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

特許第4596885号
(P4596885)

(45)発行日　平成22年12月15日(2010.12.15)　(24)登録日　平成22年10月1日(2010.10.1)

(51)Int.Cl.　　F I
G06K 17/00 (2006.01)　　G06K 17/00　V
G06F 21/20 (2006.01)　　G06F 15/00　330F

請求項の数 7　(全 10 頁)

(21)出願番号　特願2004-314998(P2004-314998)
(22)出願日　平成16年10月29日(2004.10.29)
(65)公開番号　特開2006-127178(P2006-127178A)
(43)公開日　平成18年5月18日(2006.5.18)
審査請求日　平成19年3月19日(2007.3.19)

(73)特許権者　504373093
日立オムロンターミナルソリューションズ株式会社
東京都品川区大崎一丁目６番３号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　山村　和寿
東京都品川区大崎一丁目６番３号　日立オムロンターミナルソリューションズ株式会社内
(72)発明者　伊藤　忠宏
東京都品川区大崎一丁目６番３号　日立オムロンターミナルソリューションズ株式会社内

最終頁に続く

(54)【発明の名称】生体認証システム

(57)【特許請求の範囲】
【請求項１】
生体情報を読み取る生体情報読取部と、
予め取得した第１の生体情報を記憶する記憶部と、
帳票の画像を読み取る画像読取部と、
前記第１の生体情報と、前記生体情報読取部で読み取った第２の生体情報と、を照合し、認証可であると判定したときに、所定の取引条件下で複数回の取引を実行する制御部と、を有し、
前記所定の取引条件は、前記画像読取部で読み取った帳票の画像の種類又は数に基づき、決まることを特徴とする生体認証システム。
【請求項２】
前記所定の取引条件として、２回以上の所定の取引回数以内で取引実行を許可することを特徴とする請求項１の生体認証システム。
【請求項３】
請求項２記載の生体認証システムであって
顧客又はオペレータからの入力を受ける入力部を有し、
前記所定の取引回数は、前記入力部からの入力に基づき、設定されることを特徴とする生体認証システム。
【請求項４】
請求項２記載の生体認証システムであって、

オペレータへの情報を出力する出力部を有し、
取引した回数が前記所定の取引回数を満たしていないときに、一連の取引の終了が指示された場合、前記出力部は取引回数が残っていることを出力することを特徴とする生体認証システム。
【請求項５】
請求項２記載の生体認証システムであって、
オペレータへの情報を出力する出力部を有し、
前記所定の取引回数を超えて取引を実行しようとしたとき、前記出力部は前記生体情報読取部で生体情報を再度読み取らせるよう促すことを出力することを特徴とする生体認証システム。
【請求項６】
請求項１記載の生体認証システムであって、
顧客のカードを保持するカード部を有し、
前記所定の取引条件下で複数回の取引を実行するとき、前記制御部は、ある取引を行っている間、前記カード部におけるカードの有無を監視することを特徴とする生体認証システム。
【請求項７】
請求項１記載の生体認証システムであって、
顧客の所在を検出する検出部を有し、
前記検出部で顧客の所在を検出しない場合は、取引実行を許可しないことを特徴とする生体認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
技術分野は、顧客の生体情報を用いて個人認証を行う生体認証システムに関する。
【背景技術】
【０００２】
近年、例えば、金融機関において、特に高額出金等の取引をする際に、セキュリティレベルの高い個人認証の仕組みが要求されつつある。
【０００３】
個人認証の仕組としては、例えば特許文献１は、予め各個人の持つ印鑑の印影データをサーバに登録しておき、取引毎に顧客が記入する帳票に押された印鑑の印影と、サーバに登録された印影データを照合する技術を開示している。
【０００４】
また、特許文献２は、予め各個人の生体情報を登録しておき、取引毎に個人の生体情報とサーバに登録された生体情報を照合することにより個人認証を行うシステムを開示している。
【０００５】
【特許文献１】特開平８－３３９４４２号公報
【特許文献２】特開２００４－１５２０４６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
特許文献１のように印影を照合することにより個人認証を行うシステムでは、取引毎に帳票に必要事項を記入し押印されているため、帳票を預かって印影のデータを取得し照合することができる。しかし、印影の偽造事件も発生しており、特に高額取引等の場面においてはより高いセキュリティを要求されつつある。
【０００７】
一方、特許文献２のように個人の生体情報を照合することにより個人認証を行うシステムは、偽造防止の面からセキュリティは比較的高いと言えるものの、生体情報である故に

分離が効かない。そのため例えば、複数取引分の用紙にそれぞれ印鑑で押印してテラーに預け、ロビーで待つといった運用ができない課題がある。

【０００８】

また、単純に生体情報を一度認証することで、連続する取引にその認証結果を反映できるとすれば、一つの取引を重複して処理する手違いが生じることや、顧客の要求しない取引にテラーが認証結果を用いることができてしまう等の課題がある。顧客にとっても安心してロビーで待てない等との課題が生じる懸念もある。

【課題を解決するための手段】

【０００９】

上記の課題のいくつかの改善は、例えば以下の手段によって、達成される。

【００１０】

生体情報を読み取る生体情報読取部と、生体情報読取部で読み取った生体情報を記憶する記憶部と、記憶部の生体情報による認証可のとき、所定の制限下で取引を実行する制御部とを有する生体認証システム。

【発明の効果】

【００１１】

例えば、生体情報を照合することによる個人認証を伴う連続取引において、取引毎に生体情報の読取を求めることをやめて、顧客の負担を軽減できる。また、例えば、オペレータのミスや不正等を防止することや顧客に安心感を与えることが期待できる。

【発明を実施するための最良の形態】

【００１２】

本実施形態では、生体情報を照合することによる個人認証を伴う連続取引において、最初の取引時に認証した結果を保持し、次取引ではその認証結果に基づき取引を行う。認証結果として保持する情報は、例えば、成功／失敗や生体情報の整合度等である。整合度を保持する場合は、整合度により取引条件（高額取引不可等）を設ける等の使い方ができる。このように認証した結果を保持し、取引の可否や条件等を引き継ぐことにより、取引の都度認証を行う顧客負荷を軽減できる。一取引とは、例えば出金取引において、帳票一枚（又は一式）によって処理する単位や、通帳に一項目として記載される単位を意味する。一連の取引とは顧客によってまとめて持ち込まれた複数の取引（出金や貸出等複数種の取引を含んでいても良い）を意味する。また、保持する認証結果を用いる所定の制限を設定し、所定の制限を満たす（有効な）場合のみ結果を引き継ぐ。所定の制限とは、例えば、帳票の枚数による取引回数制限、タイマ設定による時間制限、顧客保持媒体に埋め込んだチップ等により顧客の位置(店内にいる間有効)等である。このように認証結果に有効期限を設定することにより、オペレータのミスや不正を防止することや顧客に安心感を与えること等が期待できる。

【実施例１】

【００１３】

＜ＩＣカードに生体情報を保持する例＞

図３は、ＩＣカード３００に生体情報を保持する場合の端末１００と、生体認証装置２００の構成を示すブロック図の例である。ＩＣカード３００に生体情報を記憶しておくことで、顧客の個人情報を顧客自身が所有することにより、金融機関等からの個人情報の漏洩を防止することができる。端末１００は、ＣＰＵ（制御部）１１０、メモリ１２０、オペレータからの入力を受け付ける入力部１３０、帳票の画像を読み取るスキャナ等の画像読取部１３５、取引内容を表示するディスプレイ１４０、生体認証プログラム１５１を保持するハードディスク１５０を含む。生体認証装置２００は、制御部２１０、メモリ２２０、生体情報を読み取るセンサ部２６０、ＩＣカードの読み書きを行うＩＣカードＲ／Ｗ部２７０を含み、端末１００に有線又は／無線の回線を介して接続される。ＩＣカード３００は、制御部３１０、メモリ３２０を含み、生体情報及びその付随情報を記憶する。ＩＣカードＲ／Ｗ部２７０は、挿入された又は置かれたカードを保持する機構を有する。保持する機構は、容易に盗まれないよう覆う又は固定できることが望ましい。ＣＰＵ１１０

、制御部２１０、制御部３１０のいずれかを含む総称として制御部とも言う。また、メモリ１２０、メモリ２２０、メモリ３２０、ハードディスク１５０のいずれかを含む総称として記憶部とも言う。

【００１４】

図５は、生体情報及び付随情報としてＩＣカードやサーバに保持するデータの一例を示す。口座情報項目６００は、顧客の口座番号と顧客の氏名とを含む。指情報６１０は、顧客の指の静脈データと指の種類と本数を含む登録本数と各指の優先順位とを含む。登録情報６２０は、指情報を登録したときのオペレータの情報と装置の情報とホストの情報とを含む。本人確認資料項目６３０は、指情報を登録したときにともに登録した又は提示した印鑑、免許証、パスポート、保険証の有無を示す情報を含む（有りの場合は画像も含まれていて良い）。

【００１５】

図６は、複数回の取引実行を許可する所定の制限としてメモリに保持する情報の一例を示す。口座番号項目７１０には「１２３４５６」が、カウンタ項目７２０には「５（回）」が、タイマ項目７３０には「３００（秒）」が、所在項目７４０には顧客の所在が監視されるエリア（例えば営業店内）であることを示す「監視エリア内」が記憶されている。

【００１６】

図７は、ディスプレイ１４０に表示する画面例を示す。画面９０１は、ＩＣカードＲ／Ｗ部へのカード挿入を促す画面である。カードを置くだけで読取れる形態の場合にはカードをかざしてください、等のメッセージとなる。画面例９０２は、カードから読み取った情報に基づいて顧客情報を表示する画面であり、口座番号と氏名とを表示している。また、図５の指情報項目に基づいて顧客にセットしてもらう手（右手又は左手）と指（親指、人差指等）を指定している。本人確認キーは、顧客が指をセットした場合に選択するものであるが、指をセットしたことを自動的に検知することで選択を不要にできる。

【００１７】

画面９０３は、認証後に取引を実行しているときの画面であり、図６のカウンタ項目７２０に基づいて、許可された取引回数をカウントダウンする様子を示している。カウントアップでも良い。完了キーは取引が終了したときに選択する。画面９０４は、一取引が完了したときの画面であり、「次の取引」キーは連続して次の取引を実行する場合に選択し、「完了」キーは一連の取引を終える場合に選択する。

【００１８】

画面９０５は、一連の取引が終了したときにＩＣカードを顧客に返却させる画面であり、特に画面９０１で挿入させたＩＣカードの引抜を促している。画面９０６は、認証ＮＧのときの画面であり、身分証明書による認証を促している。オペレータが確認し認証可とした場合に「ＯＫ」キーを選択し、認証不可と判断した場合に「ＮＧ」キーを選択する。画面９０７は、エラーのときの画面であり、特に本人認証不可のときの画面である。画面９０８は、エラーのときの画面であり、特にＩＣカードの読み取りを実行したが、ＩＣカードをＩＣカードＲ／Ｗ部で読取れなかったことを示している。

【００１９】

画面９０９は、エラーのときの画面であり、特に図６のカウンタ７２０に設定された残りカウンタ数を超えて取引を実行しようとしたことを示している。また、再度の認証の実行を促している。画面９１０は、エラーのときの画面であり、特に図６のカウンタ７２０に設定された残りカウンタがゼロにならないうちに一連の取引を終了しようとしていることを示しており、オペレータにミスがないか確認を求めている。

【００２０】

図１と図２は、図３において、端末１００のＣＰＵ１１０や生体認証装置２００の制御部２１０が実行する処理の一例を示すフローチャートである。以下、生体情報として指静脈情報を例に挙げて説明する。

【００２１】

ＣＰＵ１１０は、画像読取部１３５を用いて、オペレータのセットした帳票の読取を順

に実行し、帳票の画像を入力するとともに、読み取った帳票の枚数をメモリ１２０に記憶された図５のカウンタ７２０に設定する（ステップ５００）。帳票枚数を記憶することにより、わざわざオペレータが数えなくとも、例えば、後述する認証結果の利用回数を帳票枚数分の取引回数に制限することができる。この設定は、読み取った画像から帳票の種類を識別し、一取引に該当する一式の帳票当りにカウンタ１回を設定することが望ましい。帳票ではない画像を読み取った場合にカウンタが設定されることを防止でき、また、一取引に対して複数枚の帳票が一式として対応することも考えられるからである。画像読取部１３５で読み取った画像の数に基づいて設定する（複数枚の帳票が一式としてあれば手入力で修正可とする）等の変更も可能である。また、カウンタを設定する契機としては、連続取引読み込み開始ボタン等が選択された後、連続取引読み込み終了ボタンが選択されるまでとしても良い。読み込んだ画像により、記載漏れがないか、等の形式点検等も実行する。

【００２２】

帳票の読取を終えると、端末１００のＣＰＵ１１０は、ディスプレイ１５０に画面９０１を表示し（ステップ５０１）、ＩＣカード３００を生体認証装置２００のＩＣカードＲ／Ｗ部２７０への挿入をオペレータ又は顧客に促す。生体認証装置２００の制御部２１０は、ＩＣカードＲ／Ｗ部２７０にセットされたＩＣカード３００から生体情報を読み取り、メモリ２２０に記憶する（ステップ５０２）。ここでメモリ１２０ではなく、メモリ２２０に記憶することで、顧客のＩＣカード３００の情報を生体認証装置２００内に留めることができ、情報漏洩を防ぐことができ良い。帳票の読取にも多少の時間を要することを鑑みて、ステップ５００が終了する前にステップ５０１を実行するようにすることも良い。

【００２３】

ＩＣカードの読取を終えると、ＣＰＵ１１０は、ディスプレイ１５０に画面９０２のように口座情報６００と、予め登録された指情報６１０の優先順位に従ってセットする指の種類を表示する（ステップ５０３）。このように、指静脈の情報を複数本の指について登録しておくことで、指を怪我した等の場合に対応できる。優先順位をつけておくことで、指認証処理の遅延を防止し、また、オペレータが意識せずに顧客が選んだ使い易い指をセットするよう誘導することができる。顧客が指をセットしたことを検知又は画面９０２の本人確認キーを選択すると、生体認証装置２００の制御部２１０は、センサ部２６０にセットされた顧客の生体情報を読み取り、メモリ２２０に記憶する（ステップ５０４）。

【００２４】

生体認証装置２００の制御部２１０は、メモリ２２０に記憶した２種の生体情報（ＩＣカード３００から読み取った情報と、センサ部２６０で顧客の指から読み取った情報）を照合する（ステップ５０６）。

【００２５】

もし不一致ならば、ＣＰＵ１１０は、ディスプレイ１５０に画面９０６を表示する。ここでは、オペレータから身分証明書の提示を要求し、本人確認を続行している。画面９０６のＯＫキーが選択されたことを検知すると、認証可とする（ステップ５３２でＹｅｓ）。このように、照合が失敗した場合でも身分証明書の確認等により取引を行えるようにすることで、怪我等により生体認証できない場合にも取引を行うことができる。生体認証が不可の時点で取引を終了しても良いし、他の生態情報による認証や暗証番号の入力を求めるようにしても良い（身分証明書の提示と組み合わせても良い）。身分証明書の確認がＮＧであれば（ステップ５３２でＮＧ）、ＣＰＵ１１０は、ディスプレイ１５０に画面９０７を表示し（ステップ５３３）、メモリ１２０のカウンタをリセットし、制御部２１０はメモリ２２０から生体情報を破棄して（ステップ５３４）取引を終了する。

【００２６】

ステップ５０６又はステップ５３２で認証可とされると、制御部２１０は、メモリ２２０から生体情報を破棄する（ステップ５０８）。認証可とされると、ＣＰＵ１１０は、ディスプレイ１５０に画面９０３を表示し、取引を開始する（ステップ５１２）。

【００２７】
画面９０３に表示している取引残り回数は、メモリ１２０に記憶されているカウンタの値である。取引を行っている間、生体認証装置２００の制御部２１０は、ＩＣカードＲ／Ｗ部２７０にＩＣカードがセットされたままになっているかを監視する（ステップ５１４）。もしＩＣカードが抜き取られた場合は、ＣＰＵ１１０がディスプレイ１５０に画面９０８を表示し（ステップ５３５）、メモリ１２０からカウンタを破棄して（ステップ５３６）取引を中止する。このようにＩＣカードが抜き取られていないことをチェックすることにより、顧客にＩＣカードを返却した後に不正取引を行ったり、誤った取引を行ったりすることを防止することができる。ここで、監視するだけでなく、取引毎にＩＣカードから生体情報を読み出して、ステップ５０４で読み取った生体情報と認証するようにすると認証実行の手間がかかるが、ＩＣカードが本物であることを確認できるので良い。
【００２８】
一つの取引を終えると（ステップ５１６）、端末１００のＣＰＵ１１０はメモリ１２０に記憶しているカウンタ７２０から‘１’減算して（ステップ５１８）、ディスプレイ１５０に画面９０４を表示する（ステップ５１９）。
【００２９】
ステップ５１９で、オペレータにより「次の取引」ボタンが押されたら、端末１００のＣＰＵ１１０は、メモリ１２０に記憶されているカウンタ７２０をチェックし（ステップ５２２）、カウンタ７２０が０でなければ、次の取引を開始する。カウンタ７２０が０であれば、ディスプレイ１５０に画面９０９を表示し（ステップ５２３）、一旦取引を終了するためステップ５２６へ進む。カウントアップの場合には、カウントが所定の値になったかをチェックする。ゼロを含む所定の値になったことを、カウンタを満たす、所定の値になっていないことを、カウンタを満たしていないとも表現する。
【００３０】
ステップ５１９で、オペレータにより「完了」ボタンが押されると、ＣＰＵ１１０は、メモリ１２０に記憶されているカウンタ７２０をチェックし（ステップ５２４）、カウンタ７２０が０であればステップ５２６へ進む。カウンタ７２０が０でなければ、ディスプレイ１５０に画面９１０を表示して注意を促す（ステップ５２５）。取引結果に異常がなければステップ５２６へ進む。このようにカウンタ７２０と実際の取引回数を比較することにより不正取引や取引の漏れ等のミスを防止することができる。
【００３１】
全ての取引が終了したら、ＣＰＵ１１０は、メモリ１２０からカウンタを破棄し（ステップ５２６）、ディスプレイ１５０に画面９０５を表示する（ステップ５２７）。生体認証装置２００の制御部２１０は、ＩＣカードＲ／Ｗ部２７０からＩＣカードが抜き取られたことを端末１００に通知し、ＣＰＵ１１０は取引を終了する（ステップ５３０）。
【実施例２】
【００３２】
＜サーバに生体情報を保持する例＞
以上、顧客のＩＣカードに生体情報を記憶している例を説明した。一方、サーバに生体情報を保持することにより、ネットワークからの情報漏洩を防ぐセキュリティ対策が求められるが、ＩＣカードを発行するコストを抑えることができる。
【００３３】
図４は、サーバに生体情報を記憶する場合のサーバと端末装置と生体認証装置の構成を示すブロック図の例を示す。サーバ４００は、ＣＰＵ４１０、メモリ４２０、生体情報及びその付随情報を登録する生体認証ＤＢ４５３、生体認証ＤＢ４５３を制御するＤＢプログラム４５２を記憶するハードディスク４５０、端末１００との通信を行う通信部４８０を有する。端末１００は、図３に比べて、サーバ４００との通信を行う通信部１８０を有する。
【００３４】
各部の動作について、実施例１との相違点を説明する。ステップ５０２において端末１

００のＣＰＵ１１０は、通信処理部１８０を用いてサーバ４００にアクセスする。サーバ４００のＣＰＵ４１０は、ＤＢプログラム４５１を実行し、生体情報ＤＢ４５２から生体情報を取得し、通信部４８０を用いて端末１００に読み取った生体情報を送信する。ＣＰＵ１１０は受信した生体情報を生体認証装置２００に渡し、生体認証装置２００の制御部２１０がメモリ２２０に生体情報を記憶する。

【００３５】

本実施例２では、ＩＣカードを使用しないため、ＩＣカード監視（ステップ５１４）、ＩＣカード抜き取り（ステップ５３０）の手順は行わない。他の動作は実施例１に従う。

【実施例３】

【００３６】

＜実施例１及び／又は２についてのそれぞれの変形例等＞

上述では、照合する生体情報を生体認証装置２００のメモリ２２０に一時的に記憶して制御部２１０で認証する場合を例にとったが、他にも以下のような方法で認証が可能である。

【００３７】

実施例１において、生体認証装置２００のセンサ部２６０より取得した生体情報をＩＣカード３００のメモリ３２０に保持して認証することができる。これによると、処理速度はやや劣るが、登録されている生体情報をＩＣカードの外に出さずに認証できるため、より強固なセキュリティを得ることができる。また、生体認証装置２００のセンサ部２６０より取得した生体情報とＩＣカードＲ／Ｗ部２７０より取得するＩＣカードに登録された生体情報をともに端末１００のメモリ１２０に保持して認証する方法をとることができる。これによると、装置間の通信に高いセキュリティが要求されるが、端末１２０のＣＰＵ１１０を用いることができるため認証処理自体の速度を向上することができる。

【００３８】

実施例２において、生体認証装置２００のセンサ部２６０より取得した生体情報とサーバ４００の生体情報ＤＢ４５２に登録されている生体情報をともに端末１００のメモリ１２０に保持して認証することができる。これによると、ネットワーク、装置間通信の暗号化等の高いセキュリティが要求されるが、端末１２０のＣＰＵ１１０を用いることができるため認証処理自体の処理速度を向上することができる。また、生体認証装置２００のセンサ部２６０より取得した生体情報をサーバに送信してサーバで認証する方法もあるが、ネットワーク、装置間の通信で情報をケアすることが求められる。

【００３９】

上記の実施形態においては、認証結果の有効期限として帳票の画像を読み取る際に帳票枚数を自動的にカウンタ７２０で記憶してカウントダウンする方法を例にとったが、他にも、受付用の端末等から顧客自身が入力した取引数を端末１００に送信しメモリ１２０のカウンタ７２０に記憶する方法、オペレータが枚数を数えてカウンタに入力する方法（この場合、オペレータの不正を防止するために顧客と同意の取引回数を入力することが望ましい）、認証時にタイマ７３０をセットし、所定時間が計測されるまでは有効とする方法、顧客にチップを埋め込んだ受付証等を発行して所在を検出するセンサ等の検出部を例えば店内に設置し顧客が店舗内やロビーにいることを検知しているときは認証を有効とする方法等がある。セキュリティポリシーに応じた制限を設けることにより、不正取引を防止して強固なセキュリティを得ることができる。

【００４０】

本実施例は、以下の形態も含む。

（１）予め取得した各個人の生体情報を保持し、取引開始時に個人の生体情報を読み取り、保持された生体情報を読み取り、二つの生体情報を照合し、照合の結果を複数取引の間保持し、取引毎の認証を免除する個人認証方式。

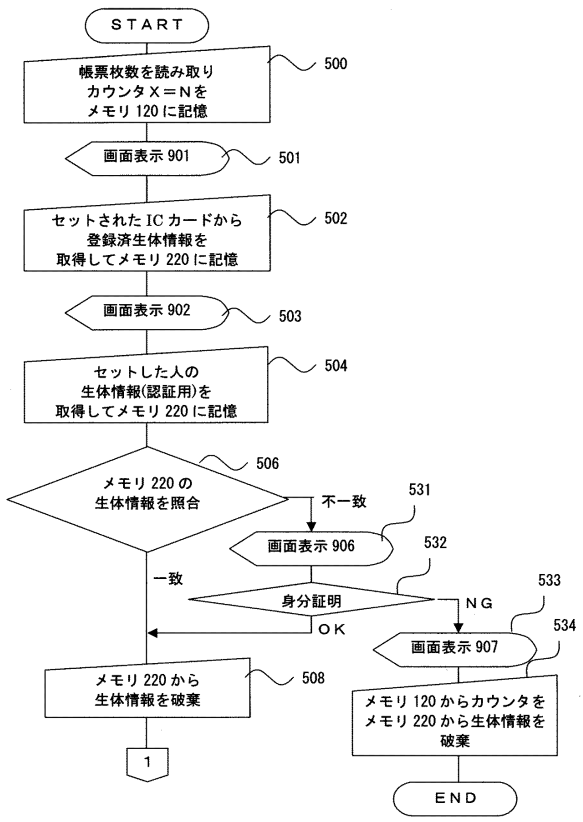
（２）取引開始時に認証の有効期限を設定し、有効期限を判定して有効である間は認証を免除し、有効期限を超えた取引を行う場合は改めて認証を行う個人認証方式。

（３）予め取得した各個人の生体情報を保持する手段と、保持された生体情報を読み取る

手段と、個人の生体情報を読み取る手段と、二つの生体情報を照合する手段と、照合の結果を保持する手段と、を有する個人認証装置及び取引端末。
（４）認証の有効期限を設定する手段と、有効期限を判定して有効である間は認証を免除し、有効期限を超えた取引を行う場合は改めて認証を行う手段と、を有する個人認証装置及び取引端末。
【００４１】
以上、一実施形態を具体的に説明したが、この具体例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。
【図面の簡単な説明】
【００４２】
【図１】処理手順を示すフローチャートの例（１）。
【図２】処理手順を示すフローチャートの例（２）。
【図３】ICカードに生体情報を保持する場合のシステムブロック図の例。
【図４】サーバに生体情報を保持する場合のシステムブロック図の例。
【図５】ICカードやサーバ等に保持する生体情報のデータテーブルの例。
【図６】メモリに保持する有効期限情報の例。
【図７】画面表示例。
【符号の説明】
【００４３】
１００　端末
２００　生体認証装置
３００　ＩＣカード
４００　サーバ

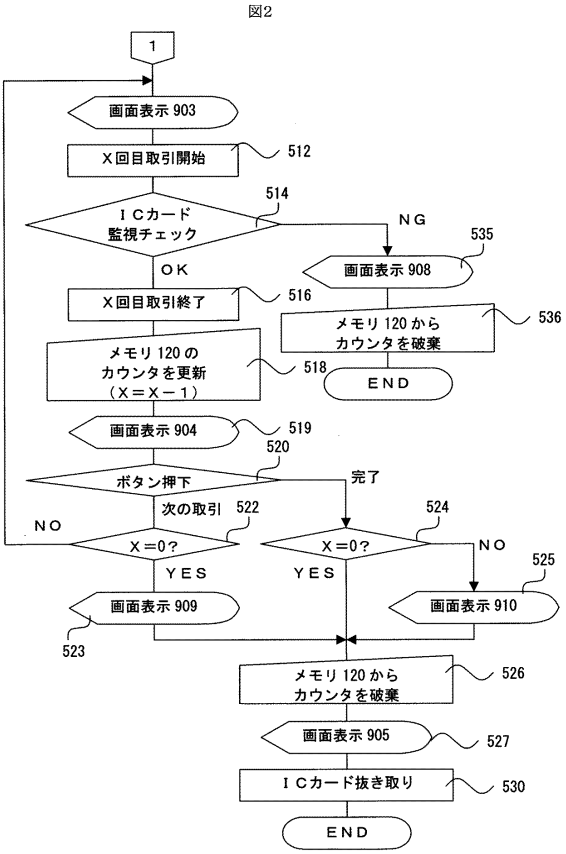
【図１】

図1



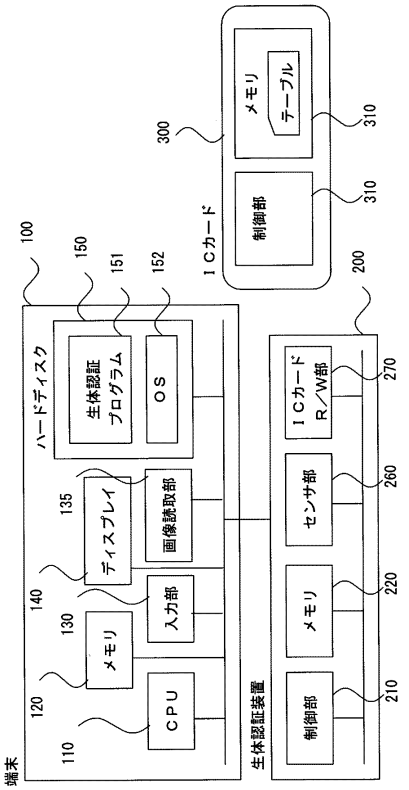
【図２】

図2



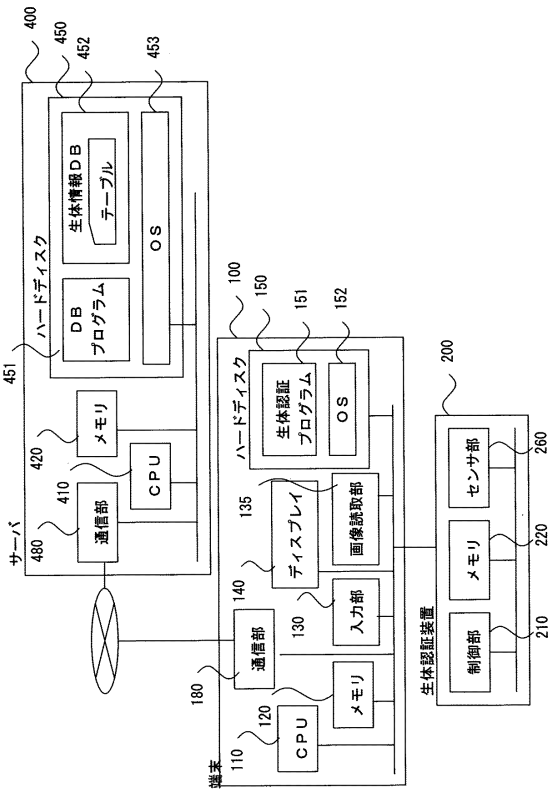
【図３】

図3



【図４】

図4



【図５】

図5

600	口座情報	口座番号
		氏名
610	指情報	静脈データ
		登録本数
		優先順位
620	登録情報	オペレータ情報
		装置情報
		ホスト情報
630	本人確認資料	印鑑の有無
		免許証の有無
		パスポートの有無
		保険証の有無

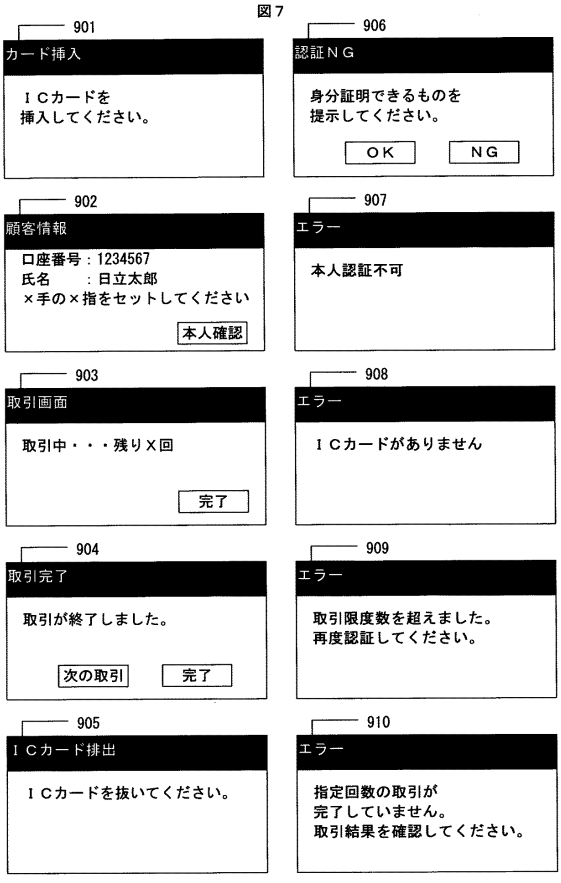
【図６】

図6

710	口座番号	１２３４５６
720	カウンタ	５(回)
730	タイマ	３００(秒)
740	所在	監視エリア内

【図７】

図7



フロントページの続き

審査官　大塚　良平

(56)参考文献　特開平１０－０６３７２１（ＪＰ，Ａ）
特開２００４－１５２０４６（ＪＰ，Ａ）
特開２００２－１３３３３２（ＪＰ，Ａ）
特開２００２－１６９７８２（ＪＰ，Ａ）
特開平１１－０７６５７９（ＪＰ，Ａ）
特開平１０－１５４１３１（ＪＰ，Ａ）
特開平１１－２７２６１３（ＪＰ，Ａ）
特開昭６２－９２０９４（ＪＰ，Ａ）
特開２００４－２４６７５７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｋ　１７／００
Ｇ０６Ｆ　１５／００