

(19) 日本国特許庁 (JP)

再公表特許(A1)

(11) 国際公開番号

W02002/008981

発行日 平成16年1月8日 (2004.1.8)

(43) 国際公開日 平成14年1月31日 (2002.1.31)

(51) Int. Cl. ⁷

F I

G06F 17/60

G06F 17/60 414

G06K 17/00

G06F 17/60 422

G06K 19/06

G06F 17/60 506

G06K 19/07

G06F 17/60 512

H04Q 7/38

G06F 17/60 ZEC

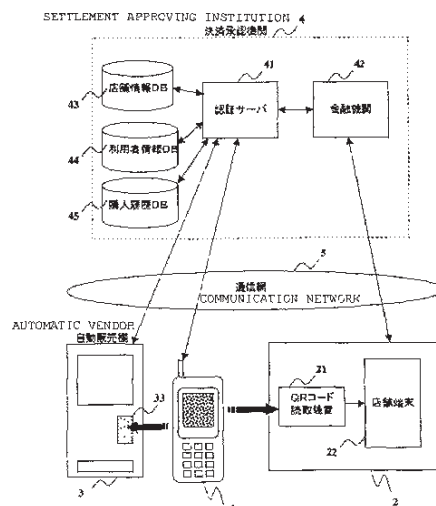
審査請求 有 予備審査請求 有 (全 47 頁) 最終頁に続く

出願番号	特願2002-514614 (P2002-514614)	(71) 出願人	500344688
(21) 国際出願番号	PCT/JP2001/004223		株式会社イマージュメディアデザイン
(22) 国際出願日	平成13年5月21日 (2001.5.21)		東京都品川区西五反田五丁目9番2号
(31) 優先権主張番号	特願2000-223658 (P2000-223658)	(74) 代理人	100088720
(32) 優先日	平成12年7月25日 (2000.7.25)		弁理士 小川 眞一
(33) 優先権主張国	日本国 (JP)	(72) 発明者	鹿野 裕司
(81) 指定国	EP (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), CN, JP, KR, US		東京都品川区西五反田四丁目9番19号

(54) 【発明の名称】 商取引方法およびネットワーク端末並びに商取引システム

(57) 【要約】

セキュアな認証と決済を提供する。購入の際、ネットワーク端末たとえば携帯電話 (1) の所有者は、売り手のIDや支払金額や暗証番号などの購入情報を入力して認証サーバ (41) に送信し、認証と与信照会の結果に基づき、決済の証明書を、携帯電話のディスプレイに2-Dバーコードとして表示できるQR決済証明鍵として受信する。店舗端末 (22) は、読取装置 (21) によってこの表示されたコードを読みとるとともにバーコードとして外部にマークされている携帯電話の製造番号と電話番号も読みとり、認証サーバに送信する。認証サーバは、このコードが以前に自ら発行したものであるかやこの製造番号が正当なものであるかなどを確認する。



43...SHOP INFORMATION DB
 44...USER INFORMATION DB
 45...PURCHASE HISTORY DB
 41...AUTHENTICATION SERVER
 42...FINANCIAL INSTITUTION
 21...QR CODE READER
 22...SHOP TERMINAL

【特許請求の範囲】**【請求項 1】**

決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、
商取引に関する決済証明鍵情報を決済承認機関から受信するステップと、
受信した決済証明鍵情報を前記表示手段に表示させるステップと、
前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送し、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップと
を備えることを特徴とする商取引方法。

10

【請求項 2】

決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、
商取引に関する決済証明鍵情報と商品購入元から発行される受託証明とを決済承認機関から受信するステップと、
受信した決済証明鍵情報付きの受託証明を前記表示手段に表示させるステップと、
前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送し、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップと
を備えることを特徴とする商取引方法。

20

【請求項 3】

前記ネットワーク端末として携帯電話機を用いたことを特徴とする請求項 1 又は請求項 2 のいずれか一項に記載の商取引方法。

【請求項 4】

前記決済証明鍵情報を受信するネットワーク端末と、商取引における注文主のネットワーク端末とを異なる端末としたことを特徴とする請求項 1 ～ 3 のいずれか一項に記載の商取引方法。

【請求項 5】

前記表示手段に表示される決済証明鍵情報はコードキャラクタ情報画像で構成されていることを特徴とする請求項 1 ～ 4 のいずれか一項に記載の商取引方法。

30

【請求項 6】

前記表示手段に表示される決済証明鍵情報は暗号化されたコードキャラクタ情報画像で構成されていることを特徴とする請求項 1 ～ 5 のいずれか一項に記載の商取引方法。

【請求項 7】

前記ネットワーク端末は各端末機器の識別情報を記録した標識を有するものとし、
前記決済端末に前記識別標識を読取らせるステップと、
前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別標識の情報を前記決済承認機関に送信し、前記識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証させるステップと、
前記識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信するステップと
をさらに備えることを特徴とする請求項 1 ～ 6 のいずれか一項に記載の商取引方法。

40

【請求項 8】

前記ネットワーク端末は、ICカード又はネットワーク端末の所有者のいずれかの識別情報を記録した識別標識を有するものとし、
前記決済端末に前記識別標識を読取らせるステップと、
前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別標識の情報を前記決済承認機関に送信し、前記識別標識の情報が決済承認機関に予め登録された正規のもの

50

であるか否かを認証させるステップと、
前記識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を
決済承認機関から商品購入元の決済端末に送信するステップと
をさらに備えることを特徴とする請求項 1 ～ 6 のいずれか一項に記載の商取引方法。

【請求項 9】

前記識別標識は、所定波長の照射光に対し前記識別標識に記録された識別情報を所定波長の
反射光により出射する標識で構成されていることを特徴とする請求項 1 ～ 8 のいずれか
一項に記載の商取引方法。

【請求項 10】

前記決済証明鍵情報の中に含まれる購入者に関する情報を商品購入元の決済端末の表示部 10
に表示させるステップをさらに備えることを特徴とする請求項 1 ～ 9 のいずれか一項に記載
の商取引方法。

【請求項 11】

決済を終えた取引の内容を商品購入元の決済端末から決済承認機関に送信し、購入者の購
入履歴情報を更新するステップをさらに備えることを特徴とする請求項 1 ～ 10 のいずれ
か一項に記載の商取引方法。

【請求項 12】

決済を終えた取引の内容を決済承認機関から購入者のネットワーク端末に送信し、取引の
内容を表示させるステップをさらに備えることを特徴とする請求項 1 ～ 11 のいずれか一
項に記載の商取引方法。 20

【請求項 13】

決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受
する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商
品に関する決済を行う商取引方法であって、
商取引に関する決済証明鍵情報と商品購入元から発行される受託証明とを決済承認機関か
ら前記ネットワーク端末で受信するステップと、
受信した決済証明鍵付きの受託証明をコードキャラクタ情報画像で印刷させるステップと
、
印刷された前記決済証明鍵情報付きの受託証明を商品購入元に設置された決済端末に読み
取らせ、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステ
ップと 30
を備えることを特徴とする商取引方法。

【請求項 14】

前記コードキャラクタ情報画像は、所定波長の照射光に対し決済証明鍵情報を所定波長の
反射光により出射する結晶粉末を混入した印刷材料で印刷することを特徴とする請求項 1
3 に記載の商取引方法。

【請求項 15】

前記ネットワーク端末は商取引に関する情報を入力する入力手段を有し、
少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番
号を含む商品の取引に関する情報を前記入力手段から入力するステップと、 40
入力された決済に関する情報を決済承認機関に送信し、商品提供元の認証と購入者自身の
認証及び与信の結果に応じて生成された決済証明鍵情報を受信するステップと
をさらに備えることを特徴とする請求項 1 ～ 13 のいずれか一項に記載の商取引方法。

【請求項 16】

前記ネットワーク端末は商取引に関する情報を入力する入力手段を有し、
少なくとも商品提供元又は商品の識別情報、決済方法、利用サービスポイント及び購入者
自身の暗証番号を含む商品の取引に関する情報を前記入力手段から入力するステップと、
入力された決済に関する情報を決済承認機関に送信し、商品提供元の認証と購入者自身の
認証及び前記購入者の獲得したサービスポイントの確認結果に応じて生成された決済証明
鍵情報を受信するステップと 50

をさらに備えることを特徴とする請求項 1 ～ 15 のいずれか一項に記載の商取引方法。

【請求項 17】

取引対象の商品の決済に関する情報を入力する入力手段と、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引装置であって、

商取引に関する決済証明鍵情報を生成する手段と、

前記決済証明鍵情報を前記ネットワーク端末に送信し表示させる手段と

を備えることを特徴とする商取引装置。

【請求項 18】

決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引装置であって、

商取引に関する決済証明鍵情報を生成する手段と

商品購入元から発行される受託証明を受信し、前記決済証明鍵情報付き受託証明として前記ネットワーク端末に送信し表示させる手段と

を備えることを特徴とする商取引装置。

【請求項 19】

前記ネットワーク端末として、携帯電話機を用いたことを特徴とする請求項 17 又は 18 のいずれか一項に記載の商取引装置。

【請求項 20】

決済に関する情報を表示する表示手段と、機器識別標識と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

前記決済承認機関装置が、

商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、

前記決済証明鍵情報の一部又は全部と前記機器識別標識の読取結果を商品提供元から受信し、前記機器識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、

前記機器識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信し、購入者が発注した商品の引渡し及び代金の決済を実行させる手段と

を備えることを特徴とする商取引システム。

【請求項 21】

決済に関する情報を表示する表示手段と、機器識別標識と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

前記決済承認機関装置が、

商取引に関する決済証明鍵情報を生成する手段と、

商品購入元から発行される受託証明と前記決済証明鍵情報とを前記ネットワーク端末に送信し表示させる手段と、

前記決済証明鍵情報の一部又は全部と前記機器識別標識の読取結果を商品提供元から受信し、前記機器識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、

前記機器識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信する手段と

を備えることを特徴とする商取引システム。

【請求項 2 2】

前記ネットワーク端末は、携帯電話機であることを特徴とする請求項 2 0 又は 2 1 のいずれか一項に記載の商取引システム。

【請求項 2 3】

前記機器識別標識は、所定波長の照射光に対し機器製造番号情報および電話番号情報を所定波長の反射光により出射する標識で構成されていることを特徴とする請求項 2 0 ～ 2 2 のいずれか一項に記載の商取引システム。

【請求項 2 4】

決済に関する情報を表示する表示手段と、通信網を介して商品の発注及び決済に関する情報を送受する送受信手段とを有する携帯端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

前記決済承認機関装置が、

商取引に関する決済証明鍵情報を生成する手段と、

商品購入元から発行される受託証明と前記決済証明鍵情報とを前記ネットワーク端末に送信する手段と、

前記ネットワーク端末に付属の印刷装置によってコードキャラクタ情報画像で印刷された受託証明と前記決済証明鍵情報の読取結果を商品購入元から受信し、前記決済証明鍵情報が正当なものであるか否かを認証する手段と、

前記決済証明鍵情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信し、購入者が発注した商品の引渡し及び代金の決済を実行させる手段と

を備えることを特徴とする商取引システム。

【請求項 2 5】

前記コードキャラクタ情報画像は暗号化されたコードキャラクタ情報画像で構成されていることを特徴とする請求項 2 4 に記載の商取引システム。

【請求項 2 6】

決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行うためのプログラムを記録した媒体であって、

決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる処理と、

前記決済証明鍵情報が表示されたネットワーク端末から商品購入元に設置された端末に前記決済証明鍵情報を転送し、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行させる処理と

を含むコンピュータが読み取り可能な商取引用のプログラムが記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

技術分野

本発明は、携帯電話機等のネットワークに接続可能な端末を用いてスーパーマーケット等の各種の店舗、インターネットのサーバ上に開設されている電子店舗、あるいは飲料水等の自動販売機で購入する商品の代金の決済を行う商取引方法及び装置並びにシステムに関するものである。

背景技術

携帯電話機に WWW 閲覧機能 (World Wide Web) を付加したことにより、携帯電話機を使用してインターネットにアクセスし、各種の情報、物品、役務サービスを開覧し、必要に応じて、それらの情報、物品、役務サービスの提供を注文するという取引形態が急速に拡大している。ここで、本発明では、形状を有しない音楽ソフトなどの情報 (コンテンツ)、形状を有する物品、宅配サービス、介護サービスなどの役務サービスを全て商取引の対象となる商品と定義する。この場合、公共機関が提供する無料の介護サービスもあるが、無料であっても取引の対象となる商品に含むものとする。

しかし、携帯電話機を使用して商品の発注を行ったとしても、その決済方法としては、銀行振込みや現金の送付、商品到着時の代金引換などの従来の商慣習に従った方法が踏襲されている。

最近では、このような旧来方法に代えて、商品の注文と同時に、クレジットカード番号を商品提供元（店舗）に通知し、クレジットカード会社を通じて決済する方法が実施されている。

しかし、この決済方法は、クレジットカード会社と本人だけが知るべき番号あるいは情報が外部に漏れないことを前提にしており、外部に漏れた場合には悪用される危険性がある。

そこで、2001年5月から開始される次世代移動通信サービスでは、携帯電話機にUIM (User Identity Module) と呼ばれるICカードを搭載し、このICカード内の暗号プログラムによりクレジットカード番号等の秘密データを暗号化し、決済を行うという方法が考えられている。 10

しかし、暗号プログラムにより暗号化して保存したとしても、携帯電話機自体を紛失した場合には、不正な第三者に解読されてしまい、悪用される危険性がある。特に、ICカード内にはクレジットカード番号のみでなく、銀行口座番号や保険証番号、電子マネーなどの他の秘密データも同時に保存する形態が多くなると考えられるので、不正な第三者に解読された場合の危険性は旧来の決済方法よりも高くなるという問題がある。

また、非接触型ICカード同様、無線を利用したネットワークは特に有線ネットワーク以上に不正アクセスを含むハッキング等、情報が外部に漏れる可能性が高くなるという問題がある。 20

また、不正な店舗の出現により、店舗での決済時に秘密データが盗聴され、悪用される危険性がある。

また、携帯電話機自体のコストも上昇し、さらに電力消費も増加し、電池寿命が短くなるという問題がある。

本発明はこのような問題を解決するためになされたものであり、その目的は、クレジットカード番号等の秘密データを本人認証機関やクレジットカード会社以外に開示することなく本人認証を行い、安全に購入商品の決済を行うことができる商取引方法及び装置、並びにシステムを提供することにある。

発明の開示 30

上記目的を達成するために、本発明の商取引方法は、以下のように構成したことを特徴とするものである。

すなわち、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、

商取引に関する決済証明鍵情報を決済承認機関から受信するステップと、受信した決済証明鍵情報を前記表示手段に表示させるステップと、前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送し、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップとを備えることを特徴とする。

また、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、 40

商取引に関する決済証明鍵情報と商品購入元から発行される受託証明とを決済承認機関から受信するステップと、受信した決済証明鍵情報付きの受託証明を前記表示手段に表示させるステップと、前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送し、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップとを備えることを特徴とする。

また、前記ネットワーク端末として携帯電話機を用いたことを特徴とする。

また、前記決済証明鍵情報を受信するネットワーク端末と、商取引における注文主のネットワーク端末とを異なる端末としたことを特徴とする。 50

また、前記表示手段に表示される決済証明鍵情報はコードキャラクタ情報画像で構成されていることを特徴とする。

また、前記表示手段に表示される決済証明鍵情報は暗号化されたコードキャラクタ情報画像で構成されていることを特徴とする。

また、前記ネットワーク端末は各端末機器の識別情報を記録した標識を有するものとし、前記決済端末に前記識別標識を読取らせるステップと、前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別標識の情報を前記決済承認機関に送信し、前記識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証させるステップと、前記識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信するステップとをさらに備えることを特徴とする。

10

また、前記ネットワーク端末は、ＩＣカード又はネットワーク端末の所有者のいずれかの識別情報を記録した識別標識有するものとし、

前記決済端末に前記識別標識を読取らせるステップと、前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別標識の情報を前記決済承認機関に送信し、前記識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証させるステップと、前記識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信するステップとをさらに備えることを特徴とする。

また、前記識別標識は、所定波長の照射光に対し前記識別標識に記録された識別情報を所定波長の反射光により出射する標識で構成されていることを特徴とする。

20

また、前記決済証明鍵情報の中に含まれる購入者に関する情報を商品購入元の決済端末の表示部に表示させるステップをさらに備えることを特徴とする。

また、決済を終えた取引の内容を商品購入元の決済端末から決済承認機関に送信し、購入者の購入履歴情報を更新するステップをさらに備えることを特徴とする。

また、決済を終えた取引の内容を決済承認機関から購入者のネットワーク端末に送信し、取引の内容を表示させるステップをさらに備えることを特徴とする。

また、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、

30

商取引に関する決済証明鍵情報と商品購入元から発行される受託証明とを決済承認機関から前記ネットワーク端末で受信するステップと、受信した決済証明鍵付きの受託証明をコードキャラクタ情報画像で印刷させるステップと、印刷された前記決済証明鍵情報付きの受託証明を商品購入元に設置された決済端末に読み取らせ、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップとを備えることを特徴とする。

また、前記コードキャラクタ情報画像は、所定波長の照射光に対し決済証明鍵情報を所定波長の反射光により出射する結晶粉末を混入した印刷材料で印刷することを特徴とする。

また、前記ネットワーク端末は商取引に関する情報を入力する入力手段を有し、

少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商品の取引に関する情報を前記入力手段から入力するステップと、入力された決済に関する情報を決済承認機関に送信し、商品提供元の認証と購入者自身の認証及び与信の結果に応じて生成された決済証明鍵情報を受信するステップとをさらに備えることを特徴とする。

40

また、前記ネットワーク端末は商取引に関する情報を入力する入力手段を有し、

少なくとも商品提供元又は商品の識別情報、決済方法、利用サービスポイント及び購入者自身の暗証番号を含む商品の取引に関する情報を前記入力手段から入力するステップと、入力された決済に関する情報を決済承認機関に送信し、商品提供元の認証と購入者自身の認証及び前記購入者の獲得したサービスポイントの確認結果に応じて生成された決済証明鍵情報を受信するステップとをさらに備えることを特徴とする。

本発明の商取引装置は、取引対象の商品の決済に関する情報を入力する入力手段と、決済

50

に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引装置であって、

商取引に関する決済証明鍵情報を生成する手段と、前記決済証明鍵情報を前記ネットワーク端末に送信し表示させる手段とを備えることを特徴とする。

また、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引装置であって、

商取引に関する決済証明鍵情報を生成する手段と商品購入元から発行される受託証明を受信し、前記決済証明鍵情報付き受託証明として前記ネットワーク端末に送信し表示させる手段とを備えることを特徴とする。

10

また、前記ネットワーク端末として、携帯電話機を用いたことを特徴とする。

また、決済に関する情報を表示する表示手段と、機器識別標識と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

前記決済承認機関装置が、商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、前記決済証明鍵情報の一部又は全部と前記機器識別標識の読取結果を商品提供元から受信し、前記機器識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、前記機器識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信し、購入者が発注した商品の引渡し及び代金の決済を実行させる手段とを備えることを特徴とする。

20

また、本発明の商取引システムは、決済に関する情報を表示する表示手段と、機器識別標識と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

前記決済承認機関装置が、商取引に関する決済証明鍵情報を生成する手段と、商品購入元から発行される受託証明と前記決済証明鍵情報とを前記ネットワーク端末に送信し表示させる手段と、前記決済証明鍵情報の一部又は全部と前記機器識別標識の読取結果を商品提供元から受信し、前記機器識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、前記機器識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信する手段とを備えることを特徴とする。

30

また、前記ネットワーク端末は、携帯電話機であることを特徴とする。

また、前記機器識別標識は、所定波長の照射光に対し機器製造番号情報および電話番号情報を所定波長の反射光により出射する標識で構成されていることを特徴とする。

また、決済に関する情報を表示する表示手段と、通信網を介して商品の発注及び決済に関する情報を送受する送受信手段とを有する携帯端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

40

前記決済承認機関装置が、商取引に関する決済証明鍵情報を生成する手段と、商品購入元から発行される受託証明と前記決済証明鍵情報とを前記ネットワーク端末に送信する手段と、前記ネットワーク端末に付属の印刷装置によってコードキャラクタ情報画像で印刷された受託証明と前記決済証明鍵情報の読取結果を商品購入元から受信し、前記決済証明鍵情報が正当なものであるか否かを認証する手段と、前記決済証明鍵情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信し、購入者が発注した商品の引渡し及び代金の決済を実行させる手段とを備えることを特徴とする。

また、前記コードキャラクタ情報画像は暗号化されたコードキャラクタ情報画像で構成さ

50

れていることを特徴とする。

また、本発明の取引方法は決済承認機関装置におけるプログラムによって実現することができる。そのプログラムは次のような処理を記録した記録媒体で提供することができる。すなわち、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行うためのプログラムを記録した媒体であって、決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる処理と、前記決済証明鍵情報が表示されたネットワーク端末から商品購入元に設置された端末に前記決済証明鍵情報を転送し、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行させる処理とを含むコンピュータが読み取り可能な商取引用のプログラムが記録されていることを特徴とする。

10

発明を実施するための最良の形態

以下、本発明の実施の形態を添付図面により詳細に説明する。

図1は、本発明の商取引方法を実施するシステムの全体構成の実施形態を示すシステム構成図であり、商品購入者が使用するネットワーク端末としての携帯電話機1、商品提供元の店舗2、飲料水等の自動販売機3、決済承認機関4で構成され、これらが通信網5で接続されている。通信網5は、無線回線と有線回線及びインターネット網を含むものである。ここで、ネットワーク端末とは、インターネット等のネットワークに接続可能な端末を示すものであり、以下の例に示す携帯電話機1の他、PHS、PDA、パーソナルコンピュータ、デジタルテレビ等、種々のものが含まれる。

20

携帯電話機1は、インターネット網に接続可能な機能を有する市販の携帯電話機であり、図2(a)の概略ブロック図に示すように、表示部11、無線送受信部12、制御部13、入力部14、送受信部15、メモリ16、外部入出力インタフェース17を備えている。表示部11にはインターネット接続モードにおいて、図2(b)に示すように、ニュース、モバイルバンキング、カード/証券/保険、モバイルショッピングなどのインターネット接続メニューが表示されるようになっている。

外部入出力インタフェース17は、Irda等の赤外線インタフェース及びブルーツースなどの微弱電波インタフェース等の無線通信インタフェースを含むものであり、本実施形態では、店舗の識別番号を店舗内に設置された発信機から受信する場合に使用される。また外部入出力インタフェース17には、携帯電話機接続型又は携帯電話機内蔵型のバーコード読取装置のインタフェースを含み、このバーコード読取装置により、バーコード情報で表示された店舗の識別情報又は商品の識別情報等を読取ることとしてもよい。さらに、携帯電話機接続型又は携帯電話機内蔵型のカメラを含み、このカメラにより、コードキャラクタ情報画像により表示された各店舗の識別情報又は商品の識別情報を、画像データとして取り込むこととしてもよい。この場合は、画像データとして取り込んだコードキャラクタ情報画像をデコードするためのプログラムを、前記決済承認機関4の認証サーバ内に設けておき、携帯電話機から送信されたコードキャラクタ情報画像を前記プログラムでデコードすることにより、店舗又は商品の識別情報を認識することとなる。また、前記プログラムは、携帯電話機内に設けることとしてもよく、この場合には、携帯電話機内でコードキャラクタ情報画像をデコードすることにより認識された前記各識別情報を、前記

30

40

認証サーバに送信することとなる。

以上のような外部入出力インタフェース17を使用することにより、入力部14の操作を行わずに店舗又は商品の識別情報の入力を行うことができる。ここで、商品の識別情報としては、商品名、商品種別、金額等が該当する。

なお、商品の金額を入力するのは、店員の金額入力に代わるものではなく、セルフスキヤニング行為を含むものであり、決済金額情報を購入者が事前に知るためのものである。

本実施形態の携帯電話機1には、図3(a)、(b)の正面図及び側面図に示すように、機器製造番号を図3(c)のようなバーコード31で記録した第1の標識19と、携帯電話番号をバーコード31で記録した第2の標識20が貼り付けられている。

これらの標識19、20のバーコードは、図4(a)に示すように、所定波長 λa の照射

50

光に対し記録情報を所定波長 λa または λb の反射光により出射する結晶粉末を混入した印刷材料で印刷されている。この結晶粉末は、米国SUNSTONE社が提供しているものであり、医薬品や紙幣の真贋識別用に採用されているものである。この場合、用途及び使用システムに応じて、照射光の波長と出射光の波長が異なるように特性が調整されている。

本発明では、このような特殊な結晶粉末を混入した記録インクまたはトナーで機器製造番号及び携帯電話番号のバーコードを標識19, 20に印刷し、これを携帯電話機1の正面あるいは側面に貼り付け、その標識19, 20に記録されたバーコードを所定波長 λa の照射光で読み取るようにしている。

このような特殊な記録インクまたはトナーで記録した機器製造番号及び携帯電話番号の標識19, 20を携帯電話機1に貼り付けておくことにより、予め定めた波長の照射光以外では機器製造番号及び携帯電話番号を読み取ることができない。よって、機器製造番号及び携帯電話番号を決済承認機関4に事前登録しておくことにより、当該携帯電話機1が本システムでの商取引を利用できる正当な機器であるか否かを識別することができる。また、側面の標識20は、携帯電話機1の改造を防止できる役目を果たしている。

なお、この場合には、必ずしも前記標識の貼り付けを必要とするものではなく、携帯電話機の筐体自体に、前記記録インク等により、前記標識を印刷することとしてもよい。

標識19, 20のバーコードは、図4(b)に示すような断面構成の読取装置40内に挿入され、予め定めた波長の照射光を照射することによって読み取られる。この読取装置40は、店舗2や自動販売機3に設置される。

一方、表示部11には図3(d)に示すようなコードキャラクタ情報画像としての2次元コード32で構成された決済承認鍵情報が表示される。この2次元コード32は、日本自動車工業会及び日本文具協会の標準コードに設定されているものである。これについては、例えば特開平10-214317号公報等で開示されているので、ここでの詳細な説明は省略する。

この2次元コード（以下、QRコードと言う）を用いれば、携帯電話機1の表示部の面積内で約7000文字（数字）をコード化して記録することができる。本発明では、このQRコードを決済承認鍵の情報を表現するために使用している。詳しくは、QRコードで構成された決済承認鍵の情報を携帯電話機1に転送して図3(a)のように表示部11に表示させ、この表示状態の携帯電話機1を標識19, 20の読取共用の読取装置21に挿入し、決済承認鍵の情報を読み取るようにしている。

QRコードを用いた場合、図3(d)に示すように、3ヶ所に配置した切り出しシンボル33~35によって360度のどの方向からでも記録内容を読み取ることができるので、読取部との位置関係の束縛がなくなり、一般の利用者が読み取り部に挿入して読み取らせる場合に好適である。また、位置関係を厳密に定める必要がないため、その分だけ読取時間も短縮することができる。さらに、コードの一部に汚れや破損があっても誤りを訂正できるので、読取ミスが減少する。特に本発明のように、携帯電話機1の表示部に表示させた状態で読み取らせる場合、表示部の汚れ等によって読取ミスが発生することが考えられるが、QRコードを用いることによって表示部の汚れ等に起因する読取ミスを減少させることができる。

図1に戻り、店舗2には標識19, 20とQRコードの読取共用の読取装置21が設置され、読み取った標識19, 20とQRコードをPOS端末で構成される店舗端末22に入力し、店舗端末で代金の決済を行うようになっている。自動販売機3にも標識19, 20とQRコードの読取共用の読取装置33が設置されている。

一方、承認機関4は、認証サーバ41と金融機関（銀行またはクレジット会社）42、店舗情報データベース(DB)43、利用者情報データベース(DB)44、購入履歴データベース(DB)45を備えている。

認証サーバ41は、携帯電話機1からの本人認証及び店舗認証要求に対して、本人認証及び店舗認証さらには金融機関42に対する与信照会を行い、予め登録してある本人および店舗であり、しかも金融機関42から与信OKの回答があった場合には商品の代金決裁を

携帯電話機 1 を使用して許可する処理を行うものであり、店舗登録処理プログラム 4 1 0、利用者登録処理プログラム 4 1 1、購入履歴管理プログラム 4 1 2、不正利用管理プログラム 4 1 3、認証処理プログラム 4 1 4、Q R 決済鍵生成プログラム 4 1 5、送受信プログラム 4 1 6 を備えている。なお、各データベース 4 3、4 4、4 5 のデータを暗号化して保存するための暗号化／複合化プログラムが必要に応じて組み込まれる。また、Q R コードを暗号化して送信するための暗号化プログラムおよび復号するための復号プログラムが組み込まれる。Q R コードを暗号化することにより、不正な取引をさらに困難にすることができる。

店舗登録処理プログラム 4 1 0 は、本システムを使用して決済を行う店舗（自動販売機やインターネット上の電子店舗を含む）を店舗情報 D B 4 3 に登録する際に使用するプログラムである。また、利用者登録処理プログラム 4 1 1 は本システムを使用して決済を行う利用者（商品購入者）を利用者情報 D B 4 4 に登録する際に使用するプログラムである。購入履歴管理プログラム 4 1 2 は、利用者（商品購入者）が購入した商品の購入履歴の情報を購入履歴 D B 4 5 に格納する際に使用するプログラムである。不正利用管理プログラム 4 1 3 は、店舗情報 D B 4 3 及び利用者情報 D B 4 4 に予め登録されていない店舗及び利用者が本システムにアクセスした場合、あるいは携帯電話機 1 の機器製造番号や電話番号を不正に書き換えてアクセスした場合の店舗識別番号あるいは携帯電話機 1 の機器製造番号や電話番号を不正利用情報データベース（図 9）に登録する際に使用するプログラムである。

認証処理プログラム 4 1 4 は、携帯電話機 1 からの本人認証及び店舗認証要求に対して、本人認証及び店舗認証さらには金融機関 4 2 に対する与信照会を行い、予め登録してある本人および店舗であり、しかも金融機関 4 2 から与信 O K の回答があった場合には商品の代金決済を携帯電話機 1 を使用して許可する処理を行うものである。

Q R 決済鍵生成プログラム 4 1 5 は、商品の代金決済を許可するために、Q R コードで構成された決済証明鍵の情報を生成して携帯電話機 1 に渡すプログラムである。Q R コードで構成された決済証明鍵の情報（以下、Q R 決済証明鍵情報）は、店舗が購入者本人及び店舗の認証結果を含む詳細な決済承認の情報を認証サーバ 4 1 から受け取るための鍵となる情報であり、本システムでこの Q R 決済証明鍵情報を店舗の読取装置 2 1 で読み取り、その読み取った Q R 決済証明鍵情報を店舗端末から認証サーバ 4 1 に送信することにより、店舗端末 2 2 では購入者本人及び店舗の認証結果を含む詳細な決済承認の情報を受け取ることができる。この場合、読取装置 2 1 で読み取った Q R 決済証明鍵情報が認証サーバ 4 1 で生成したものと異なる場合には決済承認の情報を取得することができない。

送受信プログラム 4 1 6 は、利用者および店舗からのアクセスに対し、決済に必要な情報を送受信するプログラムである。

図 6 は、店舗情報 D B の登録情報の一例を示すものであり、店舗 I D 6 0 1、店舗名称 6 0 2、住所 6 0 3、電話番号 6 0 4 が登録されるようになっている。

図 7 は、利用者情報 D B の登録情報の一例を示す図であり、利用者 I D 7 0 1、利用者名 7 0 2、住所 7 0 3、携帯電話製造番号（機器製造番号）7 0 4、携帯電話番号 7 0 5、本システムを利用する際の暗証番号 7 0 6、性別 7 0 7、生年月日 7 0 8、デビットカード番号 7 0 9、クレジットカード番号 7 1 0、W e b マネー口座番号 7 1 1、個人特徴情報 7 1 2 が登録されるようになっている。

W e b マネー口座番号 7 1 1 は、飲料水などの小額商品を自動販売機で購入する場合に W e b マネーによって決済する際に使用するものである。また、個人特徴情報 7 1 2 は、本人の写真等を登録しておき、店舗での決済時に店員が写真などの特徴によって本人確認を行えるようにするためのものであり、利用者本人の希望に応じて登録される。例えば、利用者本人の写真を登録しておけば、決済時に他人による悪用を店員が発見できるといふ利点がある。また、生年月日 7 0 8 により、未成年者であるか否かを発見でき、酒、煙草類の販売を差し止めることができる。この他に、運転免許証番号などを登録することができる。運転免許証番号などを登録しておくことによって、携帯電話機を利用して第三者である認証サーバ 4 1 から本人認証証明を発行することも可能である。

図 8 は、購入履歴 D B の格納情報の一例を示す図であり、利用日時 8 0 1、利用店舗名 8 0 2、決裁金額 8 0 3、今月分利用金額累計 8 0 4、サービスポイント累計 8 0 5、前回利用日 8 0 6 が格納されるようになっている。なお、この購入履歴情報は、利用者別に利用日時順に格納されるものである。

図 9 は、不正利用情報データベースに格納される情報の一例を示す図であり、不正利用者の携帯電話製造番号 9 0 1、携帯電話番号 9 0 2、店舗 I D 9 0 3 が登録されるようになっている。ここで、携帯電話番号 9 0 2 のみが登録されている場合は、携帯電話製造番号は正しいが、携帯電話番号の標識を改造してアクセスした者を意味する。また、店舗 I D 9 0 3 が登録されていない店舗は、本システムに未登録の店舗であるか、または店舗 I D を不正に書き換えている店舗を意味する。

ここで、悪意がない未登録の利用者および店舗については、アクセス時に登録を行うようにメッセージを送信し、複数回の登録案内を行ったにも拘わらず登録手続を行わないものについてのみ不正利用として登録するようにしてもよい。

以下、(1) スーパーマーケット等の一般の店舗で携帯電話機 1 を利用した商品購入時の決裁方法、(2) 自動販売機での商品購入時の決裁方法、(3) インタネット上の電子店舗での商品購入時の決裁方法についてフローチャートを参照して説明する。

図 1 0 及び図 1 1 は、スーパーマーケット等の一般の店舗で携帯電話機 1 を利用した商品購入時の決裁方法を示すフローチャートである。

まず、利用者(商品購入者)は、自分が所持する携帯電話機 1 をモバイルショッピングモードに設定した後、入力手段 1 4 を使用し、商品を購入しようとしている店舗の識別情報としての店舗 I D、自分の暗証番号(図 7 の 7 0 6 に登録した番号)、決裁方法、商品の購入金額を入力する(ステップ 1 0 0 1)。ここで、店舗又は商品の識別情報を、店舗内に設置されている発信機等から外部入出力インタフェース 1 7 を介して取り込むようにしてもよい。

また、決裁方法については、クレジットカード決裁、Web マネー決裁、デビットカード決裁があるが、クレジットカード決裁を選択した場合については支払い回数とクレジットカード番号を入力する。また、Web マネー決裁を選択した場合には Web マネー口座番号(図 7 の 7 1 1 に登録した番号)を入力する。同様に、デビットカード決裁を選択した場合にはデビットカード番号(図 7 の 7 0 9 に登録した番号)を入力する。なお、以下のフローチャートでは人間が行う操作はステップ 1 0 0 1 のように 2 重枠線で囲む形式で表記している。

入力が終了したならば、送信操作を行う。すると、ステップ 1 0 0 1 で入力した情報が Q R 決裁証明鍵発行要求として認証サーバ 4 1 に送信される。

この Q R 決裁証明鍵発行要求を受信した認証サーバ 4 1 は、店舗及び利用者の認証処理を行う(ステップ 1 0 0 2)。すなわち、Q R 決裁証明鍵発行要求の中に含まれる店舗 I D によって店舗情報 D B 4 3 を検索し、当該店舗 I D の店舗が登録されているか否かを調べる。同様に、暗証番号、クレジットカード番号(または Web マネー口座番号、デビットカード番号)によって利用者情報 D B 4 4 を検索し、当該暗証番号及びクレジットカード番号(または Web マネー口座番号、デビットカード番号)の利用者が利用者情報 D B 4 4 に登録されているか否かを調べる。その結果、店舗 I D が登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機 1 に返信する(ステップ 1 0 0 3)。また、暗証番号及びクレジットカード番号(または Web マネー口座番号、デビットカード番号)が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機 1 に返信する(ステップ 1 0 0 3)。携帯電話機 1 では、取引不可のメッセージが表示部 1 1 に表示されると共に、ステップ 1 0 0 1 で入力した店舗 I D 等の情報が自動消去される。

しかし、店舗 I D 及び暗証番号及びクレジットカード番号(または Web マネー口座番号、デビットカード番号)が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証 O K とする。

認証 O K となった場合には、認証サーバ 4 1 は金融機関 4 2 に対して利用限度額あるいは

残高の与信照会を送信する。そして、金融機関 4 2 における与信処理（ステップ 1 0 0 4）によって与信 O K または与信 N G の与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたは Q R 決裁証明鍵を生成する（ステップ 1 0 0 5）。すなわち、与信 N G の与信結果が返送されてきた場合には、認証サーバ 4 1 は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機 1 に送信する。しかし、与信 O K であった場合には、図 3（d）で示したような 2 次元コードで構成された Q R 決裁証明鍵を生成し（ステップ 1 0 0 6）、これを携帯電話機 1 に送信する。この Q R 決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。

携帯電話機 1 では、受信した Q R 決裁証明鍵を図 1 2（a）に符号 1 2 0 1 で示すように表示部 1 1 に表示する。同時に、例えば「この携帯電話機で決裁できます。代金決裁時に読取装置に挿入して下さい。」といったメッセージが表示される。

10

そこで、利用者は予め選択してあった購入希望商品を店舗端末 2 2 の店員に提示し、購入希望商品の発注を行う（ステップ 1 0 0 7）。店員は店舗端末によって購入希望商品の代金を入力する（ステップ 1 0 0 8）。

これと並行して、利用者は Q R 決裁証明鍵 1 2 0 1 が表示された状態の携帯電話機 1 を店舗端末 2 2 に付属した Q R コード読取装置 2 1 の読取部分に挿入装着する（ステップ 1 0 0 9）。すると、Q R コード読取装置 2 1 は、携帯電話機 1 の表示部 1 1 に表示された Q R 決裁証明鍵 1 2 0 1 を読み取ると共に（ステップ 1 0 1 1）、標識 1 9、2 0 から携帯電話製造番号と携帯電話番号を読み取り（ステップ 1 0 1 0）、その読取結果を店舗端末 2 2 に転送する。

20

店舗端末 2 2 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び Q R 決裁証明鍵 1 2 0 1 を決裁承認要求として認証サーバ 4 1 に送信する。この場合、Q R 決裁証明鍵 1 2 0 1 については、認証サーバ自身が発行したものであることが分かればよいので、決裁番号及び個人認証といった一部の情報のみを送信してもよい。図 1 1 では、決裁番号及び個人認証の情報のみを決裁承認要求の中に含ませて送信していることを示している。

認証サーバ 4 1 は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 D B 4 4 の登録内容と照合して調べる（ステップ 1 0 1 2）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図 9）に登録した後（ステップ 1 0 1 3）、不正利用メッセージを店舗端末 2 2 および携帯電話機 1 に送信する。

30

不正利用メッセージを受信した携帯電話機 1 では、不正利用メッセージ自体が Q R 決裁証明鍵 1 2 0 1 の消去コマンドとして機能し、表示部 1 1 に表示されていた Q R 決裁証明鍵 1 2 0 1 が消去される。

店舗端末 2 2 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ 1 0 1 4）。そして、店員により代金決裁ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末 2 2 から受信した Q R 決裁証明鍵 1 2 0 1 の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ 4 1 は詳細決裁承認を店舗端末 2 2 に返信する。この詳細決裁承認の情報には、Q R 決裁証明鍵 1 2 0 1 と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

40

詳細決裁承認を店舗端末 2 2 は、受信した詳細決裁承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ 1 0 1 5）。図 1 2（b）にその例を示している。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ 1 0 1 6）。

本人の購入意思の確定応答があったならば、決裁ボタン操作によって決裁を完了する（ステップ 1 0 1 7）。決裁ボタン操作が行われた場合は、店舗端末 2 2 は決裁終了メッセー

50

ジを認証サーバ41に送信する。この**決裁終了メッセージを受信した認証サーバ41は利用者の購入履歴情報を更新する（ステップ1018）**。この後、**確認用の決裁内容を携帯電話機1に送信する**。また、決裁終了情報を金融機関42に送信する。これにより、携帯電話機1の表示部11には、図13に示すような確認用の決裁内容1301が表示される。この決裁内容1301は、利用者自身が消去するまで保存することができる。ただし、QR決裁証明鍵1301は1回限り有効であるので、所定時間後に自動的に消去される。また、決裁終了情報を受信した金融機関42では利用者の指定口座から代金を引き落とす手続を行う。

以上により、携帯電話機1を使用して一般店舗での商品購入時の決裁を行うことができる

。なお、利用者が購入意思を撤回した場合に、店舗端末でのキャンセル操作によって店舗端末の処理は終了する。また、利用者自身が携帯電話機1でキャンセル操作を行った場合にも、決裁処理は途中で終了し、QR決裁証明鍵1301等の情報は全て消去される。 10

以上の説明から明らかなように、本取引方法によれば、店舗側に利用者のクレジット番号等の秘密情報を伝えることなく、認証サーバ41が発行したQR決裁証明鍵のみで代金決裁を行うことができる。また、携帯電話機1内にクレジットカード番号等の秘密情報を全く保持しない構成であるので、万一、携帯電話機1を紛失したとしても、代金決裁に悪用される危険性は全く生じない。さらに、特殊な結晶粉末を混入して記録した標識によって携帯電話製造番号と電話番号の正当性を判定しているため、携帯電話機自身の改造による悪用を防止することができ、決済に使用される機器のセキュリティ性を高めることにより、利用者および店舗の双方に有益な効果を発揮する。 20

さらに、店舗においては、読取装置21を付加するのみであるため、システムに加盟するに際してのコストが少なく済むという利点がある。同様に、携帯電話機1においても、ICカードなどを付加することなく市販の携帯電話機をそのまま利用することができる。さらに、購入履歴を管理しているため、店舗側においてはポイントカードを発行する必要がなくなる。また、利用者にとっても、利用状況が分かるので、計画的な購入計画を立てるのに役立つという利点がある。

また、QRコードを用いたことにより、360度のどの方向からでも記録内容を読み取ることができるので、読取部との位置関係の束縛がなくなり、一般の利用者が読み取り部に挿入して読み取らせる場合に好適である。また、位置関係を厳密に定める必要がないため、その分だけ読取時間も短縮することができる。さらに、コードの一部に汚れや破損があっても誤りを訂正できるので、読取ミスが減少する。特に本発明のように、携帯電話機1の表示部に表示させた状態で読み取らせる場合、表示部の汚れ等によって読取ミスが発生することが考えられるが、QRコードを用いることによって表示部の汚れ等に起因する読取ミスを減少させることができる。 30

なお、QR決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成されるものとしたが、決裁番号、個人認証、氏名の一部または全部を元に生成した1回限りのパスワードであってもよい。

この場合には、例えば、認証サーバ41と携帯電話機1とに、同一ロジックによるパスワード生成プログラムを備え、2回目にアクセスするときは、1回目に送信された暗証番号等に基づき自動生成されたパスワードを携帯電話機1から自動送信し、認証サーバ41側では、当該携帯電話機1の携帯電話番号等及び自動送信されたパスワードと、前記認証サーバ41で自動生成されたパスワードとを比較することにより、認証を行う。 40

3回目以降は、前回自動生成されたパスワードに基づき新たなパスワードを自動生成、自動送信することとしてもよい。

このような、いわゆるワンタイムパスワードと呼ばれるものを用いることにより、セキュリティ性を高めることができるとともに、2回目以降のアクセス時に、暗証番号の入力を省略することができる。

次に、自動販売機3から飲料水等の小額商品を購入する場合の決裁方法について図14及び図15のフローチャートを参照して説明する。

まず、利用者（商品購入者）は、自分が所持する携帯電話機1をモバイルショッピングモ 50

ードに設定した後、入力手段 14 を使用し、商品を購入しようとしている自動販売機 3 の店舗 ID、自分の暗証番号（図 7 の 706 に登録した番号）、決裁方法、商品の購入金額を入力する（ステップ 1401）。ここで、店舗又は商品の識別情報を、店舗内に設置されている発信機等から外部入出力インタフェース 17 を介して取り込むようにしてもよい。また、決裁方法については、クレジットカード決裁、Web マネー決裁、デビットカード決裁、非接触 IC カード決済があるが、小額決裁であるので、Web マネーを使用することとし、Web マネー口座番号（図 7 の 711 に登録した番号）を入力する。

入力が終了したならば、送信操作を行う。すると、ステップ 1401 で入力した情報が QR 決裁証明鍵発行要求として認証サーバ 41 に送信される。

この QR 決裁証明鍵発行要求を受信した認証サーバ 41 は、店舗（ここでは自動販売機）及び利用者の認証処理を行う（ステップ 1402）。すなわち、QR 決裁証明鍵発行要求の中に含まれる店舗 ID によって店舗情報 DB 43 を検索し、当該店舗 ID の店舗（自動販売機）が登録されているか否かを調べる。同様に、暗証番号、Web マネー口座番号によって利用者情報 DB 44 を検索し、当該暗証番号及び Web マネー口座番号の利用者が利用者情報 DB 44 に登録されているか否かを調べる。その結果、店舗 ID が登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 1403）。また、暗証番号及び web マネー口座番号が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 1403）。携帯電話機 1 では、取引不可のメッセージが表示部 11 に表示されると共に、ステップ 1401 で入力した店舗 ID 等の情報が自動消去される。 10

しかし、店舗 ID 及び Web マネー口座番号が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証 OK とする。

認証 OK となった場合には、認証サーバ 41 は金融機関 42 に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関 42 における与信処理（ステップ 1404）によって与信 OK または与信 NG の与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたは QR 決裁証明鍵を生成する（ステップ 1405）。すなわち、与信 NG の与信結果が返送されてきた場合には、認証サーバ 41 は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機 1 に送信する。しかし、与信 OK であった場合には、図 3（d）で示したような 2 次元コードで構成された QR 決裁証明鍵を生成し（ステップ 1406）、これを携帯電話機 1 に送信する。この QR 決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。 30

携帯電話機 1 では、受信した QR 決裁証明鍵を図 12（a）に符号 1201 で示したように表示部 11 に表示する。同時に、例えば「この携帯電話機で決裁できます。代金決裁時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は QR 決裁証明鍵 1201 が表示された状態の携帯電話機 1 を自動販売機 3 に付属した QR コード読取装置 33 の読取部分に挿入装着する（ステップ 1407）。そして、購入希望商品を自動販売機 3 の選択操作を行う（ステップ 1408）。自動販売機 3 では、購入希望商品の選択操作によって代金が自動的に確定する（ステップ 1409）。 40

QR コード読取装置 33 は、携帯電話機 1 の表示部 11 に表示された QR 決裁証明鍵 1201 を読み取ると共に（ステップ 1411）、標識 19、20 から携帯電話製造番号と携帯電話番号を読み取る（ステップ 1410）。

自動販売機 3 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び QR 決裁証明鍵 1201 を決裁承認要求として認証サーバ 41 に送信する。この場合の通信回線は、PHS 電話機を使用したデータ通信を利用することができる。図 15 では、決裁番号及び個人認証の情報のみを決裁承認要求の中に含ませて送信していることを示している。

認証サーバ 41 は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 DB 44 の登録内容と照合して調べる（ステップ 141 50

2)。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図9）に登録した後（ステップ1413）、不正利用メッセージを自動販売機3および携帯電話機1に送信する。

不正利用メッセージを受信した携帯電話機1では、不正利用メッセージ自体がQR決裁証明鍵1201の消去コマンドとして機能し、表示部11に表示されていたQR決裁証明鍵1201が消去される。

自動販売機3では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ1414）。しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも自動販売機3から受信したQR決裁証明鍵1201の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ41は詳細決裁承認を店舗端末22に返信する。この詳細決裁承認の情報には、QR決裁証明鍵1201と同様の情報の他に、当該利用者の購入履歴の情報が含まれている。

10

詳細決裁承認を受信した店舗端末22は、直ちに決裁処理を行う（ステップ1415）。そして、決裁終了メッセージを認証サーバ41に送信する。この決裁終了メッセージを受信した認証サーバ41は利用者の購入履歴情報を更新する（ステップ1416）。この後、確認用の決裁内容を携帯電話機1に送信する。また、決裁終了情報を金融機関42に送信する。これにより、携帯電話機1の表示部11には、図13に示したような確認用の決裁内容1301が表示される（ステップ1417）。

20

決裁終了メッセージを受信した金融機関42では利用者のWebマネー口座又はクレジット口座から代金を引き落とす手続を行う。

以上により、携帯電話機1を使用して自動販売機での小額商品購入時の決裁を行うことができる。

以上の説明から明らかなように、本取引方法においても、自動販売機側に利用者のクレジット番号等の秘密情報を伝えることなく、認証サーバ41が発行したQR決裁証明鍵のみで代金決裁を行うことができる。

次に、インターネット上の電子店舗での商品購入時の決裁方法について図16及び図17のフローチャートを参照して説明する。

まず、利用者（商品購入者）は、自分が所持する携帯電話機1をモバイルショッピングモードに設定した後、入力手段14を使用し、インターネット上の店舗にアクセスし、購入しようとしている商品の番号、購入金額、受取方法を入力し、商品の発注を行う（ステップ1601）。

30

商品の発注を受けた店舗は、認証サーバ41に対して個人認証依頼を送信する。この個人認証依頼を受信した認証サーバ41は、携帯電話機1に対して自分の暗証番号（図7の706に登録した番号）、決裁方法及び店舗IDの入力要求を送信する。

そこで、携帯電話機1の利用者が自分の暗証番号（図7の706に登録した番号）、決裁方法及び店舗IDを入力する（ステップ1602）。すると、その内容はQR決裁証明鍵発行要求として認証サーバ41に送信される。ここで、決裁方法については、前述の例と同様である。

40

このQR決裁証明鍵発行要求を受信した認証サーバ41は、利用者の認証処理を行う（ステップ1603）。すなわち、QR決裁証明鍵発行要求の中に含まれる店舗IDによって店舗情報DB43を検索し、当該店舗IDの店舗が登録されているか否かを調べる。同様に、暗証番号、クレジットカード番号（またはWebマネー口座番号、デビットカード番号）によって利用者情報DB44を検索し、当該暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）の利用者が利用者DB44に登録されているか否かを調べる。その結果、店舗IDが登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機1に返信する（ステップ1604）。また、暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）が登録されていなかった場合も、不正利用者であるか、未登

50

録の利用者であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 1 6 0 4）。携帯電話機 1 では、取引不可のメッセージが表示部 1 1 に表示されると共に、ステップ 1 6 0 2 で入力した店舗 I D 等の情報が自動消去される。

しかし、店舗 I D 及び暗証番号及びクレジットカード番号（または W e b マネー口座番号、デビットカード番号）が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証 O K とする。

認証 O K となった場合には、認証サーバ 4 1 は金融機関 4 2 に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関 4 2 における与信処理（ステップ 1 6 0 5）によって与信 O K または与信 N G の与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたは Q R 決裁証明鍵を生成する（ステップ 1 6 0 6）。すなわち、与信 N G の与信結果が返送されてきた場合には、認証サーバ 4 1 は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機 1 に送信する。しかし、与信 O K であった場合には、図 3（d）で示したような 2 次元コードで構成された Q R 決裁証明鍵を生成し（ステップ 1 6 0 7）、これを携帯電話機 1 に送信する。この Q R 決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。

携帯電話機 1 では、受信した Q R 決裁証明鍵を図 1 2（a）に符号 1 2 0 1 で示すように表示部 1 1 に表示する。同時に、例えば「この携帯電話機で決裁できます。お客様が指定した受取店舗での代金決裁時に読取装置に挿入して下さい。」といったメッセージが表示される。

また、認証サーバ 4 1 は、店舗に対して、受託証明の発行要求を送信する。この受託証明の発行要求を受信した店舗は、受託番号、利用者氏名、商品番号、金額、決裁方法、受取方法を含む受託証明を生成し、認証サーバ 4 1 に返信する。この受託証明は、利用者から見れば商品注文書に相当するものである。

受託証明を受信した認証サーバ 4 1 は、Q R 決裁証明鍵 1 2 0 1 と受託証明とを一体化し、Q R 決裁証明鍵付き受託証明として携帯電話機 1 に送信する。

そこで、利用者は自分が指定した受取店舗に赴き、Q R 決裁証明鍵付き受託証明を表示部 1 1 に表示させた状態で受取店舗の店舗端末 2 2 に付属した Q R コード読取装置 2 1 の読取部分に挿入装着する（ステップ 1 6 0 8）。すると、Q R コード読取装置 2 1 は、携帯電話機 1 の表示部 1 1 に表示された Q R 決裁証明鍵付き受託証明を読み取ると共に（ステップ 1 6 0 9）、標識 1 9, 2 0 から携帯電話製造番号と携帯電話番号を読み取り（ステップ 1 6 1 0）、その読取結果を店舗端末 2 2 に転送する。

店舗端末 2 2 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び Q R 決裁証明鍵付き受託証明を決裁承認要求として認証サーバ 4 1 に送信する。この場合、Q R 決裁証明鍵付き受託証明については、認証サーバ自身が発行したものであることが分かればよいので、決裁番号及び個人認証といった一部の情報のみを送信してもよい。図 1 7 では、決裁番号及び個人認証の情報のみを決裁承認要求の中に入れて送信していることを示している。

認証サーバ 4 1 は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 D B 4 4 の登録内容と照合して調べる（ステップ 1 6 1 1）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図 9）に登録した後（ステップ 1 6 1 3）、不正利用メッセージを店舗端末 2 2 および携帯電話機 1 に送信する。

不正利用メッセージを受信した携帯電話機 1 では、不正利用メッセージ自体が Q R 決裁証明鍵付き受託証明の消去コマンドとして機能し、表示部 1 1 に表示されていた Q R 決裁証明鍵付き受託証明が消去される。

店舗端末 2 2 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ 1 6 1 3）。そして、店員により商品の引渡し及び代金決裁ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末

22から受信したQR決裁証明鍵付き受託証明の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ41は詳細決裁承認を店舗端末22に返信する。この詳細決裁承認の情報には、QR決裁証明鍵1201と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決裁承認を受信した店舗端末22は、受信した詳細決裁承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ1614）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ1615）。

本人の購入意思の確定応答があったならば、商品を引き渡した上で、決裁ボタン操作によって決裁を完了する（ステップ1616）。決裁ボタン操作が行われた場合は、店舗端末22は決裁終了メッセージを認証サーバ41に送信する。この決裁終了メッセージを受信した認証サーバ41は利用者の購入履歴情報を更新する（ステップ1617）。この後、確認用の決裁内容を携帯電話機1に送信する。これにより、携帯電話機1の表示部11には、図13に示したような確認用の決裁内容1301が表示される。また、認証サーバ41は、決裁終了情報を金融機関42に送信する。 10

以上により、携帯電話機1を使用してインターネット上の店舗で商品を選択し、その商品を利用者自身が指定した受取店舗で受け取り、決裁することができる。

以上の説明から明らかなように、本取引方法によれば、インターネット上の店舗側に利用者のクレジット番号等の秘密情報を伝えることなく、認証サーバ41が発行したQR決裁証明鍵のみで代金決裁を行うことができる。 20

このような方法を利用すれば、例えばインターネット上で映画等のチケットを発注し、そのQR決裁証明鍵付き受託証明を携帯電話機1に格納しておき、映画館の入場口の読取装置に挿入することにより、チケットなしで入場するといった運用形態に活用することができる。

ここで、QR決裁証明鍵付き受託証明を表示部11に表示させて読取装置21に読み取らせる代わりに、QR決裁証明鍵付き受託証明をパーソナルコンピュータ（PC）に転送し、付属のプリンタで印刷し、受取店舗の読取装置で読み取らせる方法を採用することができる。この場合、プリンタの印字トナーまたはインクには、標識19、20と同様の結晶粉末が混入されたものを用いる。 30

図18は、その手順を示すフローチャートである。このフローチャートは、図16の続きに該当する。

まず、携帯電話機1でQR決裁証明鍵付き受託証明を受信したならば、そのQR決裁証明鍵付き受託証明をパーソナルコンピュータ（PC）に転送し（ステップ1620）、付属のプリンタで印刷する（ステップ1621）。図19（a）に印刷例を示す。

そこで、利用者は印刷されたQR決裁証明鍵付き受託証明を自分が指定した受取店舗に持参し、受取店舗の店舗端末22に付属したQRコード読取装置21の読取部分に挿入装着する。すると、QRコード読取装置21は、印刷されたQR決裁証明鍵付き受託証明を読み取り（ステップ1622）、その読取結果を店舗端末22に転送する。

店舗端末22は、印刷されたQR決裁証明鍵付き受託証明の読取結果を図17の場合と同様に決裁承認要求として認証サーバ41に送信する。 40

認証サーバ41は、決裁承認要求を受信したならば、まず、QR決裁証明鍵付き受託証明のQR決裁証明鍵が自分自身で発行した正規のものであるかの正当性を調べる（ステップ1623）。この結果、正当なものでない場合には、不正利用であるものと判断し不正利用情報データベース（図9）に登録した後（ステップ1624）、不正利用メッセージを店舗端末22および携帯電話機1に送信する。

不正利用メッセージを受信した携帯電話機1では、不正利用メッセージ自体がQR決裁証明鍵付き受託証明の消去コマンドとして機能し、表示部11に表示されていたQR決裁証明鍵付き受託証明が消去される。

店舗端末22では、不正利用メッセージを受けたことにより、表示部に不正利用者である 50

ことが表示され、処理が終了される（ステップ１６２５）。そして、店員により商品の引渡し及び代金決済ができない旨が利用者に口頭で通知される。

しかし、ＱＲ決済証明鍵が正当なものであると認められた場合には、認証サーバ４１は詳細決済承認を店舗端末２２に返信する。この詳細決済承認の情報には、ＱＲ決済証明鍵１２０１と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決済承認を受信した店舗端末２２は、受信した詳細決済承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ１６２６）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ１６２７）。

10

本人の購入意思の確定応答があったならば、商品を引き渡した上で、決済ボタン操作によって決済を完了する（ステップ１６２８）。決済ボタン操作が行われた場合は、店舗端末２２は決済終了メッセージを認証サーバ４１に送信する。この決済終了メッセージを受信した認証サーバ４１は利用者の購入履歴情報を更新する（ステップ１６２９）。この後、確認用の決済内容を携帯電話機１に送信する。これにより、携帯電話機１の表示部１１には、図１３に示したような確認用の決済内容１３０１が表示される。また、認証サーバ４１は、決済終了情報を金融機関４２に送信する。

以上により、携帯電話機１を持参しない場合でも、インターネット上の店舗で注文した商品を利用者自身が指定した受取店舗で受け取り、決済することができる。

この場合には、必ずしもＱＲ決済証明鍵付き受託証明を携帯電話機１からパーソナルコンピュータ（ＰＣ）に転送することは必要なく、直接にネットワーク端末としてのパーソナルコンピュータで受信して、プリンタで印刷することとしてもよい。

20

これら方法を利用すれば、印刷されたＱＲ決済証明鍵付き受託証明を、インターネット上で注文した例えば映画等のチケットの代わりに利用するといった運用形態に活用することができる。図１９（ｂ）に入場券の例を示す。

なお、前記各例では、商品の決済等に関する情報を発信するネットワーク端末と、ＱＲ決済証明鍵等のコードキャラクタ情報画像を受信するネットワーク端末として、同一の携帯電話機１を使用する場合を説明しているが、これに限られるものではなく、情報送信用のネットワーク端末と、コードキャラクタ情報画像受信用のネットワーク端末とを別の端末としてもよい。

30

これを利用することにより、第三者のネットワーク端末に対しコードキャラクタ情報画像を送信することもできる。従って、第三者に商品やギフト券を贈る代わりとして、第三者のネットワーク端末に送信したコードキャラクタ情報画像による決済を可能とすることができる。

以下、図２０～図２８参照して、この場合の決済処理方法を説明する。

この場合、前記決済処理機関４には、贈答情報データベース（ＤＢ）が備えられ、また、前記認証サーバ４１には贈答情報登録処理プログラム４１２が備えられることとなる。

前記贈答情報ＤＢは、例えば図２０に示すように、贈り手側ＩＤ２００１、受け手側ＩＤ２００２、贈答内容２００３、識別ＩＤ２００４、決済処理日２００５が格納されるようになっている。

40

また、前記贈答情報登録処理プログラムは、本システムを使用して特定の商品又は一定の金額の贈答を行う情報を贈答情報ＤＢに登録する際に使用するプログラムである。

本決済処理方法では、まず、注文主（商品の贈り手）は、情報送信用端末としての携帯電話機１をモバイルショッピングモードに設定した後、入力手段１４を使用し、自分の暗証番号（図７の７０６に登録した番号）、決済方法、商品の受取り手側の利用者名及び利用者ＩＤ等の受取り手情報、贈答内容（この場合には、贈りたい商品の商品番号）を入力する（ステップ２１０１）。ここで、決済方法については、前述の例と同様である。

入力が終了したならば、送信操作を行う。すると、ステップ２１０１で入力した情報が贈答情報送信要求として認証サーバ４１に送信される。

この贈答情報送信要求を受信した認証サーバ４１は、利用者の認証処理を行う（ステップ

50

2102)。すなわち、贈答情報送信要求の中に含まれる暗証番号、クレジットカード番号（またはWebマネー口座番号、デビットカード番号）によって利用者情報DB44を検索し、当該暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）の利用者が利用者情報DB44に登録されているか否かを調べる。また、受取り手情報としての利用者ID等によって、利用者情報DB44を検索し、その結果、暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機1に返信する（ステップ2103）。携帯電話機1では、取引不可のメッセージが表示部11に表示されると共に、ステップ2101で入力した暗証番号等の情報が自動消去される。

10

しかし、暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）、受取り手情報としての利用者ID、利用者名が正しく登録されていた場合には、正規登録の利用者であるものと認証し、認証OKとする。

認証OKとなった場合には、認証サーバ41は金融機関42に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関42における与信処理（ステップ2104）によって与信OKまたは与信NGの与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたは贈答情報の送信を行う（ステップ2105）。すなわち、与信NGの与信結果が返送されてきた場合には、認証サーバ41は、残高不足等のメッセージを含む取引不可メッセージを贈り手側の携帯電話機1に送信する。しかし、与信OKであった場合には、ステップ2101で入力された受取り手側の携帯電話機1に贈答情報を送信する。この贈答情報としては、図24（a）に示すように贈り手の利用者名及び贈答内容としての商品名等が表示され、受取り手側により、贈答内容の受取りについて、拒否又は受諾の情報が認証サーバ41に返信される（ステップ2106）。認証サーバ41は、この返信を受け、拒否の情報が返信された場合には、受取り手側の携帯電話機1にその旨の確認メッセージを送信するとともに、贈り手側の携帯電話機に受取り拒否のメッセージを送信した後（図24（c）参照）、ステップ2101で入力した暗証番号等の情報が自動消去される。（ステップ2107）。しかし、受諾の情報が返信された場合には、認証サーバ41は、受取り手側の携帯電話機1に対して、商品の受取り方法の入力要求を送信する（図24（b）参照）。

20

そこで、携帯電話機1の利用者が受取りの店舗ID及び受取り方法を入力する（ステップ2108）。すると、その内容はQR決済証明鍵発行要求として認証サーバ41に送信される。

30

このQR決済証明鍵発行要求を受信した認証サーバ41は、店舗の認証処理を行う（ステップ2109）。すなわち、QR決済証明鍵発行要求の中に含まれる店舗IDによって店舗情報DB43を検索し、当該店舗IDの店舗が登録されているか否かを調べる。その結果、店舗IDが登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを受取り手側の携帯電話機1に返信する（ステップ2110）。携帯電話機1では、取引不可のメッセージが表示部11に表示されたのを確認した後、別の店舗ID等を入力することとなる。

しかし、店舗IDが正しく登録されていた場合には、正規登録の店舗であるものと認証し、認証OKとする。

40

認証OKとなった場合には、認証サーバ41は、図3（d）で示したような2次元コードで構成されたQR決済証明鍵を生成する。（ステップ2211）このQR決済証明鍵は、少なくとも決済番号、個人認証、氏名、決済方法の情報を含むもので構成される。

また、認証サーバ41は、店舗に対して、受託証明の発行要求を送信する。この受託証明の発行要求を受信した店舗は、受託番号、利用者氏名、商品番号、金額、決済方法、受取方法を含む受託証明を生成し、認証サーバ41に返信する。この受託証明は、利用者から見れば商品注文書に相当するものである。

受託証明を受信した認証サーバ41は、QR決済証明鍵1201と受託証明とを一体化し、QR決済証明鍵付き受託証明として受取り手側の携帯電話機1に送信する。

50

携帯電話機 1 では、受信した Q R 決済証明鍵を前記図 1 2 に符号 1 2 0 1 で示すように表示部 1 1 に表示する。同時に、例えば「この携帯電話機で決済できます。代金決済時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は自分が指定した受取店舗に赴き、Q R 決済証明鍵付き受託証明を表示部 1 1 に表示させた状態で受取店舗の店舗端末 2 2 に付属した Q R コード読取装置 2 1 の読取部分に挿入装着する（ステップ 2 1 1 2）。すると、Q R コード読取装置 2 1 は、標識 1 9、2 0 から携帯電話製造番号と携帯電話番号を読み取ると共に（ステップ 2 1 1 3）、携帯電話機 1 の表示部 1 1 に表示された Q R 決済証明鍵付き受託証明を読み取り（ステップ 2 1 1 4）、その読取結果を店舗端末 2 2 に転送する。

店舗端末 2 2 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び Q R 決済証明鍵付き受託証明を決済承認要求として認証サーバ 4 1 に送信する。この場合、Q R 決済証明鍵付き受託証明については、認証サーバ 4 1 自身が発行したものであることが分かればよいので、決済番号及び個人認証といった一部の情報のみを送信してもよい。図 2 3 では、決済番号及び個人認証の情報のみを決済承認要求の中に含ませて送信していることを示している。

認証サーバ 4 1 は、決済承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 D B 4 4 の登録内容と照合して調べる（ステップ 2 1 1 5）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図 9）に登録した後（ステップ 2 1 1 6）、不正利用メッセージを店舗端末 2 2 および受取り手側の携帯電話機 1 に送信する。さらに、贈り手側の携帯電話機 1 にも不正利用メッセージが送信される。

不正利用メッセージを受信した携帯電話機 1 では、不正利用メッセージ自体が Q R 決済証明鍵付き受託証明の消去コマンドとして機能し、表示部 1 1 に表示されていた Q R 決済証明鍵付き受託証明が消去される。

店舗端末 2 2 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ 2 1 1 7）。そして、店員により商品の引渡し及び代金決済ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末 2 2 から受信した Q R 決済証明鍵付き受託証明の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ 4 1 は詳細決済承認を店舗端末 2 2 に返信する。この詳細決済承認の情報には、Q R 決済証明鍵 1 2 0 1 と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決済承認を受信した店舗端末 2 2 は、受信した詳細決済承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ 2 1 1 8）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ 2 1 1 9）。

本人の購入意思の確定応答があったならば、商品を引き渡した上で、決済ボタン操作によって決済を完了する（ステップ 2 1 2 0）。決済ボタン操作が行われた場合は、店舗端末 2 2 は決済終了メッセージを認証サーバ 4 1 に送信する。

この決済終了メッセージを受信した認証サーバ 4 1 は贈り手側の利用者の購入履歴情報を更新する（ステップ 2 1 2 1）。この後、確認用の決済内容を贈り手側の情報発信用端末に送信する。これにより、例えば、贈り手側の携帯電話機 1 の表示部 1 1 には、図 2 5 に示したような確認メッセージ及び決済内容 2 5 0 1、2 5 0 2 が表示される（ステップ 2 1 2 2）。また、認証サーバ 4 1 は、決済終了情報を金融機関 4 2 に送信する。

以上により、贈り手側端末を使用して、特定の商品を選択し、その商品を受取り手側が指定した店舗で受け取り、決済することができる。

以上の説明から明らかなように、本取引方法によれば、店舗側や贈答品の受取り手側に贈り手のクレジット番号等の秘密情報を伝えることなく、認証サーバ 4 1 が発行した Q R 決

済証明鍵のみで代金決済を行うことができる。また、贈答品の受取り手の認証をより確実に行うことができる。

なお、本取引方法では、受取り手側に対し贈答情報を送信し、贈答を受諾するか否かを選択することとしているが、予め贈答を受諾又は拒否する者を設定しておき、認証サーバにおいて、この設定に基づき贈答を受諾するか拒否するかの判定を行うこととしてもよい。この場合には、ステップ 2106 及びステップ 2107 に代えて、認証サーバにおける前記判定処理が行われることとなる。

また、このシステムにより贈られる贈答内容としては、特定の商品に限られず、一定金額のギフト券に相当する内容としてもよい。

図 26 及び図 27 は、その場合の手順を示すフローチャートである。図 26 のフローチャートは、図 21 の続きに該当する。 10

この場合には、前提として、図 21 のステップ 2101 において、贈答内容として商品番号に代えて一定の金額を入力することとなる。

その後、図 21 のフローチャートに示す処理がされた後、受取り手側の利用者が受取りの店舗 ID 及び商品の購入金額を入力する（ステップ 2130）。すると、その内容は QR 決済証明鍵発行要求として認証サーバ 41 に送信される。

この QR 決済証明鍵発行要求を受信した認証サーバ 41 は、店舗及び購入金額の認証処理を行う（ステップ 2131）。すなわち、QR 決済証明鍵発行要求の中に含まれる店舗 ID によって店舗情報 DB 43 を検索し、当該店舗 ID の店舗が登録されているか否かを調べる。また、贈答情報 DB を検索し、入力された購入金額が、当該 DB に格納された金額の範囲内であるかを調べる。その結果、店舗 ID が登録されていなかった場合又は購入金額が贈答金額を超えている場合は、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 2132）。受取り手側の携帯電話機 1 では、取引不可のメッセージが表示部 11 に表示されたのを確認した後、別の店舗 ID 又は購入金額を入力することとなる。しかし、店舗 ID が正しく登録されており、かつ、贈答金額の範囲内で購入金額が入力されていた場合には、正規登録の店舗で購入可能な金額であるものと認証し、認証 OK とする。 20

認証 OK となった場合には、認証サーバ 41 は、図 3（d）で示したような 2 次元コードで構成された QR 決済証明鍵を生成し、携帯電話機 1 に送信する（ステップ 2133）。この QR 決済証明鍵は、少なくとも決済番号、個人認証、氏名、決済方法の情報を含むもので構成される。 30

携帯電話機 1 では、受信した QR 決済証明鍵を図 12（a）に符号 1201 で示すように表示部 11 に表示する。同時に、例えば「この携帯電話機で決済できます。代金決済時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は予め選択してあった購入希望商品を店舗端末 22 の店員に提示し、購入希望商品の発注を行う（ステップ 2134）。店員は店舗端末によって購入希望商品の代金を入力する（ステップ 2135）。

これと並行して、利用者は QR 決済証明鍵 1201 が表示された状態の携帯電話機 1 を店舗端末 22 に付属した QR コード読取装置 21 の読取部分に挿入装着する（ステップ 2136）。すると、QR コード読取装置 21 は、受取り手側の携帯電話機 1 の表示部 11 に表示された QR 決済証明鍵 1201 を読み取ると共に（ステップ 2137）、標識 19、20 から携帯電話製造番号と携帯電話番号を読み取り（ステップ 2138）、その読取結果を店舗端末 22 に転送する。 40

店舗端末 22 は、受取り手側の携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び QR 決済証明鍵 1201 を決済承認要求として認証サーバ 41 に送信する。この場合、QR 決済証明鍵 1201 については、認証サーバ自身が発行したものであることが分かればよいので、決済番号及び個人認証といった一部の情報のみを送信してもよい。

認証サーバ 41 は、決済承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 DB 44 の登録内容と照合して調べる（ステップ 2139）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる 50

場合には、不正利用であるものと判断し不正利用情報データベース（図 9）に登録した後（ステップ 2140）、不正利用メッセージを店舗端末 22 および受取り手側の携帯電話機 1 に送信する。さらに、贈り手側の携帯電話機 1 にも不正利用メッセージが送信される。

不正利用メッセージを受信した受取り手側の携帯電話機 1 では、不正利用メッセージ自体が QR 決済証明鍵 1201 の消去コマンドとして機能し、表示部 11 に表示されていた QR 決済証明鍵 1201 が消去される。

店舗端末 22 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ 2141）。そして、店員により代金決済ができない旨が利用者に口頭で通知される。

10

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末 22 から受信した QR 決済証明鍵 1201 の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ 41 は詳細決済承認を店舗端末 22 に返信する。この詳細決済承認の情報には、QR 決済証明鍵 1201 と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決済承認を店舗端末 22 は、受信した詳細決済承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ 2142）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ 2143）。

本人の購入意思の確定応答があったならば、決済ボタン操作によって決済を完了する（ステップ 2144）。決済ボタン操作が行われた場合は、店舗端末 22 は決済終了メッセージを認証サーバ 41 に送信する。この決済終了メッセージを受信した認証サーバ 41 は贈り手側の利用者の購入履歴情報を更新する（ステップ 2145）。この後、確認用の決済内容を贈り手側の携帯電話機 1 に送信する。また、決済終了情報を金融機関 42 に送信する。これにより、例えば、贈り手側の携帯電話機 1 の表示部 11 には、図 25 に示すような確認用の決済内容 2501、2502 が表示される（ステップ 2146）。この決済内容 2501、2502 は、利用者自身が消去するまで保存することができる。ただし、QR 決済証明鍵 1201 は 1 回限り有効であるので、所定時間後に自動的に消去される。

20

また、決済終了情報を受信した金融機関 42 では贈り手側の利用者の指定口座から代金を引き落とす手続を行う。

30

以上により、贈り手側端末を使用して、一定の金額を指定し、その金額の範囲内で受取り手側が自由に商品等を店舗で購入して、決済することができる。

以上の説明から明らかなように、本取引方法によれば、一定金額のギフト券に相当する内容を贈る場合であっても、店舗側や受取り手側に贈り手のクレジット番号等の秘密情報を伝えることなく、認証サーバ 41 が発行した QR 決済証明鍵のみで贈り手側の口座から代金決済を行うことができる。また、受取り手の認証をより確実に行うことができる。

また、前記各例では、金融機関による決済を前提としているが、決済代金の一部又は全部についてサービスポイントによる決済を行う場合にも、本発明を利用することができる。

以下、図 28～図 30 を参照して、この場合の決済処理方法を説明する。

この場合、前記決済処理機関 4 には、サービスポイントデータベース（DB）が備えられ、また、前記認証サーバ 41 にはサービスポイント登録処理プログラムが備えられることとなる。

40

図 28 は、サービスポイント DB の格納情報の一例を示す図であり、更新日 2801、利用店舗名 2802、加算ポイント数 2803、利用ポイント数 2804、サービスポイント残高 2805 が格納されるようになっている。このサービスポイント情報は、利用者別に更新日時順に格納されるものである。

また、サービスポイント登録処理プログラムは、本システムを使用して商品の購入等を行うことにより得たサービスポイントに基づき、決済処理を行うものである。

なお、ここでサービスポイントの利用としては、ポイント数により商品購入時に一定金額相当の割引をして決済処理する場合、ポイント数に応じて予め決められた商品と交換する

50

場合等があるが、本実施の形態では、サービスポイントを商品購入代金として決済処理する場合を示している。

本決済処理方法では、まず、利用者（商品購入者）は、携帯電話機 1 をモバイルショッピングモードに設定した後、入力手段 14 を使用し、商品を購入しようとしている店舗の店舗 ID、自分の暗証番号（図 7 の 706 に登録した番号）、商品の購入金額に相当するサービスポイントを入力する（ステップ 2901）。ここで、店舗又は商品の識別情報を、店舗内に設置されている発信機等から外部入出力インタフェース 17 を介して取り込むようにしてもよい。

入力が終了したならば、送信操作を行う。すると、ステップ 2901 で入力した情報が QR 決済証明鍵発行要求として認証サーバ 41 に送信される。

10

この QR 決済証明鍵発行要求を受信した認証サーバ 41 は、店舗及び利用者の認証処理を行う（ステップ 2902）。すなわち、QR 決済証明鍵発行要求の中に含まれる店舗 ID によって店舗情報 DB 43 を検索し、当該店舗 ID の店舗が登録されているか否かを調べる。同様に、暗証番号によって利用者情報 DB 44 を検索し、利用者が利用者情報 DB 44 に登録されているか否かを調べる。その結果、店舗 ID が登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 2903）。また、暗証番号が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 2903）。携帯電話機 1 では、取引不可のメッセージが表示部 11 に表示されると共に、ステップ 2901 で入力した店舗 ID 等の情報が自動消去される。

20

しかし、店舗 ID 及び暗証番号が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証 OK とする。

認証 OK となった場合には、当該利用者のサービスポイント DB を検索し、サービスポイント残高の照会を行う（ステップ 2904）。そして、この照会結果に応じて、取引不可メッセージまたは QR 決済証明鍵を生成する（ステップ 2905）。すなわち、照会の結果残高無しとされた場合には、認証サーバ 41 は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機 1 に送信する。しかし、残高有りであった場合には、図 3（d）で示したような 2 次元コードで構成された QR 決済証明鍵を生成し（ステップ 2906）、これを携帯電話機 1 に送信する。この QR 決済証明鍵は、少なくとも決済番号、個人認証、氏名の情報を含むもので構成される。

30

携帯電話機 1 では、受信した QR 決済証明鍵を図 12（a）に符号 1201 で示すように表示部 11 に表示する。同時に、例えば「この携帯電話機で決済できます。代金決済時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は予め選択してあった購入希望商品を店舗端末 22 の店員に提示し、購入希望商品の発注を行う（ステップ 2907）。店員は店舗端末に購入希望商品の代金を入力することにより、この代金に相当するポイント数を算出する（ステップ 2908）。

これと並行して、利用者は QR 決済証明鍵 1201 が表示された状態の携帯電話機 1 を店舗端末 22 に付属した QR コード読取装置 21 の読取部分に挿入装着する（ステップ 2909）。すると、QR コード読取装置 21 は、携帯電話機 1 の標識 19、20 から携帯電話製造番号と携帯電話番号を読み取ると共に（ステップ 2910）表示部 11 に表示された QR 決済証明鍵 1201 を読み取り（ステップ 2911）、その読取結果を店舗端末 22 に転送する。

40

店舗端末 22 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び QR 決済証明鍵 1201 を決済承認要求として認証サーバ 41 に送信する。この場合、QR 決済証明鍵 1201 については、認証サーバ自身が発行したものであることが分かればよいので、決済番号、個人認証といった一部の情報のみを送信してもよい。図 30 では、決済番号及び個人認証の情報のみを決済承認要求の中に含ませて送信していることを示している。

認証サーバ 41 は、決済承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 DB 44 の登録内容と照合して調べる（ステップ 291

50

2)。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図11）に登録した後（ステップ2913）、不正利用メッセージを店舗端末22および携帯電話機1に送信する。

不正利用メッセージを受信した携帯電話機1では、不正利用メッセージ自体がQR決済証明鍵1201の消去コマンドとして機能し、表示部11に表示されていたQR決済証明鍵1201が消去される。

店舗端末22では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ2914）。そして、店員により代金決済ができない旨が利用者に口頭で通知される。

10

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末22から受信したQR決済証明鍵1201の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ41は詳細決済承認を店舗端末22に返信する。この詳細決済承認の情報には、QR決済証明鍵1201と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決済承認を店舗端末22は、受信した詳細決済承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ2915）。店員は、その表示内容で購入希望商品の内容及び代金に相当するポイント数を見て、利用者本人に購入意思を確認する（ステップ2916）。

20

本人の購入意思の確定応答があったならば、決済ボタン操作によって決済を完了する（ステップ2917）。決済ボタン操作が行われた場合は、店舗端末22は決済終了メッセージを認証サーバ41に送信する。この決済終了メッセージを受信した認証サーバ41は利用者の購入履歴情報及びサービスポイント情報を更新する（ステップ2918）。この後、確認用の決済内容を携帯電話機1に送信する。この決済内容は、利用者自身が消去するまで保存することができる。ただし、QR決済証明鍵1201は1回限り有効であるので、所定時間後に自動的に消去される。

以上により、携帯電話機1を使用して、一般店舗での商品購入時にサービスポイントを利用した決済を行うことができる。

以上の説明から明らかなように、本取引方法によれば、サービスポイントを利用した決済においても、認証サーバ41が発行したQR決済証明鍵のみで行うことができ、ポイントカード等を不要とすることができる。また、サービス利用者の認証をより確実に行うことができる。

30

以上の各例で示した方法は、金銭的な決済を介することを必須とするものではなく、入場券等のチケットの代わりや、商品等の受取証の代わりに用いることも可能なものである。なお、上記で説明した手順は、金融機関等の関係で一部の手順を変更して実施することができる。また、認証サーバ41が実行する手順は決済用のプログラムとしてCD-ROM等の記録媒体に記録して決済システム構築事業者に提供することができる。

また、携帯電話製造番号及び携帯電話番号の標識は、特殊な結晶粉末を混入した記録材料で記録しているが、これ以外に物理的に真偽判定が可能な記録形式で記録する方法であってもよい。

40

なお、ICカード（UIMカード）を搭載した携帯電話機等を用いる次世代移動通信サービスでは、携帯電話番号等を前記ICカードに書き込み、ICカードの差し替えにより、異なる端末で同一の携帯電話番号の使用をするといった運用形態が考えられている。

そこで、この場合には、前記ICカードに前記図3（c）に示すような標識を貼り付け又は印刷することとしてもよい。

また、この場合には、携帯電話機等に設けられたスロット等にICカードを差し込んだ状態で、前記標識を外部の読取装置で読取り可能とすることが必要となる。

この場合に用いられる携帯電話機の例を図31、32を参照して説明する。

図31、32は本実施の形態に用いられる携帯電話機の部分斜視図であり、各図において 50

、３００は携帯電話機に搭載される携帯電話番号等の情報を保存したＩＣカードであり、その表面には、前記図３（ｃ）に示すような標識３１１が貼り付けまたは印刷されている。なお、この標識３１１には、携帯電話機の製造番号に代えて、各ＩＣカード又は所有者の識別情報が携帯電話番号とともに記録されている。

本実施の形態では、例えば、図３１（ａ）に示すように、携帯電話機１の裏面側等において、ＩＣカードに貼り付けされた標識３１１が図の矢印に示す読取方向から視認可能なように、ＩＣカードを取り付け可能とする凹部３００を形成する。これにより、携帯電話機１の筐体に標識を貼り付けた場合と同様に、前記読取装置２２により、読取りが可能となる。

また、図３１（ｂ）に示すように、携帯電話機１に設けられたＩＣカード差込用スロット３０１を設けるとともに、当該スロット３０１にＩＣカード３１０が差し込まれた状態で、前記標識３１１が位置する部位に、外部の読取り装置から当該標識が読取（視認）可能となるような開口部３０２を形成することとしてもよい。この開口部３０２は、図の矢印に示す読取方向から前記標識３１１が視認可能であれば、透過性の樹脂材等により、その表面側をシールドしてもよい。

また、外部の読取装置により前記標識３１１が読取可能であれば、他の構成を用いてもよく、例えば、携帯電話機の筐体全体を内部が視認可能な透過性の樹脂材等により形成することとしてもよい。

これにより、次世代移動通信サービスに対応した携帯電話機等においても、本発明を適用することができるとともに、ＩＣカード内にクレジットカード番号等のデータを保存する必要がなくなり、セキュリティ性を高くすることができる。

なお、携帯電話機１において、前記標識３１１の読取装置を設け、その読取装置により前記標識を読取り、その読取情報を店舗側端末に送信することとしてもよい。

この場合には、例えば、図３２（ａ）に示すように、前記スロット３０１に差し込まれたＩＣカードの標識３１１が位置する部位に、前記制御部１３（図２（ａ）参照）に接続された読取センサ部３０３を設ける。これにより、当該読取センサ部３０３で読取った標識３１１の情報を携帯電話機１の送信手段を介して、前記認証サーバ４１に送信することができる。なお、標識３１１の情報の読取処理を、前記スロット３１１にＩＣカードを差し込む途中で行うこととしてもよく、この場合には、前記スロット内において前記標識３１１が通過する部位に対応する部位の一部にセンサ部を設けることとしてもよい。

また、ＩＣカード３１０を携帯電話機１に差し込むものに限らず、図３２（ｂ）に示すように、ＩＣカード３１０の一部を、携帯電話機１の側面に形成されたスリット３０４に挿入した状態で、図の矢印に示すスライド方向にスライドさせることで、図外のセンサ部により、ＩＣカード３１０内の情報を読取らせるものが考えられる。この場合には、ＩＣカード３１０の一部を前記スリット３０４内をスライドさせる際に、前記スリット３０４内において前記標識３１１が通過する部位に対応する部位の一部に、読取センサ部３０５を設けることとしてもよい。

また、ＩＣカード３１０として、無線または光による非接触型ＩＣカードを用いる場合には、各店舗等に設置された読取装置にＩＣカード３１０を挿入することにより、標識３１１を直接読取らせることとしてもよく、また、前記の例と同様に、携帯電話機１に読取装置を備えることとしてもよく、また、ＩＣカード３１０内の情報と同様に、無線又は光により、前記標識３１１の情報を認識させることとしてもよい。

【図面の簡単な説明】

第１図は、本発明の商取引方法を実施するシステムの実施形態を示すシステム構成図である。

第２図は、携帯電話機の構成を示す概略ブロック図である。

第３図は、携帯電話機に付けられる標識とバーコードおよび２次元コードの例を示す図である。

第４図は、携帯電話機に付けられたバーコードおよび表示部に表示された２次元コードを読み取る読取装置の断面構成図である。

第 5 図は、認証サーバの内部構成図である。

第 6 図は、店舗情報データベースに格納されるデータの一例を示す図である。

第 7 図は、利用者情報データベースに格納されるデータの一例を示す図である。

第 8 図は、購入履歴データベースに格納されるデータの一例を示す図である。

第 9 図は、不正利用情報データベースに格納されるデータの一例を示す図である。

第 10 図は、携帯電話機を用いて一般店舗で商品代金を決済する手順を示すフローチャートである。

第 11 図は、第 10 図の続きを示すフローチャートである。

第 12 図は、携帯電話機に表示される QR 決済証明鍵と店舗端末に表示される利用者情報の例を示す図である。

10

第 13 図は、決済終了時に携帯電話機に表示される確認用の情報例を示す図である。

第 14 図は自動販売機で小額商品の決済を行う場合の手順を示すフローチャートである。

第 15 図は第 14 図の続きを示すフローチャートである。

第 16 図は、インターネット上の店舗で注文した商品を指定の受取店舗で受け取って決済する場合の手順を示すフローチャートである。

第 17 図は、第 16 図の続きを示すフローチャートである。

第 18 図は、QR 決済証明鍵を印刷したものを店舗に持参して決済する場合の手順を示すフローチャートである。

第 19 図は、QR 決済証明鍵を印刷した例を示す図である。

第 20 図は、贈答情報データベースに格納されるデータの一例を示す図である。

20

第 21 図は、他人への贈答品の決済をする場合の手順を示すフローチャートである。

第 22 図は、図 21 の続きを示すフローチャートである。

第 23 図は、図 22 の続きを示すフローチャートである。

第 24 図は、携帯電話機に表示される贈答情報の表示例及び受諾又は拒絶の選択後の表示例を示す図である。

第 25 図は、決済終了時に贈り手側の携帯電話機に表示される確認用の情報例を示す図である。

第 26 図は、図 21 の続きを示すフローチャートである。

第 27 図は、図 26 の続きを示すフローチャートである。

第 28 図は、サービスポイント利用履歴データベースの一例を示す図である。

30

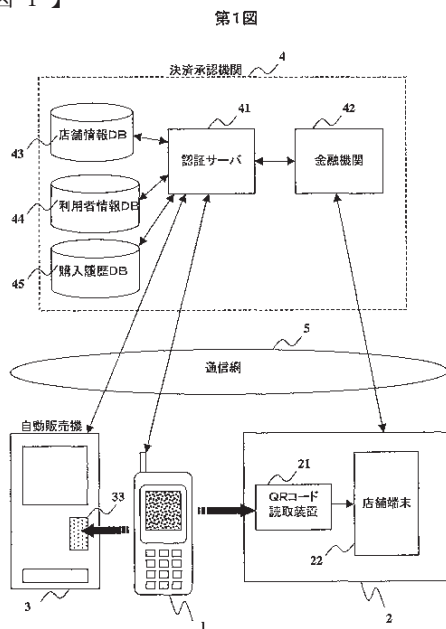
第 29 図は、携帯電話機を用いて一般店舗でサービスポイントにより決済する手順を示すフローチャートである。

第 30 図は、図 29 の続きを示すフローチャートである。

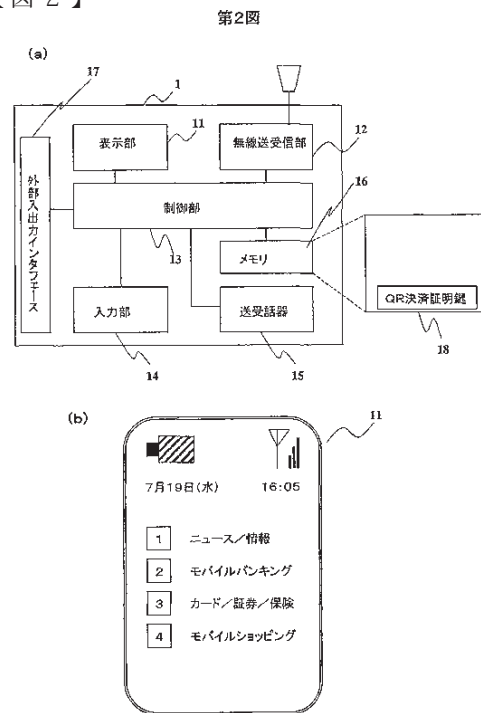
第 31 図は、本発明に用いられる携帯電話機の一部を示す部分斜視図である。

第 32 図は、本発明に用いられる携帯電話機の一部を示す部分斜視図である。

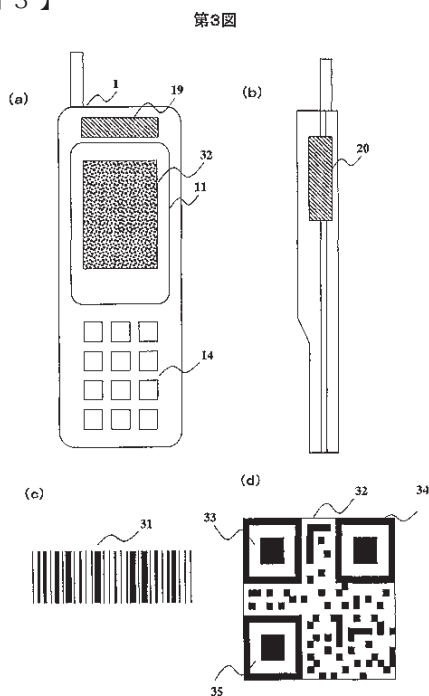
【図 1】



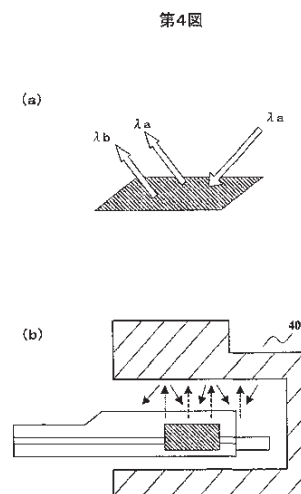
【図 2】



【図 3】

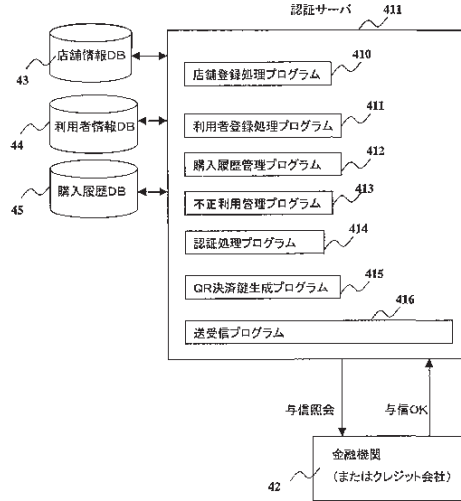


【図 4】



【図5】

第5図



【図6】

第6図

店舗情報データベース			
店舗ID	店舗名称	住所	電話番号
AA001	ABデパート	東京都中央区XX街1-2-1	03-3221-XXXX
AA002	XYスーパー	東京都目黒区XX街6-3-4	03-3332-XXXX
AB199	AF自動販売機	東京都品川区YR街3-1-1	03-4521-XXXX

【図7】

第7図

利用者情報データベース				
利用者ID	利用姓名	住所	携帯電話番号	暗証番号
UR001	木村XX	東京都中央区XX街5-2	MMA-B124	090-3221-XXXX 4123
UR002	田中XX	東京都目黒区XX街3-1	MMA-B125	090-3332-XXXX 9198
UR199	佐藤XX	東京都品川区YR街1-1	MMA-B993	090-4521-XXXX 0678

性別	生年月日	クレジットカード番号	Webメールアドレス番号	個人特性情報
男	1960/05/05	ABC銀行123899	NNM23567	WMNB578
				手帳ID4567

【図8】

第8図

購入履歴データベース				
利用日時	利用店舗名	決済金額	今月分利用金額累計	サービスポイント累計
000712	ABスーパー	¥6500	¥16500	165P
000713	ABスーパー	¥3130	¥19630	196P
000714	AZデパート	¥4520	¥24150	341P
				000713

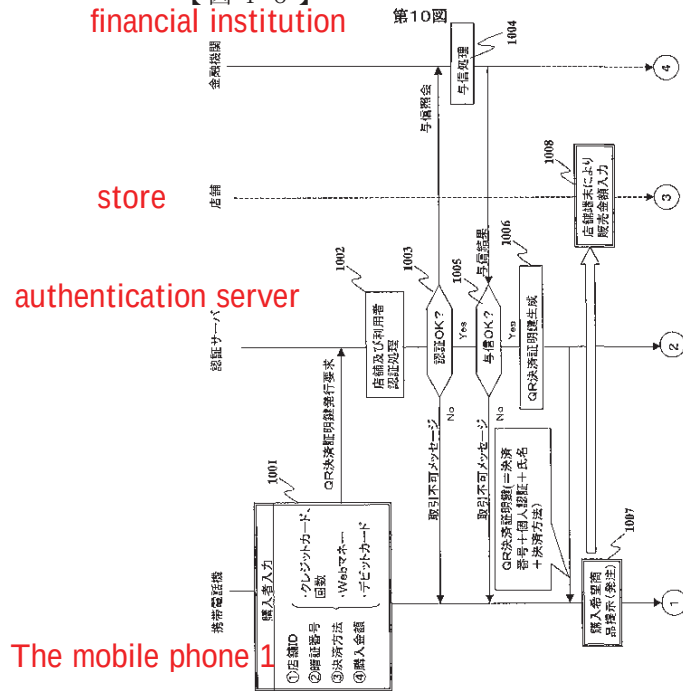
【図9】

不正利用情報データベース

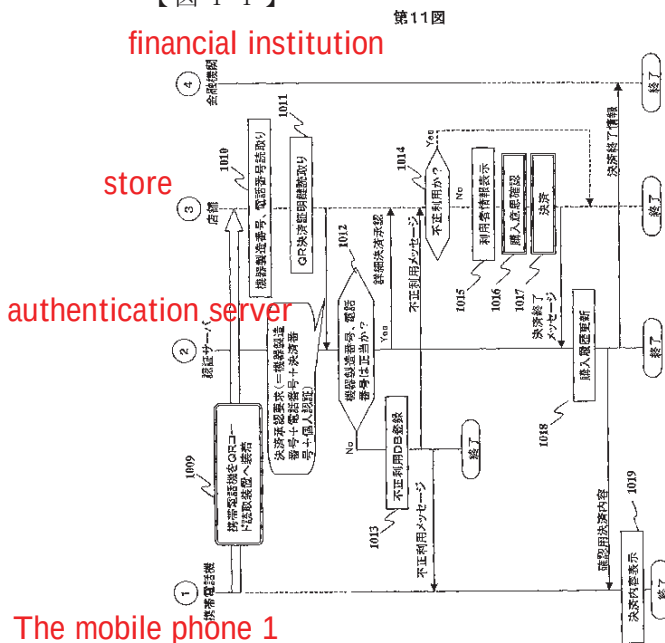
携帯電話番号	901	携帯電話番号	902	店番号	903
090-123999XX		090-123999XX		---	
NNMM4567		090-113599XX		---	
---		---		---	BB008

図9

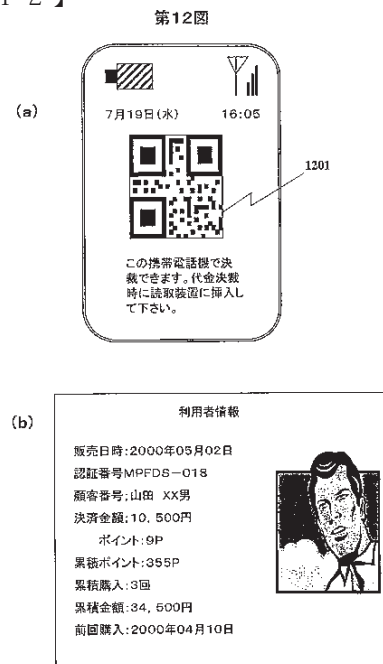
【図10】



【図11】

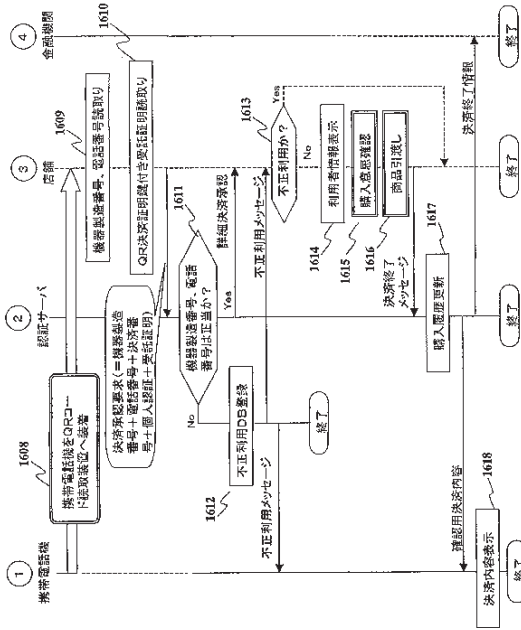


【図12】



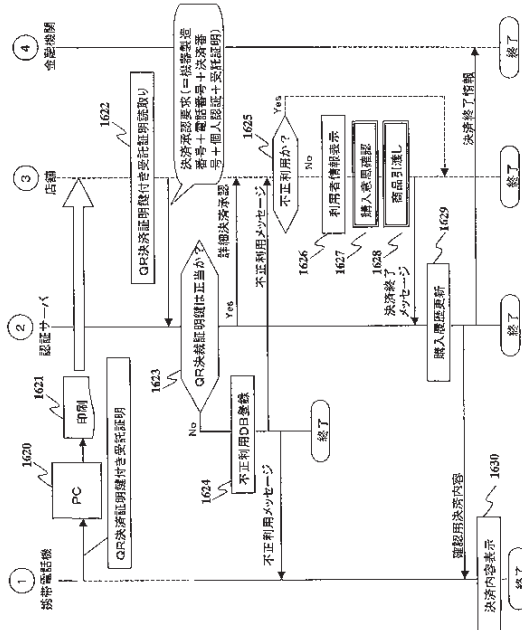
【図 17】

第17図



【図 18】

第18図



【図 19】

第19図

(a)

受託証明

1. 商品番号
2. お客様氏名
3. 金額
4. 決済方法
5. 受取場所

(b)

入場券

1. 商品番号
2. お客様氏名
3. 金額
4. 決済方法
5. 受取場所

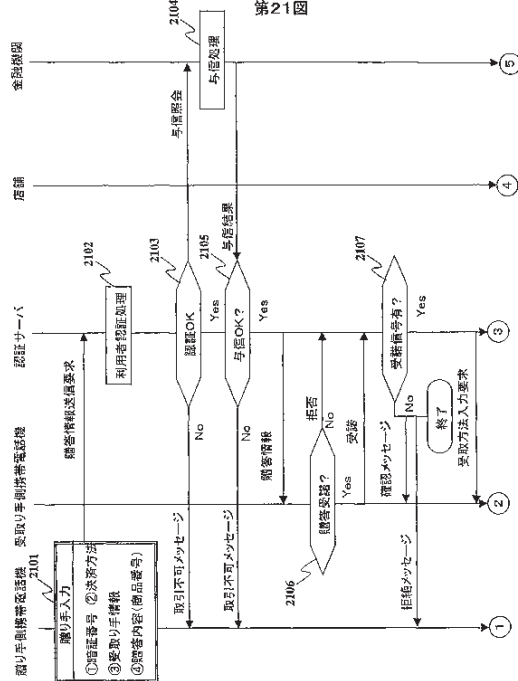
【図 20】

第20図

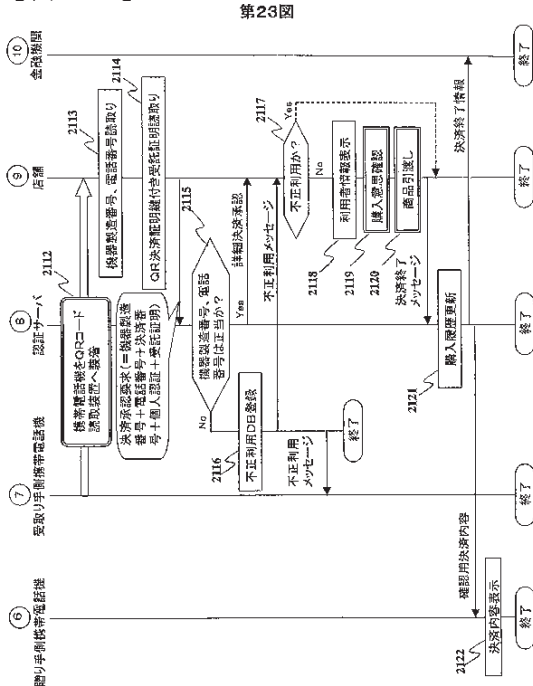
報告情報データベース

2001	2002	2003	2004	2005
送付手続ID	取引手続ID	顧客内容	取引ID	決済処理日
UR011	UR085	0000	P9856	00/07/16
UR045	UR179	¥ 10,000	P5875	00/07/20
UR135	UR034	0000	P2498	-

【 図 2 1 】

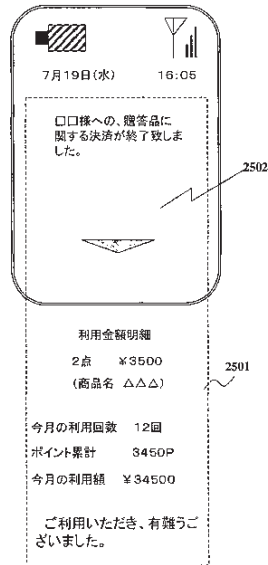


【图 2 3】



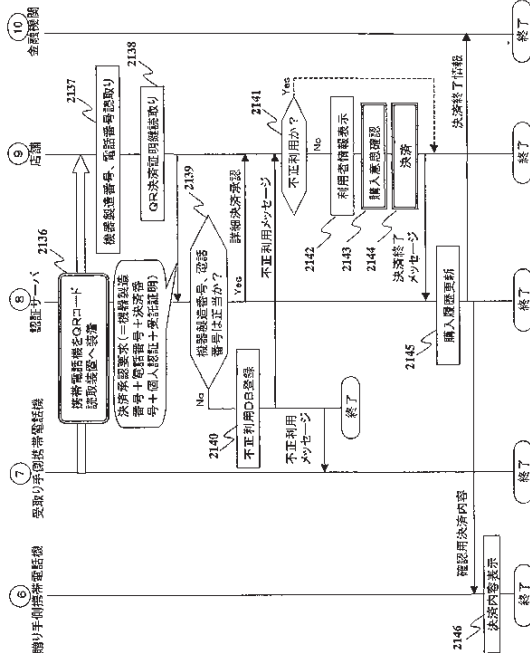
【图 2 5】

第25図



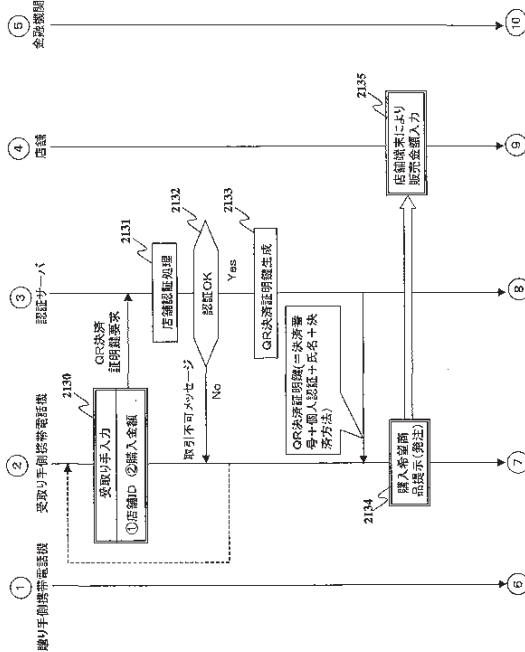
【図 27】

第27図



【图 2 6】

第26圖



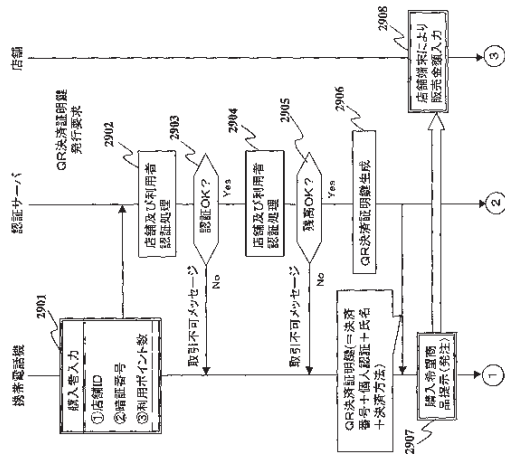
【図 28】

第28圖

2801	2802	2803	2804	2805
変更日	利用西暦名	加算ポイント数	利用ポイント数	サブポイント数
0000712	ABスーパー	65P	—	165P
0000713	ABスーパー	31P	—	166P
—	—	—	—	—
—	—	—	—	—
—	—	—	—	—
0000714	AZデパート	45P	—	341P
0000715	BCデパート	—	200P	141P

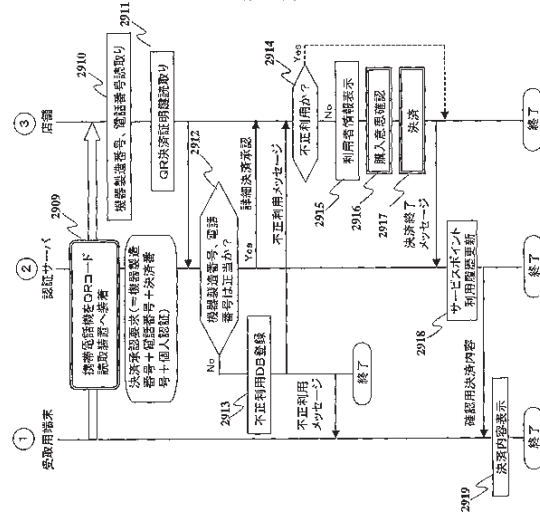
【図 29】

第29図



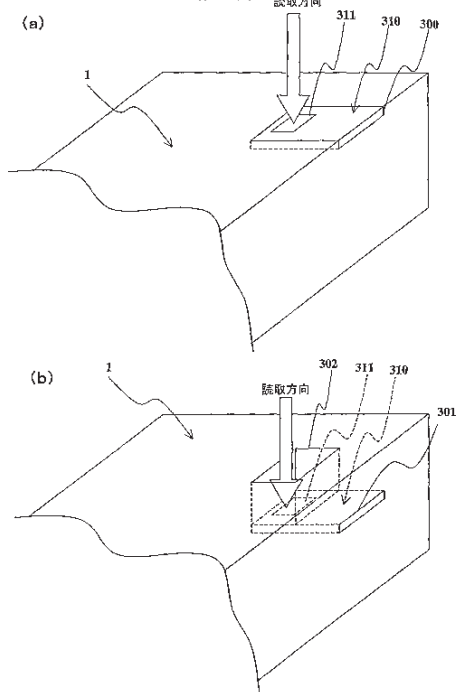
【図 30】

第30図



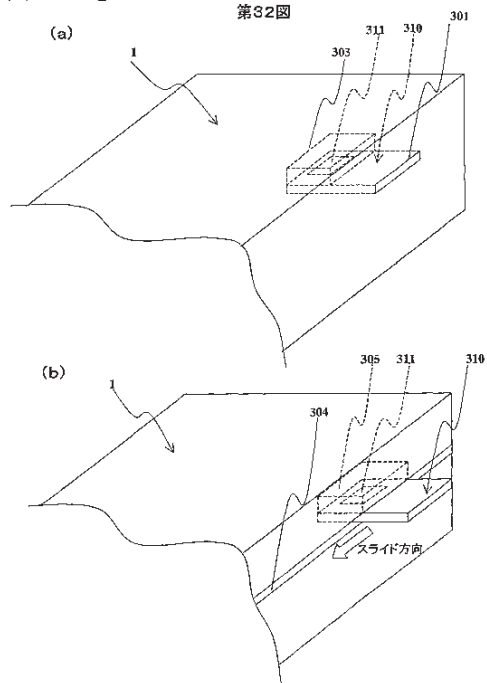
【図 31】

第31図



【図 32】

第32図



【手続補正書】

【提出日】平成14年2月14日(2002.2.14)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、
商取引に関する決済証明鍵情報を決済承認機関から受信するステップと、
受信した決済証明鍵情報を前記表示手段に表示させるステップと、
前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送し、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップと
を備えることを特徴とする商取引方法。

【請求項2】

決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、
商取引に関する決済証明鍵情報と商品購入元から発行される受託証明とを決済承認機関から受信するステップと、
受信した決済証明鍵情報付きの受託証明を前記表示手段に表示させるステップと、
前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送し、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップと
を備えることを特徴とする商取引方法。

【請求項3】

前記ネットワーク端末として携帯電話機を用いたことを特徴とする請求項1又は請求項2のいずれか一項に記載の商取引方法。

【請求項4】

前記決済証明鍵情報を受信するネットワーク端末と、商取引における注文主のネットワーク端末とを異なる端末としたことを特徴とする請求項1～3のいずれか一項に記載の商取引方法。

【請求項5】

前記表示手段に表示される決済証明鍵情報はコードキャラクタ情報画像で構成されていることを特徴とする請求項1～4のいずれか一項に記載の商取引方法。

【請求項6】

前記表示手段に表示される決済証明鍵情報は暗号化されたコードキャラクタ情報画像で構成されていることを特徴とする請求項1～5のいずれか一項に記載の商取引方法。

【請求項7】

前記ネットワーク端末は各端末機器の識別情報を記録した標識を有するものとし、
前記決済端末に前記識別標識を読取らせるステップと、
前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別標識の情報を前記決済承認機関に送信し、前記識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証させるステップと、
前記識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信するステップと

をさらに備えることを特徴とする請求項 1 ～ 6 のいずれか一項に記載の商取引方法。

【請求項 8】

前記ネットワーク端末は、ＩＣカード又はネットワーク端末の所有者のいずれかの識別情報を記録した識別標識有するものとし、

前記決済端末に前記識別標識を読取らせるステップと、

前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別標識の情報を前記決済承認機関に送信し、前記識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証させるステップと、

前記識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信するステップと

をさらに備えることを特徴とする請求項 1 ～ 6 のいずれか一項に記載の商取引方法。

【請求項 9】

前記識別標識は、所定波長の照射光に対し前記識別標識に記録された識別情報を所定波長の反射光により出射する標識で構成されていることを特徴とする請求項 1 ～ 8 のいずれか一項に記載の商取引方法。

【請求項 10】

前記決済証明鍵情報の中に含まれる購入者に関する情報を商品購入元の決済端末の表示部に表示させるステップをさらに備えることを特徴とする請求項 1 ～ 9 のいずれか一項に記載の商取引方法。

【請求項 11】

決済を終えた取引の内容を商品購入元の決済端末から決済承認機関に送信し、購入者の購入履歴情報を更新するステップをさらに備えることを特徴とする請求項 1 ～ 10 のいずれか一項に記載の商取引方法。

【請求項 12】

決済を終えた取引の内容を決済承認機関から購入者のネットワーク端末に送信し、取引の内容を表示させるステップをさらに備えることを特徴とする請求項 1 ～ 11 のいずれか一項に記載の商取引方法。

【請求項 13】

決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、

商取引に関する決済証明鍵情報と商品購入元から発行される受託証明とを決済承認機関から前記ネットワーク端末で受信するステップと、

受信した決済証明鍵付きの受託証明をコードキャラクタ情報画像で印刷させるステップと、

印刷された前記決済証明鍵情報付きの受託証明を商品購入元に設置された決済端末に読み取らせ、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップと

を備えることを特徴とする商取引方法。

【請求項 14】

前記コードキャラクタ情報画像は、所定波長の照射光に対し決済証明鍵情報を所定波長の反射光により出射する結晶粉末を混入した印刷材料で印刷することを特徴とする請求項 13 に記載の商取引方法。

【請求項 15】

前記ネットワーク端末は商取引に関する情報を入力する入力手段を有し、

少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商品の取引に関する情報を前記入力手段から入力するステップと、

入力された決済に関する情報を決済承認機関に送信し、商品提供元の認証と購入者自身の認証及び与信の結果に応じて生成された決済証明鍵情報を受信するステップと

をさらに備えることを特徴とする請求項 1 ～ 13 のいずれか一項に記載の商取引方法。

【請求項 16】

前記ネットワーク端末は商取引に関する情報を入力する入力手段を有し、少なくとも商品提供元又は商品の識別情報、決済方法、利用サービスポイント及び購入者自身の暗証番号を含む商品の取引に関する情報を前記入力手段から入力するステップと、入力された決済に関する情報を決済承認機関に送信し、商品提供元の認証と購入者自身の認証及び前記購入者の獲得したサービスポイントの確認結果に応じて生成された決済証明鍵情報を受信するステップと

をさらに備えることを特徴とする請求項 1 ～ 15 のいずれか一項に記載の商取引方法。

【請求項 17】

取引対象の商品の決済に関する情報を入力する入力手段と、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引装置であって、

商取引に関する決済証明鍵情報を生成する手段と、

前記決済証明鍵情報を前記ネットワーク端末に送信し表示させる手段と

を備えることを特徴とする商取引装置。

【請求項 18】

決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引装置であって、

商取引に関する決済証明鍵情報を生成する手段と

商品購入元から発行される受託証明を受信し、前記決済証明鍵情報付き受託証明として前記ネットワーク端末に送信し表示させる手段と

を備えることを特徴とする商取引装置。

【請求項 19】

前記ネットワーク端末として、携帯電話機を用いたことを特徴とする請求項 17 又は 18 のいずれか一項に記載の商取引装置。

【請求項 20】

決済に関する情報を表示する表示手段と、機器識別標識と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

前記決済承認機関装置が、

商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、

前記決済証明鍵情報の一部又は全部と前記機器識別標識の読取結果を商品提供元から受信し、前記機器識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、

前記機器識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信し、購入者が発注した商品の引渡し及び代金の決済を実行させる手段と

を備えることを特徴とする商取引システム。

【請求項 21】

決済に関する情報を表示する表示手段と、機器識別標識と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

前記決済承認機関装置が、

商取引に関する決済証明鍵情報を生成する手段と、

商品購入元から発行される受託証明と前記決済証明鍵情報とを前記ネットワーク端末に送

信し表示させる手段と、

前記決済証明鍵情報の一部又は全部と前記機器識別標識の読取結果を商品提供元から受信し、前記機器識別標識の情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、

前記機器識別標識の情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信する手段と

を備えることを特徴とする商取引システム。

【請求項 22】

前記ネットワーク端末は、携帯電話機であることを特徴とする請求項 20 又は 21 のいずれか一項に記載の商取引システム。

【請求項 23】

前記機器識別標識は、所定波長の照射光に対し機器製造番号情報および電話番号情報を所定波長の反射光により出射する標識で構成されていることを特徴とする請求項 20～22 のいずれか一項に記載の商取引システム。

【請求項 24】

決済に関する情報を表示する表示手段と、通信網を介して商品の発注及び決済に関する情報を送受する送受信手段とを有する携帯端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

前記決済承認機関装置が、

商取引に関する決済証明鍵情報を生成する手段と、

商品購入元から発行される受託証明と前記決済証明鍵情報とを前記ネットワーク端末に送信する手段と、

前記ネットワーク端末に付属の印刷装置によってコードキャラクタ情報画像で印刷された受託証明と前記決済証明鍵情報の読取結果を商品購入元から受信し、前記決済証明鍵情報が正当なものであるか否かを認証する手段と、

前記決済証明鍵情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信し、購入者が発注した商品の引渡し及び代金の決済を実行させる手段と

を備えることを特徴とする商取引システム。

【請求項 25】

前記コードキャラクタ情報画像は暗号化されたコードキャラクタ情報画像で構成されていることを特徴とする請求項 24 に記載の商取引システム。

【請求項 26】

決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行うためのプログラムを記録した媒体であって、

決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる処理と、

前記決済証明鍵情報が表示されたネットワーク端末から商品購入元に設置された端末に前記決済証明鍵情報を転送し、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行させる処理と

を含むコンピュータが読み取り可能な商取引用のプログラムが記録されていることを特徴とする記録媒体。

【請求項 27】

前記コードキャラクタ情報画像は、バーコード又は 2 次元バーコードで構成されていることを特徴とする請求項 5 又は 6 のいずれか一項に記載の商取引方法。

【請求項 28】

前記入力手段は、撮像手段を含むものとし、前記商品提供元又は商品の識別情報を符号化した画像情報を、前記撮像手段により撮像して入力するステップと、

入力された画像情報を復号化し、前記商品の提供元又は商品の識別情報を取得するステッ

プと

をさらに備えたことを特徴とする請求項 15 又は 16 のいずれか一項に記載の商取引方法。

【請求項 29】

前記入力手段は、商品の取引に関する情報としての商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含み、

前記画像情報を復号化する手段をさらに備えることを特徴とする請求項 17～19 のいずれか一項に記載の商取引装置。

【請求項 30】

前記表示手段に表示される決済証明鍵情報はコードキャラクタ情報画像で構成されていることを特徴とする請求項 20～23 のいずれか一項に記載の商取引システム。

【請求項 31】

前記コードキャラクタ情報画像は、バーコード又は 2 次元バーコードで構成されていることを特徴とする請求項 24 又は 30 のいずれか一項に記載の商取引システム。

【請求項 32】

前記ネットワーク端末は少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商品の取引に関する情報を入力する入力手段を有することを特徴とする請求項 20～25、30、31 のいずれか一項に記載の商取引システム。

【請求項 33】

前記入力手段は、前記商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含むものとし、

前記決済承認機関装置は、前記撮像手段により撮像され、送信された画像情報を復号化する手段をさらに備えたことを特徴とする請求項 32 に記載の商取引システム。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正の内容】

【0009】

タ情報画像で構成されていることを特徴とする。

また、本発明の取引方法は決済承認機関装置におけるプログラムによって実現することができる。そのプログラムは次のような処理を記録した記録媒体で提供することができる。

すなわち、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行うためのプログラムを記録した媒体であって、

決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる処理と、前記決済証明鍵情報が表示されたネットワーク端末から商品購入元に設置された端末に前記決済証明鍵情報を転送し、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行させる処理とを含むコンピュータが読み取り可能な商取引用のプログラムが記録されていることを特徴とする。

さらに本発明の取引方法は、前記コードキャラクタ情報画像を、バーコード又は 2 次元バーコードで構成したことを特徴とする。

また、前記入力手段は、撮像手段を含むものとし、前記商品提供元又は商品の識別情報を符号化した画像情報を、前記撮像手段により撮像して入力するステップと、入力された画像情報を復号化し、前記商品の提供元又は商品の識別情報を取得するステップとをさらに備えたことを特徴とする。

また、本発明の商取引装置は、前記入力手段が、商品の取引に関する情報としての商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含み、前記画像情報を復号化する手段をさらに備えることを特徴とする。

また、本発明の商取引システムは、前記表示手段に表示される決済証明鍵情報をコードキ

ャラクタ情報画像で構成したことを特徴とする。

また、前記コードキャラクタ情報画像を、バーコード又は２次元バーコードで構成したことを特徴とする。

また、前記ネットワーク端末は少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商品の取引に関する情報を入力する入力手段を有することを特徴とする。

また、前記入力手段は、前記商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含むものとし、前記決済承認機関装置は、前記撮像手段により撮像され、送信された画像情報を復号化する手段をさらに備えたことを特徴とする。

図面の簡単な説明

第１図は、本発明の商取引方法を実施するシステムの実施形態を示すシステム構成図である。

第２図は、携帯電話機の構成を示す概略ブロック図である。

第３図は、携帯電話機に付けられる標識とバーコードおよび２次元コードの例を示す図である。

第４図は、携帯電話機に付けられたバーコードおよび表示部に表示された２次元コードを読み取る読取装置の断面構成図である。

第５図は、認証サーバの内部構成図である。

第６図は、店舗情報データベースに格納されるデータの一例を示す図である。

【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP01/04223
A. CLASSIFICATION OF SUBJECT MATTER Int. Cl. ⁷ G06F17/60		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Int. Cl. ⁷ G06F17/60		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5706422 A (AT&T), 13 January, 1998 (1.01.98), column 14 ("A Fifth Illustrative Embodiment") & CA 2176163 A & EP 7455961 A2 & JP 8-339407 A	1-26
Y	US 5608778 A (Lucent Technologies Inc.), 04 March, 1997 (04.03.97), column 6, lines 15 to 60 & CA 2156205 A & EP 708547 A2 & JP 8-096043 A	1-26
Y	EP 1017030 A2 (International Business Machines Corporation), 05 July, 2000 (05.07.00), Figs. 2, 3 & JP 2000-194770 A	1-26
Y	JP 9-116960 A (Fujitsu Limited), 02 May, 1997 (02.05.97), Fig. 3 (Family: none)	1-26
☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "B" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "C" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "R" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "S" document member of the same patent family	
Date of the actual completion of the international search 14 August, 2001 (14.08.01)	Date of mailing of the international search report 11 September, 2001 (11.09.01)	
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer	
Facsimile No.	Telephone No.	

Form PCT/ISA/210 (second sheet) (July 1992)

(43)

JP W02002/008981 A1 2002.1.31

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP01/04223
C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5920767 A (Motorola Inc.), 27 July, 1999 (27.07.99), Figs. 3, 4: column 7, line 66 to column 8, line 13 (Family: none)	1-26
Y	JP 2-016740 A (Toshiba Corporation), 19 January, 1996 (19.01.96), Par. No. [0025] (Family: none)	1-26
Y	US 5769752 A (McMILLON, Steven A.), 04 August, 1998 (04.08.98), Figs. 1, 2 (Family: none)	1-26
Y	WO 85/03787 A1 (WHITE, Peter), 29 August, 1985 (29.08.85), page 14, lines 3 to 10 & CA 1232684 A & EP 172877 A1 & JP 61-501477 A & US 4630201 A	1-26
X, P	WO 01/09807 A1 (E-Mark Systems Inc.), 08 February, 2001 (08.02.01), Figs. 29 to 31 & AU 34559/00 A1 & AU 34560/00 A1 & WO 01/09808 A1	1-26

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

(44)

JP W02002/008981 A1 2002.1.31

国際調査報告		国際出願番号	PCT/JPO1/04223	
A. 発明の属する分野の分類 (国際特許分類 (IPC))				
Int.Cl. G06F17/60				
B. 調査を行った分野				
調査を行った最小の資料 (国際特許分類 (IPC))				
Int.Cl. G06F17/60				
最小限資料以外の資料で調査を行った分野に含まれるもの				
日本国特許庁新案公報 1922-1998年				
日本国公開特許新案公報 1971-2001年				
日本国特許庁新案公報 1994-2001年				
日本国特許庁新案公報 1996-2001年				
国際調査で利用した電子データベース (データベースの名称、調査に利用した用語)				
C. 関連すると認められる文献				
引用文献の カテゴリー*	引用文献名 及び 特許の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号		
Y	US 5708422 A (AT&T) 13. 1 月, 1998 (13.01.98) コラム 14 ("A Fifth Illustrative Embodiment") & CA 2176168 A & EP 745961 A2 & JP 8-339407 A	1-26		
☒ C欄の横書きにも文献が列挙されている。 ☐ パテントファミリーに関する引続を参照。				
* 参考文献のカテゴリー 「A」特に関連のある文献ではなく、一般の技術水準を示すもの 「E」国際出願日前の出願または特許であるが、国際出願日以前に公表されたもの 「L」従来技術に適合する文献又は他の文献の発行 「O」口頭による開示、使用、展示等に及ぼす文献 「P」国際出願日前で、かつ優先権の主張の基礎となる出願				
の日の後に公表された文献 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原意又は理論の理解のために引用するもの 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」特に関連のある文献であって、当該文献と他の文献との間で進歩性がないと考えられるもの 「&」同一パテントファミリー文献				
国際調査を完了した日		国際調査報告の発行日		
14.08.01		11.09.01		
国際調査機関の名称及び住所		特許庁調査官 (権限のある職員)		
日本国特許庁 (JSA/JP) 郵便番号 100-8915 東京都千代田区霞が関二丁目4番3号		阿波 達		
		5 L 9 1 6 8		
		電話番号 03-3581-1101 内線 8561		

様式PCT/JSA/210 (第2ページ) (1998年7月)

国際調査報告		国際出願番号 PCT/JPO1/04223
C (続き)	関連すると認められる文献	
引用文献の カテゴリー	引用文献名 及び 一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	US 5608778 A (LUCENT TECHNOLOGIES INC) 4.3月.1997 (04.03.97) コラム6, 15-60 行 & CA 2156206 A & EP 708547 A2 & JP 8-096043 A	1-26
Y	EP 1017030 A2 (INTERNATIONAL BUSINESS MACHINES CORP) 5.7月.2000 (05.07.00) 図2, 3 & JP 2000-194770 A	1-26
Y	JP 9-116960 A (富士通株式会社) 2.5月.1997 (02.05.97) 図2 (ファミリーなし)	1-26
Y	US 5930787 A (MOTOROLA INC) 27.7月.1999 (27.07.99) 図3, 4; コラム7, 66 行—コラム8, 13 行 (ファミリーなし)	1-26
Y	JP 8-016740 A (株式会社東芝) 19.1月.1996 (19.01.96) 図25[0025] (ファミリーなし)	1-26
Y	US 5789732 A (McMAHON, Steven A) 4.8月.1998 (04.08.98) 図1, 2 (ファミリーなし)	1-26
Y	WO 85/03787 A1 (WHITE, Peter) 29.8月.1985 (29.08.85) ページ14, 3-10 行 & CA 1232684 A & EP 172877 A1 & JP 61-501477 A & US 4630201 A	1-26

様式PCT/ISA/210 (第2ページの続き) (1998年7月)

(46)

JP W02002/008981 A1 2002.1.31

国際調査報告		国際出願番号	PCT/JPO1/04223
C (続き)	関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示		関連する 請求の範囲の番号
X, P	WO 01/09807 A1 (イーマークシステムズ株式会社) 8.2月, 2001 (08.02.01) //29-31 & AU 34559/00 A1 & AU 34560/00 A1 & WO 01/09808 A1		1-25

様式PCT/ISA/210 (第2ページの続き) (1998年7月)

フロントページの続き

(51)Int.Cl.⁷

F I

G 0 6 K 17/00 L

G 0 6 K 19/00 E

G 0 6 K 19/00 J

H 0 4 B 7/26 1 0 9 S

(注) この公表は、国際事務局（W I P O）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第 1 8 4 条の 1 0 第 1 項(実用新案法第 4 8 条の 1 3 第 2 項) により生ずるものであり、本掲載とは関係ありません。

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成17年5月19日(2005.5.19)

【国際公開番号】W02002/008981

【年通号数】公開・登録公報2004-001

【出願番号】特願2002-514614(P2002-514614)

【国際特許分類第7版】

G 0 6 F 17/60

G 0 6 K 17/00

G 0 6 K 19/06

G 0 6 K 19/07

H 0 4 Q 7/38

【F I】

G 0 6 F 17/60 4 1 4

G 0 6 F 17/60 4 2 2

G 0 6 F 17/60 5 0 6

G 0 6 F 17/60 5 1 2

G 0 6 F 17/60 Z E C

G 0 6 K 17/00 L

G 0 6 K 19/00 E

G 0 6 K 19/00 J

H 0 4 B 7/26 1 0 9 S

【手続補正書】

【提出日】平成14年12月24日(2002.12.24)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【書類名】明細書

【発明の名称】商取引方法およびネットワーク端末並びに商取引システム

【特許請求の範囲】

【請求項1】 決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備えるとともに、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、
 商取引に関する決済証明鍵情報を決済承認機関装置から受信するステップと、
 受信した決済証明鍵情報を前記表示手段に表示させるステップと、
 前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送するステップと、
前記標識に記録された識別情報を読取らせて前記決済端末に転送するステップと、
前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別情報とを前記決済承認機関装置に送信し、前記識別情報が決済承認機関装置に予め登録された正規のものであるか否かを認証させるステップと、
前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関装置から商品購入元の決済端末に送信するステップと、
前記決済承認の情報に基づき、商品購入元の決済端末により商品代金の決済を実行するス

テップと

を備えることを特徴とする商取引方法。

【請求項2】決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備えるネットワーク端末と、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するICカードを用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、

商取引に関する決済証明鍵情報を決済承認機関装置から受信するステップと、

受信した決済証明鍵情報を前記表示手段に表示させるステップと、

前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送するステップと、

前記標識に記録された識別情報を読取らせて前記決済端末に転送するステップと、

前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別情報を前記決済承認機関装置に送信し、前記識別情報が決済承認機関装置に予め登録された正規のものであるか否かを認証させるステップと、

前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関装置から商品購入元の決済端末に送信するステップと、

前記決済承認の情報に基づき、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップと

を備えることを特徴とする商取引方法。

【請求項3】前記ネットワーク端末は、商取引に関する情報を入力する入力手段として、商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含む入力手段を有し、

少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商取引に関する情報を前記入力手段から入力するステップと、

入力された商取引に関する情報を決済承認機関装置に送信し、前記画像情報を復号化させ、商品提供元の認証と購入者自身の認証と与信の結果に応じて生成された決済証明鍵情報を受信するステップと

をさらに備えることを特徴とする請求項1又は請求項2のいずれかに記載の商取引方法。

【請求項4】商取引に関する決済証明鍵情報を決済承認機関装置から受信して表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備え、前記表示手段に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送して、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行する商取引方法に用いられるネットワーク端末であって、

予め決済承認機関に登録された識別情報を記録した標識を有し、当該標識は所定波長の照射光に対し所定波長の反射光により前記識別情報を出射することを特徴とするネットワーク端末。

【請求項5】前記ネットワーク端末は、商取引に関する情報を入力する入力手段を備え、当該入力手段には、商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含むことを特徴とする請求項4に記載のネットワーク端末。

【請求項6】決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段を備えるとともに、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するネットワーク端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

前記決済承認機関装置が、

商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、

前記決済証明鍵情報の一部又は全部と前記識別標識の読取結果としての識別情報を前記商

品提供元装置から受信し、前記識別情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、
前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信し、購入者が発注した商品の引渡し及び代金の決済を実行させる手段と
を備えることを特徴とする商取引システム。

【請求項7】決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを備えるネットワーク端末と、予め記録された識別情報を所定波長の照射光に対し所定波長の反射光により出射する標識を有するＩＣカードと、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、

前記決済承認機関装置が、
商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、

前記決済証明鍵情報の一部又は全部と前記識別標識の読取結果としての識別情報を前記商品提供元装置から受信し、前記識別情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、

前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品提供元装置に送信する手段と

を備えることを特徴とする商取引システム。

【請求項8】前記ネットワーク端末は、少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商取引に関する情報を入力する入力手段を有し、当該入力手段として商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含むものとし、

前記決済承認機関装置は、前記撮像手段により撮像され、送信された画像情報を復号化する復号化手段をさらに備えたことを特徴とする請求項6又は請求項7に記載の商取引システム。

【発明の詳細な説明】

【0001】

技術分野

本発明は、携帯電話機等のネットワークに接続可能な端末を用いてスーパーマーケット等の各種の店舗、インターネットのサーバ上に開設されている電子店舗、あるいは飲料水等の自動販売機で購入する商品の代金の決済を行う商取引方法及び装置並びにシステムに関するものである。

【0002】

背景技術

携帯電話機にWWW閲覧機能（World Wide Web）を付加したことにより、携帯電話機を使用してインターネットにアクセスし、各種の情報、物品、役務サービスを閲覧し、必要に応じて、それらの情報、物品、役務サービスの提供を注文するという取引形態が急速に拡大している。ここで、本発明では、形状を有しない音楽ソフトなどの情報（コンテンツ）、形状を有する物品、宅配サービス、介護サービスなどの役務サービスを全て商取引の対象となる商品と定義する。この場合、公共機関が提供する無料の介護サービスもあるが、無料であっても取引の対象となる商品に含むものとする。

しかし、携帯電話機を使用して商品の発注を行ったとしても、その決済方法としては、銀行振込みや現金の送付、商品到着時の代金引換などの従来の商慣習に従った方法が踏襲されている。

最近では、このような旧来方法に代えて、商品の注文と同時に、クレジットカード番号を商品提供元（店舗）に通知し、クレジットカード会社を通じて決済する方法が実施されている。

しかし、この決済方法は、クレジットカード会社と本人だけが知るべき番号あるいは情報

が外部に漏れないことを前提にしており、外部に漏れた場合には悪用される危険性がある。

そこで、2001年5月から開始される次世代移動通信サービスでは、携帯電話機にUIM (User Identity Module) と呼ばれるICカードを搭載し、このICカード内の暗号プログラムによりクレジットカード番号等の秘密データを暗号化し、決済を行うという方法が考えられている。

しかし、暗号プログラムにより暗号化して保存したとしても、携帯電話機自体を紛失した場合には、不正な第三者に解読されてしまい、悪用される危険性がある。特に、ICカード内にはクレジットカード番号のみでなく、銀行口座番号や保険証番号、電子マネーなどの他の秘密データも同時に保存する形態が多くなると考えられるので、不正な第三者に解読された場合の危険性は旧来の決済方法よりも高くなるという問題がある。

また、非接触型ICカード同様、無線を利用したネットワークは特に有線ネットワーク以上に不正アクセスを含むハッキング等、情報が外部に漏れる可能性が高くなるという問題がある。

また、不正な店舗の出現により、店舗での決済時に秘密データが盗聴され、悪用される危険性がある。

また、携帯電話機自体のコストも上昇し、さらに電力消費も増加し、電池寿命が短くなるという問題がある。

本発明はこのような問題を解決するためになされたものであり、その目的は、クレジットカード番号等の秘密データを本人認証機関やクレジットカード会社以外に開示することなく本人認証を行い、安全に購入商品の決済を行うことができる商取引方法及び装置、並びにシステムを提供することにある。

【0003】

発明の開示

上記目的を達成するために、本発明の商取引方法は、以下のように構成したことを特徴とするものである。

すなわち、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備えるとともに、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、商取引に関する決済証明鍵情報を決済承認機関装置から受信するステップと、受信した決済証明鍵情報を前記表示手段に表示させるステップと、前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送するステップと、前記標識に記録された識別情報を読取らせて前記決済端末に転送するステップと、前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別情報とを前記決済承認機関装置に送信し、前記識別情報が決済承認機関装置に予め登録された正規のものであるか否かを認証させるステップと、前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関装置から商品購入元の決済端末に送信するステップと、前記決済承認の情報に基づき、商品購入元の決済端末により商品代金の決済を実行するステップとを備えることを特徴とする。

また、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備えるネットワーク端末と、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するICカードを用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、商取引に関する決済証明鍵情報を決済承認機関装置から受信するステップと、受信した決済証明鍵情報を前記表示手段に表示させるステップと、前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送するステップと、前記標識に記録された識別情報を読取らせて前記決済端末に転送するステップと、前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別情報を前記決済承認機関装置に送信し、前記識別情報が決済承認機関装置に予

め登録された正規のものであるか否かを認証させるステップと、前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関装置から商品購入元の決済端末に送信するステップと、前記決済承認の情報に基づき、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップとを備えることを特徴とする。

また、前記ネットワーク端末は、商取引に関する情報を入力する入力手段として、商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含む入力手段を有し、少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商取引に関する情報を前記入力手段から入力するステップと、入力された商取引に関する情報を決済承認機関装置に送信し、前記画像情報を復号化させ、商品提供元の認証と購入者自身の認証と与信の結果に応じて生成された決済証明鍵情報を受信するステップとをさらに備えることを特徴とする。

本発明のネットワーク端末は、商取引に関する決済証明鍵情報を決済承認機関装置から受信して表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備え、前記表示手段に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送して、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行する商取引方法に用いられるネットワーク端末であって、予め決済承認機関に登録された識別情報を記録した標識を有し、当該標識は所定波長の照射光に対し所定波長の反射光により前記識別情報を出射することを特徴とする。

また、前記ネットワーク端末は、商取引に関する情報を入力する入力手段を備え、当該入力手段には、商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含むことを特徴とする。

本発明の商取引システムは、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段を備えるとともに、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するネットワーク端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、前記決済承認機関装置が、商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、前記決済証明鍵情報の一部又は全部と前記識別標識の読取結果としての識別情報を前記商品提供元装置から受信し、前記識別情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信し、購入者が発注した商品の引渡し及び代金の決済を実行させる手段とを備えることを特徴とする。

また、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを備えるネットワーク端末と、予め記録された識別情報を所定波長の照射光に対し所定波長の反射光により出射する標識を有するＩＣカードと、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、前記決済承認機関装置が、商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、前記決済証明鍵情報の一部又は全部と前記識別標識の読取結果としての識別情報を前記商品提供元装置から受信し、前記識別情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品提供元装置に送信する手段を備えることを特徴とする。

また、前記ネットワーク端末は、少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商取引に関する情報を入力する入力手段を有し、当該入力手段として商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含むものとし、前記決済承認機関装置は、前記撮像手段により撮像され、送信された画像情報を復号化する復号化手段をさらに備えたことを特徴とする。

【 0 0 0 4 】

図面の簡単な説明

第 1 図は、本発明の商取引方法を実施するシステムの実施形態を示すシステム構成図である。

第 2 図は、携帯電話機の構成を示す概略ブロック図である。

第 3 図は、携帯電話機に付けられる標識とバーコードおよび 2 次元コードの例を示す図である。

第 4 図は、携帯電話機に付けられたバーコードおよび表示部に表示された 2 次元コードを読み取る読取装置の断面構成図である。

第 5 図は、認証サーバの内部構成図である。

第 6 図は、店舗情報データベースに格納されるデータの一例を示す図である。

第 7 図は、利用者情報データベースに格納されるデータの一例を示す図である。

第 8 図は、購入履歴データベースに格納されるデータの一例を示す図である。

第 9 図は、不正利用情報データベースに格納されるデータの一例を示す図である。

第 10 図は、携帯電話機を用いて一般店舗で商品代金を決済する手順を示すフローチャートである。

第 11 図は、第 10 図の続きを示すフローチャートである。

第 12 図は、携帯電話機に表示される Q R 決済証明鍵と店舗端末に表示される利用者情報の例を示す図である。

第 13 図は、決済終了時に携帯電話機に表示される確認用の情報例を示す図である。

第 14 図は自動販売機で小額商品の決済を行う場合の手順を示すフローチャートである。

第 15 図は第 14 図の続きを示すフローチャートである。

第 16 図は、インターネット上の店舗で注文した商品を指定の受取店舗で受け取って決済する場合の手順を示すフローチャートである。

第 17 図は、第 16 図の続きを示すフローチャートである。

第 18 図は、Q R 決済証明鍵を印刷したものを店舗に持参して決済する場合の手順を示すフローチャートである。

第 19 図は、Q R 決済証明鍵を印刷した例を示す図である。

第 20 図は、贈答情報データベースに格納されるデータの一例を示す図である。

第 21 図は、他人への贈答品の決済をする場合の手順を示すフローチャートである。

第 22 図は、図 21 の続きを示すフローチャートである。

第 23 図は、図 22 の続きを示すフローチャートである。

第 24 図は、携帯電話機に表示される贈答情報の表示例及び受諾又は拒絶の選択後の表示例を示す図である。

第 25 図は、決済終了時に贈り手側の携帯電話機に表示される確認用の情報例を示す図である。

第 26 図は、図 21 の続きを示すフローチャートである。

第 27 図は、図 26 の続きを示すフローチャートである。

第 28 図は、サービスポイント利用履歴データベースの一例を示す図である。

第 29 図は、携帯電話機を用いて一般店舗でサービスポイントにより決済する手順を示すフローチャートである。

第 30 図は、図 29 の続きを示すフローチャートである。

第 31 図は、本発明に用いられる携帯電話機の一例を示す部分斜視図である。

第 32 図は、本発明に用いられる携帯電話機の一例を示す部分斜視図である。

【 0 0 0 5 】

発明を実施するための最良の形態

以下、本発明の実施の形態を添付図面により詳細に説明する。

図 1 は、本発明の商取引方法を実施するシステムの全体構成の実施形態を示すシステム構成図であり、商品購入者が使用するネットワーク端末としての携帯電話機 1、商品提供元の店舗 2、飲料水等の自動販売機 3、決済承認機関 4 で構成され、これらが通信網 5 で接

続されている。通信網 5 は、無線回線と有線回線及びインターネット網を含むものである。ここで、ネットワーク端末とは、インターネット等のネットワークに接続可能な端末を示すものであり、以下の例に示す携帯電話機 1 の他、P H S, P D A, パーソナルコンピュータ、デジタルテレビ等、種々のものが含まれる。

携帯電話機 1 は、インターネット網に接続可能な機能を有する市販の携帯電話機であり、図 2 (a) の概略ブロック図に示すように、表示部 1 1、無線送受信部 1 2、制御部 1 3、入力部 1 4、送受信器 1 5、メモリ 1 6、外部入出力インタフェース 1 7 を備えている。表示部 1 1 にはインターネット接続モードにおいて、図 2 (b) に示すように、ニュース、モバイルバンキング、カード／証券／保険、モバイルショッピングなどのインターネット接続メニューが表示されるようになっている。

外部入出力インタフェース 1 7 は、I r d a 等の赤外線インタフェース及びブルーツースなどの微弱電波インタフェース等の無線通信インタフェースを含むものであり、本実施形態では、店舗の識別番号を店舗内に設置された発信機から受信する場合に使用される。また外部入出力インタフェース 1 7 には、携帯電話機接続型又は携帯電話機内蔵型のバーコード読取装置のインタフェースを含み、このバーコード読取装置により、バーコード情報で表示された店舗の識別情報又は商品の識別情報等を読取ることとしてもよい。さらに、携帯電話機接続型又は携帯電話機内蔵型のカメラを含み、このカメラにより、コードキャラクタ情報画像により表示された各店舗の識別情報又は商品の識別情報を、画像データとして取り込むこととしてもよい。この場合は、画像データとして取り込んだコードキャラクタ情報画像をデコードするためのプログラムを、前記決済承認機関 4 の認証サーバ内に設けておき、携帯電話機から送信されたコードキャラクタ情報画像を前記プログラムでデコードすることにより、店舗又は商品の識別情報を認識することとなる。また、前記プログラムは、携帯電話機内に設けることとしてもよく、この場合には、携帯電話機内でコードキャラクタ情報画像をデコードすることにより認識された前記各識別情報を、前記認証サーバに送信することとなる。

以上のような外部入出力インタフェース 1 7 を使用することにより、入力部 1 4 の操作を行わずに店舗又は商品の識別情報の入力を行うことができる。ここで、商品の識別情報としては、商品名、商品種別、金額等が該当する。

なお、商品の金額を入力するのは、店員の金額入力に代わるものではなく、セルフスキャン行為を含むものであり、決済金額情報を購入者が事前に知るためのものである。

本実施形態の携帯電話機 1 には、図 3 (a), (b) の正面図及び側面図に示すように、機器製造番号を図 3 (c) のようなバーコード 3 1 で記録した第 1 の標識 1 9 と、携帯電話番号をバーコード 3 1 で記録した第 2 の標識 2 0 が貼り付けられている。

これらの標識 1 9, 2 0 のバーコードは、図 4 (a) に示すように、所定波長 λa の照射光に対し記録情報を所定波長 λa または λb の反射光により出射する結晶粉末を混入した印刷材料で印刷されている。この結晶粉末は、米国 S U N S T O N E 社が提供しているものであり、医薬品や紙幣の真贋識別用に採用されているものである。この場合、用途及び使用システムに応じて、照射光の波長と出射光の波長が異なるように特性が調整されている。

本発明では、このような特殊な結晶粉末を混入した記録インクまたはトナーで機器製造番号及び携帯電話番号のバーコードを標識 1 9, 2 0 に印刷し、これを携帯電話機 1 の正面あるいは側面に貼り付け、その標識 1 9, 2 0 に記録されたバーコードを所定波長 λa の照射光で読み取るようにしている。

このような特殊な記録インクまたはトナーで記録した機器製造番号及び携帯電話番号の標識 1 9, 2 0 を携帯電話機 1 に貼り付けておくことにより、予め定めた波長の照射光以外では機器製造番号及び携帯電話番号を読み取ることができない。よって、機器製造番号及び携帯電話番号を決済承認機関 4 に事前登録しておくことにより、当該携帯電話機 1 が本システムでの商取引を利用できる正当な機器であるか否かを識別することができる。また、側面の標識 2 0 は、携帯電話機 1 の改造を防止できる役目を果たしている。

なお、この場合には、必ずしも前記標識の貼り付けを必要とするのではなく、携帯電話

機の筐体自体に、前記記録インク等により、前記標識を印刷することとしてもよい。
標識 19, 20 のバーコードは、図 4 (b) に示すような断面構成の読取装置 40 内に挿入され、予め定めた波長の照射光を照射することによって読み取られる。この読取装置 40 は、店舗 2 や自動販売機 3 に設置される。

一方、表示部 11 には図 3 (d) に示すようなコードキャラクタ情報画像としての 2 次元コード 32 で構成された決済承認鍵情報が表示される。この 2 次元コード 32 は、日本自動車工業会及び日本文具協会の標準コードに設定されているものである。これについては、例えば特開平 10-214317 号公報等で開示されているので、ここでの詳細な説明は省略する。

この 2 次元コード (以下、QR コードと言う) を用いれば、携帯電話機 1 の表示部の面積内で約 7000 文字 (数字) をコード化して記録することができる。本発明では、この QR コードを決済承認鍵の情報を表現するために使用している。詳しくは、QR コードで構成された決済承認鍵の情報を携帯電話機 1 に転送して図 3 (a) のように表示部 11 に表示させ、この表示状態の携帯電話機 1 を標識 19, 20 の読取共用の読取装置 21 に挿入し、決済承認鍵の情報を読み取るようにしている。

QR コードを用いた場合、図 3 (d) に示すように、3ヶ所に配置した切り出しシンボル 33~35 によって 360 度のどの方向からでも記録内容を読み取ることができるので、読取部との位置関係の束縛がなくなり、一般の利用者が読み取り部に挿入して読み取らせる場合に好適である。また、位置関係を厳密に定める必要がないため、その分だけ読取時間も短縮することができる。さらに、コードの一部に汚れや破損があっても誤りを訂正できるので、読取ミスが減少する。特に本発明のように、携帯電話機 1 の表示部に表示させた状態で読み取らせる場合、表示部の汚れ等によって読取ミスが発生することが考えられるが、QR コードを用いることによって表示部の汚れ等に起因する読取ミスを減少させることができる。

図 1 に戻り、店舗 2 には標識 19, 20 と QR コードの読取共用の読取装置 21 が設置され、読み取った標識 19, 20 と QR コードを POS 端末で構成される店舗端末 22 に入力し、店舗端末で代金の決済を行うようになっている。自動販売機 3 にも標識 19, 20 と QR コードの読取共用の読取装置 33 が設置されている。

一方、承認機関 4 は、認証サーバ 41 と金融機関 (銀行またはクレジット会社) 42、店舗情報データベース (DB) 43、利用者情報データベース (DB) 44、購入履歴データベース (DB) 45 を備えている。

認証サーバ 41 は、携帯電話機 1 からの本人認証及び店舗認証要求に対して、本人認証及び店舗認証さらには金融機関 42 に対する与信照会を行い、予め登録してある本人および店舗であり、しかも金融機関 42 から与信 OK の回答があった場合には商品の代金決裁を携帯電話機 1 を使用して許可する処理を行うものであり、店舗登録処理プログラム 410、利用者登録処理プログラム 411、購入履歴管理プログラム 412、不正利用管理プログラム 413、認証処理プログラム 414、QR 決済鍵生成プログラム 415、送受信プログラム 416 を備えている。なお、各データベース 43、44、45 のデータを暗号化して保存するための暗号化／複合化プログラムが必要に応じて組み込まれる。また、QR コードを暗号化して送信するための暗号化プログラムおよび復号するための復号プログラムが組み込まれる。QR コードを暗号化することにより、不正な取引をさらに困難にすることができる。

店舗登録処理プログラム 410 は、本システムを使用して決済を行う店舗 (自動販売機やインターネット上の電子店舗を含む) を店舗情報 DB 43 に登録する際に使用するプログラムである。また、利用者登録処理プログラム 411 は本システムを使用して決済を行う利用者 (商品購入者) を利用者情報 DB 44 に登録する際に使用するプログラムである。

購入履歴管理プログラム 412 は、利用者 (商品購入者) が購入した商品の購入履歴の情報を購入履歴 DB 45 に格納する際に使用するプログラムである。

不正利用管理プログラム 413 は、店舗情報 DB 43 及び利用者情報 DB 44 に予め登録されていない店舗及び利用者が本システムにアクセスした場合、あるいは携帯電話機 1 の

機器製造番号や電話番号を不正に書き換えてアクセスした場合の店舗識別番号あるいは携帯電話機 1 の機器製造番号や電話番号を不正利用情報データベース（図 9）に登録する際に使用するプログラムである。

認証処理プログラム 4 1 4 は、携帯電話機 1 からの本人認証及び店舗認証要求に対して、本人認証及び店舗認証さらには金融機関 4 2 に対する与信照会を行い、予め登録してある本人および店舗であり、しかも金融機関 4 2 から与信 OK の回答があった場合には商品の代金決済を携帯電話機 1 を使用して許可する処理を行うものである。

QR 決済鍵生成プログラム 4 1 5 は、商品の代金決済を許可するために、QR コードで構成された決済証明鍵の情報を生成して携帯電話機 1 に渡すプログラムである。QR コードで構成された決済証明鍵の情報（以下、QR 決済証明鍵情報）は、店舗が購入者本人及び店舗の認証結果を含む詳細な決済承認の情報を認証サーバ 4 1 から受け取るための鍵となる情報であり、本システムでこの QR 決済証明鍵情報を店舗の読取装置 2 1 で読み取り、その読み取った QR 決済証明鍵情報を店舗端末から認証サーバ 4 1 に送信することにより、店舗端末 2 2 では購入者本人及び店舗の認証結果を含む詳細な決済承認の情報を受け取ることができる。この場合、読取装置 2 1 で読み取った QR 決済証明鍵情報が認証サーバ 4 1 で生成したものと異なる場合には決済承認の情報を取得することができない。

送受信プログラム 4 1 6 は、利用者および店舗からのアクセスに対し、決済に必要な情報を送受信するプログラムである。

図 6 は、店舗情報 DB の登録情報の一例を示すものであり、店舗 ID 6 0 1、店舗名称 6 0 2、住所 6 0 3、電話番号 6 0 4 が登録されるようになっている。

図 7 は、利用者情報 DB の登録情報の一例を示す図であり、利用者 ID 7 0 1、利用者名 7 0 2、住所 7 0 3、携帯電話製造番号（機器製造番号）7 0 4、携帯電話番号 7 0 5、本システムを利用する際の暗証番号 7 0 6、性別 7 0 7、生年月日 7 0 8、デビットカード番号 7 0 9、クレジットカード番号 7 1 0、Web マネー口座番号 7 1 1、個人特徴情報 7 1 2 が登録されるようになっている。

Web マネー口座番号 7 1 1 は、飲料水などの小額商品を自動販売機で購入する場合に Web マネーによって決済する際に使用するものである。また、個人特徴情報 7 1 2 は、本人の写真等を登録しておき、店舗での決済時に店員が写真などの特徴によって本人確認を行えるようにするためのものであり、利用者本人の希望に応じて登録される。例えば、利用者本人の写真を登録しておけば、決済時に他人による悪用を店員が発見できるといった利点がある。また、生年月日 7 0 8 により、未成年者であるか否かを発見でき、酒、煙草類の販売を差し止めることができる。この他に、運転免許証番号などを登録することができる。運転免許証番号などを登録しておくことによって、携帯電話機を利用して第三者である認証サーバ 4 1 から本人認証証明を発行することも可能である。

図 8 は、購入履歴 DB の格納情報の一例を示す図であり、利用日時 8 0 1、利用店舗名 8 0 2、決済金額 8 0 3、今月分利用金額累計 8 0 4、サービスポイント累計 8 0 5、前回利用日 8 0 6 が格納されるようになっている。なお、この購入履歴情報は、利用者別に利用日時順に格納されるものである。

図 9 は、不正利用情報データベースに格納される情報の一例を示す図であり、不正利用者の携帯電話製造番号 9 0 1、携帯電話番号 9 0 2、店舗 ID 9 0 3 が登録されるようになっている。ここで、携帯電話番号 9 0 2 のみが登録されている場合は、携帯電話製造番号は正しいが、携帯電話番号の標識を改造してアクセスした者を意味する。また、店舗 ID 9 0 3 が登録されていない店舗は、本システムに未登録の店舗であるか、または店舗 ID を不正に書き換えている店舗を意味する。

ここで、悪意がない未登録の利用者および店舗については、アクセス時に登録を行うようにメッセージを送信し、複数回の登録案内を行ったにも拘わらず登録手続を行わないものについてのみに不正利用として登録するようにしてもよい。

以下、（１）スーパーマーケット等の一般の店舗で携帯電話機 1 を利用した商品購入時の決済方法、（２）自動販売機での商品購入時の決済方法、（３）インターネット上の電子店舗での商品購入時の決済方法についてフローチャートを参照して説明する。

図 10 及び図 11 は、スーパーマーケット等の一般の店舗で携帯電話機 1 を利用した商品購入時の決裁方法を示すフローチャートである。

まず、利用者（商品購入者）は、自分が所持する携帯電話機 1 をモバイルショッピングモードに設定した後、入力手段 14 を使用し、商品を購入しようとしている店舗の識別情報としての店舗 ID、自分の暗証番号（図 7 の 706 に登録した番号）、決裁方法、商品の購入金額を入力する（ステップ 1001）。ここで、店舗又は商品の識別情報を、店舗内に設置されている発信機等から外部入出力インタフェース 17 を介して取り込むようにしてもよい。

また、決裁方法については、クレジットカード決裁、Webマネー決裁、デビットカード決裁があるが、クレジットカード決裁を選択した場合については支払い回数とクレジットカード番号を入力する。また、Webマネー決裁を選択した場合にはWebマネー口座番号（図 7 の 711 に登録した番号）を入力する。同様に、デビットカード決裁を選択した場合にはデビットカード番号（図 7 の 709 に登録した番号）を入力する。なお、以下のフローチャートでは人間が行う操作はステップ 1001 のように 2 重枠線で囲む形式で表記している。

入力が終了したならば、送信操作を行う。すると、ステップ 1001 で入力した情報が QR 決裁証明鍵発行要求として認証サーバ 41 に送信される。

この QR 決裁証明鍵発行要求を受信した認証サーバ 41 は、店舗及び利用者の認証処理を行う（ステップ 1002）。すなわち、QR 決裁証明鍵発行要求の中に含まれる店舗 ID によって店舗情報 DB 43 を検索し、当該店舗 ID の店舗が登録されているか否かを調べる。同様に、暗証番号、クレジットカード番号（またはWebマネー口座番号、デビットカード番号）によって利用者情報 DB 44 を検索し、当該暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）の利用者が利用者情報 DB 44 に登録されているか否かを調べる。その結果、店舗 ID が登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 1003）。また、暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 1003）。携帯電話機 1 では、取引不可のメッセージが表示部 11 に表示されると共に、ステップ 1001 で入力した店舗 ID 等の情報が自動消去される。

しかし、店舗 ID 及び暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証 OK とする。

認証 OK となった場合には、認証サーバ 41 は金融機関 42 に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関 42 における与信処理（ステップ 1004）によって与信 OK または与信 NG の与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたは QR 決裁証明鍵を生成する（ステップ 1005）。すなわち、与信 NG の与信結果が返送されてきた場合には、認証サーバ 41 は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機 1 に送信する。しかし、与信 OK であった場合には、図 3（d）で示したような 2 次元コードで構成された QR 決裁証明鍵を生成し（ステップ 1006）、これを携帯電話機 1 に送信する。この QR 決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。

携帯電話機 1 では、受信した QR 決裁証明鍵を図 12（a）に符号 1201 で示すように表示部 11 に表示する。同時に、例えば「この携帯電話機で決裁できます。代金決裁時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は予め選択してあった購入希望商品を店舗端末 22 の店員に提示し、購入希望商品の発注を行う（ステップ 1007）。店員は店舗端末によって購入希望商品の代金を入力する（ステップ 1008）。

これと並行して、利用者は QR 決裁証明鍵 1201 が表示された状態の携帯電話機 1 を店舗端末 22 に付属した QR コード読取装置 21 の読取部分に挿入装着する（ステップ 10

09)。すると、QRコード読取装置21は、携帯電話機1の表示部11に表示されたQR決裁証明鍵1201を読み取ると共に（ステップ1011）、標識19、20から携帯電話製造番号と携帯電話番号を読み取り（ステップ1010）、その読取結果を店舗端末22に転送する。

店舗端末22は、携帯電話機1から読み取った携帯電話製造番号、携帯電話番号及びQR決裁証明鍵1201を決裁承認要求として認証サーバ41に送信する。この場合、QR決裁証明鍵1201については、認証サーバ自身が発行したものであることが分かればよいので、決裁番号及び個人認証といった一部の情報のみを送信してもよい。図11では、決裁番号及び個人認証の情報のみを決裁承認要求の中に含ませて送信していることを示している。

認証サーバ41は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報DB44の登録内容と照合して調べる（ステップ1012）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図9）に登録した後（ステップ1013）、不正利用メッセージを店舗端末22および携帯電話機1に送信する。

不正利用メッセージを受信した携帯電話機1では、不正利用メッセージ自体がQR決裁証明鍵1201の消去コマンドとして機能し、表示部11に表示されていたQR決裁証明鍵1201が消去される。

店舗端末22では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ1014）。そして、店員により代金決裁ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末22から受信したQR決裁証明鍵1201の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ41は詳細決裁承認を店舗端末22に返信する。この詳細決裁承認の情報には、QR決裁証明鍵1201と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決裁承認を店舗端末22は、受信した詳細決裁承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ1015）。図12（b）にその例を示している。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ1016）。

本人の購入意思の確定応答があったならば、決裁ボタン操作によって決裁を完了する（ステップ1017）。決裁ボタン操作が行われた場合は、店舗端末22は決裁終了メッセージを認証サーバ41に送信する。この決裁終了メッセージを受信した認証サーバ41は利用者の購入履歴情報を更新する（ステップ1018）。この後、確認用の決裁内容を携帯電話機1に送信する。また、決裁終了情報を金融機関42に送信する。これにより、携帯電話機1の表示部11には、図13に示すような確認用の決裁内容1301が表示される。この決裁内容1301は、利用者自身が消去するまで保存することができる。ただし、QR決裁証明鍵1301は1回限り有効であるので、所定時間後に自動的に消去される。また、決裁終了情報を受信した金融機関42では利用者の指定口座から代金を引き落とす手続を行う。

以上により、携帯電話機1を使用して一般店舗での商品購入時の決裁を行うことができる。なお、利用者が購入意思を撤回した場合に、店舗端末でのキャンセル操作によって店舗端末の処理は終了する。また、利用者自身が携帯電話機1でキャンセル操作を行った場合にも、決裁処理は途中で終了し、QR決裁証明鍵1301等の情報は全て消去される。

以上の説明から明らかなように、本取引方法によれば、店舗側に利用者のクレジット番号等の秘密情報を伝えることなく、認証サーバ41が発行したQR決裁証明鍵のみで代金決裁を行うことができる。また、携帯電話機1内にクレジットカード番号等の秘密情報を全く保持しない構成であるので、万一、携帯電話機1を紛失したとしても、代金決裁に悪用

される危険性は全く生じない。さらに、特殊な結晶粉末を混入して記録した標識によって携帯電話製造番号と電話番号の正当性を判定しているため、携帯電話機自身の改造による悪用を防止することができ、決済に使用される機器のセキュリティ性を高めることにより、利用者および店舗の双方に有益な効果を発揮する。

さらに、店舗においては、読取装置 21 を付加するのみであるため、システムに加盟するに際してのコストが少なく済むという利点がある。同様に、携帯電話機 1 においても、IC カードなどを付加することなく市販の携帯電話機をそのまま利用することができる。さらに、購入履歴を管理しているため、店舗側においてはポイントカードを発行する必要がなくなる。また、利用者にとっても、利用状況が分かるので、計画的な購入計画を立てるのに役立つという利点がある。

また、QR コードを用いたことにより、360 度のどの方向からでも記録内容を読み取ることができるので、読取部との位置関係の束縛がなくなり、一般の利用者が読み取り部に挿入して読み取らせる場合に好適である。また、位置関係を厳密に定める必要がないため、その分だけ読取時間も短縮することができる。さらに、コードの一部に汚れや破損があっても誤りを訂正できるので、読取ミスが減少する。特に本発明のように、携帯電話機 1 の表示部に表示させた状態で読み取らせる場合、表示部の汚れ等によって読取ミスが発生することが考えられるが、QR コードを用いることによって表示部の汚れ等に起因する読取ミスを減少させることができる。

なお、QR 決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成されるものとしたが、決裁番号、個人認証、氏名の一部または全部を元に生成した 1 回限りのパスワードであってもよい。

この場合には、例えば、認証サーバ 41 と携帯電話機 1 とに、同一ロジックによるパスワード生成プログラムを備え、2 回目にアクセスするときは、1 回目に送信された暗証番号等に基づき自動生成されたパスワードを携帯電話機 1 から自動送信し、認証サーバ 41 側では、当該携帯電話機 1 の携帯電話番号等及び自動送信されたパスワードと、前記認証サーバ 41 で自動生成されたパスワードとを比較することにより、認証を行う。

3 回目以降は、前回自動生成されたパスワードに基づき新たなパスワードを自動生成、自動送信することとしてもよい。

このような、いわゆるワンタイムパスワードと呼ばれるものを用いることにより、セキュリティ性を高めることができるとともに、2 回目以降のアクセス時に、暗証番号の入力を省略することができる。

次に、自動販売機 3 から飲料水等の小額商品を購入する場合の決裁方法について図 14 及び図 15 のフローチャートを参照して説明する。

まず、利用者（商品購入者）は、自分が所持する携帯電話機 1 をモバイルショッピングモードに設定した後、入力手段 14 を使用し、商品を購入しようとしている自動販売機 3 の店舗 ID、自分の暗証番号（図 7 の 706 に登録した番号）、決裁方法、商品の購入金額を入力する（ステップ 1401）。ここで、店舗又は商品の識別情報を、店舗内に設置されている発信機等から外部入出力インタフェース 17 を介して取り込むようにしてもよい。また、決裁方法については、クレジットカード決裁、Web マネー決裁、デビットカード決裁、非接触 IC カード決済があるが、小額決裁であるので、Web マネーを使用することとし、Web マネー口座番号（図 7 の 711 に登録した番号）を入力する。

入力が終了したならば、送信操作を行う。すると、ステップ 1401 で入力した情報が QR 決裁証明鍵発行要求として認証サーバ 41 に送信される。

この QR 決裁証明鍵発行要求を受信した認証サーバ 41 は、店舗（ここでは自動販売機）及び利用者の認証処理を行う（ステップ 1402）。すなわち、QR 決裁証明鍵発行要求の中に含まれる店舗 ID によって店舗情報 DB 43 を検索し、当該店舗 ID の店舗（自動販売機）が登録されているか否かを調べる。同様に、暗証番号、Web マネー口座番号によって利用者情報 DB 44 を検索し、当該暗証番号及び Web マネー口座番号の利用者が利用者情報 DB 44 に登録されているか否かを調べる。その結果、店舗 ID が登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携

携帯電話機 1 に返信する（ステップ 1 4 0 3）。また、暗証番号及びWebマネー口座番号が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 1 4 0 3）。携帯電話機 1 では、取引不可のメッセージが表示部 1 1 に表示されると共に、ステップ 1 4 0 1 で入力した店舗 I D 等の情報が自動消去される。

しかし、店舗 I D 及びWebマネー口座番号が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証 O K とする。

認証 O K となった場合には、認証サーバ 4 1 は金融機関 4 2 に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関 4 2 における与信処理（ステップ 1 4 0 4）によって与信 O K または与信 N G の与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたは Q R 決裁証明鍵を生成する（ステップ 1 4 0 5）。すなわち、与信 N G の与信結果が返送されてきた場合には、認証サーバ 4 1 は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機 1 に送信する。しかし、与信 O K であった場合には、図 3（d）で示したような 2 次元コードで構成された Q R 決裁証明鍵を生成し（ステップ 1 4 0 6）、これを携帯電話機 1 に送信する。この Q R 決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。

携帯電話機 1 では、受信した Q R 決裁証明鍵を図 1 2（a）に符号 1 2 0 1 で示したように表示部 1 1 に表示する。同時に、例えば「この携帯電話機で決裁できます。代金決裁時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は Q R 決裁証明鍵 1 2 0 1 が表示された状態の携帯電話機 1 を自動販売機 3 に付属した Q R コード読取装置 3 3 の読取部分に挿入装着する（ステップ 1 4 0 7）。そして、購入希望商品を自動販売機 3 の選択操作を行う（ステップ 1 4 0 8）。自動販売機 3 では、購入希望商品の選択操作によって代金が自動的に確定する（ステップ 1 4 0 9）。

Q R コード読取装置 3 3 は、携帯電話機 1 の表示部 1 1 に表示された Q R 決裁証明鍵 1 2 0 1 を読み取ると共に（ステップ 1 4 1 1）、標識 1 9、2 0 から携帯電話製造番号と携帯電話番号を読み取る（ステップ 1 4 1 0）。

自動販売機 3 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び Q R 決裁証明鍵 1 2 0 1 を決裁承認要求として認証サーバ 4 1 に送信する。この場合の通信回線は、P H S 電話機を使用したデータ通信を利用することができる。図 1 5 では、決裁番号及び個人認証の情報のみを決裁承認要求の中に含ませて送信していることを示している。

認証サーバ 4 1 は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 D B 4 4 の登録内容と照合して調べる（ステップ 1 4 1 2）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図 9）に登録した後（ステップ 1 4 1 3）、不正利用メッセージを自動販売機 3 および携帯電話機 1 に送信する。

不正利用メッセージを受信した携帯電話機 1 では、不正利用メッセージ自体が Q R 決裁証明鍵 1 2 0 1 の消去コマンドとして機能し、表示部 1 1 に表示されていた Q R 決裁証明鍵 1 2 0 1 が消去される。

自動販売機 3 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ 1 4 1 4）。しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも自動販売機 3 から受信した Q R 決裁証明鍵 1 2 0 1 の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ 4 1 は詳細決裁承認を店舗端末 2 2 に返信する。この詳細決裁承認の情報には、Q R 決裁証明鍵 1 2 0 1 と同様の情報の他に、当該利用者の購入履歴の情報が含まれている。

詳細決裁承認を受信した店舗端末 2 2 は、直ちに決裁処理を行う（ステップ 1 4 1 5）。そして、決裁終了メッセージを認証サーバ 4 1 に送信する。この決裁終了メッセージを受

信した認証サーバ41は利用者の購入履歴情報を更新する（ステップ1416）。この後、確認用の決裁内容を携帯電話機1に送信する。また、決裁終了情報を金融機関42に送信する。これにより、携帯電話機1の表示部11には、図13に示したような確認用の決裁内容1301が表示される（ステップ1417）。

決裁終了メッセージを受信した金融機関42では利用者のWebマネー口座又はクレジット口座から代金を引き落とす手続を行う。

以上により、携帯電話機1を使用して自動販売機での小額商品購入時の決裁を行うことができる。

以上の説明から明らかなように、本取引方法においても、自動販売機側に利用者のクレジット番号等の秘密情報を伝えることなく、認証サーバ41が発行したQR決裁証明鍵のみで代金決裁を行うことができる。

次に、インターネット上の電子店舗での商品購入時の決裁方法について図16及び図17のフローチャートを参照して説明する。

まず、利用者（商品購入者）は、自分が所持する携帯電話機1をモバイルショッピングモードに設定した後、入力手段14を使用し、インターネット上の店舗にアクセスし、購入しようとしている商品の番号、購入金額、受取方法を入力し、商品の発注を行う（ステップ1601）。

商品の発注を受けた店舗は、認証サーバ41に対して個人認証依頼を送信する。この個人認証依頼を受信した認証サーバ41は、携帯電話機1に対して自分の暗証番号（図7の706に登録した番号）、決裁方法及び店舗IDの入力要求を送信する。

そこで、携帯電話機1の利用者が自分の暗証番号（図7の706に登録した番号）、決裁方法及び店舗IDを入力する（ステップ1602）。すると、その内容はQR決裁証明鍵発行要求として認証サーバ41に送信される。ここで、決裁方法については、前述の例と同様である。

このQR決裁証明鍵発行要求を受信した認証サーバ41は、利用者の認証処理を行う（ステップ1603）。すなわち、QR決裁証明鍵発行要求の中に含まれる店舗IDによって店舗情報DB43を検索し、当該店舗IDの店舗が登録されているか否かを調べる。同様に、暗証番号、クレジットカード番号（またはWebマネー口座番号、デビットカード番号）によって利用者情報DB44を検索し、当該暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）の利用者が利用者DB44に登録されているか否かを調べる。その結果、店舗IDが登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機1に返信する（ステップ1604）。また、暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機1に返信する（ステップ1604）。携帯電話機1では、取引不可のメッセージが表示部11に表示されると共に、ステップ1602で入力した店舗ID等の情報が自動消去される。

しかし、店舗ID及び暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証OKとする。

認証OKとなった場合には、認証サーバ41は金融機関42に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関42における与信処理（ステップ1605）によって与信OKまたは与信NGの与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたはQR決裁証明鍵を生成する（ステップ1606）。すなわち、与信NGの与信結果が返送されてきた場合には、認証サーバ41は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機1に送信する。しかし、与信OKであった場合には、図3（d）で示したような2次元コードで構成されたQR決裁証明鍵を生成し（ステップ1607）、これを携帯電話機1に送信する。このQR決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。

携帯電話機1では、受信したQR決裁証明鍵を図12（a）に符号1201で示すように

表示部 1 1 に表示する。同時に、例えば「この携帯電話機で決裁できます。お客様が指定した受取店舗での代金決裁時に読取装置に挿入して下さい。」といったメッセージが表示される。

また、認証サーバ 4 1 は、店舗に対して、受託証明の発行要求を送信する。この受託証明の発行要求を受信した店舗は、受託番号、利用者氏名、商品番号、金額、決裁方法、受取方法を含む受託証明を生成し、認証サーバ 4 1 に返信する。この受託証明は、利用者から見れば商品注文書に相当するものである。

受託証明を受信した認証サーバ 4 1 は、Q R 決裁証明鍵 1 2 0 1 と受託証明とを一体化し、Q R 決裁証明鍵付き受託証明として携帯電話機 1 に送信する。

そこで、利用者は自分が指定した受取店舗に赴き、Q R 決裁証明鍵付き受託証明を表示部 1 1 に表示させた状態で受取店舗の店舗端末 2 2 に付属した Q R コード読取装置 2 1 の読取部分に挿入装着する（ステップ 1 6 0 8）。すると、Q R コード読取装置 2 1 は、携帯電話機 1 の表示部 1 1 に表示された Q R 決裁証明鍵付き受託証明を読み取ると共に（ステップ 1 6 0 9）、標識 1 9, 2 0 から携帯電話製造番号と携帯電話番号を読み取り（ステップ 1 6 1 0）、その読取結果を店舗端末 2 2 に転送する。

店舗端末 2 2 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び Q R 決裁証明鍵付き受託証明を決裁承認要求として認証サーバ 4 1 に送信する。この場合、Q R 決裁証明鍵付き受託証明については、認証サーバ自身が発行したものであることが分かればよいので、決裁番号及び個人認証といった一部の情報のみを送信してもよい。図 1 7 では、決裁番号及び個人認証の情報のみを決裁承認要求の中に含ませて送信していることを示している。

認証サーバ 4 1 は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 D B 4 4 の登録内容と照合して調べる（ステップ 1 6 1 1）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図 9）に登録した後（ステップ 1 6 1 3）、不正利用メッセージを店舗端末 2 2 および携帯電話機 1 に送信する。

不正利用メッセージを受信した携帯電話機 1 では、不正利用メッセージ自体が Q R 決裁証明鍵付き受託証明の消去コマンドとして機能し、表示部 1 1 に表示されていた Q R 決裁証明鍵付き受託証明が消去される。

店舗端末 2 2 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ 1 6 1 3）。そして、店員により商品の引渡し及び代金決裁ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末 2 2 から受信した Q R 決裁証明鍵付き受託証明の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ 4 1 は詳細決裁承認を店舗端末 2 2 に返信する。この詳細決裁承認の情報には、Q R 決裁証明鍵 1 2 0 1 と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決裁承認を受信した店舗端末 2 2 は、受信した詳細決裁承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ 1 6 1 4）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ 1 6 1 5）。

本人の購入意思の確定応答があったならば、商品を引き渡した上で、決裁ボタン操作によって決裁を完了する（ステップ 1 6 1 6）。決裁ボタン操作が行われた場合は、店舗端末 2 2 は決裁終了メッセージを認証サーバ 4 1 に送信する。この決裁終了メッセージを受信した認証サーバ 4 1 は利用者の購入履歴情報を更新する（ステップ 1 6 1 7）。この後、確認用の決裁内容を携帯電話機 1 に送信する。これにより、携帯電話機 1 の表示部 1 1 には、図 1 3 に示したような確認用の決裁内容 1 3 0 1 が表示される。また、認証サーバ 4 1 は、決裁終了情報を金融機関 4 2 に送信する。

以上により、携帯電話機 1 を使用してインターネット上の店舗で商品を選択し、その商品を利用者自身が指定した受取店舗で受け取り、決裁することができる。

以上の説明から明らかなように、本取引方法によれば、インターネット上の店舗側に利用者のクレジット番号等の秘密情報を伝えることなく、認証サーバ 4 1 が発行した Q R 決裁証明鍵のみで代金決裁を行うことができる。

このような方法を利用すれば、例えばインターネット上で映画等のチケットを発注し、その Q R 決裁証明鍵付き受託証明を携帯電話機 1 に格納しておき、映画館の入場口の読取装置に挿入することにより、チケットなしで入場するといった運用形態に活用することができる。

ここで、Q R 決裁証明鍵付き受託証明を表示部 1 1 に表示させて読取装置 2 1 に読み取らせる代わりに、Q R 決裁証明鍵付き受託証明をパーソナルコンピュータ (P C) に転送し、付属のプリンタで印刷し、受取店舗の読取装置で読み取らせる方法を採用することができる。この場合、プリンタの印字トナーまたはインクには、標識 1 9, 2 0 と同様の結晶粉末が混入されたものを用いる。

図 1 8 は、その手順を示すフローチャートである。このフローチャートは、図 1 6 の続きに該当する。

まず、携帯電話機 1 で Q R 決裁証明鍵付き受託証明を受信したならば、その Q R 決裁証明鍵付き受託証明をパーソナルコンピュータ (P C) に転送し (ステップ 1 6 2 0)、付属のプリンタで印刷する (ステップ 1 6 2 1)。図 1 9 (a) に印刷例を示す。

そこで、利用者は印刷された Q R 決裁証明鍵付き受託証明を自分が指定した受取店舗に持参し、受取店舗の店舗端末 2 2 に付属した Q R コード読取装置 2 1 の読取部分に挿入装着する。すると、Q R コード読取装置 2 1 は、印刷された Q R 決裁証明鍵付き受託証明を読み取り (ステップ 1 6 2 2)、その読取結果を店舗端末 2 2 に転送する。

店舗端末 2 2 は、印刷された Q R 決裁証明鍵付き受託証明の読取結果を図 1 7 の場合と同様に決裁承認要求として認証サーバ 4 1 に送信する。

認証サーバ 4 1 は、決裁承認要求を受信したならば、まず、Q R 決裁証明鍵付き受託証明の Q R 決裁証明鍵が自分自身で発行した正規のものであるかの正当性を調べる (ステップ 1 6 2 3)。この結果、正当なものでない場合には、不正利用であるものと判断し不正利用情報データベース (図 9) に登録した後 (ステップ 1 6 2 4)、不正利用メッセージを店舗端末 2 2 および携帯電話機 1 に送信する。

不正利用メッセージを受信した携帯電話機 1 では、不正利用メッセージ自体が Q R 決裁証明鍵付き受託証明の消去コマンドとして機能し、表示部 1 1 に表示されていた Q R 決裁証明鍵付き受託証明が消去される。

店舗端末 2 2 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される (ステップ 1 6 2 5)。そして、店員により商品の引渡し及び代金決裁ができない旨が利用者に口頭で通知される。

しかし、Q R 決裁証明鍵が正当なものであると認められた場合には、認証サーバ 4 1 は詳細決裁承認を店舗端末 2 2 に返信する。この詳細決裁承認の情報には、Q R 決裁証明鍵 1 2 0 1 と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決裁承認を受信した店舗端末 2 2 は、受信した詳細決裁承認の情報の全部または一部を利用者情報として表示部に表示する (ステップ 1 6 2 6)。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する (ステップ 1 6 2 7)。

本人の購入意思の確定応答があったならば、商品を引き渡した上で、決裁ボタン操作によって決裁を完了する (ステップ 1 6 2 8)。決裁ボタン操作が行われた場合は、店舗端末 2 2 は決裁終了メッセージを認証サーバ 4 1 に送信する。この決裁終了メッセージを受信した認証サーバ 4 1 は利用者の購入履歴情報を更新する (ステップ 1 6 2 9)。この後、確認用の決裁内容を携帯電話機 1 に送信する。これにより、携帯電話機 1 の表示部 1 1 には、図 1 3 に示したような確認用の決裁内容 1 3 0 1 が表示される。また、認証サーバ 4

1 は、決裁終了情報を金融機関 4 2 に送信する。

以上により、携帯電話機 1 を持参しない場合でも、インターネット上の店舗で注文した商品を利用者自身が指定した受取店舗で受け取り、決裁することができる。

この場合には、必ずしも Q R 決裁証明鍵付き受託証明を携帯電話機 1 からパーソナルコンピュータ（P C）に転送することは必要なく、直接にネットワーク端末としてのパーソナルコンピュータで受信して、プリンタで印刷することとしてもよい。

これら方法を利用すれば、印刷された Q R 決裁証明鍵付き受託証明を、インターネット上で注文した例えば映画等のチケットの代わりに利用するといった運用形態に活用することができる。図 1 9（b）に入場券の例を示す。

なお、前記各例では、商品の決済等に関する情報を発信するネットワーク端末と、Q R 決済証明鍵等のコードキャラクタ情報画像を受信するネットワーク端末として、同一の携帯電話機 1 を使用する場合を説明しているが、これに限られるものではなく、情報送信用のネットワーク端末と、コードキャラクタ情報画像受信用のネットワーク端末とを別の端末としてもよい。

これを利用することにより、第三者のネットワーク端末に対しコードキャラクタ情報画像を送信することもできる。従って、第三者に商品やギフト券を贈る代わりとして、第三者のネットワーク端末に送信したコードキャラクタ情報画像による決済を可能とすることができる。

以下、図 2 0～図 2 8 参照して、この場合の決済処理方法を説明する。

この場合、前記決済処理機関 4 には、贈答情報データベース（D B）が備えられ、また、前記認証サーバ 4 1 には贈答情報登録処理プログラム 4 1 2 が備えられることとなる。

前記贈答情報 D B は、例えば図 2 0 に示すように、贈り手側 I D 2 0 0 1、受け手側 I D 2 0 0 2、贈答内容 2 0 0 3、識別 I D 2 0 0 4、決済処理日 2 0 0 5 が格納されるようになっている。

また、前記贈答情報登録処理プログラムは、本システムを使用して特定の商品又は一定の金額の贈答を行う情報を贈答情報 D B に登録する際に使用するプログラムである。

本決済処理方法では、まず、注文主（商品の贈り手）は、情報送信用端末としての携帯電話機 1 をモバイルショッピングモードに設定した後、入力手段 1 4 を使用し、自分の暗証番号（図 7 の 7 0 6 に登録した番号）、決済方法、商品の受取り手側の利用者名及び利用者 I D 等の受取り手情報、贈答内容（この場合には、贈りたい商品の商品番号）を入力する（ステップ 2 1 0 1）。ここで、決済方法については、前述の例と同様である。

入力が終了したならば、送信操作を行う。すると、ステップ 2 1 0 1 で入力した情報が贈答情報送信要求として認証サーバ 4 1 に送信される。

この贈答情報送信要求を受信した認証サーバ 4 1 は、利用者の認証処理を行う（ステップ 2 1 0 2）。すなわち、贈答情報送信要求の中に含まれる暗証番号、クレジットカード番号（または Web マネー口座番号、デビットカード番号）によって利用者情報 D B 4 4 を検索し、当該暗証番号及びクレジットカード番号（または Web マネー口座番号、デビットカード番号）の利用者が利用者情報 D B 4 4 に登録されているか否かを調べる。また、受取り手情報としての利用者 I D 等によって、利用者情報 D B 4 4 を検索し、その結果、暗証番号及びクレジットカード番号（または Web マネー口座番号、デビットカード番号）が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 2 1 0 3）。携帯電話機 1 では、取引不可のメッセージが表示部 1 1 に表示されると共に、ステップ 2 1 0 1 で入力した暗証番号等の情報が自動消去される。

しかし、暗証番号及びクレジットカード番号（または Web マネー口座番号、デビットカード番号）、受取り手情報としての利用者 I D、利用者名が正しく登録されていた場合には、正規登録の利用者であるものと認証し、認証 O K とする。

認証 O K となった場合には、認証サーバ 4 1 は金融機関 4 2 に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関 4 2 における与信処理（ステップ 2 1 0 4）によって与信 O K または与信 N G の与信結果が返信されたならば、その与信結果に応じ

て、取引不可メッセージまたは贈答情報の送信を行う（ステップ2105）。すなわち、与信NGの与信結果が返送されてきた場合には、認証サーバ41は、残高不足等のメッセージを含む取引不可メッセージを贈り手側の携帯電話機1に送信する。しかし、与信OKであった場合には、ステップ2101で入力された受取り手側の携帯電話機1に贈答情報を送信する。この贈答情報としては、図24（a）に示すように贈り手の利用者名及び贈答内容としての商品名等が表示され、受取り手側により、贈答内容の受取りについて、拒否又は受諾の情報が認証サーバ41に返信される（ステップ2106）。認証サーバ41は、この返信を受け、拒否の情報が返信された場合には、受取り手側の携帯電話機1にその旨の確認メッセージを送信するとともに、贈り手側の携帯電話機に受取り拒否のメッセージを送信した後（図24（c）参照）、ステップ2101で入力した暗証番号等の情報が自動消去される。（ステップ2107）。しかし、受諾の情報が返信された場合には、認証サーバ41は、受取り手側の携帯電話機1に対して、商品の受取り方法の入力要求を送信する（図24（b）参照）。

そこで、携帯電話機1の利用者が受取りの店舗ID及び受取り方法を入力する（ステップ2108）。すると、その内容はQR決済証明鍵発行要求として認証サーバ41に送信される。

このQR決済証明鍵発行要求を受信した認証サーバ41は、店舗の認証処理を行う（ステップ2109）。すなわち、QR決済証明鍵発行要求の中に含まれる店舗IDによって店舗情報DB43を検索し、当該店舗IDの店舗が登録されているか否かを調べる。その結果、店舗IDが登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを受取り手側の携帯電話機1に返信する（ステップ2110）。携帯電話機1では、取引不可のメッセージが表示部11に表示されたのを確認した後、別の店舗ID等を入力することとなる。

しかし、店舗IDが正しく登録されていた場合には、正規登録の店舗であるものと認証し、認証OKとする。

認証OKとなった場合には、認証サーバ41は、図3（d）で示したような2次元コードで構成されたQR決済証明鍵を生成する。（ステップ2211）このQR決済証明鍵は、少なくとも決済番号、個人認証、氏名、決済方法の情報を含むもので構成される。

また、認証サーバ41は、店舗に対して、受託証明の発行要求を送信する。この受託証明の発行要求を受信した店舗は、受託番号、利用者氏名、商品番号、金額、決済方法、受取方法を含む受託証明を生成し、認証サーバ41に返信する。この受託証明は、利用者から見れば商品注文書に相当するものである。

受託証明を受信した認証サーバ41は、QR決済証明鍵1201と受託証明とを一体化し、QR決済証明鍵付き受託証明として受取り手側の携帯電話機1に送信する。

携帯電話機1では、受信したQR決済証明鍵を前記図12に符号1201で示すように表示部11に表示する。同時に、例えば「この携帯電話機で決済できます。代金決済時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は自分が指定した受取店舗に赴き、QR決済証明鍵付き受託証明を表示部11に表示させた状態で受取店舗の店舗端末22に付属したQRコード読取装置21の読取部分に挿入装着する（ステップ2112）。すると、QRコード読取装置21は、標識19、20から携帯電話製造番号と携帯電話番号を読み取ると共に（ステップ2113）、携帯電話機1の表示部11に表示されたQR決済証明鍵付き受託証明を読み取り（ステップ2114）、その読取結果を店舗端末22に転送する。

店舗端末22は、携帯電話機1から読み取った携帯電話製造番号、携帯電話番号及びQR決済証明鍵付き受託証明を決済承認要求として認証サーバ41に送信する。この場合、QR決済証明鍵付き受託証明については、認証サーバ41自身が発行したものであることが分かればよいので、決済番号及び個人認証といった一部の情報のみを送信してもよい。図23では、決済番号及び個人認証の情報のみを決済承認要求の中に含ませて送信していることを示している。

認証サーバ41は、決済承認要求を受信したならば、まず、携帯電話製造番号及び携帯電

話番号が正当か否かを利用者情報DB44の登録内容と照合して調べる（ステップ2115）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図9）に登録した後（ステップ2116）、不正利用メッセージを店舗端末22および受取り手側の携帯電話機1に送信する。さらに、贈り手側の携帯電話機1にも不正利用メッセージが送信される。

不正利用メッセージを受信した携帯電話機1では、不正利用メッセージ自体がQR決済証明鍵付き受託証明の消去コマンドとして機能し、表示部11に表示されていたQR決済証明鍵付き受託証明が消去される。

店舗端末22では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ2117）。そして、店員により商品の引渡し及び代金決済ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末22から受信したQR決済証明鍵付き受託証明の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ41は詳細決済承認を店舗端末22に返信する。この詳細決済承認の情報には、QR決済証明鍵1201と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決済承認を受信した店舗端末22は、受信した詳細決済承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ2118）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ2119）。

本人の購入意思の確定応答があったならば、商品を引き渡した上で、決済ボタン操作によって決済を完了する（ステップ2120）。決済ボタン操作が行われた場合は、店舗端末22は決済終了メッセージを認証サーバ41に送信する。

この決済終了メッセージを受信した認証サーバ41は贈り手側の利用者の購入履歴情報を更新する（ステップ2121）。この後、確認用の決済内容を贈り手側の情報発信用端末に送信する。これにより、例えば、贈り手側の携帯電話機1の表示部11には、図25に示したような確認メッセージ及び決済内容2501、2502が表示される（ステップ2122）。また、認証サーバ41は、決済終了情報を金融機関42に送信する。

以上により、贈り手側端末を使用して、特定の商品を選択し、その商品を受取り手側が指定した店舗で受け取り、決済することができる。

以上の説明から明らかなように、本取引方法によれば、店舗側や贈答品の受取り手側に贈り手のクレジット番号等の秘密情報を伝えることなく、認証サーバ41が発行したQR決済証明鍵のみで代金決済を行うことができる。また、贈答品の受取り手の認証をより確実に行うことができる。

なお、本取引方法では、受取り手側に対し贈答情報を送信し、贈答を受諾するか否かを選択することとしているが、予め贈答を受諾又は拒否する者を設定しておき、認証サーバにおいて、この設定に基づき贈答を受諾するか拒否するかの判定を行うこととしてもよい。この場合には、ステップ2106及びステップ2107に代えて、認証サーバにおける前記判定処理が行われることとなる。

また、このシステムにより贈られる贈答内容としては、特定の商品に限られず、一定金額のギフト券に相当する内容としてもよい。

図26及び図27は、その場合の手順を示すフローチャートである。図26のフローチャートは、図21の続きに該当する。

この場合には、前提として、図21のステップ2101において、贈答内容として商品番号に代えて一定の金額を入力することとなる。

その後、図21のフローチャートに示す処理がされた後、受取り手側の利用者が受取りの店舗ID及び商品の購入金額を入力する（ステップ2130）。すると、その内容はQR決済証明鍵発行要求として認証サーバ41に送信される。

このQR決済証明鍵発行要求を受信した認証サーバ41は、店舗及び購入金額の認証処理を行う（ステップ2131）。すなわち、QR決済証明鍵発行要求の中に含まれる店舗IDによって店舗情報DB43を検索し、当該店舗IDの店舗が登録されているか否かを調べる。また、贈答情報DBを検索し、入力された購入金額が、当該DBに格納された金額の範囲内であるかを調べる。その結果、店舗IDが登録されていなかった場合又は購入金額が贈答金額を超えている場合は、取引不可のメッセージを携帯電話機1に返信する（ステップ2132）。受取り手側の携帯電話機1では、取引不可のメッセージが表示部11に表示されたのを確認した後、別の店舗ID又は購入金額を入力することとなる。

しかし、店舗IDが正しく登録されており、かつ、贈答金額の範囲内で購入金額が入力されていた場合には、正規登録の店舗で購入可能な金額であるものと認証し、認証OKとする。

認証OKとなった場合には、認証サーバ41は、図3（d）で示したような2次元コードで構成されたQR決済証明鍵を生成し、携帯電話機1に送信する（ステップ2133）。このQR決済証明鍵は、少なくとも決済番号、個人認証、氏名、決済方法の情報を含むもので構成される。

携帯電話機1では、受信したQR決済証明鍵を図12（a）に符号1201で示すように表示部11に表示する。同時に、例えば「この携帯電話機で決済できます。代金決済時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は予め選択してあった購入希望商品を店舗端末22の店員に提示し、購入希望商品の発注を行う（ステップ2134）。店員は店舗端末によって購入希望商品の代金を入力する（ステップ2135）。

これと並行して、利用者はQR決済証明鍵1201が表示された状態の携帯電話機1を店舗端末22に付属したQRコード読取装置21の読取部分に挿入装着する（ステップ2136）。すると、QRコード読取装置21は、受取り手側の携帯電話機1の表示部11に表示されたQR決済証明鍵1201を読み取ると共に（ステップ2137）、標識19、20から携帯電話製造番号と携帯電話番号を読み取り（ステップ2138）、その読取結果を店舗端末22に転送する。

店舗端末22は、受取り手側の携帯電話機1から読み取った携帯電話製造番号、携帯電話番号及びQR決済証明鍵1201を決済承認要求として認証サーバ41に送信する。この場合、QR決済証明鍵1201については、認証サーバ自身が発行したものであることが分かればよいので、決済番号及び個人認証といった一部の情報のみを送信してもよい。

認証サーバ41は、決済承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報DB44の登録内容と照合して調べる（ステップ2139）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図9）に登録した後（ステップ2140）、不正利用メッセージを店舗端末22および受取り手側の携帯電話機1に送信する。さらに、贈り手側の携帯電話機1にも不正利用メッセージが送信される。

不正利用メッセージを受信した受取り手側の携帯電話機1では、不正利用メッセージ自体がQR決済証明鍵1201の消去コマンドとして機能し、表示部11に表示されていたQR決済証明鍵1201が消去される。

店舗端末22では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ2141）。そして、店員により代金決済ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末22から受信したQR決済証明鍵1201の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ41は詳細決済承認を店舗端末22に返信する。この詳細決済承認の情報には、QR決済証明鍵1201と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決済承認を店舗端末22は、受信した詳細決済承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ2142）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ2143）。

本人の購入意思の確定応答があったならば、決済ボタン操作によって決済を完了する（ステップ2144）。決済ボタン操作が行われた場合は、店舗端末22は決済終了メッセージを認証サーバ41に送信する。この決済終了メッセージを受信した認証サーバ41は贈り手側の利用者の購入履歴情報を更新する（ステップ2145）。この後、確認用の決済内容を贈り手側の携帯電話機1に送信する。また、決済終了情報を金融機関42に送信する。これにより、例えば、贈り手側の携帯電話機1の表示部11には、図25に示すような確認用の決済内容2501、2502が表示される（ステップ2146）。この決済内容2501、2502は、利用者自身が消去するまで保存することができる。ただし、QR決済証明鍵1201は1回限り有効であるので、所定時間後に自動的に消去される。

また、決済終了情報を受信した金融機関42では贈り手側の利用者の指定口座から代金を引き落とす手続を行う。

以上により、贈り手側端末を使用して、一定の金額を指定し、その金額の範囲内で受取り手側が自由に商品等を店舗で購入して、決済することができる。

以上の説明から明らかなように、本取引方法によれば、一定金額のギフト券に相当する内容を贈る場合であっても、店舗側や受取り手側に贈り手のクレジット番号等の秘密情報を伝えることなく、認証サーバ41が発行したQR決済証明鍵のみで贈り手側の口座から代金決済を行うことができる。また、受取り手の認証をより確実に行うことができる。

また、前記各例では、金融機関による決済を前提としているが、決済代金の一部又は全部についてサービスポイントによる決済を行う場合にも、本発明を利用することができる。

以下、図28～図30を参照して、この場合の決済処理方法を説明する。

この場合、前記決済処理機関4には、サービスポイントデータベース（DB）が備えられ、また、前記認証サーバ41にはサービスポイント登録処理プログラムが備えられることとなる。

図28は、サービスポイントDBの格納情報の一例を示す図であり、更新日2801、利用店舗名2802、加算ポイント数2803、利用ポイント数2804、サービスポイント残高2805が格納されるようになっている。このサービスポイント情報は、利用者別に更新日時順に格納されるものである。

また、サービスポイント登録処理プログラムは、本システムを使用して商品の購入等を行うことにより得たサービスポイントに基づき、決済処理を行うものである。

なお、ここでサービスポイントの利用としては、ポイント数により商品購入時に一定金額相当の割引をして決済処理する場合、ポイント数に応じて予め決められた商品と交換する場合等があるが、本実施の形態では、サービスポイントを商品購入代金として決済処理する場合を示している。

本決済処理方法では、まず、利用者（商品購入者）は、携帯電話機1をモバイルショッピングモードに設定した後、入力手段14を使用し、商品を購入しようとしている店舗の店舗ID、自分の暗証番号（図7の706に登録した番号）、商品の購入金額に相当するサービスポイントを入力する（ステップ2901）。ここで、店舗又は商品の識別情報を、店舗内に設置されている発信機等から外部入出力インタフェース17を介して取り込むようにしてもよい。

入力が終了したならば、送信操作を行う。すると、ステップ2901で入力した情報がQR決済証明鍵発行要求として認証サーバ41に送信される。

このQR決済証明鍵発行要求を受信した認証サーバ41は、店舗及び利用者の認証処理を行う（ステップ2902）。すなわち、QR決済証明鍵発行要求の中に含まれる店舗IDによって店舗情報DB43を検索し、当該店舗IDの店舗が登録されているか否かを調べる。同様に、暗証番号によって利用者情報DB44を検索し、利用者が利用者情報DB44に登録されているか否かを調べる。その結果、店舗IDが登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機1に

返信する（ステップ2903）。また、暗証番号が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機1に返信する（ステップ2903）。携帯電話機1では、取引不可のメッセージが表示部11に表示されると共に、ステップ2901で入力した店舗ID等の情報が自動消去される。

しかし、店舗ID及び暗証番号が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証OKとする。

認証OKとなった場合には、当該利用者のサービスポイントDBを検索し、サービスポイント残高の照会を行う（ステップ2904）。そして、この照会結果に応じて、取引不可メッセージまたはQR決済証明鍵を生成する（ステップ2905）。すなわち、照会の結果残高無しとされた場合には、認証サーバ41は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機1に送信する。しかし、残高有りであった場合には、図3（d）で示したような2次元コードで構成されたQR決済証明鍵を生成し（ステップ2906）、これを携帯電話機1に送信する。このQR決済証明鍵は、少なくとも決済番号、個人認証、氏名の情報を含むもので構成される。

携帯電話機1では、受信したQR決済証明鍵を図12（a）に符号1201で示すように表示部11に表示する。同時に、例えば「この携帯電話機で決済できます。代金決済時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は予め選択してあった購入希望商品を店舗端末22の店員に提示し、購入希望商品の発注を行う（ステップ2907）。店員は店舗端末に購入希望商品の代金を入力することにより、この代金に相当するポイント数を算出する（ステップ2908）。

これと並行して、利用者はQR決済証明鍵1201が表示された状態の携帯電話機1を店舗端末22に付属したQRコード読取装置21の読取部分に挿入装着する（ステップ2909）。すると、QRコード読取装置21は、携帯電話機1の標識19、20から携帯電話製造番号と携帯電話番号を読み取ると共に（ステップ2910）表示部11に表示されたQR決済証明鍵1201を読み取り（ステップ2911）、その読取結果を店舗端末22に転送する。

店舗端末22は、携帯電話機1から読み取った携帯電話製造番号、携帯電話番号及びQR決済証明鍵1201を決済承認要求として認証サーバ41に送信する。この場合、QR決済証明鍵1201については、認証サーバ自身が発行したものであることが分かればよいので、決済番号、個人認証といった一部の情報のみを送信してもよい。図30では、決済番号及び個人認証の情報のみを決済承認要求の中に含ませて送信していることを示している。

認証サーバ41は、決済承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報DB44の登録内容と照合して調べる（ステップ2912）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図11）に登録した後（ステップ2913）、不正利用メッセージを店舗端末22および携帯電話機1に送信する。

不正利用メッセージを受信した携帯電話機1では、不正利用メッセージ自体がQR決済証明鍵1201の消去コマンドとして機能し、表示部11に表示されていたQR決済証明鍵1201が消去される。

店舗端末22では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ2914）。そして、店員により代金決済ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末22から受信したQR決済証明鍵1201の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ41は詳細決済承認を店舗端末22に返信する。この詳細決済承認の情報には、QR決済証明鍵1201と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決済承認を店舗端末２２は、受信した詳細決済承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ２９１５）。店員は、その表示内容と購入希望商品の内容及び代金に相当するポイント数を見て、利用者本人に購入意思を確認する（ステップ２９１６）。

本人の購入意思の確定応答があったならば、決済ボタン操作によって決済を完了する（ステップ２９１７）。決済ボタン操作が行われた場合は、店舗端末２２は決済終了メッセージを認証サーバ４１に送信する。この決済終了メッセージを受信した認証サーバ４１は利用者の購入履歴情報及びサービスポイント情報を更新する（ステップ２９１８）。この後、確認用の決済内容を携帯電話機１に送信する。この決済内容は、利用者自身が消去するまで保存することができる。ただし、ＱＲ決済証明鍵１２０１は１回限り有効であるので、所定時間後に自動的に消去される。

以上により、携帯電話機１を使用して、一般店舗での商品購入時にサービスポイントを利用した決済を行うことができる。

以上の説明から明らかなように、本取引方法によれば、サービスポイントを利用した決済においても、認証サーバ４１が発行したＱＲ決済証明鍵のみで行うことができ、ポイントカード等を不要とすることができる。また、サービス利用者の認証をより確実に行うことができる。

以上の各例で示した方法は、金銭的な決済を介することを必須とするものではなく、入場券等のチケットの代わりや、商品等の受取証の代わりに用いることも可能なものである。なお、上記で説明した手順は、金融機関等の関係で一部の手順を変更して実施することができる。また、認証サーバ４１が実行する手順は決済用のプログラムとしてＣＤ－ＲＯＭ等の記録媒体に記録して決済システム構築事業者に提供することができる。

また、携帯電話製造番号及び携帯電話番号の標識は、特殊な結晶粉末を混入した記録材料で記録しているが、これ以外に物理的に真偽判定が可能な記録形式で記録する方法であってもよい。

なお、ＩＣカード（ＵＩＭカード）を搭載した携帯電話機等を用いる次世代移動通信サービスでは、携帯電話番号等を前記ＩＣカードに書き込み、ＩＣカードの差し替えにより、異なる端末で同一の携帯電話番号の使用をするといった運用形態が考えられている。

そこで、この場合には、前記ＩＣカードに前記図３（ｃ）に示すような標識を貼り付け又は印刷することとしてもよい。

また、この場合には、携帯電話機等に設けられたスロット等にＩＣカードを差し込んだ状態で、前記標識を外部の読取装置で読取り可能とすることが必要となる。

この場合に用いられる携帯電話機の例を図３１，３２を参照して説明する。

図３１，３２は本実施の形態に用いられる携帯電話機の部分斜視図であり、各図において、３００は携帯電話機に搭載される携帯電話番号等の情報を保存したＩＣカードであり、その表面には、前記図３（ｃ）に示すような標識３１１が貼り付けまたは印刷されている。なお、この標識３１１には、携帯電話機の製造番号に代えて、各ＩＣカード又は所有者の識別情報が携帯電話番号とともに記録されている。

本実施の形態では、例えば、図３１（ａ）に示すように、携帯電話機１の裏面側等において、ＩＣカードに貼り付けされた標識３１１が図の矢印に示す読取方向から視認可能なように、ＩＣカードを取り付け可能とする凹部３００を形成する。これにより、携帯電話機１の筐体に標識を貼り付けた場合と同様に、前記読取装置２２により、読取りが可能となる。

また、図３１（ｂ）に示すように、携帯電話機１に設けられたＩＣカード差込用スロット３０１を設けるとともに、当該スロット３０１にＩＣカード３１０が差し込まれた状態で、前記標識３１１が位置する部位に、外部の読取装置から当該標識が読取（視認）可能となるような開口部３０２を形成することとしてもよい。この開口部３０２は、図の矢印に示す読取方向から前記標識３１１が視認可能であれば、透過性の樹脂材等により、その表面側をシールドしてもよい。

また、外部の読取装置により前記標識３１１が読取可能であれば、他の構成を用いてもよ

く、例えば、携帯電話機の筐体全体を内部が視認可能な透過性の樹脂材等により形成することとしてもよい。

これにより、次世代移動通信サービスに対応した携帯電話機等においても、本発明を適用することができるとともに、ＩＣカード内にクレジットカード番号等のデータを保存する必要がなくなり、セキュリティ性を高くすることができる。

なお、携帯電話機１において、前記標識３１１の読取装置を設け、その読取装置により前記標識を読み取り、その読取情報を店舗側端末に送信することとしてもよい。

この場合には、例えば、図３２（ａ）に示すように、前記スロット３０１に差し込まれたＩＣカードの標識３１１が位置する部位に、前記制御部１３（図２（ａ）参照）に接続された読取センサ部３０３を設ける。これにより、当該読取センサ部３０３で読取った標識３１１の情報を携帯電話機１の送信手段を介して、前記認証サーバ４１に送信することができる。なお、標識３１１の情報の読取処理を、前記スロット３１１にＩＣカードを差し込む途中で行うこととしてもよく、この場合には、前記スロット内において前記標識３１１が通過する部位に対応する部位の一部にセンサ部を設けることとしてもよい。

また、ＩＣカード３１０を携帯電話機１に差し込むものに限らず、図３２（ｂ）に示すように、ＩＣカード３１０の一部を、携帯電話機１の側面に形成されたスリット３０４に挿入した状態で、図の矢印に示すスライド方向にスライドさせることで、図外のセンサ部により、ＩＣカード３１０内の情報を読み取らせるものが考えられる。この場合には、ＩＣカード３１０の一部を前記スリット３０４内をスライドさせる際に、前記スリット３０４内において前記標識３１１が通過する部位に対応する部位の一部に、読取センサ部３０５を設けることとしてもよい。

また、ＩＣカード３１０として、無線または光による非接触型ＩＣカードを用いる場合には、各店舗等に設置された読取装置にＩＣカード３１０を挿入することにより、標識３１１を直接読み取らせることとしてもよく、また、前記の例と同様に、携帯電話機１に読取装置を備えることとしてもよく、また、ＩＣカード３１０内の情報と同様に、無線又は光により、前記標識３１１の情報を認識させることとしてもよい。

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成17年5月26日(2005.5.26)

【国際公開番号】W02002/008981

【年通号数】公開・登録公報2004-001

【出願番号】特願2002-514614(P2002-514614)

【国際特許分類第7版】

G 0 6 F 17/60

G 0 6 K 17/00

G 0 6 K 19/06

G 0 6 K 19/07

H 0 4 Q 7/38

【F I】

G 0 6 F 17/60 4 1 4

G 0 6 F 17/60 4 2 2

G 0 6 F 17/60 5 0 6

G 0 6 F 17/60 5 1 2

G 0 6 F 17/60 Z E C

G 0 6 K 17/00 L

G 0 6 K 19/00 E

G 0 6 K 19/00 J

H 0 4 B 7/26 1 0 9 S

【手続補正書】

【提出日】平成15年5月29日(2003.5.29)

【手続補正1】

【補正対象書類名】手続補正書

【補正対象項目名】手続補正1

【補正方法】変更

【補正の内容】

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【書類名】明細書

【発明の名称】商取引方法およびネットワーク端末並びに商取引システム

【特許請求の範囲】

【請求項1】決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備えるとともに、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、
 商取引に関する決済証明鍵情報を決済承認機関装置から受信するステップと、
 受信した決済証明鍵情報を前記表示手段に表示させるステップと、
 前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送するステップと、
 前記標識に記録された識別情報を読取らせて前記決済端末に転送するステップと、
 前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別情報とを前記決済

承認機関装置に送信し、前記識別情報が決済承認機関装置に予め登録された正規のものであるか否かを認証させるステップと、
前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関装置から商品購入元の決済端末に送信するステップと、
前記決済承認の情報に基づき、商品購入元の決済端末により商品代金の決済を実行するステップと

を備えることを特徴とする商取引方法。

【請求項2】決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備えるネットワーク端末と、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するICカードを用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、
商取引に関する決済証明鍵情報を決済承認機関装置から受信するステップと、
受信した決済証明鍵情報を前記表示手段に表示させるステップと、
前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送するステップと、
前記標識に記録された識別情報を読み取らせて前記決済端末に転送するステップと、
前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別情報を前記決済承認機関装置に送信し、前記識別情報が決済承認機関装置に予め登録された正規のものであるか否かを認証させるステップと、
前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関装置から商品購入元の決済端末に送信するステップと、
前記決済承認の情報に基づき、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップと
を備えることを特徴とする商取引方法。

【請求項3】前記ネットワーク端末は、商取引に関する情報を入力する入力手段として、商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含む入力手段を有し、
少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商取引に関する情報を前記入力手段から入力するステップと、
入力された商取引に関する情報を決済承認機関装置に送信し、前記画像情報を復号化させ、商品提供元の認証と購入者自身の認証と与信の結果に応じて生成された決済証明鍵情報を受信するステップと
をさらに備えることを特徴とする請求項1又は請求項2のいずれかに記載の商取引方法。

【請求項4】商取引に関する決済証明鍵情報を決済承認機関装置から受信して表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備え、前記表示手段に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送して、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行する商取引方法に用いられるネットワーク端末であって、
予め決済承認機関に登録された識別情報を記録した標識を有し、当該標識は所定波長の照射光に対し所定波長の反射光により前記識別情報を出射することを特徴とするネットワーク端末。

【請求項5】前記ネットワーク端末は、商取引に関する情報を入力する入力手段を備え、当該入力手段には、商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含むことを特徴とする請求項4に記載のネットワーク端末。

【請求項6】決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段を備えるとともに、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するネットワーク端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える

商取引システムであって、
前記決済承認機関装置が、
商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、
前記決済証明鍵情報の一部又は全部と前記識別標識の読取結果としての識別情報を前記商品提供元装置から受信し、前記識別情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、
前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信し、購入者が発注した商品の引渡し及び代金の決済を実行させる手段と
を備えることを特徴とする商取引システム。

【請求項 7】 決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを備えるネットワーク端末と、予め記録された識別情報を所定波長の照射光に対し所定波長の反射光により出射する標識を有する IC カードと、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、
前記決済承認機関装置が、
商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、
前記決済証明鍵情報の一部又は全部と前記識別標識の読取結果としての識別情報を前記商品提供元装置から受信し、前記識別情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、
前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品提供元装置に送信する手段と
を備えることを特徴とする商取引システム。

【請求項 8】 前記ネットワーク端末は、少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商取引に関する情報を入力する入力手段を有し、当該入力手段として商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含むものとし、
前記決済承認機関装置は、前記撮像手段により撮像され、送信された画像情報を復号化する復号化手段をさらに備えたことを特徴とする請求項 6 又は請求項 7 に記載の商取引システム。

【発明の詳細な説明】

【0001】

技術分野

本発明は、携帯電話機等のネットワークに接続可能な端末を用いてスーパーマーケット等の各種の店舗、インターネットのサーバ上に開設されている電子店舗、あるいは飲料水等の自動販売機で購入する商品の代金の決済を行う商取引方法及び装置並びにシステムに関するものである。

【0002】

背景技術

携帯電話機に WWW 閲覧機能 (World Wide Web) を付加したことにより、携帯電話機を使用してインターネットにアクセスし、各種の情報、物品、役務サービスを閲覧し、必要に応じて、それらの情報、物品、役務サービスの提供を注文するという取引形態が急速に拡大している。ここで、本発明では、形状を有しない音楽ソフトなどの情報 (コンテンツ)、形状を有する物品、宅配サービス、介護サービスなどの役務サービスを全て商取引の対象となる商品と定義する。この場合、公共機関が提供する無料の介護サービスもあるが、無料であっても取引の対象となる商品に含むものとする。

しかし、携帯電話機を使用して商品の発注を行ったとしても、その決済方法としては、銀行振込みや現金の送付、商品到着時の代金引換などの従来の商慣習に従った方法が踏襲さ

れている。

最近では、このような旧来方法に代えて、商品の注文と同時に、クレジットカード番号を商品提供元（店舗）に通知し、クレジットカード会社を通じて決済する方法が実施されている。

しかし、この決済方法は、クレジットカード会社と本人だけが知るべき番号あるいは情報が外部に漏れないことを前提にしており、外部に漏れた場合には悪用される危険性がある。

そこで、2001年5月から開始される次世代移動通信サービスでは、携帯電話機にUIM（User Identity Module）と呼ばれるICカードを搭載し、このICカード内の暗号プログラムによりクレジットカード番号等の秘密データを暗号化し、決済を行うという方法が考えられている。

しかし、暗号プログラムにより暗号化して保存したとしても、携帯電話機自体を紛失した場合には、不正な第三者に解読されてしまい、悪用される危険性がある。特に、ICカード内にはクレジットカード番号のみでなく、銀行口座番号や保険証番号、電子マネーなどの他の秘密データも同時に保存する形態が多くなると考えられるので、不正な第三者に解読された場合の危険性は旧来の決済方法よりも高くなるという問題がある。

また、非接触型ICカード同様、無線を利用したネットワークは特に有線ネットワーク以上に不正アクセスを含むハッキング等、情報が外部に漏れる可能性が高くなるという問題がある。

また、不正な店舗の出現により、店舗での決済時に秘密データが盗聴され、悪用される危険性がある。

また、携帯電話機自体のコストも上昇し、さらに電力消費も増加し、電池寿命が短くなるという問題がある。

本発明はこのような問題を解決するためになされたものであり、その目的は、クレジットカード番号等の秘密データを本人認証機関やクレジットカード会社以外に開示することなく本人認証を行い、安全に購入商品の決済を行うことができる商取引方法及び装置、並びにシステムを提供することにある。

【0003】

発明の開示

上記目的を達成するために、本発明の商取引方法は、以下のように構成したことを特徴とするものである。

すなわち、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備えるとともに、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するネットワーク端末を用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、商取引に関する決済証明鍵情報を決済承認機関装置から受信するステップと、受信した決済証明鍵情報を前記表示手段に表示させるステップと、前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送するステップと、前記標識に記録された識別情報を読取らせて前記決済端末に転送するステップと、前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別情報とを前記決済承認機関装置に送信し、前記識別情報が決済承認機関装置に予め登録された正規のものであるか否かを認証させるステップと、前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関装置から商品購入元の決済端末に送信するステップと、前記決済承認の情報に基づき、商品購入元の決済端末により商品代金の決済を実行するステップとを備えることを特徴とする。

また、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備えるネットワーク端末と、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するICカードを用い、商品提供元が提供する取引対象の商品に関する決済を行う商取引方法であって、商取引に関する決済証明鍵情報を決済承認

機関装置から受信するステップと、受信した決済証明鍵情報を前記表示手段に表示させるステップと、前記ネットワーク端末に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送するステップと、前記標識に記録された識別情報を読取らせて前記決済端末に転送するステップと、前記決済端末に転送した前記決済証明鍵情報の一部又は全部と前記識別情報を前記決済承認機関装置に送信し、前記識別情報が決済承認機関装置に予め登録された正規のものであるか否かを認証させるステップと、前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関装置から商品購入元の決済端末に送信するステップと、前記決済承認の情報に基づき、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行するステップとを備えることを特徴とする。

また、前記ネットワーク端末は、商取引に関する情報を入力する入力手段として、商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含む入力手段を有し、少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商取引に関する情報を前記入力手段から入力するステップと、入力された商取引に関する情報を決済承認機関装置に送信し、前記画像情報を復号化させ、商品提供元の認証と購入者自身の認証と与信の結果に応じて生成された決済証明鍵情報を受信するステップとをさらに備えることを特徴とする。

本発明のネットワーク端末は、商取引に関する決済証明鍵情報を決済承認機関装置から受信して表示する表示手段と、通信網を介して商品の決済に関する情報を送受信する送受信手段とを備え、前記表示手段に表示された決済証明鍵情報を商品購入元に設置された決済端末に転送して、購入者が選択した商品の代金の決済を商品購入元の決済端末により実行する商取引方法に用いられるネットワーク端末であって、予め決済承認機関に登録された識別情報を記録した標識を有し、当該標識は所定波長の照射光に対し所定波長の反射光により前記識別情報を出射することを特徴とする。

前記ネットワーク端末は、商取引に関する情報を入力する入力手段を備え、当該入力手段には、商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含むことを特徴とする。

本発明の商取引システムは、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段を備えるとともに、予め決済承認機関装置に登録された識別情報を記録した標識として、所定波長の照射光に対し所定波長の反射光により前記識別情報を出射する標識を有するネットワーク端末と、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、前記決済承認機関装置が、商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、前記決済証明鍵情報の一部又は全部と前記識別標識の読取結果としての識別情報を前記商品提供元装置から受信し、前記識別情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品購入元の決済端末に送信し、購入者が発注した商品の引渡し及び代金の決済を実行させる手段とを備えることを特徴とする。

また、決済に関する情報を表示する表示手段と、通信網を介して商品の決済に関する情報を送受する送受信手段とを備えるネットワーク端末と、予め記録された識別情報を所定波長の照射光に対し所定波長の反射光により出射する標識を有するICカードと、決済に関する認証および承認を行う決済承認機関装置と、商品提供元において商品の代金の決済を行う商品提供元装置とを備える商取引システムであって、前記決済承認機関装置が、商取引に関する決済証明鍵情報を生成し、前記ネットワーク端末に送信し表示させる手段と、前記決済証明鍵情報の一部又は全部と前記識別標識の読取結果としての識別情報を前記商品提供元装置から受信し、前記識別情報が決済承認機関に予め登録された正規のものであるか否かを認証する手段と、前記識別情報の認証結果に応じて前記決済証明鍵情報に対応した決済承認の情報を決済承認機関から商品提供元装置に送信する手段を備えることを特徴とする。

また、前記ネットワーク端末は、少なくとも商品提供元又は商品の識別情報、決済方法、購入金額及び購入者自身の暗証番号を含む商取引に関する情報を入力する入力手段を有し、当該入力手段として商品提供元又は商品の識別情報を符号化した画像情報を撮像する撮像手段を含むものとし、前記決済承認機関装置は、前記撮像手段により撮像され、送信された画像情報を復号化する復号化手段をさらに備えたことを特徴とする。

【 0 0 0 4 】

発明を実施するための最良の形態

以下、本発明の実施の形態を添付図面により詳細に説明する。

図 1 は、本発明の商取引方法を実施するシステムの全体構成の実施形態を示すシステム構成図であり、商品購入者が使用するネットワーク端末としての携帯電話機 1、商品提供元の店舗 2、飲料水等の自動販売機 3、決済承認機関 4 で構成され、これらが通信網 5 で接続されている。通信網 5 は、無線回線と有線回線及びインターネット網を含むものである。ここで、ネットワーク端末とは、インターネット等のネットワークに接続可能な端末を示すものであり、以下の例に示す携帯電話機 1 の他、P H S、P D A、パーソナルコンピュータ、デジタルテレビ等、種々のものが含まれる。

携帯電話機 1 は、インターネット網に接続可能な機能を有する市販の携帯電話機であり、図 2 (a) の概略ブロック図に示すように、表示部 1 1、無線送受信部 1 2、制御部 1 3、入力部 1 4、送受話器 1 5、メモリ 1 6、外部入出力インタフェース 1 7 を備えている。表示部 1 1 にはインターネット接続モードにおいて、図 2 (b) に示すように、ニュース、モバイルバンキング、カード／証券／保険、モバイルショッピングなどのインターネット接続メニューが表示されるようになっている。

外部入出力インタフェース 1 7 は、I r d a 等の赤外線インタフェース及びブルーツースなどの微弱電波インタフェース等の無線通信インターフェースを含むものであり、本実施形態では、店舗の識別番号を店舗内に設置された発信機から受信する場合に使用される。また外部入出力インターフェース 1 7 には、携帯電話機接続型又は携帯電話機内蔵型のバーコード読取装置のインタフェースを含み、このバーコード読取装置により、バーコード情報で表示された店舗の識別情報又は商品の識別情報等を読取ることとしてもよい。さらに、携帯電話機接続型又は携帯電話機内蔵型のカメラを含み、このカメラにより、コードキャラクタ情報画像により表示された各店舗の識別情報又は商品の識別情報を、画像データとして取り込むこととしてもよい。この場合は、画像データとして取り込んだコードキャラクタ情報画像をデコードするためのプログラムを、前記決済承認機関 4 の認証サーバ内に設けておき、携帯電話機から送信されたコードキャラクタ情報画像を前記プログラムでデコードすることにより、店舗又は商品の識別情報を認識することとなる。また、前記プログラムは、携帯電話機内に設けることとしてもよく、この場合には、携帯電話機内でコードキャラクタ情報画像をデコードすることにより認識された前記各識別情報を、前記認証サーバに送信することとなる。

以上のような外部入出力インターフェース 1 7 を使用することにより、入力部 1 4 の操作を行わずに店舗又は商品の識別情報の入力を行うことができる。ここで、商品の識別情報としては、商品名、商品種別、金額等が該当する。

なお、商品の金額を入力するのは、店員の金額入力に代わるものではなく、セルフスキヤニング行為を含むものであり、決済金額情報を購入者が事前に知るためのものである。本実施形態の携帯電話機 1 には、図 3 (a)、(b) の正面図及び側面図に示すように、機器製造番号を図 3 (c) のようなバーコード 3 1 で記録した第 1 の標識 1 9 と、携帯電話番号をバーコード 3 1 で記録した第 2 の標識 2 0 が貼り付けられている。

これらの標識 1 9、2 0 のバーコードは、図 4 (a) に示すように、所定波長 λa の照射光に対し記録情報を所定波長 λa または λb の反射光により出射する結晶粉末を混入した印刷材料で印刷されている。この結晶粉末は、米国 S U N S T O N E 社が提供しているものであり、医薬品や紙幣の真贋識別用に採用されているものである。この場合、用途及び使用システムに応じて、照射光の波長と出射光の波長が異なるように特性が調整されている。

本発明では、このような特殊な結晶粉末を混入した記録インクまたはトナーで機器製造番号及び携帯電話番号のバーコードを標識 19, 20 に印刷し、これを携帯電話機 1 の正面あるいは側面に貼り付け、その標識 19, 20 に記録されたバーコードを所定波長 λa の照射光で読み取るようにしている。

このような特殊な記録インクまたはトナーで記録した機器製造番号及び携帯電話番号の標識 19, 20 を携帯電話機 1 に貼り付けておくことにより、予め定めた波長の照射光以外では機器製造番号及び携帯電話番号を読み取ることができない。よって、機器製造番号及び携帯電話番号を決済承認機関 4 に事前登録しておくことにより、当該携帯電話機 1 が本システムでの商取引を利用できる正当な機器であるか否かを識別することができる。また、側面の標識 20 は、携帯電話機 1 の改造を防止できる役目を果たしている。

なお、この場合には、必ずしも前記標識の貼り付けを必要とするものではなく、携帯電話機の筐体自体に、前記記録インク等により、前記標識を印刷することとしてもよい。

標識 19, 20 のバーコードは、図 4 (b) に示すような断面構成の読取装置 40 内に挿入され、予め定めた波長の照射光を照射することによって読み取られる。この読取装置 40 は、店舗 2 や自動販売機 3 に設置される。

一方、表示部 11 には図 3 (d) に示すようなコードキャラクタ情報画像としての 2 次元コード 32 で構成された決済承認鍵情報が表示される。この 2 次元コード 32 は、日本自動車工業会及び日本文具協会の標準コードに設定されているものである。これについては、例えば特開平 10-214317 号公報等で開示されているので、ここでの詳細な説明は省略する。

この 2 次元コード（以下、QR コードと言う）を用いれば、携帯電話機 1 の表示部の面積内で約 7000 文字（数字）をコード化して記録することができる。本発明では、この QR コードを決済承認鍵の情報を表現するために使用している。詳しくは、QR コードで構成された決済承認鍵の情報を携帯電話機 1 に転送して図 3 (a) のように表示部 11 に表示させ、この表示状態の携帯電話機 1 を標識 19, 20 の読取共用の読取装置 21 に挿入し、決済承認鍵の情報を読み取るようにしている。

QR コードを用いた場合、図 3 (d) に示すように、3ヶ所に配置した切り出しシンボル 33~35 によって 360 度のどの方向からでも記録内容を読み取ることができるので、読取部との位置関係の束縛がなくなり、一般の利用者が読み取り部に挿入して読み取らせる場合に好適である。また、位置関係を厳密に定める必要がないため、その分だけ読取時間も短縮することができる。さらに、コードの一部に汚れや破損があっても誤りを訂正できるので、読取ミスが減少する。特に本発明のように、携帯電話機 1 の表示部に表示させた状態で読み取らせる場合、表示部の汚れ等によって読取ミスが発生することが考えられるが、QR コードを用いることによって表示部の汚れ等に起因する読取ミスを減少させることができる。

図 1 に戻り、店舗 2 には標識 19, 20 と QR コードの読取共用の読取装置 21 が設置され、読み取った標識 19, 20 と QR コードを POS 端末で構成される店舗端末 22 に入力し、店舗端末で代金の決済を行うようになっている。自動販売機 3 にも標識 19, 20 と QR コードの読取共用の読取装置 33 が設置されている。

一方、承認機関 4 は、認証サーバ 41 と金融機関（銀行またはクレジット会社）42、店舗情報データベース (DB) 43、利用者情報データベース (DB) 44、購入履歴データベース (DB) 45 を備えている。

認証サーバ 41 は、携帯電話機 1 からの本人認証及び店舗認証要求に対して、本人認証及び店舗認証さらには金融機関 42 に対する与信照会を行い、予め登録してある本人および店舗であり、しかも金融機関 42 から与信 OK の回答があった場合には商品の代金決済を携帯電話機 1 を使用して許可する処理を行うものであり、店舗登録処理プログラム 410、利用者登録処理プログラム 411、購入履歴管理プログラム 412、不正利用管理プログラム 413、認証処理プログラム 414、QR 決済鍵生成プログラム 415、送受信プログラム 416 を備えている。なお、各データベース 43、44、45 のデータを暗号化して保存するための暗号化／複合化プログラムが必要に応じて組み込まれる。また、QR

コードを暗号化して送信するための暗号化プログラムおよび復号するための復号プログラムが組み込まれる。QRコードを暗号化することにより、不正な取引をさらに困難にすることができる。

店舗登録処理プログラム410は、本システムを使用して決済を行う店舗（自動販売機やインターネット上の電子店舗を含む）を店舗情報DB43に登録する際に使用するプログラムである。また、利用者登録処理プログラム411は本システムを使用して決済を行う利用者（商品購入者）を利用者情報DB44に登録する際に使用するプログラムである。

購入履歴管理プログラム412は、利用者（商品購入者）が購入した商品の購入履歴の情報を購入履歴DB45に格納する際に使用するプログラムである。

不正利用管理プログラム413は、店舗情報DB43及び利用者情報DB44に予め登録されていない店舗及び利用者が本システムにアクセスした場合、あるいは携帯電話機1の機器製造番号や電話番号を不正に書き換えてアクセスした場合の店舗識別番号あるいは携帯電話機1の機器製造番号や電話番号を不正利用情報データベース（図9）に登録する際に使用するプログラムである。

認証処理プログラム414は、携帯電話機1からの本人認証及び店舗認証要求に対して、本人認証及び店舗認証さらには金融機関42に対する与信照会を行い、予め登録してある本人および店舗であり、しかも金融機関42から与信OKの回答があった場合には商品の代金決済を携帯電話機1を使用して許可する処理を行うものである。

QR決済鍵生成プログラム415は、商品の代金決済を許可するために、QRコードで構成された決済証明鍵の情報を生成して携帯電話機1に渡すプログラムである。QRコードで構成された決済証明鍵の情報（以下、QR決済証明鍵情報）は、店舗が購入者本人及び店舗の認証結果を含む詳細な決済承認の情報を認証サーバ41から受け取るための鍵となる情報であり、本システムでこのQR決済証明鍵情報を店舗の読取装置21で読み取り、その読み取ったQR決済証明鍵情報を店舗端末から認証サーバ41に送信することにより、店舗端末22では購入者本人及び店舗の認証結果を含む詳細な決済承認の情報を受け取ることができる。この場合、読取装置21で読み取ったQR決済証明鍵情報が認証サーバ41で生成したものと異なる場合には決済承認の情報を取得することができない。

送受信プログラム416は、利用者および店舗からのアクセスに対し、決済に必要な情報を送受信するプログラムである。

図6は、店舗情報DBの登録情報の一例を示すものであり、店舗ID601、店舗名称602、住所603、電話番号604が登録されるようになっている。

図7は、利用者情報DBの登録情報の一例を示す図であり、利用者ID701、利用者名702、住所703、携帯電話製造番号（機器製造番号）704、携帯電話番号705、本システムを利用する際の暗証番号706、性別707、生年月日708、デビットカード番号709、クレジットカード番号710、Webマネー口座番号711、個人特徴情報712が登録されるようになっている。

Webマネー口座番号711は、飲料水などの小額商品を自動販売機で購入する場合にWebマネーによって決済する際に使用するものである。また、個人特徴情報712は、本人の写真等を登録しておき、店舗での決済時に店員が写真などの特徴によって本人確認を行えるようにするためのものであり、利用者本人の希望に応じて登録される。例えば、利用者本人の写真を登録しておけば、決済時に他人による悪用を店員が発見できるといふ利点がある。また、生年月日708により、未成年者であるか否かを発見でき、酒、煙草類の販売を差し止めることができる。この他に、運転免許証番号などを登録することができる。運転免許証番号などを登録しておくことによって、携帯電話機を利用して第三者である認証サーバ41から本人認証証明を発行することも可能である。

図8は、購入履歴DBの格納情報の一例を示す図であり、利用日時801、利用店舗名802、決済金額803、今月分利用金額累計804、サービスポイント累計805、前回利用日806が格納されるようになっている。なお、この購入履歴情報は、利用者別に利用日時順に格納されるものである。

図9は、不正利用情報データベースに格納される情報の一例を示す図であり、不正利用者

の携帯電話製造番号 9 0 1、携帯電話番号 9 0 2、店舗 I D 9 0 3 が登録されるようになっている。ここで、携帯電話番号 9 0 2 のみが登録されている場合は、携帯電話製造番号は正しいが、携帯電話番号の標識を改造してアクセスした者を意味する。また、店舗 I D 9 0 3 が登録されていない店舗は、本システムに未登録の店舗であるか、または店舗 I D を不正に書き換えている店舗を意味する。

ここで、悪意がない未登録の利用者および店舗については、アクセス時に登録を行うようにメッセージを送信し、複数回の登録案内を行ったにも拘わらず登録手続を行わないものについてののみ不正利用として登録するようにしてもよい。

以下、(1) スーパーマーケット等の一般の店舗で携帯電話機 1 を利用した商品購入時の決裁方法、(2) 自動販売機での商品購入時の決裁方法、(3) インタネット上の電子店舗での商品購入時の決裁方法についてフローチャートを参照して説明する。

図 1 0 及び図 1 1 は、スーパーマーケット等の一般の店舗で携帯電話機 1 を利用した商品購入時の決裁方法を示すフローチャートである。

まず、利用者(商品購入者)は、自分が所持する携帯電話機 1 をモバイルショッピングモードに設定した後、入力手段 1 4 を使用し、商品を購入しようとしている店舗の識別情報としての店舗 I D、自分の暗証番号(図 7 の 7 0 6 に登録した番号)、決裁方法、商品の購入金額を入力する(ステップ 1 0 0 1)。ここで、店舗又は商品の識別情報を、店舗内に設置されている発信機等から外部入出力インタフェース 1 7 を介して取り込むようにしてもよい。

また、決裁方法については、クレジットカード決裁、Webマネー決裁、デビットカード決裁があるが、クレジットカード決裁を選択した場合については支払い回数とクレジットカード番号を入力する。また、Webマネー決裁を選択した場合にはWebマネー口座番号(図 7 の 7 1 1 に登録した番号)を入力する。同様に、デビットカード決裁を選択した場合にはデビットカード番号(図 7 の 7 0 9 に登録した番号)を入力する。なお、以下のフローチャートでは人間が行う操作はステップ 1 0 0 1 のように 2 重枠線で囲む形式で表記している。

入力が終了したならば、送信操作を行う。すると、ステップ 1 0 0 1 で入力した情報が Q R 決裁証明鍵発行要求として認証サーバ 4 1 に送信される。

この Q R 決裁証明鍵発行要求を受信した認証サーバ 4 1 は、店舗及び利用者の認証処理を行う(ステップ 1 0 0 2)。すなわち、Q R 決裁証明鍵発行要求の中に含まれる店舗 I D によって店舗情報 D B 4 3 を検索し、当該店舗 I D の店舗が登録されているか否かを調べる。同様に、暗証番号、クレジットカード番号(またはWebマネー口座番号、デビットカード番号)によって利用者情報 D B 4 4 を検索し、当該暗証番号及びクレジットカード番号(またはWebマネー口座番号、デビットカード番号)の利用者が利用者情報 D B 4 4 に登録されているか否かを調べる。その結果、店舗 I D が登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機 1 に返信する(ステップ 1 0 0 3)。また、暗証番号及びクレジットカード番号(またはWebマネー口座番号、デビットカード番号)が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機 1 に返信する(ステップ 1 0 0 3)。携帯電話機 1 では、取引不可のメッセージが表示部 1 1 に表示されると共に、ステップ 1 0 0 1 で入力した店舗 I D 等の情報が自動消去される。

しかし、店舗 I D 及び暗証番号及びクレジットカード番号(またはWebマネー口座番号、デビットカード番号)が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証 O K とする。

認証 O K となった場合には、認証サーバ 4 1 は金融機関 4 2 に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関 4 2 における与信処理(ステップ 1 0 0 4)によって与信 O K または与信 N G の与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたは Q R 決裁証明鍵を生成する(ステップ 1 0 0 5)。すなわち、与信 N G の与信結果が返送されてきた場合には、認証サーバ 4 1 は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機 1 に送信する。しかし、与信 O K であっ

た場合には、図 3 (d) で示したような 2 次元コードで構成された Q R 決裁証明鍵を生成し (ステップ 1006)、これを携帯電話機 1 に送信する。この Q R 決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。

携帯電話機 1 では、受信した Q R 決裁証明鍵を図 12 (a) に符号 1201 で示すように表示部 11 に表示する。同時に、例えば「この携帯電話機で決裁できます。代金決裁時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は予め選択してあった購入希望商品を店舗端末 22 の店員に提示し、購入希望商品の発注を行う (ステップ 1007)。店員は店舗端末によって購入希望商品の代金を入力する (ステップ 1008)。

これと並行して、利用者は Q R 決裁証明鍵 1201 が表示された状態の携帯電話機 1 を店舗端末 22 に付属した Q R コード読取装置 21 の読取部分に挿入装着する (ステップ 1009)。すると、Q R コード読取装置 21 は、携帯電話機 1 の表示部 11 に表示された Q R 決裁証明鍵 1201 を読み取ると共に (ステップ 1011)、標識 19、20 から携帯電話製造番号と携帯電話番号を読み取り (ステップ 1010)、その読取結果を店舗端末 22 に転送する。

店舗端末 22 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び Q R 決裁証明鍵 1201 を決裁承認要求として認証サーバ 41 に送信する。この場合、Q R 決裁証明鍵 1201 については、認証サーバ自身が発行したものであることが分かればよいので、決裁番号及び個人認証といった一部の情報のみを送信してもよい。図 11 では、決裁番号及び個人認証の情報のみを決裁承認要求の中に含ませて送信していることを示している。

認証サーバ 41 は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 DB 44 の登録内容と照合して調べる (ステップ 1012)。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース (図 9) に登録した後 (ステップ 1013)、不正利用メッセージを店舗端末 22 および携帯電話機 1 に送信する。

不正利用メッセージを受信した携帯電話機 1 では、不正利用メッセージ自体が Q R 決裁証明鍵 1201 の消去コマンドとして機能し、表示部 11 に表示されていた Q R 決裁証明鍵 1201 が消去される。

店舗端末 22 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される (ステップ 1014)。そして、店員により代金決裁ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末 22 から受信した Q R 決裁証明鍵 1201 の情報 (全部または一部) が自分自身で発行した正規のものであると認められた場合には、認証サーバ 41 は詳細決裁承認を店舗端末 22 に返信する。この詳細決裁承認の情報には、Q R 決裁証明鍵 1201 と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決裁承認を店舗端末 22 は、受信した詳細決裁承認の情報の全部または一部を利用者情報として表示部に表示する (ステップ 1015)。図 12 (b) にその例を示している。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する (ステップ 1016)。

本人の購入意思の確定応答があったならば、決裁ボタン操作によって決裁を完了する (ステップ 1017)。決裁ボタン操作が行われた場合は、店舗端末 22 は決裁終了メッセージを認証サーバ 41 に送信する。この決裁終了メッセージを受信した認証サーバ 41 は利用者の購入履歴情報を更新する (ステップ 1018)。この後、確認用の決裁内容を携帯電話機 1 に送信する。また、決裁終了情報を金融機関 42 に送信する。これにより、携帯電話機 1 の表示部 11 には、図 13 に示すような確認用の決裁内容 1301 が表示される。この決裁内容 1301 は、利用者自身が消去するまで保存することができる。ただし、

Q R 決裁証明鍵 1 3 0 1 は 1 回限り有効であるので、所定時間後に自動的に消去される。また、決裁終了情報を受信した金融機関 4 2 では利用者の指定口座から代金を引き落とす手続を行う。

以上により、携帯電話機 1 を使用して一般店舗での商品購入時の決裁を行うことができる。なお、利用者が購入意思を撤回した場合に、店舗端末でのキャンセル操作によって店舗端末の処理は終了する。また、利用者自身が携帯電話機 1 でキャンセル操作を行った場合にも、決裁処理は途中で終了し、Q R 決裁証明鍵 1 3 0 1 等の情報は全て消去される。

以上の説明から明らかなように、本取引方法によれば、店舗側に利用者のクレジット番号等の秘密情報を伝えることなく、認証サーバ 4 1 が発行した Q R 決裁証明鍵のみで代金決裁を行うことができる。また、携帯電話機 1 内にクレジットカード番号等の秘密情報を全く保持しない構成であるので、万一、携帯電話機 1 を紛失したとしても、代金決裁に悪用される危険性は全く生じない。さらに、特殊な結晶粉末を混入して記録した標識によって携帯電話製造番号と電話番号の正当性を判定しているため、携帯電話機自身の改造による悪用を防止することができ、決済に使用される機器のセキュリティ性を高めることにより、利用者および店舗の双方に有益な効果を発揮する。

さらに、店舗においては、読取装置 2 1 を付加するのみであるため、システムに加盟するに際してのコストが少なく済むという利点がある。同様に、携帯電話機 1 においても、I C カードなどを付加することなく市販の携帯電話機をそのまま利用することができる。さらに、購入履歴を管理しているため、店舗側においてはポイントカードを発行する必要がなくなる。また、利用者にとっても、利用状況が分かるので、計画的な購入計画を立てるのに役立つという利点がある。

また、Q R コードを用いたことにより、3 6 0 度のどの方向からでも記録内容を読み取ることができるので、読取部との位置関係の束縛がなくなり、一般の利用者が読み取り部に挿入して読み取らせる場合に好適である。また、位置関係を厳密に定める必要がないため、その分だけ読取時間も短縮することができる。さらに、コードの一部に汚れや破損があっても誤りを訂正できるので、読取ミスが減少する。特に本発明のように、携帯電話機 1 の表示部に表示させた状態で読み取らせる場合、表示部の汚れ等によって読取ミスが発生することが考えられるが、Q R コードを用いることによって表示部の汚れ等に起因する読取ミスを減少させることができる。

なお、Q R 決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成されるものとしたが、決裁番号、個人認証、氏名の一部または全部を元に生成した 1 回限りのパスワードであってもよい。

この場合には、例えば、認証サーバ 4 1 と携帯電話機 1 とに、同一ロジックによるパスワード生成プログラムを備え、2 回目にアクセスするときは、1 回目に送信された暗証番号等に基づき自動生成されたパスワードを携帯電話機 1 から自動送信し、認証サーバ 4 1 側では、当該携帯電話機 1 の携帯電話番号等及び自動送信されたパスワードと、前記認証サーバ 4 1 で自動生成されたパスワードとを比較することにより、認証を行う。

3 回目以降は、前回自動生成されたパスワードに基づき新たなパスワードを自動生成、自動送信することとしてもよい。

このような、いわゆるワンタイムパスワードと呼ばれるものを用いることにより、セキュリティ性を高めることができるとともに、2 回目以降のアクセス時に、暗証番号の入力を省略することができる。

次に、自動販売機 3 から飲料水等の小額商品を購入する場合の決裁方法について図 1 4 及び図 1 5 のフローチャートを参照して説明する。

まず、利用者（商品購入者）は、自分が所持する携帯電話機 1 をモバイルショッピングモードに設定した後、入力手段 1 4 を使用し、商品を購入しようとしている自動販売機 3 の店舗 I D、自分の暗証番号（図 7 の 7 0 6 に登録した番号）、決裁方法、商品の購入金額を入力する（ステップ 1 4 0 1）。ここで、店舗又は商品の識別情報を、店舗内に設置されている発信機等から外部入出力インタフェース 1 7 を介して取り込むようにしてもよい。また、決裁方法については、クレジットカード決裁、Webマネー決裁、デビットカード

決裁、非接触 I C カード決済があるが、小額決裁であるので、Webマネーを使用することとし、Webマネー口座番号（図 7 の 7 1 1 に登録した番号）を入力する。

入力が終了したならば、送信操作を行う。すると、ステップ 1 4 0 1 で入力した情報が Q R 決裁証明鍵発行要求として認証サーバ 4 1 に送信される。

この Q R 決裁証明鍵発行要求を受信した認証サーバ 4 1 は、店舗（ここでは自動販売機）及び利用者の認証処理を行う（ステップ 1 4 0 2）。すなわち、Q R 決裁証明鍵発行要求の中に含まれる店舗 I D によって店舗情報 D B 4 3 を検索し、当該店舗 I D の店舗（自動販売機）が登録されているか否かを調べる。同様に、暗証番号、Webマネー口座番号によって利用者情報 D B 4 4 を検索し、当該暗証番号及びWebマネー口座番号の利用者が利用者情報 D B 4 4 に登録されているか否かを調べる。その結果、店舗 I D が登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 1 4 0 3）。また、暗証番号及びWebマネー口座番号が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 1 4 0 3）。携帯電話機 1 では、取引不可のメッセージが表示部 1 1 に表示されると共に、ステップ 1 4 0 1 で入力した店舗 I D 等の情報が自動消去される。

しかし、店舗 I D 及びWebマネー口座番号が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証 O K とする。

認証 O K となった場合には、認証サーバ 4 1 は金融機関 4 2 に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関 4 2 における与信処理（ステップ 1 4 0 4）によって与信 O K または与信 N G の与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたは Q R 決裁証明鍵を生成する（ステップ 1 4 0 5）。すなわち、与信 N G の与信結果が返送されてきた場合には、認証サーバ 4 1 は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機 1 に送信する。しかし、与信 O K であった場合には、図 3（d）で示したような 2 次元コードで構成された Q R 決裁証明鍵を生成し（ステップ 1 4 0 6）、これを携帯電話機 1 に送信する。この Q R 決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。

携帯電話機 1 では、受信した Q R 決裁証明鍵を図 1 2（a）に符号 1 2 0 1 で示したように表示部 1 1 に表示する。同時に、例えば「この携帯電話機で決裁できます。代金決裁時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は Q R 決裁証明鍵 1 2 0 1 が表示された状態の携帯電話機 1 を自動販売機 3 に付属した Q R コード読取装置 3 3 の読取部分に挿入装着する（ステップ 1 4 0 7）。そして、購入希望商品を自動販売機 3 の選択操作を行う（ステップ 1 4 0 8）。自動販売機 3 では、購入希望商品の選択操作によって代金が自動的に確定する（ステップ 1 4 0 9）。

Q R コード読取装置 3 3 は、携帯電話機 1 の表示部 1 1 に表示された Q R 決裁証明鍵 1 2 0 1 を読み取ると共に（ステップ 1 4 1 1）、標識 1 9、2 0 から携帯電話製造番号と携帯電話番号を読み取る（ステップ 1 4 1 0）。

自動販売機 3 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び Q R 決裁証明鍵 1 2 0 1 を決裁承認要求として認証サーバ 4 1 に送信する。この場合の通信回線は、P H S 電話機を使用したデータ通信を利用することができる。図 1 5 では、決裁番号及び個人認証の情報のみを決裁承認要求の中に含ませて送信していることを示している。

認証サーバ 4 1 は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 D B 4 4 の登録内容と照合して調べる（ステップ 1 4 1 2）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図 9）に登録した後（ステップ 1 4 1 3）、不正利用メッセージを自動販売機 3 および携帯電話機 1 に送信する。

不正利用メッセージを受信した携帯電話機 1 では、不正利用メッセージ自体が Q R 決裁証

明鍵 1 2 0 1 の消去コマンドとして機能し、表示部 1 1 に表示されていた Q R 決裁証明鍵 1 2 0 1 が消去される。

自動販売機 3 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ 1 4 1 4）。しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも自動販売機 3 から受信した Q R 決裁証明鍵 1 2 0 1 の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ 4 1 は詳細決裁承認を店舗端末 2 2 に返信する。この詳細決裁承認の情報には、Q R 決裁証明鍵 1 2 0 1 と同様の情報の他に、当該利用者の購入履歴の情報が含まれている。

詳細決裁承認を受信した店舗端末 2 2 は、直ちに決裁処理を行う（ステップ 1 4 1 5）。そして、決裁終了メッセージを認証サーバ 4 1 に送信する。この決裁終了メッセージを受信した認証サーバ 4 1 は利用者の購入履歴情報を更新する（ステップ 1 4 1 6）。この後、確認用の決裁内容を携帯電話機 1 に送信する。また、決裁終了情報を金融機関 4 2 に送信する。これにより、携帯電話機 1 の表示部 1 1 には、図 1 3 に示したような確認用の決裁内容 1 3 0 1 が表示される（ステップ 1 4 1 7）。

決裁終了メッセージを受信した金融機関 4 2 では利用者の Web マネー口座又はクレジット口座から代金を引き落とす手続を行う。

以上により、携帯電話機 1 を使用して自動販売機での小額商品購入時の決裁を行うことができる。

以上の説明から明らかなように、本取引方法においても、自動販売機側に利用者のクレジット番号等の秘密情報を伝えることなく、認証サーバ 4 1 が発行した Q R 決裁証明鍵のみで代金決裁を行うことができる。

次に、インターネット上の電子店舗での商品購入時の決裁方法について図 1 6 及び図 1 7 のフローチャートを参照して説明する。

まず、利用者（商品購入者）は、自分が所持する携帯電話機 1 をモバイルショッピングモードに設定した後、入力手段 1 4 を使用し、インターネット上の店舗にアクセスし、購入しようとしている商品の番号、購入金額、受取方法を入力し、商品の発注を行う（ステップ 1 6 0 1）。

商品の発注を受けた店舗は、認証サーバ 4 1 に対して個人認証依頼を送信する。この個人認証依頼を受信した認証サーバ 4 1 は、携帯電話機 1 に対して自分の暗証番号（図 7 の 7 0 6 に登録した番号）、決裁方法及び店舗 ID の入力要求を送信する。

そこで、携帯電話機 1 の利用者が自分の暗証番号（図 7 の 7 0 6 に登録した番号）、決裁方法及び店舗 ID を入力する（ステップ 1 6 0 2）。すると、その内容は Q R 決裁証明鍵発行要求として認証サーバ 4 1 に送信される。ここで、決裁方法については、前述の例と同様である。

この Q R 決裁証明鍵発行要求を受信した認証サーバ 4 1 は、利用者の認証処理を行う（ステップ 1 6 0 3）。すなわち、Q R 決裁証明鍵発行要求の中に含まれる店舗 ID によって店舗情報 DB 4 3 を検索し、当該店舗 ID の店舗が登録されているか否かを調べる。同様に、暗証番号、クレジットカード番号（または Web マネー口座番号、デビットカード番号）によって利用者情報 DB 4 4 を検索し、当該暗証番号及びクレジットカード番号（または Web マネー口座番号、デビットカード番号）の利用者が利用者 DB 4 4 に登録されているか否かを調べる。その結果、店舗 ID が登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 1 6 0 4）。また、暗証番号及びクレジットカード番号（または Web マネー口座番号、デビットカード番号）が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 1 6 0 4）。携帯電話機 1 では、取引不可のメッセージが表示部 1 1 に表示されると共に、ステップ 1 6 0 2 で入力した店舗 ID 等の情報が自動消去される。

しかし、店舗 ID 及び暗証番号及びクレジットカード番号（または Web マネー口座番号、デビットカード番号）が正しく登録されていた場合には、正規登録の店舗であり、かつ正

規登録の利用者であるものと認証し、認証OKとする。

認証OKとなった場合には、認証サーバ41は金融機関42に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関42における与信処理（ステップ1605）によって与信OKまたは与信NGの与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたはQR決裁証明鍵を生成する（ステップ1606）。すなわち、与信NGの与信結果が返送されてきた場合には、認証サーバ41は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機1に送信する。しかし、与信OKであった場合には、図3（d）で示したような2次元コードで構成されたQR決裁証明鍵を生成し（ステップ1607）、これを携帯電話機1に送信する。このQR決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。

携帯電話機1では、受信したQR決裁証明鍵を図12（a）に符号1201で示すように表示部11に表示する。同時に、例えば「この携帯電話機で決裁できます。お客様が指定した受取店舗での代金決裁時に読取装置に挿入して下さい。」といったメッセージが表示される。

また、認証サーバ41は、店舗に対して、受託証明の発行要求を送信する。この受託証明の発行要求を受信した店舗は、受託番号、利用者氏名、商品番号、金額、決裁方法、受取方法を含む受託証明を生成し、認証サーバ41に返信する。この受託証明は、利用者から見れば商品注文書に相当するものである。

受託証明を受信した認証サーバ41は、QR決裁証明鍵1201と受託証明とを一体化し、QR決裁証明鍵付き受託証明として携帯電話機1に送信する。

そこで、利用者は自分が指定した受取店舗に赴き、QR決裁証明鍵付き受託証明を表示部11に表示させた状態で受取店舗の店舗端末22に付属したQRコード読取装置21の読取部分に挿入装着する（ステップ1608）。すると、QRコード読取装置21は、携帯電話機1の表示部11に表示されたQR決裁証明鍵付き受託証明を読み取ると共に（ステップ1609）、標識19、20から携帯電話製造番号と携帯電話番号を読み取り（ステップ1610）、その読取結果を店舗端末22に転送する。

店舗端末22は、携帯電話機1から読み取った携帯電話製造番号、携帯電話番号及びQR決裁証明鍵付き受託証明を決裁承認要求として認証サーバ41に送信する。この場合、QR決裁証明鍵付き受託証明については、認証サーバ自身が発行したものであることが分かればよいので、決裁番号及び個人認証といった一部の情報のみを送信してもよい。図17では、決裁番号及び個人認証の情報のみを決裁承認要求の中に含ませて送信していることを示している。

認証サーバ41は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報DB44の登録内容と照合して調べる（ステップ1611）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図9）に登録した後（ステップ1613）、不正利用メッセージを店舗端末22および携帯電話機1に送信する。

不正利用メッセージを受信した携帯電話機1では、不正利用メッセージ自体がQR決裁証明鍵付き受託証明の消去コマンドとして機能し、表示部11に表示されていたQR決裁証明鍵付き受託証明が消去される。

店舗端末22では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ1613）。そして、店員により商品の引渡し及び代金決裁ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末22から受信したQR決裁証明鍵付き受託証明の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ41は詳細決裁承認を店舗端末22に返信する。この詳細決裁承認の情報には、QR決裁証明鍵1201と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決裁承認を受信した店舗端末 2 2 は、受信した詳細決裁承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ 1 6 1 4）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ 1 6 1 5）。

本人の購入意思の確定応答があったならば、商品を引き渡した上で、決裁ボタン操作によって決裁を完了する（ステップ 1 6 1 6）。決裁ボタン操作が行われた場合は、店舗端末 2 2 は決裁終了メッセージを認証サーバ 4 1 に送信する。この決裁終了メッセージを受信した認証サーバ 4 1 は利用者の購入履歴情報を更新する（ステップ 1 6 1 7）。この後、確認用の決裁内容を携帯電話機 1 に送信する。これにより、携帯電話機 1 の表示部 1 1 には、図 1 3 に示したような確認用の決裁内容 1 3 0 1 が表示される。また、認証サーバ 4 1 は、決裁終了情報を金融機関 4 2 に送信する。

以上により、携帯電話機 1 を使用してインターネット上の店舗で商品を選択し、その商品を利用者自身が指定した受取店舗で受け取り、決裁することができる。

以上の説明から明らかなように、本取引方法によれば、インターネット上の店舗側に利用者のクレジット番号等の秘密情報を伝えることなく、認証サーバ 4 1 が発行した Q R 決裁証明鍵のみで代金決裁を行うことができる。

このような方法を利用すれば、例えばインターネット上で映画等のチケットを発注し、その Q R 決裁証明鍵付き受託証明を携帯電話機 1 に格納しておき、映画館の入場口の読取装置に挿入することにより、チケットなしで入場するといった運用形態に活用することができる。

ここで、Q R 決裁証明鍵付き受託証明を表示部 1 1 に表示させて読取装置 2 1 に読み取らせる代わりに、Q R 決裁証明鍵付き受託証明をパーソナルコンピュータ（P C）に転送し、付属のプリンタで印刷し、受取店舗の読取装置で読み取らせる方法を採用することができる。この場合、プリンタの印字トナーまたはインクには、標識 1 9、2 0 と同様の結晶粉末が混入されたものを用いる。

図 1 8 は、その手順を示すフローチャートである。このフローチャートは、図 1 6 の続きに該当する。

まず、携帯電話機 1 で Q R 決裁証明鍵付き受託証明を受信したならば、その Q R 決裁証明鍵付き受託証明をパーソナルコンピュータ（P C）に転送し（ステップ 1 6 2 0）、付属のプリンタで印刷する（ステップ 1 6 2 1）。図 1 9（a）に印刷例を示す。

そこで、利用者は印刷された Q R 決裁証明鍵付き受託証明を自分が指定した受取店舗に持参し、受取店舗の店舗端末 2 2 に付属した Q R コード読取装置 2 1 の読取部分に挿入装着する。すると、Q R コード読取装置 2 1 は、印刷された Q R 決裁証明鍵付き受託証明を読み取り（ステップ 1 6 2 2）、その読取結果を店舗端末 2 2 に転送する。

店舗端末 2 2 は、印刷された Q R 決裁証明鍵付き受託証明の読取結果を図 1 7 の場合と同様に決裁承認要求として認証サーバ 4 1 に送信する。

認証サーバ 4 1 は、決裁承認要求を受信したならば、まず、Q R 決裁証明鍵付き受託証明の Q R 決裁証明鍵が自分自身で発行した正規のものであるかの正当性を調べる（ステップ 1 6 2 3）。この結果、正当なものでない場合には、不正利用であるものと判断し不正利用情報データベース（図 9）に登録した後（ステップ 1 6 2 4）、不正利用メッセージを店舗端末 2 2 および携帯電話機 1 に送信する。

不正利用メッセージを受信した携帯電話機 1 では、不正利用メッセージ自体が Q R 決裁証明鍵付き受託証明の消去コマンドとして機能し、表示部 1 1 に表示されていた Q R 決裁証明鍵付き受託証明が消去される。

店舗端末 2 2 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ 1 6 2 5）。そして、店員により商品の引渡し及び代金決裁ができない旨が利用者に口頭で通知される。

しかし、Q R 決裁証明鍵が正当なものであると認められた場合には、認証サーバ 4 1 は詳細決裁承認を店舗端末 2 2 に返信する。この詳細決裁承認の情報には、Q R 決裁証明鍵 1 2 0 1 と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人

特徴情報が含まれている。

詳細決裁承認を受信した店舗端末22は、受信した詳細決裁承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ1626）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ1627）。

本人の購入意思の確定応答があったならば、商品を引き渡した上で、決裁ボタン操作によって決裁を完了する（ステップ1628）。決裁ボタン操作が行われた場合は、店舗端末22は決裁終了メッセージを認証サーバ41に送信する。この決裁終了メッセージを受信した認証サーバ41は利用者の購入履歴情報を更新する（ステップ1629）。この後、確認用の決裁内容を携帯電話機1に送信する。これにより、携帯電話機1の表示部11には、図13に示したような確認用の決裁内容1301が表示される。また、認証サーバ41は、決裁終了情報を金融機関42に送信する。

以上により、携帯電話機1を持参しない場合でも、インターネット上の店舗で注文した商品を利用者自身が指定した受取店舗で受け取り、決裁することができる。

この場合には、必ずしもQR決裁証明鍵付き受託証明を携帯電話機1からパーソナルコンピュータ（PC）に転送することは必要なく、直接にネットワーク端末としてのパーソナルコンピュータで受信して、プリンタで印刷することとしてもよい。

これら方法を利用すれば、印刷されたQR決裁証明鍵付き受託証明を、インターネット上で注文した例えば映画等のチケットの代わりに利用するといった運用形態に活用することができる。図19（b）に入場券の例を示す。

なお、前記各例では、商品の決済等に関する情報を発信するネットワーク端末と、QR決済証明鍵等のコードキャラクタ情報画像を受信するネットワーク端末として、同一の携帯電話機1を使用する場合を説明しているが、これに限られるものではなく、情報送信用のネットワーク端末と、コードキャラクタ情報画像受信用のネットワーク端末とを別の端末としてもよい。

これを利用することにより、第三者のネットワーク端末に対しコードキャラクタ情報画像を送信することもできる。従って、第三者に商品やギフト券を贈る代わりとして、第三者のネットワーク端末に送信したコードキャラクタ情報画像による決済を可能とすることができる。

以下、図20～図28参照して、この場合の決済処理方法を説明する。

この場合、前記決済処理機関4には、贈答情報データベース（DB）が備えられ、また、前記認証サーバ41には贈答情報登録処理プログラム412が備えられることとなる。

前記贈答情報DBは、例えば図20に示すように、贈り手側ID2001、受け手側ID2002、贈答内容2003、識別ID2004、決済処理日2005が格納されるようになっている。

また、前記贈答情報登録処理プログラムは、本システムを使用して特定の商品又は一定の金額の贈答を行う情報を贈答情報DBに登録する際に使用するプログラムである。

本決済処理方法では、まず、注文主（商品の贈り手）は、情報送信用端末としての携帯電話機1をモバイルショッピングモードに設定した後、入力手段14を使用し、自分の暗証番号（図7の706に登録した番号）、決済方法、商品の受取り手側の利用者名及び利用者ID等の受取り手情報、贈答内容（この場合には、贈りたい商品の商品番号）を入力する（ステップ2101）。ここで、決済方法については、前述の例と同様である。

入力が終了したならば、送信操作を行う。すると、ステップ2101で入力した情報が贈答情報送信要求として認証サーバ41に送信される。

この贈答情報送信要求を受信した認証サーバ41は、利用者の認証処理を行う（ステップ2102）。すなわち、贈答情報送信要求の中に含まれる暗証番号、クレジットカード番号（またはWebマネー口座番号、デビットカード番号）によって利用者情報DB44を検索し、当該暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）の利用者が利用者情報DB44に登録されているか否かを調べる。また、受取り手情報としての利用者ID等によって、利用者情報DB44を検索し、その結果、暗証

番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機1に返信する（ステップ2103）。携帯電話機1では、取引不可のメッセージが表示部11に表示されると共に、ステップ2101で入力した暗証番号等の情報が自動消去される。

しかし、暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）、受取り手情報としての利用者ID、利用者名が正しく登録されていた場合には、正規登録の利用者であるものと認証し、認証OKとする。

認証OKとなった場合には、認証サーバ41は金融機関42に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関42における与信処理（ステップ2104）によって与信OKまたは与信NGの与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたは贈答情報の送信を行う（ステップ2105）。すなわち、与信NGの与信結果が返送されてきた場合には、認証サーバ41は、残高不足等のメッセージを含む取引不可メッセージを贈り手側の携帯電話機1に送信する。しかし、与信OKであった場合には、ステップ2101で入力された受取り手側の携帯電話機1に贈答情報を送信する。この贈答情報としては、図24（a）に示すように贈り手の利用者名及び贈答内容としての商品名等が表示され、受取り手側により、贈答内容の受取りについて、拒否又は受諾の情報が認証サーバ41に返信される（ステップ2106）。認証サーバ41は、この返信を受け、拒否の情報が返信された場合には、受取り手側の携帯電話機1にその旨の確認メッセージを送信するとともに、贈り手側の携帯電話機に受取り拒否のメッセージを送信した後（図24（c）参照）、ステップ2101で入力した暗証番号等の情報が自動消去される。（ステップ2107）。しかし、受諾の情報が返信された場合には、認証サーバ41は、受取り手側の携帯電話機1に対して、商品の受取り方法の入力要求を送信する（図24（b）参照）。

そこで、携帯電話機1の利用者が受取りの店舗ID及び受取り方法を入力する（ステップ2108）。すると、その内容はQR決済証明鍵発行要求として認証サーバ41に送信される。

このQR決済証明鍵発行要求を受信した認証サーバ41は、店舗の認証処理を行う（ステップ2109）。すなわち、QR決済証明鍵発行要求の中に含まれる店舗IDによって店舗情報DB43を検索し、当該店舗IDの店舗が登録されているか否かを調べる。その結果、店舗IDが登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを受取り手側の携帯電話機1に返信する（ステップ2110）。携帯電話機1では、取引不可のメッセージが表示部11に表示されたのを確認した後、別の店舗ID等を入力することとなる。

しかし、店舗IDが正しく登録されていた場合には、正規登録の店舗であるものと認証し、認証OKとする。

認証OKとなった場合には、認証サーバ41は、図3（d）で示したような2次元コードで構成されたQR決済証明鍵を生成する。（ステップ2211）このQR決済証明鍵は、少なくとも決済番号、個人認証、氏名、決済方法の情報を含むもので構成される。

また、認証サーバ41は、店舗に対して、受託証明の発行要求を送信する。この受託証明の発行要求を受信した店舗は、受託番号、利用者氏名、商品番号、金額、決済方法、受取方法を含む受託証明を生成し、認証サーバ41に返信する。この受託証明は、利用者から見れば商品注文書に相当するものである。

受託証明を受信した認証サーバ41は、QR決済証明鍵1201と受託証明とを一体化し、QR決済証明鍵付き受託証明として受取り手側の携帯電話機1に送信する。

携帯電話機1では、受信したQR決済証明鍵を前記図12に符号1201で示すように表示部11に表示する。同時に、例えば「この携帯電話機で決済できます。代金決済時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は自分が指定した受取店舗に赴き、QR決済証明鍵付き受託証明を表示部11に表示させた状態で受取店舗の店舗端末22に付属したQRコード読取装置21の読

取部分に挿入装着する（ステップ2112）。すると、QRコード読取装置21は、標識19、20から携帯電話製造番号と携帯電話番号を読み取ると共に（ステップ2113）、携帯電話機1の表示部11に表示されたQR決済証明鍵付き受託証明を読み取り（ステップ2114）、その読取結果を店舗端末22に転送する。

店舗端末22は、携帯電話機1から読み取った携帯電話製造番号、携帯電話番号及びQR決済証明鍵付き受託証明を決済承認要求として認証サーバ41に送信する。この場合、QR決済証明鍵付き受託証明については、認証サーバ41自身が発行したものであることが分かればよいので、決済番号及び個人認証といった一部の情報のみを送信してもよい。図23では、決済番号及び個人認証の情報のみを決済承認要求の中に含ませて送信していることを示している。

認証サーバ41は、決済承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報DB44の登録内容と照合して調べる（ステップ2115）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図9）に登録した後（ステップ2116）、不正利用メッセージを店舗端末22および受取り手側の携帯電話機1に送信する。さらに、贈り手側の携帯電話機1にも不正利用メッセージが送信される。

不正利用メッセージを受信した携帯電話機1では、不正利用メッセージ自体がQR決済証明鍵付き受託証明の消去コマンドとして機能し、表示部11に表示されていたQR決済証明鍵付き受託証明が消去される。

店舗端末22では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ2117）。そして、店員により商品の引渡し及び代金決済ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末22から受信したQR決済証明鍵付き受託証明の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ41は詳細決済承認を店舗端末22に返信する。この詳細決済承認の情報には、QR決済証明鍵1201と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決済承認を受信した店舗端末22は、受信した詳細決済承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ2118）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ2119）。

本人の購入意思の確定応答があったならば、商品を引き渡した上で、決済ボタン操作によって決済を完了する（ステップ2120）。決済ボタン操作が行われた場合は、店舗端末22は決済終了メッセージを認証サーバ41に送信する。

この決済終了メッセージを受信した認証サーバ41は贈り手側の利用者の購入履歴情報を更新する（ステップ2121）。この後、確認用の決済内容を贈り手側の情報発信用端末に送信する。これにより、例えば、贈り手側の携帯電話機1の表示部11には、図25に示したような確認メッセージ及び決済内容2501、2502が表示される（ステップ2122）。また、認証サーバ41は、決済終了情報を金融機関42に送信する。

以上により、贈り手側端末を使用して、特定の商品を選択し、その商品を受取り手側が指定した店舗で受け取り、決済することができる。

以上の説明から明らかなように、本取引方法によれば、店舗側や贈答品の受取り手側に贈り手のクレジット番号等の秘密情報を伝えることなく、認証サーバ41が発行したQR決済証明鍵のみで代金決済を行うことができる。また、贈答品の受取り手の認証をより確実に行うことができる。

なお、本取引方法では、受取り手側に対し贈答情報を送信し、贈答を受諾するか否かを選択することとしているが、予め贈答を受諾又は拒否する者を設定しておき、認証サーバにおいて、この設定に基づき贈答を受諾するか拒否するかの判定を行うこととしてもよい。

この場合には、ステップ 2 1 0 6 及びステップ 2 1 0 7 に代えて、認証サーバにおける前記判定処理が行われることとなる。

また、このシステムにより贈られる贈答内容としては、特定の商品に限られず、一定金額のギフト券に相当する内容としてもよい。

図 2 6 及び図 2 7 は、その場合の手順を示すフローチャートである。図 2 6 のフローチャートは、図 2 1 の続きに該当する。

この場合には、前提として、図 2 1 のステップ 2 1 0 1 において、贈答内容として商品番号に代えて一定の金額を入力することとなる。

その後、図 2 1 のフローチャートに示す処理がされた後、受取り手側の利用者が受取りの店舗 ID 及び商品の購入金額を入力する（ステップ 2 1 3 0）。すると、その内容は QR 決済証明鍵発行要求として認証サーバ 4 1 に送信される。

この QR 決済証明鍵発行要求を受信した認証サーバ 4 1 は、店舗及び購入金額の認証処理を行う（ステップ 2 1 3 1）。すなわち、QR 決済証明鍵発行要求の中に含まれる店舗 ID によって店舗情報 DB 4 3 を検索し、当該店舗 ID の店舗が登録されているか否かを調べる。また、贈答情報 DB を検索し、入力された購入金額が、当該 DB に格納された金額の範囲内であるかを調べる。その結果、店舗 ID が登録されていなかった場合又は購入金額が贈答金額を超えている場合は、取引不可のメッセージを携帯電話機 1 に返信する（ステップ 2 1 3 2）。受取り手側の携帯電話機 1 では、取引不可のメッセージが表示部 1 1 に表示されたのを確認した後、別の店舗 ID 又は購入金額を入力することとなる。

しかし、店舗 ID が正しく登録されており、かつ、贈答金額の範囲内で購入金額が入力されていた場合には、正規登録の店舗で購入可能な金額であるものと認証し、認証 OK とする。

認証 OK となった場合には、認証サーバ 4 1 は、図 3 (d) で示したような 2 次元コードで構成された QR 決済証明鍵を生成し、携帯電話機 1 に送信する（ステップ 2 1 3 3）。この QR 決済証明鍵は、少なくとも決済番号、個人認証、氏名、決済方法の情報を含むもので構成される。

携帯電話機 1 では、受信した QR 決済証明鍵を図 1 2 (a) に符号 1 2 0 1 で示すように表示部 1 1 に表示する。同時に、例えば「この携帯電話機で決済できます。代金決済時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は予め選択してあった購入希望商品を店舗端末 2 2 の店員に提示し、購入希望商品の発注を行う（ステップ 2 1 3 4）。店員は店舗端末によって購入希望商品の代金を入力する（ステップ 2 1 3 5）。

これと並行して、利用者は QR 決済証明鍵 1 2 0 1 が表示された状態の携帯電話機 1 を店舗端末 2 2 に付属した QR コード読取装置 2 1 の読取部分に挿入装着する（ステップ 2 1 3 6）。すると、QR コード読取装置 2 1 は、受取り手側の携帯電話機 1 の表示部 1 1 に表示された QR 決済証明鍵 1 2 0 1 を読み取ると共に（ステップ 2 1 3 7）、標識 1 9、2 0 から携帯電話製造番号と携帯電話番号を読み取り（ステップ 2 1 3 8）、その読取結果を店舗端末 2 2 に転送する。

店舗端末 2 2 は、受取り手側の携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び QR 決済証明鍵 1 2 0 1 を決済承認要求として認証サーバ 4 1 に送信する。この場合、QR 決済証明鍵 1 2 0 1 については、認証サーバ自身が発行したものであることが分かればよいので、決済番号及び個人認証といった一部の情報のみを送信してもよい。

認証サーバ 4 1 は、決済承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 DB 4 4 の登録内容と照合して調べる（ステップ 2 1 3 9）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図 9）に登録した後（ステップ 2 1 4 0）、不正利用メッセージを店舗端末 2 2 および受取り手側の携帯電話機 1 に送信する。さらに、贈り手側の携帯電話機 1 にも不正利用メッセージが送信される。

不正利用メッセージを受信した受取り手側の携帯電話機 1 では、不正利用メッセージ自体

がQR決済証明鍵1201の消去コマンドとして機能し、表示部11に表示されていたQR決済証明鍵1201が消去される。

店舗端末22では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ2141）。そして、店員により代金決済ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末22から受信したQR決済証明鍵1201の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ41は詳細決済承認を店舗端末22に返信する。この詳細決済承認の情報には、QR決済証明鍵1201と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決済承認を店舗端末22は、受信した詳細決済承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ2142）。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ2143）。

本人の購入意思の確定応答があったならば、決済ボタン操作によって決済を完了する（ステップ2144）。決済ボタン操作が行われた場合は、店舗端末22は決済終了メッセージを認証サーバ41に送信する。この決済終了メッセージを受信した認証サーバ41は贈り手側の利用者の購入履歴情報を更新する（ステップ2145）。この後、確認用の決済内容を贈り手側の携帯電話機1に送信する。また、決済終了情報を金融機関42に送信する。これにより、例えば、贈り手側の携帯電話機1の表示部11には、図25に示すような確認用の決済内容2501、2502が表示される（ステップ2146）。この決済内容2501、2502は、利用者自身が消去するまで保存することができる。ただし、QR決済証明鍵1201は1回限り有効であるので、所定時間後に自動的に消去される。

また、決済終了情報を受信した金融機関42では贈り手側の利用者の指定口座から代金を引き落とす手続を行う。

以上により、贈り手側端末を使用して、一定の金額を指定し、その金額の範囲内で受取り手側が自由に商品等を店舗で購入して、決済することができる。

以上の説明から明らかなように、本取引方法によれば、一定金額のギフト券に相当する内容を贈る場合であっても、店舗側や受取り手側に贈り手のクレジット番号等の秘密情報を伝えることなく、認証サーバ41が発行したQR決済証明鍵のみで贈り手側の口座から代金決済を行うことができる。また、受取り手の認証をより確実に行うことができる。

また、前記各例では、金融機関による決済を前提としているが、決済代金の一部又は全部についてサービスポイントによる決済を行う場合にも、本発明を利用することができる。

以下、図28～図30を参照して、この場合の決済処理方法を説明する。

この場合、前記決済処理機関4には、サービスポイントデータベース（DB）が備えられ、また、前記認証サーバ41にはサービスポイント登録処理プログラムが備えられることとなる。

図28は、サービスポイントDBの格納情報の一例を示す図であり、更新日2801、利用店舗名2802、加算ポイント数2803、利用ポイント数2804、サービスポイント残高2805が格納されるようになっている。このサービスポイント情報は、利用者別に更新日時順に格納されるものである。

また、サービスポイント登録処理プログラムは、本システムを使用して商品の購入等を行うことにより得たサービスポイントに基づき、決済処理を行うものである。

なお、ここでサービスポイントの利用としては、ポイント数により商品購入時に一定金額相当の割引をして決済処理する場合、ポイント数に応じて予め決められた商品と交換する場合等があるが、本実施の形態では、サービスポイントを商品購入代金として決済処理する場合を示している。

本決済処理方法では、まず、利用者（商品購入者）は、携帯電話機1をモバイルショッピングモードに設定した後、入力手段14を使用し、商品を購入しようとしている店舗の店舗ID、自分の暗証番号（図7の706に登録した番号）、商品の購入金額に相当するサ

ービスポイントを入力する（ステップ2901）。ここで、店舗又は商品の識別情報を、店舗内に設置されている発信機等から外部入出力インタフェース17を介して取り込むようにしてもよい。

入力終了したならば、送信操作を行う。すると、ステップ2901で入力した情報がQR決済証明鍵発行要求として認証サーバ41に送信される。

このQR決済証明鍵発行要求を受信した認証サーバ41は、店舗及び利用者の認証処理を行う（ステップ2902）。すなわち、QR決済証明鍵発行要求の中に含まれる店舗IDによって店舗情報DB43を検索し、当該店舗IDの店舗が登録されているか否かを調べる。同様に、暗証番号によって利用者情報DB44を検索し、利用者が利用者情報DB44に登録されているか否かを調べる。その結果、店舗IDが登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機1に返信する（ステップ2903）。また、暗証番号が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機1に返信する（ステップ2903）。携帯電話機1では、取引不可のメッセージが表示部11に表示されると共に、ステップ2901で入力した店舗ID等の情報が自動消去される。

しかし、店舗ID及び暗証番号が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証OKとする。

認証OKとなった場合には、当該利用者のサービスポイントDBを検索し、サービスポイント残高の照会を行う（ステップ2904）。そして、この照会結果に応じて、取引不可メッセージまたはQR決済証明鍵を生成する（ステップ2905）。すなわち、照会の結果残高無しとされた場合には、認証サーバ41は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機1に送信する。しかし、残高有りであった場合には、図3（d）で示したような2次元コードで構成されたQR決済証明鍵を生成し（ステップ2906）、これを携帯電話機1に送信する。このQR決済証明鍵は、少なくとも決済番号、個人認証、氏名の情報を含むもので構成される。

携帯電話機1では、受信したQR決済証明鍵を図12（a）に符号1201で示すように表示部11に表示する。同時に、例えば「この携帯電話機で決済できます。代金決済時に読取装置に挿入して下さい。」といったメッセージが表示される。

そこで、利用者は予め選択してあった購入希望商品を店舗端末22の店員に提示し、購入希望商品の発注を行う（ステップ2907）。店員は店舗端末に購入希望商品の代金を入力することにより、この代金に相当するポイント数を算出する（ステップ2908）。

これと並行して、利用者はQR決済証明鍵1201が表示された状態の携帯電話機1を店舗端末22に付属したQRコード読取装置21の読取部分に挿入装着する（ステップ2909）。すると、QRコード読取装置21は、携帯電話機1の標識19、20から携帯電話製造番号と携帯電話番号を読み取ると共に（ステップ2910）表示部11に表示されたQR決済証明鍵1201を読み取り（ステップ2911）、その読取結果を店舗端末22に転送する。

店舗端末22は、携帯電話機1から読み取った携帯電話製造番号、携帯電話番号及びQR決済証明鍵1201を決済承認要求として認証サーバ41に送信する。この場合、QR決済証明鍵1201については、認証サーバ自身が発行したものであることが分かればよいので、決済番号、個人認証といった一部の情報のみを送信してもよい。図30では、決済番号及び個人認証の情報のみを決済承認要求の中に入れて送信していることを示している。

認証サーバ41は、決済承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報DB44の登録内容と照合して調べる（ステップ2912）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図11）に登録した後（ステップ2913）、不正利用メッセージを店舗端末22および携帯電話機1に送信する。

不正利用メッセージを受信した携帯電話機1では、不正利用メッセージ自体がQR決済証

明鍵 1 2 0 1 の消去コマンドとして機能し、表示部 1 1 に表示されていた Q R 決済証明鍵 1 2 0 1 が消去される。

店舗端末 2 2 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ 2 9 1 4）。そして、店員により代金決済ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末 2 2 から受信した Q R 決済証明鍵 1 2 0 1 の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ 4 1 は詳細決済承認を店舗端末 2 2 に返信する。この詳細決済承認の情報には、Q R 決済証明鍵 1 2 0 1 と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。

詳細決済承認を店舗端末 2 2 は、受信した詳細決済承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ 2 9 1 5）。店員は、その表示内容と購入希望商品の内容及び代金に相当するポイント数を見て、利用者本人に購入意思を確認する（ステップ 2 9 1 6）。

本人の購入意思の確定応答があったならば、決済ボタン操作によって決済を完了する（ステップ 2 9 1 7）。決済ボタン操作が行われた場合は、店舗端末 2 2 は決済終了メッセージを認証サーバ 4 1 に送信する。この決済終了メッセージを受信した認証サーバ 4 1 は利用者の購入履歴情報及びサービスポイント情報を更新する（ステップ 2 9 1 8）。この後、確認用の決済内容を携帯電話機 1 に送信する。この決済内容は、利用者自身が消去するまで保存することができる。ただし、Q R 決済証明鍵 1 2 0 1 は 1 回限り有効であるので、所定時間後に自動的に消去される。

以上により、携帯電話機 1 を使用して、一般店舗での商品購入時にサービスポイントを利用した決済を行うことができる。

以上の説明から明らかなように、本取引方法によれば、サービスポイントを利用した決済においても、認証サーバ 4 1 が発行した Q R 決済証明鍵のみで行うことができ、ポイントカード等を不要とすることができる。また、サービス利用者の認証をより確実に行うことができる。

以上の各例で示した方法は、金銭的な決済を介することを必須とするものではなく、入場券等のチケットの代わりや、商品等の受取証の代わりに用いることも可能なものである。なお、上記で説明した手順は、金融機関等の関係で一部の手順を変更して実施することができる。また、認証サーバ 4 1 が実行する手順は決済用のプログラムとして C D - R O M 等の記録媒体に記録して決済システム構築事業者に提供することができる。

また、携帯電話製造番号及び携帯電話番号の標識は、特殊な結晶粉末を混入した記録材料で記録しているが、これ以外に物理的に真偽判定が可能な記録形式で記録する方法であってもよい。

なお、I C カード（U I M カード）を搭載した携帯電話機等を用いる次世代移动通信サービスでは、携帯電話番号等を前記 I C カードに書き込み、I C カードの差し替えにより、異なる端末で同一の携帯電話番号の使用をするといった運用形態が考えられている。

そこで、この場合には、前記 I C カードに前記図 3（c）に示すような標識を貼り付け又は印刷することとしてもよい。

また、この場合には、携帯電話機等に設けられたスロット等に I C カードを差し込んだ状態で、前記標識を外部の読取装置で読取り可能とすることが必要となる。

この場合に用いられる携帯電話機の例を図 3 1，3 2 を参照して説明する。

図 3 1，3 2 は本実施の形態に用いられる携帯電話機の部分斜視図であり、各図において、3 0 0 は携帯電話機に搭載される携帯電話番号等の情報を保存した I C カードであり、その表面には、前記図 3（c）に示すような標識 3 1 1 が貼り付けまたは印刷されている。なお、この標識 3 1 1 には、携帯電話機の製造番号に代えて、各 I C カード又は所有者の識別情報が携帯電話番号とともに記録されている。

本実施の形態では、例えば、図 3 1（a）に示すように、携帯電話機 1 の裏面側等におい

て、ＩＣカードに貼り付けされた標識３１１が図の矢印に示す読取方向から視認可能なように、ＩＣカードを取り付け可能とする凹部３００を形成する。これにより、携帯電話機１の筐体に標識を貼り付けた場合と同様に、前記読取装置２２により、読取りが可能となる。

また、図３１（ｂ）に示すように、携帯電話機１に設けられたＩＣカード差込用スロット３０１を設けるとともに、当該スロット３０１にＩＣカード３１０が差し込まれた状態で、前記標識３１１が位置する部位に、外部の読取り装置から当該標識が読取（視認）可能となるような開口部３０２を形成することとしてもよい。この開口部３０２は、図の矢印に示す読取方向から前記標識３１１が視認可能であれば、透過性の樹脂材等により、その表面側をシールドしてもよい。

また、外部の読取装置により前記標識３１１が読取可能であれば、他の構成を用いてもよく、例えば、携帯電話機の筐体全体を内部が視認可能な透過性の樹脂材等により形成することとしてもよい。

これにより、次世代移動通信サービスに対応した携帯電話機等においても、本発明を適用することができるとともに、ＩＣカード内にクレジットカード番号等のデータを保存する必要がなくなり、セキュリティ性を高くすることができる。

なお、携帯電話機１において、前記標識３１１の読取装置を設け、その読取装置により前記標識を読取り、その読取情報を店舗側端末に送信することとしてもよい。

この場合には、例えば、図３２（ａ）に示すように、前記スロット３０１に差し込まれたＩＣカードの標識３１１が位置する部位に、前記制御部１３（図２（ａ）参照）に接続された読取センサ部３０３を設ける。これにより、当該読取センサ部３０３で読取った標識３１１の情報を携帯電話機１の送信手段を介して、前記認証サーバ４１に送信することができる。なお、標識３１１の情報の読取処理を、前記スロット３１１にＩＣカードを差し込む途中で行うこととしてもよく、この場合には、前記スロット内において前記標識３１１が通過する部位に対応する部位の一部にセンサ部を設けることとしてもよい。

また、ＩＣカード３１０を携帯電話機１に差し込むものに限らず、図３２（ｂ）に示すように、ＩＣカード３１０の一部を、携帯電話機１の側面に形成されたスリット３０４に挿入した状態で、図の矢印に示すスライド方向にスライドさせることで、図外のセンサ部により、ＩＣカード３１０内の情報を読取らせるものが考えられる。この場合には、ＩＣカード３１０の一部を前記スリット３０４内をスライドさせる際に、前記スリット３０４内において前記標識３１１が通過する部位に対応する部位の一部に、読取センサ部３０５を設けることとしてもよい。

また、ＩＣカード３１０として、無線または光による非接触型ＩＣカードを用いる場合には、各店舗等に設置された読取装置にＩＣカード３１０を挿入することにより、標識３１１を直接読取らせることとしてもよく、また、前記の例と同様に、携帯電話機１に読取装置を備えることとしてもよく、また、ＩＣカード３１０内の情報と同様に、無線又は光により、前記標識３１１の情報を認識させることとしてもよい。

【図面の簡単な説明】

【図１】 本発明の商取引方法を実施するシステムの実施形態を示すシステム構成図である。

【図２】 携帯電話機の構成を示す概略ブロック図である。

【図３】 携帯電話機に付けられる標識とバーコードおよび２次元コードの例を示す図である。

【図４】 携帯電話機に付けられたバーコードおよび表示部に表示された２次元コードを読み取る読取装置の断面構成図である。

【図５】 認証サーバの内部構成図である。

【図６】 店舗情報データベースに格納されるデータの一例を示す図である。

【図７】 利用者情報データベースに格納されるデータの一例を示す図である。

【図８】 購入履歴データベースに格納されるデータの一例を示す図である。

【図９】 不正利用情報データベースに格納されるデータの一例を示す図である。

- 【図 1 0】 携帯電話機を用いて一般店舗で商品代金を決済する手順を示すフローチャートである。
- 【図 1 1】 第 1 0 図の続きを示すフローチャートである。
- 【図 1 2】 携帯電話機に表示される Q R 決済証明鍵と店舗端末に表示される利用者情報の例を示す図である。
- 【図 1 3】 決済終了時に携帯電話機に表示される確認用の情報例を示す図である。
- 【図 1 4】 自動販売機で小額商品の決済を行う場合の手順を示すフローチャートである。
- 【図 1 5】 第 1 4 図の続きを示すフローチャートである。
- 【図 1 6】 インターネット上の店舗で注文した商品を指定の受取店舗で受け取って決済する場合の手順を示すフローチャートである。
- 【図 1 7】 第 1 6 図の続きを示すフローチャートである。
- 【図 1 8】 Q R 決済証明鍵を印刷したものを店舗に持参して決済する場合の手順を示すフローチャートである。
- 【図 1 9】 Q R 決済証明鍵を印刷した例を示す図である。
- 【図 2 0】 贈答情報データベースに格納されるデータの一例を示す図である。
- 【図 2 1】 他人への贈答品の決済をする場合の手順を示すフローチャートである。
- 【図 2 2】 図 2 1 の続きを示すフローチャートである。
- 【図 2 3】 図 2 2 の続きを示すフローチャートである。
- 【図 2 4】 携帯電話機に表示される贈答情報の表示例及び受諾又は拒絶の選択後の表示例を示す図である。
- 【図 2 5】 決済終了時に贈り手側の携帯電話機に表示される確認用の情報例を示す図である。
- 【図 2 6】 図 2 1 の続きを示すフローチャートである。
- 【図 2 7】 図 2 6 の続きを示すフローチャートである。
- 【図 2 8】 サービスポイント利用履歴データベースの一例を示す図である。
- 【図 2 9】 携帯電話機を用いて一般店舗でサービスポイントにより決済する手順を示すフローチャートである。
- 【図 3 0】 図 2 9 の続きを示すフローチャートである。
- 【図 3 1】 本発明に用いられる携帯電話機の一例を示す部分斜視図である。
- 【図 3 2】 本発明に用いられる携帯電話機の一例を示す部分斜視図である。