関連づけ可能なオフライン方式
匿名電子マネーの提案

小出 篤史

2000 年 2 月 15 日

キーワード： 電子マネー，オフライン方式，関連づけ，信頼できる第三者機関，部分ブラインド署名．

今日，インターネットをはじめとするオープン・ネットワークの普及により，電子商取引に対する期待が高まっている．

電子商取引を実現するための決済方法として，クレジットカード，インターネットバンキング，電子マネーなどさまざまなタイプのものがある．クレジットカード，インターネットバンキングは，従来から存在する決済方法をネットワークを通した手段によって実現するものと考えることができる．これに対し，電子マネーは，電子マネーデータそのものに価値が含まれているものとして考案されたものである．

今日では多くの電子マネー方式が提案されるようになり，我が国でも各地で実証実験が行われている．電子マネーは，店頭における対面販売では従来に比べ，支払い処理が煩雑になるほど，利用者にとって現金やクレジットカードにとって代わるような利便性は期待できない．しかしながら，インターネットを利用したコンテンツサービスが脚光をあびるなか，ネットワークにおける少額の決済手段として注目されている．

実証実験をはじめ，限定的な意味での実用化は進んでいるものの，本格的な実用化を進めるうえでは，運用上の不正対策や法改正をはじめ，まだまだ多くの課題が残っている．

次に，電子マネーが現金やクレジットカードと同様な決済手段として普及するには次のような要件を満たす必要がある．

完全情報化 電子マネーを構成する電子マネーデータそのものが現金に相当する価値をもつこと．これにより，ネットワークを通して，電子マネーを送ることができる．

安全性 価値の変造，偽造やコピーによる再利用など不正利用ができないこと．もっとも重要であるこの性質は，不正な行為自体が困難である事前対策，あるいは，事前対策が難しい場合には，たとえ不正行為が行われてたとしても，不正行為者を追跡することができるような事後対策の二面からの検討が必要である．

匿名性 利用者の購買に関するプライバシが，銀行や店が結託したとしても露見しないこと．

オフライン性 電子マネーが正当なものかどうかを支払い当事者以外に問い合わせる必要がないこと．

分割利用可能性 一度発行された電子マネーを，利用合計金額が額面の金額になるまで分割して使うことができること．

譲渡可能性 電子マネーの他人への譲渡が可能であること．

分割利用可能性，**譲渡可能性**は，電子マネーの利便性を考えるときに求められる付随的な性質である．本稿では最低限満たすべき要件として，**完全情報化**，**安全性**，**匿名性**，**オフライン性**を満たすシンプルな電子マネー方式を基本としてさまざまな検討を行う．

本稿ではまず，電子マネーとして必要とされる要件，電子マネーのおける技術的背景，電子マネーにおける研究の流れについて述べる．次に，現在効率的といわれている電子マネー方式において，金額情報を改ざんできる問題点を指摘する．その上で，**提案方式１**として金額情報改ざんできないように改良した方式を新たに提案する．

従来の電子マネー方式では発行機関である銀行は不正をはたらかないという前提があった．しかしながら，現実社会においては，顧客名簿を流出させるなどの行員個人による不祥事が多発しており，この前提は即していない．組織としての銀行は信用できるとしても，銀行に携わる行員の不正を考慮すべきと考える．宮崎らは，電子マネー方式における発行機関の不正として，預け入れ済みの支払い履歴から二重使用を捏造し，正当な利用者を不正使用者として仕立て上げ違約金を請求する不正，不正な行員と利用者が結託し利用証明書を偽造することで，収益をあげる不正についてとりあげ，対応策を示している．

本稿では，不正な行員と利用者が結託した場合の不正として，不正な行員が銀行の電子マネー発行に用いられる秘密鍵を不正な利用者に漏洩させる不正に注目する．対応策として，発行機関である銀行は，引き出しプロトコルにより発行した電子マネーデータにマネーＩＤを挿入し，預け入れプロトコルで還流したものとの関連づけを行うことが必要である．しかしながら，そのようなマネーＩＤを付加した場合に銀行はマネーＩＤを手がかりに，利用者の購買履歴などのプライバシ情報を入手できることになるため，匿名性が失われてしまうという問題点が指摘されていた．そこで，新たに信頼できる第三者機関を想定し，店は信頼できる第三者機関を通して銀行へ預け入れを行う．信頼できる第三者は銀行に対して，マネーＩＤに関係する情報のみを送り，他の利用者の匿名性を損なうような情報を送らないようにすることが必要である．

提案方式２では，信頼できる第三者機関を仮定することで，銀行は発行したものと還流したものの関連づけをとりつつ，利用者の匿名性を保証できるオフライン方式の電子マネー方式を提案する．