# 5GMF 白書

## 5G ユースケースにおけるセキュリティ

第 1.0 版

2020 年 7 月 29 日

# 目次

## 1. はじめに（報告概要）

2019 年度、5G セキュリティの検討要求が各方面から多かったため、5GMF において、「セキュリティ AdHoc」を「セキュリティ調査研究委員会」に昇格させ、本格的に検討を開始した。

本白書は、セキュリティ調査研究委員会において検討した内容をまとめたものである。

## 2. セキュリティ調査研究委員会活動の目的

2019 年 7 月の総会にて承認され、「セキュリティ調査研究委員会」が設置された。

設置目的は、5G 時代のサービスのセキュリティに関する検討組織の立ち上げに向けて、国内外の「5G セキュリティ」に関する調査検討、情報の共有や発信、推進団体との連携等を図ることとした。

主に参加委員の意見などから、全体に共通の 5G セキュリティ標準化動向を踏まえて、①IoT、②Connected Vehicle、③Fintech を検討項目とし、関連したセキュリティ検討項目を抽出することを目的とした。

参加メンバーは、募集等の準備を経て 2019 年 9 月に 21 名にて本格的な活動を開始した。

以下のユースケースにおけるセキュリティ課題の抽出を実施した。

- 計算リソースに制限のある IoT デバイス、多量の IoT デバイス（認証技術等）
- Connected Vehicle（自動運転、運転支援）
- Fintech 関連サービス（モバイルコマース関連）

## 3. 用語

3GPP: Third Generation Partnership Project
5GAA: 5G Automotive Association
ACEA: European Automobile Manufacturers' Association
AECC: Automotive Edge Computing Consortium
AF: Application Function
AMF: Access and Mobility management Function
AUSF: Authentication Server Function
CN: Core Network
CR: Compliance Rules
CRL: Certificate Revocation List
C-V2X: Cellular V2X
DDoS: Distributed Denial of Services
DoS: Denial of Services
DRM: Digital Rights Management
DSRC: Dedicated Short Range Communications
ECU: Electronic Control Unit
ENISA: The European Union Agency for Cybersecurity
eSIM: embedded Subscriber Identification Module
ETSI: European Telecommunications Standards Institute
EVITA: E-safety vehicle intrusion protected applications
GSMA: GSM Association
GUTI：Global Unique Temporary Identifier
HDCP: High-bandwidth Digital Content Protection
HDMI: High-Definition Multimedia Interface
HIS: The Hersteller Initiative Software
IMSI: International Mobile Subscriber Identity
IRN: Infrastructure/Roadside Network
ITS-S: ITS Station
ITS-SCU: ITS Station Communication Unit
ITS-SU: ITS Station Unit
IVN: In-Vehicle Network
LDP: Local Dynamic Map
MEC: Mobile Edge Computing/Multi-access Edge computing
NAS: Non-Access Stratum

NESAS: Network Equipment Security Assurance Scheme
NEF: Network Exposure Function
NF: Network Function
NRF: Network Repository Function
NS: Network Slice
NSSAI: Network Slice Selection Assistance Information
NSSF: Network Slice Selection Function
OBU: Onboard Unit
OTA: Over the Air
PKI: Public Key Infrastructure
PVS: Prove Vehicle Systems
QoS: Quality of Service
RAN: Radio Access Network
RR: Robustness Rules
RSU: Road Side Unit
SAE International: Society of Automotive Engineers
SBA: Service Based Architecture
SCAS：Security Assurance Specifications
SCN: Sensor and Control Network
SMF: Session Management Function
SUCI: Subscription Concealed Identifier
TCG: Trusted Computing Group
TEE: Trusted Execution Environment
TFCS: Task Force on Cyber Security
TLS: Transport Layer Security
UE: User Equipment
UNECE: United Nations Economic Commission for Europe
UPF: User Plane Function
URLLC: Ultra-Reliable and Low Latency Communications
V2D: Vehicle-to-nomadic Devices
V2I: Vehicle-to-Infrastructure
V2N: Vehicle-to-Network
V2P: Vehicle-to-Pedestrian
V2V: Vehicle-to-Vehicle
V2X: Vehicle-to-Everything

## 4. 5G セキュリティの標準化動向

### 4.1. はじめに

本章では、3GPP においてセキュリティとプライバシ関連の標準化の議論を担当している SA3 ワーキンググループでの活動を中心に、5G セキュリティに関する標準化動向を概観する。まず、5G の標準化と導入スケジュールについて述べた後、3GPP Release 15 で規定され、5G 導入初期に用いられるノンスタンドアローン（NSA）構成の 5G におけるセキュリティ、スタンドアローン（SA）構成における LTE とのセキュリティの違い、2020 年 6 月完了予定の Release 16、および、Release 17 に向けた検討の現状について説明する。

### 4.2. 5G の標準化と導入スケジュール

モバイル通信システムの国際標準（IMT：International Mobile Telecommunications）を扱う ITU（国際電気通信連合）と 3GPP（3rd Generation Partnership Project）では、2020 年の 5G（IMT-2020）の実現に向け、標準化活動が最終フェーズを迎えている。5G によって、超高速（eMBB：Enhanced Mobile Broadband)、超低遅延（URLLC：Ultra Reliable and Low Latency Communication)）、多数同時接続（mMTC：massive Machine Type Communications）を実現する標準仕様が検討されている。

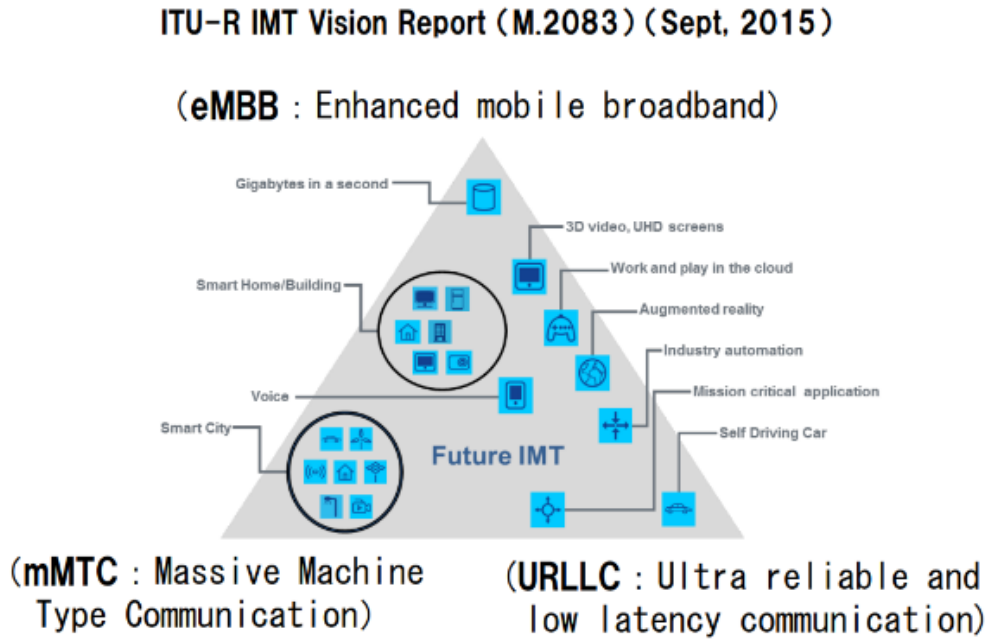



図 4.1　IMT-2020 のビジョン勧告で規定する 5G ユースケース

4G から 5G への移行については、2020 年に 5G 用の新しい周波数帯を用いた eMBB サービスを提供する。これは、新たな無線技術（NR: New Radio)に対応した基地局が、LTE 基地局と連携する NSA（Non-Standalone）構成で運用する。また 202X 年にネットワークスライシング等に対応した 5G コアネットワークを導入、SA（Standalone)構成の NR 基地局の運用が開始され、既存周波数帯域への NR 導入が進展する。これにより超高速、多数同時接続、高信頼・低遅延などの要求条件に対応した 5G サービスが提供される。

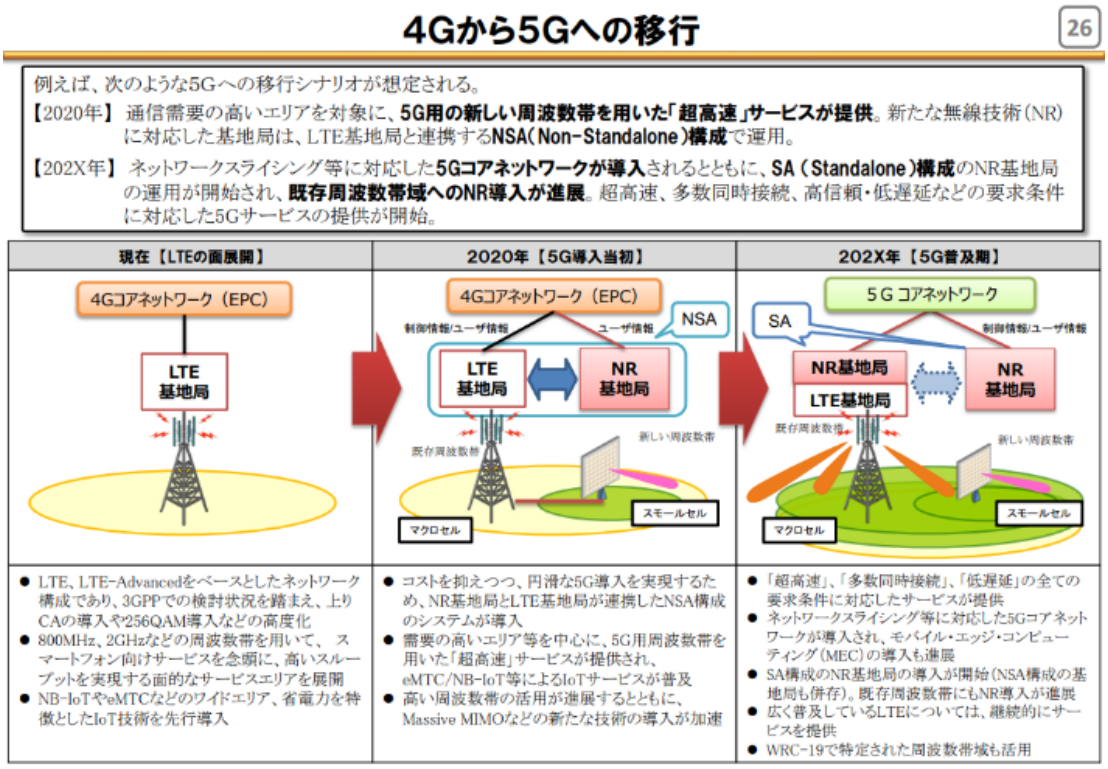



図 4.2　総務省資料（4G から 5G 移行説明部分）

3GPP SA3 における 5G セキュリティの標準化活動のこれまでの経緯と計画を以下に示す。

- 2017 年 6 月（Release 14）
  - 5G security study
    - 5G において考慮すべき 17 のセキュリティ領域を定めて課題と対策を整理
    - その後の検討のためのメモ的な位置づけであり標準ではない
- 2019 年 6 月（Release 15）
  - 5G phase 1 security
    - トラストモデル、鍵階層、事業者間セキュリティ、プライバシ保護等
    - メインのユースケースは eMBB
- 2020 年 6 月（Release 16）
  - 5G phase 2 security
    - 5G の SCAS（Security Assurance Specification）、ネットワークスライスセキュリティ、5G における 256 ビット暗号サポート等
    - mMTC, URLLC をカバーするセキュリティ強化
- 2021 年 9 月（Release 17）
  - 無線技術の革新など様々な検討
    - セキュリティに関して現時点で挙がっているワークアイテムは GBA（Generic Bootstrap Architecture）の 5G コアへの統合、IMS の SCAS、Lawful Interception の 3 件

5G の無線方式である「5G NR（New Radio）」の標準仕様が「3GPP Release 15」であり、Release 15 では、コアネットワークや基地局など無線ネットワークを構成する機器すべてに 5G 専用のものを使用して構成する SA の仕様が策定されている。5G NR のうち、LTE と NR の組み合わせで運用するケースの基本仕様（現行の LTE との連携部分）を規定する NSA は、2017 年 12 月に標準策定が完了しており、2020 年前後を予定している 5G のサービス導入初期においては、この NSA の構成が用いられる。Release 16 で規定される 5G phase 2 は mMTC や URLLC をカバーする完全な 5G 仕様であり、3GPP SA3 においては、5G コアの各ネットワーク機能の SCAS（Security Assurance Specification）、ネットワークスライスのセキュリティ、256 ビット暗号サポート、mMTC、URLLC をカバーするセキュリティ強化、バーティカルや LAN サービスのセキュリティ等について検討が進められてきた。

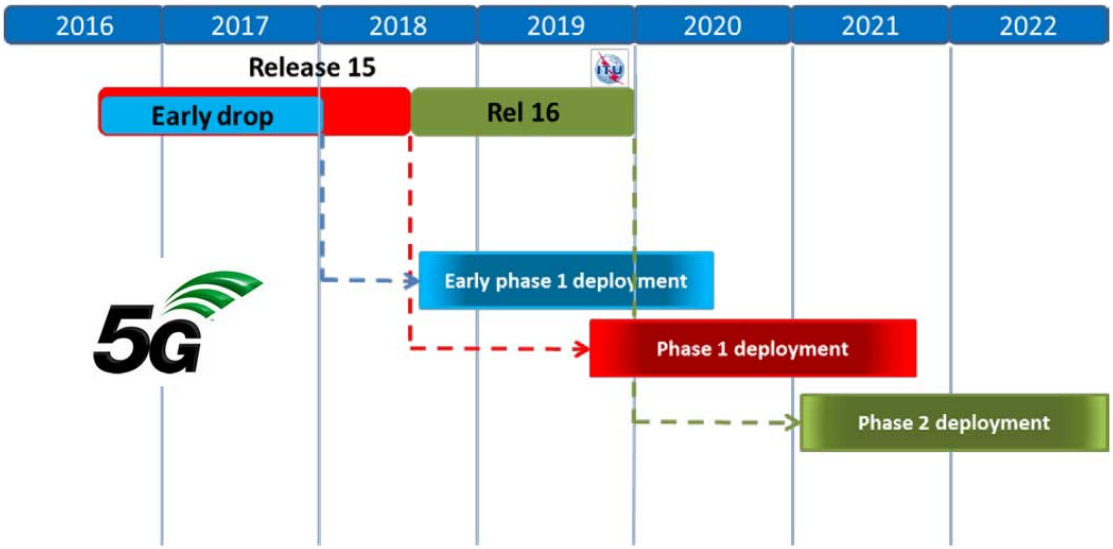



図 4.3　3GPP の検討ステータス

4.3. NSA のセキュリティ

NSA は、LTE（4G）のネットワークコア（EPC: Evolved Packet Core）を利用して 5G の導入を進めるためのアーキテクチャであり、以下の図 3.4 に示す通り、端末と基地局部分のみが 5G 化され、5G 無線を利用した高速大容量通信が可能となる。

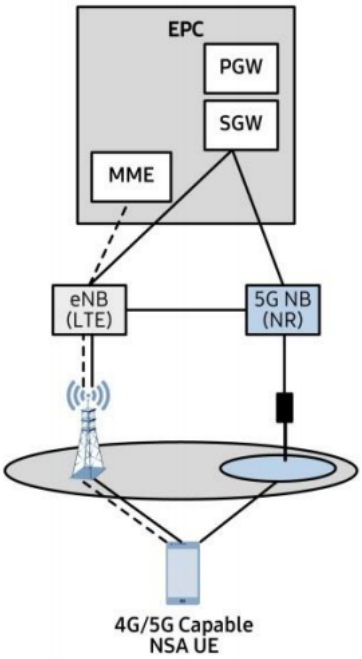



図 4.4 ノンスタンドアローン構成の 5G

NSA 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として TS 33.401 の Annex E で定められている Dual Connectivity を 5G に拡張し、LTE 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実現されている。セキュリティの手順は LTE の Dual Connectivity をほぼ流用しており、NSA においては、セキュリティに関して LTE との大きな違いはなく、次節以降で述べる通り、SA への移行により 5G のセキュリティは LTE よりも強化されることになる。しかしながら、ネットワークコアが 5G 化した後も、LTE 基地局をマスタ、5G 基地局をセカンダリとして利用する、もしくは、5G 基地局をマスタ、LTE 基地局をセカンダリとして利用する形で 5G と LTE の併存が続くと想定されているため、各ユースケースにおけるセキュリティ検討においては、5G エリア外への移動や LTE 接続へのダウングレード攻撃などの可能性を考慮する必要があると考えられる。。

## 4.4. 5G phase 1 のセキュリティ

### 4.4.1. トラストモデルの変化

5G においては、コアから遠ざかるに従いトラストが低下するとみなす考えに基づいてセキュリティが設計されている。このため、例えば RAN においては基地局が Distributed Units (DU)と Central Units (CU)に分離され、物理的に安全性の低い場所に配備される DU には鍵を保持させず、U-Plane のセキュリティは CU で終端される。また、図 3.5 に示す通り、事業者間でのローミングにおいては、ローミング先(vPLMN)での認証結果をホームネットワーク(hPLMN)における認証処理を担う AUSF（AUthentication Server Function）が検証することで Home Control の強化を図る。また、図 3.6 に示す通り、事業者間の C-Plane の通信を保護するためにローミング先(vPLMN)とホームネットワーク(hPLMN)との接続点において Security Edge Protection Proxy (SEPP)の導入などが行われている。

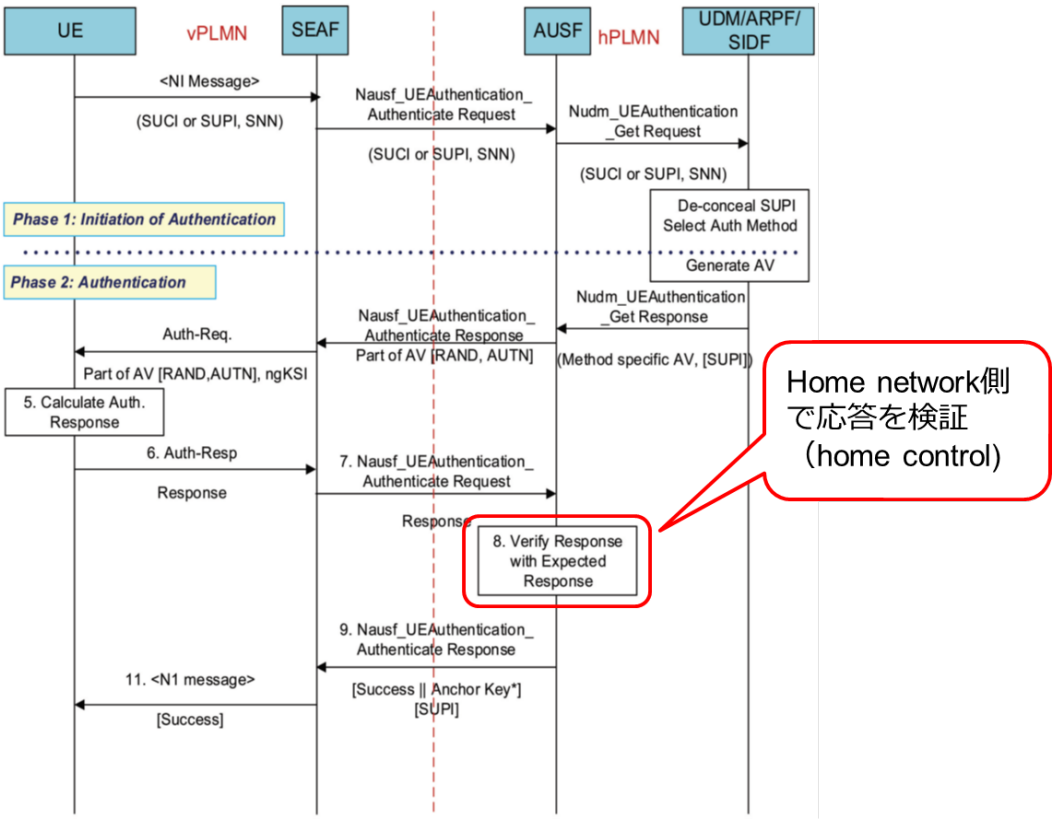



図 4.5 5G の認証手順と Home Control

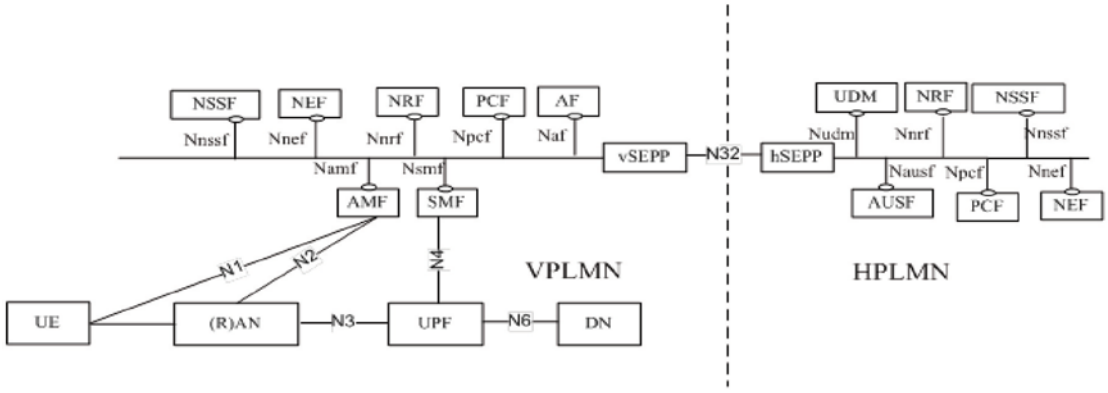



図 4.6 ローミング時のアーキテクチャ

4.4.2. 鍵階層

LTE と同様に、5G においても USIM とコアネットワークに保持された長期秘密鍵（K）がセキュリティの基点となる。5G では、モバイルネットワークサービスにアクセスするためにすべてのデバイスが実行する Primary Authentication と、外部データネットワーク（DN）が要求する場合に行われる DN との Secondary Authentication の 2 種類の認証がある。UE (User Equipment)とネットワークとの間の Primary Authentication が成功した後、サービングネットワーク固有のアンカー鍵（$K_{SEAF}$）が K から導出される。アンカー鍵から、CK (Cipher Key) と IK (Integrity Key) が導出される。K から始まる鍵の階層を図 3.7 に示す。

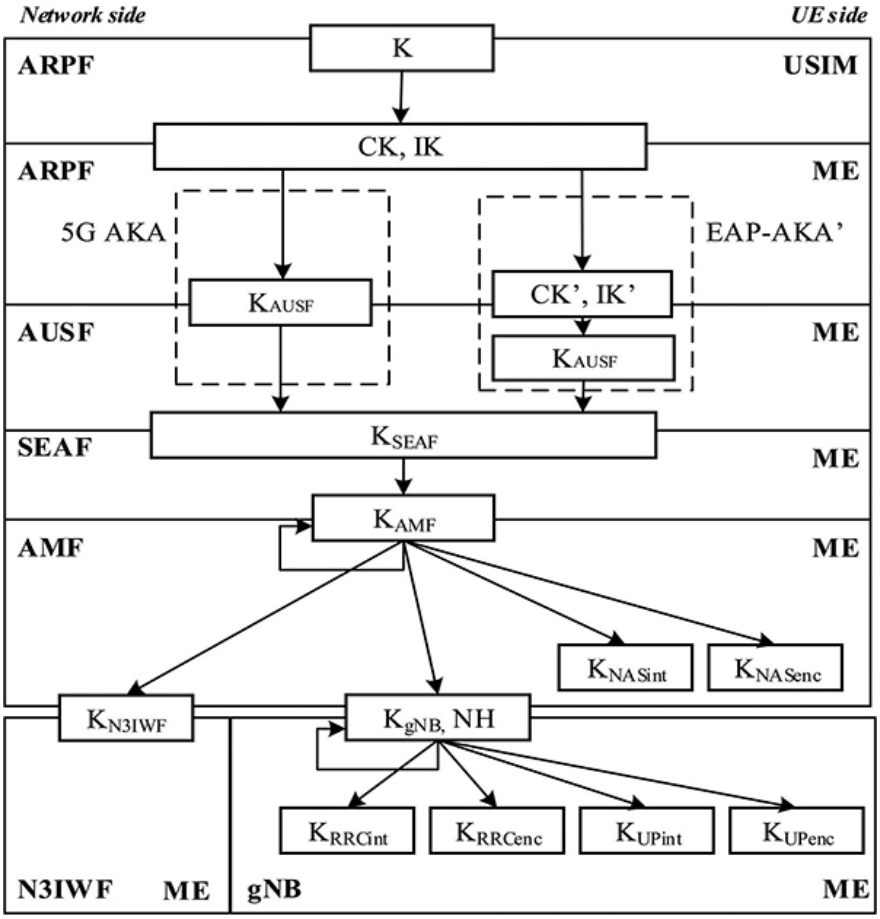



図 4.7 鍵の階層（Key hierarchy）

鍵の階層には K、CK、IK、K AUSF、K SEAF、K AMF、K NASint、K NASenc、K N3IWF、K gNB、 K RRCint、K RRCenc、K UPint、KUPenc が含まれる [1]。

- K AUSF は、5G AKA を通じて、CK および IK から端末と ARPF 各々で導出される。
- EAP をサポートする無線アクセス技術を介した認証に 3GPP クレデンシャル K が使用される場合、K AUSF は、EAP AKA '仕様に従って ME および AUSF によって導出される。
- K AUSF から、AUSF および ME はアンカー鍵 K SEAF を導出し、K SEAF は ME および SEAF によって K AMF を導出するために使用される。
- K ' AMF は、UE が、ある AMF から別の AMF に移動するとき、以前の K AMF から ME および AMF によって導き出すことができる鍵である。
- K NASint と K NASenc は NAS シグナリング保護のために、K AMF から ME および AMF によって導出される。
- K gNB は、K AMF から ME および AMF によって導出される。K gNB は、移動の際に、中間キーK gNB * を使用して、ME および移動元 gNB によって導出される場合もある。

[1] AUSF: Authentication Server Function, SEAF: Security Anchor Function, AMF: Access Management Function, NAS: Non-Access Stratum, gNB: Next generation NodeB, RRC: Radio Resource Control, UP: User Plane

- AS の完全性および機密性キー、すなわち UP（$K_{UPint}$ および $K_{UPenc}$）および RRC（$K_{RRCint}$ および $K_{RRCenc}$）は、$K_{gNB}$ から ME および gNB によって導出される。UP の完全性保護は、IoT（Internet of Things）サービスのために拡張である。中間鍵 NH は、ハンドオーバ中における forward secrecy を担保するために、ME および AMF によって導出される。

4.4.3. プライバシ保護の強化

4G までのネットワークにおいては加入者 ID（IMSI）の保護が不十分であり、IMSI キャッチャー等を用いた加入者の追跡等が可能であった。5G では加入者 ID の保護を強化するため、ホームネットワークの公開鍵を用いた加入者 ID の暗号化が行われる。

5G における加入者 ID は Subscription Permanent Identifier (SUPI)と称し、Mobile Country Code (MCC)、Mobile Network Code (MNC)、Mobile Subscriber Identification Number (MSIN)から構成される。端末は、緊急通報等の場合を除いて、必ずホームネットワークの公開鍵を用いて MSIN 部分を暗号化した Subscription Concealed Identifier (SUCI) を用いてネットワークに接続する。SUCI はホームネットワークの ARPF において SUPI に戻されて以降の認証手順が進められる。

4.4.4. Primary / Secondary Authentication

先に述べた通り、5G では、モバイルネットワークサービスにアクセスするためにすべてのデバイスが実行する Primary Authentication と、外部データネットワーク（DN）が要求する場合に行われる DN との Secondary Authentication の 2 種類の認証がある。Primary Authentication はアクセスネットワーク非依存であり、Wi-Fi 等の非 3GPP アクセスネットワークを介した接続にも利用される。認証と鍵導出には 5G-AKA もしくは EAP-AKA'が用いられる。Home Control 強化のため、ローミング先ネットワークでの認証結果をホームネットワーク側で検証する手順が組み込まれている。

Secondary Authentication は外部データネットワーク (DN) が要求した場合に行われる認証で、EAP を利用して行われる。SMF が EAP の Authenticator として振る舞い、外部の認証サーバ（DN－AAA）を利用して端末を認証する。前提として、端末は Primary Authentication により AMF とのセキュリティコンテキストを確立している必要がある。

4.4.5. On-demand セキュリティ

5G は様々な分野やサービスで利用されるため、デバイスやアプリケーションなどによって異なるセキュリティ要件や、制約を持っている場合が想定される。このため、U-Plane の暗号化や改ざん検知の有無、暗号強度などが選択可能であり、gNB（基地局）は AMF 経由で SMF から入手したセキュリティポリシと gNB と UE 双方の capability に基づいてアルゴリズムを選定し UE に通知する。

4.5. 3GPP Release 16（5G phase 2）のセキュリティ課題と Release 17 に向けた状況

Release 16 の主なセキュリティ課題として、2019 年 3 月時点では、長期鍵の更新、256 ビット鍵の利用、SECAM／SCAS、ネットワークスライスセキュリティ、位置情報サービスセキュリ　ティ、URLLC セキュリティ、バーティカルと LAN サービスのセキュリティ、SBA セキュリティ

等がワークアイテムとして挙げられていた。

| |
|---|
| Feature or Study Item: Study on authentication enhancements in 5GS |
| Feature or Study Item: Study on the security of URLLC for 5GS |
| Feature or Study Item: Study on Security for 5GS Enhanced support of Vertical and LAN Services |
| Feature or Study Item: Study on evolution of Cellular IoT security for the 5G System |
| Feature or Study Item: Study on Security of the enhancement to the 5GC location services |
| Feature or Study Item: Study on the security of the Wireless and Wireline Convergence for the 5G system architecture |
| Feature or Study Item: Mission Critical Services Security Enhancements |
| Feature or Study Item: Study on Security aspects of Enhancement of Network Slicing |
| Building Block: Study on Security Aspects of PARLOS |
| Feature or Study Item: Security Assurance Specification for 5G |
| Feature or Study Item: Study on Security Aspects of the 5G Service Based Architecture |
| Feature or Study Item: Study on 5G security enhancement against false base stations |
| Feature or Study Item: Study of KDF negotiation for 5G System Security |
| Feature or Study Item: Study on Long Term Key Update Process (LTKUP) Detailed solutions |
| Feature or Study Item: Study on User Plane Integrity Protection |
| Feature or Study Item: Study on authentication and key management for applications based on 3GPP credential in 5G |
| Feature or Study Item: Study on SECAM and SCAS for 3GPP virtualized network products |
| Feature or Study Item: Study on Security Impacts of Virtualisation |

図 4.8 5G phase 2 (Release 16) に向けた SA3 のワークアイテム（2019 年 3 月時点）

5G のコアネットワークでは、Service Based Architecture (SBA)と呼ばれるバス型のアーキテクチャが採用され、RESTful な API で規定されたコアネットワーク内の各装置の「サービス」を HTTP/2 で呼び出す形で各種の制御が行われる。SBA の導入により、インターネットで一般的に使われるプロトコルや開発用ライブラリ、ミドルウェア等が利用されることになると、それに伴い、関連する脆弱性の影響を受けることが懸念されており、特に、ローミング時の事業者間通信に関するセキュリティ検討が行われている。また、ネットワーク機器のセキュリティ的な安全性をチェックするための仕組みを確立するための取り組みとして、3GPP と GSMA が連携する Network Equipment Security Assurance Scheme (NESAS) の確立が進められており、3GPP では、NESAS で用いる Security Assurance Specification (SCAS) の策定を担当している。

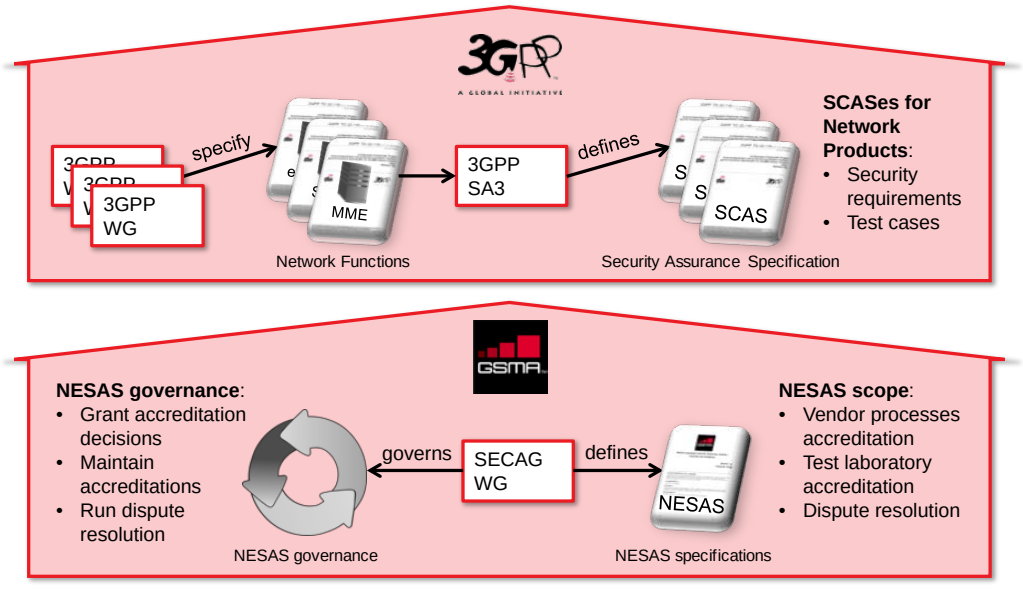



図 4.9 Network Equipment Security Assurance Scheme Overview – GSMA

2020 年 3 月現在、Release 16 に向けた検討はほぼ完了しており、2020 年 1 月からは Release 17 に向けた検討も開始されている。SA3 の Release 17 関連のワークアイテムは以下の 3 件であるが、今後、他のグループから Release 17 に向けた新機能の提案が行われると、それらに対してセキュリティ的観点から検討するワークアイテムが追加されていくものと考えられる。


図 4.10 Release 17 に向けた SA3 のワークアイテム（2020 年 3 月時点）

4.6. 他団体における 5G セキュリティ検討

3GPP 以外の標準化団体や業界団体における 5G セキュリティ関連のアクティビティについて簡単に紹介する。

- ITU-T
  - セキュリティ関連の検討を行っている Study Group 17 において 5G に関連する検討も行われている。各課題（Questions）で取り扱う項目は以下のように規定されており、いくつかの課題で 5G セキュリティに関する勧告作成を他の標準化団体とリエゾンを取りながら進めている。。
    - Q2/17 (Security architecture and framework)
      - SDN/NFV/network slicing security for 5G
    - Q6/17 (Security aspects of telecommunication services, networks and Internet of Things)
      - Mobile and infrastructure aspects for 5G security
    - Q7/17 (Secure application services)
      - Application/service aspects for 5G security
    - Q8/17 (Cloud computing security)
      - Cloud computing and big data infrastructure for 5G security
    - Q11/17 (Generic technologies to support secure applications)
      - Cryptographic profiles for 5G security
    - Q13/17 (Security aspects for ITS)
      - ITS security for 5G
- GSMA
  - 通信機器のセキュリティ認証フレームワークとして NESAS（Network Equipment Security Scheme） を構築している。NESAS は 3GPP の TS33 シリーズで規定される試験仕様（SCAS：Security Assurance Specifications）に基づく機器試験や、第 3 者監査などにより構成される。5G ネットワークのセキュリティ確保に向けて、GSMA は

NESAS を欧州 ネットワーク情報セキュリティ庁(ENISA)に提案中である。これは、欧州委員会の 5G サイバーセキュリティ対策「EU Toolbox」を補完するものであり、現在欧州各国は 5G ネットワークのセキュリティ対策の実装を進めているところである。

- 2018 年 11 月に 5G Security Task Force (5GSTF) が立ち上げられ、実装や運用の観点から標準のギャップを埋めるための議論が行われている。5G セキュリティに関連する承認済みの文書としては以下が発行されている。
  - IR.77 - Inter-operator IP Backbone Security Req. for Service and Inter-operator IP Backbone Providers (メンバー外非公開)
  - NG.113 - 5G Roaming Guidelines
  - NG.116 - Generic Network Slice Template

  また、5GSTF 内でまとめられた 5G セキュリティに関する調査資料の一部を Securing the 5G Era と題した入門文書として GSMA の Web 上で公開している

- NGMN
  - 5G セキュリティに関するレポートを 3 本発行
    - 5G Security Recommendations Package #1: Äccess Network / DoS
    - 5G Security Recommendations Package #2: Network Slicing
    - 5G Security – Package 3: Mobile Edge Computing / Low Latency / Consistent User Experience
  - 2017 年 5 月に Security Competence Team (SCT) を結成
    - 5G E2E Architecture Framework – Security requirements
    - Cellular V2X – Security and privacy aspects
    - Network Capabilities Exposure – Security aspects and requirements
    - 5G RAN Functional Decomposition – Security of new interfaces
    - Pre-commercial 5G Network Trials & Testing – Security Tests

### 4.7. 5G セキュリティ標準化動向まとめ

5G は、IMSI（SUPI）保護、U-Plane の改ざん検知、Home Control の強化、SEPP の導入、DU-CU 分離等の様々なセキュリティ強化により、LTE よりも安全なネットワークになるよう標準化の議論が進められている。一方で、SBA、仮想化、ネットワークスライスなど、5G で導入される新たな仕組みに起因するセキュリティ脅威についての懸念は存在し、これらについては、3GPP だけでなく、GSMA 等の業界団体における、実装や運用者視点での議論についても注視していく必要がある。また、2020 年 3 月にフリーズ予定の Release 16 の仕様検討の中では、バーティカル／LAN や V2X 関連のセキュリティに関する技術レポートの作成も行われており(*)、5G セキュリティ調査検討委員会の検討対象となっているユースケースと関連する部分については、引き続き 3GPP SA3 の議論をフォローしながら各々の SWG での検討を行う必要があると考えられる。

(*) https://www.3gpp.org/DynaReport/TSG-WG--S3.htm

# 5. 5G セキュリティの検討

5G セキュリティ全般から 3 つのユースケース(IoT, Connected Vehicle ,Fintech)を検討対象とした調査、検討過程及びユースケース毎の検討範囲の検討結果をまとめた。

## 5.1. ユースケース IoT セキュリティ

5GMF における課題を検討するに当たっては、2018 年 10 月に説明した文書[1]に基づき、国内外の各種団体が発行している IoT セキュリティ関連文書の記載内容を精査し、文書中で記述されている課題項目の中から 5G がセキュリティ改善のために貢献できそうな課題、ならびに、現状の 5G では直ちに貢献はできないものの、5G 仕様策定も含めた将来的方向性として貢献できる可能性のある課題を抽出することとした。

### 5.1.1. 用語

(1) エンドポイント(EP) エンドポイントは接続されたネットワークを介して双方向通信を行なう遠隔計算機器のことであり、例としてはデスクトップ/ノート PC、スマートフォン、タブレット、サーバ、ワークステーション等がある。

(2) ピア 「同等の者」を意味する語であり、クライアント-サーバ・モデルのような非対称関係ではなくすべてのエンドポイントが対等な関係にあるネットワーク・モデルにおける端末を指す

### 5.1.2. IoT セキュリティ関連文書概説

まず、使用した IoT セキュリティ関連文書に関する概要を記述する。

#### 5.1.2.1 IoT セキュリティガイドライン[2]

経産省/総務省/IoT 推進コンソーシアム(IOTAC)によって 2016 年 7 月に発行された文書であり、IoT 特有の性質と IoT でのセキュリティ対策の必要性を踏まえて、IoT 機器やシステム、サービスについて、セキュリティ・バイ・デザインを基本原則としつつ、セキュリティ確保等の観点から求められる基本的な取組を明確化するためのガイドライン。

方針 / 分析 / 設計 / 構築・接続 / 運用・保守の 5 つの指針と一般利用者ルールとから構成されている。

#### 5.1.2.2 安全な IoT システムのためのセキュリティに関する一般的枠組[3]

内閣サイバーセキュリティセンターによって 2016 年 8 月に発行された文書。IoT セキュリティの考え方を全ての IoT システムに関わる一般要求事項と個々の分野の特性を踏まえた分野固有の要求事項の 2 段階とし、一般要求事項について前者についてのセキュリティ要件の基本的要素をセキュリティ・バイ・デザインに基いて明らかにしたもの。

#### 5.1.2.3 IoT セキュリティ総合対策[4]

総務省によって 2017 年 10 月に発行された文書であり、[3]で示された枠組に基づき、脆弱性対策、研究開発、民間での対策促進、人材育成、国際連携の 5 項目について国の具体的施策を示したもの。

#### 5.1.2.4 サイバー・フィジカル・セキュリティ対策フレームワーク(案)[5]

経済産業省によって 2018 年 4 月に発行された文書であり、IoT や AI によって実現される

「Society5.0」、「Connected Industries」に必要なセキュリティの確保に向けて、産業に求められる対策の全体像を整理したもの。

CPS に必要な対策要件／対策例を米国国立標準技術研究所発行の NIST Cybersecurity Frameworks と対応付けた形で定義している。

5.1.2.5 IoT 開発におけるセキュリティ設計の手引き[6]

情報処理推進機構 (IPA)が 2016 年 5 月に発行し 2018 年 4 月に改訂が行なわれた文書。IoT 開発のセキュリティ設計において行う、脅威分析・対策検討・脆弱性への対応方法を解説する、IoT システムのセキュリティ設計を担当する開発者に向けた手引きとなっている。

5.1.2.6 IoT セキュリティ評価検証ガイドライン[7]

重要生活機器連携セキュリティ協議会(CCDS)によって 2017 年 6 月に発行された文書。スマートホームシステムに対するセキュリティ評価検証を元に、IoT セキュリティガイドライン等の評価検証項目における具体的なプロセスを示しており、IoT 機器全般を対象に具体的なセキュリティの評価検証プロセスが記述されている。

5.1.2.7 IoT セキュリティガイド 標準／ガイドライン ハンドブック[8]

日本ネットワークセキュリティ協会(JNSA)によって 2018 年 5 月に発行された文書。国内外の関連団体が公開している IoT セキュリティ指針／標準／規格等の文書に関して解説を行なったもの。

5.1.2.8 IoT セキュリティチェックシート[9]

企業が IoT を導入する際の、利用側としてのセキュリティ面の検討項目を、 IoT セキュリティガイドラインを参考にチェックシートとして整理したもの。

5.1.2.9 Draft NISTIR 8200[10]

米国国立標準技術研究所(NIST)によって 2018 年 2 月に発行された文書。IoT 向け国際的サイバーセキュリティの標準化状況に関する米政府機関間報告書であり、既存／制定中の各種標準文書と IoT の実状との照合に基づくギャップを明確化することが目的である。

11 のサイバーセキュリティコア領域について説明し、関連する標準の例を示すとともに、IoT の一般的なアプリケーションと IoT の 5 つのアプリケーションのそれぞれの分野について、IoT サイバーセキュリティの目的、リスク、及び脅威を分析している。

5.1.2.10 Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures[11]

欧州ネットワーク･情報セキュリティ機関(ENISA) によって 2017 年 11 月に公開された文書。欧州で運用される IoT 向けセキュリティベースライン設定を目指した文書であり、パラダイム／脅威＆リスク分析／対策＆良実践／ギャップ分析／高水準推奨事項を提示している。

5.1.2.11 Security Guidance for Early Adopters of the Internet of Things[12]

クラウド・コンピューティングのセキュリティを実現するための最良実践推奨のための国際的活動を展開する非営利法人である Cloud Security Alliance (CSA)によって 2016 年 2 月に公開された文書。IoT 早期採用者向けに作成されたセキュリティ・ガイダンスであり、目的／個人・組織への IoT 脅威／セキュアな IoT 配備へのチャレンジ／推奨されるセキュリティ制御／将来的努力事項を提示している。

5.1.2.12 OWASP IoT Top 10[13]

ウェブ・アプリケーション・セキュリティに関する無償の技術文書策定を目的としたオンライン・コミュニケーションである The Open Web Application Security Project (OWASP)によって 2014 年に公開され、 2018 年 12 月には改訂版が公開された文書。IoT デバイスで留意すべき 10 個の脆弱性が提示されており、2014 年版では内容の多くが IoT 固有ではなく Web アプリケーションと一致したものであったが、2018 年版では構成が大きく見直されており、より IoT 固有の記述が増加した文書となっている。

5.1.2.13 Technical Specification TS-0003 Security Solutions[14]

M2M 技術および IoT 技術に対する要件、アーキテクチャ等の策定を行なっている国際的組織である OneM2M によって 2018 年 4 月に発行された M2M グローバル標準におけるセキュリティソリューション技術仕様書。OneM2M におけるセキュリティアーキテクチャ、認証、認可、ID 管理やセキュリティフレームワーク、プライバシー保護等の仕様が定義されている

5.1.2.14 IoT Security Guidelines[15]

世界 200 ヶ国以上で展開されている移動体通信事業者および関連企業からなる業界団体である GSM アソシエーションによって 2017 年 10 月に発行された文書。同団体が提言する IoT セキュリティガイドラインであり、概要、サービス、エンドポイント、ネットワークの 4 書からなっている。IoT システムの可用性、ID、プライバシーとセキュリティの各課題に対し、モバイルネットワークが解決に寄与する事が提言されている。

### 5.1.3. 課題の抽出

5.1.1 節で列挙した日本国内/国外の各種組織から発行された IoT セキュリティ関連文書には、それぞれの文書の作成目的を反映して記述レベルに相違が見られる。たとえば[3]は安全な IoT システムが具備すべき一般要求事項としてのセキュリティ要件基本要素を明らかにするという大所高所の立場からの記述を行なっているのに対して、[14]では OneM2M という IoT の構成要素の一つである M2M システムを提供するための具体的なシステム実装である OneM2M におけるセキュリティ・ソリューションを定義した実装に大きく依存する記述となっている。

5GMF セキュリティ検討アドホックでは 5G との連携が必要な IoT を中心として検討課題を探るという方針が[16]で示されている。したがって 5.1.1 節記載の文書の中では IoT システムのセキュリティ課題に対してモバイルネットワークを用いた解決を探るというスタンスで記載された GSM アソシエーション発行の IoT Security Guidelines [15]が最も親和性が高いと考えられる。そのため、課題に関しては[15]をベースとして検討を行なうこととし、他文書からの課題については付録で示したとおり[15]の課題へ割り付けを実施した。

5.1.3.1 GSMA IoT Security Guidelines 記載の課題

GSMA IoT Security Guidelines の概要編である GSMA IoT Security Guide CLP11-v2.0 では、IoT セキュリティに対するチャレンジとなる項目を

- 可用性
- 識別・認証

- プライバシ
- セキュリティ

の 4 種類の観点からまとめている。

5.1.3.2 可用性

可用性に対するチャレンジとしては以下が列挙される。

1. 如何にして Low Power Wide Area (LPWA) ネットワーク（たとえば NB-IoT ないし LTE-M）を伝統的なセルラーシステムと同一のレベルのセキュリティで運用することが可能となるのか？
2. IoT エンドポイントがネットワーク境界をまたがって移動する際に、如何にして複数のモバイルオペレーターが同一レベルのネットワークセキュリティを提供できるのか？
3. 如何にしてゲートウェイ・エンドポイントに通信を依拠するキャピラリ・エンドポイントに対してネットワークの信頼をフォワードすることが可能となるのか？
4. 如何にしてセキュアな通信環境を用いることができるように軽量エンドポイントの電力制限を回避できるのか？

5.1.3.3 識別・認証

識別・認証に対するチャレンジとしては以下が列挙される

1. エンドポイントを操作する利用者をエンドポイントのアイデンティティに対して強力に連想付けることは可能なのか？
2. 如何にしてサービスとピアはエンドポイントのアイデンティティを検証することでエンド・ユーザのアイデンティティも検証することができるようになるのか？
3. 如何にしてエンドポイントのセキュリティ技術はピアおよびサービスを安全に認証することができるのか？
4. 悪意あるサービスおよびピアは正規のサービスおよびピアになりすますことは可能なのか？
5. 如何にしてデバイスのアイデンティティをタンパリングもしくは操作から保護することができるのか？
6. 如何にしてエンドポイントおよびネットワークは IoT サービスが当該エンドポイントに対してアクセスすることが許可されていると保証できるのか？

5.1.3.4 プライバシ

プライバシに対するチャレンジとしては以下が列挙される

1. エンドポイントのアイデンティティは認可されていない利用者に披瀝されるのか？
2. ユニークなエンドポイントないし IoT サービスの識別子を利用することでエンド・ユーザもしくはエンドポイントを物理的にモニタリングないしトラッキングできるのか？
3. エンドポイントもしくは IoT サービスから放出されるデータは、物理的なエンド・ユーザの属性（位置、行動、ないし、睡眠中/覚醒中のような状態)を示唆ないし直接的に提示するか？
4. 暗号文に存在するパターンが観察できないほど十分な機密性と完全性を備えた暗号化方式が用いられているか？

5. 製品もしくはサービスは利用者特有の個人識別可能情報（PII）をどのように保存したり取扱ったりしているか？
6. エンド・ユーザは IoT サービスないし製品における PII の保存および利用に関して制御権を保持しているか？
7. データをセキュアにするために用いられるセキュリティ鍵およびセキュリティ・アルゴリズムは新しくすることができるか？

5.1.3.5 セキュリティ

セキュリティに対するチャレンジとしては以下が列挙される。

1. セキュリティ最良実践はプロジェクト開始時から製品およびサービスに対して組み込まれているか？
2. セキュリティ・ライフサイクルがソフトウェアおよび製品開発ライフサイクルに組み込まれているか？
3. サービスと組み込みシステムで動作するアプリケーションに対してアプリケーション・セキュリティが適用されているか？
4. エンドポイントおよびサービス・エコシステムに信頼コンピューティング・ベース（TCB）が実装されているか？
5. 如何にして TCB はアプリケーション･イメージおよびサービスの自己検証を強制するか？
6. エンドポイントないし IoT サービスは構成もしくはアプリケーションに異常があることを検出できるか？
7. 如何にしてエンドポイントで悪意ある振舞が行なわれていることを示す異常の検出が行えるのか？
8. どのように認証とアイデンティティが製品ないしサービスのセキュリティ・プロセスに結び付けられているのか？
9. 危殆化を示す異常が検出された場合のためにどのようなインシデント対応計画が定義されているか？
10. 危殆化が迅速かつ効率的に閉じ込められるためにサービスおよび資源はどのようにセグメント化されているか？
11. どのように危殆化後のサービスおよび資源の再開が達成されるか？
12. 攻撃は発見できるか？
13. 危殆化したシステム・コンポーネントは発見できるか？
14. 如何にして顧客はセキュリティ的懸念を報告できるか？
15. エンドポイントは脆弱性を除去するために更新ないし修正することができるか？

### 5.1.4. 5G における新規セキュリティ機能まとめ

4G-LTE 以前と比較すると 5G には多くの新規セキュリティ機能が導入されている。別章で詳細は述べられているが、課題抽出を補助するため、本節では[17]に即して 5G で導入された新規セキュリティ機能を再度まとめている。

5.1.4.1 プライマリ認証

4G-LTE 以前では UE とモバイル・ネットワークとの間の相互認証は常に AKA（Authentication And Key Agreement）と呼ばれる単一の機構によってのみ行なわれていたが、5G ではこれをカスタマイズ可能としており、従前の AKA を拡張した 5G-AKA に加えて EAP（Extensible Authentication Protocol）の枠組で動作する EAP-AKA'が利用可能となっている。これにより従来は WiFi 等の非 3GPP アクセスを用いる場合に 3GPP アクセスとは異なる別立ての認証メカニズムをサポートする必要があったのが、5G では 3GPP アクセス利用時と非 3GPP アクセス利用時とで同じ認証メカニズムを用いることが可能になっている。

さらにプライベート・ネットワーク等の特別なケースでは EAP-AKA'以外の EAP メソッドを用いた認証メカニズムを用いることも可能とされた。

5.1.4.2 クレデンシャル・ストレージ

AKA で用いられる秘密鍵 K のような高い機微性を持ったクレデンシャルを安全に格納するために従来は UICC が用いられていたが、5G では UICC 以外のセキュアなハードウェア・ストレージ・プラットフォームにクレデンシャルを格納するというオプションも提供可能となった。

5.1.4.3 セカンダリ認証

セカンダリ認証はモバイル・ネットワークに認証された UE に対してモバイル・ネットワーク外に存在するデータ・ネットワークに対する認証を提供する機構である。セカンダリ認証ではモバイル・ネットワーク内の機能が UE に対する Authenticator となってデータ・ネットワークに EAP-AKA'とは別の EAP メソッドによる認証フローを実行することで実現される。

5.1.4.4 オペレータ間セキュリティ

従来のオペレータ間通信を実現するために用いられていた SS7 ないし Diameter に脆弱性が発見されたことを受けて、5G ではオペレータ間通信を安全に実行可能とするための SEPP（Secure Edge Protection Proxy）と呼ばれる新規機能が導入された。

5.1.4.5 プライバシ

4G-LTE 以前ではモバイル・ネットワーク契約者を一意に特定可能な IMSI を平文のままで通信しなければならない機会が存在したため、トラッキング等のプライバシに対する被害を受ける可能性を排除できていなかったのだが、5G では 4G-LTE 以前の IMSI に相当する SUPI (SUbscription Permanent ID)をネットワーク・オペレータの公開鍵によってランダム暗号化した結果である SUCI (SUbscription Concealed ID)を用いることで、プライバシへ配慮することが可能となった。

5.1.4.6 サービス・ベース・アーキテクチャ（SBA）

5G ではコア・ネットワークで用いられる各種サービスに基づいたアーキテクチャを採用することで、十分なセキュリティを導入可能となっている。

5.1.4.7 Central Unit (CU) - Distributed Unit (DU)

5G では安全でない位置に基地局を配備するユースケースも想定されているため、基地局を CU と DU の二つのエンティティとして実現し、機微情報の流通は CU までで留めることで、そのようなユースケースへの対応を可能とせしめている。

5.1.4.8 鍵階層

前項と同様の意味で、5G における鍵階層も従来とは異なる形態となっている。

5.1.4.9 モビリティ

5G においてもモビリティ自体は 4G-LTE と同様なのだが、コア・ネットワークのアンカーが安全ではない場所に置かれる可能性があることから、5G ではアンカー・ポイント間のセキュアなモビリティもプロビジョニングされる必要が生じることとなっている。

5.1.4.10 ネットワーク・スライス

5G ではモバイル・ネットワークに対する要求条件の多様化傾向に対処するために、ネットワークを分割し、分割された個々の部分（スライス）を顧客に対して専有可能とすることで、同一モバイル・ネットワークに存在する他の部分に影響することなしに適切なセキュリティ環境を提供することが可能となっている。

### 5.1.5. 5G セキュリティ機能による課題への対応可能性

本節では 5.1.3 節で紹介した 5G 新規セキュリティ機能を用いることで 5.1.2.1 節で述べた GSMA Security Guidelines が提示した課題に対して対応の可能性がある項を検討していく。5.1.2.1 節でも示した通り、他の文書から抽出された課題についても GSMA Security Guidelines 課題に割り付けを実施したため、関連文書から抽出された課題については網羅されていると考える。

本節で可能性ありと考えられた課題を中心に、今後 5G ネットワークにおける IoT セキュリティの検討を進めていきたい。

5.1.5.1 可用性

1. 如何にして Low Power Wide Area (LPWA) ネットワーク（たとえば NB-IoT ないし LTE-M）を伝統的なセルラ・システムと同一のレベルのセキュリティで運用することが可能となるのか？

   4G までのモバイル・ネットワークでは同一のセキュリティ機能が要請されたが、5G では独立したスライスへの分割が可能となったため、他に影響を与えることなしに LPWA を必要とするようなローエンド・デバイスへの柔軟な対応が可能となる可能性がある。[5.1.3.10]
2. IoT エンドポイントがネットワーク境界をまたがって移動する際に、如何にして複数のモバイル・オペレータが同一レベルのネットワーク・セキュリティを提供できるのか？5G におけるオペレータ間モビリティ関係構築により実現できる可能性がある [5.1.3.4][5.1.3.9]
3. 如何にしてゲートウェイ・エンドポイントに通信を依拠するキャピラリ・エンドポイントに対してネットワークの信頼をフォワードすることが可能となるのか？計算資源の乏しいローエンド･デバイスであっても 5G への直接アクセスを可能となる可能性がある 。[5.1.3.10]

   仮に GW に頼らなければならない EP が今後も残るのであれば、EP⇔GW 間の保護策提供方法も引き続き課題となる。

4. 如何にしてセキュアな通信環境を用いることができるように軽量エンドポイントの電力制限を回避できるのか？

   5G では電力制限がある軽量エンドポイントデバイスについてもネットワーク・スライシングにより対応できる可能性がある。 [5.1.3.10]

5.1.5.2 識別・認証

1. エンドポイントを操作する利用者をエンドポイントのアイデンティティに対して強力に連想付けることは可能なのか？

   エンドポイント利用者＝ネットワーク契約者である場合にはネットワーク内で連想付を行なえる可能性がある。[5.1.3.3]

   ただし特に IoT ではエンドポイント利用者とネットワーク契約者が異なるケースも多いと考えられ、そのようなケースへの対応は引き続き課題となる。
2. 如何にしてサービスとピアはエンドポイントのアイデンティティを検証することでエンド・ユーザのアイデンティティも検証することができるようになるのか？

   1.項に同じ
3. 如何にしてエンドポイントのセキュリティ技術はピアおよびサービスを安全に認証することができるのか？

   5G ではエンドポイントと正規ピア/サービスとの間ではセカンダリ認証による相互認証が活用できる可能性がある。[5.1.3.3]
4. 悪意あるサービスおよびピアは正規のサービスおよびピアになりすますことは可能なのか？

   3.項に同じ
5. 如何にしてデバイスのアイデンティティをタンパリングもしくは操作から保護することができるのか？

   5G ではクレデンシャル・ストレージ機能により UICC 以外のセキュア・ストレージを利用することが可能であり、これを活用できる可能性がある。 [5.1.3.2]
6. 如何にしてエンドポイントおよびネットワークは IoT サービスが当該エンドポイントに対してアクセスすることが許可されていると保証できるのか？

   5G ではモバイル・ネットワーク外に存在する IoT サービスと UE との間でのセカンダリ認証による相互認証を実施することで解決できる可能性がある。[5.1.3.3]

5.1.5.3 プライバシ

1. エンドポイントのアイデンティティは認可されていない利用者に披瀝されるのか？

   5G では契約者識別のために用いられる 4G-LTE における IMSI に相当する SUPI を秘匿するために、オペレータ公開鍵でランダム暗号化した結果である SUCI を常に用いることが可能となったため、モバイル・ネットワーク内でのエンドポイント・アイデンティティ漏洩が回避できる可能性がある。 [5.1.3.5]
2. ユニークなエンドポイントないし IoT サービスの識別子を利用することでエンド・ユーザもしくはエンドポイントを物理的にモニタリングないしトラッキングできるのか？

   1.項に同じ [5.1.3.5]

3. エンドポイントもしくは IoT サービスから放出されるデータは、物理的なエンド・ユーザの属性（位置、行動、ないし、睡眠中/覚醒中のような状態)を示唆ないし直接的に提示するか？

   5G ネットワーク内においては、モバイル・ネットワーク全区間での安全性を考慮された暗号化方式が利用されていることを活用できる可能性がある。

4. 暗号文に存在するパターンが観察できないほど十分な機密性と完全性を備えた暗号化方式が用いられているか？

   5G ネットワーク内においては、安全性を考慮された暗号化方式が利用されていることを活用できる可能性がある。

5. 製品もしくはサービスは利用者特有の個人識別可能情報（PII）をどのように保存したり取扱ったりしているか？

   製品ないしサービスが PII をどのように保存/処理するかに依存するため、5G 課題として検討することは困難と考えられる。

6. エンド・ユーザは IoT サービスないし製品における PII の保存および利用に関して制御権を保持しているか？

   6.項に同じ

7. データをセキュアにするために用いられるセキュリティ鍵およびセキュリティ・アルゴリズムは新しくすることができるか？

   5G フェーズ 2 では長期有効鍵（UICC とコア・ネットワークで共有される K)の更新可能化方式に関して検討予定であり、これを活用できる可能性がある

5.1.5.4 セキュリティ

1. セキュリティ最良実践はプロジェクト開始時から製品およびサービスに対して組み込まれているか？

   サービスにおける本課題は検討範囲外と考えられる。なお、５G コアの機能を提供する各機能要素におけるセキュリティ最良実践に関しては 3 GPP SCAS（Security Assurance Specification）の枠組を用いた取組が行なわれている。

2. セキュリティ・ライフサイクルがソフトウェアおよび製品開発ライフサイクルに組み込まれているか？

   1.項に同じ

3. サービスと組み込みシステムで動作するアプリケーションに対してアプリケーション・セキュリティが適用されているか？

   1.項に同じ。ただし 5G ネットワーク経由でアプリケーション・セキュリティの状態に関する検査機能を提供するという検討はあり、それが適用できる可能性はある

4. エンドポイントおよびサービス・エコシステムに信頼コンピューティング・ベース（TCB）が実装されているか？

   3.項に同じ

5. 如何にして TCB はアプリケーション・イメージおよびサービスの自己検証を強制するか？

   3.項に同じ

6. エンドポイントないし IoT サービスは構成もしくはアプリケーションに異常があることを検出できるか？
   3.項に同じ
7. 如何にしてエンドポイントで悪意ある振舞が行なわれていることを示す異常の検出が行えるのか？
   3.項に同じ
8. どのように認証とアイデンティティが製品ないしサービスのセキュリティ・プロセスに結び付けられているのか？
   1.項に同じ
9. 危殆化を示す異常が検出された場合のためにどのようなインシデント対応計画が定義されているか？
   1.項に同じ
10. 危殆化が迅速かつ効率的に閉じ込められるためにサービスおよび資源はどのようにセグメント化されているか？
    1.項に同じ
11. どのように危殆化後のサービスおよび資源の再開が達成されるか？
    1.項に同じ
12. 攻撃は発見できるか？
    1.項に同じ
13. 危殆化したシステム・コンポーネントは発見できるか？
    1.項に同じ
14. 如何にして顧客はセキュリティ的懸念を報告できるか？
    1.項に同じ
15. エンドポイントは脆弱性を除去するために更新ないし修正することができるか？
    1.項に同じ

### 5.1.6　IoT 課題に対する具体的対策案検討結果

本章では前章までで特定された IoT 課題に対する具体的な対策案をまとめる。

#### 5.1.6.1. 可用性 1：LPWA ネットワークの安全な配備・運用

課題: 如何にして Low Power Wide Area (LPWA) ネットワーク（たとえば NB-IoT ないし LTE-M）を伝統的なセルラーシステムと同一のレベルのセキュリティで運用することが可能となるのか？

省電力広域ネットワークである LPWA (Low Power Wide Area) 実現のためには、Km 単位の広域を低消費電力でカバー可能な無線通信技術が必要となる。そのような LPWA を配備・運用するための要件としては、バッテリーにより 15 年間駆動可能な機器を収容可能な通信環境を提供するというものが挙げられており、省電力に対する強い要請が存在している。そのような要請の下でネットワーク・セキュリティを実現するためには、軽量暗号などの低電力消費アルゴリズム

の使用といったことも必要となってくるだろう。しかしながら、4G までは UE とコア・ネットワーク間での通信保護は常に同一の暗号アルゴリズムが用いられていたため、IoT で必要とされる省電力を提供することは難しかった。


図 5.1.1 5G における既定 4 スライス達成目標値[18], [19]

5.1.6.1.1. 5G による対策

5G ではネットワーク・スライシングが導入されており、ネットワークを仮想的独立したスライスに分割し、個々のスライスでは他スライスに悪影響を与えることなく利用アルゴリズムを変更することが可能となっている。たとえば 5G における既存のユースケースとしては

1. eMBB
2. URLLC
3. mMTC
4. V2X

の 4 種類が存在しており(図 5.1.1)、この中では mMTC が LPWA 向けに事前定義されたスライス設定ということになる。

5.1.6.1.2. IoT プラットフォーム運用者要考慮事項

IoT プラットフォームを運用する事業者にとって本項目のために必要となるのは、同事業者が提供している応用に適したスライス設定が存在すること、もしくは事業者によって適切に設定可能となっていることの確認である。

5.1.6.2. 可用性 2：複数オペレータ間ローミング・セキュリティ

課題: IoT エンドポイントがネットワーク境界をまたがって移動する際に、如何にして複数のモバイルオペレーターが同一レベルのネットワークセキュリティを提供できるのか？

4G 以前でオペレータ間ローミング実施時に利用されていた Diameter プロトコルに契約者情報を漏洩するなどの脆弱性が存在することが 2018 年に発覚している[20]。具体的な脆弱性としては

- 契約者情報漏洩
- ネットワーク情報漏洩
- 詐欺
- 契約者 DoS

などの被害発生の可能性が存在した。

5.1.6.2.1. 5G による対策

5G では上述した脆弱性対策として SEPP (Secure Edge Protection Proxy）と呼ばれる新規ネットワーク機能が導入された。SEPP は各オペレータ・ネットワークのエッジに配備され、以下のような機能が提供されるようになった。

- 異なるオペレータ間で交換されるシグナリング・トラフィックの機密性・完全性保護
- トポロジー隠蔽
- FireWall ベースのフィルタリング機能

さらに、5G ではプライマリ認証で 3GPP アクセスと WiFi 等の非 3GPP アクセスのいずれにおいても 5G-AKA/EAP-AKA'によりホーム・オペレータが常に認証可能な環境が確立されたため、ローミング・シナリオでの詐欺を防止することが可能になったというメリットも生じている。

5.1.6.2.2. IoT プラットフォーム運用者要考慮事項

本項は 3GPP オペレータ間での動作に閉じているため、IoT プラットフォーム運用事業者にとって必要な事項は存在しない。

5.1.6.3. 可用性３：キャピラリ・エンドポイントへの信頼フォワード

課題: 如何にしてゲートウェイ・エンドポイントに通信を依拠するキャピラリ・エンドポイントに対してネットワークの信頼をフォワードすることが可能となるのか？

ここで言う『キャピラリ・エンドポイント』とはクラウドとの通信を直接実行することができず、ゲートウェー等による媒介を必要とする機器のことである。そのような構成を取る場合、クラウドのネットワークで確立されている信頼をゲートウェーの先に存在するキャピラリ・エンドポイントまで波及させるためのソリューションを提供する必要がある。

5G では低性能/省電力エンドポイントであっても前出の LPWA ネットワーク等を経由して機器自身が直接クラウドにアクセスできるという構成を想定しているため、基本的にはそのような状況に至らずに済むことが期待されている。

ただし、ゲートウェーを必要とするシナリオが低性能/省電力以外に実在するのであれば、キャ

ピラリ・エンドポイントに信頼を波及させるためのソリューションが必要となる可能性は残される。

5.1.6.3.1. IoT プラットフォーム運用者要考慮事項

ターゲットとする応用がゲートウェーを必要とするシナリオである場合にネットワーク側で確立された信頼をゲートウェーの先へ波及させるためのソリューションの策定が必要となる。

5.1.6.4. 可用性４：セキュアな通信環境における軽量エンドポイントの電力制約対策

課題：如何にしてセキュアな通信環境を用いることができるように軽量エンドポイントの電力制限を回避できるのか？

5.1.6.4.1. 3GPP における 5G 一般機能検討中の軽量エンドポイント向け電力制約対策

3GPP では 5G における CIoT サポートに関する主要問題と可能なソリューション検討作業を実施しており[21]、その中で電力制約解決に関する以下の現行主要問題が定義されている。

- 5.4 Key Issue 4: Power Saving Functions
- 5.5 Key Issue 5: UE TX Power Saving Functions

そして、これらに対するソリューションとしては以下が検討されている。

- Solution 8: Enhancing MICO for Mobile terminated data/signaling
- Solution 9: Enhanced MICO mode with Active Time
- Solution 22: eDRX for CM-IDLE state in 5GS
- Solution 23: MICO Mode Management for Expected Application Behaviour
- Solution 32: MO Data Buffering in the UE
- Solution 33: Delayed Paging Response
- Solution 34: Provisioning of UE TX power saving parameters
- Solution 38: eDRX RRC_INACTIVE STATE in 5GS
- Solution 41: Combining RRC-INACTIVE and 5G UP optimization

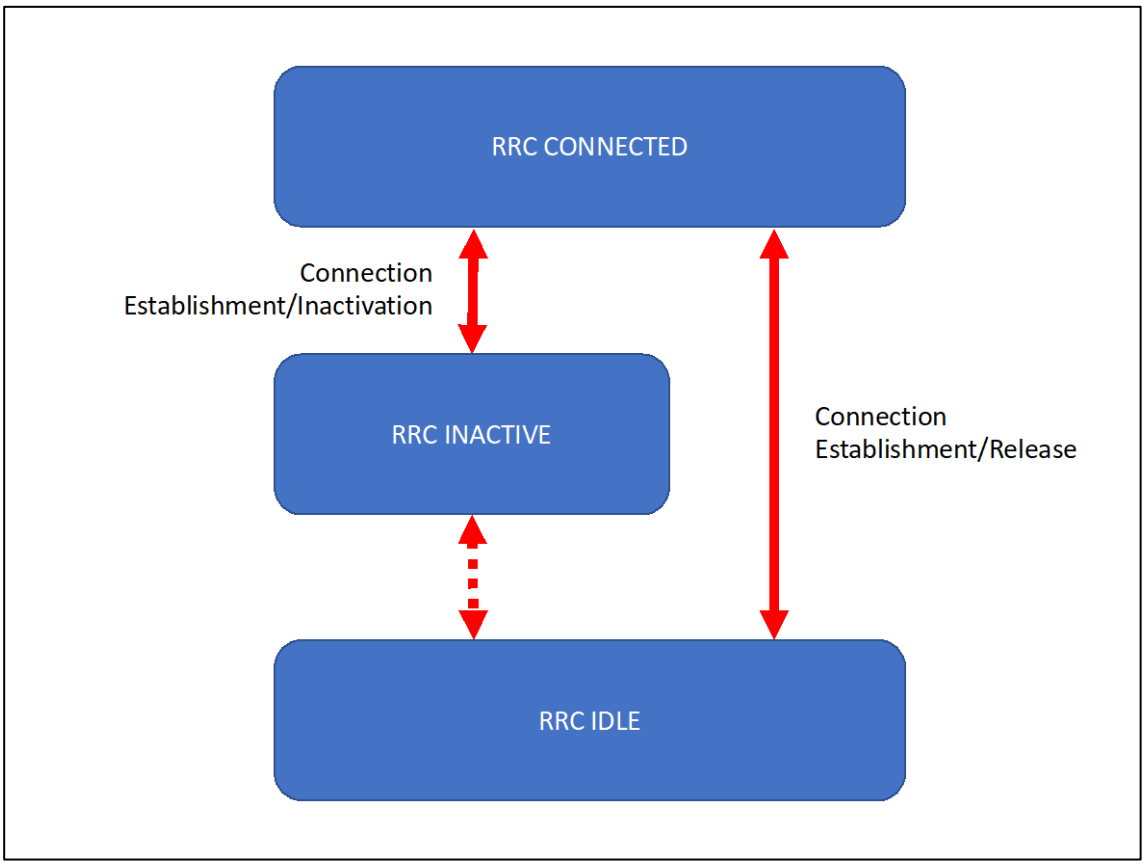



図 5.1.2 5G NR RRC 状態遷移図

また、5G では 4G までの RRC IDLE 状態と RRC CONNECTED 状態に加えて RRC INACTIVE 状態が新規に定義されている(図 5.1.2)。RRC INACTIVE 状態では UE と基地局/CN では RRC および NAS のコンテキストを保持しながら UE 内部状態としてはほぼ RRC_IDLE 同様の省電力状態が維持できるように図られている。

5G におけるセキュリティ関連検討を担当する 3GPP SA3 では上述した 5G 一般機能を実現するためのセキュリティ・ソリューションとして以下の仕様を定義している。

1. RRC_INACTIVE⇔RRC_CONNECTED 遷移時のセキュリティ手続（TS33.501 6.8.2.1 節）
   - INACTIVE 遷移時の SC 保存手続と CONNECTED 遷移時の SC 回復方法
     - 遷移時の gNB: 同/異ケース
2. RRC_INACTIVE 中モビリティ時の鍵処理（TS33.501 6.8.2.2 節）
   - 構成済 RNA (RAN based Notification Area)離脱時等の UE によるネットワークへの通知を実現

5.1.6.4.2. IoT プラットフォーム運用者要考慮事項

本節で解説した電力制約解決対策の基本的な処理は gNB/ng-eNB⇔通信プロセッサ間でなされると期待されるが、以下の UE 動作実現のためにアプリケーション・プロセッサ（AP）による補助が必要となる可能性はあるかもしれないため、AP の仕様を確認した上で対処が必要となる。

RRC CONNECTED⇒RRC INACTIVE 遷移は gNB/ng-eNB 主導で実施されるので、UE では遷移指示に従って 33.501 6.8.2.1.2 節に従って RRC INACTIVE への状態遷移処理を実施

- RRC INACTIVE 状態から RRC CONNECTED 状態に遷移する場合、UE は 33.501 6.8.2.1.3 節に従った状態遷移処理を実施

5.1.6.5. 識別・認証 1： EP 操作ユーザと当該 EP アイデンティティとの強力な連想付可能？

課題：エンドポイントを操作する利用者をエンドポイントのアイデンティティに対して強力に連想付けることは可能なのか

エンドポイント操作ユーザが同エンドポイントへのサービス提供 MNO 契約者であり、かつ、自身のスマートフォンを介してエンドポイントの操作を行なうというユースケースであれば、当該 MNO が管理する DB（5G コアにおける UDR 機能）を活用することで連想付を行なうことが可能である。

それ以外のケースでは現行の 5G コアでは提供されていないなんらかのソリューションの利用が必要となる。

5.1.6.5.1. ソリューション例：セカンダリ認証の利用

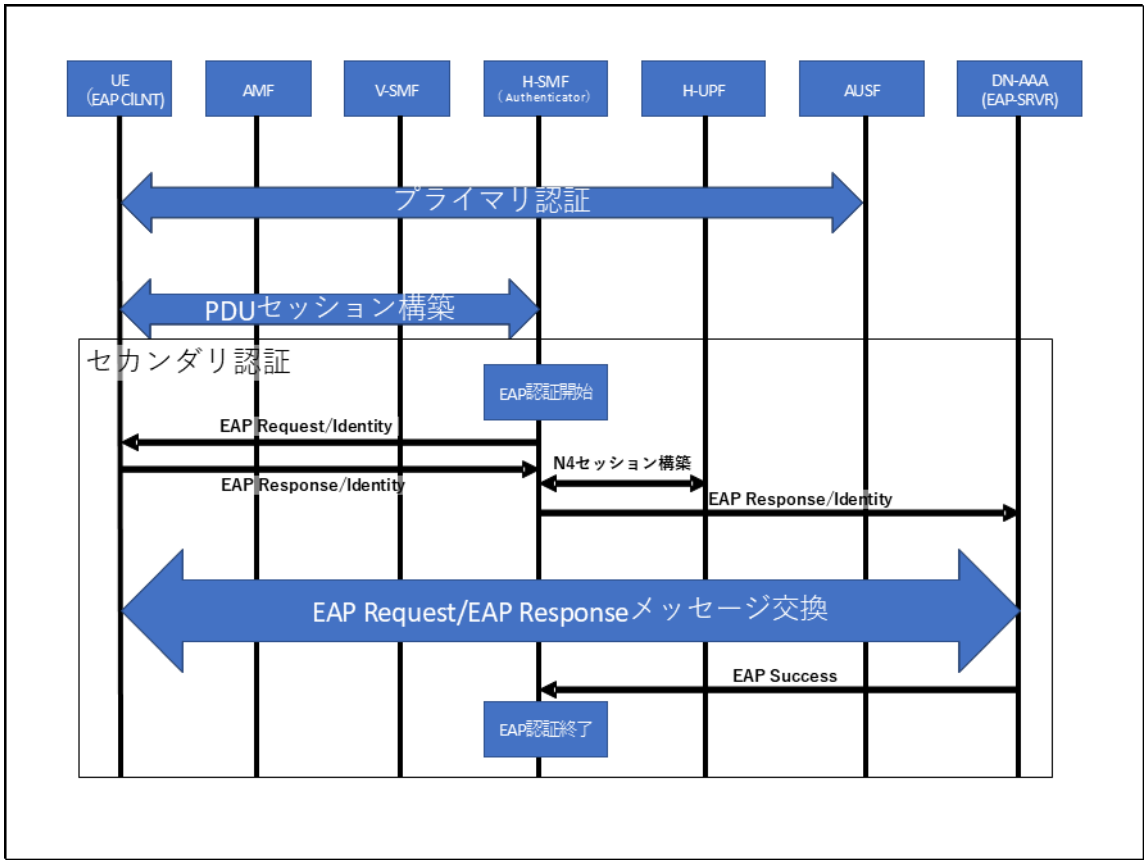



図 5.1.3 5G セカンダリ認証概略

5G セカンダリ認証は、通常の UE⇔5GC 間を認証するためのプライマリ認証が成功した後に、UE と DN が運用する AAA サーバとの間での認証を実現可能とするための機能である。

エンドポイントが同機能を利用することにより、EP と DN AAA 間で任意の EAP 認証が実行可能であるため、当該 EAP 認証処理中にエンドポイント操作ユーザに対して適切な認証クレデンシャルの提示を求めることで、ユーザとエンドポイントとを強力に連想付けることが可能となる。

5.1.6.5.2. IoT プラットフォーム運用者要考慮事項

IoT プラットフォーム運用者が 5.1.6.5.1 節に述べたようなソリューションを運用する場合、以下のような考慮が必要である。

- エンドポイント操作ユーザ認証方式決定
- 実装 EAP 方式決定

5.1.6.6. 識別・認証 2 ：エンドポイントのセキュリティ技術による、ピアとサービスの安全な認証は可能か

課題：エンドポイントのセキュリティ技術はピアおよびサービスを安全に認証することができるのか

ここで言うようなエンドポイントのセキュリティ技術によるピア/サービスの安全な認証を扱う場合、それらのエンドポイントがどのような形態でピア/サービスと通信するのかということを考慮しなければならない。

IoT において一般的に用いられる形態は以下の 2 種類に大別できる（図 5.1.4）。

1. サーバ経由間接通信
   - EP 間の通信は一旦中継サーバを経由した上で目的 EP へ届けられる
2. ローカル NW 経由直接通信
   - EP 間の通信は WiFi / Bluetooth / Zigbee 等のローカル NW を介して直接実施される

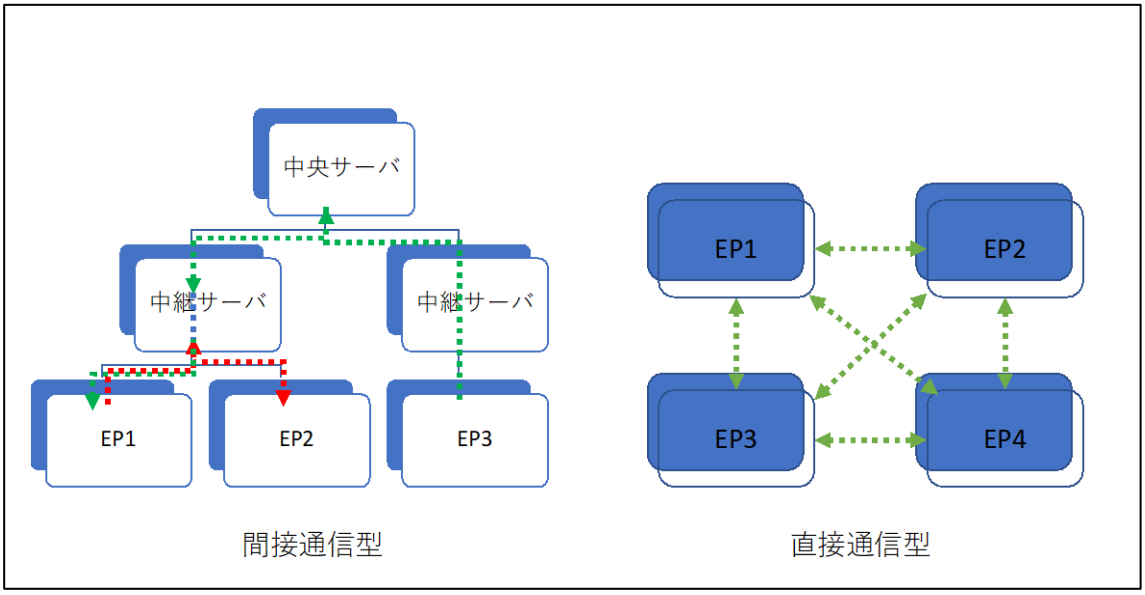



図 5.1.1 典型的エンドポイント間通信形態

1.の中継サーバ経由間接通信を採用した IoT 規格の代表例は OneM2M[22]である。また、AWS や Azure 等のクラウド・サービス・プロバイダが提供する IoT サービスもクラウド上のサービスを介してエンドポイント間通信を実現する方式を基本としている。

2.の直接通信型サービスを採用した IoT 規格の代表例は IETF ACE[23]である。また、米 Alphabet 傘下の Nest Labs が開発した規格である Weave[24]では主として直接通信型でのエンドポイント間通信がサポートされている。

エンドポイントとピア/サービスとの間での安全な認証を実現するための仕組として、5G が提供しているセカンダリ認証と AKMA という 2 つの方式が利用可能と考えられる。

5.1.6.6.1. セカンダリ認証

セカンダリ認証を用いることで、図 5.1.3 に示されている通りエンドポイントである UE とクラウド上の DN (データ・ネットワーク)上に存在する AAA サーバとの間での任意の EAP 機構を用いた安全な認証を実現することが可能である。

さらに、OneM2M のようなサーバ経由間接通信型の IoT プラットフォームでは、当該 AAA サーバが中央サーバないし中継サーバに対する PEP / PDP の役割を果たすことで、サービスに対するアクセス制御ポリシに基づく安全なアクセス可否判断を一元管理することが可能となる。

5.1.6.6.2. AKMA

AKMA (Authentication and Key Management for Application Functions)は、4G 以前から存在する GBA (Generic Bootstrapping Architecture)の 5G 向け拡張として 3GPP SA3 によって標準化作業が行われている機能である。

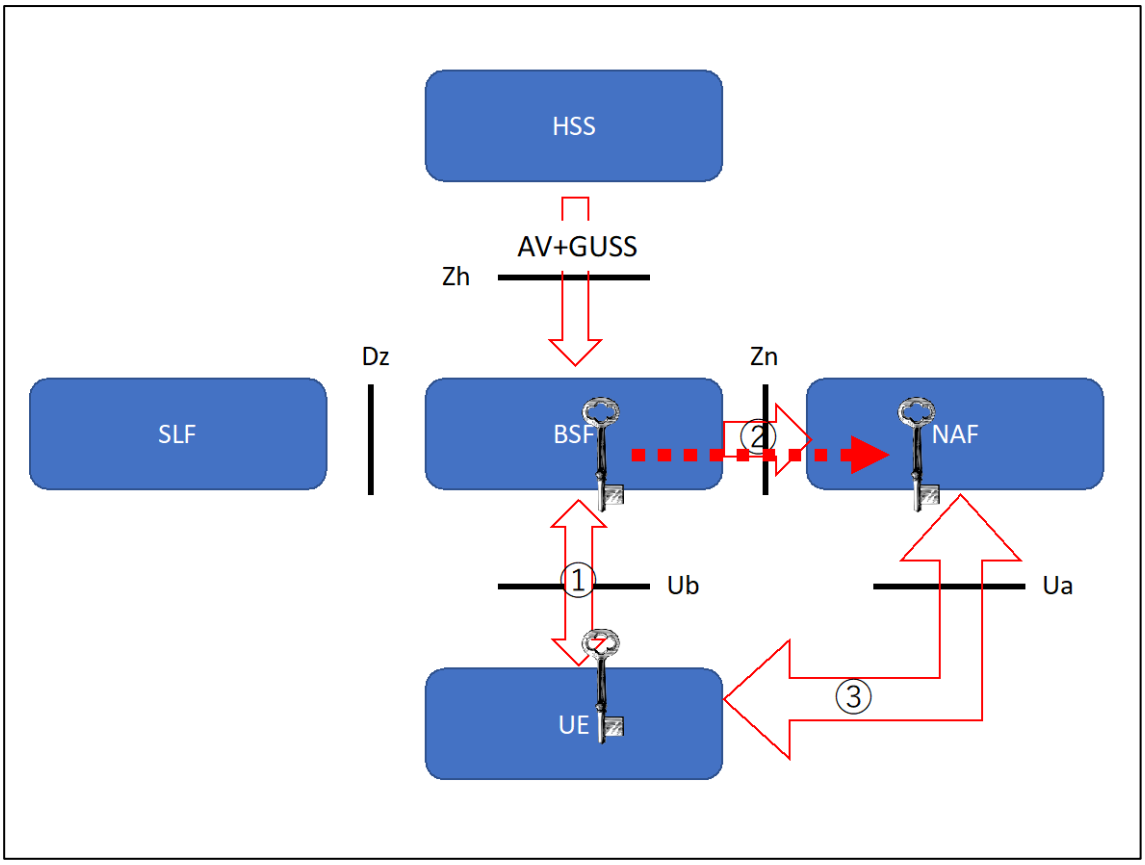



図 5.1.2 GBA における UE⇔NAF 間鍵共有方式概要

4G 以前における AKMA 同等品である GBA における UE と NAF (Network Access Function)との間での秘密鍵共有手法を図 5.1.5 に示した。UE は BSF (BootStrapping Function)との間で 4G AKA に基づく認証を行なうことで新たな共有鍵を生成し、NAF は BSF からその新たに生成された共有鍵の提供を受けることで UE と NAF との間での鍵共有に成功する。

5G では図示された HSS や BSF 等の役割を果たす 5G コア部分の機能が 4G からは大幅に変更されているため、図 5.1.5 とは異なるアーキテクチャとなる可能性があるものの、同等の機能が

AKMA として提供される予定であるため、同機能を用いることでエンドポイントとピア/サービスとの間での安全な認証が実現できる。サービス側では中央サーバによる中央集権的機能を持たない直接通信型の IoT　　プラットフォームに適した形態である。

セカンダリ認証では DN 上の AAA サービスが PEP/PDP の役割を果たすことで認証とアクセス管理とを同時に実現することができたが、AKMA では図 5.1.5 に示された GUSS (GBA User Security Setting) を利用して NAF への共有鍵提供可否を BSF が判断することでアクセス管理を実現することが可能である。

5.1.6.6.3. IoT プラットフォーム運用者要考慮事項

IoT プラットフォーム運用者が提供する IoT プラットフォームにおけるエンドポイント間通信形態に適したエンドポイント ⇔ピア/サービス間認証方式の実装検討が必要である。

5.1.6.7. 識別・認証３：デバイス・アイデンティティ解析/操作に対する防止方法

課題：デバイスのアイデンティティをタンパリングもしくは操作から保護することができるのか

IoT デバイスは物理的な保護が提供できない誰からでもアクセスできる開かれた場所に設置されることも想定されているため、そのようなデバイスに対しては分解等の物理的な手段で解析/操作が実施される可能性を否定できない。

GSM 以来の流れを受けた 3G、4G では携帯電話のネットワーク接続時認証に用いる秘密鍵 K を耐タンパ性を備える IC カードに格納することでそのような物理的攻撃に対する耐性を実現していた。それを 5G では物理的攻撃への耐性を備えたストレージとして一般化したセキュア・ストレージという概念を導入している。

セキュア・ストレージは 5G セキュリティを定義した TS 33.501 5.2.4 節によって以下のような 5G ネットワーク・アクセスに利用する契約クレデンシャルの保存および処理に対する要件としてまとめられている。

- 契約クレデンシャルは耐タンパ・セキュア HW コンポーネントにより完全性保護
- 契約クレデンシャル中の長期有効鍵(K)は耐タンパ・セキュア HW コンポーネントにより機密性保護
- 契約クレデンシャル中の長期有効鍵は耐タンパ・セキュア HW コンポーネント外に平文で持ち出せないこと
- 契約クレデンシャルを利用する認証アルゴリズムは耐タンパ・セキュア HW コンポーネント内でのみ実行

5.1.6.7.1. IoT プラットフォーム運用者要考慮事項

IoT プラットフォーム運用者が提供する IoT デバイスに関しても、独自のクレデンシャル情報の下で機器の管理・運用を行なう場合、5G と同様の物理的攻撃耐性を備えるストレージにて管理することが望ましい。そのようなストレージ実装方式としては以下の二つが選定候補となるだろう。

1. SoC 提供機能利用
    - Cortex-M TrustZone 等

2. 独立暗号認証デバイス利用
   - スマートカード
   - ATECC508/608 等

5.1.6.8. プライバシ１：EP のアイデンティティは非認証ユーザに対して披歴されるか？

課題：エンドポイントのアイデンティティは認可されていない利用者に披瀝されるのか

4G 以前では永続識別子によるトラッキング防止のため、基本的に IMSI の替わりとなるランダム値 TMSI (Temporary Mobile Subscriber Identity) が用いられるように配慮されているが、一定の条件下で IMSI を平文で送信する場面が存在していたため、エンドポイントのアイデンティティを披瀝する可能性が残されていた。

5G では SUPI を平文では送信せず、常にホームネットワーク公開鍵でランダム暗号化した形(SUCI (Subscription Concealed Identifier)) でのみ送信する形での運用が可能となったため、5G レベルでのエンドポイントのアイデンティティが非認証ユーザに対して披瀝されない形での運用が実現できるように改善されている。

5.1.6.8.1. IoT プラットフォーム運用者要考慮事項

IoT プラットフォームにつながるエンドポイントやサービス等に 5G とは異なる独自アイデンティティの割当/利用を行なう場合、本課題解決のためには 5G が実施しているものと同様の配慮を IoT プラットフォーム運用者が考慮することが必要となる。

1. アイデンティティの送信は常に TLS 等の安全な暗号通信下でのみ実施
2. アイデンティティの平文での通信が必要な場合には上記した 5G 方式同等の保護策を適用

5.1.6.9. プライバシ２：EP ないし IoT サービスから放出されるデータを位置情報等のエンド・ユーザ属性に連想付けることは可能か？

課題 : エンドポイントもしくは IoT サービスから放出されるデータは、物理的なエンド・ユーザの属性 (位置、行動、ないし、睡眠中/覚醒中のような状態)を示唆ないし直接的に提示するか

ネットワーク全区間でデータに対する安全な機密性/完全性保護が適用されていることを保証することによりこのような状況の防止は実現可能である。5G における機密性/完全性保護アルゴリズムは以下のように定義されている。

- 機密性保護
  1. NEA0
     - 非暗号化 (鍵ストリーム≡0 と平文との XOR 演算)
  2. 128-NEA1
     - Lund University の T. Johansson と P.Ekdahl により考案されたストリーム暗号 SNOW 3G
  3. 128-NEA2
     - CTR モード 128bit AES
  4. 128-NEA3

- 16 ステージ LFSR ( Linear Feedback Shift Register) 構成ストリーム暗号 ZUC

- 完全性保護

1. NIA0
   - 非完全性保護（メッセージ≡0 に対して 32bit MAC を生成）
2. 128-NIA1
   - SNOW 3G により 32bit MAC を生成
3. 128-NIA2
   - CMAC モード 128bit により 32bit MAC を生成
4. 128-NIA3
   - ZUC により 32bit MAC を生成

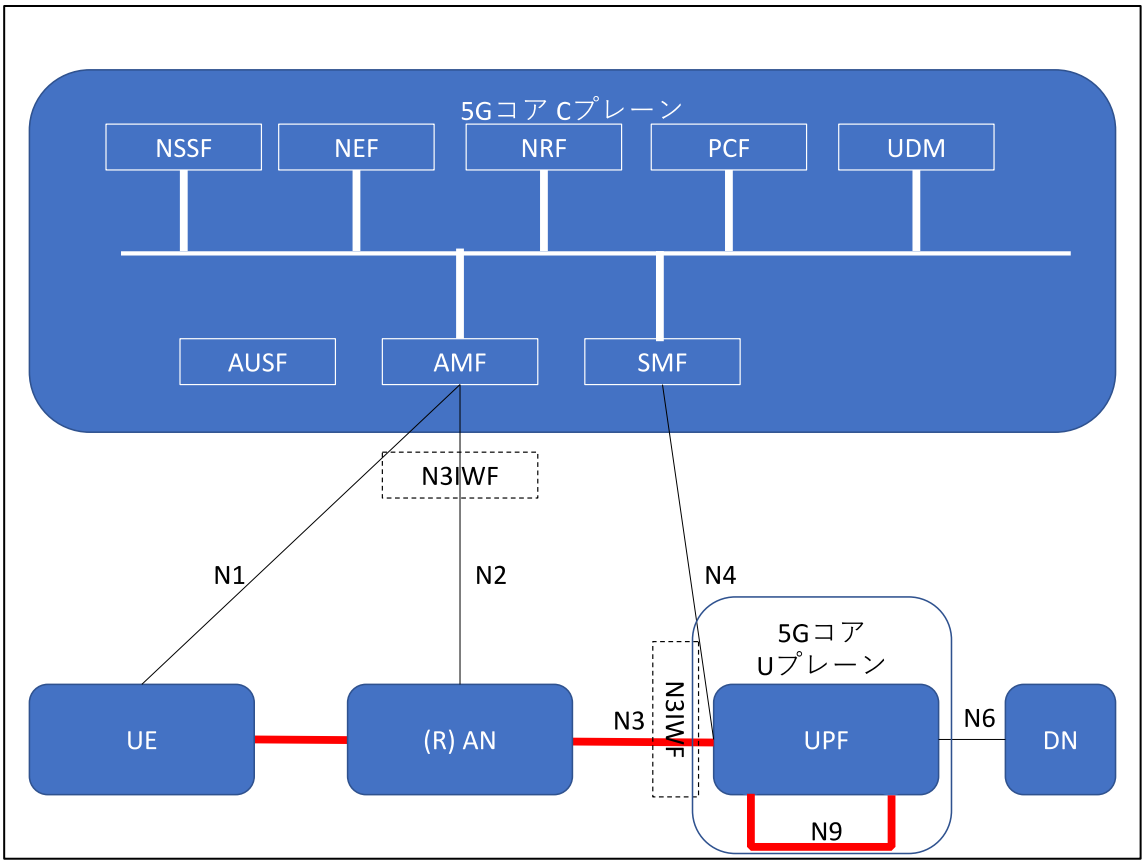



図 5.1.3 5G コア概念図

本課題を解決するためには機密性/完全性ともにオプション 2.以上のアルゴリズムを用いなければならない。なお、これらの保護が適用されるのは 5G 内部のみであるため、ユーザ・プレーンの通信は UE から UPF までしか保護されない点に注意が必要である(図 5.1.6)。

5.1.6.9.1. IoT プラットフォーム運用者要考慮事項

前節で説明したように、UPF から N6 IF を介して接続される外部データ・ネットワーク(DN)との間の通信には IoT プラットフォーム運用者によって別途保護が講じられる必要がある。そのような保護を与える実現オプションとして以下を例示する。

- UE⇔DN 間での E2E セキュア・セッション構築
  - IPsec, TLS 等による

- 5G 提供保護機能は無用に
- 同上 /w 5G 補助
  - セカンダリ認証 or AKMA で UE⇔DN が共有する共通鍵ベース IKE or TLS HS
- UPF⇔DN 間通信保護
  - UPF⇔DN 間にセキュア・セッションを構築
    - SSH Port Forwarding 等
- UPF&DN を物理的に近接配備
  - エッジ・コンピューティング的方向性

5.1.6.10. プライバシ３:暗号文からなんらかのパターンが観察できないことが保証できるように十分安全な形で機密性/完全性保護が適用されているか？

課題：暗号文に存在するパターンが観察できないほど十分な機密性と完全性を備えた暗号化方式が用いられているか

5.1.6.9 節で説明した 5G ネットワークで定義されている 2.～4.の機密性保護アルゴリズムないしその同等品をネットワーク全体で提供することで解決可能。

5.1.6.10.1. IoT プラットフォーム運用者要考慮事項

5.1.6.9.1 節に同じ

5.1.6.11.プライバシ４：データをセキュアにするために用いられるセキュリティ鍵およびセキュリティ・アルゴリズムは新しくすることができるか

課題：データをセキュアにするために用いられるセキュリティ鍵およびセキュリティ・アルゴリズムは新しくすることができるか

5.1.6.11.1. セキュリティ鍵更新

本件に関しては 3GPP SA3 において研究課題 LTKUP として議論されているが、現時点では以下の２方式をソリューション候補としている旨が TR 33.935-010 に述べられている。

1. Diffe-Hellman based Key agreement over SIM OTA
2. Multiple sets of parameters on the USIM

5.1.6.11.2. セキュリティ・アルゴリズム更新

前述の通り、3GPP SA3 では現在時点で性格の異なる複数の機密性/完全性保護アルゴリズムを定義している。

- 完全性: NIA1～NIA3
- 機密性: NEA1～NEA3

3G の時点からこれまでにアルゴリズムの追加/変更作業は何回か実施されていることから、3GPP において今後必要に応じてアルゴリズムを更新することは問題なく実施可能と判断できる。

5.1.6.11.3. IoT プラットフォーム運用者要考慮事項

IoT プラットフォーム運用者が自身のプラットフォーム独自の暗号鍵/アルゴリズムを用いているのであれば、それらの更新に対して同様の配慮が必要である。

5.1.6.12. セキュリティ 1:プロジェクト開始時点から製品/サービスに対してセキュリティ最良実

践が組み込まれているか？

課題：セキュリティ最良実践はプロジェクト開始時から製品およびサービスに対して組み込まれているか

5G の策定主体である 3GPP では通信事業者によって用いられるネットワーク製品のセキュリティ保証を実現するための取組として SCAS/SECAM と呼ばれる活動が存在している。

SCAS および SECAM ではそれぞれ以下のような作業が行なわれている。

- SCAS
  - 3GPP ネットワーク製品の特徴および同製品に対する脅威モデルを検討し、ネットワーク製品のセキュリティ保証実現のための方法論を検討
- SECAM
  - ネットワーク製品毎の SCAS 策定
  - ネットワーク製品セキュリティおよびネットワーク製品開発とネットワーク製品ライフサイクル管理に関するコンプライアンスの評価

これらの作業を通じて 3GPP では 5G コア・ネットワーク内部で用いられる製品が開発過程を通じて最良のセキュリティ実践を組み込まれたものとなるようにとの配慮がなされていると考えられるだろう。

5.1.6.12.1. IoT プラットフォーム運用者要考慮事項

自身の IoT プラットフォームで用いられる製品およびサービスに対しても 3GPP の SCAS/SECAM と同等の配慮が必要である。

5.1.7　3GPP における関連作業項目概要

5.1.3.1 AKMA

AKMA に関する研究項目において承認目的で SA#86 会合に送付された TR 33.835-200 が承認され、同研究項目は完了となった。今後は TR 33.835-200 に記された結論に基づく必須化作業(TS 化）が開始される予定であり、作業項目名は“Authentication and key management for applications based on 3GPP credential in 5G”[8]となった。承認された TR の結論に基づき作成される TS の目的は以下となっている。

- Specify security architecture enhancements for 5G system to support AKMA
- Specify AKMA authentication procedures
- Specify AKMA key management procedures
- Specify the security related interfaces and corresponding protocols

5.1.3.2 LTKUP

LTKUP に関する研究項目においては 2019 年 4 月にほぼ骨子レベルの TR 33.935 草稿が作成された段階である

5.1.3.3 SCAS

SCAS は 2012/12/20～2013/12/20 に 3GPP SA3 によって実施された研究課題項目であり、3GPP ネットワーク製品の特徴および同製品に対する脅威モデルを検討し、ネットワーク製品のセキュリティ保証実現のための方法論候補である以下の 2 種類に対する分析が行なわれた。

1. Common Criteria (ISO 15408)準拠
2. 独自方式
   - 対象製品を評価する上で必要と考えられる特徴/機能の完全なリストを作成し、脅威分析結果に基づくセキュリティ要件との適合性を評価
   - ネットワーク製品(クラス)毎に SCAS (Security Assurance Specification)を作成

結論としては 2.の独自方式を採用するが、評価過程では CC が定める方法論を適宜流用することとなっている。

5.1.3.4 SECAM

SECAM が担当するタスクは以下の二つである。

- セキュリティ要件および試験仕様である SCAS の策定
- ネットワーク製品セキュリティ評価およびベンダのネットワーク製品開発とネットワーク製品ライフサイクル管理に関するコンプライアンス評価

SECAM 認定主体と呼ばれる主体が認定および統治・維持を担当することで 3GPP 活動を補助することとされているが、SECAM 認定主体は現行では GSM Association (GSMA)のみである。

SECAM 認定主体は以下に対する要件および手続きを定義することとなっている。

- ベンダ・ネットワーク製品およびネットワーク製品ライフサイクル管理プロセス認定
- 試験ラボ (ベンダ所有ないし第三者) 認定
- 紛争解決

5.1.8　ユースケース IoT セキュリティまとめ

国内外の IoT セキュリティ関連文書を調査し、GSMA の文書を軸とした課題抽出、5G で検討すべき課題の抽出を行った。さらに方向性を大きくまとめると、5G で新たに追加された

- ネットワーク・スライシング機能
- セカンダリ認証機能
- プライバシ考慮機能

を活用することで IoT セキュリティ課題を解決できる可能性があることが判る。

これらに基づいて具体的な代表的な検討課題について対策案をまとめると表 5.1 の通りとなる。

表 5.1　代表的な検討課題と対策案

| 課題 | 対策案 |
|---|---|
| LPWA ネットワークを伝統的なセルラ・システムと同一のレベルのセキュリティで運用することが可能か | 5G のネットワーク・スライシング機能の mMTC スライス活用により柔軟な対応ができる |
| IoT デバイスが複数のモバイル・オペレータを跨る際、同一レベルのネットワーク・セキュリティを提供できるか | SEPP (Secure Edge Protection Proxy) によりオペレータ間モビリティでのセキュリティ確保が可能となる |

| 課題 | 対策案 |
| --- | --- |
| ゲートウェイ・エンドポイントに通信を依拠するエンドポイントに対してネットワークの信頼をフォワードすることが可能か? | 5G では軽量エンドポイントが直接通信可能となることにより GW ポイントを不要とできる |
| セキュアな通信環境を用いることができるように軽量エンドポイントの電力制限を回避できるのか | 電力制限がある軽量エンドポイントデバイスについてのソリューションが考案されており、それらを採用することで可能となる |
| エンドポイントを操作する利用者をエンドポイントのアイデンティティに対して強力に連想付けることは可能なのか | 5G セカンダリ認証によりエンドポイントと利用者を連想づける事が可能となる |
| エンドポイントのセキュリティ技術はピアおよびサービスを安全に認証することができるのか | 5G セカンダリ認証や AKMA によりサービスを安全に認証できることが可能となる |
| デバイスのアイデンティティをタンパリングもしくは操作から保護することができるのか | 5G ではクレデンシャル・ストレージ機能により UICC 以外のセキュア・ストレージを利用することが可能であり、これらを保護の参考にできる |
| エンドポイントのアイデンティティは認可されていない利用者に披瀝されるのか | 5G では IMSI ではなく、匿名化した SUCI を常に用いることが可能となったため、5G ネットワーク内でのエンドポイント・アイデンティティ漏洩が回避できる。サービスにおいてもこれらを構築の参考にする事ができる |
| エンドポイントもしくは IoT サービスから放出されるデータは、物理的なエンド・ユーザの属性 (位置、行動、ないし、睡眠中/覚醒中のような状態)を示唆ないし直接的に提示するか | 5G ネットワーク内においては、モバイル・ネットワーク全区間での安全性を考慮された暗号化方式が利用されている。サービスにおいてもこれらを構築の参考にする事ができる |
| 暗号文に存在するパターンが観察できないほど十分な機密性と完全性を備えた暗号化方式が用いられているか | 5G ネットワーク内においては、モバイル・ネットワーク全区間での安全性を考慮された暗号化方式が利用されている。サービスにおいてもこれらを構築の参考にする事ができる |
| データをセキュアにするために用いられるセキュリティ鍵およびセキュリティ・アルゴリズムは新しくすることができるか | 5G では長期有効鍵 (UICC とコア・ネットワークで共有される K)の更新可能化方式に関して検討中であり。サービスにおいてもこれらを構築の参考にできる |

| 課題 | 対策案 |
| --- | --- |
| セキュリティ最良実践はプロジェクト開始時から製品およびサービスに対して組み込まれているか | 5G コア製品については 3GPP SCAS (Security Assurance Specification) の枠組を用いた取組が行なわれている。サービスにおいてもこれらを構築の参考にできる |

## 5.2 ユースケース Connected Vehicle セキュリティ

### 5.2.1. 概要

5G 時代に実現するサービスのひとつとして、ネットワークへ接続する機能を備えた自動車が、他の車両や信号等の交通インフラといった様々な対象とつながる、Connected Vehicle が注目されている。Connected Vehicle により、交通の高度化や、セーフティ、新しいサービスが創出されることが期待される。Connected Vehicle においては、インフォテイメントやセーフティなど、様々な分野に関して、新たなサービスの創出や発展が見込まれている。その一方、つながることにより、従来は想定されなかった脅威が現実のものとなり、その対策としてセキュリティに留意することが重要となる。

こうした状況を受け、2018 年 7 月、5GMF の企画委員会の配下に、セキュリティ検討 AdHoc が設置され、一年間の準備期間を経て、2019 年 7 月に、セキュリティ調査研究委員会が設置された。その活動目的は、5G 時代に想定されるサービスのセキュリティに関する検討組織の立ち上げに向けて、IoT、Connected Vehicle、および Fintech の各分野を対象とした調査と検討を通じて、セキュリティ課題を抽出することである。本報告は、このうち、Connected Vehicle 分野における活動の結果を報告するもので、Connected Vehicle において実現される各種サービスに対するセキュリティの課題を整理し、5G で検討すべきセキュリティ要件を明確化する。以下、本章の構成を示す。本節にて全体概要を、5.2.2 節において、 Connected Vehicle のセキュリティに関連する標準化団体、業界団体の標準文書やガイドラインを調査した結果をまとめ、各文書の関係を整理する。また、5.2.3 節においては、5.2.2 節の各種団体で整理されたセキュリティ要件を踏まえ、5G ネットワークを用いて Connected Vehicle を実現する幾つかの技術要素に着目し、そのセキュリティ課題を整理する。

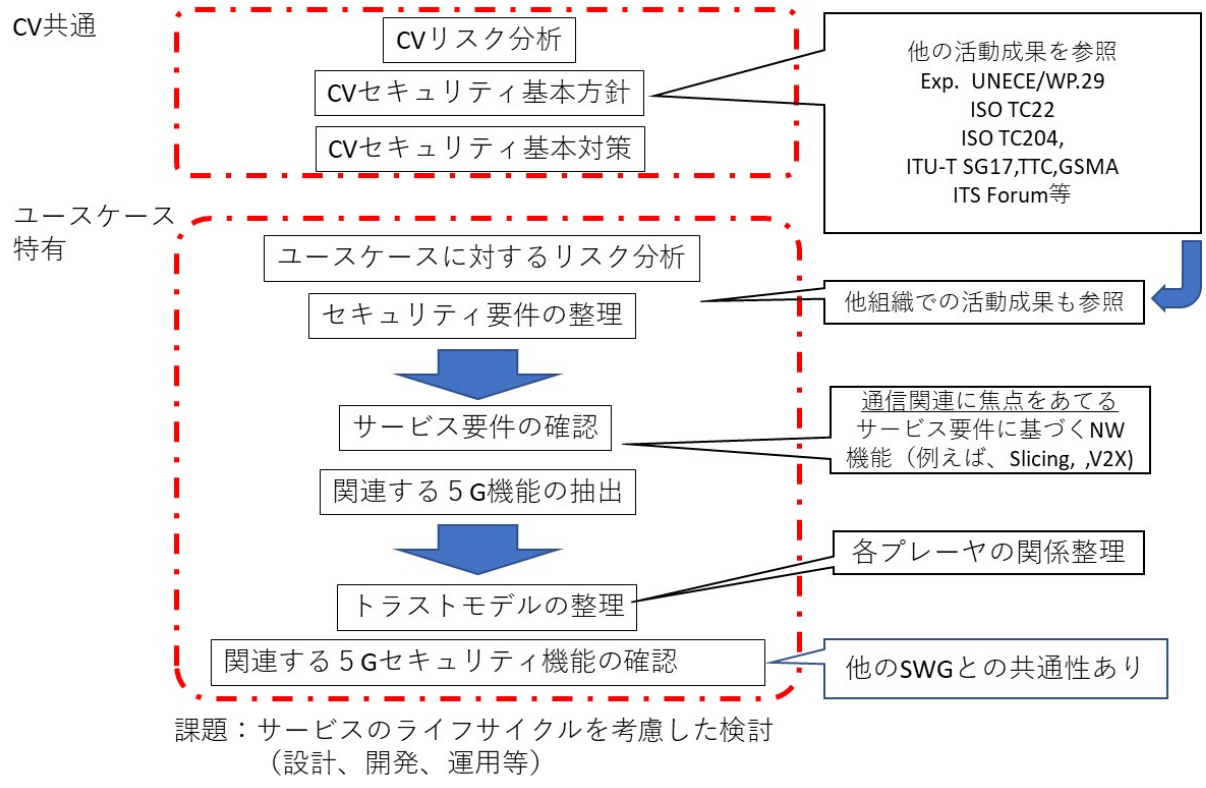



図 5.2.1　本報告書の検討プロセス

### 5.2.2. Connected Vehicle セキュリティに関連する標準

#### 5.2.2.1. UNECE/WP.29

国連欧州経済委員会(UNECE)配下の国連自動車基準調和世界フォーラム(WP.29)の ITS/AD（自動運転分科会）において、Task Force on Cyber security and OTA(Over The Air)が設立され、2016 年 12 月より活動を開始している。

サイバーセキュリティ及びデータ保護に対するガイドラインが規定されている。本ガイドラインでは、表 5.2.1 に示す通り、一般原則に加えて、パーソナルデータに対するデータ保護、機能安全やフェールセーフ等のセーフティ、不正アクセスや盗聴、データ改ざんを防止するセキュリティに対する、ハイレベルな要求条件を規定している [1](2017)。また、上記の中でも特にサイバーセキュリティとソフトウェアアップデートに焦点を充てた検討がなされ、以下の２つが Regulation 案の位置づけでガイドラインとしてまとめられている(2018,2019 改訂)。

表 5.2.1　サイバーセキュリティ及びデータ保護に対するガイドラインの概要

| 分類 | 対策指針 |
|---|---|
| データ保護 | パーソナルデータに対する法に準拠した、公平、かつ透明性のある処理 |
| | 匿名化や仮名化の技術の利用 |
| | 目的に限定したパーソナルデータの収集や処理に関する制限 |
| | プライバシーバイデザイン、プライバシーバイデフォールトの導入 |
| セーフティ | CVや自動運転技術を有する車に対するISO26262の機能安全の配慮 |
| | CVや自動運転技術を有する車への接続や通信において、CV内やCV内のデータに影響を与えないフェールセーフ、 |
| | 無線通信や診断ポートを介したサイバー攻撃による回路基盤情報への不正アクセスやソフトウェアの不正な改ざんの防止 |
| | 緊急時のセーフモードの具備 |
| セキュリティ | CVや自動運転技術を有する車に対するISO27000やISO15408などの標準による検証可能なセキュリティ対策 |
| | CVや自動運転技術を有する車における、ソフトウェア更新などによる完全性の確保や暗号鍵の適切な管理 |
| | CVや自動運転技術を有する車の車内の制御機器間の通信における相互認証 |
| | CVや自動運転技術を有する車に対するリモートアクセスにおける、強固な相互認証や暗号化や改ざん防止などによるセキュア通信の確保 |

##### 5.2.2.1.1. Proposal for a Recommendation on Cyber Security [2]

前者のガイドラインでは、クルマの製造業者と対象とし、クルマあるいはネットワークやクラウドも含むシステム全体に対するセキュリティの基本方針、脅威とその対策、さらに、開発、製品化、製品終了時の各フェーズでのセキュリティ管理の手法等を規定している。このなかで、補遺 A は、サイバーセキュリティに対する国連における Regulation 案が記載されている。

ここでは、3 章の基本方針と 4 章の脅威について概説する。3 章の基本方針では、経営トップ層によるガバナンス、サプライチェーン、多層防御の考え方、攻撃に対する防御・検知・分析機能やセキュリティ評価など一般的な指針が網羅的に規定されている（表 5.2.2　サイバーセキュリティ勧告の基本指針)。また、脅威に関しては、クルマの構成要素を意識した分類がなされている（表 5.2.3 参照及び表 5.2.4～表 5.2.9)。特にソフトウェアの更新や外部との接続性に関す

る脅威は、クルマを意識したものとなっている。この中で、通信・ネットワークの関連性がある項目としては、通信チャネルや外部接続性に対する脅威が相当する（表 5.2.5、表 5.2.8 参照)。これらの対策としては、秘匿、認証・認可、改ざん防止、否認防止等の一般的なセキュリティ対策が規定されている。

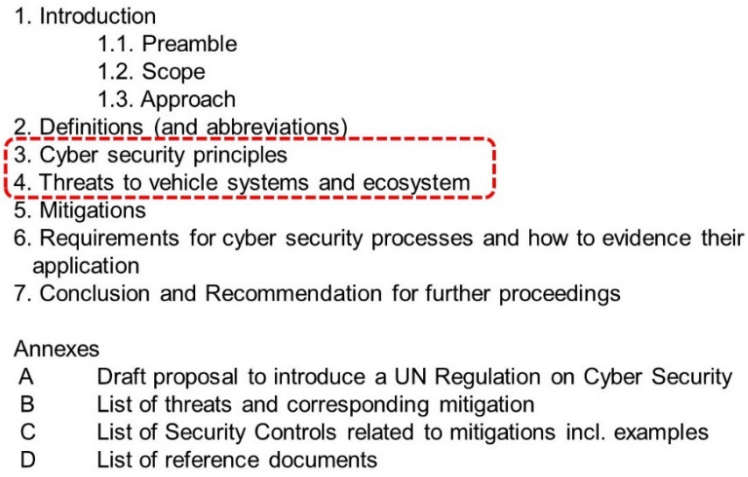



図 5.2.1　サイバーセキュリティ勧告の目次

表 5.2.2　サイバーセキュリティ勧告の基本指針

| 節 | 基本指針 |
|---|---|
| 3.3.1 | サイバーセキュリティの組織はトップレベルで、運営、統制、推進すべきである。 |
| 3.3.2 | セキュリティリスクは、サプライチェーンも含め、適切かつリスクに比例して評価・管理されるべきである。 |
| 3.3.3 | 組織は、ライフサイクルを通じて、クルマの安全性を確保するためにサイバーセキュリティを管理し、インシデントに対応する機能を具備すべきである。 |
| 3.3.4 | 下請業者、サプライヤー、潜在的な第三者を含むすべての組織は、システムのセキュリティを強化するために協力すべきである。 |
| 3.3.5 | クルマは多層防御のアプローチで設計すべきである。 |
| 3.3.6 | ハードウェア、ソフトウェアのセキュリティはクルマのライフサイクルを通じで管理すべきである。 |
| 3.3.7 | データは安全に保管、転送され、制御されるべきである。 |
| 3.3.8 | クルマの製造業者は、テストの手続きによりセキュリティ機能を評価すべきである。 |
| 3.3.9 | クルマは、サイバー攻撃に対して対抗力を持った設計をすべきである。 |
| 3.3.10 | クルマは、サイバー攻撃を検出し、適切に対応できるように設計すべきである。 |
| 3.3.11 | クルマのサービスや機能へのアクセスは、アクセス制御の仕組みによって制御され、国や領域の法律に従った役割を設定され、許可されたもののみに許容すべきである |
| 3.3.12 | クルマは、インシデントの事後解析やフォレンジックのために関連するデータのログを保持すべきである。 |

表 5.2.3　クルマに対する脅威

| 節 | クルマに対する脅威 | 通信との関係 |
|---|---|---|
| 4.3.1 | バックエンドサービスに対する脅威 | |
| 4,3,2 | 通信チャネルに関するクルマの脅威 | ◎ |
| 4.3.3 | (ファームウェア）更新に関する車の脅威 | |
| 4.3.4 | 意図しない人の操作に関する脅威 | |
| 4.3.5 | 外部接続性に関するクルマの脅威 | ○ |
| 4.3.6 | 潜在的な対象への攻撃、攻撃に対する動機 | |

表 5.2.4　バックエンドサービスに対する脅威

| 節 | バックエンドサービスに対する脅威 |
|---|---|
| 4.3.1(a) | クルマや外部データに対する攻撃にバックエンドサーバを利用(1) |
| 4.3.1(b) | バックエンドサーバの破壊による、クルマの運用に影響(2) |
| 4.3.1(c) | バックエンドサーバが保有するデータの紛失や漏洩(3) |

表 5.2.5　通信チャネルに対する脅威

| 節 | 通信チャネルに対する脅威 | 5 G関連 |
|---|---|---|
| 4.3.2(a) | クルマで受信するデータやメッセージのスプーフィング | ○ |
| 4,3,2(b) | クルマが保有するコードやデータに対して不正な修正、削除、追加するための通信チャネルを利用 | ○ |
| 4.3.2(c) | 信頼できないメッセージを受け付ける通信チャネル、あるいは、セッションハイジャック/リプレイ攻撃に対して脆弱な通信チャネル | ○ |
| 4.3.2(d) | 通信の盗聴や機微なファイル/フォルダ-への不正なアクセスによる情報の開示 | ○ |
| 4.3.2(e) | 通信チャネルへのDoS攻撃によるクルマの機能不全 | ○ |
| 4.3.2(f) | 不正な利用者によるクルマのシステムへのアクセス権の取得 | ○ |
| 4.3.2(g) | クルマのシステムを感染させる通信メディアへ埋め込まれたマルウェア | ○ |
| 4.3.2(h) | 不正なコンテンツを含むメッセージの受信や転送 | ○ |

表 5.2.6　ソフトウェア更新手続きに対する脅威

| 節 | ソフトウェア更新手続きに対する脅威 |
|---|---|
| 4.3.3(a) | 更新手続きの誤用や不正(12) |
| 4.3.3(b) | 正規更新の否認(13) |

表 5.2.7　意図しない人間の行動に対する脅威

| 節 | 意図しない人間の行動に対する脅威 |
|---|---|
| 4.3.4(a) | 所有者やメンテ業者など正当な利用者により機器やシステムの設定ミス(14) |
| 4.3.4(b) | 正当な利用者が無意識のうちにサイバー攻撃を受けやすくする(15) |

表 5.2.8　外部接続性に対する脅威

| 節 | 外部接続性に対する脅威 | 5G関連 |
|---|---|---|
| 4.3.5(a) | サイバー攻撃を可能とするクルマの接続性機能に対する改ざん。接続性機能とは、遠隔操作を許容するテレマティクスシステムや、狭帯域無線通信 | ○ |
| 4,3.5(b) | クルマのシステムへの攻撃手段となるエンタメのアプリなどの第３者ソフトウェア | |
| 4.3.5(c) | クルマのシステムへの攻撃手段となるUSBや、ODBなどの外部インターフェースに接続された機器 | |

表 5.2.9　十分に保護、強化しない場合に悪用される脆弱性

| 節 | 十分に保護、強化しない場合に悪用される脆弱性 |
|---|---|
| 4.3.6(a) | 暗号技術が解読されるあるいは、不十分な状態で利用される。(26) |
| 4.3.6(b) | 構成部品がハッキングされクルマが攻撃される(27) |
| 4.3.6(c) | ソフトウェアやハードウェアの開発過程で脆弱性が発生する(28) |
| 4.3.6(d) | ネットワークの不十分な設計が脆弱性を生み出す(29) |
| 4.3.6(e) | データの消失(30) |
| 4.3.6(f) | 意図しないデータの転送(31) |
| 4.3.6(g) | システムの物理的な改ざん(32) |

#### 5.2.2.1.2. Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues [3]

クルマの電子化が進むにつれて、利用されているソフトウェアの更新の重要性が増し、新たな機能の付加、性能の改善、不備の修正などソフトウェアを更新する必要性が増してきている。このためサイバーセキュリティタスクフォース(TFCS)において、クルマ製造業者を対象として、ソフトウェア更新のためのガイダンスと、Regulation について検討を行っている。

本構成を図 5.2.3 に示す。本文では、ソフトウェア更新の手順および、セーフティとセキュリティに関する要求条件、更新されるソフトウェアの識別に関するガイダンスが規定されている。一方、補遺においては、ソフトウェア更新およびクルマ製造業者によって定義される専用の識別子(RXSWIN)のための Regulation 案が規定されている。

ここで、5 章はセーフティおよびセキュリティ要件を規定しており、そのうちセキュリティ要件は、表 5.2.10 のとおり、更新するソフトウェアに対する改ざんや、更新処理自体に対する攻撃を防止できることとなっている。またこれらの要件が確保できていることをオーソリティが確認できる能力や、オーソリティが確認する際に必要となる情報（ドキュメント）を規定している。

本 Regulation の検討に呼応して、国内では、ソフトウェア更新（一部サイバーセキュリティ要件を含む）の実施に関する国内法令（道路運送車両法第 99 条の 3 （特定改造））の整備が 2019 年 5 月に完了している（施行は 1 年 5 か月後） [4]

1. Introduction
   1.1.Preamble
   1.2.Scope
2. Definitions
3. Document structure
4. Process for software updates
5. Safety and security requirements for software updates
6. Identification of the installed software
7. Conclusion and Recommendation for further proceedings

Annexes

A Draft proposal to introduce a UN Regulation on uniform provisions concerning the approval of software updates processes

B Draft proposal to amend existing UN Regulations to introduce software identification numbers (RXSWIN)

図 5.2.2　ソフトウェア更新のためのガイドラインの目次

表 5.2.10　ソフトウェア更新のセキュリティ要件

| 節 | 要求条件 |
|---|---|
| 5.4.1(a) | ソフトウェアの更新処理の際に、不正な改ざんを防止する。(承認された、破壊されていないソフトウェアのみがクルマに提供されるる) |
| 5.4.1(b) | システム更新プログラムやファームウェアの開発時も含み、ソフトウェアの更新処理自体が侵害されない。 |
| 5.4.1(c) | ソフトウェア更新での認証や完全性の機能により侵害と不正な更新を防止する |
| 5.5 ソフトウェア更新において、セーフティやセキュリティを保証するための要件 | ソフトウェア更新の認証のため、特にOTAに対して、オーソリティは、上記のセーフティやセキュリティの要件に関するクルマ製造業者の処理や手続きを評価するに十分な能力を有する。 |
| | クルマ製造業者の安心・安全なソフトウェア更新に関する処理や手続きを評価するために、クルマ製造業者は下記の情報をオーソリティに提供する。<br>・ソフトウェア更新時、セキュリティを確保する手法<br>・ソフトウェア更新時、セーフティを確保する方法<br>・ソフトウェア更新時、クルマの利用者に課す要件や手順 |

5.2.2.2. ISO TC 22 (Road vehicles)

ISO/TC22 では、ISO/SAE21414（Road vehicles — Cybersecurity engineering）の作成を進めている。本規格は、クルマのライフサイクル全般、すなわち、エンジニアリング（例：コンセプト、設計、開発）、生産、運用、保守、および廃止措置全体を通して、クルマ、その構成要素およびインターフェースのサイバーセキュリティリスク管理の要件を規定している。また、ステークホルダー間でサイバーセキュリティリスクを伝達・管理するためのプロセスと共通言語のフレームワークを定義している。プロセスを定義することで攻撃が成功する可能性を削減、損失を削減でき、絶えず変化する脅威に対する明確な対策を提供できる。グローバルな業界全体で一貫性を確保し、意思決定を促進できる。本規格は、WP29 のサイバーセキュリティ基準から引用される規格となる見込みである [5]。

本規格の規定項目を図 5.2.4 にまた、その全体構成を図 5.2.5 に示す。本規格の構成は [6]に要約されている。その内容は以下の通りである。

6 章のリスク管理手法では、リスク管理を行うために必要な定義、および、資産分析、脅威分

析、リスク評価を実施する際の要件を定義している、８章の開発プロセスでは、クルマの企画段階から開発完了までに、必要なサイバーセキュリティ活動の要件を定義している。特に、コンセプト、システム、ハードウェア、ソフトウェアのクルマ特有の水平分業に対応している、9 章では、生産、運用、破棄では、開発完了から破棄に至るまで必要なサイバーセキュリティ活動の要件を定義している。脆弱性情報の収集、インシデント対応、インシデント対策、破棄時の要件が含まれる。10 章のサイバーセキュリティ管理では、クルマのライフサイクルに関連するサイバーセキュリティ管理要件、組織のサイバーセキュリティ戦略を確立するための組織固有のルール、プロセスの要件を定義している。

ここで、開発プロセス時のサイバーセキュリティ活動の概要を記す（図 5.2.6 参照）。本プロセスでは機能安全の標準 ISO26262 で規定されたセーフティに関するトリプル V プロセスを参考にしている。トリプルとはシステム、ソフトウェア、ハードウェアの 3 つの構成要素を対象としている。

一方、本規格は、サイバーセキュリティ活動の要件やプロセスの定義、方法論に関する規格であり、以下の内容は含まない。

・具体的なサイバーセキュリティ技術やソリューションの適用
・具体的な改善施策に関する要件の包含
・通信システムのための要件の包含
・バックオフィスのための要件の規定
・EV 充電のための要件の規定
・自動運転車固有の要件の規定

以上、ISO/SAE 21434 は、設計、開発、運用、破棄のすべてのプロセスでのサイバーセキュリティ管理が規定されている点が特徴である。


図 5.2.3　ISO/SAE21434 の目次と概要

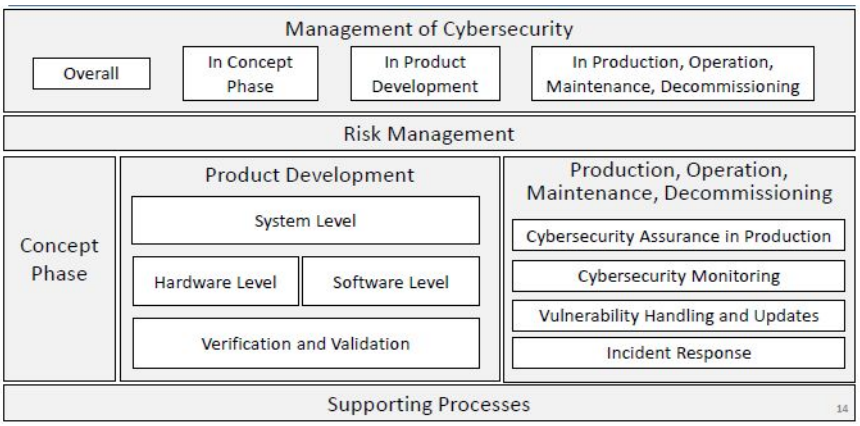



図 5.2.4　ISO/SAE21434 の構成

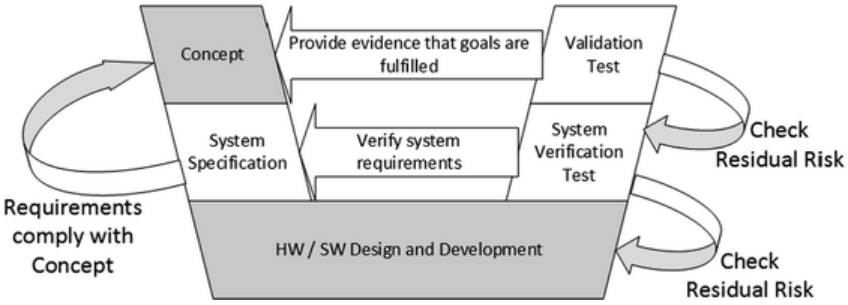



図 5.2.5　開発プロセス時のサイバーセキュリティ活動の概要

5.2.2.3. ISO TC204（Intelligent Transport Systems）

ITS に関する標準化を対象とする委員会であり、交通に関する情報、通信、および制御システムの標準化を対象とする [7]。ISO TC204/WG16（通信分科会）は、ITS における通信の規格を対象としている [8]。このなかで、セキュリティに関する規格として、ISO21217 [9]および ISO16461 [10]がある。また、ISO TC204/WG18（協調システム分科会）におけるセキュリティに関する規格としては、ISO/TS21177 [11]、ISO/TS21185 [12]がある（表 5.2.11）。

表 5.2.11　TC204 におけるセキュリティ関連の規格

TC204 セキュリティ関連規格

| 規格 | タイトル | 概要 |
|---|---|---|
| ISO21217 | CALM(Communications access for Land mobile) Architecture | プロトコルスタックの中に、セキュリティ機能を定義 |
| ISO16461 | ITS – Criteria for privacy and integrity protection prove vehicle information systems | プローブ情報のプライバシーに関する評価基準 |
| TS21177 | ITS- ITS station security services for secure session establishment and authentication between trusted devices | ITS基地局間のセキュアな通信を迅速に認証・確立するシステム |
| TS21185 | ITS- Communication profiles for secure connections between trusted devices | ITS基地局と車両との間のセキュアな通信のための下位レイヤ通信に関するプロファイル規格 |

ISO21217 は、ITS の通信ネットワークを目的として設計された ITS 基地局ユニットと呼ばれるノードの通信参照アーキテクチャを規定している。ITS の通信ノード間の様々な ISO ネットワーク上で 1 対 1 の通信をするための通信ノードを規定している。本規格での規定内容を図

5.2.7 に、規定する参照アーキテクチャを図 5.2.8 に示す。セキュリティの構成においては、侵入検知のためのファイアウォール、認証、認可プロファイル管理、SMIB におけるネットワークセキュリティ管理、ハードウェアセキュリティモジュール（HSM）の構成要素を規定している。

1 Scope
2 Normative references
3 Terms and definitions
4 Symbols and abbreviated terms
5 Requirements
6 Overview of ITS communications
7 ITS station overview
8 Details of elements of ITS-S reference architecture
9 Typical implementations of ITS station units
Annex A Illustration of typical ITS-SU implementations
Annex B ITS-S configurations

図 5.2.6　ISO21217 の目次

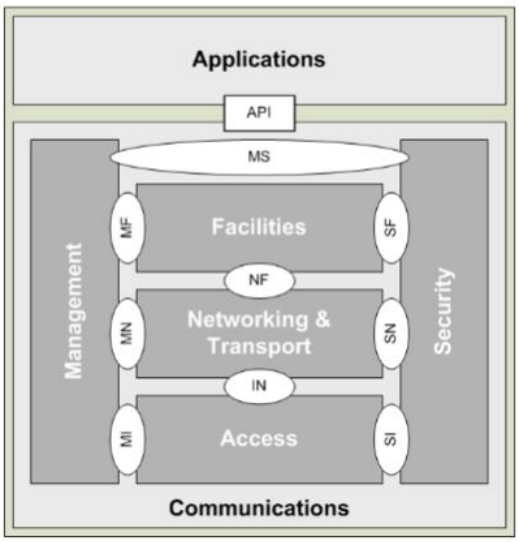



図 5.2.7　ISO21217 CALM reference architecture

ISO16461 は、プローブ車両情報サービスのプライバシに関するサービス提供者が考慮すべき評価基準を規定している（図 5.2.9 参照）。ISO16461 は、PVS（Prove Vehicle Systems）に関する規格で、以下の内容を規定している。ここで、PVS とは、個々のクルマからプローブデータを集めて、統計的な処理を行うことにより、様々な利用者に対して有益な情報を提供するためのシステムである。本規格では以下の内容を規定している。

・PVS でデータの完全性の保護と匿名性を確保するためのアーキテクチャ
・PVS のデータ完全性保護とプライバーを確保するためのセキュリティ評価基準や要件
・プローブデータの適切で匿名化されたデータの生成と扱いに関する要件

1 Scope
2 Normative references
3 Terms and definitions
4 Symbols and abbreviated terms
5 Reference architecture
6 Basic framework
7 Criteria for privacy protection

図 5.2.8　ISO16461 の目次

ISO/TS21177 は、ITS 基地局に関して、トラステッドデバイス間で、認証、秘匿、データ完全性を確保するための仕様である（図 5.2.11 参照)。図 5.2.10 に示す通り、2 つのデバイスが協調し信頼関係を構築し、保護された情報を双方向に交換する。ISO 21217 の定義に基づき、ITS 基地局(ITS-S)機能の物理実装である ITS 基地局ユニット(ITS-SU)は、トラステッドデバイスである。さらに、ITS 基地局ユニットは、ITS 内部ネットワークで相互接続される複数の ITS 基地局通信ユニット(ITS-SCU)から構成される。すなわち、ITS 基地局通信ユニットは、トラステッドデバイスの最小単位となる（図 5.2.12 参照)。ここで、ITS 基地局は、クルマ内のネットワーク(IVN)や路側のネットワーク(IRN)からセキュアにデータにアクセスする必要がある（図 5.2.13、図 5.2.14)。従って、以下の ITS アプリ間の信頼関係を確立するための ITU-S のセキュリティサービスを規定している。ITS アプリは、以下の 3 つのケースで信頼関係を確立する。

・ITS-SU 内の異なる ITS-SCU の ITS アプリ間
・異なる ITS-SU の ITS-SCU 間の ITS アプリ間
・ITS-SU とセンサーや制御ネットワーク（SCN)間

図 5.2.15 に示す通り、セキュアセッションが提供する TLS セキュリティプロトコルの上で、セキュリティアダプター層として、認証・認可、秘匿とプライバシ、データ完全性、否認防止のセキュリティサービスを ITS アプリに提供するサービスである。

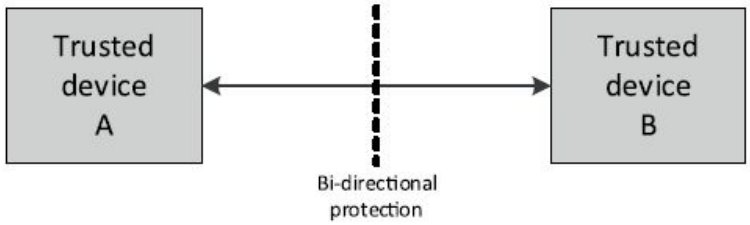



図 5.2.9　TS21177 における基本構成

1 Scope
2 Normative
3 Terms and
4 Symbols and abbreviated
5 Overview
6 Process flows and sequence diagrams
7 Security Subsystem: interfaces and data types
8 Adaptor Layer: Interfaces and data types
9 Secure Session services
Annex A (informative) Usage scenarios
Annex B (normative) ASN.1 module

図 5.2.10　TS21177 の目次

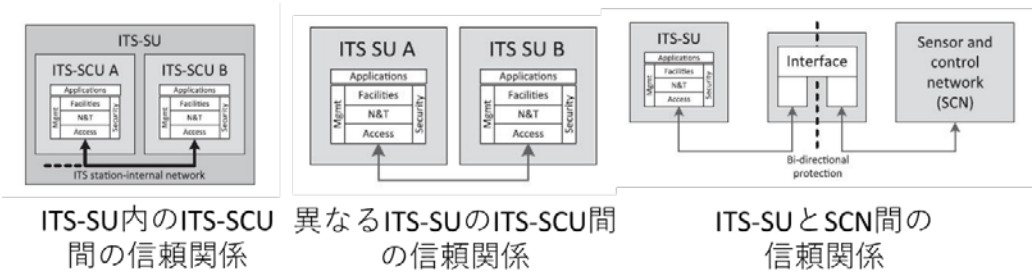



図 5.2.11　ITS サービスの信頼性関係

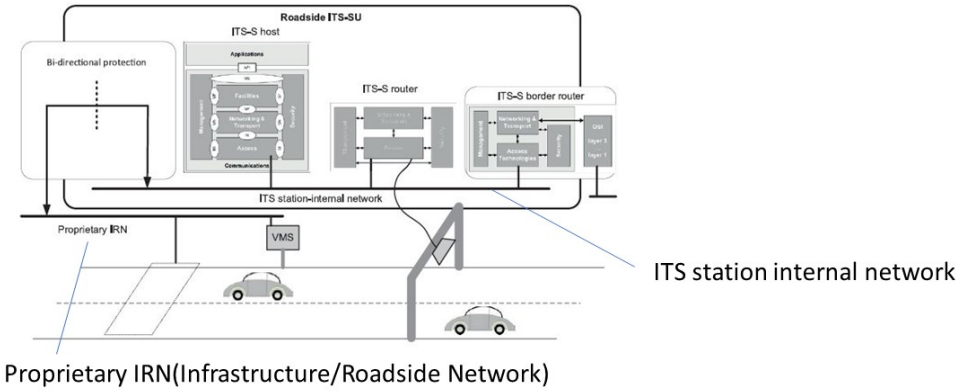



図 5.2.12　ITS-SU が非標準な IRN と接続する例

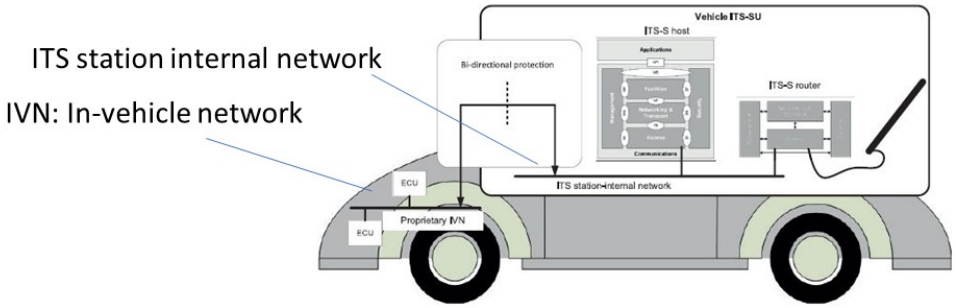



図 5.2.13　ITS-SU が非標準な IVN と接続する例

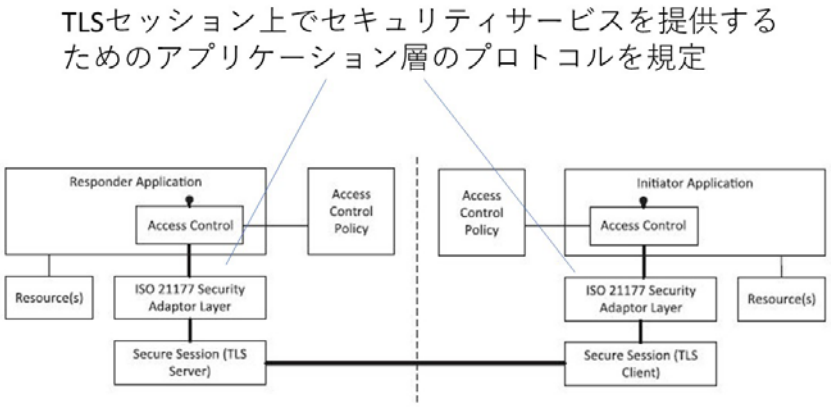



図 5.2.14　TS21177 における論理アーキテクチャ

ISO/TS21185 は、標準化されたトラステッドデバイス間の通信プロトコルに基づく ITS-S 通信プロファイルを定義するための方法論について規定している（図 5.2.16 参照）。トラステッドデバイス間で、異なる構成において、セキュアで低遅延での情報交換を可能とするプロファイルを規定する。

1 Scope.
2 Normative references
3 Terms and definitions
4 Symbols and abbreviated terms
5 OID conventions
6 Architecture
7 Communication profiles and protocol
8 ITS communication protocols
9 ITS-S communication protocol stacks
10 ITS-S communication
Annex A (normative) ASN.1 module

図 5.2.15　TS21185 の目次

5.2.2.4. ITS Forum

ITS 情報通信システムの普及促進を図るため、ITS 情報通信システムに関する研究開発及び標準化の調査研究、関係機関との連絡調整、情報の収集、啓発活動等を行うことを目的とする団体である。また、ITS を普及・促進するため、各種ガイドラインを策定し公開している。

Connected Vehicle のセキュリティに関わるものとしては、車車間・路車間通信情報におけるセキュリティガイドラインを規定した「ITS Forum RC-009 運転支援通信システムに関するセキュリティガイドライン」(2011) [13]と、本推進会議の高度化専門委員会セルラーシステム TG と 5GMF Connected Vehicle アドホック会合が共同で作成した「セルラー通信技術を用いた ITS・自動運転の高度化に向けた課題調査報告書」(2019) [14]がある。

5.2.2.6.1. ITS Forum RC-009 運転支援通信システムに関するセキュリティガイドライン

図 5.2.17 に上記ガイドラインの構成を示す。

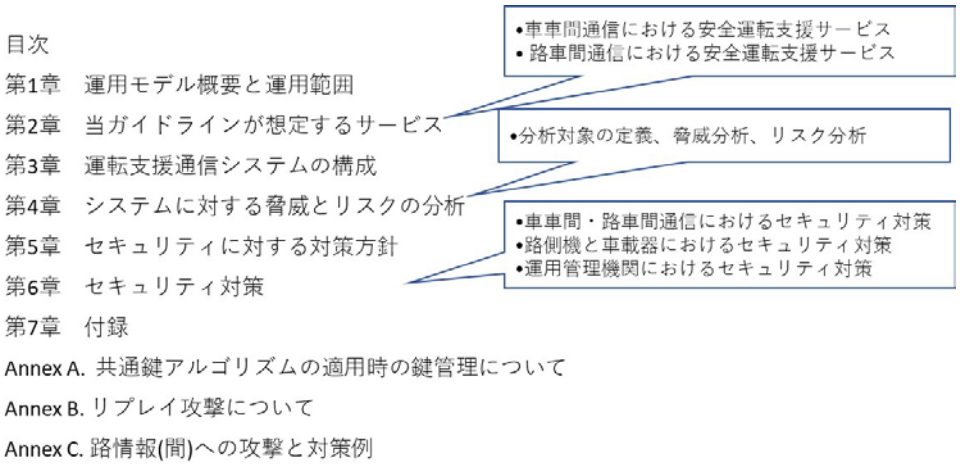



図 5.2.16　ITS Forum RC-009 運転支援通信システムに関するセキュリティガイドライン

本ガイドラインの検討対象を図 5.2.18 に示す。本分析対象の車車間・路車間での通信部分であり、ブロードキャスト通信が対象である。ここでは、一般車両が偽の優先車両の情報を配信し、優先車両になりすます、偽の路側器から偽の情報を配信するなど、サービスに紐づいた脅威を想定し、そのセキュリティ対策を規定している。

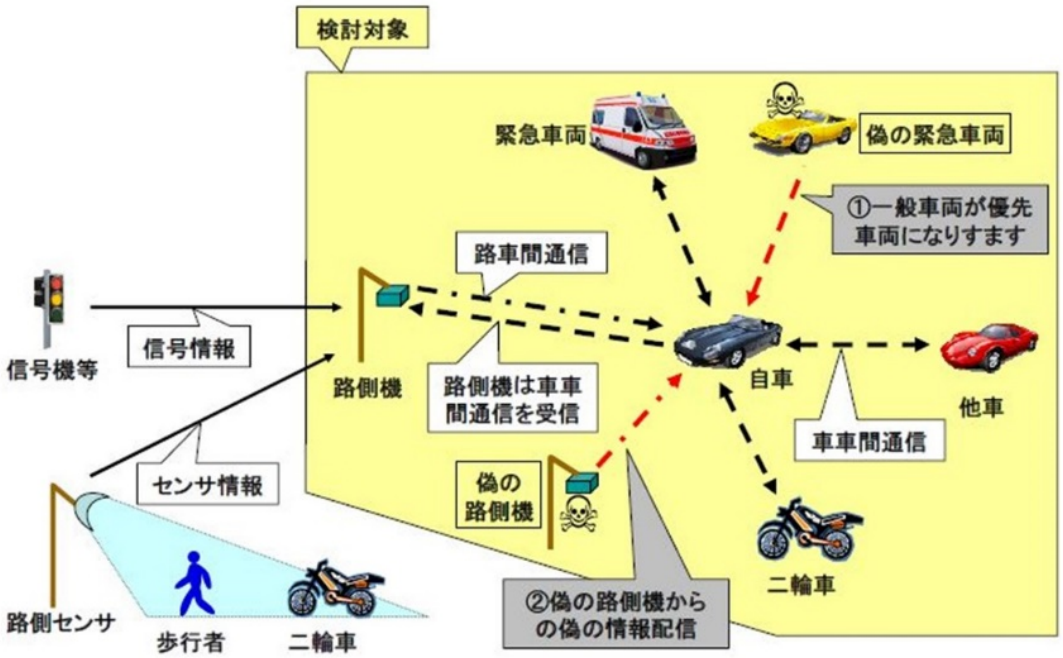



図 5.2.17　ITS Forum RC-009　ガイドラインの検討対象

また、リスク分析結果の例を表 5.2.12 に示す。これらのリスク分析に基づく具体的なセキュリティ対策として、車車間、路車間の通信情報に対するメッセージ認証コードを用いたメッセージの真正性や、電子署名を用いた発信元の認証などの暗号メカニズムを規定している。

表 5.2.12　リスク分析結果の例

| ID | 脅威 | 項目 | ランク | 根拠 |
|---|---|---|---|---|
| | | 困難さ | None | 攻撃の前例あり |
| | | 影響度 | Medium | 攻撃を受けた場所での限定的な影響 |
| N | 車両なりすまし 偽走行情報送信 | 動機 | Moderate | 混乱目的 |
| | | 困難さ | Solvable | 理論的には攻撃が可能 |
| | | 影響度 | Medium | 送信された場所での限定的な影響 |
| O | 車両なりすまし 偽汎用情報送信 | 動機 | Moderate | 混乱目的 |
| | | 困難さ | Solvable | 理論的には攻撃が可能 |
| | | 影響度 | Medium | 送信された場所での限定的な影響 |
| P | 車両なりすまし リプレイ攻撃 | 動機 | Moderate | 混乱目的 |
| | | 困難さ | None | 攻撃の前例あり |
| | | 影響度 | Medium | 攻撃を受けた場所での限定的な影響 |
| Q | ロケーショントラッキング(1) | 動機 | High | 特定個人のプロファイリング目的と明確な目的があり、利益は大 |
| | | 困難さ | Solvable | 理論的には攻撃が可能 |
| | | 影響度 | Low | 特定個人への影響であり、通信距離内での追跡が必要でストーキングと同じ(後述) |

5.2.2.6.2. セルラー通信技術を用いた ITS・自動運転の高度化に向けた課題調査報告書

本報告書は、セルラーV2X を用いた ITS・自動運転の高度化に向けた課題を整理し、今後国内でセルラーV2X の有効性検証や課題の具体化・対応検討を加速化させることを目的としている。

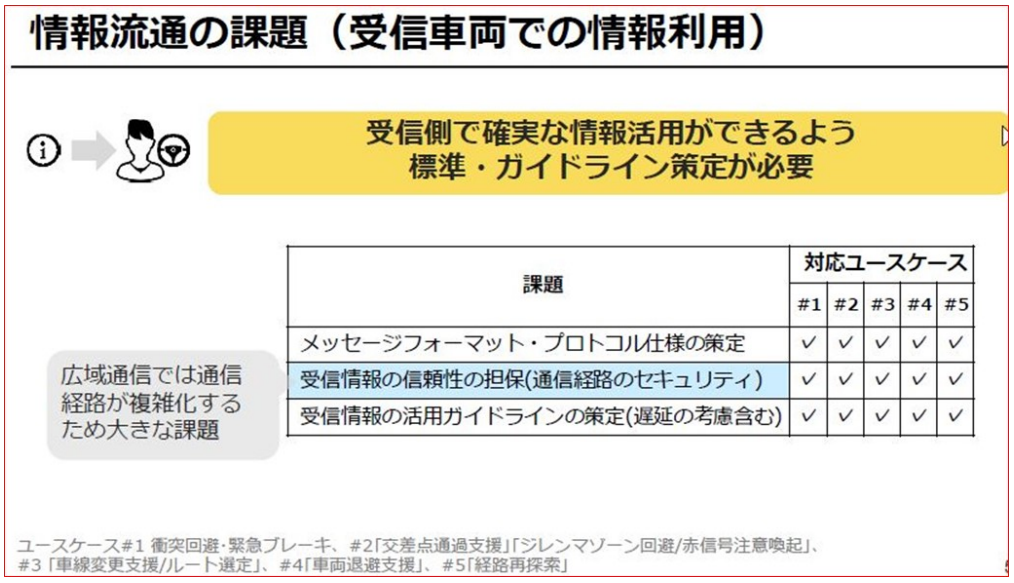
本報告書のなかには、セルラーV2X における情報流通に関するセキュリティ・プライバシの課題を整理している。

具体的には、V2X の 5 つのユースケース（１：衝突回避・緊急ブレーキ、２：交差点通過支援・ジレンマゾーン回避/赤信号注意喚起、３：車線変更支援/ルート選定、４：車両退避支援、５：経路再探索）について、送受される情報に関する課題を整理している（図 5.2.19、図 5.2.20 参照）

図 5.2.18　情報流通の課題（情報入手）


| 観点 | 課題 | 対応ユースケース | | | | |
|---|---|---|---|---|---|---|
| | | #1 | #2 | #3 | #4 | #5 |
| 団体・組織から入手 | 団体・組織から元情報取得の了解獲得 | | ✓ | ✓ | ✓ | ✓ |
| | 情報源から情報取得するシステムの構築(精度・セキュリティなど) | | ✓ | ✓ | ✓ | ✓ |
| | 情報源から情報取得する機器仕様/フォーマット等の規格化 | | ✓ | ✓ | ✓ | ✓ |
| 車両から入手 | メッセージフォーマット・プロトコル仕様の策定 | ✓ | | ✓ | ✓ | |
| | 生成情報の各車両によるばらつきを抑えるためのガイドライン策定 | ✓ | | | ✓ | |
| | セキュリティ・プライバシー対策 | ✓ | | ✓ | | |
| | 各車両所有者から情報使用に関する同意獲得 | ✓ | | ✓ | | |

図 5.2.19　情報流通の課題（受信車両での情報利用）




| 課題 | 対応ユースケース | | | | |
|---|---|---|---|---|---|
| | #1 | #2 | #3 | #4 | #5 |
| メッセージフォーマット・プロトコル仕様の策定 | ✓ | ✓ | ✓ | ✓ | ✓ |
| 受信情報の信頼性の担保(通信経路のセキュリティ) | ✓ | ✓ | ✓ | ✓ | ✓ |
| 受信情報の活用ガイドラインの策定(遅延の考慮含む) | ✓ | ✓ | ✓ | ✓ | ✓ |

5.2.2.5. ITU-T

ITU-T においては、Study Group 16（SG16: Multimedia）における課題 27（Vehicle gateway platform for telecommunication/ITS services and applications）において Connected Vehicle の通信に関わる標準化を行っており、Study Group 17（SG17: Security）の課題 13（Security aspects for Intelligent Transport System）において、Connected Vehicle やその通信システムに関わるセ

キュリティの標準化を行っている。本節では、SG17 課題 13 の活動状況と勧告化された文書の内容について説明する。

5.2.2.5.1. SG17 課題 13 で作成された勧告文書、および、議論中のワークアイテム

表 5.2.13　勧告一覧に SG13 課題 13 において作成され、勧告として発行された文書を示す。

表 5.2.13　勧告一覧

| 勧告番号 | タイトル | 概要 |
|---|---|---|
| X.1373 | Secure software update capability for intelligent transportation system communication devices | 車両に搭載された電子機器のソフトウェアを安全に更新するための手順について規定 |
| X.1372 | Security guidelines for Vehicle-to-Everything (V2X) communication systems | V2V（Vehicle-to-Vehicle）、V2I（Vehicle-to-Infrastructure）、V2D（Vehicle-to-nomadic Devices）、V2P（Vehicle-to-Pedestrian）の通信を対象としたセキュリティガイドライン。V2X 通信の脅威（盗聴、パーソナル情報の漏洩､信用情報／センサー情報／アプリケーションの改ざん、DoS 攻撃、デバイスハッキング、不正アクセス等の脅威を列挙し､これらに対応するためのセキュリティ要件と対策を提示している。 |

表 5.2.14 に、SG13 課題 13 で議論中（2020 年 3 月現在）のワークアイテムを示す。

表 5.2.14　ワークアイテム一覧

| 識別名 | タイトル | 概要 |
|---|---|---|
| X.itssec-3 | Security requirements for external device with vehicle access capability | リモート・キーレス・エントリーや検査ツール等の車両に接続する外部機器のセキュリティ要件を規定した文書。外部機器接続によるセキュリティ上の脅威を列挙し、一般的なセキュリティ要件とともに、ワイヤレス機器（Bluetooth、モバイル、WiFi)、リモート・キーレス・エントリー、充電システムに対するセキュリティ要件を規定している。 |
| X.itssec-4 | Methodologies for intrusion detection system on in-vehicle system | 車両内のネットワーク（CAN 等）上での不正な振る舞いを検知する侵入検知システムの適用方法について規定する文書。標準的な侵入 |

| | | |
|---|---|---|
| | | 検知システムのフレームワークや検知手順を示すとともに、ネットワーク上において脅威となる挙動（盗聴、なりすまし、不正コマンド送付、リプレイ攻撃、等）を示している。 |
| X.itssec-5 | Security guidelines for vehicular edge computing | 車両がエッジ・コンピューティング機能を使う際のセキュリティガイドライン。脅威分析を行うとともに、脅威に対応するためのセキュリティ要件と 3 つのユースケースにおけるセキュリティ上の注意点を示している。 |
| X.stcv | Security threats to connected vehicles | コネクテッド・カーにおけるセキュリティ上の脅威を示すもので、他の ITS セキュリティ関連のリファレンスとして用いられることを想定した文書。コネクテッド・カーのモデルを規定し、そのモデルにおけるセキュリティ上の脅威を列挙している。 |
| X.mdcv | Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles | 多くのコネクテッド・カーから収集したデータ（Big Data）を解析し、その中からセキュリティに関連する不審な挙動を検知する仕組みについて規定した文書。不審な挙動を検知する仕組みのモデルを規定し、収集できるデータの種類と複数の検知方法について説明を行っている。 |
| X.srcd | Security requirements for categorized data in V2X communication | V2X 通信で使われるデータを複数のタイプに分類し、各データタイプのセキュリティレベルを定義する文書。V2X で扱われるデータのライフサイクルについて説明し、データの種類（車両の状態、環境情報、車両制御、アプリケーションサービスデータ、機密データ、等）に対して、セキュリティレベル 1～3 に属するデータ例を提示している。また、分類されたデータに対するセキュリティ要件を規定する。 |
| X.edrsec | Security guidelines for cloud-based data recorders in automotive environment | 車両から得られるデータをクラウドに送付して蓄積する EDR（Event Data Recorder）、DSSAD（Data Storage System for Automated Driving）のセキュリティガイドライン。EDR、DSSAD の特徴から、セキュリティ上の脅威を明確にし、セキュリティ要 |

| | | |
|---|---|---|
| | | 件（セキュア・ブート、ログ、通信の暗号化、アクセス制御、等）を規定している。また、セキュリティを考慮した実装方法についても規定している。 |
| X.eivnsec | Security guideline for Ethernet-based in-vehicle networks | イーサネットをベースとした車両内ネットワークのセキュリティガイドライン。車両向けイーサネットの説明を従来のネットワークとの比較を含めて行い、セキュリティ上の脅威を明確にし、セキュリティ要件（機密性／完全性／可用性／真正性に関連する項目）を規定している。また、セキュリティを考慮したイーサネットの実装についても規定している。 |
| X.fstiscv | Framework of security threat information sharing for connected vehicles | コネクテッド・カーのためのセキュリティ脅威情報を共有するためのフレームワークと共有手順を規定した文書。 |
| X.1373rev | Secure software update capability for intelligent transportation system communication devices | X.1373 の改訂版。UNECE WP29 での検討結果と、OEM ベンダーからの実装に関する意見の反映を目的に改訂作業を行う。 |
| X.ipscv | Methodologies for intrusion prevention systems for connected vehicles | 車内システムへの侵入を防御するための仕組みのフレームワークと攻撃の検知・防御方法を規定する文書。 |
| X.rsusec | Security requirements for road-side units in intelligent transportation systems | V2I（Vehicle-to-Infrastructure）通信で利用される RSU（Road side unit）のセキュリティ要件を規定する文書。RSU の概要とセキュリティ上の脅威を示し、ハードウェア、ファームウェア／OS、アプリケーション、データセキュリティ要件を規定している。 |

#### 5.2.2.5.2. X.1373: Secure software update capability for intelligent transportation system communication devices

この勧告は、ITS（intelligent transportation system）通信機器を対象とした安全なソフトウェア更新手順を提供することを目的としている。ソフトウェア更新の基本的なモデル、ソフトウェア更新のセキュリティ制御、更新ソフトウェアモジュールの抽象データフォーマットの仕様も含まれている。

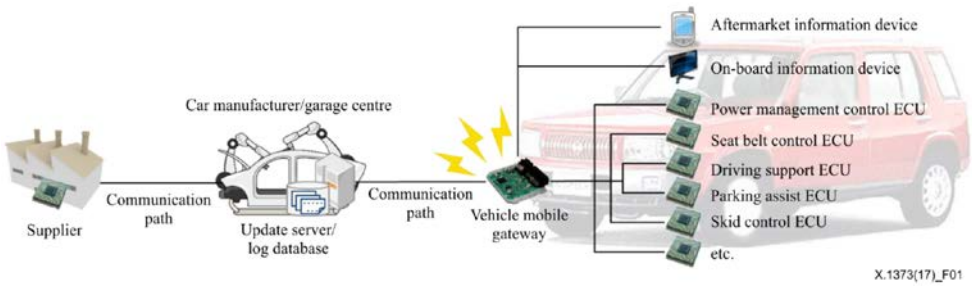



図 5.2.20　車両に組み込まれている基本的なモジュール（勧告文書より）

図 5.2.21 は、車両に組み込まれている ECU 等のモジュールと更新ソフトウェアを提供するサプライヤとの接続形態を示している。更新ソフトウェアは、車両製造会社に渡され、そこから各車両に組み込まれたゲートウェイを介して更新が必要となる ECU 等の機器に送られることになる。

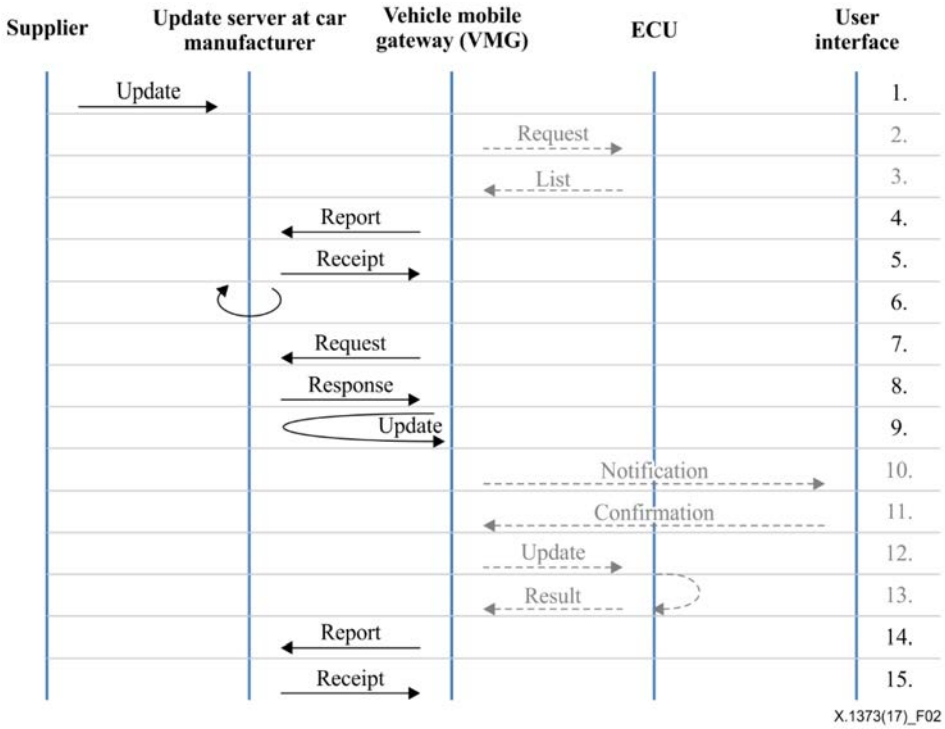



図 5.2.21　ソフトウェア更新プロセスのモデル

図 5.2.22 は、基本的なソフトウェア更新手順のモデルである。このモデルに従ってソフトウェア更新手順の仕様とメッセージフォーマットが規定されている。

5.2.2.5.3. X.1372: Security guidelines for Vehicle-to-Everything (V2X) communication systems

この勧告は、V2X（Vehicle-to-Everything"）通信のセキュリティガイドラインとなっている。V2X 通信には、V2V（Vehicle-to-Vehicle）、V2I（Vehicle-to-infrastructure）、V2D（Vehicle-to-nomadic Devices）、V2P（Vehicle-to-Pedestrian）が含まれている。V2X のセキュリティ上の脅

威、セキュリティ要件、セキュリティ機能を具備した V2X 通信の実装について規定している。脅威については、機密性、完全性、可用性、否認拒否、真正性、責任追跡性、認証の観点で分類されており、それぞれの項目について脅威を列挙している。

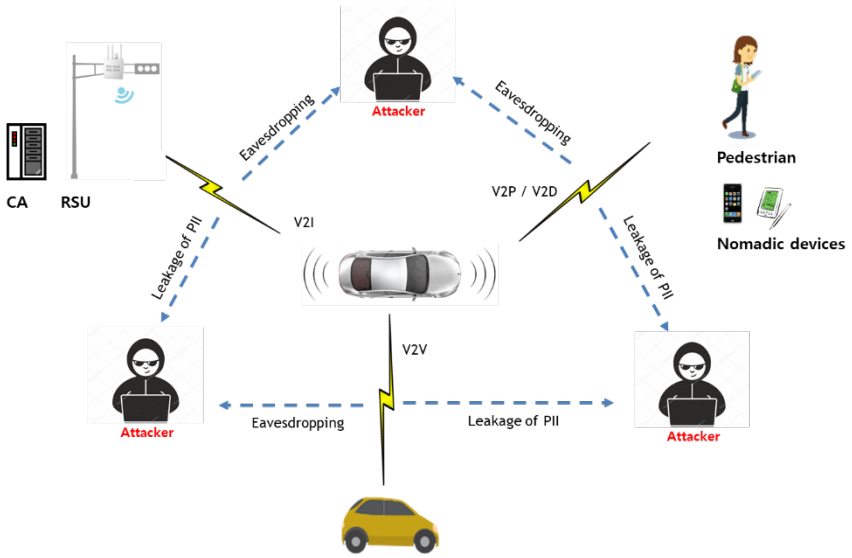



図 5.2.22　機密性に関する脅威

図 5.2.23 は、機密性に関する脅威を示しており、盗聴とパーソナル情報の漏洩が対象となっている。

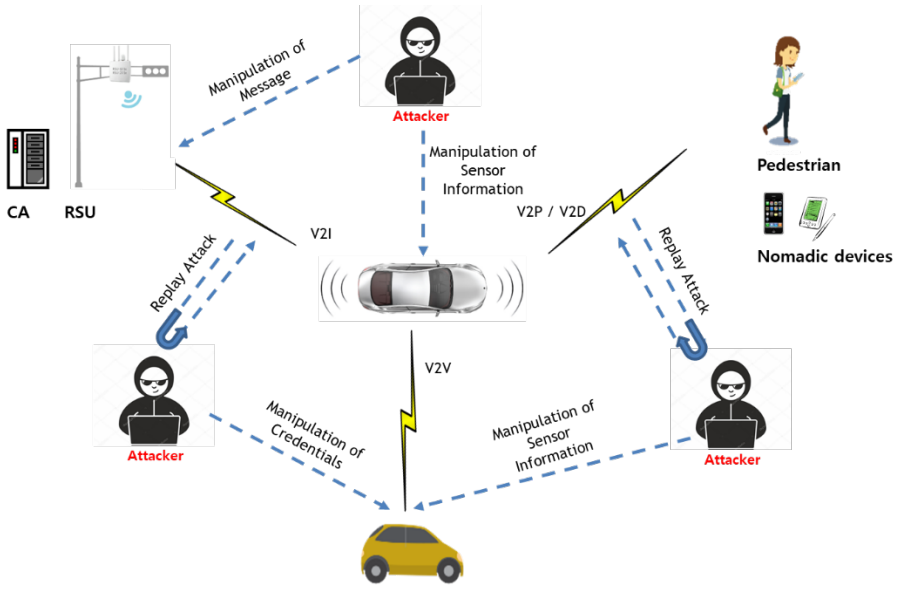



図 5.2.23　完全性に関する脅威

図 5.2.24 は、完全性に関する脅威を示しており、経路メッセージの改ざん、資格情報の改ざん、センサー情報の改ざん、デバイス上のアプリケーションの改ざんが対象となっている。

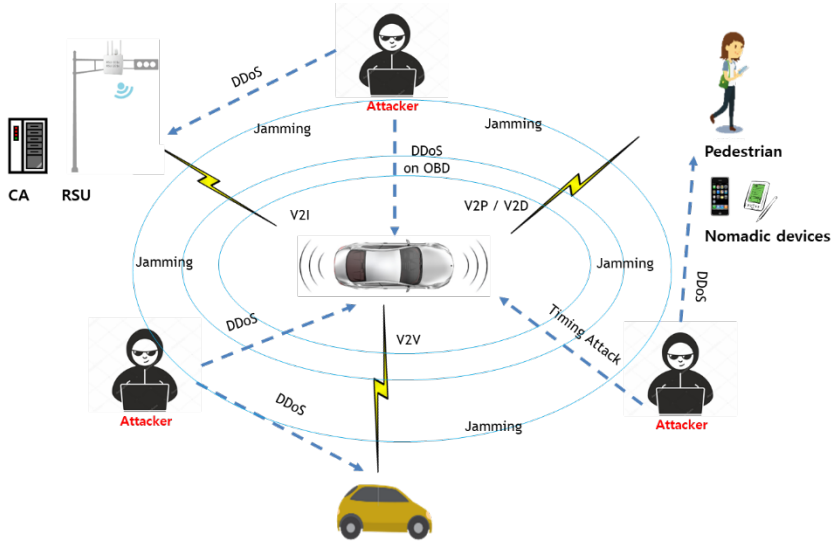



図 5.2.24　可用性に関する脅威

図 5.2.25 は、可用性に関する脅威を示しており、V2X 通信チャネルに対する妨害／DDoS 攻撃、OBU に対する DDoS 攻撃、タイミング攻撃、センサーのハッキングが対象となっている。

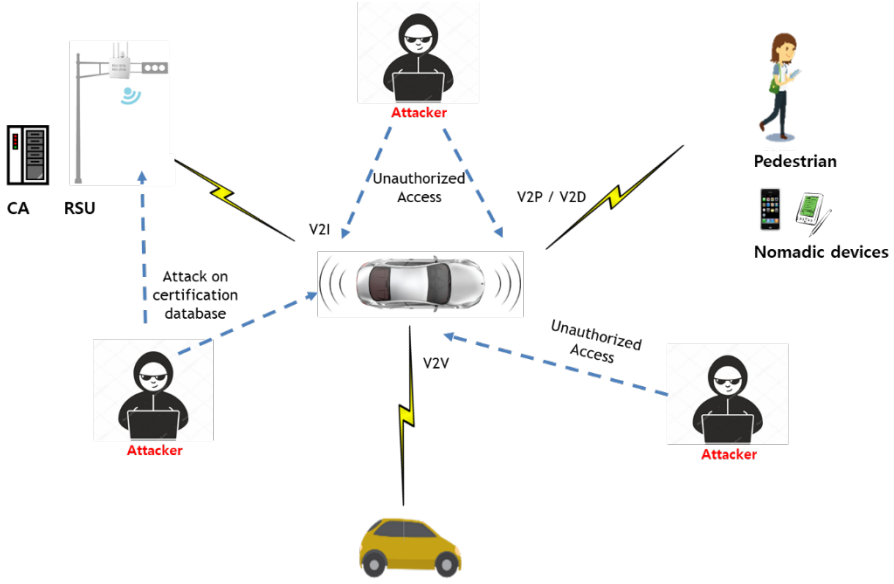



図 5.2.25　否認拒否に関する脅威

図 5.2.26 は、否認拒否に関する脅威を示しており、証明書データベースの改ざん、資格情報への不正アクセスが対象となっている。

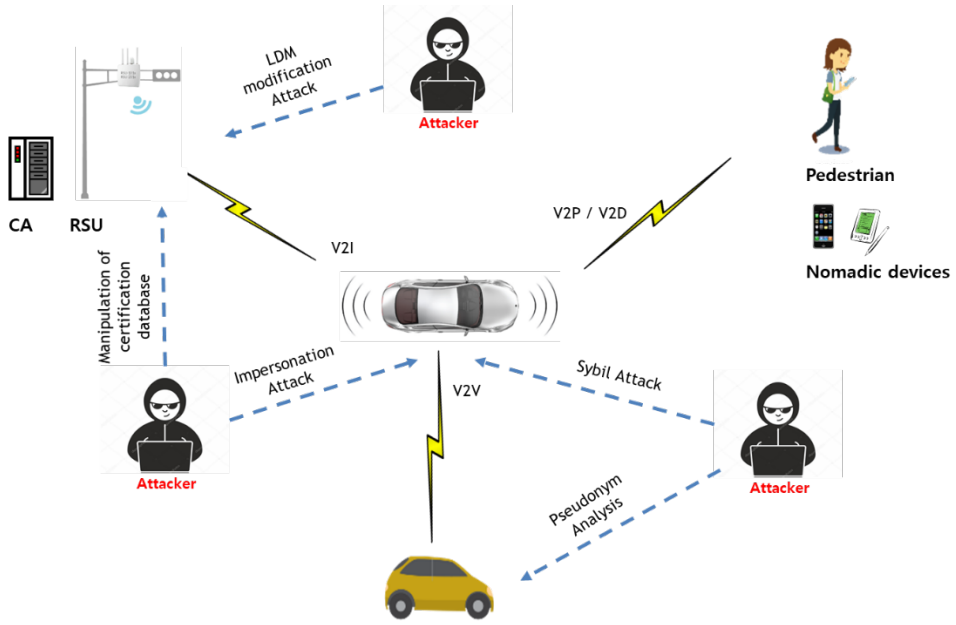



図 5.2.26　真正性に関する脅威

図 5.2.27 は、真正性に関する脅威を示しており、経路テーブル／LDP（Local Dynamic Map）への改ざん攻撃、なりすまし攻撃、Sybil 攻撃（複数 ID 攻撃）、仮名解析攻撃、証明書データベースの改ざんが対象となっている。

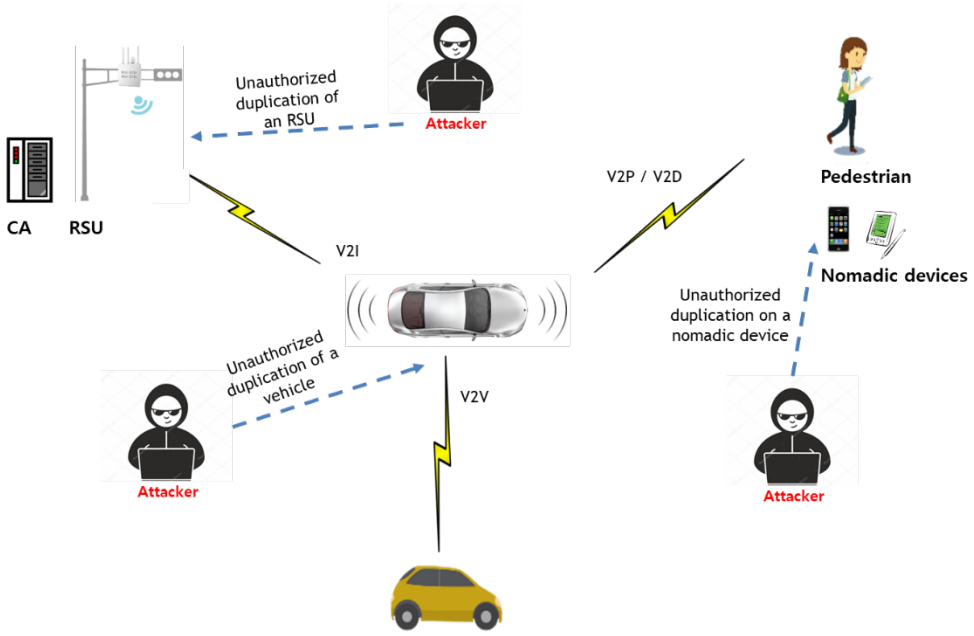



図 5.2.27　責任追跡性に関する脅威

図 5.2.28 は、責任追跡性に関する脅威を示しており、デバイスの不正な複製、車両／RSU の不正な複製が対象となっている。

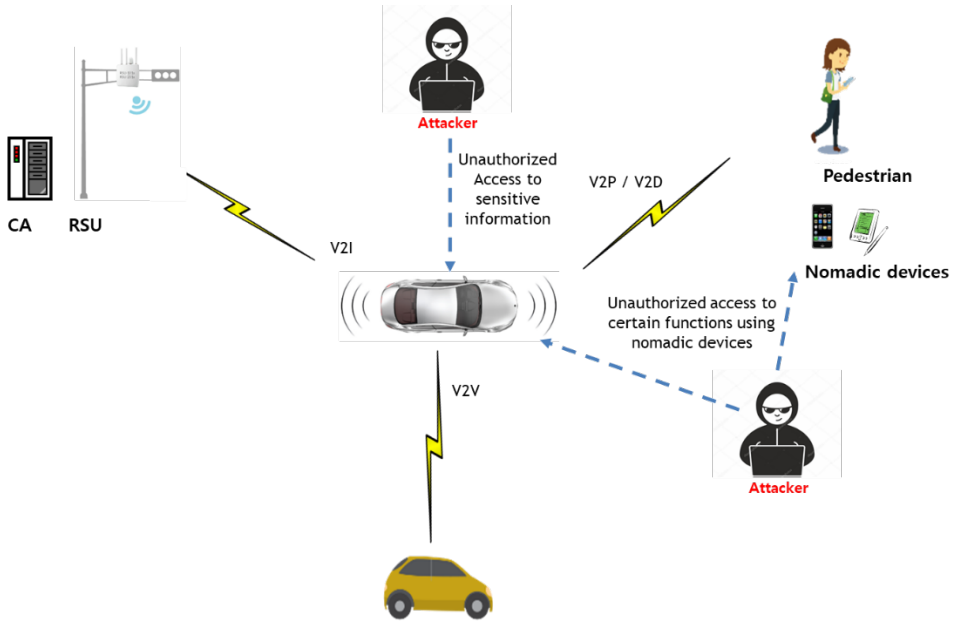



図 5.2.28　認証に関わる脅威

図 5.2.29 は、認証に関する脅威を示しており、車両内の安全性に変わる情報への不正アクセス、車両に組み込まれた機能への不正アクセスが対象となっている。

勧告では、上記の各項目に対応したセキュリティ要件が規定され、V2X 通信に関わるユースケースに対してどのセキュリティ要件への対応が必要となるかが示されている。また、セキュリティ要件に沿った実装を行うための事例として、エンティティ認証とメッセージの機密性確保を目的とした暗号の利用、緊急情報のメッセージの完全性検証、隊列走行におけるエンティティ認証、PKI の利用、の各ユースケースが示されている。

5.2.2.6. TTC（一般社団法人情報通信技術委員会）

TTC においては、セキュリティ専門委員会とコネクテッド・カー専門委員会において車両関連のセキュリティを取り扱っており、セキュリティ専門委員会の関係メンバーがコネクテッド・カー専門委員会に参加し、連携した活動を行っている。本節では、コネクテッド・カー専門委員会で作成を行っている文書について説明する。

5.2.2.6.1. 自動車の遠隔更新技術の標準化動向と実用化課題

テクニカルレポートとして 2017 年 12 月に発行された文書で、この時点における各種団体でのソフトウェアの遠隔更新技術の検討状況、標準化文書の作成状況について説明が行われている。また、2019 年 10 月に、UNECE WP.29 の情報を追加するとともに、更新作業が行われ、第 2 版として発行された。本文書は、一般公開されており、TTC のホームページからダウンロード可能となっている。

車両に搭載された ECU 等のデバイスに搭載されたソフトウェアの更新の作業は、従来は作業車が診断ツールを車両に有線で接続して実施していた。近年、ネットワーク経由で遠隔から（専門作業者を介することなく）ソフトウェア更新する遠隔ソフトウェア更新（OTA リプログラミング）

が注目されており、本文書では、このソフトウェア更新のユースケースに着目し、国内外の政府機関、 学術団体、業界団体、NPO 等での、活動状況に関して調査を行っている。

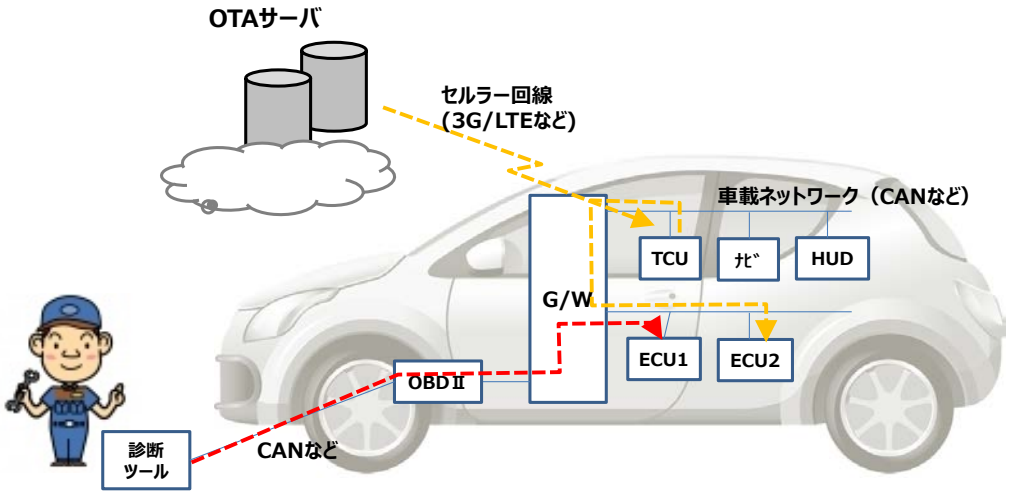



図 5.2.29　リプログラミングの例（レポートより）
（赤色：従来の有線リプログラミング、黄色：OTA リプログラミング）

調査対象とした関連団体は、以下の通りである。

・5GAA（5G Automotive Association）
・ACEA（欧州自動車工業会）
・SAE International（Society of Automotive Engineers）
・UNECE WP.29 GRVA TFCS
・Bluetooth SIG
・IEEE 802
・ISO TC22（Road vehicles）
・ISO TC204（Intelligent transport systems）
・ITS 情報通信システム推進会議（ITS 情報フォーラム）
・ITU-T FG-VM（ITU-T Focus Group on Vehicular Multimedia）
・ITU-T SG16（Multimedia）
・ITU-T SG17（Security）
・oneM2M
・W3C
・Wi-Fi Alliance
・第 5 世代モバイル推進フォーラム（5GMF）
・EVITA（E-safety vehicle intrusion protected applications）
・HIS（The Herstellerinitiative Software）
・TCG（Trusted Computing Group）

5.2.2.6.2. その他

コネクテッド・カー専門委員会では、新たに、自動運転のセキュリティに関わるレポート作成に

着手することとした。これに関連して、2020 年 1 月 31 日に「自動運転に関するセキュリティ課題」と題する勉強会を外部から講演者を招いて実施した。

5.2.2.7. GSMA

モバイル通信関連の業界団体である GSMA では、以下の IoT セキュリティガイドラインを作成し、ホームページを通じて一般公開している。英語以外の言語にも翻訳されており、日本語版も存在する。

- IoT Security Guidelines: Overview Document
- IoT Security Guidelines for Service Ecosystems
- IoT Security Guidelines for Endpoint Ecosystems
- IoT Security Guidelines for Network Operators
- IoT Security Assessment

GSMA では、IoT セキュリティガイドラインの一環として、Automotive IoT Security の取り組みについて検討を開始したが、自動車業界との連携が難しかったことと、賛同者が集まらなかったため、本格的な取り組みへ移行せずに終了した。

GSMA の IoT セキュリティのプロジェクトは、上記の IoT セキュリティガイドラインの作成を含めて様々な取り組みを行っていたが、2020 年 3 月に、活動を中止することとなった。車関連の取組としては、eSIM の活動において、自動車における eSIM 活用の検討が行われており、新たなグループ設立の要否を検討している。(2020 年 3 月時点)

また、GSMA では通信機器のセキュリティ認証フレームワークとして NESAS（Network Equipment Security Scheme） [15]を構築している。NESAS は 3GPP の TS33 シリーズで規定される試験仕様（SCAS：Security Assurance Specifications）に基づく機器試験や、第 3 者監査などにより構成される。

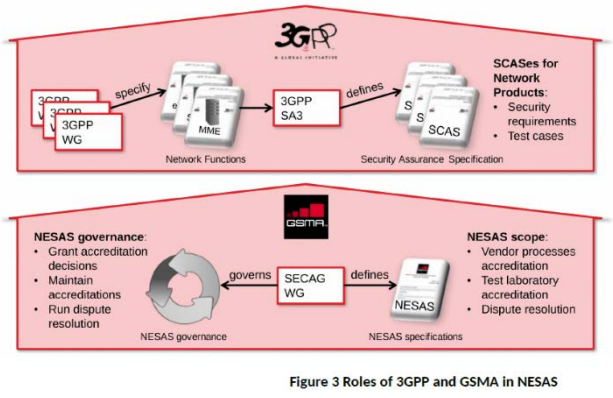



Figure 3 Roles of 3GPP and GSMA in NESAS

図 5.2.30　GSMA　NESAS と 3GPP SCAS の関係

5G ネットワークのセキュリティ確保に向けて、GSMA は NESAS を欧州 ネットワーク情報セキュリティ庁(ENISA)に提案中である [16]。これは、欧州委員会の 5G サイバーセキュリティ対策「EU Toolbox」 [17]を補完するものであり、現在欧州各国は 5G ネットワークのセキュリティ対策の実装を進めているところである。

5.2.2.8. 各標準の関係

本節においては、5.2.2.1～5.2.2.7 節で紹介した各団体およびその活動を要約しその関係性を整理する（表 5.2.15）。

UNECE/WP.29 のサイバーセキュリティタスクフォースでは、クルマあるいはネットワークやクラウドも含むシステムのライフサイクル全般（開発、製品化、製品終了時）にわたるサイバーセキュリティの基本方針、および、具体的なサービスの事例として、リモート環境でのソフトウェアアップデート(リモートリプログラミング、OTA)に関する手順および、セーフティとセキュリティに関する要求条件、更新されるソフトウェアの識別に関するガイダンスとおよびその基本となる Regulation が規定されている。UNECE/WP.29 で規定されるサーバーセキュリティの基本方針は、ISO/SAE 21434 を参照する形となっており、ISO/SAE 21434 は、ISO と SAE が共同開発を行っており、上記 UNECE/WP.29 の基本方針に従い、クルマのライフサイクル全般を通じて、サイバーセキュリティリスク管理の要件、サイバーセキュリティリスクを伝達・管理するためのプロセスと共通言語のフレームワークを規定している。クルマの製造業者や、部品の供給業者（サプライヤ）は、ISO/SAE 21434 に準拠することにより、UNECE/WP.29 のサイバーセキュリティに関する Regulation に従っていることのエビデンスとなる。また、ソフトウェアアップデートについては、ISO/SAE 24089 が Regulation に従う標準の位置づけでとなるが、まだ検討が始まったばかりである。

TC204 は ITS に係る標準化団体であり特に、WG16（通信分科会）および/WG18（協調システム分科会）において、ITS における基地局とクルマの間の通信の規格を対象としている。セキュリティに関しては、通信機器間で実現すべき認証、秘匿などのセキュリティ対策およびプローブ情報のプライバシ保護に関する対策を規定している。

ITS Forum は、ITS 情報通信システムの普及促進を図るため、ITS 情報通信システムに関する研究開発及び標準化の調査研究、関係機関との連絡調整、情報の収集、啓発活動等を行うことを目的とする国内の団体であり、セキュリティに関しては、これまで、運転支援通信システムに関するガイドラインを策定している。

ITU-T では、SG16 課題 27 において Connected Vehicle の通信に関わる標準化 SG17 課題 13 において、Connected Vehicle やその通信システムに関わるセキュリティの標準化を行っている。これまで、リモート環境でのセキュアなソフトウェアアップデートの手順や、V2X におけるセキュリティガイドラインなどの標準化を行っている。

TTC では、セキュリティ専門委員会とコネクテッド・カー専門委員会において車両関連のセキュリティを取り扱っており、セキュリティ専門委員会の関係メンバーがコネクテッド・カー専門委員会に参加し、連携した活動を行っている。

GSMA では、IoT セキュリティガイドラインの一環として、Automotive IoT Security の取り組みについて検討を開始したが、自動車業界との連携が難しかったことと、賛同者が集まらなかったため、本格的な取り組みへ移行せずに終了した。車関連の取組としては、eSIM の活動において、自動車における eSIM 活用の検討が行われており、新たなグループ設立の要否を検討している。（2020 年 3 月時点）

表 5.2.15 各標準の関係

| 団体略称 | 組織説明（階層、関係など） | 概要 |
|---|---|---|
| UNECE/WP.29 | 国連(UN)/欧州経済委員会(ECE)配下の<br>国連自動車基準調和世界フォーラム(WP.29) | 自動車の安全・環境基準の国際調和、政府による自動車の認証の国際的な相互承認などの国際基準［5］ |
| ISO TC22 | 国際標準化機構(ISO) と米国 Society of Automotive Engineers(SAE)によるジョイント組織 | 2016 年 9 月より ISO と SAE が ISO/SAE 21434 を共同開発［5］<br>車両サイバーセキュリティに関する国際標準<br>WP.29 国際基準で参照される見込み |
| ISO TC204 | 国際標準化機構(ISO)配下の技術委員会(TC204) | ITS に係る国際標準を担当<br>自動運転に係る内容は ISO/SAE21434 が主導［18］ |
| ITS Forum | ITS 情報通信システム推進会議 | ITS 情報通信システムの普及促進目的とする国内の団体。ITS を普及・促進するため、各種ガイドラインを策定し公開。 |
| ITU-T SG17 | 国際電気通信連合(ITU)電気通信標準化部門(T) 配下の研究グループ(SG17) | 電気通信に係る国際標準化<br>課題 13 で ITS セキュリティの標準化 |
| TTC | 一般社団法人　情報通信技術委員会(TTC) | 日本国内の情報通信ネットワーク標準化<br>自動車関係のセキュリティについては、動向調査・報告を実施 |
| GSMA | GSM アソシエーション<br>移動体通信事業者や関連企業からなる国際業界団体 | 機器セキュリティ認証フレームワーク NESAS を構築［19］<br>自動車 IoT セキュリティについては現在活動なし |

5.2.3. Connected Vehicle におけるセキュリティ

5.2.3.1. Connected Vehicle におけるセキュリティ要件

5.2.2 章においては、Connected Vehicle に関連する標準について整理を行い、各標準で規定している内容およびそれぞれの標準の関係を明確化し、Connected Vehicle に求められる共通のセキュリティ要件を洗い出した。これらの Connected Vehicle の標準は、クルマやクルマ製造業者を起点に、クルマ内部のセキュリティ要件に加え、路側器やクラウドも含めたエコシステムにおけるセキュリティ要件も対象となっている。すなわち、クルマやクルマ製造業者を起点に、セキュリティの対策方針やセキュリティ管理のための方法論から、Connected Vehicle システムの構成要素である ITS 基地局間でのセキュアな通信サービスやプロトコルに至るまで、非常に広範囲にセキュリティ要件が検討されている。

一方、Connected Vehicle に関わるサービスは、自動走行支援、インフォテイメント、カーライフサポート、エージェントなど様々なユースケースが想定され、これらのサービスのセキュリティを確保するためには、クルマやクルマ製造業者に加えて、Connected Vehicle に関わるサービスを実現するためのステークホルダー、すなわち、サービス事業者、クラウド事業者、通信事業者などに対するセキュリティ要件も考慮する必要がある。例えば、通信事業者に対しては、ISO27011（ITU-T X.1051） [20]、また、クラウド事業者に対しては、ISO27017(ITU-T X.1601) [21]への適合を考慮することにより通信あるいはクラウドサービスにおける安全性が保障される。

本章では、対象とする Connected Vehicle のユースケースを整理し、これらの安心・安全なサービスを実現するためのサービス要件を整理する。次に、In-Vehicle を含まないネットワークとして 5G を用いた場合を想定し、上記サービス要件を満たすための 5G ネットワークの機能を抽出する。さらに次章において、抽出した 5G のネットワーク機能に関するセキュリティの課題を整理する。

5.2.3.3.4. Connected Vehicle のユースケース概要

Connected Vehicle の普及に対しては、移動手段の効率化・高度化を達成することのみならず、従来は自動車が直接的には関係しなかった様々な分野に対して、新たな産業やサービスを創出することにも、大きな期待が寄せられている。したがって、5G 時代に想定される Connected Vehicle 分野のセキュリティ課題を抽出する場合は、はじめに、その検討対象となる分野を明確化することが重要である。

本報告では、Connected Vehicle に関係して提供されるサービスの類型として、総務省主催の「Connected Car 社会の実現に向けた研究会」 [22]が取りまとめた 4 分野に注目して、以降の議論を進めることとする。以下に、その 4 分野を整理する。

- セーフティ分野
  - 道路状況や交通状況などを、車両や運転手に伝達し、必要に応じて警告を発したりすることにより、安全運転を支援するサービス。
- カーライフサポート分野
  - 車両の状態や位置、運転手の運転の特徴などの情報を外部に送信、分析することにより、車両や運転手の状況に合わせたサービスを提供する。
- インフォテイメント分野
  - インターネットへ接続することにより、動画の視聴や VR（仮想現実）など、様々なエンターテイメントを車内に提供するサービス。
- エージェント分野
  - 事故や災害などの緊急時に役立つサービス。

また、ここでは、一般性を損なわない範囲でユースケースを具体化してセキュリティ要件を明確化するため

それぞれのサービスにおいて、総務省の報告書「Connected Car 社会の実現に向けた研究会」において検討されているユースケースについて、セーフティ分野については、運転支援（安全運転支援・自動運転支援・ドライバモニター・高齢ドライバーサポート）（UC-1 とする）を、カーライフサポートについては、車両管理・運行管理・インフラ管理・自動車保険サービス（UC-2 とする）を、インフォテイメント分野については、ネット系エンタメサービス（UC-3 とする）を、エージェント分野については、緊急通報・ロードアシスタントサービス（UC-4 とする）と対象とする。各ユースケースの通信要件や通信形態などは以下の通りである。

| サービス概要（主な特徴） | |
|---|---|
| ユースケース | ・安全運転支援 ・自動運転支援 ・ドライバモニター ・高齢ドライバー支援 |
| 情報内容 | ・周辺車両走行状態 ・車両制御情報 ・ダイナミックマップ ・ドライバー状態 |
| 通信要件 | ・高信頼 ・低遅延 |
| 通信形態 | ・狭域通信 ・広域通信 |
| 課 題 | ・メーカーによらない高信頼かつ低遅延な通信方式の検討（海外との協調を含む）<br>・専用帯域の確保 |

| 時 期 | サービス高度化イメージ | 必要な技術等 |
|---|---|---|
| 現 在 | ・交差点、事故多発地点等において、事故防止につながる運転支援情報をドライバーへ提供 | ・交差点等の特定エリアにて車両や歩行者等の状況をリアルタイムに検知／配信する通信手段（V2I）<br>・周辺車両の走行状況をリアルタイムに収集する通信技術（V2V） |
| 短期 | 情報提供型安全運転支援の高度化<br>－歩行者、自転車等への拡張<br>－ドライバー緊急時への対応<br>－高齢ドライバー支援<br>レベル2～3自動運転の支援<br>－自動運転円滑化のための情報提供<br>－隊列走行内の車両制御情報交換 | ・歩車間通信 ・測位精度向上<br>・ドライバーモニター<br>・自動運転向け協調型システム通信<br>・インフラセンサー高度化（通信器非搭載車へのシステム対応）<br>・自動運転監視/制御への通信活用 |
| 中期 | レベル4以上の自動運転の支援<br>自動運転車両の交通管制 | ・自動運転監視・制御通信<br>・自動運転車両の高度な交通管制 |

図 5.2.31　UC-1: 安全運転支援・自動運転支援・ドライバモニター・高齢ドライバー支援サービスの概要 [22]

| サービス概要（主な特徴） | |
|---|---|
| ユースケース | ・車両管理（故障分析、SWアップデート） ・運行管理（物流や旅客運送における走行ルート探索、配車計画、労務管理 等）<br>・インフラ管理（道路状態の把握 等） ・自動車保険 |
| 情報内容 | ・運行計画/状況 ・交通状況/予測 ・移動要求/需要 ・車両状態 ・ドライバー状態 |
| 通信要件 | ・常時接続 |
| 通信形態 | ・広域通信 ・(一部)スポット通信 |
| 課 題 | ・通信コスト低減 ・プライバシー/セキュリティの確保<br>・リアルタイムかつダイナミックに走行ルート探索や配車計画等を行うAI技術の確立 |

| 時 期 | サービス高度化イメージ | 必要な技術等 |
|---|---|---|
| 現 在 | ・車両位置などの走行状態、映像データを活用した動態管理<br>・定期点検時のデータ収集、故障診断<br>・ドライバーの運転診断<br>・走行時の振動情報（路面の凹凸情報）収集 | |
| 短期 | ・ドライバーの体調管理と連動した運行管理システム<br>・運行状況や交通状況やヒト(旅客)の移動要求/需要などに応じて、リアルタイムかつダイナミックに走行ルートを探索等<br>・車載ソフトウェアのアップデート（不具合修正）<br>・リアルタイムな路面状態の把握 | ・ドライバモニタリング技術<br>・動作履歴による故障予測（センサ情報のクラウド分析） |
| 中期 | ・オンデマンド自動運転車の予約・配車<br>・ヒト(旅客)に加えて、モノ(集荷や配達)の移動要求/需要などに応じて、リアルタイムかつダイナミックに走行ルートを探索等<br>・車載ソフトウェアのアップデート（新機能追加） | ・上記AIの入出力を送受信する常時接続の無線NW(送受信頻度が増加) |

図 5.2.32　UC-2: 車両管理・運行管理・インフラ管理・自動車保険サービスの概要 [22]

③－１　ネット系エンタメサービス

| サービス概要（主な特徴） | |
|---|---|
| ユースケース | ・動画、音楽視聴、オンラインゲーム、仕事 |
| 情報内容 | ・エンタメ情報（動画、音声、画像、オンラインゲーム、等） |
| 通信要件 | ・常時接続　・高スループット |
| 通信形態 | ・広域通信　・一部スポット通信 |
| 課　題 | ・クルマでのインターネット接続需要増加に伴う道路沿いのエリア設計見直し<br>・車載器側のマルチシステム、マルチバンド化 |

| 時　期 | サービス高度化イメージ | 必要な技術等 |
|---|---|---|
| 現在 | 同乗者が動画視聴やゲームをプレイ | スマホやルータ経由でのインターネット接続 |
| 短期 | ライドシェアで移動中に動画、ゲームだけでなく、仕事もするようになる | クルマの通信モジュールを利用した高速インターネット接続 |
| 中期 | 完全自動運転が普及し、ドライバーも移動中に動画、ゲーム、仕事をするようになる | 同上 |

図 5.2.33　UC-3: ネット系エンタメサービスの概要 [22]

| サービス概要（主な特徴） | |
|---|---|
| ユースケース | ・交通事故発生時の緊急通報サービス　・ロードアシスタント |
| 情報内容 | ・音声情報　・センサー情報　・ドライバモニタリング情報 |
| 通信要件 | ・常時接続 |
| 通信形態 | ・広域通信 |
| 課　題 | ・ドライバモニタリング技術<br>・ＡＩによる情報分析技術 |

| 時　期 | サービス高度化イメージ | 必要な技術等 |
|---|---|---|
| 現在 | ・エアバッグ作動時に緊急通報を実施 | |
| 短期 | ・衝突前後の詳細なセンサー情報の送信<br>・ドライバーの体調不良時の対応 | ・ＡＩによる情報分析技術<br>・ドライバモニタリング技術 |

図 5.2.34　緊急通報・ロードアシスタントサービスの概要 [22]

（1）ネットワーク要件

ここでは、UC-1～UC-4 について、それぞれ求められるネットワークの要件を整理する（表 5.2.16 参照）。

表 5.2.16　各種ユースケースとネットワーク要件

| | 用途 | ネットワーク要件 |
|---|---|---|
| UC-1 | ダイナミックマップ | 高スループット、スポット |
| | 車両制御情報 | 低遅延　常時接続 |
| | ドライバ状態 | 常時接続 |
| | 周辺車両走行状態 | 低遅延　境域通信（V2X） |
| UC-2 | 運行計画/状況、交通状況/予測 | 常時接続、スポット |
| | 移動要求/需要、車両状態、ドライバー状態 | 常時接続 |
| UC-3 | 動画視聴 | 高スループット、常時接続 |
| | オンラインゲーム | 低遅延 |
| UC-4 | 音声情報、センサー情報、ドライバモニタリング情報 | 常時接続 |

UC-1 のダイナミックマップの地図情報、自動走行支援のための車両制御情報、あるいは、動画情報などのデータ量に関して表 5.2.17 に示す [23]。動画、静止画、ECU データいずれも、ネットワーク上を多量のデータが流れるため MEC などを利活用した効率的な転送技術が必要となる。

表 5.2.17　Connected Vehicle におけるサービスで転送されるデータ量

| System Requirements * | | V2Cloud cruise assist | High-resolution map generation & distribution | Intelligent driving |
|---|---|---|---|---|
| Major Data Source | | Video Stream | Still Image (road surface image) | ECU data |
| Data Generation in vehicle | | ~ 1215EB/month[1] | ~ 375EB/month[2] | ~ 22.5EB/month[3] |
| Target Data Traffic Rate | | ~ 10EB/month in total (cost constraint might limit this number) | | |
| Response Time | Uplink | < 10 seconds | < 1 week | < 1 week |
| | Downlink | < 10 seconds | < 1 week | < 10 minutes |
| Required Availability | Uplink | Continuous | Occasional | Occasional |
| | Downlink | Continuous | Occasional | Continuous |

* - The numbers in Table 1 are total values for 100 million connected cars.

表 5.2.18 は、各種 V2X サービスにおけるネットワーク要件を表す。遅延についてはデータの授受に基づき自動的に運転制御される自動運転が 1 ms と低遅延に関して最も厳しい条件が要求される。また、遠隔運転については、人がリアルタイム操作性を損なわない程度の遅延処理として 20ms 以下が要求される。さらに、表 5.2.19 は、インフォテイメント分野におけるコンテンツ視聴やオンラインゲームに対するネットワーク要件を表す。特に、マルチプレーヤによるオンラインゲームにおいては、7.5ms 以下の応答性が要求される。

表 5.2.18　　V2X サービスにおけるネットワーク要件 [24]

| サービス | 通信形態 | 遅延 | スループット | 信頼性 |
|---|---|---|---|---|
| 安全と交通制御 | V2V, V2P | 100 ms | - | 未定義 |
| 自動運転 | V2V, V2N, V2I | 1 ms | 10 Mbps (DL/DL) | ほぼ100% |
| 遠隔運転 (TeSo) | V2N | 20 ms (end-to-end) | 25 Mbps (UL:ビデオ・センサーデータ) 1 Mbps (DL:アプリのコマンド制御) | 99.999% |
| インターネットとインフォテイメント | V2N | 100 ms (ウエブ閲覧) | 0.5 Mbps (ウエブ閲覧) 15 Mbps (高精細ビデオストリーミング) | - |
| 遠隔診断および管理 | V2I, V2N | - | - | - |

表 5.2.19　インフォテイメント分野　UC-3 でのネットワーク要件 [25]

| サービス | エンドユーザの平均スループット | 遅延（エンド—エンド） | 遅延 (無線区間) |
|---|---|---|---|
| 高精細ビデオ　8K (ストリーミング) | < 100 Mbps (DL) | < 1 s | < 200 ms |
| 高精細ビデオ (conversational) | < 10 Mbps (DL/UL) | < 150 ms | < 30 ms |
| クラウドコンピュータゲーム 4K 3D graphics | < 50 Mbps (DL/UL) (ULは、マルチプレーヤゲームで必要 | < 7.5 ms | < 1.5 ms |

その他、自動追い越しシステムでは、各メッセージ交換で約 10 ms 以下の応答性が必要とされる [26]。5G の URLLC における無線部分のネットワーク遅延は 1ms を想定しているが、上記のユースケースにおいては、エンド—エンドで 1ms～20ms 程度のリアルタイム応答性を実現する必要がある。このため、URLLC のセキュリティで検討される認証の高速化や MEC の利活用など 5G の機能を活用することにより上記のネットワーク要件を考慮する必要がある。

（2）セキュリティ要件

上述の Connected Vehicle サービスにおけるセキュリティ要件について考察する。ここでは、個別のユースケースの要件の考慮しつつ、ユースケース共通のセキュリティ要件を整理する。

まず、サービスレイヤでの下記のセキュリティ要件の明確化を目的として、クルマ、ネットワーク、クラウド、そして、サービスアプリケーションを対象として、その脅威を整理する。

サービスレイヤでの脅威

サービス利用者のなりすまし
サービスで利用されるのデータへの不正アクセス
サービス上のデータの漏洩
サービス上のデータの改ざん
サービスへの DoS 攻撃
マルウェア感染

ここでは、上記のサービスレイヤでのセキュリティ脅威を踏まえ、サービスを構成するクルマ、クラウド、ネットワークのシステム構成に対する各々セキュリティ要件を明確化し、その後、5G ネットワークを想定した場合の着目すべきセキュリティ機能とそのセキュリティ課題を整理する。

- なりすましによる不正なサービス利用

利用者が契約している Connected Vehicle に関するサービスを不正に利用することにより不当

な利益をえる。事例としては、インフォテイメントサービスにおけるコンテンツ視聴やオンラインゲーム(UC-3)、交通事故情報などの緊急通報サービス（UC-4）などの不正な利用が想定される。これらの脅威は、クルマの利用者へのなりすましにより実現の可能性がある。

この対策として、サービスレベルの利用者の認証が必要となる。

- クラウド、クルマに蓄積されたデータを改ざん

Connected Vehicle サービスにおいて利用され、蓄積されるデータを不正にアクセスし、改ざんすることにより、不当な利益を得る、あるいは、他人に損害を与える。事例としては、自動車保険サービスの運転履歴を改ざんし、保険の料率を変更する（UC-2)、ダイナミックマップにおけるハザードマップを不正に改ざんに他のクルマに事故を誘発させる(UC-1)。車両管理（ソフトウェア更新）における脆弱性のあるソフトウェアや不正な処理を挿入したソフトウェアを更新させる(UC-2)。

これらの脅威は、クラウド、クルマに不正にアクセスして、データを改ざん、あるいは、ネットワーク上の転送される関連データを改ざんすることにより実現の可能性がある。

この対策として、クラウドや車に蓄積されるデータや、ネットワーク上を流れるデータに対して改ざん検知コード（メッセージ認証子）を付与する方法がある。

- クラウド、クルマに蓄積されたデータ、ネットワーク上のデータを盗聴して不正入手

Connected Vehicle サービスで利用されるデータを不正にアクセスし、奪取する。あるいは、ネットワーク上を転送されるデータを盗聴することにより、不当な利益を得る、あるいは、他人のプライバシを侵害する。事例としては、ドライバーモニター(UC-1)や車両運行管理(UC-2)におけるクルマの移動情報を不正に入手する。これらの脅威は、クラウドや、クルマにへの不正アクセス、ネットワーク上のデータの盗聴により可能となる。

この対策として、クラウドやクルマに蓄積されるデータや、ネットワーク上を流れるデータを暗号化する手法がある。

- クラウド、クルマ、ネットワークに過負荷をかけて、サービス停止（DoS 攻撃）

Connected Vehicle サービスを実現するシステム（クラウド、クルマ、ネットワーク）に大量のトランザクション（処理）を発生させることにより、サービスを停止させる。すべてのユースケース（UC-1～UC-4）に対して、DoS 攻撃は想定されるが、サービス自体を停止される脅威と、特定のクルマのサービスを停止させる脅威など、攻撃者の狙いにより、攻撃対象が変わる。この対策として、攻撃の対象となる通信路を監視して、DoS を検知し、該当トラフィックを破棄する手法がある。

- マルウェア感染、不正アクセスによるサービスへの攻撃

不正なプログラムをクラウド、クルマ、ネットワークのシステムに感染させ、動作させることにより、上記の攻撃につながるような攻撃者の意図する任意の動作をさせる可能性がある。また、クラウド、クルマに不正にアクセスすることによりシステムの構成や設定を変え、様々な攻撃が可能となる。

この対策として、マルウェアを検知する機能を導入する、あるいは、不正アクセスに対しては、アクセス管理を行う手法がある。

- クラウド、クルマが連携して動作するサービスの仕様や実装の不備による脆弱性に対する攻撃

  Connected Vehicle サービスの UC-1～UC-4 に対して、各々のサービス仕様に対する不備や実装するユースケースを実現するハードウェア・ソフトウェアの実装の不備による脆弱性が、悪用される、あるいは、設定ミスなど誤用の可能性がある。例えば、個人データに対するアクセス制限が不十分なため、利用者が、他の利用者のプライバシ情報を取得できる、あるいは、サービス利用の履歴を変更できるなど脅威が想定される。

  この対策として、ソフトウェア設計、開発プロセスにおいて、不正プログラムや仕様の不備を排除するための開発プロセスを導入する。

上記のセキュリティ要件に対して、WP29 のクルマに対するサイバーセキュリティにおける脅威との関係を
表 5.2.20 に示す。上記の表では、各セキュリティ要件に対する WP29 Proposal for a Recommendation on Cyber Security の対応する節を記載している。WP29 では、これらの脅威に対する具体的な対策例を Annex A に規定する。

表 5.2.20　Connected　Vehicle サービスのセキュリティ要件と WP29 で規定された脅威との関係

| Connected Vehicleサービスのセキュリティ要件 | 原因となる脅威(WP29参照) |
|---|---|
| なりすましによる不正なサービス利用 | 4.3.1(a)(b)(c), 4.3.2(a)(c)(d)(f), 4.3.6(b)(c)(d) |
| クラウド、クルマに蓄積されたデータを改ざん | 4.3.1(a), 4,3,2(b), 4.3.5(a), 4.3.6(a)(b)(c)(d) |
| クラウド、クルマに蓄積されたデータ、ネットワーク上のデータを盗聴して不正入手 | 4.3.1(a), 4.3.2(c)(h), 4.3.6(a)(b)(c)(d)(f) |
| クラウド、クルマ、ネットワークに過負荷をかけて、サービス停止（DoS攻撃） | 4.3.2(e), 4.3.5(c) |
| マルウェア感染、不正アクセスによるサービスへの攻撃 | 4.3.1(a), 4.3.2(g), 4,3.5(b) |
| ユースケースの仕様や実装の不備による脆弱性に対する攻撃 | 4.3.4(a), 4.3.6(c)(d) |

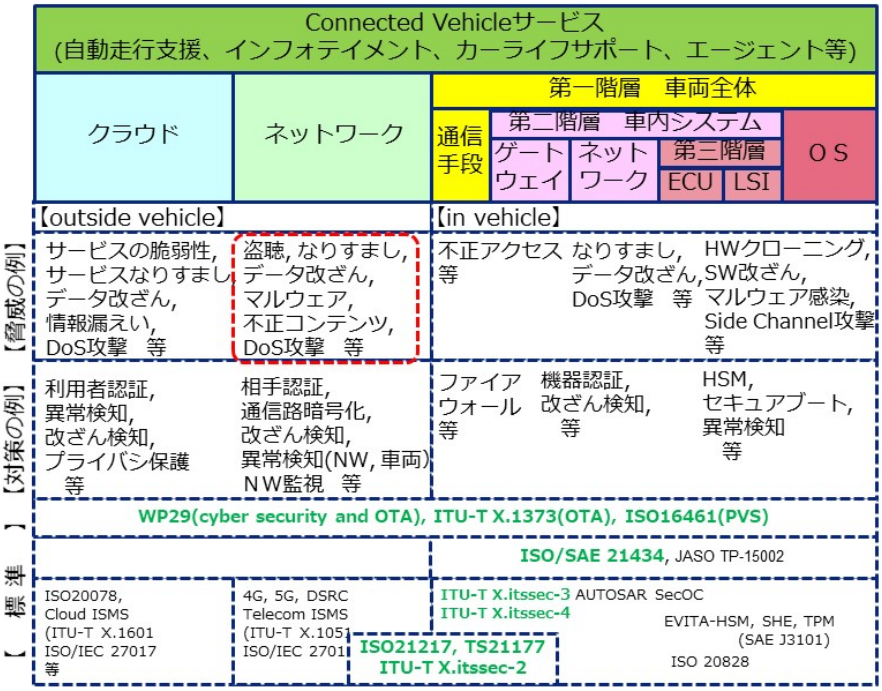



図 5.2.35　Connected Vehicle のシステム全体とその脅威、対応する標準の関係図

5.2.3.3.5. UC-3:インフォテイメント分野のディジタルコンテンツに関するセキュリティ課題

インフォテイメント分野のユースケースにおいては、動画、音声、ゲームなどのエンタメ情報が利用される。ディジタルコンテンツについては情報自体の扱いと、その配信方法が含まれるが、付加価値の高いコンテンツが扱われるため、前者のディジタルコンテンツ自体に対して、コンテンツの盗聴や不正コピーなどの不正利用に対するセキュリティ対策が課題となる。上記の課題を解決するために、DRM 技術の利用が想定される。DRM 技術については、ネットワークに依存しないサービスレイヤの技術であり、後述の 5G とは独立しているため、本節においてその課題を整理する。

DRM は不正なディジタルコンテンツの複製、変更などの防止を目的として、インターネット上でプレミアムデジタルコンテンツを配信するためのよく知られた技術である。DRM は暗号技術ではなく、デジタル権利管理システムの略である。 DRM の要点は、許可された人物/デバイスのディジタルコンテンツの使用規則を記述する。

前述の通り、DRM は WAN（LTE / 5G）/ WiFi などのベアラに依存しない。すなわち、DRM はベアラの機能を使用しない。もちろん、コンテンツの所有者やプロバイダーがコピーを防止したい場合は、暗号化技術が使用される。 このような使用法は、許可された各人物/デバイスの各 DRM スキームの「ライセンス」データで定義される。 DRM は多くの特許と方法で実現されているので、図 5.2.37 は概念のみを示す。

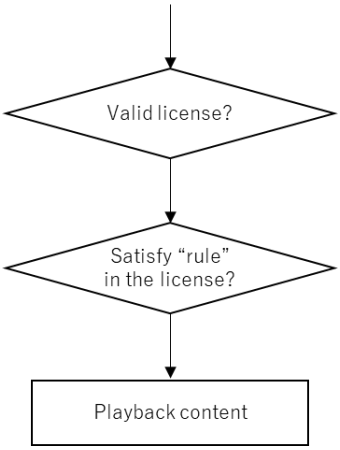



図 5.2.36 プレイバックのフロー

Google の Widevine DRM、Microsoft の PlayReady、Apple の FairPlay、Marlin Trusted Management Org の Marlin など複数の DRM 規格が存在する。コンテンツプロバイダーやアグリゲーターは通常、サービスに 1 つの DRM テクノロジーを使用する。 すなわち、クライアントシステム（プレーヤー）がサービスに接続するために DRM をサポートする必要がある。 Car OEM が複数のコンテンツサービスのサポートを希望する場合、Car OEM はいくつかの DRM テクノロジーを実装する必要がある。

通常、DRM テクノロジーは、DRM ライセンサーとライセンス契約により提供される。 ライセンス契約では、ライセンサーは、DRM で保護されたコンテンツ（DRM 処理されたコンテンツ）を処理/再生するために、RR および CR に従うようライセンシーに要求するケースがある。

RR (Robustness Rules)

RR はロバストネスルールの略である。 RR は、DRM 保護されたコンテンツプレーヤーとしてのクラッキングアクティビティを防止するためにはハードウェアとソフトウェアを準備する方法を記載している。 例えば 安全なメディアパスを使用することにより、復号化およびデコードされたビデオデータを処理し、ビデオデータを盗聴するためのデバッガーによるアクセスを防止する。

CR (Compliance Rules)

CR はコンプライアンスルールの略である。 CR は、データが DRM 保護されたコンテンツプレーヤーからモニターを含む他のデバイスに送信される場合のデータの処理方法を記載している。 HDCP は、HDMI および WiFi ディスプレイのコンテンツ保護技術として知られている（本技術は「リンク保護」と呼ばれることもある）。 CR では、DRM 保護されたコンテンツプレーヤーに対して、リンク保護テクノロジーの機能が必要になる場合がある。

Production

DRM ライセンサーは、より強固な DRM スキームを実現するために、工場で各 DRM 保護された機器にデバイス固有の鍵を事前設定するようにライセンシーに依頼することがある。工場での

主要な処理フローも RR で定義される。

Service
コンテンツホルダー/アグリゲーターが OEM に、RR / CR および再生品質を直接満たす方法を示すよう依頼する場合がある。 これは、CR / RR を満たすだけでは十分な OEM ではないことを意味する。
スマートフォンのようなモバイルデバイスの場合、DRM により管理されるコンテンツのオフライン再生用のストリーミングとキャッシュなどの使用は非常に簡易になってきている。主なサービスが昨今ではネット上で「ストリーミング」されているためである。ほとんどの DRM スキームには認証スキームがあるが、ユーザ認証は含まれていないため、ユーザは DRM 機能を使用してサービスにログインし、デバイスをサービスに紐づける必要がある。

For Car
特にヘッドユニット（DRM による管理されるコンテンツのレシーバー）からバックヘッドのスクリーンなどの AV 信号処理には、標準バスの使用が推奨される。それ以外の場合、各自動車 OEM は、コンテンツホルダー/アグリゲーターと独自のテクノロジーについて交渉する必要が生じる。
自動車 OEM は、どのユーザ認証方式を採用するかを考慮する必要がある。例えば、モバイルデバイスで用いられる ID /パスワードや SIM 認証システムを使用してサービスにログインできる。

5.2.3.3.6. Connected Vehicle における 5G セキュリティの検討対象
5G におけるセキュリティは、無線アクセス（RAN）およびコアネットワーク（CN）において、その仕様が 3GPP SA3 において検討されている。
本節では、前節のネットワーク要件を実現するための以下の 5G 機能について検討対象を明確化し、その 5G 機能に対して、前節で明確化したセキュリティ要件を踏まえ課題を整理する。

- トラストモデル
  前節のユースケースにおいては、Connected Vehicle のサービスの利用者、サービス事業者、クルマ製造業者、ネットワーク事業者など異なる役割を持った様々なプレーヤが想定される。これらの 5G は、プレーヤがどのような信頼関係を構築するかを明確化する必要がある。

- Network Slicing
  前節のユースケースにおいて、異なるネットワークの品質が要求される。5G においては、ネットワークスライシングにより、5G の共通基盤上で、RAN および NC において、品質の異なるネットワークを複数提供可能である。この際、ネットワークスライシングにおいて、前節のセキュリティ要件を考慮した課題を明確化する必要がある。

- MEC

前節の高いスループットや低遅延を実現するためには、MEC（Mobile Edge Computing/Multi-access Edge Computing）により、コンテンツのキャッシュによるネットワーク負荷の軽減、処理をエッジで行うことによる遅延の低減を実現できる。この際、MEC において前節のセキュリティ要件を考慮した課題を明確化する必要がある。

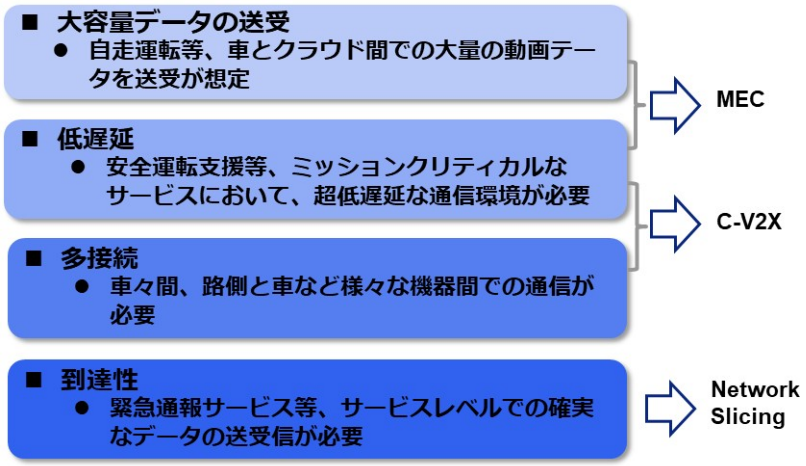
- C-V2X

走行支援などのユースケースを実現するためには、車車間、路車間などの多数の機器との通信を行う必要があり、5G においても C-V2X の利用が想定される。この際、C-V2X において前節のセキュリティ要件を考慮した課題を明確化する必要がある。

- 認証・認可

上記トラストモデルにおけるサービスの利用者、サービス事業者、クルマ製造業者、ネットワーク事業者に加え、ネットワークスライスの提供者や、MEC 上のサービス事業者、C-V2X のサービス提供者などサービスレベルでの認証・認可の課題を明確化する必要がある。

図 5.2.37　Connected Vehicle のネットワーク要件に基づく 5G 機能




5.2.3.2. トラストモデル

Connected Vehicle サービスの実現においては、様々なプレーヤが関与することが想定される。ここでは、前節で選択した 4 つのユースケースにおいて、サービスレベルからの視点でそれぞれのプレーヤ間や、そこで扱われる様々なデータに関する信頼関係について整理する。

Connected Vehicle サービスにおいては、利用者、クルマ、ネットワーク、クラウドがプレーヤとなる。WP.29 のサイバーセキュリティ対策の観点からは、通信チャネルに対する攻撃を想定した対策としては、それぞれのプレーヤ間での信頼関係の確立し、セキュアな関係（コネクション）を確立する。信頼関係を構築する対象としては、接続先の相手(Peer Entity)及び、そのプレーヤ間で授受されるデータとなる（図 5.2.39 参照）。

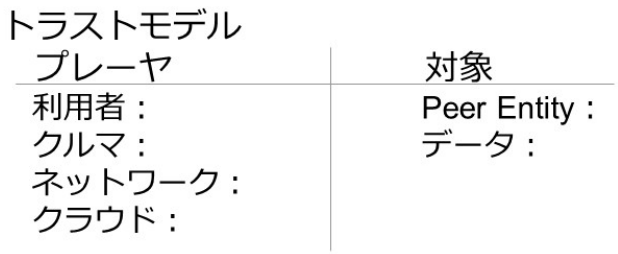



図 5.2.38　トラストモデル

表 5.2.21　ユースケースで授受される情報

| | データの内容 |
|---|---|
| UC-1 | 周辺車両走行状態・車両制御情報・ダイナミックマップ・ドライバー状態 |
| UC-2 | 運行計画/状況、交通状況/予測、移動要求/需要、車両状態、ドライバー状態 |
| UC-3 | エンタメ情報（動画、音声、画像、オンラインゲーム等） |
| UC-4 | 音声情報、センサー情報、ドライバモニタリング情報 |

ここで、各プレーヤ間は、Connected Vehicle サービス形態に固有の信頼関係を構築する。
利用者は、クルマの所有者、あるいはその家族、レンタルでの利用者、カーシェアリングでの利用者などが想定される。前提としては、Connected Vehicle サービスは、クルマが具備する機能によって利用可能なサービスが決定される。例えば、一般的に高級なクルマは、付加サービスが豊富である。すなわち、Connected Vehicle サービスは、利用者ではなくクルマに紐づくサービスと考えるのが現実的である。
このようなビジネスモデルを前提とした各プレーヤの信頼関係は以下の通りである。

・利用者によるクルマの認証
　クルマ製造業者は、社会的な信頼性があり、現在、利用者がクルマの信頼性を確認する必要性が見出されていない。
・利用者によるネットワーク認証
　Connected Vehicle サービスでは、クルマがネットワークを認証するため、利用者がネットワークを認証する必要はない。
・利用者によるクラウドサービスの認証
　Connected Vehicle サービスでは、クルマがクラウドサービスを認証するため、利用者がネットワークを認証する必要はない。
・クルマによる利用者の認証
　現在、利用者の認証は物理的な鍵（キー）により行われるが、自動車保険サービスなど、今後、ドライバーを識別したサービスも想定されるため本人を確認する技術も想定される。
・クルマによるネットワークの認証
　Connected Vehicle サービスでは、クルマがネットワークを認証するため、利用者がネットワークを認証する必要はない。（インフラによっては認証できないケースもある）
・クルマによるクラウドサービスの認証

Connected Vehicle サービスでは、クルマが提供するサービスと想定されるため、クルマがクラウドサービスを認証

・ネットワークによる利用者の認証

Connected Vehicle サービスでは、ネットワークは、接続されるクルマを認証するため利用者の認証は不要

・ネットワークによるクルマの認証

Connected Vehicle サービスでは、ネットワークは、接続されるクルマを認証する

・ネットワークによるクラウドサービスの認証

Connected Vehicle サービスでは、ネットワークは、接続されるクラウドサービスを認証する

・クラウドによる利用者の認証

Connected Vehicle サービスでは、クラウドは、接続されるクルマを認証するため利用者の認証は不要

・クラウドによるクルマの認証

Connected Vehicle サービスでは、クラウドサービスは、接続されるクルマを認証する

・クラウドによるネットワークの認証

Connected Vehicle サービスでは、クラウドがネットワークを認証する。（インフラによっては認証できないケースもある）

これらの信頼関係を表 5.2.22 にまとめる。

表 5.2.22　各プレーヤの信頼関係

| | 利用者 | クルマ | ネットワーク | クラウド |
|---|---|---|---|---|
| 利用者 | | Trust | Indirect trust | Indirect trust |
| クルマ | Don't trust | | Don't trust | Don't trust |
| ネットワーク | Indirect trust | Don't trust | | Don't trust |
| クラウド | Indirect trust | Don't trust | Don't Trust | |

5.2.3.3. ネットワークスライシング

Connected　Vehicle サービスにおいて、各ユースケースにおいて必要となるネットワークの要件が異なるため、これらの異なる要件に適合する論理的なネットワークを利用する可能性がある。

例えば、UC-1 の自動運転支援においては、ダイナミックマップのクラウドからクルマに対するデータ転送には、高スループットなネットワークが必要となるのに対し、車両制御情報をクラウド側でクルマに通知する場合には、低遅延なネットワークが要求される。これらのそれぞれの異なるネットワーク要件に従って、ネットワークの QoS を管理する仕組みが必要となる。ここで、5G の特徴として、ネットワークの仮想化にともなう、ネットワークスライシングの機能が利用できる。

5.2.3.5.4. 5G ネットワークスライシング機能におけるセキュリティ

3GPP SA3 Phase2 においてネットワークスライシングのセキュリティについて検討を行っている。ネットワークスライシングのセキュリティに関する検討項目は以下の通りである(3GPP TR 33.813) [27]。

・ネットワークスライス認証・認可
不正な端末のアクセスにより、ネットワーク資源の消費や DoS 攻撃などを防止するためスライス認証、認可の仕組みを提供する。スライス認証は、プライマリ認証と組み合わせで利用する。
・ネットワークスライシングにおける鍵の分離
スライス別の鍵を管理し、鍵の漏洩に対して他のスライスに影響を及ぼさないようにすること、鍵の更新に対して、フォワードセキュリティを効率的に保証するための仕組みを提供すること。
・スライスの提供者は、スライスの利用者に対して、利用者ごとにサービスをカスタマイズして提供すること。具体的にはネットワークの特性（無線アクセス技術、通信帯域、遅延、信頼性等）とセキュリティレベルなど。セキュリティレベルについては、スライスの利用者に対して提供するセキュリティ機能をその機能の提供方法を規定する必要がある。
・スライス認証・認可については、モバイル通信事業者の加入者情報とは異なる ID や認証情報（Credential）を管理する必要がある。上記セキュリティを確保するためには、UE（通信端末）でのスライス認証・認可のための ID や認証情報の安全な保管方法と、第 3 者が提供するスライス認証のネットワーク機能と 5G コアのネットワーク機能（AMF, SMF or NSSF）などとの安全な通信が必要となる。
・ネットワークスライスへのアクセストークンは、NRF によって発行される。スライス利用者は共有スライスに対するトークンを用いて、同じタイプのネットワークサービス提供者(NF service producer)によって提供されるサービスにアクセスすることができる。

NS-1 (NS-Producer-1)
NS-2 (NS-Producer-2)　　shared slice level　　access token
NS-3 (NS-Producer-3)

・プライバシ保護のために、NSSAI 情報を保護する。具体的には、セキュアセッションが確立するまで、初期の NAS 情報として NSSAI 情報を送らない。
・一度拒否された NSSAI を UE(通信端末)が後にアクセスすることができるように、無効な NSSAI を取り消す手段の提供

プライマリ認証およびスライス認証の手順を図 5.2.40 に示す。

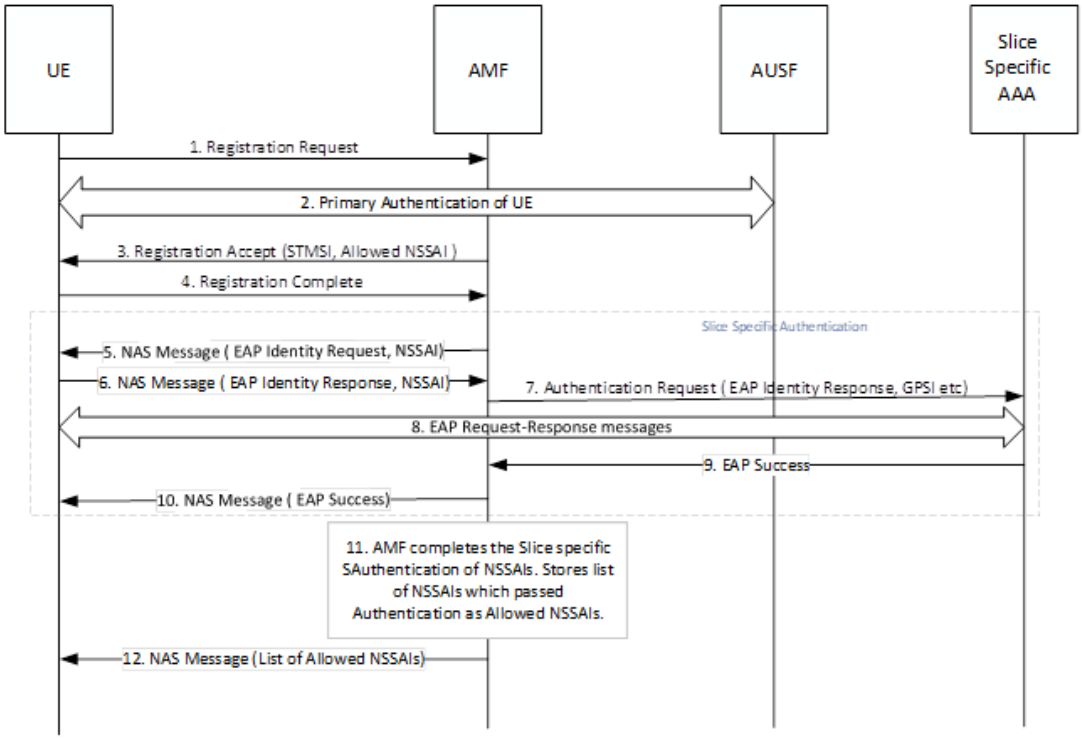



図 5.2.39　プライマリ認証およびスライス認証の手順概要

5.2.3.5.5. Connected Vehicle におけるネットワークスライシングのセキュリティ課題

安全な走行を確保するためには、他のネットワークと分離し、車両制御情報等を、高信頼、低遅延で送受する必要があり、自動運転支援専用の 5G ネットワークスライシングが想定される。このような（ある種公共性をもった）専用ネットワークスライシングの必要性や要求されるセキュリティプロファイルを規定するとともに、ネットワーク要件（遅延、サービスエリア等）を検討する必要がある。

（1）スライス提供者による認証・認可

ネットワークスライシングは、モバイルネットワーク上で構築される仮想定期な通信ネットワークであり、例えば、自動運転支援専用の仮想ネットワークを想定した場合、本仮想ネットワーク（スライス）の提供者は、自動運転支援サービスの提供者であると考えられる。従って、スライス認証・認可は、自動運転支援サービスの提供者が、自動運転支援サービスの利用契約を行った利用者を認証および、そのアクセス権を認可する必要がある。このように自動運転支援サービスは、モバイル通信基盤の上で実現されるモバイル通信事業者とは独立サービスも可能である。

上記の仮想ネットワーク上のサービスを安全に利用するために、3GPP TR 33.813 で検討されるように、UE(通信端末)においては、スライス認証のための ID や認証情報（Credential）を一定のセキュリティレベルで保管・管理する必要がある。例えば、SIM や TEE 等のハードウェア耐タンパーモジュールを用いることも想定される。加えて、UE においてプライマリ認証とスライス認証の状態を管理する必要も生じる。例えば、プライマリ認証が確立している状態で、スライス認証手順が動作するなど。

また、複数のモバイル通信事業者を経由した Connected Vehicle サービスも想定され、

Connected Vehicle サービスで利用されるスライス認証も含めたローミングの仕組みを検討する必要が生じる。

（2）スライスの品質

3GPP TR 33.813 で検討されるように、スライスの提供者は、スライスの利用者に対して、利用者ごとにサービスをカスタマイズして提供する。具体的には、各 Connected Vehicle サービスで想定されるスライスに対するネットワークの特性とセキュリティレベルを規定する必要がある。下記にそのパラメタ例を示す。

ネットワーク品質の要件： 遅延、誤り率、ジッタ

セキュリティレベル： 暗号方式、鍵長、鍵管理方式（鍵の更新頻度、Perfect Forward Security 等）

5.2.3.4. MEC

5.2.3.4.1. MEC 概要

MEC は、低遅延やネットワークの負荷を軽減が期待されるアーキテクチャであり、Connected Vehicle においてもその利用が想定される。MEC の技術については、図 5.2.41 に示すとおり、ETSI MEC、3GPP および Connected Vehicle での適用について 5GAA で検討されている [28]。ETSI MEC では、MEC の参照アーキテクチャや様々なユースケースを想定した API の標準化を進めている。また、3GPP では、5G のアーキテクチャの一機能として MEC の概念を取り込むための検討をすすめている。また、AECC においても、自動車製製造業者と通信事業者が、Connected Vehicle サービスを目的とし、複数の通信事業者にまたがるエッジ・コンピューティングを想定した分散クラウド環境の実現するためのネットワークデザインの検討を進めている [29]。

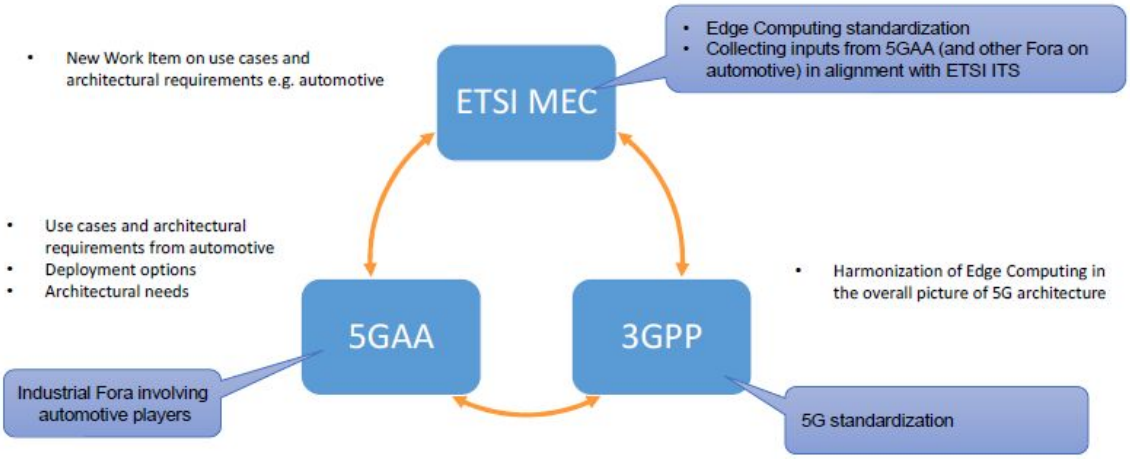



図 5.2.40 MEC の検討に関する 5GAA、ETSI、3GPP の関係図

ETSI、3GPP において検討されている 5G システムアーキテクチャと MEC の関係を図 5.2.42

に示す [30] [31]。ここでは、5G コアの SBA のアーキテクチャに基づくインターフェースを介して MEC の機能が実現される。すなわち、MEC は、3GPP の他のネットワーク機能が提供するサービスを利用する AF(Application Function)上に位置づけられ、5G コアの NEF(Network Resource Function)を介して、認証機能（AUSF)、ネットワークスライシング（NSSF)、5G のトラフィックを MEC への誘導（UPF）など 5G コアで提供される様々なネットワーク機能(NF)を利用し構築される。

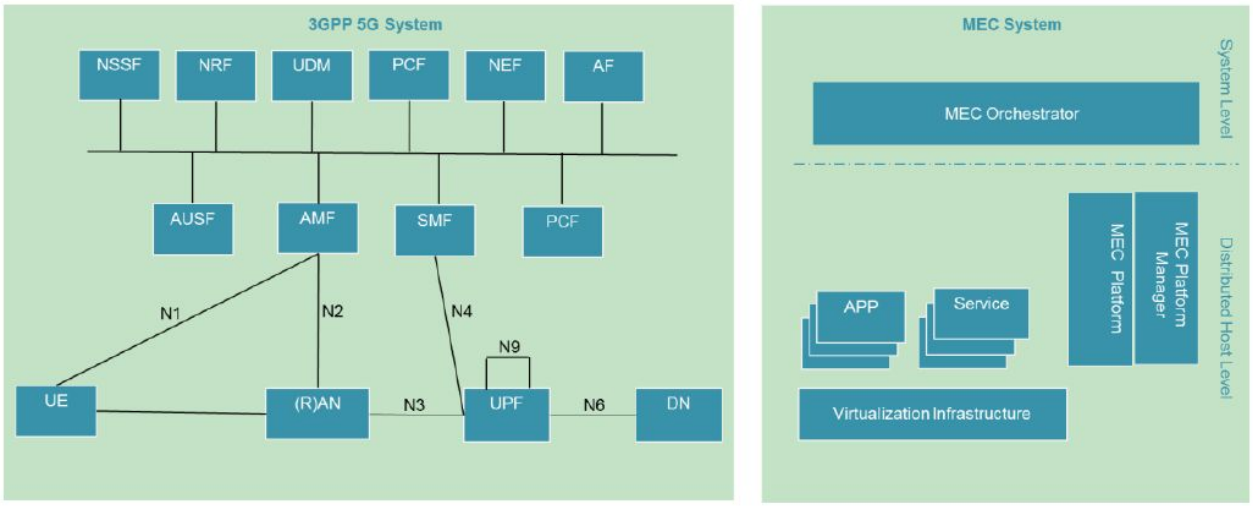



図 5.2.41　5G Service Based Architecture と MEC Architecture の関係図

5.2.3.4.2. MEC のセキュリティ

MEC のアーキテクチャのセキュリティについては、現状、検討が進められている状況である [32] [33]。ここで、Connected Vehicle のユースケースの機能の一部が、MEC 基盤上でアプリケーションとして動作する際に、Attack surface としては、ネットワークからの攻撃、MEC 基盤上で動作する他のアプリケーションからの攻撃、MEC 基盤からの攻撃、アプリ自体の不正プログラムの混入などが想定される。そのアプリケーションに対する脅威は、4.2.3.1.節の表のクラウドの位置づけと同様に、なりすまし、データの改ざん、データの漏洩、DoS がある。4.2.3.1 節で規定したセキュリティ対策が必要となる。

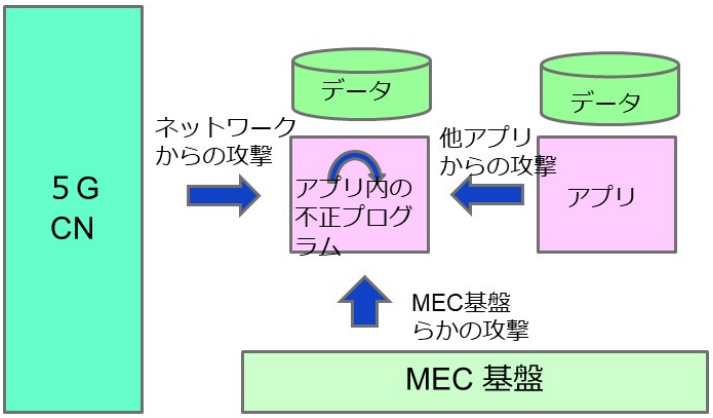



図 5.2.42　MEC アプリの Attack Surfaces

上記のなりすまし対策として MEC 基盤による利用者の認証が考えられる。利用者認証においては、5G コアの認証機能（AUSF）を活用できる。また、MEC 上の各アプリの利用については、MEC 基盤において、MEC アプリ利用者の認証・認可の機能が必要となる。具体的な手順は今後の検討課題であるが（セカンダリ認証が利用できる等）、例えば、自動運転支援による MEC 活用を想定した場合、MEC アプリの提供者は、自動運転支援サービスの提供者であると考えられる。従って、MEC アプリの利用者認証は、自動運転支援サービスの提供者が、自動運転支援サービスの利用契約を行った利用者を認証および、そのアクセス権を認可する必要がある。
複数のモバイル通信事業者を経由した自動運転支援サービスも想定され、自動運転支援サービスで利用されるローミングの仕組みを検討する必要が生じる。加えて、ローミング時にサービスやユーザに紐づくセキュリティポリシについて一貫性を保ちながら引き継ぐ仕組みが必要となる。
自動運転支援などの MEC アプリは、通信事業者から見た第三者アプリであり、MEC アプリとして登録、運用する際には、アプリケーションの安全性評価について、一定の基準を設ける必要がある。

5.2.3.5. C-V2X

5.2.3.5.1. C-V2X の概要

C-V2X は、セルラー通信により車車間、車両と路側器との通信を行う手段として、5G などの標準仕様が 3GPP で規格化されている。このなかでも、V2V（車車間）、V2I（路車間）、V2P（歩車間）の境域通信は、無線のインターフェース規格 PC5 が用いられる。また、モバイル通信網を介する広域通信として V2N（車両ネットワーク間）が規定されている。5G の検討においては、3GPP Release1 5 において V2N（参照点：Uu）が規定され、Release16 において、V2I、V2V(参照点：PC5)が規格化される予定である [34]。データの転送手法としては、unicast, groupcast, multicast の 3 つの方式が規定されている。

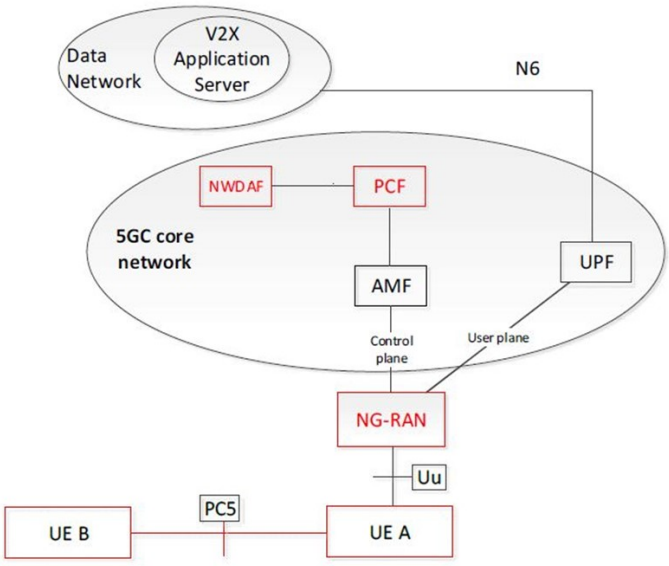



図 5.2.43　3GPP　Release16 における 5G システムアーキテクチャ内の V2X アーキテクチャ [35]

また、PC5 の参照点（モバイルネットワークを介さない通信）におけるセキュリティについては、3GPP SA3 TS33.836 において、Layer 2 ID やソース IP アドレスのプライバシ保護を対象として、以下の機能が検討されている [36]。

- PC5 上でのユニキャストメッセージにおけるプライバシ保護
  機器の ID（L2-ID）を定期的に更新して、トレーサビリティやリンカビリティを排除
- PC 上での eV2X のユニキャストメッセージにおけるセキュリティ
  機器間でセキュリティのアソシエーション（セッション）を確立
- PC5 上でのマルチキャストメッセージにおけるプライバシ保護
  マルチキャストセッションにおいて、発信元 ID（L2-ID）の追跡を防止
- グループ通信の ID に関するプライバシ保護
  グループ ID から機器の ID（L2-ID）を紐づけされないよう保護
- マルチキャスト通信の設定に関するセキュリティ
  マルチキャスト通信を行う際に、L2 のシグナリングを用いるため、そのプロトコルへの攻撃（MitM 等）
を防止
- 機器のサービス認可や破棄に関するセキュリティ
  機器のサービス認可や、破棄のプロトコルに対して、秘匿、改ざん防止、リプレイ攻撃の防止
- Cross－RAT(LTE と 5G)のサービス認可に関するセキュリティ

5.2.3.5.2. C-V2X のセキュリティ課題

C-V2X については、3.4.2 節の「セルラー通信技術を用いた ITS・自動運転の高度化に向けた課題調査報告書」にセキュリティの課題がまとめられている。上記の報告書における各ユースケースでの共通のセキュリティ課題は、以下の通りである。以下抜粋

「情報の真正性の保証、その責任所在が重要になる。本ユースケースでは、情報提供元の機関の起点での認証が必要である。認証されていない機関からの情報の改ざんされた情報が配信されないよう、例えば、配信情報への電子署名埋め込みや、情報の提供元・情報配信サーバ・情報受信車両でのセキュアな接続を利用することが考えられる。また、配信制御のための車両トラッキングによるプライバシ課題の検討も必要である。」

・ここで、C-V2X におけるアプリケーションデータのセキュリティ仕様は、3GPP の対象外としており、狭域通信 PC5 における機器間のセキュリティアソシエーションの仕様については、IEEE DSRC(WAVE)の仕様である IEEE 1609-2 Security Services for application and Management Messages の PKI ベースのメカニズムを参考としている。IEEE1609-2 においては、メッセージの秘匿、完全性、認証・認可を提供する。

・C-V2X は、UC-1 の周辺車両走行状態を車車間や路車間の通信により低遅延に情報を得る必要がある。一方、上記報告書においても同課題が指摘されているとおり、IEEE1609-2 の PKI の証明書によるデータの真正性を確認する場合、処理性能が課題となる。特に、証明書の署名検証の処理負荷、失効リスト（CRL）の確認処理、証明書のデータ量に起因する通信遅延処理な

どを効率的に行う検討が必要となる。

・プライバシ課題については、前述の 3GPP SA3 TS33.836 において、Layer 2 ID やソース IP アドレスの定期的な変更を行うプロトコルが規定されている。さらに、アプリケーションデータの暗号化が行われない場合、証明書に記載される対象者等の情報によるトレーサビリティの問題が発生する。

・また、C-V2X において、アプリケーションデータの送信者と、物理的なクルマや路側器との対応関係について整理が必要となる。例えば、路側器の機器認証は、ユースケースに依存しないが、クルマと路側器間の授受されるアプリケーションデータは、各ユースケースを利用できる契約者のみがデータを取り扱えるなど、認証の対象が異なることになる。

5.2.3.6. 認証機能

4.2.4.2 節から 4.2.4.5 節にかけて、Connected Vehicle のユースケースにおいて、5G の機能に着目してセキュリティの課題を整理しているなかで、共有のセキュリティ課題として認証がある。本節では、上記の検討におけるセキュリティ課題を認証の視点でまとめる（図 5.2.45 参照）。

- クルマによる認証

  クルマが、ドライバー及び同乗者を認証する。

- モバイル通信事業者による認証

  モバイル通信事業者が、モバイル網に接続するクルマを認証する。ここでは、クルマの利用者（ドライバー及び同乗者）は、クルマが認証することを想定しており、クルマに装備された通信モジュールをモバイル事象者が認証することを想定している。

- ネットワークスライス提供者による認証

  ネットワークスライス提供者が、ネットワークスライスの利用者を認証する。Connected Vehicle のユースケース（サービス）毎に求められるネットワークやセキュリティの品質が異なるためネットワークスライス提供者は、サービス事業者の可能性がある。また、Connected Vehicle のユースケースは、クルマの機種に依存する可能性があるため、ネットワークスライス提供者がクルマを認証する。

- MEC 基盤による認証

  MEC 基盤提供者が、MEC 基盤の利用者を認証する。また、Connected Vehicle のユースケースは、クルマの機種に依存する可能性があるため、MEC 基盤提供者がクルマを認証する。

- MEC アプリ提供者による認証

  MEC 基盤提供者が、MEC 基盤の利用者を認証する。また、Connected Vehicle のユースケースは、クルマの機種に依存する可能性があるため、MEC 基盤提供者がクルマを認証する。

- クルマ（V2V）/路側器（V2I）/歩行者（V2P）による認証

V2X は、クルマ、路側器、歩行者がクルマを認証する。

- サービス提供者による認証

サービス提供者が利用者を認証する。サービスは、クルマの機種に依存する可能性があるため、サービス提供者がクルマを認証する。

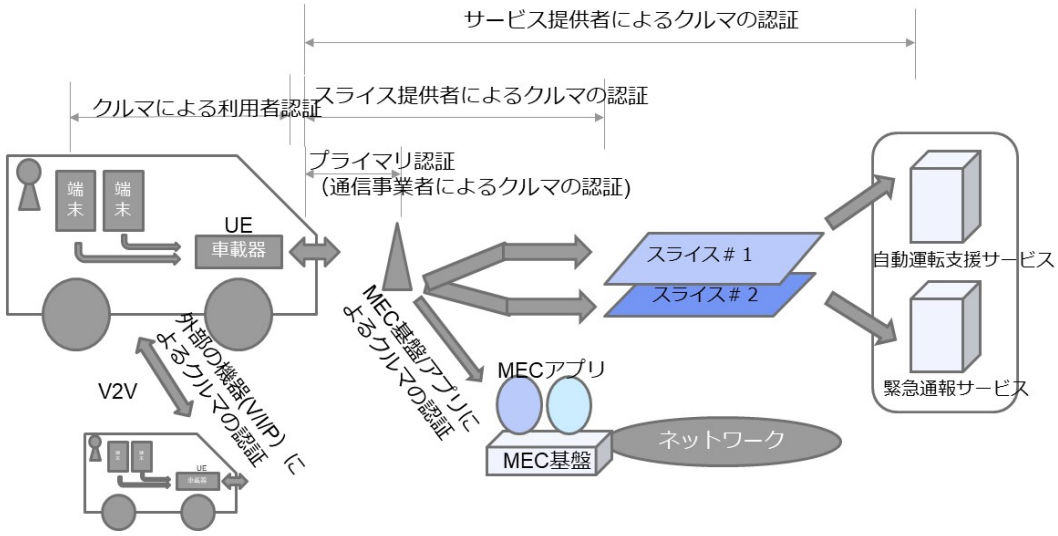



図 5.2.44 Connected Vehicle における各認証のイメージ図

サービス提供者は、サービス特有のネットワークやセキュリティの品質を提供するためにネットワークスライスを利用、MEC アプリを提供する可能性がある。この場合は、サービス提供者、ネットワークスライス提供者、MEC アプリ提供者が同一のケースが想定される。

V2X では、アプリケーションデータの認証（真正性）のメカニズムが IEEE/DSRC で規定されているが、今後の課題である。

5.2.3.7. その他

3GPP SA3 で規定される 5G セキュリティ機能において、Connected Vehicle サービスの各ユースケースでの活用が想定される機能を表 5.2.23, 表 5.2.24 に示す。

表 5.2.23　3GPP SA3 phese1 との関連

| | UC-1 | UC-2 | UC-3 | UC-4 |
|---|---|---|---|---|
| Primary authentication | ○ | ○ | ○ | ○ |
| Secondary authentication | | | | |
| Inter-operator security: | | | | |
| Privacy | | | | |
| Service based architecture (SBA): | | | | |
| Central Unit (CU) - Distributed Unit (DU) | | | | |
| Key hierarchy | | | | |
| Home Control | | | | |

表 5.2.24　3GPP SA3 phese2 との関連

| | UC-1 | UC-2 | UC-3 | UC-4 |
|---|---|---|---|---|
| Study on the security of URLLC for 5GS | ○ | | ○ | |
| Security of URLLC for 5GS | ○ | | ○ | |
| Study on Security for 5GS Enhanced support of Vertical and LAN Services | | | | |
| Security for Vertical_LAN | | | | |
| Study on evolution of Cellular IoT security for the 5G System | | | | |
| Study on Security Aspects of 3GPP support for Advanced V2X Services | ○ | | | |
| Study on Security of the enhancement to the 5GC location services | | | | |
| Study on the security of the Wireless and Wireline Convergence for the 5G system architecture | | | | |
| Mission Critical Services Security Enhancements | ○ | | | |
| Study on Security aspects of Enhancement of Network Slicing | ○ | ○ | ○ | ○ |
| Study on Security Aspects of PARLOS | | | | |
| Security aspects of single radio voice continuity from 5GS to UTRAN | | | | |
| Study on Security Aspects of the 5G Service Based Architecture | | | | |
| Security aspects of eCAPIF | | | | |
| Study on Security for NR_IAB | | | | |
| Security Assurance Specification for 5G | | | | |
| Study on 5G security enhancement against false base stations | | | | |
| Study on Long Term Key Update Process (LTKUP) Detailed solutions | | | | |
| Study on User Plane Integrity Protection | | | | |
| Study on authentication enhancements in 5GS | ○ | ○ | ○ | ○ |
| Study on authentication and key management for applications based on 3GPP credential in 5G | ○ | ○ | ○ | ○ |
| Study on SECAM and SCAS for 3GPP virtualized network products | | | | |
| Study on Security Impacts of Virtualisation | | | | |

5.2.4. ユースケース Connected Vehicle セキュリティまとめ

以上、Connected Vehicle におけるセキュリティについて、関連標準やフォーラムでの検討を踏まえ、5G ネットワークでのセキュリティの課題について整理を行った。3GPP や ETSI で検討されている 5G のセキュリティ機能については、現在進行形であり、今後、変更や仕様の具体化が想定される。これらの進捗を踏まえてセキュリティ課題の具体的な対策を検討していく予定である。

## 5.3. ユースケース Fintech セキュリティ

### 5.3.1. はじめに

5G の進展でこれまでの営業窓口を主体とした金融サービスから、Fintech 企業などの異業種と、既存の金融機関がネットワーク上で連携した新たな Fintech サービスの創出や発展が見込まれている。

その一方、多くのプレイヤーが連携することにより各事業者間の相互認証・認可や事業者が変わる都度、ユーザ認証を求められるケースが想定されるため、ユーザの利便性を留意しながら、セキュリティを検討することが重要となる。

本章では、Fintech において実現される各種サービスに対するセキュリティ課題を整理し、5G にて検討すべきセキュリティ要件を明確化する。

### 5.3.2. 5G における Fintech サービス

本節では、Fintech におけるセキュリティ課題の検討に先立って、現状の Fintech サービスを調査し、5G における Fintech サービスの全体像を明らかにする。

#### 5.3.2.1. 主な Fintech サービス

図 5.3.1 で示す通り、Fintech サービスは、大きく個人向けサービスと企業向けサービスでの分類と、金融商品サービスと決済サービスとで分類することができる。

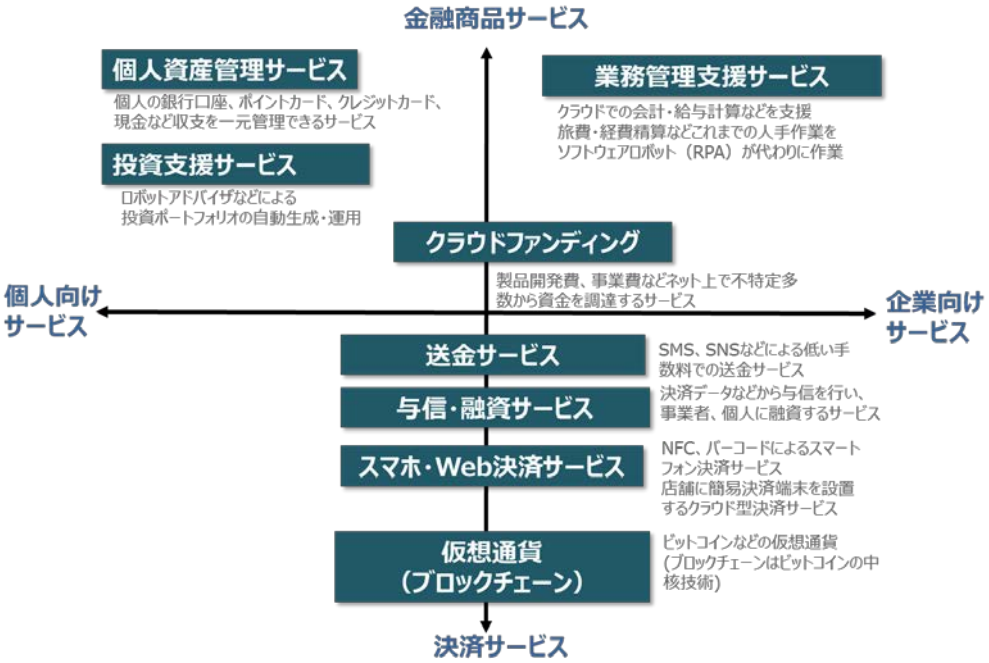



図 5.3.1　主な Fintech サービス

#### 5.3.2.2. 5G における金融サービス

これまでの金融サービスは、金融機能の一部機能を Web など活用することで、ユーザの利便性を向上させる取り組みに限られてきた。

例えば、以下のサービスがそれに相当する。

・銀行窓口の対応にインターネットバンキングを導入し、インターネット上で残高照会、振込み、送金サービス
・物理的なカードでの店舗決済からモバイル端末を活用した店舗・ネット決済サービス
・ロボットアドバイザを活用した資産管理サービス

今後、5G の進展に伴い、図 5.3.2 で示す通り、異業種間サービス連携し、異業種のデータを活用した新たなサービス創出と、ユーザ毎に最適なサービス提供の拡大が期待されている。

例えば、今後、以下のサービスが想定される。
・利用・行動データに基づく本人認証サービス
・決済情報からの融資サービス
・運転状況に応じた保険サービス
・保険と連携し、健康生活で健康食品の割引サービス
・使用量・時間に応じた課金サービスなど

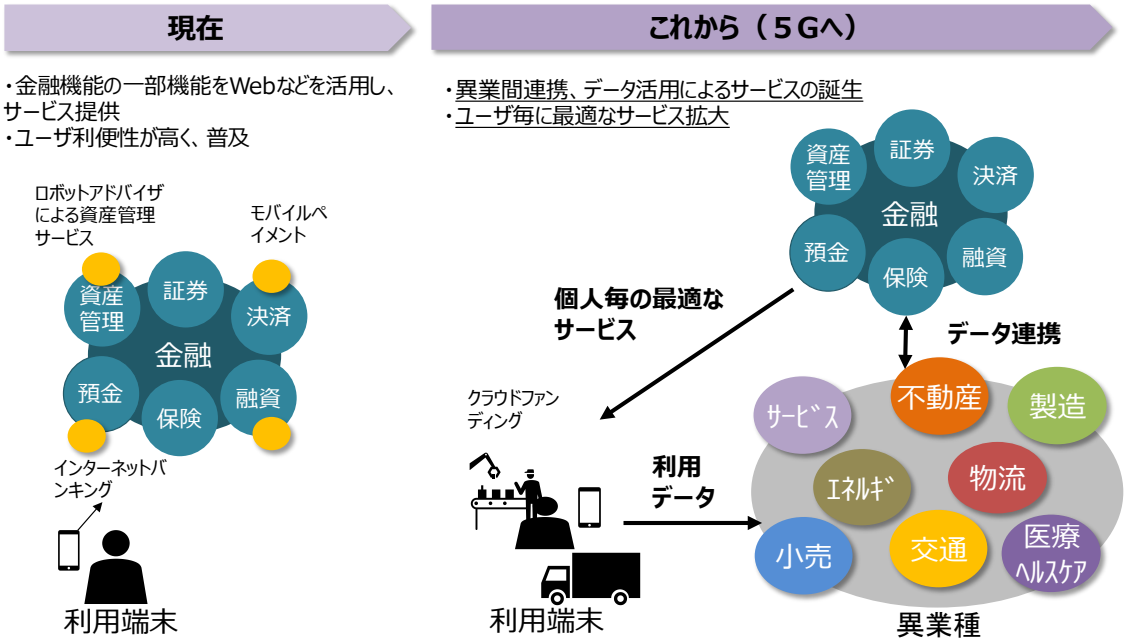



図 5.3.2　5G における Fintech サービス

5.3.3. Fintech 企業及び関連団体との連携

5G における Fintech サービスへの期待等について Fintech 企業及び関連団体にヒアリングを行った。

5.3.3.1. 株式会社 ACSiON

セブン銀行系の認証サービスベンターの株式会社 ACSiON は、以下の事業を提供している。

・本人確認プラットフォーム事業「proost（プルースト）」

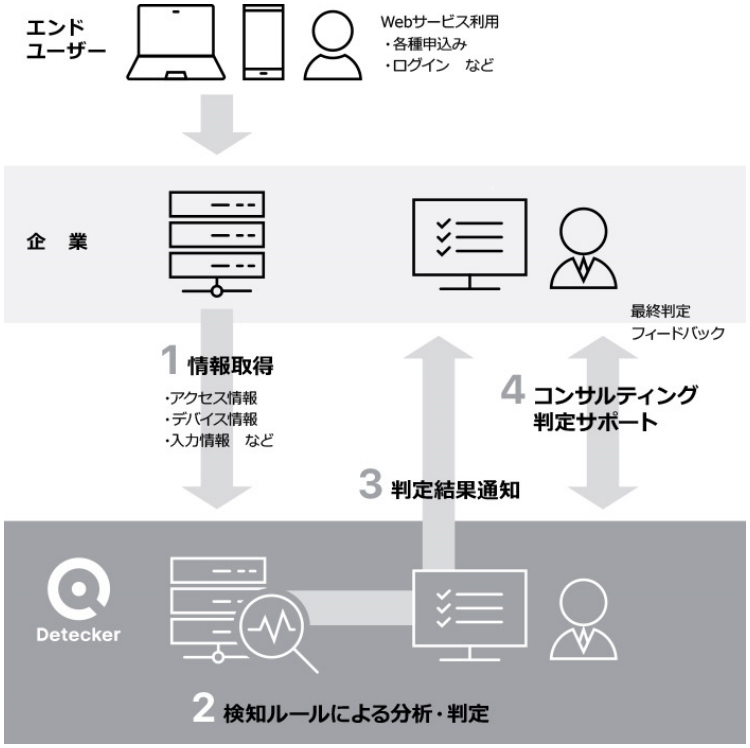
顔写真付本人確認書類の撮影データと本人の写真データを画像処理技術により照合する仕組みを提供。その他取得可能な情報と組み合わせることで厳格な本人確認を実施。

・プラットフォーム事業「Detecker（ディテッカー）」

AI を用いたビッグデータ分析により、不正申込みや不正アクセスを 24 時間 36 5 日監視、検知する仕組みを構築。

(1)サービス概要：プラットフォーム事業「Detecker（ディテッカー）」

セブン銀行のノウハウなどを活用。利用企業がエンドユーザーに提供する商品・サービスへの入会から利用まで、各取引段階に応じた不正検知を知らせるサービスとなる。




出典：株式会社 ACSiON の Web サイト

図 5.3.3　サービスイメージ

a.目指すもの

・不正アカウント開設等の不正検知の共通プラットフォームとして、利用企業間で情報を共有し、安心・安全なサービス提供を全社横断

・利用企業各社の不正利用を検知・防止するとともに、その事例を蓄積することで、より強固なプラットフォームの構築

b.取り扱う不正の事例

- Web 申込み（口座開設、カード入会等）における虚偽申込み
- 会員サイトにおける不正利用（なりすまし等）
- インターネットバンキングにおける不正利用（アカウントの第三者利用等）
- EC サイトにおける不正購買

(2)5G への期待

本当の本人であるかを検証する仕組みとして顔認証以外に以下の認証を組み合わせることでより強固な認証の実現。

・5G の低遅延の特性を活かし、行動をモニタリングや端末間の高速な認証データのやり取り

・5G の高周波数 28ＧＨｚの電波指向性を活かした正確な位置把握

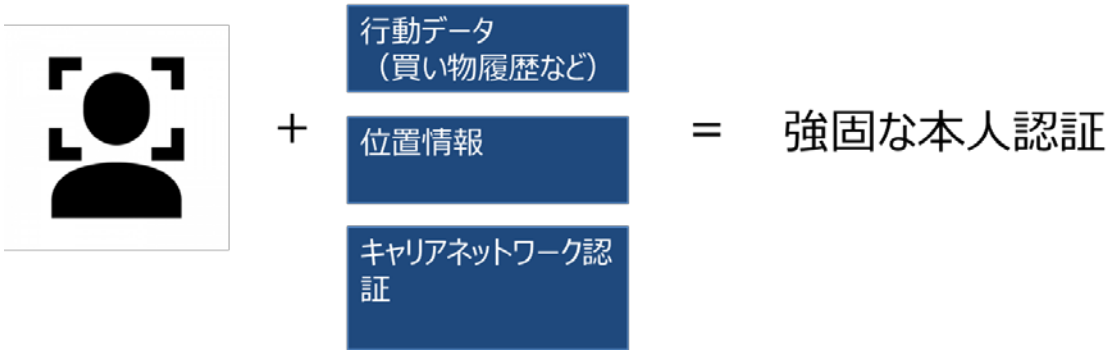



図 5.3.4　5G における強固な本人認証

5.3.3.2. 一般社団法人 Fintech 協会との連携

(1)一般社団法人 Fintech 協会の概要

a.概要

国内外の関連諸団体、関係省庁等との情報交換や連携・協力、活動を通じて、オープンイノベーションを促進させ、新たな Fintech サービスが生まれやすい環境を整え、健全な業界の発展と Fintech エコシステムの活性化、および世界の金融 IT 業界における日本のプレゼンス向上に貢献することをミッションとしている。協会には、様々なジャンルの Fintech スタートアップ 157 社及び、金融機関、通信事業者、製造業など 283 社(2020 年 7 月 1 日時点)が参加している。

b.分科会

以下のような分科会がある。

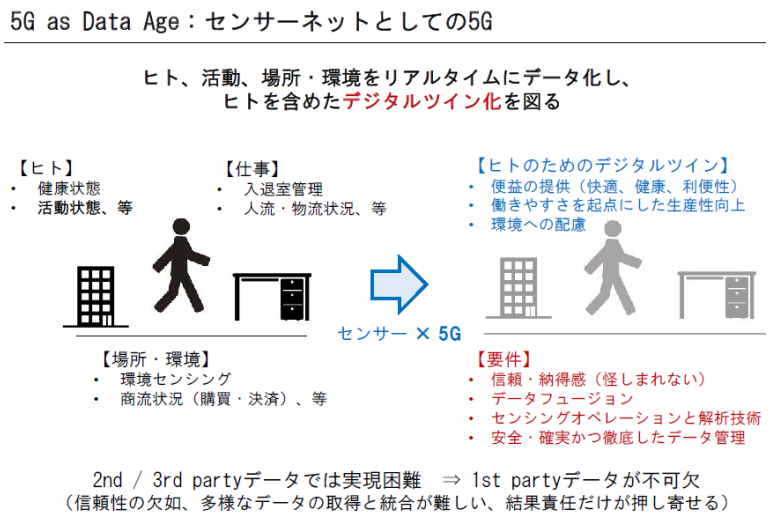
表 5.3.1　Fintec 協会　分科会一覧(2020 年 7 月 1 日時点)

| No | 分科会名 | 概要 |
|---|---|---|
| 1 | コンプライアンス | 横断的規制・eKYCなどに関する勉強・検討<br>金融庁とのFintech時代のオンライン取引研究会に出席 |
| 2 | API・セキュリティ | APIおよびセキュリティに関する研究・検討<br>全銀協・FISC・経産省等でのAPI検討会に出席 |
| 3 | キャッシュレス | 決済に関する課題検討、キャッシュレス化推進<br>経産省での割販法小委員会、カードAPI検討会等に参加 |
| | | 電子レシート推進および会計・納税の環境整備について検討 |
| 4 | 融資 | 新たな融資ビジネスモデルに向けた検討、環境整備の検討 |
| 5 | 保険 | InsurTechに関する検討・勉強会、環境整備に関する検討 |
| 6 | キャピタルマーケッツ | ICO・トークンセールについての勉強・検討（グローバル事例など） |
| 7 | 送金 | eKYCや関連規制についての意見交換<br>ペイロールの解禁によるインパクト・各社取り組みについて研究 |
| 8 | RegTech・SupTech | RegTech・SupTechに代表されるデータやテクノロジーを活用した新たなガバナンスのあり方や、監督上、規制対応上のテクノロジー利用の在り方について検討 |

出典：Fintech 協会の Web サイト

(3)5G への期待

今回、第20回API・セキュリティ分科会に出席し、「第一部5GとFintechについて」プレゼンテーション及び、パネルデスカッションに参加。株式会社 企 クロサカタツヤ氏からは、センサーと5Gが連携することで、ヒト、活動、場所・環境をリアルタイムにデータ化し、ヒトを含めたデジタルツイン化が図られる。それにより、Fintech分野におけるビジネス機会として、リアルタイムデータによる「スコアリング」サービス、キャッシュレスから、人が意識しないで決済される「ペイレス」サービス、通信とファイナンスが連携した本人認証サービス、人から物の認証による新たなファイナンスサービスなどが想定されるなど、説明がありました。




出典:(Fintech協会API・セキュリティ分科会第20回,「5GとFintech」, 株式会社 企, クロサカタツヤ

図 5.3.5　5G におけるサービスイメージ

### 5.3.4. 5G における金融サービスとセキュリティ検討ポイント

ここでは、5G で想定される金融サービスを示す。

5G で想定される金融サービスとして、車との連動した金融サービスなどを提供する「異業種連携取引分野」、個人の日々の行動に応じて金融サービスが変化する「パーソナライズされたよりきめ細かいプライベート取引分野」、実際の「使用量に応じた柔軟な決済分野」、株取引などにおける「高速取引分野」などがあげられる。

表 5.3.2　5G で想定される金融サービス

| # | 金融サービス |
|---|---|
| 1 | **異業種連携取引分野**<br>例1)コインパーキングに車を止める・移動で自動支払い<br>例2)車の使用頻度、運転状況に応じたIoT保険 |
| 2 | **パーソナライズされたよりきめ細かいプライベート取引分野**<br>例1)日々の買い物、利用頻度、健康度などに応じたダイナミックプライシングの実現やアドバイス<br>例2)走行距離に応じたガソリン価格変動<br>例3)ロボット・アドバイザーサービス(例：スマホで日々の生活データからポートフォリオ管理や投資アドバイスなどのデジタル金融窓口) |
| 3 | **使用量などに応じた柔軟な決済分野**<br>実際に利用した時間などでチャージ。本のページ数での課金など<br>例1)使用頻度ではなく、時間・感動で料金を払う<br>例2)服を着ただけ払う |
| 4 | **高速取引分野**<br>例1)株取引などにおける高速取引 |

これらのサービスを実現するためには、図 5.3.6 で示すセキュリティ検討ポイントで示す通り、異業種サービス・データ（API）連携を実現する「サービス事業者間認証」や、利用者端末とネットワーク上で異業種との「リアルタイム連携できる個人認証」の仕組みが必要となる。

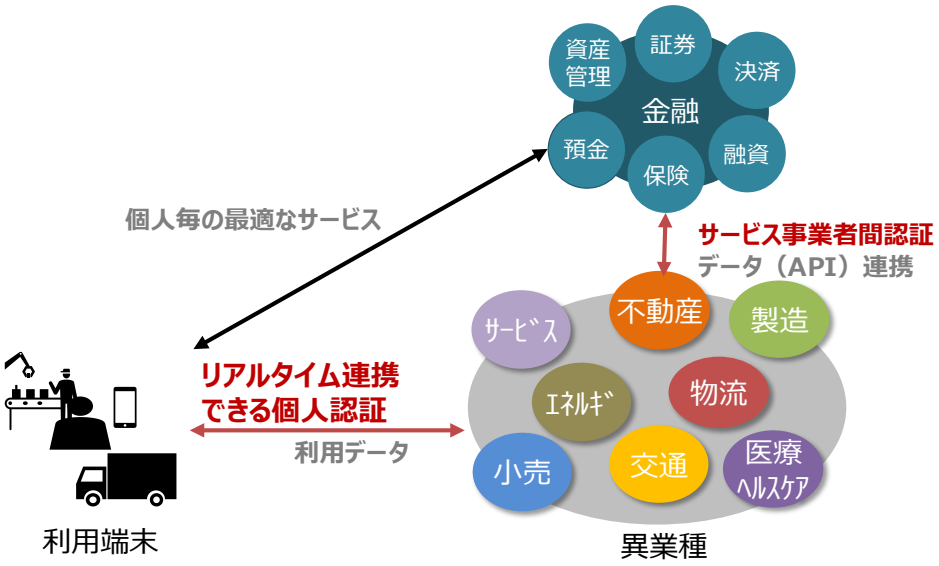



図 5.3.6　セキュリティ検討ポイント

5.3.5.　サービス事業者間認証における課題と運用者要考慮事項

5.3.5.1. 金融機関のサービスモデルの変化

従来、金融機関は垂直統合型で均一的な顧客サービスを自行で提供してきたが、マネーフォワードなどユニークなサービスを展開する Fintech 企業などの異業種が登場し、改正銀行法の施行があり、多くの金融機関が API を公開するようになってきた。

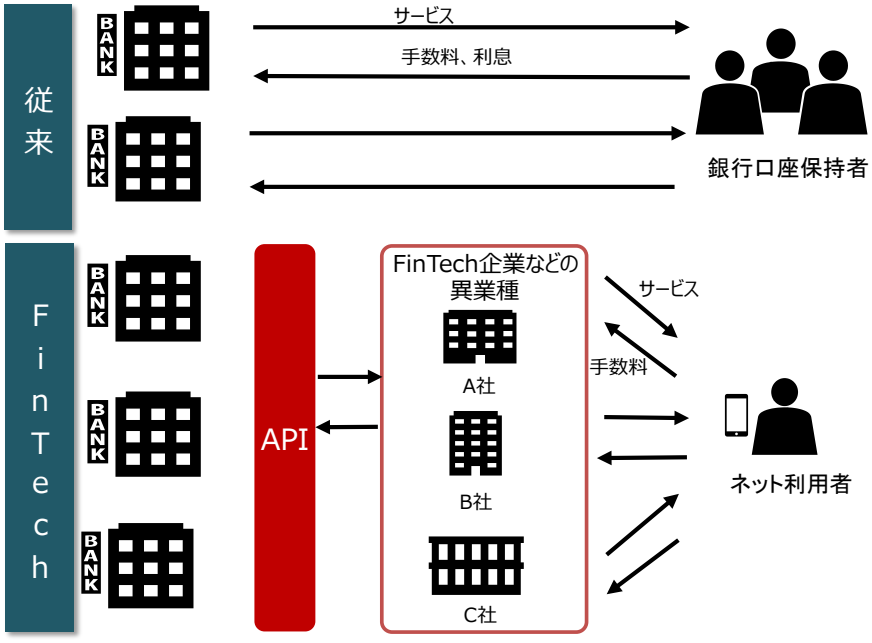



図 5.3.7　金融機関のサービスモデルの変化

5.3.5.2.　改正銀行法

2017 年 5 月 26 日「銀行法等の一部を改正する法律」が成立し、2018 年 6 月 2 日に公布された。背景として、Fintech 企業は顧客の同意の上で、顧客から入手した情報を用いて金融機関の口座にアクセスし、情報を取得しているが、以下のような問題点がある。

・セキュリティ上の問題

ID/パスワードといった個人認証に関する情報を金融機関以外の事業者が保持して金融機関のサービスにアクセス

・口座情報取得の技術的な問題

金融機関から口座情報を照会する際の API が公開されていないため、Fintech 企業は金融機関の Web サイトを解析して情報を取得

・オープンイノベーションにおける問題

Fintech 企業の法的位置付けが不明確なため、金融機関にとってセキュリティ面の不安や、Fintech 企業に金融機関が高いセキュリティレベルを要求されるなど、提携が進まない

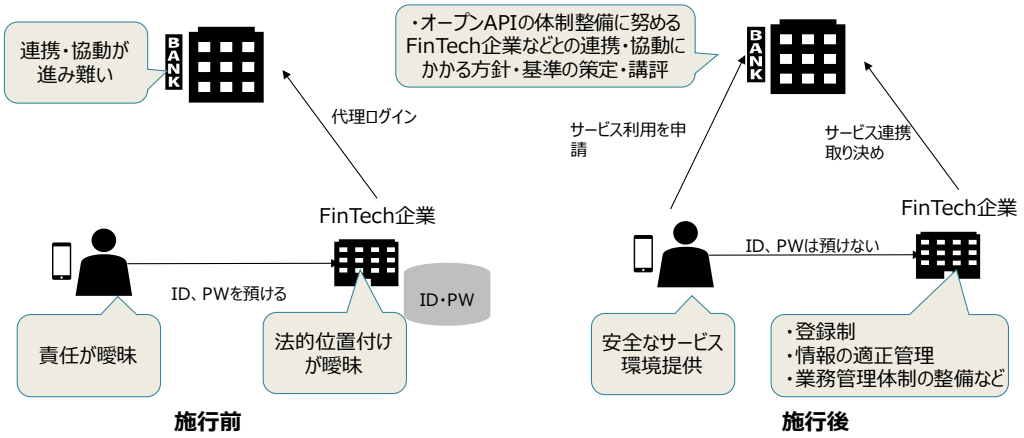



図 5.3.8　改正銀行法

5.3.5.3.　金融オープン API に用いられる認可プロセス例

オープン API を安全に活用するため、ユーザが金融機関にアクセスする権限を Fintech 企業に認可を与える。次に、金融業界などでは、オープン API の認可を行う仕組みとして「OAuth2.0」のプロトコルが推奨される。

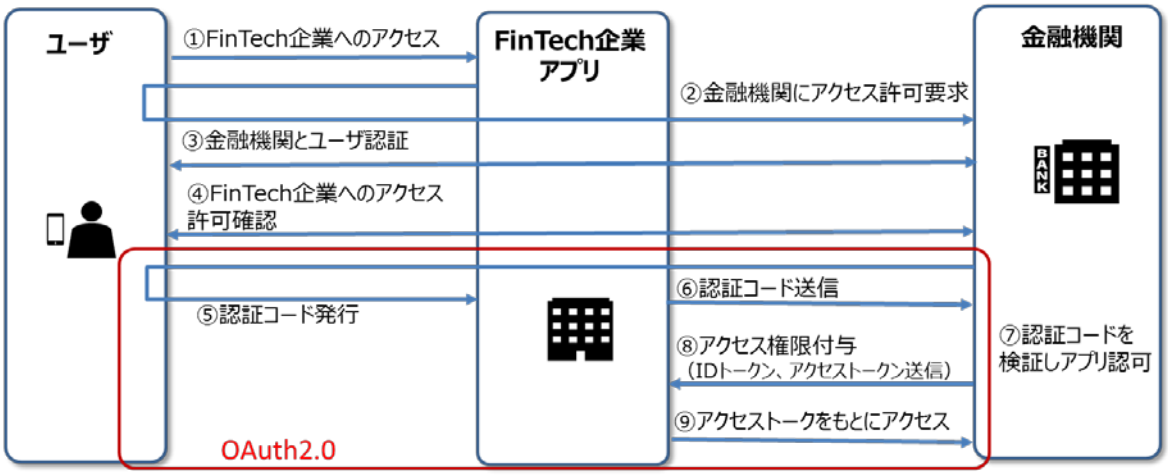



図 5.3.9　金融オープン API で用いられる認可プロセス（OAuth2.0）のフロー例

#### 5.3.5.4. 現行の金融 API 対象業界

現在、金融 API を活用している業界を以下に示す。基本、個人が利用するパソコン、スマートフォン向けのサービスとなる。

表 5.3.3　金融 API 利用状況

| # | 分類 | 内容 |
|---|---|---|
| 1 | 家計簿サービス系 | ・銀行や証券会社などの複数の口座を一括管理して、家計簿を自動作成するWebサービス<br>・銀行の入出金やカード情報をもとに、家計簿が自動作成 |
| 2 | QRコード決済サービス系 | ・スマートフォンによるQRコード決済サービス<br>・あらかじめ登録した銀行口座、クレジットカードからのチャージし、決済 |

5.3.5.5. IoT デバイスにおける金融サービス例

今後、5G が普及することで自動車、家電など向けに金融サービスが提要されることが想定される。

表 5.3.4　5G で想定される Fintech サービスと IoT デバイス

| # | 分類 | サービス案 | IoTデバイス |
|---|---|---|---|
| 1 | 自動車 | ・ガソリン代支払い（走行距離、量などで料金変動）<br>・通行料金（GPS連携し、高速道路以外での距離に応じた支払い）<br>・駐車場代金（駐車した時間で課金）<br>・ドライブスルー<br>・デジタルコンテンツ、ゲームのアイテム購入<br>・シェアリング（走行距離に応じて課金）<br>・保険（安全運転、走行距離、運転者などに応じた都度保険） | 自動車<br>(車載端末など) |
| 2 | 産業 | ・夜間の企業内コンピュータリソースの貸し出し<br>・機器のリース（利用した時間分支払う）<br>・資金調達<br>・企業間決済 | サーバなどのシステム機器 |
| 3 | シェアリング（トークン）エコノミー | ・個人間での支払い<br>（例：貸主が全体の電気代を支払い、借主には利用に応じて個別請求、自家発電による余剰電力の取引）<br>対象：光熱費、電話、インターネット、家電、民泊、車、自転車、駐車場、ウォーターサーバ等 | 家電など |
| 4 | 決済 | ・無人コンビニなどによる生体決済 | POS |

5.3.5.6. IoT デバイスにおける金融オープン API のセキュリティ課題

5G における IoT デバイスを考慮すべき、主なセキュリティ課題について、金融オープン API の認証プロセスを参考とし、示す。

(1) IoT デバイスへの攻撃：不正アクセス、改ざんと成りすましなど

(2) エンティティ間での通信路上の攻撃：通信データの盗聴・改ざんなど

(3) Fintech 企業及び、金融機関システムへの攻撃：システム、ネットワーク機器の脆弱性、DDoS 攻撃など

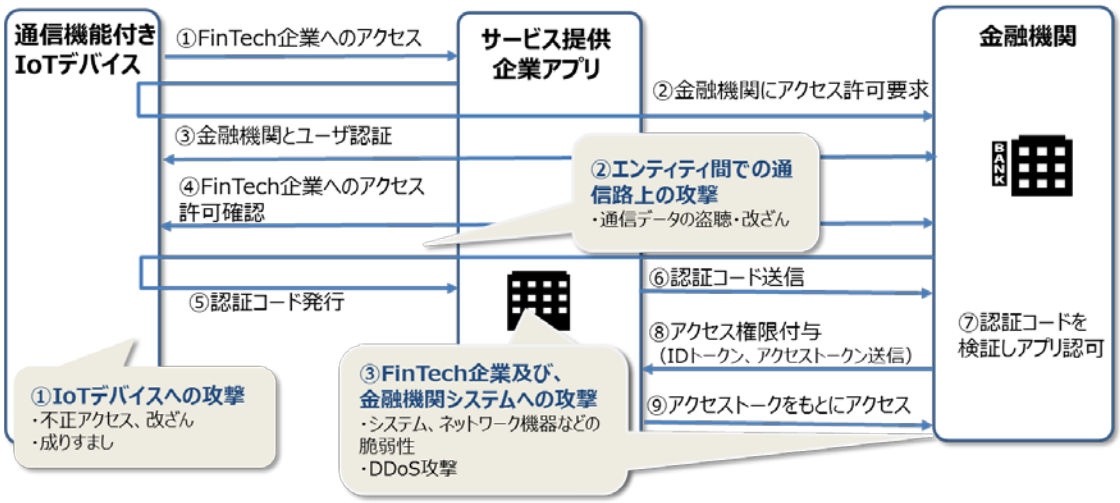



図 5.3.10　金融オープン API におけるセキュリティ考慮ポイント

5.3.5.7. セキュリティ考慮ポイントに対する運用者要考慮事項

(1)IoT デバイスへの攻撃

①クレデンシャル情報等の漏えい、改ざん

IoT デバイスの場合、誰からでもアクセスできる環境に設置されているケースが考えられるため、物理的な手段での解析/操作の可能性が増す。通信事業者は、ネットワークの接続時の認証に用いる契約クレデンシャルは、耐タンパ性を備えたクレデンシャルストレージ機能を活用し、セキュア・ストレージに格納している。運用者は、独自のクレデンシャル情報を IoT デバイスで管理・運用する際は、同様に耐タンパ性を備えた認証デバイスに格納することが望ましい。

②IoT デバイスの長期利用

携帯電話、スマートフォン等は、数年おきに機種変更されるため、その際に SIM カードの交換ができるが、5G の「超多数接続」という特徴を活かして普及が見込まれる IoT デバイスの運用期間が長く、SIM カードの交換自体が困難なケースが想定される。現在、SIM カードには、ユーザ認証のための秘匿鍵が格納されているが、これまでは SIM カードの製造時に書き込んでおり、書き換えることはできなかった。そのため、セキュリティリスクが発生した際には SIM カードを交換する必要があった。そのため、このような背景から 5G の SIM カードでは、オンラインでの書き換えが可能となっている。

(2)エンティティ間での通信路上の攻撃

5G ではネットワークスライシングが導入され、ネットワークを仮想的に独立したスライスに分解し、個々のスライスでは他スライスに悪影響を与えることなく利用できるようになり、サービスに適した暗号アルゴリズムを適用できる。例えば、IoT デバイスの場合、バッテリーによる長期間の稼働が必要となる場合があるため、軽量暗号など低電力消費アルゴリズム等の活用が可能となる。

なお、ネットワークスライシングのセキュリティについては、3GPP SA3 Phase2 にて検討を行っており、セキュリティに関する検討項目は、4.2.4.3.1.節の通りである。

(3)Fintech 企業及び、金融機関のシステムへの攻撃

プレイヤーに対するアプリケーションレイヤー及びネットワークレイヤーにおける認証/認可やサービスで集積された各種データのアクセス制御の検討が必要となる。5G においては、セカンダリ認証を用いることでサービスに対するアクセス制御ポリシーに基づく安全なアクセス可否判断を一元管理することが可能となる。中央集権的機能を持たない直接通信型の通信形態に関しては AKMA を用いることで安全な認証を実現できる。

また、Society5.0 の実現に向けて、サイバー空間の自由で安心・安全なデータの流通を実現するためには、データの信頼性を確保する仕組みとして、データの改ざんや送信元のなりすまし等を防止するトラストサービスが不可欠である。金融オープン API サービスにおいては、利用者、IoT デバイス、ネットワーク、Fintech 企業などのサービス提供事業者、金融機関がプレイヤーとして想定される。サイバーセキュリティ対策の観点から、通信チャネルに対する攻撃を想定した対策として、それぞれのプレイヤー間で信頼関係を構築し、セキュアネットワークを通じたデータ授受を実現する必要がある。

現在、総務省では、「プラットフォームサービスに関する研究会」の下に「トラストサービス検討ワーキンググループ」を設置し、2019 年（平成 31 年）１月から、以下のようなトラストサービスに関する現状や課題について検討が進められている。

・人の正当性を確認できる仕組み（電子署名）
・組織の正当性を確認できる仕組み（組織を対象とする認証、ウェブサイト認証）
・IoT デバイス等のモノの正当性を確認できる仕組み
・データの存在証明・非改ざんの保証の仕組み（タイムスタンプ）
・データの送達等を保証する仕組み（e デリバリー）

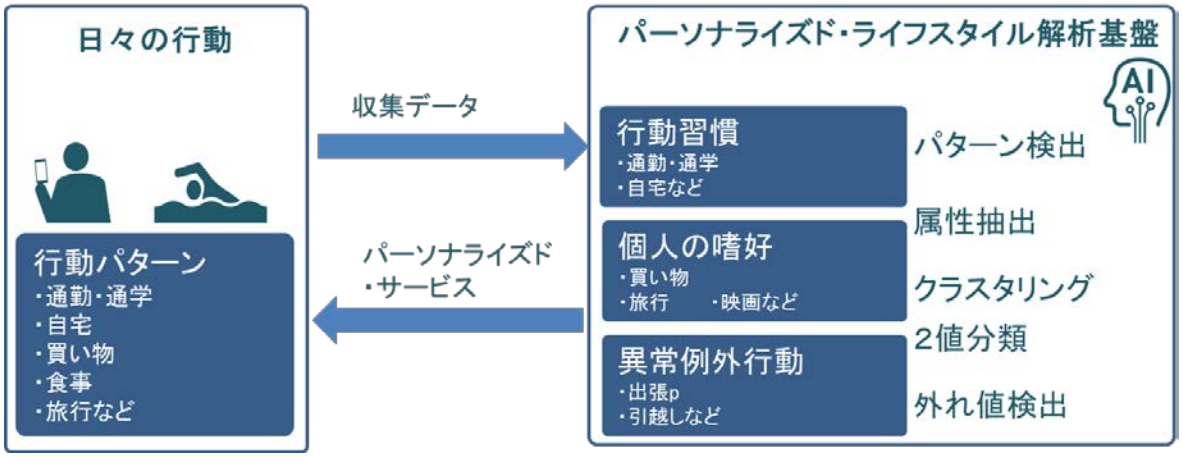
### 5.3.6. リアルタイム認証におけるセキュリティ課題と運用者要考慮事項

#### 5.3.6.1. これまでの認証方式の課題

従来の個人認証では ID/パスワードや署名、近年では、生体情報等が求められる。しかし、これらの情報を入力することはユーザにとって負担となる。例えば、医療従事者、設備機器の保守従事者等が該当する。また、生体認証の場合、個人が携帯している媒体に認証に必要となる生体情報が保持しているケースが多く、クローズドなサービスに限定され、5G のような多様な事業者間データ連携するケースには、不向きである。そのため、ユーザの利便性から、携帯電話、IC カードなどに格納されたユニークな ID を利用するケースが増えている。一方でこのような認証方法は、ユーザにとって利便性が高いが容易に成りすまされる可能性がある。

#### 5.3.6.2. 5G における本人認証の可能性

5G によって、高速・大容量化でセンサー、GPS、購買データなどの行動の認識・特定や、画像認識によるオンラインでの人物の認識・特定が可能になると想定される。例えば、東京大学大学院情報理工学系研究科ソーシャル ICT 研究センターでは、“MITHRA”プロジェクトとして、スマートフォンやウェアラブル端末の位置情報等のビックデータを解析することで、ユーザを認証するライフスタイル認証の研究・検討を進めている。




参考資料：東京大学「ライフログを利用したライフスタイル認証技術」の Web サイト

図 5.3.11　入出力系から見たライフスタイル解析イメージ

#### 5.3.6.3. ライフスタイル認証におけるセキュリティ課題

ライフスタイル認証を実現する上で以下のセキュリティ課題が想定される。

(1)エッジでの大容量の行動データの収集・解析

ライフスタイル認証を行うには、位置情報や、映像データなど膨大なデータを効率的に収集し、分析する必要がある。そのため、すべてのデータをクラウドに送信して処理するのではなく、ネットワークエッジ（ユーザに近い場所）でデータを収集、分析することで遅延が減り、広帯域幅アプリケーションをリアルタイムで、実行する必要がある。この技術の規格の一つとして、ETSIが標準化を進めている Multi-access Edge Computing(MEC)がある。MEC は、クラウド上のサーバの代わりにエリアごとに MEC プラットフォームを置き、そのエリアにある IoT デバイスへのレスポンスを早くするものである。MEC プラットフォーム上でデータ処理することで、IoT デバイスへのレスポンス時間の短縮化を図る。また、クラウドに上げるデータを最小限に限定できるため、データ通信量の減少にもつながるメリットがある。 一方で、アクセスネットワークの境界に、コンピュータ資源やデータストレージを配備し、クラウドで処理する手間を MEC プラットフォーム段階で処理を行うため、IoT デバイスと MEC プラットフォーム間でのネットワークや、複数プレイヤーの MEC プラットフォームへのアクセスに起因するセキュリティリスク（MEC プラットフォーム上の他プレイヤーのアプリケーションや、MEC プラットフォームからの攻撃など）が想定される。

なお、MEC については、ETSI 以外に 3GPP にて検討を行っており、概要については、5.2.3.4.節の通りである。

(2)端末識別子のトレーサビリティ防止

端末識別子によるトラッキング防止のため、IMSI に代わる TMSI が用いられるようになってきたが、IMSI を平文で送信する場合も損じしており、位置の特定や追跡される可能性が問題となっている。

(3)本人認証精度

GPS の位置情報等を解析することで、本人らしさを示すことができる。今後、更に 5G の進展に伴い、様々な行動データを収集・解析することで、本人性を向上させることが期待できる。一方で、金融サービスにおける本人認証においては、より高い本人認証が求められる。

5.3.6.4. セキュリティ考慮ポイントに対する運用者要考慮事項

(1)エッジ（MEC プラットフォーム）活用時のセキュリティ

MEC プラットフォームにおいては、なりすまし、データの改ざん、データの漏洩など、クラウド基盤と同様のセキュリティ対策が必要となる。例えば、IoT デバイスが直接、クラウドとの通信を行わず、MEC プラットフォームを経由するため、4.3.5.7 と同様にプレイヤーに対するアプリケーションレイヤー及びネットワークレイヤーにおける認証/認可やサービスで集積された各種データのアクセス制御の検討が必要となる。

また、IoT デバイスから行動データをクラウド又は、MEC プラットフォームに対し、転送、更に IoT デバイスにそのアクションを返答する際には低遅延、高スループットなネットワークが要求される。 5 G の特徴であるネットワークスライシング機能を利用することで、これらネットワーク要件に適合する論理的なネットワークを安全に活用することも可能となる。

(2)端末識別子のトラッキング防止

5G では、IMSI に相当する「SUPI」という識別番号が SIM カードに登録されており、これ

をネットワーク・オペレータの公開鍵によってランダムに暗号化した「SUCI」で認証を行うことで、プライバシーの配慮がなされている。また、認証が完了した端末の識別番号には「GUTI」というテンポラリな ID が使われるが、移動体通信事業者によっては、長期の更新がなされないケースがあり、5G では、定期的に変更するようより厳格に仕様で定められている。

(3)本人認証精度の向上

顔や指静脈認証などの生体認証との組み合わせが想定される。ただし、生体認証を利用に際して、以下の課題が残されている。

a.複数のサービス間の共通利用

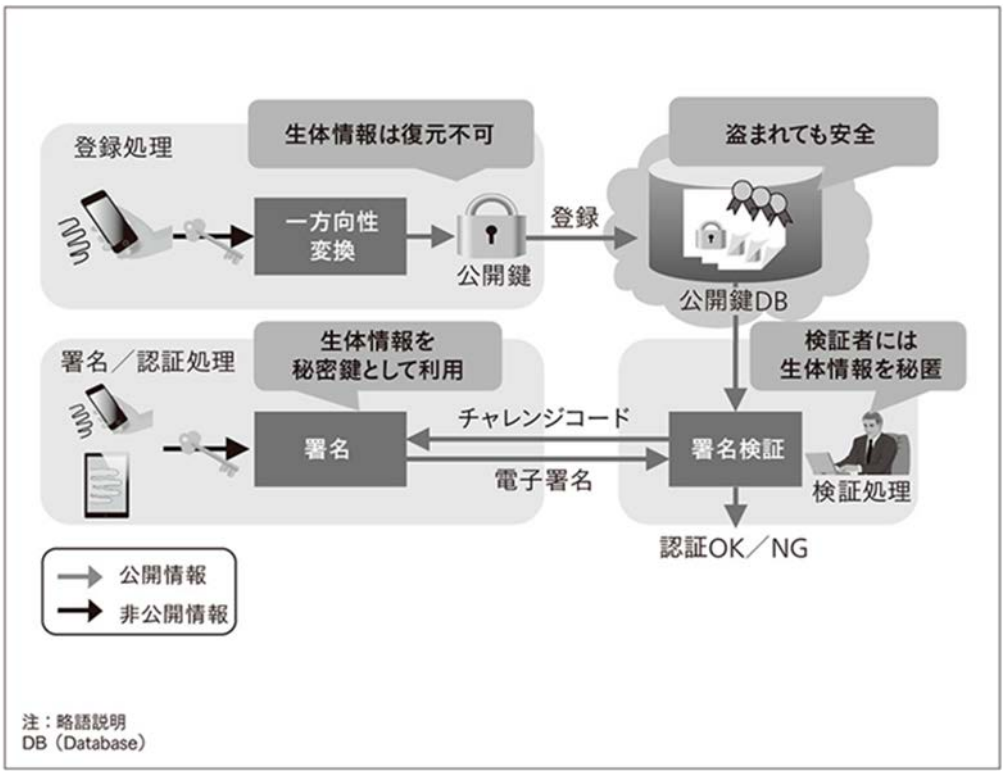
これまでの生体認証システムは、指紋、静脈、瞳の虹彩などの生体情報を単一のシステム内で管理して安全性を確保。複数のシステムで共通の生体認証を使うには、システムごとに生体情報を登録する必要があり、登録の煩雑さが生体認証の普及を阻害する要因となっている。

b.生体情報のプライバシー・セキュリティの確保

生体情報は、人種、民族、健康状態などの特定の可能性があるセンシティブな情報のため、プライバシー保護の観点から、厳重な管理が求められる。生涯不変で破棄・更新できない情報であり、ひとたび漏えいして生体偽造などの脅威が発生した場合、安全性の回復が非常に困難である。このような脅威から利用者を守るため、生体情報の漏えい防止が大きな課題となる。

このような課題解決の一つとして、日立製作所のテンプレート公開型生体認証基盤（PBI）を活用が想定される。生体認証に用いる静脈や指紋などの生体情報を、元データに復元できない公開鍵の形に変換し、生体情報を用いた電子署名により本人認証を行う仕組み。従来の PKI(Public Key Infrastructure)による認証システムでは、IC カードなどに電子証明書を鍵情報として格納していたため、これを厳重に管理する必要があった。本技術を用いたシステムでは、生体情報に対して一方向性変換(順方向の変換は容易に計算可能だが、逆方向の変換は計算困難である変換関数)をした情報を認証時につど生成して鍵情報として使うため、ユーザは鍵情報の管理が必要なく、生体情報を復元することは不可能となる。

また、従来、生体情報の安全性を確保するためにクローズドな環境で個別に構築していた認証機能について、PBI を適用することにより、クラウド上に配置し複数の業務サービスで共通利用することが可能となる。




出典：日立製作所の Web サイト

図 5.3.12　テンプレート公開型生体認証基盤（PBI）概要

5.3.7. ユースケース Fintech セキュリティまとめ

5G における Fintech サービスについて、金融オープン API、ライフスタイル認証に関して、Fintech 企業、関連団体にヒアリングを行い、セキュリティの課題、セキュリティ考慮ポイントに対する運用者要考慮事項を整理した。

今後、5G のセキュリティは、3GPP や ETSI などで引き続き、検討がされており、仕様の具体化が進むことが想定される。これらの進捗を踏まえ、セキュリティ課題に対する具体的な対策を検討していく必要がある。

# 6. 参照文献

## 6.1 ユースケース IoT セキュリティ


[1] 5G における IoT セキュリティ, 5GMF セキュリティ検討アドホック資料, 2018 年 10 月

[2] IoT セキュリティガイドライン, 経産省/総務省/IoT 推進コンソーシアム(IOTAC), 2016 年 7 月

[3] 安全な IoT システムのためのセキュリティに関する一般的枠組, 内閣サイバーセキュリティセンター, 2016 年 8 月

[4] IoT セキュリティ総合対策, 総務省, 2017 年 10 月

[5] サイバー・フィジカル・セキュリティ対策フレームワーク(案), 経産省, 2018 年 4 月

[6] IoT 開発におけるセキュリティ設計の手引き, 情報処理推進機構(IPA), 2016 年 5 月 & 2018 年 4 月改訂

[7] IoT セキュリティ評価検証ガイドライン, 重要生活機器連携セキュリティ協議会(CCDS), 2017 年 6 月

[8] IoT セキュリティガイド 標準／ガイドライン ハンドブック, 日本ネットワークセキュリティ協会(JNSA), 2018 年 5 月

[9] IoT セキュリティチェックシート, 日本スマートフォンセキュリティ協会(JSSEC), 2018 年 3 月

[10] Draft NISTIR 8200 - Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things, 米国国立標準技術研究所(NIST), 2018 年 2 月

[11] Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, 欧州ネットワーク・情報セキュリティ機関(ENISA), 2017 年 11 月

[12] Security Guidance for Early Adopters of the Internet of Things, Cloud Security Alliance (CSA), 2016 年 2 月

[13] OWASP IoT Top 10, The Open Web Application Security Project (OWASP), 2018 年 12 月改訂

[14] Technical Specification TS-0003 Security Solutions, OneM2M, 2018 年 4 月

[15] IoT Security Guidelines, GSMA, 2017 年 10 月

[16] セキュリティ検討アドホック 2018 年度活動について, セキュリティ検討アドホック事務局, 2018 年 11 月

[17] Key Points of 5G Security, Anand R. Prasad, NEC Corporation, 2018 年 7 月 http://pop.riverpublishers.com/opinions.php?id=19

[18] 3GPP TR 38.913, "Study on Scenarios and Requirements for Next Generation Access Technologies; (Release 15)"

[19] 3GPP TR 22.186, "Enhancement of 3GPP support for V2X scenarios; Stage 1 (Release 16)"

[20] Catalin Cimpanu, "Newer Diameter Telephony Protocol Just As Vulnerable As SS7," 2018.07.02, https://www.bleepingcomputer.com/news/security/newer-diameter-telephony-protocol-just-as-vulnerable-as-ss7/

[21] 3GPP TR 23.724, "Study on Cellular Internet of Things (CIoT) support and evolution for the 5G System (5GS) (Release 16)"

[22] oneM2M - Home, https://www.onem2m.org/

[23] Ace (Authentication and Authorization for Constrained Environments) Status Pages, https://tools.ietf.org/wg/ace/

[24] OpenWeave, https://openweave.io/

[25] SP-190711, "New WID Authentication and key management for applications based on 3GPP credential in 5G"

[26] 3GPP TR 33.805, "Study on Security Assurance Methodology for 3GPP network products"

[27] 3GPP TR 33.916, "Security Assurance Methodology (SCAS) for 3GPP network products"

6.2 ユースケース Connected Vehicle セキュリティ


[1] “Proposal for draft guideline on cyber security and data protection,” 2016.

[2] “Proposal for a Recommendation on Cyber Security”.

[3] “Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues”.

[4] “TTC TR-068 自動車の遠隔更新技術の標準化と実用化動向,” 2019.10.

[5] “自動走行システムにおけるサイバーセキュリティ対策,” 自動走行ビジネス検討会, 2019.6.26.

[6] “Status of the Development of ISO/SAE 21434,” 25th European Conference, EuroSPI 2018, 2018.

[7] “ITS の標準化 2018 ,” 自動車技術会 発行, 2018.

[8] “CEN TC278 WG16,”.

[9] “ISO21177: ITS station security services for secure session establishment and authentication between trusted devices,” 2019.

[10] “TS21185: Intelligent transport systems − Communication profiles for secure connections between trusted devices,” 2019.

[11] “ITS Forum RC-009 運転支援通信システムに関するセキュリティガイドライン”.

[12] “セルラー通信技術を用いた ITS・自動運転の高度化に向けた課題調査報告書,” 2019.

[13] “Network Equipment Security Assurance Scheme OverviewVersion 0.3,” 11 May 2016.

[14] “The GSMA will work with ENISA to secure 5G networks,” 2020.1.29.

[15] “Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures,” 2020.1.29.

[16] “ISO27011 (ITU-T X.1051) Information technology − Security techniques − Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations,” 2016.

[17] “ISO27017 (ITU-T X.1601) Information technology − Security techniques − Code of practice for information security controls based on ISO/IEC 27002 for cloud services,” 2015.

[18] “Connected Car 社会の実現に向けた研究会,” 総務省.

[19] “AECC：General Principle and Vision White Paper Ver 1.0.0,” 2017.12.

[20] A. M. A. I. F. M. Claudia Campolo1, “5G Network Slicing for Vehicle-to-Everything Services,” IEEE Wireless Communications, December 2017.

[21] “3GPP TR 22.891, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers; Stage 1 (Release 14)”.

[22] A. L. T. M. M. C. J. S. J. M. a. M. D. Maria A. Lema, “Business Case and Technology Analysis for 5G Low Latency Applications,” IEEE Access, March 2017.

[23] “3GPP TR 33.813”.

[24] “Toward fully connected vehicles: Edge computing for advanced automotive communications: White Paper, 5GAA”.

[25] “AECC General Principle and Vision, White Paper,” 2018.

[26] “MEC in 5G networks, ETSI White Paper No.28”.

[27] “ETSI MEC: An Introduction:”.

[28] “Cloud and MEC security,” 2018.

[29] “5G security package 3: Mobile Edge Computing / Low Latency / Consistent User Experience,” NGMN.

[30] “3GPP TS 23.285: Architecture enhancements for V2X services (Release 16),” 2019.

[31] “3GPP TR 33.836: Study on Security Aspects of 3GPP support for Advanced V2X Services (Release 16),” 2019.

[32] “5G V2X Architecture and Radio Aspects,” 2019.

[33] 香月伸一, “「ISO/TC204 における ITS の国際標準化動向」,” JARI Research Journal, 2017.

[34] “「Network Equipment Security Assurance Scheme (NESAS)」,” GSMA.

[35] “ISO16461: Intelligent transport systems − Criteria for privacy and integrity protection in probe vehicle information systems,” 2018.

[36] “ISO21217: Intelligent transport systems - Communications access for land mobiles (CALM) - Architecture,” 2014.

6.3 ユースケース　Fintech セキュリティ

[1] “5G と Fintech” 第 20 回 Fintech 協会 API・セキュリティ分科会,2019.12.03.

[2] “オープン API のあり方に関する検討会報告書ー オープン・イノベーションの活性化に向けて ー,” オープン API のあり方に関する検討会, 2017.7.13.

[3] “日銀レビュー 金融分野におけるオープン API の活用～セキュリティへの影響と対策～,”Bank of Japan Review, 2018.6. 3

[4] “日立評論:Digital Solutions to Innovate Society,デジタルソリューションの基盤技術と先端事例 汎用カメラ指静脈認証技術とその将来展望,” 2018 vol.100 No.3,2018.3

[5] 株式会社ACSiON https://www.acsion.co.jp/

[6] 一般財団法人 Fintech 協会 https://www.fintechjapan.org/members

[7] 国立大学法人東京大学大学院情報理工学系研究科ソーシャル ICT 研究センター http://www.sict.i.u-tokyo.ac.jp/research/lifestyle.html

# 7. まとめ

本白書は、2019 年度のセキュリティ調査研究委員会の活動内容をまとめたものである。

具体的には、①IoT、②Connected Vehicle、③Fintech に関して、5G セキュリティの視点からセキュリティ検討項目を抽出し調査研究課題を整理した。今後は、これらの課題をどのように解決していくかについて、次年度以降検討を進めていく予定である。

# Annex　IoT 課題まとめ

## 表　Annex 1　GSMA IoT Security Guide CLP11-v2.0

| GSMA IoT Security Guide CLP11-v2.0 | | | 5G適用可能性 |
|---|---|---|---|
| チャレンジ1 | 可用性 | How can Low Power Wide Area (LPWA) networks (e.g. NB-IoT and LTE-M) be deployed and operated with a similar level of security to traditional cellular systems? | 4Gまでのモバイル・ネットワークでは同一のセキュリティ機能が要請されたが、5Gでは独立したスライスへの分割が可能となったため、他に影響を与えることなしにLPWAを必要とするようなローエンド・デバイスへの柔軟な対応が可能となるという方向で検討 |
| | | How can multiple mobile operators support the same level of network security as IoT Endpoints migrate across network boundaries? | 5Gにおける一般的なオペレータ間モビリティ関係構築により実現可能という方向で検討 |
| | | How can network trust be forwarded to capillary Endpoints that rely on Gateway Endpoints for communication? | 計算資源の乏しいローエンド・デバイスであっても5Gへの直接アクセスを可能としたことにより解決するとという方向で検討<br>GWに頼らなければならないEPが残るのであれば（たとえば人体植込型ヘルスケア・デバイス等）にはEP⇔GW間の保護策は残存課題となる |
| | | How can the power constraints of Lightweight Endpoints be addressed in secure communications environments? | 5Gではバッテリにより15年間駆動可能なEPデバイスを収容するユースケースにも対応可能<br>技術的にはSBAの利用（UPFとMEC（Mobile Edge Computing）をデバイス近傍へ配置）という方向で検討 |
| チャレンジ2 | 識別・認証 | Can the user operating the Endpoint be strongly associated with the Endpoint's identity? | エンドポイント利用者もMNO契約者である場合にはMNO内で連想付を行なうことは可能という方向で検討<br>IoTではMNO契約者以外のユーザがEPを操作するユースケースも多数存在するため、そのようなユーザへの対応は残存課題となる |
| | | How can services and peers verify the identity of the end-user by verifying the identity of the Endpoint? | 同上 |
| | | Will Endpoint security technology be capable of securely authenticating peers and services? | 5GではEPと正規ピア/サービスとの間ではセカンダリ認証による相互認証を強制可能という方向で検討 |
| | | Can rogue services and peers impersonate authorized services and peers? | 同上 |
| | | How is the identity of a device secured from tampering or manipulation? | 5Gではクレデンシャル・ストレージ機能によりUICC以外のセキュア・ストレージを利用することが可能という方向で検討 |
| | | How can the Endpoint and Network ensure that an IoT Service is permitted to access the Endpoint? | 5Gではモバイル・ネットワーク外に存在するIoTサービスとUEとの間でのセカンダリ認証をサポート可能という方向で検討 |
| チャレンジ3 | プライバシ | Is the identity of an Endpoint exposed to unauthorized users? | 5Gでは4GまでのIMSIとは異なり、UEの長期有効識別子を漏洩させない手法が導入されたため、それを利用可能という方向で検討 |
| | | Can unique Endpoint or IoT Service identifiers allow an end-user or Endpoint to be physically monitored or tracked? | 同上 |
| | | Is data emanating from an Endpoint or IoT Service indicative of or directly associated with physical end-user attributes such as location, action, or a state, such as sleeping or awake? | モバイル・ネットワーク全区間での安全な暗号化方式の利用により対応可能という方向で検討 |
| | | Is confidentiality and integrity employed with sufficient security to ensure that patterns in the resultant cipher-text cannot be observed? | 同上 |
| | | How does the product or service store or handle user-specific Personally Identifiable Information (PII)? | 製品ないしサービスがPIIをどのように保存/処理するかに関しては5Gでは関知できない |
| | | Can the end-user control the storage or use of PII in the IoT Service or product? | 同上 |
| | | Can the security keys and security algorithms used to secure the data be refreshed? | 5Gフェーズ2では長期有効鍵（UICCとコア・ネットワークで共有されるK)の更新可能化方式に関して検討予定 |
| チャレンジ4 | セキュリティ | Are security best practices incorporated into the product or service at the start of the project? | 5Gコアに関連する機能要素に関しては3GPP SCAS（Security Assurance Specification）の枠組を用いた取組が存在するので、それを利用するという方向で検討 |
| | | Is the security life-cycle incorporated into the Software or Product Development Life Cycle? | 同上 |
| | | Is application security being applied to both services and applications running on the embedded system? | 現時点では5Gセキュリティの取り扱う範疇にないと考えられるが、検討することが必要。<br>[残存課題] 5Gネットワーク経由でアプリケーション・セキュリティの状態に関する検査機能を提供するという可能性はあるか？ |
| | | Is a Trusted Computing Base (TCB) implemented in both the Endpoint and the Service Ecosystem? | 同上 |
| | | How does the TCB enforce self-verification of application images and services? | 同上 |
| | | Can the Endpoint or IoT Service detect if there is an anomaly in its configuration or application? | 同上 |
| | | How are Endpoints monitored for anomalies indicative of malicious behaviour? | 同上 |
| | | How is authentication and identity tied to the product or service security process? | 5Gコアに関連する機能要素に関しては3GPP SCAS（Security Assurance Specification）の枠組を用いた取組が存在 |
| | | What incident response plan is defined for detected anomalies indicative of a compromise? | 現時点では5Gセキュリティの取り扱う範疇にないと考えられるが、検討することが必要 |
| | | How are services and resources segmented to ensure a compromise can be contained quickly and effectively? | 同上 |
| | | How are services and resources restored after a compromise? | 同上 |
| | | Can an attack be spotted? | 同上 |
| | | Can a compromised system component be spotted? | 同上 |
| | | How can customers report security concerns? | 同上 |
| | | Can Endpoints be updated or patched to remove vulnerabilities? | 更新データの安全な配布方式部分に関してはOTA更新機構の利用可能性があるという方向で検討 |

表　Annex 2　IoT セキュリティガイドライン

| IoT セキュリティガイドライン | | | | | 5G適用可能性 |
|---|---|---|---|---|---|
| 方針・管理 | 指針1<br>IoT の性質を考慮した基本方針を定める | 要点1 | 経営者がIoT セキュリティにコミットする | 経営者は、「サイバーセキュリティ経営ガイドライン」を踏まえた対応を行う。IoT セキュリティの基本方針を企業として策定し社内に周知するとともに、継続的に実現状況を把握し、見直していく。また、そのために必要な体制・人材を整備する。 | |
| | | 要点2 | 内部不正やミスに備える | ①IoT の安全を脅かす内部不正の潜在可能性を認識し、対策を検討する。<br>②関係者のミスを防ぐとともに、ミスがあっても安全を守る対策を検討する。 | |
| 分析 | 指針2<br>IoTのリスクを認識する | 要点3 | 守るべきものを特定する | ① IoT の安全安心の観点で、守るべき本来機能や情報などを特定する。<br>② つなげるための機能についても、本来機能や情報の安全安心のために、守るべきものとして特定する。 | |
| | | 要点4 | つながることによるリスクを想定する | ①クローズドなネットワーク向けの機器やシステムであっても、IoT 機器・システムとして使われる前提でリスクを想定する。<br>②保守時のリスク、保守用ツールの悪用によるリスクも想定する。 | |
| | | 要点5 | つながりで波及するリスクを想定する | ①セキュリティ上の脅威や機器の故障の影響が、他の機器とつながることにより波及するリスクを想定する。<br>②特に、対策のレベルが低い機器やシステムがつながると、影響が波及するリスクが高まることを想定する。 | |
| | | 要点6 | 物理的なリスクを認識する | ①盗まれたり紛失した機器の不正操作や管理者のいない場所での物理的な攻撃に対するリスクを想定する。<br>②中古や廃棄された機器の情報などの読み出しやソフトウェアの書き換え・再販売などのリスクを想定する。 | |
| | | 要点7 | 過去の事例に学ぶ | ① パソコン等のICT の過去事例から攻撃事例や対策事例を学ぶ。<br>② IoT の先行事例から攻撃事例や対策事例を学ぶ。 | |
| 設計 | 指針3<br>守るべきものを守る設計を考える | 要点8 | 個々でも全体でも守れる設計をする | ①外部インタフェース経由／内包／物理的接触によるリスクに対して個々のIoT 機器・システムで対策を検討する。<br>②個々のIoT 機器・システムで対応しきれない場合は、それらを含む上位のIoT 機器・システムで対策を検討する。 | 外部IFを5Gとすることにより他技術を用いるよりも強固なセキュリティを実現可能<br>GSMA IoT SG：プライバシ#3に同じ |
| | | 要点9 | つながる相手に迷惑をかけない設計をする | ①IoT 機器・システムの異常を検知できる設計を検討する。<br>②異常を検知したときの適切な振る舞いを検討する。 | UPFとMEC（Mobile Edge Computing）をデバイス近傍へ配置することによりデバイスのログ情報収集を省力化<br>技術的にはSBAの利用：GSMA IoT SG: 可用性#4に追記 |
| | | 要点10 | 安全安心を実現する設計の整合性をとる | ①安全安心を実現するための設計を見える化する。<br>②安全安心を実現するための設計の相互の影響を確認する。 | |
| | | 要点11 | 不特定の相手とつなげられても安全安心を確保できる設計をする | ① IoT 機器・システムがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討する。 | |
| | | 要点12 | 安全安心を実現する設計の検証・評価を行う | ①つながる機器やシステムは、IoT ならではのリスクも考慮して安全安心を実現する設計の検証・評価を行う。 | |
| 構築・接続 | 指針4<br>ネットワーク上での対策を考える | 要点13 | 機器等がどのような状態かを把握し、記録する機能を設ける | ① 機器等の状態や他の機器との通信状況を把握して記録する機能を検討する。<br>② 記録を不正に消去・改ざんされないようにする機能を検討する。 | UPFとMEC（Mobile Edge Computing）をデバイス近傍へ配置することによりデバイスのログ情報収集を省力化<br>ログ情報のMECからクラウドへの安全な退避<br>技術的にはSBAの利用：GSMA IoT SG: 可用性#4に追記 |
| | | 要点14 | 機能及び用途に応じて適切にネットワーク接続する | ① 機能及び用途に応じてネットワーク接続の方法を検討し、構築・接続する。<br>② ネットワーク接続の方法を検討する際には、IoT 機器の機能・性能のレベルも考慮する。 | 5Gにより認証・暗号化・完全性保護等の機能を適用<br>GSMA IoT SG：プライバシ#3に同じ |
| | | 要点15 | 初期設定に留意する | ① IoT システム・サービスの構築・接続時や利用開始時にセキュリティに留意した初期設定を行う。<br>② 利用者へ初期設定に関する注意喚起を行う。 | |
| | | 要点16 | 認証機能を導入する | ① IoT システム・サービス全体でセキュリティの確保を実現する認証機能を適用する。<br>② IoT 機器の機能・性能の制約を踏まえた適切な認証方式を使用する。 | 5Gによる認証機能適用可能性<br>GSMA IoT SG：識別・認証#3に同じ |
| 運用・保守 | 指針5<br>安全安心な状態を維持し、情報発信・共有を行う | 要点17 | 出荷・リリース後も安全安心な状態を維持する | ① IoT システム・サービスの提供者等は、IoT 機器のセキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用する。 | 5GによるOTA機能適用可能性<br>GSMA IoT SG：セキュリティ#15に同じ |
| | | 要点18 | 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える | ① 脆弱性情報を収集・分析し、ユーザや他のシステム・サービスの供給者・運用者に情報発信を行う。<br>② セキュリティに関する重要な事項を利用者へあらかじめ説明する。<br>③ 出荷・リリース後の構築・接続、運用・保守、廃棄の各ライフサイクルで関係者に守ってもらいたいことを伝える。 | |
| | | 要点19 | つながることによるリスクを一般利用者に知ってもらう | ① 不用意なつなぎ方や不正な使い方をすると、自分だけでなく、他人に被害を与えたり、環境に悪影響を与えたりするリスクや守ってもらいたいことを一般利用者に伝える。 | |
| | | 要点20 | IoT システム・サービスにおける関係者の役割を認識する | ① IoT 機器メーカやIoT システム・サービス提供者及び一般利用者の役割を整理する。 | |
| | | 要点21 | 脆弱な機器を把握し、適切に注意喚起を行う | ① ネットワーク上でIoT 機器を把握する仕組みを構築し、脆弱性を持つIoT 機器の特定を行う。<br>② 脆弱性を持つIoT 機器を特定した場合には、該当するIoT 機器の管理者へ注意喚起を行う。 | |

表　Annex 3 安全な IoT システムのためのセキュリティに関する一般的枠組

| 安全なIoT システムのためのセキュリティに関する一般的枠組 | | | 5G適用可能性 |
|---|---|---|---|
| 目的 | ・ITと物理的システムが融合したシステムであるIoTでは従来の情報セキュリティ確保に加えて新たに安全確保が重要<br>・すべてのIoTシステムの設計/構築/運用に求められる一般的要求事項となるセキュリティ要件基本要素を明らかにすることが本文書の目的 | | 大所高所に立つ観点からの枠組の記述であるため、5Gを利用してIoTセキュリティを向上させるという技術的問題に対しての貢献は見受けられなかった |
| 検討の視点 | ・IoTシステムはモノ同士がインターネットで接続されることにより新たな価値を創出<br>・モノが接続されるため、物理的安全性の考慮が必要<br>・IoTシステム同士が相互に接続されることでさらに新たな価値を生み出し得るが、一つのIoTシステムのリスクが他のIoTシステムに波及する可能性もあるため、『システムのシステム』として捉えることが必要<br>・IoTセキュリティ一般的枠組においては安全性/機密性/完全性/可用性の4要件の確保が前提 | | |
| 基本原則 | ・モノとネットワークが連携したシステムで全体としてのセキュリティ確保のための要件としては基本方針の設計、リスク評価、システム設計、システム構築、運用・保守の各段階で求められる要件定義が必要であり、以下の各項目の明確化が必要<br>a) システムについての範囲、対象を含めた定義の明確化およびリスクを踏まえたシステム特性に基づく分類<br>b) 情報の機密性/完全性/可用性確保およびモノの動作に係る安全性確保要件の明確化<br>c) 確実な動作の確保および障害発生時の迅速なサービス回復に必要な要件の明確化<br>d) モノとネットワークに求められる安全確保水準の明確化<br>e) 故障およびサイバー攻撃実施等で機密性/完全性/可用性/安全性が確保されること<br>f) 責任分界点/情報所有権を含めたデータ取扱の在り方の明確化 | | |
| 取組方針 | 要求事項の明確化 | 1. 法令・規制要求事項、2. 非明示要求事項、3.業界等判断の追加要求事項の各事項について明確化 | |
| | IoT システムのモデル化 | 多層的なIoTシステム構成の適切なモデル化ならびにモデルを参照にしたセキュリティ要件検討 | |
| | リスクに応じた対応 | モノの接続によってもたらされるメリットとリスクを客観的に捉え、採るべきセキュリティ対策/実装方法等を明確化 | |
| | 性能要求と仕様要求の適切な適用 | 普遍的な性能要求と採り得る有効な具体的手段を示す仕様要求の2つから構成 | |
| | 段階的・継続的アプローチ | 基本的な機能要件定義とそれに対する段階的・継続的な進化を可能とする | |
| | 役割分担及び連携した対処のあり方の明確化 | IoTシステムに関連する者の役割分担を明確化し、各主体の連携・協調によるセキュリティ確保の在り方/各主体間の責任分界点の明確化 | |
| | その他運用ルールの検討 | IoTシステム運用に係るその他の事項についての社会的ルールの具体化を図り、機器認証の在り方について主体の在り方や運用ルールを明確化 | |
| 留意事項 | 本枠組は現時点で想定されるIoT システムを前提として策定されたものであり、技術革新等によるIoT システムの機能の高度化等に併せ、適宜見直しを図ることとする。その際、広く国内外を含めた関係者(マルチステークホルダー)の意見や議論を踏まえたものとする。<br>また、既にある国内外のガイドライン2や基準等及びそれらの策定団体との連携・協調を図る | | |

# 表　Annex 4　IoT セキュリティ総合対策

| IoTセキュリティ 総合対策 | | | | 5G適用可能性 |
|---|---|---|---|---|
| 基本的考え方 | ・IoTシステムのセキュリティについては安全な『IoT システムのためのセキュリティに関する一般的枠組』を踏まえた総合的視点に立った対策構築が必要<br>・同枠組で提唱された機器、ネットワーク、認証等のプラットフォーム、サービス等のレイヤーに分けての分析・検討を行うため、各レイヤーに分けて想定課題を抽出<br>a) サービス層：IoTシステム動作が正しいデータに基づくことが必須要件でありデータ真正性担保のための対策強化が必要<br>b) プラットフォーム層：異なるシステム間の運用基準共通化/異システム間での情報共有耐性強化が必要<br>c) ネットワーク層：機器層とプラットフォームとを繋ぐデータ転送役割を担い、IoT機器で主として用いられる無線ネットワークにおける脆弱性最小化が必要<br>d) 機器層：IoT機器管理、脆弱性検知・措置・切断等を関係者が連携して実現可能な体制構築が不可欠 | | | 具体的施策としては脆弱性対策に係る体制整備、研究開発の推進、民間企業等におけるセキュリティ対策の促進等の体制整備的な側面からの文書であり、5Gを利用してIoTセキュリティを向上させるという技術的問題に対しての貢献は見受けられなかった |
| 具体的施策 | 脆弱性対策に係る体制整備 | 設計・製造段階 | セキュリティ・バイ・デザイン等の意識啓発・支援の実施<br>設計・製造段階においては、所有者・運用者・利用者による安全な設定が行われるよう、ID/パスワード設定、ファームウェアのアップデート及びWi-Fi設定の仕様を設計時に盛り込むなど、製造業者におけるセキュリティ・バイ・デザインの考え方をいかに浸透させるかが重要 | |
| | | 販売段階 | 認証マークの付与及び比較サイト等を通じた推奨<br>一定のセキュリティ要件を満たすIoT 機器への認証マーク付与や、比較サイト等を通じて認証マークが付与された機器が推奨される仕組の構築 | |
| | | 設置段階 | IoT セキュアゲートウェイ<br>機器の設置(ネットワークへの接続)段階において、脆弱性を有する機器が存在することを前提としたセキュアなシステム構築が実現できる仕組作り | |
| | | 運用・保守段階 | セキュリティ検査の仕組作り<br>機器の脆弱性に係る接続試験を行うテストベッドの構築を含む継続的な安全性を確保するためのセキュリティ検査の仕組作りおよび対策が不十分なIoT 機器への対応についての検討が必要 | |
| | | | 簡易な脆弱性チェックソフトの開発等<br>IoT 機器利用者に対して簡易に脆弱性をチェックできるソフトを開発して配布する取組や、脆弱性を調査する民間サービス実施の促進を検討 | |
| | | 利用段階 | 利用者に対する意識啓発の実施や相談窓口等の設置<br>従来の端末機器以上に利用者による十分な対応が重要となることを踏まえ、利用者に対する意識啓発を推進していくことが必要 | |
| | | 脆弱性調査の実施 | 重要IoT 機器に係る脆弱性調査 | |
| | | | サイバー攻撃の踏み台となるおそれがある機器に係る脆弱性調査 | |
| | | | 被害拡大を防止するための取組の推進 | |
| | | | IoT 機器に関する脆弱性対策に関する実施体制の整備 | |
| | 研究開発の推進 | | 基礎的・基盤的な研究開発等の推進 | |
| | | | 広域ネットワークスキャンの軽量化 | |
| | | | ハードウェア脆弱性への対応 | |
| | | | スマートシティのセキュリティ対策の強化 | |
| | | | 衛星通信におけるセキュリティ技術の研究開発 | |
| | | | AI を活用したサイバー攻撃検知・解析技術の研究開発 | |
| | 民間企業等におけるセキュリティ対策の促進 | | 民間企業のセキュリティ投資等の促進<br>IoT 産業等の関連産業等の成長を見据えて企業におけるセキュリティ投資を促進するため、高レベルのサイバーセキュリティ対策に必要なシステムの構築やサービスの利用に対して、税制優遇措置を講ずる方向での検討が必要 | |
| | | | セキュリティ対策に係る情報開示の促進<br>任意の情報開示であることを前提としつつ、企業のセキュリティ対策に係る情報開示に関するガイドラインの策定について検討することが必要 | |
| | | | 事業者間での情報共有を促進するための仕組みの構築<br>解析・対処能力が事業者間で一様ではないことを踏まえ、情報共有の目的・利点・手順、必要とされる情報を明確化するとともに、平時・非常時などの状況に応じた提供すべき情報の範囲及び提供先の範囲等を明確化することが重要 | |
| | | | 情報共有時の匿名化処理に関する検討<br>情報の秘匿性を担保する観点から情報の匿名化処理の導入を検討する必要があるため、その際、どのような方法で、どの程度まで情報を匿名化するべきかについての評価指標やガイドラインの整備の検討が必要 | |
| | | | 公衆無線LAN のサイバーセキュリティ確保に関する検討<br>普及が進む公衆無線LAN のサービスにおいて、セキュリティに対する配慮に欠けるものも多く、これらのサービスを踏み台にした攻撃や情報漏洩などのインシデントが発生することが考えられるため、公衆無線LAN におけるサイバーセキュリティ上の課題を整理し、今後必要な対策について検討することが必要 | |
| | 人材育成の強化 | | 実践的サイバー防御演習（CYDER）の充実 | |
| | | | 2020 年東京大会に向けたサイバー演習の実施 | |
| | | | 若手セキュリティ人材の育成の促進 | |
| | | | IoT セキュリティ人材の育成 | |
| | 国際連携の推進 | | ASEAN 各国との連携 | |
| | | | 国際的なISAC 間連携 | |
| | | | 国際標準化の推進 | |
| | | | サイバー空間における国際ルールを巡る議論への積極的参画 | |

表　Annex5　サイバー・フィジカル・セキュリティ対策フレームワーク(案)

| サイバー・フィジカル・セキュリティ対策フレームワーク（案） | | | 5G適用可能性 |
|---|---|---|---|
| はじめに | ・Society5.0とConnected Industriesが実現する社会においてはサイバー空間とフィジカル空間とを高度に融合させることで多様なニーズにきめ細やかに寄り添うモノやサービスを提供可能な超スマート社会の実現が期待されている<br>・同時にサイバー攻撃による脅威が増大することが懸念されており、そうした脅威の増大および新たな脅威の出現に対する防御を可能にするための新たな対策フレームワークが必要 | | |
| コンセプト | ・サイバー空間とフィジカル空間が高度に融合した産業社会における産業分野のサイバーセキュリティの在り方<br>1) サイバー空間とフィジカル空間が高度に融合した産業社会における「Society5.0」型サプライチェーン“価値創造過程（バリュークリエイションプロセス）”への対応<br>2) 価値創造過程（バリュークリエイションプロセス）のセキュリティを確保するための信頼性(trustworthiness)の基点を設定するためのモデル －三層構造アプローチと6つの構成要<br>3) 価値創造過程（バリュークリエイションプロセス）におけるリスク源とそれに対応する方針の整理 | | |
| ポリシー | ・リスク源の洗い出しと対策要件の特定<br>1) 分析対象の明確化(三層構造モデルへの落とし込み)<br>リスクアセスメントにおける分析対象の明確化について、(1) 実施プロセス、(2) 実施上の留意点を記述<br>2) 想定されるセキュリティインシデント及び事業被害レベルの設定<br>明確化された分析対象に対して重大な影響を及ぼすセキュリティインシデントの整理および事業への影響の整理を記述<br>3) リスク分析の実施<br>1) & 2) の内容を踏まえ、セキュリティインシデントに繋がる攻撃シナリオの検討、被害レベル、リスク源の評価等を実施<br>4) リスク対応の実施<br>3) の結果得られたリスクに対して回避／低減／移転／保有のいずれの対応をとるかを想定される被害の大きさ等に基づき検討 | | |
| メソッド：セキュリティ対策要件と対策例集 | 資産管理 | 企業等が事業目的を達成することを可能にするデータ、ヒト、モノ、システム、それらが管理される場所等の特定および重要性に応じた管理の実現 | |
| | ビジネス環境 | 自組織のミッション、目標、利害関係者、活動を理解し、優先順位付けを実施 | |
| | ガバナンス | 自組織に対する規制、法律、リスクと、自組織の環境、運用上の要求事項を管理しモニタリングするためのポリシー、手順、プロセスを理解し、サイバーセキュリティリスクの管理者に伝達 | |
| | リスク評価 | 自組織の業務(ミッション、機能、イメージ、評判を含む)、資産、個人に対するサイバーセキュリティリスクを把握 | |
| | リスク管理戦略 | 自組織の優先順位、制約、リスク許容度、想定を定め、運用リスクの判断に利用 | |
| | サプライチェーンリスク管理 | 優先順位、制約、リスク許容値、および想定を、サプライチェーンリスク管理に関連するリスクの決定を支援するために確立し、利用する | |
| | アイデンティティ管理、認証およびアクセス制御 | 資産およびそれが管理される場所への論理的・物理的アクセスを、承認されたソシキ、ヒト、モノ、プロシージャに限定し、承認された活動およびトランザクションに対する不正アクセスのリスクの大きさに合うよう管理 | 5Gによる認証機能の適用<br>GSMA IoT SG：識別・認証#3に同じ |
| | 意識向上及びトレーニング | 職員およびパートナーに対して、関連するポリシー、手順、契約に基づいた、サイバーセキュリティに関連する義務と責任を果たすために、サイバーセキュリティ意識向上教育と、訓練を実施 | |
| | データセキュリティ | データと記録をデータの機密性、完全性、可用性を保護するために定められた自組織のリスク戦略に従って管理 | 5Gによる暗号化・完全性保護等の機能を適用<br>GSMA IoT SG：プライバシ#3に同じ |
| | 情報を保護するためのプロセス及び手順 | (目的、範囲、役割、責任、経営コミットメント、組織間の調整を扱う)セキュリティポリシー、プロセス、手順を維持し、システムと資産の保護の管理に使用 | |
| | 保守 | 産業用制御システムと情報システムの構成要素の保守と修理をポリシーと手順に従って実施 | |
| | 保護技術 | 関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティとレジリエンス、セーフティを確保するための、技術的なソリューションを管理 | |
| | 異常とイベント | 異常な活動を検知し、事象がもたらす可能性のある影響を把握 | |
| | セキュリティの継続的モニタリング | セキュリティ事象を検知し、保護対策の有効性を検証するために、システムと資産をモニタリング | |
| | 検知プロセス | 異常なセキュリティ事象を正確に検知するための検知プロセスおよび手順を維持し、テスト | |
| | 対応計画 | 検知したセキュリティインシデントに対応し、適切に自組織の事業を継続しつつ、影響を受ける資産やシステムを復元できるよう、対応・復旧のプロセスおよび手順を実施&維持 | |
| | 伝達 | 法執行機関のような組織からの支援を得られるよう、内外の利害関係者(例えば、取引先、JPCERT/CC、他組織のCSIRT、ベンダー)との間で対応・復旧活動を調整 | |
| | 分析 | 効率的な対応を確実にし、復旧活動を支援するために、分析を実施 | |
| | 低減 | セキュリティ事象の拡大を防ぎ、その影響を緩和し、セキュリティインシデントを解消するための活動を実施 | |
| | 改善 | 現在と過去の意思決定／対応活動から学んだ教訓を取り入れることで、自組織の対応・復旧活動を改善 | |

表　Annex 6　IoT 開発におけるセキュリティ設計の手引き I

| | Ｉ ｏ Ｔ 開発におけるセキュリティ 設計の手引き | | 5G適用可能性 |
|---|---|---|---|
| はじめに | ・IoTのセキュリティ現状と課題<br>IoT固有の課題：(1) ネットに繋がる脅威を考慮していない機器の接続、(2) 生命に関わる機器やシステムの接続を想定、(3)「モノ」同士の無線等での自律的な接続を想定、(4)「モノ」のコストの観点から、不十分なセキュリティ対策が想定、(5) ネットを介して収集される情報の用途は、「モノ」側では制御が困難であり、バックエンドシステム側での管理範囲となる、(6) つながる世界を拡げていくためには、「モノ」同士の技術的（通信プロトコル、暗号、認証等）、およびビジネス的な約束事が不可欠<br>・本書のねらい<br>1) IoT の全体像をモデル化し、各々の構成要素を定義、2) IoT のセキュリティ設計において行うべき、脅威分析・対策検討・脆弱性への対応について解説、3) セキュリティを検討する上で参考となる、IoT 関連のセキュリティガイドを紹介、4) いくつかの例題をもとに、IoT システムにおける脅威分析と対策検討の実施例を示す、5) IoT システムのセキュリティを実現する上で根幹となる暗号技術の重要性を説明し、実装した暗号技術の安全性を客観的に評価するためのチェックリストを添付 | | 基本的にIoT機器開発者としての立場で機器のセキュリティ設計をどうすべきかというスタンスの文書であるため、5Gを利用してIoTセキュリティを向上させるという技術的問題に対しての貢献は見受けられなかった |
| Ｉｏ Ｔの定義 | IoT構成要素の定義<br>・サービス提供サーバ・クラウド<br>・中継機器<br>・システム（中継機器経由でネットワークに接続される複数の機器で構成されたシステムのこと）<br>・デバイス<br>・直接相互通信を行うデバイス | | |
| Ｉｏ Ｔのセキュリティ設計 | ・一般にIoT製品やサービスのセキュリティ設計を行う場合は以下の手順を実施<br>Step1：対象とするIoT 製品やサービスのシステム全体構成を明確化<br>Step2：システムにおいて、保護すべき情報・機能・資産を明確化<br>Step3：保護すべき情報・機能・資産に対して、想定される脅威を明確化【脅威分析】<br>Step4：脅威に対抗する対策の候補（ベストプラクティス）を明確化【対策検討】<br>Step5：どの対策を実装するか、脅威レベルや被害レベル、コスト等を考慮して選定<br>・IoT のセキュリティ設計における脅威分析と対策検討、セキュリティ対策の一つとして必要不可欠な脆弱性への対応について記述 | | |
| | 脅威分析 | 対象となるシステム全体/構成要素に対して想定される脅威を明確化し、脅威に対する脆弱性評価および脅威に起因するリスクの評価を行なう攻撃ツリー型脅威分析手法を用いてネットワークカメラに対して評価した結果を事例紹介 | |
| | セキュリティ対策検討 | 脅威分析の結果に基づき必要なセキュリティ対策を検討する。前項で例示した脅威分析結果に対して対策検討した結果を紹介 | |
| | 脆弱性への対応 | 脆弱性への対応として以下を記述<br>a) 開発段階での対応<br>脆弱性の新たな作り込み排除、既知脆弱性解消、残留脆弱性の検出/解消、製品出荷後に発見される新規脆弱性への準備<br>b) 運用段階での対応<br>脆弱性対策情報の継続的収集、更新SW/FW を含む脆弱性対策情報の作成、脆弱性対策情報の利用者への通知、更新SW/FWの製品への適用<br>c) IPA提供コンテンツ活用<br>脆弱性対策情報データベース：JVN iPedia、脆弱性届出制度、IoT製品・サービス脆弱性対応ガイド | |
| Ｉｏ Ｔ関連ＳＧ | IoTセキュリティ検討にあたって参考となる国内外において様々な機関・団体から公表されたIoT関連セキュリティに関するガイドライン等をIPA/国内機関・団体/国外機関・団体に分類して紹介し、以下の3団体に関する活動と同団体公表ガイドラインに関する紹介がなされている<br>a) OWASP（Open Web Application Security Project）<br>b) OTA（Online Trust Alliance）<br>c) GSMA（GSM Association） | | |
| 脅威分析／対策検討実施例 | IoTのセキュリティ設計章で示したセキュリティ設計の手順に従い1)デジタルテレビ、2)ヘルスケア機器とクラウドサービス、3)スマートハウス、4)コネクテッドカーを題材としたIoT システムに対して以下を実施<br>a) 対象IoT システム／サービスの全体構成図の作成<br>b) 保護すべき情報・機能・資産の明確化<br>c) 想定される脅威の明確化<br>d) 対策候補（ベストプラクティス）の明確化 | | |

表　Annex 7　IoT セキュリティ評価検証ガイドライン

| | IoT セキュリティ評価検証ガイドライン | 5G適用可能性 |
|---|---|---|
| IoTの現状と脅威 | 組込み機器メーカの課題:<br>・製品の競争力向上のためには、通信ネットワーク連携による高度化が必要であるが、そのためには具体的なセキュリティ基準の策定が必要<br>・同時にセキュリティ検査ツールや、検査、認証基準の整備を行い、セーフティで実施されているような第三者による客観的、定量的な検査・検証が行われる仕組みづくりが必要<br>本文書の位置づけ:<br>本文書はいくつかの団体より発行されたセキュリティガイドラインの評価検証に関する項目に対して、スマートホーム分野での実例を取り入れつつ、IoT 機器全般を対象に、具体的なセキュリティの評価検証プロセスを更に掘り下げた内容として策定 | 基本的に組込機器開発者としての立場で機器のセキュリティ評価検証のために実施する評価検証手法を説明するというスタンスの文書であるため、5Gを利用してIoTセキュリティを向上させるという技術的問題に対しての貢献は見受けられなかった |
| セキュリティ評価検証の手法 | 評価検証手法はプログラムの実行を伴わずにロジックの評価検証を行う静的な検証手法と、実際にプログラムを動作させた上で挙動を確認する動的な検証手法に大別される<br>a) 静的検証手法<br>・設計ドキュメントレビュー<br>各種設計ドキュメントに対して、「セキュリティバイデザイン」の考え方に基づき、必要なセキュリティ対策が組み込まれているかどうかをレビューによって確認する。<br>・ソースコードレビュー(解析)、コーディング規約検証<br>ソースコードに対して、セキュリティ上の脆弱性の検証や、コーディング規約に基づく実装が行われているかどうかの検証を行う。ソースコードに対する検証は各種静的検証ツールによる検証の自動化が主流であり、業務効率化のためにも有効に活用することが望ましい<br>b) 動的検証手法<br>・既知の脆弱性検証手法<br>脆弱性スキャンチェック、脆弱性情報に基づくペネトレーションテスト<br>・未知の脆弱性検証手法<br>ファジングテスト | |
| 評価検証実行 | セキュリティ評価検証の実行は、自動化されたツールを用いた場合でも評価検証内容の組み合わせによって、実行処理完了までに時間を要する可能性がある。ツールの実行所要時間については、事前に把握しておくことが望ましい。<br>ツールによる検証完了後の出力結果については、ツールが出力した結果に対して、ログ情報等をもとに、結果の正当性を評価検証者が解析し、結果判定を行う必要がある。また評価検証者が正しい判定を行うためには、DUT 側のプログラムに関する知識や、ツール側の結果判定ロジックについても理解しておくことが必要となる<br>評価検証者が結果判定を行うために必要な情報やナレッジを記載 | |

表　Annex 8　IoT セキュリティ標準／ガイドライン ハンドブック

| | IoTセキュリティ 標準／ガイドライン ハンドブック | | 5G適用可能性 |
|---|---|---|---|
| はじめに | セキュリティ課題が最も多いと考えられたコンシューマIoT向けセキュリティ提言をまとめた報告書を2016年に発行したが、その後コンシューマ向けのみならず多数の業種／産業向けIoTセキュリティに関する整理が多くの組織・団体によりなされた結果、多数の指針／標準が発行されたという現状を踏まえて、それら多数の文書を読み解くことが容易となるように主要文書の目的／対象読者／特徴などをまとめた文書が本ハンドブックである | | |
| 掲載IoTセキュリティ標準／ガイドライン概要 | ・STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT) | U.S. Department of Homeland Securityによって発行されたIoTの安全性確保のための戦略的原則と推奨される最良実践を記述した文書 | |
| | ・Security and Resilience of Smart Home Environments<br>・Security and Resilience of Inteligent Public Transport good practices and recommendations<br>・Cyber Security for Smart Cities<br>・Cyber security and resilience for Smart Hospitals<br>・Securing Smart Airports<br>・Cyber Security and resilience of smart cars<br>・Baseline Security Recommendations for IoT | IoTとスマートインフラにおけるセキュリティおよびレジリエンスに関して実務家と専門家によるWG/会議体による調査・分析結果をまとめたENISAによる公開文書群 | |
| | ・Internet of things Privacy &Security in a Connected World FTS Staff Report JAN 2015 | IoTでのプライバシー問題を中心とした法制化へ向けた専門家からなるパネリストによる議論の結果をまとめたU.S. FTCによる公開文書 | |
| | ・Best Current Practices for Securing Internet of Things (IoT) Devices | IoTデバイス・ベンダが開発中およびアップデートを作成する際にそれらのデバイスが関与するセキュリティ・インシデントの頻度と重大性を減少させるために考慮が必要な最小限の要件をまとめたIETFネットワークWGによる公開文書 | |
| | ・IoTセキュリティガイドライン | IoT推進コンソーシアムによる公開資料（本Excel Sheet #1） | |
| | ・IoT開発におけるセキュリティ設計の手引き<br>・つながる世界の開発指針<br>・安全なIoTシステムのためのセキュリティに関する一般的枠組 | IoTセキュリティに関する手引き（本Excel Sheet #4）およびフレームワークを記述したIPAによる公開資料 | |
| | ・INTERNET OF THINGS：RISK AND VALUE CONSIDERATIONS | IoTに取り組む組織が考慮すべき重要な事項を9つの質問という形で提示したISACAによる公開資料。IoTのビジネス的価値とリスクという両面からの考慮がなされている点が特徴的 | |
| | ・SP800−160 Systems Security Engineering | システムのセキュリティ・エンジニアリングの概念から各ライフサイクルでどのようにセキュリティを組み込むべきか等を記述したNISTによる公開文書。全体的にはセキュリティというものは単独で考える要件にはあらず、システム全体の中で考慮／検討されるべきという考え方を示す | |
| | ・ITU-T Recommendation Y.4806 Secyruty capabilities supporting safety of the Internet of Things | IoTがもたらすセキュリティ的脅威を分類してそれぞれが安全に対してどのような影響をもたらすかを検討したITU-Tによる公開文書 | |
| | ・OTA IoT Trust Framework (V2) | OTA (Online Trust Alliance) によるIoT向けセキュリティ機能のフレームワークを記述した公開文書 | |
| | ・OWASP IoT Security Guidance | IoTのセキュリティに関して (1) 製造者、(2) 開発者、(3) 消費者という3種類の対象者別に作成されたOWASPによるセキュリティ・ガイダンス文書 | |

表　Annex 9　JSSEC IoT セキュリティチェックシート 1/3

| JSSEC IoT セキュリティチェックシート | | | | | 5G適用可能性 |
|---|---|---|---|---|---|
| 方針・管理 | 指針1<br>IoT の性質を考慮した基本方針を定める | 要点1 | 経営者がIoT セキュリティにコミットする | 企業へIoT機器を導入しネットワークに接続する時に検討すべき内容を方針として明確にする<br>・指針2のIoTのリスクを認識し、経営層に提言し現状のセキュリティポリシーの見直しをする<br>・IoTの特性（数が多い、機器と一体、持ち出しやすい、人への安全に関わる等）を考慮する □<br>・必要な体制を整備し、人材を確保して育成する | |
| | | 要点2 | 内部不正やミスに備える | □IoT機器について内部不正やミスの対策を検討する<br>・重大な事故や障害につながる行為に対しルールなどを定める | |
| 分析 | 指針2<br>IoTのリスクを認識する | 要点3 | 守るべきものを特定する | □守りたい機能と守りたい情報を明確にする<br>・守るべき機能（人に被害を与えないなど）を明確にする □<br>・守るべき情報（蓄積情報、流れる情報、設定情報など）を明確にする □<br>□信頼出来るIoT機器（認証や実績）、IoTシステム、サービスか確認をする<br>・実績多い信頼性の高いサービスを検討する□<br>・第三者による評価や監査を受けている信頼性の高い機器やサービスの利用を検討する | |
| | | 要点4 | つながることによるリスクを想定する | □つながることにより攻撃を受けるリスクを想定する<br>・ソフトウェアやハードウェアの設定の不備（ミス）による外部からの攻撃を想定する □<br>－ 設定情報やプログラムの改ざんなど<br>－ 情報の漏洩や機能の悪用、機能停止など<br>－ 社内や外部への攻撃の踏み台など<br>・保守ポートからの攻撃を想定する<br>・不正な相手に接続するリスク（乗っ取りを含む）を想定する<br>□保守作業時のリスクを想定する<br>・保守員の悪意を想定する<br>・保守ツールからのウイルス感染を想定する | |
| | | 要点5 | つながりで波及するリスクを想定する | □つながることで異常が伝播し意図せず攻撃するリスクを想定する<br>・ソフトウェアやハードウェアの設定の不備（ミス）による外部への攻撃を想定する□<br>－ 機能停止など<br>－ 攻撃の踏み台など<br>□脆弱なIoT機器がつながることで異常が伝播するリスクを想定する<br>・連携する機器やシステムに影響をあたえるリスクを想定する □<br>・ウイルスなどが波及するリスクを想定する □<br>・既存機器（セキュリティ対策が不十分な組込系など）へ影響をあたえるリスクを想定する | |
| | | 要点6 | 物理的なリスクを認識する | □IoT機器の盗難・紛失・破壊などのリスクを想定する<br>・盗難・紛失時のリスクを評価し、対策が必要な場合には検討する<br>□IoT機器の破棄や転売時に情報を読み出されるリスクを想定する<br>・個人情報・秘密情報などが漏洩するリスクを想定する<br>□中古のIoT機器購入のリスク（不正な設定など）を想定する<br>・ウイルスや不正なソフトが組み込まれているリスクを想定する | |
| | | 要点7 | 過去の事例に学ぶ | □パソコン等、ICT におけるセキュリティ対策を参考にする<br>・不要なインターネット接続をしない、ファイアウォールの設置、初期設定の変更などを参考にする | |
| 設計 | 指針3<br>守るべきものを守る設計を考える | 要点8 | 個々でも全体でも守れる設計をする | □守るべきデータが暗号化されているか確認する<br>・IoT機器やIoTシステムに保管されている情報が暗号化されているか確認する | 外部IFを5Gとすることにより他技術を用いるよりも強固なセキュリティを実現可能 |
| | | 要点9 | つながる相手に迷惑をかけない設計をする | ①IoT 機器・システムの異常を検知できる設計を検討する。<br>②異常を検知したときの適切な振る舞いを検討する。 | UPFとMEC（Mobile Edge Computing）をデバイス近傍へ配置することによりデバイスのログ情報収集を省力化 |
| | | 要点10 | 安全安心を実現する設計の整合性をとる | ①安全安心を実現するための設計を見える化する。<br>②安全安心を実現するための設計の相互の影響を確認する。 | |
| | | 要点11 | 不特定の相手とつなげられても安全安心を確保できる設計をする | ① IoT 機器・システムがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討する。 | |
| | | 要点12 | 安全安心を実現する設計の検証・評価を行う | ①つながる機器やシステムは、IoT ならではのリスクも考慮して安全安心を実現する設計の検証・評価を行う 。 | |

表　Annex 10　JSSEC IoT セキュリティチェックシート 2/3

| | | | | | |
|---|---|---|---|---|---|
| 構築・接続 | 指針4<br>ネットワーク上での対策を考える | 要点13 | 機器等がどのような状態かを把握し、記録する機能を設ける | □IoT機器の必要なログが取れるか確認する<br>・故障やエラー情報（セーフティ解析用）が取れるか確認する<br>・動作環境の情報（リライアビリティ解析用）が取れるか確認する<br>－ データが送られて来ない、大量のデータが送られるといったIoT機器異常を検知するなど<br>・攻撃や認証の情報、アクセス履歴（セキュリティ解析用）が取れるか確認する<br>・保管期間など方針を検討する<br>□IoT機器の不要なログが取られてないか確認する<br>・センシティブな情報のログ出力をしない（センシティブな情報を含む場合は暗号化する）<br>□IoT機器の必要なログが安全に保管されるか確認する<br>・不正アクセス対策がされていること（改ざん・消去対策）を確認する<br>・ログへのアクセス権限の設定を確認する<br>・ログの暗号化を確認する<br>・保管場所を確認する | ・UPFとMEC（Mobile Edge Computing）をデバイス近傍へ配置することによりデバイスのログ情報収集を省力化<br>・ログ情報のMECからクラウドへの安全な退避 |
| | | 要点14 | 機能及び用途に応じて適切にネットワーク接続する | □IoT機器の機能及び用途に応じてネットワークへ接続する方針や条件を検討する<br>・IoT機器のインターネットへの接続が必要か否か検討する（閉域網の検討）□<br>・IoT機器をネットワークへ接続する際には、認証および暗号化によるセキュリティ対策を実施する<br>・セキュリティ対策が不十分なIoT機器を直接インターネットに接続しないように留意する<br>□IoT機器の接続、IoTシステムのゲートウェイ経由の接続などの環境に応じた暗号化を検討する<br>・Wi-Fiネットワークへの接続を設定する際には、より強い暗号方式を使用する（例、WPA2）□<br>・可能な場合、有線での接続も検討する<br>・Telnetログインを無効にし、可能な限りSSHを利用する□<br>・IoT機器に格納するデータの暗号化を検討する<br>□セキュリティの確保が難しいIoT機器を導入する際は別途セキュリティ製品を導入するなど、全体でセキュリティを確保をする<br>・セキュリティ対策が困難なIoT機器は、セキュアなゲートウェイを経由する<br>・データ暗号化、DBファイアウォールなどを実施する | ・5G Network Slicingによる閉域網の提供<br>・5Gにより認証・暗号化・完全性保護等の機能を適用<br>・5G CNのみに留める<br>・5Gではクレデンシャル・ストレージ機能によりUICC以外のセキュア・ストレージを利用することが可能 |
| | | 要点15 | 初期設定に留意する | □IoT機器、IoTシステム、サービスの管理者権限・利用者権限のIDとパスワードの設定及び管理を適切に行う<br>・IDとパスワードを初期設定のままとせず、適切に変更（変更後の文字数、文字種別等にも留意）する□<br>・第三者に知られないよう厳重に管理する□<br>・IDとパスワードを権限のないユーザと共有しない□<br>－ 管理者の権限（監視、制御、設定変更など）と利用者権限を分割する<br>□IoT機器、IoTシステムの不要なサービスやポートは停止するなど必要最小限の設定を行う<br>・デフォルトで有効になっている不要な機能やサービスは無効にする□<br>・サービスに必要のない不要なポートは停止する□<br>□IoT機器の導入時点で最新のファームウェアにアップデートする<br>・IoT機器のファームウェアを最新のバージョンにアップデートする□<br>□IoT機器への外部からの不正アクセスを防止する<br>・ファイアウォールなどにより外部からのアクセス制御を行う<br>□設定情報が改ざんや変更されないようにする<br>・管理者以外によるIoT機器、IoTシステム、サービスの設定変更を禁止する□ | ・5Gで認証用クレデンシャル等の安全な提供を行なえる可能性は？ |
| | | 要点16 | 認証機能を導入する | □IoT機器、IoTシステム、サービスに対して適切な認証機能を利用する<br>・IoT機器の認証を検討する（電子証明書、IoT機器識別子など）<br>・利用者（ユーザ）の認証を検討する（ID/パスワード、ICカード、生体認証など）<br>・IoTシステム、サービス（クラウド等）の認証を検討する（電子証明書など）<br>・ファームウェアを更新する場合、ファームウェアの真贋判定機能を検討する | ・5Gによる認証機能適用可能性<br>・利用者所有5G端末経由の認証可能性<br>・5Gセカンダリ認証<br>・5GによるOTA更新機能の適用可能性 |

表　Annex 11　JSSEC IoT セキュリティチェックシート 3/3

| | | | | | |
|---|---|---|---|---|---|
| 運用・保守 | 指針5<br>安全安心な状態を維持し、情報発信・共有を行う | 要点17 | 出荷・リリース後も安全安心な状態を維持する | □IoT機器、IoTシステム、サービスの使用期間とサポート期間を確認する<br>・IoT機器、IoTシステムやサービスのサポート期限（EOL/EOSL）が提示される/されているか確認する□<br>・アップデート可能な期間を確認する□<br>□IoT機器のアップデート手順を確認する<br>・アップデート情報やアップデートファイルの入手方法を確認する。□<br>・アップデート手順を確認する□<br>・アップデート時の安全性（認証機能やアップデートファイルの暗号化など）を確認する<br>□IoT機器のアップデート手順を策定する<br>・アップデートする判断基準を定める□<br>・安全にアップデートする手順とアップデート完了確認手順を策定する□<br>・運用可能なアップデート手順（リモート経由 or 媒体の利用など）を策定する□<br>・アップデート後の動作確認手順を策定する□<br>・アップデートの不具合があった時の戻し手順を策定する□ | ・5GによるOTA更新機能の適用可能性 |
| | | 要点18 | 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える | □IoT機器、IoTシステム、サービス提供者の基本的な構成情報を把握、管理する<br>・ハードウェア、ソフトウェアの情報を管理する□<br>・設置場所、台数、使用用途、稼動有無を管理する□<br>□IoT機器メーカーやJPCERT/CC、ISAC 等が発信している脆弱性情報の収集・分析を行う<br>・不具合や脆弱性などの情報がを、Webサイトやメール等で確認する。<br>・上記の情報に記載されている影響範囲や重要度、対応予定日等を把握する。<br>・IPA等の機関と連携した情報の場合は、連携先の情報も確認しておく<br>□構成情報と脆弱性情報がマッチングした場合、暫定対策や社内利用者への情報発信を検討する<br>・利用制限などの暫定対策を検討する<br>・異常があった時の緊急対処方法を検討する□<br>・アップデートなど恒久対策の予定を検討する<br>□インシデント情報をIoT 機器メーカーや提供者に連絡する<br>・メーカーのサポート窓口（連絡先）を管理する□<br>□重要な事項がWeb、マニュアル等に記載されているか確認する（契約書など）<br>・個人情報やプライバシーを取り扱う場合は保護などが記載されているかを確認する□<br>・集めた情報の使われ方や第三者提供および利用目的などを確認する□<br>・サポート期間、問い合わせ先などを確認する□<br>□IoT機器の廃棄や再利用時の対策を行う<br>・個人情報・秘密情報を完全に消去する□<br>・初期化する | |
| | | 要点19 | つながることによるリスクを一般利用者に知ってもらう | □リスクを社内利用者へ周知する<br>・禁止事項（機器が壊れるなど、「この様な使い方はしない」こと）□<br>・重要な説明事項（個人情報やプライバシーに関わること、生命や重大事故につながること）□<br>・システム全体に影響を及ぼす事項□ | |
| | | 要点20 | IoT システム・サービスにおける関係者の役割を認識する | □関係者の役割を把握し周知する<br>・IoT機器メーカーやサービス提供企業の役割□<br>・IoT機器、IoTシステム運用保守担当の役割□<br>・IoT機器、IoTシステムのサービス利用者の役割□<br>・CSIRT、またはインシデント対応関係部署の定義と役割（IoT機器などインシデント発生時の連携先） | |
| | | 要点21 | 脆弱な機器を把握し、適切に注意喚起を行う | □設置したIoT機器の脆弱性の影響と対応が管理できるしくみを検討する<br>・メーカーから通知が行われた脆弱性の影響（自社利用への影響）を特定する□<br>・脆弱性の影響を受ける可能性のあるIoT機器（設置場所を含む）を特定する□<br>・IoT機器の脆弱性情報を調査する（脆弱性情報データベース（http://jvndb.jvn.jp/）など）<br>・脆弱性検出（ファジング）ツールによるIoT機器の脆弱性を調査する<br>・脆弱性の影響が確認できた場合、パッチの適用、ネットワークからの切り離しなどを実施する<br>□IoT機器や、IoTシステムの異常を把握する<br>・IoT機器のログやインベントリ情報などから IoT機器の異常を検知する<br>・ネットワーク機器や IoTシステムを監視することで異常を検知する仕組みを検討する | |

表　Annex 12　Draft NISTIR 8200

| Draft NISTIR 8200 Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) | | | 5G適用可能性 |
|---|---|---|---|
| IoT概念 | ・IoTの概念：ネットワーク化された主体（センサ／アクチュエータ／情報資源／ヒト）を用いて物理的世界と相互運用するシステムを作成すること<br>・以下の2つの基盤概念から成る<br>―IoTコンポーネントは コンポーネントの間で潜在的に多対多関係性を提供するネットワークで接続される<br>―いくつかのIoTコンポーネントはセンサ／アクチュエータにより物理的世界と相互運用可能<br>・構成要素<br>―コンポーネント<br>―IoTコンポーネント<br>―システム<br>―IoTシステム<br>―IoT環境 | | 基本的にIoT利用者としての立場でセキュアな環境を実現するための阻害要因となる標準間のギャップを明らかにするというスタンスの文書であるため、5Gを利用してIoTセキュリティを向上させるという技術的問題に対しての貢献は見受けられなかった |
| IoT応用の例示 | 5Gクレデンシャルを利用可能であれば解決<br>・セカンダリ認証による実現可能性<br>GSMA IoT SG：識別・認証#3に同じ | | |
| サイバーセキュリティとIoT | 各分野においてIoTで用いられる標準規格を解説したもの<br>・暗号技術<br>・サイバー・インシデント管理<br>・ハードウェア保証<br>・アイデンティティ＆アクセス管理<br>・ISMS<br>・ITシステム・セキュリティ評価<br>・ネットワーク・セキュリティ<br>・セキュリティ・オートメーション＆継続的モニタリング（SACM）<br>・ソフトウェア保証<br>・サプライ・チェーン・リスク管理<br>・システム・セキュリティ・エンジニアリング | | |
| IoTサイバー・セキュリティ・オブジェクティブス／リスク／脅威 | 概要 | 1. サイバーセキュリティ・オブジェクティブ、2. リスク、3. 脅威の各事項について概要を記述 | |
| | コネクテッド・ヴィークル | それぞれの応用例に関してセキュリティ・オブジェクティブ／リスク／脅威を分析 | |
| | 消費者IoT | | |
| | ヘルスIoT & 医療機器 | | |
| | スマート・ビルディング | | |
| | スマート製造業 | | |
| 標準化景観 | 前出のサイバーセキュリティとIoT章で記述した各項目（暗号技術、サイバー・インシデント管理、ハードウェア保証、アイデンティティ＆アクセス管理、ISMS、ITシステム・セキュリティ評価、ネットワーク・セキュリティ、セキュリティ・オートメーション＆継続的モニタリング（SACM）、ソフトウェア保証、サプライ・チェーン・リスク管理、システム・セキュリティ・エンジニアリング）に関して、様々な団体において策定されている標準化作業の現況、市場へのインパクト、潜在的標準化ギャップに関する分析を記述 | | |

# 表　Annex 13　ENISA Baseline Security Recommendations for IoT

| ENISA Baseline Security Recommendations for IoT | | | | 5G適用可能性 |
|---|---|---|---|---|
| イントロ | ・IoTデバイス／システム／サービスに関連した脅威およびリスクは多岐に渡り急速に進化しており、市民の安全／セキュリティ／プライバシに対する大いなるインパクトをもたらすものであることから、IoTに関連する脅威景観は極度に広範囲なものとなっているため、IoTをサイバー脅威から保護するために何をセキュアにするべきかを理解し、どのようなセキュリティ機能を開発する必要があるかを理解することが重要である。その準備として以下を述べる<br>a) 目的<br>b) スコープ<br>c) EUおよび国際的ポリシー文脈<br>d) ターゲット読者<br>e) 構成 | | | |
| IoTパラダイム | IoT要素 | | ・モノ<br>・知的決断作成<br>・センサおよびアクチュエータ<br>・組込システム<br>・通信 | |
| | セキュリティ要考慮事項 | | ・超巨大攻撃表面<br>・限定的デバイス資源<br>・複雑なエコシステム<br>・標準および規制のフラグメンテーション<br>・広範な配備<br>・セキュリティ統合<br>・安全性側面<br>・低コスト<br>・熟練性不足<br>・セキュリティ更新<br>・非セキュアなプログラミング<br>・不明瞭な責任関係 | |
| | 水平的ベースラインセキュリティ・メジャー定義に関するチャレンジ | | ユースケース／利用アプリケーション／利用シナリオに依存して異なるセキュリティ対策／異なる資産の重要度に応じて異なる脅威インパクトのためにIoTセキュリティを水平的に研究することは極めて困難 | |
| | アーキテクチャ | | IoTソリューションは特有のアプリケーションに着目した特有の技術により開発されるため、標準化を欠いておりフラグメント化した異種アーキテクチャとなり易いため、複数の既存IoTアーキテクチャを研究することでハイレベルの参照モデルを抽出 | |
| | 資産分類 | | ・以下の各グループに属する個別の資産を特定<br>IoTデバイス／その他のIoTエコシステム構成デバイス／通信／インフラ／プラットフォーム＆バックエンド／決断作成／アプリケーション＆サービス／情報 | |
| 脅威およびリスク分析 | セキュリティ・インシデント<br>2009年以降に発生した主要なIoTセキュリティ・インシデントのいくつかに関して分析を実施 | | | |
| | 脅威分類<br>実際のIoTシステムに対して実施された攻撃のいくつかに注目して作成された脅威分類を提示 | | | |
| | IoTサイバーセキュリティ攻撃シナリオ例の提示<br>センサ⇔アクチュエータ間への攻撃／センサの読取値書換攻撃／アクチュエータへの設定変更／IoT管理システムへの攻撃／プロトコル脆弱性徴発／デバイスへのコマンド投入／飛び石攻撃／IoTボットネットによるDDoS／電力源操作／ランサムウェア | | | |
| | 重大な攻撃シナリオ<br>前項で記述した攻撃シナリオに対する重大性を評価した結果の提示 | | | |
| セキュリティ分析および最良実践 | ポリシ | | S.b.D ／ P.b.D ／ 資産管理 ／リスクおよび脅威識別および評価 | |
| | 組織・ヒト・プロセス | | エンド・オブ・ライフのサポート ／ 証明されたソリューション ／ セキュリティ脆弱性および/もしくはインシデント ／ 人的資源セキュリティ訓練/意識向上 ／ サードパーティとの関係性 | |
| | 技術 | | HWセキュリティ | ・5Gではクレデンシャル・ストレージ機能により物理的保護を提供可能だが、クレデンシャル・ストレージ外に保存されたデータに対する保護提供が残存課題<br>GSMA IoT SG：識別・認証#5に同じ |
| | | | 信頼および完全性管理 | |
| | | | 強力なデフォルト・セキュリティ＆プライバシ | |
| | | | データ保護およびコンプライアンス | |
| | | | システム・セーフティおよび信頼性 | |
| | | | セキュアSW / FW更新 | ・安全な配布方式部分に関してはOTA更新機構の利用可能性<br>GSMA IoT SG：セキュリティ#15に同じ |
| | | | 認証 | ・セカンダリ認証による実現可能性<br>GSMA IoT SG：識別・認証#3に同じ |
| | | | 認可 | |
| | | | アクセス制御 ― 物理的および環境セキュリティ | |
| | | | 暗号技術 | ・データ転送部分に関しては5Gで保護可能だが、保存／使用状態での保護提供が残存課題<br>GSMA IoT SG：プライバシ#3に同じ |
| | | | セキュアかつ信頼できる通信 | ・5Gにより提供可能<br>GSMA IoT SG：プライバシ#3に同じ |
| | | | セキュアなインターフェースおよびネットワーク・サービス | |
| | | | セキュアな入出力取扱 | |
| | | | ロギング | |
| | | | モニタリングおよび監査 | |
| ギャップ分析 | G1 | 既存セキュリティ・アプローチと規制との間の分断 | | |
| | G2 | 認識および知識の欠如 | | |
| | G3 | 非セキュア設計 および/もしくは 開発 | | |
| | G4 | 異なるIoTデバイス/プラットフォーム/フレームワークを跨る相互運用性の欠如 | | |
| | G5 | 経済的インセンティブの欠如 | | |
| ハイレベル推奨 | R1 | IoTセキュリティのイニシアティブおよび規制の調和の促進 | | |
| | R2 | IoTサイバーセキュリティの必要性に関する認識の向上 | | |
| | R3 | IoT向けのセキュアなSW/HW開発ライフサイクルの定義 | | |
| | R4 | IoTエコシステム間での相互運用性に関する合意の形成 | | |
| | R5 | IoTセキュリティに関する経済的および管理的なインセンティブの醸成 | | |
| | R6 | セキュアIoT製品/サービス・ライフサイクル管理の確立 | | |
| | R7 | IoT利害関係者間での責任の明確化 | | |

表　Annex 14　Security Guidance for Early Adopters of the Internet of Things (IoT)

| | Security Guidance for Early Adopters of the Internet of Things (IoT) | 5G適用可能性 |
|---|---|---|
| イントロ | ・本書はIoTをベースとしたシステムのセキュアな実装に関するガイダンスを提供するものであり、術語定義等をITU-T Y.2060に負っている<br>・IoTには以下のような特徴があるため、伝統的なエンタープライズ向けセキュリティ・ソリューションは十分な効果を持ち得ない<br>–増加するプライバシ的懸念<br>–プラットフォーム・セキュリティ限界<br>–定常的なモビリティ<br>–量的膨大さ<br>–クラウド・ベースの操作 | 基本的に大所高所に立って安全なIoTアプリケーションを実現するために必要となるセキュリティ制御を明らかにするというスタンスの文書であるため、5Gを利用してIoTセキュリティを向上させるという技術的問題に対しての貢献は見受けられなかった |
| 目的 | ・消費者セクタにおける広範なIoTの採用が見られている<br>・ビジネスおよび公共セクタ向けは若干遅れているが、B2B IoT接続も2011年～2020年まで年次28%の増加が予測されている<br>・スマート・シティ実現を目指す市政機関でも採用が進むことが推測<br>・多くの産業セクタが独自のニーズを満たすためにIoTを用いる場合、個々のユニークな実装に対してセキュリティ脆弱性の評価が必要<br>・本書はIoTの一般的セキュリティ制御のセットを記述するが、個々のIoT実装の文脈においてはいくらかのカスタム化が必要となるだろう | |
| 個人/組織へのIoT脅威 | 悪意あるアクタが利用することが想定される新規脅威および攻撃ベクタに関する例示<br>・制御システム、車両、さらには人体までもがアクセスおよび操作の対象として被害を被る<br>・改竄されたヘルス情報ないしセンサ・データに基づく不適切な診断/治療の実施<br>・個人宅/事務所等への物理的アクセス方法の取得<br>・内部バスへのDoS攻撃による車両制御の喪失<br>・IoTセンサに対するDDoS攻撃による生命に危害を与えるような重大な情報の喪失<br>・人の位置情報/振舞情報等に対する無権限でのトラッキングの実現<br>・小規模IoTデバイスが提供する遠隔モニタリング機能を利用した非合法サーベイランス | |
| セキュアなIoT配備に関するチャレンジ | IoTによって新たに生まれるセキュリティ・エンジニアリングへのチャレンジ<br>・複雑な構成を必要とする多くのプロトコル/技術を利用することで多くのIoTシステムは貧弱な設計/実装となりがち<br>・成熟したIoT技術およびビジネス・プロセスの欠如<br>・IoTデバイス向けライフサイクル維持および管理に関する限定的なガイダンス<br>・ユニークな物理的セキュリティ懸念の導入<br>・複雑かつ気付かれ難いプライバシ的懸念<br>・IoT開発者向けに得られる限定的な最良実践<br>・IoTエッジ・デバイス向け認証/認可標準の欠如<br>・IoTベースのインシデント対応活動に関する最良実践の欠如<br>・IoTコンポーネント向け監査/ロギング標準の不存在<br>・IoTデバイスとセキュリティ・デバイス/アプリケーションの間で用いられるインターフェースが限定的<br>・マルチ・テナンシをサポートする仮想化IoTプラットフォーム構成のためのセキュリティ標準が未成熟 | |
| 推奨されるセキュリティ制御 | IoT開発/配備における利害関係者へのプライバシ・インパクトの分析およびPrivacy-by-Designアプローチの採用 | |
| | 新規IoTシステムのアーキテクティングおよび配備におけるセキュア・システム・エンジニアリングの採用 | |
| | IoT資産防御のための層的セキュリティ保護の実装 | |
| | 機微情報保護のためのデータ保護最良実践の実装 | |
| | IoTデバイス向けライフサイクル・セキュリティ制御の定義 | |
| | 組織によるIoT配備のための認証/認可フレームワークの定義および実装 | |
| | 組織IoTエコシステム向けロギング/監査フレームワークの策定 | |
| 将来的努力項目 | 標準 | |
| | IoTセキュリティ心構えに関する状況的認識 | |
| | 情報共有 | |
| | SDPとIoT | |
| | IoT環境におけるプライバシ | |

表　Annex 15　OWASP IoT Top 10 Project for 2018

| OWASP IoT Top 10 Project for 2018 | | 5G適用可能性 |
|---|---|---|
| I1 | ″弱い、推測可能、もしくはコードに組み込まれ変更できないパスワード<br>容易に力任せ試行可能、公開された、ないし修正できないクレデンシャルを利用する。配備されたシステムへの無認可アクセスを可能とするFWないしクライアントSWに含まれたバックドアも含む″ | |
| I2 | ″非セキュアなネットワーク・サービス<br>特にインターネットに接続されているデバイス自体に不要ないし非セキュアなネットワーク・サービスが動作しており、情報の機密性、完全性/真正性、可用性を損なう、ないし無認可遠隔制御を可能にする″ | ・製品/サービス提供者の開発体制次第<br>・利用する既存製品やOSSまで含めて考えると実現は極めて困難か |
| I3 | 非セキュアなエコシステム・インターフェース<br>デバイス外のエコシステムに存在する非セキュアなウェブ/バックエンドAPI/クラウド/モバイルへのインターフェースが存在することにより、デバイスもしくはその関連コンポーネントの危殆化が発生。よくある問題は認証/認可の欠如、弱いもしくは無暗号化、入力および出力フィルタリングの欠如 | 同上 |
| I4 | セキュアな更新機構の欠如<br>デバイスを安全に更新する能力の欠如。デバイスでのFW検証の欠如、安全な配布方式の欠如（非暗号化経路）、耐ロールバック機構の欠如、更新に起因するセキュリティ的変更に関する通知の欠如などを含む | ・安全な配布方式部分に関してはOTA更新機構の利用可能性<br>GSMA IoT SG：セキュリティ#15に同じ |
| I5 | 非セキュアな、もしくは旧コンポーネントの利用<br>デバイスの危殆化を招く非推奨ないし非セキュアなSWコンポーネント/ライブラリの利用。OSプラットフォームの非セキュアなカスタム化、危殆化したサプライ・チェーンからのサードパーティ性SW/HWコンポーネントの利用を含む | ・製品/サービス提供者の開発体制次第<br>・利用する既存製品やOSSまで含めて考えると実現は極めて困難か |
| I6 | 不十分なプライバシ保護<br>デバイスないしエコシステムに保存された利用者個人情報の非セキュア/不適切/無許可利用 | 同上 |
| I7 | 非セキュアなデータ転送/保存<br>保存中/転送中/使用中の各状態を含むエコシステム内のどこかで機微データに対する暗号化ないしアクセス制御の欠如 | ・データ転送部分に関しては5Gで保護可能だが、保存／使用状態での保護提供が残存課題<br>GSMA IoT SG：プライバシ#3に同じ |
| I8 | デバイス管理の欠如<br>製品として配備されたデバイスに対するセキュリティ・サポートの欠如。資産管理、更新管理、廃止、システム・モニタリング、対処機能を含む | ・製品/サービス提供者の開発体制次第<br>・利用する既存製品やOSSまで含めて考えると実現は極めて困難か |
| I9 | 非セキュアなデフォルト設定<br>デバイスないしシステムの非セキュアなデフォルト設定による、ないし、システムをよりセキュアにするための操作者による構成変更防止機構が欠けた状態での出荷 | 同上 |
| IA | 物理的頑健化の欠如<br>物理的な頑健化方法が欠如することにより、潜在的攻撃者に対して将来的な遠隔攻撃ないしデバイスのローカル制御簒奪を可能とせしめる機微情報を取得可能化 | ・5Gではクレデンシャル・ストレージ機能により物理的保護を提供可能だが、クレデンシャル・ストレージ外に保存されたデータに対する保護提供が残存課題<br>GSMA IoT SG：識別・認証#5に同じ |

表　Annex 16　OneM2M TS-0003-V3.8.0 Security Solutions

| OneM2M TS-0003-V3.8.0 Security Solutions | | 5G適用可能性 |
|---|---|---|
| 5章 | Security Architecture<br>OneM2Mセキュリティ・アーキテクチャに関する概要説明、セキュリティ・レイヤに関する説明、OneM2M全体的アーキテクチャにおけるセキュリティ・アーキテクチャの統合に関する説明を記述 | OneM2Mでは利用する具体的なネットワーク技術はNSEで抽象化されており、その上のセキュリティ機能はOneM2M自身によってE2Eで提供されるため、5Gの出る幕はなし |
| 6章 | Security Services and Interactions<br>OneM2Mにおけるイベント・フローにどのようにセキュリティが統合されているのかの説明、セキュリティ・サービス・レイヤの説明、セキュア環境抽象化レイヤの説明を記述 | |
| 7章 | Authorization<br>OneM2Mシステムでサポートされているアクセス制御方式の一般的記述および動的認可 / RBAC / 分散認可などの特徴的機能に関する記述 | |
| 8章 | Security Frameworks<br>M2Mアプリケーションで用いられる可能性がある多様な配備シナリオを収容するためにサポートされているM2Mシステムのセキュリティ・プロビジョニングおよび設立のための多様な方式に関する記述 | |
| 9章 | Security Framework Procedures and Parameters<br>セキュリティ・アソシエーション設立フレームワークおよびリモート・サービス・プロビジョニング・フレームワークで用いられる手続およびパラメータを記述 | |
| 10章 | Protocol and Algorithm Details<br>証明書ベース・セキュリティFW / TLS&DTLS詳細 / 鍵エクスポート&導出詳細 / クレデンシャルID詳細 / KpsaID / KmIDフォーマット / Enrolment Expiry を記述 | |
| 11章 | Privacy Protection Architecture using Privacy Policy Manager(PPM)<br>M2Mサービス契約者のプライバシ嗜好およびサービスのプライバシ・ポリシを用いた分散認可プライバシ保護アーキテクチャであるプライバシ・ポリシ・マネージャのアーキテクチャを記述 | |
| 12章 | Security-Specific oneM2M Data Type Definitions<br>OneM2Mセキュリティ仕様でのみ用いられるデータ型の定義を行なう<br>-Simple Security-Specific oneM2M Data Types<br>-Enumerated Security-Specific oneM2M Data Types<br>-Complex Security-Specific oneM2M Data Types | |

改定履歴

| 版数 | 年月日 | 内容 | 備考 |
|---|---|---|---|
| 1.0 | 2020 年 7 月 29 日 | 第 1 版発行 | |