Technology Reports

コンシューマ向けeSIM　LPA　SM

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—

移動機開発部　笹川 哲広（ささがわ てつひろ）† 秋山 友宏（あきやま ともひろ）　ネットワーク開発部　嘉義 智紀（かぎ とものり）
プロダクト部　上田 健介（うえだ けんすけ）　井ノ上 晶浩（いのうえ あきひろ）

ドコモでは，ユーザの端末操作をトリガにプロファイルのインストールを行うコンシューマ機器（端末）にLPA機能の追加を行い，ネットワーク，SMからなる基盤を構築して，GSMAに準拠したコンシューマ機器向けのeSIMサービスを国内ではじめて導入した．本稿では，コンシューマ機器においてセキュアなインストールを実現するために今回開発したeSIM，LPA機能，ネットワークおよびSMの仕組みについて解説する．

1. まえがき

近年，ウェアラブル端末に代表されるようなさまざまな形状のコンシューマ機器（端末）が増加しており，これらの端末自身にセルラ通信機能を搭載し簡易に開通できるような仕組みに対するニーズが高まっている．そこでドコモは，タブレットやウェアラブル端末などのコンシューマ機器を対象に，通信サービスの利用に必要なプロファイル[*1]を遠隔でeSIM（Embedded Subscriber Identity Module）[*2]にインストールすることができるLPA（Local Profile Assistant）[*3]機能を搭載した端末，ネットワークおよびSM（Subscription Manager）[*4]を開発した．ドコモではネットワーク，SMなどからなるeSIMサービスを提供する基盤を「eSIMプラットフォーム[*5]」と呼んでいる．

本稿では，サービス導入にあたって開発したコンシューマ機器向けeSIM，端末，eSIMプラットフォームの仕組みについて解説する．

2. コンシューマ機器向けeSIMとは

コンシューマ機器向けeSIMは，ユーザの端末操作をトリガとしてSMからセキュアにプロファイルのインストールを行うことができるeSIMである．形状については，原義からすれば機器にembedded

† 現在，プロダクト部

＊1 プロファイル：eSIM OS上で動作するUIMソフトウェアであり，電話番号やIMSI（＊12参照）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．OPとPPの2種類が存在．
＊2 eSIM：遠隔でプロファイルをインストールできるSIMの総称．

された（組み込まれた）SIMを指すが，GSMA RSPバージョン2の定義上，チップ形状だけでなくカード形状も含む．導入メリットや標準化動向，M2M機器向けeSIMとの差分などについて以下に解説する．

2.1 導入メリット

従来，コンシューマ機器で通信サービスを利用可能にするためには，UIM（User Identity Module）*6カード用リーダライタなどを用いてUIMカードへプロファイルを記録し，その後，UIMカードを端末に挿入する必要があった（**図1**(a)）．

一方，コンシューマ機器にeSIMを用いると，次のメリットがある．

・あらかじめUIM機能を端末に内蔵させておくことができ，UIMカード抜差しの手間が不要となる（図1(b)）．
・手元に特別な機器（リーダライタ）がなくとも開通作業ができるため，端末さえ入手すれば，速やかに通信サービスの利用が可能となる．
・従来，オンラインショップで端末を購入し，購入と同時にUIMカードの発行が必要となる場合には，回線利用開始のために電話手続きによる開通処理，もしくは別途PCなどを利用してのWeb手続きによる開通処理をユーザが行う必要があった．eSIMでは，購入した端末の初回起動時における端末初期設定の中で，ユーザはガイドに従った簡易な端末操作のみで開通処理が可能になる．
・UIMカードが脱着不要となるため，カードスロット部分を省略でき，端末デザインの自由度が増す．ウェアラブル端末などの小型機器でもセルラ通信サービスへ対応し易くなる．

これにより，ユーザがより簡単に通信サービスを利用可能になり，利便性が向上する．一方従来

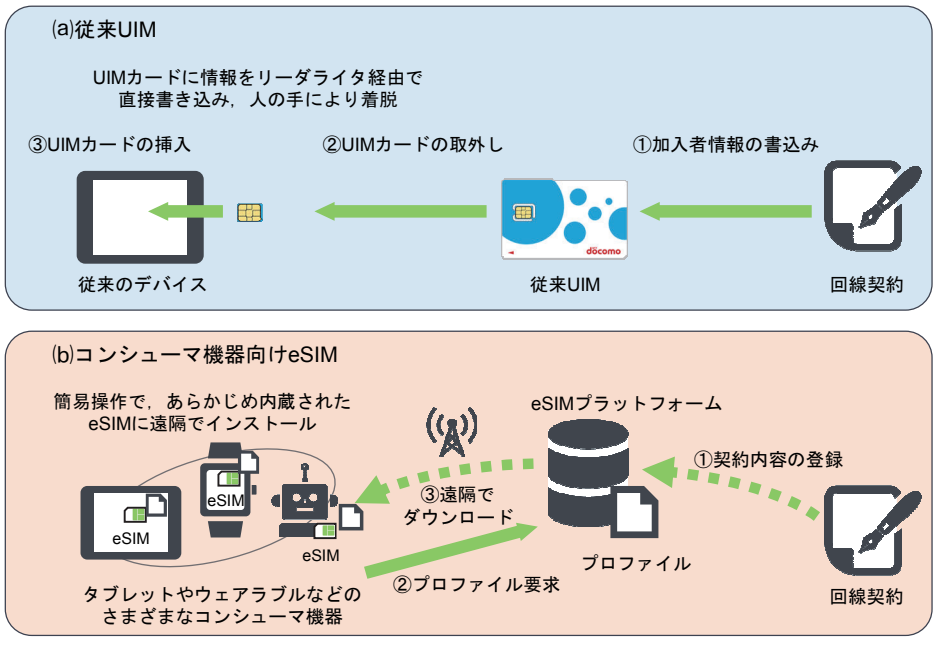


図1　従来UIMとコンシューマ機器向けeSIMの違い

*3　LPA：主にLPDとLUIの2つの機能から構成され，SMからeSIMへプロファイルをダウンロードする際に中継する機能や，ユーザがプロファイルのダウンロード，削除，切替えなどをする際のUI機能を提供．
*4　SM：オペレータ情報管理システムと連携するサーバ．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．
*5　eSIMプラットフォーム：ネットワーク，SMなどからなるeSIMサービスを提供する基盤．これを導入することで，対応端末は，あらかじめ端末に内蔵されたeSIMに対し，ユーザの端末からの操作によってプロファイルをネットワーク経由でインストールすることが可能となる．

UIMについては，例えば機種変更する場合や端末故障時に機種を取り替える場合などにおいては，ネットワークを介さずに簡易にUIM情報の切替えができるメリットもあるため，今後も従来UIMとeSIMは用途に応じて併用されていくものと考えられる．

2.2 標準化への対応

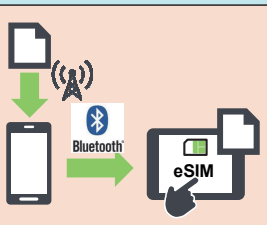
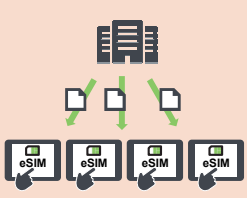
コンシューマ機器向けeSIMは主にGSMA（GSM Association）[*7] RSP（Remote SIM Provisioning）[*8]会合にて標準化活動が行われている．**図2**に示す通り，2016年10月に一般公開されたバージョン2までの仕様に加えて，現在はバージョン3として，エンタープライズ用途でのコンシューマ機器向けeSIM機器の利用に向けた仕様の拡張などについて，GSMA RSP内で議論中である．

ドコモは，日本のモバイル市場の特性を踏まえ，本会合においても接続先SMの指定方法や，ダウンロードするプロファイルと端末能力の判定機能に関する規定など，さまざまな提案を行い，それらの多くが仕様に反映されている．なお，今回の開発はGSMA RSP仕様バージョン2に準拠しており，標準化作業に深く関わることで早期の開発，商用化を実現している．

2.3 M2M機器向けeSIMとの比較

近年，M2M（Machine to Machine）[*9]機器の増加に伴い，耐久性などの観点から取外しができない組込み型のUIM（MFF（M2M Form Factor）[*10]形状）の利用が増加している．また，グローバルにビジネス展開を行う際は，製造時に1種類のUIMを組み込み，M2M機器が利用される国に応じて，通信（サービス）事業者を随時書き込み出荷することで，生産および管理の効率を向上させたいというニーズが高まっている．このような背景に対応すべく，ドコモでは2014年6月に，法人M2M市場向けに「docomo M2Mプラットフォーム[*11]」サービスを開始した［1］．

一方，コンシューマ機器においては，ユーザ自らの端末操作によってプロファイルをダウンロードする必要がある（**図3**）．そのため，端末側には後述するLPA機能を搭載し，eSIMへプロファイルをダ

仕様書バージョン	バージョン1	バージョン2	バージョン3
仕様書公開時期	2016年1月	2016年10月	議論中
ユースケース	2台目にプロファイルをダウンロード	1台目にプロファイルをダウンロード	プロファイルのプッシュ配信など
			
特　徴	• スマートフォンなどを経由して，ウェアラブル・タブレットなどのセカンダリデバイスへ転送	• プロファイルをウェアラブル・タブレットなどデバイス単体でダウンロード • 複数プロファイルのインストール対応	• 法人の，大量デバイスへのキッティング※などをサポート

※キッティング：携帯電話などの端末に対してアプリケーションのインストールや各種設定・登録などを行い，ユーザが即座に使える状態にする作業．

図2　GSMA RSPのユースケース例

＊6　UIM：電話番号やネットワーク認証鍵などの情報をもち，端末が通信ネットワークに位置登録する際のユーザ認証機能などを提供．SIMと同義．

＊7　GSMA：携帯電話事業者のほか，端末メーカー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．

＊8　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．

＊9　M2M：機器間の通信を意味する．人間の介在なしに機器同士がコミュニケーションして動作するシステム．

ウンロードする機能を提供している．

3. コンシューマ機器向けeSIMを実現する仕組み

コンシューマ機器向けeSIM（以下，eSIM）と端末およびeSIMプラットフォームを構成する各要素を**図4**に示し，以下に解説する．

3.1 eSIM

従来のUIMは**図5**(a)に示すように，UIMチップ，UIM OSの上に，各ファイル（電話番号やIMSI

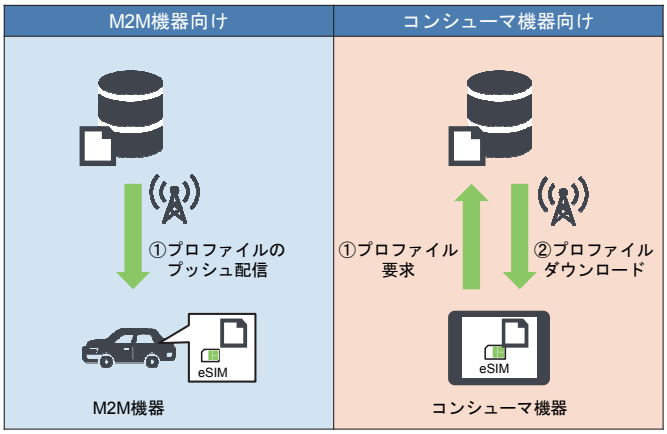


図3　M2M機器向けeSIMとコンシューマ機器向けeSIM

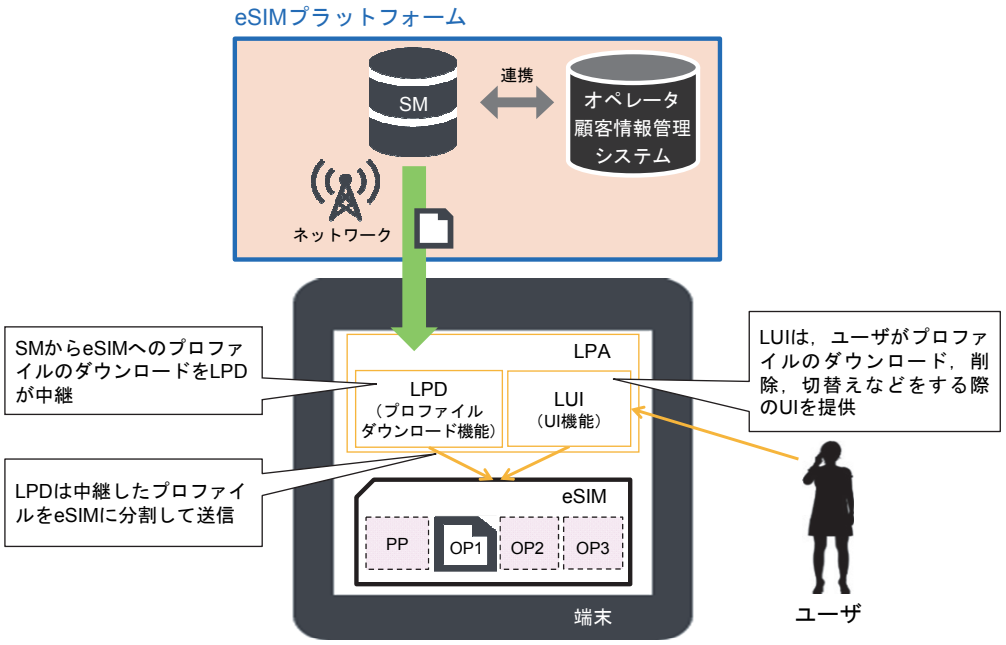
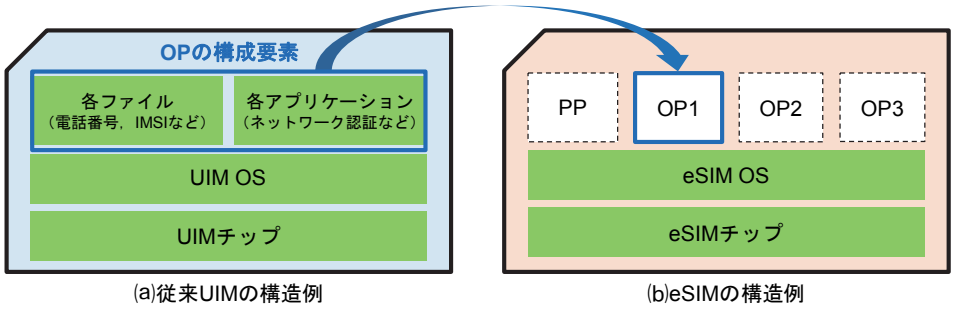


図4　eSIMと端末およびeSIMプラットフォームを構成する各要素

＊10 MFF：ETSI（European Telecommunications Standards Institute）で定義されたM2M機器向けのUICC（Universal Integrated Circuit Card）形状を指す．

＊11 ドコモM2Mプラットフォーム：ドコモが2014年6月に提供開始した法人M2M機器向けのeSIMソリューション．



(a)従来UIMの構造例　(b)eSIMの構造例

図5　従来UIMとeSIMの構造例

（International Mobile Subscriber Identity）[*12]などの情報を含む）やネットワーク認証機能などを含めた各アプリケーションからなるOP（Operational Profile）で構成されている．

また，従来のUIMでは，UIM内の情報を書き換える技術として，USAT（Universal Subscriber identity module Application Toolkit）[*13]機能がある［2］．この機能は一般にUIM内のファイルやアプリケーションを部分的に更新することが目的であった．

一方，eSIMは，SMからOPを遠隔でセキュアにインストールする機能をもつことで，ネットワーク認証用の秘密鍵などの秘匿情報を含めたOP単位での更新が可能となった（図5(b)）．

また，eSIMの容量が許す限り複数のプロファイルをeSIM内に保存することができるが，通信に利用可能なプロファイルは常に1つである．ユーザはLPAを用いることによって，どのプロファイルで通信するかなど，eSIM内のプロファイルを制御することも可能である．

保持するプロファイルにはPP（Provisioning Profile）という種別も存在する．OPが従来のUIMのソフトウェアと同様にユーザへサービス提供を行うためのプロファイルであるのに対し，PPはOPをダウンロードするためのプロファイルである．PPでは，OPのダウンロード以外の利用を制限している．

3.2　端末（LPA）

LPAがもつ主な2つの機能を以下に示す（図4）．

・LPD（Local Profile Download）：SMから暗号化されたプロファイルを一括してダウンロードし，そのプロファイルをeSIMに対して分割して送信しインストールする機能．端末とeSIM間のIFは低速であるため，LPDにて一括ダウンロードすることでモバイルネットワークを利用した通信時間短縮を実現している．

・LUI（Local User Interface）：ユーザの操作でeSIMを制御（プロファイルのダウンロード，削除，切替えなど）するためのUIを提供する機能．

これらの機能をもつLPAを用いることで，SMからの効率的なプロファイルダウンロードやユーザの端末操作を契機としたプロファイル制御が実現可能となる．

3.3　ネットワーク

PPを利用してSMと通信を行い，OPをダウンロードすることにより，音声やパケット通信などのサービスが提供可能となる．

＊12 IMSI：UIM内に格納される，移動通信で使用するユーザごとに固有の番号．
＊13 USAT：遠隔でUIM内の情報を更新する際などに用いられる3GPP TS31.111で規定された標準仕様．

PP利用中は，在圏は可能であるが契約としては未契約の扱いであるため，音声やSMS，その他サービスについてはネットワーク側で規制を行う．

SMとのパケット通信のみ可能とする通信規制については，ダウンロード通信用のAPN（Access Point Name）*14を設け，そのAPNにてSMのURL以外へのアクセスの規制を行うことで実現する．ただし，ユーザが使用する端末にSM通信用のAPNが設定されているか不明であり，これに対して，ユーザがSM通信用のAPNを手動で設定することも可能だが，手間がかかってしまう課題があった．

対策として，**図6**に示すとおり，MME（Mobility Management Entity）*15やSGSN（Serving General packet radio service Support Node）*16にてPPでのパケット通信ということを認識した場合，端末がどのAPNを指定したとしてもESPGW（EPC Serving and PDN GateWay）*17にてSM通信用のAPNに強制変換し接続，MAPS（Multi Access Platform System）*18にてSM以外の通信を規制することで，ユーザは意識せずにSMにのみ接続することが可能となる．

SMと通信し，OPをダウンロードした後は通常のユーザと同様に，契約条件に応じたサービス提供を行うことが可能となる．

3.4 SM

eSIM用のSMでは主に，プロファイルの生成・保持機能およびプロファイルをセキュアにインストールする機能を提供する．

・プロファイルの生成・保持

ユーザとオペレータ間で回線契約が成立した後，通信サービス利用に必要となるプロファイルが，今回開発したSMサーバから対象のeSIMに対してダウンロードできるよう準備される．

SMではオペレータの顧客情報管理システムから電話番号やIMSI，ネットワーク認証鍵などの情報を受け取り，プロファイルを規定に従って生成し，そのプロファイルを暗号化された形でセキュアに保持する．

・プロファイルのインストール

インストールされるeSIMでのみ復号ができるように該当のプロファイルを暗号化する．この暗号化されたプロファイルをLPA経由でeSIMに対してインストールする．eSIMプラッ

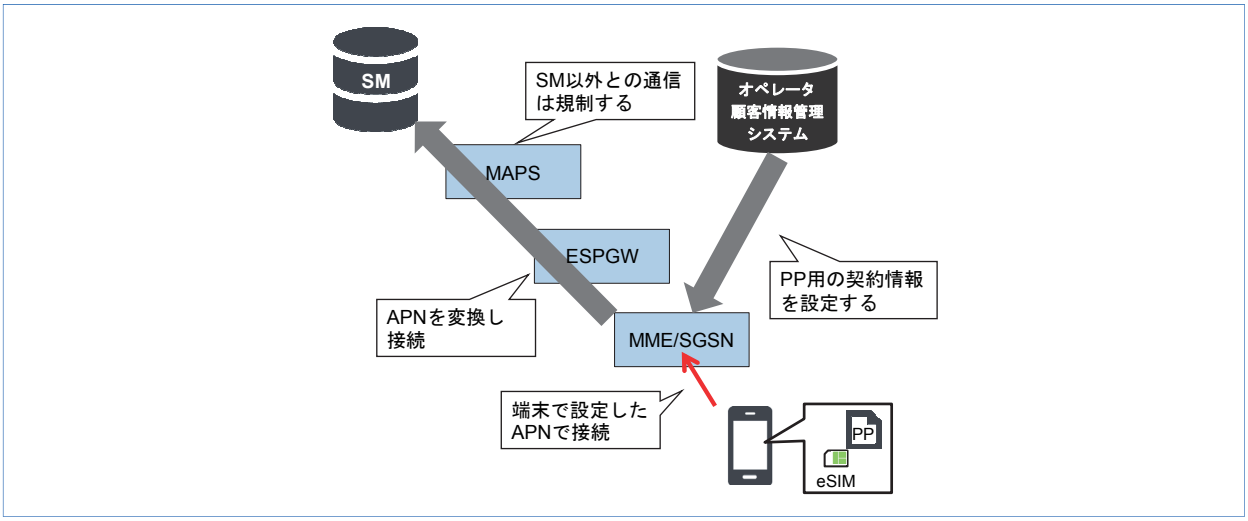


図6　PPからSMへの通信の制御

＊14 APN：ネットワーク接続によりデータ通信を行う際，接続先として設定するアドレス名．
＊15 MME：基地局（eNodeB）を収容し，モビリティ制御機能などを提供する論理ノード．
＊16 SGSN：パケット通信を行う移動端末の移動制御を行う論理ノード．
＊17 ESPGW：S-GW，P-GWの能力をもつ装置．
＊18 MAPS：さまざまなアクセス回線から，インターネット接続や企業システム接続を提供するプラットフォーム．

トフォームのシステムはPKI（Public Key Infrastructure）[*19]をベースとした強固なセキュリティが担保されている．eSIM/LPA/SMのそれぞれに，信頼できる認証局（Certificate Authority）から払い出された証明書を保持しており，システム間で通信を行う際には証明書をベースとした認証が行われる．

3.5 プロファイルダウンロードシーケンス例

これらの仕組みを用いてプロファイルがSMからネットワークおよび端末（LPA）を経由してeSIMにインストールされるまでのシーケンスについて一例を**図7**に示す．

①eSIMを格納した端末の電源をONし，PPを用いて，パケット通信の呼を確立する．

②端末内のLPAがSMにアクセスし，LPAとSMの証明書を基にHTTPSの通信を確立する．SMへのアクセスが許可された証明書をもつLPAのみがアクセス可能となる．

③SMとLPAの通信路が確立されると，eSIMとSMはLPAを介して相互認証を行う．この相互認証の中でeSIMとSM間に閉じたセキュアな通

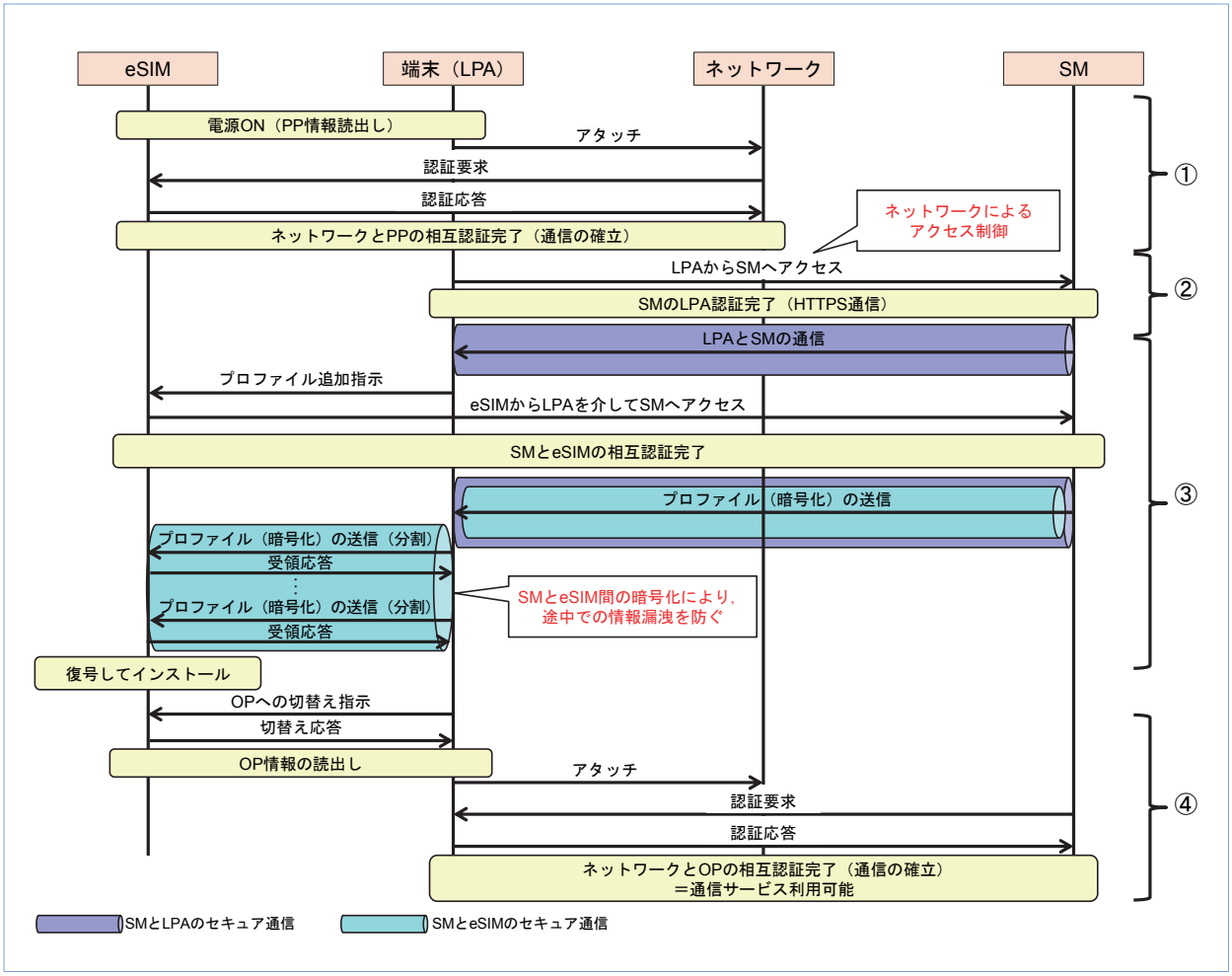


図7　プロファイルダウンロードシーケンス例

＊19 PKI：公開鍵暗号技術を用いて，安全な通信を行うようにするために構築されるシステムなどの総称．

信路を確立し，端末やLPAでプロファイル情報などが漏えいすることなくプロファイルをeSIMへインストールする．この際，前述のとおり，LPDにて一括ダウンロードした後，eSIMに対して分割送信しインストールを行うことでモバイルネットワークを利用した通信時間の短縮に貢献している．

④プロファイルのインストール後はLPAからの操作によってプロファイルの切替えや削除なども可能となり，OPを用いて各種通信サービスを利用できる．

4. あとがき

ドコモでは，幅広い用途での活用および低コストでの提供を念頭に，グローバル標準の要求仕様であるGSMAに準拠したeSIMプラットフォームを開発した．

eSIMは端末に組み込まれた状態での利用が想定され，例えば端末のネットワーク接続機能を確認する試験などにおいては従来のカード形状のUIMスロットを有する端末であればテスト用UIMを挿し替えることで対応できたが，eSIMのようにUIMの抜差しができない場合にはテスト用UIMが使用できないため新たな課題となり得る．すでに公開済みのGSMA RSP仕様バージョン2においても，テスト環境の整備など一部は継続議論中である．今後はそのような標準化動向も踏まえつつ，飛躍的に拡がる多様な端末に対し本プラットフォームを活用し，ユーザがより便利に通信サービスを利用できるよう，取り組んでいく．

文　献

[1] 鈴木，ほか：“Embedded UICC Remote Provisioningの標準化状況，”本誌，Vol.22，No.2，pp.36-41，Jul. 2014.

[2] 南，ほか：“UIMバージョン3の開発，”本誌，Vol.15，No.1，pp.24-29，Apr. 2007.

[3] GSMA SGP.21：“Architecture Specification - V2.0，”Aug. 2016.

[4] GSMA SGP.22：“Technical Specification - V2.0，”Oct. 2016.