マルチメディア通信と分散処理 76－17
（1996．5．16）

電子決済システムの実装と評価

寺内 敦、 森保 健治、 三宅 延久、明石 修

{terauchi, moriyasu, miyake, akashi}@slab.ntt.jp

NTT ソフトウェア研究所

東京都武蔵野市緑町 3-9-11

概要

電子商取引 (Electronic Commerce: EC) における決済方式を提案する。従来からも種々の決済方式が提案されているが、現金や小切手に代わるもの、あるいは現在のクレジットカードの情報を Network 上で安全にやりとりするための方式が主であった。それらに対し、提案方式ではプリペイドカードやクーポン券的な使用を想定している。そのため特定の商店あるいはその集合と顧客という比較的小さな世界ですぐに運用が開始でき、さらにシステムの構築コストも低く抑えられる。また、提案方式に基づく決済システムの実装方法に関する検討を行った。その結果に基づき実際にシステムを作成した結果についても述べる。

Implementation and Evaluation of Electronic Payment System

Atsushi TERAUCHI, Kenji MORIYASU, Nobuhisa MIYAKE, Osamu AKASHI

{terauchi, moriyasu, miyake, akashi}@slab.ntt.jp

NTT Software Laboratories

3-9-11 Midori-cho Musashino-shi Tokyo 180, Japan

Abstract

This paper describes about electronic payment system in Electronic Commerce (EC). In this field, Various payment methodologies or systems were proposed to realize electronic cash, electronic check, and use credit card over network. The proposed payment method can be used like prepaid card system in the real world. Generally, prepaid card is available only in the specified shops or the services. So, payment systems based on this method can be built small, that is, with lower cost, compared with electronic cash or check system.

Implementation of an electronic payment system based on the proposed payment method and the feasibility of the system are also described.

1 はじめに

近年のInternetの普及はめざましく、非常に多くの人々が利用できるようになっている。そのため、これらの多数のユーザを対象としてNetwork上での商取引(Electronic Commerce: EC)を行うためのシステムが多く提案されてきている。ECのシステム実現のためにはNetwork上の商店の構築、マーケティング情報を管理、運用するためのシステムなどさまざまな技術が必要であるが、商品に対する料金を確実に決済、受領することのできる決済システムはECを実現していく上での中核となる技術の1つである。現在までにECにおいて決済システムや決済方式が多く提案され、これらの決済システムおよび方式をサポートするNetwork上の商店もいくつか稼働している。

このように商店がNetwork上にあるという状態が一般的になってくると、商店にとっては今後は単にNetwork上で売買ができるだけではなくて付加サービスの充実、マーケティング情報をフィードバックした販売戦略といったものが他店との差別化の点から重要になってくると思われる。本稿ではこのような商店の付加サービスの1つである、商店によるプリペイドカードやクーポン券の発行をECにおいて実現するための決済方式を提案する。また、提案方式に基づく決済システムの実装方法に関する検討を行った。その結果に基づき実際にシステムを作成した結果についても述べる。

2 提案方式の位置付け

2.1 現実世界の決済方式

本稿で提案する方式の決済方式としての位置付けを明らかにするために、まず現実世界における決済方式の分類を試みる。

決済方式を分類するための要素としては以下のものが考えられる。

1. **匿名性**
   匿名であればユーザのプライバシが保護できるが、後の不正検出および追跡などは困難である。また、匿名にすることにより他人への譲渡あるいは流通が可能になる。逆に記名式であればユーザのプライバシは基本的に保護できないが、使用者の情報が残るので不正があったときの検出などは容易である。

2. **通用範囲**
   その決済方式がどの範囲で通用するかは決済方式の適する分野および要求されるセキュリティの強度に影響すると考えられる。現金や銀行振込みなどはほぼどのような取引にも使えるので非常に通用範囲が広い。クレジットカードは加盟店でしか使えないし、小切手も使える店は(特に日本では)限定される。プリペイドカードや商品券類はもともと特定の商店のサービスとして実施されるものであるので、さらに通用範囲が狭くなって基本的にその発行主にしか通用しないのが一般的である。

現実世界の決済方式をこの二つの基準により分類した結果を図1に示す。

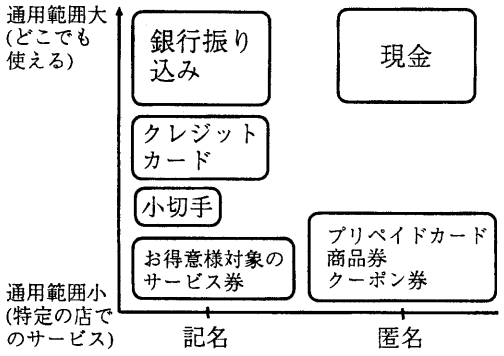


図1: 現実世界における決済方式

この図において、商店が常連客を囲い込むために行っている特別サービスの類は実際には無記名に等しい(=特に認証を行っていない場合が多い)が、商店側の論理としては購入者の情報をもとに対象者のみに行っていると考えられるので記名式のカテゴリに含めた。

2.2 ECにおける決済方式

2.2.1 従来方式

現実世界での分類を元にして、ECにおける決済方式の分類を試みる。現在までに提案されている種々の方式はおよそ以下の3つのカテゴリに大別できる。

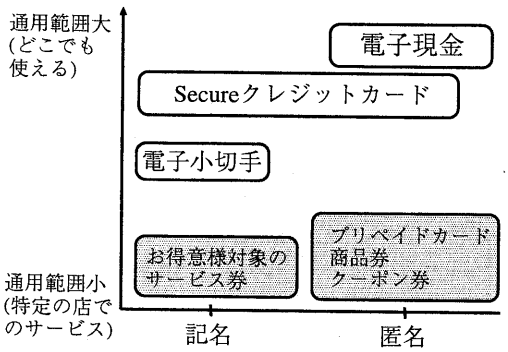
1. **電子現金**
   現金の持つ種々の性質(匿名性、譲渡性、分割性など)を持つNetwork上での決済方式を実現することを目指している。事例としてはエスクロー現金方式[1]、E-cash[2]などがある。

2. **電子小切手**
   小切手のようにできるだけSecurity強度の高いNetwork上での決済方式を提供することを目指している。現金の持つ匿名性や譲渡性などの性質はない。事例としてはNetBill[3]などがある。

3. **Secureクレジットカード**
   クレジットカードの情報を安全にNetwork上でやりとりすることを目指す。通常のクレジットカードの使用と違い、商店に対して購入者情報を隠蔽するなどの工夫がなされている。事例としてはSETなどの専用プロトコルとFirst Virtualなどのシステムの2種類が存在する。

これらはそれぞれ現実世界における現金、小切手、クレジットカードに対応すると考えられる。

ECにおける決済方式を図 1と同じ方式で分類したものを図 2に示す。



: 本方式が対象とする領域

図 2: ECにおける決済方式

この図では電子現金は現実世界と同じく最も通用範囲が広いことになっている。しかし、現状ではECにおける電子現金や小切手はまだ通用範囲(使える商店)は狭く、もともと与信などのシステムが整備されているクレジットカードの通用範囲が一番広い。しかし、電子現金の狙いとしては現実の現金と同じくらいの通用範囲になることを目指していると考えて現実世界と同様の通用範囲とした。また、Secureクレジットカードは前述のように現実世界と違い商店に対しての匿名性が確保できるので、記名式と匿名式の両方をサポートしているものとした。

2.2.2 提案する方式

前章で見た通り、過去に提案されている決済方式はいずれも多くの店で使える通用範囲の広い一般的な決済方式を提供することを目標にしてきたと言える。しかし、現実世界で行われているように商店(街)自身がお得意様へのサービスの一環として独自にブリペイドカードやクーポン券(以下、ブリペイドカード)を発行したいという要求はECにおいても存在する。また、Network上の商店ではいろいろな店を短時間に簡単にめぐることができるので一度訪れたお客をつなぎとめるための囲い込み戦略も重要になってくる。そのようなとき、お得意様だけの特別サービスなどは効果があり、やはり売る側からのニーズは多い。このようなサービスを実現するためには現金や小切手のようにどこの店でも使えるように銀行あるいはクレジットカード会社を組み入れた大規模なシステムにする必要はなく、単独の商店、あるいは幾つかの商店が集まって独自に始められるような方式で十分である。

以上の観点から本稿では現実世界におけるブリペイドカードやクーポン券的に使うことを想定した決済方式を提案する(図 2における網かけ領域)。この方式では電子現金のような汎用的な方式と比較するとCAなどの大規模な設備を必要としないため特定の商店(街)だけですぐに運用を開始することができる、管理すべきなのは基本的に顧客データベースだけなので管理コストが低くできるというメリットがある。

3 提案方式の概要

3.1 モデル

提案方式で想定しているモデルを図 3に示す。登場するplayerは「センタ」「商店(街)」「ユーザ」の3者である。それぞれの役割について説明する。

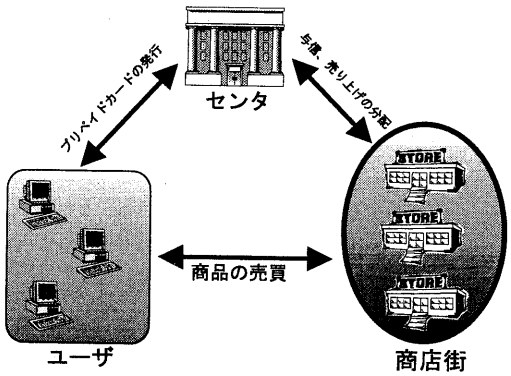


図 3: モデル

- **ユーザ**
  センタにブリペイドカードを申し込み、このブリペイドカードを用いて加盟店から商品を購入する。ユーザはすべてセンタの顧客データベースに登録されているものとする。

- **商店(街)**
  ブリペイドカードを持ったユーザに対して商品を売る。ユーザからの購入申込が来たらセンタに対して与信を行う。取引が承認されれば商品をユーザに送る。またトランザクション終了後、センタに対してカードによる売上を報告してそれに応じた利益の分配を受ける。

- **センタ**
  ユーザに対してはブリペイドカードを発行し、加盟商店に対しては購入時の与信および売上の分配を行う。センタでは登録ユーザ、商店の情報や発行したブリペイドカードの情報をDBで管理する。これらの情報は商品購入時にも商店からの与信によって参

照、更新されて、つねに最新の情報が管理されている。

このうち、「ユーザ」「商店」は(単独でも結託してでも)悪事を働く可能性があるが「センタ」は信頼できるものとする。

この図では「ユーザ」「商店」は複数あるものとしているが、それぞれが1つであるとしても提案する方式には影響は与えない。そこで簡単のため以下では「ユーザ」「商店」も1つであると仮定して議論を進める。

一般にはプリペイドカードなどは商店が発行するものでありセンタは必要ないように見えるかもしれないが、テレホンカードを例に取ると、実際にカードを販売しているのは小売店であるが、NTTがカードの発行および売上の管理を行っている。その意味ではこのモデルは現実のプリペイドカード発行モデルと一致しており妥当なものと言える。もちろん、1つの商店が独自にプリペイドカードを発行するような場合、つまり、商店がセンタを兼ねるような場合もこのモデルで扱える。

3.2 攻撃と対処

ECにおいては第三者だけでなく悪意のある利用者および商店などがさまざまな不正を行うことが想定され、これらについて十分な対処を行っておかねばならない。特に、ディジタル情報は改竄、コピーが非常に容易に行えるため、このような不正に対する対処は厳重にしておく必要がある。

1. **悪意のある使用者による改竄**
   匿名[1]式(例：クーポン券)の場合はSerial Number、記名式(例：お得意様限定サービス券)の場合は使用者の情報をカードに付加しておき、購入時にはセンタに与信を行う。センタでは常にカードの最新の状態が管理されているので、カードの内容(特に、金額)が改竄されていると即座に検出することが可能である。また、このことはユーザ側でのディスククラッシュなどのトラブルに対する対処(再発行など)も容易にする。

2. **第三者による改竄**
   第三者が使用者の知らないところでカードをコピーする、あるいは改竄するなどの不正が起こる可能性がある。提案方式では端末上に保存したプリペイドカードは使用者しか知らないパスワード[2]で暗号化して保存しておき、専用ソフトウェアを用いて復号化しなければ使用できないという対処を行っている。

3. **匿名カードに対する譲渡性**
   匿名のカードは自分のカードを自由に他人に譲渡できるという性質を満たす必要がある。基本的には本方式ではコピー防止のために端末上に保存されたカードは暗号化されており、そのままで譲渡しても使用できない。そのため、譲渡する際には使用者が明示的に(=譲渡する目的のために)譲渡できるような仕組がユーザ側に必要であると思われる。

[1] ここでの「匿名」とはセンタおよび商店に対して購入者の情報が渡らないこととする

[2] すべてのユーザは匿名のカード、記名のカードを使うかに拘らずセンタへ登録されているのでどちらの方式でもパスワードが存在する

それ以外の代表的な攻撃とそれに対する対処を表1に示す。

表1：攻撃と対処

攻撃	本システムにおける対処
通信路上のメッセージの盗聴、改竄	公開鍵暗号方式によるメッセージの暗号化
商店による売上情報の改竄	ディジタル署名付きの送り状の発行
ユーザのなりすまし	パスワード認証
メッセージの再利用による商品鍵の盗難	メッセージにタイムスタンプを付加

3.3 購入プロトコル

本システムで商品を購入する手順を以下に示す。センタとユーザはパスワードをあらかじめ共有しているものとし、商店はユーザのパスワードは知らないものとする。

1. 購入を始める前にユーザは自分のプリペイドカードをセンタからダウンロードする。このとき、センタに送る情報はユーザIDとパスワードである。センタは該当するプリペイドカードを検索してユーザに送信する。(図4のメッセージ(1)、(2))

2. ユーザは購入する商品を選び、購入トランザクションを開始する。まず始めにユーザは「鍵要求」メッセージを送り、商店の公開鍵を取得する。(図4のメッセージ(4)、(5))

3. ユーザは商店に対してプリペイドカードと購入申込を送る。このメッセージは、記名式の場合は商店の公開鍵(商店がお得意様情報を取得するため)、匿名式の場合はセンタの公開鍵(商店に内容を見せないため)で暗号化する。記名式の場合のみ、商店による購入メッセージの改竄防止のためユーザのディジタル署名[3]を付加する。(図4のメッセージ(6))

4. 商店は購入申込を受け取ったらセンタに転送する。(図4のメッセージ(7))

5. センタは転送された購入申込およびカードの残高を検証する。記名式の場合はユーザが付加したディジタル署名の検証も行う。

6. 問題がなければセンタは商店にトランザクションを承認するメッセージを送る。(図4のメッセージ(8))

[3] この署名はユーザのパスワードを用いる

7. 商店は暗号化された商品、商品の復号鍵および自分の署名付きの送り状をユーザに送る。(図 4のメッセージ (9))

8. 送られてきた復号鍵を用いて暗号化された商品の復号化を行う。復号化完了後、復号鍵は消去する。また、プリペイドカードの残高を更新する。

9. ユーザは復号が完了すれば、記名式の場合は自分の署名を付加した受領書を商店に送る。匿名の場合は署名なしの受領書を送る。(図 4のメッセージ (11))

10. 商店は受領書をもらったら売上情報の更新を行い、その情報を後日センタに送る。センタではこの情報をもとに各商店へのカード売上の配分を行う。

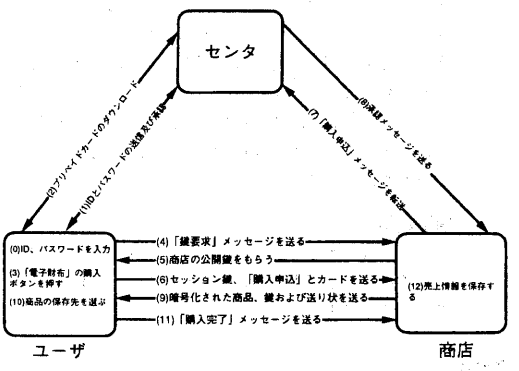


図 4: 購入プロトコル

4 システムの実装

4.1 設計方針

1. 購入する商品の情報は WWW で見せてユーザはその画面を見て商品を選ぶ

2. 既存の WWW システムにはできるだけ手を加えない

4.2 電子財布

4.2.1 実装方式

ユーザの端末上ではプリペイドカードを安全に保存、使用するために専用のソフトウェア (以下、「電子財布」と呼ぶ) を用いる。この「電子財布」と WWW クライアントとは購入手続きの中で連動して動作する必要がある。このような要求を満たすような「電子財布」の実装方式としては以下のようなものが考えられる。

1. Plug-in 方式
   Netscape などが提供する Plug-in API を用いてプログラムを作成する方式。WWW クライアントの種類に依存する。

2. 擬似 Proxy 方式
   クライアントの通信ポートを監視するプログラムを常駐させておき、そのプログラムにメッセージの暗号、復号化などの処理を行わせる方式。Proxy と WWW クライアント間の通信を Hack される恐れが生じる。

3. Helper 方式
   WWW クライアントの Helper アプリケーションとして実装する方式。作成したプログラムは WWW の種類に依存せず使用できる。

今回は、電子財布の実装方式として 3 番目の Helper 方式を採用した。これは、Helper アプリケーションは WWW と全く独立に作れるので今回のように独自の暗号通信を行うような場合は実装が容易、WWW クライアントの種類を問わない、1 つの独立したアプリケーションなので将来の機能拡張が容易にできる、などの理由による。

4.2.2 WWW クライアントとの連動

今回は図 4に示した購入プロトコルの処理はすべて電子財布に組込み、WWW を単なるカタログ的に使用する方式を取った。電子財布は購入手続きが発生するとセンタおよび商店で動作している専用のサーバプログラムと WWW での通信とは別に Socket 通信を行う。これにより従来の WWW サーバおよびクライアントは既存のものがそのまま使用できる。

購入プロトコルの処理は Helper で行うが商品情報は WWW で表示されている。そこで、WWW の画面で表示されている商品情報を電子財布に渡す仕組を提供するために通常の HTML で記述された document に付加情報を加えた multipart 形式の document type (content-type: application / infoket) を新たに定義した。前者は WWW クライアントによって表示されて、後者は電子財布が購入トランザクションを処理するために使用する。

以下に infoket type の document の例を示す。

```
<HTML>
    <CENTER>
    <H1> 電卓の販売を行っております。 </H1>
    <H4> 電子財布の購入ボタンを押して下さい。 </H4>
    </CENTER>
</BODY>

</HTML>

<!-- Contents --> ← セパレータ
S shop ← 商店名
```

```
D infoket-server.slab.ntt.jp ← 商店のホスト名
G GS0001 ← 商品 ID
F calc.exe ← 商品名
M 3000 ← 価格
```

4.3 システム構成

実際に作成したシステムの構成図を図 5に示す。ユーザの WWW クライアント以外のモジュールはすべて新規に作成した。ユーザの環境は Windows の動作する PC 上に、センタおよび商店は UNIX ワークステーション上にそれぞれ実装した。

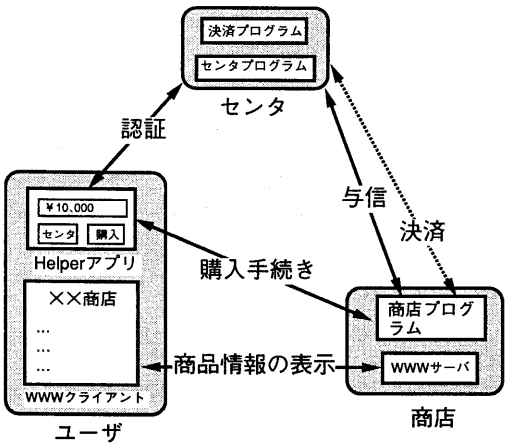


図 5: システム構成図

それぞれのモジュールのプログラムサイズは

- 電子財布： 700 step (Visual Basic) + 1500 step (C 言語)
- センタプログラムと商店プログラム： 3000 step (C 言語)[4]

であった。

本システムを用いて実際に Network 上で商品を購入することができることを確認した。また、3.2章で示したようにプリペイドカードのコピーや改竄を行ってみたがそのような不正はセンタで確実に検出することができた。

また、今回のシステム試作により提案方式ではセンタで氏名、住所などのユーザ情報と個々のユーザが所有するプリペイドカードの残高を管理するだけで十分に運用できることも分かった。電子現金方式の中には二重使用防止のために発行されたすべての電子紙幣の状態 (未使用か使用済) を保存しておかねばならないものもあり、非常に大規模な DB が必要と思われる。それらと比べると本方式ではセンタに用意すべき DB の規模もごく小さく、個々の商店が単独で運用を開始することも十分可能であると考える。

[4] このうちの 800 行は電子財布と共通

5 まとめと課題

本稿では従来あまり取り上げられることのなかった、EC におけるプリペイドカードやクーポン券的な使用を想定した決済方式の提案を行った。また、提案方式に基づくシステムを試作した結果についても述べた。

今後の課題として以下のようなものが考えられる。

1. **複数の決済方式を組み合わせて扱えるようなシステムの検討**
   今回は EC におけるプリペイドカードやクーポン券的な決済方式の提案を行ったが、今後は特定の決済方式だけが使われる、というわけではなくさまざまな手法が併用して使われていくはずである。現実世界でもクレジットカードや銀行振込みのような手段はあってもやはり現金での決済というのはなくなっているわけではないのでこの流れは妥当である。そのため、今後は EC において複数の決済方式が共存できるようなシステムの architecture を考えていきたいと考えている。
2. **適用実験**
   今回、試作したシステムを実際のサービスに適用して実験を行い、運用コストなどについて評価を行っていく予定である。

謝辞

本研究の機会と有益な御助言をいただいた NTT ソフトウェア研究所サービスソフトウェア方式研究グループおよび第一プロジェクトチームのみなさまに深謝いたします。また、システムの試作においては NTT ソフトウェア (株) の小畑氏、北見氏に多大なご尽力をいただきました。重ねて深謝いたします。

参考文献

[1] 藤崎, 岡本: “エスクロー電子現金方式”, 信学技報 SST95-112, pp. 7-12, 1996.

[2] David Chaum: “Achieving electoronic privacy”, In *Scientific American*, pp. 96-101, 1992.

[3] Marvin Sirbu and J. D. Tygar: “NetBill: An Internet Commerce System Optimized for Network Delivered Services”, In *Proc. of IEEE Compcon'95*, 1995, ftp:// www.ini.cmu.edu/ netbill/ CompCon.html.