

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4309479号  
(P4309479)

(45) 発行日 平成21年8月5日(2009.8.5)

(24) 登録日 平成21年5月15日(2009.5.15)

(51) Int.Cl. F I  
G O 6 Q 40/00 (2006.01) G O 6 F 17/60 2 4 4  
G O 7 F 7/10 (2006.01) G O 7 F 7/10

請求項の数 8 (全 14 頁)

(21) 出願番号 特願平11-507300  
(86) (22) 出願日 平成10年7月2日(1998.7.2)  
(65) 公表番号 特表2001-505339(P2001-505339A)  
(43) 公表日 平成13年4月17日(2001.4.17)  
(86) 国際出願番号 PCT/US1998/013581  
(87) 国際公開番号 WO1999/001823  
(87) 国際公開日 平成11年1月14日(1999.1.14)  
審査請求日 平成11年12月30日(1999.12.30)  
審判番号 不服2005-8633(P2005-8633/J1)  
審判請求日 平成17年3月14日(2005.3.14)  
(31) 優先権主張番号 60/051,668  
(32) 優先日 平成9年7月3日(1997.7.3)  
(33) 優先権主張国 米国(US)

(73) 特許権者  
シティコープ デベロップメント セン  
ター  
アメリカ合衆国 カリフォルニア州900  
66、ロスアンジェルス、ダヴリュー、ジ  
ェファークソン ブルバード 12731  
(74) 代理人  
弁理士 岡本 寛之  
(74) 代理人  
弁理士 小柴 雅昭  
(72) 発明者  
ホロヴィッツ、エドワード  
アメリカ合衆国 ニューヨーク州1002  
5、ニューヨーク、ウェスト エンド ア  
ヴェニュー 670、アパートメント 1  
6D

最終頁に続く

(54) 【発明の名称】 取引カードの磁気ストライプへ値を送るシステム

(57) 【特許請求の範囲】

【請求項 1】

先進技術のメモリと磁気ストライプのメモリとを有する取引カードにおける磁気ストライプのメモリを利用して金融取引を行なうシステムであって、  
先進技術のメモリと磁気ストライプのメモリとを備える取引カードであって、  
前記先進技術のメモリが、集積回路のメモリ、オプティカルメモリ、および薄膜半導体のメモリの少なくとも1つからなり、かつ、電子パースバリュを有する電子パースを備えており、  
前記磁気ストライプのメモリが、個人の口座番号を記録するための非任意データフィールドと、任意データフィールドとを有し、これらの一方または両方に、口座番号、暗証番号  
および前記電子パースバリュの少なくとも一部の金銭的値を含む暗号化された専用取引  
番号を記録可能なもの、と、  
前記取引カードの前記先進技術のメモリと通信可能で、この先進技術のメモリに対する読取りおよび書込みを行う第1読取り/書込み手段、前記取引カードの前記磁気ストライプのメモリと通信可能で、この磁気ストライプのメモリに対する読取りおよび書込みを行う第2読取り/書込み手段、ならびに前記先進技術のメモリの電子パースの電子パースバリュの少なくとも一部分の金銭的値を前記磁気ストライプのメモリに転送するアプリケーションを実行可能な処理装置を有し、前記処理装置が、前記アプリケーションを実行することによって、暗証番号および転送すべき金銭的値を含む取引データの指定を受け付ける取引指定受付手段、前記取引指定受付手段によって受け付けられた取引データを前記口座

10

20

番号とともにエンコードして前記専用取引番号に変換する手段、この変換された専用取引番号を前記第 2 読取り / 書込み手段によって前記取引カードの前記磁気ストライプのメモリに記録させる手段、ならびに前記先進技術のメモリの電子パースの電子パースバリューを、前記第 1 読取り / 書込み手段によって、前記磁気ストライプのメモリに転送した金銭的値の分だけ減少させる手段として機能する、読取り / 書込み装置と

を備え、

前記専用取引番号が、前記読取り / 書込み装置と通信関係にある金融機関のホストシステムにおいて、デコードされ、当該専用取引番号に含まれる口座番号に対応する口座の情報と照合確認されるものであることを特徴とする、システム。

【請求項 2】

前記読取り / 書込み装置が、携帯情報端末、現金自動振込支払機、顧客アクセス端末、および商人側端末の少なくとも 1 つを含むことを特徴とする、請求項 1 に記載のシステム。

【請求項 3】

前記先進技術のメモリはコンピュータ機能を有し、前記専用取引番号を暗号化するものであることを特徴とする、請求項 1 に記載のシステム。

【請求項 4】

前記読取り / 書込み装置は、前記専用取引番号を暗号化するものであることを特徴とする、請求項 1 に記載のシステム。

【請求項 5】

前記磁気ストライプのメモリの前記任意のデータフィールドまたは非任意データフィールドに、前記ホストシステムにおいて前記専用取引番号を一般の口座番号から区別するための標識文字が記録されていることを特徴とする、請求項 1 に記載のシステム。

【請求項 6】

磁気ストライプのメモリを使用する取引カードの先進技術のメモリに保存した値を使用するためのシステムであって、

先進技術のメモリと磁気ストライプのメモリとを有する前記取引カードであって、

前記先進技術のメモリが、電子パースバリューを有する電子パースを備えた集積回路のメモリからなり、

前記磁気ストライプのメモリが、個人の口座番号を記録するための非任意データフィールドと、任意データフィールドとを有し、これらの一方または両方に、口座番号および前記電子パースバリューの少なくとも一部分の金銭的値を含む専用取引番号を記録可能なもの、と、

前記取引カードの前記専用取引番号で表される前記電子パースバリューの前記一部分の金銭的値に相当する量を取り出し可能とする端末装置と、

前記取引カードの前記先進技術のメモリと通信可能で、この先進技術のメモリに対する読取りおよび書込みを行う第 1 読取り / 書込み手段、前記取引カードの前記磁気ストライプのメモリと通信可能で、この磁気ストライプのメモリに対する読取りおよび書込みを行う第 2 読取り / 書込み手段、ならびに前記先進技術のメモリの電子パースの電子パースバリューの少なくとも一部分の金銭的値を前記磁気ストライプのメモリに転送するアプリケーションを実行可能な処理装置を有し、前記処理装置が、前記アプリケーションを実行することによって、転送すべき金銭的値を含む取引データの指定を受け付ける取引指定受付手段、前記取引指定受付手段によって受け付けられた取引データを前記口座番号とともにエンコードして前記専用取引番号に変換する手段、この変換された専用取引番号を前記第 2 読取り / 書込み手段によって前記取引カードの前記磁気ストライプのメモリに記録させる手段、および前記先進技術のメモリの電子パースの電子パースバリューを、前記第 1 読取り / 書込み手段によって、前記磁気ストライプのメモリに転送した金銭的値の分だけ減少させる手段として機能する、読取り / 書込み装置と

を備え、

前記専用取引番号が、前記読取り / 書込み装置および前記端末装置と通信関係にある金融機関のホストシステムにおいて、デコードされ、当該専用取引番号に含まれる口座番号に

10

20

30

40

50

対応する口座の情報と照合確認されるものであり、  
前記端末装置が、前記取引カードの磁気ストライプのメモリから前記専用取引番号を読み取り、取引額の入力を受け付け、前記専用取引番号および取引額を含む取引ファイルを前記金融機関のホストシステムに送り、当該ホストシステムによって取引が許可された場合に、当該取引額の現金を出すものである  
ことを特徴とする、システム。

【請求項 7】

前記読取り / 書込み装置と前記端末装置とが同じ装置であることを特徴とする、請求項 6 に記載のシステム。

【請求項 8】

取引カードに備えられた先進技術のメモリの電子パースバリューの少なくとも一部分の金銭的値を、取引カードに備えられた磁気ストライプのメモリへ送るシステムであって、  
前記先進技術のメモリが、集積回路のメモリ、オプティカルメモリ、および薄膜半導体のメモリの少なくとも 1 つからなり、かつ、前記電子パースバリューを有する電子パースを備えており、  
前記磁気ストライプのメモリには、口座番号および取引の金銭的値を含む専用取引番号が記録できるようにされており、  
前記システムは、

前記先進技術のメモリと通信可能で、この先進技術のメモリに対する読取りおよび書込みを行う第 1 読取り / 書込み手段、前記磁気ストライプのメモリと通信可能で、この磁気ストライプのメモリに対する読取りおよび書込みを行う第 2 読取り / 書込み手段、ならびに前記先進技術のメモリの電子パースの電子パースバリューの少なくとも一部分の金銭的値を前記磁気ストライプのメモリに転送するアプリケーションを実行可能な処理装置を有し、前記処理装置が、前記アプリケーションを実行することによって、転送すべき金銭的値を含む取引データの指定を受け付ける取引指定受付手段、前記取引指定受付手段によって受け付けられた取引データを前記先進技術のメモリの取引カードの口座番号とともにエンコードして前記専用取引番号に変換する手段、この変換された専用取引番号を前記第 2 読取り / 書込み手段によって前記磁気ストライプのメモリに記録させる手段、および前記先進技術のメモリの電子パースの電子パースバリューを、前記第 1 読取り / 書込み手段によって、前記磁気ストライプのメモリに転送した金銭的値の分だけ減少させる手段として機能する、読取り / 書込み装置  
を備え、

前記専用取引番号が、前記読取り / 書込み装置と通信関係にある金融機関のホストシステムにおいて、デコードされ、当該専用取引番号に含まれる口座番号に対応する口座の情報と照合確認されるものであることを特徴とする、システム。

【発明の詳細な説明】

【0001】

【関連出願の相互参照】

本出願は、1997 年 7 月 3 日提出の米国仮出願第 60 / 051,668 号の利益を請求するものである。

【0002】

【発明の分野】

本発明は、金融取引に用いる取引カードに関する。特に、取引カードの値を該カードにおける先進技術のメモリーから該カードにおける磁気ストライプのメモリーへ転送するシステムに関する。

【0003】

【背景技術】

クレジットカードや、デビットカードや、ストアバリューカード等の磁気ストライプのメモリを有する各取引カードの広大な使用によって、より先進で強力なカードの発展が阻害されているとの指摘がある。最近の技術の進歩に伴い、スマートカードと呼ばれる集積回

10

20

30

40

50

路のメモリや、オプチカルメモリや、薄膜半導体メモリを有する取引カードが、消費者に優れた機能性および安全性を与えるようになってきている。しかし、磁気ストライプカードとしか相互作用しないデバイスにインストールされた大量のベースが、最新技術の取引カードの商用的成功の大きな障害になっている。そこで、磁気ストライプカード専用のデバイスにインストールされたベースと相互作用可能で、且つ最新技術のメモリの先進の機能性と安全性を提供する取引カードを1つにするシステムが望まれている。

#### 【0004】

磁気ストライプカードの利用法は共通であるが、その有用性は、各カードの比較的限られた記憶容量により限られる。一般的なカードの磁気ストライプは、データを保存しアクセスする3つのトラックを備えている。なお、これらトラックに保存するデータのロケーションおよび種類の判定基準は、国際標準化機構（ISO）による基準で認定される。一般に、このトラックのある特定部分には所定の産業情報を保存しなければならないが、他の部分はオープンデータフィールドを有することができる。カード保有者の氏名や、口座番号や発行銀行のルーティングナンバー等の基準情報は、トラックに保存しなければならない。

10

#### 【0005】

例えば、現金自動振込支払機（ATM）の取引に磁気ストライプカードを通すと、オンラインATMは、そのカードの口座番号情報を読み取り、利用者に暗証番号（PIN）を入力して身分を証明するよう促す。また、ATMは、利用者取引を確認させて当座預金からの引き出しを行なう等の取引を決定するように促す。この場合、一般的には、ATMは、オンラインシステムにおけるしかるべき口座番号にアクセスし、入力されたPINがオンラインに保存された口座のPINと合うかどうかチェックする。さらに、口座残高をチェックして、その取引が口座残高を越えていないかどうかを確認する。PINが合致し、且つ口座残高が充分である場合、ATMは、その取引の手続きを許可し、オンラインによる課金情報の調整を行なう。なお、以上は、ATMによる取引手続きのし方の一例であり、他の手続きや上記手続きの変更手続きをとることもある。このように、取引カードのATMでの使用によって、ATMにより現金として支払われる資金の入手に利用可能なオンライン口座にアクセスすることができる。

20

#### 【0006】

磁気ストライプカードが顧客の氏名および口座番号で初期化された後は、それ以降のデータは、カードの磁気ストライプ上には記録しないのが一般的である。ストライプに含ませた情報は、単に識別を目的とした読取りを行ってオンラインシステムにアクセスできるようにしているだけに過ぎず、従って、磁気ストライプカードは、オンラインシステムを介してのみ利用可能な口座へアクセスするのに使用されるのに限られている。

30

#### 【0007】

これに対して、先進技術のメモリを有するカードは非常に機能的であり、データをメモリから読取りすることもメモリに書込みすることも可能である。適合する先進技術のメモリとしては、スマートカードとしても知られている集積回路（IC）のメモリが挙げられる。スマートカードは、大きさおよび外見は磁気カードに似ているが、背面側に磁気ストライプを設ける代りに、カード内にマイクロコンピュータチップを埋め込んだものである。先進技術の集積回路のチップは、スマートカードに約16キロバイトのE スクエアドメモリを保存する能力を与えている。先進技術のメモリにはコンピュータ機能があるため、データ処理プログラムを保存し且つ動かす能力がある。スマートカードのような先進技術のメモリの利点上の特徴の一つは、データを符号化してそのデータのセキュリティを保証できるようにする暗号化技術を提供できる能力である。従って、先進技術のメモリは、磁気ストライプのメモリには無い機能および安全面での利点がある。

40

#### 【0008】

しかし、上記したように、この先進技術のメモリをうまく利用できていない消費者が多くいる。その理由は、消費者のエリア内の企業が取引カードの先進技術のメモリへの読取りおよび書込みのできる装置を提供できていないからであるかもしれない。このような状況

50

では、消費者は、自己のエリア内での使用に限られるため、先進の機能性と安全性を備えた取引カードを得ようとしたがらないと思われる。しかし、地元の企業が先進技術のメモリを有するカードの使える装置を提供できないかもしれない場合でも、依然として消費者は、ネットワーク化したコンピュータ上での使用のような個人的使用を目的としたカードを望んでいると思われる。例えば、消費者は、スマートカードメモリを有する取引カードを、スマートカードの読取り/書込み装置や、インターネット上の商人と通信関係にあるパーソナルコンピュータや携帯情報端末と共に使用することができる。スマートカードにより消費者はインターネットを介して安全な電子取引を行なうことができる。同様に、消費者は、そのようなセットアップを利用して自己の銀行と通信し、金をスマートカード内の電子パース（財布）内に送ることができる。このように、たとえ地元の企業が先進技術のカードの使用を受け付けなくても、消費者は他の理由でも先進技術のカードの利用を望んでいると思われる。

10

#### 【 0 0 0 9 】

さらには、ビジネスの国際化に伴い、世界の遠隔地における多くの地域社会がクレジットカードや、デビットカードやスマートカードのような最新の金融関係デバイスの対象となるが、地域社会には技術の新たな進歩の全てを直ちにサポートできるインフラストラクチャーを持たないため、地域社会がそれらデバイスをうまく利用できていないように思われる。このような問題はあるが、それらの地域に予備知識を与えて、外部の企業がそれらの地域社会と効果的に取引が行なえるようにすることが望ましい。さらには、そのような地域社会の消費者は、最新のデバイスを利用した取引を行なうのを望んでいるため、現行のシステムと相互作用可能な先進技術のメモリを有する単一のカードが望まれている。

20

#### 【 0 0 1 0 】

従って、これらの問題を解決して、消費者が、先進技術のメモリを有する取引カードを利用でき且つカードの磁気ストライプを読取るだけのデバイスにインストールされた現行のベースの範囲内で先進技術のメモリの機能性と安全性の特徴を利用できるようにすることが望まれている。

#### 【 0 0 1 1 】

##### 【本発明の開示】

本発明は、集積回路（IC）や、チップメモリ、すなわち“スマートカード”や、オプティカルストライプのメモリや、薄膜の半導体メモリ、等の先進技術の記憶能力を有する取引カードの、磁気ストライプカードを排他的に処理する既成のネットワーク内での利用にてこ入れすることに関する。ネットワークとしては、自動現金振込支払機（ATM's）、顧客アクセス端末（CAT's）、インターネット、商人側端末、および、その関連する資金移動通信ネットワークであって、取引カードの保有者が世界中の様々なところで現金を得たり金銭値を送れたりできるネットワークが挙げられる。また、本発明は、磁気ストライプのメモリを先進技術のメモリの一つまたはその組合せと組合せてそれらメモリを協働的に相互作用させる、カードを提供するものである。その相互作用によって先進技術のメモリの能力の少なくとも一部が磁気ストライプのメモリを介して利用することができる。特に、本発明は、取引カードにおける値を、集積回路のメモリ等の先進技術のメモリの範囲内で、電子パースから磁気ストライプに安全に送るシステムを提供するものである。このように、本発明は、磁気ストライプのメモリカードを排他的に処理する装置の現行のネットワークで、取引カードの先進技術のメモリの能力を利用できるようにするシステムを提供するものである。

30

40

#### 【 0 0 1 2 】

実施例は、磁気ストライプのメモリと、少なくとも1つの先進技術のメモリとを有する取引カードにおける前記磁気ストライプのメモリを利用して安全な金融取引を行なう方法であって以下の各ステップ：すなわち、専用取引番号を形成して資金の移動を行なうのに必要なデータを修正するステップ；および、その専用取引番号を前記カードの磁気ストライプのメモリに保存するステップ、とからなる方法を提供するものである。前記専用取引番号は、前記カードにおける前記少なくとも1つの先進技術のメモリ内に記憶された値の

50

少なくとも一部分にアクセスできるようにしている。また、前記先進技術のメモリは、集積回路メモリ、オプティカルストライプのメモリ、および薄膜の半導体メモリの少なくとも1つを含む。また、前記修正するステップは、前記カードの前記少なくとも1つの先進技術のメモリの暗号化能力で前記専用取引番号を発生させることを含むことが好ましいが、前記専用取引番号は、先進技術のメモリおよび磁気ストライプのメモリに対して読取りおよび書込みが可能で、前記カードと通信関係にある装置により暗号化するようにしてもよい。前記読取りおよび書込み可能な装置は、携帯情報端末、現金自動振込支払機、顧客アクセス端末、および商人側端末からなる群から選択される装置からなる。さらに、前記データを修正するステップは、公開キー/秘密キーによる暗号化システムおよび/または同期クロックによる暗号化システムを用いてデータを暗号化するステップを含む。

10

#### 【0013】

また、前記保存するステップは、前記磁気ストライプのメモリの前記専用取引番号を、任意データフィールド、非任意データフィールドおよび/またはその両方の組合せ、に記録するステップで構成することができる。また、前記保存するステップが非任意データフィールドに記録するステップからなる場合、前記専用取引番号は、個人の口座番号の少なくとも一部分に代えて、記録するステップから構成することもできる。さらに、実施例は、前記磁気ストライプのメモリの標識文字を記録して、前記磁気ストライプを読取るシステムに前記専用取引番号が標準的な口座番号でないことを表示するようにするようにしてもよい。前記標識文字は、任意データフィールドまたは非任意データフィールドに記録するようにできる。

20

#### 【0014】

さらに、本発明は、マルチ-メモリ取引カードの値を先進技術のメモリから磁気ストライプのメモリへ送るシステムを開示するものである。このシステムは、先進技術のメモリと磁気ストライプのメモリとを有する取引カードを備えてなり、前記先進技術メモリは、電子パースバリューを有する電子パースを備えている。また、前記磁気ストライプのメモリは、個人の口座番号を記録するための非任意データフィールドを備えてなり、前記磁気ストライプのメモリは、任意データフィールドを有している。さらに、このシステムは、前記先進技術のメモリおよび前記磁気ストライプのメモリと通信関係にある読取り/書込み装置を備えている。そして、前記磁気ストライプのメモリに暗号化済みの専用取引番号を記録し、また、その専用取引番号は、前記電子パースバリューの少なくとも一部分の転送を行なう。

30

#### 【0015】

前記先進技術のメモリは、集積回路メモリ、オプティカルメモリ、および薄膜の半導体メモリの少なくとも1つを含む。前記読取りおよび書込み可能な装置は、携帯情報端末、現金自動振込支払機、顧客アクセス端末、および商人側端末の少なくとも1つを含む。前記専用取引番号は、取引価値とも呼ばれる金銭的値と、暗証番号とを含む。また、前記専用取引番号は、前記先進技術のメモリおよび/または前記読取り/書込み装置によって暗号化される。さらに、このシステムは、前記磁気ストライプのメモリの前記任意データフィールドまたは非任意データフィールドに記録された標識文字を含んでいてもよい。

#### 【0016】

40

別の実施例では、磁気ストライプのメモリを表面に使用するマルチ-メモリ取引カードの先進技術のメモリに保存した値を使用するためのシステムであって、このシステムは、先進技術のメモリと磁気ストライプのメモリとを有する取引カードを備えてなる。前記先進技術メモリは、電子パースバリューを有する電子パースを備えた集積回路のメモリからなり、前記磁気ストライプのメモリは、個人の口座番号を記録するための非任意データフィールドと、任意データフィールドとを有している。さらに、このシステムは、前記磁気ストライプのメモリに記録される専用取引番号を有し、該専用取引番号は、前記電子パースバリューの少なくとも一部分を表わす。また、このシステムは、前記先進技術のメモリおよび前記磁気ストライプのメモリと通信関係にある読取り/書込み装置を有していて、この読取り/書込み装置は、前記専用取引番号を発生させる。そして、このシステムは、前

50

記専用取引番号で表わされる前記電子パスバリューの前記部分に相当する量のクレジットを取り出せる端末装置を有している。前記読取り／書込み装置と前記端末装置とは同じ装置であってもよい。

【 0 0 1 7 】

【 発明の実施の形態 】

図 1 に言及すると、本発明に係る取引カードの磁気ストライプのメモリを利用して安全な金融取引を行なうシステムは、一般に、カードの磁気ストライプのメモリに資金を移動するのに必要なデータをエンコードするステップを備えてなる（ブロック 1 0）。エンコードされたデータは、カードの磁気ストライプのメモリに標準形式で保存される専用取引番号を構成する（ブロック 1 2）。取引においてカードの磁気ストライプのメモリを利用する場合、専用取引番号を使って取引が行なわれる（ブロック 1 4）。専用取引番号は、金融機関によりデコードされ、照合確認される（ブロック 1 6）。照合で適性が確認されると、金融機関は、その取引成立の許可を与える（ブロック 1 8 および 2 0）。このようにして、取引カードの磁気ストライプのメモリを利用して安全な金融取引が行われる。

【 0 0 1 8 】

本発明は、クレジットカードや、ＡＴＭカードや、デビットカードのような、ある種身分証明書とも言える一般的な取引カードを利用するものである。このカードは、表面にインプリントされた一連の番号を有している。このカードには、１４文字から１９文字までの文字をインプリントすることができ、最初の４文字は、銀行がカードを発行する際のピンナンバーとしても知られているルーティングナンバーを表している。残りのナンバーは、一般には、そのカードの発行版とそのカードと関連する口座番号を表す。

【 0 0 1 9 】

また、このカードは、顧客の氏名、口座番号、および銀行のルーティングナンバー情報の保存に一般に利用される磁気ストライプのメモリを備えている。この磁気ストライプのメモリには、情報を保存できる３つのトラックがある。これらのトラックに情報をいかに記録するかについてのフォーマットは、国際基準により統制されている。例えば、各トラックの内容は、参考までに挙げると、国際標準化機構基準 ＩＳＯ／ＩＥＣ 7 8 1 1 2 : 1 9 9 5 ( E ) により統制されている。この ＩＳＯ／ＩＥＣ 7 8 1 1 2 : 1 9 9 5 ( E ) は、カードが金融のネットワークであまねく読取り可能で且つ受入れ可能なようにするため、全ての取引カードの磁気ストライプ情報のフォーマットの統一化を規定するものである。この ＩＳＯ基準は、磁気ストライプのメモリの各トラックにおけるエンコード技法、情報のフォーマットおよび情報量を統制している。

【 0 0 2 0 】

例えば、この基準は、２周波数記録法と呼ばれる２進コード化技法を、データの各トラックへの記録に用いる技法として指定している。トラック 1 は、８．２７ビット／ミリおよび 7 9 文字（英数字を含む）からなる。トラック 2 は、より小さいビット密度であって、２．９５ビット／ミリおよび 4 0 英数字からなり、磁気ストライプの読取り装置により最もよく使用されるトラックであり、高い信頼性と反復可能性のあるものでなければならない。また、トラック 3 は、読取り／書込み用トラックとして指定されており、８．２７ビット／ミリおよび 1 0 7 数字からなる。本発明は、現行の磁気ストライプ読取り装置により読取り可能な磁気ストライプのメモリのうち、前記トラックの一つ、好ましくはトラック 2、に専用取引番号を保存するようにしている。

【 0 0 2 1 】

専用取引番号は、現金自動振込支払機（ＡＴＭ）装置や、商人側端末や、顧客のアクセス端末（ＣＡＴ's）等のネットワークに受け付けられ、且つ銀行により特定の口座として認識される一群の文字群である。例えば、専用取引番号は、金融機関に特定の口座であることを示す１つの文字と、利用者の暗証番号（ＰＩＮ）を表す複数の文字と、口座番号の全てまたは一部を表す複数の文字と、その取引に必要な金額を表す複数の文字とで構成することができる。この専用取引番号は、そのような情報の基準に合うようにフォーマット化する場合、磁気ストライプのメモリの前記トラックの一つに記録させてもよい。このように

、専用取引番号は、一般の口座番号のように使って金融取引を行なうことができる。

【 0 0 2 2 】

図 2 に言及すると、取引カードの磁気ストライプのメモリを利用して安全な金融取引を行なうようにした本発明に係る実施例のシステムは、取引カード 3 2 と、金融機関のホストシステム 3 6 と通信関係にある取引カード読取り / 書込み装置 3 4 および / または金融ネットワーク 4 0 を介して前記ホストシステム 3 6 と通信関係にあるカード読取り / 書込み端末 3 8 とから構成している。取引カード読取り / 書込み装置 3 4 は、携帯情報端末 ( P D A ) や、カード 3 2 にある様々なメモリの読取り / 書込みが可能なその他の同様の装置であってもよい。また、端末 3 8 は、商人側の端末、 A T M、 C A T、および類似の装置であって、カードに少なくとも磁気ストライプのメモリ 4 2、好ましくは、先進技術のメモリ 4 4 を読取る能力を有するものとすることができる。取引カード 3 2 は、磁気ストライプのメモリ 4 2 と、集積回路 ( I C )、スマートカードメモリ、オプティカルストライプのメモリ、および薄膜型半導体メモリ等の先進技術のメモリ 4 4 の少なくとも一つから構成している。先進技術のメモリ 4 4 は、メモリにパース金額 ( パースバリュー ) 4 8 を保存する電子パースアプリケーション 4 6 を備えている。例えば、口座金額 5 0 を、前記ホストシステム 3 6 の顧客の口座 5 4 の範囲内で個別の口座 5 2 からスマートカードメモリ 4 4 へ移すことができる。適合する個別の口座 5 2 としては、給与等の払込口座 ( D D A )、普通預金口座、等々が挙げられる。口座金額 5 0 は、金融機関のホストシステム 3 6 と通信関係にある P D A 3 4 等のスマートカード読取り / 書込み装置を利用するかネットワーク 4 0 を介してホスト 3 6 と通信関係にある A T M 3 8 を介して、転送される。ネットワーク 4 0 は、カード 3 2 が、電子的な資金の移動 ( E F T ) のネットワークや、電話のネットワークや、インターネット等のホストシステム 3 6 と通信することができる通信ネットワークであればどのような通信ネットワークでもよい。ホストシステム 3 6 は、課金情報や、取引、および金融機関の顧客の口座 5 4 の残高勘定の全てを追跡記録し且つ保存する。移動が生じると、ホストシステム 3 6 は、その移動に使用するカード番号および / またはスマートカードメモリに関連付けて、口座金額 5 0 を電子パース 4 6 へ送るための口座として使用するミラー口座すなわち仮口座 5 6 を作り出す。

【 0 0 2 3 】

本発明は、先進技術のメモリ 4 4 の電子パース 4 6 に保存したパース金額 4 8 を、磁気ストライプのメモリで使用するようにするものである。上記したように、口座金額 5 0 は、ネットワーク 4 0 との相互作用により取引カード 3 2 上の先進技術のメモリ 4 4 の電子パース 4 6 に送ることも可能である。また、その金額は、一つの先進技術のメモリから同一カードにおける他の先進技術のメモリへ送ることもできるし、一つのカードから他のカードへ送ることも可能である。同様に、他のカードの磁気ストライプのメモリまたは先進技術のメモリや、カードの読取り / 書込み装置のメモリや、他の同様の装置等の複数の情報源から磁気ストライプへ金額を転送することも可能である。

【 0 0 2 4 】

図 2 および図 3 A - 3 B について言及すると、パース金額 4 8 を磁気ストライプのメモリ 4 2 に送るには、読取り / 書込み装置としての、 P D A 3 4 や、 A T M 3 8 や、商人側端末 3 8 や、あるいはカードにおける先進技術のメモリや磁気ストライプのメモリに対して読取り / 書込み可能な、他の同様な電子装置に、カード 3 2 を挿入して行なうことができる ( 図 3 A、ブロック 6 0 )。つまり、これらの読取り / 書込み装置は、先進技術のメモリと通信可能で、この先進技術のメモリに対する読取りおよび書込みを行う第 1 読取り / 書込み手段と、磁気ストライプのメモリに対する読取りおよび書込みを行う第 2 読取り / 書込み手段とを備えている。

【 0 0 2 5 】

読取り / 書込み装置としての P D A 3 4 および / または端末 3 8 は、例えばパース金額 4 8 のような値を先進技術のメモリ 4 4 の電子パース 4 6 から磁気ストライプ 4 2 に転送することが可能なアプリケーションを備えている ( 図 3 A、ブロック 6 2 )。換言すれば、これらの読取り / 書込み装置は、そのようなアプリケーションを実行することができる処



理装置を備えている。このアプリケーションにより、カード保有者は、転送すべき金額や、電子パースの識別（番号）や、専用 P I N 等の一連の取引データを指定することができる（図 3 A , ブロック 6 4）。つまり、前記処理装置は、当該アプリケーションを実行することによって、一連の取引データの指定を受け付ける取引指定受付手段として機能することができる。このアプリケーションは、取引データのエンコードと専用取引番号への変換とを行うものである（図 3 A , ブロック 6 6 および図 1、ブロック 1 0）。つまり、前記処理装置は、当該アプリケーションを実行することによって、カード保有者が指定した取引データを口座番号とともにエンコードして専用取引番号へと変換する手段として機能する。専用取引番号は、磁気ストライプのメモリに記録される（図 3 A , ブロック 6 8、および図 1、ブロック 1 2）。より具体的には、前記処理装置は、当該アプリケーションを実行することによって、前記変換された専用取引番号を前記第 2 読取り / 書込み手段によって前記取引カードの磁気ストライプのメモリに記録させる手段として機能する。また、このアプリケーションは、電子パース 4 6 の金額 4 8 等の転送アカウントを、磁気ストライプのメモリ 4 2 へ転送した金額分減少させる（図 3 A , ブロック 7 0）。より具体的には、前記処理装置は、当該アプリケーションを実行することによって、先進技術のメモリの電子パースの電子パースバリューを、前記第 1 読取り / 書込み手段によって、前記磁気ストライプのメモリに転送した金額的値の分だけ減少させる手段として機能する。このようにして、金銭的な値は、先進技術のメモリから磁気ストライプのメモリに転送され、そのとき、その値は、専用取引番号という形で利用される。

#### 【 0 0 2 6 】

一旦その専用取引番号が磁気ストライプのメモリ 4 2 に記録されると、取引カード 3 2 は、先進技術のメモリ 4 4 から転送された金銭的値を用いて、取引において利用可能となる。例えば、図 2 および図 3 A - 3 B について述べると、取引カード 3 2 を A T M 3 8 に挿入して現金を受取ることができる。すなわち、磁気ストライプのメモリ 4 2 が A T M 3 8 を通ることにより、A T M 3 8 との取引が開始される（図 3 A , ブロック 7 4）。銀行のルーティングナンバーおよび専用取引番号が A T M 3 8 で読取られる（図 1、ブロック 1 4 参照）。この場合、A T M 3 8 は、暗証番号（P I N）および取引額を入力するように促す（図 3 A , ブロック 7 6）。P I N および取引額を入力すると、A T M 3 8 は、P I N と、取引額と、専用取引番号とからなる取引ファイルを、金融のネットワーク 4 0 を介して、銀行ルーティングナンバーにより識別される金融機関のホストシステム 3 6 に送る（図 3 A , ブロック 7 8）。ホストシステム 3 6 は、そのファイルを開き、デコードし、その番号（専用取引番号）が、ミラー / 仮口座 5 6 と関連づけられた専用の口座番号であることを示す標識を認識する（図 3 A , ブロック 8 0 および図 1、ブロック 1 6 参照）。ホストシステム 3 6 は、その P I N およびミラー / 仮口座 5 6 を照合して、ミラー / 仮口座 5 6 における残額が取引き額以上であるかどうかを確認する（図 3 A , ブロック 8 2 および図 1、ブロック 1 6）。確認すると、ホストシステム 3 6 は、ミラー口座 5 6 の残額が、専用取引番号で識別される磁気ストライプのメモリ 4 2 に転送されたパース金額 4 8 以下かどうかによって、A T M 3 8 に対して許可または拒否の返答を行ない、取引額相当の現金を開放したり拒否したりする（図 3 B , ブロック 8 4 および図 1、ブロック 1 8）。取引が許可された場合には、取引き額で指示された金額分、ミラー口座 5 6 の残額を減らす（図 3 B , ブロック 8 6）。許可の返答の場合、A T M 3 8 は、取引き額に対する現金を出す（図 3 B , ブロック 8 8 9 0、および図 1、ブロック 2 0）。一方、拒否の返答の場合、A T M 3 8 は、別の取引を促すか、そのセッションを終了することができる（図 3 B , ブロック 9 0）。このようにして、先進技術のメモリの値は、磁気ストライプのメモリの取引において利用される。

#### 【 0 0 2 7 】

本発明は、専用取引番号を確実に安全なものにする多くの代替手段を提供する。実施例の一つでは、専用取引番号を、取引カードのスマートカードのメモリからシークレット（秘密キー / 公開キーの公開キー）を用いてエンコードする。なお、シークレットは、金融機構の公開キーから構成することができ、また金融機関の公開キーで暗号化した如何なる情

10

20

30

40

50

報も、金融機関が関連の秘密キーを用いない限り暗号の解読はできない。斯くして暗号化した情報の安全性を確保するようにしている。さらに、このシークレットは、おそらく金融機関によってスマートカードのメモリ内に収められ、シークレットを必要とする取引の安全性を確保するように為されることになる。

#### 【 0 0 2 8 】

なお、シークレットは、金融機関の承認を得た信用のおける第三者により提供されるようにすることもできる。この実施例の場合、資金の移動を実行するのに必要なデータを、スマートカードのメモリのシークレットを用いて暗号化し、暗号文を専用取引番号という形で表すようにしている。このようにして、データの暗号化に用いる公開キーと関連付けされた秘密キーを有する金融機関しか、その専用取引番号の暗号の解読はできないようにしている。

10

#### 【 0 0 2 9 】

別の実施例では、専用取引番号の安全性を、暗号化システムと関連付けした非常に正確なクロックを用いたタイムスタンプでそのナンバーをエンコードすることで確保するようにしている。なお、クロックは、証明用装置で使用されているものと同様のものである。このクロックと暗号化システムは P D A もしくは他の同等装置にあり、且つホストシステムに設けられたクロックおよび暗号化システムと同期状態にする。この結果、エンコード済みデータはその時点特有の特定の暗号化公式で関連付けするタイムスタンプのあるエンコード済みデータになる。結果として、タイムスタンプで記録した特定時間にエンコードしたデータのセットは、1 セットのみの暗号化済みデータになるだけであるから、専用取引番号上のタイムスタンプを読取ることにより、ホストシステムは暗号化公式を判定することができ、因って専用取引番号を復号化（解読）することができる。

20

#### 【 0 0 3 0 】

上記したように、専用取引番号は、とりわけ、P I N と取引の値との情報で構成することができる。この P I N は、磁気ストライプのメモリでの取引のためのカードに関連付けられた一般的な P I N と同じ P I N であってもよいし、また、専用取引番号のために作られた専用の取引 P I N であってもよい。取引きの時点で提供された P I N と、専用取引番号に含まれる P I N とを比較対照することで、本発明のセキュリティはさらに向上する。二つの P I N が符合することを確認することによって、本システムは、承認された者により取引が行われていることを保証するのに役立つ。

30

#### 【 0 0 3 1 】

また、専用取引番号は、P I N と金額と口座番号との組み合わせを表す圧縮フォーマットに含ませることもできる。例えば、2 進コードや、1 6 進コードを使用してもよい。例えば口座番号を記録する磁気ストライプのトラック 2 のビットを使用して、専用取引番号を表す 2 進コードや 1 6 進コードを記録するようにもできる。現行の磁気ストライプ読取り装置は、このコードを読取って、それを I S O / I E C 7 8 1 1 2 : 1 9 9 5 ( E ) で確認される現在の規格に従い翻訳する。ただし、上記したように、ビットの 1 つを使用し、その番号が専用取引番号である旨の信号をホストシステムに送るようにしているため、ホストシステムは、その番号を I S O 基準に規定されている番号から 2 進数や 1 6 進数等のコーディングシステムに基づく番号に変換する。2 進または 1 6 進コーディングシステムの使用により、専用取引番号用の圧縮フォーマットにすることができ、口座番号よりは多くの情報を表わすようにできるが、磁気ストライプにおける同一量の空白に収められる。

40

#### 【 0 0 3 2 】

2 進コードを使用することにより、本システムは次のように作用する。磁気ストライプのトラック 2 では、1 文字につき 5 ビットを使用する 4 0 文字が利用可能である。一般には、文字の多くはハードウェアの制御用に保存されるため、総文字数的一部分だけを使用して情報を保存するようにしている。従って、一般には 1 9 文字だけを使用して、この文字分で銀行のルーティングナンバーおよび顧客の口座番号を保存することができると仮定する。これら 1 9 文字は、合計 9 5 ビットを表わす。2 進コードを使用すれば、これら 9 5

50

ビットは、0 から ( 2 9 5 1 ) まで、あるいは、0 から 3 . 9 6 1 4 × 1 0 2 8 までの数を表わすことができる。ただし、ビット・シーケンスのいく分かはハードウェアの制御用に保存される。従って、P I N や、口座番号や、取引金額や、その他あらゆる関連情報を表わす非常に大きな数を磁気ストライプにエンコードするのに利用可能なビットは多数ある。なお、コーディング技法によっては、英数字を認識させるようにしてもよい。従って、前記専用取引番号は、P I N、取引金額、口座番号、標識、および、共に暗号化される他の如何なる英数字表示からも構成することができる。

#### 【 0 0 3 3 】

また、専用取引番号の各ビットを分解して、情報の様々な部分を別々に表わすようにしてもよい。例えば、銀行のルーティングナンバーは一般に 4 桁であるから、0 0 0 0 から 9 9 9 9 まで値域を定めることができる。2 進コードを使うと、0 0 0 0 から 9 9 9 9 までの数字を 1 4 ビットで表わすことができる。例えば、銀行のルーティングナンバーが 6 2 1 8 である場合、2 進法では次のように表わされる。

#### 【 0 0 3 4 】

ビット： 0 1 2 3 4 5 6 7 8 9 10 11 12 13  
 記録形態： 0 1 0 1 0 0 1 0 0 0 0 1 1 0  
 2 進法：0 + 2 + 0 + 8 + 0 + 0 + 6 4 + 0 + 0 + 0 + 0 + 2 0 4 8 + 4 0 9 6 + 0  
 = 6 2 1 8

また、銀行のルーティングナンバーの各文字を 2 進法で個別に表わしてもよい。ただし、この方法は、各文字が 4 ビットを必要とするため、さほど効果的ではない。例えば、各文字は、次のように表わすことができる。

#### 【 0 0 3 5 】

文字： 6 2 1 8  
 ビット： 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3  
 記録形態： 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 1

また、例えば、利用可能なビット総数が 2 文字列に分解される場合は、使用するビット数をより少なくすることができる。第 1 列のビットは、数 x までカウントアップし、次の列のビットは、x + 1 から y までカウントする。ここで、x、x + 1 および y は、数字を表わす。この場合、これら 2 文字列のビットは、総計するか結合して 1 つの数にする。当業者なら理解できるように、圧縮フォーマットに長い文字列の英数字または数字だけの文字を表わすのに使用可能なスキームは多数ある。

#### 【 0 0 3 6 】

また、別の実施例では、I S O / I E C 7 8 1 1 - 2 : 1 9 9 5 ( E ) で認定されているコード化した文字セットを用いて、専用取引番号を磁気ストライプのメモリに記録する。この専用取引番号は、任意データフィールド、非任意データフィールド、あるいは双方の組合わせに記録することが可能である。磁気ストライプのトラック 2 の非任意データフィールドの一例は、銀行のルーティングナンバーと個々の口座番号とからなる暗証番号 ( P I N ) 用に保存された 1 9 文字からなる。同様に、トラック 2 には、任意データとして使用可能な 1 3 文字がある。これら文字の各々は、4 ビットからなる。専用取引番号を非任意データフィールドに記録する際、その専用取引番号は、P I N 全体もしくは少なくとも一部分に書込むか記録する。同様に、専用取引番号は、1 3 文字からなる任意データフィールド全体または一部に記録することができる。最後に、一実施例では、専用取引番号を P I N 全体に記録することもできるし、また、少なくとも 1 つの文字の標識を任意データフィールドまたは非任意データフィールドに記録して、磁気ストライプを読取るシステムに対して P I N 域における番号が専用の番号であることを指示するようにしてもよい。

#### 【 0 0 3 7 】

例えば、専用取引番号を 1 0 文字から構成することもできるが、この場合、6 文字を使用して移動すべき取引金額や値を構成し、残りの 4 文字を使用して専用の取引 P I N を構成することができる。取引カードの値を集積回路のメモリから磁気ストライプのメモリに送りたい場合、カードを、読取り / 書込み装置に挿入して、取引金額および専用の P I N を

10

20

30

40

50

表示する。この情報は、暗号化されて専用取引番号を形成し、そして磁気ストライプ上に記録される。ISO基準に認定されている記録技法を使って、専用取引番号を構成する10文字は、コード化した文字セットにより1か0かで記録される合計40ビットからなる。

【0038】

本発明のシステムは、40ビットからなる暗号化された専用取引番号を記録する前に、その暗号化された専用取引番号に使用できない4ビット列が含まれていないかどうかの評価を行なう変更子を備えている。何故なら、ISO基準のコード化した文字セットに認定されているように、そのようなビット列は、ハードウェアの制御用に保存されるものであるからである。もし暗号化された専用取引番号にそのようなビット列が含まれている場合には、変更子は、そのようなビット列を含まない訂正済みの専用取引番号にすると共に、ナンバーが訂正済みであることを専用取引番号を読取るシステムに指摘する、専用取引番号の一部からなる、訂正ポイントを提供する。

10

【0039】

最後に、標識文字が、任意データフィールドまたは非任意データフィールドに記録される。この標識文字は、ホストシステムにより認識され、その専用取引番号が、一般の口座番号と混同しないように識別される。このように、本発明は、値を取引カードの磁気ストライプのメモリに安全に送るシステムを提供するものである。

【0040】

以上好適実施例を引用して本発明の説明を行なったが、他の実施例でも同じ効果を奏することができる。本発明の変更例や修正例は当業者にとっては明らかなものがあり、特許請求の範囲の記載は、そのような変更例や同等の変更を全て包含しようとするものである。

20

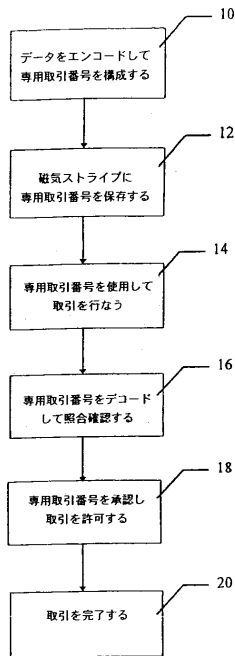
【図面の簡単な説明】

図1は、本発明の基本的ステップのいくつかを表したフローチャートである；

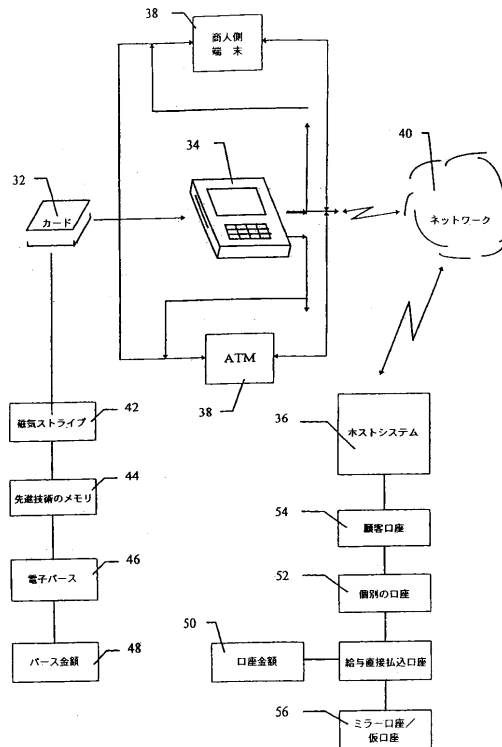
図2は、本発明の実施例の模式図である；

図3A - 3Bは、本発明の他の実施例を表すフローチャートである。

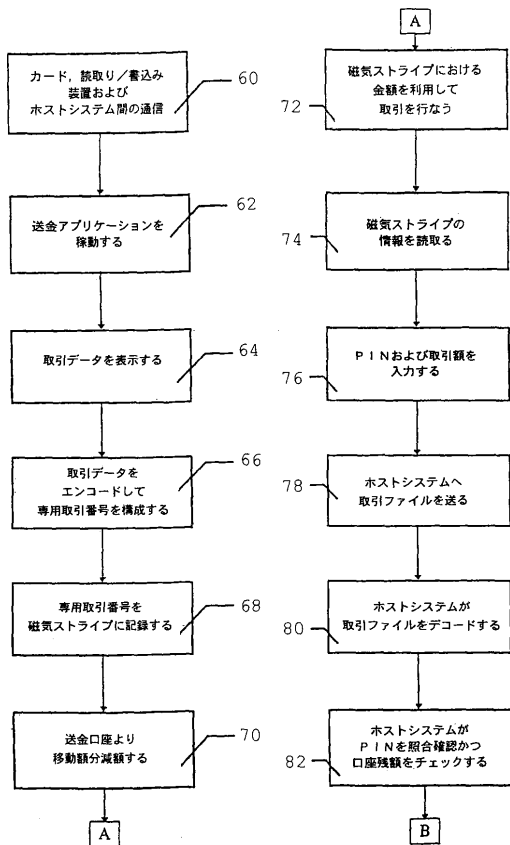
【図 1】



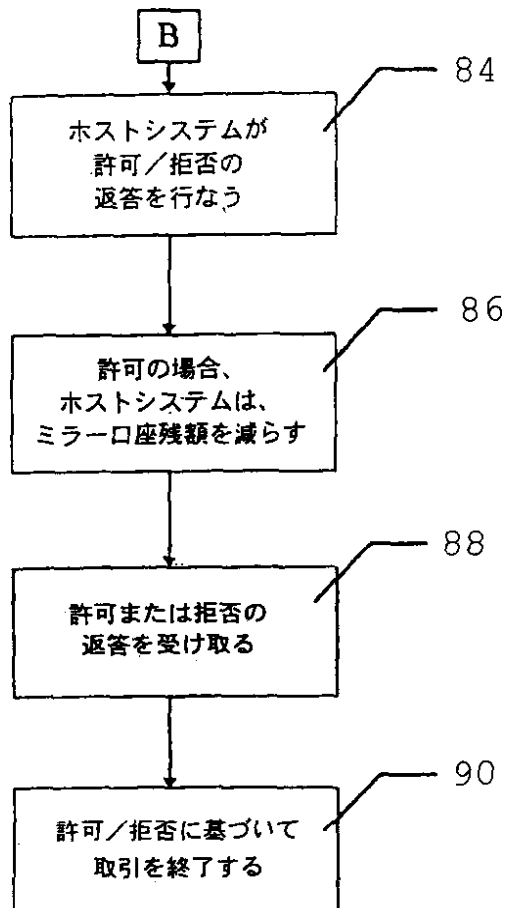
【図 2】



【図 3 A】



【図 3 B】



---

フロントページの続き

- (72)発明者 クワン, ジョセフ シー  
アメリカ合衆国 カリフォルニア州 9 0 0 6 8、ハリウッド、パラマウント ドライブ 2 0 3 4
- (72)発明者 リクステイン, ヘンリー  
アメリカ合衆国 カリフォルニア州 9 0 4 0 2、サンタモニカ、デュライド ロード 5 4 4

## 合議体

審判長 赤穂 隆雄

審判官 後藤 彰

審判官 山本 穂積

- (56)参考文献 特開昭 6 2 - 2 5 3 7 2 ( J P , A )  
特開昭 6 3 - 2 6 7 7 0 ( J P , A )  
特開平 2 - 3 1 1 9 5 5 ( J P , A )  
国際公開第 9 5 / 2 4 6 9 0 ( W O , A 1 )

- (58)調査した分野(Int.Cl. , D B 名)

G06Q40/00

G07F7/10