ICカードを用いたマイクロペイメントシステムの試作

5M－1

坂田 祐司、奈須 善幸、萩原 和典、服部 昇
ＮＴＴデータ通信(株)

１．はじめに

現在、インターネット上でデジタルコンテンツを販売するビジネスがたちあがりつつある。

例えばWWW上の情報に対しクリックごとの支払が可能に成るとユーザー及び販売する店舗にとって有利な点は多い。そこでこのような状況で想定される少額で高頻度の支払に対応した方式が必要とされる。

インターネット上の決済方法としてクレジット決済や銀行口座からの即時引き落としなどをベースとした方式が提案されている。インターネットを通じてのクレジット決済や口座の資金移動依頼はセキュリティの問題から本人のＩＣカードによる電子署名が必要に成る。

このような方式はクレジットカードや銀行カードの IC カード化とともに主流の決済方式に成ると予想されるが、決済ごとにかかる処理コストと処理時間を考慮すると上記のような一般にマイクロペイメントの分野といわれるデジタルコンテンツのコンテンツごとの支払には向いていない。

こうした背景をもとに IC カードを用いた決済システムのサブセットとしてのマイクロペイメントシステムを検討し試作した。

２．システム要件

前章で述べたようにシステムとして以下のような要件を満たす必要がある。

処理コストの抑制

商品の金額が少額であるためその処理コストはそれ以上に少額である必要がある。

処理の高速化

WWWなどでクリックごとに支払を行なう場合などにおいて一回の支払のたびに処理に時間がかかる事はユーザーの利便性を低下させる。

また、一回の決済金額が少額であるためコンテンツを提供する店舗は大量のトランザクションが発生しないと採算が取れない。よって単位時間あたりの決済処理回数は可能な限り多くする必要がある。

３．システム概要

本システムの構成は図１の通りのクライアント、決済サーバー、店舗サーバーの三者モデルである。クライアントはサービスを受けるユーザーでありＩＣカードリーダライタを搭載したＰＣを所有しているとする。

店舗サーバーはデジタルコンテンツを提供する店舗に存在するサーバーである。決済サーバーはユーザーと店舗間の実資金のやり取りが可能な第三者機関に存在する。この機関はユーザーと店舗の仮想口座を保持しており仮想口座のバランスは何らかの方法で定期的に該ユーザー、店舗の銀行の実口座に反映されるものとする。

また、ユーザーは電子署名の可能なＩＣカードを持っており、これはユーザーの口座に関わる資金移動の際の認め印としても用いられるものとする。

決済方式はプリペイド方式でありユーザーはある店舗のコンテンツを購入したい場合、以下のような手順をとる。

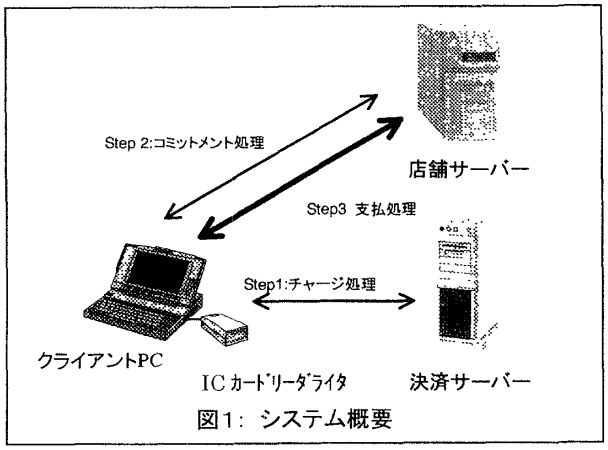

図1：システム概要

A prototype of a micropayment system using a smart card

Yuji Sakata , Yoshiyuki Nasu
Katsunori Hagiwara , Noboru Hattori
NTT Data Corporation
3-3-3, Toyosu , Koto-ku , Tokyo Japan

<Step1:チャージ処理>
ユーザーは決済サーバーにアクセスし、利用したい店舗に対するプリペイド情報を購入するため、決済サーバーに利用したい店舗ＩＤ、プリペイドしたい金額などのメッセージに対して IC カードを用いて電子署名を付し決済サーバーに送信する。

決済サーバーはユーザーから送信されたメッセージの電子署名の正当性を確認した上で、その内容に基づき決済サーバー内のユーザの仮想口座から店舗の仮想口座にプリペイド分を移動する。同時に支払証明書にあたるユーザー名、プリペイド金額や二重使用を防止するためのシリアル番号などのメッセージに決済サーバー機関の電子署名を付し、ユーザーに送信する。

<Step2：コミットメント処理>
ユーザーは次に店舗サーバーにアクセスする。プリペイドの残高管理には Rivest の PayWord [RS96]を応用したものを用いる。これはハッシュ関数の一方向性を利用したものである。
まず、ユーザーは店舗サーバに決済サーバーから受信した支払証明書と基底ハッシュの値を含むデータに対して IC カードによって電子署名を行ない送信する。

店舗サーバーではその支払証明書の正当性を決済サーバー機関の電子署名、ユーザーの電子署名から確認し、そのユーザーが使用出来るプリペイド残高と基底ハッシュ値を登録する。そして登録したことをユーザーに通知する。
これでユーザーは支払処理に移ることが出来る。

<Step3:コンテンツの購入/支払処理>
ユーザーは店舗のコンテンツを購入するためそのコンテンツの金額と支払度数を表すハッシュ値を店舗サーバーに送信する。
店舗サーバーは送信されたハッシュ値の正当性を確認した上でコンテンツをユーザーに送信する。
この支払処理をユーザーはチャージした金額まで行なう事が出来る。

4．システムの特徴

処理速度
[RS96]の論文にあるように方式的に公開鍵暗号方式による電子署名にかかる時間が処理速度に関して重要であると考えられる。特に電子署名を IC カードで行なう際には実装の面からも大きな問題に成る。
今回 512bit の RSA による電子署名が可能な IC カードを用いたがその処理の遅さは十分ユーザーが体感できるものであった。このため電子署名をプリペイド情報を使い始めるときのみに使用する事とした。使用度数の正当性の確認にハッシュ関数を用いて処理を高速化する方式は特に IC カードを電子署名に用いる場合に優れていると考えられる。

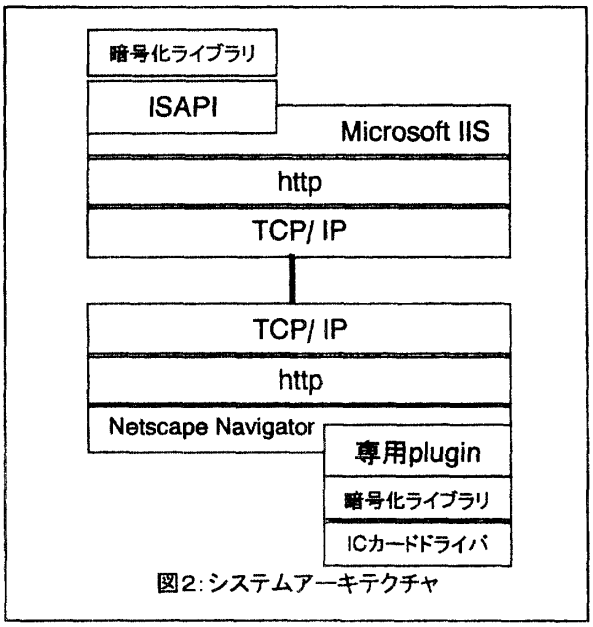

図2:システムアーキテクチャ

5．システムのアーキテクチャ

図 2 のようにプロトコルは http 上で実装している。そのためユーザーは WWW ブラウザ上ですべての処理が行なえ、また店舗は URL であらわせるコンテンツはすべて商品とすることが可能である。

6．まとめ

・ IC カードを用いたマイクロペイメントシステムを検討した。プリペイド方式としてチャージ処理時にのみ IC カードを用いることによって実際のコンテンツ購入時の処理速度を向上させた。
・検討に基づきシステムを試作し、本方式の動作を確認した。

Reference

[RS96] PayWord and MicroMint - Two Simple Micropayment Schemes by *R.L. Rivest and A.Shamir*