(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5362558号
(P5362558)

(45)発行日　平成25年12月11日(2013.12.11)　(24)登録日　平成25年9月13日(2013.9.13)

(51)Int.Cl.		F I		
G06F 21/32	(2013.01)	G06F	21/20	132
G06F 21/34	(2013.01)	G06F	21/20	134
G06F 21/31	(2013.01)	G06F	21/20	131E
H04L 9/32	(2006.01)	H04L	9/00	673D

請求項の数 16　(全 16 頁)

(21)出願番号	特願2009-516862 (P2009-516862)
(86)(22)出願日	平成19年6月26日 (2007.6.26)
(65)公表番号	特表2009-541870 (P2009-541870A)
(43)公表日	平成21年11月26日 (2009.11.26)
(86)国際出願番号	PCT/CN2007/001992
(87)国際公開番号	WO2008/006290
(87)国際公開日	平成20年1月17日 (2008.1.17)
審査請求日	平成22年6月3日 (2010.6.3)
(31)優先権主張番号	200610090945.2
(32)優先日	平成18年7月5日 (2006.7.5)
(33)優先権主張国	中国 (CN)

(73)特許権者　509002202
ヴァレー　テクノロジーズ，　エルエルシー．
アメリカ合衆国　デラウェア　１９８０８　ウィルミントン　センターヴィル　ロード　２７１１　スイート　４００
(74)代理人　100067828
弁理士　小谷　悦司
(74)代理人　100115381
弁理士　小谷　昌崇
(74)代理人　100157808
弁理士　渡邊　耕平
(74)代理人　100140660
弁理士　森本　理恵

最終頁に続く

(54)【発明の名称】生体特徴による身分認証の方法

(57)【特許請求の範囲】

【請求項１】

少なくともローカル装置及び認証サーバを有する認証システムにおいて生体特徴により身分認証を行う方法であって、

生体特徴データが生体特徴センサを介して前記ローカル装置に入力される入力工程と、

前記ローカル装置が、前記入力された生体特徴データを、前記ローカル装置のメモリに予め記憶されているオリジナル生体特徴データに対してマッチングを行うマッチング工程と、

前記入力された生体特徴データが前記メモリに予め記憶されている前記オリジナル生体特徴データとマッチする場合、前記ローカル装置が、第一の識別コードを生成する第一の識別コード生成工程と、

前記ローカル装置が、前記第一の識別コードを認証サーバに送信し、前記認証サーバが、前記システムに権限を付与して権限付与された操作を行うことを許可すべく前記第一の識別コードについて認証を行う認証工程と、を有し、

前記第一の識別コード生成工程は、前記ローカル装置が現在時刻及び静的データを用いて第一の識別コードを生成する工程を含み、

前記ローカル装置が、前記第一の識別コードを二回連続して生成する場合において、前記二回連続して生成された第一の識別コード間の間隔が所定時間間隔より大きいならば、前記認証サーバは、互いに異なる識別コードを生成し、

前記認証工程は、前記認証サーバが、認証要求を受信する工程と、前記認証サーバが、

前記第一の識別コードを受信する工程と、前記認証サーバが、前記第一の識別コード生成工程と同一の方法を用いて第二の識別コードを生成する工程と、前記認証サーバが、前記受信された第一の識別コードと前記第二の識別コードとがマッチするか否かを比較することにより、操作を行う権限を付与するか否かを決定する工程と、を有し、

前記第二の識別コードを生成する工程は、前記認証サーバが、現在の時間情報及び認証されるユーザの静的データを読み取る工程と、前記認証サーバが、前記読み取られた時間情報及び静的データを用いて、前記第二の識別コードを生成する工程と、を有し、

時間が所定の時間間隔を有する複数の連続したタイムスロットに区画され、同一のタイムスロット内に生成された識別コードはすべて同一であり、異なるタイムスロットで生成された識別コードは互いに異なり、

前記認証サーバが、前記第一の識別コードと前記第二の識別コードとがマッチしないと判定するならば、前記現在の時間情報で表される時刻から前記タイムスロットの長さ分だけ差し引いた時刻を表す時間情報に基づき第二の識別コードを生成し、当該生成された第二の識別コードが前記第一の識別コードにマッチするか否かを比較することにより、操作を行う権限を付与するか否かを決定することを特徴とする方法。

【請求項２】

前記生成された第一の識別コードの時刻と前記第二の識別コードの時刻との間の間隔が所定時間間隔よりも小さい場合、前記認証サーバは、前記生成された第一の識別コードと第二の識別コードとはマッチすると判定し、

前記生成された第一の識別コードの時刻と前記第二の識別コードの時刻との間の間隔が所定時間間隔よりも大きい場合、前記認証サーバは、生成された第一の識別コードと第二の識別コードとはマッチしないと判定することを特徴とする請求項１に記載の方法。

【請求項３】

前記所定時間間隔の値は１～５分の間に設定されていることを特徴とする請求項２に記載の方法。

【請求項４】

前記認証工程は、

ユーザの口座情報を認証サーバに送信する工程と、

認証サーバが、受信された口座情報に基づいて、第二の識別コードを生成するための静的データをデータベースから抽出する工程と、

を更に有することを特徴とする請求項１に記載の方法。

【請求項５】

前記方法は、

前記ローカル装置と前記認証サーバとを接続する工程と、

前記ローカル装置と前記認証サーバとの間でローカル装置識別子をやりとりする工程と、

前記ローカル装置のタイマを前記認証サーバのタイマに同期させる工程とを有する初期化工程を更に有する

ことを特徴とする請求項１に記載の方法。

【請求項６】

前記方法は、

前記ローカル装置のユーザに関する静的データを認証サーバに提供する工程と、前記サーバと前記ローカル装置との間で鍵セットをやりとりする工程とを有するログイン工程を更に有することを特徴とする請求項１に記載の方法。

【請求項７】

前記鍵セットはＰＫＩ鍵を含むことを特徴とする請求項６に記載の方法。

【請求項８】

前記方法は、

口座番号及び静的識別コードを含む静的データを前記認証サーバに提供する工程と、

入力された静的データについて前記認証サーバにて認証を行う工程と、

認証された場合、口座番号ごとに特定の鍵セットを生成する工程と、
前記生体特徴データを入力して前記ローカル装置に記憶する工程と、
を有する登録工程を更に有することを特徴とする請求項１に記載の方法。
【請求項９】
前記認証工程において権限付与される操作は電子バンキング及び／又はテレホンバンキング取引であることを特徴とする請求項１に記載の方法。
【請求項１０】
前記認証工程において権限付与される操作は電子商取引であることを特徴とする請求項１に記載の方法。
【請求項１１】
前記入力工程における生体特徴データは、指紋データ、顔像データ、虹膜データ、掌紋データ、オーディオデータ、皮下静脈データ及び／又は筆跡データであることを特徴とする請求項１に記載の方法。
【請求項１２】
前記入力された生体特徴データが前記メモリに予め記憶されている生体特徴データとマッチしない場合、前記ローカル装置が、エラー情報を提示する工程を更に有することを特徴とする請求項１に記載の方法。
【請求項１３】
前記生成工程の後であって前記認証工程の前に、生成された第一の識別コードをディスプレイに表示する工程を更に有することを特徴とする請求項１に記載の方法。
【請求項１４】
第一の識別コードは、標準の銀行業界プロトコル、ＰＫＩ暗号化方式及び／又は３－ＤＥＳ暗号化方式に基づいて生成されることを特徴とする請求項１に記載の方法。
【請求項１５】
前記静的データは複数のユーザ及び／又は口座の複数セットのユーザデータを含み、
第一の識別コードを生成する際に、ユーザにより必要な１セットのユーザデータが選択され、
選択されたユーザデータに基づいて第一の識別コードが生成される
ことを特徴とする請求項１に記載の方法。
【請求項１６】
前記電子バンキング取引はＰＯＳ機及び／又はＡＴＭを介して行われる取引であることを特徴とする請求項９に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、生体認証及び動的認証の分野に関し、具体的には、本発明は、生体特徴及び動的ＰＩＮコードを用いて個人身分認証をして動作／操作を行う方法、装置、サーバ及びシステムに関する。
【背景技術】
【０００２】
従来の銀行取引における認証では、銀行カードの所有者又は出納係がカード読取機で銀行カードを使用する際に、ＰＯＳ(Point of Sale)端末のソフトウェアＥＤＣ(Electronics Data Capture)が、格納されている電話番号にモデムを介してダイヤルしてアクワイアラ(acquirer)をコールする。アクワイアラは、信用認証要求を取引先から収集し、取引先に支払い保証を提供する。アクワイアラは、銀行カード認証要求を受信すると、銀行ＩＤ、有効なカード番号、有効期間、クレジットカード限度額など、銀行カードの磁気ストリップに記録されているデータを調査する。単一のダイヤル取引は、通常、例えば１２００ｂｐｓないし２４００ｂｐｓのレートで処理され、直接にインターネットに接続された場合はより速度の速い処理が提供される。このようなシステムでは、銀行カード所有者は、キーパッド又はその他の類似の装置でＰＩＮ(Personal Identification Number)コード（

又は口座のパスワード）を入力できる。このＰＩＮコードは、例えばユーザが銀行口座を開設するときに設定したパスワードである。また、ＰＩＮコードを使わなくてもよい取引もたくさんある。ＡＴＭ（現金自動預け払い機）から現金を取り出す前に、通常、ＡＴＭは入力されたＰＩＮコードを暗号化して遠隔データベースに送信してマッチするか否かを判断する。前記全過程において、ＰＩＮコードは常に「静的」状態にある。即ち、数ヶ月間、長い場合には数年間、同一のＰＩＮコードが使われる。インターネット取引の普及によって、銀行口座やＰＩＮコードが盗み取られ、又は盗用される蓋然性が高くなっているため、静的ＰＩＮコードを用いる従来の電子バンキングの取引プロセスは非常に脆弱である。

【０００３】

従来の銀行カード取引方式では、ユーザが予め設定した静的ＰＩＮコードしか存在しないため、秘密漏れを防止するためには、ユーザは、静的ＰＩＮコードを設定する際に、このＰＩＮコードの複雑性を増加させるとともに、該ＰＩＮコードを覚えやすいものにしなければならない。ユーザは、この静的ＰＩＮコードを再設定しようと考えた場合、若しくは当該ＰＩＮコードを忘れた場合には、カード発行銀行の窓口まで行って処理を行わなければならないため、ユーザに大きな不便をもたらすことになる。また、ユーザは、通常異なる銀行カードに対して同一のパスワードを使うが、これによって機密性が大幅に低下する。一方、ユーザが、異なる銀行カードに対して異なるパスワードを使用する場合は、如何にしてこれらのパスワードを記録・記憶するかが問題となる。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

一方、従来の銀行システムは、磁気カードで電子取引を行うのが一般的であるが、磁気カードは磁気ストリップにより口座情報及びその他のユーザ情報を記録することから、容易に読み取られ、又は口座情報を基に同一の情報を記録した磁気カードが容易に作製されて、ユーザの口座が盗用されることになる。磁気カードの代わりにスマートＩＣカードを使用することは、安全性を高める解決案の一つとなるが、磁気カードは広い範囲で使用されているため、磁気カードをＩＣカードに取り替える場合、既存のすべての磁気カード及び磁気カードを読み取る装置をすべてＩＣカード及びＩＣカードを読み取る装置に取り替えなければならない。従って、この解決案はコストが極めて高く、実行性が低い。よって、磁気カードのデータ読取り及び読み取ったデータのネットワーク上での伝送のための既存の磁気カードシステムのグローバルな基盤構造を変更しないという前提で取引の安全性を高めることが求められる。

【０００５】

本発明の一つの目的は、動的身分認証ソリューションを提供することにより、既存の電子取引システムへの変更を最小限にすることを前提として、電子取引の機密性、安全性を高めることにある。

【０００６】

本発明の他の目的は、本発明の動的身分認証ソリューションを実現するための携帯身分認証装置、対応する認証サーバ及びシステムを提供することにより、電子取引の便利性を高めることにある。

【課題を解決するための手段】

【０００７】

上述の目的及びその他の目的を達成するため、本発明の第一の態様によれば、少なくともローカル装置及び認証サーバを有する認証システムにおいて生体特徴により身分認証を行う方法が提供され、該方法は、生体特徴センサを介して前記ローカル装置に生体特徴データを入力する入力工程と、前記入力された生体特徴データと前記ローカル装置のメモリに予め記憶されているオリジナル生体特徴データとについてマッチングを行うマッチング工程と、入力された生体特徴データが前記メモリに予め記憶されているオリジナル生体特徴データとマッチする場合、前記ローカル装置にて第一の識別コードを生成する第一の識

別コード生成工程と、前記第一の識別コードを認証サーバに送信し、認証サーバが、前記システムに権限を付与して権限付与された操作を行うことを許可すべく、前記第一の識別コードについて認証を行う認証工程とを有する。

【０００８】

本発明の第二の態様によれば、生体特徴により身分認証を行う装置が提供され、該装置は、オリジナル生体特徴データを予め記憶するためのメモリと、生体特徴データの入力を受信するための生体特徴センサと、生体特徴センサにより入力された生体特徴データと前記メモリに予め記憶されているオリジナル生体特徴データとについてマッチングを行うためのマッチング手段と、前記入力された生体特徴データが前記メモリに予め記憶されているオリジナル生体特徴データとマッチする場合、第一の識別コードを生成する第一の識別コード生成手段とを有する。

【０００９】

本発明の第三の態様によれば、身分認証を行うサーバが提供され、該サーバは、認証要求、静的データ、及び認証すべき第一の識別コードを受信するための受信手段と、認証要求を受信すると、静的データに基づいて第二の識別コードを生成する第二の識別コード生成手段と、受信した第一の識別コードを生成した第二の識別コードと比較する比較手段と、前記比較手段の比較結果が、第一の識別コードが第二の識別コードにマッチすることを示す場合に、権限を付与する旨の情報を返し、前記比較手段の比較結果が、第一の識別コードが第二の識別コードにマッチしないことを示す場合に、権限付与を拒否する旨の情報を返す送信手段と、を有する。

【００１０】

本発明の第四の態様によれば、生体特徴により身分認証を行うシステムが提供され、該システムは、前記装置及び前記サーバを有する。

【発明の効果】

【００１１】

本発明によれば、既存の電子取引システムへの変更を最小限にすることを前提として、電子取引の機密性、安全性を高めることができる。

【００１２】

本発明の前述及びその他の機能、変更、及び優れた点は、図面を参照して、本発明の好ましい実施の形態を詳細に説明することで、より明らかになるであろう。

【００１３】

以下の図面において、同一の符号は同一の装置又は手段を示すものである。

【図面の簡単な説明】

【００１４】

【図１】本発明の一実施の形態に係る方法を示すフローチャートである。

【図２】本発明の初期化工程を示すフローチャートである。

【図３】本発明のログイン工程を示すフローチャートである。

【図４】本発明の登録処理工程を示すフローチャートである。

【図５】本発明の一実施の形態に係る装置を示す概略図である。

【図６】本発明のシステムを示す概略図である。

【図７】本発明の一実施の形態に係るサーバを示す概略図である。

【図８】動的ＰＩＮの生成原理を示す概略図である。

【発明を実施するための形態】

【００１５】

本発明の理解の便宜のため、以下の説明では、銀行カードへの本発明の適用について説明する。本発明は、また、カードアクティベータ(Card Activator)、電子商取引(E-Commerce)、電子財布(E-Purse)、個人識別装置、外部システムアクセス制御、身分証及び社会保障カードの読取機、電子セーフティ装置(Electronic safe)などに適用できる（但し、これらに制限されるものではない）と理解すべきである。

【００１６】

以下、銀行カードを例にして図１を参照しながら本発明の方法について詳しく説明する。ステップ１０１において、銀行カード所有者は、生体特徴センサを介して生体特徴データを入力する。この生体特徴センサは、例えば指紋センサであるが、顔像センサ、虹膜センサ、掌紋センサ、オーディオセンサ、筆跡センサ、音声センサ、皮下静脈センサなどその他の生体特徴センサを利用してもよい。一実施の形態において、この生体特徴センサは、１：１指紋認証に用いられるＣＯＭＳ指紋スキャナであってよい。このようなスキャナは、例えば、ＳＴＭｉｃｒｏｅｌｅｃｔｒｏｎｉｃｓ社製ＴＣＥＢＡ　ＴＯＵＣＨＣＨＩＰ（登録商標）指紋生体特徴サブシステム及びＧｒｏｕｐｅ　ＳＡＧＥＭ社製ＭＯＲＰＨＯＭＯＤＵＬＥ（商標）指紋生体特徴サブシステムであり、また、ＡＴＭＥＬ　ＡＴ７７Ｃ１０４Ｂ－ＣＢ０８ＹＶなどその他の生体特徴センサを利用してもよい。指紋スキャナは、1:nの指紋識別用に設計してもよい。また、光学式、容量式及びその他の種類の指紋スキャナを利用してもよい。

【００１７】

ステップ１０２において、入力された生体特徴が予め記憶されているオリジナル生体特徴と比較され、両者がマッチする場合、処理はステップ１０３へ進み、所定の時間（通常は数十秒）内にマッチしない場合、処理はステップ１０６へ進む。

【００１８】

ステップ１０３において、取引で使用すべく動的ＰＩＮコードを動的ＰＩＮアルゴリズムによって生成する。この動的ＰＩＮアルゴリズムについては後で詳しく説明するが、例えば、既存のVisa/IBM、3-DES(Data Encryption Standard)暗号化方式及びＰＫＩ（公開鍵基盤）暗号化方式などを利用できる。ローカル装置では、例えばユーザに関する口座番号、初期ＰＩＮコード及び装置ＭＡＣアドレスなどを含む不変のユーザデータ（静的データともいう）及び現在時間などの情報をパラメータとして、上述の既存のアルゴリズムにて動的ＰＩＮコードを生成する。一実施の形態において、ローカル装置には現在のクロック情報を提供するタイマがあり、このタイマは、サーバ側ＤＰＡＳ（動的ＰＩＮコード認証システム）のタイマと一致するように保持される。即ち、両者の誤差は、サーバ側ＤＰＡＳがローカル装置で生成された動的ＰＩＮコードを認証することが保証される程度に小さい。

【００１９】

ここで、上述の動的ＰＩＮとは、毎回動的ＰＩＮアルゴリズムにて生成されたＰＩＮコードが異なる可能性があることを言う。動的ＰＩＮアルゴリズムは、変化している現在時間をパラメータとして利用するため、ＰＩＮコードを生成する現在時間が変化した場合、生成されたＰＩＮコートが変化する可能性がある。ローカル装置とサーバ側とが同一のＰＩＮコードを生成することを保証するためには、ローカル装置とサーバ側とが、同一の動的ＰＩＮアルゴリズム、同一の静的パラメータ、及び互いに近い時間パラメータで動的ＰＩＮコードを生成することが要求される。例えば、サーバ側のＤＰＡＳがＰＩＮコードを生成する現在時間により動的ＰＩＮコードを生成した後、生成されたＰＩＮコードとローカル装置で生成されたＰＩＮコードとについてマッチングを行って認証を実現する。

【００２０】

ここで、上述の現在時間は、ＰＩＮコードを生成する際の絶対時間であってよいし、ある特定の時点に対するそのときの相対時間であってもよい。また、この現在時間はＰＩＮコードを生成する時刻に近接するある時刻でもよい。例えば、現在時間は、ＰＩＮコードを生成する時刻を分の時刻に丸め、又は、５分を単位として丸めた時刻とすることができる。即ち、仮にＰＩＮコードを生成する時刻が3:47であるならば、この時刻を3:45に丸めてＰＩＮコードを生成するための現在時間にすることができる。

【００２１】

以下、図８を参照しながら動的ＰＩＮコードを用いて認証を行う原理について更に詳しく説明する。図８に示すように、例えば時間軸を複数の一定の時間間隔を有するタイムスロットに区画する。動的ＰＩＮアルゴリズムにて、静的パラメータ及び現在時間により動的ＰＩＮコードを生成する場合、同一のタイムスロットで生成されたＰＩＮコードはすべ

て同一であり、異なるタイムスロットで生成されたＰＩＮコードは互いに異なることが要求される。図８に示すように、３つのタイムスロットで生成されたＰＩＮコードが、それぞれＰＩＮ１、ＰＩＮ２、ＰＩＮ３であるとする。ローカル装置は、時刻ｔ１で動的ＰＩＮコードを生成する場合、ｔ１が第一のタイムスロットの範囲内にあるため、ＰＩＮ１を生成する。ローカル装置にて生成されたＰＩＮ１コードで認証を行う場合、サーバ側のＤＡＰＳが認証要求を受信すると、静的データ及び現在時間により動的ＰＩＮコードを生成するが、認証要求の過程における時間遅延により、サーバはｔ１以降の例えばｔ２で動的ＰＩＮコードを生成する。しかし、ｔ２はｔ１と同一の第一のタイムスロットに入るため、同様にＰＩＮ１コードが生成される。この場合、認証要求されているＰＩＮ１コードがサーバで生成されたＰＩＮコードと一致するため、認証を完成させることにより権限を付与してその次の操作、例えば銀行取引、電子商取引、又は会員身分認証、ログインなどを行うことができる。一方、認証要求の遅延時間が長すぎて、サーバ側のＤＰＡＳでＰＩＮコードを生成する時刻と、ローカル装置でＰＩＮコードを生成する時刻とが異なるタイムスロットに入る場合、例えば、サーバ側のＤＰＡＳが時刻ｔ３で動的ＰＩＮコードを生成する場合、ＰＩＮ２が生成されることになる。そうすると、両サイドで生成されたＰＩＮコードはマッチしないと判定され、即ち、認証失敗となる。二回連続して生成されたＰＩＮコードの間の時間間隔が所定時間間隔よりも大きい場合、生成されたＰＩＮコードは互いに異なることが好ましい。前記所定時間間隔の値は１～５分の間に設定することが好ましい。

【００２２】

ここで、例えば、時刻ｔ１、ｔ２はそれぞれ異なるタイムスロットにあるが、両者の間の時間間隔は非常に近く、例えば、ｔ１は第一のタイムスロットの末尾にあり、ｔ２は第二のタイムスロットの先頭にある、という臨界状況を考えてみる。この場合、その認証過程において、好ましい方式として以下の方式を採用できる。即ち、先ず、サーバは、現在時刻ｔ２で生成されたＰＩＮ２を、ユーザが提供した時刻ｔ１で生成されたＰＩＮ１と比較し、マッチしないと判断された場合、サーバは、現在時刻ｔ２から前記タイムスロットの長さΔｔを引いて得られた時間を、ＰＩＮコードを生成するパラメータとして、ＰＩＮコードを再生成する。ｔ２がｔ１の次のタイムスロット内にある場合、ｔ２からタイムスロットの長さを引いて得られた時間は、１つ前のタイムスロット内のある時刻となり、即ち、ｔ１と同一のタイムスロット内に入るため、この修正後の時間パラメータに基づいて生成されたＰＩＮコードは、ユーザが提供した時刻ｔ１で生成されたＰＩＮコードと一致するはずである。このとき、マッチングが成功した場合、認証されたと判定する。上記の臨界問題は、他の類似の方法でも解決することができる。

【００２３】

上述した説明において、異なるタイムスロットで生成されたＰＩＮコードを異なるものと規定した目的は、ユーザがローカル装置でＰＩＮコードを生成した後の数分内に遅滞無くＰＩＮ認証を実行しなければならず、遅滞時間が長すぎると、前に生成されたＰＩＮコードは失効して、ＰＩＮコードを改めて生成しなければならないようにするためである。言い換えれば、このような方法で、生成されたＰＩＮコードごとにある短時間の有効期間を規定することにより、不法者がＰＩＮコードを窃取した後にユーザの口座を盗用して取引を行うことを防止している。

【００２４】

好ましくは、ステップ１０４において、生成された動的ＰＩＮコードがディスプレイに表示され、ユーザは、ＡＴＭ、銀行カウンタ、及び会員ログインインタフェースにて手動でＰＩＮコードを入力して認証を行ってよい。また、生成されたＰＩＮコードをＵＳＢインタフェースなどの外部インタフェース、又は赤外線、ブルートゥース（登録商標）、ＷＬＡＮ、ＲＦＩＤなどの無線インタフェースを介して認証システムに送信してもよい。

【００２５】

ステップ１０５において、ユーザは生成されたＰＩＮコードを具体的な電子商取引で用いて取引を行う。ステップ１０６では、ディスプレイに「無効な指紋」と表示することが

できる。この代替として、可視又は可聴の警報でＰＩＮコードの生成失敗を通報してもよい。

【００２６】

上述した図１に示す具体的な認証ステップを実行する前に、図２、図３、図４に示す初期化工程、ログイン工程、登録工程を行うことにより、ユーザに関する口座情報、動的ＰＩＮコードの生成に必要な鍵、動的ＰＩＮコードを生成するローカル装置識別子、及びタイマを、ローカル装置と認証サーバとの間で同期させなければならないとすることが好ましい。

【００２７】

図２は初期化工程を示す概略フローチャートである。ステップ２０１において、ネットワークを介してローカル装置と認証サーバとを接続する。ステップ２０２において、ローカル装置とサーバとの間で真実検証値(genuine verification value)、例えば、ローカル装置のＭＡＣアドレスをやりとりする。ここで、「やりとりする」とは、ローカル装置とサーバとの間でデータが一致するように維持することを言う。

【００２８】

一実施の形態においては、認証サーバがローカル装置にＭＡＣアドレスを要求し、その後、ローカル装置がそのＭＡＣアドレスを認証サーバに送信する。認証サーバは、ローカル装置のＭＡＣアドレスを受信した後、その装置データベースにて該ＭＡＣアドレスを検索する。その装置データベースから該ＭＡＣアドレスが検索されない場合、検証失敗とされ、ローカル装置はそのメモリをクリアして、認証サーバとの間の通信を終了するようにしてよい。また、そのディスプレイに例えば「無効な装置」などの情報を表示してもよい。他の実施の形態においては、ＭＡＣアドレスのようなローカル装置識別子が認証サーバの装置データベースに含まれていない場合に、認証サーバは、このローカル装置を装置データベースに加えて検証を完了する。このＭＡＣアドレスは動的ＰＩＮを生成するための静的データとして利用できる。

【００２９】

ステップ２０３において、ローカル装置は、認証サーバからファームウェア(firmware)をダウンロードする。最後に、ステップ２０４において、ローカル装置は更新後のファームウェアを使用できるように再起動する。

【００３０】

図３はログイン工程を示す概略フローチャートである。ステップ３０１において、ユーザは、例えばウェブページにある申請表にユーザデータを入力する。ステップ３０２において、ユーザは、例えば「ｓｅｎｄ」ボタンを押すことにより申請表を認証サーバに送信する。ステップ３０３において、認証サーバとローカル装置との間で新しい鍵セット（例えばＰＫＩ）がやりとりされる。この鍵セットは動的ＰＩＮを生成するための静的データとしても利用される。

【００３１】

図４は登録ステップを示す概略フローチャートである。ステップ４００において、ネットワークを介してローカル装置と認証サーバとを接続する。ステップ４０１において、ユーザは、ローカル装置で銀行カードデータ（例えば静的ＰＩＮコードを含む）及び生体特徴データを入力して（必要に応じてその他のデータを入力してもよい）、銀行カードデータを認証サーバに送信する。ステップ４０２において、認証サーバのＤＰＡＳ（動的ＰＩＮコード認証システム）は、銀行カードデータについて認証を行い、ステップ４０３において、カードごとに特定の鍵セットを生成する。その後、ステップ４０４において、認証サーバは銀行カードデータを単独のデータベースに記憶することができる。該データベースは、前述した装置データベースとは異なるデータベースであってもよい。また、１つ又は複数の口座データをローカル装置に送信してよい。

【００３２】

図５は本発明の一実施の形態に係る装置の概略図である。図５に示すように、ＰＢＤ（個人生体特徴装置）５０１は、本発明による装置である。ＰＢＤ５０１は、動的ＰＩＮコ

ード生成部５０２、マッチング部５０３、生体特徴データメモリ５０４、生体特徴センサ５０５、静的データメモリ５０６、ディスプレイ５０７、外部コネクタ５０８、電源部５０９及びタイマ５１０を有する。図５に示されたこれらの構成要素は、本発明を説明するための例示にすぎず、本発明を限定するものではない。

【００３３】

マッチング部５０３は、生体特徴センサ５０５から入力された生体特徴データと、生体特徴データメモリ５０４に予め記憶されているオリジナル生体特徴データとのマッチングに用いられる。好ましくは、マッチング部５０３は、生体特徴をキャプチャして解析するためのソフトウェア又はファームウェアを稼動する。

【００３４】

マッチング部５０３によるマッチングが成功した場合、動的ＰＩＮコード生成部５０２は、静的データメモリ５０６に予め記憶されている静的データ及びタイマ５１０から提供された現在時間により動的ＰＩＮコードを生成する。

【００３５】

上述の図８を参照して説明したＰＩＮコードの生成及び認証の原理から、動的ＰＩＮコード生成部５０２がＰＩＮコードを生成する際に使用するタイマ５１０の時間情報は、認証サーバ側の時間情報と一致するはずであることが分かる。即ち、同一の時刻において、ＰＢＤ５０１におけるタイマ５１０からの時間情報と認証サーバのタイマからの時間情報との誤差は無視できるほど小さい。

【００３６】

生体特徴センサ５０５の一実施例は指紋センサである。静的データメモリ５０６は、例えば口座データ、ユーザ名、ＰＢＤのＭＡＣアドレス、動的ＰＩＮコードを生成するための鍵セットなどのような、通常は時間に伴って変化しない静的データの記憶に用いられる。ディスプレイ５０７は、例えば動的ＰＩＮコード又はエラー情報の表示に用いられるが、必要に応じてその他のデータを表示してもよい。ディスプレイ５０７は液晶ディスプレイであることが好ましいが、その他の種類のディスプレイを利用してもよい。一実施の形態において、ディスプレイ５０７は、１行のディスプレイであってよいが、他のサイズのディスプレイを利用してもよい。外部コネクタ５０８は外部システムとの接続に用いられる。外部コネクタ５０８は他の種類の有線コネクタ（例えばシリアルポート、パラレルポート若しくはファイヤワイヤポート）、又はブルートゥース（登録商標）、その他の無線通信に利用される無線コネクタであってもよい。

【００３７】

電源部５０９はＰＢＤ５０１への電源供給に用いられる。電源部５０９は、例えば充電可能な蓄電池であってよい。この電源部５０９は、メイン電池とバックアップ電池を含んでもよい。通常、メイン電池が有効である場合には、メイン電池から電源供給されて、生体特徴データの入力、生体特徴データのマッチング、動的ＰＩＮコードの生成と出力などの操作をすべて行う。メイン電池が失効した場合又はＰＢＤ５０１が閉じている場合は、バックアップ電池で、例えば、タイマの連続的な時間カウントを保持し、生体特徴データ及び静的データの記憶を保持するなど、最低限の電力消費を維持することができるが、生体特徴データの入力、生体特徴データのマッチング、動的ＰＩＮコードの生成及び出力などの操作を行うことはできない。ローカル装置の状態を維持するバックアップ電池の電力消費は非常に低いため、通常数年間にわたって充電や電池交換をせずに使用できる。

【００３８】

本発明に係る装置に、キーパッド(keypad)を有してもよい。このキーパッド（図示しない）は、一般的な電卓の０～９のテンキーに類似するキーボード領域を含んでよいが、更に、「＋、－、×、÷」の四つの基本的な計算記号及び記号「＝」などを含んでもよい。また、データで特徴を入力するための他のキー、タイプ、又はこれらの特徴の他のレイアウトを有してもよい。専用の「オン／オフ」(on/off)ボタンでＰＢＤを起動・終了してもよいし、生体特徴センサにタッチすることによりＰＢＤを自動的に起動・終了してもよい。

【００３９】
検知された指紋と記憶されている指紋とを比較するためのロジック回路に接続する場合、指をどのようにセンサ５０５に置いたとしても（指紋が汚れている場合も含む）、生体特徴センサ５０５による指紋マッチング成功率に顕著な影響を与えないことが好ましい。
【００４０】
５０２～５１０はそれぞれ独立した部材として示されているが、製造上の理由又はその他の理由により、便宜のため、又は必要に応じて、これらの部材を更に１つ又は複数の集成チップに集成してもよいし、更に単独のモジュールに分離してもよい。
【００４１】
登録段階では、カード所有者データがＰＢＤ内に記憶される。カード所有者データは、デビットカード／クレジットカードデータ、オリジナル静的ＰＩＮコード（銀行から該オリジナル静的ＰＩＮコードを転送することによりカードをアクティブにする）を、該カード及びユーザの生体特徴と関連付けている。動的ＰＩＮコードアルゴリズムは、指紋認証により始動する。このアルゴリズムは、カード発行銀行の取引システムに接続された動的ＰＩＮ認証システムが動的ＰＩＮコードの生成に用いるアルゴリズムと同一である。生体特徴データが入力された時点から、ＰＢＤは、所定時間の間（通常は１～５分間）有効な動的ＰＩＮコードを生成し、認証サーバに認証要求があると、識別を行う。このＰＩＮコードは、ＰＯＳ及び／又はＡＴＭ上で行われる取引の認証に用いられる。動的ＰＩＮアルゴリズムは、例えばVisa/IBM、3-DES(Data Encryption Standard)暗号化方式及びＰＫＩ（公開鍵基盤）暗号化方式など、標準的な銀行業界のプロトコルを含んでよい。これにより、ＰＩＮを形式化して、銀行ネットワーク上で動的ＰＩＮをトランスペアレント伝送し、サーバ側でハードウェア安全モジュールのような標準の業界マッチングツールを利用して動的ＰＩＮを識別できる。ＰＣでオンライン接続することにより、生体特徴識別以外のユーザ入力を必要せずに、電子バンキング及び電子商取引の認証を行うことができる。
【００４２】
ＰＢＤを有する生体特徴保護システムでは、銀行プロトコル及びネットワークインフラストラクチャを変更せずに、磁気ストリップを備えるデビットカード／クレジットカードを通常の方式で取引に用いることができる。通常、購入又はその他の種類の取引過程では、デビットカード／クレジットカードが、取引の端末に挿入され、若しくは端末にスキャンされる。取引を有効にするため、ＰＢＤ５０１に表示されるＰＩＮコードを端末に入力することをカード所有者に要求することができる。動的ＰＩＮコードが要求され、かつ、該動的ＰＩＮコードが正確に提供された場合、サーバ側（動的ＰＩＮ認証システム）で取引に対して認証を行い、発行者認証システムより通常の方式で該取引を有効にする。
【００４３】
カード発行銀行によりデビットカード／クレジットカードに関連付けられているオリジナル静的ＰＩＮを利用せずに、ＰＢＤ５０１で生成された動的ＰＩＮコードを利用して、ＰＯＳ及びＡＴＭ端末を介してデビットカード／クレジットカードを使用することができる。このような場合、サーバシステムは、中央データベースに記憶されているユーザデータ及び暗号化するための鍵を収集し、受信した動的ＰＩＮとマッチングして動的ＰＩＮを再構築することができる。
【００４４】
指紋センサ５０５にてキャプチャした指紋が、ＰＢＤ５０１に記憶されている指紋とマッチしない場合、ＰＢＤ５０１は、ディスプレイ５０７にエラーメッセージを表示し、認証処理を中止することができる。
【００４５】
一実施の形態おいて、複数の人が１つのＰＢＤ５０１を共有することができる。この場合、ＰＢＤ５０１には人ごとに生体特徴データが記憶される。これらの生体特徴データは、記憶されている口座データ中のある一部又は全部のデータと関連付けることができる。これにより、例えば、個人ＡはＰＢＤ５０１に記憶されているカード１、２、３に対する口座データを利用することができ、個人ＢはＰＢＤ５０１に記憶されているカード４、５

、６に対する口座データを利用することができる。したがって、個人Ａと個人Ｂはいずれも ＰＢＤ５０１を利用でき、それによってカードを使えるようにすることができる。人と所望の記憶されている口座データへのアクセスとの任意の組み合わせを提供することができる。

【００４６】

ＰＢＤ５０１は、上述のようにして、複数のカードに対する口座データを記憶することができる。単一の静的ＰＩＮコードは、口座データに含まれている各口座と関連付けられている。動的ＰＩＮコードアルゴリズムは、毎回の取引において各口座を特定する特有の一度だけのＰＩＮコードを生成するために用いられる。認証－有効性メカニズムは生体特徴識別をトリガーとして起動される。複数のユーザの複数の口座データが記憶されている場合、ＰＢＤ５０１は、更に特定のユーザの特定口座を選択する手段を提供することによって、選択された口座に基づいて当該口座に有効な動的ＰＩＮコードを生成する。

【００４７】

一実施の形態において、ＰＢＤ５０１は、更に図に示されていない自滅装置を備えており、ＰＢＤ５０１が分解されようとした場合に、記憶されている生体特徴データ及び／又は記憶されている口座データを破壊する。

【００４８】

典型的な登録では、ＰＢＤ５０１を登録システム（サーバ）に接続した後、カード所有者は、磁気ストリップを有するデビットカード／クレジットカード又はスマートカードをＰＢＤ５０１又は外部カード読取機に挿入することができ、若しくは、接続されているコンピューターシステムにおいて手動で情報を入力することができる。その後、この磁気ストリップを有するデビットカード／クレジットカードに関連付けられているＰＩＮコード又はその他の認証鍵を入力することができる。登録システム及びＰＢＤ５０１は、公開鍵基盤技術を利用して両者間の通信を暗号化、復号化することができるため、ＰＢＤ５０１と登録システムそれぞれが相手側に自己の公開鍵を送信することができる。なお、その他の暗号化技術を利用してもよい。

【００４９】

その後、登録システムはＰＢＤ５０１にその身分を要求することができる。通常は、ＰＢＤ５０１のＭＡＣ（メディアアクセス制御）アドレスが要求される。前記ＭＡＣアドレスは、ネットワーク上の各ノード（例えば、前記ＰＢＤ）を唯一的に表記するためのハードウェアアドレスである。そして、ＰＢＤ５０１は該ＭＡＣアドレスを登録システムに送信してもよいし、又は、登録システムがＰＢＤ５０１から読み取ってもよい。通常、登録システムは、ＰＢＤデータベースで該ＰＢＤ５０１のＭＡＣアドレスを検索する。一実施の形態では、ＰＢＤ５０１のデータに当該ＰＢＤ５０１が含まれていない場合、検証は失敗となり、ＰＢＤ５０１はその静的データメモリをクリアして、登録システムとの通信を終了し、ＰＢＤ５０１のディスプレイ５０７に「無効な装置」などのエラーメッセージを表示する。他の実施の形態では、登録システムのＰＢＤデータに当該ＰＢＤ５０１が含まれていない場合、登録システムは、当該ＰＢＤ５０１を当該登録システムのデータベースに追加して検証を完了させる。

【００５０】

ＰＢＤ５０１の身分の検証が成功した場合、登録システムは、通常ＰＢＤ５０１に登録命令を送信する。その後、ＰＢＤ５０１は、指を指紋センサ５０５に置くことにより生体特徴入力データを提供するようカード所有者に要求する旨のメッセージを表示することができる。ＰＢＤ５０１は、ディスプレイ５０７においてメッセージを利用することで、指を指紋センサ５０５に置くようカード所有者に指示することができる。ＰＢＤ５０１が指紋の取得に成功した場合、該ＰＢＤ５０１は、この指紋をＰＢＤ５０１の生体特徴データメモリ５０４に記憶し、成功又は失敗したことを示す登録ステータスを登録システムに送信する。登録が失敗した場合、ＰＢＤ５０１は、登録操作を停止し、メモリをクリアして、登録サーバとの通信を終了し、ディスプレイ５０７に「登録失敗」などのメッセージを表示して登録が失敗したことをカード所有者に知らせることができる。

【００５１】
登録が成功した場合、登録システムは、該システムがＰＢＤ５０１からデータを受信する準備ができていることをＰＥＤ５０１に示すことができる。そして、ＰＢＤ５０１は、デビットカード／クレジットカードからの情報及びカード所有者の情報を登録システムに送信することができる。その他の情報については、登録システムは必要に応じて任意の有用な供給源から取得することができる。但し、ＰＢＤ５０１は、生体特徴メモリ５０４に記憶されている生体特徴データについては登録システムに送信しない。その後、登録システムにより受信されたカード及び顧客のデータが登録データベースに記憶される。この登録データベースはＰＢＤデータベースとは同一のデータベースでなくてもよい。そして、登録システムは、１又は複数の口座データをＰＢＤ５０１に送信することができる。
【００５２】
その後、サーバは、登録が成功した旨のメッセージをＰＢＤ５０１に送信することができる。ＰＢＤ５０１は、ディスプレイ５０７にそのメッセージを表示することができる。ＰＢＤ５０１は、該口座データを該ＰＢＤ５０１の口座データメモリに記憶する。上述の操作はあくまでも本発明を説明するための例示的なものであり、その他の操作又は操作手順を採用してもよいことは言うまでもない。
【００５３】
登録システムは、ＰＢＤ５０１に登録されている任意のカード又は全てのカードのカード発行機構の異なる主体によって操作される。将来の登録取引において、ＰＢＤ５０１は、登録システム又は別のカード発行機構又は他のシステムから付加的な口座データを取得できることも考えられる。ＰＢＤ５０１に複数の口座データが提供される場合、記録されている生体特徴データは、通常、各口座データとも関連付けられることになる。
【００５４】
一実施の形態において、ＰＢＤ５０１を無線通信又は有線通信でネットワーク（例えば、インターネット）に接続すれば、ＰＢＤ５０１を電子商取引に利用することができる。
【００５５】
以下、図６を参照しながら本発明による認証システムについて詳しく説明する。
【００５６】
本発明による認証システムは、ＰＢＤ５０１、カード発行銀行サーバ６０１、及び動的ＰＩＮコード認証サーバ６０２を有する。本発明のシステムは、必要に応じてその他の構成又はサブシステムを有してもよい。銀行カード６０９を用いて電子商取引を行う一実施の形態において、ＰＢＤ５０１はＵＳＢ／ファイヤワイヤ／ブルートゥース（登録商標）などを介してＰＣ６０３に直接的に接続され、ＰＣ６０３はインターネット６０４を介してカード発行銀行６０１に接続されている。銀行カード６０９を用いて電子取引を行う前に、前記図２、図３、図４を参照した説明に従い、それぞれ初期化工程、ログイン工程及び登録工程を実行する。そして、カード所有者によりＰＢＤ５０１を介して指紋データが入力されると、ＰＢＤ５０１は、入力された指紋データをＰＢＤ５０１の生体特徴データメモリに記憶されている指紋データと比較して、所定の時間（通常は数十秒）内にマッチングができない場合には、例えば「無効な指紋」などのエラー情報をＰＢＤ５０１のディスプレイ５０７に表示し、所定の時間内にマッチングができた場合は、動的ＰＩＮアルゴリズムで動的ＰＩＮコードを生成し、この動的ＰＩＮコードをディスプレイ５０７に表示する。その後、カード所有者は、ディスプレイ５０７に表示されているＰＩＮコードを、例えばＡＴＭ６０７やＰＯＳ６０６、又は将来可能となった場合には携帯電話６０８の端末に、入力することができる。カード発行銀行６０１側の動的ＰＩＮ認証サーバ６０２は、カード所有者によって入力された動的ＰＩＮコードを認証することにより、取引についての認証を実現する。認証された場合には、通常の方式で権限を付与して取引を行い、認証されなかった場合には、取引要求を拒絶する。
【００５７】
通常の電子商取引方式を完全に表示するため、図６では、更にアクワイアラ６０５及び清算システム６１０（例えば、中国銀聯（China Unionpay））も表示されている。また、

電子バンキングと電子商取引という二つの基本的な電子取引方式も、例示の方式で図に表示されている。本発明ではその他の構成の動作形態については変更していないため、説明の簡略化を図り、これらに対する説明は適宜省略した。

【００５８】

図７は、認証サーバ６０２の内部構造を示すものである。図に示すように、認証サーバ６０２は、受信部７０１、データベース７０２、比較部７０３、識別コード生成部７０４、送信部７０５及びタイマ７０６を有する。

【００５９】

認証サーバ６０２の受信部７０１は、認証要求を受信した後、認証すべきＰＩＮコード及び関連の静的データを受信する。この静的データは、例えばユーザの口座情報、ローカル装置のＭＡＣアドレス及び／又はＰＩＮを生成するための鍵セットを含む、ローカル装置において該動的ＰＩＮコードを生成するのに必要な全部又は一部の静的データであってよい。動的ＰＩＮコードの生成に用いられる静的データのデータ量は非常に大きい可能性があり、すべて銀行の通信システムで伝送する場合、大量のリソースを占用することがあるだけでなく、情報が漏れやすくなる。よって、例えば磁気カードに記録されている口座番号など、必要な静的データだけを受信するようにしてよい。動的ＰＩＮコードを生成するためのその他の付加的な静的データは、認証サーバ６０２のデータベース７０２に予め記憶しておくことができる。データベース７０２に記憶されている付加的な静的データは、口座番号と一対一で対応付けられており、受信された口座番号に基づいて対応する付加的な静的データを検索することができる。識別コード生成装置７０４は、受信された口座番号など静的データ、データベース７０２から検索された付加的な静的データ及びタイマ７０６からの現在時間に基づいて、ローカル装置と同じ動的ＰＩＮアルゴリズムで、現在の動的ＰＩＮコードを算出する。比較部７０３により、識別コード生成部７０４で生成された動的ＰＩＮコードと、受信部７０１で受信されたＰＩＮコードとが比較され、二つのＰＩＮコードが互いにマッチする場合、送信部７０５は権限を付与する旨の情報を送出し、マッチしない場合、送信部７０５は権限付与を拒絶する旨の情報を送出する。

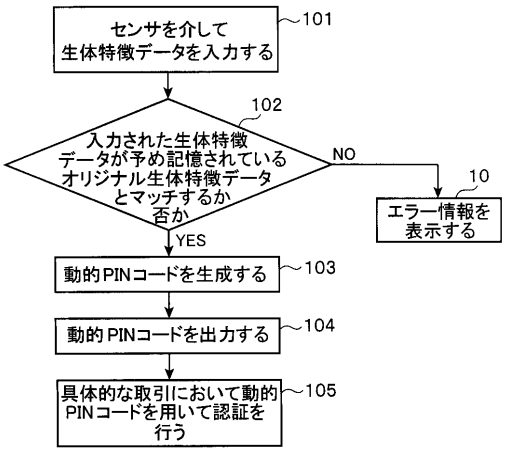
【００６０】

以上のとおり、本発明による動的ＰＩＮコード生成装置によれば、ユーザは、例えばＡＴＭで現金を引き出し、ＰＯＳ機にてカードで支払いをするなどの取引を行う場合、ＰＩＮコードを動的に生成して認証を行うことができるため、ＰＩＮコードを忘れるという心配がなくなる。また、生成されるＰＩＮコードの有効期限は非常に短く、毎回の取引を完成させるに足りる程度でしかないため、他人に盗用される心配もなくなる。本発明による動的ＰＩＮコード生成装置は、クレジットカード大の携帯装置とすることができ、又は携帯電話、ＰＤＡなど携帯可能な携帯装置に集成してもよい。また、本発明による動的ＰＩＮコード生成装置は、生体特徴データのマッチングをしてから動的ＰＩＮコードを生成するため、この動的ＰＩＮコード生成装置が紛失又は盗み取られたとしても、他人は当該装置から動的ＰＩＮコードを入手することができず、従って相当の安全性が確保されている。また、動的ＰＩＮコード生成装置の内部に分解することを防ぐ自滅装置が設置されることにより、安全性が更に向上する。

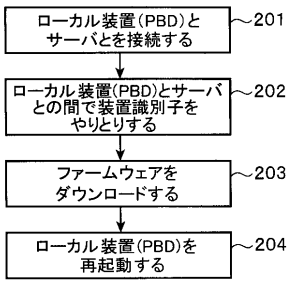
【００６１】

なお、以上では例示的な実施例を参照しながら本発明について説明したが、本発明は開示された例示的な実施例に限定して狭義に解釈されるべきものではなく、特許請求の範囲の請求項の範囲は種々変更して実施することができ、同等の構成及び機能が含まれるように最も広く解釈されるべきである。

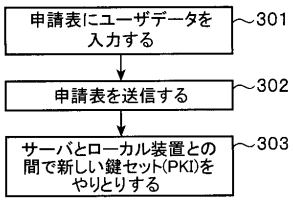
【図１】



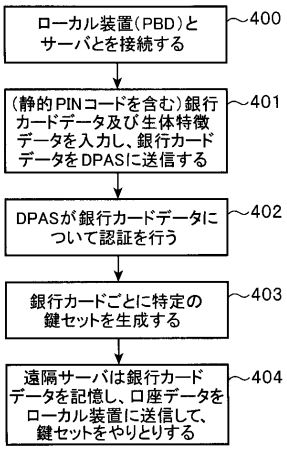
【図２】



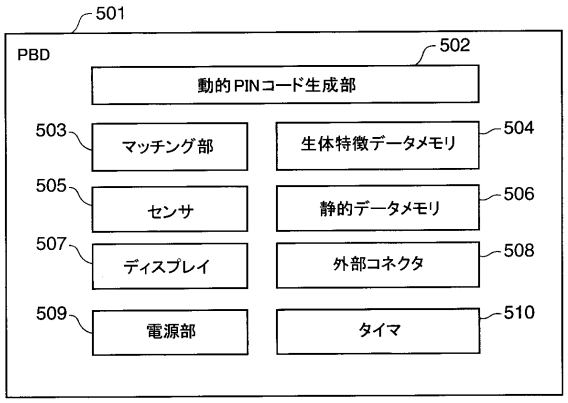
【図３】



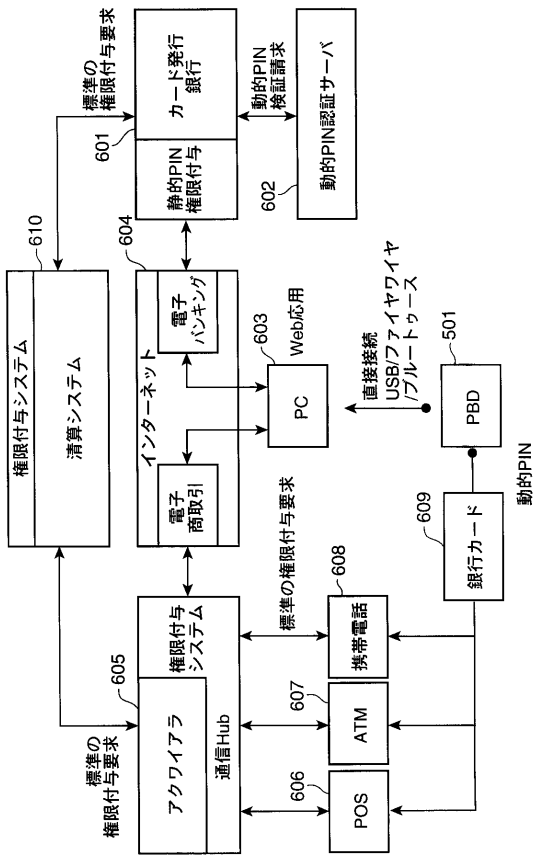
【図４】



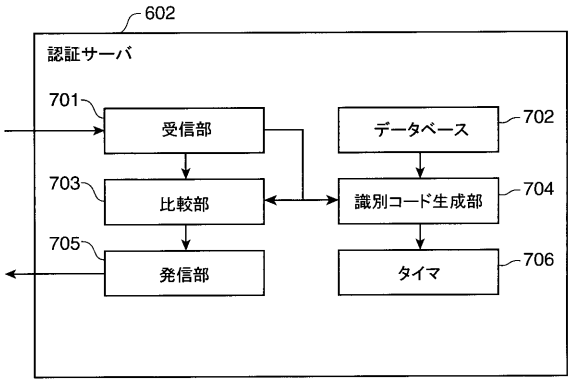
【図５】



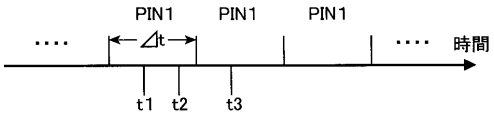
【図６】



【図７】


602
認証サーバ
701
受信部
データベース
702
703
比較部
識別コード生成部
704
705
発信部
タイマ
706

【図８】


PIN1
PIN1
PIN1
Δt
時間
t1
t2
t3

フロントページの続き

(72)発明者　ジャン　カソネ
中華人民共和国　ベイジン　１００７３８　ドンチェン　ディストリクト　イースト　チャン　アン　アヴェニュー　１　オリエンタル　プラザ　オフィス　タワー　Ｅ２　スイート　１８０９

審査官　岸野　徹

(56)参考文献　特開２００６－１５５５４７（ＪＰ，Ａ）
特開２００２－１３２７２８（ＪＰ，Ａ）
特開２００６－００４０２０（ＪＰ，Ａ）
特開２００６－１４４３５１（ＪＰ，Ａ）
特開２００２－３１８７８５（ＪＰ，Ａ）
特開２００２－２９７５４２（ＪＰ，Ａ）
特開２００３－００６１６８（ＪＰ，Ａ）
特開２００５－２３４８８２（ＪＰ，Ａ）
特開２００５－１４８９８２（ＪＰ，Ａ）
特開２００５－０８５０９０（ＪＰ，Ａ）
特開２００５－０１０８５６（ＪＰ，Ａ）
特開２００５－２０９０８３（ＪＰ，Ａ）
特開２００１－０６７３９９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３２
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／３４
Ｈ０４Ｌ　９／３２