

明細書

発明の名称 携帯端末を利用して認証および決済を行う方法およびシステム
技術分野

[0001]

本発明は、携帯端末を利用して認証および決済を行う方法およびシステムに関するものであり、特に、ネットカードに印刷されたIDパターンまたはIDパターンに対応したビットデータを利用してセキュリティの高い個人認証および決済を行うようにした携帯端末を利用して認証および決済を行う方法およびシステムに関するものである。

背景技術

[0002]

現状のクレジットカードによる決済システムでは、基本的には専用回線に接続された専用端末にて決済を行っている。専用回線や専用端末は、与信がないと設置できないし、それらの設置が困難な出店等の場所では利用できない。

クレジットカードや銀行カード等の一般の利用カードを用いてインターネットを介して認証および決済を行う場合、カード番号とパスワードをキー入力して個人認証を行っているため、それらキー入力された番号や記号がフィッシングされたり、販売業者に保存されてしまう場合もある。一旦カード番号やパスワードが盗まれると、キー入力のみで容易に不正使用することを許容してしまうという問題がある。

[0003]

このような問題を回避するために、一般の金融機関では、第2暗証番号と称する乱数表等の認証マトリックス表に示された数字を用いて、第三者にはわからないように秘密の内容を伝達する方法が利用されている。例えば、金融機関とユーザとの間で同一の認証マトリックス表を共有し、ネット上での現金取引を行う際に、ユーザは金融機関から指示された認証マトリックス表上の位置に記載された数字を返信することにより、一致を確認して個人認証を行うものがある。しかし、認証マトリックス表は視覚的に認識できるものであるから、その表が他人に盗まれたりコピーされたりして不正使用される恐れを解消することはできないばかりでなく、本質的にはキー入力をするものであるから、かかる乱数表を用いた認証方法も十分なセキュリティを保つことができない。

[0004]

また、スマートフォンに磁気カードリーダーを取り付け一般の利用カードをスマートフォンで読み取りスマートフォン上の画面にサインをして決済できるシステムもあるが、クレジットカードが不正に利用されたり、偽造されるという点については無防備である。

[0005]

一方、特許文献1に示されるように、符号化された情報を2次的に配置したQRコードをカメラで撮像し、撮像した画像を文字等に復号するようにしたQRコードシステムが

知られている。QRコードは利用カードに使用されているバーコード等に比較して情報量は飛躍的に多くできることを特徴としている。また、人の指の指紋または静脈の血管を画像登録し個人認証をするシステムやセキュリティ・トークンを用いる方法もある。

[0006]

更に、各ユーザに特有のヒューズパターンを導体で印刷したカード電極を有するカードと、このカードの挿入を受け入れ、カード電極のパターンに込められた認証コードを読み取るために、カード電極に対応して対向して配設したセンサー電極を備えたカードリーダーを備え、カードリーダーでヒューズパターンのコードを読み取るようにした技術が特許文献2および3に記載されている。

先行技術文献

特許文献

[0007]

特許文献1 日本特開2009-187198号

特許文献2 日本特許第3092012号

特許文献3 米国特許第6196465号

発明の概要

発明が解決しようとする課題

[0008]

本発明の目的は、カード番号やパスワード等の従来の情報を盗まれたとしても、利用カードの情報を不正利用できないようにすると共に、利便性の良い携帯端末を利用して認証および決済を行う方法およびシステムを提供するものである。

課題を解決するための手段

[0009]

本発明の一形態によれば、ユーザがネット取引において利用カードを使用する際に、利用カードのカード番号やパスワード等の従来の情報に加え、新たにIDパターンを保持したネットカードを発行し、ネットカードのIDパターンをカメラで画像として取り込み、取り込んだ画像からビットデータを読み出し、予めダウンロードされた各ユーザに特有のアプリケーションソフトウェア（以下、アプリという。）を用いて認証IDに変換して認証および決済を実行する。または、IDパターンに替えてIDパターンに表現されたビットデータと同一のビットデータをメモリに記憶させておき、パスワードを入力することによりアプリを起動して認証IDに変換するようにしてもよい。

しかも、販売業者においては、専用回線や専用端末を設置することなく、一般のスマートフォンまたはパソコンに販売業者用のアプリをダウンロードしておき、ユーザのネットカードを利用して認証後の決済を実行できるようにしている。

[00010]

本発明の他の形態によれば、ユーザ側では、個人認証をする毎にIDパターンをカメラで撮像する手間を省くために、取り込んだ画像をビットデータに変換してメモリに保存するかまたはアプリにビットデータと共にダウンロードしてメモリに保存しておき、予め設定したパスワードを入力した時に自動的にメモリに保存されたビットデータを読み出しビットデータからアプリによって認証IDに変換して、個人認証および決済を実行するようにすることもできる。

[0011]

本発明のさらに他の形態によれば、ネットカードには1または複数の必要な利用カードを予め設定登録しておき、商取引時にどのカードで決済するか選択できるようにして、選択したカードを使って販売業者との間で決済することができるようにする。

発明の効果

[0012]

ネットカードは利用カードを使用することもでき、ネットカードに保持されたIDパターンまたはパスワードを入力し、これからビットデータを取り出し認証IDに変換して、この認証IDを通信回線を通して送信して認証を行うようにしているので、入力したIDパターンやパスワードとは異なる認証IDが通信回線に出力される。従って、この認証IDがフィッシングされたとしても、認証IDは携帯端末に入力されるものではないので、悪用されることはない。

[0013]

また、アプリは各ユーザに特有な内容により認証IDに変換する構成になっているので、IDパターン、パスワード、または認証IDが盗まれたとしても、他の携帯端末では利用できない構成となっているので、極めてセキュリティが高いビジネスモデルを構築できる。

[0014]

更に、販売業者においては、専用回線や専用端末を設置することなく、通常のスマートフォンまたはパソコンに業者用アプリをダウンロードすることによりクレジット決済をすることができるので設置スペースを節約することができ、イベント会場の出店においても容易に販売業者用端末を利用してクレジット決済をすることができる。

図面の簡単な説明

[0015]

【図1】 ネットカードシステムの構成の一例を示す図である。

【図2】 IDパターンの構成説明図である。

【図3】 IDパターンの一例を示す図である。

【図4】 IDパターンの利用方法を説明するための図である。

【図5】 ネットカードの発行プロセスを示すフロー図である。

【図6】 アプリのダウンロードの手順を示すフロー図である。

【図7】 IDパターンまたはパスワードを用いて認証を行うユーザ用アプリの動作を示

すフロー図である。

【図 8】 ID パターンまたはパスワードを用いて認証を行うユーザ用アプリの他の動作を示すフロー図である。

【図 9】 ユーザ側アプリと販売業者側アプリとデータベース運用会社側との間の連携動作を示すフロー図である。

発明を実施するための形態

【0016】

本発明の構成の概略を説明すると、従来の利用カードとは別に ID パターンを保有したネットカードを発行する。その ID パターンは金属等の電極で構成され、ネットカード毎に異なるユニークなパターンで形成される。ID パターンは、ユーザ携帯端末に内蔵されたカメラにより画像として取り込まれ、その携帯端末に予めダウンロードされたアプリによって、認証 ID に変換されると共に、変換された認証 ID に基づいて個人認証を行う。また、販売業者側においては、販売業者の端末に業者用アプリを予めダウンロードしておき、ユーザ携帯端末との間でデータベース運用会社の管理プログラムを介して認証および決済がされる。携帯端末は好ましくはスマートフォンまたはパソコンである。特にカメラ内蔵のスマートフォンはカメラと端末が連携されているので本発明と相性が良い。販売業者の端末は、特にイベントでの出店の場合は、携帯端末にするのが好ましい。

以下、図面に基づき本発明を説明する。

【0017】

図 1 は本発明に係るシステム全体の概略を説明するためのシステム構成図である。図 1 に示すように、ネットカード 1 の一部に ID パターン 2 が形成されている。この ID パターンは、図示のようにカードの右側での配置に限らず、任意の箇所に形成することができる。ID パターンはネットカード 1 に印刷または貼付等の適切な方法で保持される。ネットカード 1 は利用カードとは別個に発行されるようにする方がセキュリティの向上のためにはよいが、必ずしも利用カードとネットカードを別体にする必要はなく、両カードを一体にして利便性を図ってもよい。

従来の第 2 暗証番号を付加して個人認証を行う方法では、利用カードは別体の乱数表を表示したカードが発行されているが、本発明では、第 2 暗証番号による認証に替えて、本発明に係る ID パターンによるセキュリティの高い認証を導入することができる。

【0018】

図 1 において、ネットカード 1 はユーザ携帯端末 3 に内蔵のカメラ 4 により ID パターンが撮像される。ユーザ携帯端末 3 はデータベース運用会社のサーバ 5 からダウンロードされたユーザ用アプリによってカメラから取り込まれた ID パターンを処理する。ユーザは自ら所有するユーザ携帯端末からパスワードを入力することもできる。その処理もユーザ用アプリにより行われる。ユーザ携帯端末内での処理の結果としての認証成立となった時、ネットカードの会員番号と、決済のために選択されたクレジットカード番号と、決済

されるべき業者端末番号が、決済情報としてサーバ5に送信されサーバに履歴として蓄積記録される。

[0019]

一方、業者端末6では、商品の売り上げが入力されたPOSレジスタ7から売上金額を取り込み、その売上金額を顧客であるユーザに提示して了解された後、ユーザからネットカードを借用して会員番号を入力する。その結果、会員番号と業者端末番号がサーバ5に決済要求として送信される。サーバ5では、業者端末6から受信した決済要求に含まれる会員番号と業者端末番号をユーザ携帯端末3から予め受信記録されている決済情報と照合して一致すれば、決済用クレジットカード情報を送信し、クレジット会社に決済承認を得る。決済承認されれば決済取引は成立することになる。決済が完了する毎に、決済データはサーバ5のユーザ決済履歴データ部8および業者決済履歴データ部9にそれぞれ決済記録として蓄積される。なお、決済情報には必ずしも業者端末番号を含める必要はなく、この場合は会員番号のみで照合が行われる。

[0020]

図2は、IDパターン2の構成の一例を示す図である。同図において、IDパターンは黒い部分が金属等の電極で構成されている。IDパターンはX軸とY軸でビットアドレス(X, Y)を表すビット構成のパターンであり、左上から4ビットずつ、Y=4の上側に対しX=2、4、6、8、次いでY=8の上側に対しX=2、4、6、8と配列され、更に、Y=4の下側に対しX=1、3、5、7、次いでY=8の下側に対しX=1、3、5、7と配列される。同様にY3からY5まで配列され、最後のY=5の下側に対してはX=1、3、5、7となる。従って、図2のIDパターンは縦8ビットと横8ビットの64ビットからなるビットパターンを構成している。なお、左下のマークMはIDパターンの座標原点を明示した原点マークである。この原点マークMはカメラ撮影の際にIDパターンの位置合わせに用いることができる。なお、IDパターンの構成は図2の形式によらなくても、再現可能なビット配列を構成するものであればQRコード、バーコード等の任意のパターンで構成してもよい。

[0021]

図3は、具体的なIDパターン2の一例を示すものである。図3から理解できるように、図2中のY行の8本の横のラインはそのまま残り、Y行の上側と下側のフューズマークが有るところは「1」で、無いところは「0」である。図3を図2のビット位置に対応させると、Y=4のラインの上側は(0000)であり、また、Y=8のラインの上側は(1110)であることが理解できる。このようにしてX方向に8ビット、Y方向に8ビットの総数64ビットからなるIDパターンを構成することができる。図3には原点マークが無いが、上下に4ビットずつ有するY軸の8本の横ラインは常に存在しているので、この8本の横ラインを基準として位置合わせをしてパターン照合を実行することができる。

[0022]

本発明の一実施例では、図3に示すようなIDパターンをカメラで撮影して得たアナログ画像を認証IDに変換し、その認証IDに基づき認証を行っている。図4はIDパターンと認証IDの関連を説明するための図である。

[0023]

図4は図2と同様のIDパターンであって、8本の横ラインと各横ラインの上と下にそれぞれ4ビットずつ配置された構成になっている。図4の横方向に配列された8ビットには左から右に順番にA B C . . . Hの符号が与えられ、また、縦方向に配列された8ビットには上から下へ順番に1 2 3 . . . 8の番号が与えられる。従って、符号と番号により64ビットからなるビットパターンのアドレスを指定することができる。即ち、図4に示すように、A1は最も左上のビットを指し、H5は右端で上から5番目のビットを指す。C7、E3 . . . も同様にビットパターン中の特定のビットのアドレスを指定することができる。

[0024]

認証IDは例えば4桁の数字で表わされる。各桁の4つの数字はそれぞれ4ビットの符号で表わされる。従って、例えば、数字「5」は(0101)であるから、図3に示すIDパターンでは(A1、A4、D1、E4)のようにIDマップアドレスを指定することにより1つの数字を特定することができる。同様にして4桁の数字に変換されて認証IDを得ることができる。

[0025]

従って、本発明においては、IDパターンは各ユーザにアトランダムなビットを構成するパターン形式で付与され、このアトランダムなビット構成のIDパターンからIDマップアドレスで認証IDを抽出するようにしている。

[0026]

図5はデータベース運用会社におけるネットカード発行プロセスを示すフロー図である。このフロー図を図1を参照して説明する。

[0027]

会員加入の申し込みがあったとき、まず、ステップ11で会員番号を発行してサーバ5に登録し、ステップ12でユーザ用アプリIDを発行しサーバ5に登録する。

[0028]

ステップ13では、ユーザを認証するための認証IDをサーバ5に登録する。

次いで、ステップ14で、IDパターンと、そのIDパターンをマップ化して記録したIDビットデータと、ビットデータから認証IDを抽出するためのIDマップアドレスとを生成しサーバ5に登録する。なお、IDビットデータは、IDマップアドレスでビット位置を指定することができるものであれば、マップ形式ではなくてもビットデータ列形式でもよい。

[0029]

ステップ15では、ネットクレジット番号を発行しサーバに登録する。ステップ16では、ネットカードと既存の利用カードのいずれかを選択的に使用したいときに、1つまたは複数の既存の使用カードのカード番号と暗証番号を含むクレジットカード情報をサーバ5に登録する。ステップ17では、ユーザ携帯端末に付与されている個体識別番号がユーザ携帯端末を特定するためのユーザ端末番号としてサーバ5に登録すると共に、個人認証のためのパスワードを同様にサーバに登録する。最後に、ステップ18で、会員番号、IDパターン、IDビットデータ、ネットクレジット番号、既存利用カード番号等を印刷したネットカードを新規に会員に発行する。上記の登録情報は相互に関連付けてサーバのデータベースに登録される。

[0030]

ユーザ用アプリとは、ユーザ携帯端末にダウンロードされユーザが携帯端末を利用して認証および決済をするためのソフトウェアであって、アプリIDとIDビットデータとIDマップアドレスが含まれている。このアプリはアプリIDにより特定されて読み出される。ユーザ用アプリIDはそのユーザ用アプリを特定するための符号である。ユーザ用アプリは、会員番号とユーザ用アプリIDと認証IDとIDパターンとIDビットデータとIDマップアドレスと共にユーザ毎にサーバ5のアプリ作成データ部10で管理されている。

[0031]

新規発行のネットカードにはIDパターンと会員番号とクレジット番号が掲載されているが、認証IDとIDマップアドレスとアプリIDおよびクレジットカードの暗証番号等の情報は一切保持されていない。なお、会員番号はバーコード形式等により掲載されてもよい。

[0032]

なお、他の既存の利用カードを追加登録することを希望する場合は、ユーザ携帯端末を利用して、先ずデータベース運用会社に既存利用カードの追加登録の申請をする。運用会社のサーバから追加登録のフォームが返送されるので、ユーザは、このフォームにユーザの会員番号と端末番号とパスワードと追加登録をしようとする利用カードのカード番号と暗証番号を含むクレジットカード情報を記入し返信することにより追加登録をすることができる。

なお、ユーザ番号は会員番号またはユーザ端末番号を指す。

[0033]

販売業者は、店舗を構えて商取引をするばかりでなく、何らかのイベント会場に出店して携帯端末を用いた商取引を望む場合がある。このような場合、出店業者は携帯容易なスマートフォンまたはパソコンを用いてユーザとの商取引を行うことができるようにすることが好ましい。この点に鑑み、販売業者がきわめて簡単な手続きで業者会員となる業者カードを発行できるようにしている。

【0034】

販売業者はデータベース運用会社に業者会員の申し込みをすると、業者会員番号と業者端末の個体識別番号に対応する業者端末番号がサーバ5に登録されると共に、その他の書誌的事項の登録をする。これにより販売業者は商取引を開始できるが、通常は業者会員番号つを掲載した業者カードが発行される。なお、業者番号は業者会員番号または業者端末番号を指すものとする。

【0035】

ネットカードを所持するユーザはネットカードを利用して商取引を行うには、予め自ら所有するスマートフォンまたはパソコンを用いてネットカード発行会社からユーザ用アプリをダウンロードする必要がある。

【0036】

図6はアプリのダウンロードの手順を示すフロー図である。

図6において、ステップ21で、ネットカードのユーザは自ら所有するユーザ携帯端末でネットカードに係るアプリのダウンロードの操作を開始する。まず、ステップ22でネットカードのデータベース運用会社のアプリサイトにアクセスし、ステップ23で運用会社から送信されたアプリリストからユーザ用アプリを選択する。その結果、ステップ24でダウンロードウェブページが返送され表示される。そのウェブページに会員番号および／またはユーザ携帯端末の端末番号を入力し送信する。

【0037】

データベース運用会社側のサーバ5は、ステップ25において、ユーザから送信された会員番号および／またはユーザ端末番号を受信し、データベースから会員番号に対応する当該会員専用のアプリIDを選択し、ステップ26で個人認証を行う。認証が成立すれば、ステップ27で会員番号に対応するユーザ用アプリをユーザ端末番号を用いて当該ユーザ携帯端末にダウンロードする。このユーザ用アプリには、アプリIDと、IDマップアドレスと、認証IDに変換するプログラムと、販売業者との間で決済取引をするためのプログラムを含んでいる。なお、ユーザ用アプリはIDビットデータと認証IDを含んでもよい。IDビットデータを含む場合はIDパターンを用いることなくパスワードで認証を行う場合であり、また、認証IDを含む場合はサーバに認証依頼をすることなくユーザ携帯端末自身で認証を行うようにする。

【0038】

ユーザはステップ28で、ダウンロードされたアプリをユーザ携帯端末に登録し、ステップ29でアプリのアイコンを作成表示し、ステップ30にてアプリのダウンロードを終了する。サーバ5はユーザ用アプリのダウンロードは1回限り実行するのみで、2回目以降は特別の手続をしなければ実行できないようにしてある。

【0039】

ステップ26で認証が不成立と判断されたときは、ステップ31で会員番号が不整合で

あるためアプリのダウンロードができない旨をユーザ携帯端末に知らせる。ユーザはステップ24の操作を再び繰り返すことができる。

[0040]

以上では、ユーザがユーザ用アプリをダウンロードする場合を説明したが、販売業者の場合は、図6に示すと同様な手順で業者用アプリをダウンロードすることができる。図6と異なるところは、ステップ24がダウンロードウェブページに業者会員番号または／および業者端末番号を入力して送信する点であり、それ以外は図6のフローに基づき業者用アプリのダウンロードが実行される。なお、業者用アプリは、ユーザとの決済商取引に使用するソフトウェアである。

[0041]

次にIDパターンがアプリを用いて認証される方法を説明する。携帯端末は通常カメラ機能を備えているので、このカメラを使ってネットカードに表示されたIDパターンを撮影することができる。図7は、IDパターンをカメラで撮像し、登録されたアプリを使って、撮像されたIDパターンに基づいて認証IDに変換し認証する手順と、IDパターンのカメラ撮影に替えてパスワードを入力して認証IDに変換し認証する手順と、を示すフロー図である。

[0042]

先ず、IDパターンにて認証する方法を図7に基づき説明する。スマートフォンは通常カメラ機能を備えているので、このカメラを使って会員カードに表示されたIDパターンを撮影することができる。

[0043]

図7において、ステップ40からIDパターンによる認証に入り、ステップ41でスマートフォンの認証用アプリのアイコンマークをタッチすると、ステップ42でウェブページ画面が表示されるので、スマートフォンに備え付けのカメラを起動する。ウェブページにはステップ43に示すようにIDパターンを納める枠が表示される。ステップ44で、その枠内にIDパターンが納まるようにカメラ位置を調節して撮影する。撮影されたIDパターンはステップ45で自動的にアナログ形式でメモリに取り込まれる。ステップ46は、取りこまれたアナログ形式のIDパターンが正常に取りこまれたかどうかを認証処理する。この認証処理はカメラで取り込まれたIDパターンが枠内に収まり且つ適切な大きさと解像度を有するものであるかどうかをチェックするものである。ステップ47でこの撮影処理が正常ではないと判断されれば、ステップ43に戻され、再びIDパターンのカメラ撮影を行う。

[0044]

ステップ47で正常と判断されれば、ステップ48でアナログ形式のIDパターンから64ビットのデータを取りこみ、マップ形式の64ビットのIDビットデータに変換し、ステップ49でIDビットデータをメモリに記録する。記録されたIDビットデータは、

ユーザ用アプリをダウンロードした際にそのアプリにIDパターンに対応するIDビットデータが含まれるようにすることもできるので、読み込んだIDビットデータをダウンロードされたものと比較することができる。

IDパターンがIDビットデータとして記録された後、直ちにステップ50でIDパターンの映像は消去され、写真として保存されないようにしてセキュリティの向上を図っている。

[0045]

ステップ51では、ステップ49で記録されたメモリ中のIDビットデータと予めダウンロードされているIDマップアドレスを読み出し、ステップ52ではIDマップアドレスに基づいてIDビットデータを参照して16ビットのデータを抽出し、4桁の数字からなる認証IDに変換する。ステップ54では変換して得られた認証IDと予めアプリと共に取り込まれている認証IDとを照合して認証する。認証結果はステップ55で判定される。なお、ここでは4桁の数字からなる認証IDを例にとりましたがこれに限らず例えば10桁の数字や記号からなる認証IDであってもよい。

[0046]

ここで認証が成立すれば、ステップ56ではデータベース運用会社のサーバ5に認証が成立したことを会員番号と共に知らせる。ネットカードによる認証が成立した後でなければ、当該クレジットカードによる商取引ができないように設定されている。その結果、サーバでは通常のクレジットカードによる商取引が可能なスタンバイの状態になる。店頭での取引やネットバンキングまたはネットショップでの取引のときには、ネットカードの会員番号を入力してサーバに認証済であることを確認した後に、使用カードによる商取引を開始することができる。

[0047]

ステップ55で認証不可の判断がされれば、ステップ43に戻り、再びIDパターンの撮影から操作を開始することができる。

[0048]

IDパターンをカメラ撮影するのに替えて、パスワードを用いて認証を行うこともできる。以下、パスワードでの認証を説明する。

図7において、ステップ73からパスワードによる認証に入り、ステップ74でパスワードを入力する。そして、ステップ51に進み、アプリはパスワード入力に応答してIDビットデータとIDマップアドレスを読み出す。以下、ステップ52からステップ56までは前述と同じ動作をする。

[0049]

なお、ステップ51において、IDビットデータはステップ49でメモリに記録されたIDビットデータを読み出すようにして、予め一旦はIDパターンによる認証をした後でなければ、パスワードによる認証はできないようにすることもできる。こうすることによ

って、画像で構成された符号化可能なIDパターンを利用して取りだされたIDマップアドレスをメモリに登録し、以降はパスワードにより認証を可能にして、セキュリティの向上とユーザの利便性を満たすようにしてもよい。

[0050]

また、パスワードによる認証の場合、IDビットデータがユーザ用アプリに含まれてダウンロードされるようにすれば、IDパターンによる認証を全くすることなくパスワードによる認証をすることができるので、ユーザは当初からパスワードによる認証を選択することができる。

[0051]

図7に示す実施例では、ユーザ携帯端末内で認証を実行する例を説明したが、図8ではサーバ5で認証を行う例を説明する。図8において図7と同一符号は同一の機能を実行するステップである。

[0052]

図8において、IDパターンをカメラで撮像して認証を行う動作はステップ40から導入される。以下、ステップ41からステップ50までは図7と同じ動作をする。

[0053]

ステップ51では、予めダウンロードされているIDマップアドレスに基づいて、ステップ49で記録されたIDビットデータまたはアプリと共にダウンロードされたIDビットデータを参照して16ビットデータを抽出し、ステップ52で4桁の数字からなる認証IDに変換する。この変換は図4に基づき説明した方法で実行される。ステップ53では、変換された認証IDと会員番号をデータベース運用会社のサーバに送信する。

[0054]

サーバでは、携帯端末から送信された認証IDと会員番号をステップ61で受信し、ステップ62でそれら受信情報をサーバのデータベースに記録された情報と照合し認証動作をする。次いで、ステップ63で認証結果をユーザの携帯端末へ送信する。

[0055]

携帯端末において、ステップ65で認証結果を受信し、ステップ66で認証が成立しているかどうかを調べる。認証不成立であればステップ67でその旨が表示され、ステップ41から再試行をすることになる。ステップ66で認証結果が成立していると判断されれば、ステップ68で、携帯端末に入力フォーム画面が表示される。ユーザは販売業者から業者会員番号を聞き取り、それを携帯端末の入力フォームに入力する。ステップ68はユーザが特定の販売業者にクレジット決済を許可するという意味において意義があるが、このステップ68は実際には取引の利便性から省略した方がよい場合が多い。

[0056]

次に、ステップ69で、ユーザはクレジットカードの選択画面を表示し、決済に使おうとするクレジットカードを選択する。そして、ステップ70で、決済のために選択された

決済クレジットカード情報と業者会員番号とユーザ会員番号をサーバに送信する。なお、業者会員番号に替えて業者端末番号を入力してもよいが、業者番号の入力を省略することもできる。

[0057]

一方、サーバはステップ72でそれら情報を受信しデータベースに保存する。その結果、サーバは当該業者会員番号を所持する販売業者から会員番号と業者端末番号が入力されるのを待機するスタンバイ状態となる。これにより、ユーザと販売業者との間で安全な取引を達成することができる。

[0058]

以上はIDパターンを撮像しそのパターンからIDビットデータに変換するようにした認証方法を説明したが、実際には買物をする毎にカメラ撮影をするのは手数が掛かり不便でもある。そこで、一度カメラ撮影をしてIDビットデータに変換したならば、そのIDビットデータを当該ユーザ携帯端末のメモリに記憶しておき、それ以降はIDパターンをカメラ撮影することなく、パスワードを入力するのみで自動的にIDビットデータを読み出しできるようにするのが便利である。また、IDビットデータはアプリと共にダウンロードされメモリに記録しておくこともできる。このIDビットデータはそのユーザの携帯端末特有のものであり通信回線を通して送信することもないので、他人により悪用される可能性は極めて少ない。

[0059]

ステップ73は、このパスワードで入力して認証する場合の入口である。先ず、ステップ74でパスワードを入力すると、ユーザ用アプリの動作で自動的にIDビットデータとIDマップアドレスが読み出され前述のステップ51へ進む。以下は前述したとおりの過程を経て認証がなされる。この場合、パスワードは、ユーザ用アプリをダウンロードしたユーザ携帯端末でのみ有効に用いることができるものであり、他の端末では、同一のアプリを保持することができないので、当該パスワードは無効であるから、他人に悪用される恐れはない。

[0060]

なお、さらに他の認証方法として、図7には図示されていないが、例えば、IDビットデータがアプリと共にダウンロードされておらず、かつ、カメラが不調な場合に、カメラ入力に替えてネットカードに記載されたIDビットデータをユーザ携帯端末に入力してメモリに記憶させる方法がある。その手順は、パスワードを入力すると共に、ネットカードに表記されたIDビットデータを入力してステップ49に進むようにすればよい。この場合、ステップ50はスキップされる。

[0061]

以上はユーザ携帯端末とデータベース運用会社のサーバとの間の動作を説明したものであるが、これに引き続き操作されるユーザ側と販売業者側とサーバ側の三者の間の情報の

流れを図9に基づいて説明する。

[0062]

ユーザは、販売業者提供の購入商品とその価格に合意したことに基づき、ユーザからネットカードを借用した販売業者又はユーザ自身がユーザ会員番号をステップ75で入力する。会員番号の入力はキー入力でもカードリーダーによる入力でもよい。なお、ネットショップやネットバンキングの場合は、ユーザが取引を申し込むと、入力用フォームが返送されてくるから、これに会員番号その他の必要事項を入力して送信するという手続をすることになる。

[0063]

次いで、ステップ76でユーザ会員番号と業者会員番号をサーバへ送信する。サーバはユーザ携帯端末と業者端末からそれぞれ受信したユーザ会員番号と業者会員番号をステップ77で照合する。なお、ステップ68が省略されている場合は業者会員番号の照合は省略される。その照合の結果、照合不成立であれば販売業者側に不成立の通知を送信し、販売業者はステップ79でそれを受信しクレジット決済はできないことを確認する。

[0064]

一方、ステップ78で、照合が一致すれば、ステップ80で決済クレジットカード情報を販売業者に送信する。販売業者側はステップ81で決済クレジットカード情報を受信し、ステップ82でPOSレジスタから請求金額を取り込み、ステップ83でクレジットカード番号と請求金額をクレジット会社へ送信し決済承認を依頼する。

[0065]

決済承認依頼の結果がステップ84でチェックされ、NOと判断されれば、その旨がサーバに送信される。サーバではステップ91で決済不可通知を受信し、ステップ92で決済不可の処理をしてユーザ携帯端末にその旨を知らせる。そして、ユーザ携帯端末はステップ93で決済不可通知を受信する。その結果、ユーザは現金取引にするか、または他のクレジットカードを利用するべく再試行をすることができる。なお、決済不可の情報はユーザ決済履歴データ部および業者決済履歴データ部に記録されるようにしてもよい。

[0066]

ステップ84で、決済承認が得られれば、ステップ85でクレジット会社へ決済請求をすると共にクレジット売上表をプリントアウトし、ステップ86でクレジット処理情報をサーバへ送信する。

[0067]

サーバでは、ステップ87で、クレジット処理情報を受信し、クレジット決済済みの処理を行い、その旨をユーザ携帯端末に送信する。

[0068]

ユーザ携帯端末では、ステップ88でクレジット決済済みの通知を受信し、その旨を表示する。これによりユーザは無事に決済が終了したことを確認することができる。

[0069]

サーバでは、ステップ87でクレジット決済が完了した後、ステップ89で、ユーザ決済履歴データ部8と業者決済履歴データ部9にクレジット決済情報のデータを蓄積記録する。

[0070]

ユーザまたは販売業者は、それぞれ自らの端末を使ってデータベース運用会社のサーバにアクセスして、所定の手続きの下にユーザ決済履歴データ部8または販売業者決済履歴データ部9の履歴情報を読み取り、過去の取引の確認を行うことができる。

[0071]

以上に説明したように本発明によれば、ユーザの所持するネットカードとユーザ携帯端末は一对になって機能するようになっているので、ネットカードを紛失・盗難にあったとしても他の端末では利用できない構成になっており、ネットカードとユーザ携帯端末が一緒に盗まれない限りは不正利用を防止でき、高いセキュリティを維持することができる。

[0072]

また、ユーザ携帯端末にダウンロードされたユーザ用アプリは、1つのネットカードに対応したユーザ用アプリIDが付与されているので、対応するネットカードにしか利用することができない。しかも、ユーザ用アプリは携帯端末固有の端末番号を有するユーザ携帯端末にのみダウンロードすることができ、他の携帯端末にはダウンロードされることはない。従って、ユーザ用アプリの不正なダウンロードはできなくなっており、高いセキュリティが維持されている。しかも、IDビットデータから認証IDに変換はアプリがない限りはできない。

[0073]

更に、ユーザ携帯端末に入力されるパスワードとIDビットデータから変換された認証IDは異なるデータであるので、それらがユーザ携帯端末またはサーバから流出したとしても不正使用されることはない。

[0074]

しかも、アトランダムに設定されたIDパターンと、認証IDと、IDパターンを認証IDに変換するためのIDマップアドレスは、ネットカード発行時に作成され、3者一体として当該ユーザ携帯端末でのみ使用できるように設定されたものであるので、これらそれぞれは他の携帯端末や他のアプリには使用できないものとなっている。従って、高度のセキュリティを維持することができる。

[0075]

また、ユーザ携帯端末への入力、IDパターンまたはパスワードであって、クレジット番号を入力することはなく、また、販売業者はサーバから送信されたクレジット番号のみを使用でき、販売業者がクレジット番号を入力されることはないので、クレジット番号がフィッシングされる恐れは極めて少ない。

[0076]

また、インターネット取引において、本発明に基づくセキュリティチェックが実行された後においてのみ、現在普通に行われているインターネット取引を行うことができる構成を取ることができるので、本発明に係るセキュリティチェックにおいて認証が得られない限り、通常のインターネット取引を開始することができない構成とすることができる。その結果、本発明に係る第1のセキュリティの関門の存在を第3者に知られることなく通常のインターネット取引を行うことができるので、その取引過程でフィッシングやスキミングで他人に認証IDやパスワードを盗まれたとしても、他人は第1のセキュリティ関門をくぐることはできないため不正なインターネット取引を行うことができない。

[0077]

以上の説明では、店舗での商取引の場合について説明したが、これに限らず、例えばネットワーク取引において業者端末はインターネットに接続された端末であってもよい。なお、本発明では本発明の精神を逸脱することなく種々の改変をすることができる。

[0078]

以上の説明では、ユーザが店頭で商取引をする場合を例に挙げて説明したが、ネットワークやネットバンキングにおいても本発明を利用することができる。

符号の説明

[0079]

- | | |
|----|---------------|
| 1 | ネットカード |
| 2 | IDパターン |
| 3 | ユーザ携帯端末 |
| 4 | カメラ |
| 5 | サーバ |
| 6 | 業者端末 |
| 8 | ユーザ決済履歴データベース |
| 9 | 業者決済履歴データベース |
| 10 | アプリ作成管理データベース |

請求の範囲

【請求項1】 運用会社のサーバ（5）からダウンロードされた、認証および決済を行うプログラムと少なくともIDマップアドレスとユーザ番号を含むアプリ、

ID情報を入力する第1の入力装置（40-50, 73, 74）、

前記アプリによって前記ID情報を認証IDに変換する変換装置（51, 52）

前記アプリに基づいて前記認証IDに基づき認証する認証装置（52, 53, 61-63, 65, 66）、

ネットカードに掲載された前記ユーザ番号とクレジット情報を前記サーバに送信する第1の送信装置（70）、

前記ユーザ番号を入力する第2の入力装置（75）、

前記ユーザ番号と運用会社に登録された業者番号を前記サーバに送信する第2の送信装置（76）、

前記第1と第2の送信装置から受信した前記ユーザ番号を照合し一致したとき、前記クレジット情報を業者端末に送信する第3の送信装置（77, 78, 80）、および

前記クレジット情報に基づきユーザに請求する金額を決済処理する決済装置、
を有し、

前記第1の入力装置、変換装置、認証装置および第1の送信装置を有するユーザ携帯端末（3）、

前記第3の送信装置を有する前記サーバ（5）、および

前記第2の入力装置、第2の送信装置および決済装置を有する前記業者端末（6）、
を備えた携帯端末を利用して認証および決済を行うシステム。

【請求項2】 請求項1に記載のシステムにおいて、

前記第1の入力装置は、前記運用会社からユーザに発行されたネットカードに印刷されたIDパターンを撮影する前記ユーザ携帯端末に備え付けのカメラである前記システム。

【請求項3】 請求項1に記載のシステムにおいて、

前記第1の入力装置は、所定のパスワードを入力するための前記ユーザ携帯端末の符号入力装置（74）である前記システム。

【請求項4】 請求項2に記載のシステムにおいて、

前記第1の入力装置は、更に、所定のパスワードを入力するための前記ユーザ携帯端末の符号入力装置を備え、前記カメラと前記符号入力装置の一方を選択できるようにした前記システム。

【請求項5】 請求項1に記載のシステムにおいて、

前記変換装置は、前記アプリによって、前記ID情報の入力に応答してIDビットデータとIDマップアドレスを読み出し、前記IDマップアドレスに基づいて前記IDビットデータを参照して前記認証IDに変換する前記システム。

【請求項 6】 請求項 1 に記載のシステムにおいて、

前記ダウンロードされたアプリには予めサーバに登録された当該ユーザの認証 ID が含まれており、

前記認証装置は、前記変換装置で変換された認証 ID を前記アプリに含まれた認証 ID と照合して認証を実行する前記システム。

【請求項 7】 請求項 1 に記載のシステムにおいて、

前記認証装置は、前記変換装置で変換された認証 ID と前記ユーザ番号を前記サーバに送信し、該サーバにおいて受信した認証 ID とユーザ番号を該サーバに登録されている認証 ID とユーザ番号と照合して一致したとき認証成立をユーザ携帯端末が返信するようにした前記システム。

【請求項 8】 請求項 1 に記載のシステムにおいて、

前記第 3 の送信装置におけるクレジット情報は、予め設定され前記ネットカードに掲載された複数のクレジット情報の内からユーザによって選択された 1 つのクレジット情報である。

【請求項 9】 請求項 1 に記載のシステムにおいて、

前記決済装置は、決済処理が完了したときその旨をサーバに送信する決済完了通知装置 (86) を有し、

前記サーバは、更に、前記決済完了通知装置からの決済完了通知を受信し、決済情報として蓄積記録する決済履歴データ部 (8、9) を有する前記システム。

【請求項 10】 請求項 9 に記載のシステムにおいて、

前記決済履歴データ部は、前記決済情報をユーザ決済履歴データ部 (8) と業者決済履歴データ部 (9) にそれぞれ記録する記録装置 (89) を有する前記システム。

【請求項 11】 請求項 10 に記載のシステムにおいて、

前記ユーザ携帯端末は前記ユーザ決済履歴データ部にアクセスして決済履歴を閲覧できるようにした前記システム。

【請求項 12】 請求項 10 に記載のシステムにおいて、

前記業者端末は前記業者決済履歴データ部にアクセスして決済履歴を閲覧できるようにした前記システム。

【請求項 13】 請求項 9 に記載のシステムにおいて、

前記サーバは前記業者端末から前記決済完了通知を受け取ったとき前記ユーザ携帯端末にその旨を通知する通知装置 (87) を有し、前記ユーザ携帯端末は前記決済完了通知を受信したときその旨を該ユーザ携帯端末に表示する決済表示装置 (88) を有する前記システム。

【請求項 14】 請求項 1 に記載のシステムにおいて、

前記ユーザ携帯端末はスマートフォンである前記システム。

【請求項 15】 請求項 1 に記載のシステムにおいて、

前記業者端末はスマートフォンまたはパソコンである前記システム。

【請求項 16】 請求項 1 に記載のシステムにおいて、

前記決済装置は前記認証装置による認証が成立した後でなければ実行できないようにした前記システム。

【請求項 17】 ユーザの所有する携帯端末において、

運用業者からダウンロードされた、認証を実行するプログラムと、IDビットデータと、IDビットデータの複数のビット位置をアドレスするIDマップアドレスと、を含むアプリ、および

パスワードを入力する第1の入力装置、

を備え、前記アプリは、

前記第1の入力装置からのパスワードの入力に応答して、前記IDマップアドレスに基づいて前記IDビットデータから認証IDに変換するようにした認証装置。

【請求項 18】 請求項 17 に記載の認証装置において、

前記運用業者が前記ユーザに発行したネットカードに掲載されたIDパターンを撮像するカメラ(4)を含む第2の入力装置、

前記第2の入力装置で読み取ったIDパターンからIDビットデータを取り込み記憶するメモリ(48、49)、

前記アプリによって前記メモリから読み出された前記IDビットデータから前記IDマップアドレスに基づいて認証IDに変換するようにした認証装置であって、前記第1と第2の入力変換装置の一方を選択して使用することができるようにした認証装置

【請求項 19】 ユーザと販売業者との間で商品とその価格に合意が成立した場合、

ユーザの所持するユーザ携帯端末は、入力されたID情報を認証IDに変換し、この認証IDに基づいて認証が成立したとき、ユーザ番号とクレジット情報をサーバに送信し、

前記サーバは、前記ユーザ携帯端末からの前記ユーザ番号とクレジット情報を該サーバのメモリに保存し待機状態にし、

前記業者端末は、前記ユーザ番号が入力されたとき、該ユーザ番号と前記サーバに登録された当該業者番号を前記サーバに送信し、

前記サーバは、前記業者端末からの前記ユーザ番号と業者番号および前記メモリに保存された前記ユーザ番号と業者番号を照合し一致すれば、前記クレジット情報を前記業者端末に送信し、

前記業者端末は、前記サーバからのクレジット情報に基づき決済処理をし、前記サーバに決済完了の通知をし、および

前記サーバは、前記業者端末からの決済処理完了通知に基づき決済履歴データとして決済履歴データ部に記録する、

携帯端末を利用して認証および決済を行う方法。

【請求項 20】 ID情報を入力する入力装置、

該ID情報に基づき認証IDを発生する変換装置、
該認証IDに基づき認証のための動作を実行する認証装置、および
認証が成立したとき、運用会社のサーバに登録されたユーザ番号と、決済に利用するクレジット情報を前記サーバに送信する送信装置、
を備えたユーザ携帯端末。

【請求項21】 認証に用いるIDビットデータと認証IDとユーザ番号とクレジット情報を含むユーザ情報、および、販売業者の業者番号を含む業者情報を登録したデータベース、
ユーザ携帯端末からユーザ番号と認証IDを受信したとき、当該ユーザの個人認証を実行する認証装置、

個人認証の結果を前記ユーザ携帯端末に送信する第1の送信装置、
前記認証をしたユーザ携帯端末からユーザ番号とクレジット情報を受信したとき、それらをメモリに一時記憶し待機状態にするメモリ、
業者端末から当該ユーザ番号と業者番号の送信を受けたとき、前記ユーザ携帯端末から受信したユーザ番号を照合し、一致したならば、前記クレジット情報を前記業者端末に送信する第2の送信装置、および

前記業者端末から決済完了通知を受けたとき、決済完了履歴データとして登録する決済履歴データ部、

を備えた運用会社のサーバ。

【請求項22】 業者とユーザとの間で商取引について合意された後、運用会社のサーバに登録されたユーザ番号を入力する入力装置、

前記ユーザ番号と運用会社のサーバに登録された業者番号をサーバに送信する第1の送信装置、

該サーバから当該ユーザのクレジット情報を受信したとき、クレジット決済を実行する決済処理装置、および

該決済が完了したときは、決済完了通知を前記サーバに送信する第2の送信装置、
を備えたクレジット決済端末。