2020年4月　年4回季刊発行

NTT DOCOMO

# テクニカル・ジャーナル

Technical Journal

Vol.28 No.1 | Apr. 2020

**DOCOMO Today**

- 5G時代の幕開け

**Technology Reports（速報）**

- 5G商用サービス概要

**Technology Reports & Standardization（特集）**

パスワード課題を解決するFIDO（ファイド）認証特集

- ID・パスワードのあり方を変える dアカウント パスワードレス認証
- FIDOアライアンスにおける オンライン認証の標準化動向とドコモの貢献

**Technology Reports**

- ドコモのサービスを支える加入者データベース仮想化

**Standardization**

- 2019年ITU無線通信総会（RA-19），世界無線通信会議（WRC-19）報告

**Event Reports**

- DOCOMO Open House 2020 ―ようこそ，5Gリアルワールドへ．そしてその先へ．―

NTT docomo

# 5G時代の幕開け

5G事業推進室　室長
太口（たぐち）　努（つとむ）

2020年3月，日本でも第5世代移動通信システム（5G）の商用サービスがスタートしました．移動通信システムは，アナログ方式の第1世代から，デジタル方式（第2世代），IMT-2000（第3世代），LTE（第4世代），そして第5世代と，これまでおおむね10年に1度その世代を進化させてきました．その間，通信速度の飛躍的な高速化とネットワークの大容量化が図られ，人々の日常生活をより便利にし，また産業分野での生産性向上，付加価値創造などにも寄与してきました．5Gにおいてはさらなる高速化・大容量化が図られ，高精細な映像伝送やVR（Virtual Reality），MR（Mixed Reality）などがこれまで以上にスムーズに利用可能となります．さらに，5Gの特長には低遅延，多数同時接続もあり，これらにより素早いリアクションが要求されるeスポーツをはじめとするゲーム分野，さまざまな多数のセンサデバイスを利用するIoT分野などでの活用も期待されています．

5Gの導入は，その技術的性能の向上による移動通信システム基盤の進化であるとともに，それに加えて新たなビジネス創出に繋がる事業基盤の進化でもあり，ひいては社会的課題の解決や地方創生に資する社会基盤の進化と捉えられます．ドコモは，これらの進化の実現に向け，2018年2月より推し進めているドコモ5Gオープンパートナープログラムを通して，さまざまな業種の企業，日本各地の自治体，また，大学などの研究機関などとともにサービス・ソリューションの創出を行ってきました．その一部については今年1月に東京で開催したDOCOMO Open House 2020でも展示し，その成果は多くの来場者に評価されました．

このように広範にわたるサービスや産業が創出される5G時代では，これまで使用されてきたスマートフォンやタブレットに加え，多様なデバイスも積極的な活用が想定されます．例えば，VR映像サービスを，5Gスマートフォンを経由したVR用ヘッドマウントディスプレイ（HMD：Head Mounted Display）や将来的には5G通信可能なVR用HMDを利用することで，モバイル環境において没入感や直感に訴えるような体感を得ることが可能となります．ほかにも，高精細カメラ，ウェアラブルデバイス，センサデバイスなどとの連携により，スマートフォンなどのUI/UXの制約から解放され，新たなユーザ体験が提供される時代となっていくでしょう．また，デバイスを提供するベンダにとっても5Gを活用したエコシステムへの参入が容易になり，ビジネスチャンスが広がります．

今後ますます多種多様となるお客様のニーズに対応していくためには，その時代の最先端のICTによって付加価値を産み出し，それらをどう活用していくかが重要となります．次の10年を支える重要な基盤となる5Gを有効に活用し，お客様にその価値を体感していただける未来のデザインが，今の時代に期待されています．

本誌に掲載されている社名，製品およびソフトウエア，サービスなどの名称は，各社の商標または登録商標．

NTT DOCOMO
テクニカル・ジャーナル
Technical Journal
Vol.28 No.1 Apr. 2020

# [ Contents ]

## DOCOMO Today

5G時代の幕開け　太口 努　1

## 特別寄稿

「No 5G, No Life」　大鐘 武雄　4

## Technology Reports（速報）

5G商用サービス概要　6

5G　高速・大容量／低遅延／多数端末接続　商用サービス化

## パスワード課題を解決するFIDO（ファイド）認証特集

## Technology Reports（特集）

ID・パスワードのあり方を変えるdアカウント パスワードレス認証　11

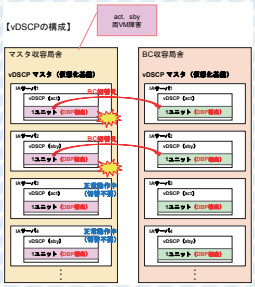
生体認証　セキュリティ　FIDO認証

（P.11）

## Standardization（特集）

FIDOアライアンスにおけるオンライン認証の標準化動向とドコモの貢献　22

FIDO認証　セキュリティ　公開鍵暗号方式




(P.33)

## Technology Reports

ドコモのサービスを支える加入者データベース仮想化　33

D-SCP　仮想化　信頼性

## Standardization

2019年ITU無線通信総会（RA-19），世界無線通信会議（WRC-19）報告　42

ITU　WRC　5G

(P.48)

## Event Reports

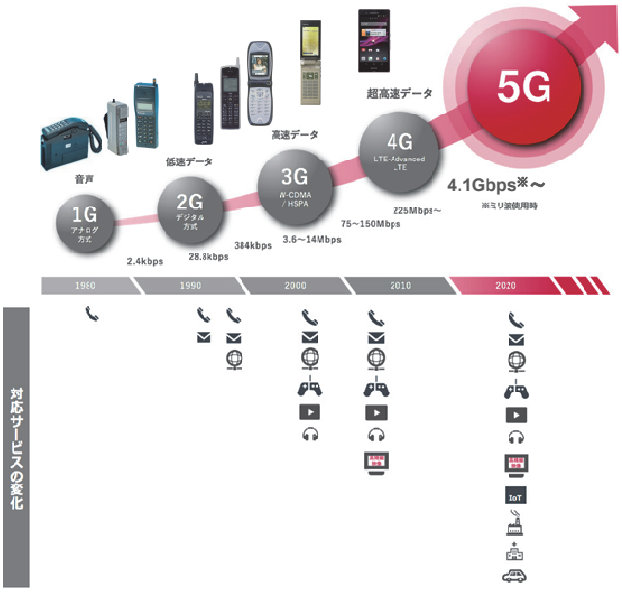
DOCOMO Open House 2020
―ようこそ，5Gリアルワールドへ．そしてその先へ.―　48

5G　Open House　展示会レポート

(P.56)

## News

「第1回KPMGジャパン秘密計算ハッカソン」で
サービスイノベーション部のチームが優勝　56




Technology Reports（速報）　5G商用サービス概要（P.6）
移動通信システムの進化

特別寄稿

# 「No 5G, No Life」

北海道大学　大学院情報科学研究院　教授　大鐘（おおがね）　武雄（たけお）さん

分社化により誕生したドコモという企業が大きな発展を遂げ，第5世代移動通信システム（5G）の実現までに至ったことに，無線通信研究者の端くれとして心よりお喜び申し上げます．そして，5Gの本格サービス開始の時期にこの特別寄稿の機会を頂きましたこと大変嬉しく思います．

とはいえ，特段誇るべき実績もない私が本稿でどのようなお話をするべきか，随分と迷いました．最近取り組んでいる確率伝搬法の話など，多くの読者は見向きもしないことでしょう．そんな折DOCOMO Open House 2020に参加したところ，5Gを取り巻く世界に想像以上の熱気を感じました．本稿では，その印象も交えながら，今後携帯電話事業に大きな変化が訪れるかもしれないという私の勝手な期待と展望を述べたいと思います．

携帯電話システムは，ほぼ10年ごとに新しい世代が登場しています．しかし，細かく見ますと，技術革新が中心だった2Gと3Gに対し，3.5G以降はスマートフォン需要が新世代の登場を後押ししたように思います．しかし，そのスマートフォンが出現したきっかけは，2G時代のi-modeに遡るといっても過言ではありません．当時，9.6kbpsのサービスにどれほどの需要があるのかと懐疑的だったのですが，蓋を開けてみると瞬く間に利用者が増加し，携帯電話は誰もが必要とするツールへと変貌しました．その後のスマートフォンの出現は必然と思います．

では5Gはどうでしょうか．私は当初，大規模MIMO（Multiple Input Multiple Output）[*1]やNOMA（Non-Orthogonal Multiple Access）[*2]技術，ミリ波帯の利用など技術革新主導の世代と考えていました．実際，2019年までのDOCOMO Open Houseでは，技術革新を前面に押し出した展示が印象に残っています．ユースケースの3つの柱：eMBB（enhanced Mobile BroadBand），URLLC（Ultra-Reliable and Low Latency Communications），mMTC（massive Machine Type Communications）における具体的なアプリケーションは，5Gサービス開始後に徐々に立ち上がるものと安易に考えていたのです．

しかし，2020年のDOCOMO Open Houseでは様相ががらりと変わり，アプリケーションに関する展示企業の多さに驚きを覚えました．IoT，AIというキーワードを代表にして，スマートオフィス，スマートシティ，XR（VR（Virtual Reality）/AR（Augmented Reality）/MR（Mixed Reality）），デジタルマーケティング，顔認証，自動運転，遠隔操作，ワイヤレス給電など，書ききれないほどのさまざまなアプリケーションや関連技術が登場しています．このような潜在的な需要をサービス開始前に掘り起こしたことが5Gの最大の成果であり，このことが逆に今後の技術革新にも大きな影響を与えると思われます．

将来を占う良い例が，最終日の5Gイノベーション推進室長の中村 武宏氏による5G Evolution & 6Gと題したパネルセッションでした．Ericsson社のErik Dahlman氏，Nokia社のAmitabha Ghosh氏に加え，NVIDIA社副社長の大崎 真孝氏も登壇されたことが，5Gと5G以降のAI（人工知能）の立ち位置を象徴しています．5G以降の仕様上の要求条件は，例えば遅延0.1ms以下，99.9999999％（“nine nines”）の信頼性などの数値が挙げられる例もあります．しかし，今後登場するアプリケーションは単純な数値では表せない多様な要求条件を必要とすると思われます．個々の具体的なユースケースとその要求条件に応えることが5G以降にとって最も重要だという認識はパネリスト共通の理解でした．

例えば，遅延1つとっても，300kmの通信距離で片道1msの遅延が最低限生じることを考えると，無線回線の遅延削減のみを議論することは無意味でしょう．近年注目されているMEC（Multi-access Edge Computing）[*3]もセットで考えた遅延評価が必要です．また，5Gや5G以降の通信サービスをあまねく展開するには，ドローン・HAPS（High-Altitude Platform Station）[*4]などを用いた補完ネットワークも重要になるでしょう．

より高速な伝送速度を達成するためにテラヘルツ帯の利用はもちろんのこと，超多数の大規模MIMOも実現されるかもしれません．しかし，このような技術の革新を促すのは，ビッグデータを利

**Profile**

1986年北海道大学大学院工学研究科修士課程修了．同年郵政省電波研究所入所．1992年ATR光電波通信研究所出向．1994年博士（工学）（北海道大学）．1995年北海道大学工学部助教授．2015年同大学大学院情報科学研究科教授．現在に至る．主に空間領域信号処理の研究に従事．電子情報通信学会学術奨励賞，論文賞など受賞．

本誌に掲載されている社名，製品およびソフトウエア，サービスなどの名称は，各社の商標または登録商標．

用したAIなどのアプリケーションによる需要です．我々の生活をより豊かに・便利にする進化は，このようなアプリケーションによって加速され，さらに要求条件が高まるという正帰還の状態が続いていくと考えられます．

2018年9月の北海道胆振東部地震では，道内すべてが停電するという事態になりました．そのとき，我が家で唯一利用できた情報源が携帯電話ネットワークでした．水道・エネルギーインフラに加え，通信インフラはすでに生活に欠かせない最重要公共設備となっています．5Gおよび5G以降では，多彩なアプリケーションの利用が促進されることにより，さらに携帯電話ネットワークへの依存度が高まることは間違いありません．“DOCOMO 202X CONCEPT”によれば，AIがさまざまな，しかも，欲しいと思う情報を示し，服のレコメンドもしてくれるし，家の温度管理もしてくれます．車は自動運転で，運転から解放された時間を仕事や趣味に当てることもできます．体調は体に付けたセンサがいつでも注意してくれていて，顔認証や生体認証でセキュリティも簡単にクリア．買い物も好きな品物をただ持ち出すだけで精算終了です．

一方で，そのような便利な世界も，災害などで携帯電話ネットワークが使えなくなれば，服も選べない，食品も調達できない，体温も測れない，家の温度も調整できない，車にも乗れない，などなど一転して恐ろしい事態になりかねません．Dahlman氏は信頼性をTrustyという単語で表現していました．通信回線の品質だけでなく，災害などにも強いということがこれからの重要課題であると述べています．我々も何がその解なのかを真剣に考えなければなりません．

現在，ビッグデータはGoogle社などITプラットフォーマーに集中しています．しかし，MECの利用を通して，今後は通信事業者が匿名の個人情報を入手可能となるかもしれません．さらにいえば，移動方向や利用アプリケーションなどの匿名個人情報の対価として，AIを用いてよりユーザ体験の高いサービス（MECなど）や品質（切れにくいビームトラッキング*5，HAPSなどによるエリアの充実など）を提供できる可能性があります．そして，これにIoTなどのセンサ情報が加われば，通信事業者がビッグデータ収集・活用においてITプラットフォーマーと肩を並べる時代が来ることは間違いありません．ビッグデータ企業として将来を見据えることも重要な課題と考えられます．

ただ，少し心配なのは，災害以外のネットワーク障害です．生活に深く密着した携帯電話ネットワーク上のアプリケーションが動作不能となれば，大きな混乱が生じることでしょう．クラッキングによるネットワーク機器への侵入だけでなく，電波妨害や，IoTデバイスの破壊・データの汚染など，無線通信に特有ないくつかの危険性が考えられます．このようなことがないよう，悪意ある無線ネットワーク攻撃に対する研究もさらに進める必要があるように思います．

世界は“No 5G, No Life”という時代に足を踏み入れました．最重要インフラを提供し，近い将来ビッグデータ企業になると期待される通信事業者はもちろんのこと，我々研究・教育者の責任も重大です．会場の熱気に上気しながらも，身の引き締まる思いを感じたDOCOMO Open Houseでした．

---

*1 MIMO：送受信に複数のアンテナを配備し，マルチパスによって生じる空間的な伝搬の性質の違いを利用することで，アンテナ数に比例して無線リンクの容量を増大させる無線技術．

*2 NOMA：時間，周波数，符号のリソースを複数のユーザに割り当てる際，ユーザ間でリソースの重複を許すことで効率化を図る多元接続方式．

*3 MEC：ユーザに近い位置にサーバを設置したシステムのこと．通常サーバはインターネット上に設置されるが，MECサーバはキャリア網内に設置することで，遅延を減らすことができる．これにより，通信の応答速度（レスポンス）を大幅に向上させる．

*4 HAPS：成層圏中で風が弱いとされる高度20km付近を飛ぶ無人航空無線局のこと．高高度プラットフォーム局などと呼ばれる．

*5 ビームトラッキング：複数のアンテナの振幅および位相の制御によってアンテナに指向性パターンを形成し，移動端末の移動方向を追従し，その方向に対してアンテナ利得が増加するように指向性パターンを更新する技術．

Technology Reports（速報） 5G 高速・大容量／低遅延／多数端末接続 商用サービス化

# 5G商用サービス概要

R&D戦略部 古城 悠 加藤 大世 河田 隆弘 奥山 卓 大橋 亜希

2020年3月，ドコモは5G商用サービスを開始した．5Gは高速・大容量，低遅延，多数端末接続を特長としており，その通信スペックの高さから社会課題解決や産業創出のための手段として産業界からの期待も高い．本稿では5Gの技術的特長，システム概要について解説する．

## 1. まえがき

ドコモは，2020年3月より，第5世代移動通信システム（5G）商用サービスを開始した．これまでドコモは，動画コンテンツの普及によるデータトラフィックの増加に合わせ，第3世代移動通信システム（3G）から第4世代移動通信システム（4G）へ，4GにおいてもLTEからLTE-Advancedへと，ネットワークの高度化を図ってきたが，今後も大容量プランの普及や，動画・サービスなどコンテンツのリッチ化に伴い，データトラフィックの増加傾向の継続が見込まれる．

また，5Gの高速・大容量，低遅延，多数端末接続の特長とAIを組合せることにより，従来は困難だった社会課題の解決や，新たな産業の創出が可能となり，移動通信への期待はますます高まると考えられる（**図1**）．

ドコモは，5G商用サービス開始に至るまで，2010年の5Gの基礎検討，2014年から高周波数帯の実証実験を開始．世界主要モバイル企業と共同で5Gの3GPP標準規格の早期策定に貢献しつつ，2019年9月からは5Gプレサービス実施し，協創パートナーとともに多くのソリューションを創出してきた．

今後，5Gサービスの提供エリアは，都市部や各地域における主要駅・主要空港，スタジアムのほか，パートナーとの協業を念頭においた施設などから順次5Gエリアを構築し，展開していく．

本稿では5Gの技術的特長，システム概要，提供

©2020 NTT DOCOMO, INC.
本誌掲載記事の無断転載を禁じます．
本誌に掲載されている社名，製品およびソフトウエア，サービスなどの名称は，各社の商標または登録商標．

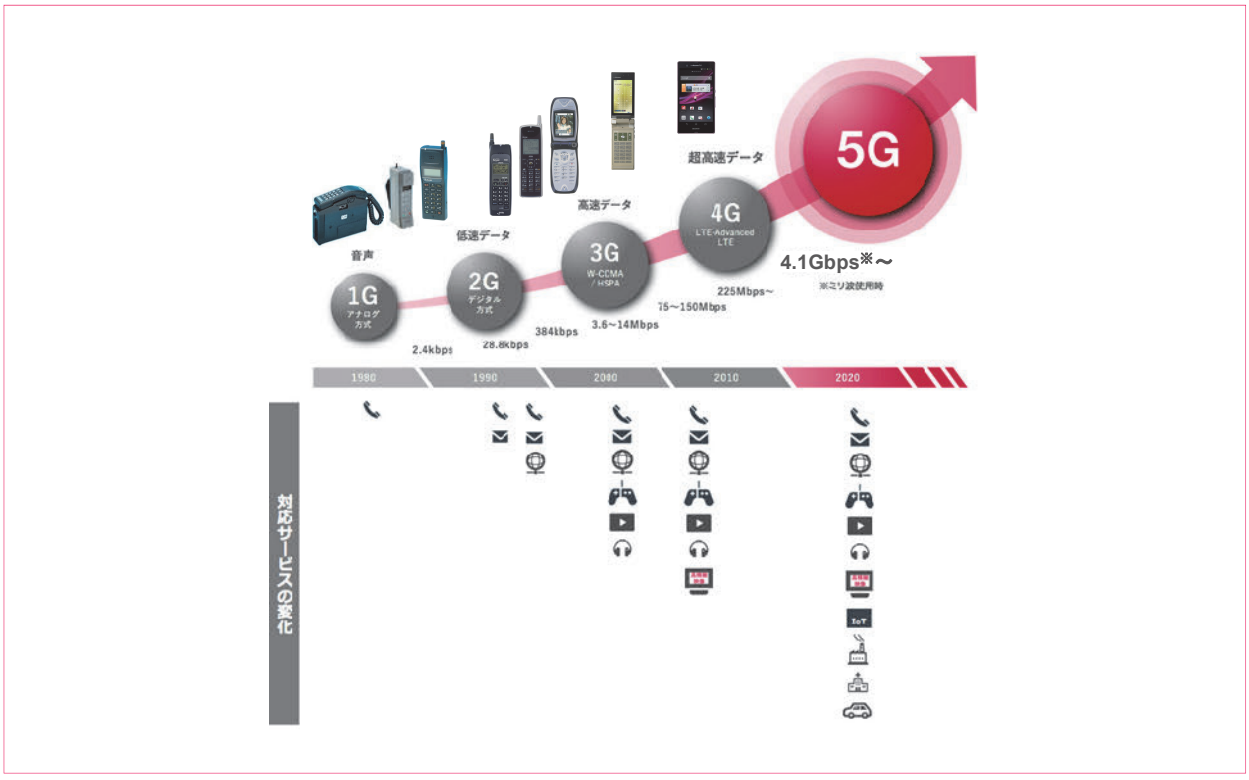



**図1　移動通信システムの進化**

サービスと端末概要について解説する．

なお，5Gを構成する無線方式やコアネットワーク技術，基地局や装置類，端末とそのプラットフォーム技術については次号以降の特集で扱う予定である．

## 2. 5Gの技術的概要

### 2.1　3つの技術的特長

ドコモは高速・大容量，低遅延，多数端末接続を特長とする5Gにより，今まで経験したことのない新しい世界を創出し，人々の暮らしがもっと便利で，そして快適になることをめざしている．それぞれの技術的特長を以下に解説する．

⑴高速・大容量

5Gでは，これまでに比べて高速に，大容量のデータを伝送することが可能となる．これにより例えばVR（Virtual Reality）*1，AR（Augmented Reality）*2を含む高精細な映像の配信が可能になり，ユーザはより臨場感のある映像やサービスを身近に楽しむことができるようになる．

高次MIMO（Multiple Input Multiple Output）*3の使用やより多くの周波数帯域の組合せを行うなどの機能向上により，最大受信速度は3.4Gbpsとなる．5G商用サービス開始時点では，**表1**のとおりの速度であり，今後も周波数の利用効率の改善をはじめとするさまざまな技術アプローチによって，さらなる高速化に向けて開発を進める．

⑵低遅延

5Gでは，遅延がより短くなることで，リアルタイム性の高い制御が可能となる．例えば工場の設備や機械の稼働状況をリアルタイムに把握，制御，運

＊1　VR：コンピュータを利用して「仮想現実」を作り出す技術．
＊2　AR：現実世界を写した映像に，電子的な情報を実際にそこにあるかのように重ねて，ユーザに提示する技術．
＊3　MIMO：複数の送受信アンテナを用いて送信信号の空間多重を行い，伝送速度の高速化，伝送容量の増大を図る信号伝送技術．

表1　最大通信速度

| サービス | 対応時期 | 速度 | | |
|---|---|---|---|---|
| LTE商用サービス | 2010年12月 | 受信時 | | 75Mbps |
| | | 送信時 | | 25Mbps |
| 5Gプレサービス | 2019年9月 | Sub6 | 受信時 | 2.4Gbps |
| | | | 送信時 | 107Mbps |
| | | ミリ波 | 受信時 | 3.2Gbps |
| | | | 送信時 | 202Mbps |
| 5G商用サービス | 2020年3月 | Sub6 | 受信時 | 3.4Gbps |
| | | | 送信時 | 182Mbps |
| | 2020年6月以降（予定） | ミリ波 | 受信時 | 4.1Gbps |
| | | | 送信時 | 480Mbps |

※通信速度は，送受信時の技術規格上の最大値

用することでオートメーション化にいっそう寄与することができる．

5Gの無線信号の送信単位は，4Gのそれに比べ周波数帯域によって1/2～1/8ほどに短縮されており，加えて送達確認を行うタイミングをデータ送信の直後にすることも可能であり，これらの技術の組合せにより，従来の4Gに比べ無線区間の低遅延化が期待される．また，MEC（Multi-access Edge Computing）*4の採用により，End-Endでの遅延低減を図っている．

⑶多数端末接続

5Gでは，スマートフォンだけでなく，センサやデバイスなど，あらゆるモノが同時に多数接続可能となることで，IoTのさらなる普及や，生活の手助けになる情報（例えば，自動販売機内の在庫状況や電気・水道・ガスなどの計量器情報などを人の手を介さず収集し，分析やその後の対応に用いる）の一層の活用が可能となる．

現状では，LTE-M*5とNB（Narrow Band）-IoT*6の2方式が広く使用されている．

## 2.2　主な5Gの無線技術

⑴高速・大容量を実現する技術

高速・大容量を実現する技術として高周波数・超広帯域*7伝送と，Massive MIMO*8に代表されるアンテナ技術などが挙げられる．

⑷高周波数・超広帯域伝送

LTEでは6GHz以下の周波数帯を利用していたが，5Gでは超広帯域化を実現するために6GHz以下の周波数帯だけでなく，高周波数帯として100GHzまでの利用が想定されている．特に5Gプレサービスでも活用した28GHz帯を含む高周波数帯は，従来の周波数帯と比較して電波伝搬特性*9が異なるため，高周波数帯の利用に適した新たな諸元が規定され，400MHzの基本帯域幅が規定されている．

なお，ドコモでは5G向けの新たな周波数帯域だけでなく従来の4Gで使用している周波数帯域を複数組み合わせて同時に無線伝送に使用することで，高速・大容量を実現している．

＊4　MEC：ユーザに近い位置にサーバを設置したシステムのこと．通常サーバはインターネット上に設置されるが，MECサーバはキャリア網内に設置することで，遅延を減らすことができる．これにより，通信の応答速度（レスポンス）を大幅に向上させる．

＊5　LTE-M：狭い周波数帯を用いてIoT（センサなど）向けに低速データ通信を行う端末用LTE通信仕様．

＊6　NB-IoT：LTE-Mよりもさらに狭い周波数帯を用いてIoT（センサなど）向けに低速データ通信を行う端末用LTE通信仕様．

＊7　超広帯域：100MHz以上の帯域幅のこと．日本では，28GHz帯において400MHzの帯域幅が5G無線通信用に割り当てられた．

(b)Massive MIMO

Massive MIMOは多数のアンテナ素子を用いることで，送受信ビームの形状を制御し環境に応じた最適なエリア構成を実現する技術である．各アンテナ素子を合成しエネルギーを一方向に集中させることでエリアを拡大することや，複数のビームを同時に生成し，同時接続数を増加させることで大容量化を可能とする．

(2)低遅延化を実現する技術

新たに導入される無線アクセス方式技術であるNR（New Radio）では，無線の最小送信単位を短くすることで，無線区間のさらなる遅延の短縮を実現している．なお，各種サービスの提供において低遅延化を実現するためにはコア装置や伝送遅延などを含めたトータルでの遅延短縮が必要であるため，無線区間に加えて有線区間での遅延短縮を併せて実現することが重要である．具体的には，より端末に近いところにコンピューティングリソースを配備するMECを5Gと組み合わせることにより，End-Endでの遅延短縮が可能となる．ドコモがMECの1つの形態として提供するドコモオープンイノベーションクラウド™＊10を用いることで，低遅延を活かした5G時代のサービスやソリューション創出を推進させる．

(3)多数端末接続を実現する技術

継続的なLTE/LTE-Advancedの進化であるeLTE（enhanced LTE）＊11規格のIoT技術であり，信号処理の簡易化などを目的に導入されたLTE-M，NB-IoTなどの技術を活用することで，一定のエリア内に設置された，少量のデータを低頻度で送るIoT端末（環境センサや計測器など）の多数端末接続が実現される．

なお，これらの技術は3GPPのRel.13～15で仕様化されたものである．5G NRにおけるIoT方式は，Rel.17での仕様化に向けて3GPPで議論中であり，NRとしての特徴を有しつつIoTに求められる低価格・低消費電力などの実現が期待されている．

## 3. システム概要

### 3.1 5G導入コンセプト

ドコモでは，幅広い周波数帯を用いて飛躍的な高速・大容量化などの性能改善を実現するNRと，基本的なエリアのカバーやブロードキャストなどのサービスを提供可能なeLTEとの組合せにより5Gの導入を進めている．

### 3.2 5Gシステム構成

ドコモでは，端末がNRとeLTEの両方の無線アクセス方式を介してモバイル網に接続するノンスタンドアローン＊12という形態により，5Gサービスを実現した．特にLTEにおける高度化C-RAN（Centralized Radio Access Network）＊13導入の際に得られたノウハウを活用し，NRとeLTEの両方が利用可能なエリアでは，2つの無線アクセス方式を用いたDC（Dual Connectivity）＊14による高速通信を提供した．5Gサービスのシステム構成図を**図2**に示す．

### 3.3 基地局装置間のマルチベンダ接続

これまでは，基地局装置同士を接続するための仕様（信号の送受信ルール）が十分に国際標準化されておらず，ベンダごとに実装が異なっていた．そのため異なるベンダの基地局装置間の接続は困難であり，通常は同じベンダの基地局装置同士が接続されていた．ところが，5G導入初期では，既存の4Gネットワークを活用しながら5Gエリアを広げていくため，選択できる5G基地局装置のベンダが4G基地局装置のベンダに制限されてしまうことになる．

この課題を解決するため，ドコモが参画しているO-RAN Allianceで基地局装置間の接続仕様の国際標準化を進めた結果，4G・5G基地局における接続仕様が統一され，マルチベンダ接続が可能となった．

＊8 Massive MIMO：非常に多数のアンテナを用いるMIMO伝送技術の総称．MIMOとは同一時間，同一周波数において複数の送受信アンテナを用いて信号の伝送を行い，通信品質および周波数利用効率の向上を実現する信号技術．

＊9 **電波伝搬特性**：伝搬損失，電力遅延プロファイル，角度プロファイルなどの特性を指す．

＊10 ドコモオープンイノベーションクラウド™：㈱NTTドコモの商標．

＊11 eLTE：3GPP Rel.15以降に準拠したLTE規格．

＊12 ノンスタンドアローン：NR単独ではエリアを提供せず，LTEのエリアと組み合わせてサービスを提供する運用形態．

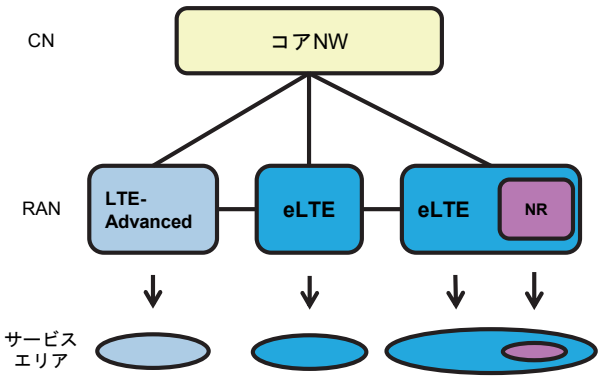



図2　システム構成図

これにより，ドコモでは既存の4G基地局ベンダに依存せず，新たに開発した5G基地局を導入できるようになったため，既存4G資産を活かしつつスピーディーな5G展開が可能である．

## 4. 提供サービス・ソリューションと端末概要

5G商用サービスにおいては，5Gの特長である高速・大容量を活かした，マルチアングル（多視点）視聴や高臨場パブリックビューイングといった観戦支援サービスを始め，さまざまなサービス・ソリューションを提供している．また今後，東京2020オリンピック・パラリンピック競技大会などのイベントにおいて，さらに新しいサービス・ソリューションを提供していく予定である．

5G商用サービスにおける対応端末は，Sub6といわれる3.7GHz帯／4.5GHz帯の100MHz幅と，ミリ波*15といわれる28GHz帯の400MHz幅の周波数を利用してNR通信を行う．従来にはない広い周波数帯域幅を利用することで5Gの特長である高速・大容量が実現できるが，広い周波数帯域幅であることに加え，高い周波数帯となるため，従来にはない高周波数・超広帯域伝送といった高度なアンテナ技術を備えた無線端末が必要となる．

## 6. あとがき

本稿では，ドコモにおける5G商用サービスの概要について解説した．

ドコモは5Gにより，今まで経験したことのない新しい世界を創出し，人々の暮らしがもっと便利で，快適になることをめざし，技術開発を進めていく．

### 文　献

[1]　下条，ほか：“5G時代に向けた将来コアネットワーク，”本誌，Vol.23，No.4，pp.49-58，Jan. 2016.
[2]　原田，ほか：“世界主要ベンダとの5G伝送実験，”本誌，Vol.23，No.4，pp.59-68，Jan. 2016.
[3]　安部田，ほか：“5G時代を支える無線アクセスネットワーク，”本誌，25周年記念号，pp.14-21，Oct. 2018.

*13 高度化C-RAN：ドコモが提唱する新しいネットワークアーキテクチャで，LTEAdvancedの主要な技術であるキャリアアグリゲーション技術を活用し，広域エリアをカバーするマクロセルと局所的なエリアをカバーするスモールセルを同一の基地局制御部により高度に連携させる無線アクセスネットワーク．
*14 DC：複数の基地局に接続し，それらの基地局でサポートされる複数のコンポーネントキャリアを用いて送受信すること．
*15 ミリ波：周波数帯域の区分の1つ．30GHzから300GHzの周波数であり，5Gで有望な周波数である28GHz帯を含めて慣習的にミリ波と呼ぶ．

Technology Reports（特集）
生体認証 セキュリティ FIDO認証
パスワード課題を解決するFIDO（ファイド）認証特集

# ID・パスワードのあり方を変えるdアカウント パスワードレス認証

プロダクト部
尾崎 友彦（おざき ともひこ）
上坂 浩貴（うえさか ひろき）
牧野 由樹子（まきの ゆきこ）
富山 由希子（とみやま ゆきこ）
森山 光一（もりやま こういち）

近年，フィッシングなどで奪取されたパスワードを用いた不正アクセスが問題となっている．また，類推しにくい複雑なパスワードを覚えなければならないなどパスワード管理にも煩わしさがある．このようなパスワード認証の課題を解決しつつ，セキュリティと利便性を両立するため，ドコモは2020年3月にFIDO®*1認証を活用したdアカウント®*2 パスワードレス認証の提供を開始した．スマートフォンの生体認証などを利用し，パスワードを無効化して不要とすることで，利便性を確保しつつ，dアカウントの不正利用を防止する．

## 1. まえがき

近年，インターネットサービスへのログインや，ネットショッピングにおける決済などさまざまな場面でオンライン認証の必要性が増している．一方，第三者による不正アクセスや不正決済などのニュースが後を絶たない．特に最近では，巧妙なフィッシングサイト*3でパスワードを奪取し，それらを悪用した不正アクセスが増加している．

ドコモは，スマートフォンやPCなどからdポイントの確認やdマーケット®*4などドコモのサービスを利用する際の共通IDとしてdアカウントを提供しており，ドコモ回線のユーザだけではなく，ドコモ回線以外のユーザにも広く利用されている．このdアカウントのログインや決済時の本人確認などのシーンにおいて，ドコモは2015年からシンプルで堅牢なオンライン認証を可能にするオープンな標準規格，FIDO（Fast IDentity Online）（ファイド）認証を活用したdアカウント生体認証を提供してきた［1］．パスワード入力の代わりにスマートフォンの生体センサに指紋や虹彩をかざすだけのシンプルな動作で認証を可能とし，dアカウント認証の利便性向上を

©2020 NTT DOCOMO, INC.
本誌掲載記事の無断転載を禁じます．
本誌に掲載されている社名，製品およびソフトウエア，サービスなどの名称は，各社の商標または登録商標．

＊1 FIDO®：FIDO Allianceの商標または登録商標．
＊2 dアカウント®：㈱NTTドコモの登録商標．
＊3 フィッシングサイト：実在する企業などの公式サイトとそっくりな偽サイト．巧みにIDやパスワードなどの個人情報を入力させて奪取する．
＊4 dマーケット®：㈱NTTドコモの登録商標．

行ったものである．しかし，パスワード認証をユーザが選択できる限り，パスワードを取り巻くセキュリティ課題を常にもち続けることとなる．そのため，FIDO認証導入当初から，将来的にはパスワードを無くすことでdアカウント認証をよりセキュアにすることを構想していた．

今回，dアカウントFIDO生体認証の十分な普及を背景として，パスワード認証をいよいよ無効にする機能を開発し，全面的にFIDO認証に移行可能なオプション機能の提供を開始した．これによりパスワードに起因したdアカウントへの不正アクセスを防止することができる．

本稿では，まずdアカウント パスワードレス認証のベースとなるdアカウント FIDO生体認証の概要について述べる．次にパスワードレス認証の実現にあたっての課題，設計・開発と導入の詳細について解説する．そして，今後の展望について述べる．

## 2. dアカウント FIDO生体認証の導入背景と概要

ドコモは，スマートフォンやタブレットからユーザがもっと便利にログインしてサービスを使えるようにするため，「あんしんをもっと便利に」をキャッチフレーズとして，2015年5月にdアカウントFIDO生体認証を導入した．ドコモ回線のユーザには，dアカウント（旧docomo ID）とそのパスワードに加えて，spモードパスワードとネットワーク暗証番号（いずれも数字4桁）を提供しており，それらをまとめる便利な認証手段として生体認証の機能を積極的に展開することとした．

生体認証を導入するにあたり，FIDO認証に着目した理由の1つは，ユーザと認証器（例えばスマートフォン）の間の本人照合の部分と，公開鍵暗号方式を活用した認証器とサーバ間の検証部分が完全に分離されていることである．これにより，スマートフォンそれぞれの機種の特徴にあった生体センサを搭載でき，異なる種類の指紋センサを搭載した複数のスマートフォンと世界初の虹彩認証スマートフォンを対象として，dアカウント FIDO生体認証の同時提供を開始するなど，端末ラインアップの魅力を高めることができた．また，機種ごとに生体センサが異なっていても認証サーバ側の個別対応を不要にできた．

そして，FIDO認証に着目したもう1つの大きな理由は，セキュリティにおける優位性である．FIDO認証では，オンライン上に生体情報やパスワードのような秘密情報を流さないため，フィッシング耐性がある．そのため，dアカウント FIDO生体認証を提供開始した当初から，将来的にはパスワード認証を無くし，FIDO認証の特長を活かしてセキュリティ強化につなげたいという構想をもっていた［1］．

一方，提供開始当初はFIDO生体認証対応スマートフォン4機種でスタートしており，多くのサービス・アプリを継続的に提供する必要性から，従来のパスワード認証も併存させる必要があった．生体センサが反応しなかった場合などへの考慮もあった．

### 2.1 FIDO UAFの採用とアーキテクチャ

dアカウント FIDO生体認証の当初の導入にあたっては，2014年12月に正式に仕様が公開されたFIDO UAF（Universal Authenticator Framework）1.0[*5]を採用した．そして，すでに商用導入していたdアカウント認証サーバと端末のdアカウント設定アプリに対してFIDO UAF 1.0の追加対応を行った．

dアカウント設定アプリは，ドコモのさまざまなサービスからの認証要求に対して一元的に処理を行うアプリである．ドコモのサービスはWebで提供しているもの，ネイティブアプリで提供しているものがあり，合わせて100以上存在する．そして，それらのサービス・アプリを原則としてdアカウント設定アプリと連携させることで，dアカウント認証

＊5 FIDO UAF 1.0：パスワードレス認証のためにデザインされた仕様．2014年12月に策定された．

サーバとの結合インタフェースをシングルポイントにしている．

このdアカウント設定アプリにFIDO UAF 1.0クライアントを内包し，端末メーカにてFIDO認証器として必要な要件を実装することで，dアカウントへのFIDO認証の導入をスムーズに実現することができた．

## 2.2 dアカウントFIDO生体認証における本人確認方法

dアカウント FIDO生体認証では，ドコモ回線のユーザがスマートフォンなど生体センサを具備する端末をFIDO認証器として設定する際，ネットワーク暗証番号の入力を必須とすることでオンライン認証に使われる生体情報がdアカウント認証の対象である本人のものであることを担保した．すなわち，本人確認できた場合にのみFIDO認証を設定させることで，本人確認の結果をFIDO認証器に括り付けることができる．

⑴ネットワーク暗証番号と本人確認

ネットワーク暗証番号とは，ドコモショップやドコモオンライン手続きでのご注文受付時などにユーザが入力する数字4桁の番号である．

ドコモでは，電気通信事業者として携帯電話不正利用防止法順守のため，従前から回線契約時などの本人確認に必要な事業基盤を確保している．1つはドコモショップなど店頭における対面での身分証明書の提示を受けての本人確認，1つは本人確認書類に記載された住居に，携帯電話などを転送不要郵便や特定事項伝達型本人限定受取郵便などで送付することによる本人確認，そしてもう1つが回線契約時に発行するネットワーク暗証番号による本人確認である．

ネットワーク暗証番号で本人確認を行うには，回線契約済みのSIM（Subscriber Identity Module）[*6]カードを挿入してドコモ回線に接続した端末において4桁の番号を入力する．SIMカードは個体として唯一性があり，かつ契約していないと回線接続できないため，それ自体が強力な所持認証（回線認証）である．また，このとき入力された4桁の番号はインターネットを流れない．すなわち，ネットワーク暗証番号は，一般のオンラインパスワードと異なり，回線認証と契約者本人のみが記憶する知識による認証を組み合わせた強力な多要素認証で，堅牢性の高いオンラインでの本人確認手段である．

⑵キャリアフリーのdアカウント FIDO生体認証

dアカウントはドコモの回線以外のユーザでも利用可能（キャリアフリー）だが，ネットワーク暗証番号は利用できない．そのためFIDO生体認証の設定においては，認証器である端末の画面ロックを必須とし，第三者がその端末を使用できないことを前提に，dアカウントのパスワード入力が必要な設計とした．

## 2.3 スマホ認証

dアカウント FIDO生体認証を発表したとき，「あんしんをもっと便利に」と合わせて将来構想として発表したのが「スマホが暮らしの鍵になる」である．すなわち，生体センサを具備しない周辺デバイスで提供するサービスを使う場合の認証においても，生体認証対応スマートフォンを使って安心・便利に認証していただきたいという構想である．

当時のPCは現在と比較して，生体センサを具備しているものは大変少なかった．また，テレビやセットトップボックスにリモコンでカーソルを何度も移動させてパスワードを毎回入力するのは面倒である．2017年1月に提供開始したスマホ認証では，あらかじめPCやセットトップボックスなどの周辺デバイスを登録しておくことで，それらのデバイスで提供するサービス・アプリにおいて「スマホで認証」ボタンを選択するだけで，パスワードを入力することなく，dアカウント FIDO生体認証対応のスマートフォンで簡単に認証することができる．

＊6 SIM：携帯電話会社と契約した電話番号などを記録しているICカード．

### 2.4 対応機種の拡大

dアカウント認証における「あんしんをもっと便利に」をより多くのユーザに提供するため，dアカウントFIDO生体認証の提供開始以降，対応機種の速やかな拡大を図った．

まず，いち早くiOS*7に対応する取組みを行った．iPhone®*8・iPadでは，すでにTouch IDを搭載している機種が普及し始めていたことから，2016年3月からTouch ID搭載機種への対応を行った［2］．また，2017年12月からFace ID搭載機種へも正式対応を開始した．

さらに，Android™*9においてもさらなる対応機種増に向けた取組みを行った．当初は，端末メーカへのFIDO UAF 1.0対応について積極的な働きかけを行った．また，ドコモがFIDOアライアンスに加入してから［3］並行して，FIDO UAF対応端末が普及するための仕組みづくりとその採用を推進した［4］．すなわち，Android OSの新しい機能を活用することで，端末メーカがFIDO認証器として必要な要件を実装するためにAndroid OSを特別にカスタマイズする必要がないFIDO UAF 1.1*10［5］の仕様化で貢献し，2017年11月から対応端末を提供開始した［6］．これにより端末メーカの開発負担を低減でき，dアカウント FIDO生体認証対応機種の継続的な提供を確実にした．

結果として，2019年末時点で，FIDO生体認証対応機種はAndroid，iOS搭載端末合計で93機種にまで広がっている（Android FIDO UAF 1.0：36機種，Android FIDO UAF 1.1：32機種，iOS：25機種）．

## 3. dアカウント パスワードレス認証の実現に向けた課題

ドコモが販売するほぼすべてのスマートフォンとタブレットで，dアカウント FIDO生体認証が利用できる土台を整えることができた背景を踏まえ，dアカウントのパスワード認証を無効化し，FIDO認証に全面的に移行するパスワードレス認証の導入が現実的となった．

dアカウント パスワードレス認証により，第三者によるパスワードの不正奪取やリスト型攻撃*11などを防ぐとともに，パスワード管理の煩雑さからも解放され，安全かつ快適なオンライン認証を提供することができる．しかし，パスワードレス認証の実現に向けては，下記のような検討すべき多くの課題があった．

・パスワードレス認証への移行方法
・生体認証の代替手段
・アカウント再設定と端末紛失時などの復旧手段の提供
・多様なデバイスへの対応
・多数のドコモサービス・アプリへの影響

(1)パスワードレス認証への移行方法

セキュリティを考慮すると，すべてのユーザがパスワードレス認証を利用することが望ましい．しかし，日々使い慣れたパスワードが使えなくなったときのユーザへの影響やサービスの継続性などを踏まえて，移行可能な対象範囲と移行方法を丁寧に検討する必要があった．

(2)生体認証の代替手段

パスワードが無効化されると，指の怪我などで生体センサが利用できない場合の代替手段として従来のパスワード認証が利用できないため，これに代わる手段を確保する必要があった．また，生体認証対応端末を持っていても生体センサを利用しないユーザが約3割いるため（ドコモ調べ），そのようなユーザもパスワードレス認証を利用できる手段を検討する必要があった．

(3)アカウント再設定と端末紛失時などの復旧手段の提供

パスワードを無効化した後に機種変更をするときの再設定や，端末紛失・故障した場合のFIDO認証

＊7 iOS：「IOS」は米国およびその他の国におけるCisco社の商標または登録商標であり，ライセンスに基づき使用されている．
＊8 iPhone®：「iPhone」「iPad」はApple Inc．の商標．ただし，「iPhone」商標は日本国内では，アイホン株式会社のライセンスに基づき使用されている．
＊9 Android™：Google LLCの商標または登録商標．
＊10 FIDO UAF 1.1：FIDO UAF 1.0の拡張版で2016年12月に策定された．「キーの構成証明機能（Key Attestation）」を利用可能で，これにより端末メーカによる機種ごとのカスタム実装なしにFIDO UAFアプリの開発・搭載が可能となる．
＊11 リスト型攻撃：不正に入手したIDとパスワードの一覧を用い，アカウントへの不正アクセスを試みる攻撃手法．

器としての端末の復旧について，ユーザや応対部門にも分かりやすい手段を提供する必要があった．

⑷多様なデバイスへの対応

生体センサを具備しないPCやセットトップボックスなどのデバイスや，2台目のスマートフォンなどからログインや認証を利用するシーンも想定されるため，それらのデバイスからパスワードレス認証を使ってもらうための手段の検討が必要であった．

⑸多数のドコモサービス・アプリへの影響

現在，dアカウントを利用しているすべてのサービス・アプリがFIDO生体認証に対応しているわけではない．また，店頭などの装置でdアカウントのIDとパスワードを入力することを求めるサービスや，dアカウント設定アプリとシングルポイントで連携していないサービス・アプリも存在する．そのため，パスワードを無効化した場合のあらゆる場面での影響を考慮し，認証手段の提供を確保する必要があった．

## 4. 設計・開発と導入

dアカウント パスワードレス認証の実現にあたっては，セキュリティ強化を目的とし，前述した複数の課題を解決しながら，利便性を損なわず，ユーザが簡単に利用できることを念頭に設計した．

### 4.1 全体構想とアーキテクチャ

dアカウント パスワードレス認証は，dアカウントFIDO生体認証のアーキテクチャをベースとして実現することとした．dアカウント設定アプリに新たな設定項目の1つとして，dアカウントのパスワードを無効化できる機能を設ける．ユーザがこの機能を選択することで，dアカウントのオンラインパスワードをサーバ側で一切無効化する．また，合わせてdアカウント設定アプリと連携するサービス・アプリのdアカウント認証画面のすべてでパスワード入力欄を削除することでパスワードレス認証を実現する（**図1**）．

**図1　パスワードレス認証の概要**

dアカウント パスワードレス認証は，最初はドコモ回線のユーザを対象にスタートした．ドコモ回線のユーザはネットワーク暗証番号が利用できるため，本人確認した結果をFIDO認証器（スマートフォンなど）に括り付けることができる．パスワード認証を無効化することで，適切に設定されたFIDO認証器のみを使ってパスワードレスでのログインや本人確認のためのオンライン認証ができることになるため，パスワードを取り巻くセキュリティ課題を解決できる．

## 4.2 パスワードレス認証への移行設定

セキュリティ強化という目的を考慮すると，できるだけ多くのユーザがパスワードの無効化の設定をすることが望ましい．一方，日々使い慣れたパスワードが使えなくなったときのユーザの懸念を考慮し，まずはオプション機能としてオプトイン*12で提供を開始した．

dアカウント パスワードレス認証へ移行するには，dアカウント FIDO生体認証対応機種にプリインストールしてあるdアカウント設定アプリをバージョンアップし，新たに設けたメニュー「パスワード無効化設定」からユーザ自身の操作によってパスワードの無効化をONに設定する．

その際，すでにdアカウント 生体認証を設定しているユーザについては，「パスワード無効化設定」をONにする際に1回だけ生体認証を行えば完了するようにした．また，生体認証を設定していないユーザについては，ネットワーク暗証番号の入力で設定を完了するようにした．このように簡単な操作でdアカウントのパスワードを無効化することができる（**図2**）．

なお，必要に応じてパスワードの無効化をOFFに戻すときには，ONに設定するときと同様にdアカウント設定アプリから切替え可能な仕様とした．

**図2 dアカウント設定アプリの「パスワード無効化設定」と設定時の画面遷移**

*12 オプトイン：ユーザの選択により利用や設定を許可すること．

## 4.3 生体認証が使えない場合への対応

⑴画面ロック解除の活用

生体認証対応端末を持っていても生体センサを利用しないユーザがいること，また指の怪我などで生体センサが利用できない場合を考慮し，生体以外の手段でもパスワードレス認証の実現を検討する必要があった．FIDO認証の特徴はユーザと認証器（スマートフォンなど）の間の本人照合の部分と，公開鍵暗号方式を活用した認証器とサーバ間の検証部分が完全に分離していることである．つまり，FIDO認証器ローカルでの本人照合には生体認証に加えて，本人のみがもつ知識，例えば端末の画面ロック解除で使われるローカルPINなどもFIDO認証に活用することができる．

幸い近年のスマートフォンOSでは端末の画面ロック解除は端末の所有者のみが知る情報としてセキュアに実装されており，かつアプリケーションからも活用可能である．そこで，dアカウント パスワードレス認証では生体認証に加えて，画面ロック解除のためのローカルなPIN／パスコード／パターンでもdアカウントのログインや決済時の本人確認をできるようにする．

なお，dアカウント パスワードレス認証は，前述したようにドコモ回線のユーザへの対応から始めるため，生体認証ができない場合の代替手段としてネットワーク暗証番号を入力して本人確認を行うこともできる．こうした状況から，画面ロック解除によるdアカウント パスワードレス認証は段階的に提供を開始する方針とした．

⑵FIDO UAFからFIDO2[*13]［7］への移行

画面ロック解除を活用した認証を実現するため，Android OS端末向けに提供しているdアカウント設定アプリは，FIDO UAF 1.1からFIDO2へ移行することとした．Android OS 7.0以降のバージョンで標準的に利用できるようになったFIDO2の実装を活用することで，端末の画面ロック解除で用いるローカルなPIN／パスコード／パターンを本人照合の手段として利用することが可能となる（**図3**）．また

**図3 画面ロック解除を用いたdアカウント パスワードレス認証（Android OS端末におけるFIDO2の活用事例）**

＊13 FIDO2：FIDO認証のさらなる普及のため，FIDO認証モデルをプラットフォーム対応させた仕様群．FIDOアライアンスとして策定した機器間連携仕様（CTAP：Client to Authenticator Protocol）とFIDOアライアンスが提案し，W3Cとして策定したWeb認証APIで構成されている．Web認証APIの最初のバージョンは2019年3月に正式に勧告化された．

将来，ドコモの回線契約を持っていないユーザに対しdアカウント パスワードレス認証を提供する場合にも，より多くの端末でFIDO認証が提供可能になる．

Android OSの画面ロック解除でdアカウントによるログインや本人確認をするためには，dアカウント設定アプリをバージョンアップし，FIDO UAF 1.1からFIDO2へ移行する．

移行の操作は単純で，dアカウント認証の動線の1画面で，生体認証に加えて画面ロック解除でもdアカウント認証が可能になることを案内した上で，FIDO2への登録のための操作として指紋センサなどにタッチする．つまり，ユーザはFIDO仕様の違いを意識する必要がない（**図4**）．本機能は2020年5月以降，提供開始予定である．

なお，端末メーカにFIDO認証器として必要な要件を実装するためにAndroid OSを特別にカスタマイズする必要があったFIDO UAF 1.0対応端末については，FIDO2への移行対象外とした．

## 4.4 アカウント再設定と端末紛失時の復旧手段

機種変更をする場合，新しい端末でdアカウントの再設定が必要になる．dアカウント パスワードレス認証を設定済みのユーザはパスワードが無効化された状態であるが，設定のときと同様にネットワーク暗証番号を利用して本人確認を行うことで，再設定を完了することができる．

端末を紛失した場合には，dアカウント FIDO生体認証でも実績がある通り，ドコモの端末紛失時の手続きに従う．すなわち，SIMカードを再発行して新たな端末を準備すれば，上記の再設定と同様にネットワーク暗証番号で本人確認を行ってdアカウント パスワードレス認証を再設定することで復旧できる．

なお，ユーザがドコモ回線を解約した場合には，パスワード無効化設定は自動的にOFFに戻る仕様とした．

FIDO2登録時画面
（ユーザがFIDO仕様の違いを意識する必要はない）

**図4　FIDO UAF 1.1からFIDO2への移行時の画面遷移**

### 4.5 多様なデバイスへの対応

FIDO UAFからFIDO2へ移行することにより，生体認証を使えない場合の代替手段としてだけではなく，生体センサをもたない機種でも画面ロック解除を利用することでdアカウント パスワードレス認証を利用できるようにした．

PCやテレビ，セットトップボックスなど生体センサの搭載されていないデバイスでログインするユースケースには，既述のスマホ認証の仕組みをdアカウント パスワードレス認証にも応用した．すなわち，あらかじめ設定をしておくことで，PCやセットトップボックスなどの周辺デバイスで提供するサービス・アプリでdアカウント認証ボタンを選択すると，パスワードレス認証設定済みのスマートフォンに認証要求を通知するようにした．そして，そのスマートフォンでパスワードを入力することなく，生体認証や画面ロック解除で簡単に認証することができる（**図5**）．あらかじめ必要な設定においては，第三者のなりすましによる認証要求を防ぐための工夫をしている．

パスワードレス認証（パスワード無効化）設定済みのdアカウントは，マルチデバイスでの認証にも対応する．つまり，ユーザが複数の回線を持つ場合，それらに1つのdアカウントを紐づけることができる．そのため，ユーザが所持する回線数に応じたFIDO認証器を設定可能であり，どちらの端末でもdアカウント パスワードレス認証をすることができる．

### 4.6 多数のドコモサービス・アプリへの対応

dアカウント パスワードレス認証の企画に際して網羅的な確認を行った結果，dアカウント設定アプリとシングルポイントで連携していないサービ

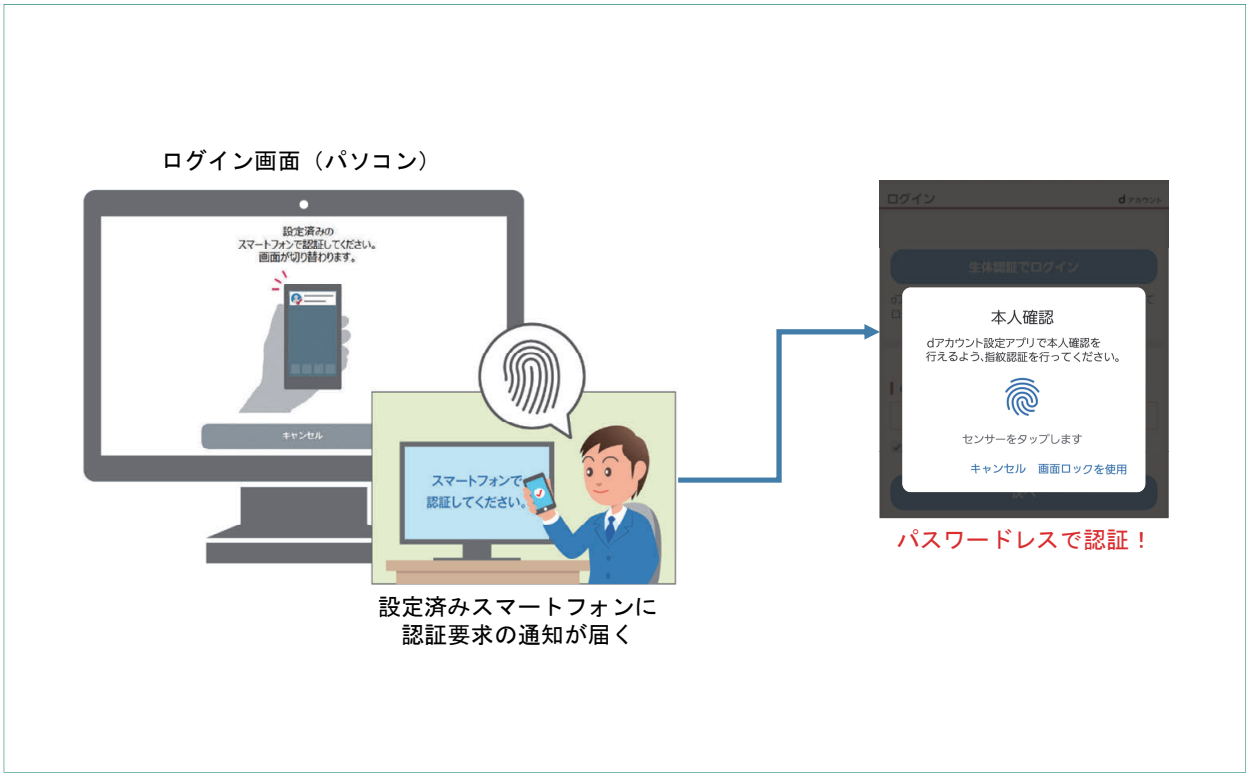



図5　パソコンからdアカウント パスワードレス認証

ス・アプリが一定数あることが分かった．この解決のため，スマホ認証の仕組みを応用した．

すなわち，それらのサービス・アプリでパスワードレス認証が必要なシーンを生体センサが搭載されていないデバイスで認証が必要なユースケースと捉える．そして，それらのサービス・アプリでdアカウント認証ボタンを選択すると，dアカウントパスワードレス認証を設定済みであるそのスマートフォンに認証要求を通知することで，スマートフォンにパスワードを入力することなく，認証することができる．

いくつかの特定の装置でdアカウントのID・パスワードを入力して認証している場面があることも分かったが，この新しいスマホ認証の仕組みで同様に解決を図った．

## 5. 今後の展望

今回，提供を開始したdアカウント パスワードレス認証は，FIDO認証の特長を活かしてセキュリティ強化につなげる取組みの第一歩である．

現在のdアカウント パスワードレス認証は，dアカウントをより安心して利用するためのオプション機能であり，dアカウントのパスワードが存在する状態からパスワードを無効化する仕様となっている．将来的には，dアカウントを新規作成する段階からパスワードレスとする機能を提供し，オプション機能としての提供ではなく，デフォルトでの提供も視野に入れている．

また，ドコモのサービスの多くはドコモの回線契約を持たないユーザにも提供している．このようないわゆるキャリアフリーのユーザもdアカウントをさまざまな用途で利用しているため，dアカウントパスワードレス認証のキャリアフリー対応についても検討している．

このような複数のアプローチで，より多くのユーザにあんしんでもっと便利なdアカウント パスワードレス認証を提供する取組みを継続していく予定である．

## 6. あとがき

本稿では，dアカウント FIDO生体認証の導入背景と概要を述べ，パスワードレス認証の実現にあたっての課題，設計・開発と導入の詳細について解説し，今後の展望について述べた．

dアカウント パスワードレス認証の導入により，ドコモはこれまで当り前であったIDとパスワードのあり方を根本から変える．既存のアセット＊14を十分に活用することで，利便性を損なうことなく，幅広いユーザがより安心してdアカウントを利用するための機能を提供開始することができた．第三者による不正アクセスや不正決済などのニュースが後を絶たない昨今，FIDO認証への注目度も年々増してきている．ドコモは今後もFIDO認証を積極的に活用した先進的な端末の提供とサービス展開を通じて，「パスワードのいらない世界」の実現をめざしていく．

### 文　献


[1] 森山 光一：“パスワードのいらない世界へ：NTTドコモにおけるFIDO（ファイド）標準を活用したdアカウント生体認証の取組みと将来展望，”電気通信，Vol.80，No.840，pp.13-19，Jan. 2017.

[2] NTTドコモ：“dアカウントログイン等のオンライン認証にTouch IDが対応．”
https://www.nttdocomo.co.jp/info/notice/pages/160307_00.html

[3] 森山，ほか：“FIDOアライアンスにおけるオンライン認証の標準化動向とドコモの貢献，”本誌，Vol.28，No.1，pp.22-32，Apr. 2020.

[4] M.Hata and R.Lindemann：“FIDO Alliance White Paper：Hardware-backed Keystore Authenticators (HKA) on Android 8.0 or Later Mobile Devices,” Jun. 2018.
https://fidoalliance.org/wp-content/uploads/Hardware-


＊14 アセット：保有する有用な資産や資材，利点のこと．

backed_Keystore_White_Paper_June2018.pdf
［5］ FIDO Alliance：“First FIDO UAF 1.1 Implementations Ease Deployment of Advanced Biometric Authentication on Android Devices,” Dec. 2017.
https://fidoalliance.org/first-fido-uaf-1-1-implementations-ease-deployment-advanced-biometric-authentication-android-devices/
［6］ FIDOアライアンス：“FIDO（ファイド）UAF 1.1の初実装が登場，Androidデバイスへの先進的生体認証の導入が容易に ～ドコモ スマートフォン Xperia™の二機種が市場初の対応デバイスに～,” Dec. 2018.
https://prtimes.jp/main/html/rd/p/000000006.000029122.html
［7］ W3C：“W3CとFIDO Alliance - パスワード不要の安全なログインが勧告化に,” Mar. 2019.
https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.ja

Standardization（特集）

FIDO認証　セキュリティ　公開鍵暗号方式

パスワード課題を解決するFIDO（ファイド）認証特集

# FIDOアライアンスにおけるオンライン認証の標準化動向とドコモの貢献

プロダクト部　森山 光一（もりやま こういち）　富山 由希子（とみやま ゆきこ）
牧野 由樹子（まきの ゆきこ）

FIDO®＊1（ファイド）アライアンスは，オンライン認証におけるセキュリティと利便性の両立をめざし，ID・パスワードに代わる新しい認証方式を提唱するグローバルな非営利団体である．ドコモは2015年からボードメンバーとして加入し，FIDO仕様策定とエコシステムの発展に貢献している．本稿では，FIDOアライアンスとFIDO認証について解説する．また，ドコモの貢献と国内外におけるFIDO認証の広がりを紹介し，今後を展望する．

## 1. まえがき

FIDOとはFast IDentity Onlineの略称で，FIDOアライアンスが提唱するオンライン認証方式のモデルとそれに基づく仕様群を指している．この認証モデルの特徴は，ID・パスワードに代わり公開鍵暗号方式＊2を活用することで，「共有の秘密」に依存しない認証方式としていることである．そして，FIDO認証モデルに生体認証などを組み合わせることで，シンプルで堅牢なオンライン認証を実現し，セキュリティと使い勝手の良さの両立をめざしている［1］．

近年，キャッシュレスによる決済やその他さまざまな場面でオンライン認証の必要性が増している一方，不正アクセスや不正決済などに関するニュースが後を絶たず，使い勝手を確保したまま安全に認証できる手段の提供がますます重要になっている．そのような中，ドコモは2020年3月からdアカウント®＊3パスワードレス認証の提供を開始した．これは，2015年5月から提供しているdアカウントFIDO生体認証［2］の十分な広がりをベースとして，全面的にFIDO認証に移行するオプション機能をお客様に提供することで，より安心してオンライン認証を使っていただくものである［3］．

この実現は，単にFIDO認証を技術の1つとして採用したというものではない．まず，商用サービスの提供開始当初から，FIDO認証の特長を最大限活

©2020 NTT DOCOMO, INC.
本誌掲載記事の無断転載を禁じます．
本誌に掲載されている社名，製品およびソフトウエア，サービスなどの名称は，各社の商標または登録商標．

＊1　FIDO®：FIDOおよびFIDO AllianceロゴはFIDO Allianceの商標または登録商標．
＊2　公開鍵暗号方式：秘密鍵と公開鍵のペアを用いる非対称な暗号方式．秘密鍵は安全に保持する必要があるが，公開鍵は秘匿する必要がなく，共通鍵暗号方式と異なる特徴をもつ．
＊3　dアカウント®：㈱NTTドコモの登録商標．

用した．そして，FIDOアライアンスにボードメンバーとして加入した上でその経験をフィードバックし，FIDO認証の可能性をさらに探求し，FIDOアライアンスにおける標準化活動において貢献してきたことで成し遂げることができたものである．また，結果として，国内外においてより広くFIDO認証が使われ始めていることについても注目いただきたい．

本稿では，FIDOアライアンスとFIDO認証について解説し，ドコモの貢献と国内外におけるFIDO認証の広がりを紹介し，今後を展望する．

## 2. FIDOアライアンスとFIDO認証

### 2.1 FIDO認証モデル

FIDO認証モデルは，セキュリティと使い勝手の両立を実現するため，公開鍵暗号方式を活用したオンライン認証のための新しいモデルである．FIDO認証モデルでは，FIDO認証器（以下，認証器）によってユーザが認証器の所有者であることをローカル検証する部分と，公開鍵暗号方式に基づく秘密鍵と公開鍵のペアを使った署名検証によってオンライン認証を成立させる部分に分離している（**図1**）．

認証に際しては，あらかじめ設定が必要である．設定では，まず認証に必要な秘密鍵と公開鍵のペアを認証器で生成し，秘密鍵を認証器に格納し，公開鍵を認証サーバ（以下，サーバ）に登録する（**図2**(a)）．登録要求に対しては，まずサーバから認証器にチャレンジコード（ランダムな文字列）が送られる．そして，認証器で鍵ペアを生成して秘密鍵を認証器の安全な領域に格納した上で，秘密鍵で署名したチャレンジコードと公開鍵をサーバに送信する．チャレンジコードを使うのは，サーバと認証器のや

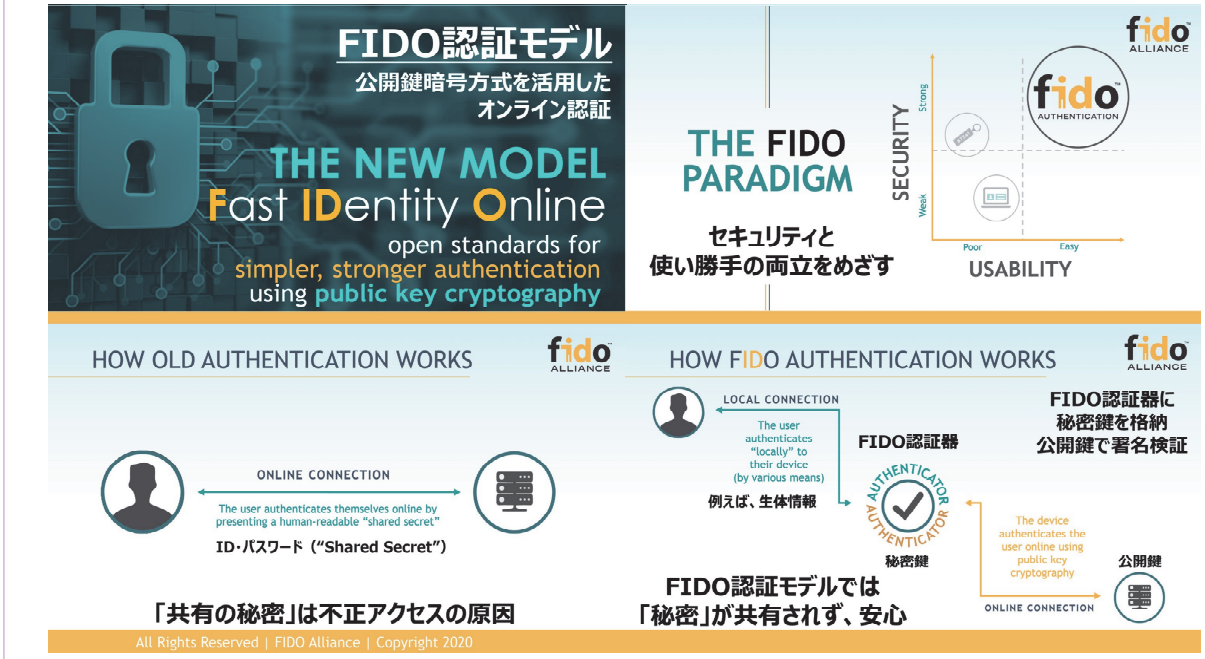



図1　FIDOアライアンスの目標とFIDO認証モデル

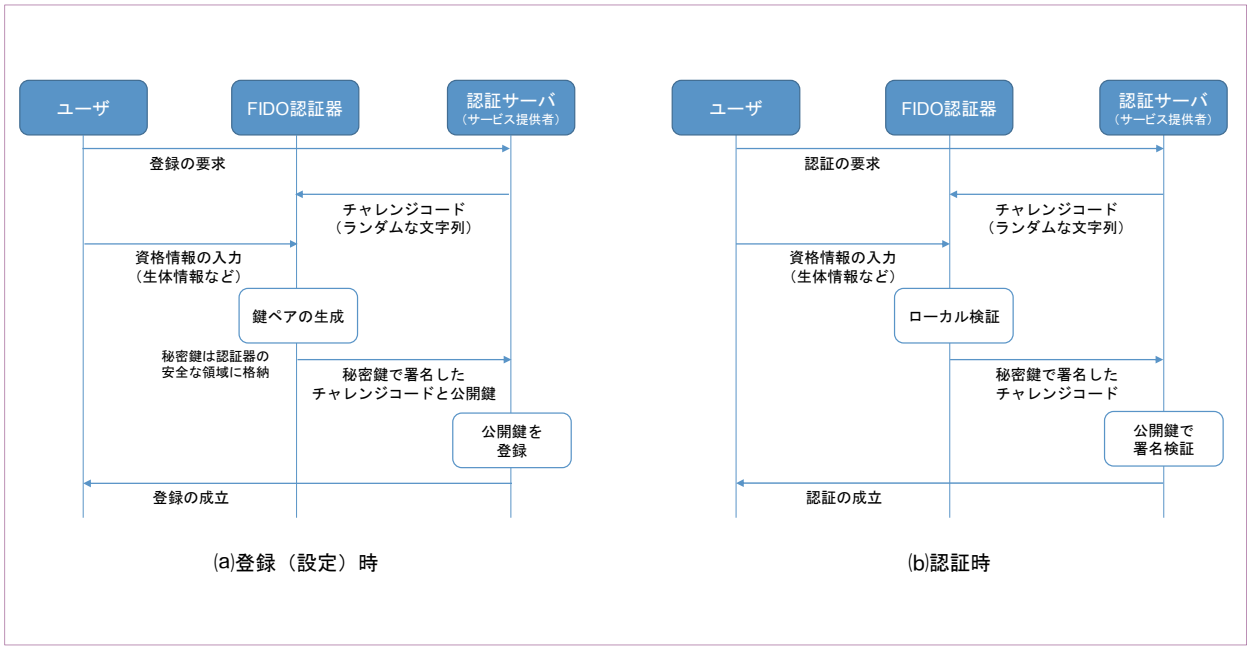



**図2　FIDO認証の流れ（「秘密」がインターネットを通過しない）**

りとりが対になっていることを担保するためである．

ユーザからの認証要求に対しては，まずサーバから認証器にチャレンジコードが送られる．次に，生体情報や端末ローカルでのみ有効な知識情報（例えば，パスコード）などの資格情報で認証器のユーザを検証する．検証できた場合には，秘密鍵でチャレンジコードに署名し，サーバに返却する．そして，サーバでは署名されたチャレンジコードをペアとなる公開鍵で署名検証し，検証できた場合にオンライン認証が成立する（図2(b)）．

このように，FIDO認証モデルでは従前のID・パスワードを使った認証と異なり，ユーザ・認証器とサーバとで「秘密」が共有されず，パスワードのような「共有の秘密」がインターネットを通過することもない．そのため，フィッシング耐性があり，異なるサービス提供者に対する認証のための操作も，指紋をかざすなどの動作のみで同一にできるという特長がある．すなわち，シンプルで堅牢なオンライン認証を実現することが可能である．

## 2.2　FIDOアライアンス

FIDOアライアンスは，2012年に設立されたパスワード課題の解決に注力するグローバルな非営利団体である．FIDO認証モデルに基づく技術仕様の策定，相互運用性を確保するための認定プログラムの運営，そして各標準化団体との協業などを通じたFIDO認証の導入推進を行っている．さまざまな業界から現在約250社が参画し，業界の垣根を超えるコンソーシアムとなっている（**図3**）．

(1)メンバーシップ

FIDOアライアンスには，年会費とベネフィットの違いに応じて，ボードメンバー，スポンサーメンバー，アソシエイトメンバー，ガバメントメンバーと4つのメンバーシップのレベルと区別がある．これらのうち，FIDOアライアンスで特にリーダーシップを発揮できるのがボードメンバーである．

ボードメンバーは，FIDOアライアンスにおける意思決定に参加する権利をもつ．すなわち，ボード会議への参加，新たな戦略やその遂行に必要な作業

図3　FIDOアライアンスのボードメンバー

部会（WG：Working Group）の設置など各種提案のボード会議への付議，そして意思決定のための投票権をもつ．また，FIDOアライアンスとボード会議を代表する執行評議会（Executive Council）のメンバー，および作業部会の座長・共同座長として選出され，定められた任期を務めることを権利としてもつ．さらに，マーケティング活動に優先的に参加できる権利などをもつ．

ドコモは，FIDOアライアンスに加入した2015年5月からボードメンバーである．

⑵作業部会

FIDOアライアンスの日々の活動は，主にそれぞれの役割を担った作業部会によって推進されている．現在，FIDOアライアンスには15の作業部会がある．作業部会の種類には，FIDO認証の技術仕様，セキュリティ要件，認定プログラム仕様などを定める技術作業部会（Technical WGs），FIDO認証の導入・展開を推進する作業部会（Adoption WGs），そしてFIDOアライアンスのミッションを国・地域ごとに効果的に実行することを目的とした作業部会（Regional WGs）の3つがある．

ドコモが座長・共同座長を務めている，または務めてきた作業部会は下記の通りである．

・コンシューマー・デプロイメント作業部会（Consumer Deployment WG）
・セキュリティ・プライバシー要件作業部会（Security and Privacy Requirement WG）
・日本作業部会（FIDO Japan WG）

## 2.3　FIDO仕様

FIDO認証モデルを実装可能にするFIDO仕様には，2014年12月にそれぞれバージョン1.0として仕

様を公開したFIDO UAF（Universal Authenticator Framework）とFIDO U2F（Universal Second Factor），そして2018年から積極的に展開しているFIDO2がある（**図4**）．

・FIDO UAF：パスワードレス認証のために設計した仕様
・FIDO U2F：2段階認証の2要素目のために設計した仕様
・FIDO2：FIDO UAFとFIDO U2Fのそれぞれの特長を活かし，FIDO認証をより広く展開するため，OS・ブラウザなどのプラットフォームに組み込みやすくするために設計した仕様

FIDO仕様策定におけるドコモの貢献の1つに，FIDO UAF 1.1がある．これは，ドコモがdアカウント認証にFIDO UAF 1.0をいち早く採用して商用導入した経験をフィードバックし，Android™[*4] OS 8.0以降に搭載された「キーの構成証明機能（Key Attestation）」を活用することで，端末メーカによる機種ごとのカスタム実装なしに，FIDO UAFアプリの開発・搭載を可能にしたものである．2017年11月に商用導入を開始し，同年12月に発表した．これは，FIDO2の離陸を待たずにFIDO認証を普及させる一助となった．

⑴FIDO2とWeb認証

FIDOアライアンスは，FIDO認証のさらなる展開に向けて，OS・ブラウザなどのプラットフォーム対応が不可欠と判断した．そこで，ブラウザでの対応のためにはW3C®（The World Wide Web Consortium）[*5]での標準化が必須であることから，2015年11月にFIDOアライアンスからW3CにWeb部分の基本仕様（案）を提供し，リエゾンパートナーとして連携して標準化することに貢献した．そして，W3CとしてFIDO認証モデルをWebブラウザで提供

**図4　FIDO認証モデルに基づくFIDO仕様群**

＊4　Android™：米国Google LLCの商標または登録商標．

＊5　W3C®：Web技術の標準化を進める国際機関．The World Wide Web Consortiumの略称であり，商標または登録商標．

するためのJavaScript*6 API（Application Programming Interface）*7（Web認証）を標準化し，2019年3月にLevel 1として正式勧告とした．現在，主要なブラウザがWeb認証Level 1に対応し，W3CではLevel 2の策定が進んでいる［4］［5］．

ブラウザでWeb認証を提供する場合にも，ユーザは認証器の利用が必要になる．この認証器としてはブラウザが動作する端末に組み込まれたプラットフォーム認証器，またはUSBなどを介して接続する外部認証器（いわゆるセキュリティキーなど）を使うことができる．後者を実装可能とするためFIDOアライアンスとして策定したのがCTAP（Client to Authenticator Protocol）（デバイス間連携仕様）である．このCTAPはFIDO U2F仕様の該当部分を継承して策定された．

⑵国際標準化

FIDOアライアンスでは国際標準化団体との連携も進めており，その成果の1つとして，認証器の実装に必要なFIDO UAFとCTAPは，2018年12月に国際電気通信連合（ITU：International Telecommunication Union）の電気通信標準化部門（ITU-T：ITU Telecommunication Standardization Sector）によって，国際標準として以下の通り採択された．

・ITU-T勧告X.1277 - FIDO UAF 1.1
・ITU-T勧告X.1278 - FIDO2 CTAP（U2F CTAP1含む）

### 2.4 認定プログラム

FIDOアライアンスは，FIDO認証に対応する製品のFIDO仕様への適合性を検証し，主に製品とサービス間で相互運用性を確保するための認定プログラム制度を設けている．認定を受けた企業は，FIDO認定ロゴを製品に付与することができる．FIDO認定プログラムは，FIDOアライアンスに加入していない企業・団体でも参加することが可能である．

相互運用性を確保するための認定プログラムには，認証器とサーバの機能に関して開発者が自ら実施する適合性（Conformance）テスト，FIDOアライアンス主催としてFIDOアライアンスメンバー企業がホストとして実施する相互接続性（Interoperability）テスト，そして第三者ラボによって検証する認証器のセキュリティ認定がある．

認証器のセキュリティ認定では，後述するセキュリティ・プライバシー要件作業部会が定めるセキュリティ要件（L1，L1＋，L2，L2＋，L3，L3＋の6段階）の適合性を検証しており，L1認定の取得は必須，L1＋～L3＋認定の取得はオプションである．2018年からは生体センサの性能に関するバイオメトリック部品認定プログラム（オプション）も開始している．

ドコモは，2015年4月にカリフォルニア州サンノゼで開催された第1回相互接続性テストに参加し，2015年5月のFIDO UAF 1.0を採用したdアカウントFIDO認証の提供開始当初からFIDO認定を取得した端末で商用サービスに対応することができた．また，その経験を踏まえ，カリフォルニア州パロアルトに拠点を持つDOCOMO Innovations, Inc. でFIDO認定プログラム黎明期の相互接続性テストをホストし，そのフィードバックで貢献している．

2019年11月には，国内で初めて相互接続性テストが開催され，10の国・地域から14の企業が参加し，国内から新たに3製品がFIDO認定を取得した．

## 3. ドコモのFIDOアライアンスにおける貢献

現在，ドコモはFIDOアライアンスにおいて複数の役割を果たしている．1つはボードメンバー企業としての役割である．FIDOアライアンスにおけるボード会議はその意思決定を担っており，ドコモはその一員である．

＊6 JavaScript：Webブラウザなどでの利用に適したスクリプト言語．JavaScriptは，Oracle Corp. およびその子会社，関連会社の米国およびその他の国における登録商標または商標．
＊7 API：OSやミドルウェアなどが提供する機能を，他のアプリケーションソフトウェアが利用するためのインタフェース．

また，ボードメンバー企業であることから可能な役割として，ドコモは複数の作業部会の設立に貢献するとともに，座長・共同座長を務め，リーダーシップを発揮している．また，ボード内に設置されている複数の委員会（Board Committees）で委員も務めている．そして，ボードメンバー企業の代表者から選出された7名のメンバーで構成される執行評議会メンバーの一員としても2019年から推挙され，大切な役割を果たしている．

さらに，特筆すべきは，FIDO認証の特長を積極的に活かしたドコモにおける導入と，さまざまなチャネルを通じたFIDOエコシステム*8へのフィードバックと考える．

## 3.1 座長・共同座長を務める作業部会での貢献

⑴コンシューマー・デプロイメント作業部会（Consumer Deployment WG）

ドコモは，FIDOアライアンスに加入後2度めのボード会議（2015年6月）にて，ドコモにおけるFIDO導入事例の紹介とそれを通じて認識した主な課題に関するプレゼンテーションを行った．その結果，FIDO認証をより広く導入推進していくための作業部会の設置について機運が高まり，FIDOアライアンスにとって初めてのAdoption WGとなるD@S WG（Deployment-at-Scale WG）の設置を提案し，ボード会議での議論と承認の結果，起案者のドコモが座長を務めることになった．

設置当初においては，FIDO認証の導入事例がまだ少なく，並行して検討が進む当時のFIDO2の将来性を支持しつつ，認証モデルは同一ながらも，異なる複数のFIDO仕様間の差異とは独立する課題の解決とFIDO UAF・U2Fのさらなる展開の可能性を模索した．その1つとして，D@S WG座長として，韓国で進みつつあった導入事例をホワイトペーパーとしてまとめる作業を推進した［6］．また，のちに国内大手銀行でFIDO認証の採用につながる活動を行った．さらに，前述したFIDO UAF 1.1の基礎となる考えをまとめ，FIDOアライアンスのボードメンバーでもあるパートナー企業とともにホワイトペーパーを執筆し，公開した［7］．

こうした活動を通じて，現在では一般消費者向け，法人ビジネス向け，そして政府系機関向けにそれぞれ作業部会を分化して活動することがより効果的との段階に至り，ドコモはコンシューマー・デプロイメント作業部会での活動に注力している．

・アカウントリカバリー

近年取り組んでいるテーマの1つに，アカウントリカバリーと呼ばれる課題がある．これは，ユーザが認証器を紛失したとき，「共有の秘密」をもたない条件下で，どのように新しい認証器に秘密鍵を再設定することができるのかという課題である．

この課題に対してドコモは，dアカウントのFIDO生体認証の導入に際して，電気通信（携帯電話）事業者として，携帯電話不正利用防止法への順守などのため従前から保持していた「本人確認」に必要な事業基盤を活用し，初期設定と端末紛失時の対応を当初から確保している．また，dアカウント パスワードレス認証においてもその基盤を活用している．しかし，ドコモとして回線契約の有無にかかわらない「会員基盤」を軸とした事業運営を推進するにあたり，回線契約の無いお客様に対しても適切なアカウントリカバリーの手段を提供することが重要であり，業界とFIDOエコシステム共通の課題として，解決に向けて取り組んでいる．

ドコモはコンシューマー・デプロイメント作業部会での活動を通じて，アカウントリカバリーに関するホワイトペーパーのとりまとめで貢献し，引き続き活動をリードしている．

⑵セキュリティ・プライバシー要件作業部会（Security and Privacy Requirements WG）

セキュリティ・プライバシー要件作業部会は，ク

*8 エコシステム：複数の企業が連携して，お互いの技術や資産を活かし，社会を巻き込んで，技術開発から導入へと普及にいたる一連の流れを形作る共存共栄の仕組み．

レジットカード事業を営むボードメンバー企業の提案でセキュリティ要件作業部会として発足し，共同座長にプラットフォームチップセットベンダのセキュリティ専門家が加わって運営されてきた．

ドコモは，dアカウント FIDO認証の提供開始当初からドコモ スマートフォン（Android）における生体情報と秘密鍵の格納および生体情報の照合動作に端末上の安全な特別領域，例えばTEE（Trusted Execution Environment）を活用し，プライバシー情報の漏洩対策を重視した実装を要件化していた．この要件には，生体センサから安全な特別領域までの生体情報の伝送に関することも含まれる．

そのため，FIDOアライアンスにおけるセキュリティとプライバシー保護に関する認定プログラム強化に向けた正式な要件化に際しては，その経験を積極的にフィードバックした．そして，関係者で議論を深め，現在の6段階に分類されたセキュリティ要件の骨子が固まった．

なお，2018年7月から2020年3月までは，ドコモが共同座長としてそのファシリテーションでも貢献した．

⑶日本作業部会（FIDO Japan WG）

2015年に日本でFIDOアライアンスに参画する企業が集まり，FIDOアライアンスとしてのFIDO認証の普及活動を開始した．翌年の2016年12月には，FIDOアライアンスのミッションである，「パスワードに代わるシンプルで堅牢なFIDO認証モデルの展開・推進」を日本国内でより効果的に実践することをミッションとして，11社で日本作業部会を発足することを発表した．現在では45社が参加し，FIDOアライアンスで最も多くのメンバーが参加する作業部会となっている．

ドコモは発足時から座長を務めており，国内におけるFIDO認証のプレゼンス向上と普及に微力ながら貢献している．国内に事業拠点をもつ国内外のFIDOアライアンスメンバー企業ならびに関係者の方々の多くのご協力によって活動を推進できており，グローバルなアライアンスにおいて日本から世界に向けて貢献する1つのかたちとして成り立ちつつある．ご協力をいただいているすべての方々にこの場を借りて深くお礼を申し上げたい．

なお，日本作業部会としての活動とその成果は，プレスリリースや発表資料で公開しており，発足以来，毎年記者説明会・記者発表会の開催を通じて多く記事にしていただいているので，ここではその活動の詳細は，割愛する［8］［9］．

## 3.2 FIDO認証を活用しての貢献

FIDOアライアンスにおける活動を通じての貢献に加えて，ドコモでは端末からサービスまでトータルでFIDO認証の特長を積極的に活用し，その経験をフィードバックすることでFIDOアライアンスとそのエコシステムに貢献している．

⑴さまざまな生体センサの活用

ドコモにおいて，FIDO認証を採用したきっかけの1つは，お客様により魅力的な端末を提案するところにあった．当時，ドコモではdアカウント（当時のdocomo ID）以外にも多くのパスワードをお客様にご利用いただいており，より便利な認証手段として生体認証について検討を進めていた．そのような中，世界初の虹彩認証搭載スマートフォンARROWS NX（F-04G）（製造：富士通株式会社）を含む2015年夏モデルの企画において，FIDO認証はユーザ検証のための生体センサの種類を問わないという特長を活かし，メーカ・機種ごとに異なる種類の生体センサを搭載することができた．なお，搭載にあたっては，生体センサに求める性能とセキュリティ＆プライバシー保護の要件定義とその実現，そして継続性の確保には万全を期した．

その後，複数の端末メーカから装置として虹彩・指紋と複数のセンサを搭載可能なスマートフォンの提案を受け，FIDO UAF仕様を改めて振り返り，

その解釈と実装上の工夫により，ドコモとして新しいdアカウント設定アプリを開発し，お客様が意識することなく虹彩と指紋のどちらでも認証できる機能の提供も行った．

⑵オープンな標準技術であることの活用

オープンな標準技術である特長を活かし，異なる認証器の実装を受け入れた．これにより，（FIDO UAF 1.1に移行する前の）FIDO UAF 1.0準拠のドコモ スマートフォン（Android）全36機種を製造した7メーカで5つの異なる実装に分かれたが，いずれもFIDO認定を取得することにより相互運用性があることを確認しており，機能・サービス提供上も問題は発生していない．もちろん，その後のFIDO UAF 1.1に基づく実装においても相互運用性を確保している．今後導入予定のFIDO2についても，問題ないものと考えている．

⑶ID連携との親和性の良さの活用

FIDO認証は，OpenID® Connect*9などのID連携技術と親和性が良い．そこで，ドコモではdアカウントのOpenID Connect対応により，ドコモのパートナー企業におけるIDと連携し，パートナー企業が提供するサービスサイトへのログインなどにおいても，dアカウント FIDO生体認証が利用可能となっている．

⑷「共有の秘密」に依存しない認証方式の最大活用

ドコモとしてFIDO認証の採用当初からその実現を構想していたのが，FIDO認証への全面的な移行を見据えた機能提供である［2］．すなわち，dアカウントパスワードレス認証は「共有の秘密」に依存しないFIDO認証方式の特長を最大限に活用するものである．詳細は本特集の別記事を参照されたい［3］．

## 4. 国内外におけるFIDO認証の導入状況と広がり

dアカウント FIDO生体認証の提供開始は，通信事業者として，また虹彩認証を含む複数のメーカによるFIDO認定端末によるものとして世界初であった．当時は，FIDO認証が商用導入された事例は世界的にみても，FIDO UAF 1.0に先立つFIDO Ready仕様*10に基づくSamsungとPayPalによる事例などに限られ，決して多くはなかった．しかし，現在では国内外を問わず，広くFIDO認証が使われるようになってきている．

### 4.1 国内におけるFIDO認証の導入状況

国内では，2017年10月の大手銀行におけるFIDO認証による生体認証でのログイン機能提供開始をきっかけとして，金融機関，通信事業者，インターネットサービス事業者，そしてエンタープライズ向けと，FIDO認証の実際の活用が急速に増えている．

具体的には，FIDO UAFについてはその利用・提供開始時期の順にNTTデータ（社内向けモバイルアプリ），みずほ銀行，ソフトバンク，三菱UFJ銀行，アフラック，NTTコミュニケーションズ（SSO（Single Sign On）サービス*11），テプコシステムズ（社内向けシステム），ゆうちょ銀行などに導入された事例がある．また，FIDO2についてはヤフー（Yahoo! JAPAN ID），インターナショナルシステムリサーチ（SSOサービス），LINE Payなどに導入された事例がある．その他，FIDO U2Fの活用事例も含めると，国内でFIDO認証が実際に活用されている事例は多数に及ぶ．

これらの中には，FIDO2の活用で世界初の事例も複数含まれ，日本はFIDOエコシステムの発展でリーダーシップを発揮している国と地域の1つと言える．

### 4.2 海外におけるFIDO認証の導入状況

海外では，ドコモのFIDO認証提供開始からまもなく北米でBank of AmericaがFIDO UAFを活用したサービスを提供開始した．ドコモとBank of Americaは早い時期からAndroidとiOS*12の両方に

＊9 OpenID® Connect：OpenID Foundationが策定するID連携のためのプロトコル．OpenIDはOpenID Foundationの商標または登録商標．

＊10 FIDO Ready仕様：FIDO UAF 1.0が公開される前に，FIDO認証の先行商用を可能とするために策定された仕様．

＊11 SSOサービス：あらかじめID連携しておくことで，あるIDにログインすることで複数のIDにログインできるサービス．

対応したFIDOアライアンスのボードメンバー企業である．また，韓国ではFIDO Korea WGの共同座長を務めるSamsung，BC Cardらがリーダーシップを発揮し，日本と同様に早い時期からFIDO認証が広く使われてきた．

⑴北　米

Google社内で，FIDO認証に基づくTitan Security Keyを活用することで不正ログインを防止できたことが広く知られるようになった．

また，先ごろ，米Intuit社がSMS OTP（One Time Password）[*13]からFIDO認証に移行したことによる効果をFIDOアライアンスメンバーとしてケーススタディとして発表した［10］．これによれば，FIDO認証はユーザ体験の観点からログインに掛かる時間を約20％にまで短縮し，認証の成功率の改善も図っている．

さらに，米国連邦調達庁（GSA：General Services Administration），すなわち米国の公務員，連邦政府職員向けのSSOサービスのためのWebサイトがWindows Hello[*14]とセキュリティキーを使ったFIDO認証に対応したとのことである．

このように，北米でFIDO認証の利用シーンが広がっている．

⑵欧　州

欧州では，欧州一般データ保護規則（GDPR：General Data Protection Regulation）[*15]が施行された．GDPRにおいて，生体情報はもっとも高レベルなプライバシー情報であるため，生体情報を認証器の安全な領域に格納するFIDO認証に期待がある．また，金融・決済の領域で近く施行されるとみられる欧州決済サービス指令（PSD2：Payment Services Directive II）[*16]で2要素認証が必須となり，その対応でFIDO認証の採用が検討されている．

一方，英国の国民保健サービス（NHS：National Health Service）で，開発者がアプリのログインにFIDO生体認証を使えるようにするためのオープンソースをリリースしたとのニュースもある．

欧州で，FIDO認証の利用に期待が高まっている．

⑶アジア・パシフィック

アジア・パシフィックは，世界の中でもFIDO認証の活用が先行している地域であり，日本と並び，韓国と台湾でFIDO認証が広く利用されている．

韓国では，銀行などの金融機関で広くFIDO認証が使われている他，国民IDに対応するK-FIDO［6］の対応により，さまざまなシーンでFIDO認証が使われている．また，台湾ではPKI（Public Key Infrastructure）[*17]ベースのMOICAと呼ばれる市民IDにTAIWAN FidOとしてFIDO認証に対応した．

FIDOアライアンスはAPKIC（Asia PKI Consortium）とリエゾンパートナーとして連携もしており，アジア・パシフィックでは国民・市民IDへのFIDO認証の対応事例が特徴的である．

## 5. あとがき

本稿では，FIDOアライアンスとFIDO認証について解説し，ドコモの貢献と国内外におけるFIDO認証の広がりを紹介した．

ドコモにおけるFIDO認証の取組みの第一歩は，米Nok Nok Labs社との2014年6月のシリコンバレーでの打合せにさかのぼる．Nok Nok Labsは，FIDOアライアンスの創設メンバー6社のうちの1社である．ドコモは，dアカウント FIDO認証の提供開始当初からFIDO認証サーバの提供を受けており，2015年5月の運用開始以来一度も障害なく運転を続けている．

パスワード課題はデジタルトランスフォーメーション[*18]時代において解決すべき社会的な問題の1つであり，ドコモ1社のみで解決できることではない．「共有の秘密」に依存しない認証方式を提唱するFIDOアライアンスは，Nok Nok Labsのような認証とセキュリティ技術に特化した企業も，Google

＊12 iOS：「IOS」は米国およびその他の国におけるCisco社の商標または登録商標であり，ライセンスに基づき使用されている．
＊13 SMS OTP：SMS（ショートメッセージサービス）で配信されるワンタイムパスワード．
＊14 Windows Hello：米国Microsoft Corp.の米国およびその他の国における登録商標または商標．
＊15 欧州一般データ保護規則（GDPR）：EU加盟国および欧州経済領域で適用される個人情報の取扱いに関する保護規則．個人情報の取得や移動にも適用される．
＊16 欧州決済サービス指令（PSD2）：EU域内における安全で便利な電子決済を実現するための規則．インターネットやモバイルでの新しい決済サービスが考慮されている．

やMicrosoftのような大手のOS・プラットフォーム企業も集まる，企業の規模を問わず，ビジネス領域の垣根を超えて，まさにダイバーシティ＆インクルージョンを体現する業界の連携であり，ドコモがその中で役割の一端を微力ながらも担うことができていることは望外の喜びである．

引き続き，ドコモにおけるdアカウント パスワードレス認証の取組みを進めながら，FIDO認証とそのエコシステムの発展に貢献できればと考えている．

## 文　献


［1］ FIDOアライアンス ホームページ．
https://fidoalliance.org/

［2］ 森山 光一：“パスワードのいらない世界へ：NTTドコモにおけるFIDO（ファイド）標準を活用したdアカウント生体認証の取組みと将来展望，”電気通信，Vol.80，No.840，pp.13-19，Jan. 2017.

［3］ 尾崎，ほか：“ID・パスワードのあり方を変えるdアカウントパスワードレス認証，”本誌，Vol.28，No.1，pp.11-21，Apr. 2020.

［4］ W3C Recommendation：“Web Authentication：An API for accessing Public Key Credentials Level 1，”Mar. 2019.
https://www.w3.org/TR/webauthn/

［5］ 松浦 由美子，田中 清，藤村 滋，森山 光一：“W3C TPAC2019@FUKUOKAでの活動，”NTT技術ジャーナル，Vol.32，No.1，pp.72-74，Jan. 2020.

［6］ FIDO Alliance：“FIDO Alliance White Paper：Korean FIDO Deployment Case Study Accredited Certification System for Safe Usage of Accredited Certificate using FIDO in Smartphone in Korea (K-FIDO)，”Sep. 2017.
https://fidoalliance.org/white-paper-korean-fido-deployment-case-study-accredited-certification-system-for-safe-usage-of-accredited-certificate-using-fido-in-smartphone-in-korea-k-fido/

［7］ FIDO Alliance：“FIDO Alliance White Paper：Hardware-backed Keystore Authenticators (HKA) on Android 8.0 or Later Mobile Devices，”Jun. 2018.
https://fidoalliance.org/white-paper-hardware-backed-keystore-authenticators-hka-on-android-8-0-or-later-mobile-devices/

［8］ FIDOアライアンス：“パスワードに代わる新たなオンライン認証を推進するFIDO（ファイド）アライアンスの記者説明会，”Jul. 2019.
https://fidoalliance.org/パスワードに代わる新たなオンライン認証を推進/?lang=ja

［9］ FIDOアライアンス：“パスワードに代わる新たなオンライン認証を推進するFIDO（ファイド）アライアンスの記者発表会，”Dec. 2019.
https://fidoalliance.org/パスワードに代わる新たなオンライン認証を推進-2/?lang=ja

［10］ FIDO Alliance：“The Right Mix：Intuit’s Journey with FIDO Authentication，”Oct. 2019.
https://fidoalliance.org/the-right-mix-intuits-journey-with-fido-authentication/


＊17 PKI：公開鍵暗号方式で用いる公開鍵の所有者を保証し，安全な通信を行うようにするための基盤．

＊18 デジタルトランスフォーメーション：IT技術を活用してサービスやビジネスモデルを変革させ，事業を促進するとともに人々の生活をあらゆる面で良い方向に変化させること．

Technology Reports

D-SCP　仮想化　信頼性

# ドコモのサービスを支える加入者データベース仮想化

ネットワーク開発部　西田（にしだ）　慎（しん）　筒見（つつみ）　拓也（たくや）
髙山（たかやま）　一樹（かずき）　藤森（ふじもり）　祐司（ゆうじ）

ドコモのコアネットワークにおける各種サービスの提供は，サービス制御装置群により支えられている．中でも管理が重要なユーザ（加入者）情報の制御は呼制御部F-SCP／データベース機能部D-SCPと呼ばれる装置で行っている．このたび，D-SCPがEoLを迎えるにあたり，ドコモが近年積極的に進めているネットワーク仮想化をサービス制御装置群にも適用し，仮想化のメリットである信頼性と経済性の向上を達成した後継機装置（vDSCP）の導入を実現した．

## 1. まえがき

移動通信ネットワークにおいて，ユーザの加入者情報や位置情報を管理し，位置登録や発着信制御を行うHLR（Home Location Register）*1/HSS（Home Subscriber Server）*2機能などを提供する装置を，ドコモではサービス制御装置（SCP：Service Control Point）群と呼ぶ．その中でも，呼制御部をF-SCP（Front end SCP）*3，加入者データベース機能部をD-SCP（Database SCP）*4という装置で実現している［1］［2］．

このたび，商用で運用しているD-SCPのハードウェアがEoL（End of Life）*5を迎えるに伴い，後継装置の開発が必要となった．

ネットワーク仮想化［3］に関しては，ドコモは2016年3月にvEPC（virtualized Evolved Packet Core）*6を導入し，その後もコアネットワーク*7装置におけるネットワーク仮想化の適用を進めている．コアネットワーク装置の仮想化適用は，2019年度末時点で約40％となっており，今後も適用を推進していく．

仮想化のメリットとしては，通信サービスの信頼性，およびネットワーク設備の経済性の向上に加え，通信混雑時のつながりやすさの向上，サービスの早期提供が挙げられる（**図1**①～④）．D-SCPの後継装置もネットワーク仮想化を適用する方針で開発した．

©2020 NTT DOCOMO, INC.
本誌掲載記事の無断転載を禁じます．
本誌に掲載されている社名，製品およびソフトウエア，サービスなどの名称は，各社の商標または登録商標．

＊1　HLR：3GPP上で規定される加入者情報の管理機能，および呼処理機能を有する論理ノード．
＊2　HSS：3GPP上で規定される加入者情報データベースであり，認証情報および在圏情報の管理を行う．
＊3　F-SCP：加入者系サービス制御を行うユニット．F-SCPは呼制御を担当する．

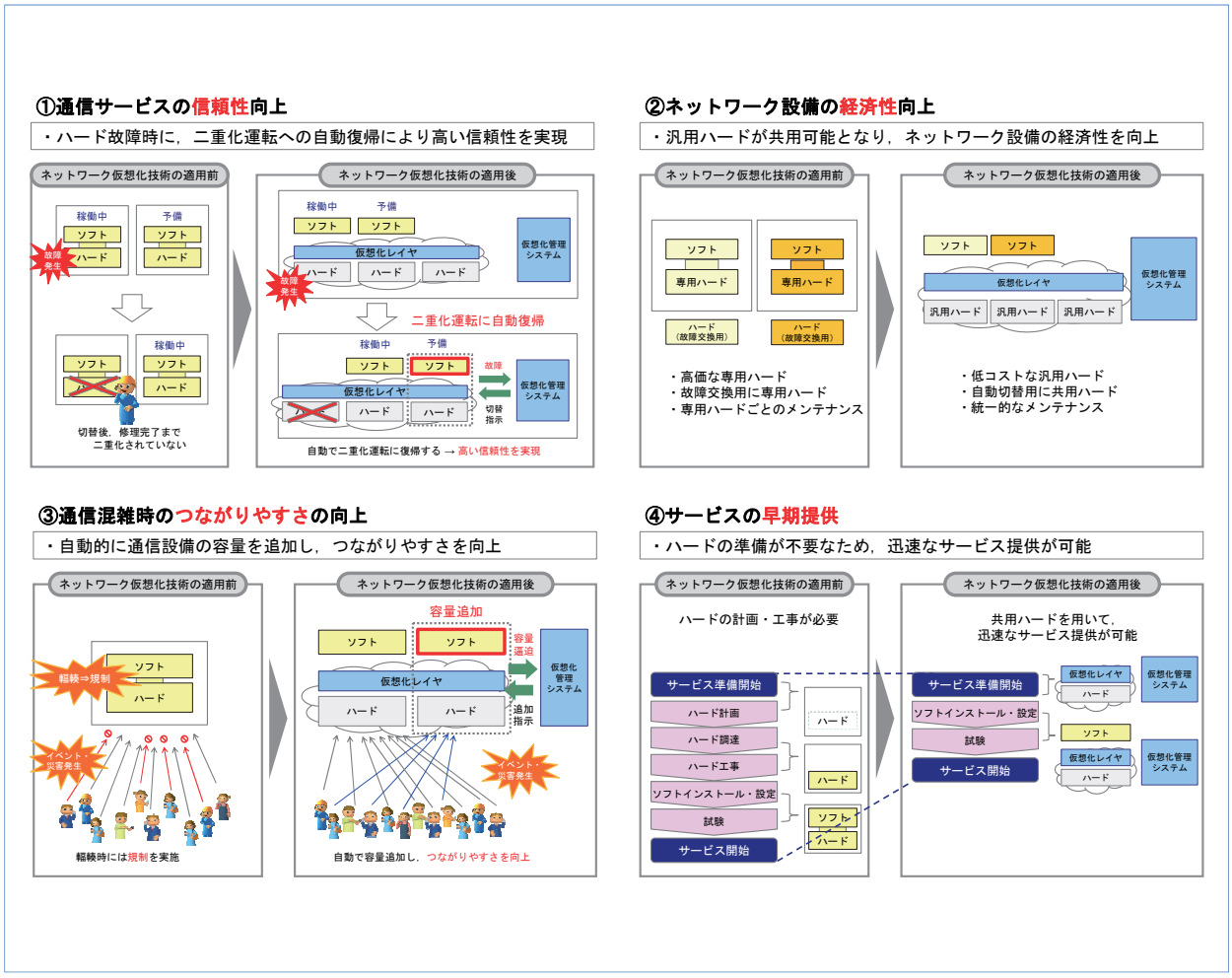



図1　ネットワーク仮想化のメリット

本稿では，D-SCPの後継装置であるvDSCP（virtualized D-SCP）*8導入における装置構成や機能分担の見直し，および，同装置に適用したネットワーク仮想化によるメリット，特に信頼性・経済性の向上を実現した仕組みについて解説する．

## 2. D-SCP仮想化適用の課題

搭載するハードウェアに依存しないという仮想化の特性上，ハードウェア上に加入者情報をもたないステートレスな機能のほうが仮想化対応を行いやすい．ドコモでは，F-SCP/D-SCPで加入者情報の制御を実現しているが，F-SCPが加入者情報に括りつかないステートレスな機能であるのに対し，D-SCPは加入者情報の制御をステートフルな機能で実現しており，ハードウェア上に状態を保持している．そのため，故障発生時，運用するD-SCPを切り替えるだけでなく，保持している加入者情報についても引継ぎを行う必要がある（図2）．

加入者情報は移動通信ネットワークにおいて非常に重要であるため，迅速な復旧が必要である．しかし，仮想化を適用したD-SCPに障害が発生した場合，

＊4　D-SCP：加入者系サービス制御を行うユニット．D-SCPはデータベース機能を担当する．
＊5　EoL：製品・サービスの販売終了やソフトウェアのサポート終了，更新・修正の提供終了を意味する用語．
＊6　vEPC：LTEおよび他のアクセス技術向けに3GPPで規定された，IPベースのコアネットワークであるEPCをVMとして機能するように提供された通信ソフトウェア．
＊7　コアネットワーク：交換機，加入者情報管理装置などで構成されるネットワーク．移動端末は無線アクセスネットワークを経由してコアネットワークとの通信を行う．
＊8　vDSCP：仮想化基盤上で動作するD-SCP．本稿ではVNFとしてのvSSCP/vDSCPを総称する場合にも本名称を用いる．

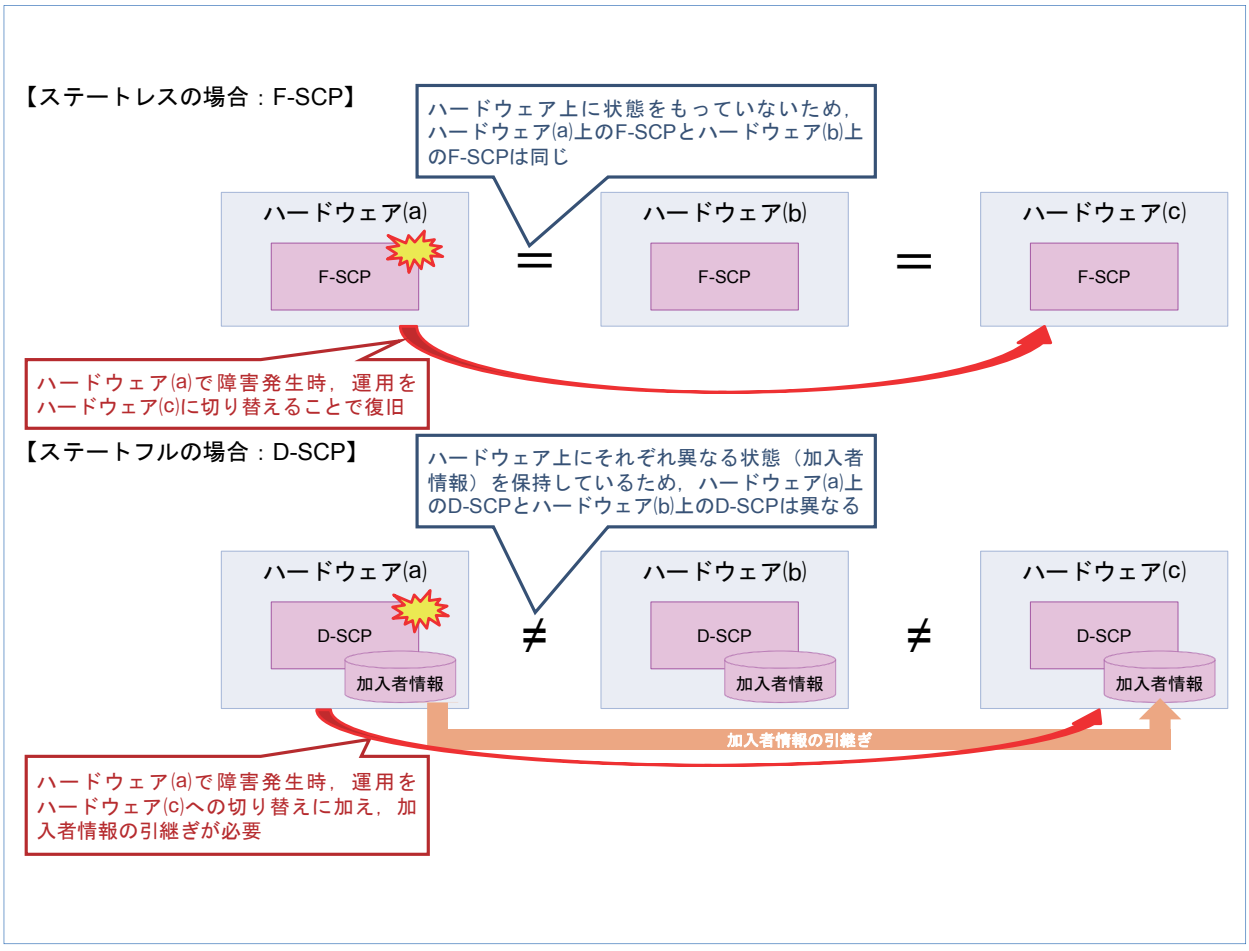



**図2　ハードウェア障害発生時の動作概要**

膨大な量の加入者情報の同期処理が必要となり，復旧までに時間がかかるという課題が存在する．

今回ドコモでは，一部機能を専用装置にて実現することにより上記課題を解決した．

## 3. 装置構成

D-SCPおよび仮想化更改後の加入者データベースであるvDSCPのハードウェア構成を**図3**に示す．vDSCPはSM（Storage/System Manager）[*9]とDB（DataBase）[*10]の2つのVM（Virtual Machine）[*11]で実現している．

①vDSCPにおけるSM-VMは，D-SCPのシステム保守運用および装置管理に関するデータを保持するFS（File Server）[*12]機能の一部（システム保守機能や再開制御）に相当する．SM-VMにより構成されるVNF（Virtual Network Function）[*13]をvSSCP（virtual SM for SCP）[*14]と呼び，vSSCPはシステムおよびストレージの管理を行う．

②vDSCPにおけるDB-VMは，D-SCPのDBP（DataBase Processor）[*15]機能に加え，FS機能の一部（システム保守機能やバックアップセンタ（以下，BC）切替制御）を有する．DB-VMにより構成

*9　SM：RAID，ストレージルータの容量を管理する機能．
*10　DB：本稿におけるDBは，呼制御，バックアップ制御，BC切替，リロケーション制御を行う機能を指す．
*11　VM：仮想マシン．
*12　FS：システムの保守運用，装置管理に関するデータを保持し，RAIDへバックアップを行う機能．
*13　VNF：仮想化基盤上で動作するアプリケーションの構成要素．
*14　vSSCP：vDSCPのシステム管理，およびストレージ管理を行う装置．
*15　DBP：加入者情報のデータベース機能．

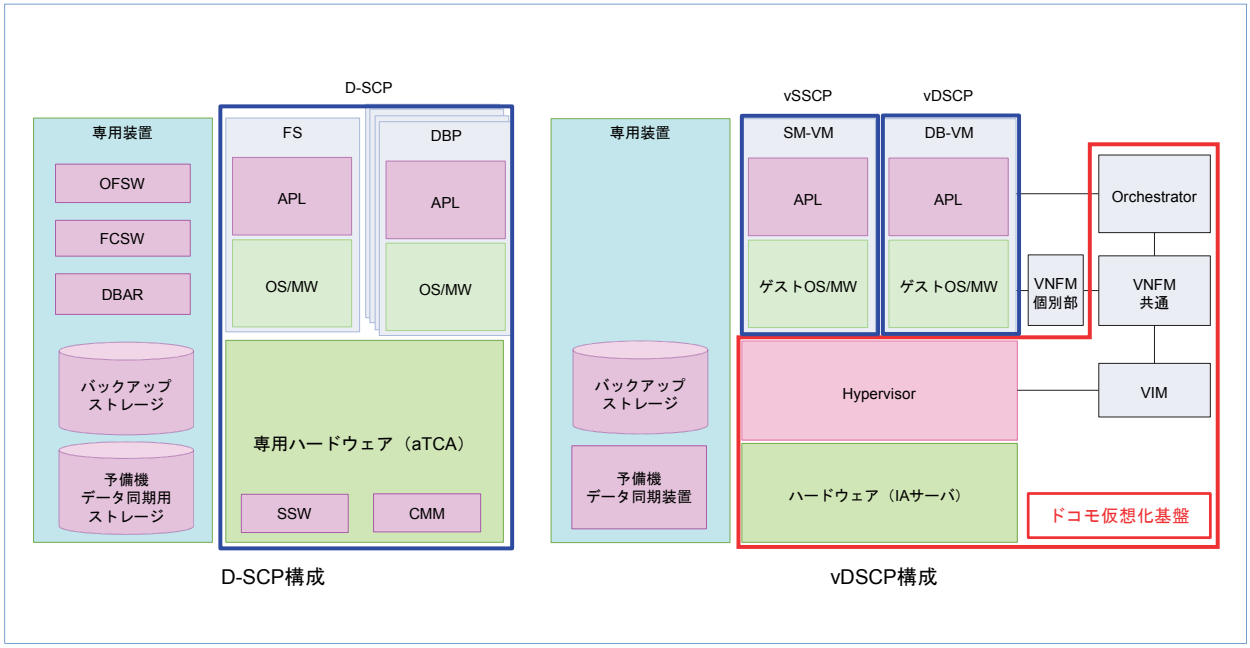



図3　D-SCPとvDSCPのハードウェア構成

されるVNFを狭義のvDSCPと呼び，vDSCPは呼制御やバックアップ制御，BC切替制御を行う．

専用ハードウェアや専用装置の一部については，ソフトウェア化によるアプリケーションとしての実装や，vL3SW（virtual Layer3 SWitch）[*16]などの仮想化ネットワーク側に機能の移行を行った．これにより，専用ハードウェアの内部スイッチSSW（Shelf SWitch）[*17]と専用装置のFCSW（Fibre Channel SWitch）[*18]，DBAR（Data Base Access Router）[*19]を仮想化し，専用ハードウェアのCMM（Chassis Management Module）[*20]，専用装置のOFSW（Open Flow SWitch）[*21]の廃止を実現した．

その結果，専用ハードウェアの運用が不要となり，IAサーバ[*22]やvL3SWなど汎用製品の他仮想化装置との共用化や一括調達が可能となり，設備調達費用および保守費用の効率化が図られたため，ネットワーク設備の経済性が向上した．

## 4. vSSCP（SM-VM）とvDSCP（DB-VM）の機能分担

監視機能部であるSM-VMをデータベース部であるDB-VMに従属させない事で，必要に応じSM-VM，DB-VMの数を柔軟に変更可能な構成をとることが可能となり，SM-VM障害時もサービス影響を抑止できる．また，SM-VMは，DB-VM内部構成の違いを意識せずシステム管理を行うことで，将来的な新規DB-VM種別追加に対するSM-VM開発影響を極小化できる．以上から，耐障害性，拡張性双方の観点で優位性があるため，SM-VMとDB-VMを独立したVNF（＝ユニット）であるvSSCPとvDSCPとして分離して機能配備させる方式を採用している．

## 5. 専用装置の適用

D-SCPの専用装置（バックアップストレージ，予備機データ同期用ストレージ（HS3[*23]））で提供し

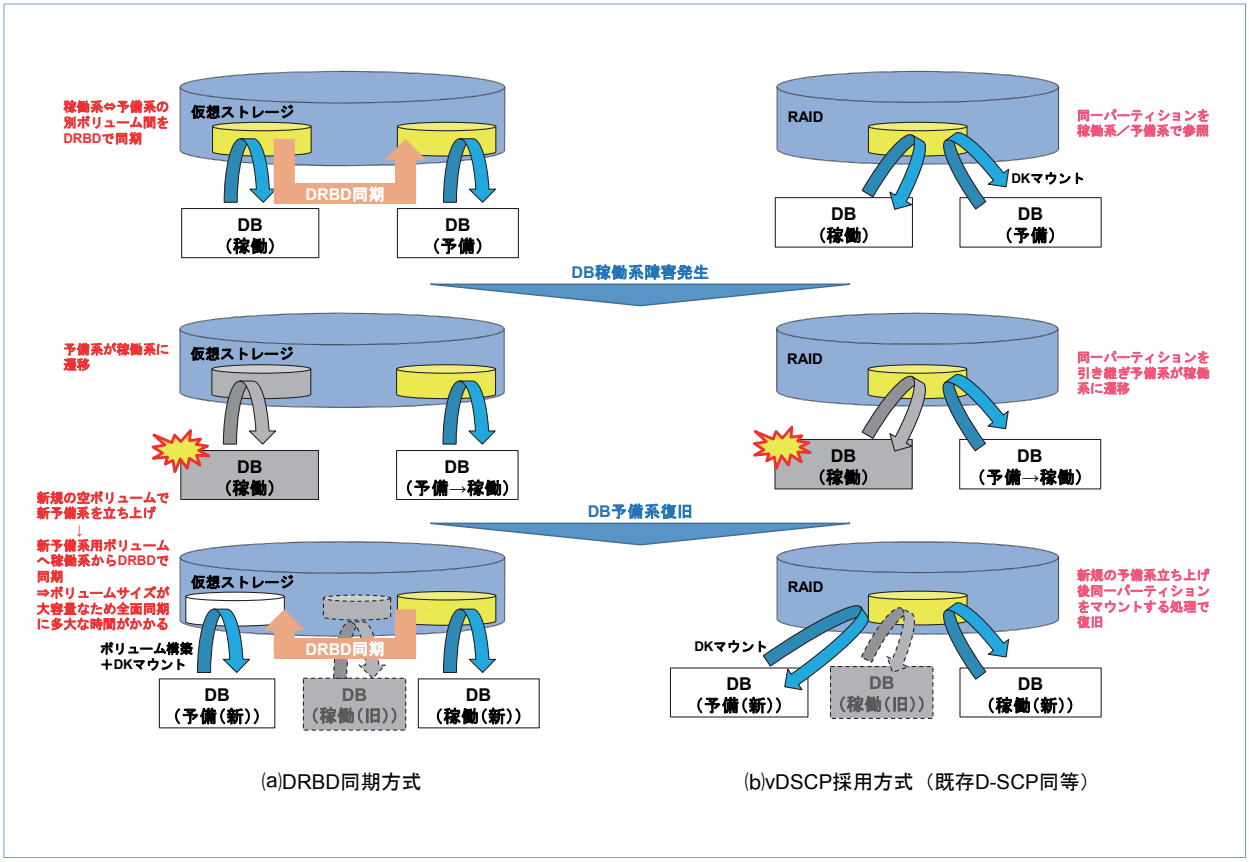
＊16 vL3SW：サービスネットワーク装置とのL3接続を行う仮想スイッチ．
＊17 SSW：通信事業者向け次世代通信機器の業界規格であるaTCAにおける，FSとDBP間を接続する内部スイッチブレード．
＊18 FCSW：バックアップストレージとDBPを接続するスイッチ．
＊19 DBAR：外部対向装置との接続に使用するルータ．
＊20 CMM：aTCAにおけるシャーシ内管理を行う．
＊21 OFSW：F-SCPがデータにアクセスする際，該当の加入者データが収容されたDBPへ振り分ける機能をもつスイッチ．

ていた機能は，取り扱うデータの必要容量，および使用用途を考慮し，vDSCPでも仮想化基盤側機能を利用せず，専用装置（バックアップストレージ，予備機データ同期装置*24）を設置する．

## 5.1 バックアップストレージ

仮想化基盤で提供する仮想ストレージでは，1つのボリュームを複数VMでマウントするマルチアタッチ機能に現状対応していない．そのため，これまで仮想化したコアネットワーク装置では，稼働系／予備系のVM間でデータの共有を行うために，データ同期を行うDRBD（Distributed Replicated Block Device）*25というアプリケーションをVNF上に実装し，稼働系と予備系それぞれがマウントしたボリューム間のデータ同期を行う方式を採用している．DRBDを利用している場合，障害発生後などに稼働系用，予備系用ボリューム間で全面同期が必要となるケースがある．この場合，処理完了まで多大な時間が必要となり，その期間片系運用状態となってしまう（**図4**(a)）．vDSCPでは大容量，かつ重要な加入者情報を取り扱うため，DRBDを採用するのはリスクがある．そこで，vDSCPでは専用のストレージ装置を採用した．

専用ストレージを仮想化基盤収容NWに接続し，DB-VM稼働／予備両系から仮想化基盤収容NW経由で同一パーティションをマウントする，D-SCPと同等の方式で構築する．稼働系で障害が発生した場合は，予備系で同じ領域を引き継ぐ．また旧稼働系




(a)DRBD同期方式　　(b)vDSCP採用方式（既存D-SCP同等）

**図4　DRBD同期方式とvDSCP採用方式の動作の比較**

*22 IAサーバ：Intel社製のマイクロプロセッサ，およびIntel互換プロセッサを搭載したサーバ．内部構造はパソコンとほぼ同様であり，他社製プロセッサベースのサーバと比べて安価であることが特長．

*23 HS3：ユニット内のバックアップデータを保存し，BCとのレプリケーションに使用される外部記憶装置．D-SCPとのレプリケーションにより，複数ユニットのバックアップデータを保存する．

*24 予備機データ同期装置：遠隔に配置されたストレージ装置同士でのデータレプリケーションを行うための装置．

を障害から復旧させる際には，現稼働系にマウントされたパーティションをマウントすることで，同期時間が無くなるため，瞬時に立上げが可能となり，片系運用期間を極小化できる（図4(b)）．

### 5.2 予備機データ同期装置

vDSCPはD-SCPと同様，通常時に稼働するマスタユニット1ユニットに対し，2ユニットのBCを別局舎に配置し，マスタユニットがサービス継続困難な障害が発生した場合にBCに切り替えるBC切替機能をもつ．この機能を実現するために異なる局舎間でバックアップストレージに格納した加入者情報のバックアップデータを同期（レプリケーション）する必要があるが，仮想化基盤の仮想ストレージでは他局舎ボリューム間の同期機能を提供していない．このため，vDSCPではバックアップストレージと同様に，専用の予備機データ同期装置を導入することとした．当該装置には転送時データ圧縮機能をもつ機器を採用し，専用装置を導入せずVMのアプリケーションで実現する方式とした場合と比べて，VMの呼処理性能に影響を与えず，かつ効率的に局舎間同期を行える．

vDSCPのマスタ／BC構成と予備機データ同期装置を用いたバックアップファイルの流れを**図5**に示す．

## 6. 導入メリット

### 6.1 障害時の影響ユーザ数の極小化

加入者情報を管理するvDSCPにおいて，障害発生時のユーザ影響をできる限り減らすことが最重要課題である．今後，信頼性を必要とするIoTデバイスなどが社会インフラや生活環境へ浸透していくに伴い，vDSCPの社会的重要性がさらに高まると予想し，ユーザ影響を極小化する方針を検討した．

従来のD-SCPは加入者情報を収容するデータベース装置であり，ハードウェア上にデータベース機能を有するDBPを1つの単位とし，DBPの数で1ユニッ

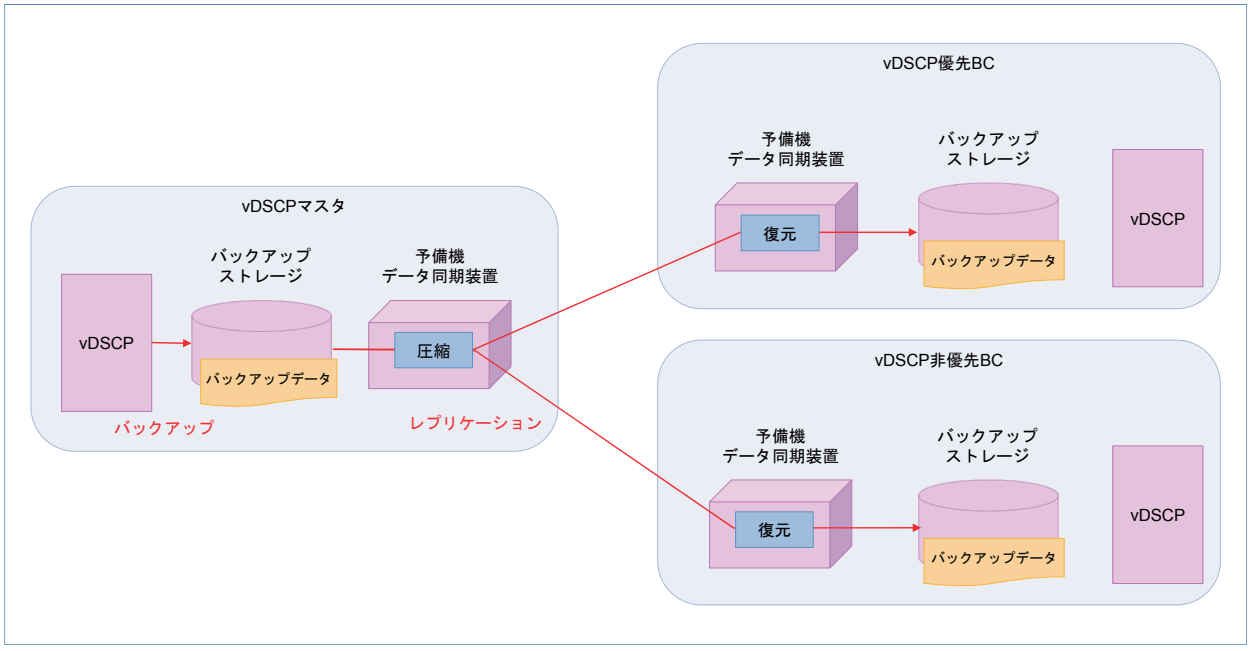



**図5　vDSCPマスタ／BC構成とバックアップファイルの流れ**

＊25 DRBD：複数のLinuxサーバ間でディスクパーティションのミラーリングするミドルウェア．DRBDはLINBIT Information Technologies GmbHのオーストラリア，米国およびその他の国々における商標または登録商標．

ト当りの収容ユーザ数が規定される．また，FS機能は複数のDBPを管理・制御する．D-SCPでは，1つのFSと複数のDBPをまとめてD-SCP 1ユニットとする構成であった．

vDSCPでは，DB-VMにFS機能を移行させた上で，DB-VMとSM-VMを独立したVNF（＝ユニット）として扱う方式を採用したため，1DBP相当のユーザデータを，単独のVNFとして扱い，かつそのVNFを1ユニットとして定義可能となる（**図6**）．

D-SCPでは，前述のユニット構成単位レベルでの障害（装置故障，NW障害）が発生した場合，ユニットごとにBC切替を行っている．

一方vDSCPでは，IAサーバ上にDBP相当のVMを分散配備させたことにより，VM単位での障害の場合は，VM個別でのBC切替を実現できるようになった．これにより，障害時のユーザ影響を極小化することが可能となった（**図7**）．

また，ユニット単位でのDBの増減が可能なことから，需要数の増加に対し設備構築も柔軟に対応することで費用低減が可能となる．

## 6.2 障害に対する復旧の迅速化

⑴D-SCPにおける障害時の動作

D-SCPでは，データベースが収容されているプロセッサ（DBP）の稼働系（act），待機系（sby）の二重故障が発生した場合，同一装置内の他のDBPへユーザを再配置させる，リロケーションと呼ばれる機能が存在する．これは，故障時にデータベースの情報を再配置する機能であり，装置の信頼性向上を目的に行っている．また，リロケーションを行ってもサービス復旧不可となるような障害が発生した場合は，前述の通りD-SCPのBCに切り替えを行い，障害が発生した装置の代替ユニットとして稼働させる．このように，D-SCPでは，二段階の耐障害機能により，ユーザ影響を最小限にしている．

リロケーションおよびBC切替動作中は，データベースへのアクセスを必要とする関連呼処理に影響が生じるため，信頼性向上のためには，当該動作に要する時間および影響ユーザ数を最小化することが重要となる．

D-SCPでは，BCをホットスタンバイ（常時稼働）

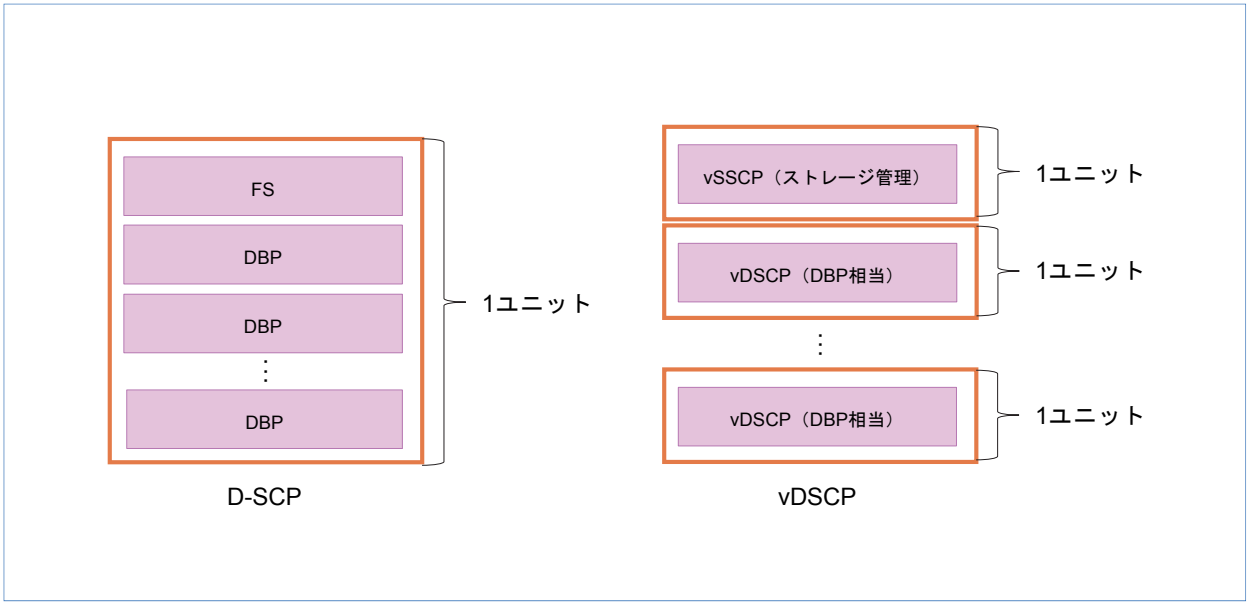



**図6　D-SCPとvDSCPのユニット構成比較**

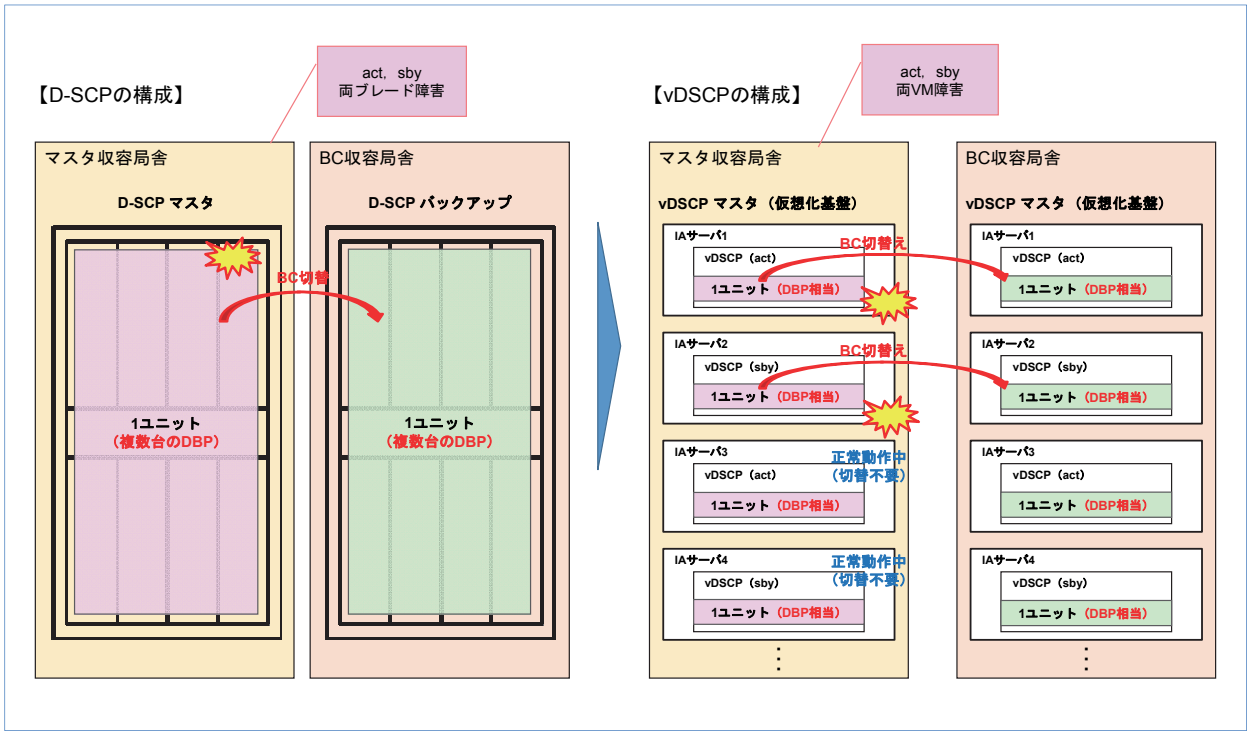



図7　BC切替発生時の耐障害リアクション概要

状態で待機させる方式を採用しているため，BC切替に要する時間は，リロケーションによる切替時間よりも大幅に短いが，複数のDBPから成るユニット単位でBC切替を行うため，リロケーションよりも影響ユーザ数は大きかった．

⑵vDSCPの効果

一方vDSCPでは，前述の通り，ユーザ収容構成単位を見直すことで，BC切替による影響ユーザ数を，D-SCPのリロケーション時の影響ユーザ数であるDBP単位と同等に抑えることが可能となった．そのため，vDSCPでは，復旧時間や代替手順の有無の観点から評価を行い，予備ハードウェアへの退避による対障害機能として，D-SCPの特長であるBC切替時間の短さを活かしつつ，切替ユーザ数単位をDB-VM（DBP相当）へ縮小したBC切替機能を採用した．これにより，D-SCPと同等の復旧時間で，影響ユーザ数をD-SCPから大幅に抑制することができるようになった．

また仮想化基盤システムでは，VMもしくは仮想化基盤上のハードウェアに障害が発生した場合に，予備で確保している別ハードウェア上にVM復旧を行うヒーリングと呼ばれる機能がある．仮想化前は人が現地に赴き，故障したハードウェアを交換する必要があったが，仮想化のヒーリング機能により，短時間で復旧できるようになった．片系運用から両系運用に復旧するまでの時間が短縮されることにより，両系障害が起こる確率の低減，稼働率の向上につながり，信頼性向上を実現した．

## 7. あとがき

本稿では，データベース機能部に仮想化適用したvDSCPの装置構成および機能分担，適用における信頼性，および経済性の向上を図った点について解

説した．

サービス制御装置群のマイグレーションに関しては，各種装置のEoL時期を見据え，段階的に実施することを計画している．最初にEoLを迎えるD-SCPはユーザ情報を管理する重要な装置であることから，品質低下を招かぬよう，仮想化装置vDSCPの導入開発と，D-SCPからvDSCPへの加入者データ移行機能の開発時期を分離することで，万全を期した．

今後はサービス制御装置群の他装置についても，ネットワーク仮想化適用の検討を進めていく．

## 文　献


［1］ 大塚，ほか：“ドコモの多彩なサービスを支えるサービス制御装置の高度化，”本誌，Vol.20，No.4，pp.37-42，Jan. 2013.

［2］ 嘉義，ほか：“信頼性の高いサービス提供に向けたサービス制御装置「F-SCP」の開発，”本誌，Vol.23，No.1，pp.33-38，Apr. 2015.

［3］ NTTドコモ報道発表資料：“世界初，複数ベンダーのEPCソフトウェアを動作可能なネットワーク仮想化技術を開発　―2016年3月から商用ネットワークでの運用を開始―，”Feb. 2016.
https://www.nttdocomo.co.jp/info/news_release/2016/02/19_00.html

# 2019年ITU無線通信総会（RA-19），世界無線通信会議（WRC-19）報告

ネットワーク部　伊藤（いとう） 裕紀（ゆうき）　坂本（さかもと） 信樹（のぶき）
無線アクセス開発部　新（あたらし） 博行（ひろゆき）

国際電気通信連合の無線通信総会が2019年10月21～25日，世界無線通信会議が10月28日～11月22日に，エジプトのシャルム・エル・シェイクで開催された．本稿では，移動通信システムを総称するIMTに関し，両会議において審議された事項を中心に解説する．特に，5Gでの利用を念頭に24.25～86GHzの周波数範囲からIMT向けの周波数を新たに特定した，世界無線通信会議における議題1.13の議論状況については，詳しく説明する．

## 1. まえがき

国際電気通信連合（ITU：International Telecommunication Union）は，国際連合の専門機関の1つであり，電気通信や無線通信に関する国際標準や規則を定めることを主要任務として活動を行っている．その活動の中で，無線通信総会（RA：Radiocommunication Assembly）と世界無線通信会議（WRC：World Radiocommunication Conference）は，3～4年ごとに開催される重要な会議であり，ITU加盟国（合計193カ国）の電気通信に関わる主管庁の関係者が多数出席する．

2019年の10～11月に，エジプトのシャルム・エル・シェイクで開催された無線通信総会（以下，RA-19）には88カ国の主管庁などから約500名，世界無線通信会議（以下，WRC-19）には166カ国の主管庁などから約3,300名の参加があった．RAおよびWRCの開催は，2015年以来4年ぶりの開催であり，ITU本部が設置されているスイス・ジュネーブ以外では，2000年のトルコ・イスタンブール以来の開催となった．

本稿では，RA-19およびWRC-19における，IMT（International Mobile Telecommunications）に関わる審議内容と審議結果を中心に解説する．

## 2. RA-19の審議内容と審議結果

ITUの無線通信部門（ITU-R：ITU Radiocommunication Sector）では，国際的な周波数利用に関する各種技術検討や技術仕様の標準化，これらに

©2020 NTT DOCOMO, INC.
本誌掲載記事の無断転載を禁じます．
本誌に掲載されている社名，製品およびソフトウエア，サービスなどの名称は，各社の商標または登録商標．

関係する文書の作成，国際的な周波数利用に関する調整業務などを実施している．RAは，ITU-Rの活動全般に関わる総会として開催され，ITU-R決議（Resolution），研究課題（Question），勧告（Recommendation）の各文書の承認や，技術検討を行う研究委員会（SG：Study Group）の議長・副議長の任命などが行われる．

### 2.1 ITU-R決議，研究課題，勧告の審議

ITU-Rの各種作業の進め方などを規定する決議については，今回のRA-19において，28件（新規決議の策定2件，既存決議の改訂23件，既存決議の廃止3件）の承認が行われた．このうち，ITU-R全般の作業方法を規定した決議ITU-R 1とWRC準備会合（CPM：Conference Preparatory Meeting）[*1]の作業方法を規定した決議ITU-R 2の改訂については，過去4年間のITU-Rにおける活動で生じた課題などを踏まえ，本会期中，精力的に議論が続けられ，承認された．

研究課題については204件が提出され，2023年までの研究会期における各研究委員会への割振りが承認された．この中には，ITUでの移動通信システムの総称であるIMTについて，さらなる高度化に向けた検討を継続するための研究課題［1］の改訂や，特定の産業分野または企業向けアプリケーションにおける利用用途を念頭にIMTがサポートすべき要件を検討する新規の研究課題［2］の策定が含まれている．

勧告については，RAでの承認が必要なものとして，ITUの無線通信規則で参照されている勧告や，研究委員会での審議状況からRAでのさらなる審議が必要な勧告についての議論が行われた．IMTに関係する勧告としては，ITUの無線通信規則でIMTに特定されている周波数の使用方法を規定した勧告ITU-R M.1036の改訂案が審議され，研究委員会での審議で結論の得られていなかった項目（IMTに特定されていない周波数でのIMT展開の扱いなど）について合意に至り，承認された［3］．

### 2.2 ITU-Rの各研究委員会の議長・副議長の任命

各研究委員会の議長の任命については，電波伝搬に関わるSG3，地上業務に関わるSG5，放送業務に関わるSG6，科学業務に関わるSG7については，現任の議長が2期目として再任された．また，周波数管理に関わるSG1と，衛星業務に関わるSG4については，新たな議長が任命された．SG6の議長には，日本から西田氏（NHK）が再任された．

各研究委員会の副議長も任命され，日本から，SG4副議長に河野氏（スカパーJSAT）が新たに任命され，SG5副議長に新（筆者の1人）が再任された．

## 3. WRC-19の審議内容と審議結果

WRCでは，ITUの無線通信規則の改正に向け，多種多様な無線システムについて幅広い審議事項（議題）が設定されており，過去3～4年間におけるITU-Rでの研究結果に基づいて，これらの議題の審議が行われる．今回のWRC-19では，30程度の議題の審議が行われた．

### 3.1 議題1.13（IMT向けの周波数の追加特定に関する議題）

⑴概　要

携帯電話が使用する周波数については，国際的に調和の取れた利用を行うことにより，基地局や端末の装置調達や，国際ローミング[*2]などのメリットを享受することができる．ITUでは，移動通信システムの総称としてIMTという名称を定義している．そして，IMT向けの周波数をITUの無線通信規則に明記（特定）し，移動通信システムの周波数の利用が世界各国でできるだけ共通となるような取組みを継続して行っている．

＊1　CPM：WRC準備会合．WRCの準備のために，ITU-R SGの検討結果やその他WRCでの議論の材料となる事項をとりまとめたWRC準備会合レポートの作成を行う会合．

＊2　ローミング：利用者が契約している通信事業者のサービスエリア外でも，提携事業者のサービスエリア内であれば，契約している事業者と同様のサービスを利用できる仕組み．

また，5Gの導入が世界各国で進められている中，5Gの利用シナリオの1つとして，4Gを上回る高速通信の実現が求められており，より広帯域幅の周波数を確保することが必要となる．このため，2015年に開催されたWRC-15において，それまでにIMT向けに特定されてきた周波数よりも高い周波数を対象として，24.25～86GHzの中から12個の候補周波数帯が選定され，WRC-19の議題1.13として審議を行うことになった．

⑵審議結果

WRC-19での審議の結果，**図1**および**表1**に示す通り，24.25～27.5GHz，37～43.5GHz，66～71GHzの各周波数帯が，第一地域（欧州，ロシア諸国，アフリカ，アラブ地域の国々），第二地域（南北アメリカ地域の国々），第三地域（アジア・太平洋地域の国々）の全地域で，IMT向けの周波数としてグローバルに特定された．また，45.5～47GHzと47.2～48.2GHzの各周波数帯が，IMT向けの周波数として一部の地域または国を対象として特定され，日本については，47.2～48.2GHzの周波数帯がIMT特定された．これらの周波数帯を合算すると，WRC-19では合計17.25GHzの帯域幅がIMTに特定されたことになり，これまでにITUの無線通信規則で特定されてきた合計約1.9GHzの帯域幅を大きく上回る周波数が，IMT向けの周波数として特定されたことになる．

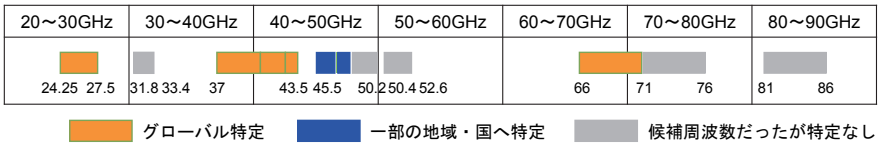



**図1　WRC-19議題1.13における候補周波数とIMTに特定された周波数**

**表1　WRC-19でIMTに特定された周波数の詳細**

| | 第一地域<br>（欧州，ロシア諸国，アラブ，<br>アフリカ）<br>122カ国 | 第二地域<br>（南北アメリカ）<br>35カ国 | 第三地域<br>（アジア・太平洋）<br>36カ国 |
|---|---|---|---|
| 24.25～27.5GHz | グローバル特定 | | |
| 37～43.5GHz | グローバル特定 | | |
| 45.5～47GHz | 50カ国に特定<br>（欧州の一部，ロシア諸国，<br>アラブ，アフリカ地域） | 1カ国に特定<br>（ブラジル） | 2カ国に特定<br>（イラン，韓国） |
| 47.2～48.2GHz | 62カ国に特定<br>（欧州の一部，ロシア諸国，<br>アラブ，アフリカ地域） | 地域全体に特定 | 7カ国に特定<br>（オーストラリア，韓国，<br>インド，イラン，日本，<br>マレーシア，シンガポール） |
| 66～71GHz | グローバル特定 | | |

⑶審議における論点

IMT向けの周波数の特定に際して，既存の無線システムとの周波数共用条件が大きな論点となった．24.25～27.5GHzおよび37～43.5GHzに関する審議では，隣接する23.6～24GHz，36～37GHzの周波数で運用される地球探査衛星業務（受動）への電波干渉を避けるための条件が議論された．具体的な条件として，ITU-Rの技術検討を踏まえ，地球探査衛星の受信周波数におけるIMTの無線局（基地局および端末）の不要発射*3の強度を制限することが示されていたが，技術検討の前提条件などの違いに起因して，提案を行った地域や国の間で，求める不要発射の強度の制限値が大きく異なっており，大きな議論となった．また，24.25～27.5GHz，42.5～43.5GHzにおいて運用される衛星間業務および固定衛星業務への電波干渉を避けるための条件も議論され，IMT基地局の出力制限，屋外IMT基地局の送信指向方向や機械チルト*4の規定といった，具体的な案が議論された．

地球探査衛星業務（受動），衛星間業務および固定衛星業務との周波数共用条件に関するこれらの論点は，公式会合の審議のみでは意見集約を図ることが困難と想定されたため，WRC-19の会合期間の後半に入り，各地域を代表するメンバや，具体的な提案を行っている各国代表のメンバを中心として，少人数での非公式会合が複数回にわたり開催され，合意可能な妥協案の検討が進められた．最終的にこれらの妥協案は，WRC-19の全体会合に上程され，合意にこぎつけた．

## 3.2 その他のIMT関係議題

WRC-15において，1,427～1,518MHzがIMT向けの周波数として特定されたことに伴い，第一地域と第三地域を対象とした，1,452～1,492MHzの放送衛星業務（音声）とIMTとの両立性に関する検討が，議題9.1の課題9.1．2として取り扱われた．本周波数帯において，国内ではWRC-15以前から移動通信システムの運用が行われており，日本としては，今後の国内運用への制約が発生しないように対応を行った．本件もWRC-19の最終週までもつれこむ難しい議論となったが，最終的には放送衛星業務（音声）とIMTへの規制のバランスを配慮した上での解決策が導かれた．

また，日本では一部の周波数が5G向けに割当済みとなっている27.5～29.5GHzの周波数において，固定衛星業務として運用される，移動する地球局（ESIM：Earth Station in Motion）*5の技術・運用特性や他の無線システムとの周波数共用に関する検討が，議題1.5として取り扱われた．議論の中心は，航空機に搭載されるESIM（以下，航空ESIM）が人工衛星に対する送信を行う際に，地上に展開される既存システムに及ぼす電波干渉の影響をいかに回避するか，という点であった．27.5～29.5GHzの周波数においてESIMの展開を考える欧州などと，5Gでの利用を考える日本，韓国，米国との間で大きな議論となったが，最終的に，運用に関わる規定については，航空ESIMの地表面への電力束密度（PFD：Power Flux Density）*6の制限が規定され，ITU-Rの無線通信局による航空ESIMの審査を厳格に実施すること，国境外へのPFD制限順守の責任規定をWRCの決議に明記することで合意された．

## 3.3 WRC-23で審議する議題

各WRCでは，将来のWRCで審議する議題も決定することとなっており，WRC-19でも，4年後に開催予定のWRC-23の議題が審議・合意された．IMTに関係のある各議題の周波数帯を**図2**に示す．

WRC-19議題1.13に引き続き，複数の国や地域からIMT向けの周波数の追加特定に向けた検討を行う新議題設立の提案が行われた．提案された3.3～24GHzの周波数範囲の中で，各地域の代表メンバ間での調整が進められた結果，WRC-23議題1.2として

＊3 **不要発射**：希望帯域外に発生する不要な電波．隣接周波数に対する干渉となる．

＊4 **チルト**：アンテナから放射される電波の，最大放射方向の垂直面内における傾き角を表す．また，チルトの方向を制御する方法として，アンテナを物理的に傾ける機械チルトと，アンテナ素子の振幅・位相を制御して電波の最大放射方向を傾ける電気チルト方式がある．

＊5 **ESIM**：固定衛星業務において，静止軌道上の宇宙局と通信を行う，移動する地球局の総称．

＊6 **電力束密度（PFD）**：単位面積を通過する電波の電力の強度．

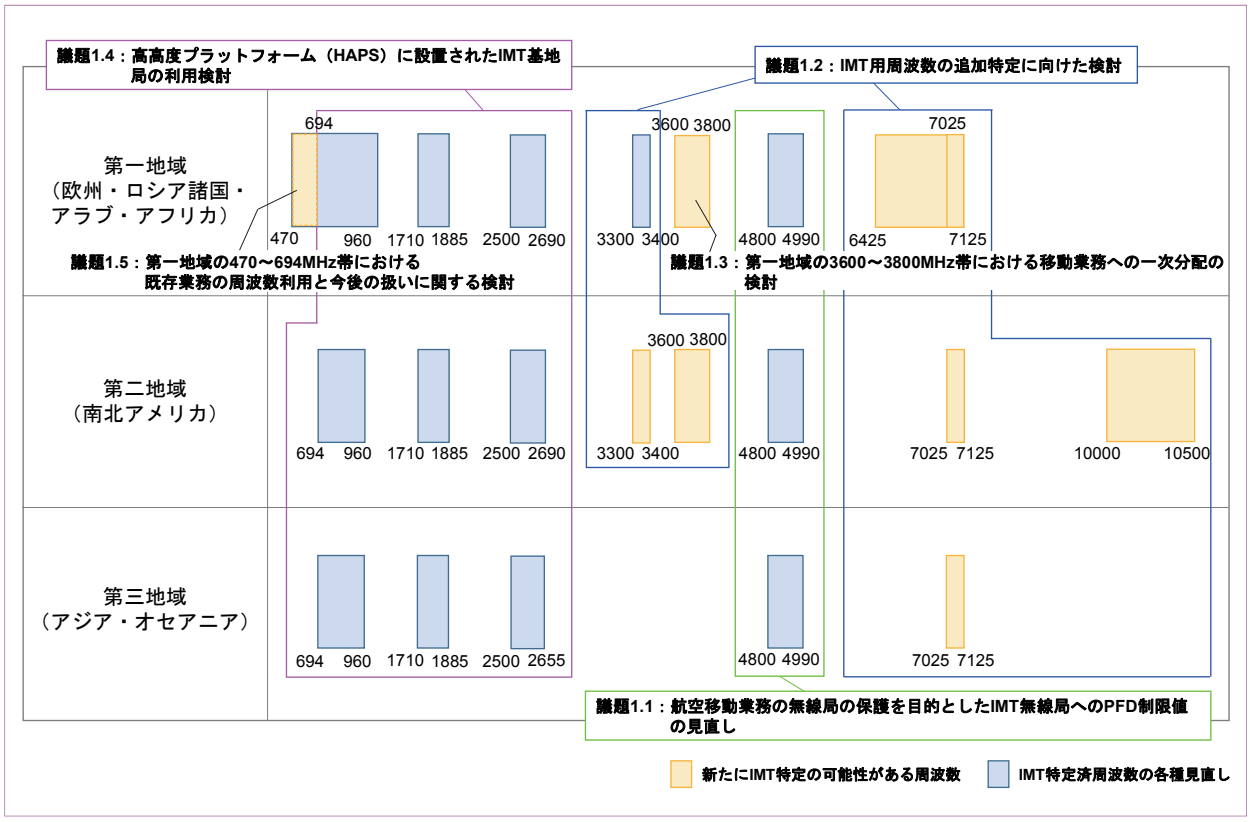



図2　WRC-23におけるIMT関連議題の周波数帯

図2に示す各周波数帯を検討対象とすることが合意された．

また，WRC-15においてIMT向けの周波数として一部の国に特定された4,800～4,990MHzの周波数帯について，航空移動業務の無線局の保護を目的としたIMT無線局へのPFD制限値の扱いを見直す議論がWRC-19期間中に行われたが，結論が出ず，WRC-23議題1.1として継続審議することが合意された．

さらに日本からは，2.7GHz以下のIMTに特定された周波数において，高高度プラットフォーム（HAPS：High Altitude Platform Stations）[*7]に設置されたIMT基地局の利用を検討する新議題設立の提案を行い，対象周波数と対象地域を絞り込んだ上で，WRC-23議題1.4として合意された．

この他，第一地域の3,600～3,800MHz帯における移動業務への一次分配[*8]の検討（議題1.3），第一地域の470～694MHz帯における既存業務の周波数利用と今後の扱いに関する検討（議題1.5）も合意されており，今後の議論によってはこれらの議題も，IMT向けの周波数の特定の議論に関係してくる可能性がある．

## 4. あとがき

本稿では，RA-19およびWRC-19について，審議結果の概要を解説した．WRC-19における議題1.13の審議では，非常に広い帯域幅の周波数をIMT向けに特定することが合意され，過去のWRCにおける結果と比較しても，将来のIMTのさらなる発展に向けて大きな成果が得られたと考えられる．一方

＊7　高高度プラットフォーム（HAPS）：高度約20kmの成層圏で一定の場所に滞空する航空機などの無人機体に通信機器を搭載し，上空から通信サービスを提供するシステムの総称．

＊8　一次分配：無線通信規則における一次業務への周波数分配．周波数分配を受ける業務は一次業務と二次業務に分類される．一次業務は，他の一次業務または二次業務に対して有害な干渉からの保護を受けることができるが，二次業務は一次業務に対して，有害な干渉を与えてその運用を妨げることはできず，また干渉保護を求めることもできない．

で，既存の無線システムとの周波数共用条件に関し，各地域・各国で考え方に大きな差があり，今回のWRC-19での審議の過程においても，合意形成に多くの時間，労力が費やされた．

WRC-23においてもIMT向けの周波数の追加特定に関する検討が行われるが，いずれの周波数帯でも既存システムが運用されており，周波数共用条件に関する議論が，活発に行われるものと想定される．WRC-19の会合期間の終盤において，各地域の代表者などによる非公式会合が重ねられ，妥協点を見出されたことを踏まえると，WRC-23でも難航する事案において同様の調整手法が採られると考えられる．このような議論の進め方に対して適切に対応していくためには，事前に各地域での見解の統一を図っておくことや，各地域での代表者として認知される必要があり，ITU-Rでの技術的検討に関わる会合や各地域での準備会合でのプレゼンスがより一層重要になると考えられる．引続きドコモは，これらの会合へ積極的な参画を行っていく所存である．

## 文　献


［1］ 研究課題ITU-R 229-5/5：“Further development of the terrestrial component of IMT,” Nov. 2019.

［2］ 研究課題ITU-R 262/5：“Usage of the terrestrial component of IMT systems for specific applications,” Nov. 2019.

［3］ 勧告ITU-R M.1036-6：“Frequency arrangements for implementation of the terrestrial component of International Mobile Telecommunications (IMT) in the bands identified for IMT in the Radio Regulations,” Oct. 2019.

Event Reports　5G　Open House　展示会レポート

# DOCOMO Open House 2020 ―ようこそ，5Gリアルワールドへ．そしてその先へ.―

R＆D戦略部　玉置（たまおき） 真大（まさひろ）

2020年1月23，24日の2日間にわたり，東京ビッグサイトにて「DOCOMO Open House 2020　―ようこそ、5Gリアルワールドへ。そしてその先へ。―」が開催された．本稿では，本イベントの開催模様の紹介，ならびに主だった展示の詳細について解説する．

## 1. まえがき

ドコモは，2020年1月23，24日の2日間にわたり，東京ビッグサイトにて「DOCOMO Open House 2020　―ようこそ、5Gリアルワールドへ。そしてその先へ。―」を開催した（**写真1**）．

ドコモは2020年のさらにその先を見据え，ビジネスパートナー（以下，パートナー）の皆様とともにお客様の期待を超えることにより，お客様への「驚き」と「感動」の提供，パートナーとの「新しい価値」の協創をめざしている．本イベントは従来，さまざまな分野のパートナーとの協創事例などを基に先進性・技術力を世の中に広く伝え，新たな協創を生む場という位置づけであったが，今回はこれに加え，来場者に利用者目線でドコモの描く未来感が伝わるよう趣向を凝らした．会場では，協創を進めているパートナーの皆様とともに，5G，AIやIoTなどの最新技術と，それらを活用したビジネスソリューションについて紹介し（**写真2**），また多彩な講演やプログラム，ドコモの考える未来の暮らしを体現した「DOCOMO 202X CONCEPT」も紹介した．5G商用サービスの提供元年ということで本イベントは注目され，来場者数は昨年度と比較し，約10,000人増の約24,000人と盛況であった．

本稿では，本イベントにおける主だった展示の詳細について解説する．

©2020 NTT DOCOMO, INC.
本誌掲載記事の無断転載を禁じます．
本誌に掲載されている社名，製品およびソフトウエア，サービスなどの名称は，各社の商標または登録商標．

**写真1　DOCOMO Open House開催模様**

**写真2　事業創出**

## 2. イベント概要

展示は286件にのぼり，「AI」「デバイス・UI/UX」「デジタルマーケティング」「IoT」「事業創出」「グローバル」「5G Vision」「5G Lifestyle」「5G Business」「5G Future & Technology」の10カテゴリに分類した（**写真3**）．各展示では，実際に動作可能な実機による体験やデモを通して，来場者にドコモの描く未来観を伝えた．

講演においては，初日の基調講演にて，吉澤 和弘代表取締役社長が「5G，より豊かな未来の到来」と題して，5G時代に向けたドコモがめざす未来や中期戦略について紹介し（**写真4**），2日めには，中村 寛取締役常務執行役員が「5G時代の幕開けとサスティナブルな社会の実現」と題して，5G，およびその先の通信技術やAIなどが普及するであろう未来において，現実世界とサイバー空間が融合する事で実現される社会について講演した（**写真5**）．

写真3　5G Vision

写真4　吉澤社長による基調講演

写真5　中村常務による特別講演

その他，ドコモだけではなく，冨田 直美氏（hapi-robo st社，ハウステンボス㈱），Rony Abovits氏（Magic Leap社），大畑 大介氏（元ラグビー日本代表，神戸製鋼コベルコスティラーズ，アンバサダー）などによる，多彩なテーマに沿った講演も開催した．

## 3. DOCOMO 202X CONCEPT

本パビリオンは，会場内の展示の一部をピックアップして，ドコモの考える未来の暮らしを「HOME」「MOBILITY」「CAFE」「LIBRARY」「HALL」「ARENA」の6シーンで表現した．技術的な説明は極力省いた体験型展示とし，各シーンそれぞれが組み合わさった際に，いったいどのような未来のユーザ体感が得られるのかを紹介した．

例えば「HOME」では，居住者が朝起きるとAIが体の状態を把握し，気分や状態に合わせて室内の環境を心地よいものに切り替えるシーンがある．これらは，下記の展示物が組み合わされている．

①「高齢者見守りソリューション」：プライバシーに配慮し，ビデオカメラを使わずに居住者の健康状態・位置・姿勢を取得可能とするソリューション．

②「スマートホーム」「未来の家プロジェクト」：各種IoTセンサが居住者のデータを集め，AIに基づいてユーザへのリコメンドやIoTデバイスを制御するソリューション．

その他にも，「カフェ」に入店すると「長距離ワイヤレス充電*1技術」を用いて自動でスマートフォンの充電が始まり，UWB（Ultra Wide Band）*2と各種無線規格を連携させた「おサイフケータイのタッチレス対応」技術により，レジの前に立つだけでポケットの中のスマートフォンが支払いを完了させるシーンがある．

このパビリオン内で示したすべての生活シーンは決して夢物語ではなく，ドコモとパートナーがもつ技術を基にすることで実現可能な未来である（**写真6，7**）．

＊1　ワイヤレス充電：電気的な接点を介さずに電力を送る技術．電磁気的な方式，光による送電，音波による送電などがある．
＊2　UWB：500MHz以上の広い周波数帯域に拡散して送受信を行う無線通信方式．

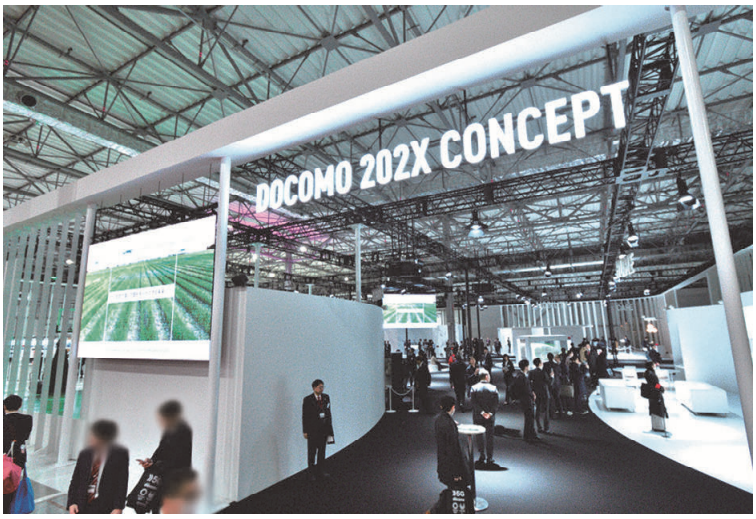



写真6　DOCOMO 202X CONCEPT入口

写真7　DOCOMO 202X CONCEPTスポーツ観戦

## 4. カメラで人の動きを三次元デジタル化「VMocap」

本ブースでは，会場内に設置された円形のステージ上で，特殊な装置やスーツを用いずに，広い空間における複数人のモーションキャプチャを行うデモを行い，多数の来場者の関心を集めた（**写真8**，**9**，**図1**）．

本技術は東京大学　情報理工学系研究科　中村・山本研究室との共同研究で開発された技術で，同研究室の開発したカメラ映像だけからモーションキャプチャを行う技術「VMocap（ブイモーキャプ）」を応用することでこちらを実現している．

一般的にモーションキャプチャを行うためには特殊な装置やスーツが必要で，計測場所や利用シーンが限定されるが，本技術は解析に用いるべき最適な

写真8　デモンストレーションの様子

写真9　会場の様子

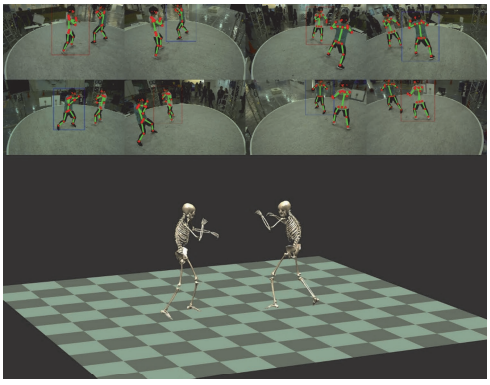


図1　ビデオモーションキャプチャのイメージ

映像を，複数のカメラから自動的に選択して切り替えることで，広い空間における複数人のモーションキャプチャを行う．また，人同士の体が映像上で重なって見える状況下でも，人の骨格構造と運動の連続性，そして最新の画像認識技術を活用することで頑強に運動を推定することができ，フットサルのように複数の選手が激しく動き回るようなシーンでも，高精度で滑らかなモーションデータや骨の動きを取得できる（**図2**）．

今後は本技術を，サッカー・野球・体操・フィギュアスケートなどのスポーツに適用し，トレーニングや戦術解析，けがや故障の予防，運動のアーカイブ化などに役立てる．また，エンターテインメント領域における3Dアニメーション作成や，介護・リハビリ現場での運動評価などにも活用していく予定である．

## 5. ARクラウドで実現する未来の生活スタイル

新体感コミュニケーションとして期待されるAR（Augmented Reality）*3/MR（Mixed Reality）*4について，「ARクラウド」の技術を活用し，未来の生活スタイルを想起させるデモの展示を行った．

ARクラウドとは，あらかじめ展示ブース内の空間構造データを収集し，現実空間のコピーであるデジタルツイン*5を構築，特徴点群マップ*6による現実空間とデジタルツイン内の位置合わせを行う自己位置推定技術により，ARグラス／VR（Virtual Reality）*7ゴーグル／タブレットなどの異なる複数のデバイス間で共通のAR/MR体験を提供可能とする技術である．

展示では，古都をイメージした屋外の街並み，屋内のリビングの2つのエリアを模擬した（**図3**）．来場者には，自分の位置に応じて近くの（模擬）店舗などのクーポンを提供する，複数の折り鶴がのれんから飛び出してくる，バス停の上に渋滞情報などを加味した到着予定時刻を表示する，人の動きに追従

＊3　AR：現実世界を写した映像に，電子的な情報を実際にそこにあるかのように重ねて，ユーザに提示する技術．
＊4　MR：現実世界を写した映像に，電子的な情報を重ねて，ユーザに提示する技術．ARと異なり，自由視点での表示など情報を実際にそこにあるかのように提示する．
＊5　デジタルツイン：現実世界のありとあらゆるものの位置や形状，各種センサ情報などをデジタルの世界にリアルタイムに再現されたもの．
＊6　特徴点群マップ：現実空間とデジタルツインとの位置合わせ（自己位置認識）を行うために必要となる，カメラ画像が抽出された，画像の特徴点の集まり．

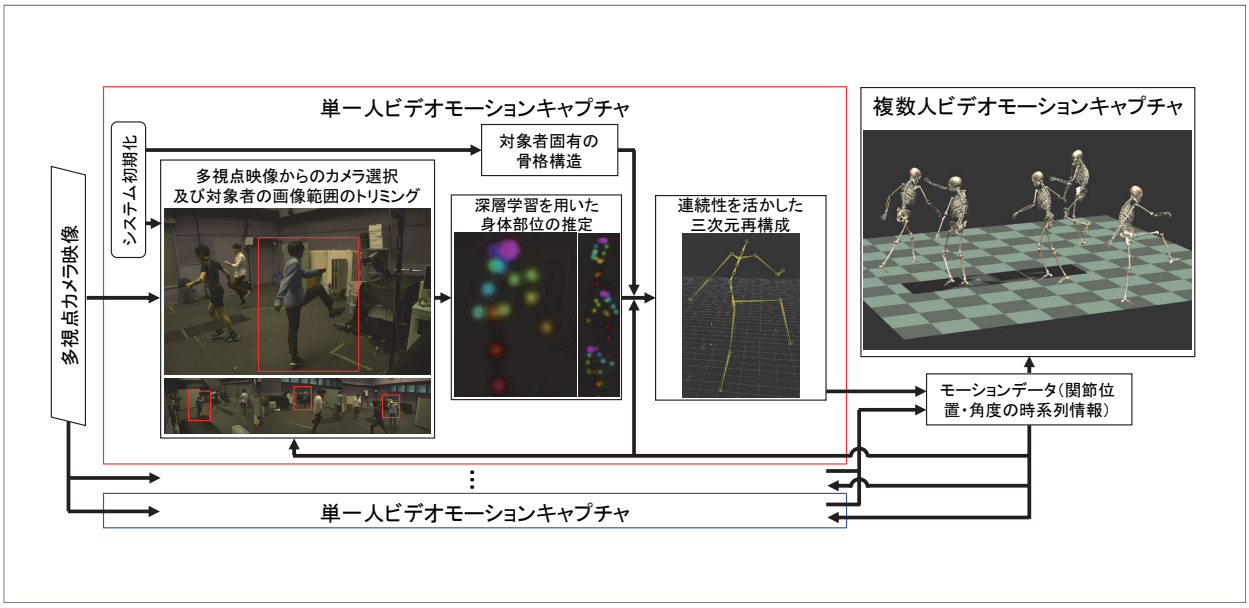



**図2　VMocap概略図**

**図3　展示ブース全体概要**

して頭の上にテキストメッセージを表示する，バーチャルペットや，リビングが一瞬にして美しい砂浜に変化するなど，さまざまなコンテンツをMagic Leap 1[*8]，Mirage Solo，iPad[*9]の3つの端末でサイバーとフィジカルが融合した体験をしてもらった（**写真10**，**図4**）．

来場者からは，Magic Leap 1を体験したいとの要望が多く，最先端の空間コンピューティングデバ

＊7　VR：まるであたかも仮想世界にいるかのように錯覚を与える技術．近年はHMDを用いて主に視覚に働きかけ，このような錯覚を実現する手法が主流である．

＊8　Magic Leap 1：「MAGIC LEAP」「MAGIC LEAP 1」，Magic Leapのロゴおよびその他のすべての商標は，Magic Leap, Inc.の商標．

＊9　iPad：Apple，Appleのロゴ，iPadは，米国および他の国々で登録されたApple Inc.の商標．TM and © 2020 Apple, Inc. All rights reserved.

イスで体験するARクラウドの世界観に，共感の声が多く聞かれた．

## 6. 透明動的メタサーフェスによる柔軟な5Gエリア形成

5G以降の世代で利用されるミリ波帯の柔軟なエリア整備に向けて，ドコモとAGC㈱（以下，AGC）が開発した「透明動的メタサーフェス*10」のプロトタイプを展示するとともに，実証実験の様子を動画で紹介した．ドコモは昨年，同イベントで反射波の方向やビーム形状が設計可能なメタマテリアル*11反射板の展示を行ったがいくつかの課題があった．まず，メタマテリアル反射板はエリア拡大に有効である一方，設置場所に合わせた設計が必要となる点，反射板の裏が見通し外となり通信品質が劣化する点，加えて景観に影響を与える点である．そこで，ドコモが新たに原理提案・設計をし，AGCが材料・微細加工技術の検討および製造を行ったのが今回展示した「透明動的メタサーフェス」である．

本透明動的メタサーフェスは，透明化したメタサーフェス基板に重ねたガラス基板のμmオーダの微小な動きによって，メタサーフェス基板の透過／反射特性が大きく変化するよう設計することにより“透明性を維持したまま透過／反射率の動的制御”および“基板の大面積化”を実現している（**写真11**）．

会場では，2020年1月に実証した28 GHz帯における400 MHz以上の帯域幅の電波をほぼ損失なく透過／反射制御した際の動画展示も実施し，透明動的メタサーフェスにより景観を損なうことなく動的に電波伝搬を制御することで，よりきめ細やかで柔軟な5Gエリア構築が可能となることを示した（**図5**，**写真12**）．

## 7. あとがき

本稿では，2020年1月23，24日に開催された「DOCOMO Open House 2020　―ようこそ、5Gリアルワールドへ。そしてその先へ。―」の開催模様の紹介，および展示について解説した．

**写真10　デモを体験いただいたお客様の様子**

**図4　iPadに表示された実際のコンテンツ**

**写真11　展示した透明動的メタサーフェス**

*10 メタサーフェス：波長に対して小さい構造体を周期配置して任意の誘電率・透磁率を実現する人工媒質（メタマテリアル）の一種で，構造体の周期配置を2次元とした人工表面技術．

*11 メタマテリアル：電磁波に対して自然界の物質にはない振舞いをする人工物質のこと．

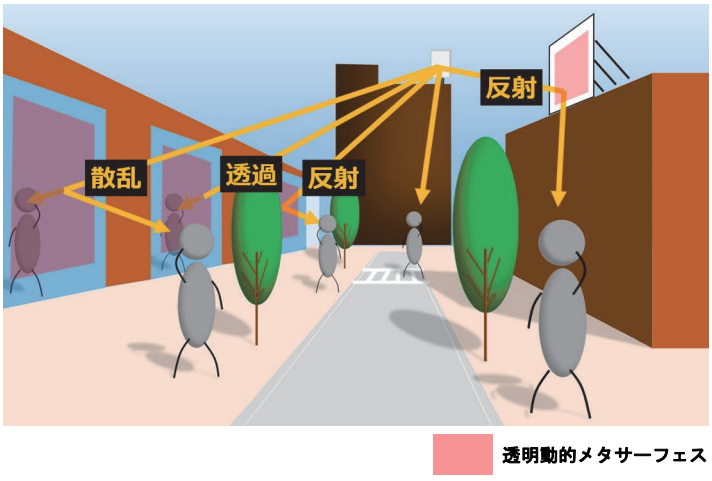



図5　将来ユースケースのイメージ

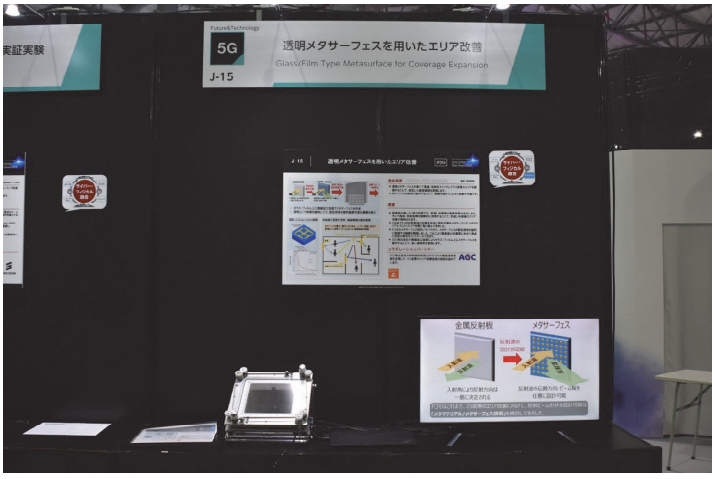



写真12　展示の様子

ドコモでは，5Gの本格商用サービスを開始しており，将来に向けてお客様の生活スタイルやコミュニケーションを革新する，楽しさ，驚きのあるサービスを創り出し，また，日本の成長と豊かな社会の実現をめざして，社会課題の解決に取り組んでいく．

# 「第1回KPMGジャパン秘密計算ハッカソン」でサービスイノベーション部のチームが優勝

2019年11月7～8日にかけ，KPMGジャパン主催「第1回KPMGジャパン秘密計算ハッカソン」が開催され，サービスイノベーション部の森田 康介，長谷川 慶太，千田 拓矢，KPMG Ignition Tokyoのクラナ・タルン氏が企画開発した「秘密計算を使った電子投票システム」が優勝しました．

秘密計算とは，データを暗号化したまま，復号することなくデータ分析や処理などの利活用を可能とする技術で，今回のハッカソンでは，「秘密計算でビジネス課題を解決する」をテーマに参加者数名でチームを作り，秘密計算技術を活用したプログラムを作成し，開発アイデアや性能を競いました．

今回提案した，秘密計算を使った電子投票システムは，課題意識やアイデア，企画からプログラミングの実装までが非常に優れていたと評価され，今回の受賞となりました．

長谷川は今回の提案した電子投票システムに関して，「電子投票システムのアーキテクチャは，オークションや競争入札のような例にも応用が可能」とコメントしています．

本誌に掲載されている社名，製品およびソフトウエア，サービスなどの名称は，各社の商標または登録商標．

（左から）長谷川，クラナ・タルン氏，千田

**NTT DOCOMO**
**テクニカル・ジャーナル　Vol.28 No.1**

2020年４月発行

企画編集　株式会社NTTドコモ　R&D戦略部
〒100-6150
東京都千代田区永田町 2-11-1
山王パークタワー39階

発　行　一般社団法人 電気通信協会
〒101-0003
東京都千代田区一ツ橋 2-1-1
如水会ビルディング6階

本誌掲載内容についてのご意見は
e-mail: dtj@nttdocomo.com宛

本誌に掲載されている会社名，商品名などは，各社の商標または登録商標です．
本誌掲載記事の無断転載を禁じます．

© 2020 NTT DOCOMO, INC.