Technology Reports

eSIM　LPA　ワンナンバーサービス

GSMA eSIM仕様に準拠したLPAアプリケーションの開発

移動機開発部　合田 晶生（ごうだ あきお）　山口 久美子（やまぐち くみこ）†
浅野 浩一（あさの こういち）

ドコモは，2017年にコンシューマ向けeSIM対応端末を国内ではじめて開発・導入した．今後，eSIM対応端末のラインナップを拡充していくとともに，eSIMを活用した新たなサービスやユースケース数の拡大をめざしている．そこで，Android™*1スマートフォン上で汎用的に動作するLPAアプリケーションを開発し，2018年以降発売の端末に搭載していくこととした．本稿では，今回ドコモが開発したLPAアプリケーションの仕組みについて解説する．

1. まえがき

近年，ウェアラブル端末をはじめとする各種IoT（Internet of Things）機器へのセルラ通信機能の搭載需要が高まっている．ドコモではこの需要に応えるため，GSMA（GSM Association）*2RSP（Remote SIM Provisioning）*3仕様に準拠したeSIM（embedded SIM）*4プラットフォームを開発・導入済みである［1］．eSIMプラットフォームを利用することで端末のドコモ回線開通が容易になる一方，端末機種ごとにeSIMプラットフォーム対応のLPA（Local Profile Assistant）*5機能を開発しなければならない点が課題であった．

そこで，今後eSIM搭載端末数の増大や，eSIMを利用するサービスの拡大を見据え，Androidプラットフォーム上で動作するLPAアプリケーションをドコモが開発して端末に搭載することとした．本稿では，開発したLPAアプリケーションの仕組みについて解説する．

2. LPAアプリ開発の目的

2.1　キャリアが提供するメリット

一般にAndroid端末メーカは，ハードウェアとソフトウェアの両面で開発を行う必要がある．Android端末のハードウェアは，当該端末のスペック（ディ

©2018 NTT DOCOMO, INC.
本誌掲載記事の無断転載を禁じます．

† 現在，プラットフォームビジネス推進部

＊1 Android™：Google Inc.の商標．
＊2 GSMA：携帯電話事業者のほか，端末メーカやソフトウェア企業などを取りまとめるモバイル通信事業の世界的な業界団体．事業者間のローミングルール策定などに加えて，eSIM関連では標準化を先導．

スプレイサイズやカメラ性能など）や筐体デザインなど端末を特徴付ける部分であるため，基本的には端末ごとにすべて異なるものである．対して，ソフトウェアは共通化できる部分が比較的多い．また，ハードウェアを直接操作するような端末機能ソフトウェアであっても，単体のAndroidアプリケーションとして端末依存なく動作させることも可能である．これらの特長を活かし，eSIM開通処理に必要となるLPA機能を具備したAndroidアプリケーション（以下，LPAアプリ）を共通化することが可能である．

そこで，従来端末メーカが開発していたLPAアプリをドコモが開発し端末メーカへ配布することとした（**図1**）．これにより端末メーカはLPA開発の負担が減り，ハードウェア開発や端末ラインナップの拡充に注力しやすくなり，ドコモもeSIM搭載端末の拡充に間接的に寄与することが可能となる．

また，ドコモがLPAアプリを開発することで，ドコモネットワークやサーバ装置類との連携部分の開発・評価の一元化による効率化や，アプリUIを端末間で統一し，ユーザ案内をしやすくするなどの副次的効果も生まれる．

2.2　eSIM開通におけるLPAアプリの役割

LPAアプリがもつ機能は，主に次の2つである（**図2**）．

- LPD（Local Profile Download）：SM（Subscription Manager）*6からプロファイル*7をダウンロードし，端末内のeSIMに格納・インストールする機能
- LUI（Local User Interface）：eSIM内のプロファイルの操作（一覧表示，切替え，削除など）を行うためのUIを提供する機能

LPA機能を端末上に実装する場合，eSIMの回線開通処理において当該端末がどのような役割を果たすかを考慮し，機能の配置を決定する必要がある．現行のGSMA仕様Version2［2］［3］では，次の2通

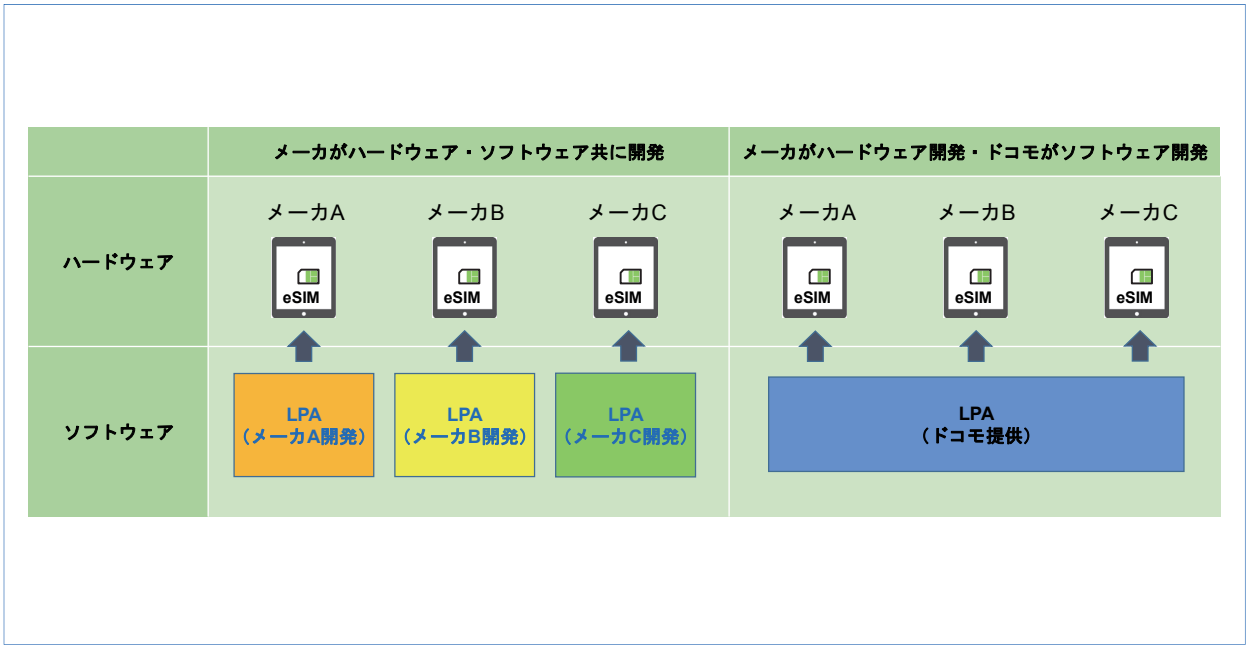

図1　ハードウェア・ソフトウェアの開発分担

*3　RSP：GSMAにて定義されたeSIM用の遠隔プロファイル書込み技術の総称．
*4　eSIM：遠隔でプロファイルをインストールできるSIMの総称．
*5　LPA：SMと連携しeSIMにプロファイルをダウンロードする機能や，プロファイルの切替えや削除などの管理機能を提供する端末機能．
*6　SM：プロファイルの生成・保持する機能や，プロファイルをLPA経由でeSIMにダウンロードしインストールさせる機能を提供するサーバ．
*7　プロファイル：eSIM OS上で動作するUIMソフトウェアであり，電話番号などの各種ファイル情報や，ネットワーク認証機能をもつアプリケーションなどから構成される．

りの機能実装方法が示されている（**図3**）．

1つめは，回線開通対象の端末にeSIMとLPA全機能が搭載されており，端末単体でeSIMの開通能力をもつ場合である．このような端末を，以下「単体デバイス」と呼ぶ．

2つめは，回線開通対象の端末にはeSIMおよびLPAの一部機能のみが搭載され，端末単体ではeSIMの開通能力をもたない場合である．この場合，

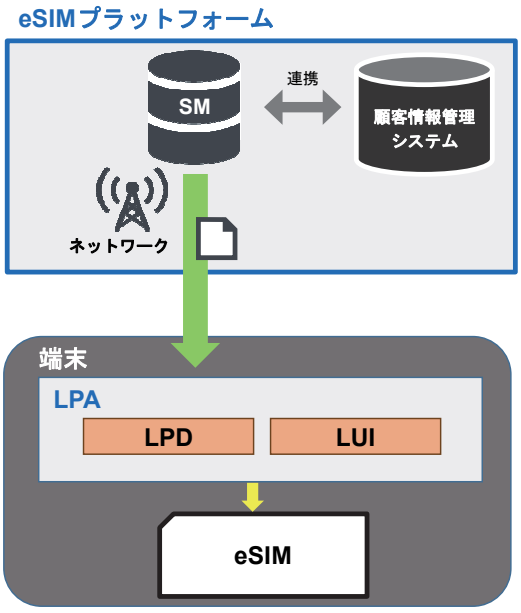

図2　eSIMプラットフォームとLPAアプリの概要

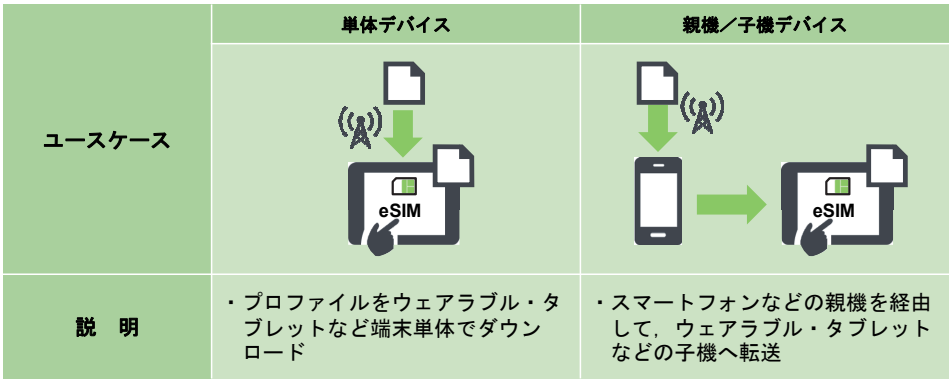

図3　単体デバイスと親機／子機デバイス

LPAの残りの機能を搭載した別端末と連動・協力して回線開通を行うことになる．以下，前者を「子機デバイス」，後者を「親機デバイス」と呼ぶ※1．

ドコモが開発したLPAアプリは，「単体デバイス」「子機デバイス」「親機デバイス」のすべてをサポートしている．

3. 単体デバイスモデル

3.1 単体デバイス向けLPAアプリの機能構成

単体デバイスモデルでは，当該端末1台のみでeSIM回線開通が可能であるため，単体デバイス向けLPAアプリはLPD，LUIのすべての機能を内包している．機能構成は図2の通りである．

ドコモの開発したLPAアプリは，GSMA仕様に準拠するのはもちろんのこと，どのAndroid端末上でもユーザが使いやすいアプリケーションとなるよう工夫されている．具体的には，使いやすさの向上のためセキュリティが確保されつつユーザ認証が極力簡素化されていることや，Androidのマテリアルデザイン＊8やセットアップウィザードに適合したUI設計がなされていることなどである．

3.2 単体デバイスにおける開通の仕組み

eSIMプラットフォームにおいては，端末とLPAアプリ以外の主な構成要素としてeSIMとSMが存在する．各要素の役割について簡単に解説する．詳細は過去の本誌記事［1］も参照されたい．

・eSIM：従来は，内部ファイル（電話番号や各種ユーザ識別子など）やネットワーク認証機能，各種アプリケーションからなるOP（Operational Profile）を「事前に」書き込んだ上でエンドユーザへSIMを配布していたのに対し，eSIMは，SMサーバから遠隔かつセキュアにOPをダウンロードすることにより，「後から」プロファイルの追加・変更が可能という特長がある．

・SM：ユーザごとのプロファイルデータを生成・保持する．LPAからのプロファイルダウンロード要求に基づき，該当ユーザのプロファイルの準備および目的のeSIMへのセキュアなダウンロードを行う．

これら要素が連携することで，eSIM回線開通が可能となる．OPがeSIMにダウンロードされるまでの一連の手順概要を**図4**に示す．

①端末電源ON時，端末がeSIM内のプロファイル情報を読み出す．eSIM内にOPが1件もない，すなわち回線未開通の場合は，自動的にPP（Provisioning Profile）＊9が読み出される．PPによりパケット通信呼が確立され，端末はSMへの接続が可能となる．

②LPAアプリを起動する（通常は端末のセットアップウィザード内でLPAアプリが自動的に呼び出される）．LPAアプリはSMへ接続し，HTTPS通信セッション＊10を確立する．この際LPAアプリ自身で保持する証明書を利用してサーバ証明書＊11の検証を行うことにより，SMの正当性確認を行っている．これにより，ユーザデータを端末から不正ななりすましSMにアップロードしてしまったり，不正なプロファイルデータをなりすましSMからダウンロードしてしまう，といった事故を防止できる．

③LPAアプリが②で作成した通信路を介してeSIMとSMが相互認証を行い，eSIM―SMの2者間でEnd-to-endのセキュアな暗号通信路を確立する．この通信路上でeSIMがSMからプロファイルをダウンロードする．プロファイルはLPAアプリのLPD機能にいったんダウンロードされた後，LPD機能からeSIMへ分割送信される．これは，端末―eSIM間の通信インタフェースにおけるメッセージサイズ上限があるためである．分割プロファイルはeSIM内で結

※1 GSMA仕様［2］［3］においてはそれぞれのデバイスを「Companion Device」「Primary Device」と呼称している．

＊8 マテリアルデザイン：Androidにおいて推奨されている，アプリケーションのグラフィック，画面構成や操作感など，デザイン全般におけるガイドライン．

＊9 PP：OPをダウンロードする際に用いる専用プロファイル．他用途に利用することはできない．

＊10 セッション：クライアントとサーバ間でやり取りされる一連の通信のこと．

＊11 サーバ証明書：サーバ所有者情報，暗号化鍵，証明書発行者の署名データをもった電子証明書．

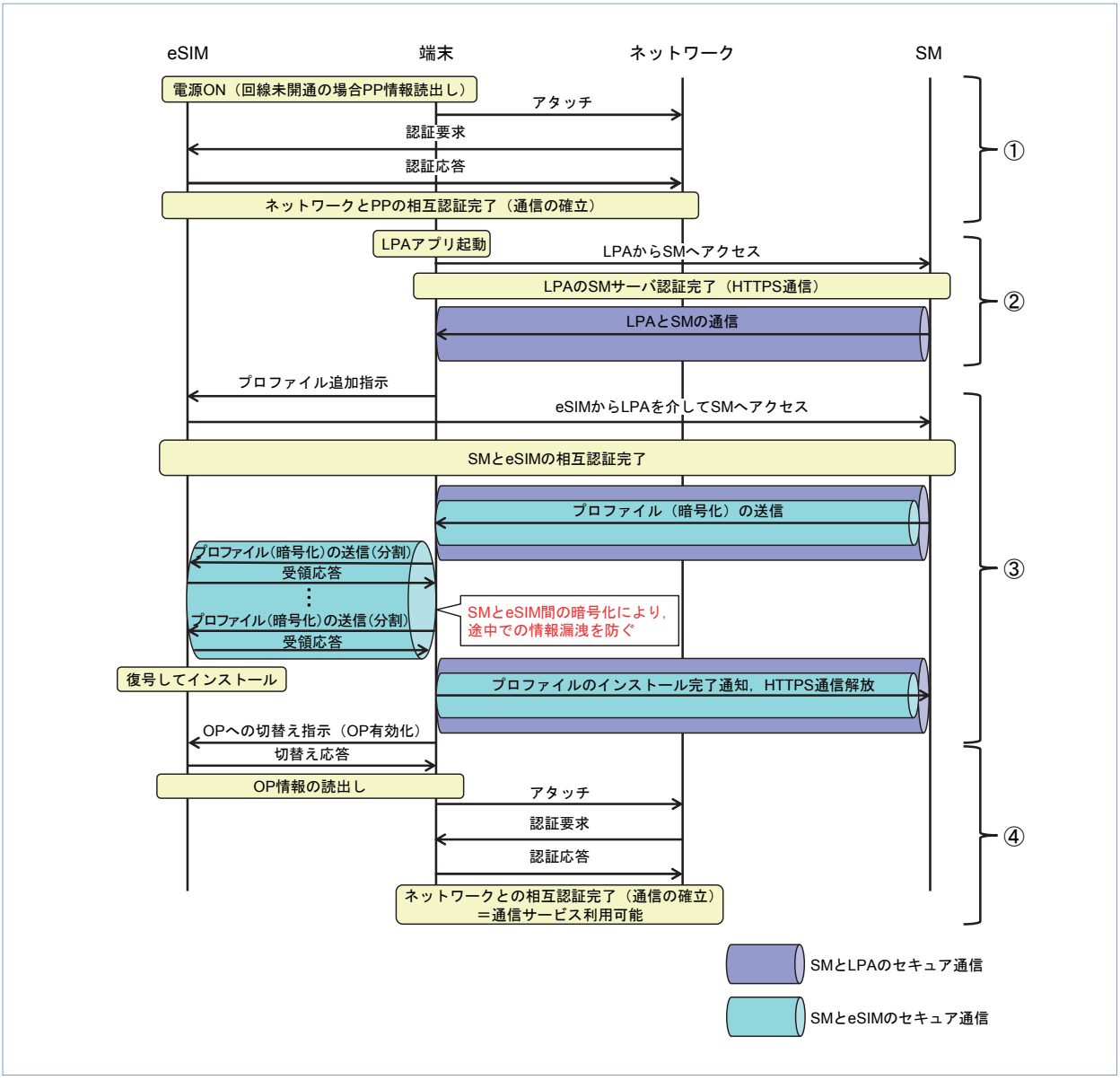

図4　単体デバイスの開通シーケンス

合，復号化した後にインストールされる．

④LPAアプリからインストール済みプロファイルを有効化すると，端末はOPを利用して再度ネットワークへアタッチ[*12]し，通話やパケット通信などの各種サービスが利用可能となる．

4. 親機・子機モデル

4.1　子機デバイスにおけるeSIM搭載のメリット

親機・子機モデルの代表的なユースケースとしては，ウェアラブル端末や車載機器など単体では

＊12 アタッチ：移動端末の電源投入時などにおいて，移動端末をネットワークに登録する処理．

eSIM回線開通処理が困難な端末（子機デバイス）のeSIM回線開通を，開通手続き処理に必要となる入力操作や画面表示などUI表現に適したスマートフォン端末（親機デバイス）を経由して行うといったケースが挙げられる．

一般的に子機デバイスでは，端末内に固定された埋込み型eSIMが搭載されることが多い．埋込み型の場合は従来の挿抜型とは異なりSIMスロットが不要となるため，ハードウェア実装体積が削減できる，防水・防塵機構と相性が良いなどのメリットがある．さらに子機デバイスでは，eSIM回線開通に伴う操作・諸手続きを親機デバイスに肩代わりしてもらうことにより，タッチパネルやキーボードなどの入力機器の省略やディスプレイサイズの縮小など，機器自体の目的に特化したハードウェア・ソフトウェア設計を実現することが可能となる．

また，回線開通を親機デバイス経由によってオンラインで行うことになるため，従来の端末とは異なり「端末の入手」と「セルラ回線の開通」を分けて扱うことができるという点は，これまでの端末にはなかった特長である．これにより子機デバイスは，従来のキャリアショップや量販店だけではなく，さまざまな販路で自由に流通できるようになる可能性がある．

4.2 ドコモにおける子機デバイスの開発

ドコモでは，2018年冬モデルとして「ワンナンバー＊13フォン＊14 ON 01」を開発した（**写真1**）．ワンナンバーフォンはeSIMを搭載した子機デバイスであり，親機デバイスのAndroidスマートフォンを経由してeSIMへのOPダウンロードが可能である．これにより，ワンナンバーフォンは電話機能に特化した小型設計を実現している．

また，ワンナンバーフォンはGSMA Compliance Process［4］による認定を受けた世界初のeSIM子機デバイスである※2．

4.3 子機デバイス向けLPAアプリの機能構成

親機デバイス向けLPAアプリ（以下，親機アプリ）と子機デバイス向けLPAアプリ（以下，子機アプリ）は，単体デバイス向けLPAアプリをベースとして開発された．LPAの主要機能を親機アプリと子機アプリに分割した上で，親機アプリ―子機アプリ間でBluetooth®＊15通信によるリアルタイム連携する仕組みとしている．構成概要は**図5**の通りである．

写真1　ワンナンバーフォン ON 01

＊13 ワンナンバー：1つの電話番号を，スマートフォンなどの親機デバイスと，アクセサリ端末などの子機デバイスとで共有して，どちらの端末でも音声通話・データ通信が使用できるサービス．

＊14 ワンナンバーフォン：NTTドコモの商標または登録商標．

＊15 Bluetooth®：移動端末，ノートPC，PDAなどの携帯端末向け短距離無線通信規格．米国Bluetooth SIG Inc.の登録商標．

※2　2018年10月23日現在．ドコモ調べ．

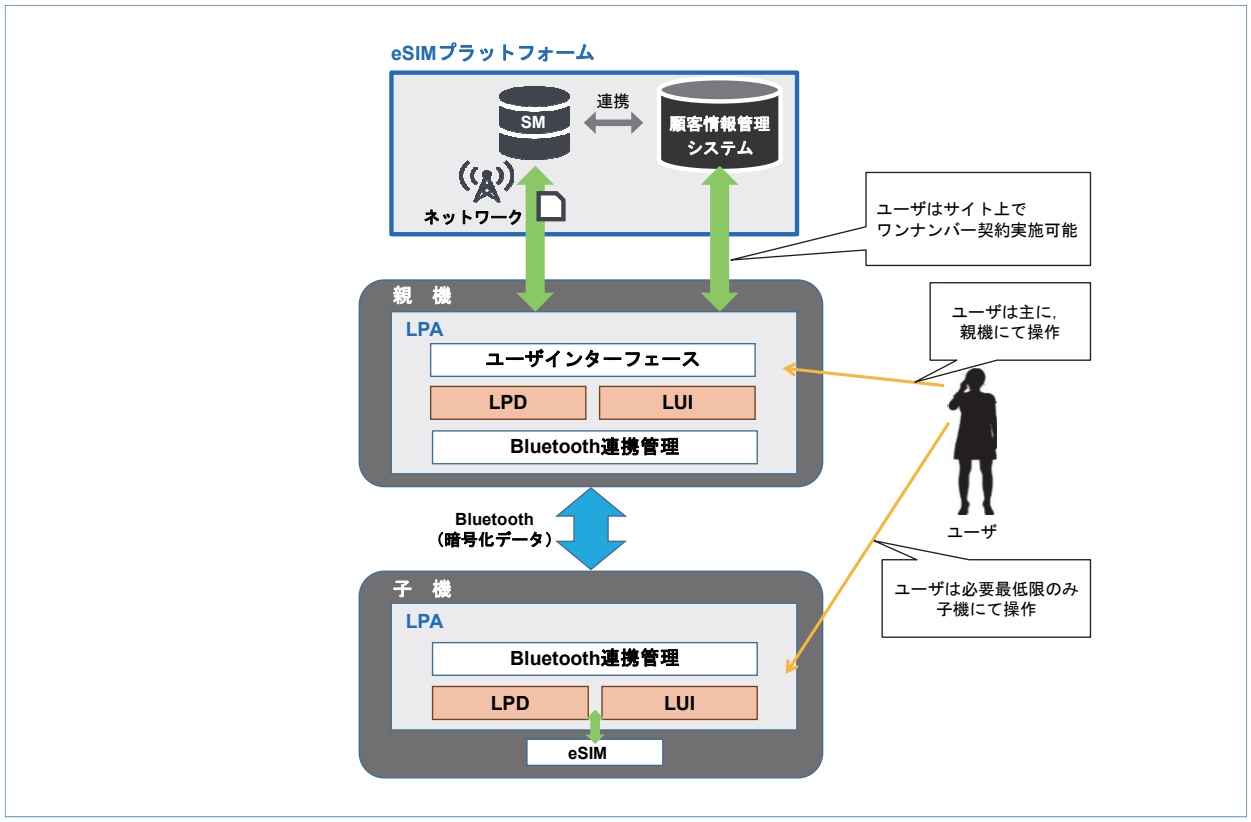

図5　親機・子機モデルにおけるLPAアプリの構成

4.4　子機デバイスにおける開通の仕組み

子機デバイスにおけるeSIM開通においては，単体デバイス開通で登場した構成要素に加え，新たに顧客情報管理システムとの連携が必要になる．本システムは親機デバイス回線利用者のワンナンバーサービス®＊16契約状態の管理や，未契約の場合にオンラインで即時契約手続きを行うなどの機能をもつ．

子機デバイスにおける開通シーケンスを**図6**に示す．親機デバイスにはセルラ通信可能なSIMがすでに挿入されており，パケット通信の呼が確立されている前提とする．

①親機アプリ，子機アプリの両方を起動する．

②親機アプリがAndroidのBluetooth機能を用いて，親機デバイスと子機デバイスをBluetoothペアリング＊17する．これにより，Bluetooth通信セッション内で，親機アプリと子機アプリが直接セキュアに連携動作することが可能となる．

③親機アプリが顧客情報管理システムに接続し，ワンナンバーサービスの契約状態を確認する．未契約の場合は，そのまま契約手続きを行う．

④親機アプリのLPD機能がSMへアクセスし，セキュアなHTTPS（HyperText Transfer Protocol Secure）＊18通信を確立する．

⑤すでに確立済みの子機アプリ―親機アプリ間のBluetooth通信および親機アプリ―SMサーバ間のHTTPS通信の2つを経由し，子機デバイス上のeSIMとSMが相互認証を行い2者間のセキュアな暗号通信路を確立する．これにより，伝送路上のインターネット回線はもちろん，親機ア

＊16　ワンナンバーサービス®：NTTドコモの登録商標．

＊17　ペアリング：Bluetoothにて，接続相手を特定するための手順．一度ペアリングを行った機器間では，次からは，自動的あるいは半自動的に接続が確立される．

＊18　HTTPS：TLSプロトコルを用いて，HTTP通信を安全に行う通信手法．なりすまし・中間者攻撃・盗聴などの攻撃を防ぐことができる．

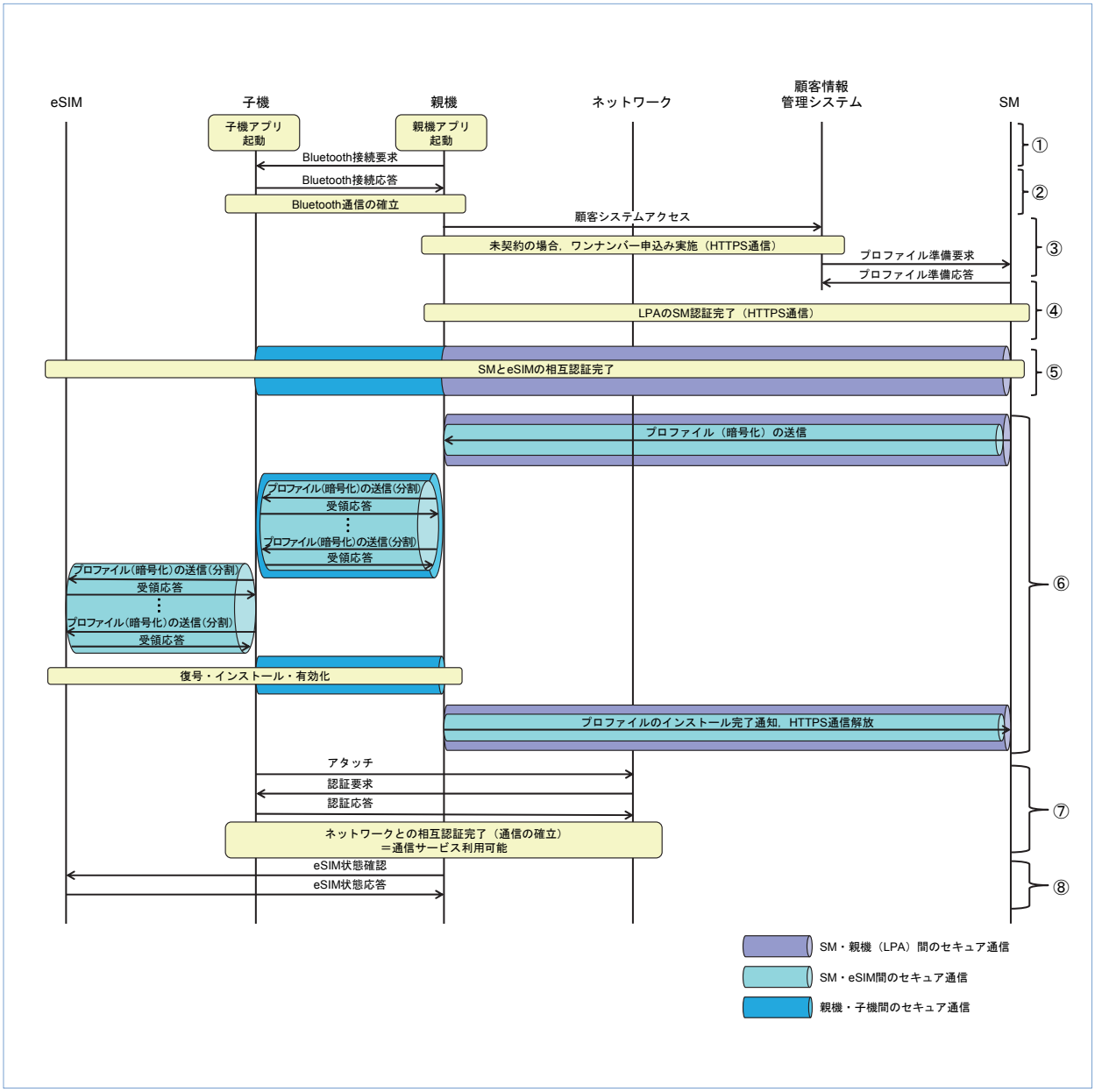

図6　子機デバイスの開通シーケンス

プリや子機アプリであってもプロファイル情報を盗聴・改竄することはできなくなり，eSIMにダウンロードされるプロファイルの正真性が保証される．

⑥親機アプリのLPD機能は，SMから暗号化されたプロファイル情報をダウンロードした後，子機アプリのLPD機能へプロファイル情報を分割送信する．これは，親機―子機間のBluetooth通信におけるメッセージサイズ上限があるためである．子機アプリのLPD機能は，受け取っ

たプロファイル情報をeSIMへ分割送信し，OPをeSIMにインストールする．

⑦OPが正しくインストールされると，子機デバイスはネットワークへアタッチを行う．これにより，子機デバイス単体でセルラ通信が可能となる．

⑧親機アプリのLUI機能から子機アプリのLUI機能を経由してeSIMにアクセスすることで，eSIM内部状態の確認（インストール済みのOP情報の閲覧など）を行うことも可能である．

ワンナンバーフォンにおいては，上記手順の後に親機デバイス内の電話帳データを子機デバイスにコピーするという機能も実装している．ワンナンバーサービスにより電話やSMSを親機／子機どちらの端末でもシームレスに利用できるよう工夫している．

5. あとがき

ドコモは今後のeSIM対応機器の拡大を見据え，グローバル標準の要求仕様であるGSMA RSPに準拠したLPAアプリケーションを開発した．単体デバイス向けLPAアプリにより，従来型のAndroidスマートフォン／タブレットへのeSIM搭載の促進が期待できる．また，親機デバイス／子機デバイス向けLPAアプリの実現により，ウェアラブルをはじめとするさまざまなIoT機器へのセルラ通信能力付与，およびこれら機器特有のユニークなユースケースの創出にも寄与していくものと考えられる．

今後はGSMAで策定中の次期RSP仕様へ対応したLPAアプリケーションの継続開発や，eSIM搭載IoT機器の拡充および新たなユースケースの創出など，コンシューマ機器向けeSIM技術を利用したより便利な通信サービスの提供に取り組んでいく．

文　献

[1] 笹川，ほか：“利用シーンを拡大するコンシューマ機器向けeSIMの導入―GSMAに準拠したセキュアなインストールを実現―，”本誌，Vol.25，No.2，pp.6-12，Jul. 2017.

[2] GSMA SGP.21：“RSP Architecture Version 2.1,” Feb. 2017.

[3] GSMA SGP.22：“RSP Technical Specification Version 2.1,” Feb. 2017.

[4] GSMA SGP.24：“RSP Compliance Process Version 1.1,” May 2017.