IMES DISCUSSION PAPER SERIES

電子マネー技術と特許

中山　靖司

Discussion Paper No. 98-J-33

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒100-8630 東京中央郵便局私書箱 203 号

IMES Discussion Paper Series 98-J-33
1998 年 12 月

電子マネー技術と特許

中 山 靖 司

要 旨

インターネットの普及に伴い、インターネットを利用してビジネスを行う「電子商取引」に対する期待が高まり、そこで利用される決済手段として電子マネーが注目を集めている。世界各国で、電子マネーの実用化に向けた様々な試みが行われ、わが国でも大規模な実証実験が進められている。IC チップ・モジュールをプラスチック・カードに埋め込んだ IC カードを利用し、そこに格納された電子的な情報を利用して店頭での小口決済に利用するという構想については、従来から様々な実験が繰り返されてきた。しかし、現在試みられている電子マネーのプロジェクトの中には、従来のものとは異なり、店頭での支払いという機能に加えて、インターネット上で「電子商取引」を行うための手段としても提案されるものが出てきている。

電子マネーは、情報セキュリティ技術（暗号技術）をはじめとした様々な技術の統合によって実現される。優れた技術を使うことによって、安全で便利な電子マネーを提供することは、実用に供する電子マネーを実現するためには重要なことであるが、これらの技術の中には、特許が取得されているものも存在する。電子マネーを実用化していくうえでは、こうした特許の存在に配慮する必要があり、現在、電子マネーに関する技術が特許によってどのように保護されているかについて分析し、特許の存在による影響について検討しておくことは重要なことである。

本稿では、まず、電子マネーを実現するために必要な技術にはどのようなものがあるかを整理したうえで、特に「電子マネー・スキーム技術」に焦点をあてて、その技術の系譜や相互の関連について解説する。次に、電子マネー特許に関する特許法の問題についての研究に繋がるよう、既に特許が成立している主要な電子マネー特許について、そのクレーム（請求の範囲）を中心に分析・整理し、実際にどのようなクレームが認められているかを明らかにする。

キーワード： 電子マネー、特許、クレーム、電子現金、暗号、IC カード
JEL classification: K11、L86、L96、O34

*日本銀行金融研究所研究第 2 課（E-mail: yasushi.nakayama@boj.or.jp）

本論文を作成するにあたっては、相澤英孝助教授（早稲田大学）から有益なコメントを頂戴した。

目　次

頁

Ⅰ． はじめに

インターネットの普及に伴い、インターネットを利用してビジネスを行う「電子商取引」に対する期待が高まり、そこで利用される決済手段として電子マネーが注目を集めている。世界各国で、電子マネーの実用化に向けた様々な試みが行われ、わが国でも大規模な実証実験が進められている。従来から、特定のビルや商店街、大学構内などに限定して提供される決済サービスとしての小規模なICカード実験は数多く行われていた。しかし、現在試みられている電子マネーのプロジェクトの中には、従来のものとは異なり、店頭での支払いという機能に加えて、インターネット上で「電子商取引」を行うための手段としても提案されるものが出てきている。電子商取引という新しいニーズが発生したことに伴って、従来の技術先行的なICカード実験とは異なり、電子マネーの新しい可能性が期待されるようになってきた。最近行われている多くの実証実験は、利用できる地域を広げて十万人規模の参加者を募ったり、インターネット上での支払手段としても使えるよう利便性を高めるなど、単なる実験にとどまらず、実用化を強く意識するようになっている。

電子マネーは様々な技術が組み合わされることによって実現される。例えば、取引相手の認証や電子マネーを構成するデータの真正性の確保等のためには暗号技術が、電子マネーの受渡し等の取引にはインターネット等の各種通信技術が、また、ICカード型電子マネーにおいて複製を防止したりデータの携帯性を確保するためにはICカード技術が使われている。また、これらの個々の技術をいかに組み合わせて電子マネーシステムを設計するかということも重要な技術である。

こうした電子マネー関連技術についても、他の技術同様に特許出願を行い、特許を取得しようとするケースが増えてきている。こうした状況下、電子マネーを本格的に実用化していく際には先行する特許に配慮することが当然必要となる。しかしながら、電子マネーは新しい技術であるため特許庁における審査蓄積が少なく、また、関連する判例も少ないため、特許法による保護についての法律的取扱いが明確ではなく、学会における検討も十分になされているとは言い難い。そのため、電子マネーについての特許が認められるか、認められるとしてもどのようなクレームで認められるか、あるいはどのような保護が与えられるか、が明らかではなく、関係者の注目を集めている。今後、電子マネーが本格的に普及してくると、こうした電子マネーの特許を巡る問題が重要となると考えられるが、この問題を検討するためには、まず、実際にどのような電子マネーが特許として認められているかを整理し、それらの特許の効力やその保護の範囲について分析することが有用であろう。

そこで、本稿では、電子マネー技術を概観したうえで、いくつかの代表的な電子マネーに関する特許を取上げて、その内容を整理・分析することにする。まず、第Ⅱ章において電子マネー関連技術にはどのようなものがあるかを整理し、特に本論文で焦点をあてて取上げる「電子マネー・スキーム技術」の位置づけを明らかにする。次に、第Ⅲ章で、この「電子マネー・スキーム技術」をその技術的系譜によって３つに分類し、それぞれについ

て研究・開発がどのように進められたかをフォローしつつ、電子マネーの技術的な内容を概説する。第IV章では、それぞれの分類に属する主要な特許を取上げ、実際にどのようなクレームが発明として認められているのか、また、技術の開示はどのように行われているのか等を明らかにする。但し、取上げる特許の内容については、クレームに記載されている事実を指摘するに止め、その効力の範囲に関して著者自身の価値判断を行っていない。最後に、第Ⅴ章でまとめを行っている。

なお、本稿では「電子マネー」[1]のうち、特に「ストアードバリュー型」の電子マネーを議論の対象とすることにする[2]。

[1] 「電子マネー」という言葉は、様々な電子決済方法を表すものとして多義的に用いられるが、ここでは「商店の店頭からインターネットまで、オープンな環境下での資金決済に利用されることを目的として、暗号や IC カードなどの技術を利用して構成された新しい決済サービス」と考える。こうした決済サービスは、「ストアードバリュー型」と「アクセス型」に分類することができる。「ストアードバリュー型」の電子マネーとは、利用者の保持する電子機器に記録されたディジタル・データがそれ自体「価値」を有するものとされ、これを交換または増減することにより決済を行うものである。一方、「アクセス型」の電子マネーとは、利用者が決済のための「価値」の移転を第 3 者に対して指図する場合にその指図を電子的機器や通信機器を通じた電子的な方法により行うものであり、たとえば、インターネット上で安全にクレジットカード取引を行うサービスや、紙の小切手による取引をディジタル署名技術によって実現する「電子小切手」、銀行口座をインターネット経由で指図する「インターネットバンキング」等がある。

[2] アクセス型の電子マネーは、既存の決済制度の枠組みを活用している分、実用化は比較的容易であると考えられるのに対して、ストアードバリュー型電子マネーは、既存の制度を本質的に変化させる可能性を秘めた革新的なアイデアであるため、「ストアードバリュー型」の電子マネーを本稿の議論の対象とする。

Ⅱ． 電子マネー関連技術

実際に電子マネーを実現するのには、多岐に亘る様々な技術を統合することが必要である。電子マネーを可能にするための技術としては、暗号技術に加え、IC カード関連の実装技術（安全性を高める耐タンパー技術他）、インターネット等の情報通信技術があげられる。また、電子マネーは単体で存在するだけでは機能できず、発行機関、金融機関、CA（Certification Authority:認証機関）等の間での業務の進め方（ビジネス・スキーム）が周到に考えられてはじめて機能するものである。どのようにビジネス・スキームを考え、これを技術的にシステムとして実現するかということも一種の技術といえる。さらに、このようなシステムを構築するためのコンピュータ機器等のハードウェア技術やプログラム等のソフトウェア技術も欠くことのできないものである。

以下は、こうした電子マネー関連技術を 4 つの側面から分類・整理する。

(1) 基礎暗号技術

電子マネーで利用される代表的な暗号として、「共通鍵暗号」、「公開鍵暗号」、「ディジタル署名」、「ブラインド署名」等が挙げられる。「共通鍵暗号技術」や「公開鍵暗号技術」は、他者には漏洩しては困るデータ（秘密鍵、暗証番号等）を通信回路に流したり、IC カードに格納したりする際に、こうしたデータの機密性を確保するために使われる。「ディジタル署名」は電子マネーが真正な発行機関によって発行され、取引における正規の手続を経て流通しているものであって、偽造・変造されたり、二重使用[3]されたものではないことを保証するために使われる。電子マネー自体に発行機関の「ディジタル署名」を付けることによって正当な発行機関によって発行されたものということが証明できるほか、受渡しの履歴情報に支払者が「ディジタル署名」することによって、取引における正規の手続を経て使用されたものであることが確認できる。また、電子マネーに匿名性を与えるための特殊なディジタル署名技術として「ブラインド署名[4](blind signature）」が使われ

---

[3] 本稿では、偽造とは電子マネーを不正に作成すること、変造とは正規の電子マネーの額面情報等を不正に改変すること、二重使用は正規の電子マネーを不正に複数回使用することと区別している。

[4] ブラインド署名とはディジタル署名の応用技術であり、署名依頼者が署名者にデータの内容を知られることなく署名を受ける方法であり、電子マネーにおいて追跡不可能性を実現するための基本的な技術である。RSA 法に基づくブラインド署名のほか、ゼロ知識対話証明に基づくブラインド署名等が提案されている。具体的な手順としては、①署名対象を署名者にわからないように撹乱する「ブラインド前処理」、②署名者による「ディジタル署名」、③撹乱を解いて必要な署名のみを取出す「ブラインド後処理」の３つの手順から成り立つ。以下に、RSA 法によるブラインド署名の基本手順を、署名依頼者 A が文書 M に署名者 B のブラインド署名を受ける場合で示す。なお、署名者 B の RSA 暗号の公開鍵を(e,n)、秘密鍵を d とする。

①署名依頼者 A は秘密の乱数 r を生成した後、署名者 B の公開鍵(e,n)を用いて $X = Mr^e \bmod n$ を計算し、結果 X を B に送信する。

②B は自分の秘密鍵(d,n)を用いて $Y= X^d \bmod n= M^d r \bmod n$ を計算し、結果 Y を A に送信する。

③A は受け取った Y に秘密の乱数の逆数 r^{-1}（$r \cdot r^{-1} \bmod n =1$ を満たす整数）をかけること

ることもある。

このように、暗号技術なくして電子マネーは成り立たないといえるほど、電子マネーにとって暗号は大変重要な技術である。なお、この電子マネーで用いられる基礎暗号技術と特許については、相澤・宇根・楠田 [1998][5]が詳しくまとめている。

(2) 電子マネー実現方法（およびその装置）に関する技術

電子マネーを実現するための、システム・デザイン方法に関するものであり、電子マネーシステムの構成要素、各要素の管理情報、処理内容、処理手順のほか、使用する基礎暗号技術およびその適用の仕方等、どのような技術を組み合わせ、いかに処理を行えば電子マネーが実現できるかに関する技術である。暗号学者の間で電子マネープロトコルと呼ばれているものがこれに該当する。電子マネーの種類によっては、ハードウェアと技術的に不可分な実現方法もあり、実際に処理を行うハードウェア装置も含めて、電子マネー実現方法に関する技術と考えられる。さらに、電子マネーに関するビジネス・スキームのアイデアをもとに、これをシステムとして技術的に実現するための方法も含まれる。Even, Goldreich, Yacobi が考案した IC カード間の価値移転の方法、Chaum の ecash の仕組み、あるいは日本電信電話(株)の「理想的電子現金方法」に関する一連の研究[6]のほか、Citibank, N. A.の EMS[7]に関する発明がここに含まれると考えられる。これらは、電子マネーを実現するためにのみ開発された技術である。

(3) 実装関連技術／基盤技術

電子マネーを構築するためには、机上の理論研究とは異なり、実際の機器を用いて、数々の制約条件の下で実装を行う必要がある。このために必要な技術としては、例えば IC カード[8]等の媒体に関する技術（耐タンパー技術を含む）や情報通信に関する技術のほか、コンピュータ技術、プログラミング関連技術（乱数の生成、べき乗・剰余などの高速演算、素数探索等）といった各様々な分野に亘るものが挙げられる。

なお、これらは(1)基礎暗号技術同様、必ずしも電子マネーのためだけのものではない汎用的な技術である。

により B の署名 $S = M^d \bmod n$ を得、署名 S の正当性を B の公開鍵により $M = S^e \bmod n$ と検証する。

[5] 相澤英孝・宇根正志・楠田浩二、「暗号と特許」、『ディスカッションペーパーシリーズ』、98- J-8、日本銀行金融研究所、1998 年

[6] 日本電信電話（株）における暗号研究の一環であり、電子現金を実現する方法に関する研究である。理想的な電子現金が備えるべきと考えられる 6 つの条件（後述）をあげ、これを実現する様々な方法を研究している。

[7] EMS(Electronic Monetary System): Citibank, N. A.が開発した電子マネーに関する発明のことである。

[8] ブル社（仏）のプログラマブル IC カード基本特許（特願昭 53-102790：1990 年 4 月 23 日登録）等。

(4) その他運用関連技術

電子マネーを実際に運用するときの仕組みや工夫等に関するもので、技術というよりは、どちらかというと取り決めに近い性格を持ったアイデアも含まれる。例えば、電子マネーの偽造等を早期に発見するための電子マネーの発行・還流過程を監視し、統計的に分析する方法や MONDEX で安全性を高めるために採用されているとされるセキュリティ・マイグレーション（Security Migration）[9]、フロー・コントロール（Flow Control）[10]等のアイデアがこれに該当する。

(1)～(4)はいずれも、電子マネーにとって重要な技術ではあるが、本稿では電子マネーシステムを実現するための基本的な技術（以後：電子マネー・スキーム技術）として、主に(2)の電子マネー実現方法（およびその装置）に関する技術を検討の対象とする。

[9] セキュリティ･マイグレーション（Security Migration）： IC カードの中に常に 2 世代分のセキュリティ・スキーム（カード発行時に有効なスキームと将来切り替えて使う予定のスキーム）を内蔵しておき、一方のセキュリティ・スキームの安全性が薄れたところでこれを無効にし、他方に切り替えることによって、セキュリティ・スキームの切り替えをスムーズに行う方法である。

[10] フロー・コントロール（Flow Control）：顧客と顧客、顧客から商店、商店から銀行、銀行から発行銀行といった電子マネーを移転する方向、取引者の属性によって、予め移転可能な上限金額を設定し、不自然な資金の移転を禁止することによって、不正を防止する仕組みである。

Ⅲ.　電子マネー・スキーム技術の系譜

電子マネー・スキーム技術は、その発想の起源、あるいは研究・開発のアプローチの仕方等により、次の３つ技術的系譜に分類することができる。

①暗号理論研究から派生した技術

暗号理論の応用事例の１つとして暗号学者によって理論的に研究されてきた電子マネーに関する技術であり、暗号処理を施したデータを物理的な現金等の代わりに受渡すことによって、保有する価値の移転を可能とするものである。電子現金、あるいは電子証書型電子マネーなどとも呼ばれる。なお、実際にこれを実用化するためには、さらに実装するための技術の研究やこれに合せたビジネス・スキームの検討が必要となる。

②実装技術研究から生まれた技術

①が暗号理論研究の延長線上にある研究から派生した技術であるのに対し、これは電子マネーシステムを開発することを目的に始まった研究で生まれた技術である。多くの場合、IC カードや取引装置等の物理的構成機器を前提に暗号技術を組み合わせ、現実に実装することを考慮しながら研究されたものであり、IC カード型の電子マネープロジェクトにおける電子マネーの多くは、これに属すると考えられる。なお、実際にこれを実用化するためには、具体的に適用する暗号技術の研究やこれに合せたビジネス・スキームの検討も必要となる。

③ビジネスの方法としてのアイデアを実現する技術

新たな金融商品、金融サービスの１つと位置づけられる電子マネーのビジネス・スキームに関するアイデアを、システムとして技術的に実現する具体的な方法等に関する技術である。構成要素およびその機能、あるいはビジネス・フロー等に関するアイデアを基に、どのような手段、方法を用いて、どのような手順で処理を行えばこれを実現できるか等といった具体的な技術的思想を含んだものである。なお、実際にこれを実用化するためには、具体的に適用する暗号や実装技術の研究等が必要となる。

以下では、これらの３種類の分類に則して説明する。

1. 暗号理論研究から派生した技術（電子証書型電子マネー）

(1) 電子証書型電子マネーの基本的な考え方

貨幣や紙幣といった有体物の代わりに、電子的にやり取りされるデータを用いて決済を行うというアイデアは、もともと暗号学者による学術的な暗号研究の一環の中で生まれてきたものである。これらは、公開鍵暗号やディジタル署名方式の応用例として考えられたものであり、電子証書型（note-based model）電子マネーあるいは電子現金[11]などと呼ばれている。個々の電子マネー（電子証書）にユニークな番号が付与されており、同じ額面のものであっても区別できることが特徴である。実際に実用化するためには、さらに実装技術の研究、これに合せたビジネス・スキーム等の検討が必要ではあるが、この電子マネーを実現する理論的研究自体が暗号分野の学術論文として、学会等の場で活発に発表されており、安全性等について研究者の間で客観的な評価を受けてきた技術である。

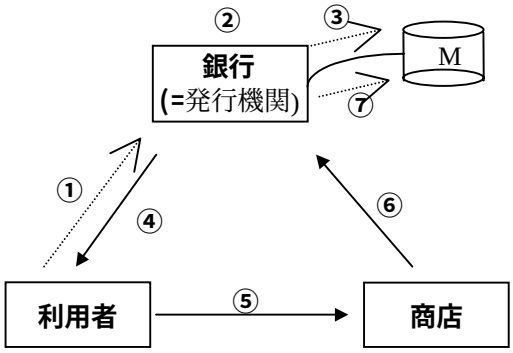
これらの技術の基本的な考え方は、電子マネーであることを表すデータに対して電子マネー発行機関がディジタル署名したものを電子証書（電子紙幣）として扱うというものである。銀行の顧客は、検証鍵によって発行機関の署名を検証することによって正規の電子証書であることを確認することができる。電子証書たるディジタル署名は、電子マネー発行用の署名鍵を知る発行機関にしか生成することができず、不正行為者が偽造、変造することは非常に困難であることによって、その価値が保証されている。ただし、データ自体はコピーすることが容易であり、そのコピーはオリジナルとまったく区別がつかないため、これだけでは同じ電子証書を繰り返し何度も使用するという不正行為を防ぐことができない。そこで、個々の電子証書に埋め込んであるユニークな識別番号（銀行券の記番号に相当）を発行機関に登録しておき、使用される都度、まだ１回も使われていない電子証書であることを発行機関にオンラインで問合せることによって、二重使用を防ぐ方法が考えられた。これは「オンライン検証型電子マネー」と呼ばれる基本的な考え方（図１参照）であるが、発行機関がどの利用者に対して何番の電子証書を発行したかを知りうる立場にあるため、現金の主要な特徴であるプライバシー[12]を備えているわけではない。

---

[11] 暗号学者の発表する論文では、電子マネーのことを電子現金と表現することが通例である。また、電子証書についても、電子コイン、あるいは電子紙幣と呼ぶことも多い。

[12] ここでいうプライバシーとは、利用者がいつ何処で、何を購入したかといった購買履歴が誰にも知られることがないということであり、匿名性ということも多い。追跡不可能性と同じ意味でも使用される。

（図１）簡単なオンライン検証型電子マネーの処理方法



①利用者は、銀行（＝発行機関）にアクセスし、自分の口座からα円の引き出しを要求する。
②銀行は、利用者の口座からα円を減額し、金額α、識別番号 M 等のついた電子署名を作成する。
③この作成した電子署名を識別番号 M とともに、データベースに登録する。
④電子署名をα円の電子証書として利用者に送付する。
⑤利用者は、α円の決済手段として、この電子証書を商店に送付する。
⑥商店は、受け取った電子証書の署名をチェックのうえ、未使用かどうか銀行に問合せを行う。
⑦銀行は、商店から照会された電子証書がデータベースに登録されているか識別番号 M をインデックスキーにしてチェックする。登録されていれば未使用の電子証書と判断し、これをデータベースから消去するとともに商店の口座をα円増額する。登録されてない場合は使用済みの電子証書と判断し、商店は受取りを拒否する。

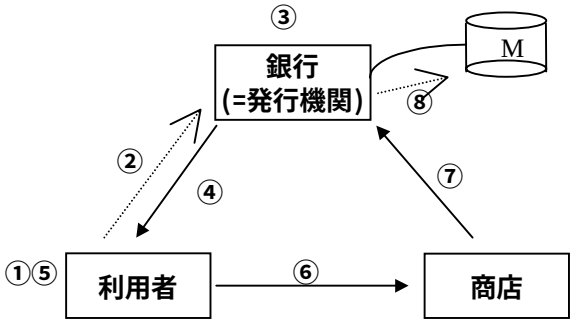
(2) 匿名性を持った電子証書型電子マネーのアイデア

―― *プライバシーを保持しつつオフライン性を持つ電子マネー*

D. Chaum は 1985 年、この基本的なオンライン検証型電子マネーのスキームをもとに、ブラインド署名等の暗号技術を採用することによって、現金の大きな特徴の１つである匿名性を備えた電子マネーを論文で発表している（Chaum [1985][13]）。具体的には、発行機関が電子証書の識別番号を知ることのないように、利用者が識別番号を含む署名対象情報を作成し、これに発行機関がブラインド署名することによって電子マネーの発行処理を行うように処理手順が改良されている（図 2 参照）。ただし、このようなブラインド署名を使用した電子マネーでは、発行機関が識別番号を知り得ないために、発行時にこれをデータベースに登録することができない。そのため、電子マネー使用時のオンラインチェックにおける電子証書の二重使用の判断法が、発行機関のデータベースに識別番号が登録されていなければ未使用とみなしてはじめて登録を行い、逆に登録されているときは既に使用済みと判断するように変更されている。DigiCash 社の ecash は、この考え方をもとにインプリメントされているとされ、1994 年 12 月よりインターネット上で希望者によるフィー

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

（図 2）匿名性のあるオンライン検証型電子マネーの処理方法



(e, n)：銀行公開鍵(α円)
(d, n)：銀行秘密鍵(α円)
R ：乱数
h(・) ：一方向性関数

①利用者は、銀行（＝発行機関）にわからないように、識別番号 M を含む署名対象を準備し、ブラインド前処理を行う。

$X = h(M)\ R^e \bmod n$

②利用者は、銀行にアクセスし、ブラインド前処理された署名対象(X)を送付し、自分の口座からα円の引き出しを要求する。

③銀行は、利用者の口座からα円を減額し、ブラインド前処理された署名対象に対してα円の電子署名(Y)を行う。

$Y = X^d \bmod n = h(M)^d\ R \bmod n$

④銀行は、電子署名(Y)を利用者に送付する。

⑤利用者は、銀行から受け取った電子署名をブラインド後処理して識別番号 M を含む署名対象に対する銀行の電子署名を取り出し、これを電子証書として保管する。

$S = Y/R \bmod n = h(M)^d \bmod n$

⑥利用者は、α円の決済手段として、この電子証書を商店に送付する。

⑦商店は、受け取った電子証書の署名をチェックのうえ、未使用かどうか銀行に問合せる。

⑧銀行は、商店から照会された電子証書がデータベースに登録されているか識別番号 M をインデックスキーにしてチェックする。登録されていなければ未使用の電子証書と判断し、データベースに追加するとともに商店の口座をα円増額する。既に登録されている場合は使用済みと判断し、商店は受取りを拒否する。

ルドテスト（現実のマネーとのリンクは無し）を実施したことで知られている。もっとも、この方法では、過去に使用された電子マネーすべてを発行機関のデータベースに登録しておくことが必要となり、そのままではデータベース容量が肥大化することが欠点としてあげられる。

さらに、これに改良を加え、発行機関にオンラインで問合わせることなく、オフラインでも安全に電子マネーの支払いを行えるようにしたのが、Chaum, Fiat, Naor [1988][14]であり、電子証書型の電子マネーの元祖（オフライン検証型電子マネー）ともいうべきものである。電子マネーを受け取った商店がこれを銀行に還流させる時点で事後的な二重使用のチェックを行い、二重使用があったことが判明した場合にはその不正行為者が誰なのか追跡できる仕組みを設けることことによって安全性を確保している（図 3 参照）。具体的には、電子証書自体に通常では決して露見することのない利用者の ID 情報を埋め込んでおき、二重使用が行われた場合に限り、この 2 つの電子証書の情報からかなりの高確率で不正を

[14] D.Chaum, A.Fiat, M.Naor, “Untraceable Electronic Cash (Extended Abstract),” Advances in Cryptology-CRYPTO’88, LNCS, No.403, Springer-Verlag, pp.328-335, 1989.

行った利用者の ID が露見する仕組みを組み込んだものであり、カット・アンド・チューズ技法[15]を使用している。「二重使用を行うと事後的に不正行為者が露見する」ということによる抑制効果によって二重使用を防ぐ仕組みとなっている。

なお、オフライン環境下でも二重使用を防ぐ仕組みとしては、IC カード等の耐タンパー装置[16]に処理を行わせることによって、不正行為のおよぶ余地をなくす方法も Brands 等によって提案されている（Brands [1993][17]）。

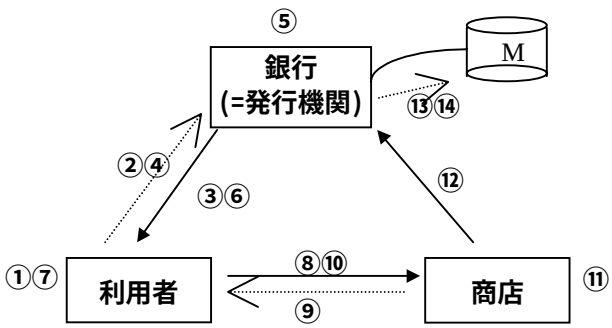
[15] カット・アンド・チューズ技法とは、例えばケーキを 2 人で切分ける際に、一方がケーキを 2 つに切り（カット）、もう一方が切分けた２つの候補から選択する（チューズ）ことによって、公平に配分を行う方法をいう。ここではブラインド署名をする際、署名対象が正しく作成されているかを確認する方法として応用されている。具体的には、署名依頼者は本来必要な署名対象を複数作成しておき、署名者はこのうち任意のものを選択して開示を求め、署名対象が正しく作成されているかを確認し、問題なければ他の未開示の署名対象に対して署名を行うという手順となる。

なお、二重使用を行った不正行為者検出する技法としては、Chaum, Fiat, Naor [1988]のように「カット・アンド・チューズ」技法と衝突回避関数の性質を組み合わせる方法のほか、「カット・アンド・チューズ」技法とゼロ知識対話証明の性質を組み合わせる方法、「カット・アンド・チューズ」技法と「合成数を法とする平方根」の性質を組み合わせる方法、「制約付きブラインド署名」技法と離散対数問題（DLP）に基づくゼロ知識対話証明の性質を組み合わせる方法、等がよく知られている。なお、カット・アンド・チューズ技法では安全性を高めるためにはデータサイズが大きくなるという制約があったが、これを用いない方法は「シングル・ターム」方式と呼ばれ、データサイズや計算量が小さく効率的である。

[16] 耐タンパー装置とは、ハードウェアの内部に保管されている情報を不正な手続等によって盗み出そうとすると、自動的にその情報が消去されたり、ハードウェアが破壊されたりして、情報を盗み出せないような機構を持った装置である。

[17] S.Brands, “Untraceable Off-line Cash in Wallet with Observers,” Advances in Cryptology-CRYPTO’91, LNCS 773, pp.302-318, Springer-Verlag, 1993.

（図 3）オフライン検証型電子マネーの処理方法



(e, n)：銀行公開鍵(α円)
(d, n)：銀行秘密鍵(α円)
Ri ：乱数
f(・) ：一方向性関数
g(・) ：一方向性関数
ID ：利用者の識別子

①利用者は、乱数 Mi (i=1,･･･,k)を発生し、ブラインド前処理をした Xi (i=1,･･･,k)を準備する。

$$Xi = f(g(Mi), g(Mi+ID)) Ri^{e} \bmod n$$

②利用者は、銀行にアクセスし、$(X_1,\cdots,X_k)$を送付するとともに、自分の口座からα円の引き出しを要求する。

③銀行は、提示された Xi のうち、ランダムに K/2 個を選び、利用者にそれぞれが計算に使った情報を開示するよう要求する（以下では説明をわかりやすくするため、k/2+1, k/2+2, ･･･, k が選択されたものとして扱う）。

④利用者は、指定された Mi, Ri (i = k/2+1, k/2+2, ･･･, k)を銀行に送信する。

⑤銀行は、 $f(g(Mi), g(Mi+ID)) Ri^{e} \bmod n$ を計算し、先に送られた Xi が正しく計算されているかどうか検査する（検査が不合格のときは取引を中止する）。全てに対し検査が合格の場合、利用者の口座からα円を減額し、開示されていない Xi に対し、一括してα円の電子署名(Y)を行う。

$$Y = [\Pi X_i (i=1,k/2)]^{d} \bmod n = [\Pi\{f(g(Mi),g(Mi+ID)) Ri^{e}\}(i=1,k/2)]^{d} \bmod n$$

⑥銀行は、電子署名(Y)を利用者に送付する。

⑦利用者は、銀行から受け取った電子署名をブラインド後処理して、これを電子マネーとして保管する。

$$S = Y/[\Pi Ri(i=1,k/2)] \bmod n = [\Pi\{f(g(Mi),g(Mi+ID))\}(i=1,k/2)]^{d} \bmod n$$

⑧利用者は、α円の決済手段として、この電子マネーを商店に送信する。

⑨商店は、{0, 1}に属する乱数 e_i(i=1,k/2)を発生させ、利用者に送信する。

⑩利用者は、ei=0 のときは Mi と g(Mi+*ID*)を、ei=1 のときは g(Mi)と Mi+*ID* を商店に送信する。

⑪商店は、利用者から受け取った情報から f(g(Mi),g(Mi+*ID*))を計算し、以下を検証して合格ならば電子マネーを受け取る。

$$S^{e} \equiv [\Pi\{f(g(Mi),g(Mi+ID)) Ri^{e}\}(i=1,k/2)] \bmod n$$

⑫後に商店は、利用者の支払履歴(H)をすべて銀行に送信する。

⑬銀行は受け取った履歴の正当性を検証する。合格であればこの電子マネー(S)を履歴(H)とともにデータベースに登録し、商店の口座をα円増額する。

⑭二重使用が見つかった場合（電子証書が既に登録されている場合）、同一の電子証書に対して 2 つの履歴が存在するため、$1-1/2^{k/2}$ の確率[18]で両履歴の ei が異なる i が存在し、Mi と Mi+ID から二重使用を行った利用者の識別情報(ID)が露見する。

[18] 例えば、k=4 の場合で 75%、K=10 の場合で約 96.9%、K=20 の場合で 99.9%の確率となる。

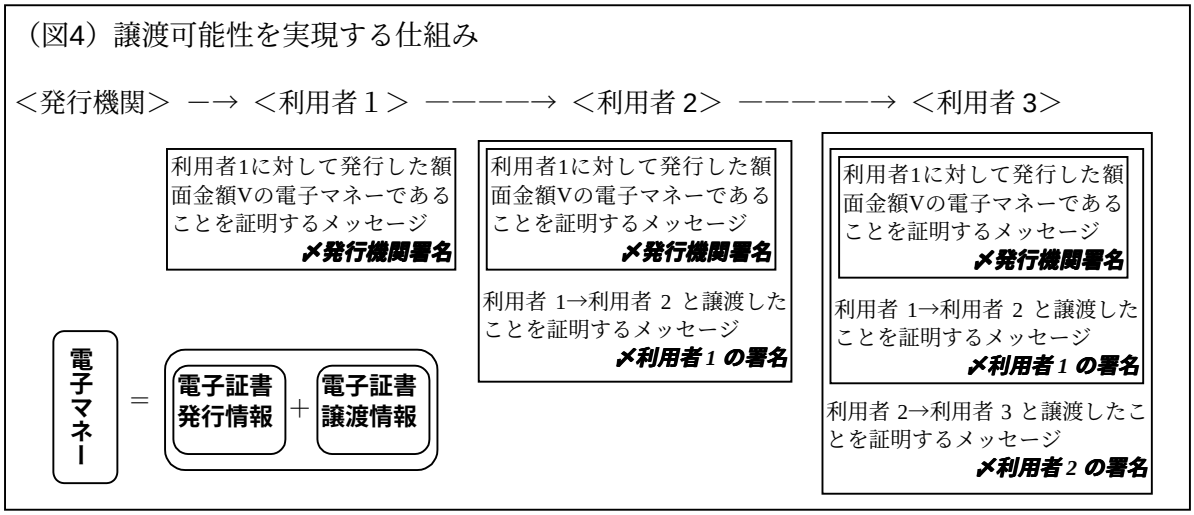
(3) より機能的な電子証書型電子マネー

―― *譲渡も分割利用も可能な電子証書型マネー*

Chaum の電子マネーはプライバシーを持たせることにはじめて成功したが、なお現金の持つ他の便利な特徴を実現したり、逆に現金の持つ問題点を改善する理論的研究の余地が残されていた[19]。そのため、その後は、譲渡可能性や分割利用可能性を満たす電子証書型電子マネーの論文発表が相次いでいる。

譲渡可能性の要件をはじめて満たしたのは Okamoto and Ohta [1989][20]である。これは、譲渡元の利用者による譲渡履歴に対するディジタル署名を、手形の裏書きのように連ねていくこと（図 4 参照）によって、電子マネーが転々と流通してきたものである証跡を確認できるようにして実現している。なお、ここで使用する署名鍵は予め銀行からブラインド署名によって真正であると認められたものであるため、どの利用者の署名鍵かについては二重使用を行わない限り露見することはない仕組みとなっており、引き続き匿名性を保っている。ただし、譲渡を重ねるに連れて、受渡す電子マネーのデータサイズが増大するという難点を持っている。

（図4）譲渡可能性を実現する仕組み



[19] 電子マネーがどのような特徴を持つべきかについては、岡本・太田 [1993]が次のような「理想的電子現金」の６条件を提示している。

①完全情報化･･･現金が完全に情報のみで自立して実現されること。
②安全性･･･電子現金のコピー、偽造等による不正利用ができないこと。
③プライバシー･･･利用者の購買に関するプライバシーが、小売店や電子現金発行者が結託しても露見しないこと。
④オフライン性･･･小売店での電子現金の支払いのときの処理がセンターなどに問合せることなく処理できること。
⑤譲渡可能性･･･電子現金の他人への譲渡が可能であること。
⑥分割利用可能性･･･1 回発行された電子現金を、利用合計金額が額面の金額になるまで何回でも使うことができること。

[20] T.Okamoto 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.

さらに Okamoto and Ohta [1991][21]や Eng and Okamoto [1994][22]ではバイナリーツリー構造に素因数分解問題や離散対数問題を埋め込んだ技法を用いることで分割利用可能性を実現している。

(4) 実装を考慮した電子証書型電子マネー

理論的には Eng and Okamoto [1994]までに、必要と考えられる要件をほぼ満たす電子マネーが実現された。しかしながら、一方で、これらの電子マネーは分割や譲渡を行う度にデータ量が肥大化するため、現在の IC カードの性能ではとても収まりきらないとか、署名・検証にかかる処理に時間がかかりすぎるために、現実の取引の場面ではとても許容できないものであった。日本電信電話（株）が 1995 年 12 月に発表した「電子現金方式」の実験システムは、現実に動く電子マネーを試作するという最低限の目的は達成したものの、一方で、複雑な電子証書型電子マネーの実装の困難さを実際に認識することとなり、分割可能性と譲渡可能性の同時実現や、全ての処理を IC カードに行わせることが次の課題となった。この頃から、電子証書型の電子マネーについても、単なる暗号理論研究の領域を脱しはじめ、実際にこれを実現するための研究に比重を置くようになってきた。

処理時間が膨大にかかる等、あまり現実的ではない処理部分については、必ずしも暗号技術を使ったエレガントな処理にこだわらない他の処理方式に置き換えたり、運用でカバーするといった実装を考慮した方法も検討されるようになった。例えば、Chaum の方法ではいかなる主体が結託しても決して失われない絶対的な匿名性を実現している反面、処理が複雑で重たいものであったが、藤崎・岡本 [1996][23]では信頼できる第 3 者機関の存在を仮定し、これに匿名性に関する情報の管理[24]を行わせることによって、電子マネー発行処理等を軽減した。これは同時に、犯罪捜査等必要なときに限り信頼できる第 3 者機関から情報開示を受けて不正行為者を特定する等の追跡可能性を実現するなど、匿名性のレベルを運用によって制御することを可能としている。

また、電子マネーの発行機関と顧客の口座を持つ銀行を分離し、電子マネーの流通に階層構造を持たせたのが、中山・森畠・阿部・藤崎 [1997][25]である。この方式では、複数の

---

[21] T.Okamoto and K.Ohta, “Universal Electronic Cash,” Advances in Cryptology-CRYPTO’91, LNCS 576, pp.324-337, Springer-Verlag, 1991.

[22] T.Eng and T.Okamoto, "Single-Term Divisible Electronic Coins," Proc. of EUROCRYPT’94, LNCS 950, pp. 306-319, Springer-Verlag, 1995.

[23] 藤崎・岡本、「エスクロー電子現金」、信学技報、IT95-51, ISEC95-46、SST95-112、pp.7-12、1996 年。

[24] 具体的には、通常公開していない電子マネーの利用者と、公開鍵（署名鍵）のリンケージを管理。

[25] 中山・森畠・阿部・藤崎, 「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」,” 『金融研究』 第 16 巻第 2 号, 日本銀行金融研究所, 1997 年 6 月

銀行が同一の発行機関を利用することによって共通の電子マネーを扱うことができ、利用者にとってもどの銀行から引き出された電子マネーかを意識することなく扱うことができるというメリットがある。本方式は、1996 年 9 月、「新しい電子マネー実現システム」として、日本電信電話（株）によって発表されている。

2. 実装技術研究から生まれた技術（残高管理型電子マネー）

これは、理論的に実現可能な電子マネーを研究するというよりも、まず、実装できる電子マネーの開発を目的に始まった技術研究である。IC カードやカード読み取り装置、コンピュータ機器等の物理的な構成と暗号技術を組み合わせ、実際に動かすことのできる電子マネーを実現する研究であり、現在、フィールドテストあるいは実用を開始している電子マネープロジェクトの多くはこの系譜に属するといえる。残高管理型（balance-based model）電子マネーの系譜と言い換えることもでき、IC カード等の耐タンパー装置の存在を前提にすることによって、必ずしも複雑で重い暗号処理によらずに安全性を確保し、実装を可能としているのが特徴である。これらの技術は、実際のビジネスを前提に開発され、その内容も必ずしも学術論文発表には馴染まないものがほとんどのため、技術開示が行われていないことが多く、特許関連資料等によってその一端を垣間見ることができる程度である。

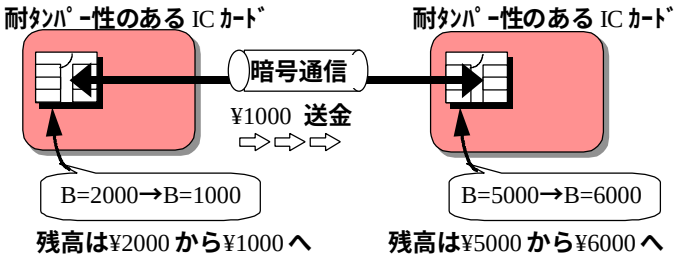
(1) 残高管理型の電子マネーの特徴

残高管理型電子マネーの大きな特徴は、IC カード等の耐タンパー装置を電子財布として使用することを前提にしていることである。耐タンパー装置内に、改竄されては困る残高金額情報や価値の受け払いなどで使用する秘密鍵を閉じこめておくことによって、電子マネーの安全性を確保している。残高金額情報等の不正な書き換えは IC カード等の耐タンパー性によって不可能とされることが前提になっていることから、電子マネーの価値の保証を複雑な暗号処理に求める必要がなく、単に IC カード内に残高情報を保持（度数管理）すればよいため、実装がより現実的になっている。この方式では電子マネー自体に個性はなく、異なる取引で入手した電子マネーも電子財布の中に収められた時点で財布の残高金額として合算されるため、個々の電子マネーを区別することができない反面、電子マネーとして管理する情報が少なくて済むというメリットがある（図 5 参照）。

ただし、IC カード等の耐タンパー性は一定の条件の下での安全性を保証するに過ぎないため[26]、IC カードの耐タンパー性が破られ、暗号鍵の露見などにより残高金額の不正な書き換えが可能となっても、システムのトータルフェイルを導かない工夫を施すことによって、総合的な安全性を確保することが大きな課題となる。

[26] 中山靖司・太田和夫・松本勉、「電子マネーを実現する情報セキュリティ技術と安全性評価」、『IMES ディスカッション・ペーパー・シリーズ』、98-J-26、日本銀行金融研究所、1998 年を参照。

（図５）残高管理型電子マネーの仕組み



セキュリティの基本思想

残高を表す情報を IC カードのような耐タンパー性を持つデバイスに閉じこめて改竄を防止し、デバイス間での残高更新のための通信を暗号化することによって、セキュリティの確保を図る。

(2) 残高管理型電子マネーの基本となる暗号研究

残高管理型の電子マネーのスキーム技術においては、IC カード等の耐タンパー性を実現する物理的媒体や処理機器の選択及びその構成方法はもちろんのこと、機器相互間の通信処理の方法にかかる技術が大きなポイントとなる。特に電子マネー固有の重要な技術としては、電子財布間の価値移転のための相互の通信処理方法があり、Even, Goldreich, Yacobi [1983][27]の研究がもとになっていると考えられる。電子証書型電子マネーでは暗号技術は主に電子マネーたるデータが正しいものであることを保証することに利用されていたのに対し、残高管理型の電子マネーでは取引時に価値移転を安全に行うことを保証する仕組みに使われている。Even, Goldreich, Yacobi [1983]では IC カード等の耐タンパー装置を使って電子財布を構成し、この IC カード内に価値の残高情報を記憶するとともに、取引にかかる処理をすべてこの IC カードで行うことを前提として、両装置間で価値を安全に移転させるプロトコルを実現している（図 6 参照）。具体的には、電子財布毎に固有の公開鍵暗号を使用した暗号通信によって、移転金額の送受信を行っているが、取引毎に毎回異なる識別情報を織り交ぜて通信を行うことによって、外部から送受信情報を観察して、後にこれを不正に利用しようとしても残高情報の更新を行うことができないように配慮している。

[27] S. Even, O. Goldreich, 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.

（図 6）残高管理型電子マネーの価値移転の仕組み　――価値移転方法の一例――

【IC カード内に格納されている秘密情報】

資金の送り手(U1)	
PkB	電子マネー発行機関の公開鍵
PkU1	送り手の公開鍵
SkU1	送り手の秘密鍵
[PkU1]*SkB	送り手の公開鍵に対する発行機関のディジタル署名

資金の受け手(U2)	
PkB	電子マネー発行機関の公開鍵
PkU2	受け手の公開鍵
SkU2	受け手の秘密鍵
[PkU2]*SkB	受け手の公開鍵に対する発行機関のディジタル署名

【暗号通信の手順】

④発行機関の公開鍵 PkB を用いて受け手の公開鍵 PkU2 を取出す。
　PkU2　　{[PkU2]*SkB}*PkB
⑤入手した受け手の公開鍵 PkU2 を用いて復号し、識別番号 R を取出す。
　R　　{[R]*SkU2}*PkU2
⑥入手した識別番号 R と移転希望金額 V を結合したものを送り手の秘密鍵で暗号化する。
　[V+R]*SkU1
⑦残高データから送金分を減額する。
⑧送り手の公開鍵に対する発行機関のディジタル署名[PkU1]*SkB と共に受け手に送信する。
　[PkU1]*SkB　+　[V+R]*SkU1

①IC カードの ID と、取引のシリアル・ナンバーから、識別番号 R を生成する。
②識別番号 R を受け手の秘密鍵 SkU2 で暗号化する。
　[R]*SkU2
③受け手の公開鍵に対する発行機関のディジタル署名[PkU2]*SkB と共に送り手に送信する
　[PkU2]*SkB　+　[R]*SkU2

（注）1. [x]*y は、情報 x を鍵 y を用いて公開鍵暗号により暗号化／復号することを示す.
　　2. a+b は、情報 a と情報 b を結合することを示す

⑨発行機関の公開鍵 PkB を用いて送り手の公開鍵 PkU1 を取出す。
　PkU1　　{[PkU1]*SkB}*PkB
⑩入手した送り手の公開鍵 PkU1 を用いて復号し、移転金額 V と識別番号 R を取出す。
　V+R　　{[V+R]*SkU1}*PkU1
⑪取り出した識別番号 R が、①で作成したものと同じであることを確認する。
⑫残高データに送金分を加算する。

(3) 電子マネープロジェクトでの実装

現在、IC カードを使った多くの電子マネープロジェクトが進行中であるが、その技術内容について公表されているものはほとんどない。電子証書型電子マネーを IC カードに実装するものもわずかながら存在するようであるが、使用している IC カードの性能から推測して、その多くは残高管理型電子マネーと推測される[28]。

なお、IC カード等によって実現される電子マネーでは、実際には IC カードを利用者の識別・認証にのみ使用し、残高情報自体はカードに保有せずセンター側で管理するということも可能である。技術的にはクレジットカードや銀行振込等の支払手段をインターネット上で使用できるようにした電子クレジットカードやオンラインバンキングと類似のもので、センターで管理する価値の受渡し指図情報を電子的に受渡すことによって決済を行う。取引は常にセンターとオンラインで行うため、通信コストが嵩むというデメリットはあるものの、利用者の識別・認証さえしっかりと行えば必要な安全性を確保できる手段であることから、IC カード型電子マネーの中にはこのような方法が採られているものもあると思われる。なお、IC カードの耐タンパー性のみに頼らずに安全性を高める手段として、IC カードとセンターの両方に残高情報を持ち、照合する方法を採っているものもある。

具体的なプロジェクトについて、その使用している技術を垣間見ることができるものとしては MONDEX がある。MONDEX は、セキュリティに関する基本的な設計方針は、セキュリティの仕組みは固定ではなく常に安全と評価できるものに切り替えていくというスキームであると表明していることから、実際に MONDEX が採用したことのある技術かどうかは判断できないが、それらの技術の一例を表すものとして、MONDEX が英国等で特許取得（日本では出願中）している発明[29]が参考になる。ただし、これだけでは実際にどの程度の耐タンパー強度を持った IC カードを使い、どのように電子マネーが設計されているか等のシステム全体像を読み取ることはできない。

---

[28] 電子証書型電子マネーを IC カードに実装するためには、IC カードに埋め込まれた IC モジュール・チップが、暗号を処理するための専用プロセッサーと共に、十分に大きな容量の EEPROM（電気的に一括消去が可能な読出し専用メモリ）を搭載していることが必要といわれている。

[29] ヨーロッパ特許番号は EP0479982B1（発効日 1995 年 9 月 13 日）。電子マネー・スキームと共に、IC カードの処理能力に応じて 3 通りの価値移転の方法を記載したものである（特許の詳細については後述）。

3. ビジネスの方法としてのアイデアを実現する技術

今日では、金融商品、サービスの提供のためにコンピュータ・ソフトウェア等の技術が利用されることが多い。従来、そのほとんどは、通常のシステム開発手法によって人間の行っている業務ないし抽象的なアイデアを具体的にシステム化（ソフトウェア化）するものであって、通常の創作能力の発揮により実現可能なものであった。しかしながら、電子マネーをはじめとする最先端の金融商品、サービスについては、通常のシステム開発手法を使ってビジネスが可能となるように具体的にシステム化を図るにしても、通常の創作能力を発揮するだけでは実現できないと考えられるものが増えてきており、これ自体が特別な技術であるとの考え方から、こうした技術について特許を取得する動きがある。

電子マネーにおいては、電子マネー・システムの構成要素およびその機能、あるいは処理フロー等のビジネス・フローに関するアイデアを基に、どのような手段、方法を用いて、どのような手順で処理を行えばこれを実現できるかといった具体的な技術的思想がこれに該当し、ソフトウェア特許の一種とみることもできる。なお、必ずしもその個々の部分を実現するための詳細な技術までを特定しているわけではないが、それぞれの構成要素がどのような要件を満たすべきであるかが明らかになれば、それに適合する実装製品、暗号理論等を適用することによって電子マネーを構築することができるため、これも電子マネー・スキーム技術と分類することができる。Citibank, N. A.が「電子通貨システム」を特許出願（米国等では既に登録）して、注目を集めた分野の技術がこれに当たる。銀行券に例えると、製造を担当する印刷業者、発行あるいは流通して戻ってきた銀行券の鑑査を行う発券銀行、利用者と発券銀行の間を取り持つ金融機関等の構成要素やその役割、およびそれらの間で受け渡しされる情報等に関するビジネス・スキームやそのフローを含んだ技術的思想ということになろう。

Ⅳ. 電子マネー・スキーム技術に関する特許

以下では、電子マネーのスキーム技術に関する特許のうち主要なものについて、各発明国におけるオリジナル特許を中心に解説する。なお、取上げる特許の内容については、クレームに記載されている事実を指摘するに止め、その効力の範囲に関して著者自身の価値判断を行っていない。

1. 暗号理論研究から派生した技術に関する特許（電子証書型電子マネー）

(1) One-show blind signature systems（米国）

本特許は暗号学者である Chaum 氏の発明によるもので、１回しか使用（提示）することができないように工夫されたブラインド署名の方法を記述したものである。必ずしも電子マネーのためにのみ使われる技術というわけではないため、クレームも電子マネーに限定されないような表現が使われているが[30]、DigiCash 社の ecash を実現するのに使われた技術に関連しており、他の分野での利用も今のところはあまり考えにくい技術[31]であるため、特に電子マネー・スキーム技術として取上げた。

米国では、1988 年 3 月に出願されたのち、1989 年 7 月に継続出願がなされ（元の出願は取り下げ）[32]、1990 年 3 月に成立[33]している。その後、1990 年 4 月に、さらに同特許の内容を詳細化した方法およびそれに対応したシステムをクレームした継続出願があり、これについても 1991 年 1 月に特許として成立[34]している。

この間、1989 年 3 月に特許協力条約に基づき、日本を含む約 40 カ国を指定する国際特許出願が行われており、日本では、1996 年 3 月に、1991 年 1 月に成立した米国特許のクレームを統合する内容の補正手続と同時に審査請求が行われ、現在も審査中である[35]。

以下では、米国における２つの特許について説明する。

＜US Patent No.4,914,698＞

本特許のクレームは１つのみであり、『1 回提示ブラインドサインシステム』を実現する基本的な手順をクレームしている。

---

[30] 例えば、特許明細書中の概要説明等においてみられる、パーティ B、パーティ P、パーティ S との表現は、用途を制限するものではないが、覚えやすいように、それぞれ Bank, Payer, Shop の頭文字からとったとの説明がある。

[31] 特許明細書にはブラインドサインの利用法としては、決済手段や信任状があると書かれている。

[32] Continuation of Ser. No.168,802, Mar. 16, 1988, abandoned.

[33] U.S. Patent No. 4,914,698（出願日 1989 年 7 月 24 日、発効日 1990 年 4 月 5 日）

[34] U.S. Patent No. 4,987,593（出願日 1990 年 4 月 5 日、発効日 1991 年 1 月 22 日）

[35] 日本国内では特表平 4-500440（特願平 1-505209、出願日 1989 年 3 月 15 日）。

クレーム1**：**

「パブリックキーデジタルサインシステムにおいて、

①サインが２以上の部分に分割された識別情報を含むことを確保して複数のサインを発行するステップと、

②前記２以上の部分の少なくとも１つを明らかにするように前記デジタルサインを提示してチェックするステップと、

③チェックされたサインのセットについて試験を行い、前記発行されたサインの少なくとも１つの異なった部分がその少なくとも１つの発行されたサインを２回以上示すならば、識別子の少なくとも１つを生成するステップ

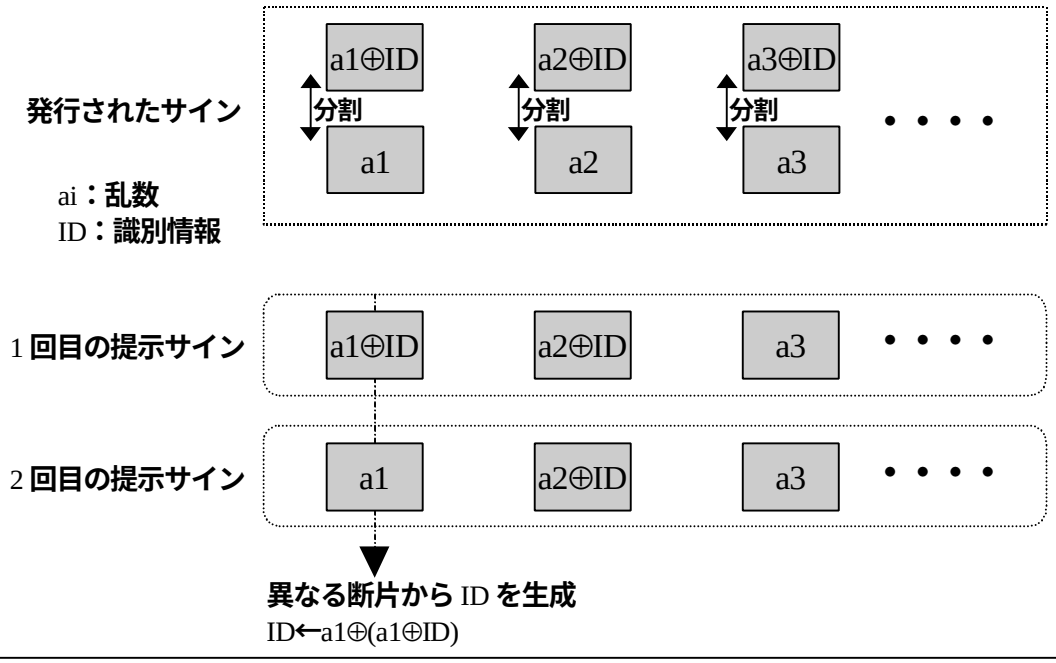
からなることを特徴とするデジタルサイン方法」[36]

このクレームに記載されているデジタルサイン方法は、実施例によると、発行パーティ（銀行）、提示パーティ（利用者）、チェックパーティ（商店）の３者間のやり取りであることが開示されてはいるものの、スキームの構成要素や処理を行う主体が誰なのかについては記載されていない。具体的には３つのステップ（①デジタルサインの発行処理、②デジタルサインの提示処理、③二重提示チェック）から構成され、同じデジタルサインを１回だけ提示する分には匿名性が保たれるが、もし２回以上使用するならば匿名性が失われるという特徴を持っていることが明記されている。なお、実施例をみると、「サインが２以上の部分に分割された識別情報を含むことを確保して複数のサインを発行し」については、提示パーティが識別情報を少なくとも２つの部分に分割したものを複数用意し、発行パーティによってブラインド署名してもらうことによってサインを発行してもらうことや、その際サイン対象をカット・アンド・チューズ技法によって確認するなどの方法が開示されている。また、「前記２以上の部分の少なくとも１つを明らかにするようにデジタルサインを提示して」については、提示パーティは発行された複数のサインそれぞれについて、チェックパーティによって選択された方の分割部分を提示することを、「前記発行されたサインの少なくとも１つの異なった部分がその少なくとも１つの発行されたサインを２回以上示すならば、識別子の少なくとも１つを生成するステップを有する」については、もし同じ分割部分を１つでも含むように選択されてサインを複数回提示すると、識別子が露見することが開示されている（図７参照）。

---

[36] **原文は**「In a public key digital signature system, a method of digitally signing comprising the steps of : issuing a plurality of signatures to ensure that each said signature contains identifying information divided between at least two parts; showing and checking said digital signatures to reveal at least one of said at least two parts of each; and performing a test on a set of said signatures shown, that would yield at least one of said identifiers if different parts of at least one of said issued signatures had been revealed in showing the at least one issued signature more than once.」。**なお、クレームの翻訳では、日本における出願の同内容のクレーム表現を参考にした。また、○数字は当方で見やすくするために補記したものである。**

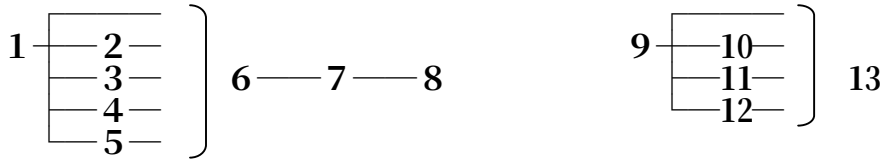
（図７）One-Show Blind signature の仕組み



＜US Patent No.4,987,593＞

クレームは２つの独立クレームと 11 の従属クレームから構成されている（図８参照）。クレーム 1～8 は US Patent No.4,914,698 の内容をもとに実際に処理する方法をクレームしたもの、クレーム 9～13 はさらにこの方法を実現する手段やシステムをクレームしたものである。

（図８） クレームの従属関係



処理する方法に関する独立クレームであるクレーム 1 は、以下のとおりである。

クレーム 1：

「パブリックキーデジタルサインシステムにおいて、

①発行パーティによってデジタルサインを発行し、その発行パーティは実質的な確率で発行された各サインが識別情報を含むことを確保するステップと、

②チェックパーティが提示されたサインのデジタルサイン特性を確認してしかも全てのチェックパーティおよび前記発行パーティの共同動作から最大１回示されたサインに含まれた識別情報を隠蔽することを可能にするために少なくとも１つの

チェックパーティに前記発行されたサインのいくつかを提示するステップと、
③前記提示されたサインについて試験して、１回よりも多く示されたサインに含まれた前記識別情報を実質的な確率で生成するステップ
からなることを特徴とする改良」

ここでは、US Patent No. 4,914,698 では明示されていなかった構成要素（発行パーティ、提示パーティ、チェックパーティ）を明記したほか、US Patent No. 4,914,698 では「サインが２以上の部分に分割された識別情報を含むことを確保して」としているところを「実質的な確率で発行された各サインが識別情報を含むことを確保し」と、識別情報が分割されているかどうかには無差別であるようにするなど、やや一般化した表現を使用している。また、US Patent No. 4,914,698 では 1 回のみ提示した場合のことには特に明示的には触れていなかったところを、「最大１回示されたサインに含まれた識別情報を隠蔽することを可能にする」と、匿名性が保たれることを明記しているほか、サインを２回以上提示に使うと識別情報が高確率で露見するのは、「全てのチェックパーティおよび前記発行パーティの共同動作」から行われることが示されている。

クレーム 1 に従属するクレーム 2 では、「識別情報は２つ以上の部分に分割され、そのうち少なくとも１つはサインを提示しチェックされるときに明らかにされ、1 回より多く提示されたサインによって識別情報が生成される方法」と、特に識別情報を２つ以上に分割する方法について記載している。同じくクレーム１に従属するクレーム 3 は、「サインを提示するステップは①チェックパーティによるチャレンジの送信、②これに対する応答値の送信、を含んでおり、多数の異なるチャレンジに対する異なる応答は識別情報を明らかにするが、単一の応答値では識別情報が明らかにならない方法」と、サインの提示のステップについて記載している。また、クレーム 5 は、「識別情報によってサインが複数の発行取引のうちどの取引で発行されたものかを特定できること」と識別情報によって、どの取引によって発行されたサインかをトレースすることができることを記載している。
クレーム 6 は、「前記発行されたサインが価値と交換に提示されるクレーム 1〜5 の方法」となっており、サインを電子マネーとして使うことを想定したクレームである。さらに、これに従属するクレーム 7 では、「サインを発行されたパーティによって、支払額を決めるための指示を与えるステップと、払戻し額を決めるための指示を与えるステップと、両者の合計が予め定められた最大値を越える払戻しの指示を認識するステップからなる方法」を記載しており、支払者は引き出した電子マネーの額面内で支払額を自由に設定でき、その残金分は銀行に戻すことによって精算することを記述している。また、クレーム 8 は「クレーム 7 の方法であって、払戻し額は複数の支払いに亘って集計され、そのため個々の支払いとの対応関係が隠蔽されること、払戻しの指示は、払戻し額のそれぞれが特定の支払額に対応した場合に与えられること」を記載しており、払戻しの額から銀行に支払い

の匿名性が露見するのを防いでいる。

なお、クレーム 9〜13 は、それぞれ、クレーム 1, 2, 3, 5, 6 が「方法」<method>に関するクレームとして記述されているところを、「手段」<means>や「システム」<system>に関するクレームとしたものである。

(2) 電子現金実施方法およびその装置[37]（日本）

本特許は、日本電信電話（株）がこれまで行ってきた暗号研究の成果の１つとしての電子証書型電子マネーの実現方法に関して、はじめて特許として出願したもので、既に日本のほか米国、カナダ、フランス、ドイツ、英国で登録されている。日本電信電話（株）はその後も、論文で発表している様々な電子マネーについても多数の出願を行っており、それらの基本の特許としての位置づけを持つものと考えられる。なお、こうした暗号研究における論文や、これに基づく特許では、「電子マネー」のことを「電子現金」と表現することが普通であり、本特許でも「電子現金」という言葉が用いられている。さらに、特に一つ一つの電子マネーを区別して呼ぶときには、電子コイン、電子紙幣という言葉が使用されることもある。

本特許は、技術的には、先行技術である Chaum, Fiat, Naor の”Untraceable Electronic Cash”が電子マネーの二重使用検出を可能にするために、使用する一方向性関数の２成分の不干渉性という特殊な条件を仮定しているところを、プロトコルを改良することによって必ずしも仮定しなくても同様の効果が得られるようにしたものである。また、同時に、「利用許可証」という概念を加えることによって、電子マネー発行時の処理負担を軽減するとともに、利用者間の電子マネーの譲渡や、同一の電子マネーを予め決められた一定回数以内で複数回利用できるようにした方法をも含んでいる。なお、日本電信電話（株）が後に出願している多数の電子現金方法に関する特許[38]や日本電信電話（株）と日本銀行が 1996 年 9 月に出願している「番号登録式電子現金方法およびその利用者装置」[39]、「発行機関分離型番号登録式電子現金方法およびその利用者装置」[40]は、本特許に続く一連の研究に属するものである。

具体的にクレームの内容をみると、全部で 54 のクレームからなっており、クレーム 1～15 で電子現金実施方法の基本的なプロトコルについて、クレーム 15～51 で電子現金実施方法の詳細なプロトコルについて、クレーム 52～54 で電子現金を実施する利用者装置について記載している。独立クレームは、方法に関するクレーム、装置クレームそれぞれ１つ（クレーム 1, クレーム 52）のみであり、特にクレーム 1 は方法に関するクレームのすべて（50 クレーム）が従属する範囲の広いクレームとなっている（図 9 参照）。

---

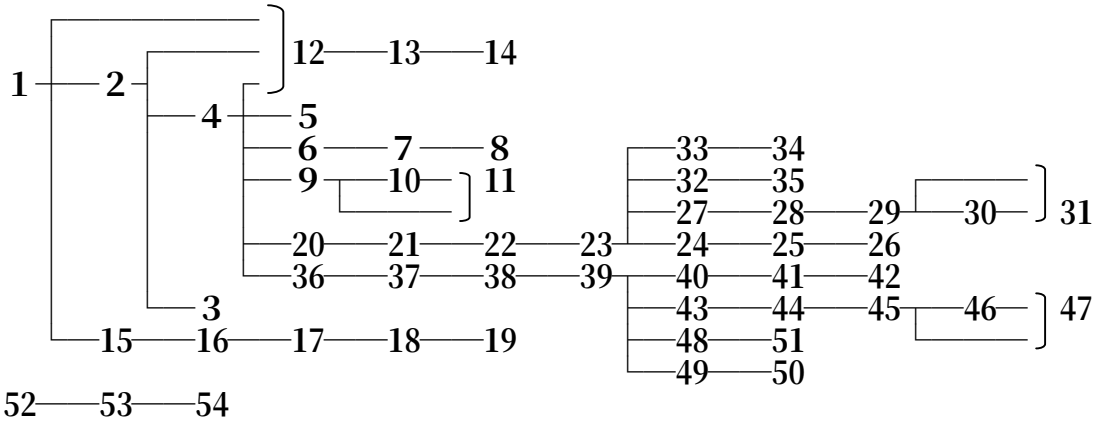
[37] 特願平 2-88838, 特公平 7-52460（出願日 1990 年 4 月 3 日、発効日 1995 年 6 月 5 日）。米国では、U.S. Patent No. 4,977,595（出願日 1990 年 3 月 28 日、発効日 1990 年 12 月 11 日）。発明者は太田・岡本。

[38] 特願平 3-143530、特願平 3-170131、特願平 6-093390、特願平 6-225353、特願平 8-187547、特願平 7-180281、特願平 7-246416、特願平 7-246415、特願平 7-287457、特願平 8-057536、特願平 8-057537、特願平 8-121688、特願平 8-135167、特願平 8-121689 等。

[39] 特開平 10-091696（出願日 1996 年 9 月 11 日）

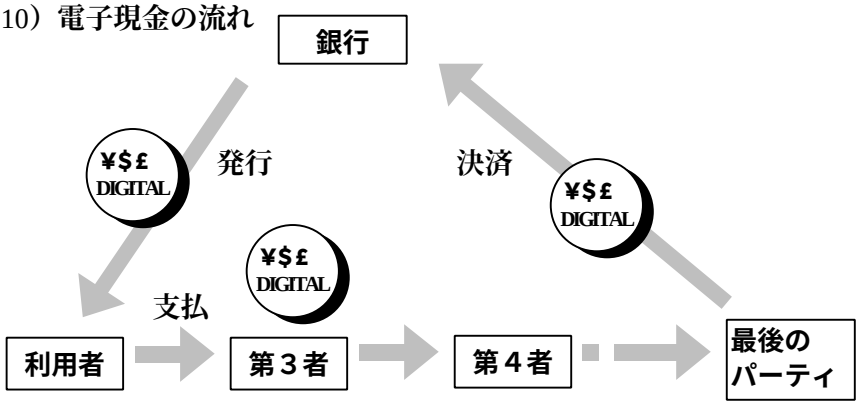
[40] 特開平 10-091697（出願日 1996 年 9 月 11 日）

（図９）クレームの従属関係



まず、クレーム 1～3 は電子現金実施の基本的な方法についての記載である。クレーム 1 は電子現金実施方法に関する唯一の独立クレームであり、「銀行が利用者に対し電子現金を発行し、利用者はその電子現金を使って第 3 者に支払いをし、銀行は使用された電子現金を持っている最後のパーティとの間で決済をする電子現金方法であり次の工程を含む」と、電子現金実施方法における構成主体が銀行、利用者、第 3 者、…、最後のパーティであることと、電子現金の流れを示すとともに（図 10 参照）、「次の工程」で電子現金の発行・支払いの基本的なプロトコルを記載している。

（図 10）電子現金の流れ



クレーム 1:

「銀行が利用者に対し電子現金を発行し、利用者はその電子現金を使って第 3 者に支払いをし、銀行は使用された電子現金を持っている最後のパーティとの間で決済をする電子現金実施方法であり次の工程を含む：

利用者は

(a)自分の識別情報を含んだ秘密情報から第 1 の一方向性関数により利用者情報を生成し、

(b)銀行に対し前記利用者情報を含む情報にブラインド署名をさせて署名付利用者情報を得、

(c)乱数情報から第 2 の一方向性関数により認証用情報を作成し、

(d)銀行に対し前記認証用情報を含む情報にブラインド署名をさせて署名付認証用情報を得、

(e)前記利用者情報と、前記署名付利用者情報と、前記認証用情報と、及び前記署名付認証用情報とを含む電子現金情報を前記銀行が発行した電子現金として第 3 者に渡し、

前記第 3 者は

(f)受け取った前記電子現金情報中の前記署名付利用者情報と前記署名付認証用情報の正当性を検証し、

(g)前記正当性が検証されたならば問合わせ文を作成して前記利用者に与え、

前記利用者は

(h)少なくとも自分の作成した前記秘密情報と前記第 3 者から受け取った前記問合せ文とを使って応答文を作成して前記第 3 者に与え、

前記第 3 者は

(i)受け取った前記電子現金情報中の前記利用者情報と前記認証用情報とを使って前記応答文の正当性を検査し、前記応答文が正当であれば前記電子現金を正当なものとして受け、

(j)必要に応じて少なくとも前記電子現金情報と、前記第 3 者の前記問合せ文と、前記利用者の前記応答文とを第 4 者に渡す。」

また、これに従属するクレーム 2、3 は、電子現金の銀行への預け入れ[41]の基本的なプロトコルを追加するものであり、クレーム 2 が電子現金情報の銀行への送信および正当性検査の工程を、クレーム 3 が不正使用（二重使用）の検査を行う工程を記載している。以下は、クレーム 1 に記載された電子現金の発行、支払いの基本的なプロトコルとクレーム 2,3 に記載された預け入れの基本的なプロトコルについて、一連の流れとして整理したものである。

[41] クレーム中では「決済」という言葉を使用している。

（電子現金の発行）

ｸﾚｰﾑ	利用者	銀行
1	①自分の識別番号を含んだ秘密情報から第１の一方向性関数により利用者情報を作成する ②銀行に利用者情報を含む情報にブラインド署名をさせて署名付利用者情報を得る ③乱数情報から第 2 の一方向性関数により認証用情報を作成する ④銀行に認証用情報を含む情報にブラインド署名をさせて署名付認証用情報を得る	ブラインド署名を行う ブラインド署名を行う

（電子現金の支払い）

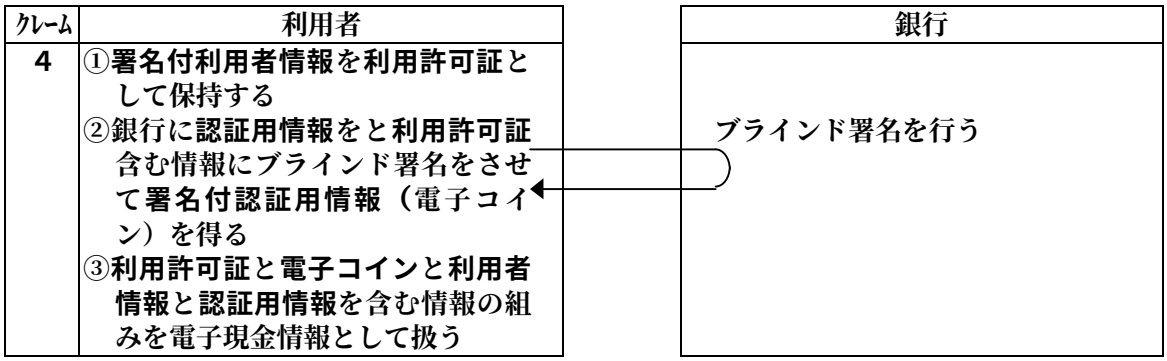
ｸﾚｰﾑ	利用者	第 3 者
1	⑤利用者情報、署名付利用者情報、認証用情報、署名付認証用情報を含む情報を銀行が発行した電子現金としてとして第 3 者に渡す ⑧自分の作成した秘密情報と受け取った問合文等を使って応答文を作成し第 3 者に送付する	⑥署名付利用者情報と署名付認証用情報を検証する ⑦検証結果が正しければ問合文を作成して利用者に与える ⑨電子現金情報の中の利用者情報と認証用情報を使って、応答文の正当性を検証し、正当であれば受け取る ⑩必要に応じて電子現金情報と問合文と応答文等を第 4 者に渡す

（銀行預入）

ｸﾚｰﾑ	最後のパーティ	銀行
2 3	⑪電子現金情報と問合文と応答文を渡す	⑫電子現金情報中の署名付利用者情報と署名付認証用情報の正当性と問合文に対する応答文の正当性を検査する ⑬電子現金情報中の署名付利用者情報と署名付認証用情報の組と同じ値の組が、メモリにあるかどうかを検査することによって不正使用の有無を検出する。 ⑭電子現金情報、問合文、応答文を含む情報をメモリに蓄積する。

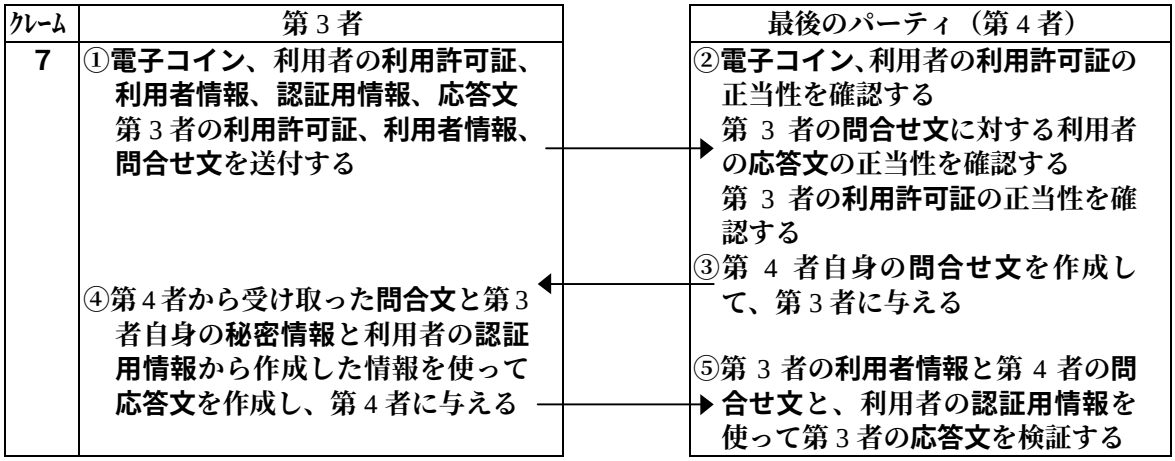
クレーム 4（クレーム 2 に従属）は、発行処理における１つ目のブラインド署名で得た署名付き利用者情報を利用許可証として保持し、これを繰り返し使用する方法で、認証用情報と利用許可証を含む情報に対しブラインド署名したものを電子コインとする方法を記載している。新たに考案した利用許可証の考え方によって、発行処理の都度、利用者情報に署名をしてもらう必要がなくなり、従来方式に比べてデータ通信等の処理負担が軽減されたほか、電子現金の譲渡も可能になっている。

（利用許可証を使った電子現金発行）

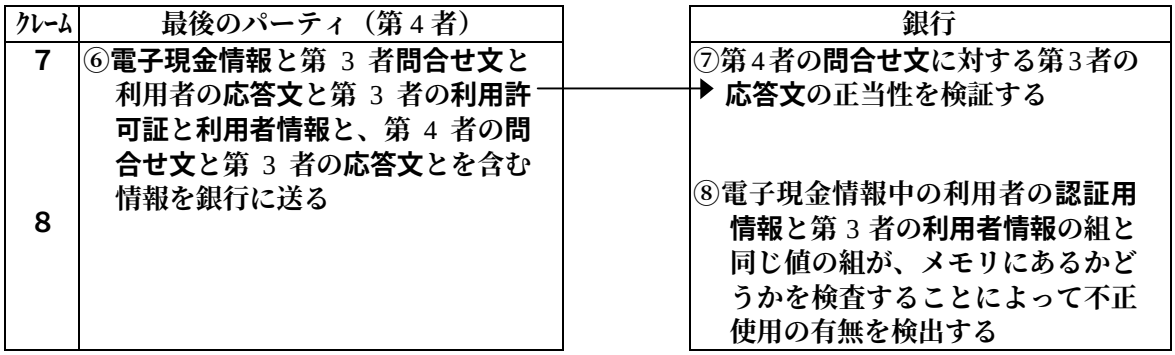


利用許可証を用いること等によって利用者間での電子現金の譲渡も可能となっているが、電子現金の受取者がそのまま銀行に預け入れるか、それともさらに使用するかによって支払いのプロトコルは異なっている。クレーム 5（クレーム 4 に従属）は前者の場合（最後のパーティは第 3 者）の処理であり、支払処理における問合文中に第 3 者の識別情報と時刻情報を含むことを記載している。一方、クレーム 6（クレーム 4 に従属）は後者の場合（以下譲渡処理）であり、第 3 者は応答文の正当性を確認した後、自らの利用許可証に対する利用者の署名を受け、これを譲渡証として電子現金情報と一緒に保有する方法が記載されている。なお、譲渡処理で受け取った電子現金の支払い、預け入れの基本的なプロトコルは、クレーム 7, 8（クレーム 6 に従属）に記載されており、以下のとおりである。

（譲渡された電子現金の支払い）



（譲渡された電子現金の預け入れ）



また、クレーム 9～11（クレーム 4 に従属）は、電子コインを予め決められた一定回数以内で複数回利用できるように工夫した電子現金方法についての記載であり、1 個のコインを保持するときと同等の情報量で、多数のコインを保持することと同様の効果を得られるなど保持情報量を少なくすることが可能となっているほか、クレーム 12～14（クレーム 1,2,4 に従属）はブラインド署名の際にカット・アンド・チューズ技法を使って署名対象を確認することを記載している。

クレーム 15～51 は、電子現金実施のプロトコルを具体的な計算式を示しながら詳細に記載したクレームである。クレーム 15～19（クレーム 1 に従属）は電子現金を発行する度に署名付利用者情報を作成する基本的な電子現金実施の方法を、クレーム 20～35（クレーム 4 に従属）は電子現金を発行する際に予め作成しておいた利用許可証を使用する場合の電子現金実施の方法について記載したクレームであるほか、クレーム 36～51（クレーム 4 に従属）は、クレーム 20～35 のそれぞれに対応し、特に利用許可証が一括署名によって作られている記載に書き換えたクレームである。なお、クレーム 15～19 に対応する具体例は実施例 1 に、クレーム 20～51 に対応する具体例は実施例 2 に開示されている。

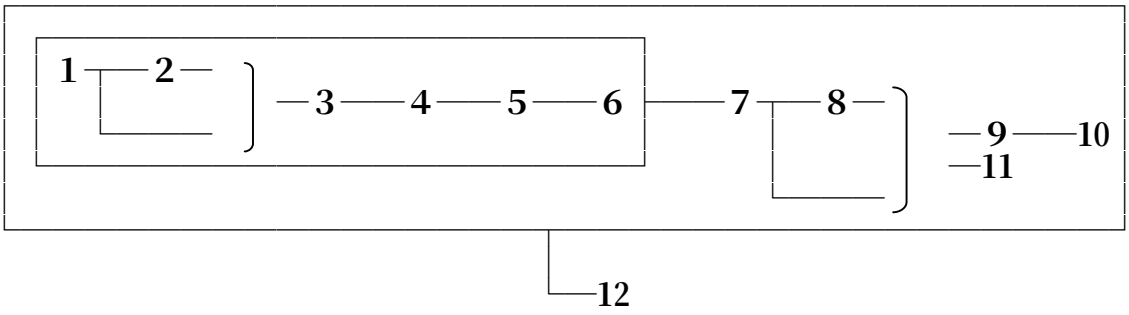
最後にクレーム 52, 53, 54 は電子財布たる利用者装置、利用許可証を使用する利用者装置、譲渡機能付きの利用者装置について記載している。

2. 実装技術開発から生まれた技術関する特許（残高管理型電子マネー）

(1) Value Transfer System[42]（英国）

本特許は英国 MONDEX 社の幹部である Timothy Jones と Graham Higgins による共同発明で、MONDEX システムを実現している基本的なアイデアと考えられる技術である。1990 年 4 月に英国内で出願された後、1991 年 4 月に特許協力条約に基づき米国や日本を含む 50 数カ国を指定する国際出願が行われ、既に英国を含む約 20 カ国以上の国で成立[43]している。

（図 11）クレームの従属関係



クレームは１つの独立クレームとそれに続く 11 の従属クレームから構成されている（図 11 参照）。クレーム 1～5 がシステムのスキームや各構成要素の機能を、クレーム 6 が金銭移転の基本的な処理の流れを、クレーム 7～9 が金銭移転における基本的な暗号の仕組みを記載しているほか、クレーム 10, 11 では、特に一方の電子財布（IC カード）のマイクロプロセッサの計算能力が劣る場合の金銭移転における暗号処理の流れを、クレーム 12 では、電子マネーの発行機関が複数あるシステムについて記載している。

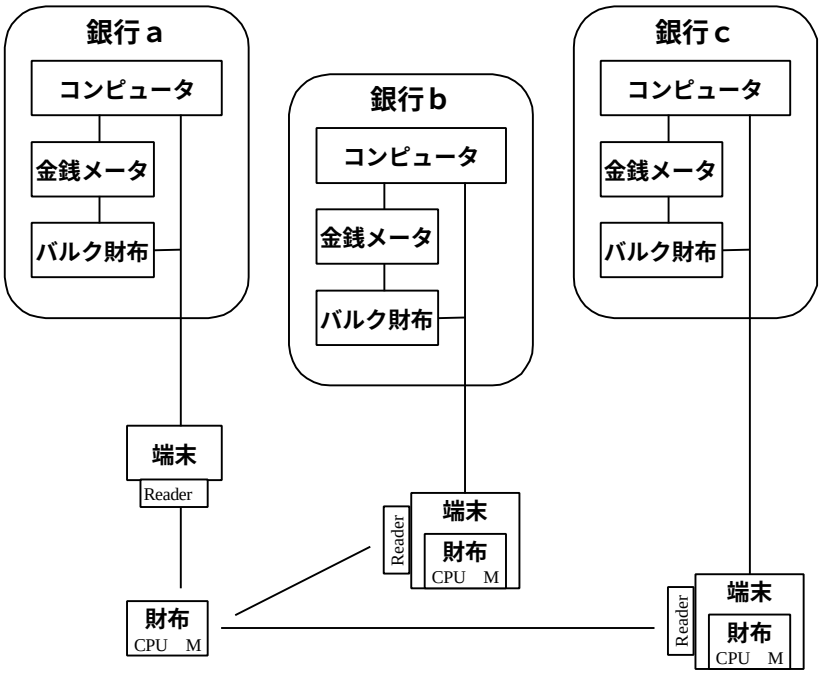
まず、クレーム 1 ではシステムの構成要素として、コンピュータ、複数の電子財布、交換装置、引き下ろし手段、精算手段、金銭メータを示すとともに、うち１つ以上の電子財布は金銭メータを介して電子マネーを発行および精算するバルク財布であり、金銭メータに記録される変動金額記録が電子マネーの発行金額と精算金額の差（発行残高）を表すことを記載している（明細書に添付されているスキーム概要図は図 12 のとおり）。

---

[42] もともと U.K. Application No.9008362（出願日 1990 年 4 月 12 日）として、英国内で出願されたものであるが、英国を指定国の１つとするヨーロッパ特許として成立（ヨーロッパ特許番号は EP0479982B1：発効日 1995 年 9 月 13 日）。なお、国際特許出願番号は、PCT/GB91/00566 である。

[43] 米国では、請求の範囲を変更したうえで、U.S. Patent No. 5623547 として成立（発効日 1997 年 4 月 22 日）。さらに、継続出願を行い、U.S. Patent No.5778067 として成立（発効日 1997 年 7 月 7 日）。なお、日本においては、現在（1998 年 8 月）審査継続中（特願平 3-506996、特表平 5-504643：出願日 1991 年 4 月 10 日、公表日 1993 年 7 月 15 日）。

（図 12）スキーム概要図



クレーム 1：

「①コンピュータシステムと、

②複数の電子財布と、

③1 またはそれ以上のバルク財布である電子財布と、

④電子財布が互いに通信して前記コンピュータシステムからオフライン状態の取引における金額を転送することが可能な交換装置と、

⑤金銭メータシステムと、

⑥前記コンピュータシステムの制御に従い、前記金銭メータシステムを通して、前記 1 又は複数のバルク財布に金額をロードする引き下ろし手段と、

⑦前記コンピュータシステムの制御に従い、前記金銭メータシステムを通して、前記 1 又は複数のバルク財布から金額を精算する精算手段とを有し、

⑧前記金銭メータシステムは 1 又はそれ以上の変動金額記録を記録し、かつ 1 又は複数のバルク財布に与えられた正味の金額を導き出すことができ、前記正味の金額は前記 1 又は複数のバルク財布に引き下ろされた総計金額と、前記 1 又は複数のバルク財布から積算された総計金額との間の差であり、変動金額記録は個々の取引に関して非特定的であること

を特徴とする金銭振替システム」[44]

[44] **原文は、**「A value transfer system having a computer system; a plurality of electronic purses, one or more of the electronic purses being bulk purses; exchange devices whereby purses may communicate with each other to transfer value in transactions which are off-line from the computer system; a value meter system; draw-down means for loading said bulk purse or bulk purses with value under control of the computer system via the value meter system; redemption means for redeeming value from said bulk purse or bulk purses under control of the computer system via the value meter system; the value meter system recording one or more float value records whereby the net value released to the bulk purse or purses may

クレーム 2〜6 はクレーム 1 に直接ないし間接的に従属したクレームであり、クレーム 2 では金銭メータシステムは複数のバルク財布の金額を増減するインターフェースを持っていることを、クレーム 3 では各財布は累積する金額を記録でき、マイクロプロセッサが財布間における取引において、送出財布の金額を減少すると同時に、受取財布の金額を同額だけ増額する処理を行うようプログラムされていることを、クレーム 4 では各財布は、取引時に財布および財布内で個々の取引を区別する取引識別番号を発生するようプログラムされていることを、クレーム 5 では取引識別番号は受取財布固有の ID と、財布内で発生するシーケンス番号で構成されるようプログラムされていることをクレーム 1 に追加している。また、クレーム 5 に従属するクレーム 6 は、金銭移転時の基本的な処理の流れについて記載したクレームであり、さらに以下のステップからなることを記載している。

①受取財布から送出財布に取引識別番号を含む要求を送出する。

②送出財布から受取財布へ渡す取引金額メッセージに取引識別番号を組入れる。

③受取財布は受け取った取引識別番号の有効性によって取引金額メッセージの受取りを制御する。

クレーム 7〜9 は、各財布が基本的な暗号処理を行えるようになっていることを記載したクレームで、クレーム 7 はクレーム 1〜6 の各々[45]に、クレーム 8 はクレーム 7 に、クレーム 9 はクレーム 8 に従属している。クレーム 7 では各財布は公開鍵暗号系を処理可能なようにプログラムされており、少なくとも 1 つのシステムの公開鍵を保持していることを、クレーム 8 では各財布はグローバル秘密鍵によって暗号化されたデータを持っており、マイクロプロセッサがグローバル公開鍵によって検証するステップを含むようにプログラムされていることを、クレーム 9 では各財布は固有の公開鍵／秘密鍵のペアを有し、取引データの送信時に、マイクロプロセッサはこれらの鍵を使って暗号化／復号を行うようにプログラムされていることを記載している。クレーム自体には、具体的に使用する暗号方式やプロトコル等は特定されないが、第 1 の実施例で取引を行う双方の財布が RSA 暗号を計算するに十分な能力を持っている場合についての具体的な処理が開示されている（図 13）。

さらに、クレーム 10,11 は、それぞれ取引時に一方の財布の CPU の計算能力が低くても適用できる金銭移転にかかかる暗号処理の流れについてのクレームであり、クレーム 10 で

---

be derived, the net value being the difference between the total of values drawn down to the bulk purse or bulk purses and the total of values redeemed from the bulk purse or bulk purses, the float value record being non-specific with regard to individual transactions.」。なお、クレームの翻訳では、日本における出願の同内容のクレーム表現を参考にした。また、〇数字は当方で見やすくするために補記したものである。

[45] クレーム 7 には in any of the preceding claims と書かれており、クレーム 1〜6 の各々に従属する場合についてクレームしている。

は、

①処理能力が劣る財布内の秘密鍵を処理能力が高い財布に送出、

②処理能力が劣る財布は処理能力が高い財布の公開鍵でデータを暗号化するステップを踏む

ことを、クレーム 11 が、

①処理能力が劣る財布は共通鍵を持ち、この共通鍵を処理能力が高い財布に送出、

②処理能力が劣る財布は共通鍵で暗号化するステップを踏む

ことを記載している。具体的な暗号方式やプロトコルについては、これらのクレームでは特定していないが、それぞれ第 2 の実施例、第 3 の実施例として開示されている（図 14、15）。

最後のクレーム 12 は、クレーム 1～11 に従属し、前記コンピュータシステムが複数のコンピュータからなり、かつ金銭メータシステムがそれぞれ関連する前記コンピュータに対応した金銭メータを有する金銭振替システムについて記載している。

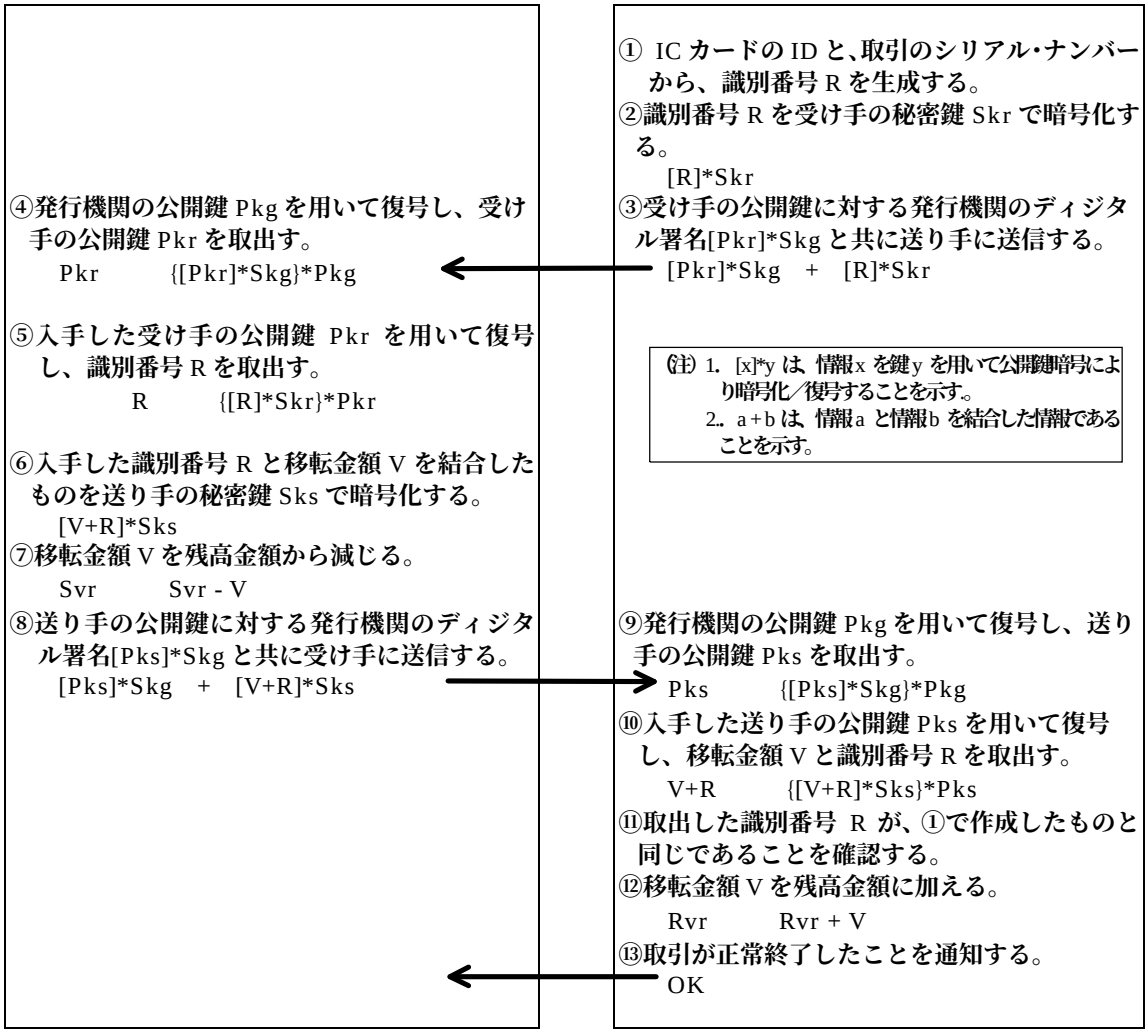
（図 13）送出財布、受取財布ともに RSA 暗号計算が可能な高い計算能力を持つ場合で、RSA 暗号を用いた暗号通信方法。

【財布内に格納されている秘密情報】

資金の送り手(S)	
Pkg	電子マネー発行機関の公開鍵
Pks	送り手の公開鍵
Sks	送り手の秘密鍵
[Pks]*Skg	送り手の公開鍵に対する発行機関のディジタル署名
Svr	送り手の財布の残高金額
Stl	ロジック記録 （取引不正終了ログ等）

資金の受け手(R)	
Pkg	電子マネー発行機関の公開鍵
Pkr	受け手の公開鍵
Skr	受け手の秘密鍵
[Pkr]*Skg	受け手の公開鍵に対する発行機関のディジタル署名
Rvr	受け手の財布の残高金額
Rtl	ロジック記録 （取引不正終了ログ等）

【暗号通信の手順】



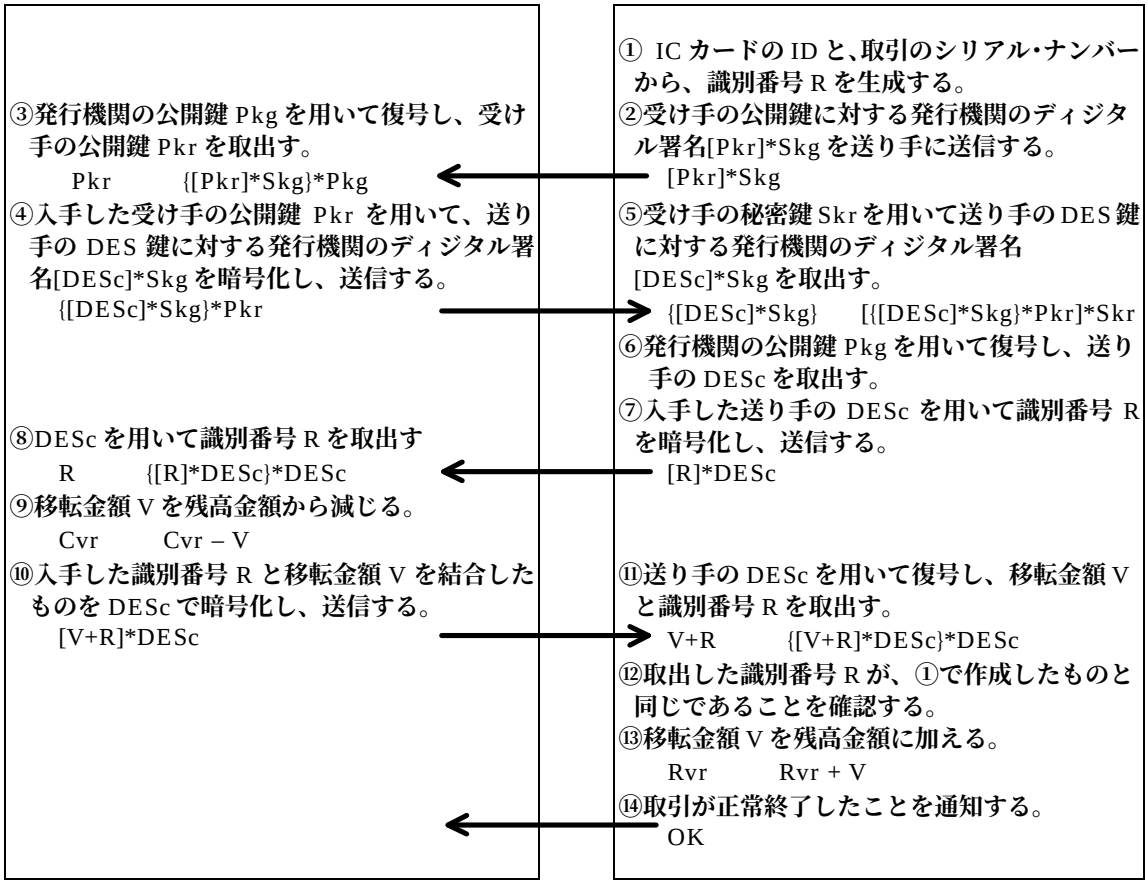
（図 14）受取財布は RSA 暗号計算が可能な計算能力を持つが、送出財布は計算能力が劣る場合で、DES 暗号を用いた暗号通信方法。

【財布内に格納されている秘密情報】

資金の送り手(S)	
Pkg	電子マネー発行機関の公開鍵
DESc	送り手の DES 鍵
[DESc]*Skg	送り手の DES 鍵に対する発行機関のディジタル署名
Cvr	送り手の財布の残高金額
Ctl	ロジック記録 （取引不正終了ログ等）

資金の受け手(R)	
Pkg	電子マネー発行機関の公開鍵
Pkr	受け手の公開鍵
Skr	受け手の秘密鍵
[Pkr]*Skg	受け手の公開鍵に対する発行機関のディジタル署名
Rvr	受け手の財布の残高金額
Rtl	ロジック記録 （取引不正終了ログ等）

【暗号通信の手順】



※ただし、本プロトコルでは[・]*Pks にかかる計算処理負荷が[・]* Sks に比べて軽くなるように鍵を設定している。

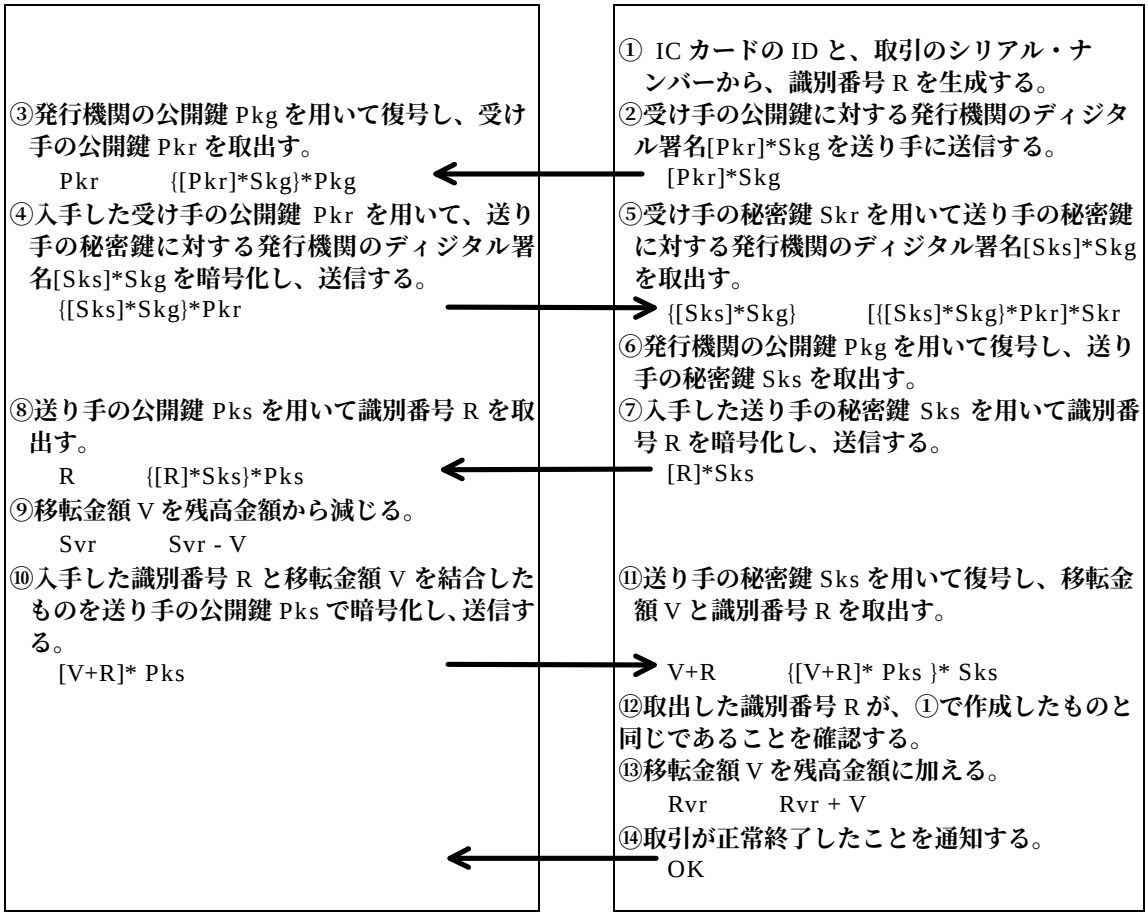
（図 15）受取財布は RSA 暗号計算が可能な計算能力を持つが、送出財布は計算能力が劣る場合で、送出財布が受取財布に対し RSA の秘密鍵を送ることによる暗号通信方法。

【財布内に格納されている秘密情報】

資金の送り手(S)	
Pkg	電子マネー発行機関の公開鍵
Pks	送り手の公開鍵
Sks	送り手の秘密鍵
[Sks]*Skg	送り手の秘密鍵に対する発行機関のディジタル署名
Svr	送り手の財布の残高金額
Stl	ロジック記録 （取引不正終了ログ等）

資金の受け手(R)	
Pkg	電子マネー発行機関の公開鍵
Pkr	受け手の公開鍵
Skr	受け手の秘密鍵
[Pkr]*Skg	受け手の公開鍵に対する発行機関のディジタル署名
Rvr	受け手の財布の残高金額
Rtl	ロジック記録 （取引不正終了ログ等）

【暗号通信の手順】



※ただし、本プロトコルでは[・]*Pks にかかる計算処理負荷が[・]*Sks に比べて軽くなるように鍵を設定している。

3. ビジネスの方法としてのアイデアを実現する技術に関する特許

この系譜に属する特許としては、Citibank, N. A.の Electronic monetary system （電子通貨システム）が有名である。以下ではこの特許の概略について、その審査の経緯を含めて説明する。

(1) Electronic monetary system (米国)

本特許[46]は、現在使っている現金の仕組みをネットワーク上にそのまま実現するとの発想に基づいて Citibank, N. A.の Rosen によって考案されたもので、世界 40 数カ国に亘って広く出願され、既に米国等一部の国では成立している。米国における特許審査の経緯をみると、2 回の拒絶査定を受け、度重なる補正を行ったたうえで成立するなど、審査官との間で様々な議論が行われた末の結論であることがわかる。

本特許は、1991 年 11 月に出願され（クレーム数は 32）、1992 年 1 月のクレームを追加する補正（クレーム数は 108 に増加）を経て審査にかけられたが、1994 年 2 月に第 1 回目の拒絶査定を受けている。米国特許商標庁の審査官は大半のクレームを対象にあげ、『これらのクレームは電子マネーの各機能を実現するための手順や手段を列挙したビジネスを行う方法を、実際に実行する装置に依存する等の制約を設けずに説明したものであり、米国特許法に定める特許の保護の対象である「方法、機械、製品、合成物、またはこれらの改良」（米国特許法＜35U.S.C＞101 条）に該当しない[47]』としている。また、すべてのクレームについて、前述の太田・岡本の「電子現金実施方法およびその装置」の米国特許や Jones and Higgins の「Value Transfer System」の国際特許公開資料等の『引用文献に開示されている内容により容易に想到できるため、米国特許法＜35U.S.C＞103 条により特許として保護することができない』と結論づけている。

これに対し、Citibank, N. A.は 1994 年 6 月に全てのクレームを書き換える補正を行ったが（クレーム数は 92 に変更）、1994 年 8 月、再び同様の理由によって 2 度目の拒絶査定を受けている。Citibank, N. A.は米国特許商標庁の審査官に対して、電子マネーシステムのデモンストレーションを行うとともに、電話インタビュー等により意見陳述を行い、一部のクレームについて、「データ処理システムを持つ決済銀行」、「プロセッサに依存した電子モジュール」等と装置に依存した制約を付加する記述に訂正する補正（削除 3、修正 2、追加 12）を行って（クレーム数は 101 に増加）、『ビジネスを行う方法そのものであって米国特許法＜35U.S.C＞101 条に定められている特許の保護の対象ではない』との拒絶理由を解消した。さらに、各独立クレームについて引用文献から想到できるアイデアと

---

[46] US Patent Number は 5,453,601（出願日 1991 年 11 月 15 日、発効日 1995 年 9 月 26 日）である。

[47] 審査官は次の判例を参照するよう例示している。
Hotel Security Checking Co. v. Lorraine Co.事件の判決<160 F. 467 (1908)>、In re Wait 事件の判決<24 USPQ 88 (CCPA 1934)>、Loew's Drive-In Theatres v. Park-In Theatres Inc.事件の判決<53 USPQ 376 (CCPA 1942)>、In re Patton 事件の判決<81 USPQ 149 (Ct. of App., 1st Cir. 1949)>、Ex parte Murray 事件の判決<9 USPQ 2d 1819 (PTO Bd. Pat. App. & Int'f, 1988)>。

の違いを明確にし、非自明性の主張を行って、1995 年 9 月に特許として成立している（一部のクレームについては単一性を理由に分割され、最終的なクレーム数は 98）。なお、1995 年 1 月には、同特許を優先権主張の拠り所にクレームを追加した同名の分割出願[48]が行われており（同 10 月に成立）、両者をあわせて「EMS 特許」と呼ぶことが多い。

<特許審査の経緯>
1991 年 11 月 15 日　米国において出願（米国出願番号 794,112）
1992 年　1 月 17 日　請求の範囲の補正（クレーム数 32→108）
1994 年　2 月　9 日　1 回目の拒絶理由通知（全クレームについて拒絶）
1994 年　6 月 27 日　請求の範囲の補正（クレーム数 108→92）
1994 年　8 月 15 日　2 回目の拒絶理由通知（全クレームについて拒絶）
1994 年 11 月 10 日　請求の範囲の補正（クレーム数 92→101）
1994 年 12 月　5 日　審査官が請求の範囲を認める（3 クレームは分割）
1995 年　9 月 26 日　U.S. Patent Number5,453,601 として発効
1995 年　1 月 27 日　米国出願番号 794,112 の分割出願（米国出願番号 378,955）
1995 年 10 月　3 日　米国出願番号 378,955 が U.S. Patent Number5,455,407 として発効

<U.S. Patent Number 5,453,601>

本特許は、顧客<subscriber>の電子財布<transaction module>、3 種類の銀行（発行銀行<issuing bank>、コルレス銀行<correspondent bank>、決済銀行<clearing bank>）、保証機構<certification agency>から構成されるスキームの中で、銀行預金の見合いに発行される電子マネー<electronic representation of currency / money>ないし貸付として発行される電子クレジット<electronic credit authorization>を実現する電子通貨システムの仕組み等について記述されているものである。なお、各機能を実現する具体的な技術については特に触れておらず[49]、システムを実現するときの構成要素、およびそれらの機能・要件等を記載しているのが特徴である。クレームは全部で 98 項（独立項 21、従属項 77）からなり、クレーム 1 からクレーム 48 およびクレーム 87 からクレーム 98 が様々な特徴を持った電子マネーのシステムを記載しているのに対し、クレーム 49 からクレーム 86 は各処理の手順ないし方法を記載している。

電子マネーのシステムを記載したクレームは、それぞれ発行銀行と電子財布からなる基本的なスキームをもとに、コルレス銀行や決済銀行等の付加する構成要素毎に微妙に請求の範囲、対象をずらしながら書き分けられており、これらを組み合わせることで様々なバリエーションの電子マネーシステムが特許の保護対象となるように工夫されている（図 16 参照）。電子マネー処理の手順ないし方法を記載したクレームは、預け入れ、引き出し、支払い、外国通貨建て電子マネーとの交換等の処理毎に、各構成要素間のやり取りの方法

[48] US Patent Number は 5,455,407（出願日 1995 年 1 月 27 日、発効日 1995 年 10 月 3 日）。
[49] 日本電信電話（株）等の一連の特許では、電子マネーを実現する方法を数学的に裏付けしながら、具体的方法を記述しているのに対し、Citibank, N. A.特許は個々の技術については特定しないとしている。

等を記載している（図 17 参照）。

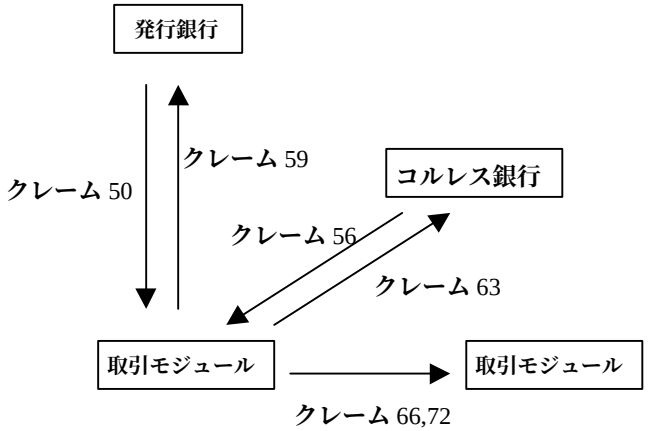
以下では、個々のクレームについて説明する（各独立クレームの関係およびクレームの従属関係については図 18 参照）。

（図 16）各独立クレームが記載しているシステムの構成要素等

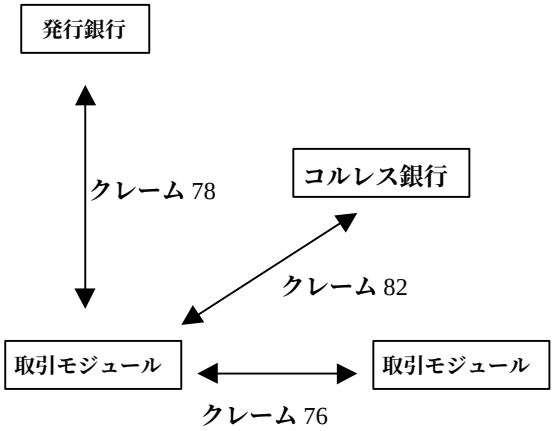
独立クレームの番号	1	13	20	26	33	37	41	45	47	87
決済銀行						○	○			
データ処理システム						○	○			
発行銀行	○	○	○	○	○	○複数	○複数	○	○	
オンライン会計システム	○	○	○	○	○	○	○	○	○	
金銭発生モジュール	○	○	○	○	○	○	○	○	○	
出納モジュール	○	○	○	○	○	○	○	○	○	
コルレス銀行					○					
オンライン会計システム					○					
出納モジュール					○					
取引モジュール	○	○	○	○	○					
（電子モジュール<取引+出納>）										
保証機構			○							
金銭発生調整システム								○		
取引調整システム									○	
通貨の電子的象徴	○	○	○		○	○		○		
初期の貨幣的価値（を含む）	○									
移転レコード	○									
満了日		○								
発行銀行認識票						○				
手形認識票								○		
電子的信用認可				○			○			
口座番号、貨幣的価値、署名				○						
発行銀行認識票							○			
電子手形										○
本体グループ(貨幣的価値等)										○
移転グループ(移転レコード)										○
署名＆証明グループ										○

※斜線部は、特に他のクレームとの構成要素の違いが表れている部分。

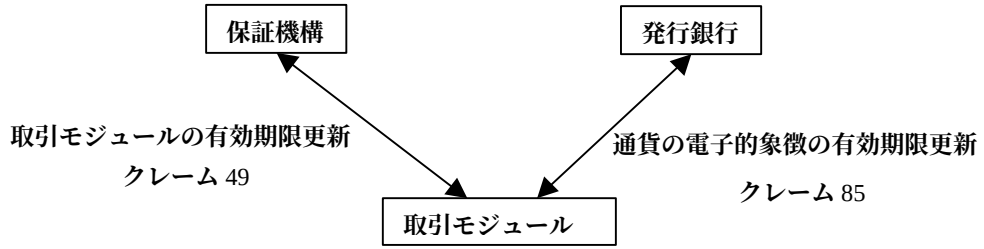
（図 17）各独立クレームが記載している処理の方法



通貨の電子的象徴の移転処理方法
（預け入れ、引き出し、支払い）

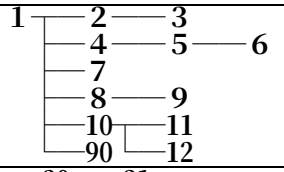
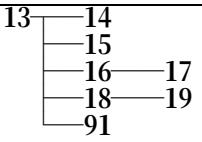
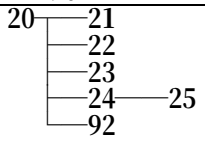
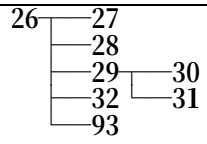
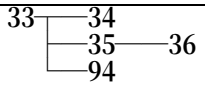
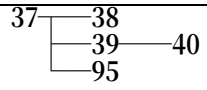
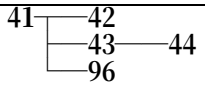
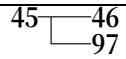
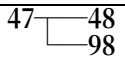
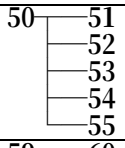
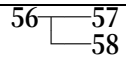
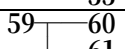
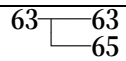
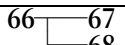
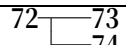
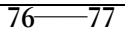
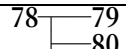
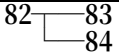
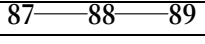


外国通貨の電子的象徴の交換処理方法



有効期限の更新処理方法

（図 18）各クレームの従属関係および主な記載内容

クレームの記載内容	従属関係	クレームの記載内容	従属関係
発行銀行と電子財布からなる基本的なスキームにおいて転々流通可能な電子マネーを扱うシステム		基本的なスキームにおいて有効期限のある電子マネーを扱うシステム	
各モジュールを一定有効期間保証する保証機構を加えたスキームにおいて電子マネーを扱うシステム		基本的なスキームにおいて電子クレジットを扱うシステム	
電子マネーを取り扱う複数のコルレス銀行を加えたスキームにおいて電子マネーを扱うシステム		発行銀行が複数あり、各々の電子マネーを交換決済する決済銀行を加えたスキームにおいて電子マネーを扱うシステム	
発行銀行が複数あり、各々の電子マネーを交換決済する決済銀行を加えたスキームにおいて電子クレジットを扱うシステム		金銭発生調整システムが還流してきた電子マネーの消込みチェックを行うことによって偽造を検出可能な、電子マネーを扱うシステム	
全体としての処理の整合性を保つための取引調整システムを備えた、電子マネーを扱うシステム。		取引モジュールの有効期限を更新する方法	49
加入者が取引モジュールを使って発行銀行から預金を引き出す方法		加入者が取引モジュールを使って発行銀行に預金する方法	
加入者が取引モジュールを使ってコルレス銀行から預金を引き出す方法		加入者が取引モジュールを使ってコルレス銀行に預金する方法	
取引モジュール間で電子マネーの移転を行うことによって支払いを行う方法		耐タンパー性のある金銭モジュール間で電子マネーの移転を行うことによって支払いを行う方法	
取引モジュール間で異なる外国通貨の電子マネーを交換する方法		取引モジュールと発行銀行の間で異なる外国通貨の電子マネーを交換する方法	
取引モジュールとコルレス銀行の間で異なる外国通貨の電子マネーを交換する方法		取引モジュール内の電子マネーの有効期限を更新する方法	
電子マネーの構成情報			

(a)クレーム 1 からクレーム 12 について

クレーム 1（独立クレーム）では電子通貨システムの構成要素として、「オンライン会計システムを有する発行銀行」、「通貨の電子的象徴」（電子マネー）、「発行銀行に関連装備された金銭発生モジュール」と「出納モジュール」、「取引モジュール」（電子財布）を示すとともに、通貨の電子的象徴は初期の貨幣的価値を含むものであること、出納モジュールと取引モジュールは、移転レコードにかかる処理を行う能力を持つプロセッサを有するものであること等を記載している。なお、「移転された貨幣的価値を有する移転レコードを発生し、かつ前記移転された通貨の電子的象徴において前記移転レコードを含む」から、電子マネーは分割可能性のほか転々流通性を持つものとして記述されていることがわかる。

クレーム 1:

「①オンライン会計システムを有する発行銀行と、

②前記発行銀行の流動負債として前記オンライン会計システムにおいて貸し越される通貨の電子的象徴と、

③前記通貨の電子的象徴を発生するために前記発行銀行に関連装備された金銭発生モジュールと、

④前記通貨の電子的象徴をストアするとともに、前記通貨の電子的象徴を含む銀行取引を中継することができるように前記発行銀行に関連装備された出納モジュールと、

⑤前記通貨の電子的象徴をストアし、前記発行銀行とオンライン取引を行い、さらに、前記通貨の電子的象徴をオフライン取引において他の取引モジュールとの間で交換することができる取引モジュールを備え、

⑥前記通貨の電子的象徴の各々が前記金銭発生モジュールにより生成された初期の貨幣的価値を含むものであり、

⑦前記出納モジュール及び取引モジュールはそれらのモジュールが前記通貨の電子的象徴の１つを振込先モジュールに移転する振出元モジュールとして機能するときにおいて、移転された貨幣的価値を有する移転レコードを発生し、かつ前記移転された通貨の電子的象徴において前記移転レコードを含むことができるプロセッサを有するものであること

を特徴とする電子通貨システム。」[50]

[50] 原文は、「An electronic monetary system comprising: an issuing bank having an on-line accounting system; electronic representations of currency that are credited in said on-line accounting system as current liabilities of said issuing bank; a money generator module associated with said issuing bank, for generating said electronic representations of currency; a teller module associated with said Issuing bank, capable of storing said electronic representations of currency, and intermediating banking transactions involving said electronic representations of currency; a transaction module capable of storing said electronic representations of currency, performing on-line transactions with said Issuing bank, and exchanging said electronic representations of currency with other transaction modules in off-line transactions; where said electronic representations of currency each include an original monetary value

なお、このクレームに従属するクレーム 2～12 では、それぞれ、クレーム 2～3 では出納モジュールおよび取引モジュールは、個々の電子マネーの現在の価値を記録する領域を持ち、この記録が移転した価値に応じて減額されることを、クレーム 4～6 では電子マネーが金銭発生モジュールおよび譲渡元モジュールのディジタル署名と、それらを検証する保証機構のディジタル署名付き検証鍵を含むことを、クレーム 7 では電子マネーの移転レコードに移転日および振込先モジュールの認識票が含まれることを、クレーム 8～9 では電子マネーに振出元および振込先のモジュールの認識票が含まれ、電子マネーに収められた最新の振出元のモジュール認識票が振出元のモジュール認識票に等しいかどうかを確認することを、クレーム 10～12 では各モジュールが「暗号保証セッション」により不正行為を防止する機能を持つほか、状態を元に戻すことによって取引を中止することができないよう取引の記録を取りながら処理することを記載している。

(b)クレーム 13 からクレーム 19 について

クレーム 13（独立クレーム）に記載された内容は、クレーム 1 において、通貨の電子的象徴に含まれるものの内容（初期の貨幣的価値、移転レコード）に関する記載を削除し、電子マネーに有効期限の概念を持たせるために必要な記載に置き換えたものである。基本的な構成要素は同じであるため、①から⑤まではまったく同じ記載となっている。

クレーム 13：

「①オンライン会計システムを有する発行銀行と、
②前記発行銀行の流動負債として前記オンライン会計システムにおいて貸し越される通貨の電子的象徴と、
③前記通貨の電子的象徴を発生するために前記発行銀行に関連装備された金銭発生モジュールと、
④前記通貨の電子的象徴をストアするとともに、前記通貨の電子的象徴を含む銀行取引を中継することができるように前記発行銀行に関連装備された出納モジュールと、
⑤前記通貨の電子的象徴をストアし、前記発行銀行とオンライン取引を行い、さらに、前記通貨の電子的象徴をオフライン取引において他の取引モジュールとの間で交換することができる取引モジュールとを備え、
⑥前記通貨の電子的象徴の各々が満了日を含み、

---

generated by said money generator module; and said teller and transaction modules having processors operative, when said modules are functioning as transferor modules transferring one of said electronic representations of currency to a transferee module, to generate and include in said transferred electronic representations of currency a transfer record having a transferred monetary value」。なお、クレームの翻訳では、日本における出願の同内容のクレームを参考にした。また、○数字は当方で見やすくするために補記したものである。

⑦前記他の取引モジュールは前記試みられた移転が前記通貨の電子的象徴の満了日後に生じた場合において、その電子的象徴の移転の受入れを拒否するようにしたプロセッサを有するものであること

を特徴とする電子通貨システム。」

なお、クレーム 14 からクレーム 19 はこれに従属するクレームであり、クレーム 14 では（オンライン会計システムを有する）「発行銀行が前記通貨の電子的象徴の預け入れ及び引き出し中において適当な会計手段を維持するための会計処理手段を有する」ことを、クレーム 15 では有効期限が電子マネーの貨幣的価値に応じて変化することを、クレーム 16～17 では出納モジュールとの取引において電子マネーを新たなものに交換することによって有効期限を更新することができることを、クレーム 18～19 では各モジュールが「暗号保証セッション」により不正行為を防止する機能を持つほか、状態を元に戻すことによって取引を中止することができないよう取引の記録を取りながら処理することができることを記載している。

(c)クレーム 20 からクレーム 25 について

クレーム 20（独立クレーム）に記載された内容は、クレーム 1 において、通貨の電子的象徴に含まれるものの内容（初期の貨幣的価値、移転レコード）に関する記載を削除し、「システム全体を通じた保証を実行するための保証機構」を新たな構成要素として加え、さらに、各モジュールがこの保証機構によって発行された「一定の時間内のみ有効性を与える」証明手段によって、有効期限を持つことを記載している。

クレーム 20：

「①オンライン会計システムを有する発行銀行と、

②前記発行銀行の流動負債として前記オンライン会計システムにおいて貸し越される通貨の電子的象徴と、

③前記通貨の電子的象徴を発生するために前記発行銀行に関連装備された金銭発生モジュールと、

④前記通貨の電子的象徴をストアするとともに、前記通貨の電子的象徴を含む銀行取引を中継することができるように前記発行銀行に関連装備された出納モジュールと、

⑤前記通貨の電子的象徴をストアし、前記発行銀行とオンライン取引を行い、さらに、前記通貨の電子的象徴をオフライン取引において他の取引モジュールとの間で交換することができる取引モジュールと、

⑥システム全体を通じた保証を実行するために用いられる保証機構とを備え、

⑦前記金銭発生モジュール、前記出納モジュール、および前記取引モジュールの各々が前記保証機構によってディジタル署名された証明手段内に収められた独自のモジュール認識票に関連し、前記証明手段が一定の時間内のみ有効性を与えるもので

あり、その時間が経過した後は前記認識票に関連付けられたモジュールが新たな証明手段を得るまでは他のモジュールとの取引ができないこと

を特徴とする電子通貨システム。」

(d)クレーム 26 からクレーム 32 について

クレーム 1 が「通貨の電子的象徴」である電子マネーを扱う電子通貨システムについて記載しているのに対し、クレーム 26（独立クレーム）は加入者の貸付勘定に依存する「電子的信用認可」である電子クレジットを扱う電子通貨システムについて記載している点が大きな違いである。クレーム 1 の①から⑤に記載されている構成要素等はそのままに、電子マネーは電子クレジットに置き換えられ、電子クレジットを構成する情報や、これに伴って変更となる預け入れ時の発行銀行の勘定処理等が記載されている。なお、これに従属するクレーム 32 では取引モジュールが電子マネーと電子クレジットの両方を一つの取引で扱うことが可能であるとしている。

クレーム 26：

「①オンライン会計システムを有する発行銀行と、

②前記オンライン会計システムにおける加入者の利用可能な信用供与限度を減少させるように、前記加入者の貸付勘定に依存する電子的信用認可と、

③前記電子的信用認可を発生するために前記発行銀行に関連装備された金銭発生モジュールと、

④前記電子的信用認可をストアするとともに、前記電子的信用認可を含む銀行取引を中継することができるように前記発行銀行に関連装備された出納モジュールと、

⑤前記電子的信用認可をストアし、前記発行銀行とオンライン取引を行い、さらに、前記電子的信用認可をオフライン取引において他の取引モジュールとの間で交換することができる取引モジュールとを備え、

⑥前記電子的信用認可が前記加入者の貸付勘定の口座番号、前記金銭発生モジュールにより生成された初期の貨幣的価値及びディジタル署名を含むものであり、

⑦前記電子的信用認可が預け入れられたとき、前記発行銀行は前記加入者の貸付勘定に前記貨幣的価値の借方記入を行うものであること

を特徴とする電子通貨システム。」

(e)クレーム 33 からクレーム 36 について

クレーム 33（独立クレーム）は、電子マネーを発行する発行銀行以外に、これを取り扱って流通させる複数のコルレス銀行の存在を前提にしている。クレーム 1 において、通貨の電子的象徴の内容（初期の貨幣的価値、移転レコード）に関する記載を削除し、クレーム 1 で記載している構成要素に加えて、オンライン会計システムを有し「発行銀行における会計を維持することができる複数のコルレス銀行」、「各々のコルレス銀行の１つに関連し複数個設けられた出納モジュール」を追加するとともに、電子財布たる取引モジュールは

発行銀行あるいはコルレス銀行の出納モジュールとの間で相互に電子マネーを交換できること、それぞれの出納モジュールは取引を仲介できるプロセッサを持つことを記載している。

クレーム 33：

「①第 1 のオンライン会計システムを有する発行銀行と、
②前記発行銀行の流動負債として前記第 1 のオンライン会計システムにおいて貸し越される通貨の電子的象徴と、
③前記通貨の電子的象徴を発生するために前記発行銀行に関連装備された金銭発生モジュールと、
④前記通貨の電子的象徴をストアするために前記発行銀行に関連装備された第 1 の出納モジュールと、
⑤各々が第 2 のオンライン会計システムを有するとともに、前記発行銀行における会計を維持することができる複数のコルレス銀行と、
⑥各々が前記コルレス銀行の１つに関連し、前記通貨の電子的象徴をストアすることができるように複数個設けられた第 2 の出納モジュールと、
⑦前記通貨の電子的象徴をストアし、前記複数のコルレス銀行又は前記発行銀行との間でオンライン取引を行い、さらに、前記通貨の電子的象徴をオフライン取引において他の取引モジュールとの間で交換することができる取引モジュールとを備え、
⑧前記第 1 の出納モジュールは前記第 1 のオンライン会計システム、前記金銭発生モジュール、前記第 2 の出納モジュール、及び／又は前記取引モジュール相互間における取引を仲介することができる第 1 のプロセッサを有し、
⑨前記第 2 の出納モジュールは前記第 2 のオンライン会計システム、前記第 1 の出納モジュール、及び／又は前記取引モジュール相互間における取引を仲介することができる第 2 のプロセッサを有するものであること
を特徴とする電子通貨システム。」

(f)**クレーム** 37 **からクレーム** 44 **について**

クレーム 37（**独立クレーム**）**は、電子マネーの発行銀行が複数存在することを前提としている。クレーム** 1 **において、通貨の電子的象徴に含まれるものの内容（初期の貨幣的価値、移転レコード）に関する記載を削除し、クレーム** 1 **で示している構成要素に、「オンライン会計システムを有する複数の発行銀行」、電子マネーを「精算するためのデータ処理システムを有する決済銀行」を加えているほか、電子マネーの各々には発行銀行の認識票が含まれ、これによって決済銀行は電子マネーの交換･決済を行うことを記載している。**

クレーム 37：

「①オンライン会計システムを有する複数の発行銀行と、
②前記発行銀行の流動負債として前記オンライン会計システムにおいて貸し越される通貨の電子的象徴と、

③前記通貨の電子的象徴を発生するために前記複数の発行銀行に関連装備された複数の金銭発生モジュールと、
④前記通貨の電子的象徴をストアすることができるように前記複数の発行銀行に関連装備された複数の出納モジュールと、
⑤前記複数の発行銀行が各々１つの口座を有する場合において、前記通貨の電子的象徴を精算するためのデータ処理システムを有する決済銀行とを備え、
⑥前記通貨の電子的象徴の各々が発行銀行認識票を含み、
⑦前記複数の出納モジュールの各々がその発行銀行において預け入れられたものであるが、別の発行銀行により発行された通貨の電子的象徴を、前記決済銀行のデータ処理システムに送ることにより、前記発行銀行の口座を均衡させるとともに、前記通貨の電子的象徴の各々をその発行銀行認識票により指示された前記発行銀行に送ることができること
を特徴とする電子通貨システム。」

なお、クレーム 41（独立クレーム）はクレーム 37 における構成要素等をそのままに、電子マネーを電子クレジットに置き換えた独立クレームであり、発行銀行が複数存在することを前提に、各々が発行した「電子クレジット」を交換決済する決済銀行からなるスキームにおいて、電子クレジットを扱う電子通貨システムについて記載したものとなっている。

(g)クレーム 45 からクレーム 46 について

クレーム 45（独立クレーム）は、電子マネーを発行時に登録しておき、還流時に登録の有無を確認することによって、偽造を事後的にチェックする金銭発生調整システム<money issued reconciliation system>を発行銀行が備えている電子通貨システムについての記述である。クレーム 1 において、通貨の電子的象徴に含まれるものの内容（初期の貨幣的価値、移転レコード）に関する記載を「独自性の証明のために用いられる手形認識票」を含むことだけを記した記載に置き換え、構成要素としては「取引モジュール」については特に記載せず、「金銭発生調整システム」を新たに加え、これが発行銀行から発行された電子マネーの記録を保持し、預け入れられた通貨の電子的象徴と照合することにより、偽造をチェックすることを記載している。

クレーム 45：
「①オンライン会計システム及び金銭発生調整システムを有する発行銀行と、
②前記オンライン会計システムにおいて勘定される通貨の電子的象徴と、
③前記通貨の電子的象徴を発生するために前記発行銀行に関連装備された金銭発生モジュールと、
④前記通貨の電子的象徴をストアできるように前記発行銀行に関連装備された出納モジュールとを備え、
⑤前記通貨の電子的象徴が各々の独自性の証明のために用いられる手形認識票を含み、

⑥前記金銭発生調整システムが前記発行銀行から発行された前記通貨の電子的象徴のレコードを維持するものであり、
⑦預け入れられた前記通貨の電子的象徴が、それに対して発行された通貨の電子的象徴に符合させるためのプロセッサを有する前記金銭発生調整システムに送られるものであり、
⑧符合しない場合には、システムにおいて偽造手形であることを表示できるようにしたこと
を特徴とする電子通貨システム。」

(h)クレーム 47 からクレーム 48 について

クレーム 47（独立クレーム）は、発行銀行が処理の整合性を保つための取引調整システムを備えた電子通貨システムについてのクレームである。構成要素としては、「オンライン会計システム及び取引調整システムを有する発行銀行」、「通貨の電子的象徴」（電子マネー）、「発行銀行に関連装備された金銭発生モジュール」および「出納モジュール」といった取引調整システムと直接関連のある要素のみが示され、取引調整システムが金銭発生モジュール、出納モジュール、及びオンライン会計システムからの取引レコードの相互の整合性を定期的にチェックすることを記載している。

クレーム 47：
「①オンライン会計システム及び取引調整システムを有する発行銀行と、
②前記オンライン会計システムにおいて勘定される通貨の電子的象徴と、
③前記通貨の電子的象徴を発生するために前記発行銀行に関連装備された金銭発生モジュールと、
④前記通貨の電子的象徴をストアすることができるように前記発行銀行に関連装備された出納モジュールとを備え、
⑤前記金銭発生モジュール、前記出納モジュール、及び前記オンライン会計システムからの取引レコードが前記取引調整システムに周期的に送られるようにし、
⑥前記取引調整システムが前記取引レコードを分析して出納モジュールの取引が妥当な会計処理と符合し、かつ金銭発生モジュールの取引が妥当な出納モジュールの取引及び会計処理と符合していることを確認するためのプロセッサを有し、
⑦何らかの不一致があったときは不完全処理又はセキュリティ侵害があったことを表示できること
を特徴とする電子通貨システム。」

(i)クレーム 50 からクレーム 75 について

これまでのクレームが構成要素やそれぞれの要素が満たす機能や要件を記載したシステムに関するものであったのに対し、クレーム 50 からクレーム 75 は、預け入れ、引き出し、支払い等の具体的な処理を実現するためのステップを順を追って記載した方法に関するも

のとなっている。

まず、クレーム 50 は、「出納モジュール、金銭発行モジュール、及びオンライン会計システムを有する発行銀行において、加入者の銀行口座から預金引き出しを行うために加入者が取引モジュールを利用する方法」の具体的なステップを記載したクレームで、発行機関、取引モジュール、電子マネーからなる基本的なスキームにおける電子マネー引き出しの方法を記載したものである。

クレーム 50：

「出納モジュール、金銭発生モジュール、及びオンライン会計システムを有する発行銀行において、加入者の銀行口座から預金引き出しを行うために加入者が取引モジュールを利用する方法であって、

(a) 前記加入者が前記取引モジュールを介して前記預金引き出しを行うべき前記銀行口座、及び引き出し額を選択するステップと、

(b) 前記取引モジュールが前記出納モジュールとの間で第 1 の暗号保証セッションを確立するステップと、

(c) 前記取引モジュールが前記第 1 の暗号保証セッションを介して前記取引モジュールに対して引き出し要求を送り、この場合において、前記引き出し要求が前記引き出し額及び前記銀行口座に対応する銀行口座情報を含むようにしたステップと、

(d) 前記銀行口座情報をチェックしてその有効性を検証するステップと、

(e) 前記銀行口座に十分な資金があるか否かをチェックするステップと、

(f) 前記出納モジュールが前記金銭発生モジュールとの間で第 2 の暗号保証セッションを確立するステップと、

(g) 前記出納モジュールが前記第 2 の暗号保証セッションを介して前記金銭発生モジュールに対して、要求された手形価値を有する通貨の発生要求を送るステップと、

(h) 前記要求された手形価値だけ前記オンライン会計システムにおいて金銭発行勘定を貸方記入するステップと、

(i) 前記オンライン会計システムにおいて、前記銀行口座に前記引き出し額を借方記入するステップと、

(j) 前記金銭発生モジュールが前記要求された手形価値における第1の通貨の電子的象徴を発生するステップと、

(k) 前記第 2 の暗号保証セッションを介して前記第 1 の通貨の電子的象徴を前記出納モジュールに移転するステップと、

(l) 前記第1の暗号保証セッションを介して前記第1の通貨の電子的象徴を前記出納モジュールから前記取引モジュールに移転するステップと、

(m) 前記取引モジュールと前記出納モジュールのセッションを関連させるステップと、

(n) 前記出納モジュール及び前記貨幣発生モジュールセッションを関連させるステップとからなること

を特徴とする加入者が取引モジュールを利用して引き出しを行う方法。」

同じく基本的なスキームにおける電子マネーを預け入れるための方法がクレーム 59 に記載されているほか、コルレス銀行が存在するスキームにおいて、コルレス銀行から電子マネーを引き出すための方法がクレーム 56 に、預け入れのための方法がクレーム 63 に記載されている。

また、クレーム 66 では、「加入者が第 1 の取引モジュールを用いて第 2 の取引モジュールに通貨の電子的象徴を移転することにより支払いを行うための方法」と、取引モジュール間の電子マネーの移転方法を記載している。なお、クレーム 71 は特にクレーム 66 における第 1 の加入者と第 2 の加入者が「ある一人の人物、又はその人物により前記取引モジュールを制御するために用いられた電子処理装置のいずれかであることを特徴」とする方法を記載した従属項であり、加入者が複数保有する取引モジュール間での電子マネーの移転についてもクレームの範囲であることを敢えて明記したかたちとなっている。さらに、クレーム 72 は、「第 1 の金銭モジュール<money module>を用いて第 2 の金銭モジュールに通貨の電子的象徴を移転することにより支払いを行うための方法」を金銭モジュールが対タンパー性を持つことを前提に、そのステップを記載したクレームである。

(j)クレーム 76 からクレーム 84 について

クレーム 76 からクレーム 84 は、加入者の取引モジュールにストアされている電子マネーを異なる外国通貨の電子マネーと交換するための方法を記載したクレームであり、３つの交換に応じる対象（他の加入者の取引モジュール、発行銀行、コルレス銀行）毎に、独立したクレームが存在する。まず、クレーム 76 は、「加入者が第 1 の取引モジュールにストアされた第 1 の外国通貨の電子的象徴を第 2 の取引モジュールにストアされた第 2 の外国通貨の電子的象徴に交換するための方法」の具体的なステップを記載したクレームである。２つの電子財布間における電子マネーの移転を行うための方法を記載したものであるが、その安全性が具体的にどのように実現されているかについては「暗号保証セッションを通じて」と書かれているのみであり、実施例にも特に記載はない。以下、加入者が取引モジュールにストアされた第 1 の外国通貨の電子的象徴を、「発行銀行から発行された第 2 の外国通貨の電子的象徴と交換するための方法」（クレーム 78）、「発行銀行から発行され、かつコルレス銀行が受け入れた第 2 の外国通貨の電子的象徴と交換するための方法」（クレーム 82）、に関するステップを記載したクレームが続いている。

クレーム 76：

「加入者が第 1 の取引モジュールにストアされた第 1 の外国通貨の電子的象徴を第 2 の取引モジュールにストアされた第 2 の外国通貨の電子的象徴に交換するための方法であって、

(a) 前記第 1 の取引モジュールと前記第 2 の取引モジュールとの間において第 2 の外国通貨暗号保証セッションを確立するステップと、

(b) 第 1 の加入者が前記第 1 の取引モジュールを介して売られるべき前記第 1 の外国

通貨を表す第 1 の金額と交換レートを選択するステップと、
(c) 前記第 1 の取引モジュールが十分な資金を有するか否かをチェックするステップと、
(d) 前記第 1 の取引モジュールが前記第 1 の金額及び前記交換レートを前記暗号保証セッションを介して前記第 2 の取引モジュールに送るステップと、
(e) 前記第 2 の取引モジュールがその所有者に対し前記第 1 の金額及び前記交換レートを検証するように促すステップと
(f) 前記第 2 の取引モジュールが十分な資金を有するか否かをチェックするステップと、
(h) 前記第 1 の取引モジュールが前記暗号保証セッションを介して前記第 2 の取引モジュールに前記第 1 の金額における前記第 1 の外国通貨の電子的象徴を送るステップと、
(i) 前記第 2 の取引モジュールが前記暗号保証セッションを介して前記第 1 の取引モジュールに前記第 1 の金額及び前記交換レートから計算された第 2 の金額において、前記交換レートから計算された第 2 の金額において、前記第 2 の外国通貨の電子的象徴を送るステップと、
(j) 前記第 1 および第 2 の取引モジュールセッションを関連動作させるステップを含むこと
を特徴とする電子通貨交換方法。」

(k)クレーム 49 およびクレーム 85 からクレーム 86 について

クレーム 49 は「保証機構との相互作用により更新されるようにした時間的保証を有する取引モジュールの更新方法」、すなわち、取引モジュールの有効期限を更新する方法について記載したクレームである。また、クレーム 85 は「取引モジュールにストアされた満了日を有する通貨の電子的象徴を通貨の更新された電子的象徴によって更新するための方法」に関するステップを記載したクレームであり、見かけ上電子マネーの有効期限を延長することができる方法について記述している。

(l)クレーム 87 から 89 について

クレーム 87 は、電子マネーに含まれる情報を記載したものであり、「電子手形<electronic note>をストアするメモリを有するプロセッサを主体とする電子モジュール」間で電子手形を移転する電子通貨システムにおいて、電子通貨のデータ構造が「貨幣的価値を示すデータを含むデータフィールドの本体グループ」、「複数の移転レコードのリストを含むデータフィールドからなる移転グループ」、「振出人の電子モジュールのディジタル署名及び証明手段を収容した振出人リストを含むデータフィールドからなる署名及び証明手段グループ」からなる場合を記載している。なお、さらに詳細な具体的な内容が実施例に開示されている。

クレーム 87：

「①プロセッサを主体とする電子モジュール間において電子手形を移転するためのシステムであって、

②暗号保証チャンネルを形成し、かつ前記暗号保証チャンネルを介して電子手形を移転し及び受信することができるとととともに、前記電子手形をストアするためのメモリを有する複数のプロセッサを主体とする電子モジュールを備えたものにおいて、

③ストアされた電子手形の各々が、前記電子手形の貨幣的価値を示すデータを含むデータフィールドの本体グループと、

④振出人の電子モジュールにより発生し、移転中において前記電子手形に付与される複数の移転レコードのリストを含むデータフィールドからなる移転グループと、

⑤振出人の電子モジュールのディジタル署名及び証明手段を収容した振出人リストを含むデータフィールドからなる署名及び証明グループを含むものであること

を特徴とする電子手形移転システム。」

(m)**クレーム** 90 **から** 98 **まで**

クレーム 90 **から** 98 **は、クレーム** 1 **からクレーム** 48 **における** 9 **種類のスキームの電子通貨システムにおいて、特に金銭発生モジュールと出納モジュールが単一のプロセッサを有する装置内に組み込まれたものであることを記載した従属クレームである。**

<U.S. Patent Number 5,455,407>

本特許は、U.S. Patent Number 5,453,601 **の分割特許であり、**4 **つの独立するクレームとそれぞれに従属する** 5 **つのクレームからなる。クレームはすべて電子マネーのシステムに関する** means plus function **クレームであり、**U.S. Patent Number 5,453,601 **ではカバーされていない電子マネーシステムのバリエーションや、発行銀行やコルレス銀行等の構成要素を敢えて明記しない電子マネーシステムに関して記載している。**

クレーム 1 **は、電子マネーを発行する発行銀行以外に、これを取り扱い流通させる複数のコルレス銀行の存在を前提にした電子マネーシステムに関するクレームであり、**U.S. Patent Number 5,453,601 **のクレーム** 33 **から、取引モジュールが発行銀行とも取引を行うように記載していた部分を削除したものである（変更点は下線部）。**U.S. Patent Number 5,453,601 **のクレーム** 33 **では、発行銀行、コルレス銀行、顧客からなる電子マネーシステムにおいて、発行銀行と顧客が直接取引をしないシステムを構築すれば、特許の保護対象から外れる可能性があったところを、本クレームにより保護する範囲に含めたものと考えられる。**

クレーム 1：

「①第 1 のオンライン会計システムを有する発行銀行と、

②前記発行銀行の流動負債として前記第 1 のオンライン会計システムにおいて貸し越

される通貨の電子的象徴と、
③前記通貨の電子的象徴を発生するために前記発行銀行に関連装備された金銭発生モジュールと、
④前記通貨の電子的象徴をストアするために前記発行銀行に関連装備された第 1 の出納モジュールと、
⑤各々が第 2 のオンライン会計システムを有するとともに、前記発行銀行における会計を維持することができる複数のコルレス銀行と、
⑥各々が前記コルレス銀行の１つに関連し、前記通貨の電子的象徴をストアすることができるように複数個設けられた第 2 の出納モジュールと、
⑦前記通貨の電子的象徴をストアし、前記複数のコルレス銀行又は前記発行銀行との間でオンライン取引を行い、さらに、前記通貨の電子的象徴をオフライン取引において他の取引モジュールとの間で交換することができる取引モジュールとを備え、
⑧前記第 1 の出納モジュールは前記第 1 のオンライン会計システム、前記金銭発生モジュール、前記第 2 の出納モジュール相互間における取引を仲介することができる第 1 のプロセッサを有し、
⑨前記第 2 の出納モジュールは前記第 2 のオンライン会計システム、前記第 1 の出納モジュール、及び前記取引モジュール相互間における取引を仲介することができる第 2 のプロセッサを有するものであること
を特徴とする電子通貨システム。」

クレーム 2 は、複数の電子取引モジュールからなる移転システムにおいて、電子手形が有効期限を持つよう記載されたものである。U.S. Patent Number 5,453,601 のクレーム 13 から、発行銀行および発行銀行に関わる記載を削除するとともに、取引モジュールの構成要素をやや具体的に「メモリ」、「クロック」、「プロセッサ」を有する耐タンパー性を持つものであると記載している。取引モジュールの構成要素を一部特定する一方で、逆に取引モジュール以外の電子マネーシステムの基本的な構成要素については限定しない電子マネーシステムをクレームしている。

クレーム 2：
「①満了日を含む電子手形をストアするメモリと、システム時間を維持するクロックと、前記電子手形を移転し及び受信するための暗号保証チャンネルを提供するためのプロセッサを有し、耐タンパー性を持つ複数の電子取引モジュールであって、
②前記プロセッサがさらに、前記移転が前記手形の満了日の後に生じた場合において、前記取引モジュール間における前記電子手形の移転を許容しないように構成されたものを含む時間制取引モジュールによる移転システム。」

クレーム 6 は、複数の電子取引モジュールからなる移転システムにおいて、電子手形が移転レコードを持つよう記載されたものである。U.S. Patent Number 5,453,601 のクレーム 1 から、発行銀行および発行銀行に関わる記載を削除するとともに、取引モジュールの

構成要素をやや具体的に「メモリ」、「プロセッサ」を有する耐タンパー性を持つものであると記載している。取引モジュールの構成要素を一部特定する一方で、逆に取引モジュール以外の電子マネーシステムの基本的な構成要素については限定しない電子マネーシステムをクレームしている。

クレーム 6：

「①各々が移転された貨幣的価値を有する移転レコードを含む電子手形をストアするメモリと、前記電子手形を移転し及び受信するための暗号保証チャンネルを提供するためのプロセッサを有し、耐タンパー性を持つ複数の電子取引モジュールであって、
②前記プロセッサがさらに、移転中において前記移転レコードを発生するとともに、その移転レコードを前記電子手形に付記するようにしたものを備えた取引モジュールによる移転システム。」

クレーム 9 は、複数の電子取引モジュールからなる移転システムにおいて、各電子モジュールが有効期限付きの証明手段を有するように記載されたものである。U.S. Patent Number 5,453,601 のクレーム 20 から、発行銀行および発行銀行に関わる記載を削除するとともに、取引モジュールの構成要素をやや具体的に「モジュール認識票」、「クロック」、「メモリ」、「プロセッサ」を有する耐タンパー性を持つものであると記載している。取引モジュールの構成要素を一部特定する一方で、逆に取引モジュール以外の電子マネーシステムの基本的な構成要素については限定しない電子マネーシステムをクレームしている。

クレーム 9：

「①通貨取引システムの安全性を確保する安全保証機構と、
②各々が前記保証機構によってディジタル署名された時限保証の範囲内に収められた独自のモジュール認識票と、システム時間を維持するクロックと、通貨の電子的象徴をストアするメモリと、前記通貨の電子的象徴を移転し及び受信するための暗号保証チャンネルを提供するプロセッサを有し、耐タンパー性を持つ複数の電子取引モジュールを備え、
③前記プロセッサがさらに、証明期間の満了した取引モジュールが他の取引モジュールとの間で取引することを新たな証明が得られるまで許容しないものであること
を特徴とする取引モジュールによる通貨取引システム。」

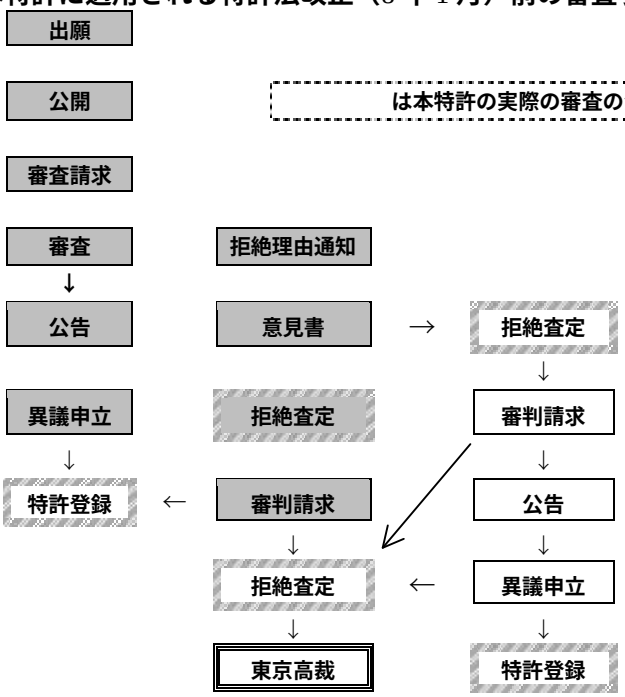
(2) 電子通貨システム (日本)

本特許は、日本においては 1995 年 11 月に公告はされたものの、多数の異議申立てがなされ、審査された結果、1997 年 12 月に拒絶査定がなされている。その後、さらに拒絶査定不服審判請求が行われるなど、最終的に決着しているわけではないが、少なくとも現時点で、同内容の特許が日米で異なる審査結果となっている興味深い事例でもあるため、この間の、日本における同特許の出願から拒絶査定を受けるまでの主な経緯、および拒絶査定の事由について概説する。

<特許審査の経緯および審査の手順>

1992 年 11 月 16 日　出願（特願平 04-330971、米国出願番号 794,112 による優先権主張）。
1993 年　2 月 10 日　請求の範囲の補正（クレーム数 108→66）
1993 年　3 月 15 日　出願審査請求（受付日 1993 年　3 月 17 日）
1994 年　6 月 10 日　出願公開（特開平 6-162059）
1994 年　9 月 28 日　拒絶理由通知（発送日 1994 年　10 月 11 日）
1995 年　4 月 11 日　意見書、請求の範囲の補正等（クレーム数 66→104）
1995 年 11 月 29 日　出願公告（特公平 7-111723）
1996 年　2 月　　特許異議申立て
1997 年　1 月 31 日　請求の範囲の補正（クレーム数 104→54）
1997 年　12 月 24 日　特許異議の決定および拒絶査定（発送日 1998 年　1 月 12 日）
1998 年　4 月 13 日　拒絶査定不服審判請求（拒絶査定不服審判番号　平 10-05570）

＜本特許に適用される特許法改正（8 年 1 月）前の審査手続の流れ＞



(a) 特許審査の経緯

（出願および審査請求）

日本においては、1992 年 11 月に米国出願番号 794,112 に対応した特許「電子通貨システム」が出願された。当初、クレーム数は 108 項目（優先権を主張する米国出願番号 794,112 の特許の第 1 回目の請求範囲補正後のクレームに対応）であったが、約 3 ヶ月後に請求の範囲を全面的に書き直し、クレーム数を 66 項目に減らしたうえで審査請求を行っている。その結果、特許庁の審査官は以下の３つの引用文献を示し、『この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明に基づいて、その出願前にその発明の属する技術の分野における通常の知識を有するものが容易に発明をすることができたものであるから、特許法第 29 条第２項の規定により特許を受けることができない。』として、全ての請求項について拒絶する判断を行っている。

（引用文献１）特開平 3-73065 号公報（前述の特許「電子現金実施方法およびその装置」）

（引用文献２）Okamoto, T. and Ohta, K., "Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash," Proc. of CRYPTO 89, LNCS 435, pp.481-496, Springer-Verlag, 1990.**（前述の特許「電子現金実施方法およびその装置」の内容を学会で発表したもの）**

（引用文献３）Chaum, D., “Security Without Identification: Transaction Systems to Make Big Brother Obsolete,” Communications of the ACM, Vol.28 NO.10, pp.1030-1044, 1985.

個々の請求項に対する拒絶理由をみると、その多くについては引用文献に記載されたものとの間には『格別の差異があるものとは認められず公知である』、あるいはこれに基づいて『容易に発明をすることができる』として新規性、進歩性を否定している。例えば、審査官は、以下のクレーム 1 等については、『引用文献１に記載されたものにおける（電子コイン）は他の加入者に譲渡することが可能である（引用文献１公報第 29 頁右上欄第９行～第３２頁右下欄第 2 行）。また、引用文献 2 に記載されたものも、第 492～493 頁の「5. Transferable Untraceable Electronic Cash」の頁に記載されているように、他の加入者に譲渡可能である。したがって、本願の請求項 1, 2, 3 ,5 および 6 に係る各発明と引用文献１あるいは２に記載されたものとの間に格別の差異があるものとは認められない。』としている。

クレーム 1（1993 年 2 月 10 日補正後）：

「金銭の電子的象徴を用い、かつ少なくとも１つの金融機関と前記金融機関により奉仕される加入者を含む通貨システムであって、

①各々が前記電子的象徴を、それが象徴する金額及び前記電子的象徴の有効性を支持するデータを含む機械読取可能なディジタル型において収容できるようにした複数の加入者プロセッサと、

②前記金融機関により用いられて前記加入者プロセッサと通信することにより、前記加入者プロセッサにストアされた電子的象徴を前記金融機関に預金すること、又は前記加入者プロセッサに対し前記金融機関から前記電子的象徴を払い戻すことを可能にした処理手段とを備え、
③前記加入者プロセッサはさらに、加入者プロセッサ間において前記電子的象徴の交換を行うことができるようにするための通信及び処理機能を含むものであること
を特徴とする通貨システム。」

また、引用文献には記載されていない処理を含むクレームについても、例えば、時間的制限を設けたり（クレーム 9）、回数制限を設けることによって安全性を図ること（クレーム 15）等は『周知の事項にすぎない』とか、複数の通貨単位を取り扱えるようにすること（クレーム 13）は、『当業者が容易に想到しうる設計的事項にすぎない』、等の理由で拒絶されている。

クレーム 9（1993 年 2 月 10 日補正後）：
「前記安全保障手段がさらに、前記取引手段間における前記信用および通貨の電子的象徴の移転可能性に時間的制限を与えるものであることを特徴とする請求項 8 記載のシステム」

クレーム 13（1993 年 2 月 10 日補正後）：
「前記発生手段がさらに、信用及び通貨のための電子的象徴を複数の通貨単位について発生するものであることを特徴とする請求項 7 記載のシステム」

クレーム 15（1993 年 2 月 10 日補正後）：
「前記信用の電子的象徴が前記取引手段により 1 回だけ移転されるようにしたことを特徴とする請求項 14 記載のシステム」

（拒絶理由通知を受けた補正手続および公告）

Citibank, N. A.では、拒絶理由通知を受け、クレームの全面的な補正（クレーム数は 104 項目に増加）[51]等を行うとともに、拒絶の理由はすべて解消したとする意見書を提出した。この意見書によれば Citibank, N. A.は、『上記３つの引用文献は、発行銀行、前記発行銀行に関連装備された金銭発生モジュール及び出納モジュール、前記発行銀行とオンライン取引を行い、かつ他の取引モジュールとの間におけるオフライン取引で電子通貨の交換を

[51] 1995 年 4 月の手続補正により、請求範囲は U.S. Patent Number 5,453,601 および U.S. Patent Number 5,455,407 を合せたものに相当するように変更された。なお、米国においても、出願時の米国出願番号 794,112 とそれが後に発効となった U.S. Patent Number 5,453,601 ではクレームの数が明らかに異なっており（前者が 32 項目に対し、後者は 98 項目）、日本出願と同様の内容修正が行われた模様である。

行うための取引モジュールからなる本願の電子マネー取引システムの構成を当業者に対して教示するものではない』ため、『本願発明は引用例からは教示されない進歩性を有するもの』であると主張している。この主張は審査官に受け入れられ、米国における特許が発効されてから間もない 1995 年 11 月、出願公告が行われている[52]。

なお、参考までに、請求の範囲の補正が行われた後のクレーム 1 を以下に示す。電子通貨システムが様々なモジュール等で構成されるものとして表現を改められており、補正前に比べると詳細な記述に変更されたため、請求の範囲は狭くなったと考えられる。

クレーム 1（1995 **年** 4 **月** 11 **日補正後**）:

「①オンライン会計システムを有する発行銀行と、
②前記発行銀行の流動負債として前記オンライン会計システムにおいて貸し越される通貨の電子的象徴と、
③前記通貨の電子的象徴を発生するために前記発行銀行に関連装備された金銭発生モジュールと、
④前記通貨の電子的象徴をストアするとともに、前記通貨の電子的象徴を含む銀行取引を中継することができるように前記発行銀行に関連装備された出納モジュールと、
⑤前記通貨の電子的象徴をストアし、前記発行銀行とオンライン取引を行い、さらに、前記通貨の電子的象徴をオフライン取引において他の取引モジュールとの間で交換することができる取引モジュールとを備え、
⑥前記通貨の電子的象徴の各々が前記金銭発生モジュールにより生成された初期の貨幣的価値を含むものであり、
⑦前記出納モジュール及び取引モジュールはそれらのモジュールが前記通貨の電子的象徴の１つを振込先モジュールに移転する振出元モジュールとして機能するときにおいて、移転された貨幣的価値を有する移転レコードを発生し、かつ前記移転された通貨の電子的象徴において前記移転レコードを含むことができるプロセッサを有するものであること
を特徴とする電子通貨システム。」

（異議申立ておよび拒絶査定）

公告期間が満了となる 1996 年 2 月、「電子マネーの仕組みや全体の考え方には新規性がなく、また、この種のシステムの仕組みが特許として認められるべきではない」等の意見に基づく複数の特許異議申立てが行われた。特許異議申立ての１つによれば、特許異義申立人は、複数の証拠を提示し、『この出願の発明はこれらの証拠に記載された事項及び周知の技術に基づいて当業者が容易に発明をすることができたものであるから、特許法第 29 条第 2 項の規定により特許を受けることができない』と主張した。これに対し、Citibank,

[52] 本特許は、1994 年の特許法改正前に出願された特許であるため、旧制度に基づいて審査手続が行われており、登録前に 3 ヶ月の公告期間が設けられている。

N. A.では、1997 年 1 月にクレームの範囲を縮小[53]する等（クレーム数は 54 項目）の補正を行うとともに、これを分割[54]する等の対抗策を打っているが、審査の結果、『出願の発明は、異義申立て人が提出した資料の記載事項や周知の技術に基づいて当事者が容易に発明をすることができたものであり、これらの請求項にかかる発明については、特許法第 9 条第 2 項の規定により、特許を受けることができない』として、1997 年 12 月に拒絶査定が下っている[55]（拒絶の事由の詳細については後述）。

（拒絶査定不服審判請求および審判）

Citibank, N. A.は拒絶査定を不服として、さらに 4 月に拒絶査定不服審判請求（不服審判番号：平 10-05570）を行うとともに、その後の補正可能期間内に手続補正書を提出している。補正は翻訳の誤りによる文言訂正や一部の補足説明の追加等、請求の範囲に関する軽微なものであり、あまり本質的なものではないが、補正書が提出されたことにより審査前置[56]が行われている。不服審判請求書に記されている拒絶査定が取り消されるべき理由によると、①出願内容と証拠として提出された資料が開示する内容はまったく異なるものであり、これをもとに容易に本発明を得られるとはいえないこと、②拒絶査定において、審査官は『請求項に記載された発明は、金融業界において普通に行われている手続を規定したにすぎず、電子的象徴の取引を実際に運用するうえで銀行側において普通に必要とされる機能を表明したというにすぎない』と判断しているが、拒絶査定は何らの引用文献も提示していないこと、等をあげ、合理的根拠を欠いた極めて偏った主観的な判断であると反論している。

既に審判請求に対する審査前置は 6 月に終了しているが、請求者の主張は審査官には受け入れられず、拒絶理由は解消されていないと判断されたため、現在、手続は審判官による審理[57]へと進んでいる。なお、前置報告書によると、『請求項に規定された事項を支持する記載は、技術的な部分は従来技術の援用に終始しており、内容に乏しい』、あるいは『電子的象徴を分割して使用する場合の実際的なプロトコルは何も開示しておらず．．．』等と、本出願内容が技術的開示に乏しいとの判断を行ない、『本願の各請求項に規定された事項を理解する場合には、詳細な説明に開示されたレベルで理解すべきであり、請求項や

[53] 主に、発行銀行やコルレス銀行から電子マネーを引き出したり預け入れる処理を行うなどの方法に関するクレームのすべてが削除された。
[54] 特開平 9-245108（公開日 1997 年 9 月 19 日）。
[55] なお、分割特許（特開平 9-245108）ついては拒絶査定の範囲には含まれていない。
[56] 補正書が審判請求後の補正可能期間（30 日）以内に提出されると、以前に審査した審査官が再び審査（審査前置）することになっている。従って、拒絶理由が解消しているときには、実質的な審判手続を経ずに出願がその審査官によって許可されるため、審査は早いとされている。
[57] 審判請求後、出願人が補正書を敢えて提出しなかったとき、あるいは審査前置の段階ででも拒絶理由が解消されないときは、審判官が審理を行う。審理は一般には 3 名の審判官による再度の審査であり、「審決」というかたちで結論が出され、さらに不服がある場合は東京高等裁判所に審決取り消し訴訟を提起することになる。

発明の詳細は説明で支持されていないレベルの主張は、排除されるべきである』と、拒絶査定の事由にはなかった一歩踏み込んだ判断が加えられていることが注目される。前置報告書のむすびにおいても、『本願は、電子的象徴に持たせる情報の内容、取引の形態、決済の形態、取引の内符合処理の形態など、思考実験で考えられる形態を包括的に特許請求するものである。しかし、詳細な説明での技術的裏付けの乏しさからみて、その実態は、何らかの取引価値を有するものに移転レコード（裏書き）を付し、これをハードウェアを介して転々流通させる場合の、取引、決済、符合処理の一形態を一般的に規定したにすぎず、技術的貢献をもたらすものではない。』という判断が示されている。

(b) 特許異議に対する拒絶査定の事由

以下、いくつかのクレームを例に特許拒絶理由の主要なものについて解説する。審査は、異議申立て後に行われた 1997 年 1 月の特許請求範囲の補正を、『特許請求の範囲を拡大し、又は変更するものではない』との判断から有効としたうえで、これを対象に行われている。特許異議の決定の続葉に記述されている理由によれば、審議は異議申立人の提出した証拠[58]に記載された内容を分析し、これをクレームと比較することによって行われている。

まず、クレーム 1（1997 年 1 月 31 日補正後）の記載は次のとおりである。

クレーム 1（1997 年 1 月 31 日補正後）:

「①発行銀行に備えられたオンライン会計システムと、

②通貨の電子的象徴を発生し、発生した該通貨電子的象徴の額だけ前記発行銀行の前

---

[58] 提出された証拠は以下の 13。

甲第 1 号証　IC カード実用化研究会報告書、IC カード実用化研究会事務局、昭和 63 年 12 月発行

甲第 2 号証　特開平 2-1049 号公報

甲第 3 号証　特開昭 61-94177 号公報

甲第 4 号証　特開平 3-73065 号公報

甲第 5 号証　岡本龍明、太田和夫、「理想的電子現金方法」電子情報通信学会技術研究報告、Vol.91 No.127、第 39 頁から 47 頁、1991 年 7 月 15 日発行

甲第 6 号証　藤井友位、金融ネットワークマニュアル、（株）企画センター、昭和 63 年 8 月 10 日発行

甲第 7 号証　特開昭 60-198683 号公報

甲第 8 号証　D.Davies、W.L. Price、上園忠広訳、ネットワークセキュリティ、日経マグロウヒル社、昭和 60 年 12 月 5 日発行

甲第 9 号証　木下宏揚、辻井重男「プライバシー保護を考慮した電子資金移動方式の提案」電子情報通信学会論文誌 D、Vol.J70-D No.12、第 2713 頁から 2721 頁

甲第 10 号証　太田和夫「ZKIP と電子現金プロトコル」電子情報通信学会技術研究報告、Vol.89 No.483、第 57 頁から 68 頁、1990 年 3 月 28 日発行

甲第 11 号証　経済企画庁国民生活局編、カード社会の指針、平成 2 年 10 月 1 日発行

甲第 12 号証　日本電気情報処理教育部編、新版オペレーティング・システム入門、日本能率協会マネジメントセンター、1998 年 1 月 18 日発行

甲第 13 号証　IC カードのアプリケーション展望、（株）矢野経済研究所、1991 年 5 月 28 日発行

記会計システムにおける金銭発行流動負債勘定として前記オンライン会計システムにおいて貸し越されるようにするために前記発行銀行に関連装備された金銭発生モジュールと、
③前記通貨の電子的象徴をストアするとともに、前記通貨の電子的象徴を含む銀行取引を中継することができるように前記発行銀行に関連装備された出納モジュールと、
④前記通貨の電子的象徴をストアし、前記発行銀行に備えられた前記出納モジュールとオンライン取引を行い、さらに、前記通貨の電子的象徴をオフライン取引において他の取引モジュールとの間で交換することができる取引モジュールとを備え、
⑤前記通貨の電子的象徴の各々が前記金銭発生モジュールにより生成された初期の貨幣的価値と移転した貨幣的価値と該通貨の電子的象徴を受け取った取引モジュールを表示するためのモジュール認識票を含むものであり、
⑥前記出納モジュール及び取引モジュールはそれらのモジュールが前記通貨の電子的象徴の１つを振込先モジュールに移転する振出元モジュールとして機能するときにおいて、移転された貨幣的価値と振込先モジュール認識票とを有する移転レコードを発生し、
⑦かつ前記移転された通貨の電子的象徴において前記移転レコード及び前記初期の貨幣的価値を含むことができるプロセッサを有するものであること
を特徴とする電子通貨システム。」

このクレームについて、異議申立人の提出した証拠のうち、「理想的電子現金方法」を引用して判断している。

審査官は、「理想的電子現金方法には」、

『利用者は、銀行等からの電子現金の使用許可を発行してもらい、必要なときに、口座からの引き落とし処理等の何らかの会計処理を前提として、電子現金（電子紙幣）の支払いを受け、IC カード上に電子現金情報を格納する。カード上の電子現金は、譲渡、分割譲渡が可能で、譲渡処理がオフラインでできる。電子現金のデータに織り込まれる情報には、銀行から発行された電子現金の額面金額、銀行から発行された利用許可証、利用者識別情報、譲渡された金額に関する情報が含まれ、譲渡時に譲渡額や譲受人の利用者識別情報等に関する情報が電子現金データに付加される。電子現金のやり取りは、暗号化技術、電子署名技術、認証技術により、そのセキュリティが確保されている。電子現金は、利用者が発行銀行に支払い、必要な会計処理を行うことによって決済される。使用された電子現金のデータに基づいて不正使用を検出する機能を有しており、銀行等において不正使用者を特定することができる。』

ということが記載されていると判断している。これとクレーム１を対比した結果、『「理想的電子現金方法」においても、会計システム、電子現金の発行手段、電子現金情報を IC

カードとやりとりする手段が示唆されている』と考えられ、また、『発明の詳細な説明を参酌すれば、――「IC カード」は請求項における「取引モジュール」に相当する』ほか、『「電子現金（電子貨幣）」は請求項における「通貨の電子的象徴」に、譲渡時に発生される他の情報は請求項における「移転レコード」に、それぞれ相当するものといえる』ことから、クレーム１に係る発明と「理想的電子現金方法」に記載された発明は、

『発行銀行に備えられた会計システムと、通貨の電子的象徴を発生する手段（モジュール）と、通貨の電子的象徴を含む銀行取引を中継するために発行銀行に装備された出納モジュールと、これとオンライン取引を行い、通貨の電子的象徴を他の取引モジュールとの間で交換することができる取引モジュールとを備え、通貨の電子的象徴の各々が金銭発生手段により生成された初期の貨幣的価値と移転した貨幣的価値と振込先識別情報とを有する移転レコードを発生し、かつ移転された通貨の電子的象徴において移転レコード及び初期の貨幣的価値を含むことができるプロセッサを有するものであることを特徴とする電子通貨システム。』

である点で共通し、

『①請求項に係る発明においては、発生した通貨の電子的象徴の額だけ発行銀行の会計システムにおける金銭発生流動負債勘定として貸し越されるように規定しているのに対し、甲第 5 号証のものは、電子的象徴の発行に伴う会計上の取り扱いや処理について具体的に開示していない点、及び、
②請求項に係る発明においては、振込先識別情報として、モジュール認識票を用いているのに対し、甲第 5 号証のものでは、個人識別情報を用いている点、』

で相違すると結論づけている。

しかしながら、相違するとされる部分についても、①については『通貨の電子的象徴を発行する際に、会計上どのような勘定項目としてどのように処理するかは、電子的象徴に与える性格（例えば現金的性格、小切手的性格、手形的性格、クレジット的性格）や、商業上の慣行、商法上の規定などを考慮して、設定されるべきものであるから、金銭発生手段を、会計上所望の形式の取り扱いができるものとすることは、当業者が普通に配慮すべき設計的事項といえる。』ほか、②についても、『通貨の電子的象徴を移転する際に、その発生源として転送先を特定するための情報として利用可能なのは、通常、利用者に関する情報か、取引モジュールに関する情報のいずれかであり、これをどちらにするかは、電子的象徴に伴う取引履歴情報としてどちらを重視するかによるものであって、技術的な考察を要する問題ではない。』として、特許として認められないとの判断を行っている。

クレーム 1 に従属するクレーム 2 からクレーム 11 についても、各々個別の理由が述べられており、すべて拒絶されている。

クレーム 2：
「前記取引モジュール及び前記出納モジュールの各々がその中にストアされた前記通貨の電子的象徴の各々における現在の貨幣的価値を追跡記録した手形ディレクトリを有することを特徴とする請求項 1 記載の電子通貨システム」

クレーム 3：
「①前記振込先モジュールの前記手形ディレクトリに記載され、
②かつその中にストアされた通貨の電子的象徴の１つに関連付けられた前記通貨の貨幣的価値が、前記振込先モジュールに前記通貨の電子的象徴が移転されたときにおける前記移転された貨幣的価値により減額されるものであること
を特徴とする請求項 2 記載の電子通貨システム。」

例えば、クレーム 2 は取引モジュールおよび出納モジュールが手形ディレクトリ（手形の履歴情報）を有することを記載するものであるが、「理想的電子現金方法」においても、『電子現金は分割移転の履歴情報を保有しており、取引のためにこの情報の処理が必要とされるのであるから、当該現金がストアされるモジュールはこの情報を有することになるはずである』としているほか、クレーム 3 は、取引モジュール間で通貨の電子的象徴が移転されたときの電子的価値の決定について規定するものであるが、これについても『貨幣的価値の移転に伴う当然の手続を規定したことにすぎない』としている。

クレーム 4：
「前記通貨の電子的象徴が前記金銭発生モジュールにより生成されたそのモジュールのディジタル署名及び前記振出元モジュールによって生成された振出元ディジタル署名を含むことを特徴とする請求項 1 記載の電子通貨システム」

また、クレーム 4，5，6，10 は、ディジタル署名やこれに対する証明手段、さらには暗号保障セッションを介した通信について記載しているが、これらは「理想的電子現金方法」、甲第 3 号証、甲第 1 号証のものにおいても前提とされている事項であることを指摘するとともに、『ディジタル署名や証明手段などは、既に技術標準とされているものであり、周知のものである（CCITT BLUE BOOK 分冊Ⅷ-6，8，勧告 X.509 及びその付録 A から H（1988 年））』として新たな証拠を提示してこれを拒絶している。

クレーム 7:
「前記移転レコードがさらに、移転日を含むことを特徴とする請求項 1 記載の電子通貨システム」

クレーム 8：
「前記通貨の電子的象徴が、振出元モジュールの認識票及び振込先モジュールの認識票を含むことを特徴とする請求項 1 記載の電子通貨システム」

クレーム 9：
「前記振込先モジュールは、前記移転された通貨の電子的象徴に収められた最新の前記振出元モジュールの認識票が振出元モジュールのモジュール認識票と同一であることを特徴とする請求項 8 記載の電子通貨システム」

クレーム 11：
「前記モジュールの各々が電子処理装置のモジュール共同プロセッサとして動作するように構成されたことを特徴とする請求項 10 記載の電子通貨システム」

審査官は、クレーム 7, 8, 9 についても、「理想的電子現金方法」との相違部分については自明であるとしているほか、クレーム 11 についても、共同プロセッサについて言及しているが、『「共同プロセッサ」そのものについては発明の詳細な説明にも記載がなく、どのようなものか不明であるが、仮に co-processor（協調プロセッサー）を意味するのであれば、関連する複数の処理を行う場合に普通に知られたコンピュータ構成法にすぎない』としている。実施例によれば、「各モジュールは個々に具体化されるのが望ましいが、プロセッサによって制御される単一の装置において具体化されてもよい」といった記載が各所に見られており、これがクレームにかかれている「共同プロセッサ」を開示した部分であると考えられる。

さらに、拒絶の理由の特徴的なものとして、クレーム 23、39 を取上げる。

クレーム 23：
「①発行銀行に備えられたオンライン会計システムと、
②前記加入者の貸付勘定に依存する電子的信用認可を発生し、発生した該電子的信用認可に関連する額だけ前記オンライン会計システムにおける加入者の貸付口座に記入を行って、その利用可能な信用供与限度を減少させるために前記発行銀行に関連装備された金銭発生モジュールと、
③前記電子的信用認可をストアするとともに、前記電子的信用認可を含む銀行取引を中継することができるように前記発行銀行に関連装備された出納モジュールと、
④前記電子的信用認可をストアし、前記発行銀行の前記出納モジュールとオンライン取引を行い、さらに、前記電子的信用認可をオフライン取引において他の取引モジュールとの間で交換することができる取引モジュールとを備え、
⑤前記電子的信用認可が、前記加入者の貸付勘定の口座番号、前記金銭発生モジュールにより生成された初期の貨幣的価値及びディジタル署名を含み、前記初期の貨幣

的価値より少ないか，又はそれに等しい価値の範囲で前記取引モジュール間で移転可能であり、
⑥前記電子的信用認可が振り込まれたとき、前記発行銀行は前記加入者の貸付勘定に移転された前記貨幣的価値についての借方記入を行うものであること
を特徴とする電子通貨システム。」

クレーム 23 に記載された内容は、クレーム 1 において、モジュール認識票を含む移転レコードに関する記述を削除し、通貨の電子的象徴を電子的信用認可に置換え、会計処理もそれに合うものに置換え、電子的象徴の内容に代えて電子的信用認可の内容を記載したものに相当するが、審査官は『電子的象徴を、現金と呼ぶか信用と呼ぶかは、これらの電子的象徴の経済的又は法的根拠を現実の貨幣に置くか信用に置くかによる相違にすぎず、技術的な問題ではない』等として拒絶している。実際には、電子的象徴を信用と呼べるものに変えるためには、経済的又は法的根拠に従って、処理内容、処理手順に関するソフトウェア等の技術的変更が必要であり、この技術的変更の容易性の観点からの審査官の判断がこのような表現になったものと考えられる。

クレーム 39：
「①発行銀行に備えられたオンライン会計システム及びコンピュータにより実行される取引調整システムと、
②前記オンライン会計システムにおいて勘定される通貨の電子的象徴を発生するために前記発行銀行に関連付けられた金銭発生モジュールと、
③前記通貨の電子的象徴をストアできるように前記発行銀行に関連付けられた出納モジュールとを備え、
④前記金銭発生モジュール、前記出納モジュール、及び前記オンライン会計システムからの取引レコードが前記取引調整システムに周期的に送られるようにし、
⑤前記取引調整システムが前記取引レコードを分析して出納モジュールの取引が妥当な会計取引と符合し、かつ金銭発生モジュールの取引が妥当な出納モジュールの取引及び会計取引と符合していることを確認するためのプロセッサを有し、さらに、
⑥何らかの不一致があったときは不完全処理又は安全破壊であることを表示できるようにしたこと
を特徴とする電子通貨システム。」

クレーム 39 では、電子的象徴の内容や取引モジュールについては何ら記述がなく、ただ、発行銀行に取引調整システムが備えられており、銀行の各モジュールと会計システムから定期的に送られる取引レコードを分析、符合させて、不一致の場合にこれがわかるように表示する機能を持つことを記載している。審査官は『しかしながら、各取引ポイントで取引レコードや会計レコードを定期的に収集して分析、符合して、チェックすることは、金融業界において普通に行われている手続である。また、履歴データを定期的に収集して分

析する、いわゆるデータ収集技術そのものは、文献を引用する必要がないほど知られているものである。そうすると、請求項 39 に規定された上記の事項は、電子的象徴の取引を実際に運用するうえで銀行側において普通に必要とされる機能を表明したというにすぎない』として拒絶している。

以降のクレームについても同様に、証拠の資料にある記載内容とクレームとの対比が行われ、相違が認められるとした部分について、特許としての要件を備えているかどうかの判断が行われている。しかしながら、相違が認められる部分はいずれのクレームについてもわずかであり、それについても『当然の手続を規定したにすぎない』、『当業者が容易になしうる設計変更』、『常識的事項を明示したというにすぎない』、『自明の事項を表明したにすぎない』、『処理上当然に必要となる情報を明示したというにすぎない』、等の理由から特許を受けることができないとして、全てのクレームについて拒絶の判断を行っている。

Ⅴ．終わりに

本稿では、電子マネー・スキーム技術を、その技術的発想の起源、研究･開発の系譜等をもとに概説し、それぞれの系譜に属する主要な特許を取上げ、実際にどのようなクレームが出願／登録されているのかについて分析を試みた。電子マネーの特許といっても、その技術的発想の起源や技術的な切り口などによってクレームの記載の仕方は大きく異なり、また、保護しようとする対象、保護の範囲も異なる。中には、技術的発明というよりは、ビジネスの方法を定めたものに近い性格のものもあり、そうしたものがどこまで特許として認められるかについては、幾つもの事例の積み重ねが必要であろう。

電子マネーを業として運営あるいは利用しようという場合、その電子マネーに関連する特許が存在するのかどうか、存在するとすればその特許の効力はどこまでおよぶのか、そして提供しようとする電子マネーがその特許の効力の範囲に含まれていないかどうかについて、事前に調査・分析を行うことは重要なことである。そうした場合に、本稿で検討したような特許の分析が有用であろう。

今後、オープンなネットワーク上における電子商取引を支える決済インフラ技術として、電子マネーへの要請が一層高まることが予想される。こうした中、特許が成立している電子マネーの使用に関して法律的な問題が生じる可能性も着実に高まってくると予想される。こうした観点から、今後も電子マネーの研究開発に関する動向に加えて、その特許の出願･登録状況あるいは特許制度等の動向にも注視していく必要があるといえよう。

以　　上

【参考文献】

相澤英孝・宇根正志・楠田浩二、「暗号と特許」、『ディスカッションペーパーシリーズ』、98- J-8、日本銀行金融研究所、1998 年

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

斎藤治・森田泰子・加藤壮太郎、「金融業務における特許権の成否」、『金融研究』、第 14 巻第 2 号、日本銀行金融研究所、1995 年

中山靖司、「実現せまる電子マネーの現状」、『Dr. Dobb's JOURNAL JAPAN』、1998 年 2 月号、pp.70-81、翔泳社、1998 年

――――、「電子決済について」、『ITU ジャーナル』、Vol26、No.7、pp.54-62、新日本 ITU 協会、1996 年

――――・太田和夫・松本勉、「電子マネーを構成する情報セキュリティ技術と安全性評価」、『ディスカッションペーパーシリーズ』、98-J-26、日本銀行金融研究所、1998 年

――――・森畠秀実・阿部正幸・藤崎英一郎、「電子現金の一実現方式について」、『金融研究』、第 15 巻第 2 号、日本銀行金融研究所、1997 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

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-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-CRYPTO '88, LNCS, No.403, Springer-Verlag, pp.328-335, 1989.

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

Even, S., Goldreich, O., Yacobi, Y. "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.

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 Ohta, K. "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," 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.