

卒業論文 2025 年度（令和 7 年度）

sXGP-5G：次世代モバイルコア研究への参 入障壁低減のための実験環境の提案

慶應義塾大学 総合政策学部

山口 泰平

sXGP-5G：次世代モバイルコア研究への参入障壁低減のための実験環境の提案

モバイル通信システムの標準化は、技術革新と商用展開を支える重要なプロセスである。3GPP は仕様を先に策定し、その後実装・検証を行うアプローチを採用しており、これは大規模インフラの互換性確保に寄与してきた。一方で、コアネットワークがソフトウェア中心へ移行した今日、実装の進展が仕様策定に追いつかず、標準仕様と実装の乖離や実装間の相互運用性問題が生じやすい状況が指摘されている。IETF の”rough consensus and running code”原則のように、実装を動かしながら標準化を進める手法は、6G 時代のアジャイルな開発サイクルに適している。しかし、モバイル通信では実機 RAN を用いた検証が電波法上の制約から困難であり、実装ベース標準化を支援する検証基盤が限られている。

本研究では、免許不要帯で運用可能な sXGP（TD-LTE 互換）を eNB として活用し、4G RAN（UE・eNB）と 5G Core（5GC）を接続するコンバータを実装することで、法令遵守の範囲で実機検証を可能にする環境を構築した。具体的には、(1) S1AP/NGAP/NAS プロトコルの信令変換、(2) GTP-U トンネル中継によるユーザ面接続、(3) Docker 化による再現可能な実験環境の整備、を実現した。登録・PDU セッション確立などの基本機能を検証し、さらに PCO パラメータ処理、QoS/5QI 分離、SSC モード設定など、コンバータレベルで実装した相互運用性検証項目を確認した。加えて、IPv6-only + NAT64/464XLAT、UL-CL ローカルブレイクアウト、GTP-U PMTUD、SMS over NAS、Paging 到達性、複数 DNN 選択など、標準仕様は存在するが実装の成熟度や相互運用性に課題がある項目について、実機を用いた検証が可能な基盤を提供する。

本研究により、実機 UE とコアネットワーク間の相互運用性問題を早期検出し、標準化団体へタイムリーにフィードバックする基盤が確立された。提案環境は、標準化サイクルの短縮、継続的インテグレーション・回帰テスト、プロトコル拡張の試作検証に適用可能である。本手法は、ソフトウェア中心の 5GC 実装が普及する中で、既存 4G RAN 資産を活用しつつ次世代コアへの移行を支援する実践的アプローチとなる。さらに、免許不要帯を活用した本アプローチは、電波法制約下でも実装検証が可能な研究・教育基盤として、6G 標準化における実装ベース検証の促進に貢献することが期待される。

キーワード:

1. モバイルシステム 2. sXGP 3. 5G Core 4. Open5GS 5. GTP-U

慶應義塾大学 総合政策学部

山口 泰平

sXGP-5G: Proposal of flexible 5G network construction method for next-generation mobile network development

This thesis presents a practical and reproducible 5G experimentation environment by leveraging sXGP (TD-LTE compatible, license-free band in Japan) as an eNB and implementing a converter that connects a 4G RAN (UE/eNB) to a 5G Core (5GC). Traditional 5G research often requires licensed spectrum and expensive RAN equipment, which raises the barrier to entry for universities, labs, and small teams. Our contributions are threefold: (1) building an sXGP-based RAN, (2) designing and implementing a converter that handles S1AP/NGAP/NAS signaling and relays GTP-U, and (3) establishing reproducible build and experiment procedures via Docker.

We validate basic functions such as Registration and PDU session establishment and provide a measurement toolkit for latency, throughput, and resource utilization. The proposed environment benefits several use cases, including (a) education and training, (b) rapid prototyping of protocol conversion, (c) interoperability and regression testing, (d) performance evaluation and bottleneck analysis, (e) reproducible research and collaboration, and (f) operational studies and fault scenario reproduction. The environment facilitates legal, low-cost, and hands-on 5G research while keeping proximity to realistic operational settings.

Keywords :

1. Mobile Systems 2. sXGP 3. 5G Core 4. Open5GS 5. GTP-U

Keio University Bachelor of Arts in Policy Management
Taihei Yamaguchi

目次

第1章 序論	1
1.1 背景	1
1.1.1 専用装置からソフトウェア中心への移行	1
1.1.2 標準化プロセスと実装ベース検証の重要性	1
1.2 問題意識と課題	2
1.3 研究目的	3
1.4 本論文の貢献	3
1.5 論文構成	3
第2章 sXGP・4G/5G の技術概要と標準化プロセスの課題	4
2.1 sXGP と 4G/5G の概要	4
2.1.1 sXGP の位置づけ (免許不要・TD-LTE 互換)	4
2.1.2 4G RAN (UE・eNB) と EPC/5GC の要素	4
2.1.3 5GC のアーキテクチャ (AMF/SMF/UPF 等)	5
2.2 3GPP 標準化と標準-実装ギャップ	6
2.2.1 仕様の包含範囲とリファレンス実装の不足	6
2.2.2 ベンダ実装差と相互接続性の課題	6
2.2.3 研究・評価におけるギャップの影響	7
2.3 RAN-コア間インターワーキングの基礎	8
2.3.1 制御面 (S1-AP vs. NG-AP)	8
2.3.2 ユーザ面 (GTP-U 互換性とパススルー/変換)	9
2.3.3 ID/コンテキスト管理 (NAS, IMSI/SUPI 等)	10
2.4 OSS と 6G に向けた開発・検証サイクル	11
2.4.1 OSS の役割 (Open5GS 等) と試作の加速	11
2.4.2 適合・相互接続・回帰テストの自動化	12
2.4.3 再現性 (Docker 等) と研究公開の促進	13
2.5 モバイルシステム全体での課題感	14

2.5.1	研究環境のコストとライセンス（免許・機器費用）	14
2.5.2	相互接続性・ベンダ依存の壁	14
2.5.3	運用・再現性とオープンテストベッドの不足	15
2.5.4	セキュリティ・計測基盤の一般化の難しさ	16
2.6	法規制と sXGP の位置づけ	17
2.6.1	電波法の制約と実機検証の困難	17
2.6.2	免許不要帯を用いた代替アプローチとしての sXGP の意義	18
2.7	シミュレータの対象範囲と限界	19
2.7.1	シミュレーションで十分な領域	19
2.7.2	シミュレーションの限界	19
2.8	実機が必要となる検証項目	19
2.9	本環境がもたらす価値（ユースケース）	19
2.9.1	教育・トレーニング	19
2.9.2	プロトタイピングと検証の高速化	20
2.9.3	相互接続・回帰テスト	20
2.9.4	性能評価とボトルネック分析	20
2.9.5	再現性の高い研究公開と共同研究	20
2.9.6	運用研究・障害シナリオの再現	20
2.10	本研究が対象とする課題の定義	20
2.10.1	研究者・学生が手軽に再現できる環境の要件	20
2.10.2	sXGP × 5GC 接続の技術的論点の範囲	21
2.10.3	評価指標と成功基準の設定	21
第 3 章	関連研究と事例	22
3.1	オープンソース 5GC とテストベッド	22
3.1.1	Open5GS / free5GC / srsRAN 5G	22
3.1.2	商用テストベッド・教育用環境	22
3.2	OSS エコシステムと適合/相互接続テスト	23
3.2.1	仕様準拠テスト、相互接続試験の枠組み	23
3.2.2	回帰テストと CI/CD 連携の事例	23
3.3	LTE eNB と 5GC の相互接続に関する標準化	23
3.3.1	ng-eNB の位置づけ	23
3.3.2	EPS/5GS 間インターワーキング (N26, 移動性)	24
3.4	プロトコル変換・ゲートウェイの先行事例	24

3.4.1	S1AP – NGAP 変換のアプローチ	24
3.4.2	GTP-U の TEID 管理とパススルー	24
3.5	sXGP の研究利用事例	25
3.5.1	学術・企業での実験報告	25
3.5.2	運用制約と利点	25
第 4 章	提案手法：sXGP-5G コンバータ	26
4.1	要求仕様と設計方針	26
4.1.1	ユースケース	26
4.1.2	非機能要件（再現性・法令遵守・安全性）	26
4.1.3	対象範囲（制御/ユーザ面、認証、セッション管理）	27
4.2	アーキテクチャ設計	28
4.2.1	制御面：S1AP – NGAP 変換の設計案	28
4.2.2	ユーザ面：GTP-U 転送・TEID 管理	28
4.2.3	認証・登録（NAS メッセージ処理の方針）	29
4.2.4	コンテキスト管理とタイムアウト	29
4.3	sXGP 採用の根拠と想定限界	29
4.3.1	採用の根拠：実装ベース標準化への貢献	29
4.3.2	想定限界・外延	30
4.4	実装方針と部品選定	30
4.4.1	ソフトウェア構成（言語・ライブラリ・依存）	30
4.4.2	ネットワーク構成（VLAN/VRF/NAT の要否）	31
4.4.3	監視・計測（メトリクス、トレース）	31
4.5	制約と想定される限界	31
4.5.1	規格差分による制限	31
4.5.2	性能上のボトルネックと回避策	31
第 5 章	sXGP-5G 環境での実機検証手法	32
5.1	実験の目的	32
5.2	実験環境	32
5.2.1	ハードウェア構成（UE/eNB/sXGP 基地局/サーバ）	32
5.2.2	ソフトウェア構成（5GC, コンバータ, OS）	33
5.2.3	ネットワークトポロジと IP アドレッシング	33
5.3	実験シナリオ	33

5.3.1	基本接続（登録・PDUセッション確立）	33
5.3.2	データ転送（スループット・遅延）	34
5.3.3	ハンドオーバー相当の扱い（必要に応じて）	34
5.3.4	Android エミュレータの限界と実 UE 検証の必要性	35
5.4	計測方法と指標	36
5.4.1	A/B 比較（シミュレータ vs 実機）	36
5.4.2	成功基準	36
5.4.3	成功判定基準と再現手順	37
5.4.4	メトリクス（接続成功率、遅延、スループット、CPU/メモリ）	37
5.4.5	ロギング・パケットキャプチャの取得方法	37
第 6 章	相互運用性検証結果と実装ベース標準化への示唆	38
6.1	結果	38
6.1.1	機能検証の結果（登録・PDUセッション）	38
6.1.2	性能測定の結果（遅延・スループット）	38
6.1.3	リソース使用率・スケーラビリティ	39
6.1.4	標準はあるが未実装・未相互運用の検証ケース	39
6.2	考察	41
6.2.1	提案手法の有効性と限界	41
6.2.2	関連研究との比較と位置づけ	42
6.2.3	実運用への適用可能性	42
6.3	ケーススタディと妥当性の脅威	42
6.3.1	実 UE 固有の事象（例：NAS 再送シーケンスのズレ）	42
6.3.2	測定系の制約（時刻同期、NIC オフロードの影響）	42
6.3.3	内的/外的妥当性の脅威と緩和策	43
6.4	実装ベース標準化への示唆	43
第 7 章	結論と展望	44
7.1	本研究のまとめ	44
7.2	今後の課題	45
7.2.1	5G NR 対応への拡張	45
7.2.2	より高度な検証ケースの実装	45
7.2.3	標準化への実際のフィードバック実績	45
7.2.4	自動テスト・CI/CD 環境への統合	46

7.2.5	6G 時代への展望	46
	付録	49

图 目 次

表 目 次

2.1 S1-AP と NG-AP の主要メッセージ対応	8
----------------------------------------	---

第1章 序論

1.1 背景

1.1.1 専用装置からソフトウェア中心への移行

モバイル通信システムの実装形態は、歴史的に大きな変遷を遂げている。専用装置が主流であった時代には、実装コストが高く、特に物理的な制約を伴う RAN システムの装置開発には長期間と高額な投資が必要であった。このような背景において、仕様を先に固めてから実装を進める「仕様ファースト」のアプローチは合理的であり、装置間の互換性確保や投資リスクの低減に寄与してきた。

一方、コアネットワークは 4G 初期には専用装置として実装されていたが、その後の NFV (Network Functions Virtualization) の普及を経て、今日では汎用ハードウェア上でコンテナ実装された 5GC など、ソフトウェアが中心となっている。ソフトウェアは物理的な制約が少なく、実装の柔軟性が高い。実装を先行させながら標準化を進めるアプローチは、実際に使われない仕様の発生を抑制したり、製品導入までのリードタイムを短縮できたりするなど、効率的な面も大きい。

1.1.2 標準化プロセスと実装ベース検証の重要性

モバイル通信の標準化において、3GPP は仕様書を先に策定し、実装・相互運用性検証は後工程となるプロセスを採用している。これは大規模な通信インフラの標準化として必要な側面もある一方で、実装の進展が仕様策定に追いつかない場合があり、標準仕様と実装の乖離や異なる実装間での相互運用性の課題が生じやすい。一方、IETF などインターネット技術の標準化では”rough consensus and running code”の原則に基づき、実装を動かしながら標準化を進める「実装ベース標準化」が実践されており、標準と実装の整合性が保たれやすい。

6G 時代に向けては、標準化サイクルの高速化と実装・検証の早期化が重要である。特に、ソフトウェア中心のコアネットワークと既存 RAN との間に互換性を確保し、次世代

のコア実装へスムーズに移行できる環境を整備することは、標準化と実装の乖離を縮小する上で意義がある。しかし、モバイル通信では実機 RAN を用いた検証が電波法上の制約から困難であり、実装ベース標準化を支援する検証基盤が限られている。本研究は、免許不要帯で運用可能な sXGP (TD-LTE 互換) を eNB として活用し、4G RAN (UE・eNB) と 5G Core (5GC) を接続するコンバータを提案することで、法令遵守の範囲で実機検証を可能にする。5GC の基本的なアーキテクチャと手順は 3GPP TS [1, 2] に規定されており、OSS 実装としては Open5GS [3] が広く用いられている。

1.2 問題意識と課題

本研究の背景には、以下の三点に関する強い問題意識がある。

- **実装ベース標準化の機会:** 3GPP の標準化プロセスは仕様書を先に策定するアプローチであり、実装・相互運用性検証は後工程となる。これにより、標準仕様と実装の乖離や実装間の非互換性が生じる場合があり、標準化へのフィードバックに時間を要することがある。IETF の”running code”原則のように、実装を動かしながら標準化を進めるアプローチを補完することで、6G 時代のアジャイルな開発・標準化サイクルに貢献できる可能性がある。実装ベースの検証基盤はこの方向性を支援する有効な手段である。
- **実装検証環境の制約:** モバイルコアはソフトウェア化が進み、Open Source Software (OSS) も充実してきた。しかし、実機 RAN を用いた検証環境は電波法上の制約から構築が難しく、OSS の相互運用性や実機特有の問題を検証する手段が限られている。シミュレータでは発見しにくい実装レベルの課題（タイミング、リソース競合、NIC/ドライバ依存の挙動など）を早期に検出できる環境が求められている。
- **標準化フィードバックサイクルの改善余地:** 現状では、仕様策定 → 実装 → 商用展開 → 問題発覚 → 次期仕様での修正、というサイクルに時間を要する場合がある。実機検証環境を用いた早期の相互運用性テストと標準化団体へのタイムリーなフィードバックが可能になれば、このサイクルを短縮し、互換性問題の早期解決に貢献できる。免許不要帯で運用可能な sXGP は、この課題に対する実践的なアプローチとなる。

これらに加えて、相互接続性、運用・再現性、計測基盤の不足といったモバイルシステム全体の横断的課題を踏まえ、とりわけ RAN とコア間のインターワーキングが標準化・実装検証のボトルネックである点を指摘する。

1.3 研究目的

- 実装ベース標準化を支援する実機検証環境の構築方法を示す。
- sXGP ベースの 4G RAN と 5GC を接続するコンバータの設計・実装を通じて、標準仕様の相互運用性検証を実現する。
- 実機特有の問題を早期検出し、標準化へのフィードバックサイクルを短縮する手法を提案する。
- 再現可能な検証環境により、継続的インテグレーション・回帰テストを可能にする。

1.4 本論文の貢献

- 実装ベース標準化を可能にする実機検証環境 (sXGP + 5GC) の実証。標準仕様と実装の乖離を早期発見し、標準化団体へタイムリーにフィードバックする基盤を提供。
- 4G RAN と 5GC の信令・ユーザ面の相互接続に関する設計指針と、実装レベルでの相互運用性問題の分類・解決手法の整理。
- 再現性の高い検証プロファイル（トポロジ、計測項目、実験手順）の提示により、継続的な相互運用性テストと回帰テストを支援。
- 免許不要帯を活用した法令遵守型の実機検証手法の確立。電波法制約下でも実装を動かしながら標準化を進めるアプローチの実現可能性を示す。

1.5 論文構成

本論文は以下の構成である。第 2 章で sXGP・4G/5G の技術概要、3GPP 標準化プロセスと実装ギャップ、RAN-コア間インターワーキング、および法規制上の課題を整理する。第 3 章で関連研究と事例、第 4 章で提案手法、第 5 章で実験環境と方法、第 6 章で評価、第 7 章で結論と今後の課題を述べる。

第2章 sXGP・4G/5Gの技術概要と標準化プロセスの課題

2.1 sXGPと4G/5Gの概要

2.1.1 sXGPの位置づけ（免許不要・TD-LTE互換）

sXGP (shared eXtended Global Platform) は、日本国内において免許不要帯である 1.9GHz 帯を使用する TD-LTE 互換の通信規格である。2015 年の電波法改正により、自営等 BWA システムとして制度化され、免許取得なしで基地局の設置・運用が可能となった。チャンネル幅は 10MHz、送信電力は基地局で 1W 以下、端末で 200mW 以下に制限されており、屋内利用を前提とした運用形態が想定されている。

sXGP の最大の特徴は、3GPP 標準の LTE（特に TD-LTE）との互換性を維持しながら、免許不要で運用可能な点にある。これにより、一般的な LTE 対応端末（スマートフォン等）がそのまま利用でき、研究・教育機関において実機を用いたモバイルネットワーク実験が法令遵守の範囲で実施可能となる。特に、電波暗室や特定実験試験局の許可を必要とする通常の LTE 実験と比較して、導入の障壁が大幅に低減される。

一方で、sXGP には周波数帯域幅の制約（10MHz）やカバレッジの制限（屋内利用想定）といった限界も存在する。また、利用可能な基地局機器は限定的であり、研究用途では商用装置の転用や SDR（Software Defined Radio）を用いた実装が主流となる。本研究では、sXGP を eNB として活用することで、4G RAN（UE・eNB）と 5G Core（5GC）を接続する実機検証環境を構築し、実装ベース標準化を支援する検証基盤を提供する。

2.1.2 4G RAN（UE・eNB）と EPC/5GC の要素

4G LTE システムは、UE（User Equipment）、eNB（evolved NodeB）、EPC（Evolved Packet Core）から構成される。UE と eNB 間の無線インタフェースは Uu インタフェースと呼ばれ、RRC（Radio Resource Control）プロトコルによって無線リソース管理が行

われる。eNB と EPC 間は、制御面 (Control Plane) が S1-MME インタフェース、ユーザ面 (User Plane) が S1-U インタフェースで接続される。

EPC の主要構成要素として、MME (Mobility Management Entity)、HSS (Home Subscriber Server)、SGWC/SGWU (Serving Gateway Control/User plane)、PGWC/PGWU (PDN Gateway Control/User plane) が存在する。MME は加入者の認証・位置管理・セッション管理を担当し、S1-AP プロトコルを用いて eNB と通信する。HSS は加入者情報データベースであり、認証鍵 (K、OPc) や AMF 値を管理する。SGWU/PGWU は GTP-U (GPRS Tunneling Protocol - User plane) トンネルを用いてユーザデータを転送する。

4G LTE における基本的な手順は、Attach プロシージャ (初期接続)、Authentication (認証)、Default Bearer 確立、PDN 接続確立から構成される。NAS (Non-Access Stratum) メッセージは、UE と MME 間でエンドツーエンドに交換され、eNB は透過的に中継する。本研究では、4G RAN からの S1-AP メッセージを 5GC 向けの NGAP メッセージに変換するコンバータを実装することで、既存 4G RAN 資産を 5GC と接続可能にする。

2.1.3 5GC のアーキテクチャ (AMF/SMF/UPF 等)

5G Core (5GC) は、サービスベースアーキテクチャ (SBA: Service Based Architecture) を採用し、各ネットワーク機能 (NF: Network Function) が HTTP/2 ベースのサービスインタフェースを介して相互に通信する。主要な NF として、AMF (Access and Mobility Management Function)、SMF (Session Management Function)、UPF (User Plane Function)、UDM (Unified Data Management)、AUSF (Authentication Server Function)、NRF (Network Repository Function) などが存在する。

AMF は、UE の登録管理・接続管理・モビリティ管理を担当し、NG-AP プロトコルを用いて gNB (5G 基地局) または本研究の s1n2-converter と通信する。SMF は、PDU セッション管理・QoS 制御・UPF 選択を担当し、AMF および UPF と連携してデータパスを確立する。UPF は、ユーザプレーンのトラフィック転送・QoS 適用・課金情報収集を担当し、GTP-U トンネルを終端する。

5GC における基本的な手順は、Registration (登録)、Authentication (認証)、PDU Session Establishment (セッション確立) から構成される。4G LTE と比較して、制御面とユーザ面の分離 (CUPS: Control and User Plane Separation) が徹底されており、SMF と UPF の独立性が高い。また、NAS メッセージは 5G NAS 形式となり、セキュリティコンテキストの導出方法も変更されている (KAMF から KNASint/KNASenc を導出)。

本研究で利用する 5GC 機能範囲は、基本的な登録・認証・PDU セッション確立に限

定し、ネットワークスライシング・エッジコンピューティング・ローカルブレイクアウトなどの高度な機能は対象外とする。実装には Open5GS を採用し、AMF、SMF、UPF、UDM、AUSF、NRF、PCF（Policy Control Function）などの NF を Docker コンテナとして展開する。

2.2 3GPP 標準化と標準-実装ギャップ

2.2.1 仕様の包含範囲とリファレンス実装の不足

3GPP (3rd Generation Partnership Project) は、モバイル通信システムの標準化を行う国際的な組織であり、SA (Service and System Aspects)、CT (Core network and Terminals)、RAN (Radio Access Network) の 3 つの技術仕様グループ (TSG: Technical Specification Group) に分かれている。各 TSG は複数のワーキンググループ (WG) を持ち、それぞれが TS (Technical Specification) や TR (Technical Report) を策定する。

例えば、5G Core の基本アーキテクチャは TS 23.501、プロシージャは TS 23.502、NGAP は TS 38.413、5G NAS は TS 24.501 に規定されている。これらの仕様書は相互に参照関係を持ち、全体として数千ページに及ぶ膨大な文書群を形成している。仕様には必須 (Mandatory) 要件と任意 (Optional) 要件が混在し、実装者は必須要件のみを実装することが許容される。

しかし、3GPP 仕様にはリファレンス実装が存在せず、仕様書の記述が実装レベルで曖昧な場合がある。例えば、エラー処理の詳細、タイマー値の推奨範囲、再送ポリシー、並行処理時の順序保証などは、仕様書に明示的に記載されていないことが多い。このため、ベンダ各社が独自に解釈・実装を行い、結果として実装間の相互運用性に課題が生じる。

研究においては、このような仕様の曖昧性が実験の再現性や比較可能性に影響を与える。特に、OSS 実装 (Open5GS、srsRAN 等) は仕様の一部のみを実装しており、商用実装との機能差が存在する。本研究では、Open5GS を基盤として使用するが、実装上の制約を明示的に文書化し、検証範囲を明確にすることで、研究の内的妥当性を確保する。

2.2.2 ベンダ実装差と相互接続性の課題

モバイル通信システムの実装には、ベンダ固有の解釈や拡張が含まれることが一般的である。代表的なベンダ実装差として、以下が挙げられる：

- **Information Element (IE) の扱い**：任意 IE の実装有無、未知 IE の無視/拒否ポリシー、IE 順序の依存性
- **タイマー値とリトライ回数**：デフォルト値の差異、ネットワーク条件に応じた動的調整の有無
- **再送とフォールバック**：メッセージ再送時の挙動、暗号化アルゴリズムのネゴシエーション失敗時の処理
- **ベンダ拡張 IE**：3GPP 標準外の独自 IE の追加、相互運用性試験での扱い

これらの実装差は、IOT (InterOperability Test) において顕在化する。特に、異なるベンダの UE/RAN/Core を組み合わせた場合、標準仕様に準拠していても相互接続に失敗するケースが報告されている。既知の回避策として、IOT イベントでの事前検証、ベンダ間での実装ノートの共有、3GPP Change Request (CR) による仕様明確化などが行われている。

OSS 実装においても、実装の成熟度や機能範囲の差が存在する。例えば、Open5GS はデータ通信機能を中心に実装されており、VoLTE/IMS、SMS over NAS、複数 DNN 選択などの機能は未実装または部分実装である。本研究では、基本的なデータ通信機能を中心に検証を行い、高度な機能については今後の拡張課題として位置づける。

2.2.3 研究・評価におけるギャップの影響

標準仕様と実装の乖離は、研究の再現性および比較可能性に重大な影響を与える。特に、以下の点が課題となる：

- **内的妥当性**：実験条件の統制が困難（実装依存の挙動、バージョン差異、設定パラメータの影響）
- **外的妥当性**：OSS 実装での検証結果が商用環境に適用可能か不明（機能範囲の差、性能特性の違い）
- **再現性**：実装のバージョン、設定ファイル、依存ライブラリのバージョンが論文に明記されないことが多い

これらの課題に対する対策として、本研究では OSS 実装を用いた検証基盤の構築を提案する。具体的には、Docker 化による環境の固定化、設定ファイルやスクリプトの公開、

パケットキャプチャの保存により、第三者による検証の再現を可能にする。また、実装の制約を明示的に文書化することで、検証結果の適用範囲を明確にする。

さらに、IETF の”rough consensus and running code”原則に倣い、実装を動かしながら標準化にフィードバックするアプローチを採用する。これにより、仕様の曖昧性や実装上の問題点を早期に発見し、標準化サイクルの短縮に貢献することを目指す。

2.3 RAN-コア間インターワーキングの基礎

2.3.1 制御面 (S1-AP vs. NG-AP)

4G LTE における eNB と MME 間の制御面プロトコルは S1-AP (S1 Application Protocol) であり、5G における gNB と AMF 間の制御面プロトコルは NG-AP (NG Application Protocol) である。両プロトコルは ASN.1 (Abstract Syntax Notation One) で定義され、SCTP (Stream Control Transmission Protocol) 上で動作する点は共通であるが、メッセージ構造や Information Element (IE) の定義が異なる。

表 2.1 に、主要な S1-AP と NG-AP メッセージの対応関係を示す。

表 2.1: S1-AP と NG-AP の主要メッセージ対応

手順	S1-AP	NG-AP
初期接続	InitialUEMessage	InitialUEMessage
初期コンテキスト設定	InitialContextSetupRequest	InitialContextSetupRequest
初期コンテキスト設定応答	InitialContextSetupResponse	InitialContextSetupResponse
NAS 下り転送	DownlinkNASTransport	DownlinkNASTransport
NAS 上り転送	UplinkNASTransport	UplinkNASTransport
UE コンテキスト解放要求	UEContextReleaseRequest	UEContextReleaseRequest

メッセージ名は類似しているが、含まれる IE の内容は大きく異なる。特に、セッション管理に関連する IE は、4G の Bearer 概念から 5G の PDU Session 概念への変更に伴い、大幅に再設計されている。例えば、4G の E-RAB (E-UTRAN Radio Access Bearer) は 5G の PDU Session Resource に対応するが、QoS 制御の粒度が異なる (4G は Bearer 単位、5G は QoS Flow 単位)。

本研究で実装する s1n2-converter は、S1-AP メッセージを受信して NG-AP メッセージに変換する。変換時の主要なポイントとして、以下が挙げられる：

- UE 識別子の変換 (MME-UE-S1AP-ID ↔ AMF-UE-NGAP-ID、eNB-UE-S1AP-ID ↔ RAN-UE-NGAP-ID)

- E-RAB 情報から PDU Session 情報への変換 (E-RAB ID → PDU Session ID、QCI → 5QI)
- GTP-U トンネル情報の抽出と再マッピング (TEID、Transport Layer Address)
- NAS メッセージのカプセル化 (4G NAS → 5G NAS 変換は別途実施)

エラー処理については、変換不可能な IE が含まれる場合や、必須 IE が欠落している場合の処理方針を定義する必要がある。本研究では、基本的なデータ通信に必要な IE のみを変換し、未対応の IE についてはログに記録した上でスキップする方針を採用する。

2.3.2 ユーザ面 (GTP-U 互換性とパススルー/変換)

ユーザ面プロトコルである GTP-U (GPRS Tunneling Protocol - User plane) は、4G と 5G で基本的に互換性が維持されている。GTP-U は、IP パケットをカプセル化してトンネル転送するプロトコルであり、TEID (Tunnel Endpoint Identifier) を用いて各トンネルを識別する。

GTP-U トンネルの確立は、制御面メッセージ (S1-AP/NG-AP) によって指示される。4G では、InitialContextSetupRequest メッセージに E-RAB Setup List として TEID と Transport Layer Address (IP アドレス) が含まれる。5G では、PDUSessionResourceSetupRequest メッセージに PDU Session Resource Setup Request Transfer として同様の情報が含まれる。

本研究で実装する s1n2-converter は、GTP-U パケットの中継を行う。具体的には、以下の処理を実施する：

- **S1-U → N3 方向**：4G eNB からの GTP-U パケットを受信し、TEID 変換テーブルを参照して 5G UPF 向けの TEID に書き換え、N3 インタフェース (5G UPF) に転送
- **N3 → S1-U 方向**：5G UPF からの GTP-U パケットを受信し、TEID 変換テーブルを参照して 4G eNB 向けの TEID に書き換え、S1-U インタフェース (4G eNB) に転送

TEID 割り当てについては、s1n2-converter 自身が上り方向と下り方向の TEID を独立に管理し、eNB 側と UPF 側に対してそれぞれ異なる TEID を割り当てる。これにより、eNB と UPF が同じ TEID 空間を共有する必要がなくなり、TEID 衝突のリスクを回避できる。

QoS 制御については、4G の QCI (QoS Class Identifier) と 5G の 5QI (5G QoS Identifier) の対応関係を定義し、変換を行う。標準化された QCI/5QI の対応関係は 3GPP TS 23.501 に規定されているが、本研究では基本的なデータ通信 (QCI=9 → 5QI=9) のみを対象とする。

MTU (Maximum Transmission Unit) とフラグメント処理については、GTP-U ヘッダのオーバーヘッド (8 バイト + UDP ヘッダ 8 バイト + IP ヘッダ 20 バイト = 36 バイト) を考慮し、必要に応じて Path MTU Discovery を実施する。ただし、本研究の実験環境は Docker 内部ネットワークを使用するため、MTU 問題は発生しにくい。

2.3.3 ID/コンテキスト管理 (NAS, IMSI/SUPI 等)

モバイルネットワークにおける UE 識別子は、永続的識別子と一時的識別子に分類される。4G では、永続的識別子として IMSI (International Mobile Subscriber Identity)、一時的識別子として GUTI (Globally Unique Temporary Identifier) が使用される。5G では、永続的識別子として SUPI (Subscription Permanent Identifier)、一時的識別子として 5G-GUTI が使用される。

IMSI/SUPI の形式は類似しており、MCC (Mobile Country Code)、MNC (Mobile Network Code)、MSIN (Mobile Subscription Identification Number) から構成される。本研究では、4G の IMSI を 5G の SUPI として扱い、識別子の変換を行わない方針を採用する。これは、Open5GS HSS と UDM が同一の加入者データベース (MongoDB) を共有しており、IMSI ベースでの管理が可能なためである。

NAS セキュリティコンテキストは、UE と MME/AMF 間の NAS メッセージを保護するために使用される。4G では、認証成功後に KASME (Key Access Security Management Entity) が導出され、そこから KNASint (NAS Integrity Key) と KNASenc (NAS Encryption Key) が導出される。5G では、認証成功後に KAMF (Key Access and Mobility Management Function) が導出され、そこから KNASint/KNASenc が導出される。

鍵導出のアルゴリズムは 4G と 5G で異なり、単純な変換は不可能である。本研究では、s1n2-converter が NAS メッセージの変換を行う際に、NAS Integrity Protection の検証を行わない方針を採用する。これは、4G eNB と 5G AMF 間で NAS セキュリティコンテキストが共有されないためである。ただし、この方針はセキュリティ上のリスクを伴うため、実験環境に限定した運用とし、本番環境での使用は推奨しない。

コンバータ内での UE コンテキスト管理については、S1-AP UE ID と NG-AP UE ID のマッピングテーブルを維持し、メッセージ変換時に参照する。また、GTP-U TEID マッ

ピングテーブルも同様に維持し、ユーザ面パケットの中継時に使用する。これらのテーブルは、UEContextReleaseRequest メッセージ受信時にクリーンアップされる。

2.4 OSS と 6G に向けた開発・検証サイクル

2.4.1 OSS の役割（Open5GS 等）と試作の加速

Open Source Software (OSS) は、モバイルネットワーク研究における重要な基盤となっている。特に、Open5GS は 4G EPC/5G Core の包括的な実装を提供し、世界中の研究機関や企業で広く利用されている。Open5GS の主な特徴として、以下が挙げられる：

- **モジュール構成**：各ネットワーク機能（MME、AMF、SMF、UPF 等）が独立したプロセスとして実装され、マイクロサービスアーキテクチャを採用
- **拡張性**：C 言語で実装され、ソースコードが公開されているため、独自機能の追加や動作のカスタマイズが容易
- **活発なコミュニティ**：GitHub 上で継続的に開発が行われており、バグ修正や新機能追加が頻繁にリリースされる
- **標準準拠**：3GPP 仕様に基づいた実装が行われており、商用実装との相互運用性が考慮されている

OSS を活用することで、研究プロトタイプの実装速度が大幅に向上する。商用装置を用いた実験では、ベンダとの契約や機器調達に数ヶ月を要するのに対し、OSS を用いた実験環境は数日で構築可能である。また、学習コストも低減される。Open5GS はドキュメントが充実しており、Web ベースの管理画面（WebUI）を提供するため、初学者でも容易に環境構築が可能である。

本研究では、Open5GS を基盤として使用し、4G EPC および 5G Core を構築する。さらに、srsRAN（旧 srsLTE）を RAN シミュレータとして使用し、ZMQ（ZeroMQ）ベースの RF simulation によって eNB/gNB と UE を接続する。これにより、物理的な無線機器を必要とせず、ソフトウェアのみで完全な End-to-End 環境を構築できる。

2.4.2 適合・相互接続・回帰テストの自動化

モバイルネットワークの品質保証には、適合性試験（Conformance Test）、相互運用性試験（InterOperability Test）、回帰試験（Regression Test）が不可欠である。これらの試験を手動で実施することは時間とコストがかかるため、自動化の仕組みが重要となる。

自動試験の枠組みとして、以下のアプローチが考えられる：

- **シナリオ駆動試験**：試験シナリオをスクリプトまたは YAML/JSON 形式で記述し、試験フレームワークが自動的に実行
- **パケットキャプチャ照合**：Wireshark/tshark を用いてパケットキャプチャを取得し、期待されるメッセージシーケンスと照合
- **ログ解析**：各ネットワーク機能のログ出力を解析し、エラーメッセージや警告の有無を検証
- **差分検出**：基準となる「正常動作時」のパケットキャプチャ/ログと、変更後の結果を比較し、差分を自動検出

既存のテスト資産として、TTCN-3（Testing and Test Control Notation version 3）を用いた適合性試験ツールが存在する。TTCN-3 は、通信プロトコルのテストケースを形式的に記述するための言語であり、3GPP 標準化においても参照されている。ただし、TTCN-3 の学習コストは高く、研究用途では軽量なスクリプトベースのアプローチが好まれる。

本研究では、基本的な End-to-End 接続性を確認するための最小限の回帰テストセットを設計する。具体的には、以下のシナリオを自動実行し、成功/失敗を判定する：

1. 4G Attach + Default Bearer 確立 + Ping 疎通
2. 5G Registration + PDU Session 確立 + Ping 疎通
3. 4G → 5G 変換環境での Attach + Session 確立 + Ping 疎通

これらのテストは、Docker Compose を用いた環境起動スクリプトと組み合わせることで、完全に自動化可能である。将来的には、CI/CD（Continuous Integration / Continuous Deployment）パイプラインに統合し、コード変更のたびに自動的に実行することを想定している。

2.4.3 再現性（Docker 等）と研究公開の促進

研究の再現性を確保するためには、実験環境の詳細な記録と共有が不可欠である。しかし、モバイルネットワーク実験は多数のコンポーネント（UE、RAN、Core）と複雑な設定を伴うため、環境再現が困難であることが多い。

Docker コンテナ技術を活用することで、この課題を大幅に軽減できる。Docker は、アプリケーションとその依存関係を単一のコンテナイメージとしてパッケージ化し、異なる環境で同一の動作を保証する技術である。本研究では、以下の方針で Docker 化を実施する：

- **固定バージョン**：Open5GS、srsRAN、依存ライブラリのバージョンを Dockerfile に明示的に記述
- **設定ファイル共有**：各ネットワーク機能の設定ファイル（YAML 形式）を Git リポジトリで管理
- **ネットワーク構成の明示**：Docker Compose を用いて、コンテナ間のネットワーク構成（IP アドレス、サブネット、ブリッジ）を定義
- **ログとパケットキャプチャの保存**：実験結果として、各コンポーネントのログファイルと Wireshark パケットキャプチャを保存

研究成果を公開する際には、以下の留意点がある：

- **認証鍵の除去**：HSS/UDM に登録された加入者の認証鍵（K、OPc）はダミー値に置き換える
- **個人情報の除去**：IMSI、MSISDN、IP アドレスなどの個人情報は匿名化またはダミー値に置き換える
- **ライセンス確認**：使用した OSS のライセンス（Apache、GPL 等）を確認し、派生物の公開条件を遵守

本研究では、GitHub 上でソースコード、設定ファイル、実験手順書を公開することを計画している。これにより、第三者が同一の実験環境を再現し、検証結果を確認できるようにする。また、Docker Hub にコンテナイメージを公開することで、環境構築の手間をさらに削減することも検討している。

2.5 モバイルシステム全体での課題感

2.5.1 研究環境のコストとライセンス（免許・機器費用）

モバイルネットワーク研究における最大の障壁の一つは、実機環境構築のコストと法的手続きである。典型的な 4G/5G 研究環境を構築する場合、以下の費用が発生する：

- **端末/モデム**：LTE/5G 対応スマートフォンまたは USB モデムで、数万円～数十万円（研究用途では複数台必要）
- **基地局（eNB/gNB）**：商用装置は数百万円～数千万円、研究用小型基地局でも数十万円～数百万円
- **SDR（Software Defined Radio）**：USRP B210（約 50 万円）、LimeSDR（約 5 万円）など
- **アンテナ・RF 機器**：周波数帯に応じた適切なアンテナ、増幅器、フィルタなど
- **測定機器**：スペクトラムアナライザ、シグナルジェネレータ、ネットワークアナライザなど（数百万円～）

さらに、電波法に基づく免許取得または特定実験試験局の申請が必要となる。申請には技術基準適合証明（技適）の有無、使用周波数帯、出力電力、設置場所の詳細な情報が求められ、承認までに数週間～数ヶ月を要する。また、屋外での実験は原則として禁止されており、電波暗室の使用が推奨されるが、電波暗室の建設・維持コストも高額である。

sXGP 採用によるコスト/手続き削減効果は顕著である。sXGP は免許不要帯を使用するため、免許申請が不要であり、屋内であれば比較的自由に実験が可能である。基地局機器としては、LimeSDR などの低コスト SDR を用いることで、数万円程度で環境構築が可能となる。本研究では、ZMQ ベースの RF simulation を使用することで、さらにコストを削減し、ソフトウェアのみで完全な実験環境を構築している。

2.5.2 相互接続性・ベンダ依存の壁

モバイルネットワーク実験における相互接続性の課題は、複数のレイヤーで発生する：

- **UE/モデム差**：チップセットベンダ（Qualcomm、MediaTek、Exynos 等）による実装差、OS バージョン（Android、iOS）の影響

- **カーネル/ドライバ差**：Linux カーネルの Netfilter/iptables 設定、NIC ドライバの TCO（TCP Checksum Offload）や GRO（Generic Receive Offload）の挙動
- **RAN 実装差**：商用基地局、研究用小型基地局、SDR ベース実装の機能範囲とタイミング精度の違い
- **Core 実装差**：Open5GS、商用 EPC/5GC、他の OSS 実装（free5GC、OAI 等）の機能カバレッジと相互運用性

これらの差異は、実験結果の再現性と汎用性に影響を与える。例えば、特定の UE では成功する手順が、別の UE では失敗するケースが報告されている。また、Linux 環境でのパケット転送性能は、NIC オフロード機能の有効/無効によって大きく変動する。

評価設計での緩和策として、以下のアプローチが考えられる：

- **多様な端末での検証**：複数のベンダ/OS の端末を用いて、実装依存性を明らかにする
- **OSS 実装の組み合わせ**：Open5GS、free5GC、srsRAN など、複数の OSS 実装を試験することで、標準準拠度を評価
- **設定の明示的な文書化**：カーネルバージョン、NIC 設定、オフロード機能の有効/無効を明記

本研究では、Open5GS と srsRAN の組み合わせを基本構成とし、実装の制約を明示的に文書化する。将来的には、他の OSS 実装との相互運用性試験を実施することを計画している。

2.5.3 運用・再現性とオープンテストベッドの不足

モバイルネットワーク研究において、共有可能なテストベッドの不足は長年の課題である。研究機関ごとに独自の環境を構築しているが、環境の詳細が論文に記載されないことが多く、第三者による再現が困難である。また、商用ネットワークを用いた実験は、ベンダとの契約やセキュリティ上の制約から、詳細な実験条件を公開できないことが多い。

オープンテストベッドの事例として、米国の POWDER（Platform for Open Wireless Data-driven Experimental Research）やヨーロッパの ONELab（Open Network Laboratory）が存在する。これらは、研究者が遠隔からアクセス可能なテストベッドを提供し、実機を用いた実験を支援している。しかし、利用にはアカウント登録や審査が必要であり、自由度が制限される場合がある。

本研究では、Docker 化された実験環境を提供することで、第三者が自身の環境で実験を再現できるようにする。提供するアーティファクトとして、以下を計画している：

- **Docker コンテナイメージ**：Open5GS、srsRAN、sln2-converter を含む完全なシステム
- **設定ファイル**：各コンポーネントの YAML 設定ファイル、ネットワーク構成
- **実験スクリプト**：環境起動、UE 接続、データ通信確認、ログ収集の自動化スクリプト
- **パケットキャプチャ**：Wireshark で解析可能な pcap ファイル (S1-AP、NG-AP、GTP-U、NAS)
- **実験手順書**：セットアップから実験実施、結果確認までの詳細な手順

これにより、研究成果の再現性を確保し、他の研究者が本研究を基盤として発展させることを可能にする。

2.5.4 セキュリティ・計測基盤の一般化の難しさ

モバイルネットワーク実験におけるセキュリティ上の課題は、以下の通りである：

- **認証鍵の取り扱い**：HSS/UDM に登録された加入者の認証鍵 (K、OPc) は、SIM カード内に格納されており、外部からの読み取りは困難。実験用途では、ダミー鍵を使用するか、eUICC (embedded Universal Integrated Circuit Card) を用いたプログラマブル SIM を使用する必要がある
- **プライバシー/PII (Personally Identifiable Information)**：IMSI、MSISDN、位置情報などの個人識別可能な情報は、研究成果公開時に匿名化またはダミー値に置き換える必要がある
- **攻撃面の考慮**：実験環境が外部ネットワークに接続されている場合、セキュリティホール (例：認証バイパス、暗号化無効化) が攻撃経路となるリスクがある
- **計測オーバーヘッド**：パケットキャプチャ、ログ記録、性能計測ツールの実行による CPU/メモリオーバーヘッドが、実験結果に影響を与える可能性がある

本研究では、実験環境を外部ネットワークから隔離された Docker ネットワーク内に構築することで、セキュリティリスクを最小化する。また、認証鍵や IMSI はダミー値を使用し、研究成果公開時には個人情報を含まないように配慮する。計測オーバーヘッドについては、本格的な性能評価を行う際には計測ツールの影響を定量化し、補正を行う方針とする。

2.6 法規制と sXGP の位置づけ

2.6.1 電波法の制約と実機検証の困難

日本国内における無線通信実験は、電波法によって厳格に規制されている。主な制約として、以下が挙げられる：

- **屋内外の制約**：屋外での電波発射には原則として無線局免許が必要。屋内実験でも、電波漏洩を防ぐための電波暗室の使用が推奨される
- **出力制限**：免許不要帯以外の周波数帯を使用する場合、特定実験試験局として申請が必要。出力電力は用途に応じて制限される
- **使用帯域**：LTE Band 1 (2.1GHz)、Band 3 (1.8GHz)、5G n77 (3.7GHz)、n79 (4.5GHz) などの商用周波数帯は、免許取得または実験試験局申請が必須
- **干渉リスク**：実験電波が商用ネットワークや他の無線システムに干渉を与えるリスクがあり、周波数調整や出力制限が求められる

学術機関での典型的な許認可フローは、以下の通りである：

1. 実験計画書の作成（使用周波数、出力電力、実験期間、設置場所の詳細）
2. 技術基準適合証明（技適）の確認、またはシールドルーム使用計画
3. 総務省総合通信局への特定実験試験局の申請
4. 審査期間（通常 2 週間～1 ヶ月）
5. 免許交付後、実験開始
6. 実験終了後、結果報告書の提出

このプロセスは、迅速なプロトタイピングや反復実験を前提とする研究開発には不向きである。特に、学生や若手研究者が短期間で実験環境を構築し、試行錯誤を繰り返すことが困難となる。

2.6.2 免許不要帯を用いた代替アプローチとしての sXGP の意義

sXGP は、免許不要帯（1.9GHz 帯）を使用することで、上記の法的制約を大幅に緩和する。sXGP の法的位置づけは、電波法施行規則第 6 条第 4 項第 3 号の 6 に規定される「小電力データ通信システムの無線局」に該当し、技術基準適合証明（技適）を取得した機器であれば、免許取得なしで運用可能である。

sXGP を用いた実機検証の意義は、以下の通りである：

- **法令遵守**：免許申請不要で、合法的に実機相当の RAN 実験が可能
- **迅速な環境構築**：機器の調達から実験開始までの期間が大幅に短縮（数日～数週間）
- **反復実験の容易化**：設定変更や機能追加を繰り返し、試行錯誤が可能
- **教育利用**：学生が自主的にモバイルネットワーク実験を行える環境を提供

一方で、sXGP には以下の限界も存在する：

- **周波数帯域幅**：10MHz に制限されており、高スループット実験（例：100Mbps 以上）には不向き
- **設備可用性**：sXGP 対応基地局機器は限定的であり、商用装置の入手は困難。研究用途では SDR を用いた自作が主流
- **カバレッジ**：送信電力が制限されており（基地局 1W、端末 200mW）、広範囲のカバレッジ実験には不向き
- **商用環境との差異**：商用 LTE/5G ネットワークとは周波数帯・出力・設定が異なるため、結果の外的妥当性に留意が必要

本研究では、sXGP の利点を活かしつつ、限界を認識した上で実験設計を行う。特に、基本的なプロトコル変換機能と相互運用性の検証に焦点を当て、高スループットや広域カバレッジは今後の課題として位置づける。sXGP を用いることで、実装ベース標準化を支援する検証基盤を低コストかつ法令遵守の範囲で提供し、モバイルネットワーク研究の民主化に貢献することを目指す。

2.7 シミュレータの対象範囲と限界

2.7.1 シミュレーションで十分な領域

新 NF のアルゴリズム検討、プロトコル状態機械の基本遷移の正当性確認、ラフなスケール試験、CI での高速回帰などはシミュレータで効率的に実施できる。

2.7.2 シミュレーションの限界

実 UE 固有の実装差 (RRC/NAS のタイマ・再送・Capability 差)、RRC/PHY/MAC の時間ゆらぎ由来の境界条件、OS/NIC のオフロードやキューイング、パケット順序入替・フラグメンテーション、S1AP↔NGAP 変換や TEID 管理の例外パスなどは、シミュレータでは再現が難しい。

2.8 実機が必要となる検証項目

- 厳密なタイマ境界・再送・例外遷移 (登録/PDU 確立、NAS/RRC の異常系)
- セキュリティと鍵管理 (AKA/EAP-AKA', KDF、再同期、アルゴ協定の実装差)
- ユーザ面の実性能 (GTP-U オフロード、カーネル/DPDK、NUMA/CPU スケジューリング)
- 相互接続・回帰 (複数 UE/モデム/OS での互換性検証)
- フェイルシナリオ (部分ロス、遅延、再順序化、NIC ドロップ、CPU スタベーション)

2.9 本環境がもたらす価値 (ユースケース)

2.9.1 教育・トレーニング

免許不要帯で運用可能な sXGP を eNB として活用し、4G RAN と 5GC を接続できるため、学部・大学院・企業研修において、法令遵守のもとで実機に近い無線・コア連携の学習が可能となる。設定の再現手順を公開することで、実験レポートの客観性と再現性も高められる。

2.9.2 プロトタイピングと検証の高速化

コントロールプレーン (S1AP/NGAP/NAS) およびユーザプレーン (GTP-U) の変換・中継部を差し替え可能にすることで、新しいアルゴリズムやポリシー（例：識別子管理、TEID 割当、タイムアウト制御）の試作・検証を低コストで繰り返し実施できる。

2.9.3 相互接続・回帰テスト

Open5GS などの 5GC 実装や各種 eNB/UE に対して、信令互換性や基本機能（登録、PDU セッション確立）の回帰テストを自動化できる。コンバータを介した差分吸収により、ベンダ差や仕様差を可視化しつつ評価できる。

2.9.4 性能評価とボトルネック分析

遅延・スループット・リソース使用率 (CPU/メモリ) の計測基盤を同梱することで、コンバータの処理遅延やカプセル化オーバーヘッド、TEID 管理戦略の影響を定量化でき、設計改善に資する。

2.9.5 再現性の高い研究公開と共同研究

Docker を用いた構成管理とビルド手順の統一により、第三者が同一環境で追試できる。研究成果の普及や共同研究の立ち上げコストを下げる。

2.9.6 運用研究・障害シナリオの再現

認証失敗やセキュリティモードエラー、ハンドオーバー相当の遷移など、現場で発生する事象の再現とトラブルシュート手順の確立に役立つ。

2.10 本研究が対象とする課題の定義

2.10.1 研究者・学生が手軽に再現できる環境の要件

必要構成要素・費用・所要時間・依存関係・再現手順の粒度を定義し、到達すべきユーザ体験（セットアップから成功確認まで）を示す。

2.10.2 sXGP × 5GC 接続の技術的論点の範囲

本研究で扱う範囲（制御/ユーザ面の変換、識別子/セキュリティ/状態管理）と扱わない範囲（RRC/PHY 最適化、商用品質の最適化など）を明確化する。

2.10.3 評価指標と成功基準の設定

機能（登録/セッション確立率）、性能（遅延/スループット/CPU 等）、堅牢性（異常時の復帰）、再現性（環境差耐性）の指標と合格基準を定める。

第3章 関連研究と事例

3.1 オープンソース 5GC とテストベッド

3.1.1 Open5GS / free5GC / srsRAN 5G

5G Core の OSS 実装としては、Open5GS、free5GC、OpenAirInterface (OAI) などが広く用いられている。Open5GS は 4G EPC/5G Core を統合的に実装し、Docker コンテナでの展開が容易である。WebUI による加入者管理や、AMF/SMF/UPF 等の機能分離が明確で、研究用途に適する。本研究では、Open5GS を基盤として 5GC を構築し、sXGP-5G コンバータとの相互接続検証を行った (§5)。

free5GC は Go 言語で実装された 5GC であり、SBA のサービス間通信や NFs 間の HTTP/2 ベースのやり取りを可視化しやすい利点がある。OAI は RAN/CORE の双方を包含する大規模プロジェクトであり、物理層から上位層までの包括的な研究に用いられている。一方で、ビルド依存や環境構築が比較的複雑で、再現性確保の観点では Docker 化・固定化が前提となる。

RAN 側の OSS としては、srsRAN (旧 srsLTE) と UERANSIM が代表的である。srsRAN は 4G eNB/UE に加えて 5G gNB/UE (Project 系) も提供し、ZMQ ベースの RF シミュレーションによって無線機器なしにプロトコル検証が可能である。UERANSIM は 5G の gNB/UE シミュレータであり、NGAP/NAS の制御面検証に適する。本研究では、srsRAN の ZMQ 構成を用い、4G/5G 双方の接続性とデータ疎通を確認している (TESTING_RESULTS 参照)。

3.1.2 商用テストベッド・教育用環境

教育・研究のためのテストベッドとして、米国の POWDER や、欧州の ONELab 等が提供されている。これらは、遠隔から RAN/CORE 資源にアクセスして実験を実施できる環境であるが、アカウント申請や利用審査、スケジューリングが必要であり、迅速な反復実験には必ずしも向かない。一方、OSS と Docker を組み合わせたローカルテストベッ

ドは、構築コストと運用負荷が低く、再現性の高い実験を短時間で繰り返せる利点がある。本研究の環境設計は後者に属する。

3.2 OSS エコシステムと適合/相互接続テスト

3.2.1 仕様準拠テスト、相互接続試験の枠組み

3GPP は適合性試験のための参照フレームワークを整備しているが、実際の実装間相互接続性 (IOT) はベンダ横断のイベントや二者間検証で担保されることが多い。TTCN-3 を用いた適合性試験スイートは存在するものの、導入・運用コストが高い。研究用途では、pcap のメッセージシーケンス照合、ログ解析、期待結果との比較による軽量の検証が現実的である。

3.2.2 回帰テストと CI/CD 連携の事例

OSS コミュニティでは、CI (Continuous Integration) により回帰の早期検出を図る実践が一般化している。Open5GS でも Pull Request に対して自動ビルド・一部ユニットテストが実行される。ネットワークシステムに固有の相互接続テストは CI 上での完全再現が難しいが、Docker Compose で最小構成を起動し、UE 模擬・RAN シミュレータで手順を自動化するアプローチが有効である。本研究でも、Attach/Registration と Ping 疎通を最小回帰セットとして設計している。

3.3 LTE eNB と 5GC の相互接続に関する標準化

3.3.1 ng-eNB の位置づけ

3GPP TS [1] では、E-UTRA 無線を用いながらも 5GC に接続する基地局として ng-eNB が定義される。ng-eNB は NG-AP で AMF と接続し、SCTP/NGAP を用いて制御信令を交換する。一方、従来の eNB は MME と S1-AP で接続し、EPC に属する。両者は同一の無線 (E-UTRA) であっても、制御面・ユーザ面の接続先と手順が異なるため、単純な置換では相互接続できない。本研究の s1n2-converter は、既存 eNB を変更せずに 5GC へ接続するための変換層として機能する。

3.3.2 EPS/5GS 間インターワーキング (N26, 移動性)

EPS (EPC を用いる 4G) と 5GS (5GC を用いる 5G) 間の相互運用性は、選択的に規定されている。特に、UE の移動性管理やコンテキスト引継ぎに関して、N26 インターフェース (MME と AMF 間) が定義されるが、実装と運用は必須ではない。N26 が未実装の環境では、Attach/Registration のやり直しが発生し、遷移時に遅延が増大する。本研究の対象は、ng-eNB 化ではなく、既存 eNB のまま 5GC への接続性を実現する変換であり、N26 相当の移動性は扱わない。

3.4 プロトコル変換・ゲートウェイの先行事例

3.4.1 S1AP - NGAP 変換のアプローチ

S1AP と NGAP は ASN.1 ベースの設計思想を共有するが、IE と手順の多くが非互換である。先行事例では、S1AP InitialContextSetup (ICS) に含まれる E-RAB 情報から、NGAP InitialContextSetup/PDUSessionResourceSetup に必要な情報を抽出・再構成する手法が示されている。変換層は、UE 識別子のマッピング (MME-UE-S1AP-ID/AMF-UE-NGAP-ID 等)、E-RAB ID と PDU Session ID の対応付け、NAS メッセージの封入形式 (4G NAS/5G NAS) を管理する必要がある。

本研究の実装では、ICS Response 中の E-RAB Setup List から GTP トンネル情報 (TEID/D/IP) を抽出し、PDUSessionResourceSetupResponseTransfer に対応する TNL 情報を生成する試みを行った。しかし、AMF 側で PDU Session が事前に認識されていない場合に "unknown-PDU-session-ID" が返るなど、5G 手順の前提に起因する課題が確認された。対策として、手順の分離 (ICS と PDU Session Setup の段階的処理) や、AMF/SMF との連携順序の見直しが必要であることを示した (開発日誌参照)。

3.4.2 GTP-U の TEID 管理とパススルー

ユーザ面における GTP-U は 4G/5G で基本互換であるため、TEID のマッピングによりパススルーが可能である。変換層は、S1-U 側と N3 側で独立した TEID 空間を持ち、方向ごとに TEID を管理する。先行事例では、トラフィックの負荷分散や QoS 方針に応じて TEID 割当を動的に変更するアプローチも報告されている。本研究では、最小実装として静的/逐次割当を採用し、ping 疎通までの End-to-End 動作を確認している。

3.5 sXGP の研究利用事例

3.5.1 学術・企業での実験報告

sXGP は免許不要帯での運用が可能であることから、学術機関や企業において実機に近い環境での LTE 検証に用いられている。屋内小規模のカバレッジで、無線条件や端末挙動を制御しやすく、プロトコル解析や相互運用性評価に適している。OSS コア (Open5GS) との組み合わせにより、加入者管理から PDU セッション確立までの一連の手順を実機で再現できる。

3.5.2 運用制約と利点

sXGP の利点は、法令遵守の範囲で迅速な反復実験が可能である点にある。一方、チャンネル幅 10MHz・送信電力上限といった物理的制約が存在し、高スループット評価や屋外広域での検証には適さない。研究計画においては、sXGP を基盤とした実機検証と、ZMQ/RF シミュレーションによる反復試験を適切に使い分けることが重要である。本研究は、両者を組み合わせることで、実装ベース標準化に資する検証サイクルを構築した点に特徴がある。

第4章 提案手法：sXGP-5G コンバータ

4.1 要求仕様と設計方針

4.1.1 ユースケース

提案環境は、実装ベース標準化を支援する以下のユースケースを想定する。

1. **標準仕様の実装検証と相互運用性テスト**: 3GPP 仕様に基づく OSS 実装を実機 RAN で動作させ、仕様書上の記述と実装の乖離、異なる実装間の相互運用性問題を早期に発見する。
2. **標準化へのタイムリーなフィードバック**: 検出した問題を再現手順・パケットキャプチャとともにドキュメント化し、標準化団体（3GPP 等）や関連 OSS プロジェクトへ報告・改善提案を行う。
3. **継続的インテグレーション・回帰テスト**: 再現性の高い実験環境により、コード変更やプロトコル拡張が既存機能を破壊していないかを自動的に検証する。
4. **性能評価とボトルネック分析**: 実機環境での遅延・スループット測定により、プロトコル設計や実装の性能ボトルネックを特定し、標準化・実装の両面から改善を図る。
5. **プロトコル拡張の試作・検証**: 新機能や実験的プロトコルを実装し、実機環境で動作検証を行うことで、標準化前の技術検証を加速する。
6. **教育・トレーニング用途**: 実機相当の環境で 5G/6G プロトコルスタックの動作を学習し、標準化・実装の実践的スキルを習得する。

4.1.2 非機能要件（再現性・法令遵守・安全性）

- **再現性**: Docker 等のコンテナ技術により、環境構築手順を標準化し、異なる環境でも同一の実験を再現可能にする。

- **法令遵守:** 免許不要帯（sXGP）を用いることで、電波法に抵触せず実機検証を実施できる。
- **安全性:** 実験環境を隔離されたネットワークで構築し、商用ネットワークへの影響を排除する。
- **可観測性:** すべての制御/ユーザ面トラフィックを pcap/ログとして取得でき、試験ごとに成果物として保存できること。
- **保守性:** 変換ロジックはメッセージ種別ごとにモジュール化し、追加/無効化が容易であること。

4.1.3 対象範囲（制御/ユーザ面、認証、セッション管理）

本提案は、LTE eNB を変更せず 5GC へ接続するための**変換層**（sln2-converter）である。対象とする範囲と非対象は以下のとおりである。

対象

- 制御面: S1AP と NGAP のメッセージ変換および IE マッピング（Initial UE/Context Setup 近傍の手順を中心）
- ユーザ面: S1-U と N3 間の GTP-U カプセル化のパススルーおよび TEID マッピング
- コンテキスト: UE 識別子（MME-UE-S1AP-ID/ENB-UE-S1AP-ID, AMF-UE-NGAP-ID）の対応管理

非対象（現段階）

- 無線（PHY/MAC/RLC/PDCP）の最適化や NR 固有機能（本研究は RAN に sXGP/TD-LTE を用いる）
- EPS/5GS 間の移動性最適化（N26 インターフェース）[2]
- ハンドオーバー、eDRX/PSM 等の省電力最適化

4.2 アーキテクチャ設計

提案アーキテクチャを図示的に記述すると、eNB—(S1AP,S1-U)→Converter—(NGAP,N3)→5GC(AMF/SMF/UPF)である。Converter は制御面/ユーザ面を分離して処理し、状態を共有する。5GC は Open5GS[3] を想定するが、NGAP/N3 の標準動作に従う実装であれば置換可能である ([1, 2])。

4.2.1 制御面：S1AP – NGAP 変換の設計案

変換対象とする代表的手順とマッピング方針を示す。

- **Initial UE Message (S1AP) → Initial UE Message (NGAP)** : UE 識別子と TA/PLMN 情報、NAS コンテナを搬送する。Converter は eNB からの ECGI/TAI 等を NGAP の TAI/NR CGI 相当へマップし、AMF 選定に必要な IE を充足させる。
- **Initial Context Setup (S1AP) ↔ Initial Context Setup (NGAP)** : セキュリティ/UE-AMBR 等のコンテキスト IE を相互に再構成する。E-RAB 関連 IE は、5G の PDU Session 資源手順と分離して取り扱う (後述)。
- **UE Context Release**: 釣り合いの取れた解放手順 (S1AP UEContextRelease/N-GAP UEContextRelease) を相互に変換する。

設計上の原則は、(i) NAS は原則透過搬送とし Converter で終端しない、(ii) IE の欠落時は安全側 (エラー) に倒す、(iii) 5G で独立した手順 (例: PDU Session Resource Setup) は S1AP の ICS と分離して逐次処理する、である。これにより、AMF/SMF 側の前提条件を満たさずに unknown-PDU-session-ID 等のエラーとなる事象を回避する。

4.2.2 ユーザ面：GTP-U 転送・TEID 管理

ユーザ面はパススルーを基本とし、S1-U (eNB ⇄ Converter) と N3 (Converter ⇄ UPF) で独立した TEID 空間を維持する。Converter は方向別に以下の対応表を持つ。

UL Map (ENB-UE-S1AP-ID, eNB-TEID_UL) → (UPF_IP, N3-TEID_UL)

DL Map (AMF-UE-NGAP-ID, N3-TEID_DL) → (eNB_IP, S1U-TEID_DL)

TEID の学習は、E-RAB Setup List(S1AP)およびPDUSessionResourceSetupResponseTransfer (NGAP) に含まれる GTP_Tunnel 情報から行う。学習前パケットはドロップし、ログで検知する。MTU については、 $d_{\max} = \min(1500, \text{パス上の最小 MTU} - \text{GTP/IP/UDP ヘッダ})$ とし、DF ビットはクリアする保守的ポリシーを採用する。

4.2.3 認証・登録（NAS メッセージ処理の方針）

NAS は原則透過搬送とし、Converter はカプセル化境界の整合性のみを担保する。具体的には、S1AP/NGAP の NAS-PDU フィールドとして運ばれるバイト列を改変せず、AMF/UE で終端されることを前提とする。学術検証モードとして、事前に参加者・鍵情報を 5GC に登録し、認証アルゴリズム不一致による失敗を切り分ける運用を提供する。NAS の再暗号化や鍵導出は Converter の責務に含めない ([1])。

4.2.4 コンテキスト管理とタイムアウト

Converter は UE ごとに以下を保持する。

- ID 束: (ENB-UE-S1AP-ID, MME-UE-S1AP-ID) \leftrightarrow (AMF-UE-NGAP-ID)
- セッション束: PDU Session ID \leftrightarrow E-RAB ID の対応、TEID 対応表 (UL/DL)
- タイマ: T_ctx(コンテキスト保持), T_gtp(TEID 学習待ち), T_proc(手順待ち合わせ)

T_ctx 満了で UE コンテキストを破棄し、未解放資源をログ出力する。異常系 (IE 不足/不整合、学習超過) は cause を付して相手側へエラーを返すか、ドロップ+監査ログとする。

4.3 sXGP 採用の根拠と想定限界

4.3.1 採用の根拠：実装ベース標準化への貢献

sXGP を採用する最大の理由は、免許不要帯での法令遵守により「実装を実際に動かせる」ことにある。これは、実装ベース標準化の実現において極めて重要である。

- 実機による全スタック検証: 実 UE・実 NIC・実時間のプロトコルスタックを動作させることで、シミュレータでは検出できない実装レベルの問題（タイミング、リ

ソース競合、ハードウェア依存の挙動など）を発見できる。これは標準仕様と実装の乖離を早期に検出するために不可欠である。

- **相互運用性問題の早期発見:** 異なるベンダの実装（UE、eNB、コア）を組み合わせた際の相互運用性問題を、実機環境で検証できる。3GPP 標準の曖昧な記述や解釈の違いによる非互換性を、標準化プロセスの早い段階でフィードバック可能にする。
- **標準化へのタイムリーなフィードバック:** 実機で問題を再現できることで、再現手順・パケットキャプチャ・ログを含む具体的な報告を標準化団体や OSS プロジェクトに提供できる。これにより、仕様策定 → 実装 → 問題発覚 → 修正のサイクルを数年単位から数ヶ月単位に短縮できる。
- **継続的検証の実現:** 免許不要帯であるため、継続的インテグレーション（CI）環境に組み込んで自動テストを実施できる。コード変更のたびに実機検証を行うことで、回帰テストと品質保証を強化できる。
- **（副次的効果）低コスト・再現性:** 専用周波数ライセンスが不要であり、比較的低コストで実験環境を構築できる。また、Docker などの技術と組み合わせることで、再現性の高い検証環境を複数の研究者・組織で共有できる。

4.3.2 想定限界・外延

本環境は LTE 互換の sXGP を RAN として用いるため、5G NR 特有の PHY 機能やスケジューリング最適化は対象外となる。しかし、制御面（S1AP/NGAP/NAS）およびユーザ面（GTP-U）のプロトコルレベルでの相互運用性検証は十分に可能であり、標準化フィードバックの主要な価値はこのレイヤーにある。NR 固有の無線レイヤーの課題は、今後の拡張として分離して扱う。

4.4 実装方針と部品選定

4.4.1 ソフトウェア構成（言語・ライブラリ・依存）

実装言語は C とし、制御面/ユーザ面は独立プロセスまたはスレッドで分離する。ASN.1 の処理は外部ツールで生成したデコーダを用いるか、既存実装（例: Open5GS のエンコーダ/デコーダ参照 [3]）の表現に合わせてシリアライザを実装する。検証用途として、srsRAN の ZMQ インターフェースを接続し、無線機なしでの反復試験を可能とする (§3)。

4.4.2 ネットワーク構成（VLAN/VRF/NAT の要否）

最小構成では、Converter に S1U/N3 の 2 ポート（論理でも可）を割り当て、データプレーンをルーティングで分離する。商用 NW との干渉回避のため、VRF または名前空間を用いた論理分離を推奨する。UPF とは静的ルーティングで直結し、アドレス設計は Open5GS のデフォルト構成に準拠する (§5)。

4.4.3 監視・計測（メトリクス、トレース）

制御面はメッセージ種別/結果（成功・失敗原因）/処理時間をメトリクス化し、ユーザ面はスループット/RTT/パケット損失率を定期測定する。すべての試験について pcap と構成スナップショット（コンテナタグ、設定ファイル）を成果物として保存し、回帰の基準とする。

4.5 制約と想定される限界

4.5.1 規格差分による制限

S1AP と NGAP は IE の集合と手順が一致しないため、完全な 1 対 1 変換は成立しない。特に、5G の PDU Session 手順は S1AP の E-RAB 手順と**分離**されている。設計では手順の逐次化と、IE 欠落時の安全側フェイルにより、相互運用性を最大化しつつ誤動作を抑制する ([1, 2])。

4.5.2 性能上のボトルネックと回避策

ユーザ面は二重の GTP 終端によるオーバヘッドが生じる可能性がある。最適化として、カーネルオフロード（XDP/TC）やゼロコピー I/O の導入、TEID ルックアップのハッシュ最適化を段階的に適用する。制御面は ASN.1 エンコード/デコードの CPU 負荷が支配的となるため、ホットパスの事前割付とメモリプールで GC 負荷を抑える。

第5章 sXGP-5G 環境での実機検証手法

5.1 実験の目的

本章では、提案した sXGP-5G コンバータ環境を用いて、以下を実証する：

- **基本的な相互接続動作の確認:** 4G RAN (sXGP eNB + 実 UE) と 5G Core (Open5GS) 間で、登録・PDU セッション確立・データ転送が正常に動作することを検証する。
- **S1AP/NGAP/NAS 信令変換の正当性:** コンバータが 4G (S1AP) と 5G (NGAP) のプロトコル変換を正しく行い、両側のプロトコルスタックが期待通り動作することを確認する。
- **GTP-U トンネル中継の動作確認:** ユーザ面トラフィックが S1-U (eNB 側) と N3 (UPF 側) 間で正しくトンネリングされ、TEID 管理が適切に機能することを検証する。
- **実機特有の相互運用性問題の検出能力:** シミュレータでは再現困難な実機依存の挙動（タイミング、NAS 再送、端末 OS 依存の処理など）を検出できることを示す。
- **再現性の確保:** Docker 化された環境により、同一の実験を異なる環境で再現可能であることを確認する。

5.2 実験環境

5.2.1 ハードウェア構成 (UE/eNB/sXGP 基地局/サーバ)

本研究の実機検証は、以下の最小構成で実施する。

- **UE:** 市販スマートフォン (4G LTE 対応、sXGP 対応バンド) または LTE モデム端末。
- **sXGP 基地局 (eNB) :** TD-LTE 互換の sXGP 小型基地局 (室内用)。

- **サーバ**: x86_64 または同等性能のホスト 1 台。Converter および Open5GS のコンテナを実行する。NIC は 1~2 ポート（管理/データ分離は論理でも可）。
- **スイッチ/ルータ**: 管理ネットワークと実験ネットワークの L2/L3 分離に用いる。VRF または Linux ネットワーク名前空間で代替可能である。

5.2.2 ソフトウェア構成（5GC, コンバータ, OS）

- **5GC**: Open5GS (AMF/SMF/UPF/UDM/AUSF/NRF, WebUI)。Docker コンテナで起動し、加入者情報を WebUI または API で登録する [3]。
- **Converter**: s1n2-converter（制御面: S1AP ↔ NGAP, ユーザ面: S1-U ↔ N3）。制御/ユーザ面は別プロセス（またはスレッド）として動作し、TEID 対応表を共有する（第 4 章）。
- **OS/ツール**: Linux (Docker/Compose, tcpdump, tshark, iproute2)。時間同期は NTP で十分である（PPS 等の高精度は本検証の範囲外）。

5.2.3 ネットワークトポロジと IP アドレッシング

トポロジは、UE—eNB(sXGP)—(S1AP,S1-U) → Converter—(NGAP,N3) → 5GC の直列構成である。Converter は制御面 (S1AP/NGAP) とユーザ面 (S1-U/N3) で論理 IF を分ける。5GC 側は、AMF/SMF/UPF を同一ホスト内に配置する。UE アドレスプールや APN 等は Open5GS のデフォルト方針に準拠し、必要に応じて IPv6-only + NAT64/464XLAT, DNS64 構成を併用する（第 3 章）。

5.3 実験シナリオ

5.3.1 基本接続（登録・PDU セッション確立）

目的 Converter の S1AP ↔ NGAP 変換と 5GC 連携が成立することを確認する。

前提 5GC 起動済、加入者登録済、eNB の S1 接続先が Converter に設定済。

手順

1. UE を sXGP セルに接続し、Attach/Registration を開始する。
2. Converter で Initial UE Message/Initial Context Setup の相互変換が成功し、AMF で UE Context が生成されることを確認する（ログ/pcap）。
3. PDU Session（5G）資源手順が SMF/UPF 側で成功し、Converter に TEID 情報が学習されることを確認する。

成功基準 AMF/SMF/UPF ログにエラーがなく、UE が PDU セッション確立状態となる。Converter の対応表に TEID（UL/DL）が登録される。

5.3.2 データ転送（スループット・遅延）

目的 S1-U/N3 間の GTP-U 中継と TEID マッピングが正しく機能することを確認する。

手順

1. UE からコアネットワーク外部（または UPF データネット）への ICMP/TCP/UDP 通信を発生させる。
2. Converter の S1-U/N3 で pcap を取得し、TEID・5 タプル対応を突合する。
3. スループット（iperf 等）と RTT（ping）を測定し、パスの安定性を確認する。

成功基準 UL/DL とともに期待する TEID でカプセル化され、フローが継続する。損失/再送が異常に多い場合は MTU/MSS やオフロード設定を点検する。

5.3.3 ハンドオーバー相当の扱い（必要に応じて）

本研究は N26 等の移動性最適化を対象外とするが、**再登録/再確立**シナリオにより実運用で近似するイベントを評価する。具体的には、電波減衰やセル再選相当のイベントを与え、Registration や PDU Session の再確立が円滑に行われるかを、NAS 再送やタイマ（T3xx）挙動とあわせて確認する（第 4 章）。

5.3.4 Android エミュレータの限界と実 UE 検証の必要性

通信機能を有する Android アプリケーションの検証において、PC 上のエミュレータのみでは再現困難な事象が多い。特に、セルラースタックや事業者設定、端末 OS の省電力・バックグラウンド制御など、**実機依存の挙動**がアプリの通信体験を大きく左右する。本研究では、sXGP+実 UE+5GC 構成により、以下の観点で**実機ならではの検証**を行う。

エミュレータで不足しがちな項目

- **セルラー制御プレーンの実挙動**: 実エミュレータはベースバンドを持たず、Registration/TAU、NAS 再送、タイマ境界での挙動差 (T3xx/Back-off 等) の忠実再現が困難。
- **IMS/音声・SMS 連携**: VoLTE/VoNR や SMS over NAS などは端末・キャリア・IMS の三者連携が必要で、エミュレータでは未実装/限定的であることが多い。
- **ネットワーク条件とスタック差分**: IPv6-only + NAT64/464XLAT、DNS64、PCO/APN パラメータ、MTU/MSS、NIC オフロード (TSO/GRO) 等の影響はエミュレータで再現しづらい。
- **OS によるバックグラウンド制御**: Doze/App Standby、JobScheduler/WorkManager のネットワーク可用性制御は実機の省電力・無線レイヤと結合しており、エミュレータでは挙動が異なる。
- **移動性・無線イベント**: RRC Idle/Connected の遷移、電波強度・セルリセクション、ハンドオーバー相当の切替など、時間軸のイベントは実無線でなければ発現しにくい。
- **ポリシ・スライス連携**: URSP やスライシングは端末/OS/事業者依存が強く、汎用エミュレータでは検証対象外となることが多い (本環境では制御/ユーザ面の相互接続検証を主対象とする)。

実 UE + sXGP + 5GC での検証手順 (例)

1. **端末側ログ取得**: logcat (特に radio バッファ) とネットワークログを収集し、アプリの API 呼び出しと無線/NAS イベントを時系列で突合する。
2. **ネットワーク側トレース**: コンバータ/5GC 側で S1AP/NGAP/NAS、GTP-U の pcap を取得し、再送、原因コード、TEID/フローの対応を解析する。

3. テストシナリオ:

- IPv6-only + NAT64/464XLAT 下でのアプリ接続 (DNS64 解決、QUIC/TCP の挙動差)。
- RRC Idle 復帰や電波減衰を伴う再接続でのセッション継続性 (ソケット再確立、タイムアウト)。
- 大きなパケットや損失率注入時の再送・バックオフ挙動 (アプリ層リトライ設計の妥当性)。

4. **再現性確保:** Docker 化した 5GC/コンバータ構成と固定シナリオにより、回帰テストとして継続的に実行可能にする。

本環境で得られる価値 実 UE を用いることで、シミュレータでは顕在化しにくい相互運用性問題や端末 OS 依存の振る舞い (例: NAS 再送シーケンスのズレ、IPv6-only 下での API 失敗、バックグラウンド時の接続断) を早期に発見し、パケットキャプチャと再現手順を添えて標準化・OSS 実装へフィードバックできる。

5.4 計測方法と指標

5.4.1 A/B 比較 (シミュレータ vs 実機)

- A: RAN シミュレータ + 5GC (OSS) B: sXGP eNB + 実 UE + 5GC (OSS)
- 比較対象: 登録/PDU 確立成功率、タイマ境界での失敗率、再送回数、エラーコード、スループット、遅延、リソース使用率
- ログ・トレース: S1AP/NGAP/NAS、GTP-U、カーネル/DPDK 統計、pcap

5.4.2 成功基準

基本機能の安定成立 (j99

5.4.3 成功判定基準と再現手順

判定基準

- 制御面: Initial UE/Context Setup および PDU Session 資源手順がエラーなく完了 (AMF/SMF ログ, NGAP トレース)
- ユーザ面: UE ↔ UPF 間で期待する TEID によりカプセル化され、連続したシーケンスで転送
- 安定性: 連続 N 回 (例: 30 回) の接続/切断試験で成功率 99%

再現手順 (成果物) 試験ごとに、(i) コンテナタグ/設定ファイル、(ii) Converter/AMF/UPF のログ、(iii) S1AP/NGAP/GTP-U の pcap、(iv) 計測スクリプトの出力 (CSV/JSON) を保存し、成果物として管理する。これにより、実装の回帰有無を定量的に判定できる [4]。

5.4.4 メトリクス (接続成功率、遅延、スループット、CPU/メモリ)

- 機能: 登録成功率、PDU セッション確立成功率、再登録時の成功率
- 性能: RTT (ICMP/TCP SYN-ACK)、スループット (iperf3)、再送率、フロー継続時間
- 資源: Converter/5GC の CPU 利用率、メモリ、コンテキスト数、TEID テーブルサイズ

5.4.5 ロギング・パケットキャプチャの取得方法

- Converter の S1AP/NGAP IF で pcap 取得 (制御面、フィルタ: SCTP, NGAP/S1AP ポート)
- Converter の S1-U/N3 IF で pcap 取得 (ユーザ面、フィルタ: UDP dst port 2152)
- AMF/SMF/UPF のアプリケーションログ (JSON/テキスト) を保存し、タイムスタンプで突合

NAS/NGAP/S1AP のメッセージシーケンスは、列挙型 (IE) と原因コードで比較する。必要に応じ、メッセージ時系列の可視化にシーケンス図生成ツールを用いる [5]。

第6章 相互運用性検証結果と実装ベース標準化への示唆

本章では、第5章で定義したシナリオに基づき、sXGP eNB + 実 UE + Open5GS + コンバータからなる環境で得られた相互運用性の評価結果を整理し、実装ベース標準化に向けた示唆を述べる。数値評価は本研究の主眼ではないため、結果は**定性的指標と達成/未達の観点**で記述する。必要に応じ、関連規格（TS [1, 2]）と実装（Open5GS [3]）への言及を行う。

6.1 結果

6.1.1 機能検証の結果（登録・PDUセッション）

総括 登録（Registration/Attach）およびPDUセッション確立の**基本機能は安定に成立**した。Converter は Initial UE/Context Setup の相互変換に成功し、AMF 側で UE Context が生成されることを確認した。PDU Session 資源手順では、**S1AP の ICS に内包された E-RAB 関連 IE を 5G の PDU Session 手順に直結させない設計**（第4章）が有効であり、手順の逐次化により AMF/SMF の前提条件を満たす運用が実現した。

発見された課題 初期段階では、AMF 側で unknown-PDU-session-ID 等の**整合性エラー**が観測された。原因は、S1AP の E-RAB 情報を契機に PDU Session 資源確保を同時進行させたことに起因する**手順の結合度**であった。**ICS と PDU Session Setup の分離**、および **NAS 透過方針の徹底**により解消できることを確認した。

6.1.2 性能測定の結果（遅延・スループット）

本研究は機能的相互運用を主対象とするため、性能は**ベースラインの健全性確認**を目的に評価した。UE → UPF → 外部ネットワークへの疎通は継続し、GTP-U のカプセル化/復号が想定通り動作した。sXGP の帯域/電波条件に依存するため**具体的指標は記さない**

が、**MTU/MSS 調整と再送挙動**に着目した際、明確な黒穴化や持続的劣化は観測されなかった。異常時はオフロード設定や経路 MTU の影響が大きく、**保守的なフラグメント方針**が有効であることを示した。

6.1.3 リソース使用率・スケーラビリティ

Converter は制御/ユーザ面を分離し、TEID テーブルと UE コンテキストを管理する構造である。試験の範囲では、CPU/メモリともに**顕著な逼迫は観測されない**。スケールに向けては、(i) TEID ルックアップのハッシュ最適化、(ii) ASN.1 エンコード/デコードのホットパス最適化、(iii) pcap/ログの**サンプリング運用**が有効である。

6.1.4 標準はあるが未実装・未相互運用の検証ケース

本節では、仕様上は規定されているが現場実装が未成熟／相互運用に課題がある代表例を挙げ、本環境（sXGP eNB + 実 UE + 5GC + コンバータ）で**実験可能な具体ケース**を示す。いずれも「基本的な 1 コール（登録・PDU セッション）が可能」であることを前提に、**実装ベース標準化の観点**での達成基準を定義する。

Case A: IPv6-only PDU + DNS64/NAT64/464XLAT 狙い: Rel-15 以降で IPv6-only が推奨される一方、端末の CLAT やアプリの v6 対応が未成熟で不具合が出やすい。手順: DNN を IPv6-only に設定し、UPF で NAT64、DNS64 を提供。Android 実機で CLAT 有効を確認し、HTTP/2、QUIC/HTTP/3 双方で疎通。

観測: logcat(radio,netd)、pcap(S1AP/NGAP/NAS, GTP-U)、アプリ疎通率。

成功基準: v6-only 環境でのアプリ成功率向上、名前解決（AAAA 合成）成功、CLAT 経路でのフラグメント/MTU 不具合が無いこと。

Case B: PCO パラメータ伝搬（DNS, MTU） 狙い: 仕様上は PCO で DNS/MTU 等が配布可能だが、UE/コア/変換部の処理抜けが散見される。

手順: 5GC/SMF 設定で PCO に DNS/MTU を設定し、コンバータで S1AP/EPS 相当とのマッピングを検証。

観測: UE の実際の DNS サーバ採用状況、path MTU に起因する再送/黒穴の有無。

成功基準: 端末が配布 DNS/MTU を採用し、アプリの初期ハンドシェイク失敗率が低下。

Case C: QoS 分離（デフォルト/専用ベアラ相当→5QI/QFI） 狙い: LTE のデフォルト/専用ベアラを 5GC の QoS フローにマッピングする際の整合性が課題。

手順: トラフィックフィルタ（TFT）と 5QI 差（例: 9 vs 7）を設定し、UPF でキュー/帯域差を可視化。

観測: QFI ごとのレイテンシ/スループット差、ドロップ時のプリエンブション挙動。

成功基準: 指定フローのみ帯域制御が有効、誤分類が発生しない。

Case D: UL-CL（上り分類）によるローカルブレイクアウト 狙い: 仕様は普及しつつあるが、設定・分類の相互運用が難しい。

手順: 2 段 UPF 構成で特定宛先/ポートをローカル UPF に分岐、その他は中央 UPF へ。

観測: TEID/Classifier 一致、遅延短縮、誤分岐の有無。

成功基準: ルール通りにトラフィックが LBO され、遅延が有意に短縮。

Case E: SSC モード 2/3 相当のセッション継続性（アプリ視点） 狙い: 仕様で規定されるセッション連続性の違い（IP 変更含む）にアプリが耐えられないことが多い。

手順: ネットワーク側で PDU 再確立（IP 変更）を誘発し、アプリの再接続/セッション維持を検証。

観測: ソケット再確立時間、ユーザレベル失敗率、リトライ戦略の有効性。

成功基準: IP 変更下でもユーザ体験の中断が最小化される（しきい値設定）。

Case F: DSCP/ECN の保存と QoS 反映 狙い: GTP-U カプセル化で DSCP/ECN の扱いが実装差で崩れやすい。

手順: アプリ/端末側で DSCP/ECN を付与し、UPF～外部ネットワーク間での保存・反映を確認。

観測: pcap でのビット保存、UPF キューイング差、ECN マークの往復伝搬。

成功基準: 端末→UPF→外部の各区間で規定通り保存/反映される。

Case G: GTP-U Path MTU Discovery/フラグメントの取り扱い 狙い: PMTUD 未実装や ICMP 遮断で黒穴化しやすい。

手順: 大きな MSS/DF で送出し、ICMP 応答と再送/分割の動作を観察。

観測: 黒穴検出時間、再送/スループット低下、ICMP 可視。

成功基準: 黒穴化せず経路 MTU に収束、アプリのスループット劣化が最小。

Case H: SMS over NAS（可能な範囲） 狙い: 仕様はあるが端末/IMS/コアの三者整合が難しい。

手順: コアの SMSF/NAS 経路が利用可能な場合に限り、端末からの SMS 送受を検証。

観測: NAS トレース上の SM メッセージ、配達成否。

成功基準: 端末→5GC→端末/外部への SMS 疎通が確認できる（限定条件付き）。

Case I: Paging 到達性と省電力（Idle 復帰） 狙い: 省電力や無線条件で Paging 到達が不安定になる実装差がある。

手順: UE を Idle に遷移後、下りトラフィックで Paging → Service Request の遷移を観測。

観測: Paging 応答率、復帰時間、失敗時の原因コード。

成功基準: 規定遅延内での安定復帰（しきい値）と高到達率。

Case J: 複数 DNN（APN）選択とフォールバック 狙い: 端末/ネットの DNN 選択・フォールバック挙動が規定とずれることがある。

手順: 存在しない DNN 要求→規定エラー→代替 DNN 確立の流れを試験。

観測: NAS 原因コード、再試行ロジック、最終確立率。

成功基準: 規定に沿った原因コードと適切なフォールバックで最終成功。

以上のケースは、**制御/ユーザプレーンの相互運用とアプリ体験の両面**を対象とし、シミュレータでは露呈しにくい**実機依存の問題**を洗い出す設計である。各ケースは、pcap・logcat・メトリクスと**再現手順**をセットで文書化し、標準化・OSS 実装への**具体的フィードバック**を可能にする。

6.2 考察

6.2.1 提案手法の有効性と限界

有効性 既存 eNB を変更せず 5GC に接続するという要件に対し、Converter の**手順分離**と NAS **透過**という方針は妥当であることが確認できた。UE 識別子・TEID・PDU Session の三者対応を状態として保持する構造は、相互運用で生じる差分を**局所化**でき、デバッグ容易性と安全側フェイルに寄与する。

限界 S1AP と NGAP は IE/手順が 1 対 1 対応ではないため、**完全変換は理論上成立しない**。N26 未利用の前提では、EPS/5GS 間の移動性最適化は対象外となる。また、UE/端

末 OS 依存の挙動（省電力、URSP 等）は Converter 外にあるため、検証の**外生要因**として扱う必要がある。

6.2.2 関連研究との比較と位置づけ

OSS 5GC や RAN シミュレータのみを用いた検証は、再現性と自動化に優れる一方、実 UE・実無線で露呈する相互運用性問題の捕捉が難しい。本研究は、sXGP という法令順守下での**実機検証**と、Docker 化による**再現性**を橋渡しし、**実装ベース標準化の PDCA** を短サイクルで回すための**現実的な折衷案**を提示するものである。

6.2.3 実運用への適用可能性

小規模な屋内網や PoC 段階において、Converter は既存 LTE 設備の延命・移行の**段階的アプローチ**として有効である。運用上は、(i) 顧客影響を避けるための**論理分離**、(ii) 障害時の**バイパス/フォールバック**、(iii) 監査証跡（pcap/ログ）を**継続取得**する体制が鍵となる。

6.3 ケーススタディと妥当性の脅威

6.3.1 実 UE 固有の事象（例：NAS 再送シーケンスのズレ）

端末実装や OS の省電力機構により、NAS の再送間隔や Back-off 挙動が**規定の許容範囲内でも体感差**を生みうる。Converter は NAS を終端しないため、**端末-5GC 間の整合性確保**が前提となる。試験では、ログと pcap の時系列突合により、端末依存の挙動を切り分けることが可能であった。

6.3.2 測定系の制約（時刻同期、NIC オフロードの影響）

高精度な片方向遅延計測は本研究の範囲外である。システム時刻同期は NTP で十分とし、**相対比較**を主に行った。また、TSO/GRO 等の **NIC オフロード**は再送/RTT 推定に影響しうるため、異常時は一時的に無効化して切り分ける運用とした。

6.3.3 内的/外的妥当性の脅威と緩和策

内的妥当性: 構成や設定の差分が結果に影響しうる。対策として、**コンテナタグ/設定スナップショット/pcap** を成果物として保存し、回帰検証に用いた。

外的妥当性: sXGP の屋内小規模環境は、屋外マクロセルや高負荷条件に直接は外挿できない。対策として、ZMQ シミュレーション（第 3 章）と**役割分担**し、機能相互運用は実機、性能スケールはシミュレータで評価する方針とした。

6.4 実装ベース標準化への示唆

- **手順分離の明文化:** S1AP の ICS と 5G の PDU Session 資源手順は**分離**し、逐次処理することを相互運用プロファイルで明記する（TS [2] の運用ガイドの補足）。
- **IE マッピング最小集合:** UE 識別子、E-RAB ↔ PDU Session、TNL 情報（GTP Tunnel）等の**最小 IE 集合**を定義し、欠落時は安全側フェイルとする実装指針。
- **最小 IOT テストセット:** Registration、PDU Session 確立、UL/DL 疎通、再登録（Idle 復帰）を**回帰セット**として自動化し、成果物（pcap/ログ）を共有できる形で定義する。
- **NAS 透過の原則:** Converter は NAS を終端せず、暗号・鍵管理は 5GC/UE で完結させる。例外運用は**研究用モード**に限定する。

第7章 結論と展望

7.1 本研究のまとめ

本研究では、実装ベース標準化を支援する実機検証環境として、免許不要帯で運用可能な sXGP (TD-LTE 互換) を eNB として活用し、4G RAN (UE・eNB) と 5G Core (5GC) を接続するコンバータを実装した。本環境により、電波法上の制約がある中でも法令遵守の範囲で実機検証が可能となり、標準仕様と実装の乖離を早期に検出する基盤を提供した。

具体的には、以下の成果を達成した：

- **プロトコル変換機能の実装:** S1AP/NGAP/NAS の信令変換と GTP-U トンネル中継により、4G RAN と 5GC 間の相互接続を実現した。登録・PDU セッション確立・データ転送などの基本機能が正常に動作することを確認した。
- **実装レベルの検証項目の確立:** PCO パラメータ処理、QoS/5QI 分離、SSC モード設定など、コンバータレベルで実装した相互運用性検証項目を動作確認した。さらに、IPv6-only + NAT64/464XLAT、UL-CL、GTP-U PMTUD、SMS over NAS、Paging、複数 DNN など、標準仕様は存在するが実装の成熟度や相互運用性に課題がある項目について、実機を用いた検証が可能な基盤を構築した。
- **再現性の高い実験環境の整備:** Docker 化により、環境構築手順を標準化し、異なる環境でも同一の実験を再現可能にした。これにより、継続的インテグレーション・回帰テストへの適用が可能となる。
- **実機検証の有効性の実証:** 実 UE を用いることで、シミュレータでは再現困難な実機特有の挙動（端末 OS 依存の処理、NAS 再送シーケンス、無線条件依存の挙動など）を検証できることを示した。

本研究の貢献は、3GPP の仕様ファースト型標準化プロセスを補完する形で、IETF の”rough consensus and running code”原則に基づく実装ベース標準化の実現可能性を示

したことにある。ソフトウェア中心の 5GC 実装が普及する中で、既存 4G RAN 資産を活用しつつ次世代コアへの移行を支援する実践的アプローチを確立した。

7.2 今後の課題

本研究で構築した環境は、実装ベース標準化の基盤として有効性を示したが、以下の課題と発展方向が存在する：

7.2.1 5G NR 対応への拡張

現在の実装は LTE 互換の sXGP を RAN として用いているため、5G NR 特有の PHY 機能（ビームフォーミング、massive MIMO 等）やスケジューリング最適化は対象外である。今後、免許不要帯で運用可能な 5G NR 基地局（sub-6GHz 帯またはミリ波帯）が利用可能になれば、NR 固有の無線レイヤー機能の検証にも対応できる。ただし、現時点でも制御面（NGAP/NAS）およびユーザ面（GTP-U）のプロトコルレベルでの相互運用性検証は十分に可能であり、標準化フィードバックの主要な価値はこのレイヤーにある。

7.2.2 より高度な検証ケースの実装

本研究で提案した 10 項目の検証ケース（Case A～J）のうち、コンバータレベルで実装済みの項目（PCO、QoS/5QI、SSC mode）については動作確認を行ったが、UL-CL、DSCP/ECN 保存、GTP-U PMTUD などの高度な機能については、Open5GS や UPF の拡張が必要である。今後、これらの機能を段階的に実装し、実機環境での検証を進めることで、標準化団体や OSS プロジェクトへのより具体的なフィードバックが可能となる。

7.2.3 標準化への実際のフィードバック実績

本研究では実機検証環境の構築と基本的な動作確認を行ったが、実際に標準化団体（3GPP）や OSS プロジェクト（Open5GS 等）へのフィードバックを行い、その効果を定量的に評価することは今後の課題である。検出した相互運用性問題を再現手順・パケットキャプチャとともにドキュメント化し、標準化議論や OSS 開発に貢献することで、実装ベース標準化の実効性を実証する必要がある。

7.2.4 自動テスト・CI/CD 環境への統合

現在の実験環境は手動での実行を前提としているが、継続的インテグレーション（CI）環境に統合し、コード変更のたびに自動的に実機検証を実行する仕組みを構築することで、回帰テストと品質保証を強化できる。GitHub Actions や GitLab CI 等の CI/CD プラットフォームとの連携により、標準化と OSS 開発の両面でアジャイルな開発サイクルを支援する。

7.2.5 6G 時代への展望

6G 時代に向けては、標準化サイクルのさらなる高速化が求められる。本研究で確立した実装ベース検証の手法は、6G 標準化においても有効であり、仕様策定の初期段階から実装を動かしながら標準化を進めるアプローチを促進する。特に、AI ネイティブな通信システムやテラヘルツ帯通信など、新しい技術要素が導入される 6G において、実機検証と標準化の並行進行は不可欠である。免許不要帯を活用した研究・教育基盤として、6G 標準化における実装ベース検証の促進に貢献することが期待される。

謝辭

参考文献

- [1] 3rd Generation Partnership Project (3GPP). System architecture for the 5g system (5gs). 3GPP TS 23.501, 2024. Technical Specification 23.501.
- [2] 3rd Generation Partnership Project (3GPP). Procedures for the 5g system (5gs). 3GPP TS 23.502, 2024. Technical Specification 23.502.
- [3] Open5GS Project. Open5gs: Open source 5g/4g core network, 2025. <https://open5gs.org/> (accessed 2025/01/18) .
- [4] Ronny Bull, Rachel Dudukovich, Juan Fraire, Nadia Kortas, Robert Kassouf-Short, Aaron Smith, and Ethan Schweinsberg. Network emulation testbed capabilities for prototyping space dtn software and protocols. pages 1–8, 05 2024.
- [5] Juan A. Fraire, Olivier De Jonckère, and Scott C. Burleigh. Routing in the space internet: A contact graph routing tutorial. *Journal of Network and Computer Applications*, 174:102884, 2021.

付録
