

(51)Int.Cl. ⁷	識別記号	F I	テマコード*(参考)
G 0 6 F 17/60	2 3 4	G 0 6 F 17/60	2 3 4 A 5 B 0 4 9
	2 3 2		2 3 2 5 B 0 5 5
	2 4 2		2 4 2
	4 1 4		4 1 4

審査請求 有 請求項の数30 O L (全 21 頁)

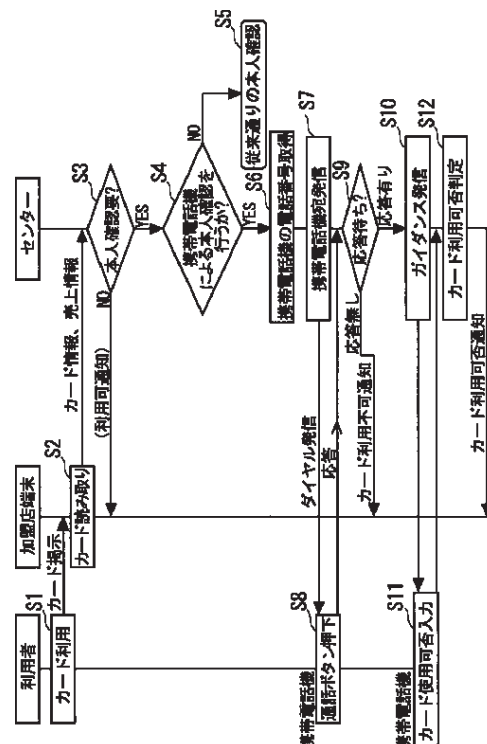
(21)出願番号	特願2000-118673(P2000-118673)	(71)出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22)出願日	平成12年4月19日(2000.4.19)	(72)発明者	小林 真一 東京都港区芝五丁目7番1号 日本電気株式会社社内
		(74)代理人	100080816 弁理士 加藤 朝道
		Fターム(参考)	5B049 BB11 EE23 GG00 5B055 EE15 HA12 HB07 JJ03 KK05

(54) 【発明の名称】 カードの不正使用防止方法及びシステム並びに記録媒体

(57) 【要約】

【課題】利用者がカードを利用するとき、利用者が本人であることを確認でき、第三者による不正使用を防止する方法及びシステムの提供。

【解決手段】加盟店でカードを利用するカード利用者が前記カードを所持する本人であることを確認するにあたり、加盟店端末で読み取られたカード番号を受信した、カード会社のセンターでは、カード番号から、前記センターのデータベースに予め登録されている前記利用者の移動体通信端末の電話番号を検索して前記カード利用者の移動体通信端末宛に発信し、前記利用者の移動体無線端末からカード使用可の旨が入力された場合に、本人確認ができたものとして、前記カードの利用を許可する。



【特許請求の範囲】

【請求項1】加盟店でカードを利用するカード利用者が前記カードを所持する会員本人であることを確認するにあたり、加盟店端末で読み取られ前記加盟店端末から送信されるカード番号を受信したセンターでは、前記カード番号に基づき、前記センターの記憶手段に予め登録されているカード会員の移動体通信端末の電話番号を検索して前記カード番号に対応する電話番号の移動体通信端末を呼び出し、前記移動体通信端末から、カード使用可の旨が入力された場合に、前記カードの利用を許可する、ことを特徴とするカードの不正使用防止方法。

【請求項2】前記移動体通信端末が前記呼び出しに応答しない場合、及び、前記呼び出しに応答した前記移動体通信端末からカード使用不可の旨が入力された場合に、前記センターでは、本人確認ができないものと判定し、前記カードの利用不可の旨を前記加盟店側に通知する、ことを特徴とする請求項1記載のカードの不正使用防止方法。

【請求項3】加盟店でカードを利用するカード利用者が前記カードを所持する会員本人であることを確認するにあたり、加盟店端末で読み取られ前記加盟店端末から送信されるカード番号を受信したセンターでは、前記カード番号に基づき、前記センターの記憶手段に予め登録されているカード会員の移動体通信端末の電話番号を検索して前記カード番号に対応する電話番号の移動体通信端末を呼び出し、前記移動体通信端末からパスワードが入力された際に、該パスワードを受け取った前記センターでは、前記受け取ったパスワードを、前記センターの記憶手段に予め登録されている、前記カード番号に対応する会員のパスワードと照合し、これらのパスワードが一致した場合に、前記カードの利用を許可する、ことを特徴とするカードの不正使用防止方法。

【請求項4】前記呼び出した移動体通信端末が応答しない場合、及び、前記呼び出した移動体通信端末から入力されたパスワードが、前記センターの記憶手段に予め登録されている、前記カード番号に対応する会員のパスワードと一致しない場合、本人確認ができないものと判定し、前記カードの利用不可の旨を、前記加盟店側に通知する、ことを特徴とする、請求項3記載のカードの不正使用防止方法。

【請求項5】加盟店端末に通信接続されカードの管理を行うセンター側に、会員のカード番号と対応させて、前記会員の個人情報として、前記会員が所持する移動体通信端末の電話番号を記憶保持するデータベースを設け、利用者が加盟店でカードを利用する時、前記加盟店端末で読み取られたカード番号を受信した前記センターでは、前記カード番号に基づき、前記データベースを検索し、前記カード番号に対応した電話番号を取得する第1のステップと、前記取得された電話番号の移動体通信端末宛に前記セン

ターから発信する第2のステップと、前記移動体通信端末への前記センターからの着信を受けて、前記利用者が前記移動体通信端末の操作部からカード使用可に対応する情報を入力し、前記センター側で前記移動体通信端末からのカード使用可に対応する情報を受信した場合に、本人であることが確認されたものとし、前記センターから、前記カードの利用が可である旨の通知を、前記加盟店端末に送信する第3のステップと、前記呼び出した移動体通信端末が応答しない場合、及び、前記呼び出した移動体通信端末からカード使用不可の情報が入力され、前記センター側でカード使用不可の情報を受信した場合に、前記センターは、前記カードの利用不可の旨の通知を、前記加盟店端末に送信する第4のステップと、を含む、ことを特徴とするカードの不正防止方法。

【請求項6】加盟店端末に通信接続されカードの管理を行うセンター側に、会員のカード番号と対応させて、前記会員の個人情報として、前記会員が所持する移動体通信端末の電話番号とパスワードとを記憶保持するデータベースを設け、利用者が加盟店でカードを利用する時、前記加盟店端末で読み取られたカード番号を受信した前記センターでは、前記カード番号に基づき、前記データベースを検索し、前記カード番号に対応した電話番号を取得する第1のステップと、前記取得された電話番号の移動体通信端末宛に前記センターから発信する第2のステップと、前記移動体通信端末への前記センターからの着信を受けて、前記利用者が前記移動体通信端末の操作部からパスワードを入力し、前記センター側で前記移動体通信端末から送信された前記パスワードを受信した場合に、前記受信したパスワードを、前記データベースに予め登録されている、前記カード番号に対応する会員のパスワードと照合し、パスワードが互いに一致した場合に、前記センターは前記カードの利用を許可する第3のステップと、前記呼び出した移動体通信端末が応答しない場合、及び、前記呼び出した移動体通信端末から入力されたパスワードが、前記データベースに予め登録されている前記カード番号に対応する会員のパスワードと一致しない場合、前記センターでは、本人確認ができないものと判定し、前記カードの利用不可の旨を、前記加盟店側に通知する第4のステップと、を含む、ことを特徴とするカードの不正防止方法。

【請求項7】前記移動体通信端末からのパスワード入力にかえて、前記加盟店端末から、前記利用者がパスワードを入力し、入力されたパスワードが、通信回線を介して、前記センター側に送信され、前記センター側でパスワードの認証が行われる、ことを特徴とする請求項6記

載のカードの不正防止方法。

【請求項 8】前記加盟店端末側に指紋入力手段を用意しておき、前記利用者の指紋情報が前記指紋入力手段から入力され、該入力された指紋情報が、通信回線を介して、前記センター側に送信され、前記センターでは、前記指紋情報を、前記データベース内に、前記カード番号に対応付けて登録されている指紋情報と照合することで、本人確認を行う、ことを特徴とする請求項 5 記載のカードの不正防止方法。

【請求項 9】加盟店でカードを利用するカード利用者が前記カードを所持する会員本人であることを確認するにあたり、加盟店端末で読み取られ前記加盟店端末から送信されるカード番号を受信したセンターでは、前記カード番号に基づき、前記センターの記憶手段に予め登録されているカード会員のメールアドレスを検索して、カード利用可否を問う電子メールを送信し、前記利用者が前記移動体通信端末からカード利用可の返信メールを受信した場合、前記カードの利用を許可する、ことを特徴とするカードの不正使用防止方法。

【請求項 10】加盟店端末に通信接続され前記加盟店でのカードの不正使用を防止する装置であって、会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末の電話番号を記憶保持する記憶手段を備え、カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記記憶手段を検索し、前記カード番号に対応した電話番号を取得する手段と、前記取得された電話番号の移動体通信端末宛に自動発信する手段と、前記移動体通信端末への着信に応答し、前記利用者が前記移動体通信端末の操作部から、カード使用可の情報を入力した場合、前記入力情報を無線通信回線及び電話網を介して受け取り、カード利用可の旨の通知を前記加盟店端末に送信する手段と、前記移動体通信端末が応答しない場合、及び、前記利用者が前記移動体通信端末からカード使用不可の情報を入力し、前記カード使用不可情報を無線通信回線及び電話網を介して受けとった場合、カード利用不可の旨の通知を前記加盟店端末に送信する手段と、を備えたことを特徴とするカード不正使用防止制御装置。

【請求項 11】加盟店端末に通信接続され前記加盟店でのカードの不正使用を防止する装置であって、会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末の電話番号と前記会員のパスワードとを記憶保持する記憶手段を備え、カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記

記憶手段を検索し、前記カード番号に対応した電話番号を取得する手段と、

前記取得された電話番号の移動体通信端末宛に自動発信する手段と、

前記移動体通信端末への着信に応答し、前記利用者が前記移動体通信端末の操作部からパスワードを入力した際、無線通信回線及び電話網を介して送信される前記パスワードを受け取り、前記パスワードを、前記記憶手段に前記カード番号に対応付けて登録されているパスワードと照合し、パスワードが一致した場合、カード利用可の旨の通知を、前記加盟店端末に送信し、一方、パスワードが不一致の場合、カード利用不可の旨の通知を、前記加盟店端末に送信する手段と、を備えたことを特徴とするカード不正使用防止制御装置。

【請求項 12】加盟店端末に通信接続され前記加盟店でのカードの不正使用を防止する装置であって、会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末用のメールアドレスを記憶保持する記憶手段を備え、カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記記憶手段を検索し、前記カード番号に対応したメールアドレスを取得する手段と、前記取得されたメールアドレス宛に、カード使用可否を問い合わせる電子メールを自動送信する手段と、前記利用者が、前記センターから送信されたメールを前記移動体通信端末で取り出し、前記移動体通信端末からカード使用可のメールを返信した場合、カード利用可の旨の通知を前記加盟店端末に送信し、一方、前記利用者が前記移動体通信端末からカード使用不可のメールを返信した場合、カード利用不可の旨の通知を前記加盟店端末に送信する手段と、を備えたことを特徴とするカード不正使用防止制御装置。

【請求項 13】カード読み取り装置を備えた加盟店端末と、前記加盟店端末に通信接続されカードの管理を行うセンターと、を含むカードオーソライゼーションシステムにおけるカード不正使用防止システムであって、前記センターが、会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末の電話番号を記憶保持するデータベースを備え、カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応した電話番号を取得する手段と、前記取得された電話番号の移動体通信端末宛に自動発信する手段と、前記利用者が、前記移動体通信端末への着信報知を受けてオフフックした際に、カード使用可否について入力す

るように指示するガイダンス情報を、前記移動体通信端末に送信する手段と、
前記利用者が前記移動体通信端末の操作部からカード使用可の情報を入力した場合、前記カード使用可情報を無線通信回線及び電話網を介して受け取り、前記カードの利用可の旨の通知を、前記加盟店端末に送信する手段と、
前記移動体通信端末が前記センターからの呼び出しに 응답しない場合、及び、前記利用者が前記移動体通信端末の操作部からカード使用不可の情報を入力し前記カード使用不可情報を無線通信回線及び電話網を介して受信した場合に、前記カードの利用不可の旨の通知を、前記加盟店端末に送信するように制御する手段と、
を備えたことを特徴とするカード不正使用防止システム。

【請求項 14】カード読み取り装置を備えた加盟店端末と、前記加盟店端末に通信接続されカードの管理を行うセンターと、を含むカードオーソライゼーションシステムにおけるカード不正使用防止システムであって、
前記センターが、会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末の電話番号とパスワードとを記憶保持するデータベースを備え、
利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応した電話番号を取得する手段と、
前記取得された電話番号の移動体通信端末宛に自動発信する手段と、
前記利用者が、前記移動体通信端末への着信報知を受けてオフフックした際に、パスワードを入力するように指示するガイダンス情報を、前記移動体通信端末に送信する手段と、
前記利用者が前記移動体通信端末の操作部からパスワードを入力した際、無線通信回線及び電話網を介して送信される前記パスワードを受け取り、前記パスワードから前記データベースを参照して、前記カード番号に対応して登録されているパスワードと照合し、照合の結果、パスワードが一致した場合、前記カードの利用可の旨の通知を、前記加盟店端末に送信する手段と、
前記移動体通信端末が前記センターからの呼び出しに 응답しない場合、及び、前記パスワードの照合の結果、パスワードが不一致の場合に、前記カードの利用不可の旨の通知を、前記加盟店端末に送信するように制御する手段と、
を備えたことを特徴とするカード不正使用防止システム。

【請求項 15】カード読み取り装置を備えた加盟店端末と、前記加盟店端末に通信接続されカードの管理を行うセンターと、を含むカードオーソライゼーションシステム

におけるカード不正使用防止システムであって、
前記センターが、会員のカード番号と対応させて、前記会員の個人情報として、メール送受信機能を備えた移動体通信端末を所持する会員について前記移動体通信端末用のメールアドレスを記憶保持するデータベースを備え、
カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応したメールアドレスを取得する手段と、
前記取得されたメールアドレス宛に、カード使用可否を問い合わせる電子メールを自動送信する手段と、
前記利用者が、前記センターから送信されたメールを前記移動体通信端末で取り出し、前記移動体通信端末からカード使用可のメールを返信した場合、前記カードの利用可の旨の通知を、前記加盟店端末に送信する手段と、
前記移動体通信端末からの応答がない場合、及び、前記移動体通信端末からカード使用不可のメールが返信された場合、前記カードの利用不可の旨の通知を前記加盟店端末に送信するように制御する手段と、
を備えたことを特徴とするカード不正使用防止システム。

【請求項 16】前記データベースに、前記会員毎に、カード利用時に、移動体通信端末の呼出しによる本人確認を行うか否かを記録する領域を備え、移動体通信端末の呼出しによる本人確認を行うか否かの設定が変更自在とされている、ことを特徴とする請求項 13 乃至 15 のいずれかに記載のカード不正使用防止システム。

【請求項 17】前記加盟店端末に接続され、指紋情報を入力する指紋入力装置を備え、
前記利用者の指紋情報が前記指紋入力装置から入力され、該入力された指紋情報が、前記加盟店端末から、通信回線を介して、前記センター側に送信され、前記センターでは、前記指紋情報を、前記データベース内に、前記カード番号に対応付けて登録されている指紋情報と照合することで、本人確認を行う、ことを特徴とする請求項 13 又は 14 記載のカード不正使用防止システム。

【請求項 18】前記加盟店端末がパスワード入力手段を備え、前記移動体通信端末からのパスワードの入力にかえて、前記加盟店端末のパスワード入力手段から、前記利用者がパスワード入力し、入力されたパスワードが、通信回線を介して、前記センター側に送信され、前記センターでは、前記パスワードを受け取り、前記パスワードから前記データベースを参照して、前記カード番号に対応して登録されているパスワードと照合する、ことを特徴とする請求項 14 記載のカード不正使用防止システム。

【請求項 19】カード読み取り装置を備えた加盟店端末に通信接続され、カードの管理を行うセンターにおいて、

会員のカード番号と対応させて、前記会員の個人情報として、移動体通信端末の電話番号を記憶保持するデータベースを備え、

(a) カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索し、前記カード番号に対応した電話番号を取得する処理と、

(b) 前記取得された電話番号の移動体通信端末宛に自動発信する処理と、

(c) 前記利用者が、前記移動体通信端末への着信報知を受けてオフフックした際に、カード使用可否について入力するように指示するガイダンス情報を、前記移動体通信端末に送信する処理と、

(d) 前記利用者が前記移動体通信端末の操作部からカード使用可の情報を入力した場合、前記カード使用可情報を無線通信回線及び電話網を介して受け取り、前記カードの利用可の旨の通知を前記加盟店端末に送信し、一方、前記利用者が前記移動体通信端末の操作部からカード使用不可の情報を入力した際、前記カード使用不可情報を無線通信回線及び電話網を介して受けて、前記カードの利用不可の旨の通知を前記加盟店端末に送信する処理と、

の前記(a)乃至(d)の各処理を前記センターのコンピュータ上で実行させるためのプログラムを記録した記録媒体。

【請求項20】カード読み取り装置を備えた加盟店端末に通信接続されカードの管理を行うセンターにおいて、会員のカード番号と対応させて、前記会員の個人情報として、移動体通信端末の電話番号とパスワードとを記憶保持するデータベースを備え、

(a) 利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索し、前記カード番号に対応した電話番号を取得する処理と、

(b) 前記取得された電話番号の移動体通信端末宛に自動発信する処理と、

(c) 前記利用者が、前記移動体通信端末への着信報知を受けてオフフックした際に、パスワードを入力するように指示するガイダンス情報を、前記移動体通信端末に送信する処理と、

(d) 前記利用者が前記移動体通信端末の操作部からパスワードを入力した際、無線通信回線及び電話網を介して送信される前記パスワードを受け取り、前記パスワードから前記データベースを参照して、前記カード番号に対応して登録されているパスワードと照合し、照合の結果、一致した場合、前記カードの利用可の旨の通知を、前記加盟店端末に送信し、パスワードが不一致の場合、前記カードの利用不可の旨の通知を、前記加盟店端末に送信する処理と、

の前記(a)乃至(d)の各処理を前記センターのコン

ピュータ上で実行させるためのプログラムを記録した記録媒体。

【請求項21】カード読み取り装置を備えた加盟店端末に通信接続されカードの管理を行うセンターにおいて、会員のカード番号と対応させて、前記会員の個人情報として、メール送受信機能を備えた移動体通信端末を所持する会員についてそのメールアドレスを記憶保持するデータベースを備え、

(a) カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応した前記メールアドレスを取得する処理と、

(b) 前記メールアドレス宛に、カード使用可否を問い合わせる電子メールを自動送信する処理と、

(c) 前記利用者が、前記センターから送信されたメールを前記移動体通信端末で取り出し、前記移動体通信端末からカード使用可のメールを返信した場合、前記カードの利用可の旨の通知を前記加盟店端末に送信し、一方、前記利用者が前記移動体通信端末からカード使用不可のメールを返信した場合、前記カードの利用不可の旨の通知を前記加盟店端末に送信する処理と、

の前記(a)乃至(c)の各処理を前記センターのコンピュータ上で実行させるためのプログラムを記録した記録媒体。

【請求項22】請求項19乃至21のいずれか一に記載の記録媒体において、

前記加盟店端末に接続された指紋入力装置から入力された前記利用者の指紋情報が、前記加盟店端末から、通信回線を介して、前記センター側に送信され、

前記センターにおいて、前記指紋情報を、前記データベース内に、前記カード番号に対応付けて登録されている指紋情報と照合することで、本人確認を行う処理を前記センターのコンピュータ上で実行させるためのプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、カードの不正使用防止方法及びシステムに関し、特に、カード会員が商品代金の決済及び融資等に利用するクレジットカード等のカードの不正使用防止に用いて好適な方法及びシステム並びに記録媒体に関する。

【0002】

【従来の技術】クレジットカードは、現金、小切手につぐ第三の通貨として、広範に利用されており、現在、クレジットカード業務も、信販系、銀行系、小売り系、石油系等、多業種にわたっている。また現今、クレジットカード、キャッシュカード、デビットカードの共通化(一元化)の提案もなされている。

【0003】クレジットカード利用時、カード会員は、自己のクレジットカードを加盟店に提示し、加盟店端末

(カード・オーソライゼーション・ターミナル)でクレジットカードを読み取らせ、該端末から、クレジットカード情報と、売り上げ内容等が、通信回線を介して、カード会社のカード管理センターのホストコンピュータにオンラインで送信され、クレジットカードの信用度を調べる等必要に応じてオーソライゼーションが行われる。

【0004】上記オーソライゼーション結果に問題がなく、カード利用可の場合、カード利用者は、利用明細伝票の所定箇所に署名記入等を行うことで、カードによる一連の商品購入手順が完了し、該商品の代金はクレジットカード会社等から支払われ、後に、利用者の銀行口座から所定の手数料とともに代金が引き落とされる。

【0005】

【発明が解決しようとする課題】ところで、クレジットカードは、それが真正でありさえすれば、カード会員本人でなくても、他者により、不正利用されてしまい、紛失盗難等によりクレジットカードが無断使用された会員は損失を被り、また偽造のクレジットカードであっても、オーソライゼーションがパスしてしまえば、該偽造クレジットカードで、商品購入、融資等の不正使用が行われ、カード会社が損失を被る、ことになる。

【0006】これらカードの不正使用に対するセキュリティ管理として、カード利用時に、本人確認のため、典型的には、以下の手順が取られている。

【0007】すなわち、カード利用者が、クレジットカードを利用して所定の金額以上の商品の購入を行うことが、クレジットカード会社側で検出された場合、クレジットカード会社の担当者が、加盟店に電話連絡し、加盟店の電話口に出たカード利用者に対して、担当者は、会員の個人情報に基づき、本人であることを確認するためにいくつかの質問を発する。この質問としては、利用者の勤務先電話番号等、通常、本人でしか、即座、且つ自然に答えることのできない質問とされる。

【0008】そして、カード利用者が、担当者の質問に正しく応答できた場合、カード利用者がカードを所持する会員本人であることが確認され、その結果、カードの利用(カードによる決済)が許可される。

【0009】しかしながら、カード利用者が商品の購入等にあたり、カード会社の担当者が会員情報等をみながら電話でカード利用者に対して本人確認の質問を行うことは、作業工数の点で、非効率であるといえる。

【0010】今後、カード利用件数の激増が予測されることから、本人確認の正確さを低下させることなく、カード会社で行われる、本人確認作業の自動化、省力化が望まれる。

【0011】さらに、上記した従来の本人確認作業は、カード利用者をして、クレジットカード会社、あるいは加盟店の売場担当者等から、本人であることが確認されるまでの間、自分に疑いをかけられているという思いを抱かせることにもなりかねず、カード利用者の気分を害

する可能性も全くなきにしもあらずといえる。結果として、十分な顧客満足(CS; Customer Satisfaction)が提供できない場合もあり、販売促進活動の逆効果ともなりかねない。

【0012】したがって、本発明は、上記問題点を鑑みてなされたものであって、その主たる目的は、カード利用者がカードを所持する会員本人であることをセンター側で確認する作業を容易化し、第三者による不正使用を防止する方法と装置及びシステム並びに記録媒体を提供することにある。

【0013】本発明の他の目的は、カード不正使用を防止するにあたり、開発コスト、設備投資の増大を抑止し、加盟店、カード会社の負担を軽減しながら、高いセキュリティを保ち、販促活動に貢献する方法と装置及びシステム並びに記録媒体を提供することにある。

【0014】

【課題を解決するための手段】前記目的を達成する本発明は、加盟店でカードを利用するカード利用者が前記カードを所持する会員本人であることを確認するにあたり、加盟店端末で読み取られ前記加盟店端末から送信されるカード番号を受信したセンターでは、前記カード番号に基づき、前記センターの記憶手段に予め登録されているカード会員の移動体通信端末の電話番号を検索して前記カード番号に対応する電話番号の移動体通信端末を呼び出し、前記移動体通信端末から、カード使用可の旨が入力された場合に、前記カードの利用を許可する。

【0015】本発明においては、前記呼び出した移動体通信端末が応答しないか、あるいは、前記呼び出した移動体通信端末からカード使用不可の旨が入力された場合に、本人確認ができないものと判定し、前記カードの利用の不許可の旨を前記加盟店側に通知する。

【0016】本発明においては、好ましくは、前記カード利用者の移動体通信端末からパスワードが入力され、該パスワードをセンターの記憶装置に登録されているパスワードと照合し、パスワードが一致した場合に、前記カードの利用を許可するようにしてもよい。

【0017】さらに、本発明においては、パスワードを加盟店端末から入力するか、あるいは、カード利用者の指紋を入力し、センターにおいて、指紋情報を、データベースに登録された特徴情報と照合することで本人確認を行うようにしてもよい。そして、以下の説明からも明らかとされるように、上記目的は、特許請求の範囲の各請求項に記載された本発明によって、同様に達成される。

【0018】

【発明の実施の形態】本発明の実施の形態について以下に説明する。本発明の好ましい一実施の形態において、加盟店端末に通信接続されるカード会社のセンターに設置されるオーソライゼーション用のデータベースには、カード番号(カードID)と対応させて、カード会員の

個人情報として、カード会員の所持する携帯電話機またはPHS（パーソナルハンディホンシステム）端末等の移動体通信端末の電話番号が登録される。

【0019】カード作成手続の上で、利用者は、カード作成時、申請書に、所用情報として、利用者の所持する移動体通信端末の電話番号を記載する。カード会社における当該申請書に対する審査の結果、利用者に対してカード発行が認められた場合、この電話番号は、発行されたカードを一義的に識別するためのカード番号（ID）と対応付けて、会員個人情報として、カード会社のデータベースに登録される。また、申請書に記載されたパスワードもカード番号（ID）と対応付けて、データベースに登録される。なお、カード会員の所持する移動体通信端末の電話番号に変更があった場合、カード会員は、カード会社にその旨を連絡して、センターのデータベースの内容が更新される。

【0020】またカードの不正使用防止のために、移動体通信端末への呼出しによる本人確認処理を行うか否かについて、カード作成時に選択できるものとし、カード作成後も、移動体通信端末への呼出しによる本人確認処理を行うか否かについての設定が変更できるものとする。カード利用時に移動体通信端末への呼出しによる本人確認を行わない場合、従来通りの手順で、本人確認が行われることになる。このため、移動体通信端末を所持しない会員も、そのままカードの利用を行うことができる。

【0021】利用者が、加盟店でカード利用時、加盟店端末から、センターに送信される情報のうち、カード番号に基づき、センターでは、データベースから、カード利用時に移動体通信端末への呼出しによる本人確認を行うモードに設定されているか否かを確認し、カード利用時に移動体通信端末への呼出しによる本人確認を行うモードの場合、データベースからカード番号に対応した電話番号を検索する。

【0022】センターでは、検索された電話番号宛に発信する。この場合、好ましくは、検索された電話番号（発信電話番号）を自動ダイヤル発信装置にセットすることで、移動体通信端末宛に自動発信される。

【0023】利用者が、利用者本人が所持する移動体通信端末への着信報知（鳴動又はバイブレータ振動）を受けて、オフフック（すなわち通話ボタンを押下）した際に、カード使用の可否について応答するように、音声ガイダンス、もしくは文字表示で、移動体通信端末に通知する。

【0024】利用者が、移動体通信端末の操作部から、カード使用可の情報を入力した場合に、これを受信したセンターでは、本人確認が行われたものと判定し、カード利用可の通知を、前記加盟店に端末に送信する。

【0025】一方、センター側からの移動体通信端末への呼出しに対して、移動体通信端末が応答せず、必要に

応じて、所定のリトライを行ってもなお通話接続不可の場合には、カード利用が不可であることを、加盟店に通知する。

【0026】また利用者が、移動体通信端末の操作部から、カード使用不可の情報を入力した場合に、これを受信したセンターでは、カード利用不可の通知を、加盟店端末に送信する。

【0027】例えば第三者が、カード会員のカードを盗んで不正使用するか、あるいは偽造カードを用いる場合、当該カード会員は、カード会社のセンターから移動体通信端末に呼出しを受けることで、自分以外の者が、自分のカードを不正使用していることを認識することができ、移動体通信端末から、カード使用不可の情報を入力して、センター側に知らせる。

【0028】本発明の一実施の形態においては、移動体通信端末から入力されるカード使用可を示す情報は、前記移動体通信端末で通知されるガイダンスで指示したコードであってもよい。

【0029】すなわち、この実施の形態においては、
・カード利用者が、契約（カード利用規則）に従い、カード利用時、予め登録済みの電話番号の移動体通信端末を所持しており、

・センターからの移動体通信端末への呼出しに応答し、カード使用化を入力した、
ということで、本人確認が行えたものとしている。カード会員は、カード作成時の契約等で、所定金額以上の商品をカードで決済する場合、携帯電話機による本人確認を行うことを承知した上で、携帯電話機による本人確認モードを選択しており、また今日、携帯電話機は、多数の者が所持していることから、携帯電話機の所持に対する利用者の負担等は、ほとんどないものといえる。

【0030】さらにセキュリティを高めるためには、利用者が、移動体通信端末への着信報知を受けて、オフフックした際に、利用者が、パスワードを入力するように、音声ガイダンスもしくは文字表示で該移動体通信端末に通知し、該通知を認識した利用者は、該移動体通信端末から、所定桁数のパスワードを入力し、このパスワードは、センター側に送信され、センタでは、データベースに登録されているパスワードと照合することで、本人確認を行うようにしてもよい。

【0031】さらに、本発明の別の実施の形態において、移動体通信端末からのパスワード入力に換えて、加盟店端末からパスワード入力し、通信回線を介して、前記センター側にパスワードを送信する構成としてもよい。この場合も、カード利用時に、移動体通信端末に発信し、その応答をうけて、本人確認を行うシステムと組み合わせることで、セキュリティの向上を図ることができる。

【0032】さらにまた、本発明の別の実施の形態において、加盟店端末が指紋入力手段を備え、前記利用者の

指紋情報が指紋入力手段から入力され、該入力された指紋情報が、通信回線を介して、前記センター側に送信され、前記データベースに前記カード番号に対応して登録されている指紋情報と照合され、本人確認が行われる構成としてもよい。現今、コンピュータにログイン時のユーザID、パスワード入力に換えて、指紋照合により認証を行う装置も開発されており、指紋照合に要する時間も短縮されていることから、本人確認に有効であるといえる。

【0033】さらに、本発明の別の実施の形態において、加盟店でカードを利用するカード利用者が前記カードを所持する会員本人であることを確認するにあたり、加盟店端末から送信されるカード番号を受信したセンターでは、前記カード番号に基づき、前記センターのデータベースに予め登録されているカード会員のメールアドレスを検索して、カード利用可否を問う電子メールを送信し、前記利用者が、電子メール送受機能を備えた移動体通信端末等からカード利用可の返信メールを受信した場合、前記カードの利用を許可する構成としてもよい。

【0034】上記した実施の形態において、カード利用者が本人であるにもかかわらず、カード利用時、カード会員が所持する移動体通信端末へ発信等が成功せず、本人確認が行えない場合、従来通りの処理手順による本人確認作業が行われることになり、本発明のシステムの導入及び運用による利用者側の不都合（カードが利用できなくなるといった事態の発生）等は生じない。

【0035】本発明の一実施の形態において、カード読み取り装置を備えた加盟店端末に通信接続され、カードの管理を行うセンターが、会員のカード番号と対応させて、前記会員の個人情報として、会員の所持する移動体通信端末の電話番号を記憶保持するデータベースを備え、（a）カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応した電話番号を取得する処理と、（b）前記取得された電話番号の移動体通信端末宛に自動発信する処理と、（c）前記利用者が、前記移動体通信端末への着信報知を受けてオフフックした際に、カード使用可否について入力するように指示するガイダンス情報を、前記移動体通信端末に送信する処理と、（d）前記利用者が前記移動体通信端末からカード使用可を入力した場合、前記カード使用可情報を無線通信回線及び電話網を介して受け取り、前記カードの利用可の旨の通知を前記加盟店端末に送信し、一方、前記利用者が前記移動体通信端末からカード使用不可の情報を入力した際、前記カード使用不可情報を無線通信回線及び電話網を介して受けて、前記カードの利用不可の旨の通知を前記加盟店端末に送信する処理と、を実行する。前記（a）乃至（d）の各処理は、センターのコンピュータ上でプログラムを実行することで実現される。

【0036】本発明の別の一実施の形態において、カード読み取り装置を備えた加盟店端末に通信接続されカードの管理を行うセンターが、会員のカード番号と対応させて、前記会員の個人情報として、会員の所持する移動体通信端末の電話番号とパスワードとを記憶保持するデータベースを備え、（a）利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応した電話番号を取得する処理と、（b）前記取得された電話番号の移動体通信端末宛に自動発信する処理と、（c）前記利用者が、前記移動体通信端末への着信報知を受けてオフフックした際に、パスワードを入力するように指示するガイダンス情報を、前記移動体通信端末に送信する処理と、（d）前記利用者が前記移動体通信端末の操作部からパスワードを入力した際、無線通信回線及び電話網を介して送信される前記パスワードを受け取り、前記パスワードから前記データベースを参照して、前記カード番号に対応して登録されているパスワードと照合し、照合の結果、一致した場合、前記カードの利用可の旨の通知を、前記加盟店端末に送信し、パスワードが不一致の場合、前記カードの利用不可の旨の通知を、前記加盟店端末に送信する処理と、を実行する。前記（a）乃至（d）の各処理は、センターのコンピュータ上でプログラムを実行することで実現される。

【0037】本発明のさらに別の一実施の形態において、カード読み取り装置を備えた加盟店端末に通信接続されカードの管理を行うセンターが、会員のカード番号と対応させて、前記会員の個人情報として、メール送受信機能を備えた移動体通信端末を所持する会員についてそのメールアドレスを記憶保持するデータベースを備え、（a）カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応した前記メールアドレスを取得する処理と、（b）前記メールアドレス宛に、カード使用可否を問い合わせる電子メールを自動送信する処理と、（c）前記利用者が、前記センターから送信されたメールを前記移動体通信端末で取り出し、前記移動体通信端末からカード使用可のメールを返信した場合、前記カードの利用可の旨の通知を前記加盟店端末に送信し、一方、前記利用者が前記移動体通信端末からカード使用不可のメールを返信した場合、前記カードの利用不可の旨の通知を前記加盟店端末に送信する処理と、を実行する。前記（a）乃至（c）の各処理は、センターのコンピュータ上でプログラムを実行することで実現される。

【0038】上記実施の形態において、前記各処理を、センターのコンピュータに実行させるプログラムを記録した記録媒体（FD（フロッピー（登録商標）ディスク）、CD-ROM、DVD（digital versatile disk）、HDD（ハードディスク媒体）、磁気テープ、半

導体メモリ等)から該プログラムをコンピュータに読み出して実行するか、遠隔サーバ装置等から通信媒体を介してセンターのコンピュータに該プログラムをダウンロードしてインストール及び実行する、ことで本発明を実施することができる。

【0039】

【実施例】上記した本発明の実施の形態についてさらに詳細に説明すべく、本発明の実施例について図面を参照して説明する。

【0040】図1は、本発明の一実施例のシステム構成を示す図である。図1を参照すると、本発明の一実施例は、クレジットカード読み取り装置を備えた加盟店端末2と、加盟店端末2と通信回線3で接続されカード管理を行う、クレジットカード会社のセンター1と、を備えている。加盟店端末2と通信接続されるクレジットカード会社のセンター1とは、例えば専用の通信回線3で接続されるが、さらに公衆網等の地上ネットワークの他、衛星通信回線等で接続してもよい。なお、図1には、簡単のため、加盟店端末2一台が示されているが、通常、センター1には、複数の加盟店端末2が接続される。クレジットカード読み取り装置を備えた加盟店端末2は周知の構成の端末が用いられ、本実施例では、加盟店に既設の端末がそのまま用いられる。

【0041】本発明の一実施例の処理動作の概略は以下のようなものとなる。

【0042】利用者7が、カード加盟店で商品購入時等の支払いにカードを利用する際に、利用者7のカード8を加盟店の店員(不図示)に渡し、加盟店端末2でカード情報の読み取りが行われ、カード情報、及び売り上げ情報が、加盟店端末2から通信回線3を介してセンター1に送信される。

【0043】センター1では、加盟店端末2から送信されたカード番号から、予め登録されている利用者の携帯電話機の電話番号を検索して、利用者の携帯電話機6宛に発信する。

【0044】センター1からの呼は、電話網4、携帯電話機6のゾーンを管理する無線基地局5を介して、利用者7の携帯電話機6に着信する。利用者が携帯電話機6の着信報知に回答して通話接続し、携帯電話機6からカード使用可の旨が入力された場合に、カードの利用が可とされる。

【0045】なお、利用者が所持する移動体通信端末として携帯電話機を例に説明するが、PHS(パーソナルハンディホンシステム)端末(簡易携帯電話機)であってもよいことは勿論である。

【0046】図2は、本発明の一実施例におけるセンター1の構成の一例を示す図である。なお、図2には、センター1において、本発明の要部をなすカード不正使用防止機能に関連する構成要素だけが図示されており、他の構成要素は省略されている。

【0047】図2を参照すると、本発明の一実施例におけるセンター1は、会員毎に、カードの番号(ID)と対応付けて、会員情報として、会員の携帯電話番号、パスワード等が登録されているデータベース12と、加盟店端末2との間で通信回線3を介してデータを送受するためのインタフェースを提供する通信回線インタフェース18と、加盟店端末2から送信されるカード情報を受信する通信回線インタフェース18からカード情報を受け取りカード番号を取得するカード番号取得部10と、カード番号取得部10で取得されたカード番号を受け取り、該カード番号からデータベース12を検索し、該カード番号に対応するレコードデータから、携帯電話機による本人確認を行うモードに設定されているか否かを確認する本人確認要否判定部11と、携帯電話機による本人確認を行う場合に、データベース12から該カード番号に対応した電話番号を取得する携帯電話番号取得部13と、電話端末インタフェース15を制御して、携帯電話番号取得部13から渡された電話番号に基づき、カード利用者の携帯電話機に自動発信し、カード利用者の携帯電話機からの応答、ガイダンス送信等を管理する電話発信・応答制御部14と、カード利用者の携帯電話機6の操作部からの入力情報に基づき、カードの利用の可否を判定するカード利用可否判定部16と、カード利用可否判定部16の判定結果を、通信回線インタフェース18を介して加盟店端末2に送信するカード利用可否通知部17と、を備えている。センター1における上記各部分は、センター1のコンピュータ上で実行されるプログラム制御により、その処理・機能が実現される。なお、通信回線3は電話網であってもよい。

【0048】携帯電話機6(図1参照)に対するセンター1からの呼出しに対して、携帯電話機6が応答し、カード使用可の情報が入力された場合、該カード使用可の情報を電話網4を介して受け取る電話発信・応答制御部14からの情報に基づき、カード利用可否判定部16において、カード利用可とする。

【0049】一方、携帯電話機6から、カード使用不可の情報が入力された場合、あるいは、携帯電話機6に対する呼出しに対して、携帯電話機6が応答しない場合(圏外、電源オフ等も含む)、カード利用可否判定部16は、カード利用を不可に設定する。電話発信・応答制御部14は、携帯電話機6の呼び出しに対する着信応答受信のタイムアウト管理機能を具備している。

【0050】なお、カード作成時に、利用者は申請書に、携帯電話機による本人確認を行うか否かの有無、携帯電話機による本人確認を行う場合、利用者の所持する携帯電話機の電話番号、パスワードを記載し、携帯電話機の電話番号と、必要に応じてパスワードもカード番号(ID)と対応付けて、データベース12に登録される。

【0051】すでにカードを保有しているカード会員

は、カード会社に、該カード会員の所有する携帯電話番号を通知するだけで、本発明に係るシステムのサービスを受けることができ、新たにカードの発行等を行う必要はない。

【0052】図3は、本発明の一実施例におけるカード会員を管理するデータベース12の構成の一例を模式的に示す図である。図3を参照すると、カード番号（識別情報）と、カード会員の氏名、性別、年齢、住所等の個人情報に加えて、カード利用時携帯電話機による本人確認を行うか否かの情報、携帯電話機による本人確認を行う場合の会員の携帯電話機の電話番号、及びパスワード情報等を、一エントリあたり含む。データベース12には、これ以外にも、カード利用の履歴情報、信用度チェック用の各種情報が含まれるが、これらの情報は、本発明の主題に直接関係するものでないことから、いずれも省略されている。

【0053】図4は、本発明の一実施例における利用者7（携帯電話機6）、加盟店端末2、及び、センター1の処理フローを説明するための図である。図1乃至図4を参照して、本発明の一実施例の動作について説明する。

【0054】利用者7が、加盟店で、カード利用時（ステップS1）、加盟店端末2では、カードを読み取り（ステップS2）、カード情報、売り上げ情報が、センター1に送信される。

【0055】センター1では、加盟店端末2からの情報を受信し、例えば利用金額が低額である等、本人確認を要しない場合には、カード利用可を通知し、通常通りのカード決済処理が行われる（ステップS3のNO）。

【0056】一方、カードによる高額代金の支払い等の場合、センター1では、データベース12を参照して、カード番号に基づき、カード利用時携帯電話機による本人確認を行うモードに設定されているかチェックし（ステップS4）、携帯電話機による本人確認を行うモードに設定されていない場合、従来通り、センター1の担当者から、加盟店に設置されている電話口の利用者を呼び出して本人確認等を行う（ステップS5）。

【0057】携帯電話機による本人確認を行うモードに設定されている場合、データベース12から、カード番号に対応して登録されている携帯電話機の電話番号を検索して取得し（ステップS6）、携帯電話機の電話番号に自動ダイヤルする（ステップS7）。

【0058】利用者が携帯電話機6の着信鳴動等に応答して通話ボタンを押下（オフフック）した場合（ステップS8）、センター1では、この応答を受けて（ステップS9の「応答有り」）、ガイダンス発信を行う（ステップS10）。ガイダンスは音声でも文字情報であってもよい。例えば、音声ガイダンスの場合、「弊社クレジットカードをご利用いただきましてありがとうございます。ただいまのご利用につきまして、カードご使用可で

したら、使用可を入力してください。」といった類のガイダンス情報を流す。このガイダンス情報の記憶及び送信制御は、電話発信・応答制御部16と電話端末インタフェース15によって行われる。

【0059】このガイダンス情報には、カードが利用される加盟店の店舗情報を通知するようにしてもよい。カード利用者がカード会員本人以外の者である場合、カード会員本人は、このガイダンス情報から、カードの不正使用が行われたこと、及びその場所を認識することができる。

【0060】利用者は、携帯電話機6から、カード使用可否の入力（カード会社との間で決められた数字と#等）を入力する（ステップS11）。このカード使用可、使用不可の入力情報は、カード作成時等に取り決められる数字（例えば使用可は1、使用不可は0）、もしくは、所定の操作ボタンであってもよい。

【0061】センター1は、携帯電話機6から送信されたカード使用可否情報を判断して、カードの利用可否を判定し（ステップS12）、利用可否の判定結果を加盟店端末2に通知する。

【0062】ところで、このシステムを何度も利用しており、すでに携帯電話機によるカード使用可否の入力に慣れており、詳細ガイダンスの通知が不要の利用者には、ガイダンス情報を簡略化、もしくは省略するようにしてもよい。会員毎のガイダンス要・不要等は、センター1のデータベース12で、会員毎に、適宜登録管理される。

【0063】利用者7が携帯電話機6から、カード使用可の情報を入力し、本人であることが確認された旨の通知（カード利用可の通知）が、加盟店端末2に送信されることで、カードにより決済が行われることになる。すなわち、利用者は、明細伝票にサイン（署名）を記入し、カードによる商品購入処理が完了する。

【0064】一方、図4のステップS9の着信応答待ちの結果、タイムアウト発生等により、携帯電話機6からの応答がない場合（圏外、電源オフ等で通話不能も含む）、センター1は、加入者端末2にカード利用不可を通知する。

【0065】本発明の一実施例において、利用者がカード会員本人であり、カード利用時に携帯電話機不携帯であるか、電池切れ等により、携帯電話機による応答ができない場合、加盟店の電話機等を介して、従来の方法により、カード会社との間で、本人確認を行った上で、カードの利用が行われる。なお、上記実施例では、カード番号から検索された携帯電話機の電話番号宛に自動発信する構成を例に説明したが、オペレータ等が、カード番号から検索された携帯電話機の電話番号に基づき、手動で、携帯電話機に発信するようにするビジネス業務形態にも、本発明が適用可能であることは勿論である。

【0066】次に、本発明の第2の実施例について説明

する。本発明の第2の実施例は、カード利用者が、本人確認のためにセンター1側から携帯電話機6に対して行われる呼出しに対して、携帯電話機6から、パスワードを入力するものである。本発明の第2の実施例において、システムの基本構成は、図1に示したものと同様とされる。

【0067】図5は、本発明の第2の実施例におけるセンター1の構成を示す図である。図5を参照すると、本発明の第2の実施例は、前記第1の実施例のカード利用可否判定部16を、パスワード認証部19に置き換えたものである。本発明の第2の実施例において、カード番号取得部10、本人確認要否判定部11、携帯電話番号取得部13、電話発信・応答制御部14の構成は、前記第1の実施例と基本的に同一である。センター1における上記各部は、センター1のコンピュータ上で実行されるプログラム制御により、その処理・機能が実現される。

【0068】本発明の第2の実施例においては、加盟店端末2で読み取られたカード番号を受信した、カード会社のセンター1が、利用者の携帯電話機6の電話番号に自動発信し、携帯電話機6から所定桁数のパスワードが入力された際に、電話網4からのPB（プッシュボタン）信号としてパスワードを受信した電話端末インタフェース15は、電話発信・応答制御部14を介して、受信したパスワード（テキストコードに変換される）を、パスワード認証部19に供給する。

【0069】パスワード認証部19は、受信したパスワードを、カード番号に対応してデータベース12に登録されているパスワードと照合し、一致した場合、本人確認が行えたものとして、カード利用可と判定する。

【0070】一方、パスワード認証部19で、パスワードが不一致の場合、所定回数のリトライ入力等のガイダンスを電話発信・応答制御部14を介して携帯電話機6に送信し、パスワードの入力、照合処理が、再び行われる。リトライ入力においてもなお、パスワードが不一致の場合、カード利用不可と判定する。カード利用可否通知部17は、パスワード認証部19の判定結果に基づき、カード利用可／カード利用不可を、加盟店端末2に通知する。

【0071】図6は、本発明の第2の実施例における利用者7（携帯電話機6）、加盟店端末2、及び、センター1の処理フローを説明するための図である。図6において、図4と同一の処理についての説明は省略し、以下では相違点について説明する。

【0072】センター1で携帯電話機6に発信し（ステップS7）、携帯電話機6でオンフックし応答を受け取った場合、センター1は、パスワード入力に関するガイダンス情報を携帯電話機6に送信する（ステップS10）。利用者が携帯電話機6の操作部からパスワード（例えば4桁数字）を入力し、センター1側に送信さ

れ、パスワード認証部19でパスワードを照合し（ステップS14）、認証がOK（可）の場合（ステップS15）、センター1は加盟店端末2に、カード利用可を通知する。

【0073】所定回数のリトライ後もなおパスワード不一致の場合、パスワード認証部19は、パスワード認証NG（不可）と判定し（ステップS15のNO）、カード利用不可通知を加盟店端末2に通知する。

【0074】このように、本発明の第2の実施例においては、利用者7が、携帯電話機6への着信報知を受けて、オフフックした際に、パスワードを入力するように、音声ガイダンスもしくは文字表示で携帯電話機6に通知し、前記通知を認識した利用者は、携帯電話機6から、所定桁数のパスワードを入力し、このパスワードは、センター1側に送信され、センター1では、このパスワードを、データベース12に登録されているパスワードと照合することで、本人確認を行っており、セキュリティを向上している。

【0075】なお、前記各実施例では、加盟店端末としては、既存の端末をそのまま利用することが可能とされ、本発明を実施するにあたり、必要とされる開発コストの増大、加盟店の負担の増大を抑止している。

【0076】本発明は、上記実施例以外にも各種変形が可能である。変形例の一例として、本発明の第3の実施例について説明する。本発明の第3の実施例は、利用者本人の認証を、加盟店端末から入力されるパスワードを用いて行うものであり、本発明の第2の実施例の変形例である。図7は、本発明の第3の実施例を説明するための図である。

【0077】図7を参照すると、利用者7がカード利用時、加盟店端末2のカード読み取り機から取得されたカード情報をセンター1で受け取り、利用者7の携帯電話機6を呼び出すまでは、前記実施例と同様とされる。利用者7が携帯電話機6への着信に応答しカード使用可を入力した場合、第1段階の本人確認が行われ、この時点で、センター1と携帯電話機6との通話接続は切断される。

【0078】つづいて、利用者7が加盟店端末2のキーボード又はテンキー等のパスワード入力部21から、本人のパスワードを入力することで、パスワード情報がセンター1に送信され、データベース12に登録されているパスワードとの照合が行われる。

【0079】次に、本発明の第4の実施例について説明する。本発明の第4の実施例においては、利用者本人の認証を、予めカード作成時等にセンター1に登録した指紋情報を照合することで行うものである。図8は、本発明の第4の実施例を説明するための図である。

【0080】利用者7は、カード利用時に、前記第3の実施例のパスワード入力かわりに、指紋入力装置22に所定の指を置き、指紋入力を行う。指紋入力装置22

から入力された指紋情報（画像情報）から、指紋入力装置 22 内で所定の特徴情報の抽出を行い、抽出された特徴情報がセンター 1 に送信され、センター 1 のデータベース 12 において、カード番号に対応した個人情報として登録されている指紋の特徴情報との照合が行われ、本人確認が行われる。なお、指紋入力装置 22 として画像入力装置を備え、画像入力装置で取得された、指紋の画像情報をセンター 1 に送信し、センター 1 側で、受け取った指紋の画像情報から、指紋照合処理を行う構成としてもよい。

【0081】クレジットカード等を用いた決済金額が高額になる場合、携帯電話機の呼出し、指紋照合等の組み合わせにより、セキュリティ管理を向上させている。

【0082】次に、本発明の第 5 の実施例について説明する。図 9 は、本発明の第 5 の実施例の構成を示す図である。図 9 を参照すると、本発明の第 5 の実施例においては、電子メール機能を具備している携帯電話機または PHS 端末をカード会員が所持している場合、本人確認を、センター 1 側から、カードの使用の可否を問う内容の電子メールを送信し、カード利用者が、このメールを見て返信メールをセンター 1 宛に送信した場合に、カード利用を許可するものである。

【0083】図 9 を参照すると、携帯電話機 6 は、無線基地局 5 を介してサーバ（SMTP（Simple Mail Transfer Protocol）サーバ及び POP サーバ等のメールサーバ、DNS サーバ）51、及びインターネット 9 にアクセスする。なお無線パケットサービスにおいては、無線基地局 5 は、不図示のパケット制御装置、ゲートウェイ、ルータを介して、インターネットに接続される。

【0084】加盟店でカード 8 を利用する利用者 7 がカードを所持する会員本人であることを確認するにあたり、加盟店端末 2 から送信されるカード番号を受信したセンター 1 では、カード番号に基づき、センター 1 のデータベースに予め登録されているカード会員のメールアドレスを検索して、メールアドレス宛に、カード利用可否を問う内容の電子メールを送信する。

【0085】利用者 7 が、電子メール送受信機能を備えた携帯電話機 6 で、メールサーバ（不図示）から受信メールを取り出し、カード使用可の場合には、その旨を返信メールをセンター 1 宛に送信する。センター 1 で、携帯電話機 6 からの返信メールを受け取った場合、カードの利用が許可される。

【0086】一方、カード会員以外の者が当該会員のカードを不正使用する等の場合、携帯電話機 6 で取り出したメールでこの事実を知ったカード会員は、カード使用不可の返信メールをセンター 1 宛に送信する。センター 1 で携帯電話機 6 からのカード使用不可の返信メールを受け取った場合、カードの利用の不許可を加盟店に通知する。また、会員の登録メールアドレス宛への電子メールが送信できない場合、返信メールがセンター宛に返送

されない場合、カード利用不可を、加盟店に通知する。この場合、前述した従来の本人確認手順が行われる。

【0087】図 10 は、本発明の第 5 の実施例のセンターの構成を示す図である。図 10 を参照すると、センター 1 は、図 2 に示した前記実施例の構成と相違して、メールアドレス取得部 23 と、メール送受信部 24 と、インターネット 9 とのインタフェースをなすインターネットプロトコル通信部 25 と、を備えている。

【0088】また、データベース 12 には、送受信機能を備えた移動体通信端末を所持する会員についてそのメールアドレスを記憶保持する。

【0089】メールアドレス取得部 23 は、カード番号に基づき、データベース 12 から、前記カード番号に対応したメールアドレスを検索して取得する。

【0090】メール送受信部 24 は、メールアドレス取得部 23 で取得されたメールアドレスを宛先として、カード使用可否を問い合わせる内容の電子メールを自動送信するとともに、返信メールの受信を管理する。

【0091】カード利用可否判定部 16 は、メール送受信部 24 で送信したメールが正しく宛先に送信され、宛先（利用者の携帯電話機 6）からの返信メールを受け取り、その内容がカード利用可であるか、カード使用不可であるかを判定する。

【0092】カード利用可否通知部 17 は、携帯電話機 6 からカード使用可のメールが返信された場合、カード利用可の旨の通知を、加盟店端末 2 に送信し、一方、前記利用者が携帯電話機 6 からカード使用不可のメールを返信した場合、あるいは、返信メールを所定時間内に受け取ることができない場合、カード利用不可の旨の通知を加盟店端末 2 に送信する。本実施例においても、センター 1 における上記各部は、センター 1 のコンピュータ上で実行されるプログラム制御により、その処理・機能が実現される。

【0093】なお、簡易ブラウザ機能を搭載しサーバ群及びインターネットにアクセス可能な移動体通信端末においては、パスワード入力を行う場合、移動体通信端末側から、センター 1 のウェブサイトにアクセスする（ユーザ ID、パスワード入力）ことで、センター 1 側でこのアクセスを認識し、本人確認を行う構成としてもよい。

【0094】また上記実施例においては、クレジットカードの利用を例に説明したが、本明細書における「カード」は、クレジカード会社で発行・管理されるクレジットカードのみに限定されるものでなく、カード加盟店での商品購入、融資を受けることができる会員カードであれば、任意のカードに適用可能とされる。

【0095】また図面に示したセンターの構成は、その機能構成の一例を示したものであり、本発明は、上記実施例の構成にのみ限定されるものでなく、本発明は、本願特許請求の範囲の各請求項の発明の範囲内で、当業者

であればなし得るであろう各種変形、修正を含むことは勿論である。

【0096】

【発明の効果】以上説明したように、本発明によれば下記記載の効果を奏する。

【0097】本発明の第1の効果は、利用者がカード利用時、センター側に予め登録されている会員の移動体通信端末の電話番号から、利用者の移動体通信端末を呼び出して、カード使用の可否を確認する構成としたことにより、本人確認作業を省力化し、さらに、開発コスト、設備投資の増大を抑止しながら、カードの不正使用を防止することができる、ということである。

【0098】本発明の第2の効果は、移動体通信端末からのカード使用可否の入力、パスワード入力、さらには、個人を特徴付ける指紋情報等の組み合わせを適宜用いることで、所望するセキュリティレベルに応じて不正使用を排除するシステムを構築することができる、ということである。

【図面の簡単な説明】

【図1】本発明の第1の実施例のシステム構成を模式的に示す図である。

【図2】本発明の第1の実施例におけるセンターの構成を示す図である。

【図3】本発明の第1の実施例におけるセンターのデータベースの一例を模式的に示す図である。

【図4】本発明の第1の実施例の処理フローを説明するための図である。

【図5】本発明の第2の実施例のセンターの構成を示す図である。

【図6】本発明の第2の実施例の処理フローを説明するための図である。

【図7】本発明の第3実施例のシステム構成を模式的に

示す図である。

【図8】本発明の第4の実施例のシステム構成を模式的に示す図である。

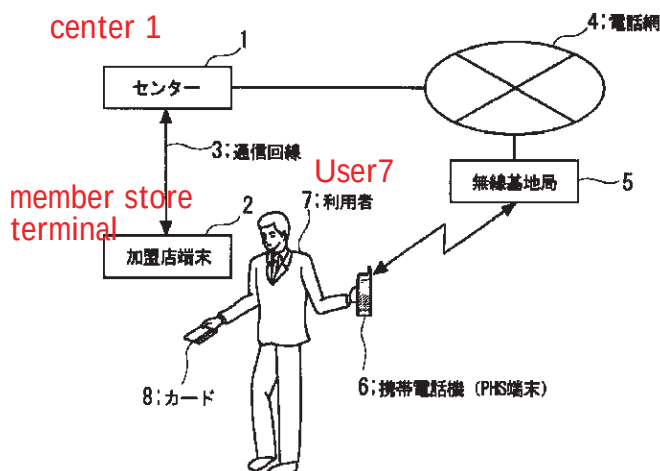
【図9】本発明の第5の実施例のシステム構成を模式的に示す図である。

【図10】本発明の第5の実施例のセンターの構成を示す図である。

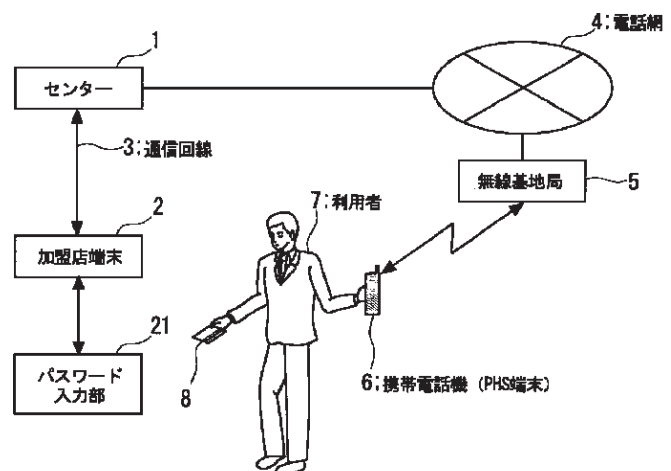
【符号の説明】

- 1 センター
- 2 加盟店端末
- 3 通信回線
- 4 電話網
- 5 無線基地局
- 6 移動体通信端末（携帯電話機、PHS端末）
- 7 利用者（ユーザ）
- 8 カード（クレジットカード）
- 9 インターネット
- 10 カード番号取得部
- 11 本人確認要否判定部
- 12 データベース
- 13 携帯電話番号取得部
- 14 電話発信・応答制御部
- 15 電話端末インタフェース
- 16 カード利用可否判定部
- 17 カード利用可否通知部
- 18 通信回線インタフェース
- 19 パスワード認証部
- 21 パスワード入力部
- 22 指紋入力装置
- 23 メールアドレス取得部
- 24 メール送受信部
- 25 インターネットプロトコル通信部

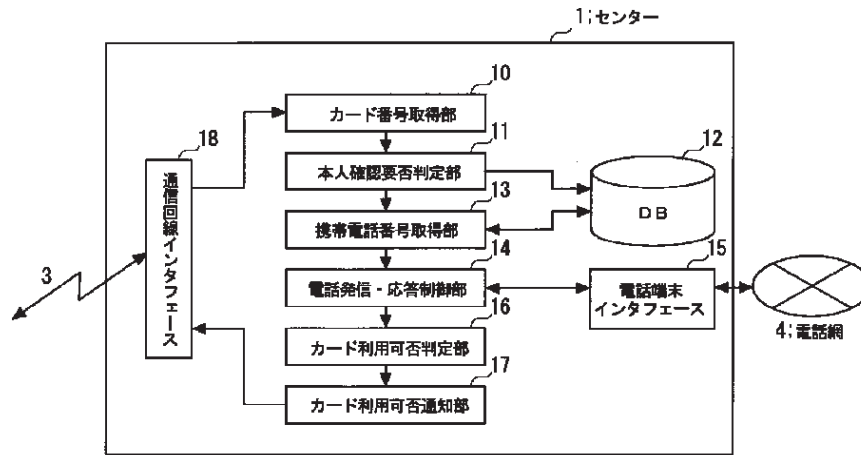
【図1】



【図7】



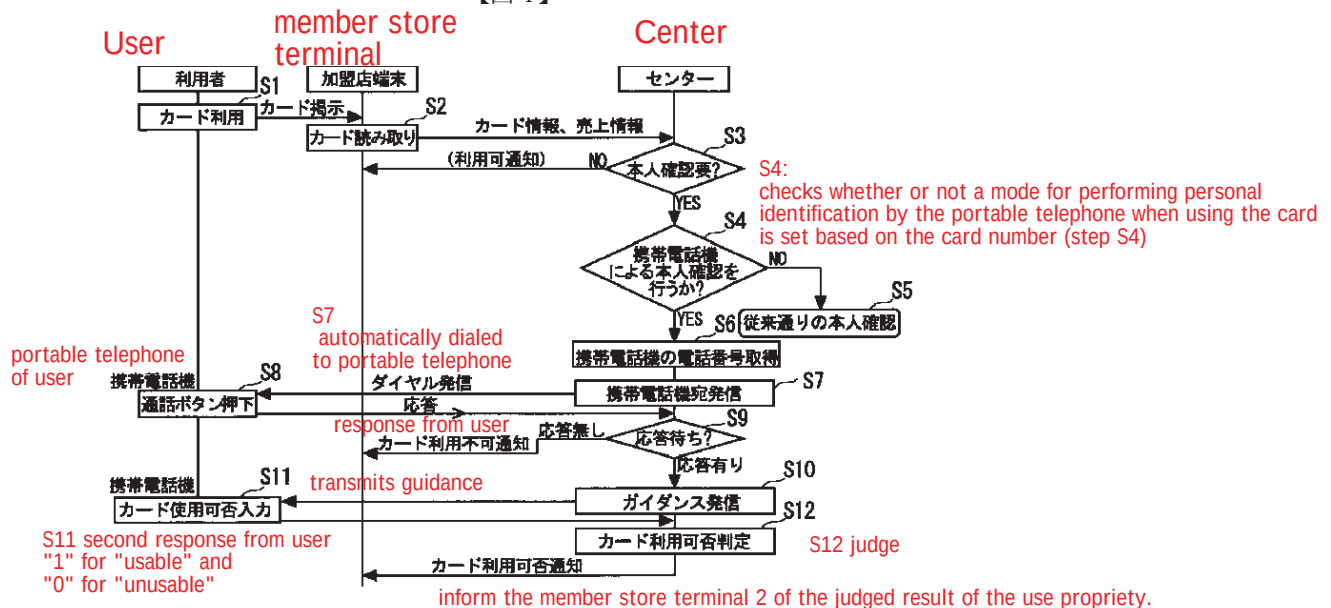
【図2】



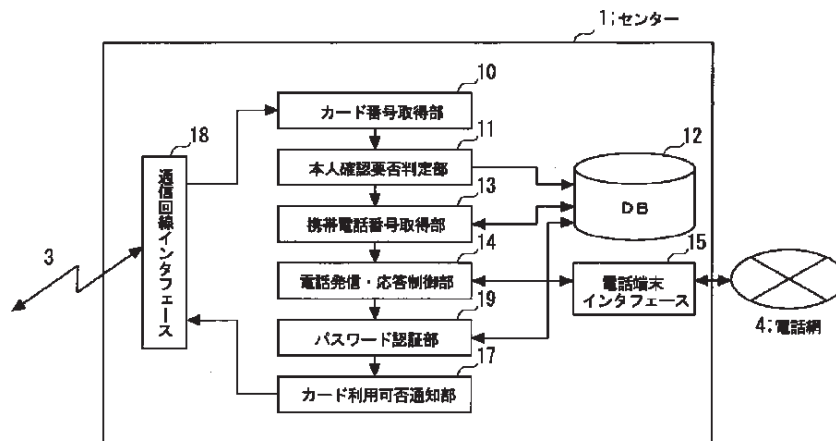
【図3】

カード番号 (ID)	氏名	年齢	性別	住所	勤務先	携帯電話による本人確認の有無	携帯電話番号	パスワード
100XXXXX	特許一郎	35	男	C	A	YES	090-abcc-cddd	KJMN
201YYYYY	日本花子	40	女	D	B	NO		QPRS

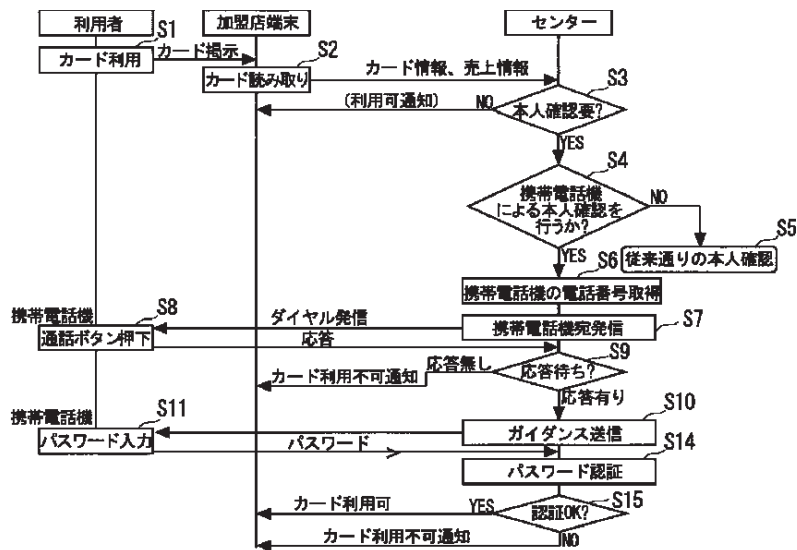
【図4】



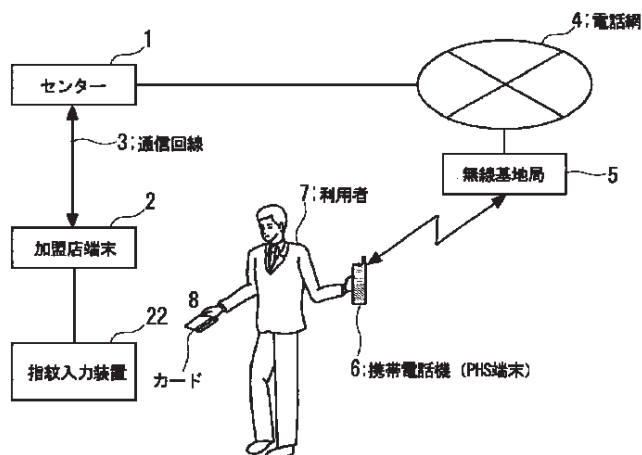
【図5】



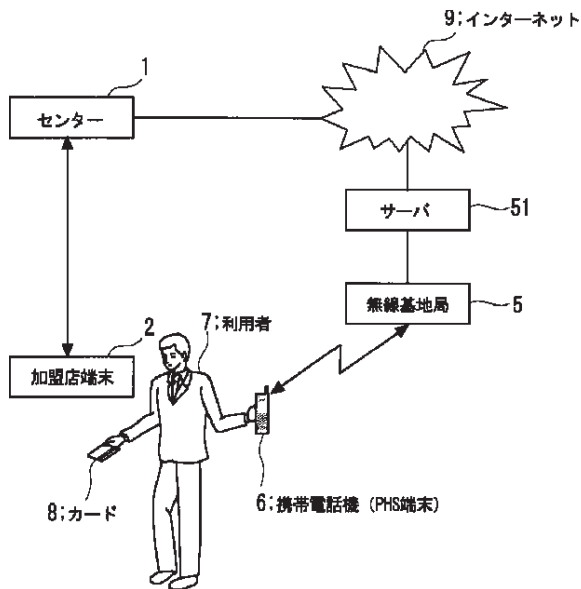
【図6】



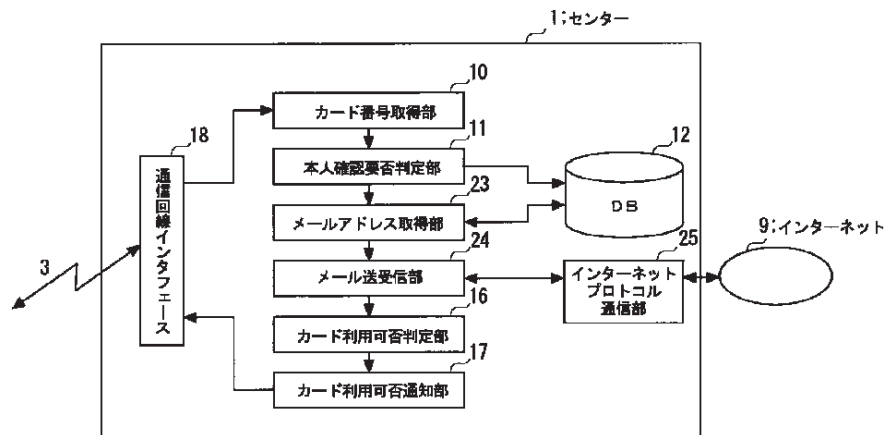
【図8】



【図9】



【図10】



【手続補正書】

【提出日】平成12年12月25日（2000.12.25）

【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

【補正内容】

【特許請求の範囲】

【請求項1】加盟店でカードを利用するカード利用者が前記カードを所持する会員本人であることを確認するにあたり、加盟店端末で読み取られ前記加盟店端末から送信されるカード番号を受信したセンターでは、前記カー

ド番号に基づき、前記センターの記憶手段に予め登録されているカード会員の移動体通信端末の電話番号を検索して前記カード番号に対応する電話番号の移動体通信端末を呼び出し、前記移動体通信端末から、カード使用可の旨が入力された場合に、前記カードの利用を許可すること、ことを特徴とするカードの不正使用防止方法。

【請求項2】前記移動体通信端末が前記呼び出しに 응답しない場合、及び、前記呼び出しに 응답した前記移動体通信端末からカード使用不可の旨が入力された場合に、前記センターでは、本人確認ができないものと判定し、前記カードの利用不可の旨を前記加盟店側に通知すること、ことを特徴とする請求項1記載のカードの不正使用防止

方法。

【請求項 3】加盟店でカードを利用するカード利用者が前記カードを所持する会員本人であることを確認するにあたり、加盟店端末で読み取られ前記加盟店端末から送信されるカード番号を受信したセンターでは、前記カード番号に基づき、前記センターの記憶手段に予め登録されているカード会員の移動体通信端末の電話番号を検索して前記カード番号に対応する電話番号の移動体通信端末を呼び出し、前記移動体通信端末からパスワードが入力された際に、該パスワードを受け取った前記センターでは、前記受け取ったパスワードを、前記センターの記憶手段に予め登録されている、前記カード番号に対応する会員のパスワードと照合し、これらのパスワードが一致した場合に、前記カードの利用を許可する、ことを特徴とするカードの不正使用防止方法。

【請求項 4】前記呼び出した移動体通信端末が応答しない場合、及び、前記呼び出した移動体通信端末から入力されたパスワードが、前記センターの記憶手段に予め登録されている、前記カード番号に対応する会員のパスワードと一致しない場合、本人確認ができないものと判定し、前記カードの利用不可の旨を、前記加盟店側に通知する、ことを特徴とする、請求項 3 記載のカードの不正使用防止方法。

【請求項 5】加盟店端末に通信接続されカードの管理を行うセンター側に、会員のカード番号と対応させて、前記会員の個人情報として、前記会員が所持する移動体通信端末の電話番号を記憶保持するデータベースを設け、利用者が加盟店でカードを利用する時、前記加盟店端末で読み取られたカード番号を受信した前記センターでは、前記カード番号に基づき、前記データベースを検索し、前記カード番号に対応した電話番号を取得する第 1 のステップと、前記取得された電話番号の移動体通信端末宛に前記センターから発信する第 2 のステップと、前記移動体通信端末への前記センターからの着信を受けて、前記利用者が前記移動体通信端末の操作部からカード使用可に対応する情報を入力し、前記センター側で前記移動体通信端末からのカード使用可に対応する情報を受信した場合に、本人であることが確認されたものとし、前記センターから、前記カードの利用が可である旨の通知を、前記加盟店端末に送信する第 3 のステップと、前記呼び出した移動体通信端末が応答しない場合、及び、前記呼び出した移動体通信端末からカード使用不可の情報が入力され、前記センター側でカード使用不可の情報を受信した場合に、前記センターは、前記カードの利用不可の旨の通知を、前記加盟店端末に送信する第 4 のステップと、を含む、ことを特徴とするカードの不正防止方法。

【請求項 6】加盟店端末に通信接続されカードの管理を

行うセンター側に、会員のカード番号と対応させて、前記会員の個人情報として、前記会員が所持する移動体通信端末の電話番号とパスワードとを記憶保持するデータベースを設け、

利用者が加盟店でカードを利用する時、前記加盟店端末で読み取られたカード番号を受信した前記センターでは、前記カード番号に基づき、前記データベースを検索し、前記カード番号に対応した電話番号を取得する第 1 のステップと、

前記取得された電話番号の移動体通信端末宛に前記センターから発信する第 2 のステップと、

前記移動体通信端末への前記センターからの着信を受けて、前記利用者が前記移動体通信端末の操作部からパスワードを入力し、前記センター側で前記移動体通信端末から送信された前記パスワードを受信した場合に、前記受信したパスワードを、前記データベースに予め登録されている、前記カード番号に対応する会員のパスワードと照合し、パスワードが互いに一致した場合に、前記センターは前記カードの利用を許可する第 3 のステップと、

前記呼び出した移動体通信端末が応答しない場合、及び、前記呼び出した移動体通信端末から入力されたパスワードが、前記データベースに予め登録されている前記カード番号に対応する会員のパスワードと一致しない場合、前記センターでは、本人確認ができないものと判定し、前記カードの利用不可の旨を、前記加盟店側に通知する第 4 のステップと、

を含む、ことを特徴とするカードの不正防止方法。

【請求項 7】前記移動体通信端末からのパスワード入力にかえて、前記加盟店端末から、前記利用者がパスワードを入力し、入力されたパスワードが、通信回線を介して、前記センター側に送信され、前記センター側でパスワードの認証が行われる、ことを特徴とする請求項 6 記載のカードの不正防止方法。

【請求項 8】前記加盟店端末側に指紋入力手段を用意しておき、前記利用者の指紋情報が前記指紋入力手段から入力され、該入力された指紋情報が、通信回線を介して、前記センター側に送信され、前記センターでは、前記指紋情報を、前記データベース内に、前記カード番号に対応付けて登録されている指紋情報と照合することで、本人確認を行う、ことを特徴とする請求項 5 記載のカードの不正防止方法。

【請求項 9】加盟店でカードを利用するカード利用者が前記カードを所持する会員本人であることを確認するにあたり、加盟店端末で読み取られ前記加盟店端末から送信されるカード番号を受信したセンターでは、前記カード番号に基づき、前記センターの記憶手段に予め登録されているカード会員のメールアドレスを検索して、カード利用可否を問う電子メールを送信し、前記利用者が前記移動体通信端末からカード利用可の返信メールを受信

した場合、前記カードの利用を許可する、ことを特徴とするカードの不正使用防止方法。

【請求項 10】加盟店端末に通信接続され前記加盟店でのカードの不正使用を防止する装置であって、
会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末の電話番号を記憶保持する記憶手段を備え、
カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記記憶手段を検索し、前記カード番号に対応した電話番号を取得する手段と、
前記取得された電話番号の移動体通信端末宛に自動発信する手段と、
前記移動体通信端末への着信に応答し、前記利用者が前記移動体通信端末の操作部から、カード使用可の情報を入力した場合、前記入力情報を無線通信回線及び電話網を介して受け取り、カード利用可の旨の通知を前記加盟店端末に送信する手段と、
前記移動体通信端末が応答しない場合、及び、前記利用者が前記移動体通信端末からカード使用不可の情報を入力し、前記カード使用不可情報を無線通信回線及び電話網を介して受けとった場合、カード利用不可の旨の通知を前記加盟店端末に送信する手段と、
を備えたことを特徴とするカード不正使用防止制御装置。

【請求項 11】加盟店端末に通信接続され前記加盟店でのカードの不正使用を防止する装置であって、
会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末の電話番号と前記会員のパスワードとを記憶保持する記憶手段を備え、
カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記記憶手段を検索し、前記カード番号に対応した電話番号を取得する手段と、
前記取得された電話番号の移動体通信端末宛に自動発信する手段と、
前記移動体通信端末への着信に応答し、前記利用者が前記移動体通信端末の操作部からパスワードを入力した際、無線通信回線及び電話網を介して送信される前記パスワードを受け取り、前記パスワードを、前記記憶手段に前記カード番号に対応付けて登録されているパスワードと照合し、パスワードが一致した場合、カード利用可の旨の通知を、前記加盟店端末に送信し、一方、パスワードが不一致の場合、カード利用不可の旨の通知を、前記加盟店端末に送信する手段と、
を備えたことを特徴とするカード不正使用防止制御装置。

【請求項 12】加盟店端末に通信接続され前記加盟店でのカードの不正使用を防止する装置であって、

会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末用のメールアドレスを記憶保持する記憶手段を備え、
カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記記憶手段を検索し、前記カード番号に対応したメールアドレスを取得する手段と、
前記取得されたメールアドレス宛に、カード使用可否を問い合わせる電子メールを自動送信する手段と、
前記利用者が、前記センターから送信されたメールを前記移動体通信端末で取り出し、前記移動体通信端末からカード使用可のメールを返信した場合、カード利用可の旨の通知を前記加盟店端末に送信し、一方、前記利用者が前記移動体通信端末からカード使用不可のメールを返信した場合、カード利用不可の旨の通知を前記加盟店端末に送信する手段と、
を備えたことを特徴とするカード不正使用防止制御装置。

【請求項 13】カード読み取り装置を備えた加盟店端末と、前記加盟店端末に通信接続されカードの管理を行うセンターと、を含むカードオーソライゼーションシステムにおけるカード不正使用防止システムであって、
前記センターが、会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末の電話番号を記憶保持するデータベースを備え、
カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応した電話番号を取得する手段と、
前記取得された電話番号の移動体通信端末宛に自動発信する手段と、
前記利用者が、前記移動体通信端末への着信報知を受けてオフフックした際に、カード使用可否について入力するように指示するガイダンス情報を、前記移動体通信端末に送信する手段と、
前記利用者が前記移動体通信端末の操作部からカード使用可の情報を入力した場合、前記カード使用可情報を無線通信回線及び電話網を介して受け取り、前記カードの利用可の旨の通知を、前記加盟店端末に送信する手段と、
前記移動体通信端末が前記センターからの呼び出しに応答しない場合、及び、前記利用者が前記移動体通信端末の操作部からカード使用不可の情報を入力し前記カード使用不可情報を無線通信回線及び電話網を介して受信した場合に、前記カードの利用不可の旨の通知を、前記加盟店端末に送信するように制御する手段と、
を備えたことを特徴とするカード不正使用防止システム。

【請求項 14】カード読み取り装置を備えた加盟店端末と、前記加盟店端末に通信接続されカードの管理を行う

センターと、を含むカードオーソライゼーションシステムにおけるカード不正使用防止システムであって、前記センターが、会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末の電話番号とパスワードとを記憶保持するデータベースを備え、

利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応した電話番号を取得する手段と、

前記取得された電話番号の移動体通信端末宛に自動発信する手段と、

前記利用者が、前記移動体通信端末への着信報知を受けてオフフックした際に、パスワードを入力するように指示するガイダンス情報を、前記移動体通信端末に送信する手段と、

前記利用者が前記移動体通信端末の操作部からパスワードを入力した際、無線通信回線及び電話網を介して送信される前記パスワードを受け取り、前記パスワードから前記データベースを参照して、前記カード番号に対応して登録されているパスワードと照合し、照合の結果、パスワードが一致した場合、前記カードの利用可の旨の通知を、前記加盟店端末に送信する手段と、

前記移動体通信端末が前記センターからの呼び出しに回答しない場合、及び、前記パスワードの照合の結果、パスワードが不一致の場合に、前記カードの利用不可の旨の通知を、前記加盟店端末に送信するように制御する手段と、

を備えたことを特徴とするカード不正使用防止システム。

【請求項 15】カード読み取り装置を備えた加盟店端末と、前記加盟店端末に通信接続されカードの管理を行うセンターと、を含むカードオーソライゼーションシステムにおけるカード不正使用防止システムであって、前記センターが、会員のカード番号と対応させて、前記会員の個人情報として、メール送受信機能を備えた移動体通信端末を所持する会員について前記移動体通信端末用のメールアドレスを記憶保持するデータベースを備え、

カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応したメールアドレスを取得する手段と、

前記取得されたメールアドレス宛に、カード使用可否を問い合わせる電子メールを自動送信する手段と、

前記利用者が、前記センターから送信されたメールを前記移動体通信端末で取り出し、前記移動体通信端末からカード使用可のメールを返信した場合、前記カードの利用可の旨の通知を、前記加盟店端末に送信する手段と、前記移動体通信端末からの応答がない場合、及び、前記

移動体通信端末からカード使用不可のメールが返信された場合、前記カードの利用不可の旨の通知を前記加盟店端末に送信するように制御する手段と、を備えたことを特徴とするカード不正使用防止システム。

【請求項 16】前記データベースに、前記会員毎に、カード利用時に、移動体通信端末の呼出しによる本人確認を行うか否かを記録する領域を備え、移動体通信端末の呼出しによる本人確認を行うか否かの設定が変更自在とされている、ことを特徴とする請求項 13 乃至 15 のいずれかに記載のカード不正使用防止システム。

【請求項 17】前記加盟店端末に接続され、指紋情報を入力する指紋入力装置を備え、

前記利用者の指紋情報が前記指紋入力装置から入力され、該入力された指紋情報が、前記加盟店端末から、通信回線を介して、前記センター側に送信され、前記センターでは、前記指紋情報を、前記データベース内に、前記カード番号に対応付けて登録されている指紋情報と照合することで、本人確認を行う、ことを特徴とする請求項 13 又は 14 記載のカード不正使用防止システム。

【請求項 18】前記加盟店端末がパスワード入力手段を備え、前記移動体通信端末からのパスワードの入力にかえて、前記加盟店端末のパスワード入力手段から、前記利用者がパスワード入力し、入力されたパスワードが、通信回線を介して、前記センター側に送信され、前記センターでは、前記パスワードを受け取り、前記パスワードから前記データベースを参照して、前記カード番号に対応して登録されているパスワードと照合する、ことを特徴とする請求項 14 記載のカード不正使用防止システム。

【請求項 19】カード読み取り装置を備えた加盟店端末に通信接続され、カードの管理を行うセンターにおいて、会員のカード番号と対応させて、前記会員の個人情報として、移動体通信端末の電話番号を記憶保持するデータベースを備え、

(a) カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索し、前記カード番号に対応した電話番号を取得する処理と、

(b) 前記取得された電話番号の移動体通信端末宛に自動発信する処理と、

(c) 前記利用者が、前記移動体通信端末への着信報知を受けてオフフックした際に、カード使用可否について入力するように指示するガイダンス情報を、前記移動体通信端末に送信する処理と、

(d) 前記利用者が前記移動体通信端末の操作部からカード使用可の情報を入力した場合、前記カード使用可情報を無線通信回線及び電話網を介して受け取り、前記カードの利用可の旨の通知を前記加盟店端末に送信し、一

方、前記利用者が前記移動体通信端末の操作部からカード使用不可の情報を入力した際、前記カード使用不可情報を無線通信回線及び電話網を介して受けて、前記カードの利用不可の旨の通知を前記加盟店端末に送信する処理と、
 の前記（a）乃至（d）の各処理を前記センターのコンピュータ上で実行させるためのプログラムを記録した記録媒体。

【請求項 20】カード読み取り装置を備えた加盟店端末に通信接続されカードの管理を行うセンターにおいて、会員のカード番号と対応させて、前記会員の個人情報として、移動体通信端末の電話番号とパスワードとを記憶保持するデータベースを備え、

（a）利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索し、前記カード番号に対応した電話番号を取得する処理と、

（b）前記取得された電話番号の移動体通信端末宛に自動発信する処理と、

（c）前記利用者が、前記移動体通信端末への着信報知を受けてオフフックした際に、パスワードを入力するように指示するガイダンス情報を、前記移動体通信端末に送信する処理と、

（d）前記利用者が前記移動体通信端末の操作部からパスワードを入力した際、無線通信回線及び電話網を介して送信される前記パスワードを受け取り、前記パスワードから前記データベースを参照して、前記カード番号に対応して登録されているパスワードと照合し、照合の結果、一致した場合、前記カードの利用可の旨の通知を、前記加盟店端末に送信し、パスワードが不一致の場合、前記カードの利用不可の旨の通知を、前記加盟店端末に送信する処理と、
 の前記（a）乃至（d）の各処理を前記センターのコンピュータ上で実行させるためのプログラムを記録した記録媒体。

【請求項 21】カード読み取り装置を備えた加盟店端末に通信接続されカードの管理を行うセンターにおいて、会員のカード番号と対応させて、前記会員の個人情報として、メール送受信機能を備えた移動体通信端末を所持する会員についてそのメールアドレスを記憶保持するデータベースを備え、

（a）カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記データベースを検索して、前記カード番号に対応した前記メールアドレスを取得する処理と、

（b）前記メールアドレス宛に、カード使用可否を問い合わせる電子メールを自動送信する処理と、

（c）前記利用者が、前記センターから送信されたメールを前記移動体通信端末で取り出し、前記移動体通信端末からカード使用可のメールを返信した場合、前記カー

ドの利用可の旨の通知を前記加盟店端末に送信し、一方、前記利用者が前記移動体通信端末からカード使用不可のメールを返信した場合、前記カードの利用不可の旨の通知を前記加盟店端末に送信する処理と、
 の前記（a）乃至（c）の各処理を前記センターのコンピュータ上で実行させるためのプログラムを記録した記録媒体。

【請求項 22】請求項 19 乃至 21 のいずれかに記載の記録媒体において、

前記加盟店端末に接続された指紋入力装置から入力された前記利用者の指紋情報が、前記加盟店端末から、通信回線を介して、前記センター側に送信され、前記センターにおいて、前記指紋情報を、前記データベース内に、前記カード番号に対応付けて登録されている指紋情報と照合することで、本人確認を行う処理を前記センターのコンピュータ上で実行させるためのプログラムを記録した記録媒体。

【請求項 23】カードによる決済を利用するカード利用者のカード情報を読み取る装置を備えた加盟店端末から送信される情報を受信したセンターでは、受信した情報のうちカード番号に基づき、前記センターの記憶手段に予め登録されているカード会員の移動体通信端末の電話番号を検索し、前記カード番号に対応する電話番号の移動体通信端末を呼び出す、ことを特徴とするカードの不正使用防止方法。

【請求項 24】カードによる決済を利用するカード利用者のカード情報を読み取る装置を備えた加盟店端末から送信される情報を受信したセンターでは、受信した情報のうちカード番号に基づき、前記センターの記憶手段に予め登録されているカード会員の移動体通信端末のメールアドレスを検索し、該メールアドレスの移動体通信端末宛にカード利用確認用の情報を電子メールで通知する、ことを特徴とするカードの不正使用防止方法。

【請求項 25】加盟店端末に通信接続され前記加盟店でのカードの不正使用を防止する装置であって、
会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末の電話番号を記憶保持する記憶手段を備え、
カード利用者が加盟店でカード利用時、前記加盟店端末から送信される情報のうち、カード番号に基づき、前記記憶手段を検索し、前記カード番号に対応した電話番号を取得する手段と、
前記取得された電話番号の移動体通信端末宛に自動発信する手段と、
を備えたことを特徴とするカード不正使用防止制御装置。

【請求項 26】加盟店端末に通信接続され前記加盟店でのカードの不正使用を防止する装置であって、
会員のカード番号と対応させて、前記会員の個人情報として、前記会員の所持する移動体通信端末用のメールア

ドレスを記憶保持する記憶手段を備え、
カード利用者が加盟店でカード利用時、前記加盟店端末
から送信される情報のうち、カード番号に基づき、前記
記憶手段を検索し、前記カード番号に対応した移動体通
信端末用のメールアドレスを取得する手段と、
前記取得されたメールアドレス宛に、カード利用確認用
の情報を電子メールを自動送信する手段と、
を備えたことを特徴とするカード不正使用防止制御装
置。

【請求項27】カード読み取り装置を備えた加盟店端末
と、前記加盟店端末に通信接続されカードの管理を行う
センターと、を含むカードオーソライゼーションシステ
ムにおけるカード不正使用防止システムであって、
前記センターが、会員のカード番号と対応させて、前記
会員の個人情報として、前記会員の所持する移動体通信
端末の電話番号を記憶保持するデータベースを備え、
カード利用者が加盟店でカード利用時、前記加盟店端末
から送信される情報のうち、カード番号に基づき、前記
データベースを検索して、前記カード番号に対応した電
話番号を取得する手段と、
前記取得された電話番号の移動体通信端末宛に自動発信
する手段と、
を備えたことを特徴とするカード不正使用防止システ
ム。

【請求項28】カード読み取り装置を備えた加盟店端末
と、前記加盟店端末に通信接続されカードの管理を行う
センターと、を含むカードオーソライゼーションシステ
ムにおけるカード不正使用防止システムであって、
前記センターが、会員のカード番号と対応させて、前記
会員の個人情報として、メール送受信機能を備えた移動
体通信端末を所持する会員について前記移動体通信端末
用のメールアドレスを記憶保持するデータベースを備
え、
カード利用者が加盟店でカード利用時、前記加盟店端末
から送信される情報のうち、カード番号に基づき、前記
データベースを検索して、前記カード番号に対応した移

動体通信端末用のメールアドレスを取得する手段と、
前記取得されたメールアドレス宛に、カード利用確認用
の情報を電子メールを自動送信する手段と、
を備えたことを特徴とするカード不正使用防止システ
ム。

【請求項29】カード読み取り装置を備えた加盟店端末
に通信接続され、カードの管理を行うセンターにおい
て、
会員のカード番号と対応させて、前記会員の個人情報と
して、移動体通信端末の電話番号を記憶保持するデータ
ベースを備え、

(a) カード利用者が加盟店でカード利用時、前記加盟
店端末から送信される情報のうち、カード番号に基づ
き、前記データベースを検索し、前記カード番号に対応
した電話番号を取得する処理と、

(b) 前記取得された電話番号の移動体通信端末宛に自
動発信する処理と、
の前記(a)と(b)の処理を前記センターのコンピュ
ータ上で実行させるためのプログラムを記録した記録媒
体。

【請求項30】カード読み取り装置を備えた加盟店端末
に通信接続されカードの管理を行うセンターにおいて、
会員のカード番号と対応させて、前記会員の個人情報と
して、メール送受信機能を備えた移動体通信端末を所持
する会員についてそのメールアドレスを記憶保持するデ
ータベースを備え、

(a) カード利用者が加盟店でカード利用時、前記加盟
店端末から送信される情報のうち、カード番号に基づ
き、前記データベースを検索して、前記カード番号に対
応した移動体通信端末用のメールアドレスを取得する処
理と、

(b) 前記メールアドレス宛に、カード利用確認用の電
子メールを自動送信する処理と、
の前記(a)と(b)の処理を前記センターのコンピュ
ータ上で実行させるためのプログラムを記録した記録媒
体。