「TTCセミナー～5Gにおけるセキュリティに関する最新動向」開催報告

一般社団法人情報通信技術委員会　担当部長　竹内（たけうち）　正憲（まさのり）

1. はじめに

4月に米国と韓国の通信事業者から5Gサービスを開始したとのアナウンスが行われ、5Gの時代への移行が始まった。5Gでは、eMBB（enhanced Mobile BroadBand：高速大容量）、URLLC（Ultra-Reliable and Low Latency Communications：超高信頼低遅延）、mMTC（massive Machine Type Communications：多数端末接続）を実現することを目的とし、ネットワーク側でも新しい技術が取り入れられようとしている。

2019年6月17日にTTCのセキュリティ専門委員会と5GMF企画委員会セキュリティ検討アドホックとの共催で、5G時代に向けたセキュリティの取組みについて焦点を当てたセミナーを開催した。これまでのモバイルネットワークのセキュリティ対策では、モバイル通信システムやプロトコルに対する攻撃の防御、通信事業者が想定していない不正な利用への対応が主なものであった。5G時代になってもこれらの対応は必要だが、さらに、ネットワーク側の新しい機能や、これに伴う新しいユースケースに対してもセキュリティ対応を行う必要があると言われている。

本セミナーでは、5Gに向けたネットワークの移り変わりの観点から、NTTドコモの青柳健一郎氏による「5Gコア概要―5Gコアの技術的特徴及び3GPPにおける標準化状況概説―」、KDDI総合研究所の窪田歩氏から「5Gセキュリティに関する標準化動向」について、5Gネットワークの利用方法の観点から、5GMFセキュリティ検討アドホックサブリーダーであるNTTドコモの石井一彦氏から「5GMFセキュリティアドホックの活動」、TTCセキュリティ専門委員会委員長及びITU-T SG17副議長であるKDDI総合研究所の三宅優氏から「ITU-T SG17での5Gセキュリティの議論」についての講演があった。以下にセミナー講演の概要を紹介する。

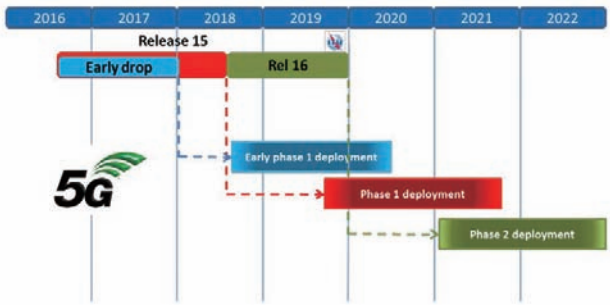
2. セミナー講演の概要

2.1 5Gコア部分のセキュリティについて

5Gセキュリティとプライバシー関連については、3GPPのSA WG3が担当しており、5Gセキュリティの標準化活動は、リリース14で17のセキュリティ領域を定めて課題と対策を整理し（～2017年8月）、リリース15のフェーズ1（～2018年3月）、リリース16のフェーズ2（～2019年末）のスケジュールでセキュリティの強化が進められている（図1）。以下に5Gコアの特徴技術と標準化動向を紹介する。

2.1.1 NSA（Non Standalone）のセキュリティ

NSAは、2019年から始める5Gのサービスで、LTEのコアを使って無線部分は5G無線を使用するLTE Dual Connectivity同等のサービスである。Dual Connectivityとは、LTEの高速大容量化のために、複数基地局間でのLTEキャリアの同時通信を行う仕様であり、LTE基地局と5Gの基地局を使ってより高速大容量の通信を行う。NSAでは、LTE基地局がマスタとなり、5G基地局がセカンダリとなる。セキュリティの手順はLTEのDual Connectivityをほぼ流用しており、5Gで追加されるU-Plane改ざん検知機能は使われない。そのため、NSAでのセキュリティはLTEのセキュリティとほぼ同じとなる。



■図1. 5Gのタイムライン
（出典：http://www.3gpp.org/images/5g_timeline_imt2020.jpg）

2.1.2 SAのセキュリティ

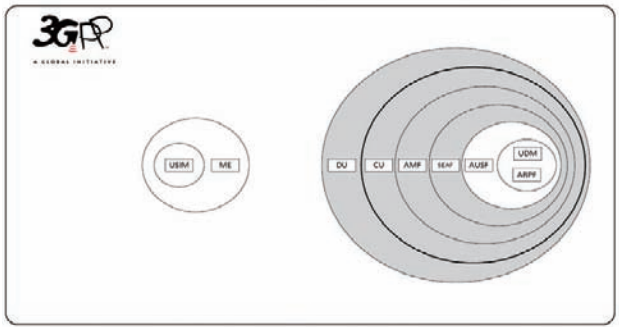
リリース15のフェーズ1セキュリティでのメインのユースケースはeMBBであり、LTEからはセキュリティが非常に強化されている。

リリース16のフェーズ2セキュリティでは、mMTC、URLLCをカバーするセキュリティ検討が行われており、mMTC関連ではV2Xのセキュリティ検討がワークアイテムに挙がっており、URLLC関連では、冗長化による高信頼化のための複数セッションを利用する場合のセキュリティポ

リシーや、ハンドオーバーや認証処理の停遅延化に関する検討などが行われている。

(1) トラストモデル

5Gのトラストモデル（図2）は、コアから遠ざかるに従いトラストが低下するという考え方により、RAN（Radio Access Network）をDU（Distributed Units）とCU（Central Units）に分離し、安全性の低い場所に配置されるDUには暗号鍵を持たせず、コアに近いCUに暗号鍵を持たせるというものである。



■図2. 5Gトラストモデル
（出典: https://www.3gpp.org/news-events/1975-sec_5g）

ホームネットワークとVisited Network（ローミング先のネットワーク）の信頼関係においても、ホームネットワークから見てVisited Networkはコアから遠く、そこの信頼を必ずしも前提としないというホームコントロールの強化を行い、ローミング先で加入者が認証したとしても、ホーム側で確認してから接続を受け付けるようにしている。

(2) SBA（Service Based Architecture）におけるセキュリティ

従来のLTEのノードの構成を見直してC-planeとU-planeを分離し、C-plane装置をNF（Network Function）単位で扱う技術であるSBAを導入した。SBAでは統一的なインタフェースであるSBI（Service Based Interface）を介してネットワーク機能間を接続する。SBIのプロトコルとしては、インターネットの世界で広く使われるHTTP/2やJSONを採用し、Web技術者が使いやすいネットワークになっている。SBAで特徴的なのがNRF（Network Repository Function）で、NFの登録を行ったり、目的とするサービスをどのNFが提供しているのかを検知したりする機能を有する。リリース16では、NRFの代わりにオープンソースのソフトウェアを使うこともできるようになる。

ローミングにおける事業者間の接続においては、ネットワーク事業者間のセキュリティ向上のためにSEPP（Security Protection Proxy）が導入された。SEPPはSBAのNF間の信号を一旦終端しており、事業者間の相互接続時にC-planeを中継する。

5Gでは利用方法が多様化するため、低遅延を優先するとヘビーなセキュリティには対応できないといったことが考えられる。そのため、用途ごとに基地局と5Gコアとのネゴシエーションによりu-planeアルゴリズムを選択する仕組み（オンデマンドセキュリティ）が追加された。例えば、暗号化と改ざん検知を行うのか、暗号化のみ行うのか等の選択ができる。

SBAのセキュリティ要件として、①NFサービスの検知機能は、完全性、機密性及び繰り返し攻撃対策をサポートする必要がある。②NRFは検知機能及び登録要求が認可されていることを保証する必要がある。③検知機能と登録は信頼ドメインの構成を隠すことができなければならない。④加入者とNFの相互認証をサポートする必要がある。⑤NFは全ての受信メッセージを検証する必要がある。⑥NFとNRFは相互認証しなければならない等の、攻撃や認証に対する強化を行う必要がある。

(3) ネットワークスライシングにおけるセキュリティ

ネットワークスライスとは、従来の装置単位から機能に分割していき、用途に応じてリソースを割り振るものである。ネットワークスライスを特定する識別子NSSAI（Network Slice Selection Assistance Information）を用いて、End-to-Endで端末からネットワークまでのリソースを確保する。

ネットワークスライスのスライス管理のセキュリティ要件として、①相互認証のための証明書とTLS、②完全性保護、繰り返し攻撃対策、秘匿のためのTLSなど、セキュリティ機構や認証、プライバシーに対する強化を行う必要がある。

(4) プライバシーの強化

3G以降、ユーザを一意に特定するIMSI（加入者識別子）が使用されていたが、IMSI catcherを使用した攻撃による加入者IDの追跡等のリスクがあった。加入者IDの保護を強化するため、5Gでは、IMSIに相当するSUPI（Subscription Permanent Identifier）のMSIN（Mobile Subscriber Identification Number）部分をホームネットワークの公開鍵で暗号化したSUCI（Subscription Concealed Identifier）にて送信することにより加入者IDを保護している。

(5) U-Planeのセキュリティ強化

従来の通信ベアラという単位の概念がNon-3GPPでは扱いにくい単位なので、QoSを扱うためにトンネルという単位（QoS flow）で行うことにした。また自局の近傍にデータ

を乗せることにより信頼性の高い通信を行うMEC（Multi-access Edge Computing）では、複数のハンドオーバーによりセッションを途切れさせないようにつなぐ方法が規定された。

また、認証についてホームネットワークのコントロールを強化するのとU-planeの完全性保証などのセキュリティ機能のために、LTEの鍵階層にU-Plane改ざん検知機能（UPint）が追加された。従来からU-Planeも暗号化されていたが暗号化されたまま改ざんされるという悪用もあるため、U-Planeを守るために追加された機能である。

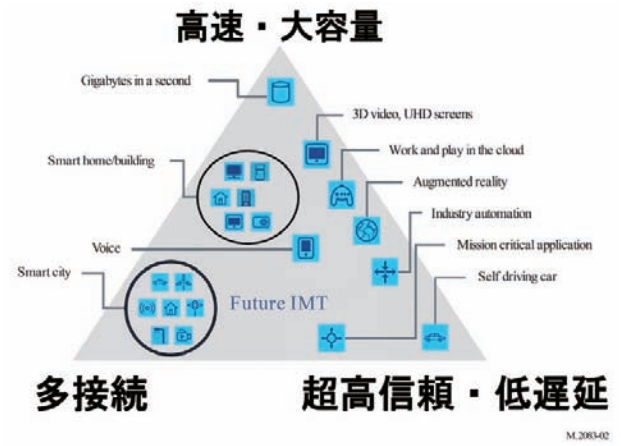
U-planeおけるセキュリティ要件として、U-Planeの完全性や機密性の保護などU-planeのセキュリティ強化を行う必要がある。

（6）SCAS（Security Assurance Specification）

3GPPとGSMAの連携によるネットワーク機器のセキュリティ上の安全性をチェックするため、3GPPでセキュリティ保証仕様（SCAS）を決め、GSMAが認証（Network Equipment Security Assurance Scheme：NESAS）を担当している。

2.2　5Gコア部分以外のセキュリティについて

5Gネットワークの利用方法として各種のユースケースが想定される(**図3**)。以下に利用方法の観点からのセキュリティの話題について紹介する。



■図3.　Usage scenarios of IMT for 2020 and beyond
（出典：IMT Vision-"Framework and overall objectives of the future development of IMT for 2020 and beyond", ITU-R, 勧告M. 2083-0, Sept, 2015）

2.2.1　5GMFセキュリティアドホックの活動

5GMFセキュリティ検討アドホックは、第5世代モバイル推進フォーラム（5GMF）にて2018年より活動を開始している。アドホックでは、以下の3つのユースケースについてトラストサービスモデルを構築し、5Gネットワークを使うことで解決できる検討項目の抽出と整理を行った。2019年に設立した「セキュリティ調査研究委員会」の活動にて、これらの課題の具体策を検討していく。

（1）IoTセキュリティ

GSMAの「IoTセキュリティガイドライン」などの標準文書からIoTセキュリティ課題を抽出し、これと5Gセキュリティ新機能から、12項目の課題（可用性：4件、ID：4件、プライバシー：4件）を抽出・整理した。IoTセキュリティ課題の対応策として、5Gセキュリティ新機能のうち、セカンダリー認証、プライバシー保護、ネットワークスライスの各機能を活用できる可能性が高いと考えている。

（2）Connected Vehicleセキュリティ

Connected Vehicleは、様々なプレイヤー間が関与するサービスであり、各サービスにおける5Gのトラストモデルとして以下のセキュリティ課題を検討している。

① 事業者の提供するモバイルエッジ上で複数のサービス提供者が動作するマルチテナント環境における、サービスの安全性検証の問題、プラットフォームの安全性の問題、各サービスの独立性の問題。

② C-V2Xで想定される、なりすまし、盗聴、データ改ざん等のセキュリティ対策として電子証明書を活用する場合、電子証明書による追跡性（プライバシー）の問題及び膨大な電子証明書の作成に伴う失効リストの効率的な検証方法の問題。

③ Connected Vehicleの各種サービスに応じた複数ネットワークスライシングの利用とその適切なセキュリティ管理において、スライス間での通信の規制・制御の問題、スライスへのアクセス認可・認証の問題、他スライスへの攻撃・悪影響の阻止の問題。

（3）Fintechセキュリティ

金融取引などのサービスでは、より高いセキュリティが求められる一方で、ユーザの利便性を向上させていくことが重要となる。そこで、モバイルネットワークを活用したパーソナライズペイメントをターゲットに、下記のセキュリティ課題を検討している。

① モバイル端末とクラウドとのリアルタイム連携による連続的な個人・機器認証。

② 異業種間サービス・データ（API）連携を実現するサービス事業者間認証。

2.2.2　ITU-T SG17での5Gセキュリティの議論

5Gセキュリティに関しては、5Gの要件から想起されるセキュリティ脅威が出てくると考えられる。eMBB（高速・大容量）及びmMTC（多接続）については、既に顕在化しているセキュリティ脅威の深刻化として、スマホ/IoTマルウェアの増加、ボットネットによる攻撃威力の増大、シグナリングDoSが考えられ、セキュリティとの両立が難しい要件であるURLLC（超高信頼低遅延）では、暗号処理オーバーヘッドと低遅延とのバランス、エッジコンピューティングとセキュリティとのバランスが考えられる。

5Gセキュリティは3GPP等の団体で議論されているが、5Gコア以外にも検討することがあるので、SG17では検討課題を整理して勧告化の作業を進めている。他の標準化団体の活動状況を確認しながら実施項目を調整し、リエゾンによる情報交換を行いながら作成作業を進めている。

ITU-T SG17ではQ2（アーキテクチャ）、Q6（サービスセキュリティ）、Q13（セキュリティ）の各グループにおいて5Gセキュリティで勧告すべきものを提案し、議論を行っており、その一部を紹介する。

（1）Security Service Chain Architecture and its Application（Q2）

複数のネットワーク機器を統合的に扱うアーキテクチャSSC（Security Service Chain）の提案。SSCにより、統合的な監視による攻撃発信源のトレース及び攻撃を効果的に遮断する部位の特定ができる。

（2）Security Requirements of Network Virtualization（Q2）

ITU-T勧告Y.3011、Y.3012で規定されているネットワーク仮想化について、物理リソース層、仮想リソース層、LINP（logically isolated network partitions）層のセキュリティ上の脅威を整理し、セキュリティ要件を議論。

（3）Guideline on Software-defined Security in Software-defined Networking / Network Function Virtualization Network（Q2）

SDN/NFV用に特別なセキュリティ機構（Software-defined Security）を提案。セキュリティ上の課題として、SDNコントローラでのDoS、盗聴、ルールの不整合等を想定。仮想化により物理的なセキュリティ境界が不明確になり、セキュリティの監視がこれまで以上に困難になると考えられるために提案された。

（4）Security framework based on trust relationship for 5G ecosystem（Q6）

5Gになると多くのステークホルダーやエンティティが出てきてトラスト関係を結ぶことになるので、シナリオをベースにサービスを実現する際のエンティティ間のトラスト関係を明確にし、その際のセキュリティ上の脅威と要件を整理してトラスト関係に基づくセキュリティフレームワークを構築した。シナリオとして、オペレータ領域での仮想ネットワークの運用、相互接続とローミング、遠隔操作によるレンタカーサービス、ネットワーク機能の開放、5Gエコシステムのサプライチェーン管理がある。

（5）Security guideline for 5G communication system based on ITU-T X.805（Q6）

X.805（Security architecture for systems providing end-to-end communications）をベースとした、End-to-End セキュリティに焦点を当てた5G通信におけるセキュリティガイドラインの提案。

（6）Security framework for 5G edge computing services（Q6）

5G環境におけるエッジコンピューティングサービスの脅威とセキュリティ要件を明確にし、これを満たすフレームワークを提案。盗聴、サービス利用状況の解析、DDoS、ネットワーク構成の解析等の攻撃に対する要件整理と対策案を検討。

（7）Security guidelines for vehicular edge computing（Q13）

車両向けエッジコンピューティングに特化したセキュリティ上の脅威と要件規定を提案。情報漏えい、センサー等から得られる情報（GPS、信号、CAN-BUS等）の改ざん、可用性に対する攻撃、不正なゲートウェイ/データセンサー、マルウェア、APT攻撃等の脅威を列挙し、その影響と脅威に対応するための要件を整理。追い越し補助や交通弱者発見のユースケースに特化して議論を進めている。

3. おわりに

本テーマの関心は高く、セミナーには約100名の方の参加があり、各講演においては活発な質疑応答があった。

本セミナーの4名の講演者の方々には、5Gに関する様々な場面でのセキュリティについて分かりやすく紹介していただいた。ここに深謝の意を表する。