マルチメディア情報処理特集

eTRONを搭載した携帯端末による電子価値／権利流通方式の研究

近年，携帯端末を利用したモバイルEコマースの機運が高まりつつあるが，充分な安全性とシステム運用の低廉なコストを両立しつつ広範な用途に適用可能な方式は，まだ確立されてはいない．

本稿では，これらの要件を満足するモバイルEコマース環境の実現を目指し，相互認証機能と暗号化通信機能を備えた耐タンパーICチップであるeTRONチップを利用した，新しい電子価値／権利流通方式の設計／実装ならびに実現性の評価について報告する．

石井 一彦　寺田 雅之
森 謙作　本郷 節之

New Technology Reports

1. まえがき

近年，携帯電話を介したモバイルEコマースは，有料情報の入手や着信メロディのダウンロードといったサイバー世界での利用の枠を超え，電子マネー・電子チケットの利用のような，リアル世界と連動して利用できるサービスへと広がりつつある．例えば電子チケットぴあ[*1]では携帯電話に電子チケットをダウンロードし，赤外線通信機能を用いて会場の改札ゲートを通ることが可能である．また，電子マネーサービスのシステムFeliCa[*2]を搭載した携帯電話も実現しつつあり，携帯電話で電子マネーをチャージして支払いをする，携帯電話をかざして鉄道の改札を通る，といった行為が可能になりつつある．このように，チケット・通貨・切符などの電子価値／権利情報を，携帯電話に格納して利用できる世界は，今まさに現実のものとなりつつある．

しかし，これらのモバイルEコマースサービスは従来の紙のチケットや通貨と違い，ユーザの間でチケットや電子マネーを自由に受渡しすることはできない．電子チケットぴあでは携帯電話と改札機は赤外線通信機能により改札を

＊1　電子チケットぴあ：http://t.pia.co.jp/
＊2　FeliCa：FeliCa®はソニー株式会社の登録商標です．

行うものの，携帯電話間で赤外線通信機能を使ってチケットの受渡しをする機能は実現されていない．現在の方式では，ユーザ間でチケットの受渡しをしたい場合，必ず専用のサーバに電子チケットをいったん戻し，サーバを介してチケットを受渡しする必要がある．またFeliCaも同様に，電子マネーを他のユーザと受渡しする実装は全く考慮されていない．

FeliCaを例に取ると，ユーザ間での自由な電子価値／権利の流通が行えないのは，それを安全に実現することが困難であることが大きな要因と考えられる．現行方式において電子価値／権利をユーザの携帯電話とやりとりをすることができるのは，専用のサーバや改札機などの信頼できる機器に限られている．これら信頼できる機器がユーザ端末の正当性を認証することにより，不正な端末を使って電子価値／権利がコピーされたり改ざんされたりすることを防ぐとともに，仮に途中で通信が途切れたとしても電子価値／権利が複製されたり逆に消滅したりしないことを保証している．

しかし，ユーザ同士のやりとりでは双方の携帯端末が必ずしも信頼できるものとは限らない．このような状況のもとで，従来の紙のチケットや通貨のように電子価値／権利の自由な流通を可能とするには，電子価値／権利を，複製や改ざんから守りつつ，かつ安全にやりとりできる仕組みが必要となってくる．

そこで著者らは，自由で安全な電子価値／権利流通の実現を目指し，相互認証機能と暗号化通信機能を備えた耐タンパーICチップであるeTRON（entity and economy TRON）[1]チップを用いたモバイル向け電子価値流通プラットフォーム（STeP：Securely Transferable entity Platform for eTRON）[3]を開発した．本稿ではeTRONアーキテクチャの概略と，それを用いたモバイル向け電子価値流通プラットフォームの設計方針，具体的システムの構築，ならびに実現性の評価について述べる．

2. eTRON

従来のEコマースシステムでは，保存された電子価値／権利情報に対する耐タンパー性が十分とはいえなかった．近年，ICカードを用いて対タンパー性を向上させた方式が普及しつつあり，共通鍵を利用して高速な認証（touch and go）を実現している．しかし共通鍵の性質上，鍵が漏洩した際のシステム全体への多大な被害と，1台1台別々の鍵を使用することによる鍵管理にかかる膨大なコストとのトレードオフという問題が存在している．これに対し，eTRONアーキテクチャ[2]では公開鍵を使った相互認証と暗号通信機能を備えたICチップを使用する．このため共通鍵方式に比べ速度は劣るものの，鍵漏洩時の被害を最小限に抑えると同時に鍵管理のコストも極めて小さくてすむという特長を有している．

図1にeTRONアーキテクチャの概略を示す．eTRONアーキテクチャでは耐タンパー装置であるICチップのコンテンツホルダ，それを操作するサービスクライアントから構成される．コンテンツホルダはeTRON IDというユニークなIDを持ち，安全に電子価値／権利を格納する．コンテンツホルダ同士はeTRON IDを用いた相互認証と暗号化通信を行う．このようなセキュア通信をeTP（entity Transfer Protocol）と呼ぶ．サービスクライアントはコンテンツホルダ内の電子価値／権利の操作や，eTPによるセキュア通信の中継をする装置である．

3. モバイル向け電子価値流通プラットフォームSTeP

著者らはeTRONアーキテクチャをモバイル環境に応用し，電子価値／権利流通を可能にするプラットフォームSTePを開発した．本章では，想定サービスを説明し，次に，それを実現するためのシステム要件を述べ，その上で，それを満たすシステムの設計を記す．

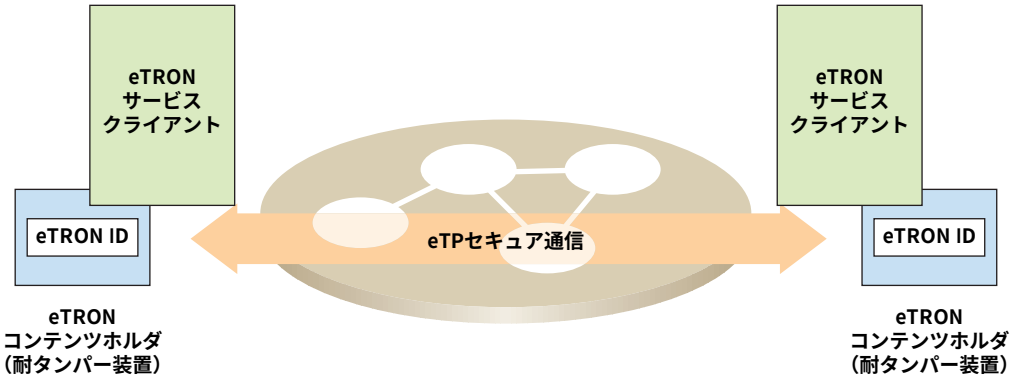

図1　eTRONアーキテクチャの概略

3.1 STePの想定サービス

電子価値／権利流通サービスには以下の2つの場合が考えられる．

(1) 電子価値／権利がそのままの形で流通／消費されるサービス

(2) 電子価値／権利が分割して流通／消費されるサービス

ここでは(1)の例として電子チケット販売サービス，(2)の例として電子ブック課金サービスを想定する．

(1) 電子チケット販売

STePの想定サービスとしての電子チケットの販売システムを示す．本システムは電子チケットの購入，ユーザ間でのチケットの自由なやりとり，イベント会場での改札までの一連の流れを，すべてSTeP携帯端末を使って行うことができる．

全体の概要を図2に示し，これに沿ってチケットの購入から利用までの流れを説明する．

ユーザはSTeP携帯端末を使って，販売サーバのwebサイトから購入したい電子チケットを選び購入手続きを行う．電子チケットは自由にやりとりできるので，友人などの分も含め複数枚を購入することができる（図2①）．

販売サーバはSTeP発行サーバに電子価値の発行を依頼する（図2②）．

発行サーバはSTeP携帯端末と通信を行い，電子チケットを発行する．この時，発行サーバと実際に通信を行うのはSTeP携帯端末内にあるSTePチップである．STePチップと発行サーバは相互認証を行い，お互いが正しいことを確認した後，暗号化通信により電子チケットの発行を行う．暗号化はSTePチップと発行サーバの間で行われるのでネットワークやSTeP携帯端末を盗聴しても不正を行うことはできない（図2③）．

ユーザは友人などが持つ，他の端末へ電子チケットの受渡しを行う．その際，例えば非接触インタフェースを使ったオフライン通信で電子チケットを送ることができる．この時も通信を行うのはお互いが持つSTePチップであるため，相互認証と暗号化通信をチップ同士が行うことにより利用者は不正ができない．また，受渡し中に，途中で通信が途切れても電子チケットが消失したり複製ができてしまったりすることはない（図2④）．

電子チケットを持ったユーザはSTeP携帯端末を持ってイベント会場に行く（図2⑤）．

イベント会場では改札ゲートにSTeP携帯端末をかざす．このときも改札ゲートと端末内のSTePチップの間で相互認証が行われる．改札ゲートは正しい電子チケットを見つけたらチケットを改札してゲートを開ける．1度使った電子チケットは回収されるか，改札マークが入れられて2度と利用することはできなくなる（図2⑥）．

(2) 電子ブック課金

STePの想定するサービスの2つめとして，電子ブックの課金システムを示す．本システムは電子ブックを暗号化して自由に配布し，それとは別に電子価値として電子ブックカードを販売することで課金を行う．電子ブックカードの中にはプリペイドカードのような度数情報と電子ブックを復号する鍵およびプログラムが入っている．これにより，ページ単位で電子ブックを復号して読み，課金することができる．

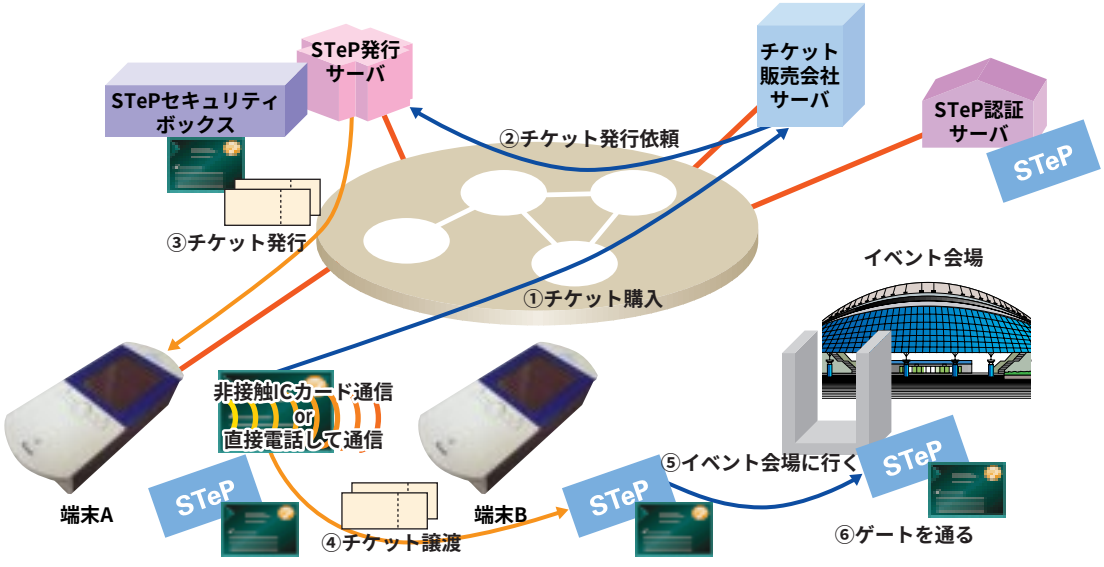

図2　電子チケット販売

全体の概要を図3に示し，これに沿って電子ブックカードの購入からブックの閲覧までの流れを説明する．

電子ブックサーバは電子ブックを暗号化して用意しておく．ユーザが電子ブックカードを購入しようとすると，電子ブックサーバは発行サーバに，暗号化した電子ブックを復号できる鍵とユーザが購入した度数情報を送り，電子ブックカードの発行を依頼する（図3①）．

発行サーバはユーザのSTeP携帯端末に電子ブックカードを発行する．電子ブックカードには，ユーザが購入した度数情報と電子ブックを復号するための鍵が入っている．発行サーバとSTePチップは相互認証と暗号化通信を行っているため，ユーザがSTeP携帯端末やネットワーク上で盗聴しても復号する鍵が漏れることはない（図3②）．

ユーザは暗号化された電子ブックを自由にダウンロードできる．電子ブックを復号するには電子ブックカードの中にある鍵が必要だが，電子ブックカードは所有者にも読めないようにACL（Access Control List）が設定されているため，STePチップ内の鍵情報をユーザが盗みだすことはできない（図3③）．

ユーザがSTeP携帯端末の電子ブックリーダを使って電子ブックを読む．このとき，端末に表示できる1ページ分だけが取り出されてSTePチップに送られる（図3④）．

STePチップの中では送られてきた電子ブックをSTePチップ内の復号プログラムで復号しようとする．復号する前にプログラムは電子ブックカードの度数情報を減らす（図3⑤）．

度数はページごとや文字ごとなど，決められた単位で減算することができる．例えば，1文字ごとなどの細かい単位で減らすことも可能である（図3⑥）．

度数を減らすことができたら，復号プログラムは電子ブックカードの中の鍵を使って電子ブックを復号して出力する．この度数の減算から復号までの処理はSTePチップの中で行われるため，ユーザは度数を減らさずに復号するなどの不正を行うことはできない（図3⑦）．

上記の処理を経て，復号された1ページが端末に表示される（図3⑧）．

3.2 STePのシステム要件

従来のeTRONチップは非接触の近接通信のみで他のeTRONチップと電子価値／権利の送受信を行う単機能なものであるため携帯端末に搭載して柔軟な電子価値／権利流通を行おうとした場合，以下のような問題がある．

(1) パッシブ型の非接触ICカードインタフェースしか持っておらず，ICカードリーダ／ライタを介さない場合，他のeTRONカードと電子価値／権利情報を授受できない．

(2) moperaを含むインターネット経由で電子価値／権利流通を行う際，eTRON IDのみでは通信先（eTPセッションを張りに行く相手）のIP（Internet Protocol）アドレスが分からず，電子価値／権利流通が行えない．

(3) 電子価値／権利情報へのアクセスコントロール機能が無いため，アクセスレベルの異なる複数の電子価値／権利情報を混在させられない．

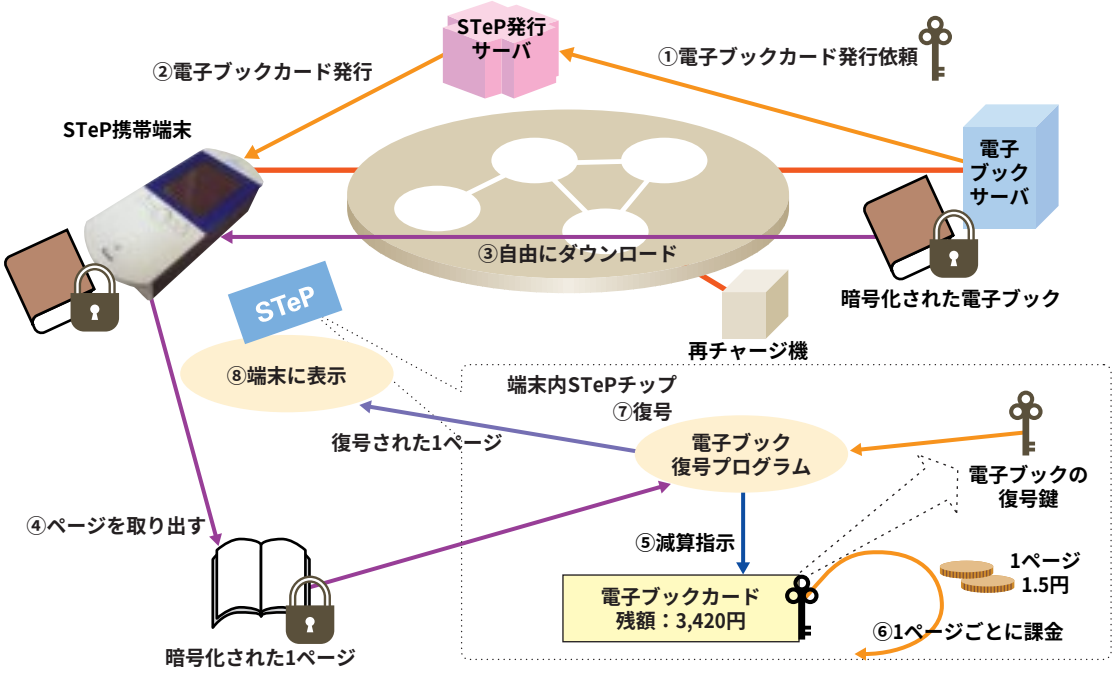

図3　電子ブック課金

3.3 STePの設計方針

前節で述べたシステム要件を満たすために，以下の方針に従ってシステムを設計する．

(1) STePチップ自体は接触型ICカードインタフェースを備えることとし，携帯端末との通信はこの接触インタフェースで行う．携帯端末側には非接触型ICカードリーダ／ライタを備え，非接触カードとして使用する場合にはこれを利用して通信を行う．

(2) インターネット内にアドレス解決サーバ（ARS：Address Resolution Server）を配備し，インターネットでeTPセッションを張る場合にはこのサーバを参照してIPアドレスを取得する．これに加え，携帯端末内にもeTRON IDとIPアドレスの対応情報のキャッシュ（ルーティングキャッシュ）を設けて過去にARSから取得した情報を蓄積することで，通信確立までの時間短縮とARSの負荷軽減を同時に達成する．

(3) 電子価値／権利データ仕様にACL領域を加えることにより，ICカード所有者が自分の所有する電子価値／権利情報へアクセスできる権限を柔軟に制御することを可能にする．

3.4 STePのシステム設計

前節の設計方針を基に，eTRONを応用し，図4のようなモバイル向け電子価値／権利流通システムを設計した．図中の構成要素は以下のとおりである．

(1) STePチップ

STePチップは接触型インタフェースを持つUIM（User Identity Module）と同サイズのカードであり，後で説明するSTeP携帯端末に挿入してユーザ同士での自由な電子価値の交換を可能とする．

今回開発したSTePチップを写真1に示す．

(2) STeP携帯端末

STeP携帯端末はT-Engine[*3]をベースにしてタッチパネル付の大画面液晶ディスプレイやボタンスイッチなどに併せ，以下の機能を持っている．

今回開発したSTeP携帯端末を写真2に示す．

①電子価値取扱機能

本機能はSTePチップ内の電子価値の操作に用いる．ユーザは本機能を通じて購入した電子価値を格納したり，チップ内の電子価値を閲覧したり，他のSTeP携帯端末と電子価値をやりとりすることができる．

②移動通信機能

本機能はSTeP携帯端末のPCカードスロットにPHS（Personal Handy-phone System）カードやFOMA（Freedom Of Mobile multimedia Access）カードなどの移動通信カードを挿してのデータ通信に用いる．ユーザは本機能によりサーバから電子チケットを購入したり，インターネットと接続したりすることができる．

＊3 http://www.t-engine.org/

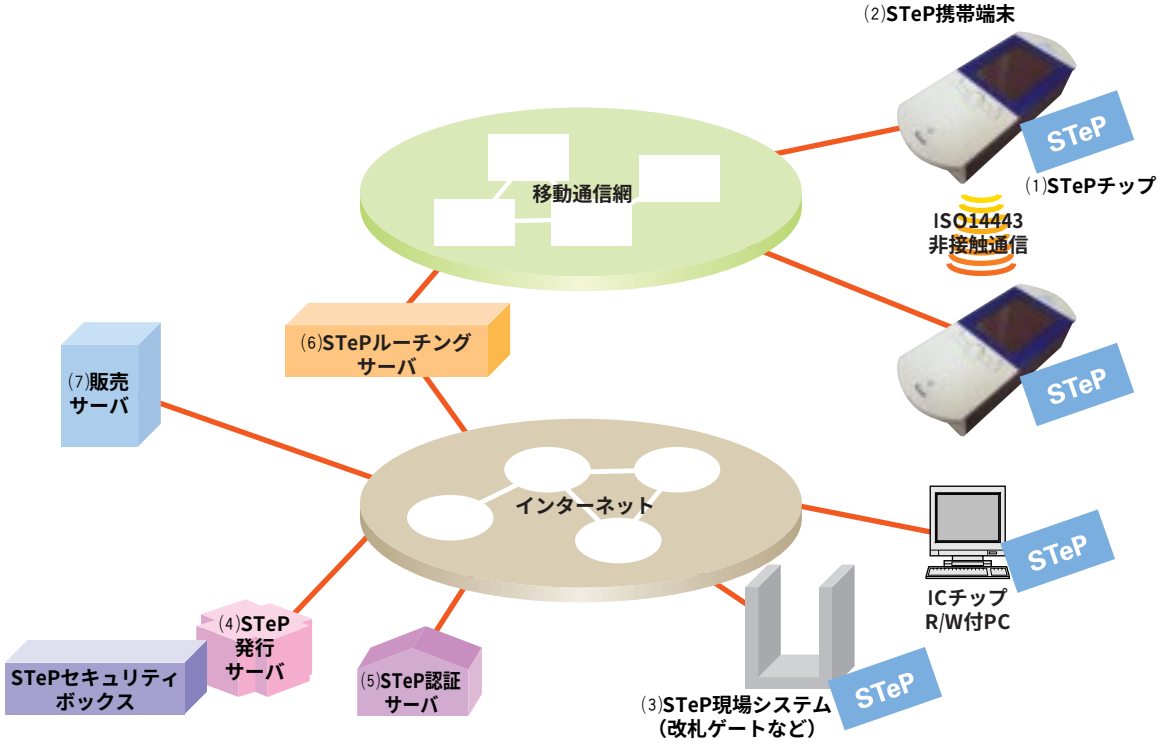

図4 STeP構成

写真1　STePチップ

写真2　STeP携帯端末

③非接触通信インタフェース

STeP携帯端末は背面にIEEE（Institute of Electrical and Electronics Engineers）の規約による，IEEE14443の非接触ICカードインタフェースを持つ．これを使ってSTeP携帯電話同士を近づけることにより電子価値のやりとりが行える．また改札ゲートを通過する時もかざすだけで利用できる．

(3) STeP現場システム

STeP現場システムは改札ゲートや店舗レジスタなど，電子価値を利用する現場に置かれるシステムである．現場システムはeTRONサービスクライアントの一種であり，STeP携帯端末と通信して電子価値の回収や発行を行う．

(4) STeP発行サーバ

STeP発行サーバは後で説明する販売サーバからの依頼を受け電子価値を発行するeTRONサービスクライアントである．発行サーバは大量の電子価値を取り扱うために，eTRONコンテンツホルダとして小型の耐タンパーセキュリティボックスを持つ．

(5) STeP認証サーバ

STeP認証サーバは各eTRON IDの正当性を保証し，公開鍵証明書を発行するサーバである．STePチップ内には，eTRON IDとSTeP認証サーバが発行した公開鍵証明書および秘密鍵が格納されている．STePチップは通信のときに公開鍵証明書と署名を用いて相互認証を行い，相手の正当性を確認する．

(6) STePルーチングサーバ

STePルーチングサーバはeTRON IDによるルーチング機構を実現するためのサーバである．STePチップがネットワークに接続されるとIPアドレスや電話番号などの情報がルーチングサーバに登録される．STePチップ同士がネットワークを使って通信する際にはルーチングサーバに相手のeTRON IDを問い合わせ，得られたIPアドレスや電話番号を使って通信を行う．

(7) 販売サーバ

販売サーバは一般的なwebサーバとほぼ同じ機能を持つ．STeP携帯端末が販売サーバから電子チケットなどの電子価値を購入すると，販売サーバはSTeP発行サーバに電子価値の発行を依頼し，実際の電子価値の発行は発行サーバを通して行われる．これにより，通信販売などを行っている一般のwebサーバに対する変更を最小限に抑えたまま，STePを利用して安全に電子価値の発行を行うことが可能になる．

4. STePの評価

前章で述べたシステムで想定サービスを実現する実験環境を構築し，STePの実現性について以下のように評価した．

(1) 評価：その1

STePチップを接触型として携帯端末と組み合わせることにより，チップを携帯端末に内蔵しつつ，非接触型通信も可能となった．図5に示すとおり，従来は非接触通信のみで，それ以外の通信方式を利用するには非接触カードリーダ／ライタを経由するしかなかったが，本方式は非接触通信以外にも携帯端末を通して移動通信網，インターネットなどの直接利用が可能となった．

(2) 評価：その2

ARSの配備によりインターネットを利用したeTP通信においても，eTRON IDからIPアドレスを検索し接続することが可能となった．従来方式ではeTRON IDから接続する相手が検索できないため，相手のeTRONチップと接続することは不可能であるが，ARSに問い合わせることによりネットワークに依らず相手のSTePチップと接続することが可能となった．図6にその画面を示す．図6(a)は電子チケットを携帯端末に転送している場面である．ARSがない場合は図6(b)のように，転送先がみつ

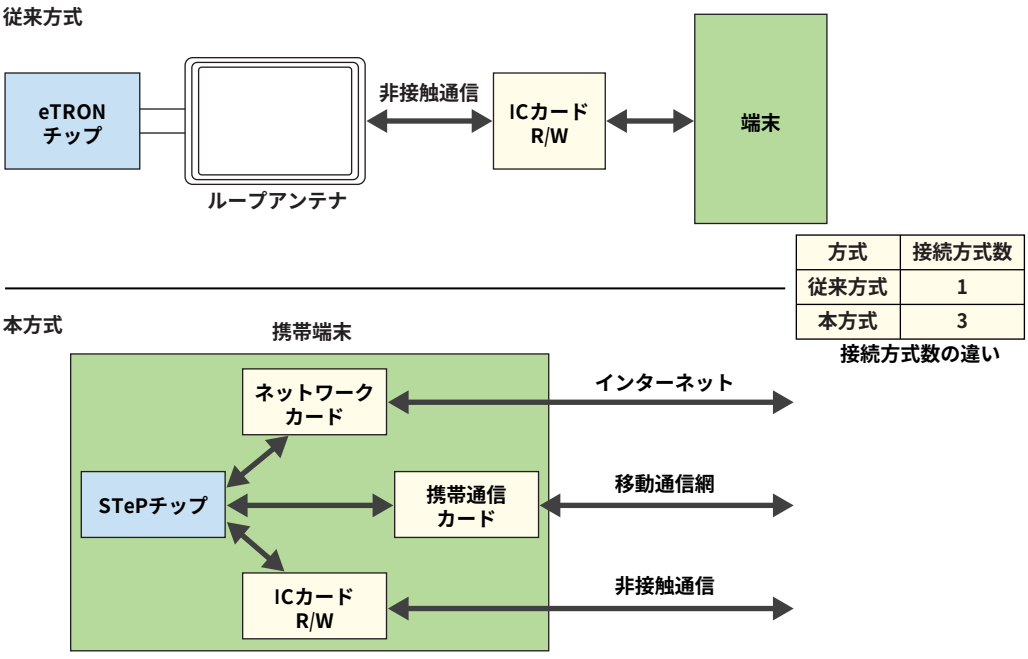

図5　利用可能通信方式の拡大

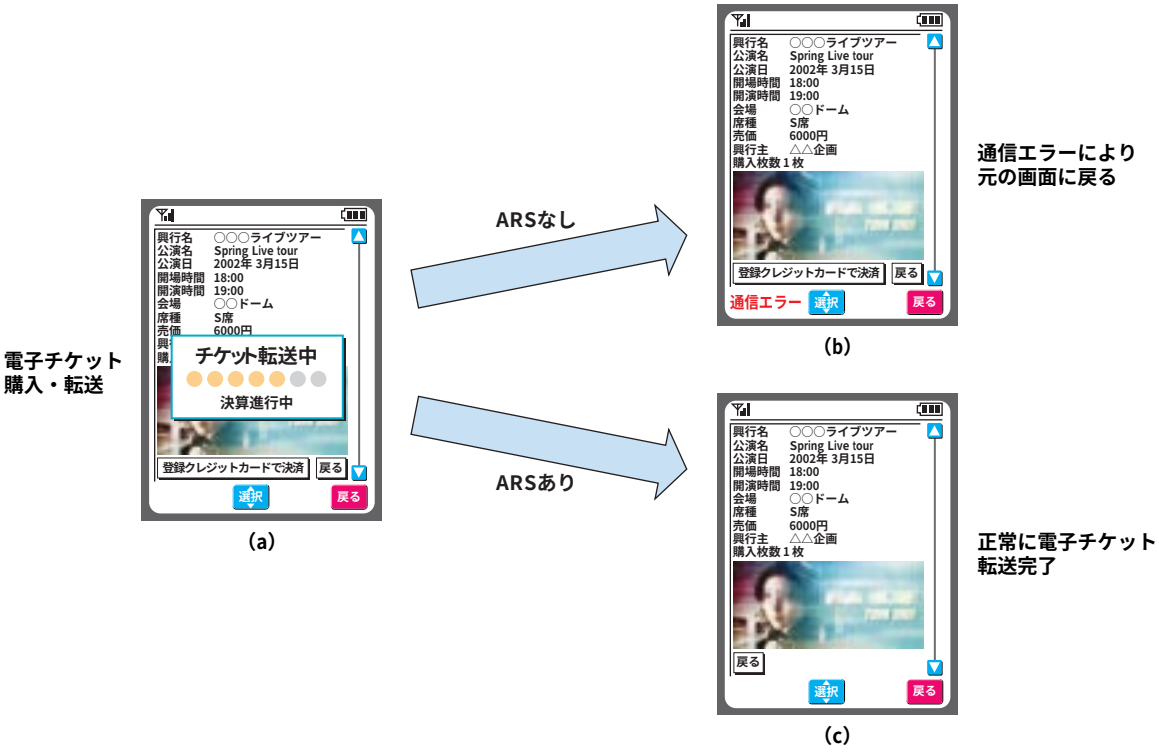

図6　ARSによる接続先検索

からず通信エラーとなるが，ARSがある場合には図6(c)のように正常に完了する．

(3) 評価：その3

ACLの設定により，所有者が自分の電子価値／権利に対する他者からのアクセス権限を制御できることが可能になった．従来はアクセス権の制御がICカード側に存在しないため，電子価値／権利を不正アクセスから保護するには，アプリケーションがカード内の電子価値に対するアクセスが適切であるかを電子価値ごとにすべて監視する必要があり，カードの入替えや電子価値の増減により不整合が起きる恐れがあったが，本システムではSTePチップのACLにより，不整合なく個々の電子価値ごとに

柔軟なアクセス制御が可能である（図7）．図7(a)に示すとおり，アクセス権の異なる電子ブックカードと電子チケットとを1つのSTePチップの中に混在させ得ることが確認できた．電子ブックカードは所有者以外からはアクセス不可能であり，電子チケットは所有者のほかに改札ゲートからアクセス可能となっている．

また，eTRONの機能を利用して携帯端末環境でユーザ同士が電子価値／権利を流通でき，その際にコピー／改ざんができず，通信途中の切断でも複製や消失が起きないことも確認できた．

5. 考察

(1) STePではSTePチップ同士が直接相互認証や暗号化通信を行っているが，ICカードのCPU（Central Processing Unit）はパソコンのCPUと比較しても計算能力は1/10～1/100と低く，認証や暗号計算を行うのに時間がかかる．このため，相互認証には平均1,200msを要し，現在主流となっている共通鍵ICカードの認証時間の約6倍の時間を要している．今後は，高速な暗号アルゴリズムを搭載して処理速度の向上を目指す．

(2) STePチップの基となるeTRONアーキテクチャは，セキュリティ分散アーキテクチャとして広い応用を可能とするために，シンプルで必要最小限の機能しか持っていない．そのため，モバイル環境に応用した場合に必要な，チップ内の電子価値／権利を一覧する機能やアクセス権を簡単に変更する機能などが用意されておらず，代替法では多大な時間がかかったり，本来利用できるはずの機能が利用できない場面がある．今後は，eTRONアーキテクチャの応用性を保ちながら，モバイル環境に必要な機能の拡張を行う．

(3) STePチップでは電子価値のやりとりを一方から一方への受渡しとして実現しているが，現実の世界では価値と価値との交換により取引が成立していることがほとんどである．電子価値の交換を行う場合には，単純に受渡しを2回行うだけでは途中で通信が切れた場合に受渡しが片方しか行われず不公平が生じる恐れがあるため，今後は安全で公平な電子価値の交換が行える方式をSTePチップに実装する．

6. あとがき

本稿では，eTRONアーキテクチャを使ったモバイル向け電子価値／権利流通プラットフォームSTePについて解説した．STePを用いるとセキュリティを保ったままユーザ同士で自由な電子価値のやりとりを行うことができる．本研究では，eTRONをモバイル環境に応用する際の問題点を解決し，携帯端末ベースで柔軟な電子価値／権利流通を可能とする方式を設計するとともに，実際にシステム構築を行い，具体的な適用例でその実現性を示すことにより評価を

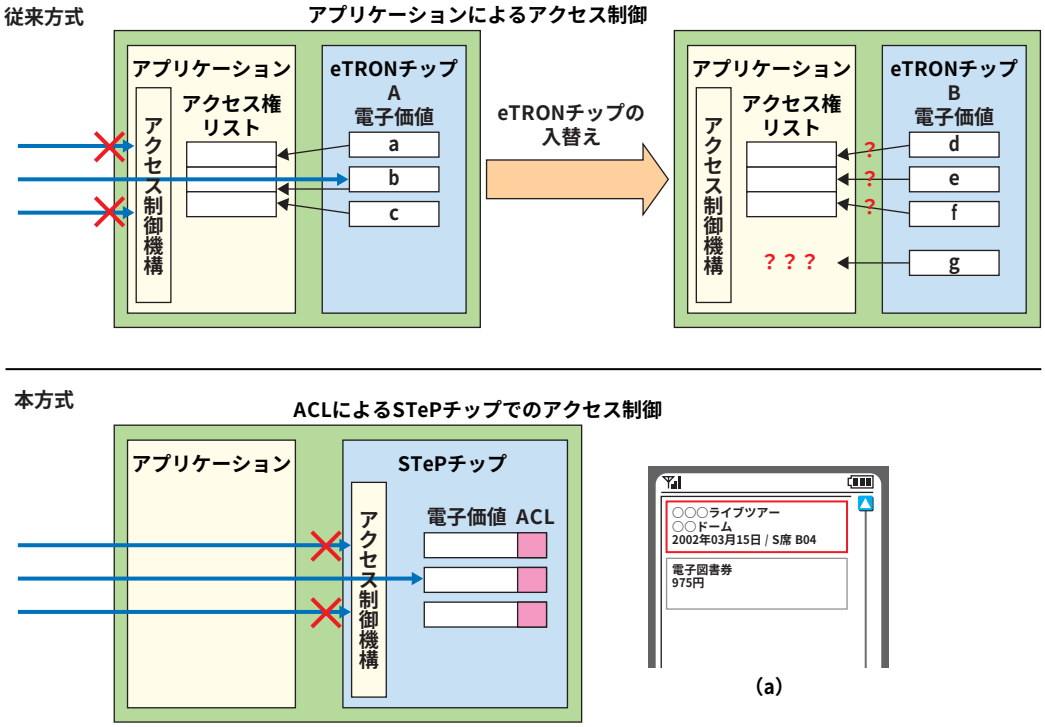

図7　アクセス権方式

行った．また考察で述べたような問題点も新たに抽出された．今後はこれらに対する改良を行うとともに，より安全で便利なモバイルEコマースサービスのプラットフォームとしてSTePを簡単に携帯電話で利用できるような環境の実現を目指していきたい．

文　献

[1] K.Sakamura and N.Koshizuka: “The eTRON Wide-Area Distributed-System Architecture for E-Commerce,” IEEE MICRO, pp.7-12, Vol.21, No.6, Dec.2001.
[2] 越塚 登，坂村 健，ほか：“eTRON: Entity and Economy TRON,” 情報処理学会研究報告，第19回CSEC研究会.
[3] 青野 博，ほか：“モバイル向け電子価値流通プラットホームの研究,” 情報処理学会研究報告，第19回CSEC研究会.

用 語 一 覧

ACL：Access Control List
ARS：Address Resolution Server（アドレス解決サーバ）
CPU：Central Processing Unit
eTP：entity Transfer Protocol
eTRON：entity and economy TRON
FOMA：Freedom Of Mobile multimedia Access
IEEE：Institute of Electrical and Electronics Engineers
IP：Internet Protocol
PHS：Personal Handy-phone System
STeP：Securely Transferable entity Platform for eTRON
（モバイル向け電子価値流通プラットフォーム）
UIM：User Identity Module