特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

# 3 5G 移動通信システムのサイバーセキュリティ
## ―移動通信におけるセキュリティ対策の変遷とこれから―

応用 一般

窪田　歩　（株）KDDI 総合研究所

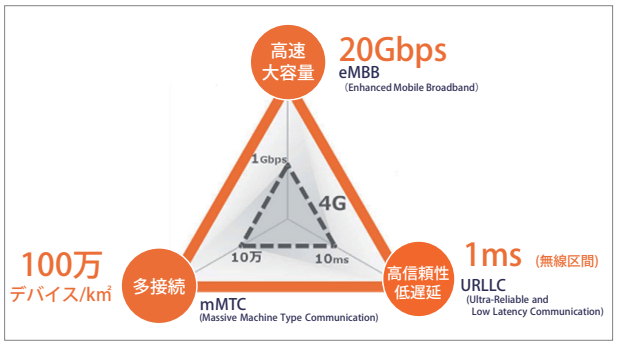
## 社会インフラとしての移動通信システム

移動通信システムは，図 -1 に示すように，音声通話が主体となっていた 1990 年代の 1 ～ 2G から，モバイルインターネット利用が広がった 3G を経てスマートフォン等によるモバイルブロードバンド通信を支える 4G へと発展する中で，社会インフラとしての重要性を高めてきた．5G では，図 -2 に示す通り，高速大容量通信，多接続，高信頼・低遅延の面で 4G からさらなる性能向上が図られ，新たなサービスの創出を促進することが期待されるとともに，今後さまざまな分野の DX（デジタルトランスフォーメーション）を支える基盤としての活用が進み，より一層重要な社会インフラとなっていくことが予想される．

本稿では，移動通信システムの発展を振り返り，移動通信システム特有のセキュリティ脅威とその対策の変遷について説明した後，5G の技術仕様におけるセキュリティ強化ポイント，5G システムの構築・運用におけるセキュリティ課題，5G セキュリティに関する国内外の動向について解説する．

## 移動通信システムにおけるセキュリティ脅威

図 -3 に移動通信システムの大まかな構成を示す．移動通信システムは，ユーザ端末（UE）が無線により基地局に収容される無線エリアネットワーク（RAN）と，認証，移動管理，セッション管理，課金，ポリシー制御等を担う機器群から構成されるコアネットワークからなり，インターネットやプライ




■図 -2　5G の技術進化


■図 -1　移動通信システムの発展

ベートネットワーク等のデータネットワークや，他通信事業者のネットワークと相互接続されて通信サービスを提供している．

移動通信システムにおけるセキュリティ脅威としては，アクセス回線に無線が使われることから，なりすましや盗聴，サービス妨害等の脅威があり，また，端末が常時携帯して利用されることから，端末の位置情報を捕捉，追跡されることによるプライバシー脅威もある．さまざまな場所に設置される基地局への物理攻撃の脅威なども考えられる．このため，移動通信システムにおいては，その初期からセキュリティ対策は重要課題として取り組まれてきている．以下ではまず，移動通信システムがデジタル化された 2G 以降のセキュリティ対策の変遷について概観する．

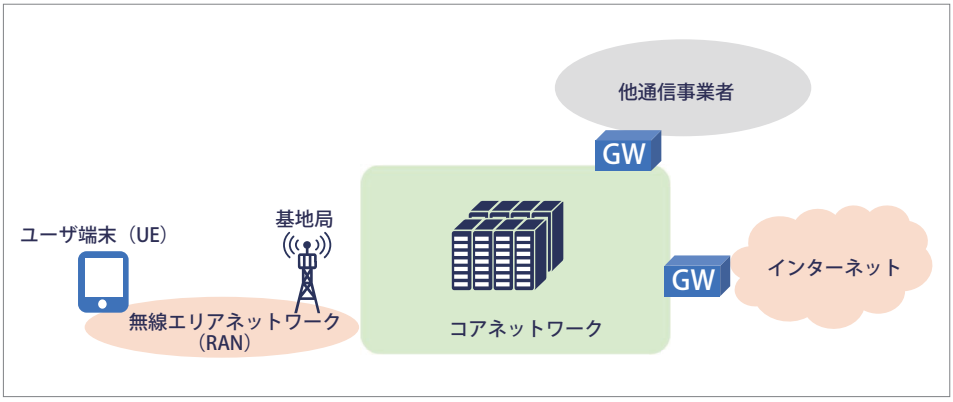
## 2G のセキュリティ

移動通信システムにおいて，正しく確実な課金を実現し，無線を利用して行われる加入者通信と加入者のロケーションプライバシーを保護するため，2G においてすでにさまざまなセキュリティ対策が導入されている．2G の通信規格として海外での主流である GSM（Global System for Mobile communication）の場合は，SIM（Subscriber Identity Module）を用いた強力な加入者認証によりなりすましや不正利用を防止し，無線区間においては加入者通信保護のため，通信の暗号化が行われている．また，IMSI（International Mobile Subscriber Identity）と呼ばれる加入者 ID を無線の傍受等を行う攻撃者から秘匿し，ロケーションプライバシーを保護するため，ネットワークに接続された端末の識別には TMSI（Temporary Mobile Subscriber Identities）が使われる．

GSM にはこのようなセキュリティ対策が導入されていたものの，セキュリティ上の課題も残っていた．加入者端末は SIM を利用して認証されるのに対して，端末による基地局認証は省略されていたため，偽基地局を用いた加入者 ID の収集や盗聴等が行われる脅威があった．これは 3G で端末と基地局の相互認証が導入された後も，2G のサービスが残っている地域では，3G への接続を妨害して 2G にフォールバックさせて偽基地局へ接続させる方法で攻撃に利用される事例が報告されている．また，2G 当時の技術的な制約により，鍵長が 64 ビットの弱い暗号アルゴリズムが使われており，改ざん検知も省略されていた．加えて，基地局から先のコアネットワーク内は信頼できる安全な区間であるとみなして暗号化は行われていなかった．

## 3G のセキュリティ

3G では端末と基地局間の相互認証の導入により偽基地局への対策が講じられた．暗号アルゴリズムは鍵長が 128 ビットとなり，制御信号に対する改ざん検知も導入されたほか，基地局から先のコアネットワークへも IPsec（TCP/IP 通信において IP パケット単位での認証，改ざん検知，暗号化による秘匿を実現するプロトコル）の利用によるセキュリティ対策が導入された．これらの対策により，安心・安全に広く利用される通信システムとなっている．




■図 -3　移動通信システムの構成

## 4G のセキュリティ

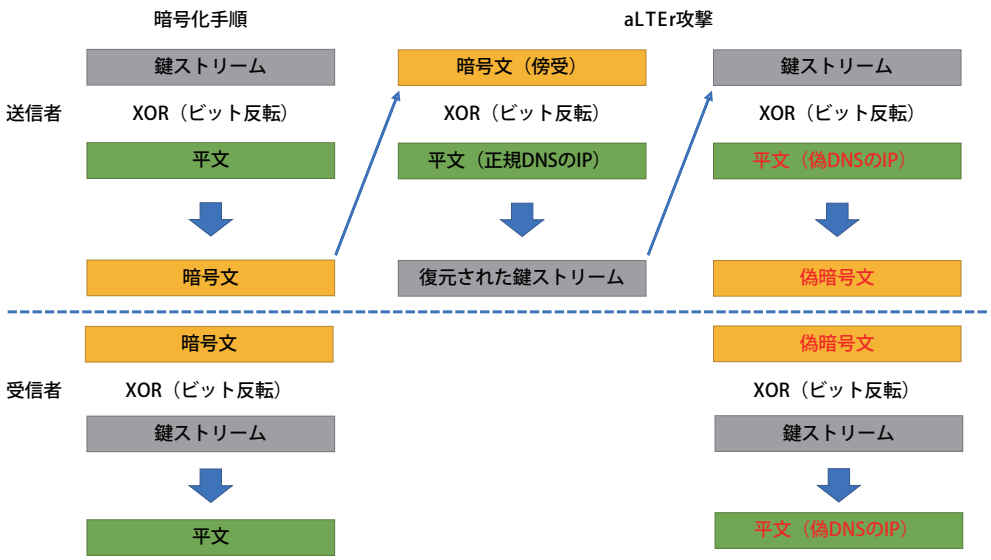
3G によりモバイルインターネット利用が進み，移動通信システムの利用シーンが広がったことで，屋内を含む無線アクセスのカバレッジの拡大や，通信容量の確保のため，より身近な場所に基地局が設置されるようになった．そうした場合，基地局が物理的な攻撃にさらされ，暗号鍵が盗み出されるリスクが存在する．実際に，一部の小型基地局で，ストレージから暗号鍵を取り出せたり，デバッグポートが無効化されていなかったりするなどの脆弱性がセキュリティ研究者により報告されている．こうした鍵の漏洩リスクへの対処と，通信の高速化，大容量化に伴って効率化が必要となる暗号鍵の更新処理の見直しのため，4G においては鍵の階層化が導入された．端末の認証手続きの結果として認証のたびに新たに生成される鍵から，端末の在圏時の鍵階層の基となる鍵を生成・保持し，そこからさらに鍵導出を繰り返して生成した個別の鍵をコアネットワーク内や基地局で利用することで，鍵の漏洩時の影響範囲の限定と，鍵更新処理のたびに端末の認証を繰り返さずに済む処理の効率化を実現している．

## 5G に向けた残存課題

移動通信システムは 2G から 3G，4G でのセキュリティ対策強化を経て安全性を高め，社会インフラとして広く利用されるようになっているが，いくつかのセキュリティ課題も指摘されている．以下ではそれらのうち主なセキュリティ課題について紹介する．

### U プレーンの改ざん検知

3G において制御信号（C プレーン）に対する改ざん検知が導入されたが，ユーザ通信（U プレーン）に関しては 4G においても暗号化しか行われていない．2019 年には，この U プレーンの改ざん検知が省略されていることを突いた攻撃手法（aLTEr）が研究者によって発表されている[1]．図 -4 に示すように，4G における暗号文は，鍵ストリームと平文の XOR（排他的論理和）によって作られているため，なんらかの条件や手段により平文が攻撃者にとって既知である場合，無線を傍受して得られる暗号文と平文との XOR により鍵ストリームを復元し，偽の平文と再度 XOR することで，偽の暗号文を作成することができる．aLTEr 攻撃では，端末がデフォルトで利用する DNS サーバの IP アドレスが既知であることを利用し，端末と基地局間の無線通信を不正




■図 -4　aLTEr 攻撃

に中継する攻撃者が，端末から送信される DNS クエリパケットの宛先部分の鍵ストリームを復元し，攻撃者が用意した偽の DNS サーバの IP アドレスと再度 XOR することにより作成した暗号文に書き換えて基地局に送信する．DNS クエリの宛先アドレス部分の偽暗号文は，U プレーンの改ざん検知がないため偽の IP アドレスに復号され，そのまま偽の DNS サーバにルーティングされることになる．攻撃者は偽 DNS サーバに届くクエリに対して偽の応答を返すことで，端末の通信を偽サーバに誘導することができる．

**加入者 ID の保護**

TMSI の利用による加入者 ID の秘匿や，3G で導入された基地局認証等により，加入者 ID の収集やロケーショントラッキングへの対策は強化されているが，4G においても残存リスクが指摘されている．加入者 ID が平文で無線区間を流れる手順が一部残っているほか，加入者 ID を秘匿するために利用されるテンポラリーな ID である TMSI が，通信事業者の設定によっては長期間更新されず，TMSI ベースのロケーショントラッキングが可能なケースがあることなどが指摘されている．

**事業者間通信**

ローミングなどのための通信事業者間の接続はクローズドな交換ネットワークを介して行われるため，2G や 3G では通信事業者間の相互信頼を前提とし，セキュリティを考慮していない古いプロトコルである SS7（Common Channel Signaling System No.7）が使われている．通信事業者の数が増えるに従い，事業者間の信頼に関する前提が崩れてきており，SMS の不正な転送による 2 要素認証の突破などの事例も発生している．このため，通信事業者では SS7 ファイアウォールの導入などの対策が進められている．4G では SS7 に代わり Diameter（インターネット技術の国際標準を議論・策定している IETF が策定した認証・認可・課金のためのプロトコル）が採用されているが，セキュリティ研究者により Diameter にも脆弱性の存在が指摘されている状況である．

## 5G の技術仕様におけるセキュリティ強化ポイント

5G は 4G までに導入されたセキュリティ対策を踏襲しつつ，上述の残存課題への対応を含めたさらなるセキュリティ強化が図られている[2), 3), 4)]．以下では Non-Stand Alone（NSA）の 5G と Stand Alone（SA）の 5G のセキュリティ面での違いについて述べた後，5G の技術仕様における主なセキュリティ強化ポイントについて説明する．

### NSA と SA

5G 導入の初期段階では，4G のコアネットワークを利用して 5G 無線を利用する NSA によるサービス展開が進められており，その後，5G のコアネットワークを持つ SA の導入が進められることになる．NSA では，複数基地局を同時利用して高速大容量通信を実現する 4G の仕様である Dual Connectivity を拡張し，4G 基地局をマスタ，5G 基地局をセカンダリとして利用可能にすることで 5G 無線の利用を実現している．このため，NSA では 5G 無線を利用した高速大容量通信は可能になるが，セキュリティ面では 4G と大きな違いはなく，以下で述べるセキュリティ強化は SA の導入によって実現されることになる．

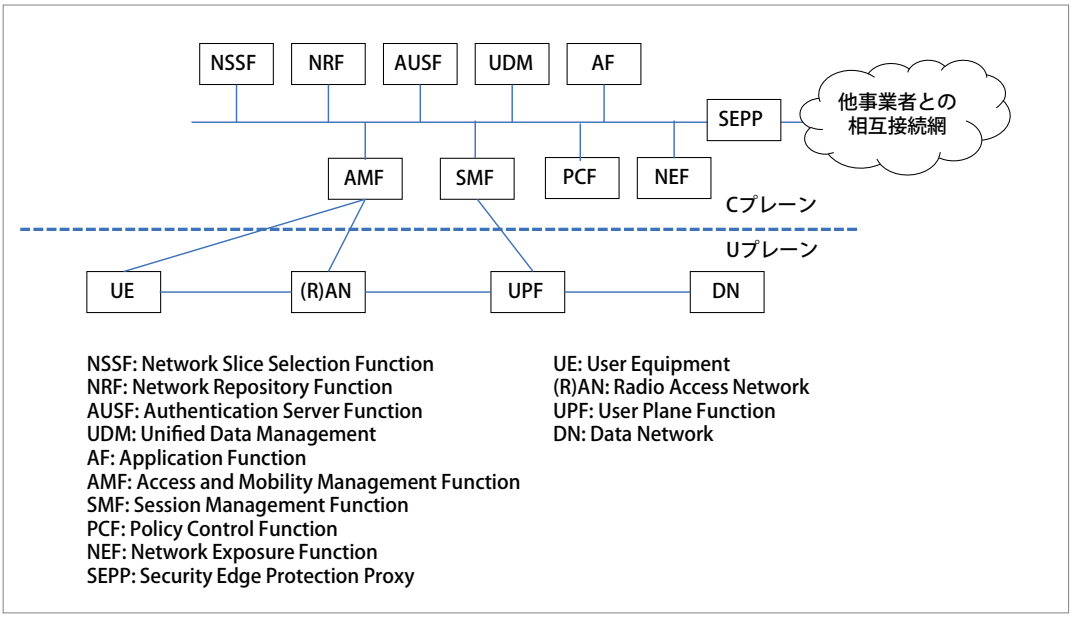
### トラストモデルの見直し

無線区間と異なりコアネットワークは安全であるとして基地局以降のコアネットワーク内のセキュリティ対策を省略していた 2G のセキュリティ設計や，通信事業者間の信頼を前提として SS7 を利用していた事業者間通信など，過去の移動通信システムでは仕様策定時のトラストに関する前提に基づいてセキュリティ対策の省略や最適化が図られてきた．5G では，信頼できるとみなす対象や範囲をより限

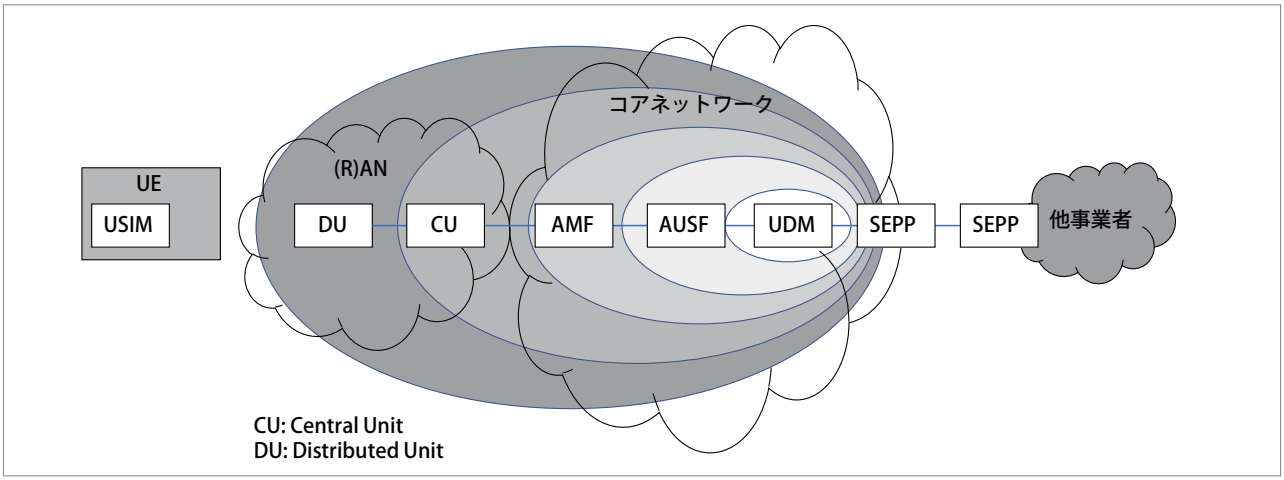
定した上でセキュリティ設計を行うことにより，セキュリティのさらなる強化が図られている．図 -5 に 5G のアーキテクチャを示しているが，トラストモデルの見直しでは，具体的には，コアネットワーク内で，加入者情報管理や認証処理を担う UDM（Unified Data Management）と AUSF（Authentication Server Function）を信頼のコアとし，図 -6 に示すようにコアから遠ざかるに従いトラストが低下するモデルとし，それに従ったセキュリティの設計が行われている．

## RAN における CU/DU 分離

トラストモデルの見直しにより，コアから離れたネットワークエッジに展開される基地局はセキュリティ確保が難しく信頼度が低いという前提が置かれている．これは，5G においてはカバレッジ確保のために膨大な数の基地局のきめ細かな配備が必要になり，物理的セキュリティの確保が困難な場所にも多数の基地局を設置する必要があるためである．このため 5G では，基地局機能を CU（Central Unit）と DU（Distributed Unit）に分離し，末端に位置す




■図 -5　5G のアーキテクチャ




■図 -6　5G のトラストモデル

る DU には暗号処理に関する情報を保持させず，コア側に近く，セキュリティ確保が可能な場所に設置できる CU で暗号処理を終端させることで，DU がセキュリティ侵害を受けたとしても加入者通信が保護される設計になっている．

## 加入者 ID 保護の強化

5G では加入者 ID を IMSI ではなく SUPI(Subscriber Permanent Identifier）と呼称するが，5G の仕様では，ネットワークへの初期登録の手順も含めて SUPI が平文で無線区間を流れることはなく，必ず，契約先の通信事業者の公開鍵を用いて SUPI を暗号化した SUCI（Subscriber Concealed Identifier）の形で送信されるよう仕様が規定されている．また，端末の識別に利用されるテンポラリな ID（5G-GUTI : Globally Unique Temporary Identifier）の更新頻度についても厳格に仕様で定められており，GUTI ベースのロケーショントラッキングにも対策が講じられている．

## RAN のセキュリティ強化

4G で省略されていたセキュリティ機能として，U プレーンの改ざん検知がある．5G では，U プレーンへの改ざん検知機能が新たに追加されたが，移動通信システムの仕様検討・作成を行う 3GPP（3rd Generation Partnership Project）が Release 15 として発行した 5G の初期仕様では，処理負荷を考慮し，64Kbps までの通信では改ざん検知を必須とし，それ以上の高速通信ではオプションとなっていた．2019 年の aLTEr 攻撃の発表を受け，その後に発行された 3GPP Release 16 の仕様ではフルレートでの改ざん検知の実施が必須と定められている．

## 事業者間セキュリティ（SEPP と Home Control 強化）

トラストモデルの見直しに伴い，通信事業者同士であっても必ずしも信頼できないという前提でアーキテクチャの見直しやセキュリティ手順の見直しが図られている．図 -5 に示した通り，5G では他事業者との相互接続は SEPP（Security Edge Protection Proxy）を介して行われる形になり，SEPP により事業者間通信における認証，認可，秘匿，改ざん検知，リプレイ攻撃対策などのセキュリティ機能が提供される．

また，加入者が契約先事業者のネットワーク（Home Network）から他事業者のネットワーク（Visited Network）へローミングした際の認証に際しては，ローミング先で行われた認証の結果を Home Network 側の事業者が検証する Home Control の強化が図られている．

## セキュアな実装と脆弱性への対応

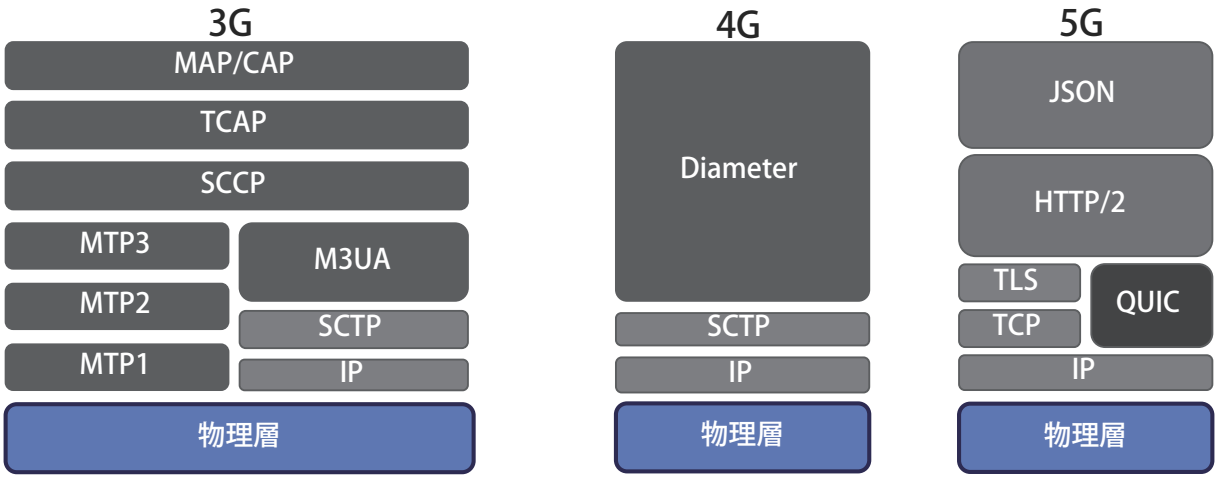
以上のようなセキュリティ強化に加え，5G の仕様ではさまざまなセキュリティ対策についての規定が定められているが，5G システムを構成する通信機器が仕様に従って正しく実装されていなければ実際に安心・安全な移動通信システムを実現することはできない．また，技術仕様自体や運用中の製品にセキュリティ上の問題が発見され，仕様の改訂や通信機器の更新等が必要になる場合もあり，そうした場合の情報開示や対応のプロセスを整備することも長期間に渡り運用される社会インフラとしての移動通信システムのセキュリティ確保において重要である．このため，5G の技術仕様を定める 3GPP と，移動通信の業界団体である GSMA（GSM Association）が連携し，通信機器が一定レベルのセキュリティを有していることを保証するための枠組みとして NESAS（Network Equipment Security Assurance Scheme)が整備されている．NESAS では，通信機器ベンダの製品の設計開発やライフサイクル管理プロセスの監査や，3GPP が定めたネットワーク機器のセキュリティ仕様である SCAS（Security Assurance Specification）に基づいて個々の製品が正しく実装されていることの認定ラボでの試験結果を通じて，導入する通信機器のセキュリティレベル

を通信事業者が確認可能にする枠組みであり，すでにいくつかの大手通信機器ベンダや製品が認定を取得している．また，移動通信システムにかかわる脆弱性等の情報の開示や対応については，GSMA のCVD（Coordinated Vulnerability Disclosure）プログラムにより，GSMA が窓口となって，セキュリティ研究者等が発見した問題の一般公表前の情報共有や影響分析，関係組織による対応のコーディネーションが行われている．

## 構築・運用面での課題

技術仕様の上では，5G は 4G からのセキュリティ強化が図られ，より安心・安全に利用できる移動通信システムになっているが，5G システムの構築・運用の全体を考えた場合にはセキュリティ上の懸念や課題が存在する．

図 -7 に示す通り，移動通信システム固有のプロトコルが使われていた過去の世代と異なり，5G のコアではインターネットで利用されている一般的なプロトコルが使われるようになっている．このため，移動通信システムへのサイバー攻撃も，特殊な専用機器やプロトコルの知識を要するものではなく，Web アプリへの攻撃に近くなると考えられ，脆弱性の発見や対処などのセキュリティ運用の重要性が一層高まることが想定される．また，さまざまなユースケースに応じて 5G の性能をチューニングした専用の仮想ネットワークを提供するネットワークスライシングの実現などのため，5G コアネットワークでは仮想マシンやコンテナなどの仮想化技術の活用が進み，これに伴うシステム構成の複雑化や，物理適切に設定し運用することが難しくなることが想定される．このように，安心・安全な 5G システムの構築・運用には，5G セキュリティの技術仕様への準拠だけでなく，ベースとなる仮想化基盤のセキュリティや組織面，運用面の考慮など，広範な検討が必要になる．このリファレンスとするため，国内では，5G セキュリティ検証環境を構築して実施したセキュリティ検証結果と，技術的対策だけではなく組織や運用面も含めたトータルな 5G セキュリティの分析結果に基づき，5G セキュリティのガイドライン文書の策定が総務省主導で進められており，その中間とりまとめ結果が「5G ネットワーク構築におけるセキュリティに関する対策等の留意点（令和 2 年度版）」として公表されている [5]．




■図 -7　プロトコルスタックの変遷

## 国内外の動向

さまざまな産業分野での活用が期待されている5Gの社会インフラとしての重要性はきわめて高いため，各国政府当局や関係機関では，5Gセキュリティに関して技術的な課題だけでなく，地政学上のリスクも含めたさまざまな取り組みを進めている．

米国では2020年春に「National Strategy to Secure 5G」を公表し，5Gにおけるサイバー脅威と脆弱性のリスク評価やサプライチェーンリスク管理等の政策を推進しており，特にサプライチェーンリスクが懸念される機器の排除やサプライチェーンの信頼性確保に向けて同盟国との連携を強化する動きが見られる．

欧州では2020年1月にEU委員会（European commission）がEUにおける5Gのセキュリティ課題に取り組むためのフレームワークであるEU Toolboxを発表している．Toolboxは5Gネットワークのセキュリティリスクに対処するために取り得る政策的手段や技術的手段をまとめたもので，EU各国に対してToolboxを利用した5Gシステムのセキュリティ対策を要請している．また，ENISA（欧州ネットワーク情報セキュリティ庁）はEU Toolboxの策定にあわせ，5Gにおけるさまざまな脅威の分析，カテゴリ，5Gネットワークの安全な設計やアーキテクチャ等，5Gのセキュリティに関する事項を網羅的かつ体系的にまとめた「ENISA Threat Landscape for 5G Networks」を公表した．現在，EU各国において5Gインフラの安全・信頼性確保のための取り組みを進めている．

国内では上述した5Gセキュリティガイドライン策定に向けた総務省の取り組みのほか，第5世代モバイル推進フォーラム（5GMF）のセキュリティ調査研究委員会において，ユースケース視点での5Gセキュリティ検討が行われ，白書「5Gユースケースにおけるセキュリティ第1.0版」が発行されている．また，ICT-ISACにおいても5Gセキュリティ推進グループが設置され，主にローカル5Gをターゲットに5Gセキュリティの情報交換やガイドライン文書の作成が進められている．

## 5Gセキュリティの今後

4Gコアを利用するNSAでスタートした5Gが，今後5Gコアを利用するSAに移行し，ネットワークスライスやMEC（Multi-access Edge Computing）等の5Gコアにより実現する新たな仕組みがさまざまなサービスや産業分野で活用されるようになると，社会インフラとしての5Gの重要性はますます高まっていくと想定される．重要社会インフラとしての5Gのセキュリティ確保には，5Gの技術仕様に閉じた議論だけではなく，仮想化やクラウド技術などの周辺技術のセキュリティや，サプライチェーンの信頼性確保など，広範な検討が必要であり，5Gを提供・活用するさまざまなステークホルダ間での情報共有や連携による継続的・長期的な取り組みが求められる．

**参考文献**

1）Rupprecht, D., Kohls, K., Holz, T. and Pöpper, C. : Breaking LTE on Layer Two, in 2019 IEEE Symposium on Security and Privacy(S&P), San Fransisco, CA, US (2019).
2）3GPP TS 23.501:System architecture for the 5G System (5GS), Release 16, v16.4.0 (Mar. 2020).
3）3GPP TS 33.501: Security Architecture and Procedures for 5G System, Release 16, v 16.2.0 (Mar. 2020).
4）Prasad, A. R. : Sivabalan Arumugam, Sheeba B and Alf Zugenmaier, 3GPP 5G Security, Journal of ICT Standardization, River Publishers, Vol.6, Iss.1&2.
5）総務省サイバーセキュリティタスクフォース（第31回）参考資料1（2021年5月）．

（2022年1月11日受付）

■窪田　歩（正会員）　ay-kubota@kddi.com

1995年国際電信電話（株）（現KDDI）入社．IPネットワークにおけるQoS制御，モビリティサポート，サイバー攻撃検知・対策技術等の研究開発に従事．現在，（株）KDDI総合研究所サイバーセキュリティGグループリーダー．2019～2020年本会理事．