IIJにおけるeSIMの取り組み

3.1 eSIMとは何か

2018年9月にiPhone XSが発表されて以降、eSIMというキーワードがよく聞かれるようになりました。本リサーチでは、eSIMの技術的な説明、及びIIJとしての取り組みについて説明します。

従来のSIMカードは以下で構成されており、これらを耐タンパ性を持ったパッケージにして製造されています。

- **モバイルサービスを提供するために必要なデータ**
- **SIMに付加価値を持たせるアプレット**
- **データとアプレットを安全に保持するためのストレージ**
- **認証処理、暗号鍵生成などの処理を行うプロセッサ**

特に認証や暗号化に使用する鍵情報は、SIMの外部から直接読み出すことが不可能な仕組みとなっています。

これに対しeSIMは、データとアプレットから構成されるプロファイルと、ストレージとプロセッサから構成されるeSIMカードの2つに分離し、プロファイルを専用のサーバからネットワーク経由でeSIMカードに書き込めるようにしました。この仕様は、業界団体であるGSMA[*1]で策定されました。プロファイルをネットワークから書き込むための仕組みをRSP(Remote SIM Provisioning)と呼びます。RSP自体は、従来のSIMにおいても、OTA(Over the Air)によるリモートからSIM内のデータを変更する手段として使われています。IIJでも、フルMVNOで提供している一部のSIMカードに対して、回線開通のタイミングで電話番号を書き込むために、OTAを利用しています。

eSIMという単語はEmbedded Subscriber Identifier Moduleの略で、組み込み用のSIMという意味です。現在では、RSPを利用してネットワーク経由でプロファイルを書き込むことが可能なSIMを指す言葉として用いられる場合がほとんどです。背景として、組み込み用途に使用されるSIMに対して、ネットワーク経由でプロファイルを書き込む仕組みが要求されたからです。

組み込み用途では、一般的なカードタイプのSIMではなく、基盤に直接ハンダ付けするチップタイプのSIMが使われる場合があります。理由として、チップタイプのSIMに次のようなメリットがあるからです。

- **産業用機器などをターゲットとしているため、高い耐久性を持つ**
- **基盤にハンダ付けされており、振動による接触不良が発生しにくい**
- **製造時に基盤にハンダ付けされるため、SIMカードを挿す工程を省略できる**
- **部品サイズが小さく、デバイスの小型化ができる**

なお、IIJでは上記のメリットを享受できるよう、2019年2月より、フルMVNOのSIMのラインナップにチップタイプのSIMを追加しています。

上記のようなメリットのあるチップタイプのSIMですが、製造時にデバイスに組み込むため、後からSIMを変更することが事実上不可能です。このため、使用するモバイル回線を製造時に決めておく必要があり、以下のような問題点を抱えています。

- **輸出先が異なる製品の在庫を共通化できない**
- **製品製造時の動作確認をする場合も正規契約の回線を使う必要がある**
- **製品を使用する場所が移動してもモバイル回線を切り替えることができない**
- **通信コスト削減などの理由でモバイル回線を切り替えることができない**

＊1　携帯通信事業者の業界団体「GSM Association」の略称。2Gの通信方式「GSM」の普及を目的に1995年に設立。約800社の携帯電話事業者を中心に、220ヵ国1000社以上が参加している業界最大の団体。毎年2月に開催される世界最大規模のモバイル関連展示会「Mobile World Congress (MWC)」の主催団体としても知られている。

一方で、カードタイプのSIMを採用した場合、上記の問題点は解消されますが、カード交換の現地作業コストが発生します。

上記のような問題点を解消するために、eSIMは作られました。プロファイルを後から書き込み可能なため、組み込み時にモバイル回線を契約しておく必要がなくなります。また、リモートからプロファイルを書き込み可能なため、SIMの交換に関する現地作業コストもなくなります。

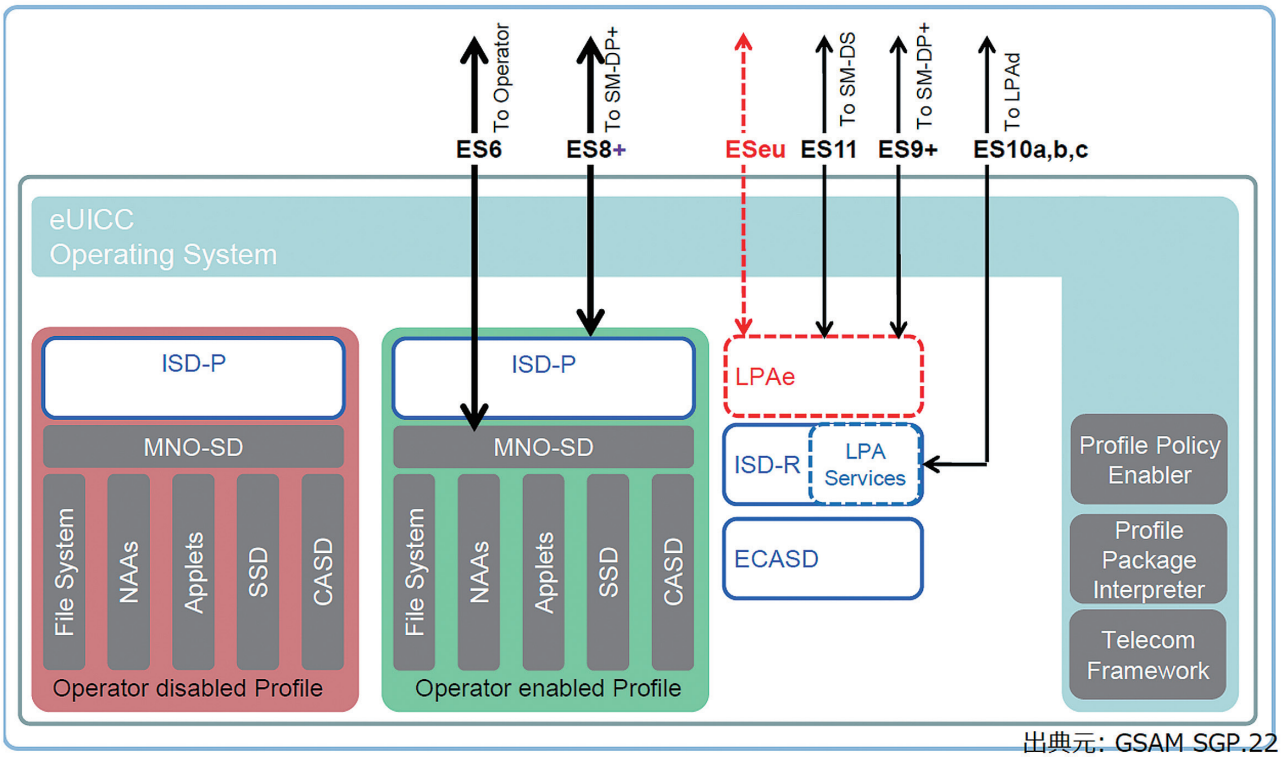
3.2 eSIMの仕組み

3.2.1 eSIMの内部構造

eSIM内部は、図-1のような構造となっています。この内、eSIMを特徴付ける要素が、ISD-R、ISD-P、ECASDの3つです。

ISD-R[*2]はeSIM内部とeSIM外部との直接的なインタフェースとなり、eSIMを管理します。プロファイルのダウンロードやダウンロードしたプロファイルのインストール、インストールしたプロファイルの切り替えや削除といった操作はすべてISD-R経由で行われます。

ISD-P[*3]は従来のSIMカードに相当し、インストールされたプロファイルごとに作成されます。サーバからダウンロードされたプロファイルはISD-Pを作成する手順を記述したフォーマットとなっており、インストール時にこのプロファイルを解釈してISD-Pが作られます。通信に使用するISD-Pをアクティベートすることで、デバイスからは通常のSIMとして見えます。



出典元：GSAM SGP.22

図-1 eSIM内部の構造

＊2　ISD-R：Issuer Security Domain Rootの略称。
＊3　ISD-P：Issuer Security Domain Profileの略称。

ECASD[*4]はプロファイルをダウンロードする際のデータ保護に使用する鍵を格納した領域です。格納された鍵を使用して、サーバとeSIMカード間の認証を行います。また、サーバからダウンロードするプロファイルは暗号化されており、プロファイルの復号化にも、格納された鍵を使用します。

ECASDに格納されている、データの保護のための鍵は、公開鍵基盤にもとづき署名されており、同様に署名された鍵がサーバ側にも格納されています。SIMとしてのセキュリティを担保するため、GSMAがルート証明局としてこれらの鍵に署名しており、他の証明局で署名された鍵は不正なものとして扱われます。GSMAから署名を受けるためには、eSIMの製造拠点、プロファイルを格納するサーバの設置拠点それぞれに対してSASと呼ばれる認定を受ける必要があります。SASの認定には多くのコストがかかるため、認定を受けたeSIMの製造拠点も、サーバの設置拠点も限られています。サーバについては、個々の事業者が独自に持つのではなく、SAS認定を受けたサプライヤのサービスを使うことが現状ではほとんどです。

このような、リモートからのプロファイル書き込みに対応したeSIMには、2019年6月現在、大きく分けて以下の2種類の仕様が存在します。

■ M2Mモデル

M2Mデバイス向けに策定された規格で、リモートからeSIMを制御します。当初の目的である組み込み機器向けの仕様です。

■ コンシューマモデル

人間が操作するデバイス向けに策定された規格で、デバイス側でeSIMを制御します。人間が操作する上で、M2Mモデルでは対応が難しい部分を改善した仕様です。

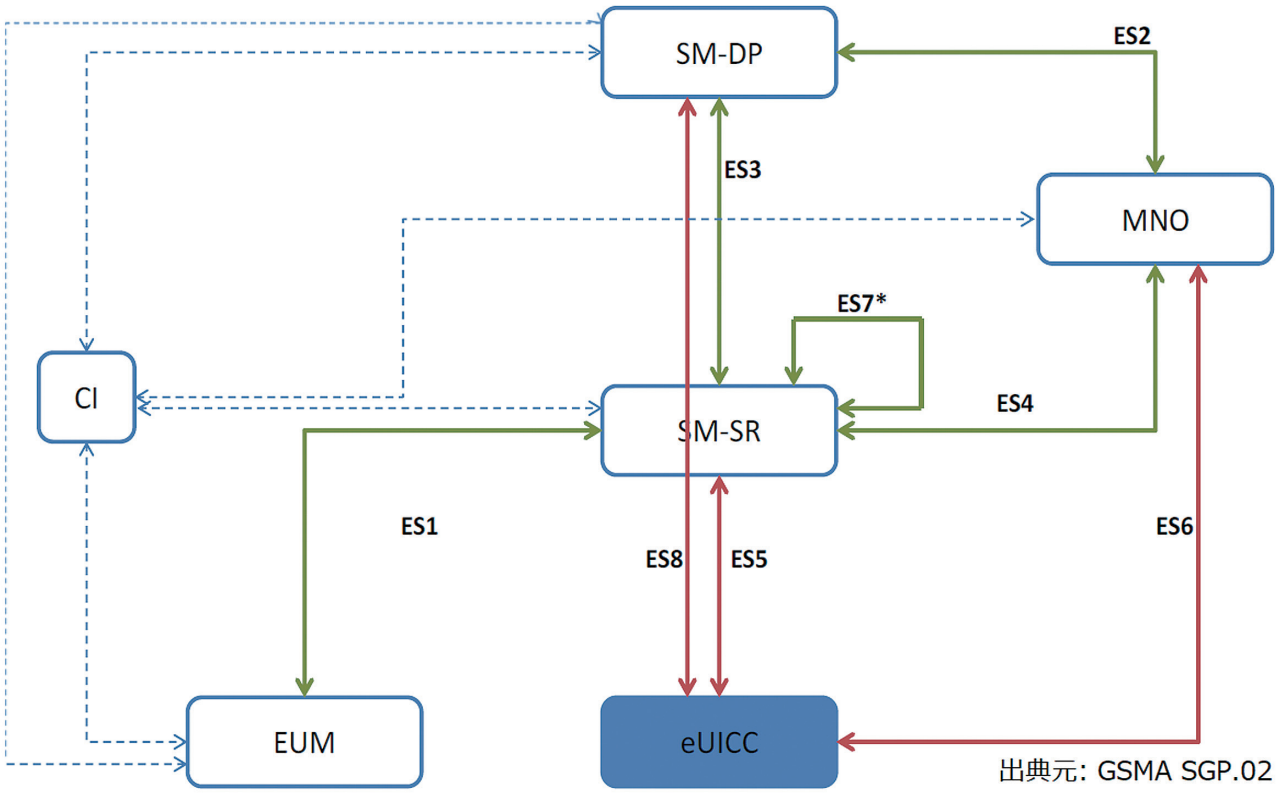


図-2 M2Mモデルのインタフェース

＊4　ECASD：eUICC Controlling Authority Security Domainの略称。

3.2.2 M2Mモデル

M2Mモデルは、eSIMの最初の仕様となります。IoT機器が対象のため、リモートからプロファイルのインストールや切り替え、削除まで行うことが可能です。M2Mモデルの構成要素を図-2に示しますが、主要な構成要素は以下のとおりです。

- **eSIMカード**
- **eSIMカードが組み込まれたデバイス**
- **eSIMカードに対してセキュアな経路を確立するSM-SR[*5]サーバ**
- **プロファイルを提供するSM-DP[*6]サーバ**

M2Mモデルでは、SM-SRサーバを起点としてeSIMカードを制御します。SM-SRサーバからeSIMカードに対しSMSを送信して、SM-SRサーバとeSIMカード間にセキュアな経路を開き、以下の操作を行います。

- **プロファイルのダウンロードとインストール**
- **プロファイルの切り替え**
- **プロファイルの削除**

SM-SRサーバとの通信はeSIMカードが直接行い、eSIMカードが組み込まれたデバイス側ではSMSやパケットの転送のみを行います。デバイス自体に必要となる機能は少なく、最近の一般的なモデムでおおむね対応しています。組み込み機器のように実装可能な機能が限られている環境でも対応可能な仕様と言えます。

M2Mモデルでは、SM-SRサーバがeSIMカードを制御するため、eSIMカードは特定のSM-SRサーバとのみ通信を行います。特定のSM-SRサーバとのみ通信する構成となるため、SM-SRサーバを持つプラットフォーマが、物理的なeSIMカードの供給も併せて行うこととなります。また、すべてのプロファイルがSM-SRサーバを経由してインストールされるため、インストールするプロファイルもSM-SRサーバを持つプラットフォーマが調達することとなります。このため、プロファイルの選択肢はプラットフォーマ側に依存します。

eSIMカードとSM-SRサーバとの通信はIPプロトコルで行われますが、SM-SRサーバからeSIMカードにアクセスするための最初のトリガーには、SMSが使用されます。SMSを利用するためにモバイル回線が必要となることから、M2Mモデルで使用するeSIMカードには、ブートストラップと呼ばれるプロファイルが最初からインストールされています。eSIMの操作はすべてリモートで行うことからブートストラップにはあらゆる国での接続性が求められるため、このプロファイルの調達方法が1つの課題となります。また、プロファイルの切り替えが必要とならないケースでは、ブートストラップは無駄となります。国内向け限定の製品であれば、プロファイルを入れ換える必要がないため、従来のチップタイプのSIMで問題ないと言えます。

3.2.3 コンシューマモデル

コンシューマモデルは、M2Mモデルの次に策定された仕様です。スマートフォンなど、エンドユーザが直接操作するデバイスが対象で、eSIMの操作はすべてデバイス上で行えるようになっています。コンシューマモデルの構成要素を図-3に示しますが、主要な構成要素は以下の通りです。

- **eSIMカード**
- **eSIMカードが組み込まれたデバイス**
- **デバイス上でeSIMカードを管理するためのLPA[*7]**
- **プロファイルを提供するSM-DP+サーバ**
- **eSIMに提供されたプロファイルの検索を行うSM-DS[*8]サーバ**

M2Mモデルと比較すると、eSIMカードのプロファイルの管理をリモートから行うSM-SRサーバがなくなり、代わりにデ

＊5　SM-SR：Subscription Manager Secure Routingの略称。
＊6　SM-DP：Subscription Manager Data Preparationの略称。
＊7　LPA：Local Profile Assistantの略称。
＊8　SM-DS：Subscription Manager Discovery Serverの略称。

バイス上でプロファイルを管理するLPAというアプリケーションが追加されています。また、M2Mモデルでは存在しなかった、SM-DSサーバが構成要素として追加されています。その他、SM-DPサーバも、コンシューマ向けの要件を満たすための機能変更が行われており、区別するためにSM-DP+サーバと呼ばれます。

コンシューマモデルで追加されたLPAは、エンドユーザが端末上で以下の操作を行うためのインタフェースを提供します。

- **プロファイルが格納されているSM-DP+サーバのアドレスとプロファイルの識別子の入力**
- **インストールするプロファイルのダウンロードとeSIMチップへのインストール**
- **使用するプロファイルの切り替え**
- **不要なプロファイルの削除**

LPAはデバイス側で動作するLPAdとeSIMカード側で動作するLPAeという2つの実装形態が定義されています。デバイスベンダーがコンシューマモデルのeSIMデバイスを開発する場合、LPAe対応のeSIMを採用するか、LPAdをデバイスに実装するかのいずれかを選択する必要があります。今のところLPAe対応のeSIMは普及していないため、デバイスベンダーはLPAdを実装する必要があり、この点がコンシューマモデルのデバイス開発を行う上での1つのハードルとなっています。

LPAによりデバイス上ですべての操作を行うモデルのため、M2Mモデルで必須となっていたSMSは不要です。プロファイルのダウンロードもWi-Fi経由で可能なため、M2Mモデルでのブートストラップに相当するプロファイルが不要となります。余分なモバイル回線の契約が不要となるため、IoT機器向けでもLPAを実装してコンシューマモデルを採用するケースもあるようです。一方で、エンドユーザの利便性を考慮して、プ

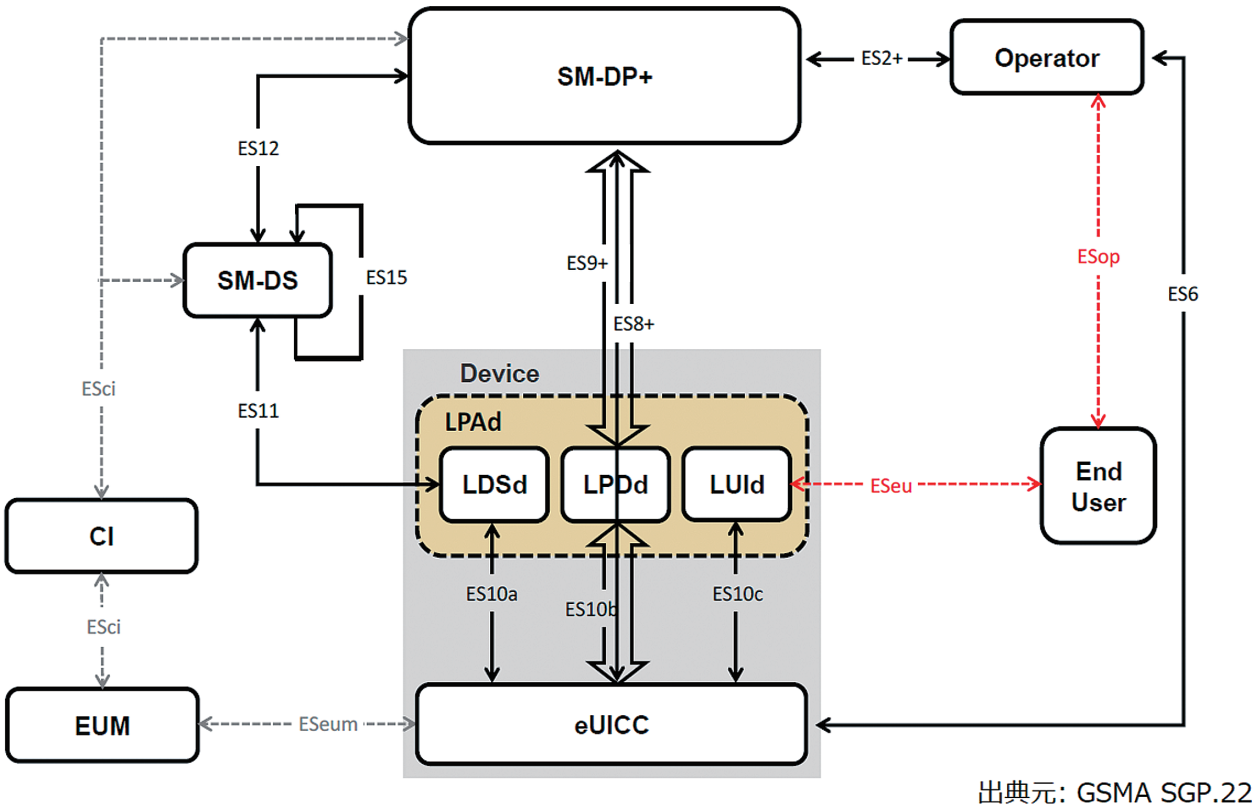


図-3 コンシューマモデルのインタフェース

ロファイルダウンロード用のモバイル回線用プロファイルをインストールした状態で提供される場合もあります。

プロファイルをインストールするにあたり、SM-DP+サーバのアドレスとインストールするプロファイルを特定するためのMatching IDと呼ばれる識別子をLPAに入力する必要があります。このために使用するのが以下のようなアクティベーションコードと呼ばれる文字列です。

```
1$SM-DP-PLUS.EXAMPLE.COM$MY-MATCHING-ID-0123456789
```

「$」を区切り文字として、バージョン番号(現在は1で固定)、SM-DP+サーバのアドレス、Matching IDで構成されます。この文字列を手動で入力するのは大変なため、通常はQRコードに変換してデバイスに読み込ませます(図-4)。

3.3 主要ベンダーの動き

3.3.1 Apple

Appleは早くからApple SIMという形でeSIMに相当する機能を提供してきました。Apple SIMの詳細は公開されていませんが、仕組みとしてはM2MモデルのeSIMが使われていたと考えられます。ただし、エンドユーザが各々で回線契約を実施するため、デバイス上で回線契約が行える仕組みを組み込むなど、独自色の強いサービスとなっています。Appleはプラットフォームを提供するのみですが、Apple自身の強いブランド力を背景に、各国のモバイル事業者のプロファイルを集めることに成功しています。

図-4 アクティベーションコードのQRコード

1枚のSIMカードにより、世界中のユーザにコネクティビティを提供する点がApple SIMの特徴です。しかし、Apple SIMで提供されるのはデータ回線契約のみで、音声回線契約は提供されていません。おそらくですが、データ回線の契約と比較して、音声回線の契約には本人確認などが必要となり、そのレギュレーションは各国様々なため、単独のプラットフォームでこれに対応することが困難だったと考えられます。

iPad向けにApple SIMを使い続けてきたAppleですが、2018年に発売したiPhone XSでは、標準のコンシューマモデルのeSIMを採用しました。電話であるiPhoneでは音声契約を切り離すことができなかったことが理由と思われます。eSIMに対応したiPhone XSの後に発売されたiPadなど、音声回線を利用しないデバイスでApple SIMが採用されていることを考えると、音声契約だけはApple SIMでの提供を断念したと考えられます。標準のeSIMを採用するのであれば、モバイル事業者がプラットフォームを作ることとなり、音声契約にかかわるレギュレーションを満たせるという判断だと思われます。

Apple SIMでは、Appleを経由した回線契約となり、IIJのようなMVNOが回線を提供することは困難でした。しかし、iPhone XS以降に採用されたコンシューマモデルのeSIMでは、インストールするプロファイルに制限はなく、IIJのフルMVNOのプロファイルを利用することが可能です。2019年夏に提供開始を予定しているIIJのeSIMサービスでは、iPhone XS/XRユーザを主要なターゲットの1つに定めています。

3.3.2 Microsoft

MicrosoftはWindows 10 バージョン1703において、OSに標準的なLPAを搭載しました。Microsoftが掲げるAlways Connected PCのコンセプトに、eSIMが有効と判断された結果と考えられます。OSにLPAが標準で搭載されたことで、デバイスベンダーは自社でLPAを実装する必要がなくなり、eSIMカードと対応するモデムモジュールを調達すれば、容易にeSIMに対応したデバイスを製造することが可能となりました。デバイスの製造が容易となったことで、今後eSIMを搭載したデバイスが普及していくと考えられます。普及の動きの1つとして、Microsoft自身もeSIMを内蔵したSurface Proを販売しています。

また、Microsoftは、Apple SIMのようにデバイス上で回線契約まで行える、モバイル通信プランというアプリも提供しています。日本国内では2019年6月現在、KDDI、GigSky World Mobile Data、Ubigiのプロファイルを購入することができます。

この他に、2018年11月末に米国で開催されたMicrosoft Ignite 2018では、企業向けMDM[*9]へのeSIMの統合を計画していることも公表されました。企業で使われるPCとしてデバイスの管理は必須となりますが、モバイル回線の管理もMDMの中に取り込み、企業のデバイス管理者が個々のデバイスで使うeSIMプロファイルの管理も行うことが可能となります。

3.3.3 Google

GoogleのeSIMへの対応は、AppleやMicrosoftと比べると遅れているようです。Android Piで、eSIMに関係するAPIを定義しましたが、OS自身にLPA機能を搭載していないため、各ベンダーがLPAアプリを実装する必要があります。なお、Google自身はLPAを組み込んだ、Pixel 2やPixel 3、Pixel 3aといったeSIM対応端末を提供しています。ただし、本稿を執筆している2019年6月現在で日本向けに発売されている端末については、eSIMの代わりにNFC[*10]が搭載され、国内ユーザはeSIMを使うことができないようです。

Google自身のサービスとしてはeSIMを利用して、Google FiというMVNOサービスにより、世界各国のコネクティビティを提供するサービスを開始しました。対応するAndroid端末は限定される一方で、iPhoneへの対応も行われています。iPhoneなど、自社で管理していない端末にも提供されていることから、プロファイルの提供はM2Mモデルではなく、コンシューマモデルだと考えられます。一方で、利用可能なエンドユーザは米国在住者に限られており、世界中のユーザが利用できるわけではありません。ただ、サービスの提供範囲は、米国在住者に限られるものの、Apple SIMとは異なり音声サービスも提供されています。これは、GoogleがMVNOとして提供すること、そして提供の対象を北米在住のユーザに絞ることで、エンドユーザの音声契約に関するレギュレーションを米国の基準に限定することができたからだと考えられます。

3.3.4 類似のサービス

eSIMとは異なりますが、中華圏を中心に、独自の仕様でプロファイルの販売が行われています。独自のSIMと、そのSIMにプロファイルをインストールするOTAサービスが提供され、エンドユーザは様々な国のモバイル事業者のプロファイルをダウンロードして使えるようになっています。ターゲットとなるエンドユーザは自国のアウトバウンドの旅行者で、旅行先でのローミングより安価なコネクティビティを提供することを目的としています。日本での例として、H.I.S.モバイルが販売している「変なSIM」シリーズがこの系統にあたります。

なお、これらのサービスも、iPhone XSなど、eSIMを搭載したデバイスが出てきたことで、独自仕様からオープンなeSIMのプラットフォームへの転換を行っているようです。

3.4 IIJの取り組み

フルMVNO事業者であるIIJは、eSIMにインストールするプロファイルを自社で提供することが可能です。現在、フルMVNO回線の新規販売チャンネルとして、eSIM向けにフルMVNOプロファイルを提供するサービスの開発を進めています。

先に述べたとおり、eSIMの提供形態は、M2Mモデルとコンシューマモデルの2つのパターンがあります。IIJでは、まずはコンシューマモデルをターゲットとしています。理由は、現在IIJが発行できるプロファイルは国内のみのため、国外展開を前提としたM2Mモデルより、コンシューマモデルの方がフ

＊9　MDM：Mobile Device Managementの略称。モバイルデバイス管理。
＊10　NFC：Near Field Communicationの略称。近距離無線通信規格。

ルMVNO回線に合っていると考えているからです。更に、フルMVNOのプロファイルでは国外の接続性の担保が難しく、ブートストラップとして利用できないことも理由の1つです。

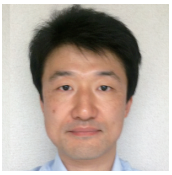
eSIMサービス提供に向けた取り組みの一環として、昨年度にはコンシューマモデルの構成で実証実験を行いました。実証実験では、フルMVNO用のプロファイルを設計し、Microsoft Surface Proにプロファイルをインストールし、モバイル通信を行うことに成功しました。また、Microsoft Surface Pro以外の端末もターゲットとして動作確認を行い、ノウハウを蓄積しています。その1つとして、プロファイルとeSIMカードの間に相性の問題があることを確認しました。前述しましたが、eSIMカードにインストールするプロファイルは専用のフォーマットで記述されます。この中で、記述を簡略化するためにテンプレートという記法が定義されていますが、テンプレートを利用した場合に、特定のeSIMカードでインストールに失敗してしまうパターンが存在することを確認しました。また、特定の非必須パラメータの記述が存在しないことに起因して、インストールできない問題も確認しています。eSIMカード自体を管理下に置けるM2Mモデルと異なり、コンシューマモデルでは、様々なeSIMカードがターゲットとなるため、このようなノウハウの蓄積は、サービスを提供する上で必須と言えます。

本稿を執筆している2019年6月の段階では、実証実験も終わり、商用提供に向けたサービス開発を行っています。SM-DP+サーバについては、GSMAのSASの認定が必要となるため、自社独自で持つことが難しいこともあり、他のモバイル事業者と同様、SaaS型のサービスを利用しますが、国内で提供されているeSIMサービス(ドコモのdtabや、KDDIのWindows向けプリペイドプラン)とは異なり、特定のデバイスに縛られない、汎用的なサービスの提供を目標としています。2019年の夏には読者の皆様にご利用いただけるサービスを提供する予定です。

3.5 eSIMの活用シーンと今後の動向

eSIMを利用することで、どのような未来が描かれるでしょうか。

eSIMが従来のSIMと大きく異なる点は、物理的なSIMが排除される点です。物理的なSIMカードがなくなり、電子データとしてプロファイルがやりとりされることで、SIMカードの配送にかかるコスト(距離的、時間的なものも含める)が不要になります。コストと言うと価格部分に注目しがちですが、プロファイルの購入にあたって、店舗に行く、あるいは、SIMの配送を待つといったことが不要となります。この結果、エンドユーザは、いつでも、どこでも、必要なときにプロファイルを購入することが可能となります。長期の契約ではこのメリットは活かし難いかも知れませんが、プリペイド、特に渡航者が現地で一時的な回線を契約するケースでは、購入が容易となる点が活きてきます。併せて、物理的なSIMカードの交換が不要となるため、紛失リスクがなくなるなどといったメリットも生じます。特にiPhone XSのようなDSDS[*11]端末であれば、メインの音声契約のSIMカードをSIMスロットに入れ、データ用のSIMを必要なときにプリペイドで購入するといった使い方が考えられます。ただ、日本国内市場で言えば、流動性の高いeSIMを本格的に採用することは、モバイル事業者側にとって直接的な利益につながるものではありません。そのため、端末メーカ主導でSIMフリー端末を導入していかない限り、eSIMの普及は難しいのではないかと考えられます。IIJとしては、いち早くeSIMサービスを開始することで、端末メーカがeSIMに対応した端末を導入していくような土壌となればと考えています。



執筆者:
圓山 大介(まるやま だいすけ)
IIJ MVNO事業部 技術開発部 MVNOサービス開発課。
2018年IIJ入社。フルMVNO向けのサービス基盤の開発に従事。直近では本文に記載したeSIMのサービス基盤の開発に携わる。

*11 DSDS:Dual SIM Dual Standbyの略称。