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

成果報告書

令和５年３月

東日本電信電話株式会社

目次

1. 実証概要 1

1.1 背景・目的 1

1.2 実施事項および検証目標 2

(1) 検証実施の概要 2

(2) 共用パターン 4

(3) 相互接続検証 4

(4) コアの共用におけるローカル５Ｇシステム検証 6

1.3 実施体制 6

1.4 構築・検証のスケジュール 12

1.5 免許申請の概要 14

(1) 申請者、申請先、申請概要 14

(2) 申請者を免許人とした理由 28

2. 実証環境 29

2.1 複数企業共用パターン 29

2.2 業界共用パターン 31

2.3 相互接続検証 35

3. 検証環境の構築 39

3.1 ネットワーク構成 39

(1) ネットワーク・システム構成図（全体像） 39

(2) センタ拠点・エンド拠点間ネットワーク 42

3.2 ネットワーク・システム構成機器 43

3.3 ネットワーク・システム構成機器仕様 52

3.4 システム機能・性能・要件 72

3.5 免許および各種許認可 74

4. 相互接続検証 75

4.1 検証概要 75

4.2 検証環境 76

4.3 検証内容・結果 78

(1) R4 年度の異ベンダー組み合わせパターン検証 78

(2) R3 年度に相互接続が実現しなかったパターンの検証 86

(3) R3 年度に相互接続が実現したパターンの検証 90

(4) 東京大学開発基地局を用いたパターン 92

4.4 相互接続の検証結果のまとめ 95

(1) 相互接続に関連する項目、パラメータ 95

(2) 相互接続の結果に関する考察 100

(3) 相互接続組合せごとのまとめ.....109
(4) 相互接続の検証結果を踏まえたコアの共用における考察.....119

5. ローカル５Ｇシステムの検証.....120

5.1 検証概要.....120
5.2 検証環境.....120
5.3 ローカル５Ｇ交換設備の共用における性能検証.....122
(1) 検証目標.....122
(2) 評価・検証項目.....123
(3) 評価・検証方法.....124
(4) 測定結果.....128
(5) 考察.....145
5.4 ローカル５Ｇ交換設備の共用における機能検証.....148
(1) 検証目的.....148
(2) 評価・検証項目.....148
(3) 評価・検証方法.....149
(4) 検証結果.....154
(5) まとめ.....188
5.5 ローカル５Ｇ交換設備の共用におけるセキュリティ検証.....191
(1) 検証目標.....191
(2) 評価・検証項目.....195
(3) 評価・検証方法.....197
(4) 測定結果.....200
(5) 結果考察.....256
5.6 ローカル５Ｇ交換設備の共用における監視等および運用検証.....260
(1) 検証目標.....260
(2) 評価・検証項目.....260
(3) 評価・検証手法.....262
(4) 検証結果.....264

6. ユースケース検証.....283

6.1 検証概要.....283
(1) 複数企業共用パターン 4K AI カメラソリューション.....284
(2) 業界共用パターン 大学間リアルタイム 8K 映像伝送.....286
6.2 検証環境.....287
(1) 複数企業共用パターン 4K AI カメラソリューション.....287
(2) 業界共用パターン.....288
6.3 検証内容・評価方法.....289
(1) 複数企業共用パターン.....289
(2) 業界共用パターン.....290
6.4 検証結果.....291
(1) 複数企業共用パターン.....291

(2) 業界共用パターン 292
6.5 考察 295
(1) 複数企業共用パターン 295
(2) 業界共用パターン 295
7. 関係者ヒアリング 297
7.1 ヒアリング概要 297
(1) ヒアリング方法 297
(2) ヒアリング対象およびヒアリング内容 297
7.2 ヒアリング結果 298
(1) ローカル５Ｇ全般 298
(2) 相互接続におけるニーズおよび課題 299
(3) コア共用におけるニーズおよび課題 302
(4) 考察 303
8. まとめ 305

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。５Ｇの中でも、令和元年 12 月 24 日に制度化されたローカル５Ｇは、企業や自治体等の様々な主体が自らの建物や敷地内で柔軟にネットワーク（NW）を構築できることから、様々な分野における課題の解決や新たな価値の創造への活用デジタルトランスフォーメーションの推進等にも寄与することが期待されています。ローカル５Ｇは、28GHz 帯（ミリ波）に加えて 4.6GHz-4.9GHz 帯（Sub6）においても利用が可能となる等、ローカル５Ｇの導入・利活用が更に活発化していくことが見込まれています。

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

異ベンダー組合せに関しては、O-RAN を始めとして標準化団体において規格化が進められておりますが、細部の要件等における解釈の違い等によって相互接続が実現できないことを R3 年度の実証で確認されております。本実証では、多くの組合せでの試験を行い、原因究明、相互接続を実現する方策や条件等を明らかしました。また、相互接続組合せにおける伝送性能等を検証し、今後ローカル５Ｇシステムの導入を検討する企業やベンダーが設計上で参考にできる情報等を整理し、技術的手引（仮称）を作成しました。技術的手引（仮称）をもとに導入の促進に繋げることが望まれます。

コアを共用する仕組みに関しては、ローカル５Ｇの無線設備を運用する上での諸課題やそのノウハウを導入検討事業主体に周知し、システム構築をしやすい環境を早急に整備する必要があります。

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

また、ユーザは、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、アプリケーション毎に柔軟な NW 構成を実現するためのポリシー制御など、より高度なコア共用形態の実装を目指す必要があります。

さらに、コア共用形態が浸透するにつれて、同一ユーザ内の他、産業集積エリアなど、複

数の異なるユーザ間や、特定の業種におけるサプライチェーンを構成する企業グループ間で、共用形態を運用するニーズが顕在化します。この場合、異なるユーザ間でローカル５Ｇ交換設備を共用することで生じる相互接続性の検証を行うとともに、技術面・運用面等からローカル５Ｇ交換設備共用の実現性を検証し、今後ローカル５Ｇシステムの導入を検討する企業やそれを支援する SIer 向けに技術的手引（仮称）を作成することが重要です。

今年度の本実証事業においては、

① ローカル５Ｇシステムの相互接続性の検討（コア等相互接続検証）を実施するため、ローカル５Ｇの交換設備・基地局・端末の相互接続を実現するための仕組みの整理

② コアの共用の実現（コア共用技術実証）に向けた、異なるユーザ間において設備を共用していく上での、設備面・技術面・運用面等の課題の整理

上記の整理を行い、地域や中小企業等の各産業分野の振興に資する効果的な主に「ローカル５Ｇのハード面の整備等の普及展開方策」を調査しました。

なお、令和３年度「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」（以下「令和３年度交換設備の接続等検証」という。）において、①コア等相互接続検証については、異なるベンダーの機器による相互接続試験を実施し、相互接続できるパターンの取りまとめ等を行い、②コア共用技術実証については、現実の利活用場面を想定した共用パターン（実証フィールド）を検討・構築し、共用するに当たって想定される詳細の機器配置検証、セキュリティ検証等を行いました。

今年度の本実証においては、R3 年度の成果を踏まえた上で、①について、さらに異なるベンダーの機器による相互接続検証を実施することで相互接続の実現性をより高め、②については、共用に当たり検証すべき異なる機器配置、システム全体のセキュリティ検証等を実施することで交換設備共用に向けた最適な設備構成等を整理するとともに、ローカル５Ｇの普及に向けて相互接続試験方法も含めた相互接続のための技術的手引および交換設備等共用のための技術的手引を作成しました。

1.2 実施事項および検証目標

(1) 検証実施の概要

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

他方、コアの共用は、現時点でユーザ側に顕在化しているニーズではないため、以下の３つの視点に基づくローカル５Ｇの展開シナリオに基づき、ニーズが顕在化していくことを想定することが重要になります。

表 1-2-1　今後のローカル５Ｇ展開シナリオと共用ニーズ

視点	現状のL5G構築	今後のL5G展開シナリオ ⇒ コア共用ニーズ	共用化のメリット
エリア	特定のエリアや拠点で構築 例：〇〇地区に基地局を設置	地域内(県域等)で様々なユーザが構築を進める。 ⇒ 各ユーザのコストを抑えるため地域内でコアを共用したい。トラヒ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)によるトラヒックコストの低減 ● 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	特定の単一拠点で構築 (例：〇〇自動車の〇〇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)をユーザ設備内にオンプレで構築)	ユーザ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

本検証ではローカル５Ｇの導入において、中小企業はコスト面で障壁がある一方、工場をはじめとする製造業では、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、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「複数企業共用パターン」とし、また、業界共用高速バックボーン NW（団体が業界共用 NW に接続するための接続点（POI）間を繋ぐ 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、同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「業界共用パターン」としローカル５Ｇの展開シナリオに基づき、本検証では「図 1-2-1 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コア共用検証を行いました。

交換設備と接続拠点（ローカル５Ｇ交換設備と通信する基地局を設置する拠点）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おいてどのような設備構成がふさわしいか等を整理しました。各実証パターンは、交換設備の共用が実現することでローカル５Ｇの普及が見込まれるターゲットとなり得ます。そのため早期の普及展開を目指し、各実証パターンの検証を実施しました。

モデル	考え方	ローカル５G設備の在り方	アプリケーション
複数企業共用パターン (パターンA)	• 異なる企業間でコア設備を共用	・共用パターンについて、双方のモデルで最適な構成を検証	• 製造現場の遠隔監視（4Kカメラ）とAIソリューションを活用した侵入検知や混雑度検知に関する実証
業界共用パターン (パターンB)	• 同一業界の異なる団体でコア設備を共用		• 大学間での８K高精細映像を用いた遠隔講義等、同一業界内での映像伝送実証

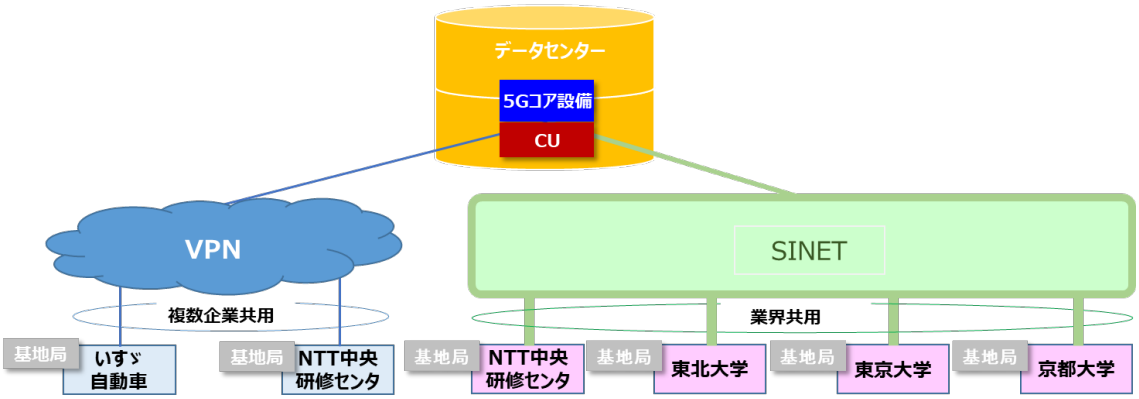


図 1-2-1 本検証イメージ

(2) 共用パターン

① 複数企業共用パターン（異ユーザ間の共用）の想定される特徴

- 複数のユーザ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。
- アプリケーションは拠点内閉域網とする。ただし一部外部インターネット等のプラットフォームを利用する場合は MEC で外部環境と接続するが、コア共用拠点間でのアプリケーションやデータ等の共用は行わない。

② 業界共用パターン（同一業界内の共用）の想定される特徴

- 同一業界（産業界や官公庁等）内の全国複数拠点でコア共用形態を実装する。
- 同一業界内では、NW 構成や利活用アプリケーションは類似しているケースが多い。
- 設備・機能をユーザ施設内または事業者施設に具備する。

(3) 相互接続検証

ローカル５Ｇシステムを導入する際、ユーザ個別の所要性能や予算に応じたローカル５Ｇ機器の導入ニーズが生じることが想定されます。今後ローカル５Ｇのさらなる普及を見

据えると、異ベンダーでの構成でシステムを正常に稼働させることが求められます。R3 年度は、コア 1 台、基地局 2 台、端末 4 台の計 8 つの組み合わせで相互接続検証を実施し、7 つの組合せで問題ないことが確認できました。また、3GPP に準拠した製品同士において、異ベンダー間の相互接続を実現しました。しかし、一部の相互接続組み合わせでは、3GPP 規格に準じていても接続不可となるケースが確認されました。そのため、本調査研究では、R3 年度の相互接続機器へコア 1 台、基地局 1 台、端末 2 台を加えることで、新たに 27 パターンの相互接続組み合わせを検証しました。これにより、相互接続が不可となるパターンを確認し改善方法を示すことでより多くの異ベンダー間での相互接続について検証しました。図 1-2-2 に R3 年度・R4 年度の相互接続検証で用いたすべての機器を示します。

異ベンダー機器間接続によるシステム構成が将来的に普及していくためには、相互接続が実現されたパターン数を増やしていくと共に、パターン毎の伝送性能を整理することが必要です。よって、R3 年度に相互接続が実現しなかった機器を含め、相互接続が不可となるパターンについて要因を究明し、相互接続の実現に向けた方策を実施しました。また、相互接続が実現したパターンについて、それぞれの通信の性能、品質を評価することで、相互接続の組み合わせパターン毎の伝送性能の特性を考察しました。

コア装置については A 社、B 社の製品を用い、基地局に関しては以下の O-RAN（Open-RAN Alliance）に準拠した製品と未準拠の製品それぞれを用意し、相互接続実現に対しての O-RAN 関連性についての検証を実施しました。

・O-RAN Split Option7.2 準拠：2 機種（B 社、C 社）
・O-RAN 未準拠：2 機種（D 社、東京大学開発基地局）

端末には A 社、B 社、E 社、F 社、G 社、H 社の 6 機種を使用しました。

また、企業の実情等に応じた柔軟なシステム構成を実現することでローカル 5 G導入を検討する企業等の導入障壁を軽減することおよび導入する企業等を支援する SIer 等の技術面での負担を軽減することを目的として、ローカル 5 G を今後導入する企業等向けに相互接続の必要性、意義、効果、留意事項等を、また、導入企業等を支援する SIer 等向けには具体的に異ベンダー接続を実施する際の技術的な要件等を記載した相互接続のための技術的手引を作成しました。

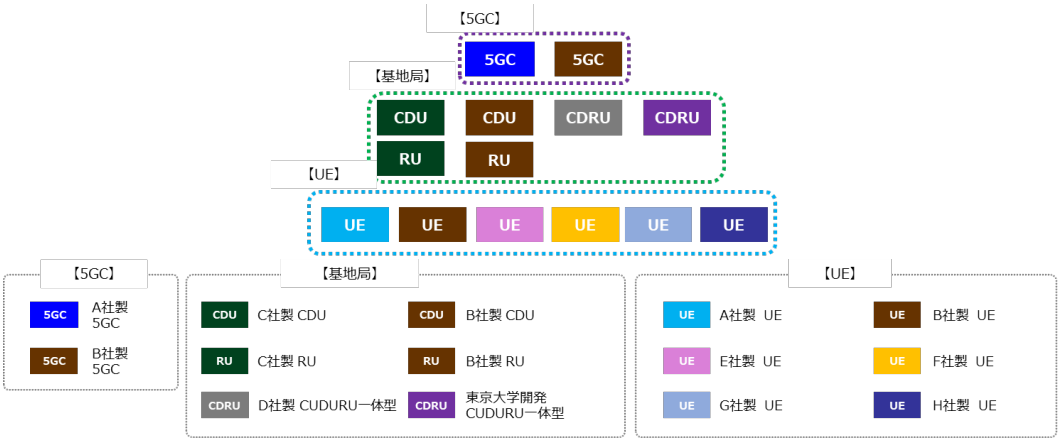


図 1-2-2 相互接続に用いた機器一覧

(4) コアの共用におけるローカル５Ｇシステム検証

R3 年度の実証では、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。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。

R4 年度では、R3 年度の調査研究結果を踏まえ、新たに CU を共用するシステム構成（図 1-2-3）を用意し、設置場所による機能比較の検証、複数企業共用パターンおよび業界共用パターンにおける有効性や課題を検証しました。具体的には、伝送性能（伝送スループット、遅延時間等）の関係性や、システム機能の有効性、セキュリティ対策、システム運用モデルや監視および障害時対応の体系について考察し、推奨する構成や設定、導入すべき機能等を提言します。

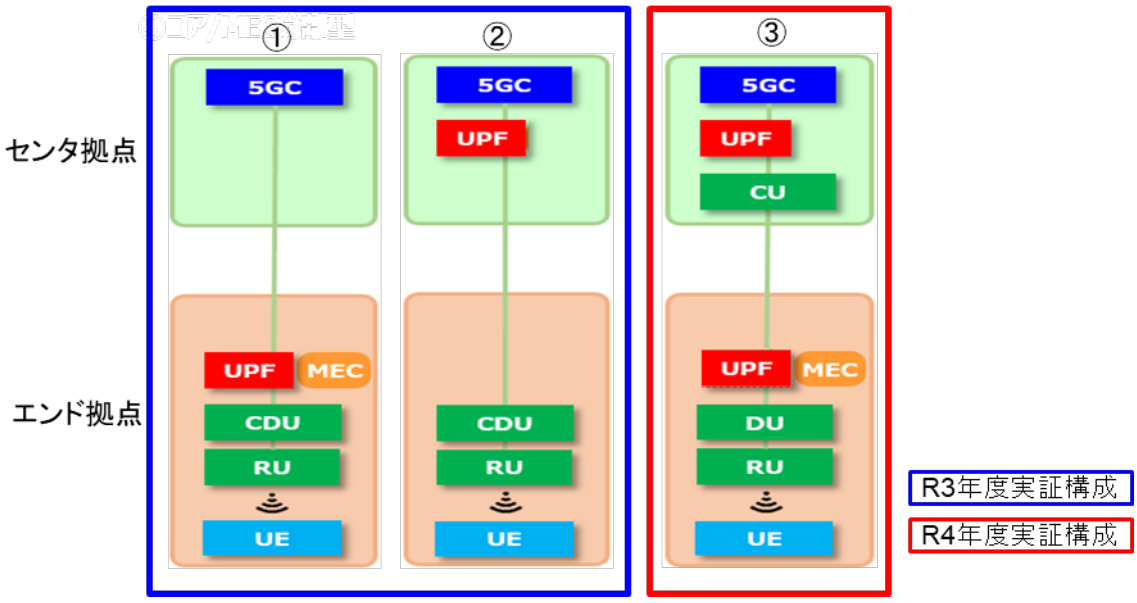


図 1-2-3　ローカル５Ｇ機器配置パターン

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

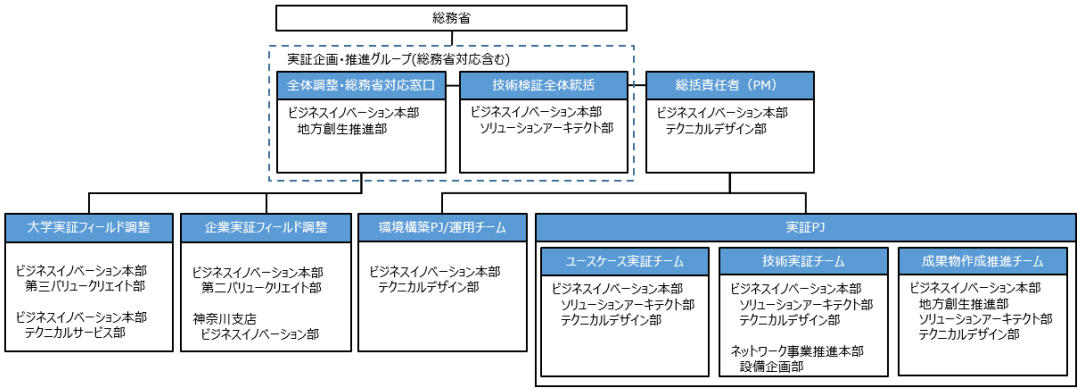
	機関名	役割

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および助言を担当。 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および助言を担当。 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および助言を担当。 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および助言を担当。 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および助言を担当。
	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。
	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。
	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

主管課および関係課並びに検証全体調整事業者および分野別検証調整、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を配置しました。

(6)情報取扱責任者

情報取扱者のうち、情報取扱責任者は、守秘義務等の情報の取り扱いに関する社内教育又はこれに準ずる講習等を受講し、情報取扱者を統括する立場にある者一名を情報取扱責任者として配置しました。

なお、「情報管理計画書」には、上記に従って指定した情報取扱者等の所属、役職、氏名および社内情報セキュリティ教育の受講状況を明記しました。

(7)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および情報保全のための履行体制については以下の「表 7-1-3　再委託内容一覧」のとおりです。

また、請負者自体が業務を実施する場合に求められる水準と同一水準の情報セキュリティ対策を再委託先においても確保しました。再委託先における情報セキュリティの十分な確保を請負者が担保するとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を主管室に提供し、主管室の承認を受けました。

表 7-1-3　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およ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・ワン	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社。	・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。
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。
日本コムシス株式会社	東京都品川区東五反田 2-17-1	・物品手配、設計、構築、測定関連作業、書類作成にあたり必要な会社。	・ローカル５Ｇシステムの設計、構築、電波測定、分析業務、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。
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	・西日本拠点における情報通信インフラ構築の施工管理およびそれに伴う安全管理を実施するにあたり必要な会社。 ・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、施工管理およびそれに伴う安全管理に関する知見・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。
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	・ローカル５Ｇ交換設備共用パターンの技術実証における既設機器ラック内移設および令和４年度に追加	・大型案件における設計・設定実績および専門的なスキルを有しており、迅速なサーバ機器の設計・設定が可能

		構築するサーバの設計・設定にあたり必要な会社。	・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。
株式会社三菱総合研究所	東京都千代田区永田町二丁目10番3号	・ローカル５Ｇ交換設備等相互接続検証およびローカル５Ｇシステムの検証について技術的手引書の作成支援に必要な会社	・ユーザーや業界団体等へのヒアリング調査スキル、さらにニーズや課題への対応策を取りまとめるノウハウ等について熟知 ・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。
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システムの検証において APRESIA 社製品範囲内でのローカル５Ｇ機器のキッティング、製品・技術仕様の問い合わせ対応を行う技術支援に必要な会社。	・ローカル５Ｇ機器の開発元であるため機器について熟知。 ・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。
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	・相互接続検証およ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	・令和４年度の本実証で必要となるローカル５Ｇ機器の保守を担当する。	・ローカル５Ｇ機器の代理店保守専門子会社であり機器の保守について熟知。 ・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。
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およ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およびそれに伴う安全管理を熟知。 ・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。
シャープ株式会社	大阪府堺市堺区匠町１番地	・ローカル５Ｇの大容量性および低遅延性を活かした「高精細映像による大学間遠隔講義」システムを構築し、拠点間リアルタイム 8K	・ソリューション事業を通じた高精細映像環境の設計・構築・施工管理実績を十分に有している。 ・東日本電信電話株式会社との

		映像伝送の検証およびSHARP 社製品範囲内でのローカル５Ｇ機器のキッティング、製品・技術仕様の問い合わせ対応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。
FCNT 株式会社	東京都港区芝 4-13-3 PMO 田町Ⅱ 7 階	・ローカル５Ｇシステムの検証」における、FCNT 社製範囲内での機器選定、製品・技術仕様の問い合わせ対応・技術支援を行うにあたり必要な会社。	・ローカル５Ｇ端末機器の開発元であるため機器について熟知。 ・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。
エクシオエンジニアリング東北株式会社	仙台市青葉区大町 2 丁目 15 番地 28 号	・実証環境構築に向け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	・東北大学における電機工事を熟知。 ・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。
モバイルコミュニケーションズ株式会社	東京都港区赤坂１－１１－２８ＪＭＦビル赤坂０１１０階	・交換設備共用パターンの技術実証、相互接続検証において、技術実証における無線電波測にあたり必要な会社	・ローカル５Ｇシステムの無線電波測定業務を熟知。 ・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。
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	・実証環境構築に向け東京大学、中央研修センタにおける機器設置業務を実施するにあたり必要な会社	・東京大学、中央研修センタ内での機器据え付け業務を熟知。 ・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。
サンコムテクノロジ株式会社	東京都北区中十条 4-16-25	・東京大学・中央研修センタにおけるメタル配線・光配線業務を実施するにあたり必要な会社	・東京大学、中央研修センタ内での配線業務を熟知。 ・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。
有限会社オーエスシステム	仙台市宮城野区宮千代３丁目６番１号ヴェール宮千代Ⅱ-１０２号	・実証環境構築に向け東北大学での電気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天井内配線業務を熟知。 ・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。
新光電機株式会社	大阪府豊中市蛍池南町 3-9-1	・実証環境構築に向け京都大学の基盤構築における配線工事、機器設置を行うにあたり必要な会社	・基盤構築における配線工事、機器設置およびそれに伴う安全管理業務を熟知。 ・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。
有限会社ヤスカワグループ	東京都杉並区井草１－１９－４	・東京大学・中央研修センタにおける電気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における電気配線業務。 ・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	仙台市青葉区大町 2 丁目 15 番地 28 号	・実証環境構築に向け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	・東北大学における電機工事を熟知。 ・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。

1.4 構築・検証のスケジュール

本調査研究の構築および検証のスケジュールを「図 1-4 構築・検証スケジュール」に示します。

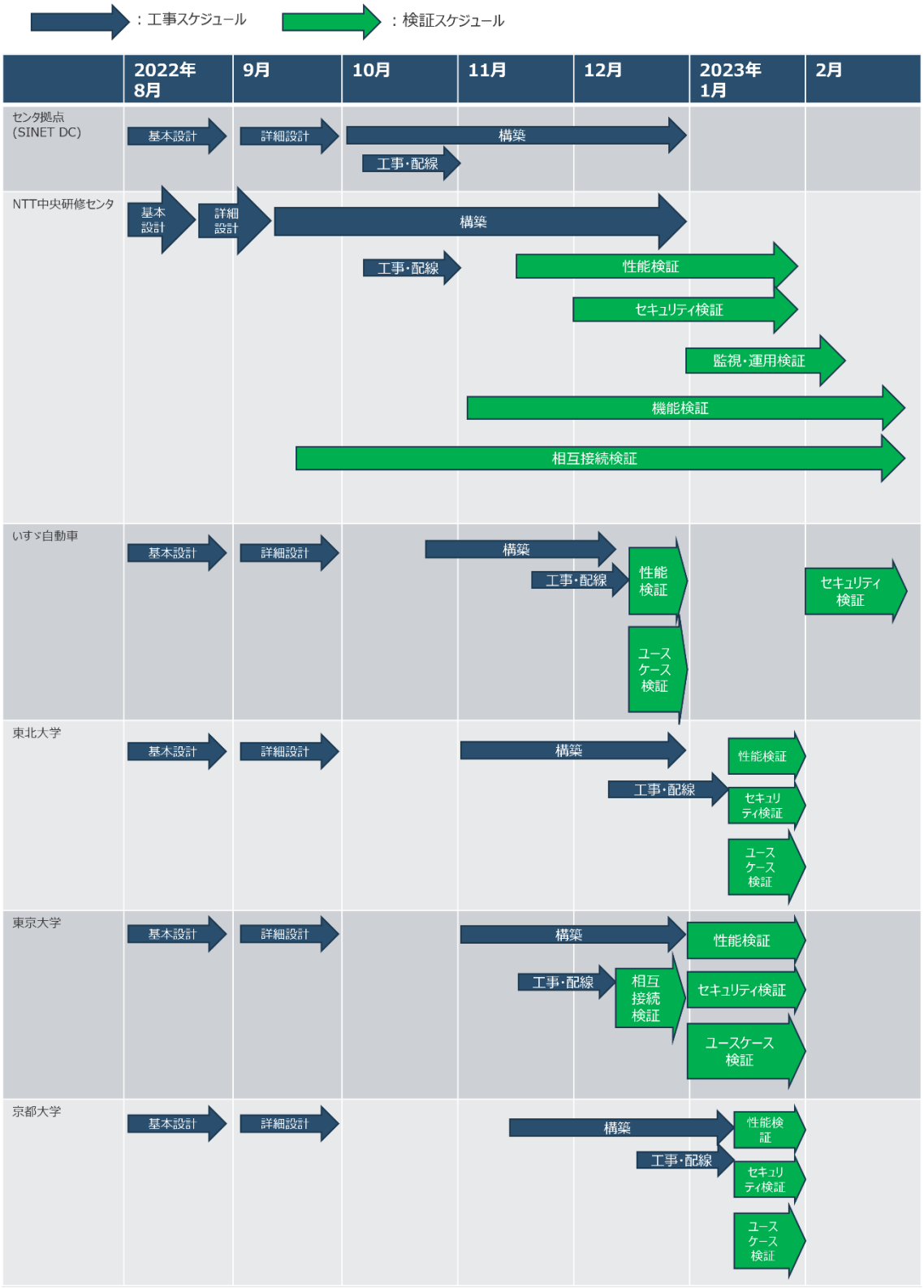


図 1-4 構築・検証スケジュール

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およ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、希望期間は免許の交付日より令和5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」のとおりです。

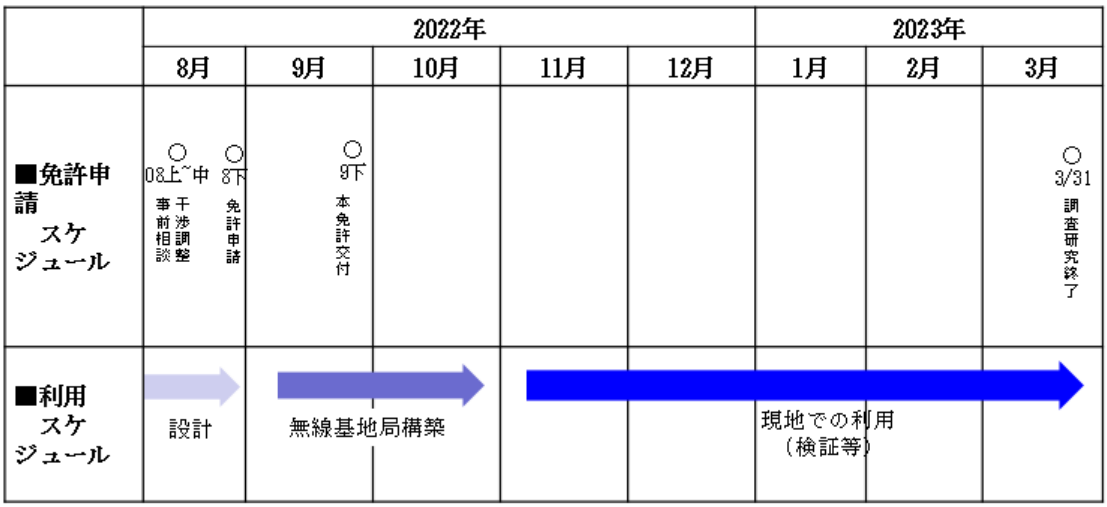


図1-5-1　免許申請スケジュール

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、免許人および申請先（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：14局（関東総合通信局：13局、近畿総合通信局：1局）

・陸上移動局相当：28局（関東総合通信局：26局、近畿総合通信局：2局）

基地局配置のイメージ図を「図1-5-2」に示します。

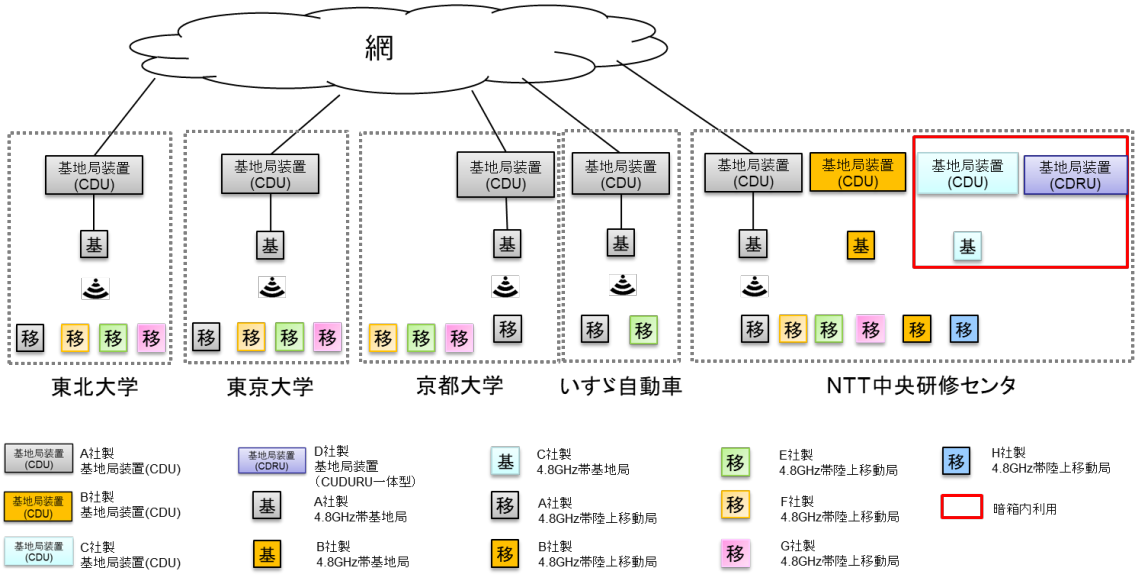


図 1-5-2　基地局配置イメージ図

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した。

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。

・　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」～「表 1-5-10」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　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
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)
アンテナ指向性（※）	無指向性
アンテナ利得（※）	5.0dBi/port
キャリアとの同期条件	同期、準同期1
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ ・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 ・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　ダイワユビキタス学術研究館1階A105 ・神奈川県藤沢市土棚8　いすゞ自動車　藤沢第二工場

表 1-5-2　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	4
識別信号	ひがしでんでんちゅうけんじっけんきち9～12
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	4T4R
電波の型式	X7W
変調方式	(DL)OFDMA：QPSK、16QAM、64QAM、256QAM (UL)OFDMA：QPSK、16QAM、64QAM（256QAMは実装検討中）
送信出力 [W(dBm)](※)	29dBm(total)
アンテナ指向性 （※）	指向性
アンテナ利得 （※）	12.57dBi
キャリアとの同期条件	同期、準同期1
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ ・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 ・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　ダイワユビキタス学術研究館1階A105 ・神奈川県藤沢市土棚8　いすゞ自動車　藤沢第二工場
監視制御所	・茨城県土浦市木田余3550番地つくばネットワーク技術センタ

表 1-5-3　B 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	1
識別信号	ひがしでんでんちゅうけんじっけんきち13
機器ベンダ	B社
中心周波数	4.84986 GHz
占有帯域幅	99.72MHz
空中線構成	4T2R
電波の型式	X7W
変調方式	DFT-s-OFDM: Pi/2BPSK、QPSK、16QAM、64QAM、256QAM CP-OFDM: QPSK、16QAM、64QAM、256QAM
送信出力 [W(dBm)](※)	15dBm
アンテナ指向性 （※）	指向性
アンテナ利得 （※）	11dBi
キャリアとの同期条件	・同期、準同期1、2、3 ※準同期2、3に関してはMNO事業者と干渉調整を実施したします。
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ

表 1-5-4　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
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
変調方式	(DL)OFDMA：QPSK、16QAM、64QAM、256QAM (UL)OFDMA：QPSK、16QAM、64QAM
アンテナ指向性（※）	無指向性
アンテナ利得（※）	ant1:2.3dBi ant2:2.0dBi ant3:1.1dBi ant4:1.6dBi
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ ・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 ・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　ダイワユビキタス学術研究館1階A105 ・神奈川県藤沢市土棚8　いすゞ自動車　藤沢第二工場

表 1-5-5　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	2
識別信号	ひがしでんでんちゅうけんじっけんたんまつ9～10
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 X7W
変調方式	OFDM：QPSK、16QAM、64QAM、256QAM
送信出力[W(dBm)](※)	23dBm(200mW)
アンテナ指向性（※）	無指向性
アンテナ利得（※）	2.4dBi
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ
移動範囲	・東京都調布市入間町1-44 NTT中央研修センタ ・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 ・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 ダイワユビキタス学術研究館1階A105 ・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

表 1-5-6　G 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	2
識別信号	ひがしでんでんちゅうけんじっけんたんまつ11、17
機器ベンダ	G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	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)
アンテナ指向性（※）	無指向性
アンテナ利得（※）	TX0/RX0アンテナ: +0.4dBi TX1/RX1アンテナ: -0.1dBi RX2アンテナ: +1.0dBi RX3アンテナ: 0.0dBi
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ
移動範囲	・東京都調布市入間町1-44 NTT中央研修センタ ・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 ・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 ダイワユビキタス学術研究館1階A105 ・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

表 1-5-7　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	5
識別信号	ひがしでんでんちゅうけんじっけんたんまつ12～16
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	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)
アンテナ指向性(※)	無指向性
アンテナ利得(※)	空中線1:-5.3,空中線2:-13.2,空中線3:-11.8,空中線4:-10.1
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ
移動範囲	・東京都調布市入間町1-44 NTT中央研修センタ ・神奈川県藤沢市土棚8　いすゞ自動車 藤沢第二工場

表 1-5-8　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	5
識別信号	ひがしでんでんちゅうけんじっけんたんまつ18～22
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	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)
アンテナ指向性（※）	無指向性
アンテナ利得（※）	空中線1:−6.5,空中線2:−13.3,空中線3:−5.5,空中線4:−14.5
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ
移動範囲	・東京都調布市入間町1-44 NTT中央研修センタ ・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 ・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 ダイワユビキタス学術研究館1階A105 ・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 ・神奈川県藤沢市土棚8 いすゞ自動車 藤沢第二工場

表 1-5-9　B 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	2
識別信号	ひがしでんでんちゅうけんじっけんたんまつ23～24
機器ベンダ	B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	G1A G1B G1C G1D G1E G1F G1X G7W D1A D1B D1C D1D D1E D1F D1X D7W
変調方式	DFT-s-OFDM: Pi/2BPSK、QPSK、16QAM、64QAM、256QAM CP-OFDM: QPSK、16QAM、64QAM、256QAM
送信出力 [W(dBm)](※)	23dBm(200mW)
アンテナ指向性 （※）	無指向性
アンテナ利得 （※）	1.0 dBi
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ

表 1-5-10　H 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	2
識別信号	ひがしでんでんちゅうけんじっけんたんまつ25～26
機器ベンダ	H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	D1A,D1B,D1C,D1D,D1F,D1X,D7W,G1A,G1B,G1C,G1D,G1F,G1X,G7W X1A,X1B,X1C,X1D,X1F,X1X,X7W
変調方式	OFDM：QPSK、16QAM、64QAM、256QAM
送信出力[W(dBm)](※)	23dBm(200mW)
アンテナ指向性（※）	無指向性
アンテナ利得（※）	2.94 dBi
常置場所	・東京都調布市入間町1-44　NTT中央研修センタ
移動範囲	・東京都調布市入間町1-44　NTT中央研修センタ

・　**京都大学が免許人となる無線局の諸元**

「表 1-5-11」～「表 1-5-12」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 1-5-11　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	1
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	4T4R
電波の型式	X7W
変調方式	(DL)OFDMA：QPSK、16QAM、64QAM、256QAM (UL)OFDMA：QPSK、16QAM、64QAM（256QAMは実装検討中）
送信出力[W(dBm)](※)	29dBm(total)
アンテナ指向性（※）	指向性
アンテナ利得（※）	12.57dBi
キャリアとの同期条件	同期、準同期1
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
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

表 1-5-12　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（移動局相当装置）
無線局数	2
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
変調方式	(DL)OFDMA：QPSK、16QAM、64QAM、256QAM (UL)OFDMA：QPSK、16QAM、64QAM
アンテナ指向性（※）	無指向性
アンテナ利得（※）	ant1:2.3dBi ant2:2.0dBi ant3:1.1dBi ant4:1.6dBi
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
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

干渉調整については、「表 1-5-13」のとおり各事業者に対し実施しました。

表 1-5-13　　干渉調整先事業者

	事業者名
キャリア	株式会社 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） 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) 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、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、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・システム構成」にて示します。

以下の図において、各拠点におけるローカル５Ｇ基地局の設置場所を記載します。



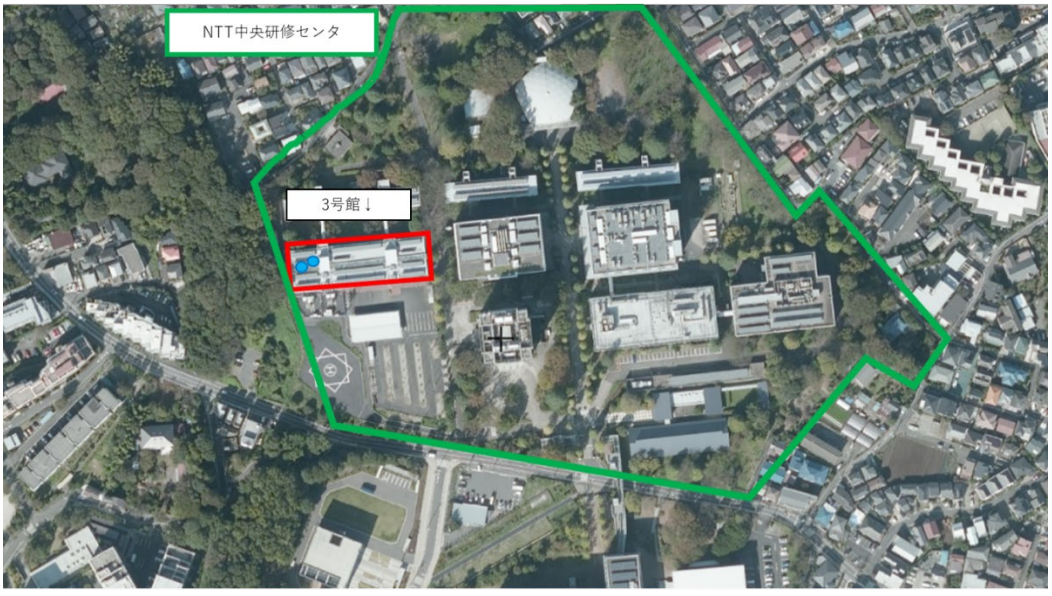
図 2-1-1　いすゞ自動車検証エリア　全体

（出典：国土地理院ウエブサイトより航空写真を加工し作成。以後、航空写真については特記無い場合同じ）



：検証範囲　　：RU設置位置

図 2-1-2　いすゞ自動車検証エリア



：検証範囲　　：RU設置位置

図 2-1-3　　NTT 中央研修センタ 検証エリア　全体

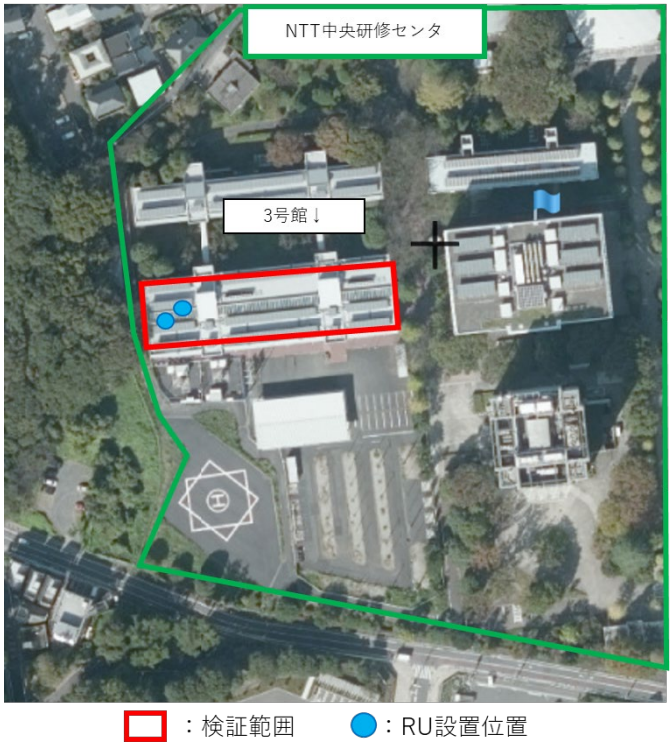


図 2-1-4　NTT 中央研修センタ 検証エリア 3 号館

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基地局を設置し、RU と UE は屋内に設置して検証を行いました。詳細は「2.5 章　ネットワーク・システム構成」にて示します。

以下の図において、各拠点におけるローカル５Ｇ基地局の設置場所を記載します。



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

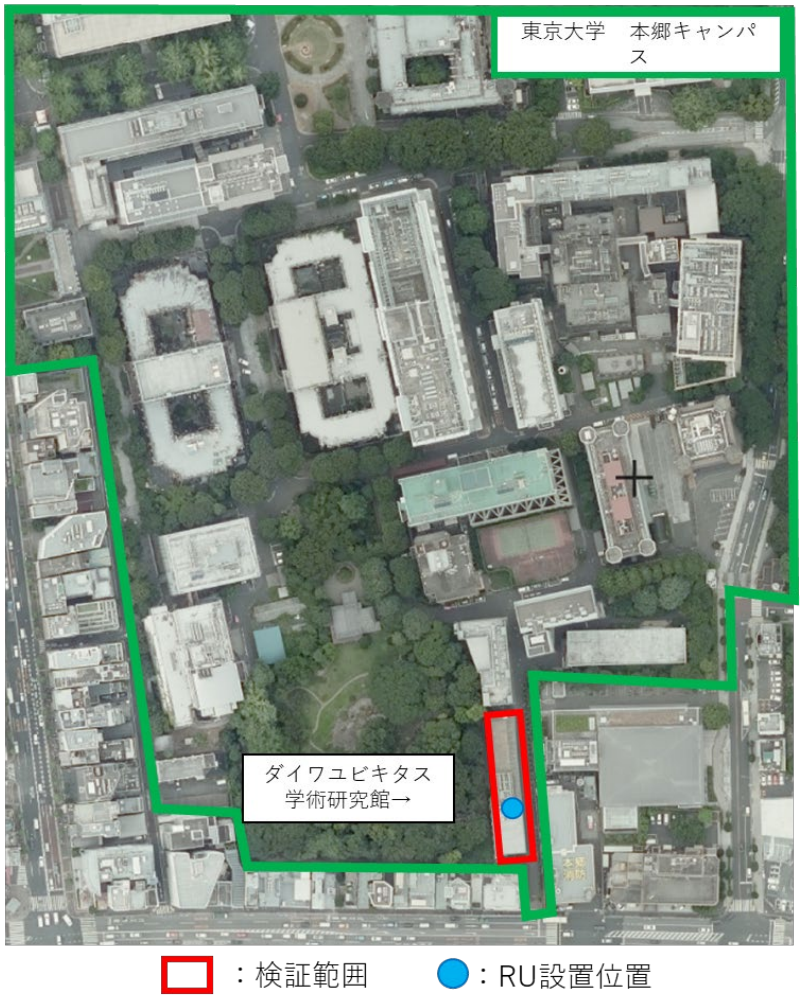


図 2-2-4 東京大学　検証エリア　ダイワユビキタス学術研究館



図 2-2-5 京都大学　検証エリア　全体

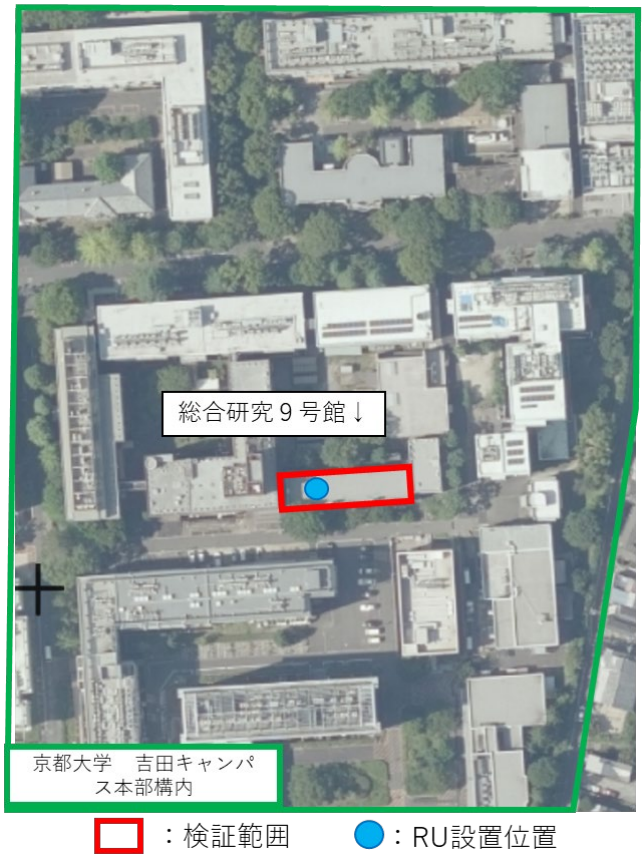


図 2-2-6 京都大学　検証エリア　総合研究９号館

2.3 相互接続検証

相互接続検証では、「NTT 中央研修センタ」および「東京大学」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・システム構成」にて示します。



図 2-3-1　NTT 中央研修センタ 検証エリア　全体（再掲）

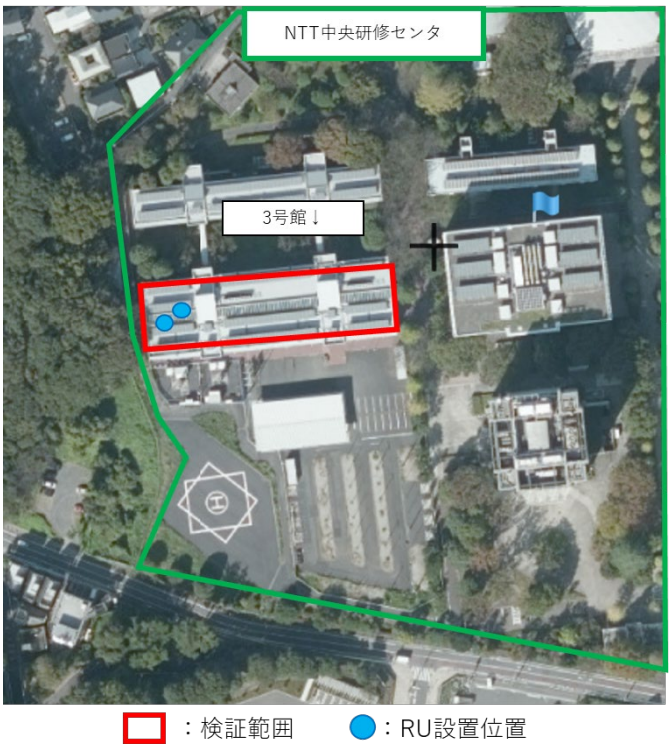


図 2-3-2　NTT 中央研修センタ 検証エリア 3 号館（再掲）



図 2-3-3 東京大学　検証エリア全体（再掲）

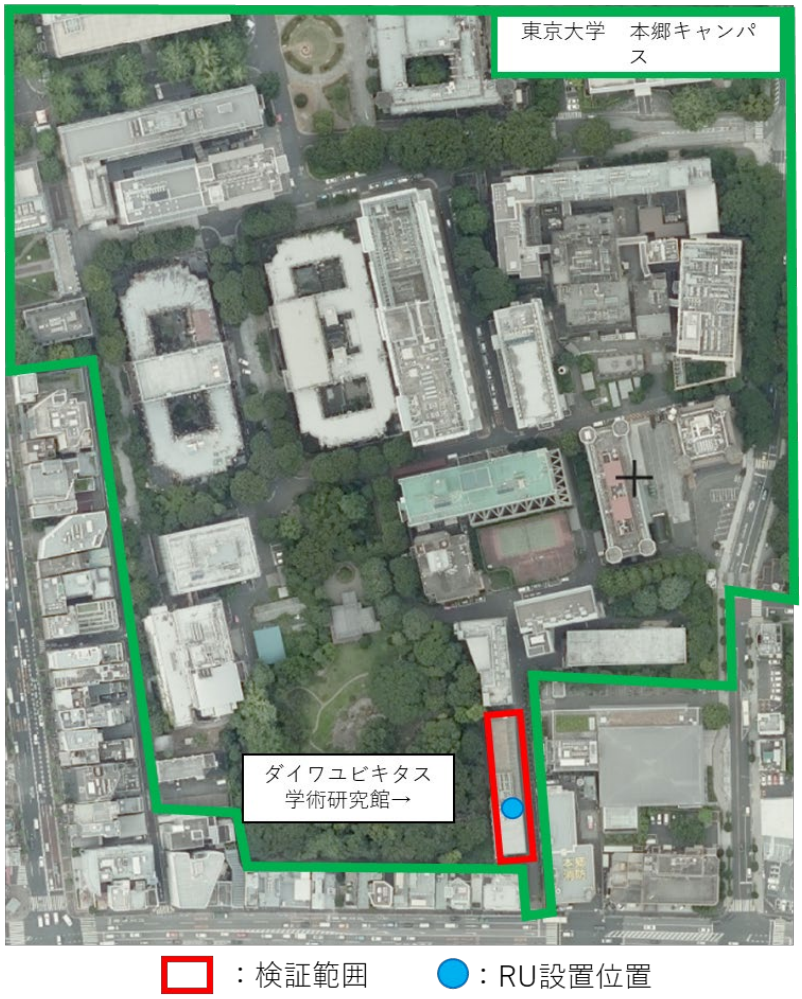


図 2-3-4 東京大学　検証エリア　ダイワユビキタス学術研究館（再掲）

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。また、B 社製コア装置用ハードウェア 1 台でローカル５Ｇ基地局 1 拠点分を収容しました。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 および 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。システム・端末監視サーバ上で SIM のセキュリティ機能を提供する仮想マシンである TMMNS Inspector および TMMNS マネジメントを配置し、さらに各機器の死活監視を行うためのシステム監視ツール(M 社製)も同一サーバで配置しました。これにより、複数の拠点でそれぞれ SIM のセキュリティ機能、機器の死活監視を実現しています。仮想 CU 用基盤サーバのハードウェア 1 台に CU 機能を搭載した仮想マシンを拠点毎に配置することにより、5 拠点間での CU/DU 分割化を実現しています。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。センタ拠点 UTM は、複数の拠点と量子暗号鍵交換方式を行うための機能を有しています。

また、センタ拠点では、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-D、RU-A、DU-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、NTT 中央研修センタは、センタ拠点と SIM のセキュリティ機能を提供するため TMMNS Inspector を配置しています。

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。

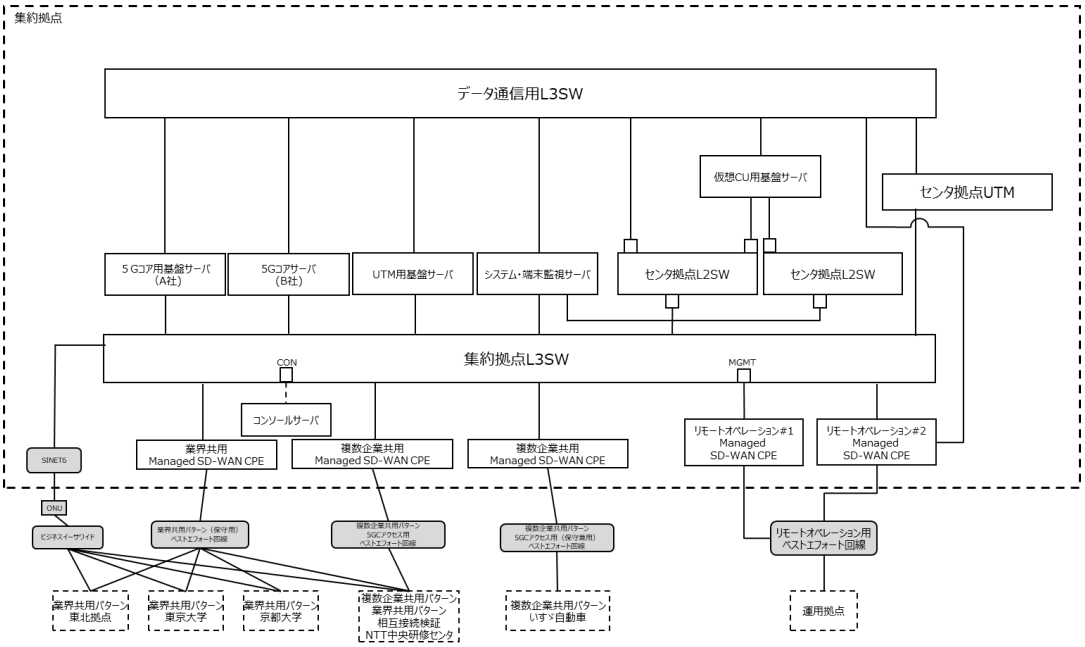


図 3-1-1-1 センタ拠点（SINET DC） ネットワーク構成図

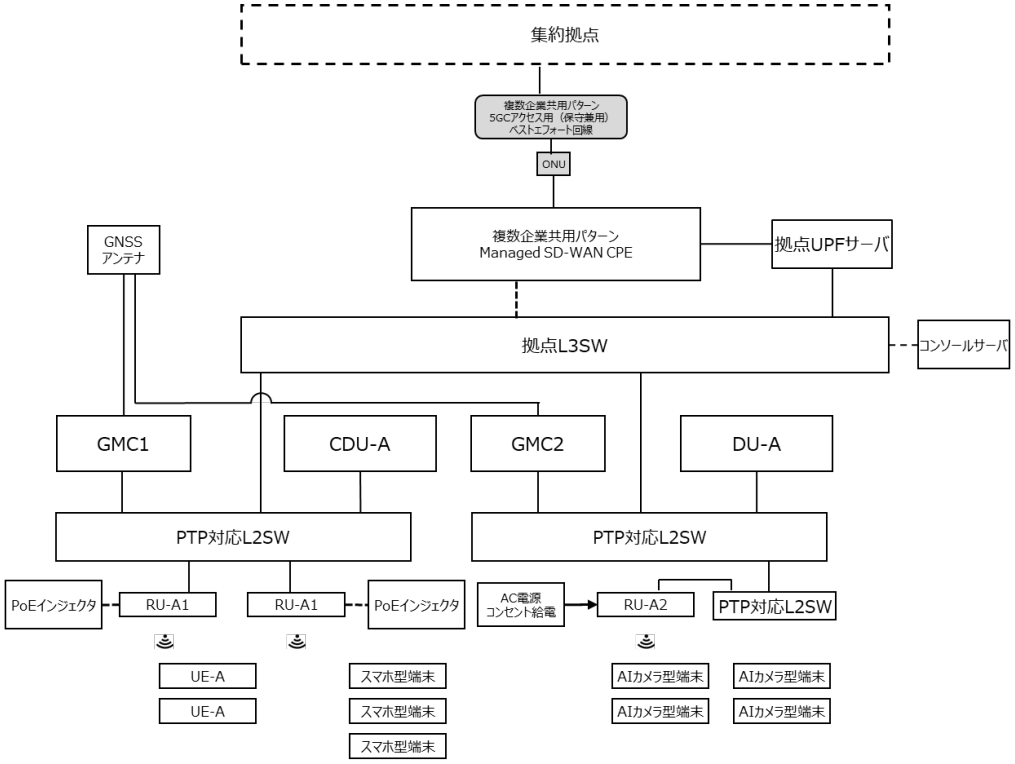


図 3-1-1-2 いすゞ自動車 ネットワーク構成図

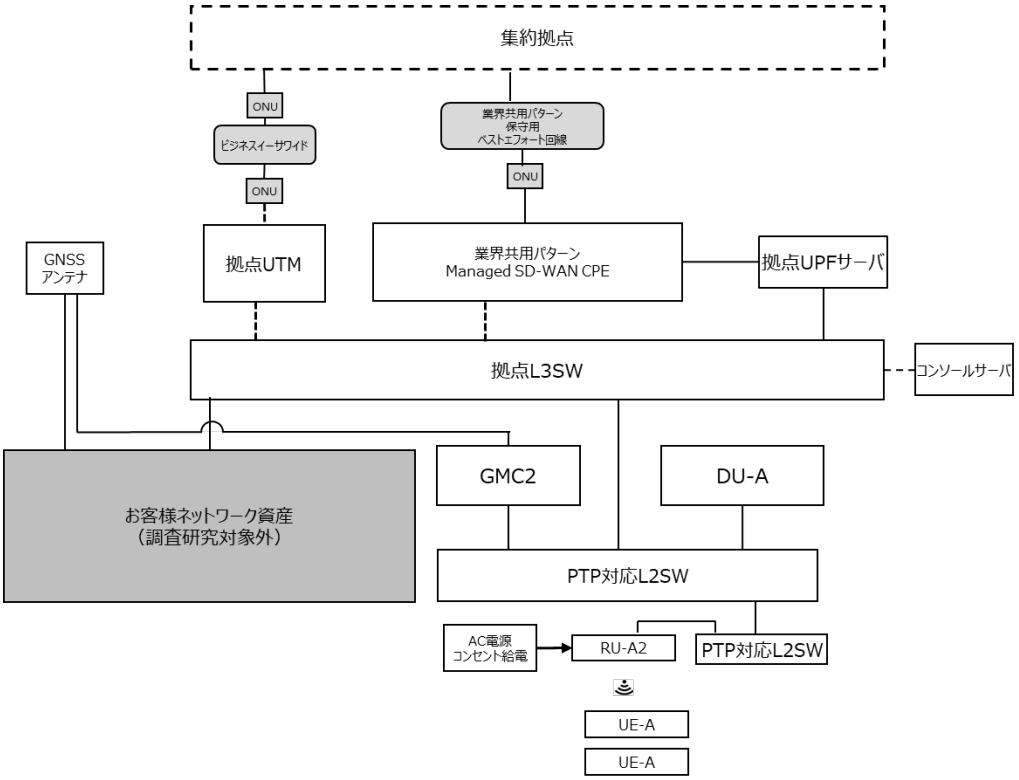


図 3-1-1-3 東北大学、京都大学 ネットワーク構成図

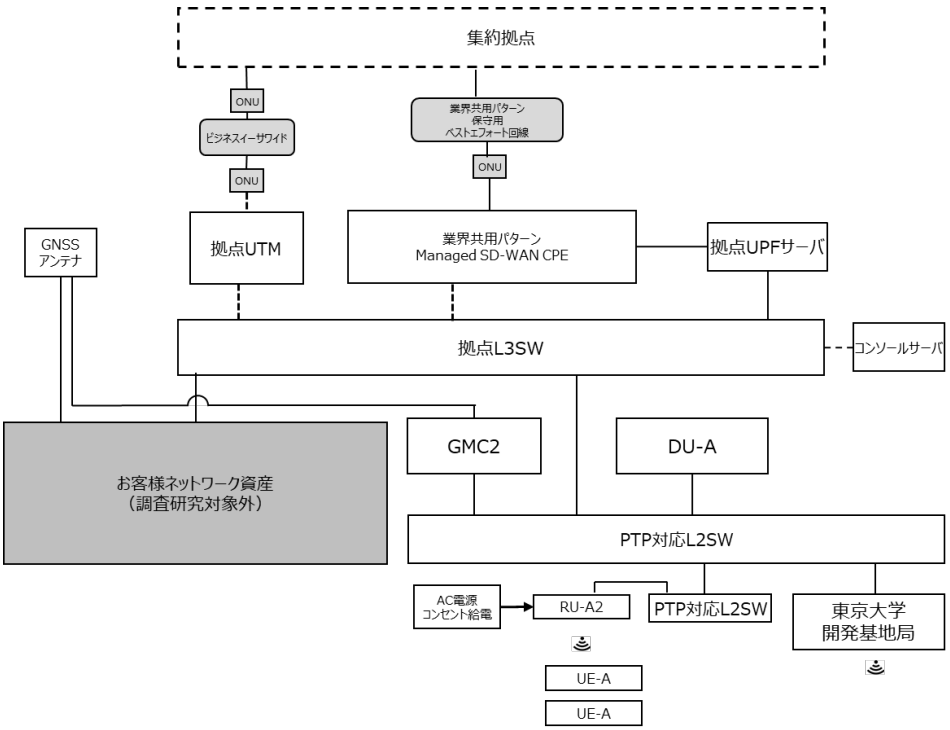


図 3-1-1-4 東京大学 ネットワーク構成図

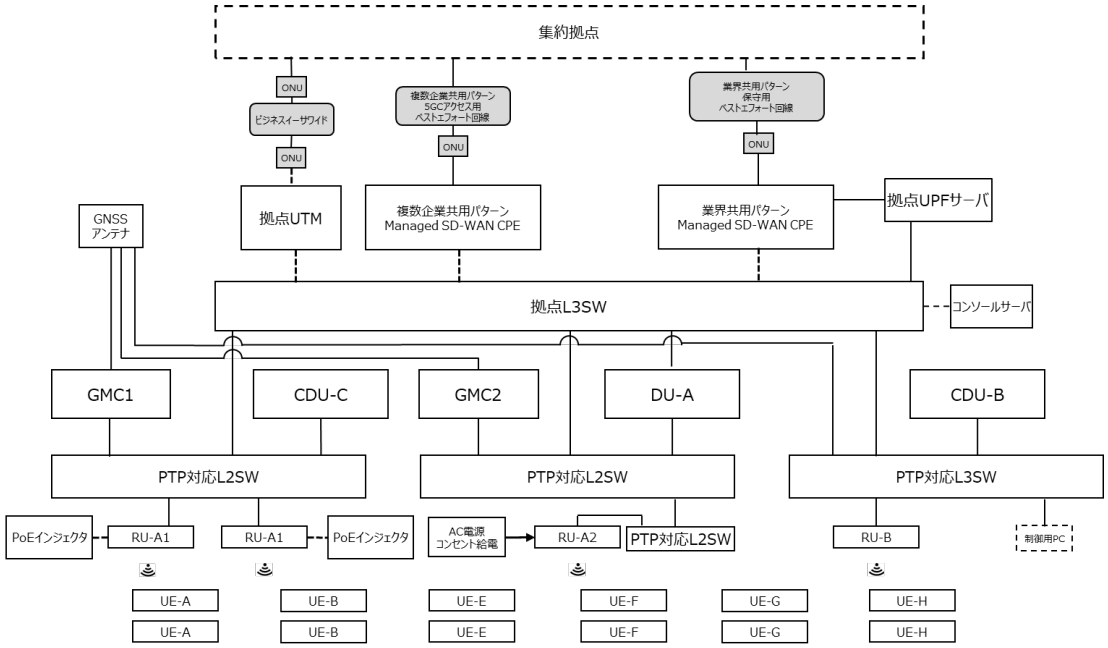


図 3-1-1-5 NTT 中央研修センタ ネットワーク構成図

(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)、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、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、1Gbps 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 通信および 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およ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 通信および 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ています。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。

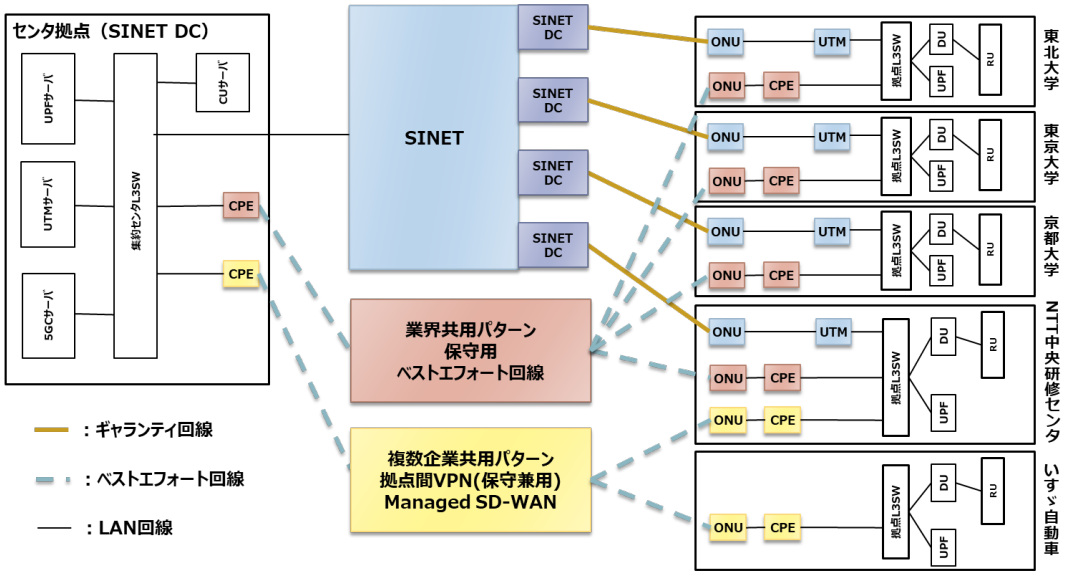


図 3-1-2-1 拠点間ネットワーク

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
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	・1Gbps ギャランティ回線 ・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
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

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 3-2-8」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（A 社）	I 社	XXXXXXXXXX	1	CPU：Intel Xeon 32 コア メモリ：288GB DISK：1.6TB
		A 社	XXXXXXXXXX	5	5GC VM
		A 社	XXXXXXXXXX	5	UPF VM
		J 社	XXXXXXXXXX	2	仮想基盤ソフト（vSwitch,ESXi）
2	５Ｇコアサーバ（B 社）	B 社	-	1	3GPP Release 15
3	UTM 用基盤サーバ	I 社	XXXXXXXXXX	1	CPU：Intel Xeon 32 コア メモリ：288GB DISK：1.6TB
		K 社	XXXXXXXXXX	1	UTM VM
		K 社	XXXXXXXXXX	1	UTM VM
		K 社	XXXXXXXXXX	1	
		K 社	XXXXXXXXXX	1	UTM VM
		K 社	XXXXXXXXXX	2	Web Application Firewall – 仮想アプライアンス(8 x vCPU core まで)
		K 社	XXXXXXXXXX	2	WAF VM
		J 社	XXXXXXXXXX	2	仮想基盤ソフト（vSwitch,ESXi ）
		J 社	XXXXXXXXXX	1	vCenter
4	システム・端末監視サーバ	L 社	XXXXXXXXXX	1	CPU：Intel Xeon 32 コア メモリ：96GB DISK：1.8TB
		J 社	XXXXXXXXXX	1	仮想基盤ソフト（vSwitch,ESXi ）
		M 社	XXXXXXXXXX	1	CPU:8 メモリ:16 DISK:100
		A 社	XXXXXXXXXX	1	CPU:8

					メモリ:16 DISK:100
		N 社	XXXXXXXXXX	1	CPU:4 メモリ:8 DISK:100
		N 社	XXXXXXXXXX	1	CPU:2 メモリ:12 DISK:8
5	センタ拠点 L3SW	O 社	XXXXXXXXXX	2	
6	コンソールサーバ	P 社	XXXXXXXXXX	1	
7	センタ拠点 L2SW	A 社	XXXXXXXXXX	2	
8	仮想 CU 基盤サーバ	I 社	XXXXXXXXXX	1	CPU：Intel Xeon 32 コア メモリ：192GB DISK：1.6TB
		J 社	XXXXXXXXXX	1	仮想基盤ソフト （vSwitch,ESXi ）
		J 社	XXXXXXXXXX	1	vCenter
		A 社	XXXXXXXXXX	5	
9	センタ拠点 UTM	K 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	O 社	XXXXXXXXXX	1	
2	コンソールサーバ	P 社	XXXXXXXXXX	1	
3	拠点 UPF サーバ	I 社	XXXXXXXXXX	1	CPU：Intel Xeon 16 コア メモリ：32GB DISK：800G
		A 社	XXXXXXXXXX	1	
		J 社	XXXXXXXXXX	2	
4	PTP 対応 L2SW	A 社	XXXXXXXXXX	3	
5	CDU-A	A 社	XXXXXXXXXX	1	

6	DU-A	A 社	XXXXXXXXXX	1	
7	RU-A1	A 社	XXXXXXXXXX	2	PoE インジェクタは付属品を使用
	RU-A2	A 社	XXXXXXXXXX	1	PoE インジェクタは付属品を使用
8	UE-A	A 社	XXXXXXXXXX	2	
9	AI カメラ型端末	E 社	XXXXXXXXXX	4	
10	UE-E	E 社	XXXXXXXXXX	3	
11	GMC	P 社	XXXXXXXXXX	1	
		P 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	O 社	XXXXXXXXXX	1	
2	コンソールサーバ	P 社	XXXXXXXXXX	1	
3	UTM	K 社	XXXXXXXXXX	1	
		K 社	XXXXXXXXXX	1	Unified Threat Protection (UTP) ライセンス+製品保守
4	拠点 UPF サーバ	I 社	XXXXXXXXXX	1	CPU：Intel Xeon 16 コア メモリ：32GB DISK：800G
		A 社	XXXXXXXXXX	1	
		J 社	XXXXXXXXXX	2	
5	PTP 対応 L2SW	A 社	XXXXXXXXXX	2	
6	DU-A	A 社	XXXXXXXXXX	1	
7	RU-A	A 社	XXXXXXXXXX	1	PoE インジェクタは付属品を使用
8	UE-A	A 社	XXXXXXXXXX	2	
9	GMC	P 社	XXXXXXXXXX	1	
		P 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	0 社	XXXXXXXXXX	1	
2	コンソールサーバ	P 社	XXXXXXXXXX	1	
3	UTM	K 社	XXXXXXXXXX	1	
		K 社	XXXXXXXXXX	1	Unified Threat Protection (UTP) ライセンス+製品保守
4	拠点 UPF サーバ	I 社	XXXXXXXXXX	1	CPU：Intel Xeon 16 コア メモリ：32GB DISK：800G
		A 社	XXXXXXXXXX	1	
		J 社	XXXXXXXXXX	2	
5	東京大学開発基地局	-	-	1	
6	PTP 対応 L2SW	A 社	XXXXXXXXXX	2	
7	DU-A	A 社	XXXXXXXXXX	1	
8	RU-A2	A 社	XXXXXXXXXX	1	PoE インジェクタは付属品を使用
9	UE-A	A 社	XXXXXXXXXX	2	
10	GMC	P 社	XXXXXXXXXX	1	
		P 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	O 社	XXXXXXXXXX	1	
2	コンソールサーバ	P 社	XXXXXXXXXX	1	
3	UTM	K 社	XXXXXXXXXX	1	
		K 社	XXXXXXXXXX	1	Unified Threat Protection（UTP）ライセンス+製品保守
4	拠点 UPF サーバ	I 社	XXXXXXXXXX	1	CPU：Intel Xeon 16 コア メモリ：32GB DISK：800G
		A 社	XXXXXXXXXX	1	
		J 社	XXXXXXXXXX	2	
5	PTP 対応 L2SW	A 社	XXXXXXXXXX	2	
6	DU-A	A 社	XXXXXXXXXX	1	
7	RU-A2	A 社	XXXXXXXXXX	1	PoE インジェクタは付属品を使用
8	UE-A	A 社	XXXXXXXXXX	2	
9	GMC	P 社	XXXXXXXXXX	1	
		P 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	O 社	XXXXXXXXX	1	
2	コンソールサーバ	P 社	XXXXXXXXX	1	
3	UTM	K 社	XXXXXXXXX	1	
		K 社	XXXXXXXXX	1	Unified Threat Protection（UTP）ライセンス+製品保守
4	拠点 UPF サーバ	I 社	XXXXXXXXX	1	CPU：Intel Xeon 16 コア メモリ：32GB DISK：800G
		A 社	XXXXXXXXX	1	
		J 社	XXXXXXXXX	2	
		N 社	XXXXXXXXX	1	CPU:2 メモリ:12 DISK:8
5	PTP 対応 L2SW	A 社	XXXXXXXXX	3	
6	CDU-C	C 社	XXXXXXXXX	1	
7	DU-A	A 社	XXXXXXXXX	1	
8	CDRU-D	D 社	XXXXXXXXX	1	
9	CDRU-D 用暗箱	Q 社	XXXXXXXXX	1	
10	RU-A1	A 社	XXXXXXXXX	2	PoE インジェクタは付属品を使用
	RU-A2	A 社	XXXXXXXXX	1	PoE インジェクタは付属品を使用
11	RU-C	C 社	XXXXXXXXX	1	
12	UE-A	A 社	XXXXXXXXX	2	
13	UE-F	F 社	XXXXXXXXX	2	
14	UE-E	E 社	XXXXXXXXX	2	
15	UE-G	G 社	XXXXXXXXX	2	
16	UE-B	B 社	XXXXXXXXX	2	
17	UE-H	H 社	XXXXXXXXX	1	
18	AI カメラ型端末	E 社	XXXXXXXXX	1	
19	GMC	P 社	XXXXXXXXX	1	

		P 社	XXXXXXXXXX	1	
20	PTP 対応 L3SW	R 社	XXXXXXXXXX	1	
21	CDU- B	B 社	-	1	
22	RU- B	B 社	-	1	
23	制御用 PC	S 社	XXXXXXXXXX	1	

表 3-2-7　4K カメラ AI 監視ソリューション　機器一覧

No.	物品	メーカ	型番	数量	備考
1	AI カメラ型端末	E 社	XXXXXXXXXX	5	
2	スマホ型端末	E 社	XXXXXXXXXX	3	

表 3-2-8　8K 高精細映像伝送システム　機器一覧

No.	物品	メーカ	型番・品名	数量	備考
1	8K カメラ	B 社	XXXXXXXXXX	1	
2	送信クライアント PC	S 社	XXXXXXXXXX	1	
3	8K テレビ	B 社	XXXXXXXXXX	1	
4	エンコーダ	T 社	XXXXXXXXXX	1	
5	デコーダ PC	U 社	XXXXXXXXXX	1	

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。

(1) ５Ｇコア用基盤サーバ（A 社）

５Ｇコア用基盤サーバ（A 社）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	

(2) 5G コアサーバ（B 社）

５Ｇコアサーバ（B 社）はローカル５Ｇシステムのソフトウェアを搭載し、センタ拠点（SINET DC）内のラックに設置します。

表 3-3-2 ５Ｇコアサーバ仕様

項目	仕様	備考
電源	AC100V	
消費電力	150 W	
CPU	Intel® Xeon® D-2146NT CPU@2.30GHzx16	
メモリ容量	64GB DDR4	
DISK 容量	256GB	
概算質量	3.4 kg 以下	
外形寸法	254(W)×226(D)×43(H) mm	

(3) 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ます。

表 3-3-3 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	

(4) システム・端末監視サーバ

システム・端末監視サーバを 1 台、センタ拠点（SINET DC）内のラックに設置します。

表 3-3-4　システム・端末監視サーバ仕様

項目	仕様	備考
電源	AC100V~240V	
消費電力	644W（MAX Potential Power）	
CPU	Intel® Xeon® Silver (16 コア 32 スレッド)×2	
メモリ容量	96GB	
DISK 容量	1.8TB	
概算質量	21.0kg	
外形寸法	H4.28×W48.20×D77.2	

(5) L3SW

センタ拠点（SINET DC）では５Ｇコア用基盤サーバ（A 社）、５Ｇコアサーバ（B 社)、UTM 用基盤サーバ、システム・端末監視サーバ、仮想 CU 基盤サーバ、PTP 対応 L2SW、UTM、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 2 台構築します。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）構築します。各 L3 スイッチは各拠点内のラックに設置します。

表 3-3-5 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	

(6) コンソールサーバ

５Ｇコア用基盤サーバ（A 社）、５Ｇコアサーバ（B 社)、UTM 用基盤サーバ、システム・端末監視サーバ、仮想 CU 基盤サーバ、UTM、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 台構築します。コンソールサーバは各拠点内のラックに設置します。

表 3-3-6 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	

(7) 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トラヒックを暗号化する機器として UTM を各大学および NTT 中央研修センタにそれぞれ 1 台（計 4 台）構築します。また、センタ拠点（SINET DC）には 4 拠点を集約できるマルチテナント型の UTM を 1 台構築します。各 UTM は各拠点内のラックに設置します。

表 3-3-7 拠点 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/最大）	17.0 W / 18.5 W	

表 3-3-8 センタ拠点 UTM 仕様

項目	仕様	備考
ファイアウォール スループット	67.5 M pps	
ファイアウォール 同時セッション（TCP）	8 M	
ファイアウォールポリシー	100,000	
外形寸法	88.9 x 443 x 447.4 mm	
重量	11.3 kg	
消費電力（平均/最大）	217 W / 336 W	

(8) 拠点 UPF サーバ（NTT 中央研修センタ）

NTT 中央研修センタでは、複数企業共用パターン・業界共用パターンにおいて、センタ拠点を介せずにローカル５Ｇのトラヒックを転送するために、UPF サーバを 1 台拠点内のラックに構築します。

表 3-3-9 拠点 UPF サーバ（NTT 中央研修センタ）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	64GB	
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	

(9) 拠点 UPF サーバ（いすゞ自動車、東北大学、東京大学、京都大学）

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のトラヒックを転送するために、拠点 UPF サーバを各拠点 1 台（計 4 台）構築します。拠点 UPF サーバは各拠点内のラックに設置します。

表 3-3-10 拠点 UPF サーバ（いすゞ自動車、東北大学、東京大学、京都大学）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	

(10)PTP 対応 L2SW

PTP 対応 L2SW 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、DU、RU と接続します。PTP 対応 L2 スイッチはセンタ拠点、NTT 中央研修センタ、いすゞ自動車に 2 台、各大学に 1 台(計 9 台)ラックに収容します。

表 3-3-11 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	

(11)PTP 用 L3SW

PTP 対応 L3SW は GMC(Grand Master Clock)と接続し、GPS アンテナから得た時刻等を接続する機器に同期させるためのスイッチです。DU、RU、GNSS アンテナと接続します。PTP 対応 L3SW は中央研修センタに 1 台ラック収容します。

表 3-3-12　PTP 対応 L3SW 仕様

項目	仕様	備考
SFP スロット数	2(100GE/QSEP28) 8(25GE/SFP28) 20(10GE/SFP+)	
LAN ポート数	4	
スイッチング容量	100Gbps	
外形寸法	440(W)×302(D)×43.5(H) mm	
重量	6.6 kg	
消費電力	400 W 以下	

(12)仮想 CU 基盤サーバ

仮想 CU 基盤サーバは、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)を５台、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ます。

表 3-3-13 仮想 CU 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® Silver(8 コア 16 スレッド)×2	
メモリ容量	192GB	
ストレージ容量	1.6TB	
概算質量	23.6kg（最大）	
外形寸法	4455×7302×873mm、2U ラックマウント型	

(13)DU-A

DU-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分散ノード機能を担う DU(Distributed Unit)を実装するサーバです。DU-A サーバはセンタ各拠点に 1 台（計 5 台）ラックに収容します。

表 3-3-14 DU-A 仕様

項目	仕様	備考
電源	AC100~120V(50-60Hz)、AC200~240V(50-60Hz)	
消費電力	1000W@100V, 2000W@200V(定格値)	
CPU	Intel® Xeon® Silver 4314 Processor (16C/32T)	
メモリ容量	64GB	
ストレージ容量	240GB	
概算質量	17.5kg (サーバ 15.6kg、FPGANIC1.5kg、その他 0.3kg)	
外形寸法	89 x 437 x 574mm (HxWxD)	

(14)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 サーバはルーター（拠点用）、時刻同期対応スイッチした PTP 対応 L2SW を接続します。CDU-A サーバはセンタ拠点・NTT 中央研修センタ・いすゞ自動車にそれぞれ 1 台ずつラックに収容します。

表 3-3-15 CDU-AP 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	

(15)CDU-C

CDU-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 DU(Distributed Unit)を実装する仮想サーバです。CDU-C サーバはルーター（拠点用）、時刻同期対応スイッチした PTP 対応 L2SW を接続します。NTT 中央研修センタに 1 台設置します。

表 3-3-16 CDU-C 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	

(16)CDU-B

CDU-B は B 社製のローカル５Ｇの CDU で、NTT 中央研修センタに 1 台設置します。

表 3-3-17 CDU-B 仕様

項目	仕様	備考
電源	AC100V×2	
消費電力	800W	
CPU	Intel® Xeon® Scalable Processor Purley product family (Dual Skylake SP-6248)	
メモリ容量	128GB DDR4	
ストレージ容量	480GB	
概算質量	446(W)×711(D)×87(H) mm	
外形寸法	30 kg	

(17)CDRU-D

CDRU-D 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。NTT 中央研修センタに 1 台設置します。

表 3-3-18 CDRU-D 仕様

項目	仕様	備考
対応周波数帯	4.7~4.8GHz/4.8~4.9GHz　2 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℃	

(18)CDRU-D 用暗箱

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

表 3-3-19 CDRU-D 用暗箱 仕様

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	

(19)東京大学開発基地局

東京大学開発基地局サーバは、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。東京大学に 1 台設置します。

表 3-3-20　東京大学開発基地局 仕様

項目	仕様	備考
無線局数	1 局	
中心周波数	4849.98MHz	
占有帯域幅	100MHz(99.96MHz)	
空中線構成	2T2R	
電波の型式	100M X7W	
変調方式	OFDM	
送信出力[W(dBm)]	18dBm(63mW)	
空中線指向性	指向性外部アンテナ x 2 基	
アンテナ利得	12dBi	

(20)RU-A1/RU-A2

RU-A1/RU-A2 は A 社製のローカル５ G の RU で、NTT 中央研修センタ、いすゞ自動車に RU-A1 を 2 台ずつ（計 4 台）、全拠点に RU-A2 を 1 台ずつ（計 5 台）設置します。

表 3-3-21 RU-A1 仕様

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	

表 3-3-22 RU-A2 仕様

項目	仕様	備考
電源	AC100V	
消費電力	100w	
概算質量	12kg 以下	
外形寸法	(L x W x H)：：389.6mm x 389.6mm x134.9mm	
動作温度	-40~55℃	
対応周波数	4.8~4.9GHz	
最大送信電力	24dBm/Ant	
本体同梱品	AC 電源アダプター、ポールマウント金具	

(21)RU-C

RU-C は C 社製のローカル５ G の RU で、NTT 中央研修センタに 1 台設置します。

表 3-3-23 RU-C 仕様

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	

(22)RU-B

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

表 3-3-24 RU-B 仕様

項目	仕様	備考
電源	DC -48V	
消費電力	100 W	
概算質量	12g	
外形寸法	389.6(W) x 389.6(D) x 134.9(H) mm	
動作温度	-40℃～55℃	
対応周波数	n79(4.8～4.9GHz)	
最大送信電力	24dBm/port	
本体同梱品	屋外向け電源ユニット一式､マウンティングキット	

(23)UE-A

UE-A は A 社製のローカル５Ｇ端末（UE）で、各拠点に 2 台（計 10 台）用意します。

表 3-3-25 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 x 1	

(24)UE-F

UE-F は F 社製のローカル５Ｇ端末（UE）で、NTT 中央研修センタに 2 台用意します。

表 3-3-26 UE-C0 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/0	USB3.1 Gen2, Type C, Nano-SIM, RJ45	

(25)UE-E

UE-E は E 社製のローカル５Ｇ端末（UE）で、NTT 中央研修センタに 2 台用意します。

表 3-3-27 UE-FC 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）	

(26)UE-G

UE-G は G 社製のローカル５G端末（UE）で、NTT 中央研修センタに 2 台用意します。

表 3-3-28 UE-KY 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。	

(27)UE-B

UE-B は B 社製のローカル５Ｇ端末（UE）で、NTT 中央研修センタに 2 台用意します。

表 3-3-29 UE-SH 仕様

項目	仕様	備考
電池/充電端子	4570mAh（内蔵電池）/USB Type-C(PD3.0)	
概算質量	178 g	
外形寸法	148×71×8.9 mm	
ディスプレイ	約 5.8 インチ Full HD+(1,080×2,280 ドット)	
CPU	Qualcomm® Snapdragon™ 690 5G Mobile Platform,2.0GHz+1.7GHz オクタコア	
メモリ	RAM：4GB / ROM：64GB	
通信方式	5G(sub6/NR 化)/4G LTE/WiMAX 2+	
ネットワークタイプ	NSA/SA	

(28)UE-H

UE-H は H 社社製のローカル５Ｇ端末（UE）で、NTT 中央研修センタに 2 台用意します。

表 3-3-30 UE-NK 仕様

項目	仕様	備考
電源	12V DC 供給	
消費電力	最大 36W	
概算質量	1000g	
外形寸法	直径 125mm x 高 218.5mm	
動作温度	-5 ~ +40℃	
対応周波数	n79, B41, n41	
最大空中線電力	23dBm(0.2W)	
本体同梱品	電源アダプタ	

(29)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(5GC システム無線基地局)に対して行います。各拠点に GMC1 を 1 台（計 5 台)、GMC2 を 1 台（計 5 台）設置します。

表 3-3-31　GMC1 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	

表 3-3-32　GMC2 仕様

項目	仕様	備考
定格電圧	AC100~240V +-10%(50/60Hz)	
定格電流	0.34A/0.19A	
消費電力	20W	
発熱量	72.0kJ/h	
設置方式	棚置き（横）	
外形寸法	208(W)×282(D)×44(H)mm	
質量	約 2kg	

(30)AI カメラ型端末

AI カメラ型端末には、E 社の製品を使用します。

表 3-3-33　AI カメラ型端末　仕様

項目	仕様	備考
OS	Android 11.0	
メモリ	8GB/128GB	
カメラ画素数	4,850 万画素(79 度/f1.8) 800 万画素(120 度/f2.4) 500 万画素(83 度/f2.2) *3	
電池容量	3600mAh/USB Type-C による外部給電	
重量	約 600g	
堅牢性	・温度-30℃～60℃ ・防水・防塵(IP65)	

(31)スマホ型端末

スマホ型端末には、E 社の製品を使用します。

表 3-3-34　スマホ型端末　仕様

項目	仕様	備考
OS	Android 11.0	
メモリ	8GB/128GB/microSD	
カメラ画素数	フロント：32M，リア：48M+16M(広角)+8M(深度)	
電池容量	4,070mAh	
重量	約 171g	
堅牢性	・温度 5～35℃ ・IPX5,8 相当/IP6X 相当	

(32)8K カメラ

8K カメラには、B 社の製品を使用します。

表 3-3-35　8K カメラ　仕様

項目	仕様	備考
解像度	7680×4320@60fps 対応	
外形寸法	155mm x 188mm x 312mm	
重量	約 5kg	
入出力端子	12G-SDI	

(33)送信クライアント PC

送信クライアント PC には、S 社の製品を使用します。

表 3-3-36　送信クライアント PC　仕様

項目	仕様	備考
CPU	Intel Core i5-1135G7	
メモリ	8GB	
ストレージ	SSD 256GB	
入出力	USB3.0(Type-A,Type-C)	
重量	約 979g	
外形寸法	約 303.9（幅）×197.4（奥行）×17.9（高さ）mm	
OS	Ubuntu 22.04	

(34)8K テレビ

8K テレビには、B 社の製品を使用します。

表 3-3-37　8K テレビ　仕様

項目	仕様	備考
画面サイズ	60V 型ワイド(対角 152.7cm)	
最大解像度/フレームレート	7680×4320 60p / 3840×2160 120p 対応	
入力端子	HDMI2.1×2 系統, HDMI2.0×2 系統	
重量	約 34kg (スタンド込み)	
外形寸法	約 135.6×29.0×87.0cm(スタンド込み)	

(35)エンコーダ

エンコーダには、T 社の製品を使用します。

表 3-3-38　エンコーダ　仕様

項目	仕様	備考
解像度	7680×4320@60fps 対応	
映像符号化方式	H.265	
符号化情報速度	最大 200Mbps	
外形寸法	190mm x 44mm x 187mm	
重量	約 1.7kg	
入出力	12G-SDI, Ethernet, HDMI2.1	

(36)デコーダ PC

デコーダ PC には、U 社の製品を使用します。

表 3-3-39　デコーダ PC　仕様

項目	仕様	備考
CPU	Core i7-11700	
GPU	NVIDIA GeForce RTX 3070	
メモリ	64GB	
ストレージ	SSD 1TB	
入出力	Gigabit ethernet / HDMI2.1	
重量	約 14kg	
外形寸法	220（幅）×440（奥行き）×480（高さ）　mm	
OS	Ubuntu 22.04	

3.4 システム機能・性能・要件

技術検証に関するローカル５Ｇシステムに関する各システムについて、本検証の実施および検証目標の達成に必要な機能、性能および要件について下記に示します。

(1) ローカル５Ｇネットワーク

表 3-4-4-1　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ーネント機能（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 1.6Gbps、UL:約 221Mbps ・ 準同期 TDD1 パターンでのスループット理論値 DL:約 1.1Gbps、UL：約 414Mbps
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 ・ 複数ベンダーのコア、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 ・ CU/DU が分離できること

(2) 拠点間ネットワーク

① 複数企業共用パターン

表 3-4-4-2　複数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 CU-DU 区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出来ること

② 業界共用パターン

表 3-4-4-3　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	・ 各システムにおけるデータ通信、および CU～DU 間のデータ通信を可

機能	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、隣接する地方区分およ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) 4K カメラ AI 監視ソリューション

表 3-4-4-4　4K カメラ AI 監視ソリューション機能・性能・要件

システム機能	・ 人侵入検知(人物検知、指定領域侵入検知、アラート通知) ・ 人数カウント(人物検知、性別・年齢推定、マスク着用判定、クラウドで集計情報を可視化) ・ 混雑度推定(人物検知、混雑度推定、クラウドで集計情報を可視化)
性能	(映像伝送) ・ 配信解像度：最大 4K(3840×2160) ・ ビデオ圧縮：H.264 および H.265 に対応
要件	・ 最大 4K の映像配信をルーター等の追加デバイスを介さずに可能であること ・ AI カメラ内で画像解析 AI を動作させ、指定エリア内への人侵入検知や人数カウント、混雑度推定が可能であること ・ AI カメラで解析した結果をクラウド上で可視化できること ・ AI カメラが人侵入を検知した場合、メール等にて予め指定した宛先にアラート通知が配信できること

(4) 8K 高精細映像伝送システム

表 3-4-4-5　8K 高精細映像伝送システム機能・性能・要件

システム機能	・ 8K 高精細カメラによるリアルタイム映像伝送 ・ 映像飛びやブロックノイズなどの映像エラーを極力抑えたスムースな 8K 映像伝送
性能	(8K カメラ・エンコーダ) ・ 映像解像度：8K(7680×4320) ・ ビデオ圧縮：H.265

	（送信クライアントPC） ・　CPU：Intel Core i5-1135G7 ・　メモリ：8GB （デコーダPC） ・　CPU：Intel Core7-11700 ・　GPU：NVIDIA Gforce RTX3070 ・　メモリ：64GB
要件	・　8Kカメラ映像(100Mbps程度)の伝送が可能であること ・　スムースなリアルタイム伝送が実現できること

3.5　免許および各種許認可

無線局の運用に必要となる無線局免許の申請と、免許申請の前提となる干渉調整については、採択後スケジュールに合わせて対応しました。

また今回使用を想定しているローカル５Ｇ無線機器は、技術基準適合証明を取得済みの機器です。なお、一部機器（CDRU-D）は技術基準適合証明を未取得のため、当該機器は暗箱内部でのみの使用とし、本検証で使用する機器は全て登録点検を省略します。

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」に該当し、東日本電信電話株式会社が指定を受けている「999-002」から始まる番号を使用するため、貴省への認定申請は不要です。

4. 相互接続検証

4.1 検証概要

本検証では、異なるベンダー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した。

R3 年度にはコア 1 機種（A 社）、基地局 2 機種（C 社、D 社）、端末 4 機種（A 社、E 社、F 社、G 社）の合計 8 パターンの相互接続試験を実施し、7 パターンで相互接続を実現しました。相互接続を実現するにあたり、3GPP で規定されるパラメータの設定に加えて、以下の改修が必要であることが判明しました。

表 4-1-1　R3 年度異ベンダーの相互接続実現に必要となった改修

項番	改修対象	改修内容
①	A 社製コア	“InitialContextSetupRequest” メッセージ内の当該フィールドを削除
②	A 社製コア	“PDUSessionEstablishmentAccept” メッセージ内へ当該フィールドを追加
③	A 社製コア	“NASSecurityModeCommand” 内の構成を V15.3 以降のシーケンスに対応する措置を実施

本調査研究では、R3 年度に相互接続が実現しなかった 1 パターンにおいて、相互接続が不可となった原因を究明すると共に、新たに B 社製コア、基地局、端末と H 社製端末を加えた 27 パターンの新規相互接続試験を実施しました。また、相互接続が実現したパターンについて、それぞれの通信の性能、品質を評価し、相互接続の組み合わせパターン毎の伝送性能の特性を考察しました。

また、より多くの組み合わせによる相互接続を確認することおよび相互接続実現のために必要な措置の効果を確認するため、参考として R3 年度に相互接続のための改修が多数必要であった A 社製コアと東京大学開発基地局を用いた 6 パターンでの追加検証を実施しました。こちらは、東京大学既設の環境で可能な検証のみを実施いたしました。検証環境による差分が想定されるため、NTT 中央研修センタで実施した組み合わせとの比較は行わないが、検証結果についての考察を「4.4-(3)章　相互接続組み合わせごとのまとめ」に示します。

O-RAN（Open-RAN Alliance）規格の相互接続への影響について、準拠製品と未準拠の製品を用意し、O-RAN 準拠・未準拠による相互接続性について考察しました。

・O-RAN Split Option7.2 準拠：2 機種（B 社、C 社）
・O-RAN 未準拠：2 機種（D 社、東京大学開発基地局）

端末には A 社、B 社、E 社、F 社、G 社、H 社の 6 機種を使用しました。

4.2 検証環境

本調査研究で使用した構成は「図 4-2-1　相互接続検証構成」のとおりです。R4 年度の相互接続の組合せは「表 4-2-1　R4 年度異ベンダーの組合せパターン」、「表 4-2-2　R3 年度異ベンダーの組合せの内、相互接続が実現しなかったパターン」、「表 4-2-3　R3 年度異ベンダーの組合せの内、相互接続が実現したパターン」、「表 4-2-4　東京大学開発基地局を用いたパターン」に記載するとおりです。

本検証の A 社製コアは、「表 4-1-1　R3 年度異ベンダーの相互接続実現に必要となった改修」に記載する改修を施したソフトウェアで実施しました。

また、本検証は「表 4-2-4　東京大学開発基地局を用いたパターン」のみ東京大学で実施し、その他の検証は全て NTT 中央研修センタで実施しました。

基地局と端末間は電界強度による影響を避けるため、遮蔽物の無い見通しの良い場所で検証を行いました。

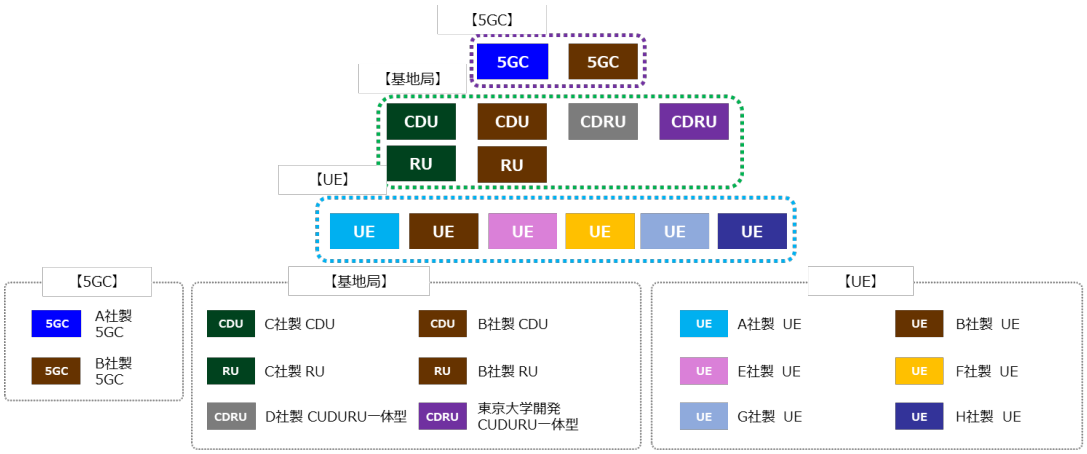


図 4-2-1　相互接続検証構成

表 4-2-1　R4 年度異ベンダーの組合せパターン

パターン No.	コア	基地局	端末
1-1	A 社製	D 社製	B 社製
1-2	A 社製	D 社製	H 社製
1-3	A 社製	C 社製	B 社製
1-4	A 社製	C 社製	H 社製
1-5	A 社製	B 社製	A 社製
1-6	A 社製	B 社製	E 社製
1-7	A 社製	B 社製	G 社製
1-8	A 社製	B 社製	F 社製
1-9	A 社製	B 社製	B 社製
1-10	A 社製	B 社製	H 社製
1-11	B 社製	D 社製	A 社製

1-12	B 社製	D 社製	E 社製
1-13	B 社製	D 社製	G 社製
1-14	B 社製	D 社製	F 社製
1-15	B 社製	D 社製	B 社製
1-16	B 社製	D 社製	H 社製
1-17	B 社製	C 社製	A 社製
1-18	B 社製	C 社製	E 社製
1-19	B 社製	C 社製	G 社製
1-20	B 社製	C 社製	F 社製
1-21	B 社製	C 社製	B 社製
1-22	B 社製	C 社製	H 社製
1-23	B 社製	B 社製	A 社製
1-24	B 社製	B 社製	E 社製
1-25	B 社製	B 社製	G 社製
1-26	B 社製	B 社製	F 社製
1-27	B 社製	B 社製	H 社製

表 4-2-2　R3 年度異ベンダーの組合せの内、相互接続が実現しなかったパターン

パターン No.	コア	基地局	端末
2-1	A 社製	D 社製	A 社製

表 4-2-3　R3 年度異ベンダーの組合せの内、相互接続が実現したパターン

パターン No.	コア	基地局	端末
3-1	A 社製	D 社製	F 社製
3-2	A 社製	D 社製	E 社製
3-3	A 社製	D 社製	G 社製
3-4	A 社製	C 社製	A 社製
3-5	A 社製	C 社製	F 社製
3-6	A 社製	C 社製	E 社製
3-7	A 社製	C 社製	G 社製

表 4-2-4　東京大学開発基地局を用いたパターン

パターン No.	コア	基地局	端末
4-1	A 社製	CDRU-東京大学	A 社製
4-2	A 社製	CDRU-東京大学	E 社製

4-3	A 社製	CDRU-東京大学	G 社製
4-4	A 社製	CDRU-東京大学	F 社製
4-5	A 社製	CDRU-東京大学	B 社製
4-6	A 社製	CDRU-東京大学	H 社製

4.3 検証内容・結果

「表 4-2-1　R4 年度異ベンダーの組合せパターン」、「表 4-2-2　R3 年度異ベンダーの組合せの内、相互接続が実現しなかったパターン」、「表 4-2-3　R3 年度異ベンダーの組合せの内、相互接続が実現したパターン」、「表 4-2-4　東京大学開発基地局を用いたパターン」に記載する各パターンの検証内容・結果を下記のように記載します。

(1) R4 年度異ベンダーの組合せパターン
(2) R3 年度異ベンダーの組合せの内、相互接続が実現しなかったパターン
(3) R3 年度異ベンダーの組合せの内、相互接続が実現したパターン
(4) 東京大学開発基地局を用いたパターン

(1) R4 年度の異ベンダー組み合わせパターン検証

「表 4-2-1」に示した 27 パターンの組み合わせについて相互接続の可否（否の場合、その要因)、通信の品質・性能を検証しました。
本検証の項目は、以下の「表 4-3-1-1　R4 年度異ベンダー組合せパターンの検証内容」のとおりです。以下、以下①～④の検証を順番に実施します。

表 4-3-1-1　R4 年度異ベンダー組合せパターンの検証内容

項番	検証項目	検証内容
①	相互接続検証	コアと基地局、端末をそれぞれ接続し、端末の接続可否を確認
②	相互接続の実現に向けた要因分析	相互接続の結果、正常に端末が接続されなかった組み合わせパターンについて、原因の特定と要因を分析
③	相互接続の実現方策の検討	特定された要因に対して改修を行い、相互接続を実現
④	通信の評価・考察	相互接続が実現した組み合わせパターンについて、通信の品質や性能を確認

①　相互接続検証

「表 4-2-1　R4 年度異ベンダーの組合せパターン」に記載する 27 パターンについて、相互接続の可否を検証しました。
本検証は、3GPP で規定されるパラメータの設定に加えて、A 社製コアは「表 4-1-1　R3 年度異ベンダーの相互接続実現に必要となった改修」に記載する改修を施したソフトウェ

アで実施しました。また、B 社製コアに特別な改修は行っていません。

本項目の検証結果は「表 4-3-1-2　R4 年度異ベンダーの組合せパターンの相互接続結果」のようにまとめました。

表 4-3-1-2　R4 年度異ベンダーの組合せパターンの相互接続結果

パターン No.	コア	基地局	端末	接続可否
1-1	A 社製	D 社製	B 社製	○
1-2	A 社製	D 社製	H 社製	○
1-3	A 社製	C 社製	B 社製	○
1-4	A 社製	C 社製	H 社製	○
1-5	A 社製	B 社製	A 社製	×
1-6	A 社製	B 社製	E 社製	○
1-7	A 社製	B 社製	G 社製	○
1-8	A 社製	B 社製	F 社製	○
1-9	A 社製	B 社製	B 社製	○
1-10	A 社製	B 社製	H 社製	○
1-11	B 社製	D 社製	A 社製	○
1-12	B 社製	D 社製	E 社製	○
1-13	B 社製	D 社製	G 社製	○
1-14	B 社製	D 社製	F 社製	○
1-15	B 社製	D 社製	B 社製	○
1-16	B 社製	D 社製	H 社製	○
1-17	B 社製	C 社製	A 社製	○
1-18	B 社製	C 社製	E 社製	○
1-19	B 社製	C 社製	G 社製	○
1-20	B 社製	C 社製	F 社製	○
1-21	B 社製	C 社製	B 社製	○
1-22	B 社製	C 社製	H 社製	○
1-23	B 社製	B 社製	A 社製	×
1-24	B 社製	B 社製	E 社製	○
1-25	B 社製	B 社製	G 社製	○
1-26	B 社製	B 社製	F 社製	○
1-27	B 社製	B 社製	H 社製	○

②　相互接続の実現に向けた要因分析

相互接続検証の結果、正常に接続できなかったパターン 1-5, 1-23 について、原因の特定と要因分析をしました。

要因分析は以下のデータを用いて行いました。

・コア、基地局、端末でのログ
・コア、基地局、端末、中継となるネットワーク機器でのパケットキャプチャーの結果

本項目の検証結果は「表 4-3-1-3　エラー事象、要因分析」にまとめました。本項目の検証結果に対する分析については、「4.4-(1)章 相互接続に関連する項目、パラメータ」で示します。

表 4-3-1-3　エラー事象、要因分析

パターン No.	エラー事象	検知箇所	分析結果	対処方法
1-5、1-23	SIM の認証失敗により、端末の５Ｇ通信が疎通不可	端末の GUI 画面において、認証未完了が表示	基地局からコアへ送付される認証用通信の伝送失敗（フラグメント処理に異常が発生）	基地局の MTU サイズを適切な値に設定

③　相互接続の実現方策の検討

「表 4-3-1-3　エラー事象、要因分析、改善結果イメージ」で得られた要因分析結果を元に、相互接続が不可となる要因に改修を施しました。

本項目の検証結果は「表 4-3-1-4　改修後の相互接続可否」にまとめました。本項目の検証結果に対する分析については、「4.4-(1)章」で示します。

表 4-3-1-4　改修後の相互接続可否

パターン No.	改修対象	改修内容	対象機器	接続可否
1-5、1-23	基地局装置の MTU 値	基地局装置の MTU 値を 1500(default)から 1300 に設定	B 社製基地局	認証用通信が疎通し、接続成功

④　通信の評価

「表 4-3-1-1　R4 年度異ベンダー組合せパターンの検証内容」に記載する①～③の検証実施により表 4-3-1-2 の全ての組み合わせパターンで相互接続が実現しました。その上で、全ての組み合わせパターンに対して、「表 4-3-1-5 通信の評価項目・確認方法」の検証を実施しました。

表 4-3-1-5　通信の評価項目・確認方法

大項目	評価項目	確認方法
接続断後、再接続時の挙動	電源 ON/OFF 動作時の挙動確認	基地局（CU／DU／RU）および端末の電源をそれぞれ ON/OFF させ、再度起動した際、コアや端末と正常に接続できることを確認する。
	電波 ON/OFF 動作時の挙動確認	停波後、発波させた際、コアや端末と正常に接続できることを確認する。
認証時間	認証時間の確認	Wireshark を用いて、端末の SIM 認証開始から認証完了までの時間を確認する。
長期安定性	長期安定試験	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、48 時間の疎通試験上異常が無いことを確認する。
遅延	遅延の確認	端末からセンタ UPF へ ping 疎通試験を実施し、遅延時間を確認する。
通信品質	通信性能の確認	iperf による伝送スループット試験を実施し、性能差分を評価する。
	準同期の動作確認	準同期 TDD1/2/3 それぞれのパターンにおいて正常に接続できること確認し、性能差分を評価する。

（ア）　接続断後、再接続時の挙動

組み合わせパターン毎に基地局(CU/DU/RU)および端末の電源をそれぞれ ON/OFF させ、再度起動する検証と、組み合わせパターン毎に停波、発波を実施し、コアと端末と接続する検証を行いました。結果は「表 4-3-1-6　R4 年度異ベンダーの組合せパターンごとの電源 ON/OFF、機内モード ON/OFF 時の挙動結果」にまとめ、全ての組み合わせにおいて、相互接続の挙動に問題の無いことを確認いたしました。

表 4-3-1-6　R4 年度異ベンダーの組合せパターンごとの電源 ON/OFF、機内モード ON/OFF 時の挙動結果

パターン No.	コア	基地局	端末	電源 ON/OFF 時の正常接続		機内モード ON/OFF 時の正常接続
				基地局	端末	
1-1	A 社製	D 社製	B 社製	○	○	○
1-2	A 社製	D 社製	H 社製	○	○	－
1-3	A 社製	C 社製	B 社製	○	○	○
1-4	A 社製	C 社製	H 社製	○	○	－
1-5	A 社製	B 社製	A 社製	○	○	○
1-6	A 社製	B 社製	E 社製	○	○	○

1-7	A 社製	B 社製	G 社製	○	○	○
1-8	A 社製	B 社製	F 社製	○	○	○
1-9	A 社製	B 社製	B 社製	○	○	○
1-10	A 社製	B 社製	H 社製	○	○	―
1-11	B 社製	D 社製	A 社製	○	○	○
1-12	B 社製	D 社製	E 社製	○	○	○
1-13	B 社製	D 社製	G 社製	○	○	○
1-14	B 社製	D 社製	F 社製	○	○	○
1-15	B 社製	D 社製	B 社製	○	○	○
1-16	B 社製	D 社製	H 社製	○	○	―
1-17	B 社製	C 社製	A 社製	○	○	○
1-18	B 社製	C 社製	E 社製	○	○	○
1-19	B 社製	C 社製	G 社製	○	○	○
1-20	B 社製	C 社製	F 社製	○	○	○
1-21	B 社製	C 社製	B 社製	○	○	○
1-22	B 社製	C 社製	H 社製	○	○	―
1-23	B 社製	B 社製	A 社製	○	○	○
1-24	B 社製	B 社製	E 社製	○	○	○
1-25	B 社製	B 社製	G 社製	○	○	○
1-26	B 社製	B 社製	F 社製	○	○	○
1-27	B 社製	B 社製	H 社製	○	○	―

○：正常接続　×：接続不可

※―(ハイフン)と記載しているパターンは端末(H 社製)に機内モードが実装されていないため検証していない項目となります。

(イ) 認証時間

組み合わせパターン毎に端末の認証に要する時間を計測しました。

結果は「表 4-3-1-7　R4 年度異ベンダーの組合せパターンごとの認証時間の結果」にまとめました。

表 4-3-1-7　R4 年度異ベンダーの組合せパターンごとの認証時間の結果

パターン No.	コア	基地局	端末	認証時間 [s]
1-1	A 社製	D 社製	B 社製	2.83
1-2	A 社製	D 社製	H 社製	1.95
1-3	A 社製	C 社製	B 社製	1.26
1-4	A 社製	C 社製	H 社製	3.75
1-5	A 社製	B 社製	A 社製	40.20

1-6	A 社製	B 社製	E 社製	3.33
1-7	A 社製	B 社製	G 社製	1.63
1-8	A 社製	B 社製	F 社製	1.12
1-9	A 社製	B 社製	B 社製	2.48
1-10	A 社製	B 社製	H 社製	2.24
1-11	B 社製	D 社製	A 社製	40.28
1-12	B 社製	D 社製	E 社製	1.96
1-13	B 社製	D 社製	G 社製	1.67
1-14	B 社製	D 社製	F 社製	1.38
1-15	B 社製	D 社製	B 社製	1.41
1-16	B 社製	D 社製	H 社製	2.05
1-17	B 社製	C 社製	A 社製	40.08
1-18	B 社製	C 社製	E 社製	3.33
1-19	B 社製	C 社製	G 社製	1.40
1-20	B 社製	C 社製	F 社製	1.07
1-21	B 社製	C 社製	B 社製	1.46
1-22	B 社製	C 社製	H 社製	2.07
1-23	B 社製	B 社製	A 社製	40.59
1-24	B 社製	B 社製	E 社製	2.00
1-25	B 社製	B 社製	G 社製	1.87
1-26	B 社製	B 社製	F 社製	1.37
1-27	B 社製	B 社製	H 社製	2.32

（ウ） 長期安定性

組み合わせパターン毎に端末からセンタ UPF へ 48 時間の ping 疎通試験を行い通信の成功率を計測しました。

結果は「表 4-3-1-8　R4 年度異ベンダーの組合せパターンごとの長期安定試験の結果」にまとめました。

表 4-3-1-8　R4 年度異ベンダーの組合せパターンごとの長期安定試験の結果

パターン No.	コア	基地局	端末	疎通率 [%]	判定
1-1	A 社製	D 社製	B 社製	100	○
1-2	A 社製	D 社製	H 社製	99.0	○
1-3	A 社製	C 社製	B 社製	97.7	○
1-4	A 社製	C 社製	H 社製	99.0	○
1-5	A 社製	B 社製	A 社製	99.1	○
1-6	A 社製	B 社製	E 社製	99.9	○

1-7	A 社製	B 社製	G 社製	99.9	○
1-8	A 社製	B 社製	F 社製	99.9	○
1-9	A 社製	B 社製	B 社製	99.9	○
1-10	A 社製	B 社製	H 社製	99.9	○
1-11	B 社製	D 社製	A 社製	99.9	○
1-12	B 社製	D 社製	E 社製	99.0	○
1-13	B 社製	D 社製	G 社製	100	○
1-14	B 社製	D 社製	F 社製	100	○
1-15	B 社製	D 社製	B 社製	100	○
1-16	B 社製	D 社製	H 社製	100	○
1-17	B 社製	C 社製	A 社製	100	○
1-18	B 社製	C 社製	E 社製	99.2	○
1-19	B 社製	C 社製	G 社製	99.1	○
1-20	B 社製	C 社製	F 社製	97.6	○
1-21	B 社製	C 社製	B 社製	100.0	○
1-22	B 社製	C 社製	H 社製	99.6	○
1-23	B 社製	B 社製	A 社製	99.9	○
1-24	B 社製	B 社製	E 社製	99.7	○
1-25	B 社製	B 社製	G 社製	99.7	○
1-26	B 社製	B 社製	F 社製	99.8	○
1-27	B 社製	B 社製	H 社製	99.7	○

○：疎通率≧90%　×：疎通率＜90%

（エ） 遅延

組み合わせパターン毎に、各 TDD パターンにおいて端末からセンタ UPF へ ping を送付し遅延の測定を行いました。結果は「表 4-3-1-9　R4 年度異ベンダーの組合せパターンごとの遅延の測定結果」にまとめました。

表 4-3-1-9　R4 年度異ベンダーの組合せパターンごとの遅延の測定結果

パターン No.	コア	基地局	端末	同期 [s]	準同期 TDD1 [s]	準同期 TDD2 [s]	準同期 TDD3 [s]
1-1	A 社製	D 社製	B 社製	40	32	30	30
1-2	A 社製	D 社製	H 社製	32	26	31	26
1-3	A 社製	C 社製	B 社製	34	36	37	－
1-4	A 社製	C 社製	H 社製	31	32	31	－
1-5	A 社製	B 社製	A 社製	54	42	43	38
1-6	A 社製	B 社製	E 社製	58	64	49	43

1-7	A 社製	B 社製	G 社製	87	46	61	49
1-8	A 社製	B 社製	F 社製	42	45	61	46
1-9	A 社製	B 社製	B 社製	35	45	43	33
1-10	A 社製	B 社製	H 社製	38	40	42	43
1-11	B 社製	D 社製	A 社製	30	26	26	27
1-12	B 社製	D 社製	E 社製	25	26	27	28
1-13	B 社製	D 社製	G 社製	29	29	35	32
1-14	B 社製	D 社製	F 社製	33	28	30	28
1-15	B 社製	D 社製	B 社製	26	27	26	28
1-16	B 社製	D 社製	H 社製	23	26	24	26
1-17	B 社製	C 社製	A 社製	36	40	32	―
1-18	B 社製	C 社製	E 社製	35	39	34	―
1-19	B 社製	C 社製	G 社製	34	36	38	―
1-20	B 社製	C 社製	F 社製	35	35	36	―
1-21	B 社製	C 社製	B 社製	35	35	36	―
1-22	B 社製	C 社製	H 社製	29	32	38	―
1-23	B 社製	B 社製	A 社製	45	38	43	41
1-24	B 社製	B 社製	E 社製	49	43	43	56
1-25	B 社製	B 社製	G 社製	45	46	41	46
1-26	B 社製	B 社製	F 社製	44	49	48	45
1-27	B 社製	B 社製	H 社製	42	42	41	40

※―(ハイフン)と記載しているパターンは基地局(C 社製)に TDD3 が実装されていないため測定していない項目となります。

(オ) 通信性能

組み合わせパターン毎に通信性能を確認する試験を行いました。端末からセンタ UPF へ iperf を実施し、TDD パターンごとに DL/UL のスループットを測定しました。結果は「表 4-3-1-10　R4 年度異ベンダーの組合せパターンごとの性能試験の結果」にまとめました。

表 4-3-1-10　R4 年度異ベンダーの組合せパターンごとの性能試験の結果

パターン No.	同期		準同期 TDD1		準同期 TDD2		準同期 TDD3	
	DL [Mbps]	UL [Mbps]	DL [Mbps]	UL [Mbps]	DL [Mbps]	UL [Mbps]	DL [Mbps]	UL [Mbps]
1-1	309(674)	84.3	314(484)	128	250	133	163	223
1-2	305	65.8	241	115	228	131	185	219
1-3	314(476)	51.0	240	99.3	172	128	―	―
1-4	451	50.9	275	103	125	130	―	―
1-5	691	67.1	585	110	431	140	135	190

1-6	317(787)	57.5	317(644)	106	317(459)	143	134	189
1-7	686	42.7	462	90.7	403	152	135	184
1-8	661	60.7	516	110	423	130	132	166
1-9	310(768)	59.4	305(524)	115	312(452)	135	133	157
1-10	666	60.9	497	133	390	163	139	2.91
1-11	608	86.7	409	174	240	201	188	244
1-12	317(641)	75.8	314(428)	123	142	200	137	165
1-13	606	79.1	426	119	208	178	178	233
1-14	695	94	494	144	250	168	168	254
1-15	313(714)	76.8	307(450)	137	149	140	137	161
1-16	325	76.3	247	153	226	157	190	239
1-17	447	50.5	234	102	171	126	―	―
1-18	315(460)	49.6	239	103	162	126	―	―
1-19	379	50.6	222	103	166	129	―	―
1-20	455	51.0	225	102	159	128	―	―
1-21	315(435)	50.9	236	103	172	129	―	―
1-22	434	50.7	276	102	128	129	―	―
1-23	691	53.1	546	117	416	144	306	177
1-24	301(787)	58.1	317(608)	106	317(443)	136	210	149
1-25	598	54.9	590	99.3	432	128	297	150
1-26	682	53.1	553	111	425	138	304	171
1-27	678	67.7	493	136	398	142	313	3.38

※括弧書きの数値は基地局の通信ログから計測した伝送量になります。
B 社、E 社の端末については、テザリング機能を用いてスループットの計測を実施したため、USB2.0 の実行値 310Mbps 程度がスループットの上限となっています。代わりに基地局での通信ログを用いて伝送量を計測しました。

※―(ハイフン)と記載しているパターンは基地局(C 社製)に TDD3 が実装されていないため測定していない項目となります。

(2) R3 年度に相互接続が実現しなかったパターンの検証

「表 4-3-2-1 R3 年度異ベンダーの組合せパターンの相互接続結果」のとおり、R3 年度に実施した相互接続検証では、1 パターンで相互接続が不可となりました。本調査研究では、相互接続が不可となったパターン No.2-1 の要因を分析し改善措置を施すことで相互接続を実現し、通信の品質・性能を検証しました。

本検証の項目は、「表 4-3-2-2　R3 年度に相互接続が実現しなかったパターンの検証項目」のとおりです。以下、以下①～③の検証を順番に実施します。

表 4-3-2-1　R3 年度異ベンダーの組合せパターンの相互接続結果

パターン No.	コア	基地局	端末	接続可否
2-1	A 社製	D 社製	A 社製	×
3-1	A 社製	D 社製	F 社製	○
3-2	A 社製	D 社製	E 社製	○
3-3	A 社製	D 社製	G 社製	○
3-4	A 社製	C 社製	A 社製	○
3-5	A 社製	C 社製	F 社製	○
3-6	A 社製	C 社製	E 社製	○
3-7	A 社製	C 社製	G 社製	○

表 4-3-2-2　R3 年度に相互接続が実現しなかったパターンの検証項目

項目	検証内容	詳細
①	相互接続の実現に向けた要因分析	相互接続の結果、正常に端末が接続されなかった組み合わせパターンについて、原因の特定と要因を分析しました。
②	相互接続の実現方策の検討	特定された要因に対して改修を行い、相互接続を実現しました。
③	通信の評価・考察	相互接続が実現した組み合わせパターンについて、通信の品質や性能を確認しました。

①　相互接続の実現に向けた要因分析

「表 4-2-2　R3 年度異ベンダーの組合せの内、相互接続が実現しなかったパターン」に記載する 1 パターンについて、原因の特定と要因の分析をしました。

本項目の検証結果は「表 4-3-2-3　エラー事象、要因分析」のようにまとめました。本項目の検証結果に対する分析については、「4.4-(1)章 相互接続に関する項目、パラメータ」で示します。

表 4-3-2-3　エラー事象、要因分析

パターン No.	エラー事象	検知箇所	分析結果	対処方法
2-1	SIM の認証失敗により、端末の５G通信が疎通不可	端末の GUI 画面において、認証未完了が表示	基地局からコアへ送付される認証用通信の伝送失敗（フラグメント処理に異常が発生）	基地局の MTU サイズを適切な値に設定

②　相互接続の実現方策の検討

本項目では「表 4-3-2-3　エラー事象、要因分析」で得られた要因分析結果を元に、相互接続が不可となる要因の改修を行いました。

本項目の検証結果は「表 4-3-2-4　改修後の相互接続可否」にまとめました。本検証結果に対する分析については、「4.4-(1)章」で示します。

表 4-3-2-4　改修後の相互接続可否

パターン No.	改修対象	改修内容	対象機器	接続可否
2-1	基地局装置の MTU 値	基地局装置の MTU 値を 1500(default)から 1300 に設定	D 社製基地局	認証用通信が疎通し、接続成功

③　通信の評価

①～②の実施により相互接続が実現した組み合わせパターンに対して、「表 4-3-1-5　通信の評価項目・確認方法」の検証を実施しました。

（ア）　接続断後、再接続時の挙動

基地局(CDRU)および端末の電源を ON/OFF させ、再度起動する検証と電波の停波、発波を実施し、コアと端末と接続する検証を行いました。

結果は「表 4-3-2-5　R3 年度に相互接続が実現しなかったパターンの電源 ON/OFF、機内モード ON/OFF 時の挙動結果」にまとめました。

表 4-3-2-5　R3 年度に相互接続が実現しなかったパターンの電源 ON/OFF、機内モード ON/OFF 時の挙動結果

パターン No.	コア	基地局	端末	電源 ON/OFF 時の正常接続		機内モード ON/OFF 時の正常接続
				基地局	端末	
2-1	A 社製	D 社製	A 社製	○	○	○

（イ） 認証時間

端末の認証にかかる時間を測定する検証を行いました。
結果は「表 4-3-2-6　R3 年度に相互接続が実現しなかったパターンの認証時間の結果」にまとめました。

表 4-3-2-6　R3 年度に相互接続が実現しなかったパターンの認証時間の結果

パターン No.	コア	基地局	端末	認証時間 [sec]
2-1	A 社製	D 社製	A 社製	40.04

（ウ） 長期安定性

端末からセンタ UPF へ 48 時間の ping 疎通試験を行い通信の成功率を計測しました。結果は「表 4-3-2-7　R3 年度に相互接続が実現しなかったパターンの長期安定試験の結果」にまとめました。

表 4-3-2-7　R3 年度に相互接続が実現しなかったパターンの長期安定試験の結果

パターン No.	コア	基地局	端末	疎通率 [%]	判定
2-1	A 社製	D 社製	A 社製	100	○

○：疎通率≧90%　×：疎通率＜90%

（エ）遅延

各 TDD パターンにおいて端末からセンタ UPF へ ping を送付し遅延の測定を行いました。結果は「表 4-3-2-8　R3 年度に相互接続が実現しなかったパターンの遅延の測定結果」にまとめました。

表 4-3-2-8　R3 年度に相互接続が実現しなかったパターンの遅延の測定結果

パターン No.	コア	基地局	端末	同期 [ms]	準同期 TDD1 [ms]	準同期 TDD2 [ms]	準同期 TDD3 [ms]
2-1	A 社製	D 社製	A 社製	26	27	28	26

（オ）通信性能

通信性能を確認する試験を行いました。
結果は「表 4-3-2-9　R3 年度に相互接続が実現しなかったパターンごとの性能試験の結果」にまとめました。

表 4-3-2-9　R3 年度に相互接続が実現しなかったパターンの性能試験の結果

パターン No.	同期		準同期 TDD1		準同期 TDD2		準同期 TDD3	
	DL [Mbps]	UL [Mbps]	DL [Mbps]	UL [Mbps]	DL [Mbps]	DL [Mbps]	UL [Mbps]	DL [Mbps]
2-1	652	61.8	402	142	201	181	152	241

(3) R3 年度に相互接続が実現したパターンの検証

「表 4-2-3」に示した R3 年度に相互接続が実現した組み合わせ 7 パターンについて、新たに準同期 TDD2、TDD3 の性能を検証しました。

本検証の項目は、「表 4-3-3-1　R3 年度に相互接続が実現した組み合わせパターンの検証項目」のとおりです。

表 4-3-3-1　R3 年度に相互接続が実現した組み合わせパターンの検証項目

項目	検証内容	詳細
①	通信の評価・考察	新しく追加された TDD パターンについて、通信の性能を確認しました。

① 通信の評価

「表 4-2-3　R3 年度異ベンダーの組合せの内、相互接続が実現したパターン」に記載する 7 パターンについて、「表 4-3-3-2 通信の評価項目・確認方法」の検証を実施しました。

表 4-3-3-2　通信性能の評価項目・確認方法

大項目	評価項目	確認方法
遅延	遅延の確認	端末からセンタ UPF へ ping による疎通試験を実施し、遅延時間を確認する。
通信性能	通信性能の確認	iperf による伝送スループット試験を実施し、性能差分を評価する。
	準同期の動作確認	準同期 TDD2/3 それぞれのパターンにおいて正常に接続できること確認し、性能差分を評価する。

（ア）遅延

各 TDD パターンにおいて端末からセンタ UPF へ ping を送付し遅延の測定を行いました。結果は「表 4-3-3-3　R3 年度の異ベンダーの組合せの内、相互接続が実現したパター

ンごとの遅延の測定結果」にまとめました。

表 4-3-3-3　R3 年度の異ベンダーの組合せの内、相互接続が実現したパターンごとの遅延の測定結果

パターン No.	コア	基地局	端末	同期 [ms]	準同期 TDD1 [ms]	準同期 TDD2 [ms]	準同期 TDD3 [ms]
3-1	A 社製	D 社製	F 社製	32 ※2	28 ※2	34	31
3-2	A 社製	D 社製	E 社製	30 ※2	29 ※2	31	34
3-3	A 社製	D 社製	G 社製	27 ※2	30 ※2	34	35
3-4	A 社製	C 社製	A 社製	35 ※2	36 ※2	33	―
3-5	A 社製	C 社製	F 社製	40 ※2	36 ※2	36	―
3-6	A 社製	C 社製	E 社製	39 ※2	40 ※2	35	―
3-7	A 社製	C 社製	G 社製	39 ※2	40 ※2	43	―

※1　―(ハイフン)と記載しているパターンは基地局(C 社製)に TDD3 が実装されていないため測定していない項目となります。

※2　同期、準同期 TDD1 の結果は R3 年度に測定したものを掲載しております。R4 年度に用いた R3 年度と同ベンダーの製品については、製品の性能向上に係るファームアップを実施しております。

（イ）　通信性能

組み合わせパターン毎に通信性能の確認試験を行いました。

結果は「表 4-3-3-4　R3 年度に相互接続が実現したパターンごとの性能試験の結果」にまとめました。

表 4-3-3-4　R3 年度に相互接続が実現したパターンごとの性能試験の結果

パターン No.	同期		準同期 TDD1		準同期 TDD2		準同期 TDD3	
	DL [Mbps]	UL [Mbps]	DL [Mbps]	UL [Mbps]	DL [Mbps]	DL [Mbps]	UL [Mbps]	DL [Mbps]
3-1	300※2	65※2	200※2	150※2	279	132	150	244
3-2	180※2	77※2	180※2	135※2	249	159	162	233
3-3	250※2	30※2	280※2	80※2	227	130	182	219
3-4	300※2	28※2	170※2	60※2	152	129	―	―
3-5	200※2	28※2	100※2	58※2	168	120	―	―
3-6	150※2	30※2	150※2	60※2	172	126	―	―
3-7	250※2	30※2	115※2	60※2	206	128	―	―

※1　―(ハイフン)と記載しているパターンは基地局(C 社製)に TDD3 が実装されていないため測定していない項目となります。

※2　同期、準同期 TDD1 の結果は R3 年度に測定したものを掲載しております。R4 年度は R3 年度と同様の製品も用いていますが、製品の性能向上に係るファームアップ等を適用しております。

表 4-3-2-9　R3 年度に相互接続が実現しなかったパターンの性能試験の結果

パターン No.	同期		準同期 TDD1		準同期 TDD2		準同期 TDD3	
	DL [Mbps]	UL [Mbps]	DL [Mbps]	UL [Mbps]	DL [Mbps]	DL [Mbps]	UL [Mbps]	DL [Mbps]
2-1	652	61.8	402	142	201	181	152	241

(4) 東京大学開発基地局を用いたパターン

より多くの組み合わせによる相互接続を確認することおよび相互接続実現のために必要な措置の正確性を確認するため、参考として R3 年度に相互接続のための改修が多数必要であった A 社製コアと東京大学開発の基地局を用いて相互接続の可否とその要因、通信の品質・性能を検証しました。

本検証の項目は、「表 4-3-4-1　東京大学様の新型基地局を用いたパターンの検証項目」のとおりです。以下、以下①～④の検証を順番に実施しました。

表 4-3-4-1　東京大学様の新型基地局を用いたパターンの検証項目

項目	検証内容	詳細
①	相互接続検証	コアと基地局、端末をそれぞれ接続し、端末の接続可否を確認しました
②	相互接続の実現に向けた要因分析	相互接続の結果、正常に端末が接続されなかった組み合わせパターンについて、原因の特定と要因を分析しました。
③	相互接続の実現方策の検討	特定された要因に対して改修を行い、相互接続を実現しました。
④	通信の評価・考察	相互接続が実現した組み合わせパターンについて、通信の品質や性能を確認しました。

①　相互接続検証

「表 4-2-4　東京大学開発基地局を用いたパターン」に記載する 6 パターンについて、相互接続の可否を検証しました。

本検証は、3GPP で規定されるパラメータの設定に加えて、A 社製コアは「表 4-1-1　R3 年度異ベンダーの相互接続実現に必要となった改修」に記載する改修を施したソフトウェアで実施しました。

本項目の検証結果は「表 4-3-4-2　東京大学開発基地局を用いたパターンの相互接続結果」のようにまとめました。

表 4-3-4-2　東京大学開発基地局を用いたパターンの相互接続結果

パターン No.	コア	基地局	端末	接続可否
4-1	A 社製	CDRU-東京大学	A 社製	○
4-2	A 社製	CDRU-東京大学	E 社製	○
4-3	A 社製	CDRU-東京大学	G 社製	○
4-4	A 社製	CDRU-東京大学	F 社製	○
4-5	A 社製	CDRU-東京大学	B 社製	○
4-6	A 社製	CDRU-東京大学	H 社製	○

②　相互接続の実現に向けた要因分析

「表 4-2-4　東京大学開発基地局を用いたパターン」では、全ての組み合わせで相互接続に成功したため、相互接続の実現に向けた要因分析は実施しませんでした。

③　相互接続の実現方策

「表 4-2-4　東京大学開発基地局を用いたパターン」では、全ての組み合わせで相互接続に成功したため、相互接続の実現方策の検討は実施しませんでした。

④　通信の評価

相互接続が実現した組み合わせに対して、「表 4-3-4-3 通信の評価項目・確認方法」の検証を実施しました。

表 4-3-4-3 通信の評価項目・確認方法

大項目	評価項目	確認方法
接続断後、再接続時の挙動	電源 ON/OFF 動作時の挙動確認	基地局（CU／DU／RU）および端末の電源をそれぞれ ON/OFF させ、再度起動した際、コアや端末と正常に接続できることを確認する。
	電波 ON/OFF 動作時の挙動確認	停波後、発波させた際、コアや端末と正常に接続できることを確認する。
遅延	遅延の確認	端末からセンタ UPF へ ping による疎通試験を実施し、遅延時間を確認する。
通信性能	通信性能の確認	iperf による伝送スループット試験を実施し、性能差分を評価する。
	準同期の動作確認	準同期 TDD1/3 それぞれのパターンにおいて正常に接続できること確認し、性能差分を評価する。

※東京大学既設の環境で実施可能な検証のみを行いました。

（ア） 接続断後、再接続時の挙動

組み合わせパターン毎に基地局(CDRU)の電源をそれぞれ ON/OFF させ、再度起動する検証と停波、発波を実施し、コアと端末と接続する検証を行いました。

結果は「表 4-3-4-4　東京大学開発基地局を用いたパターンごとの電源 ON/OFF、機内モード ON/OFF 時の挙動結果」にまとめ、全ての組み合わせにおいて、相互接続に問題の無いことを確認いたしました

表 4-3-4-4　東京大学開発基地局を用いたパターンごとの電源 ON/OFF、機内モード ON/OFF 時の挙動結果

パターン No.	コア	基地局	端末	電源 ON/OFF 時の挙動		機内モード ON/OFF 時の挙動
				基地局	端末	
4-1	A 社製	CDRU-東京大学	A 社製	○	○	○
4-2	A 社製	CDRU-東京大学	E 社製	○	○	○
4-3	A 社製	CDRU-東京大学	G 社製	○	○	○
4-4	A 社製	CDRU-東京大学	F 社製	○	○	○
4-5	A 社製	CDRU-東京大学	B 社製	○	○	○
4-6	A 社製	CDRU-東京大学	H 社製	○	○	―

※―(ハイフン)と記載しているパターンは端末(H 社製)に機内モードが実装されていないため検証していない項目となります。

（イ） 遅延

組み合わせパターン毎に遅延の測定を行いました。

結果は「表 4-3-4-5　東京大学開発基地局を用いたパターンごとの遅延の測定結果」にまとめました。

表 4-3-4-5　東京大学開発基地局を用いたパターンごとの遅延の測定結果

パターン No.	コア	基地局	端末	同期 [ms]	準同期 TDD1 [ms]	準同期 TDD3 [ms]
4-1	A 社製	CDRU-東京大学	A 社製	25	26	30
4-2	A 社製	CDRU-東京大学	E 社製	27	29	32

4-3	A 社製	CDRU-東京大学	G 社製	33	32	31
4-4	A 社製	CDRU-東京大学	F 社製	29	29	29
4-5	A 社製	CDRU-東京大学	B 社製	26	26	32
4-6	A 社製	CDRU-東京大学	H 社製	29	26	27

（ウ） 通信性能

組み合わせパターン毎に通信性能を確認する試験を行いました。
結果は「表 4-3-4-6　東京大学様の新型基地局を用いたパターンごとの性能」にまとめました。

表 4-3-4-6　東京大学様の新型基地局を用いたパターンごとの性能

パターン No.	同期		準同期 TDD1		準同期 TDD3	
	DL [Mbps]	UL [Mbps]	DL [Mbps]	UL [Mbps]	DL [Mbps]	UL [Mbps]
4-1	517	59.8	497	91.2	285	159
4-2	317	58.3	317	130	277	176
4-3	688	47.8	470	113	276	144
4-4	682	34.9	489	100	278	163
4-5	314	50.4	310	124	287	166
4-6	491	54.1	391	103	277	156

4.4　相互接続の検証結果のまとめ

本章は、コア、基地局、端末の相互接続実現に向けた検証結果についてまとめ、考察したものです。

※本調査研究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、今後実際に利用する場合は本検証と異なった結果になる可能性があります。

(1) 相互接続に関連する項目、パラメータ

相互接続の実現に向けて、コア、基地局、端末のパラメータを合わせる必要があります。3GPP に規定される相互接続のために設定が必要なパラメータは、「表 4-4-1-1　コア-基地局間の相互接続に関係するパラメータ」、「表 4-4-1-2　コア-端末間の相互接続に関係するパラメータ」のとおりです。

表 4-4-1-1　コア-基地局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 4-4-1-2　コア-端末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

加えて、R3 年度の調査研究から、3GPP の規定上明確な指定が無いにも関わらず、実際は相互接続のために改修が必要な項目が 3 点発見されました。

表 4-4-1-3　R3 年度異ベンダーの相互接続実現に必要となった改修

項番	改修対象	改修内容
①	A 社製コア	“InitialContextSetupRequest” メッセージ内の当該フィールドを削除
②	A 社製コア	“PDUSessionEstablishmentAccept” メッセージ内へ当該フィールドを追加
③	A 社製コア	“NASSecurityModeCommand” 内の構成を V15.3 以降のシーケンスに対応する措置を実施

本調査研究では、上記パラメータを設定し、A 社製コアに改修を施した上で相互接続検証を行いました。B 社製コアでは上記パラメータによるエラーは発生しなかったため特に改修は行っていません。これらパラメータはベンダーによる自由な実装が可能な箇所であり、B 社製コアについては最初からこれらの内容が満たされていたものと考えられます。

結果として、「表 4-2-2　R3 年度異ベンダーの組合せの内、相互接続が実現しなかったパターン」に記載の 1 パターンと、「表 4-3-1-2　　R4 年度異ベンダーの組合せパターンの相互接続結果」に記載の 2 パターンで、端末の接続が不可となりました。

・相互接続検証において、端末の接続が不可となった組み合わせ
1-5　コア：A 社製／基地局：B 社製／端末：A 社製
1-23　コア：B 社製／基地局：B 社製／端末：A 社製
2-1　コア：A 社製／基地局：D 社製／端末：A 社製

解析を行い、これらのパターンで相互接続が不可となった原因のパラメータについてまとめました。

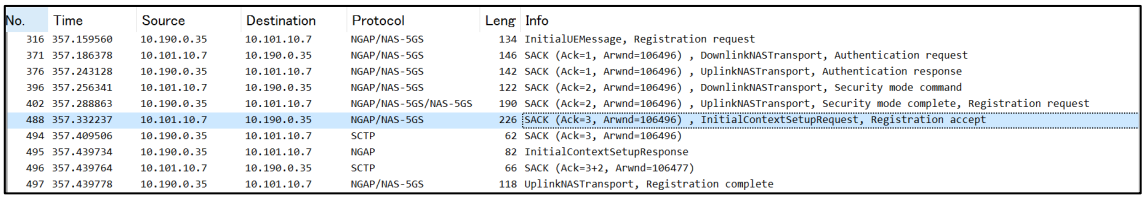
①　MTU(Maximum Transmission Unit)の設定

調査の結果、相互接続が実現しなかった 3 パターンにおいて、MTU の設定が不適切であることにより、SIM の認証のための通信が一部疎通できず、端末の接続ができない状態となっていたことが判明いたしました。

以下の「図 4-4-1-4　R3 年度に相互接続が実現したパターンのパケットキャプチャー」と「図 4-4-1-5　R3 年度に相互接続が実現しなかったパターンのパケットキャプチャー」で、相互接続が実現したパターンとしなかったパターンの認証のための通信を比較いたしました。

No.	Time	Source	Destination	Protocol	Leng	Info
1	0.000000	10.190.0.34	10.101.10.7	NGAP/NAS-5GS/NAS-…	190	InitialUEMessage, Registration request, Registration request
2	0.004631	10.101.10.7	10.190.0.34	NGAP/NAS-5GS	106	SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request
3	0.039126	10.190.0.34	10.101.10.7	NGAP/NAS-5GS	146	SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response
4	0.056928	10.101.10.7	10.190.0.34	NGAP/NAS-5GS	146	SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request
5	0.119257	10.190.0.34	10.101.10.7	NGAP/NAS-5GS	150	SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response
6	0.128020	10.101.10.7	10.190.0.34	NGAP/NAS-5GS	122	SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command
7	0.159171	10.190.0.34	10.101.10.7	NGAP/NAS-5GS/NAS-…	194	SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request
8	0.185770	10.101.10.7	10.190.0.34	NGAP/NAS-5GS	226	SACK (Ack=3, Arwnd=106496) , InitialContextSetupRequest, Registration accept
9	0.241240	10.190.0.34	10.101.10.7	NGAP	638	SACK (Ack=3, Arwnd=106496) , UERadioCapabilityInfoIndication
	0.280338	10.190.0.34	10.101.10.7	NGAP/NAS-5GS	118	UplinkNASTransport, Registration complete

図 4-4-1-4　R3 年度に相互接続が実現したパターンのパケットキャプチャー

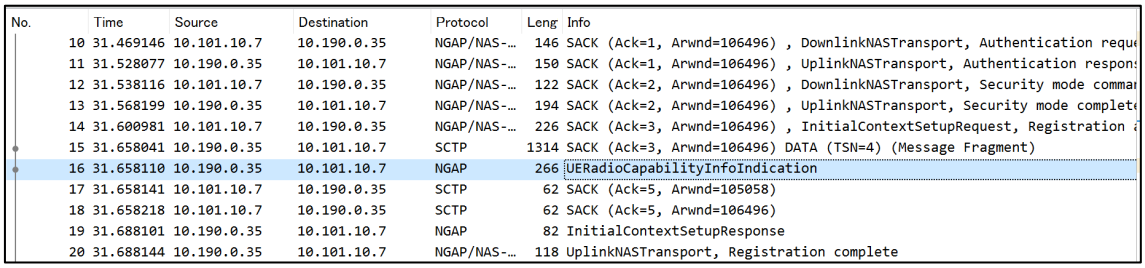


No.	Time	Source	Destination	Protocol	Leng	Info
316	357.159560	10.190.0.35	10.101.10.7	NGAP/NAS-5GS	134	InitialUEMessage, Registration request
371	357.186378	10.101.10.7	10.190.0.35	NGAP/NAS-5GS	146	SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request
376	357.243128	10.190.0.35	10.101.10.7	NGAP/NAS-5GS	142	SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response
396	357.256341	10.101.10.7	10.190.0.35	NGAP/NAS-5GS	122	SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command
402	357.288863	10.190.0.35	10.101.10.7	NGAP/NAS-5GS/NAS-5GS	190	SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request
488	357.332237	10.101.10.7	10.190.0.35	NGAP/NAS-5GS	226	SACK (Ack=3, Arwnd=106496) , InitialContextSetupRequest, Registration accept
494	357.409506	10.190.0.35	10.101.10.7	SCTP	62	SACK (Ack=3, Arwnd=106496)
495	357.439734	10.190.0.35	10.101.10.7	NGAP	82	InitialContextSetupResponse
496	357.439764	10.101.10.7	10.190.0.35	SCTP	66	SACK (Ack=3+2, Arwnd=106477)
497	357.439778	10.190.0.35	10.101.10.7	NGAP/NAS-5GS	118	UplinkNASTransport, Registration complete

図 4-4-1-5　R3 年度に相互接続が実現しなかったパターンのパケットキャプチャー

相互接続に成功したパターンでは”UERadioCapabilityInfoIndication”のフレームが確認できますが、認証が不可となったパターンでは該当のフレームが確認できません。特定の端末が不可となる事象は、対象フレームの不通により発生しておりました。対象のフレームが不通となった区間を調査の結果、基地局からコアへ伝送される際に対象フレームがドロップしていたことが判明したため、基地局の MTU サイズを適切なサイズへ調整しました。その結果該当フレームの疎通に成功し、端末の認証に成功いたしました。

「表 4-2-2　R3 年度の異ベンダーの組合せの内、相互接続が実現しなかったパターン」の組み合わせにおいて、相互接続が成功した際のパケットキャプチャーを以下の「図 4-4-1-6 MTU 調整後の R3 年度に相互接続が実現しなかったパターンのパケットキャプチャー」として掲載いたしました。



No.	Time	Source	Destination	Protocol	Leng	Info
10	31.469146	10.101.10.7	10.190.0.35	NGAP/NAS-…	146	SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication reque
11	31.528077	10.190.0.35	10.101.10.7	NGAP/NAS-…	150	SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication respons
12	31.538116	10.101.10.7	10.190.0.35	NGAP/NAS-…	122	SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode comma
13	31.568199	10.190.0.35	10.101.10.7	NGAP/NAS-…	194	SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complet
14	31.600981	10.101.10.7	10.190.0.35	NGAP/NAS-…	226	SACK (Ack=3, Arwnd=106496) , InitialContextSetupRequest, Registration a
15	31.658041	10.190.0.35	10.101.10.7	SCTP	1314	SACK (Ack=3, Arwnd=106496) DATA (TSN=4) (Message Fragment)
16	31.658110	10.190.0.35	10.101.10.7	NGAP	266	UERadioCapabilityInfoIndication
17	31.658141	10.101.10.7	10.190.0.35	SCTP	62	SACK (Ack=5, Arwnd=105058)
18	31.658218	10.101.10.7	10.190.0.35	SCTP	62	SACK (Ack=5, Arwnd=106496)
19	31.688101	10.190.0.35	10.101.10.7	NGAP	82	InitialContextSetupResponse
20	31.688144	10.190.0.35	10.101.10.7	NGAP/NAS-…	118	UplinkNASTransport, Registration complete

図 4-4-1-6　MTU 調整後の R3 年度に相互接続が実現しなかったパターンのパケットキャプチャー

「図 4-4-1-4　R3 年度に相互接続が実現したパターンのパケットキャプチャー」と同様に、”UERadioCapabilityInfoIndication”のフレームが確認できます。フレームサイズが大きいことで二つにフラグメントされており、図上の No. 15、No. 16 が該当のフレームになります。MTU の設定が不適切であったことにより、このフラグメントの処理が正常に行われず、該当フレームの疎通が不可となっていたと考えられます。

また、相互接続が不可となった「表 4-2-2　R3 年度の異ベンダーの組合せの内、相互接続が実現しなかったパターン」に記載の 1 パターンと、「表 4-3-2　新たに追加する異ベンダーの組合せパターンの相互接続結果」で相互接続が不可となった 2 パターンの端末はいずれも A 社製でした。端末起因の問題であることをさらに調査するため端末ごとの該当フレームのサイズを調査した結果を「表 4-4-1-7　キャプチャから取得した各端末の”UERadioCapabilityInfoIndication”フレームのサイズ」にまとめました。A 社製端末のみフレームサイズが大きいことがわかります。

表 4-4-1-7　キャプチャから取得した各端末の”UERadioCapabilityInfoIndication”フレームのサイズ

端末	合計フレームサイズ[byte]
A 社製	1580
B 社製	486
E 社製	274
F 社製	642
G 社製	526
H 社製	358

“UERadioCapabilityInfoIndication”のサイズは、主に端末の対応するバンド数に応じて増加します。これにより、A 社製端末は不適切な MTU の設定下において相互接続が不可となっていたと推測されます。コアと基地局を接続する際は、各装置の MTU を両機器間を接続する回線のパス MTU 以下に設定することが必要となります。ただし、MTU の値を小さくすることで通信の効率が低下するため、MTU の設定は回線のパス MTU と同値にすることが望ましいです。

(2) 相互接続の結果に関する考察

本調査研究で実施した通信の評価結果について考察いたします。

本項目の結果と考察は下記のようにまとめました。

- ①　電源 ON/OFF、機内モード ON/OFF 時の挙動確認
- ②　認証時間
- ③　長期安定試験
- ④　遅延
- ⑤　性能試験

① 電源 ON/OFF、機内モード ON/OFF 時の挙動

基地局、端末の電源 ON/OFF、端末の機内モード ON/OFF によって再度の認証が行われた場合であっても、接続が復旧することを確認しました。ON/OFF 切り替えにおける復帰動作の遅延や挙動不備等はなく、相互接続において問題がない結果であると考えられます。よって、機器の選定に際して電源 ON/OFF、機内モード ON/OFF 時の挙動を考慮する必要は低いと言えます。

②　認証時間

端末の SIM 認証開始から認証完了までの時間を確認しました。A 社製端末を除く全て組み合わせパターンで認証は 4 秒以内に完了し、大きな差はありませんでしたが、APPRESIA Systems 製端末のみ認証には 40 秒程度を要しました。これは端末の仕様に起因しております。端末が起動し認証が開始されてからモデムの起動が完了し通信が可能となるまでに時間がかかります。これは、全てのコア、基地局において共通の事象でした。

また、コアと基地局の組み合わせによる認証時間への影響はありませんでした。端末ごと

の平均認証時間を下記にまとめました。

表 4-4-2-1　端末ごとの平均認証時間

端末	平均認証時間[s]
A 社製	40.24
B 社製	1.89
E 社製	2.66
F 社製	1.24
G 社製	1.64
H 社製	2.40

仕様により認証に時間のかかる A 社製の端末を除き、全ての端末において 3 秒程度で認証が完了しており、相互接続組み合わせパターンによる認証時間の遅延や課題等はないと考えられます。機器の選定に際して、頻繁な端末の再起動を想定する場合、端末で通信が可能となるまでにかかる時間を確認しておくことが有効と考えられます。

③　長期安定性

長時間の通信時も端末の切断や多数の通信エラーが発生しないことを確認しました。全ての組み合わせにおいて、相互接続状態の継続によりエラーの蓄積や装置への過負荷などは発生しておらず、相互接続において問題がない結果であると考えられます。よって、機器の選定に際して長期安定性を考慮する必要性は低いと言えます。

④　遅延

端末からセンタ UPF へ ping 疎通試験を実施し、遅延時間を確認しました。

組み合わせパターンごとで遅延に差分があり、基地局間で差が開く傾向がありました。TDD パターンごとに最も優れた遅延の組み合わせは以下となります。

表 4-4-2-2　TDD パターンごとに最も遅延の少ない組み合わせ

TDD パターン	コア	基地局	端末	遅延値 [ms]
同期	B 社製	D 社製	H 社製	23
準同期 TDD1	A 社製	D 社製	H 社製	26
	B 社製	D 社製	A 社製	26
	B 社製	D 社製	E 社製	26
準同期 TDD2	B 社製	D 社製	H 社製	24
準同期 TDD3	A 社製	D 社製	H 社製	26
	B 社製	D 社製	H 社製	26

全ての TDD パターンにおいて、基地局：D 社製／端末：H 社製がもっとも遅延の少ない組

み合わせとなりました。
さらに、コア、基地局ごとの平均遅延を以下にまとめました。

表 4-4-2-3　コア、基地局ごとの平均遅延

TDD パターン	コア	基地局	平均遅延 [ms]
同期	A 社製	B 社製	52
		C 社製	33
		D 社製	33
	B 社製	B 社製	45
		C 社製	34
		D 社製	28
準同期 TDD1	A 社製	B 社製	47
		C 社製	34
		D 社製	28
	B 社製	B 社製	44
		C 社製	36
		D 社製	27
準同期 TDD2	A 社製	B 社製	50
		C 社製	36
		D 社製	32
	B 社製	B 社製	43
		C 社製	36
		D 社製	28
準同期 TDD3	A 社製	B 社製	42
		C 社製	―
		D 社製	30
	B 社製	B 社製	46
		C 社製	―
		D 社製	28

D 社製基地局は端末、コアに依らず遅延が短く、平均遅延は 35ms 以下になっています。この結果から、遅延性能は主に基地局の性能に依存していると想定されます。基地局機能の CU/DU/RU が一体となった構成では、各機能間の伝送遅延が無くなることで遅延が短くなっているという可能性が考えられます。このことから、機器の選定に際して遅延の要件がある場合、コア/CU/DU/RU といった各機能間の遅延が少ない構成が可能であることを確認することが有効であると考えられます。

⑤　通信性能

iperf による伝送スループット試験を実施しました。

組み合わせパターンごとに、各 TDD パターン、DL/UL での測定結果を以下に図示しました。

- 「図 4-4-2-1　同期 DL のスループット」
- 「図 4-4-2-2　準同期 TDD1 DL のスループット」
- 「図 4-4-2-3　準同期 TDD2 DL のスループット」
- 「図 4-4-2-4　準同期 TDD3 DL のスループット」
- 「図 4-4-2-5　同期 UL のスループット」
- 「図 4-4-2-6　準同期 TDD1 UL のスループット」
- 「図 4-4-2-7　準同期 TDD2 UL のスループット」
- 「図 4-4-2-8　準同期 TDD3 UL のスループット」

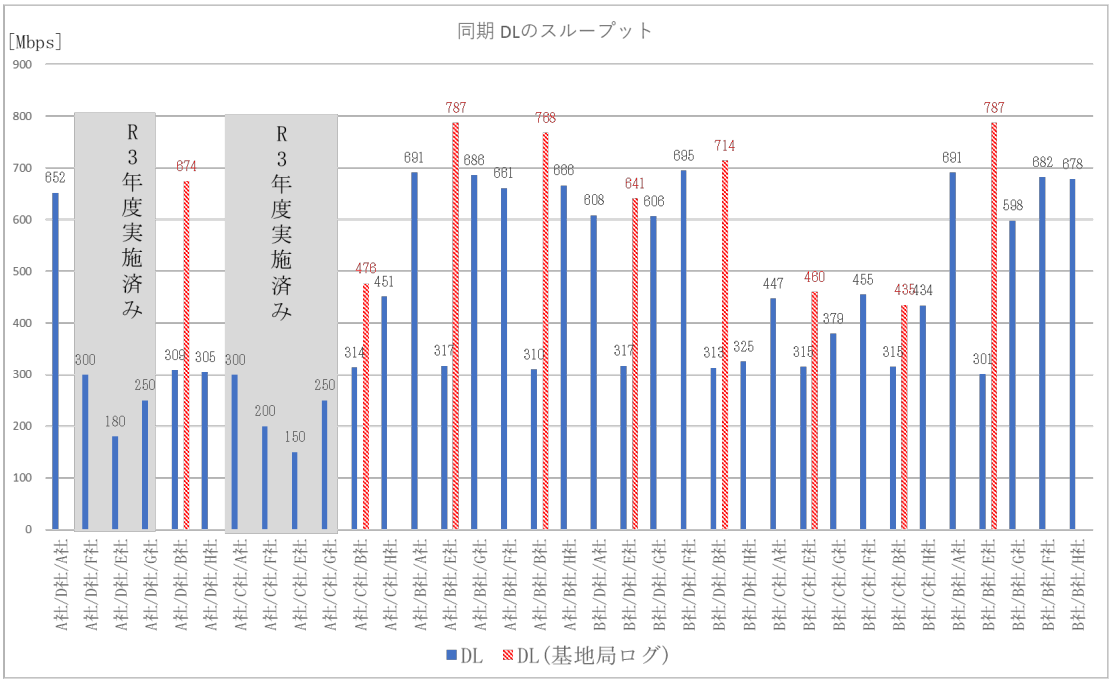


図 4-4-2-1　同期 DL のスループット

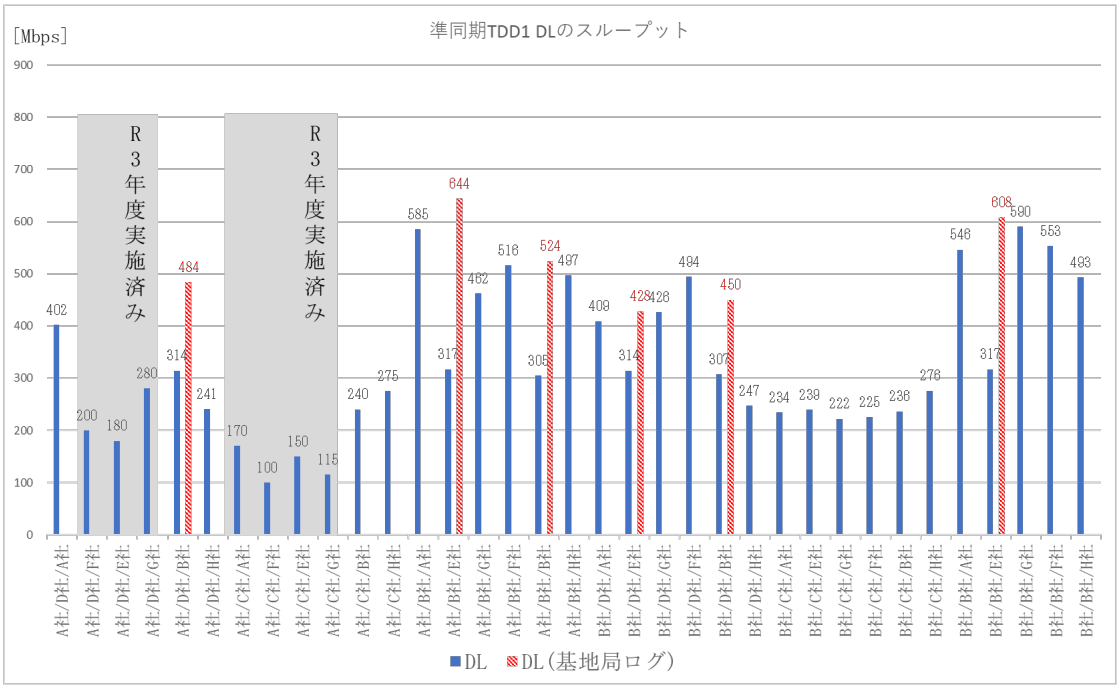


図 4-4-2-2　準同期 TDD1 DL のスループット

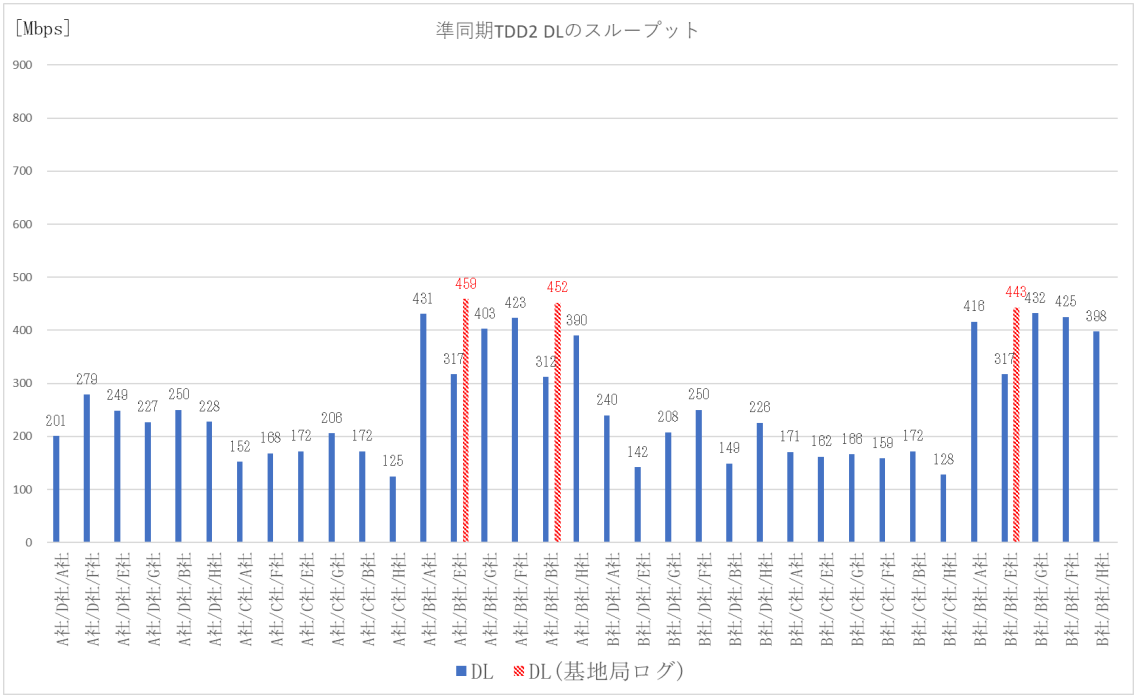


図 4-4-2-3　準同期 TDD2 DL のスループット

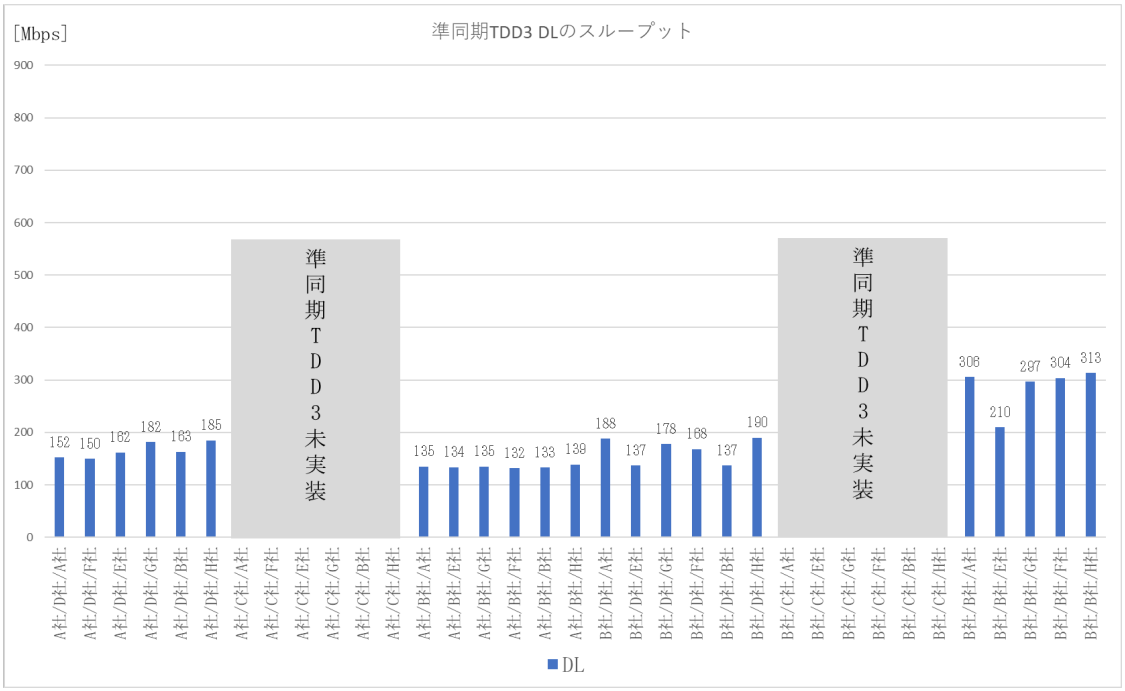


図 4-4-2-4　準同期 TDD3 DL のスループット

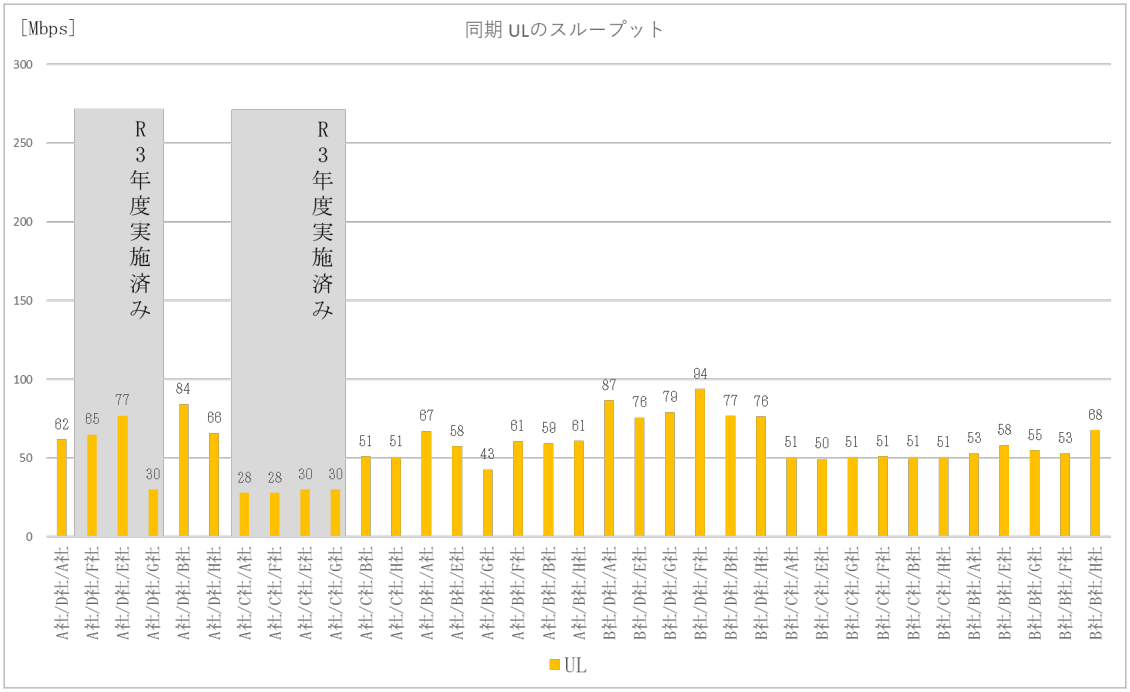


図 4-4-2-5　同期 UL のスループット

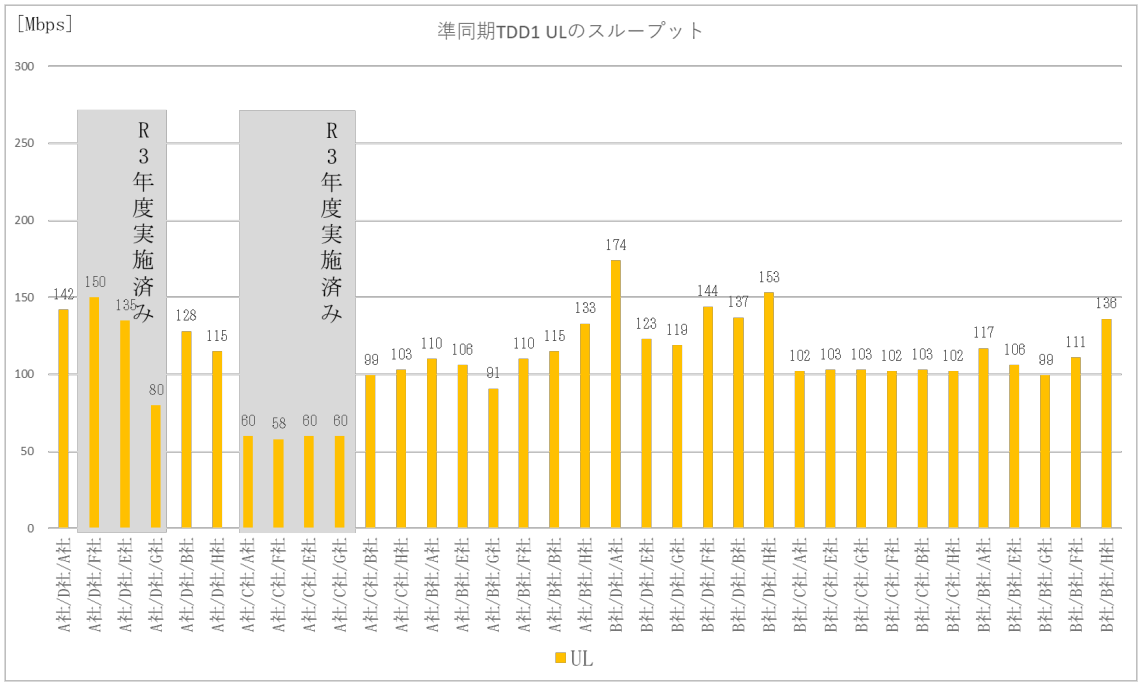


図 4-4-2-6　準同期 TDD1 UL のスループット

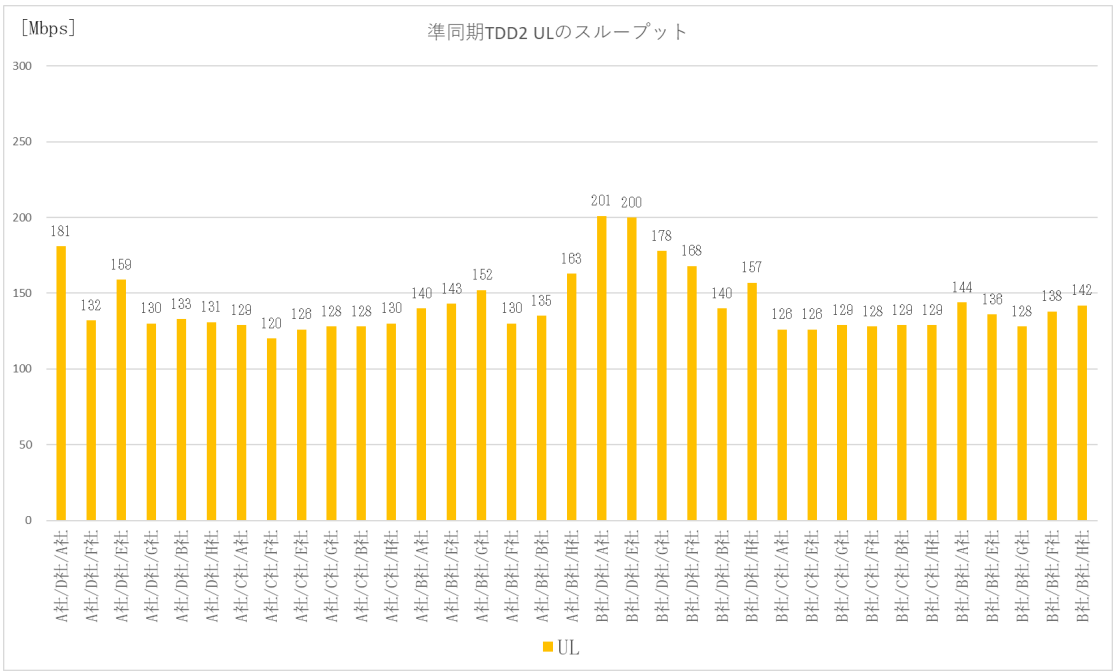


図 4-4-2-7　準同期 TDD2 UL のスループット

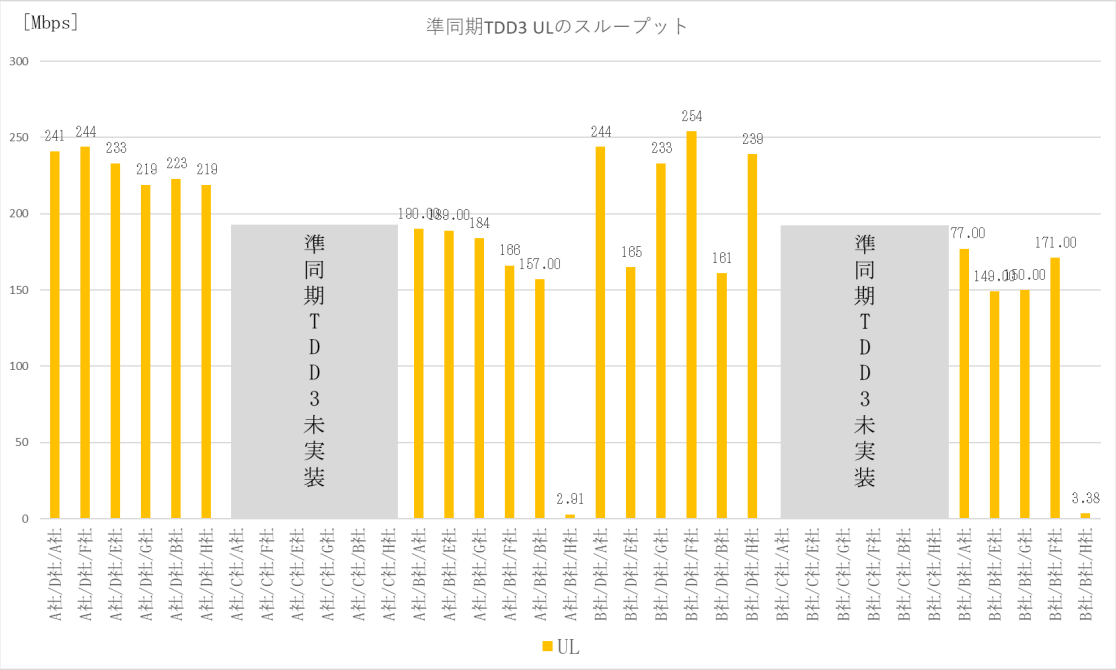


図 4-4-2-8　準同期 TDD3 UL のスループット

※1　赤字数字と赤帯は基地局の通信ログから計測した伝送量になります。
B 社、E 社の端末については、テザリング機能を用いてスループットの計測を実施したため、USB2.0 の実行値 310Mbps 程度がスループットの上限となっています。代わりに基地局での通信ログを用いて伝送量を計測しました。

※2　同期、準同期 TDD1 の結果は R3 年度に測定したものを掲載しております。R4 年度は R3 年度と同様の製品も用いていますが、製品の性能向上に係るファームアップ等を適用しており、数値の向上が確認できております。

主に基地局、端末間でスループットの差分が生じました。特に、以下組み合わせでの準同期 TDD3 UL スループットが極端に低い値となりました。

表 4-4-2-5　準同期 TDD3 UL スループットが極端に低い値となった組み合わせ

TDD パターン	パターン No.	コア	基地局	端末	UL [Mbps]
準同期 TDD3	1-10	A 社製	B 社製	H 社製	2.91
	1-27	B 社製	B 社製	H 社製	3.38

解析の結果、2 台の端末を接続した時、上り方向の無線通信に高い割合でエラーが発生していることが判明いたしました。これは基地局側が端末の無線を正常に解釈できていないことに起因しております。しかし、H 社製端末を D 社製基地局と接続した場合、その他の端末と同程度の TDD3 UL スループットが確認できております。

H 社製端末は準同期 TDD3 パターンをベンダーとしてサポートしていないこと、H 社製端末は V 社製のチップセットを採用しており、W 社製のチップセットを採用しているその他

の端末とは仕様が異なることにより、端末と基地局の無線仕様の不整合が発生し、こうした通信の異常が発生した可能性が考えられます。

このことから特定の TDD パターンの確実な動作や、通信に異常が発生した場合のサポートを必要とする場合などは、基地局、端末の両者で該当 TDD パターンのサポート状況を確認することが有効と言えます。

同期準同期の実現性について、DL スループットが同期、準同期 TDD1、準同期 TDD2、準同期 TDD3 の順に小さくなっていき、UL スループットでは同期、準同期 TDD1、準同期 TDD2、準同期 TDD3 の順に大きくなっていくという傾向が、上記を除いた全てのパターンで確認できました。このことから、複数の組み合わせで相互接続においても準同期 TDD1、準同期 TDD2、準同期 TDD3 の特性が得られることを確認しました。

TDD パターン毎に最も合計のスループットの高い組み合わせは以下となります。

表 4-4-2-6　各 TDD パターンにおいて最もスループットが高い組み合わせ

TDD パターン	パターン No.	コア	基地局	端末	合計 [Mbps]
同期	1-14	B 社製	D 社製	F 社製	789
準同期 TDD1	1-5	A 社製	B 社製	A 社製	695
準同期 TDD2	1-5	A 社製	B 社製	A 社製	571
準同期 TDD3	1-23	B 社製	B 社製	A 社製	483

B 社製、D 社製基地局のスループットが高くなる傾向にありました。

さらに、コア、基地局ごとの平均スループットを以下にまとめました。

表 4-4-2-7　コア、基地局ごとの平均スループット

TDD パターン	コア	基地局	平均 DL [Mbps]	平均 UL [Mbps]
同期	A 社製	B 社製	676	58
		C 社製	451	51
		D 社製	479	71
	B 社製	B 社製	662	57
		C 社製	429	51
		D 社製	559	81
準同期 TDD1	A 社製	B 社製	515	111
		C 社製	258	101
		D 社製	322	128

	B 社製	B 社製	546	114
		C 社製	239	103
		D 社製	394	142
準同期 TDD2	A 社製	B 社製	412	144
		C 社製	166	127
		D 社製	239	144
	B 社製	B 社製	418	138
		C 社製	160	128
		D 社製	203	174
準同期 TDD3	A 社製	B 社製	135	177
		C 社製	―	―
		D 社製	166	230
	B 社製	B 社製	286	162
		C 社製	―	―
		D 社製	166	216

※異常値となったパターン 1-10、1-27 の準同期 TDD3 UL、およびテザリングによる上限値となってしまった値は除外して計算しております。

D 社製基地局はコアに依らず UL スループットが高く、B 社製基地局はコアに依らず DL スループットが高い結果となりました。遅延と同様に、通信性能は主に基地局の性能に依存していると考えられ、より多くのレイヤー数、より効率の高い変調方式へ対応している基地局のスループットが高くなる可能性が考えられます。

(3) 相互接続組み合せごとのまとめ

R3 年度と合わせて、コア：2 種、基地局：3 種、端末：6 種を用いた 35 パターンの組み合わせと、東京大学開発基地局を用いた追加検証を合わせた全 41 パターンの相互接続検証を実施しました。全ての組み合わせパターンの相互接続結果は「表 4-4-3-1 全ての相互接続パターンの結果」のとおりです。

表 4-4-3-1 全ての相互接続パターンの結果

No.	コア	基地局	端末	接続可否
1	A 社製	D 社製	A 社製	○
2	A 社製	D 社製	B 社製	○
3	A 社製	D 社製	E 社製	○
4	A 社製	D 社製	F 社製	○
5	A 社製	D 社製	G 社製	○
6	A 社製	D 社製	H 社製	○
7	A 社製	C 社製	A 社製	○※1
8	A 社製	C 社製	B 社製	○

9	A 社製	C 社製	E 社製	○※1
10	A 社製	C 社製	F 社製	○※1
11	A 社製	C 社製	G 社製	○※1
12	A 社製	C 社製	H 社製	○
13	A 社製	D 社製	A 社製	○
14	A 社製	D 社製	B 社製	○
15	A 社製	D 社製	E 社製	○※1
16	A 社製	D 社製	F 社製	○※1
17	A 社製	D 社製	G 社製	○※1
18	A 社製	D 社製	H 社製	○
19	B 社製	B 社製	A 社製	○
20	B 社製	B 社製	E 社製	○
21	B 社製	B 社製	F 社製	○
22	B 社製	B 社製	G 社製	○
23	B 社製	B 社製	H 社製	○
24	B 社製	C 社製	A 社製	○
25	B 社製	C 社製	B 社製	○
26	B 社製	C 社製	E 社製	○
27	B 社製	C 社製	F 社製	○
28	B 社製	C 社製	G 社製	○
29	B 社製	C 社製	H 社製	○
30	B 社製	D 社製	A 社製	○
31	B 社製	D 社製	B 社製	○
32	B 社製	D 社製	E 社製	○
33	B 社製	D 社製	F 社製	○
34	B 社製	D 社製	G 社製	○
35	B 社製	D 社製	H 社製	○
36	A 社製	CDRU-東京大学	A 社製	○
37	A 社製	CDRU-東京大学	B 社製	○
38	A 社製	CDRU-東京大学	E 社製	○
39	A 社製	CDRU-東京大学	F 社製	○
40	A 社製	CDRU-東京大学	G 社製	○
41	A 社製	CDRU-東京大学	H 社製	○

※1 R3 年度に相互接続を実現済み

R3 年度と合わせた本調査研究での各コア、基地局の組み合わせ毎の結果を、以下のようにまとめました。

- ①コア：A 社製 / 基地局：B 社製
- ②コア：A 社製 / 基地局：C 社製
- ③コア：A 社製 / 基地局：D 社製

- ④コア：B 社製 / 基地局：D 社製
- ⑤コア：B 社製 / 基地局：C 社製
- ⑥コア：B 社製 / 基地局：B 社製
- ⑦コア：A 社製 / 基地局：東京大学

① コア：A 社製 / 基地局：B 社製

A 社製コアと B 社製基地局、各端末の接続検証した結果を「表 4-4-3-2 A 社製コアと B 社製基地局の接続結果・考察」に示します。

表 4-4-3-2 A 社製コアと B 社製基地局の接続結果・考察

項目	検証結果・考察
相互接続可否	以下 6 つの異なるベンダー製端末と相互接続に成功 ・A 社 ・B 社 ・E 社 ・F 社 ・G 社 ・H 社
電源 ON/OFF、機内モード ON/OFF 時の挙動	基地局、端末の電源 ON/OFF 時、端末の機内モード ON/OFF 時に再度端末が正常に認証されることを確認
認証時間	【端末の認証にかかる時間】 平均認証時間：2.16 秒
長期安定性	【48 時間の連続 Ping 疎通】 平均疎通率：99.9%
遅延時間	【同期】 平均遅延：52ms 【準同期 TDD1】 平均遅延：47ms 【準同期 TDD2】 平均遅延：50ms 【準同期 TDD3】 平均遅延：42ms ※端末配下のサーバと UPF 配下のサーバ間での Ping 応答時間(50 回分)の平均
伝送スループット	【同期】 平均 DL：676Mbps　　平均 UL：58Mbps 【準同期 TDD1】 平均 DL：515Mbps　　平均 UL：111Mbps 【準同期 TDD2】 平均 DL：412Mbps　　平均 UL：144Mbps 【準同期 TDD3】 平均 DL：135Mbps　　平均 UL：177Mbps ※端末配下のサーバと UPF 配下のサーバ間の最大伝送スループットを iperf により測定 ※動的な変調方式の調整機能を有効にし測定

	※最大 MIMO レイヤー数：DL 4layer / UL 1layer ※対応変調方式：DL 64QAM まで / UL 64QAM まで ※DL スループットについてはテザリングによりスループットが制限されてしまった B 社、E 社製端末を除いて平均値を算出
考察	・本調査研究で使用した全ての端末との相互接続が可能 ・認証時間、期安定性、遅延時間はすべて正常 ・同期、準同期 TDD1、準同期 TDD2、準同期 TDD3 において、順に DL スループットが低下し、UL スループットが向上することを確認 ・DL 4layer かつ動的な変調方式の調整に対応しており、高い DL スループットを確認できた ・H 社製端末との接続時、準同期 TDD3 の UL スループットが著しく低い値となった 準同期 TDD3 を適用する際、端末側の TDD3 対応状況に特に留意することで、問題なく相互接続が可能と考えられます。

② コア：A 社製 / 基地局：C 社製

A 社製コアと C 社製基地局、各端末の接続検証した結果を「表 4-4-3-3 A 社製コアと C 社製基地局の接続結果・考察」に示します。

表 4-4-3-3 A 社製コアと C 社製基地局の接続結果・考察

項目	検証結果・考察
相互接続可否	以下 2 つの異なるベンダー製端末と相互接続に成功 ・A 社(※1) ・B 社 ・E 社(※1) ・F 社(※1) ・G 社(※1) ・H 社 ※1：R3 年度実施済み
電源 ON/OFF、機内モード ON/OFF 時の挙動	基地局、端末の電源 ON/OFF 時、端末の機内モード ON/OFF 時に再度端末が正常に認証されることを確認
認証時間	【端末の認証にかかる時間】 平均認証時間：2.5 秒
長期安定性	【48 時間の連続 Ping 疎通】 平均疎通率：99.1% ※ R4 年度実施分を集計
遅延時間	【同期】 平均遅延：33ms 【準同期 TDD1】 平均遅延：34ms 【準同期 TDD2】

	平均遅延：36ms ※ R4 年度実施分を集計 ※端末配下のサーバと UPF 配下のサーバ間での Ping 応答時間(50 回分)の平均
伝送スループット	【同期】 平均 DL：451Mbps　　平均 UL：51Mbps 【準同期 TDD1】 平均 DL：258Mbps　　平均 UL：101Mbps 【準同期 TDD2】 平均 DL：166Mbps　　平均 UL：127Mbps ※ R4 年度実施分を集計 ※端末配下のサーバと UPF 配下のサーバ間の最大伝送スループットを iperf により測定 ※DL MCS=24、UL MCS=16 にし測定 ※最大 MIMO レイヤー数：DL 4layer / UL 1layer ※対応変調方式：DL 64QAM まで / UL 64QAM まで ※DL スループットについてはテザリングによりスループットが制限されてしまった B 社製端末を除いて平均値を算出
考察	・本調査研究で使用した全ての端末との相互接続が可能 ・認証時間、期安定性、遅延時間はすべて正常 ・同期、準同期 TDD1、準同期 TDD2 の適用が可能 総合的に問題なく相互接続が可能と考えられます。

③ コア：A 社製 / 基地局：D 社製

A 社製コアと D 社製基地局、各端末の接続検証した結果を「表 4-4-3-4 A 社製コアと D 社製基地局の接続結果・考察」に示します。

表 4-4-3-4 A 社製コアと D 社製基地局の接続結果・考察

項目	検証結果・考察
相互接続可否	以下 6 つの異なるベンダー製端末と相互接続に成功 ・A 社 ・B 社 ・E 社(※1) ・F 社(※1) ・G 社(※1) ・H 社 ※1：R3 年度実施済み
電源 ON/OFF、機内モード ON/OFF 時の挙動	基地局、端末の電源 ON/OFF 時、端末の機内モード ON/OFF 時に再度端末が正常に認証されることを確認
認証時間	【端末の認証にかかる時間】 平均認証時間：2.39 秒 ※仕様により特に認証に時間のかかる A 社製端末は除いて平均値を算出
長期安定性	【48 時間の連続 Ping 疎通】

	平均疎通率：98.9% ※ R4 年度実施分を集計
遅延時間	【同期】 平均遅延：33ms 【準同期 TDD1】 平均遅延：28ms 【準同期 TDD2】 平均遅延：32ms 【準同期 TDD3】 平均遅延：30ms ※ R4 年度実施分を集計 ※端末配下のサーバと UPF 配下のサーバ間での Ping 応答時間(50 回分)の平均
伝送スループット	【同期】 平均 DL：479Mbps　　平均 UL：71Mbps 【準同期 TDD1】 平均 DL：322Mbps　　平均 UL：128Mbps 【準同期 TDD2】 平均 DL：239Mbps　　平均 UL：144Mbps 【準同期 TDD3】 平均 DL：166Mbps　　平均 UL：230Mbps ※ R4 年度実施分を集計 ※端末配下のサーバと UPF 配下のサーバ間の最大伝送スループットを iperf により測定 ※動的な変調方式の調整機能を有効にし測定 ※最大 MIMO レイヤー数：DL 2layer / UL 2layer ※対応変調方式：DL 256QAM まで / UL 256QAM まで ※DL スループットについてはテザリングによりスループットが制限されてしまった B 社製端末を除いて平均値を算出
考察	・R3 年度に相互接続が実現されなかった端末との組み合わせパターンを含め、本調査研究で使用した全ての端末との相互接続が可能 ・認証時間、長期安定性、遅延時間はすべて正常、特に遅延時間は短い傾向にある ・同期、準同期 TDD1、準同期 TDD2、準同期 TDD3 の適用が可能 ・UL 2Layer かつ 256QAM 変調に対応した設定での安定的な通信であり、高い UL スループットが確認できた 総合的に問題なく相互接続が可能と考えられます。

④ コア：B 社製 / 基地局：B 社製

B 社製コアと B 社製基地局、各端末の接続検証した結果を「表 4-4-3-5 B 社製コアと B 社製基地局の接続結果・考察」に示します。

表 4-4-3-5 B 社製コアと B 社製基地局の接続結果・考察

項目	検証結果・考察
相互接続可否	以下 5 つの異なるベンダー製端末と相互接続に成功 ・A 社 ・E 社 ・F 社 ・G 社 ・H 社
電源 ON/OFF、機内モード ON/OFF 時の挙動	基地局、端末の電源 ON/OFF 時、端末の機内モード ON/OFF 時に再度端末が正常に認証されることを確認
認証時間	【端末の認証にかかる時間】 平均認証時間：1.89 秒
長期安定性	【48 時間の連続 Ping 疎通】 平均疎通率：99.8%
遅延時間	【同期】 平均遅延：45ms 【準同期 TDD1】 平均遅延：44ms 【準同期 TDD2】 平均遅延：43ms 【準同期 TDD3】 平均遅延：46ms ※端末配下のサーバと UPF 配下のサーバ間での Ping 応答時間(50 回分)の平均
伝送スループット	【同期】 平均 DL：662Mbps　　平均 UL：57Mbps 【準同期 TDD1】 平均 DL：546Mbps　　平均 UL：114Mbps 【準同期 TDD2】 平均 DL：418Mbps　　平均 UL：138Mbps 【準同期 TDD3】 平均 DL：286Mbps　　平均 UL：162Mbps ※端末配下のサーバと UPF 配下のサーバ間の最大伝送スループットを iperf により測定 ※動的な変調方式の調整機能を有効にし測定 ※最大 MIMO レイヤー数：DL 4layer / UL 1layer ※対応変調方式：DL 64QAM まで / UL 64QAM まで ※DL スループットについてはテザリングによりスループットが制限されてしまった B 社、E 社製端末を除いて平均値を算出
考察	・本調査研究で使用した全ての端末との相互接続が可能 ・認証時間、期安定性、遅延時間はすべて正常 ・同期、準同期 TDD1、準同期 TDD2、準同期 TDD3 において、順に DL スループットが低下し、UL スループットが向上することを確認

	・DL 4layer かつ動的な変調方式の調整に対応しており、高い DL スループットを確認できた ・H 社製端末との接続時、準同期 TDD3 の UL スループットが著しく低い値となった 準同期 TDD3 を適用する際、端末側の TDD3 対応状況に特に留意することで、問題なく相互接続が可能と考えられます。

⑤ **コア**：**B 社製 / 基地局**：C 社製

B 社製コアと C 社製基地局、各端末の接続検証した結果を「表 4-4-3-6 B 社製コアと C 社製基地局の接続結果・考察」に示します。

表 4-4-3-6 B 社製コアと C 社製基地局の接続結果・考察

項目	検証結果・考察
相互接続可否	以下 6 つの異なるベンダー製端末と相互接続に成功 ・A 社 ・B 社 ・E 社 ・F 社 ・G 社 ・H 社
電源 ON/OFF、機内モード ON/OFF 時の挙動	基地局、端末の電源 ON/OFF 時、端末の機内モード ON/OFF 時に再度端末が正常に認証されることを確認
認証時間	【端末の認証にかかる時間】 平均認証時間：1.87 秒
長期安定性	【48 時間の連続 Ping 疎通】 平均疎通率：99.2%
遅延時間	【同期】 平均遅延：34ms 【準同期 TDD1】 平均遅延：36ms 【準同期 TDD2】 平均遅延：36ms ※端末配下のサーバと UPF 配下のサーバ間での Ping 応答時間(50 回分)の平均
伝送スループット	【同期】 平均 DL：429Mbps　　平均 UL：51Mbps 【準同期 TDD1】 平均 DL：239Mbps　　平均 UL：103Mbps 【準同期 TDD2】 平均 DL：160Mbps　　平均 UL：128Mbps ※端末配下のサーバと UPF 配下のサーバ間の最大伝送スループットを iperf により測定 ※DL MCS=24、UL MCS=16 にし測定

	※最大 MIMO レイヤー数：DL 4layer / UL 1layer ※対応変調方式：DL 64QAM まで / UL 64QAM まで ※DL スループットについてはテザリングによりスループットが制限されてしまった B 社製端末を除いて平均値を算出
考察	・本調査研究で使用した全ての端末との相互接続が可能 ・認証時間、期安定性、遅延時間はすべて正常 ・同期、準同期 TDD1、準同期 TDD2 において、順に DL スループットが低下し、UL スループットが向上することを確認 総合的に問題なく相互接続が可能と考えられます。

⑥ コア：B 社製 / 基地局：D 社製

B 社製コアと D 社製基地局、各端末の接続検証した結果を「表 4-4-3-7 B 社製コアと D 社製基地局の接続結果・考察」に示します。

表 4-4-3-7 B 社製コアと D 社製基地局の接続結果・考察

項目	検証結果・考察
相互接続可否	以下 6 つの異なるベンダー製端末と相互接続に成功 ・A 社 ・B 社 ・E 社 ・F 社 ・G 社 ・H 社
電源 ON/OFF、機内モード ON/OFF 時の挙動	基地局、端末の電源 ON/OFF 時、端末の機内モード ON/OFF 時に再度端末が正常に認証されることを確認
認証時間	【端末の認証にかかる時間】 平均認証時間：1.69 秒 ※仕様により特に認証に時間のかかる A 社製端末は平均より除外
長期安定性	【48 時間の連続 Ping 疎通】 平均疎通率：99.8%
遅延時間	【同期】 平均遅延：28ms 【準同期 TDD1】 平均遅延：27ms 【準同期 TDD2】 平均遅延：28ms 【準同期 TDD3】 平均遅延：28ms ※端末配下のサーバと UPF 配下のサーバ間での Ping 応答時間(50 回分)の平均
伝送スループット	【同期】 平均 DL：559Mbps　　平均 UL：81Mbps 【準同期 TDD1】

	平均 DL：394Mbps　　平均 UL：142Mbps 【準同期 TDD2】 平均 DL：203Mbps　　平均 UL：174Mbps 【準同期 TDD3】 平均 DL：166Mbps　　平均 UL：216Mbps ※端末配下のサーバと UPF 配下のサーバ間の最大伝送スループットを iperf により測定 ※動的な変調方式の調整機能を有効にし測定 ※最大 MIMO レイヤー数：DL 2layer / UL 2layer ※対応変調方式：DL 256QAM まで / UL 256QAM まで ※DL スループットについてはテザリングによりスループットが制限されてしまった B 社、E 社製端末を除いて平均値を算出
考察	・認証時間、長期安定性、遅延時間はすべて正常、特に遅延時間は短い傾向にある ・同期、準同期 TDD1、準同期 TDD2、準同期 TDD3 の適用が可能 ・UL 2Layer かつ 256QAM 変調に対応した設定での安定的な通信ができており、高い UL スループットが確認できた 総合的に問題なく相互接続が可能と考えられます。

⑦ コア：A 社製 / 基地局：東京大学

A 社製コアと東京大学製基地局、各端末の接続検証した結果を「表 4-4-3-8 A 社製コアと東京大学製基地局の接続結果・考察」に示します。

表 4-4-3-8 A 社製コアと東京大学製基地局の接続結果・考察

項目	検証結果・考察
相互接続可否	以下 6 つの異なるベンダー製端末と相互接続に成功 ・A 社 ・B 社 ・E 社 ・F 社 ・G 社 ・H 社
電源 ON/OFF、機内モード ON/OFF 時の挙動	基地局、端末の電源 ON/OFF 時、端末の機内モード ON/OFF 時に再度端末が正常に認証されることを確認
遅延時間	【同期】 平均遅延：28ms 【準同期 TDD1】 平均遅延：28ms 【準同期 TDD3】 平均遅延：30ms ※端末配下のサーバと UPF 配下のサーバ間での Ping 応答時間(50 回分)の平均

伝送スループット	【同期】 平均 DL：595Mbps　　平均 UL：51Mbps 【準同期 TDD1】 平均 DL：462Mbps　　平均 UL：110Mbps 【準同期 TDD3】 平均 DL：280Mbps　　平均 UL：161Mbps ※端末配下のサーバと UPF 配下のサーバ間の最大伝送スループットを iperf により測定 ※動的な変調方式の調整機能を有効にし測定 ※DL 2layer UL 2layer ※DL スループットについてはテザリングによりスループットが制限されてしまった B 社、E 社製端末を除いて平均値を算出
考察	・本調査研究で使用した全ての端末との相互接続が可能 ・認証時間、期安定性、遅延時間はすべて正常 ・同期、準同期 TDD1、準同期 TDD3 において、順に DL スループットが低下し、UL スループットが向上することを確認 総合的に問題なく相互接続が可能と考えられます。

(4) 相互接続の検証結果を踏まえたコアの共用における考察

R3 年度と合わせて、コア：2 種、基地局：3 種、端末：6 種を用いた 35 パターンの組み合わせと東京大学開発基地局を用いた追加検証を合わせた全 41 パターンの相互接続検証を実施しました。3GPP で規定されるパラメータ、3GPP 上自由設計となっているパラメータや準拠する 3GPP のリリースバージョンの差異、機器を導入するネットワーク環境に合わせたパラメータの調整を行うことで、全 41 パターンの相互接続が実現しました。これにより、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。

本検証で得た相互接続に必要なパラメータの知見をもとに「相互接続のための技術的手引」を作成しました。今後相互接続を必要とする一般ユーザや SIer が本手引を活用することで異ベンダー間相互接続の普及促進が期待されます。

また、相互接続後の通信試験において、準同期 TDD3 での UL 通信が不良となるパターンが 2 つ発見されました。相互接続を実現する際には、TDD パターンを含め、MIMO レイヤー数、変調方式などの無線機能について基地局と端末のサポート有無を事前に確認する必要があると考えます。

5. ローカル５Ｇシステムの検証

5.1 検証概要

本調査研究では、複数企業共用パターンおよ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、監視および運用の検証を行うことで、各種課題を洗い出し、コア/CU 共用の実現に向けて実装が必要な要件等をまとめました。

5.2 検証環境

検証環境は図 5-2-1～5-2-3 のとおりです。NTT 中央研修センタではすべての検証を、各大学およびいすゞ自動車では性能検証およびセキュリティ検証の一部を実施いたしました。

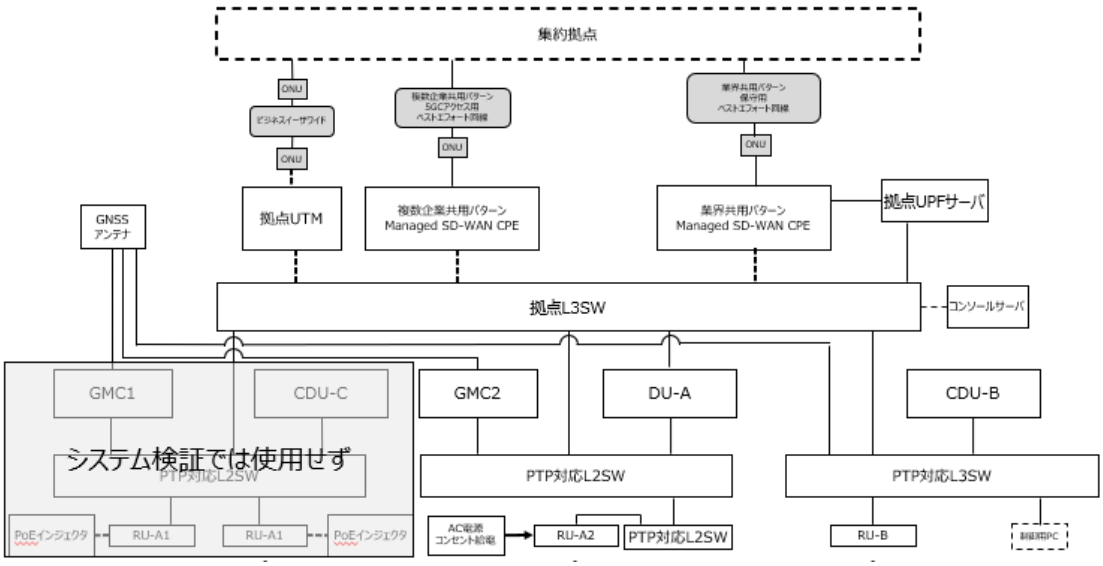


図 5-2-1 システム検証におけるネットワーク構成図(NTT 中央研修センタ)

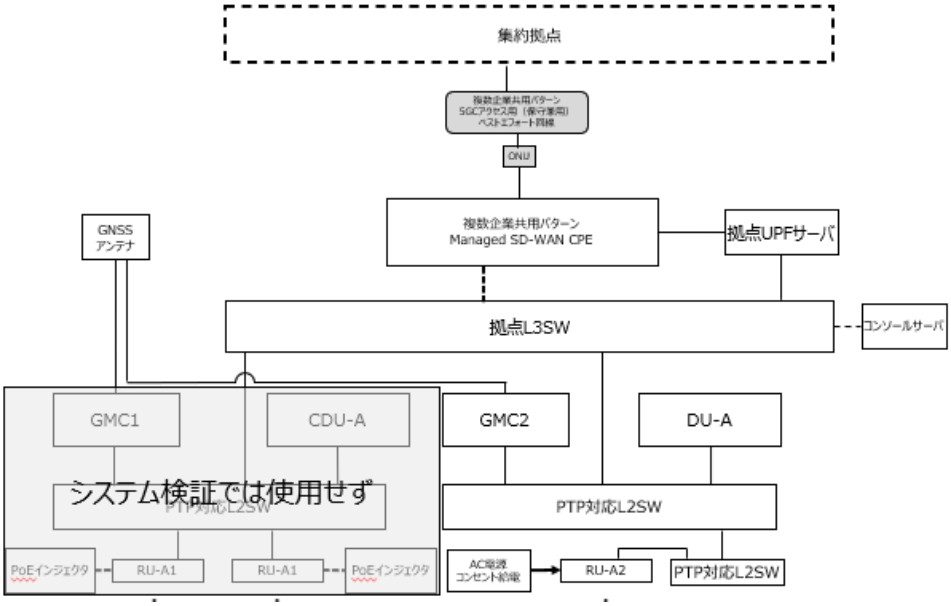


図 5-2-2 システム検証におけるネットワーク構成図（いすゞ自動車）

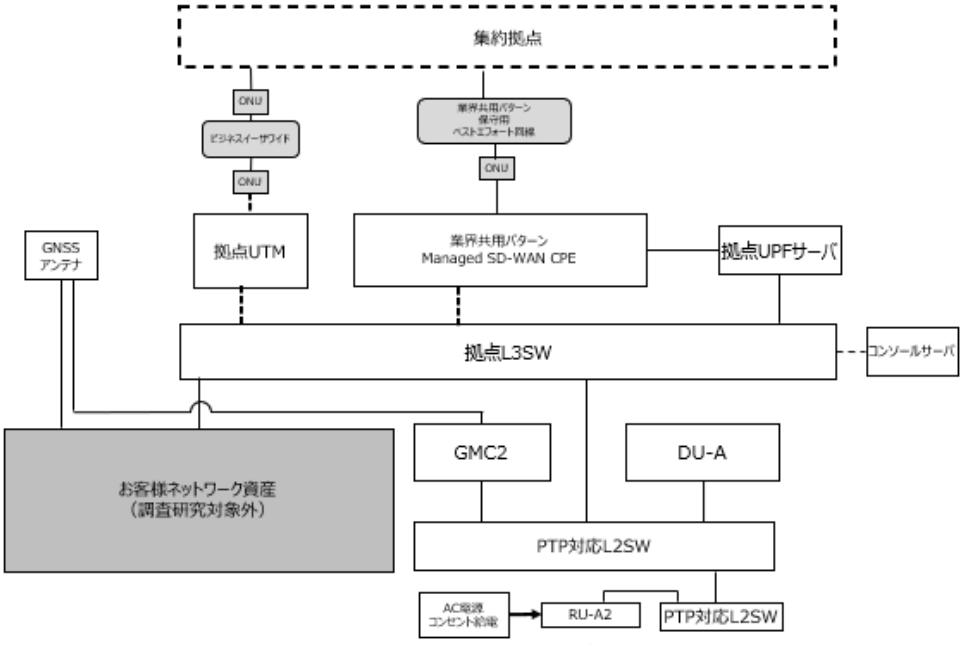


図 5-2-3 システム検証におけるネットワーク構成図（東北大学、東京大学、京都大学）

RU、UE、測定用 PC の設置については以下の図 5-2-4、図 5-2-5 のとおりです。



図 5-2-4 RU 設置状況（NTT 中央研修センタ）

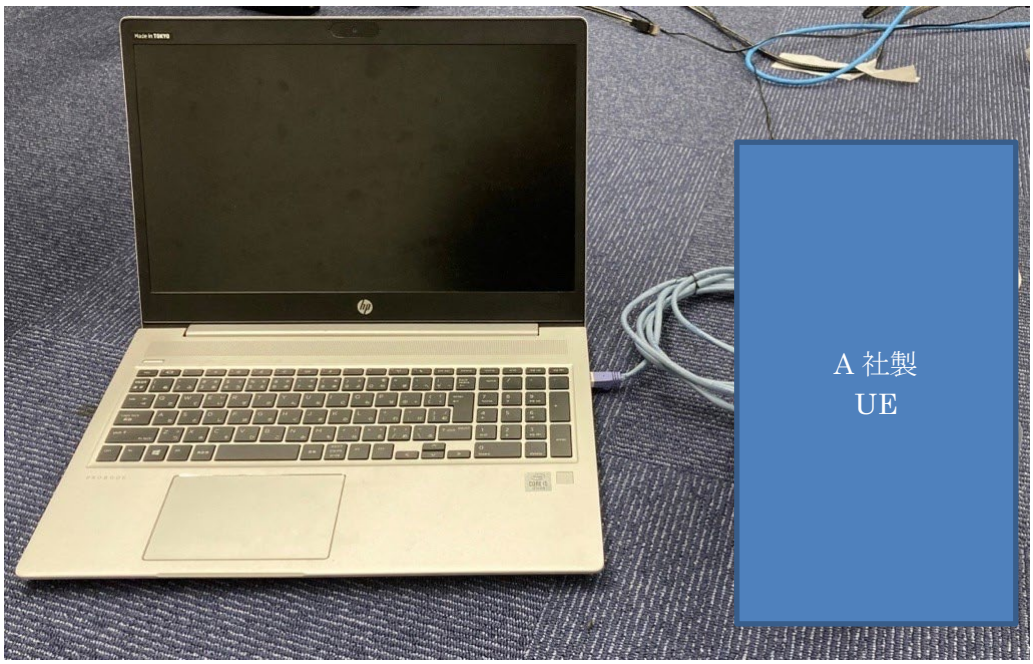


図 5-2-5 UE、測定用 PC 設置状況 （NTT 中央研修センタ）

5.3 ローカル５Ｇ交換設備の共用における性能検証

(1) 検証目標

R3 年度の調査研究の結果として、コア共用環境において UE～UPF の伝送性能検証、CPU 等消費リソースの検証、UE 認証時間の検証および UE 多接続検証を実施しました。伝送性能については R3 年度のユースケース所要性能を満たすスループットおよび遅延時間が測定されたことで、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しています。消費リソースについてはUE数が増大した場合にCPU利用率は大きな変動がなく、メモリ利用率は微増したという結果のため、基本的にUE数はローカル５Ｇシステムの消費リソースに対する大きな課題とならないとしています。またUE認証時間については、複数企業共用パターン/業界共用パターンの別およびセンタ拠点～エンド拠点の物理的な距離に影響されず1分間以内で認証するという結果から、コア共用環境はUE認証時間に差分を生じないとしています。UE多接続検証については、RU～UE区間の最大伝送スループット相当まで通信可能であり、コア共用によって通信性能が逼迫しないとしています。

これらの結果を踏まえて、本調査研究のモデルではコア/CU共用環境下において、各種性能を検証しローカル５Ｇのシステム構成や環境の違いによる伝送性能への影響や相関性について比較・考察しました。具体的には複数企業共用パターン/業界共用パターンの拠点間通信回線の違い、UPFの設置位置の違い、センタ拠点～エンド拠点の物理的な距離の違いを考慮した上で、十分な伝送性能が発揮できるか、スループットおよび遅延時間を測定し、比較・検証しました。またUE多接続状態での消費リソースおよび認証時間については R3年度で検証済みですが、UE 数の増大によって認証パケットがセンタ拠点～エンド拠点のネットワークを圧迫するものであるか確認するため、UE 多接続時の認証パケットに必要な帯域を測定し、比較しました。そしてTDDの準同期方式(総務省告示第23号別図第一号に規定された準同期方式のフレーム構成)を適用した場合の伝送性能が複数企業共用パターン/業界共用パターンの別、センタUPF/エンドUPFの別によって変動するものかについても検証しました。

検証における機器配置について「図1-2-3　ローカル５Ｇ機器配置パターン」を次に再掲します。

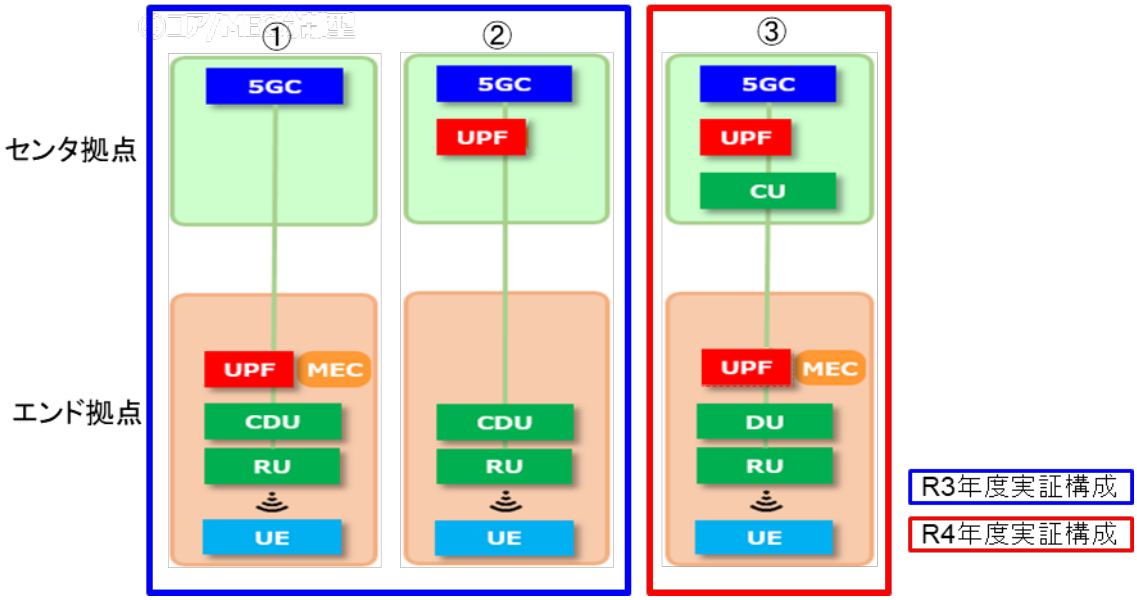


図1-2-3　ローカル５Ｇ機器配置パターン　（再掲）

(2) 評価・検証項目

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

表 5-3-2-1 評価・検証項目

大項目	小項目	検証概要	検証環境	検証項目
性能検証	複数企業共用パターン(※1)	各種性能の相関性	コア＋CU共用	・TCP/UDP スループット(※2) ・パケットロス、ジッタ(※2) ・遅延時間(※3)
		UE 多接続	コア＋CU共用	・認証パケットの必要帯域 (※2)
		準同期方式での性能変動	コア＋CU共用	・TCP/UDP スループット(※2) ・パケットロス、ジッタ(※2) ・遅延時間(※2)
	業界共用パターン(※1)	各種性能の相関性	コア＋CU共用	・TCP/UDP スループット(※2) ・パケットロス、ジッタ(※2) ・遅延時間(※3)
		UE 多接続	コア＋CU共用	・認証パケットの必要帯域 (※2)
		準同期方式での性能変動	コア＋CU共用	・TCP/UDP スループット(※2) ・パケットロス、ジッタ(※2) ・遅延時間(※2)

(※1)を付した環境にあってはセンタ UPF およびエンド UPF の 2 パターンで測定を行う。
(※2)を付した測定項目は NTT 中央研修センタにおいて測定を行う。
(※3)を付した測定項目はすべてのエンド拠点それぞれにおいて測定を行う。

(3) 評価・検証方法

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

表 5-3-3-1　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
	使用帯域測定：Wireshark
	UE 多接続検証：UE エミュレータ

※UE 多接続検証においては、UE エミュレータを用いて数十台分の UE 接続状態を再現します。

本検証にて想定している手順を、「表 5-3-3-2　検証手順（各種性能の相関性)」～「表 5-3-3-4　検証手順（準同期方式での性能変動)」に示します。また、検証イメージを「図 5-3-3-1　検証イメージ（各種性能の相関性)」～「図 5-3-3-3　検証イメージ（準同期方式での性能変動)」に示します。

表 5-3-3-2 検証手順（各種性能の相関性）

項番	実施内容	対応図表
1	【UE 接続確認】 検証時、UE を次の条件の位置に設置し、RU と接続 ・RU の主ビーム方向上の位置で RU から見通しがあること ・人体等による一時的な遮蔽等を受けない位置であること ・SS-RSRP から UE が受信する受信電力が十分であることを確認	図 5-3-3-1
2	【測定】 測定はそれぞれの拠点に個別で実施 ・UE を 1 台のみ RU にアタッチ ・SS-RSRP から UE が受信する受信電力が十分であることを確認 ・ダウンリンク方向(RU→UE)の測定 ・TCP スループット最大値 ・UDP スループット最大値、ジッタ ・ping（遅延時間、パケットロス） ・アップリンク方向(UE→RU)の測定 ・TCP スループット最大値 ・UDP スループット最大値、ジッタ ・ping（遅延時間、パケットロス）	
3	【分析】 複数企業共用パターンのコア＋CU 共用環境および業界共用パターンのコア＋CU 共用環境に対する測定結果を比較 なお、遅延時間の測定に関してはエンド拠点それぞれで実施することでセンタ拠点からエンド拠点までの距離による影響を分析 環境の違いに対して測定値の変動が顕著な場合は、その原因を考察	

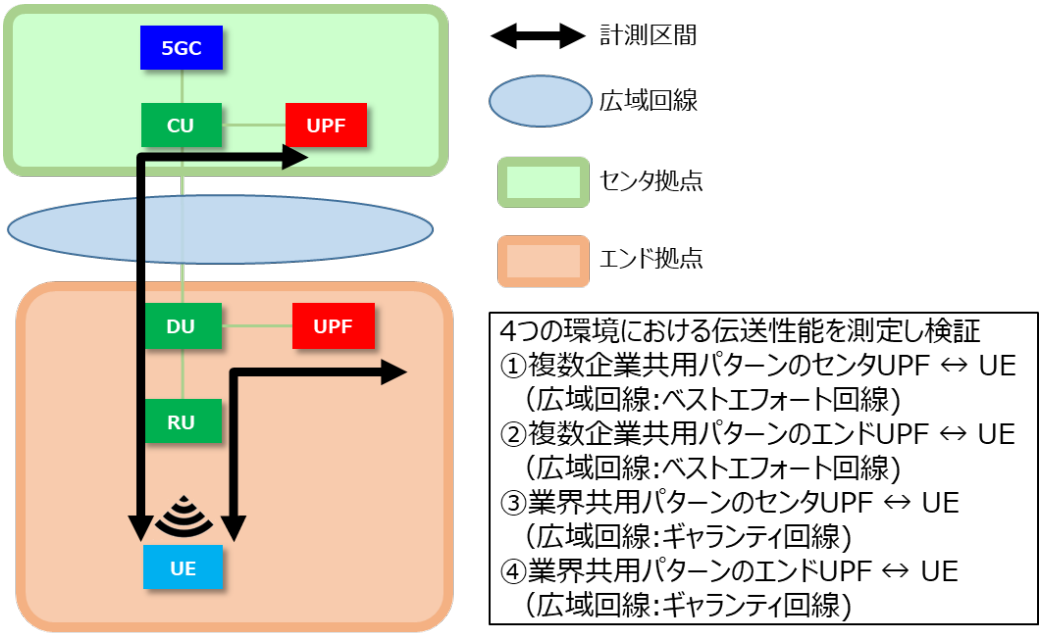


図 5-3-3-1　検証イメージ（各種性能の相関性）

表 5-3-3-3 検証手順（UE 多接続）

項番	実施内容	対応図表
1	【UE エミュレータ接続】 ・RU を停波状態としアンテナ取り外し ・同軸ケーブルを用いて RU アンテナポートに UE エミュレータを接続（減衰器により電力を調整） ・RU から電波発射	図 5-3-3-2
2	【測定】 測定はそれぞれの拠点に個別で実施 UE 接続数は次のパターン ・UE 数　1 台 ・UE 数　10 台 ・UE 数　20 台 ・UE 数　30 台 測定手順は次のとおり ・想定する UE 接続数が全てアタッチしたことを確認 ・認証パケットの使用帯域を測定	
3	【分析】 複数企業共用パターンのコア＋CU 共用環境および業界共用パターンのコア＋CU 共用環境といった環境の変化並びに同時に接続する UE 数について測定結果を比較 環境および UE 数の違いに対して測定値の変動が明らかである場合は、その原因を考察	

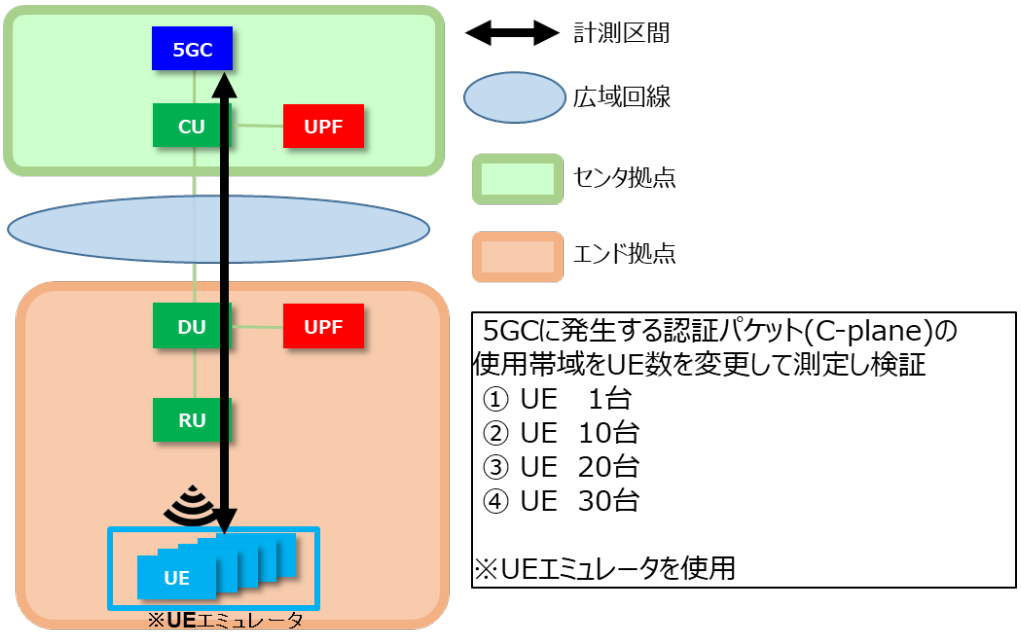


図 5-3-3-2　検証イメージ（UE 多接続）

表 5-3-3-4 検証手順（準同期方式での性能変動）

項番	実施内容	対応図表
1	【UE 接続確認】 検証時、UE を次の条件の位置に設置し、RU と接続 ・RU の主ビーム方向上の位置で RU から見通しがあること ・人体等による一時的な遮蔽等を受けない位置であること ・SS-RSRP から UE が受信する受信電力が十分であることを確認	図 5-3-3-3
2	【測定】 測定はそれぞれの拠点に個別で実施 ・UE を 1 台のみ RU にアタッチ ・SS-RSRP から UE が受信する受信電力が十分であることを確認 ・DL 方向(RU→UE)の測定 ・TCP スループット最大値 ・UDP スループット最大値、ジッタ ・ping（遅延時間、パケットロス） ・UL 方向(UE→RU)の測定 ・TCP スループット最大値 ・UDP スループット最大値、ジッタ ・ping（遅延時間、パケットロス）	
3	【分析】 複数企業共用パターンのコア＋CU 共用環境および業界共用パターンのコア＋CU 共用環境といった環境の変化並びに無線フレームの同期タイミングの違いについて測定結果を比較 環境および無線フレームの同期タイミングの違いに対して測定値の変動が顕著である場合は、その原因を考察	

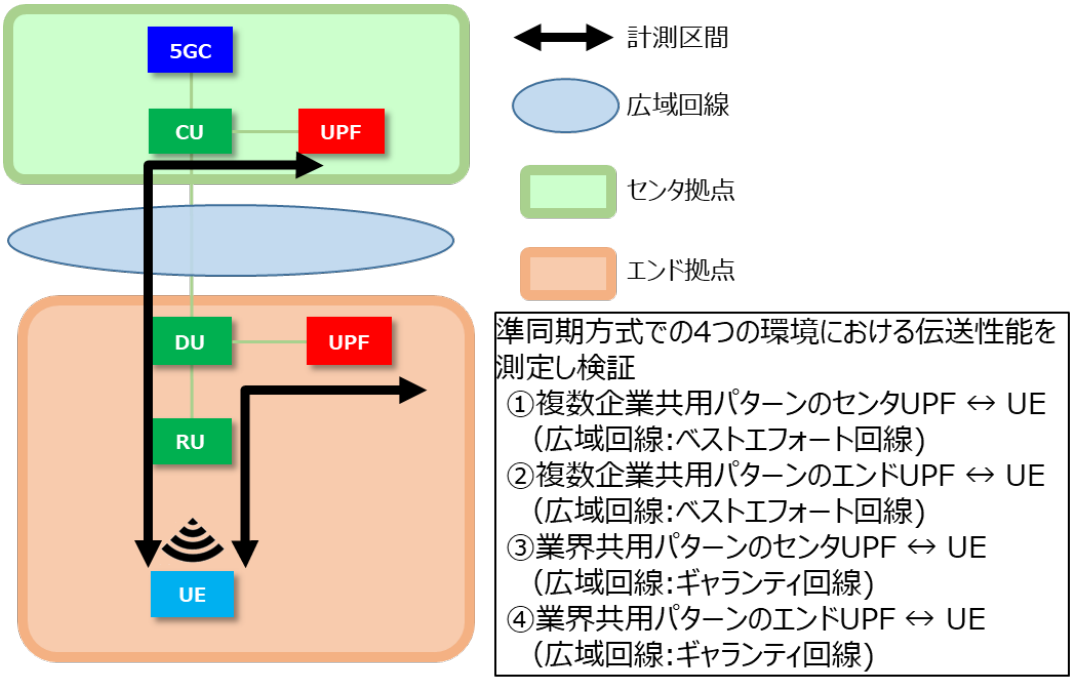


図 5-3-3-3　検証イメージ（準同期方式での性能変動）

(4) 測定結果

評価・検証項目に沿って行った検証結果は下記のとおりです。

① 各種性能の相関性

ア スループット等の比較

スループット、ジッタ、パケットロスの測定結果を「表 5-3-4-①-1 各種性能の相関性（スループット、ジッタ、パケットロス)」にまとめました。

表 5-3-4-①-1 各種性能の相関性（スループット、ジッタ、パケットロス）

エンド拠点	環境	UPF	測定項目	DL/UL	測定値
NTT 中央研修 センタ	複数企業 共用 パターン コア＋CU 共用	センタ UPF	TCP スループット	DL	47.4Mbps
				UL	63.8Mbps
			UDP スループット	DL	224.0Mbps
				UL	65.2Mbps
			ジッタ	DL	1ms 程度
				UL	1ms 程度
			パケットロス※	DL	68.0%
				UL	91.0%
		エンド UPF	TCP スループット	DL	658.0Mbps
				UL	63.5Mbps
			UDP スループット	DL	698.0Mbps
				UL	65.0Mbps
			ジッタ	DL	1ms 程度
				UL	1ms 程度
			パケットロス※	DL	0.2%
				UL	91.0%
	業界共用 パターン コア＋CU 共用	センタ UPF	TCP スループット	DL	159.0Mbps
				UL	63.9Mbps
			UDP スループット	DL	686.0Mbps
				UL	65.1Mbps
			ジッタ	DL	1ms 程度
				UL	1ms 程度
			パケットロス※	DL	2.0%
				UL	91.0%
		エンド UPF	TCP スループット	DL	643.0Mbps
				UL	62.3Mbps
			UDP スループット	DL	700.0Mbps
				UL	65.1Mbps
			ジッタ	DL	1ms 程度
				UL	1ms 程度
			パケットロス※	DL	0.0%
				UL	91.0%

上表において、※ を付したパケットロスにあっては、DL は 700Mbps 送出時のパケットロスの割合を、UL は 300Mbps 送出時のパケットロスの割合を記載。

スループット等について次のとおり比較します。

（ア） TCP/UDP の DL スループット

TCP/UDP の DL スループットについて測定結果を「図 5-3-4-①-1 TCP/UDP の DL スループット比較」に図示します。

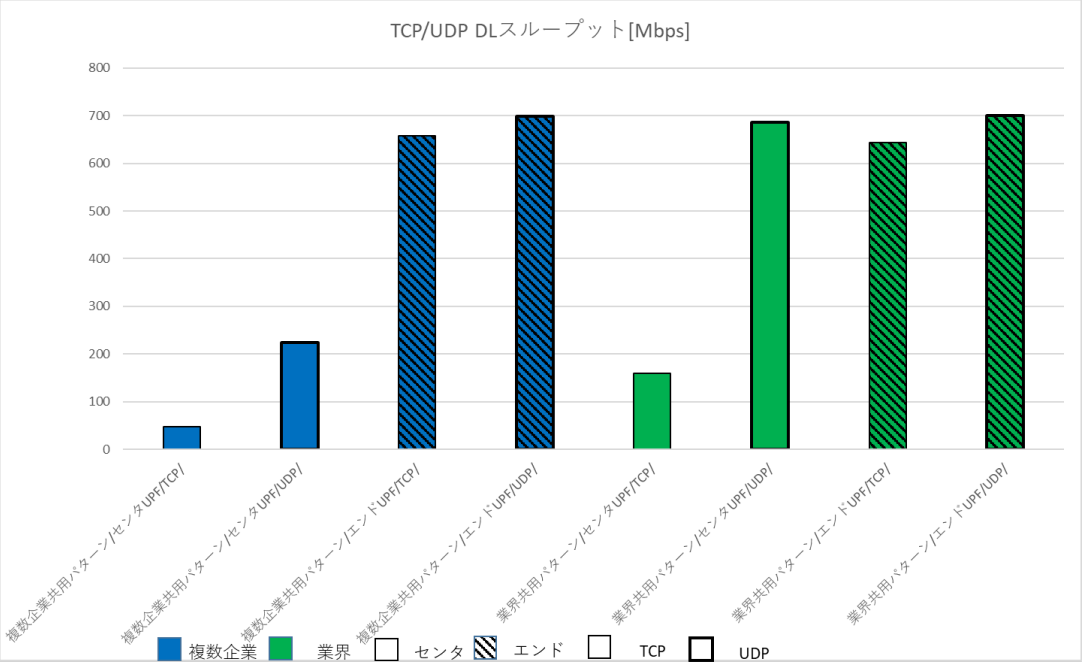


図 5-3-4-①-1 TCP/UDP の DL スループット比較

TCP/UDP の DL スループットについて測定結果を比較すると、エンド UPF 構成の場合には複数企業共用パターンで TCP/UDP：658Mbps/698Mbps、業界共用パターンで TCP/UDP：643Mbps/700Mbps と、双方で高い DL スループットを実測することができました。一方、センタ UPF 構成の場合には業界共用パターンでは TCP/UDP：159Mbps/686Mbps と TCP の DL スループットが低下し、複数企業共用パターンでは TCP/UDP：47Mbps/224Mbps であり TCP/UDP 両方の DL スループットが大きく低下しています。

エンド UPF 構成の場合は UE～RU～DU～エンド UPF という比較的シンプルな構成であるため、スループットを低下させる要素が最小限であることで、複数企業共用パターンおよび業界共用パターンの双方で高い DL スループットを実測できたといえます。

業界共用パターンのセンタ UPF の場合は UE～RU～DU～ギャランティ回線～CU～センタ UPF という構成であり、エンド UPF と比較して経由する機器の増加等によって TCP の DL スループットが影響を受け、エンド UPF よりも DL スループットが低下したものと考えます。

複数企業共用パターンのセンタ UPF の場合は UE～RU～DU～ベストエフォート回線～CU～センタ UPF という構成であり、業界共用パターンと同様に機器の増加等による影響に加えてベストエフォート回線の区間は通信の伝送帯域・速度が保証されないことから、TCP/UDP の両方の DL スループットが大きく制限され、比較的低い DL スループットという結果になったものと考えます。

（イ）　TCP/UDP の UL スループット

TCP/UDP の UL スループットについて測定結果を「図 5-3-4-①-2　TCP/UDP の UL スループット比較」に図示します。

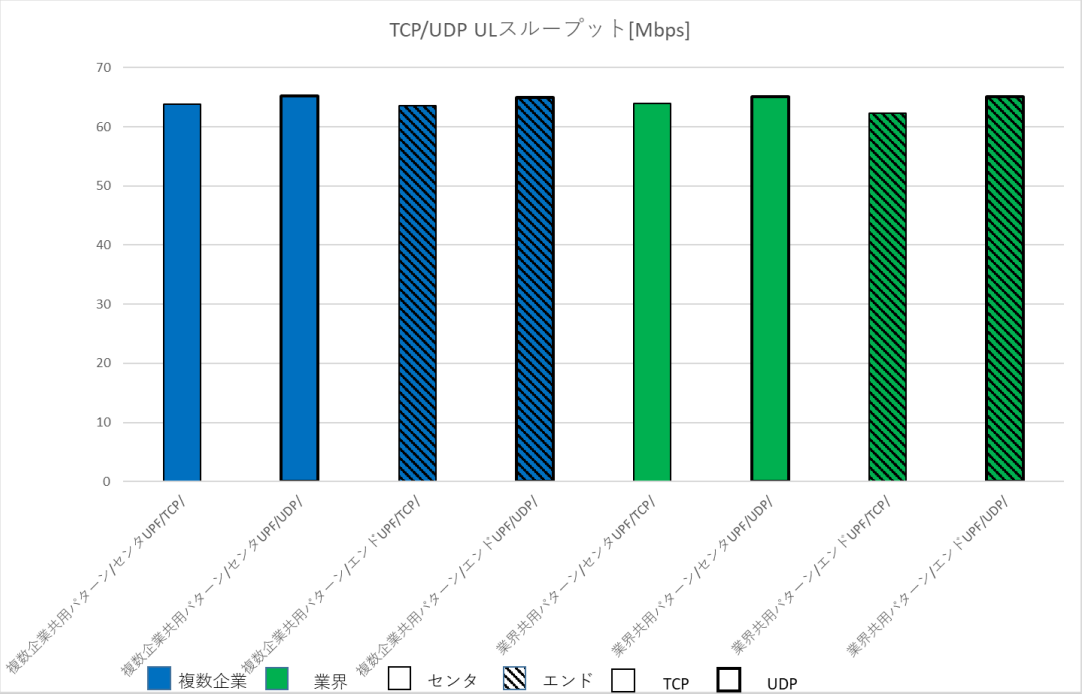


図 5-3-4-①-2　TCP/UDP の UL スループット比較

TCP/UDP の UL スループットについて測定結果を比較すると、複数企業共用パターンのセンタ UPF 構成で TCP/UDP：63.8Mbps/65.2Mbps、複数企業共用パターンのエンド UPF 構成で TCP/UDP ： 63.5Mbps/65.0Mbps 、 業 界 共 用 パ タ ー ン の セ ン タ UPF 構 成 で TCP/UDP ： 63.9Mbps/65.1Mbps、業界共用パターンのエンド UPF 構成で TCP/UDP:62.3Mbps/65.1Mbps と、どの組み合わせもほぼ同程度の UL スループットを実測できました。これは本検証の環境下では 65Mbps 程度の UL スループットが構成によらず許容できたためといえます。ただし、前述のとおり、複数企業共用パターンのセンタ UPF 構成の場合は通信の伝送帯域・速度が保証されないベストエフォート回線を経由するため、その回線種別がタイミング次第で UL スループットのパフォーマンスに影響を及ぼすことがあると考えます。

（ウ）　ジッタ

ジッタについて測定結果を比較すると、複数企業共用パターンおよび業界共用パターン並びにセンタ UPF およびエンド UPF のいずれの組み合わせであっても 1ms 程度のジッタでした。ジッタは通信上のゆらぎを表す項目として測定しました。本検証では大きくゆらぎを発生させる構成がなかったといえます。

（エ）　パケットロス

パケットロスについて測定結果を「図 5-3-4-①-3　パケットロス比較」に図示します。

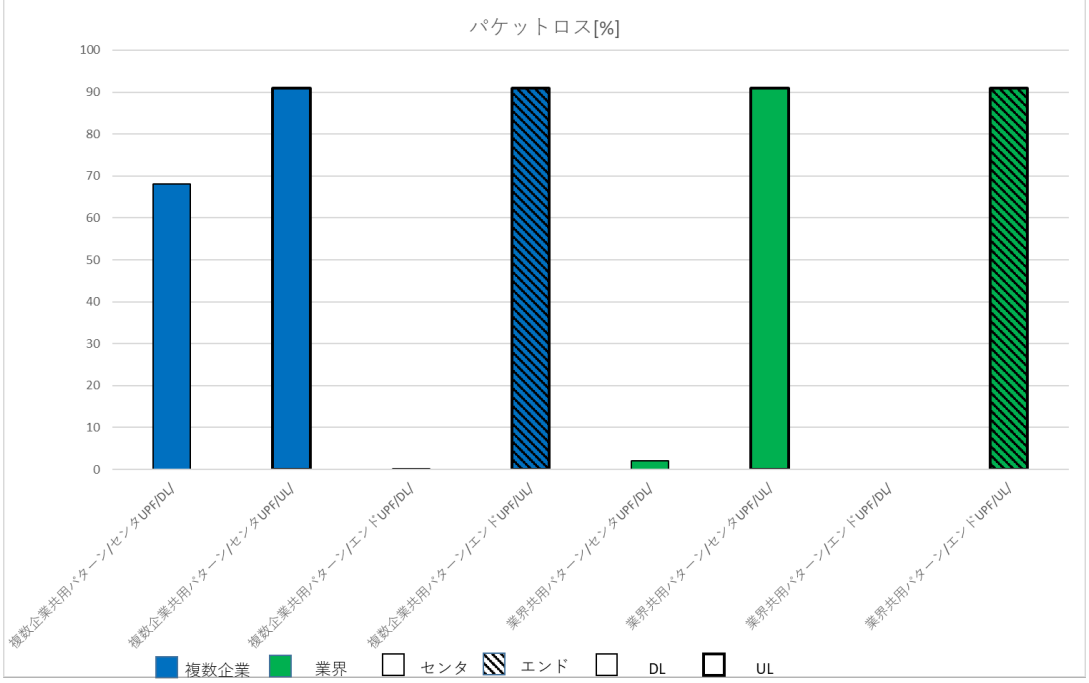


図 5-3-4-①-3　パケットロス比較

本検証では DL パケットロスは 700Mbps でパケットを UDP で送出した場合のパケットロスを測定し、UL パケットロスは 300Mbps でパケットを UDP で送出した場合のパケットロスを測定しました。エンド UPF 構成の場合には複数企業共用パターンで 0.2%、業界共用パターンで 0.0%とほぼ DL パケットロスが発生していない結果を実測することができました。一方、センタ UPF 構成の場合には業界共用パターンでは 2.0%とやや DL パケットロスが発生し、複数企業共用パターンでは 68%と明らかに DL パケットロスが大きくなっています。

DL パケットロスの結果の違いは前述した DL スループットの違いと完全に一致しています。エンド UPF というシンプルな構成に対するギャランティ回線を経由する影響あるいはベストエフォート回線を経由する影響によって生じたものと考えます。

また UL パケットロスは複数企業共用パターンおよび業界共用パターン並びにセンタ UPF およびエンド UPF のいずれの組み合わせであっても 91.0%でした。これは UL スループットで述べたように、本検証の環境下では 65Mbps 程度の UL スループットが構成によらず許容できたためといえます。

イ　遅延時間の比較

遅延時間の測定結果を「表 5-3-4-①-2　各種性能の相関性（遅延時間）」にまとめました。

表 5-3-4-①-2　各種性能の相関性（遅延時間）

エンド拠点	環境	UPF	測定項目	測定値[ms]
NTT 中央研修センタ	複数企業共用パターン コア＋CU 共用	センタ UPF	遅延時間	42
		エンド UPF	遅延時間	28
	業界共用パターン コア＋CU 共用	センタ UPF	遅延時間	33
		エンド UPF	遅延時間	29
いすゞ自動車	複数企業共用パターン コア＋CU 共用	センタ UPF	遅延時間	47
		エンド UPF	遅延時間	28
東北大学	業界共用パターン コア＋CU 共用	センタ UPF	遅延時間	32
		エンド UPF	遅延時間	28
東京大学	業界共用パターン コア＋CU 共用	センタ UPF	遅延時間	26
		エンド UPF	遅延時間	26
京都大学	業界共用パターン コア＋CU 共用	センタ UPF	遅延時間	38
		エンド UPF	遅延時間	29

遅延時間について測定結果を「図 5-3-4-①-4　遅延時間比較」に図示します。

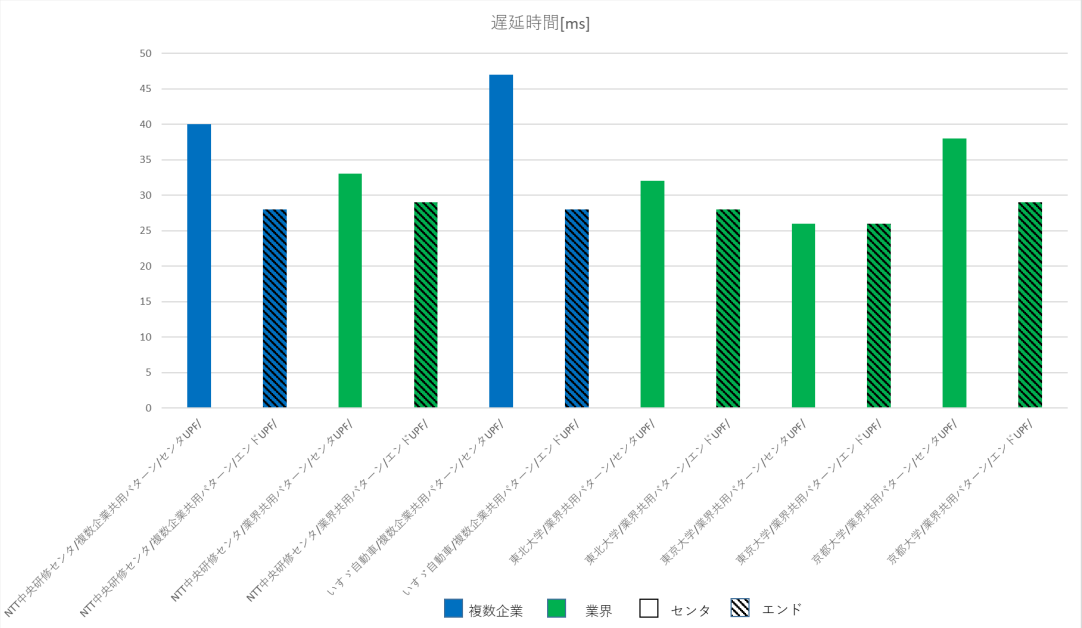


図 5-3-4-①-4　遅延時間比較

複数企業パターンの NTT 中央研修センタおよびいすゞ自動車について比較すると、それぞれのセンタ UPF 環境での遅延時間がエンド UPF 環境と比べて 10ms 以上大きい結果でした。R3 年度でも複数企業パターンではセンタ UPF 環境はエンド UPF 環境と比較して、約 5ms～11ms の遅延時間が劣化している結果であり、複数企業パターンにおいて広域回線として使用しているベストエフォート回線による伝送遅延であると考察しています。本検証においても R3 年度と同様にベストエフォート回線による伝送遅延が見られたものと考えます。またセンタ UPF 環境での遅延時間はいすゞ自動車の方が NTT 中央研修センタより大きい結果でした。これはセンタ拠点（東京都豊島区）からいすゞ自動車（神奈川県藤沢市）までの物理的な距離が NTT 中央研修センタ（東京都調布市）よりも遠いためであると考えます。

業界共用パターンの NTT 中央研修センタ、東北大学、東京大学および京都大学についてセンタ UPF 環境における遅延時間を比較します。東京大学はセンタ UPF 環境での遅延時間が 26ms と最も短く、同拠点のエンド UPF 環境での遅延時間と同程度です。東京大学（東京都文京区）からセンタ拠点（東京都豊島区）の物理的な距離が近く広域回線による伝送遅延の影響 をほぼ受けなかったため、センタ UPF 環境とエンド UPF 環境で差が生じなかったものと考えます。次に東北大学および NTT 中央研修センタはセンタ UPF 環境での遅延時間が 32～33ms とほとんど差がありませんでした。ベストエフォート回線を使用する複数企業共用パターンではセンタ拠点からの距離が遠い拠点で遅延時間が大きくなる傾向にありましたが、ギャランティ回線を使用する業界共用パターンでは NTT 中央研修センタ（東京都調布市）と東北大学（宮城県仙台市）のセンタ拠点からの距離の差に対してその傾向が見られませんでした。これはギャランティ回線がベストエフォート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。しかし京都大学の遅延時間は 38ms と業界共用パターンの中で最も大きく、ギャランティ回線によっても伝送遅延が発生したものと考えます。京都大学（京都府京都市）からセンタ拠点までの物理的な距離が直線で約 370km と最も遠いことに加え、センタ拠点が東日本エリアに、京都大学が西日本エリアにあるため、エリアをまたぐことによる伝送遅延が発生したものと考えます。

またエンド UPF 環境では複数企業パターンおよび業界共用パターンに区別なく遅延時間は30ms 未満であり、いずれの拠点でもセンタ UPF 環境以下という結果でした。

② UE 多接続

UE が多数接続した場合に C-plane がどれだけのスループットを発生させるかを測定しました。Linux コマンドを用いて 5GC の通信ポートのパケットキャプチャを行い、Wireshark を用いてスループットをグラフ化しました。以下に測定結果を示します。

ア　複数企業共用パターン

（ア）　UE1 台の場合

パケットキャプチャからグラフ化した C-plane スループットを「図 5-3-4-②-1　複数企業共用パターン　UE1 台接続」に示します。

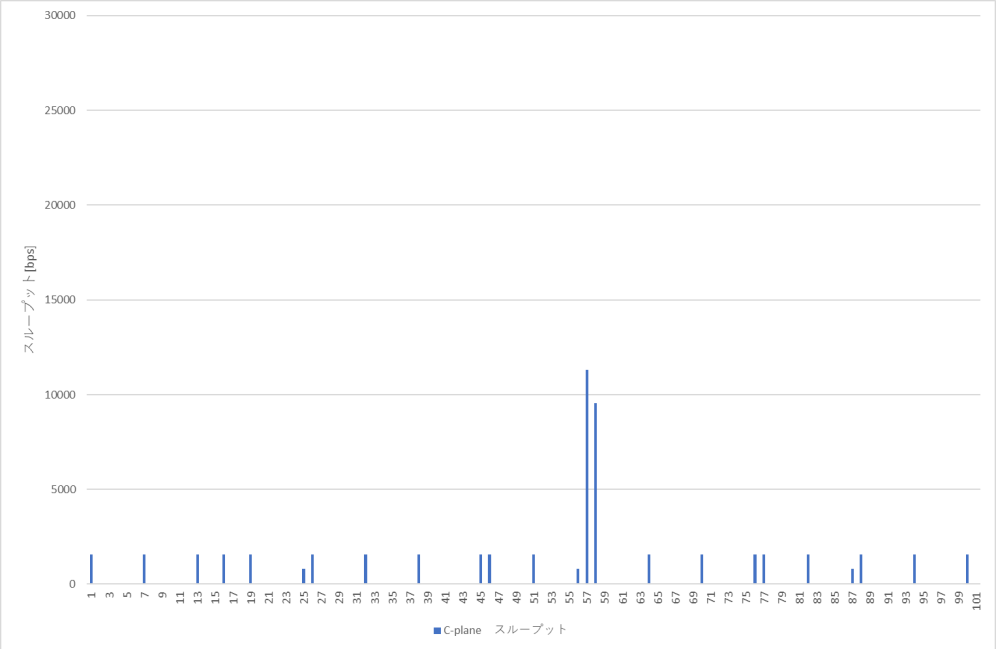


図 5-3-4-②-1　複数企業共用パターン　UE1 台接続

ピークとして 11,296bps=12kbps 程度のスループットが確認できました。これは UE アタッチ時に発生した C-plane 通信です。またアタッチの処理以外で一定の間隔で 1,568bps=1.6kbps 程度のスループットが発生していました。

（イ）　UE10 台の場合

パケットキャプチャからグラフ化した C-plane スループットを「図 5-3-4-②-2　複数企業共用パターン　UE10 台接続」に示します。

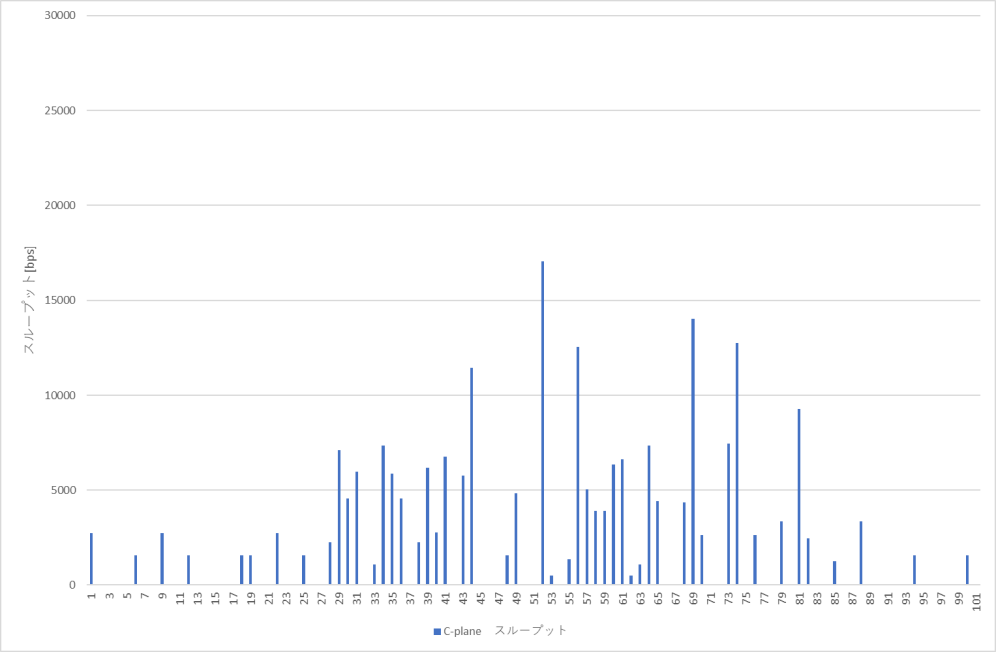


図 5-3-4-②-2　複数企業共用パターン　UE10 台接続

ピークとして 17,040bps=17kbps 程度のスループットが確認できたほか、5,000bps=5kbps～15,000bps=15kbps の間で散逸的にスループットが発生しています。それぞれが 10 台の UE が順次アタッチした時に発生した C-plane 通信です。

（ウ）　UE20 台の場合

パケットキャプチャからグラフ化した C-plane スループットを「図 5-3-4-②-3　複数企業共用パターン　UE20 台接続」に示します。

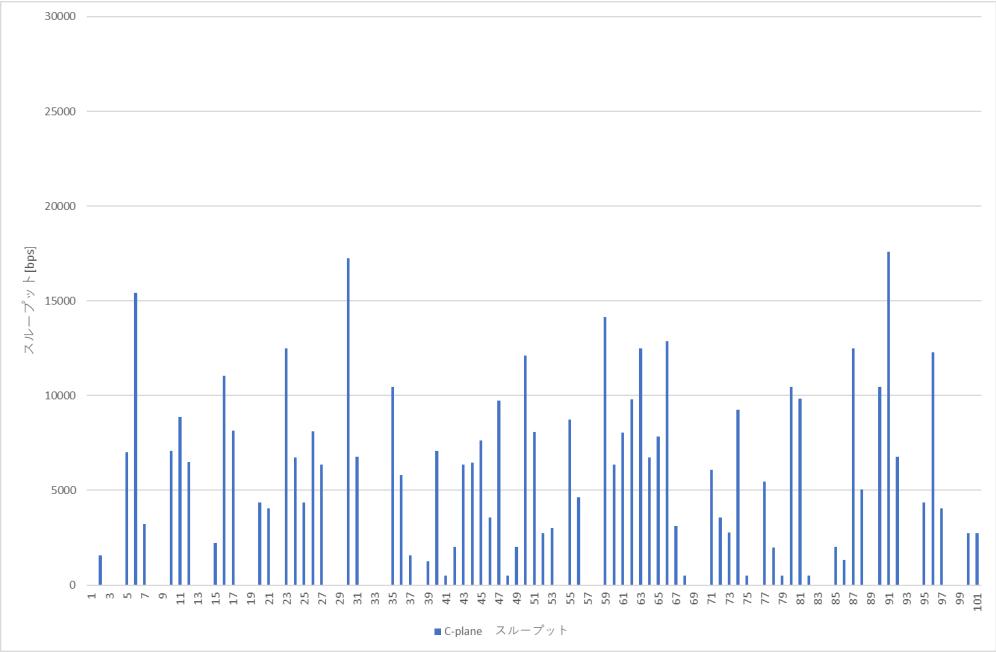


図 5-3-4-②-3　複数企業共用パターン　UE20 台接続

ピークとして 17,584bps=18kbps 程度のスループットが確認できたほか、5,000bps=5kbps～15,000bps=15kbps の間で散逸的にスループットが発生しています。それぞれが 20 台の UE が順次アタッチした時に発生した C-plane 通信です。UE 数が増えたことに対して、使用する帯域はそれほど変動していないと考えます。

（エ）　UE30 台の場合

パケットキャプチャからグラフ化した C-plane スループットを「図 5-3-4-②-4　複数企業共用パターン　UE30 台接続」に示します。

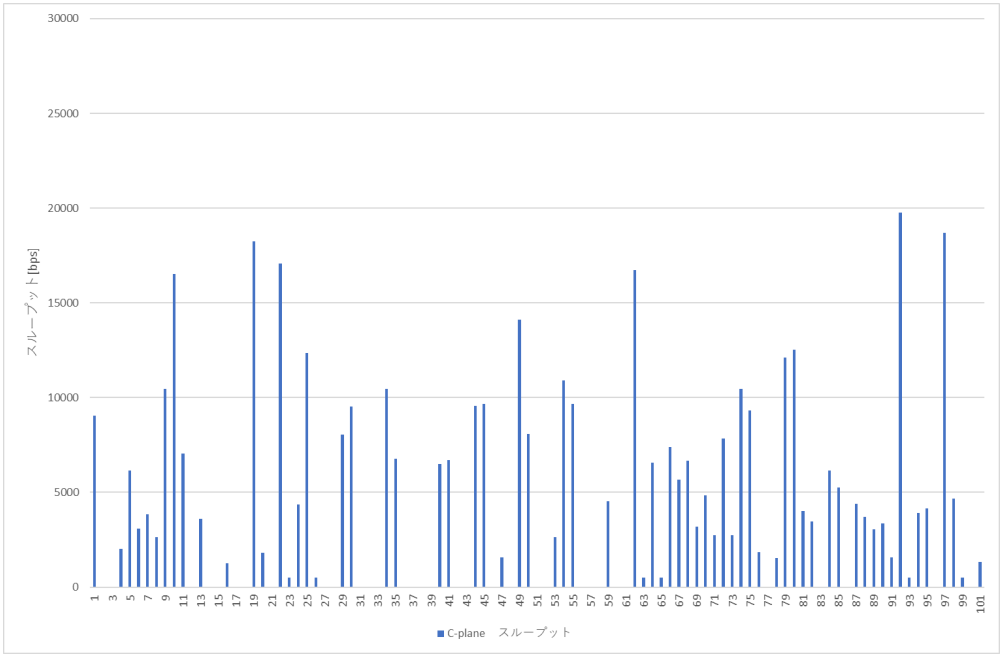


図 5-3-4-②-4　複数企業共用パターン　UE30 台接続

ピークとして 19,776bps=20kbps 程度のスループットが確認できたほか、5,000bps=5kbps～18,000bps=18kbps の間で散逸的にスループットが発生しています。それぞれが 30 台の UE が順次アタッチした時に発生した C-plane 通信です。アタッチするタイミングが重なったことでピークの値はやや増えたものの、使用する帯域としてはそれほど変動していないと考えます。

イ　業界共用パターン

（ア）　UE1 台の場合

パケットキャプチャからグラフ化した C-plane スループットを「図 5-3-4-②-5　業界共用パターン　UE1 台接続」に示します。

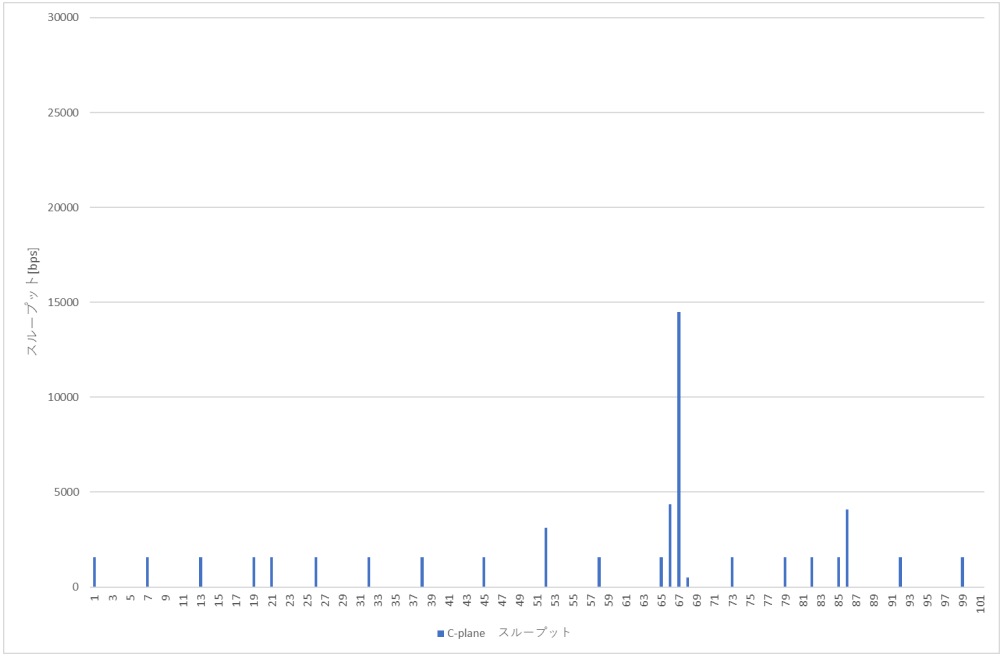


図 5-3-4-②-5　業界共用パターン　UE1 台接続

ピークとして 14,480bps=15kbps 程度のスループットが確認できました。これは UE アタッチ時に発生した C-plane 通信です。またアタッチの処理以外で一定の間隔で 1,568bps=1.6kbps 程度のスループットが発生していました。複数企業共用パターンとほぼ同様の結果といえます。

（イ）　UE10 台の場合

パケットキャプチャからグラフ化した C-plane スループットを「図 5-3-4-②-6　業界共用パターン　UE10 台接続」に示します。

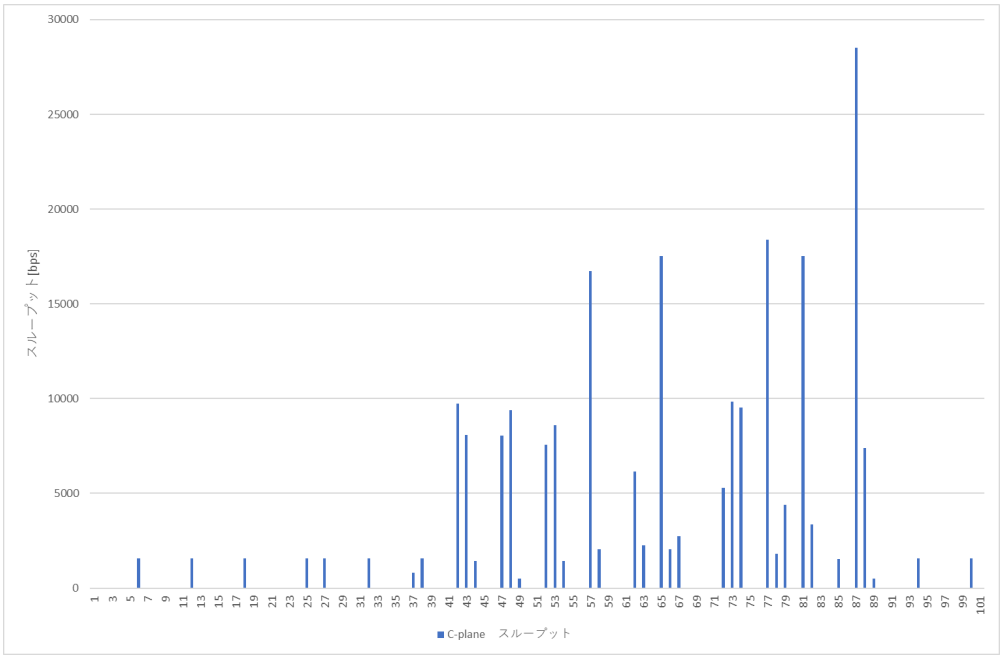


図 5-3-4-②-6　業界共用パターン　UE10 台接続

ピークとして 28,528bps=29kbps 程度のスループットが確認できました。これは UE アタッチ時に発生した C-plane 通信です。アタッチするタイミングが重なったことでピークの値が増えていますが、複数企業共用パターンとほぼ同様の結果といえます。

（ウ）　UE20 台の場合

パケットキャプチャからグラフ化した C-plane スループットを「図 5-3-4-②-7　業界共用パターン　UE20 台接続」に示します。

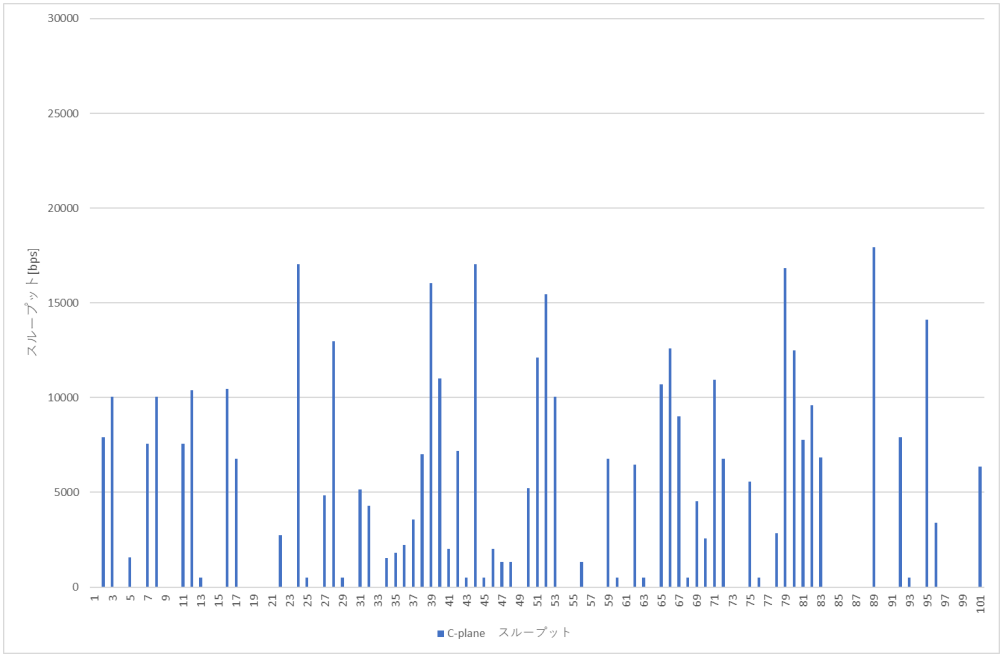


図 5-3-4-②-7　業界共用パターン　UE20 台接続

ピークとして 17,920bps=18kbps 程度のスループットが確認できました。それぞれが 20 台の UE が順次アタッチした時に発生した C-plane 通信です。UE 数が増えたことに対して、使用する帯域はそれほど変動していないと考えます。複数企業共用パターンとほぼ同様の結果といえます。

（エ）　UE30 台の場合

パケットキャプチャからグラフ化した C-plane スループットを「図 5-3-4-②-8　業界共用パターン　UE30 台接続」に示します。

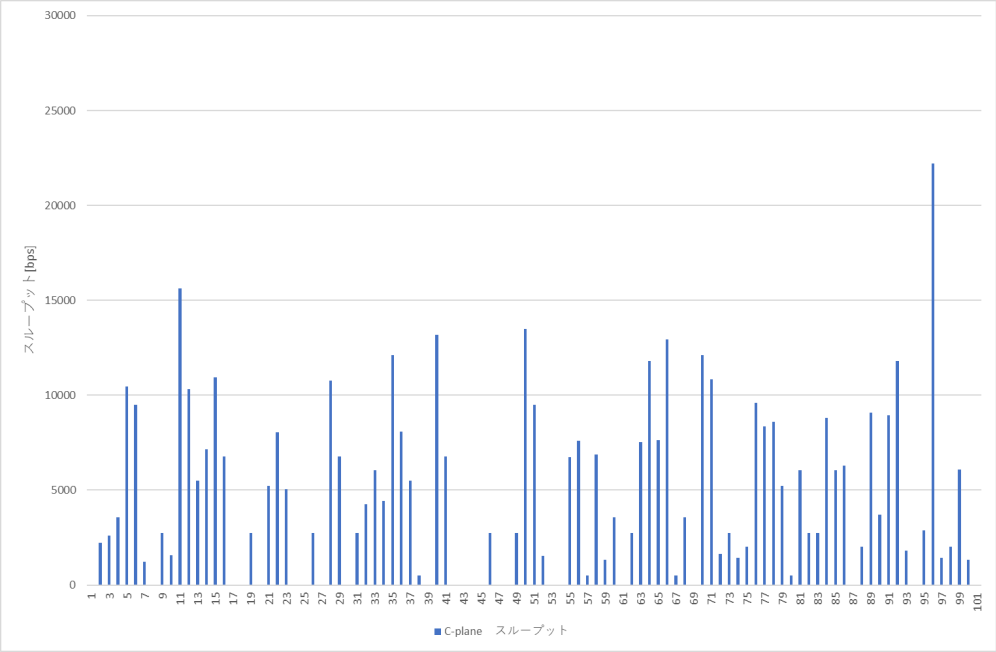


図 5-3-4-②-8　業界共用パターン　UE30 台接続

ピークとして 22,224bps=22kbps 程度のスループットが確認できたほか、5,000bps=5kbps～20,000bps=20kbps の間で散逸的にスループットが発生しています。それぞれが 30 台の UE が順次アタッチした時に発生した C-plane 通信です。アタッチするタイミングが重なったことでピークの値はやや増えたものの、使用する帯域としてはそれほど変動していないと考えます。複数企業共用パターンと同様の結果であるといえます。

ウ　使用する帯域のピーク値の比較

アおよびイで示した各グラフのピーク値を「表 5-3-4-②-1　スループットピーク値の比較」にまとめました。

表 5-3-4-②-1　スループットピーク値の比較

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

アタッチのタイミングが重なることでピーク値に変動がみられるものの、最大ピーク値は 30kbps に満たない数値でした。このことから本検証の環境下では複数企業共用パターンと業界共用パターンの別並びに接続する UE 数の変動は、C-plane に使用する帯域に大きな影響を与えないものと考えます。

③　準同期方式での性能変動

測定結果を「表 5-3-4-③-1　準同期方式での性能変動」にまとめました。

表 5-3-4-③-1　準同期方式での性能変動

エンド拠点	環境	UPF	測定項目	DL/UL	測定値
NTT 中央研修 センタ	複数企業 共用 パターン コア＋CU 共用	センタ UPF	TCP スループット	DL	53.4Mbps
				UL	95.1Mbps
			UDP スループット	DL	227Mbps
				UL	130Mbps
			遅延時間		34ms
			ジッタ	DL	1ms 程度
				UL	1ms 程度
			パケットロス	DL	68.0%
				UL	66.0%
		エンド UPF	TCP スループット	DL	546Mbps
				UL	117Mbps
			UDP スループット	DL	569Mbps
				UL	130Mbps
			遅延時間		28ms
			ジッタ	DL	1ms 程度
				UL	1ms 程度
			パケットロス	DL	19.0%
				UL	61.0%
	業界共用 パターン コア＋CU 共用	センタ UPF	TCP スループット	DL	124Mbps
				UL	128Mbps
			UDP スループット	DL	539Mbps
				UL	130Mbps
			遅延時間		31ms
			ジッタ	DL	1ms 程度
				UL	1ms 程度
			パケットロス	DL	23.0%
				UL	66.0%
		エンド UPF	TCP スループット	DL	390Mbps
				UL	128Mbps
			UDP スループット	DL	552Mbps
				UL	130Mbps
			遅延時間		27ms
			ジッタ	DL	1ms 程度
				UL	1ms 程度
			パケットロス	DL	21.0%
				UL	66.0%

上記の結果について、(4)①および②で測定した同期方式の性能と比較しました。

ア　TCP　DL スループットの比較

TCP　DL スループットについて同期方式および準同期方式の結果を「図 5-3-4-③-1　TCP DL スループット比較」に図示します。

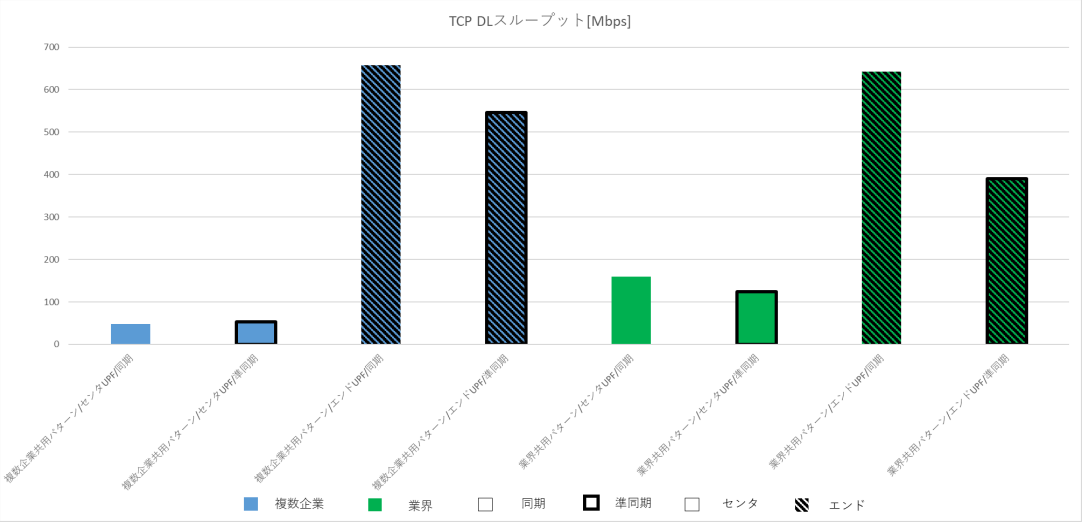


図 5-3-4-③-1　TCP DL スループット比較

TCP の DL スループットについて測定結果を比較すると、複数企業共用パターンのセンタ UPF の場合には同期/準同期：47.4Mbps/53.4Mbps とほとんど変化していませんでした。しかし、複数企業共用パターンのエンド UPF では同期/準同期：658Mbps/546Mbps、業界共用パターンのセンタ UPF では同期/準同期：159Mbps/124Mbps、業界共用パターンのエンド UPF では同期/準同期：643Mbps/390Mbps と 3 割程度の低下を確認できました。

複数企業共用パターンのセンタ UPF の場合は通信の伝送帯域・速度が保証されないベストエフォート回線の区間を受けたため、同期方式でも DL スループットが大きく制限されており、準同期方式へ切り替えたことによる低下が見られなかったものと考えます。

イ　UDP　DL スループットの比較

UDP　DL スループットについて同期方式および準同期方式の結果を「図 5-3-4-③-2　UDP DL スループット比較」に図示します。

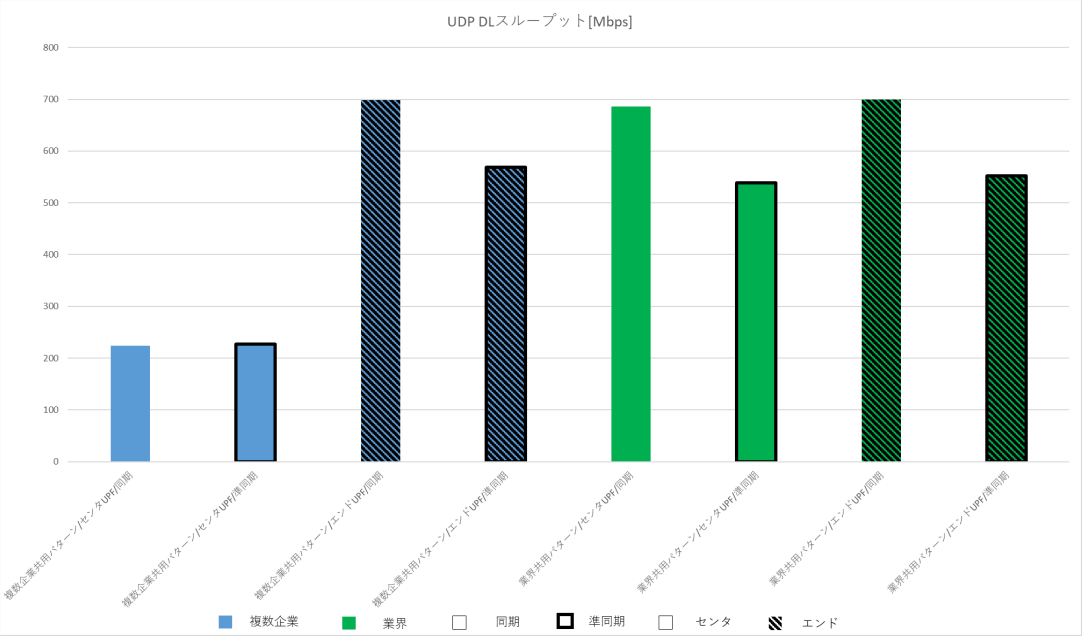


図 5-3-4-③-2　UDP DL スループット比較

UDP の DL スループットについて測定結果を比較すると、複数企業共用パターンのセンタ UPF の場合には同期/準同期：224Mbps/227Mbps とほとんど変化していませんでした。しかし、複数企業共用パターンのエンド UPF では同期/準同期：698Mbps/569Mbps、業界共用パターンのセンタ UPF では同期/準同期：686Mbps/539Mbps、業界共用パターンのエンド UPF では同期/準同期：700Mbps/552Mbps と 2 割程度の低下を確認できました。

複数企業共用パターンのセンタ UPF の場合は TCP の DL スループットと同様にベストエフォート回線による低下が見られなかったものと考えます。

ウ　UL スループットの比較

TCP/UDP　UL スループットについて同期方式および準同期方式の結果を「図 5-3-4-③-3 UL スループット比較」に図示します。

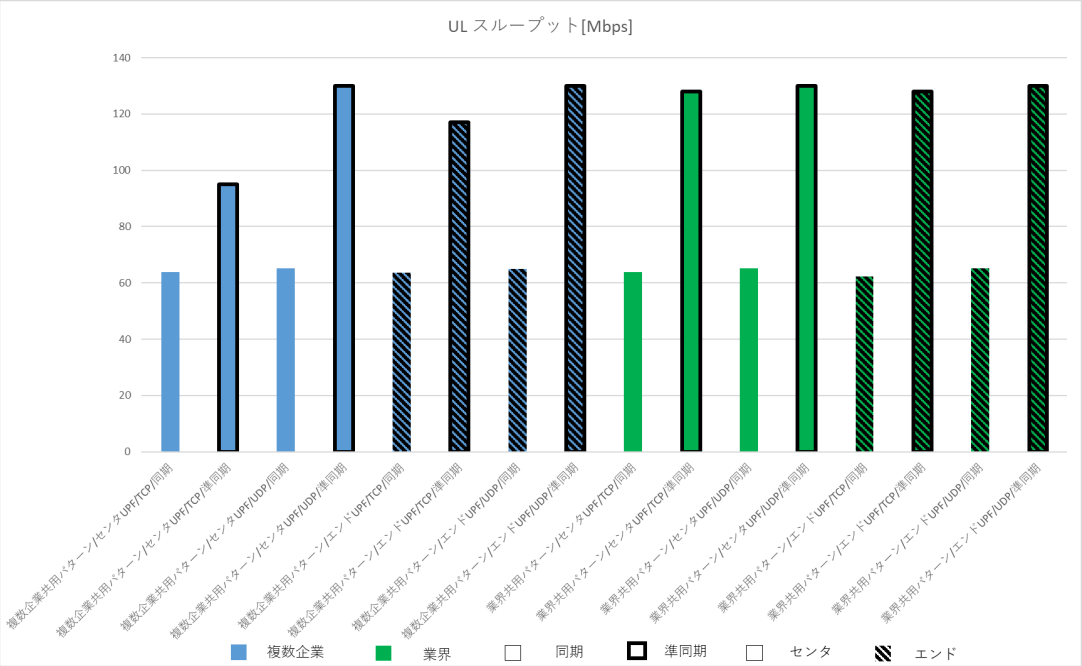


図 5-3-4-③-3　UL スループット比較

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

エ　遅延時間の比較

遅延時間について同期方式および準同期方式の結果を「図 5-3-4-③-4　遅延時間比較」に図示します。

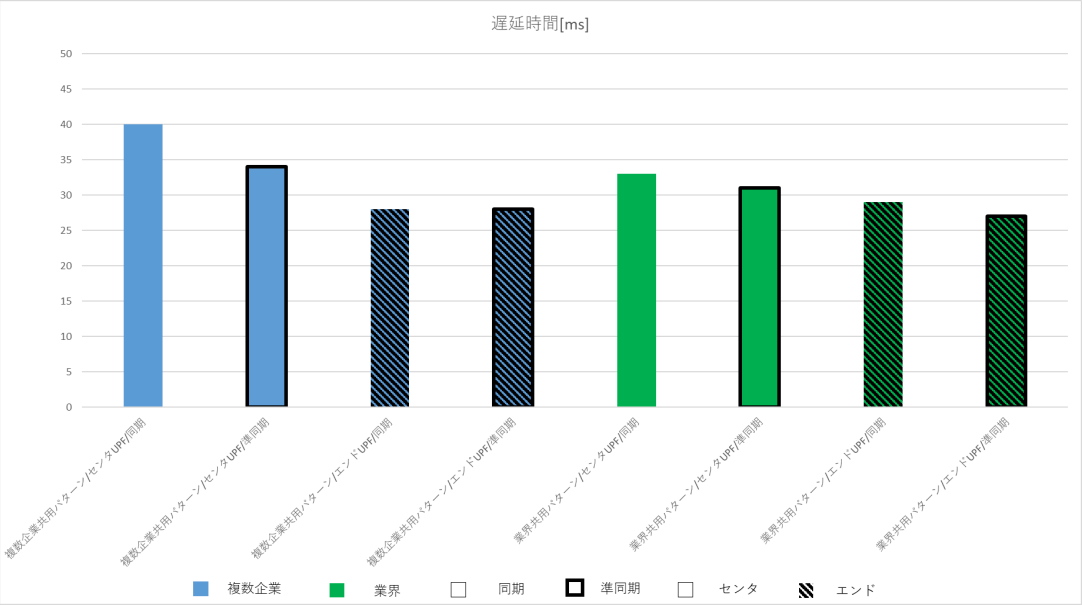


図 5-3-4-③-4　遅延時間比較

遅延時間について測定結果を比較します。同期方式の遅延時間よりも準同期方式の遅延時間がやや小さくなる結果でした。最も大きく差が表れたのは複数企業パターンのセンタ UPF 環境で、8ms の差でした。この環境ではベストエフォート回線の影響によっての遅延時間事態が最も大きい結果であり、同期方式と準同期方式の差が大きく出たこともベストエフォート回線の影響と考えます。そのほかの環境では 4ms 以下の差であり、同期方式と準同期方式の違いによる遅延時間の差はほぼないものと考えます。

ジッタも同様にすべての結果が 1ms 程度であるため、環境および同期方式/準同期方式の違いはネットワークのゆらぎに影響していないと考えます。

オ　DL パケットロスの比較

DL パケットロスについて同期方式および準同期方式の結果を「図 5-3-4-③-5　DL パケットロス比較」に図示します。

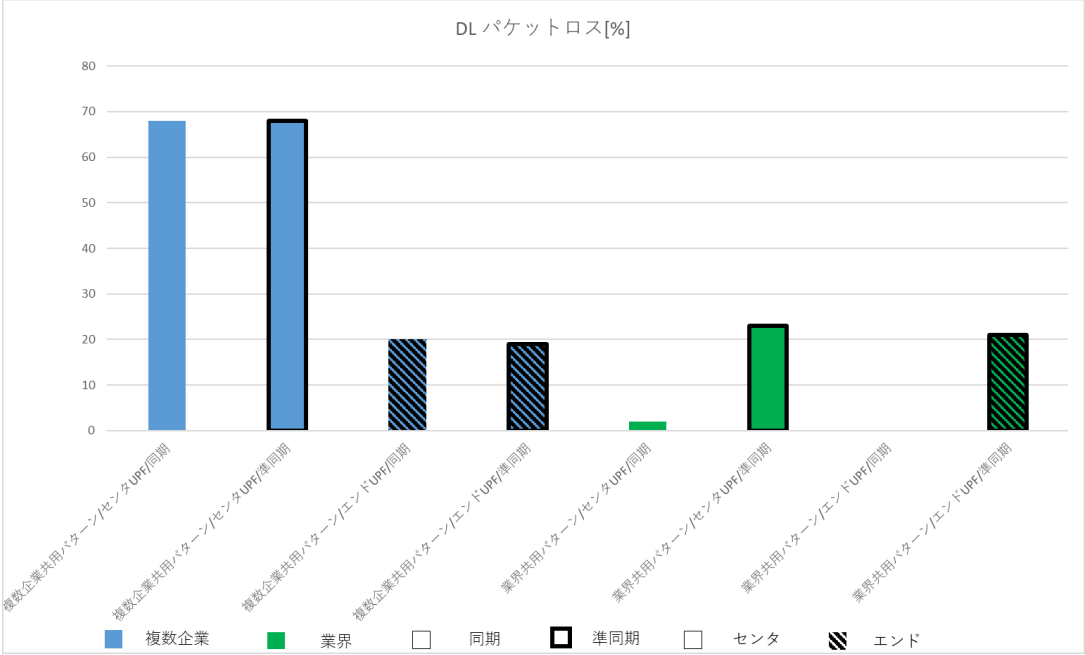


図 5-3-4-③-5　DL パケットロス比較

本検証では DL パケットロスは 700Mbps でパケットを UDP で送出した場合のパケットロスを測定しました。複数企業共用パターンのセンタ UPF 環境を除き、パケットロスは準同期方式の方が同期方式よりも上昇しています。この結果は DL スループットの結果と一致しています。複数企業共用パターンのセンタ UPF 環境はベストエフォート回線によって帯域が制限されたことが考えられます。そのため同期方式の時点からパケットロスが高い結果となり、準同期方式に切り替えたことによるパケットロスの変動が見られなかったものといえます。

カ　UL パケットロスの比較

UL パケットロスについて同期方式および準同期方式の結果を「図 5-3-4-③-6　UL パケットロス比較」に図示します。

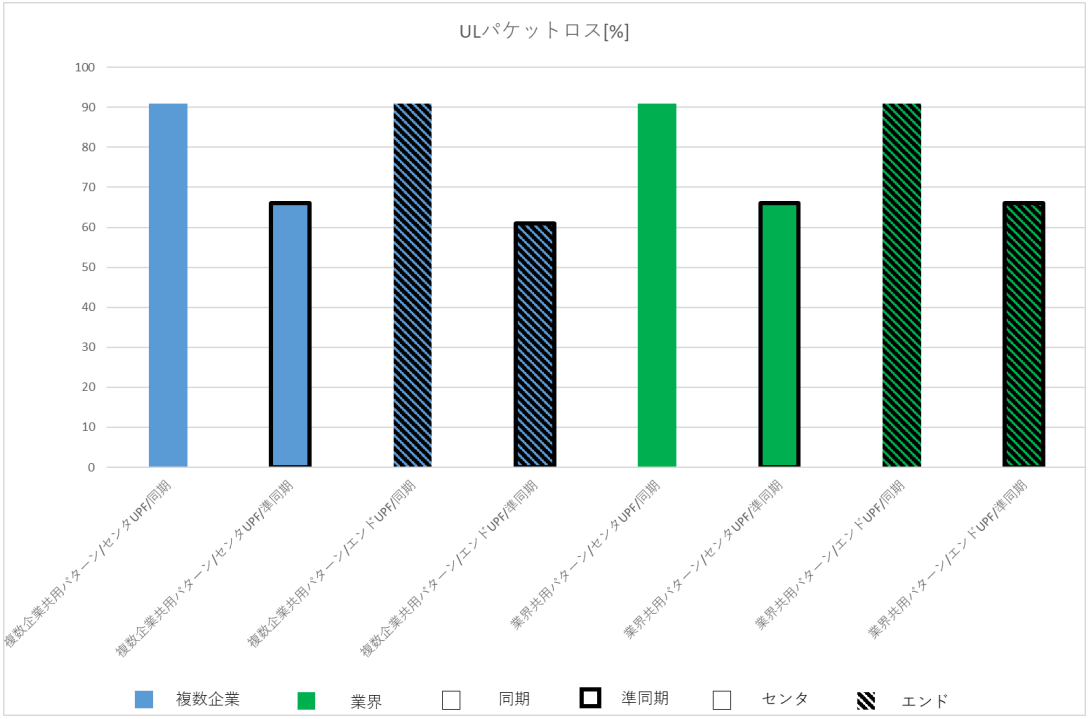


図 5-3-4-③-6　UL パケットロス比較

本検証では UL パケットロスは 300Mbps でパケットを UDP で送出した場合のパケットロスを測定しました。複数企業共用パターンおよび業界共用パターンの別並びにセンタ UPF およびエンド UPF の別に関係なく、同期方式に比べて準同期方式の方でパケットロスが減少しています。この結果は UL スループットの結果と一致します。

(5) 考察

ア　各種性能の相関性

（ア）　伝送性能（スループットおよびパケットロス）について

R3 年度の検証ではコアのみを共用した環境を構築し、複数企業共用パターン（ベストエフォート回線）/業界共用パターン(ギャランティ回線)の別並びにセンタ UPF/エンド UPF の別といった環境の違いによらず、当時のユースケース所要性能を満たすスループット 15Mbps 以上が測定されました。環境の違いに影響されず一定のスループットを発揮したことで、伝送スループットの所要性能が高いユースケースには R3 年度で使用した無線機等のスペックでは満たせないこと、その場合に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しています。

本検証で使用した無線機は R3 年度より伝送性能が向上しており、同期方式において UDP の DL は約 700Mbps、UL は約 65Mbps という性能を実力値として有してします。検証の結果、複数企業共用パターンのエンド UPF 環境、業界共用パターンのセンタ UPF 環境および業界共用パターンのエンド UPF 環境において、ほぼ実力値に匹敵する性能を測定できました。以上の結果から、コア共用並びにコアおよび CU の共用という構成によってローカル５Ｇシステムのスループットの性能が劣化するものではないことを確認できたものと考えます。

一方、複数企業パターンのセンタ UPF 環境では DL が約 220Mbps まで制限されました。

こうしたスループットの制限は R3 年度の 15Mbps 程度と比較的小さいスループットの検証下では見られませんでした。しかし、本検証で使用した無線機は R3 年度と比べて性能が向上しており、DL は最大で 700Mbps という性能でした。複数企業パターンのセンタ UPF 環境では DL が約 220Mbps まで制限されたことは、無線機の高いスループット伝送する性能に対して、複数企業共用パターンで使用するベストエフォート回線によってスループットが制限されることを確認できたものと考えます。この結果からコア等を共用する構成でセンタ UPF を利用する環境の場合は、センタ拠点～エンド拠点の広域回線の種別によってスループットに影響を受ける場合があり、高いスループットを要求するユースケースの場合は所要性能を元に広域回線の種別を選択する必要があるものと考えます。

（イ）　遅延時間について

R3 年度の検証ではコアのみを共用した環境を構築し、複数企業共用パターン（ベストエフォート回線）/業界共用パターン(ギャランティ回線)の別、センタ UPF/エンド UPF の別並びにセンタ拠点～エンド拠点の物理的な距離の違いによる遅延時間を比較しました。本検証ではコアおよび CU を共用した環境について、R3 年度と同様の遅延時間の測定および比較を実施しました。その結果から、コアのみ共用した環境とコアおよび CU を共用した環境とで遅延時間に大差はないこと、まずはセンタ UPF/エンド UPF の別、次に複数企業共用パターン/業界共用パターンの別、そしてセンタ拠点～エンド拠点の物理的な距離の違いの順に遅延時間に影響を与えることが確認できました。

コア等を共用する環境で遅延時間が最も良好となるのはエンド UPF～UE という環境です。この環境では、UE とやり取りする通信が複数企業共用パターン/業界共用パターンの別並びにセンタ拠点～エンド拠点の物理的な距離の影響を受けないためであり、遅延時間に高い水準を要求するユースケースの場合はエンド UPF 環境が望ましいものと考えます。

逆に最も遅延時間の劣化が大きいのはセンタ UPF～UE という環境で、ベストエフォート回線を使用する複数企業共用パターンの環境です。エンド UPF 環境と比較した場合、本検証では NTT 中央研修センタおよびいすゞ自動車の両方の拠点で 10ms 以上の遅延時間の劣化を確認しました。特にいすゞ自動車の遅延時間は大きい結果であることから、ベストエフォート回線を使用しセンタ UPF と通信するする環境の場合はセンタ拠点～エンド拠点の物理的な距離にも注意する必要があると考えます。

センタ UPF～UE という環境で遅延時間の劣化が少なくなるのは、ギャランティ回線を使用した業界共用パターンの環境です。エンド UPF 環境と比較した場合、本検証では東北大学、東京大学および NTT 中央研修センタでは 4ms 程度の遅延時間の劣化が見られました。センタ拠点～エンド拠点の物理的な距離が最も遠い京都大学でも遅延時間の劣化が 9ms 程度でした。センタ UPF 環境を利用する場合にギャランティ回線を使用することで、ベストエフォート回線を使用する場合と比べて遅延時間の劣化を軽微に収めることができると考えます。

以上の結果から、コア等を共用することは遅延時間の劣化を生じるものではないものの、センタ UPF～UE という環境では広域回線の種別および拠点間の距離による遅延時間への影響について留意すべきものと考えます。

イ　UE 多接続

UE を多数同時に接続した場合の影響について、R3 年度は UE 最大同時接続数、UE 多接続時の 5GC 等の CPU/メモリの消費リソースの変動および UE 多接続時の認証時間の変動を検証しました。UE 最大同時接続数は R3 年度の製品において仕様上の最大数７台の同時接続が可能であり、RU～UE の最大伝送スループット相当まで通信可能であることを確認しています。消費リソースについては UE 数が増大した場合に CPU 利用率は大きな変動がなく、メモリ利用率は微増したという結果のため、基本的に UE 数はローカル５Ｇシステムの消費リソース

に対する大きな課題とならないとしています。またUE認証時間については、複数企業共用パターン/業界共用パターンの別およびセンタ拠点～エンド拠点の物理的な距離に影響されず1分間以内で認証するという結果から、コア共用環境はUE認証時間に差分を生じないとしています。これらの結果から、コア等を共用した環境によって、UE が多数接続した場合のコア等の機器の処理に劣化を及ぼすものではないことが確認できました。

そこで本検証では UE が多接続した場合に認証パケットがコア～UE 区間のネットワークに対して負担を生じるものであるかを検証しました。結果として使用したUEエミュレータで実現可能な30台同時接続が良好に実施できることを確認できました。30台同時接続の際にUEのアタッチ処理のためにC-planeの通信が発生しており、このC-planeに必要な帯域は瞬間的なピーク値で30kbps程度であることを実測しました。本検証の機器における同時接続UEの最大数は80台です。実測結果のピーク値を基準としてC-planeが比例的に増大したと仮定した場合に、80台でのC-plane必要帯域は80kbpsとなり、センタ拠点とエンド拠点を接続するWAN回線の帯域に対してわずかであるといえます。C-planeに関しては接続UE 数の増大はコア等の共用という環境での運用に対する妨げにはならないものと考えます。例えば、最大 100Mbps のベストエフォート回線を WAN 回線として使用する環境での運用を想定した場合、帯域が保証されないためにWAN回線の実力値が10Mbpsまで制限された状態であっても、10000台程度のUEのアタッチ処理が可能であるといえます。エンドUPF環境においてはC-planeの通信のみがWAN回線を流れるため、こうした比較的狭い帯域のWAN回線サービスを選択することができると考えます。一方、センタUPF環境の場合は、C-planeに加えてU-planeの通信もWAN回線を流れます。UEのアタッチ処理に要するC-planeと比較してU-planeは大きな帯域を必要とするケースが想定されます。そのため、センタUPF環境においてはU-planeに必要とする帯域を確保できる回線サービスの選定が必要です。

以上の結果からコア等を共用した環境においてUEを多接続するケースは、ローカル５Ｇ機器の性能の範囲において実現可能であると考えます。

ウ　準同期方式での性能変動

同期方式から制度化済み準同期方式に切り替えることで、DLスループットが約2～3割程度減少し、UL スループットが約 2 倍に増加することを確認できました。これらの変動は準同期方式に切り替えたことによる比率の変動に一致しています。

したがって、コアおよびCUの共用という環境であっても準同期方式の伝送性能を十分に発揮できるといえます。ただし、同期方式と同様に、WAN回線の種別によるスループットの制限ついては留意すべきものと考えます。

5.4　ローカル５Ｇ交換設備の共用における機能検証

(1) 検証目的

コア装置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。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るため、それらの実用性についてR3年度とは異なるコア装置で検証しました。

コア共用下では異なるユースケースが混在することが想定されるため、UE ごとに異なるUPFを選択する等の自由度および柔軟性の高い構成が望ましいと考えられます。また、アプリケーションによって大容量伝送や低遅延通信等、柔軟なNW設計が可能なネットワークスライシング機能も有効だと考えます。加えて、マルチテナント型においては在圏情報やトラヒックモニタリング等の管理機能も求められます。

本調査研究では、コア共用下でそれらの機能の有効性について 2 種類のコア装置を用いて検証しました。具体的な検証パターンは「表 5-4-1-1　機能検証　検証パターン」に示すとおりです。

表 5-4-1-1　機能検証　検証パターン

機器ベンダー	共用パターン	管理機能等確認検証※1	トラヒックモニタリング検証	在圏管理検証※1	ネットワークスライス検証※2
A社	複数企業共用パターン	対象外	対象	対象	対象
	業界共用パターン	対象外	対象	対象外	対象
B社	複数企業共用パターン	対象	対象	対象	対象外
	業界共用パターン	対象外	対象	対象外	対象外

※1：管理機能および在圏管理機能は5GCに設定された情報を取得・表示・操作する機能であるため、複数企業共用パターン/業界共用パターンの違いは影響しないことから、複数企業共用パターンのみを検証対象とする。また、A社製機器の管理機能はR3年度に検証を実施済みのため、本検証では対象外とする。

※2：A 社製機器ではネットワークスライシング機能を実装しているためすべてのパターンで検証を実施する。B社製機器では未実装機能のため対象外とする。

(2) 評価・検証項目

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

表 5-4-2-1 評価・検証項目

大項目	中項目	小項目	検証概要	検証項目	対応図表
機能検証	管理機能等確認検証	複数企業共用パターン	R3 年度実施項目であるコア装置内の管理機能やログ情報の実装状況を確認し、R3 年度の結果との比較考察	SIM 認証の管理状況	図 5-4-3-1
				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	
				ログの蓄積、管理状況	
				管理権限の設定状況	
	トラヒックモニタリング検証	複数企業共用パターン	ローカル５Ｇ通信状況を把握・管理する機能について検証	UE1 台での通信状況	図 5-4-3-2
				UE2 台での通信状況	
				UL/DL で互いの通信への影響	
		業界共用パターン		UE1 台での通信状況	
				UE2 台での通信状況	
				UL/DL で互いの通信への影響	
	在圏管理検証	複数企業共用パターン	DU の管轄内の端末情報の閲覧等の機能について検証	１台の RU に 1 台の UE を接続して在圏情報を確認	図 5-4-3-3
				１台の RU に 2 台の UE を接続して在圏情報を確認	
				2 拠点の RU にそれぞれ UE を接続し、在圏情報を確認	
	ネットワークスライス検証	複数企業共用パターン	ネットワークスライス機能の有効性に関する検証	ネットワークスライスの設定確認	図 5-4-3-4
				ネットワークスライスを設定した状態での通信品質確認	
				各スライス同時通信検証	
		業界共用パターン		ネットワークスライスの設定確認	
				ネットワークスライスを設定した状態での通信品質確認	
				各スライス同時通信検証	

(3) 評価・検証方法

本検証で用いた測定ツールは、以下の「表 5-4-3-1　測定ツール」のとおりです。

表 5-4-3-1　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
	パケットキャプチャ解析：Wireshark

①　管理機能等確認検証

本検証では、B 社製機器で接続企業等の利用ユーザに関する顧客管理機能の実用性の検証を行い、コア装置の製品による顧客管理機能の違いを R3 年度の結果と比較考察します。

検証イメージは「図 5-4-3-1　機能確認検証イメージ」に示し、検証手順は「表 5-4-3-1 機能確認　検証手順」に示します。

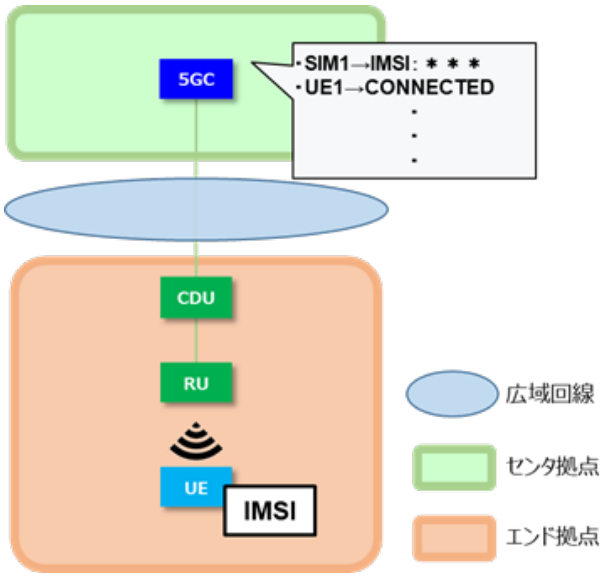


図 5-4-3-1　機能確認検証イメージ

表 5-4-3-1 機能確認　検証手順

項番	評価項目	検証手順
1	顧客管理機能の確認	B 社製機器を用いて、以下の機能を本環境において利用可能であることを確認。特に、拠点ごとに区切られて情報の閲覧登録が出来ることを確認する。 ・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 ・ログの蓄積、管理状況 ・管理権限の設定状況
2	R3 年度の実施結果(A 社製 5GC)との比較考察	・課題、留意事項の考察 ・コア共用モデルにおける実装機能に関する分析、考察

②　トラヒックモニタリング検証

本検証では、A 社製機器と B 社製機器を用いて通信状況の把握・管理機能確認の検証を行

います。検証は複数企業共用パターンと業界共用パターンで実施し、UPF 設置もセンタ・エンドどちらでも行います。

検証イメージは「図 5-4-3-2　トラヒックモニタリング検証イメージ」、検証手順は「表 5-4-3-2 トラヒックモニタリング検証　検証手順」に示します。

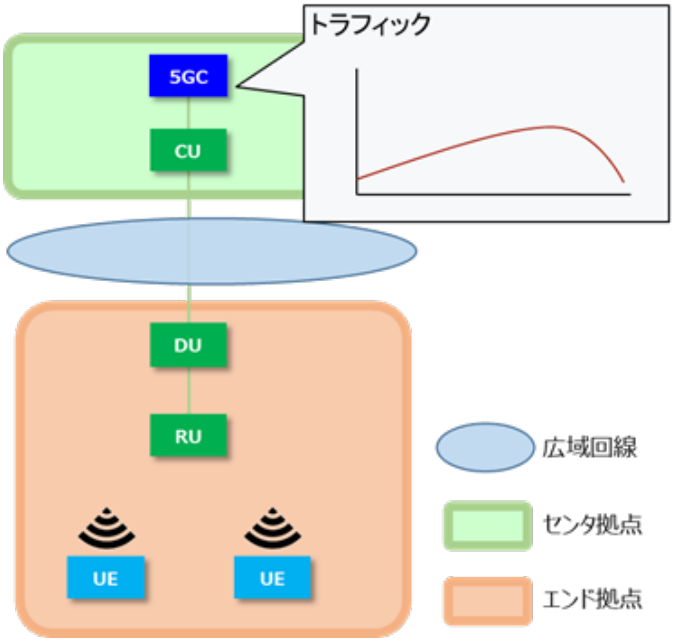


図 5-4-3-2　トラヒックモニタリング検証イメージ

表 5-4-3-2　トラヒックモニタリング 検証手順

項番	評価項目	検証手順
1	ローカル５Ｇにおける通信状況管理機能の確認（A 社）	A 社製機器を用いて、以下の手順で通信状況管理機能を確認 ・UE1 台での通信状況 ・UE2 台での通信状況 ・UL/DL で互いの通信への影響
2	ローカル５Ｇにおける通信状況管理機能の確認（B 社）	B 社製機器を用いて、以下の手順で通信状況管理機能を確認 ・UE1 台での通信状況 ・UE２台での通信状況 ・UL/DL で互いの通信への影響
3	結果分析・考察	・課題、留意事項の考察 ・コア共用モデルにおける実装機能に関する分析、考察

③　在圏管理検証

本検証では、A 社製機器と B 社製機器を用いて DU 管轄内の端末情報の閲覧等の機能について検証します。

検証イメージは「図 5-4-3-3　在圏管理検証イメージ」、検証手順は「表 5-4-3-3 在圏管

理　検証手順」に示します。

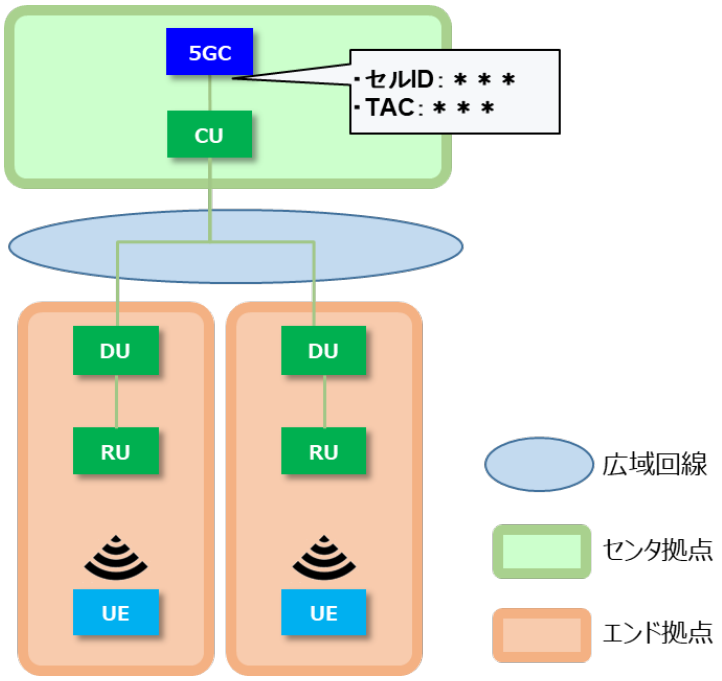


図 5-4-3-3　在圏管理検証イメージ

表 5-4-3-3 在圏管理　検証手順

項番	評価項目	確認項目
1	在圏情報の閲覧等の機能確認 (A 社)	A 社製機器を用いて、以下の手順で機能を確認 ・１台の RU に 1 台の UE を接続して在圏情報を確認 ・１台の RU に 2 台の UE を接続して在圏情報を確認 ・2 拠点の RU にそれぞれ UE を接続し、在圏情報を確認
2	在圏情報の閲覧等の機能確認 (B 社)	B 社製機器を用いて、以下の手順で機能を確認 ・１台の RU に 1 台の UE を接続して在圏情報を確認 ・１台の RU に 2 台の UE を接続して在圏情報を確認
3	結果分析・考察	・課題、留意事項の考察 ・コア共用モデルにおける実装機能に関する分析、考察

④　ネットワークスライス検証

本検証では、A 社製機器を用いてネットワークスライスの設定・通信品質の検証を行います。検証は複数企業共用パターンと業界共用パターンのそれぞれで実施し、UPF 設置もセンタ・エンドどちらでも行います。

検証イメージは「図 5-4-3-4　ネットワークスライス検証イメージ」、検証手順は「表 5-4-3-4 ネットワークスライス　検証手順」に示します。

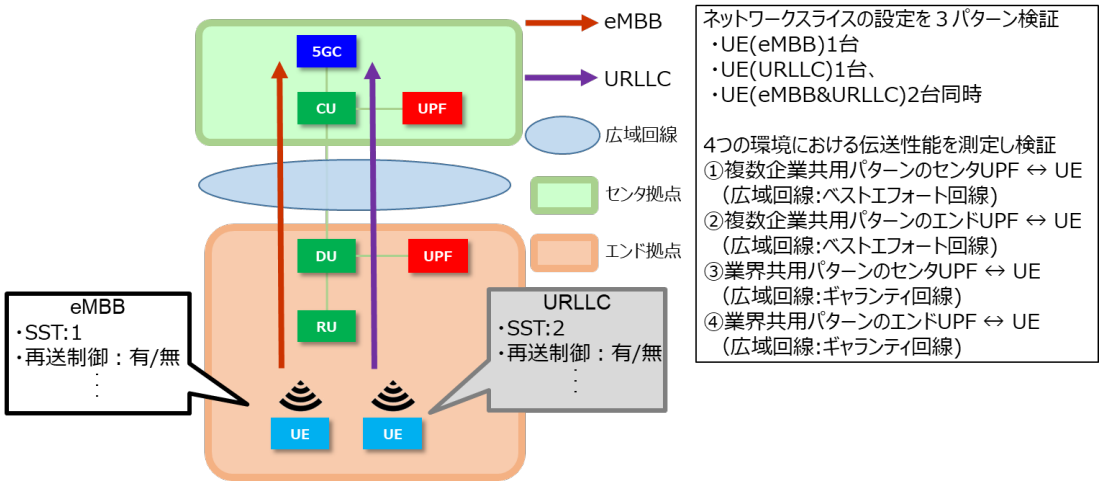


図 5-4-3-4　ネットワークスライス検証イメージ

表 5-4-3-4 ネットワークスライス検証　検証手順

項番	評価項目	確認項目
1	ネットワークスライスの設定確認	・eMBB と URLLC を設定 ・各端末に NSSAI 識別子が正しく設定されているか確認
2	ネットワークスライスを設定した状態での通信品質確認	eMBB と URLLC それぞれで以下の項目について通信品質を確認 ・スループット ・遅延時間 ・パケット損失率 ・ジッタ ・入出力グラフ
3	各スライス同時通信検証	2UE に eMBB と URLLC をそれぞれ設定し、以下の項目について同時通信による通信品質を確認 ・スループット ・遅延時間 ・パケット損失率 ・ジッタ ・入出力グラフ
4	結果分析・考察	・課題、留意事項の考察 ・コア共用モデルにおける実装機能に関する分析、考察

(4) 検証結果

① 管理機能等確認検証の結果

ア　A 社製機器の場合

A 社製機器では R3 年度同様の検証を実施しているため、今年度は実施しませんでした。

イ　B 社製機器の場合

（ア）　SIM 認証の管理状況

SIM 認証の管理状況は WebGUI 上のメニューから「図 5-4-4-①-1　SIM 情報　Export」のように Operation＞Control を選び、Export　Suscribers をクリックすることでテキストファイルの形式でダウンロードすることができます。Export　Subscribers を押下すると「図 5-4-4-①-2　UserName　Password 入力」のとおり UserName と Password の入力を求められます。正しく入力するとテキストファイルが「図 5-4-4-①-3　テキストファイルのダウンロード」のとおりダウンロードされます。テキストファイルの内容は「図 5-4-4-4　SIM 情報のテキストファイル」のようになっています。「図 5-4-4-①-4　SIM 情報のテキストファイル」を編集し SIM 固有の IMSI、OPc 値および K 値並びに AMBR 値(最大可能ビットレート)、DNN、割当 IP アドレスを追記後、「図 5-4-4-①-1　SIM 情報　Export」の Import Subscribers をクリックすることで SIM の登録、変更、削除が可能です。実行により「図 5-4-4-①-5 Import 実行結果」が表示されます。

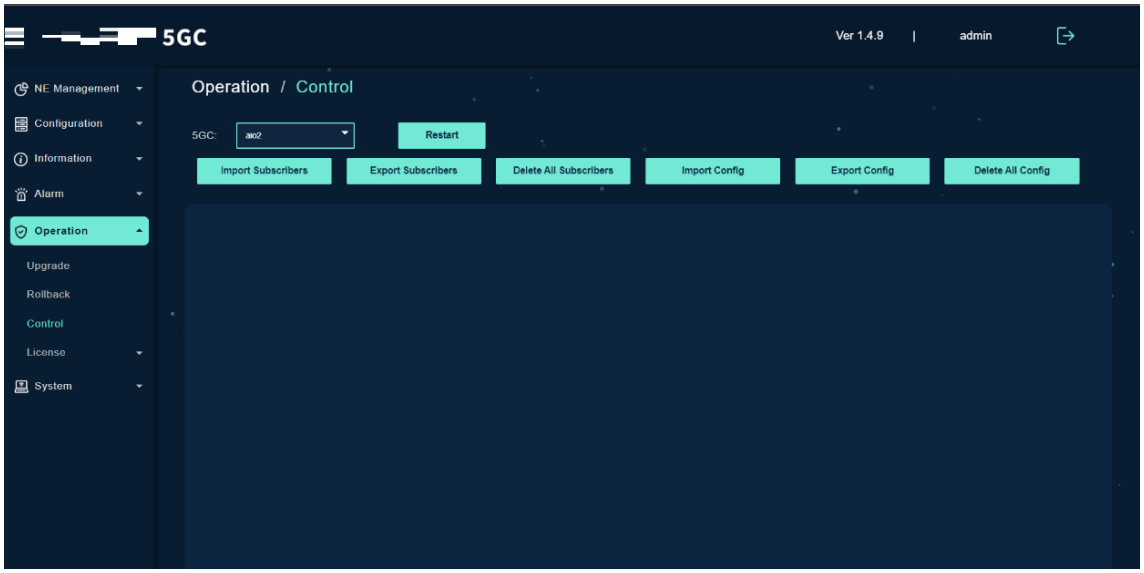


図 5-4-4-①-1　SIM 情報　Export

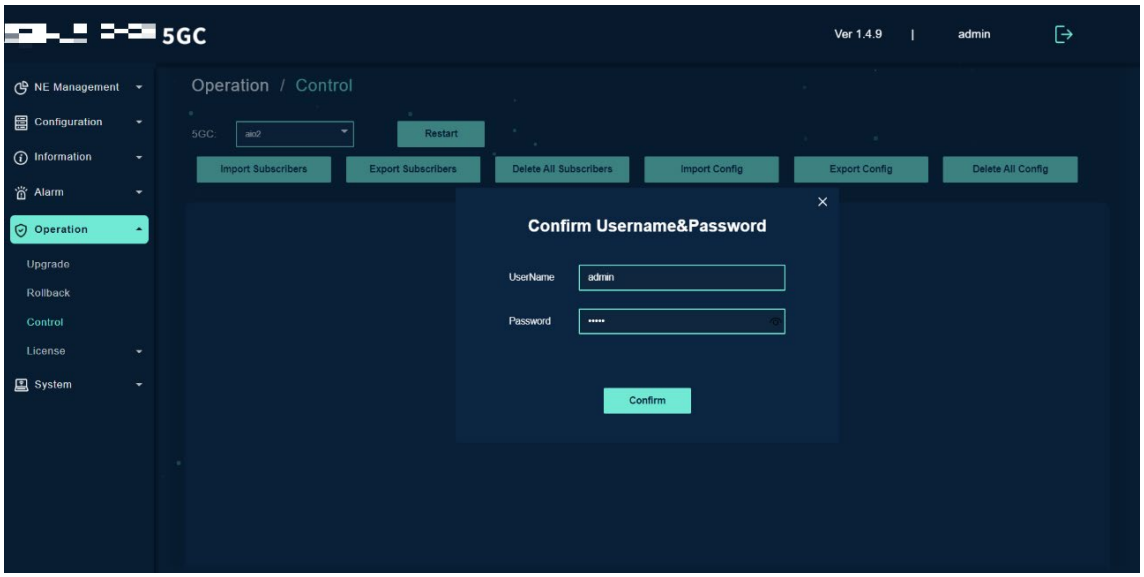


図 5-4-4-①-1　UserName　Password 入力

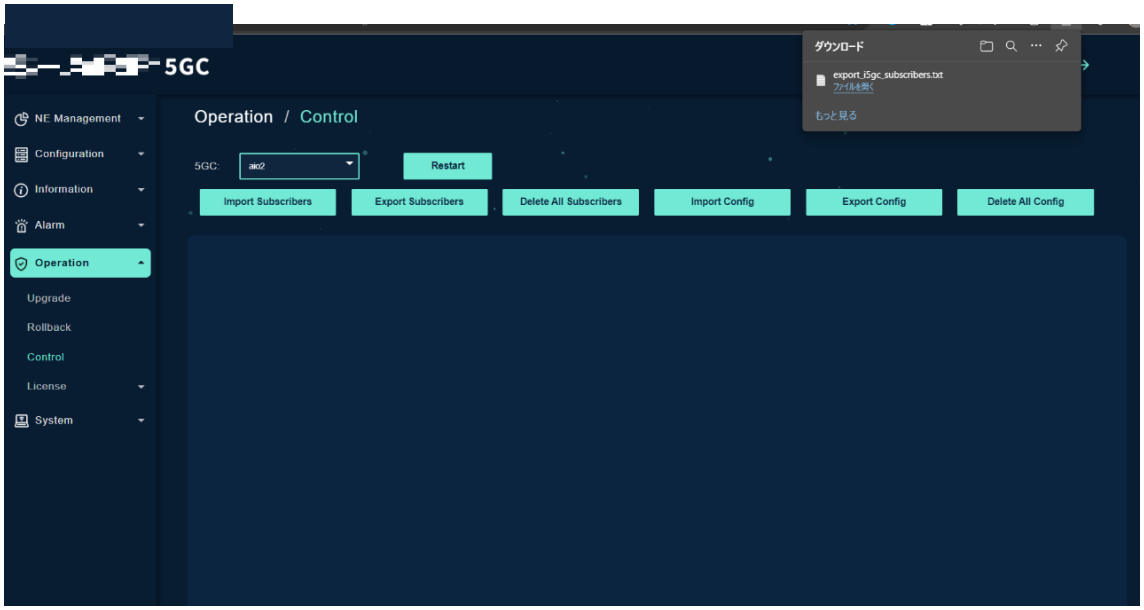


図 5-4-4-①-2　テキストファイルのダウンロード



図 5-4-4-①-3　SIM 情報のテキストファイル

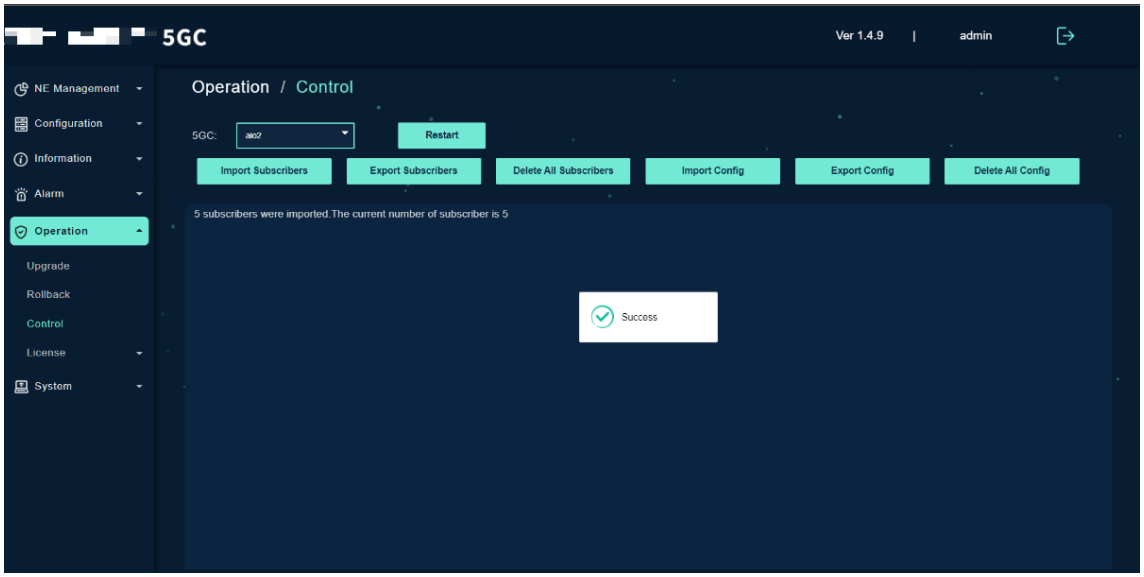


図 5-4-4-①-4　Import 実行結果

（イ）　端末情報の管理状況

端末情報の管理状況は、

端末が 5GC に接続している状態を表す情報であり、WebGUI 上のメニューから「図 5-4-4-①-6　MM information」のように Information＞MM Information を選ぶことで確認できます。基地局と通信状態の場合は「CONNECTED」、通信がない状態は「IDLE」と表示されます。5GC にアタッチしていない端末は表示されません。この機能によって現在利用中の端末を確認

することが可能です。

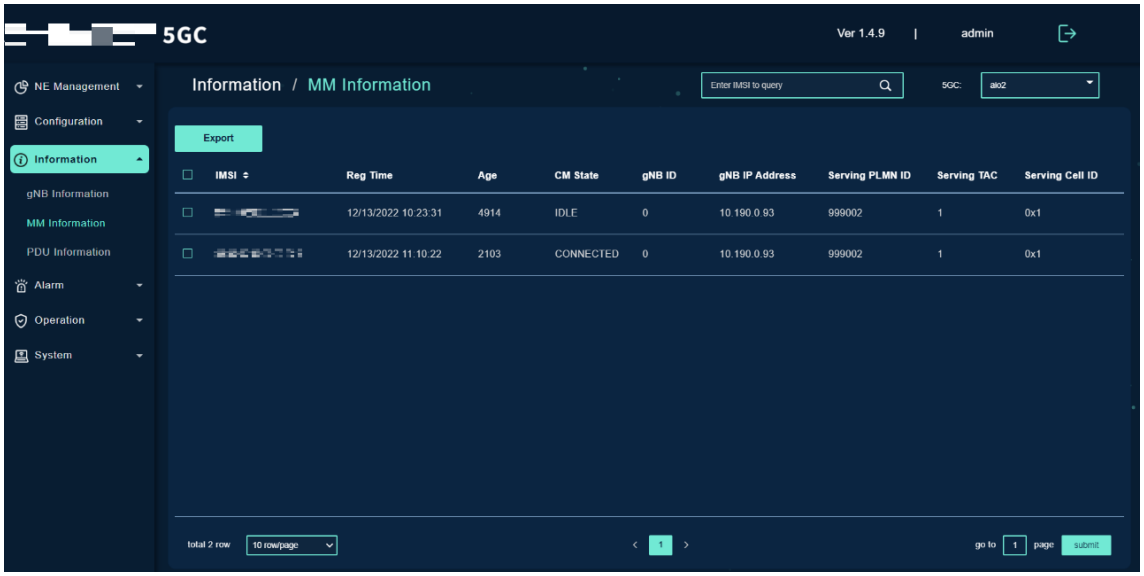


図 5-4-4-①-5　MM information

（ウ）　ポリシーの管理状況

ポリシーの管理状況は、WebGUI 上のメニューから「図 5-4-4-①-7　QoS　Profile」のように Configuration＞QoS　Profile を選ぶことで確認できます。5GC のポリシーとして 5QI を設定することが可能です。

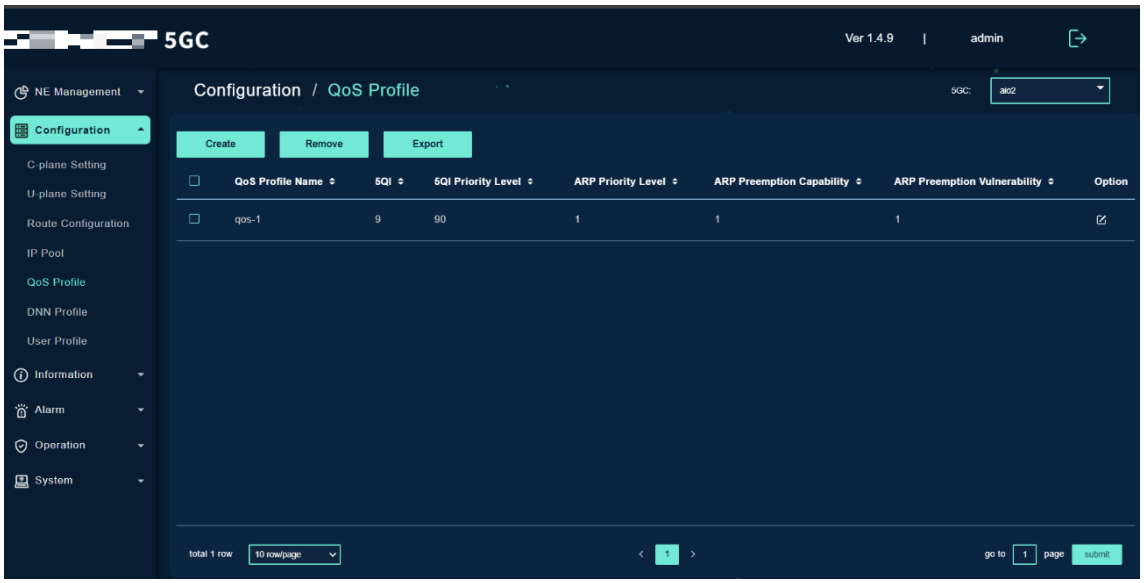


図 5-4-4-①-7　QoS　Profile

（エ）　セッション管理の管理状況

セッションの管理状況は、WebGUI 上のメニューから「図 5-4-4-①-8　PDU Information」のように Information＞PDU Information を選ぶことで確認できます。セッションの状態として ACTIVE あるいは INACTIVE を表示します。セッションで N3 の接続相手の CU を Remote N3 Address から確認できます。INACTIVE の場合は 0.0.0.0 と表示されます。

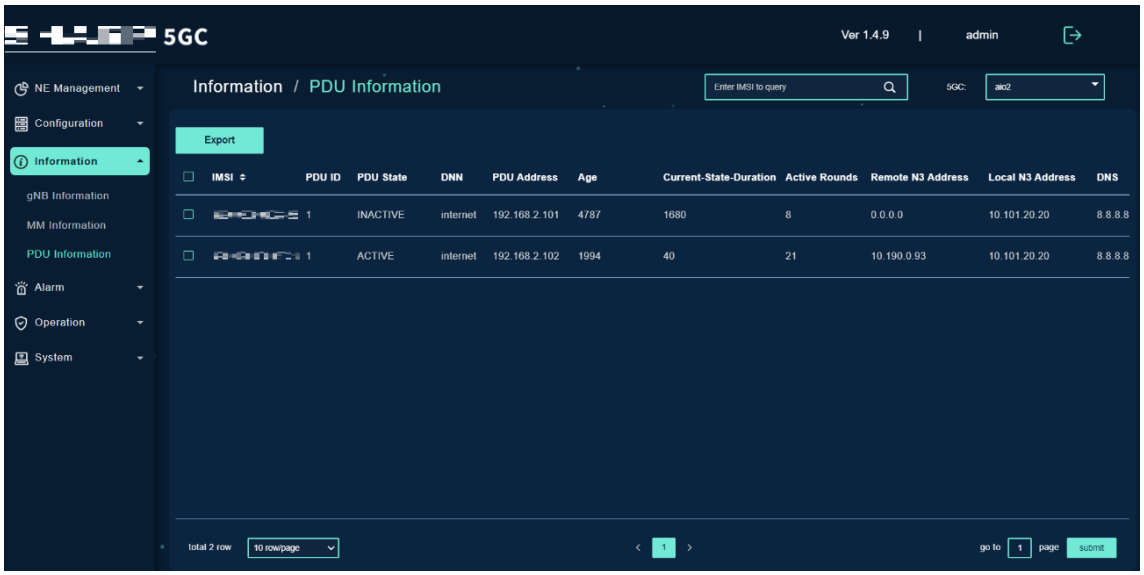


図 5-4-4-①-8　PDU Information

（オ）　ログの蓄積、管理状況

ログの管理状況は、WebGUI 上のメニューから「図 5-4-4-①-9　Log」のように System＞Log を選ぶことで確認できます。NMS(5GC GUI)上でユーザが行った操作のログを確認できます。また Alarm を選ぶことで「図 5-4-4-①-10　Alarm Summary」～「図 5-4-4-①-13 Alarm History」のとおり、5GC が検知したアラームを確認できます。「図 5-4-4-12 Alarm Details BBU Stopped」では故意に CDU を停止し、警報を表示させています。

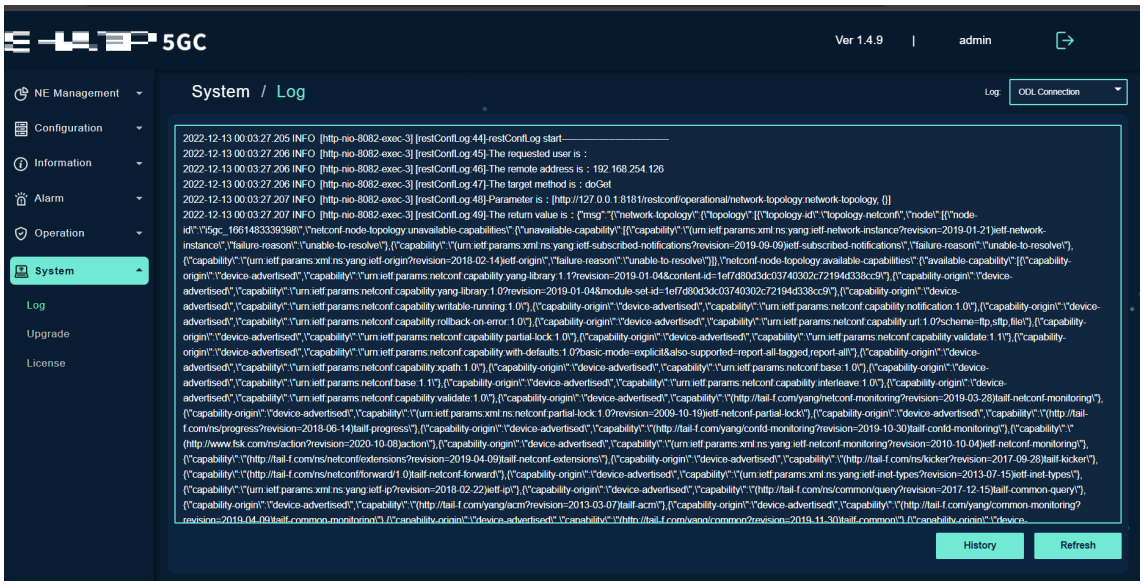


図 5-4-4-①-9　Log

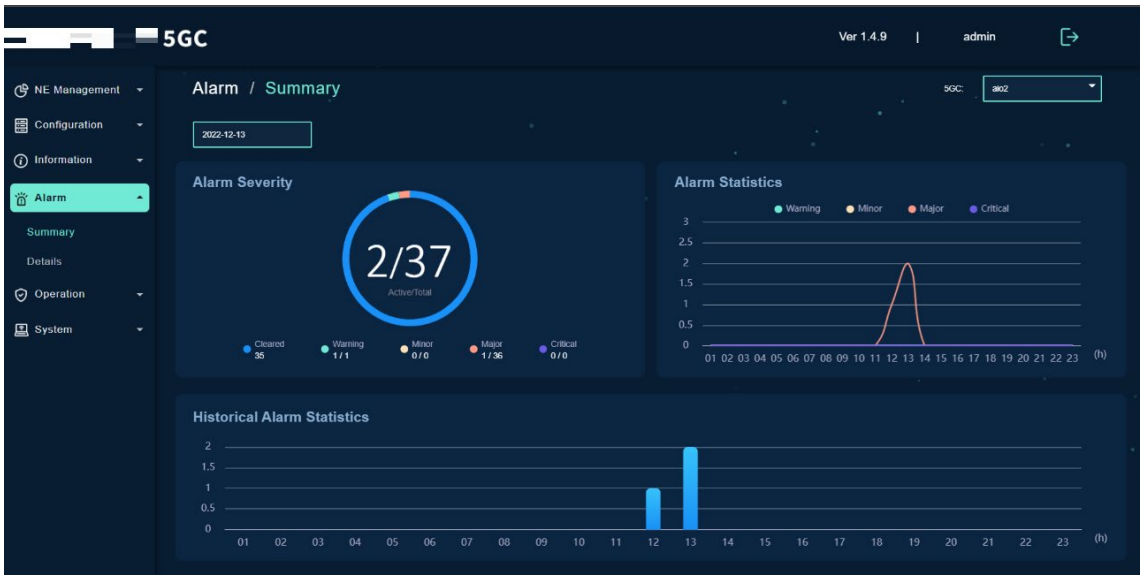


図 5-4-4-①-10　Alarm Summary

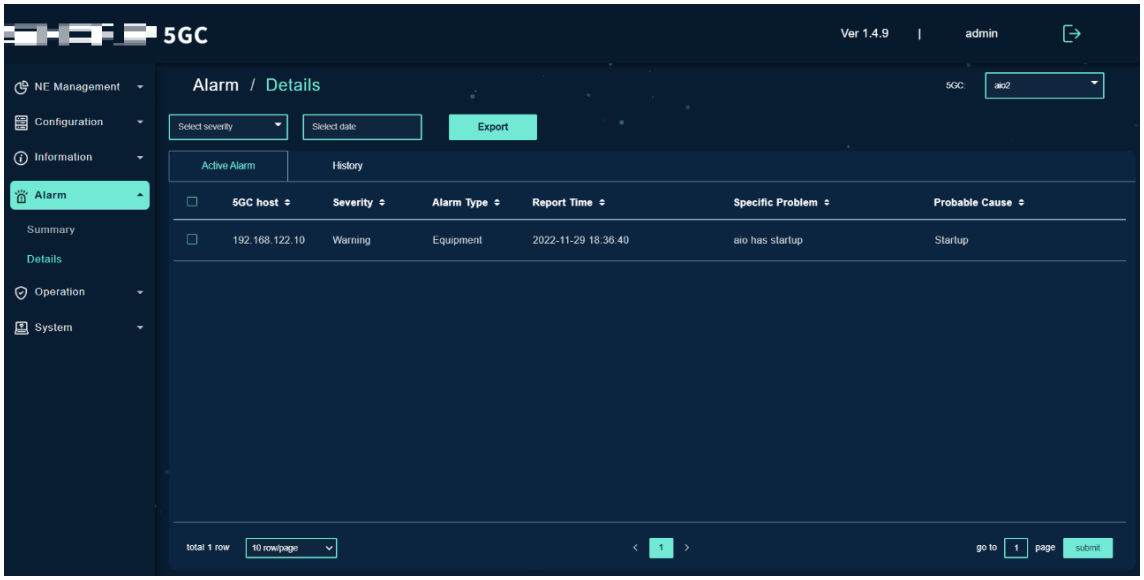


図 5-4-4-①-11 Alarm Details

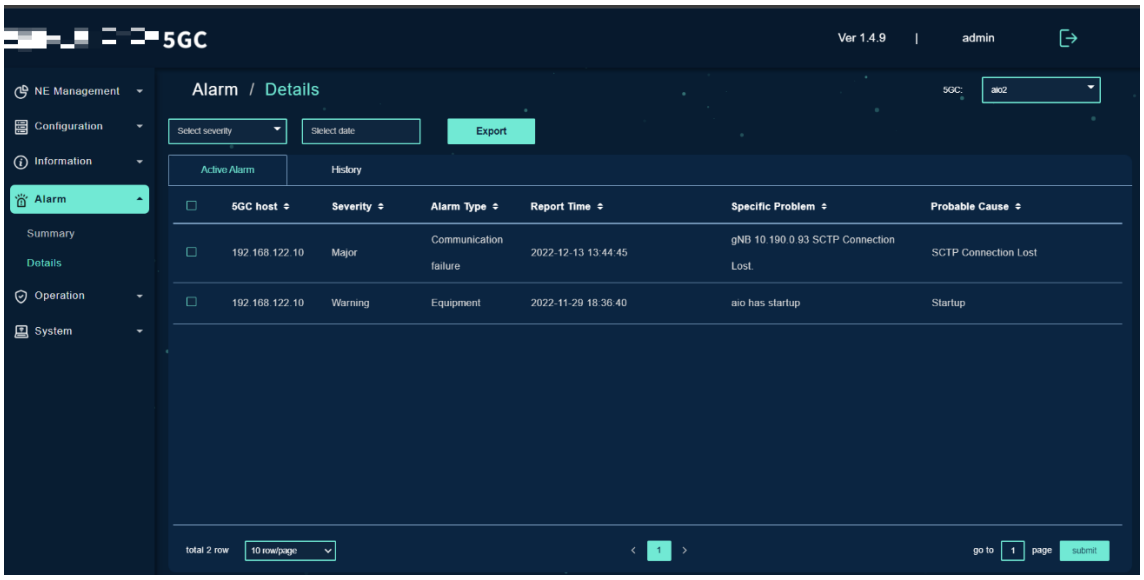


図 5-4-4-①-12 Alarm Details BBU Stopped

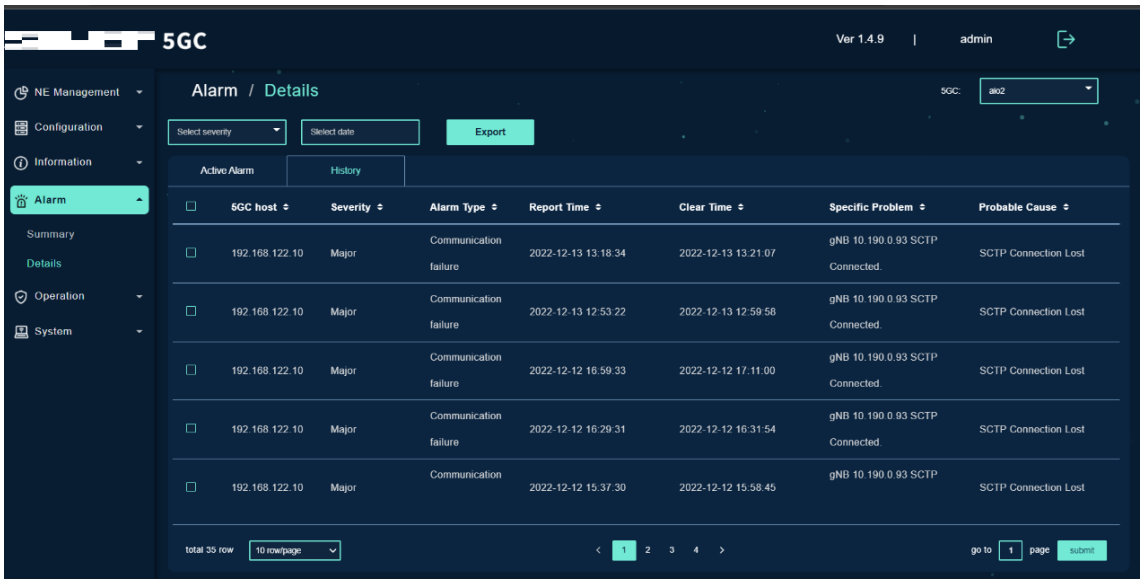


図 5-4-4-①-13 Alarm History

（カ）　管理権限の設定状況

B 社のコアに対し（ア）～（オ）の操作・閲覧を行う際は、Web ブラウザに指定の URL を入力し、「図 5-4-4-①-14　ログイン画面」の画面にて UserName と Password を入力しログインする必要があります。URL、UserName および Password によって拠点ごとに SIM 情報等の操作・閲覧管理が可能であることを確認しました。

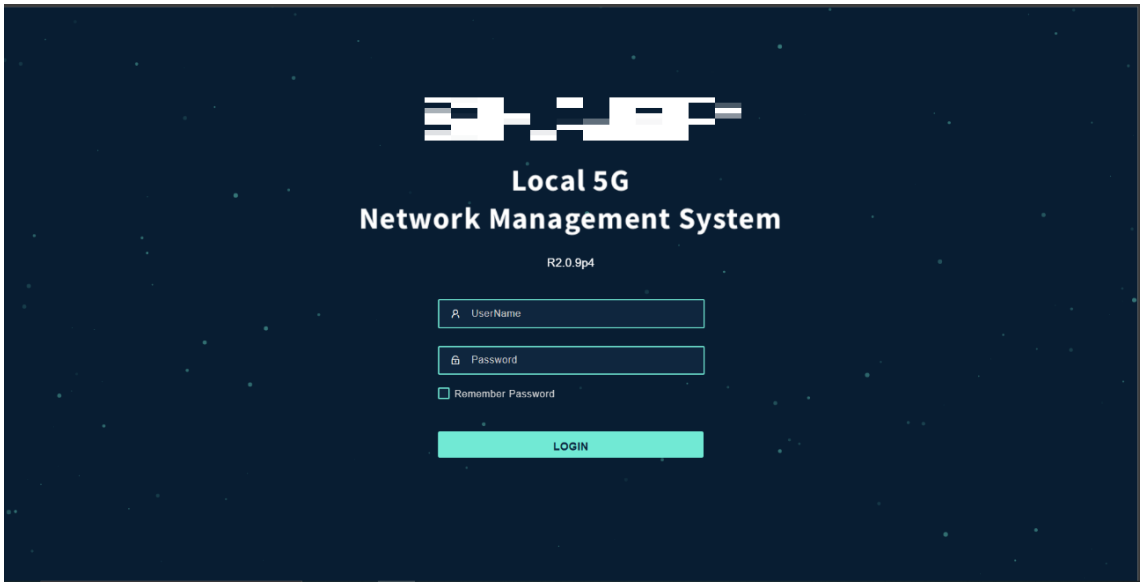


図 5-4-4-①-14　ログイン画面

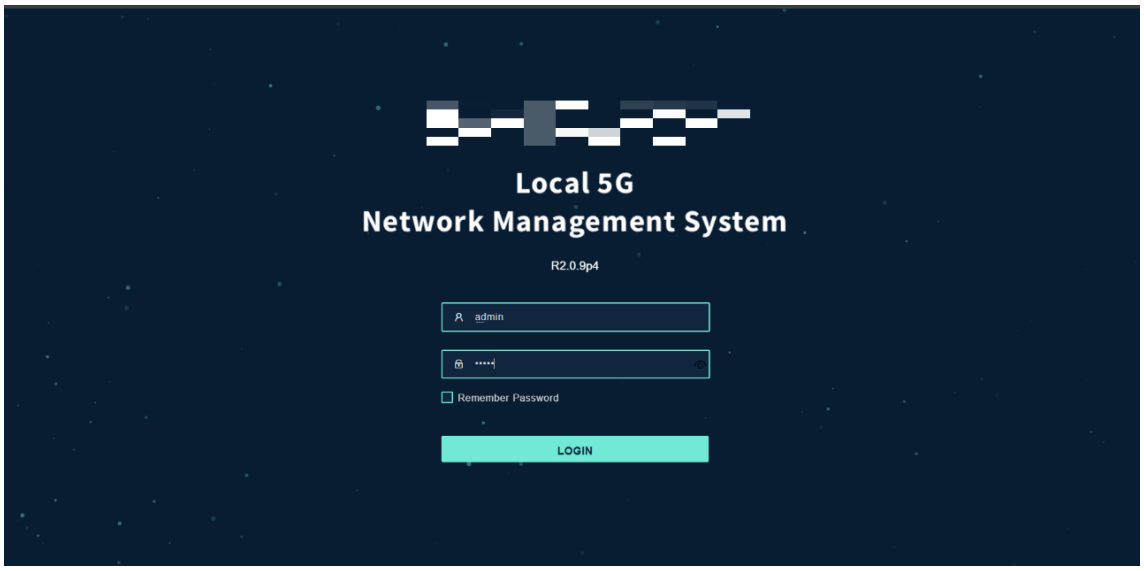


図 5-4-4-①-15　ログイン画面　入力状態

②　トラヒックモニタリング検証の結果

ア　A 社製機器の場合

トラヒックモニタリング機能が WebGUI によって閲覧できることを NTT 中央研修センタにて検証しました。実際の画面表示を次に示します。

（ア）　複数企業共用パターン

UE 1 台を接続しセンタ UPF と UDP での通信を発生させたときのトラヒックモニタリング画面を「図 5-4-4-②-1　複数企業共用パターン　UE 1 台(センタ UPF　UDP)」に示します。初めにセンタ UPF→UE 方向の DL の通信を発生させ、続いて UE→センタ UPF 方向の UL の通

信を発生させました。画面左上に UL スループット、左下に DL スループット、右上に UL パケット数、右下に DL パケット数が表示されていることが確認できます。また、各グラフの下には UE の IMSI が表示されています。縦軸のスケールは通信量に応じて自動的に調節されます。横軸の時間軸は画面右上のメニューによって表示したい範囲を変更することができます。



図 5-4-4-②-1　複数企業共用パターン　UE１台(センタ UPF　UDP)

TCP での通信を発生させたときのトラヒックモニタリング画面を「図 5-4-4-②-2　複数企業共用パターン　UE１台(センタ UPF　TCP)」に示します。TCP の場合には UDP と比べると DL を発生させたときにも UL 方向の通信が発生し、UL を発生させたときにも DL 方向の通信が発生していることが確認できます。



図 5-4-4-②-2　複数企業共用パターン　UE１台(センタ UPF　TCP)

UE２台を接続しセンタ UPF と UDP での通信を発生させたときのトラヒックモニタリング画面を「図 5-4-4-②-3　複数企業共用パターン　UE２台(センタ UPF　UDP)」に示します。一方の UE でセンタ UPF→UE 方向の DL の通信を発生させ、他方の UE で UE→センタ UPF 方向

の UL の通信を発生させました。各グラフの下には各 UE の IMSI が表示され、グラフの色によってどちらの UE で通信が発生しているかを確認できます。



図 5-4-4-②-3　複数企業共用パターン　UE２台(センタ UPF　UDP)

TCP での通信を発生させたときのトラヒックモニタリング画面を「図 5-4-4-②-4　複数企業共用パターン　UE２台(センタ UPF　TCP)」に示します。TCP の場合には UDP と比べると DL を発生させたときにも UL 方向の通信が発生し、UL を発生させたときにも DL 方向の通信が発生していることが確認できます。



図 5-4-4-②-4　複数企業共用パターン　UE２台(センタ UPF　TCP)

（イ）　業界共用パターン

業界共用パターンでも前項と同様に UE とセンタ UPF または UE とエンド UPF とで通信を発生させたときのトラヒックモニタリング画面を「図 5-4-4-②-5　業界共用パターン　UE１台(センタ UPF　UDP)」～「図 5-4-4-②-8　業界共用パターン　UE２台(エンド UPF　TCP)」に示します。複数企業共用パターンと同様にトラヒックモニタリング機能によって良好に通信状態を確認することができました。



図 5-4-4-②-5　業界共用パターン　UE１台(センタ UPF　UDP)



図 5-4-4-②-6　業界共用パターン　UE１台(センタ UPF　TCP)



図 5-4-4-②-7　業界共用パターン　UE２台(センタ UPF　UDP)



図 5-4-4-②-8　業界共用パターン　UE２台(センタ UPF　TCP)

イ　B 社製機器の場合

トラヒックモニタリング機能が WebGUI によって閲覧できることを NTT 中央研修センタにて検証しました。実際の画面表示を次に示します。トラヒックモニタは WebGUI 上のメニューから NE Management＞Summary を選ぶことで確認することができます。

（ア）　複数企業共用パターンの場合

UE１台を接続しセンタ UPF と UDP での通信を発生させたときのトラヒックモニタリング画面を「図 5-4-4-②-9　複数企業共用パターン　UE１台(センタ UPF　UDP DL)」および「図 5-4-4-②-10　複数企業共用パターン　UE１台(センタ UPF　UDP　UL)」に示します。初めにセンタ UPF→UE 方向の DL の通信を発生させ、続いて UE→センタ UPF 方向の UL の通信を発生させました。画面右上に DL スループット、左上に UL スループットが表示されていることが確認できます。

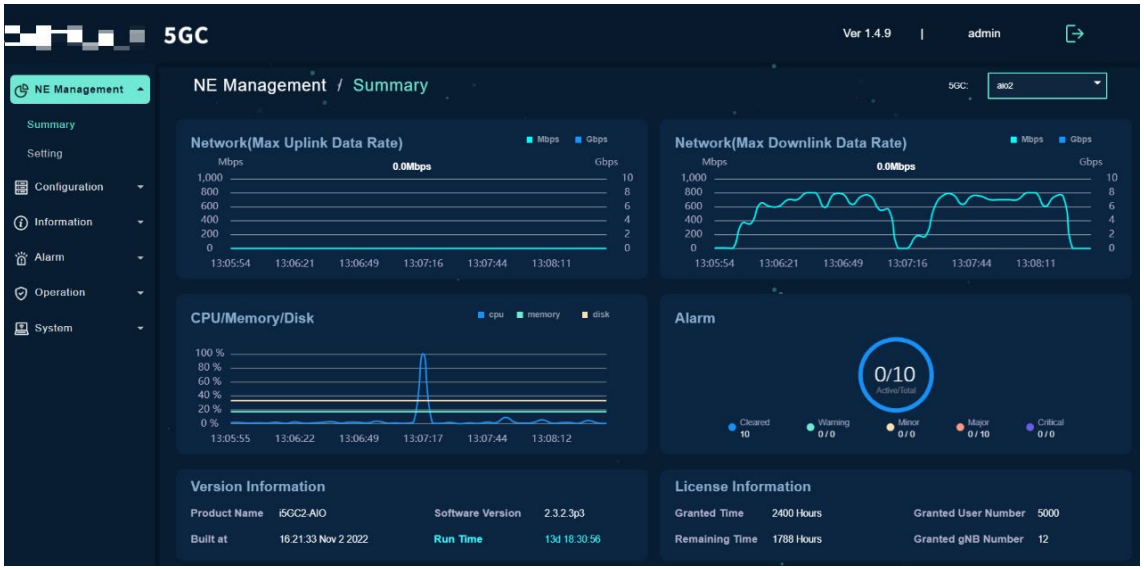


図 5-4-4-②-9　複数企業共用パターン　UE 1 台(センタ UPF　UDP DL)



図 5-4-4-②-10　複数企業共用パターン　UE 1 台(センタ UPF　UDP UL)

UE を 2 台接続した状態での複数企業共用パターンにおけるトラヒックモニタは「図 5-4-4-②-11　複数企業共用パターン　UE2 台(センタ UPF　UDP)」および「図 5-4-4-②-12　複数企業共用パターン　UE2 台(センタ UPF　TCP)」のとおりです。DL/UL 双方のスループットの発生をトラヒックモニタで確認することができました。

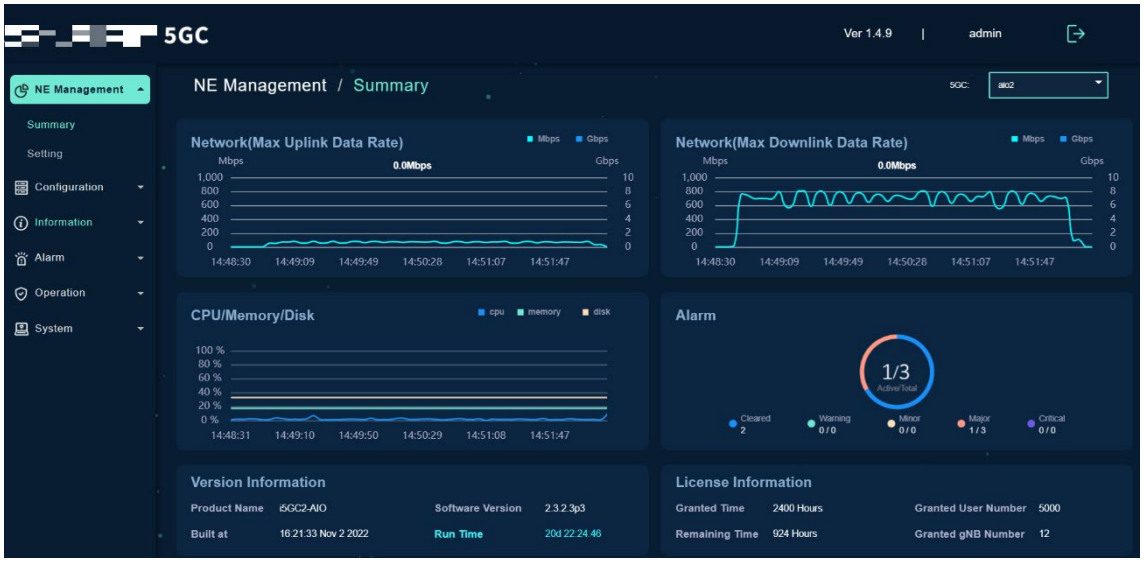


図 5-4-4-②-11　複数企業共用パターン　UE2 台(センタ UPF　UDP)

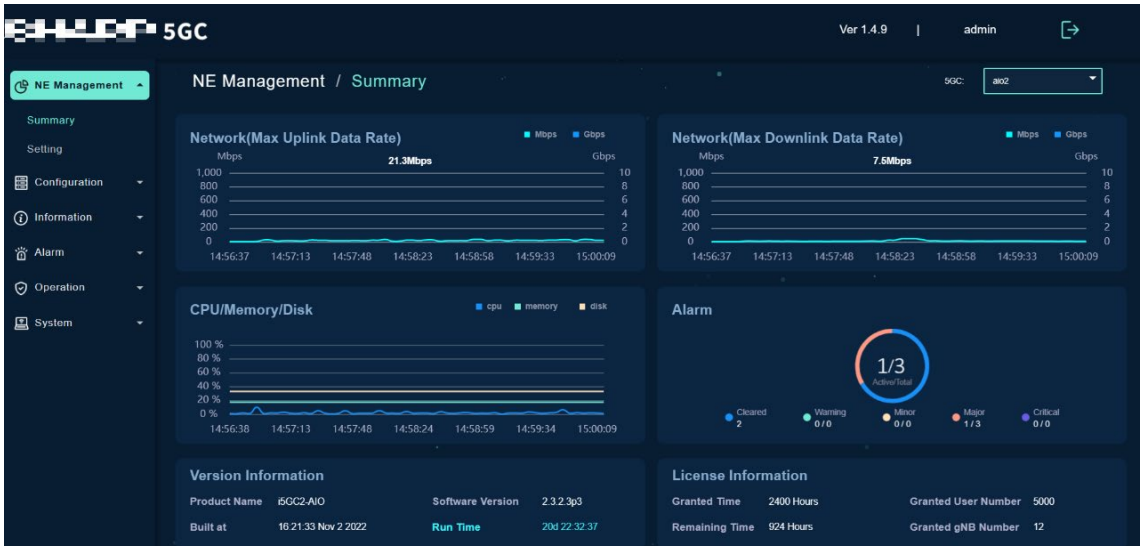


図 5-4-4-②-12　複数企業共用パターン　UE2 台(センタ UPF　TCP)

（イ）　業界共用パターン

業界共用パターンでも前項と同様に UE とセンタ UPF とで通信を発生させたときのトラヒックモニタリング画面を「図 5-4-4-②-13　業界共用パターン　UE１台(センタ UPF　UDP)」～「図 5-4-4-②-16　業界共用パターン　UE２台(センタ UPF　TCP)」に示します。複数企業共用パターンと同様にトラヒックモニタリング機能によって良好に通信状態を確認することができました。

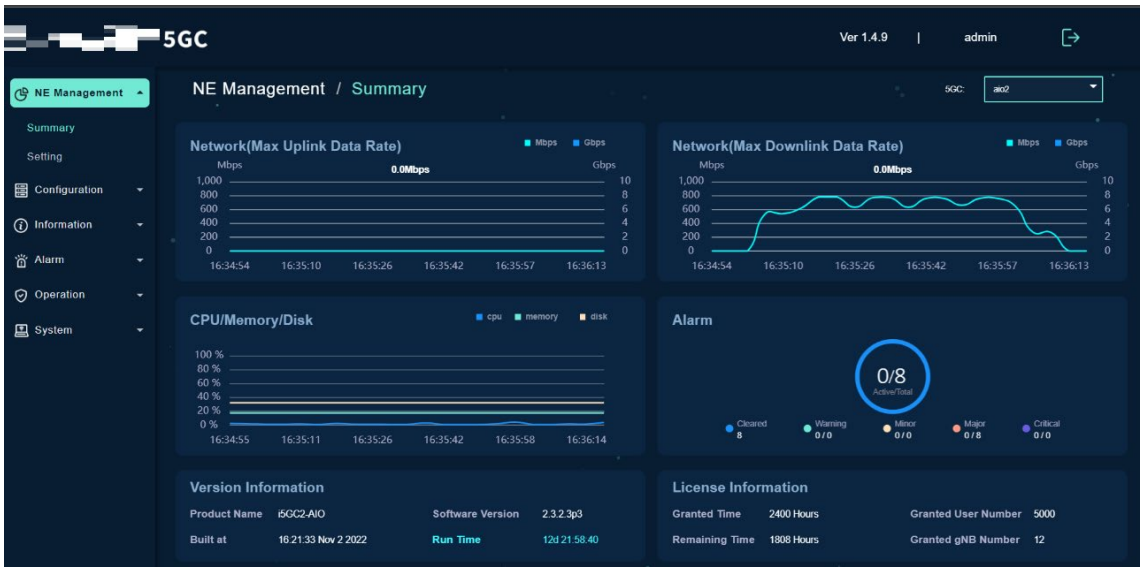


図 5-4-4-②-13　業界共用パターン　UE１台(センタ UPF　UDP DL)

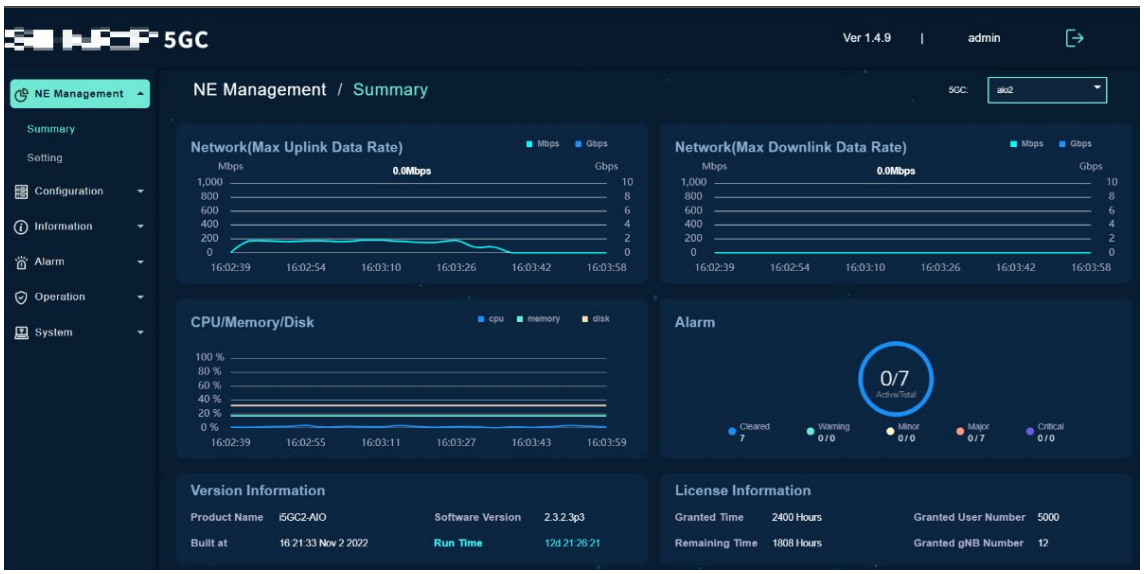


図 5-4-4-②-14　業界共用パターン　UE１台(センタ UPF　UDP UL)

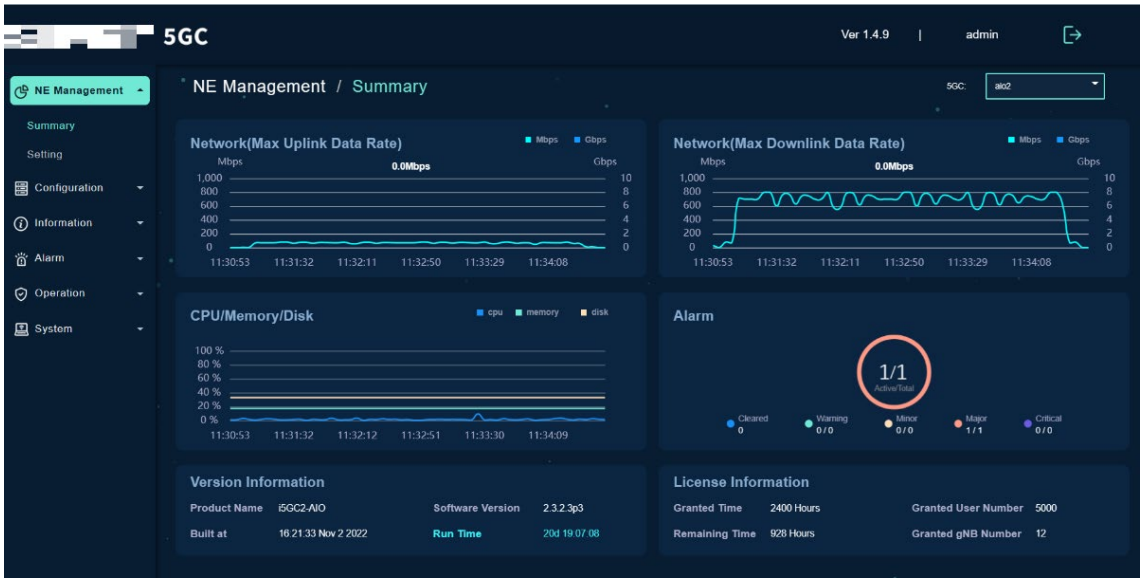


図 5-4-4-②-15　業界共用パターン　UE2 台(センタ UPF　UDP)

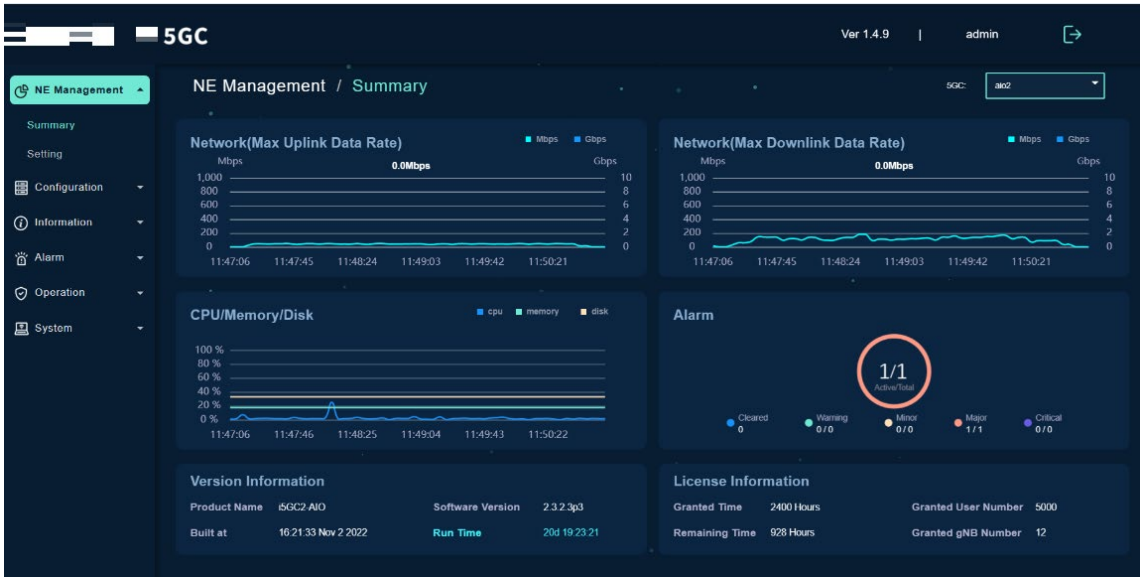


図 5-4-4-②-16　業界共用パターン　UE2 台(センタ UPF　TCP)

③　在圏機能の確認の結果

ア　A 社製機器の場合

在圏機能が WebGUI によって閲覧できることを NTT 中央研修センタおよびいすゞ自動車において検証しました。GUI 左メニューの「REALTIME STATUS」を選択すると、各 UE と基地局の接続状態が確認できます。Cell ID 列によってコア配下のどの基地局と通信しているか判別することができます。

「図 5-4-4-③-1　REALTIME STATUS　NTT 中央研修センタ」は NTT 中央研修センタ内での在圏状況を表示した画面です。UE２台が同じ基地局と接続しているので、Cell ID は２台とも同じです。

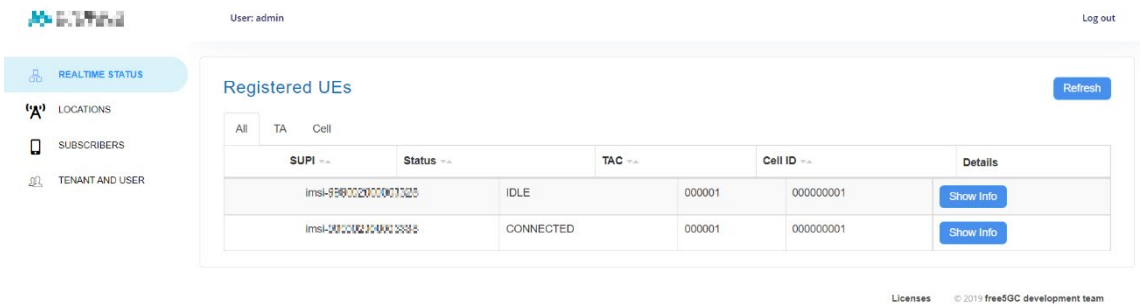


図 5-4-4-③-1　REALTIME STATUS　NTT 中央研修センタ

「図 5-4-4-③-2　REALTIME STATUS　いすゞ自動車」はいすゞ自動車内での在圏状況を表示した画面です。UE４台がコアに接続していますが、１台のみ異なる基地局と接続しています。そのため、１台だけ Cell ID が異なっています。このように画面上からどの UE がどの基地局と接続しているか判別することができます。

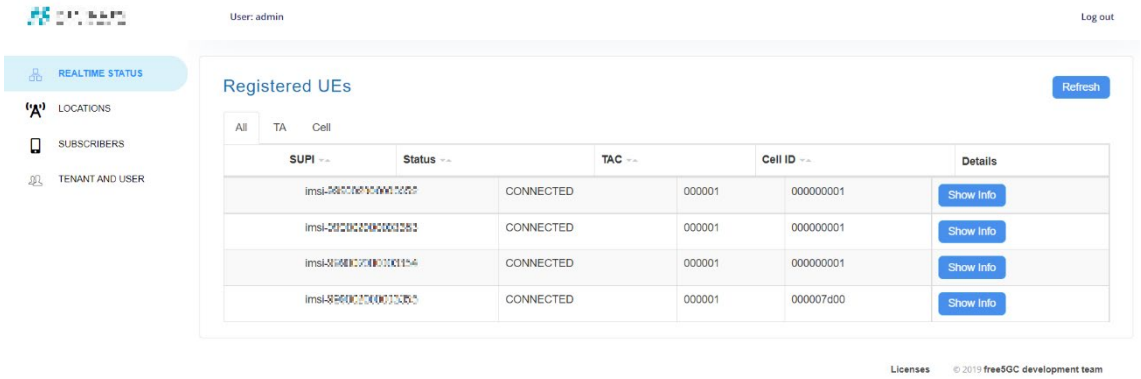


図 5-4-4-③-2　REALTIME STATUS　いすゞ自動車

以上の在圏機能は拠点に応じて表示する画面を切り替えます。そのため拠点ごとに UE の在圏を確認することができます。

イ　B 社製機器の場合

在圏機能が WebGUI によって閲覧できることを NTT 中央研修センタにおいて検証しました。WebGUI 上のメニューから「図 5-4-4-③-3　MM information」のように Information＞MM Information を選ぶことで表示できます。端末が接続している gNB は gNB ID および gNB IP Address によって判別することができ、gNB に対する在圏確認機能として使用することができます。

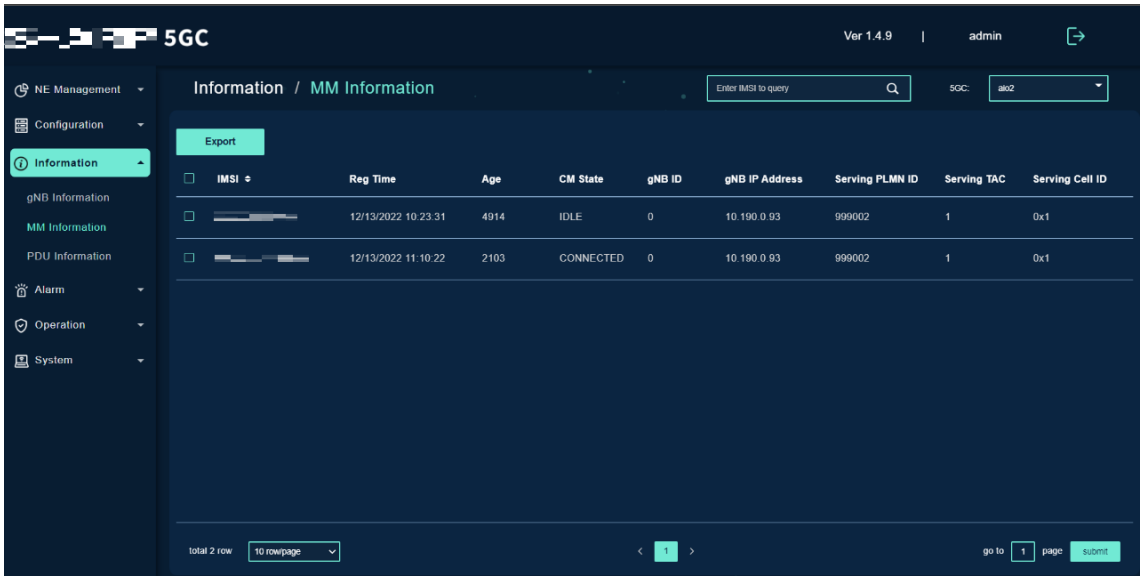


図 5-4-4-③-3　MM information

以上の在圏機能は拠点に応じて表示する画面を切り替えます。そのため拠点ごとに UE の在圏を確認することができます。

④　ネットワークスライス機能の確認の結果

ネットワークスライス検証は A 社製機器のみ、NTT 中央研修センタにおいて検証しました。

ア　eMBB 機能

eMBB に設定した UE 1 台を接続し、スループット等を検証しました。測定結果は「表 5-4-4-④-1 ネットワークスライス検証（eMBB)」のとおりです。

表 5-4-4-④-1 ネットワークスライス検証（eMBB）

			スループット [Mbps]		遅延時間 [ms]	パケット損失率 [%]		ジッタ [ms]	
			DL	UL		DL	UL	DL	UL
複数企業共用パターン	センタ UPF	eMBB	224	59	33	68	80	1ms 程度	1ms 程度
	エンド UPF	eMBB	694	56	24	0.9	81	1ms 程度	1ms 程度
業界共用パターン	センタ UPF	eMBB	689	61	25	1.6	80	1ms 程度	1ms 程度
	エンド UPF	eMBB	686	64	26	2	79	1ms 程度	1ms 程度

（ア）　eMBB スループット測定結果

スループット測定結果を「図 5-4-4-④-1　eMBB　スループット比較」に図示します。

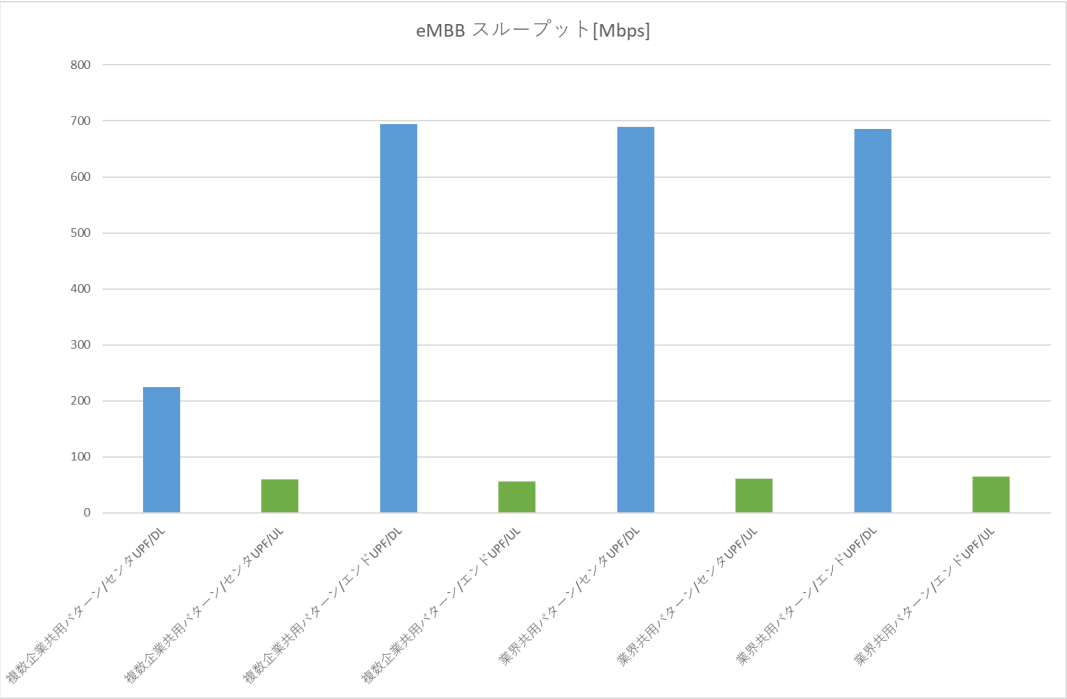


図 5-4-4-④-1　eMBB　スループット比較

eMBB の DL スループットについて測定結果を比較すると、複数企業共用パターンのエンド UPF 環境で 694Mbps、業界共用パターンのセンタ UPF 環境で 686Mbps、業界共用パターンのエンド UPF 環境で 686Mbps と高い DL スループットを実測することができました。一方、複数企業共用パターンのセンタ UPF 環境では 224Mbps であり DL スループットが大きく低下しています。

エンド UPF 構成の場合は UE～RU～DU～エンド UPF という比較的シンプルな構成であるため、スループットを低下させる要素が最小限であることで、複数企業共用パターンおよび業界共用パターンの双方で高い DL スループットを実測できたといえます。

業界共用パターンのセンタ UPF の場合は UE～RU～DU～ギャランティ回線～CU～センタ UPF という構成であり、エンド UPF と比較して経由する機器の増加等によって TCP の DL スループットが影響を受け、エンド UPF よりも DL スループットが低下したものと考えます。

複数企業共用パターンのセンタ UPF の場合は UE～RU～DU～ベストエフォート回線～CU～センタ UPF という構成であり、業界共用パターンと同様に機器の増加等による影響に加えてベストエフォート回線の区間は通信の伝送帯域・速度が保証されないことから、TCP/UDP の両方の DL スループットが大きく制限され、比較的低い DL スループットという結果になったものと考えます。

次に eMBB のパケットキャプチャを実施し、Wireshark を用いて作成した入出力グラフを「図 5-4-4-④-2　eMBB 入出力グラフ(複数企業共用パターン　センタ UPF)」～「図 5-4-4-④-5　eMBB 入出力グラフ(業界共用パターン　エンド UPF)」に図示します。

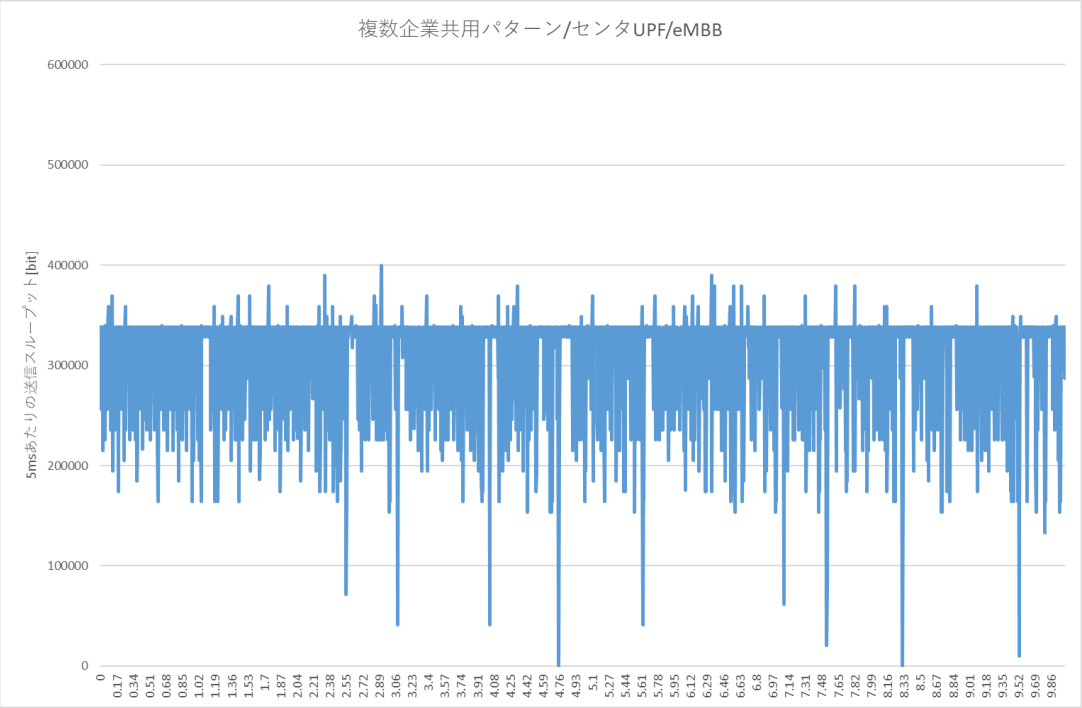


図 5-4-4-④-2　eMBB 入出力グラフ(複数企業共用パターン　センタ UPF)

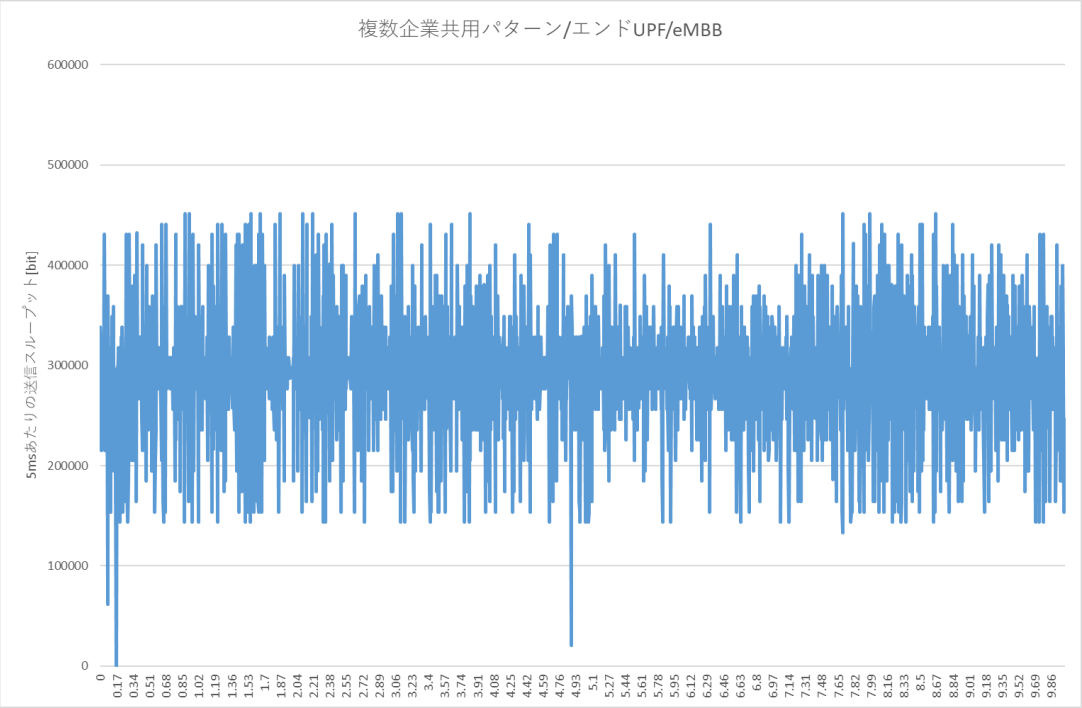


図 5-4-4-④-3　eMBB 入出力グラフ(複数企業共用パターン　エンド UPF)

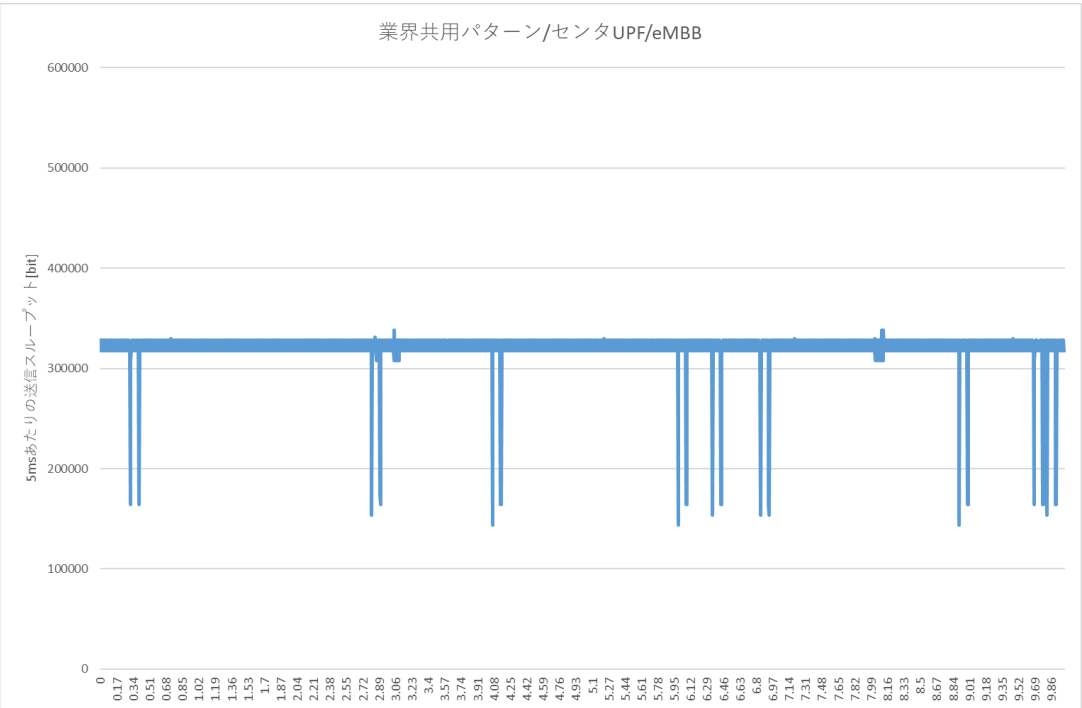


図 5-4-4-④-4　eMBB 入出力グラフ(業界共用パターン　センタ UPF)

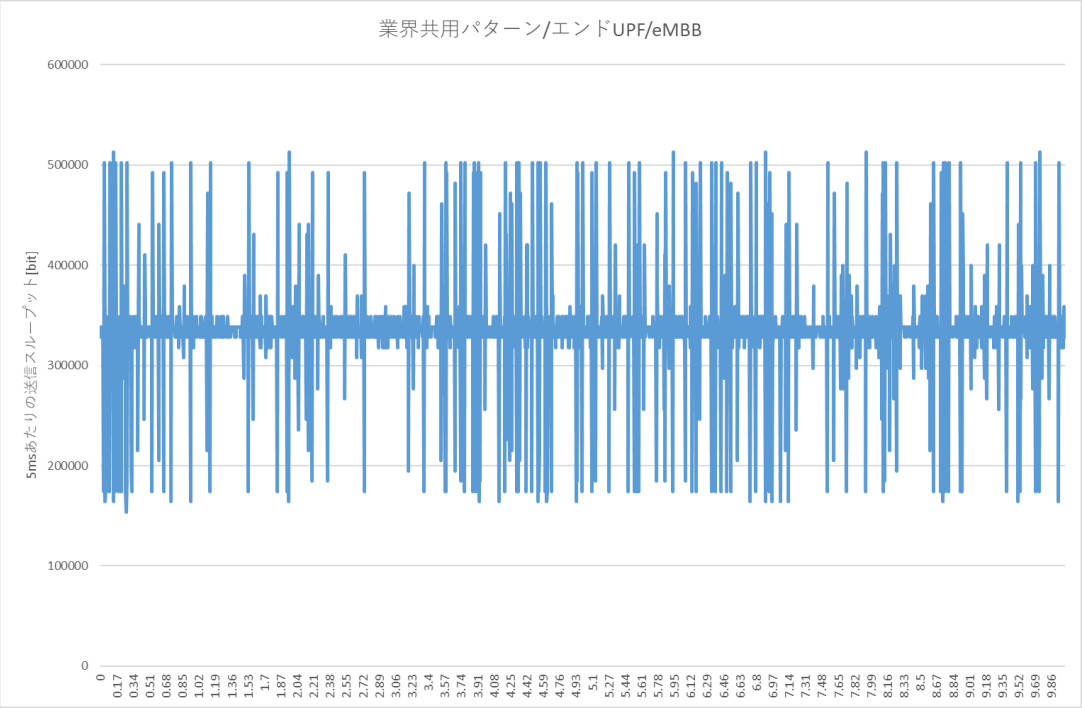


図 5-4-4-④-5　eMBB 入出力グラフ(業界共用パターン　エンド UPF)

パケットキャプチャのタイミングによってそれぞれ入出力グラフの変動に差異が生じるものですが、センタ UPF とエンド UPF の別によってグラフに傾向を見ることができます。上下に大きな変動がみられるエンド UPF に対し、センタ UPF の場合はグラフの上に抜けるピークがほとんど見られません。これはエンド拠点とセンタ拠点を接続するベストエフォート回線およびギャランティ回線を構成するネットワーク機器によって、通信パケットが均等化されていることが考えられます。

（イ）　eMBB 遅延時間測定結果

遅延時間測定結果を「図 5-4-4-④-6　eMBB　遅延時間比較」に図示します。

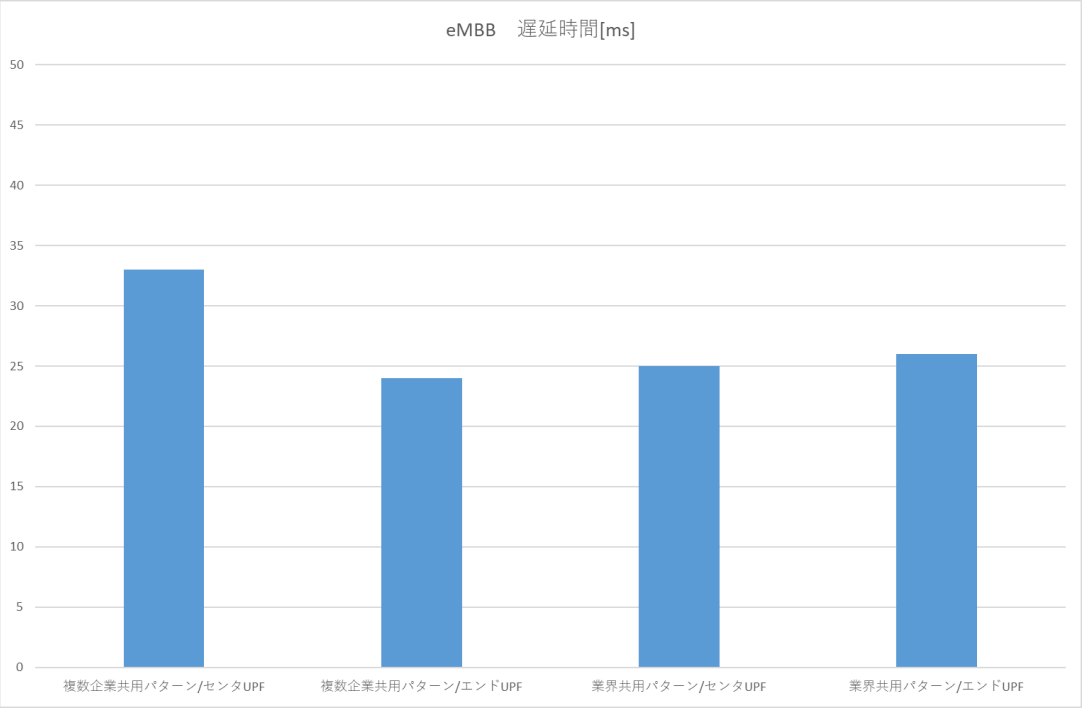


図 5-4-4-④-6　eMBB　遅延時間比較

複数企業共用パターンのセンタ UPF の場合が最も大きい遅延時間でした。業界共用パターンのセンタ UPF およびエンド UPF の場合、遅延時間はほぼ同程度という結果でした。また、この結果は「5.3　ローカル５Ｇ交換設備の共用における性能検証」と同様の結果でした。

次に 200ms 間隔で 1000Byte の ping パケットを送出しネットワークの負荷を高めた状態での遅延時間を比較するため、遅延時間測定の結果を「図 5-4-4-④-7　eMBB 遅延時間　箱ひげ図」を図示します。

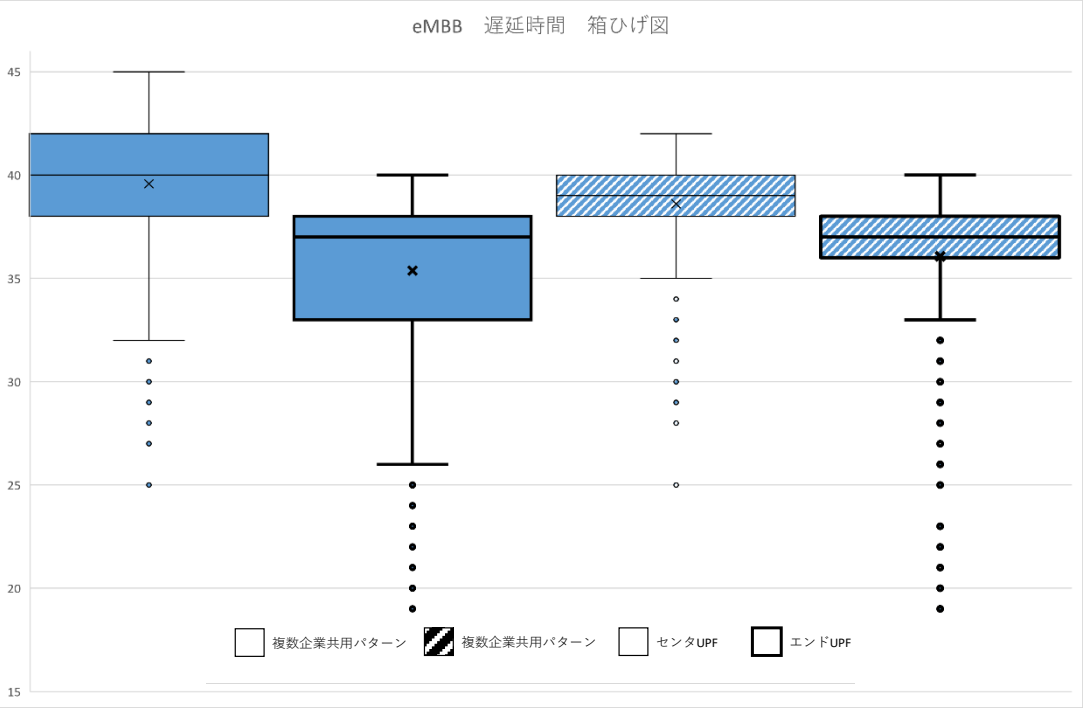


図 5-4-4-④-７　eMBB 遅延時間　箱ひげ図

ネットワーク高負荷によって、平均的な遅延時間は「図 5-4-4-④-6　eMBB　遅延時間比較」より大きくなっています。しかし同様に複数企業共用パターンおよび業界共用パターンの両方で、センタ UPF の方がエンド UPF より遅延時間が大きい傾向が見られます。これはセンタ拠点とエンド拠点の物理的な距離による遅延が影響していると考えます。また複数企業共用パターンのセンタ UPF はベストエフォート回線を経由するため、より遅延が大きい傾向であるものと考えます。

（ウ）　パケット損失率およびジッタの測定結果

パケット損失率は複数企業共用パターンのセンタ UPF 環境で高く出たものの、他の環境では同様の結果でした。この結果はスループットと一致しています。

またジッタは環境およびネットワークスライスの設定に関係なく、1ms 程度であり、ネットワークのゆらぎに影響を与えないことが確認できました。

イ　URLLC 機能

URLLC に設定した UE１台を接続し、スループット等を検証しました。測定結果は「表 5-4-4-④-2 ネットワークスライス検証（URLLC)」のとおりです。

表 5-4-4-④-2 ネットワークスライス検証（URLLC）

			スループット [Mbps]		遅延時間 [ms]	パケット損失率 [%]		ジッタ [ms]	
			DL	UL		DL	UL	DL	UL
複数企業共用パターン	センタ UPF	URLLC	224	54	25	68	82	1ms 程度	1ms 程度
	エンド UPF	URLLC	696	60	19	0.7	80	1ms 程度	1ms 程度
業界共用パターン	センタ UPF	URLLC	648	60	21	7.5	80	1ms 程度	1ms 程度
	エンド UPF	URLLC	696	60	22	0.8	80	1ms 程度	1ms 程度

（ア） URLLC スループット測定結果

スループット測定結果を「図 5-4-4-④-8 URLLC スループット比較」に図示します。

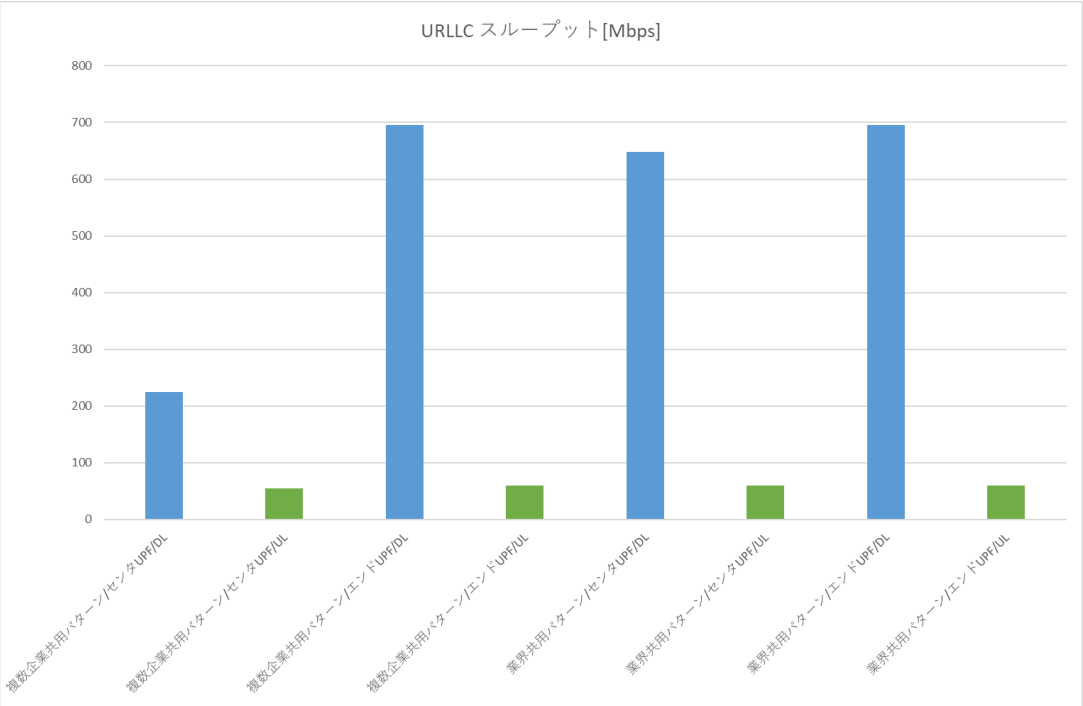


図 5-4-4-④-8 URLLC スループット比較

URLLC のスループットは eMBB のスループットとほぼ同様の結果でした。UE1 台のみが接続している状況下では eMBB と URLLC の機能に差がないためといえます。

次に URLLC のパケットキャプチャを実施し、Wireshark を用いて作成した入出力グラフを「図 5-4-4-④-9　URLLC 入出力グラフ(複数企業共用パターン　センタ UPF)」～「図 5-4-4-④-12　URLLC 入出力グラフ(業界共用パターン　エンド UPF)」に図示します。本検証で設定した URLLC 機能では UM モード（再送なし）という設定となっています。eMBB 機能ではパケットの送出は均等化されますが、UM モードによってパケット送出の即応性が高まることでスループットが短時間でバースト的に増加します。これにより URLLC 機能に設定した場合は入出力グラフでバースト上の波形（マイクロバースト信号）を観測することができます。

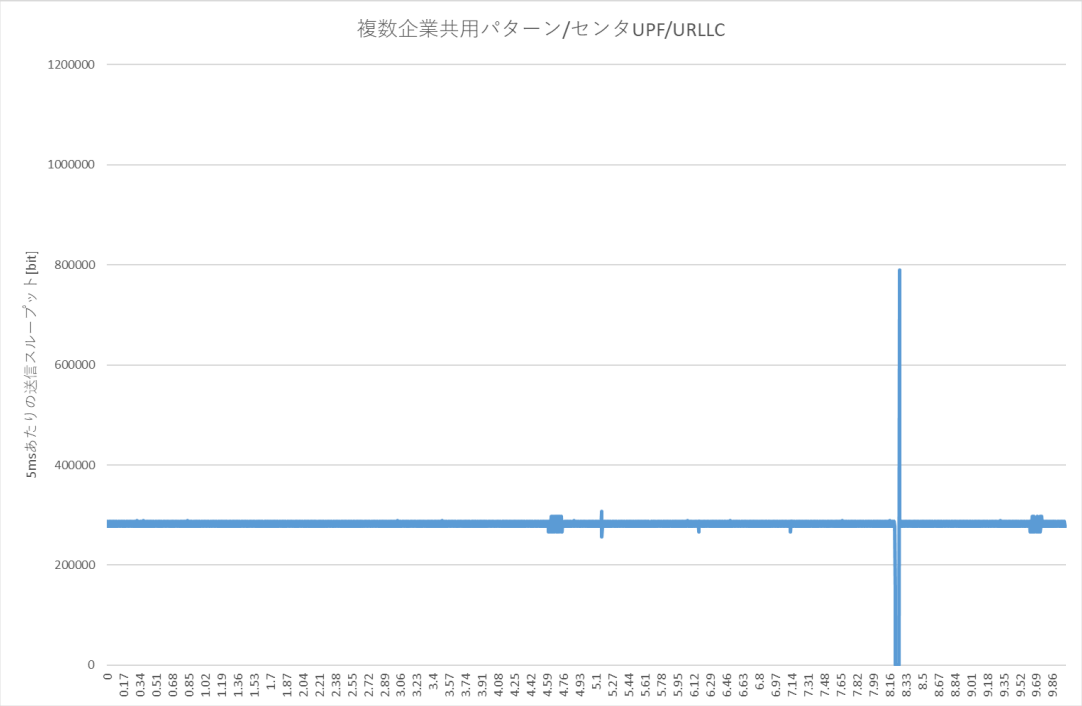


図 5-4-4-④-9　URLLC 入出力グラフ(複数企業共用パターン　センタ UPF)

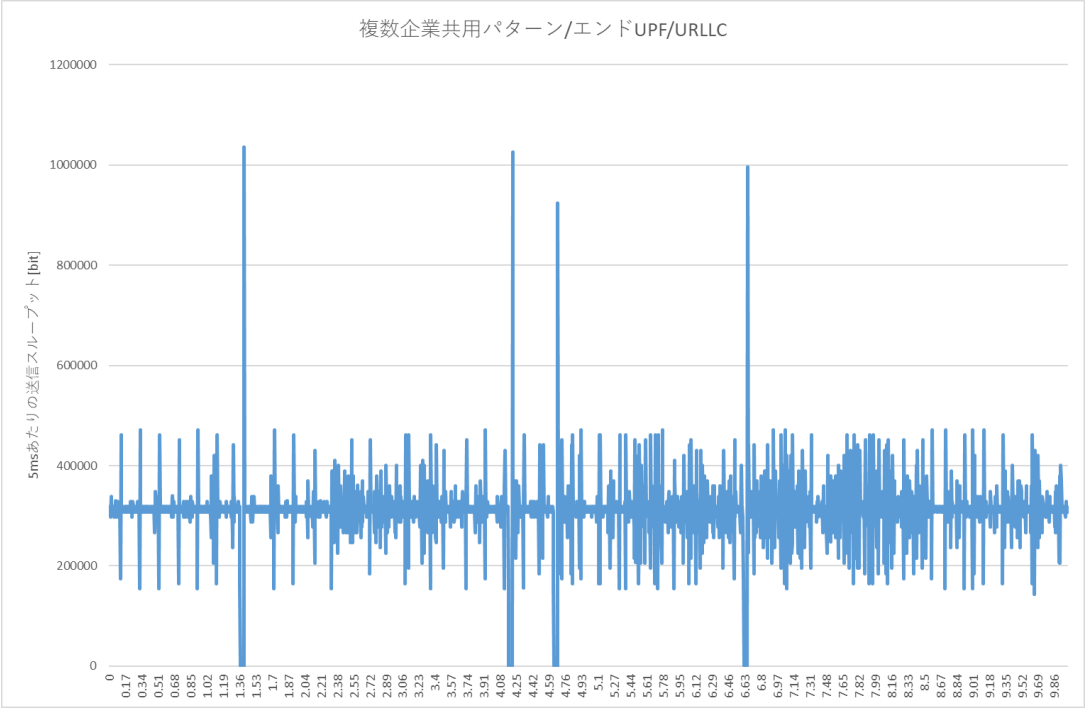


図 5-4-4-④-10　URLLC 入出力グラフ(複数企業共用パターン　エンド UPF)

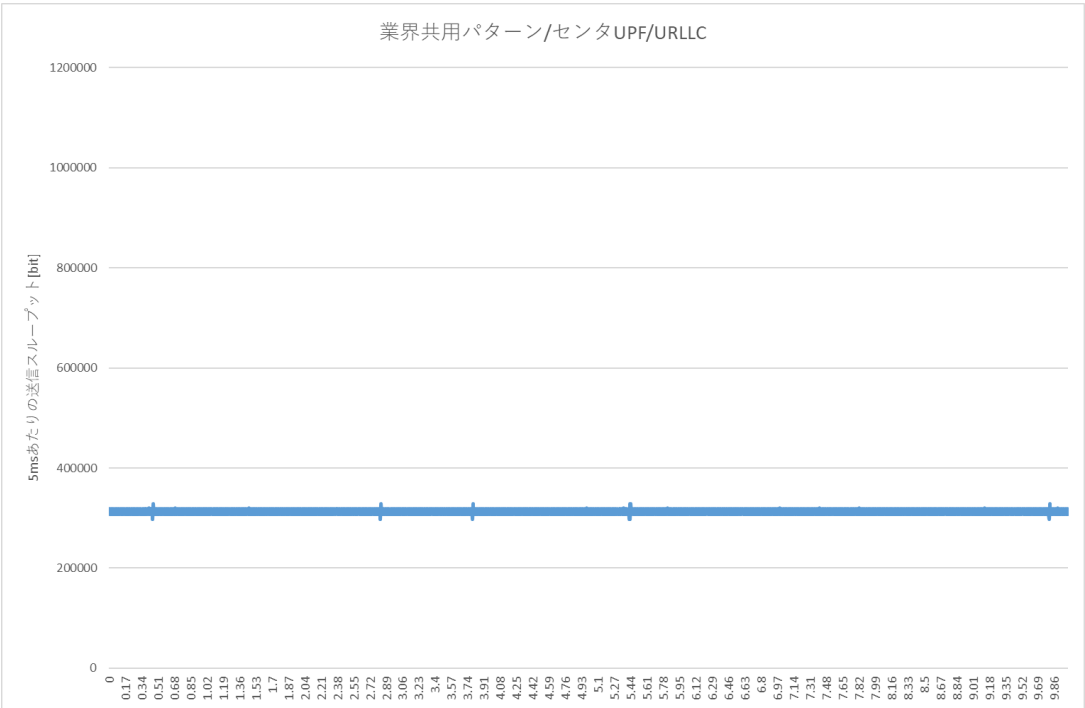


図 5-4-4-④-11　URLLC 入出力グラフ(業界共用パターン　センタ UPF)

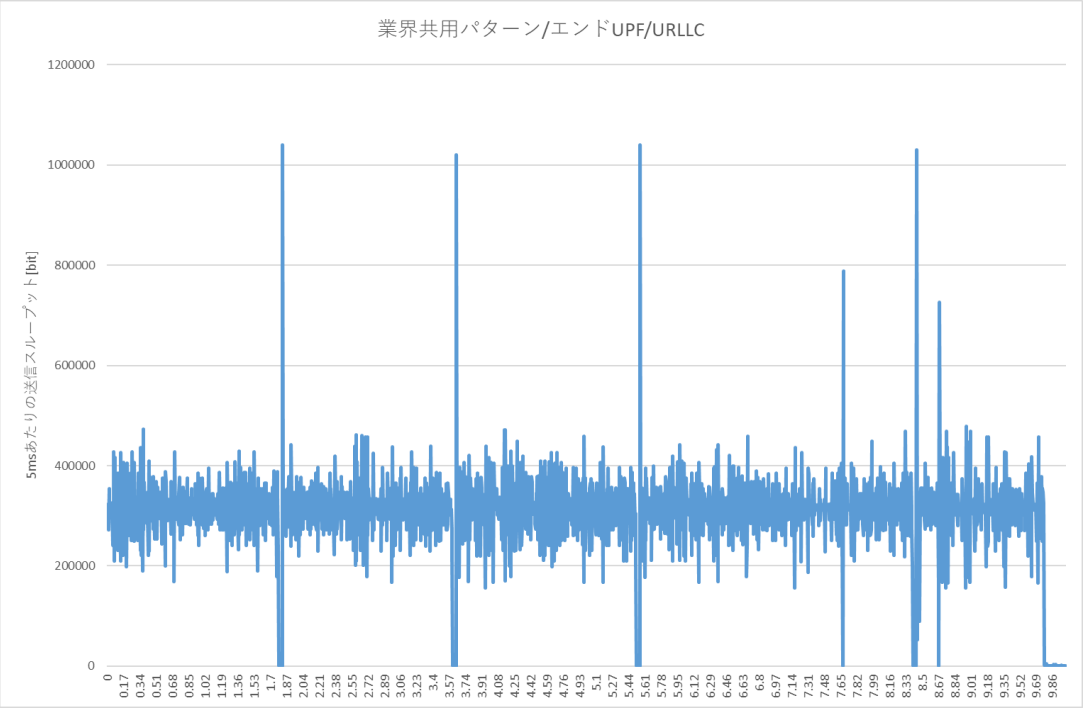


図 5-4-4-④-12　URLLC 入出力グラフ(業界共用パターン　エンド UPF)

複数企業共用パターンおよび業界共用パターンのどちらもエンド UPF 環境では入力したマイクロバースト信号をピークとして波形から観測することができます。

一方、センタ UPF 環境の場合には、ピークを観測できませんでした。これはエンド拠点とセンタ拠点を接続するベストエフォート回線およびギャランティ回線を構成するネットワーク機器によって、通信パケットが均等化されていることが考えられます。この結果から、WAN 回線を経由するセンタ UPF 環境では URLLC 機能バースト的に増加するスループットを十分に再現できない可能性が考えられます。

（イ）　遅延時間測定結果

遅延時間測定結果を「図 5-4-4-④-13　URLLC　遅延時間比較」に図示します。

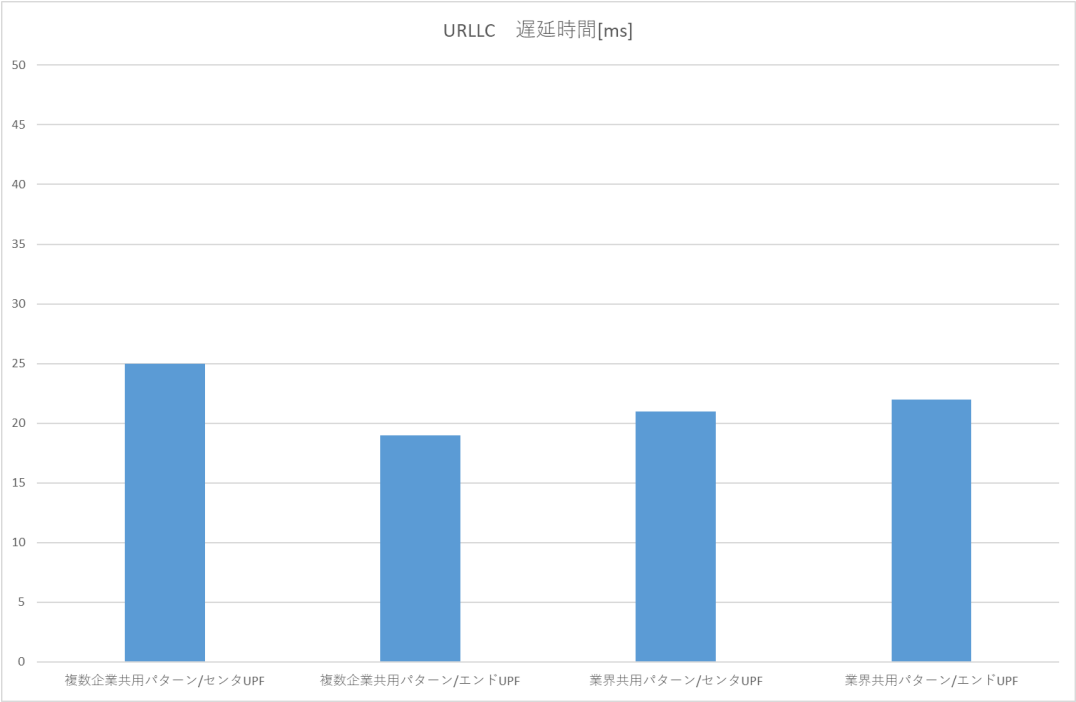


図 5-4-4-④-13　URLLC　遅延時間比較

それぞれの環境の違いによる差は「図 5-4-4-④-6　eMBB　遅延時間比較」で示した eMBB の場合と同様といえます。

次に 200ms 間隔で 1000Byte の ping パケットを送出しネットワークの負荷を高めた状態での遅延時間を比較するため、遅延時間測定の結果を「図 5-4-4-④-14　URLLC　遅延時間箱ひげ図」を図示します。

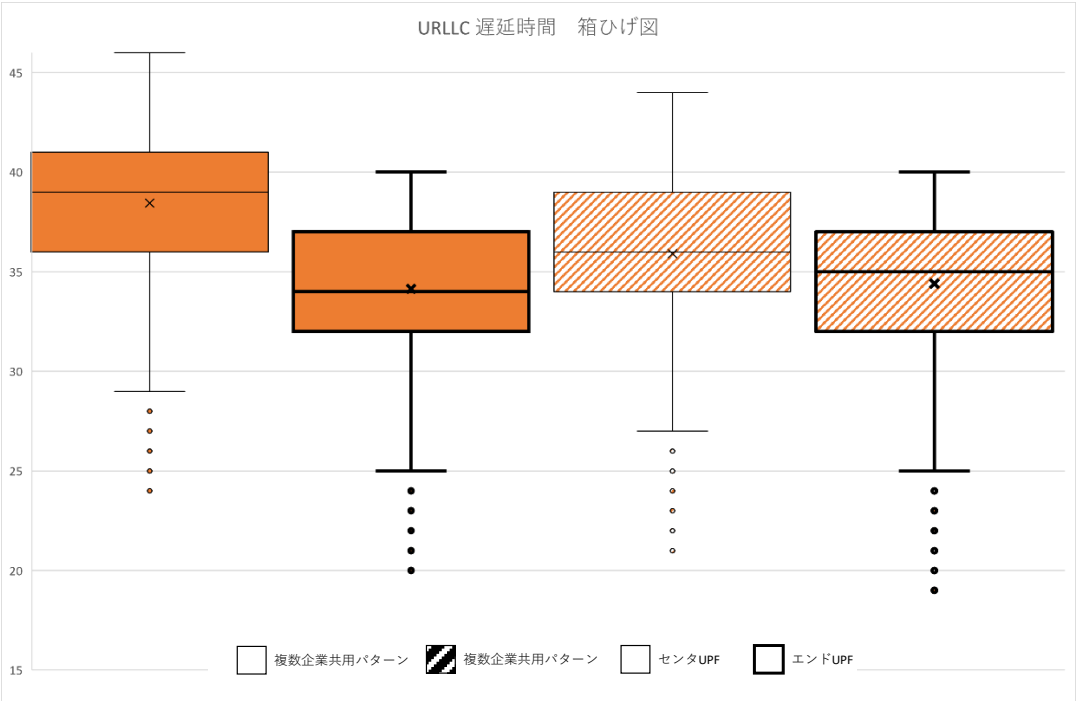


図 5-4-4-④-14　URLLC 遅延時間　箱ひげ図

ネットワーク高負荷によって、平均的な遅延時間は「図 5-4-4-④-12　URLLC　遅延時間比較」より大きくなっています。しかし同様に複数企業共用パターンおよび業界共用パターンの両方で、センタ UPF の方がエンド UPF より遅延時間が大きい傾向が見られます。これは eMBB と同じく拠点間の物理的な距離および回線種別の影響によるものと考えます。eMBB と URLLC の比較は「ウ　eMBB/URLLC 同時接続」の項で行います。

（ウ）　パケット損失率およびジッタの測定結果

パケット損失率は複数企業共用パターンのセンタ UPF 環境で高くでたものの、他の環境では同様の結果でした。この結果はスループットと一致しています。

またジッタは環境およびネットワークスライスの設定に関係なく、1ms 程度であり、ネットワークのゆらぎに影響を与えないことが確認できました。

ウ　eMBB/URLLC 同時接続

eMBB に設定した UE 1 台および URLLC に設定した UE 1 台を同時に接続し、スループット等を検証しました。結果は「表 5-4-4-④-3　ネットワークスライス検証（eMBB,URLLC 同時）」のとおりです。

表 5-4-4-④-3 ネットワークスライス検証（eMBB,URLLC 同時）

			スループット [Mbps]		遅延時間 [ms]	パケット損失率 [%]		ジッタ [ms]	
			DL	UL		DL	UL	DL	UL
複数企業共用パターン	センタ UPF	eMBB	148	24	32	50.7	50.7	1ms 程度	1ms 程度
		URLLC	76	9	31	74.7	74.7	1ms 程度	1ms 程度
	エンド UPF	eMBB	201	24	26	29.3	29.3	1ms 程度	1ms 程度
		URLLC	78	9	24	74.0	74.0	1ms 程度	1ms 程度
業界共用パターン	センタ UPF	eMBB	211	24	26	29.7	29.7	1ms 程度	1ms 程度
		URLLC	78	8	26	74.0	74.0	1ms 程度	1ms 程度
	エンド UPF	eMBB	211	24	24	29.7	29.7	1ms 程度	1ms 程度
		URLLC	77	9	25	74.3	74.3	1ms 程度	1ms 程度

（ア）　スループット測定結果

スループット測定結果を「図 5-4-4-④-15　同時設定　スループット比較」に図示します。

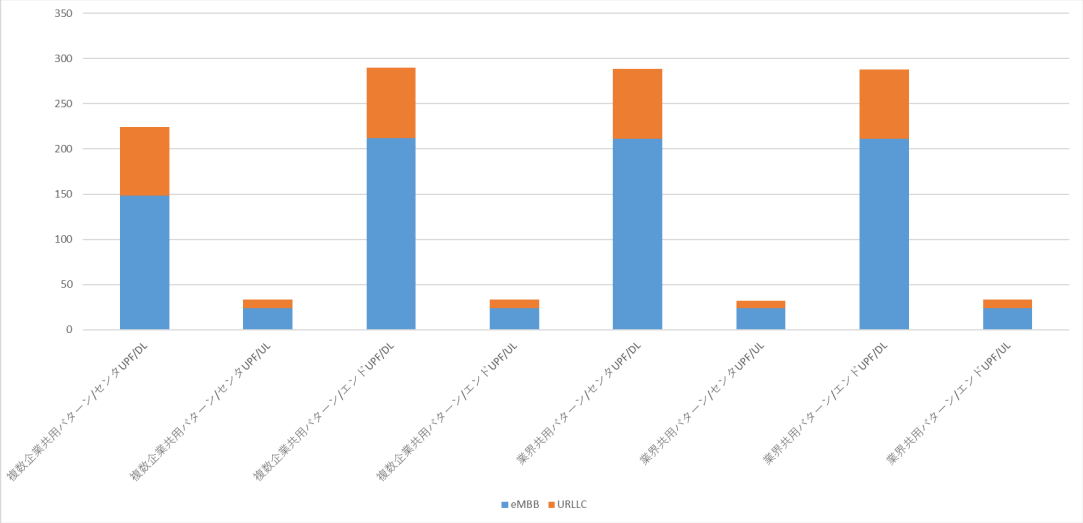


図 5-4-4-④-15　同時設定　スループット比較

スループットの数値は性能検証等と比べて低い値となりました。検証時点ではネットワークスライス機能において eMBB/URLLC 同時接続の設定は開発段階であり、使用可能なリソースブロック数および変調方式に制限があるためです。そのため性能検証時と比べて eMBB では 3 割程度、URLLC では 1 割程度までスループットが低下し合計で 300Mbps 弱という結果でした。

また複数企業共用パターンのセンタ UPF 環境では合計のスループットが他の環境を下回っています。これはベストエフォート回線によって通信帯域に制限を受けたためと考えます。

次にパケットキャプチャを実施し、Wireshark を用いて作成した入出力グラフを「図 5-4-4-④-16　同時設定入出力グラフ(複数企業共用パターン　センタ UPF)」～「図 5-4-4-④-19 同時設定入出力グラフ(業界共用パターン　エンド UPF)」に図示します。

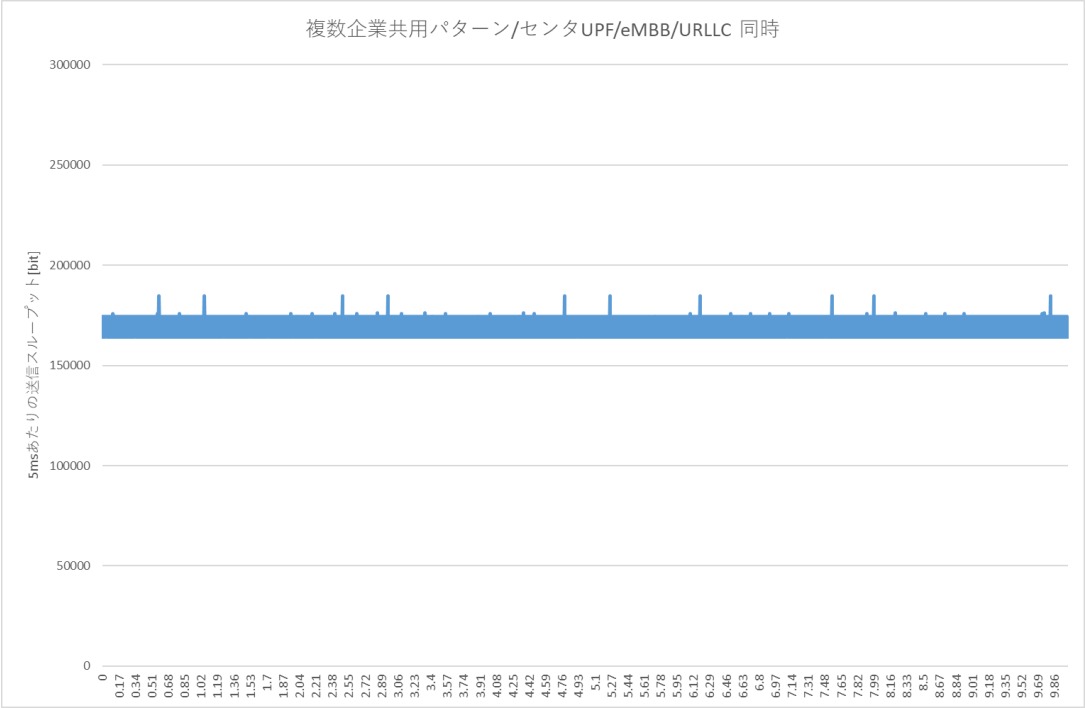


図 5-4-4-④-16　同時設定入出力グラフ（複数企業共用パターン　センタ UPF）

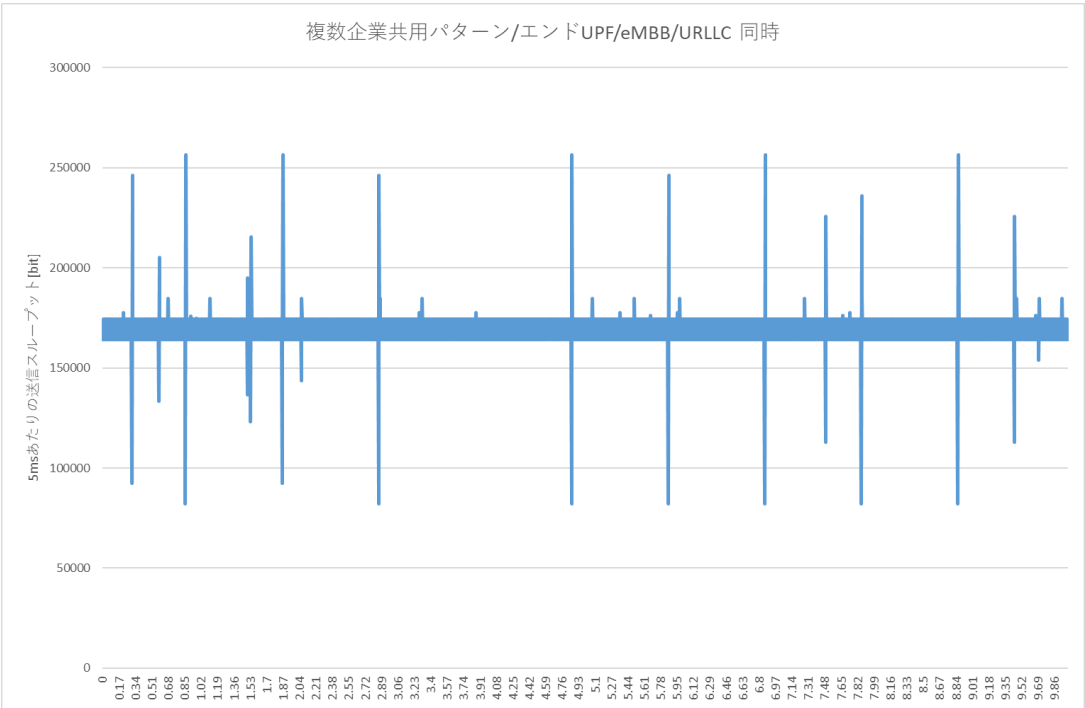


図 5-4-4-④-17　同時設定入出力グラフ（複数企業共用パターン　エンド UPF）

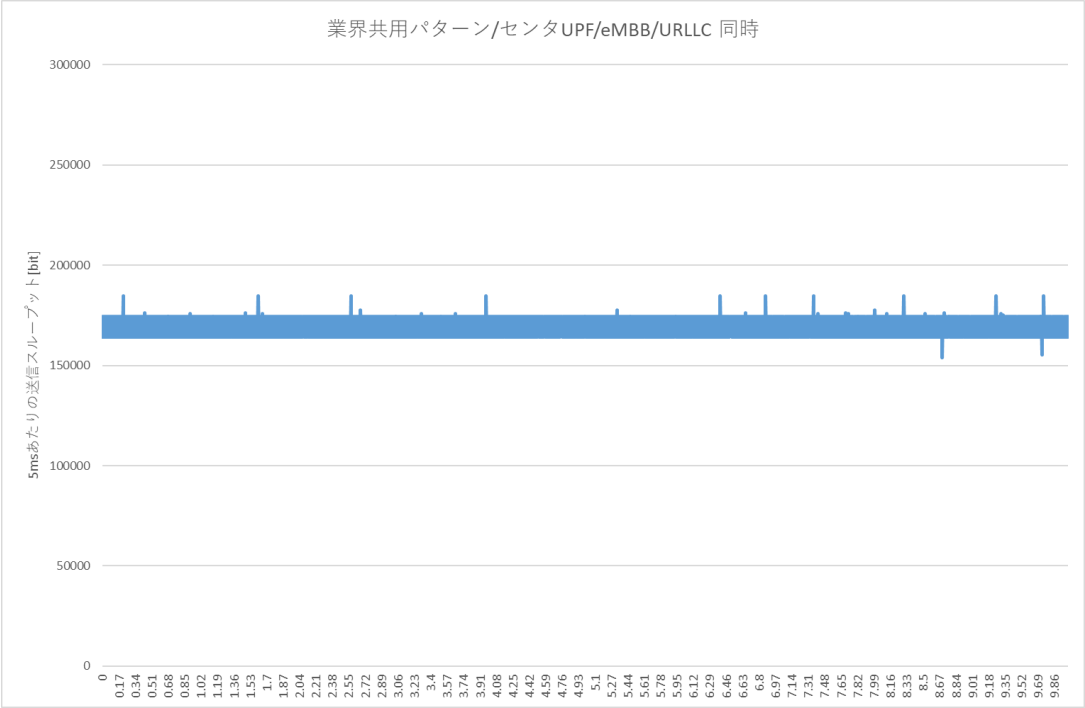


図 5-4-4-④-18　同時設定入出力グラフ(業界共用パターン　センタ UPF)

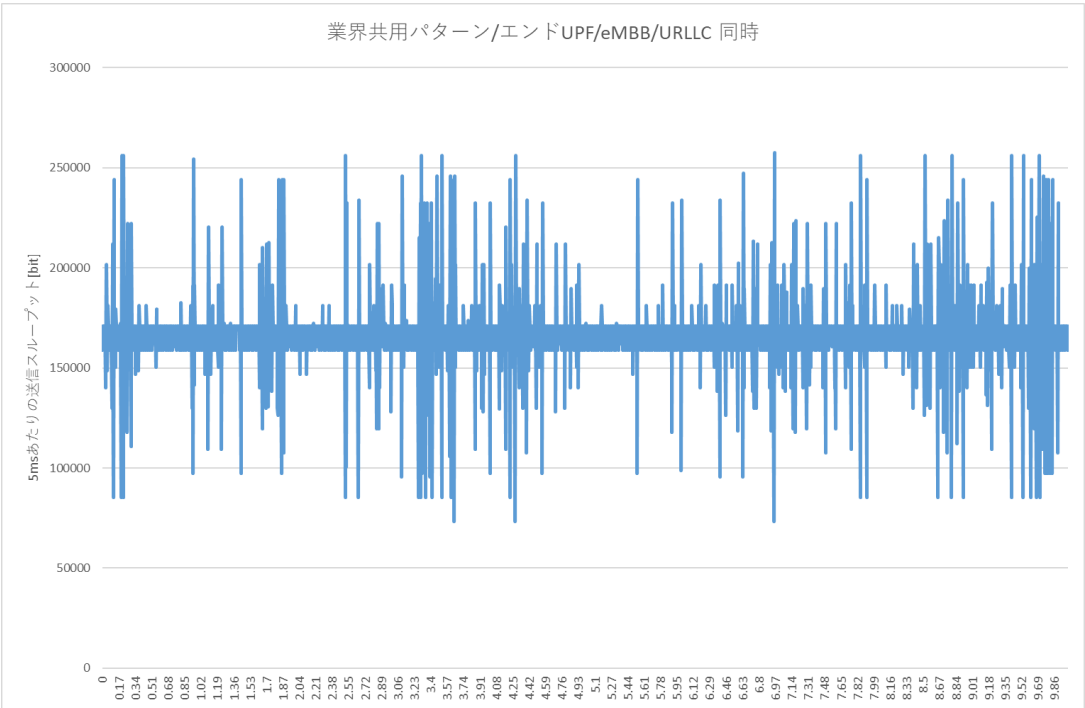


図 5-4-4-④-19　同時設定入出力グラフ(業界共用パターン　エンド UPF)

eMBB/URLLC 同時接続の場合もエンド UPF ではマイクロバースト信号のピークがグラフ中に登場しているといえます。一方センタ UPF ではピークが見えず、スループットが均等化されているものと考えます。

（イ）　遅延時間測定結果

遅延時間測定結果を「図 5-4-4-④-20　同時設定　遅延時間比較」に図示します。

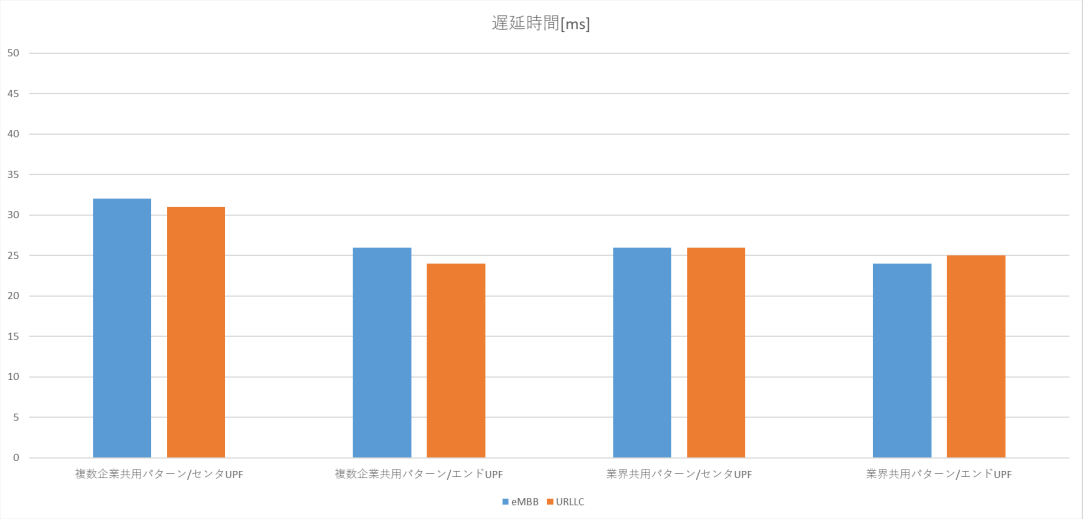


図 5-4-4-④-20　同時設定　遅延時間比較

それぞれの環境の違いによる差は本項アおよびイにおいて eMBB と URLLC それぞれを単独運用で測定した結果と同様です。これは良好な通信環境では伝送遅延に対する eMBB と URLLC の機能に差がないためと考えます。

次に 200ms 間隔で 1000Byte の ping パケットを送出しネットワークの負荷を高めた状態での遅延時間を比較するため、遅延時間測定の結果を「図 5-4-4-④-21　eMBB 遅延時間　箱ひげ図」を図示します。

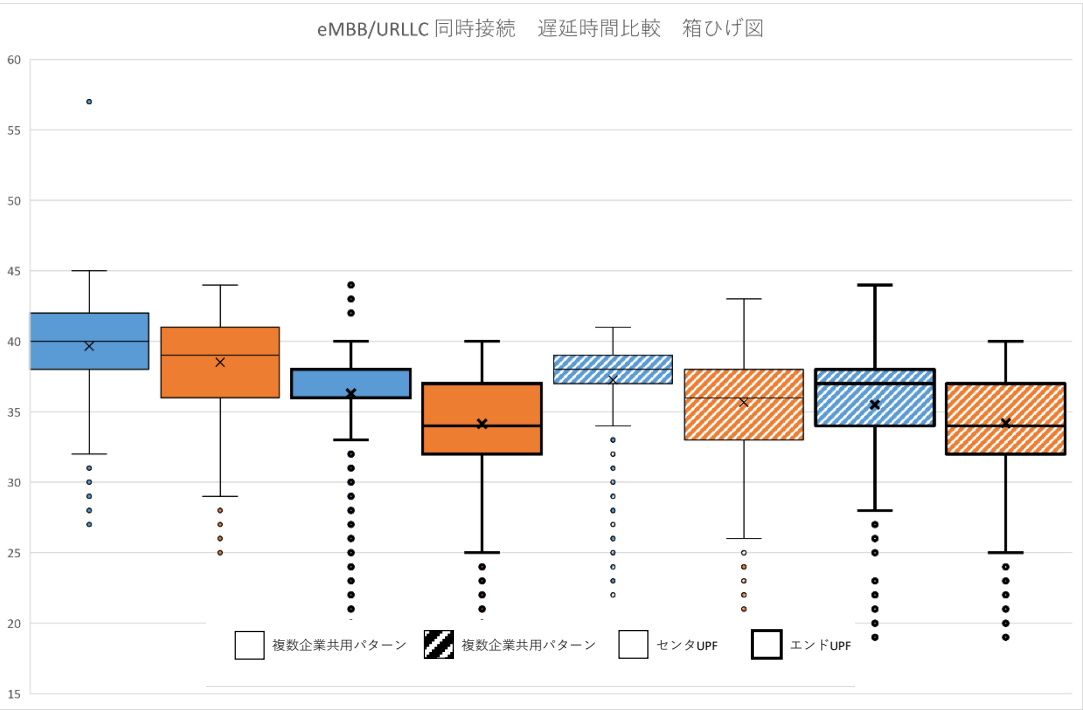


図 5-4-4-④-21　eMBB 遅延時間　箱ひげ図

隣り合った 2 つずつの組み合わせで見ることで、同時に接続した場合に eMBB よりも

URLLC の方が遅延時間が小さくなる傾向が確認できます。
エンド UPF の場合は複数企業共用パターンと業界共用パターンとで大きな差は見られません。
センタ UPF で比較すると複数企業共用パターンの eMBB は突出して大きな遅延時間のデータが含まれています。URLLC も他の環境より遅延時間が大きい傾向が見受けられます。これはベストエフォート回線による影響と考えられます。
業界共用パターンではエンド UPF と比較すると遅延時間が大きくなります。これはセンタ拠点とエンド拠点の物理的な距離による遅延が考えられます。
したがって、遅延時間の改善にはどの環境でも URLLC の設定が有効であると考えます。

（ウ）　パケット損失率およびジッタの結果
パケット損失率は複数企業共用パターンのセンタ UPF 環境で高くでたものの、他の環境では同様の結果でした。この結果はスループットと一致しています。
またジッタは環境およびネットワークスライスの設定に関係なく、1ms 程度であり、ネットワークのゆらぎに影響を与えないことが確認できました。

(5) まとめ

機能検証の結果を下記のとおりまとめます。
① 管理機能等
R3 年度に実施した A 社製機器の検証結果および本検証で実施した B 社製機器の検証結果を「表 5-4-5-① 管理機能の実装一覧」にまとめました。

表 5-4-5-① 管理機能の実装一覧

機能	A 社製機器				B 社製機器			
	実装の有無	ログの格納状況	端末別の管理	拠点毎の閲覧・管理	実装の有無	ログの格納状況	端末別の管理	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	○	○	○	○	○	-※	○	○
管理権限	○	○		○	○	-※		○
その他		ログ閲覧により ALERT 確認可能	端末ごとにエンド UPF/センタ UPF の接続先設定が可能			GUI で ALERT 確認可能		

※　ベンダーにおいて将来の実装を検討予定とのこと

R3 年度に実施した A 社製機器ではログの閲覧によって SIM 認証情報の登録等、各管理機能に関する操作履歴を確認することができるうえ、5GC 上で検知する ALERT についてもログから確認することができました。またポリシー管理として AMBR によって UE が出力可能な伝送スループットの上限値を UE ごとに設定することが可能でした。本検証で確認した B 社製機器では 5GC 上で検知する ALERT が GUI 上に自動で表示されるため、ALERT の発生をリアルタイムに検知することができました。各管理機能のログの格納は本検証時点で機能として提供されていませんでしたが、将来実装されることが望ましいです。またポリシー管理は拠点ごとに 5QI を設定することが可能というものでした。AMBR の UE ごとの設定は、将来の実装を検討予定とのことでした。このように製品によって差が見られたものの、本検証によってコア共用の環境下でローカル５Ｇシステムを管理運営するにあたり、必要な機能が A 社製機器および B 社製機器の双方で実装されていることを確認できたものと考えます。SIM 認証管理は、IMSI 番号などの SIM 情報、K 値や OPc 値といった暗号化情報等の登録および閲覧を行うための機能です。コアへ UE の追加登録、登録変更、登録削除を行い、UE をローカル５Ｇシステムで利用可能とするために不可欠な機能です。本検証では SIM 認証管理をコア共用サービスとして提供する SIer が担う想定で検証しました。例えば UE の接続可否を利用シーンに応じて柔軟に変更するといったユースケースでは、ユーザ企業等自身が直接 SIM 認証を管理することを望むケースも考えられます。今後の開発によって、SIM 認証機能のみを分離してユーザ企業がエンド拠点で利用することで、ユースケースに対する更なる柔軟性の向上が期待できます。操作性の向上が実現することで運用時の利便性がさらに増すものと期待できます。

端末情報管理およびセッション管理は、SIM 認証管理機能によって登録された SIM を実装した UE について、接続状態であるか否か、通信中であるか否かを表示することで UE の運用実態を確認できる機能です。例えば監視カメラのように、特定の UE に対して定常的に接続中および通信中であることを要求するユースケースでは、本機能を元に監視体制を構築することで、システムの正常性確認に有効であると考えます。また、本検証では IMSI 番号によってどの UE であるかを識別しています。UE が多種類存在するユースケースでは、UE の型名や外観等を登録したデータベースと連携することで、どの UE に関する端末情報およびセッション情報であるかが、視覚的に区別できると考えます。このように監視体制等との連携や GUI のデザインをユースケースに応じて工夫することで、将来的に運用時の利便性がさらに増すものと期待できます。

ポリシー管理は、エンド拠点ごとまたは UE ごとにネットワーク上の挙動を制御するためのポリシー設定を行う機能です。例えば、単信音声のようなユースケースでは、リアルタイム性が要求されますが小容量の通信が主となります。対してセンサ類に蓄積したログを一括で送出するようなユースケースでは大容量の通信が主となります。これらの多様なユースケースに対し、適切なポリシーを設定することで柔軟なネットワーク構築でのユーザニーズへの対応が期待できるものと考えます。また本検証で確認できたポリシー設定は限定的であったため、今後の開発・検証によって多様なポリシーに対応した高機能化の実現が望ましいと考えます。

管理権限は、コア等を共用した環境下において複数のエンド拠点を個別に管理するため、コアの各機能へのアクセス権限をエンド拠点ごとに分離する機能です。本検証ではコアへのログイン画面、Username、Password によって実現しています。ユーザによってはユーザ自らによるコアの操作を最小限とし、例えばポリシー管理などは SIer に委任することを望むことが考えられます。そういったユーザニーズに対応するため、ユーザ向け管理画面と SIer 向け管理画面をそれぞれ用意するなど、今後の高機能化が望ましいと考えます。

② トラヒックモニタリング検証

A 社製機器では、スループットおよびパケットダイヤグラムを UE(IMSI 番号)ごとに色分けされたグラフによって表示することが可能です。またグラフのピークに応じて縦軸のスケールが自動的に追従します。そのため UE ごとの時単位や分単位といった短期的な通信量の変動を確認することに適していると考えます。一方、B 社製機器では、エンド拠点(CU)におけるスループットの総量をグラフによって表示することが可能です。縦軸スケールが固定であり、拠点における日単位や月単位といった長期的な通信量の変動の確認に適していると考えます。また 2 社双方とも UPF の通信ポートにおけるスループットに相当する数値をグラフ化しています。そのため、DL ではトラヒックモニタ機能でグラフ表示されたスループットと実際に UE へ到達しているスループットが乖離している可能性があることに注意が必要です。このように製品によって差が見られたものの、本検証によってトラヒックモニタリングの機能が A 社製機器および B 社製機器の双方で実装されていることを確認できました。

本機能はコア等を共用した環境をサービスとしてユーザへ提供する SIer にとっては、ユーザごとの通信量に応じた従量課金システムの構築において必要であると考えます。また、エンド拠点で端末を運用するユーザにとっても UE またはローカル５Ｇシステムの運用実態を確認するために有効な機能であると考えます。このように本機能はユーザニーズおよび SIer のニーズが高いと考えられることから、グラフ表示のデザイン工夫や通信量の統計といった機能の追加によってさらに実用性が向上することを期待できます。

③ 在圏機能検証

在圏機能は、接続中のある UE がどの拠点のどの基地局と接続しているか確認する機能です。A 社製機器および B 社製機器の双方で接続中の UE（IMSI 番号）がどの基地局 ID と接続しているか表示する機能が実装されていることを確認できました。

本機能は、拠点ごとに UE 接続数を把握することで、コア等を共用した環境をサービスとしてユーザへ提供する SIer は利用者数に応じた従量課金システムの構築に必要であると考えます。また基地局と UE の通信の正常性確認や複数の基地局がある拠点ではハンドオーバー機能の確認および管理をすることができます。さらに基地局の利用率について統計を取ることによって、基地局の再配置検討に有効な情報を取得できます。UE の大まかな位置を取得することにも利用できるなど、今後、ユースケースに応じて柔軟に高機能化されていくことが望ましいと考えます。

④ ネットワークスライス機能

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

5.5 ローカル５Ｇ交換設備の共用におけるセキュリティ検証

(1) 検証目標

コア/CU 共用下において、ローカル５Ｇシステムにおけるセキュリティの懸念や対策についての検討が必要になります。本調査研究では、コア/CU 共用の実現に向けた課題やセキュリティ向上のために実装が必要とされる機能等を整理しました。

R3 年度の調査研究では、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、コアを共用した環境下におけるローカル５Ｇシステムの外部/内部ネットワークからの攻撃に対するセキュリティを評価し、セキュリティを向上させる手段を見出すための検証を行いました。結果として、CU-コア間通信の傍受や他拠点からの侵入等の外部からの攻撃に対しては IPsec が有効であることと、エンド拠点からコア装置への攻撃や侵入されたコアから UPF への攻撃に対してはファンクション別のファイアウォールが有効であることが示されました。

R4 年度の調査研究ではさらにセキュリティ検討範囲を広げ、コアに加え CU を共用した環境で新たに発生する拠点間通信への攻撃に対するセキュリティと、端末からの不正通信や SIM の不正利用等の攻撃に必要なセキュリティに対して検証を行いました。R3・R4 年度の調査研究結果を通して、想定しうる各種セキュリティホールについて網羅的に検証が行えたことになります。

① CU-DU 区間通信の暗号化

オンプレミス構成においては CU-DU 区間の通信は暗号化されないことが一般的です。しかし、本調査検証においては CU を複数ユーザで共有し異なる拠点に設置する構成をとるため、CU-DU 区間が遠隔での通信となり経路上での盗聴のリスクがあります。

CU-DU 区間を流れる通信には、端末認証情報等の重要情報が含まれているため、3GPP では CU-DU 区間には認証・権限付与、完全性保護、機密保持が必須であると定義されています。(文書番号：ETSI TS 133 501 V15.2.0 (2018-10))

本調査研究では CU-DU 区間の通信に IPsec を用い、その効果を確認しました。IPsec の鍵交換においては Diffie-Hellman 方式（以下、DH 方式)を採用しました。また、さらに高度なセキュリティを求めるユーザを想定して、量子暗号鍵交換方式の有効性についても検証を行いました。

本検証の構成を「図 5-5-1-1 検証構成（CU-DU 区間通信の暗号化)」に、検証イメージを「図 5-5-1-2 検証イメージ（CU-DU 区間通信の暗号化)」に示します。通常、量子暗号鍵交換方式を用いる際は各拠点のオンプレミス環境にセキュリティ製品を導入し、拠点間を光ファイバーで直接接続することが必要ですが、本調査研究では、検証用に準備されたパブリッククラウド上で交換・生成した量子暗号鍵をインターネット経由で ETSI で標準化された API を用いて各拠点のセキュリティ装置に配布し、拠点間通信の暗号化を行いました。(文書番号：ETSI GS QKD 014 V1.1.1 (2019-02))

② セキュリティ機能付き SIM を用いた端末のセキュリティ

R3 年度の調査研究ではコア装置～基地局装置間のセキュリティについて検証しましたが、本年度は無線および端末側のセキュリティについて検証を行いました。

具体的には、SIM スワッピング等の SIM の不正な利用や、SIM が搭載された端末からの不正通信のようなセキュリティリスクに対し、SIM が搭載されている端末が正規の端末か否かを判別できるセキュリティ機能付き SIM を用いて、当該 SIM が搭載された端末からの通信を検知・遮断できることを確認しました。

また、数多くの端末の接続が想定されるローカル５Ｇにおいては、不正な通信を行った端末への対応稼働の負荷が想定されるため、それら管理稼働削減のための接続端末の可視化方法についても検証を行いました。

本検証の結果を踏まえ、コア/CU 共用環境下においてユーザ環境や通信の内容に応じたセキュリティの推奨設定について検討し、セキュリティコストと比較を行い、端末のセキュリティレベルのモデル化を行いました。

本検証の構成を「図 5-5-1-3 検証構成の概要（セキュリティ機能付き SIM を用いた端末のセキュリティ」に、検証イメージを「図 5-5-1-4 検証イメージ（セキュリティ機能付き SIM を用いた端末のセキュリティ)」に示します。各拠点の端末にセキュリティ機能付き SIM を挿入し、センタ拠点に端末通信を監視する監視装置と端末管理システムが搭載された端末管理装置を設置しました。また、エンド UPF を使用した際の検知を行うため NTT 中央研修センタにも監視装置を設置しました。監視装置にて検知した不正な通信に対し、端末管理システムから SIM 隔離等の措置を行いました。また、端末管理システムでは通信の可視化も行いました。

本調査研究では、セキュリティ機能付き SIM/監視装置(TMMNS Inspector)/端末管理システム(TMMNS マネジメント)にトレンドマイクロ社の製品を使用し、同社および伊藤忠テクノソリューションズ株式会社とともに端末セキュリティレベルのモデル化を実施しました。

表 5-5-1-1　セキュリティ検証対象箇所および検証拠点

共用パターン	CU-DU 区間通信の暗号化		セキュリティ機能付き SIM を用いた端末のセキュリティ	
	IPsec 通信の確立	CU-DU 区間の遅延測定	セキュリティ脅威の検知・遮断	端末状態の監視・可視化
業界共用ﾊﾟﾀｰﾝ	NTT 中央研修センタ※1	NTT 中央研修センタ、各大学	NTT 中央研修センタ※1	NTT 中央研修センタ、いずれかの大学
複数企業共用ﾊﾟﾀｰﾝ	NTT 中央研修センタ※1	NTT 中央研修センタ、いすゞ自動車	NTT 中央研修センタ※1	NTT 中央研修センタ、いすゞ自動車

※1：ロケーションによる差分がないため NTT 中央研修センタでのみ実施

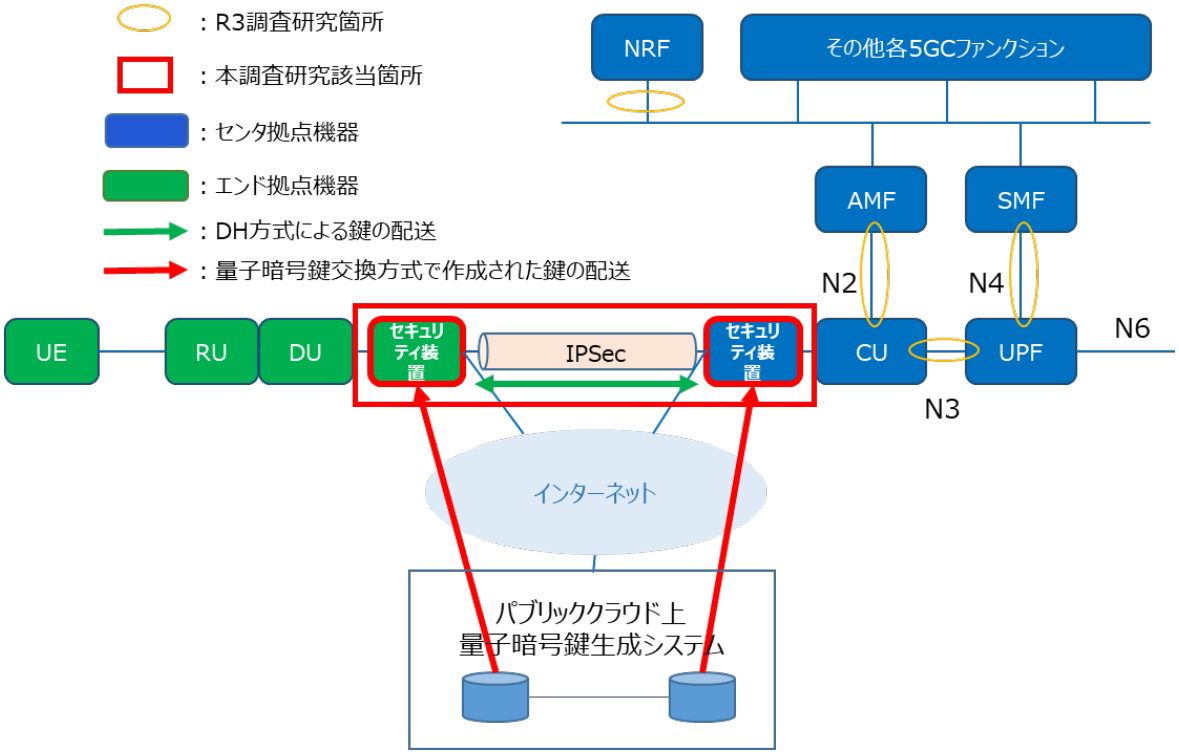


図 5-5-1-1 検証構成（CU-DU 区間通信の暗号化）

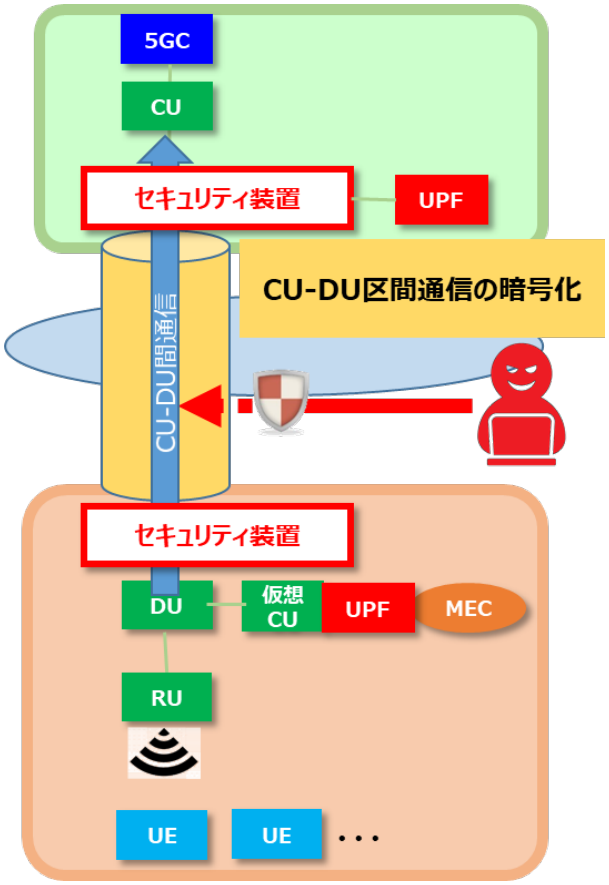
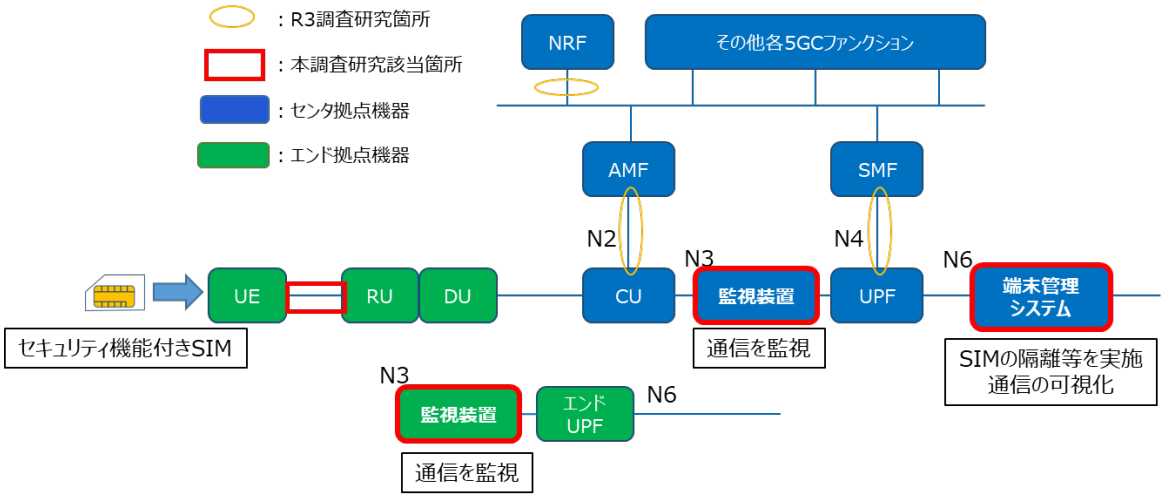


図 5-5-1-2　検証イメージ（CU-DU 区間通信の暗号化）



※中研のみ

図 5-5-1-3　検証構成概要（セキュリティ機能付き SIM を用いた端末のセキュリティ）

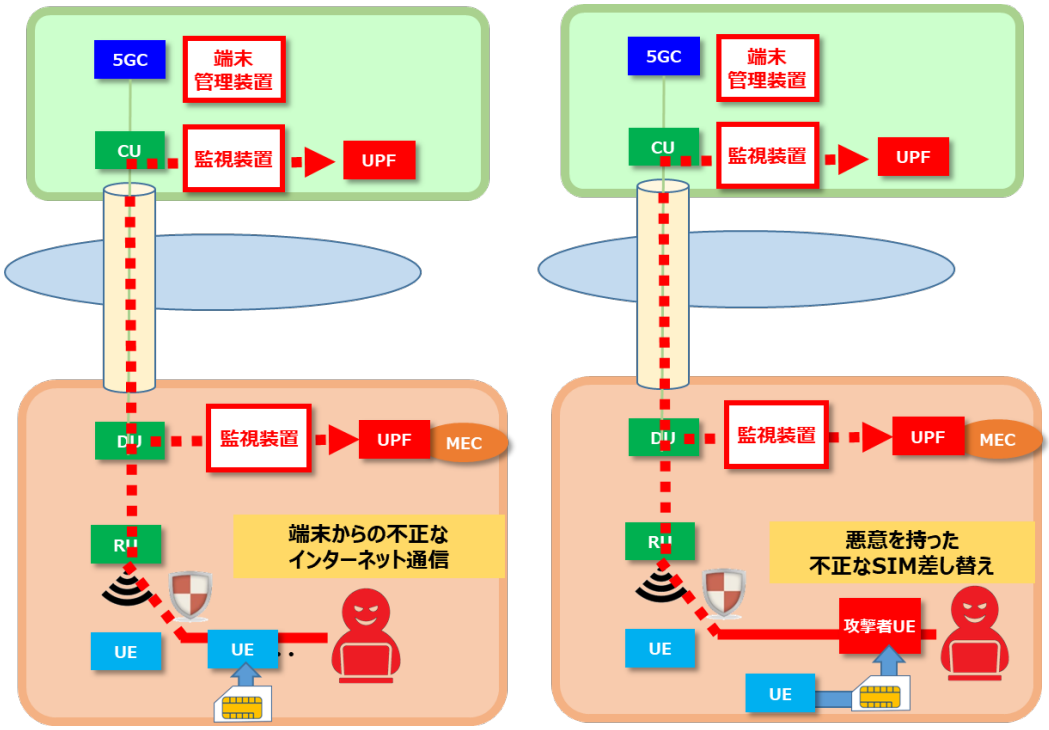


図 5-5-1-4 検証イメージ（セキュリティ機能付き SIM を用いた端末のセキュリティ）

(2) 評価・検証項目

本検証での評価・検証項目は、以下の「表 5-5-2-1 評価・検証項目」のとおりです。

表 5-5-2-1 評価・検証項目

大項目	中項目	UPF 配置	共用パターン	検証概要	対応図表
セキュリティ検証	CU-DU 区間通信の暗号化	センタ拠点 UPF	複数企業共用パターン	IPsec 通信の確立	図 5-5-1-1 図 5-5-1-2
				CU-DU 区間の遅延測定	図 5-5-1-1 図 5-5-1-2
			業界共用パターン	IPsec 通信の確立	図 5-5-1-1 図 5-5-1-2
				CU-DU 区間の遅延測定	図 5-5-1-1 図 5-5-1-2
	セキュリティ機能付き SIM を用い	センタ拠点 UPF	複数企業共用パターン	セキュリティ脅威の検知・遮断	図 5-5-1-3 図 5-5-1-4
				接続端末の可視化	図 5-5-1-3 図 5-5-1-4
			業界共用	セキュリティ脅威の検知・	図 5-5-1-3

	端末のセキュリティ		パターン	遮断	図 5-5-1-4
				接続端末の可視化	図 5-5-1-3 図 5-5-1-4
		エンド拠点 UPF	複数企業共用パターン	セキュリティ脅威の検知・遮断	図 5-5-1-3 図 5-5-1-4
				接続端末の可視化	図 5-5-1-3 図 5-5-1-4
			業界共用パターン	セキュリティ脅威の検知・遮断	図 5-5-1-3 図 5-5-1-4
				接続端末の可視化	図 5-5-1-3 図 5-5-1-4

(3) 評価・検証方法

① CU-DU 区間通信の暗号化

本検証の検証手順は、以下の「表 5-5-3-1 検証手順（複数企業共用パターン・業界共用パターン共通)」のとおりです。

表 5-5-3-1 検証手順（複数企業共用パターン・業界共用パターン共通）

項番	検証概要	評価項目	検証手順
1	IPsec 通信の確立	IPsec の成立確認	DH 方式、量子暗号鍵交換方式のそれぞれについて以下を実施 ・両拠点の鍵を用いて IPsec トンネルを構築 ・C-plane および U-plane の通信がともに正常に行えることを確認
2		暗号化の確認	DH 方式、量子暗号鍵交換方式のそれぞれについて以下を実施 ・C-plane の通信のみ暗号化を施す設定の実施 ・CU-DU 区間で暗号化されることを確認
3	CU-DU 区間の遅延測定	遅延値の確認	DH 方式、量子暗号鍵交換方式のそれぞれについて以下を実施 ・CU-DU 区間の通信遅延値を測定
4	分析・考察	分析・考察	・セキュリティリスクの洗い出し ・セキュリティ対策の評価 ・導入に関する懸念事項の検討

② セキュリティ機能付き SIM を用いた端末のセキュリティ

本検証の検証手順は、以下の「表 5-5-3-2 端末セキュリティ検証手順（複数企業共用パターン・業界共用パターン共通)」のとおりです。

なお、「表 5-5-1-1 セキュリティ検証対象箇所および検証拠点」に示すとおり、セキュリティ脅威の検知・遮断のセンタ/エンド UPF 構成および、端末状態の監視・可視化のエンド UPF 構成の検証は NTT 中央研修センタのみで行い、端末状態の監視・可視化のセンタ UPF 構成の検証は NTT 中央研修センタ、東北大学、いすゞ自動車で行います。

表 5-5-3-2 端末セキュリティ検証手順(複数企業共用パターン・業界共用パターン共通)

項番	検証概要	評価項目	検証手順
1	端末状態の監視・可視化	拠点毎の端末の真正性の確認	端末管理システムから以下情報が取得できることを確認 ・IMSI / IMEI ・Cell ID ・IP アドレス ・端末情報 ・オープンポート
2		端末情報のトレーサビリティ確認	・端末 IP アドレスを変更 ・端末管理システム上の端末情報が更新されていることを確認
3		拠点毎の端末情報整理	・端末管理システム上で Radio ID 等の情報を使って拠点単位に端末情報をソートできることを確認
4		端末情報の可視化	・端末管理システム上で可視化画面を確認し、端末の一覧表示、稼働状況に関する管理閲覧等の運営手法を考察
5	セキュリティ脅威の検知・遮断	アクセス制御	・特定の拠点に対しセキュリティポリシーを適用 ・該当拠点に属する端末に対して、アクセス制御ができることを確認
6		端末不正利用防止	・正規の端末に搭載した SIM を別の端末（疑似不正端末）へ挿入 ・疑似不正端末からの接続を遮断できることを確認
7		内部拡散防止	・正規の端末から疑似不正通信を送信 ・当該不正通信を検知・遮断し、当該端末からの接続を遮断できることを確認
8	分析・考察	分析・考察	・セキュリティリスクの洗い出し ・セキュリティ対策の評価 ・導入に関する懸念事項の検討

			・端末のセキュリティレベル

また、本検証においてはローカル５Ｇに接続する端末を「表 5-5-3-3 デバイス種別」に示す 3 種のデバイスに分類し、各分類別で必要な端末セキュリティの設定について検証を行いました。

表 5-5-3-3 デバイス種別

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

各デバイスグループに対するセキュリティポリシーは「表 5-5-3-4 デバイスグループおよびポリシー（抜粋)」のように設定を行いました。デバイス種別ごとに侵入検知(Intrusion prevention)や URL フィルタリング(URL filtering)等のポリシーを作成し、拠点毎のデバイスグループに適用しました。

表 5-5-3-4 デバイスグループおよびポリシーの設定（抜粋)

デバイスグループ名＝デバイスポリシー名	Intrusion prevention	URL filtering	Application control
NTT 中央研修センタ_Critical_Device	Critical_IPS	Critical_WTP	Critical_Application
NTT 中央研修センタ_Monitoring_Device	Monitoring_IPS	Monitoring_WTP	Monitoring_Application
NTT 中央研修センタ_Communication_Device	Communication_IPS	Communication_WTP	Communication_Application
東北大学_Critical_Device	Critical_IPS	Critical_WTP	Critical_Application
いすゞ自動車_Critical_Device	Critical_IPS	Critical_WTP	Critical_Application

(4) 測定結果

① CU-DU 区間通信の暗号化

本検証ではすべての拠点で IPsec を確立し検証を行いましたが、本項目では代表して NTT 中央研修センタで実施した結果について報告します。

(ア) IPsec 通信の確立・暗号化の確認

ア 業界共用パターン

DH 方式および量子暗号鍵交換方式のそれぞれについてセンタ拠点とエンド拠点間に IPsec トンネルを構築し、CU-DU 区間の暗号化を行いました。「図 5-5-4-1-1-1」に示すとおり、IPsec が確立(established)され、DH 方式(QKD のステータスが No)であることが確認できました。IPsec の確立は「図 5-5-4-1-1-2」のように GUI でも確認できました。

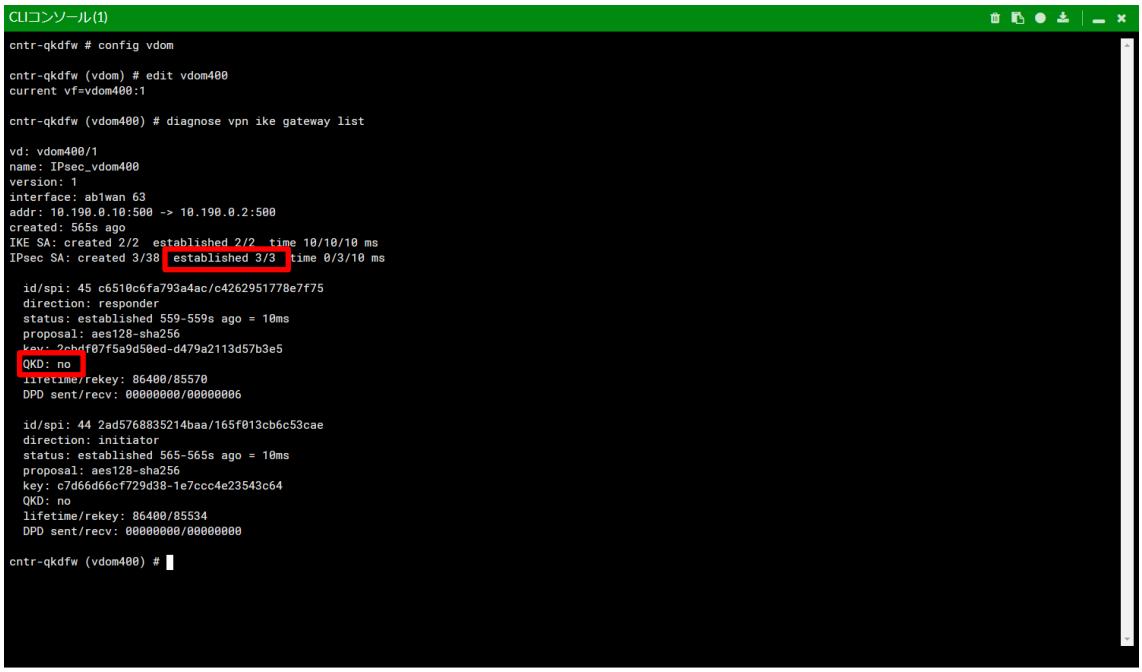


図 5-5-4-1-1-1 IPsec の確立確認 CLI(業界共用 / DH 方式)

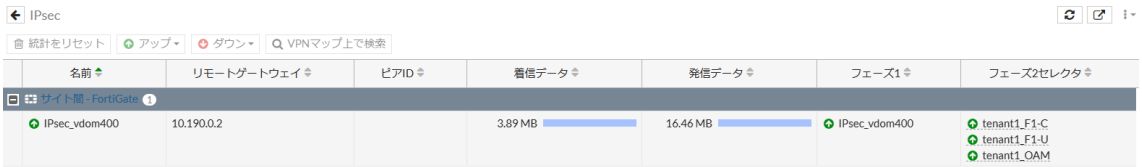


図 5-5-4-1-1-2 IPsec 確立確認 GUI(業界共用 / DH 方式)

IPsec トンネルによる暗号化の設定を「図 5-5-4-1-1-3」に示します。認証情報等を平文で送信する C-Plane の通信には暗号化の設定を行います。(図内表記 ” tenant_F1-C”)、U-Plane は PDCP によって無線区間における暗号化が施された通信のため、暗号化は行わず

IPsec の拠点間認証のみ有効とします。(図内表記 ” tenant_F1-U”)

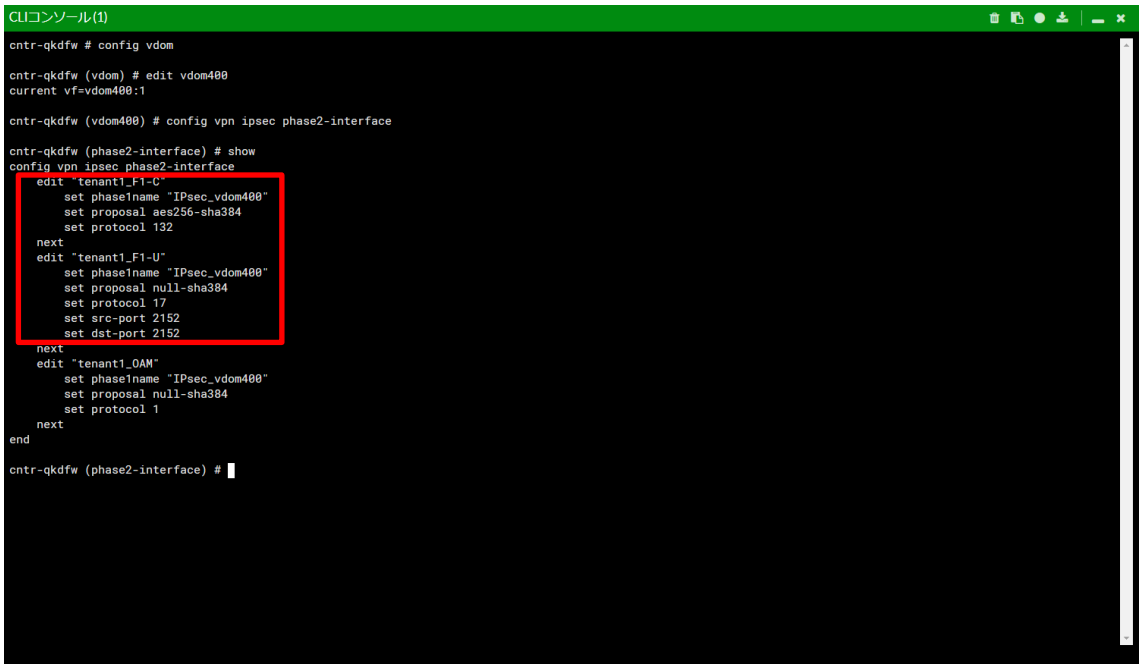


図 5-5-4-1-1-3 IPsec の設定の確認(業界共用 / DH 方式)

同様の設定を量子暗号鍵方式で実施した結果を「図 5-5-4-1-2-1～図 5-5-4-1-2-3」に示します。「図 5-5-4-1-2-1」で IPsec が確立(established)され、QKD のステータスが yes であることが確認できました。

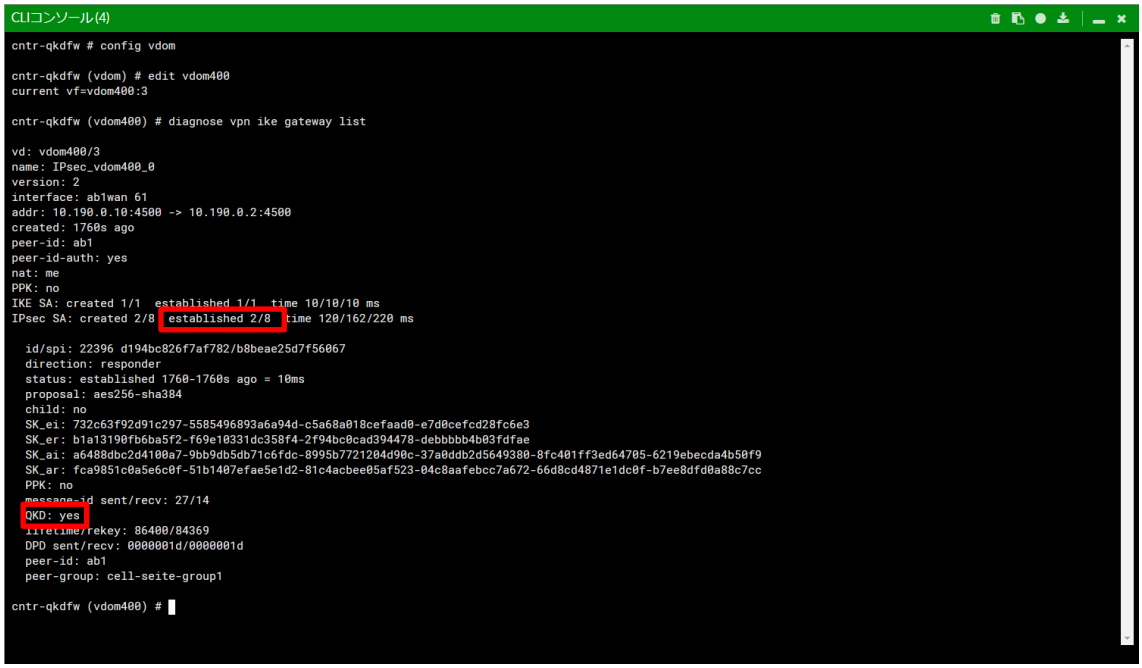


図 5-5-4-1-2-1 IPsec の確立確認 CLI(業界共用 / 量子暗号鍵方式)

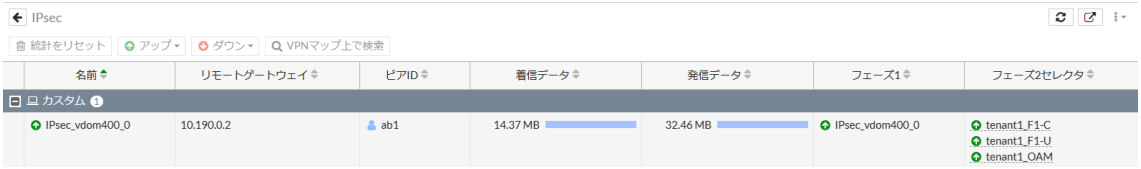


図 5-5-4-1-2-2 IPsec 確立確認 GUI(業界共用 / 量子暗号鍵方式)

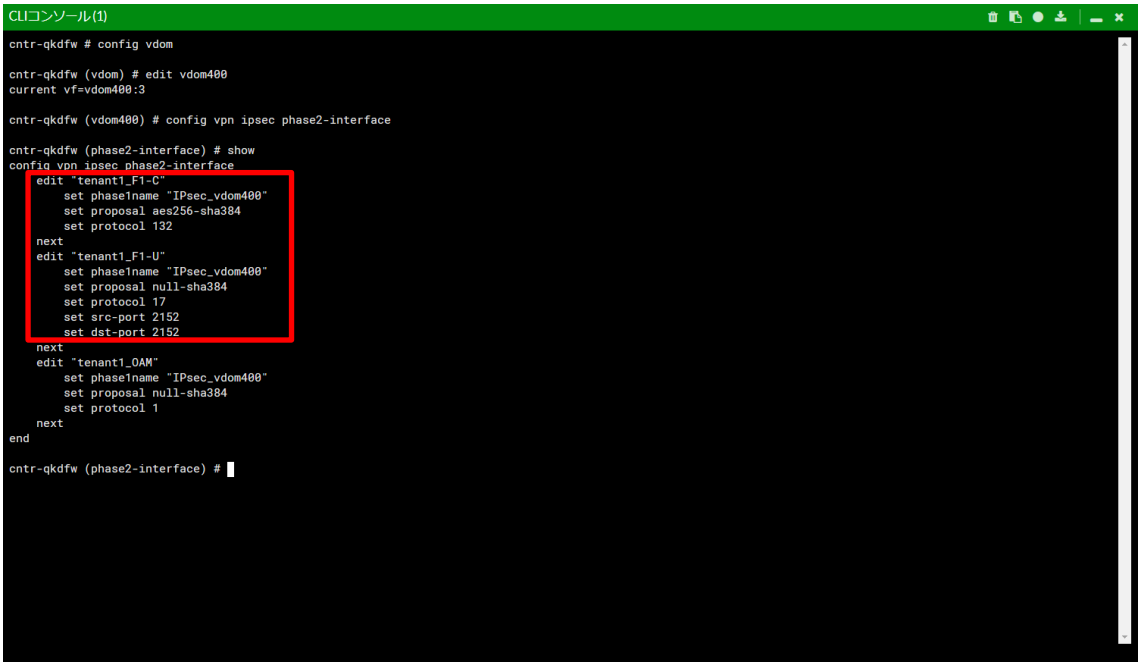


図 5-5-4-1-2-3 IPsec の設定の確認(業界共用 / 量子暗号鍵方式)

イ　複数企業共用パターン

ア 業界共用パターンと同様に NTT 中央研修センタにて複数企業共用パターン回線を用いて実施した結果を「図 5-5-4-1-3-1～図 5-5-4-1-3-3」および「図 5-5-4-1-4-1～図 5-5-4-1-4-3」に示します。

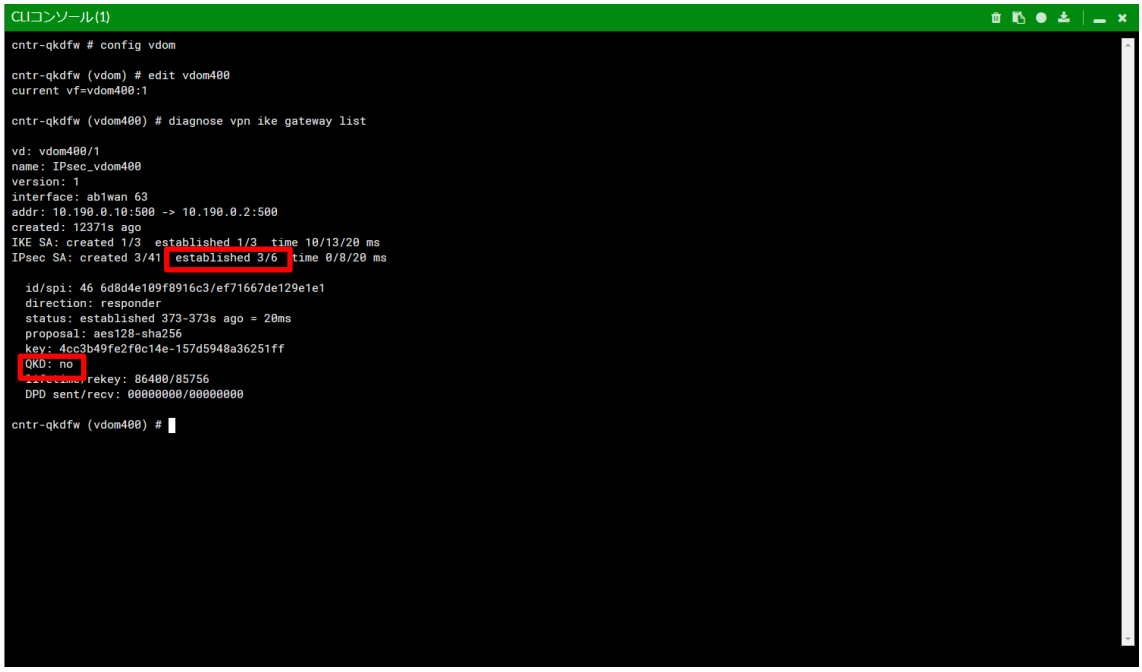


図 5-5-4-1-3-1 IPsec の確立確認 CLI(複数企業共用 / DH 方式)



図 5-5-4-1-3-2 IPsec 確立確認 GUI(複数企業共用 / DH 方式)

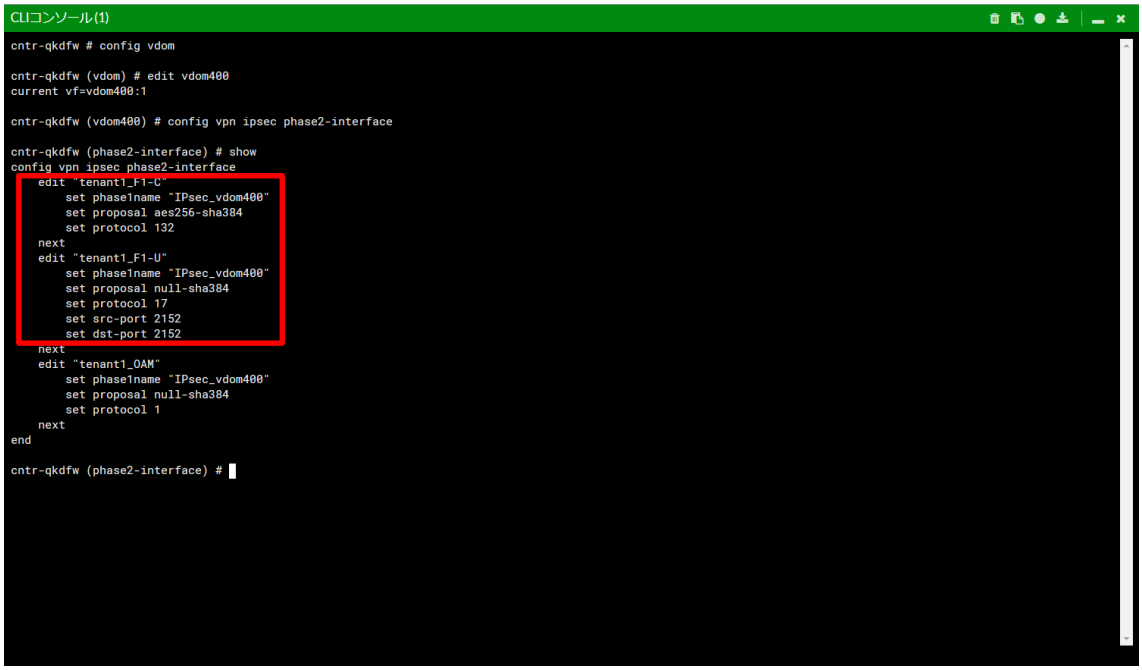


図 5-5-4-1-3-3 IPsec の設定の確認(複数企業共用 / DH 方式)

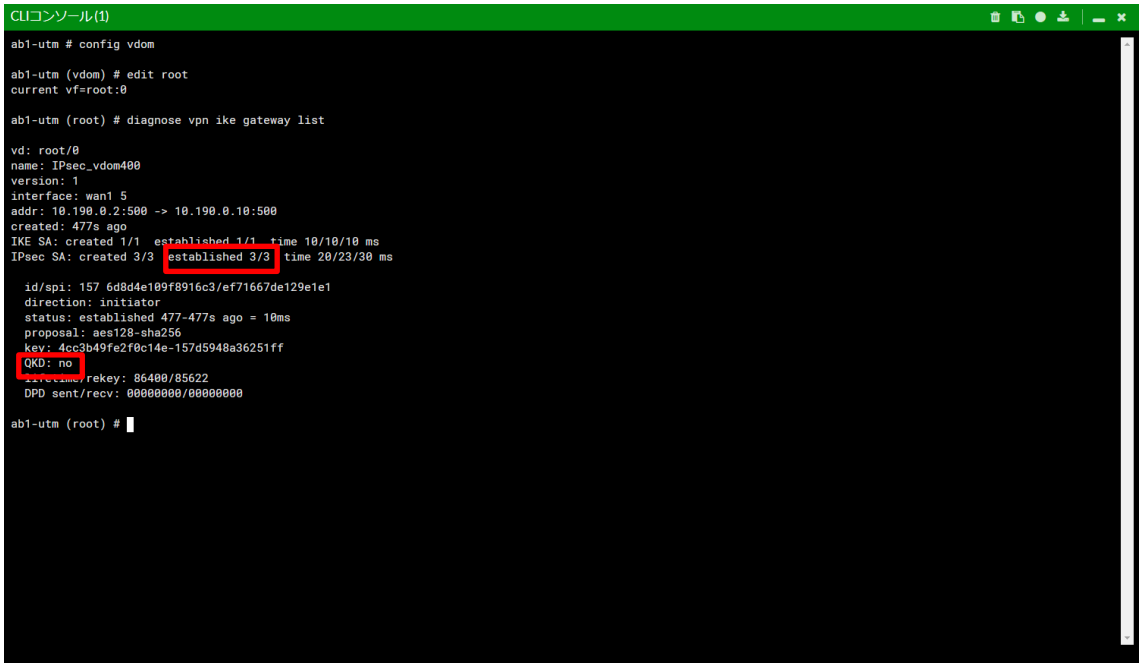


図 5-5-4-1-4-1 IPsec の確立確認 CLI(複数企業共用 / 量子暗号鍵方式)



図 5-5-4-1-4-2 IPsec 確立確認 GUI(複数企業共用 / 量子暗号鍵方式)

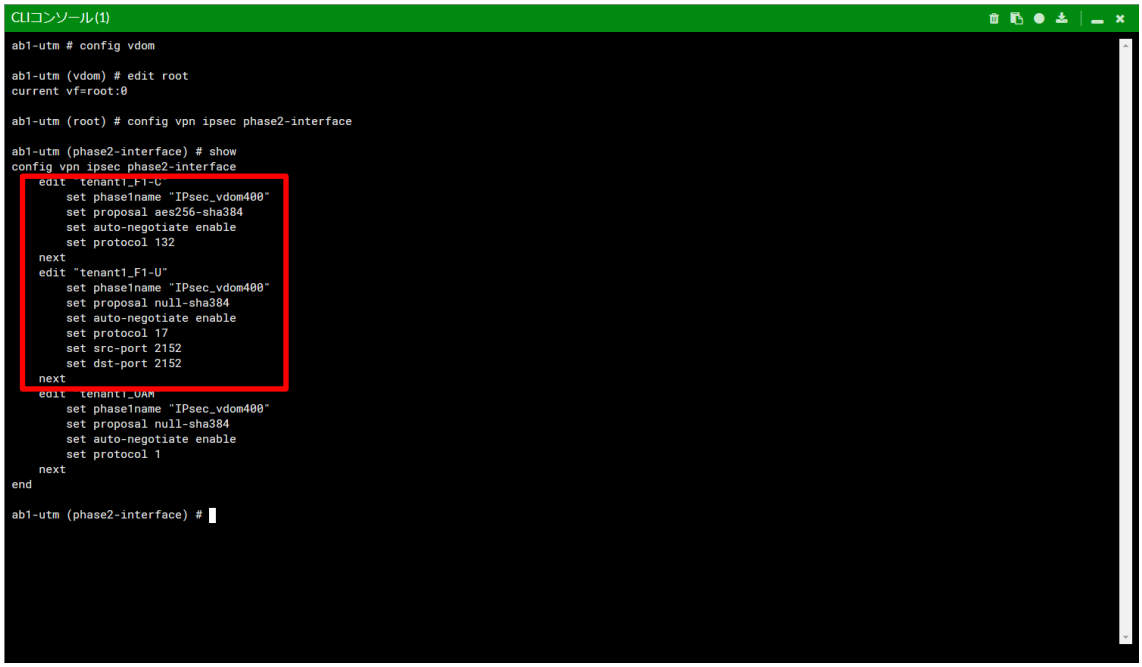


図 5-5-4-1-4-3 IPsec の設定の確認(複数企業共用 / 量子暗号鍵方式)

（イ）暗号化の確認

ア　業界共用パターン

DH 方式および量子暗号鍵交換方式のそれぞれについて構築した IPsec が適切に動作することを確認しました。具体的には、IPsec トンネルに入る前後のパケットの違いについてパケットキャプチャを実施し比較しました。

DH 方式について、「図 5-5-4-2-1-1」「図 5-5-4-2-1-2」に IPsec に入る前の C-Plane および U-Plane のパケットキャプチャの結果を示します。C-Plane は SCTP、U-Plane は GTP というそれぞれの通信で使用されるプロトコル名が見えていることが確認できます。

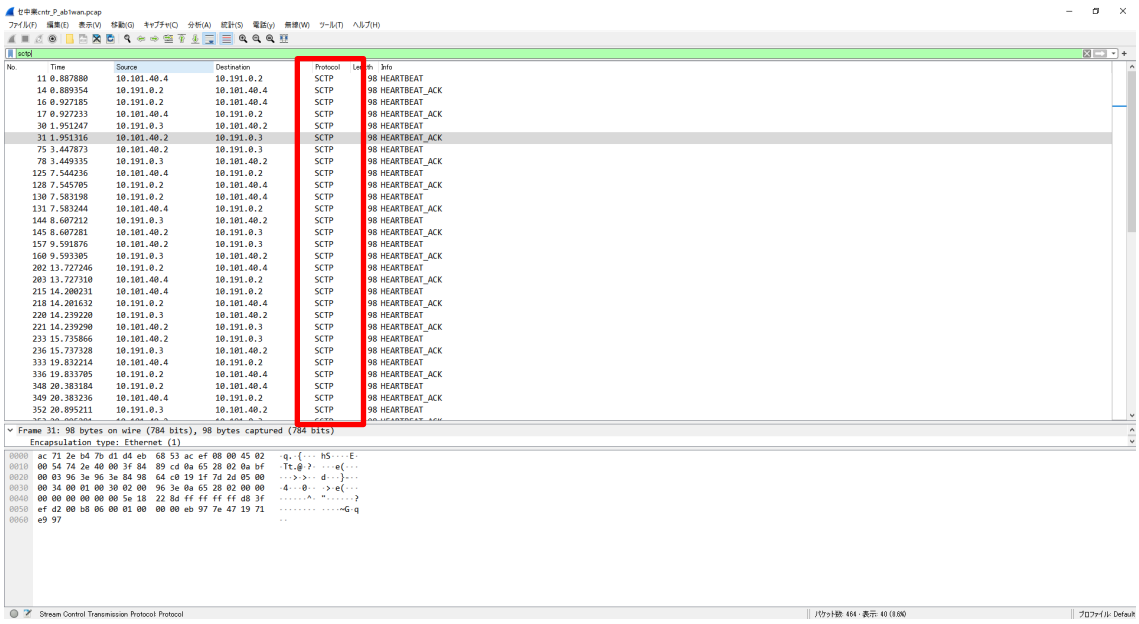


図 5-5-4-2-1-1 IPsec トンネルに入る前の C-Plane パケット（業界共用 / DH 方式）

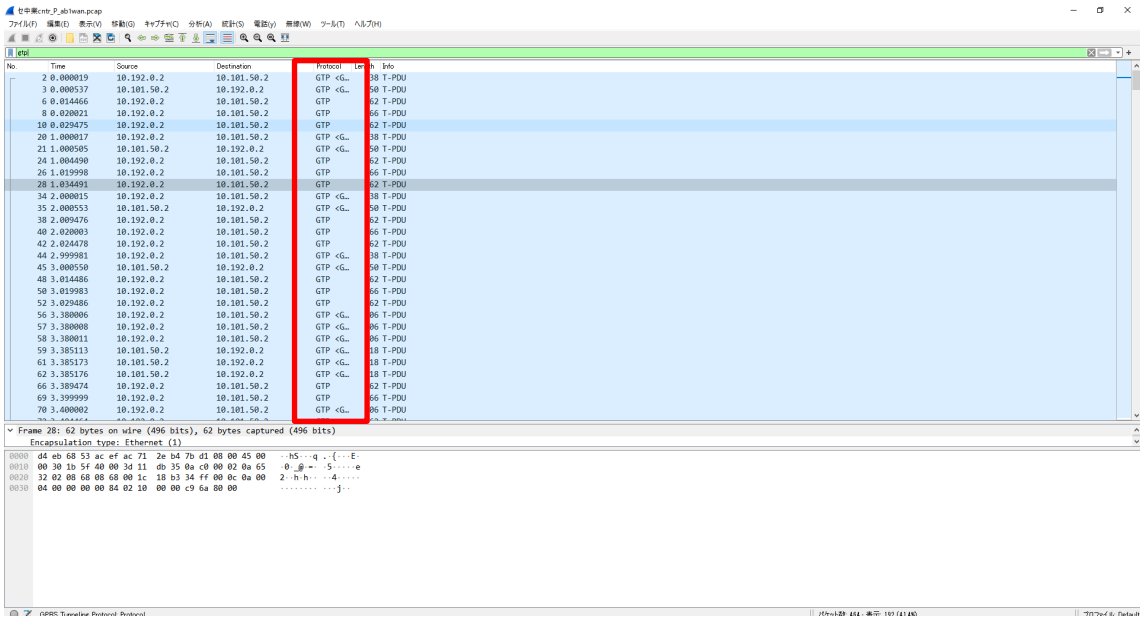


図 5-5-4-2-1-2 IPsec トンネルに入る前の U-Plane パケット（業界共用 / DH 方式）

「図 5-5-4-2-1-3」に IPsec トンネル区間のパケットキャプチャの結果を示します。IPsec パケットを示す ESP という見え方になっていることが確認できます。また、「図 5-5-4-2-1-4」「図 5-5-4-2-1-5」に IPsec による処理が行われたあとの C-Plane ／ U-Plane パケットの詳細を記載します。下部のパケットを 16 進数で表現した箇所を確認すると、C-Plane は暗号化されているため読み取れるビット列はありません。U-Plane については暗号化されていないため、送信元 IP アドレス、送信先 IP アドレス、ポート番号等が読み取れます。具体的には赤線箇所で以下の情報が読み取れます。

・11（17 ： UDP）プロトコル番号
・0a c0 00 02（10.192.0.2）送信元 IP アドレス
・0a 65 32 02（10.101.50.2）送信先 IP アドレス
・08 68（2152 ： GTP）送信元/先 ポート番号

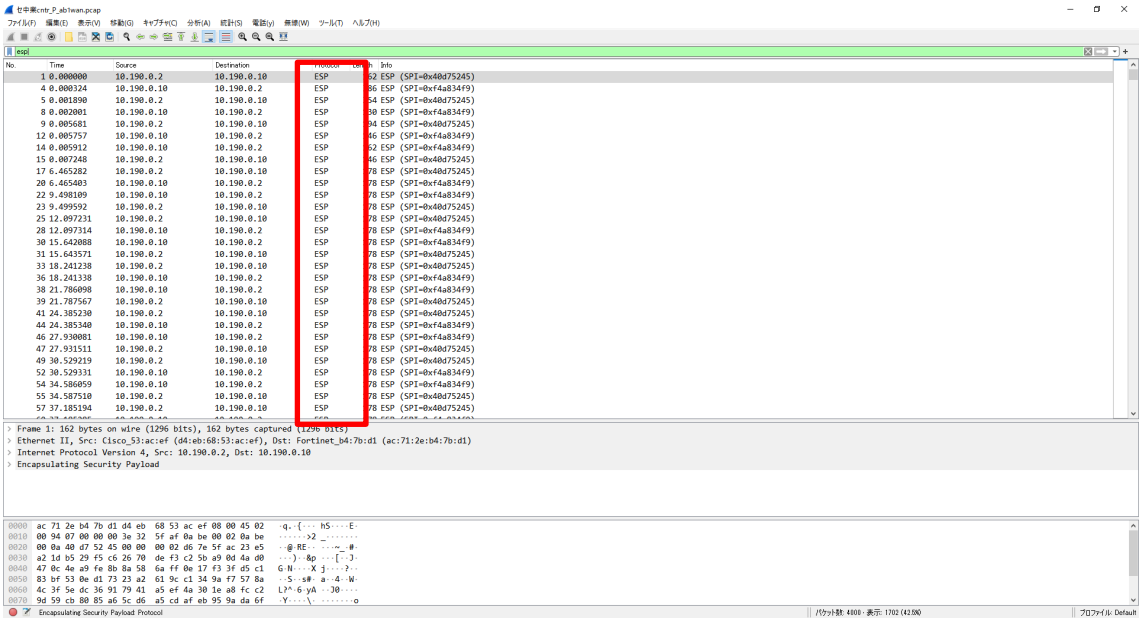


図 5-5-4-2-1-3 IPsec パケットのキャプチャ(業界共用 ／ DH 方式)

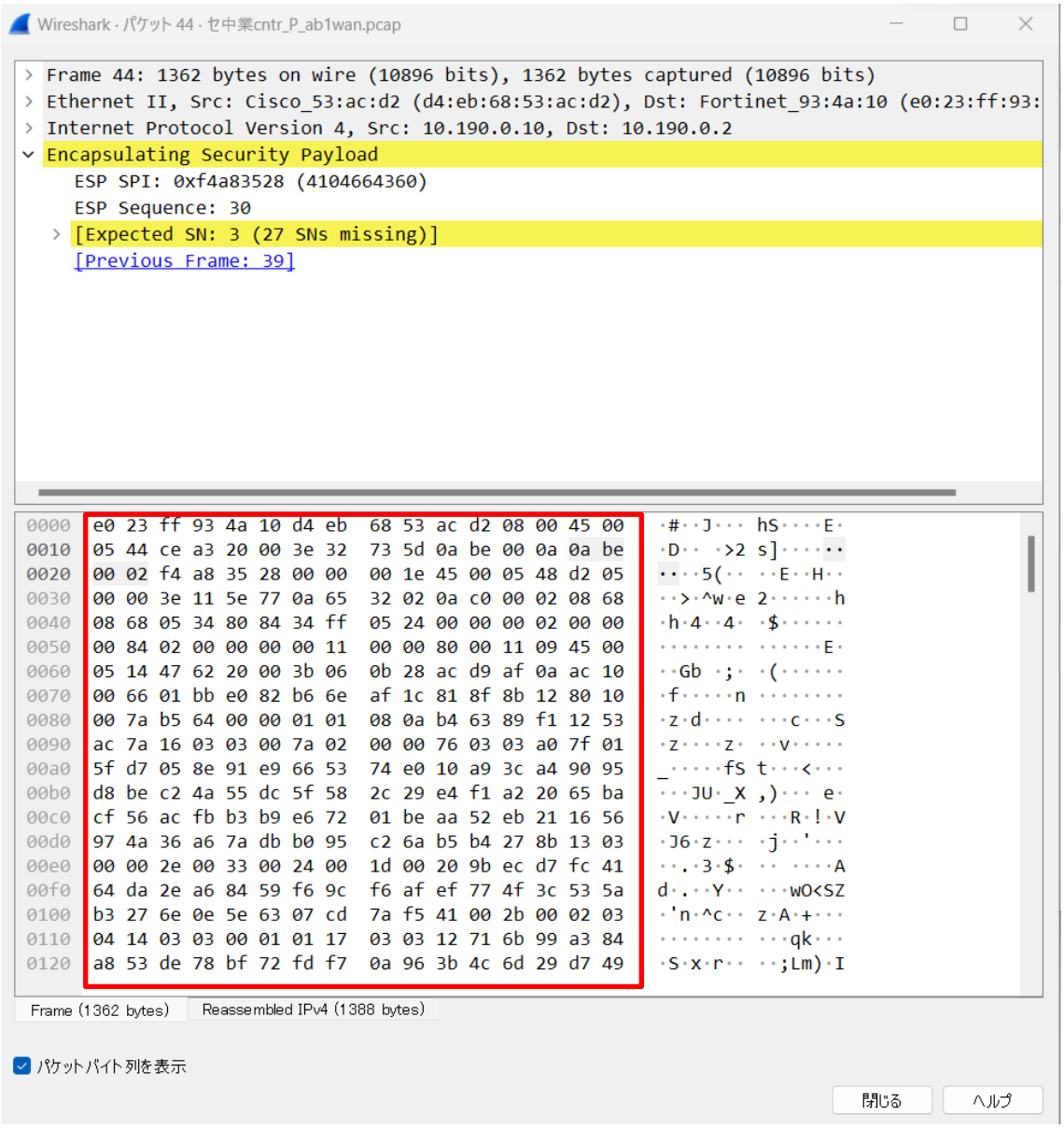


図 5-5-4-2-1-4 IPsec 内で暗号化された C-Plane パケットの詳細(業界共用 / DH 方式)

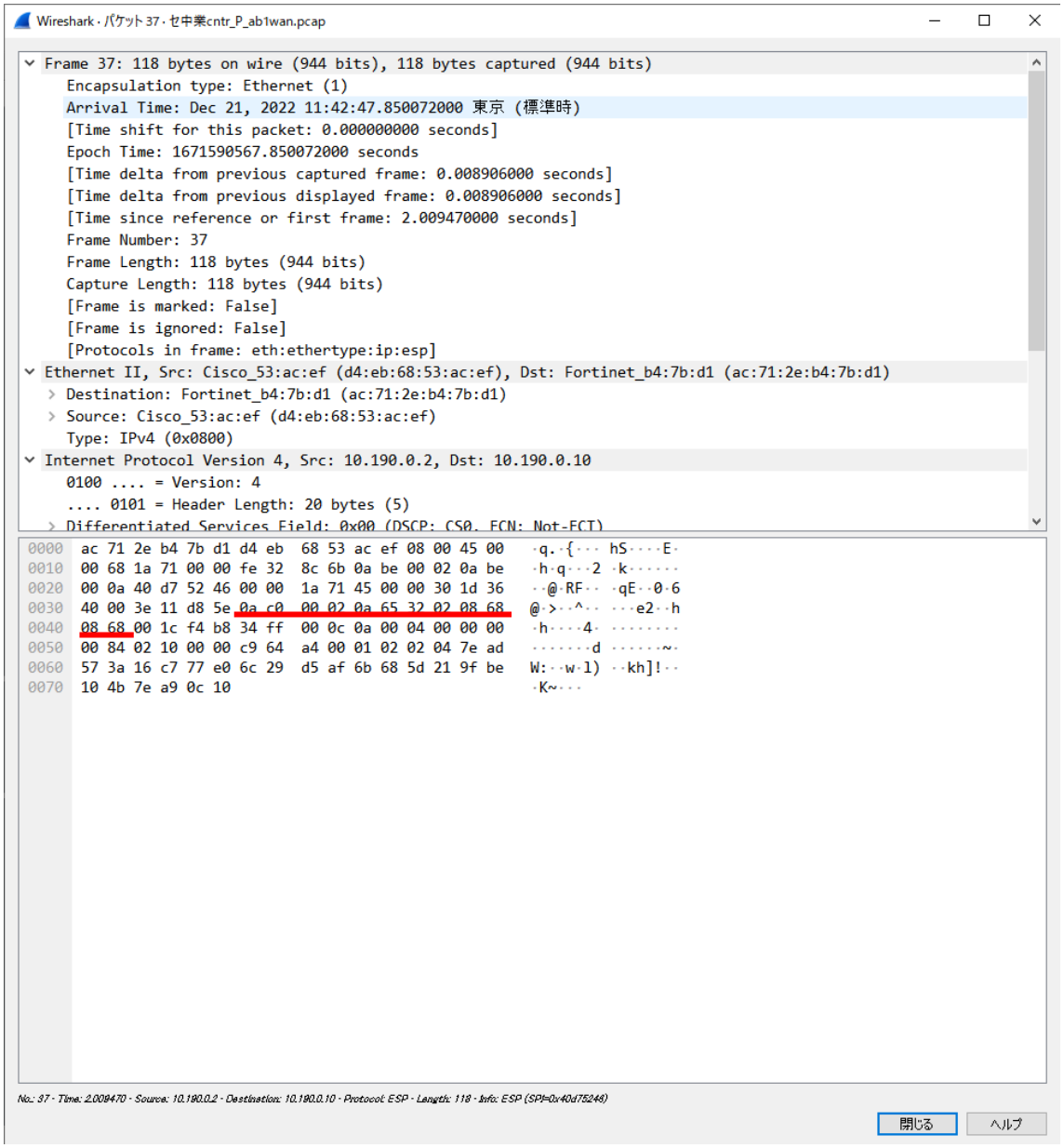


図 5-5-4-2-1-5 IPsec 内で暗号化されていない U-Plane パケットの詳細
（業界共用 / DH 方式）

続いて量子暗号鍵方式について同様の検証を行った結果を「図 5-5-4-2-2-1～図 5-5-4-2-2-5」に示します。

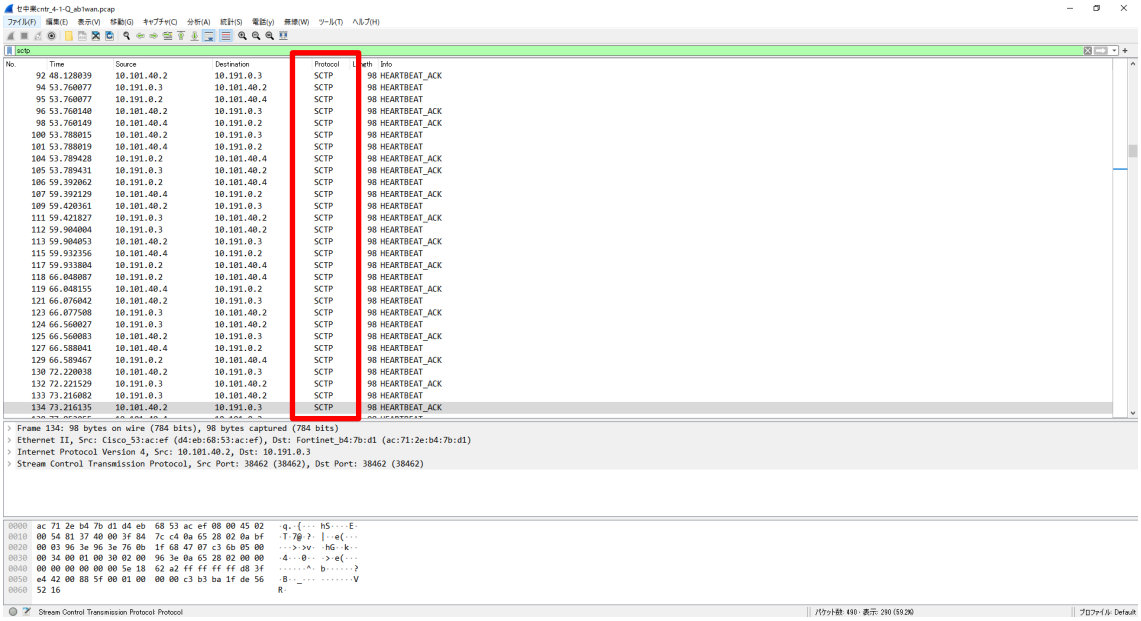


図 5-5-4-2-2-1 IPsec トンネルに入る前の C-Plane パケット(業界共用/量子暗号鍵方式)

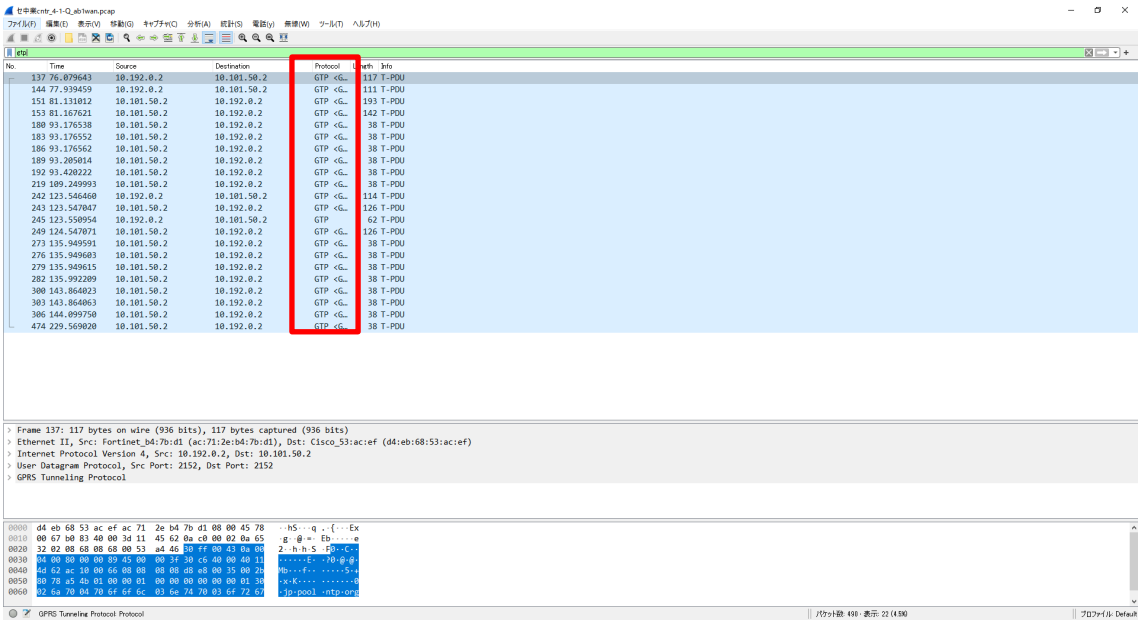


図 5-5-4-2-2-2 IPsec トンネルに入る前の U-Plane パケット(業界共用/量子暗号鍵方式)

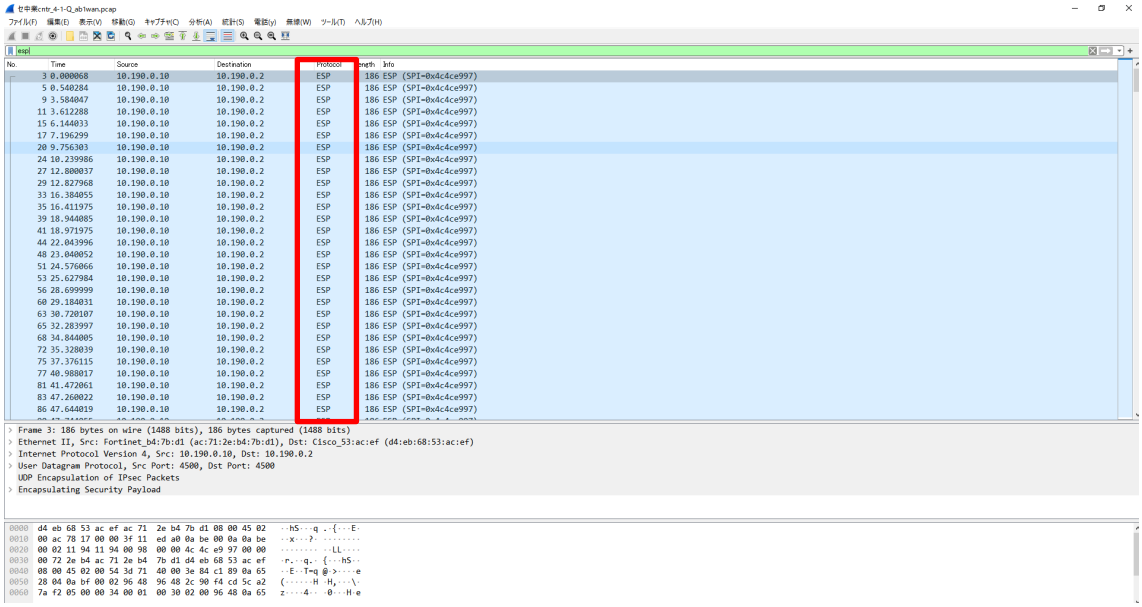


図 5-5-4-2-2-3 IPsec パケットのキャプチャ(業界共用 / 量子暗号鍵方式)

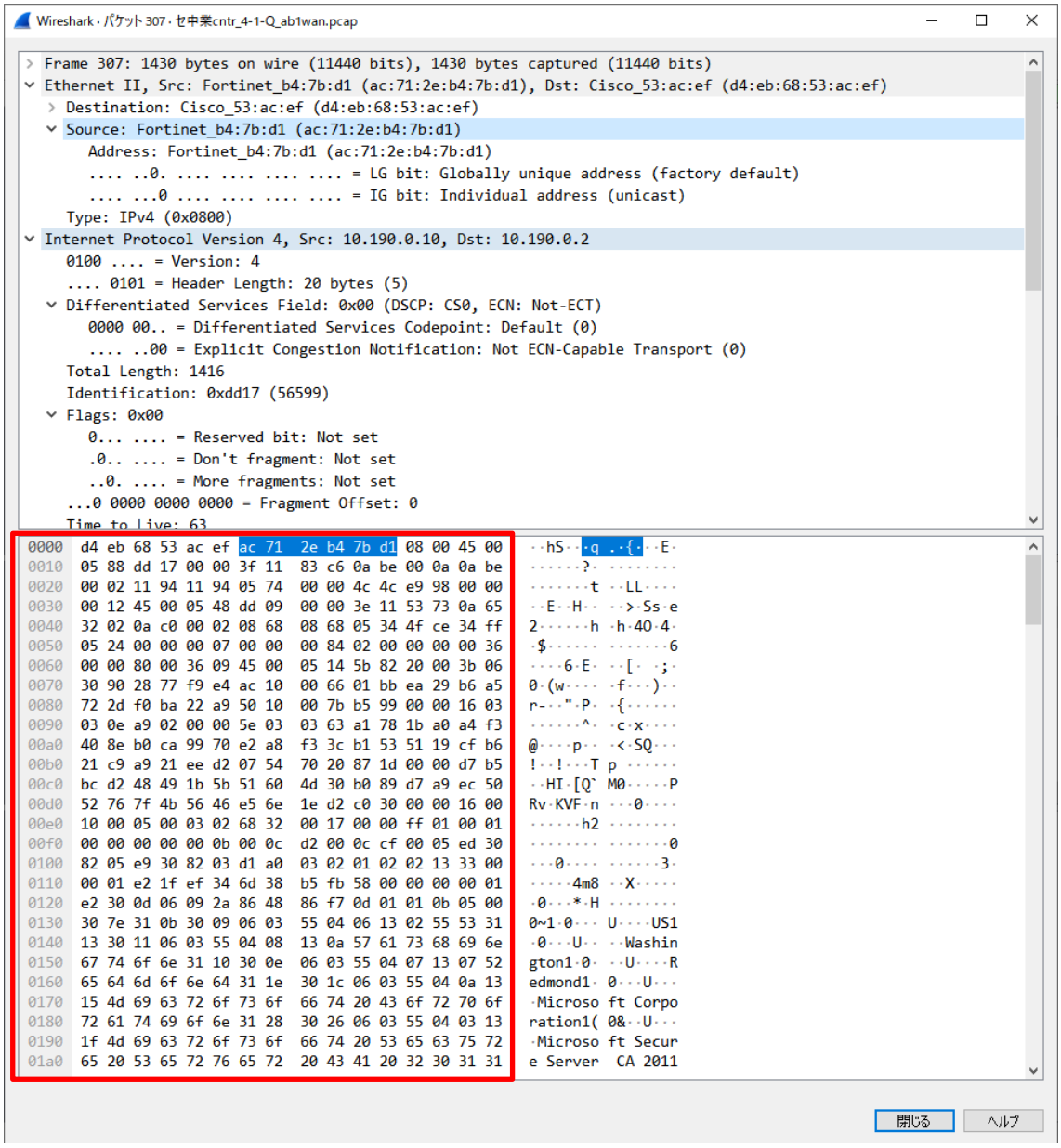


図 5-5-4-2-2-4 IPsec 内で暗号化された C-Plane パケットの詳細
(業界共用/量子暗号鍵方式)

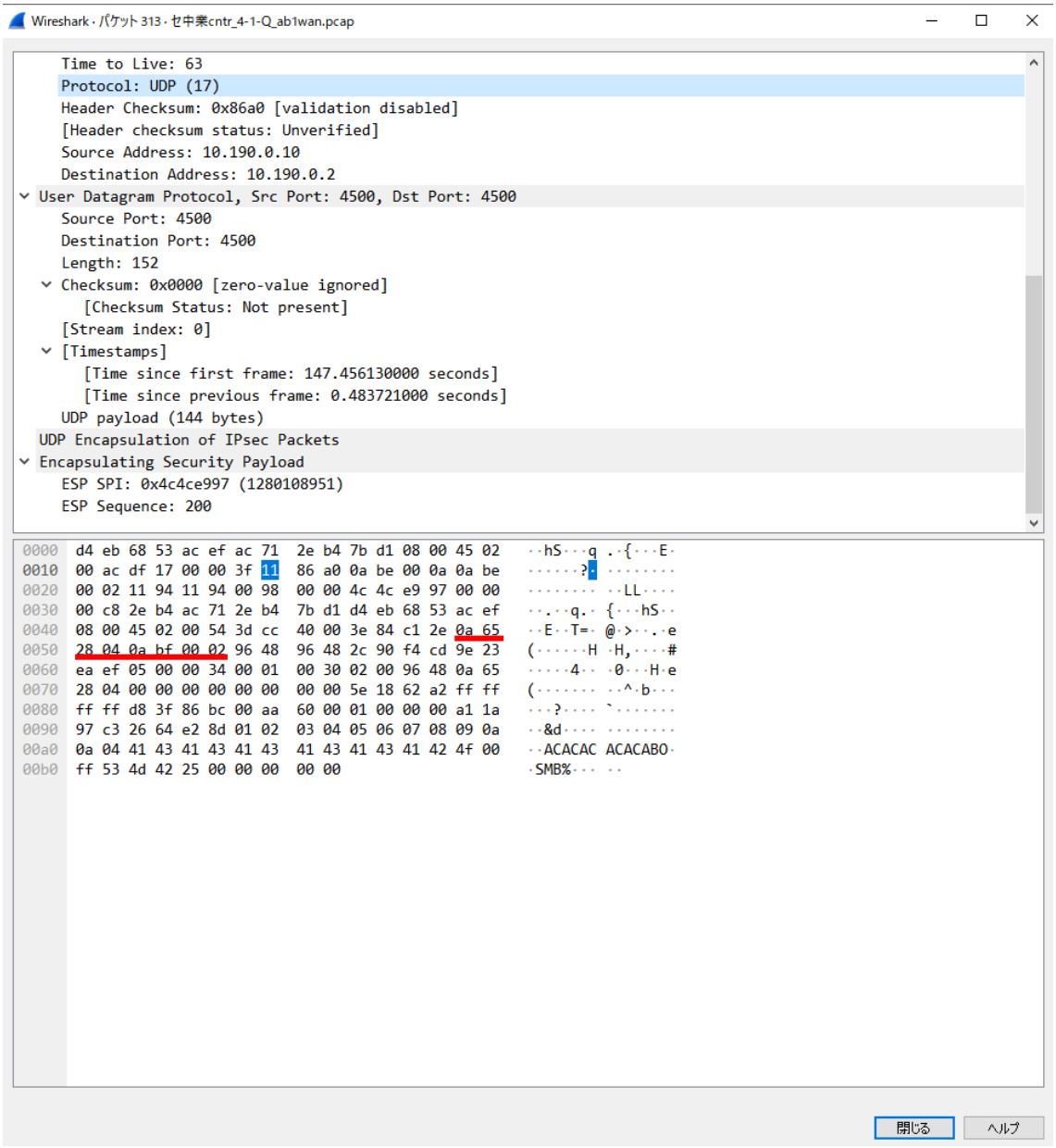


図 5-5-4-2-2-5 IPsec 内で暗号化されていない U-Plane パケットの詳細
（業界共用/量子暗号鍵方式）

イ　複数企業共用パターン

ア 業界共用パターンと同様に NTT 中央研修センタにて複数企業共用パターン回線を用いて実施した結果を「図 5-5-4-2-3-1～図 5-5-4-2-3-5」および「図 5-5-4-2-4-1～図 5-5-4-2-4-5」に示します。

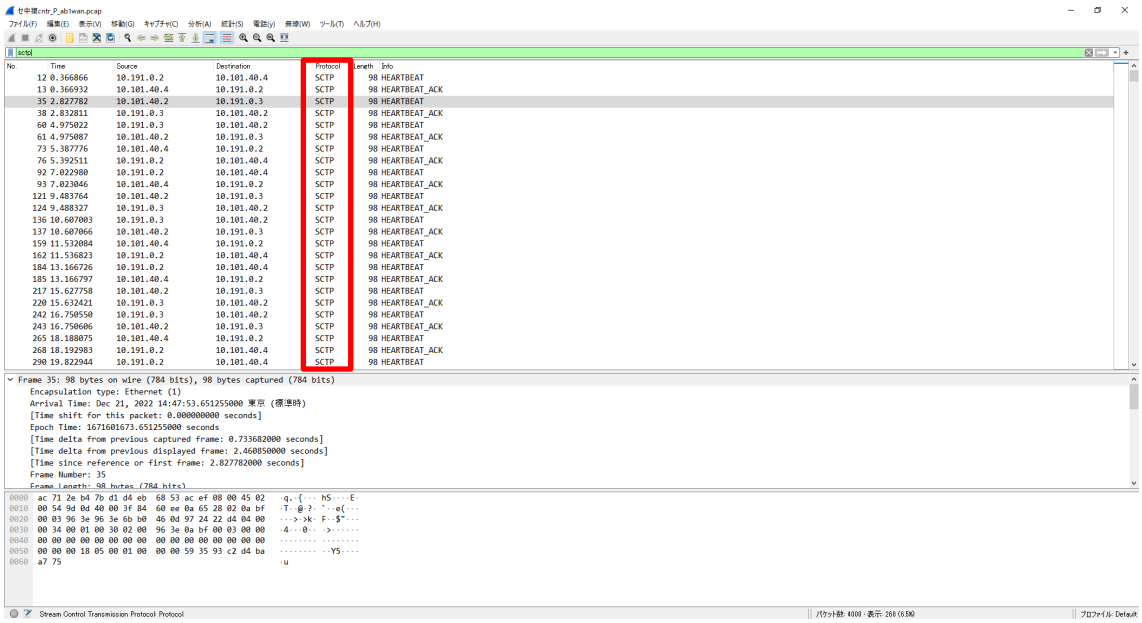


図 5-5-4-2-3-1 IPsec トンネルに入る前の C-Plane パケット(複数企業共用 / DH 方式)

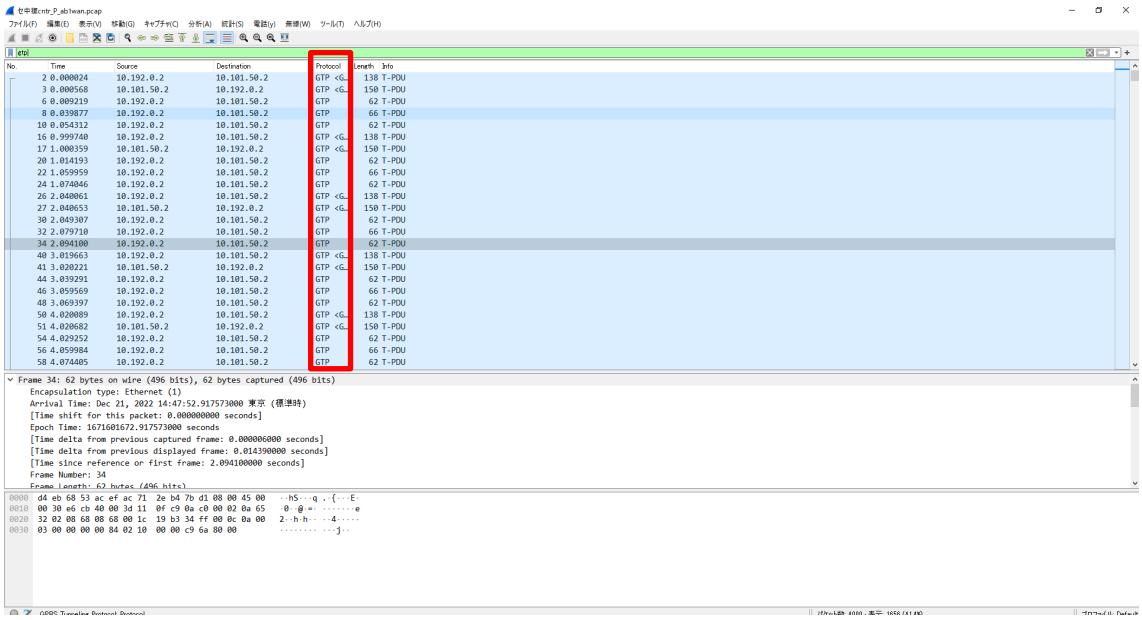


図 5-5-4-2-3-2 IPsec トンネルに入る前の U-Plane パケット(複数企業共用 / DH 方式)

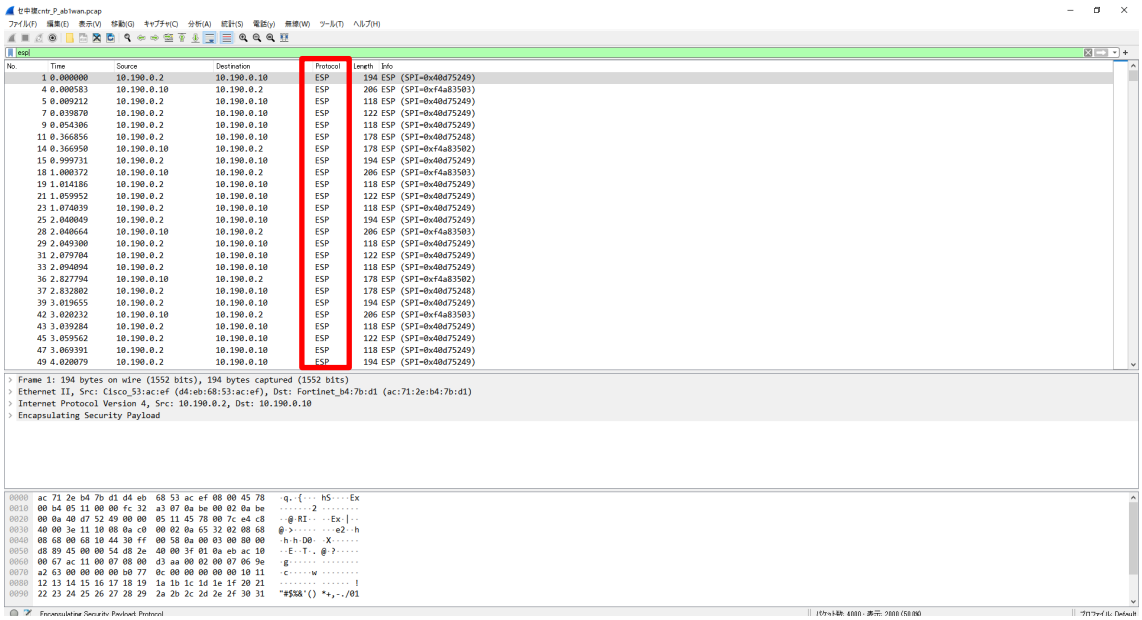


図 5-5-4-2-3-3 IPsec パケットのキャプチャ(複数企業共用 / DH 方式)

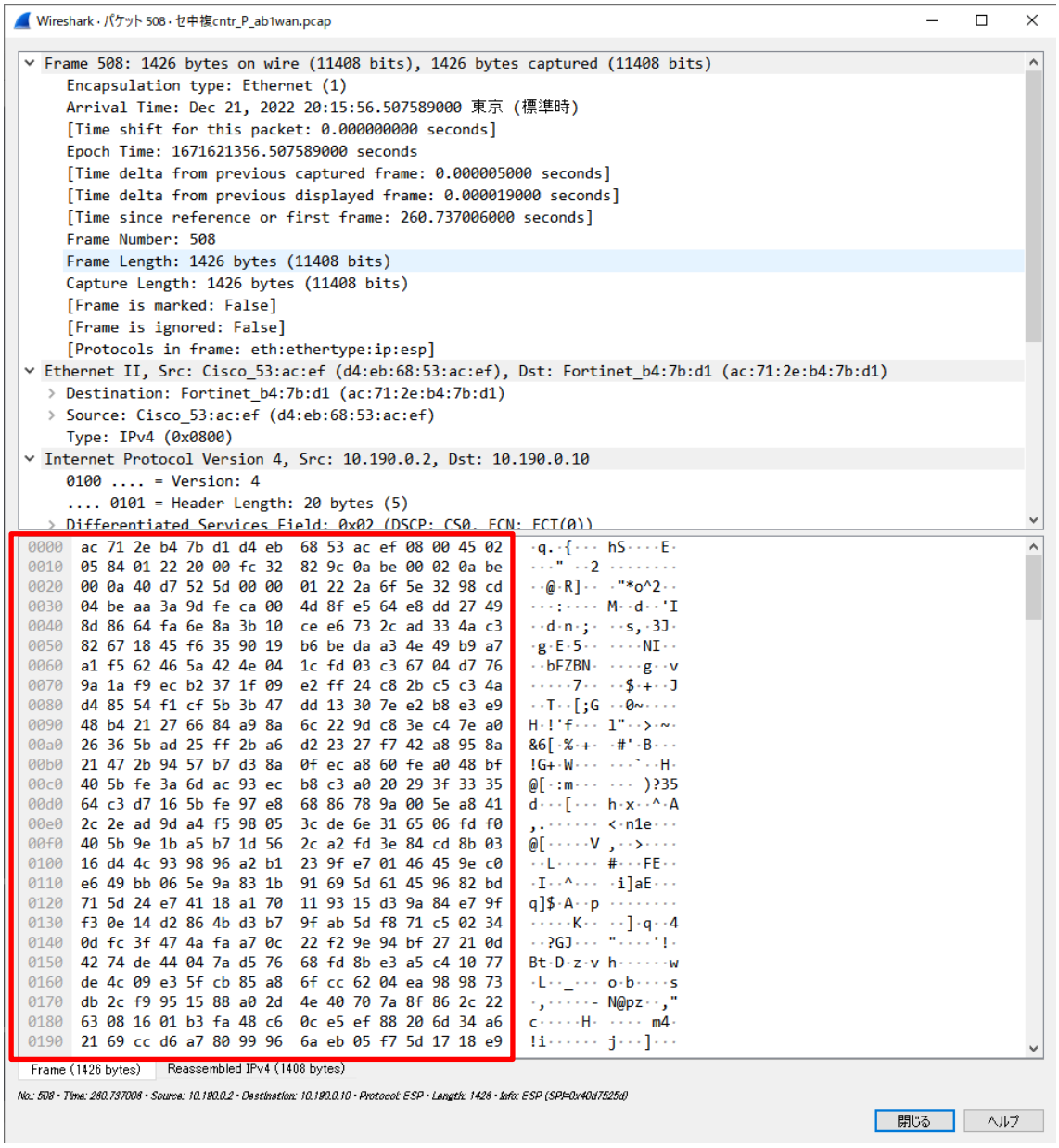


図 5-5-4-2-3-4 IPsec 内で暗号化された C-Plane パケットの詳細(複数企業共用/DH 方式)

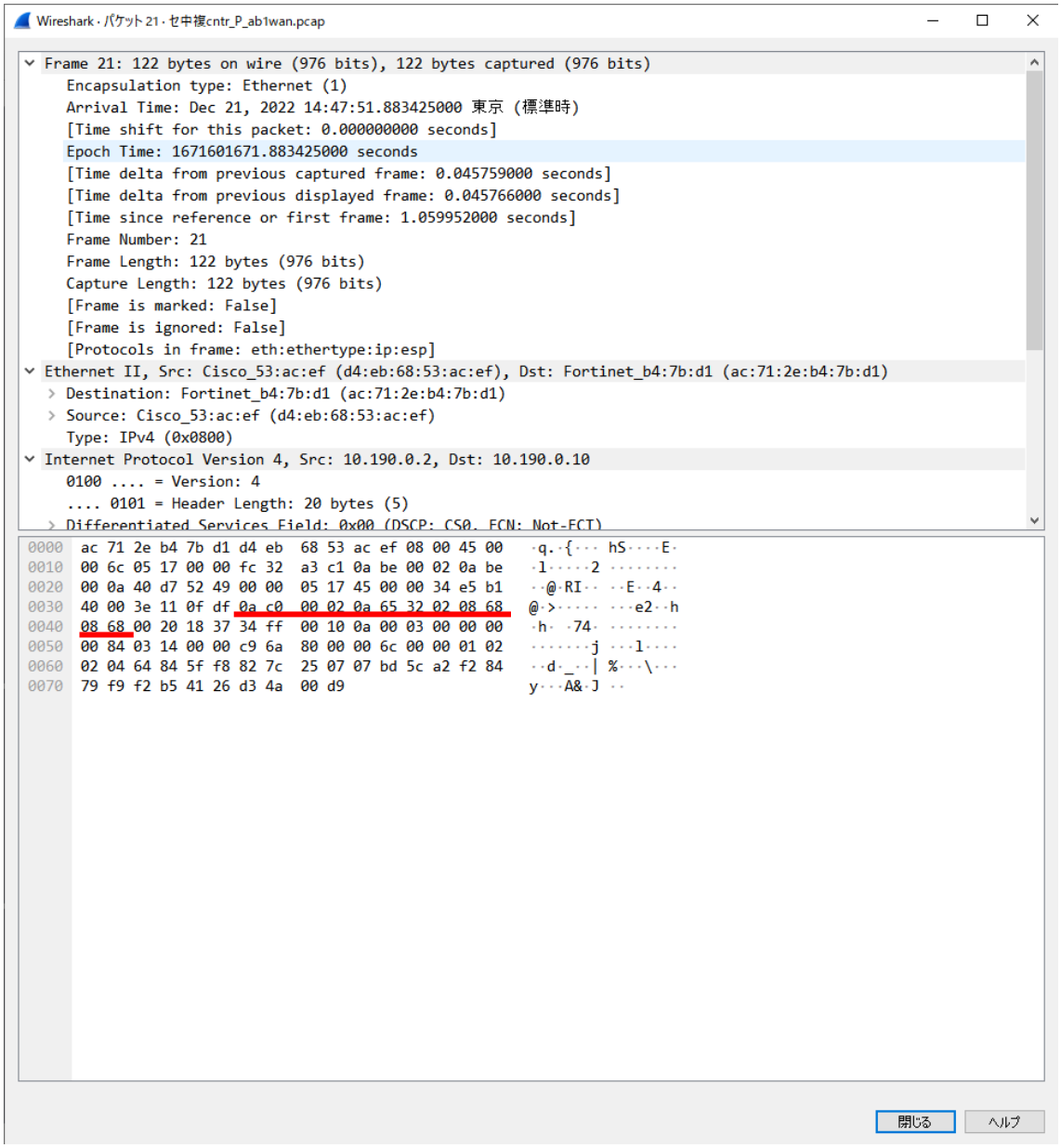


図 5-5-4-2-3-5 IPsec 内で暗号化されていない U-Plane パケットの詳細
（複数企業共用/DH 方式）

続いて量子暗号鍵方式について同様の検証を行った結果を「図 5-5-4-2-4-1～図 5-5-4-2-4-5」に示します。

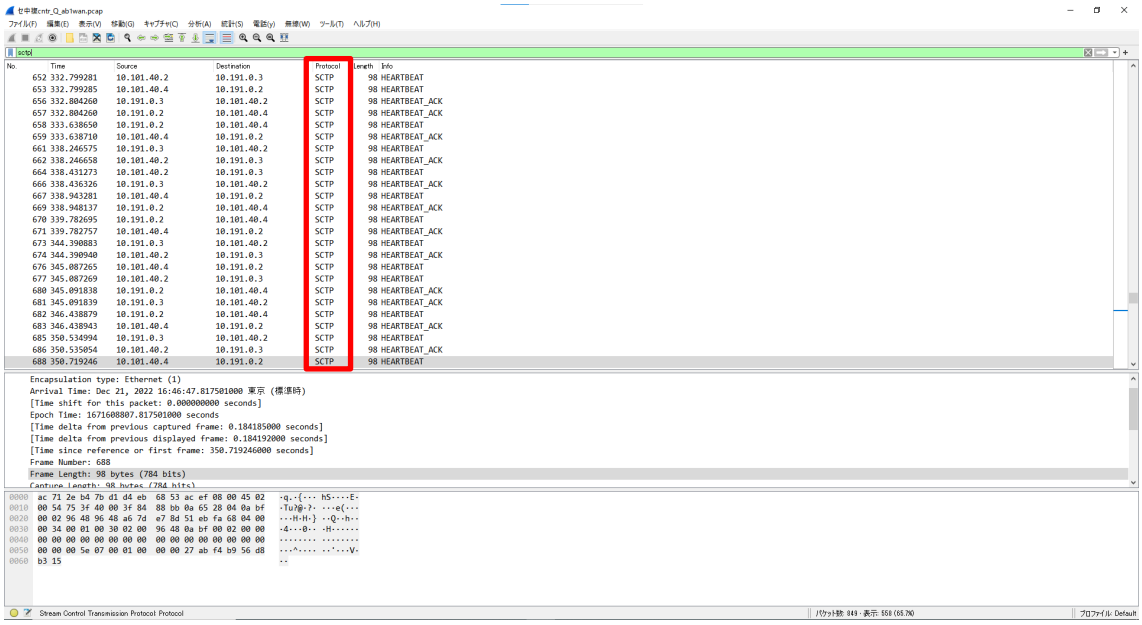


図 5-5-4-2-4-1 IPsec トンネルに入る前の C-Plane パケット
(複数企業共用/量子暗号鍵方式)

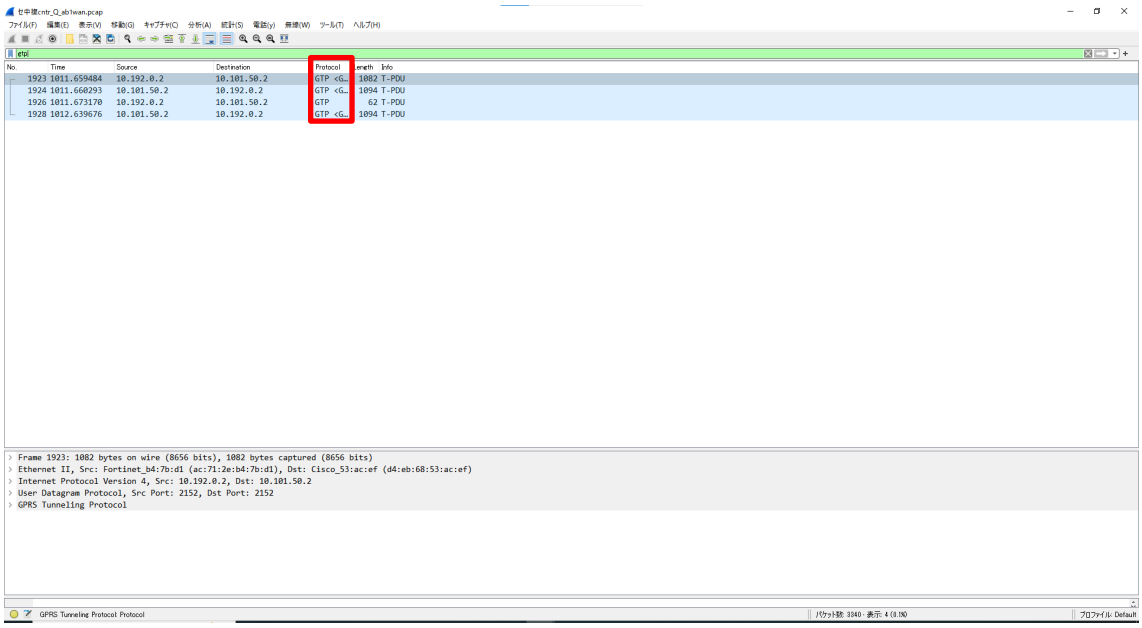


図 5-5-4-2-4-2 IPsec トンネルに入る前の U-Plane パケット
(複数企業共用/量子暗号鍵方式)

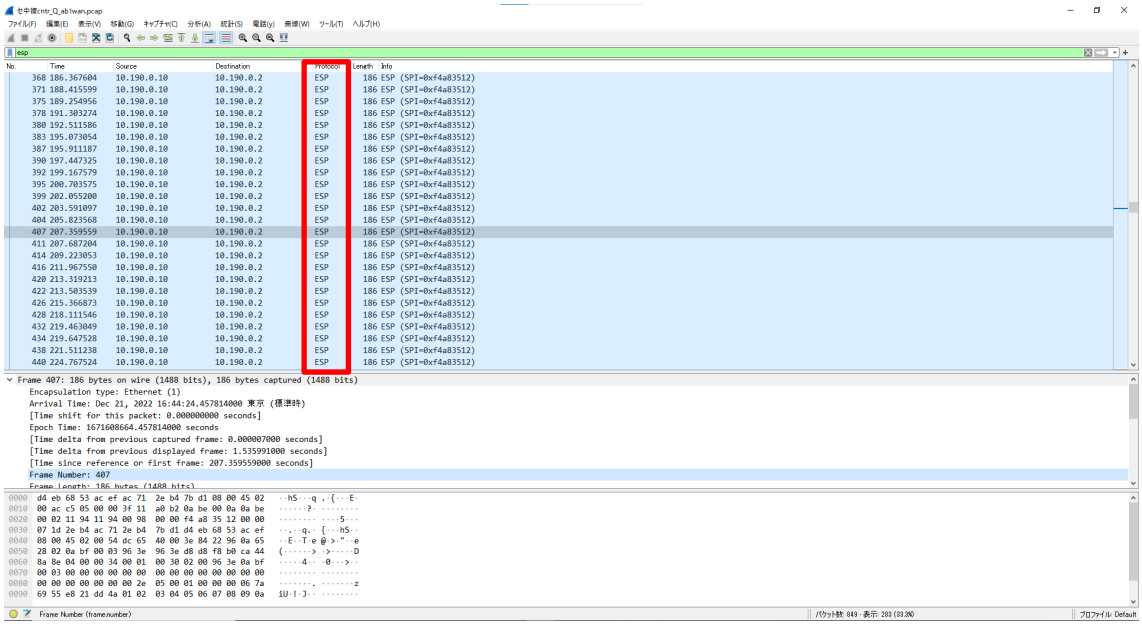


図 5-5-4-2-4-3 IPsec パケットのキャプチャ(複数企業共用/量子暗号鍵方式)

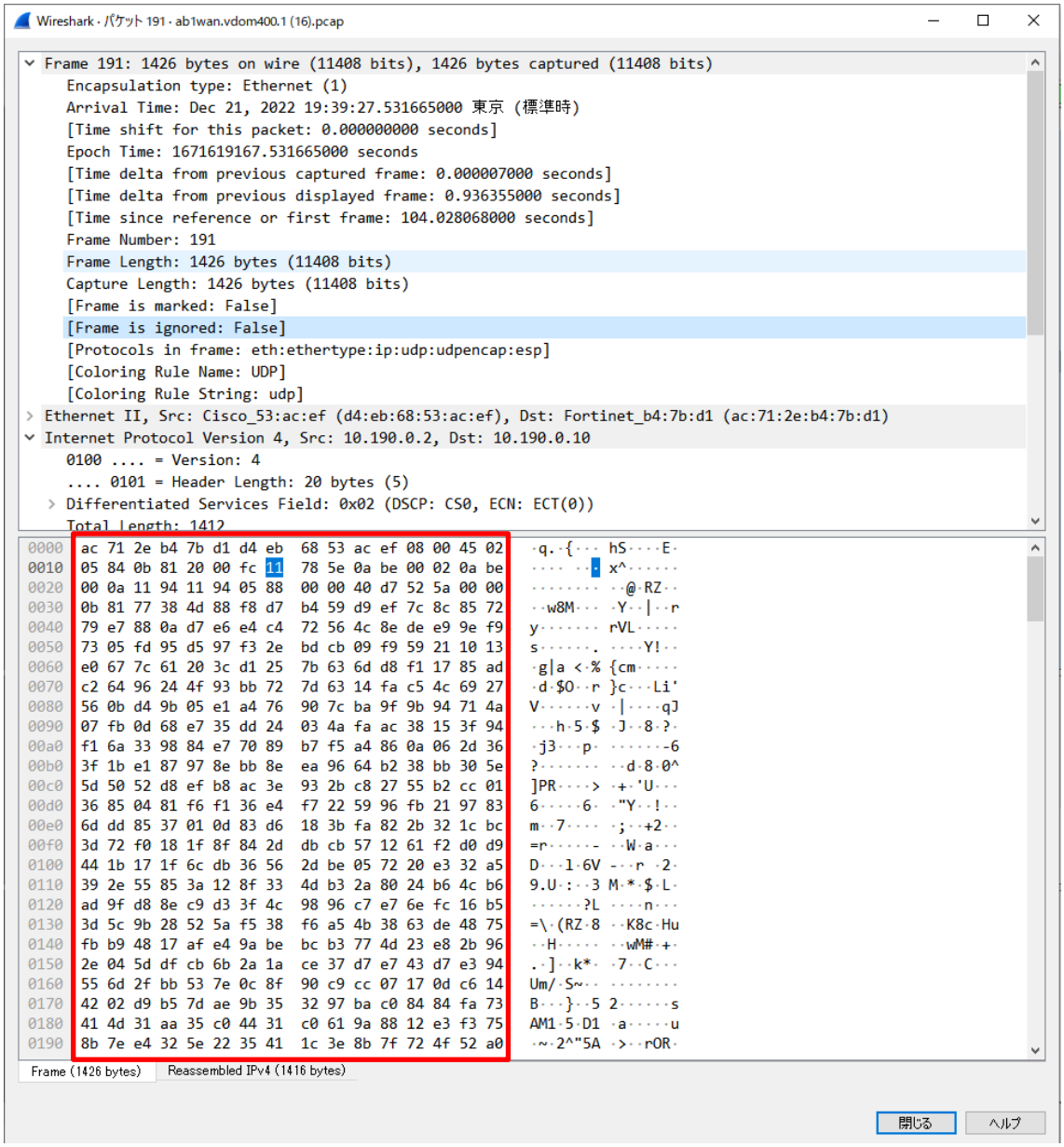


図 5-5-4-2-4-4 IPsec 内で暗号化された C-Plane パケットの詳細
（複数企業共用/量子暗号鍵方式）

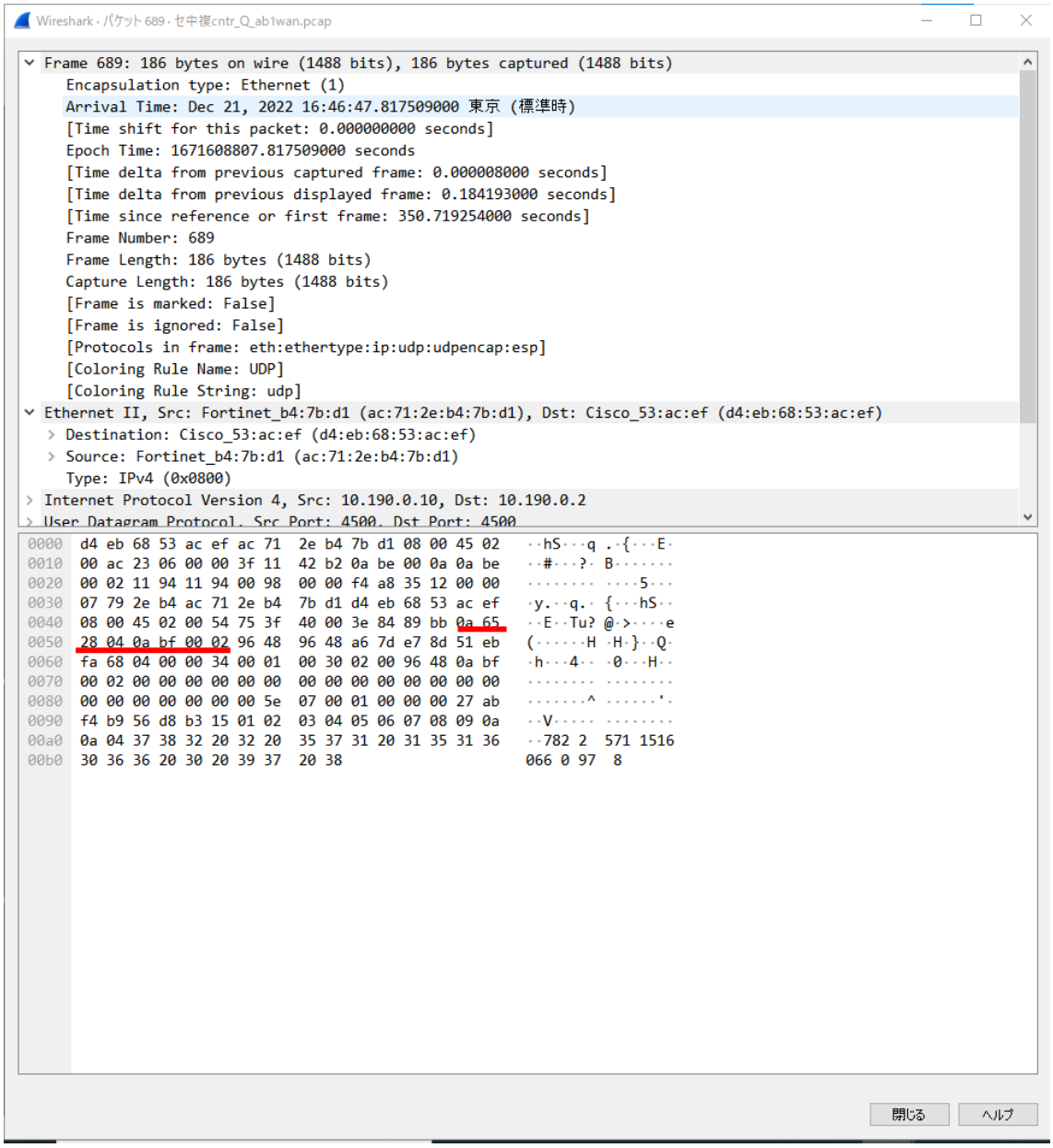


図 5-5-4-2-4-5 IPsec 内で暗号化されていない U-Plane パケットの詳細
（複数企業共用/量子暗号鍵方式）

（ウ）CU-DU 区間の遅延値の確認

NTT 中央研修センタ（業界共用/複数企業共用）、いすゞ自動車、東北大学、東京大学、京都大学の各拠点で、DH 方式および量子暗号鍵方式のそれぞれで C-Plane / U-Plane それぞれの IPsec トンネルについて CU-DU 区間の遅延値を測定した結果を以下の「表 5-5-4-1」にまとめます。測定には DU から CU への ping を用いました。

本結果から、CU-DU 区間の遅延は地理的な距離や回線種別による影響は受けるが、鍵交換の方式による影響はないことが確認できました。これは、鍵交換の種別は、IPsec の通信を始めるための IKE フェーズ 1 にのみ関わり、実際の C-Plane/U-Plane の通信パケットが送られる IKE フェーズ 2 には関わらないため、

と考えられます。また、C-Plane および U-Plane のトンネルには暗号化の有無の設定を除いて違いがないため、遅延結果にも差異がない結果となっていると考えます。

表 5-5-4-1 CU-DU 区間遅延測定結果

拠点名	鍵交換方式	C-Plane 遅延(msec)	U-Plane 遅延(msec)
NTT 中央研修センタ（業界共用）	DH 方式	1.363	1.370
	量子暗号鍵方式	1.405	1.410
NTT 中央研修センタ（複数企業共用）	DH 方式	4.697	4.603
	量子暗号鍵方式	4.631	4.650
いすゞ自動車（複数企業共用）	DH 方式	6.411	6.343
	量子暗号鍵方式	6.349	6.440
東北大学（業界共用）	DH 方式	5.869	5.855
	量子暗号鍵方式	5.921	5.874
東京大学（業界共用）	DH 方式	0.382	0.353
	量子暗号鍵方式	0.402	0.375
京都大学（業界共用）	DH 方式	7.931	7.946
	量子暗号鍵方式	7.926	7.957

② セキュリティ機能付き SIM を用いた端末のセキュリティ

「表 5-5-3-3 デバイス種別」「表 5-5-3-4 デバイスグループおよびポリシーの設定（抜粋)」に示す 3 種類のデバイスの設定を行うための設定を示します。拠点別、デバイス種別に異なるセキュリティレベルの運用がなされることを想定し、拠点別、デバイス種別のデバイスグループを作成し、デバイスグループ毎にセキュリティポリシーを設定しました。「図 5-5-4-3-1-1」にデバイスグループの一覧、「図 5-5-4-3-1-2」にセキュリティポリシーの一覧、「図 5-5-4-3-1-3」にセキュリティポリシーの詳細の一例を示します。

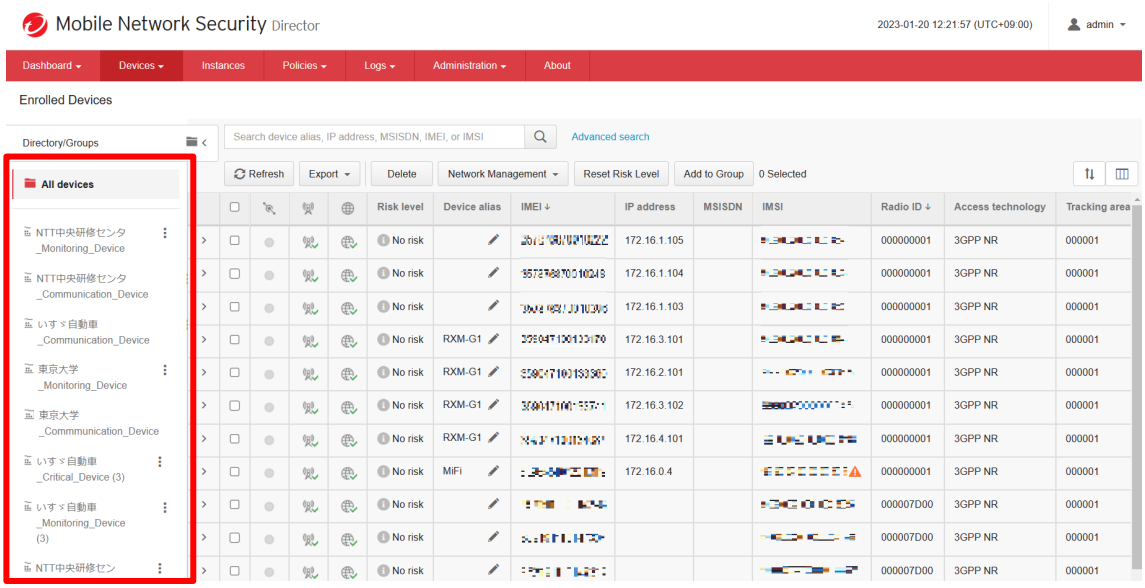


図 5-5-4-3-1-1 デバイスグループの一覧

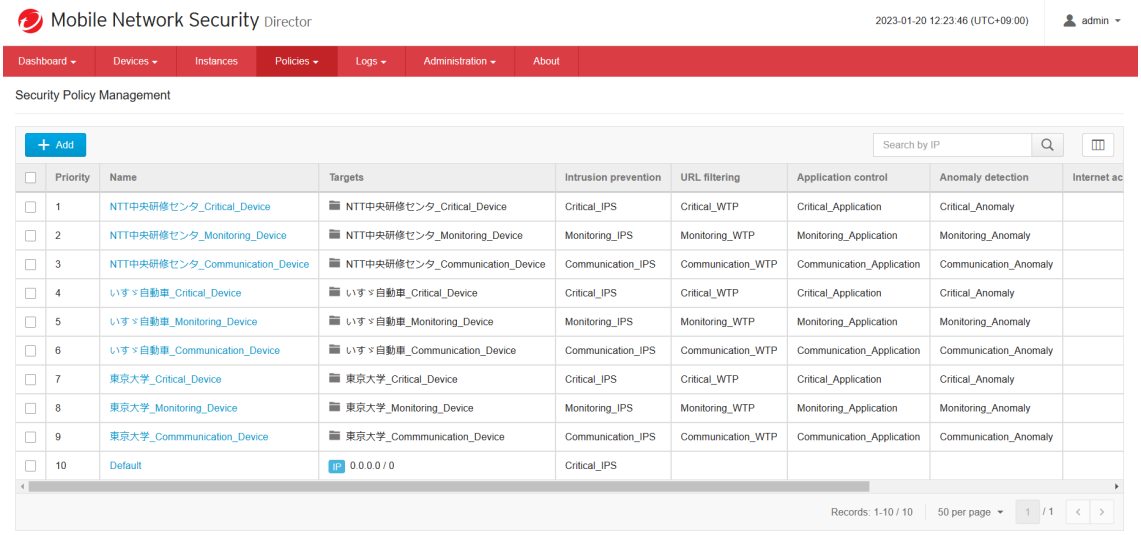


図 5-5-4-3-1-2 セキュリティポリシーの一覧

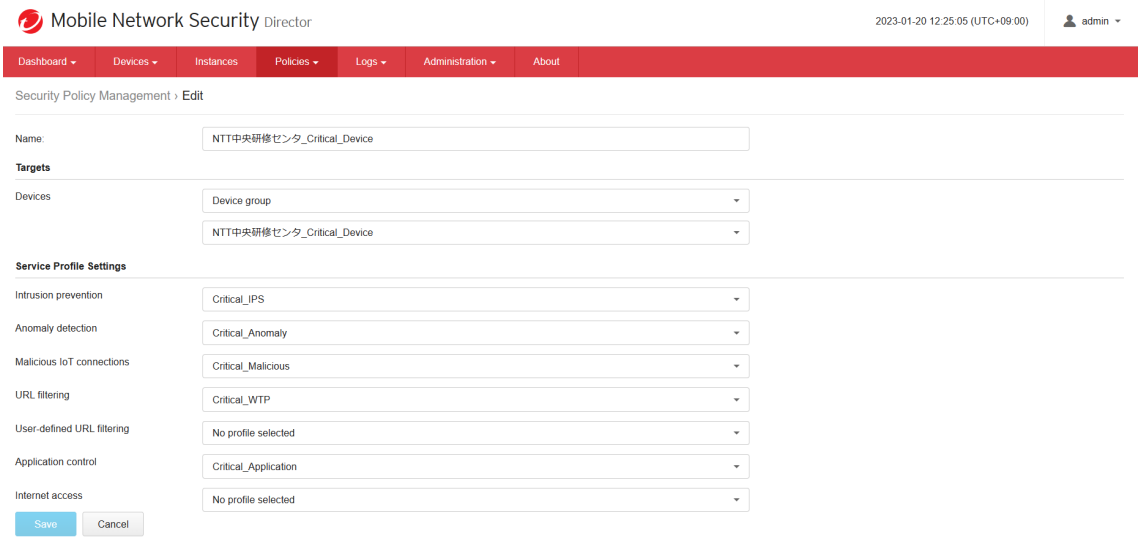


図 5-5-4-3-1-3 セキュリティポリシー詳細(NTT 中央研修センタ/Critical Device の例)

(ア)端末状態の監視・可視化

ア 全体管理

コア共用形態で複数の拠点の複数の端末を管理するために必要となる、端末の真正性の確認と端末情報の整理機能について確認しました。

・端末の真正性の確認

端末のオンライン/オフライン状態が適切に確認できること、IMSI/IMEI、Cell ID、端末情報、オープンポートが確認できることを検証するため、UE1～UE3 と名前を付けた端末のみをローカル５Ｇに接続した後、UE2 のみオフラインにし GUI の表示を確認しました。「図 5-5-4-4-1-1」に 3 台ともオンラインの際の表示、「図 5-5-4-4-1-2」に UE2 のみオフラインにした際の表示、「図 5-5-4-4-1-3」に表示列を変更し各情報が確認できる様子を示します。「図 5-5-4-4-1-1」の赤で囲んだ枠内の〇表示は、緑色の丸がオンライン、灰色の丸がオフライン(端末電源 OFF 等)、赤色の丸がセキュリティ違反によるオフライン(システムからの遮断)を示します。(以下同様)

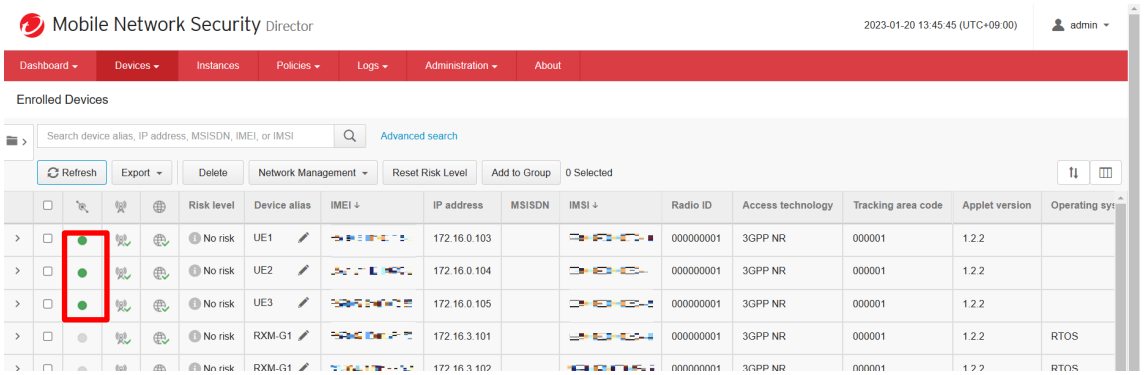


図 5-5-4-4-1-1 3 台オンラインの様子

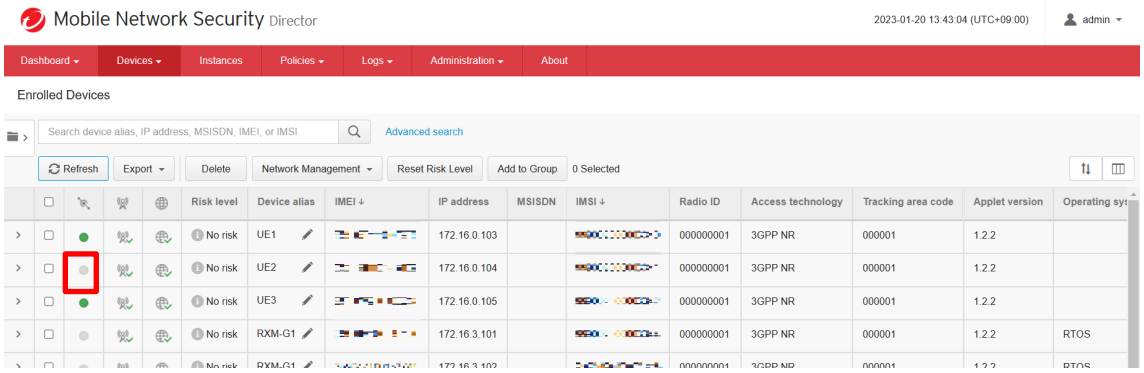


図 5-5-4-4-1-2 UE2 のみオフラインの様子

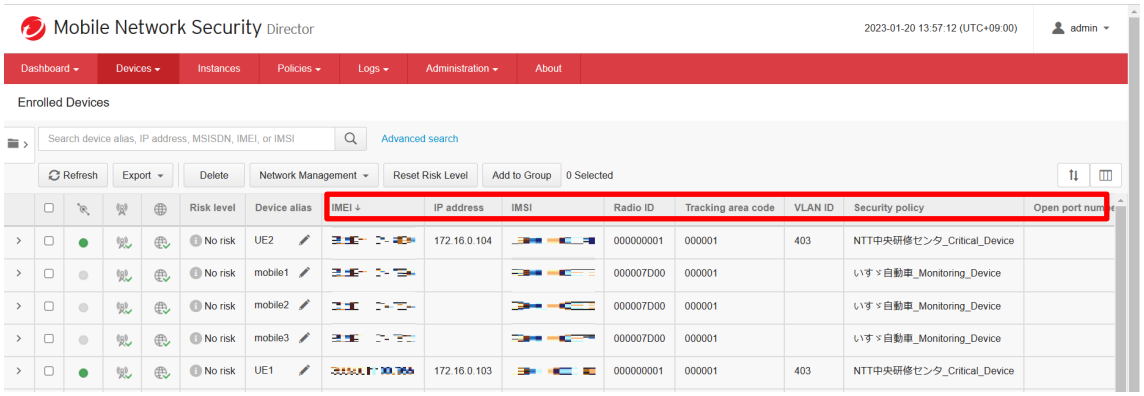


図 5-5-4-4-1-3 端末情報の可視化

・端末情報整理

端末を一覧表示した際に IMEI / IMSI / Radio ID / Tracking Area Code / Risk Level でソートできることを確認しました。IMEI については「図 5-5-4-4-1-1」が該当します。「図 5-5-4-4-1-4～図 5-5-4-4-1-7」に残りの基準でのソートを実施した結果を示します。

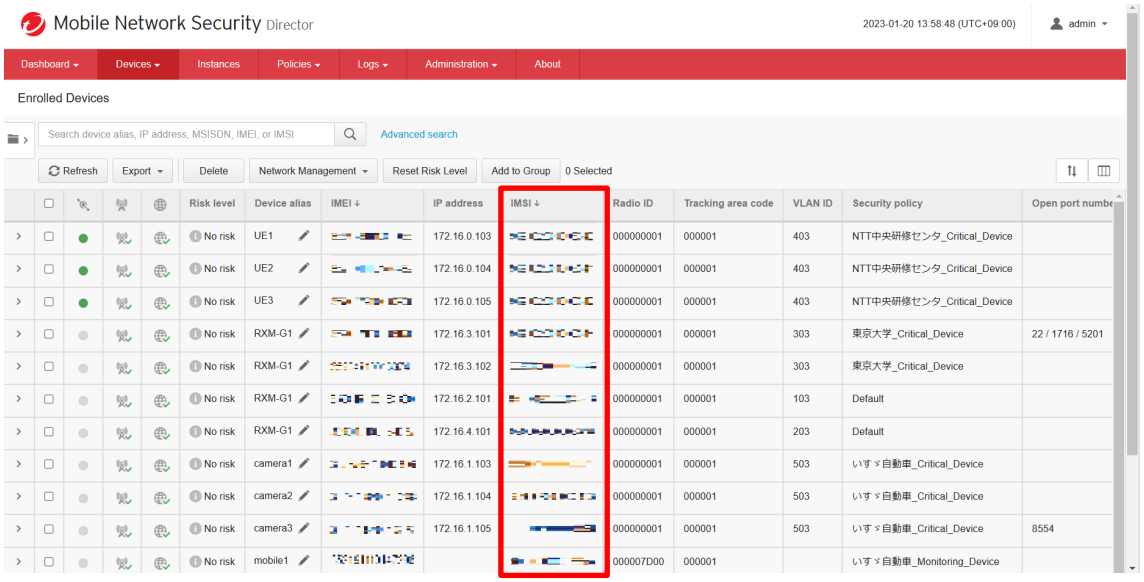


図 5-5-4-4-1-4 IMSI によるソート

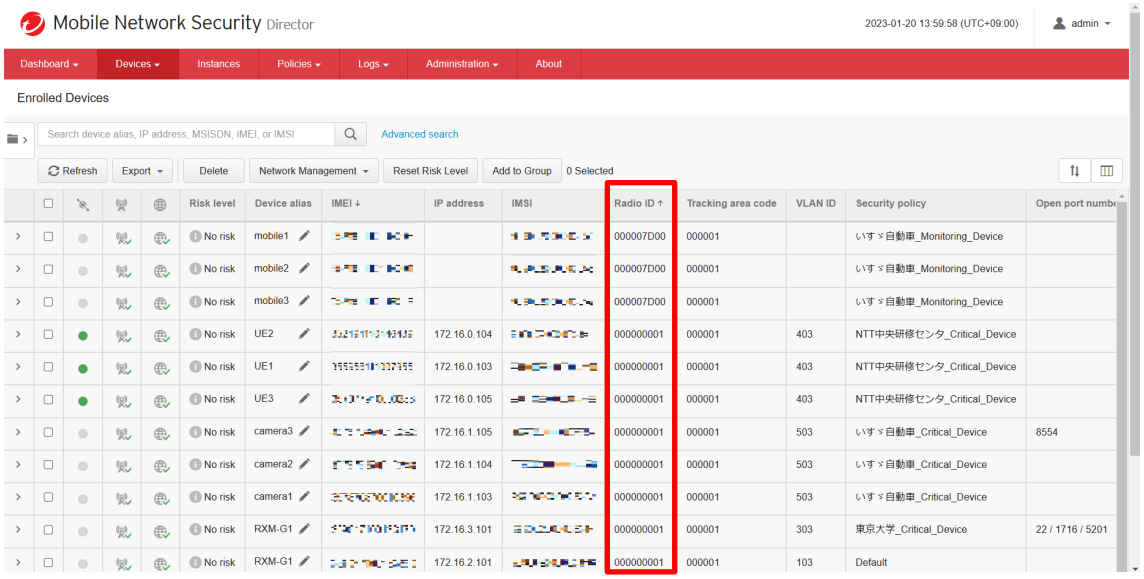


図 5-5-4-4-1-5 Radio ID によるソート

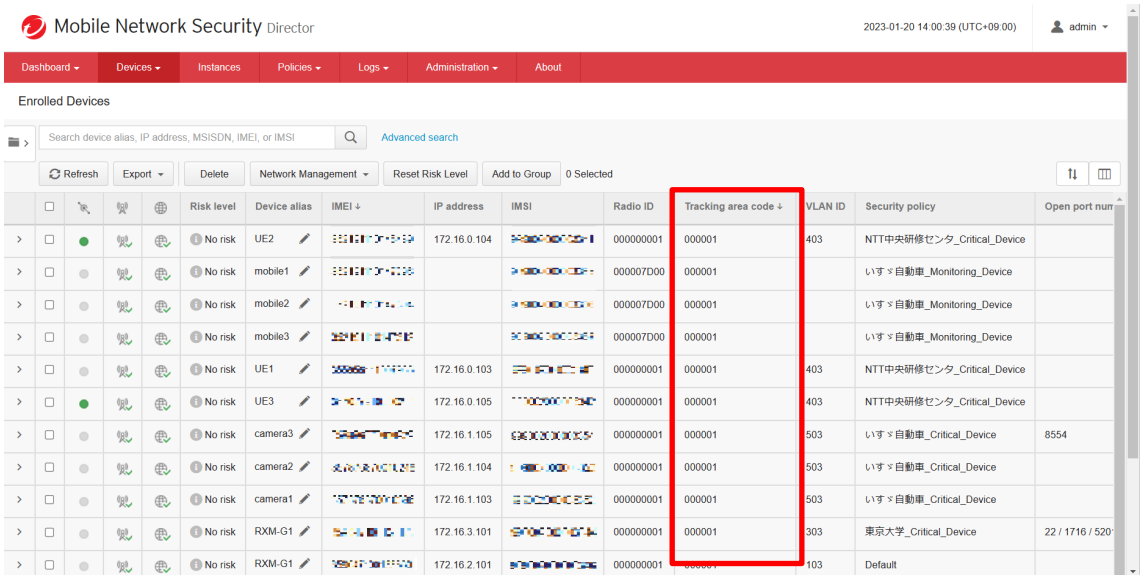


図 5-5-4-4-1-6 Tracking Area Code によるソート

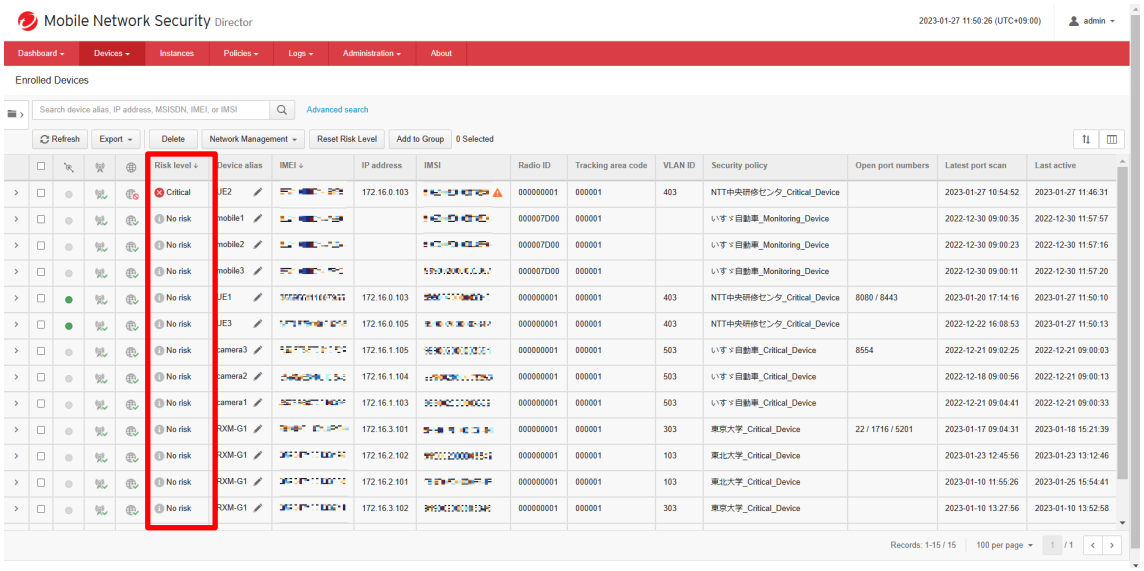


図 5-5-4-4-1-7 Risk Level によるソート

次項からは拠点毎の端末状態の監視・可視化について検証を行いました。

イ　NTT 中央研修センタ 業界共用パターン

・拠点毎の端末の真正性の確認

「図 5-5-4-4-2-1」に UE1～UE3 を NTT 中央研修センタ_Critcal_Device に設定しオンラインにした結果、「図 5-5-4-4-2-2」に UE2 のみオフラインにした結果、「図 5-5-4-4-2-3」に各情報を表示した結果を示します。

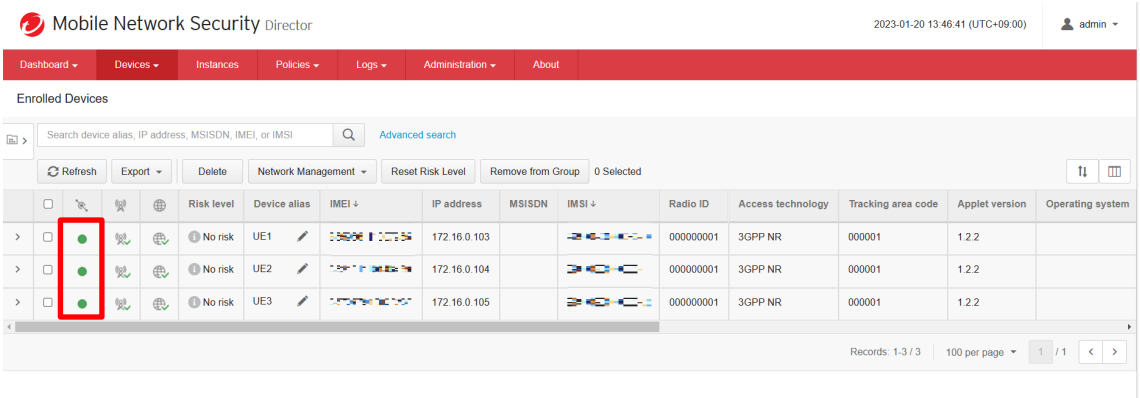


図 5-5-4-4-2-1 3 台オンラインの様子(NTT 中央研修センタ / 業界共用 / センタ UPF)

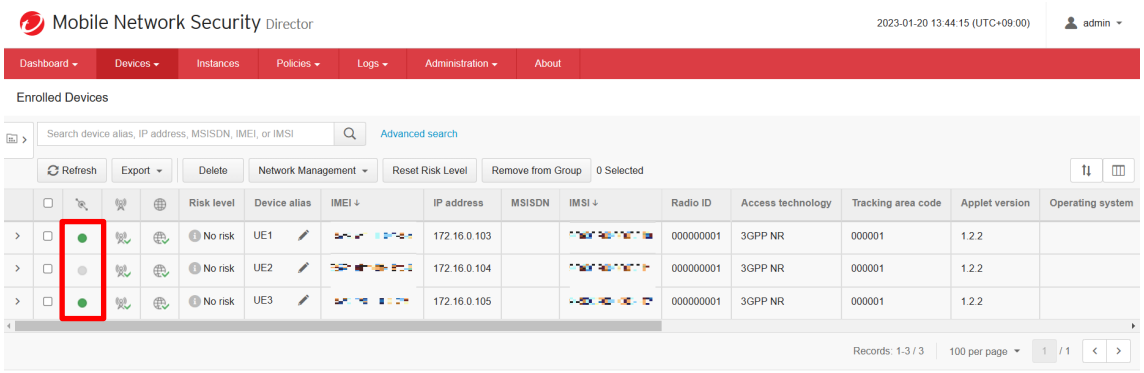


図 5-5-4-4-2-2 UE2 のみオフラインの様子(NTT 中央研修センタ / 業界共用 / センタ UPF)

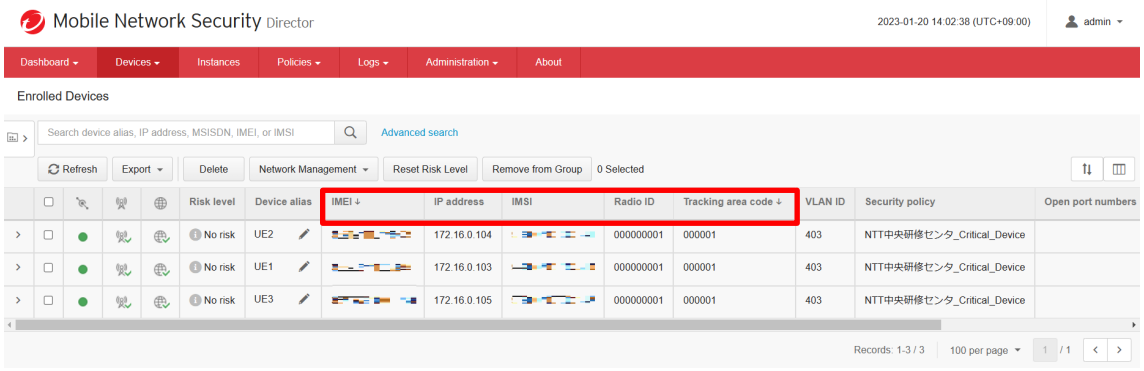


図 5-5-4-4-2-3 端末情報の可視化(NTT 中央研修センタ / 業界共用 / センタ UPF)

・端末情報のトレーサビリティの確認

端末の情報が更新された場合にその情報が反映されることを検証するため、端末の IP アドレスを変更し、GUI 上の情報が更新されることを確認しました。「図 5-5-4-4-2-4」に変更前(172.16.0.104)、「図 5-5-4-4-2-5」に変更後(172.16.0.130)の GUI 画面を示します。これにより端末の情報の変更がトレースできていることが確認できました。

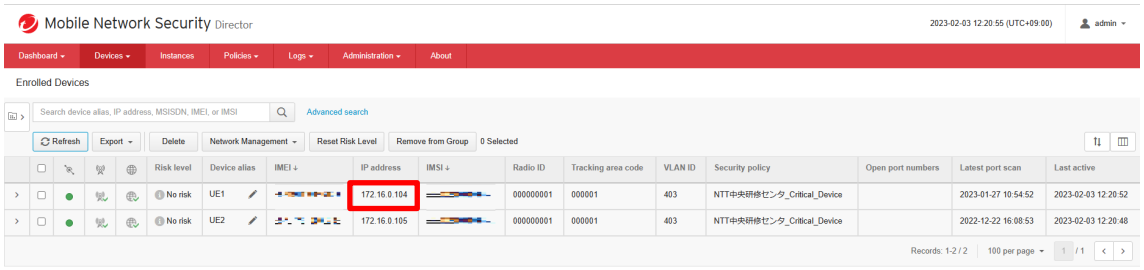


図 5-5-4-4-2-4 IP アドレス変更前(NTT 中央研修センタ / 業界共用 / センタ UPF)

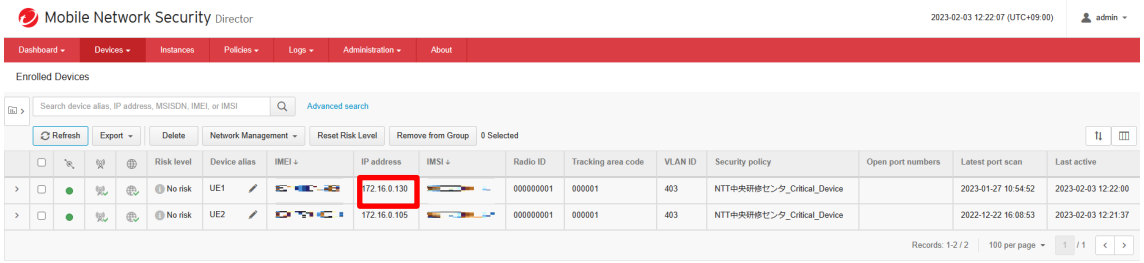


図 5-5-4-4-2-5 IP アドレス変更後(NTT 中央研修センタ / 業界共用 / センタ UPF)

・拠点毎の端末情報整理

端末を拠点毎に一覧表示した際に IMEI / IMSI / Radio ID / Tracking Area Code / Risk Level でソートできることを確認しました。IMEI については「図 5-5-4-4-2-1」が該当します。「図 5-5-4-4-2-6」「図 5-5-4-4-2-7」に IMSI/Risk Level でソートを実施した結果を示します。Radio ID および Tracking Area の結果については同一拠点ですべて同じ値を示すため割愛いたします。

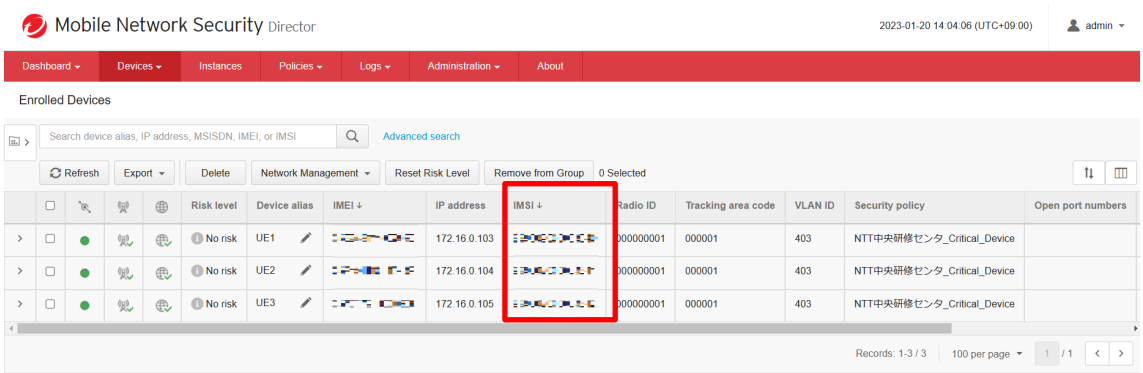


図 5-5-4-4-2-6 IMSI によるソート

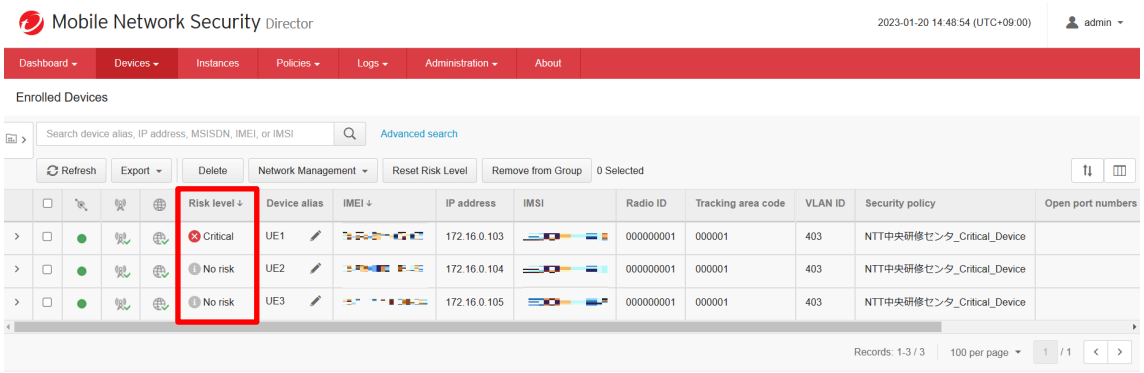


図 5-5-4-4-2-7 Risk Level によるソート

・端末情報の可視化

端末からの不正な通信を検知した際に通信の内容をログで確認できることと、どの拠点のどの端末が不正な通信を行ったか可視化できることを確認しました。本調査研究では疑似的な不正通信として web サーバに保存されたパスワードを盗み見るディレクトリトラバーサル攻撃を想定し、/etc/passwd を含む http リクエストを端末または端末下部の PC から送信しました。端末から不正な通信を送信すると「図 5-5-4-4-2-7」のように Risk Level が自動的に Critical に上がることが確認できました。また「図 5-5-4-4-2-8」に示す通信のログから、/etc/passwd を含む通信が検知されていることが確認できました。

「図 5-5-4-4-2-9～図 5-5-4-4-2-11」に不正通信を行った端末の特定のための可視化機能を示します。「図 5-5-4-4-2-11」についてこのように、トラフィック監視装置ごと、Radio ID ごとの可視化機能を有することで複数拠点の管理に有効であると考えます。

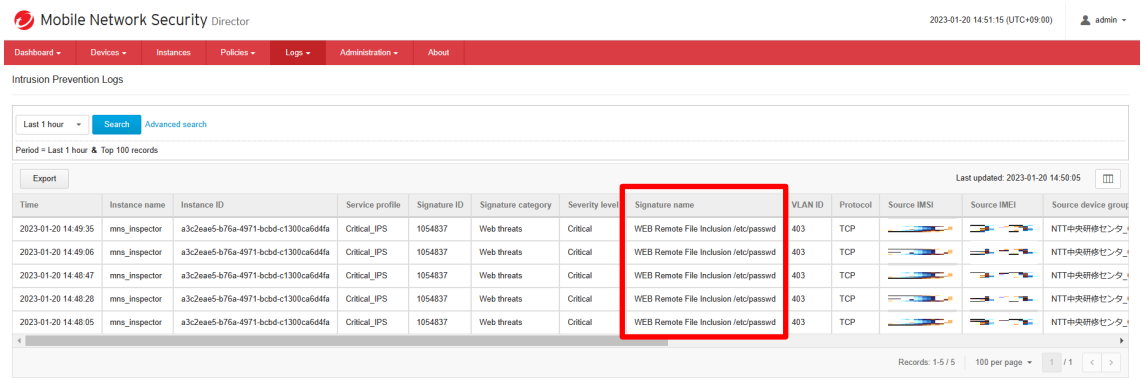


図 5-5-4-4-2-8 不正通信のログ

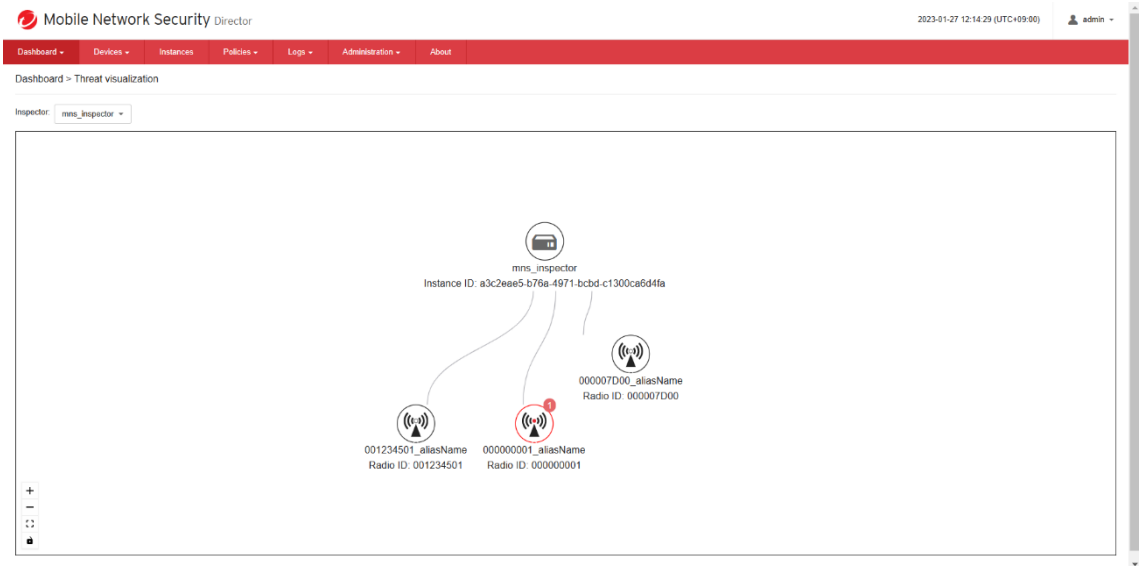


図 5-5-4-4-2-9 監視装置ごとの可視化(赤い〇が不正通信のあった Radio ID)

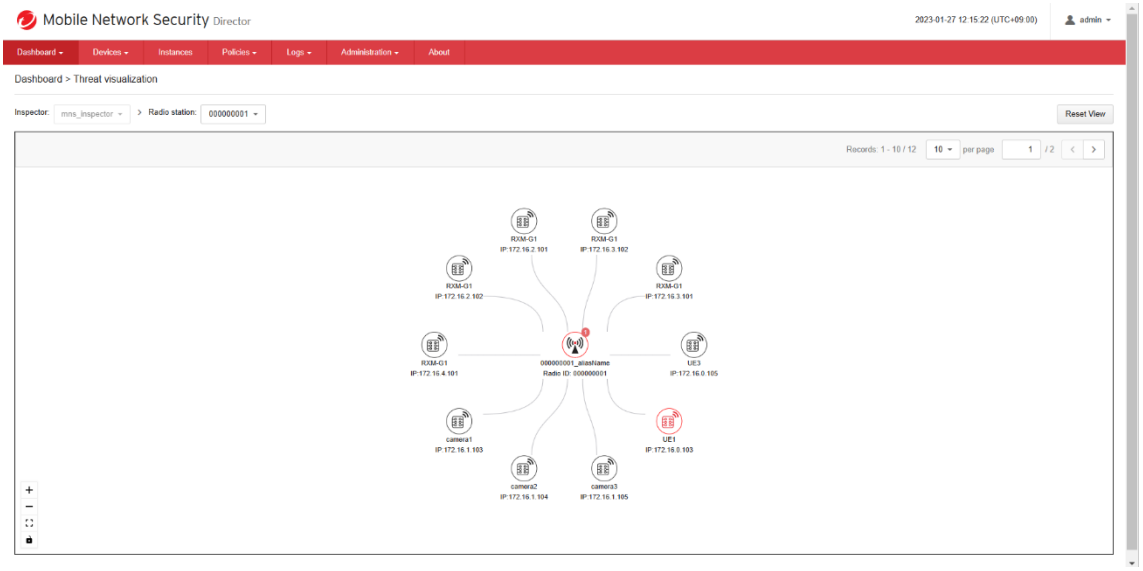


図 5-5-4-4-2-10 Radio ID ごとの可視化(赤い〇が不正通信を行った端末)

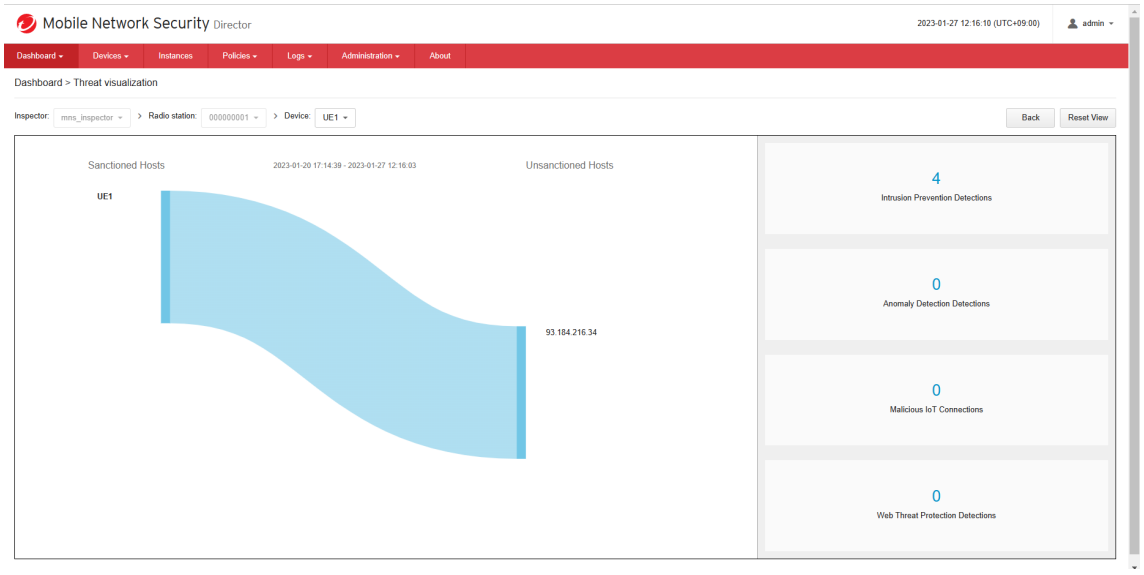


図 5-5-4-4-2-11 不正通信の様子(左：不正通信を行った端末 右：不正通信の宛先)

また、「図 5-5-4-4-2-1～図 5-5-4-4-2-11」の検証について、エンド UPF に監視装置を設置した場合も同様の結果が得られました。結果の見え方についてはセンタ UPF の構成と同様のため割愛いたします。

ウ NTT 中央研修センタ 複数企業共用パターン

・拠点毎の端末の真正性の確認

「図 5-5-4-4-3-1」に複 UE1～複 UE3 を NTT 中央研修センタ_Critcal_Device として設定しオンラインにした結果、「図 5-5-4-4-3-2」に複 UE3 のみオフラインにした結果、「図 5-5-4-4-3-3」に各情報を表示した結果を示します。

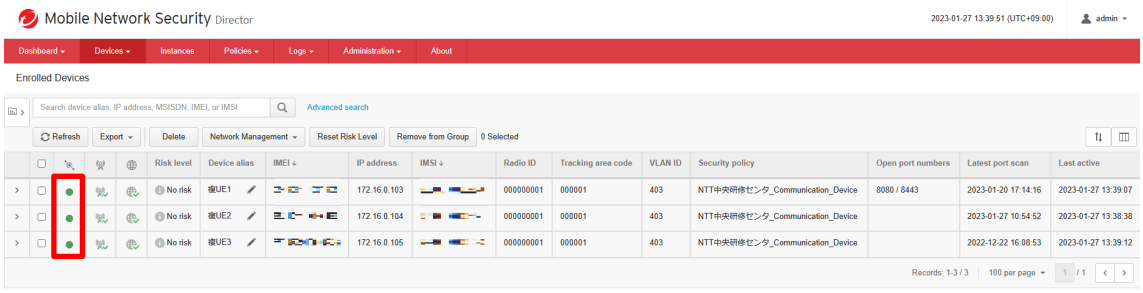


図 5-5-4-4-3-1 3 台オンラインの様子
(NTT 中央研修センタ / 複数企業共用 / センタ UPF)

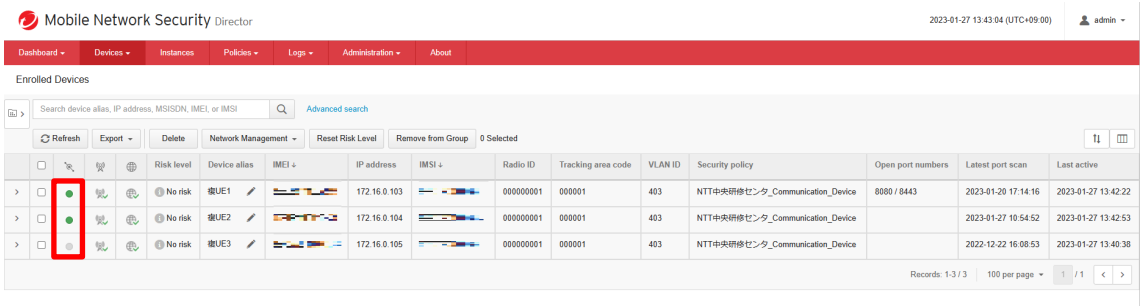


図 5-5-4-4-3-2 UE3 のみオフラインの様子
(NTT 中央研修センタ / 複数企業共用 / センタ UPF)

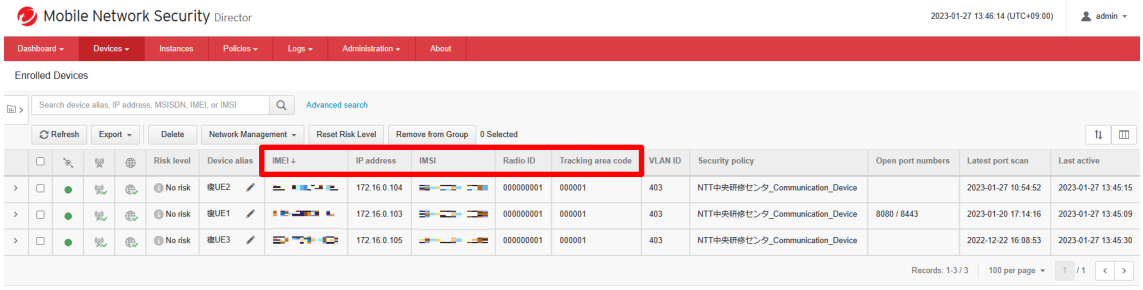


図 5-5-4-4-3-3 端末情報の可視化(NTT 中央研修センタ / 複数企業共用 / センタ UPF)

・端末情報のトレーサビリティの確認

端末の情報が更新された場合にその情報が反映されることを検証するため、端末の IP アドレスを変更し、GUI 上の情報が更新されることを確認しました。「図 5-5-4-4-3-4」に変更前(172.16.0.104)、「図 5-5-4-4-3-5」に変更後(172.16.0.131)の GUI 画面を示します。これにより端末の情報の変更がトレースできていることが確認できました。

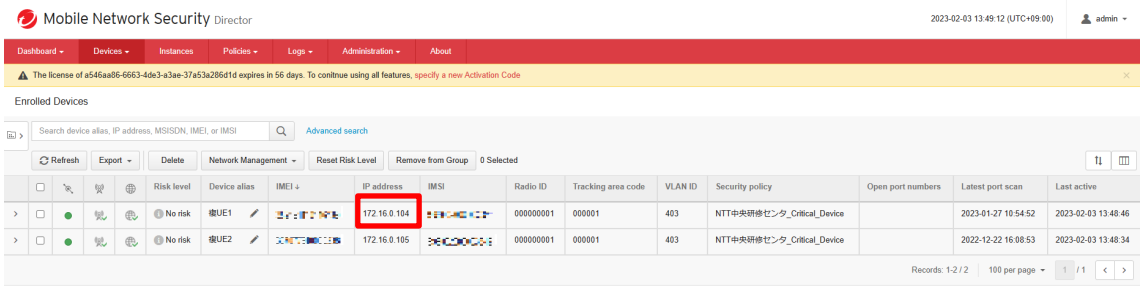


図 5-5-4-4-3-4 IP アドレス変更前(NTT 中央研修センタ / 複数企業共用 / センタ UPF)

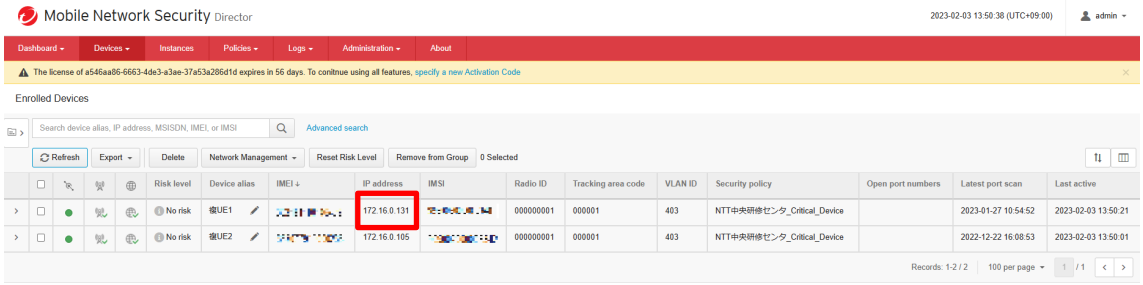


図 5-5-4-4-3-5 IP アドレス変更後(NTT 中央研修センタ / 複数企業共用 / センタ UPF)

・拠点毎の端末情報整理

端末を拠点毎に一覧表示した際に IMEI / IMSI / Radio ID / Tracking Area Code / Risk Level でソートできることを確認しました。IMEI については「図 5-5-4-4-3-1」が該当します。「図 5-5-4-4-3-6」「図 5-5-4-4-3-7」に IMSI/Risk Level でソートを実施した結果を示します。Radio ID および Tracking Area の結果については同一拠点ですべて同じ値を示すため割愛いたします。

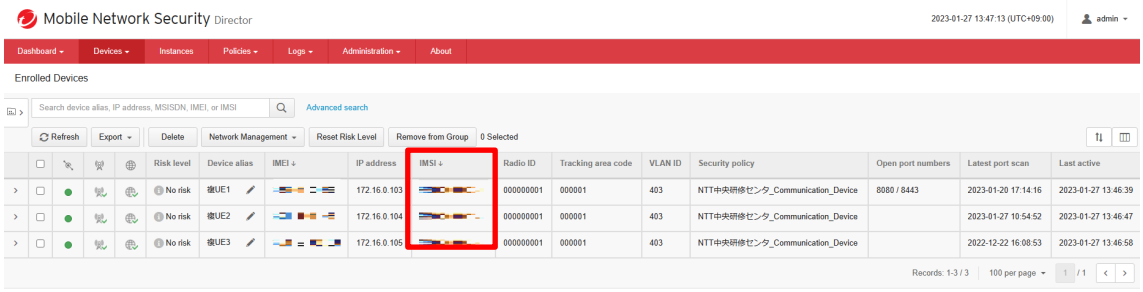


図 5-5-4-4-3-6 IMSI によるソート

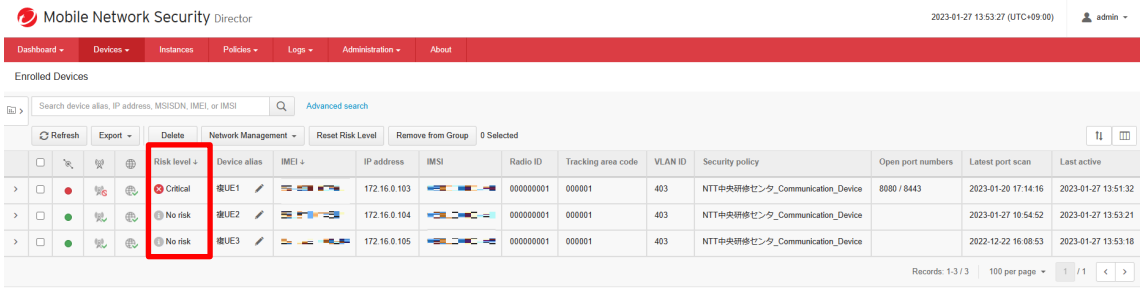


図 5-5-4-4-3-7 Risk Level によるソート

・端末情報の可視化

端末からの不正な通信を検知した際に通信の内容をログで確認できることと、どの拠点のどの端末が不正な通信を行ったか可視化できることを確認しました。端末から不正な通信を送信すると「図 5-5-4-4-3-7」のように Risk Level が自動的に Critical に上がることが確認できました。また「図 5-5-4-4-3-8」に示す通信のログから/etc/passwd を含む通信が検知されたことが確認できました。

「図 5-5-4-4-3-9～図 5-5-4-4-3-11」に不正通信を行った端末の特定のための可視化機能の様子を示します。

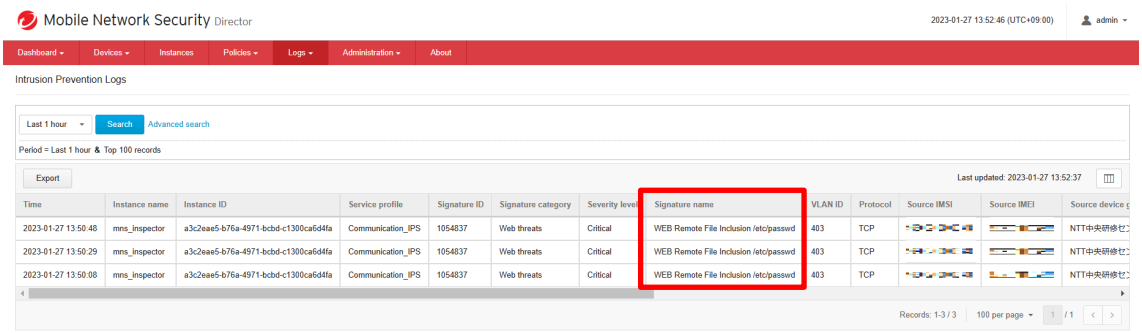


図 5-5-4-4-3-8 不正通信のログ

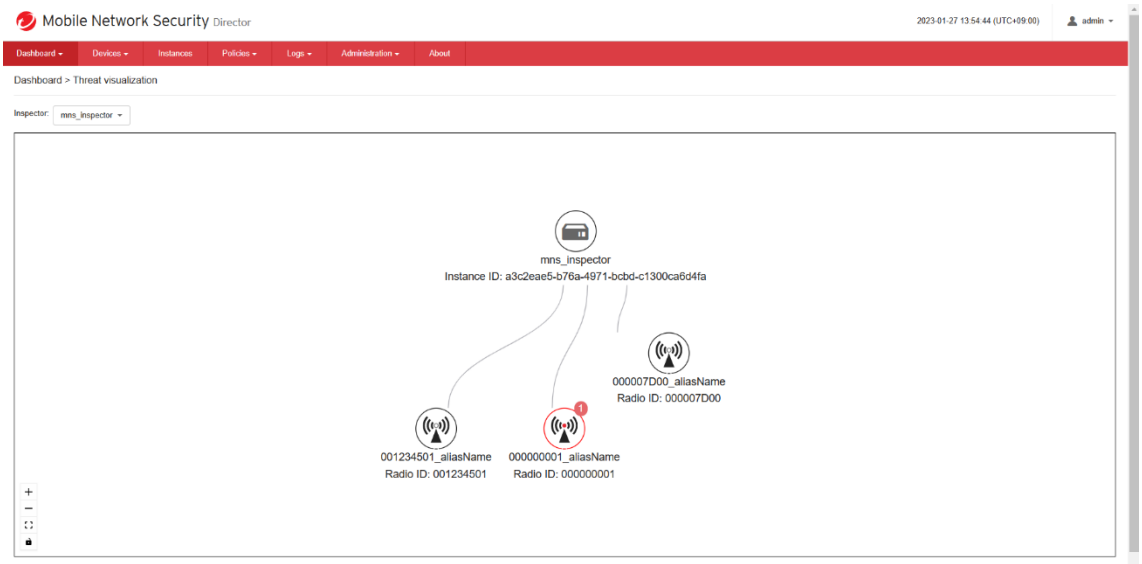


図 5-5-4-4-3-9 監視装置ごとの可視化(赤い〇が不正通信のあった Radio ID)

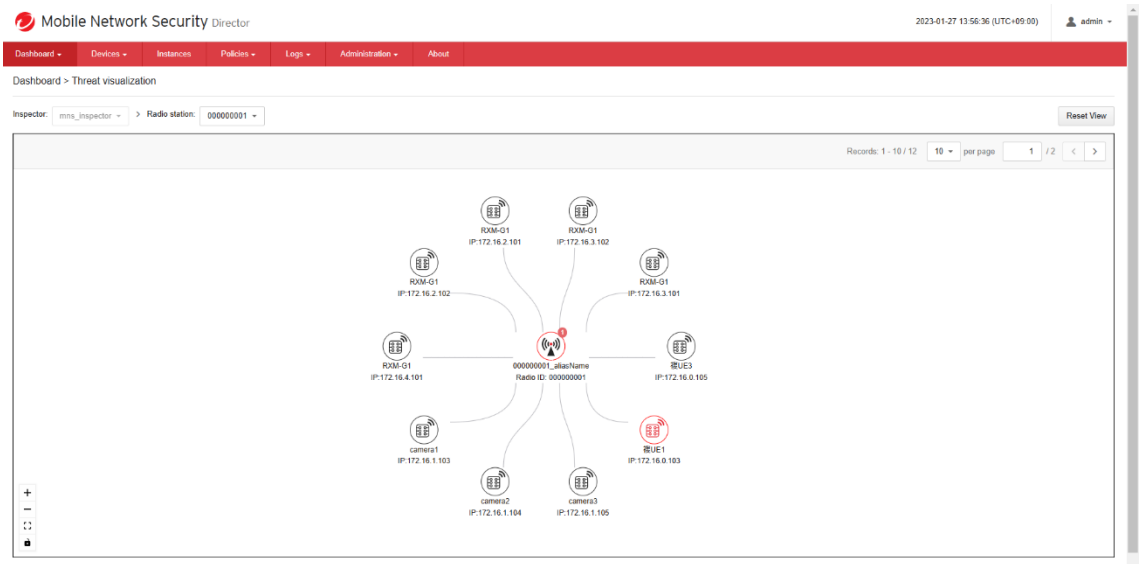


図 5-5-4-4-3-10 Radio ID ごとの可視化(赤い〇が不正通信を行った端末)

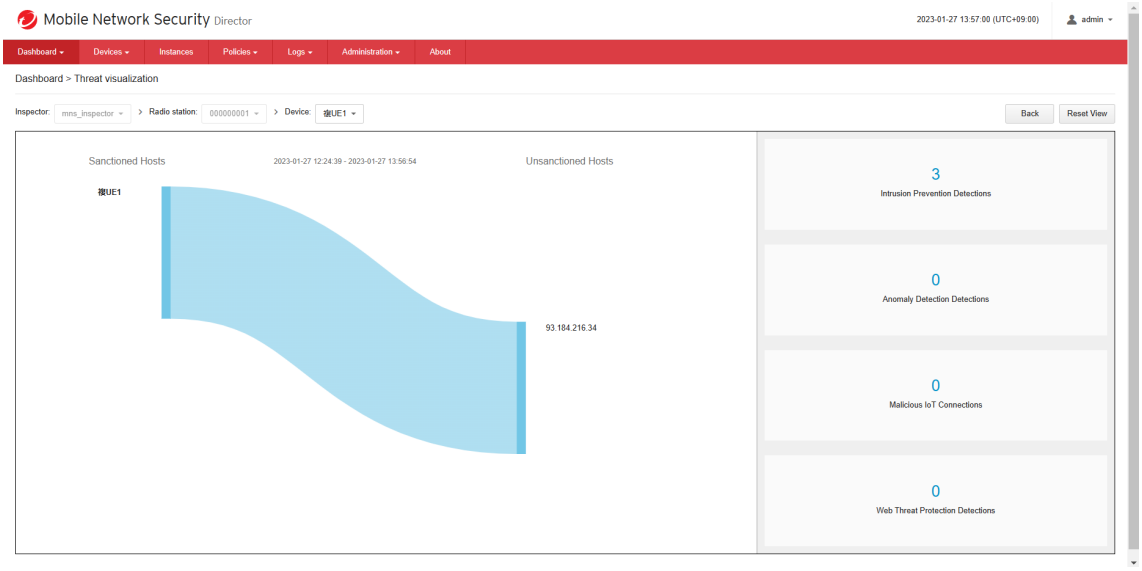


図 5-5-4-4-3-11 不正通信の様子(左：不正通信を行った端末 右：不正通信の宛先)

また、「図 5-5-4-4-3-1～図 5-5-4-4-3-11」の検証について、エンド UPF に監視装置を設置した場合も同様の結果が得られました。結果の見え方についてはセンタ UPF の構成と同様のため割愛いたします。

エ　いすゞ自動車

・拠点毎の端末の真正性の確認

「図 5-5-4-4-4-1」に UE1～UE3 をいすゞ自動車_Critcal_Device に設定しオンラインにした結果、「図 5-5-4-4-4-2」に UE1 のみオフラインにした結果、「図 5-5-4-4-4-3」に各情報を表示した結果を示します。

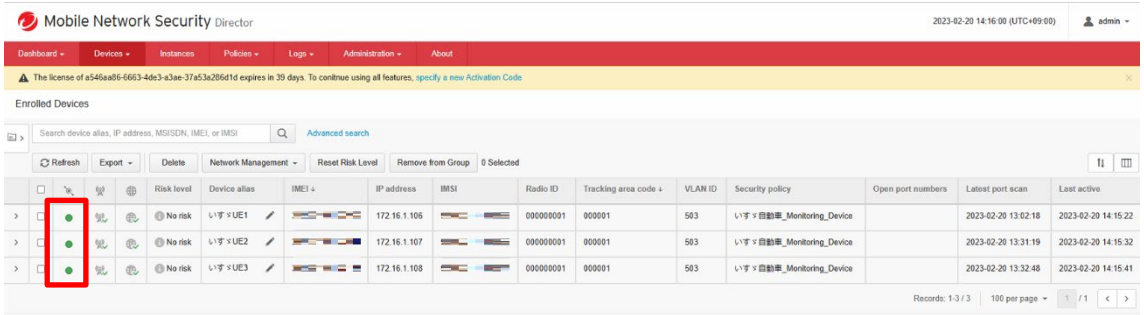


図 5-5-4-4-4-1 3 台オンラインの様子(いすゞ自動車)

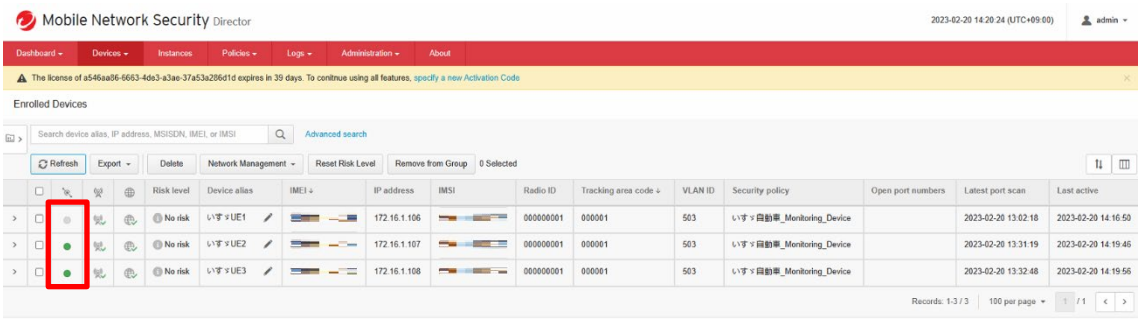


図 5-5-4-4-4-2 UE1 のみオフラインの様子(いすゞ自動車)

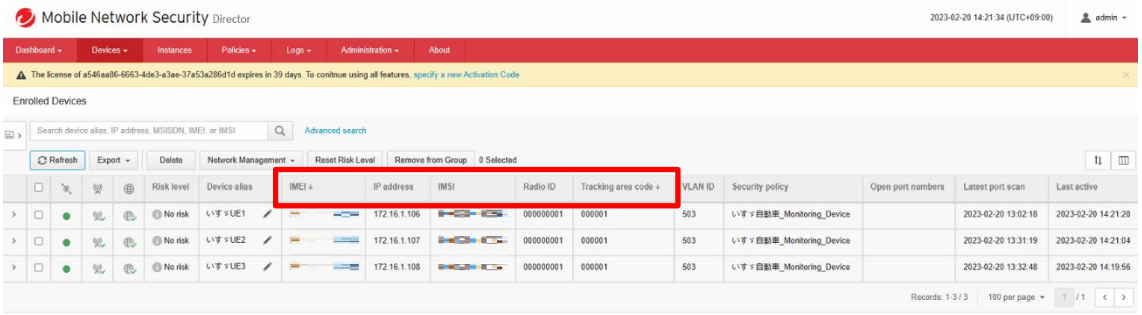


図 5-5-4-4-4-3 端末情報の可視化(いすゞ自動車)

・拠点毎の端末情報整理

端末を拠点毎に一覧表示した際に IMEI / IMSI / Radio ID / Tracking Area Code / Risk Level でソートできることを確認しました。IMEI については「図 5-5-4-4-4-1」が該当します。「図 5-5-4-4-4-4」「図 5-5-4-4-4-5」に IMSI/Risk Level でソートを実施した結果を示します。Radio ID および Tracking Area の結果については同一拠点ですべて同じ値を示すため割愛いたします。

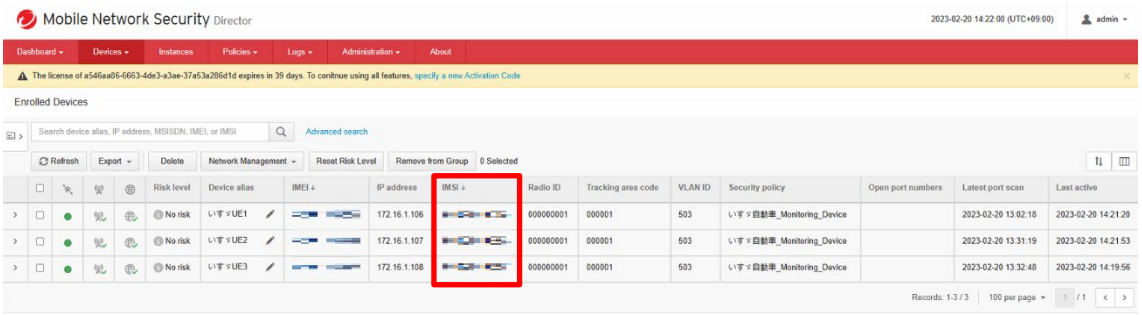


図 5-5-4-4-4-4 IMSI によるソート(いすゞ自動車)

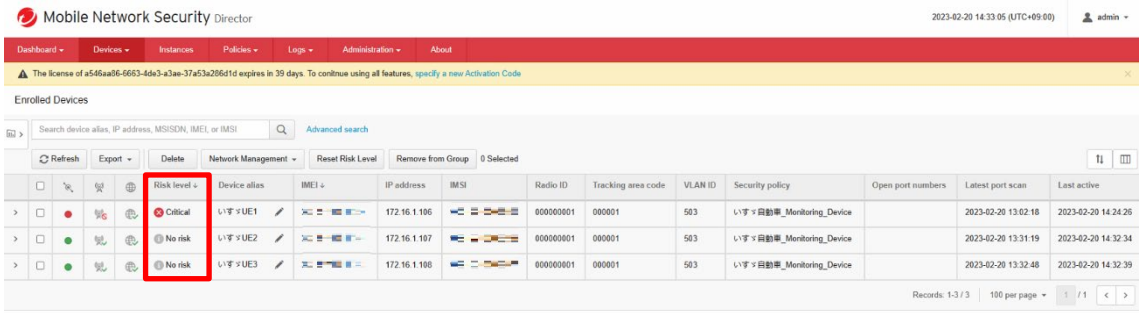


図 5-5-4-4-4-5 Risk Level によるソート(いすゞ自動車)

・端末情報の可視化

端末からの不正な通信を検知した際に通信の内容をログで確認できることと、どの拠点のどの端末が不正な通信を行ったか可視化できることを確認しました。本調査研究では疑似的な不正通信として web サーバに保存されたパスワードを盗み見るディレクトリトラバーサル攻撃を想定し、/etc/passwd を含む http リクエストを端末または端末下部の PC から送信しました。端末から不正な通信を送信すると「図 5-5-4-4-4-5」のように Risk Level が自動的に Critical に上がることが確認できました。また「図 5-5-4-4-4-6」に示す通信のログから、/etc/passwd を含む通信が検知されていることが確認できました。

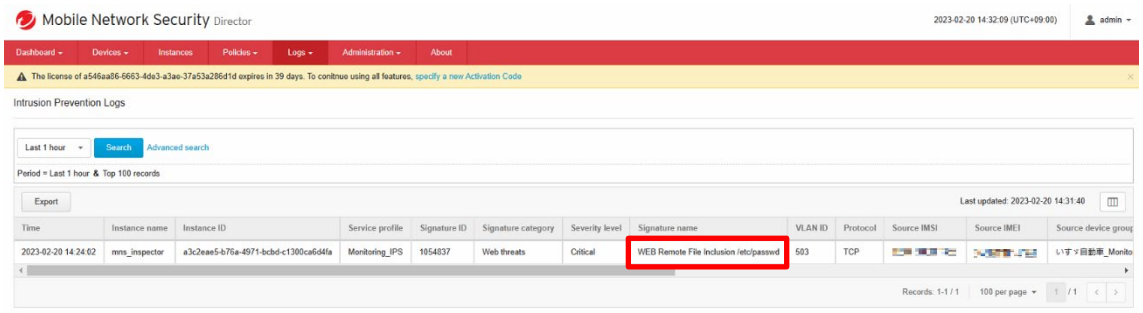


図 5-5-4-4-4-6 不正通信のログ（いすゞ自動車)

端末の特定のための可視化機能については「図 5-4-4-2-9～図 5-4-4-2-11」と同様のため割愛します。

オ　東北大学

・拠点毎の端末の真正性の確認

「図 5-5-4-4-5-1」に UE1～UE3 を東北大学_Critcal_Device に設定しオンラインにした結果、「図 5-5-4-4-5-2」に UE3 のみオフラインにした結果、「図 5-5-4-4-5-3」に各情報を表示した結果を示します。

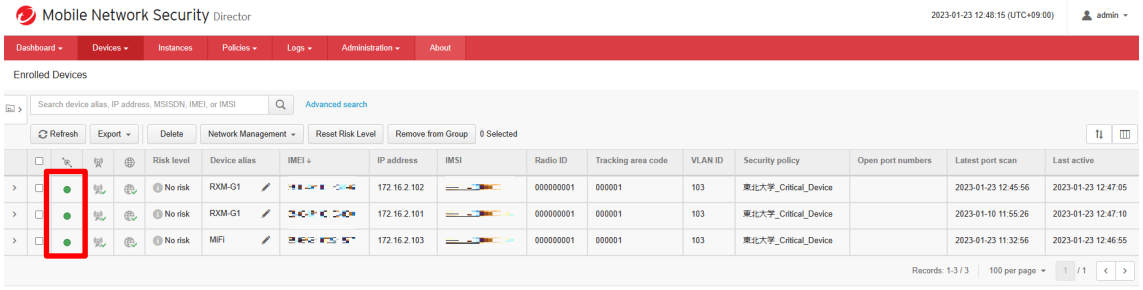


図 5-5-4-4-5-1 3 台オンラインの様子(東北大学)

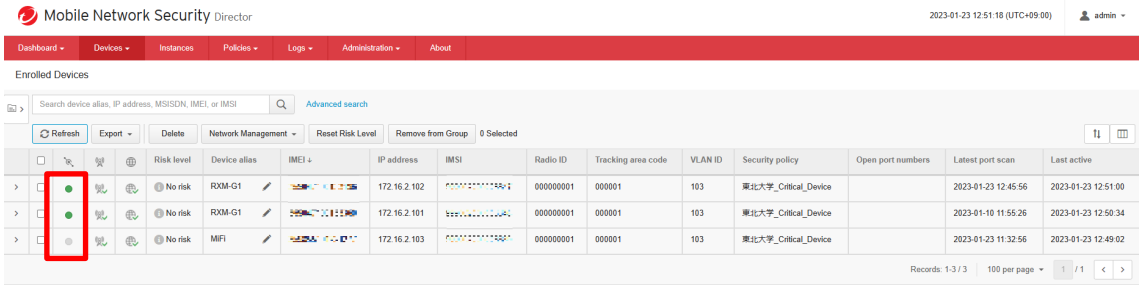


図 5-5-4-4-5-2 UE3 のみオフラインの様子(東北大学)

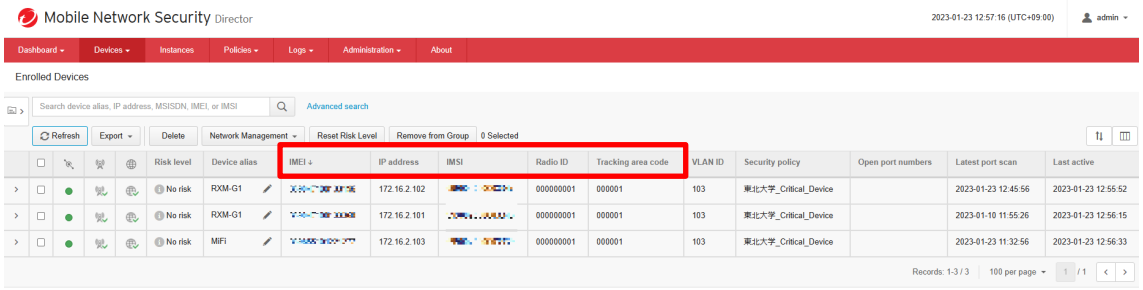


図 5-5-4-4-5-3 端末情報の可視化(東北大学)

・拠点毎の端末情報整理

端末を拠点毎に一覧表示した際に IMEI / IMSI / Radio ID / Tracking Area Code / Risk Level でソートできることを確認しました。IMEI については「図 5-5-4-4-5-1」が該当します。「図 5-5-4-4-5-4」「図 5-5-4-4-5-5」に IMSI/Risk Level でソートを実施した結果を示します。Radio ID および Tracking Area の結果については同一拠点ですべて同じ値を示すため割愛いたします。

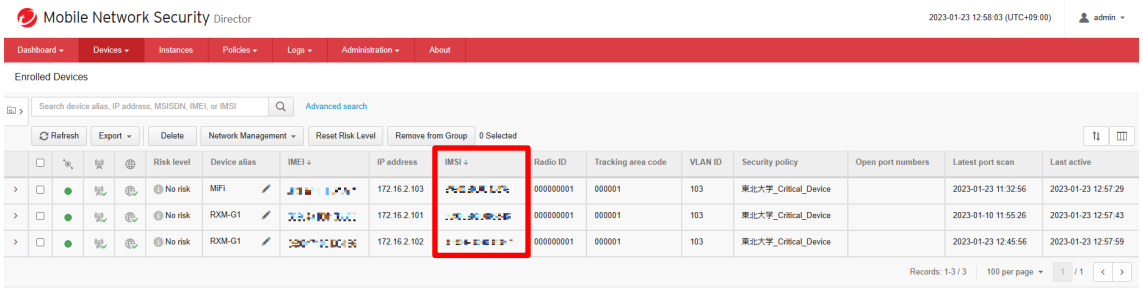


図 5-5-4-4-5-4 IMSI によるソート（東北大学）

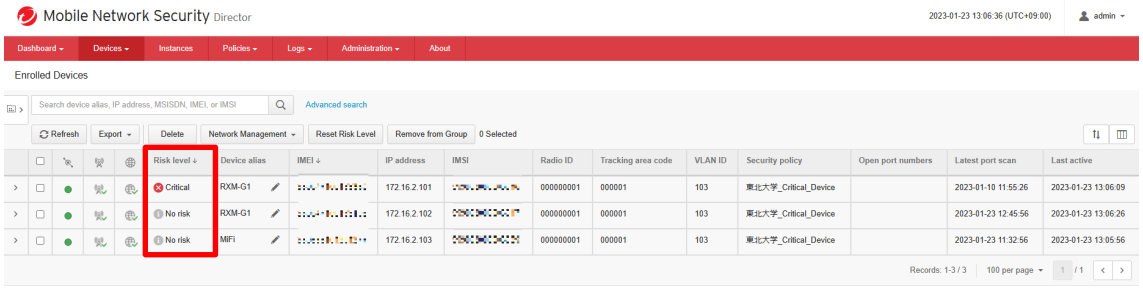


図 5-5-4-4-5-5 Risk Level によるソート（東北大学）

・端末情報の可視化

端末からの不正な通信を検知した際に通信の内容をログで確認できることと、どの拠点のどの端末が不正な通信を行ったか可視化できることを確認しました。本調査研究では疑似的な不正通信として web サーバに保存されたパスワードを盗み見るディレクトリトラバーサル攻撃を想定し、/etc/passwd を含む http リクエストを端末または端末下部の PC から送信しました。端末から不正な通信を送信すると「図 5-5-4-4-5-5」のように Risk Level が自動的に Critical に上がることが確認できました。また「図 5-5-4-4-5-6」に示す通信のログから、/etc/passwd を含む通信が検知されていることが確認できました。

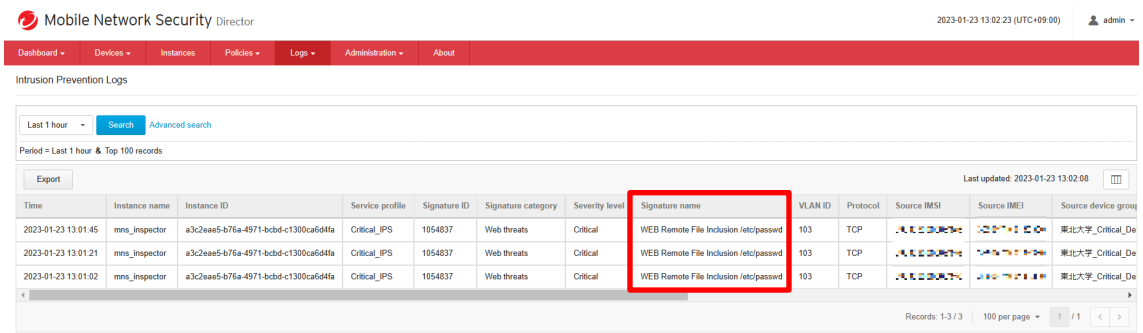


図 5-5-4-4-5-6 不正通信のログ（東北大学）

端末の特定のための可視化機能については「図 5-5-4-4-3-9～図 5-5-4-4-3-11」と同様のため割愛します。

（イ）セキュリティ脅威の検知・遮断

ア　NTT 中央研修センタ 業界共用パターン

・アクセス制御

本項目ではセキュリティ機能付き SIM を使用した端末がアクセスできるネットワークを制限できることを端末間の通信を用いて検証します。端末間の通信に関するセキュリティポリシーは「表 5-5-3-3」に示すとおりです。Monitoring Device はカメラや相互連携しないセンサであり、端末間の通信が不要であることが想定されます。本検証ではセキュリティ機能により Monitoring Device のみが互いに通信不可となっていることを確認しました。「図 5-5-4-5-1-1～図 5-5-4-5-1-3」にそれぞれ Critical Device / Monitoring Device / Communication Device に設定した端末間で ping を送付した際のログを示します。（送信元 IP 172.16.0.103 から送信先 IP 172.16.0.104 への ping） Action の列から Monitoring Device のみ Block していることが確認できました。

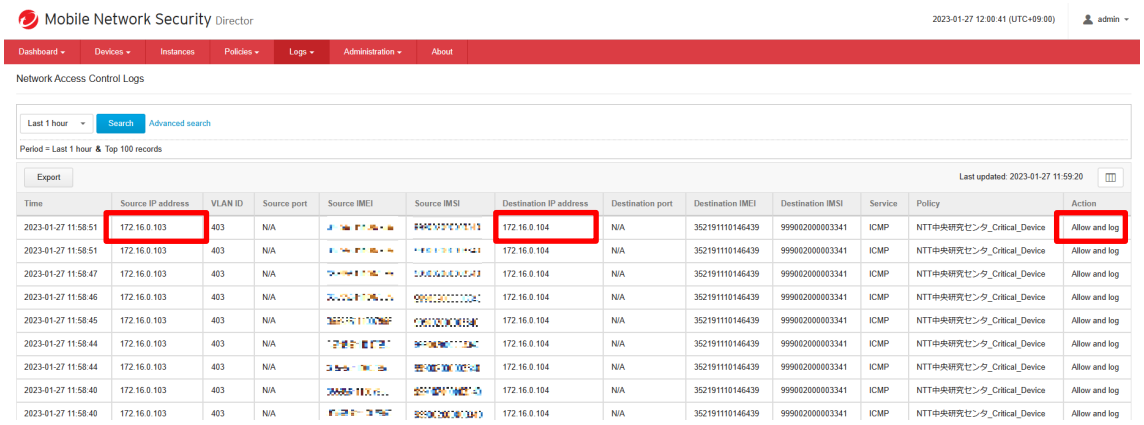


図 5-5-4-5-1-1 端末間 ping のログ Critical Device（業界共用）

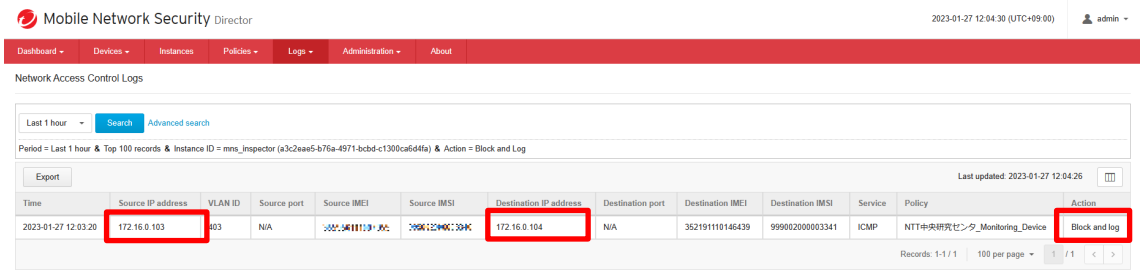


図 5-5-4-5-1-2 端末間 ping のログ Monitoring Device（業界共用）

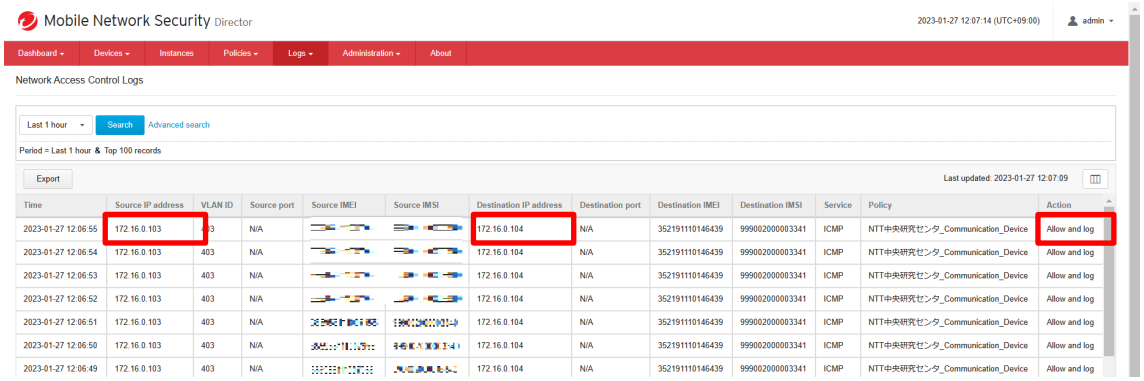


図 5-5-4-5-1-3 端末間 ping のログ Communication Device（業界共用）

・端末不正利用防止

本項目では悪意を持った攻撃者が正規の端末から SIM を抜き取り、他の端末に接続してローカル５Ｇシステムを悪用する攻撃(SIM スワッピング)に対するセキュリティ機能を検証します。この攻撃は端末種別に限らず SIM スワッピングが検知された時点で通信を禁止することが有効だと考えられます。正規端末から抜き取った SIM を攻撃者自身の端末(システム未登録)に差し替えた場合の可視化画面の様子およびログを「図 5-5-4-5-1-4～図 5-5-4-5-1-9」に示します。また、別の正規端末(システム登録済)に差し替えた場合の様子およびログを「図 5-5-4-5-1-10～図 5-5-4-5-1-15」に示します。いずれの場合も SIM スワッピングが検知でき、端末が通信不可になっていることが確認できます。

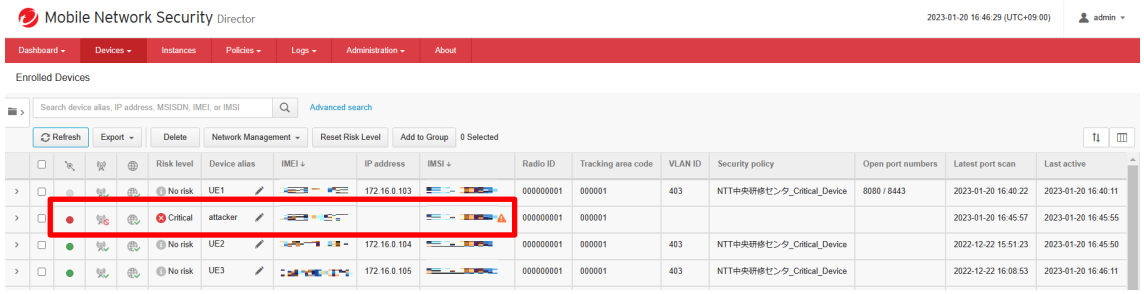


図 5-5-4-5-1-4 UE1→攻撃者端末 SIM スワッピング時の遮断の様子
（Critical Device / 業界共用）

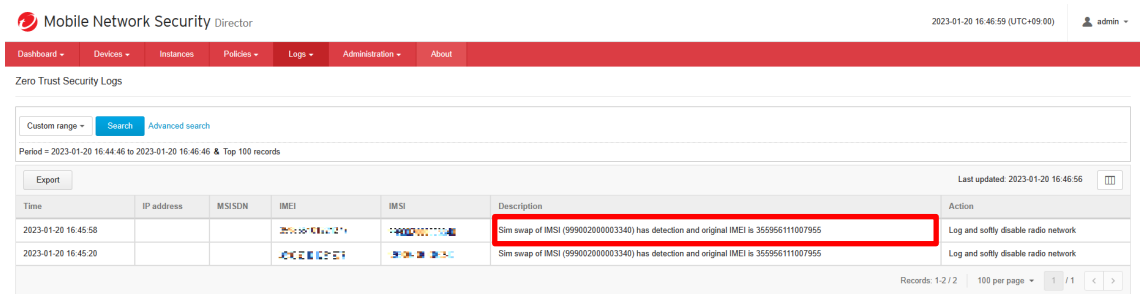


図 5-5-4-5-1-5 UE1→攻撃者端末 SIM スワッピングログ（Critical Device / 業界共用）

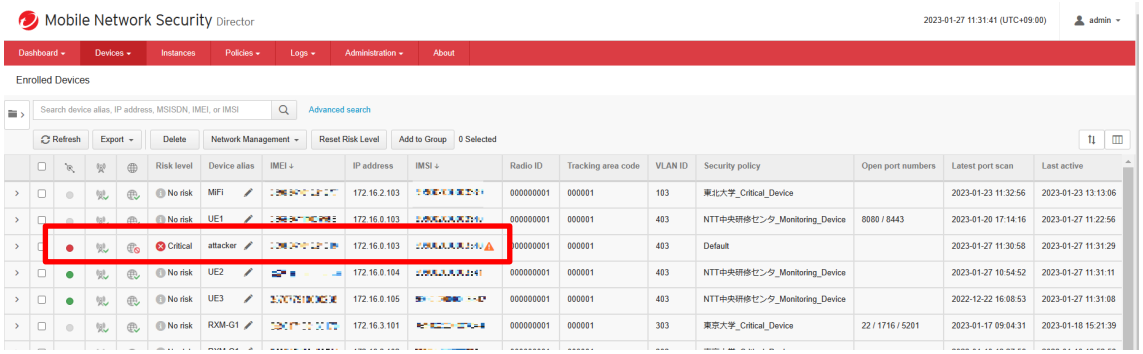


図 5-5-4-5-1-6 UE1→攻撃者端末 SIM スワッピング時の遮断の様子
(Monitoring Device / 業界共用)

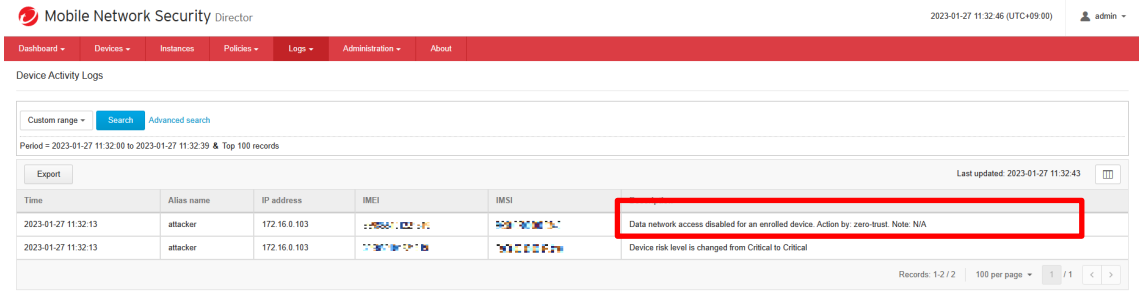


図 5-5-4-5-1-7 UE1→攻撃者端末 SIM スワッピングログ(Monitoring Device/業界共用)

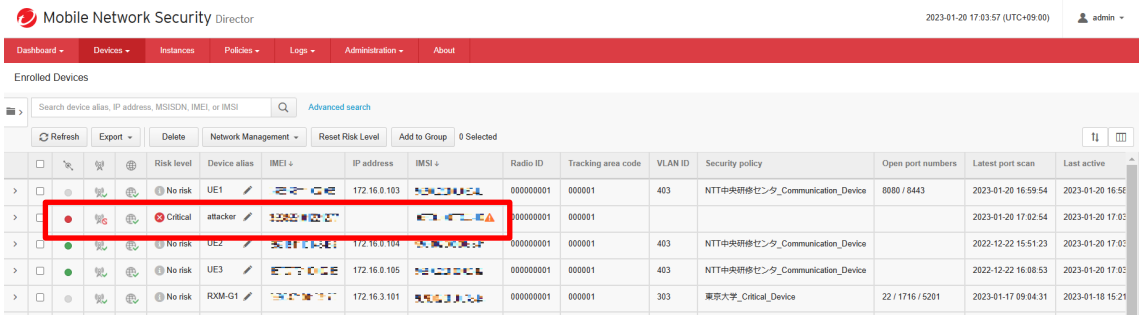


図 5-5-4-5-1-8 UE1→攻撃者端末 SIM スワッピング時の遮断の様子
(Communication Device/業界共用)

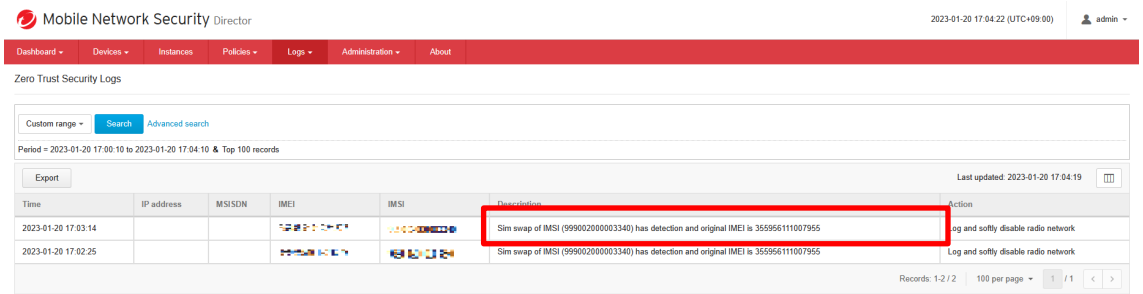


図 5-5-4-5-1-9 UE1→攻撃者端末 SIM スワッピングログ
(Communication Device/業界共用)

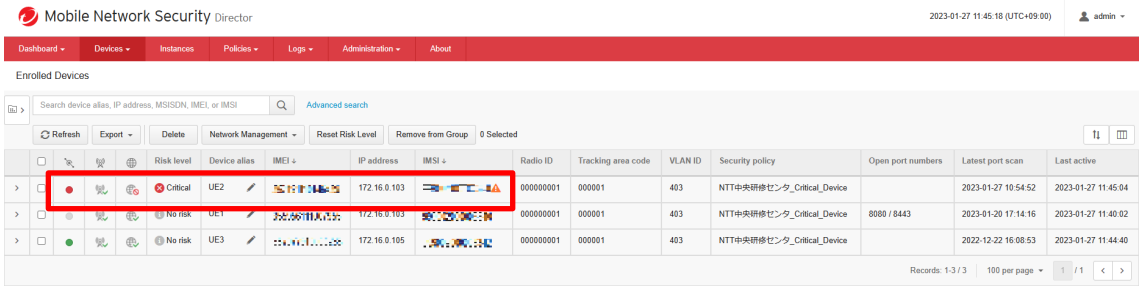


図 5-5-4-5-1-10 UE1→UE2 SIM スワッピング時の遮断の様子
(Critical Device / 業界共用)

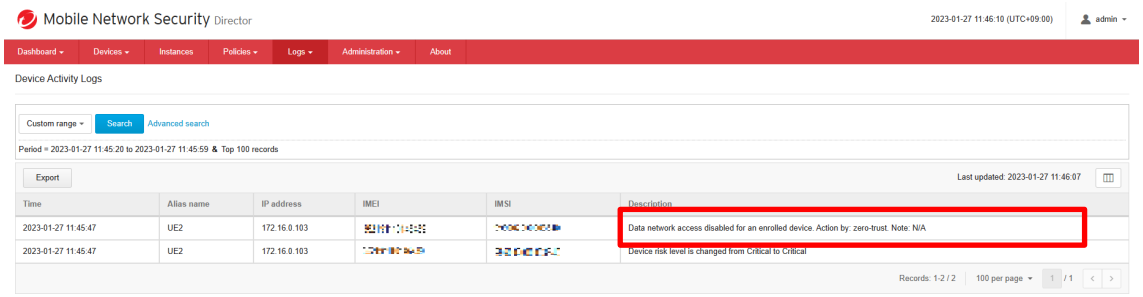


図 5-5-4-5-1-11 UE1→UE2 SIM スワッピングログ(Critical Device / 業界共用)

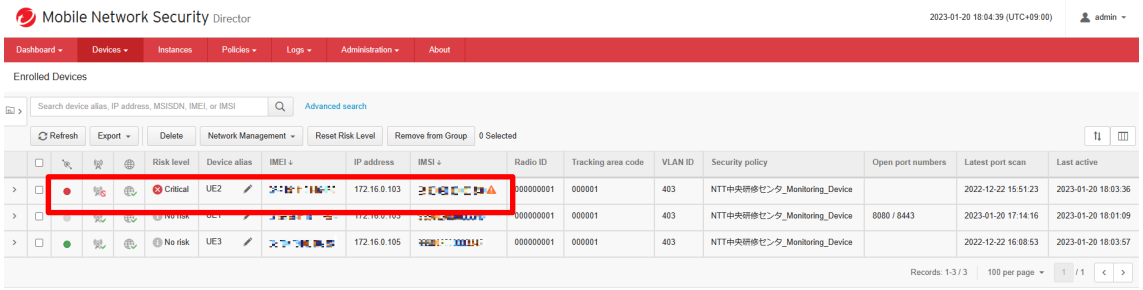


図 5-5-4-5-1-12 UE1→UE2 SIM スワッピング時の遮断の様子
(Monitoring Device / 業界共用)

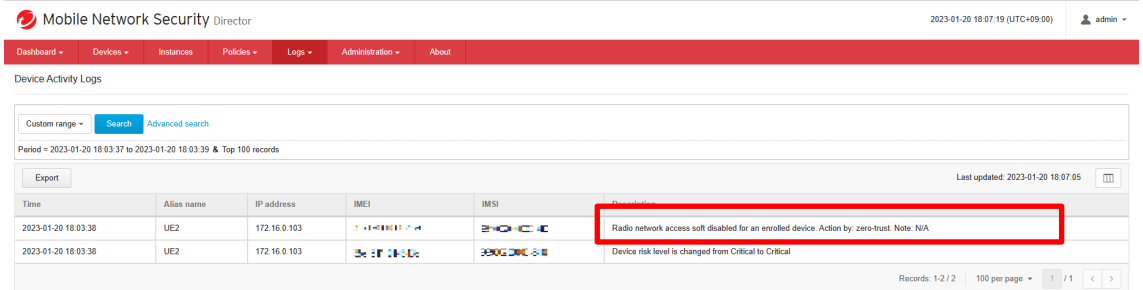


図 5-5-4-5-1-13 UE1→UE2 SIM スワッピングログ(Monitoing Device / 業界共用)

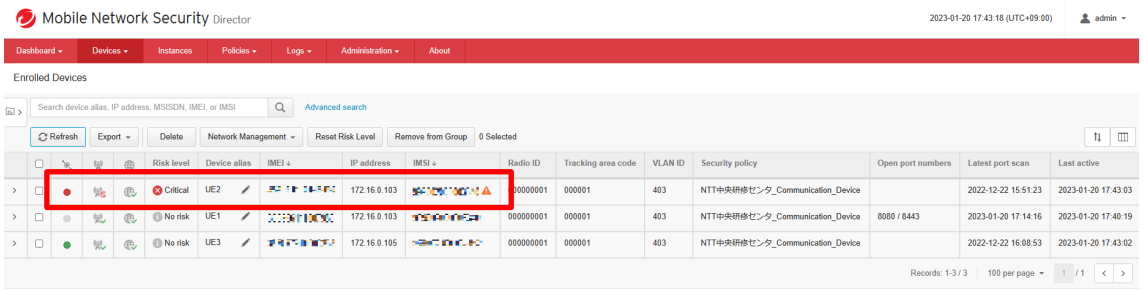


図 5-5-4-5-1-14 UE1→UE2 SIM スワッピング時の遮断の様子
(Communication Device / 業界共用)

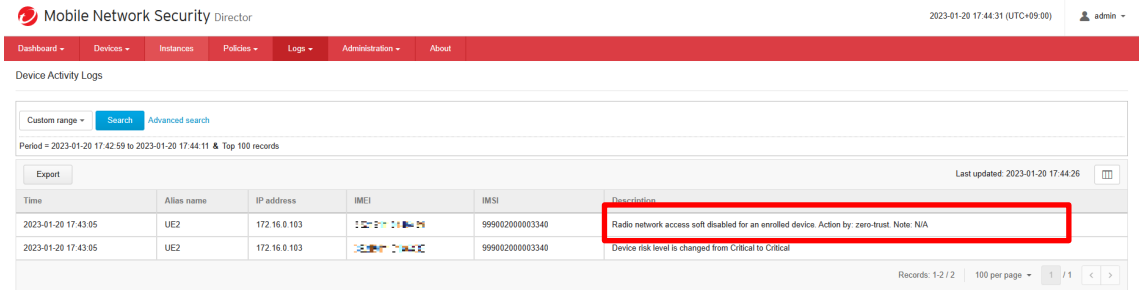


図 5-5-4-5-1-15 UE1→UE2 SIM スワッピングログ(Communication Device/業界共用)

スワッピング後の SIM を正規の組み合わせで元の端末に戻した場合の様子を「図 5-5-4-5-1-16～図 5-5-4-5-1-18」に示します。いずれの場合も正規の組み合わせであれば元通りオンラインになることが確認できました。

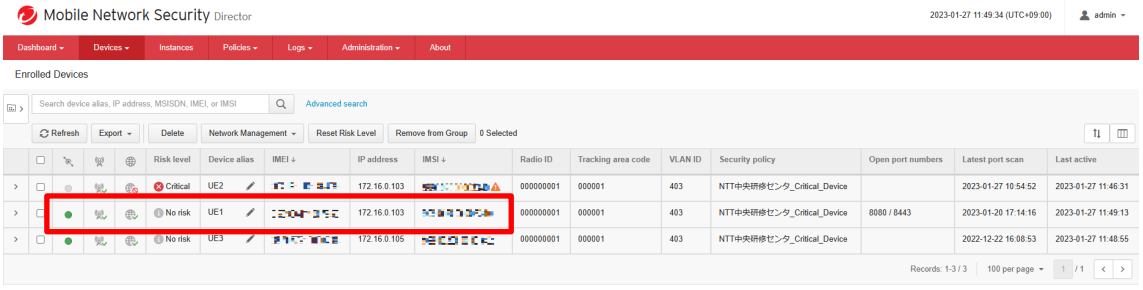


図 5-5-4-5-1-16 UE1→UE2→UE1 元の端末へ戻した様子(Critical Device/業界共用)

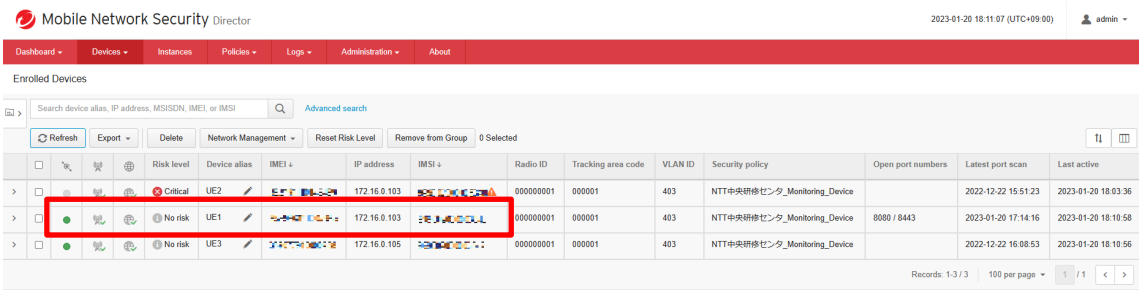


図 5-5-4-5-1-17 UE1→UE2→UE1 元の端末へ戻した様子(Monitoring Device/業界共用)

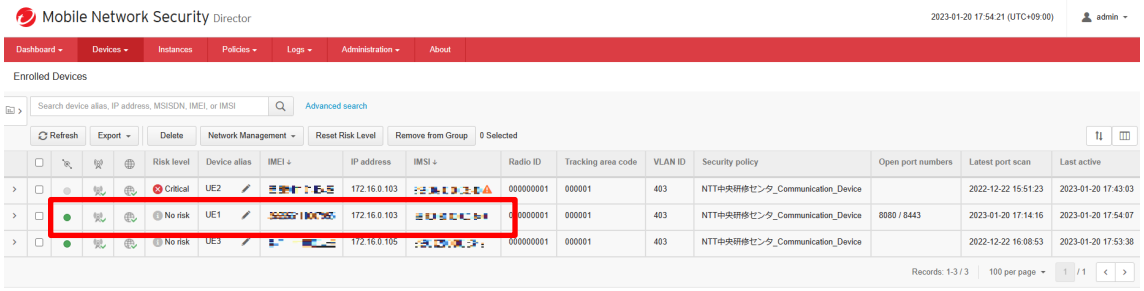


図 5-5-4-5-1-18 UE1→UE2→UE1 元の端末へ戻した様子(Communication Device/業界共用)

・内部拡散防止

本項目では攻撃者により正規の端末が乗っ取られるあるいは踏み台にされる等、正規端末から不正な通信を行う攻撃が行われた場合のセキュリティ機能について検証します。web サーバに保存されたパスワードを盗み見るディレクトリトラバーサル攻撃を想定し、/etc/passwd を含む http リクエストを検証用の疑似不正通信として使用しました。

端末からの不正通信に対するポリシーについては「表 5-5-3-3」に示すとおりです。Critical Device は即時対応をすると人命や可用性にかかわる可能性があるため不正通信発生時には検知のみを行い、その後手動でネットワークからの遮断を行うか判断します。Monitoring Device と Communication Device は即時ネットワークからの遮断を行います。「図 5-5-4-5-1-19～5-5-4-5-1-23」に Critical Device の場合の検知から手動のオペレーションの様子を、「図 5-5-4-5-1-24～図 5-5-4-5-1-27」に Monitoring Device と Communication Device の自動遮断の様子を示します。

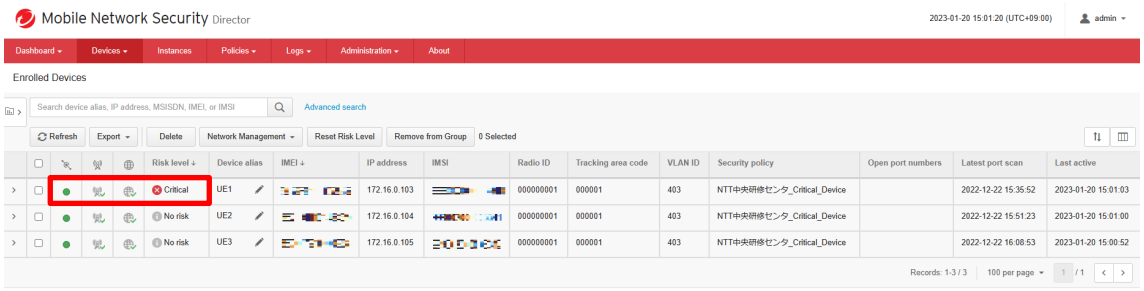


図 5-5-4-5-1-19 UE1 から不正通信発生時 (Critical Device / 業界共用)

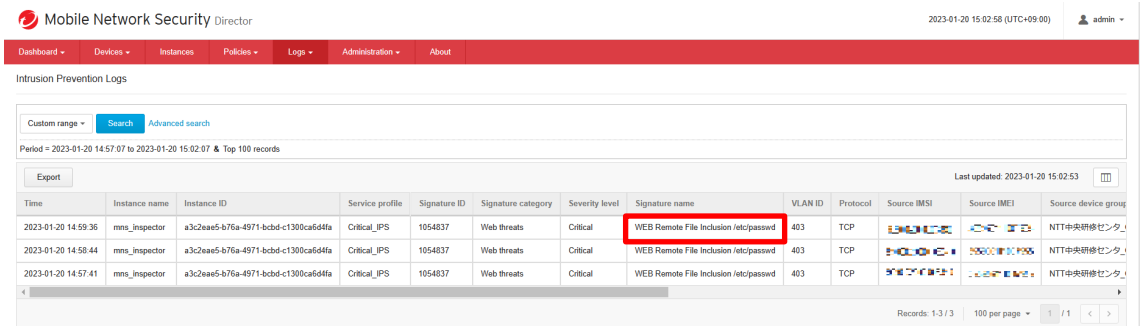


図 5-5-4-5-1-20 不正通信検知時のログ（Critical Device / 業界共用）

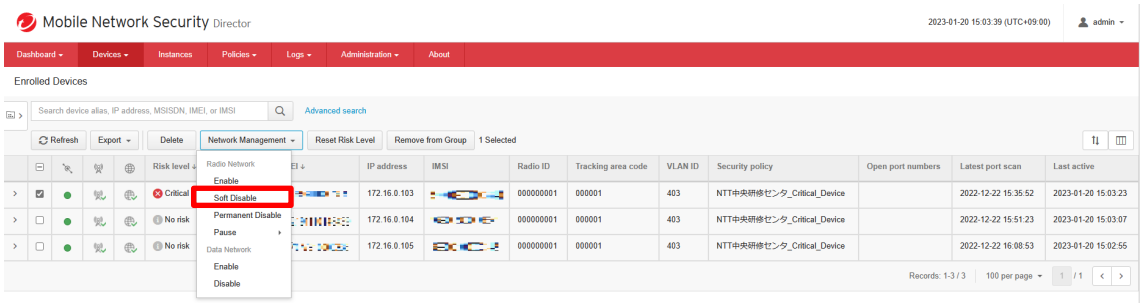


図 5-5-4-5-1-21 UE1 を手動でネットワークから遮断するオペレーション

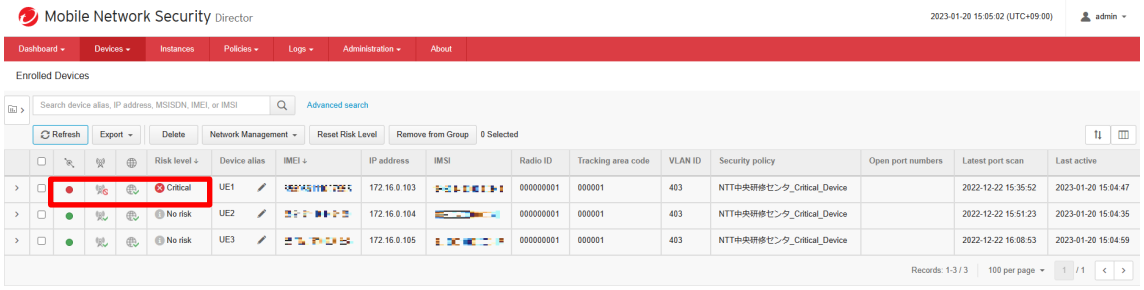


図 5-5-4-5-1-22 UE1 が手動でネットワークから遮断された様子

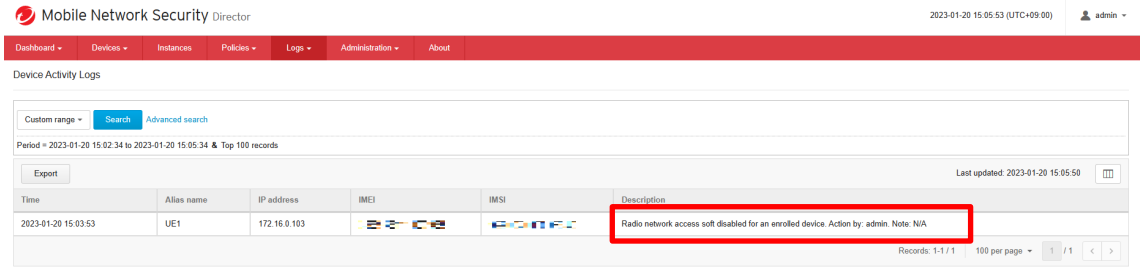


図 5-5-4-5-1-23 UE1 を手動でネットワークから遮断したことのシステムログ

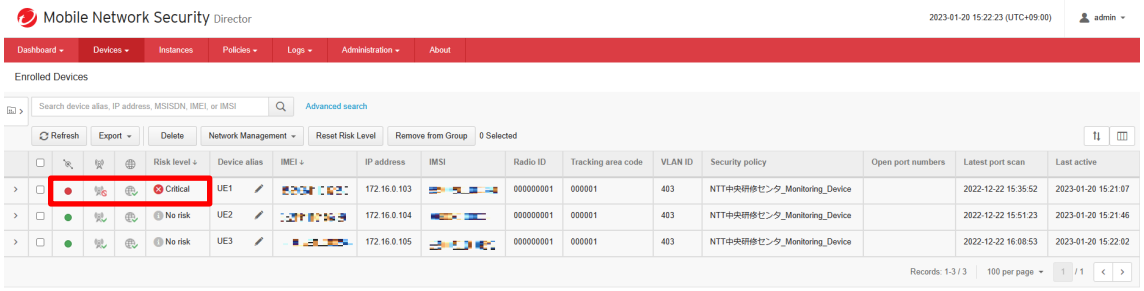


図 5-5-4-5-1-24 UE1 から不正通信発生時の遮断の様子（Monitoring Device / 業界共用）

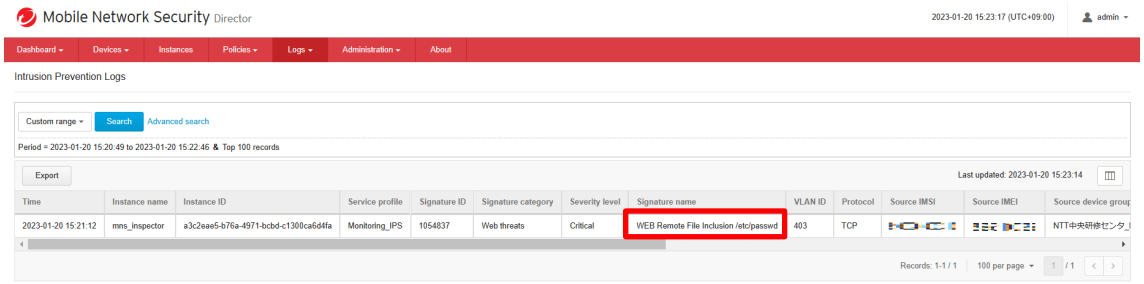


図 5-5-4-5-1-25 不正通信検知時のログ（Monitoring Device / 業界共用）

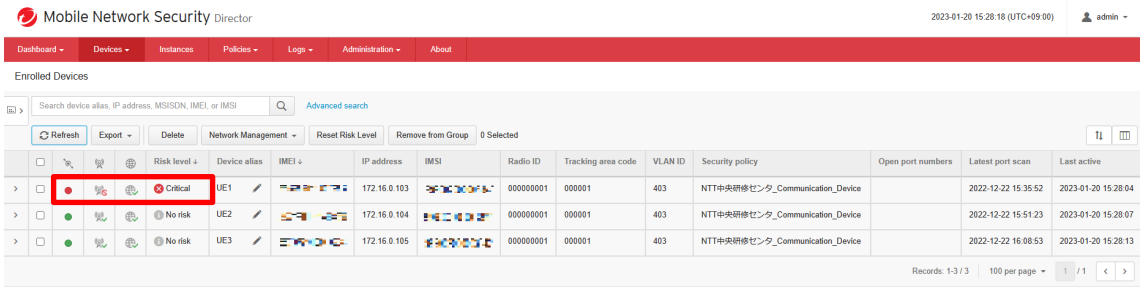


図 5-5-4-5-1-26 UE1 から不正通信発生時の遮断の様子
（Communication Device / 業界共用）

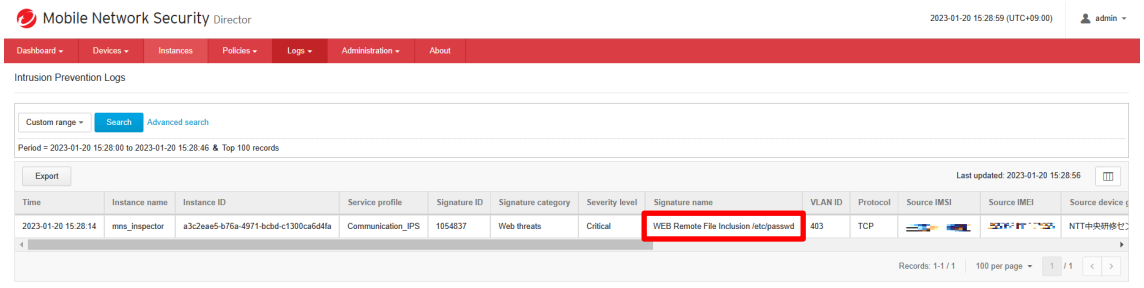


図 5-5-4-5-1-27 不正通信検知時のログ（Communication Device / 業界共用）

また、「図 5-5-4-5-1-1～図 5-5-4-5-1-27」の検証について、エンド UPF に監視装置を設置した場合も同様の結果が得られました。結果の見え方についてはセンタ UPF の構成と同様のため割愛いたします。

イ　NTT 中央研修センタ 複数企業共用パターン

・アクセス制御

本項目ではセキュリティ機能付き SIM を使用した端末がアクセスできるネットワークを制限できることを端末間の通信を用いて検証します。端末間の通信に関するセキュリティポリシーは「表 5-5-3-3」に示すとおりです。Monitoring Device はカメラや相互連携しないセンサであり、端末間の通信が不要であることが想定されます。本検証ではセキュリティ機能により Monitoring Device のみが互いに通信不可となっていることを確認しました。「図 5-5-4-5-1-1～図 5-5-4-5-1-3」にそれぞれ Critical Device / Monitoring Device / Communication Device に設定した端末間で ping を送付した際のログを示します。（送信元 IP 172.16.0.103 から送信先 IP 172.16.0.104 への ping） Action の列から Monitoring Device のみ Block していることが確認できました。

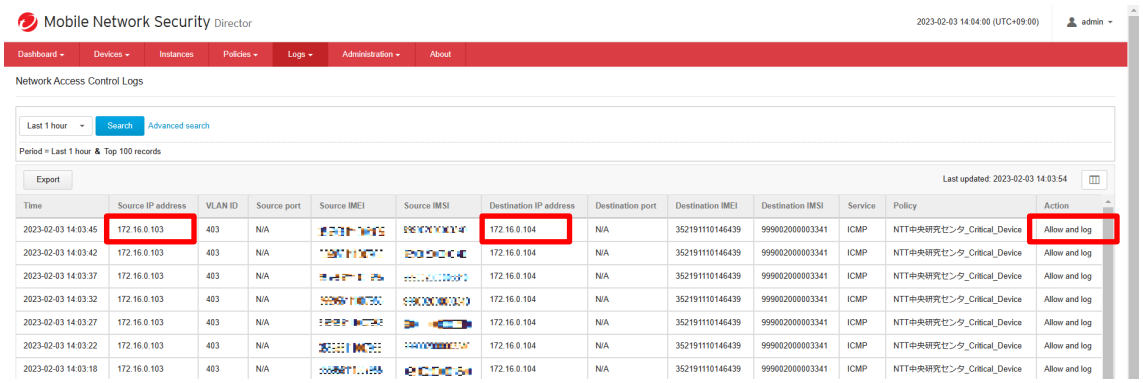


図 5-5-4-5-2-1 端末間 ping のログ Critical Device（複数企業共用）

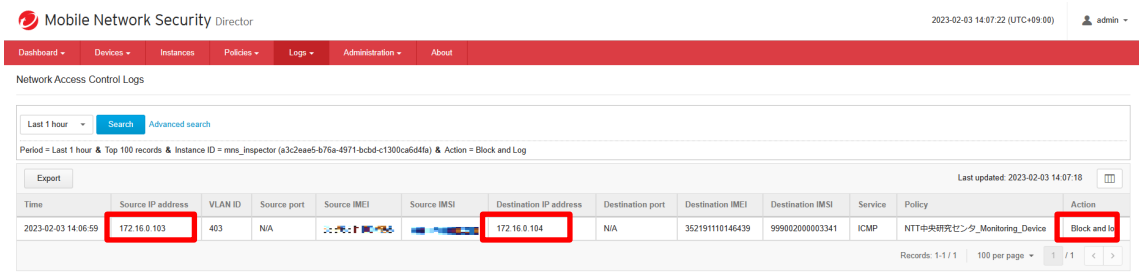


図 5-5-4-5-2-2 端末間 ping のログ Monitoring Device（複数企業共用）

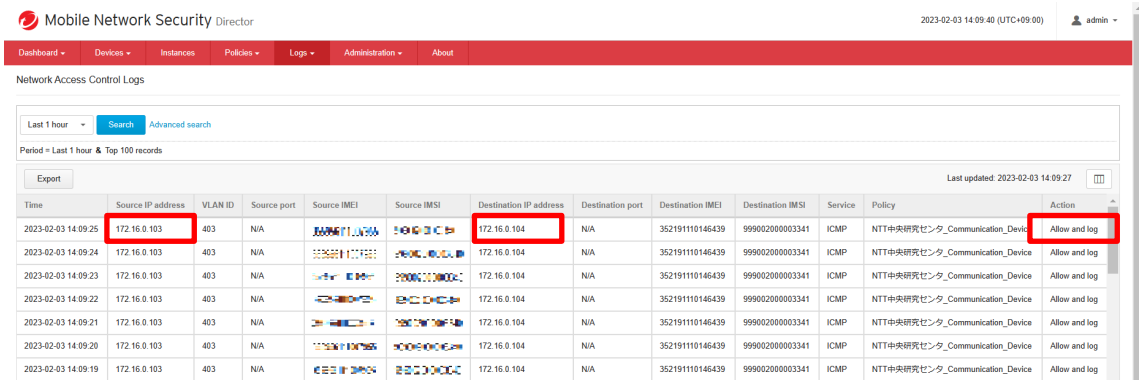


図 5-5-4-5-2-3 端末間 ping のログ Communication Device（複数企業共用）

・端末不正利用防止

本項目では悪意を持った攻撃者が正規の端末から SIM を抜き取り、他の端末に接続してローカル５Ｇシステムを悪用する攻撃(SIM スワッピング)に対するセキュリティ機能を検証します。この攻撃は端末種別に限らず SIM スワッピングが検知された時点で通信を禁止することが有効だと考えられます。正規端末から抜き取った SIM を攻撃者自身の端末(システム未登録)に差し替えた場合の可視化画面の様子およびログを「図 5-5-4-5-2-4～図 5-5-4-5-2-9」に示します。また、別の正規端末(システム登録済)に差し替えた場合の様子およびログを「図 5-5-4-5-2-10～図 5-5-4-5-2-15」に示します。いずれの場合も SIM スワッピングが検知でき、端末が通信不可になっていることが確認できます。

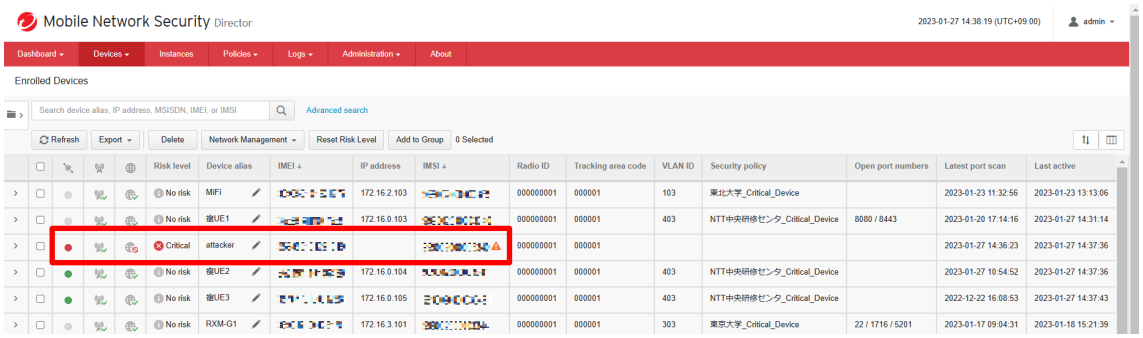


図 5-5-4-5-2-4 複 UE1→攻撃者端末 SIM スワッピング時の遮断の様子
（Critical Device / 複数企業共用）

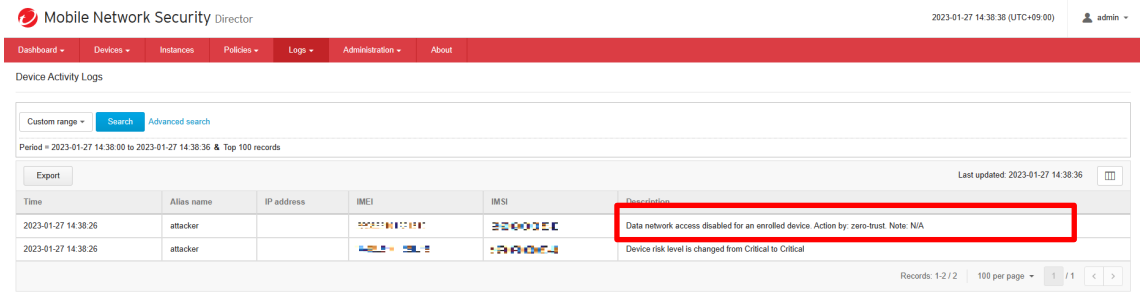


図 5-5-4-5-2-5 複 UE1→攻撃者端末 SIM スワッピングログ
（Critical Device / 複数企業共用）

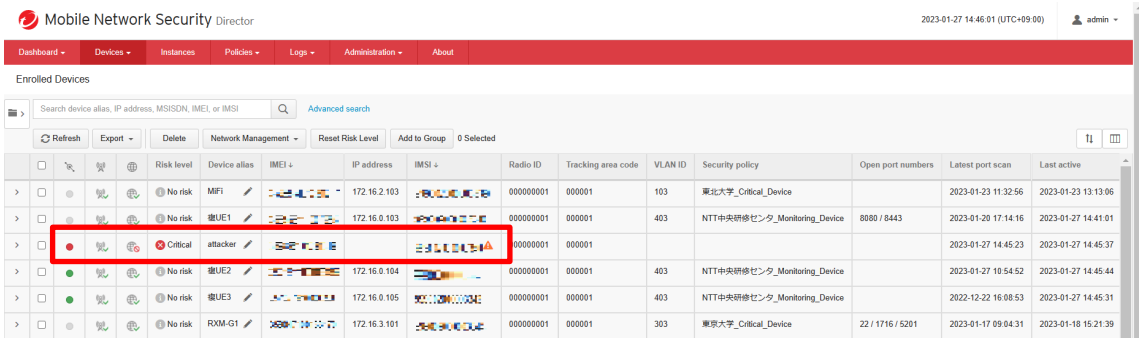


図 5-5-4-5-2-6 複 UE1→攻撃者端末 SIM スワッピング時の遮断の様子
(Monitoring Device / 複数企業共用)

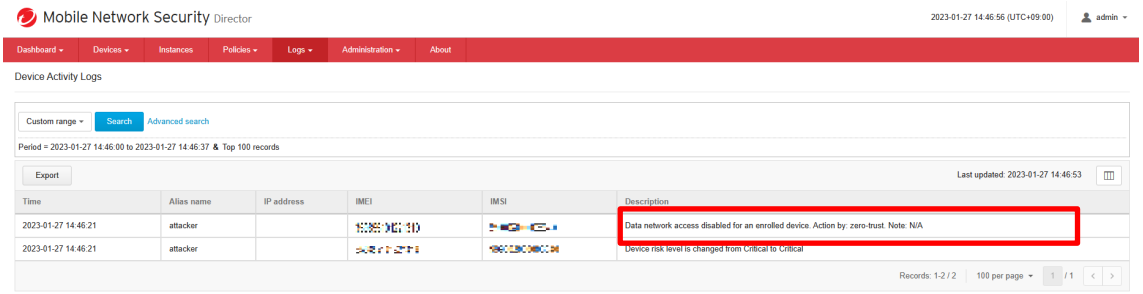


図 5-5-4-5-2-7 複 UE1→攻撃者端末 SIM スワッピングログ
(Monitoring Device / 複数企業共用)

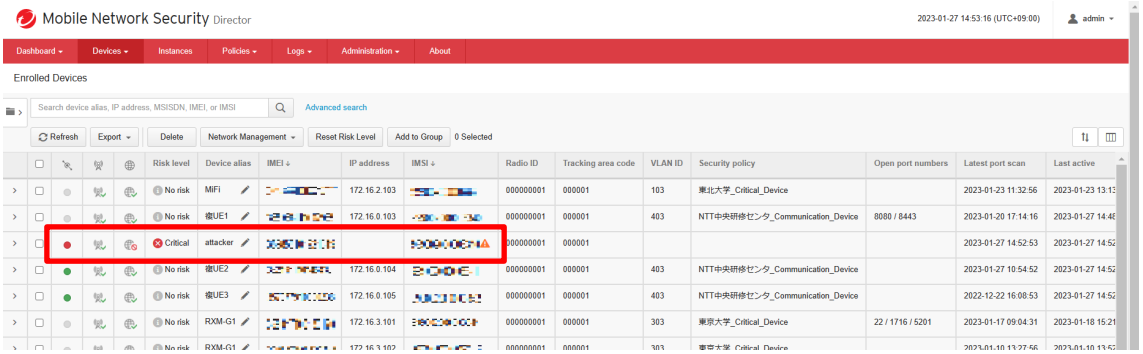


図 5-5-4-5-2-8 複 UE1→攻撃者端末 SIM スワッピング時の遮断の様子
(Communication Device/複数企業共用)

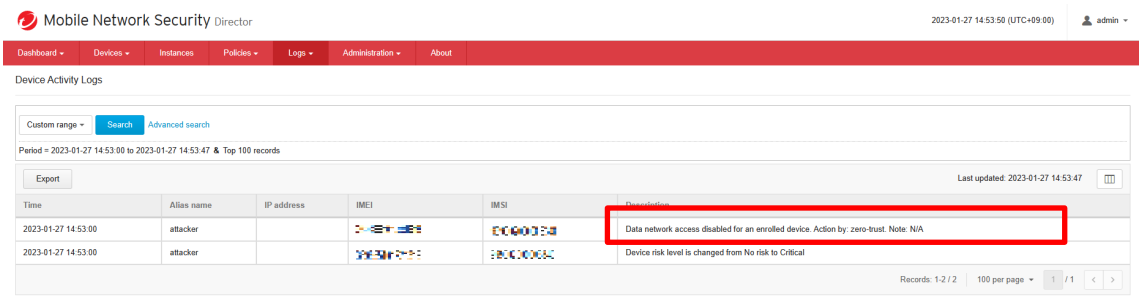


図 5-5-4-5-2-9 複 UE1→攻撃者端末 SIM スワッピングログ
(Communication Device/複数企業共用)

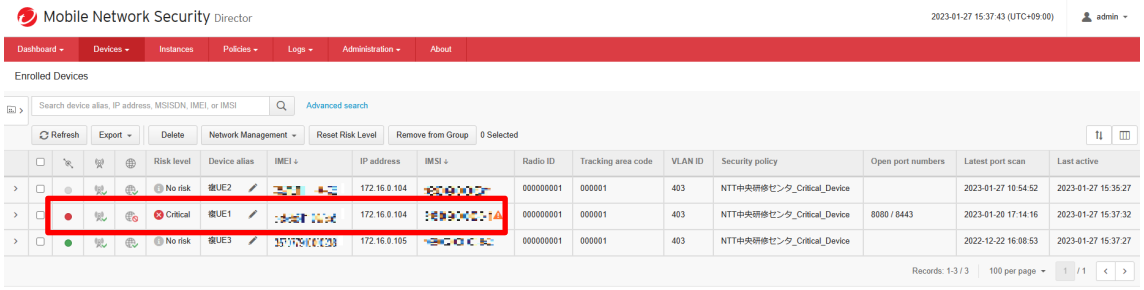


図 5-5-4-5-2-10 複 UE2→複 UE1 SIM スワッピング時の遮断の様子
(Critical Device / 複数企業共用)

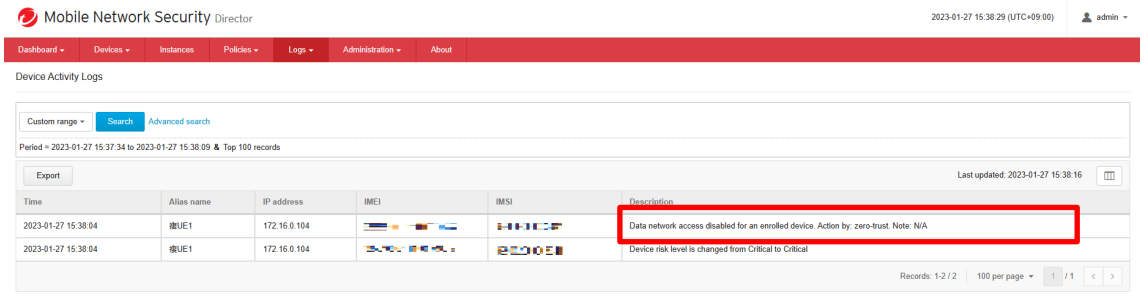


図 5-5-4-5-2-11 複 UE2→複 UE1 SIM スワッピングログ
(Critical Device / 複数企業共用)

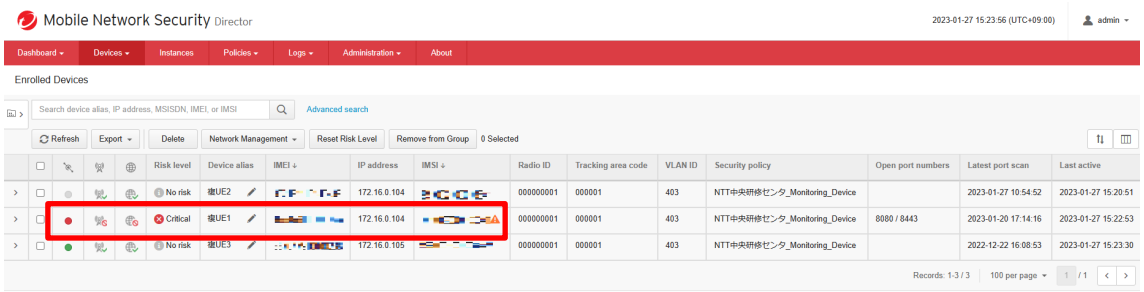


図 5-5-4-5-2-12 複 UE2→複 UE1 SIM スワッピング時の遮断の様子
(Monitoring Device / 複数企業共用)

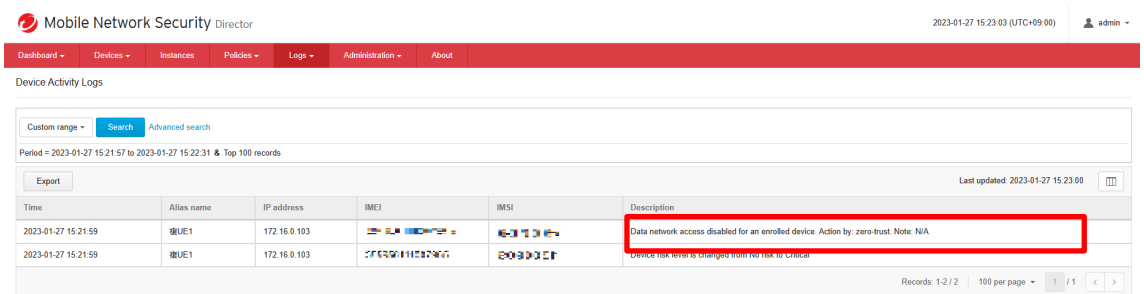


図 5-5-4-5-2-13 複 UE2→複 UE1 SIM スワッピングログ
(Monitoing Device / 複数企業共用)

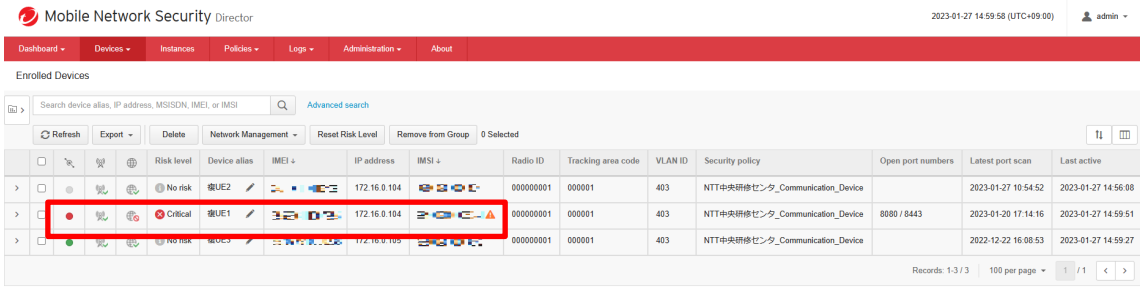


図 5-5-4-5-2-14 複 UE2→複 UE1 SIM スワッピング時の遮断の様子
(Communication Device / 複数企業共用)

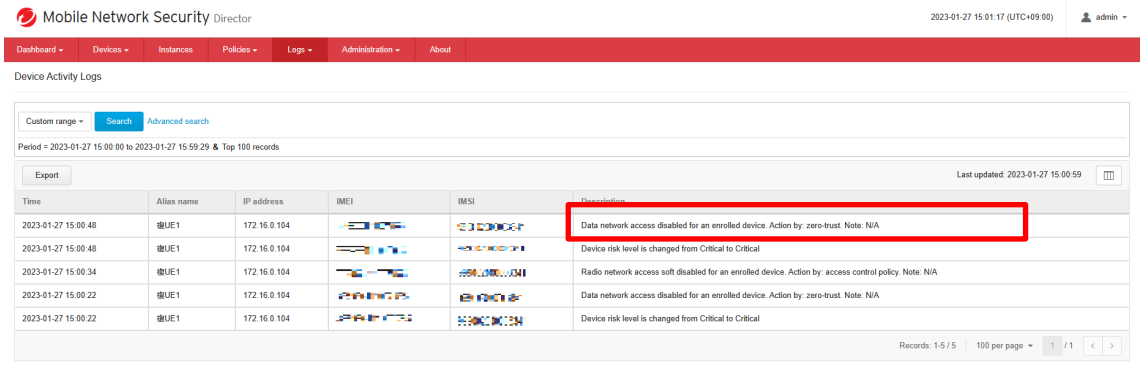


図 5-5-4-5-2-15 複 UE2→複 UE1 SIM スワッピングログ
(Communication Device / 複数企業共用)

スワッピング後の SIM を正規の組み合わせで元の端末に戻した場合の様子を「図 5-5-4-5-2-16～図 5-5-4-5-2-18」に示します。いずれの場合も正規の組み合わせであれば元通りオンラインになることが確認できました。

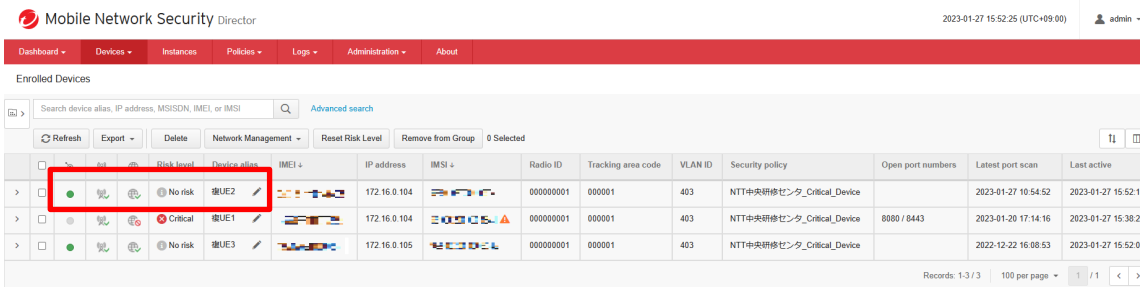


図 5-5-4-5-2-16 複 UE2→複 UE1→複 UE2 元の端末へ戻した様子
(Critical Device/ 複数企業共用)

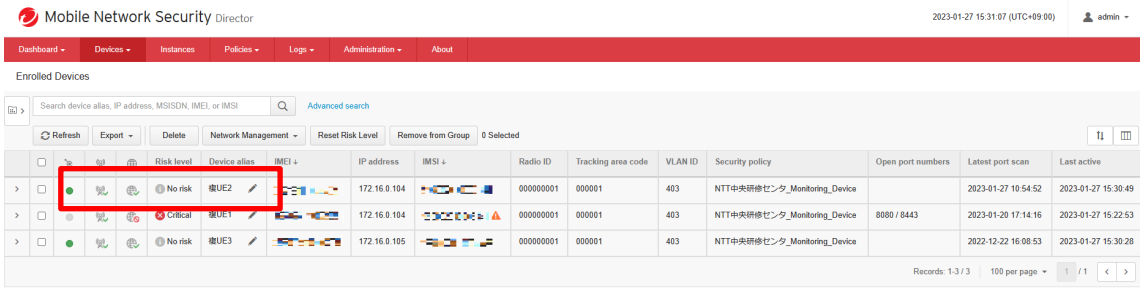


図 5-5-4-5-2-17 複 UE2→複 UE1→複 UE2 元の端末へ戻した様子
(Monitoring Device/ 複数企業共用)

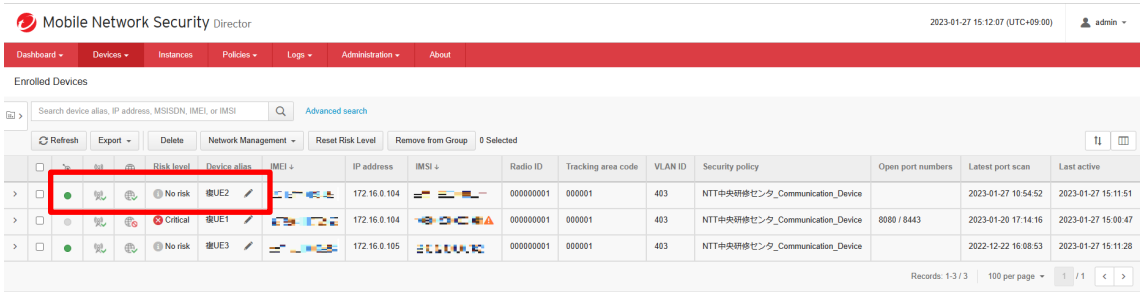


図 5-5-4-5-2-18 複 UE2→複 UE1→複 UE2 元の端末へ戻した様子
(Communication Device/ 複数企業共用)

・内部拡散防止

本項目では攻撃者により正規の端末が乗っ取られるあるいは踏み台にされる等、正規端末から不正な通信を行う攻撃が行われた場合のセキュリティ機能について検証します。web サーバに保存されたパスワードを盗み見るディレクトリトラバーサル攻撃を想定し、/etc/passwd を含む http リクエストを検証用の疑似不正通信として使用しました。

端末からの不正通信に対するポリシーについては「表 5-5-3-3」に示すとおりです。Critical Device は即時対応をすると人命や可用性にかかわる可能性があるため不正通信発生時には検知のみを行い、その後手動でネットワークからの遮断を行うか判断します。Monitoring Device と Communication Device は即時ネットワークからの遮断を行います。「図 5-5-4-5-2-19～5-5-4-5-2-23」に Critical Device の場合の検知から手動のオペレーションの様子を、「図 5-5-4-5-2-24～図 5-5-4-5-2-27」に Monitoring Device と Communication Device の自動遮断の様子を示します。

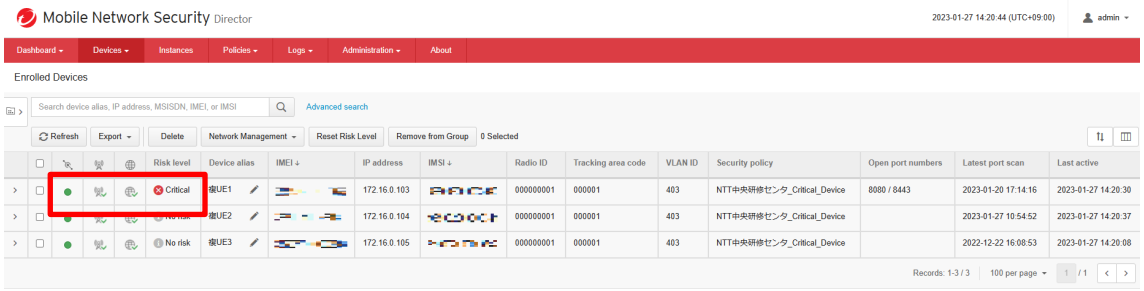


図 5-5-4-5-2-19 複 UE1 から不正通信発生時（Critical Device / 複数企業共用）

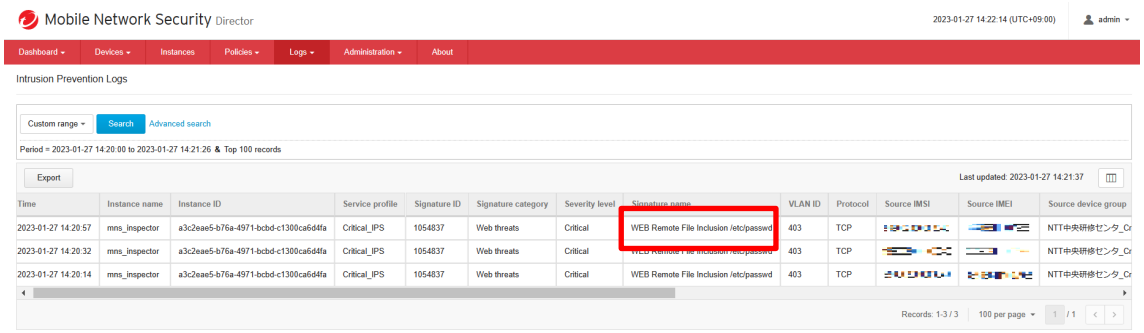


図 5-5-4-5-2-20 不正通信検知時のログ（Critical Device / 複数企業共用）

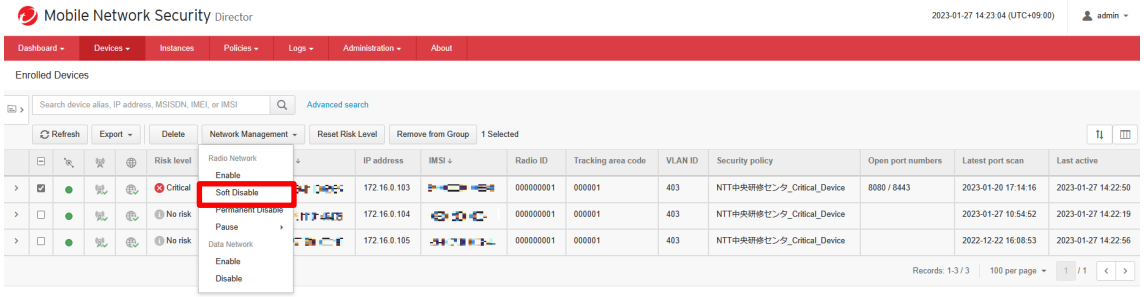


図 5-5-4-5-2-21 複 UE1 を手動でネットワークから遮断するオペレーション

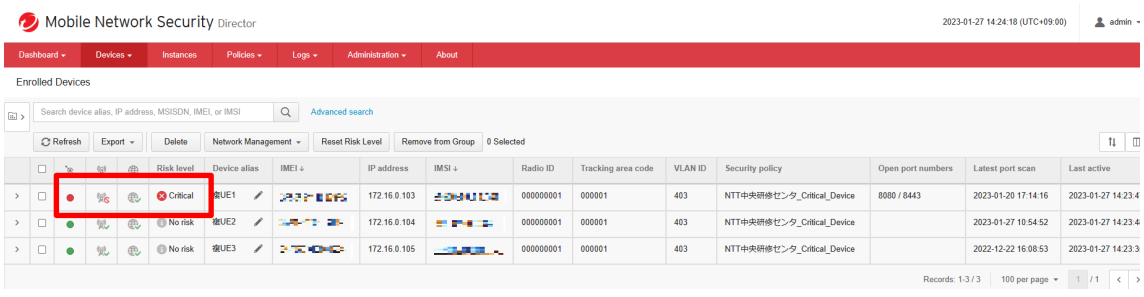


図 5-5-4-5-2-22 複 UE1 が手動でネットワークから遮断された様子

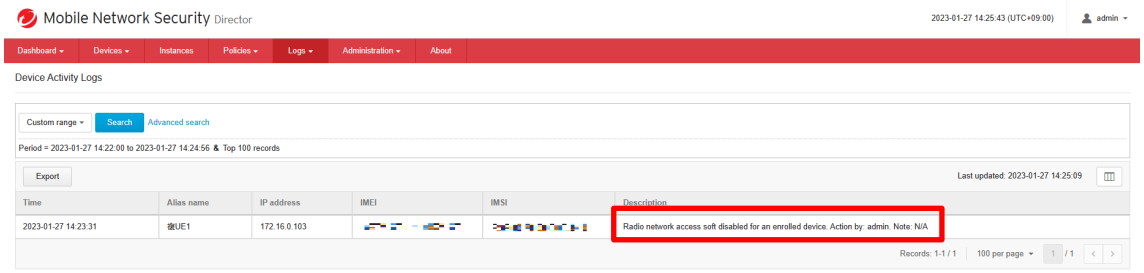


図 5-5-4-5-2-23 複 UE1 を手動でネットワークから遮断したことのシステムログ

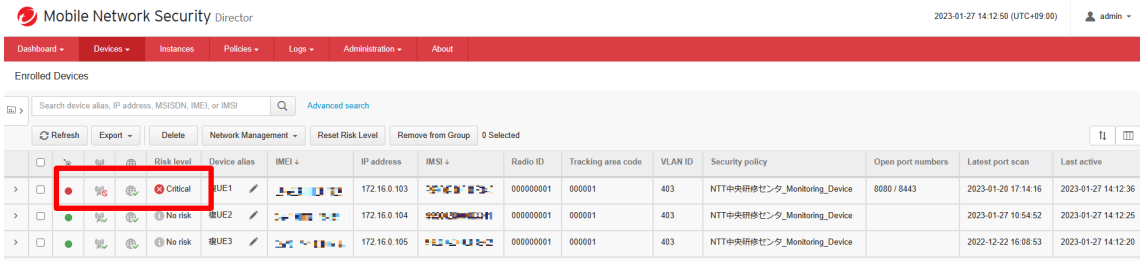


図 5-5-4-5-2-24 複 UE1 から不正通信発生時の遮断の様子
（Monitoring Device / 複数企業共用）

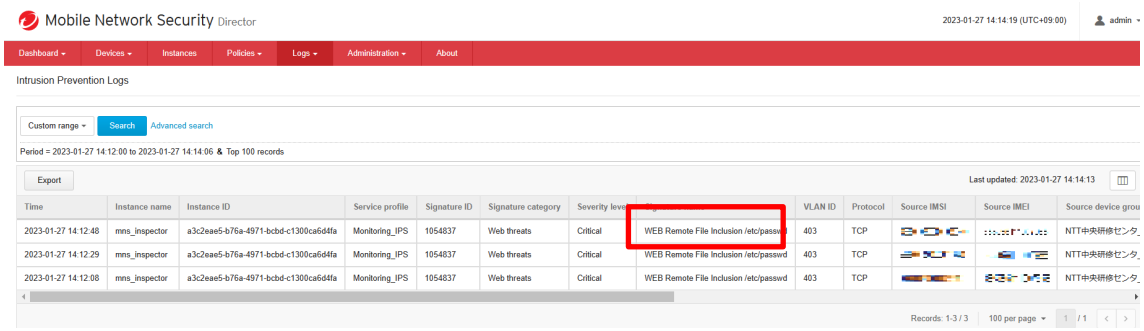


図 5-5-4-5-2-25 不正通信検知時のログ（Monitoring Device / 複数企業共用）

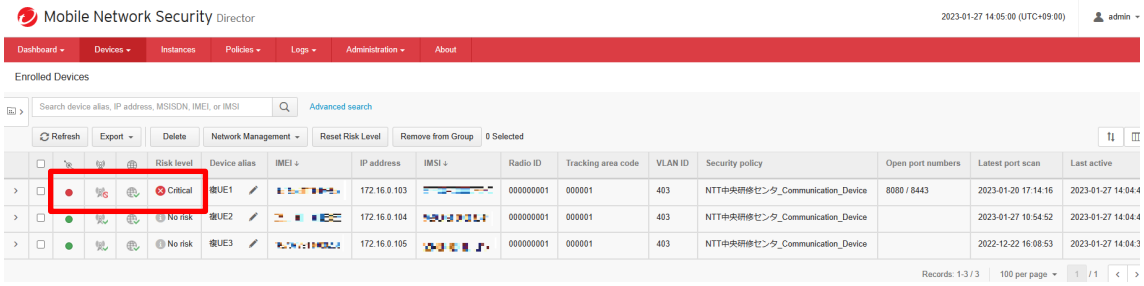


図 5-5-4-5-2-26 複 UE1 から不正通信発生時の遮断の様子
（Communication Device / 複数企業共用）

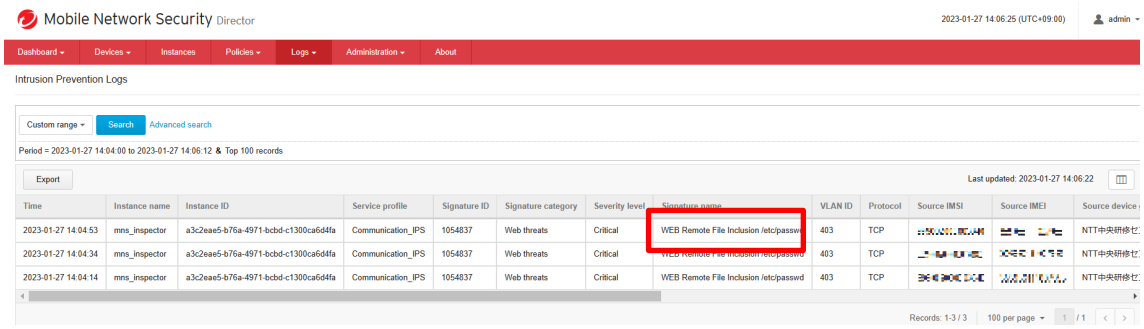


図 5-5-4-5-2-27 不正通信検知時のログ（Communication Device / 複数企業共用）

また、「図 5-5-4-5-2-1～図 5-5-4-5-2-27」の検証について、エンド UPF に監視装置を設置した場合も同様の結果が得られました。結果の見え方についてはセンタ UPF の構成と同様のため割愛いたします。

(5) 結果考察

以下の内容にて考察する想定。

■CU-DU 区間暗号化

(拠点間通信の暗号化方式について)

本調査研究においてユーザ拠点とコア拠点をつなぐ VPN には、業界共用パターンで L2VPN、複数企業共用パターンで閉域 VPN を採用したため盗聴の危険は極めて低いものでした。しかしインターネット VPN 等盗聴の危険のある VPN による共用形態を考えると、盗聴された際の対策として暗号化を考慮する必要があります。

CU を共用し CU-DU 区間が分離することにより WAN 区間を流れる通信は F1-C(C-Plane)と F1-U(U-Plane)の 2 種類があるため、それぞれについて暗号化の必要性について考察します。まず、F1-C はユーザの認証情報等の重要情報を含む通信であり、その通信は SCTP を用いた平文で行われるため、拠点間通信時には暗号化を施すことが有効です。次に、F1-U は無線区間で PDCP を用いてすでに暗号化されたパケットが送信されるため、拠点間通信時に改めての暗号化は不要と考えます。

本調査研究の結果からそれら拠点間通信の暗号化に IPsec を用いることが有効であると考えます。

(IPsec の鍵交換方式について)

IPsec は Phase 1 と Phase 2 に分かれます。Phase 1 で暗号化に使う鍵を交換し、Phase 2 で Phase 1 で交換した鍵を用いて実際の暗号化通信を行うための VPN を構築します。本調査研究では Phase 1 の鍵交換について、DH 方式と量子暗号鍵交換方式の二種類の方式を検証しました。上記の F1-C や F1-U の通信は Phase 2 で行われるため、ローカル５Ｇシステムに必要なそれらの通信において、遅延や IPsec の強固性に DH 方式と量子暗号鍵交換方式の間に差分はないことが確認できました。本調査研究の結果から、コア共用の構成における拠点間の暗号化には DH 方式および量子暗号鍵交換方式がいずれも使用可能であると言えます。

DH 方式および量子暗号鍵交換方式の違いについて、量子暗号鍵交換方式は Phase 1 の鍵交換の際に CU-DU 区間で盗聴された場合でも量子(光子)レベルでそれを検知することがで

きるため、鍵をすぐさま変更することが可能であり、DH 方式のように盗聴されて量子コンピューティングで解読される心配はありません。金融業や OT 機器の使用等の従来の IPsec よりもさらに厳重なセキュリティを求める場合に、量子暗号鍵交換方式の採用が有効であると考えます。

また、今回の調査研究においては ETSI 標準 API を使用して量子暗号鍵の受け渡しの確認を行いました。将来的なマルチベンダー化を考慮した際には、ベンダー独自の実装ではなく ETSI 標準 API を使用することが望ましいと考えます。

■セキュリティ機能付き SIM

（端末セキュリティの背景）

多目的かつ多種類の端末が接続されるローカル５Ｇシステムにおいて、端末からの不正な通信を適切に防ぎ、システムの可用性と機密性を守ることは重要です。また、コア共用構成のように複数のテナントが同じローカル５Ｇシステムに接続する環境の運用にあたっては、テナント毎に求められる適切なポリシーが設定できること、およびテナント毎の端末の可視化・管理機能を有することが効果的と考えます。本調査研究においては端末を SIM 単位で管理し、不正な通信を監視装置で検知し遮断できること、また必要に応じて端末からローカル５Ｇシステムへの接続を拒否できることを確認しました。

（端末の分類と各セキュリティポリシーについて）

本調査研究の結果を以て、ローカル５Ｇシステムに接続する端末の種類を以下の三つに分けて、それぞれ異なるセキュリティポリシーで運用することを提唱します。

- Critical Device（P2P 通信あり / 不正通信の検知はするが自動での隔離はしない）
- Monitoring Device（P2P 通信なし / 不正通信を検知次第自動隔離する）
- Communication Device（P2P 通信あり / 不正通信を検知次第自動隔離する）

Critical Device は医療機器や OT 機器のように、不正通信時に即座にローカル５Ｇから隔離してしまうと人命や可用性に大きな影響を及ぼす端末と定義します。これらの端末から不正通信が発生した際には前述の理由から検知にとどめ、即時の隔離は行わないことが求められます。実際の運用にあたっては、検知を確認したあと不正通信の内容をログで確認し、必要に応じて手動で隔離を行えるシステムが望ましいと考えます。またその際には手動で隔離したこともログに残ることが運用上有効であると考えます。

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

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

これらの端末分類を採用するため、SIM ごとに端末を分類し、その端末分類毎に異なるセキュリティポリシーを適用できるシステムが有効と考えます。また、コアを共用するシステムにおいては、テナント毎に必要とする端末の分類が異なる場合や、さらに細かな設

定が求められる場合が想定されるため、テナント毎にも異なるセキュリティポリシーを適用できることが望ましいと考えます。

（端末からの不正な通信について）

端末からの攻撃として考えられる不正な通信の種類について考察します。

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

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

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

最後に、上記のような端末からの不正な通信の監視においては、コアのみを共用する場合、コアと CU の両方を共用する場合の両方ともに CU-UPF 間の通信を監視し、端末からのすべての通信を監視することが効果的と言えます。このとき、エンド UPF からユーザ通信が行われ、その通信も監視する場合には、エンド拠点にも監視装置を入れることが必要となります。

（端末通信の可視化による管理稼働削減効果について）

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

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

（セキュリティ機能付き SIM の採用について）

上記のような端末分類を採用し、各種攻撃に対してのセキュリティ対策および可視化を

行うことを考える際、多種多様な特性を持ちOSにて動作している端末本体に管理エージェントのようなソフトウェアを導入することは現実的ではないため、本調査研究で採用したようなセキュリティ機能付きSIMを用いることが有効であると考えます。セキュリティ機能付きSIMを用いることで、端末の種類によらず、不正通信発見時に端末の隔離を即座に、かつ他の端末やネットワークに影響を与えず行うことが可能と考えます。

■R3・R4年度のセキュリティ検証まとめ
(セキュリティホールについて)
コアを共用する環境におけるセキュリティリスクのあると想定される箇所は、R3年度調査研究で実施した「コア-基地局間におけるネットワークファンクション間のセキュリティ」と、R4年度に実施した「CU-DU区間におけるセキュリティ」および「端末-基地局間のセキュリティ」と、インターネットの出口である「N6インターフェースに関するセキュリティ」となります。このうちN6インターフェースのセキュリティについては、コア共用環境特有のものではなく、一般のネットワークセキュリティ同様UTM等を用いてインターネットからの不正アクセス等の対策を行うことが重要であると考えます。
R3年度・R4年度に実施したセキュリティ検証について以下でまとめます。

(拠点間通信の暗号化について)
コアを共用した際のセンタ拠点のコアとエンド拠点のCU間のN2/N4の通信や、コアおよびCUを共用した際のセンタ拠点のCUとエンド拠点のDU間の通信はいずれも平文でやり取りをされるため、いずれの共用形態においても、拠点間通信はIPsecによる暗号化を行うことが望ましいと考えます。その際には、センタ拠点にて複数拠点を収容可能な製品を採用することで、トータルのコストを抑えながらセキュリティ対策が可能です。
拠点間のIPsecの鍵交換手法について、さらに厳重なセキュリティを求める場合に、量子暗号鍵交換方式の採用が有効であると考えます。この方式の採用には、拠点間に直接光ケーブルを敷設する必要がありそのコストがかかるため、全ユーザに対してではなく、金融業やOT機器の使用等の機密性や可用性を重視するユーザに採用することが望ましいと考えます。

(コアファンクションへの攻撃について)
不特定多数のユーザを収容するマルチテナントの構成を考える際、コアが乗っ取られることで他のユーザへの影響が考えられるため、いずれの共用形態においても、コアのファンクションを守るためのファイアウォール機能を具備することが望ましいと考えます。その際には、上記拠点通信の暗号化で記載した仮想アプライアンス製品について、IPsecに加えてファイアウォール機能を持つものを採用することで、同じくコストを抑えながらセキュリティを保つことが可能です。

(端末に対するセキュリティについて)
多様な用途かつ多数の端末を使用する場合、複数の異なるユーザを収容する場合、端末に高いセキュリティが求められる場合等において端末のセキュリティを保ちつつそれらの管理稼働を削減が必要な場合には、セキュリティ機能付きSIM/通信の監視装置/端末管理システムを導入することが効果的です。これらの装置のうちセンタUPFを使う場合にはセンタ拠点に複数拠点収容可能な監視装置、端末管理システム機能を有する製品を導入することでコストを押さえながらセキュリティを保つことが可能です。また、監視装置にセキュリティ機能付きSIM以外の通信を透過する機能を持つものを採用することにより、拠点

側についてはセキュリティ機能の必要な端末のみセキュリティ機能付き SIM を採用し、その他の端末については従来の SIM を使用する、という柔軟な運用が可能になります。

5.6 ローカル５Ｇ交換設備の共用における監視等および運用検証

(1) 検証目標

本調査研究のモデルであるコア装置の共用パターンでは、自治体や業界団体での共用ケースなど、ローカル５Ｇシステムに対して電気通信事業者等による運用監視が行われないケースが想定されます。

システムの維持・運用においては、正常性等の監視や障害等が発生した場合の原因切り分け等が必要であるため、ローカル５Ｇシステムに起こりうる障害事例について実際の環境下で再現し、有効な監視体系について検証しました。

具体的には、障害の発生から原因の切り分け、復旧、復旧後の正常性確認について検証し、システム正常性等の監視に有効となる指標 KPI および障害等の原因切り分けに有効となる指標（サブ KPI）について考察します。これらの KPI およびサブ KPI の有効性および妥当性を評価することで、ローカル５Ｇシステムの監視体制モデルについて提言します。

(2) 評価・検証項目

検証の対象とする項目は、以下「表 5-6-1 評価・検証項目」のとおりです。

表 5-6-1 評価・検証項目

項番	評価・検証項目
1	・障害に対する KPI およびサブ KPI の仮設 ・疑似的な障害の再現による KPI の有効性および妥当性の評価 過去に移動通信システムで発生した障害事例を参考に、ローカル５Ｇシステムにおいても発生が見込まれる次の４つの障害事例について再現し検証 a. RU 装置故障による電波送出停止（図 5-6-1） b. 設備故障による WAN 回線のエンド拠点側通信断（図 5-6-2） c. GMC 故障による同期外れ（図 5-6-3） d. SIM カード破損による SIM 認証エラー（図 5-6-4）
2	・監視運用モデルの考察および提言 監視対象とすべきパラメータ、運用上のルール等、監視運用モデルに盛り込むべき事項を洗い出し、評価

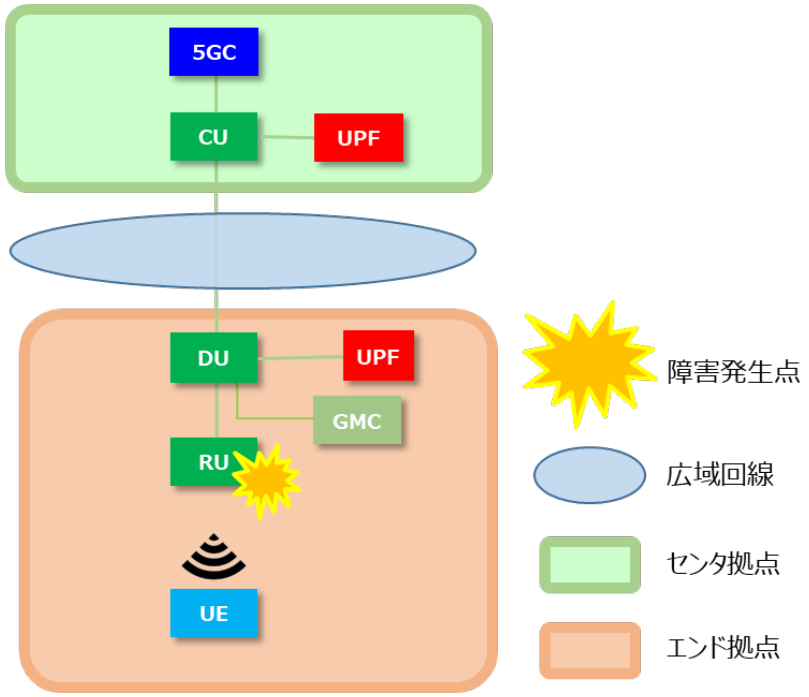


図 5-6-1　検証イメージ(RU 装置故障による電波送出停止)

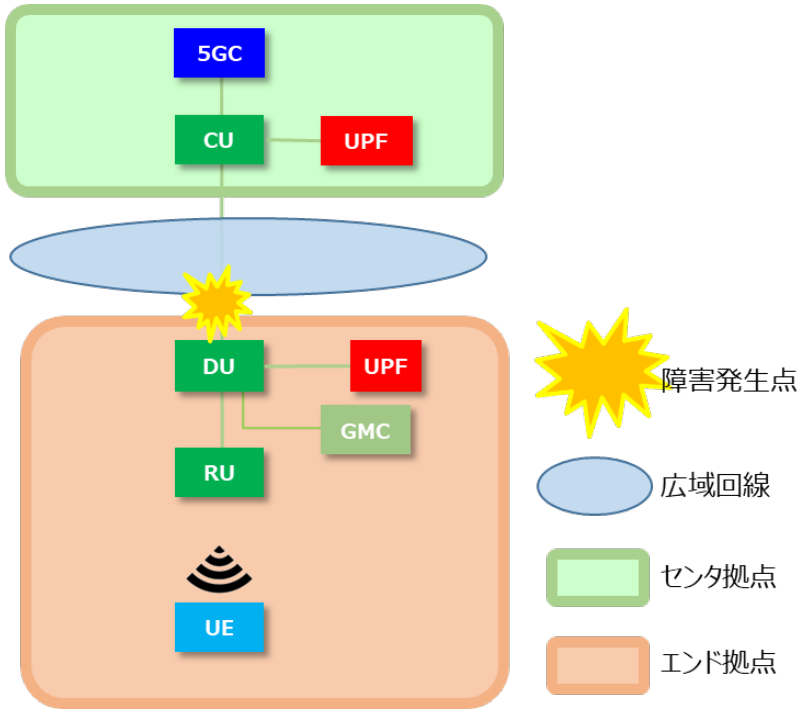


図 5-6-2　検証イメージ(設備故障による WAN 回線のエンド拠点側通信断)

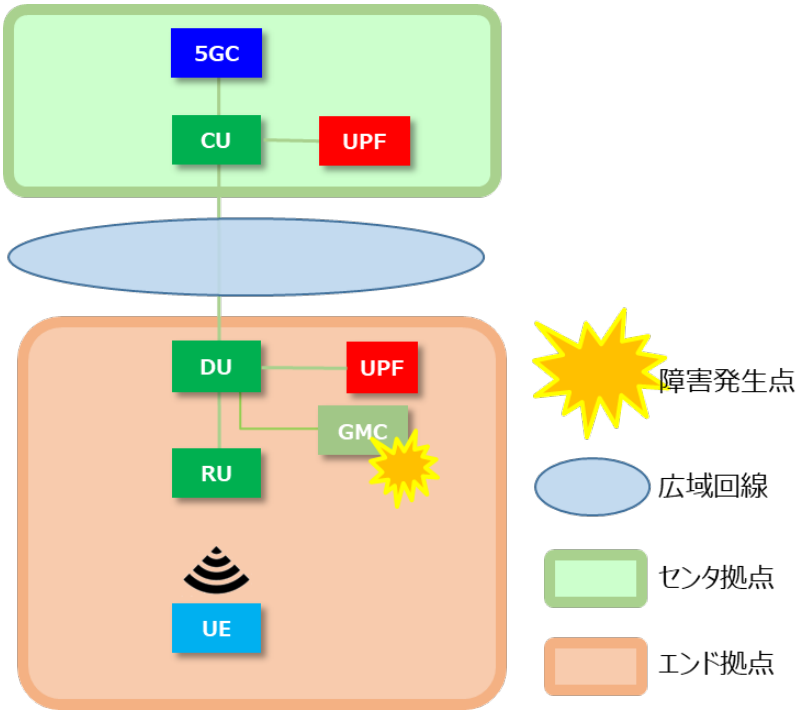


図 5-6-3　検証イメージ(GMC 故障による同期外れ)

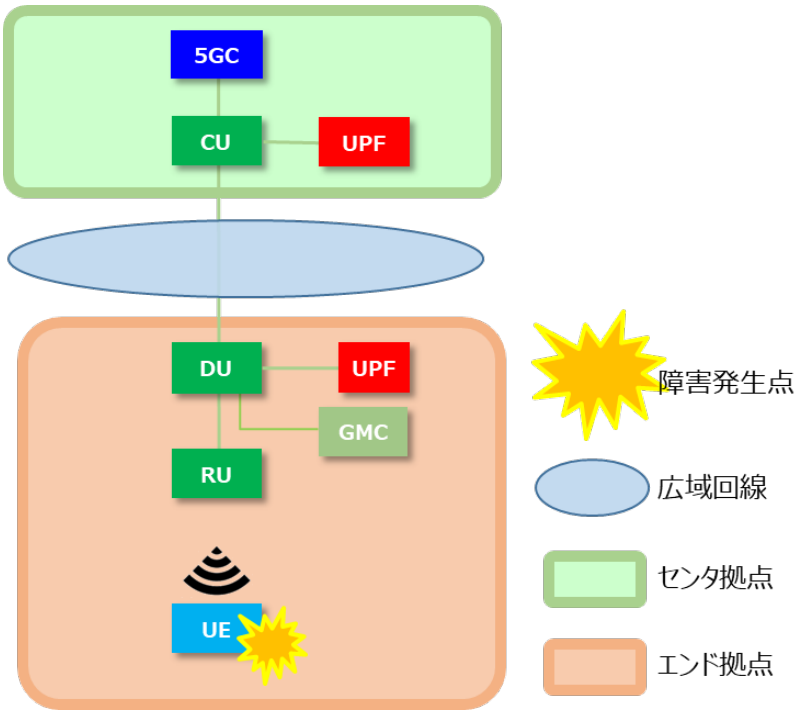


図 5-6-4　検証イメージ(SIM カード破損による SIM 認証エラー)

(3) 評価・検証手法

本検証で用いた測定ツールは、以下の「表 5-6-2 測定ツール」のとおりです。

表 5-6-2 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	常時監視および遠隔監視の環境：システム監視ツール(M 社製)

本検証にて想定した手順は、以下の「表 5-6-3 検証手順」のとおりです。

表 5-6-3 検証手順

項番	実施内容
1	【KPI およびサブ KPI の仮説立て】 ・検証する障害事例に対し、有効性が見込まれる KPI およびサブ KPI について机上検討による仮説立て ・障害の原因切り分け手法に関して、センタ拠点からの遠隔監視および操作並びに現場駆け付け時の対応についてシナリオ作成
2	【障害事例の再現および検証】 ・障害事例の再現は NTT 中央研修センタで実施 ・基準値として正常な状態で前項にて仮説した KPI およびサブ KPI を検証 ・障害が発生した場合を想定し、可能な限り症状を再現 ・シナリオに従い、障害発生時の KPI およびサブ KPI について監視 ・UE の通信性能に関する測定を行う場合は良好な電波環境下となる位置で測定を実施
3	【KPI およびサブ KPI の評価】 ・仮設した KPI およびサブ KPI について、正常な状態と障害発生時の値を比較し、障害発生による変動から KPI およびサブ KPI の有効性を評価 ・KPI、サブ KPI の各項目について、常時監視および遠隔監視の環境を構築するにあたっての難易度、コスト等を検証
4	【分析・考察】 次の項目について分析 ・ローカル５Ｇの管理に必要となる KPI およびサブ KPI ・常時監視および遠隔監視の環境を構築する際のポイント ・想定したシナリオと障害事例の検証結果との比較

本検証にて監視可能なパラメータを以下の「表 5-6-4 監視可能パラメータ」に示します。

表 5-6-4 監視可能パラメータ

機器名	監視可能パラメータ
5GC	・機器死活監視 ・ポート状態（リンクアップ／リンクダウン） ・5GC の呼処理の Log ファイル出力 ・伝送スループット
CU	・機器死活監視 ・ポート状態（リンクアップ／リンクダウン）
DU	・機器死活監視 ・ポート状態（リンクアップ／リンクダウン） ・伝送スループット
RU	・機器死活監視 ・電波送信レベル ・電波受信レベル ・GPS 同期状態 ・Fronthaul の疎通状態
GMC	・機器死活監視 ・同期源 ・GPS 捕捉数
L2SW	・機器死活監視 ・ポート状態（リンクアップ／リンクダウン）
L3SW	・機器死活監視 ・ポート状態（リンクアップ／リンクダウン）

(4) 検証結果

「表 5-6-3　検証手順」に従い、次のとおり実施しました。

① KPI およびサブ KPI の仮説立て

ア　KPI の仮設

本検証ではシステム正常性等の監視に有効となる指標を KPI とし、実際に監視した場合の効果を検証します。このため、KPI は機器個別の異常を検知する項目ではなく、システム全体に影響を及ぼす項目が対象となると考え、「表 5-6-4-①-1　仮説 KPI」のとおりとしました。

表 5-6-4-①-1　仮説 KPI

仮説KPI項目	選定理由
・５GCの機器死活監視	ローカル５Ｇシステムの中核となる機器であり、機器がダウンした場合のみならず、監視不可の状態が発生することは重大な障害であると想定されるため。
・呼処理の異常検知	UEから5GCまでの疎通や認証処理といったローカル５Ｇシステム全体の正常性から影響を受ける項目と想定されるため。
・RUの機器死活監視	エンド拠点の正常性を象徴する機器であるとともに、屋外設置など他の機器と比べて環境条件が悪く障害の可能性が高いものと想定されるため。
・RU電波送信レベル	RUの機器死活監視に加えてKPIとすることで、一層監視の効果を高めると想定されるため。
・RU電波受信レベル	RUの機器死活監視に加えてKPIとすることで、一層監視の効果を高めると想定されるため。
・RUのGPS同期状態	RUの機器死活監視に加えてKPIとすることで、一層監視の効果を高めると想定されるため。
・VPNセッション状態	コア共用に必須となるセンタ拠点とエンド拠点を接続するWAN回線は、一般的に電気通信事業者からサービス提供を受けるものでローカル５Ｇユーザの管理外だが、WAN回線の異常は重大な障害であると想定されるため。
・GMCの機器死活監視	ローカル５Ｇシステムにクロック信号を供給する装置であり、直接的に通信を経由する機器ではないが、その障害は重大な障害であると想定されるため。
・GMCのGPS捕捉状態	ローカル５Ｇシステムにクロック信号を供給する装置であり、直接的に通信を経由する機器ではないが、その障害は重大な障害であると想定されるため。

イ　サブ KPI

本検証では KPI による異常検知の後、障害等の原因切り分けを行います。原因切り分けの際に有効となる指標をサブ KPI として、実際に切り分けへの効果を検証します。このためサブ KPI は各機器の状態を監視するものであり、本検証では「表 5-6-4-①-2　仮説サブ KPI」のとおりとしました。

表 5-6-4-①-2　仮説サブ KPI

仮説サブKPI項目		選定理由
5GC	通信ポート状態（リンクアップ/リンクダウン）	5GCの各通信ポート状態を監視することで、対向機器やネットワークの異常検知が可能となると想定されるため。
	CPU利用率（閾値80%）	5GCの性能に関する異常検知が可能となると想定されるため。閾値は暫定値。
	メモリ利用率（閾値80%）	5GCの性能に関する異常検知が可能となると想定されるため。閾値は暫定値。
CU	機器死活監視	ローカル５Ｇシステムの構成要素として監視が必要と想定されるため。
	通信ポート状態（リンクアップ/リンクダウン）	対向機器やネットワークの異常検知が可能となると想定されるため。
	CPU利用率（閾値80%）	CUの性能に関する異常検知が可能となると想定されるため。閾値は暫定値。
	メモリ利用率（閾値80%）	ＣUの性能に関する異常検知が可能となると想定されるため。閾値は暫定値。
DU	機器死活監視	ローカル５Ｇシステムの構成要素として監視が必要と想定されるため。
	通信ポート状態（リンクアップ/リンクダウン）	対向機器やネットワークの異常検知が可能となると想定されるため。
	CPU利用率（閾値80%）	DUの性能に関する異常検知が可能となると想定されるため。閾値は暫定値。
	メモリ利用率（閾値80%）	DUの性能に関する異常検知が可能となると想定されるため。閾値は暫定値。
L2SW	機器死活監視	エンド拠点のネットワークの中核的な機器であり監視が必要と想定されるため。
	通信ポート状態（リンクアップ/リンクダウン）	対向機器やネットワークの異常検知が可能となると想定されるため。
L3SW	機器死活監視	センタ拠点のネットワークの中核的な機器であり監視が必要と想定されるため。
	通信ポート状態（リンクアップ/リンクダウン）	対向機器やネットワークの異常検知が可能となると想定されるため。

ウ　机上検討

検証する障害事例に対し、有効性が見込まれる KPI およびサブ KPI について、次の（ア）～（エ）のとおり机上検討を行いました。

（ア）　RU 装置故障による電波送出停止の机上検討

RU は屋外設置となる場合も多く、台風などによって外因的に故障が生じる可能性が高いものと想定されます。本検証では、明白な物理的破損ではなく、内部回路の損傷によって送

信が意図せず停止する障害を想定しました。この障害が発生した場合は 5GC、CU、DU および各ネットワーク機器等は正常稼働しているものの UE がアタッチできない状態となりますが、RU 送信レベルを KPI とすることで異常発生を検知できると予想しました。

（イ）　設備故障による WAN 回線のエンド拠点側通信断

コア共用では 5GC が設置されているセンタ拠点と RAN 設備が運用されているエンド拠点の間を WAN 回線によって接続する必要があります。一般的に WAN 回線はユーザ企業が自ら構築するものではなく電気通信事業者からサービスの提供を受けるものです。そのためユーザ企業が直接 WAN 回線を監視することはできないものの、その障害発生時には多大な影響が生じることが想定されます。サービス用の WAN 回線に障害が生じた場合に VPN セッションを KPI とすることで異常検知できると予想しました。

なお、本調査研究ではサービス用の WAN 回線と並行して保守用の WAN 回線が存在しており、サービス用の WAN 回線が断となった場合もエンド拠点の監視を継続することができます。

（ウ）　GMC 故障による同期外れ

GMC はエンド拠点の機器がセンタ拠点と同期するために必要なクロック信号の供給元となる機器です。直接的にローカル５Ｇの通信が通過する機器ではないため、GMC に対しては積極的な監視をしなければならないと考えました。GPS アンテナ破損などによる GPS 捕捉状態の遷移を KPI とすることで異常検知できると予想しました。

（エ）　SIM カード破損による SIM 認証エラー

UE はユーザが最も触れ、操作する機器であり、様々な故障が発生する可能性があると考えます。本検証では SIM が破損し認証にエラーが生じる障害を想定しました。呼処理の異常検知を KPI とし、SIM 認証に関する 5GC のエラーメッセージを監視することで本障害を検知できると予想しました。

② 障害事例の再現および検証

ア　開始前の正常状態

本検証ではセンタ拠点において各種エラーメッセージ監視のためにシステム監視ツールサーバを設置し、自動的に異常を検知できる環境を構築しました。KPI およびサブ KPI の Alert は全てシステム監視ツールで確認できます。正常な状態は「図 5-6-4-②-1　システム監視ツール正常状態」のとおり表示されます。

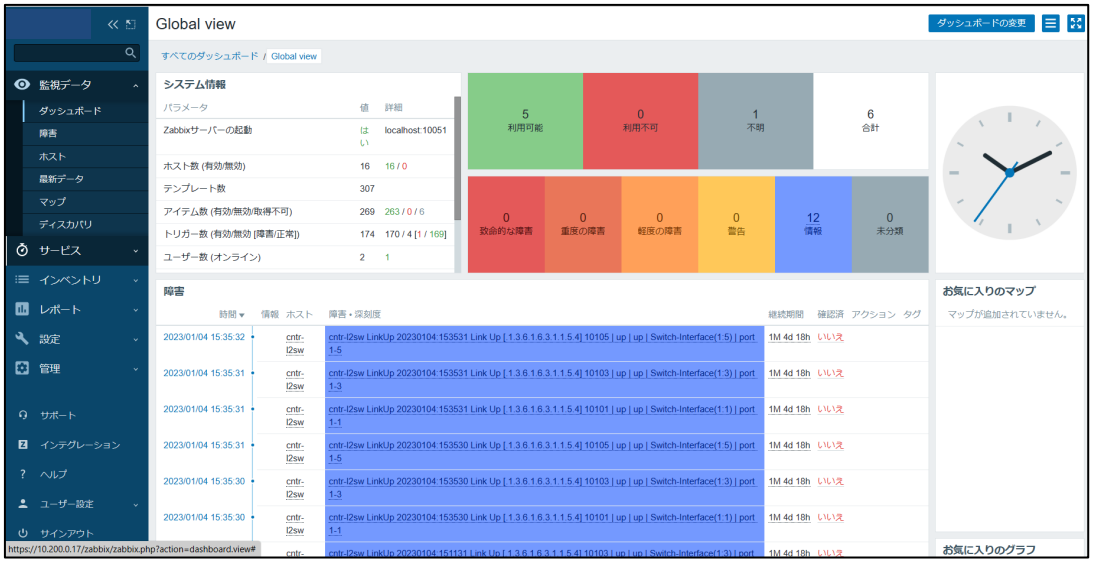


図 5-6-4-②-1　システム監視ツール正常状態

画面中央下の障害の欄に青く表示されているのは、検証当日のシステム起動に関するメッセージです。

なお、本検証ではシステム監視ツールの画面更新間隔を 1 分間にしています。

イ　RU 装置故障による電波送出停止

（ア）　障害の発生（再現）

RU 装置故障による電波送出停止を再現します。正規の停波手順をとるのではなく、より障害発生状況に近づけるためダミーの RU 送信レベル値を出力させ、再現しました。

（イ）　障害検知

障害の発生（再現）の設定後、すぐにシステム監視ツールが「図 5-6-4-②-2　システム監視ツール　RU Tx レベル低下」のとおり Alert メッセージを出力しました。

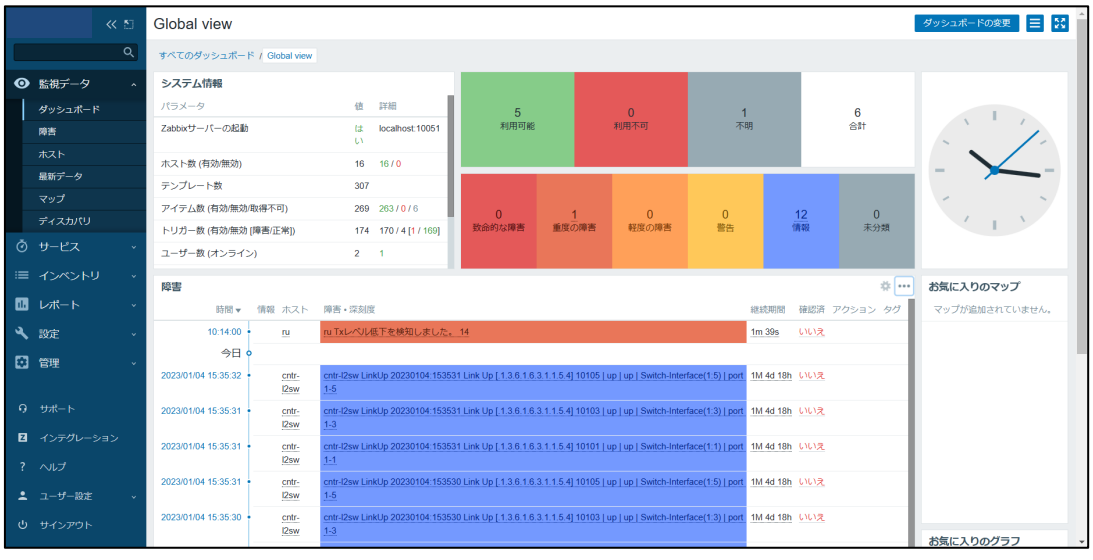


図 5-6-4-②-2　システム監視ツール　RU Tx レベル低下

コア共用においては、ユーザではなくコア共用を提供するSIer等がシステム監視者を担うケースが主であり、障害検知時にはシステム監視者からユーザへ障害検知を第0報として連絡する運用が想定されます。こうした監視運用体制を構築する際には、連絡方法(電話、メール、ほか)、連絡時間帯（24時間365日、平日昼間帯のみ、など)、速報すべきアラートの設定について事前に取り決める必要があると考えます。

（ウ）　リモート切り分け

障害検知によりシステム監視者がリモート切り分けを開始します。まずはKPIおよびサブKPIの全項目に対してAlert発生の有無およびAlert内容の点検を実施します。「図5-6-4-②-3　システム監視ツール　RU　Txレベル低下　再確認」のとおり、RU　Txレベル低下のAlertだけが出力されています。

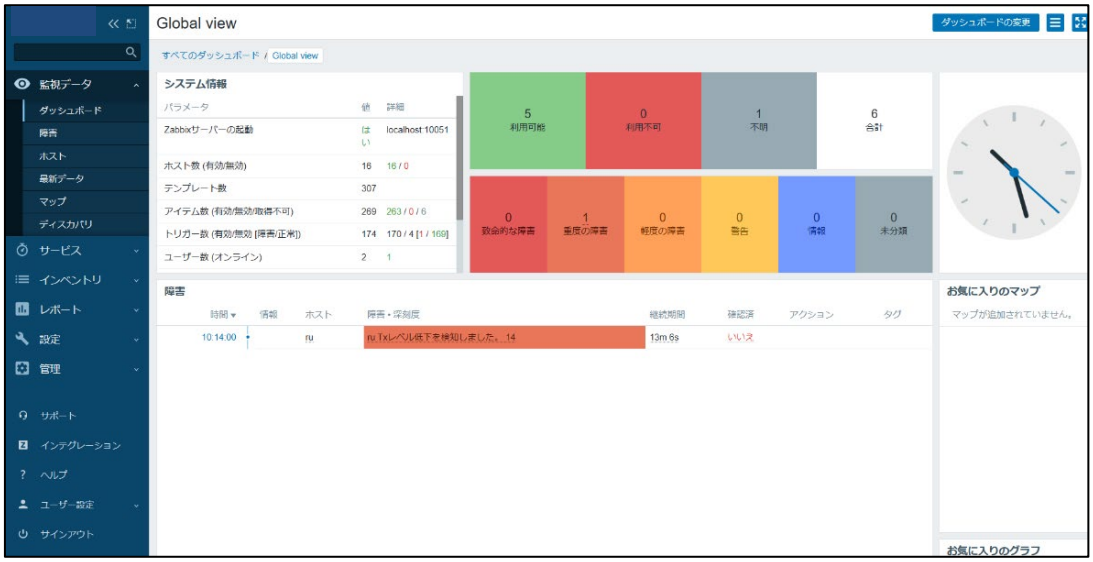


図5-6-4-②-3　システム監視ツール　RU　Txレベル低下　再確認

KPIおよびサブKPIから各機器の死活監視や通信ポート状態監視にAlertが出ておらず、RU　Txレベル低下だけのAlertという状態から、RUが当該障害の原因個所であると切り分けることができます。

運用対応としてはリモート操作によるRUの再起動を実施することが想定されます。そのためユーザへの作業前後の連絡手順、RUその他必要な機器に対するシステム監視者によるリモート操作権限に関するユーザ合意、リモート操作手順のマニュアル化について事前に取り決める必要があると考えます。

リモート操作によるRUの再起動で復旧しないとして、現場駆け付けによる対応に移行します。

（エ）　現地駆け付け対応

現地駆け付け対応について机上検討を行い、次の手順を想定しました。

・交換用物品としてRUの予備品、ケーブル類、測定器類その他必要な資材を準備
・資材準備完了後、ユーザにエンド拠点への入局を申請し、ユーザが承認
・現場に到着し、測定器を使用してRU送信電波停止を確認
・エンド拠点においてRU以外の機器が正常に動作していることを確認

・RU を予備品に交換
・上記作業についてはユーザおよびシステム監視者に逐次報告し連携して実施
　各対応をスムーズに実施するためには、予備品・資材の確保、予備 RU の無線局免許取得、RU 交換手順のマニュアル化、エンド拠点入局申請/承認の手続き、エンド拠点入局可能時間帯、ユーザ立会の有無、高所作業等についてのエンド拠点内作業ルール、エンド拠点内の図面・通信系統図・電源系統図の整備について事前に取り決める必要があると考えます。
　なお、本検証では現場にて RU を交換したものと想定し、RU を通常の設定に戻しました。

（オ）　復旧後の正常性確認
　現地駆け付け対応が完了後、システムの正常性を確認します。システム監視ツールにて再度すべての KPI およびサブ KPI の確認を実施し、「図 5-6-4-②-4　システム監視ツール　RU Tx レベル低下　復旧」のとおり、障害から復旧したことを確認しました。

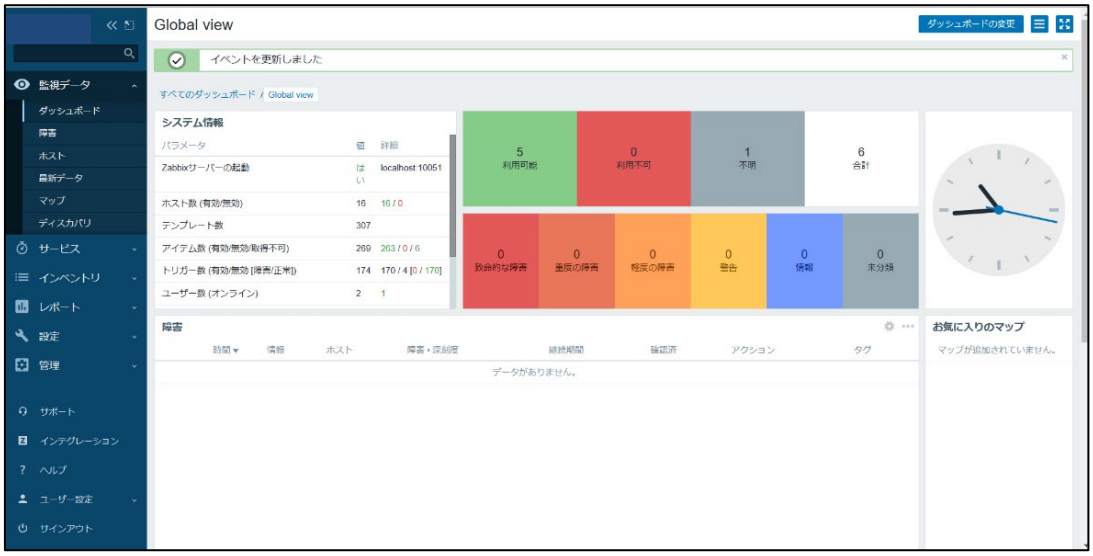


図 5-6-4-②-4　システム監視ツール　RU　Tx レベル低下　復旧

ウ　設備故障による WAN 回線のエンド拠点側通信断
（ア）　障害の発生（再現）
　設備故障による WAN 回線のエンド拠点側通信断を再現します。エンド拠点において WAN 回線と接続されている通信ケーブルを通信ポートから抜去することで障害を再現しました。

（イ）　障害検知
　障害の発生（再現）の設定後、すぐにシステム監視ツールが「図 5-6-4-②-5　システム監視ツール　VPN セッション切断」のとおり Alert メッセージを出力しました。

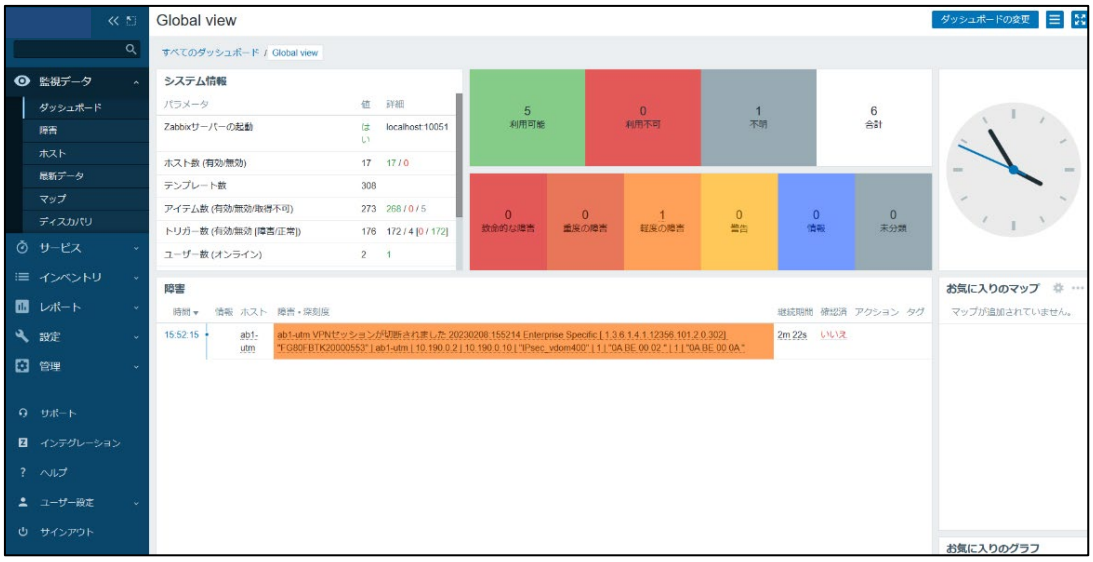


図 5-6-4-②-5　システム監視ツール　VPN セッション切断

障害検知時にはシステム監視者からユーザへ障害検知を第 0 報として連絡する運用が想定されます。

（ウ）　リモート切り分け

障害検知によりシステム監視者がリモート切り分けを開始します。まずは KPI およびサブ KPI の全項目に対して Alert 発生の有無および Alert 内容の点検を実施します。「図 5-6-4-②-6　システム監視ツール　VPN セッション切断と Remove　RAN」のとおり、VPN セッション切断および DU との通信異常による Alert が出力されています。

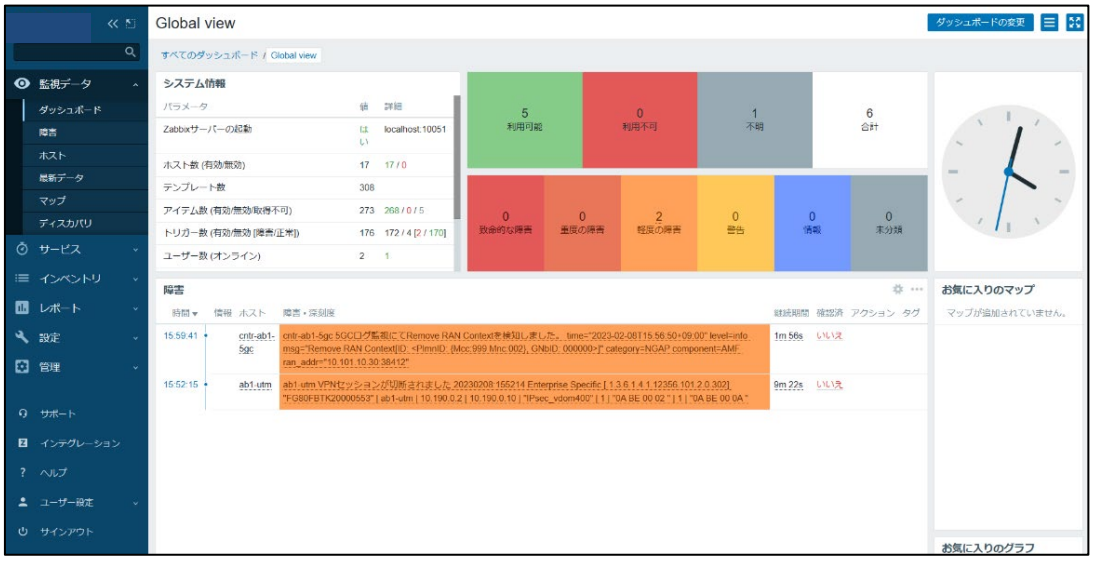


図 5-6-4-②-6　システム監視ツール　VPN セッション切断と Remove　RAN

本検証ではサービス用の WAN 回線と別に保守用の WAN 回線が存在し、サービス用の WAN 回線が断となった場合もエンド拠点の機器監視を継続することが可能です。センタ拠点およびエンド拠点の機器が正常に動作していること、VPN セッション断が発生していること、センタ拠点の CU とエンド拠点の DU が疎通できていないことから、WAN 回線が当該障害の原因

箇所であると切り分けることができます。

（エ）　WAN 回線事業者による対応

WAN 回線事業者による対応について机上検討を行い、次の手順を想定しました。

・WAN 回線事業者へ WAN 回線断の疑いがある旨を連絡し、対応を依頼

・WAN 回線事業者からの復旧連絡

・システム監視ツールでの WAN 回線復旧確認「図 5-6-4-②-7　システム監視ツール　VPN セッション復旧」

・リモートでの電波再発射「図 5-6-4-②-8　システム監視ツール　電波再発射」

・上記作業についてはユーザおよびシステム監視者に逐次報告し連携して実施



図 5-6-4-②-7　システム監視ツール　VPN セッション復旧

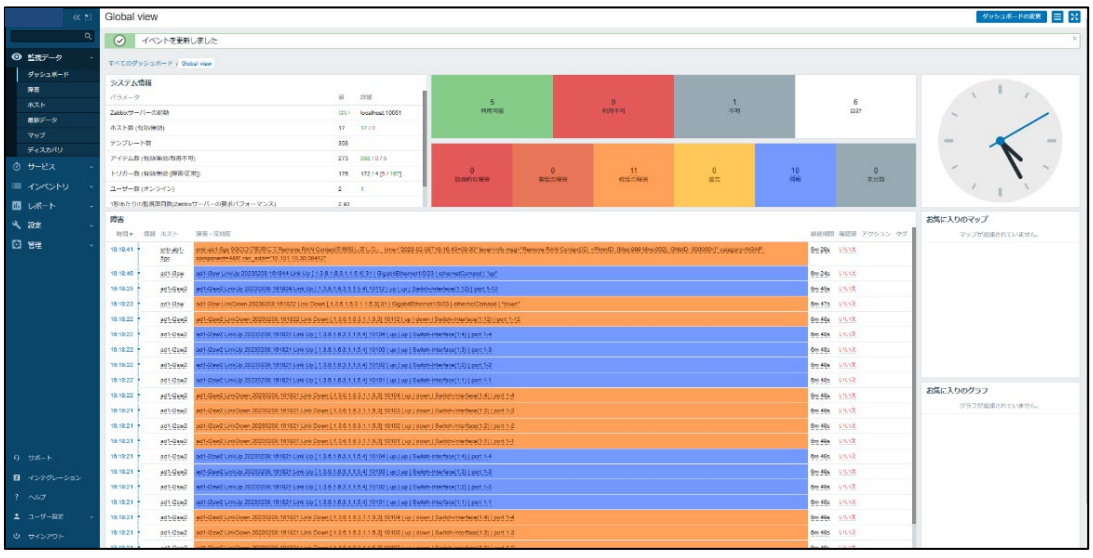


図 5-6-4-②-8　システム監視ツール　電波再発射

各対応をスムーズに実施するためには、WAN 回線事業者への連絡をユーザが行うかシステ

ム監視者が行うか、WAN 回線設備とローカル５Ｇシステムの責任分界点の整理、WAN 回線事業者への連絡手順、WAN 回線に関する SLA について事前に取り決める必要があると考えます。

なお、本検証では WAN 回線設備内で復旧作業が行われたものと想定し、抜去したケーブルを元に戻した後、電波再発射の手順を実施しました。

（オ）　復旧後の正常性確認

WAN 回線事業者の復旧対応が完了後、システムの正常性を確認します。システム監視ツールにて再度すべての KPI およびサブ KPI の確認を実施し、「図 5-6-4-②-9　システム監視ツール　正常性確認」のとおり、障害から復旧したことを確認しました。

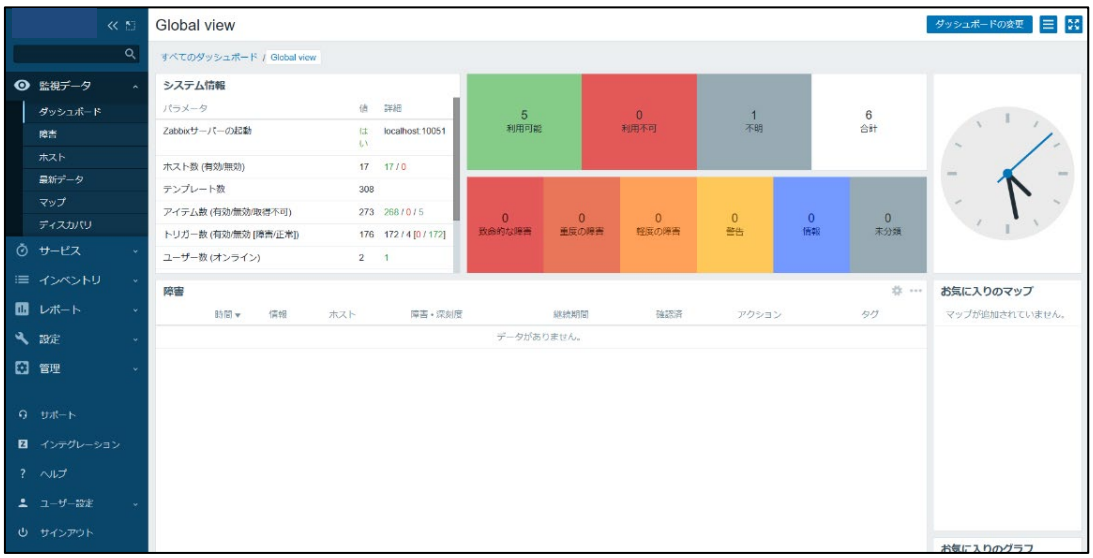


図 5-6-4-②-9　システム監視ツール　正常性確認

エ　GMC 故障による同期外れ

（ア）　障害の発生（再現）

GMC 故障による同期外れの障害を再現するため、エンド拠点に設置された GMC から GPS アンテナ用同軸ケーブルを抜去しました。

（イ）　障害検知

障害の発生（再現）の設定後、すぐにシステム監視ツールが「図 5-6-4-②-10　システム監視ツール　GNSS 状態遷移」のとおり Alert メッセージを出力しました。

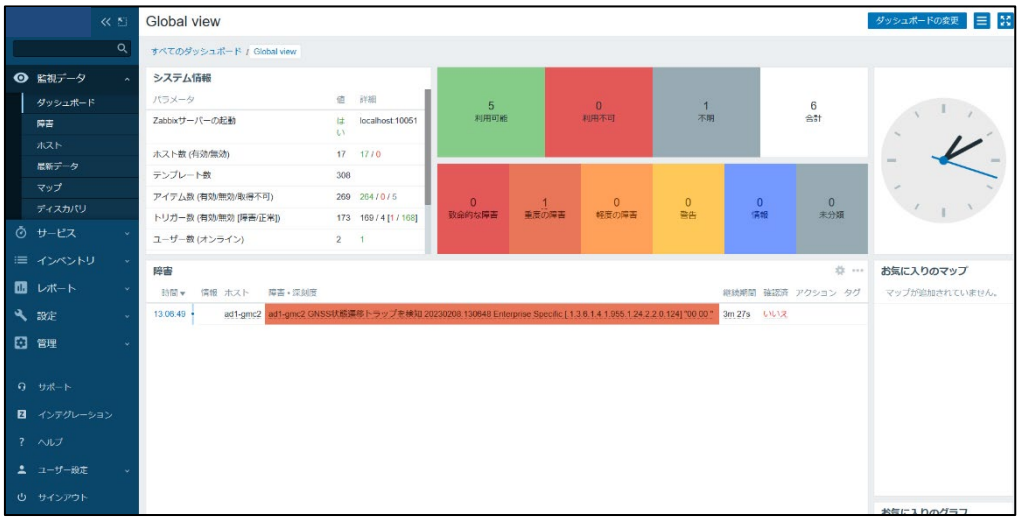


図 5-6-4-②-10　システム監視ツール　GNSS 状態遷移

これは GMC が GPS 衛星からの信号を受信して同期状態であったものが、同期から外れた自走状態となったことを示すメッセージです。

障害検知時にはシステム監視者からユーザへ障害検知を第 0 報として連絡する運用が想定されます。ただし、GMC 状態遷移は直ちにユーザの通信が途絶するものとはいいがたいため、速報の対象とするか否かを事前に取り決める必要があると考えます。

（ウ）　リモート切り分け

障害検知によりシステム監視者がリモート切り分けを開始します。まずは KPI およびサブ KPI の全項目に対して Alert 発生の有無および Alert 内容の点検を実施します。「図 5-6-4-②-11　システム監視ツール　GNSS 状態遷移のみ」のとおり、GNSS 状態遷移による Alert だけが出力されています。

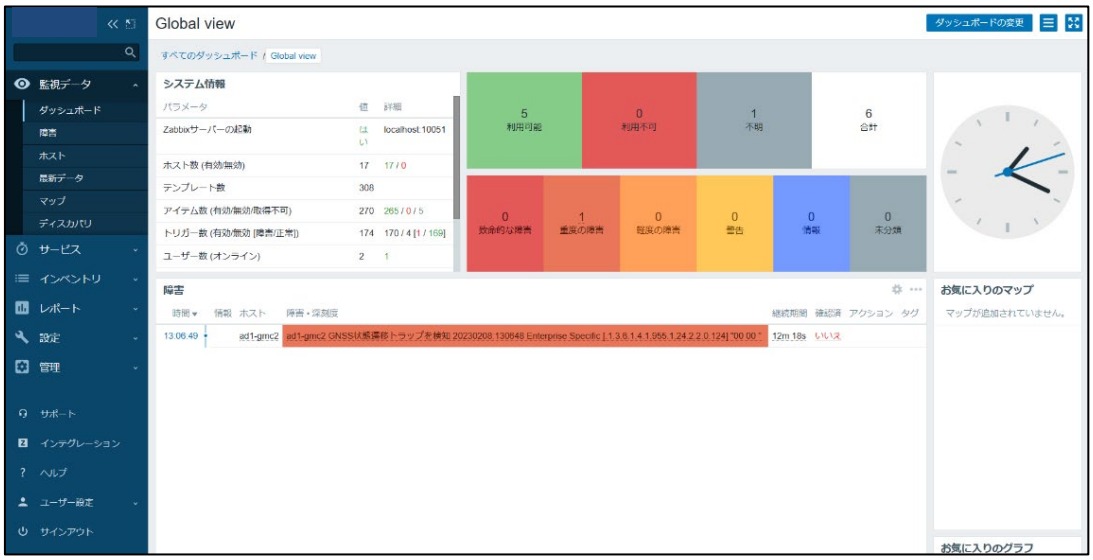


図 5-6-4-②-11　システム監視ツール　GNSS 状態遷移のみ

Alert の詳細を確認するため、「図 5-6-4-②-12　システム監視ツール　GNSS 状態の詳細確認」のとおり、システム監視ツールの最新データメニューからホスト「ad1-gmc2」を選択

し、GNSS 状態の詳細を閲覧します。「図 5-6-4-②-13　システム監視ツール　GNSS 状態　124（衛星断）」が表示されており、GMC が GPS 衛星を捕捉できていないことがわかります。

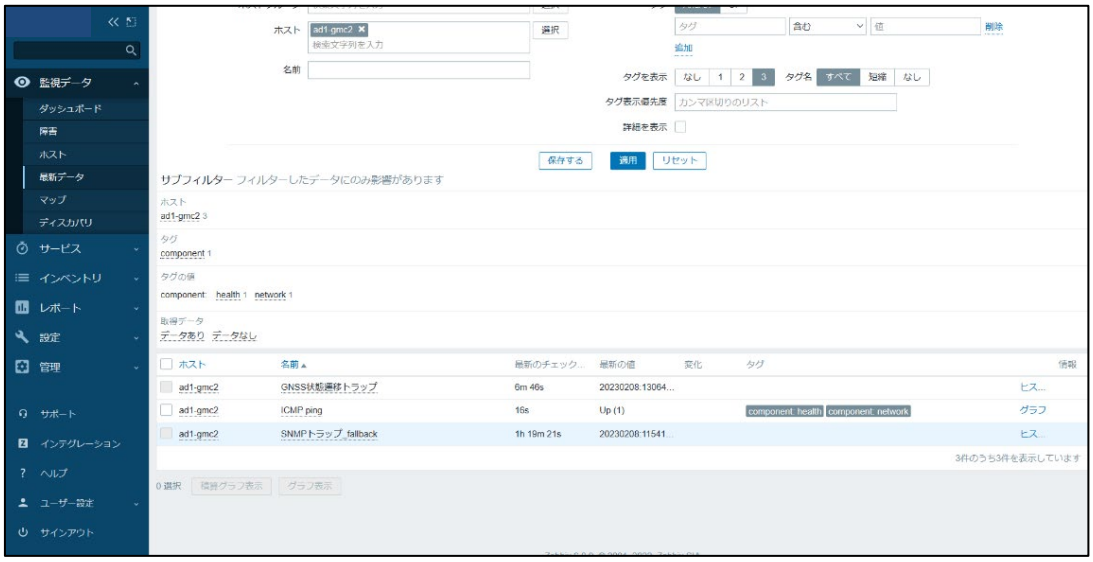


図 5-6-4-②-12　システム監視ツール　GNSS 状態の詳細確認



図 5-6-4-②-13　システム監視ツール　GNSS 状態　124（衛星断）

運用対応としてはリモート操作による GMC の再起動を実施することが想定されます。GMC その他必要な機器に対するシステム監視者によるリモート操作権限に関するユーザ合意、リモート操作手順のマニュアル化について事前に取り決める必要があると考えます。

リモート操作による GMC の再起動で復旧しないとして、現場駆け付けによる対応に移行します。

（エ）　現地駆け付け対応

現地駆け付け対応について机上検討を行い、次の手順を想定しました。

・交換用物品として GMC の予備品、GPS アンテナ、ケーブル類、測定器類その他必要な資材を準備

・資材準備完了後、ユーザにエンド拠点への入局を申請し、ユーザが承認
・現場に到着し、測定器を使用して機器に挿入されたケーブルまで正常に GPS 信号が到達していることを確認
・エンド拠点において GMC 以外の機器が正常に動作していることを確認
・GMC を予備品に交換
・上記作業についてはユーザおよびシステム監視者に逐次報告し連携して実施
　各対応をスムーズに実施するためには、予備品・資材の確保、GMC 交換手順のマニュアル化について事前に取り決める必要があると考えます。
　なお、本検証では現場にて GMC を交換したものと想定し、同軸ケーブルを元に戻しました。

（オ）　復旧後の正常性確認
　現地駆け付け対応が完了後、システムの正常性を確認します。システム監視ツールにて再度すべての KPI およびサブ KPI の確認を実施し、「図 5-6-4-②-14　システム監視ツール GNSS 復旧」および「図 5-6-4-②-15　システム監視ツール　GNSS 状態　123（衛星捕捉）」のとおり、障害から復旧したことを確認しました。

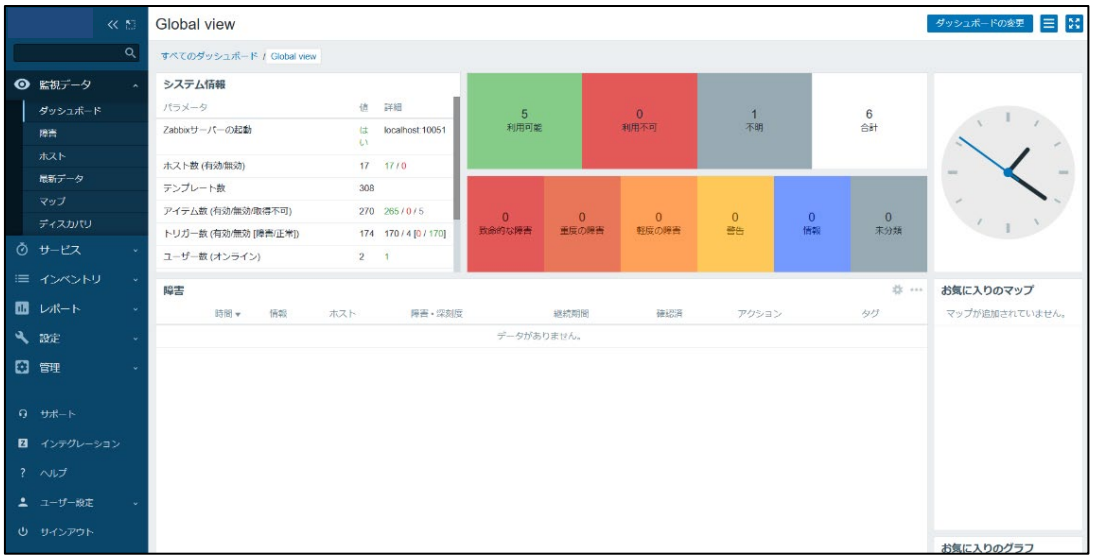


図 5-6-4-②-14　システム監視ツール　GNSS 復旧

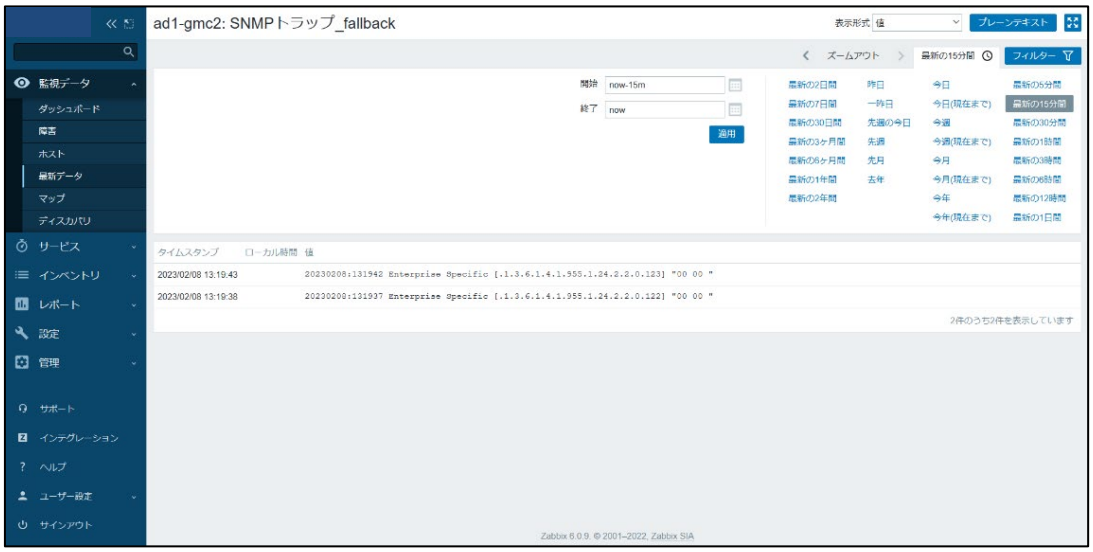


図 5-6-4-②-15　システム監視ツール　GNSS 状態　123（衛星捕捉）

オ　SIM カード破損による SIM 認証エラー

（ア）　障害の発生（再現）

SIM が破損し、正常に認証できない状況を再現するため、未登録 SIM を挿した UE を用意し、ローカル５Ｇのエリア内でフライトモードを解除しました。

（イ）　障害検知

障害の発生（再現）の設定後、すぐにシステム監視ツールが「図 5-6-4-②-16　システム監視ツール　Send Registration Reject」のとおり Alert メッセージを出力しました。

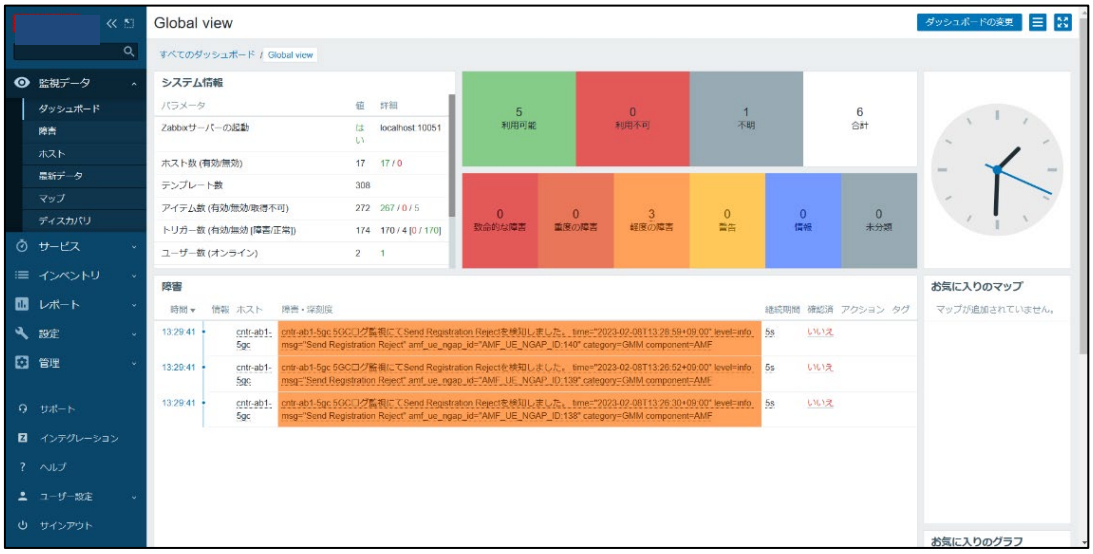


図 5-6-4-②-16　システム監視ツール　Send Registration Reject

障害検知時にはシステム監視者からユーザへ障害検知を第０報として連絡する運用が想定されます。ただし、Send Registration Reject は異なるローカル５Ｇシステムの UE がエリア内に侵入した場合でも出力されるメッセージであるため、速報の対象とするか否かを事前に取り決める必要があると考えます。

（ウ）　リモート切り分け

障害検知によりシステム監視者がリモート切り分けを開始します KPI およびサブ KPI の全項目に対して Alert 発生の有無および Alert 内容の点検を実施します。前述の「図 5-6-4-②-16　システム監視ツール　Send Registration Reject」以外の Alert が出力されないことから、UE が障害の原因個所であると切り分けることができます。

（エ）　現地駆け付け対応

現地駆け付け対応について机上検討を行い、次の手順を想定しました。

・交換用物品として UE 予備品、SIM 予備品その他必要な資材を準備
・資材準備完了後、ユーザにエンド拠点への入局を申請し、ユーザが承認
・現場に到着し、当該 UE が正常に動作しないことを確認
・エンド拠点において当該 UE 以外の機器が正常に動作していることを確認
・UE を予備品に交換
・上記作業についてはユーザおよびシステム監視者に逐次報告し連携して実施

各対応をスムーズに実施するためには、予備 UE および予備 SIM の確保並びに予備 UE の無線局免許取得について事前に取り決める必要があると考えます。また、他の障害と比較して簡易的に復旧できる内容であるため、マニュアルおよび予備品をエンド拠点に常備し、ユーザ自身による交換作業を取り決めておくことも有効であると考えます。

なお、本検証では現場にて正常な SIM に交換したものと想定し、登録済みに SIM を交換することで復旧しました。

（オ）　復旧後の正常性確認

現地駆け付け対応が完了後、システムの正常性を確認します。システム監視ツールにて再度すべての KPI およびサブ KPI の確認を実施し、「図 5-6-4-②-17　システム監視ツール　正常性確認」のとおり、障害から復旧したことを確認しました。

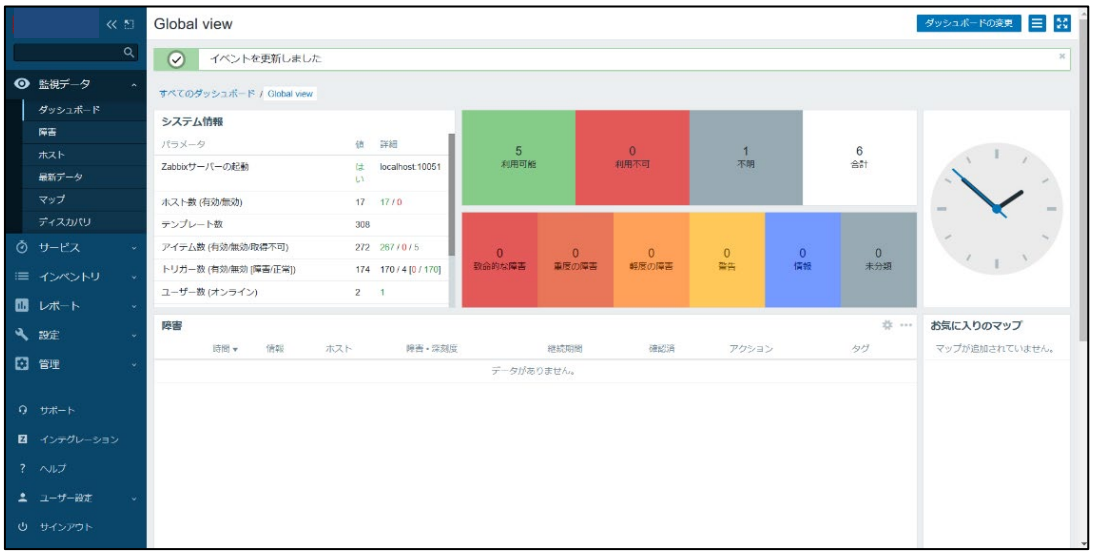


図 5-6-4-②-17　システム監視ツール　正常性確認

③　KPI およびサブ KPI の評価

障害事例の再現および検証の結果を踏まえて、本検証における KPI およびサブ KPI について「表 5-6-4-③-1　KPI の評価」および「表 5-6-4-③-2　サブ KPI の評価」にまとめました。

表 5-6-4-③-1　KPI の評価

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

					術的な協力が必要となるため、実装の難易度は高いと考えます。
・RU 電波受信レベル	－	－	－	－	本検証では Alert を出す対象ではなかったものの、RU 電波送信レベルと同様に KPI として有効であると考えます。 監視の難易度についても RU 電波送信レベルと同様に高いと考えます。
・RU の GPS 同期状態	－	－	－	－	本検証では Alert を出す対象ではなかったため、GMC 障害が 5GC から RU までの区間を原因としないものである判断材料として有効でした。もし、RU の GPS 同期状態について Alert が発生した場合は、途中区間の通信区間断や RU 装置故障などが疑われるため、KPI として必須と考えます。 また、監視するには RU ベンダーの技術的な協力が必要となるため、実装の難易度は高いと考えます。
・VPN セッション状態	－	○	－	－	コア共用において WAN 回線は不可欠であり、WAN 回線の障害は重大な影響を発生させるものであるため、WAN 障害を検知する項目として KPI として有効であると考えます。 ネットワーク機器のベンダーの技術的な協力が必要となるため、実装の難易度は高いと考えます。 WAN 回線事業者と SLA を取り交わすことで、ローカル５Ｇシステム内で監視せずに、WAN 回線事業者に監視体制を求めることも選択できると考えます。
・GMC の機器死活監視	－	－	－	－	GMC はエンド拠点の機器がセンタ拠点と同期するために必要なクロック信号の供給元となる機器です。直接的にローカル５Ｇの通信が通過する機器ではないため、GMC に対しては積極的な監視をしなければならないため、KPI として必須と考えます。 また、監視するには GMC ベンダーの技術的な協力が必要となるため、実装の難易度は高いと考えます。

・GMC の GPS 捕捉状態	－	－	○	－	GMC 障害において異常検知した項目であり、KPI として有効であると考えます。 また、監視するには GMC ベンダーの技術的な協力が必要となるため、実装の難易度は高いと考えます。

表 5-6-4-③-2　サブ KPI の評価

仮説サブKPI項目		評価と難易度
5GC	通信ポート状態 CPU利用率 メモリ利用率	通信ポート状態を監視することで、通信ポート自身の故障、通信ポートに接続するケーブル故障、対向する機器の故障の３つを監視できます。機器の死活監視や対向機器の通信ポート状態と見比べることで原因箇所を切り分けるサブKPIとして有効であると考えます。 またCPU利用率およびメモリ利用率は機器自身の動作が正常であるか否かを判断する材料として有効であり、動作不安定時に確認すべきサブKPIとして有効であると考えます。 本検証ではこれらのAlertが出力されないことで5GCではなく、エンド拠点側の故障が原因であると切り分ける判断材料となりました。
CU	機器死活監視 通信ポート状態 CPU利用率 メモリ利用率	本検証ではCU/DU分離構成であるため、それぞれを監視しましたが、一体であっても監視の必要性は変わらず、サブKPIとして必須であると考えます。ユースケースによっては機器死活監視をKPIとする場合も想定されます。 通信ポート状態並びにCPU利用率およびメモリ利用率は5GCと同様にサブKPIとして有効であると考えます。 本検証ではこれらのAlertが出力されないことで、エンド拠点内のどこに障害の原因があるかを切り分ける判断材料となりました。
DU	機器死活監視 通信ポート状態 CPU利用率 メモリ利用率	
L2SW	機器死活監視 通信ポート状態	機器死活監視、通信ポート状態ともに、5GC、CU、DUの項に記載のとおりサブKPIとして有効であると考えます。 本検証ではこれらのAlertが出力されないことで、エンド拠点内のどこに障害の原因があるかを切り分ける判断材料となりました。
L3SW	機器死活監視 通信ポート状態	機器死活監視、通信ポート状態ともに、5GC、CU、DUの項に記載のとおりサブKPIとして有効であると考えます。 本検証ではこれらの Alert が出力されないことで、エンド拠点内のどこに障害の原因があるかを切り分ける判断材料となりました。

④　分析・考察

本検証では Alert の監視および通知の機能を有するシステム監視ツールサーバをセンタ拠点に設置し、コア共用での監視運用体制の基本形として SIer がシステム監視者となる想定で実施しました。そして本検証を通して、この体制に置いて KPI およびサブ KPI を設定

し監視することが、障害の原因箇所のリモート切り分けおよび現地駆け付けまでの時間を短縮し、障害復旧の迅速化に資するという結果を得たものと考えます。

特に機器死活監視は、単に対象の機器の状態を通知するだけでなく、その機器までのネットワークの正常性を判別するためにも有効な情報でした。KPI またはサブ KPI として重要であると考えます。ただし、ユースケースによっては本検証以外の項目が KPI として適切である場合も想定されます。そのため、ユーザが重要視する Alert についてシステム監視者と事前に取り決めることが有効であると考えます。

しかし、KPI 等の Alert から適切に切り分けを実施するためには、システムの構成・系統を正確に把握することが求められます。そのため、システム監視者の元には 5GC が設置されたセンタ拠点に限らず、主としてユーザが管理するエンド拠点および拠点間を接続する WAN 回線まで含めた系統図等を事前に整備することが必要であると考えます。

本検証では機器故障を原因とし、機器交換による復旧を想定しました。そのため予備の機器が必要であり、障害復旧までの時間を短くするため、予備品を事前に確保しておくことが有効です。また RU および UE を予備品に交換する場合、無線局免許についても手続きが必要であることに注意すべきと考えます。

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

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

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、コアおよびCU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、またコアおよびCUを共用する他の拠点への影響への有無について検証し考察を行いました。

R3 年度の本検証では、複数企業パターンにおいて「ウェアラブルカメラを用いた遠隔支援検証」、業界共用パターンにおいて「映像AIシステムを用いた顔認証検証」を実施し、コアを共用する環境下でそれぞれのユースケースが実現可能であることを確認しました。しかし、複数企業パターンにおいて用いた360°カメラ、ウェアラブルカメラの映像にカクつきやフリーズが見られ、いすゞ自動車の作業場周辺環境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る旨の考察を行いました。

上記反省を踏まえ、本年度は複数企業共用パターンにおいて 4K AI カメラを用いる新たなユースケースを選定し、カメラの設置の際に金属や鉄板素材による影響を軽減するために事前の電波測定を実施しカメラの位置とRUの設置位置を調整した上で検証を実施し、その効果についても考察を行いました。

また、R3 年度においてはコアを共用する各拠点の同時利用について他拠点への影響がないことを確認しましたが、いずれの共用パターンにおいても共用する拠点間の直接の通信は発生しないユースケースでした。

本年度は業界共用パターンにおいて8Kカメラによる大容量映像の拠点間通信が発生する新たなユースケースを選定し、拠点間通信を行うために必要な要件についても考察を行いました。

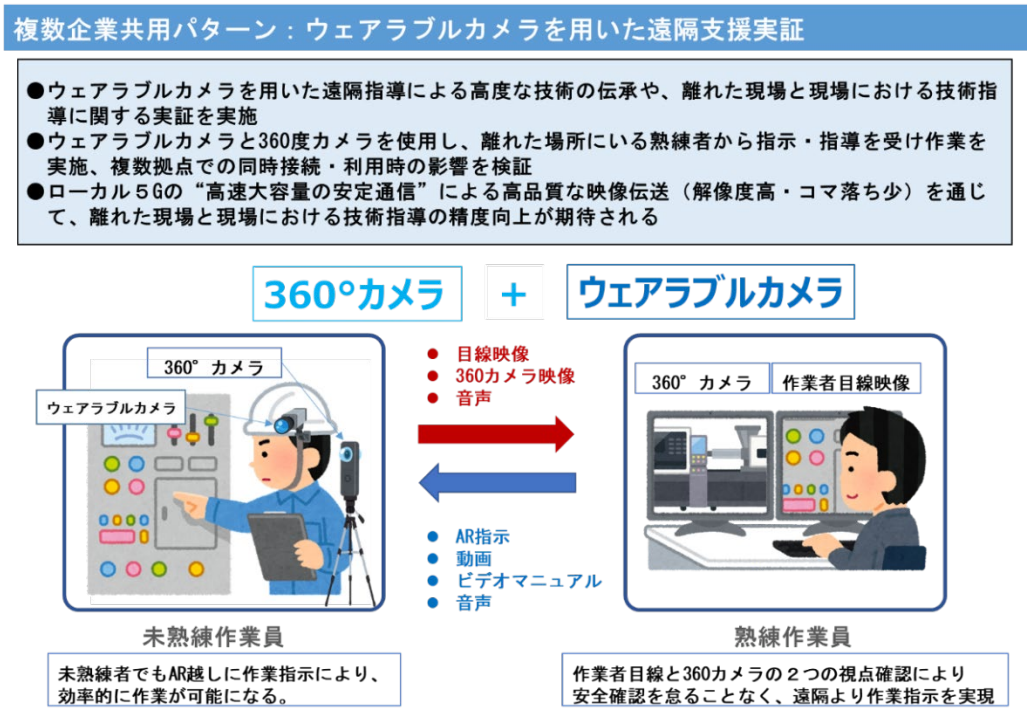


図 6-1　（参考）R3 年度調査研究 複数企業共用パターン　ユースケース概要図（参考）

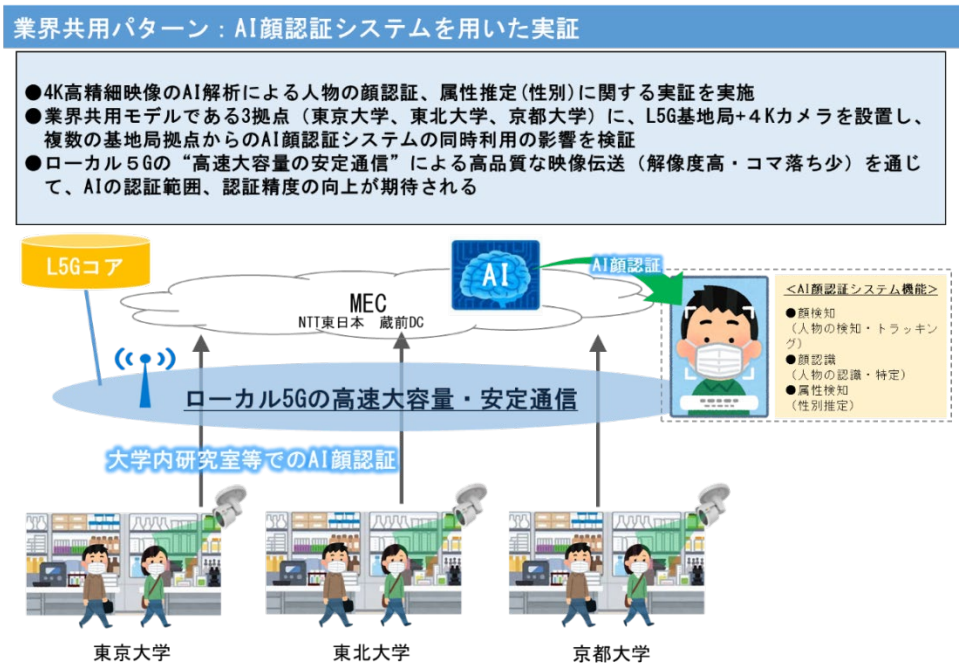


図 6-2　（参考）R3 年度調査研究 業界企業共用パターン　ユースケース概要図

(1) 複数企業共用パターン 4K AI カメラソリューション

厚生労働省が公表した令和 3 年労働災害発生状況によると、労働災害による死亡者数が

867 人（前年比 65 人・8.1%増）と 4 年ぶりに増加となりました。製造業における安全確保は最優先事項であり、安全が損なわれた結果として起こる人的損害、物的損害、生産損失は工場運営に大きな影響をもたらすと考えます。

しかし、労働災害の発生の可能性がある場所に対し、常に監督者または監視員を配置することは人的リソース、費用の両観点から企業にとって大きな負担となります。

また、製造業における新型コロナウイルス感染症対策においても、作業エリア内における密集の対策に人的リソースを投入することの企業負担の課題があります。

これらの課題に対し 4K 監視カメラの AI 技術を活用することで、現場に専用の人員を配置することなく、危険エリアへの立ち入り検知・管理者への通知・遠隔地からの現場映像の確認や、作業エリアにおける人数検知・密検知を行うことが可能になります。本活用シーンは、ローカル５Ｇの大容量通信性・低遅延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、いすゞ自動車の藤沢工場にて 4K 画質の AI カメラ・スマートフォン型端末を利用し、遠隔地の管理者が現場の作業員の安全管理を行いました。具体的には、AI カメラによって人侵入検知および混雑度検知を行い、有事の通知の受け取りや映像確認をスマートフォン型端末で行い、業務活用における課題を検証しました。各撮影エリアについてはいすゞ自動車へヒアリングを実施し、人侵入検知については無人搬送車が往復するため人が立ち止まることが危険なエリア、混雑度検知については複数の作業者がライン作業を行い作業者が密集しやすいエリアを選定しました。

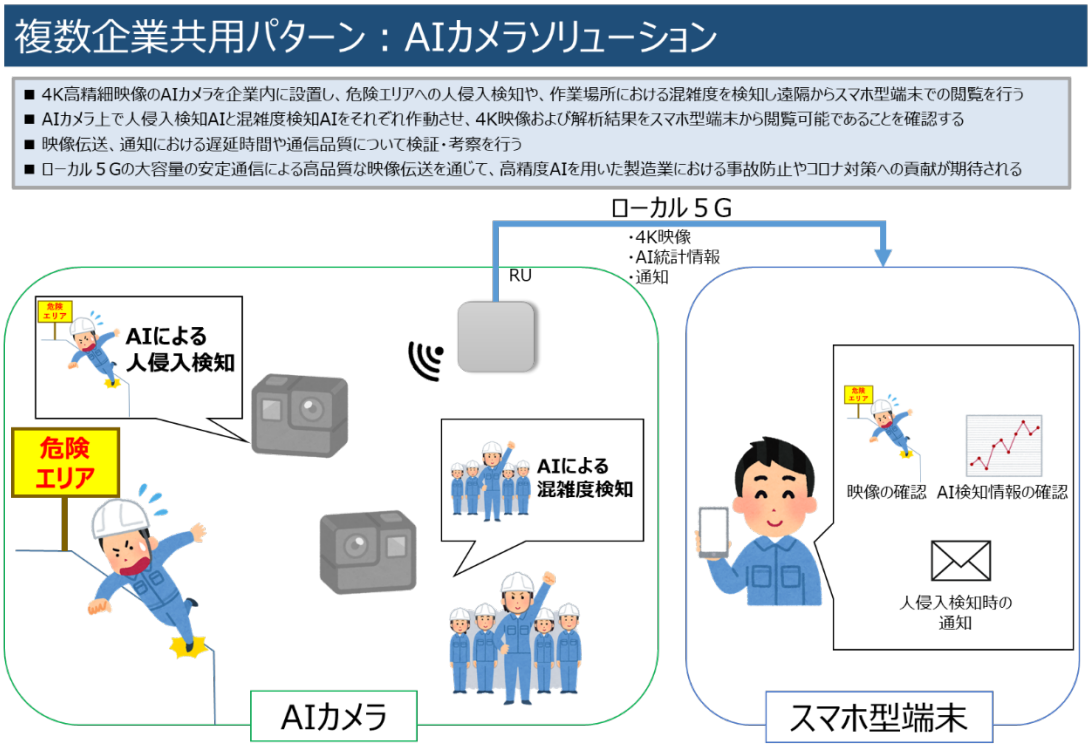


図 6-1-1 複数企業共用パターン　ユースケース概要図

(2) 業界共用パターン 大学間リアルタイム 8K 映像伝送

専門性の高い大学の教育においては、工学部や医学部の高額な精密機器・農学部や獣医学部の研究対象のように、研究に必要な設備や環境が特定の大学に限られる場合があります。また、設備だけでなく、人が持つスキルも距離的な制約を受けます。例えば、熟練医師の手術は限られた人数しか間近で見ることが出来ません。

こうした教育現場の課題に対し、遠隔教育は多様性のある学習環境や専門性の高い授業の実現等、最新かつ専門的な知識や技能に触れることのできる質の高い学習の実現に資するとして注目されています。高精細な映像をリアルタイムに配信することで、遠隔地からも精密機器の細かな箇所や有スキル者の繊細な作業を見ることが出来ます。

このような教育分野での活用を想定し、大学間のリアルタイム 8K 映像伝送の検証を行います。ローカル５Ｇの大容量通信性・低遅延性という特徴との親和性が高いと考え、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。

本検証では、高品質映像を用いた遠隔授業のユースケースを想定し、コアを共用した大学間のリアルタイム 8K 映像伝送の検証を行いました。具体的には、送信拠点に 8K カメラ・エンコーダ PC、受信拠点にデコーダ PC・映像確認用の 8K モニタを設置し片方向の映像伝送を行い、地理的な距離による映像遅延や映像品質への影響および 8K 映像伝送に必要な通信帯域について検証を行いました。検証にあたっては遠隔会議アプリ(teams)を使用する PC を 8K カメラシステムと同じ５Ｇシステムに接続し、両拠点の双方向コミュニケーションを行える環境で検証を実施しました。また、地理的な距離による影響を確認するため東北大学・東京大学・京都大学がそれぞれ一度ずつ送信拠点・受信拠点となるように、三パターンの組み合わせで検証を行いました。

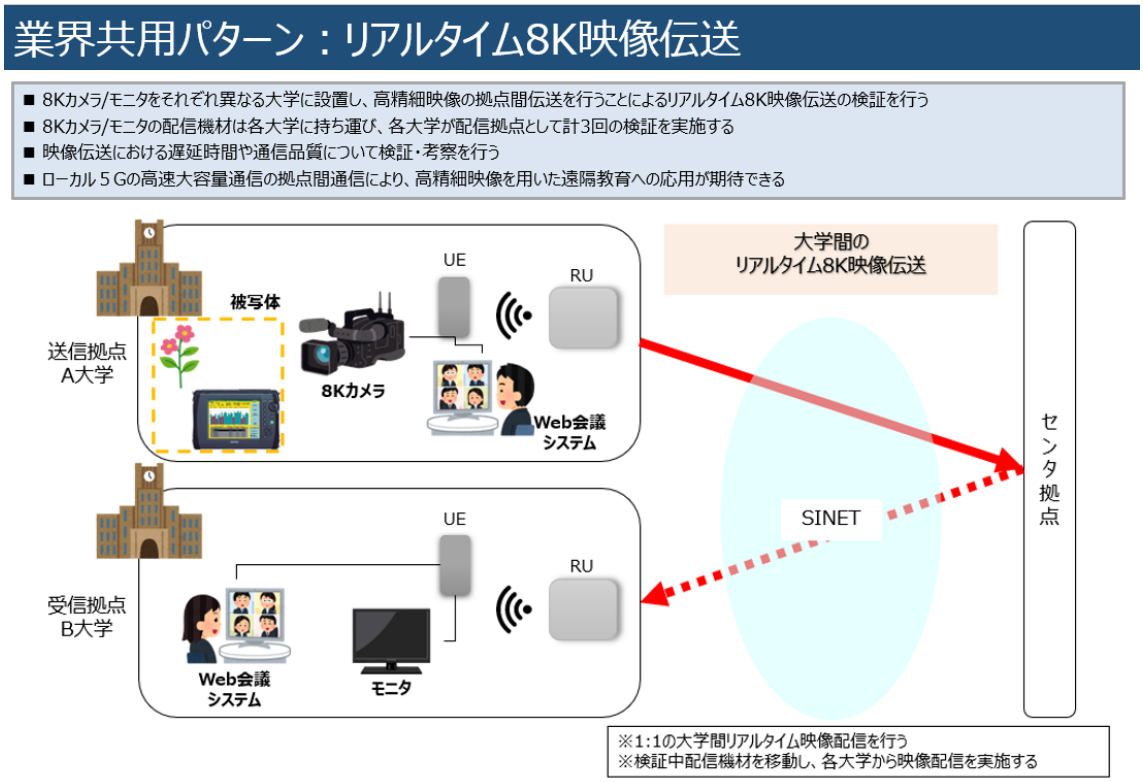


図 6-1-2 業界共用パターン　ユースケース概要図

6.2 検証環境

(1) 複数企業共用パターン

4K AI カメラソリューションでは、いすゞ自動車の工場・PBX 室の二箇所に一台ずつ無線基地局を設置しました。工場の基地局には AI カメラを人侵入検知用の二台と混雑度検知用の一台の計三台接続しました。PBX 室は管理者が待機する事務室を想定しており、PBX 室の基地局には遠隔からカメラ映像を確認する用途のスマートフォン型端末二台を接続しました。

AI カメラのリアルタイムの映像はインターネットを介さずにスマートフォン型端末から直接確認することができます。また、AI カメラの各検知 AI が取得した統計データ(例 人侵入を検知した時間、リアルタイムの混雑度レベル 等)はインターネット経由でクラウドへ蓄積され、スマートフォンからクラウドへアクセスすることで確認が可能です。本検証では映像の確認とクラウドの確認のそれぞれについて検証を行いました。また、すべての検証をセンタ UPF・エンド UPF の両方で実施し、性能に与える影響を比較しました。

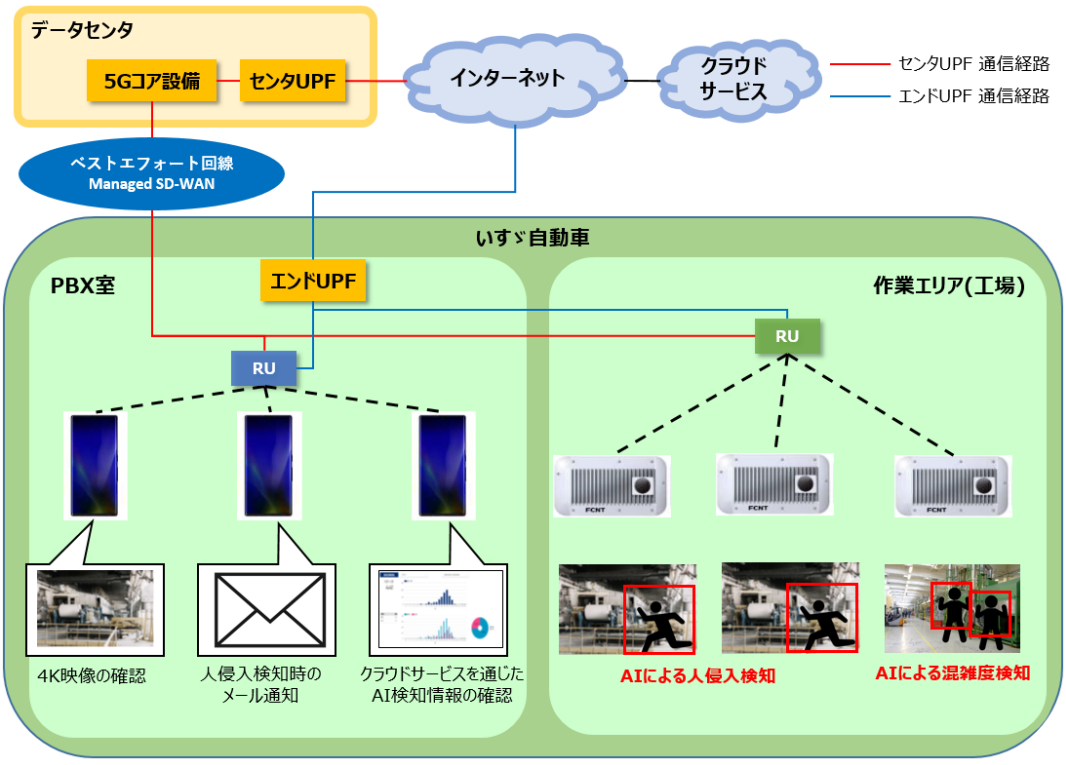


図 6-2-1 いすゞ自動車内検証構成イメージ

検証に用いた人侵入検知 AI と混雑度検知 AI の概要を以下に示します。

・人侵入検知 AI

カメラ画角内の指定した監視エリアに人侵入を検知するとメールでアラートを通知

する AI システムです。警備/監視員の負荷軽減と見落とし低減など作業効率化を実現します。本調査研究においては、工場内で人が立ち入ると危険とされる無人搬送車が往復するエリアを監視エリアとして指定しました。

・混雑度検知 AI

カメラ画角内の人による混雑状況を監視し、クラウド上でリアルタイムに状況を確認できる AI システムです。三密状態を回避し、安心安全な施設等の運営貢献を実現します。本調査研究においては、複数人の作業者が並んで作業を行い、密集の危険があるエリアにおいて本システムを使用しました。

(2) 業界共用パターン

大学間リアルタイム 8K 映像伝送の検証では、大学を送信拠点・受信拠点に分け、送信拠点と受信拠点にそれぞれ一台ずつ無線基地局を設置しました。送信拠点の基地局にはエンコーダ PC、遠隔会議アプリ(teams)を使用する PC を接続し、エンコーダ PC には 8K カメラを接続しました。受信拠点の基地局にはデコーダ PC、遠隔会議アプリ(teams)を使用する PC を接続し、デコーダ PC には 8K モニタを接続しました。
映像配信は送信拠点と受信拠点の間で実施し、送信拠点に設置した 8K カメラの映像はギャランティ回線を介して受信拠点に設置した 8K モニタから確認しました。また拠点間の音声・映像通信はインターネットを介して各拠点に設置した遠隔会議アプリ(teams)を使用する PC 間で確認し、双方向性ならびに 8K 映像伝送と音声伝送の併用についても検証を行いました。

業界共用パターンの大容量バックボーン NW 回線を活かすため、センタ UPF を用いて拠点間検証を行いました。また、業界共用パターンは複数企業共用パターンと比較して低遅延での通信が可能と R3 年度調査研究で結論付けられていることと、映像全体の遅延はエンコーダデコーダによる処理遅延が大きいと想定されることからも、本ユースケースではセンタ UPF のみを使用しました。

8K を用いたユースケースを想定し、被写体については機材と植物の二種類を選定しました。選定理由について「表 6-2-1」に示します。

表 6-2-1 8K 映像伝送被写体

被写体	選定理由
機材(通信機,解析機等)	実験用の器材や測定器などを想定した場合、エリアテスター等の表示されるパラメータ数が多い機材では、一つ一つの数字を読むために高精細な映像伝送が必要となるため選定しました。また、リアルタイムなグラフィカルデータが含まれる場合、データの変化をはっきりと追うためにも乱れのない映像伝送が必要となります。
植物	農業分野における植物等の観察を想定した場合、葉脈の筋や皮膚の下の静脈等、拡大して確認すべき細かな観察部位があるため選定しました。細かな部位を現地と同様の品質で遠隔地からも確認するために高精細な映像が必要となります。

6.3 検証内容・評価方法

(1) 複数企業共用パターン

① 人侵入検知 AI の利用

一名の検証作業員が人侵入検知 AI の監視エリアを縦断することで意図的にシステム動作させ、遠隔地の携帯端末でメール通知を受信するまでの時間および要求してから AI カメラの映像が確認できるまでの時間とその映像品質についての検証を行いました。

② 混雑度検知 AI の利用

複数の検証作業員が混雑度検知 AI の画角に入り、遠隔地の携帯端末からクラウドを確認し、状況反映にかかる時間および要求してから AI カメラの映像が確認できるまでの時間とその映像品質について検証しました。

なお、上記のいずれの検証においても映像品質については「図 6-3-1、6-3-2」に示すアンケートを用いた評価を行いました。また、各検証についてセンタ UPF/エンド UPF を用いたそれぞれで検証を行いました。

ローカル5Gコア接続・共用調査研究　AIカメラ　実証実験後アンケート

コックピット 1回目（UPFセンタ）

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. 人侵入検知カメラ①		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】AIカメラ映像の鮮明度							映像は精細だが、細かい所が見にくい
1-1	AIカメラ映像の鮮明度						
1-2	映像の遅延						
1-3	状況の確認ができるか						
1-4	システムとしての利便性						
1-5	その他ご意見等						
2. 人侵入検知カメラ②		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	AIカメラ映像の鮮明度						
2-2	映像の遅延						
2-3	状況の確認ができるか						
2-4	システムとしての利便性						
2-5	その他ご意見等						
3. 混雑度検知カメラ		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	AIカメラ映像の鮮明度						
3-2	映像の遅延						
3-3	状況の確認ができるか						
3-4	システムとしての利便性						
3-5	その他ご意見等						

図 6-3-1　複数企業共用パターンアンケートフォーマット 1

ローカル5Gコア接続・共用調査研究　AIカメラ　実証実験後アンケート

コックピット 2回目（UPFエンド）　　2022.12.15

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. 人侵入検知カメラ①		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】AIカメラ映像の鮮明度							映像は精細だが、細かい所が見にくい
1-1	AIカメラ映像の鮮明度						
1-2	映像の遅延						
1-3	状況の確認ができるか						
1-4	システムとしての利便性						
1-5	その他ご意見等						
2. 人侵入検知カメラ②		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	AIカメラ映像の鮮明度						
2-2	映像の遅延						
2-3	状況の確認ができるか						
2-4	システムとしての利便性						
2-5	その他ご意見等						
3. 混雑度検知カメラ		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	AIカメラ映像の鮮明度						
3-2	映像の遅延						
3-3	状況の確認ができるか						
3-4	システムとしての利便性						
3-5	その他ご意見等						

図 6-3-2　複数企業共用パターンアンケートフォーマット 2

(2) 業界共用パターン

① 8K 映像伝送の伝送量およびバッファの設定毎の遅延、映像品質への影響

8K の放送品質と呼ばれる 80Mbps を基準とし、40Mbps / 80Mbps / 120Mbps それぞれでエンコード PC に固定ビットレート方式を設定し、実際に無線区間を流れる伝送量と映像品質への影響を確認しました。また、デコード PC にデコード時間として設けるバッファ時間を 125msec / 650 msec の二種類を設定し、映像品質と映像遅延への影響を確認しました。

② 8K/4K の映像品質の比較

4K と 8K 映像をローカル５Ｇのネットワーク上でそれぞれ動作させ、映像品質の差分を確認しました。

映像品質に関する評価には、「図 6-3-3」のアンケートを用いました。本調査研究において大学間通信にはセンタ拠点を通ることが不可欠なため、センタ UPF のみを用いて検証を行いました。

ローカル5Gコア接続・共用調査研究　8K映像伝送　実証実験後アンケート

映像評価(8Kパラメータ変更)　　日付＿＿＿＿＿＿＿＿＿＿

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
8K映像　被写体：植物　伝送レート(　)Mbps　キャッシュ(　)msec		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】映像の鮮明度							映像は精細だが、細かい所が見にくい
1-1	映像の鮮明度						
1-2	映像の乱れの有無						
1-3	植物の細かな筋や模様が確認できるか						
1-4	その他ご意見等						
8K映像　被写体：機材　伝送レート(　)Mbps　キャッシュ(　)msec		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	映像の鮮明度						
2-2	映像の乱れの有無						
2-3	機材画面の数値や図が確認できるか						
2-4	その他ご意見等						
8K映像　被写体：植物　伝送レート(　)Mbps　キャッシュ(　)msec		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	映像の鮮明度						
3-3	映像の乱れの有無						
3-4	植物の細かな筋や模様が確認できるか						
3-5	その他ご意見等						
8映像　被写体：機材　伝送レート(　)Mbps　キャッシュ(　)msec		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	
4-1	映像の鮮明度						
4-2	映像の乱れの有無						
4-3	機材画面の数値や図が確認できるか						
4-4	その他ご意見等						

図 6-3-3　業界共用パターンアンケートフォーマット

6.4 検証結果

(1) 複数企業共用パターン

いすゞ自動車にて 4K AI カメラソリューションを利用し、4K AI カメラソリューションが正常に動作したことを確認しました。

- AI カメラ内で画像解析 AI を動作させ、指定エリア内への人侵入検知や人数カウント、混雑度推定が可能であること
- AI カメラで解析した結果をクラウド上で可視化できること
- AI カメラが人侵入を検知した場合、メール等にて予め指定した宛先にアラート通知が配信できること
- NTT 中央研修センタにてトラフィックを発生させた際も、いすゞ自動車における映像品質に影響がなかったこと

人侵入検知 AI と混雑度検知 AI のそれぞれのカメラに対し携帯端末で映像を要求してから映像が表示されるまでに要した時間と、人侵入検知 AI で侵入後からメール受信までに要した時間を「表 6-4-1」に示します。

表 6-4-1 いすゞ自動車測定結果

		映像が表示されるまでに要した時間[s]	メール受信に要した時間[s]
人侵入検知 AI	センタ UPF	1.84	18.04
	エンド UPF	1.93	14.23
混雑度検知 AI	センタ UPF	2.02	-
	エンド UPF	1.75	-

アンケートは 5 段階評価の良いものから降順に 5～1 の点数で平均スコアを算出した結果

を「表 6-4-2」に示します。いずれの結果もカメラの鮮明度が最高評価となっており、遅延時間や映像の鮮明さについてはエンド UPF の方がよい結果であることが確認できます。

表 6-4-2 いすゞ自動車アンケート結果

	アンケート項目		平均点 (センタ UPF)	平均点 (エンド UPF)
1-1	人侵入検知カメラ①	AI カメラ映像の鮮明度	5	5
1-2		映像の遅延	5	5
1-3		状況の確認ができるか	4.5	5
1-4		システムとしての利便性	2.5	2.5
2-1	人侵入検知カメラ②	AI カメラ映像の鮮明度	5	5
2-2		映像の遅延	4	5
2-3		状況の確認ができるか	4.5	5
2-4		システムとしての利便性	2.5	2.5
3-1	混雑度検知カメラ	AI カメラ映像の鮮明度	5	5
3-2		映像の遅延	4.5	5
3-3		状況の確認ができるか	5	5
3-4		システムとしての利便性	1.5	1.5

(2) 業界共用パターン

各大学において大学間リアルタイム 8K 映像伝送の検証を実施し、下記項目の確認をもって、大学間リアルタイム 8K 映像伝送が正常に動作したことを確認しました。

- 放送品質における 8K カメラ映像(80Mbps 程度)の伝送が可能であること
- スムーズなリアルタイム伝送が実現できること

三大学での 8K 映像伝送の伝送量およびバッファを変更した際の遅延、映像品質への影響に関する測定結果を「表 6-4-3～6-4-5」に示します。遅延時間はエンコーダ PC からデコーダまでの ping 結果、パケットの再送率は映像転送プロトコルの再送率をエンコーダ PC で測定したものです。

表 6-4-3 8K 映像伝送(送信拠点:東京大学、受信拠点:東北大学)

パターン	設定値			測定結果		
	画質	ビットレート [Mbps]	レイテンシー [ms]	遅延評価	映像品質評価	
				遅延時間 [ms]	パケットの再送率[%]	映像品質
1	8K	80	125	55.5	0.019	○
2	8K	80	650	60.7	0.34	△
3	8K	40	125	53.8	0.0019	○
4	8K	120	125	214.1	22.9	×
5	4K	80	125	56.5	0.057	○

※映像品質について、

○：乱れがほとんどない映像配信に毎回成功する状態
△：映像配信にたまに乱れが生じる状態
×：映像配信に毎回失敗していた状態
上記凡例は以下の結果においても同様。

表 6-4-4　8K 映像伝送(送信拠点:京都大学、受信拠点:東京大学)

パターン	設定値			測定結果		
	画質	ビットレート[Mbps]	レイテンシー[ms]	遅延評価	映像品質評価	
				遅延時間[ms]	パケットの再送率[%]	映像品質
1	8K	80	125	57.9	0.0036	○
2	8K	80	650	56.0	0.18	○
3	8K	40	125	57.5	0.00035	○
4	8K	120	125	230.7	12.3	×
5	4K	80	125	57.4	0.0027	○

表 6-4-5　8K 映像伝送(送信拠点:東北大学、受信拠点:京都大学)

パターン	設定値			測定結果		
	画質	ビットレート[Mbps]	レイテンシー[ms]	遅延評価	映像品質評価	
				遅延時間[ms]	パケットの再送率[%]	映像品質
1	8K	80	125	69.8	0.000050	○
2	8K	80	650	65.4	0.0012	○
3	8K	40	125	74.2	0.0	○
4	8K	120	125	238.3	18.6	×
5	4K	80	125	73.6	0.0013	○

続いて映像品質に関するアンケート結果を「表 6-4-6、表 6-4-7」に示します。アンケートは 5 段階評価となっているため、評価の良いものから降順に 5～1 の点数で平均スコアを算出しました。パターン 1，2 を比較すると本検証においてはいずれの被写体においてもレイテンシーを変えることによる映像品質への影響がないことが確認できました。また、アンケートの平均点は「表 6-4-3～表 6-4-5」の映像品質の評価と概ね同じ傾向であることが見て取れます。

表 6-4-6 三大学アンケート結果(被写体：植物)

パターン	設定値			評価	
	画質	ビットレート[Mbps]	レイテンシー[ms]	アンケート項目	平均点
1	8K	80	125	映像の鮮明度	4
				映像の乱れの有無	4
				植物の細やかな筋や模様が確認できるか	5
2	8K	80	650	映像の鮮明度	4
				映像の乱れの有無	4

				植物の細やかな筋や模様が確認できるか	4
3	8K	40	125	映像の鮮明度	4
				映像の乱れの有無	4
				植物の細やかな筋や模様が確認できるか	4
4	8K	120	125	映像の鮮明度	2
				映像の乱れの有無	1
				植物の細やかな筋や模様が確認できるか	2
5	4K	80	125	映像の鮮明度	4
				映像の乱れの有無	4
				植物の細やかな筋や模様が確認できるか	4

表 6-4-7 三大学アンケート結果(被写体：機材)

パターン	設定			評価	
	画質	ビットレート[Mbps]	レイテンシー[ms]	アンケート項目	平均点
1	8K	80	125	映像の鮮明度	4
				映像の乱れの有無	4
				機材画面の図や数値が確認できるか	4
2	8K	80	650	映像の鮮明度	4
				映像の乱れの有無	4
				機材画面の図や数値が確認できるか	4
3	8K	40	125	映像の鮮明度	4
				映像の乱れの有無	4
				機材画面の図や数値が確認できるか	4
4	8K	120	125	映像の鮮明度	1
				映像の乱れの有無	1
				機材画面の図や数値が確認できるか	2
5	4K	80	125	映像の鮮明度	3
				映像の乱れの有無	4
				機材画面の図や数値が確認できるか	3

6.5 考察

(1) 複数企業共用パターン

(センタ UPF / エンド UPF の比較)

表 6-4-1 の測定結果に示すとおり、人侵入検知 AI と混雑度検知 AI においてセンタ UPF とエンド UPF による映像表示までにかかった時間に差はほとんどありませんでした。一方で侵入検知 AI におけるメール受信に関してはセンタ UPF よりもエンド UPF の方が短い時間で受信できる結果となりました。この結果について、映像の表示は携帯端末からカメラへ直接アクセスするため UPF の位置にあまり影響を受けない一方で、メール受信はインターネットを経由する必要があるため、エンド拠点から直接インターネットへ接続できるエンド UPF の方が短い結果が得られたと考えられます。また、映像品質についてはセンタ UPF / エンド UPF で差が見られませんでした。

(コアを共用した状況での利用について)

本検証中にいすゞ自動車とコアを共用した NTT 中央研修センタ拠点で通信のトラフィックを発生させましたが、映像の品質への影響は見られませんでした。R3 年度の調査研究における報告と同様、コアおよび CU を共用した本調査研究の構成においても、別の拠点に対す通信影響はないと考えます。

(2) 業界共用パターン

(映像の遅延と地理的距離について)

表 6-4-3～表 6-4-5 に示すとおり、拠点間の映像遅延は東北大学-東京大学間が最も小さく、東北大学と京都大学間が最も遅延が大きい結果となりました。この結果について、本調査研究の構成では大学間通信は東京に存在するセンタ拠点を経由するため、性能検証のセンタ UPF までの遅延時間(表 5-3-4-①-2)の各大学の測定結果を足した結果と概ね一致しています。

(エンコーダ PC デコーダの設定別の映像品質について)

表 6-4-3～表 6-4-5 のパケット再送率および表 6-4-6、表 6-4-7 のアンケート結果のまとめより、8K 映像についてビットレート 80Mbps レイテンシー125ms の設定(パターン 1)でパケット再送がほとんど起こることなく十分な品質の映像が送信できたことが確認できました。80Mbps のビットレートは 8K 放送でも用いられる設定であるため、8K の品質を十分に活かした結果が得られたと考えます。

また、ビットレートを 80Mbps のままデコードにかけるレイテンシーを 650ms に変更した場合(パターン 2)、デコードの処理時間が増えた分遅延時間が増えたというアンケート結果が得られた一方で、映像の品質には影響がありませんでした。この結果から本調査研究の撮影環境においては 125ms の設定で問題なくデコードが可能であるといえます。そのため残りの検証は 125ms で実施いたしました。

次に、ビットレートを 40Mbps に落とした場合(パターン 3)、映像に乱れはないものの 80Mbps に比べて映像の鮮明さが下がる結果となりました。これはエンコーダ PC で 40Mbps まで圧縮を行った結果映像品質に劣化が生じたためと考えられます。

逆にビットレート 120Mbps まで上げた場合(パターン 4)について、本調査研究で用いた RU の上り方向のスループットの上限は 120Mbps 程度であるため、映像が流れる想定でしたが、実際は映像が固まり全く流れない結果となりました。これについてエンコーダ PC でパケットキャプチャを実施したところ、実際には 125Mbps～130Mbps ほどのパケットが流れており

その結果パケット再送が頻発しうまく映像として組み立てられなかったと考えられます。この挙動についてエンコーダ製品ベンダーへ確認したところ、固定ビットレート設定にしていても映像に人が映りこむ等で動きが大きい場合 120Mbps を超える場合がある、と回答を受領しました。実運用においてはその挙動を十分考慮した上で、RU の上り方向スループットの上限値よりも低い値で固定ビットレートの設定を施すことが必要であると考えます。

最後に、ビットレート 80Mbps で同じカメラで 4K の画質設定を行った場合(パターン 5)について、8K と 4K の品質に対する感じ方には個人差がある結果になりました。しかし、モニタに近づき植物の葉脈や機器の細かな文字を確認された方からは 8K の方がよりよく見える、という回答を得られました。

(大学間通信の実現について)

本調査研究では業界共用パターンの大容量のバックボーン NW を活かし、センタ UPF を経由する経路で 1 対 1 の拠点間の通信を行いました。この構成について、1 対多の通信を行う場合と、大学間を直接つなぐ経路が存在する場合についてそれぞれ考察します。

本調査研究では送信拠点のエンコーダ PC から受信拠点のデコーダまでエンド to エンドの通信を行いましたが、一つの送信拠点から多数の受信拠点に配信をする構成を考える場合は、センタ拠点に映像配信用サーバを設置し各受信拠点がサーバまで映像を要求しにいく構成が望ましいと考えます。これにより送信拠点の上り方向の通信量が 1 対 1 の場合と同程度まで抑えられるためです。この構成を考えた際もエンド UPF を利用する利点はなく、センタ UPF の利用が推奨されると考えます。

次に、L2VPN 等大学間を直接つなぐ経路が存在する場合、各大学のエンド UPF を使用する形をとることでセンタ拠点を経由する本調査研究よりも遅延が低く抑えられる可能性があると考えられます。しかし、上述のとおり 1 対多の配信をする場合は映像配信用サーバをいずれかの拠点に設置しないと送信拠点の上り方向の通信が拠点数分必要になってしまうため、大学間を直接つなぐ経路を利用する場合はいずれかの大学に映像配信用サーバを設置するか送信拠点の上り方向の通信が RU の上限を超えないよう受信拠点数を減らす等の対処が必要となると考えます。

7. 関係者ヒアリング

7.1 ヒアリング概要

ユーザ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、ヒアリング等の調査を通じて、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。本実証では複数の団体にヒアリングをし、コア共用におけるニーズ・課題の整理を行いました。

(1) ヒアリング方法

関係者のヒアリングについては以下のとおり実施しました。

表 7-1-1 ヒアリング方法

区分	内容
調査対象	2022 年 10 月～2022 年 12 月
調査方法	オンラインによるヒアリング調査を実施。 事前調査：５Ｇとの関わり方等の把握および企業・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

(2) ヒアリング対象およびヒアリング内容

本実証ではコア共用におけるニーズや課題の整理のため以下「図 7-1-1 ヒアリング項目」のとおりヒアリングを行いました。

区分	項目	No.	ヒアリング内容
L5G 全般	ユースケース	1	L5G事業を進める中で、注力している分野やサービスはありますか。
	実装状況	2	実証事例、および商用化している事例があれば、教えてください。
	課題	3	L5G事業を進める中で、課題と感じていることがあれば、教えてください。
相互接続	効果	4	相互接続に係る、貴社プロダクト、ビジネス領域について、教えてください（P2ポイント①ご参照）。また、貴社のユーザへの訴求ポイントがあれば、教えてください。
	実装モデル例	5	相互接続に係るニーズやユースケースがあれば、教えてください（P2ポイント②ご参照）。
		6	相互接続を実現するにあたって、課題意識（技術/制度/運用面等）や、改善・対応方法等があれば、教えてください（P2ポイント②ご参照）。
	相互接続に必要なパラメータ、環境	7	SIer等が参照することが望ましい項目・パラメータについての定義や記載範囲について、ご意見などがあれば、教えてください。
	相互接続不良時の対応	8	相互接続が不可となった場合の対応について、原因の切り分け、改善方策の取り方など、SIer等で把握しておくべく点などご意見があれば、教えてください。
	各種運用規定	9	接続不良時を見据え、ユーザ・SIer・ベンダー等の運用・連携体制の在り方について、ご意見があれば、教えてください。
コア共用	効果	10	コア共用に係る、貴社プロダクト、ビジネス領域について、教えてください。また、貴社のユーザへの訴求ポイントがあれば、教えてください。
	実装モデル例	11	コア共用に係るニーズやユースケースがあれば、教えてください。
		12	コア共用を実現するにあたって、課題意識や、改善・対応方法等があれば、教えてください。
	セキュリティ要件	13	コア共用に係るセキュリティリスク及び対策（利便性や運用要件とのバランス等）について、課題感やご意見があれば、教えてください。
	運用要件	14	コア共用に係る運用体制及び対策（要因特定、責任分界点、復旧方法等）について、課題感やご意見があれば、教えてください。
全体	その他	15	『技術的手引書（仮称）』に記載すべき事項などご意見があれば、教えてください。

図 7-1-1 ヒアリング項目

7.2 ヒアリング結果

(1) ローカル５Ｇ全般

①課題意識

対象者	ヒアリング結果
ベンダー	✓ ローカル５Ｇを自分たちで構築・運用できるスキルセットがユーザ側にいない。民間企業が自分たちでローカル５Ｇを運用していくための**技術・経験が圧倒的に不足している**。 ✓ ローカル５Ｇで他の NW を置き換えるのではなく、他の NW と共存しながら、**様々なユースケースに総合的に応えていくアプローチが必要**。そのフィールド全体の最適化を考えて、WiFi、有線も含めて、最適なアクセス手段を**統合的な運用管理面も含めて提供していく**必要がある ✓ ビジネス観点では、仮説までできていても、実装となったときに、**コストモデルが課題になる**
SIer	✓ **免許取得申請の手続きが煩雑である**。特に国内では、免許制であることが足かせになっていると感じている。**登録制にしてもらうだけで煩雑さが改善するのではないか**。 ✓ 現状は垂直統合モデルがメインであり、**相互接続は課題である**。パーツはバラバラにできるが、各社相互接続する義理がないため、垂直統合モデルを各社が進められている印象。**3GPP がネックになっている**と考えている。現状では、3GPP の規格をすべて満たさないと相互接続できず、インテグレーションを含めて大きな重荷になっていると感じる。

	✓ 技術が特殊でありエンジニアが希少である。 ✓ 商用化するにあたっての**最適なユースケースが見つけられておらず**ユーザへの訴求が出来ていない
通信事業者/CATV	✓ 導入コストが、5GC/基地局/端末共通の課題である。端末において、実証で数台購入する程度ならよいが、商用でもう少し規模が大きくなると、トータルコストが上がってしまう。 ✓ **制度面や免許申請が複雑**で、導入企業（ユーザ）単体での取扱いが難しい。**SIer やサービス事業者等の支援が必要**になる。 ✓ ユースケースも課題である。例えば工場だと、同時多数接続・低遅延といった Release 16 以降に見込まれている機能で実現したいというニーズがある中で、現状対応できる製品がないことが課題。 ✓ 高精細映像が将来当たり前になるのは間違いないと考えるが、現状は「本当に必要か」を問われてしまう状況。高精細映像が、大きなペインポイントに対する課題解決となるケースは少ない。他方で、価格が抑えられれば、大きなペインポイントでなくても導入が進むようになるのではと感じる。

②ユースケース・実装事例

対象者	ヒアリング結果
ベンダー	✓ **製造業、交通、運輸、エネルギー、公共、ISP 事業者**、等など幅広い市場分野に提供。また、自社利用の企業様だけでなくローカル５Ｇ通信サービス提供を行う事業者に対しても提供。 ✓ **教育を含む公共・行政サービス、鉄道・空港・港湾**といった社会インフラ、製造業（スマートファクトリー）、建設業（i-Construction、無人化施工等）をターゲットにしている。 ✓ ソリューションとしては、**映像や仮想空間を活用したもの**に注力している。
SIer	✓ **製造業やヘルスケア**に注力している。ユーザは**電力系やインフラ事業者**が多い印象。 ✓ ソリューションとしては**遠隔作業支援、AGV、AGF、ロボティクス等**に注力している。
通信事業者/CATV	✓ ユーザーとしては**自治体や大学、製造業**が多い印象。ローカル５Ｇ自体が Release 15 ベースの機能実装として大容量伝送がメインであるため、**映像系のソリューション**が多い ✓ ケーブルテレビ業界でかねてより掲げているテーマである FWA に注力している。

(2) 相互接続におけるニーズおよび課題

対象者	ヒアリング結果
ベンダー	✓ 相互接続という観点で重視しているのは、自社基地局と他社端末間の接続。NW 機器をマルチベンダーで接続したいというユーザはそんなにいな

	い。ユーザは、安定的に稼働し、運用が簡便であれば、基本的にはNW機器の細部にこだわりを持たない印象。 ✓ 相互接続として可能性があるのは、**5GC/UPF と CU/DU 間**。当社でも相互接続の取組みを行っている。5GC/UPF 間もあると思うが、ここは同じベンダーの装置を使うのが基本ではないかと思う。**端末は、3GPP 準拠のものであれば、基本的につながる**認識。これまでも様々な端末を接続している。 ✓ 技術面では、**3GPP に準拠していれば**、時間はかかるかもしれないが、相互接続は可能（試験をすればつながる）と思う。運用面では、EMS、NMSがベンダー毎に異なること。上位での監視・管理をどう統合するか、が課題になる。 ✓ 運用面の負荷を踏まえると、**民間企業において相互接続へのモチベーションは現時点ではない**。通信キャリアやCATV事業者といったサービス提供事業者は、**サービスとして提供してスケールさせる前提で、相互接続を検討する**というケースはあると認識している。 ✓ **5GC/基地局間の接続検証実績の情報がオープン**になると、SIer としては機器の選定がしやすくなると思う。 ✓ ユースケースに応じて様々なタイプの端末導入のニーズがあることから、**基地局/端末間での相互接続が最もニーズがあり**、かつ実現性の高いインターフェースと考える。 ✓ 相互接続性の担保（企業やSIerによる接続検証の実施）、異なるベンダー設備それぞれに必要な管理システムの導入、不具合発生時の切り分け作業、将来の機能導入時やソフトウェア更新時のたびの相互接続検証、などの観点からマルチベンダー化には課題やデメリットも多いと考える。 ✓ 基本的には検証してつながるが、サービスとして運用していく中で問題があったら、**『誰の責任で対処していくか』**という論点が出てくる。ユーザとしては、サプライヤーにまとめて保証してほしいと期待するが、実際はユーザ側である程度解決しないといけない部分が出てくるため、**ユーザが安心して運用する形が取りにくくなってしまう。**
SIer	✓ 製品やお客様要件に依存するがローカル５Ｇインフラ一式を SI することが役割と考えているため、**全コンポーネントが自社のビジネス領域**である。 ✓ **他メーカ製品を相互接続したいというニーズは特に出てきていない**。相互接続は目的でなく手段であると考えられるため。もし、相互接続により安価且つ高付加価値なローカル５Ｇインフラを構成できるようになれば、手段として求められてくると考える。 ✓ 現状、5GC/UPF/基地局間において、他社製品と接続している実績はない。端末だけは、相互接続の検証を行っている。**端末部分については、技術面・ビジネス面の両面から、相互接続を進めている**。 ✓ マルチベンダー構成の場合、**RU メーカが複数の DU メーカと相互接続した結果**をもって工事設計認証を取得する必要があるため、**RU メーカ側に負荷**がかかってしまう。 ✓ マルチベンダーなコンポーネントを SI することで **SI 費が増加する**、ロー

	カル５Ｇシステム全体の品質が下がる、或いは品質低下を防止するため、不具合時の切り分けが複雑化するために保守・運用費が増加する可能性がある点も考慮のうえ、ケースバイケースで適用シーンを考える必要がある ✓ コアを共用するとコストが下がるという目論見と思うが、コストが下がるのは機器費だけと思われる。サプライヤー側が相互接続をきちんと主導していかないとユーザは安心して使うことができない。機器費をどう下げるかという観点と、それが安定して使えるかという観点の、両方を実現していく必要があると考えている。パラメータをメーカが開示してくれるというよりも、メーカ間で相互接続できた実績をどんどん公開してくれると、そもそもパラメータを利用者が気にしなくてよくなる。それぞれの機器がどういうスペックの機能実装をしているかが明確である必要がある。現状は、O-RAN 準拠といっても、いざ組み合わせてみようとなったときに、誰も保証してくれない世界観であり、それでは困る。せめて、どういう機能をインターフェースとして実装しているか、直近ではフロントホールの部分の相互接続がメインになると思うので、Open front interface に則り試験ができている等の試験結果を開示して頂きたい。その結果がオープンになっていれば、机上でこの機器とこの機器はつながりそうという検討ができ、その上で、Plug Fest のような場で接続できた結果・実績がある等、様々な土台があった上で、相互接続にトライできるものだと考えている。 ✓ 相互接続不可とならないようにするために、ベンダー/メーカ間の協力サポート体制はまず大前提として確立する必要がある。SIer としても、稼働担保を取るように動くが限界がある。そのため仕組み化は必要と考える。 ✓ 各種運用規定としては、①メーカ推奨の製品選定の実施、②相互接続構成を組み入念な検証の実施、③予め不具合発生時の連絡フローをメーカ含めて定めておくことが必要。
通信事業者/CATV	✓ ユーザ側から「相互接続したい」と言及されることはない。当社が提案する段階で、ユーザニーズに合わせて、複数メーカ製品を組み合わせるか、同一ベンダーで提案するか、を検討する。そのため、ユーザからは、導入コスト安くする方法はあるか、こういうことをやりたいが実現できるか、といった形での問い合わせが多い。 ✓ 5GC や基地局においても、異なるベンダー間の相互接続のニーズはあると考える。上位（監視機能や 5GC）になるほど、複数の垂直統合モデルを別々で持つことは非効率である。また、基地局 CU/DU/RU は、ユースケースごとに最適な機種が変わってくる。したがって、同じベンダーですべてを提供できるとは限らないため、将来的には、基地局と 5GC 間で、基地局は複数のベンダー、5GC は 1 つのベンダーというような相互接続のニーズは出てくると考える。 ✓ 各メーカが積極的に取り組んでいる動きが見えていないのは課題と感じている。当社は 5GC/基地局の利用者、ローカル５Ｇサービスの提供者として、各装置の組み合わせがベンダーロックインになっていると、ユーザへの提案の幅が狭まるので、相互接続に係る技術面、例えば相互接続性試験のガイドライン等の整備が必要になってくると感じている。 ✓ 各メーカそれぞれで、動作確認ができている 5GC/基地局/端末の情報を公

	表してほしい。 ✓ SIer が把握すべき情報としては、**3GPP 等のガイドラインに規定されているインターフェースは最低限把握**頂く必要がある。その中でも、セル ID、トラッキングエリアのような、相互接続する上で共通的に必要なパラメータについては、理解を頂く必要がある。**異なるローカル５G のシステム間で干渉が及ぼすパラメータもある**ので、こちらも理解頂く必要がある。 ✓ 無限にあるパラメータの中でローカル５G の観点で最低限担保が必要なパラメータは何か、相互接続する際の定量的な合格基準は何かなど、**明確なルール作りがスタートライン**として必要と感じる。

(3) コア共用におけるニーズおよび課題

対象者	ヒアリング結果
ベンダー	✓ コア共用モデルニーズは**通信キャリアや CATV に高いニーズがある**と考える。 ✓ 運用体制としては、**RU と端末の責任分界点がはっきりしていない**点は課題。マルチベンダー化が進む中で、マーケット全体としての課題が出てくるのではないか、と感じている。 ✓ クラウド型は、コストが下がるイメージを持たれるが、**クラウド利用料、WAN 回線料がネック**になっている。 ✓ 地域共用型では、地域・行政サービスの視点で見ると、固定 NW がないことが課題。実装を考えたときに、固定 NW が必要になり、その回線を敷設するとなると、投資コストがかかってしまう。 ✓ 多くの企業ユーザを共通の５G コアに収容することから、**セキュリティ面での担保、メンテナンス時のシステム停止**などが全ユーザに波及することの認識、対策が必要と考える。 ✓ **放送と５G は親和性が高く**、期待される分野である。ユースケースとしては、系列局等の複数の拠点に RAN を設置して、5GC はクラウドで共用するケースがある。
SIer	✓ コア共用ニーズはこれまであまり出てきていないが、**複数拠点を持った企業が商用化を行う場合にはコア共用ニーズは上がる**と考える。 ✓ ５G のドメインからデータを切り出す出口である **UPF をどこに置くか**、がアーキテクチャーを考える上でのポイントになると考えている。ローカル５G においては、UPF をローカル拠点に置きたいユースケースが圧倒的ではないか、と考えている。遅延の考え方や、データをどう扱いたいか、によって UPF の場所が決まってくる。MEC についても、UPF の近くにないとデータ処理ができないので、**MEC も UPF と同じ考え方で、ユーザに近いところ（ローカル拠点）にあるのが望ましい**と考える。 ✓ 様々なコンポーネントを安く組み合わせるというのは理想であるが、メーカからすると、必ずしも検証環境を持っているわけではない中で、他社製品を使う義理はなく、SIer が担保する形になることが想定される。そうなると、今後 **SIer 側にメーカ以上の技術力が必要**になるかもしれない。メ

	ーカ側からの**ログの開示は不可欠である**。 ✓ コア共用を行う際にはそれなりの大規模向け製品が必要となり初期投資が莫大となる。現在のようなローカル５Ｇ黎明期においては、費用回収の見込みが読みづらく、二の足を踏むケースが考えられる。スモールスタートを行いながら**徐々にスケールできるような製品が期待される**。 ✓ 広範囲に渡るため**障害時の要因特定に向けた切り分け手順、責任分界点**、なるべく他のユーザや拠点に影響を及ぼさないような復旧方法を入念な検討・検証を繰り返したうえで整備する必要があると考える。
通信事業者/CATV	✓ セキュリティについては、どういうサービスモデルを実現するか次第であるが、**UPF/MEC を置く場所による**と考える。 ✓ セキュリティについて、セントラルコアとして 5GC を保有した場合に、マルチテナントで提供する形になるため、**UDM が共用になる**。つまり、基地局で報知される PLMN は同じ情報になる。A 企業/B 企業といった別の企業が 5GC を共有して利用する場合、SIM の情報として同じ PLMN が見えてしまえば、基地局にアタッチしようとする動作はするため、そういった点に対する **IMSI のトラッキングや暗号化**も含めて考える必要がある。 ✓ 5GC の共用は、すでに**ニーズ（＝コストメリット）**がある。UPF に関しても、同様の文脈でニーズはあると考えている。

(4) 考察

上記のヒアリングよりコア共用、相互接続ともに一定のニーズはあるものの実装に向けては課題を感じているベンダーや SIer、通信事業者が多いことが分かりました。

相互接続については各ベンダーそれぞれで、動作確認ができている 5GC/基地局/端末の情報を公表してほしいという声が多数ありました。今後推進していく上では、情報の公表が必須になると考えます。また、不具合発生時の対応についても責任分界点の明確化やルール作りが必要になります。これらのルールが不明瞭な場合、ユーザ側での負担の増加が懸念されます。そのため、各社での連携体制が必須となります。

コア共用についてはコストメリットが見込めるため、複数拠点を持った企業や CATV などには一定数のニーズが想定されます。UPF や MEC の設置場所についてはユースケースに応じて検討が必要になります。また、今後推進していく上では、運用体制(責任分界点等)やセキュリティ面が課題に挙がりました。多くのユーザを収容することが想定されるため、不具合発生時の影響も大きくなります。広範囲に渡るため障害時の要因特定に向けた切り分け手順、責任分界点、なるべく他のユーザや拠点に影響を及ぼさないような復旧方法を入念な検討・検証を繰り返したうえで整備する必要があると考えます。

本実証においては相互接続、コア共用ともにユーザ向け、SIer 向けの手引書を作成しました。相互接続については R3 年度から 2 年間の実証で複数のパターンの検証をしました。検証結果については接続の可否や改善方策を集約し、ガイドラインとして標準的な相互接

続要件を手引書にまとめています。今後、ベンダーやSIer等が相互接続を進めていくうえで手引書を参考に推進していくことが可能と考えます。

コア共用においても相互接続同様に各ベンダーや事業者が課題に感じているセキュリティ検証等を実施した結果を手引書に取りまとめています。そのほかにも運用面や機能面、性能面等での検証を基にした考察を記載していますので、コア共用モデルを推進する際には手引書を参考にすることが有効だと思います。

8. まとめ

相互接続およびコア設備の共用については、利用者側（企業・団体側）および提供側（ベンダー・業界団体・SIer 等）共に一部のユースケースによっては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

コア 2 種、基地局 3 種、端末 6 種を組み合わせた 36 パターンから、同じベンダーの組み合わせとなる 1 パターンを除いた 35 パターンでの相互接続検証を実施しました。検証は事前に 3GPP で規定されるパラメータの設定を施した上で実施しました。

以下の措置を施すことで、全てのパターンで相互接続を実現することができました。

・相互接続を実現するために実施した措置

①自由設計パラメータへの措置：コア側で“InitialContextSetupRequest”メッセージ内の当該フィールドを削除

②自由設計パラメータへの措置：コア側で“PDUSessionEstablishmentAccept” メッセージ内へ当該フィールドを追加

③3GPP リリースバージョンによるシーケンスの差異：コア側の“NASSecurityModeCommand”内の構成を V15.3 以降のシーケンスに対応する措置

④ネットワーク関連パラメータの措置：ローカル５Ｇコア、基地局の MTU を WAN 回線のパス MTU を下回るよう設定

しかし、接続後の通信試験では 2 パターンの準同期 TDD3 での通信結果が不良となりました。解析の結果、基地局が端末からの無線通信の正常に受信することができず、通信のエラーが多数発生してしまっていることが原因と判明しました。準同期 TDD3 は端末として未サポートの設定であったため、相互接続時は装置ごとの各機能のサポート状況を確認することで、こうした動作不良を未然に防ぐことができると考えられます。

本調査研究を通して、3GPP で規定されるパラメータの設定に加えて、3GPP 上自由設計となっているパラメータや準拠する 3GPP のリリースバージョンの差異、機器を導入するネットワーク環境に合わせたパラメータの調整が必要となることが判明しました。相互接続に必要なパラメータについて判明した検証結果や知見は、併せて作成した相互接続の技術的手引きへ反映することで、今後に相互接続を企図する一般ユーザや SIer が活用することができるものといたしました。

（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/CU 共用を進めるには、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。

本調査研究では様々なユースケースについて、推奨されるシステム形態や回線種別等について検証しました。

コア/CU 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はコアを共用することによる対応が求められるものの、適切な UPF 配置や回線種別を選択することで対応が可能であることが分かりました。

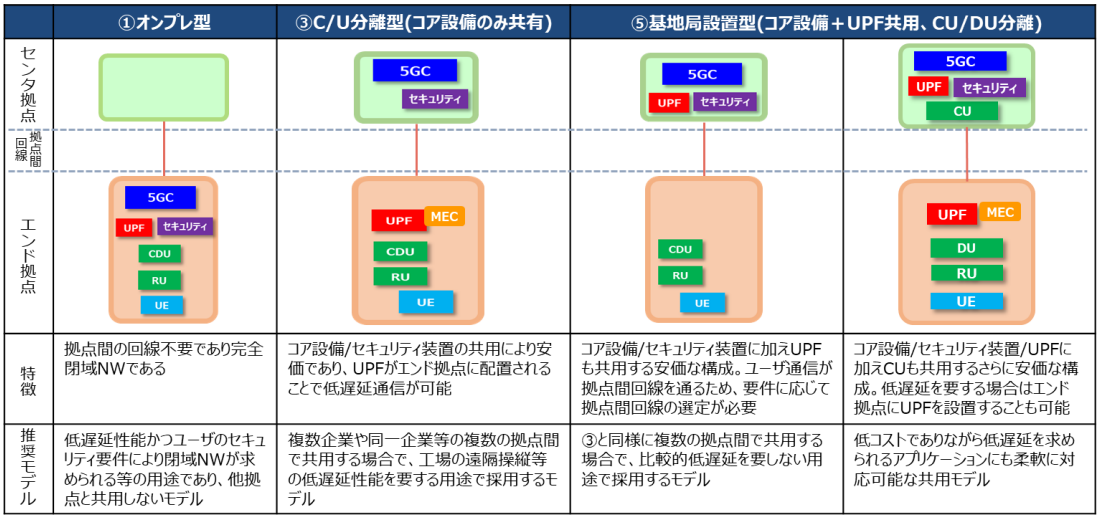


図 8-1 コア共用における共用形態

（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、コアに加えて CU も共用する形態を取り、性能面、機能面、セキュリティ面、監視運用面から検証しコアおよび CU 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

本調査研究ではコアのみ共用した環境およびコア＋CU を共用した環境を構築し、それぞれの環境において共用によって生じる影響を確認しました。具体的にはスループットおよび遅延時間といった通信の伝送性能、複数の UE を同時接続する場合の要件、コア等における CPU 利用率等の消費リソースの要件並びに UE 認証時間への影響について、コア等を共用した環境で広域回線の種別やセンタ UPF/エンド UPF といった環境の違いによる測定結果を比較、検証しました。

伝送性能についてはコア等を共用した環境によるスループット等の劣化は見られませんでした。同期方式においても準同期方式においてもローカル５Ｇシステムの伝送性能を十分に発揮できるといえます。ただし、広域回線の種別によるスループットの制限または広域回線の種別あるいは拠点間の距離による遅延時間への影響については留意すべきものと考えます。また UE 多接続、消費リソースおよび UE 認証時間については製品仕様に依存するものであり、コア等を共用した環境による影響は見られませんでした。

こうした結果から、コア等を共用した環境は技術的に実現可能であると考えます。ただし、構築にあたってはユースケースの所要性能から伝送性能の要件を定め、適切な広域回線および拠点の選定が必要であると考えます。

② 機能面

コア等を共用する環境ではシステムの運用や管理を拠点ごと（ユーザごと）に分けて実施できることが求められます。本検証では２社のベンダーの異なるコア環境を構築し、SIM 認証管理、端末情報管理等といった顧客情報管理機能、トラヒックモニタリング機能および在圏管理機能について実装を検証し、コアによる統合的な運営および拠点ごとの情報管理が実現できることを確認しました。

混在するユースケースに対応し自由度の高い利用方法を実現する機能として、同一の拠点内で UE ごとに異なる UPF を通信相手として選択可能である機能を有することを確認しました。本機能によってユーザのデータをセンタ拠点に集約したいユースケースではセンタ UPF を通信相手として設定し、低遅延を要求するユースケースの場合はエンド UPF を通信相手とする等、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 を選択することが可能です。

また、大容量伝送や低遅延通信等、柔軟な NW 設計を可能とするネットワークスライス機能の実用性を検証しました。eMBB/ URLLC それぞれの特性を確認し、URLLC はセンタ UPF で性能を発揮できない可能性が見られました。コアを共用した環境でのスライス設計の際には、センタ拠点への回線によるトラヒックへの影響も考慮すべきと考えます。ネットワークスライス機能については今後の開発・検証による実用性の向上に期待したいと考えます。

③ セキュリティ面

コア/CU を複数ユーザで共有し異なる拠点に設置する構成では、コア-基地局間または CU-DU 区間が遠隔での通信となり経路上での盗聴のリスクがあります。R3・R4 年度の調査研究を通して、拠点間通信を暗号化できる仮想アプライアンス製品を導入することで、コア/CU 共用環境下においてもコストを抑えながら拠点間のセキュリティ対策が可能と考えられます。

また、R4 年度は無線と端末間のセキュリティについて検証を行いました。検証の結果、セキュリティ機能を持つ SIM を利用し UPF の手前に監視装置を導入することで、拠点毎端末毎にセキュリティポリシーを適用し、端末からの不正な通信や SIM スワッピング等の攻撃に対する端末のセキュリティ対策を行うことが可能と考えます。

また、インターネットの出口となる UPF の N6 のインターフェースについては、コア共用環境特有のものではなく、一般のインターネット環境同様 UTM 等でインターネットからの攻撃を防ぐことが可能です。

これら R3・R4 年度の調査研究を通して、コア/CU 共用環境下において想定しうる各セキュリティホールに対し網羅的にセキュリティ検証を行うことができました。今後、ユーザや SIer 等がセキュリティを担保しながらコア共用を進めていくために参考とすべきセキュリティ機能について手引書にまとめています。

④ 監視・運用面

自治体や業界団体での共用ケースなど、ローカル５Ｇシステムに対して電気通信事業者等による運用監視が行われないケースを想定し、ローカル５Ｇシステムに起こりうる障害事例について実際の環境下で再現し、有効な監視体系について検証しました。システムの維持・運用のため必要な正常性の監視や障害が発生した場合の原因切り分けについて、コア共用の環境下においてローカル５Ｇシステムに起こりうる障害事例を再現し、障害発生検知および正常性の確認のため「KPI」を、障害原因切り分けのため「サブ KPI」を設定しました。本検証では Alert の監視および通知の機能を有するシステム監視ツールサーバをセンタ拠点に設置し、コア共用での監視運用体制の基本形として SIer がシステム監視者となる想定で実施しました。

本検証によって、KPI としてシステム全体の正常性監視に有効な RU および 5GC の監視、コア等の共用下で不可欠な WAN 回線の障害検知に有効な VPN セッションの監視、システム同期状態という潜在的な障害発生の検知に有効な GMC の監視が有効であること、サブ KPI としてシステムを構成する全機器の死活監視と通信ポート状態監視が有効であることを確認しました。

KPI およびサブ KPI によるリモート切り分けには正確なシステム構成把握が必要であり、事前にシステム監視者の元にシステムの構成・系統図等の情報を整備することが重要であると考えます。監視体制に加えて予備機器の確保、WAN 回線の SLA 整備、現場駆け付けに漢 s るユーザとの事前協議、マニュアル提供によるユーザの一次対応といった運用体制を構築することで、障害復旧の迅速化に資するという結果を得ました。

上記の結果より、ローカル５Ｇにおける相互接続およびコア共用の実現の可能性が高いことが分かりました。また、実環境での活用を調査するためのユースケース検証においても 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。

検証結果については接続の可否や改善方策を集約し、ガイドラインとして標準的な相互接続要件を手引書にまとめています。コア共用についても運用面や機能面、性能面等での検証を基にした考察を記載し手引書にまとめています。

今後、ベンダーや SIer 等が相互接続およびコア共用を進めていくうえで手引書を参考に推進していくことが可能と考えます。また、ヒアリングから判明した各社の課題についても解消に繋がると想定しています。手引書を活用頂くことでローカル５Ｇの普及促進に繋がることに期待します。