電子マネーのプロトコル研究の動向

竹村 彰通
A.Takemura@e.u-toyo.ac.jp
東京大学大学院経済学研究科

2000 年 2 月

Abstract

インターネットを情報基盤とするネットワーク社会にとって電子マネーは重要な役割を担うと期待されている. 一方で本来の意味での電子マネーの普及は, 必ずしも当初期待されていたほどに速いものとは言えないように思われる. その一つの原因は, 電子マネーのプロトコルとして種々多様なものが提案され, どのプロトコルが標準的なものとなるべきかが理論的な観点からもはっきりしないためであると思われる. ここでは現時点 (2000 年 2 月) での電子マネープロトコル研究の動向をサーベイすることによって, 電子マネーの現状と今後について考える[1].

1 導入

電子マネーはさまざまな期待を持って語られることが多い. 現在では銀行のキャッシュカードで現金をひきおろすことは日常茶飯事になっているし, 電車に乗る時にも自動改札機に対応したプリペイドカードを使えばいちいち現金で切符を買う必要がなく便利である. これから類推して考えれば汎用のプリペイドカードをイメージした「電子財布」 にもそれなりの現実感がある. 他方で, インターネットの急速な普及により, インターネットを通じた通信販売の場面で支払を安全かつ容易におこなうことが重要になっている. 特に音楽やソフトウェア等のデジタル情報そのものをインターネットを通じて直接販売するような場合には, 財の物理的な運搬は不要であるから, 支払のシステムの整備が本質的なものとして要求される. 現状ではインターネットを介した通信販売の際の支払はクレジットカードによるものがほとんどであるが, セキュリティーの観点からは 4 節でふれるように現状のクレジットカードの利用には問題が多い.

[1]電子マネー研究の分野の性格にてらして, 本サーベイは随時改定し, 著者のホームページ `http://www.e.u-tokyo.ac.jp/~takemura/em-survey.html` より新しい版にアクセスできる形にする予定である.

このような中で電子マネーは一種の理想的な支払手段として期待されるわけである. しかしながら, 電子財布的な電子マネー (「ストアド・バリュー型」[22]) とインターネット上の支払システムとしての電子マネー (「アクセス型」あるいは「ネットワーク型」) の二つを考えてみても, 両者はかなり性格を異にするものであり単一の電子マネーとは考えにくい面がある. 一方で貨幣の本質は一般受容性等の汎用性にあると考えられるから, 電子マネーの多くの方式が並立している状況は, 電子マネーが一般的な支払手段として用いられことに対する障害であるとも考えられる.

以上のような問題意識から最近の電子マネープロトコルの理論研究の動向をながめて見ると, 90 年代初頭に理論的に想定された単一かつ汎用的な電子マネーのプロトコル (例えば [38]) にかわって, 最近では場面に応じて必要な機能をプロトコルとして実現するより簡便な方式が多数提案されるようになって来ている. 特に匿名性の剥奪をどのように保証するかで様々な方式が考えられている (例えば [12]). 電子マネープロトコルの理論研究の成果は必ずしもただちに実際に実装されるわけではないから, 理論研究においてさまざまな方式が検討されている現状は, 実際面においても汎用的な電子マネーの普及がかなり先になることを意味するかもしれない. このサーベイでは以上のような観点から最近までの電子マネープロトコル研究の文献を概観していく. 本サーベイの対象は電子マネープロトコルの理論を扱った文献であり, 電子マネー実装の具体的なプロジェクトについては対象としていない. もっとも, 個々の文献でのプロトコルの詳細を紹介するわけではなく, あくまで研究の方向性を概観することが目的である.

以下の 2 節では議論の準備として, 電子マネープロトコルの文献において前提とされることの多い諸仮定について簡単にふれる. 3 節は本サーベイの中心的な節であり, 最近までの文献において電子マネーに要求されるさまざまな性質がどのようなプロトコルで実現されているかを概観している. 最後に 4 節で筆者の若干の感想をまじえて, いくつかの論点をあげる.

本サーベイの動機は, 筆者が推進している「電子社会と市場経済」のプロジェクトにとって電子マネーの問題が重要なテーマであり, 電子マネーの性格について正しい理解を持つ必要があると考えたためである. 「電子社会と市場経済」のプロジェクトでは電子マネーに関してすでに [20], [31] の成果を得ているが, これらは経済学の視点から電子マネーを論じたものであり, さらに電子マネーのプロトコルにさかのぼって電子マネーの性格を検討することも重要である. また電子マネーに関する日本語の概説的な文献 ([21], [34], [36], [49] 等) の記述も, 必ずしも最近の電子マネープロトコル研究の動向を反映しているとは言えないため, 本稿のような日本語での概説も意味があるものと考える. 筆者の専門は数理統計学であり, 本稿で扱う現代暗号理論等については専門家ではない. したがって以下の議論には専門的観点から見て不十分な点があるかも知れないが, 不十分な点については今後随時本稿を改定することによっておぎなっていくつもりである.

2　電子マネープロトコルの諸前提

この節では電子マネーのプロトコルの考察の際に前提とされている諸点を整理する. 電子マネーが一般的な支払い手段として広く用いられる状況ではここで述べる諸前提も変化せざるを得ないであろうが, 電子マネーのプロトコル自体の理論的な考察のためには前提条件を単純化し固定する必要がある.

• 銀行間の決済システム

電子マネーの文献では, 電子マネーシステムは既存の銀行間の決済システムの外側にあると想定されることが多い. 電子マネーの利用者 U は銀行 B に (要求払い) 預金口座を持っており, 預金からの引落しとひきかえに銀行から電子マネーを発行してもらう. 利用者 U が商店 M に電子マネーによる支払をおこなうと, 商店 M は銀行の自分の口座にこの電子マネーを預け入れる. 電子マネーの動きとしてはこのように $B \to U \to M \to B$ の形の流れが一サイクルをなす. $B \to U$ が電子マネーの**発行** (withdrawal), $U \to M$ が**支払い** (payment) , $M \to B$ が**預け入れ** (deposit) である. 電子マネーの文献では議論の簡単のために銀行 B を単一の銀行と考えている場合が多いが, 実際には U の口座のある銀行と M の口座のある銀行は異なる場合が多いから, M の預け入れの後, 銀行同士の決済がおこなわれると考える必要がある. すなわちここで銀行 B と書いているのは実際には銀行間の決済システムを一まとめにして考えていることになる.

電子マネーの利点の一つとして取引費用が低いことがあげられる. しかしながら, 電子マネーの移動にともない既存のシステムを用いた銀行間の決済が必要となれば, 取引費用の中に銀行間の決済費用も含めて考える必要がある. これは実際には電子マネーに対する手数料という形で銀行から商店に請求される場合が多いであろう.

電子マネーの技術は既存の銀行間のオンライン決済システムにも応用することができるから, 電子マネーを広義にとらえれば銀行間のオンライン決済システムを含んで理解すべきであるが, 電子マネーのプロトコルに関する文献では既存の銀行間の決済システムを前提とした上で, その外側に電子マネーのシステムを考えることが多いのが現状である.

• 公開鍵基盤

電子マネーの技術的基礎は公開鍵暗号の技術にあるが, 公開鍵暗号方式が広く使われるには一定の公的な性格を持つ認証局の存在などの基盤整備 (PKI, public key infrastructure) が前提である. 個人が本来の意味での電子マネーを扱うには, 個人が公開鍵と秘密鍵を保有し, 公開鍵が認証局によって保証されていることが必要である.

公開鍵暗号の技術はすでに確立されており, 大企業では今後公開鍵暗号の利用が促進されていくであろう. 企業や商店がインターネット上に仮想的な商店を開設するような場合には, それらの企業や商店の公開鍵がきちんと認証

されていることは重要である．しかしながらこの認証のためには消費者の側の公開鍵は不要であることに注意する必要がある．また, 消費者がブラウザを用いてインターネット上の商店にアクセスする際の安全な通信を確保するためにも, 現状のブラウザにもすでに実装され盛んに利用されているように, 商店側の公開鍵を用いるだけでよく, 消費者側の公開鍵は不要である．

秘密鍵の安全な保管にはコンピュータに関するある程度の知識が必要であることなどを考慮すると, 個人にまで公開鍵暗号基盤が整備されていくためには, 個人が公開鍵を保有することにそれなりのメリットのある状況になる必要がある．公開鍵方式に基づく電子マネーが他の支払手段に比べて大幅に有利な状況になれば個人が公開鍵を持つインセンティブになると思われるが, 一方公開鍵基盤が広く整備されていない状況では公開鍵方式に基づく電子マネーの有利性は発揮されないと思われるので, これはいわば鶏と卵の関係である．

• 使用済み電子マネーのデータベース

電子マネーはデジタル情報でありコピーすることが簡単であるために, 同じ電子マネーをコピーして用いるという二重使用の問題が発生する．多くの文献では二重使用を防止する方策として, 使用済みの電子マネーのリストを銀行のデータベースにたくわえ, このデータベースを参照することによって銀行が使用済みの電子マネーの受け入れを拒否するとしている．理論的にはこれでいいわけであるが, 実際にはこのデータベースがどのような形で管理可能かという問題があると思われる．すべての使用済みの電子マネーを永遠に蓄積して行くようなデータベースはやがて管理不能になってしまうであろうから, 例えば発行される電子マネーに有効期限を設け有効期限を過ぎた電子マネーについてはデータベースを参照することなく無効とする, などの処置が必要となる．しかしながら例えば日常的にも使い残しのプリペイドカードが多く見られるように, 有効期限内に使用されなかった電子マネーの処理の問題等が残る．

概念的には使用済み電子マネーのデータベースではなく使用可能な (すなわち発行されたがまだ未使用な) 電子マネーのデータベースを維持するほうが簡明であると思われるが, これには次節で述べる匿名性の問題などがからんでおり, 文献では使用済み電子マネーのデータベースを想定することが多い．この点についてはさらに次節の仮名口座の項でふれている．

• 二重使用に対するペナルティー

もし二重使用ができないというだけで二重使用に対するペナルティーがないならば, とりあえず二重使用をしてみようというインセンティブが働く．さらには大量の二重使用によりシステムを混乱させるような攻撃 (DoS, Denial of Service Attack) の可能性も生じる．これに対する通常の抑止策は, 二重使用の際に二重使用者の身元が判明するようにしておき, 使用者に対してペナルティーを課すという方法である．そしてペナルティーが十分大きければ二重使用が避けられるという考え方である．しかしながら, ここで使用者の身元とは何なのかという問題を考慮する必要がある．多くの文献では使用者自体と使

用者の銀行口座を区別して考えていない．つまり二重使用者の特定とは二重使用者の銀行口座の特定と同じことであると考えられている場合が多い．しかしながら, 時代と場所によって事情は異なるであろうが, 銀行口座による本人特定は必ずしも厳密なものではない．例えば偽名によって銀行口座が開かれたような場合には事後的なペナルティーの抑止効果は小さいであろう．

これに関連して, 次節で述べるように最近では仮名 (匿名) の銀行口座を電子マネーのシステムとして積極的に利用する考え方も文献にあらわれて来ており興味深い．

3　電子マネーに要求されるさまざまな性質とプロトコル

本節では電子マネーに要求されるさまざまな性質と, それらに対応して現状で提案されているプロトコルを整理する．

実際の電子マネーは様々なプロトコル構成要素の複合として構成される．電子マネーはデジタル情報そのものであると説明されることが多いが, それはあまり正確ではないと思われる．デジタル情報に特定の演算を順番に施すことによって価値が確認されることを考えると, 電子マネーはデジタル情報そのものではなく, その情報に対する複合的なプロトコルであると考えるほうが正しいと思われる．それぞれのプロトコル構成要素は貨幣の持ついろいろな機能を電子的に実現するために用いられる．この観点からは, 貨幣に要求されるあらゆる機能を組み込んだ複合的なプロトコルが汎用的な電子マネーであると理解することもできる．実際電子マネーに関する一般向けの概説書 (例えば [36]) では, より多くの機能を実装したより汎用的な電子マネーが今後実現していくであろうという説明がなされていることが多い．しかしながら, 電子マネーに要求されるさまざまな機能にはお互いに相矛盾する面があり, すべての機能をプロトコルとして実現した電子マネーが望ましいかどうか, また技術的にも実現性があるかどうか, は現時点ではあきらかではないと思われる．もっとも, 暗号学的なプロトコルの中には, ゼロ知識証明をはじめとして一見不可能に思われる機能を実現するものがあるので, 今後理想的な電子マネーのプロトコルが発見される可能性もあることには留意する必要がある．

以上で「本来の意味での電子マネー」という表現を定義なしに使ってきたが, これはさまざまな暗号学的なプロトコルを用いて貨幣の持ついろいろな機能を実現した電子マネーをさしたものである．特に匿名性の有無が本来の意味での電子マネーとそれ以前の支払方式の違いであると考えられる．以下では議論の順序として, 複雑な暗号学的プロトコルを用いる必要のないオンライン口座振込や電子小切手を最初に考える．これらはもちろん広義の電子マネーと考えることはできるが, 電子マネーのプロトコルの観点からみると理論的な興味はほとんどないことに注意する必要がある．

• 安全な通信路と口座振込

要求払い口座は通貨の一種と理解されており, 口座振込は現金についで直接的な決済方法である. 現状では, 小額の支払に用いるには手数料が高すぎるために, 口座振込はある程度高額の支払に用いられている. しかしながら, 例えばインターネット通じた口座振込依頼が容易になりかつ手数料が安価に設定されれば, 口座振込がインターネット上の支払手段として広く用いられるようになる可能性も考えられる.

今後普及が予想されるデビットカードも, 回線は専用回線に準ずるものであるが, 口座振込の利便性を高め手数料を安価にしたものと考えることができる.

さて, 我々が日常的におこなっている現金引出し機 (ATM) による口座振込をプロトコルの観点から考えてみよう. ATM は銀行のオンラインシステムと接続された専用の端末であり, 専用回線を用いて使用者と銀行のオンラインシステムの間の安全な通信路を確保している. また ATM を用いる際にはキャッシュカードと暗証番号を用いるが, これは本人認証のためである. この認証は公開鍵暗号を用いた本人認証ではなく, 基本的にパスワード方式 (例えば [39] の 9.1 節) によるものであり, 安全な通信が確保できればハッシュ関数を用いて可能となるものである. 以上により, 口座振込の依頼には安全な通信路が確保できれば十分であることがわかる. インターネットのように途中で盗聴の可能性があるようなオープンなネットワークでも公開鍵暗号を用いた通信の暗号化をおこなえば安全な通信路を容易に確保できるから, 口座振込の依頼はインターネットを用いてもおこなうことができる. これがインターネットによるバンキングサービスの根拠となっている.

通信路はいわゆるインターネットである必要はなく携帯電話等でもよい. 電話回線による接続は一応安全と考えられている. さらに携帯電話には発信者通知機能が標準的に備わっているので, 本人認証の一部として用いることができる. このような事情から, 携帯電話を用いたバンキングサービスがすでに実用化されているし, 今後も大いに利用されて行くと考えられる.

なお, 暗号学の観点からすればインターネットのようなオープンなネットワーク上に安全な通信路を確保するには, 対称暗号の鍵の事前配送ができればよいから, 例えば Diffie and Hellman [13] による鍵配送方式を用いればよく, 公開鍵暗号までは必要としない. もちろん二人の通信者 A,B のいずれか一方が (例えば A とする) 公開鍵・秘密鍵のペアを保有していれば, B が A の公開鍵を用いて対称暗号の鍵を事前に送信することにより対称暗号の鍵を共有することができる. したがって二人の通信者のいずれか一方が公開鍵・秘密鍵のペアを保有していれば安全な通信路の確保には十分である. この事実はブラウザで標準的に用いられている Secure Socket Layer (SSL) プロトコルで利用されている. SSL プロトコルの簡単な解説は [18] の付録 C にある. プロトコル全体は `http://home.netscape.com/eng/ssl3/` に与えられている.

• デジタル署名と電子小切手

口座振込についで暗号の観点から簡便なのは電子小切手である. 小切手は口座振込に対する依頼書と考えることができる. いま利用者 U が商店 M に電子小切手で支払をする場合を考える. 利用者 U は個人の公開鍵・秘密鍵のペアを持っているとする. U は振出人である自分の口座番号, 受取人である M の口座番号, 金額, 日付, 通し番号等をまとめた情報に自分の秘密鍵でデジタル署名を施し, これを M に送る. M はこれを銀行 B に預け入れる. B は U の署名を確認し確認できれば U から M への口座振込の手続きをおこなう. このようにして個人の公開鍵基盤を前提とすれば個人小切手の電子化を実現することができる.

さて, 電子小切手がデジタル情報でありコピーが容易であることから, 紙の小切手とはやはりやや異なった事情が生じる. まず受け取った小切手を M がコピーして二重に請求する可能性を考えなければならない. これを防ぐために銀行は U が振り出した使用済みの小切手の通し番号のリストを保管し参照する必要がある. このリストは個人ごとに作ればよいので簡易ではあるが, 主旨は使用済みの電子マネーのリストと同様である. また紙の小切手の場合には「持参人を受取人とする」という方式にすれば小切手に受取人の名前を記入する必要は必ずしもないが, 電子小切手の場合は受取人の名前が書かれているかどうかは重要な論点になる. それは U の振り出した同じ電子小切手が二つの商店 M と M' から銀行に持ち込まれた場合, 誰がコピーをおこなったかがただちにははっきりしないからである.

小切手には銀行小切手 (cashier's check) のように銀行自身がデジタル署名した小切手も考えられる. このような小切手はすでに本来の電子マネーに近い性質を持っているが, ここでは小切手として受取人が指定されているものを考えており, その点で本来の貨幣とは考えにくいものになっている.

ここでさらに受取人の指定されていない銀行小切手を考えればこれが電子マネーの基本的な形と考えられる. さて以下の議論の準備のために電子マネーの通し番号と銀行によるデジタル署名について整理しておこう. 署名の対象となる情報の最も重要な部分は電子マネーを特定するための一意的な情報 (紙幣の通し番号に対応するもの) である. さて通し番号と言うと連番の整数のように聞こえるが, 電子マネーの場合には非常に桁数の多い (例えば 150 桁) ランダムな整数を一意的な情報とする場合が多い. 桁数が十分に大きければランダムに選ばれた整数がたまたま重なる確率は無視できるほどに小さいから, 一意的な情報として必ずしも順番に整数を用いる必要はない. 以下ではこのことを前提とした上で電子マネーを特定するための一意的な情報を単に通し番号ということにする.

電子マネーを表す情報には通し番号の他に額面, 発行年月日等の補足的な情報を含むことが望ましいであろう. さらに匿名性に関連して, 電子マネーの利用者 U の識別情報を部分的に含めることが重要な課題であり, 以下でさまざまな観点から議論することとなる. ところでデジタルマネーの額面につい

ては署名の対象となる情報の中に含めるのではなくて, 署名そのもので額面をあらわすのが普通である. つまりデジタルマネーの額面については, 額面ごとに署名用の銀行の秘密鍵を異なるものとし, 署名の種類により額面を区別するのである. 以下で主に考える電子紙幣型 (例えば [49] 第 2 章) の電子マネーの場合には, 現金と同様に 1000 円, 5000 円, 10000 円というように特定の額面のもののみが発行されるから, 額面を署名によって区別することが合理的である. 同様に考えれば, 電子マネーの有効期間の設定に関連して, 例えば 1 年毎に銀行の署名用の秘密鍵を変更することも考えられる. このようにすれば例えば 10 年以上前の銀行の署名が施された電子マネーを受けつけないような処理が可能となる. セキュリティーの観点からも定期的な鍵の変更は重要である. ただし銀行の署名は電子マネーによる支払の都度に秘密鍵とペアをなす公開鍵によって確認される必要があるから, あまりにもたくさんの公開鍵があると, これらの公開鍵の検索が非効率となる可能性があることに注意する.

以上で電子マネー以前と考えられる口座振込及び電子小切手を考えてきたが, これからは Chaum ([9]) にはじまる電子マネーのさまざなプロトコルを検討していく.

電子マネーとして満たされることが望ましい条件はいろいろとあるが, まずは Okamoto and Ohta ([38]) が指摘した電子マネーの 6 条件をあげ, これらの条件を満足させるプロトコルを考察していく.

1. 独立性 (independence): 電子マネーが物理的な媒体の性質に依存せずに構成されていること. これによりネットワークを通じた電子マネーを自由に送ることができるようになる.
2. 安全性 (security): コピー (copy 複製) や偽造 (forge) ができないこと.
3. 匿名性, 追跡不可能性 (privacy, untraceability): 電子マネーの使用者や使用履歴が特定されないこと.
4. オフライン性: 電子マネー支払時にオンライン検査をともなわないこと.
5. 譲渡可能性, 転々流通可能性 (transferability) : 電子マネーがただちに銀行に還流せず, 他の利用者に譲渡され得ること.
6. 分割可能性: 電子マネーの額面を分割して使用可能なこと.

以上の条件のうち 1. の独立性の条件は, 電子マネーとしてストアド・バリュー型の電子マネーではなくアクセス型の電子マネーを考えることを示している. また電子マネーの他の分類として「電子紙幣型」か「残高管理型」かという区別がなされるが, 6. の分割可能性を考えるということはおもに電子紙幣型の電子マネーを考えることとなる. つまり以上の 6 条件ではアクセス型および電子紙幣型の電子マネーが想定されている. ただし文献で論じられている電子マネーのプロトコルには耐タンパー性を持つ媒体 (IC カード等) の

存在を前提とするものやホスト側の口座の存在を前提とするものもあることから, 以下ではストアド・バリュー型や残高管理型についても論じていく.

さて上の 6 条件の中でまずは電子マネーの基本的な特徴と考えられる匿名性について考えよう.

• 匿名性とブラインド 署名

電子マネーが暗号プロトコルの応用として関心を持たれるようになったのは Chaum ([8],[9]) による画期的なブラインド 署名の発見以来である. Chaum の考え方は, 利用者 U がランダムに電子マネーの通し番号を選び, 銀行 B はその番号を全く知らずに金額についてだけの署名をおこなうというものである. この結果銀行 B は電子マネーの発行時にどの通し番号の電子マネーを利用者 U に発行したたがわからず, その意味で利用者 U の B に対する完全な匿名性が得られる. 銀行 B が特定の利用者 U の身元を知っており U と通信していることを知っていたとしても, 発行される電子マネーに対してメクラ判を押すことを可能にするのがブラインド 署名の興味深いところである. 一方上で扱った口座振込や電子小切手の場合には署名される情報の中に振出人及び受取人が特定されており匿名性はない. 匿名性は現金の大きな特徴であるから, ブラインド 署名による匿名性は本来の意味の電子マネーと電子マネー以前の支払方式を分ける基本的な性質と考えられた.

ところで利用者の不正行為の可能性を考えると, ブラインド 署名による利用者の完全な匿名性は必ずしも望ましいものではない. 電子マネー発行時にブラインド 署名が用いられると通し番号やその他の補足的な情報についても銀行 B は発行時には内容を知ることができない. これらが銀行に知られるのは電子マネーが使用されて銀行に還流した時点であり, この時点で二重使用防止のため銀行 B は還流した電子マネーの通し番号を使用済みリストに登録することとなる. もしブラインド 署名された電子マネーに利用者 U の情報が全く含まれないと, 二重使用は無効となるだけで二重使用者にペナルティーを課すことができないために, 二重使用を試すインセンティブがはたらくし, また大量の二重使用によりシステムを混乱させる DoS 型の攻撃の可能性もある. つまりブラインド 署名を用いる場合には匿名性をどのように制限するかという点が重要となる.

この意味では, 電子マネーのいろいろなプロトコルをブラインド 署名による匿名性の制限をどのような形で実現するか, という観点から整理することもできる. 現金の場合にも紙幣には通し番号が印刷してあるから匿名性は絶対的なものではなく, コストを無視して考えれば通し番号を通じて追跡可能であることに注意する必要がある.

またブラインド 署名を用いると電子マネーの通し番号の選択について銀行側がコントロールできないという点も問題となり得る.

• 発行時のカット–選択法と利用者の識別情報

匿名性の制限のためには U の識別情報が電子マネーの中に埋め込まれて

いる必要があるが, ブラインド署名では U の識別情報が正しく埋め込まれているかどうかを確認できない. この難点を克服するための簡明な方法がカット–選択法 (cut and choose) である. カット–選択法のアイディアは [42] に見られるが, [10] がこれを電子マネーに応用した. [37], [38] では電子マネーの発行を, 初回のみの「利用許可証」の発行とその後の日常的な電子マネーの発行に分けているが, 利用許可証の発行時にやはりカット–選択法を用いている.

カット–選択法 は, ケーキを二人で分ける際に一人が先にケーキを切りもう一人が選ぶことによって公平性が確保される, という考え方に基づくプロトコルの構成要素である. [10] では利用者 U が銀行 B から電子マネーを発行してもらう際に, U の識別情報を含む K 個の情報にブラインド処理を施して送る. K は数十程度の偶数である. B はこのうち $K/2$ 個を無作為に選び U にブラインド解除を要求する. ブラインドが解除された $K/2$ 個の情報に U の識別情報が正しく埋め込まれていた場合には, B は残りの $K/2$ 個の情報をまとめたものに対してブラインドのままで一定金額の署名をおこない, これが電子マネーとなる. ブラインドを解除された $K/2$ 個の情報は捨てられる. U が自分の識別情報について不正をおこなおうとしてもカット–選択法の手続きによって高い確率で不正が発覚する. したがって識別情報の不正埋込みに対して十分なペナルティーがかかるようにしておけば, 利用者 U は識別情報を正しく埋め込むと考えられる.

カット–選択法は概念的にも簡明であり, 他のプロトコル構成要素と自由に組み合わせられることが利点である. 一方, 十分高い確率で不正が発覚するには K を大きくする必要があり, 多量の情報がやりとりされ捨てられるという効率性の観点からの問題がある. [37], [38] で「利用許可証」の発行とその後の日常的な電子マネーの発行に分けているのは, 非効率的なカット–選択法を「利用許可証」の発行時のみに用い, その後の日常的な電子マネーの発行時にカット–選択法を省略して効率化をはかったものである.

• 支払い時の challenge and response

ここで扱う challenge and response は通常は対話的ゼロ知識証明の一部であり, 独立したプロトコル構成要素としては考えられていないが, U から M への支払い時のプロトコルの本質的な部分をなす.

利用者の識別情報は (暗号化されない) なまの形で電子マネーに含まれるわけではない. もしなまの形で識別情報が含まれていれば, 1 回のみの正当な電子マネーの利用でも U の身元が判明してしまう. 従って電子マネーに含まれる U の識別情報は何らかの形で暗号化されたものである. U から M への電子マネーでの支払いに際しては, 暗号化された識別情報の一部が U から M に開示される. この部分情報は単独では U の身元を明かにしないが, 2 つの異なる部分情報からは U の身元が明かになるようにしておけばよい. こうすることによって U がもし電子マネー二重使用すると U の身元が判明することとなる. さて U から M への電子マネーでの支払いの際に U の識別情報

のどの部分が開示されるかをもし U が選べるとすると, 二重使用の際にも U は前と同じ部分を開示することによって身元を隠すことができてしまう. 従って U の識別情報のどの部分が開示されるかを U が決められない形のプロトコルにしておく必要がある. 特に簡明な方法として, M が U の識別情報の無作為な一部の開示を求めるようにしておけば, 二重使用の際に異なる部分情報が開示される確率が高くなり, U の身元が判明する. このように M が U に開示すべき情報を指定して U がそれに応じて応答することを challenge and response という.

Chaum ([10]) の電子マネーでは (前項のカット–選択法で残された) $K/2$ 個の情報のそれぞれについて challenge and response をおこなう. [10] では 1 回ごとの challenge and response で 2 つの異なる部分情報が開示される確率は $1/2$ と高くないが, これを 計 $K/2$ 回おこなうことによって全体としては U の身元が判明する確率を $1 - (1/2)^{K/2}$ と十分高くしている.

U が応答すべき challenge は必ずしもランダムである必要はない. 2 つの異なる部分情報からかならず U の身元が明かになるような場合には challenge が使用ごとに異なりさえすればいいから, challenge を商店の固有の識別番号や支払いの時刻に確定的に依存させる方法でもよい. このことはすでに [10] でも示唆されている. 後の文献では [37],[38],[52],[26] などがランダムな challenge を用い, [2],[17],[16],[12] などが 確定的な challenge を用いている.

• Single term 法

すでにふれたようにカット–選択法はあまり効率のよい方法ではない. より効率的な方法は [1] や [15] で提案されたが, ここでは [15] にしたがい single term 法とよぶ. カット–選択法のプロトコルでは複数の同様の情報からの取捨選択がおこなわれるが, このような取捨選択の必要がないために single term 法とよばれる.

Single term 法では, 電子マネーの発行時に利用者 U は銀行 B に対して U の識別情報が正しくうめこまれていることをゼロ知識証明の方法を用いて示すこととなる. 識別情報のうめこみは支払い時の challenge and response とも整合的でなければならないから, single term 法による電子マネーの発行と支払いのプルトコルは密接に結びついたかなり巧妙なものとなる. このため single term 法てはプロトコルの細部が理解しにい点がある.

• オフライン性

電子マネーによる支払い時に一々オンライン検査が必要であるとすれば, 商店は常時オンライン接続されている必要があるし, 検査結果待ち時間等の問題も生じる. 従って支払い時の電子マネーの検査はオフラインかつ簡便なものであることが望ましい. しかしながら, オフライン支払いでは電子マネーの二重使用はその場では判明しないから, オフライン支払いは二重使用の誘因となる. すなわち二重使用の検査がおこなわれる前に同じ電子マネーを多量に使用するような攻撃がおこなわれる可能性がある. これをここでは食い逃げ

攻撃とよぶことにする.

二重使用に対する通常の抑止策は, 二重使用者の身元が事後的に判明した時のペナルティーを十分に高くしておくことである. しかしながら, 例えば何らかの手段によって他人名義で電子マネーの発行を受けることに成功したような場合には, 食い逃げ攻撃は避けられないことに注意しなければならない. これは例えばクレジットカード盗難時にそのクレジットカードの多量使用が発生するのと同様である.

オンライン方式とオフライン方式の中間として, 一定以上の金額の時のみオンライン検査を行なう方式が考えられる. さらにこれを柔軟にして, 確率的にオンライン検査をおこない, しかも検査の確率を金額に依存させることが提案されている ([53],[29]). 食い逃げ攻撃は多額かつ多量に発生するであろうから, ある程度の確率でオンライン検査がおこなわれれば攻撃が発覚すると考えられる.

オフライン方式が望ましいとされるのは, 常時オンライン接続のためのコストが高いという前提のもとである. 無線技術を含めた通信技術の発展により常時接続のコストは急速に下がって来ており, あらやる情報機器が常時オンライン接続されているような状況が生じる可能性も高い. また二重使用検査に必要な通信量は小量であるから, オンライン接続が一般化した状況になれば必ずしもオフライン性にこだわる必要はない.

• 譲渡可能性

通貨 (currency) という言葉が表しているように, 現金はすぐには銀行に還流せずに人の手から人の手へと渡っていく. 現金の持つ性質をすべて満たすような電子マネーを望ましいと考えるならば, 譲渡可能性も電子マネーが実現すべき一つの性質である. 電子マネーの譲渡可能性を考えるには, オンライン方式とオフライン方式の電子マネーを区別して考える必要がある. オンライン方式においては電子マネーを譲渡する必要はない. すなわち電子マネーを預けいれるとともにただちに新しい電子マネーを次の利用者に発行すればいいからである. オンライン方式においては電子マネーの銀行への還流は即時かつほぼ無コストであると考えてよいから, そもそも譲渡の必要がないわけである. したがって電子マネーの譲渡可能性を考えるのはオフライン方式の電子マネーの場合に限る.

さて, 現金が流通していくのは, 利用者の情報が含まれないという現金の匿名性と表裏一体の関係にあると考えられる. 電子マネーでは二重使用の問題があるために, 利用者の識別情報を何らかの形で電子マネーに埋め込む必要があった. 従って電子マネーを譲渡可能にするためには, 譲渡されるごとに新たな利用者の識別情報を新たにうめこんで行く必要がある. つまり譲渡可能な電子マネーの場合, 電子マネーの発行から始まって順にすべての利用者の識別情報を暗号化された形でうめこんで行く必要がある. これは, 電子マネーが譲渡されて行く過程でどの利用者が二重使用をおこなうかわからないからで

ある．この点で同じ譲渡可能性と言っても現金と電子マネーでは全く事情が異なる．つまり現金には流通経路の情報は何も残されていないが, オフラインの電子マネーの場合には流通経路がすべて暗号化されて記録されていくこととなる．この事から電子マネーは譲渡されるごとにサイズが大きくなって行くこととなる ([11]).

電子マネーの譲渡のプロトコルの考え方は次のようなものである．電子マネーの価値は銀行の署名を根拠としている．利用者 U から次の利用者 U' に電子マネーが譲渡される際には, 利用者 U が一時的に銀行の役目を果たす．すなわち利用者 U が譲渡される電子マネーに署名を追加することとなる．これは「譲渡証」の作成と考えることができる．匿名性の要請から, U の署名に U の本来の公開鍵・秘密鍵のペアを用いることはできないから, この署名のためには一時的な公開鍵・秘密鍵のペアを用いる必要がある．すなわち U が一時的な公開鍵・秘密鍵のペアを用意し, この一時的な公開鍵に銀行が金額分の署名をする．そして, U から利用者 U' に電子マネーが譲渡される時には, U' が新たに一時的な公開鍵・秘密鍵のペアを用意し, これに U の一時的な秘密鍵で署名をすることとなる．このようにして, 銀行の署名からはじまって譲渡のたびに署名の鎖が長くなっていく事となる．このような考え方は [37] で示されたものである．特に [37] では利用許可証と個々の電子マネーを分離し, 署名の連鎖の機能を利用許可証で実現しているので, 譲渡の手続きが簡明となる．

電子マネーの譲渡可能性は望ましい性質ではあるが, 不正使用の誘因となる可能性もある．電子マネーが何回も流通して行き, なかなか銀行に還流しないことが予想される場合には, 食い逃げ攻撃がおこりやすくなるかも知れない．また譲渡が無制限に許容される場合には, 譲渡の回数を非常に大きくすることによって経路の検索を混乱させるような DoS 型の攻撃も考えられる．これを防ぐためには譲渡の回数の制限が必要となるかも知れない．あるいは, オフライン性のところでもふれたように, 適当な確率で銀行に還流することを要求するようなシステムも考えられる．

- **分割可能性**

現金には分割可能性がないために, おつりや両替といった操作が必要となる．これに比してプリペイドカードは残高管理型のためにおつりが不要となることが一つの長所となっている．電子マネーでも (残高管理型ではなく) 電子紙幣型の場合には額面が一定であるから, おつりや両替の問題が発生する．オンラインの電子マネーの場合には, 支払いに際しておつりが必要な場合には, 即時に新たな電子マネーを発行してもらう形で処理することができる．しかしながら, オフライン電子マネーの使用時におつりを受け取るには, おつりの金額分の電子マネーを譲渡してもらう必要があり, 前項でふれた電子マネーの譲渡という問題が必然的に生じる．このような難点を解決する方法として分割可能性のあるオフライン電子マネーが提案されている．

分割可能性の一つの考え方は, 一定の額面の電子マネーを回数券の集まり

としてとらえるものである ([37]). この方法では回数券全体の額面に銀行が金額分の署名をし, 利用者は必要に応じて回数券にわけて小額を使用することができる. さらに [38] は, 回数券の中に回数券が入れ子になっているような再帰的な木構造に基づいた分割可能性を示した. この構成法はきわめて巧妙であり, 一定の金額を柔軟に分割して使用することができる. 木構造を用いた分割のプロトコルは [14] において single term 法と組み合わされ, さらに [35], [6] において効率化されている. このような分割可能性を実現することによって, 現金に比した電子マネーの利便性が高まると考えられる.

一方で二重使用の防止という観点から考えると, 分割可能性を持つ電子紙幣型の電子マネーは残高管理型の電子マネーの一種と見ることもできる. すなわち分割可能な電子マネーが使用された時点で, 銀行はそのマネーを使用済みの電子マネーのリストに加えるが, その際にどの部分が分割して使用されたかを記録しておく必要がある. この情報は全額が使用済みになるまで順次記憶しておく必要があるが, そのことは使用済みの電子マネーのリストにその電子マネーの残高が記録されていることにほかならない. さらに言えば, 残高管理型の場合は残額のみが記録されればよいが, 分割可能性を持つ電子紙幣型の場合にはどの部分が使用されたの情報まで記録される必要があり, より複雑である. この観点からは, 分割可能性を有する電子紙幣型の電子マネーは, 使用履歴を明確にすることによって不正使用に対する防止策を強化した残高管理型の電子マネーであると考えることもできる.

分割可能性と譲渡可能性の両方の性質を要求すると, 二重使用の防止のために銀行は, 電子マネーの分割使用を表す木構造のそれぞれのノードについて譲渡履歴をリストに記憶する必要があり, 使用済みリストがかなり複雑となる. 一方分割可能性があればおつりが不要となり, おつりにともなう譲渡可能性も要求されないから, 譲渡可能性は必ずしも必要とされないとも考えられる. したがって分割可能性と譲渡可能性は両者とも同時に満たすべき性質ではなく, 補完的な性質であると理解したほうがよいと思われる.

- **第三者機関による匿名性の剥奪**

Chaum ら ([10]) によって提示された銀行のブラインド署名に基づく匿名の電子マネーは, [37], [38] 等によって上で述べた 6 条件を満たす形に拡張された. しかしながら, 不正使用の防止という観点から見ると, これまでに見てきた様々なプロトコルによる対応では不十分ではないかという指摘がなされるようになった ([51]). その指摘はやや極端なものではあるが, 例えば銀行のブラインド署名用の秘密鍵が盗まれたりあるいは脅迫されることによって犯罪者に知れてしまった場合, 電子マネーのシステム全体が崩壊してしまうのではないか, という点にある. このような極端な場合でなくても, 例えば銀行の内部の者がブラインド署名用の秘密鍵を盗み, その秘密鍵を用いて電子マネーを偽造した場合, もし偽造の量が大量でなければ偽造そのものが発覚しないこともある. 仮にもし電子マネーの発行高と還流高の差によって偽造が発覚し

たとしても, 特定の電子マネーが二重使用されない限りは利用者の身元は全く判明しないから, 犯人の身元は全くわからないことになる. このような意味で, ブラインド署名に基づく電子マネーは “完全犯罪” (perfect crime) の余地のあるものとなっている. つまり犯罪捜査の観点からはブラインド署名に基づく完全な匿名性は望ましいものではなく, (二重使用がなくても) 必要に応じて電子マネーの利用者や電子マネーの利用経路の追跡が担保されたシステムが必要とされる. これを匿名性の強制剥奪 (revocation of anonymity) という.

匿名性の剥奪はプロトコルのみによって実現するのは極めて難しく, 現状で提案されている方法は第三者機関 (trustee, judge, ombudsman, escrow) への利用者の身元情報の登録に基づくものがほとんどである. 第三者機関の介在は [3], [47] 等で提案され, その後 [26], [4], [5], [17], [16],[12], [32], [40], [41], [27], [28], [25], [30] 等の多くの文献で論じられている. これらの文献では第三者機関の介在の程度や方法によりさまざまな方式が提案されている. これらについては [41] の比較検討が参考になる.

第三者機関に基づくシステムで概念的にわかりやすいのは, 利用者 U が身元 (本名) を第三者機関に登録するとともに 第三者機関から仮名 (pseudonym) を得るという方式である ([47],[5],[17],[32] 等). そして利用者のその後の銀行や商店との取引をこの仮名に基づいておこなうこととすれば匿名性が確保されることになる. 仮名を用いるのであれば, 発行される電子マネーには仮名を暗号化されない形でそのまま含めばよい. このことによって, 犯罪捜査等の必要が生じた場合には二重使用等がない場合でも第三者機関の登録情報を参照することによってユーザの身元をあきらかにする事ができる. また利用者による二重使用の際にもやはり第三者機関の登録情報をするだけでよいから発行時のカット–選択法や single term 法などのプロトコルを省略する事ができ, 電子マネーのプロトコルを大幅に簡略化できる.

このように仮名を用いると利用者の匿名性を確保することができるが, 実はもし利用者が匿名性にこだわらなければ本名をそのまま仮名として用いることも可能であることに注意する必要がある. もし本名をそのまま使うのであれば第三者機関への登録は不要となる. 銀行, 税務当局あるいは警察当局は仮名の利用を必ずしも歓迎しないであろうから, 仮名の登録に関して何らかの制度的な制約がかかる事も考えられる. また第三者機関の運営費用の問題もあるから, 利用者が匿名性を得るかわりに「仮名使用手数料」を要求される可能性も高い. ちなみに, 仮名使用手数料を設定することによって, 消費者が匿名性をどの程度重視しているかを測ることができるという利点もあるかも知れない.

第三者機関の介在の是非についてはさまざまな立場からの議論がある. 公開鍵基盤のためには認証局の存在が当然前提されているから, 例えば認証局の機能の一環として仮名の発行を担わせることも考えられる. その意味では第三者機関の存在はそれほど不自然なものではないかも知れない. 一方現金の有する独立性を理想とする電子マネーにとっては第三者機関を介在は必ずし

も望ましいものではないかも知れない. また些細な点であるが, 暗号理論の観点からは第三者機関を前提とする事によって電子マネーのプロトコルが大幅に単純化してしまい, 理論的な興味が減少することも事実である.

第三者機関を用いず犯罪に対処する方法としては, 最近になって [44], [45] の提案がある. [44] は銀行の秘密鍵を用いないため銀行の秘密鍵に対する攻撃を防ぐことができることが利点であるが, 他方ユーザ U が電子マネーの通し番号に関する情報を常に更新して行く必要がある点でプロトコルが複雑となっている. [45] では一定期間内に使用できる電子マネーの量を一定額以内に制限する事によって第三者機関の介在なしに犯罪に対処できるとしているが, 分譲渡可能性を排除するなどプロトコルとしては制約の多いものとなっている.

• 匿名通信

仮名の取得によって利用者の匿名性がいったんは確保されるが, 仮名と本名の対応が知られてしまえばその匿名性は失われる. 例えば通信販売で商品を購入する場合, 電子マネーの支払いの際には仮名を用いることができるとしても, 商品の配達のためには通常は住所及び宛名を知らせる必要があるから, この場合商店に本名と仮名の対応が知られてしまう. このような文脈では匿名通信 (anonymous communication) が重要な概念となる.

匿名通信は [7] の “mix” プロトコルによって実現方法が示され, [46] によって電子マネーのプロトコルの一部として用いられた. [46] の議論はやや抽象的であるが, その後匿名通信は [24], [23] でより具体的に用いられている.

匿名通信とは通信相手の身元のわからない通信である. 例えば差出人名のない手紙や名前を名乗らない電話などが匿名通信にあたる. 差出人名のない手紙の場合, 差出人は受取人を知っているが, 受取人は差出人がわからないため, 匿名性は一方向であり非対称性が存在することに注意する. ただし私書箱のような仕組を用いれば, 受取人の匿名性もある程度確保することができる. 例えば, 通信販売で仮名の注文者が注文した商品を特定のコンビニエンスストアに配達することを依頼し, コンビニエンスストアでは注文者のみが知り得た情報を提示できる者に商品を引き渡すといった方法が考えられる. このような匿名性は消費者には有利であるが顧客の情報を知りたいと考えている商店側は一般にはあまり歓迎しないであろう. 電話については, 最近まで発信元の電話番号を特定することはできなかったが, 技術的な進歩により一般の加入電話でも発信者番号通知機能が導入され議論をよんだ. この議論でも, 発信者と受信者とで匿名性に対する有利不利の非対称性があることが論点となったことに注意する必要がある.

インターネット上の通信では通常は IP アドレスがお互いに確認されるので IP アドレスレベルでは匿名性はないが, これは通信機器が特定されるだけで必ずしも利用者までは特定されない. しかしながら機器の管理者は利用者を特定できる場合も多い. 例えば, あるインターネットプロバイダーで利用者

名あるいはメールアドレスを本名と無関係なものにしている場合でも, 法的に必要があれば本名と利用者名の関係を明かにすることが求められるであろう. このように匿名通信は, 私書箱における郵便局のように, 通信の仲介者によって提供されることが多い. つまり基本的には匿名通信は代理者を介した通信であり, この意味では前項で述べた第 3 者機関による仮名の提供と類似した側面を持っている. Chaum ([7]) の mix プロトコルでは, 匿名の電子メール通信を扱っているが, メールを仲介する代理者となるコンピュータを mix とよんでいる.

• 仮名 (pseudonym) の銀行口座

仮名の銀行口座は [5],[46] 等によって電子マネーのプロトコルの一部として考えられようになった. 仮名の銀行口座は本人確認を必要としない銀行口座であり, 例えば現金を銀行に持って行くと身元の確認なしに預金口座が開設できる場合を考えればよい. 仮名口座とその暗証番号及び匿名通信を組み合わせれば, この節の冒頭で述べた口座振込のみによって匿名性を持つ支払いシステムを構築することができる. この考え方は [46] によってやや抽象的に提示されたが, [23] ではより明解に示されている.

通常の口座と仮名口座の両方を持つ利用者は, かなり頻繁に通常口座から仮名口座への振込を必要するであろうが, このために本名と仮名の対応が知られてしまう可能性がある. 従って通常口座と仮名口座の対応が容易には知られないようなプロトコル上の処理が必要となる. [5] では single term 法の応用によって本名と仮名の対応を知られることなく通常口座から仮名口座への振込が可能であることを示している. 実は, 通常口座から仮名口座への振込は現金を用いれば簡単である. すなわち ATM を用いて通常口座から現金を引き出し, 続いてそれを仮名口座に預け入れればよい. この例でわかる事は, 物理的な媒体を用いれば自明に実現できることが, デジタル情報のみで実現しようとすると複雑なプロトコルを必要とする場合もあるということである. この点に注目すると, 物理的な媒体の利点も補助的に考慮した支払いシステムを考えることも重要であると考えられる.

仮名については, 第三者機関による仮名の保証を要求するか否かで考え方がわかれる. 匿名性の剥奪という観点からは第三者機関によって保証された仮名のみを許容するという考え方となる. 一方で電子マネーのプロトコルの一部としての仮名口座の目的はもっぱら比較的小額の支払いのためであり, 預金額の上限を設けるなど一定の制度的な制限のもとに, 第三者機関による保証なしに仮名口座を認めることも考えられる.

ところで, 時代と場所によって異なるが, 銀行口座の名義確認は必ずしも厳密なものではないことに注意する必要がある. 例えばスイスの銀行は顧客の身元を秘密にすることによって世界中から顧客を集めている. 我が国でも納税者番号制度に関する長年の議論にあらわれているように, 税金対策としての家族名義口座の利用などは広く見られるところである. 納税者番号制度に

対する反対理由としてプライバシー保護があげられることが多く, これは消費者の匿名性に対する選好を表しているとも考えられるが, 実際にはやはり税金対策が主であろう. 電子マネーにおける匿名性は, 消費者が消費行動を記録されたくない, という点が主旨であり, 貯蓄目的の口座の匿名性とは全く異なるものであることに注意する必要がある.

以上のような実態を考慮するならば, 第三者機関による保証の有無を含めて一定の範囲で仮名の銀行口座を認めることには意味があると考えられる. 実際に, 銀行口座という枠組を離れて支払いサービスの一つの形態という視点から見れば, インターネット上の支払いサービスで仮名口座と同様なシステムをすでにいくつか見出すことができる. これは webmoney[2] や bitcash[3] などのサービスで, こするとはがれる特殊な塗料で暗証番号を隠したカードを書店やコンビニエンスストアなどで購入し, 塗料を硬貨などでスクラッチすることによって暗証番号を入手する. この暗証番号が仮名口座の番号をかねている. このようなシステムは現金の匿名性と特殊な塗料による安全性を利用することによって匿名口座の開設を簡便化したものと理解することができる.

最後に仮名口座と電子マネーの使用済みデータベースの関係についてふれておく. 上の分割可能性の項で論じたように, 分割可能な電子マネーの場合銀行は残高を管理する必要が生じる. この意味では分割可能な電子マネーあるいはその通し番号自体が仮名口座と同様のものであると考えることができる. ブラインド署名に基づく電子マネーにおいては, 電子マネーの通し番号は銀行に還流した後でないと知られない. そのため銀行は未使用の電子マネーのリストを作成することができず, 使用済み電子マネーのリストを管理する必要が生じる. しかしながら銀行口座の管理がその時点で利用者が使用可能な金額の管理であることを考えると, 仮名口座の管理は発行済みでまだ (全額は) 使用されていない電子マネーのデータベース管理と同等であると見ることができる. すなわち, 電子マネーの通し番号が発行時点でわかっているならば使用可能な電子マネーのデータベース (仮名口座) を管理すればよく, このほうが使用済み電子マネーのデータベースを管理するより簡明であると思われる. 匿名通信における仲介者と同様の役割を果たす第三者機関の存在を前提とすればこのような方式も可能であると思われる. また最近では [44] が未使用の電子マネーのリストを “ハッシュ木” に基づいて構成する方法を示している.

• 匿名性とリンク可能性

仮名の使用によって匿名性が得られたとしても, 同じ仮名を持つ利用者の購買行動は互いに関係づけ追跡するできる. これをリンク可能性 (linkability) といい匿名性と区別して考える必要がある. [37], [38] の利用許可証を用いる方法でも, 匿名性は確保されるがリンク可能性は残る. 電子マネーを正常に使用している限りは利用許可証からは本名は判明しないから, この意味では利用

[2] http://www.webmoney.ne.jp
[3] http://www.bitcash.co.jp

許可証は仮名と同様の機能をはたしていると考えことができる.

リンク可能性がある場合は同一利用者の購買履歴が累積し利用者の行動範囲等が特定されて, 利用者の身元が判明する場合があり得る. 従って匿名性を重視するならば利用者は仮名や利用許可証を一定の頻度で更新する必要がある. 最近になって [33] は group signature という技法によってリンク不可能性を持つ電子マネーを提案している.

• マイクロペイメント

電子マネーの一つの機能として非常に小額の支払い (マイクロペイメント) が考えられている. たとえばブラウザで有用な情報を提供しているサイトにアクセスする際に 1 画面ごとに 1 円を払うというような場合である. マイクロペイメントではもちろん 1 円単位で電子マネーの銀行への預け入れが発生するわけではない. 非常に小額の電子マネーの処理に通信費用等のコストをかけることはできないから, マイクロペイメントの場合には支払いが一定額に達した場合や一定期間がすぎた場合に預け入れの処理がおこなわれる. すなわちマイクロペイメントは電話料金と同様に従量制のシステムとなる. また支払いの累積額を処理するために何らかのカウンターの機能を実現している必要がある. ここでのカウンターは電気やガスの利用量を表すメーターのように理解すればよい. プリペイドカードのような前払いのシステムの場合はカウンターは残高を表し, クレジットカードのように後払いのシステムの場合にはカウンターは累積使用量を表すものとなる. [43] では同一のハッシュ関数を何回も適用し, その適用回数をカウンターに対応させている. [48] では商店 M に耐タンパー性を有する装置を用意し, これにカウンターの機能を持たせている. “Millicent”([19]) では残高がユーザ U と商店 M の間で交信され相互確認される.

現在提案されているマイクロペイメントのシステムは残高管理型の電子マネーの一種と考えることができる. これらのシステムでは利用者 U から商店 M への決済を仲介する「ブローカー」が存在し, このブローカーがカウンターの正当性を管理している. この場合, カウンターを相互に区別するためのカウンターの識別子が口座番号にあたり, カウンターの値が残額であると考えることができる.

匿名性の処理のプロトコルを組み込むと処理のコストがかかるために, マイクロペイメントでは匿名性を組み込まない場合が多い. 例えば Millicent では残高管理の情報に利用者名と商店名が含まれている. この意味ではマイクロペイメントと現金の「小銭」では大きな違いがある. 現金の場合, 紙幣とコインを比較すると, 前者には通し番号が印刷してあり原則的には追跡可能であるが, コインの場合には同じ額面のコインは互いに区別がつかず追跡可能性はない. この意味では紙幣より額面の小さいコインの方が匿名性が高いと考えることができる. 一方マイクロペイメントの場合には匿名性がない. つまりマイクロペイメントの主眼は単発的な小額の支払い処理にあるわけではなく, 利

用者 U と商店 M の一定期間にわたる取引において従量的な支払いを可能にするものであると考えられる.

4 いくつかのコメント

ここでは筆者の感想をまじえて電子マネーについていくつかの論点をあげる.

• 匿名性に対する選好

すでに何回も述べてきたように電子マネーにとっては匿名性がキーとなる概念であるが, 人々が匿名性をどれほど重視しているかは必ずしも明かではない. クレジットカードと現金のどちらで支払いをおこなうかを考える場合, 必ずしも匿名性が判断の基準となっているのではなく, 手持ちの現金の量や現金引き出しの手間が判断の基準になっている場合も多いと思われる. 一方でネットワーク社会の到来とともに個人情報のデジタル化と蓄積が問題視されるようになっており, 人々が匿名性により多くの関心を払うようになるかも知れない. 前節の匿名性の剥奪の項で述べたように, 金融システム側や警察が匿名性を好まないこと, そして匿名性の確保に費用もかかることから, 匿名性に一定の制限が設けられたり手数料が請求されることが予想される. 手数料の存在は消費者の匿名性に対する選好を測る意味もあり, 消費者がどのように反応していくかは興味深い点である.

• クレジットカードの問題点

現状ではインターネットを介した通信販売における支払はクレジットカードによるものがほとんどであるが, クレジットカードのシステムは対面販売を前提としている作られてきたために, インターネットでの利用には問題が多い. 特に利用者の署名というプロトコルが欠落している点が基本的な難点である. クレジットカードを用いた対面販売では利用者が伝票に署名し伝票のコピーをその場で受け取る[4]. ところがインターネット上でクレジットカードを用いる場合には, (利用者個人の公開鍵基盤が未整備という現状では) 利用者が署名をおこなうことができない. したがってクレジットカードの名義と番号を知っているものは誰でもそのクレジットカードを用いることができる. 特に注文先の商店の店員が利用者のクレジットカードの名義と番号を不正に使用する被害が実際にも問題となっている.

このように現状の形でインターネット上でクレジットカードを用いることには根本的な問題点があるが, これを解決するものとして SET (Secure Electronic Transaction) というプロトコルがクレジットカード会社によって開発推進されている. SET プロトコルについて簡単な解説は [50] の 12 章にあるが, 完全

[4] クレジットカードの不正使用としてカードの偽造が深刻な問題となりつつあり, 署名による本人確認は実際には不正防止のために必ずしも有効ではないが, クレジットカード利用時の署名が本人確認の手続きであると理解されていることは間違いがないであろう.

な情報は SET プロトコルのホームページ (`http://www.setco.org/`) から得られる. SET プルトコルでは利用者 U から商店 M への支払い時に M は U のカード番号を知ることができない. SET プロトコルは公開鍵基盤に基づく本格的な支払いシステムであるが, 現状ではまだ広く用いられるにはいたっていない.

クレジットカードについては対面販売においても偽造カードの問題が深刻化しており, 今後クレジットカードの安全性の強化がはかられることになると思われる.

• 電子マネーの今後

本論文で概観してきたように, 電子マネーのプロトコルの要素は非常に多種多様であり, どのような電子マネーが用いられるようになるかは明かではない. あらゆる機能を実現した最も汎用的な電子マネーが用いられるようになるという考え方は, 最近の電子マネーのプロトコルの文献ではあまり見られない. 完全犯罪等の可能性を考えると, 匿名性の強制剥奪可能性を組み込まない電子マネーシステムが金融システム側によって許容される可能性は少ないと考えられる. 匿名性の剥奪を第三者機関によって実現するとすれば, その設置形態が問題となる.

匿名性を要求しない形であれば, 銀行やクレジットカード会社はインターネットバンキングサービスやクレジットカードのサービスの安全性や利便性を今後もますます高めて行くであろう. そのような中で本来の電子マネーが実現するようになるとすれば, その要因は消費者の側からの匿名性に対する選好あるいは要求であると考えられる. [9] の言う “big brother 不要論” は消費者自らの匿名性に対する強い要求に支えられる必要がある.

前節で見たように, 現状で提案されている電子マネーのプロトコルの限りでは, 匿名性・オフライン性・譲渡可能性を兼ね備えた電子マネーにはさまざまの攻撃が考えられ, 大量の発行・流通が実現する可能性は低いであろう. 自立性を持つ電子マネーが大量に国境を越えて流通する, といった議論には現状ではほとんど現実性はない.

References

[1] S. Brands, “An efficient off-line electronic cash system based on the representation problem”, C.W.I. Technical Report CS-R9323 (1993).

[2] S. Brands, “Untraceable off-line cash in wallet with observers”, *Advances in Cryptology – CRYPTO’93* pp.302–318 (1994).

[3] E. Brickell, P. Gemmel and D. Kravitz, “Trustee-based tracing extensions to anonymous cash and the making of anonymous ex-

change", *Proc. 6th annual ACM-SIAM symposium on Discrete algorithms (SODA)*, pp.457–466 (1995).

[4] J. Camenisch, U. Maurer and and M. Stadler, "Digital payment systems with passive anonymity-revoking trustee", *Computer Security – ESORICS'96*, LNCS 1146, pp.31–43 (1996).

[5] J. Camenisch, J.M. Piveteau and M. Stadler, "An efficient fair payment system", *3rd ACM Conference on Computer Communications Security*, ACM Press, pp.88–94 (1996)

[6] A. Chan, Y. Frankel and Y. Tsiounis, "Easy come - easy go divisible cash", *Advances in cryptology – EUROCRYPT'98*, LNCS 1403, pp.561–575 (1998).

[7] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", *Communications of the ACM*, pp.84–88 (1981).

[8] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology – CRYPTO'82*, pp.199–203 (1982).

[9] D. Chaum, "Security without identification: transaction system to make big brother obsolete", *Communications of the ACM*, **28**, pp.1030-1044 (1985).

[10] D. Chaum, A. Fiat and M. Naor, "Untraceable electronic cash", *Advances in Cryptology –CRYPTO'88*, pp.319–327 (1988)

[11] D. Chaum and T.P. Pedersen, "Transferred cash grows in size", *Advances in Cryptology – EUROCRYPT'92*, LNCS 658, pp.357–367 (1993).

[12] G. Davida, Y. Frankel, Y. Tsiounis and M. Yung, "Anonymity control in E-cash systems", *Advances in Cryptology – Financial Cryptology '97* , LNCS 1318, pp.1-16 (1997).

[13] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, IT–22, **6**, pp. 644–654 (1976).

[14] T. Eng and T. Okamoto, "Single-term divisible electronic coins", *Advances in Cryptology – CRYPTO'94*, pp.306–319 (1994).

[15] N. Ferguson , "Single term off-line coins", *Advances in Cryptology – EUROCRYPT'93*, pp.318–328 (1994).

[16] Y. Frankel, Y. Tsiounis and M. Yung, "Indirect discourse proofs: achieving efficient fair off-line E-cash", *Advances in Cryptology – ASIACRYPT'96*, LNCS 1163, pp.286-300 (1996).

[17] E. Fujisaki, and T. Okamoto, "Practical escrow cash systems", LNCS 1189, Springer, pp.33–48 (1997).

[18] S. Garfinkel and G. Spafford (安藤 進 訳),『Web セキュリティー & コマース』 オライリー・ジャパン (1998).

[19] S. Glassman, M. Manasse, M. Abadi, P. Gauthier and P. Sobalvarro, "The Millicent protocol for inexpensive electronic commerce", *World Wide Web Journal, Fourth International World Wide Web Conference Proceedings*, O'Reilly, pp.603–618 (1995). (available from `http://www.millicent.digital.com/`)

[20] 池尾和人, "電子マネーと経済秩序の変容可能性", ITME discussion paper No.18 (1999).

[21] 岩村 充,『電子マネー入門』, 日本経済新聞社 (1996).

[22] 岩村 充, "電子マネーは金融政策を変えるか",『電子貨幣論』(西垣通編), 第 3 章, NTT 出版 (1999).

[23] M. Jakobsson, "Mini-Cash: a minimalistic approach to E-commerce", *Public Key Cryptography '99* , H. Imai and Y. Zheng eds. LNCS 1560, pp.122–135 (1999).

[24] M. Jakobsson and D. M'Raihi, "Mix-based electronic payments", *SAC'98*, LNCS 1556, pp.157–173 (1998).

[25] M. Jakobsson and J. Müller, "Improved magic ink signatures using hints", *Advances in Cryptology – Financial Cryptology '99*, LNCS 1648, pp.253–268 (1999).

[26] M. Jakobsson and M. Yung, "Revokable and versatile electronic money", in *Third ACM Conference on Computer and Communication Security*, ACM Press, pp.76–87 (1996).

[27] M. Jakobsson and M. Yung, "Distributed Magic-Ink signatures", *Advances in Cryptology – EUROCRYPT'97*, LNCS 1233, pp.450–464 (1997).

[28] M. Jakobsson and M. Yung, "Applying anti-trust policies to increase trust in a versatile e-cash", *Advances in Cryptology – Financial Cryptology '97*, LNCS 1318, pp.217–238 (1997).

[29] S. Jarecki and A. Odlyzko, "An efficient micropayment system based on probabilistic polling", *Advances in Cryptology – Financial Cryptology '97*, pp.175–191 (1997).

[30] A. Juels, "Trustee tokens: simple and practical anonymous digital coin tracing", *Advances in Cryptology – Financial Cryptology '99*, LNCS 1648, pp.29–45 (1999).

[31] 本西泰三, "電子マネー導入に向けた環境整備", ITME discussion paper No.26 (1999).

[32] D. M'Raihi, "Cost-effective payment schemes with privacy regulation", *Advances in Cryptology – ASIACRYPT'96*, LNCS 1163, pp.266–275 (1996).

[33] T. Nakanishi, N. Haruna and Y. Sugiyama, "Unlinkable electronic coupon protocol with anonymity control", *Information Security Workshop '99*, LNCS 1729, pp.37–46 (1999).

[34] 西垣 通 編, 『電子貨幣論』, NTT 出版 (1999).

[35] T. Okamoto, "An efficient divisible electronic cash scheme", *Advances in Cryptology – CRYPTO'95*, pp. 438–451 (1995).

[36] 岡本栄司・満保雅浩, 『電子マネー』, 岩波書店 (岩波科学ライブラリー 53) (1997).

[37] T. Okamoto and K. Ohta, "Disposable zero-knowledge authentication and their applications to untraceable electronic cash", *Advances in Cryptology – CRYPTO'89* pp.481–496 (1989).

[38] T. Okamoto and K. Ohta, "Universal electronic cash," *Advances in Cryptology – CRYPTO'91*, pp. 324-337 (1991).

[39] 岡本龍明・山本博資, 『現代暗号』, 産業図書 (1997).

[40] H. Petersen and G. Poupard, "Efficient scalable fair cash with off-line extortion prevention", LNCS 1334, pp.463–477 (1997).

[41] H. Petersen and G. Poupard, "Efficient scalable fair cash with off-line extortion prevention" (full version of the [40]), Technical Report LIENS-97-07, `http://www.dmi.ens.fr/EDITION/preprtins/` (1997).

[42] M. O. Rabin, "Digitalized signatures", *Foundations of Secure Computation*, pp.155–168 (1978).

[43] R. L. Rivest and A. Shamir, "PayWord and MicroMint: two simple micropayment schemes", *CroyptoBytes*, **2**, pp.7–11 (1996). `http://theory.lcs.mit.edu/~rivest` .

[44] T. Sander and A. Ta-Shma, "Auditable, anonymous electronic cash", *Advances in Cryptology – CRYPTO'99*, pp.555–572 (1999).

[45] T. Sander and A. Ta-Shma, "Flow control: a new approach for anonymity control in electronic cash systems", *Advances in Cryptology – Financial Cryptology '99*, LNCS 1648, pp.46-61 (1999).

[46] D. R. Simon, "Anonymous communication and anonymous cash", *Advances in Cryptology – CRYPTO'96*, pp.61–73 (1996).

[47] M. Stadler, J.M. Piveteau and J. Camenisch, "Fair blind signatures", *Advances in Cryptology – EUROCRYPT'95*, pp.209–219 (1995).

[48] J. Stern and S. Vaudenay, "SVP: a flexible micropayment scheme", *Advances in Cryptology – Financial Cryptology '97*, pp.161–171 (1997).

[49] 須藤 修・後藤玲子, 『電子マネー』, 筑摩書房 (1998).

[50] P. Wayner (川副 博 監訳), 『デジタルキャッシュテクノロジー』, ソフトバンク (1997).

[51] S. Von Solms and D. Naccache, "On blind signatures and perfect crimes", *Computer & Security*, **11**, 581–583 (1992).

[52] Y. Yacobi, "Efficient electronic money", *Advances in Cryptology – ASIACRYPT'94*, pp.153–164 (1994).

[53] Y. Yacobi, "On the continuum between on-line and off-line e-cash systems – I", *Advances in Cryptology – Financial Cryptology '97*, pp.193–201 (1997).