コンピュータセキュリティ 19−12
（２００２．１２．２０）

モバイル向け電子価値流通プラットホームの研究

青野博† 石井一彦† 森謙作† 本郷節之† 越塚登‡ 坂村健§

近年，インターネットにおけるＥコマースが行われ，電子チケットなどの電子価値の販売も行われている．しかし，セキュリティの問題から個人間の電子価値のやり取りやまだ実用段階ではない．筆者らは，バーチャルとリアルの 世界双方で利用でき，安全に電子価値実体を流通させることのできるプラットホームの研究を行なっている．本稿では，デジタル情報を安全に格納，流通させることを可能にする耐タンパー技術をベースとした分散セキュリティーアーキテクチャである eTRON（Entity and Economy TRON)をモバイル環境に適用したモバイル向け電子価値流通プラットホーム(STeP:Securely Transferable Entity Platform for Mobile Communications)について設計方針と構成および STeP を用いた具体的なシステムについて述べる．

キーワード：モバイルＥコマース，電子価値流通，IC カード

Securely Transferable Entity Platform for Mobile Communications

Hiroshi Aono†, Kazuhiko Ishii†, Kensaku Mori†, Sadayuki Hongo†,
Noboru Koshizuka‡, Ken Sakamura§

Recently, we can buy digital value such as an electronic ticket using E-Commerce in the Internet. But we can't transfer digital value between terminals directly for the viewpoint of the security. We research the secure platform that can transfer digital entities between mobile terminals directly in the Internet and real world. We applied eTRON architecture which is the secure distributed architecture based on tamper-resistant technology for our securely transferable entity platform for mobile communications (STeP). In this paper, we describe about the design policy and structure of STeP, and introduce concrete system using STeP.

Keywords: Mobile E-Commerce, IC Card

† 株式会社 NTT ドコモ マルチメディア研究所
Multimedia Laboratories, NTT DoCoMo, Inc.
‡東京大学情報基盤センター
Information Technology Center, The University of Tokyo/
§東京大学大学院情報学環
Interfaculty Initiative in Information Studies, The University of Tokyo.

1. はじめに

デジタル情報を安全に格納，流通させることを可能にする 耐タンパー技術をベースとした分散セキュリティーアーキテクチャ，(eTRON: Entity and Economy TRON)が東京大学坂村教授らにより提案されている[1]．筆者らは，モバイル環境において電子価値流通を安全に行うことを目的とし，eTRON アーキテクチャをモバイル環境に適用した電子価値流通プラットホーム(STeP: Securely Transferable Entity Platform for Mobile Communications)を開発し，電子チケット流通および電子ブック流通システムに適用した．本稿では，本プラットホームの設計方針と構成およびそれぞれの具体的なシステムの実装とその結果について述べる．

2. 本研究の目的と背景

近年のモバイル E コマースの利用状況は[2]にあるように，有料情報や音楽ダウンロードが中心である．しかし，将来期待するサービスとしては，オンライン・クーポンやチケットの予約などがあげられている．一方，固定網における E コマースと比較して，モバイル環境における E コマースのメリットは，ネットワークを利用して購入した電子価値を実世界で利用できることである．このメリットを生かせば，チケットは予約だけでなく，電子チケットとしてモバイル環境で流通，利用が可能である．しかし，そのメリットを最大限に生かすためには，電子価値の流通をサーバを介して行うのではなく，端末間，端末/改札間といったローカルな電子価値の流通が必要になってくる．従来の方法で，ローカルな電子価値流通を行った場合には以下のような問題がある．

・端末の紛失，盗難による電子価値の不正利用
・端末の改造による電子価値の偽造および不正利用
・IC カードに格納した場合も，従来の IC カードは端末からの命令による動作しか行わないため，端末または流通の途中での不正が可能

権利の流通という観点からは，藤村らによる FlexTicket[3]が研究されている．FlexTicket はさまざまな権利をデジタル化し流通させる技術である．チケット自身に改ざん防止，二重使用防止等の安全な流通のための対策はとられている．しかし，端末間(IC カード間)のチケットの流通は報告されていない．

また，電子マネーに使われている技術ではあるが，Mondex で使われている VTP(Mondex Value Transfer Protocol)[4]があり，IC カード間の Value の交換が可能である．VTP では，IC カード間で Value をやり取りされるそれぞれのメッセージ対してデジタル署名を付与される．そのためやり取りする相手すべての公開鍵証明書を保持しておく必要がある．

Mana[5]らは，GSM-Ticket と呼ばれる GSM の SIM をベースとしたチケットシステムの提案を行っている．本システムは，チケットに Merchant の署名を付し，購入者の公開鍵を用いて暗号化し流通させる(Open Ticket 状態)．利用時には購入者がチケットを復号して利用者の ID を含めた Hash 値をチケット(Closed Ticket 状態)として使用する．Open Ticket の状態では転々流通が可能であるが，いったん Closed Ticket にすると流通不可能である．また，Closed Ticket でチケット利用時にはユーザの ID を提示する必要である．

一方，eTRON アーキテクチャは，IC カードをはじめとする耐タンパーデバイス間で相互認証および鍵の交換を行い，その鍵を用いた安全な通信路を確保してから電子価値流通のプロトコルを実行するため，端末や流通途中での不

正が困難となっている.

3. eTRON(Entity and Economy TRON)アーキテクチャ

eTRON とは，デジタル情報を安全に格納し，デジタル情報インフラ上で流通させられる，耐タンパーデバイス（例えば IC カード.以下 eTRON カード）を核技術とした分散広域システムアーキテクチャである．本章では，eTRON の特徴である eTRON 電子実体および eTP についての概略を述べる.

3.1. eTRON 電子実体

eTRON 電子実体とは，物理的な実体の持つ一体性，製造困難性，複製不能性，改竄困難性，携帯性などの性質を持つデジタル情報である．eTRON 電子実体は eTRON カード内のみに格納され，eTRON カード間のみで転送される．また，IC カードに対しての攻撃による eTRON 電子実体の改ざん，複製を防ぐために，eTRON カード内の eTRON 電子実体に対し行える操作を限定する.

3.2. eTP(Entity Transfer Protocol)

eTP は，eTRON カード間で eTRON 電子実体を安全にやり取りするためのプロトコルである．本プロトコルは，eTRON カードにユニークに割り当てられる eTRON ID 対する公開鍵証明書を利用して，相互認証と鍵交換を行う．そこで得られた鍵を利用した安全な通信路内で，2-Phase Commitment をベースとした eTRON 電子実体の流通を行なうトランザクションが実行される．eTP により通信途中での盗聴，改ざんを防ぎ，通信切断時等にも eTRON 電子実体の不整合が起こらない.

また，eTRON ID は eTRON アーキテクチャをもつハードウェアに対して付与される ID であり，個人を特定するものではない.

4. モバイル向け電子価値流通プラットホーム

4.1. プラットホーム概要

筆者らは，下記のような要件を満たす安全に電子価値流通を可能とするプラットホームの検討を行なった.

- 電子価値のオフラインでの転々流通を可能とする
- 利用時には匿名性を確保する
- 電子価値を格納するハードウェアは耐タンパー性を有する

これら要件を満たすために eTRON アーキテクチャを採用し，電子価値を eTRON 電子実体として流通させる方針で設計を行なった．また，モバイル環境の利用を前提とし，端末を含めた以下のような特徴を持つプラットホームとして STeP の設計および開発を行った.

・強固なセキュリティ
IC カードが直接相手の IC カードを認証し，IC カード間の通信は暗号化を行うため，携帯端末を分解・解析されてもデータは安全．各 IC カードには eTRON ID が付与され，その ID に対して公開鍵証明書が発行されている．この公開鍵証明書に基づき，IC カード間で相互認証を行う.

・1 台で多様な利用シーンに対応
データ通信 ・非接触 IC カード ・IC カードチャージ機の機能を持つ

・自由な電子価値の流通が可能
端末同士のみで安全に電子価値の授受が可能なため，サーバ経由および端末間の価値流通が可能

これらの特徴を実現するために，STeP は eTRON カード，モバイル向け電子価値流通用端末，eTRON 発行サーバを構成要素として持つ．本章ではそれぞれの機能ついて述べる.

4.2. eTRON カード

eTRON アーキテクチャ仕様にもとづいた電子価値を保存, 操作および eTP を利用して eTRON エンティティの安全な交換を行う機能を持つ. eTP における相互認証および秘匿通信に必要な, 暗号アルゴリズムを搭載している. また, 本 IC カードは ISO 7816 で外部と交信できる機能を持つ.

4.3. モバイル向け電子価値流通用端末

モバイル向け電子価値流通端末(以下, STeP 端末)は, ユーザが電子価値を受け取り保持し, 実際に利用する場でそれを操作し, 他に送り出すため機能を持つ. STeP 端末は, 電子価値の内容の提示, 譲渡, 削除, 発行要求などのやりとりが行える.

STeP 端末は, タッチパネルカラー液晶画面, ボタンスイッチ, eTRON カードスロットを搭載し, PCM/CIA カードスロット, CF カードスロットを持つ. PCM/CIA カードスロットに NTT ドコモ社製コンパクトフラッシュ型 PHS 端末 P-inComp@ct™ 等を装着することでデータ通信可能な携帯端末となり, PHS 網を経由して電子価値をやりとりする機能を持つ.

主な機能は以下のとおりである.

（1） 電子価値取扱い機能

装着された eTRON カード内の電子価値の内容の提示, 譲渡, 削除, 発行要求などのやりとりが行える操作する機能をもつ.

（2） 端末側ルーティング機能

電子価値を流通させるとき, eTRON カードの持つ eTRON-ID による宛先指定での通信要求があった場合に, eTRON-ID から通信を確立できる機能である. STeP 端末でルーティング情報を記憶し, 可能な場合にはルーティング用サーバに接続せずに通信を確立できる機能をもつ.

（3） eTRON ハンドラ

STeP 端末上で実際にユーザに電子実体の操作を行わせるためのマンマシンインタフェース.

（4） 非接触インタフェース

STeP 端末には, ISO14443 非接触通信を行うための R/W およびアンテナを持つ. これにより, STeP 端末間および利用現場における R/W との eTP による通信を行い, 端末間の電子価値流通, 利用が可能である.

4.4. eTRON 発行サーバ

eTRON アーキテクチャ仕様に基づきユーザが持つ STeP 端末に装着された eTRON カードに対し, 電子価値を発行するサーバであり, 以下の機能を持つ.

（1） 電子実体生成機能

eTRON アーキテクチャ 仕様に基づく電子価値を安全かつ改変のできない形式で発行するための機能である. 発行とは, 通常の電子データによる電子価値のフォーマット定義とその具体的な内容データから, 暗号化を行い, eTRON における電子価値のフォーマットに従った電子価値を生成する機能である.

（2） 電子実体送付機能

発行された電子価値を, サーバから STeP 端末上の eTRON カードへ eTP を利用して電子実体を送付する機能である.

（3） ルーティング機能

eTRON カードが，多様なネットワーク経由で接続されるような場合，遠隔の eTRON カードに対し，eTRON ID を指定することによりその eTRON カードと通信を開始できる必要がある．このため，その時点で対象となる eTRON カードが，インターネットや移動体通信網などの中でどこに，そしてどのホストに接続されているかを判断して通信経路を確立する機能である．

5． 電子チケット流通システム

STeP の適用システムのひとつとして，電子チケット流通システムの開発を行った．本システムは，紙のチケットを出力する代わりに，eTRON 電子価値の生成を行い，STeP 端末を利用して流通，消費を行うシステムである．STeP で持つ機能に加えて以下の機能の開発を行った．図１にシステムの概要を示す．

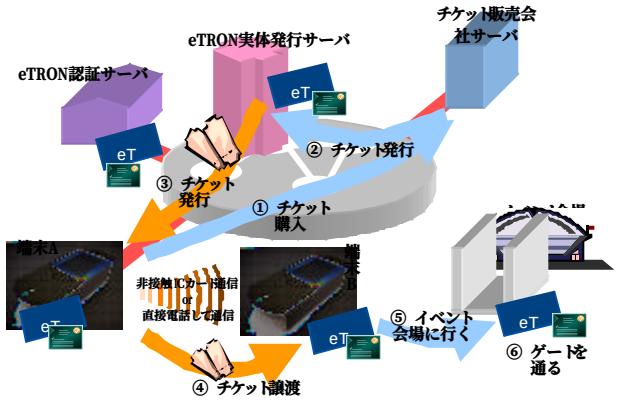

図１．STeP を用いた電子チケットシステム

（１） 電子チケット販売サーバ

既存の電子チケット販売サーバに eTRON 電子価値を取り扱う機能を付加したものである．既存のシステムが紙のチケットを印刷または，電子メール等による予約 ID を送付する機能の代わりに，発行サーバに対して，eTRON 電子価値の発行の依頼を行う．

（２） 改札システム

本システムは，ISO14443 の R/W 機能を持ち，STeP 端末を経由して eTRON カード内の電子チケットの電子価値を参照することにより，いわゆる“もぎり”を実現する．

本システムの特徴は，STeP 端末の PHS 通信および非接触 I/F を用いて，端末間で電子チケットのやり取りが行えることである．本システムを利用することにより，電子チケットの購入，譲渡，利用が実際に行えることを確認した．

6． 電子ブック流通システム

STeP のもうひとつの適用システムとして，電子ブック流通システムの開発を行った．本システムは，STeP 端末に自由にダウンロード可能な暗号化された電子ブックを，eTRON カードに電子価値として格納された電子図書券を利用することによりマイクロペイメントを実現したシステムである．STeP で持つ機能に加えて以下の機能の開発を行った．図２にシステムの概要を示す．

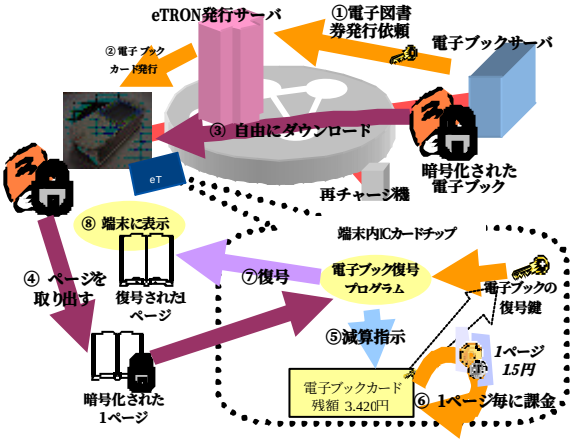

図２． STeP を使った電子ブック課金

（1） リロードサーバ

マイクロペイメントを実現するためにeTRON電子価値としての電子図書券の発行を行う．また，有料電子ブックの利用に伴い電子図書券内のアカウントが減算されるが，必要に応じてユーザはネットワーク経由でそれをリロードする必要がある．このアカウントのリロードする機能も持つ．また，リロード操作時にマイクロペイメントの課金内訳情報をユーザのeTRONカードから読み出して解析する．この課金内訳情報のアップロードと解析により，電子ブックのプロバイダに対して，購読料の支払いが可能となる．

（2） 電子ブックViewer機能

本機能は，STeP端末上の機能である．電子ブック購読時には，eTRONカードで書籍データを復号し、残高データを減算する事(課金処理)をアトミックに処理する機能を持つ．書籍データ復号および課金処理をアトミックに行うことにより，復号された書籍データの複製や課金処理の不正を防ぐことができる．

本システムの特徴は，以下のとおりである．

・電子ブック自体は自由に配布が可能である
・ページ単位などのマイクロペイメントが可能である
・eTRONを利用して安全にリロードおよび課金内訳情報が流通可能であるため，電子ブックプロバイダに対して正確な売り上げの計上が可能

本システムを利用して，暗号化された電子ブックをページ単位に課金しながら復号表示し，購読することを確認した．現在の実現では電子ブックの復号をICカード内で行っているために復号表示までに時間がかかりすぎる問題がある．

7. まとめ

本稿では，eTRONアーキテクチャをモバイル環境に適用したSTePの開発およびSTePを利用した2つのEコマースシステムの開発について述べた．

eTRONを利用することにより，モバイル環境で電子価値を流通できることが確認できた．今後は，今回開発した実システムについて有効性の検証を行い，STePへ更なる改善を行っていく．また，STePを用いて，他の電子価値を流通することによるさまざまなサービスについて検討を行う．

8. 謝辞

本研究に対して，ご指導いただいたマルチメディア研究所中野所長ならびに同研究所各位に感謝する．

[参考文献]

[1] 越塚，坂村他，” eTRON: Entity and Economy TRON”，情報処理学会研究報告，第19回CSEC研究会

[2] “モバイルインターネットの利用実体と今後の利用意向”，H13 ECOM モバイル EC-WG報告書

[3]http://info.isl.ntt.co.jp/flexticket/index_j.html

[4] http://www.mondexusa.com/

[5]Antonio Mana 他，”GSM-Ticket:Generic Secure Mobile Ticketing Service”，2001 Gemplus Developer Conference