5GMFセキュリティ検討AdHocの紹介

5GMFセキュリティ検討AHサブリーダー
株式会社NTTドコモ
石井 一彦

目次

1. 5GMFセキュリティ検討AHの紹介
2. 5Gセキュリティの全体概要
3. IoTセキュリティ
4. Connected Viechleセキュリティ
5. Fintechセキュリティ

The Fifth Generation Mobile Communications Promotion Forum

1

5GMFセキュリティ検討AHの紹介

- 報告内容
  - 2018年度活動目標、活動実績
  - 2018年度活動報告書概要
  - 2019年度活動計画

- 2018年度活動目標

活動報告書を作成し、企画委員会にて
「セキュリティ調査研究委員会」(仮称)の設置を提案する。

2018年度活動実績

活動	日時	内容
アドホック会合	第1回2018年9月5日	・運営方針、進め方についての議論、決定 ・IoT, Connected-Vehicle, FinTech各テーマサブリーダー指名 ・ワークショップ準備
	第2回2018年10月15日	・ワークショップ振り返り ・今後の活動の進め方議論、決定
	第3回2018年11月19日	・活動報告書のまとめ方、目次案、分担について議論、決定
	第4回2019年1月25日	・活動報告書内容検討。SWGメンバー配置見直し
	第5回2019年2月28日	・活動報告書内容検討 ・プラサド氏より3GPPにおける5Gセキュリティの検討状況を共有
	第6回2019年3月29日	・活動報告書内容レビュー ・ワークショップ等3件の予定（5月～7月）の共有と対応検討 ①WTP2019_5Gセキュリティワークショップ ②セキュリティセミナー（TTCと合同開催） ③第2回セキュリティ検討アドホックワークショップ （3GPP 5Gセキュリティワークショップ）
ワークショップ	第1回2018年10月1日	5Gセキュリティの取り組み、標準化動向、各テーマのセキュリティ動向 (IoT, Connected Vehicle, Fintech)、キャッシュレス決済動向 についてメンバーより講演

2018年度活動報告書

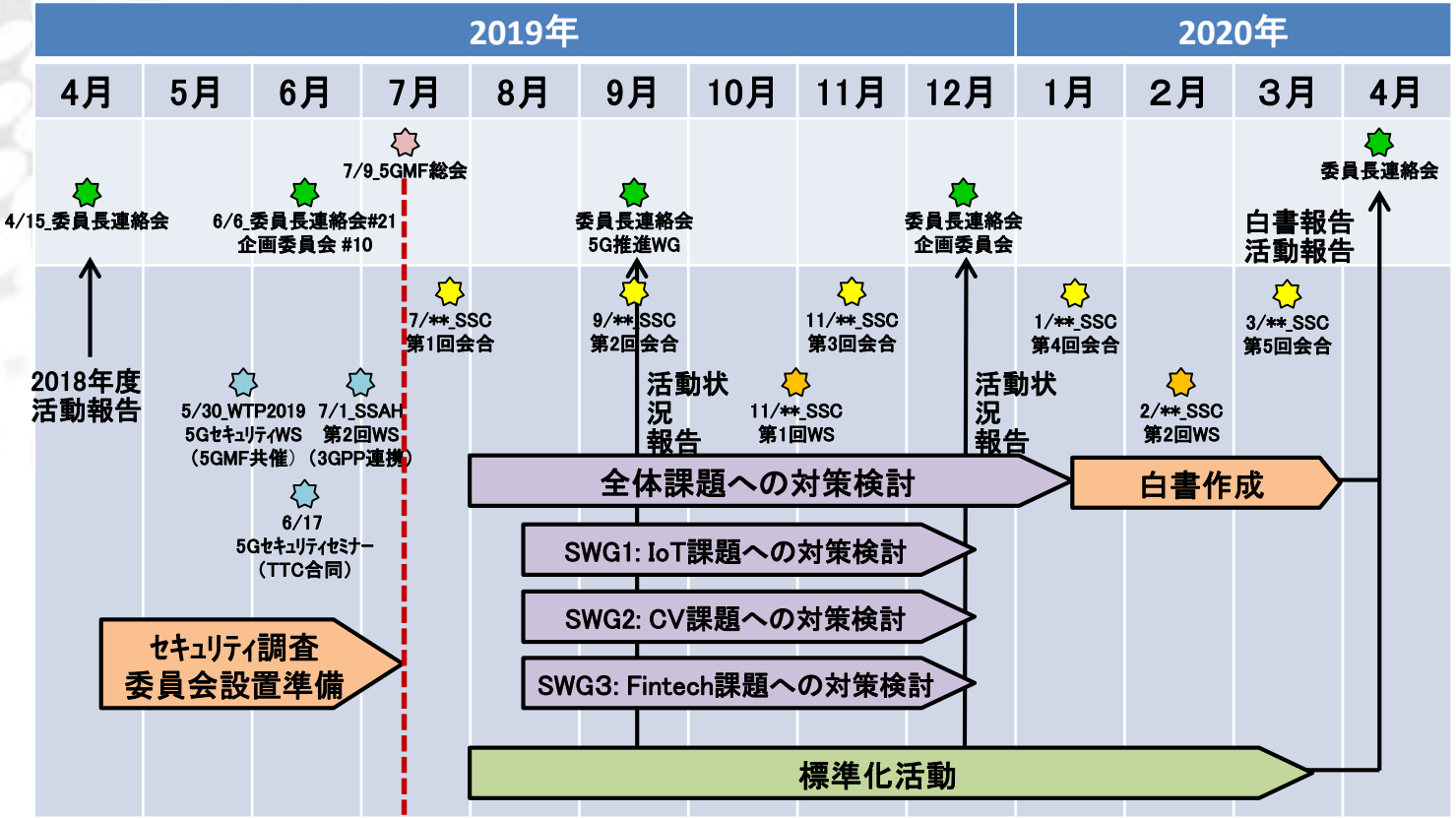
1. 報告概要
2. セキュリティ検討アドホック活動の目的
3. 5Gセキュリティの標準化動向
4. 5Gセキュリティの検討範囲の検討
   - ・5Gセキュリティ全般から3つのユースケース(IoT,CV,Fintech)を検討対象とした調査、検討過程
   - ・ユースケース毎の検討範囲の検討結果
5. 5Gセキュリティの検討課題及び検討項目の抽出と整理
   - ・調査、検討過程を含め、各ユースケースにおける課題と項目を整理する
6. 今後の活動計画調査

⇒ 活動計画に基き、2019年度は委員会として活動

2019年度活動計画（委員会活動）

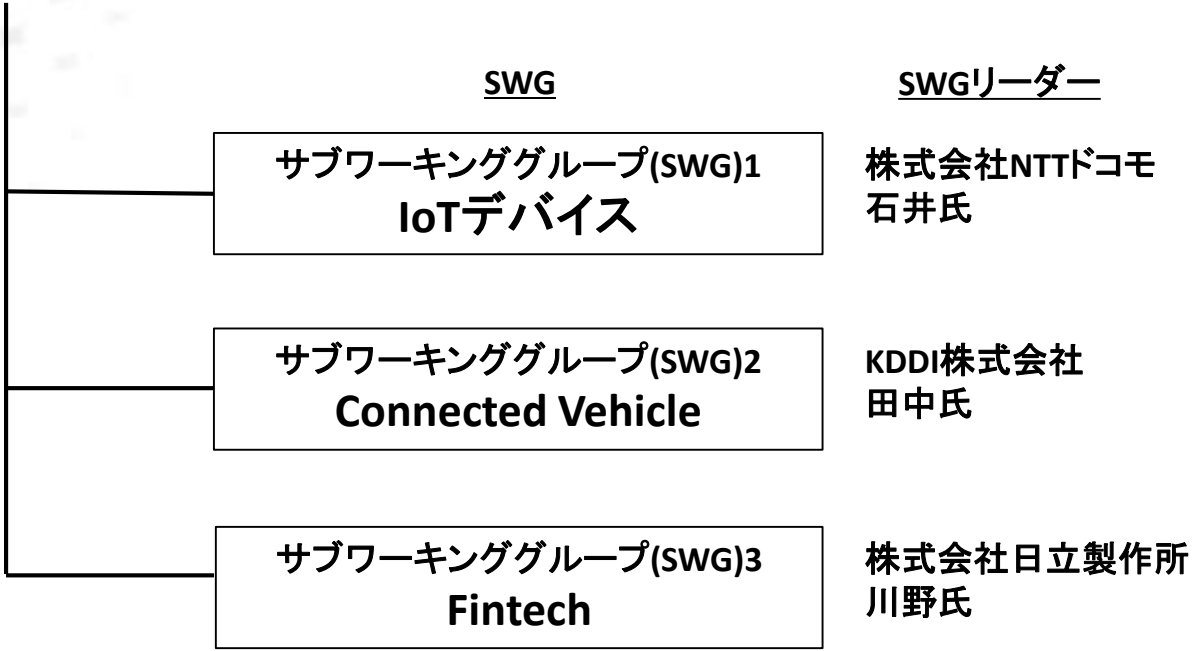
1. 目的
   - 5G時代の安心・安全なサービスの実現に向け、国内外の「セキュリティ」の調査検討、情報の共有や発信、推進団体との連携等を図る
2. スコープ
   - セキュリティ検討アドホックでの検討内容をもとに下記のような項目を検討する
3. 主な検討項目
   a. IoTデバイス
   b. Connected-Vehicle
   c. Fintech
   d. 標準化(3GPP, TTCなど)との連携
   e. 白書策定 など
4. 成果物
   a. 白書の策定
   b. 標準化(3GPP, TTCなど)への寄与
5. 年間計画
   - 次ページ表参照

2019年度年間計画



2019年度 セキュリティ調査研究委員会（仮称）活動体制（案）

委員長　　慶應義塾大学　手塚先生
委員長代理　KDDI株式会社　田中氏



5GMF セキュリティ検討アドホックについて

- 5GMF セキュリティ検討アドホックについて
  - 2018年7月企画委員会にて承認、企画委員会配下に設置
  - メンバー募集等の準備を経て2018年9月、21名にて本格的な活動開始
  - 参加企業・団体一覧

- 慶應義塾大学
- 株式会社NTTドコモ
- エアロフレックスジャパン株式会社
- NTTコミュニケーションズ株式会社
- 沖電気工業株式会社
- 株式会社カオスウェア
- KDDI株式会社
- シスコシステム合同会社
- セコム株式会社
- ソニー株式会社
- ソニーモバイルコミュニケーションズ株式会社
- 日本電気株式会社
- 日本コムシス株式会社
- 株式会社日立製作所
- 華為技術日本株式会社
- 古河電気工業株式会社
- 三菱電機株式会社
- 楽天モバイル株式会社

(2019年4月現在、18社・団体　26名)

【オブザーバー】

- 一般社団法人情報通信技術委員会(TTC)
- 山本国際コンサルタンツ
- 富士通株式会社

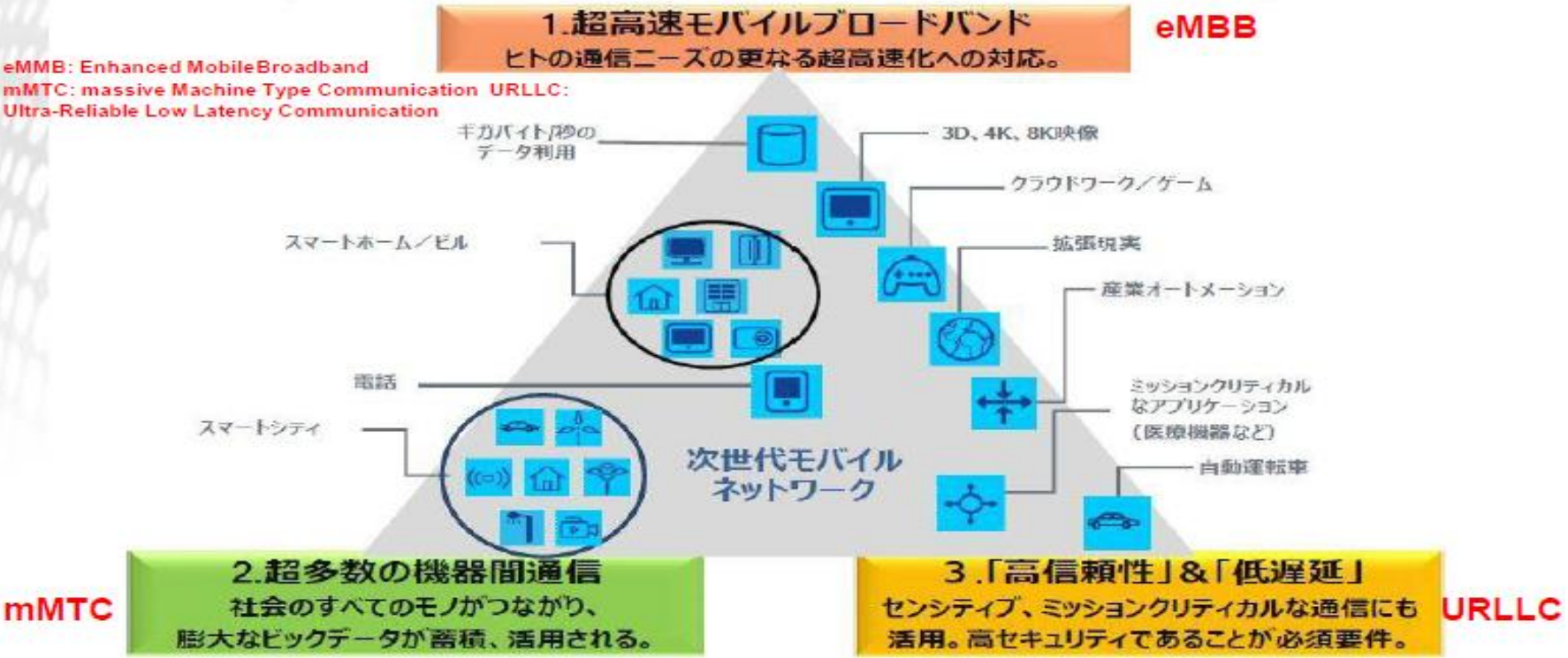
The Fifth Generation Mobile Communications Promotion Forum

2

5Gセキュリティの全体概要

あらゆる、ヒトとモノを繋ぐたに重要な3要素

eMMB: Enhanced MobileBroadband
mMTC: massive Machine Type Communication URLLC:
Ultra-Reliable Low Latency Communication



IMT Vision –"Framework and overall objectives of the future development of IMT for 2020 and beyond", ITU-R勧告M.2083-0　2015年9月
https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

出典：第1回5GMFセキュリティ検討アドホック資料より

標準化、国際研究開発プロジェクト

■ 標準化

標準化は初期段階だが、様々な団体で検討が進められている

- **3GPP SA3**
  - 脅威分析、セキュリティ要件定義、セキュリティアーキテクチャとプロトコル仕様
  - アーキテクチャ、認証、RANセキュリティ、鍵管理、スライスセキュリティ等の**17のセキュリティ領域**を定義して課題と対策を整理
- **ETSI ISG NFV**
  - NFVのセキュリティ監視・管理、NFVプラットフォームのセキュリティ検証、他
- **GSMA**
  - 5Gトラストモデル検討
- **NGMN**
  - DoS protection, Network slicing, MEC
- **その他**
  - IETF (5GIP, NETSLICING, etc.)
  - ONF(Open Networking Foundation) – SDN関連

■ 国際研究開発プロジェクト

- **5G-ENSURE in 5G-PPP**
  - ユースケース、トラストモデル、アーキテクチャ、実現技術（AAA, Privacy, Trust, Security monitoring, Network management and virtualization Isolation）
- **5G NORMA （led by Nokia）**
  - Novel radio multiservice adaptive network architecture for the 5G era
- **NSF – Advanced Wireless Network Research**
  - https://www.nsf.gov/cise/5G/

出典：第1回5GMFセキュリティ検討アドホック資料より

5Gセキュリティ調査研究委員会(仮称)での検討範囲

■無線アクセスのセキュリティ
- LTEを踏襲しつつ、さらに機能向上

■外部環境の変化
- IoT対策

■ユースケース依存のセキュリティ要件
- トラストモデル

- Fintech
- IoT
- Connected Car

■仮想化／クラウドセキュリティ
- NFV、スライス等

出典：第1回5GMFセキュリティ検討アドホック資料より

安心安全な5G社会に向けて

1. 安心安全な5G社会を実現するために、5Gインフラを構築するのみでなく、5Gを活用した安心安全なサービス(トラストサービス)を実現する。

2. 安心安全なサービス(トラストサービス)の対象として、以下を検討する。
   - IoTセキュリティ
   - Connected Vehicleセキュリティ
   - Fintechセキュリティ

The Fifth Generation Mobile Communications Promotion Forum

3

IoTセキュリティ

5GMFで検討すべき課題の抽出方法

- IoTセキュリティの課題の中から、5Gで新たに加わったセキュリティ機能で解決できる可能性がある課題を抽出する

- 5Gで新設されたセキュリティ機能
  - プライマリ認証
  - セカンダリ認証
  - クレデンシャル・ストレージ
  - オペレータ間セキュリティ
  - プライバシ保護
  - サービスベースアーキテクチャ
  - CU – DUの分離
  - 鍵階層
  - ネットワーク・スライス
- 標準文書から抽出したIoTセキュリティ課題
  - 可用性: 4項目
  - ID: 6項目
  - プライバシー: 7項目
  - セキュリティ (システムの完全性維持): 15項目

5GにおけるIoTセキュリティ課題

- 5GにおけるIoTセキュリティ検討課題として、標準文書と5Gセキュリティ新機能から12項目の課題を抽出・整理した
  - 可用性：4項目
  - ID: 4項目
  - プライバシー: 4項目

- 5Gセキュリティ新機能のうち、IoTセキュリティでの活用という面では以下機能の可能性が高い
  - セカンダリ認証
  - プライバシ保護
  - ネットワーク・スライス

【参考】5Gのセキュリティ機能 – 可用性

課題	検討方向性
従来のセルラーシステムと同程度のセキュリティ水準で、いかにしてローパワー・ワイドエリア（LPWA）ネットワーク（NB-IoT、LTE-M など）を展開および運用することができるか	ネットワーク・スライシング機能により、ネットワーク全体に影響を与えずに柔軟な対応ができる可能性がある
IoT エンドポイントがネットワークの境界をまたいで移動する場合、複数の移動体通信事業者で同水準のセキュリティを確保するにはどうすればよいか	オペレータ間セキュリティによるモビリティ関係構築により、解決できる可能性がある
通信をゲートウェイのエンドポイントに依拠するキャピラリーネットワークのエンドポイントまでネットワーク信頼性を転送するにはどうすればよいか	ネットワーク・スライシング機能により、GWポイントを介さず軽量エンドポイントが直接通信可能となる可能性がある
安全性の高い通信環境で軽量エンドポイントの電力制限に対応するにはどうすれはよいか	ネットワーク・スライシング機能により、軽量エンドポイントも安全に収容できる独立したネットワークを用意できる可能性がある

【参考】5Gのセキュリティ機能 – ID

課題	検討方向性
エンドポイントを操作するユーザーとエンドポイントのID を強く関連付けることは可能か	セカンダリ認証を用いた関連付けを行える可能性がある
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	セカンダリ認証を用いてピアとサービスの安全な認証をネットワークに依頼できる可能性がある
デバイスのID をいかにして不正操作や改ざんから守るか	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・ストレージを用いることでデバイスIDを保護できる可能性がある
エンドポイントとネットワークは、どのようにしてIoTサービスによるエンドポイントへのアクセスを許可することを保証するか	セカンダリ認証を用いた相互認証を行うことで、エンドポイントのアクセス許可を保証できる可能性がある

【参考】5Gのセキュリティ機能 – プライバシー

課題	検討方向性
エンドポイントやIoT サービスの固有の識別子によって、エンドユーザーやエンドポイントが物理的に監視または追跡される恐れはないか	5GではIMSI,TMSIに代わり、匿名化したSUCIを常に用いる事ができるため、エンドポイントの監視・追跡を回避できる可能性がある
エンドポイントやIoT サービスから収集されるデータが、エンドユーザーの物理的属性（位置、動作、スリープ中か起動中かなどの状態）を示唆したり、それに直接関連付けられてないか	5Gネットワーク内の安全性を考慮した暗号化方式や、ネットワークスライシングによる独立したセキュリティ環境構築により安全性を確保できる可能性がある
生成された暗号文のパターンを読み取られないようにするために、万全なセキュリティに機密性と完全性が確保されているか	5Gネットワーク内の安全性を考慮した暗号化方式を活用できる可能性がある
データを保護するために使用されるセキュリティキーやセキュリティ・アルゴリズムは、リフレッシュできるか	5G Phase2において長期有効鍵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

【参考】5Gのセキュリティ機能 – セキュリティ

- 本項目はシステムの完全性維持(セキュリティバイデザインやセキュリティマネジメント)に関連するもので、5Gセキュリティ機能による課題解決は困難だと思われるが、5Gコア製品に対しての3GPP SCAS (Security Assurance Specification) の枠組を用いた取組が参考になる可能性がある

課題	検討方向性
プロジェクト開始時点において、セキュリティのベストプラクティスが製品やサービスに組み込まれているか	
ソフトウェアや製品の開発ライフサイクルの中に、セキュリティのライフサイクルが組み込まれているか	
……	

The Fifth Generation Mobile Communications Promotion Forum

4

Connected Viechleセキュリティ

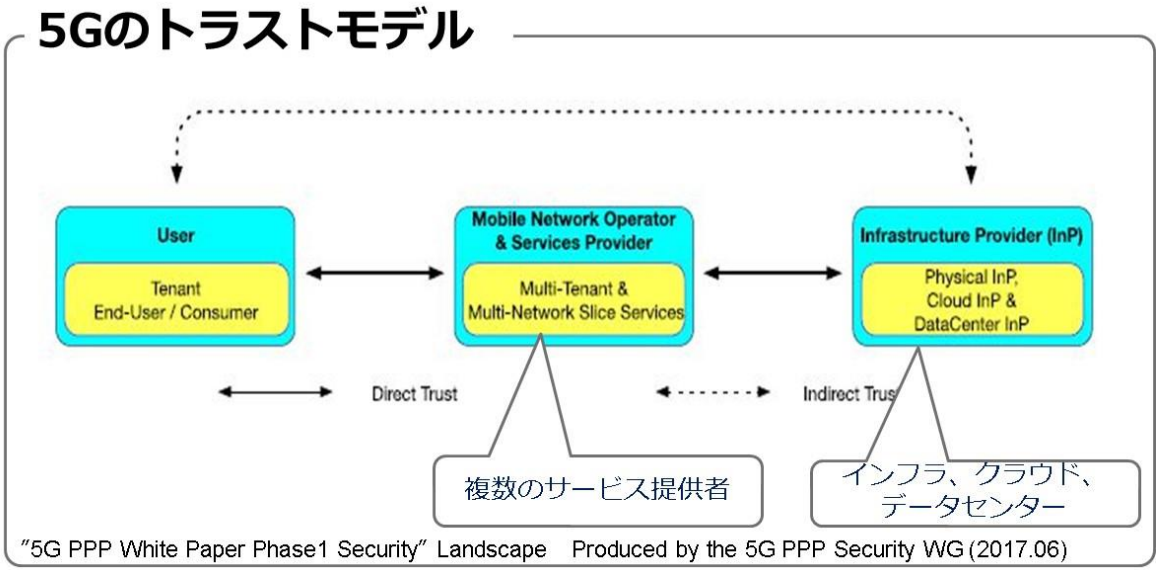
Connected Vehicleの実現に向けた5Gのセキュリティ課題

様々なプレーヤ間が関与するサービスのセキュリティ対策検討

■ 各サービスにおけるトラストモデルの検討

✓ 新しいビジネスモデルとエコシステム

- **OEM**
- **クラウドプロバイダ**
- **MEC上で動作する3rd Partyアプリ**
- **通信事業者等**

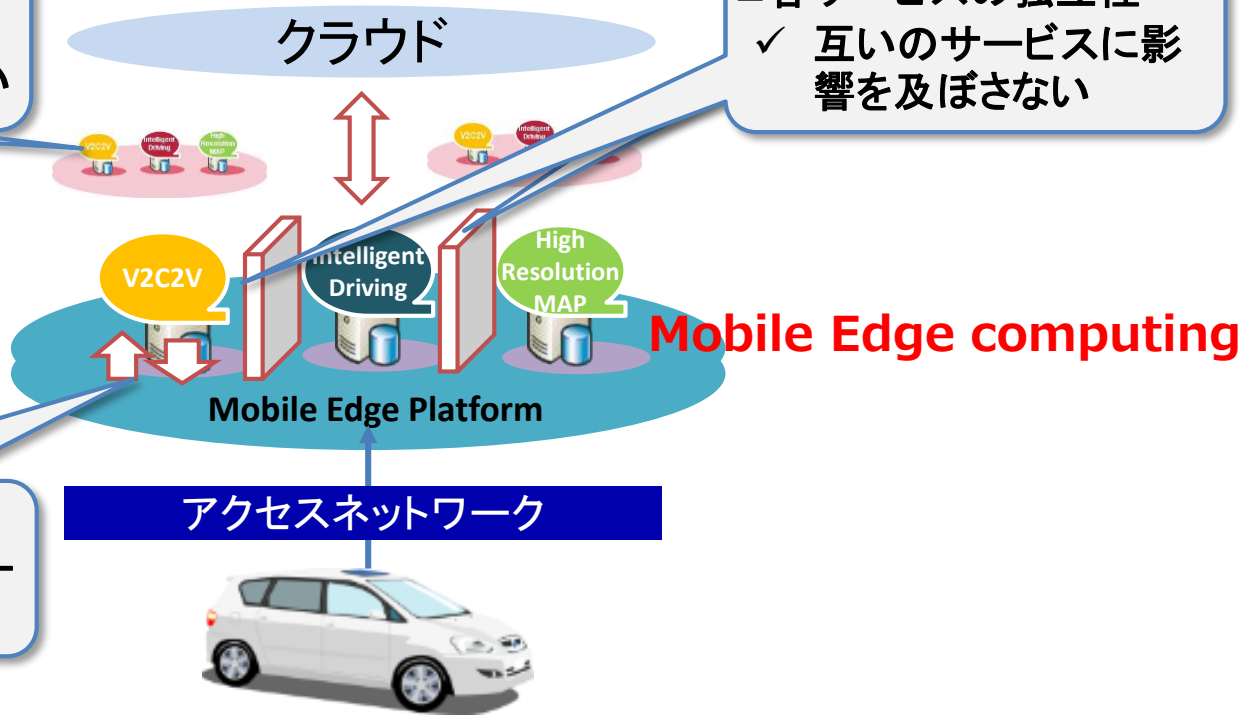


Connected Vehicleの実現に向けた5Gのセキュリティ課題　続き

事業者が提供するMobile Edge上に複数のサービス提供者が動作する
マルチテナント環境でのセキュリティ

■サービスの安全性検証
✓サービスがEdgeプラットフォームに影響を及ぼさない

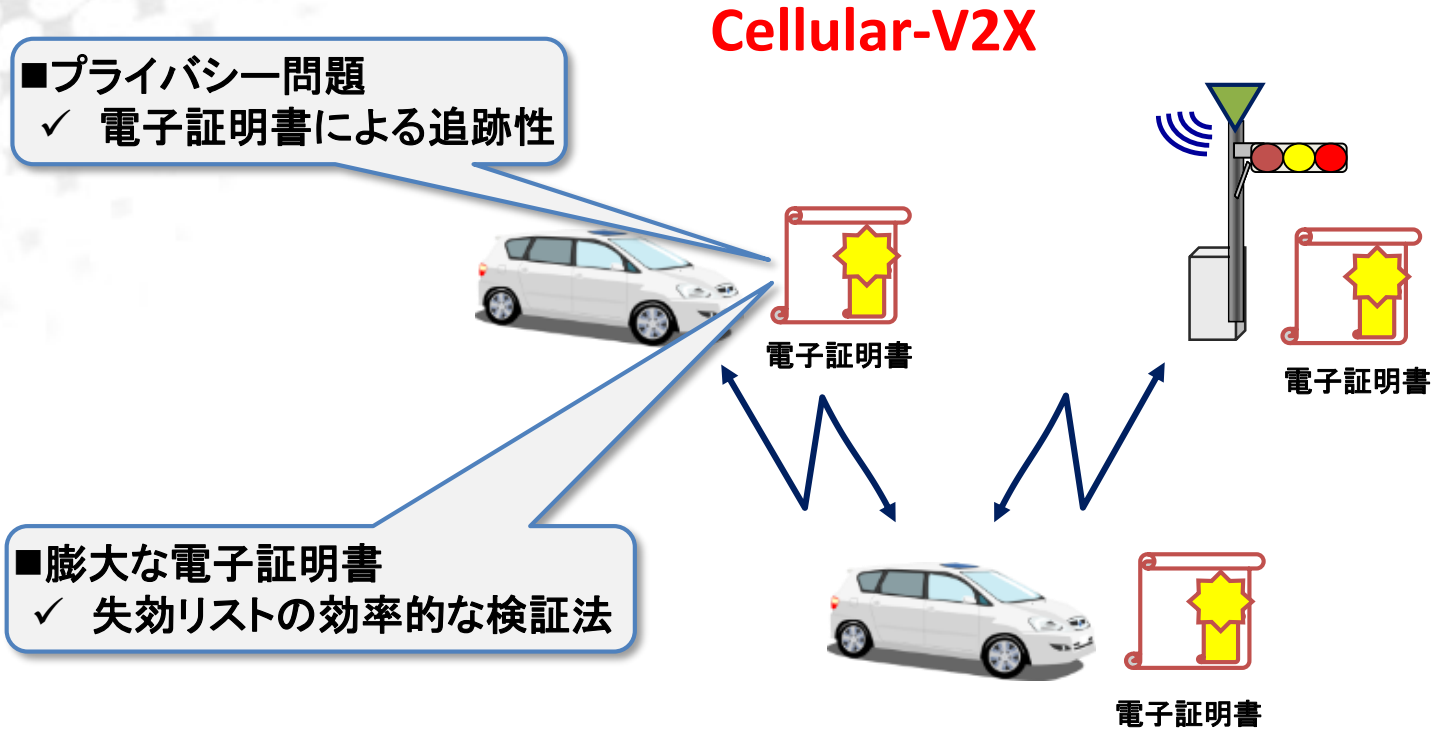
■各サービスの独立性
✓ 互いのサービスに影響を及ぼさない



■プラットフォームの安全性
✓ Edgeプラットフォームがサービスに影響を及ぼさない

Connected Vehicleの実現に向けた5Gのセキュリティ課題　続き

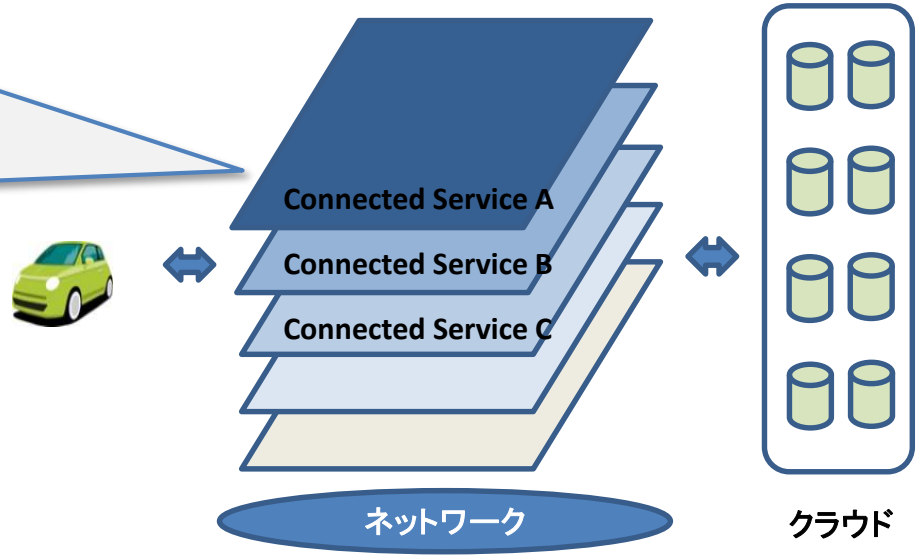
C-V2Xのセキュリティ対策としてなりすまし、盗聴、データ改ざん対策のため電子証明書を活用



Connected Vehicleの実現に向けた5Gのセキュリティ課題　続き

Connected Vehicleの各種サービスに応じた複数ネットワークスライシングの利用とその適切なセキュリティ管理

■ネットワークスライシングのセキュリティ課題
3GPP等での検討
- ✓ スライス間通信の規制・制御
- ✓ スライスへのアクセス認証、認可
- ✓ 他スライスへの攻撃・悪影響の阻止



5

Fintechセキュリティ

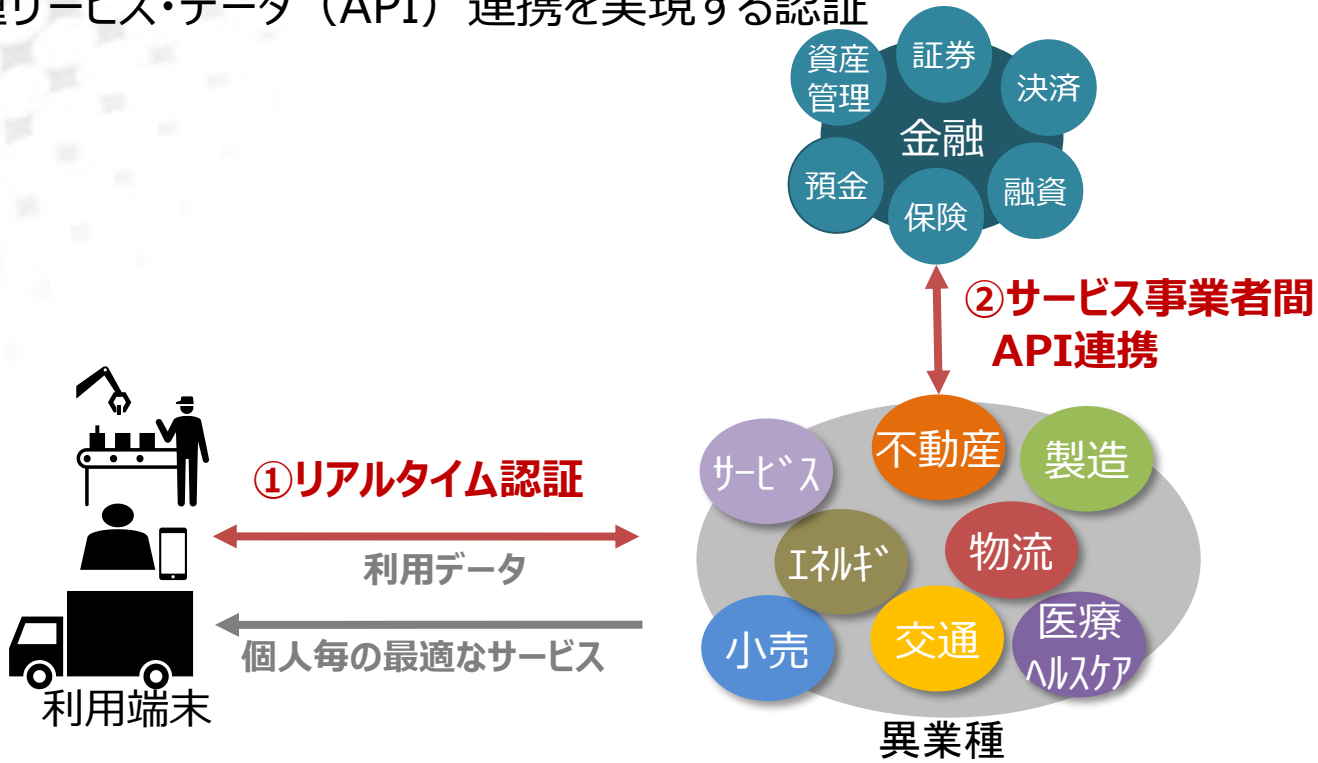
５Gにおけるアプリケーション

モバイルネットワークを活用したパーソナライズペイメントの進展
・ユーザの行動をリアルタイムにモニタリングし、それに応じた金融サービスを提供
・それに応じた認証方式が必要

#	金融サービス
1	**異業種連携取引分野** 例1)コインパーキングに車を止める・移動で自動支払い 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** 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 例2)走行距離に応じたガソリン価格変動 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** 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 例1)使用頻度ではなく、時間・感動で料金を払う 例2)服を着ただけ払う
4	**高速取引分野** 例1)株取引などにおける高速取引

セキュリティ検討ポイント

①モバイル端末とクラウドとのリアルタイム連携による連続的な個人・機器認証
（例：行動データなどによる認証と生体認証との連携）
②異業種サービス・データ（API）連携を実現する認証



セキュリティ検討ポイントまとめ

5Gにおけるセキュリティの検討課題及び検討項目の抽出と整理

金融取引などのサービスでは、より高いセキュリティが求められる一方で、ユーザの利便性は重要な観点である。5Gが進展することでよりインターネットを通じた金融サービスが加速することが想定され、より高いセキュリティを確保しながら、ユーザの利便性をあげていくかが重要となる。

引き続き、以下の検討項目などについて、関連機関などと連携を図りながら、5Gにおける必要となるセキュリティ機能について検討を行う

（１）異業種サービス･データとのAPI連携を実現するサービス事業者間認証

5Gにおいて、現状の金融APIが様々な異業種のサービスで対応可能か。更なるセキュリティ向上や、ユーザの利便性向上などを考慮する必要がないかなど検討が必要となる

（２）ユーザとネットワーク上で常時リアルタイム連携できる個人認証

常時リアルタイム連携できる個人認証としてライフスタイル認証を紹介したが、金融サービスにも適用できるか。本認証以外に他の認証と組み合わせることでより強固な本人認証が可能かなど検討が必要となる

5G MMF
The Fifth Generation Mobile Communications Promotion Forum

ご清聴ありがとうございました。