# 電子決済システムの構築に関する検討*

寺内 敦、森保 健治、三宅 延久、明石 修†

NTT ソフトウェア研究所‡

terauchi@slab.ntt.jp

**概要**

ネットワークを用いた商取引である電子商取引 (EC : Electronic Commerce) への注目が高まっており研究開発が盛んに行われている。中でも電子決済に関しては従来より電子現金などの多くの方式が提案されており、すでに実用化も始まっている。
今後のECの発展を考えると商品の販売方法や決済方式が多様になってくることが予想される。そのため今後の電子決済システムは、商品の販売方法に依存しないことや新たな電子決済方式の追加が容易に行えることなどシステムの拡張性が重要な要求条件になる。
筆者らも電子決済システムの1つとして電子プリペイドカードシステムを提案しており、現在システムの構築を行っている。本稿では、拡張性の高い電子決済システムの構築に関する検討結果をソフトウェアモジュールの構成法およびそれに伴うセキュリティの保護という観点から述べる。

## 1 はじめに

ネットワークを用いた商取引である電子商取引 (以下、EC : Electronic Commerce) への注目が高まっている。電子商取引を実現するための諸技術に関する研究開発が盛んに行われており、また、技術だけでなく法律の整備などの制度面でも電子商取引の実現に向けた動きが活発になってきている。

電子商取引を実現するための中核技術の1つである電子決済に関しては、従来より電子現金などの多くの方式が提案されており、いくつかの方式では実用化も始まっている。しかし、現在、実際に稼働している電子決済システムは単一の決済方式のみをサポートしているだけである。これは多くの方式が現状では実用化の前の実験フェーズであることを考えると妥当なことであるが、このように多くの電子決済方式が提案され、それらを受け入れるNetwork上の商店が増加してきている現状を考慮すると、今後は電子決済システムに対して従来のような単一の決済方式だけではなくて、さまざまな決済方式が使える、など将来的な機能拡張も容易にできるような構造が要求されていくであろう。その要求を満たすためには、まず各決済方式を処理するためのソフトウェアがモジュール化されており、通信処理のような共通部分やアプリケーションから独立していることは必須の要件と言える。また、言うまでもなく決済方式のモジュール化を行っても、セキュリティは十分に守られていなければならない。

筆者らも電子決済システムの1つとして電子プリペイドカードシステムを提案しており、現在システムの構築を行っている。本稿ではその試作から得られた電子決済システムの構築に関する検討結果を、特に決済ソフトウェアのモジュール化およびそれに伴うセキュリティの保護という観点から報告する。

## 2 電子決済

### 2.1 従来方式

従来提案されてきた電子決済方式は以下のように大きく3つのカテゴリに分類することが可能である。

*A study on software architecture for Electronic Payment Systems

†Atsushi TERAUCHI, Kenji MORIYASU, Nobuhisa MIYAKE, Osamu AKASHI

‡NTT Software Laboratories

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],CheckFree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。各方式の位置付けを示したものを図1に示す。

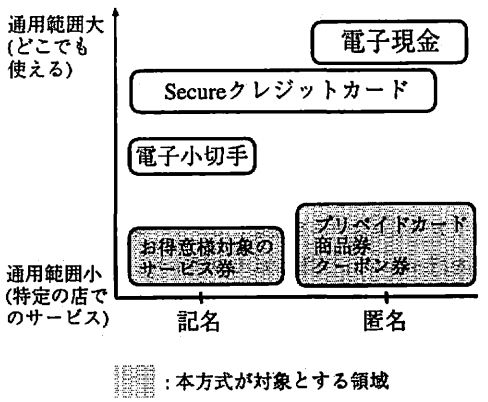


図1: 電子決済方式

図1における分類軸は以下の通り。

1. 匿名性
   匿名性の有無はプライバシの保護や犯罪発生時の追跡の容易さなどに影響がある。

2. 通用範囲
   現金のような汎用的なものか特定の店でのサービスにすぎないのかなどその決済方式の適用分野に関係する。

## 2.2 電子プリペイドカード

### 2.2.1 概要

従来の電子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方式を提供することを目標にしてきたといえる。しかし、商店自身がサービスの一環として独自にプリペイドカードやクーポン券(以下、プリペイドカード)を発行したいという要求は現実の世界と同様、ECにおいても存在すると考えられる。また、Network上ではユーザ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店にとっては重要である。そのような囲い込みの1つとしてクーポン券などの発行はやはり効果がある。このようなサービスを実現するためには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。

以上の観点から我々は現実世界におけるプリペイドカードやクーポン券的に使うことを想定した電子決済方式を提案してきた(図1における網かけ領域)[4]。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。

### 2.2.2 モデル

提案方式で想定しているモデルを図2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。

- ユーザ
  センタにプリペイドカードを申し込み、このプ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)
  プ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

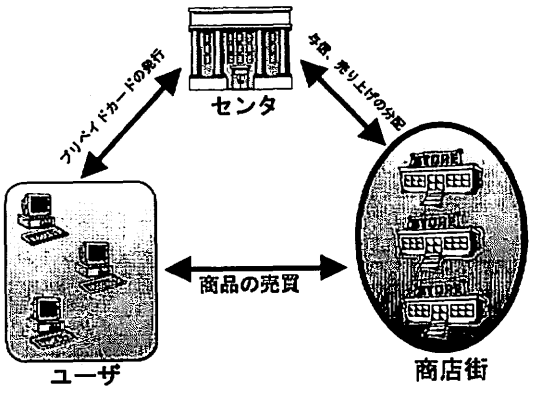


図 2: 電子プリペイドカードシステムのモデル

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、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
  ユーザに対してはプ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プ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。

#### 2.2.3 方式

提案している電子プリペイドカードシステムは、プリペイドカードに相当するデータをユーザ端末上に保存し、商品の購入により商品の価格をプリペイドカードの残高から減算することにより課金を行うシステムである。このようにユーザ端末上に価値のあるデータを保存する方式はユーザがオフライン、オンラインにかかわらず任意の時点で残高を確認でき、サーバの負荷も減らせる利点がある。

また、商取引形態として本稿では[5]や[6]などに提案されているような情報流通システムを想定する。これらのシステムではディジタル情報を商品とし、商品は予め暗号化された状態で安価あるいは無料で配布される。そして、ユーザがその情報を利用するときに始めて情報が有効になる、すなわち、復号鍵を取得して復号化される。このとき、同時に当該情報の代金が課金される。

次に、本プリペイドカードシステムを用いて商品を購入する手順を示す。ここで、プリペイドカードはあらかじめユーザの端末上に保存されているものとする。

1. ユーザは商店に対して購入申込を行う。このメッセージには価格などの購入する商品の情報や支払に用いるプリペイドカードなどが含まれている。
2. 商店は購入申込の内容をセンタに転送する。
3. センタではメッセージ中に含まれるプリペイドカードの情報を自分の持つDBの情報と比較してその結果を商店に返送する。また、トランザクションを承認したことを示すメッセージも商店に返送する。
4. 商店はセンタからの返答および商品の暗号を解くための鍵をユーザに送る。
5. ユーザはセンタの返答および商品の鍵を受信すると、商品の復号化を行い、プリペイドカードの残高から商品の価格を減算する。

## 3 要求条件

今までに電子決済方式は多く提案されてきており、それぞれに適した商品や販売形態がある。このように多くの電子決済方式が提案され、それらを受け入れるNetwork上の商店が増加してきている現状を考慮すると、今後、一人のユーザが状況に応じて複数の決済方式を自由に選択、利用したいという要求が生じてくる。このように、電子決済システムにおいても今後は機能拡張の容易さが重要な要求条件となっていくと思われる。

そのような要求の実現に向けては、まず個々の決済方式を処理するためのソフトウェアが、アプリケーションや通信処理などから独立した状態でモジュール化されていることが必須である。同時に、そのライブラリのAPIがサービスに非依存な形で提供されていなければならない。

一方、電子決済システムにおいては購入者の個人情報や決済に必要な情報が電子的なデータとしてNetworkをやりとりされるため、盗聴や改竄などの攻撃に対する十分な対処が必要であることは言うまでもない。このセキュリティの観点から電子決済システムのモジュール化について考えると、決済に関する重要な情報が商店以外には直接操作できないようにモジュール化されていることが必要である。電子プリペイドカードシステムの場合では「決済に関する重要な情報」とは(I)電子プリペイドカード、(II)商品価格の二つである。

この二つの情報に対して攻撃が行われる箇所および攻撃内容の組は以下のようになる。

(i) 通信路 …二つのデータともネットワーク上をやりとりされるので盗聴、改竄などの攻撃を受ける可能性がある。これに対しては本システムでは暗号化、ディジタル署名の付加によって対処している。

(ii) ユーザ端末 …ユーザのプリペイドカードは端末上に保存されているので改竄の恐れがある。また、課金プログラムの解析により実際の商品価格やプリペイドカードを改竄されることがある。

(iii) 商店 …提案システムでは、購入時のやりとりにおいてユーザとセンタの間に必ず商店が介在する。そのため、商店がユーザからの購入申込を受信したときにメッセージ中の価格を(与信の前に)改竄してユーザの知る価格とは違う額で与信を受け、トランザクションを実行するという攻撃がありうる。また、商店がユーザからの購入申込メッセージを録音しておき、後日そのメッセージだけを用いてセンタに与信を行い自分の売上を増やすという攻撃も想定される。

(iv) センタ …信頼できるという仮定のため、攻撃はないものとする

以上より電子プリペイドカードシステムの構築における要求条件をまとめると以下のようになる。

要求条件1：モジュール性 それぞれの電子決済を処理するソフトウェアがアプリケーションや通信処理などから独立した形でモジュール化されていること

要求条件2：安全性 要求条件1を満たした上で、セキュリティが十分に守られていること。具体的には以下の2つの情報が防御できていることとする。

1. 電子プリペイドカード
2. 価格

## 4 試作システムの概要

筆者らが試作した電子プリペイドカードシステムの構成図を図3に示す。ユーザのWWWクライアントおよび商店のWWWサーバ以外の全モジュールが試作した範囲である。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。

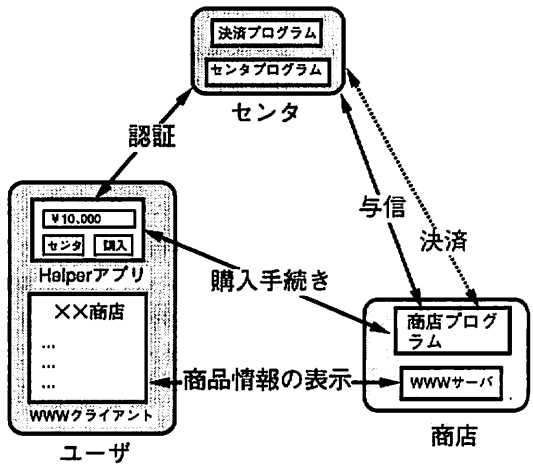


図3: システム構成図

ユーザ端末上で通信処理、課金処理などを行う専用ソフトウェア「電子財布」はWWWクライアントのHelperアプリケーションとして動作する。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修正なしに使用できる。

## 5 要求条件の実現

第3章において電子プリペイドカードシステムに対する要求をまとめた。本章ではそれぞれの要求条件の実現方法について述べる。

### 5.1 モジュール構成

電子プリペイドカードシステムに必要な処理はおおよそ以下の通りである。

- ユーザ側
  - 商品購入処理
  - 課金処理
- 商店側
  - 商品購入処理
  - 与信処理
  - DB 処理
- センタ側
  - プリペイドカード販売処理
  - 与信処理
  - DB 処理

上記の処理を AP および通信ライブラリから独立させた形にすると、ソフトウェアのアーキテクチャは図4のようになる。

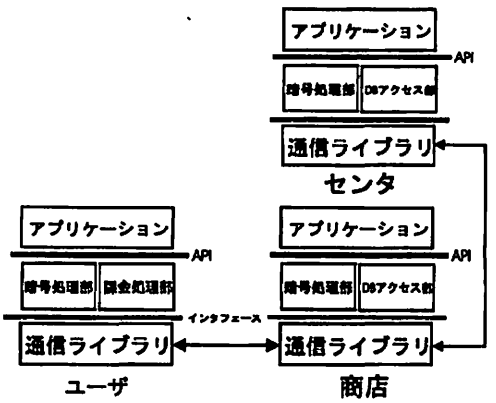


図 4: ソフトウェアアーキテクチャ

図中において「課金処理部」とは電子プリペイドカードの処理 (更新、照会) に関する処理のみを行う部分で、「暗号処理部」とはメッセージの暗号、復号化や署名の付加、および商品の復号化など暗号に関わる処理をすべて行う。また、「DB アクセス処理」は購入履歴の保存など DB アクセスに関する処理を行う部分である。「通信ライブラリ」は WinSock.dll などの汎用的な通信ライブラリを指す。

### 5.2 安全性

#### 5.2.1 プリペイドカードの防御

プリペイドカードは一旦購入された後は常にユーザの端末上に存在するので、最低限、暗号化した状態で保存するという対処は講じなければならない。また、利用時にはプリペイドカードを復号化しなければならないが、この復号化も必ずメモリ上のみで行い、HD 上には絶対に復号化ファイルを生成しないことも必要である。

この暗号化に用いる共通鍵は利用者のパスワードを利用して生成する。鍵を利用者 (のみ) が知っているデータにすることで、利用時に入力させることが可能になる。鍵を利用者の知らない、例えばセンタの生成したものなどにすると、鍵の管理方法として (1) ユーザ端末上に保存する、(2) センタが管理しておき利用時に問い合わせる、(3) プログラム中に埋め込んで配布する、といった方法を取らなければならない。しかし、これらの方法は (1)、(2) の場合は鍵が盗難される恐れがある、オフラインでの利用ができないなどの問題があるし、(3) の場合は配布の手間が非常に掛かるというデメリットがある。そのため、鍵を利用者の知っているパスワードなどのデータにして、利用時に入力する方式は合理的であると言える。

ただし、上記の方法は利用者に悪意のない場合、すなわち、第三者の攻撃に対しては効果があるが、利用者自身が悪意を持っている場合は共通鍵は自明であるため、暗号アルゴリズムも公開であればプリペイドカードを復号化することが可能であるという問題がある。提案する電子プリペイドカードシステムではこの問題を解決するために、センタの DB にも各プリペイドカードの残高を管理しておき、購入トランザクション中に照会を掛けることにしている。そのため、悪意のある利用者が自分のプリペイドカードの残高を改竄するなどの悪事を行っても購入時には必ず発覚する。

この他、プログラム解析によりプリペイドカードを間接的に改竄される可能性があるが、そのような攻撃に対する防御は次章で述べる。

#### 5.2.2 「価格」の防御

次に、商店およびユーザから価格などの情報を隠蔽する方法について述べる。今回のように課金処理をユーザ端末上で行うような場合では、ユーザに悪意があれば、自分の端末上の課金プログラムやプリペイドカードをオ

フラインで解析することができる。1つのモジュール内部で処理されるデータについては盗聴や改竄をされる恐れはないと考えられるので、問題になるのは決済モジュールとAPおよび通信ライブラリ間のインタフェースである。つまり、重要な情報がAPIに露出していると、適当なプログラムを作成してデータを盗まれたり操作される可能性がある。これに対する防御として、本システムでは「重要なデータをAPIに露出させるときは暗号化した状態で渡す」という方針で設計を行った。

図4のアーキテクチャを用いて提案システムにおいて価格がどういう経路でやりとりされているかを説明し、要求が満たされていることを示す。

価格などの商品情報の流れは図5、図6のようになる。図5に示すのが、ユーザからセンタまでまでの流れ、図6に示すのが、センタからユーザまでの流れである。

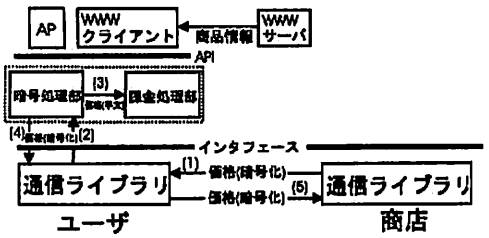


図5: 「価格」の流れ(その1)

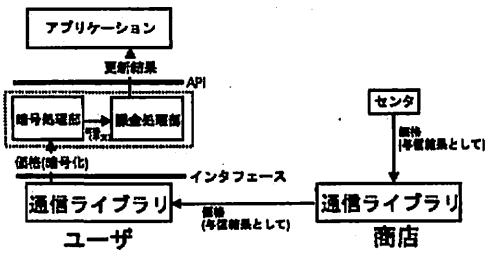


図6: 「価格」の流れ(その2)

1. ユーザが購入を決定する前に商店から商品の価格や商品IDなどの情報(商品情報とよぶ)がユーザに送られている必要がある。この商品情報も暗号化した状態で転送し、ユーザや第三者に改竄されないようにしておかねばならない。このときの暗号鍵はユーザにも第三者にも知ることができないことが必要であるので、ユーザの暗号処理部で暗号鍵(セッション鍵)を1つ生成して、その鍵を用いることにする。生成したセッション鍵をDiffie-Hellman方式などの鍵共有方式[7]を用いてあらかじめ商店と共有しておけば秘密通信ができる。セッション鍵自身はモジュール内部で生成されるのでユーザにも第三者にも知られることはない。また、商品情報は暗号化されたままの状態でモジュールに渡されるため、インタフェースを平文の状態で渡ることはない。

2. 暗号処理部では商品情報を復号化して「価格」を取り出す。まず、この「価格」を利用中の電子プリペイドカードの現在の残高と比較する。そのため、取り出した「価格」を課金処理部に渡す必要があるが、問題になるのは暗号方式および鍵を何にするかである。課金処理部は前述のように課金のみを行うモジュールなのでプリペイドカードに関する処理以外を含めるのは望ましくない。その場合、暗号方式も鍵もプリペイドカードの処理と同一のものにする必要があるが、課金処理部と暗号処理部とが独立にならない。そのため、暗号処理部と課金処理部はAPからは1つのモジュールとして見えるようにし、APIもそのように定義した。ただし、内部的には図に示すように2つのモジュールになっている。課金処理部での比較の結果、残高が足りていれば暗号処理部が処理を続行し、残高が足りなければ処理を終了する。

3. 暗号処理部では、プリペイドカードやメッセージへの署名の付加、メッセージの暗号化、などの処理をして商店に送る購入申込メッセージを作成する。このメッセージ中には価格も含まれている。

4. 購入申込メッセージのうち、価格やプリペイドカードなどの情報はユーザによる署名のうえセンタの公開鍵で暗号化する。そのため、仲介者の商店も盗聴、改竄はできない。[1]商店ではこれらの情報をそのままセンタに転送して与信を依頼する。

5. センタでは転送された情報をDBと比較して与信を行い、その結果を商店に返送する。また、転送されたメッセージの内容に対して署名を付加した

[1]さらに、商店のソフトウェアにおいてはメッセージを直接操作するようなAPIは提供していない。

ものも返送する。これにより、ユーザ自身が自分の起こしたトランザクションがセンタに承認されたこと、および商店によりトランザクションの内容が改竄されていないこと、を知ることができる。

6. 商店では与信の結果および商品を解く鍵をユーザに送信する。このときにも、センタからの与信の結果には署名が付加されているので商店が改竄することはできない。

7. 与信結果を受信したユーザの暗号処理部では署名の検証や商品の復号化などを行う。メッセージは暗号処理部に渡されるときはやはり暗号化されているので盗聴、改竄の心配はない。復号化まで成功した場合は暗号処理部から価格が渡され課金処理部によりプリペイドカードの残高更新が行われる。

上記より、提案するソフトウェアアーキテクチャは価格やプリペイドカードなどの重要な情報はAPおよび通信ライブラリとのインタフェースに露出することはないのでユーザ端末上や商店でのプログラム解析に対しても強固である。また、メッセージを仲介する商店が、ユーザおよびセンタからのメッセージを盗聴、改竄することもできないのでトランザクションの実行も安全に行える。

### 5.3 API

5.1章、5.2章の検討結果を反映して、電子プリペイドカードシステムでは以下のAPIを提供している(決済に関するもののみ)。

**ユーザ**

1. 商品を購入する(決済方法はパラメータにより指定)
2. 商品情報を取得する
3. 利用中のプリペイドカードの残高照会を行う

**商店**

1. 与信を依頼する
2. 購入履歴を保存する

**センタ**

- 与信を行う
- 購入履歴を保存する

これらのAPIを用いた試作システムを運用した結果、決済に関するAPIとしては上記のものだけで不足はなかった[2]。また、上記のAPIは特定のサービス、販売形式に依存するものではないので、今回想定したような情報の販売だけでなくInternetを用いた物品販売などにも広く使えると考えている。

### 5.4 結論

以上のようにソフトウェアモジュールおよびAPIを構成すれば、悪意をもった攻撃者の攻撃に対して強固で拡張性の高い電子決済システムが構成できる。また、特定の商品や販売形式にも依存することもないので適用範囲も広い。ただし、一般にはソフトウェアだけで構成したシステムで完全にセキュリティを守ることは不可能であると言われており、本システムも例外ではない。しかし、本稿で示した方針に従った決済モジュール、すなわち暗号処理部および課金処理部をTamper-freeなハードウェア化すれば、より安全なシステムが構築可能であると思われる。

## 6 まとめと課題

本稿では筆者らが提案してきた電子プリペイドカードシステムの試作結果から、拡張性および安全性の高い電子決済システムの構築に関する検討結果について述べた。

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**
   本稿では電子決済システムをモジュール化する際の方針について報告を行った。複数の決済方式を使うときには、決済方式のライブラリ化に加え、各方式におけるプロトコルなどの違いを吸収する仕組、1つの決済方式がうまくいかなかった場合にトランザクション全体をキャンセルする機構など検討すべき課題は多く残されている。これらの課題について今後検討していく予定である。

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

[2] クレジットカードのように端末で課金を行わない場合は残高照会のAPIは不要である。

して実験を行い、APIの十分性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.

[4] 寺内他: "電子決済システムの実装と評価", マルチメディア通信と分散処理研究会, Vol. 96-DPS-76, pp. 97-102, 1996.

[5] 金井他: "マルチメディア情報流通システム (InfoKet)", マルチメディア通信と分散処理研究会, Vol. 70-6, pp. 31-37, 1995.

[6] 明石他: "FleaMarket方式による情報流通システムの実装", マルチメディア通信と分散処理研究会, Vol. 96-DPS-76, pp. 103-108, 1996.

[7] 岡本栄司, 「暗号理論入門」共立出版, 1993.