令和3年度 総務省「5Gネットワークのセキュリティ確保に向けた調査・検討等の請負」事業報告

資料37－2－2

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 及び 5Gセキュリティガイドライン（第1版）について

KDDI株式会社

2022年 4月 22日

Tomorrow, Together

KDDI

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 事業 概要

■ 考え方：

- 様々な社会産業やミッションクリティカルな領域での5G活用の期待の高まりとともにモバイル通信サービスの安全性や信頼性への要求が一層高まっている
- 5Gを含むモバイル通信サービスのセキュリティは、個々の機器のセキュリティだけではなく、ネットワーク全体を踏まえた各オペレータの運用に依存する部分も大きい
- 5G SAやインターフェースのオープン化も見据えると、ネットワークはソフトウェア化が進むとともに、機器ベンダーも多様化しており、OSSプロジェクトでの進展も見られる
- このため、足下で入手可能な個々の機器の検証ではなく、仮想化基盤や管理系など含む5G全体を考えた検証を実施し、オペレータが留意すべきセキュリティ課題を洗い出してその対策とともに普及を図るとともに、検証能力を含む5Gのセキュリティに関する国内への技術的蓄積をめざす

■ 実施内容（令和元年度～3年度）：

- 5Gセキュリティに関する標準化機関や海外政府当局等の検討動向調査
- 5Gネットワークのセキュリティに係る技術的検証の実施
  - 検証環境として、NICTに5Gネットワークをエミュレート可能な仮想化基盤を構築
  - 検証環境上で、5Gネットワークに対する脅威や脆弱性等の技術的検証を実施
  - 検証結果を踏まえて対策要件等を整理
- 取組により得られた知見に基づき、事業成果文書として「5Gセキュリティガイドライン」を策定・公表

（参考） 5Gで想定される環境変化に伴うセキュリティ懸念事項・課題（想定例）

想定される環境変化	懸念事項・課題
ネットワーク機能の多様化	新しい機能の導入の際には仕様上、実装上のセキュリティ脆弱性が発見されやすい。 例：MEC（Multi-access Edge Computing）、ネットワークスライシング
通信インフラの仮想化	仮想化インフラ自体のセキュリティ対策の強化が必要。通信システムの複雑化による脆弱性管理の複雑化。　例：5Gコアや5G基地局への仮想化プラットフォーム適用
インタフェースのオープン化	インタフェース部分の処理の厳格化、セキュリティ対策が必要。 例：フロントホール等RAN設備のインタフェースオープン化
オープンソースの活用	攻撃者がシステムの脆弱性を探しやすくなる。
通信制御機能の外部への公開	信頼関係の確立が必要。監視機能の強化が必要。 例：5Gコア機能のローカル5G事業者等への提供
汎用プロトコルの利用	攻撃の敷居が下がる。　例：HTTPベースの通信
ネットワークの複雑化	セキュリティ対策が不十分なソフトウェア、ハードウェアが組み込まれる可能性が増える。 セキュリティ対策のための機器の導入が難しくなる。攻撃されたことが発見しにくくなる。

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 事業 全体像

5Gセキュリティに関する標準化機関や海外の政府当局等の検討動向の調査と、検証環境の構築、同環境を用いたセキュリティ脅威や脆弱性等の検証、対策要件の整理等を実施。これらの取組によって得られた知見に基づき5Gセキュリティガイドラインを策定。

1．外部動向等の調査等

- 3GPP、ITU-T、GSMA等におけるセキュリティ検討動向やガイドライン策定状況を調査。
- 海外のBeyond5G/6G検討プロジェクト (FG NET-2030、6Genesis Flagship、HEXA-X等) におけるセキュリティ検討動向を調査。
- 欧米政府当局における5Gセキュリティに関する政策動向、ガイドライン化の状況等を調査。
- 海外キャリアの5Gセキュリティ関連動向を調査。

2．セキュリティ課題の検討及び検証環境の構築

1. 5G SAを想定したセキュリティ分析
   - NFV、MEC、スライス等の新技術活用とセキュリティ課題整理
   - 5G活用（IoT、エッジ、ローカル5G等）に関する課題整理
2. 5Gセキュリティに関する検証環境の構築
   - NFV、MEC、スライスを含む包括的な5G検証環境
   - 複数実装（Open5GCore, OAI, Free 5GC）の5Gコア
   - 実運用を想定した管理系を含むVM、コンテナ混在NFV基盤
   - 無線エリアネットワーク検証環境
3. 検証環境上でのセキュリティ課題の洗い出しの実施
   - セキュリティ仕様への適合試験、ファジングテスト、DoS攻撃、ペネトレーションテスト、不正機能組み込み

個々の5G機器の検証ではなく、仮想化基盤や管理系など含む5G全体を考えた検証を実施しオペレータが留意すべきセキュリティ課題を洗い出した → 5Gセキュリティ検証の国内への技術蓄積も実現

検証結果を反映

標準化の議論内容、他のガイドライン等との整合性を確認

3．ガイドラインの策定

- 5Gコア、RANだけでなく仮想化、MEC、スライスなど5Gシステム全体を対象とした包括的なガイドラインとして策定。
- STRIDE-LMモデルを使用して脅威を洗い出し、検証の成果も踏まえて体系的に整理。
- 対策要件は、以下の分類で管理策(対策の基準)とガイダンス(対策のTIPS集)を整理。
  - 組織的・人的管理策
  - 運用管理策
  - 物理的管理策
  - 技術的対策

1．外部動向等の調査等

標準化動向調査

- 3GPP
  SA3での議論を中心にセキュリティ保証仕様、産業向けIoT、非公衆ネットワーク、エッジコンピューティング等の検討状況について調査を実施。
- GSMA
  5Gセキュリティに関連するプロジェクトやワーキンググループ（NESAS、FASG、CVD、Future Network Program等）の活動状況や公表されている白書類の調査を実施
- ITU-T
  SG17における5Gセキュリティ関連の勧告文書の作成状況や5Gセキュリティ標準化ロードマップに関する調査を実施。
- NGMN Alliance
  5Gセキュリティ強化に向けたワーキンググループ活動（Operating Disaggregated Networks、Sustainability/Green Future Networks、6G）や白書類の調査を実施。

各国動向調査

- 米国
  NIST CCoEの5G Cybersecurity Project、国土安全保障省、商務省 国家電気通信情報庁等の活動状況について調査を実施。
- EU/英国政府
  ENISAの発行した各種文書や2021年3月に発表された「デジタルコンパス2030」における5G,6G関連の目標、英国における5G普及に向けた取り組み（2G・3G廃止やOpen RANへの投資計画）やハイリスクベンダへの対応等について調査を実施。
- 中国
  中国における5G関連の主な研究開発動向や、中国政府当局によるデジタル・イノベーション強化のための取り組み等について調査を実施。
- 海外通信キャリア
  AT&T、Verizon Wireless、Vodafone、DISH Network Corporationが公表している白書や技術情報の調査を実施。

B5G/6G等の次世代通信関連動向調査

- 次世代通信に関連するプロジェクトの動向調査としてITU-T FG NET-2030、ComSenTer、5G Americas、6Genesis Flagship、Hexa-Xに関する調査を実施。

有識者会議の開催と外部関連プロジェクトとの意見交換

- 令和2年度～3年度に計4回の有識者会議を開催
- NIST CCoE 5G Cybersecurity Project、仏EURECOM、5GMF セキュリティ調査研究委員会と意見交換を実施。

- **調査結果は脅威分析の参考などに活用するとともに、技術文書は本事業で策定したガイドラインの中でリファレンスとして活用**
- **ITU-T SG17の5Gセキュリティ標準化ロードマップに関する議論の中でセキュリティ管理策をまとめたガイドライン文書の策定の必要性が示されており、本事業の成果文書をベースとした勧告化について準備中**

2-1. セキュリティ課題の検討及び検証環境の構築：5G SAを想定したセキュリティ分析

■ 5Gにおける新技術活用とセキュリティ課題

- **仮想化技術の活用の進展（NFV、ネットワーク・スライス）**
  - 汎用ハードウェアやOSS利用にまつわる脅威
  - 増加する攻撃対象（オーケストレータ、管理I/F、ハイパーバイザ等）
  - 分離性の保証（仮想ネットワーク機能間、ネットワーク・スライス間）

- **MEC（Multi-access Edge Computing）**
  - MEC基盤／アプリと5Gシステムの安全な連携（トラフィック誘導、課金制御等）
  - 第3者MECアプリも想定した対策（分離性保証、MECアプリからの攻撃対策等）

検証環境構築に反映

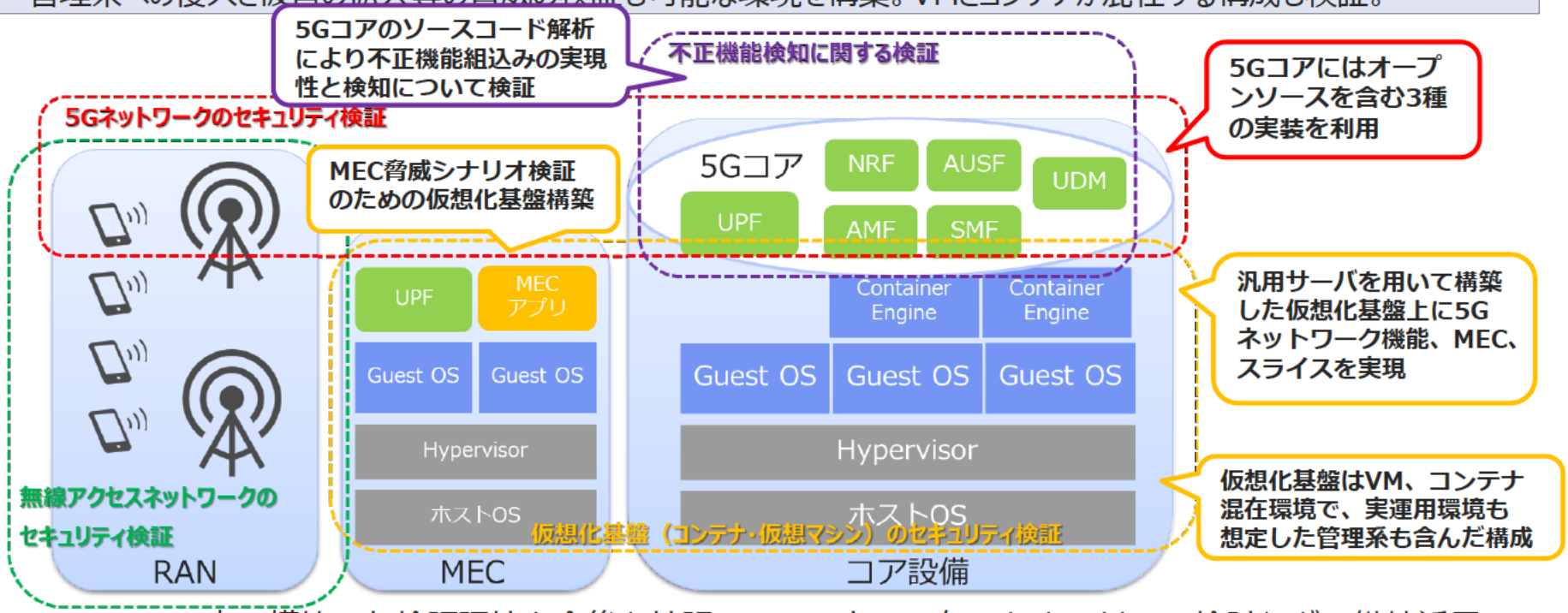
■ 5G活用に関するセキュリティ課題の整理

- **各産業分野におけるセキュリティ目的に関して5G新機能により実現可能となる対策案を整理**
  - 組込みシステム／IoT、自動車、プラント、医療、金融・決済、制御システム

→ ユースケース毎の課題の深堀、検証は今後の取り組み

2-2. 5Gセキュリティ検証環境の構築

- 5G SAを想定したセキュリティ分析結果を踏まえ、仮想化（NFV、スライス）、MECを含む形で5Gセキュリティに関する検証環境の構築、拡張を実施。5Gコアには複数種類の実装を利用し、実装による挙動の差異も把握可能に。
- 実運用環境を想定し、MANO（Management and Orchestration）やログ収集等の付帯系設備も含む構成とし、管理系への侵入と被害の拡大等の脅威の検証も可能な環境を構築。VMとコンテナが混在する構成も検証。



NICT内に構築した検証環境を今後も拡張しユースケース毎のセキュリティ検討などに継続活用

2-3. 検証によるセキュリティ課題の洗い出しの実施

■ **検討した脅威シナリオと検証方法（2-1. の分析結果も活用）**

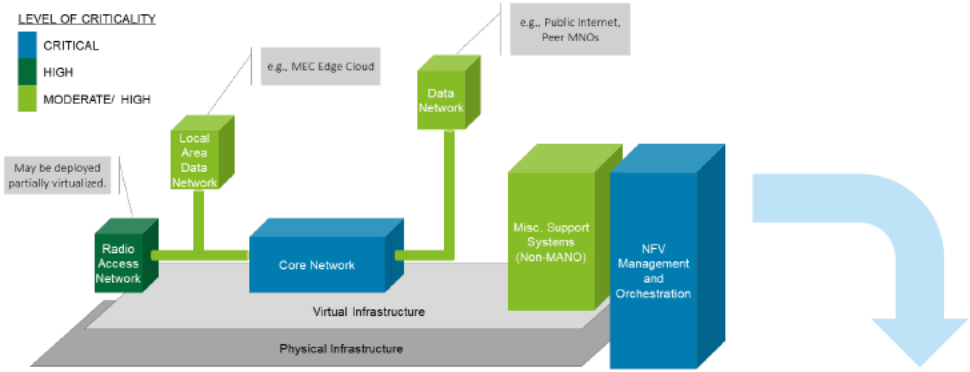
- **5Gセキュリティ仕様からの逸脱**
  - 3GPPのセキュリティ保証仕様がカバーしていないテスト項目27件を洗い出しテストシナリオを作成
- **5Gネットワーク機能の重要インタフェースへの攻撃**
  - 3GPP仕様を精査し脅威分析を行った結果に基づいて抽出した主要インタフェースへのファジングテストを実施、ツールも開発
- **端末登録要求の大量送信等によるDoS攻撃**
  - 端末エミュレータによる不正登録要求の送信
- **仮想化や管理系の脆弱性や分離設定の不備を突いた侵入・攻撃の拡大**
  - ペネトレーションテストの実施
- **サプライチェーンにおける不正機能組込み**
  - 5Gコアのネットワーク機能へのバックドアの組み込みの検証

■ **発見された問題（一部）**

- **セキュリティ仕様からの逸脱**
  - コア内ネットワーク機能間の認証・認可不備、セキュリティパラメータの保護の不備等
- **APIの実装上の問題**
  - コア内部のI/Fでネットワーク機能の再起動を引き起こす実装エラー
- **一部実装におけるDoS攻撃への耐性欠如**
- **VM、コンテナ混在環境での攻撃面の増加や分離の不備**
  - 管理系への侵入、他のワークロードのリソース圧迫、コンテナにおけるパフォーマンス最適化によるセキュリティ機能のバイパス

✓**ガイドラインへの反映**
✓**これらを検証する能力を含め5Gセキュリティに関する国内への技術的知見を蓄積**

3. ガイドラインの策定: 脅威シナリオ検討と検証に基づく5Gシステムドメインの重要度の整理



システム ドメイン	ネットワーク機能・エンティティの例	情報漏えいによる影響度	情報改ざんによる影響度	利用不可時の影響度	総合的な重要度の考え方
5Gコア	AMF、SMF、UPF、AUSF、UDM、NRF、SCP、SEPP 等	Critical	Critical	Critical	**Critical**
NFV運用管理・支援システム	NFV Orchestrator & Security Manager、VNF Managers 等	High	Critical	Critical	**Critical**
5G RAN	gNB、non-3GPP Access	High	High	High	**High**
(Non-MANO) その他支援システム	課金システム 等	High	High	Moderate	**Moderate /High**
通信路及び通信機器類	ルータ、スイッチ 等	Moderate	Moderate	High	**Moderate /High**
相互接続先	外部データ網、公衆インターネット、エッジクラウド等	Moderate	Moderate	High	**Moderate /High**

3. ガイドラインの策定:ガイドライン策定に向けた包括的な脅威分析の実施

- ガイドラインの策定にあたっては、5Gコア、RANだけではなく仮想化基盤や仮想化ワークロード、ネットワークスライス、MECを対象にSTRIDE-LMモデルを用いて体系的に脅威の洗い出しを行い、検証の結果を踏まえて整理した。
- また、5Gシステムの構築・運用形態（MNO、MVNO、ローカル5G等）によって想定される攻撃者も異なるため、脅威アクター(脅威の主体) を整理し、各脅威との関連付けを行っている。これによりガイドラインの利用者が、各々の5構築形態や運用形態に応じて脅威の深刻度や対策の優先度を検討できるようにしている。

脅威	脅威に対応したセキュリティ目的
なりすまし	認証
改ざん	完全性の確保
否認	否認防止
情報漏えい	機密性の確保
サービスの拒否	可用性の確保
特権の昇格	適切な認可
ラテラルムーブメント	ネットワークの分離

STRIDE-LMモデル

脅威分析の対象

・5Gシステム全般
・NFVインフラストラクチャとMANO
・NFVワークロード
・RAN
・コアネットワーク
・ネットワークスライス
・MEC

脅威アクターの分類

- 内部アクター:
  - 不注意な者（Negligent Insiders）（Ⓝ）
  - 内部犯行者（Malicious Insiders）（Ⓜ）
- 外部アクター：
  - サプライヤー・通信事業者 (Ⓢ)
  - 取引先・契約者 (Ⓒ)
  - その他の外部の者 (Ⓞ)（ハッカー、組織的犯罪者等を含む）

3. ガイドラインの策定: 5Gセキュリティガイドラインの目的と使い方

想定読者

主に5Gシステムのオペレータ。一部サプライヤ向けの推奨事項も含まれる。

目的

5Gシステムのセキュリティを実際に確保するための包括的なガイダンスを提供すること。

- 技術面だけでなく、5Gサービスのセキュリティに影響を与える人やプロセスの側面も考慮。
- 推奨されるセキュリティ対策は、関連する確立されたスタンダート及びベストプラクティスを参照し、ハイレベルに記述。

想定する使い方

5Gシステムをセキュアに展開するための出発点。
（セキュリティ対策手順を詳細に規定するものではない）

5Gシステムに対するセキュリティ上の脅威と関連するセキュリティ対策を構造化して提示。

→ 利用者の側で想定する展開シナリオや関連する脅威に応じて対策の優先度付けをし、
継続的なリスク管理活動に活用。

3. ガイドラインの策定: 5Gセキュリティガイドラインの構成

1章　適用領域
- ガイドラインの目的・適用範囲、想定読者を明確化

2章　序論
1）用語の解説
  - 脅威の分析（STRIDE-LM）
  - セキュリティ対策（Control）の分類

2）ガイドラインの構成
3）ガイドラインの使い方

3章　主要5G技術の概説
- 5Gセキュリティのキーとなる対策ポイントを解説。
- 5Gシステムの対策ポイントについて優先度付けの考え方を解説

1）5Gシステム
2）ネットワーク仮想化
3）ネットワークスライシング
4）MEC（Multi-Access Edge Computing）
5）5Gシステムドメインの重要度

4章　脅威の分析
4.1 一般的なセキュリティ脅威
4.2 NFVインフラストラクチャとMANOに対する脅威
4.3 NFVワークロードに対する脅威
4.4 RANに対する脅威
4.5 コアネットワークに対する脅威
4.6 ネットワークスライシングに対する脅威
4.7 MECに対する脅威

5章　対策
5.1 組織的な管理策
5.2 人的な管理策
5.3 運用管理策
5.4 物理的管理策
5.5 技術的対策
  5.5.1 共通的な対策
  5.5.2 仮想化の対策
  5.5.3 RANの対策
  5.5.4 5Gコアの対策
  5.5.5 スライスの対策
  5.5.6 MECの対策

6章　用語の定義

付録
Open RAN

3. ガイドラインの策定:ガイドラインの策定概要（脅威と対策の紐づけ）

2.1 用語の解説
2.1.1 セキュリティ脅威
(略)
脅威アクターの種類
- 内部アクター:
  - 不注意な者（Negligent Insiders）（Ⓝ）
  - 内部犯行者（Malicious Insiders）（Ⓜ）
- 外部アクター：
  - サプライヤー・通信事業者（Ⓢ）
  - 取引先・契約者（Ⓒ）
  - その他の外部の者（Ⓞ）
    （ハッカー、組織的犯罪者等を含む）

4.1 一般的なセキュリティ脅威
4.1.2.1 通信中データの改ざん

脅威ID	#TC_T_01
関連する脅威アクター	ⓂⓈⒸⓄ

ネットワーク上でデータ通信する際に、プロトコルの完全性保護が欠落していたり、受信側で情報の完全性を検証できなかったりすることで、意図せざる変更が加えられている可能性がある。ネットワーク上で通信データの完全性を確保することは、管理トラフィックにとって特に重要である。

5.5.4 5Gコアの対策
5.5.4.1 ユーザープレーンの保護

優先度	Critical
役割責任	通信事業者
コントロールタイプ	予防的
セキュリティ概念	保護
セキュリティの目的	認証,機密性, 完全性
関連する脅威	#TC_T_01, #TN_T_01, #TN_I_01

管理策：ユーザプレーンのトラフィックが、5Gコアに接続しているインタフェースや内部のインタフェースを介して保護されていない状態で転送されることがないようにすることが望ましい。

ガイダンス：ユーザデータの保護は、5G NRと5Gコアネットワークの接点における保護にはとどまらない。特に～　（略）

3. ガイドラインの策定:脅威と対策要件の記載例

4.5.2.1 ユーザープレーンのトラフィックの改ざん

脅威 ID	#TN_T_01
関連脅威アクター	ⓂⓄ

5Gコア内のユーザープレーンデータを伝送するインタフェースにおいて、完全性保護の欠如は、重要な個人情報の漏えいにつながる。RAN内のトラフィックよりも露出は少ないが、クラウド展開への移行のため、次のとおりオペレータのコアネットワークインタフェース内で対策を実施することが強く推奨される。

- 異なるUPFインスタンス間のN9インタフェース
- UPFと他のデータネットワーク間のN6インタフェース（公共のインターネットやLADN等）

5.5.4.1 ユーザープレーンの保護

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証, 機密性, 完全性
関連する脅威	#TC_T_01, #TN_T_01, #TN_I_01

管理策：ユーザープレーンのトラフィックが、5Gコアまたは5Gコア内部に接続しているインタフェースを介して保護されずに転送されることがないようにすることが望ましい。

（右上へ続く）

（左下より続く）

ガイダンス：ユーザープレーンデータの保護は5G NRのみに関連する訳ではない。展開シナリオによっては、5Gコアネットワークの特定の部分（特にUPF）も、信頼性の低い環境で実行される場合がある。これらのシナリオでは、確立されたセキュリティプロトコルを使用することで、すべての外部通信が保護される必要がある。したがって、5Gオペレータは、関連するすべてのコアネットワークインタフェース上でユーザープレーンのトラフィックの相互認証、機密性及び完全性を保護することが望ましい。

- UPFを5G NRに接続するインタフェース(N3インタフェース)
- 異なるUPFインスタンスを接続するインタフェース(N9インタフェース)
- UPFをLADN又は外部ネットワークに接続するインタフェース(N6インタフェース)

3GPP TS 33 501では、上記のインタフェースを保護するために他のセキュリティ手段が提供されていない場合は、NDS/IP（Network Domain Security/IP network layer security）を使用すると規定している。NDS/IPに加えて、5Gでは、UPFインスタンスを介して他の5Gオペレータとの通信を保護する方法として、Inter PLMN UP Security（IPUPS）機能も導入している。UPFの論理的な部分であるIPUPSは、N9インタフェース上の着信トラフィックに、例えば以下を含むGTP-Uセキュリティを適用することが考えられる。：

- 3GPPプロトコル標準に対するGTP-Uメッセージの有効性の検証
- GTP-Uメッセージにアクティブなpduセッションのトンネルエンドポイント識別子が含まれていることの検証

3GPPで規定されている制御を超えて、5Gオペレータは、5Gシステムとその加入者を保護するために、ユーザープレーン通信に関連するさらなる管理を実施することも考えられる。

今後の展開

- ガイドラインによる国内の5Gネットワークのセキュリティ確保への貢献に加え、国際標準化に向けた取り組みを推進
  - ICT-ISAC、5GMFセキュリティ調査研究委員会等、5Gネットワークのセキュリティに関する関係者に対して、作成したガイドラインの普及を進め、国内の5Gネットワークのセキュリティ確保を図る
  - ITU-T SG17で作成中の5Gセキュリティ標準化ロードマップの中で整理されている今後の標準化トピックのひとつとして、セキュリティ管理策をまとめたガイドライン文書の策定が挙げられているところ、本ガイドラインをベースとした勧告化提案を進めていく
- 構築した5Gセキュリティ検証環境の活用
  - NICT内に構築した検証環境を拡張して5Gを高度に活用する様々なユースケースに対応した検討や検証が行えるようにし、今後もNICTや5Gにかかわる我が国の産業界が5Gセキュリティ研究のために活用できるようにしていく

Tomorrow, Together

KDDI