2-3　エマージングセキュリティ技術
2-3　Emerging Security Technology

2-3-1　5G ネットワークにおけるセキュリティ確保に向けた取組
2-3-1　Efforts to Ensure Security in 5G Networks

澤本 敏郎　鈴木 未央　大迫 勇太郎　中尾 康二
SAWAMOTO Toshiro, SUZUKI Mio, OSAKO Yutaro, and NAKAO Koji

第 5 世代移動通信システム（5G）は現在国内をはじめ世界中で運用が広がっている。5G では超高速大容量、超高信頼低遅延、超多接続の 3 つの厳しい要求条件を達成するため、従来の移動通信のプロトコルを一部踏襲しつつ、これまでにはない全く新しい技術や概念が導入されている。これはサービス利用者に対し新しい体験をもたらし、運用側にとっても仮想化等によりシステム構築や運用の自由度を高め、新しいサービスを提供できるメリットがある一方で攻撃者にとってのアタックサーフェスを一層拡大させる可能性についても指摘 [1] されている。サイバーセキュリティ研究所では、こうした脆弱（ぜいじゃく）性につながる可能性に対応し安全な 5G ネットワークを確保するため、外部組織とも連携し様々な研究開発を行っている。本稿ではこれまでに実施した 5G ネットワークに関するセキュリティ確保に向けた研究開発と、今後のセキュリティ検証強化の方向性に関する検討について報告する。

The fifth-generation mobile communication system(5G) is being rolled out not only in Japan but also around the world. 5G system introduces a whole new technology and concept to fulfill harsh requirements such as eMBB, URLLC, and mMTC while following some of legacy technologies. This brings a new experience to customers, also improves flexibility of building system and operation as well as having advantages of providing new services, however has potential probability to expand attack surfaces to a malicious attacker. Cybersecurity Laboratory has been working on research and development for ensuring secure 5G network to treat those potential vulnerability while working together with external organizations. In this paper, we report our research and development toward ensuring secure 5G network and evaluation regarding enhancement of our 5G security validation from now on.

1　まえがき

1979 年に自動車電話として登場した第 1 世代の移動通信システム（1G）は、2024 年 5 月現在で実に第 5 世代まで進化を遂げている。当初は自動車での使用を想定した重さ数キロの第 1 世代の移動端末も現在では片手で簡単に操作できるタブレット型の端末や、身につけて使用する腕時計タイプの端末等へと変貌を遂げた。通信プロトコルも、音声波形をそのまま搬送波に乗せる第 1 世代のアナログ方式から、第 2 世代（2G）の PDC（Personal Digital Cellular）方式ではデジタル化され、第 3 世代（3G）の W-CDMA（Wideband Code Division Multiple Access）、第 4 世代（4G）の LTE（Long Term Evolution）そして第 5 世代の 5G へと進化 [2] した。

日本国内では 2020 年より商用サービスが開始された 5G は、3GPP（3rd Generation Partnership Project）と呼ばれる標準化団体においてプロトコルが規定されており、超高速大容量（eMBB、Enhanced Mobile Broadband）、超高信頼･低遅延（URLLC、Ultra-Reliabile and Low Latency Communications）、超多数端末接続（mMTC、massive Machine Type Communication）の 3 つの厳しい要求条件を満たすべく従来の移動通信のプロトコルを一部踏襲しつつ、新しい技術や概念の導入により大幅な刷新が行われている。例えば物理レイヤにおいては Massive-MIMO などの空間多重技術による細やかなビーム制御がもたらす周波数利用効率

の向上や、LDPC 符号や Polar 符号などのより強力な誤り訂正方式の導入等により、これまで以上にシャノン限界にも近づく理論スループットを実現している。また、コアネットワークにおいては、従来の機能ブロック間における point-to-point の通信から、細分化されたコア機能である NF（Network Function、5G コアネットワークにおける機能ブロック）同士が HTTP/2 プロトコルによりメッシュ的に通信できる SBA（Service Based Architecture）と呼ばれる構成が導入された。さらに、近年の演算装置の処理性能の飛躍的な向上も手伝い、5G では、汎用計算機を活用した仮想化技術の採用を可能とし、従来のような通信事業者の施設内を中心とした閉じたエリア内での専用ハードウェアによるネットワーク構成からクラウド等も活用したより自由度の高いシステム構築も視野に入れることができるようになった。こうした進化は様々な業者の新規参入の障壁を下げることにも貢献しており、例えば大手通信事業者の展開する「パブリックネットワーク」とは別に、オフィスや工場など「ローカル 5G」と呼ばれるノンパブリックな 5G ネットワークの設置が今後ますます増加することが予想される。この状況は、5G ネットワークの普及を促進し、革新的なキラーコンテンツの誕生を大いに後押しするものである一方、通信事業者にとってはこれまで経験したことのないネットワーク構成への対応を迫られ、また、移動通信ネットワークの運用経験の浅い新規参入業社によるローカル 5G の運営など、脆弱性の可能性につながる要素がこれまで以上に増加することも考えられる。

これらの状況に鑑み、サイバーセキュリティ研究所では、外部組織とも連携し、安心・安全な 5G ネットワーク実現のため、5G セキュリティに関する基礎的な検証や調査など様々な研究開発に取り組んでいる。まず、令和元年度から令和 3 年度にかけて 4 社共同プロジェクトである総務省委託案件「5G ネットワークにおけるセキュリティ確保に向けた調査・検討等の請負（令和 3 年度 0049-0022）」に参加し、基本的な 5G ネットワークにおけるセキュリティ検証を実施した。本プロジェクトの成果としてセキュリティガイドライン第 1 版を 4 社共同で発行し、現在総務省のウェブサイト [3] において公開されているとともに ITU-T における勧告化 [4] も進められている。また、令和 5 年度における総務省委託案件「5G ネットワークにおけるセキュリティ確保に向けた調査・検討等の請負（令和 5 年度 0049-0248）」では、KDDI デジタルセキュリティ株式会社と共同で標準化団体等における 5G セキュリティに関する最新トレンドやユースケースの種類及びそのリスク、Beyond5G / 6G を見据えたセキュリティリスク、ローカル 5G や O-RAN、5G セキュリティラボ事例など、移動通信におけるセキュリティリスクやその対策、今後の標準化動向や諸外国の 5G セキュリティに関する取組等についての最新情報に関する調査を実施している。

本稿では、まず、**2** で令和元年度から令和 3 年度にかけて実施した総務省委託案件において取り組んだ 5G ネットワークにおけるセキュリティの基本検証と、その成果である 5G セキュリティガイドラインの内容について、**3** では令和 5 年度に実施した総務省委託案件における調査結果をもとに検討した、今後のサイバーセキュリティ研究所における 5G ネットワークのセキュリティ検証強化について、それぞれ説明を行う。最後に **4** でまとめと今後の方向性について述べる。

2　5G セキュリティ基本検証

2.1　背景

日本国内における 5G サービスは、4G ネットワークから 5G ネットワークへの段階的な移行のため、NSA（Non Stand Alone）と呼ばれるネットワーク構成から SA（Stand Alone）と呼ばれるネットワーク構成へと移行しており、現在は国内通信事業者各社において SA 型のサービスエリアが順次拡大されている。4G ネットワークから 5G ネットワークへのスムースな移行のための NSA 型は、EPC（Evolved Packet Core）と呼ばれる 4G のコアネットワークに 5G の無線基地局である gNB（global Node B）を接続し、制御情報は 4G ネットワーク経由、ユーザ情報は 5G ネットワーク経由でそれぞれ通信を行うのに対し、SA 型のネットワークは無線基地局及びコアネットワークの全てが 5G 専用のプロトコルで構成されている。SA 型の 5G サービスは高スループット化や低遅延化といった単なる技術的な性能向上にとどまらず、この特徴的な機能が多様な社会基盤のインフラや制御系システム等へ利活用されることも想定されており、産業のみならず我々の生活環境をも大きく高度化することが期待されている。一方で、5G ネットワークの様々な社会基盤への適用が進み、よりミッションクリティカルな領域にも 5G 技術が浸透することで、5G ネットワークの安全性が社会環境に及ぼす影響も大きくなると考えられる。

これまで概説したとおり、5G ネットワークは、多様な分野での活用を見据え、様々な新しい技術や概念が導入されている。**1** で説明した 5G ネットワークの仮想化や SBA のほか、NEF（Network Exposure Function）と呼ばれる NF を介し、5G ネットワーク内の他の NF の機能や情報の一部を API により外部のアプリケーションへ開示する機能も定義されている。また、5G を取り巻く環境も様変わりしてきている。例えば、仮想

化 5G ネットワークを汎用計算機上に簡単に構成することが可能なオープンソースソフトウェア [5][6] が様々な研究機関や大学等において開発されている。本来は 5G ネットワークシステムのコモディティ化や普及促進を目的としたものであるが、構築の手軽さと完成度の高さからオープンソースを悪用した様々な攻撃の可能性についても指摘 [7] されている。もちろんこれらは 5G の新しい側面のごく一部に過ぎないが、これらの新しい技術をどのように組み合わせることで管理、設定し、あるいはオープンソースソフトウェア等の悪用により今後出現するであろう新しい脅威にどのように対応することで安全に 5G ネットワークを運用することができるかに関しては、一般的には 5G サービスを展開する通信事業者各社や通信機器メーカが個別に検証を重ね、ノウハウを蓄積する必要がある。

令和元年（2019 年）当時、日本国内においては 5G のサービスインに向け個々の通信事業者や通信機器メーカが、安心・安全な 5G ネットワークの実現に向けたセキュリティに対する取組を模索しつつ技術開発を進めている状態であった。それと同時に、上述のような全く新しい 5G ネットワークの安全な設定や運用、機器の設計や新しい脅威への対応に関する包括的なガイダンスに対する要望も、国内において 5G ネットワークの運用を目指す通信事業者や通信機器メーカの間で高まりつつある状況であった。この状況に対処するため、我が国においては、5G ネットワークのセキュリティ課題の洗い出しと対策の推進を目的に、通信事業者である KDDI 株式会社及び株式会社 NTT ドコモ、通信機器メーカである日本電気株式会社及び NICT サイバーセキュリティ研究所が連携し、5G セキュリティガイドラインの発行に向け総務省の請負案件である「5G ネットワークにおけるセキュリティ確保に向けた調査・検討等の請負（令和 3 年度 0049-0022）」に関する研究開発を行った。

2.2　検証の全体概要

本プロジェクトでは、オープンソースの 5G ネットワークシステムを活用した 5G セキュリティに関する総合的な検証環境を構築し、ファジングや DoS 攻撃などのコアネットワークを対象とした脆弱性に関する検証、3GPP 標準仕様の定めたセキュリティ仕様からの逸脱の有無に関する検証であるセキュリティコンフォーマンステスト、コンテナ及び仮想化混在環境のセキュリティに関する検証、NF に仕込まれた不正機能検知など、各社が今後の 5G サービスの急速な展開において想定される脅威に着目したテーマについて、様々な角度からの実機検証を行っている。検証に必要なソフトウェアはオープンソース 5G ネットワークのソースコードをベースに作成したものや、C 言語等により自前で作成、あるいはネットワークテスタと呼ばれる 5G ネットワークの動作検証に使用されるソフトウェア等を活用した。検証内容及びその結果について以下に概説する。

2.2.1　ファジングテスト

本検証では、悪意のある攻撃者がコアネットワーク内のノードへ侵入している前提でコア内部のインターフェースに対するファジングテストを実施した。ここでは脅威分析の結果から 5G ネットワークの運用に深刻な打撃を与えると考えられる NRF（Network Repository Function、各 NF のサービスを登録する機能を持つ）を対象に選定し検証を実施した。その結果、NF 登録要求メッセージの長い URI 文字列の処理に関する不具合を発見した。

2.2.2　DoS 攻撃

仮想化基盤上に基地局 10 台と UE（User Equipment、ユーザ端末）エミュレータ 1.3 万台を構成、UE 登録メッセージの大量送信によるコアネットワーク側への負荷状況を確認した。AMF（Access and Mobility Management Function、UE のアクセスと移動を管理する NF）における CPU 使用率の異常な上昇等は観測されず、トラフィック増による単純な DoS 攻撃に対しては冗長化や仮想化によるスケーリング等の一般的な対策で対応可能と考えられる。しかしながら、UE 登録メッセージをリプレイすることで悪用した DoS 攻撃では 5G コアネットワークの可用性を妨げる深刻な脆弱性が確認された。この脆弱性検証についてはサイバーセキュリティ研究所が担当しており、別途 **2.2.6** にて詳しく説明する。

2.2.3　セキュリティコンフォーマステスト

セキュリティコンフォーマンステストでは、5G システムが保証すべきセキュリティ要件を整理し、3GPP SCAS（Security Assurance Specification、ネットワーク機器のセキュリティ要件を定めた仕様）でカバーされていないテストシナリオを作成し検証を行った。その結果、認証の度に更新されるべき SUCI（Subscriber Concealed Identifier、暗号化された加入者識別子）が更新されない、不正な AS（Access Stratum、無線インターフェースで動作するプロトコルスタック）アルゴリズムを受け入れる、ネットワークのケーパビリティ情報が保護されていないなど、主に実装不足や設定不足に起因すると考えられるセキュリティ要件からの逸脱を発見した。

2.2.4　コンテナ・仮想化混在環境のセキュリティ

5G ネットワークにおいて特徴的なインフラ構成の一つであるコンテナ及び仮想化混在環境におけるセキュリティに関し検証を行った。現在想定される通信事業

者におけるコアネットワーク設備の構築方法として、URLLCサービス等の提供のために、5Gコア、特にUPF（User Plane Function、ユーザ情報を処理するNF）をユーザロケーション近くに配置し、物理的に異なる仮想化基盤上に構成することが考えられる。このことから、本検証では別拠点を想定したMEC（Multi-access Edge Computing、モバイル機器からのアクセスに特化したエッジコンピューティング技術）環境と5Gコアを稼働させる環境である静的ネットワークスライス環境（ネットワークスライスについては**3.2**を参照）の構成を検証対象としている。本構成において、MEC環境内部への侵入拡大や攻撃の影響拡大を引き起こす可能性のあるセキュリティ課題に関し検証シナリオを作成し検証を行った結果、物理サーバや仮想化レイヤ、NF等の複数の観点における適切なアクセス制御や認証の導入により侵入拡大を防止できること、スライス間のリソースの適切な分離、例えば同一のHypervisor（サーバ仮想化等で利用されるコンピュータを仮想化するための制御プログラム）において物理リソースの過剰コミットを防止し適切に分離、制限、確保を実施することにより、ネットワークスライス間における攻撃の影響を回避できること等を明らかにした。

2.2.5　不正機能検知に関する検証

サプライチェーンリスクの顕在化がICT分野で喫緊の課題となっている。上述のとおり5Gにおいては仮想化によるネットワーク構築が主流になると考えられており、5Gにおけるインフラにおいても同様のリスクに対する対策が必要である。本検証ではサプライチェーンリスクの一つであるソフトウェアへの不正機能混入リスクを踏まえ、5Gシステム、特にバイナリファイルで提供されると考えられるNFにおける不正機能（バックドア）混入リスク対策の一つとして不正機能検出可否の検証を実施した。AMFのソースコードに対して不正機能のサンプルコードを組み込み検証用バイナリを作成、独自に研究開発を行っている不正機能検知ツールによる検査により有効性を確認した。呼び出し元の関数が存在せず、処理フロー上到達不可能なコードブロックであるデッドコード処理を悪用したバックドアを埋め込み、ユーザ端末や保守運用者が脆弱性を悪用するメッセージを送信することでバックドアを起動させる様々なタイプのサンプルコードを検証用に作成した。このバイナリにおいて、不正機能検知ツールによる検査を実施したところ、すべての不正機能コードの検知に成功し、サプライチェーンにおける5Gコアのソフトウェアに対する不正機能混入リスク対策、セキュリティ保証の観点における不正機能の検査フェーズの重要性及び検証に用いた不正機能検知ツールの有効性を確認することができた。

2.2.6　UE登録メッセージを悪用したDoS攻撃

2.2.2に記載のとおり、サイバーセキュリティ研究所では、本プロジェクトにおいてUE登録メッセージをリプレイし悪用したDoS攻撃に対する5Gコアネットワークの耐性について検証を行い、その可用性を妨げる深刻な脆弱性を確認した。検証内容及び結果について以下に詳述する。

2.2.6.1　検証概要

本検証は、攻撃者にとって比較的攻撃が容易なNFであるAMFをターゲットとしている。AMFは5Gにおけるユーザ端末及び無線基地局を含む無線アクセスネットワークのプロトコルが終端されるコアネットワーク内における唯一のNFであり、ユーザ端末からのアクセスやユーザ端末の移動管理などの機能を持っている。

図1に示すように、ユーザ端末は、電源ONと同時

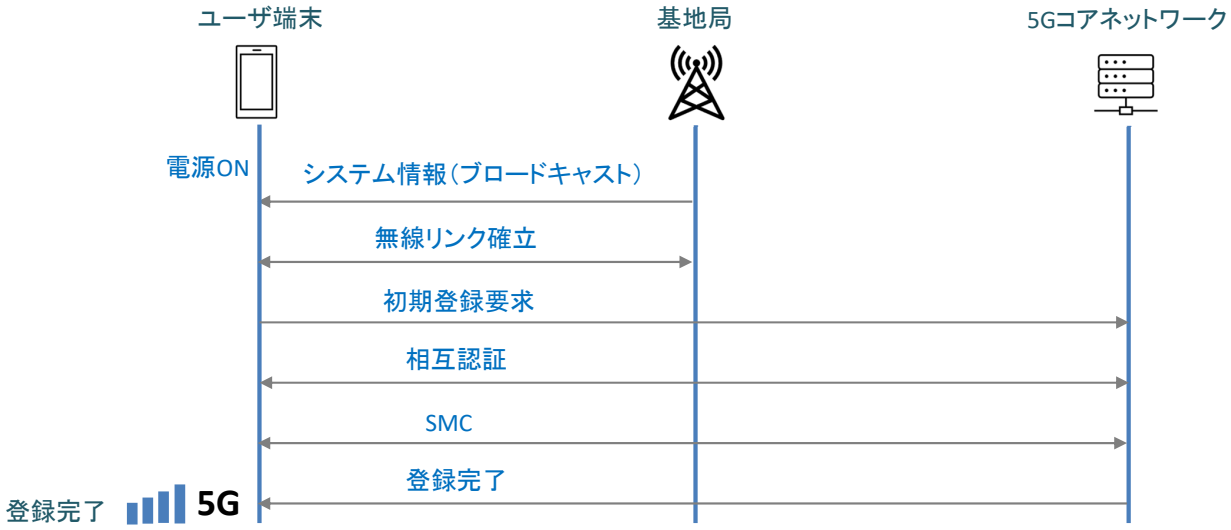

図1　ユーザ端末の5Gネットワークへの登録シーケンス

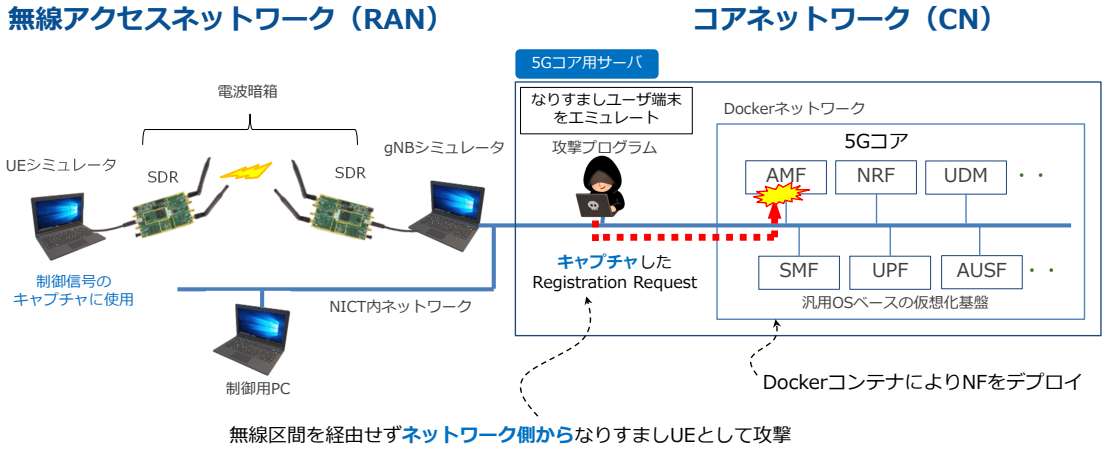

図 2　検証系

図 3　無線アクセスネットワーク検証系（左：全体構成、右：電波暗箱内）

に基地局よりブロードキャストされているシステム情報を受信したのちに無線リンクの同期を確立し、5G ネットワークに対し初期登録と呼ばれる相互認証処理を実施する。続いて暗号化に使用するセキュリティアルゴリズムの合意である SMC（Security Mode Control）が実施される。この一連の相互認証処理及び合意 [8] が完了して初めてユーザ端末は 5G ネットワークに正規のユーザとして認識され、サービスを安全に使うことが可能となる。

初期登録時における相互認証処理では、ユーザ端末は Registration Request と呼ばれる登録要求メッセージを送信する必要がある。Registration Request には SUPI（Subscription Permanent Identifier）と呼ばれる加入者識別子が暗号化された SUCI（Subscription Concealed Identifier）が含まれており、5G ネットワークにあらかじめ当該識別子が登録されているユーザのみ相互認証に成功するようになっている。本検証では、この Registration Request を SUCI ごとキャプチャし AMF へリプレイ送信することで、正規ユーザになりすました DoS 攻撃を行った。

2.2.6.2　検証系

図 2 に検証系の全体図を示す。

検証系は RAN（Radio Access Network、無線アクセスネットワーク）及び CN（コアネットワーク）より構成され、すべて NICT 内ネットワークに構築した。無線アクセスネットワークは、オープンソースの UE シミュレータ及び gNB シミュレータのインストールされた Linux PC と、実際の 5G プロトコルの無線信号を送信することが可能な図 4 の SDR（Software Defined Radio、ナショナルインスツルメント社 USRP-2901）により構成され、電波が外部に漏洩（ろうえい）しないようアンテナ部分は図 3 のような暗箱内に設置されている。暗箱内の左右には UE シミュレータ用及び gNB シミュレータ用のオムニアンテナが送受信それぞれ 1 本、合計 2 本ずつ設置されている。一方コアネットワークはすべて NICT 内ネットワークの Linux サーバ内に Docker コンテナ [9] により構築されている。コアネットワーク内の NF は Docker compose[10] により全て同じサブネットにデプロイされている。

2.2.6.3　検証方法

(1) Registration Request のキャプチャ

DoS 攻撃に悪用する Registration Request は、図 2 のような検証ネットワーク上において TShark などのフリーのパケットキャプチャツールを用いることで簡単にキャプチャすることができる。図 5 に 5G ネットワークにおけるワンコールシーケンスの実際のキャプチャ結果を示す。ワンコールとは、ユーザ端末が 5G ネットワークへの初期登録を経てユーザデータ（ここでは ping）の送受信を実施し終呼するまでの一連の処理を示している。Registration Request は図中の赤い点線で囲まれた No.15 の部分に該当する。

(2) 攻撃プログラム

実環境における攻撃の場合、例えばユーザ端末が無線区間を経由し 5G コアネットワークに対し攻撃を実施するパターンが考えられるが、ここでは 5G コアネットワークの脆弱性検証が目的であるため、無線区間を経由する攻撃ではなく、攻撃者が 5G ネットワークに入り込み自由にアクセスできる前提で、ネットワーク側から直接 AMF を攻撃することとした。

DoS 攻撃を実施するプログラムは C 言語により構築し、通常の gNB のように、まず AMF との間に SCTP セッションを確立した後に NG Setup Request を送信、続いて事前にキャプチャした Registration Request を設定回数分送信する機能を持つものとした。5G では gNB-AMF 間の N2 論理インターフェースにおいて SCTP が採用されており、N2 においてやりとりされる NGAP と呼ばれるプロトコルのメッセージが SCTP の DATA チャンクのペイロードとしてマッピングされている。Registration Request を受信すると、AMF は認証に必要な情報を含む制御メッセージである Authentication Request をユーザ端末へ返すが、攻撃プログラムでは AMF からの Authentication Request を全て無視して Registration Request を規定回数に達するまで一方的に送信し続けるものとする。ここで、NG Setup Request とは、gNB と AMF が正しく相互運用するために必要なアプリケーションレベルのデータの交換に使用されるメッセージである。

図 4　SDR

2.2.6.4　検証結果

本検証では、5G ネットワークの可用性を損なう恐れのある二種類の脆弱性について確認された。いずれも、相互認証が確立する前の制御メッセージを UE 及びネットワークが暗黙的に信頼するという、AKA と呼ばれるプロトコルの元々の思想に起因している。

(1) DoS 攻撃に対する脆弱性

本検証において、まず Docker コンテナとしてデプロイされている NF のクラッシュが確認された。DoS 攻撃により最初にクラッシュしたのは直接の攻撃対象である AMF であるが、UDR（User Data Repository、

ngap || http || pfcp || gtp

No.	Time	Source	Destination	Info
7	3.032490	172.29.16.20	172.29.16.8	NGSetupRequest
10	3.035455	172.29.16.8	172.29.16.20	NGSetupResponse
15	5.499916	172.29.16.20	172.29.16.8	InitialUEMessage, Registration request
19	5.521515	172.29.16.8	172.29.16.20	DownlinkNASTransport, Authentication request
20	5.522034	172.29.16.20	172.29.16.8	UplinkNASTransport, Authentication response
21	5.529495	172.29.16.8	172.29.16.20	DownlinkNASTransport, Security mode command
22	5.529630	172.29.16.20	172.29.16.8	UplinkNASTransport, Security mode complete, Registration request
23	5.569800	172.29.16.8	172.29.16.20	InitialContextSetupRequest, Registration accept
24	5.570035	172.29.16.20	172.29.16.8	InitialContextSetupResponse
25	5.570116	172.29.16.20	172.29.16.8	UERadioCapabilityInfoIndication
26	5.570142	172.29.16.20	172.29.16.8	UplinkNASTransport, Registration complete
29	7.499543	172.29.16.20	172.29.16.8	UplinkNASTransport, UL NAS transport, PDU session establishment request
32	7.530112	172.29.16.10	172.29.16.2	PFCP Session Establishment Request
33	7.535809	172.29.16.8	172.29.16.20	PDUSessionResourceSetupRequest, DL NAS transport, PDU session establishment accept (PDU sess
34	7.536209	172.29.16.20	172.29.16.8	PDUSessionResourceSetupResponse
38	9.500445	60.60.0.16	172.29.16.21	Echo (ping) request id=0xabcd, seq=16236/27711, ttl=64 (no response found!)
43	9.532575	172.29.16.21	60.60.0.16	Echo (ping) reply id=0xabcd, seq=16236/27711, ttl=63
44	10.500233	60.60.0.16	172.29.16.21	Echo (ping) request id=0xabcd, seq=16237/27967, ttl=64 (no response found!)
47	10.501370	172.29.16.21	60.60.0.16	Echo (ping) reply id=0xabcd, seq=16237/27967, ttl=63
48	11.500228	60.60.0.16	172.29.16.21	Echo (ping) request id=0xabcd, seq=16238/28223, ttl=64 (no response found!)
52	11.501144	172.29.16.21	60.60.0.16	Echo (ping) reply id=0xabcd, seq=16238/28223, ttl=63

UEから登録要求
UEとコアネットワーク間での相互認証
暗号化アルゴリズムの決定
登録許可
登録完了
PDUセッション確立
ping送受信

図 5　ワンコールシーケンス

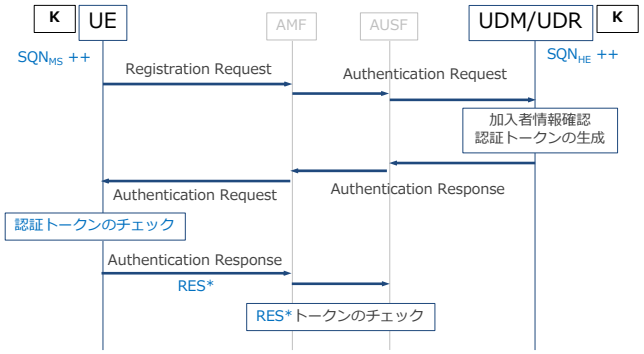

図 6　5G ネットワークにおける相互認証シーケンス (5 G-AKA)

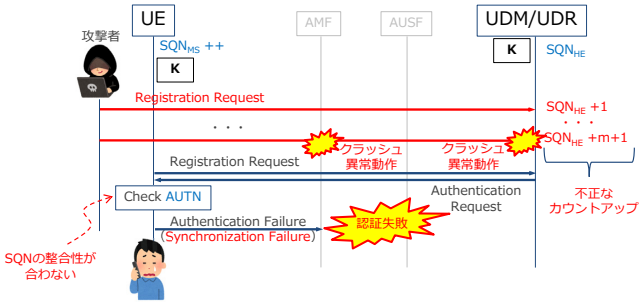

図 7 5G-AKA において認証失敗を誘発するメカニズム

5G コアにおいて加入者情報や在圏情報など、アプリケーションやシステムの設定情報をまとめて記録する NF) など、AMF 以外の NF も連鎖的にクラッシュすることが確認された。図 6 に 5G ネットワークにおける相互認証方式の一つである 5G-AKA [11]の制御メッセージのシーケンスを示す。5G-AKA では、AMF はユーザ端末からの Registration Request を受信すると、メッセージに含まれる加入者識別子が当該 5G ネットワークに登録されている正規のユーザであることを確認するため認証手順を開始し、AUSF (Authentication Server Function、5G における認証を担う NF) へ認証要求を送信する。AUSF は更に UDM (Unified Data Management、AKA にて使用する認証クレデンシャル生成や加入者データ、セッション情報などの格納や提供を行う情報管理を担う NF) に対し、認証に必要な認証トークン等の生成を要求する。UDM は、AUSF より受信した加入者識別子が正規のユーザであるかどうかを確認するため UDR に対し問い合わせを実施する。UDR は保存されている加入者情報と照らし合わせた結果を、リプレイ防止用のシーケンス番号である SQN をインクリメントしたものと合わせて UDM へ通知する。UDM は、これらの情報を基に、認証に必要なトークンや鍵の生成を行い、これらを含む認証ベクトルを認証応答として AUSF へ送信することで相互認証プロトコルが開始される。認証に必要なトークンは AUSF から AMF を経由し、最終的に認証要求としてユーザ端末へ届けられる。ユーザ端末では 5G コアネットワークと共有している秘密鍵により認証トークンを検証する。検証に成功した場合は、ユーザ端末はネットワークが認証されたとみなすとともに、RES と呼ばれるトークンを AMF 及び AUSF へ返すことで認証処理を継続する。AUSF では RES トークンの検証を実施し、成功した場合に相互認証が完了したとみなされる。このように、5G ネットワークにおけるユーザ端末の認証処理には様々な NF が関わっており、お互いに情報をやり取りすることによって相互認証処理が行われている。

AMF は、相互認証処理を開始するため、受信したすべての Registration Request を暗黙的に信頼してデコードし、その都度他の NF に対し問い合わせを行う必要がある。本検証において見られた連鎖的な NF のクラッシュは、AMF が DoS 攻撃である Registration Request を受信する度に実施する他の NF に対する問い合わせが結果的に新しい DoS 攻撃となることで引き起こされていると考えられる。

なお、これらの NF は毎回クラッシュするわけではないが、クラッシュしなかった場合においても通常は “healthy” であるはずの Docker コンテナのステータスが “unhealthy” となったり、ステータスが “healthy” であるにもかかわらずレスポンスが無くなりフリーズする、オールゼロの認証トークンを返す、不明な IP アドレスのユーザ端末へ Authentication Request を返す等の異常な動作が確認された。AMF が DoS 攻撃のスピードについていけなくなった場合に処理破綻し、クラッシュや “unhealthy” な状態に陥っていると考えられる。

対策としては、エラーハンドリングのプロセスを追加することが望ましいと考えられる。5G におけるプロトコルが規定されている 3GPP 標準仕様では、同一の加入者識別子を持つユーザから、全く同じ内容の Registration Request が何度も立て続けに送信されるシーケンスは規定されていない。Registration Request に限らず、このようなイリーガルな制御情報を受信した場合におけるエラーハンドリングプロセスをあらかじめ実装しておくことが 5G ネットワークの可用性確保に有効であると考えられる。

(2) 相互認証の失敗を誘発する脆弱性

本検証では、相互認証の失敗を誘発する脆弱性についても確認された。5G-AKA では、図 7 のように、共有される秘密鍵 K に基づき相互認証処理が実施される。この相互認証処理は、Authentication Request のリプレイ送信防止のため、ユーザ端末及びネットワークでそれぞれ個別に管理している SQN (シーケンス番号) によるワンパスプロトコルとなっている。相互認

証が実施される度に、SQN_{MS} はユーザ端末が、SQN_{HE} はネットワーク側がそれぞれインクリメントし、ユーザ端末側でこれらのシーケンス番号の一致を確認した場合にのみ相互認証処理が継続される仕組みとなっている。一方、ネットワーク側には、Registratin Request に対するこうした機能は標準仕様で定義されていない。本検証では、正規ユーザになりすました攻撃プログラムからの Registration Request を悪用した DoS 攻撃により、ネットワーク側のシーケンス番号である SQN_{HE} が不正にカウントアップされることを確認した。これによりユーザ端末側での認証トークン検証時に実施される SQN の整合性確認において不一致となり、最終的に相互認証の失敗が誘発される。

ユーザ端末と 5G コアネットワーク間においてやりとりされる制御メッセージは NAS メッセージ [12] と呼ばれ、図 1 の SMC 手順を使用して機密性及び完全性が保護され、リプレイプロテクションも適用される。一方でセキュリティ保護が有効になる前は、特定のケースにおいてセキュリティ保護のない NAS メッセージの送受信が許容されている。本検証において DoS 攻撃に悪用した Registration Request は、ユーザ端末の初期登録時における最初の NAS メッセージであることから、特に初期 NAS メッセージと呼ばれ、ユーザ端末がセキュリティコンテキストを持たない場合は、セキュリティ保護されていない制御メッセージの送受信が標準仕様において許容されている。したがって、標準仕様の面からは不正にキャプチャした Registration Request を何度繰り返し送信しても正規のメッセージであるとコアネットワークに誤認識させることが可能であり、本検証から、それが実機検証によっても明らかとなった。

対策としては、初期 NAS メッセージにおいてもリプレイプロテクションを導入し、できるだけ他の NF へ悪影響を及ぼさないよう AMF 内で閉じて判定を実施することが望ましいと考えられる。

2.3　5G セキュリティガイドライン

本プロジェクトにおける成果として、4 社共同で 5G セキュリティガイドライン第 1 版を発行した。本ガイドラインでは、5G ネットワークにおいて想定されるセキュリティ脅威を図 8 に示す 7 つに分類し、各項目に関し STRIDE-LM モデルによる脅威分析を行っている。

これらの 7 つの分類結果には関連する脅威アクターへのリンク付けも行われている。さらに、これらの分類結果に対し 5 つのセキュリティ対策要件を定義しており、**2.2** で説明した実機による検証で得られた知見も盛り込まれている。例えば **2.2.6** で説明した UE 登録メッセージを悪用した DoS 攻撃は「なりすまされた登録要求」として「コアネットワークに対する脅威」に分類されており、ユニークな ID が付与され、その対策要件は「技術的対策」の「CN」の項に記載されている。

本ガイドラインは、5G システムの安全な展開の出発点として、ハイレベルな記載による実用的なアドバイス提供を目的としており、サービスプロバイダや通信事業者、通信機器メーカを想定読者としている。なお、ここでは 5G SA システムの無線アクセスネットワーク及びコアネットワーク、仮想インフラ及び管理システムをスコープとしており、NSA システムについてはスコープ外としている。また、図 8 からもわかるとおり、技術的な側面のみならず 5G セキュリティに関わる人や運用プロセスの側面についてもカバーしている。

本ガイドラインは、一度読んで終わりという性質のものではなく、組織における継続的なリスク管理活動の一部としての活用を期待するものである。具体的に

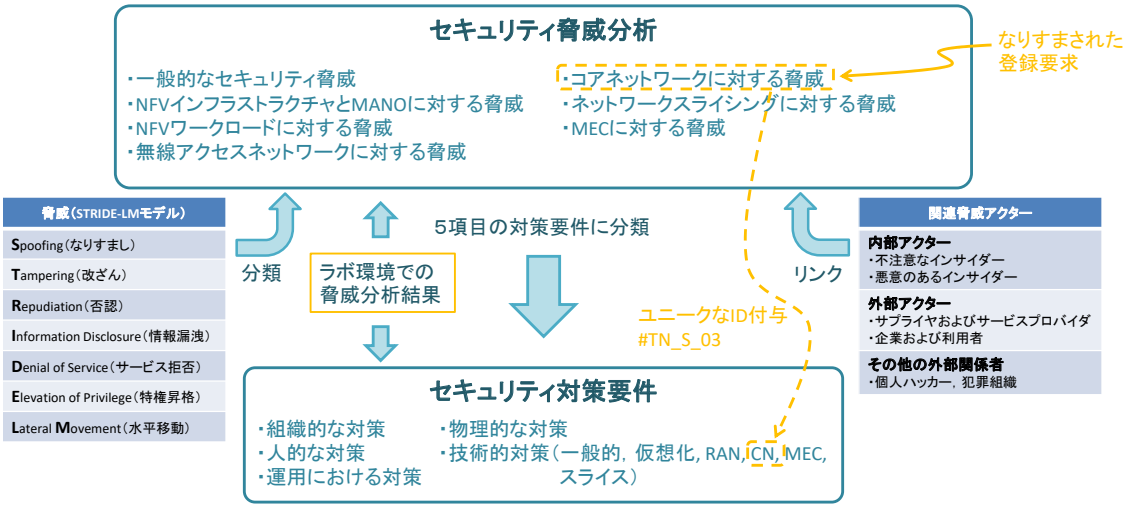

図 8　5G セキュリティガイドライン

は、本ガイドラインを活用し、まず個々の 5G システム展開における脅威分析とリスク評価を実施し、重要度に基づきセキュリティ対策の優先度付けと選択を行い、具体的な実施計画を策定したのちに、レビューを実施することでリスク評価を定期的に見直し、対策の適切性を繰り返し評価する必要がある。リスク環境は常に変化するものであり「セキュリティに終わりなし」の意気込みで本ガイドラインの活用を望むものである。

3　5G セキュリティ検証の今後の強化

2 にて詳述したとおり、サイバーセキュリティ研究所では、オープンソースソフトウェアを活用した基礎的な 5G ネットワークアーキテクチャに基づくセキュリティ検証を行い、4 社共同で 5G セキュリティガイドラインを発行した。ここでは、今後の更なる 5G セキュリティ検証の強化とガイドラインの更新に向けた課題について、標準化、ユースケース、諸外国の動きの 3 つの観点から整理する。

3.1　標準化

5G ネットワークのプロトコル策定を行っている標準化団体である 3GPP では、SA3（Service & System Aspects Working Group3）[13] においてセキュリティとプライバシーの要件定義やセキュリティアーキテクチャ、プロトコル策定等が行われている。現在の最新リリースは Release-18 であり、セキュリティに関しては、RAN とコアを含むすべてのシステムドメインで細かな強化が適用されている。これらは主に、地上波以外のネットワーク、非公衆ネットワーク、無人航空機システム、ミッションクリティカルなサービスなど、特定のユースケースや業種向けのサービスと機能を対象にしたものとなっている。また、最近検討作業が開始された Release-19 では、Release-18 においてすでに議論されている Zero Trust や、新たに追加された 256 ビット暗号化アルゴリズム、SBA における自動証明書管理のための ACME 等の 3GPP システムへの導入等に関し議論が行われている。

一方、通信事業者を中心とした業界団体である GSMA（GSM Association）[14] では、ワーキンググループである FASG（Fraud and Security Group）においてモバイル通信システム及びモバイルサービスに関するセキュリティの議論・検討が行われている。5G セキュリティに関しては 5GSTF（5G セキュリティタスクフォース）[15] を立ち上げ、セキュリティ上の課題整理を行うとともに、ネットワーク機器に対するサプライチェーンセキュリティの取組が進められている。5GSTF において発行されているドキュメントである FS.40 “5G Security Guide” によると、3GPP 標準化と同様、既存プロトコルの明確化や修正に関する様々なトピックに加え、暗号プロトコルの強化、PQC、ゼロトラスト、NPN（Non Public Network、非公衆網ネットワーク）、ミッションクリティカルサービスのセキュリティ等、重要な最新トピックに関する方向性はおおむね一致しているが、3GPP と GSMA の位置付けの違いに起因すると考えられる幾らかの差分も見られる。3GPP 標準仕様のスコープ外の内容として、例えばオープンソースの安全な活用やコンテナ化ネットワーク環境の安全な運用などが挙げられる。3GPP 標準仕様及び GSMA における、これらの多くの新しいトピックは **2** で詳述した 5G セキュリティガイドラインには含まれておらず、当時の我々の検証内容にも含まれていないテーマである。今後の検証の強化やガイドライン更新の必要性及び方向性を検討するにあたり、こうした標準化の動向は引き続き注視する必要がある。

なお、5G セキュリティに関する国際標準化は、ITU における電気通信標準化部門である ITU-T の「セキュリティ」に関わる活動を行っている研究グループ（Study Group）SG17 において検討されている。SG17 では、それぞれの課題に対応する WP（Working Party）が設置されており、5G に関連する研究課題は WP2 配下に存在する課題 2 において議論されている。SG17 の課題 2 では 5G に関連する勧告、または技術文書（TR）の策定を行っており、それらの一部についてはすでに勧告化（勧告が発行されること）、TR 化（TR が発行されること）が完了している。**2** に記載の 5G セキュリティガイドラインは X.1818（ex X.5 Gsec-ctrl）という勧告名で、タイトル名 “Security controls for operation and maintenance of IMT-2020/5G network systems” にて 2024 年の夏頃に勧告化完了の見込みである。5G セキュリティガイドラインの今後の方向性を検討するにあたり、ITU-T SG17 課題 2 において扱われている日本主導のこれまでの勧告及び技術文書に対する位置付けや相対関係を明確にした上で、体系的な勧告開発の推進についても考慮する必要があると考えられる。

3.2　ユースケース

5G を活用したユースケースはビジネスや産業の様々な分野における幅広い展開が想定 [16] されており、それぞれのユースケースごとに、モビリティ、データレート、スケール、レイテンシ、信頼性などの異なるネットワーク要件を持っている。5G ネットワークでは、このようにパフォーマンス属性が異なるサービスやユースケースをサポートするため、ネットワークスライス [17] と呼ばれる新しい概念が導入されている。ネットワークスライスは 5G ネットワーク内にお

表 1　ユースケースの実装に必要なネットワークタイプの組み合わせ例

	カテゴリ	eMBB	URLLC	mMTC	C-V2X
1	自動運転・運転支援		○		○
2	エンターテイメント	○	○		
3	公共インフラ	○	○	○	
4	医療	○	○		
5	産業利用	○	○	○	
6	FWA・バックホール	○			
7	ドローン・ロボット	○	○		
8	XR（AR/VR）	○	○		
9	農業	○	○	○	

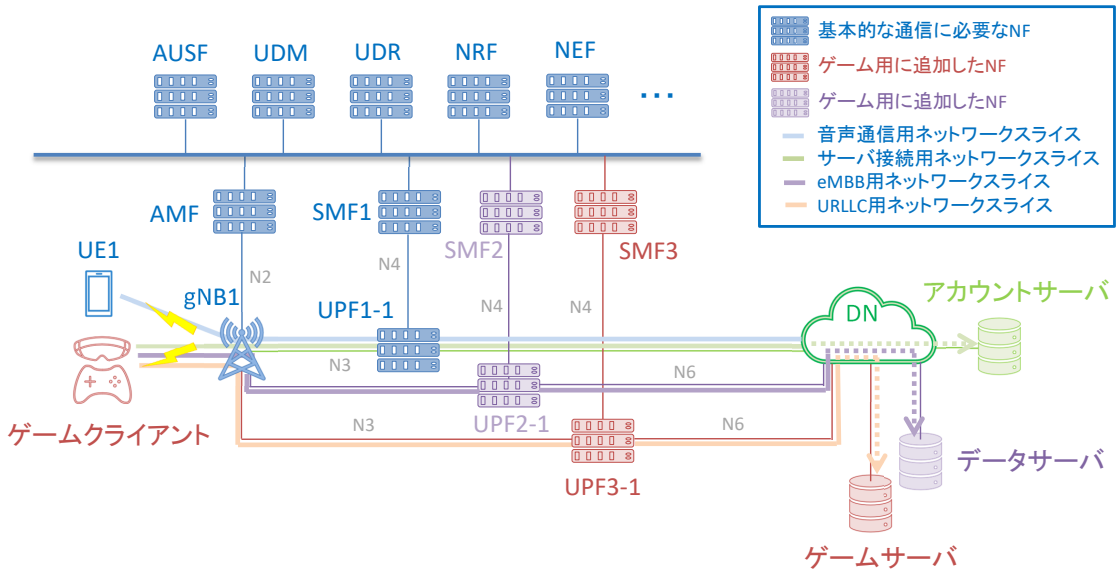

図 9　ゲームストリーミング用ネットワークアーキテクチャ例

ける論理的なユーザ情報のパスであり、ネットワークの物理インフラストラクチャを仮想的に分割し各サービスの性質や要件に適した仮想ネットワークを提供することで、異なるサービスやアプリケーションへの対応が可能となる。3GPP 標準仕様においてあらかじめ定義されているネットワークスライスのタイプとしては、冒頭で説明した eMBB、URLLC、mMTC に加え自動運転用の C-V2X 等があり、公共インフラや産業利用などの様々なケースにおいて、これらのネットワークタイプを単体、あるいは組み合わせての使用が想定されている。これらのネットワークスライスのタイプは 3GPP 標準仕様においてあらかじめ定義されているもののほかに、5G ネットワークを運用する通信事業者において任意の要件を満たすネットワークスライスを定義することもできる。

ユースケースのカテゴリと、ユースケース実装に必要なネットワークスライスの組み合わせの一例を表 1 にまとめた。

図 9 に、ネットワークタイプの一例として、エンターテイメントにおけるユースケースであるゲームストリーミングの実現に必要と考えられるネットワーク構成を示す。一般的にゲームストリーミングに要求されるエンターテイメント性として、臨場感や没入感の向上による再現度の高い大迫力なゲーム体験が挙げられる。これを実現するためのネットワーク要件として、eMBB による高精細な映像データと URLLC による低遅延かつ高信頼な操作性の双方が要求される。図 9 において、比較用の基本的な例である UE1 は、gNB1 を経由して通信事業者が独自に定義した音声通信用ネットワークスライスにより他基地局配下の別の UE と音声通信を行っている。これに対し、同じ無線基地局である gNB1 配下のゲームクライアントは、複数のネットワークスライスを並列に確立するマルチスライス構成によりゲームストリーミングサービスの提供を受けている。まず、通信事業者が独自に定義したサーバ接続用のネットワークスライスによりアカウントサーバ

表 2　諸外国における主な 5G セキュリティラボ

カテゴリ	名称	目的	対象	機能	備考
産学官協力	5G Security Test Bed	商用グレードの機器と施設を使用5Gセキュリティ推奨事項を検証	ベンダ、MNO、大学	5Gセキュリティ推奨事項(FCC's CSRICⅦ, Ⅷ)に基づくセキュリティ検証	CTIAが設立 設立メンバ6社
産学官協力	5G INFIRE University of Bristol UK	5Gアーキテクチャをフルソフトウェア化、5G垂直産業の実験、5Gユースケース調査	研究者、ベンダ	5G-NFVベース環境、Programmable Optical White-box、Elastic Bandwidth-Variable Transponders	5GinFIREは3年プロジェクト、活動期間2017年～2022年
公的	Australia "Secure-G" Connectivity Test Labs	透過的で安全な5G接続を支える対策・プロトコル・標準・ソフトウェアを試験、ソリューションを確認	5G利用企業	5G機器とプロトコル、システムの相互運用性とセキュリティをチェック 将来的に6Gもスコープ	Securing Australia's Future Connectivity 計画全体で$31.7M/4年
ベンダ	Nokia Advanced Security Testing and Research (ASTaR)	サイバーセキュリティのE2E 5G テストラボ	MNO	5Gネットワークのセキュリティ回復力を評価するツールと技術を開発・評価	ダラスにNokia全体のテスト＆ラボ機機能を終結
ベンダ	SecurityGen 5G Cyber-security Lab	テレコムセキュリチームの支援	MNO	5G商用展開に先立ち、セキュリティ脆弱性をテストして、対策を行う	
ベンダ	OneLayer 5G private network security labs	研究目的、一般公開	Private 5G導入企業	企業ネットワークに生じる脅威シナリオをシミュレートするデジタルツイン機能	
キャリア	Verizon Innovation Labs	顧客コラボレーション	5G利用企業	コラボレーション、技術検証、ネットワーク最適化	セキュリティはスコープの一部

表 3 5G セキュリティラボ比較

5G STB	NCCoE 5 G Cybersecurity Project
運営形態	
・CTIA がマネジメント、創設メンバにより運営	・NIST 主導の団体ではあるが主に協力パートナーによって推進
実証範囲、対象	
・3 GPP 標準仕様で規定された基本的なセキュリティ対策や FCC's CSRIC による推奨事項を主にカバー	・3GPP 標準仕様の複数のセキュリティ機能をカバーするような技術的カテゴリと、インフラやアプリケーション、仮想化を含む 3 GPP 標準仕様範囲外のセキュリティ課題にもフォーカス
テストケース選定方法	
・主に CTIA 会員の CSWG からのインプットでテストケース選定、ただし非会員も会費を支払うことでインプットを受け付ける	・オープンな選定手法を採用、発行文書にはコメントを提出できるパブリックレビュー期間が設けられている
技術的な構成	
・エリクソン商用機による NSA 及び SA	・主にノキア商用機による SA のみ
モチベーション、成果物	
・3 GPP 標準仕様で規定されている標準的なセキュリティ管理策の有効性をテストし効果を測定すること ・四半期ごとにテストレポートを発行	・5G 事業者が直面する可能性のある 3GPP 標準仕様以外のセキュリティ課題への対処に関する実践的ガイドライン ・業界全体と協力しながら特定した課題に向けて対処することも目標として掲げる

へ接続する。更に 3GPP 標準仕様において定義されている eMBB 用ネットワークスライスによりデータサーバからゲーム用の高精細映像をストリーミング、同じく 3GPP 標準仕様において定義されている URLLC 用ネットワークスライスをゲームサーバとの通信に用いることで超低遅延の操作性を実現している。

上記構成はあくまで一例であるが、例えば負荷分散や更なる低遅延化、高信頼化の観点から UPF をコアから独立させて異なる物理リソース上に分散配置させる構成や、N3 及び N9 インターフェースの冗長化、また、ゲームクライアントに地理的に近い 5G コアネットワーク内にエッジコンピューティングサーバを配置しゲームサーバとすることも可能である。いずれの場合においても、基本的な通信に必要な NF 構成に比べ、ゲームストリーミングには安定した通信を意図したマルチスライス構成を実現するために SMF (Session Management Function、ユーザ情報のとおり道である PDU セッションを管理する NF)や UPF などユーザ情

報を扱うNFをより多く必要とすることが予想される。さらに、5Gコアネットワークの外部に構成されているアカウントサーバなど、ゲームストリーミングに必要な様々なサーバ群も追加されている。このユースケースの場合、5Gネットワークにおける基本的なセキュリティ検証に加え、新たに追加となったNFやサーバの認証及び認可、鍵情報の管理、ユーザ情報や制御情報の機密性及び完全性保護、アクセス制御、ネットワーク設定、さらにはネットワークスライス間の分離や生成から廃棄までのライフサイクル管理等の設定が全て正しく実施されている必要がある。3GPP標準仕様においても、新しいリリースにおいて特定のユースケースや業種向けのサービスと機能を対象としたセキュリティ要件の検討が行われているのは**3.1**に記載のとおりであり、5Gセキュリティ検証における今後の強化の方向性として、このようなユースケース固有のセキュリティ検証も考慮に入れる必要がある。現在のところ、5Gネットワークにおける特徴的な機能を活用したユースケースは、アプリケーション実装や検証の難易度の高さから、まだ世の中にほとんど出回っていないと考えられるが、ユースケースが実装されサービスインされた後にリスクが表面化してからセキュリティ検証に取り組むのではなく、事前にユースケースを実装した固有の検証を行った上で脆弱性を炙り出し対策を打っておくことが望ましいと考えられる。

3.3　諸外国の動向

諸外国においては、5Gネットワークの商用機を用いたセキュリティ検証に特化した「セキュリティラボ」が存在する。表2に示すとおり、これらのセキュリティラボは地域ごとに特色を持っており、おおむね「産学官協力／公的」「ベンダ主導」「キャリア主導」の3つのカテゴリに分類することができる。

例えば米国の5G Security Test Bed [18]は、政府機関が発行した勧告を産学の連携組織が実機検証を行っており、具体的には、CTIAによるマネジメントの下、FCC's CSRIC Ⅶ及びⅧ [19]と呼ばれる5Gセキュリティの勧告に関する検証環境を提供している。一方、欧州では、ベンダ主導のセキュリティラボが中心となっており、また、豪州では、5G機器とプロトコル、システムの相互運用性とセキュリティをチェックするためのSecure-G Connecting Test Labsプロジェクトが内務省主管において進められている。

公開情報を基に、産学官連携による5Gセキュリティ検証を実施している米国5G Security Test BedとNCCoE 5G Cybersecurity Project [20]について表3のように比較を行った。

5G STBは3GPP標準仕様で規定されている基本的なセキュリティ対策やFCC's CSRICと呼ばれる推奨事項を主にカバーしているのに対し、NCCoE 5G Cybersecurity Projectでは、3GPP標準仕様で規定されているセキュリティ機能にとどまらず、5G事業者が直面する可能性のあるインフラやアプリケーション、仮想化を含む3GPP標準仕様範囲外の実装を意識したセキュリティ課題にもフォーカスしている。このように目指す方向性は異なっているが、注目すべき大きな特徴は、双方とも実際の商用5Gネットワーク設備によるセキュリティ検証が可能である点である。**2**で詳述したとおり、サイバーセキュリティ研究所では、システムの完成度や環境構築の容易さ、機能実装の早さ、検証内容や予算等を考慮しオープンソースによる5Gネットワークシステムによるプロトコルレベルの基本的なセキュリティ検証を実施した。しかしながら、システムの完成度はもとより、5Gネットワークとしてのパフォーマンス、幅広いユースケース実装の可能性等の観点から、商用機を用いることで、より実践に即した形での極めて精度の高いセキュリティ検証が可能であることは疑う余地はない。

もう一つの大きな特徴として、5Gセキュリティに関する共通の懸念、興味、効果を有するメンバを集め、技術的な問題や課題を解決し、それらを報告書やガイドラインという形でナレッジを蓄積する環境を実現しているという点である。**3.2**にも記載のとおり、5Gネットワークは、産業や社会基盤を支える様々なユースケースの実現により生活を一層豊かにすると期待されており、もはや欠くことのできない極めて重要なネットワークインフラの一つとなっている。しかしながらこうした期待は、より複雑なアプリケーションとの融合によるユースケースの実現を要求しており、もはや個社の通信事業者や通信機器ベンダでは解決できないような技術的な問題及び課題への対応が今後更に必要になると予想される。公開情報によると、日本国内においては、現時点では上記諸外国のようなテストベッドは存在せず、テストベッドに対する産業界からの要望も表面的には見られていない。しかしながら、今後予想されるこのような状況に対応するためには、まずは個社が抱える課題、データや検証結果の共有の有効性を考慮しながら、上記のようなテストベッドの必要性について、多様な関係者との意見交換を進める必要がある。サイバーセキュリティ研究所としても上記を考慮し、5Gセキュリティ検証に関する今後の強化の一環として関係者を巻き込んだ議論を始める枠組みについてまずは検討を始める予定である。

4 まとめ

本稿では、サイバーセキュリティ研究所において取り組んでいる 5G ネットワークに関するセキュリティ確保に向けた基本的な研究開発と、今後のガイドライン更新及びセキュリティ検証強化の方向性に関する検討について報告した。

5G ネットワークのセキュリティに関する基本的な研究開発では、総務省委託案件である 4 社共同プロジェクトに参加し、オープンソースを活用した 5G ネットワーク検証系においてユーザ端末の初期登録メッセージを悪用した DoS 攻撃に対する 5G ネットワークの脆弱性を明らかにしたとともに、対策についても検討を行い、それらの成果として 4 社共同で 5G セキュリティガイドライン第 1 版を発行した。

今後の 5G セキュリティガイドラインの更新及びセキュリティ検証の強化については、ITU-T における体系的な勧告開発も意識した上で、標準化において今後追加される新たなセキュリティトピックを継続的に注視しつつ、これまで実施した基本的な 5G ネットワークにおけるセキュリティ検証に加えユースケース固有のネットワークアーキテクチャに着目した実機検証に関しても検討する必要がある。検証精度の向上や様々なユースケース実装の可能性、ナレッジ共有による検証の効率化等を考慮すると、すでに海外での実例が確認されている、実際の商用機により構成される 5G セキュリティに特化したテストベッドも有効な選択肢の一つであるが、日本国内における必要性や事情を最大限に考慮しながら、通信事業者及び通信機器ベンダ各社が抱える課題や検証結果の共有の有効性などに関し、まずは多様な関係者との意見交換を開始する必要がある。

謝辞

本研究は総務省の「5G ネットワークにおけるセキュリティ確保に向けた調査・検討等の請負（令和 3 年度 0049-0022）」及び「5G ネットワークにおけるセキュリティ確保に向けた調査・検討等の請負（令和 5 年度 0049-0248）」によって実施した成果を含みます。

【参考文献】

1 GSMA, “5G Security Guide,”FS.40, Version 2.0, Oct.20, 2021.
2 総務省, “移動通信システムの進化とその影響,” 総務省情報通信白書令和 2 年版, 2020.
3 総務省, “5G セキュリティガイドライン第一版,” April 22, 2022, https://www.soumu.go.jp/main_content/000812253.pdf
4 ITU-T, “ITU-T work programme,” March 25, 2024, https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18494
5 https://openairinterface.org/
6 https://free5gc.org/
7 上松亮介, “IoT ソフトウェア無線の教科書 IoT システムに潜む脅威と対策,” 株式会社データハウス, March 27, 2020.
8 3GPP, “Procedures for the 5G System(5GS); Stage 2(Release16),” technical specification TS23.502, V16.9.0(2021-06)
9 https://www.docker.com
10 https://docs.docker.com/compose/
11 3GPP, “Security architecture and procedures for 5G system (Release 16),” technical specification TS33.501, V16.5.0(2020-12)
12 3GPP, “Non-Access-Stratum (NAS) protocol for 5G System(5GS); Stage3; (Release16), ” technical specification TS24.501, V16.8.0(2021-03)
13 https://www.3 gpp.org/3 gpp-groups/service-system-aspects-sa/sa-wg3
14 https://www.gsma.com/
15 https://www.gsma.com/publicpolicy/wp-content/uploads/2022/10/Securing-the-Mobile-ecosystem_2022.pdf
16 3GPP, “Service requirements for 5G System(5GS); Stage1; (Release16),” technical specification TS22.261, V16.16.0(2021-12)
17 3GPP, “Service architecture for the 5G System(5GS); Stage2; (Release16),” technical specification TS23.501, V16.9.0(2021-06)
18 https://5 gsecuritytestbed.com/
19 https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0
20 https://www.nccoe.nist.gov/5 g-cybersecurity

澤本 敏郎（さわもと としろう）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
研究技術員
5G セキュリティ
【受賞歴】
2022 年　コンピュータセキュリティシンポジウム奨励賞

鈴木 未央（すずき みお）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
主任研究技術員
博士（工学）
5G セキュリティ、ネットワークセキュリティ、ネットワークシミュレーション
【受賞歴】
2022 年　コンピュータセキュリティシンポジウム奨励賞

大迫 勇太郎（おおさこ ゆうたろう）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
リサーチアシスタント
5G セキュリティ
【受賞歴】
2024 年　NISC-CTF 総合第 2 位
2021 年　第 6 回 EMM 研究会（オンライン）優秀学生発表賞

中尾 康二（なかお こうじ）
サイバーセキュリティ研究所
主管研究員
サイバーセキュリティ全般
【受賞歴】
2022 年　TTC 表彰　総務大臣賞
2019 年　日本 ITU 協会賞
2015 年　大臣表彰賞　総務省