NFC　UIM　FeliCa

Technology Reports

# 進化するおサイフケータイサービスを実現する技術 ―NFC対応移動機およびドコモUIMカードの開発―

ドコモでは，国内外での近距離無線通信方式NFC TypeA/Bサービス普及と，類似機能として先行するFeliCa®[*1]サービスとの共存共栄の観点から，従来のおサイフケータイ機能の特長や使い勝手の良さを活かしつつ，NFCの国際標準仕様を取り入れた開発を行う必要があった．そこで既存の仕組みを活かしつつ，NFC Type A/Bにも対応した移動機およびUIMを開発し，2012年度より商用化した．

本稿では，NFCサービスを支える移動機およびUIMの基盤技術について解説する．

移動機開発部　秋山 友宏（あきやま ともひろ）　丹野 哲宏（たんの てつひろ）
笹川 哲広（ささがわ てつひろ）　山口 久美子（やまぐち くみこ）

## 1. まえがき

世界で広く利用されているNFC（Near Field Communication）Type A/B機能を利用した非接触タグやカードは，モバイル向けサービスとして，新たな転換点を迎えようとしている．日本では，すでにFeliCaを利用したおサイフケータイサービスが，クレジットカードや乗車券，社員証などといったさまざまな用途に利用されており，FeliCaの長所を活かしつつ非接触タグやカードをType A/Bに対応させることが求められる．また，スマートフォンに搭載するにあたって，不正アクセスや盗難などに対するセキュリティ面での対策も検討する必要がある．

ドコモでは，2012年度冬よりNFC機能に対応した移動機およびNFC Type A/BのSE（Secure Element）[*2]を搭載したUIM（User Identity Module）[*3]を商用化している．

本稿では，NFCサービスを実現するための技術的な取組みについて，移動機およびUIMの観点から解説する．

## 2. NFC概要

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）[*4]で規定された国際標準の近距離無線通信技術である．近距離無線通信とは，対応する機器と機器を数cm程度に近づけるだけで，機器どうしが認識して自動的に通信が行われ，さまざまな情報を簡単に送受信できる技術である．

NFCに対応した移動機においては，主に以下に示す3つの動作モードが存在する．本稿ではCard Emulationモードを中心に記述する．

(1) Card Emulationモード

Card Emulationモードとは，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モードである．これにより，携帯電話をR/W（Reader/Writer）機器にかざすことによって，プラスチックカード同等の機能を利用するこ



＊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 SE：暗号化鍵や秘匿情報などをセキュアに格納する領域．
＊3 UIM：電話番号などの契約者情報を記録したICカード．移動端末に差し込み，利用者の識別に用いる．UIMの例としてFOMAカードやドコモUIMカードが挙げられる．IMT-2000システムに関するITU勧告の中で，加入者情報を記憶する媒体をUIMと呼ぶ．

とができる．

アクセス方法は大きく2つに分類される．R/Wからアクセスする非接触アクセスと，残高情報確認などのために移動機からUIMのSEへのアクセスである．前者については，CLF（ContactLess Frontend）[*5]を経由しUIMのSEへアクセスを行い，店頭でかざして決済などが実現される．後者の例としては，残高情報確認以外に発行，チャージなどの際に利用されているTSM（Trusted Service Manager）[*6]サーバからUIMのSEへのアクセスが挙げられる．

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電子マネーを利用可能で，残高表示や場所を選ばずにチャージ可能など，Card Emulationモードとして動作している．

(2)R/Wモード

R/Wモードとは，携帯電話をNFC対応R/W端末として利用できるモードである．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．具体的には，スマートポスター[*7]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，ICカード情報の書換えなどを行うことできる．

(3)P2P（Peer-to-Peer）[*8]モード

P2Pモードは，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モードである．Android Beam[*9]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．

**表1**にType A/B，FeliCaの比較表を示す．外部R/W端末の通信速度に依存するが，通信速度の下限ではType A/BとFeliCaで2倍の差がある．FeliCaが高速な処理に適しているといわれるのはそれに加え，コマンドが独自である点も大きい．

**図1**に各近距離通信の関係を示す．ISOで標準化されているのは無線通信方式のみであり，コマンドや管理システムはType A/BとFeliCaで大きく異なる．Type A/BではコマンドはISO7816など，管理システムはGlobalPlatform[*10]などで規定されている．

なお「おサイフケータイ」の利用には，それぞれの管理システム，コマンドに対応したSEが必要となる．SEにはデータとアプリケーションが，耐タンパ性[*11]の高いセキュア領域に格納されており，FeliCaでは移動機内蔵チップ，Type A/BではUIMに搭載されている．本開発では，すべての通信方式および機能への対応を，移動機およびUIMで実現している．

**表1　Type A/B, FeliCaの方式比較**

| | Type A | Type B | FeliCa |
|---|---|---|---|
| 変調方式 | ASK 100% | ASK 10% | ASK 10% |
| 符号化 | Modified Miller | NRZ | Manchester |
| 速度 | 106kbps～ | 106kbps～ | 212kbps～ |
| コマンド | ISO7816 | ISO7816 | 独自 |
| 主な用途 | Taspoなど | 運転免許証など | JR定期券など |

ASK：Amplitude-Shift Keying
NRZ：Non Return to Zero

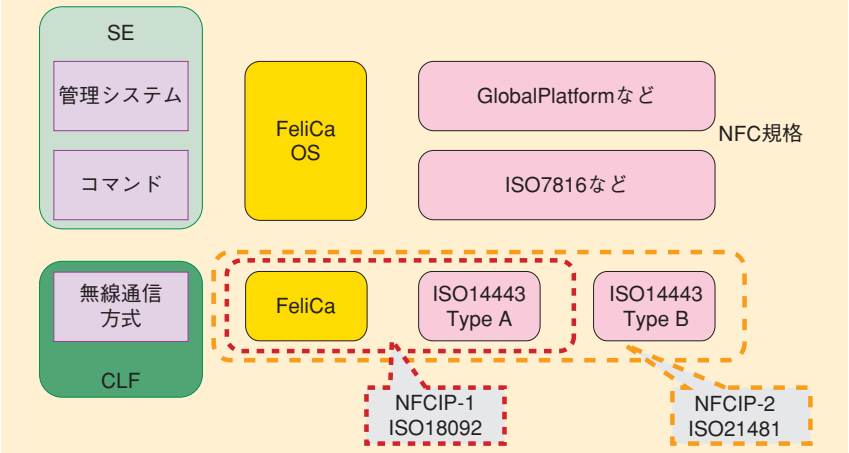


**図1　各近距離通信の関係**

＊4 **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．

＊5 **CLF**：NFCの無線通信機能を担うモジュール．

＊6 **TSM**：キャリア，サービスプロバイダから委任を受け，UIMカードに対してカードアプリの1次発行を行う事業者．

＊7 **スマートポスター**：NFC Forum（＊21参照）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．

＊8 **P2P**：サーバ・クライアント通信と対照的に，複数のコンピュータが対等な立場で相互に情報をやり取りする通信形態．本稿では，移動端末どうしや移動端末と周囲の機器が対等な立場で情報をやり取りすることを示す．

## 3. NFC対応移動機／UIM

### 3.1 NFC対応移動機の構成

(1)ハードウェア構成

**図2**にハードウェア構成図を示す．既存のFeliCaのみ搭載移動機との相違点として，次の2点がある．FeliCaのみであった非接触RF（Radio Frequency）チップであるCLFがType A/B，FeliCaの両対応となったこと，UIMとの通信を行うためのSWP/HCI（Single Wire Protocol/Host Controller Interface）が追加されたことである．

両対応のCLFチップ搭載により，Type A/B，FeliCaの無線通信方式を自動判別して受信することが可能となる．SWP/HCIはETSI（European Telecommunications Standards Institute）[*12]で標準化された通信方式であり，UIMとCLFチップ間を物理的な一本の通信路（Single-Wire）で接続し，双方向の通信を行うことが特徴の通信方式である．

(2)ソフトウェア構成

**図3**にソフトウェア構成図を示す．Android™[*13]OS層に実装されたNFCミドルウェア[*14]，Open Mobile API，Access Control，について述べる．なお，アプリケーション層に実装されたTSMプロキシエージェントはUIMとTSMサーバの通信制御を担うアプリケーションである（詳細は文献[9]参照）．

①NFCミドルウェア

NFCミドルウェアについては前述の3つのモードのうち，R/W，P2Pを実現している．また，Android OSではDiscoveryモードという機能が搭載されている．設定により画面がONなどの条件下でタグや対向移動機を自動で検出するため搬送波を送出する機能であり，NFCミドルウェアで実現している．

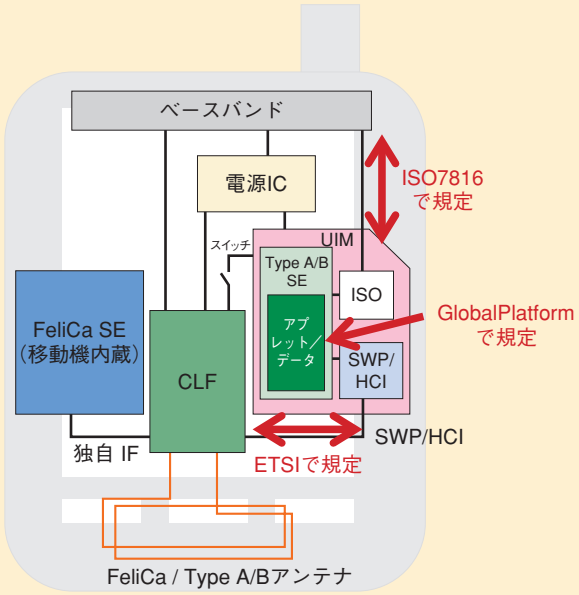


**図2　NFC対応移動機およびUIMのハードウェア構成図**

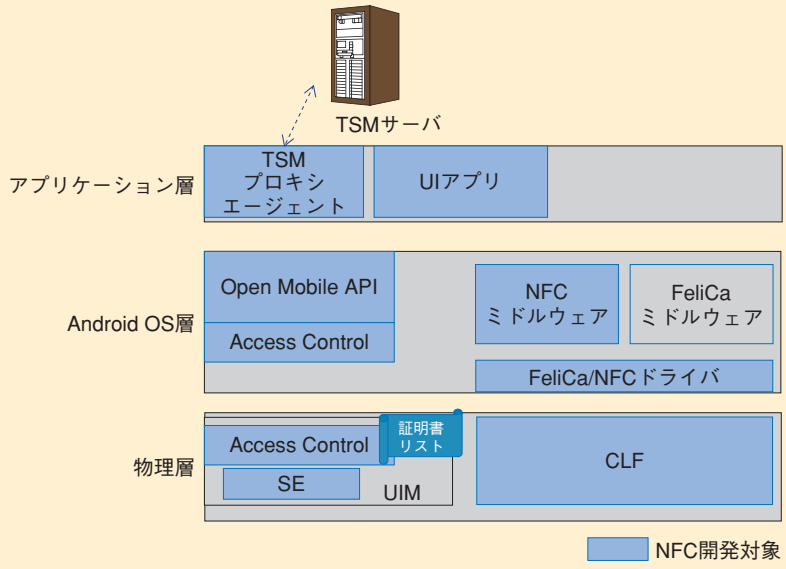


**図3　NFC対応移動機およびUIMのソフトウェア構成図**

---

＊9 **Android Beam**：スマートフォン同士で近距離無線通信を用いてデータ送受信を行う機能．

＊10 **GlobalPlatform**：VISA Open Platform仕様をベースとしたカードプラットフォームの標準仕様．金融業界を中心に規定．

＊11 **耐タンパ性**：内蔵するプログラム，データなどの不正な参照や書換えを防止する性質．

＊12 **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．

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

②Open Mobile API

Open Mobile APIはUIMへのアクセスAPIである．Android OSではUIMへの汎用的なアクセスAPIが提供されていないため，SIMalliance[1]で標準化されたAPIを搭載している．実現にはオープンソースを利用することで，開発負担の軽減をしている．サービスプロバイダがコンテンツ（NFCアプレット＊15）を提供するうえで最低限の共通仕様を規定している．

③Access Control

Access ControlはUIMへのアクセス制御を行うアプリケーションである．本UIMには，クレジットカードアプリを始め，セキュアに保持されるべき多くのアプリケーションおよび情報が格納されることが想定されるため，移動機からのアクセスを適切に制御することにより，ユーザに安心して利用いただくことが重要である．しかしながら，UIMへのアクセスを可能にするAPIを用意することにより，悪意のあるアプリケーションから攻撃のおそれがあるため，それを制御するためにGSMA（Global System for Mobile communications Association）＊16[2]で標準化されたのがAccess Control機能である．UIM内に各UIアプリ＊17を署名＊18した証明書（HASH値＊19）のリストを保持しており，それらとアクセスするUIアプリ自身が所持する証明書からHASHした値を移動機で照合することにより，制御を行う．

例えば，ユーザが移動機のUIアプリAのサービスを利用したい場合，ユーザ操作により，UIアプリAからインストール要求を受けたTSMプロキシエージェントは，TSMサーバに対してサービス発行要求を行う．発行要求を受けたTSMサーバは，サーバ内のNFCアプレットAのダウンロードおよびインストール処理を行う．その際TSMサーバは，UIアプリAの証明書（HASH値）も発行する．これらを受けたTSMプロキシエージェントは，Access Control経由でUIM内の証明書リストにNFCアプレットAに紐付けて当該証明書（HASH値）を保存し，UIM内のSEにNFCアプレットAをインストールする（**図4**）．

その後，UIアプリAからUIM内のNFCアプレットAに対し

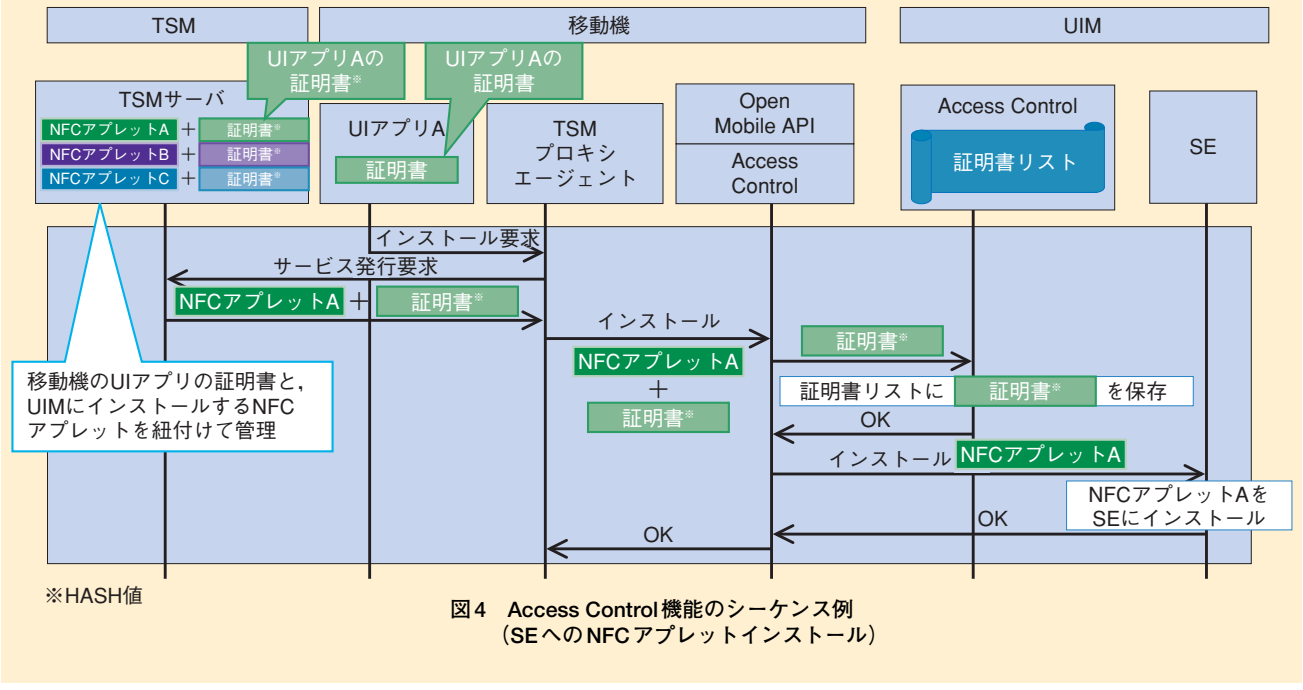


図4　Access Control機能のシーケンス例（SEへのNFCアプレットインストール）

＊14 **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．

＊15 **NFCアプレット**：UIMに搭載するNFCサービス用アプレット．

＊16 **GSMA**：携帯電話事業者を代表する世界的な業界団体．

＊17 **UIアプリ**：ユーザ向けのインタ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アプリを指す．

＊18 **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．

＊19 **HASH値**：HASH関数で演算した値．

てアクセス要求が行われる際，移動機のAccess Controlから，UIMの証明書リストに対して，NFCアプレットAに紐付けて格納された証明書（HASH値）の取得を要求する．UIアプリAの所持していた証明書をHASHした値と，ここで取得したNFCアプレットAに紐付いた証明書（HASH値）を照合し，問題なければUIM内のNFCアプレットAへのアクセスが許可される（**図5**）．証明書リスト内の当該証明書（HASH値）と照合失敗した場合には，NFCアプレットへのアクセスはエラーとなる（**図6**）．これにより，許可されていないアプリケーションからの不正なアクセスなどを防止することが可能となる．

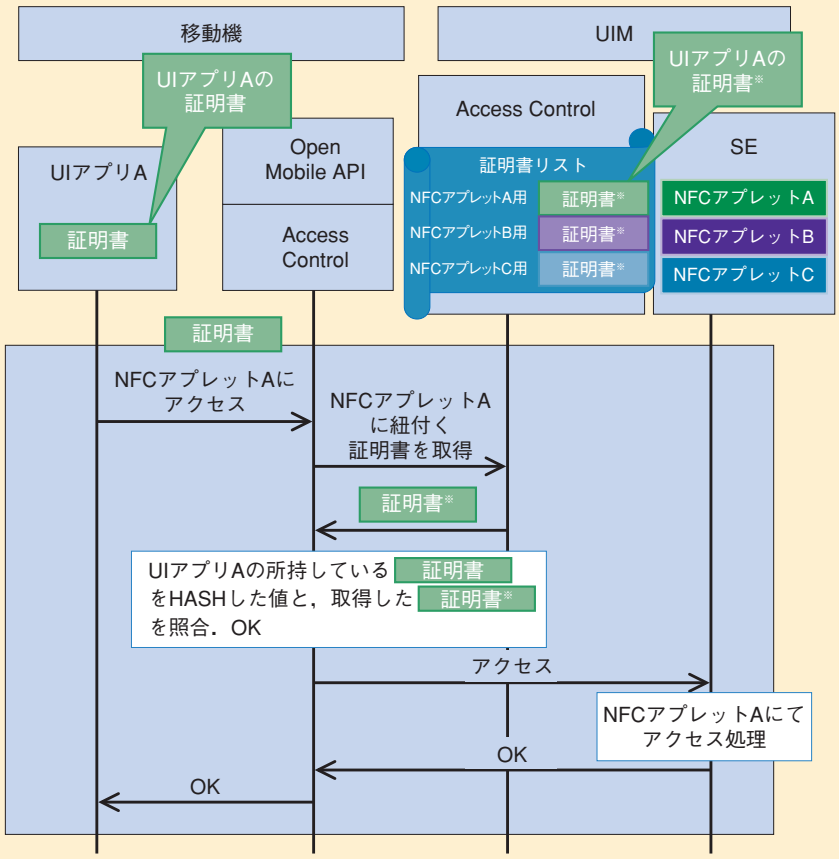


**図5　Access Control機能のシーケンス例（NFCアプレットへのアクセス（成功））**

## 3.2　NFC対応UIM（ドコモUIMカード）の構成

本UIMは，移動機のベースバンド[*20]と接続するISO7816インタフェースと，移動機のCLFと接続するSWP/HCIインタフェースの2つのインタフェースを持つ（図2）．前者は従来の3GやLTEなどの通信や位置登録などのために移動機との間でコマンドを送受信するために用いられているインタフェースであり，今回の開発対象であるGlobalPlatform対応のコマンドも本インタフェースを使用して送受信する．一方，後者のSWP/HCIインタフェースは，非接触R/Wからのコマンドを CLF経由で送受信するのに用いられる．

UIM内部には，GlobalPlatform規定の機能を実現するさまざまなアプリケーションおよびデータを格納するためのセキュア領域としてSEを有している．

# 4. NFCの特徴

## 4.1　NFC標準準拠機能

### (1) NFC Forum[*21]

NFC Forum[3]では前述の3つのモードのうち，R/W，P2Pモードを主に標準化している．タグの種類や，タグ検出時の動作，P2Pを実現するためのプロトコルなど規定しているが，本移動機はこれらに対応している．今後，安価なNFC タグが普及すると予想され，タグを利用したスマートポスターなどユーザに身近なコンテンツの普及が始まると，移動機を利用した情報取得や，現実世界との連携などが多彩になると考えられる．

### (2) GlobalPlatform

GlobalPlatform仕様はもともとVISA International社がクレジットカード向け仕様を規定したVISA OPEN Platform仕様がベースとなっている．中でもGlobalPlatform Card

＊20 **ベースバンド**：デジタル信号処理を行う回路またはその機能ブロック．

＊21 **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．

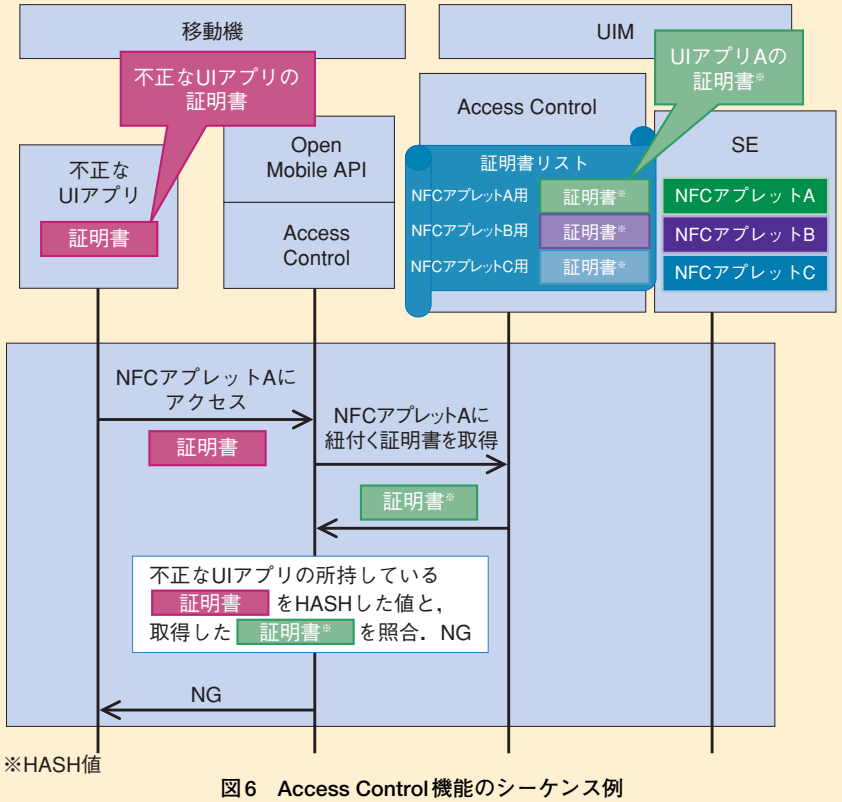


**図6　Access Control機能のシーケンス例（NFCアプレットへのアクセス（失敗））**

Specification[4]は，Java Card™＊22仕様などに準拠した，カードコンテンツの追加（インストール）および削除（デリート）などの用途を想定した各種コマンドおよびセキュリティの仕組みについて規定した公開仕様であり，主に金融系のカードなどで広く参照されている．これに加え，モバイル環境で利用されるUIMを想定してより詳細なパラメータなどを規定したGlobalPlatform UICC（Universal Integrated Circuit Card）Configuration[5]や，非接触R/Wからアクセスされるカード内非接触サービスコンテンツの状態変更や画面表示を想定したGlobalPlatform Card Contactless Services Card Specification - Amendment C[6]も存在し，本UIMはこれらすべてに対応している．

これらの技術仕様に準拠することで，本UIMが保持するセキュア領域へTSMから遠隔でアプリケーションをインストールする機能，およびCLF経由で非接触R/WからUIMのアプリケーションへアクセスする機能を実現する．

(3) ETSI

ETSIではUIMとCLFの通信方式であるSWP/HCIについて規定がされており，本UIMはこれらに準拠している．参照技術仕様[7]はSWPについて規定がされており，参照技術仕様[8]はHCIについて規定がされている．

本技術仕様に準拠することで，CLFを経由してUIMへ通信を行う非接触インタフェースの通信を実現する．

## 4.2 NFC拡張機能

(1) ロック機能

安心・安全という観点より，既存FeliCa機能でもロック機能が実現されている．ロック機能はユーザが意図したロックを行うローカルロックと，紛失した際などに必要となる遠隔ロックの大きく2つに分類される．本開発におけるNFC Type A/Bでも同様の機能が具備されている．

しかし，NFC Type A/Bに対応したUIMは決済サービスなどのアプリケーションを保持した状態で対応した移動機より挿抜される可能性がある．そのため，移動機のロック機能とは独立してUIMのNFC Type A/B機能をロックする機能が必要である．

本UIMでは，移動機から独立した状態管理を実現している．また，従来のFeliCa機能と融和性を高めるために遠隔ロック，およびローカルロックの2種を独立させて状態管理できる実装とした．

UIMにロック機能が搭載されたことにより，ロック状態制御が複雑になる．さらにFeliCaとUIMでのロックパスワードが異なる場合を考慮しなくてはならない．ユー

＊22 Java Card™：米Sun Microsystems社（現Oracle社）が開発したICカード用プラットフォーム．Oracle社の商標．

ザが混乱することなく操作をすることを考慮し，ロック，ロック解除時に一定のパターンを設けることとした．**表2**に提示したようにUIM，FeliCaのうち一方のみロックがされている場合は解除のみ実施可能とし，複雑な状態となることを回避している．

⑵Access Controlアプリケーション

3.1節で述べたように，UIM内部に新たにアプリケーションをインストールする際などにはAccess Controlと呼ばれるアプリケーションに都度登録を行うことによって，アクセス制御を行う．

海外事業者ではAccess Control機能を実現する際，アプリケーションではなくファイル形式で実装する場合も見られるが，本UIMでは，あえてアプリケーション形式を採用している．ファイル形式を採用する場合には，NWサーバから遠隔でUIM内のファイルを更新する制御が必要となるため，TSMサーバとNWサーバがリアルタイムで連携する必要がある．しかしながら，アプリケーション形式の場合には，今回開発したGlobalPlatform準拠の機能によりUIM内の他のアプリケーションと同様にAccess Controlアプリケーションも TSMサーバから遠隔で更新可能となるため，NWサーバへの追加開発や制御が不要となり，システム全体の構築および運用が容易である．

⑶FeliCaとの共通化

既存機能であるFeliCaとは図2で示しているようにアンテナ，CLFは共通で利用しているが，ソフトウェアではミドルウェアから分離され独立して動作している．しかし，同じCLFを利用するため，FeliCaとNFC Type A/Bの制御を行う必要があり，ドライバで競合管理を行っている．例えば，NFC Type A/BのP2P動作時にFeliCaのバリューチャージが実行された場合，処理が衝突してしまうため排他制御を行っている．

また，FeliCaでは電源ON時にはもちろんのこと，電池残量がある状態での電源OFF時にも利用可能である．ユーザにとって，FeliCaと同じ利便性を実現するため，同様の動作となるよう仕様を規定した．これらは国内3キャリアで協議され，共通仕様ともなっている．例えば，電源OFF時にCard Emulationを動作させるにはUIMに電源供給する必要があるが，UIMの電源供給を常に続けることは消費電力の観点から望ましくなく，搬送波検出時のみ電源供給する仕組みとした．その際，UIMへの電源供給のタイミングは，電源ON時には既存のISOインタフェース利用に依存し，電源OFF時にはCLFを経由し，今回新たに加わったSWP/HCIインタフェース利用タイミングに依存している．制御が複雑になるため，CLFに搭載された搬送波検知機能とスイッチを用いた制御機構を実装している．

表2　ロック／ロック解除パターンの例

| 状態 | FeliCa | UIM | 可能な操作 |
|---|---|---|---|
| A | ロック | ロック | 解除のみ |
| B | 解除 | 解除 | ロックのみ |
| C | ロック | 解除 | 解除のみ |
| D | 解除 | ロック | 解除のみ |

※例えば，状態CやDにあるとき，FeliCa/UIMの両者をロックするには，いったん状態Bに遷移した後，状態Aに遷移すればよい．

## 5. あとがき

本稿では，新たに開発したNFC対応移動機とUIMの機能概要を解説した．

本開発では既存の仕組みを活かしつつ，グローバルスタンダードのType A/BをUIMのSEに取り込んだが，FeliCaのSEが移動機側に，Type A/BのSEがUIM側にあるため，SEの管理が煩雑になっている．そこで将来に向けてはFeliCa SEもUIMに搭載することを検討している（**図7**）．しかし，上記実現には日本の交通機関の改札で求められる処理速度要件を満たせないことなどが課題として挙げられる．現在とは別のSEをUIM内に搭載すれば処理速度要件は満足できる可能性もあるが，UIMの形状がMini-UICC（miniSIM）[*23]や4FF（nanoSIM）[*24]に小型化・薄型化する傾向にある中，現時点で実現は困難と考えられ，今後のさらなる検討が必要である．

＊23 **Mini-UICC（miniSIM）**：ETSIにて規定されたUIM物理形状の規格．標準化上の正式名称はMini-UICC．従来のUIM（Plug-in UICC）が25×15mmであるのに対し，15×12mmに縮小されている．厚みはともに0.76mmで端子配置も同じ．

＊24 **4FF（nanoSIM）**：4th Form Factorの略．ETSIにて規定されたUIM物理形状の規格．3FFからさらに縮小され，12.3×8.8mm．端子配置は同じだが，厚みは0.67mmに変更された．

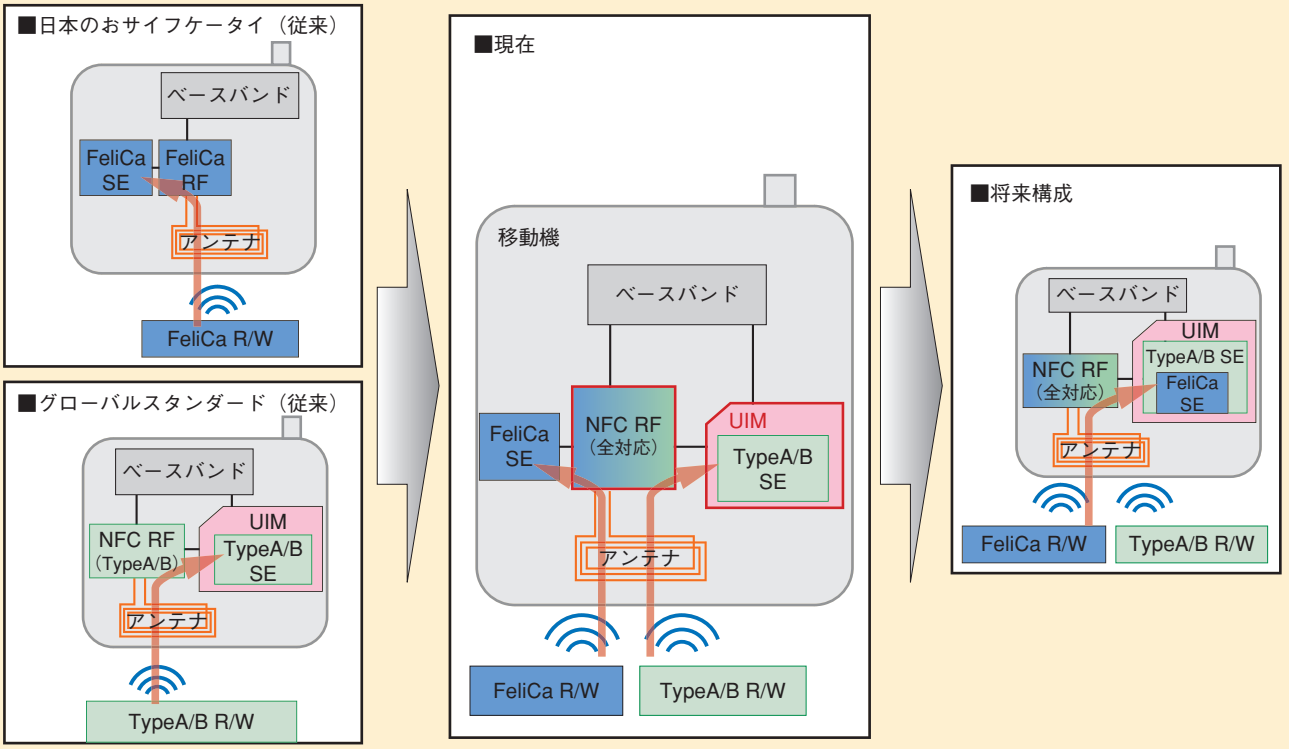


**図7　NFC移動機およびUIMの構成の変遷**

NFC関連機能については今後も国内外のさまざまな用途での利用が想定されており，上記検討事項を含めサービス・機能の両面からユーザ利便性のさらなる向上に向けた検討を行う．

## 文　献


[1] SIMalliance：“Open Mobile API Specification v2.02,” Nov. 2011.

[2] GSM Association：“NFC Handset APIs & Requirements v2.0,” Nov. 2011.

[3] NFC Forum：“NFC Forum Device Requirements v1.0,” Oct. 2010.

[4] GlobalPlatform：“GlobalPlatform Card Specification v2.2,” Mar. 2006.

[5] GlobalPlatform：“GlobalPlatform Card UICC Configuration v1.0.1,” Jan. 2011.

[6] GlobalPlatform：“GlobalPlatform Card Contactless Services Card Specification v2.2 - Amendment C v1.0,” Feb. 2010.

[7] ETSI TS 102 613：“Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics v9.2.0,” Mar. 2011.

[8] ETSI TS 102 622：“Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) v9.3.0,” Mar. 2011.

[9] 菅野，ほか：“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―，” 本誌，Vol.21，No.1，pp.22-28，Apr. 2013.