Type A/B　GP　TSM

Technology Reports

進化するおサイフケータイ―ドコモUIMカードへのNFC（Type A/B）対応サービス発行のしくみ―

現在，国内で提供されている「おサイフケータイ」は，FeliCa®[*1]をベースとしたモバイル非接触ICカードサービスである．

一方，海外に目を向けると，NFC（Type A/B）を利用したサービスが普及しており，このモバイル化が急速に進んでいる．そこで，現在のおサイフケータイの仕組みに加え，新たに開発したType A/Bを利用したサービスの発行管理を行うTSMというサーバを構築し，両方式が利用できるNFC対応の「新しいおサイフケータイ」を実現した．本稿では，このサービス発行管理の機能概要について解説する．

フロンティアサービス部　菅野 利博（すがの としひろ）　塩野入 匡宏（しおのいり まさひろ）†
木川 真孝（きかわ まさたか）

1. まえがき

ドコモでは，これまで約8年間にわたり日本国内でFeliCaをベースとした非接触ICカードサービスとして，おサイフケータイを提供し，非接触ICカードを利用したモバイルサービスの商用として，世界に先駆けて提供してきた．その結果，2012年7月末時点での利用者が，約3500万人と，世界に類を見ない普及を成し遂げることができた．

一方，海外に目を向けると，非接触ICカードの国際規格としていち早く採用された，NFC（Near Field Communication）[*2] Type A/B[*3]を利用したサービスが普及しており，これらをモバイル化したサービスが，本格商用サービスとして急速に立ち上がろうとしている．

Type A/Bについては日本国内においても，運転免許証やタスポ，住民基本台帳などで採用され，サービスが徐々に増えている状況にある．

日本では，前述のとおりFeliCaに対応したサービス（インフラ）が確立されているため，その継続利用が可能な環境を維持しつつ，グローバルマーケットへの展開も可能なType A/Bのサービスが利用できるサービス（インフラ）を追加することが必要であった．

そこで，FeliCaとType A/Bが共存する携帯電話の実現，およびTSM（Trusted Service Manager）[*4]と呼ばれるサービス発行管理システムの構築を行うことで，FeliCaもType A/Bも利用できる「新しいおサイフケータイ」を実現することが可能となった．これにより，ユーザはおサイフケータイを国内外で利用可能となる．

本稿では，このTSMの機能を中心に，新しいおサイフケータイの概要と，サービス発行管理機能について解説していく．

† 現在，日本電気株式会社　新事業推進本部

＊1 **FeliCa®**：ソニー㈱が開発した非接触型ICカード技術方式．同社の登録商標．

＊2 **NFC**：NXPセミコンダクターズ社とソニーが開始した13.56MHz帯の近距離無線通信規格で，FeliCaやMifareおよびType A/B（ISO14443）（＊3参照），ICタグ（ISO/IEC 15693）を統一してサポートしている．

＊3 **Type A/B**：非接触ICカードのうち，通信距離が10cm程度の近接型ICカードの国際標準がISO14443として規定され，この中でR/W間の通信方式の違いにより，Type A，Type Bの2つの方式が規定されている．

＊4 **TSM**：キャリア，SPから委任を受け，UIMカード（＊11参照）に対してカードアプリの1次発行を行う事業者．

2. 非接触ICカードサービスの概要

2.1 NFC

NFCは，非接触ICカードインタフェースの規格として国際標準化機構（ISO：International Organization for Standardization）[*5]で規定された国際標準の近距離無線通信技術である． FeliCaやType A/BはNFCの1つであり，このNFCの技術を携帯電話に搭載することでさまざまなサービスを提供することが可能となる．

NFCが搭載された携帯電話においては，主に以下に示す3つの機能が実現できる．

(1)カードエミュレーション機能

カードエミュレーション機能とは，クレジットカードや電子マネー，交通チケットなど，プラスチックカードの機能を携帯電話上でエミュレートする機能である．

現在のおサイフケータイにおいても，携帯電話をかざすことでiDやJR定期券を利用でき，カードエミュレーション機能として動作している．

また，携帯電話にこれらの機能を搭載することで，電子マネーの残高確認や，場所を選ばずにオンラインでチャージできるなど，利便性も向上する．

(2)R/Wエミュレーション機能

R/Wエミュレーション機能とは，携帯電話をNFC対応R/W端末として利用できる機能である．ICカードやICタグに携帯電話をかざすことで，かざされた側のICカード内に格納されたデータの参照や書換えを行うことができる．スマートポスター[*6]に代表されるサイトアクセスや，プリペイド方式の電子マネーICカードの残高照会などとして利用されている．

(3)P2P（Peer-to-Peer）機能

P2P機能は，NFC対応の携帯電話どうし，または，対応する機器（非接触IC通信機能を搭載したPC／タブレット端末／家電機器など）と，データの転送や交換を実施するための機能である．Android Beam[*7]に代表されるような電話帳データ／画像などの転送に利用されている．

2.2 カードエミュレーション機能におけるマルチアプリケーションプラットフォーム

プラスチックカードの非接触ICカードでは，1枚のICカードに1つのサービスが搭載され，カード発行事業者（イシュア）がサービス提供事業者（SP：Service Provider）[*8]としてカード全体を管理することになる．また，搭載されるサービスは固定されていることが通例であり，サービスを追加／削除することができない．

一方，NFC機能を搭載した携帯電話では，プラスチックカードと異なり，1つの携帯電話内で複数サービスを利用（搭載）することが前提であり，利用者の意思でサービスの追加や削除をすることができる．これらの環境をマルチアプリケーションプラットフォームと呼ぶ．

そのため，複数のイシュア＝SPが存在することとなり，SP以外の第三者（カード管理者）が領域を分割し，SPに割り当てるという領域管理を行う必要がある．このカード管理者の役割をキャリアであるドコモ＝MNO（Mobile Network Operator）が担い，各SPはカード管理者から与えられた領域内で，提供しているサービスの管理を行う．

また，カード管理者の役割として，利用者が安心・安全にサービスを利用できるよう，携帯電話上に搭載（発行）されるサービスが利用するメモリの管理と，不正なコンテンツ提供の防止を担う（**図1**）．

3. システム構成

カード管理者であるキャリアにとって携帯電話上のサービス領域を管理するシステムが必要になる．既存のおサイフケータイは，FeliCaを用いてサービスの管理を実現してきたが，今まで培ってきたマルチアプリケーション管理プラットフォームのノウハウを活用し，国際標準のType A/Bにも対応したインフラへ拡大した．

Type A/Bにおいては，金融業界を中心に設立されたGP（GlobalPlatform）[*9]に準拠したシステムが広く普及している．

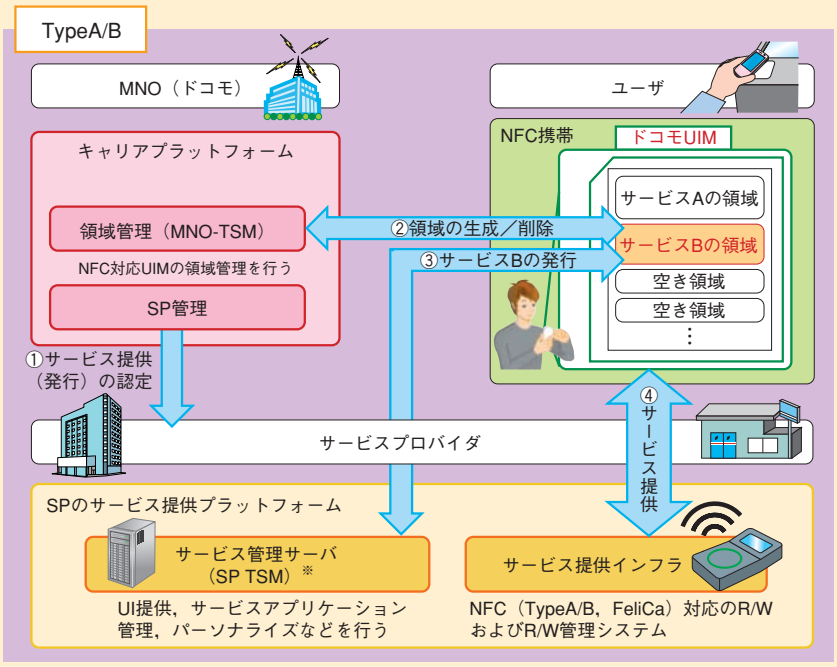
＊5 **国際標準化機構（ISO）**：情報技術分野の標準化を行う組織であり，電気および電子通信分野を除く全産業分野に関する国際規格を作成する．

＊6 **スマートポスター**：NFC Forum（近距離無線通信の普及，技術仕様の策定などを行っている団体）で規定されているブラウザ情報などを保持するタグの一種．

＊7 **Android Beam**：Android 4.0から追加されている，近距離無線通信を用いたデータ送受信機能．

＊8 **サービス提供事業者（SP）**：本稿では特に，NFCプラットフォームを利用した非接触ICカードサービス（NFCサービス）を提供する事業者のことを指す．

＊9 **GP**：リモートサーバがICカードの管理を行うための仕様を策定する標準化団体．またその仕様．当初はICクレジットカードを対象としたものだったが，その後ICカード全般に適用できるように発展した．



※サービス管理サーバはフェリカネットワークスのような他社が提供するASP機能を利用する事も可能．

図1　おサイフケータイ（NFC対応）のサービスを提供する上での全体構成

ドコモにおける，Type A/B（＋GP）の技術を用いたマルチアプリケーションを実現するシステム構成と役割を**図2**に示す．

3.1 キャリア側のシステム構成

①MNO-TSM[＊10]

GPでは，ICカード（UIM（User Identity Module）[＊11]）にキャリア網経由でアクセスするTSMが規定されており，このうちキャリアがカード管理を行うために用いるTSMをMNO-TSMとしている．このサーバを利用して，SPのサービスを提供するために必要なUIM上の領域（SD（Secure Domain）[＊12]）の構築や，サービスを提供するため必要なApplet[＊13]をインストールする処理を実施することで，カード管理を行っている．

GP上では，MNOおよびSPの責任分界点の明確な規定はない．しかしキャリアの所有物であるUIMに対し，キャリア＝領域管理者，SP＝サービス提供者であることから，SPの所有するAppletをキャリアが預かり，MNO-TSMを用いて登録することとしている．

②TSMプロキシエージェント[＊14]

GPにおいては，MNO-TSMとUIM間の通信として，HTTPやSMSなどいくつかの方式が規定されている[1]．現行のスマートフォンでの利用を考慮すればHTTPを利用した方式が極めて親和性も高いと判断できるが，GPの規定ではHTTPを利用する場合にはSCWS（Smart Card Web Server）[＊15]の利用を推奨されている．

SCWSはUIMへの実装インパクトや，他用途での利用シーンがないなど採用するうえでの懸念点が多く存在する．そのため，UIM上のSCWS機能の一部をAndroid™[＊16]上のアプリケーションとして切り出すこととした．この手法により，GPで規定されているHTTP利用時のインターフェースに準拠しながらも，SCWSを利用せずに，MNO-TSMとUIM間の通信を実現することができる．このAndroid上のアプリケーションがTSMプロキシエージェントである．

TSMプロキシエージェントは，各TSMからのHTTPによるコマンドを解析することなく，そのままUIM上のセキュア領域（SE：Secure Element）[＊17]に対して命令を実行するプロキシ的役割を担う．

③Type A/B SE

Type A/B SEとは，ICチップのセキュリティを含めたコア部分であり，サービスで用いるセ

＊10 **MNO-TSM**：MNOの責任範囲の処理を実施するTSMを指す．具体的には，APSDの作成，サービスAppletのロードなど．

＊11 **UIM**：移動体ネットワークにおけるユーザの識別情報と認証情報を格納したカード．

＊12 **SD**：カードアプリの一種．アプリケーションを管理するための特権アプリケーション．設定された特権に応じて，コンテンツのインストール／アンインストール，アプリケーションの階層（ツリー構造）管理，暗号化通信のサポートと暗号鍵の管理などを行うことができる．

＊13 **Applet**：UICC（＊25参照）プラットフォーム上で動作するJavaCardアプリケーション．UICC製造時の書き込み，もしくはTSMからダウンロードすることにより，UICCに格納される．本稿ではパッケージとインスタンスの双方を指す．

＊14 **TSM プロキシエージェント**：TSMとSE（＊17参照）の間の通信制御を担う．SEへ送信するコマンドを解析するわけではなく，TSMからのHTTPによるコマンドをそのままUICC（SE）に対して実行するプロキシ的役割を担う．

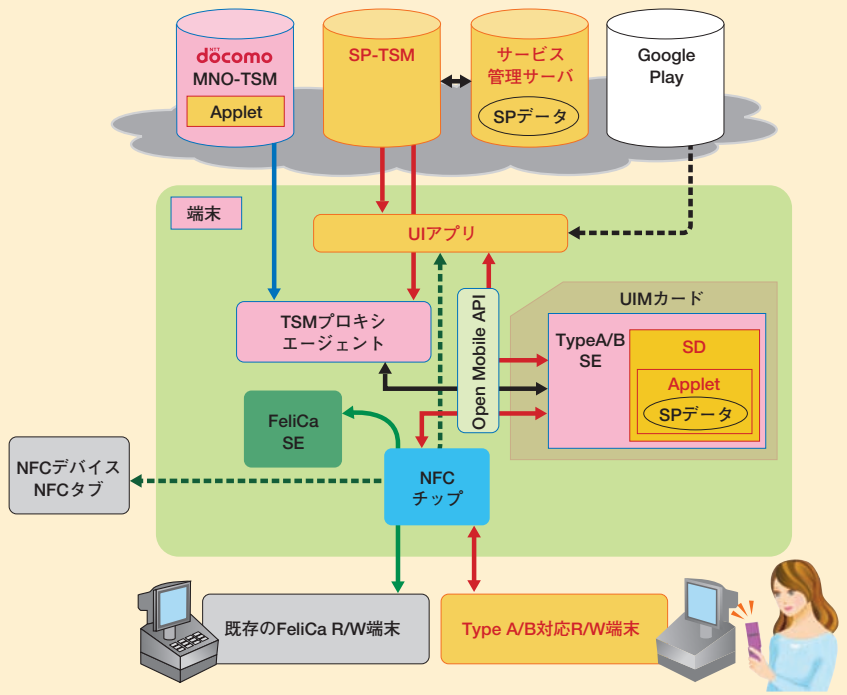


図2　Type A/B向けサービスのシステム構成

キュアなデータとAppletを管理する機能が搭載された領域である．ドコモではこのTypeA/B SEをUIM上に実装しており，後述のAppletはこれらの領域に格納される．

④端末（携帯電話）

ここで記載する端末（携帯電話）とは，NFCチップを搭載したType A/B対応サービスを利用する環境が構築された携帯電話のことを指す．

また，これらの端末にはTSMプロキシエージェントやOpen Mobile API（Application Progamming Interface）[*18]など，Type A/Bサービスを利用するうえで必要となるミドルウェア[*19]も含まれている．

⑤サービス情報一覧表示アプリ[*20]

複数サービスをマルチアプリケーションプラットフォームで利用する場合，ユーザが携帯電話（UIM）内にどのサービスを発行しているか，常に確認できる必要がある．そのため，キャリアはカード領域の管理者として，SE領域上に含まれる情報をユーザへ見える形で表示する仕組みを構築することが求められる．さらに，ユーザにとってFeliCaとType A/Bの区別なく，おサイフケータイを利用していただくことを考慮し，領域内で管理しているサービス情報を一覧表示することとした．

3.2 SP側のシステム構成

SPが構築するシステムとしては，AppletやSP-TSM[*21]，UIアプリ[*22]，R/W端末などがある．

①Applet

Appletとは，UIMに搭載するJava®アプリケーション[*23]である．Appletは，サービスを提供するうえで必要なデータをUIMで管理するとともに，UIアプリやR/W端末からの命令を処理する機能を搭載する．Appletで管理するデータの例としては，クレジットカードの番号や電子マネーなどのデータなどがある．

②SP-TSM／サービス管理サーバ

クレジットカード番号の書込み処理や電子マネーの残高書換えなど，SPの責任範囲の処理を実施するTSMをSP-TSMとしている．SPは，サービスを提供するうえで必要となるSPデータをサーバ上で管理し，携帯電話（UIM）へ格納したAppletに対してセキュアな通信を行う役割を担う．また，これらの通信内容はカード管理者にも秘匿となっている．

③UIアプリ

UIアプリとは，SPがユーザへ提供するAndroidのアプリのことを指し，ICカードを用いた

＊15 **SCWS**：UIM内でWebサーバとして動作し，遠隔でコンテンツ管理をする標準プラットフォーム．

＊16 **Android™**：米国Google, Inc.の商標または登録商標．

＊17 **セキュア領域（SE）**：ICチップのセキュリティを含めたコア部分であり，電子マネー，クレジットカード番号などセキュアな管理が必要なバリューの格納領域．UICCがその役割を担うケースのほか，携帯電話端末に埋め込まれた内蔵チップや，外部メモリーカードに内蔵するケースなどがある．

＊18 **Open Mobile API**：SIM Allianceが規定するAPIであり，UIアプリ／端末ベースバンドからUIM上のセキュア領域にアクセスするためのAPIなどが含まれている．

＊19 **ミドルウェア**：OSと実際のアプリケーションとの間に位置し，さまざまなアプリケーションに対して共通の機能を提供するソフトウェアのことで，アプリケーション開発の効率化が可能となる．

＊20 **サービス情報一覧表示アプリ**：FeliCa対応アプリとGP対応アプリを一覧で表示するAndroidアプリケーションのこと．

サービスを実現するために必要なユーザインタフェースを提供する．ユーザは，Google Play™＊24またはdマーケットから携帯電話へアプリをインストールする．

また，UIMのSE領域を用いたサービス登録やサービス利用を行う際には，UIアプリからTSMプロキシエージェントへ処理要求を送ることで，MNO-TSMおよびSP-TSMからUICC（Universal Integrated Circuit Card）＊25へのコマンドが送信される．また，電子マネーの残高表示など，Appletに書き込まれた情報をUIアプリから読み取るようなユースケースでも利用される[2][3]．

④R/W端末

携帯電話をR/W端末にかざすことで，UIMに格納されているApplet内に書き込まれたSPデータをR/W端末から読み書きし，サービス提供を行うために利用される．具体的には，レジなどでの決済時にクレジットカード番号や電子マネーの読み書きを実施する．

4. フロー／処理シーケンス

4.1 サービス発行

ユーザが利用したいサービスをインストールすることを発行と呼ぶ．

サービスを発行するためには，まずユーザがSPのUIアプリを事前にインストールする．その後，そのUIアプリを操作することにより，MNO-TSMから対応するモバイルNFCサービス＊26（Applet）をインストールし，SP-TSMからユーザの固有のデータを書込み（パーソナライズ），利用できる状態にする（**図3**）．この時，インストール処理はキャリアの責任で実施し，SP-TSMからのパーソナライズ処理はSPの責任で実施する．

4.2 Appletへのアクセス

ユーザがサービスを発行した後，サービスを利用する上ではUIアプリなどの操作によりそのサービスを提供しているApplet内のデータ書き換え等を行う場合がある．例えば，電子マネーサービスであれば，電子マネーのチャージを行う処理がこれにあたる．この際に，SP-TSMからAppletへのデータ書き換えが必要な場合は，TSMプロキシエージェントを介して処理を実行することとなる（**図4**）．

4.3 サービス削除

カード会員から退会するなど，ユーザがSPのサービス利用を止めるには，事前にSPのUIアプリなどからサービスの退会処理を実施するとともに，携帯端末（UIM）内のサービス関連データ（AppletやSDなど）を削除する必要がある．ユーザが発行したサービスを携帯電話から削除することをサービス削除という．ユーザは，SPのUIアプリを操作することにより，MNO-TSMから，当該サービスのAppletをアンインストー

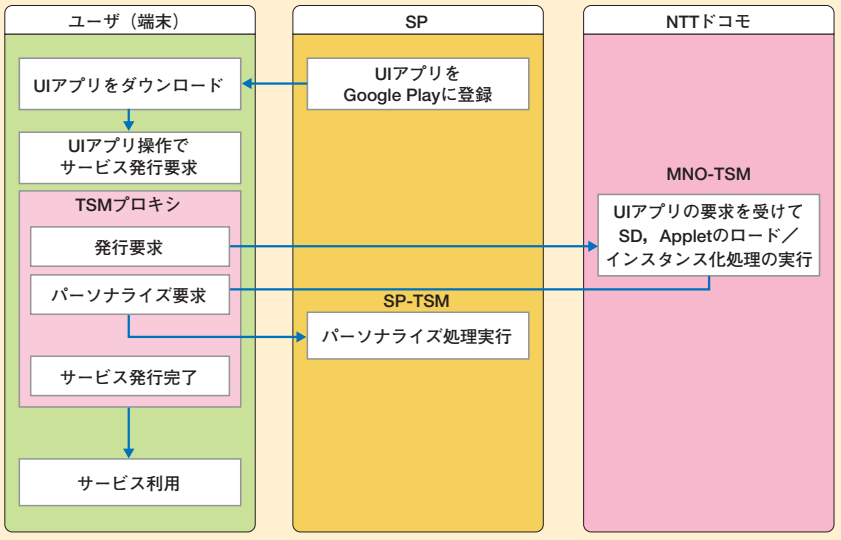


図3　サービス発行の処理フロー

＊21 **SP-TSM**：SPの責任範囲の処理を実施するTSMを指す．具体的には，パーソナライズなど．

＊22 **UIアプリ**：ユーザ向けのインターフェースを提供する移動機上で動作するアプリケーション．具体的には，Android端末におけるJavaアプリケーション（＊23参照）を指す．

＊23 **Java®アプリケーション**：Javaによって作成されたプログラムのうち，Webブラウザとは別に単独で動作できるもの．JavaAppletとは異なり，ローカルの記憶装置上のファイルを読み書きできる．なお，Androidのアプリケーションソフトは，Java言語でプログラミングされ，Linuxカーネル上で動作する．OracleとJavaは，Oracle Corporationおよびその子会社，関連会社の米国およびその他の国における登録商標．文中の社名，商品名などは各社の商標または登録商標である場合がある．

＊24 **Google Play™**：GoogleのAndroid端末向けアプリケーション・映画・音楽・書籍の配信サービス．Google Play™は，米国Google, Inc.の商標または登録商標．

＊25 **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カード，SIMカードと同義で使用している．

ルする．なお，SPのサービスによっては，事前にSPのサービスの退会処理などを実施する必要がある（**図5**）．

4.4 SP認証

前述のサービス発行や利用，削除の要求に伴う処理は，サービス運営の観点で大きな影響をおよぼす重要な処理であることから，不正（偽装）されてはならない．そのため，これらキャリアの責任範囲である重要な処理については，SP認証を実施することで，UIアプリやSP-TSMからの各処理要求が正当なものであることを認証している．

ドコモが提供するSP認証の仕組みとしては，処理要求のパラメータを用いた署名[*27]方式を採用している．また，署名元のパラメータが静的なものか，動的に生成されるものを活用するかをSPにて選択できることで，SPのセキュリティポリシーに合わせて実装できる環境を提供している．

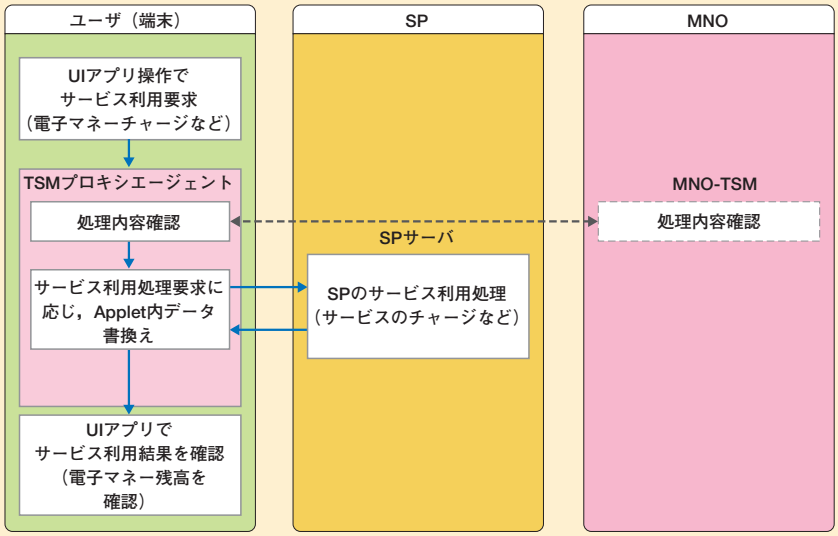


図4　サービス利用の処理フロー

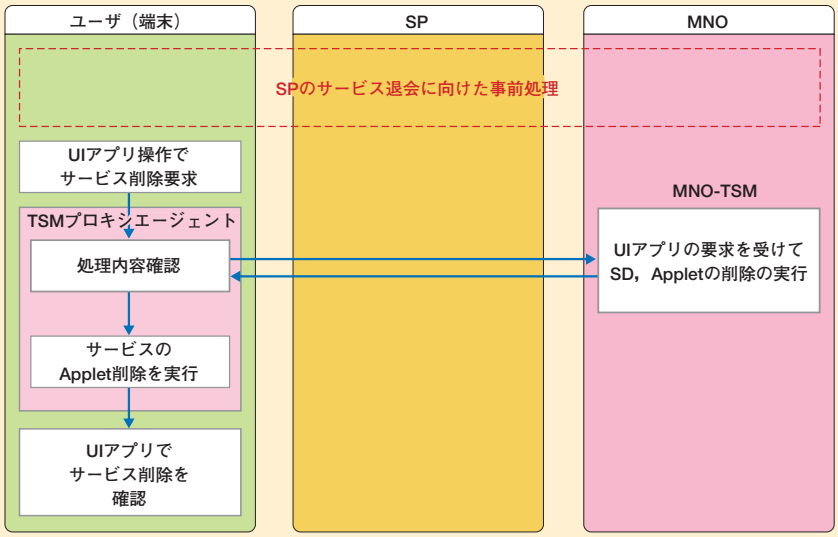


図5　サービス削除の処理フロー

5. 協議会による仕様共通化

3章で記載したMNO-TSMやTSMプロキシエージェントの仕様は，GP規格に準拠している．しかしGP規格ではSPとキャリアの責任分界点における実装の詳細が明確化されておらず，複数キャリアで仕様の差分が生じる可能性が高い．また，サービスを提供するうえでSPが構築するシステムが多く存在しており，キャリアの仕様差分が多い分だけSPの開発負担が増加することから，サービス普及の妨げになることが予想される．

そのため，国内3キャリアでは，モバイル非接触ICサービス普及協議会を設立し，SP向けの技術面／運用面での共通仕様の策定や，サー

＊26 **モバイルNFCサービス**：UICCまたはNFC対応移動機に格納されたアプリケーションの使用を前提としたNFCサービス．NFCサービスは，本稿では，主にNFC対応ICカードと対向するインフラストラクチャ（リーダ）を利用するものを指す．

＊27 **署名**：Androidアプリケーションを配布するときに必要な，開発元を証明する電子的な署名．

ビス普及拡大施策を行っている．

6. あとがき

Type A/B技術における，今後のサービスの広がりとしては，EMV規格[*28]に準拠したPayPass™[*29]やpayWave[*30]などのクレジットカードのモバイルサービスや，海外のサービス事業者が提供する電子マネーやクーポン，交通系サービスを渡航者が利用することが期待できる．

また，ドコモはマルチアプリケーションのプラットフォーム構築により基盤を築いてきたが，今後はこのプラットフォームをドコモ自身が活用し，新たなサービスを提供することによって，ユーザーの利便性向上に貢献していくことも考えていきたい．

文　献

[1] GlobalPlatform：“Remote Application Management over HTTP, Card specification V2.2, Amendment B, V1.1,” Jun. 2009.
[2] ETSI TS 102 622：“ ‘Smart Cards; UICC _Contactless Front-end(CLF) Interface; Host Controller Interface (HCI). v9.3.0,” Mar. 2011.
[3] Sun Microsystems, Inc.：“Java Card 3.0.1 Application Programming Interface,” May. 2009.

＊28 **EMV規格**：磁気ストライプ入りのカードから，ICカードへスムーズに切り替えるため，ICカードの読み取り機仕様と，磁気ストライプとICカード双方の取引実行手順を定めたICクレジットカード端末の統一規格．金融向けの規格であり，デビットカードとクレジットカードの標準仕様とされている．
＊29 **PayPass™**：MasterCardの非接触決済サービス．PayPass™は，MasterCard International Incorporatedの登録商標．
＊30 **payWave**：VISAの非接触決済サービス．