Technology Reports

安全な電子価値流通のためのTENeT仕様と実現技術

2006年春に，安全な電子価値流通のための仕様であるTENeT仕様群がT-Engine Forumにおいて標準化された．安全な電子価値流通を実現する技術の1つである，新しいICカード通信アーキテクチャについての概要を解説する．

寺田 雅之　森 謙作　本郷 節之

1. まえがき

著者らは，電子価値（例えば各種のポイントやクーポン，チケットやコンテンツ再生権など）を，利用者間で安全に取引するための技術を研究開発してきた．この技術は，移動端末を持った利用者どうしで電子価値の売買や相互交換を行うことができる，安全かつ公平な電子市場サービスを実現可能としている[1][2]．

また，研究開発と並行して電子市場サービスを迅速に展開していくための仕様策定と標準化活動を，標準化団体であるT-Engine Forumにおいて展開してきた．策定した仕様は，同フォーラムにおいて一連の標準仕様群として制定され，2006年春に一般公開された[3]～[7]．以後，これらの標準仕様群をTENeT（Trusted Environment with Networking eTRON[*1]）仕様と総称する．

TENeT仕様の策定にあたっては，電子市場サービスを実現するためのアプリケーションプログラム（AP：Application Program）を，移動端末やICカードスロットを備えた携帯情報端末（PDA：Personal Digital Assistance）などのモバイル機器上に簡単かつ効率良く構築できることを設計目標の1つとした．この目標を実現するため，著者らは東京大学と共同で，複数のICカードを連携させた（電子価値取引などの）分散処理をサポートする，新しいICカード通信アーキテクチャを確立した．

本稿では，仕様策定の目的と本仕様が実現可能とするサ

＊1　eTRON：複製や改ざんが困難な電子情報である「電子実体（electronic entity）」を実現し，情報機器間で流通させるために，T-Engine Forumを中心として開発が進められている，ユビキタス環境を構築するためのセキュリティインフラ．

ービス例を示すとともに，その設計目標と実現技術の概要と，仕様策定と並行して行った試作実装の概要と評価結果を述べる．

2. 仕様策定の目的

T-Engine Forumは，「あらゆるものにコンピュータが入りネットワークでつながれる」ユビキタス・コンピューティング環境の構築を目指した標準化団体であり，組込み機器[*2]で高いシェアを持つITRON OS（Industrial TRON Operating System）[*3]の後継となるT-Kernel[*4]，組込み機器の安全性を保証するための耐タンパ性[*5]を提供するeTRONなどの仕様策定を行っている[3]．TENeT仕様は，前述のeTRON仕様に対して大幅な拡張を加え，モバイル組込み機器上の利用者AP（iアプリなど）を用いて，UIM（User Identity Module）[*6]などのICチップに格納された電子価値を安全に取引・利用するサービスを簡単かつ効率良く構築すること，およびこれらを実現するICカードやAPの相互運用性を確保することを目的として制定された．

本仕様により実現可能となるサービスのイメージ例を**図1**に示す．それぞれの利用者はTENeT仕様を実装したICカードとモバイル機器を所持している．利用者はこれらの機器を用い，ネットワークを介して自由に電子価値の売買や交換を行うことができる．

3. 設計目標と課題

ユビキタス・コンピューティング環境を実現するTENeT仕様を策定するにあたり，設計目標として以下の4点を設定した．

①さまざまな電子価値を統一的に扱えること．

②ネットワークを介した「顔が見えない」相手とでも安心して取引が行えるように，「お金を払ったのにチケットがもらえない」などの不正を防止できること．

③本仕様を利用するAPの構築を容易にするインタフェースを提供すること．

④リソースが限られたデバイスであるICカードやモバイル機器上でも，効率的に実装可能であること．

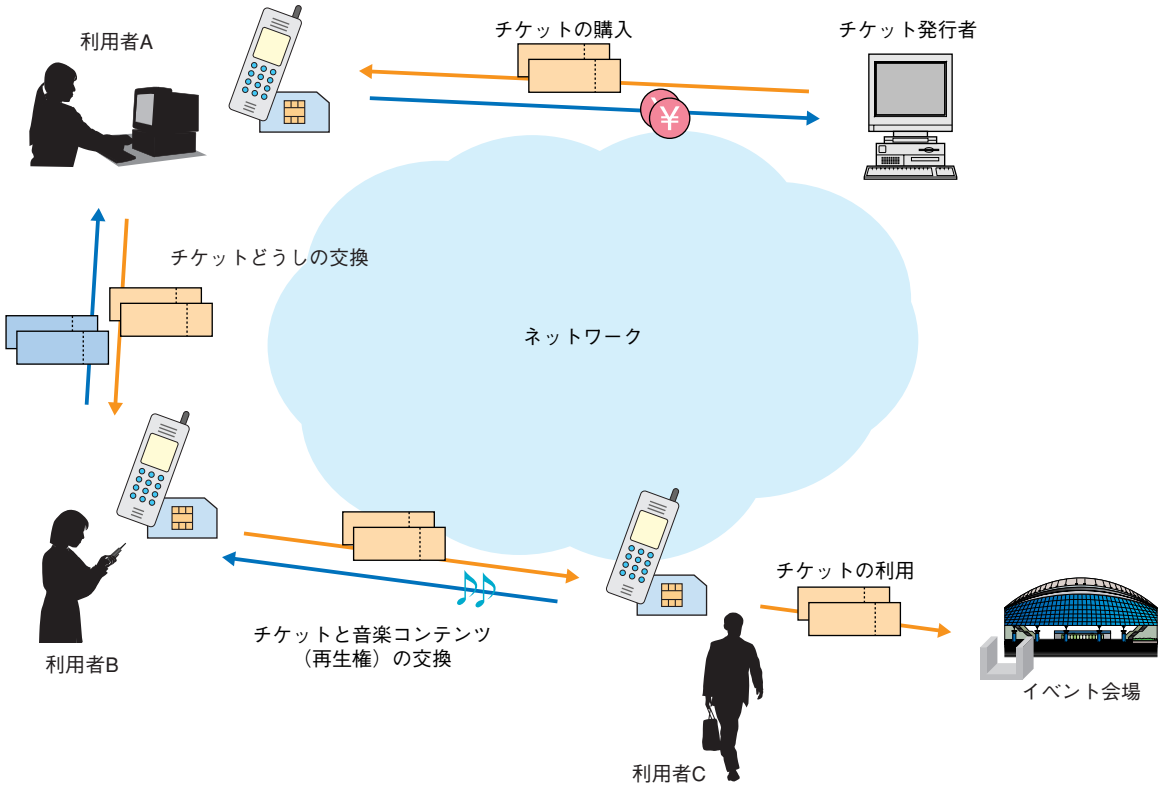

図1　TENeT仕様が実現するサービスのイメージ

＊2　組込み機器：携帯情報端末や家電製品など，CPUとソフトウェアが搭載され，用途が特定されている機器．

＊3　ITRON OS：組込み機器向けのリアルタイムOSの規格の1つ．第2世代移動端末のOSとして広く採用された．

＊4　T-Kernel：リアルタイムOSの規格の1つ．ITRONの技術を基に開発され，各種資源の動的管理機能などが拡張されている．

＊5　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．

＊6　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カードが挙げられる．

前述のうち，目標①，②については，「電子価値取引のための楽観的な公平交換プロトコル」の技術を確立し，これを用いることにより達成した[2]．

このプロトコルはICカード間の分散プロトコルとして実現されることを前提としている．しかし，ISO7816などの従来のICカードインタフェース仕様は複数のICカードが相互に通信するような利用法を想定しておらず，これらの仕様をそのまま用いるとAPの実装が複雑になるという問題が生じる．

例えば，ISO7816においてICカードとやり取りするコマンドフォーマットを規定しているISO7816-4[8]は，ホスト（ICカードを内蔵した移動端末といったようなICカードを使用する機器）からICカードにコマンドを送り，ICカードがそのコマンドに対する処理結果をホストに返送するという，ホストとICカード間に閉じた単純なアクセス方法のみを提供する（**図2**）．これを用いてICカード間の分散プロトコルを実現しようとする場合，各移動端末上のAPはICカード間でやり取りされるメッセージを適宜コマンドに変換しながら中継する機構を提供する必要が生じる．これはAPの構成と実装を煩雑にし，目標③，④の達成を困難にする（**図3**）．

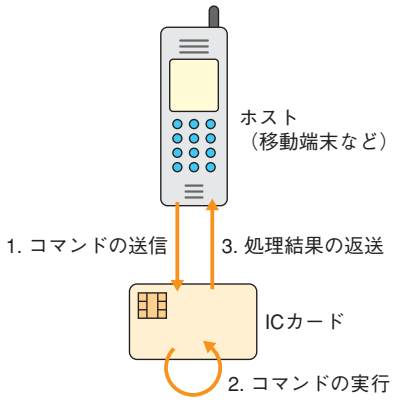

図2　ISO7816-4を用いたICカード処理の流れ

4. 技術の概要

前章で示した課題を解決し，設計目標③，④を達成するためには，APによる中継を必要とせずにICカード間で自律的にメッセージのやり取りを可能とする方式が必要となる．そこで，著者らは従来のICカードインタフェースとは異なり，移動端末上のAPと他の移動端末上のICカード間，およびICカード相互間などで直接通信を行えるようにする技術[9][10]を開発し，TENeT仕様では本技術に基づくアーキテクチャを採用した．

これにより，電子価値の送受プロトコルなどによるICカード間でのメッセージの送受はAPを介在せずに行われる．そのため，それらの内容や手順を具体的に意識することなくAPを構築することが可能となる（**図4**）．

以下，TENeTのアーキテクチャを**図5**に示すとともに，TENeTにおけるメッセージ構成，メッセージの配送方式，電子価値取引ライブラリ[*7]についてそれぞれ概略を示す．

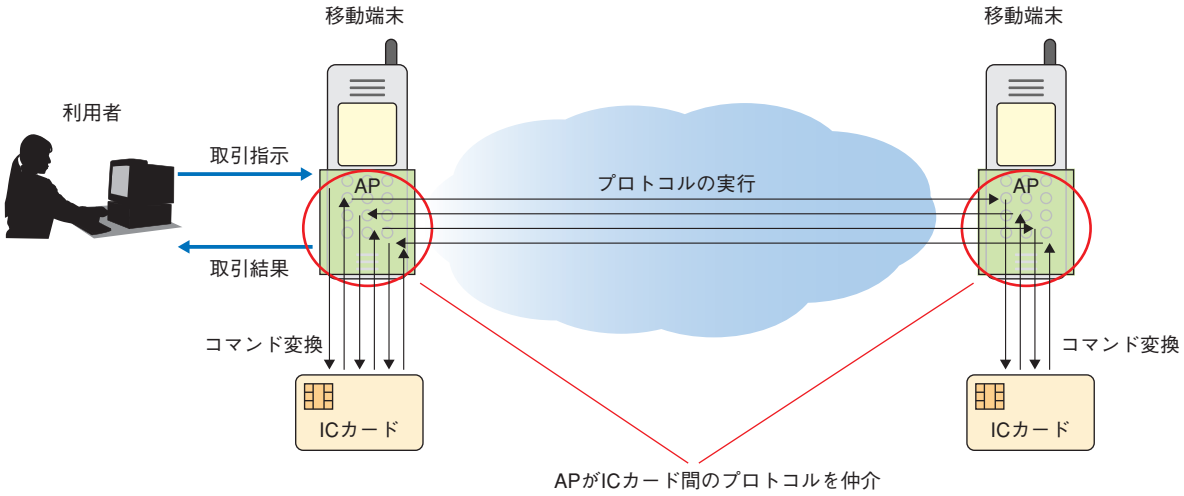

図3　従来のICカード通信アーキテクチャによるICカード間プロトコルの実行

＊7　ライブラリ：汎用性の高い複数のプログラムを，再利用可能な形でひとまとまりにしたもの．

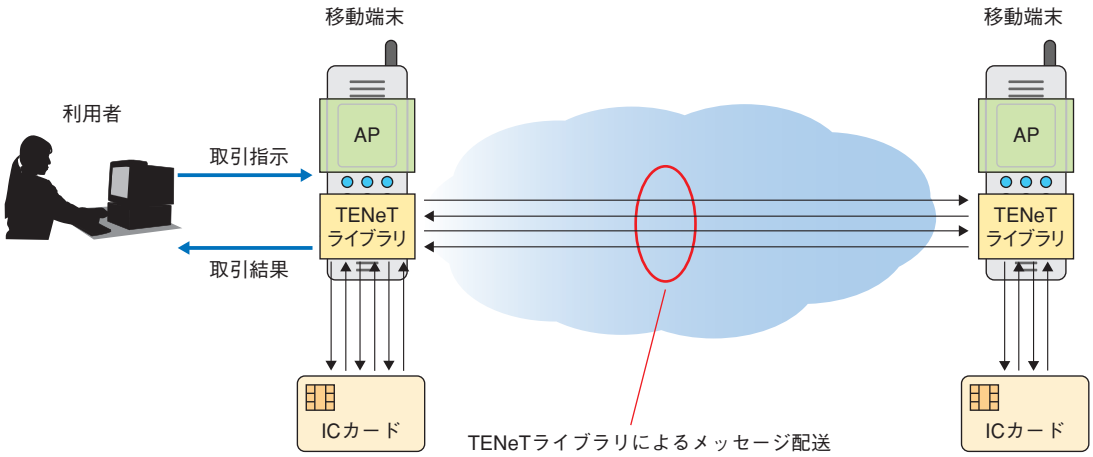

図4　TENeTによるICカード間プロトコルの実行

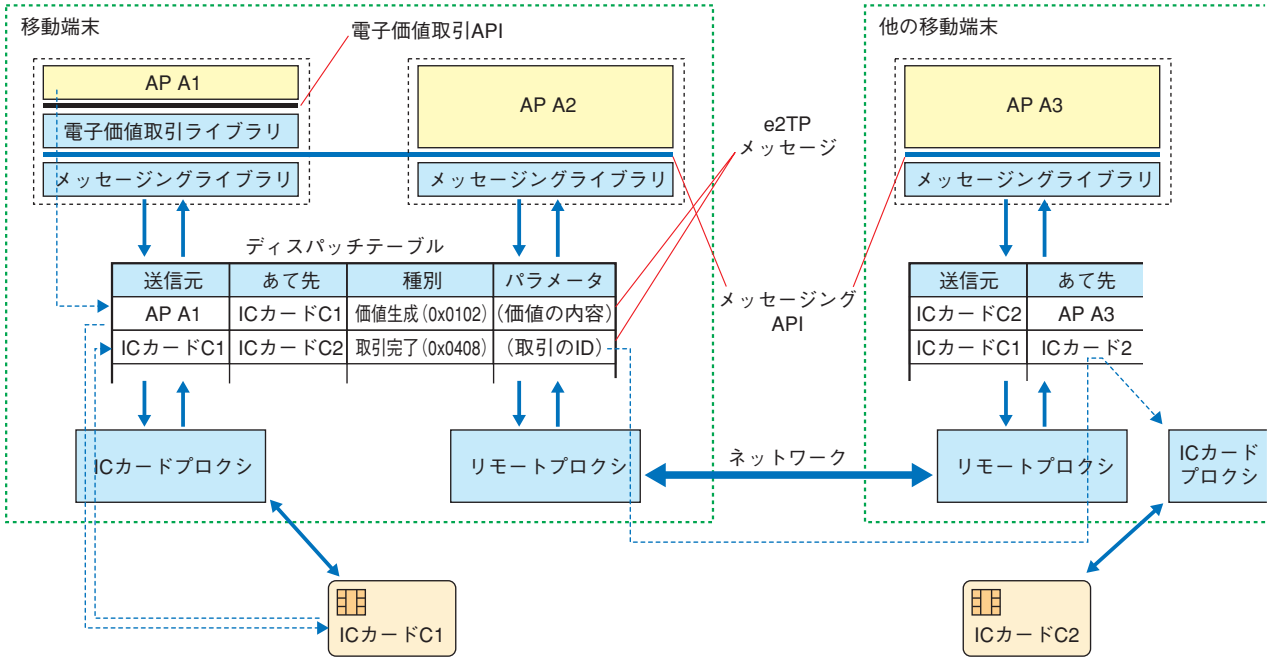

図5　TENeTのアーキテクチャ

4.1 メッセージ構成

TENeT仕様において，APやICカード間でやり取りされるメッセージはe²TP（extended eTRON Protocol）メッセージと呼ばれ，「送信元ID」，「あて先ID」，「種別」，「パラメータ」の4要素からなるデータにより構成される．ここで，「送信元ID」はメッセージを送信したAPもしくはICカードの識別子，「あて先ID」はメッセージのあて先となるAPもしくはICカードの識別子，「種別」は「電子価値の生成」「電子価値の交換開始」などのメッセージの種別ごとに定められたメッセージ種別コード，「パラメータ」はメッセージの内容を示す情報（「電子価値の生成」の場合，生成する電子価値の内容）である．

例えば，識別子A1を持つAPから識別子C1を持つICカードに対して，電子価値の生成を指示するメッセージは，(A1, C1, 0x0102,＜生成する電子価値の内容＞）となる．ここで，0x0102は電子価値の生成指示を表すメッセージ種別

コードの16進表記である．

前述のe²TPメッセージの構成の詳細は「e²TPメッセージ仕様」[3]に，メッセージの種別コードとメッセージ種別ごとのパラメータは「TENeTメッセージ仕様」[5]においてそれぞれ定義されている．

4.2 メッセージの配送方式

TENeTにおいてAPからのメッセージの送信は，メッセージングライブラリと呼ばれるメッセージ配送のためのライブラリを介し，ディスパッチテーブルと呼ばれる共有メモリに対してメッセージの書込みを行うことにより行われる．また，ICカードから送信されたメッセージはICカードプロクシと呼ばれるプログラムモジュール，他の移動端末から送信されたメッセージはリモートプロクシと呼ばれるプログラムモジュールにより，それぞれディスパッチテーブルに書き込まれる（図5）．

APは，メッセージングライブラリに対し自分あてのメッセージの到着を知らせるためのハンドラ[*8]を登録することによりメッセージの受信を行う．このハンドラは，そのAPあてのメッセージがディスパッチテーブルに書き込まれると呼び出され，メッセージの到着を通知する．

ICカードプロクシおよびリモートプロクシも同様のハンドラを備え，それぞれICカードあてのメッセージもしくは他の移動端末あてのメッセージが登録されたときに呼び出される．ICカードプロクシはハンドラにより取得したメッセージをそのままICカードに送信し，リモートプロクシはネットワークを介して他の移動端末のリモートプロクシに送信する．

このように，それぞれのメッセージはAPの介在なしに自律的に配送されるため，電子価値取引など，ICカード間での分散通信が必要なAPの負担は大幅に軽減される．また，前述したメッセージングライブラリあるいは各プロクシの動作はAPやICカードの介在なしに行われる．そのため，APやICカードプログラムの開発者はこれらのメッセージ配送機構を意識することなく，他の移動端末上のものを含めて他のAPやICカードとの間でメッセージをやり取りすることができる．

このメッセージ配送機構を利用するためにAPに対して提供される機能およびインタフェースの詳細は，「e²TPメッセージングAPI（Application Program Interface）[*9]仕様」[6]に定義されている．

4.3 電子価値取引ライブラリ

前節で示したメッセージ配送機構により，APはICカード間で実行されるプロトコルの詳細について意識する必要がなくなるため，AP構築の負担は大幅に軽減される．しかし，メッセージングライブラリを直接利用してAPを構築するためには，APがe²TPメッセージを作成・解釈しなくてはならない．また，通信の途絶によるプロトコルの中断などの異常に対してきめ細かい対処が必要な場合，ICカード間のプロトコルの実行状態を監視する機能が要求される．

前述のような要求に対して，e²TPメッセージの作成・解釈を自動化し，さらに必要に応じてプロトコルの実行状態をAPから監視可能とするために，TENeTでは電子価値取引ライブラリと呼ばれるライブラリを提供している．このライブラリは，メッセージングライブラリの上位レイヤに位置し，ICカード内の電子価値，電子価値を取引する際の取引相手や取引の遂行状態などをそれぞれオブジェクト[*10]として提供する．また，電子価値の生成や取引の開始，取引状態の確認などの機能は，それらのオブジェクトの中の機能として実現される．

このライブラリは，TENeT仕様のICカードが提供する電子価値取引機能の主要部分を網羅しており，電子財布などの電子価値を扱う一般的なAPは，本ライブラリが提供する機能のみを用いて構築することができる．すなわち，これらのAPの開発者は本ライブラリが提供するAPI以外の各種仕様を意識する必要はない．

本ライブラリが提供する機能およびインタフェースの詳細は「電子価値取引API仕様」[7]に定義されている．

5. 試作評価について

TENeT仕様群の策定に際し，ICカードおよび各ライブラリの実証試作とその評価を通じて実現の可能性および性能についての確認を併せて行った．

ICカード部分の試作は，数年後のミドルレンジICカードを想定して，現状では比較的高性能な市販ICカード（32bit CPU，clock：66MHz，EEPROM：400KB，RAM：16KB）を用いて実装を行った．取引の開始から終了までの処理時

＊8 ハンドラ：イベントの発生により起動される処理ルーチン（プログラム）．例えばメッセージの発生により起動される処理ルーチンはメッセージハンドラ，外部割込みの発生により起動される処理ルーチンは割込みハンドラなどと呼ばれる．

＊9 API：OSやミドルウェアなどが提供する機能を，上位のソフトウェアが利用するためのインタフェース．

＊10 オブジェクト：現実世界に実体や概念として存在するものをプログラム上で扱えるように表現したもの．表現対象となる実体の属性を表すデータと，実体に対する操作の組合せとして表現される．

間は，本実装では約1秒であった．これにより本仕様が，現在市販されているICカードを用いて十分な性能で実装可能であることが確認できた．

ライブラリの試作は，移動端末への実装を想定してJ2ME™（Java2 Micro Edition）[*11]（MIDP（Mobile Information Device Profile）[*12]2.0）シミュレータであるJava Wireless Toolkit 2.2上で行った．ライブラリはシミュレータ上のJ2ME環境にJAR（Java ARchive）[*13]ファイルとして追加し，動作確認用の取引APはMIDlet[*14]として実装した．実装の結果，電子価値取引ライブラリを除いたメッセージ通信機構（メッセージングライブラリ，各種プロクシ）のサイズは45KB，電子価値取引ライブラリのサイズは99KBであった（いずれもJARファイルのサイズ）．これは，近年の移動端末への実装に障害とならないサイズであると考えられる．また，本シミュレーション環境では，メッセージの配送によるオーバヘッドは1メッセージ当り10ms未満であり，ほぼ無視できるものであった．

6. あとがき

本稿では，移動端末を用いた安全な電子価値取引市場を実現するための仕様であるTENeT仕様について紹介し，その実現技術の1つであるICカード通信技術についての設計目標と概要を説明した．また，本仕様は実際の市販ICカードとJ2MEシミュレータ環境においてそれぞれ試作実装を行い，実現可能性および性能を評価した．

本仕様の策定にあたっては，標準仕様としての汎用性を提供するとともにAP開発者にとっての「使い勝手の良さ」を提供することを重視し，1編の大きな仕様ではなく仕様の利用目的と利用対象者の2つの観点から分割した4つの仕様群として構成した．

今後は，実機環境での評価や安全性検証などを通じて本仕様に基づく実装の精査と仕様改善を進めるとともに，本技術を適用した新たなサービスの可能性について継続的に検討を進めていく予定である．

文　献

[1] M. Terada, M. Iguchi, M. Hanadate and K. Fujimura: “An Optimistic Protocol for Trading Electronic Rights,” Proc. 6th intl. conf. Smart Card Research and Advanced Applications (CARDIS’04), 2004.

[2] 寺田，ほか：“移動端末間の電子価値流通技術,” 本誌，Vol. 13，No. 3，pp. 11-15，Oct. 2005.

[3] T-Engine Forum; http://www.t-engine.org/

[4] T-Engine Forum: “e²TPメッセージ仕様,” 2006.

[5] T-Engine Forum: “TENeTメッセージ仕様,” 2006.

[6] T-Engine Forum: “e²TPメッセージングAPI仕様,” 2006.

[7] T-Engine Forum: “電子価値取引API仕様,” 2006.

[8] ISO/IEC: “Integrated circuit(s) cards with contacts-Part 4: Interindustry commands for interchange,” ISO/IEC 7816-4:1995(E), 1995.

[9] M. Terada, K. Mori, K. Ishii, S. Hongo, T. Usaka, N. Koshizuka and K. Sakamura: “TENeT: A Framework for Distributed Smartcard,” Proc. 2nd intl. conf. Security in Pervasive Computing (SPC2005), LNCS 3450, 2005.

[10] M. Terada, K. Mori, K. Ishii, S. Hongo, T. Usaka, N. Koshizuka and K. Sakamura: “A Framework for Distributed Inter-smartcard Communication,” IPSJ Journal, Vol. 47, No. 2, Feb. 2006.

＊11 J2ME™：Java言語の機能セットの1つで，組込み機器向けに消費リソースを少なく抑えたもの．
J2MEおよびすべてのJava関連の商標およびロゴは，米国およびその他の国における米国Sun Microsystems, Inc. の商標または登録商標．

＊12 MIDP：J2ME用のプロファイルの1つで，移動端末などの携帯端末向けに定義されたJava実行環境の仕様．

＊13 JAR：Javaソースコードをコンパイルすることにより生成される複数のJavaバイトコードを1つにまとめたファイル形式．

＊14 MIDlet：ネットワークを通じてダウンロード実行可能な，MIDP環境で動作するJavaプログラムの形式の1つ．