電子マネーの一実現方式について
― 安全性、利便性に配慮した新しい電子マネー実現方式の提案 ―

中山靖司 / 森畠秀実 / 阿部正幸/ 藤崎英一郎

要　旨

インターネットが広範に普及する中、電子商取引（エレクトロニック・コマース）の実現に向けて、世界各国でさまざまな取組みが進められている。とりわけ、お金の情報を電子化し、オープンなネットワークの中でも利用可能とするような「電子マネー」は、電子商取引実現のための基幹技術として、実用化に向けた研究・実験が一段と活発化してきている。

本稿では、電子マネーが安価で信頼性の高い新たな金融サービスとなるために求められる要求条件を「安全性」、「電子マネー特有の利便性」、「現金のメリットの継承」の３つの観点から考察する。次に、この要求条件を満足する電子マネーを実現するための設計方針を明らかにし、新たに考案したアイデアを加えた新しい電子マネー実現方式についてのプロトコル概要等を提示する。

キーワード：電子商取引、電子マネー、暗号技術、デジタル署名、安全性、プライバシー

本稿を作成するに当たっては、松本勉助教授（横浜国立大学）から有益なコメントを頂戴した。なお、本稿の内容・意見は筆者個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。

中山靖司　日本銀行金融研究所研究第２課
森畠秀実　日本電信電話株式会社情報通信研究所
阿部正幸　日本電信電話株式会社情報通信研究所
藤崎英一郎　日本電信電話株式会社情報通信研究所

1．電子マネーへの要求条件

電子商取引を実現するための電子決済方法としては、現在さまざまなタイプが考えられている。例えば、クレジットカードの電子化、電子小切手、オンラインバンキング、狭義の電子マネー[1] 等である。このうち、電子マネー以外の方法は、クレジットカードや銀行口座振替等の従来から存在する支払手段への新たなアクセス方法を電子的コミュニケーション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、電子マネーたるデータ自体に価値が含まれているとのコンセプトで考案されたものであり、最近注目を浴びている。電子マネーのプロジェクトの中には、フィールド実験を行ったり、限定的な実用化の段階に進んだものもあるが、本格的な実用化を進めていくうえでは、セキュリティレベルをいっそう高めたり、さらに利便性を高めるべく実現スキームを改善する必要があるなど、まだ多くの課題が残っているとみる向きも多い。

以下では、電子マネーが世の中に受け入れられていくためには、どのような要求条件を満たす必要があるか、（１）安全性、（２）電子マネー特有の利便性、（３）現金の持つメリットの継承、の３つの観点から掘り下げて検討する。

（1）安全性

電子マネーの安全性とは、価値の変造、偽造あるいは複製による再使用等の不正利用が限りなく不可能に近いことを意味する。電子マネーが決済手段として広く普及し、誰にも拒絶されずに安心して受け取ってもらえるようにするためには、人々にその安全性が認識され、信頼されるものでなければならない。このためには、異なる視点にもとづく複数の安全対策が施されており、万一、１つの対策が破られたとしても、他の対策がこれに歯止めをかけられるような仕組みが必要である。例えば、「不正な行為自体が非常に困難であること」（事前対策）と、「もし不正が行われたとしても不正行為者を追跡するための情報を提供する仕組みが用意されていること」（事後対策）の２つの視点からの対策が考えられる。

（2）電子マネー特有の利便性

電子マネーは現在の現金を上回る利便性を実現する可能性を持っており、これが普及するための最大の誘因となると考えられる。例えば、現金同様に店頭での支払いが行えることはもちろんであるが、今後増加することが予想される電子商取引において利用できるように、インターネット等のオープンなネットワークを介して電子マネーを送れるようにすることが考えられる。また、取引時に両替えや釣銭の授受が不要なように必要金額ちょうどを支払えること（分割利用可能性）も特徴である。

1 「電子マネー」については未だ世間に認知された明確な定義は存在せず、人によってさまざまな捉え方をしているのが現状であるが、ここでは「現金と類似の機能を電子的に実現したもの」と考える。岡本・太田［1993］、中山［1996］、藤崎・岡本［1996］、森畠ほか［1997］における「電子現金」とほぼ同義。

（3）現金のメリットの継承

現在の現金には他の決済手段に比べて独特のメリットが多くあるが、世の中に受け入れられる電子マネーを設計するためには、現金のメリットをできるだけ多く継承することが重要と考えられる。

現金の大きな特徴としては、現金自体が価値を表章したものと考えられるため、使用にあたって与信チェックの必要もなく、信用力のない未成年も含めて誰にでも利用することができることがある。取引当事者間のみでその場ですべての処理を完結させることが可能（オフライン取引）なため、その支払いの目的や場所も限定されず、また、商店以外の利用者間で譲渡し転々と流通させることも可能（転々流通性）である。さらに、どの銀行から引き出しても、これを意識して区別することもなく同じように流通させることができる（複数金融機関対応）。

もう１つの現金の特徴は、誰がいつどこで何を買ったかといった購買履歴等の情報が残らないことであり、プライバシーが保たれるというところにある。なお、電子マネーにおいて実現されるプライバシー保護策は、必要なプライバシーのレベルによって以下の２つに分けられる。

(i) 利用者の購買履歴等の情報が小売店や金融機関が結託したとしても決して露見しないこと（追跡不能性）。

(ii) 誰が使用した電子マネーかが露見しないことはもちろん、個々の電子マネーが少なくとも同一の利用者によって使用されたものであると判断することすらできないこと（関連づけ不能性）。

以上をまとめると、電子マネーに対して要求される条件の候補としては、次のものがあげられる。

（安全性）

(a) 事前対策（コピー等の不正な行為が行えないこと等）

(b) 事後対策（不正が行われた場合不正者が発覚すること等）

（電子マネー特有の利便性）

(c) 分割利用可能性（保有する価値を任意の単位に分割して利用可能）

(d) 店頭・ネットワーク双方にて支払い可能（価値が情報のみで構成されるため、店頭での支払いはもちろんネットワーク経由での支払いも可能であること）

(e) 効率的な電子マネー発行管理（電子マネーの発行・管理を効率的に行い、発行コストを抑えるとともに、高速な処理を可能とすること）

（現金が持つメリットの継承）

(f) プライバシー保護

(f-1) 追跡不能性（利用者の購買に関するプライバシーが小売店や金融機関等が結託しても露見しないこと）

（f-2）関連づけ不能性（同一利用者により使用された電子マネー情報が相互に関連づけられないこと）

（g）オフライン性（第三者の介入を必要とせず取引当事者のみで支払処理が可能なこと）

（h）転々流通性（受け取った電子マネーをそのまま他への支払い等に使用可能なこと）

（i）携帯性（ICカード等の持ち運び可能な媒体で処理できること）

（j）複数金融機関対応（複数の金融機関が同一の電子マネーを扱えること）

2．代表的な電子マネー

これまでに発表された電子マネーは、1.で整理した要求条件をすべて満たしているわけではない。それぞれの電子マネーの間には使われるであろう場面・状況等の想定に差異があることから、個々の要求条件の重要度や優先度に対する考え方において異なる思想の下に開発されており、さらにコストとの兼ね合いもあって、必ずしもすべての条件を実現していない。今後実用化が進められるにあたっては、こうした異なる多くの電子マネーが競争することによってイノベーションが進むと考えられる。また、それぞれが持つ特徴によって、「棲み分け」が行われていくとの見方も多い。

BIS［1996］では、このような電子マネーの具体的製品について調査を行い、その特徴や機能に着目したうえで技術面でのリスクを分析しているほか、併せて、不正の防止、検出を行ううえでの信頼できるセキュリティ対策案についての提示を行っており、これらの点についての詳細についてはこちらに譲る。

理論面での研究では岡本・太田［1993］が、初めて電子マネーに対する要求条件を整理し、これが電子紙幣方式により実現できることを示した。さらに、藤崎・岡本［1996］の方式では、現在のICカードでの実装が可能となるように、これに改良を加えている。この方式は信用できる（電子マネー取引に関わらない）第三者を設けることでプライバシーを確保するとともに、電子マネーを流通させるにあたって通常のデジタル署名をベースとして採用したことで処理量、通信量を削減し、ICカードでの引出し／支払いを行えるよう設計されている。しかしながら、電子マネーの二重使用チェック等の発行管理処理の負荷が大きいという従来からの課題を解決していないほか、不正使用未然防止、複数金融機関対応などの条件を満足しているわけではない。

3．電子マネーの設計方針

今回設計する新しい電子マネーは、基本的には1.であげた要求条件をすべて満足させることを目標とする。具体的な設計に当たっては、藤崎・岡本［1996］を参考にし、さらに先に検討した電子マネーの要求条件を満たすために、新たに考案したアイデアを取り入れることにする。

なお、要求条件のうち、(b）不正者特定、(c）分割利用可能性、(d）店頭・ネットワーク双方にて支払い可能、(f）プライバシー保護、(g）オフライン性、(h）転々流通性、(i）携帯性、については、すでに藤崎・岡本［1996］が満たしており、以下の基本方針により上記以外の要求条件を満足させるように設計する。

（1）安全性

二重使用などの不正使用を防止する技術として、藤崎・岡本［1996］、Eng and Okamoto［1995］、Okamoto and Ohta［1990］などで用いられた暗号技術による不正者特定方式に加えて、電子マネーの取引を行う都度ICカードのセキュリティ機構を用いたチェックを行う方式を採用する。従来の電子マネー実現方式のうち、ゼロ知識証明を利用して電子マネーを支払う方式（Eng and Okamoto［1995］, Okamoto and Ohta ［1990］）では、引出し／支払い時の利用者側の演算量、データ量が多く、ICカードへの実装は不可能であった。そこで、藤崎・岡本［1996］と同様にデジタル署名を利用して電子マネーを支払う方式とすることにより、これを可能とする。

現在のICカードのセキュリティ機能はある程度の費用と時間をかければ破られる可能性がある。一方、事後対策のみでは「やり逃げ」型の犯罪のリスクがある。ICカードの耐タンパー性による事前対策と暗号技術による事後対策の二重の安全対策を実現しておけば、仮に攻撃者が巨額の費用をかけてICカードを解析・偽造しても、暗号技術による不正検出システムにより事後的に攻撃者の追跡が可能となるため、結果的に偽造等が露見し、攻撃自体を「引き合わない」ものとすることができる。なお、これらのセキュリティ対策は、利用環境（利用金額など）に応じて柔軟に組み合わせを変えることができるようにする。

（2）プライバシー保護

利用者は自らの利用者情報を開示する代わりに、登録機関が発行する登録書を提示することによって必要な認証を行い、電子マネーの支払処理を行う。登録機関のみがこの登録書を誰に対して発行したかを知りうる立場にあるため、これを取引に関わらない信用できる第三者に任せ、秘密を遵守させることによって追跡不能性を実現する。なお、必要があれば電子マネー引出しの都度、登録機関への再登録を行う運用を採ることによって、異なる電子マネー間での関連づけ不能性を実現可能とする。

（3）複数金融機関対応

電子マネー利用者の利便性や、効率的な電子マネーの発行・流通・還流を考慮して、複数の金融機関が同一の電子マネーを受入れ・払出すことを可能とする。具体的には、一般の金融機関（利用者が預金口座を持つ金融機関）とは別に、電子マネーを発行する専門の機関を設け、この発行機関を介して金融機関間の資金決済を実施することにより、同一の電子マネーを複数の金融機関で自由に取り扱うことを可能とする。利用者は、一般の金融機関に預金口座を持ち、そこから預金を引き落とす代わりに発行機関から電子マネーを受け取る。発行機関は、金融機関からの依頼を受けて利用者に電子マネーを発行し、金融機関経由で還流してきた電子マネーの不正使用チェックを一元的に行う。

（4）効率的な電子マネー発行管理

藤崎・岡本［1996］等従来の電子マネー実現方式では、利用者のプライバシーを保護する観点から、利用者の購買履歴を追跡不能とするため、ブラインド署名を利用して発行機関による認証を行うことで発行処理を行ってきた。ブラインド署名を用いた電子マネーの発行は、発行機関が電子マネー発行（署名作成）時に署名対象を知り得ないので、発行機関は自身が発行した電子マネーに含まれる識別番号を管理することができなかった。そこで、今回はブラインド署名を利用する範囲を利用者と金融機関の間だけに限定し、発行機関は通常のデジタル署名を利用する方法とする。

具体的には、利用者が金融機関にアクセスし電子マネーの引出しを要求するときは、実名や口座番号を明らかにしてから処理が行われるため、銀行がこれらの利用者情報と電子マネー情報を結び付けることを防止するためにブラインド署名を用いて、まず電子マネー発行依頼書を取得する。利用者は続いて発行機関にアクセスし、この銀行から取得した電子マネー発行依頼書のみを発行機関に送信し、実名などの情報を提示することなく電子マネーを取得する。このような手順を踏むことによって、発行機関は電子マネー情報と利用者情報を結び付けることが不可能となるため、通常のデジタル署名を用いても利用者のプライバシーは保護される。

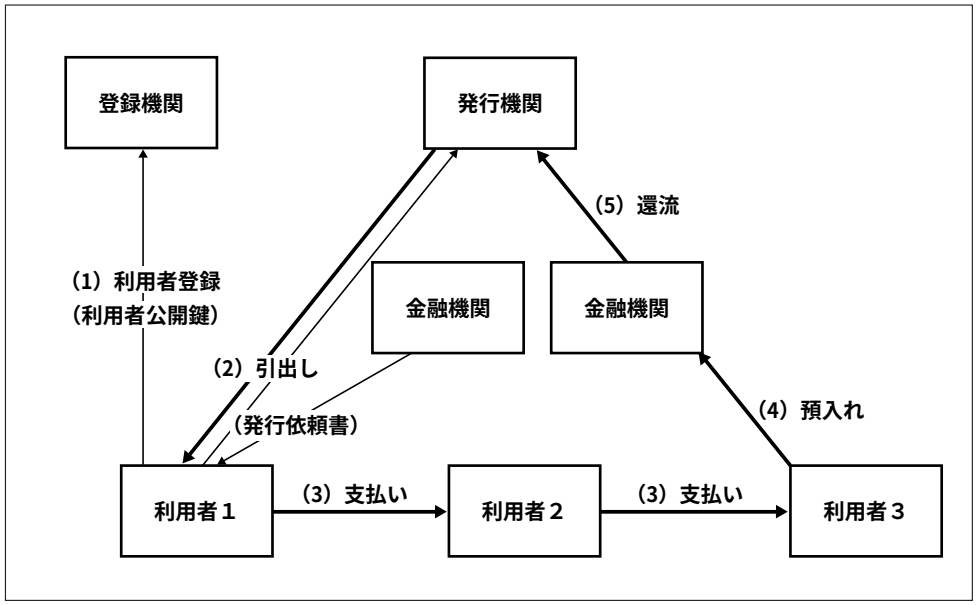
また、ここで発行機関は、発行した電子マネー情報を識別してデータベースに登録し、これが還流してきたところで消し込み処理を行うことによって不正検出を行う。つまり、もし、登録されていない電子マネーが還流してきたらこれを二重使用されたものと判断することができる。この場合、発行した電子マネーのうち、発行機関に戻ってきていない電子マネー情報のみをデータベースで管理すれば済むため、従来に比べ必要とされるデータベース量を大幅に削減することが可能となる。

4．電子マネー実現方式のプロトコル概要

3. の方針にしたがって電子マネーを構成する。以下に新方式の概要を述べる。図１に新方式の全体構成図を示す。図中で太線は電子マネーの流れを示す。

まず、各ノードの役割を説明する。登録機関は、利用者が電子マネーを使うにあたって、予め登録を行うための機関であり、利用者の正当性を保証するものである。発行機関は、電子マネーの「発行」、「管理」、「不正使用検出」を行う機関である。金融機関は、利用者の口座を管理する機関であり、利用者からの要求に応じて発行依頼書を発行する。利用者は、電子マネーの「引出し」、「支払い」、「預入れ」処理を行う。

図１　全体構成図

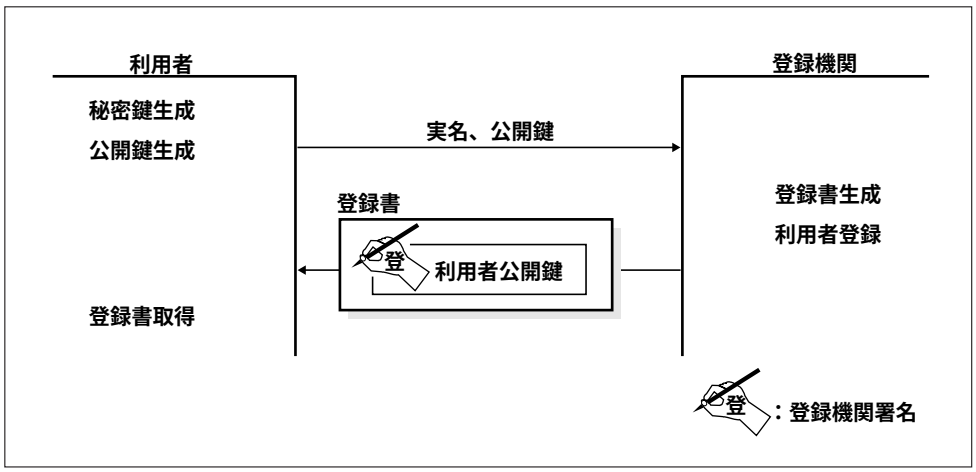


次に図に沿って全体の流れを説明する。

（1）利用者登録

利用者登録とは、電子マネーを利用する際に必要となる登録書を作成する部分であり、このプロトコルの流れを図２に示す。利用者は、まず署名生成のための秘密鍵および公開鍵を生成する。この秘密鍵／公開鍵のペアのうち、公開鍵と、利用者実名を登録機関に送信する。

図２　利用者登録プロトコル



登録機関では、受信した公開鍵と利用者実名の組を利用者登録データベースに登録し、公開鍵に対する登録機関のデジタル署名（以降、登録書という）を作成し、利用者に送信する。

以降で説明する支払いプロトコルにおいて、支払者は公開鍵と登録書を受領者に提示する。受領者は、登録書が支払者公開鍵に対する登録機関署名であることを検証することにより、支払者が登録機関に登録済の正当な利用者であることを確認することができる。一方、支払者は実名を明かすことがないので、支払者のプライバシーは守られる。

登録処理は、１.で示した要求条件のうち、「追跡不能性」を確保するためには、システムに参加するときただ一度だけ行えばよい。「関連づけ不能性」が必要な場合は電子マネー引出しの度に利用者登録を行う。

（2）電子マネー引出し

利用者が金融機関および発行機関へアクセスし、電子マネーを取得する部分であり、このプロトコルの流れを図３に示す。電子マネーの引出処理は利用者からみて、(i) 金融機関から発行依頼書を取得、(ii) 発行機関から電子マネーを取得、という２つのステップで行われる。

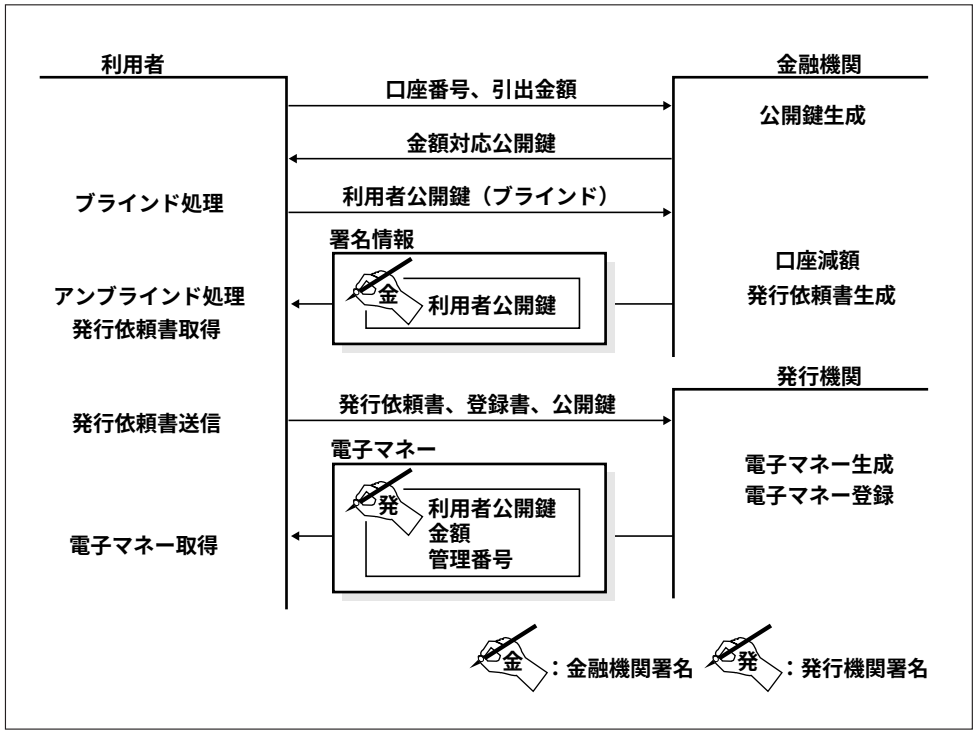
(i) 金融機関から発行依頼書を取得

利用者と金融機関は相互認証を行った後、利用者は口座番号、引出金額などを金融機関に送信する。金融機関は、引出金額対応の金融機関公開鍵を生成し、利用者に送信する。金融機関公開鍵を受け取った利用者はブラインド関数を用いて利用者公開鍵をブラインドし、金融機関に送信する。金融機関は、利用者の口座を引出金額だけ減額し、ブラインドされた利用者公開鍵に対する金融機関デジタル署名を作成し、利用者に送信する。利用者は受け取った金融機関デジタル署名をアンブラインドし、発行依頼書を取り出す。

(ii) 発行機関から電子マネーを取得

次に、利用者は発行機関にアクセスする。利用者は発行機関を認証した後、発行依頼書、登録書および利用者公開鍵を発行機関に送信する。これらの情報を受け取った発行機関は、署名が正しいことを検証し、電子マネー管理番号、発行金額および利用者公開鍵に対する発行機関デジタル署名を電子マネーとして生成し、電子マネー管理データベースに登録した後、電子マネーを利用者に送信する。

図3　引出しプロトコル

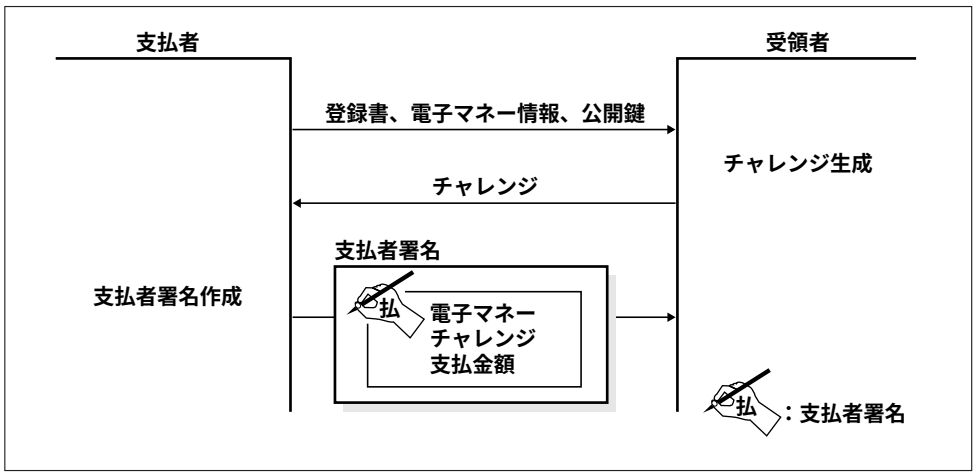


（3）電子マネー支払い

電子マネーの授受を行う処理部分であり、このプロトコルの流れを図４に示す。なお、電子マネーとは、当初は発行機関から引出した電子マネー情報だけを指すが、一度使用されると支払処理のやりとりを記録した履歴情報も電子マネーを構成する情報に付け加えられる。

支払者は登録書、支払者公開鍵および電子マネー情報を受領者に示す。受領者は登録書を検証することで支払者公開鍵が登録機関に登録された公開鍵であることを確認するほか、電子マネー情報が正しく構成されているかをチェックする(発行機関が正しい利用者に対して発行した電子マネーであるか、また、転々流通している電子マネーの場合は正しい譲渡手続きを経ているかを確認する)。次に受領者はチャレンジ情報として乱数情報および受領者の情報(実名および公開鍵を特殊処理したもの)を支払者に送信する。支払者は、チャレンジを含む必要な情報に対する支払者デジタル署名を作成し送信する。

図４　支払いプロトコル



（4）電子マネー預入れ

電子マネーを預け入れる処理は、（３）でやり取りされた情報（以降、電子マネー取引情報）を金融機関に送信することにより実現される。

（5）還流

還流処理は、金融機関が（４）で受け取った電子マネー取引情報を発行機関に送信することにより実現される。

（6）不正使用検出

発行機関には金融機関からすべての電子マネー取引情報と支払履歴情報が還流されてくる。電子マネー取引情報は発行時に生成された電子マネー管理番号ごとに管理される。まず、発行機関はこれらの情報のうち、電子マネーの使用額を抽出する。電子マネーが複数回に分けて使われた場合、各々の使用額の和を求める。電子マネー発行金額と使用額の和を比較し、等しくなった時点で電子マネー管理データベースから電子マネー関連情報を削除し、バックアップ用媒体に移す。電子マネー管理データベースに登録されていない電子マネーが戻ってきた場合、あるいは使用額が発行額を超えた場合は、不正使用が行われたものと判断する。

不正使用が行われた場合、電子マネー関連情報から利用者公開鍵を抽出し、不正者が生成した署名情報とともに登録機関に送信される。登録機関は、受信した公開鍵と対応づけられている利用者、すなわち不正者の実名を検索する。

5．本電子マネー実現方式の評価

本電子マネー実現方式が1.で述べた電子マネーの要件を満たしていることを示すために整理したものを表1に示す。

表1　本電子マネー実現方式の評価

要件			本方式での対処
安全性	事前対策		ICカードの耐タンパー性を利用した偽造等の未然防止
	事後対策		デジタル署名等の暗号技術による偽造防止、不正者追跡
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		暗号技術により電子マネーを情報のみで構成しているほか、処理をICカードで行うため、店頭での支払いはもちろんネットワーク経由での支払いの両方を実現
	効率的な電子マネー管理		発行済み未還流電子マネーをデータベースで管理し、還流時に消込み処理を行う方式にすることで電子マネー管理データベースのデータ量を抑制
現金が持つメリットの継承	プライバシー	追跡不能性	登録機関の設置およびブラインド署名利用で利用者プライバシーを保護
		関連づけ不能性	必要があれば、電子マネー引出しごとに登録処理を行い、異なる登録書を使用する運用を行うことで実現可能
	オフライン性		支払時、当事者間（支払者、受領者）で署名情報などを確認することにより電子マネーの授受を実現
	転々流通性		利用者の署名の連鎖により譲渡を可能とし、転々流通性を確保
	携帯性		ICカード等で支払い／受取り可能な処理量、データ量
	複数金融機関対応		発行機関と金融機関を分離することによって、複数金融機関で同一の電子マネーを取扱い可能とした

参考文献

岡本龍明・太田和夫、「理想的電子現金方式の一方法」、『電子情報通信学会論文誌』、J76-D-I、No. 6、pp. 315-323、1993年

中山靖司、「電子決済について」、『ITUジャーナル』、Vol 26、No. 7、pp. 54-62、新日本ITU協会、1996年

藤崎英一郎・岡本龍明、「エスクロー電子現金」、『電子情報通信学会論文誌』、IT95-51、ISEC95-46、SST95-112、pp. 7-12、1996年

森畠秀実・阿部正幸・藤崎英一郎・中山靖司、「電子現金方式」、『暗号と情報セキュリティシンポジウム'97』、SCIS97-3C、1997年

Abe, M. and E. Fujisaki, “How to Date Blind Signatures,” Advances in Cryptology-ASIACRYPT'96, LNCS 1163, pp. 244-251, Springer-Verlag, 1996.

————, and Camenisch, J., “Partially Blind Signature Schemes,” 暗号と情報セキュリティシンポジウム'97, SCIS97-33D, 1997.

BIS, “Security of Electronic Money,” Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries, Aug. 1996.（日本銀行電算情報局訳、『電子マネーのセキュリティ』、ときわ総合サービス、1997年）

Brands, S., “Untraceable Off-line Cash in Wallet with Observers,” Advances in Cryptology- Proc. of CRYPTO'91, LNCS 773, pp. 302-318, Springer-Verlag, 1993.

Chaum, D., “Security Without Identification: Transaction Systems to Make Big Brother Obsolete,” Communications of the ACM, Vol. 28 No.10, pp. 1030-1044, 1985.

————, A.Fiat and M.Naor, “Untraceable Electronic Cash (Extended Abstract),” Advances in Cryptology- Proc. of CRYPTO'88, LNCS, No. 403, Springer-Verlag, pp. 328-335, 1989.

Eng, T. and T. Okamoto, “Single-Term Divisible Electronic Coins,” Proc. of EUROCRYPT '94, LNCS 950, pp. 306-319, Springer-Verlag, 1995.

Even, S., O. Goldreich and Y. Yacobi, “Electronic Wallet,” Proc. of CRYPTO'83. A later version appeared in Proc. of 1984 International Zurich Seminar on Digital Communications, pp. 199-201, IEEE cat No. 84CH1998-4, 1984.

Matsumoto, T., “An Electronic Retail Payment System with Distributed Control - A Conceptual Design -,” *IEICE Trans. Fundamentals*, Vol. E78-A, No. 1, 1995.

Okamoto, T. and K. Ohta, “Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducibility,” Advances in Cryptology-EUROCRYPT'89, LNCS 434, pp. 134-149, Springer-Verlag, 1989.

————, and————, “Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash,” Advances in Cryptology- Proc. of CRYPTO '89, LNCS 435, pp. 481-496, Springer-Verlag, 1990.

————, and————, “Universal Electronic Cash,” Advances in Cryptology-CRYPTO'91, LNCS 576, pp. 324-337, Springer-Verlag, 1991.