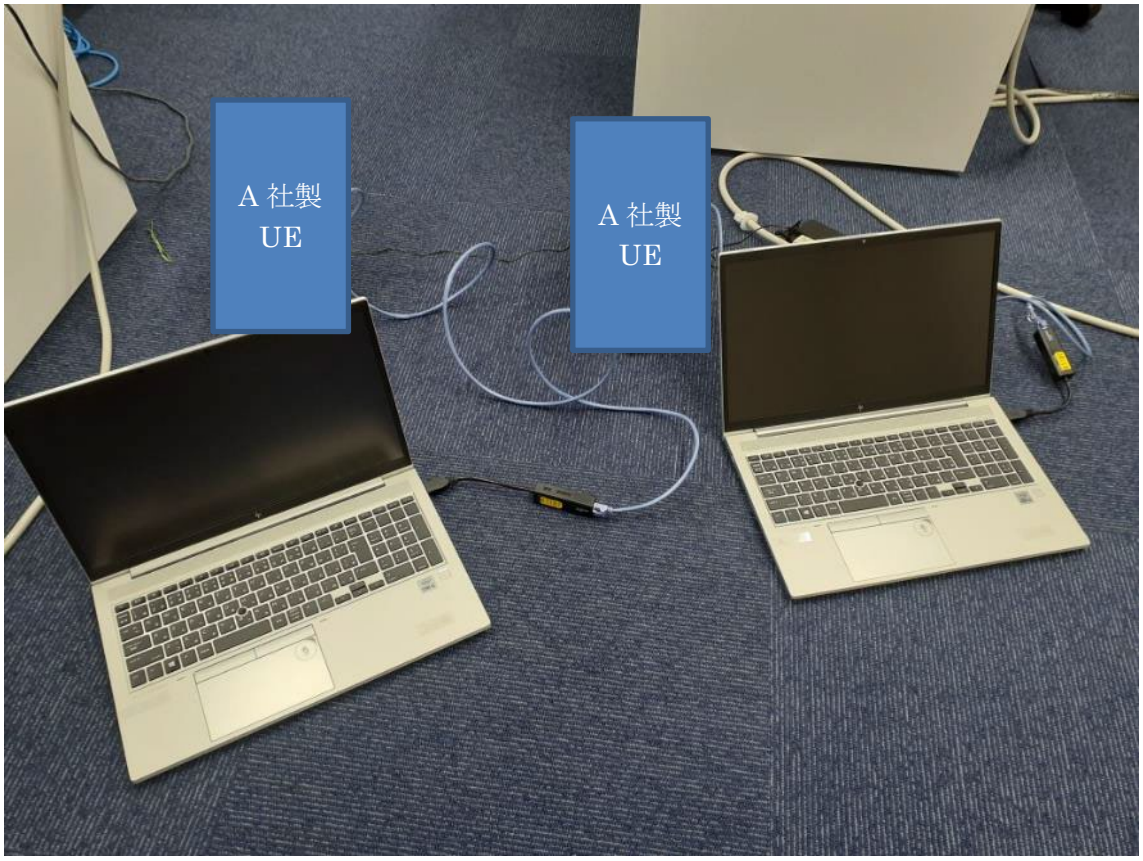


図 5-2-3　接続可能台数検証の様子（NTT 中央研修センタ）

RU と UE の設置距離は「図 5-2-4　RU と UE の設置の様子（NTT 中央研修センタ）」に示すとおりです。なお、どの拠点でも RU と UE 間は 5-10ｍであるよう設置しました。

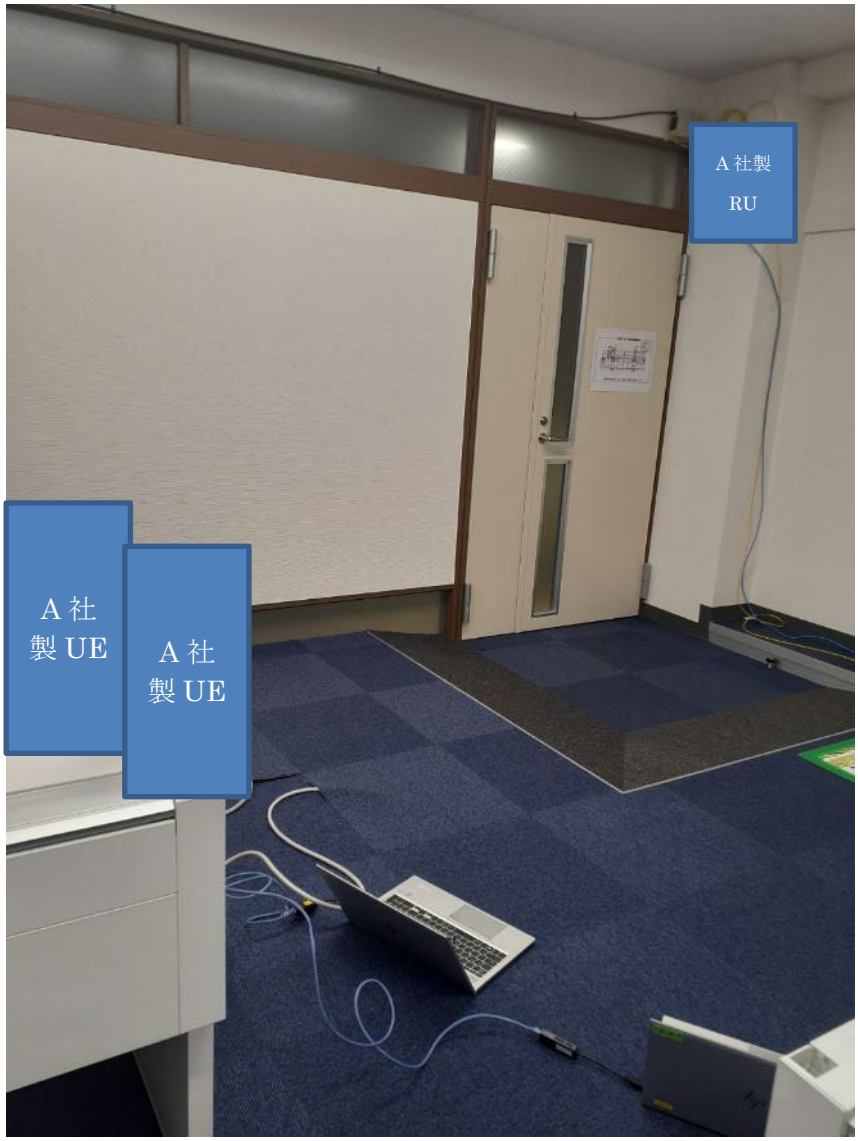


図 5-2-4　RU と UE の設置の様子（NTT 中央研修センタ）

ローカル５Ｇコアを共用する際、コアおよび基地局の配置パターンが複数考えられます。本検証においてはローカル５Ｇ構成要素の配置方法を「図 5-2-5　ローカル５Ｇ機器配置パターン」に示す 3 パターンとし、費用低減に向けた設備集約配置やネットワーク遅延回避に向けたアクセス方法を検討します。

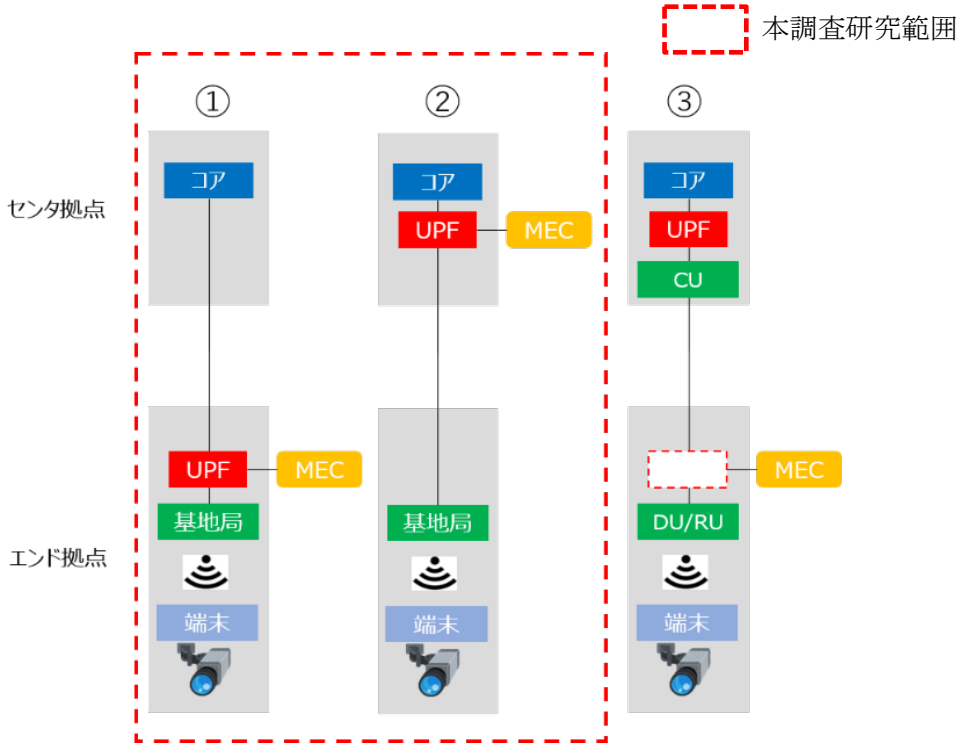


図 5-2-5　ローカル５Ｇ機器配置パターン

今年度はその中でも基本的な構成である「①」を中心に検証を行います。また、UPF の設置場所による機能比較も検証し、「複数企業共用パターン」及び「業界共用パターン」における最適な配置を検討するため「②」も加えて検証を行います。なお、基地局と端末間は電界強度による検証への影響を避けるため、遮蔽物の無い見通しの効くスペースにて検証を行います。

5.3 検証内容・評価分析

(1) コアの共用における性能検証

① 検証目標

コア設備を共用する環境下において、端末数やデータ通信量等の変化に伴い有限なリソースである CPU やメモリの所要量を検証します。また、伝送スループットや伝送遅延時間の性能について、UPF の設置位置や地上回線網の回線種別による差分を比較し、影響を明らかにします。

② 評価・検証項目

本検証での評価・検証項目は、以下の「表 1-2-4-1 性能検証項目概要」及び「表 5-3-1-2-1　評価・検証項目」のとおりです。

表 1-2-4-1　性能検証項目概要（再掲）

項番	項目	概要
(1)-1	消費リソースの検証	コアの共用環境では、複数の拠点でローカル５Ｇのネットワークが構築されるため、各拠点では端末（UE）がそれぞれ共用しているコアに接続される形態であり、コアを共用しない形態と比較すると端末数が多くなることが推定されます。 コアの共用環境を設計構築するうえでは、各拠点の端末が同時接続されるとき、各機器（5GC、UPF、CDU、RU）の UE の接続時の消費リソースを把握する必要があるため、UE1 台が接続した際の消費リソースと複数台 UE が接続した際の消費リソースを検証しました。また、UL 方向のデータ通信（5Mbps/1UE）の状況を模擬し、複数台接続時の消費リソースの変化を考察しました。 消費リソースは、メモリ消費量と CPU 使用率の 2 点を対象に確認しました。
(1)-2	UE 接続台数の最大数検証	端末の最大接続数は、5GC や CDU の性能によって異なります。コア共用環境下において、複数の拠点でローカル５Ｇシステムが稼働している状況で､RU-UE 区間の伝送性能が共用環境によって劣化するのか検証することを目的に、最大接続端末数を検証するとともに、(1)-4 における伝送スループットの結果と比較し、コアの共用における影響を検証しました。
(1)-3	UE 接続時間の検証	センタ拠点（5GC 設置拠点）に対して、異なる地方等で地上の広域回線の距離や回線種別が異なる各実証フィールドにおいて、UE が 5GC システムにアクセスし認証完了するまでの接続時間を計測することで、その差分を比較す

		るとともに、コア装置を共用するうえで実用的な回線種別や範囲について考察しました。
(1)-4	UE～UPF 間の通信性能の検証	コアの共用環境では、ローカル５Ｇシステムの通信はエンド拠点の UE 端末からセンタ拠点まで物理的に長い距離を介することが想定されます。この地上の広域回線区間について、ギャランティ型とベストエフォート型の回線を用意し、この回線の種別による伝送スループット及び遅延時間への影響を検証しました。 また、地上の広域回線の区間が特に長いロケーションの場合、低遅延が要求されるアプリケーションでは実用が困難となることが考えられるため、エンド拠点に UPF を設置したケースにおける遅延時間を検証しました。 本検証における結果を分析し、センタ拠点で UPF を共用するモデルの実用可否を考察しました。

表 5-3-1-2-1 評価・検証項目

大項目	中項目	小項目	検証概要	検証項目
性能検証	性能確認	複数企業共用パターン	接続に必要なリソース	コア装置の CPU、メモリ
				UPF の CPU、メモリ
				CDU、RU の CPU、メモリ
			接続後に必要なリソース	コア装置の CPU、メモリ
				UPF の CPU、メモリ
				CDU、RU の CPU、メモリ
				PC1～PC-A へのスループット、遅延値
			端末接続台数の限界数	１つのコアに対して接続可能な UE の数量
		業界共用パターン	接続に必要なリソース	コア装置の CPU、メモリ
				UPF の CPU、メモリ
				CDU、RU の CPU、メモリ
			接続後に必要なリソース	コア装置の CPU、メモリ
				UPF の CPU、メモリ
				CDU、RU の CPU、メモリ
				PC1～PC-A へのスループット、遅延値
			端末接続台数の限界数	１つのコアに対して接続可能な UE の数量
	接続確認	複数企業共用パターン	接続に必要な時間	UE がコア装置で認証されるまでに要する時間
		業界共用パターン	接続に必要な時間	UE がコア装置で認証されるまでに要する時間

③　評価・検証方法

本検証で用いる測定ツールは、「表 5-3-1-3-1　測定ツール」のとおりです。

表 5-3-1-3-1　測定ツール

項目	測定内容および具体的なツール
測定ツール	OS リソース取得：Linux コマンド等
	伝送スループット：iperf 等の測定ツール
	伝送遅延時間：ping 試験

各評価・検証項目の実施イメージは以下のとおりです。

UE の接続時及び U-Plane 通信時のそれぞれにおいて、5GC、UPF（エンド拠点及びセンタ拠点それぞれ）、CDU、RU の消費リソースを確認しました。また、UE 接続台数を増やした状況での消費リソースの変動状況を確認しました。

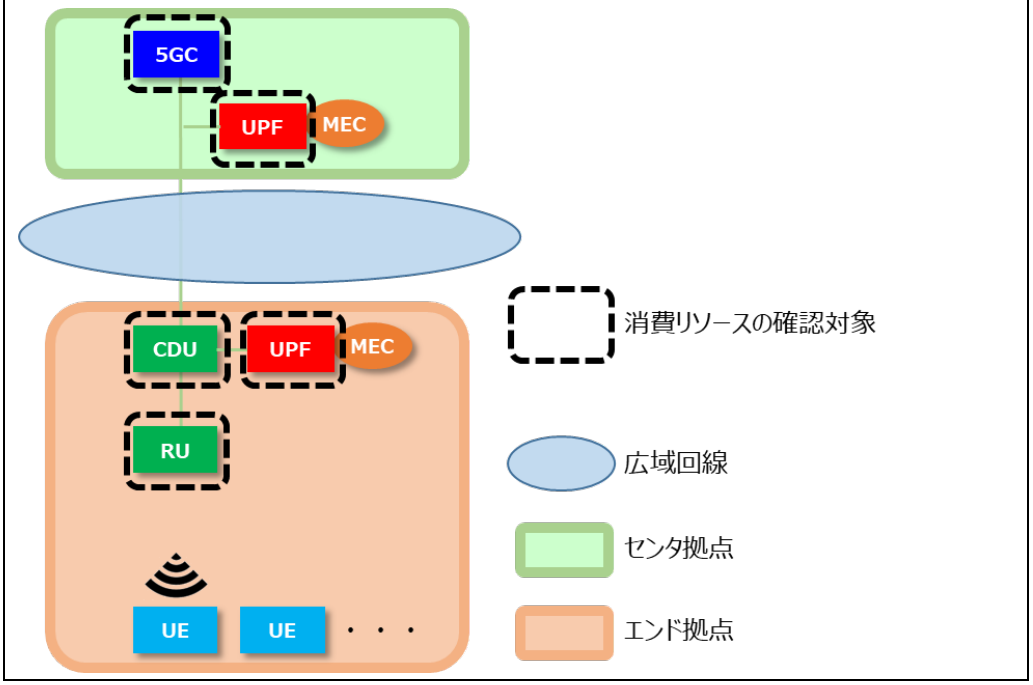


図 1-2-4-2　検証イメージ　消費リソースの検証　（再掲）

エンド拠点において、1 台の RU 及び CDU に接続できる端末数の限界数について確認を行いました。また、1 台の UE 接続時の最大伝送スループットと複数台 UE 接続時の Total 伝送スループットの差分比較を実施しました。

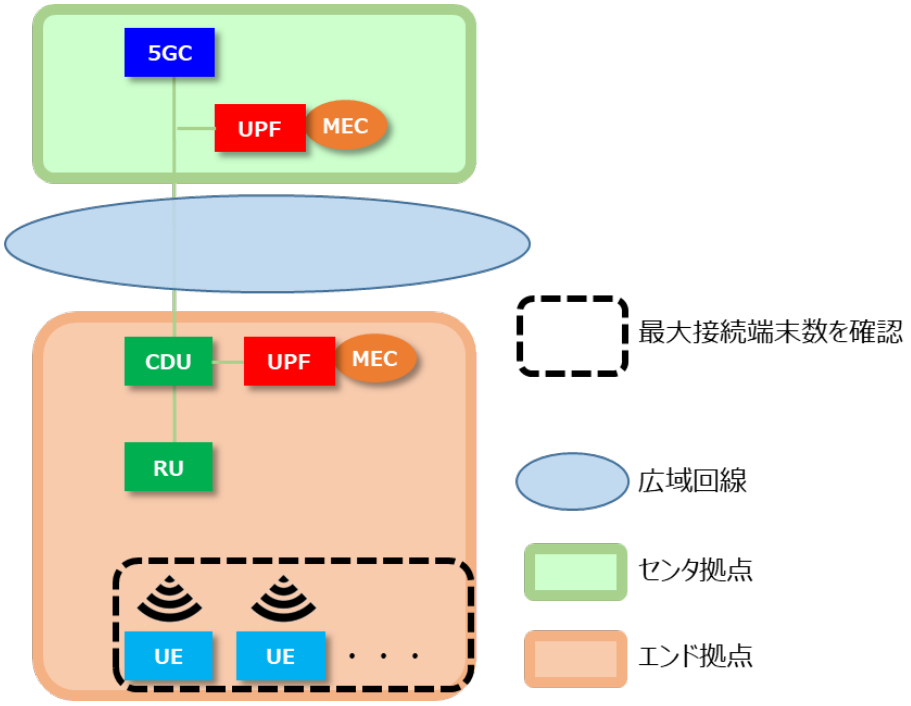


図 1-2-4-3　検証イメージ　UE 接続台数の最大数検証　(再掲)

本実証フィールドのすべてのエンド拠点において、UE 端末が接続に要する時間を確認しました。加えて、UE からセンタ拠点 UPF とエンド拠点 UPF の双方について pingRTT による遅延影響を確認しました。

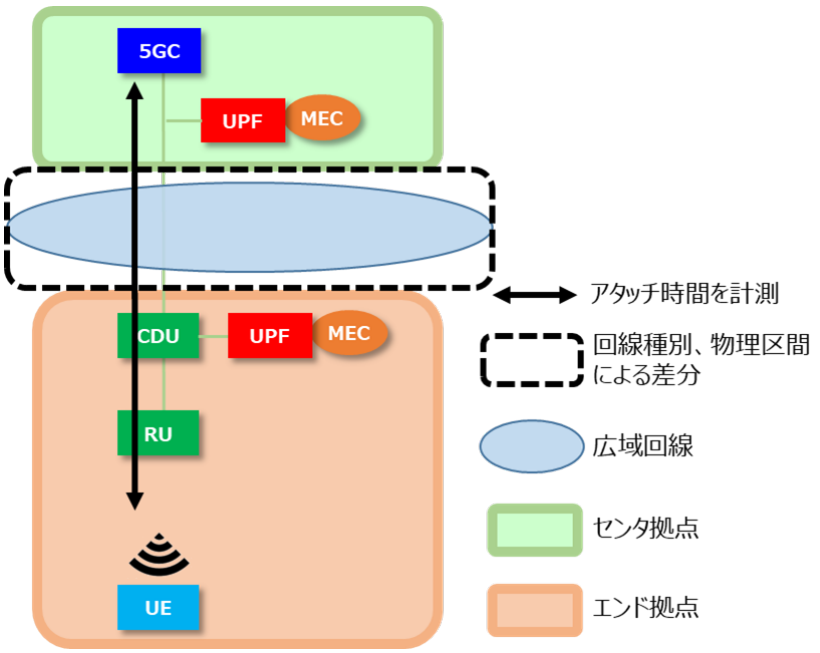


図 1-2-4-4　　UE 接続時間の検証　(再掲)

伝送スループット及び遅延時間の検証として、広域回線による差分と UPF 設置位置による性能への影響を確認しました。

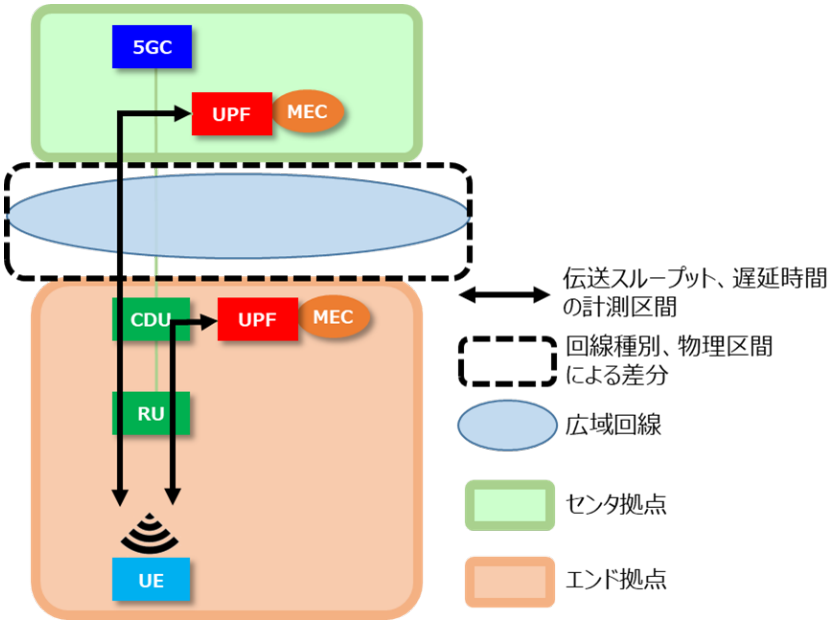


図 1-2-4-5　検証イメージ　UE～UPF 間の通信性能の検証　(再掲)

本検証において、UPF の設置位置と各共用パターンについては、「表 5-3-1-3-2　UPF 設置位置と共用パターンの組合せ」のとおり検証を実施します。

表 5-3-1-3-2　UPF 設置位置と共用パターンの組合せ

項番	使用する UPF の設置位置	共用パターン
1	エンド拠点設置の UPF	複数企業共用パターン
2	センタ拠点設置の UPF	複数企業共用パターン
3	エンド拠点設置の UPF	業界共用パターン
4	センタ拠点設置の UPF	業界共用パターン

検証手順及び検証イメージは、以下の表 5-3-1-3-3～表 5-3-1-3-6 及び図 5-3-1-3-1～図 5-3-1-3-6 のとおりです。

「表 5-3-1-3-3　検証手順（複数企業共用パターン）」及び「表 5-3-1-3-4　検証手順（業界共用パターン）」については検証拠点である NTT 中央研修センタで実施します。「表 5-3-1-3-5　接続検証手順（複数企業共用パターン）」については複数企業共用パターンのエンド拠点であるいすゞ自動車で、「表 5-3-1-3-6　接続検証手順（業界共用パターン）」については業界共用パターンのエンド拠点である東北大学、東京大学、京都大学で実施します。

表 5-3-1-3-3 検証手順（複数企業共用パターン）

項番	実施内容	対応図表
性性複-1	エンド拠点設置の UPF を使うようローカル５Ｇシステムに設定	―
性性複-2	PC1 を UE1 に有線で接続（1000Base-T）し、ローカル５Ｇシステムに接続	図 5-3-1-3-1
	表 5-3-1-2-1 の項番 1 のリソース情報を取得	
性性複-3	正常に接続されたことを確認し、PC1 から PC-A に対して 5Mbps のトラフィック負荷を印加	図 5-3-1-3-1
	表 5-3-1-2-1 の項番 2 のリソース情報を取得	
性性複-4	PC2 を UE2 に有線で接続（1000Base-T）し、ローカル５Ｇシステムに接続	図 5-3-1-3-1
	表 5-3-1-2-1 の項番 1 のリソース情報を取得	
性性複-5	正常に接続されたことを確認し、PC2 から PC-A に対して 5Mbps のトラフィック負荷を印加	図 5-3-1-3-1
	表 5-3-1-2-1 の項番 2 のリソース情報を取得	
性性複-6	UE の接続が不安定となり、UE を増やすことができなくなる、もしくは 8 台目の検証が終了するまで性性複-4、5 を繰り返す	―
性性複-7	センタ拠点設置の UPF を使うようローカル５Ｇシステムに設定	―
性性複-8	PC1 を UE1 に有線で接続（1000Base-T）し、ローカル５Ｇシステムに接続	図 5-3-1-3-2
	表 5-3-1-2-1 の項番 1 のリソース情報を取得	
性性複-9	正常に接続されたことを確認し、PC1 から PC-B に対して 5Mbps のトラフィック負荷を印加	図 5-3-1-3-2
	表 5-3-1-2-1 の項番 2 のリソース情報を取得	
性性複-10	PC2 を UE2 に有線で接続（1000Base-T）し、ローカル５Ｇシステムに接続	図 5-3-1-3-2
	表 5-3-1-2-1 の項番 1 のリソース情報を取得	
性性複-11	正常に接続されたことを確認し、PC2 から PC-B に対して 5Mbps のトラフィック負荷を印加	図 5-3-1-3-2
	表 5-3-1-2-1 の項番 2 のリソース情報を取得	
性性複-12	UE の接続が不安定となり、UE を増やすことができなくなる、もしくは 8 台目の検証が終了するまで性性複-10、11 を繰り返す	―

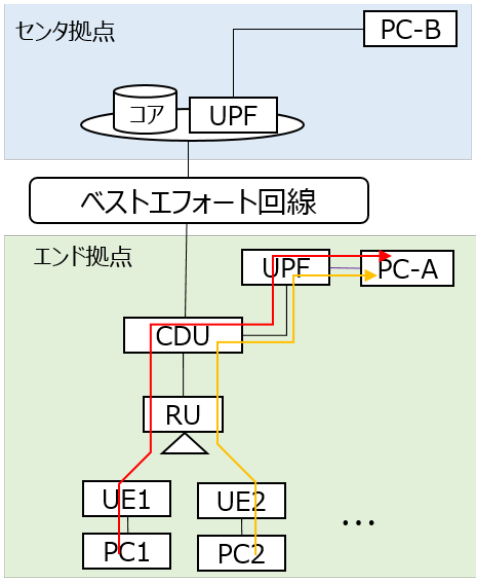


図 5-3-1-3-1　検証イメージ（エンド拠点設置の UPF を使用）

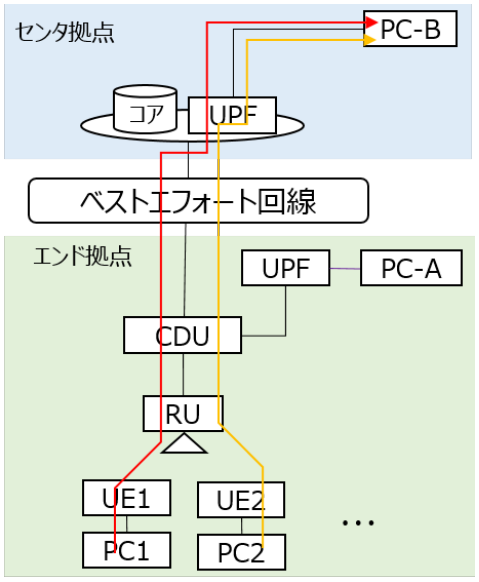


図 5-3-1-3-2　検証イメージ（センタ拠点設置の UPF をベストエフォート回線経由で使用）

表 5-3-1-3-4 検証手順（業界共用パターン）

項番	実施内容	対応図表
性性業-1	エンド拠点設置の UPF を使うようローカル５Ｇシステムに設定	―
性性業-2	PC1 を UE1 に有線で接続（1000Base-T）し、ローカル５Ｇシステムに接続	図 5-3-1-3-3
	表 5-3-1-2-1 の項番 1 のリソース情報を取得	
性性業-3	正常に接続されたことを確認し、PC1 から PC-A に対して 5Mbps のトラフィック負荷を印加	図 5-3-1-3-3
	表 5-3-1-2-1 の項番 2 のリソース情報を取得	
性性業-4	PC2 を UE2 に有線で接続（1000Base-T）し、ローカル５Ｇシステムに接続	図 5-3-1-3-3
	表 5-3-1-2-1 の項番 1 のリソース情報を取得	
性性業-5	正常に接続されたことを確認し、PC2 から PC-A に対して 5Mbps のトラフィック負荷を印加	図 5-3-1-3-3
	表 5-3-1-2-1 の項番 2 のリソース情報を取得	
性性業-6	UE の接続が不安定となり、UE を増やすことができなくなる、もしくは 8 台目の検証が終了するまで性性業-4、5 を繰り返す	―
性性業-7	センタ拠点設置の UPF を使うようローカル５Ｇシステムに設定	―
性性業-8	PC1 を UE1 に有線で接続（1000Base-T）し、ローカル５Ｇシステムに接続	図 5-3-1-3-4
	表 5-3-1-2-1 の項番 1 のリソース情報を取得	
性性業-9	正常に接続されたことを確認し、PC1 から PC-B に対して 5Mbps のトラフィック負荷を印加	図 5-3-1-3-4
	表 5-3-1-2-1 の項番 2 のリソース情報を取得	
性性業-10	PC2 を UE2 に有線で接続（1000Base-T）し、ローカル５Ｇシステムに接続	図 5-3-1-3-4
	表 5-3-1-2-1 の項番 1 のリソース情報を取得	
性性業-11	正常に接続されたことを確認し、PC2 から PC-B に対して 5Mbps のトラフィック負荷を印加	図 5-3-1-3-4
	表 5-3-1-2-1 の項番 2 のリソース情報を取得	
性性業-12	UE の接続が不安定となり、UE を増やすことができなくなる、もしくは 8 台目の検証が終了するまで性性業-10、11 を繰り返す	―

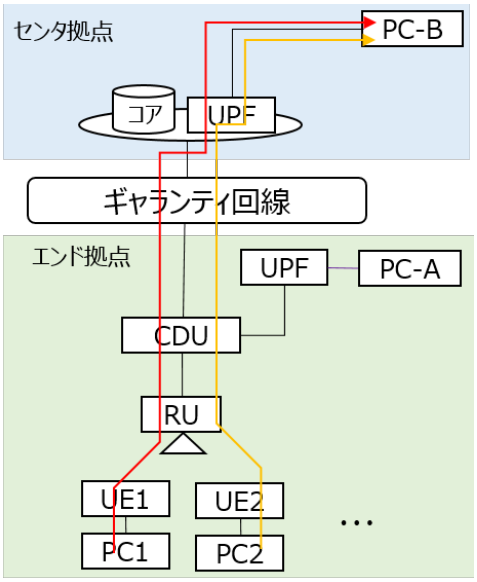


図 5-3-1-3-3　検証イメージ（センタ拠点設置の UPF をギャランティ回線経由で使用）

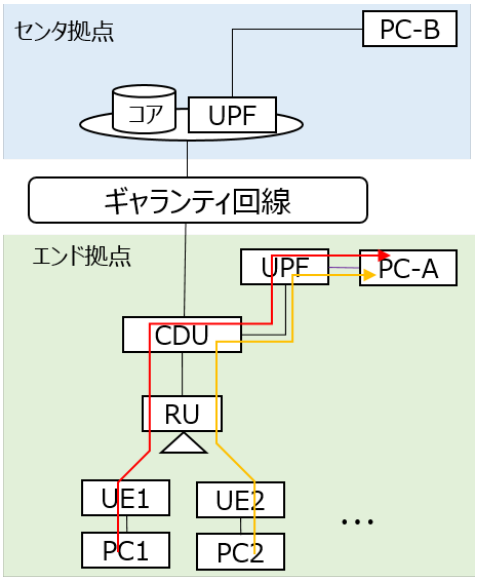


図 5-3-1-3-4　検証イメージ（エンド拠点設置の UPF を使用）

表 5-3-1-3-5 接続検証手順（複数企業共用パターン）

項番	実施内容	対応図表
性ア複-1	エンド拠点設置の UPF を使うようローカル５Ｇシステムに設定	―
性ア複-2	PC1 から PC-A に対し疎通試験を開始した後、UE1 の接続を開始	図 5-3-1-3-5
性ア複-3	正常に接続されたことを確認し、UE の接続処理に要した時間を測定	図 5-3-1-3-5
性ア複-4	PC1 から PC-A、PC-B に対して疎通試験および遅延値を測定	図 5-3-1-3-5

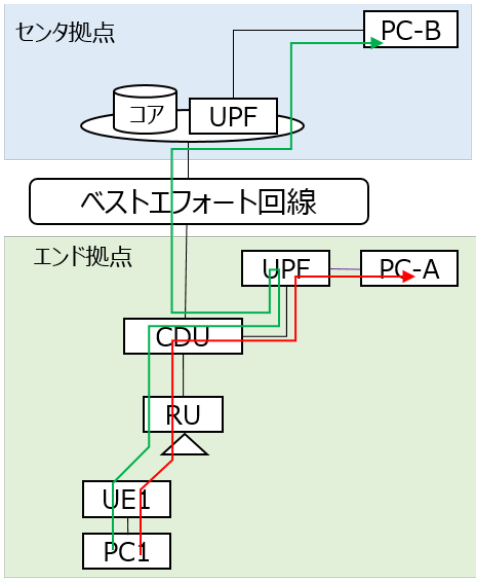


図 5-3-1-3-5　検証イメージ（エンド拠点設置の UPF を使用）

表 5-3-1-3-6 接続検証手順（業界共用パターン）

項番	実施内容	対応図表
性ア業-1	エンド拠点設置の UPF を使うようローカル５Ｇシステムに設定	―
性ア業-2	PC1 から PC-A に対し疎通試験を開始した後、UE1 の接続を開始	図 5-3-1-3-6
性ア業-3	正常に接続されたことを確認し、UE の接続処理に要した時間を測定	図 5-3-1-3-6
性ア業-4	PC1 から PC-A、PC-B に対して疎通試験および遅延値を測定	図 5-3-1-3-6

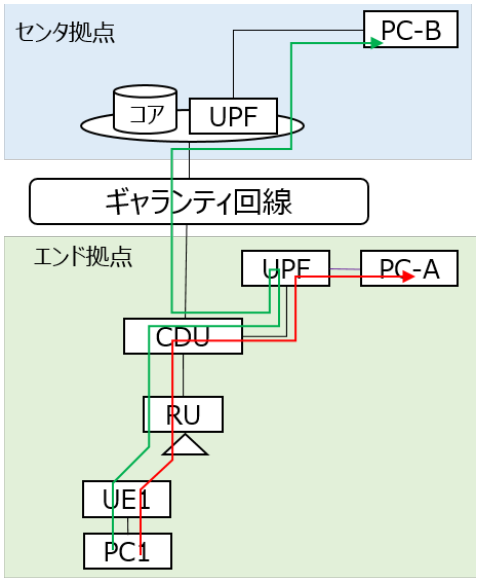


図 5-3-1-3-6　検証イメージ（エンド拠点設置の UPF を使用）

本検証において、伝送スループット及び伝送遅延時間の測定は「表 5-3-1-3-7 伝送スループット及び伝送遅延時間の測定ツール」のとおり実行します。

表 5-3-1-3-7　伝送スループット及び伝送遅延時間の測定ツール

項目	測定ツール	測定条件
伝送遅延時間	ping 応答	応答数 20 回
伝送スループット（DL）	iperf2	1 回／3 分
伝送スループット（UL）	iperf2	1 回／3 分

伝送遅延時間は ping RTT を用いて測定を行い、測定値は応答数 20 回の平均値とし、測定ルートは要求/応答の折り返し総合伝送遅延時間とします。

伝送スループットは iperf2 を用いて通信トラフィックを疑似的に印加し測定します。対象プロトコルは UDP とし、連続して 3 分間測定します。このとき、安定的な通信環境の前提を、「パケット損失（瞬時値）5%以下」とし伝送スループットを測定します。

※上記の測定は、RU－UE 間を LOS 環境かつ離隔距離を 5m として測定します。

④　結果

ア 複数企業共用パターン

（ア）　消費リソースの検証

i.　　エンド拠点 UPF 時

UE の接続台数を増加させ、リソースの推移を測定しました。結果は下記の表 5-3-1-4-1～5-3-1-4-2、図 5-3-1-4-1～5-3-1-4-4 のとおりです。

表 5-3-1-4-1　複数企業共用・エンド UPF 時接続リソース

台数/通信状態		5GC		UPF		CDU			RU	
		消費CPU [%]	消費メモリ [MiB]	消費CPU [%]	消費メモリ [MiB]	消費CPU(CU) [%]	消費CPU(DU) [%]	消費メモリ [KiB]	消費CPU [%]	消費メモリ [KB]
0台	-	0.6	449.2	0.3	365.8	82.82	37.72	54,981,972	18.07	127,732
1台目	アタッチ後	0.7	459.21	0	367.6	83.32	38.34	54,982,474	16.72	127,701
	UL5Mbps印加後	0.3	454.46	0	367.5	83.42	40.02	54,983,086	16.95	127,815
2台目	アタッチ後	1	458.62	0.3	367.3	83.85	39.32	54,983,811	16.18	127,912
	UL5Mbps印加後	0.3	460.55	0.3	367.4	83.63	40.15	54,984,436	17.81	127,968
3台目	アタッチ後	0.6	465.9	0.3	368.0	83.81	40.07	54,984,401	17.56	127,871
	UL5Mbps印加後	0.6	457.99	0.3	368.7	84.34	40.76	54,984,880	18.28	128,079

※「消費 CPU」はシステム総和に対する使用率で示す

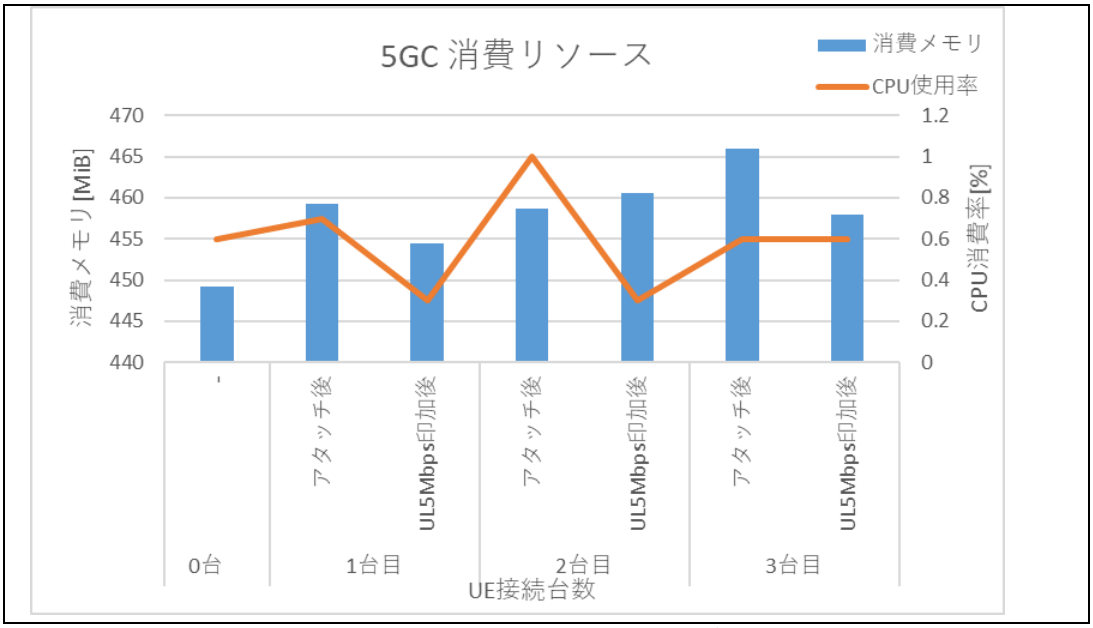


図 5-3-1-4-1 5GC 消費リソース推移（複数・エンド）

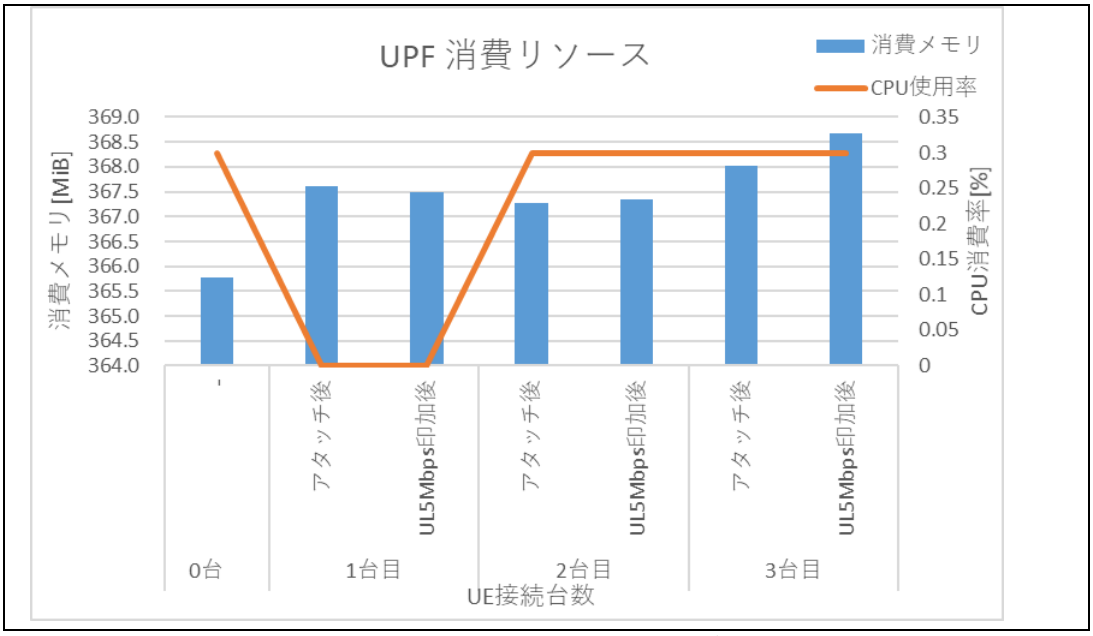


図 5-3-1-4-2 UPF 消費リソース推移（複数・エンド）

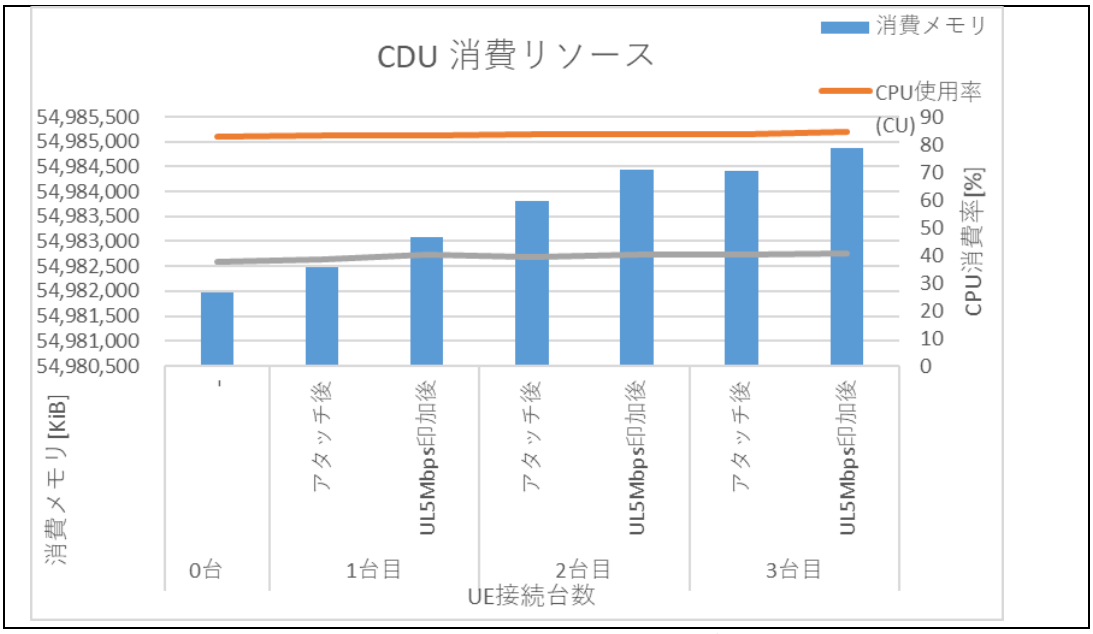


図 5-3-1-4-3 CDU 消費リソース推移（複数・エンド）

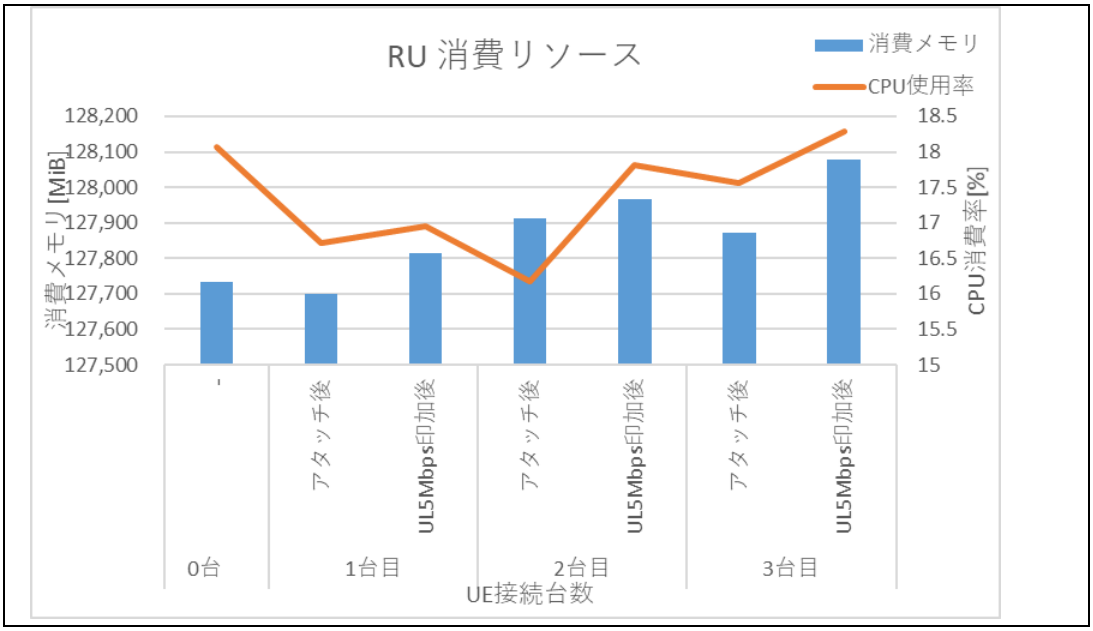


図 5-3-1-4-4 RU 消費リソース推移（複数・エンド）

表 5-3-1-4-2　UE1 台のデータ通信実行における消費リソースの偏移（複数・エンド）

対象装置	UE1 台（UL5Mbps 印加）における消費リソースの偏移状況	
	消費メモリ	CPU 使用率
5GC	最大 約 6[MiB]の増加	増加影響は見られない
UPF	最大 約 2[MiB]の増加	増加影響は見られない
CDU	最大　約 1,400[KiB]の増加	増加影響は見られない
RU	最大　約 150[KB]の増加	増加影響は見られない

ii.　　センタ拠点 UPF 時

UE の接続台数を増加させ、リソースの推移を測定しました。結果は下記の表 5-3-1-4-3～5-3-1-4-4、図 5-3-1-4-5～5-3-1-4-8 のとおりです。

表 5-3-1-4-3　複数企業共用・センタ UPF 時接続リソース

台数/通信状態		5GC		UPF		CDU			RU	
		消費CPU [%]	消費メモリ [MiB]	消費CPU [%]	消費メモリ [%]	消費CPU(CU) [%]	消費CPU(DU) [%]	消費メモリ [KiB]	消費CPU [%]	消費メモリ [KB]
0台	-	0.6	477.54	99.3	0.5	82.82	37.9	54,975,238	16.5	127,732
1台目	アタッチ後	0.6	480.71	99.7	0.5	82.67	38.35	54,974,977	16.7	127,701
	UL5Mbps印加後	0.6	481.02	99.7	0.5	82.47	40.6	54,976,938	18.19	127,815
2台目	アタッチ後	0.3	483.32	99.7	0.5	83.44	39.54	54,978,218	17.76	127,912
	UL5Mbps印加後	0.7	483.34	99.7	0.5	83.77	39.51	54,977,259	16.78	127,968
3台目	アタッチ後	0.6	485.38	99.7	0.5	84.6	40.16	54,978,056	17.61	127,871
	UL5Mbps印加後	0.3	487.16	99.7	0.5	84.87	41.4	54,978,952	17.26	128,079

※「消費 CPU」はシステム総和に対する使用率で示す

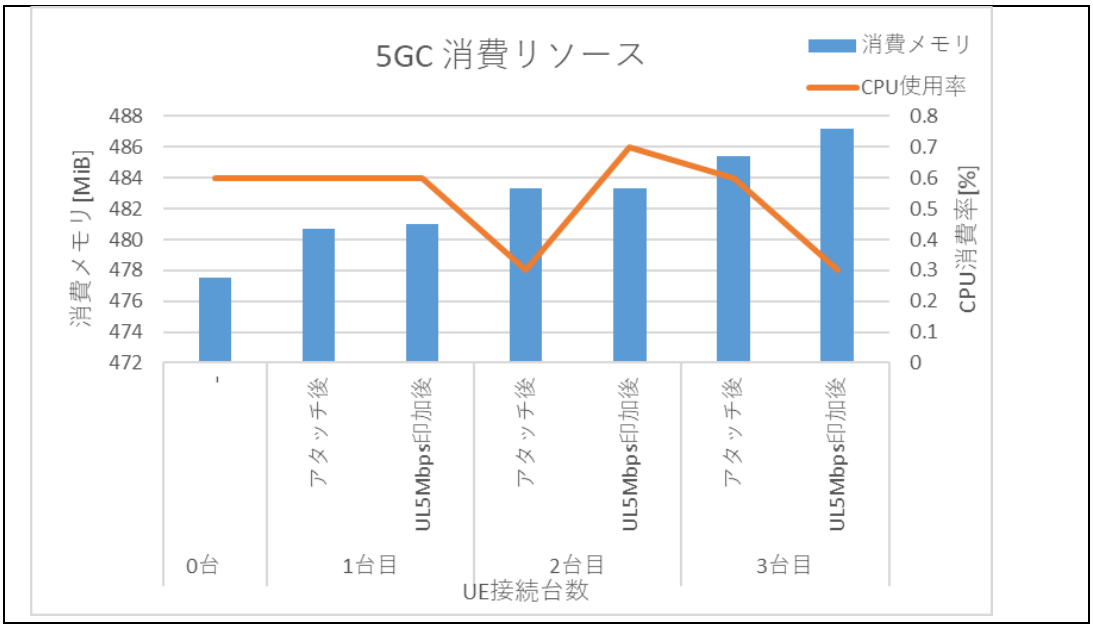


図 5-3-1-4-5　5GC 消費リソース推移（複数・センタ）

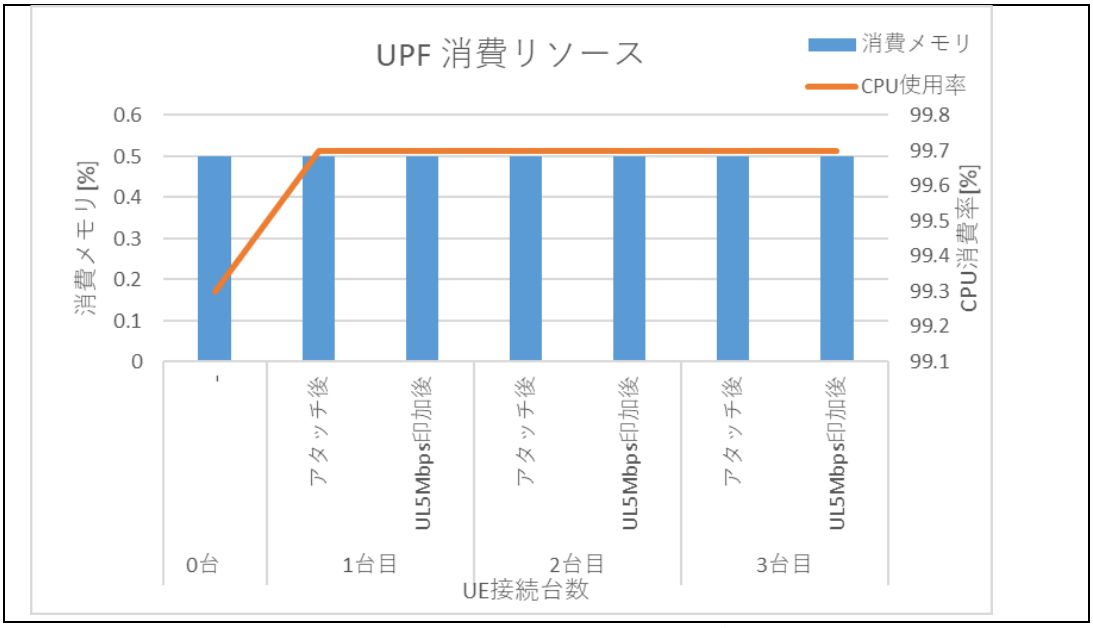


図 5-3-1-4-6　UPF 消費リソース推移（複数・センタ）

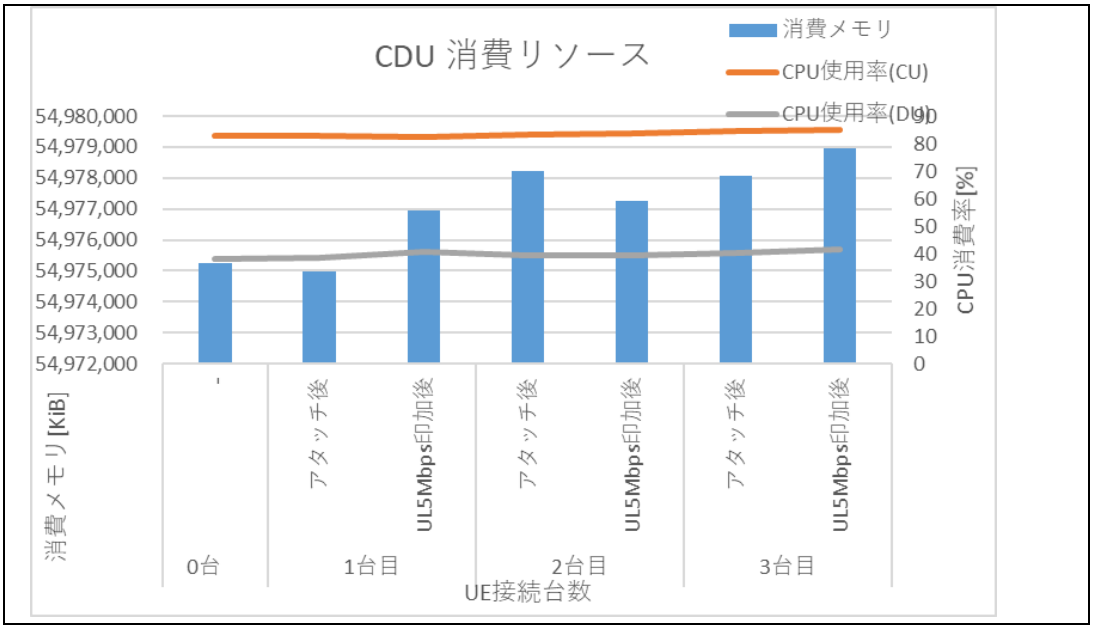


図 5-3-1-4-7　CDU 消費リソース推移（複数・センタ）

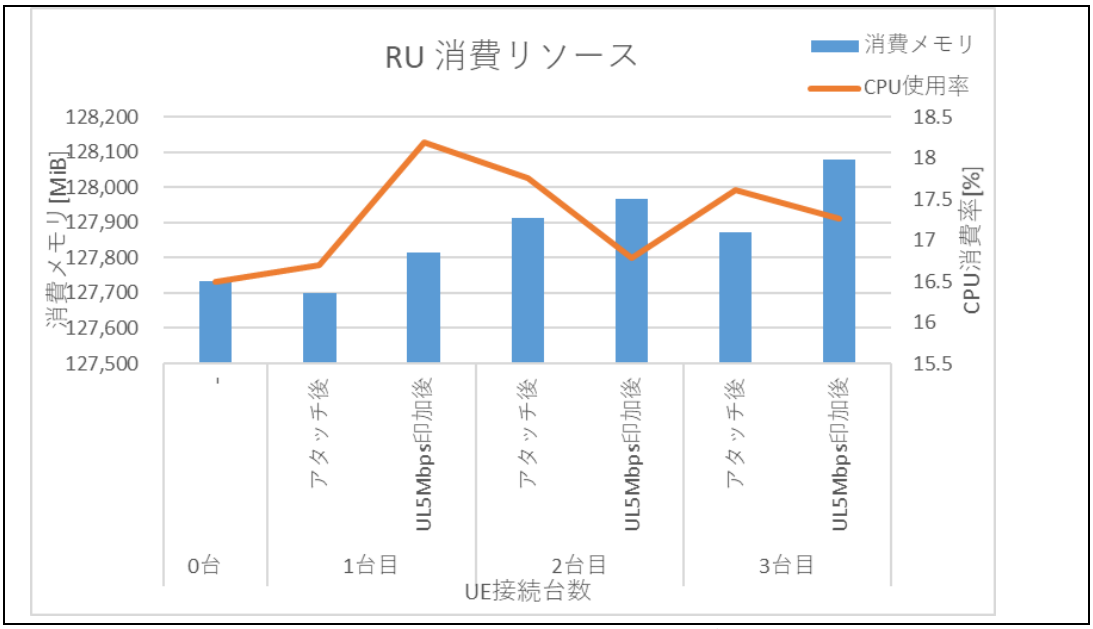


図 5-3-1-4-8　RU 消費リソース推移（複数・センタ）

表 5-3-1-4-4　UE1 台のデータ通信実行における消費リソースの偏移　（複数・センタ）

対象装置	UE1 台（UL5Mbps 印加）における消費リソースの偏移状況	
	消費メモリ	CPU 使用率
5GC	最大 約 4[MiB]の増加	増加傾向は見られない
UPF	増加傾向は見られない	増加傾向は見られない
CDU	最大 約 1,700[KiB]の増加	増加傾向は見られない

RU	最大 約 150[KB]の増加	増加傾向は見られない

CPU の消費リソースに関しては、UE 接続台数及び UL 通信の印加を増やすことによる大きな変化は見られませんでした。これは、各装置においてローカル５Ｇシステム環境の維持のためのノードやステータスの確認等の処理に伴う利用率が支配的であるため、これに比べると UE 接続数等での消費量が微量であり、結果、リソースの変動傾向が見られなかったと推定されます。

一方、メモリの消費リソースに関しては、5GC、CDU、RU において UE 接続台数及び UL 通信の印加に伴って増加する傾向が見られました。しかし、各システムにおける UE が接続していない状態（0 台）、つまり、ローカル５Ｇシステムにおける各ファンクション機能を維持するために必要な所要リソースが大きく、UE 接続に伴って増加するメモリ量は、システム維持のリソースと比べると微小であるため、本検証のシステムでは UE 台数による消費リソースの増加は大きな課題にならないと考察しました。

本検証で確認できた UE の接続限界数は、UL 伝送スループットの上限値に到達したため仕様上の限界数 7 台まで到達しておりませんが、UE1 台あたりに必要なリソースは軽微であり 7 台接続時も問題ないことが推定されます。よって、TDD 準同期①方式等、ローカル５Ｇ無線区間の UL 伝送比率を高めることで、UE の接続限界数を増やすことが可能です。

また、他のユースケース等において例えば、大容量通信を実施する場合や多数同時接続（100 台以上等）の状況においては、これに伴う消費リソースも増えることが想定されるため、各システムにおけるリソースの設計は留意が必要であると考えられます。

（イ） UE 接続台数の最大数検証

本検証で用いる CDU 装置における仕様上の UE の最大接続数は 7 台ですが、本実証環境での UE 接続限界数は、以下の結果となりました。

センタ拠点 UPF 時： 3 台

エンド拠点 UPF 時： 3 台

※TDD Configuration は「同期 TDD」を用いて検証

※各 UE は、UL5Mbps の印加を継続した状態で検証

※検証はそれぞれ 3 回実施し同一の結果となることを確認

エンド拠点 UPF 及びセンタ拠点 UPF 時、それぞれにおいて検証を行いましたが、UPF 設置拠点によって接続限界数の差異は生じませんでした。

UE 接続台数 3 台の状態では、UL：5Mbps × 3 = 計 15Mbps となり、同期 TDD 時の UL 最大スループット 22Mbps に対して余長がある状態と言えますが、UE4 台目を接続したことで、計 20Mbps ≒ 22Mbps（UL 最大スループット）となり、通信が不安定になったことでパケットロス及び制御信号の破綻によるデタッチが発生したと推定できます。

本結果より、複数台接続時の UL スループット総和値が、UL 最大スループットの近似値に到達すると接続不可が生じるため、ローカル５Ｇ無線区間の UL 伝送スループットの上限値に達したことが要因であると考えられます。ゆえに、準同期 TDD 方式を使用した場合は、UE 接続限界数が増加することが推測できます。

なお、本考察の裏付けのために、UE を接続（圏内/通信可能）させた状態で、UL5Mbps の印加を行わない状態で接続限界数を検証しました。結果、仕様通り 7 台まで接続が可能であり、7 台同時に ping 疎通状態を維持できることを確認しました。

その他の要因としてリソース（CPU やメモリの使用率）不足についても考察しましたが、本環境における 5GC や CDU のリソースは「ア.複数企業共用パターン（ア）消費リソースの検証」の結果に示すとおり UE 接続に伴う消費リソースに対して、システムが有するリソースは充足しているため要因ではありません。

上記の結果を踏まえて、UE 収容可能台数を推定して「表 5-3-1-4-5 UE 収容可能台数（複数)」にまとめました。

表 5-3-1-4-5 UE 収容可能台数（複数）

収容可能台数	根拠	考察
最大数７台 ※UE1 台あたりデータ通信 5Mbps 印加時は３台	・本製品の仕様によるものであり実際に接続し確認した ・最台数以内であっても UL 最大伝送スループット同等となる UE 数までしか収容できない	収容可能台数が接続限界数に到達しないのは、同期 TDD 方式の UL 最大伝送スループットが少ないことが要因。 UL：5Mbps 程度の通信を各 UE 側で実行する場合、その UE を収容したい台数に応じて TDD 準同期①方式に変更するのが望ましい。 最大伝送スループットの差異 TDD 同期：22Mbps TDD 準同期①：60Mbps

（ウ） UE 接続時間の検証

広域回線の区間長や拠点地域による影響を検証するため、各拠点での接続に要する時間と遅延値を測定しました。

表 5-3-1-4-6 接続に要する時間

エンド拠点	共用パターン	接続に要する時間 [s]	UE～センタ UPF 区間の遅延時間 [ms]	UE～エンド UPF 区間の遅延時間 [ms]
NTT 中央研修センタ	複数企業共用パターン	42	40	29
いすゞ自動車	複数企業共用パターン	42	40	28

接続に要する時間は、いずれも 42 秒程度であることが判明しました。広域回線の物理的な距離に応じて接続時間が変動していることも推定されますが、秒単位での差分は生じないことを確認しました。また、システム起動時等において 1 分以内に接続が完了することは実利用の観点から問題ないと考えられます。

遅延時間について、複数企業共用パターンでは、ベストエフォート型（SDN）の広域回線を使用しています。本実証では NTT 中央研修センタ及びいすゞ自動車の 2 拠点で使用しており、センタ拠点（東京都豊島区）からの物理的距離は比較的近い距離になりますが、センタ UPF とエンド UPF における遅延時間が 10ms 程度確認できました。

（エ） UE～UPF 間の通信性能の検証

UPF 設置位置の違いによる伝送遅延時間及び伝送スループットを検証しました。

i. UE1 台を接続した状態における UL 最大伝送スループット

同期 TDD 時の UL 最大スループット： 22Mbps
準同期 TDD 時の UL 最大スループット： 60Mbps
※UL 変調方式は、MCS9（QPSK 方式）に固定し測定

ii. UE を複数台接続しデータ通信を疑似的に印加した際の性能（TDD 同期方式）

表 5-3-1-4-7 スループット（複数・エンド）

台数	エンド拠点UPF				
	ULスループット [Mbps]	DLスループット [Mbps]	ULパケット損 [Loss]	DLパケット損 [Loss]	遅延時間 [msec]
1台目	4.99	5.00	0.12	0.01	35
2台目	4.90	5.00	2.00	0.13	36
3台目	4.98	5.00	0.40	0.00	32

※伝送スループットは DL/UL ともに 5Mbps 印加時の測定結果
※4 台目を接続し UL を印加（UL 総和 20Mbps）すると、全 UE の通信が破綻

表 5-3-1-4-8 スループット（複数・センタ）

台数	センタ拠点UPF				
	ULスループット [Mbps]	DLスループット [Mbps]	ULパケット損 [Loss]	DLパケット損 [Loss]	遅延時間 [msec]
1台目	5.00	5.00	0.01	0.20	40
2台目	4.96	5.00	0.72	0.02	44
3台目	5.00	5.00	0.01	0.01	43

※伝送スループットは DL/UL ともに 5Mbps 印加時の測定結果
※4 台目を接続し UL を印加（UL 総和 20Mbps）すると、全 UE の通信が破綻

本実証結果より、UL 総和:20Mbps 程度で通信断が発生することが分かりました。
これは UE1 台における同期 TDD 時の UL 最大スループット（22Mbps）とほぼ同等であるため、複数台の UE が同時に UL 通信を実施した場合、複数台の UE による UL スループットの総和は、1 台の UE における UL 最大スループットと同等となる結果と言えます。
また、伝送遅延時間に関して、センタ拠点 UPF 時はエンド拠点 UPF 時と比較して、約 5ms～11ms の遅延時間が劣化していることを確認しました。複数企業共用パターンでは拠点間の広域回線にベストエフォート側回線（SDN）を敷設しており、この広域回線における伝送遅延となります。
本検証は、エンド拠点（東京都調布市）、センタ拠点（東京都豊島区）にて計測を実施

しており、この区間長に伴うのSDN回線による伝送遅延時間と考えられるため、同様のSDN回線を使用した場合でも、区間長が異なれば伝送遅延時間も差分が生じることが推定されます。

センタ拠点UPFの場合は広域回線の距離によって遅延時間の劣化が生じる可能性を確認しましたが、専用線やギャランティ回線等、回線種別が異なれば、遅延時間への影響も差分が生じると想定されます。本検証において確認した遅延時間に関しては、「④－ウ考察」で結果をまとめています。

イ 業界共用パターン

（ア） 消費リソースの検証

i. エンド拠点 UPF 時

UE の接続台数を増加させ、リソースの推移を測定しました。結果は下記の表 5-3-1-4-9～5-3-1-4-10、図 5-3-1-4-9～5-3-1-4-12 のとおりです。

表 5-3-1-4-9 業界共用・エンド UPF 時接続リソース

台数/通信状態		5GC		UPF		CDU			RU	
		消費CPU [%]	消費メモリ [MiB]	消費CPU [%]	消費メモリ [MiB]	消費CPU(CU) [%]	消費CPU(DU) [%]	消費メモリ [KiB]	消費CPU [%]	消費メモリ [KB]
0台	-	1	456.1	100	366.3	82.17	38.19	55,007,532	17.37	127,732
1台目	アタッチ後	0.7	457.4	100	368.2	82.48	38.3	55,009,334	17.86	127,701
	UL5Mbps印加後	0.9	459.9	99.3	368.3	82.14	39.41	55,013,658	17.72	127,815
2台目	アタッチ後	1	461.0	100	374.2	82.53	39.35	55,016,818	17.79	127,912
	UL5Mbps印加後	1	461.5	99.4	374.6	83.52	40.48	55,016,773	16.64	127,968
3台目	アタッチ後	1	463.5	100	374.8	84.44	41.11	55,025,356	15.76	127,871
	UL5Mbps印加後	0.3	464.5	100	375.1	84.12	41.66	55,026,459	16.74	128,079

※「消費 CPU」はシステム総和に対する使用率で示す

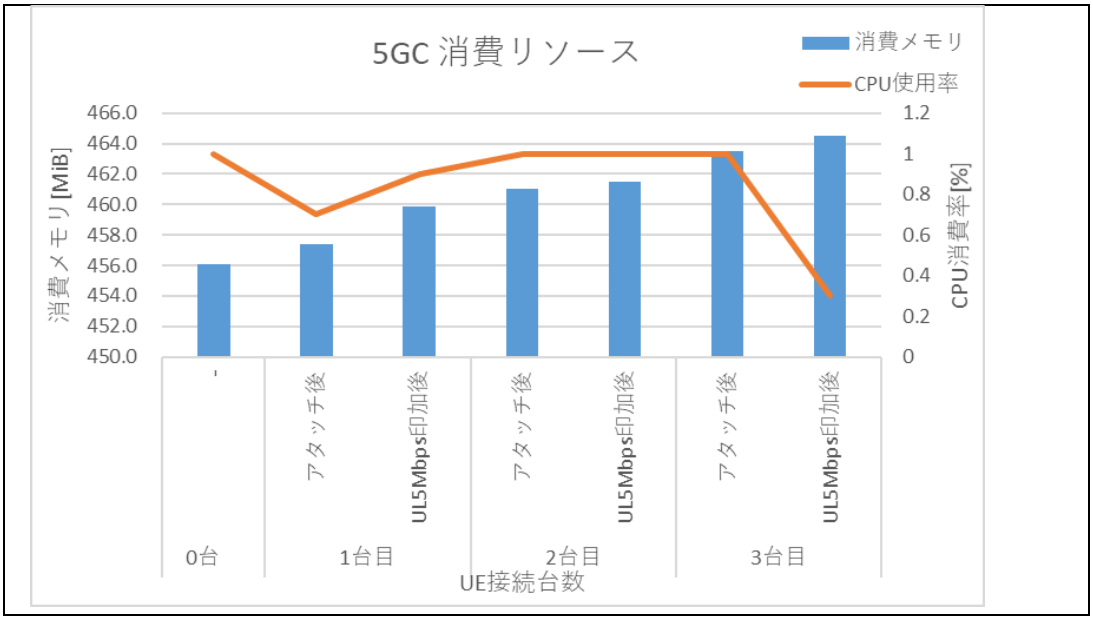


図 5-3-1-4-9 5GC 消費リソース推移（業界・エンド）

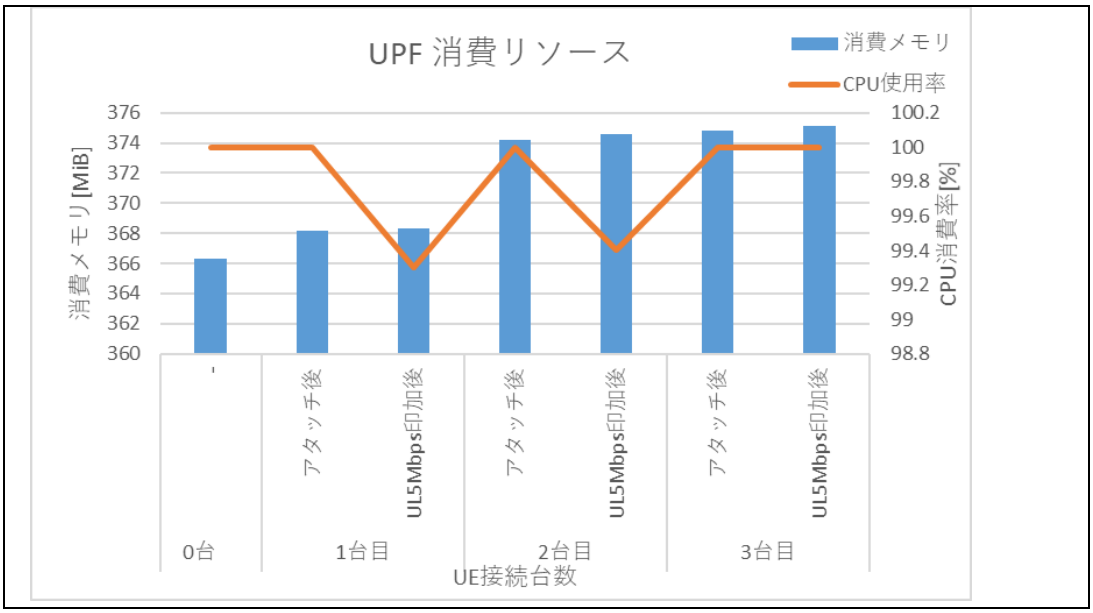


図 5-3-1-4-10　UPF 消費リソース推移（業界・エンド）

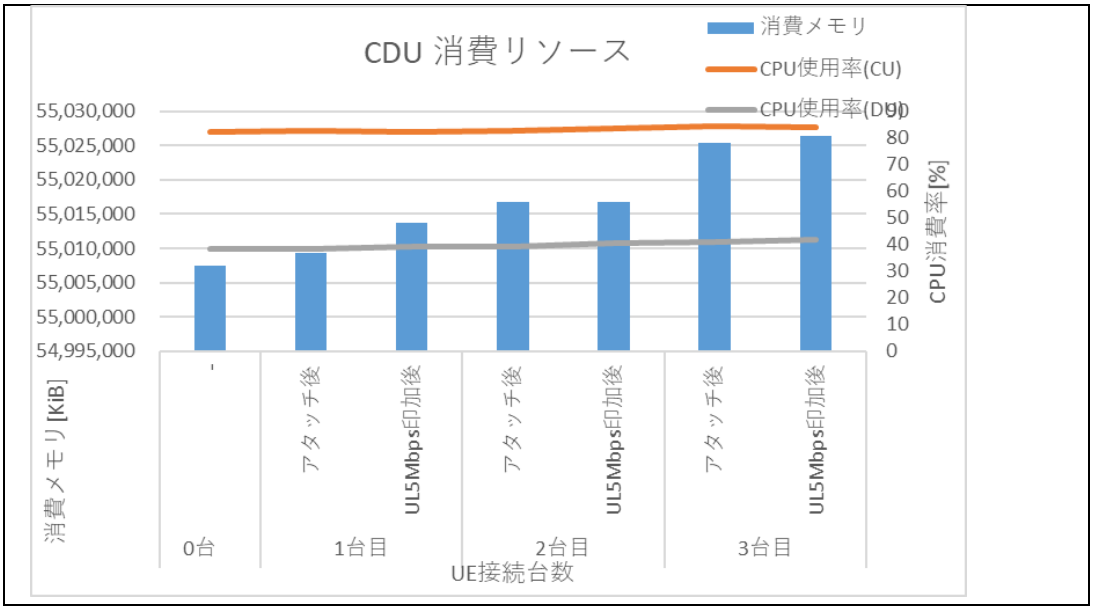


図 5-3-1-4-11　CDU 消費リソース推移（業界・エンド）

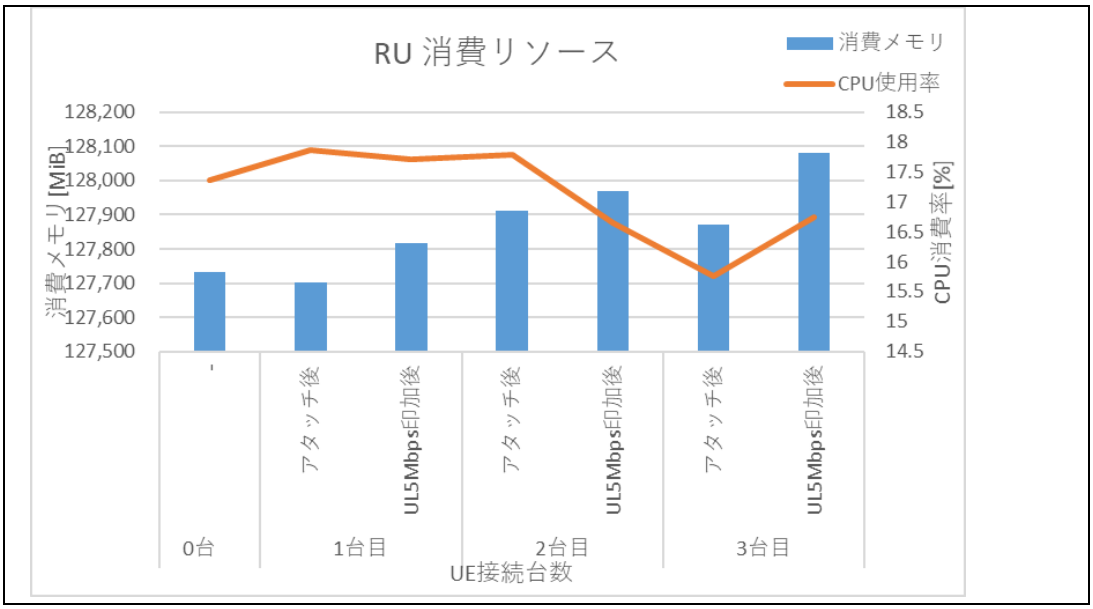


図 5-3-1-4-12　RU 消費リソース推移（業界・エンド）

表 5-3-1-4-10 UE1 台のデータ通信実行における消費リソースの偏移　（業界・エンド）

対象装置	UE1 台（UL5Mbps 印加）における消費リソースの偏移状況	
	消費メモリ	CPU 使用率
5GC	最大 約 4[MiB]の増加	増加傾向は見られない
UPF	最大 約 7[MiB]の増加	増加傾向は見られない
CDU	最大 約 10,000[KiB]の増加	増加傾向は見られない
RU	最大 約 150[KB]の増加	増加傾向は見られない

ii.　　センタ拠点 UPF 時

UE の接続台数を増加させ、リソースの推移を測定しました。結果は下記の表 5-3-1-4-11～5-3-1-4-12、図 5-3-1-4-13～5-3-1-4-16 のとおりです。

表 5-3-1-4-11　業界共用・センタ UPF 時接続リソース

台数/通信状態		5GC		UPF		CDU			RU	
		消費CPU [%]	消費メモリ [MiB]	消費CPU [%]	消費メモリ [%]	消費CPU(CU) [%]	消費CPU(DU) [%]	消費メモリ [KiB]	消費CPU [%]	消費メモリ [KB]
0台	-	0.7	448.72	0.3	0.5	82.2	38.91	54,916,696	16.98	127,732
1台目	アタッチ後	0.7	464.19	0	0.5	82.76	38.32	54,952,118	17.55	127,701
	UL5Mbps印加後	0.6	465.94	0.6	0.5	83.06	38.59	54,955,948	16.95	127,815
2台目	アタッチ後	1.3	467.84	0.3	0.5	83.88	39.8	54,959,286	16.35	127,912
	UL5Mbps印加後	0.3	468.33	0	0.5	83.65	40.7	54,960,796	16.75	127,968
3台目	アタッチ後	0.9	470.37	0.3	0.5	83.8	40.14	54,968,306	17.17	127,871
	UL5Mbps印加後	1	473.65	0.3	0.5	84.31	40.83	54,970,362	16.51	128,079

※「消費 CPU」はシステム総和に対する使用率で示す

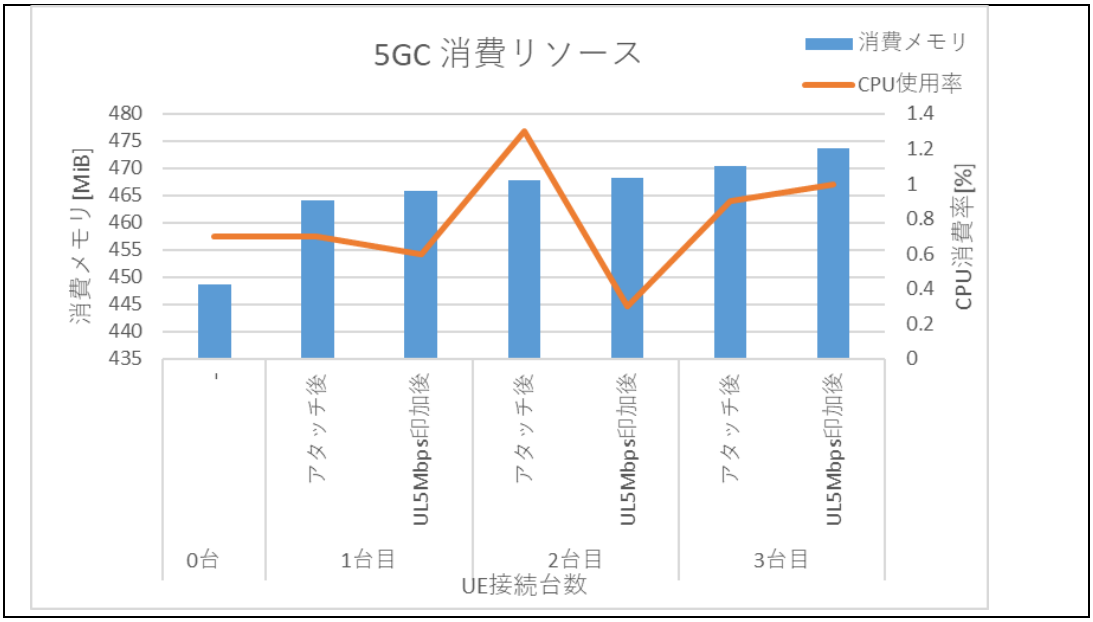


図 5-3-1-4-13　5GC 消費リソース推移（業界・センタ）

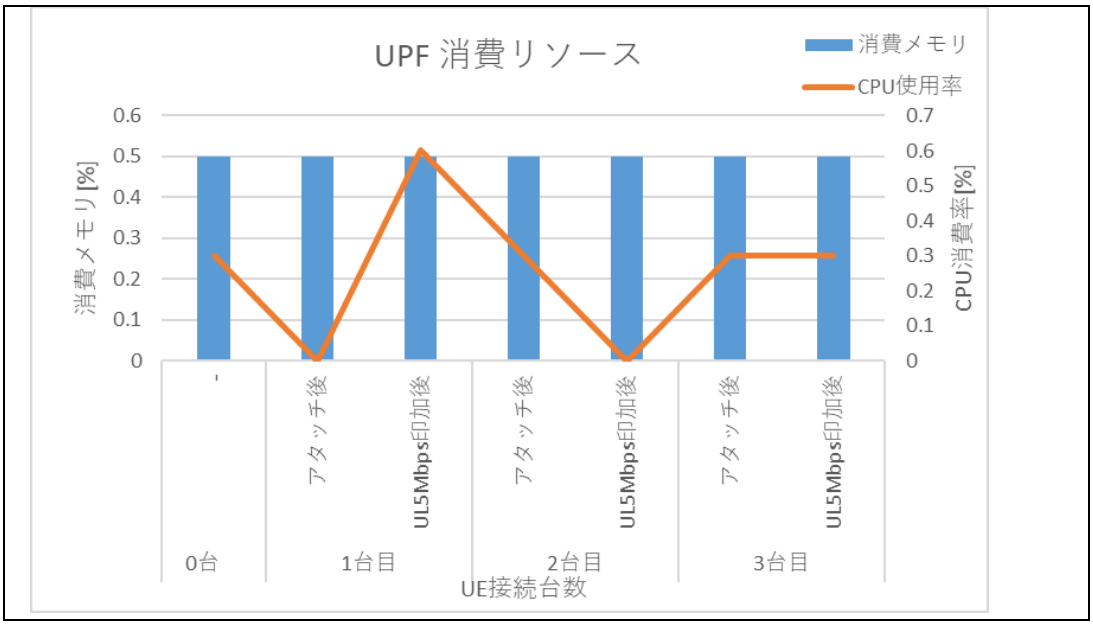


図 5-3-1-4-14　UPF 消費リソース推移（業界・センタ）

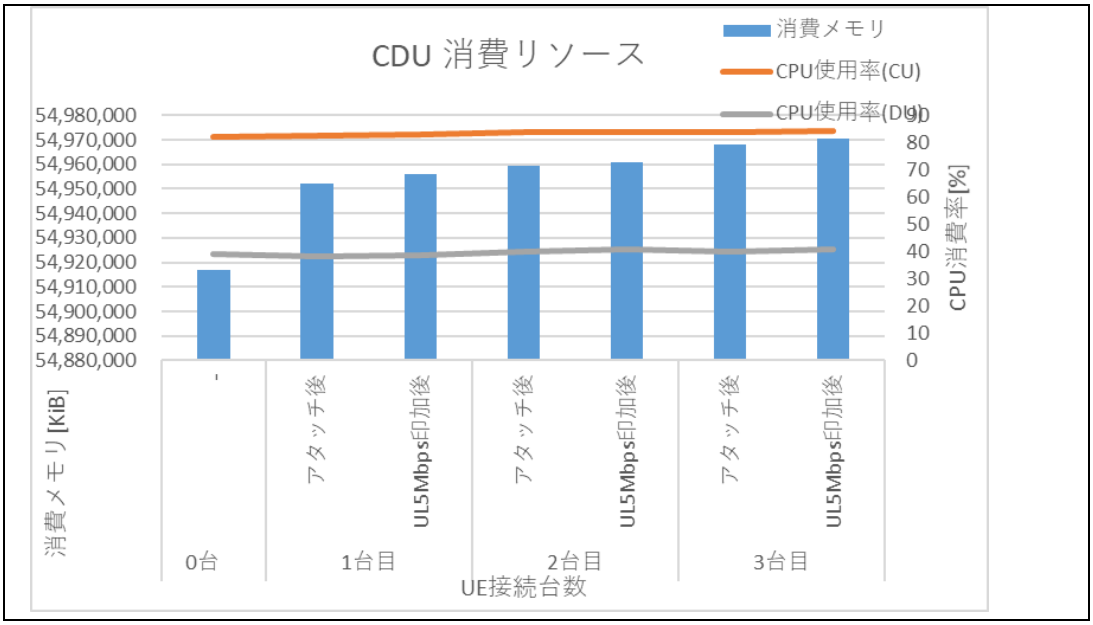


図 5-3-1-4-15　CDU 消費リソース推移（業界・センタ）

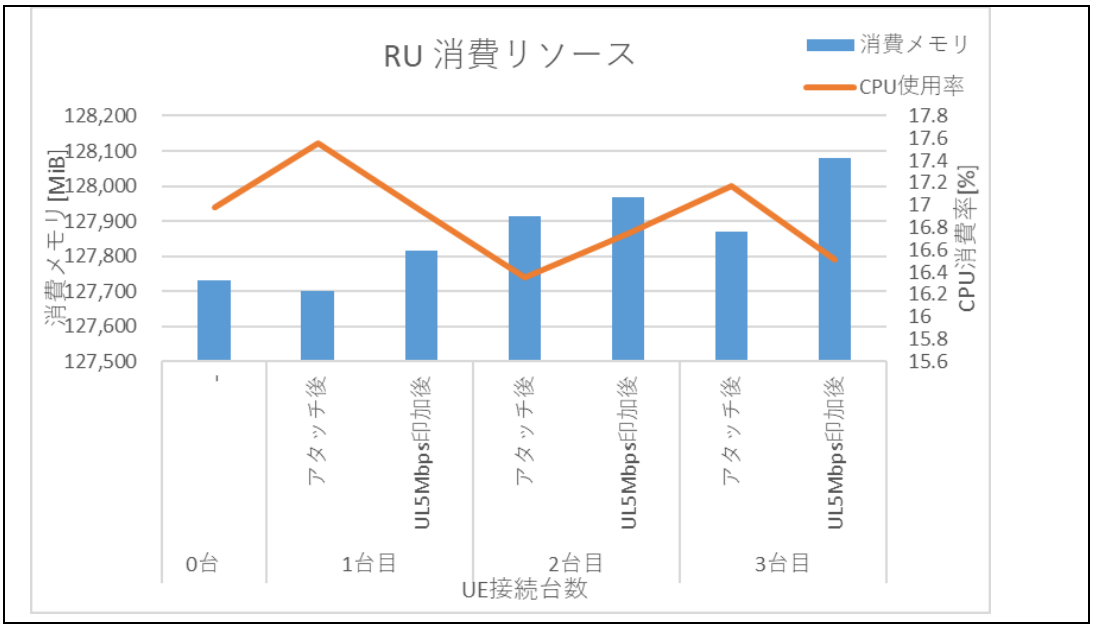


図 5-3-1-4-16　RU 消費リソース推移（業界・センタ）

表 5-3-1-4-12 UE1 台のデータ通信実行における消費リソースの偏移　（業界・センタ）

対象装置	UE1 台（UL5Mbps 印加）における消費リソースの偏移状況	
	消費メモリ	CPU 使用率
5GC	最大 約 18[MiB]の増加	増加傾向は見られない
UPF	増加傾向は見られない	増加傾向は見られない
CDU	最大 約 40,000[KiB]の増加	増加傾向は見られない
RU	最大 約 150[KB]の増加	増加傾向は見られない

CPU の消費リソースに関しては、UE 接続台数及び UL 通信の印加を増やすことで大きな変化は見られませんでした。これは、各装置においてローカル５Ｇシステム環境の維持のためのノードやステータスの確認等の処理に伴う利用率が支配的であるため、これに比べると UE 接続数等での消費量が微量であるため、結果、リソースの変動傾向が見られなかったと推定されます。

一方、メモリの消費リソースに関しては、5GC、CDU、RU において UE 接続台数及び UL 通信の印加に伴って増加する傾向が見られました。しかし、各システムにおける UE が接続していない状態（0 台）、つまり、ローカル５Ｇシステムで担うファンクション機能を維持するために必要な所要リソースが大きく、UE 接続に伴って増加するメモリ量は所要リソースと比べると微小であるため、本検証システムでは大きな課題等は生じないと判断しました。

本検証で確認できたUEの接続限界数は、UL伝送スループットの上限値に到達したため仕様上の限界数7台まで到達しておりませんが、UE1台あたりに必要なリソースは軽微であるため7台接続時も問題ないことが推定されますので、TDD準同期①方式等、ローカル５Ｇ無線区間のUL伝送比率を高めることで、UEの接続限界数を増やすことが可能です。

また、他のユースケース等において例えば、大容量通信を実施する場合や多数同時接続（100台以上等）の状況においては、これに伴う消費リソースも増えることが想定されるため、各システムにおけるリソースの設計は留意が必要であると考えられます。

（イ） UE 接続台数の最大数検証

業界共用パターンにおける UE 接続限界数は以下の結果でした。

センタ拠点 UPF 時： 3 台

エンド拠点 UPF 時： 3 台

※TDD Configuration は「同期 TDD」を用いて検証

※各 UE は、UL5Mbps の印加を継続した状態で検証

※検証はそれぞれ 3 回実施し同一の結果となることを確認

エンド拠点 UPF 及びセンタ拠点 UPF 時、それぞれにおいて検証を行ったところ、複数企業共用パターンと同様に、接続可能台数は 3 台という結果でした。

UE 接続台数 3 台の状態では、UL：5Mbps × 3 = 計 15Mbps となり、同期 TDD 時の UL 最大スループット 23Mbps に対して余長がある状態と言えますが、UE4 台目を接続したことで、計 20Mbps ≒ 23Mbps（UL 最大スループット）となり、通信が不安定になったことでパケットロス及び制御信号の破綻によるデタッチが発生したと推定できます。

本結果より、複数台接続時の UL スループット総和値が、UL 最大スループットの近似値に到達すると接続不可が生じるため、ローカル５Ｇ無線区間の UL 伝送スループットの上限値に達したことが要因であると考えられます。ゆえに、準同期 TDD 方式を使用した場合は、UL 最大スループット 59Mbps となるため、UE 接続限界数が増加することが推測できます。

なお、本考察の裏付けのために、UE を接続（圏内/通信可能）させた状態で、UL5Mbps の印加を行わない状態で接続限界数を検証しました。結果、仕様通り 7 台まで接続が可能であり、7 台同時に ping 疎通状態を維持できることを確認しました。

その他の要因としてリソース（CPU やメモリの使用率）不足についても考察しましたが、本環境における 5GC や CDU のリソースは「イ.業界共用パターン（ア）UE 接続リソース」の結果に示すとおり UE 接続に伴う消費リソースに対して、システムが有するリソースは充足しているため要因ではありません。

上記の結果を踏まえて、UE 収容可能台数を推定して「表 5-3-1-4-13 UE 収容可能台数（業界)」にまとめました。

表 5-3-1-4-13 UE 収容可能台数（業界）

収容可能台数	根拠	考察
最大数７台 ※UE1 台あたりデータ通信 5Mbps 印加時は３台	・本製品の仕様によるものであり実際に接続し確認した ・最台数以内であっても UL 最大伝送スループット同等となる UE 数までしか収容できない	収容可能台数が接続限界数に到達しないのは、同期 TDD 方式の UL 最大伝送スループットが少ないことが要因。 UL：5Mbps 程度の通信を各 UE 側で実行する場合、その UE を収容したい台数に応じて TDD 準同期①方式に変更するのが望ましい。 最大伝送スループットの差異 TDD 同期：23Mbps TDD 準同期①：59Mbps

（ウ） UE 接続時間の検証

広域回線の区間長や拠点地域による影響を検証するため、各拠点での接続に要する時間と遅延値を測定しました。

表 5-3-1-4-14 接続に要する時間

エンド拠点	共用パターン	接続に要する時間 [s]	UE～センタ UPF 区間の遅延時間 [ms]	UE～エンド UPF 区間の遅延時間 [ms]
NTT 中央研修センタ	業界共用パターン	42	33	32
東北大学	業界共用パターン	42	36	28
東京大学	業界共用パターン	41	37	28
京都大学	業界共用パターン	42	41	32

接続に要する時間は、41～42 秒程度であることが判明しました。広域回線の物理的な距離に応じて接続時間が変動していることも推定されますが、秒単位での差分は生じないことを確認しました。また、システム起動時等において 1 分以内に接続が完了することは実利用の観点から問題ないと考えられます。

遅延時間について、業界共用パターンはギャランティ型（ビジネスイーサワイド）の広域回線を使用しました。本実証では NTT 中央研修センタ、東北大学、東京大学、京都大学の 4 拠点で使用しています。センタ拠点 UPF 時とエンド拠点 UPF 時における遅延時間の差分は、1ms～9ms となり、物理的な距離による遅延時間劣化の相関は確認できませんでした。この結果は、物理的距離以外にも広域回線の構造や交換装置等も影響していると想定されるため、あくまで参考値であり導入に際しては設計等を詳細に検討することを推奨します。

NTT 中央研修センタについて本結果と「ア複数企業共用パターン(ウ)UE 接続時間の検証」の結果と比較すると、センタ拠点 UPF 時とエンド拠点 UPF 時の遅延時間の差分は、ベストエフォート型が 11ms、ギャランティ型が 1ms となり、回線の帯域向上によって遅延時間の改善が可能であることが確認できました。

（エ） UE～UPF 間の通信性能の検証

UPF 設置位置の違いによる伝送遅延時間及び伝送スループットを検証しました。

i. UE1 台を接続した状態における UL 最大伝送スループット

同期 TDD 時の UL 最大スループット： 23Mbps
準同期 TDD 時の UL 最大スループット： 59Mbps
※UL 変調方式は、MCS9（QPSK 方式）に固定し測定

ii. UE を複数台接続しデータ通信を疑似的に印加した際の性能（TDD 同期方式）

表 5-3-1-4-15 スループット（業界・エンド）

台数	エンド拠点UPF				
	ULスループット [Mbps]	DLスループット [Mbps]	ULパケット損 [Loss]	DLパケット損 [Loss]	遅延時間 [msec]
1台目	5.00	5.00	0.10	0.00	35
2台目	5.00	5.00	0.30	0.00	34
3台目	4.97	5.00	0.66	0.00	38

※伝送スループットは DL/UL ともに 5Mbps 印加時の測定結果
※４台目を接続し UL を印加（UL 総和 20Mbps）すると、全 UE の通信が破綻

表 5-3-1-4-16 スループット（業界・センタ）

台数	センタ拠点UPF				
	ULスループット [Mbps]	DLスループット [Mbps]	ULパケット損 [Loss]	DLパケット損 [Loss]	遅延時間 [msec]
1台目	5.00	5.00	0.01	0.05	33
2台目	4.99	5.00	0.09	0.00	34
3台目	4.93	5.00	1.40	0.04	39

※伝送スループットは DL/UL ともに 5Mbps 印加時の測定結果
※4 台目を接続し UL を印加（UL 総和 20Mbps）すると、全 UE の通信が破綻

本実証結果より、UL 総和:20Mbps 程度で通信断が発生することが分かりました。
これは UE1 台における同期 TDD 時の UL 最大スループット（22Mbps）とほぼ同等であるため、複数台の UE が同時間軸で UL 通信を実施した場合、複数台の UE による総和と UL 最大スループットは同等となる結果と言えます。

また、伝送遅延時間に関して、センタ拠点 UPF 時とエンド拠点 UPF 時を比較しましたが、遅延時間に差異は生じませんでした。これは、業界共用パターンでは拠点間の広域回線にギャランティ型回線（ビジネスイーサワイド）を敷設しており、ベストエフォート型回線と比較して通信性能が高く、距離による伝送遅延が軽微であるためと考えられます。

本検証結果は、エンド拠点（東京都調布市）、センタ拠点（東京都豊島区）にて計測を実施したものであるため、この区間長が伸びた場合は伝送遅延が劣化する可能性もあります。本検証において確認した遅延時間に関しては、「④－ウ考察」で結果をまとめています。

ウ　考察

消費リソースについて、CPU とメモリはエンド拠点 UPF とセンタ拠点 UPF では大きな違いはありませんでした。複数企業共用と業界共用の両パターンで結果に差は見られませんでしたので、広域回線の性能や距離による影響はないと考えられます。また、1 台の UE がデータ通信を実施する際の消費メモリに関しては、導入するコア共用形態において、UE の接続想定数やデータ通信量を鑑みて適切に設計することが重要だと考えます。

伝送スループットに関して、エンド拠点 UPF とセンタ拠点 UPF では変化はありませんでした。本実証で使用するユースケースでは、UL 伝送スループット 15Mbps 程度が所要性能であったため、同期 TDD 方式で問題なく実証を行えました。(ユースケース実証の結果については 6 章に記載)

他のユースケース等では UL 伝送スループットの所要性能が高いものもあることが想定され、本実証で使用した無線機等のスペックでは満たせないことも考えられますが、ユースケースの所要性能に見合った無線機の採用や、準同期 TDD 方式を用いることでコア共用環境でのローカル５Ｇシステムの構築が実現可能であると考えられます。

一方、伝送遅延時間に関しては、複数企業共用パターンの地上回線（SDN/ベストエフォート型）及び業界共用パターンの地上回線（ビジネスイーサワイド/ギャランティ型）の回線種別と物理的な距離が影響することを確認しました。本実証環境である、近畿地方・関東地方・東北地方を結ぶコア共用モデルにおいては、遅延時間の計測値は実用に問題ないことを確認しました。しかし、伝送スループットと同様にユースケースによっては遅延時間の所要性能が厳しいことも想定されます。例えば、重機や建機の遠隔操縦等のユースケースが該当します。その場合の改善策として、広帯域回線の敷設やエンド UPF 構成（MEC）による遅延時間の短縮が有効的であると推定できます。また、ネットワークスライス等の技術を実装する解決法も考えられますので、今後の検証等に期待します。

UE の同時接続に関して、UE の接続台数を増やした場合でも、UL 伝送スループットはローカル５Ｇ区間の最大伝送スループット相当となることを確認しました。この結果については、gNB 製品の性能等に左右されるものと考えられます。本実証で使用した A 社製の gNB は、無線区間の DL/UL 回線性能を複数台の UE でシェアする場合、複数台 UE の伝送スループットの総和は、無線区間の総和の伝送スループット相当となる仕様であったため、当該結果が得られています。コアの共用環境下においても、共用しない環境と同様に、最大伝送スループット相当の複数台 UE の同時通信が可能であることが確認できました。そのため、コア共用環境において各拠点におけるローカル５Ｇの所要伝送スループットに見合った無線設備を選定することで、コア共用環境下においても問題なく実用できます。

接続時間に関して、UE 起動から 1 分以内での接続を確認できており、コア共用環境下においてもシステム起動時のストレスは高くないことが確認できました。

NTT 中央研修センタでは、同一拠点間においてベストエフォート型とギャランティ型それぞれの遅延時間を検証しました。回線種別以外は同一条件下において計測したところ、センタ拠点 UPF 時とエンド拠点 UPF 時の遅延時間の差分は、ベストエフォート型が 11ms、ギャランティ型が 1ms となり、回線の帯域向上によって遅延時間の改善が可能であることが確認できました。

(2)　　コアの共用における機能検証

①　検証目標

コアを共用する際、接続企業等の利用ユーザーに関する SIM 認証情報や在圏情報等の顧客管理機能の実用性を検証し、コア共用の実現に向けた課題や実装が必要とされる機能等を整理し報告書にまとめます。

②　評価・検証項目

ローカル５Ｇシステムの管理機能について、コアの共用環境下において複数の拠点で異なる企業や団体が利用する状況において、管理・運営に関する各機能の実装状況を確認し、必要と考えられる機能を考察しました。

また、ユーザーや UE 端末単位での UPF の指定制御の実用性について検証しました。対象とした管理機能と説明は以下となります。

- 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。

- 端末認証機能（AUSF）
  Authentication Server Function
  UE 認証の機能を担います。

- 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。

- 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。

上記の各ファンクションに従い、本検証での評価・検証項目は、以下の「表 5-3-2-2-1　評価・検証項目」のとおりです。

表 5-3-2-2-1 評価・検証項目

大項目	中項目	小項目	検証概要	検証項目
機能検証	機能確認	複数企業共用パターン	コア装置内の管理機能やログ情報の実装状況を確認	SIM 認証の管理状況
				端末認証の管理状況
				ポリシーの管理状況
				セッション管理の管理状況
				在圏情報の管理状況
				ログの蓄積、管理状況
				管理権限の設定状況
	アクセス確認	複数企業共用パターン	コア配下における、UE 個別の UPF 指定・制御	UE 別 UPF アクセス検証
		業界共用パターン	コア配下における、UE 個別の UPF 指定・制御	UE 別 UPF アクセス検証

③　評価・検証方法

本検証で用いる測定ツールは、以下の「表 5-3-2-3-1　測定ツール」のとおりです。

表 5-3-2-3-1　測定ツール

項目	測定内容および具体的なツール
測定ツール	伝送スループット：iperf 等の測定ツール
	伝送疎通試験：ping 試験
	Linux コマンド等

本検証の手順及び検証イメージは、以下の表 5-3-2-3-2～表 5-3-2-3-4 及び図 5-3-2-3-1～図 5-3-2-3-4 のとおりです。

なお、「表 5-3-2-3-2　検証手順」については「複数企業共用パターン」と「業界共用パターン」において差分はないため、業界共用パターンの記載は割愛します。

表 5-3-2-3-2 検証手順

項番	実施内容	対応図表
機機複-1	SIM 認証情報の格納状況、閲覧権限の設定の可否を確認	―
機機複-2	端末情報の格納状況、閲覧権限の設定の可否を確認	―
機機複-3	ポリシー情報の格納状況、閲覧権限の設定の可否を確認	―
機機複-4	セッション管理情報の格納状況、閲覧権限の設定の可否を確認	―
機機複-5	在圏情報の格納状況、閲覧権限の設定の可否を確認	―
機機複-6	ログの蓄積、格納状況、閲覧権限の設定の可否を確認	―
機機複-7	その他格納されているログ情報の内容を確認	―

表 5-3-2-3-3 検証手順

項番	実施内容	対応図表
機ア複-1	UE1 は UPF1 を経由する設定	図 5-3-2-3-1
機ア複-2	UE2 は UPF2 を経由する設定	図 5-3-2-3-1
機ア複-3	UE1 は PC-A へアクセスできること、PC-B へアクセスできないことを確認	図 5-3-2-3-2
機ア複-4	UE2 は PC-B へアクセスできること、PC-A へアクセスできないことを確認	図 5-3-2-3-2
機ア複-5	UE1 と UE2 のアクセスしたログが同一コア内でどのように格納され、分離して管理可能か確認	―

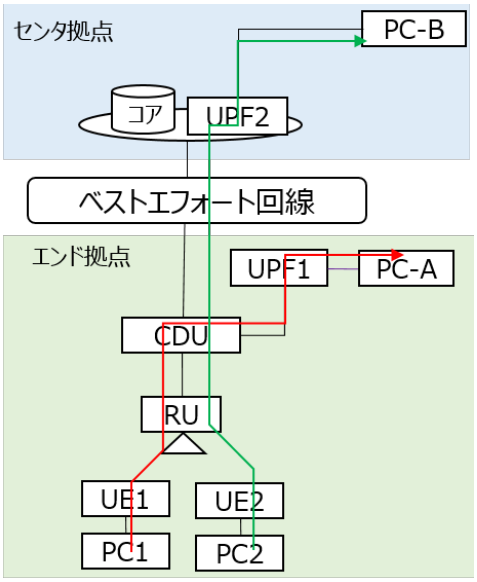


図 5-3-2-3-1　検証イメージ

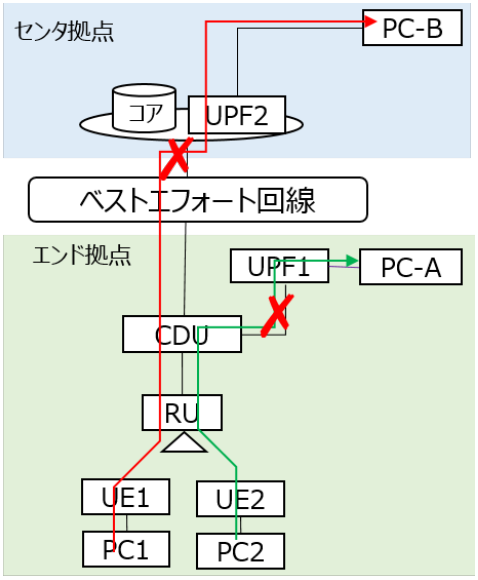


図 5-3-2-3-2　検証イメージ

表 5-3-2-3-4 検証手順

項番	実施内容	対応図表
機ア業-1	UE1 は UPF1 を経由する設定	図 5-3-2-3-3
機ア業-2	UE2 は UPF2 を経由する設定	図 5-3-2-3-3
機ア業-3	UE1 は PC-A へアクセスできること、PC-B へアクセスできないことを確認	図 5-3-2-3-4
機ア業-4	UE2 は PC-B へアクセスできること、PC-A へアクセスできないことを確認	図 5-3-2-3-4
機ア業-5	UE1 と UE2 のアクセスしたログが同一コア内でどのように格納され、分離して管理可能か確認	―

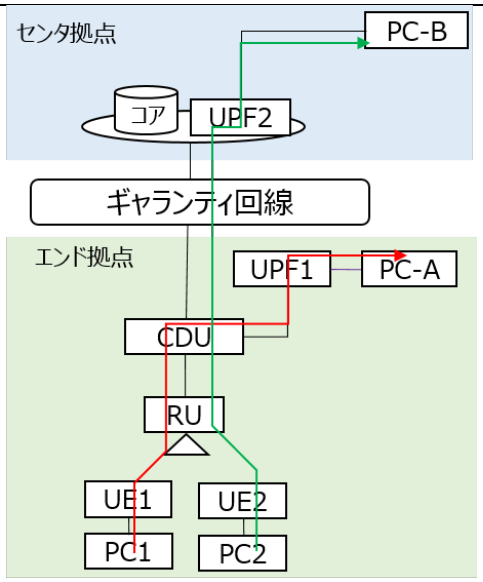


図 5-3-2-3-3　検証イメージ

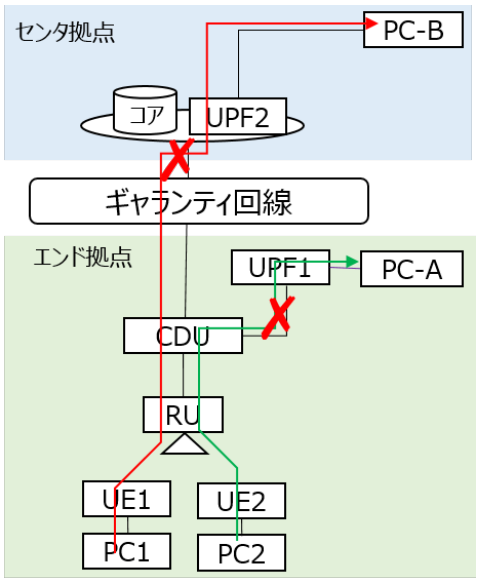


図 5-3-2-3-4　検証イメージ

④　結果

ア 機能検証

コアを共用する際に、各拠点でどの程度情報が管理可能なのかを把握するべく下記機能のログや設定状況を検証しました。

※後述する（ア）～（オ）の検証項目は、共用パターン（複数企業/業界）による差が生じないため、代表して「複数企業共用パターン」で実施

(ア)SIM 認証情報の格納状況、各種の閲覧権限の設定

A 社のコアに SIM 情報を登録する際は「図 5-3-2-4-1　A 社　ログイン画面」のようなWebGUI 画面を通って実行することができます。Username とパスワードを設定しログインする設計であり、この Username 及びパスワードを複数登録し、拠点毎の SIM 情報や端末情報等の閲覧管理を実行可能であることを確認しました。

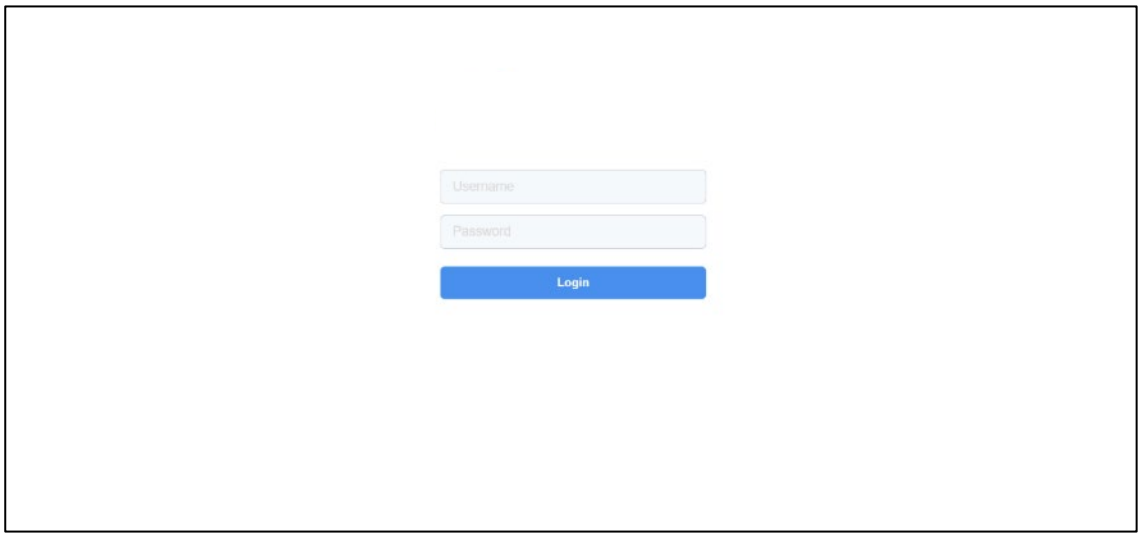


図 5-3-2-4-1　A 社　ログイン画面

下記のように Username とパスワードを設定しログインします。

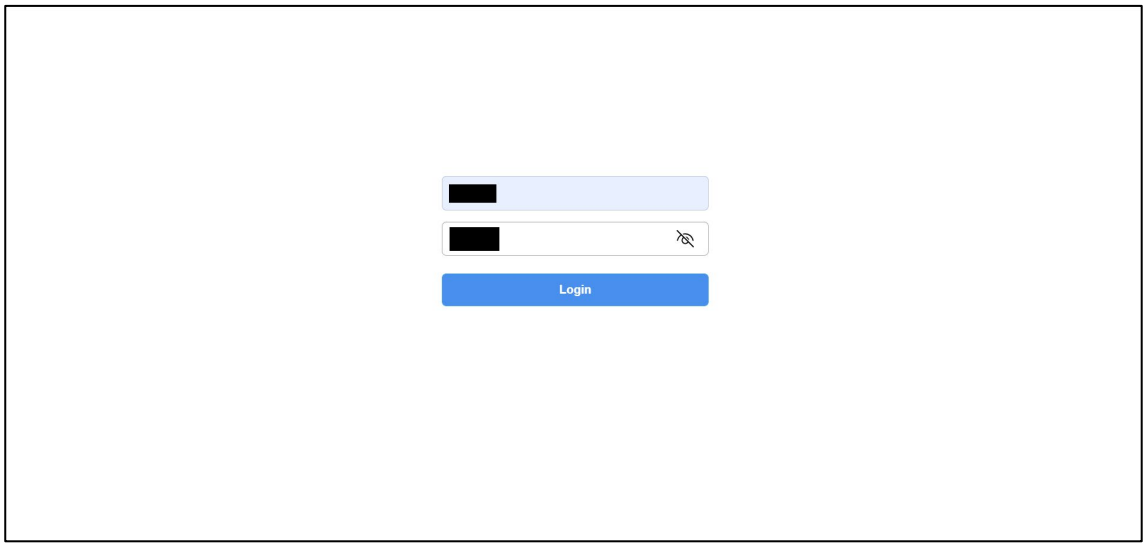


図 5-3-2-4-2　A 社　ログイン画面　ログインパスワードあり

SIM の登録は、WebGUI 上に準備されたメニューSUBSCRIBERS に情報が格納されます。SIM 情報の新規登録、登録されている SIM 情報の確認を当該メニューで実行可能です。

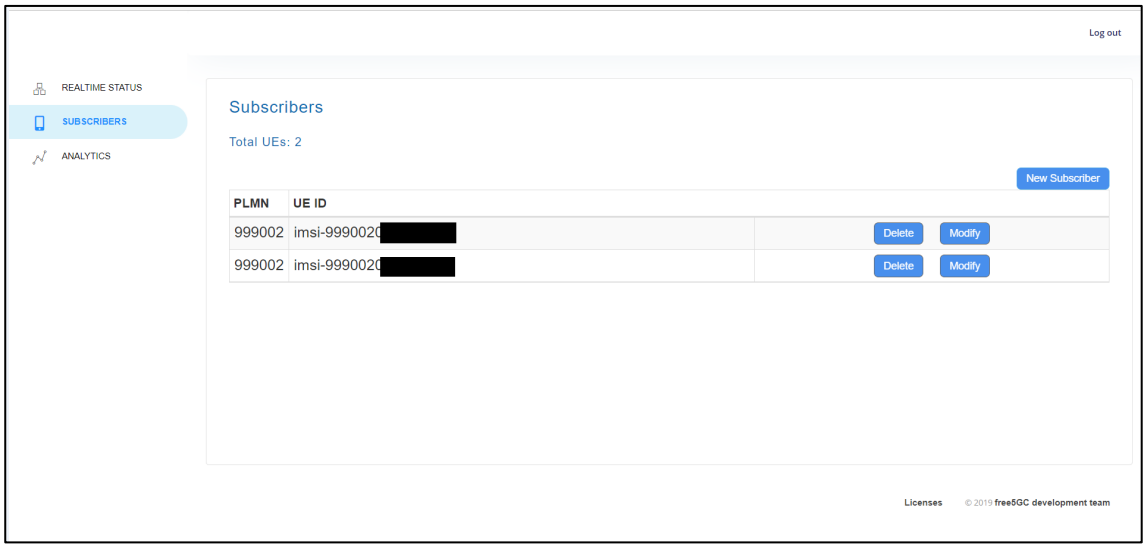


図 5-3-2-4-3　A 社　WebGUI SIM subscribes

登録した SIM 情報は、SUBSCRIBERS のメイン画面に UE ID（IMSI 情報）が表示され確認できます。このとき、拠点毎にログイン情報を分けて管理した場合、該当拠点で使用可能な SIM 情報のみ閲覧管理できるため、マルチテナントによる各企業の SIM 情報等の漏洩は生じません。

(イ)端末情報の格納状況

端末がコアに接続されたかどうかは、WebGUI 上の REALTIME STATUS にて確認することができます。基地局に接続できていない場合は「IDLE」と表示され、接続できている場合は「CONNECTED」と表示されます。この仕組みを用いることで、現在利用中（通信中）の端末と休止中（または接続が切れた等の不通状態）の端末を確認することが可能です。

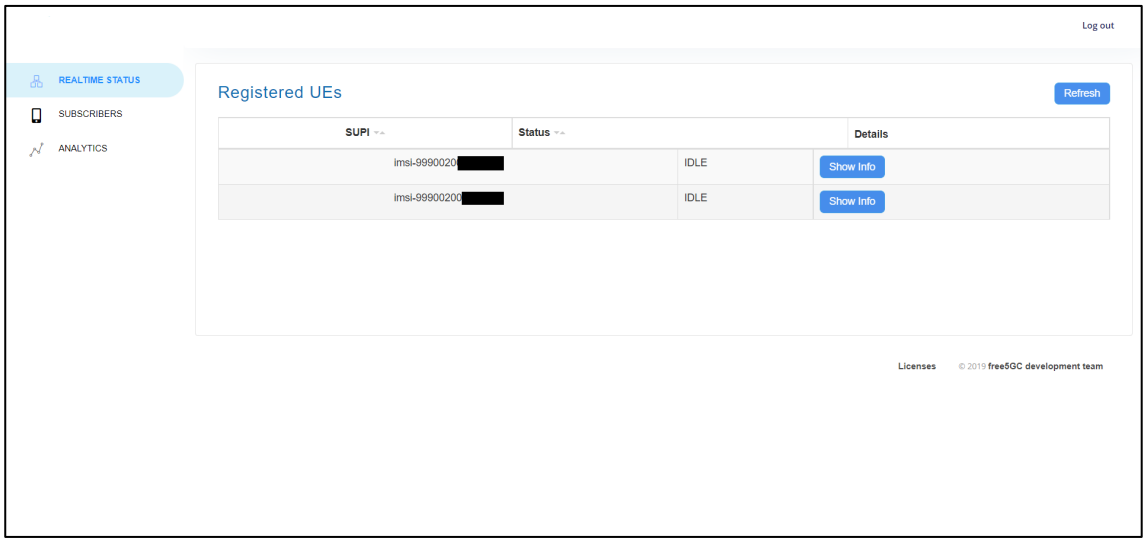


図 5-3-2-4-4　A 社　WebGUI SIM IDLE

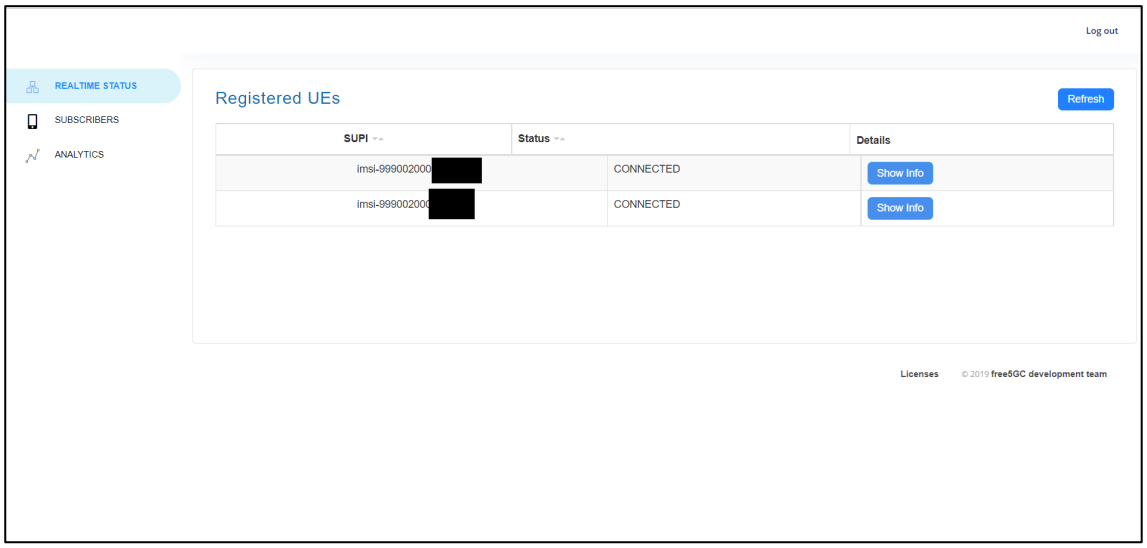


図 5-3-2-4-5　A 社　WebGUI SIM CONNECTED

また、上記画面の REALTIME STATUS における「Show Info」ボタンを押すことで詳細な SIM 登録情報を確認することができます。この画面で確認可能なポリシーは SST です。本実証環境では、SST を 1 と設定することにより eMBB を重視した検証を実施しました。

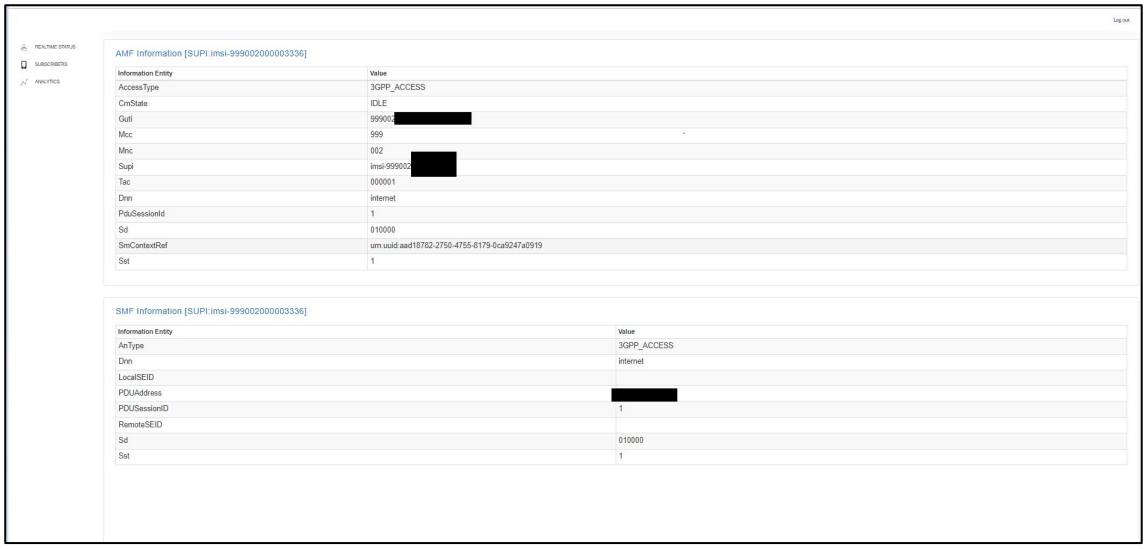


図 5-3-2-4-6　A 社　WebGUI SIM 情報詳細

(ウ)ポリシー情報の格納状況

SUBSCRIBERS における SIM 情報の中で「Modify」を選択すると設定編集モードになり、UE ごとに IMSI 番号やポリシー等設定することが可能です。この場合で確認・設定することができるポリシーは SST と Uplink/Downlink AMBR です。AMBR とは最大可能ビットレートで、UE が出力可能な伝送スループットの上限値です。設定された AMBR 値を超えて gNB-UE 区間での伝送を実施することは不可能です。拠点毎に UE 毎の AMBR を設定することで、複数台稼働時の負荷超過による通信断を設計上で防止できます。

加えて、本編集モードにおいて、SIM 認証に関する情報（K 値や OPc 値）の登録も可能です。SIM カードで認証する暗号情報を登録することで、該当する UE とのセッションが確立できます。

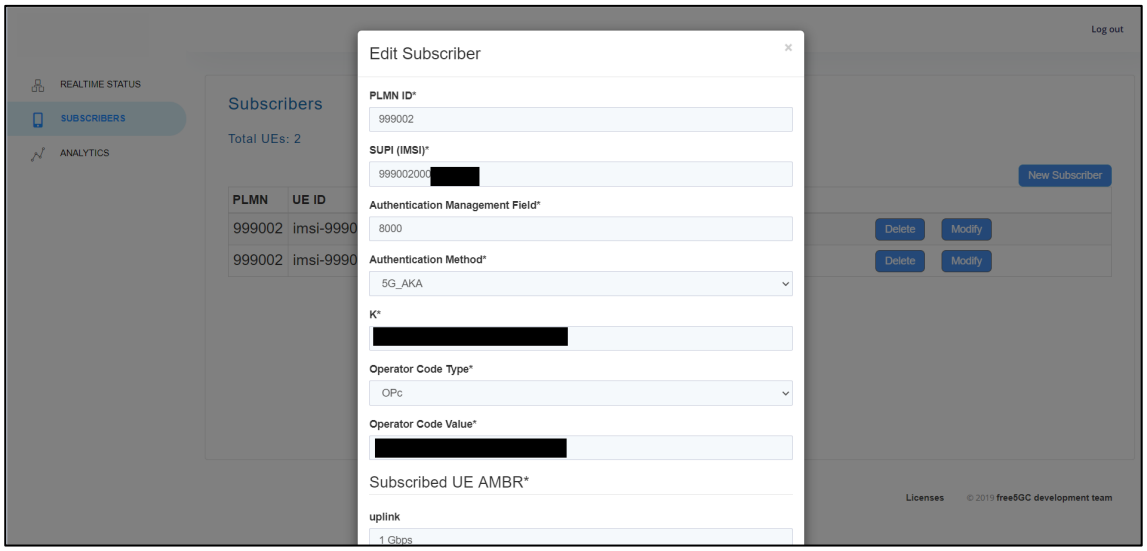


図 5-3-2-4-7　A 社　WebGUI ポリシー ①

K 値及び OPc 値は上記のタブより入力、編集が可能です。

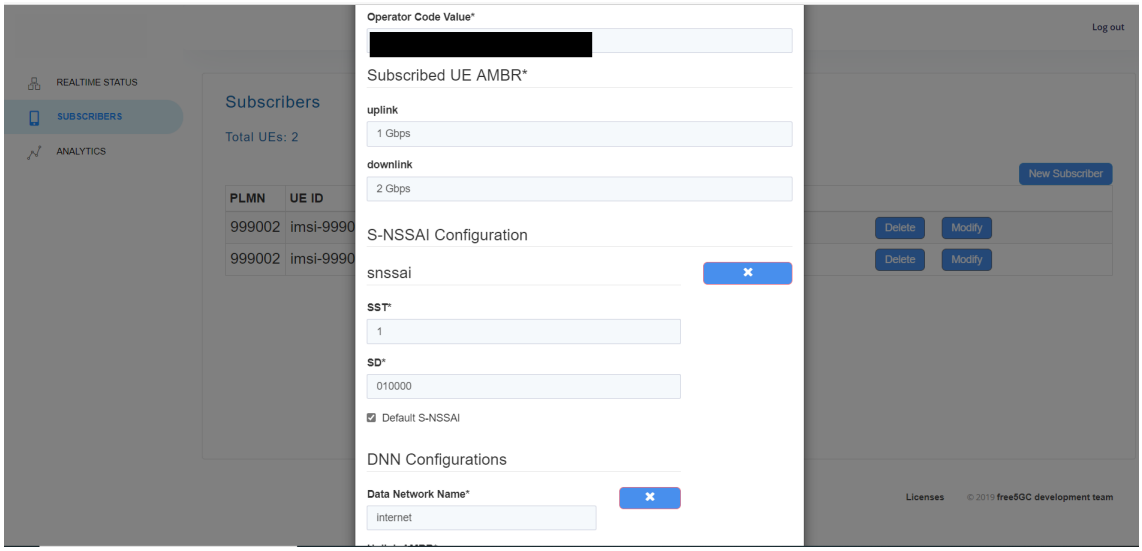


図 5-3-2-4-8　A 社　WebGUI ポリシー ②

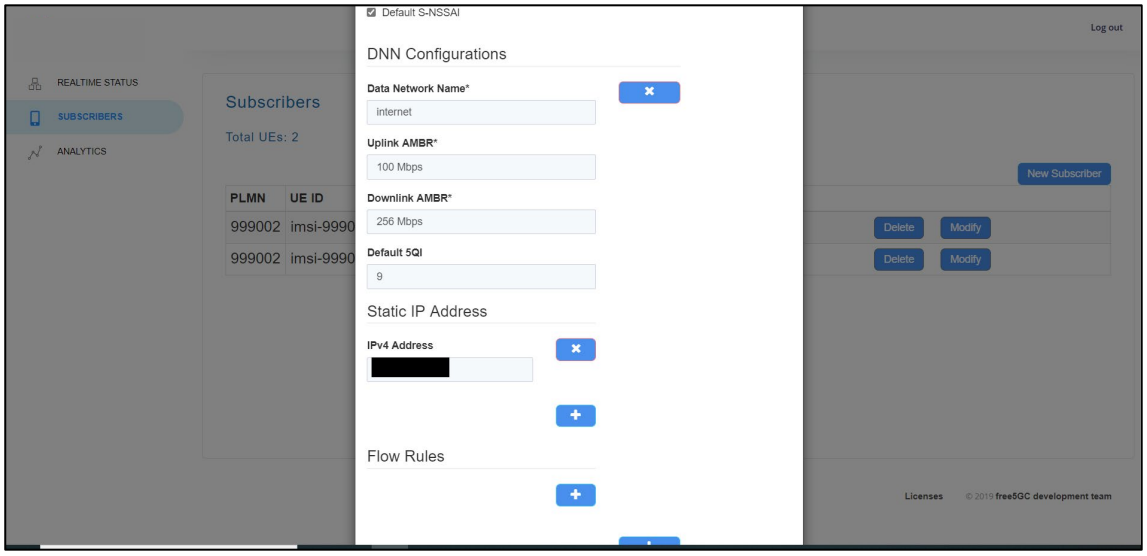


図 5-3-2-4-9　A 社　WebGUI ポリシー ③

(エ)在圏情報の格納状況

各 UE 端末の基地局との接続状態が確認できます。

しかし、在圏情報（どの PCI に接続しているか、あるいは端末の位置情報）について確認できる機能は有していません。

※「図 5-3-2-4-10　A 社　WebGUI 基地局接続状態　範囲外に出た際」の「Show info」から確認できるのは、(イ）項の端末情報のみ

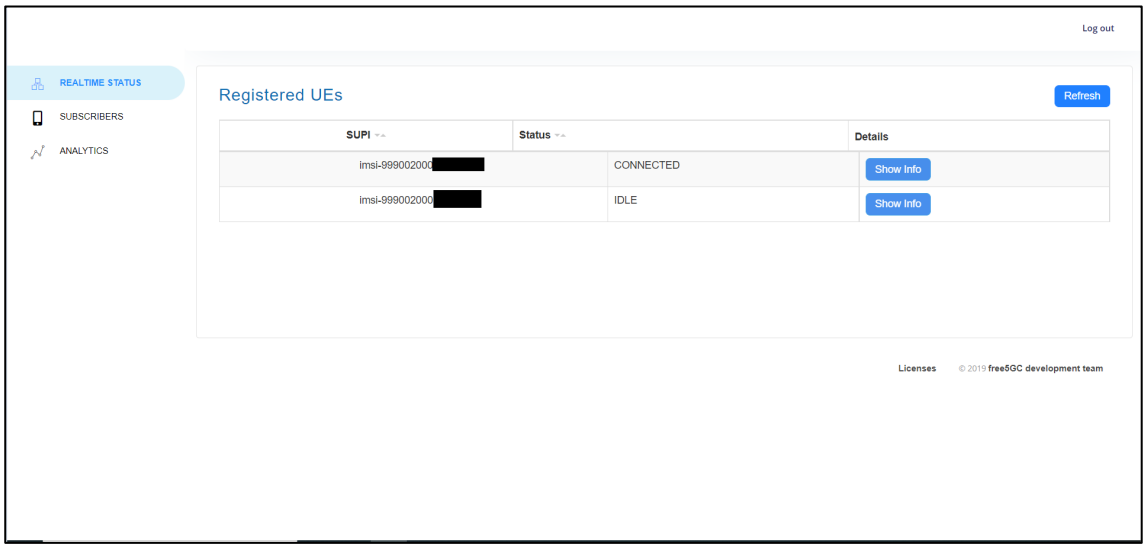


図 5-3-2-4-10　A 社　WebGUI 基地局接続状態　範囲外に出た際

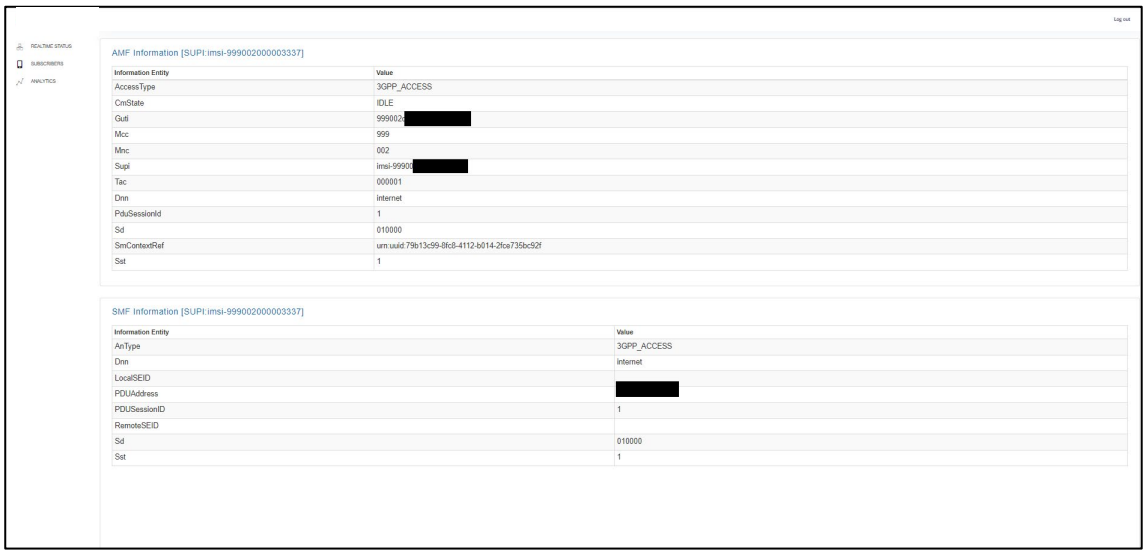


図 5-3-2-4-11　A 社　WebGUI 基地局接続状態　詳細

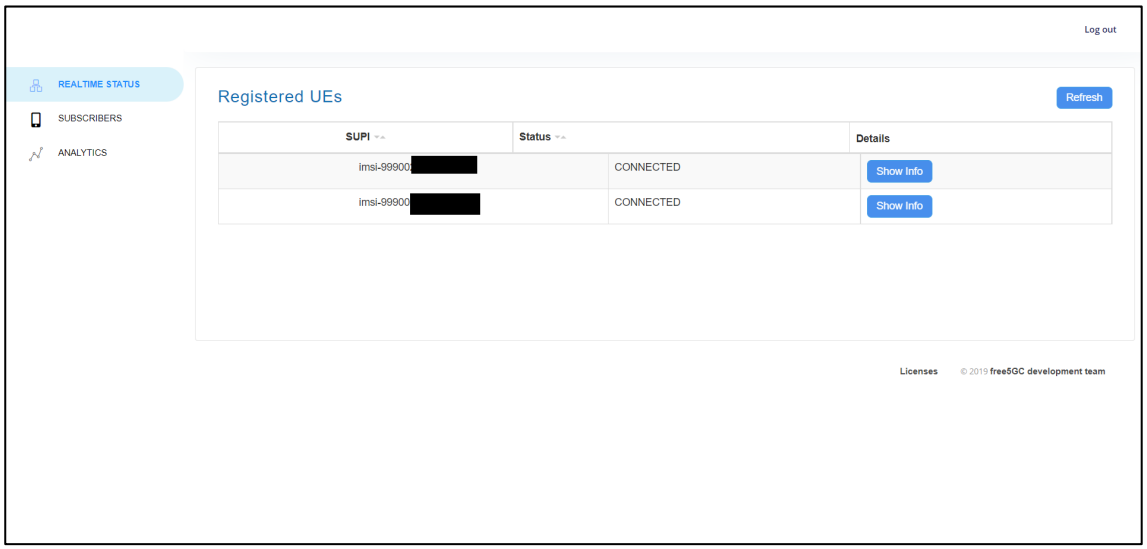


図 5-3-2-4-12　A 社　WebGUI 基地局接続状態　範囲内

(オ)セッション管理情報、ログの蓄積、管理状況

5GC では、セッション情報やステータス及びアラート等のログが蓄積され閲覧が可能です。主に取得できるログの情報は「表 5-3-2-4-1　5GC で確認できるログ情報」のとおりです。

表 5-3-2-4-1　5GC で確認できるログ情報

	内容
NF の起動・終了	各 NF の動作状況、NF からのエラー情報等
gNB 接続（N2）	gNB と AMF の接続状況
UE 認証情報	認証経過、認証可否、認証リクエスト中の SIM 情報、認証エラー情報、認証不可原因
SIM 登録情報	SIM 新規登録、登録済み SIM の更新情報

(カ)まとめ

本システムにおける機能は「表 5-3-2-4-2　A 社 機能検証結果」のとおりであることを確認しました。

表 5-3-2-4-2　A 社 機能検証結果

機能	実装の有無	ログの格納状況	コア共用の運用に関する個別設定可否	拠点毎の閲覧・管理
SIM 認証	○	○	○	○
端末情報	○	○	○	○
ポリシー管理情報	○	○	○	○
セッション管理情報	○	○	○	○
在圏情報	×	×	×	×
その他	―	機器の ALART 情報等の確認が可能	SIM 単位での UPF の接続先（エンド/センタ）の設定、切替変更が可能	―

・SIM 認証

SIM 情報、暗号化情報等の登録及び閲覧が可能であり、登録または変更時は内容がログ発行されることを確認しました。拠点毎にログイン権限を分けることでユーザーによる直接管理が行えます。運用に関しても SIM 単位での UPF 割当て等の個別権限の設定が可能です。

・端末情報

端末の設定情報や接続/通信状態の閲覧が可能です。ただし、端末へのユニーク ID(名称)等の設定や、種別または通信方式等を個別には設定できませんでした。

・ポリシー管理情報

端末個別に SST と Uplink/Downlink AMBR の設定が可能であるため、コア共用環境下においても柔軟なネットワーク構成を設計することができます。一方で、累積通信容量等のポリシー制御は実装されていません。

・セッション管理情報

セッション情報はログとして記録、抽出され確認することが可能です。この情報をもとに UE の接続情報や、認証エラー等のコントロールプレーンに関する情報を確認することができます。

・在圏情報

本検証で採用したシステムでは在圏情報は、管理/閲覧ができませんでした。拠点毎の接続端末数は端末情報より確認可能ですが、同一拠点内に複数の RU が設置されている環境では、通信先の RU の判別や UE 端末の位置情報等の確認ができません。

・その他

ログ情報として、各種機器やノードのステータス、ALART や WARNING 等の取得が可能なため、システムの正常性や障害時の切り分け対応を実施可能です。

イ　アクセス検証

同一のセル内で通信する 2 つの UE 端末について、センタ拠点 UPF 及びエンド拠点 UPF を個別に設定し通信が可能であることを検証しました。なお、本検証に関しては「複数企業共用パターン」と「業界共用パターン」それぞれのパターンで検証しています。

表 5-3-2-4-3　アクセス検証―複数企業共用パターン

対象装置	物理動作	検証結果
UE1	エンド拠点 UPF を指定	エンド拠点 UPF へアクセス可を確認 センタ拠点 UPF へアクセス不可を確認
UE2	センタ拠点 UPF を指定	エンド拠点 UPF へアクセス不可を確認 センタ拠点 UPF へアクセス可を確認

表 5-3-2-4-4　アクセス検証―業界共用パターン

対象装置	物理動作	検証結果
UE1	エンド拠点 UPF を指定	エンド拠点 UPF へアクセス可を確認 センタ拠点 UPF へアクセス不可を確認
UE2	センタ拠点 UPF を指定	エンド拠点 UPF へアクセス不可を確認 センタ拠点 UPF へアクセス可を確認

同一の gNB（RU）に接続する 2 以上の UE 端末に対して、UE 個別に UPF（通信先）を指定することが可能でした。アプリケーション等によって UE 個別にエンド拠点 UPF（MEC）を指定できることで NW の柔軟性が高まると考えられます。

ウ　考察

コア設備を共用するローカル５Ｇシステム環境下において、システムの運用及び管理に関する各種機能について評価を実施しました。

本検証で採用した製品（A 社製）の有する機能については、必要と考えられる機能を複数具備していることを確認し、事前に仮設していた当該機能を利用することで、コア共用環境下での運用が問題なく行えることを確認しました。特に、異なる企業間、拠点間でコア設備を共用するケースでは、システム運用及び管理を各拠点に区切った構成が必須であると考えられますが、当該ケースを想定したシステム設計が行われていることが確認できました。
また、SIM 管理、端末管理、ポリシー管理等の標準的な機能も問題なく有しており、当該システムはコア設備の共用化が可能であると総合的に考察できます。

一方で、UE 個別での異なる UPF へのアクセス設定の機能は有しているものの、在圏情報や UPF におけるトラフィックモニタリング機能等は有しておりません。特定の企業や団体がコア共用型のサービスを提供するうえで需要が高いと考えられるため、今後の課題であると推定します。特に従量課金型のサービス等では、ローカル５Ｇ市場を促進するうえでこれらの機能の充足を求められることが想定されます。

加えて、ネットワークのスライシング技術を導入することで、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。大容量伝送や低遅延通信等、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 NW 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。

以上をふまえ、コア装置の共用環境下において必要と考えられる機能及び本実証での実装有無は「表 5-3-2-4-5　A 社 機能実装有無」のとおりです。

表 5-3-2-4-5　A 社 機能実装有無

必要機能	実装有無	用途
SIM 登録/変更/閲覧 （拠点毎に権限範囲を分けること）	○	新規端末の登録、既設端末の変更、通信端末の管理
端末情報の閲覧	○	接続状態と通信状態の把握
ポリシー情報の登録/閲覧	○	端末に対するポリシーの設定及び管理
アクセス設定（UPF 指定制御）	○	センタ側 UPF とエンド型 UPF（MEC）の指定と制御
ログ蓄積/閲覧	○	システム状態の把握、トラブルシュート
セッション管理	○	コントロールプレーンの通信状況、認証判定結果等の確認
在圏情報	×	接続先 RU（PCI）の把握

トラフィックモニタリング（UPF）	×	トラフィックモニタ、累積通信量の把握
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

さらに、運用/監視という観点でも複数の拠点を含めた統合的な NW 監視体系が必要であると考えられます。監視項目の検討評価、障害切り分け方策等の考察、インシデントへの対処等の要素について、コア設備を共用する環境における方策検討を実施していく必要があると考えます。

(3) コアの共用におけるセキュリティ検証

① 検証目標

コア共用下においてはオンプレミスの構成と異なり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あります。本検証ではコア-基地局間におけるネットワークファンクション間通信に着目し、それら通信に対するセキュリティを評価し、セキュリティ向上させる手段を見出すため検証を行いました。

外部からの攻撃については、コアを共用している異なる拠点やコア共用と関係ない外部ネットワークからの侵入や通信の傍受が考えられ、これらの攻撃を IPsec によって防げることを確認しました。

内部からの攻撃については、エンド拠点からコアに対する攻撃、侵入されたコアから UPF に対する攻撃が考えられ、これらの攻撃をファンクション別のファイアウォールで防げることを確認しました。

具体的には以下の攻撃を想定しました。

・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)

上記の各種攻撃について疑似的に攻撃トラフィックを発生させ、それぞれ N2 Firewall / N3 Firewall / N4 Firewall / SBA Firewall にて該当の攻撃の検知・遮断ができることを確認しました。

表 1-2-4-2 想定される攻撃（再掲）

攻撃の種類	外部からの攻撃		内部からの攻撃	
	不正な外部からコアへの接続	マルチテナント間の攻撃	エンド拠点からコアに対する攻撃	侵入されたコアからUPFに対する攻撃
想定される攻撃の例	コアへの侵入	コア共用する異なる拠点への攻撃	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
攻撃によってもたらされる影響	コアからの攻撃への踏み台	異なる拠点への攻撃や通信の傍受	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	ネットワーク仮想化 (本構成ではセキュリティ装置が持つ機能を採用)		セキュリティ装置の各機能 (N2 Firewall / N3Firewall / N4 Firewall / SBA Firewall)	

表 1-2-4-3　セキュリティ検証対象箇所（再掲）

共用 パターン	UPF 配置	N6 Firewall	SecGW	N2 Firewall	N3 Firewall	N4 Firewall	SBA Firewall	マルチ テナント
		ユーザー 通信	拠点間	ファンク ション間	ファンク ション間	ファンク ション間	ファンク ション間	閉域性
		外部から の攻撃	外部から の攻撃	内部から の攻撃	内部から の攻撃	内部から の攻撃	内部から の攻撃	外部から の攻撃
複数企業 共用ﾊﾟﾀｰﾝ	ｾﾝﾀ拠点	対象外※1	対象外※2	セセ複 1	セセ複 2	セセ複 3	セセ複 4	セセ複 5
	ｴﾝﾄﾞ拠点	対象外※1	対象外※2	セエ複 1	対象外※3	セエ複 2	セエ複 3	セエ複 4
業界 共用ﾊﾟﾀｰﾝ	ｾﾝﾀ拠点	対象外※1	セセ業 1	セセ業 2	セセ業 3	セセ業 4	セセ業 5	セセ業 6
	ｴﾝﾄﾞ拠点	対象外※1	セエ業 1	セエ業 2	対象外※3	セエ業 3	セエ業 4	セエ業 5

※1：一般的な IP ネットワークのセキュリティ確保の問題であるため対象外とする

※2：回線サービス（SDN）により WAN 区間の安全性を確保するため対象外とする

※3：拠点内の有線ケーブル区間通信のため安全確保済という考えで対象外とする

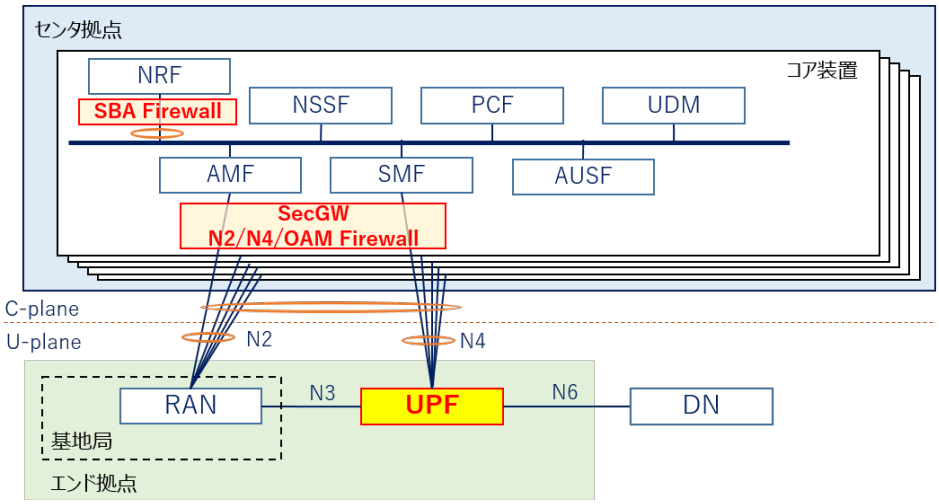


図 1-2-4-6　検証イメージ（エンド拠点の UPF を使用）（再掲）

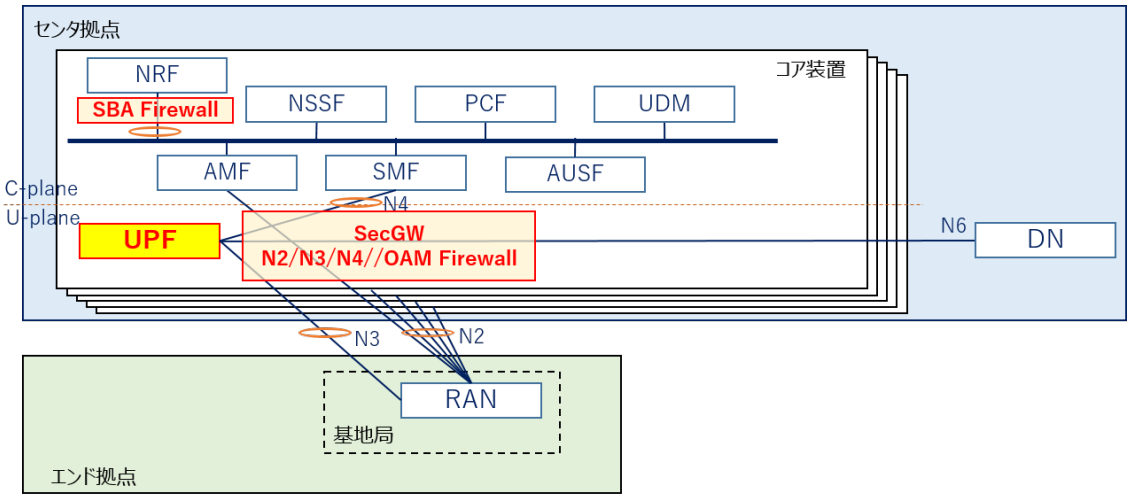


図 1-2-4-7　検証イメージ（センタ拠点の UPF を使用）（再掲）

② 評価・検証項目

エンド拠点に設置したUPFを使用する構成での評価・検証項目は、以下の「表5-3-3-2-1 検証項目(エンドUPF)」のとおりです。

表5-3-3-2-1 検証項目(エンドUPF)

大項目	中項目	小項目	検証概要	検証項目
セキュリティ検証	エンド拠点 UPF	業界共用パターン	SecGWの検証	不正な拠点から5Gコアへの接続の防止
		複数企業共用パターン	N2 Firewallの検証	CellSiteRouterとSecGW間での通信傍受の防止
				SCTP DoS攻撃の遮断
				不正なN2信号の検知と遮断
		業界共用パターン	N2 Firewallの検証	CellSiteRouterとSecGW間での通信傍受の防止
				SCTP DoS攻撃の遮断
				不正なN2信号の検知と遮断
		複数企業共用パターン	N4 Firewallの検証	UPF上のセッション情報の書き換え及び削除の検知・遮断
				不正なPFCP信号の検知・遮断
		業界共用パターン	N4 Firewallの検証	UPF上のセッション情報の書き換え及び削除の検知・遮断
				不正なPFCP信号の検知・遮断
		複数企業共用パターン	SBA Firewallの検証	5Gコア内のOpenAPI通信のモニタリング
				5Gコア内におけるバッファオーバーフロー等によるDoS攻撃検知・遮断
		業界共用パターン	SBA Firewallの検証	5Gコア内のOpenAPI通信のモニタリング
				5Gコア内におけるバッファオーバーフロー等によるDoS攻撃検知・遮断
		複数企業共用パターン	マルチテナントの検証	5Gコアマルチテナント間の閉域性の確認
		業界共用パターン	マルチテナントの検証	5Gコアマルチテナント間の閉域性の確認

センタ拠点に設置したUPFを使用する構成での評価・検証項目は、以下の「表5-3-3-2-2 検証項目(センタUPF)」のとおりです。

表 5-3-3-2-2　検証項目(センタ UPF)

大項目	中項目	小項目	検証概要	検証項目
セキュリティ検証	センタ拠点 UPF	業界共用パターン	SecGW の検証	C&C サーバへのアクセス検知・遮断
				マルウェアダウンロードの検知・遮断
				使用しているアプリケーションの検知・遮断
				UE の脆弱性を突いた攻撃検知・遮断
				不正な拠点から 5G コアへの接続
		複数企業共用パターン	N2　Firewall の検証	CellSiteRouter と SecGW 間での通信傍受の防止
				SCTP DoS 攻撃の遮断
				不正な N2 信号の検知と遮断
		業界共用パターン	N2　Firewall の検証	CellSiteRouter と SecGW 間での通信傍受の防止
				SCTP DoS 攻撃の遮断
				不正な N2 信号の検知と遮断
		複数企業共用パターン	N3　Firewall の検証	中間者攻撃、不正な GTP-U パケットを UPF に連続して送信
		業界共用パターン	N3　Firewall の検証	中間者攻撃、不正な GTP-U パケットを UPF に連続して送信
		複数企業共用パターン	N4　Firewall の検証	UPF 上のセッション情報の書き換え及び削除の検知・遮断
				不正な PFCP 信号の検知・遮断
		業界共用パターン	N4　Firewall の検証	UPF 上のセッション情報の書き換え及び削除の検知・遮断
				不正な PFCP 信号の検知・遮断
		複数企業共用パターン	SBA　Firewall の検証	5G コア内の OpenAPI 通信のモニタリング
				5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断
		業界共用パターン	SBA　Firewall の検証	5G コア内の OpenAPI 通信のモニタリング
				5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断
		複数企業共用パターン	マルチテナントの検証	5G コアマルチテナント間の閉域性の確認
		業界共用パターン	マルチテナントの検証	5G コアマルチテナント間の閉域性の確認

③　検証手順・結果

本検証で用いる測定ツールは、以下のとおりです。

表 5-3-3-3-1　測定ツール

項目	測定内容および具体的なツール
攻撃パケットツール	疑似攻撃生成ツール：Scapy
トラフィック解析ツール	トラフィックキャプチャツール：Wireshark
セッション確認	Ping

ア　エンド拠点に設置した UPF を使用する構成

(ア)複数企業共用パターン

エンド拠点に設置した UPF を使用する構成の複数企業共用パターンにおける検証手順と該当する攻撃の対応は「表 5-3-3-3-2　検証項目と該当する攻撃（エンド拠点 UPF 複数企業共用パターン)」のとおりです。

なお、「表 5-3-3-2-1 検証項目(エンド UPF)」のとおり「SecGW の評価」は「複数企業共用パターン」においては対象外とします。

表 5-3-3-3-2 検証項目と該当する攻撃（エンド拠点 UPF 複数企業共用パターン）

項番	評価項目	検証項目	該当する攻撃
セエ複-1	N2 Firewall の評価	CellSiteRouter と SecGW 間での通信傍受の防止	N2 通信の傍受
		SCTP　DoS 攻撃の遮断	同一 N2 リクエストを大量送信する DoS 攻撃
		不正な N2 信号の検知と遮断	AMF へ不正な N2 信号の送信
セエ複-2	N4 Firewall の評価	UPF 上のセッション情報の書き換え及び削除の検知・遮断	エンド UPF に対するセッション情報の危険リクエストの送信
		不正な PFCP 信号の検知・遮断	エンド UPF に対する不正な N2 リクエストの送信
セエ複-3	SBA Firewall の評価	5G コア内の OpenAPI 通信のモニタリング機能の確認	
		5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断	NRF に対するバッファオーバーフローを引き起こす http リクエストの送信
セエ複-4	マルチテナントの評価	5G コアマルチテナント間の閉域性の確認	

検証の手順・結果の詳細を以下にまとめます。

各図における IP アドレスは構成の一例です。また、検証結果に関係のない表示をトリミングしています。

セエ複-1：N2 Firewall の評価

- CellSiteRouter と SecGW 間での通信傍受の防止

SecGW により WAN 区間における N2 通信が暗号化され傍受できないことを確認するため、SecGW の 5GC 側と WAN 側においてトラフィックキャプチャを行いました。

結果は、5GC 側では PFCP、SCTP の通信が平文で見える一方、WAN 側では ESP(IPSec による暗号化)と表示されることを確認し、WAN 区間では IPSec による通信の暗号化がされていることが確認できました。

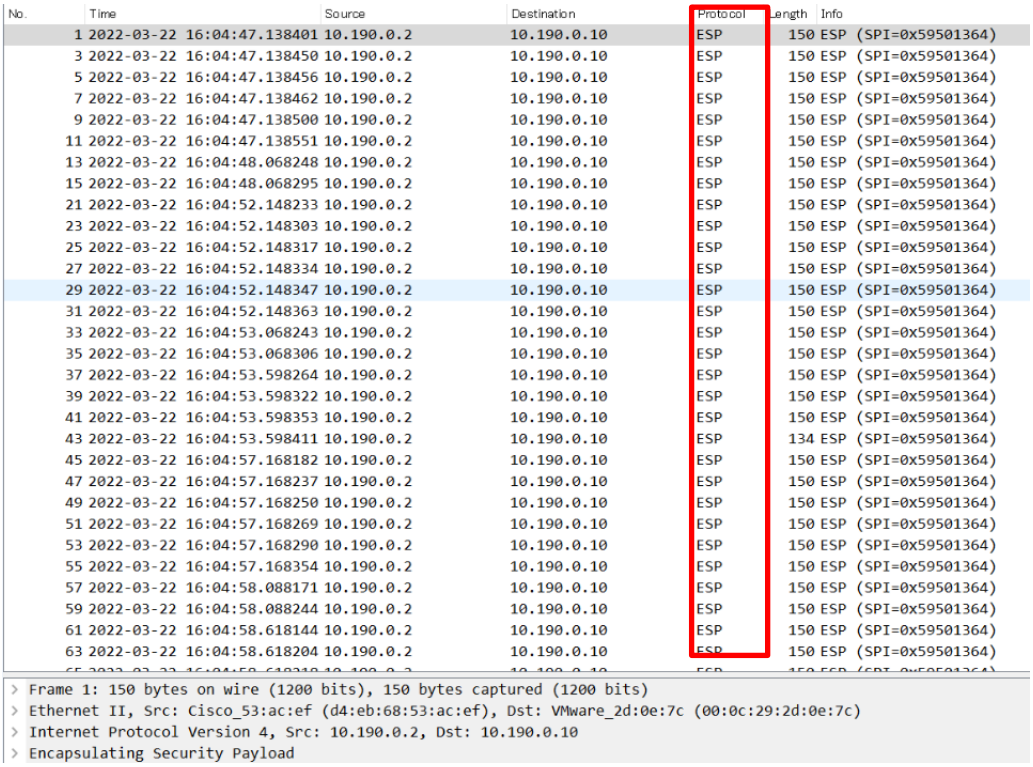
この結果より、CellSiteRouter と SecGW 間での通信傍受が防止できることが確認できました。

表示フィルタ … <Ctrl-/> を適用

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-03-22 16:04:50.212721	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Request
2	2022-03-22 16:04:50.217887	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
3	2022-03-22 16:04:50.217904	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Request
4	2022-03-22 16:04:50.218337	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Response
5	2022-03-22 16:05:00.218542	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Request
6	2022-03-22 16:05:00.223163	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
7	2022-03-22 16:05:03.623777	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT
8	2022-03-22 16:05:03.628040	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT_ACK
9	2022-03-22 16:05:10.223815	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Request
10	2022-03-22 16:05:10.228619	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
11	2022-03-22 16:05:15.464788	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT
12	2022-03-22 16:05:15.465087	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT_ACK
13	2022-03-22 16:05:20.229193	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Request
14	2022-03-22 16:05:20.234616	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
15	2022-03-22 16:05:20.234639	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Request
16	2022-03-22 16:05:20.235068	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Response
17	2022-03-22 16:05:30.235725	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Request
18	2022-03-22 16:05:30.241051	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
19	2022-03-22 16:05:34.343200	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT
20	2022-03-22 16:05:34.347442	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT_ACK
21	2022-03-22 16:05:40.241616	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Request
22	2022-03-22 16:05:40.247146	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response

```
> Frame 10: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
> Ethernet II, Src: VMware_2d:0e:86 (00:0c:29:2d:0e:86), Dst: VMware_28:00:1f (00:0c:29:28:00:1f)
> Internet Protocol Version 4, Src: 10.102.30.7, Dst: 10.101.10.7
> User Datagram Protocol, Src Port: 8805, Dst Port: 8805
> Packet Forwarding Control Protocol
```

図 5-3-3-3-1 セエ複-1 通信傍受 5GC 側



No.	Time	Source	Destination	Protocol	Length	Info
1	2022-03-22 16:04:47.138401	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
3	2022-03-22 16:04:47.138450	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
5	2022-03-22 16:04:47.138456	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
7	2022-03-22 16:04:47.138462	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
9	2022-03-22 16:04:47.138500	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
11	2022-03-22 16:04:47.138551	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
13	2022-03-22 16:04:48.068248	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
15	2022-03-22 16:04:48.068295	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
21	2022-03-22 16:04:52.148233	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
23	2022-03-22 16:04:52.148303	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
25	2022-03-22 16:04:52.148317	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
27	2022-03-22 16:04:52.148334	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
29	2022-03-22 16:04:52.148347	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
31	2022-03-22 16:04:52.148363	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
33	2022-03-22 16:04:53.068243	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
35	2022-03-22 16:04:53.068306	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
37	2022-03-22 16:04:53.598264	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
39	2022-03-22 16:04:53.598322	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
41	2022-03-22 16:04:53.598353	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
43	2022-03-22 16:04:53.598411	10.190.0.2	10.190.0.10	ESP	134	ESP (SPI=0x59501364)
45	2022-03-22 16:04:57.168182	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
47	2022-03-22 16:04:57.168237	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
49	2022-03-22 16:04:57.168250	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
51	2022-03-22 16:04:57.168269	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
53	2022-03-22 16:04:57.168290	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
55	2022-03-22 16:04:57.168354	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
57	2022-03-22 16:04:58.088171	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
59	2022-03-22 16:04:58.088244	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
61	2022-03-22 16:04:58.618144	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)
63	2022-03-22 16:04:58.618204	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501364)

```
> Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
> Ethernet II, Src: Cisco_53:ac:ef (d4:eb:68:53:ac:ef), Dst: VMware_2d:0e:7c (00:0c:29:2d:0e:7c)
> Internet Protocol Version 4, Src: 10.190.0.2, Dst: 10.190.0.10
> Encapsulating Security Payload
```

図 5-3-3-3-2　セエ複-1 通信傍受 WAN 側

● SCTP DoS 攻撃の遮断

SCTP DoS 攻撃の検知・遮断を検証するため、AMF へのトラフィック量が閾値を超えた場合に N2 Firewall によって検知・遮断できることを検証しました。具体的には閾値として 2pps を設定し、AMF 宛てに 9pps のトラフィックを発生させ、検知・遮断できることを確認しました。

結果は、GUI にて検知設定時には「detected」、遮断設定時には「dropped」と表示され、いずれにおいても 7 回分のパケットが検知・遮断できていることを確認しました。

この結果より、SCTP DoS 攻撃の検知・遮断ができることが確認できました。

図 5-3-3-3-3-1 セエ複-1 SCTP DoS 攻撃 検知①

図 5-3-3-3-3-2 セエ複-1 SCTP DoS 攻撃 検知②

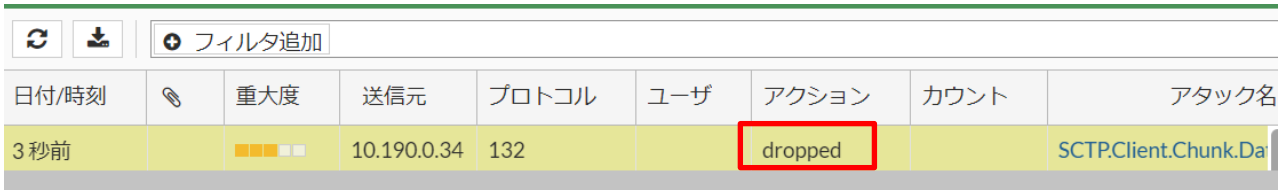


図 5-3-3-3-4-1 セエ複-1 SCTP DoS 攻撃 遮断①

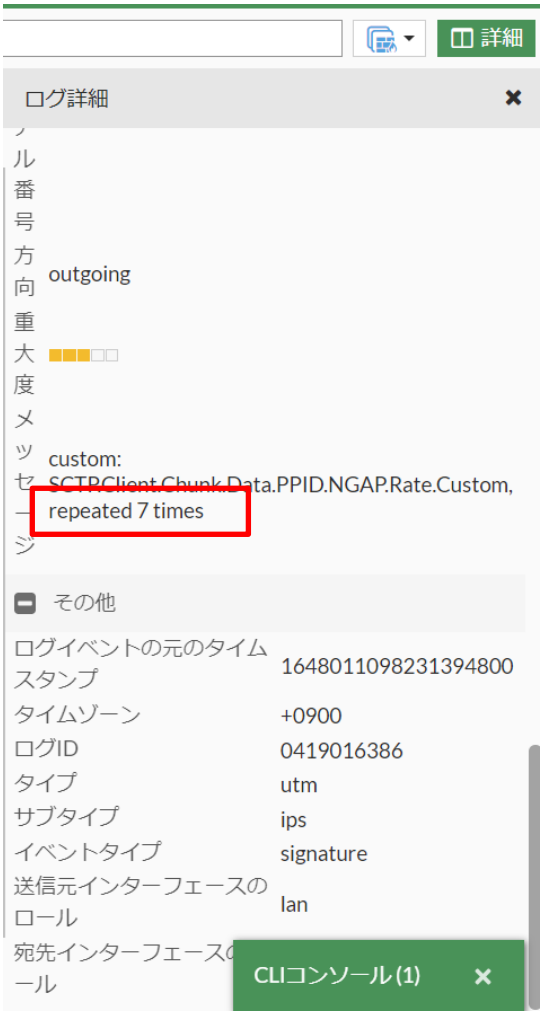


図 5-3-3-3-4-2 セエ複-1 SCTP DoS 攻撃 遮断②

- 不正な N2 信号の検知と遮断

不正な N2 信号を送信し、N2 Firewall によって検知・遮断できることを確認しました。具体的には不正な N2 信号として不正な ppid 値(0)をセットしたパケットを AMF 宛てに送信し、N2 Firewall にて検知・遮断できることを確認しました。

結果は、CLI にて検知設定時には「pass」、遮断設定時には「reset」と表示され、検知・遮断ができていることを確認しました。

この結果より、不正な N2 信号の検知と遮断ができることが確認できました。

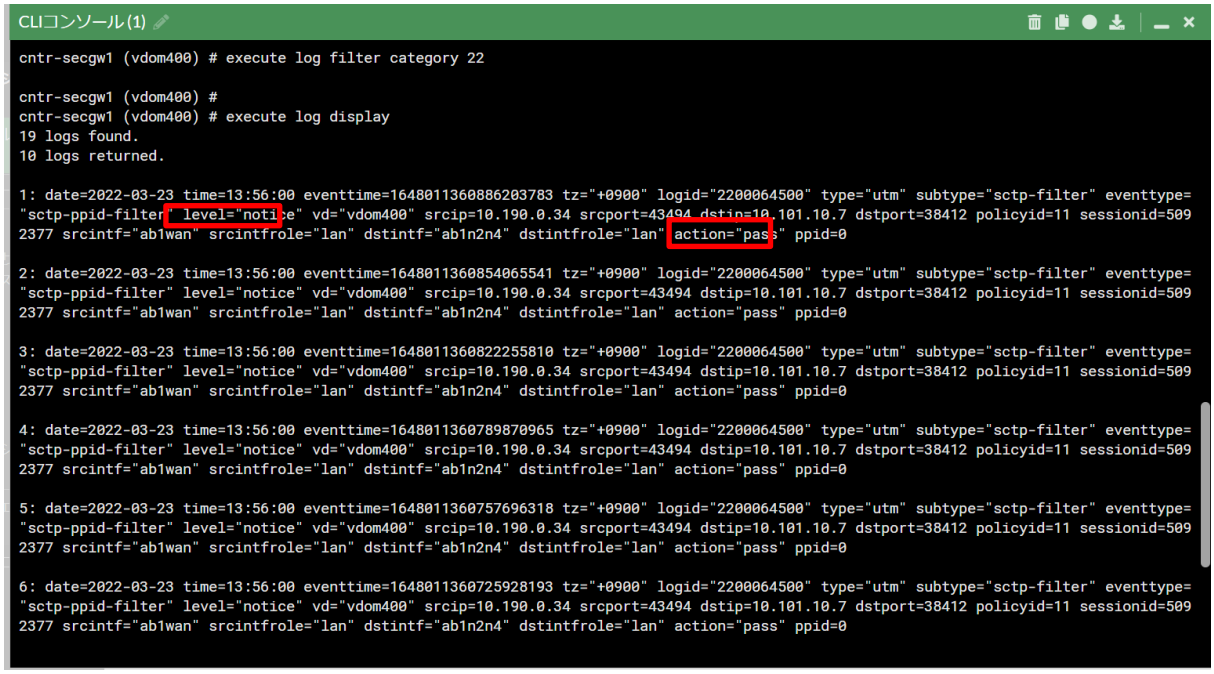


図 5-3-3-3-5 セエ複-1 不正な N2 信号 検知

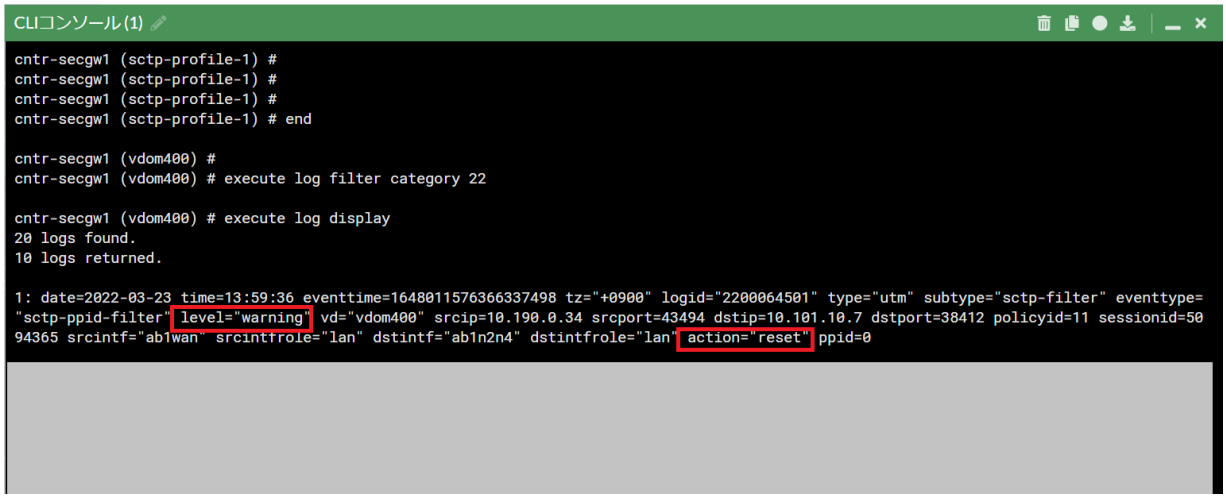


図 5-3-3-3-6 セエ複-1 不正な N2 信号 遮断

セエ複-2：N4 Firewall の評価

- UPF 上のセッション情報の書き換え及び削除の検知・遮断

UPF 宛てにセッション情報の書き換えを行うパケットを送信し、N4 Firewall によって攻撃を検知・遮断する検証を行いました。具体的には SMF を偽装する疑似 SMF から拠点側の UPF 宛てにセッションを削除する攻撃を行い、検知・遮断ができていることを確認しました。

GUI にて該当パケットが検知設定時には「forwarded」、遮断設定時には「prohibited」となっていることを確認しました。

また、攻撃を遮断しなかった場合にセッションが切れることを、拠点 UE 下部の端末から UPF 宛ての ping で確認し、検知設定時のみ ping が切れることを確認しました。

この結果より、UPF 上のセッション情報の書き換え及び削除の検知・遮断ができることが確認できました。

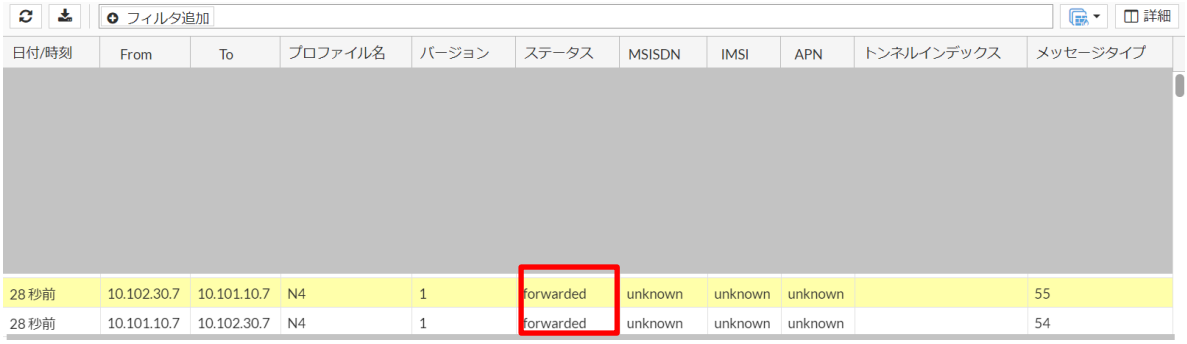


図 5-3-3-3-7 セエ複-2 セッション削除 検知

```
C:¥Users¥ＢＦＬ>ping 172.17.200.2 -t

172.17.200.2 に ping を送信しています 32 バイトのデータ:
172.17.200.2 からの応答: バイト数 =32 時間 =117ms TTL=61
172.17.200.2 からの応答: バイト数 =32 時間 =131ms TTL=61
172.17.200.2 からの応答: バイト数 =32 時間 =148ms TTL=61
172.17.200.2 からの応答: バイト数 =32 時間 =150ms TTL=61
<中略>
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
<中略>

172.17.200.2 の ping 統計:
    パケット数: 送信 = 151、受信 = 105、損失 = 46 (30% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 10ms、最大 = 167ms、平均 = 57ms
```

図 5-3-3-3-8 セエ複-2 セッション削除時 ping

図 5-3-3-3-9 セエ複-2 セッション削除 遮断

- 不正な PFCP 信号の検知・遮断

UPF 宛てに不正な PFCP 信号を送信し、N4 Firewall によって攻撃を検知・遮断する検証を行いました。具体的には SMF を偽装する疑似 SMF から拠点側の UPF 宛てに不正な Message Type(254)をセットしたパケットを送信し、N4 Firewall にて検知・遮断ができていることを確認しました。

結果は、GUI にてメッセージタイプ 254 が届いた際、検知設定時には「prohibitted monitor」、遮断設定時には「prohibited」と表示され検知・遮断できていることを確認しました。

この結果より、不正な PFCP 信号の検知・遮断ができることが確認できました。

図 5-3-3-3-10 セエ複-2 不正な PFCP 検知

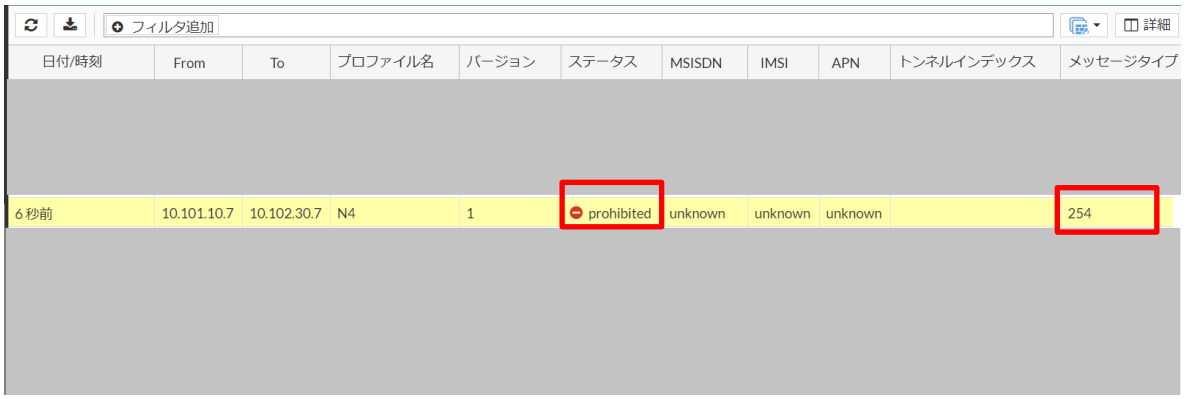


図 5-3-3-3-11 セエ複-2 不正な PFCP 遮断

セエ複-3：SBA Firewall の評価

- 5G コア内の OpenAPI 通信のモニタリング

http2/tls1.2 によって行われる NRF への SBI 通信をテナント毎にモニタリングできることを確認しました。複数企業共用パターンである NTT 中央研修センタ(NRF-policy1)およびいすゞ自動車(NRF-policy2)のそれぞれについて GUI ログをフィルタリングし、該当のテナントの情報のみを抽出できることを確認しました。また、同様に http2/tls1.2 の通信のみをフィルタリングできることを確認しました。

この結果より、5G コア内の OpenAPI 通信のモニタリングができることが確認できました。

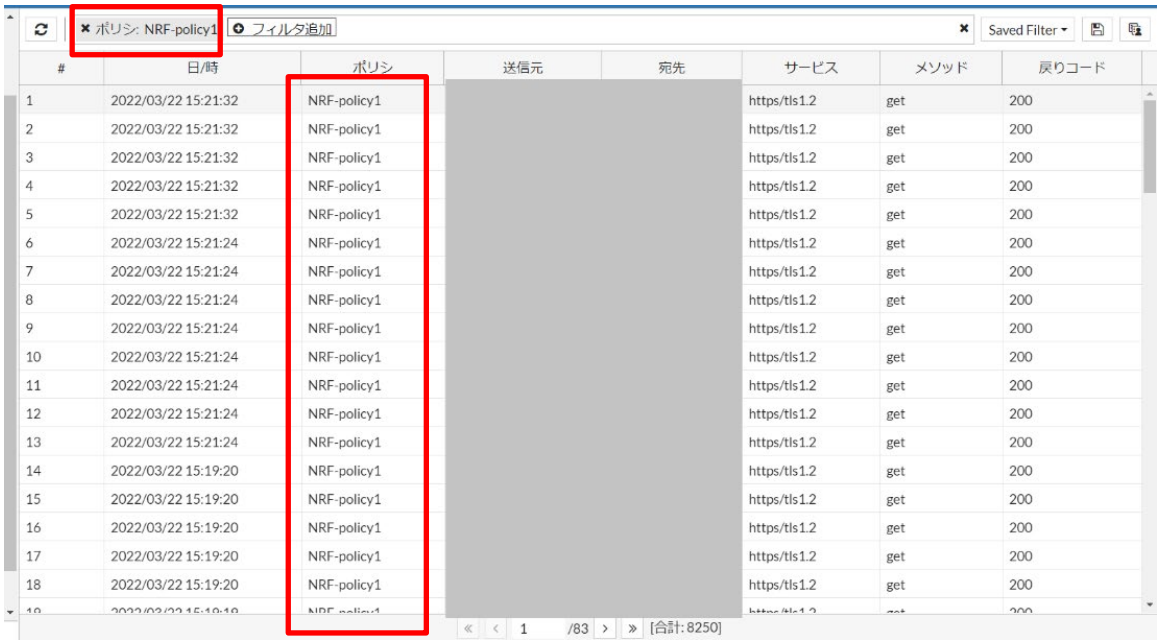


図 5-3-3-3-12 セエ複-3 OpenAPI モニタリング NTT 中央研修センタ

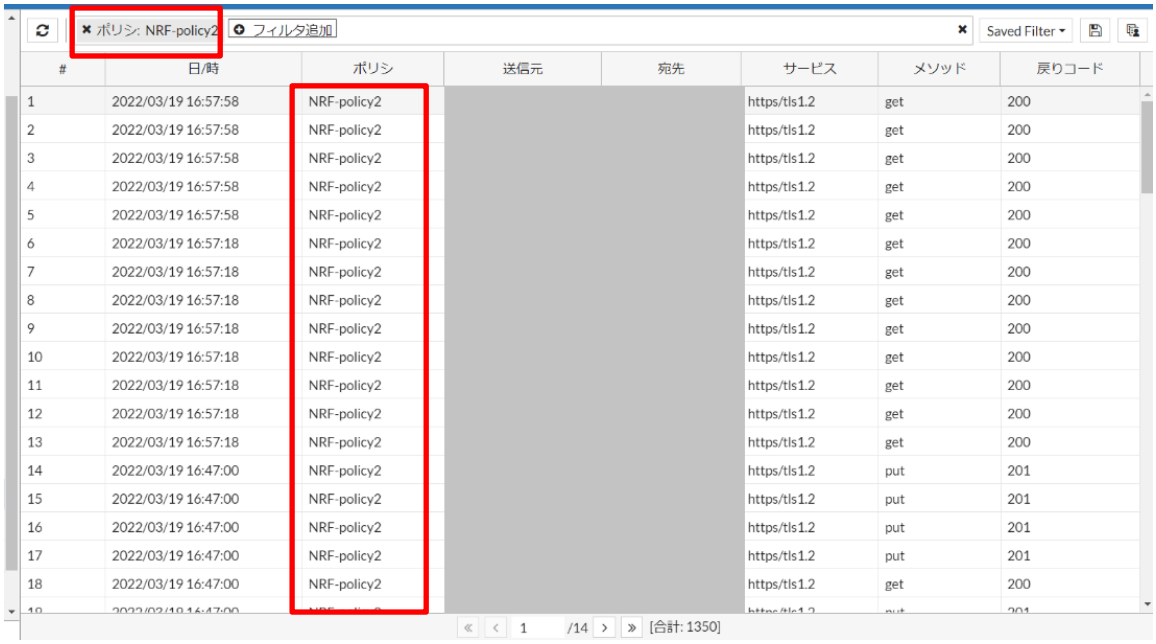


図 5-3-3-3-13 セエ複-3 OpenAPI モニタリング いすゞ自動車

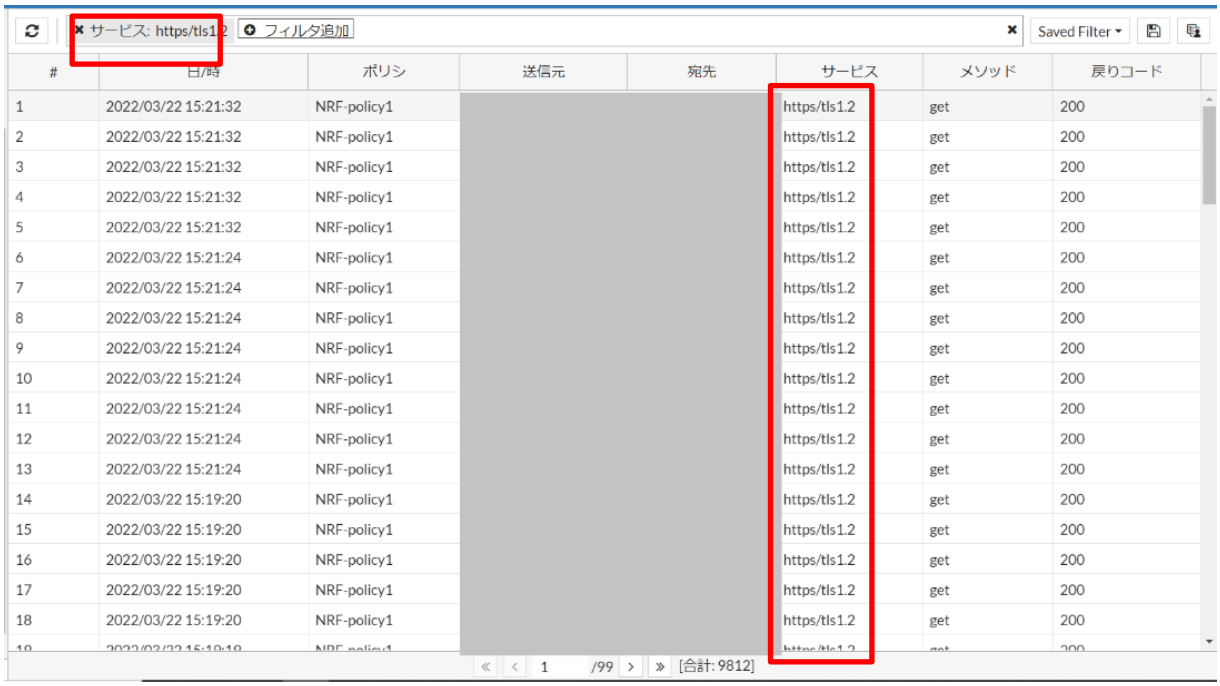


図 5-3-3-3-14 セエ複-3 OpenAPI モニタリング http/tls1.2

- 5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断

NRF への OpenAPI を使用した DoS 攻撃を SBA Firewall にて検知・遮断する検証を行いました。具体的には NRF 宛てに不正な API 通信として長大な URL の http リクエストを送信し、SBA Firewall にて検知・遮断ができることを確認しました。

結果は、GUI にて検知設定時には「Alert」、遮断設定時には「403 Forbidden エラー」を返していることと、128Byte 以上の長大な URL のリクエストを検知・遮断した旨のメッセージを確認しました。

この結果より、5G コア内におけるバッファオーバーフロー等による DoS 攻撃の検知・遮断ができることが確認できました。

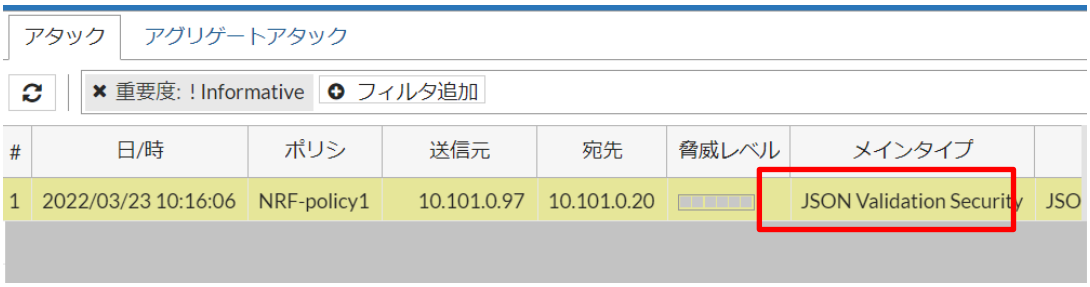


図 5-3-3-3-15-1 セエ複-3 バッファオーバーフロー 検知①

図 5-3-3-3-15-2 セエ複-3 バッファオーバーフロー 検知②

図 5-3-3-3-16-1 セエ複-3 バッファオーバーフロー 遮断 ①

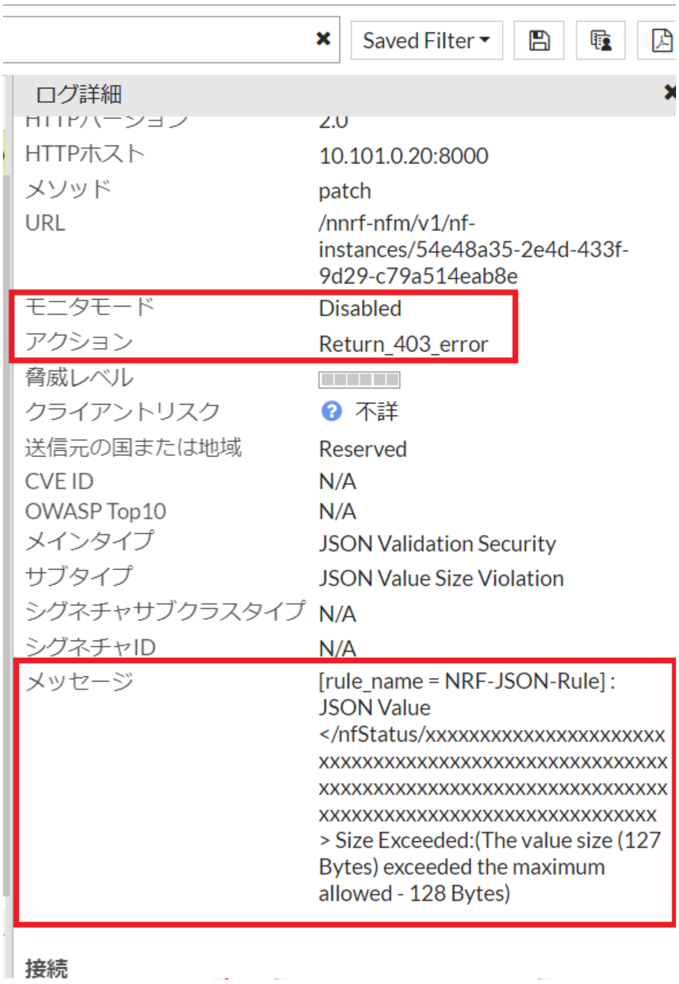


図 5-3-3-3-16-2 セエ複-3 バッファオーバーフロー 遮断②

セエ複-4：マルチテナントの評価

- 5G コアマルチテナント間の閉域性の確認

マルチテナントの閉域性を検証するため、異なるテナントのネットワーク情報が独立して管理されていることを確認しました。具体的にはNTT 中央研修センタ(vdom400)のルーティングテーブル、GTP-U セッション、SCTP セッション、PFCP セッションの情報にいすゞ自動車(vdom500)の情報が含まれないことを確認しました。

この結果より、5G コアマルチテナント間の閉域性が確認できました。

```
cntr-secgw1 (vdom400) # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 10.190.0.9, ab1wan
C       10.101.10.0/24 is directly connected, ab1n2n4
C       10.101.20.0/24 is directly connected, ab1n3
C       10.101.30.0/24 is directly connected, ab1n4
C       10.190.0.8/30 is directly connected, ab1wan
S       10.190.0.12/30 [5/0] via IPsec_vdom400 tunnel 10.190.0.2
C       10.190.0.13/32 is directly connected, IPsec_vdom400
```

図 5-3-3-3-17-1 セエ複-4 マルチテナント①

```
cntr-secgw1 (vdom400) # get system session list
PROTO   EXPIRE SOURCE           SOURCE-NAT       DESTINATION      DESTINATION-NAT
udp     179    10.190.0.2:500   -                10.190.0.10:500  -
udp     174    10.190.0.14:3588 -                208.91.112.52:53 -
udp     179    10.190.0.14:3588 -                208.91.112.53:53 -
sctp    3592   10.190.0.34:38413 -                10.101.10.7:38412 -
udp     176    10.101.10.7:8805 -                10.102.30.7:8805 -
```

図 5-3-3-3-17-2 セエ複-4 マルチテナント②

```
cntr-secgw1 (vdom400) # diagnose ip arp list
index=46  fname=ab1wan 10.190.0.9 d4:eb:68:53:ac:ef state=00000002 use=45 confirm=682 update=682 ref=7
index=25  fname=vdom400 0.0.0.0 00:00:00:00:00:00 state=00000040 use=60529273 confirm=60535273 update=60529273 ref=1
index=47  fname=ab1n2n4 10.101.10.7 00:0c:29:28:00:1f state=00000008 use=329 confirm=2830 update=329 ref=3
```

図 5-3-3-3-17-3 セエ複-4 マルチテナント③

エンド拠点 UPF を使用した場合の複数企業共用パターンの検証結果を以下にまとめます。いずれの項目においても検証内容に対し、検知・遮断ができることが確認できました。

表 5-3-3-3-3 検証結果まとめ（エンド拠点 UPF 複数企業共用パターン）

項番	評価項目	検証内容	結果
セエ複-1	N2 Firewall の評価	CellSiteRouter と SecGW 間での通信傍受の防止	○
		SCTP DoS 攻撃の検知・遮断	○
		不正な N2 信号の検知と遮断	○
セエ複-2	N4 Firewall の評価	UPF 上のセッション情報の書き換え及び削除の検知・遮断	○
		不正な PFCP 信号の検知・遮断	○
セエ複-3	SBA Firewall の評価	5G コア内の OpenAPI 通信のモニタリング	○
		5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断	○
セエ複-4	マルチテナントの評価	5G コアマルチテナント間の閉域性の確認	○

（イ）業界共用パターン

エンド拠点に設置した UPF を使用する構成の業界共用パターンにおける検証項目と該当する攻撃の対応は「表 5-3-3-3-4 検証項目と該当する攻撃 エンド拠点 UPF 業界共用パターン」のとおりです。

複数企業共用パターンと同様、評価項目ごとに疑似攻撃とそれに対する防御方法を検証し、セキュリティ装置によるセキュリティ向上が図れていることを確認します。

表 5-3-3-3-4 検証項目と該当する攻撃（エンド拠点 UPF 業界共用パターン）

項番	評価項目	検証項目	該当する攻撃
セエ業-1	SecGW の評価	不正な拠点から 5G コアへの接続の防止	不正な拠点からの 5G コアへの接続
セエ業-2	N2 Firewall の評価	CellSiteRouter と SecGW 間での通信傍受の防止	N2 通信の傍受
		SCTP DoS 攻撃の遮断	同一 N2 リクエストを大量送信する DoS 攻撃
		不正な N2 信号の検知と遮断	AMF への不正な N2 信号の送信
セエ業-3	N4 Firewall の評価	UPF 上のセッション情報の書き換え及び削除の検知・遮断	エンド UPF に対するセッション情報の危険リクエストの送信
		不正な PFCP 信号の検知・遮断	エンド UPF に対する不正な N2 リクエストの送信
セエ業-4	SBA Firewall の評価	5G コア内の OpenAPI 通信のモニタリング	
		5G コア内におけるバッファ	NRF に対するバッファオーバーフロ

		オーバーフロー等による DoS 攻撃検知・遮断	ーを引き起こす http リクエストの送信
セエ業-5	マルチテナントの評価	5G コアマルチテナント間の閉域性の確認	

検証の手順・結果の詳細を以下にまとめます。

各図における IP アドレスは構成の一例です。また、検証結果に関係のない表示をトリミングしています。

セエ業-1：SecGW の評価

- 不正な拠点から 5G コアへの接続の防止

不正な拠点として、拠点間の IPSec トンネルにおいて、SecGW に設定されているものと異なる事前共有鍵または Proxy-ID を設定した拠点ルータからの接続を行い、トンネルが確立されないことを確認しました。

結果は、GUI でステータスが「negotiated error」の後に「failure」と表示されることが確認でき、トンネルが確立されないことを確認できました。

この結果より、不正な拠点から 5G コアへの接続が防止できることが確認できました。

日付/時刻	レベル	アクション	ステータス	メッセージ	VPN トンネル
10 秒前		negotiate	failure	progress IPsec phase 1	IPsec_vdom400
10 秒前		negotiate	negotiate_error	IPsec phase 1 error	IPsec_vdom400
10 秒前		negotiate	failure	progress IPsec phase 1	IPsec_vdom400
10 秒前		negotiate	negotiate_error	IPsec phase 1 error	IPsec_vdom400
16 秒前		negotiate	failure	progress IPsec phase 1	IPsec_vdom400
16 秒前		negotiate	negotiate_error	IPsec phase 1 error	IPsec_vdom400
16 秒前		negotiate	failure	progress IPsec phase 1	IPsec_vdom400
16 秒前		negotiate	negotiate_error	IPsec phase 1 error	IPsec_vdom400
17 秒前		delete_phase1_sa		delete IPsec phase 1 SA	IPsec_vdom400
19 秒前		negotiate	failure	progress IPsec phase 1	IPsec_vdom400
19 秒前		negotiate	negotiate_error	IPsec phase 1 error	IPsec_vdom400
19 秒前		negotiate	success	progress IPsec phase 1	IPsec_vdom400
19 秒前		negotiate	success	progress IPsec phase 1	IPsec_vdom400

図 5-3-3-3-18 セエ業-1 不正な拠点からの接続

セエ業-2：N2 Firewall の評価

- CellSiteRouter と SecGW 間での通信傍受の防止

SecGW により WAN 区間における N2 通信が暗号化され傍受できないことを確認するため、SecGW の 5GC 側と WAN 側においてトラフィックキャプチャを行いました。

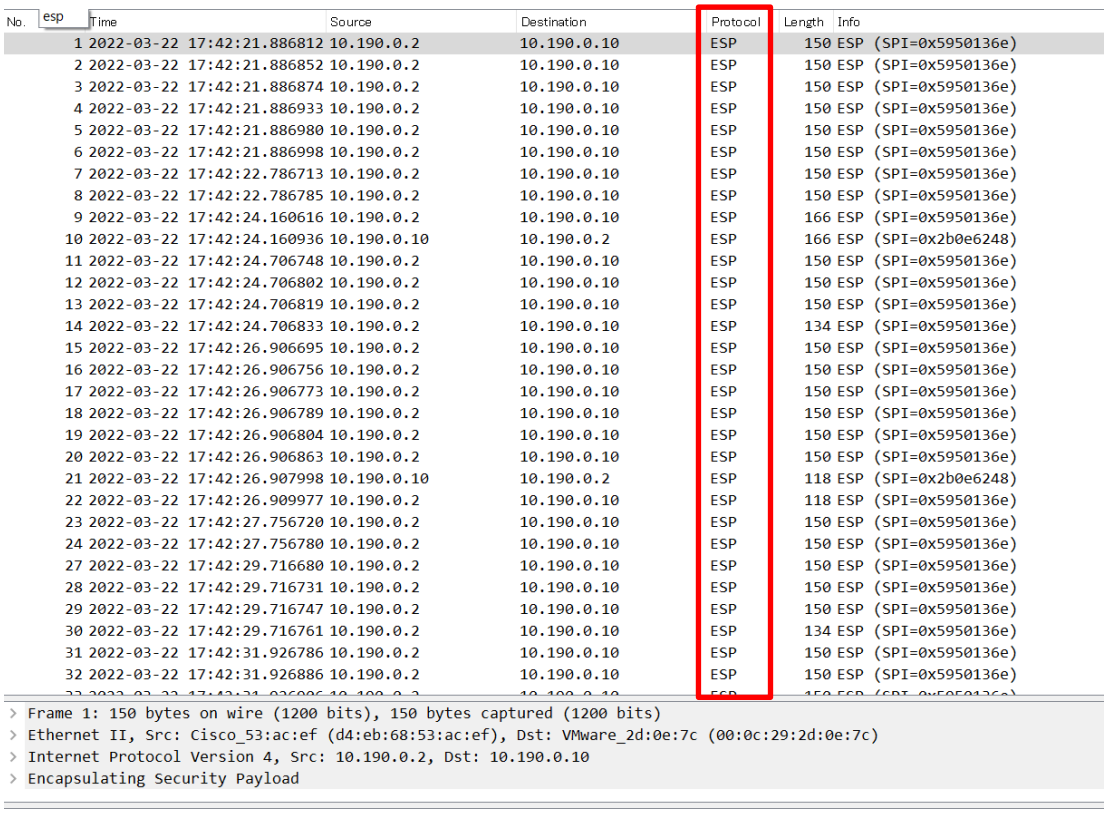
結果は、5GC 側では PFCP、SCTP の通信が平文で見える一方、WAN 側では ESP(IPSec による暗号化)と表示されることを確認し、WAN 区間では IPSec による通信の暗号化がされていることが確認できました。

この結果より、CellSiteRouter と SecGW 間での通信傍受が防止できることが確認できました。

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-03-22 17:42:24.160646	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT
2	2022-03-22 17:42:24.160909	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT_ACK
3	2022-03-22 17:42:26.907960	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Request
4	2022-03-22 17:42:26.909994	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
5	2022-03-22 17:42:34.772190	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT
6	2022-03-22 17:42:34.773861	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT_ACK
7	2022-03-22 17:42:36.910574	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Request
8	2022-03-22 17:42:36.912689	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
9	2022-03-22 17:42:46.913483	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Request
10	2022-03-22 17:42:46.915630	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
11	2022-03-22 17:42:46.915970	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Request
12	2022-03-22 17:42:46.916284	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Response
13	2022-03-22 17:42:56.916349	10.101.10.7	10.102.30.7	PFCP	60	PFCP Heartbeat Request
14	2022-03-22 17:42:56.918523	10.102.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
15	2022-03-22 17:42:56.992095	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT
16	2022-03-22 17:42:56.992297	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT_ACK

```
> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: VMware_2d:0e:86 (00:0c:29:2d:0e:86), Dst: VMware_28:00:1f (00:0c:29:28:00:1f)
> Internet Protocol Version 4, Src: 10.190.0.34, Dst: 10.101.10.7
> Stream Control Transmission Protocol, Src Port: 38413 (38413), Dst Port: 38412 (38412)
```

図 5-3-3-3-19 セエ業-2 通信傍受 5GC 側



No.	Time	Source	Destination	Protocol	Length	Info
1	2022-03-22 17:42:21.886812	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
2	2022-03-22 17:42:21.886852	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
3	2022-03-22 17:42:21.886874	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
4	2022-03-22 17:42:21.886933	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
5	2022-03-22 17:42:21.886980	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
6	2022-03-22 17:42:21.886998	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
7	2022-03-22 17:42:22.786713	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
8	2022-03-22 17:42:22.786785	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
9	2022-03-22 17:42:24.160616	10.190.0.2	10.190.0.10	ESP	166	ESP (SPI=0x5950136e)
10	2022-03-22 17:42:24.160936	10.190.0.10	10.190.0.2	ESP	166	ESP (SPI=0x2b0e6248)
11	2022-03-22 17:42:24.706748	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
12	2022-03-22 17:42:24.706802	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
13	2022-03-22 17:42:24.706819	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
14	2022-03-22 17:42:24.706833	10.190.0.2	10.190.0.10	ESP	134	ESP (SPI=0x5950136e)
15	2022-03-22 17:42:26.906695	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
16	2022-03-22 17:42:26.906756	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
17	2022-03-22 17:42:26.906773	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
18	2022-03-22 17:42:26.906789	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
19	2022-03-22 17:42:26.906804	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
20	2022-03-22 17:42:26.906863	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
21	2022-03-22 17:42:26.907998	10.190.0.10	10.190.0.2	ESP	118	ESP (SPI=0x2b0e6248)
22	2022-03-22 17:42:26.909977	10.190.0.2	10.190.0.10	ESP	118	ESP (SPI=0x5950136e)
23	2022-03-22 17:42:27.756720	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
24	2022-03-22 17:42:27.756780	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
27	2022-03-22 17:42:29.716680	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
28	2022-03-22 17:42:29.716731	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
29	2022-03-22 17:42:29.716747	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
30	2022-03-22 17:42:29.716761	10.190.0.2	10.190.0.10	ESP	134	ESP (SPI=0x5950136e)
31	2022-03-22 17:42:31.926786	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)
32	2022-03-22 17:42:31.926886	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x5950136e)

```
> Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
> Ethernet II, Src: Cisco_53:ac:ef (d4:eb:68:53:ac:ef), Dst: VMware_2d:0e:7c (00:0c:29:2d:0e:7c)
> Internet Protocol Version 4, Src: 10.190.0.2, Dst: 10.190.0.10
> Encapsulating Security Payload
```

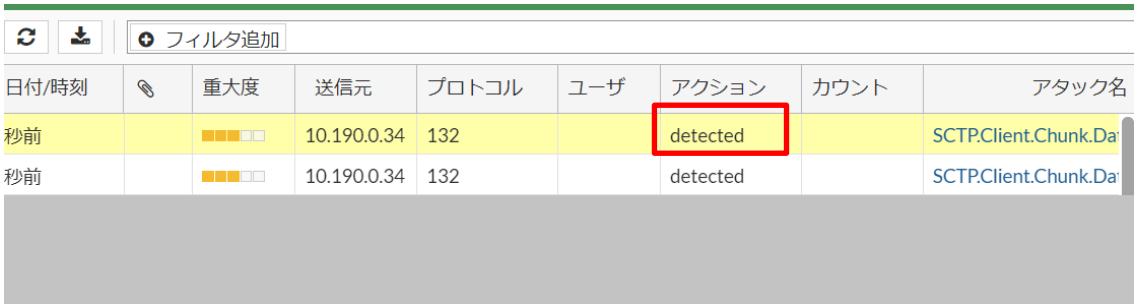
図 5-3-3-3-20 セエ業-2 通信傍受 WAN 側

● SCTP DoS 攻撃の遮断

SCTP DoS 攻撃の検知・遮断を検証するため、AMF へのトラフィック量が閾値を超えた場合に N2 Firewall によって検知・遮断できることを検証しました。具体的には閾値として 2pps を設定し、AMF 宛てに 9pps のトラフィックを発生させ、検知・遮断できることを確認しました。

結果は、GUI にて検知設定時には「detected」、遮断設定時には「dropped」と表示され、いずれにおいても 7 回分のパケットが検知・遮断できていることを確認しました。

この結果より、SCTP DoS 攻撃の検知・遮断ができることが確認できました。



フィルタ追加

日付/時刻		重大度	送信元	プロトコル	ユーザ	アクション	カウント	アタック名
秒前			10.190.0.34	132		detected		SCTP.Client.Chunk.Da
秒前			10.190.0.34	132		detected		SCTP.Client.Chunk.Da

図 5-3-3-3-21-1 セエ業-2 DoS 攻撃 検知①

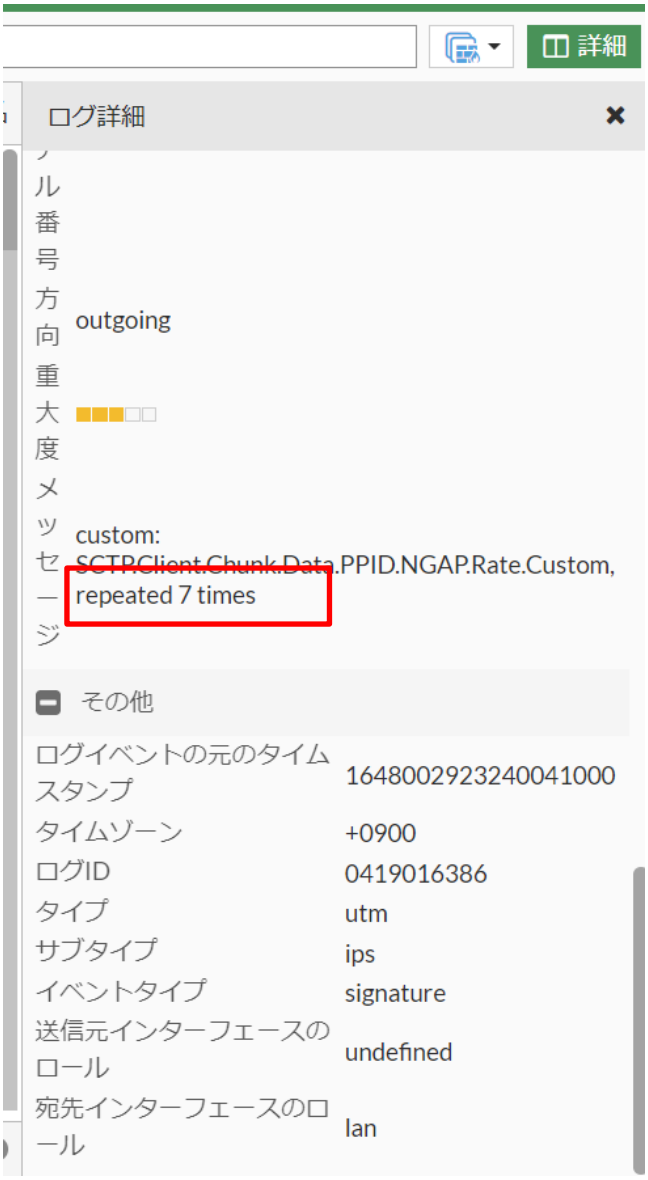


図 5-3-3-3-21-2　セエ業-2 DoS 攻撃 検知②

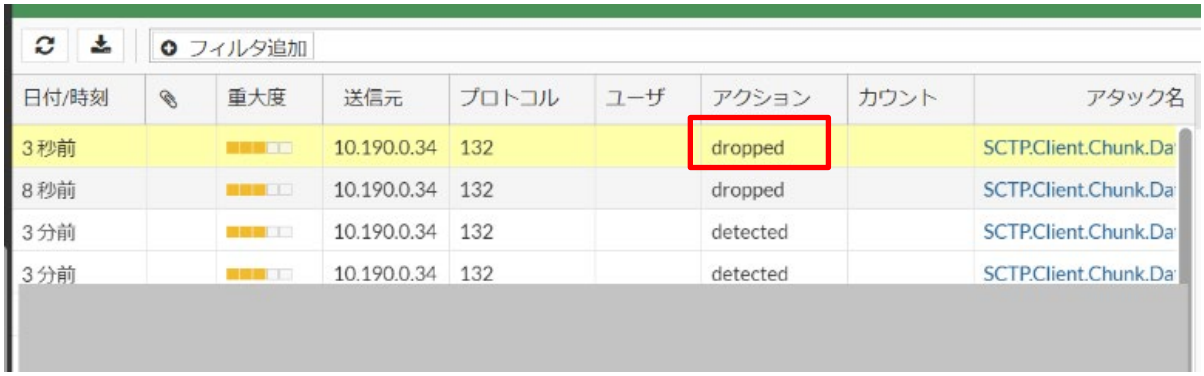


図 5-3-3-3-22-1　セエ業-2 DoS 攻撃　遮断①

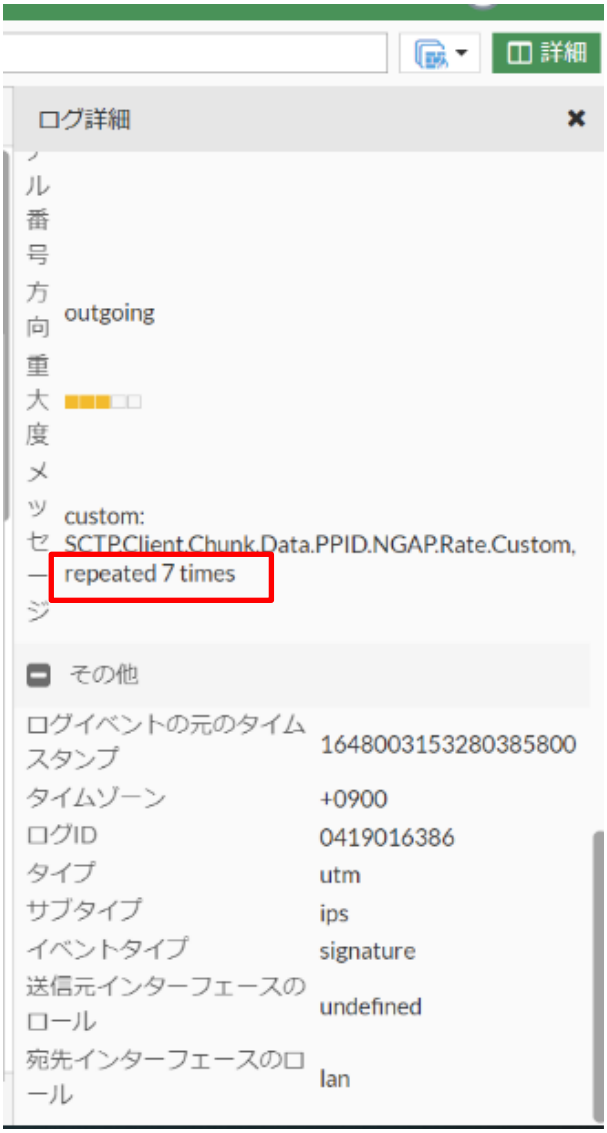


図 5-3-3-3-22-2　セエ業-2 DoS 攻撃　遮断②

● 不正な N2 信号の検知と遮断

不正な N2 信号を送信し、N2 Firewall によって検知・遮断できることを確認しました。具体的には不正な N2 信号として不正な ppid 値(0)をセットしたパケットを AMF 宛てに送信し、N2 Firewall にて検知・遮断できることを確認しました。

結果は、CLI にて検知設定時には「pass」、遮断設定時には「reset」と表示され、検知・遮断ができていることを確認しました。

この結果より、不正な N2 信号の検知・遮断ができることが確認できました。

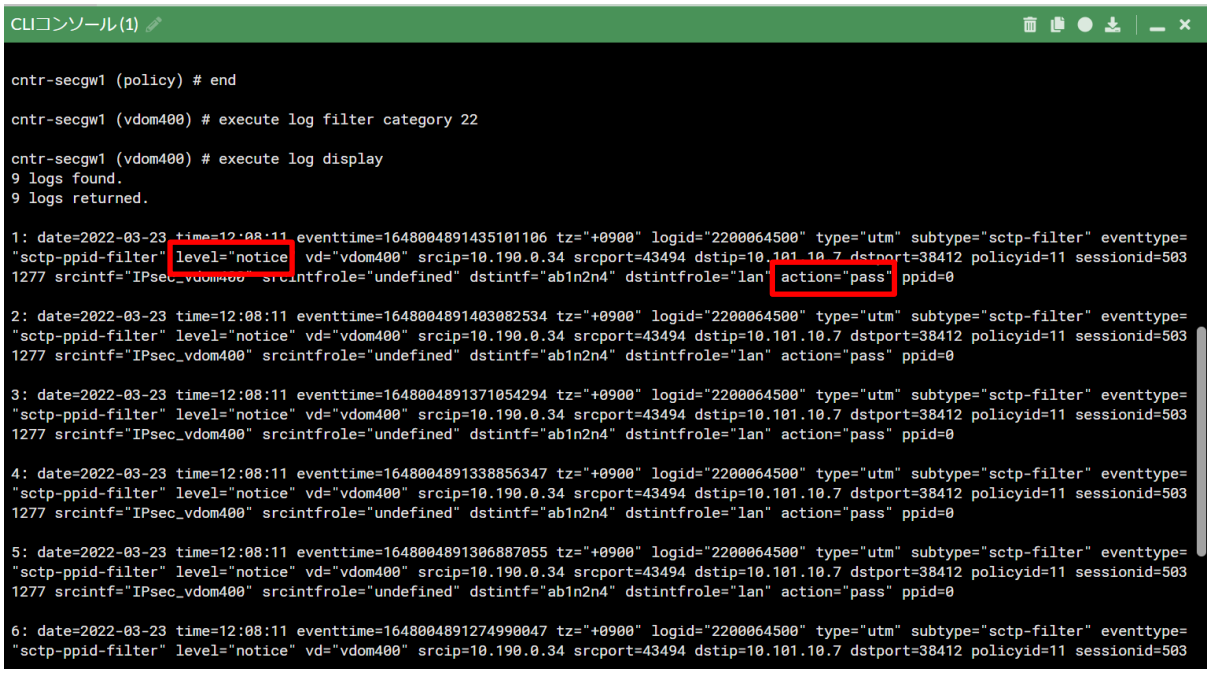


図 5-3-3-3-23 セエ業-2 不正な N2 信号 検知

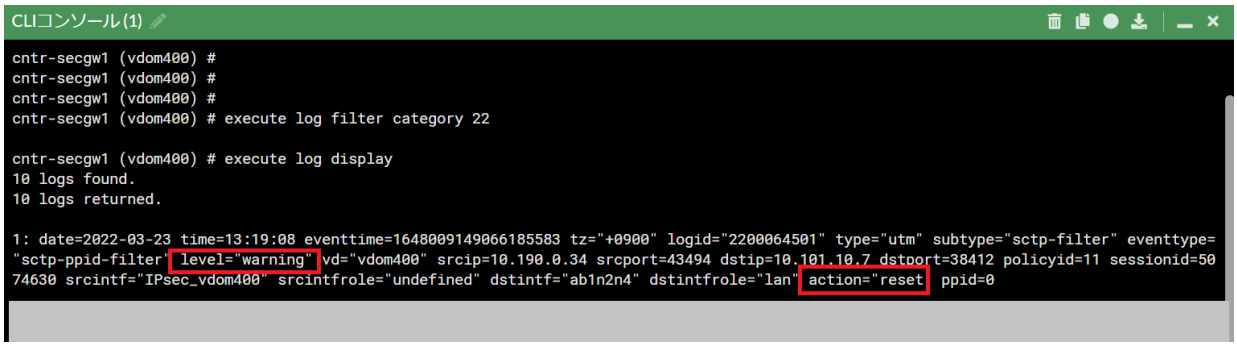


図 5-3-3-3-24 セエ業-2 不正な N2 信号 遮断

セエ業-3：N4 Firewall の評価

- UPF 上のセッション情報の書き換えおよび削除の検知・遮断

UPF 宛てにセッション情報の書き換えを行うパケットを送信し、N4 Firewall によって攻撃を検知・遮断する検証を行いました。具体的には SMF を偽装する疑似 SMF から拠点側の UPF 宛てにセッションを削除する攻撃を行い、検知・遮断ができていることを確認しました。

GUI にて該当パケットが検知設定時には「forwarded」、遮断設定時には「prohibited」となっていることを確認しました。

また、攻撃を遮断しなかった場合にセッションが切れることを、拠点 UE 下部の端末から UPF 宛ての ping で確認し、検知設定時のみ ping が切れることを確認しました。

この結果より、UPF 上のセッション情報の書き換えおよび削除の検知・遮断ができることが確認できました。

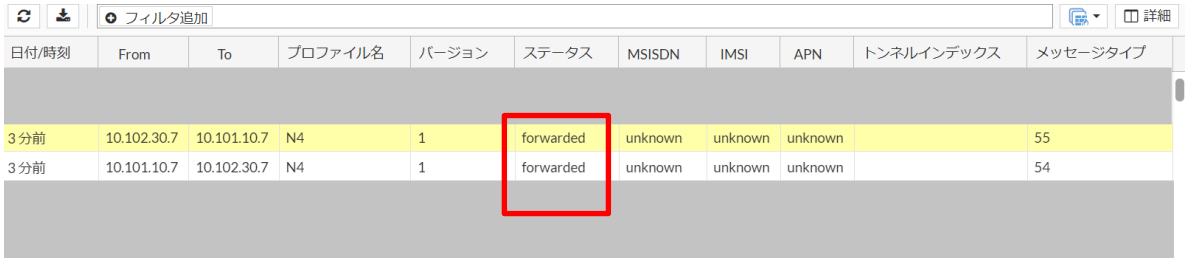


図 5-3-3-3-25 セエ業-3 セッション削除 検知

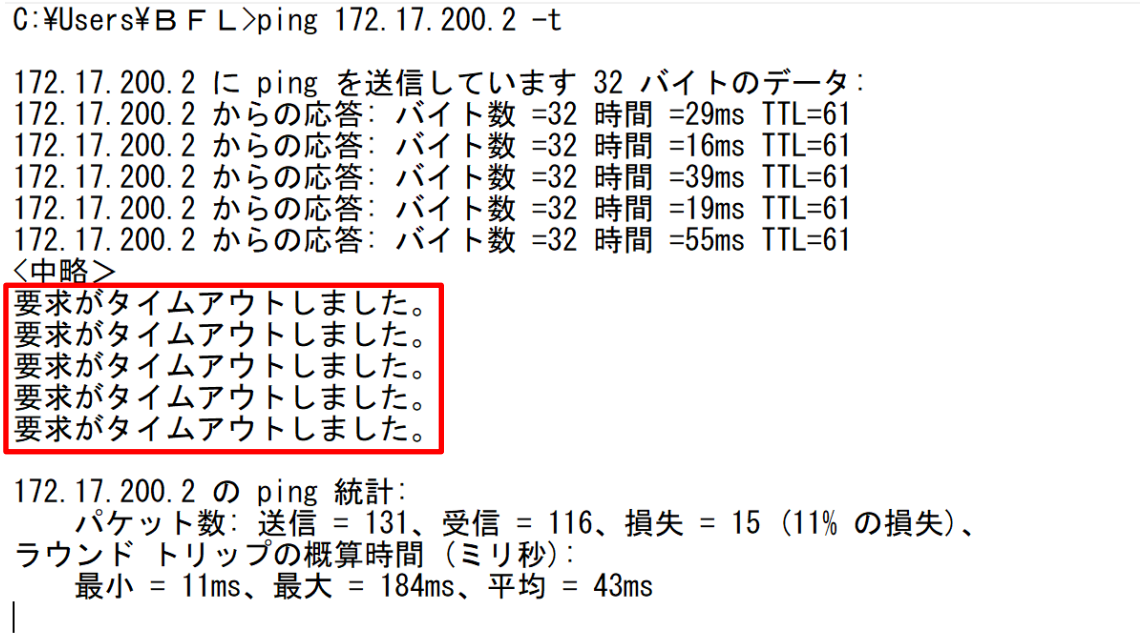


図 5-3-3-3-26 セエ業-3 セッション削除時 ping

図 5-3-3-3-27 セエ業-3 セッション削除 遮断

● 不正な PFCP 信号の検知・遮断

UPF 宛てに不正な PFCP 信号を送信し、N4 Firewall によって攻撃を検知・遮断する検証を行いました。具体的には SMF を偽装する疑似 SMF から拠点側の UPF 宛てに不正な Message Type(254)をセットしたパケットを送信し、N4 Firewall にて検知・遮断ができていることを確認しました。

結果は、GUI にてメッセージタイプ 254 が届いた際、検知設定時には「prohibitted monitor」、遮断設定時には「prohibited」と表示され検知・遮断できていることを確認しました。

この結果より、不正な PFCP 信号の検知・遮断ができることが確認できました。

図 5-3-3-3-28 セエ業-3 不正な PFCP 検知

図 5-3-3-3-29 セエ業-3 不正な PFCP 遮断

セエ業-4：SBA Firewall の評価

- 5G コア内の OpenAPI 通信のモニタリング

http2/tls1.2 によって行われる NRF への SBI 通信をテナント毎にモニタリングできることを確認しました。複数企業共用パターンである NTT 中央研修センタ(NRF-policy1)および東北大学(NRF-policy3)のそれぞれについて GUI ログをフィルタリングし、該当のテナントの情報のみを抽出できることを確認しました。また、同様に http2/tls1.2 の通信のみをフィルタリングできることを確認しました。

この結果より、5G コア内の OpenAPI 通信がモニタリングできることが確認できました。

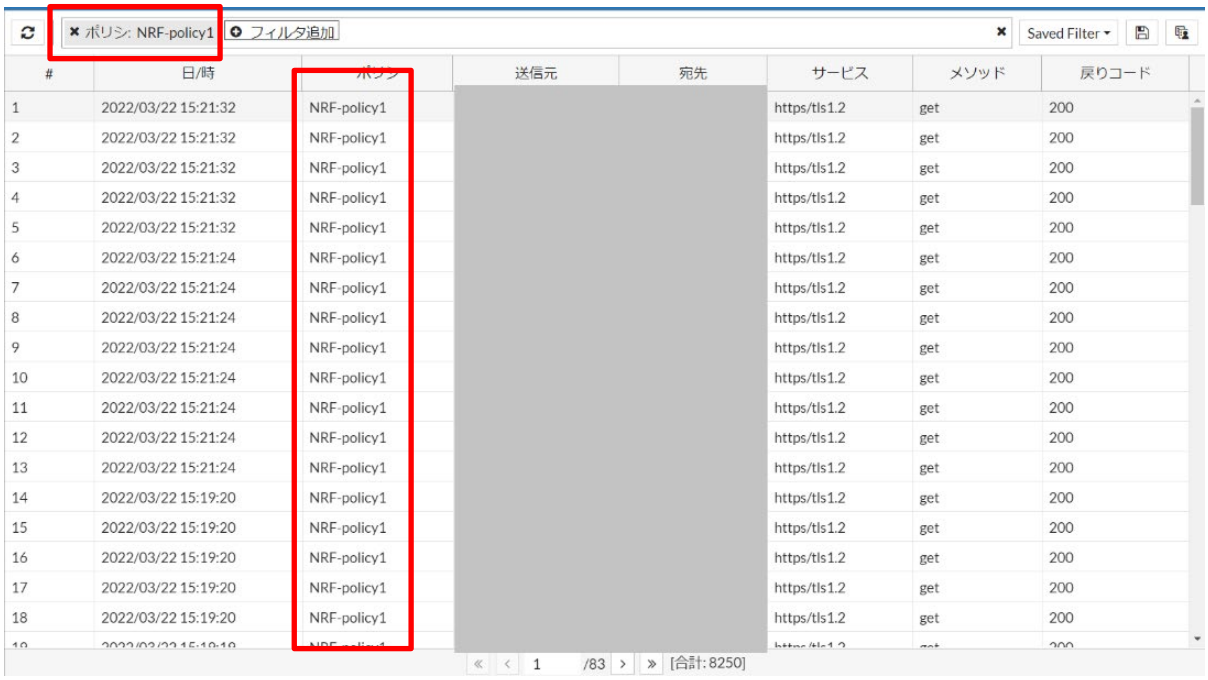


図 5-3-3-3-30 セエ業-4 OpenAPI モニタリング NTT 中央研修センタ

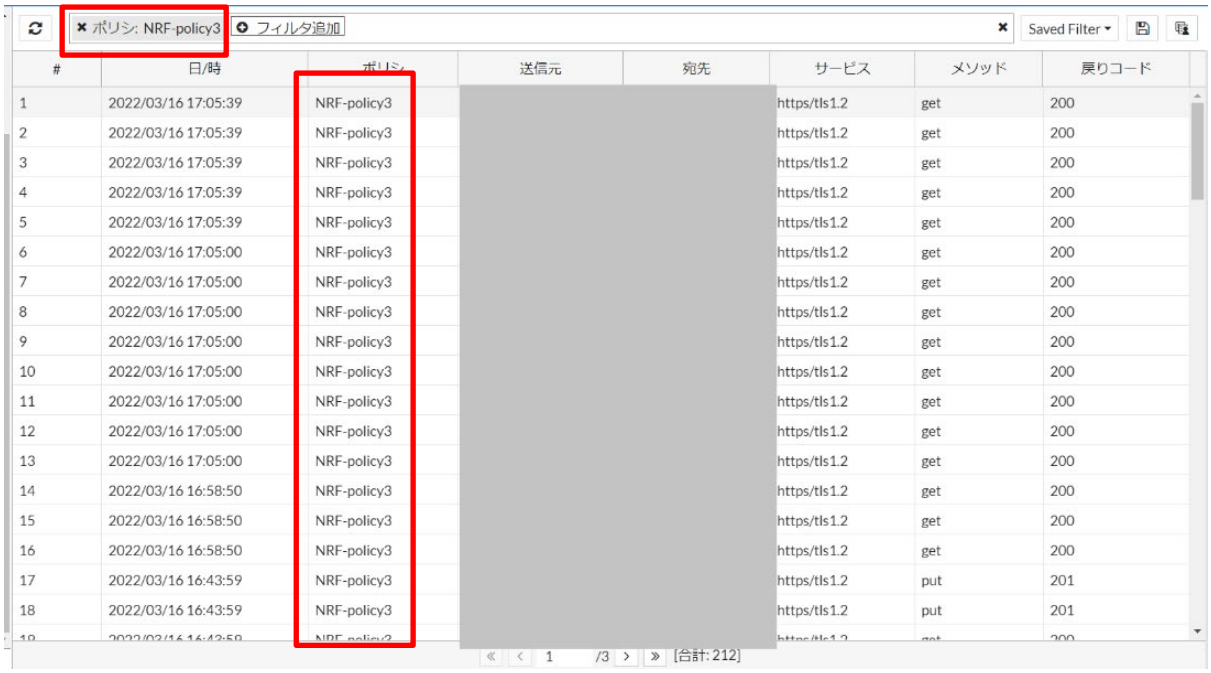


図 5-3-3-3-31 セエ業-4 OpenAPI モニタリング 東北大学

図 5-3-3-3-32 セエ業-4 OpenAPI モニタリング http/tls1.2

- 5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断

NRF への OpenAPI を使用した DoS 攻撃を SBA Firewall にて検知・遮断する検証を行いました。具体的には NRF 宛てに不正な API 通信として長大な URL の http リクエストを送信し、

SBA Firewall にて検知・遮断ができることを確認しました。

結果は、GUI にて検知設定時には「Alert」、遮断設定時には「403 Forbidden エラー」を返していることと、128Byte 以上の長大な URL のリクエストを検知・遮断した旨のメッセージを確認しました。

この結果より、5G コア内におけるバッファオーバーフロー等による DoS 攻撃の検知・遮断ができることが確認できました。

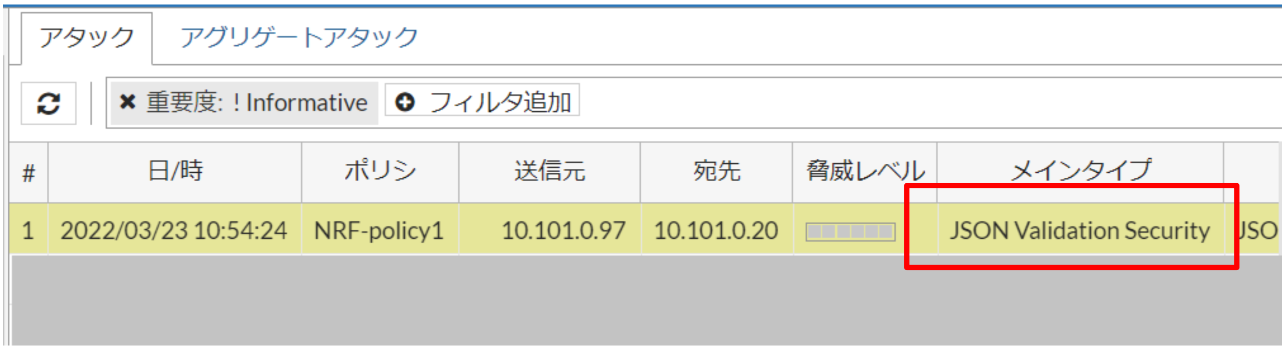


図 5-3-3-3-33-1 セエ業-4 バッファオーバーフロー 検知①

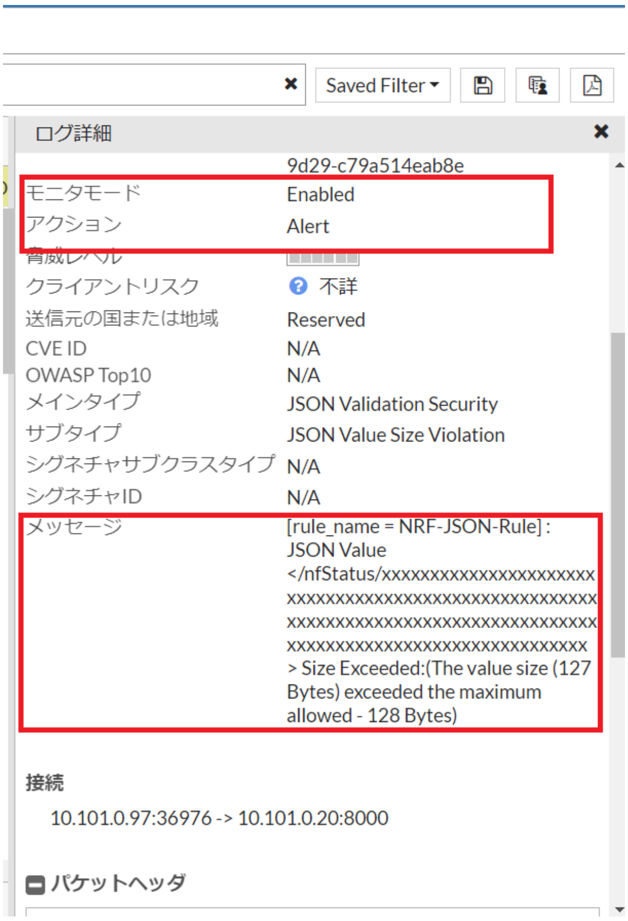


図 5-3-3-3-33-2 セエ業-4 バッファオーバーフロー 検知②

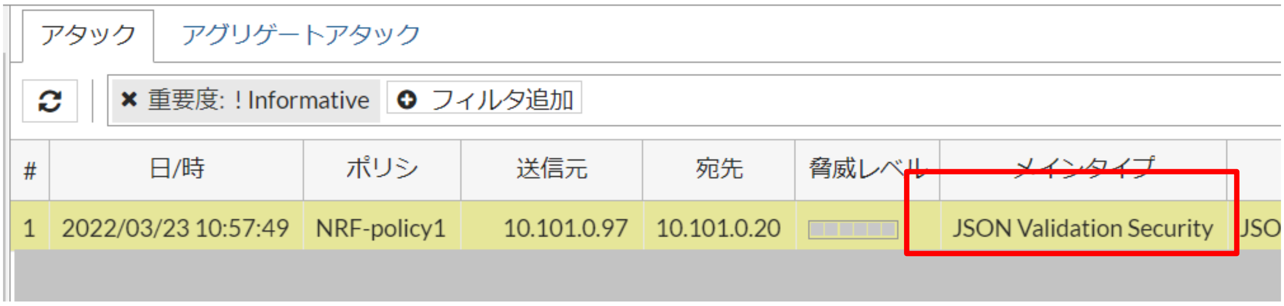


図 5-3-3-3-34-1 セエ業-4 バッファオーバーフロー 遮断①

図 5-3-3-3-34-2 セエ業-4 バッファオーバーフロー 遮断②

セエ業-5：マルチテナントの評価

- 5G コアマルチテナント間の閉域性の確認

マルチテナントの閉域性を検証するため、異なるテナントのネットワーク情報が独立して管理されていることを確認しました。具体的には NTT 中央研修センタ（vdom400）のルー

ティングテーブル、GTP-U セッション、SCTP セッション、PFCP セッションの情報にいすゞ自動車(vdom500)の情報が含まれないことを確認しました。

この結果より、5G コアマルチテナント間の閉域性が確認できました。

```
cntr-secgw1 (vdom400) # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via IPsec_vdom400 tunnel 10.190.0.2
C       10.101.10.0/24 is directly connected, ab1n2n4
C       10.101.20.0/24 is directly connected, ab1n3
C       10.101.30.0/24 is directly connected, ab1n4
S       10.190.0.0/30 [10/0] via 10.190.0.9, ab1wan
C       10.190.0.8/30 is directly connected, ab1wan
S       10.190.0.12/30 [5/0] via IPsec_vdom400 tunnel 10.190.0.2
C       10.190.0.13/32 is directly connected, IPsec_vdom400
```

図 5-3-3-3-35-1 セエ業-5 マルチテナント①

```
cntr-secgw1 (vdom400) # get system session list
PROTO    EXPIRE SOURCE            SOURCE-NAT        DESTINATION      DESTINATION-NAT
sctp     3582   10.190.0.34:38413 -                  10.101.10.7:38412 -
udp      173    10.101.10.7:8805 -                   10.102.30.7:8805 -
```

図 5-3-3-3-35-2 セエ業-5 マルチテナント②

```
cntr-secgw1 (vdom400) # diagnose ip arp list
index=46 ifname=ab1wan 10.190.0.9 d4:eb:68:53:ac:ef state=00000002 use=491 confirm=990 update=990 ref=3
index=25 ifname=vdom400 0.0.0.0 00:00:00:00:00:00 state=00000040 use=61116131 confirm=61122131 update=61116131 ref=1
index=66 ifname=IPsec_vdom400 0.0.0.0  state=00000040 use=213698 confirm=219698 update=213698 ref=4
index=47 ifname=ab1n2n4 10.101.10.7 00:0c:29:28:00:1f state=00000002 use=491 confirm=122 update=122 ref=3
```

図 5-3-3-3-35-3 セエ業-5 マルチテナント③

エンド拠点 UPF を使用した場合の業界共用パターンの検証結果を以下にまとめます。いずれの項目においても検証内容に対し、検知・遮断ができることが確認できました。

表 5-3-3-3-5 検証結果まとめ（エンド拠点 UPF 業界共用パターン）

評価項目	検証内容	結果
SecGW の評価	不正拠点から５G コアへの接続	○
N2 Frewall の評価	CellSiteRouter と SecGW 間での通信傍受の防止	○
	SCTP　DoS 攻撃の遮断	○
	不正な N2 信号の検知と遮断	○
N4 Frewall の評価	UPF 上のセッション情報の書き換え及び削除の検知・遮断	○
	不正な PFCP 信号の検知・遮断	○
SBA Firewall の評価	5G コア内の OpenAPI 通信のモニタリング	○

	5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断	○
マルチテナントの評価	5G コアマルチテナント間の閉域性の確認	○

イ　センタ拠点に設置した UPF を使用する構成

(ア)複数企業共用パターン

センタ拠点に設置した UPF を使用する構成の複数企業共用パターンにおける検証項目と該当する攻撃の対応は「表 5-3-3-3-6　検証項目と該当する攻撃（センタ拠点 UPF 複数企業共用パターン)」のとおりです。

なお、「表 5-3-3-2-1　検証項目(エンド UPF)」のとおり「SecGW の評価」は「複数企業共用パターン」においては対象外とします。

表 5-3-3-3-6 検証項目と該当する攻撃（センタ拠点 UPF 複数企業共用パターン）

項番	評価項目	検証項目	該当する攻撃
セセ複-1	N2 Firewall の評価	CellSiteRouter と SecGW 間での通信傍受の防止	N2 通信の傍受
		SCTP　DoS 攻撃の遮断	同一 N2 リクエストを大量送信する DoS 攻撃
		不正な N2 信号の検知と遮断	AMF への不正な N2 信号の送信
セセ複-2	N3 Firewall の評価	中間者攻撃、不正な GTP-U パケットの検知と遮断	UPF への不正な GTP-U パケットの送信
セセ複-3	N4 Firewall の評価	UPF 上のセッション情報の書き換え及び削除の検知・遮断	センタ UPF に対するセッション情報の危険リクエストの送信
		不正な PFCP 信号の検知・遮断	センタ UPF に対する不正な N2 リクエストの送信
セセ複-4	SBA Firewall の評価	5G コア内の OpenAPI 通信のモニタリング機能の確認	
		5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断	NRF に対するバッファオーバーフローを引き起こす http リクエストの送信
セセ複-5	マルチテナントの評価	5G コアマルチテナント間の閉域性の確認	

検証の手順・結果の詳細を以下にまとめます。

各図における IP アドレスは構成の一例です。また、検証結果に関係のない表示をトリミ

ングしています。

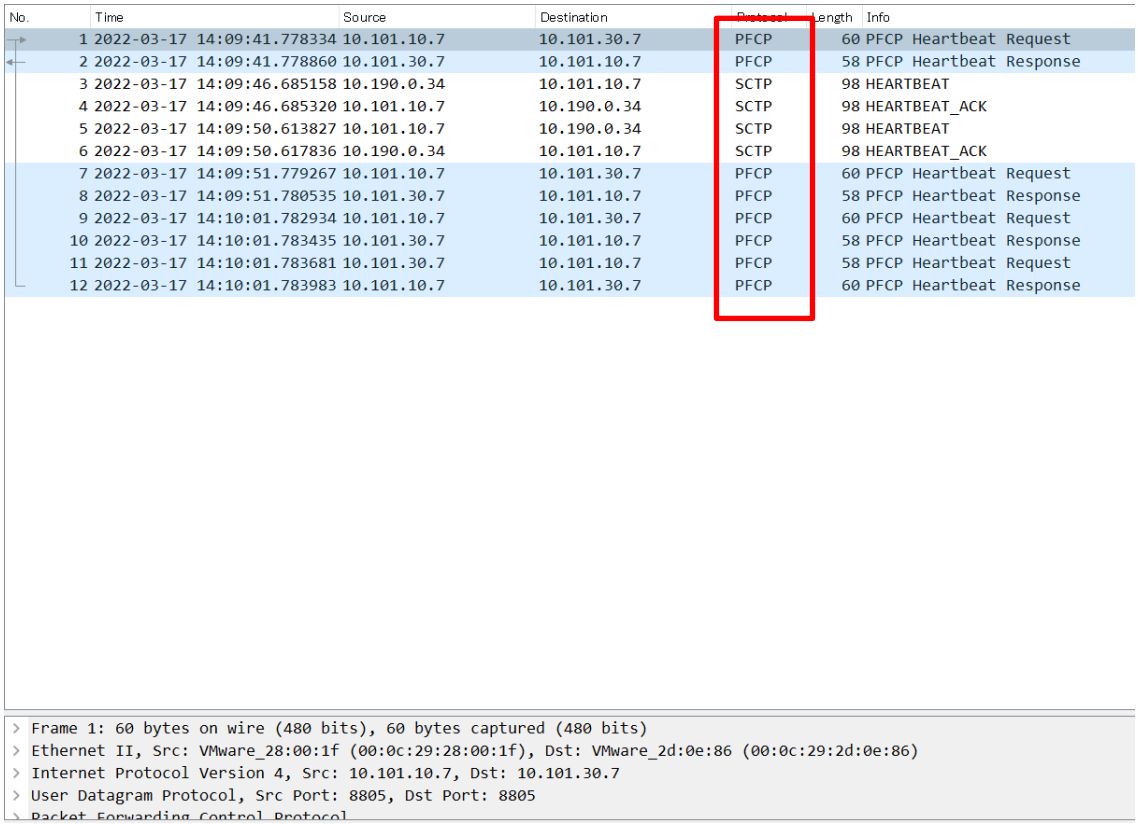
セセ複-1：N2 Firewall の評価

- CellSiteRouter と SecGW 間での通信傍受の防止

SecGW により WAN 区間における N2 通信が暗号化され傍受できないことを確認するため、SecGW の 5GC 側と WAN 側においてトラフィックキャプチャを行いました。

結果は、5GC 側では PFCP、SCTP の通信が平文で見える一方、WAN 側では ESP(IPSec による暗号化)と表示されることを確認し、WAN 区間では IPSec による通信の暗号化がされていることが確認できました。

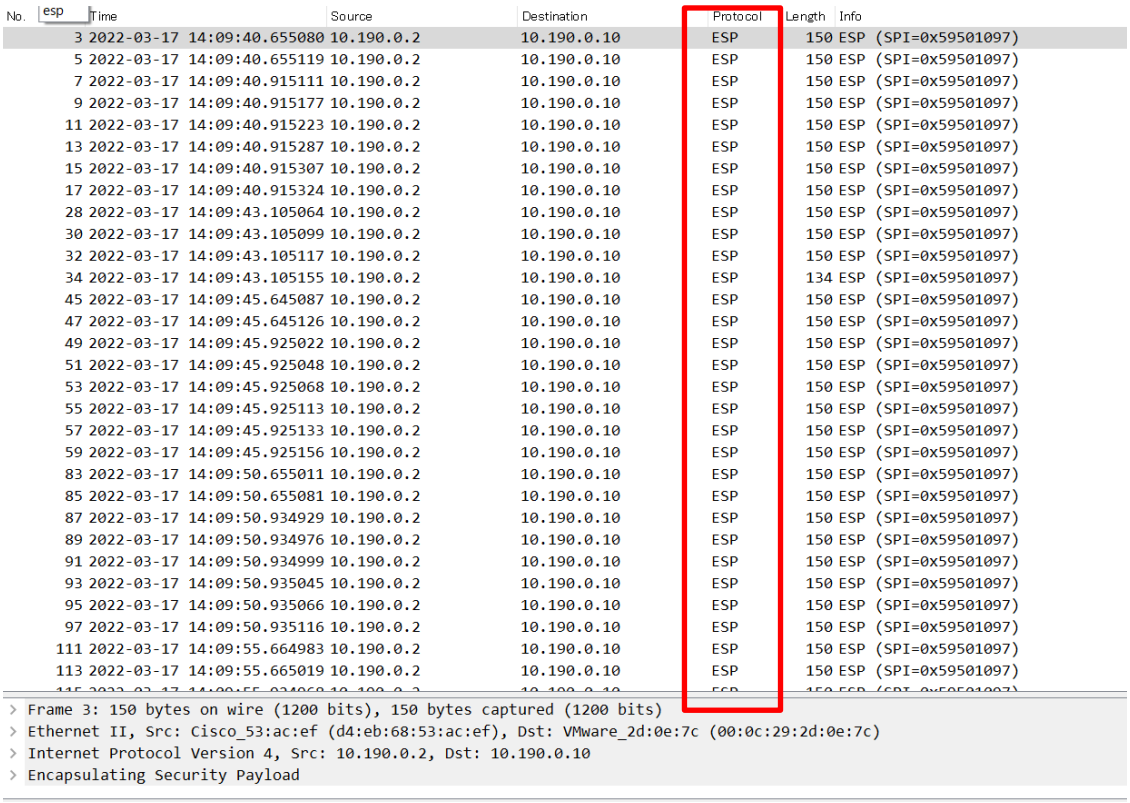
この結果より、CellSiteRouter と SecGW 間での通信傍受が防止できることが確認できました。



No.	Time	Source	Destination	Protocol	Length	Info
1	2022-03-17 14:09:41.778334	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
2	2022-03-17 14:09:41.778860	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
3	2022-03-17 14:09:46.685158	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT
4	2022-03-17 14:09:46.685320	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT_ACK
5	2022-03-17 14:09:50.613827	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT
6	2022-03-17 14:09:50.617836	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT_ACK
7	2022-03-17 14:09:51.779267	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
8	2022-03-17 14:09:51.780535	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
9	2022-03-17 14:10:01.782934	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
10	2022-03-17 14:10:01.783435	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
11	2022-03-17 14:10:01.783681	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Request
12	2022-03-17 14:10:01.783983	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Response

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: VMware_28:00:1f (00:0c:29:28:00:1f), Dst: VMware_2d:0e:86 (00:0c:29:2d:0e:86)
> Internet Protocol Version 4, Src: 10.101.10.7, Dst: 10.101.30.7
> User Datagram Protocol, Src Port: 8805, Dst Port: 8805
> Packet Forwarding Control Protocol
```

図 5-3-3-3-36 セセ複-1 通信傍受 5GC 側



No.	Time	Source	Destination	Protocol	Length	Info
3	2022-03-17 14:09:40.655080	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
5	2022-03-17 14:09:40.655119	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
7	2022-03-17 14:09:40.915111	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
9	2022-03-17 14:09:40.915177	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
11	2022-03-17 14:09:40.915223	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
13	2022-03-17 14:09:40.915287	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
15	2022-03-17 14:09:40.915307	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
17	2022-03-17 14:09:40.915324	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
28	2022-03-17 14:09:43.105064	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
30	2022-03-17 14:09:43.105099	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
32	2022-03-17 14:09:43.105117	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
34	2022-03-17 14:09:43.105155	10.190.0.2	10.190.0.10	ESP	134	ESP (SPI=0x59501097)
45	2022-03-17 14:09:45.645087	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
47	2022-03-17 14:09:45.645126	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
49	2022-03-17 14:09:45.925022	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
51	2022-03-17 14:09:45.925048	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
53	2022-03-17 14:09:45.925068	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
55	2022-03-17 14:09:45.925113	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
57	2022-03-17 14:09:45.925133	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
59	2022-03-17 14:09:45.925156	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
83	2022-03-17 14:09:50.655011	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
85	2022-03-17 14:09:50.655081	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
87	2022-03-17 14:09:50.934929	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
89	2022-03-17 14:09:50.934976	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
91	2022-03-17 14:09:50.934999	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
93	2022-03-17 14:09:50.935045	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
95	2022-03-17 14:09:50.935066	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
97	2022-03-17 14:09:50.935116	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
111	2022-03-17 14:09:55.664983	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)
113	2022-03-17 14:09:55.665019	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59501097)

図 5-3-3-3-37 セセ複-1 通信傍受 WAN 側

● SCTP DoS 攻撃の遮断

SCTP DoS 攻撃の検知・遮断を検証するため、AMF へのトラフィック量が閾値を超えた場合に N2 Firewall によって検知・遮断できることを検証しました。具体的には閾値として 2pps を設定し、AMF 宛てに 9pps のトラフィックを発生させ、検知・遮断できることを確認しました。

結果は、GUI にて検知設定時には「detected」、遮断設定時には「dropped」と表示され、いずれにおいても 7 回分のパケットが検知・遮断できていることを確認しました。

この結果より、SCTP DoS 攻撃の検知・遮断ができることが確認できました。

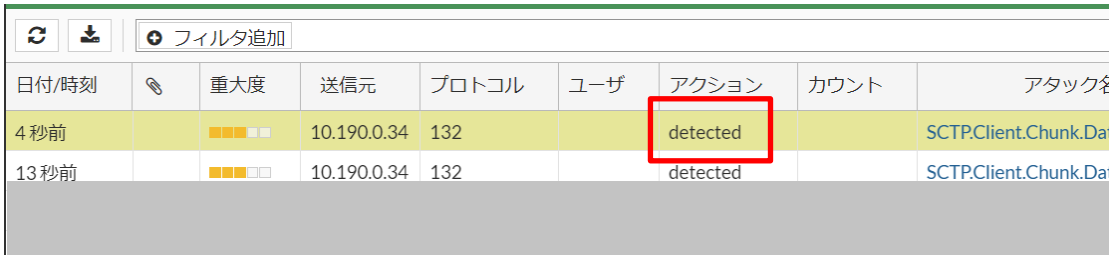


図 5-3-3-3-38-1 セセ複-1 DoS 攻撃 検知①

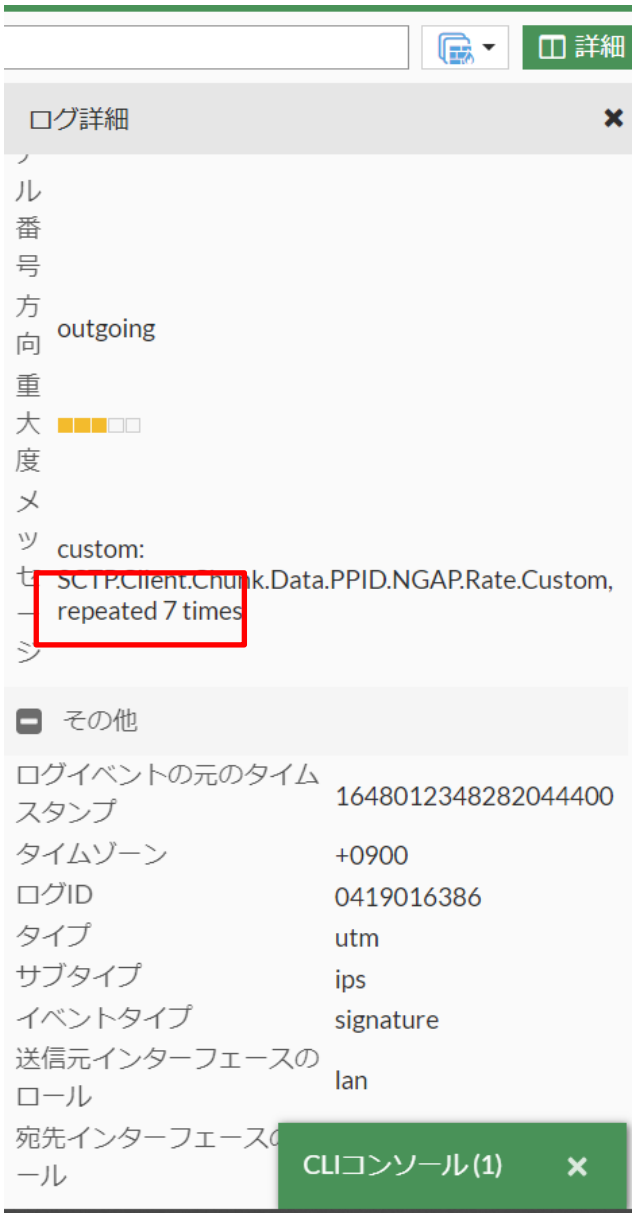


図 5-3-3-3-38-2 セセ複-1 DoS 攻撃 検知②

図 5-3-3-3-39-1 セセ複-1 DoS 攻撃 遮断①

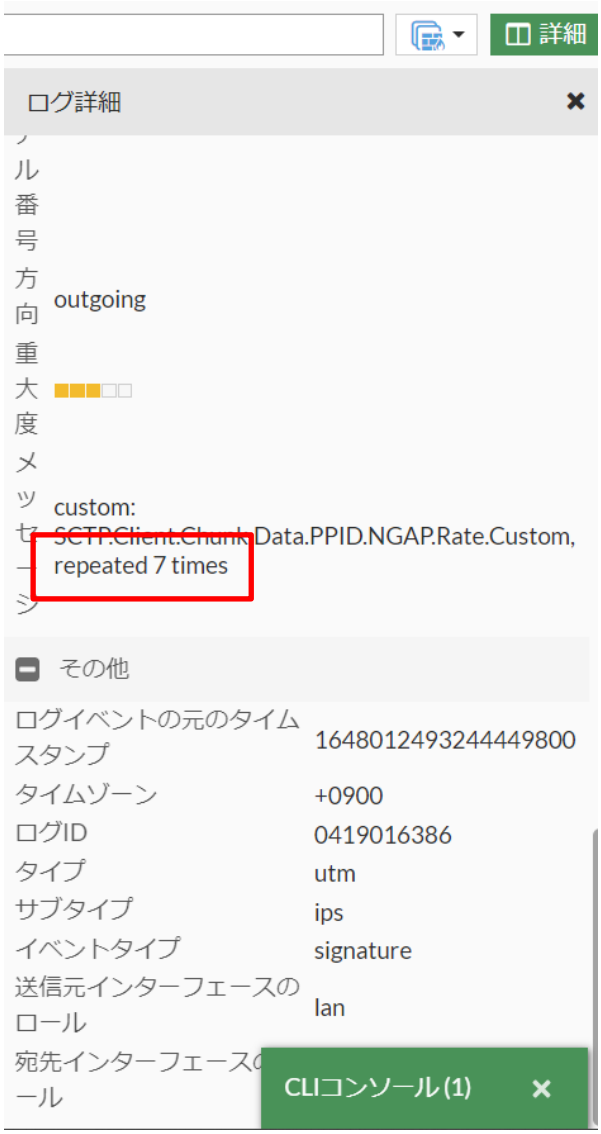


図 5-3-3-3-39-2 セセ複-1 DoS 攻撃 遮断②

● 不正な N2 信号の検知と遮断

不正な N2 信号を送信し、N2 Firewall によって検知・遮断できることを確認しました。具体的には不正な N2 信号として不正な ppid 値(0)をセットしたパケットを AMF 宛てに送信し、N2 Firewall にて検知・遮断できることを確認しました。

結果は、CLI にて検知設定時には「pass」、遮断設定時には「reset」と表示され、検知・遮断ができていることを確認しました。

この結果より、不正な N2 信号の検知と遮断ができることが確認できました。

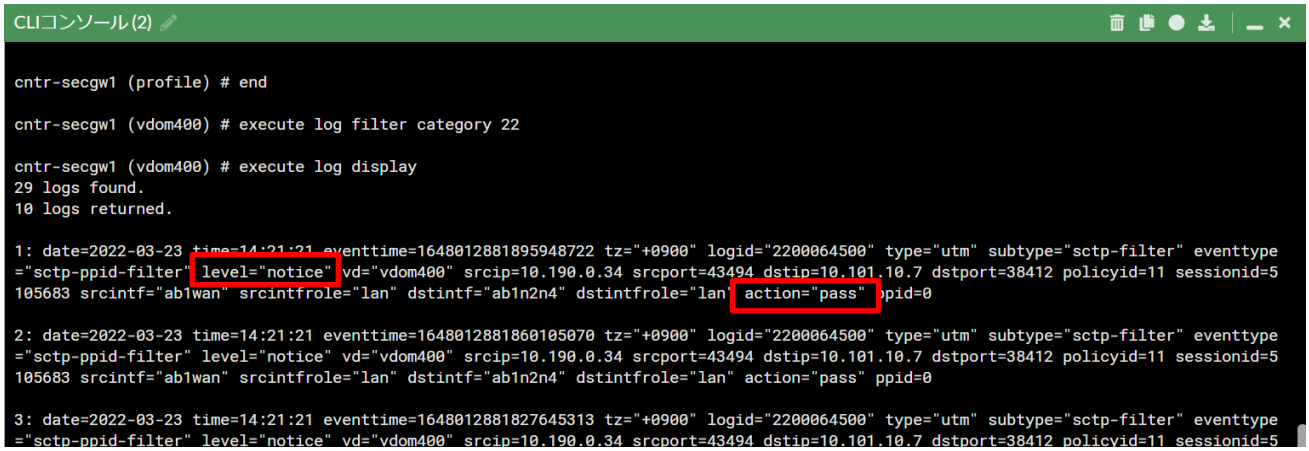


図 5-3-3-3-40 セセ複-1 不正な N2 信号 検知

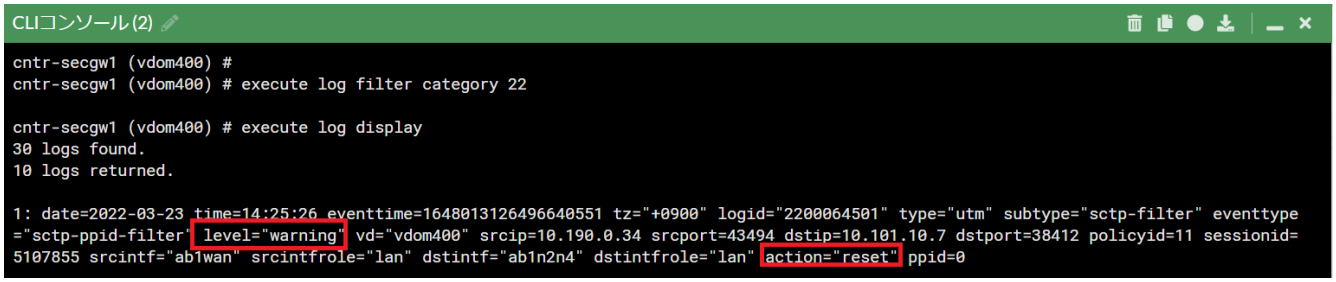


図 5-3-3-3-41 セセ複-1 不正な N2 信号 遮断

セセ複-2：N3 Firewall の評価

● 中間者攻撃、不正な GTP-U パケットの検知と遮断

不正な GTP-U パケットを UPF に送信する攻撃を N3 Firewall にて遮断できることを確認しました。具体的には一度確立されたセッションを終了させた後、そのセッション宛てのパケットを送ることで中間者攻撃を再現し、不正な GTP-U パケットとして遮断されるかを検証しました。

結果は、GUI にて「prohibited」という表示とその理由として「invalid-state」と表示され、遮断されていることを確認できました。

この結果より、不正な GTP-U パケットの検知と遮断ができることが確認できました。

図 5-3-3-3-42-1 セセ複-2 不正な GTP-U パケット 遮断①

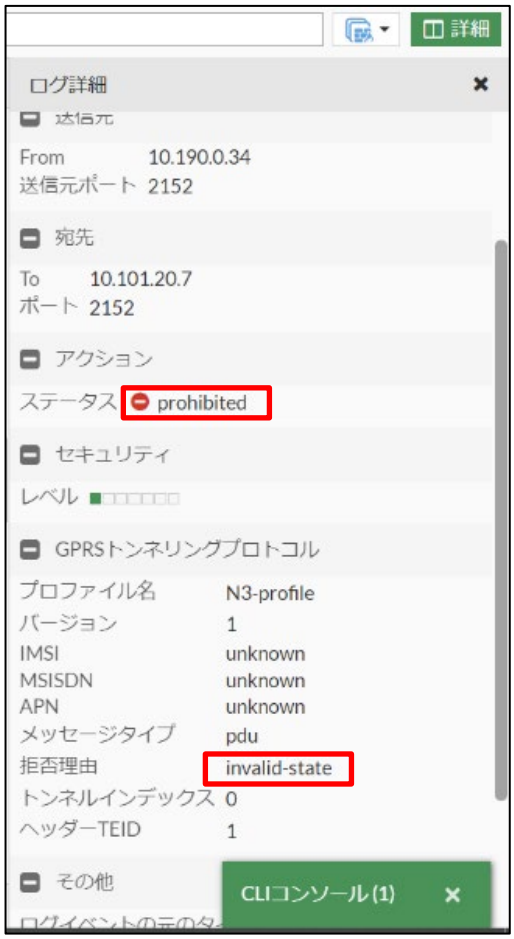


図 5-3-3-3-42-2 セセ複-2 不正な GTP-U パケット 遮断②

セセ複-3：N4 Firewall の評価

- UPF 上のセッション情報の書き換えおよび削除の検知・遮断

UPF 宛てにセッション情報の書き換えを行うパケットを送信し、N4 Firewall によって攻撃を検知・遮断する検証を行いました。具体的には SMF を偽装する疑似 SMF から拠点側の UPF 宛てにセッションを削除する攻撃を行い、検知・遮断ができていることを確認しました。

GUI にて該当パケットが検知設定時には「forwarded」、遮断設定時には「prohibited」となっていることを確認しました。

また、攻撃を遮断しなかった場合にセッションが切れることを、拠点 UE 下部の端末から UPF 宛ての ping で確認し、検知設定時のみ ping が切れることを確認しました。

この結果より、UPF 上のセッション情報の書き換え及び削除の検知・遮断ができることが確認できました。

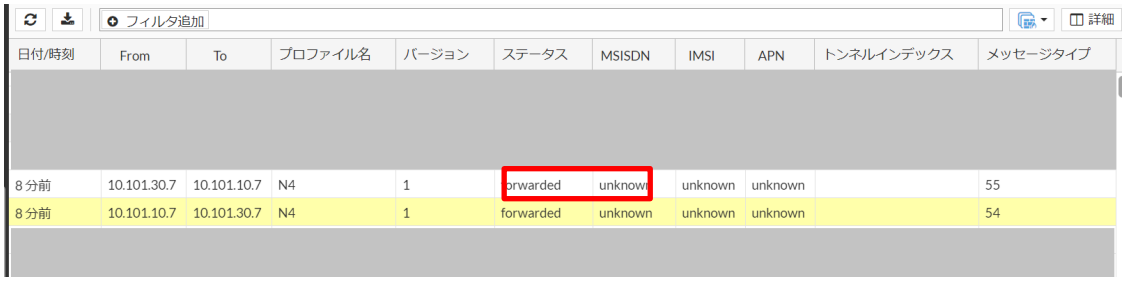


図 5-3-3-3-43 セセ複-3 セッション削除 検知

```
C:¥Users¥ＢＦＬ>ping 172.17.199.2 -t

172.17.199.2 に ping を送信しています 32 バイトのデータ:
172.17.199.2 からの応答: バイト数 =32 時間 =32ms TTL=61
172.17.199.2 からの応答: バイト数 =32 時間 =27ms TTL=61
172.17.199.2 からの応答: バイト数 =32 時間 =44ms TTL=61
172.17.199.2 からの応答: バイト数 =32 時間 =39ms TTL=61
172.17.199.2 からの応答: バイト数 =32 時間 =48ms TTL=61
<中略>
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。

172.17.199.2 の ping 統計:
    パケット数: 送信 = 171、受信 = 138、損失 = 33 (19% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 27ms、最大 = 52ms、平均 = 39ms
```

図 5-3-3-3-44 セセ複-3 セッション削除時 ping

図 5-3-3-3-45-1 セセ複-3 セッション削除 遮断①

図 5-3-3-3-45-2 セセ複-3 セッション削除 遮断②

- 不正な PFCP 信号の検知・遮断

UPF 宛てに不正な PFCP 信号を送信し、N4 Firewall によって攻撃を検知・遮断する検証を行いました。具体的には SMF を偽装する疑似 SMF から拠点側の UPF 宛てに不正な Message Type(254)をセットしたパケットを送信し、N4 Firewall にて検知・遮断ができていることを確認しました。

結果は、GUI にてメッセージタイプ 254 が届いた際、検知設定時には「prohibitted monitor」、遮断設定時には「prohibited」と表示され検知・遮断できていることを確認しました。

この結果より、不正な PFCP 信号の検知・遮断ができることが確認できました。

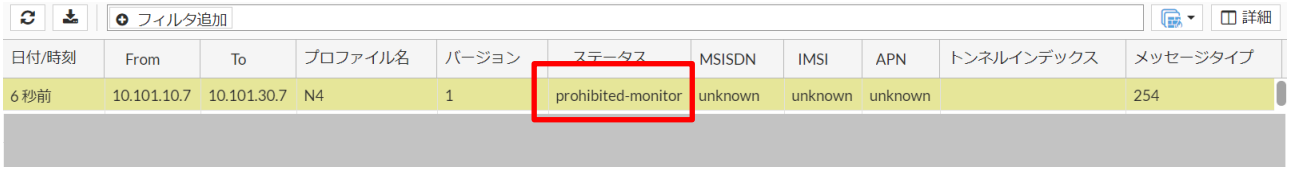


図 5-3-3-3-46 セセ複-3 不正な PFCP 検知

図 5-3-3-3-47 セセ複-3 不正な PFCP 遮断

セエ業-4：SBA Firewall の評価

- 5G コア内の OpenAPI 通信のモニタリング

http2/tls1.2 によって行われる NRF への SBI 通信をテナント毎にモニタリングできることを確認しました。複数企業共用パターンである NTT 中央研修センタ(NRF-policy1)およびいすゞ自動車(NRF-policy2)のそれぞれについて GUI ログをフィルタリングし、該当のテナントの情報のみを抽出できることを確認しました。また、同様に http2/tls1.2 の通信のみをフィルタリングできることを確認しました。

この結果より、5G コア内の OpenAPI 通信のモニタリングができることが確認できました。

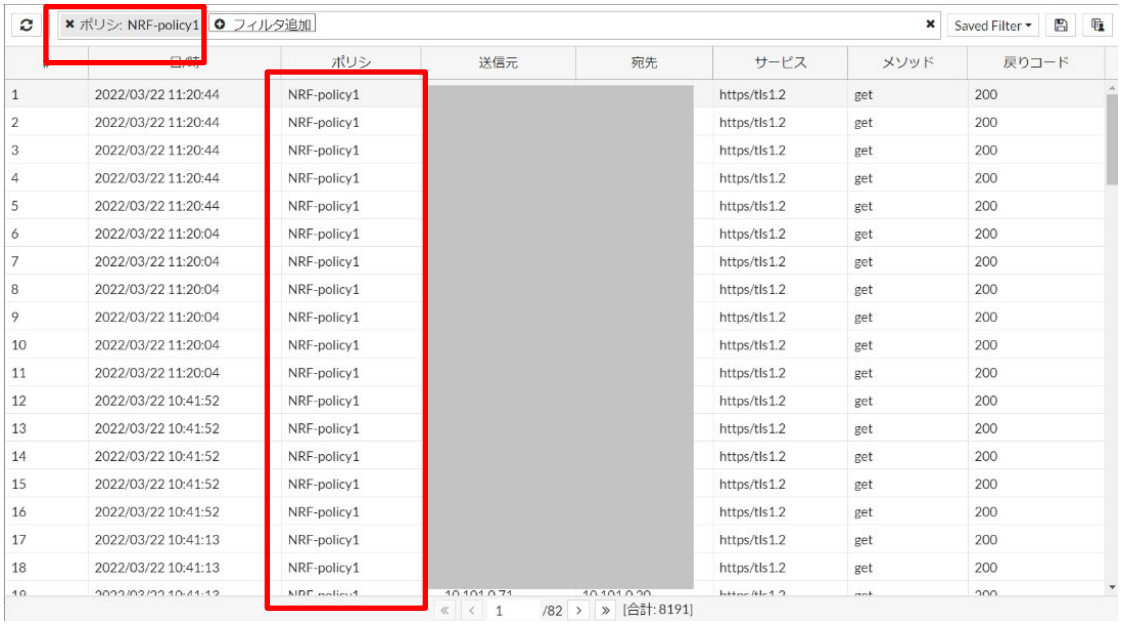


図 5-3-3-3-48 セセ複-4 OpenAPI モニタリング NTT 中央研修センタ

図 5-3-3-3-49 セセ複-4 OpenAPI モニタリング いすゞ自動車

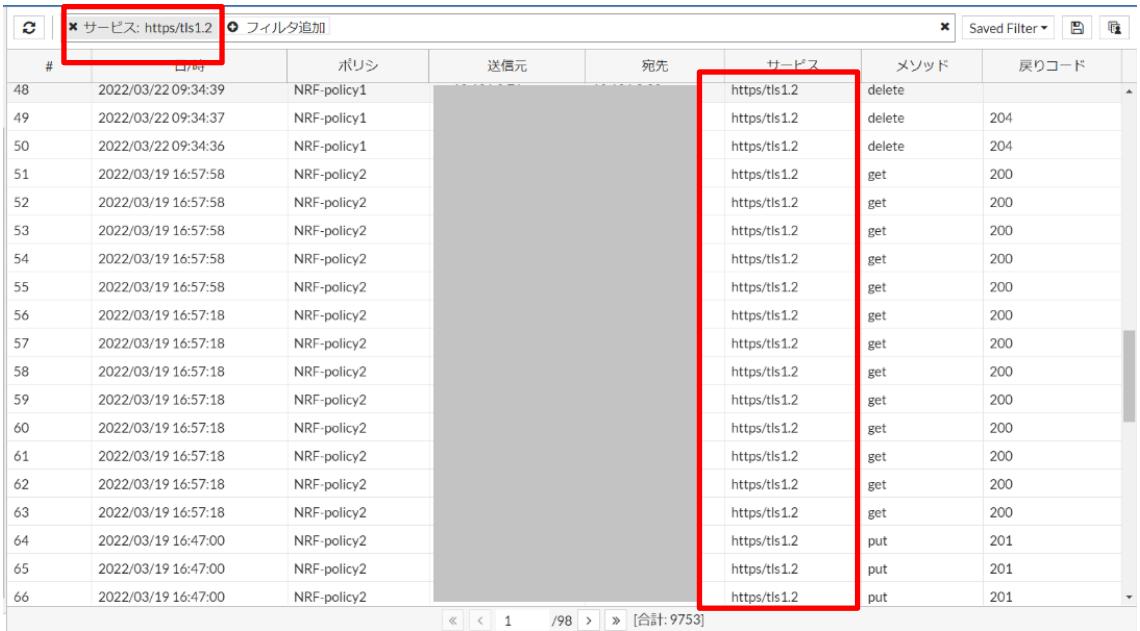


図 5-3-3-3-50 セセ複-4 OpenAPI モニタリング http/tls1.2

- 5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断

NRF への OpenAPI を使用した DoS 攻撃を SBA Firewall にて検知・遮断する検証を行いました。具体的には NRF 宛てに不正な API 通信として長大な URL の http リクエストを送信し、

SBA Firewall にて検知・遮断ができることを確認しました。

結果は、GUI にて検知設定時には「Alert」、遮断設定時には「403 Forbidden エラー」を返していることと、128Byte 以上の長大な URL のリクエストを検知・遮断した旨のメッセージを確認しました。

この結果より、5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断ができることが確認できました。

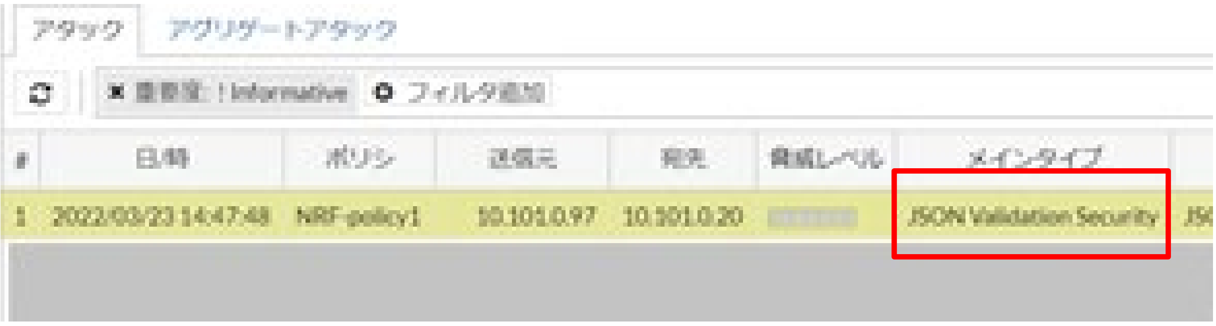


図 5-3-3-3-51-1 セセ複-4 バッファオーバーフロー 検知①

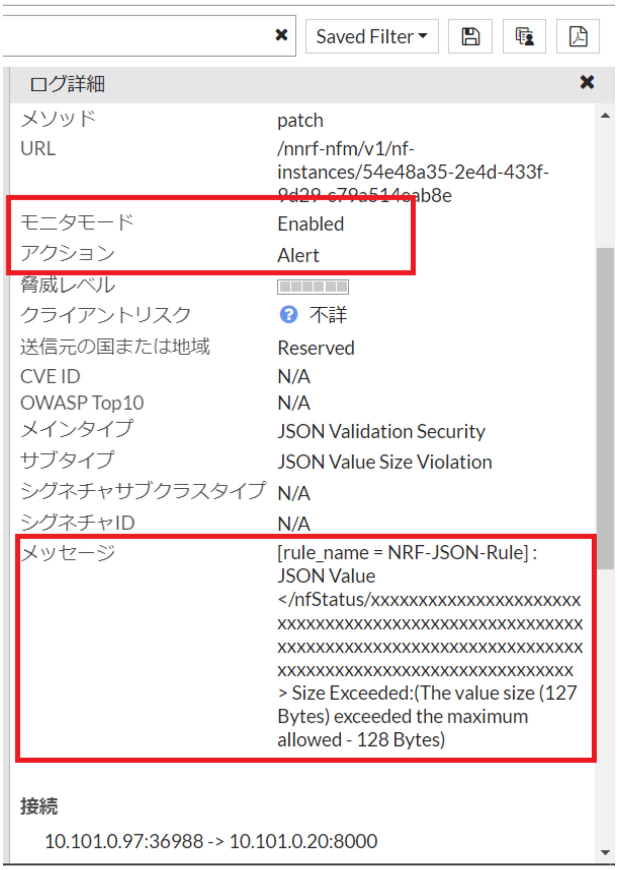


図 5-3-3-3-51-2 セセ複-4 バッファオーバーフロー 検知②

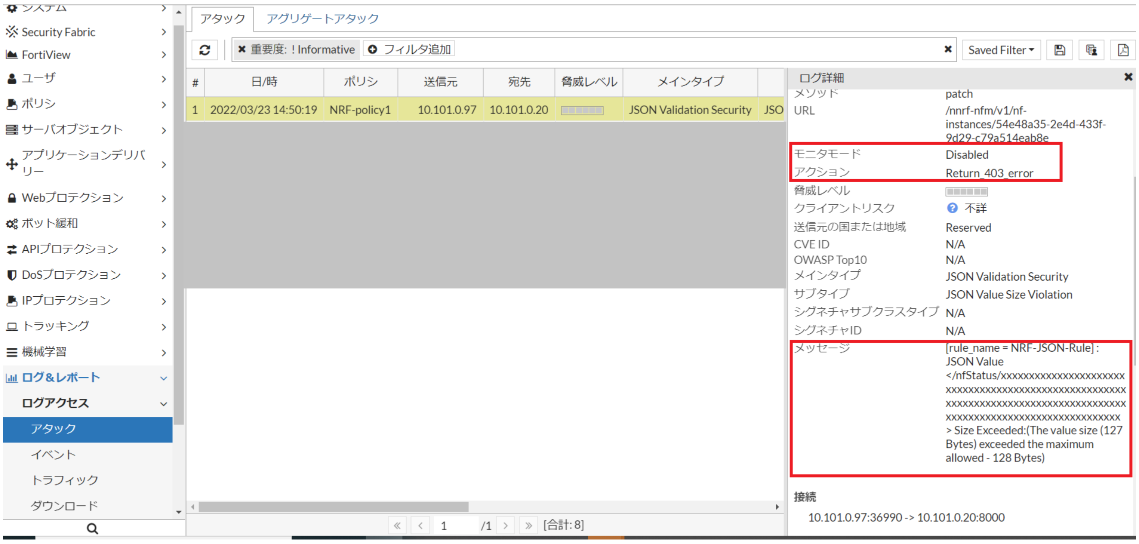


図 5-3-3-3-52 セセ複-4 バッファオーバーフロー 遮断

セセ業-5：マルチテナントの評価

● 5G コアマルチテナント間の閉域性の確認

マルチテナントの閉域性を検証するため、異なるテナントのネットワーク情報が独立して管理されていることを確認しました。具体的には NTT 中央研修センタ(vdom400、10.190.0.0/24)のルーティングテーブル、GTP-U セッション、SCTP セッション、PFCP セッションの情報にいすゞ自動車(vdom500、10.190.1.0/24)の情報が含まれないことを確認しました。

この結果より、5G コアマルチテナント間の閉域性が確認できました。

```
cntr-secgw1 # config vdom

cntr-secgw1 (vdom) # edit vdom400
current vf=vdom400:3

cntr-secgw1 (vdom400) # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 10.190.0.9, ab1wan
C       10.101.10.0/24 is directly connected, ab1n2n4
C       10.101.20.0/24 is directly connected, ab1n3
C       10.101.30.0/24 is directly connected, ab1n4
C       10.190.0.8/30 is directly connected, ab1wan
S       10.190.0.12/30 [5/0] via IPsec_vdom400 tunnel 10.190.0.2
C       10.190.0.13/32 is directly connected, IPsec_vdom400
```

図 5-3-3-3-53-1 セセ複-5 マルチテナント①

```
cntr-secgw1 (vdom400) # get system session list
PROTO    EXPIRE SOURCE           SOURCE-NAT       DESTINATION      DESTINATION-NAT
udp      179    10.190.0.34:2152 -                10.101.20.7:2152 -
udp      166    10.190.0.2:500   -                10.190.0.10:500  -
sctp     3593   10.190.0.34:38413 -                10.101.10.7:38412 -
udp      177    10.190.0.14:3149 -                208.91.112.53:53 -
udp      177    10.190.0.14:3149 -                208.91.112.52:53 -
udp      174    10.101.10.7:8805 -                10.101.30.7:8805 -
```

図 5-3-3-3-53-2 セセ複-5 マルチテナント②

```
cntr-secgw1 (vdom400) # diagnose ip arp list
index=46 ifname=ab1wan 10.190.0.9 d4:eb:68:53:ac:ef state=00000002 use=48 confirm=5 update=5 ref=7
index=25 ifname=vdom400 0.0.0.0 00:00:00:00:00:00 state=00000040 use=59957300 confirm=59963300 update=59957300 ref=1
index=47 ifname=ab1n2n4 10.101.10.7 00:0c:29:28:00:1f state=00000008 use=315 confirm=2815 update=315 ref=3
index=49 ifname=ab1n4 10.101.30.7 00:0c:29:28:00:ed state=00000002 use=315 confirm=2589 update=1790 ref=2
index=48 ifname=ab1n3 10.101.20.7 00:0c:29:28:00:f7 state=00000002 use=864 confirm=1114 update=613 ref=2
```

図 5-3-3-3-53-3 セセ複-5 マルチテナント③

センタ拠点 UPF を使用した場合の複数企業共用パターンの検証結果を以下にまとめます。いずれの項目においても検証内容に対し、検知・遮断ができることが確認できました。

表 5-3-3-3-7 検証結果まとめ（センタ拠点 UPF 複数企業共用パターン）

評価項目	検証手順	検証結果
N2 Firewall	CellSiteRouter と SecGW 間での通信傍	○

の評価	受の防止	
	SCTP DoS 攻撃の遮断	○
	不正な N2 信号の検知と遮断	○
N3 Firewall の評価	中間者攻撃、不正な GTP-U パケットを UPF に連続して送信	○
N4 Firewall の評価	UPF 上のセッション情報の書き換え及び削除の検知・遮断	○
	不正な PFCP 信号の検知・遮断	○
SBA Firewall の評価	5G コア内の OpenAPI 通信のモニタリング	○
	5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断	○
マルチテナントの評価	5G コアマルチテナント間の閉域性の確認	○

（イ）業界共用パターン

センタ拠点に設置した UPF を使用する構成の業界共用パターンにおける検証項目と該当する攻撃の対応は「表 5-3-3-3-8　検証項目と該当する攻撃（センタ拠点 UPF 業界共用パターン）」のとおりです。

表 5-3-3-3-8 検証項目と該当する攻撃（センタ拠点 UPF 業界共用パターン）

項番	評価項目	検証項目	該当する攻撃
セセ業-1	SecGW の検証	C&C サーバへのアクセス検知・遮断	C&C サーバへの通信
		マルウェアダウンロードの検知・遮断	マルウェアのダウンロード
		使用しているアプリケーションの検知・遮断	悪意あるアプリケーションによる通信
		UE の脆弱性を突いた攻撃検知・遮断	ICMP フラッド攻撃
		不正な拠点から 5G コアへの接続	不正な拠点からの 5G コアへの接続
セセ業-2	N2 Firewall の評価	CellSiteRouter と SecGW 間での通信傍受の防止	N2 通信の傍受
		SCTP DoS 攻撃の遮断	同一 N2 リクエストを大量送信する DoS 攻撃
		不正な N2 信号の検知と遮断	AMF への不正な N2 信号の送信
セセ業-3	N3 Firewall の評価	中間者攻撃、不正な GTP-U パケットの検知と遮断	UPF への不正な GTP-U パケットの送信
セセ業-4	N4 Firewall	UPF 上のセッション情報の	センタ UPF に対するセッション情報

	の評価	書き換え及び削除の検知・遮断	の危険リクエストの送信
		不正な PFCP 信号の検知・遮断	センタ UPF に対する不正な N2 リクエストの送信
セセ業-5	SBA Firewall の評価	5G コア内の OpenAPI 通信のモニタリング機能の確認	
		5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断	NRF に対するバッファオーバーフローを引き起こす http リクエストの送信
セセ業-6	マルチテナントの評価	5G コアマルチテナント間の閉域性の確認	

検証の手順・結果の詳細を以下にまとめます。

各図における IP アドレスは構成の一例です。また、検証結果に関係のない表示をトリミングしています。

セセ業-1：SecGW の検証

● C&C サーバへのアクセス検知・遮断

UE に接続された端末から C&C サーバリストに登録されているアドレス宛ての通信を行い、その通信が検知・遮断されることを確認しました。本構成はインターネットに接続していないため、C&C サーバリストに登録されているアドレス(BlackMoon)をコア内部の疑似 C&C 仮想サーバに割り振り、そのサーバ宛てに通信することで疑似的に C&C サーバへのパケットを生成し検証を行いました。

結果は、GUI にて検知設定時には「detected」、遮断設定時には「dropped」と表示され正常に検知・遮断が行えていることを確認できました。

また、UE に接続した端末上では検知設定時に疑似 C&C サーバへの通信が行え、遮断時には行えないことが確認できました。

この結果より、C&C サーバへのアクセス検知・遮断ができることが確認できました。

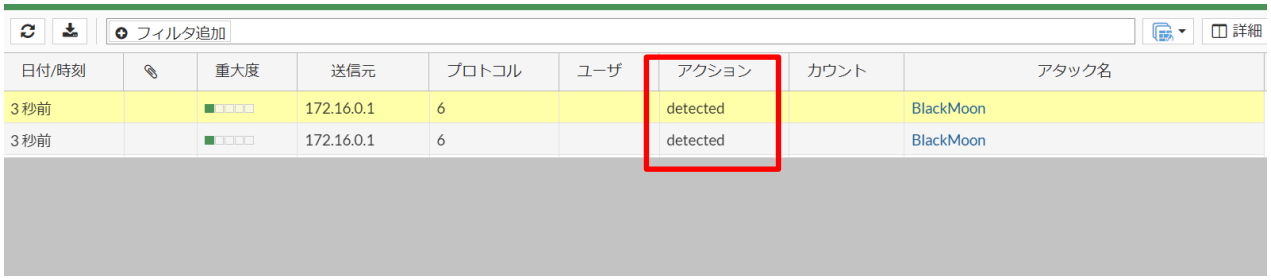


図 5-3-3-3-54 セセ業-1 C&C サーバアクセス 検知

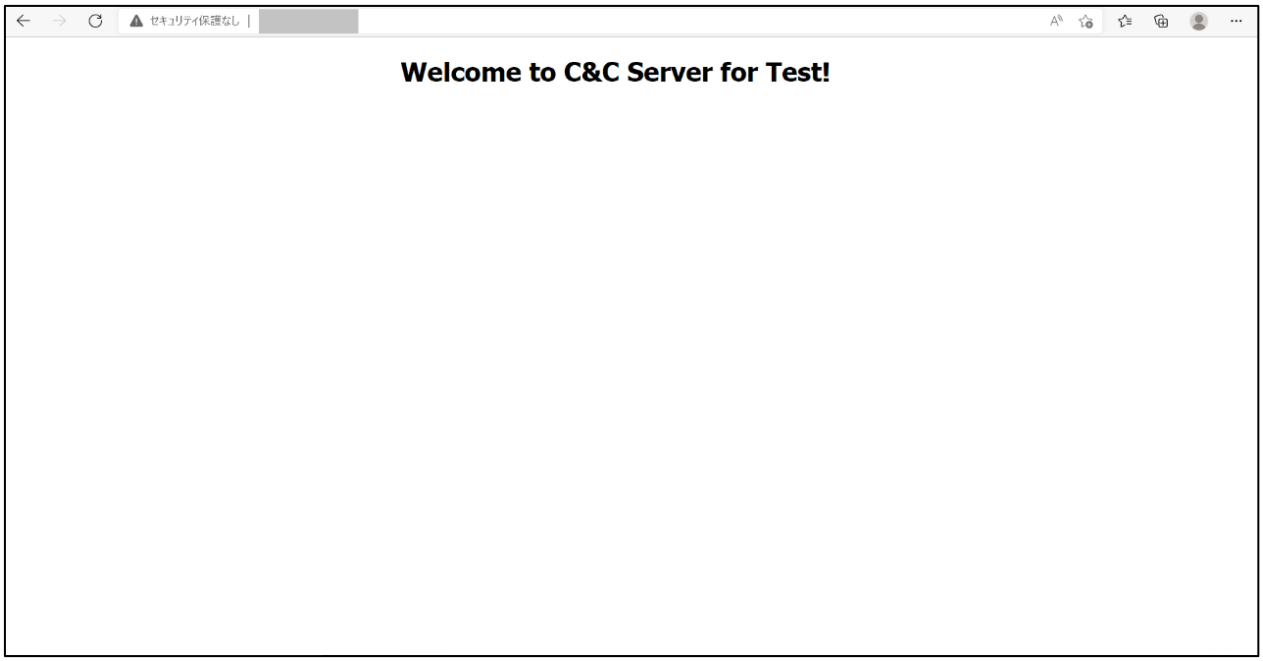


図 5-3-3-3-55 セセ業-1 C&C サーバアクセス成立

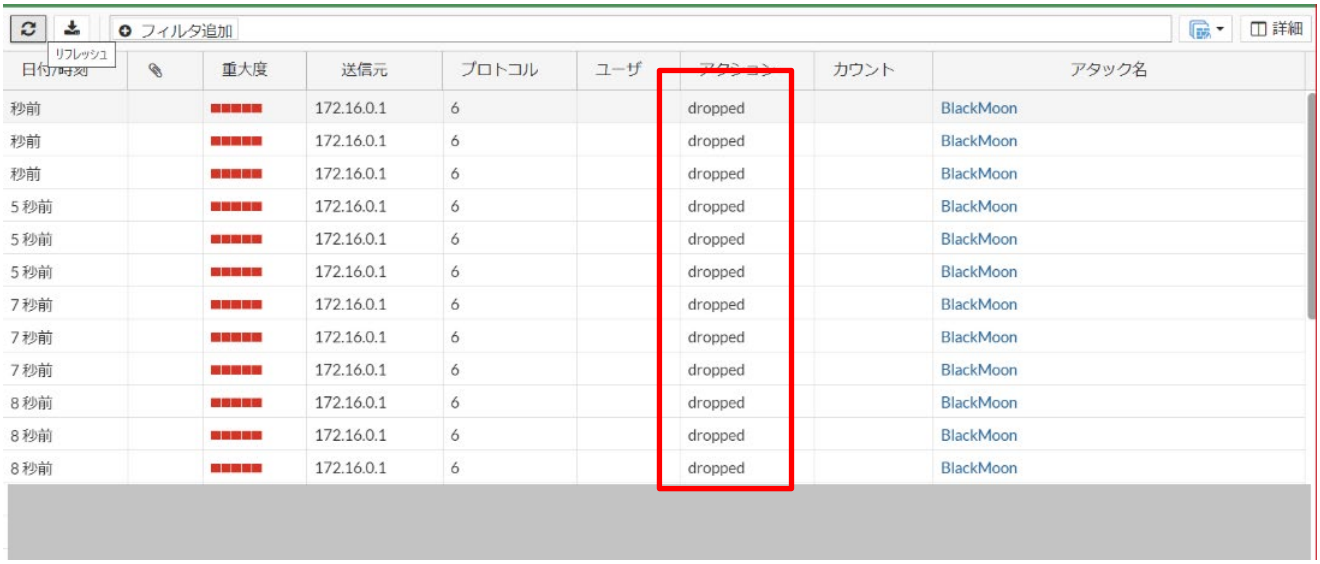


図 5-3-3-3-56 セセ業-1 C&C サーバアクセス 遮断

図 5-3-3-3-57 セセ業-1 C&C サーバアクセス不成立

● マルウェアダウンロードの検知・遮断

UE に接続された端末からマルウェアのダウンロード通信が検知・遮断されることを確認しました。本構成はインターネットに接続していないため、EicarVirus のテストファイルをコア内部の疑似仮想サーバに格納し、そのサーバ宛てに wget の通信を行うことで疑似的にマルウェアサーバへのパケットを生成し検証を行いました。

結果は、GUI にて検知設定時には「detected」、遮断設定時には「dropped」と表示され、正常に検知・遮断できていることが確認できました。

この結果より、マルウェアダウンロードの検知・遮断ができることが確認できました。

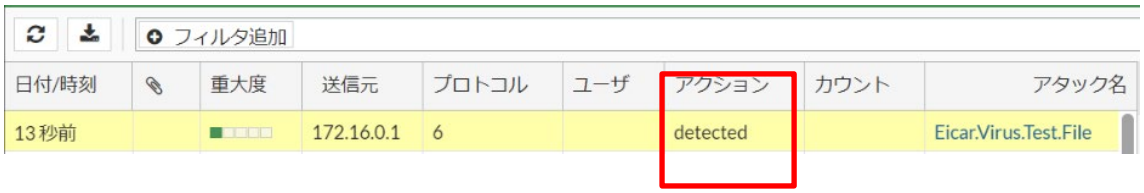


図 5-3-3-3-58-1 セセ業-1 マルウェアダウンロード 検知①

図 5-3-3-3-58-2 セセ業-1 マルウェアダウンロード 検知②

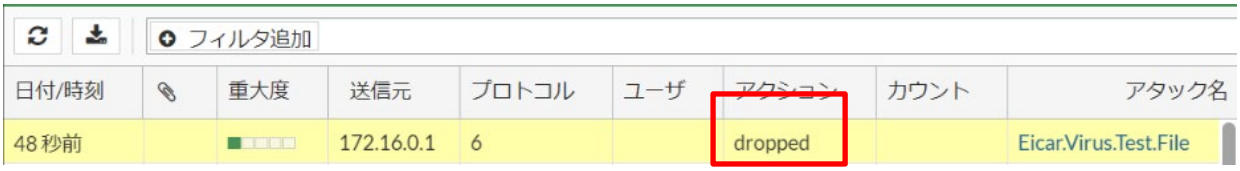


図 5-3-3-3-59-1 セセ業-1 マルウェアダウンロード 遮断①

図 5-3-3-3-59-2 セセ業-1 マルウェアダウンロード 遮断②

- 使用しているアプリケーションの検知・遮断

UE に接続された端末から特定の悪意あるアプリケーション通信を指定して検知・遮断できることを確認しました。疑似的な悪意あるアプリケーション通信として「Wget」を指定し、EicarVirus のテストファイルをコア内部の疑似仮想サーバに格納し、そのサーバ宛てに wget の通信を行うことで疑似的に悪意あるアプリケーションの通信を生成し検証を行いました。

結果は、GUI にて検知設定時には「detected」、遮断設定時には「dropped」と表示さ

れ、正常に検知・遮断できていることが確認できました。
　この結果より、使用しているアプリケーションの検知・遮断ができることが確認できました。

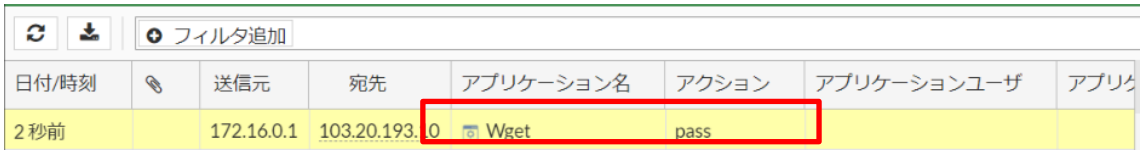


図 5-3-3-3-60-1 セセ業-1 特定アプリケーション 検知①

図 5-3-3-3-60-2 セセ業-1 特定アプリケーション 検知②

図 5-3-3-3-61-1 セセ業-1 特定アプリケーション 遮断①

図 5-3-3-3-61-2 セセ業-1 特定アプリケーション 遮断②

- UE の脆弱性を突いた攻撃検知・遮断

UE に対する攻撃のアノーマリー検知・遮断ができることを確認しました。具体的には UE に対して ICMP フラッディングを送信し SecGW にてアノーマリー検知・遮断ができるこ

とを確認しました。

結果は、GUI にて検知設定時には「detected」、遮断設定時には「dropped」と表示され、正常に検知・遮断できていることが確認できました。

この結果より、UE の脆弱性を突いた攻撃のアノーマリー検知・遮断ができることが確認できました。

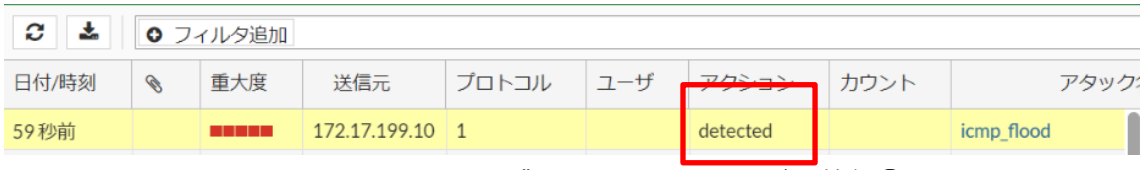


図 5-3-3-3-62-1 セセ業-1 アノーマリー通信 検知①

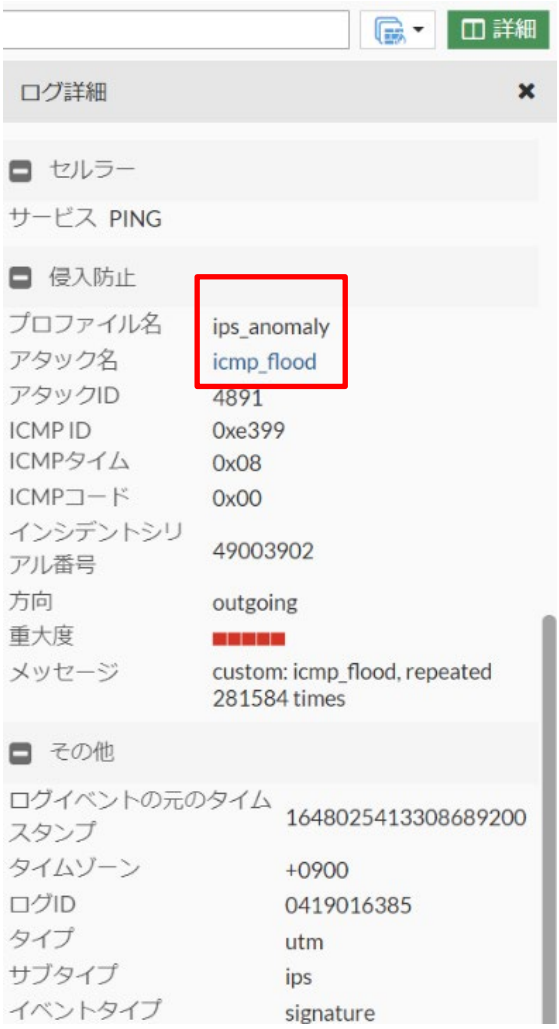


図 5-3-3-3-62-2 セセ業-1 アノーマリー通信 検知②

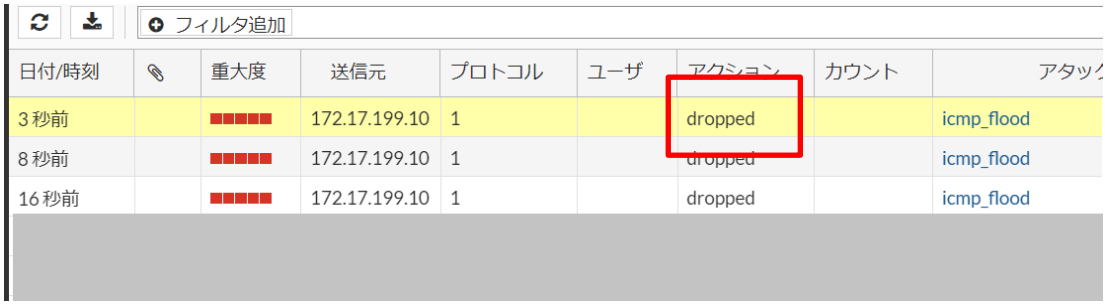


図 5-3-3-3-63-1 セセ業-1 アノーマリー通信 遮断①

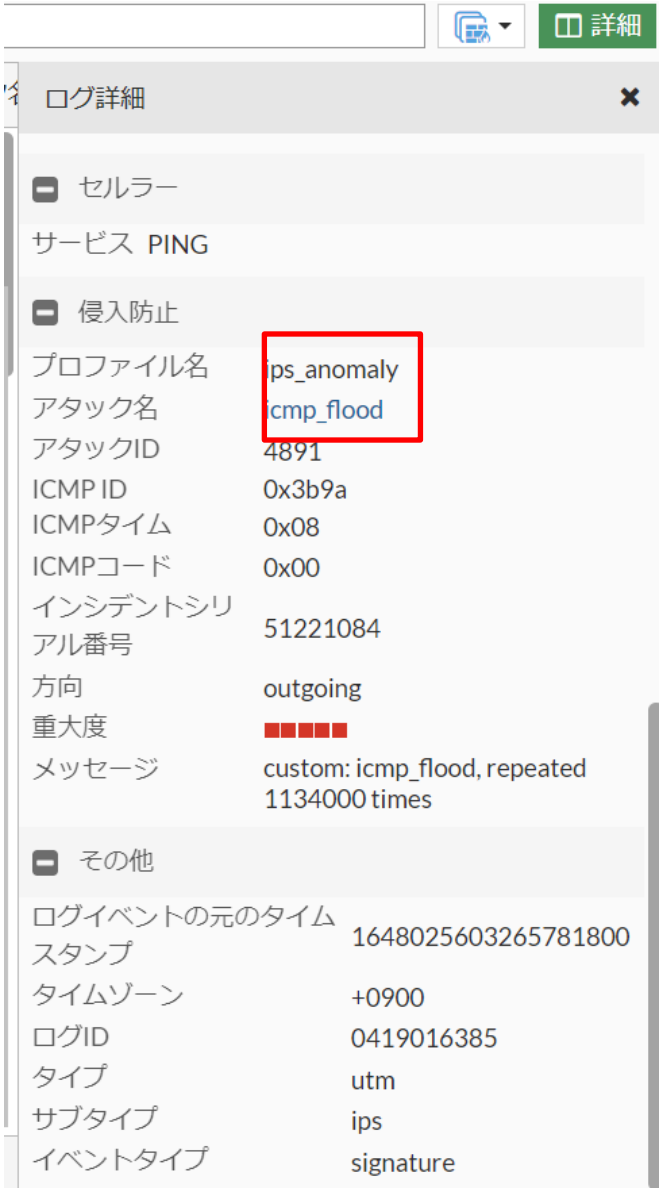


図 5-3-3-3-63-2 セセ業-1 アノーマリー通信 遮断②

- 不正な拠点から 5G コアへの接続の防止

不正な拠点として、拠点間の IPSec トンネルにおいて、SecGW に設定されているものと異

なる事前共有鍵またはProxy-IDを設定した拠点ルータからの接続を行い、トンネルが確立されないことを確認しました。

結果は、GUIでステータスが「negotiated error」の後に「failure」と表示されることが確認でき、トンネルが確立されないことを確認できました。

この結果より、不正な拠点から5Gコアへの接続が防止できることが確認できました。

日付/時刻	レベル	アクション	ステータス	メッセージ	VPNトンネル
5秒前		negotiate	failure	progress IPsec phase 1	IPsec_vdom400
5秒前		negotiate	negotiate_error	IPsec phase 1 error	IPsec_vdom400
5秒前		negotiate	failure	progress IPsec phase 1	IPsec_vdom400
5秒前		negotiate	negotiate_error	IPsec phase 1 error	IPsec_vdom400
12秒前		negotiate	failure	progress IPsec phase 1	IPsec_vdom400
12秒前		negotiate	negotiate_error	IPsec phase 1 error	IPsec_vdom400
12秒前		negotiate	failure	progress IPsec phase 1	IPsec_vdom400
12秒前		negotiate	negotiate_error	IPsec phase 1 error	IPsec_vdom400
14秒前		negotiate	failure	progress IPsec phase 1	IPsec_vdom400
14秒前		negotiate	negotiate_error	IPsec phase 1 error	IPsec_vdom400

図 5-3-3-3-64-1 セセ業-1 不正な拠点からの接続①

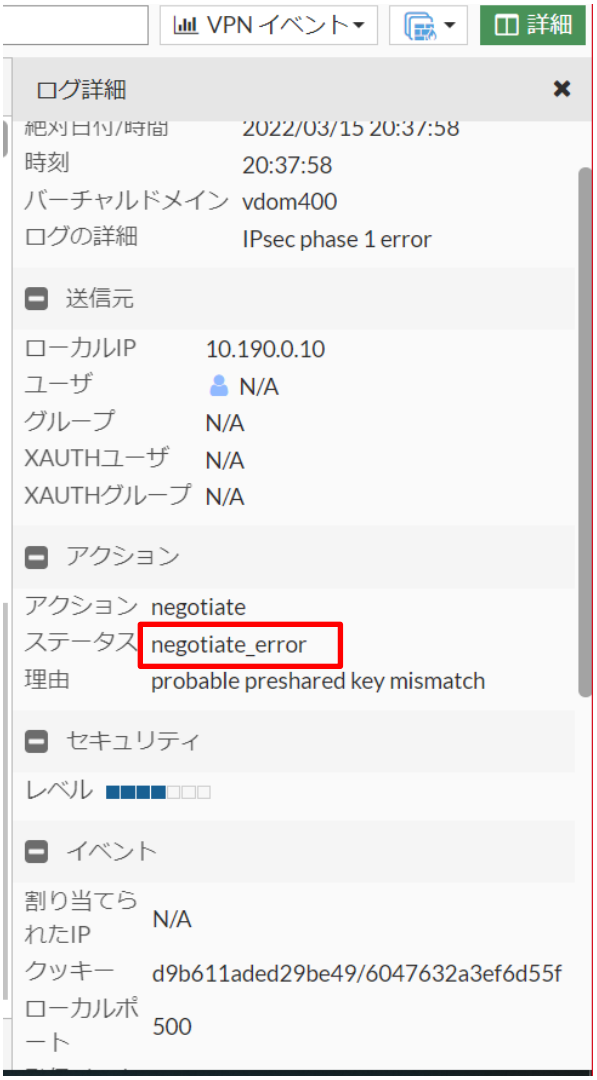


図 5-3-3-3-64-2 セセ業-1 不正な拠点からの接続①

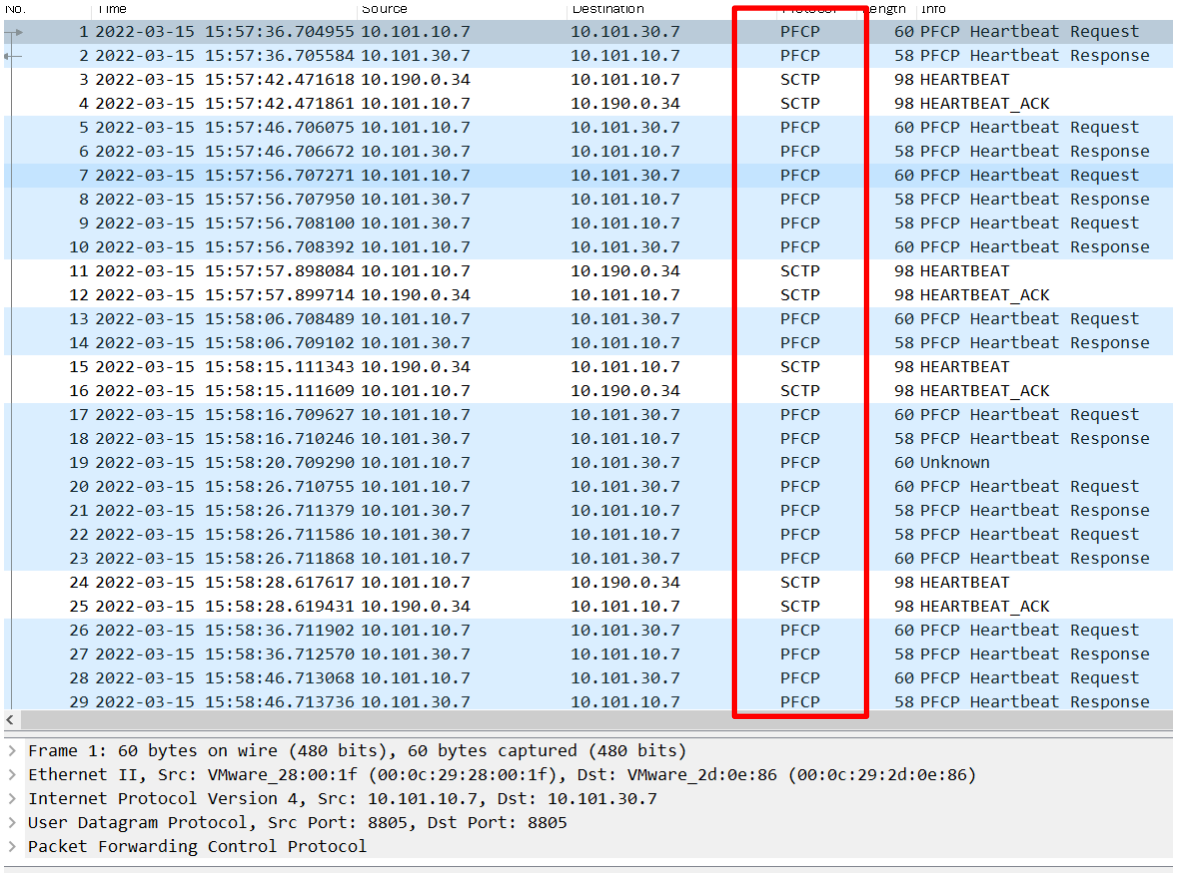
セセ業-2：N2 Firewall の評価

- CellSiteRouter と SecGW 間での通信傍受の防止

SecGW により WAN 区間における N2 通信が暗号化され傍受できないことを確認するため、SecGW の 5GC 側と WAN 側においてトラフィックキャプチャを行いました。

結果は、5GC 側では PFCP、SCTP の通信が平文で見える一方、WAN 側では ESP(IPSec による暗号化)と表示されることを確認し、WAN 区間では IPSec による通信の暗号化がされていることが確認できました。

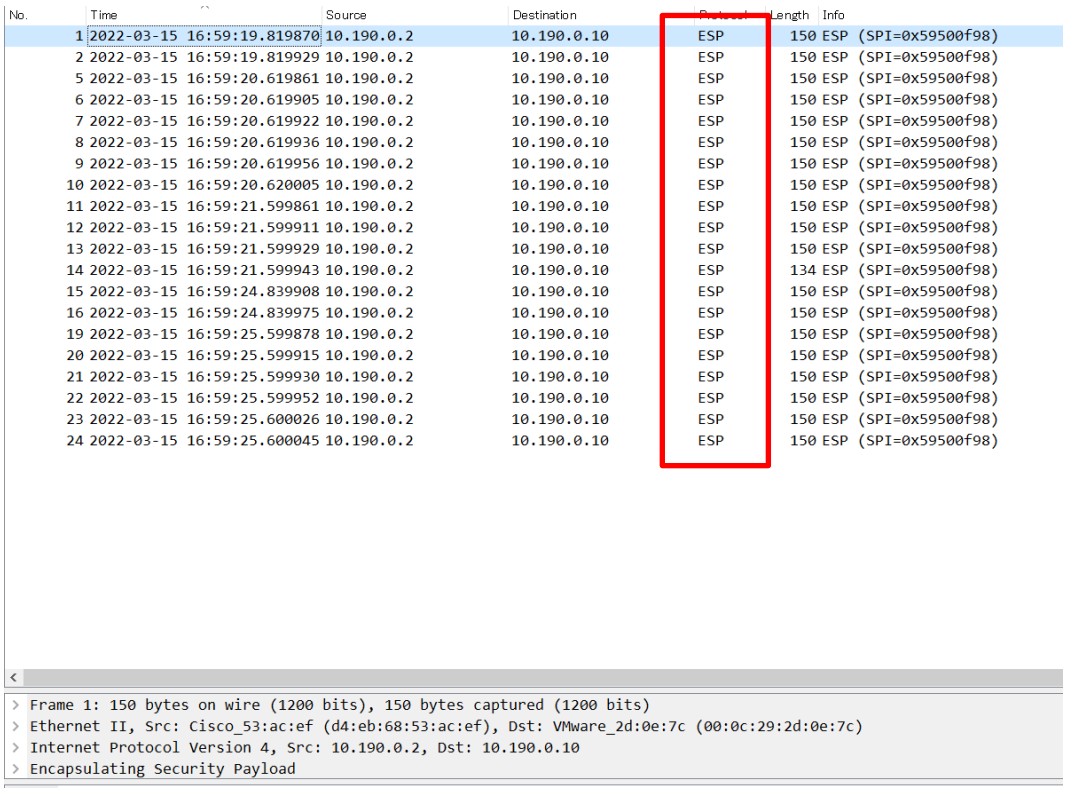
この結果より、CellSiteRouter と SecGW 間での通信傍受が防止できることが確認できました。



No.	Time	Source	Destination	Protocol	Length	Info
1	2022-03-15 15:57:36.704955	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
2	2022-03-15 15:57:36.705584	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
3	2022-03-15 15:57:42.471618	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT
4	2022-03-15 15:57:42.471861	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT_ACK
5	2022-03-15 15:57:46.706075	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
6	2022-03-15 15:57:46.706672	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
7	2022-03-15 15:57:56.707271	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
8	2022-03-15 15:57:56.707950	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
9	2022-03-15 15:57:56.708100	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Request
10	2022-03-15 15:57:56.708392	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Response
11	2022-03-15 15:57:57.898084	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT
12	2022-03-15 15:57:57.899714	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT_ACK
13	2022-03-15 15:58:06.708489	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
14	2022-03-15 15:58:06.709102	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
15	2022-03-15 15:58:15.111343	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT
16	2022-03-15 15:58:15.111609	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT_ACK
17	2022-03-15 15:58:16.709627	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
18	2022-03-15 15:58:16.710246	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
19	2022-03-15 15:58:20.709290	10.101.10.7	10.101.30.7	PFCP	60	Unknown
20	2022-03-15 15:58:26.710755	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
21	2022-03-15 15:58:26.711379	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
22	2022-03-15 15:58:26.711586	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Request
23	2022-03-15 15:58:26.711868	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Response
24	2022-03-15 15:58:28.617617	10.101.10.7	10.190.0.34	SCTP	98	HEARTBEAT
25	2022-03-15 15:58:28.619431	10.190.0.34	10.101.10.7	SCTP	98	HEARTBEAT_ACK
26	2022-03-15 15:58:36.711902	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
27	2022-03-15 15:58:36.712570	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response
28	2022-03-15 15:58:46.713068	10.101.10.7	10.101.30.7	PFCP	60	PFCP Heartbeat Request
29	2022-03-15 15:58:46.713736	10.101.30.7	10.101.10.7	PFCP	58	PFCP Heartbeat Response

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: VMware_28:00:1f (00:0c:29:28:00:1f), Dst: VMware_2d:0e:86 (00:0c:29:2d:0e:86)
> Internet Protocol Version 4, Src: 10.101.10.7, Dst: 10.101.30.7
> User Datagram Protocol, Src Port: 8805, Dst Port: 8805
> Packet Forwarding Control Protocol
```

図 5-3-3-3-65 セセ業-2 通信傍受 5GC 側



No.	Time	Source	Destination	Protocol	Length	Info
1	2022-03-15 16:59:19.819870	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
2	2022-03-15 16:59:19.819929	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
5	2022-03-15 16:59:20.619861	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
6	2022-03-15 16:59:20.619905	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
7	2022-03-15 16:59:20.619922	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
8	2022-03-15 16:59:20.619936	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
9	2022-03-15 16:59:20.619956	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
10	2022-03-15 16:59:20.620005	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
11	2022-03-15 16:59:21.599861	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
12	2022-03-15 16:59:21.599911	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
13	2022-03-15 16:59:21.599929	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
14	2022-03-15 16:59:21.599943	10.190.0.2	10.190.0.10	ESP	134	ESP (SPI=0x59500f98)
15	2022-03-15 16:59:24.839908	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
16	2022-03-15 16:59:24.839975	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
19	2022-03-15 16:59:25.599878	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
20	2022-03-15 16:59:25.599915	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
21	2022-03-15 16:59:25.599930	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
22	2022-03-15 16:59:25.599952	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
23	2022-03-15 16:59:25.600026	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)
24	2022-03-15 16:59:25.600045	10.190.0.2	10.190.0.10	ESP	150	ESP (SPI=0x59500f98)

```
> Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
> Ethernet II, Src: Cisco_53:ac:ef (d4:eb:68:53:ac:ef), Dst: VMware_2d:0e:7c (00:0c:29:2d:0e:7c)
> Internet Protocol Version 4, Src: 10.190.0.2, Dst: 10.190.0.10
> Encapsulating Security Payload
```

図 5-3-3-3-66 セセ業-2 通信傍受 WAN 側

- SCTP DoS 攻撃の遮断

SCTP DoS 攻撃の検知・遮断を検証するため、AMF へのトラフィック量が閾値を超えた場合に N2 Firewall によって検知・遮断できることを検証しました。具体的には閾値として 2pps を設定し、AMF 宛てに 9pps のトラフィックを発生させ、検知・遮断できることを確認しました。

結果は、GUI にて検知設定時には「detected」、遮断設定時には「dropped」と表示され、いずれにおいても 7 回分のパケットが検知・遮断できていることを確認しました。

この結果より、SCTP DoS 攻撃の検知・遮断ができることが確認できました。

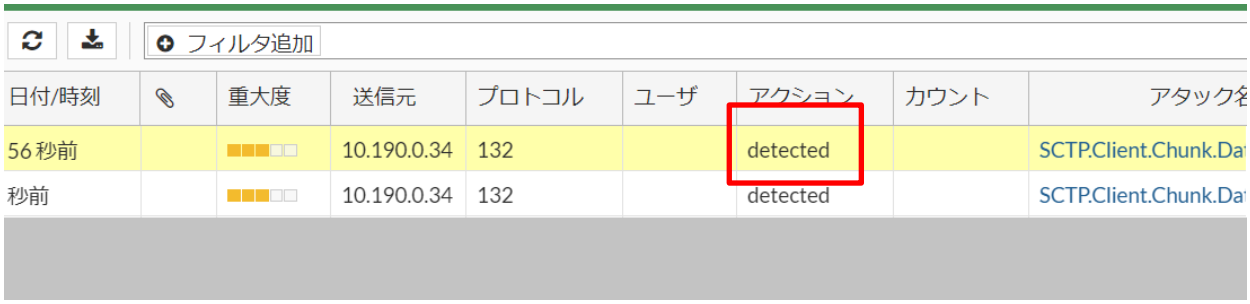


図 5-3-3-3-67-1 セセ業-2 DoS 攻撃 検知①

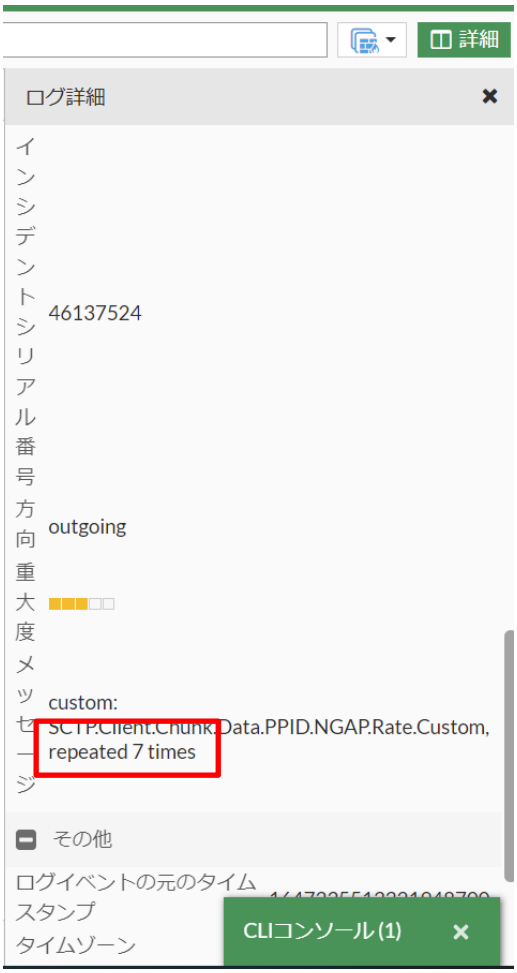


図 5-3-3-3-67-2 セセ業-2 DoS 攻撃 検知②

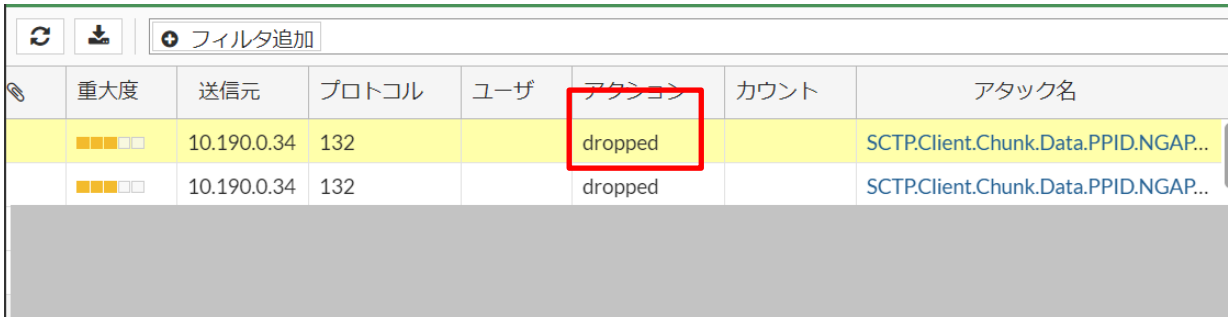


図 5-3-3-3-68-1 セセ業-2 DoS 攻撃 遮断①

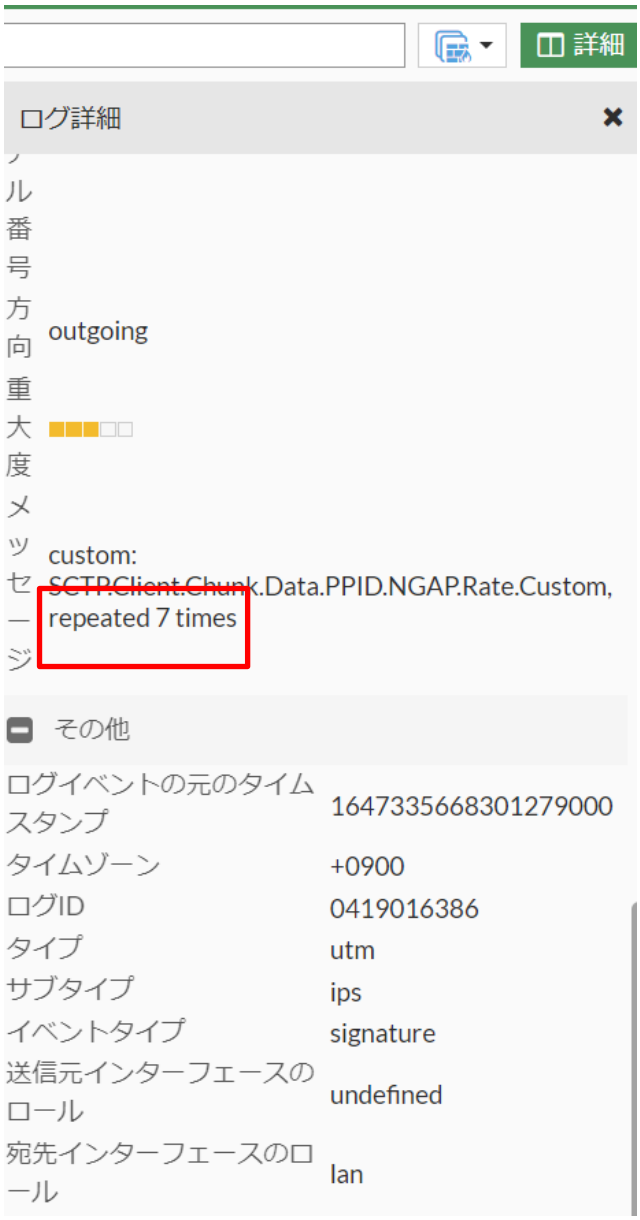


図 5-3-3-3-68-2 セセ業-2 DoS 攻撃 遮断②

● 不正な N2 信号の検知と遮断

不正な N2 信号を送信し、N2 Firewall によって検知・遮断できることを確認しました。具体的には不正な N2 信号として不正な ppid 値(0)をセットしたパケットを AMF 宛てに送信し、N2 Firewall にて検知・遮断できることを確認しました。

結果は、CLI にて検知設定時には「pass」、遮断設定時には「reset」と表示され、検知・遮断ができていることを確認しました。

この結果より、不正な N2 信号の検知と遮断ができることが確認できました。

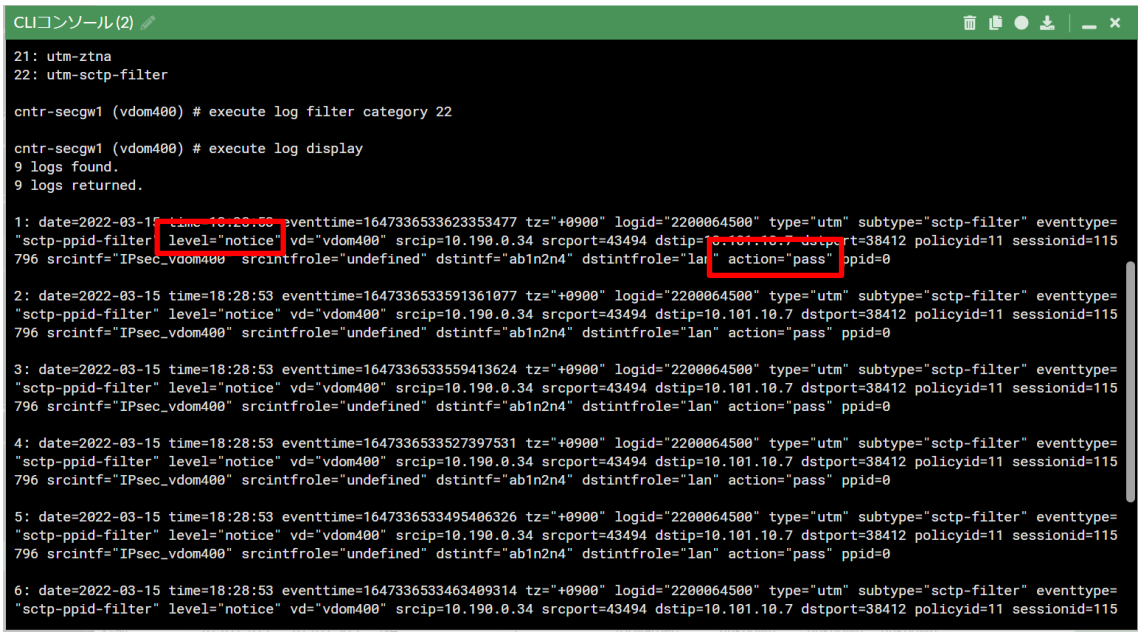


図 5-3-3-3-69 セセ業-2 不正な N2 信号 検知

図 5-3-3-3-70 セセ業-2 不正な N2 信号 遮断

セセ業-3：N3 Firewall の評価

- 中間者攻撃、不正な GTP-U パケットの検知と遮断

不正な GTP-U パケットを UPF に送信する攻撃を N3 Firewall にて遮断できることを確認しました。具体的には一度確立されたセッションを終了させた後、そのセッション宛てのパケットを送ることで中間者攻撃を再現し、不正な GTP-U パケットとして遮断されるかを検証しました。

結果は、GUI にて「prohibited」という表示とその理由として「invalid-state」と表示され、遮断されていることを確認できました。

この結果より、不正な GTP-U パケットの検知と遮断ができることが確認できました。

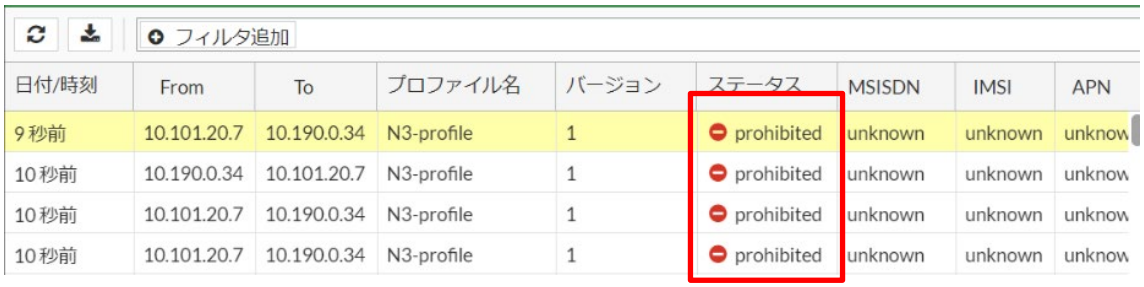


図 5-3-3-3-71-1 セセ業-3 不正な GTP-U パケット 遮断①

図 5-3-3-3-71-2 セセ業-3 不正な GTP-U パケット 遮断②

セセ業-4：N4 Firewall の評価

● UPF 上のセッション情報の書き換えおよび削除の検知・遮断

UPF 宛てにセッション情報の書き換えを行うパケットを送信し、N4 Firewall によって攻撃を検知・遮断する検証を行いました。具体的には SMF を偽装する疑似 SMF から拠点側の UPF 宛てにセッションを削除する攻撃を行い、検知・遮断ができていることを確認しました。

GUI にて該当パケットが検知設定時には「forwarded」、遮断設定時には「prohibited」となっていることを確認しました。

また、攻撃を遮断しなかった場合にセッションが切れることを、拠点 UE 下部の端末から UPF 宛ての ping で確認し、検知設定時のみ ping が切れることを確認しました。

この結果より、UPF 上のセッション情報の書き換え及び削除の検知・遮断ができることが確認できました。

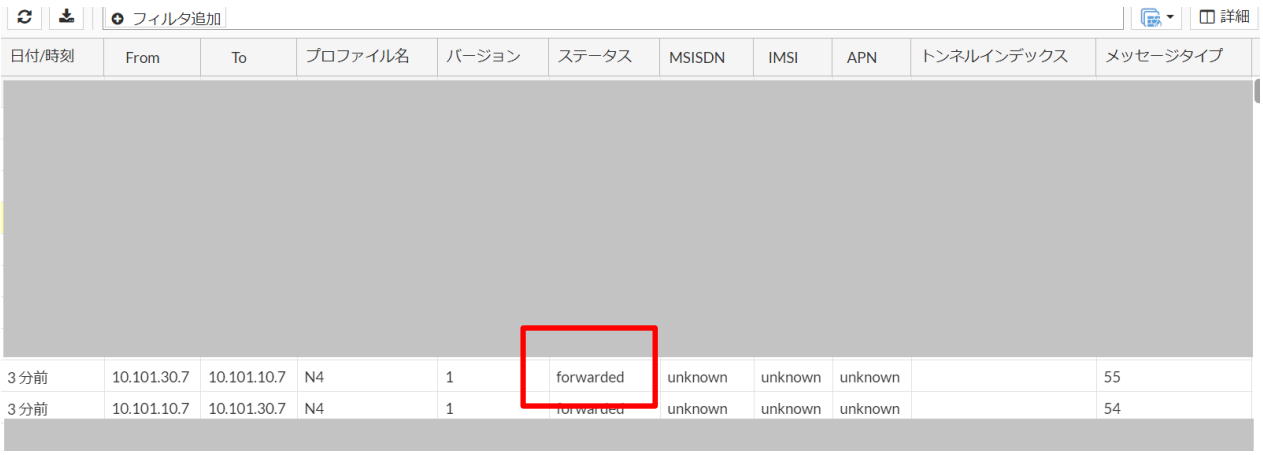


図 5-3-3-3-72 セセ業-4 セッション削除 検知

```
C:¥Users¥BFL>ping 172.17.199.2 -t

172.17.199.2 に ping を送信しています 32 バイトのデータ:
172.17.199.2 からの応答: バイト数 =32 時間 =26ms TTL=61
172.17.199.2 からの応答: バイト数 =32 時間 =22ms TTL=61
172.17.199.2 からの応答: バイト数 =32 時間 =36ms TTL=61
172.17.199.2 からの応答: バイト数 =32 時間 =38ms TTL=61
172.17.199.2 からの応答: バイト数 =32 時間 =36ms TTL=61
<中略>
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。

172.17.199.2 の ping 統計:
    パケット数: 送信 = 96、受信 = 55、損失 = 41 (42% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 15ms、最大 = 46ms、平均 = 32ms
```

図 5-3-3-3-73 セセ業-4 セッション削除時 ping

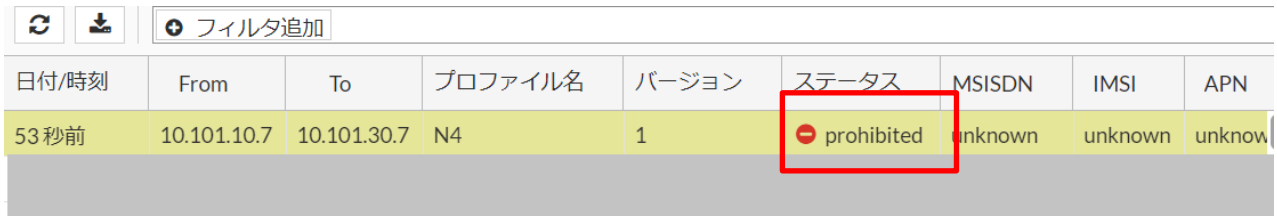


図 5-3-3-3-74-1 セセ業-4 セッション削除 遮断①

図 5-3-3-3-74-2 セセ業-4 セッション削除 遮断②

● 不正な PFCP 信号の検知・遮断

UPF 宛てに不正な PFCP 信号を送信し、N4 Firewall によって攻撃を検知・遮断する検証を行いました。具体的には SMF を偽装する疑似 SMF から拠点側の UPF 宛てに不正な Message Type(254)をセットしたパケットを送信し、N4 Firewall にて検知・遮断ができていることを確認しました。

結果は、GUI にてメッセージタイプ 254 が届いた際、検知設定時には「prohibitted monitor」、遮断設定時には「prohibited」と表示され検知・遮断できていることを確認しました。

この結果より、不正な PFCP 信号の検知・遮断ができることが確認できました。

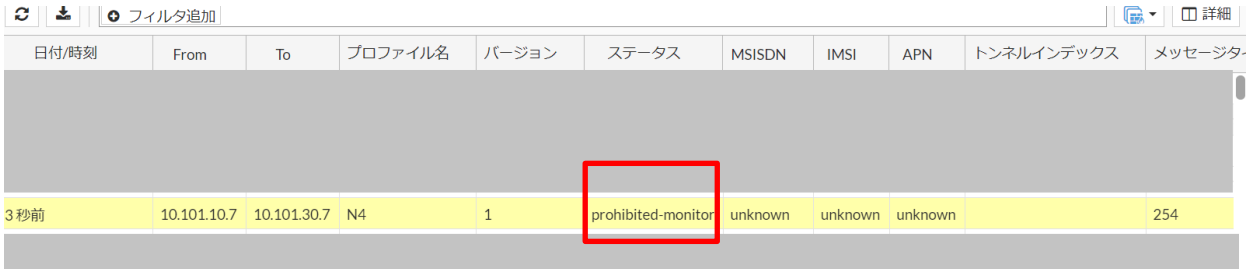


図 5-3-3-3-75 セセ業-4 不正な PFCP 検知

図 5-3-3-3-76 セセ業-4 不正な PFCP 遮断

セセ業-5：SBA Firewall の評価

- 5G コア内の OpenAPI 通信のモニタリング

http2/tls1.2 によって行われる NRF への SBI 通信をテナント毎にモニタリングできることを確認しました。複数企業共用パターンである NTT 中央研修センタ(NRF-policy1)および東北大学(NRF-policy3)のそれぞれについて GUI ログをフィルタリングし、該当のテナントの情報のみを抽出できることを確認しました。また、同様に http2/tls1.2 の通信のみをフィルタリングできることを確認しました。

この結果より、5G コア内の OpenAPI 通信がモニタリングできることが確認できました。

図 5-3-3-3-77 セセ業-5 OpenAPI モニタリング NTT 中央研修センタ

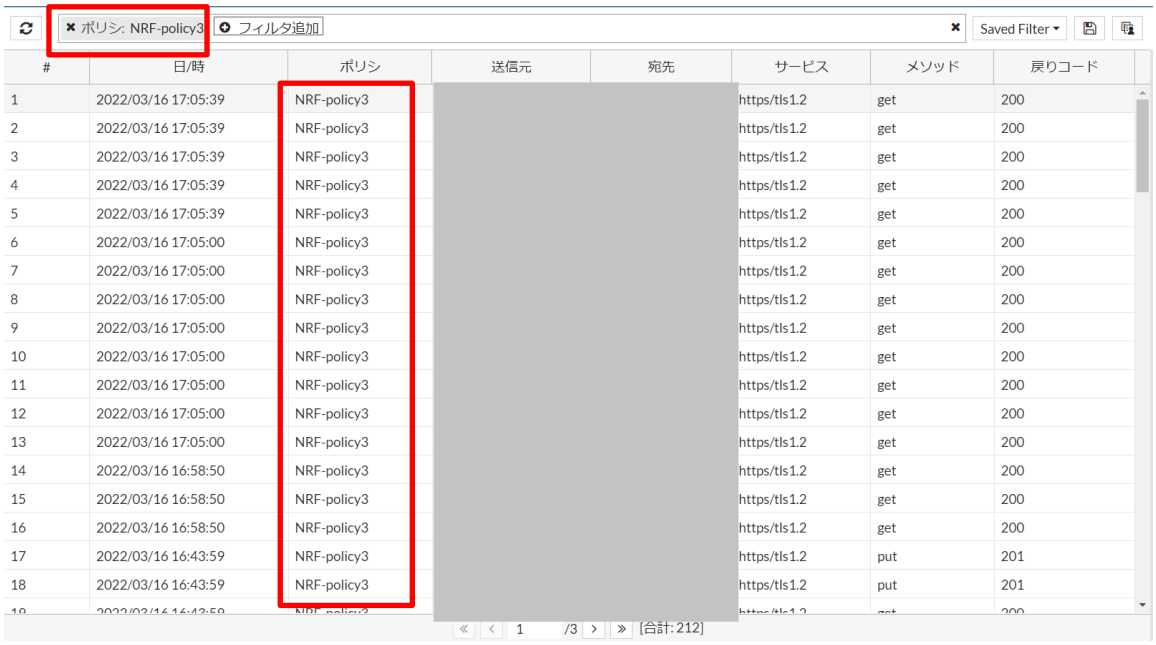


図 5-3-3-3-78 セセ業-5 OpenAPI モニタリング 東北大学

図 5-3-3-3-79 セセ業-5 OpenAPI モニタリング http/tls1.2

● 5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断

NRF への OpenAPI を使用した DoS 攻撃を SBA Firewall にて検知・遮断する検証を行いました。具体的には NRF 宛てに不正な API 通信として長大な URL の http リクエストを送信し、SBA Firewall にて検知・遮断ができることを確認しました。

結果は、GUI にて検知設定時には「Alert」、遮断設定時には「403 Forbidden エラー」を返していることと、128Byte 以上の長大な URL のリクエストを検知・遮断した旨のメッセージを確認しました。

この結果より、5G コア内におけるバッファオーバーフロー等による DoS 攻撃の検知・遮断ができることが確認できました。

図 5-3-3-3-80-1 セセ業-5 バッファオーバーフロー 検知①

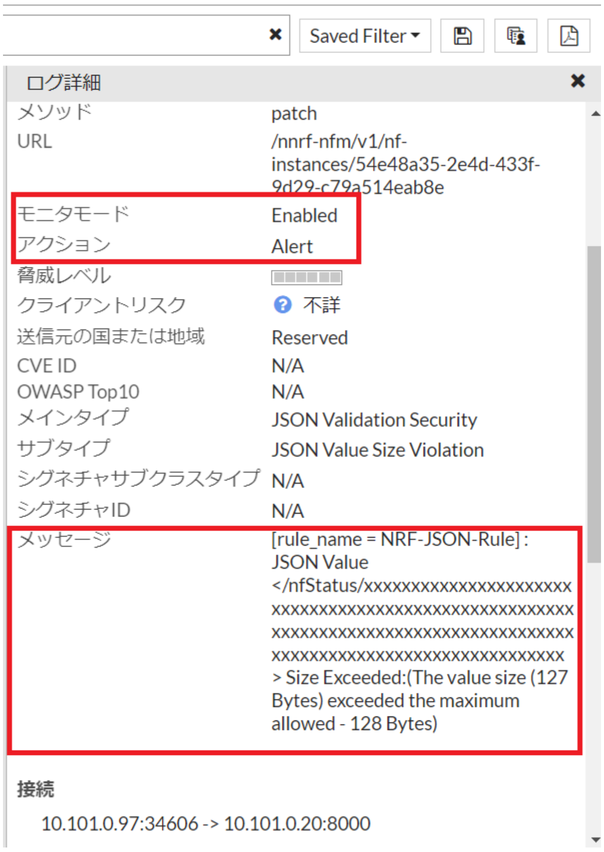


図 5-3-3-3-80-2 セセ業-5 バッファオーバーフロー 検知②

図 5-3-3-3-81-1 セセ業-5 バッファオーバーフロー 遮断①

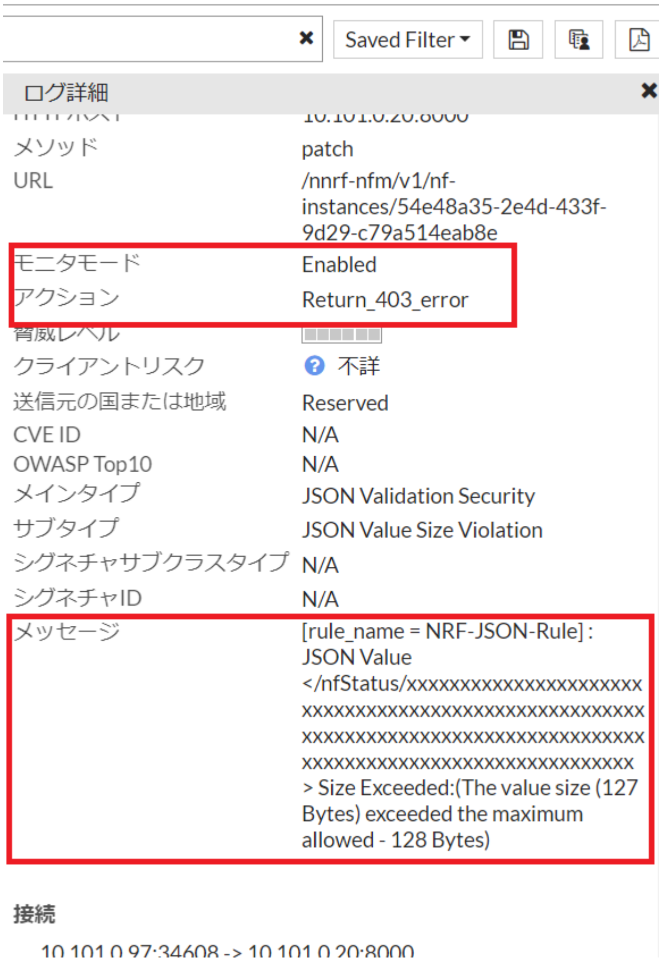


図 5-3-3-3-81-2 セセ業-5 バッファオーバーフロー 遮断②

セセ業-6：マルチテナントの評価

● 5G コアマルチテナント間の閉域性の確認

マルチテナントの閉域性を検証するため、異なるテナントのネットワーク情報が独立して管理されていることを確認しました。具体的には NTT 中央研修センタ(vdom400)のルーティングテーブル、GTP-U セッション、SCTP セッション、PFCP セッションの情報にいず自動車(vdom500)の情報が含まれないことを確認しました。

この結果より、5G コアマルチテナント間の閉域性が確認できました。

```
cntr-secgw1 (vdom400) # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via IPsec_vdom400 tunnel 10.190.0.2
C       10.101.10.0/24 is directly connected, ab1n2n4
C       10.101.20.0/24 is directly connected, ab1n3
C       10.101.30.0/24 is directly connected, ab1n4
S       10.190.0.0/30 [10/0] via 10.190.0.9, ab1wan
C       10.190.0.8/30 is directly connected, ab1wan
S       10.190.0.12/30 [5/0] via IPsec_vdom400 tunnel 10.190.0.2
C       10.190.0.13/32 is directly connected, IPsec_vdom400
```

図 5-3-3-3-82-1 セセ業-6 マルチテナント①

```
cntr-secgw1 (vdom400) # get system session list
PROTO    EXPIRE SOURCE            SOURCE-NAT       DESTINATION      DESTINATION-NAT
udp      149    10.190.0.34:2152  -                10.101.20.7:2152 -
udp      147    10.190.0.2:500    -                10.190.0.10:500  -
sctp     3583   10.190.0.34:38413 -                 10.101.10.7:38412 -
udp      174    10.101.10.7:8805  -                10.101.30.7:8805 -
```

図 5-3-3-3-82-2 セセ業-6 マルチテナント②

```
cntr-secgw1 (vdom400) # diagnose ip arp list
index=46 ifname=ab1wan 10.190.0.9 d4:eb:68:53:ac:ef state=00000002 use=48 confirm=1869 update=1869 ref=3
index=25 ifname=vdom400 0.0.0.0 00:00:00:00:00:00 state=00000040 use=59844348 confirm=59850348 update=59844348 ref=1
index=66 ifname=IPsec_vdom400 0.0.0.0  state=00000040 use=24659485 confirm=24665485 update=24659485 ref=4
index=47 ifname=ab1n2n4 10.101.10.7 00:0c:29:28:00:1f state=00000008 use=380 confirm=3879 update=380 ref=3
index=49 ifname=ab1n4 10.101.30.7 00:0c:29:28:00:ed state=00000002 use=379 confirm=879 update=879 ref=2
index=48 ifname=ab1n3 10.101.20.7 00:0c:29:28:00:f7 state=00000002 use=162 confirm=161 update=146 ref=2
```

図 5-3-3-3-82-3 セセ業-6 マルチテナント③

センタ拠点 UPF を使用した場合の業界共用パターンの検証結果を以下にまとめます。いずれの項目においても検証内容に対し、検知・遮断ができることが確認できました。

表 5-3-3-3-9 検証結果まとめ（エンド拠点 UPF 業界共用パターン）

評価項目	検証手順	検証結果
SecGW の評価	C&C サーバへのアクセス検知・遮断	○
	マルウェアダウンロードの検知・遮断	○
	使用しているアプリケーションの検知・遮断	○
	UE の脆弱性を突いた攻撃検知・遮断	○
	不正な拠点から 5G コアへの接続	○
N2 Frewall の評価	CellSiteRouter と SecGW 間での通信傍受の防止	○
	SCTP DoS 攻撃の遮断	○

	不正な N2 信号の検知と遮断	○
N3 Frewall の評価	中間者攻撃、不正な GTP-U パケットを UPF に連続して送信	○
N4 Frewall の評価	UPF 上のセッション情報の書き換え及び削除の検知・遮断	○
	不正な PFCP 信号の検知・遮断	○
SBA Firewall の評価	5G コア内の OpenAPI 通信のモニタリング	○
	5G コア内におけるバッファオーバーフロー等による DoS 攻撃検知・遮断	○
マルチテナントの評価	5G コアマルチテナント間の閉域性の確認	○

④ 考察

本検証結果により、本検証のすべての構成パターンで、セキュリティが無効化されている場合、同一テナントのコア内のすべての通信が不正に侵入可能であり、検証したすべての攻撃が成立することが確認できました。また、それらの攻撃をセキュリティ装置で遮断できることが確認できました。

コア共用の構成を取りコアと基地局を別の拠点で構築した場合においては、拠点間通信の回線上をファンクションの通信が流れることになります。そうした拠点間通信を狙う外部からの攻撃に対しては、IPsec のように暗号化によってセキュリティを担保する拠点間 VPN 等の導入についての考慮が必要となると考えます。

また、サーバおよびネットワークを仮想化しマルチテナント間の通信を禁止することで、コアを共用する他テナントへの攻撃を防ぐ他、いずれかの拠点のコアが攻撃された際にその他のテナントへの影響を防ぐ効果が期待できます。

また、本検証はインターネット接続のない閉域の環境で実施しましたが、インターネットへの接続があるケースでは、一般のローカルネットワークのセキュリティ同様にインターネットからの攻撃に対するセキュリティ対策が有効です。

内部からの攻撃は、本検証で取った構成を一例とし、各種ファンクション通信(N2 / N3 / N4 / SBA 通信)に対する Firewall 機能を持つセキュリティ装置を導入することが有効です。

上記のような内外からの攻撃に対するセキュリティ対策を施す際は、複数のユーザーで共用できる仮想アプライアンス製品や IPsec 機能を有するセキュリティ機器を採用することで全体のコストを抑えながら効果的にセキュリティ対策が行えると考えます。

(4) コアの共用における運用課題の洗い出し

令和 4 年度以降のコアの共用実現に向けて運用面で検証が必要な項目・内容の洗い出しを行いました。

① 性能

・性能検証により明らかになった課題

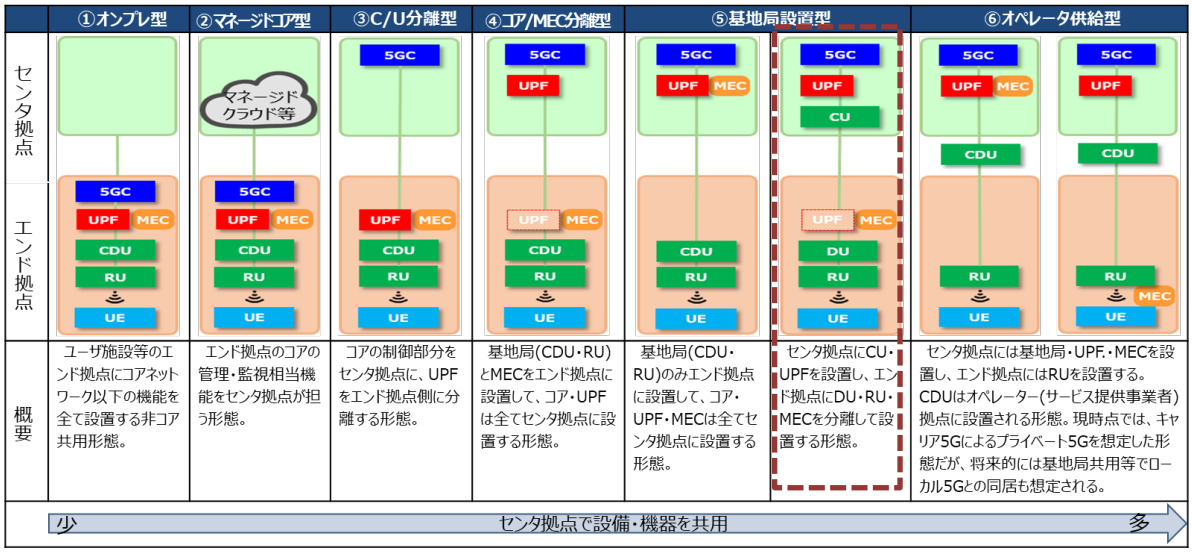
コアの共用における拠点間の物理的な地上回線（広域回線）によって、10ms 程度の伝送遅延の差分が生じることが判明しました。使用するアプリケーションやユースケースによって、センタ拠点 UPF とエンド拠点 UPF の構成を使い分けることが重要と考えられます。

伝送スループットに関しては TDD 準同期方式の実用が可能であることを確認しましたが、ローカル５Ｇでは用途やユースケースの特性上、UL 伝送スループットの需要が高いためより UL 伝送スループットの比率の高い準同期方式が規格化されることが重要であると考えます。

また、ネットワークスライシング等を用いた柔軟な NW 構成により遅延時間等の課題解決に繋がると考えられるため、今後の調査研究で検討されることに期待します。

・市場動向から推定する課題

3GPP 標準化の動きとして、CU と DU を分離して CU を集約拠点で共有するモデルの実用化が進んでいます。コア装置と UPF に加えて CU の共有が実現することで、更なる費用の低廉化が目指せると推定できるため、今後の調査研究で検討されることに期待します。



今後検証が望まれる構成

図 5-3-4-1-1　CU, DU 分離構成（UPF の設置位置）

② 機能

・コアの共用における管理機能

コアの共用環境下における管理機能として必要と考えられる項目は「表 5-3-4-2-1　コア共用環境下において求められる管理機能」のとおりとなります。

表 5-3-4-2-1　コア共用環境下において求められる管理機能

必要機能	実装有無	用途
SIM 登録/変更/閲覧 （拠点毎に権限範囲を分けること）	○	新規端末の登録、既設端末の変更、通信端末の管理
端末情報の閲覧	○	接続状態と通信状態の把握
ポリシー情報の登録/閲覧	○	端末に対するポリシーの設定及び管理
アクセス設定（UPF 指定制御）	○	センタ側 UPF とエンド型 UPF（MEC）の指定と制御
ログ蓄積/閲覧	○	システム状態の把握、トラブルシュート
セッション管理	○	コントロールプレーンの通信状況、認証判定結果等の確認
在圏情報	×	接続先 RU（PCI）の把握
トラフィックモニタリング（UPF）	×	トラフィックモニタ、累積通信量の把握
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

本実証で採用した製品には、「在圏管理」、「トラフィックモニタリング（UPF）」及び「ネットワークスライス」の機能が未実装でしたので、今後はこれら機能の検証が有効だと考えます。

・運用監視、障害切り分けや対応のモデル化

ローカル５Ｇシステムの管理として、システム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手法、拠点毎の対応方法等のモデル化が必要だと推定されます。特に、自治体や業界団体での共用体系では電気通信事業者による運用監視が行われないことも想定されるため、実態に即した監視・対応体制について検証し、課題等を洗い出されることに期待します。

③　セキュリティ

・外部からの攻撃に必要なセキュリティ対策

コアを共用し、基地局と異なる拠点にコア装置を置く構成を取る場合、拠点間通信の暗号化によって外部からの傍受を防ぐ必要があると考えます。また、不特定多数のユーザーを収容するマルチテナントの構成を考えると、その際にはテナント間の閉域性を担保する設計を取る必要があります。これらの対策に加え、インターネットへの接続がある場合は、一般のネットワーク同様にインターネットからの攻撃に対するセキュリティ対策を施すことで、アタックサーフェスは内部からの攻撃のみとなります。

・内部からの攻撃に必要なセキュリティ対策および費用対効果

内部からの攻撃に関しては、各種ファンクション通信(N2 / N3 / N4 / NRF への通信)に一元的に対応できる仮想アプライアンス製品や IPsec 機能を有するセキュリティ機器を導入することで防ぐことができます。その際には複数のマルチテナントをまとめて管理できる製品を採用することでコストを低減しながらセキュリティが担保できると考えます。

・RU-UE 間のセキュリティ対策

ローカル５Ｇのユースケースを考えると、複数のユーザーが同一の RU に収容されるケースが考えられ、RU-UE の間のセキュリティを担保する必要があると考えます。

5.4　コアの共用におけるシステム検証結果考察のまとめ

本調査研究で検証した（１）～（４）の結果踏まえて考察を以下にまとめます。

(1) 性能について

・コアの共用環境下においてローカル５Ｇの性能上の問題は生じないと考えます。
・消費リソースは、1UE 毎のメモリ消費量を確認しました。この消費量は製品仕様に依存するものであり、コアの共用環境において消費量の増加等はありませんでした。
　※製品の仕様に依存するため、設計時に確認されることを推奨
・伝送スループットについて、コアの共用における広域回線や UPF 配置で差分は見られず、コアの共用環境に起因した性能劣化等もありませんでした。
　※広域回線の所要性能によっては差分が生じる可能性があります
・伝送遅延時間は、以下の結果を確認しました。

－ベストエフォート型（SDN）の広域回線では、NTT 中央研修センタ及びいすゞ自動車の 2 拠点で使用している。センタ拠点（東京都豊島区）からの物理的距離はいずれも比較的近い距離になるが、センタ UPF とエンド UPF における遅延時間の差が 10ms 程度となることを確認。

－ギャランティ型（ビジネスイーサワイド）の広域回線では、NTT 中央研修センタ、東北大学、東京大学、京都大学の 4 拠点で使用しているが、センタ拠点 UPF 時とエンド拠点 UPF 時における遅延時間の差分は、1ms～9ms となり、物理的な距離による遅延時間劣化の相関は確認できず。

－同一拠点における、ベストエフォート型（SDN）とギャランティ型（ビジネスイーサワイド）それぞれの遅延時間を検証。センタ拠点 UPF 時とエンド拠点 UPF 時の遅延時間の差分は、ベストエフォート型が 11ms、ギャランティ型が 1ms となり、回線の帯域向上によって遅延時間の改善が可能であることを確認。

以上の結果より、コアの共用環境において、ローカル５Ｇの性能面での問題は生じないことが確認できました。

ただし、コアの共用環境では、センタ拠点とエンド拠点を地上回線で接続する必要があり、この回線種別や拠点間の物理的距離によって若干の伝送遅延が生じることを確認できました。この遅延量は特定のユースケース（遠隔操縦等）を除くと許容できる可能性があるため、UPF の共用も実用可能であると考えられます。遅延量の要件が高いアプリケーションと同一のコア共用環境を使用する場合等は、エンド拠点 UPF を併用する形で共存可能であると考えられます。

(2) 機能について

本実証で用いたA社製5GCシステムは、以下の必要と想定される機能を実装していることを確認しました。

－SIM登録/変更/閲覧
－端末情報の登録/閲覧
－ポリシー情報の登録/閲覧
－アクセス設定（UPF指定制御）
－ログ蓄積/閲覧

これらの機能により、基本的なローカル５Ｇシステムの管理運営は可能であることを確認しました。一方で、「在圏情報」や「トラフィックモニタリング（UPF)」が未実装であったため、例えばサービス型のマルチテナント構成の場合は、顧客ごとの通信容量に応じた従量課金や、テナント毎のUE接続数、RU間のハンドオーバー機能の実装等に影響があると推測できます。

ポリシー制御機能は搭載されており、UEやアプリケーション毎にUPFを選択する柔軟なNW構成を設けることが可能でした。一方で、運用監視、状態監視としてはログ機能のみであるため、異常検知や冗長構成等に対応できていませんでした。今後は監視、運用手法やコア装置の冗長化に関する検証が必要であると考えますし、障害発生時の原因究明から改善措置までを体系化していくことが望まれます。

(3) セキュリティについて

本検証結果により、本検証のすべての構成パターンで、セキュリティが無効化されている場合、同一テナントのコア内のすべての通信が不正に侵入可能であり、検証したすべての攻撃が成立することが確認できました。

そういった攻撃に対し、外部からの攻撃に対してはIPsecのような暗号化機能を持つVPN技術が、内部からの攻撃に対しては各種ファンクション通信(N2 / N3 / N4 / SBA通信)に対応するFirewall機能が効果的であることを確認しました。

それらの機能を備え、複数のユーザーで共用できる仮想アプライアンス製品やIPsec機能を有するセキュリティ機器を採用することで全体のコストを抑えながらセキュリティが担保できると考えます。

(4) コアの共用における運用課題について

本調査研究において、今後コアの共用モデルが普及する上での運用課題は以下の「表 5-4-4-1　運用課題」のとおりと考えます。

表 5-4-4-1　運用課題

課題	内容
共用装置/機能の追加	更なる費用の低廉化に向けて、コア装置、UPF に加えて、CU 機能を共用するモデルを検証
コア装置の冗長構成	コア装置の障害等によりローカル５GNW の断が生じないよう冗長化について検証
運用監視機能の実装 障害時対応等の体系化	機器やノードのアラートを監視/通知する機能を実装し、各機器等の障害時の対応措置について体系化を検討
RU-UE 区間のセキュリティ	5GC-基地局間のセキュリティに加え、RU-UE 区間のセキュリティについて検証し、ローカル５Ｇシステム全体の統合的なセキュリティ措置を検討

6. ユースケース検証

6.1 検証概要

複数企業共用パターン、業界共用パターンそれぞれについてローカル５Ｇを利用するユースケースを想定し、コア設備を共用する環境下においてそれらアプリケーション機能が正常に動作するかを検証しました。また、複数拠点からの同時利用について、UPF の設置位置や地理的距離による差分を比較し、影響を明らかにしました。

(1) 複数企業共用パターン 遠隔支援システム

複数企業共用パターンでは、いすゞ自動車の藤沢工場および NTT 中央研修センタでウェアラブルカメラ・360 度カメラを利用し、遠隔地のモニタ用 PC から熟練作業員が現場の未熟練作業員の作業サポートを行う検証を実施しました。作業者が実施する作業内容及び指示・指導内容についてはいすゞ自動車にヒアリングを実施し、経験値の必要な業務であり、視覚情報で知覚、思考、行動に伴う作業がある業務を選定しました。

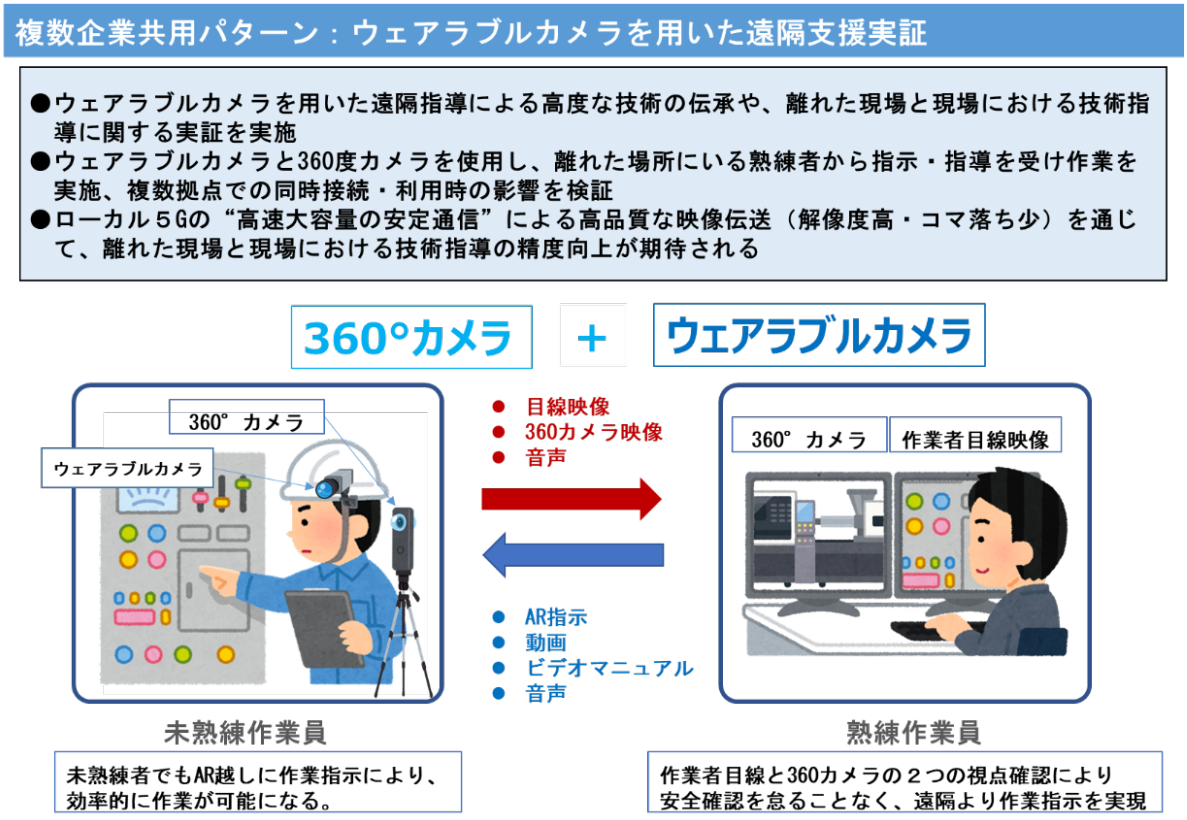


図 1-2-2-1 複数企業共用パターン　ユースケース概要図（再掲）
遠隔支援実証概要

(2) 業界共用パターン AI 顔認証システム

業界共用パターンでは、東北大学、東京大学、京都大学および NTT 中央研修センタで AI 顔認証システムを利用し、4K カメラで撮影した人物に対する AI 顔認証の検証を実施しました。AI 顔認証システムでは、事前に顔写真と名前を登録した人物の人物特定と、属性推定(性別)を行いました。

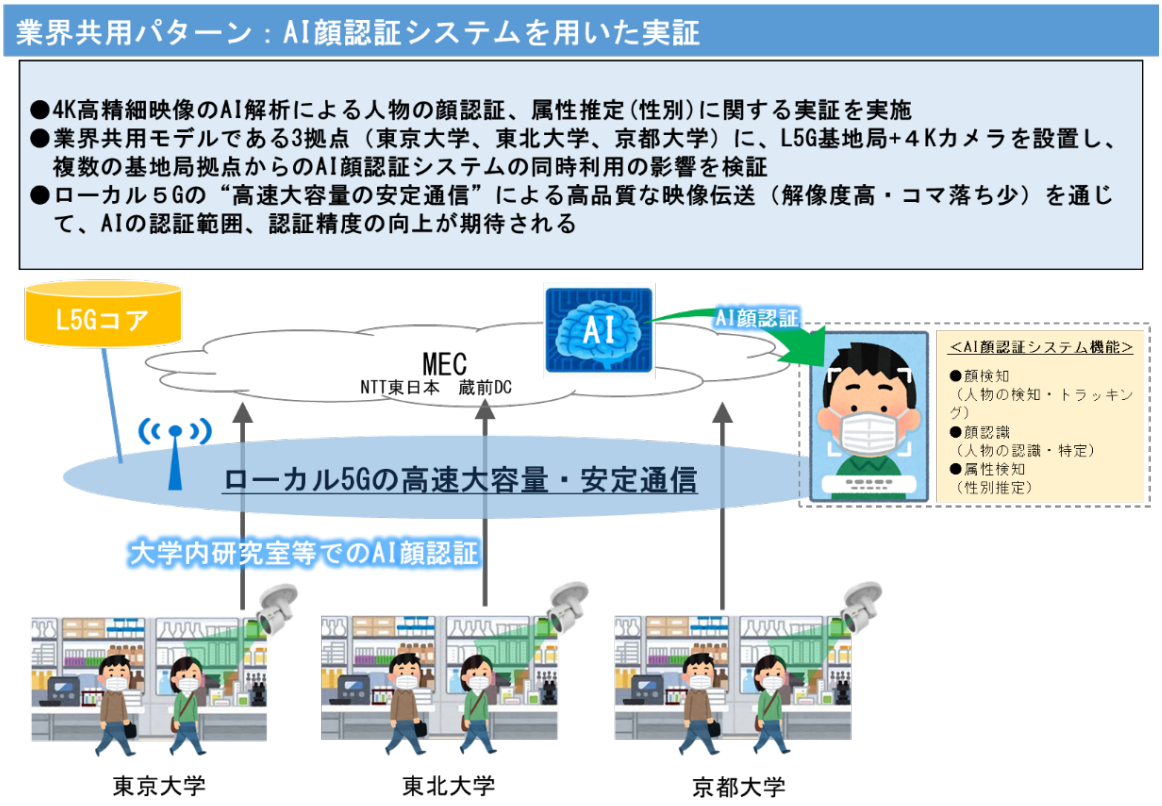


図 1-2-2-2 業界共用パターン　ユースケース概要図（再掲）

6.2 検証環境

(1) 複数企業共用パターン 遠隔支援システム

複数企業共用パターンの検証では、「いすゞ自動車」と「NTT 中央研修センタ」に検証環境を構築しました。

360°カメラとウェアラブルカメラを同一 RU に接続した別々の UE にそれぞれ接続したものを 1 セットとし、いすゞ自動車および NTT 中央研修センタに 2 セットずつ環境を構築しました。作業はいすゞ自動車の 1 セットを使用し、360°カメラの UE は平置きで設置、ウェアラブルカメラの UE は作業者が持ち運びました。遠隔支援者用のモニタ用 PC は、いすゞ自動車の作業場から数百メートル離れた別の部屋（PBX 室）と NTT 中央研修センタにそれぞれ設置し、有線で遠隔支援システムへ接続しました。

各拠点からの遠隔支援システムの MEC 拠点との接続は 1G ベストエフォート回線を使用しました。

遠隔支援システムは、360°カメラの映像配信が可能かつ FullHD での多拠点映像配信が可能なものを選出しました。

表 6-2-1-1 作業者用遠隔支援システム配置内訳

No.	作業員装備セット設置位置	モニタ用 PC 設置位置	備考
1	いすゞ自動車作業場	いすゞ自動車 PBX 室	作業者が使用
2	いすゞ自動車 PBX 室	いすゞ自動車 PBX 室	同時利用検証用
3	NTT 中央研修センタ 1	NTT 中央研修センタ	同時利用検証用
4	NTT 中央研修センタ 2	NTT 中央研修センタ	同時利用検証用

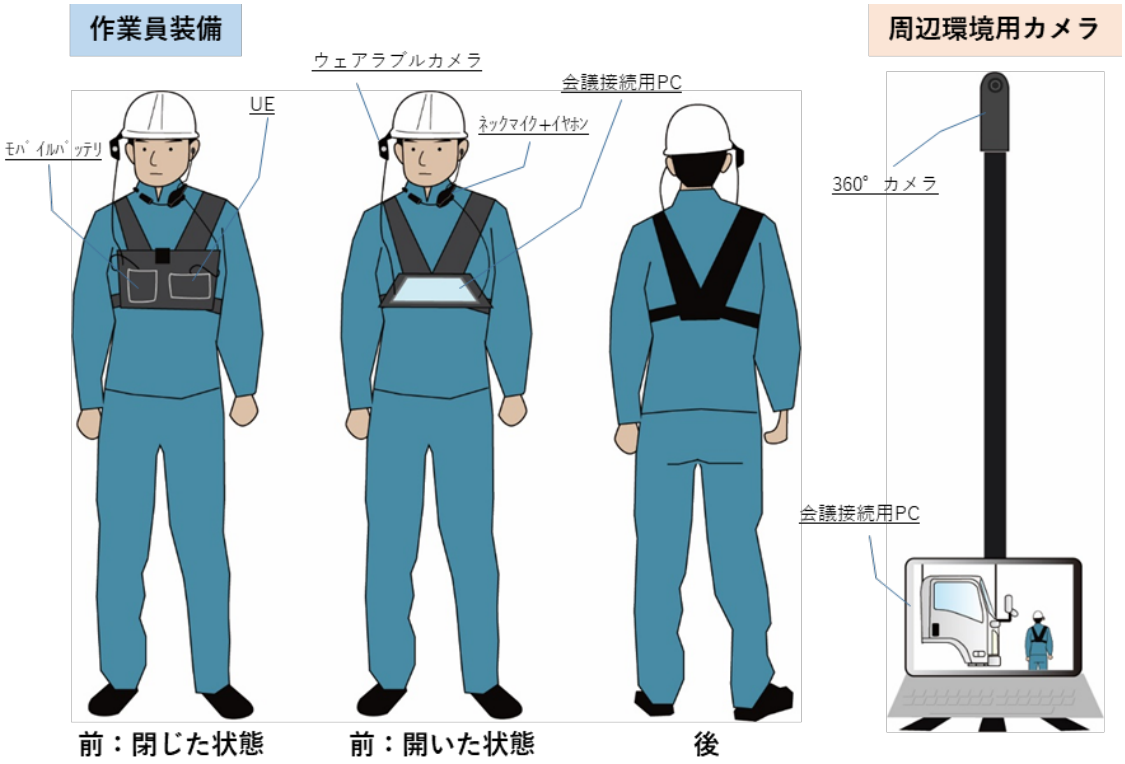


図 6-2-1-1 作業者装備および 360°カメラのイメージ

(2) 業界共用パターン AI 顔認証システム

業界共用パターンの検証では、「東北大学」、「東京大学」、「京都大学」、「NTT 中央研修センタ」に検証環境を構築しました。

UE に接続した 4K カメラを 1 台各拠点に設置し、モニタ用 PC を NTT 中央研修センタに設置しました。NTT 中央研修センタにおける検証環境のイメージとモニタ用 PC 上の画面イメージをそれぞれ「図 6-2-2-1 AI 顔認証システム検証機器イメージ」、「図 6-2-2-2 モニタ用 PC 画面イメージ」に示します。

各拠点からの AI 顔認証システム MEC 拠点との接続は 1G ベストエフォート回線（SDN）を使用しました。

図 6-2-2-1 AI 顔認証システム検証機器イメージ

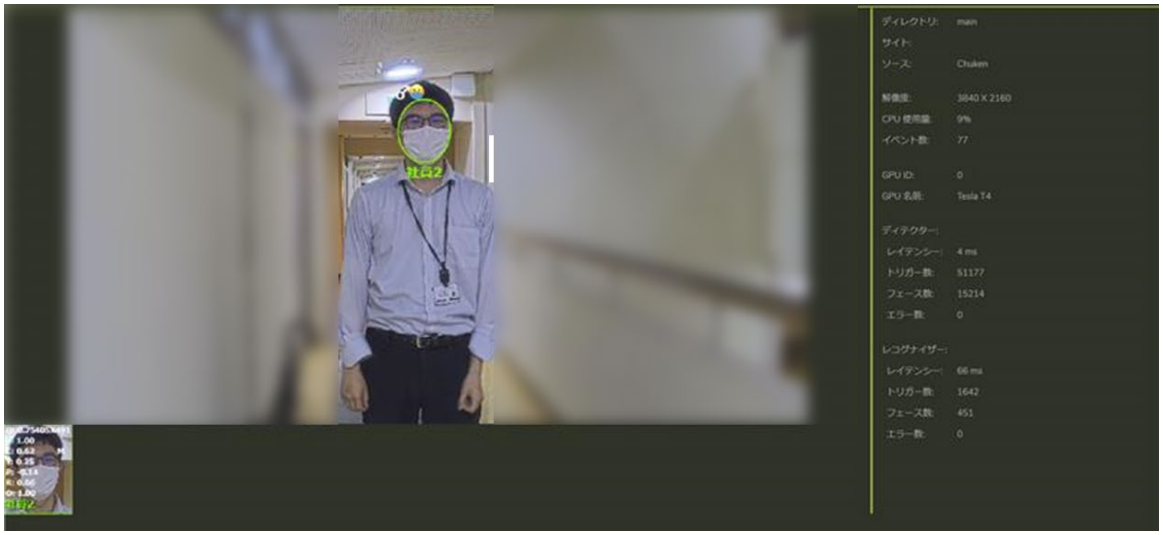


図 6-2-2-2 モニタ用 PC 画面イメージ

AI 顔認証システムは業界最高水準の認識精度と認識スピードを誇る AI 顔認証ソフトウェアを選出しました。

6.3 検証内容

(1) 複数企業共用パターン 遠隔支援システム

複数企業共用パターンでは、いすゞ自動車のトラックのキャブの点検業務に遠隔支援システムを使用しました。検証は NTT 中央研修センタで同様のシステムを起動した状態で行いました。センタ拠点に UPF を設置した場合、エンド拠点に UPF を設置した場合で同様の点検作業を行い、それぞれの作業後に作業者およびモニタ者に使用感に関するアンケートを実施しました。

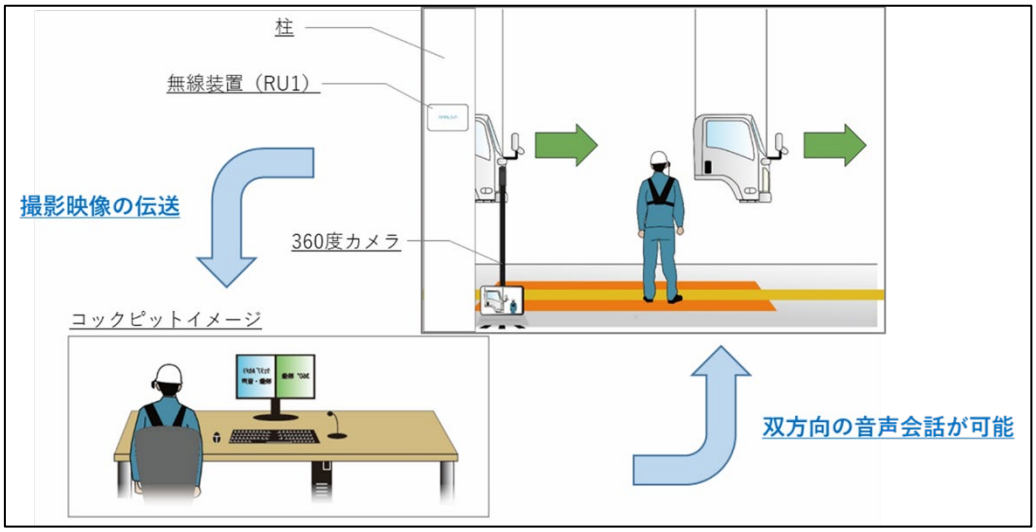


図 6-3-1-1 遠隔支援システム検証イメージ

現場作業員　1回目（UPFセンタ）　2022.3.19

当システムをお使いいただき、それぞれの感想を該当します欄に○またはチェックを入れてくださいご協力の程宜しくお願い致します

項目		評価					コメント
1.映像、音声の精細性（作業現場からコックピットへ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
【記入例】ウェラブルカメラ映像の鮮明度			○				映像は精細だが暗部を撮影した際、細かい所が見にくい
1-1	ウェラブルカメラ映像の鮮明度						
1-2	360° カメラ映像の鮮明度						
1-3	作業員の音声の明瞭度						
1-4	その他ご意見等						
2.音声の精細性（コックピットから作業現場へ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
2-1	コックピットからの音声の明瞭度						
2-2	その他ご意見等						
3.機器のレスポンス（作業現場からコックピットへ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
3-1	映像と音声のズレ（遅延等）						
3-2	映像のカクつきやフリーズ等						
3-3	音声の途切れ						
3-4	その他ご意見等						
4.仕様環境下での操作性および実用性		高い	問題なく運用ができる	どちらとも言えない	問題はあるが運用はできる	低い	
4-1	ウェラブルカメラ						
4-2	360° カメラ						
4-3	チェストハーネスおよびタブレット						
4-4	モバイルルータ						
4-5	ケーブル類						
4-6	全体的な業務における運用の現実性						
4-7	その他ご意見等						

図 6-3-1-2 アンケートフォーマット

(2) 業界共用パターン AI 顔認証システム

業界共用パターンでは、予め顔写真を登録した人物を各大学のカメラで撮影し、NTT 中央研修センタのモニタ用 PC で人物特定および属性推定(性別)の正誤について、検知率を測定しました。検証は中央研修センタで同様のシステムを起動した状態で行いました。センタ拠点に UPF を設置した場合、エンド拠点に UPF を設置した場合でそれぞれ同様の撮影を行いました。

被写体は NTT 東日本社員 2 名(男女 1 名ずつ)とし、いずれもマスクを着用した状態で撮影を行いました。

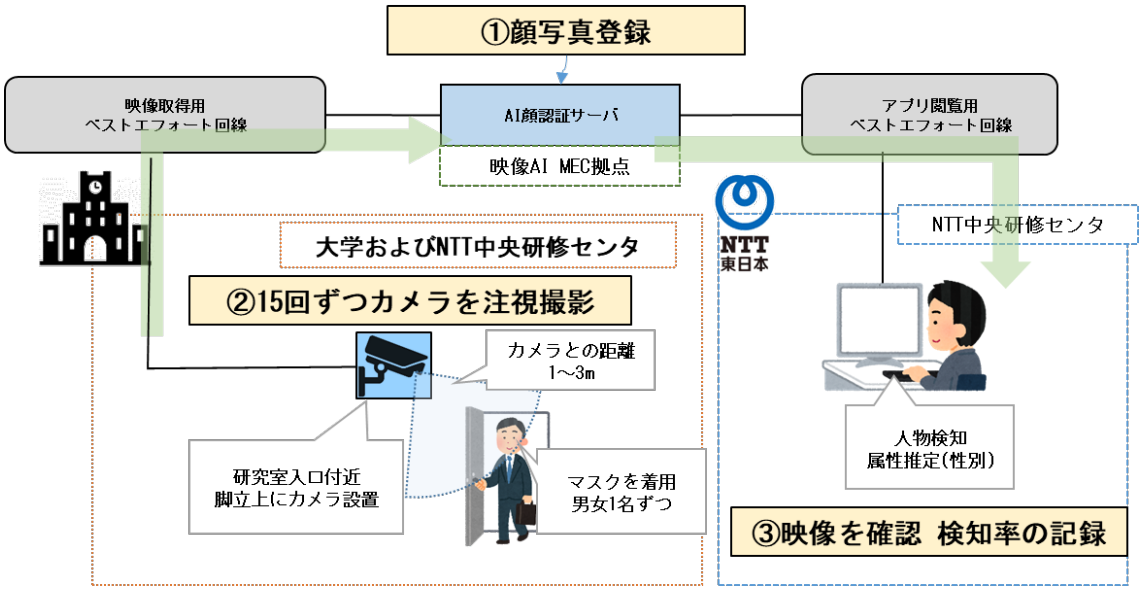


図 6-3-2-1 AI 顔認証システム検証イメージ

表 6-3-2-1 検証パターンおよび検証条件

	条件						
No.	拠点	UPF構成	カメラのパラメータ			人物-カメラ距離	被写体
			画質	配信モード	フレームレート		
1-セ	中央研修センタ	センタUPF	4K (3840 * 2160)	フレームレート指定	30fps	1~3m	マスク着用
1-エ	中央研修センタ	エンドUPF					
2-セ	東北大学(+中央研修センタ)	センタUPF					
2-エ	東北大学(+中央研修センタ)	エンドUPF					
3-セ	東京大学(+中央研修センタ)	センタUPF					
3-エ	東京大学(+中央研修センタ)	エンドUPF					
4-セ	京都大学(+中央研修センタ)	センタUPF					
4-エ	京都大学(+中央研修センタ)	エンドUPF					

6.4 検証結果及び評価・分析

(1) 複数企業共用パターン 遠隔支援システム

いすゞ自動車およびNTT 中央研修センタにて遠隔支援システムを同時に使用し、NTT 中央研修センタおよびいすゞ自動車PBX 室において、下記項目の確認を以て、遠隔支援システムが正常に動作したことを確認しました。

・両拠点ともにモニタ用PC で360° カメラ、ウェアラブルカメラの映像がそれぞれ確認できき、映像が更新され続けること
・両拠点ともに作業者とモニタ者で双方向の音声通話ができること

ただし、いすゞ自動車の作業場における 360° カメラ、ウェアラブルカメラの映像のみ、カクつきやフリーズが見られました。NTT 中央研修センタおよびいすゞ自動車PBX 室では問題なく動作したことを考慮すると、いすゞ自動車の作業場周辺に特有の金属や鉄板素材による乱反射やマルチパスの影響が考えられます。

また、エンド拠点 UPF を使用した場合の方が多少映像のカクつきが改善されたというアンケート結果がありました。これはエンド拠点の UPF を使用することで遠隔支援システムのサーバへの通信を拠点から直接行えるようになり、通信経路が減ったことによる影響と考えられます。一方でエンド拠点 UPF の方がフリーズが増えたというモニタ者アンケートもありますが、これは作業者が検証に慣れた後半にエンド拠点UPF の検証を行った関係で、作業者が試しに遠くまで歩く等、本ユースケース外の検証を行ったことによる影響になります。

表 6-4-1-1 複数拠点同時利用の際のシステムの利用可否(センタ UPF)

作業員装備セット設置位置	モニタ用PC で360° カメラ、ウェアラブルカメラの映像が更新され続けること	音声通話ができること
いすゞ自動車作業場 (アンケート実施)	△ 映像のカクつき有り	○
いすゞ自動車PBX 室	○	○
NTT 中央研修センタ 1	○	○
NTT 中央研修センタ 2	○	○
○はいずれも作業利用に対する問題なし		

表 6-4-1-2 複数拠点同時利用の際のシステムの利用可否(エンド UPF)

作業員装備セット設置位置	モニタ用PC で360° カメラ、ウェアラブルカメラの映像が更新され続けること	音声通話ができること
いすゞ自動車作業場 (アンケート実施)	△ 映像のカクつき有り センタ UPF と比較して多少改善	○

いすゞ自動車 PBX 室	○	○
NTT 中央研修センタ 1	○	○
NTT 中央研修センタ 2	○	○
○はいずれも作業利用に対する問題なし		

現場作業員　1回目（UPFセンタ）　2022.3.19

当システムをお使いいただき、それぞれの感想を該当します欄に○またはチェックを入れてくださいご協力の程宜しくお願い致します

項目		評価					コメント
1.映像、音声の精細性（作業現場からコックピットへ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
【記入例】ウェラブルカメラ映像の鮮明度			○				映像は精細だが暗部を撮影した際、細かい所が見にくい
1-1	ウェラブルカメラ映像の鮮明度						
1-2	360°カメラ映像の鮮明度						
1-3	作業員の音声の明瞭度						
1-4	その他ご意見等						
2.音声の精細性（コックピットから作業現場へ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
2-1	コックピットからの音声の明瞭度	○					
2-2	その他ご意見等	問題なく良く聞こえ、遅れ等感じませんでした					
3.機器のレスポンス（作業現場からコックピットへ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
3-1	映像と音声のズレ（遅延等）						
3-2	映像のカクつきやフリーズ等						
3-3	音声の途切れ						
3-4	その他ご意見等						
4.仕様環境下での操作性および実用性		高い	問題なく運用ができる	どちらとも言えない	問題はあるが運用はできる	低い	
4-1	ウェラブルカメラ			○			
4-2	360° カメラ			○			
4-3	チェストハーネスおよびタブレット				○		
4-4	モバイルルータ			○			
4-5	ケーブル類				○		
4-6	全体的な業務における運用の現実性			○			
4-7	その他ご意見等	長時間身に付けると重さで疲れそう。通常より腕の可動域が小さくなるので肩が凝りそう。 ケーブルがよりスッキリすると良い。					

図 6-4-1-1 作業者アンケート（センタ UPF）

コックピット側　1回目（UPFセンタ）　　2022.3.19

当システムをお使いいただき、それぞれの感想を該当します欄に○またはチェックを入れてくださいご協力の程宜しくお願い致します

項目		評価					コメント
1.映像、音声の精細性（作業現場からコックピットへ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
【記入例】ウェラブルカメラ映像の鮮明度			○				映像は精細だが暗部を撮影した際、細かい所が見にくい
1-1	ウェラブルカメラ映像の鮮明度				○		品番等の文字の判別が困難
1-2	360°カメラ映像の鮮明度					○	部品形状の判別が困難
1-3	作業員の音声の明瞭度	○					問題なし
1-4	その他ご意見等						
2.音声の精細性（コックピットから作業現場へ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
2-1	コックピットからの音声の明瞭度						
2-2	その他ご意見等						
3.機器のレスポンス（作業現場からコックピットへ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
3-1	映像と音声のズレ（遅延等）	○					問題なし
3-2	映像のカクつきやフリーズ等			○			特定の条件下において、カクツキ、フリーズ有
3-3	音声の途切れ	○					問題なし
3-4	その他ご意見等						
4.仕様環境下での操作性および実用性		高い	問題なく運用ができる	どちらとも言えない	問題はあるが運用はできる	低い	
4-1	ウェラブルカメラ					○	画質の面で運用は困難
4-2	360°カメラ					○	操作性は良いが、画質の面で運用は困難
4-3	チェストハーネスおよびタブレット						
4-4	モバイルルータ						
4-5	ケーブル類						
4-6	全体的な業務における運用の現実性					○	通信の安定性と、画質の向上がないと、運用は困難
4-7	その他ご意見等						

図 6-4-1-2 モニタ者アンケート（センタ UPF）

現場作業員　2回目（UPFエンド）　　2022.3.19

当システムをお使いいただき、それぞれの感想を該当します欄に○またはチェックを入れてくださいご協力の程宜しくお願い致します

項目		評価					コメント
1.映像、音声の精細性（作業現場からコックピットへ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
【記入例】ウェラブルカメラ映像の鮮明度			○				映像は精細だが暗部を撮影した際、細かい所が見にくい
1-1	ウェラブルカメラ映像の鮮明度						
1-2	360°カメラ映像の鮮明度						
1-3	作業員の音声の明瞭度						
1-4	その他ご意見等						
2.音声の精細性（コックピットから作業現場へ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
2-1	コックピットからの音声の明瞭度	○					
2-2	その他ご意見等						
3.機器のレスポンス（作業現場からコックピットへ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
3-1	映像と音声のズレ（遅延等）						
3-2	映像のカクつきやフリーズ等						
3-3	音声の途切れ						
3-4	その他ご意見等						
4.仕様環境下での操作性および実用性		高い	問題なく運用ができる	どちらとも言えない	問題はあるが運用はできる	低い	
4-1	ウェラブルカメラ			○			
4-2	360°カメラ			○			
4-3	チェストハーネスおよびタブレット				○		
4-4	モバイルルータ			○			
4-5	ケーブル類				○		
4-6	全体的な業務における運用の現実性			○			
4-7	その他ご意見等	通信せずフリーズor落ちた時、自動で再起動すると良い。　バッテリーが落下したので、落ちない仕組みが必要。 タブレットを見ながら上体を倒すと、上下反転してしまう、戻そうとするとつい電源ボタンを押してしまう。					

図 6-4-1-3 作業者アンケート（エンド UPF）

コックピット側　2回目（UPFエンド）							2022.3.19
当システムをお使いいただき、それぞれの感想を該当します欄に〇またはチェックを入れてくださいご協力の程宜しくお願い致します							
項目		評価					コメント
1.映像、音声の精細性（作業現場からコックピットへ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
【記入例】ウェラブルカメラ映像の鮮明度			〇				映像は精細だが暗部を撮影した際、細かい所が見にくい
1-1	ウェラブルカメラ映像の鮮明度			〇			1回目より良い
1-2	360°カメラ映像の鮮明度				〇		1回目より良い
1-3	作業員の音声の明瞭度	〇					
1-4	その他ご意見等						
2.音声の精細性（コックピットから作業現場へ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
2-1	コックピットからの音声の明瞭度						
2-2	その他ご意見等						
3.機器のレスポンス（作業現場からコックピットへ）		とても良い	どちらかというと良い	どちらでもない	どちらかというと悪い	悪い	
3-1	映像と音声のズレ（遅延等）	〇					問題なし
3-2	映像のカクつきやフリーズ等				〇		1回目よりフリーズが多かった
3-3	音声の途切れ				〇		1回目よりフリーズが多かった
3-4	その他ご意見等						
4.仕様環境下での操作性および実用性		高い	問題なく運用ができる	どちらとも言えない	問題はあるが運用はできる	低い	
4-1	ウェラブルカメラ					〇	フリーズが多く、運用は困難
4-2	360°カメラ					〇	画質の面で運用は困難
4-3	チェストハーネスおよびタブレット						
4-4	モバイルルータ						
4-5	ケーブル類						
4-6	全体的な業務における運用の現実性					〇	1回目より画質は良いがフリーズが多く、運用は困難
4-7	その他ご意見等	アンテナの向きやバッテリーにも課題有り					

図 6-4-1-4 モニタ者アンケート（エンド UPF）

(2) 業界共用パターン AI 顔認証システム

各大学と NTT 中央研修センタにおいて AI 顔認証システムを使用し、下記項目の確認を以て、AI 顔認証が正常に動作したことを確認しました。

・モニタ用 PC で 4K カメラの映像が確認でき、映像が更新され続けること
・AI 顔認証システムにより映像から人物検知および属性推定(性別)が行えること

また、各大学と NTT 中央研修センタの 2 拠点ずつにおいて AI 顔認証システムを使用し、下記項目の確認を以て、複数拠点同時接続による影響がないことを確認しました。

・各大学の映像について、単拠点でシステムを利用した場合と同様に、NTT 中央研修センタの接続を行った場合も映像伝送と人物検知と属性推定(性別)が行えること

センタ拠点に UPF を設置した場合と、エンド拠点に UPF を設置した場合による映像伝送への影響や検知率への影響は見られませんでした。

表 6-4-2-1 検証結果全体

	条件				映像伝送	検知率	
	拠点	画質	人物―カメラ距離	UPF 構成	○ or ×	人物推定	属性推定
1-セ	NTT 中央研修センタ	4K	1～3m	センタ UPF	○	100%	100%
1-エ	NTT 中央研修センタ	4K	1～3m	エンド UPF	○	100%	100%
2-セ	東北大学 (+NTT 中央研修センタ)	4K	1～3m	センタ UPF	○	100%	100%
2-エ	東北大学 (+NTT 中央研修センタ)	4K	1～3m	エンド UPF	○	100%	100%
3-セ	東京大学 (+NTT 中央研修センタ)	4K	1～3m	センタ UPF	○	100%	100%
3-エ	東京大学 (+NTT 中央研修センタ)	4K	1～3m	エンド UPF	○	100%	100%
4-セ	京都大学 (+NTT 中央研修センタ)	4K	1～3m	センタ UPF	○	100%	83.3%
4-エ	京都大学 (+NTT 中央研修センタ)	4K	1～3m	エンド UPF	○	100%	86.7%

表 6-4-2-2 中央研修センタ センタ UPF 構成

拠点	UPF 構成	映像伝送	人物推定	属性推定
NTT 中央研修センタ	センタ UPF	○	100%	100%

No.	人物推定		属性推定		No.	人物推定		属性推定	
	人物	検知	性別	検知		人物	検知	性別	検知
A-1	社員 1	社員 1	F	F	B-1	社員 2	社員 2	M	M
A-2	社員 1	社員 1	F	F	B-2	社員 2	社員 2	M	M
A-3	社員 1	社員 1	F	F	B-3	社員 2	社員 2	M	M
A-4	社員 1	社員 1	F	F	B-4	社員 2	社員 2	M	M
A-5	社員 1	社員 1	F	F	B-5	社員 2	社員 2	M	M
A-6	社員 1	社員 1	F	F	B-6	社員 2	社員 2	M	M
A-7	社員 1	社員 1	F	F	B-7	社員 2	社員 2	M	M
A-8	社員 1	社員 1	F	F	B-8	社員 2	社員 2	M	M
A-9	社員 1	社員 1	F	F	B-9	社員 2	社員 2	M	M
A-10	社員 1	社員 1	F	F	B-10	社員 2	社員 2	M	M
A-11	社員 1	社員 1	F	F	B-11	社員 2	社員 2	M	M
A-12	社員 1	社員 1	F	F	B-12	社員 2	社員 2	M	M
A-13	社員 1	社員 1	F	F	B-13	社員 2	社員 2	M	M
A-14	社員 1	社員 1	F	F	B-14	社員 2	社員 2	M	M
A-15	社員 1	社員 1	F	F	B-15	社員 2	社員 2	M	M
検知率	100%		100%		検知率	100%		100%	

表 6-4-2-3 中央研修センタ エンド UPF 構成

拠点	UPF 構成	映像伝送	人物推定	属性推定
NTT 中央研修センタ	エンド UPF	○	100%	100%

No.	人物推定		属性推定		No.	人物推定		属性推定	
	人物	検知	性別	検知		人物	検知	性別	検知
A-1	社員 1	社員 1	F	F	B-1	社員 2	社員 2	M	M
A-2	社員 1	社員 1	F	F	B-2	社員 2	社員 2	M	M
A-3	社員 1	社員 1	F	F	B-3	社員 2	社員 2	M	M
A-4	社員 1	社員 1	F	F	B-4	社員 2	社員 2	M	M
A-5	社員 1	社員 1	F	F	B-5	社員 2	社員 2	M	M
A-6	社員 1	社員 1	F	F	B-6	社員 2	社員 2	M	M
A-7	社員 1	社員 1	F	F	B-7	社員 2	社員 2	M	M
A-8	社員 1	社員 1	F	F	B-8	社員 2	社員 2	M	M
A-9	社員 1	社員 1	F	F	B-9	社員 2	社員 2	M	M
A-10	社員 1	社員 1	F	F	B-10	社員 2	社員 2	M	M
A-11	社員 1	社員 1	F	F	B-11	社員 2	社員 2	M	M
A-12	社員 1	社員 1	F	F	B-12	社員 2	社員 2	M	M
A-13	社員 1	社員 1	F	F	B-13	社員 2	社員 2	M	M
A-14	社員 1	社員 1	F	F	B-14	社員 2	社員 2	M	M
A-15	社員 1	社員 1	F	F	B-15	社員 2	社員 2	M	M
検知率	100%		100%		検知率	100%		100%	

表 6-4-2-4 東北大学＋NTT 中央研修センタ センタ UPF 構成

拠点	UPF 構成	映像伝送	人物推定	属性推定
東北大＋NTT 中央研修センタ	センタ UPF	○	100%	100%

No.	人物推定		属性推定		No.	人物推定		属性推定	
	人物	検知	性別	検知		人物	検知	性別	検知
A-1	社員 1	社員 1	F	F	B-1	社員 2	社員 2	M	M
A-2	社員 1	社員 1	F	F	B-2	社員 2	社員 2	M	M
A-3	社員 1	社員 1	F	F	B-3	社員 2	社員 2	M	M
A-4	社員 1	社員 1	F	F	B-4	社員 2	社員 2	M	M
A-5	社員 1	社員 1	F	F	B-5	社員 2	社員 2	M	M
A-6	社員 1	社員 1	F	F	B-6	社員 2	社員 2	M	M
A-7	社員 1	社員 1	F	F	B-7	社員 2	社員 2	M	M
A-8	社員 1	社員 1	F	F	B-8	社員 2	社員 2	M	M
A-9	社員 1	社員 1	F	F	B-9	社員 2	社員 2	M	M
A-10	社員 1	社員 1	F	F	B-10	社員 2	社員 2	M	M
A-11	社員 1	社員 1	F	F	B-11	社員 2	社員 2	M	M
A-12	社員 1	社員 1	F	F	B-12	社員 2	社員 2	M	M
A-13	社員 1	社員 1	F	F	B-13	社員 2	社員 2	M	M
A-14	社員 1	社員 1	F	F	B-14	社員 2	社員 2	M	M
A-15	社員 1	社員 1	F	F	B-15	社員 2	社員 2	M	M
検知率	100%		100%		検知率	100%		100%	

表 6-4-2-5 東北大学＋NTT 中央研修センタ エンド UPF 構成

拠点	UPF 構成	映像伝送	人物推定	属性推定
東北大＋NTT 中央研修センタ	エンド UPF	○	100%	100%

No.	人物推定		属性推定		No.	人物推定		属性推定	
	人物	検知	性別	検知		人物	検知	性別	検知
A-1	社員 1	社員 1	F	F	B-1	社員 2	社員 2	M	M
A-2	社員 1	社員 1	F	F	B-2	社員 2	社員 2	M	M
A-3	社員 1	社員 1	F	F	B-3	社員 2	社員 2	M	M
A-4	社員 1	社員 1	F	F	B-4	社員 2	社員 2	M	M
A-5	社員 1	社員 1	F	F	B-5	社員 2	社員 2	M	M
A-6	社員 1	社員 1	F	F	B-6	社員 2	社員 2	M	M
A-7	社員 1	社員 1	F	F	B-7	社員 2	社員 2	M	M
A-8	社員 1	社員 1	F	F	B-8	社員 2	社員 2	M	M
A-9	社員 1	社員 1	F	F	B-9	社員 2	社員 2	M	M
A-10	社員 1	社員 1	F	F	B-10	社員 2	社員 2	M	M
A-11	社員 1	社員 1	F	F	B-11	社員 2	社員 2	M	M
A-12	社員 1	社員 1	F	F	B-12	社員 2	社員 2	M	M
A-13	社員 1	社員 1	F	F	B-13	社員 2	社員 2	M	M

A-14	社員 1	社員 1	F	F	B-14	社員 2	社員 2	M	M
A-15	社員 1	社員 1	F	F	B-15	社員 2	社員 2	M	M
検知率	100%		100%		検知率	100%		100%	

表 6-4-2-6 東京大学＋NTT 中央研修センタ センタ UPF 構成

拠点	UPF 構成	映像伝送	人物推定	属性推定
東大＋NTT 中央研修センタ	センタ UPF	○	100%	100%

No.	人物推定		属性推定		No.	人物推定		属性推定	
	人物	検知	性別	検知		人物	検知	性別	検知
A-1	社員 1	社員 1	F	F	B-1	社員 2	社員 2	M	M
A-2	社員 1	社員 1	F	F	B-2	社員 2	社員 2	M	M
A-3	社員 1	社員 1	F	F	B-3	社員 2	社員 2	M	M
A-4	社員 1	社員 1	F	F	B-4	社員 2	社員 2	M	M
A-5	社員 1	社員 1	F	F	B-5	社員 2	社員 2	M	M
A-6	社員 1	社員 1	F	F	B-6	社員 2	社員 2	M	M
A-7	社員 1	社員 1	F	F	B-7	社員 2	社員 2	M	M
A-8	社員 1	社員 1	F	F	B-8	社員 2	社員 2	M	M
A-9	社員 1	社員 1	F	F	B-9	社員 2	社員 2	M	M
A-10	社員 1	社員 1	F	F	B-10	社員 2	社員 2	M	M
A-11	社員 1	社員 1	F	F	B-11	社員 2	社員 2	M	M
A-12	社員 1	社員 1	F	F	B-12	社員 2	社員 2	M	M
A-13	社員 1	社員 1	F	F	B-13	社員 2	社員 2	M	M
A-14	社員 1	社員 1	F	F	B-14	社員 2	社員 2	M	M
A-15	社員 1	社員 1	F	F	B-15	社員 2	社員 2	M	M
検知率	100%		100%		検知率	100%		100%	

表 6-4-2-7 東京大学+中央研修センタ エンド UPF 構成

拠点	UPF 構成	映像伝送	人物推定	属性推定
東大＋NTT 中央研修センタ	エンド UPF	○	100%	100%

No.	人物推定		属性推定		No.	人物推定		属性推定	
	人物	検知	性別	検知		人物	検知	性別	検知
A-1	社員 1	社員 1	F	F	B-1	社員 2	社員 2	M	M
A-2	社員 1	社員 1	F	F	B-2	社員 2	社員 2	M	M
A-3	社員 1	社員 1	F	F	B-3	社員 2	社員 2	M	M
A-4	社員 1	社員 1	F	F	B-4	社員 2	社員 2	M	M
A-5	社員 1	社員 1	F	F	B-5	社員 2	社員 2	M	M
A-6	社員 1	社員 1	F	F	B-6	社員 2	社員 2	M	M
A-7	社員 1	社員 1	F	F	B-7	社員 2	社員 2	M	M
A-8	社員 1	社員 1	F	F	B-8	社員 2	社員 2	M	M
A-9	社員 1	社員 1	F	F	B-9	社員 2	社員 2	M	M

A-10	社員 1	社員 1	F	F	B-10	社員 2	社員 2	M	M
A-11	社員 1	社員 1	F	F	B-11	社員 2	社員 2	M	M
A-12	社員 1	社員 1	F	F	B-12	社員 2	社員 2	M	M
A-13	社員 1	社員 1	F	F	B-13	社員 2	社員 2	M	M
A-14	社員 1	社員 1	F	F	B-14	社員 2	社員 2	M	M
A-15	社員 1	社員 1	F	F	B-15	社員 2	社員 2	M	M
検知率	100%		100%		検知率	100%		100%	

表 6-4-2-8 京都大学＋中央研修センタ センタ UPF

拠点	UPF 構成	映像伝送	人物推定	属性推定
京大＋NTT 中央研修センタ	センタ UPF	○	100%	83.3%

No.	人物推定		属性推定		No.	人物推定		属性推定	
	人物	検知	性別	検知		人物	検知	性別	検知
A-1	社員 1	社員 1	F	F	B-1	社員 2	社員 2	M	M
A-2	社員 1	社員 1	F	F	B-2	社員 2	社員 2	M	M
A-3	社員 1	社員 1	F	F	B-3	社員 2	社員 2	M	F
A-4	社員 1	社員 1	F	F	B-4	社員 2	社員 2	M	M
A-5	社員 1	社員 1	F	F	B-5	社員 2	社員 2	M	M
A-6	社員 1	社員 1	F	F	B-6	社員 2	社員 2	M	M
A-7	社員 1	社員 1	F	F	B-7	社員 2	社員 2	M	F
A-8	社員 1	社員 1	F	F	B-8	社員 2	社員 2	M	M
A-9	社員 1	社員 1	F	F	B-9	社員 2	社員 2	M	M
A-10	社員 1	社員 1	F	F	B-10	社員 2	社員 2	M	F
A-11	社員 1	社員 1	F	F	B-11	社員 2	社員 2	M	F
A-12	社員 1	社員 1	F	F	B-12	社員 2	社員 2	M	M
A-13	社員 1	社員 1	F	F	B-13	社員 2	社員 2	M	M
A-14	社員 1	社員 1	F	F	B-14	社員 2	社員 2	M	M
A-15	社員 1	社員 1	F	F	B-15	社員 2	社員 2	M	F
検知率	100%		100%		検知率	100%		66.7%	

表 6-4-2-9 京都大学+中央研修センタ エンド UPF

拠点	UPF 構成	映像伝送	人物推定	属性推定
京大＋NTT 中央研修センタ	エンド UPF	○	100%	86.7%

No.	人物推定		属性推定		No.	人物推定		属性推定	
	人物	検知	性別	検知		人物	検知	性別	検知
A-1	社員 1	社員 1	F	F	B-1	社員 2	社員 2	M	M
A-2	社員 1	社員 1	F	F	B-2	社員 2	社員 2	M	M
A-3	社員 1	社員 1	F	F	B-3	社員 2	社員 2	M	M
A-4	社員 1	社員 1	F	F	B-4	社員 2	社員 2	M	M
A-5	社員 1	社員 1	F	F	B-5	社員 2	社員 2	M	F

A-6	社員 1	社員 1	F	F	B-6	社員 2	社員 2	M	M
A-7	社員 1	社員 1	F	F	B-7	社員 2	社員 2	M	M
A-8	社員 1	社員 1	F	F	B-8	社員 2	社員 2	M	F
A-9	社員 1	社員 1	F	F	B-9	社員 2	社員 2	M	F
A-10	社員 1	社員 1	F	F	B-10	社員 2	社員 2	M	M
A-11	社員 1	社員 1	F	F	B-11	社員 2	社員 2	M	M
A-12	社員 1	社員 1	F	F	B-12	社員 2	社員 2	M	M
A-13	社員 1	社員 1	F	F	B-13	社員 2	社員 2	M	M
A-14	社員 1	社員 1	F	F	B-14	社員 2	社員 2	M	F
A-15	社員 1	社員 1	F	F	B-15	社員 2	社員 2	M	M
検知率	100%		100%		検知率	100%		73.3%	

(3) 考察

複数企業共用パターン、業界共用パターンのいずれもコア共用の構成で各システムが動作することが確認できました。また、マルチテナントの構成で複数拠点が同時にシステムを利用してもシステム利用に影響を与えないことが確認できました。

・複数ユーザー同時利用について

今回の検証により複数の企業がアプリケーションを提供する同一の MEC 拠点にアクセスする構成において、今回のユースケースでは２ユーザーの同時利用ができることを確認できました。MEC 拠点への U-plane 通信はユーザーごとに独立しているため、コア共用による影響はないものと考えます。

・UPF 構成について

遠隔支援システムにおいては遠隔支持者と作業者がリアルタイムで連携する必要があるため低遅延性が要求され、エンド UPF 構成が望ましいと考えられます。一方で AI 顔認証システムにおいてはセンタ UPF でも顔認証の品質に問題がなかったため、センタ UPF の構成でも問題ないと思われます。

・トラフィック設計について

今回はいずれのユースケースの全拠点とも 1 拠点あたり 20Mbps ほどの想定トラフィックであったため準同期 TDD 方式を採用しました。実際の運用を考える場合、カメラの要求帯域 × 台数により計算される必要帯域について、無線区間における実行 UL スループットおよび MEC 接続回線や拠点間回線(センタ UPF の場合)の帯域設計が必要と考えます。

また、今回の検証では限界負荷試験を行っていないので、同時接続拠点数の増加や、カメラ台数の増加によるトラフィック流量を変えての検証は今後検証すべき課題となります。

・無線設計について

工場環境が想定されるユースケースでは、金属や鉄板による乱反射やマルチパスによる影響が考えられるため、事前に詳細な電波調査を実施した上での無線設計が必要だと考えます。

7. コア共用モデルの普及展開

7.1 コア共用に係るニーズと課題

(1) コア共用ニーズ及び想定ユースケース

コア共用モデルの普及に向け展開シナリオの検討及び共用化のメリットについて整理をしました。ローカル５Ｇの潜在ユーザーにおいては、現在のSI型（オンプレ型コア＋ソリューション構築）で提供可能なローカル５Ｇ環境提供価格と、ユーザーが求めている価格の間に大きなギャップがあります。今後、地域の自治体や中堅・中小企業等の5G関連の新製品や新技術の開発に対するサポートから導入促進を想定すると、コア設備等の共用に基づくプラットフォームの提供については、経済合理性の観点から必然性が高いといえます。また、ローカル５Ｇのユースケースと組合せ展開シナリオを考えた場合、以下のとおり共用化のメリットを挙げることができます。

表 7-1-1-1　ローカル５Ｇ展開シナリオと共用化メリット

視点	現状のローカル５Ｇ構築	今後のローカル５Ｇ展開シナリオ ⇒　コア設備等の共用ニーズ	共用化のメリット
エリア	特定のエリアや拠点で構築 例：○○地区に基地局を設置	地域内（県域等）で様々なユーザーが構築を進める。 ⇒　各ユーザーのコストを抑えるため地域内でコアを共用したい。トラフィックの地産地消化を目指したい。	地域IXとの連携（ローカルブレークアウト）によるトラフィックコストの低減 地域の通信基盤の魅力向上（コア共用で安く5Gを利用できる⇒企業誘致等）
ユーザー	特定の単一拠点で構築 例：民企業の工場にオンプレで構築	企業が複数拠点で構築を進める。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。 ⇒　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	システムの最適化・一元化等によるコスト低減 他のプラットフォームやシステムとの接続・連携
ユースケース	特定のユースケースや性能要件に応じて最適なNW構成で構築 例：低遅延が求められるため、コア(UPF)をユーザー設備内にオンプレで構築	ユーザーが多様なユースケースの実装が進める。 例：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。 ⇒　ユースケース毎にNWを構築するのではなく、コア共用する等でNWを再構成しつつ複数のユースケースを実装したい。	5Gの特性を活かした多様なユースケースの実装

また、上記ユースケース別の展開シナリオにより以下のとおり業界共用パターン、複数企業共用パターン(同一エリア)、複数企業共用パターン(複数地域)モデルの３のパターンが挙げられます。

表 7-1-1-2　共用モデルのパターン

パターン	モデルの概要
① 業界共用パターン	・ユーザーが複数拠点でコア共用形態を実装する。 ・拠点内 and/or 各拠点で異なる 5G アプリケーションの要件を有し、それぞれの要件を満たすための共用形態を構成する。 ・大手企業はユーザー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、企業規模・共用形態のバリエーション等でモデルをさらに分けることができる。 ・設備・機能をユーザー施設内または事業者施設に具備する。 ・MEC and/or クラウド側のサーバ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。
② 複数企業共用パターン(同一エリア)	・一定のエリア（県・地域ブロック等）内で、複数のユーザー間でコア共用形態を実装する。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構成する。 ・各ユーザーで異なる 5G アプリケーションの要件を有し、それぞれの要件を満たすための共用形態を構成する。 ・設備・機能を特定のユーザー施設、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）に具備する。必要に応じて、監視・管理機能等も具備する。 ・MEC and/or クラウド側のサーバでアプリケーションを実装し、ユーザー企業間でアプリケーションやデータ等を共用する。
③ 複数企業共用パターン(複数地域)	・上記①や②の組み合わせやプラットフォーム型のコアネットワークインフラとの連携で、より広域で複数地域における拠点でコア共用形態を実装する。 ・コアネットワーク同士の相互接続や多段構成（冗長化含む）等を実装し、シームレスな利用を実現する各種機能（管理・認証等）を具備する。

7.2 ローカル５Ｇ（相互接続・コア共用等）に関するユーザー意向調査

「7.1 コア共用に係るニーズと課題」を踏まえローカル５Ｇ市場が立ち上がり段階であり、かつ同市場の普及仮説として相互接続・コア共用等ニーズについて検証することから、企業・団体の規模や業種等を問わず幅広く調査を実施しました。具体的には、事前調査と本調査による二段階調査を実施し、事前調査において回答者の所属する企業・団体の業種や規模、意思決定等の関与度などに応じて割付を行い、本調査を実施しました。

表 7-2-1　調査内容

区分	内容
調査対象	2022 年 2 月 （同様の設計で実施した２０２１年２月調査との比較を実施）
調査方法	Ｗｅｂアンケートによる二段階調査を実施。 事前調査：５Ｇとの関わり方等の把握及び企業・団体のスクリーニング 本調査：ローカル５Ｇ等をソリューションの利用意向や課題等を聴取 ※本調査では、自社・団体の ICT の導入・利活用に関する判断権限または知識を有する人に限定
本調査対象	全国の民間企業及び地方公共団体に所属する個人、本社または所属事業所等は問わない。以下の２区分を対象とした。
実施時期	一次産業を除き、事業所統計に基づき業種・規模区分別に比例割付。規模は中小企業庁の定義に基づき、従業員数をもとに定義

7.3 調査結果

(1) ローカル５Ｇの免許・導入主体に関する意向

ローカル５Ｇの導入・利活用の積極的なユーザーにおいては、自前（免許取得や無線システム・ネットワーク導入等）意向が高い一方、今後導入・利活用しうる潜在層においては、現時点では他社への依存度が高い傾向がみられました。

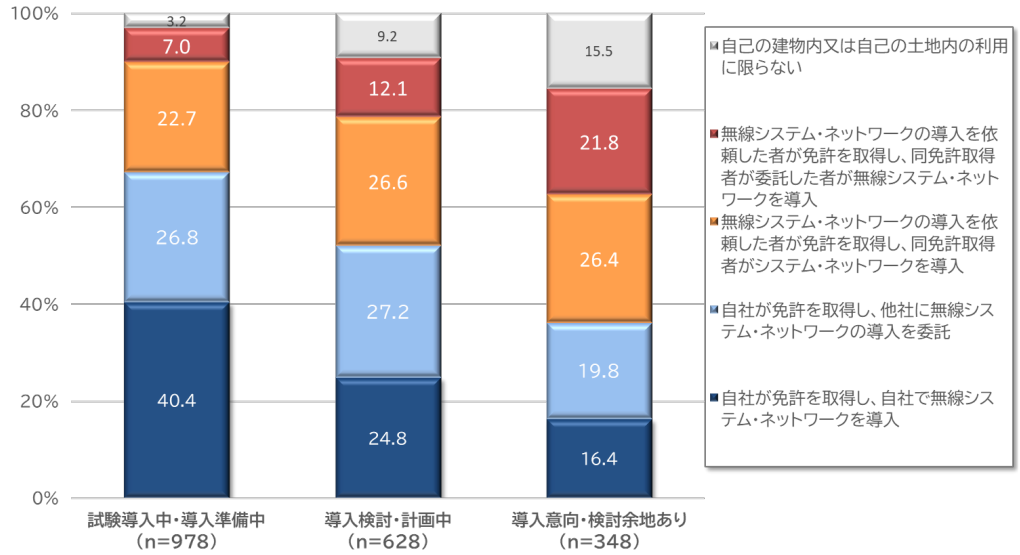


図 7-3-1-1　ローカル５Ｇの免許・導入主体に関する意向

(2) ローカル５Ｇの運用形態に関する意向

ローカル５Ｇの導入・利活用の積極的なユーザーにおいては、自営型の意向が高い一方、今後導入・利活用しうる潜在層においては、現時点ではアウトソーシング型やサービス利用型の意向が高い傾向がみられました。普及展開に向けては、後者のニーズへの対応が求められると想定され、コアネットワークの共用の潜在的ニーズがあると考えられます。

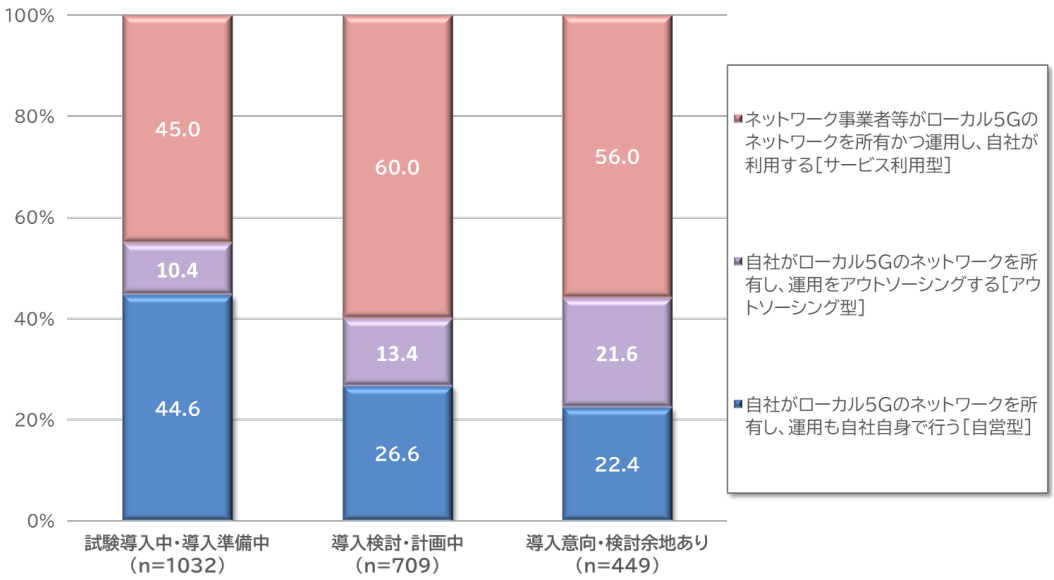


図 7-3-2-1　ローカル５Ｇの運用形態に関する意向

また、令和２年度の調査と比較すると令和３年度は「同一企業内・複数拠点間でのローカル５Ｇのネットワークの共有・一元的な運用」に対するニーズは増大していることがわかりました。

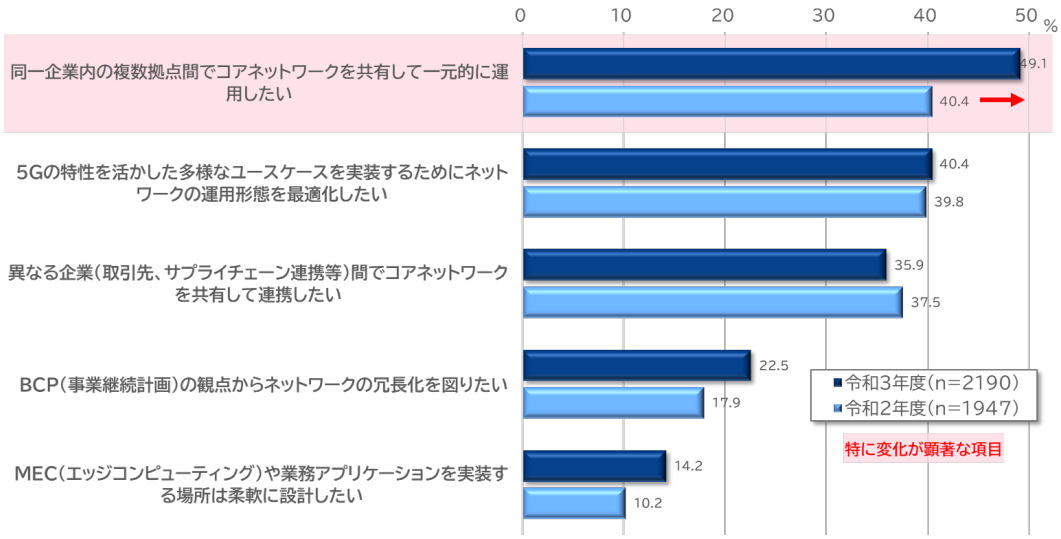


図 7-3-2-2　ローカル５Ｇの整備・運用の意向に関する意向

7.4　実証が必要な検証課題・項目等の整理

(1) 技術・標準化の動向

5G の進展において 2020 年代半ばにおいては、ネットワークにおけるコア機能の仮想化やネットワークのクラウド化、エンドツーエンドでのスライスネットワークの提供の進展が予想されます。こうしたネットワークの迅速かつ柔軟な拡張、リソース（計算処理・データ容量など）の共有、俊敏な最適化等を実現する技術は、5G の超高速・大容量、超低遅延、多数同時接続といった特長の真価を発揮させるものです。

特に、ネットワークのスライシング技術により、多様なアプリケーションのニーズに応じてネットワークの特性を切り出してユーザー向けに提供することが可能になります。例えば、センサーなどの高速通信を要しないものについては、低頻度・低速度の通信サービスを低廉な価格でスライス（提供）することにより、多数同時接続を前提とするサービスの普及が進むと考えられます。5G 時代において飛躍的に増大するコンテンツを処理するためのコンピューティングリソースを活用し、大容量かつ低遅延を実現できます。例えば、映像データ等、広帯域スライスでクラウドへ伝送する、ロボットの制御操作等は低遅延・高信頼のあるネットワークスライスを活用することができます。地域での利活用を想定した場合、地域の作業現場において CAD データを MEC サーバで処理して結果や画像のみ 5G 端末へ伝送する、地域に必要な医療等に係る高精細画像処理やコンテンツを MEC サーバから 5G

端末へ転送する、等、中央のコア網やサーバへ伝送せずに「地産地消型」に効率的な 5G ネットワークの活用の実現が想定されます。

特にコアネットワークや基地局が、ソフトウェアにより制御され、必ずしも特定のハードウェアに限られず様々な組み合わせ（ハードとソフトが m 対 n の関係）で動作するとともに、これらがクラウド上でも実現可能となります。交換設備、伝送路設備、基地局設備などの複数の設備をまたいで、これらの設備の機能がソフトウェアにより一体的に制御（ネットワークスライスが構築）されます。多数のネットワークスライスが併存することになるため、ネットワークオーケストレータ（仮想化管理機能）が、複数のサービス向け、あるいは複数の事業者向けのネットワークスライスを統合管理することができます。

現在、3GPP では第５世代移動通信システム(5G)のサービス要求実現に向けて、新しいコアネットワークの策定検討を行われています。3GPP での標準化は、各国及び各ベンダー間の仕様の指標となっており、3GPP に準拠した製品間での相互接続が今後期待されています。一方でコア・基地局・端末に関して、フィールドの要件やアプリケーションを使用する上での所要性能に応じて、柔軟に組み合わせて設計することが望まれています。

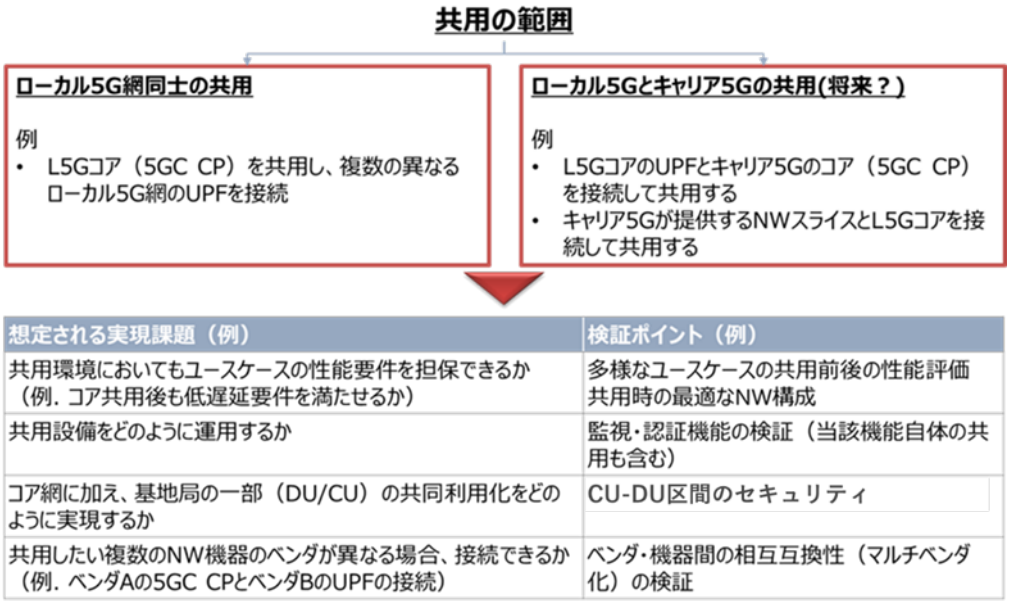
こうした技術的トレンドは、柔軟かつ効率的な運用、またユーザーが早期に 5G を享受するためにも、コア網などネットワークの上位に位置する設備をユーザーや地域間や地域内で共用する形態が派生的に生まれていくことを予期させます。他方で、共用基盤としてのクラウドについては、セキュリティやネットワーク障害・災害時における BCP 等の観点からデメリットも指摘されます。

上記を踏まえ、ローカル５Ｇのネットワーク・システムにおける共用形態を実現するにあたって、技術面・運用面から検証すべき事項について整理します。また、必ずしも専門的知識を有していないユーザーが円滑に導入・利用できる環境や、事業者による多様なサービス提供やビジネスモデルの創出に資する環境構築に向けたルール整備とその方策が必要となります。

(2) 共用形態を実現させるための方策等

コア網の共用形態を実現するための方策の枠組みについて「図 7-4-2-1　共用の範囲及び実現課題・検証ポイントの例」に示します。まず、共用の範囲について定義する必要があります。範囲の定義は、「ローカル５Ｇ網同士の共用」と「ローカル５Ｇとキャリア５Ｇの共用」に大別されます。本テーマが、まずはローカル５Ｇの普及展開における課題解決の方向性に立脚していることから、方策の検討としてはまずは前者を優先して考えるべきです。後者については、制度・技術・運用など多様な面から実現上の課題があることから、将来的な方向性として位置付けるのが適当です。

また、想定される実現課題及び検証ポイントは、上記の共用の範囲ごとに挙げられます。



想定される実現課題（例）	検証ポイント（例）
共用環境においてもユースケースの性能要件を担保できるか（例. コア共用後も低遅延要件を満たせるか）	多様なユースケースの共用前後の性能評価 共用時の最適なNW構成
共用設備をどのように運用するか	監視・認証機能の検証（当該機能自体の共用も含む）
コア網に加え、基地局の一部（DU/CU）の共同利用化をどのように実現するか	CU-DU区間のセキュリティ
共用したい複数のNW機器のベンダが異なる場合、接続できるか（例. ベンダAの5GC CPとベンダBのUPFの接続）	ベンダ・機器間の相互互換性（マルチベンダ化）の検証

図 7-4-2-1　共用の範囲及び実現課題・検証ポイントの例

特にローカル５Ｇ網同士の共用形態を実現する際の具体的に必要とする検証内容は「図 7-4-2-2　主な検証ポイント」のとおりです。ここでは、コア網（C プレーン、U プレーン）、基地局、端末などの各レイヤーで検証のポイントを考えていくことが重要です。

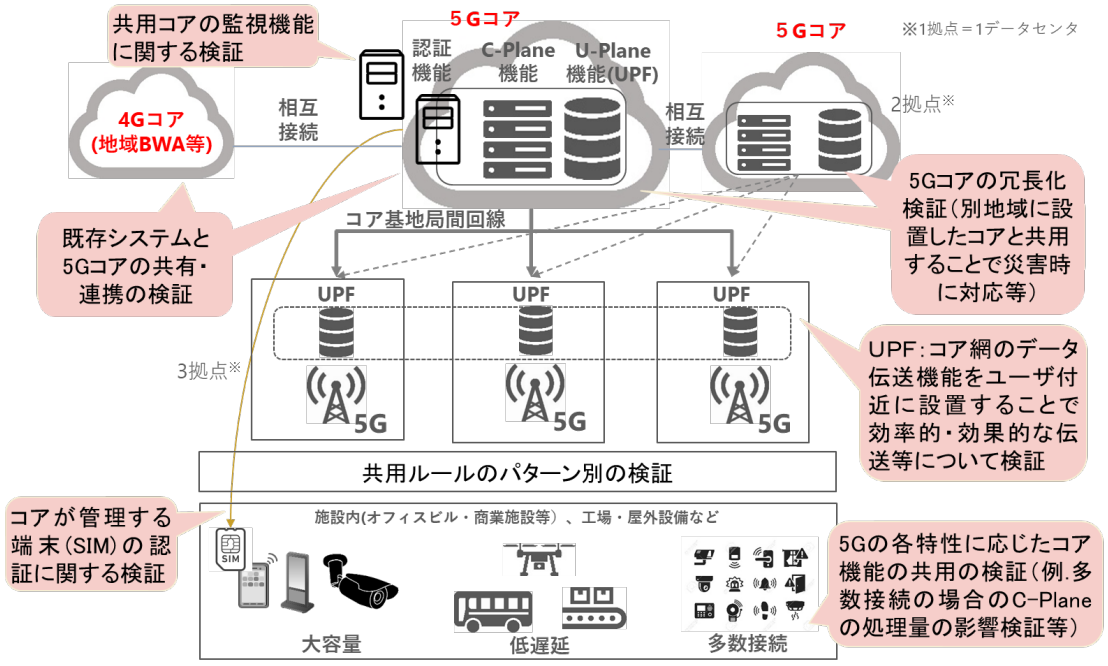


図 7-4-2-2　主な検証ポイント

（3）検証の流れ

共用形態のモデル化と検証の流れは、ユーザー側の利用者目線の要件をモデル化してい

くことが肝要になります。次に、オペレータ側の地域等のインフラ事業者の目線でどのように利用者目線の要件を満たしていくことができるかを検証します。その上で、さらに上流に位置するプラットフォーマや通信事業者による広域での実現モデルを検証します。最後に、自治体系や中小企業など、モデル化並びにコスト低減化を図れるかの検証を行います。

(4) 具体的な検証項目

上記を踏まえ、具体的な検証項目を「表 7-4-4-1　具体的な検証項目（例）」に示します。

表 7-4-4-1　具体的な検証項目（例）

区分	課題	検証項目（案）
技術・機能検証	多用なコア等の共用形態における、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。 ※コア共用形態を前提とした 5G 性能検証	・ コア設備と離れた拠点の基地局について、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の検証 (パターン例) ➢ 帯域型 NW(専用線/VPN 等)、ベストエフォート型 NW(インターネット) ➢ エリア内(例:首都圏内)、エリア間(例:首都圏～東北・北海道エリア) ・ コア設備と離れた拠点の基地局について、通信制御はコア設備が行い、ユーザートラフィ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証 ➢ UPF の設置箇所の違い(コア or ローカル側)による機能比較等の検証 ➢ UPF の共用に関する検証
	ローカル５Ｇ網の信頼性をどのように担保できるか。 ※手段としてのコア共用の活用	・ 異なるコア網間で切り替えられる障害を考慮した最適なアーキテクチャに関する検証 ➢ コア等冗長化に関する検証 ➢ 回線冗長化の検証 ・ 共用するユーザー数やデータ処理量等に合わせたコア設備の機器性能担保に関する検証 ・収容上限(収容設計)の検証
	コアの他要素の機能をどこまで共用可能か。 ※コア共用の定義	・ コア機能の共用範囲に関する検証 ➢ 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） ➢ 加入者契約情報管理（加入者情報 DB 等、加入者とポリシーの紐づけ、課金情報 UDR） ➢ ポリシー管理（PCF） 例：スライス・インスタンス毎に立てる方が良い（共有しない）、企業内の SDN 連携では、SMF と

		UPF は 1 セットにする（スライスの中に構築する必要）など
	コアで異なる品質等の要件を有するサービスをどのように共存させることができるか。 ※先進的なコア活用	・ 通信品質の区分けに関する検証 ➢ NW スライシングの検証
運用・実装検証	異なるベンダー間での接続をどのように担保するか。	・ コア設備と基地局が異なるメーカの場合や、基地局が複数のメーカの場合の相互接続(3GPP 準拠)に関する検証 ・ ユーザー間でのセキュリティ担保、コア設備や基地局への不正アクセス制御等に関する検証 ➢ SIM 認証基盤の検証 ➢ ユーザー間の区分けに関する検証 ➢ 不正操作、不正プログラムの対策 ➢ 情報窃取、情報改ざん、情報破壊の対策
	コア共用型の運用時における公平性や責任分解等をどのように担保するか。	・ 増減設時における影響範囲、ヘビーユーザー対応などのユーザーの公平性担保に関する検証 ・ コアとアクセス網の主体者が違うため、責任分界点の定義、POI の管理（契約・費用）、SLA 定義 ➢ NNI 定義（BBU-RRH、CU-DU-RU の切り方） ➢ UPF（GTP 処理），DN（IP Router）→実装方法に依存する ・ 障害時における、影響範囲、切り分け方法、責任分界、費用負担等が複雑化を想定した整理
	どのようなサービスデリバリ体制を想定するか。	・ システム監視、セキュリティ監視の在り方に関する検証 ・ SIM カードの発行、回収、廃棄等の運用 ➢ SIM のアクティベーション（←コア共用として必須の機能） ➢ eSIM の運用 ➢ SIM カードの持ち込みもしくは提供（サービス提供の考え方に依存） ・ サービス利用者への接続性・セキュリティ提供モデル（ポリシー展開） ➢ サービス利用者同士の接続性（ローカル５Ｇ間の接続など）

特に上記の検証にあたっては、以下の論点が検証において重要になります。

論点例１：監視運用や管理の在り方

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ります。

論点例２：セキュリティの在り方

5G の新たなネットワークインフラは、SDN、NFV、クラウド・ネイティブなアーキテクチャを前提に設計されています。ネットワークの機能は、中央集約型ネットワークから切り離され、ローカル・地域・中央などのそれぞれのデータセンターに分散配置されます。クラウドベースの 5G ネットワークでは、多くのネットワーク機能がパブリック及びプライベートクラウド上で実装されます。

また、5G のネットワークは、既存のネットワーク（3G・4G 等）、インターネット、自動車、医療、工場、IoT デバイスなどの垂直産業向けネットワークなど、複雑な異種ネットワークで構成されます。そのため、様々なセキュリティレベルや要件、セキュリティ技術が混在することから、共用形態を運用する上では、強靭性を失うセキュリティ上の潜在リスクが存在します。

(5) 相互接続等環境整備に向けた課題

コア共用形態の実現に向けた環境整備とは、すなわちレイヤー間、コア間の相互接続の実現が重要となります。具体的には、レイヤー間のインターフェースに着目することで、それぞれ必要な検証や運用ルールを定めていくことになります。早期の環境整備の点からは、特に標準化・共通化、あるいは検証をフォーカスする必要がある領域に着目し、関係するプレイヤーを巻き込み、業界統一標準の策定や、認証等のエンフォースメントを伴う形での運用が望ましいと考えます。特に、後者の場合は、担い手の選定が重要となります。なるべく多くのユーザー企業（需要側）やインフラ・サービス事業者（供給側）へ裨益するように、利害関係者を囲い込める座組や関係団体が担うことが望ましいと考えられます。既にエンフォースメントが構築されている体制などを拡張するなどのアプローチも考えられます。

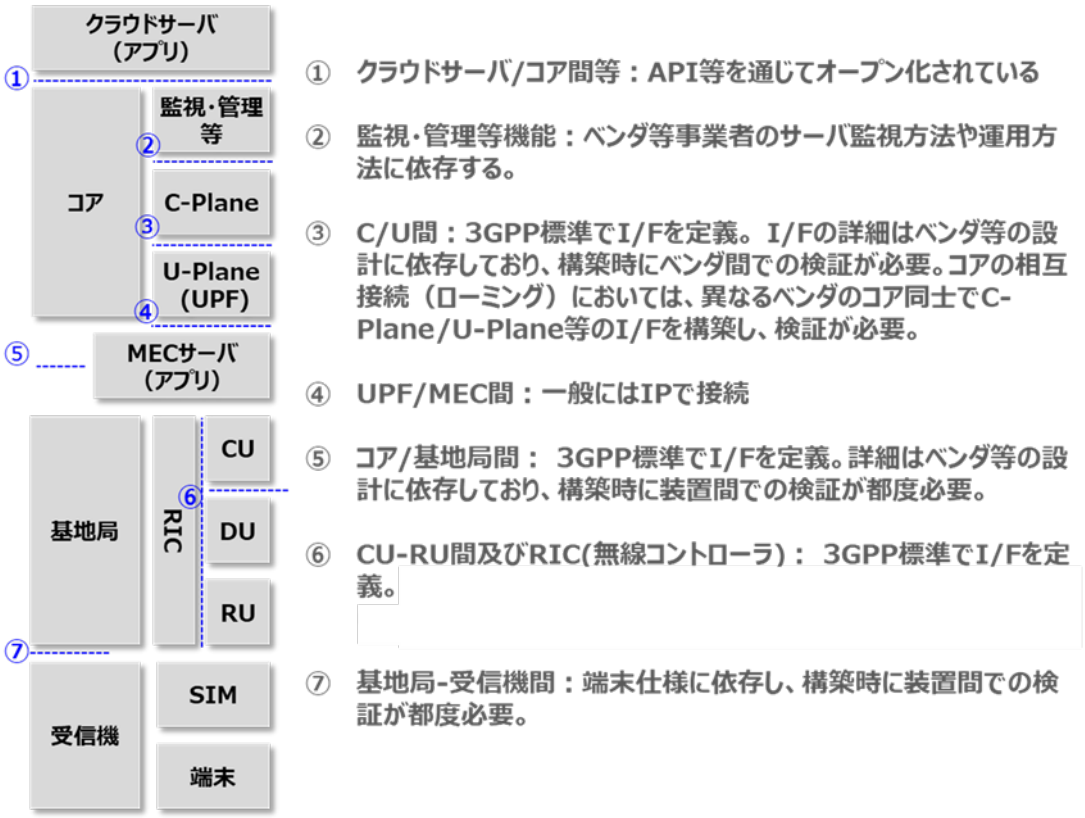


図 7-4-5-1　インターフェースの必要な検証や運用ルール

(6) 令和 4 年度実証項目

本検証において、令和 3 年度は、ローカル５Ｇとコアの構築が主となるため、検証については令和 4 年度も継続的に進めることが望ましいと考えます。弊社が考えるコア共用実現に向けたロードマップは「図 7-4-6-1 相互接続・コア共用ロードマップ」のとおりです。

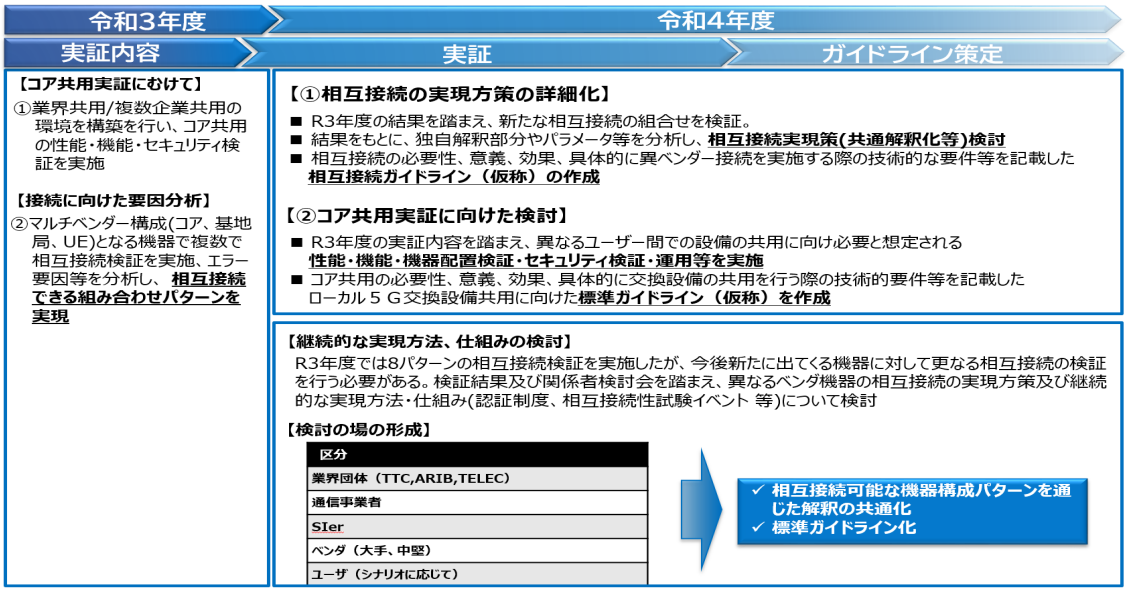


図 7-4-6-1 相互接続・コア共用ロードマップ

また、令和 4 年度においては以下の令和 3 年度の実証を踏まえ以下の検証が望ましいと考えます。

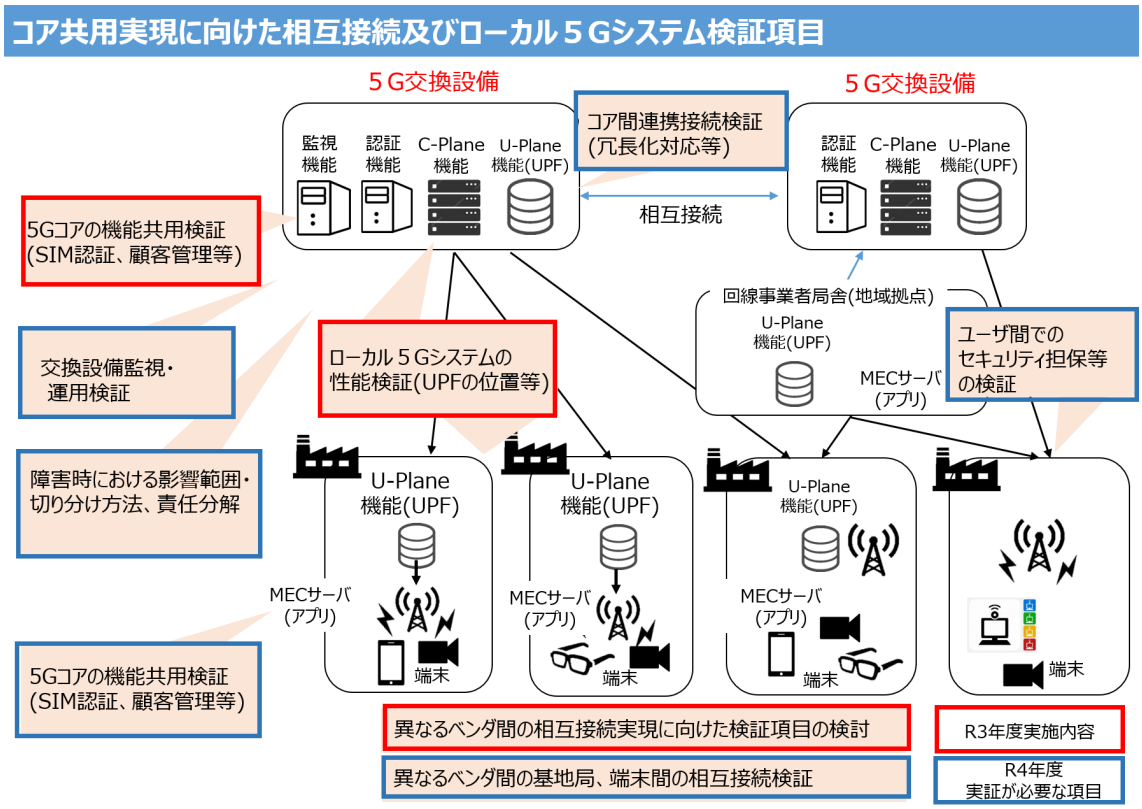


図 7-4-6-2　コア共用実現に向けた相互接続及びローカル５Ｇシステム検証項目

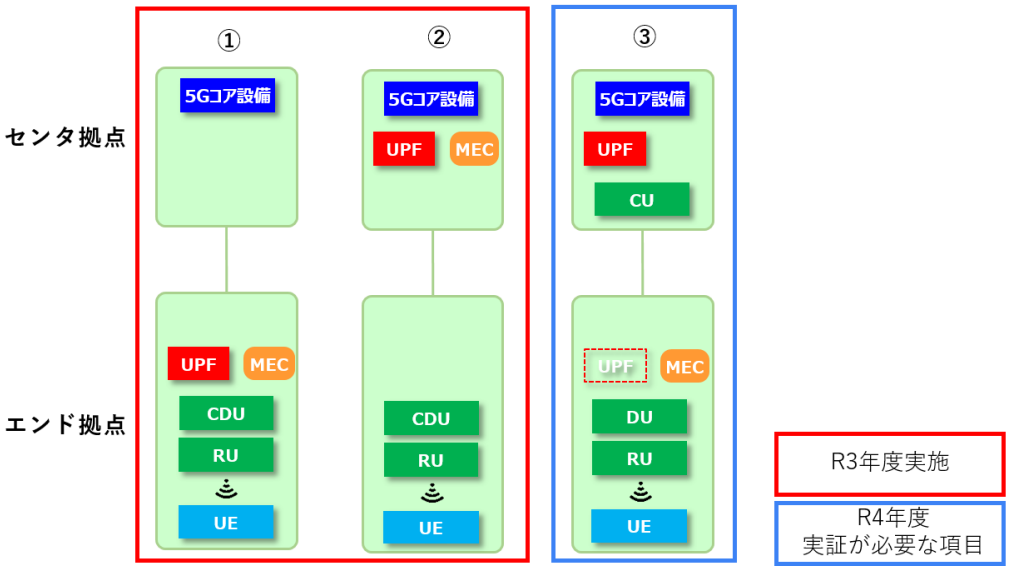


図 7-4-6-3　ローカル５Ｇ機器配置パターン

3GPP の定める標準化仕様等によりローカル５Ｇに具備される機能も変化していくため、検証に活用するユースケースについてもローカル５Ｇの機能を有効に活用できるアプリケーションを選定していくことが望ましいと考えます。

①ローカル５Ｇ交換設備等相互接続検証
・ローカル５Ｇ交換設備、基地局、端末をマルチベンダー構成にて相互接続試験
・異なるベンダー機器等による相互接続の実現に向けた要因分析・実現方策の検討
・ガイドラインの作成

②ローカル５Ｇ交換設備共用パターンの検討・構築
・交換設備と接続拠点の距離、使用する回線の種類等に応じて、それぞれのパターンに最適な接続構成の検討
・各実証パターンの設備面・技術面・運用面の課題及び課題解決策の検討
・ガイドラインの作成

③ローカル５Ｇシステムの検証
・ローカル５Ｇ交換設備の共用における性能検証
・ローカル５Ｇ交換設備の共用における機能検証
・ローカル５Ｇ交換設備の共用における拡張性検証
・ローカル５Ｇ交換設備の共用におけるセキュリティ検証
・ローカル５Ｇ交換設備の共用における監視等及び運用検証

7.5 相互接続・コア共用実装に向けた合意形成の推進

(1) 利害関係者の認識・意向

相互接続・コア共用実装には各関係者の合意形成の推進が求められます。ユーザー、ベンダー、通信事業者の 3 つの区分に分け相互接続・コア共用に係る認識・意向を確認しました。また、ベンダーや業界団体、SIer 等の関係者へ相互接続・コア共用について意向や課題等のヒアリングを実施しました。今後、コア共用の推進に向けては下記内容を踏まえた普及シナリオの検討が必要になると考えています。

表 7-5-1-1　コア共用に係る認識・意向

区分	コア共用に係る認識・意向
ユーザー	・ インフラ運用の合理化や ROI 向上の観点から、企業内複数拠点間でのコア設備等の共用化に対するニーズはある。今後、企業 NW・IT システムへの組み込みなど、5G の実装に向けては顕在化する蓋然性が高い。
ベンダー	・ SI からサービス提供ビジネスへの足掛かりとしてコア共用を捉えている。
通信事業者	・ 効率的なインフラ投資・既存資産活用（局舎等）の観点から、5G 規格の特性を活かしながら、コア共用化と共通サービス開発展開という従前のインフラビジネスの観点で捉えている。

(2) 各社ヒアリング結果

ユーザー側のニーズの顕在化はローカル５Ｇの普及に必要な課題だと考えています。それを念頭に置き、ユーザーを含む各ステークホルダの真のニーズや課題を踏まえながら、今後コア共用のニーズが顕在化していくシナリオを検討することが重要となります。

そのため、ユーザー・サプライヤ（ベンダー・SIer 等）・業界団体等へのヒアリング等の調査を通じて、相互接続・コア共用に資するニーズ、共用形態の在り方やその実現に向けた課題・対応策を整理する必要があります。以下のとおり、対象者へヒアリングを実施しました。

表 7-5-2-1　ヒアリング対象候補及びヒアリング項目

ヒアリング対象候補	主なヒアリング項目
ケーブルテレビ事業者	● ローカル５Ｇビジネスの方向性 ● ローカル５Ｇに係るニーズ・課題 ● コア共用に係るニーズ・課題 ● 検証項目に対する意見 ● 相互接続・標準化ニーズ・標準化すべき領域 ● 標準化・認証等スキームに対する考え方（各種試験、仕様作成～業務、実施主体等） ● その他出口論に関する意見
ベンダ	
SIer	
業界団体	

① ベンダ

・ コア共用は、オンプレミスと違い、ユーザ側で用意するものが少なくなることから、ユーザ側でサービス導入の素早い判断が可能、スモールスタートが可能である。さらに、運用を提供側にアウトソースすることが可能なためローカル 5G 導入の障壁は下がると想定される。懸念点としては、クラウド回線が必要なこと。例えば、山の中の土木現場はクラウド回線がないので、一部オンプレのコアを希望される顧客もいる。

・ 想定するコア共用は、顧客管理・SIM 管理を裏で行い、IaaS/PaaS 上のコアのレイヤから、完全に個者ごとに論理分離し、加入者情報(HSS)も含めて分離する必要がある。ただし、企業によってはセキュリティポリシーによってクラウドコアがそぐわない場合もあり得る。

② SIer

・ ・大規模企業へのローカル５Ｇの展開にあたってはターゲット分野を定め、ターゲット価格を想定。但し、ローカル５Ｇの裾野拡大に当たっては、コアを含む共用モデルも検討する。

③ CATV

・ ローカル５Ｇの普及展開に向けては、コア共用ネットワークが必要であるが、共用によるメリットを最大化するにはネットワークのマルチベンダ環境を実現することが望ましい。

④ 業界団体

・ マルチベンダーベースで安定してつながるために、相互接続のための規格化や相互接続試験が重要であると考えている。
・ 例えば、認証の仕組みでは、一般的に規格適合性試験と相互接続性試験の 2 種類の実機試験が必要である。但し、仕様作成から、業務フローの整理、試験機関としての認定要件の整理等の作業が発生するため、ニーズを精査した上で実施すべきである。

・　ローカル５Ｇを活用したソリューションにおいて、接続がうまくいかない原因が、基地局、コア、ゲートウェイなど色々な切り分け方があるが、何らかの公式な場でヒアリングをし、問題点を明確化した上で担当を分けて検討していく形式が望ましい。相互の組み合わせにより事象が変わってくる。今後、コア共用の検討においては、共用した際の責任分界点、運用面について議論していくことが重要と考えられる。

(3) 考察

上記のヒアリング結果より、相互接続・コア共用モデルについては大手ベンダーをはじめSIer やCATV、業界団体ともに各社ごとに懸念点はあるものの肯定的であるあることが分かりました。また、各社ともに相互接続の重要性を認識しており、特定のベンダーに依存した性能上の課題も生じているため、改めてマルチベンダー環境を構築する必要性が分かりました。

工場での運用など、複雑かつ高い要件が求められる 5G のユースケースにおいては、ネットワーク構成のみならず、コアネットワークの個々の機能群において、より詳細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、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形態の実装を目指す必要があります。上記の導入・運用に向けては、コアネットワークを含むインフラ・サービスを提供する事業者（キャリア、ベンダー、クラウド事業者等）は、実績やノウハウを蓄積しながら、最適なインフラ構築やエリア展開を今後進めること必要があります。

ユーザー・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され、中堅・中小企業など、大企業以外のローカル５Ｇ導入意向ユーザーにおける導入ハードルが低減化していくと考えます。また、普及を加速化させるためには、5G アプリケーションの要件に応じた性能評価・検証を含む共有知化を進める必要があります。共用形態が浸透するにつれ、同一ユーザー企業内の他、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します。コア共用の実現にむけては相互接続に向けた標準化のルール制定、コア共用における運用要件整理、ガイドラインの作成等の課題が残っているため、令和 4 年度以降はこれらの課題を踏まえ関係者間での合意形成が必要になります。

8. まとめ

相互接続及びコア設備の共用については、利用者側（企業・団体側）及び提供側（ベンダ・業界団体・SIer 等）共にニーズを有していることが各社ヒアリング結果より判明しました。ローカル５Ｇの普及促進に向け利用者側は、ユースケースや予算に合わせ、必要なスペックの機器を選択可能な状態にし、かつ様々な「コア設備の共用を含むシステム形態」や「サービス提供形態」から選択可能な状態になることが望ましいと考えます。

上記を踏まえ、コア共用形態の実現に向けた相互接続の検証、コア共用形態における各ユースケースで推奨される構成や回線種別等についての検証、コア設備の共用を進めるにあたり必要な機能である性能面、機能面、セキュリティ面について検証しました。

（１）相互接続

最適なローカル５Ｇ機器を選定していくためには、コア設備及び RAN 機器等を異なるメーカから選定していくことが必要であり、ローカル５Ｇシステム形態の選択肢の一つとなるコア共用形態が実現していくために相互接続が重要となります。

相互接続については、異メーカの組合せによるローカル５Ｇシステムの相互接続環境において、相互接続に必要な要件を検証しました。今回の調査研究を通して、3GPP で自由設計となっているパラメータ等の差異が相互接続可否に影響し、改善措置が必要となることが判明しました。接続不可の組合せについては今後も継続して要因分析と改善方策を検討する必要があり、下記「図 8-1　相互接続検証」の通り、今後より多くの相互接続組合せについて検証することで更なる知見を集約し、ガイドラインとして標準的な相互接続要件をまとめることが重要と考えられます。

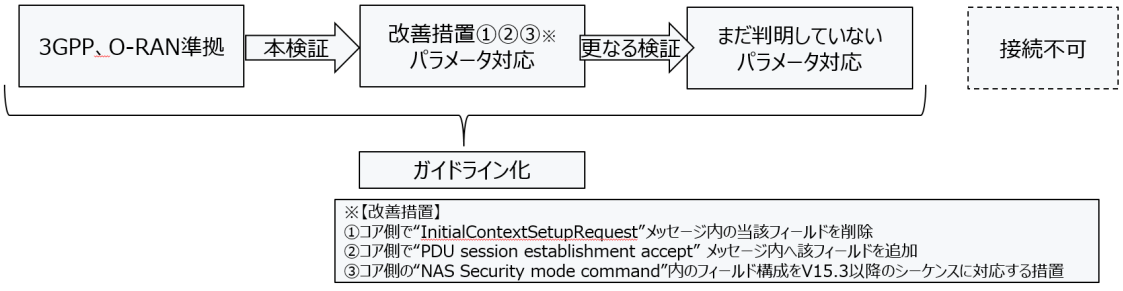


図 8-1　相互接続検証

（２）コア共用における共用形態（ユースケース検証含む）

コア設備共用を進めるには、利用者側が、ユースケースに応じて様々なシステム形態から選択可能な状態にする必要があります。

本調査研究では AI 顔認証や遠隔支援をコア共用下におけるユースケースとしそれぞれで推奨される構成や回線種別等について検証しました。

コア設備共用下では、センタ拠点・エンド拠点の物理的距離が離れるため、特に低遅延用途でのユースケースにおいて対応が求められる場合があるものの、UPF 配置や回線種別を工夫することで一定の対応が可能であることが分かりました。また、「図 8-2 コア共用における共用形態」の通り①オンプレ、②コア設備+UPF 共用、③コア設備のみ共用について推奨されるモデルについて検討しました。

今後の普及促進に向けては、利用者側の多様なニーズを想定し、センタ拠点・エンド拠

点の機器配置が異なるパターンについて更なる検証を実施する必要があります。

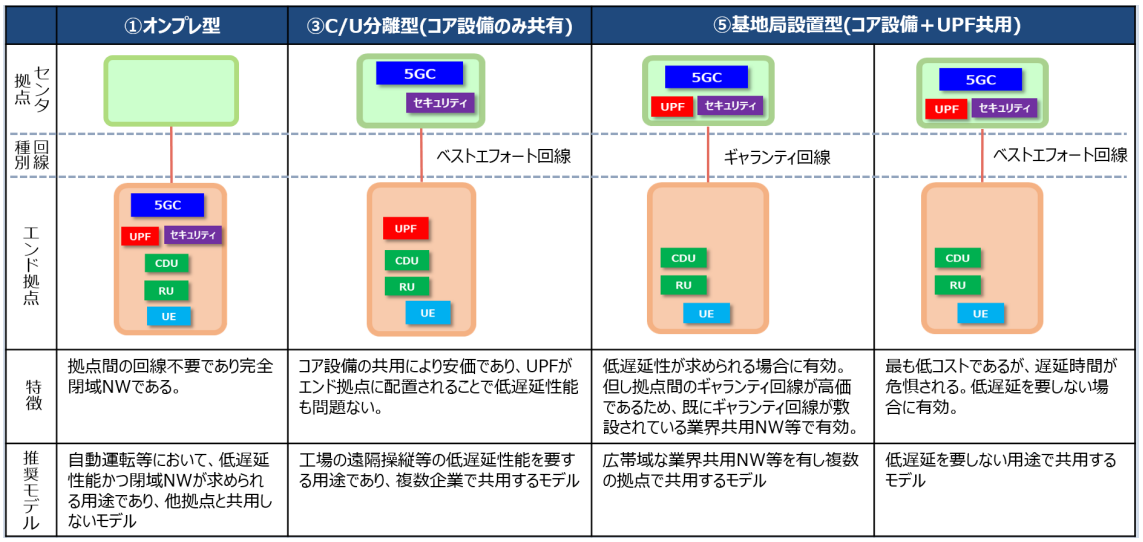


図 8-2 ローカル５Ｇにおける共用形態

（３）コアの共用におけるローカル５Ｇシステム検証

コア設備の共用を進めるためには、共用するにあたり必要な機能を抽出し、その機能がオンプレミスと同様に動作することが必要になります。

本調査研究では、性能面、機能面、セキュリティ面から検証しコアを共用することは技術的に実現可能であることが分かりました。

① 性能面

コア設備を共用する環境下において、端末数やデータ通信量等の変化に伴い有限なリソースである CPU やメモリの所要量を検証しました。また、伝送スループットや伝送遅延時間の性能について、UPF の設置位置や地上回線網の回線種別による差分を比較しました。必要なリソースであるメモリ消費量を明らかにし、UE 台数に応じて設計することでコア共用を実現可能であることを確認しました。コアの共用環境では、拠点間の回線における遅延時間の劣化が懸念されるため、低遅延が求められるユースケースでは性能を考慮した回線種別の選定や UPF の機器配置が必要になります。

② 機能面

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。そのため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、それらの実用性について確認し、統合運営及び拠点毎の管理を実現できることが分かりました。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、より自由度の高い利用方法を実現するには、UE ごとに異なる UPF を選択できる必要があります。本検証

を通して、コア共用下においてもその機能が利用可能であることを確認しました。様々なユースケースの混在が想定されるコア共用下において、アプリケーションの所要性能に応じてUEごとに適切なUPFを選択できる本機能の実装が望ましいと考えられます。

③ セキュリティ面

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あります。コアと基地局が別拠点に分かれることによって想定される攻撃に対し、効果的なセキュリティ対策を検証しました。検証の結果、複数ユーザで共用可能な仮想アプライアンス製品や IPsec 機能を有するセキュリティ機器を活用することで、コア共用下においてもコストを抑えながらセキュリティ対策が可能と考えられます。

上記の結果より、今年度の調査研究においてローカル５Ｇにおける相互接続は、その実現の可能性が高まったが、今回接続不可パターンの措置解明や相互接続要件となるパラメータ等の検証の必要性も判明しました。また、コア共用は、技術的に実現可能であることは確認できましたが、ユースケースや運用面等を踏まえた更なる検討の必要性も明らかになりました。

今後、多様な相互接続の実現、ユースケースに合わせたコア共用モデルの確立、コア共用の運用要件等の明確化の観点から検証を進めることが必要になります。また、コア設備共用の技術的実現性の担保のため、以下の要件等に関する検証が必要と考えられます。

・コア設備の冗長性要件
　コア設備の障害等におけるシステム維持・運営等の冗長構成に関する要件

・今回未検証である新たなセキュリティ要件
　CU-DUを分離する構成における同区間のセキュリティ及び無線区間のセキュリティにおける要件

・コア共用下での運用要件
　複数拠点で共用利用の環境における統合運用方法、監視体制及び障害時の措置方策等の要件

上記検証結果を取りまとめることで相互接続・コア共用モデルに関する「ガイドライン」を作成し、ローカル５Ｇの普及促進を目指されることに期待します。