eTRONを搭載した携帯端末による電子価値・電子権利流通方式の研究

十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，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・電子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します．

石井 一彦 / 寺田 雅之
森 謙作 / 本郷 節之
NTTドコモ

自由な電子価値・電子権利流通の必要性

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っています．電子マネーサービスのシステムFeliCaを搭載した携帯電話が実現されつつあり，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ってきています．このようにチケット・通貨・切符などの電子価値・電子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ります．

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ません．

FeliCaを例に取ると，ユーザ間での自由な電子価値・電子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ます．現行方式において電子価値・電子権利をユーザの携帯電話とやり取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ます．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・電子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・電子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のです．

しかし，ユーザどうしのやり取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りません．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・電子権利の自由な流通を可能とするには，電子価値・電子権利を，複製や改ざんから守りつつ，かつ安全にやり取りできる仕組みが必要となってきます．

そこでNTTドコモでは，自由で安全な電子価値・電子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 The Real-time Operating system Nucleus）[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）[2]を開発しました．本稿ではeTRONアーキテクチャ[3]の概略と，STeP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ていきます．

eTRON

従来のeコマースシステムでは，保存された電子価値・電子権利情報に対する耐タンパー性が十分とはいえませんでした．近年，ICカードを用いて耐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）を実現しています．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台個別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ます．これに対し，eTRONアーキテクチャ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チップを使用します．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備えています．

図１　eTRONアーキテクチャの概略

図２　STeP携帯端末

図１にeTRONアーキテクチャの概略を示します．eTRONアーキテクチャ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ます．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・電子権利を格納します．コンテンツホルダどうしはeTRON IDを用いた相互認証と暗号化通信を行います．このようなセキュア通信をeTP（entity Transfer Protocol）と呼びます．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・電子権利の操作や，eTPによるセキュア通信の中継をする装置です．

STeP

我々はeTRONアーキテクチャをモバイル環境に応用し，電子価値・電子権利流通を可能にするプラットフォームSTePを開発しました．ここでは，想定されるサービスを説明し，次に，それを実現するためのシステム要件を述べ，そのうえで，それを満たすシステムの設計を示していきます．

■STePの想定サービス

電子価値・電子権利流通サービスには以下の２つの場合が考えられます．

①　電子価値・電子権利がそのままのかたちで流通・消費されるサービス

②　電子価値・電子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します．

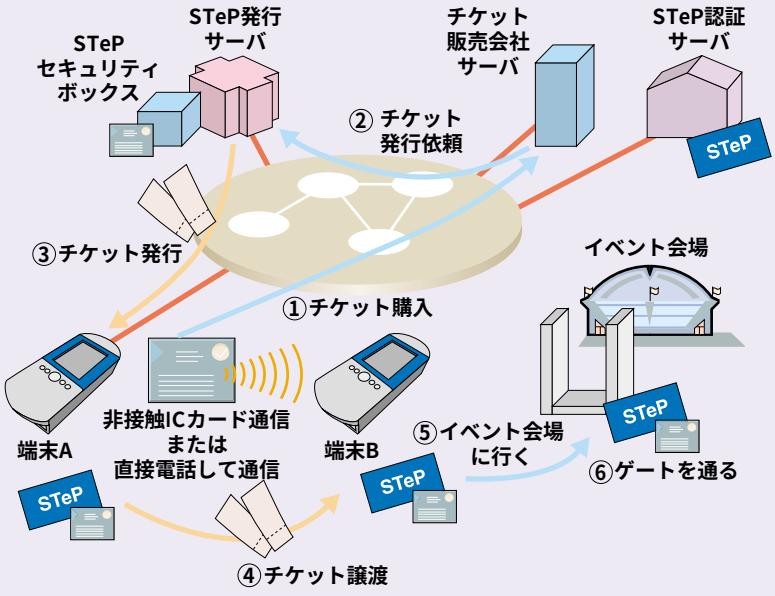


図３　電子チケット販売

(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します．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取り，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（図２）を使って行うことができます．

チケットの購入から利用までの流れを説明していきます（図３の①～⑥）．

図４　STePチップ

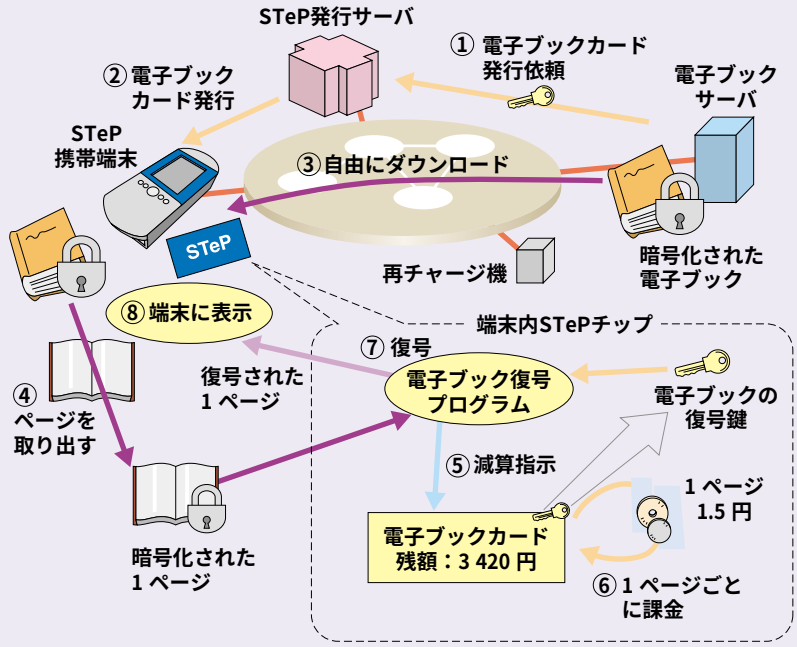


図５　電子ブック課金

① 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，購入手続きを行います．

② 販売サーバはSTeP発行サーバに電子価値の発行を依頼します．

③ 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します．このとき，STeP発行サーバが通信を行うのはSTeP携帯端末内にあるSTePチップ（図４）です．これらは相互認証を行った後，暗号化通信により電子チケットの発行を行います．暗号化はSTePチップとSTeP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内容を知ることはできません．

④ 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います．このとき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どうしが行うことにより，なりすましや盗聴を防ぐことができます．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ありません．

⑤ 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き，改札ゲートにSTeP携帯端末をかざします．

⑥ 改札ゲートと端末内のSTePチップの間で相互認証と暗号化通信が行われます．

(2) 電子ブック課金

STePの想定するサービスの２つ目として，電子ブックの課金システムを示します．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います．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ます．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ます．

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していきます（図５の①～⑧）．

① 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きます．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STeP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します．

② STeP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します．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ます．STeP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ありません．

③　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ます．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ですが，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出すことはできません．

④　ユーザは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みます．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チップに送られます．

⑤　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ますが，復号前にプログラムは電子ブックカードの度数情報を減らします．

⑥　度数はページごとや文字ごとなど，決められた課金単位に基づいて減算します．

⑦　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します．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ません．

⑧　①～⑦の処理を経て，復号された1ページが端末に表示されます．

■STePのシステム要件

従来のeTRONチップは非接触の近接通信だけで他のeTRONチップと電子価値・電子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・電子権利流通を行おうとした場合，次のような問題がでてきます．

①　パッシブ（受動）型の非接触ICカードインタフェースしか持っていないため，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・電子権利情報を授受できません．

②　インターネット経由で電子価値・電子権利流通を行う際，eTRON IDだけでは通信先（eTPセッションを用いて接続する相手）のIP（Internet Protocol）アドレスが分からず，電子価値・電子権利流通が行えません．

③　電子価値・電子権利情報へのアクセスコントロール機能がないため，アクセスレベルの異なる複数の電子価値・電子権利情報を混在させられません．

■STePの設計方針

前述のシステム要件を満たすために，次の方針に従ってシステムを設計します．

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こととします．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います．

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セッションを接続する場合には，このサーバを参照してIPアドレスを取得するようにします．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（ルーチングキャッシュ）を設け，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します．

③　電子価値・電子権利データ仕様に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・電子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します．

■STePのシステム設計

前述の設計方針を基に，eTRONを応用し，図6のようなモバイル向け電子価値・電子権利流通システムを設計しました．図中の構成要素は次のとおりです．

(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どうしでの自由な電子価値の交換を可能とします．

(2)　STeP携帯端末

STeP携帯端末は，T-Engine*を基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合

＊T-Engine：ITRONをベースに発展させた，ユビキタス・コンピューティング環境構築のための，オープンなリアルタイムシステム標準開発環境．

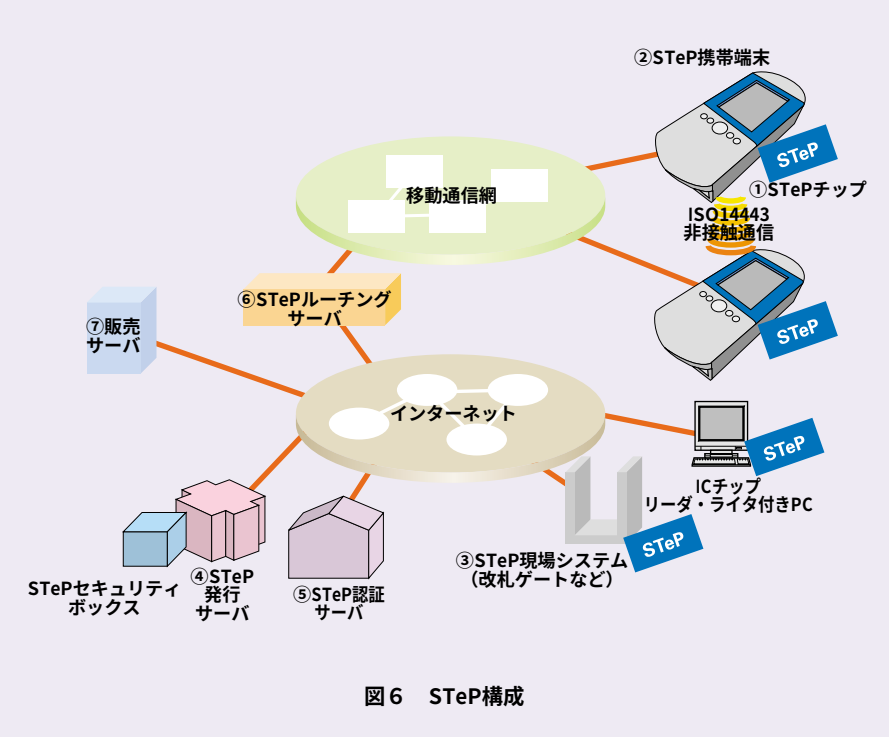


図6　STeP構成

わせ，次の機能を持っています．

①　電子価値取扱機能：STePチップ内の電子価値の操作に用います．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取りすることができます．

②　移動通信機能：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データ通信に用います．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ます．

③　非接触通信インタフェース：STeP携帯端末は背面に非接触ICカードインタフェースを持っています．これを使ってSTeP携帯電話どうしを近づけることにより電子価値のやり取りが行えます．また改札ゲートを通過するときもかざすだけで利用できます．

(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す．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います．

(4)　STeP発行サーバ

STeP発行サーバは後述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す．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っています．

(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す．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ます．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します．

(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す．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ます．STePチップどうし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います．

(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っています．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ます．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て，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ります．

STePの評価

前述し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の実現性について次のように評価しま

した．

(1)　評価その1

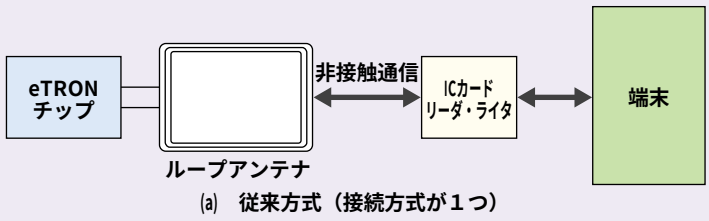
STePチップを接触型として携帯端末と組み合わせることにより，チップを携帯端末に内蔵しつつ，非接触型通信も可能となりました．図7に示すとおり，従来は非接触通信だけで，それ以外の通信方式を利用するには非接触カードリーダ・ライタを経由するしかありませんでしたが，本方式は非接触通信以外にも携帯端末を通して移動通信網，インターネットなどの直接利用が可能となりました．

(2)　評価その2

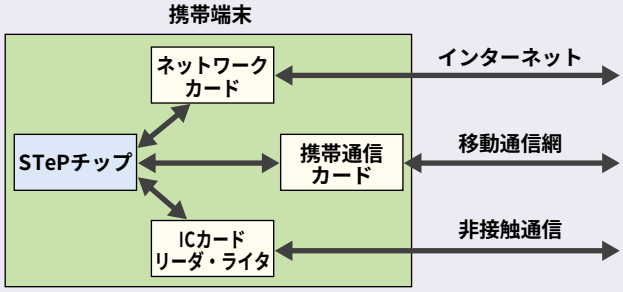
ARSの配備によりインターネットを利用したeTP通信においても，eTRON IDからIPアドレスを検索し接続することが可能となりました．従来方式ではeTRON IDから接続する相手が検索できないため，相手のeTRONチップと接続することは不可能でしたが，ARSに問い合わせることによりネットワークによらず相手のSTePチップと接続することが可能となりました．図8にその画面を示します．図8(a)は電子チケットを携帯端末に転送している場面です．ARSがない場合は図8(b)のように，転送先が見つからず通信エラーとなりますが，ARSがある場合には図8(c)のように正常に完了します．

(3)　評価その3

ACLの設定により，所有者が自分の電子価値・電子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りました．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・電子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，カードの入替や電子価値の増減により不整合が起きる恐れがありました．本方式では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となっています（図9）．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ました．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すが，電子チケットは所有者のほかに改札

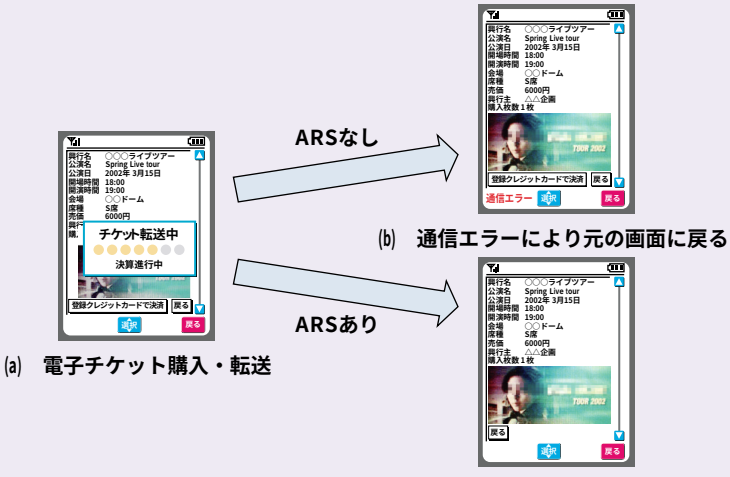


(a)　従来方式（接続方式が1つ）



(b)　本方式（接続方式が3つ）

図7　評価その1

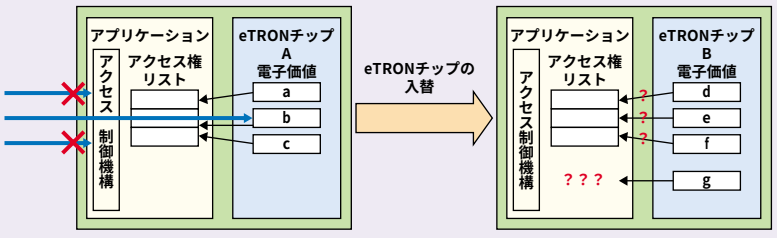


(a)　電子チケット購入・転送

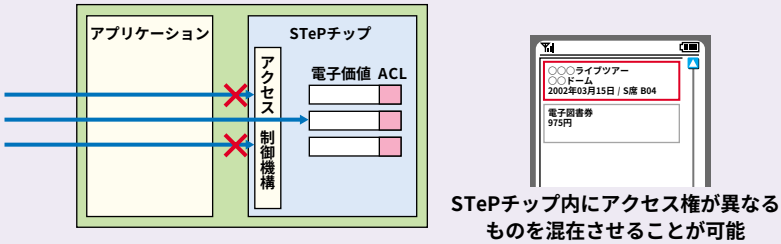
(b)　通信エラーにより元の画面に戻る

(c)　正常に電子チケット転送完了

図8　評価その2



(a) 従来方式（アプリケーションによるアクセス制御）



STePチップ内にアクセス権が異なるものを混在させることが可能

(b) 本方式（ACLによるSTePチップでのアクセス制御）

図9 評価その3

ゲートからアクセス可能となっています．

またeTRONの機能を利用して携帯端末環境でユーザどうしが電子価値・電子権利を流通でき，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ました．

今後の展開

STePではSTePチップどうしが直接相互認証や暗号化通信を行いますが，ICカードのCPU（Central Processing Unit）はPCのCPUと比較しても計算能力は10～100分の1と低く，認証や暗号計算を行うのに時間がかかります．このため，相互認証には平均1 200 ms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ます．現在，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しているところです．

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ません．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・電子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，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ったりします．そこで，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を拡張する試みも併せて行っています．

STePチップでは電子価値のやり取りを一方から一方への受渡しとして実現していますが，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す．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とき，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，安全で公平な電子価値の交換が行える方式の検討も行っています．

■参考文献

(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) 青野・石井・森・本郷・越塚・坂村：“モバイル向け電子価値流通プラットホームの研究,” 情処学研報，第19回CSEC研究会.
(3) 越塚・坂村：“eTRON: Entity and Economy TRON,” 情処学研報，第19回CSEC研究会.

（後列左から）寺田 雅之/ 本郷 節之
（前列左から）森 謙作/ 石井 一彦

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・電子権利流通プラットフォームSTePについて解説しました．STePを用いるとセキュリティを保ったままユーザどうしで自由な電子価値のやり取りを行うことができます．今後はさらな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ます．

◆問い合わせ先
NTTドコモ
ネットワークマネジメント開発部
TEL 046-840-3809
FAX 046-840-3705
E-mail ishiikaz@nttdocomo.co.jp