8ZA-4

ネットワーク型電子マネーにおける譲渡方法の提案とその評価

小森 旭　梅澤 健太郎　奥乃 博
東京理科大学 理工学部 情報科学科

電子商取引 (EC : Electronic Commerce) を普及させるには，便利で安全な電子決済技術が必要不可欠である．本稿では，電子決済方法の一つである電子マネーについて，鍵とお金の関係を明確にするため，公開鍵基盤 (PKI : Public Key Infrastructure) と呼ばれるインフラを利用して実装を行った．さらに，システム構築の際，電子マネーの転々流通性をソフトウェアのみで実現し，効率性・安全性について定量的・定性的評価を行った．

1. 電子マネーとセキュリティ

1.1 電子マネーの分類

既存の電子マネーはその形態により表1のように分類することができる．[1)2)]

表1 電子マネーの分類

システムの構成	IC カード型	格納形態	残高管理型
	ネットワーク型		**電子紙幣型**
システムの運用形態	クローズド・ループ型	価値の保管場所	サーバ管理型
	オープン・ループ型		**端末管理型**

これらの分類を基に，利便性や匿名性をどの程度許すかによって，さまざまな電子マネー方式が考案されている．

1.2 従来の方式の問題点と解決策

我々は，より現実のお金に近い形態を目指すため，表1のゴシック体で示された形態を選択した．従来の電子マネー実現方式[3)] の多くは，公開鍵に対してデジタル署名を施すことにより，鍵自身にお金の価値を持たせるという方式であった．しかし，この方法だと，

- 秘密鍵の漏洩による公開鍵の廃棄と電子マネーの失効
- 公開鍵自身の有効期限

といった問題が考えられる．つまり，公開鍵の廃棄・失効と電子マネーの失効との整合性がとりにくい．よって，我々は単なる公開鍵ではなく PKI に基づく X.509 証明書を用いることで，この問題の解決を図る．PKI では，公開鍵の廃棄・失効などに関して，例えば CRL (Certificate Revocation List) という形で対策を考えており，これを利用すれば証明書の廃棄と電子マネーの失効を関連付けられ都合が良い．また，X.509 証明書の中には有効期限が含まれているので，公開鍵自身の有効期限も即座に確認できる．

1.3 PKI (Public Key Infrastructure)

公開鍵暗号方式を用いる場合，入手した公開鍵が確かに通信相手のものであることを確認できなくてはならない．PKI では CA (Certification Authority) と呼ばれる信頼できる第三者機関 (TTP : Trusted Third Party) を導入することで，主体者の名前と公開鍵の対応を公開鍵証明書により保証してくれる．一般に証明書は主体者の名前を一意に識別できる仕組みになっているが，名前の部分にニックネームなどを用いることで，証明書に匿名性を持たせることも可能である．

2. 提案する電子マネー方式の概要

2.1 ソフトウェアだけによる実装方法

我々は，匿名性を持った (ローカルな) 公開鍵証明書を用いることでプライバシーを確保した電子マネー方式を提案する．この方式は 1996 年 9 月に発表された NTT 電子マネーをベースにし，主に文献[4)] を参考にした．システムを構築する際，IC カード等の耐タンパ性のある機器を用いると，コストがかかるといった欠点がある．そこで我々は，耐タンパ性に頼ることなくソフトウェアだけでの実装を試みた．その上で，発生し得る不正のリスクを分析・評価し，総合的な安全性を確保した電子マネーを実現するためには，さらにどのような要素技術を追加する必要があるかといった検討を 4.2 節で行う．利用者登録プロトコルを図1に，引出しプロトコルを図2に示す．

2.2 電子マネーの譲渡

電子マネーの利便性を満たすには，転々流通性を確保することにより，譲渡を可能にする必要がある．一般に電子マネーの譲渡というと，額面金額そのままか分割した一部を他者に譲ることを意味する．しかし，そうすると必然的に電子マネーの端数がたまってしまい，端数をどのように譲渡するかが問題となる．そこで我々は，新たに電子マネーの統合を行う TTP を設け，統合も可能な譲渡プロセスを導入した (図4)．転々流通性の実現は，従来の方式では電子マネーへの裏書きの付加 (署名の連鎖) であったが，我々は領収書という譲渡が行われた証明書を電子マネーに付加する方法を採った (図3)．この結果，X509 に基づいた PKI だけでなく，SPKI (Simple PKI) などにも応用することができる．また，転々流通性を確保したり新たに TTP を設けることは，利便性向上のみならず，従来からの問題点である発行機関 (IA) の負荷を減らすことにも役立つ．

Proposal and Evaluation of Transfer Method in Network Type Electronic Money
by Akira Komori, Kentaro Umesawa, Hiroshi G. Okuno
Department of Information Sciences, Science University of Tokyo

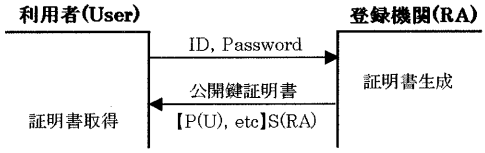

図 1 利用者登録プロトコル

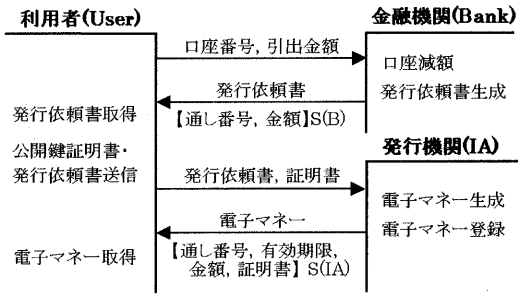

図 2 引出しプロトコル

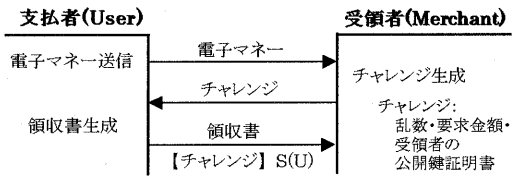

図 3 支払い（分割譲渡）プロトコル

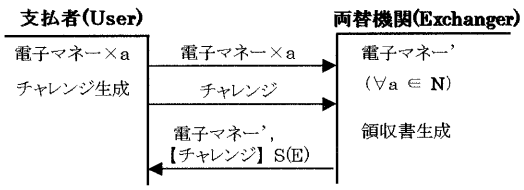

図 4 統合プロトコル

（図で使用している記号の意味）

P(X)：X の公開鍵
S(X)：X の秘密鍵
【A】S(X)：X の秘密鍵でデータ A を暗号化（電子署名）

3. 実　　装

以上の理論に基づき，簡易な電子マネーシステムをクライアント/サーバシステムとして実装した．言語は Java (**JDK1.2**, **IAIK-JCE2.61**[5], **IAIK-iSaSiLk3.02**[5]) を用いて作成した．各エンティティ間は，通信の盗聴・改ざん・なりすましといった不正を防止するため，SSL を用いてセキュアチャネルを確保した．

4. 評　　価

4.1 定量的評価 — トラフィックの測定

表 2 ネットワークパフォーマンスの測定結果

	送信量	受信量	処理時間（含転送）
SSL セッション確立	481byte	18byte	3510 ～ 3790msec
発行依頼書発行	224byte	0byte	330 ～ 550msec
証明書発行	505byte	0byte	330 ～ 440msec
電子マネー発行	950byte	0byte	330 ～ 440msec
発行依頼書検証	6byte	241byte	380 ～ 490msec
証明書検証	6byte	505byte	270 ～ 280msec
電子マネー検証	6byte	962byte	440 ～ 550msec
チャレンジ生成	517byte	0byte	170 ～ 270msec
領収書検証	9byte	875byte	710 ～ 780msec

	OS	CPU	メモリ
クライアント	Windows98	433MHz	128MB
サーバ	WindowsNT	600MHz	128MB

上記の実験環境上で，図 1 から図 4 の各手順における，アプリケーション層レベルで測定したデータ転送量と処理時間を表 2 に示す．送受信量はサーバ側から見たデータ量を表し，時間はクライアント側から見たレスポンスタイムを表す．測定の結果，電子マネーや領収書の検証に時間がかかるが，譲渡を可能にしたり他の TTP を設けたりすることにより IA の負荷が分散できるので，スループットへの影響は極めて少ないと思われる．より詳細な解析のためには，電子マネーの発行・更新・検証といったすべての処理を IA が行う中央管理型によるサーバ負荷と，我々が提案する方法によるサーバ負荷について，待ち行列モデルによる理論的な解析と実測をする必要がある．

4.2 定性的評価 — 電子マネーの具備すべき要件

本電子マネー実現方式の評価を表 3 にまとめる．

表 3 本電子マネー実現方式の評価（文献 4，p85 の表 1 を修正）

要件		本方式での対処
安全性	事前対策	やり逃げ型の犯罪を防止することができない
	事後対策	不正行為者の追跡が可能
電子マネー特有の利便性	分割利用可能	支払時のデジタル署名の中に支払金額を入れることで任意分割を実現
	店頭・ネットワーク支払い	ネットワーク経由での支払いのみ実現
	効率的な発行・管理	転々流通性を確保することで，発行機関の負荷を軽減することが可能
現金が持つ利点の継承	追跡不能性	登録機関を設置することで実現可能
	関連づけ不能性	電子マネー引出しごとに異なる公開鍵証明書を使用すれば実現可能
	オフライン性	サービス停止攻撃等を受け，発行機関がダウンしていても，当事者間で一時的な譲渡が可能
	転々流通性	譲渡をする場合，手元に電子マネーのコピーを保持することが可能なので，あまり好ましくない
	携帯性	ネットワークでの支払いを目的としているので携帯性はない
	複数金融機関対応	発行機関が電子マネーを発行することで，複数金融機関で同一の電子マネーを取り扱い可能とした

この表が示すように，電子マネーをソフトウェアのみで構成した場合，いくつかの欠点が生じる．したがって，欠点となる部分については，電子マネーの格納に IC カード等の耐タンパ性のある機器を用いることで，さらに安全性を高めることができる．もちろん，IC カード等を使用するか否かは，要求されるセキュリティレベルやコストとの兼ね合いになる．

5. おわりに

本稿では，PKI と電子マネーの整合性について検討した．我々が提案する方式は，PKI をベースに構築されようとしている電子政府のサービスにも適応可能と考えられる．

参 考 文 献

1) 須藤 修, 後藤玲子: 電子マネー, 筑摩書房, 1998.
2) 松本隆明, 岡本龍明: 情報セキュリティ技術, オーム社, Aug. 2000.
3) 岡本栄司, 満保雅浩: 電子マネー, 岩波書店, 1997.
4) 中山靖司, 森畠秀実, 阿部正幸, 藤崎英一郎:電子マネーの一実現方法について, 日本銀行金融研究所, Jun.1997.
5) http://jcewww.iaik.tu-graz.ac.at