Technology Reports

IoT/M2M　eSIM　SM

オペレータ間連携によるGSMA3.1準拠IoT/M2M向けeSIM商用化システムの構築

ソリューションサービス部　牧野（まきの） 弘治（こうじ）　岸（きし） 大智（だいち）
IoTビジネス部　辺（べん） 軍（ぐん）

ドコモは，IoT/M2M製品に関するグローバル化の流れを踏まえ，海外オペレータと連携してSIMの情報を柔軟に書き換えることができるマルチベンダeSIM連携システムを，世界で初めて構築した．
本稿では，IoT/M2M向けeSIMを実現するための仕組みについて解説する．

1. まえがき

ドコモと中国の通信事業者であるチャイナモバイル（China Mobile Communications Corporation）は，異なるベンダ間でのeSIM（embedded Subscriber Identity Module）*1連携システムを2017年6月に開発完了した．本システムは，GSMA（GSM Association）*2により策定された仕様「Remote Provisioning Architecture for Embedded UICC Technical Specification Version 3.1」（以下，GSMA3.1）に基づくものであり，商用環境における世界初のマルチベンダ間IoT（Internet of Things）*3/M2M（Machine to Machine）*4向けeSIM連携システムとなる［1］．

ドコモでは自動車や建機，産業機器などの海外展開におけるBtoB（Business to Business）向けソリューションとして本技術の導入を行っている．

本稿では，GSMA3.1の標準仕様をベースとして構築したRemote Provisioning*5のシステムの仕組みを解説する．

2. IoT/M2M向けeSIM

2.1　従来技術との違い

IoT/M2Mの世界では，小型化や部品点数削減による高耐久性の実現といった実装上の要件から，IoT/M2M製品に実装されているデバイス*6に直接SIMを埋め込み，取外しができないような設計が主流になってきている．また，これらのIoT/M2Mにおけるビジネスはグローバル化の流れがあり，製品

＊1　eSIM：一般的なSIMとは異なり，無線通信（OTA：Over-The-Air）によって遠隔から通信事業者の通信プロファイルの情報を書き換えることのできるSIMの総称．
＊2　GSMA：モバイル通信事業における世界的な標準化団体．

を各国の現地キャリアの通信サービスで利用したいというニーズも高まっている．

しかしながら，従来の技術ではSIMに書き込まれているMNO（Mobile Network Operator）*7の情報は固定されており，書換えを行うことは不可能であったため，海外利用では現地キャリアのSIMに差し替えるかローミング*8などで対応せざるを得なかった．

製品に組み込まれたSIMの差替えを行わず，各国の現地キャリアの通信サービスを利用したいというニーズの高まりに伴い，書き込まれたMNOの情報を柔軟に変更する技術がGSMAで標準化された［2］［3］．ドコモもアーキテクチャの検討に携わった事業者の1つである［4］．

2.2 コンシューマ向けeSIMとの違い

eSIMのサービスで用いられる技術としては，大きく分けてコンシューマ向けとIoT/M2M向けの2つが存在している［5］．これらは用途および標準規定が異なっている．これらの比較を**図1**に示す．

コンシューマ向けeSIMの技術は，ユーザ自身による開通処理を，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簡易な端末操作のみで可能とする用途に用いられている．コンシューマ向けeSIMで用いられている技術もGSMAにて規定されている［6］～［9］．

IoT/M2M向けのeSIMの技術は，通信事業者の切替えを遠隔のサーバ側から起動する用途に用いられる．

図1に示す通り，コンシューマ向けeSIMでは端末操作によりプロファイル*9のダウンロードが行われるが，IoT/M2M向けeSIMでは通信事業者がもつIoT回線管理プラットフォームからのリクエストによりプロファイルのダウンロードが行われる．

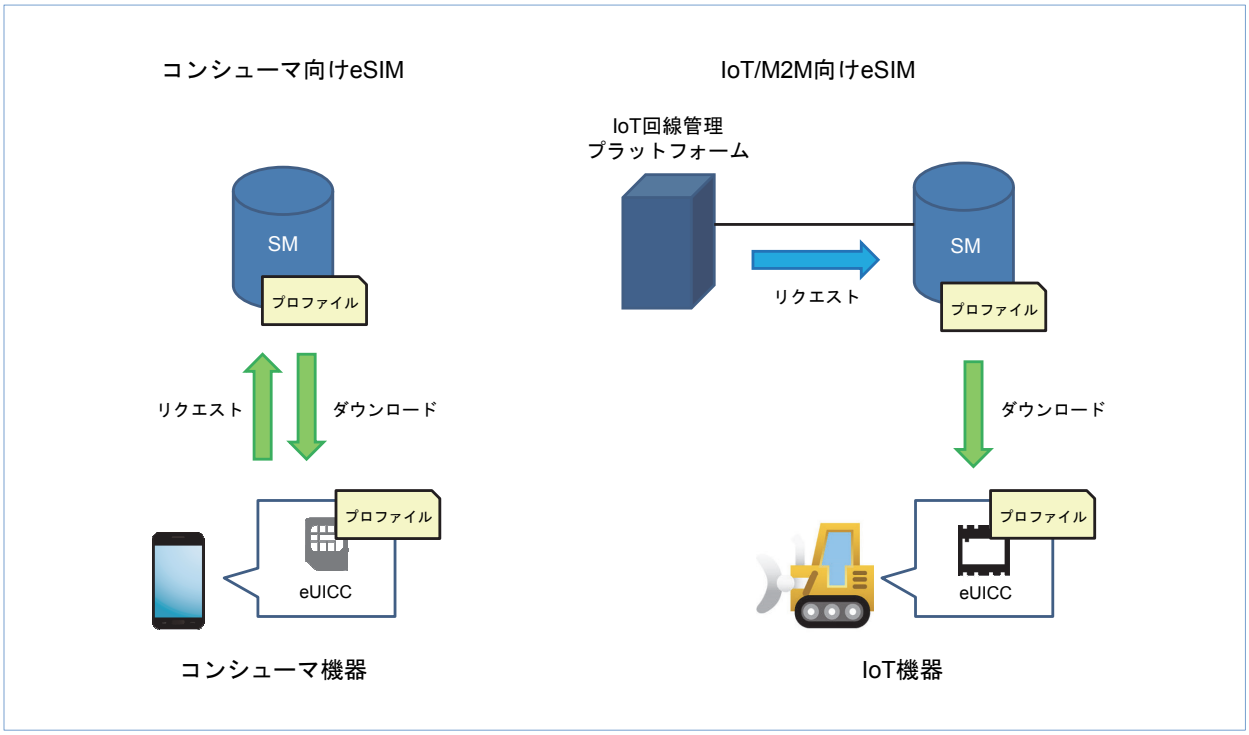

図1　コンシューマeSIMとIoT/M2M向けeSIMの違い

＊3　IoT：あらゆる「モノ」がインターネットに接続されることで，これまで実現されていなかったさまざまな情報共有を行うことができる仕組み．
＊4　M2M：機器間での通信．
＊5　Remote Provisioning：OTAによって遠隔から通信プロファイルを書き換えること．
＊6　デバイス：本稿ではM2Mモジュールなどのモバイル通信機能をもつ機器のことを指す．
＊7　MNO：移動通信事業者．
＊8　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．

2.3 ユーザエクスペリエンス

日本国内の工場で生産され，初期状態としてドコモ回線が設定された製品を日本国内からの輸出するケースを1例として，Remote Provisioningのユーザエクスペリエンス*10について解説する．このような例はBtoB向けソリューションとして実際にニーズが生じている．

初めに，ユーザはドコモに対してeSIMの発行申請を行い，ドコモからeSIMを受領する．次に，ユーザ自身でeSIMを製品に組み込み，ドコモ回線としてアクティベートを行い通信可能な状態にした後に，日本国内にて製品の出荷試験などを行う．eSIMが組み込まれた製品の海外出荷後は，ドコモ回線としてローミングを開始する．その後，ユーザが移行したい回線と切替先キャリアを指定しトリガをかけることで，指定された回線のRemote Provisioningがローミング経由で行われる．それが完了すると，現地キャリアの回線として通信が可能な状態になり，その通信サービスが利用可能となる．

2.4 GSMA3.1対応による効果

GSMA3.1［3］では以下の標準が規定されていて，理論上Remote Provisioning Architectureにおけるコンポーネント間でのマルチベンダによる接続が実現可能となっている．

- eUICC（embedded Universal Integrated Circuit Card）*11のアーキテクチャ
- Remote Provisioning Architectureにおけるインタフェース
- Remote Provisioning Architectureにおけるセキュリティ機能

GSMA3.1に対応することによるMNOのメリットとしては，SM（Subscription Manager）*12とeUICCをマルチベンダでシステム構築可能な点が挙げられ，また，ユーザメリットとしてはRemote Provisioningを実現するうえで機器に組み込むデバイスの条件が明確になり，今後の対応デバイスの増加が見込めることなどが挙げられる．

なお，現在，Remote Provisioning Architecture for Embedded UICC Technical Specificationのバージョン最新版は3.2となっている［10］．

3. IoT/M2M向けeSIMを実現する仕組み

3.1 構成および動作概要

ドコモがチャイナモバイルと構築したシステムでは，GSMA3.1で規定されている構成のうちの1つが採用されている．構成および動作概要を**図2**に示す．

SMはSM-DP（SM Data Preparation）とSM-SR（SM Secure Routing）の2つの機能に分離されている．それぞれの機能の概要は次の通りとなる．

- SM-DP：MNOの通信プロファイルをセキュアに格納する
- SM-SR：EIS（eUICC Information Set）を保有し，eUICCとの間のセキュアな通信を確立する

図2では，eUICCが最初に所属するMNOをMNO1（例：ドコモ）とし，MNO1からMNO2（例：チャイナモバイル）へと通信プロファイルを切り替える様子を示している．

図におけるMNO1とMNO2の通信プロファイルは，それぞれのSM-DPに格納されている．

本図の例のような構成の場合，Remote Provisioningは以下の手順で行われる．

- SM-SR Change（図2①～⑥）
- Profile DownloadとProfile Enable（図2⑦）

切替先の通信プロファイルのダウンロードを，切替先のMNOに所属しているSM-SRを経由して行う必要がある場合は，Remote Provisioningの手順上

＊9 プロファイル：電話番号や加入者識別番号などの各種情報や，ネットワーク情報などを集約したデータ．
＊10 ユーザエクスペリエンス：製品やサービスなどを使用・消費・所有した際に，ユーザが体験できる内容．
＊11 eUICC：組込みUICC，またはRemote Provisioning可能なUICCのこと．本稿ではRemote Provisioningの仕組みの説明で用いている．なお，UICCは加入者を特定するための固有のID番号が記録されたICカード．SIMカードと同義で使用している．
＊12 SM：遠隔でeUICCの通信プロファイルを書き換えるサーバ．

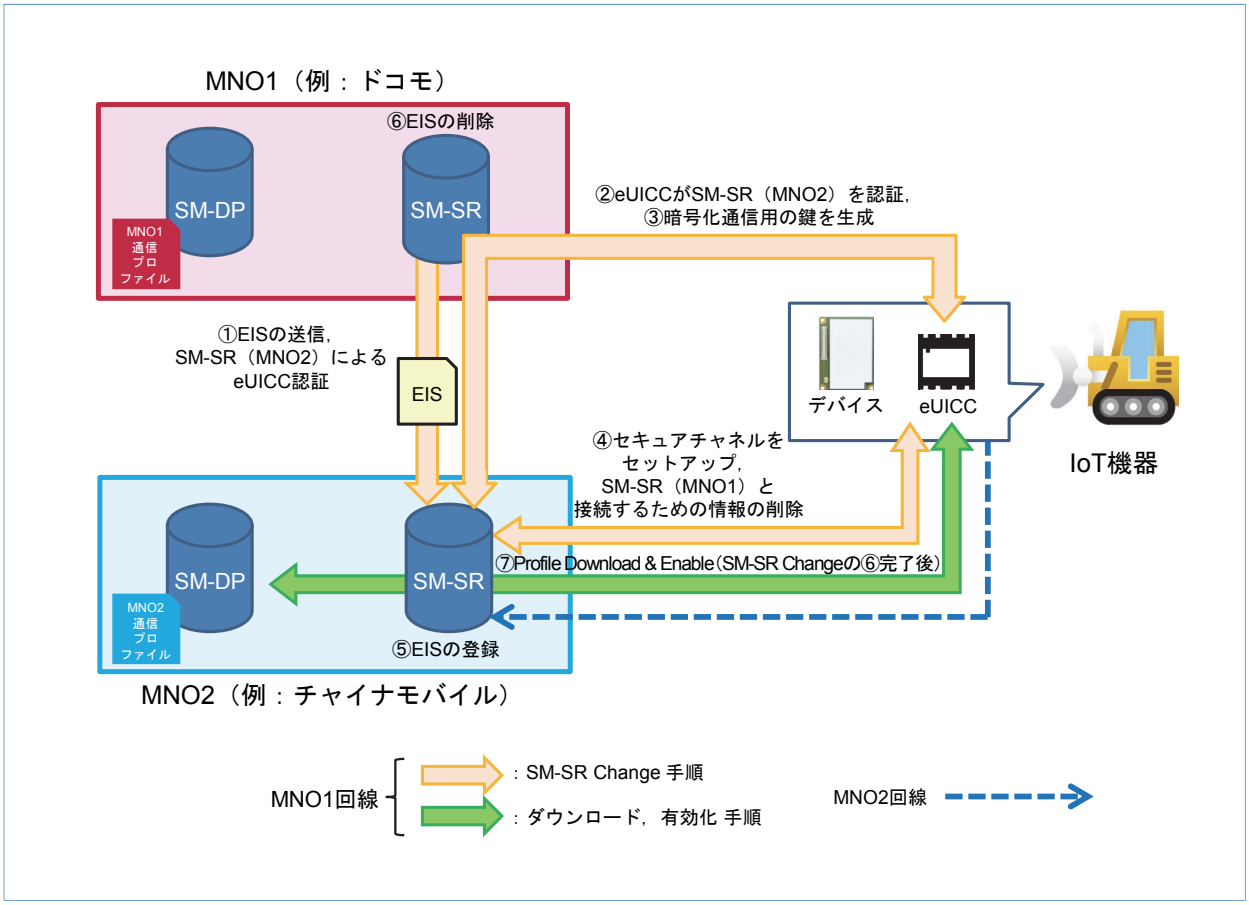

図2　構成および動作概要

SM-SR Changeの手順が必要となる．

なお，GSMA3.1の規定では，SM-DPとSM-SRは本図の例で示す構成に限定されているわけではないことを付記しておく．

3.2　SM-SR～eUICC間通信経路の概要

次にSM-SR～eUICC間の通信経路の一般的な構成例を解説する．

⑴通信経路の種別

SM-SR～eUICC間の通信経路を**図3**に示す．

GSMA3.1では，SM-SR～eUICC間においてSMSとパケット（HTTPS[*13]）による通信手段が規定されている．

SMSはサイズの小さいRemote Provisioningのコマンド送受信で利用され，パケット（HTTPS）はサイズの大きいRemote Provisioningのコマンド送受信で利用される．

なお，パケット（HTTPS）については当該通信経路の確立の前段で，SM-SR側からeUICCに対して，プッシュ型のBIP channel（Bearer Independent Protocol channel）確立を指示するSMSを送信することにより，BIP channelがeUICCとデバイスの間で確立される．

⑵SM-SR～IoT回線管理プラットフォーム[*14]間構成

SM-SRとMNOがもつIoT回線管理プラットフォームのコンポーネント間は次のように構成される．

＊13 HTTPS：TLSのプロトコルを用いてHTTPの通信を行うことでなりすまし・中間者攻撃・盗聴などの攻撃を防ぐ通信手法．GSMA3.1ではHTTPS以外にもCAT-TP（Card Application Toolkit Transport Protocol）によるパケット通信方法も規定されている．

＊14 IoT回線管理プラットフォーム：IoT/M2Mの機器を管理し収容するプラットフォーム．

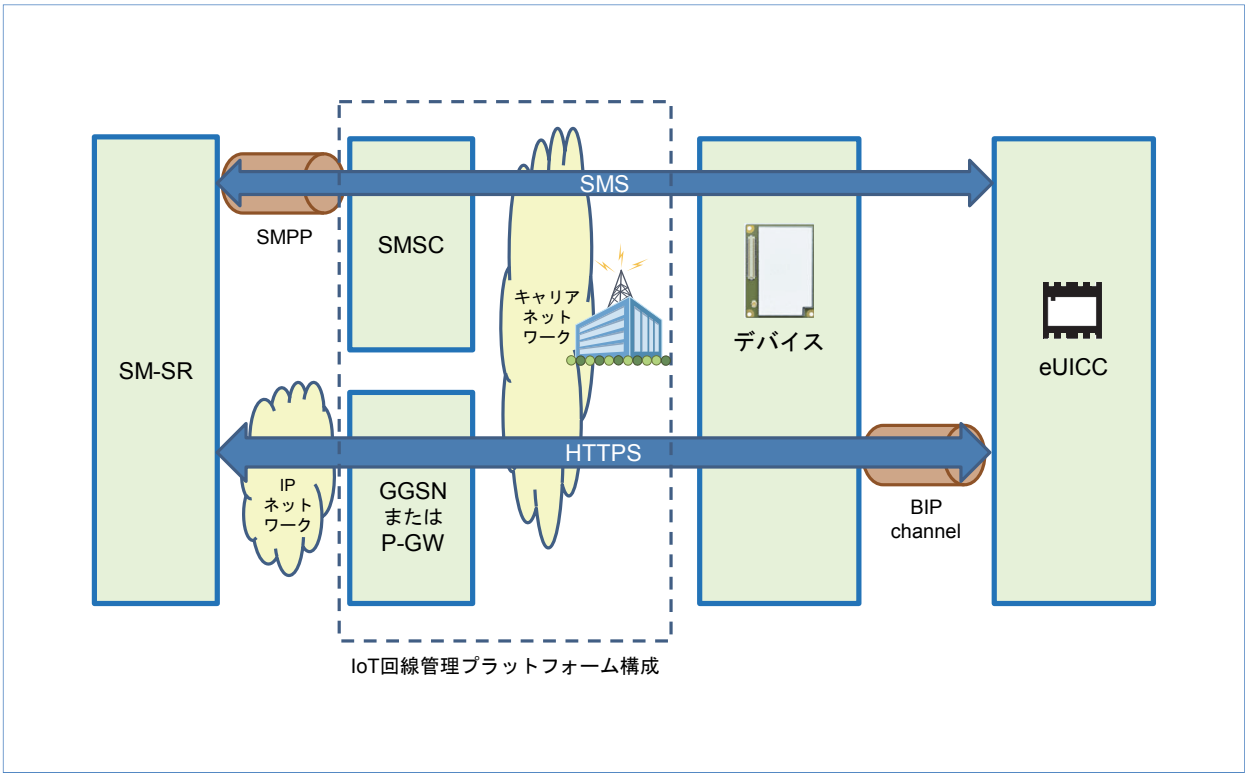

図3　SM-SR～eUICC間通信経路

・SM-SRとeUICC間でSMSによるコマンドの送受信が可能となるようSM-SRとSMSC（SMS Center）*15の間がSMPP（Short Message Peer to Peer Protocol）*16で接続される．
・SM-SRとeUICC間でパケットによるコマンドの送受信が可能となるようSM-SRとパケット交換機（GGSN（Gateway GPRS Support Node）*17またはP-GW（Packet Data Network-Gateway）*18）の間がIPで接続される．

⑶IoT回線管理プラットフォーム～デバイス間構成

通常のGSM（Global System for Mobile communications）*19/UMTS（Universal Mobile Telecommunications System）*20/LTEによる構成となるため詳細の説明は割愛する．

⑷デバイス～eUICC間構成

SM-SR～eUICC間におけるHTTPSの通信のために，デバイスとeUICCの間はBIP［11］［12］のプロトコルによる通信が必要となる．デバイス側ではBIP対応をはじめとするGSMA3.1 Annex G Device Requirementsに対応している必要がある．

3.3　Remote Provisioningシーケンス概要

⑴Remote Provisioningに必要な情報要素

Remote Provisioningの仕組みに必要な主な情報要素として以下が存在する．

・EID（eUICC ID）：eUICCの製造番号．EIDにより対象となるeUICCを特定する．
・EIS：eUICCの認証情報およびeUICCにアクセスするための情報の組合せで，SM-SRに格納される．対応するEISが登録されているSM-SRのみが当該eUICCに対してコマンドを発行できる．

＊15 SMSC：SMSのセンタサーバ．SMSの蓄積，および再送を行う．
＊16 SMPP：SMSのセンタサーバとSMS送受信用のアプリケーション間で利用される通信プロトコル．
＊17 GGSN：PDNとの接続点であり，IPアドレスの割当てや，SGSNへのパケット転送などを行うゲートウェイ．
＊18 P-GW：PDNとの接続点であり，IPアドレスの割当てや，S-GWへのパケット転送などを行うゲートウェイ．
＊19 GSM：ヨーロッパやアジアを中心に世界中で広く利用されている，第2世代移動通信方式の1つ．
＊20 UMTS：第3世代移動通信システム．ドコモ採用のW-CDMA方式のほか，TD（Time Division）-CDMA方式などがある．

⑵Remote Provisioningシーケンス

Remote Provisioningのシーケンスを**図4**および**図5**に示す.

SM-DP/SM-SRとeUICCは，互いに共通の認証局（CI：Certificate Issuer）[*21]によって証明されている認証情報があらかじめ内部に設定されており，SM-SR Change手順およびProfile Download手順においてセキュアに相互認証が取れるよう設計されている.

eUICCにはISD-R（Issuer Security Domain Root）とISD-P（Issuer Security Domain Profile）の領域が規定されている.

・ISD-R：eUICC上で1つのみ存在し，SM-SRとコマンドの通信を行う.

・ISD-P：プロファイルが格納される領域. eUICC上で複数存在し，SM-DPとコマンドの通信を行う.

ISD-R/ISD-P共に必要な認証情報へのアクセスが可能となっている.

⑶SM-SR change手順（図4）

eUICCの製造時の段階では，最初にホストとなるSM-SRにEISが登録されており，eUICCにアクセス

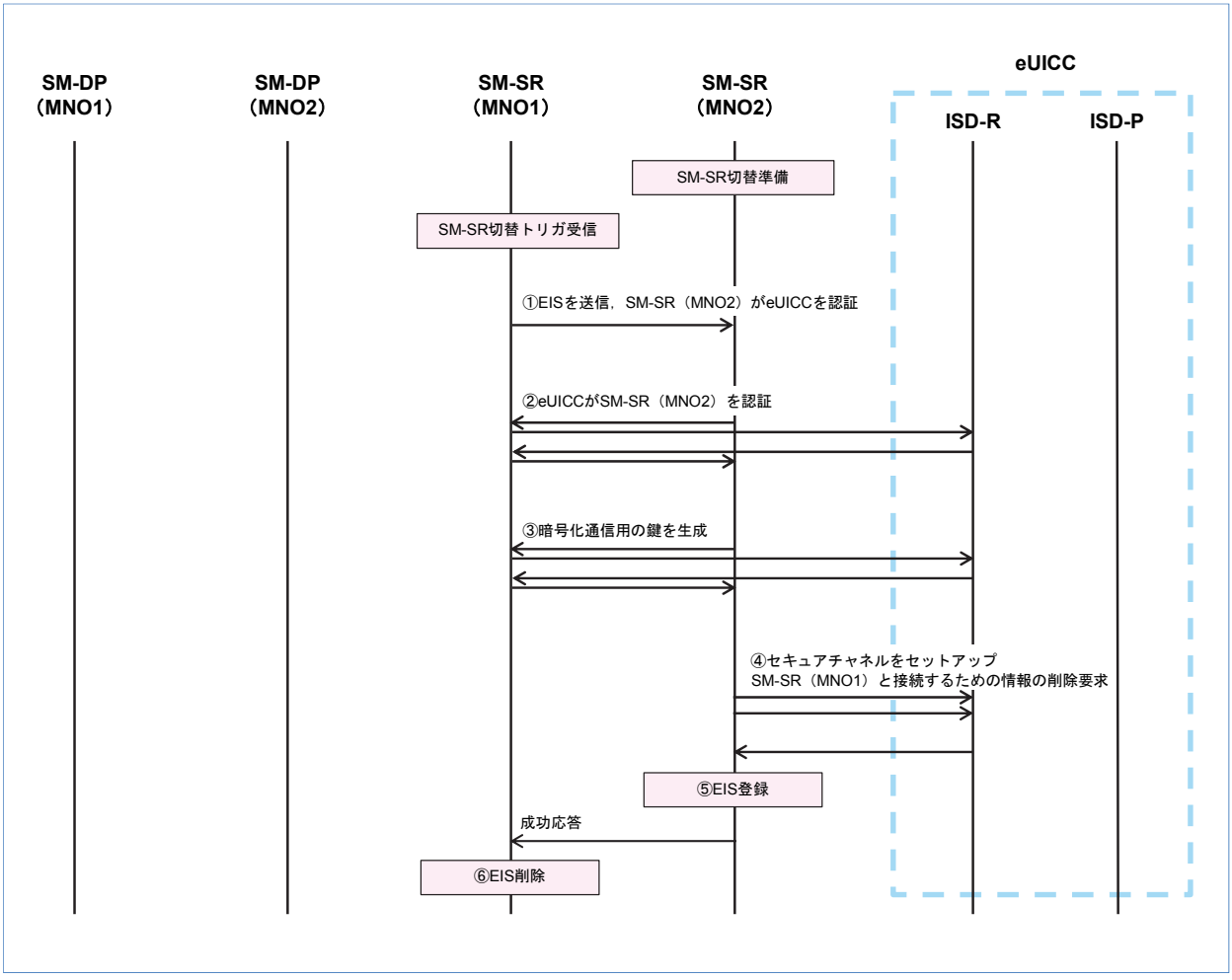

図4　SM-SR Change手順概要

＊21 認証局（CI）：セキュアなRemote Provisioningを実現するために必要な電子署名を発行する役割をもつ.

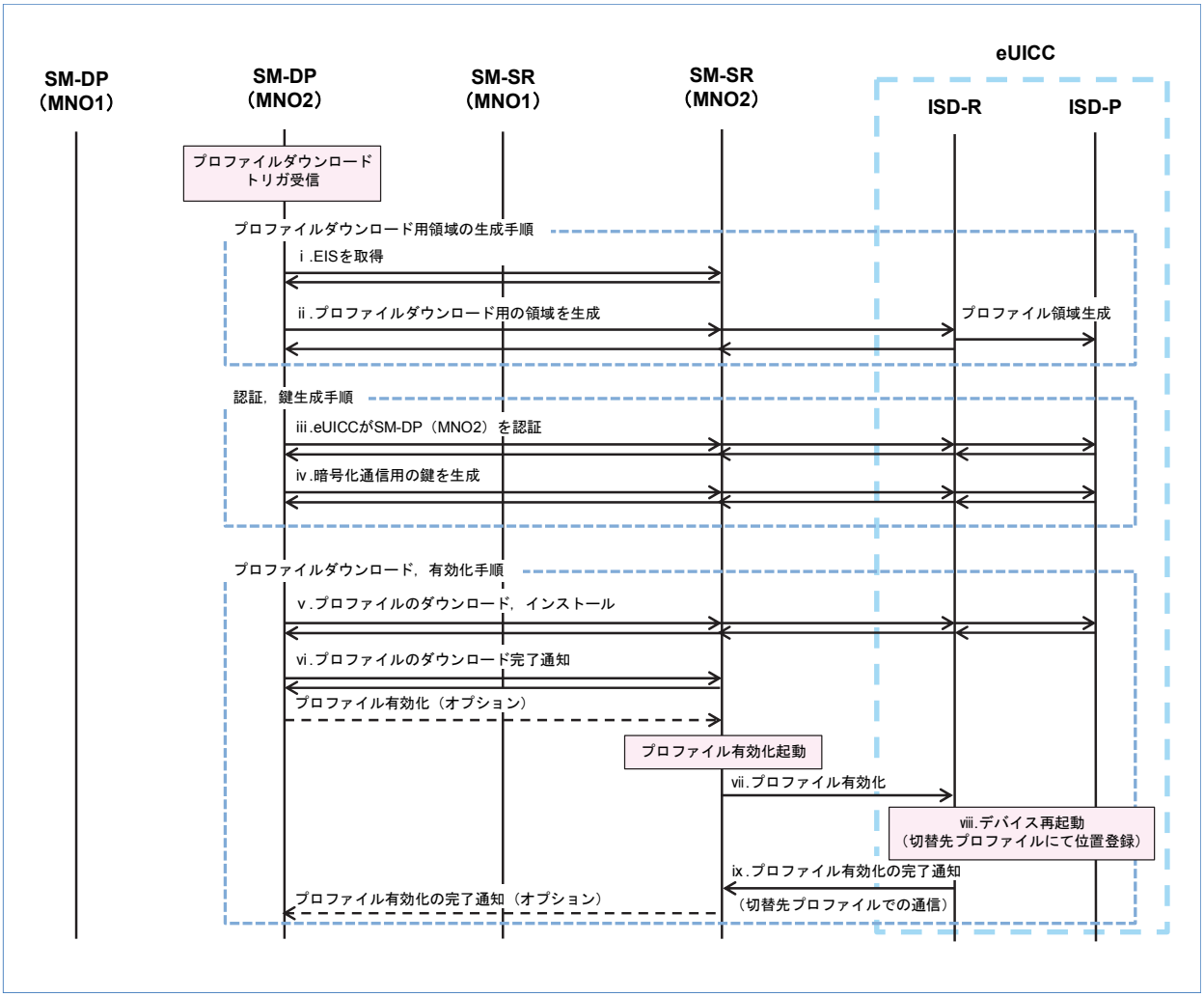

図5　Profile Download & Enable手順概要

するための管理権限をもっている．SM-SR Change手順が実施されればEISの格納先のSM-SRが切り替わり管理権限が移る．

SM-SR changeの手順は，図4に示すようにSM-SR（MNO1）からSM-SR（MNO2）にeUICCとの通信の管理権限を移譲する手順であり，以下の順番で実行される．

①SM-SR（MNO1）がSM-SR切替トリガを受信後，SM-SR（MNO1）からSM-SR（MNO2）へEISが渡される．SM-SR（MNO2）がEISに基づきeUICCの認証を行う．

②SM-SR（MNO1）を介しSM-SR（MNO2）とeUICCのISD-Rとの間で通信が行われ，eUICCがSM-SR（MNO2）を認証する．

③SM-SR（MNO1）を介しSM-SR（MNO2）とeUICCのISD-Rとの間で通信が行われ，SM-SR（MNO2）とeUICC間の暗号化通信用の鍵が生成される．

④SM-SR（MNO2）とeUICCのISD-Rとの間でセキュアチャネルをセットアップ後，SM-SR

（MNO1）と接続するための鍵情報が削除される．

⑤SM-SR（MNO2）にてEISの登録が行われる（本時点からSM-SR（MNO2）に管理権限が移る）．

⑥SM-SR（MNO1）にてEISが削除される（SM-SR（MNO1）からはeUICCにアクセスできなくなる）．

⑷Profile Download & Enable手順概要（図5）

Profile Downloadの手順により切替先のMNOの通信プロファイルの情報がeUICCにダウンロードされる．その後，Profile Enableの手順により切替先のMNOの通信プロファイルへの切替えがeUICCに指示される．

図5に示す通りProfile Download & Enableは，通信Profileを切り替えるために以下の順番で実行される．

ⅰ．SM-DP（MNO2）がプロファイルダウンロードトリガを受信後，SM-SR（MNO2）からEISを取得し，手順開始前の必要なチェックを行う．

ⅱ．SM-DP（MNO2）とeUICCとの間で通信が行われ，プロファイルダウンロード用の領域がeUICCのISD-Pとして生成される．

ⅲ．SM-DP（MNO2）とeUICCとの間で通信が行われ，eUICCがSM-DP（MNO2）を認証する．

ⅳ．SM-DP（MNO2）とeUICCとの間で通信が行われ，SM-DP（MNO2）とeUICC間の暗号化通信用の鍵が生成される．

ⅴ．SM-DP（MNO2）とeUICCとの間で通信が行われ，プロファイルがダウンロードされISD-Pにインストールされる．

ⅵ．SM-DP（MNO2）からSM-SR（MNO2）に対して，プロファイルのダウンロード完了通知が送信される．

ⅶ．SM-SR（MNO2）とeUICC内のISD-Rとの間で通信が行われ，ダウンロードしたプロファイル有効化のコマンドが送信される．

ⅷ．プロファイル有効化のコマンドを受信したISD-Rは，デバイスに対して再起動の指示を行い，デバイス再起動後はダウンロードした新しい通信プロファイルで位置登録が行われる．

ⅸ．新しい通信プロファイルでの位置登録に成功した後，ISD-RはSM-SRに対しプロファイル有効化の完了通知を行う．

4. あとがき

本稿ではGSMA3.1の標準をベースとして構築したRemote Provisioningのシステムの仕組みを解説した．今回，商用のシステムにおいてGSMA3.1の標準に対応したSMを備えたNWサービスが提供できる環境を整え，システムの結合検証を行った．

GSMA3.1では理論上はマルチベンダでの接続が可能となっている．今回のシステムを構築するにあたり，マルチベンダによる実装上の解釈の違いといった課題も一部発生したが，ドコモとチャイナモバイル間で連携することで早期に解消を図り，GSMA3.1の標準仕様を適用した，マルチベンダによるeSIMシステムを世界で初めて実現した．

現時点においては，eSIMサービスを受けるために必要なGSMA3.1準拠のデバイスがまだ少ないことなど，eSIMサービスの本格的な普及に向けていくつか課題が存在する．また，実際に製品に組み込まれ商用導入を予定するデバイスとのシステム結合試験も必要となる．今後については，これらの課題に対し，継続して取組みを進めていく予定である．

文　献

[1] NTTドコモ報道発表資料：“チャイナモバイルとドコモが世界初のIoT/M2M向けマルチベンダ間eSIM連携システムを開発，”Jun. 2017.

https://www.nttdocomo.co.jp/info/news_release/2017/06/27_02.html
［2］ GSM Association: “Embedded SIM Remote Provisioning Architecture, Version 1.1,” Dec. 2013.
［3］ GSM Association: “Remote Provisioning Architecture for Embedded UICC Technical Specification, Version 3.1,” May 2016.
［4］ 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.
［5］ 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,” 本誌，Vol.25，No.2，pp.6-13，Jul. 2017.
［6］ GSM Association: “RSP Technical Specification, Version 2.2,” Sep. 2017.
［7］ GSM Association: “RSP Architecture, Version 2.0,” Aug. 2016.
［8］ GSM Association: “RSP Technical Specification, Version 1.1,” Jun. 2016.
［9］ GSM Association: “RSP Architecture Version1.0,” Dec. 2015
［10］ GSM Association: “Remote Provisioning Architecture for Embedded UICC Technical Specification, Version 3.2,” Jun. 2017.
［11］ ETSI TS 102 226 Release9: “Smart Cards; Remote APDU structure for UICC based applications,” Jun. 2009.
［12］ SIMalliance: “UICC Configuration for Mobile NFC Payments v1.0,” Aug. 2014.