6G サービスが提供する IoT と AI のプラットフォームとセキュリティ対策

味戸 克裕[†a)]　　張　毅波[†]

A platform for IoT and AI and the security provided by 6G service

Katsuhiro AJITO[†a)], Yibo ZHANG[†]

あらまし　2030 年ごろにサービスが開始される超高速ワイヤレス通信の 6G（第 6 世代移動通信システム）サービスは, IoT と AI のプラットフォームとして期待される．この 6G に関する要求条件, 国際標準化動向, アプリケーションと今後課題となるセキュリティ対策やセキュリティ・アーキテクチャについて議論する．

キーワード　6G，サイバーフィジカルシステム，ウエアラブルデバイス，IoT デバイス，メタバース，HAPS, テラヘルツ, XR, VR, AR, MR, デジタルツイン, インダストリー 5.0, スマートグリッド 2.0, セキュリティ・アーキテクチャ，AI 補助診断

Abstract　The 6G (6th Generation Mobile Communications System) service, an ultra-high-speed wireless communication service to be launched around 2030, is expected to serve as a platform for IoT and AI. The 6G related requirements, international standardization trends, applications, security measures, and security architecture are discussed.

Keywords　6G, cyber-physical system, wearable device, IoT device, metaverse, HAPS, terahertz, XR, VR, AR, MR, digital twin, industry 5.0, smart grid 2.0, security architecture, AI-assisted diagnosis

1. まえがき

5G（第 5 世代移動通信システム）のサービスが始まり数年が経ち，現在は 6G（第 6 世代移動通信システム）のサービスに向けた研究開発や標準化などが進んでいる．5G では，国際電気通信連合 無線通信部門（ITU-R，ITU Radio communication Sector）において eMBB（enhanced Mobile Broadband：高速大容量），URLLC（Ultra-Reliable and Low Latency Communications：超高信頼低遅延），mMTC（massive Machine Type Communication：超大量端末）の 3 つのカテゴリーが要求条件として規定されたが，6G では自動運転や VR（Virtual Reality：仮想空間）などを使うメタバースによるサイバー・フィジカル空間の融合がより進み，IoT のクラウド連携やクラウド上での AI 処理が高速に行えるプラットフォーム上で，この 3 つが連携するより複雑なカテゴリーのユースケースが想定される [1]．本稿では 6G の要求条件, 標準化動向, アプリケーション．セキュリティの課題と対策，セキュリティ・アーキテクチャについて議論する．

† 大阪国際工科専門職大学 工科学部 情報工学科，大阪府
Department of Information Technology, Faculty of Technology, International Professional University of Technology in Osaka, 3-3-1 Umeda, Kita-ku, Osaka, 530-0001 Japan

a) E-mail: ajito.katsuhiro@iput.ac.jp

2. 6G サービスの要求条件と国際標準化

2.1　6G の周波変遷と通信速度

日本での移動通信システムの始まりは，1979 年 12 月に開始された 800MHz 帯を用いたアナログ方式の自動車電話サービスで，これが音声通話の 1G サービスとなる [2]．その後，図 1 に示すように，10 年ごとに次世代移動通信システムが提供される．2G では，音声通話に加え，SMS

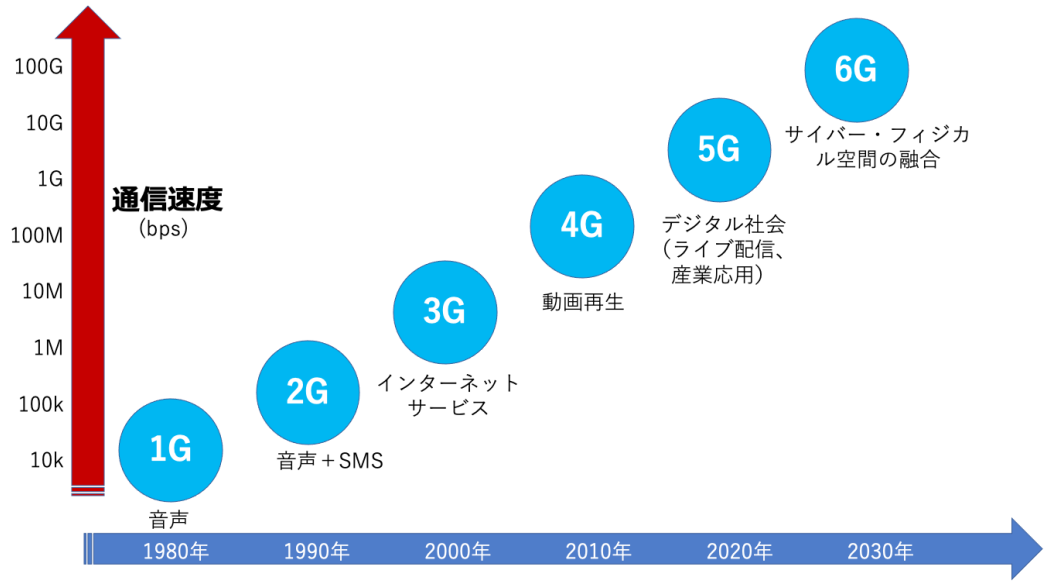

図 1　移動通信システムの進化
Figure 1　The evolution of mobile communication from 1G to 6G.

と呼ばれるメッセージ機能が加わり，3G ではスマートフォンやタブレットを使用できるインターネット環境が提供された．世代ごとに通信速度が 10 倍程度ずつ高速化して，4G ではスマートフォンでのユーチューブなどの動画再生，5G では動画のライブ配信や産業応用，さらに 6G では高度な自動運転やメタバースによるサイバー空間とフィジカル空間が統合した CPS（Cyber-Physical System：サイバーフィジカルシステム）がより進化すると考えられる．

2.2　6G の周波要求条件

VR デバイスなど含むウェアラブルデバイスの高機能化，4K や 8K それを超える高精細映像やホログラム，五感による感覚的な情報伝達が実現し，人と人，人とモノとの通信がよりリアルなものとなる．これにより，ゲーム，スポーツ観戦などで革新的なエンターテイメントサービスや遠隔医療や遠隔教育が場所と時間の制約なく提供される．これら eMBB，URLLC，mMTC の 3 つが連携するような，より複雑なカテゴリーのユースケースは 2026 年までに策定される予定であり [1]，日本では NTT ドコモが，6G の 2030 年のサービス提供開始を目指している [3]．5G の高速・大容量，低遅延，多数接続の各性能をさらに高めるとともに，テラヘルツ波などの新たな高周波数帯の開拓，地上だけでなく空・海・宇宙などへの通信エリアの拡大，超低消費電力通信実現などを目指して，研究開発が進められている．また，ワイヤレス通信のネットワーク自身が電波を用いて測位や物体検知など，実世界をセンシングする機能を備えていくような進化も想定され，誤差数センチメートル以下の超高精度な測位が実現できると期待される．ここでは，様々なユースケースを実現するための 6G に関する 6 つの要求条件について述べる．

(1)　超高速ワイヤレス通信

6G の場合，多くのユーザーが同時に楽しんだり，仮想協同作業をしたりするなどサイバー空間上での新たなシンクロアプリケーションの実現も期待される．具体的には 100Gbps（毎秒 100 ギガビット）を超えるワイヤレス通信速度が要求条件となり，通信速度が人間の脳の情報処理速度レベルに近づくにつれ，単なる画像伝達（視覚や聴覚）だけでなく，五感による感覚的な情報伝達，さらには多感覚コミュニケーションなどの拡張も考えられる．そして，産業やサイバー・フィジカル融合のユースケースなどの動向を考えると，実世界のさまざまなリアルタイム情報をクラウドに伝送し AI 処理することになる．

(2) 超低遅延

CPS を人体に例えると，AI とデバイスをつなぐワイヤレス通信は情報を伝達する神経系に相当するといえ，リアルタイムかつインタラクティブな AI によるサービスをより高度に実現するには，常時安定した E2E（End to End）での低遅延性が基本的な要求条件になると考えられる．6G に向けて，具体的には E2E で 1 ミリ秒以下の超低遅延が目標となる．これによって例えば，ロボティクスによる無人化店舗において，客の声のトーンや表情を見て人間のように気の利く，違和感のないインタラクティブな遠隔ロボット接客を可能にする．さらに，遠隔医療，遠隔教育など，さまざまな分野での応用が期待される．

(3) 超多接続

CPS の高度化により，ウェアラブルデバイスやマイクロデバイスといった IoT デバイスを人体に装着することで，サイバー空間が人間の思考や行動をリアルタイムでサポートするユースケースが考えられ，人とモノのコミュニケーションに関わる超大量のデバイスが普及し，5G の要求条件のさらにその 10 倍（1 平方 km あたり 1000 万デバイス相当）という究極の多重接続が要求条件となる．

(4) 超低消費電力

通信速度単位（ビット / 秒）あたりに必要な消費電力の大幅な削減を目指す．ネットワークの低消費電力化は，地球環境問題に配慮した持続可能な社会という世界的な目標を達成するための要求条件であり，IoT デバイスのセンサーなどの端末数が増加し，ユーザーインターフェースがウェアラブルに進化するユースケースが想定される場合にも，使用時間の面から低消費電力は重要な要素となる．

(5) 超カバレッジ拡張

6G の場合，陸上でのエリアカバー率は 100%，そして現在の移動通信システムがカバーしていない空（高度 10 ー 20km 程度）・海・宇宙などを含むあらゆる場所でのユースケースを想定した「超カバレッジ拡張」が要求条件となる．HAPS（High-Altitude Platforms の略）とよばれる携帯電話の基地局装置を搭載し高い高度を飛び続ける無人飛行機を使った空中ネットワークは，6G の次世代のネットワークとして期待されている [4]．すでに，2019 年 4 月，ソフトバンクの子会社 HAPS モバイルが，地上約 20km の成層圏を飛行する成層圏通信プラットフォーム向け無人航空機を開発している [5]．HAPS 搭載基地局のカバーエリアは直径 200km であり，日本全土ならば約 40 機でカバーでき，繋がらないところが無いことが大きな利点である．例えば，ドローンを活用した宅配や農作物の運搬，空飛ぶ自動車や宇宙旅行などのユースケースへも対応できる．

(6) 超高信頼性通信

産業向けユースケースの中には，遠隔制御や工場自動化など，必要な性能を担保することが要求されるものが多くあるため，高信頼な制御情報のワイヤレス通信は重要な要求条件であり，6G では 5G よりもさらにレベルの高い信頼性や高セキュリティの実現が期待される．さらにロボットやドローンの普及や，空，海等への無線カバレッジの拡大に伴い，工場等の限られたエリアだけでなく，より広いエリアでの通信では，サイバー攻撃の高度化や個人情報の漏えいなど，セキュリティ上の脅威が増大するが，これらについては，後に詳しく述べる．

2.3 6G の周波数帯の国際標準化とテラヘルツ波

6G では超高速ワイヤレス通信を実現するため，図 2 に示すように広い周波数帯を使うことが検討されているが，その中にサブテラヘルツあるいはテラヘルツ（THz = 10^{12}Hz）と呼ばれる非常に高い周波数が含まれる．具体的には 100GHz（= 10^{11}Hz）から 3THz（= 3×10^{12}Hz）の周波数の利用が検討されている．より高い周波数の利用は高速データ転送には有利だが，光の性質に近くなり直進性が増すため，無線基地局アンテナのカバー範囲が狭くなり，多くのアンテナを張り巡らせる必要がある．スマートフォンに搭載させる技術はまだ先だが，バックホール（無線基地局アンテナと基幹通信網を繋ぐ中継回線）やフロントホール（無線基地局とアンテナ部が離れている場合の

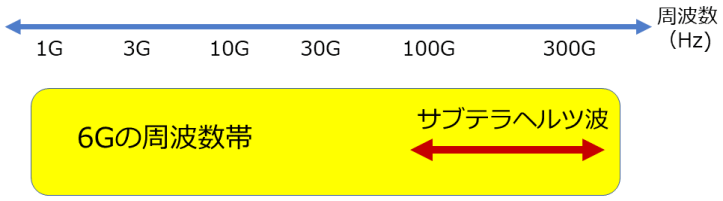

図 2　6G の周波数帯
Figure 2　Frequency bands in 6G.

両者をつなぐ中継回線）での業務利用は，既に 2017 年 IEEE 802.15.3d-2017 で 252GHz ー 325GHz（通称 300GHz 帯）にて通信速度 100Gbps の国際的標準化がされている [6]．この 300GHz 帯の研究では日本が先行しており [7]，the Horizon 2020 EU-Japan project ThoR（“TeraHertz end-to-end wireless systems supporting ultra-high data Rate applications,” 2018-2022）の日本 -EU プロジェクトでは，160m の距離を 40Gbps の実証実験に成功している [8].

また，2019 年の WRC（Word Radio Conference：世界無線通信会議）で日本，ドイツ，IEEE などからの寄与文書によって議題 1.15 によって 275 ー 450GHz の標準化が進められている [9]. さらに，波長が短くなり光のように直進性が高くなる特徴を活かして，ワイヤレス通信のネットワーク自身が電波を用いて測位や物体検知など，実世界をセンシングする機能を備えていくような進化も想定される．300GHz の波長は約 1mm であり，波長程度の誤差でも電波として超高精度な測位が実現できる可能性が高いと考える．

3. 6G サービスのセキュリティ

6G に関するセキュリティ課題は，大別すると 6G への新しい通信技術の導入によりもたらされる課題と，6G を利用した新しいサービスやアプリケーションを実現するために解決しなければならない課題があると考えられる．前者は，主に 6G の物理層とネットワーク層，つまり 6G コアネットワークでセキュリティ対策をたてる必要がある．一方，後者は，6G の物理層を含む各レイヤでセキュリティ対策を講じる必要がある．ここでは後者の方を中心に議論する．

3.1　6G における典型的なアプリケーションとその特徴

6G の上に展開しようとされている典型的な 7 つのアプリケーションを図 3 に示す [10]．ここで，VLC は可視光通信（Visible Light Communications の略）である．

（1）　UAV/CAV

UAV（Unmanned Aerial Vehicles の略）とは，ドローンなどを指す. そのデバイスとシステムには，物理的ハイジャックをされる可能性，制御信号の完全性を維持することの重要性，デバイスの多様性，消費電力の制限，低いコンピューティング能力といった特徴がある．

CAV（Connected Autonomous Vehicles の略）とは，自動運転機能付き車のことである．例えば，物理的ハイジャックをされる可能性，制御信号の完全性を維持することの重要性，デバイスの多様性など，UAV と似た特徴がある．加えて，データセキュリティや個人情報が非常に重要であるというような特徴もある．

（2）　XR

XR（eXtended Reality の略）とは，VR（Virtual Reality の略），AR（Augmented Reality の略），MR（Mixed Reality の略）といった画像処理技術を用いて現実世界と仮想世界を融合する技術の総称である．個人利用歴やクレジットカード情報，および感情，行動，判断，所在を含む個人情報が使われる．また，XR アプリケーションではいろいろなデータのやりとりがなされ，利用者の認証やアクセス制御も行わなければならない．そのほかに，デバイスの多様性，高いスケーラビリティと低いオーバヘッドが要求されるというような特徴がある．

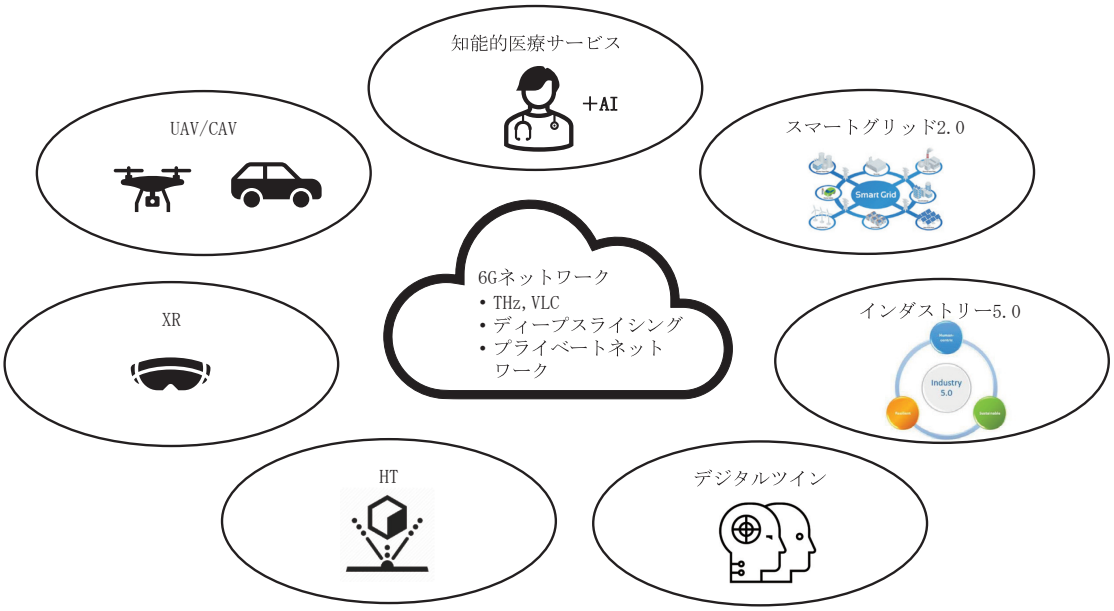

図 3　典型的な 6G アプリケーション
Figure 3　Typical 6G Applications.

(3)　HT

HT（Holographic Telepresence の略）とは，離れた場所にいる人や物体を，物理的な存在に匹敵する高いレベルの現実性があるフルモーションでリアルタイムの 3 次元ホログラムで投影して表現する技術である．使用する通信自体がすでに広帯域を必要とするため，そのセキュリティシステムはさらに通信に負荷をかけてはならない．また，多様なデバイスが使用され，運用コストを抑えなければならないといった特徴もある．

(4)　デジタルツイン

デジタルツインは，物理的オブジェクトを正確に反映するように設計された仮想モデルであり，機器制御や自動化において 6G のひとつの重要なアプリケーションになるとみなされている．具体的には，健康管理，工業自動化，電気・ガス・水道など公共サービス設備管理などに応用される．物理的な領域とサイバー領域間のデータのやりとりが保護されなければならない．また，グループ通信のセキュリティ維持も重要であり，ブロックチェーンなどが有効な手段だと考えられる．

(5)　インダストリー 5.0

インダストリー 5.0 はインダストリー 4.0 の次期バージョンであり，人間とロボット・知能機械とのより密接な協同関係が自動化と効率化の柱に加えられるとされる．制御コマンドや監視データなどの完全性の保護が重要である．認証やアクセス制御，可用性維持も必要不可欠である．また，多様なデバイスが使用され，運用コストを抑えなければならないといった特徴もある．

(6)　スマートグリッド 2.0

スマートグリッド 1.0 を進化させたものであり，メータデータの自動分析，知能的動的価格設定，配電網の自動化管理および高信頼電力配送などの機能を提供することが見込まれている．メータ設備，通信機器，ソフトウェアなどはすべてセキュリティ攻撃の対象とされる可能性がある．また，自動料金請求システムや分散化された電力取引システムも，攻撃の対象として狙われやすい．

(7)　知能的医療サービス

AI 補助診断，医療設備インターネット（IoMT = Internet of Medical Things），知能化ウェアラブルデバイス（IWD = Intelligent Wearable Devices）およびホスピタルツーホーム（H2H = Hospital-to-Home）などに基づいた知能的医療サービスが開発されるであろう．医療設備インターネットおよび知能化ウェアラブルデバイスは 6G を主要な通信プラットフォームとして使う．人々の健康や命に

かかわるものであるため，医療データの機密性と完全性は非常に大事である．また，機器認証，アクセス制御，個人情報保護および AI のセキュリティもとても重要である．

3.2　セキュリティ課題と対策

本節では，前述した各アプリケーションとその特徴において潜在しているセキュリティ課題，およびその対策を表 1 にまとめた [11]—[13]．さらに，これらの対策に関連して，次のような新しい技術の適用が検討されている．

(1) ネットワークアクセス制御：6G-AKA，耐量子計算 EAP-TLS.
(2) シグナリングデータ暗号化：256-NEA1/256-NEA2/256-NEA3, 256-NIA1/256-NIA2/256-NIA3（耐量子計算）
(3) トランスポート層セキュリティ：耐量子計算 TLS, 量子鍵配布（QKD）
(4) アプリケーション層セキュリティ：SEPP with HTTP/3
(5) ネットワーク管理：SD-WAN セキュリティ技術，ディープスライシングによるネットワーク隔離
(6) 侵入防止：AI を利用したファイアウォール／侵入検知システム（IDS）／移動目標防衛（MTD）

3.3　セキュリティ・アーキテクチャ

6G の応用システムにおいては，セキュリティ対策に応じたセキュリティ・アーキテクチャを構築しなければならない．過去の研究の中で，文献 [11] では 3 階層（物理層，コネクション層とサービス層），文献 [14] では 5 階層（デバイス層，コミュニケーション層，システム層，データ層とアプリケーション層）に分けられていることが見られる．文献 [11] は 6G コアネットワークを中心に考えられているためシンプルな層構成になっている．一方，文献 [14] は，システム層とデータ層の内容は実は他の層に属するべきであり，また，この文献も 6G コアネットワークを超えたインターネットの範囲まで考えていない．従って，本稿では，これら文献を参照しながら，実際のネットワークおよびハードウェアとソフトウェアの構造と配置を考慮して 4 階層に分けることにした（図 4）．

表 1　セキュリティ課題と対策
Table 1　Security issues and countermeasures.

セキュリティ課題	対策
物理的ハイジャック	・耐タンパー設計 ・ワイヤレス通信の盗聴，ジャミングとパイロット汚染対策
制御コマンドや監視データの完全性	・なりすまし対策 ・中間者攻撃対策
デバイスの多様性	・複数セキュリティ技術の同時サポート ・システマティックセキュリティ設計 ・セキュリティ機能デレゲーション
消費電力の制限	・ライトウェイト暗号 ・ライトウェイト暗号通信
低いコンピューティング能力	・ライトウェイト暗号 ・セキュリティ機能デレゲーション
データセキュリティ，個人情報保護	・次世代暗号技術 ・次世代電子署名技術
利用者の認証，アクセス制御	・次世代認証技術 ・リプレイ対策 ・ファイアウォール
高いスケーラビリティと低いオーバヘッド	・分散型公開鍵暗号基盤 ・ブロックチェーン
セキュリティ仕組みの通信負荷低減	・ライトウェイト暗号通信
運用コストの低減	・攻撃の自動検知 ・マルウェアの自動排除 ・ソフトウェア脆弱性の自動修復
物理的な領域とサイバー領域間のデータ通信保護	・次世代暗号技術 ・次世代電子署名技術
グループ通信	・ブロックチェーン ・マルチキャストセキュリティ
可用性維持	・DoS 対策 ・リアルタイムセキュリティ対策
設備，通信機器，ソフトウェアへの攻撃	・多層防御対策 ・ゼロトラスト対策
AI に関するセキュリティ	・AI 技術を用いたセキュリティ対策 ・AI を用いた攻撃への対策
システム機密性への攻撃	・次世代暗号技術 ・次世代電子署名技術 ・次世代認証技術

(1) デバイス層セキュリティでは，ハードウェアの耐タンパー性，そしてソフトウェアとデー

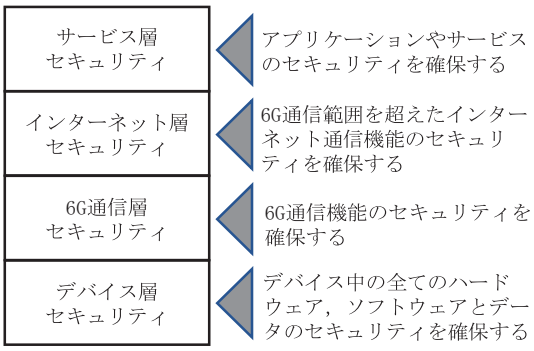

図 4　セキュリティ・アーキテクチャ
Figure 4　Security Architecture.

タの機密性，完全性，可用性を維持するための仕組みを備える．

(2) 6G 通信層セキュリティでは，6G 通信の物理層やネットワーク層のセキュリティを保証する．

(3) インターネット層セキュリティでは，6G 通信範囲を超えた広い範囲の通信ネットワークと通信する際のセキュリティを保証する．

(4) サービス層セキュリティでは, アプリケーションやサービスを実現するにあたって求められる特有なセキュリティを保証する．

また，すでに提唱されているゼロトラストという概念は，6G のセキュリティ・アーキテクチャでも提唱・実現すべきであろう．

4. むすび

6G は超高速ワイヤレス通信として，さまざまな要求条件に対して研究開発や国際標準化が進み，2030 年ごろサービスが開始されると期待される．これにより，データのクラウド処理が高速となり IoT と AI のプラットフォームができることになる．この 6G に関する要求条件，国際標準化動向，6G を利用した新しいサービスやアプリケーションを紹介すると共に、それらに対するセキュリティ対策やセキュリティ・アーキテクチャについて議論した．

5. 謝辞

本稿をまとめるに際し，情報通信研究機構（NICT）笠松章史にご助言を頂いたことに感謝する．

文　献

[1] ITU-R WP5D, “Attachment 2.12 to Chapter 2 of Document 5D/1341, *Meeting report WP5D #41*, June 2022.

[2] ドコモ歴史展示スクエア
http://history-s.nttdocomo.co.jp/list_car.html

[3] ドコモ 6G ホワイトペーパー 5.0 版（2022 年 11 月公開）
https://www.docomo.ne.jp/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperJP_20221116.pdf

[4] N. Saeed, H. Almorad, H. Dahrouj, T. Y. Al-Naffouri, J. S. Shamma, and M. -S. Alouini, “Point-to-Point Communication in Integrated Satellite-Aerial 6G Networks: State-of-the-Art and Future Challenges,” *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1505-1525, June 2021.

[5] https://www.softbank.jp/sbnews/entry/20190826_01

[6] “IEEE Standard for High Data Rate Wireless Multi-Media Networks--Amendment 2: 100 Gb/s Wireless Switched Point-to-Point Physical Layer,” in IEEE Std 802.15.3d-2017, pp.1-55, 18 October 2017.

[7] H.-J. Song, K. Ajito, Y. Muramoto, A. Wakatsuki, T. Nagatsuma, and N. Kukutsu, “24 Gbit/s data transmission in 300 GHz band for future terahertz communications,” Electronics Letter, vo. 48, No. 25, pp. 953–954, July 2012.

[8] T. Kürner and T. Kawanishi, “Demonstrating 300 GHz Wireless Backhaul Links - The ThoR Approach,” 2022 47th International Conference on Infrared, Millimeter and Terahertz Waves (IRMMW-THz), pp. 1-1, 2022.

[9] 総務省 世界無線通信会議 WRC-19 の議題及び結果概要 ,
https://www.tele.soumu.go.jp/j/adm/inter/wrc/wrc19/kaitai.htm.

[10] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, “The Roadmap to 6G Security and Privacy,” *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094-1122, May 2021.

[11] V-L, Nguyen, P-Ching Lin, B-C, Cheng, R-H Hwang, and Y-D Lin, “Security and privacy for 6G: A survey on prospective technologies and challenges,” *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, pp. 2384-2428, August 2021.

[12] Y. Zhang, “A Systematic Security Design Approach for Heterogeneous Embedded Systems,” Proceedings of *IEEE 10th Global Conference on Consumer Electronics (GCCE)*, pp. 577-579, October 2021.

[13] Y. Zhang, “Delegation of Security Functions in Heterogeneous Embedded Systems,” *Proceedings of IEEE 40th International Conference on Consumer Electronics (ICCE)*, pp. 709-714, January 2022.

[14] Z. Chen, K-C Chen, C. Dong, and Z. Nie, “6G Mobile Communications for Multi-Robot Smart Factory,” *Journal of ICT Standardization*, vol. 9, no. 3, pp.371-404, December 2021.

（2023 年 1 月 8 日受付　2023 年 2 月 6 日再受付）

味戸 克裕

1995 年東京大学 大学院工学系研究科 応用化学専攻 博士課程修了．博士（工学）．同年 NTT 研究所に入所．総務省テラヘルツ波プロジェクトに参画し，6G 次世代 ICT の国際標準化に従事．その後，現職にて 6G による現実空間と仮想空間を融合したサービスを研究．

張　毅波

1982 年中国清華大学計算機科学系卒．1994 年東京大学大学院電子工学修士課程修了，1998 年同博士課程修了．博士（工学）．現在，IoT とセキュリティ分野の研究に従事．