



Embedded UICC Remote Provisioningの標準化状況

M2M分野において、注目される技術の1つにEmbedded UICC Remote Provisioningがある。ドコモはGSMAのFastTrackプロジェクトに参加し、諸外国の通信事業者、SIMベンダとアーキテクチャ検討を行った。本稿では、その概要とユースケースについて解説する。

M2Mビジネス部 すずき かずなり あずま てっぺい
鈴木 和成 東 哲平

1. まえがき

多様なニーズが存在するM2M (Machine-to-Machine) デバイスにおいて、デバイスの耐久性向上やさらなる小型化の実現は、M2Mビジネスの発展に不可欠な要素となっている。通常、3GやLTEの通信サービスを利用する場合、SIM^{*1}カード挿入口をデバイスに設けて通信サービスを利用するが、SIMカード挿入口を設けることで部品点数の増加につながっていた。そのため、M2Mデバイスは小型化や部品点数を削減することで高耐久性を実現するために、Machine to Machine UICC^{*2} (MFF^{*3}) をデバイスに組み込み、取外しが容易ではない形でデバイスが設計されるようになってきている。

このように、SIMカードとデバイスの一体化が進むのと平行して、M2Mビジネスの流れとしてグローバル化の加速化もある。一般的

にはグローバルビジネスを展開するために各国通信事業者のサービスを利用するが、前述のように、SIMカードをデバイスに組み込む場合、SIMカードの取換えが困難となる。

このようなSIMカードは差替えができない状況においても、各国通信事業者のサービスを利用したいなどといったニーズを満たすために Embedded UICC Remote Provisioning (以下、eSIM) が検討されており、サービスのグローバル化、多様化が加速度的に進んでいるM2Mビジネスにおいて、今後導入が進むと考えられる技術の1つとなっている。eSIMは、SIMカードに登録されている通信事業者を、OTA (Over-The-Air)^{*4} 技術を利用して遠隔で更新可能とする技術である。

eSIMについては、本稿執筆時点においてETSI (European Telecommunications Standards Insti-

tute)^{*5}などの国際標準化組織で標準化活動が進められているが、標準化完了に先立ち2013年12月13日にGSMA (GSM Association)^{*6}が仕様書を公開した[1]。

本アーキテクチャの策定にあたっては、世界の通信事業者10社とSIMベンダ4社にてドキュメントの作成を行った。ドコモもアーキテクチャの検討に携わった事業者の1社である。

本稿では、GSMAから公開されたドキュメントに基づいたeSIMの概要とアーキテクチャ概要とユースケースについて解説する。

2. eSIMの概要

2.1 現在のSIMカード

現在普及しているSIMカードを利用した通信のイメージを図1に示す。SIMカードには1つの携帯通信事業者 (MNO: Mobile Network Operator) の通信プロファ

©2014 NTT DOCOMO, INC.
本誌掲載記事の無断転載を禁じます。

^{*1} 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。GSMでの加入者識別モジュールをSIMと呼ぶ。
^{*2} UICC: 電話番号を特定するための固有のID番号が記録されたICカード。UIM (User Identity Module) カード、SIMカ

ードと同義で使用している。

^{*3} MFF: M2M Form Factorの略称。M2M向けのUICCを指す。

^{*4} OTA: 無線通信を利用してデータの書き込みや更新を行う技術。

イル^{*7}が格納されており、それを利用して通信が行われる。通信プロファイルには、MSISDN (Mobile Subscriber ISDN number)^{*8}、IMSI (International Mobile Subscriber Identity)^{*9}などの各MNOとの通信に必要な情報が格納されている。SIMカードごとにMNOが固定されており、MNOを変更することはできない。

そのため、MNOを変更するためにはSIMカードをデバイスにその都度差し替える必要がある。

2.2 eUICC

eUICCは、デバイスからの取外しや取換えを意図しないRemote Provisioning機能を有したSIMカードである。複数の通信プロファイルを格納することができ、その中から1つの通信プロファイルをenable（デバイスから認識され、通信可能）プロファイルとして扱う。enableプロファイルのMNO NWを利用し通信を行う。enable以外の状態をdisable（デバイスから認識はされない）状態プロファイルとなる（図2）。従来のSIMカードでは、ICCIDがSIMカードを識別するユニークキーとして用いてきたが、eUICCにおいては、ICCIDはプロファイルを識別するキーの位置づけとなり、eSIMのユニークキーはeUICC-IDと呼ばれる新しいIDを定義し、それを利

用する（表1）。

なお、GSMAでは、プロファイルを大きく2種類に定義している。

(1)Provisioning Profile

eUICCの初期出荷時に格納されている通信プロファイル。後述するOperational Profileのダウン

ロードや切替えを行うためのみに使用する、用途限定の通信プロファイル。

(2)Operational Profile

企業サーバやインターネットに接続するためのプロファイル。Provisioning Profileの役割を果た

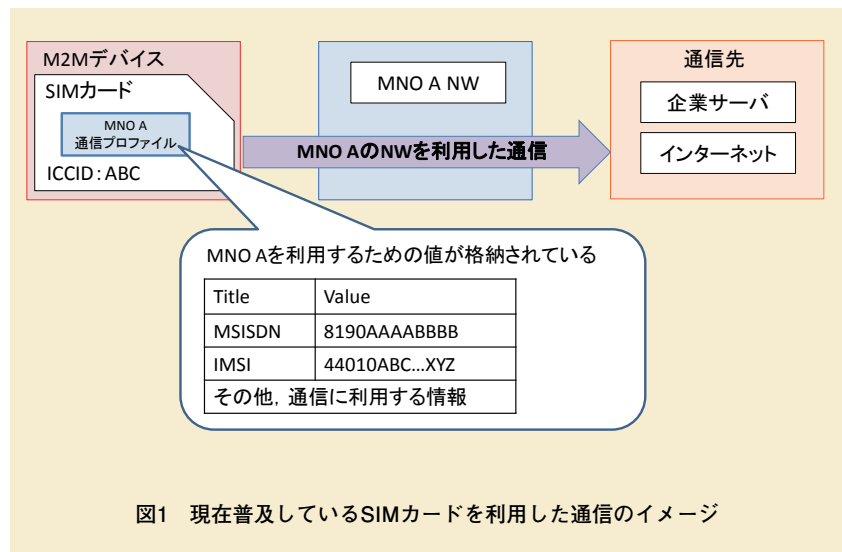


図1 現在普及しているSIMカードを利用した通信のイメージ

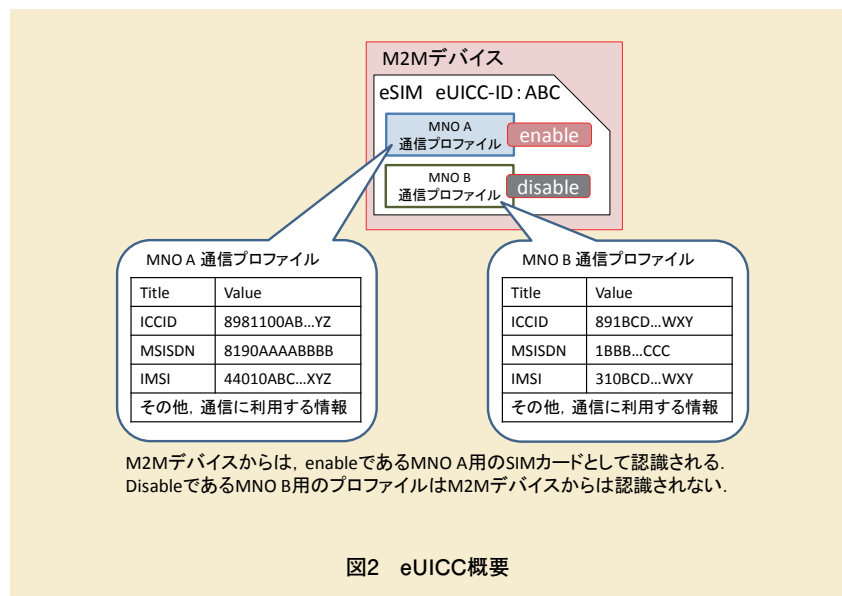


図2 eUICC概要

*5 ETSI：欧州電気通信標準化機構。ヨーロッパの標準化団体。電気通信技術に関する標準化を行っている。本部はフランスのSophia Antipolisにある。

*6 GSMA：ローミングルールの策定をはじめとした、さまざまなモバイル業界の活

動を支援・運営する、世界最大の移動通信関連の業界団体。219地域・約800の移動通信事業者と200を超える中継事業者や端末・装置ベンダ、ソフトウェアベンダなどの関連企業が参加している。

*7 プロファイル：通信に必要な情報（IMSI、

MSISDNなど）が記述されているファイル群。

*8 MSISDN：3GPP上で規定される加入者に割り当てられる電話番号。

*9 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。

Standardization

す事もできる通信プロファイル。

3. eSIMのアーキテクチャ概要

eSIMはICカード単体の機能としてプロファイルの切替えを実行するのではなく、Subscription Managerと呼ばれる装置からの指示に基づきプロファイルの切替え

を行う。Subscription ManagerはMNOなどが保有・管理する。

eUICC内のプロファイル切替えを例に、Subscription Managerを中心としたeSIMのアーキテクチャ全体像を図3に示す。

eUICCには、OTAを可能とするために少なくとも1つのプロファイルが格納されており、格納さ

れているプロファイルの1つをenableのプロファイルとして扱う。enableのプロファイルはMNO AのNWを利用し通信を行っている。ユーザはプロファイル切替えを行いたいタイミングで、Subscription Managerに対して切替え指示を行う。その際に切替え先のプロファイルがeUICCに格納されて

表1 eUICCとSIMカードの比較

	eUICC	SIMカード
カードのユニークキー	eUICC-ID ※ICCIDはプロファイルのユニークキーとして存在	ICCID
プロファイルの数	複数	1
enableプロファイルの数	1	1

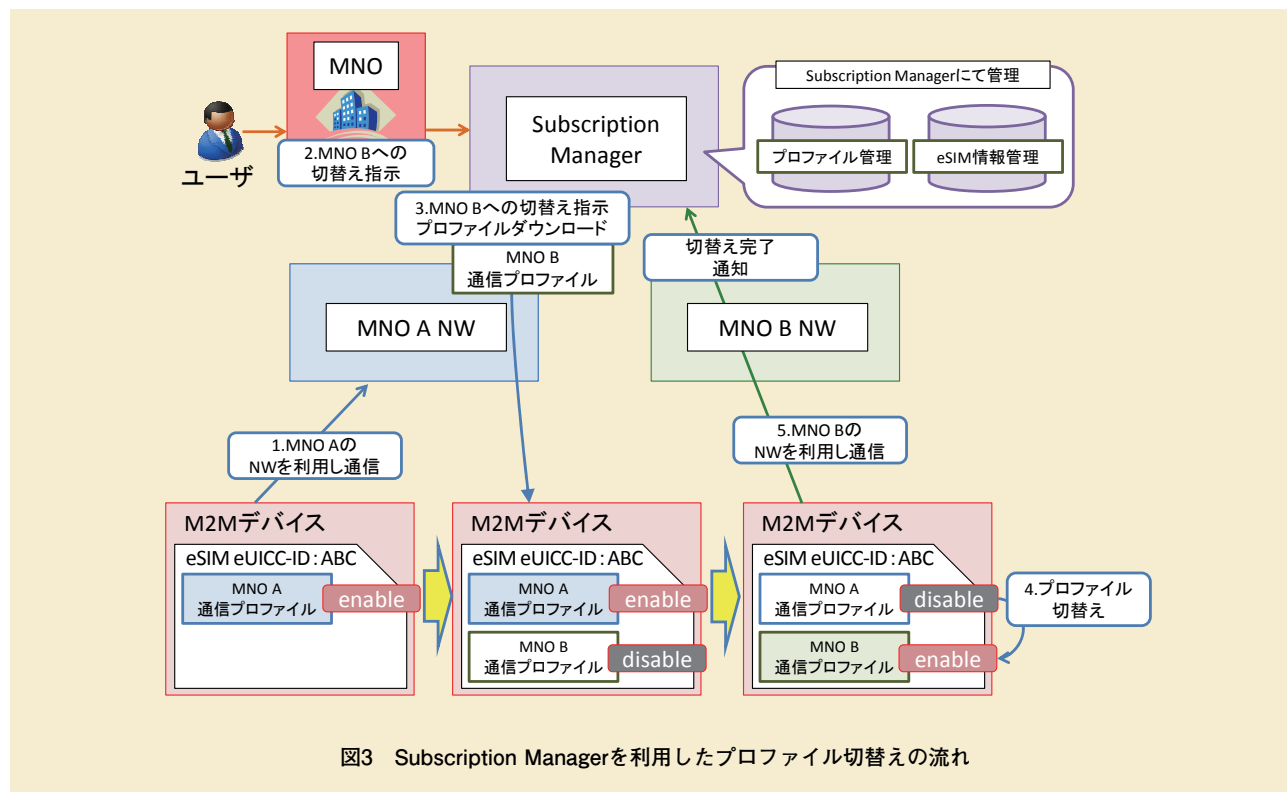


図3 Subscription Managerを利用したプロファイル切替えの流れ

いない場合、切替え先のプロファイルDLを先に行う。切替え指示を受け取ったeUICCは、eUICCの内部処理でenableプロファイルの切替えを行う。切替え完了後に、切替え後のMNO BのNWを利用し、切替え完了通知をSubscription Managerに送ることで切替え処理が完了する。元のMNO Aに戻すケースや、他のMNO Cなどに切替えるケースにおいても同様の手順を踏み、切替えを行っていく。

前述のとおり、Subscription Manager機能によりプロファイル切替えを実現する。Subscription ManagerはSM-DP（Subscription Manager Data Preparation）とSM-SR（Subscription Manager Secure Routing）の2つの役割をもつ。ここでは、Subscription Managerの機能詳細について図4を用いて解説する。

(1)SM-DPの役割

SM-DPは、通信プロファイルの作成と保管をセキュアに行う役割をもつ。SM-DPは通信プロファイル作成に必要な情報（MSISDN、IMSIなど）をMNOから受け取り、通信プロファイルを作成する。その後、作成されたプロファイルを保管する。

(2)SM-SRの役割

SM-SRは、eUICCとのセキュアな通信を確立する役割をもつ。eUICCに格納される通信プロファイルは秘匿性の高い情報であり、外部からの参照、書換えが容易に行うことができない仕組みが求められる。そこで、プロファイルの作成を行うSM-DPとeUICCとの通信を確立するSM-SRを分けることでセキュアな環境を構築している。SM-SRは、eUICCとのセキュアな通信を確立するため、

EIS（eUICC Information Set）をもつ。EISには、eUICCにアクセスするための鍵情報（the Platform Management Credential）や、プロファイルごとにenableなのかdisableなのかの状態などをもつ。

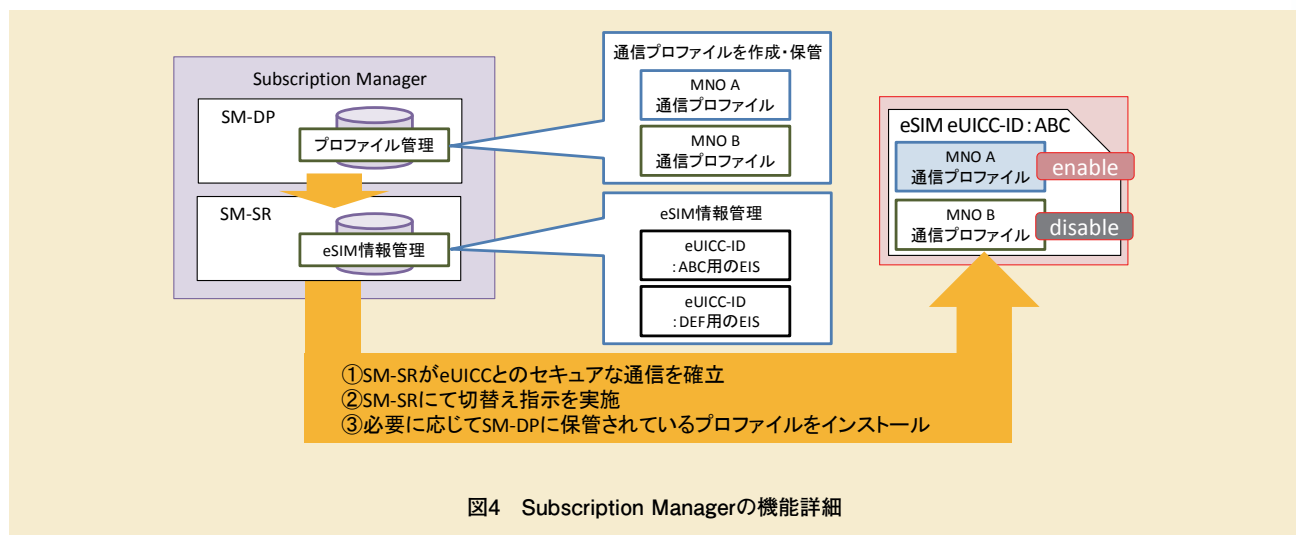
SM-SRは、the Platform Management CredentialをもつことでeUICCにセキュアなアクセスが可能となり、SM-SRからenableプロファイルの切替え指示を行うことが可能となる。

4. ユースケース

以下に、eSIMを利用した代表的なユースケースを2件紹介する。

(1)ロジスティクスの効率化

M2M分野においてはSIMの取外しが容易ではないデバイスが存在したり、デバイスが人手の届きにくい遠隔地に設置されたりすることが多い。そのような状況にお



Standardization

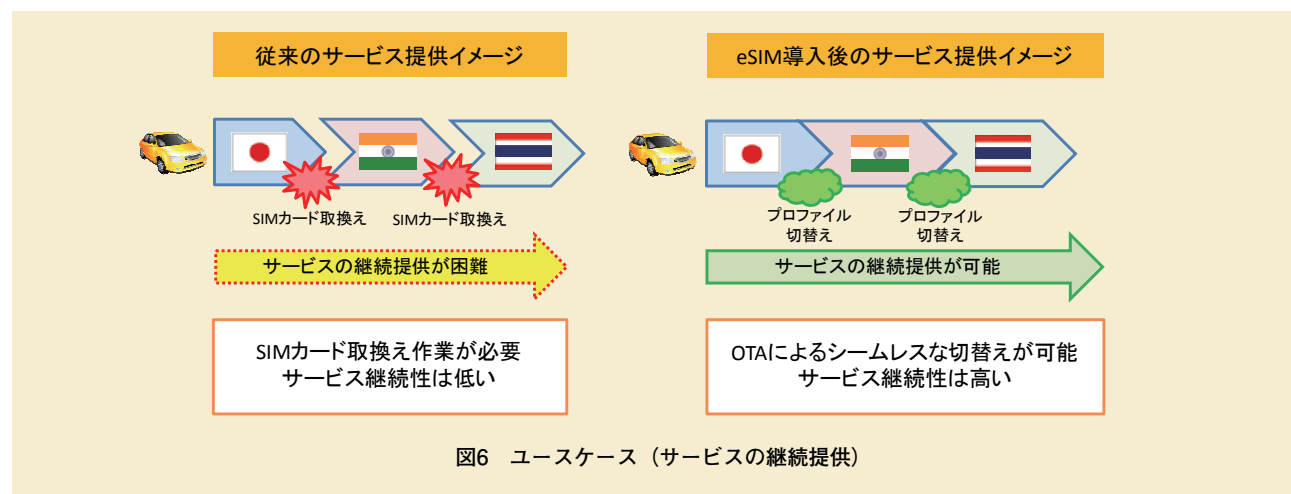
いて、例えばグローバルに製品を製造・出荷するケースを考える。従来のSIMカードでは、出荷する各国ごとに異なる通信プロファイルをもつSIMカードを組み込む必要があり、製品を展開する地域ごとに製造・物流ラインを設け管理する必要があり、地域ごとに製造・出荷数の事前調整が必要であった。eSIMを導入すると、プロファイルの切替えをユーザが希望す

る過程にて行うことでできるようになり、製造・出荷後でも実際の需給バランスに基づいて製品を出荷する国を変更することができるなど、効率的なロジスティクスが実現されると考えられる (図5)。

(2)サービスの継続提供

M2Mデバイスをグローバルで利用するケースにおいて、従来のSIMカードでは、地域が変わるたびにSIMを取り換える作業が必要

になるため、サービスを継続的に利用することが困難になることが考えられる。一方、eSIMを導入した場合は、OTAによるプロファイルの切替えが可能であるため、従来のSIMカードを利用する場合と比べるとグローバルなユースケースにおいてもシームレスなサービス利用が可能となり、グローバルビジネスの展開の障壁が低くなることが考えられる (図6)。



5. あとがき

本稿では、eSIMの概要とユースケースについて、GSMAから公開されたドキュメントに基づき解説した。今後はGSMAからのドキュメントをインプットとして、国際標準化団体（ETSIなど）にて標準化活動が進むと想定される。

技術標準化と並行して、運用面を考慮したSubscription Managerなどの認定基準の策定がGSMAにて行われる。

これからも、ドコモはIOT（Internet Of Things）時代のM2Mビジネスの発展に寄与する標準化活動や技術検討を続けていく。

文 献

- [1] GSM Association : “Embedded SIM Remote Provisioning Architecture.”
<http://www.gsma.com/connectedliving/wp-content/uploads/2014/01/1.-GSMA-Embedded-SIM-Remote-Provisioning-Architecture-Version-1.1.pdf>