

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4500834号
(P4500834)

(45) 発行日 平成22年7月14日 (2010. 7. 14)

(24) 登録日 平成22年4月23日 (2010. 4. 23)

(51) Int. Cl.	F I
G 0 7 D 9/00 (2006. 01)	G O 7 D 9/00 4 6 1 A
G 0 7 D 13/00 (2006. 01)	G O 7 D 9/00 3 2 1 C
G 0 7 F 19/00 (2006. 01)	G O 6 K 17/00 L
G O 6 K 17/00 (2006. 01)	G O 6 K 17/00 V
G O 6 K 19/10 (2006. 01)	G O 6 K 19/00 S

請求項の数 8 (全 21 頁) 最終頁に続く

(21) 出願番号	特願2007-186449 (P2007-186449)	(73) 特許権者	504373093
(22) 出願日	平成19年7月18日 (2007. 7. 18)		日立オムロンターミナルソリューションズ株式会社
(62) 分割の表示	特願2005-303838 (P2005-303838) の分割		東京都品川区大崎一丁目6番3号
原出願日	平成17年10月19日 (2005. 10. 19)	(74) 代理人	100100310
(65) 公開番号	特開2008-4104 (P2008-4104A)		弁理士 井上 学
(43) 公開日	平成20年1月10日 (2008. 1. 10)	(72) 発明者	今井 啓允
審査請求日	平成19年7月18日 (2007. 7. 18)		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
審判番号	不服2008-25813 (P2008-25813/J1)		社内
審判請求日	平成20年10月8日 (2008. 10. 8)	(72) 発明者	佐川 大介
			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
			社内

最終頁に続く

(54) 【発明の名称】 ICカード内認証システム

(57) 【特許請求の範囲】

【請求項1】

現金の取引を自動的に行う現金自動取引装置において、

ICカードの情報を読み取るカード機構部と、前記現金自動取引装置を利用する利用者の生体特徴量を取得する生体認証機構部と、制御部とを有し、

前記制御部は、第1の生体情報から得られ、個人を特定不可能な情報であってかつICカード内に予め格納されている情報である前処理データを前記カード機構部から受信し、受信した前記前処理データを前記生体認証機構部に送信し、

前記生体認証機構部に対し、前記生体認証機構部により取得された第2の生体情報と前記前処理データとを不可逆的に組み合わせ、逆変換により生体情報を作成できないデータである認証データを作成させ、

前記認証データを前記生体認証機構部から受信し、

受信した前記認証データを前記ICカードに送信し、

前記第1の生体情報と前記前処理データとを組み合わせ作成された情報であってかつ前記ICカード内に予め格納されている情報である登録データと前記認証データとを前記ICカード内で照合させ、

前記登録データと前記認証データとの認証の結果を示す認証結果データを前記ICカードから受信し、

受信した前記認証結果データを前記生体認証機構部に送信し、

前記生体認証機構部に対し、前記認証結果データに基づいて、認証した生体部位や失敗

10

20

した原因に関する情報を作成させ、

前記認証した生体部位や失敗した原因に関する情報を前記生体認証機構部から受信することを特徴とする現金自動取引装置。

【請求項 2】

請求項 1 記載の現金自動取引装置において、

前記生体認証機構部は、当該生体認証機構部に置かれた生体に対して光を照射する生体照射部と、前記生体照射部によって照射された前記生体の画像を取得する画像取得部とを有し、

前記画像取得部によって取得した前記生体特徴量と、前記 IC カードから前記制御部を介して受信した前記前処理データとから或るアルゴリズムに従って前記認証データを生成することを特徴とする現金自動取引装置。

10

【請求項 3】

請求項 2 記載の現金自動取引装置において、

前記制御部は、生体情報の認証処理を実行する認証制御ミドルを記憶し、記憶した前記認証制御ミドルから指示によって前記生体認証機構部で前記認証データを生成し、生成された前記認証データを前記 IC カードに送信することを特徴とする現金自動取引装置。

【請求項 4】

請求項 1 記載の現金自動取引装置において、

前記カード機構部は、前記 IC カードとの接続を確立すると共に前記 IC カードから生体認証におけるサポート情報を読み出して前記制御部に送信し、

20

前記制御部は、受信した前記サポート情報に基づき、IC カード内認証処理のときは前記認証処理を継続し、装置内認証処理のときは前記カード機構部から前記 IC カードを排出することを特徴とする現金自動取引装置。

【請求項 5】

請求項 1 記載の現金自動取引装置において、

前記制御部は、前記 IC カードによる認証処理に応答して利用者の選択した取引を実行し、前記認証処理の結果が失敗のとき前記 IC カードより受信した前記前処理データを再度、前記生体認証機構部に送信して再度の認証処理を実行することを特徴とする現金自動取引装置。

【請求項 6】

30

請求項 1 記載の現金自動取引装置において、

紙幣入出金を行う紙幣入出金部と、

利用者に操作内容を表示し、利用者からの入力を受け付ける操作部とを有し、

前記制御部は、前記操作部により利用者が希望する支払取引を受け付け、前記 IC カードによる認証処理に応答してその結果が成功であった場合に、前記紙幣入出金部から紙幣を出金することを特徴とする現金自動取引装置。

【請求項 7】

請求項 1 記載の現金自動取引装置において、

取引に関連の操作内容を表示し、利用者からの入力を検知する操作部を有し、

前記制御部は、前記操作部により利用者が希望する残高照会を検知し、前記 IC カードによる認証処理に応答してその結果が前記照会結果が成功であった場合に、前記操作部に預金又は借入残高を表示し、その後、前記操作部より認証を必要とする取引を受け付けると、前記 IC カードより受信し記憶した前記前処理データを前記生体認証機構部に再送信し、前記生体認証機構部から新たに入力された生体特徴量と再出力された前記前処理データとから認証データを生成することを特徴とする現金自動取引装置。

40

【請求項 8】

請求項 1 乃至 7 の何れかの項記載の現金自動取引装置において、

前記制御部は、前記前処理データを利用者が選択した取引終了まで一時記憶し、取引終了に起因して前記前処理データを削除処理することを特徴とする現金自動取引装置。

【発明の詳細な説明】

50

【技術分野】

【0001】

本発明は、現金自動預払装置（ＡＴＭ）などで使用される生体認証システムに関する。

【背景技術】

【0002】

従来、現金自動預払装置（ＡＴＭ）などで行われてきた生体認証システムには、以下のようなものがある。

【0003】

特許文献１には、生体識別情報内蔵型ＩＣカード及びその本人認証方法が記載されている。この技術はＩＣカードを用いた本人認証方法において、ＩＣカードに生体識別内情報を内蔵し、この生体識別情報と本人固有の生体情報識別情報とをＩＣカード内の生体識別照合処理部で処理し、本人認証を行うものである。

10

【0004】

特許文献２には、生体情報を用いた個人認証方法が記載されている。この技術は利用者から取得した生体情報を分割し、一方を電子カードに、他方をデータベースにそれぞれ格納し、認証の際、電子カード利用者から生体情報を取得し、前記電子カードからもう一方の生体情報を読み出し、その後、この一方の生体情報と関連する他方の生体情報が前記データベースに存在するか否かを検索し、存在するときはそれらの生体情報を結合して先に取得した電子カード利用者の生体情報と比較し、認証判定を行うものである。

20

【0005】

特許文献３には、携帯電子装置及び生体情報を用いた個人認証方法が記載されている。この技術は事前にＩＣカードなどの携帯電子装置に登録データ（生体情報の特徴量）を記憶しておき、ＩＣカード内で認証時に得る特徴データ（生体情報の特徴量）と登録データとを照合することで認証を実施するものである。

【0006】

【特許文献１】特開２０００－２１５２９４号公報

【特許文献２】特開２００５－１１５８００号公報

【特許文献３】特開平１０－３１２４５９号公報

【発明の開示】

【発明が解決しようとする課題】

30

【0007】

特許文献１では、生体情報を記憶したＩＣカード内で生体認証しているが、ＩＣカード内に生体情報をそのまま記憶しているので、ＩＣカードの盗難・紛失により生体情報が漏洩する可能性がある。

【0008】

特許文献２では、生体情報を電子カードとデータベースとの２つに分けて記憶（登録）し、認証時にそれら２つを結合しているが、データベースに多くの利用者のデータを記憶して管理を徹底する必要もあり、処理が煩雑である。

【0009】

特許文献３では、生体情報から生体特徴量を抽出し登録データとして記憶したＩＣカード内で認証時に新たに得た生体特徴量と登録データとを照合しを用いて生体認証しているが、生体特徴量を携帯電子装置（ＩＣカード）とデータ処理装置（ＩＣカードターミナル）との間で転送しているので、この転送過程で個人情報である生体特徴量が漏洩する可能性がある。

40

【0010】

本発明は、ＩＣカードを用いた生体認証システム及びその方法において、生体情報の高い秘匿性を実現することを目的とする。

【課題を解決するための手段】

【0011】

上記課題の解決のため、生体認証処理を携帯電子装置（ＩＣカード）内の認証プログラ

50

ムで行うＩＣカード内認証方式を実施する。本発明の生体認証制御方法は、生体情報から得られる前処理データを携帯電子装置から受信し、前記前処理データを生体認証機構部に送信し、前記生体認証機構部により取得された生体情報と前記前処理データとを組み合わせ作成する認証データを前記生体認証機構部から受信し、受信した前記認証データを前記携帯電子装置に送信し、前記携帯電子装置内に予め格納されている登録データと前記認証データとを、前記携帯電子装置内で照合させるように動作させるものである。

【発明の効果】

【００１２】

本発明はＩＣカード、認証装置に対してデータの転送、認証処理指示するために認証制御ソフトウェアを採用したことにより、セキュリティの高い生体認証方式を提供できる。さらに、認証制御ソフトウェアを構成する認証制御アプリケーションと認証制御ミドルウェアを異なる複数の認証方式に対応可能なものとして作成することにより、複数の認証に端末に複数の生体に対する認証装置が搭載されている場合に複数の認証装置の種々に対応した制御が可能になる。

10

【発明を実施するための最良の形態】

【００１３】

以下、本発明を用いた実施の一形態について説明する。

【実施例１】

【００１４】

本実施形態では、金融機関の営業店においてオペレータ（窓口担当者）と利用者間で、利用者が所有する携帯電子装置、特に、ＩＣカードへ利用者の生体情報（例、指静脈）を登録する生体情報登録処理と、金融機関、コンビニ等に設置され、主に現金にかかる取引を自動的に取引する現金自動取引装置、現金自動預払機（ＡＴＭ）を使用して利用者の生体情報を使用して認証する生体認証処理、との大きく２つに分けて説明する。図１～４にて生体情報登録処理を説明し、図５～１２にて生体認証処理を説明する。

20

【００１５】

最初に、生体情報の登録処理と、認証処理との概要を簡単に説明する。

【００１６】

生体情報登録処理では、利用者の指静脈から特徴量を抽出して前処理データと生成すると共に、登録データも生成してＩＣカードに登録する。この処理の過程で使用される窓口端末はＩＣカード装置付生体情報登録装置と接続されており、登録用の生体情報（前処理データ、登録データ）が暗号化されて、窓口端末を経由せずに生体情報登録装置からＩＣカードに直接転送、書き込みが実行される。

30

【００１７】

一方、生体認証処理では、利用者の指静脈からの特徴量と、ＩＣカードに登録された前処理データ、登録データとを特有の認証、照合技術に基づいてその処理を実行する。この処理の過程ではＡＴＭを中心として、ＡＴＭに接続された生体認証機構部により新たに取得した生体情報と、ＩＣカードから読み出した前処理データにより認証データを生成し、これをＩＣカードに転送してＩＣカード内にて認証処理を行う。

【００１８】

40

本発明の説明において、生体情報の登録処理は営業店システムを使用し、認証処理はＡＴＭを使用する態様で説明するが、営業店システムにおいても認証処理を、ＡＴＭにおいても登録処理を行う態様でも良い。但し、生体情報の登録処理は本人であることを確実にする上でも、オペレータが立ち会う営業店システムにおいて実行するのが望ましい。また、生体情報を登録しておく媒体としてＩＣカードを例に挙げるがこれに限らず、携帯電話やＲＦＩＤ（Radio-Frequency-Identification）タグなど、携帯可能な電子媒体（携帯電子装置）であっても良いが、現在、利用者に最も普及しているキャッシュカードにＩＣチップを搭載したＩＣカードが望ましく、システムの変更を抑えることができる。

【００１９】

図１は金融機関の営業店内においてオペレータが使用する営業店システムのうち、特に

50

生体情報の登録に係る生体情報登録処理システムを抜き出した概要図である。この生体情報登録システムは、生体情報読取装置102を備えた生体情報登録装置101と、この生体情報登録装置101を制御する登録用端末装置104とを接続して構成する。このシステムは金融機関のオペレータ（窓口担当者）が登録用端末装置104を操作して、ICカード105に利用者の生体情報を登録するものである。具体的には、操作部107を窓口担当者が操作し、表示部106に表示する種々のメニューより選択し、生体情報の登録の他、金融機関における様々な取引を可能とするものである。

【0020】

窓口担当者はICカード105を生体情報登録装置101の一構成であるICカード装置103に挿入し、ICカード105を書き込み可能な状態にする。一方、利用者は利用
10
者自らの指を図示する形状に沿って生体情報読取装置102に置く。窓口担当者の操作により、生体情報読取装置102は近赤外線を置かれた指に透過し、カメラにより指の静脈パターンを撮影し、その画像を得る。この画像から生体特徴量を抽出し、抽出した生体特徴量に後述する処理を加えてICカード装置103によってICカード105に記録、書き込みの処理を実行する。なお、生体特徴量は指の静脈データ（静脈パターン）から得た個人を特定できるデータである。

【0021】

ICカード装置103は、上述したとおりICカード105に情報を書き込む機能を有している他、ICカード105に記憶されている情報を読み取る機能も有している。すな
20
わち読取又は書込機能を有しているが、以下ではICカード105内に生体情報を書き込む例にて説明する。

【0022】

図2は図1で説明した生体情報登録処理システムの一実施例の構成を示すブロック図を示す。

【0023】

生体情報登録装置101は、生体情報登録装置101全体を制御するCPU201、様々な情報を記憶する主記憶部202、生体情報を読み取る生体情報読取装置102、IC
カード105に生体情報を書き込むICカード装置103、及び登録用端末装置104と接続する通信部215とにより構成される。

【0024】

主記憶部202は、各種プログラムを記憶するROM203と、主にデータを記憶し、記憶したデータの書き換えが可能なRAM204とに分けられる。ここでは、ROM203、RAM204による主記憶部（単に、記憶部とも言う）202として説明するが、それぞれハードディスク、種々の半導体メモリによる構成でも良い。ROM203は、生体情報の登録処理のための登録処理プログラム205、認証時に用いる登録データを作成するための登録データ作成プログラム206、生体情報読取装置102を制御するための生体
30
情報読取装置制御プログラム207、ICカード105へ情報の書き込み処理のためのICカード装置制御プログラム208、及び通信部215を制御するための通信制御プログラム209を備えている。

【0025】

生体情報読取装置102は、生体画像（指静脈パターン）を取得し、CCDカメラなどで構成される画像センサ（画像取得部）210、画像センサ210の画像取得可能領域に指が置かれたか否かを検知する生体有無検知用照明LED211、生体画像（指静脈パ
40
ターン）取得時に指に対し近赤外線を照射する生体取得用照明LED（生体照射部）212とを備えている。ICカード装置103は、ICカード105に情報を書き込むICカード書込部213、ICカード105と接続するための接点端子214を備えている。

【0026】

ICカード105は、ICカード105全体を制御するCPU221、生体情報に関連するデータや金融取引に係るプログラム等を記憶する記憶部222、生体情報登録装置1
50
01と接続するための接点端子223とを備えている。なお、ICカード装置103とI

Cカード105とを接点端子による接触式に限らず、非接触式でも構成できる。

【0027】

登録用端末装置104は、登録用端末装置104全体を制御するCPU231、データやプログラムを記憶する主記憶部232、CRTや液晶ディスプレイなどで構成され、操作案内を表示する表示部106、窓口担当者の入力操作を受け付けるキーボード、マウスなどで構成された操作部107、生体情報登録装置101と生体登録用端末装置104と接続する通信部235により構成される。そして、主記憶部232は、生体情報登録装置101を制御するための生体情報登録装置制御プログラム233の他、窓口にて取引される種々の金融取引用のプログラムを格納している。

【0028】

図3により生体情報登録処理でICカード105に登録する登録データの作成過程について説明する。但し、作成過程におけるアルゴリズム等の開示はセキュリティ上、即ち、情報漏洩等による偽造を防止する関係から、その説明を省略する。生体情報の認証処理でも同様である。

【0029】

最初に、画像センサ210により得られた生体画像（指静脈パターン）に基づき、あるアルゴリズムを用いてその特徴をあらわす生体特徴量を抽出する（ステップ301）。そしてこの生体特徴量から更にあるアルゴリズムを用いて前処理データを作成する。更に、生体特徴量と前処理データとを組み合わせる登録データを作成する（ステップ302）。

【0030】

ここで、前処理データというものは、登録データを作成するために用いられる暗号鍵、という解釈もできる。また、登録データは上述及び図から明らかなように、生体特徴量から直接作成することが不可能なデータである。また、前処理データと登録データは利用者自身の特徴を明確にあらわす生体特徴量から作成したデータであるが、この作成過程では不可逆変換処理によるアルゴリズムを用いられる。従って、逆変換による作成処理として、登録データから生体特徴量又は前処理データを作成すること、前処理データと登録データとの2つのデータから生体特徴量を作成することはできない。なお、前処理データは利用者個人を特定できない部分を抜き出して作成した情報で、登録データは個人を特定できる部分を抜き出して作成した情報である態様が望ましい。また、前処理データ、登録データ共に、カード保有者しか得られない特有な情報である。

【0031】

最後に、作成した前処理データと登録データとをICカード105に記憶する（ステップ303）。ICカード105に記憶されたこれらのデータは暗号化された状態で記憶され、更に上述したとおり、逆変換による作成処理が不可能な状態で記憶されている。よって、仮に前処理データ、登録データが悪意の者によって読み出され、且つ両データが解読されたとしても生体特徴量を生成することは不可能である。このように、データの暗号化、逆変換が不可能なデータ生成化、という二重のセキュリティ化によってICカード内のデータが守られていることも特徴の一つである。

【0032】

上記のデータ作成アルゴリズムを以下、数式で表す。

【0033】

生体特徴量を x とすると、前処理データ y はある関数 f （アルゴリズムに相当）を用いて「 $y = f(x)$ 」として表せる。

【0034】

登録データ z は生体特徴量 x と前処理データ y との組み合わせにより、作成されるので、ある関数 g を用いて「 $x + y \rightarrow z = g(x, y)$ 」と表せる。

【0035】

そして、この作成過程は不可逆的なものであることから、 $z = g(x, y) \rightarrow x$ 、 $z = g(x, y) \rightarrow y$ 、 $z = g(x, y) \rightarrow x + y$ のように登録データから生体特徴量や前処理データを復元することはできない。

10

20

30

40

50

【0036】

図4は生体情報登録装置101のCPU201が、又はCPU201からの指示に基づいて各機構、各部（プログラムも含む）が実行する生体情報の登録処理のフローチャート例である。

【0037】

ICカード装置103にはICカード105が挿入されており、ICカード接続状態（ICカード105へのデータの書き込みが可能な状態）になっている。ICカード接続を成立させるには、ICカード105の接点端子223にICカード装置103の接点端子214を接触させる必要がある。以下では、窓口担当者が登録用端末装置104を操作し利用者の生体情報をICカード105内に登録する過程を説明すると共にその操作に基づく各機構等が実行する処理、制御について説明する。また、図2で説明した通信制御プログラム209は特に生体情報登録装置101と生体登録用端末装置104との間でデータの送受信を制御するものであるが、以下では省略して説明する。

10

【0038】

登録用端末装置104は表示部106にメニュー画面（登録、認証、変更、終了などの処理の選択を案内する画面）を表示し、窓口担当者の入力操作を操作部107により受け付ける。表示された取引項目の中から登録処理が操作部107によって選択されると、登録用端末装置104のCPU231は登録処理プログラム205、生体情報登録装置制御プログラム233を実行し、生体情報登録装置101に登録処理開始の指示を出す。登録処理開始の指示を受けた生体情報登録装置101のCPU201は登録処理プログラム205を実行し、システム全体として登録処理を実施する。

20

【0039】

登録用端末装置104の表示部106に生体情報登録装置101にICカード105を挿入するよう案内が表示される。ICカード105がICカード装置103に挿入されると（ステップ401）、ICカード105の接点端子223とICカード装置103の接点端子214を接触させ、生体情報登録装置101とICカード105との接続を行う（ステップ402）。このとき挿入したICカード105の記憶部222における生体情報に関連するプログラムの有無を判断し（ステップ403）、プログラムがない場合（データを登録できないカードの場合）は、ICカード105を返却する（ステップ411）。一方、挿入したICカード105の記憶部222に生体情報に関連するプログラムがある場合（データを登録できるカードの場合）は、表示部106に登録する指を生体情報読取装置102に置くよう案内が表示される。それに応じて、利用者は登録する指を生体情報読取装置102におく。生体情報登録装置101のCPU201は、生体情報読取装置制御プログラム207を実行し、生体情報読取装置102に生体情報読取開始の指示を出す。生体情報読取装置102は、画像センサ210の画像取得可能領域に物体（指）が置かれると生体有無検知用照明LED211により物体（指）の進入を検知し（ステップ404）、物体（指）が生体であるか否かを調べる（ステップ405）。挿入された物体（指）が生体でなかった場合は、ICカード105に何の情報も書き込むことなくICカード105を返却する（ステップ411）。挿入された物体（指）が生体だった場合は、生体取得用照明LED212により物体（指）に近赤外線を照射し、画像センサ210で生体画像（指静脈パターン）を取得し、RAM204に記憶する（ステップ406）。次に、生体画像（指静脈パターン）から生体特徴量を抽出する（ステップ407）。そして、登録データ作成プログラム206を実行することで、図3のように生体特徴量から前処理データを作成した後（ステップ408）、生体特徴量と前処理データから登録データを作成する（ステップ409）。続いて、ICカード装置制御プログラム208を実行して、作成したRAM204内の前処理データと認証データをICカード書込部213、更にはICカード105内のCPU221によりICカード105の記憶部222に記憶して、生体情報登録が完了し（ステップ410）、ICカード105を返却する（ステップ411）。

30

40

【0040】

50

以上、各CPU201, 221, 231や記憶部に記憶された各プログラムの処理、制御を基に、生体情報の登録処理、制御について説明したが、各プログラムは登録処理に移行する当初の段階で既に起動されていても良く、またこれらのハード及びソフトによる構成を制御部として捉え、上述の各種制御、処理はこの制御部の機能、手段であることは言うまでもない。また、次に説明する生体情報の認証処理についても同様である。

【0041】

生体情報の認証処理を実行するにあたり、上述した登録処理によって登録された情報、即ち、ICカード105に記憶、登録、書き込まれた前処理データと、登録データとを使用して、認証処理を行うことを前提として説明する。

【0042】

図5は生体認証処理システムの概要図である。生体認証システムは、生体情報を読み取る機能と、ICカード105の情報に対する読み取り（又は書き込み）機能とを備えた現金自動取引又は預払装置（ATM）501と、金融商品に関係する取引に必要な情報を記憶するサーバ502とを接続して構成する。ATM501は入金、支払、振込など利用者の希望する種々な取引を自動的に実行する装置であり、利用者はカード／明細票機構部504にICカード105を挿入し、操作部503により希望する取引や金額などを入力し、生体認証機構508により認証が成功することにより取引を行うことが可能となる。特に、現金取引では、紙幣入出金機構部506による紙幣の入金又は出金、硬貨入出金機構部507による硬貨の入金又は出金が行われ、ATM501は利用者が希望する現金のやりとりを行う。また、利用者が通帳記入を希望する際には、通帳機構部505にて通帳

10

20

【0043】

図6は生体認証処理システムの一実施例の構成を示すブロック図である。ATM501は、ATM全体を制御するCPU601、取引項目の画面表示やキー入力検知、具体的には利用者の操作や指で押下されたキー入力を受け付けるタッチパネルなどで構成された操作部503、カードの挿入及び排出動作、カードの磁気ストライプ又はICカード105へのリード／ライト動作、カードエンボス部分のイメージの読み取りや、取引した内容を明細票に印字し、装置内から排出する機能を有するカード／明細票機構部504、利用者の通帳の挿入／排出動作、磁気ストライプのリード／ライト動作、通帳への印字部による印字機能などを有する通帳機構部505を有する。

30

【0044】

さらに、紙幣の鑑別や搬送、収納機能などを有し、紙幣の入金又は出金処理を行う紙幣入出金機構部506、硬貨の鑑別や搬送、収納機能などを有し、硬貨の入金又は出金処理を行う硬貨入出金機構部507、生体情報を取得し、その認証をサポートする生体認証機構部508、データやプログラムを記憶する主記憶部（単に記憶部とも言う）602、及びサーバ502と接続する通信部610により構成される。

【0045】

なお、図1、2で説明した登録用端末装置104の操作部107は窓口担当者が利用者の生体情報をICカード105に登録する際に入力操作を行うためのもので、キーボードやマウスなどで構成されており、一方、図5、6のATM501の操作部503は利用者がATM501で取引を行う際に入力操作するためのもので、タッチパネルなどで構成されており、この2つは同じ操作部でも構成・用途が異なるものである。

40

【0046】

カード／明細票機構部504は、ICカード105の情報を読み取るICカード読取部603と、明細票に取引内容を印字する明細票印字部604、及びICカード105と接続するための接点端子605を備えている。

【0047】

生体認証機構部508は、種々のデータ等を記憶する記憶部606と、利用者の生体画像（指静脈パターン）を取得し、CCDカメラなどで構成される画像センサ（画像取得部）607と、画像センサ607の画像取得可能領域に指が置かれたか否かを検知する生体

50

有無検知用照明LED608と、生体画像（指静脈パターン）取得時に指に対し近赤外線を照射する照明LED（生体照射部）609とを備えている。つまり、生体認証機構部508は図1、2に示す生体情報読取装置102とほぼ同様な生体情報を取得する機能を有している。

【0048】

主記憶部（単に記憶部とも言う）602は、ハード的には、各種プログラムを記憶するROM620と、主にデータを記憶し、記憶したデータの書き換えが可能なRAM621とで構成される。上述の登録処理で説明したとおり、それぞれハードディスクや種々の半導体メモリによる構成でも良く、また第1、2記憶部とも言う。また、ROM620は、以下に説明する生体画像の取得、認証などの処理をCPU601等の指示に従って行い、生体認証機構部508を制御するための認証制御ソフトウェア622を備えている。この他、図示しないがATM501の操作部503への画面データ、ATM501における現金取引、振込取引等に必要なプログラム、ソフトウェアも記憶されている。ATM501と通信網を介して接続されたサーバ502は、サーバ502全体を制御するCPU611、記憶部612、及びATM501と接続する通信部613により構成される。

10

【0049】

図7はATM501における生体情報の認証に係る制御、特に、生体認証機構部508の制御するための認証制御ソフトウェア622を中心にした主記憶部602、生体認証機構部508、カード/明細票機構部504内のICカード105、に関連する制御ブロック（ソフトウェア構成）を図示したものである。

20

【0050】

認証制御ソフトウェア622は、大きく、認証制御アプリケーション701と、認証制御ミドルウェア702とに分けられ、それぞれ、ソフトウェアのことをソフト、アプリケーションのことをアプリ、ミドルウェアのことをミドルと称することができる。認証制御アプリ701とは、生体認証機構部508を搭載するATM501を導入する金融機関などの個別の機能を有するプログラムであり、その認証の手順や方式、認証時における画面表示など金融機関個々でその仕様を作成し、また変更される。特に、本認証制御アプリ701は認証処理開始指示などを認証ミドル702に対して行う。

【0051】

認証制御ミドル702とは、金融機関が異なり、生体情報が異なっても認証処理に必要な共通機能を有するプログラムであり、生体認証機構部508を制御する生体認証機構部制御プログラム703、ICカード105からカードとデータのやり取り、ICカード105内のプログラムの実行を制御するICカード制御プログラム704といった生体情報の認証に係る各種プログラムの制御、処理を司るプログラムである。

30

【0052】

また、認証制御ミドル702によって実行され、得られるデータはRAM621に一時的に記憶される。RAM621は、生体認証機構部508とICカード105との間のデータをやり取りするためのバッファ領域である認証結果データバッファ705、認証データバッファ706、前処理データバッファ707といった各データバッファを有する。これらのデータはハード的にはRAM621に記憶されるが、ソフト的には認証制御ソフトウェア622、特に認証制御ミドル702に記憶される、とも言える。

40

【0053】

また認証制御ミドル702は認証制御アプリ701からの指示によりドライバ（図示しない）を経由してカード/明細票機構部504や生体認証機構部508を動作させる。そして、上述のように、これらの各部位はATM501のCPU601によってその処理が制御される。なお、ドライバとはコンピュータ周辺機器・装置（デバイス）を利用するための制御用ソフトウェアある。

【0054】

認証制御ソフト622より制御される生体認証機構部508の記憶部606は、認証データを作成するための認証データ作成プログラム709、認証結果データから認証の成否

50

を判定するための認証結果判定プログラム710を有する。またカード/明細票機構部504は認証処理を実施するための認証プログラム711を有する。

【0055】

図8により生体認証処理における認証の仕組み、データのやり取りについて説明する。後述の図11の生体認証フローの説明の補完としても用いる。以下の動作の主体は認証制御アプリ701から実行命令を受けた認証制御ミドル702であるが、認証制御アプリ701と認証制御ミドル702とが共同して行うことから認証制御ソフト622によって動作する、とも言える。また、受信、送信をそれぞれ入力、出力とも言える。

【0056】

ATM501の取引において生体情報の認証が実行されると、ICカード105に予め記憶されている前処理データ、登録データのうち、前処理データが認証制御ミドル702に送信される。認証制御ミドル702は、ICカード105から前処理データを受信し、RAM621（認証制御ソフト622、認証制御ミドル702を含む）の前処理データバッファ707に一時記憶してから、生体認証機構部508に送信する（ステップ801）。一方、生体認証機構部508は認証制御ソフト622から前処理データを受信し、その後又は並行して、利用者の生体情報を取得し、生体情報から生体特徴量を抽出する。そして、受信した前処理データと取得、抽出した生体特徴量とを組み合わせる認証データを作成する（ステップ802）。

【0057】

このように、生体情報の認証処理において、前処理データは、認証データを作成するための暗号鍵としての機能も有している。また、この認証データを仮に取得できたとしても、このデータから生体特徴量直接作成することはできない。認証データは生体特徴量から作成したデータであるが、この作成過程では不可逆変換処理によるアルゴリズムを用いていることから、逆に認証データから生体特徴量を作成することはできず、更に、前処理データと認証データとの2つのデータから生体特徴量を作成することはできない。前処理データは個人を特定できない部分を抜き出して作成した情報で、認証データは個人を特定できる部分を抜き出して作成した情報である。

【0058】

ここで、上記のデータ作成アルゴリズムを生体情報登録時と同様に数式で表す。

【0059】

生体認証機構部508によって認証時に得る情報、即ち、新たに得た生体特徴量を x' とする。そして前処理データ y は登録時と変わらないので、「 $y = f(x)$ 」である。

【0060】

認証データ z' は生体特徴量 x' と前処理データ y との組み合わせにより作成されるので、ある関数 g を用いて「 $x' + y \rightarrow z' = g(x', y)$ 」と表せる。そして、この作成過程は不可逆過程なので、 $z' \rightarrow x'$ 、 $z' \rightarrow y$ 、 $z' \rightarrow x' + y$ のように登録データから生体特徴量や前処理データを復元することはできない。

【0061】

S802の認証データ作成後、生体認証機構部508で作成した認証データを認証制御ソフト622の指示、制御によって認証データバッファ706に一時記憶してから、ICカード105に送信する（ステップ803）。ICカード105は認証データを受信し、ICカード105に記憶しておいた登録データと認証データとをあるアルゴリズムによって照合し（生体認証処理とも言う）、認証結果データを作成する（ステップ804）。さらに作成した認証結果データを認証制御ミドル702に送信する。認証制御ミドル702はICカード105から認証結果データを受信し、認証制御ソフト622の認証結果データバッファ705に一時記憶してから、生体認証機構部508に送信する。そして、生体認証機構部508は生体認証機構部508内で認証結果データの判定（分析）を行い（ステップ805）、認証結果データと認証成功部位・認証失敗原因を認証制御ミドル702に通知し（ステップ806）、生体認証処理は終了する。

【0062】

このように、生体認証処理では、利用者の生体情報そのものに最も近い生体特徴量は I C カード 1 0 5 内に記憶しておらず、また生体認証機構部 5 0 8 によって生体特徴量を取得、抽出するものの、生体認証機構部から外には出さない特徴を有している。

【0063】

また、認証制御ソフト 6 2 2 を介して、またその制御の基に、I C カード 1 0 5 と生体認証機構部 5 0 8 との間でやり取りするデータは前処理データ、認証データ、認証結果データの 3 つであるが、上述のとおりこれらのデータを如何様に組み合わせても生体特徴量を作成することはできない特徴も有している。

【0064】

また、生体情報に係る各データの作成など生体認証処理において、I C カード 1 0 5、生体認証機構部 5 0 8 のそれぞれに分担して認証結果を得る特徴を有している。そのため、I C カードまたは生体認証機構部が盗まれ、またその内部を解読したとしても生体認証処理を実行することができないように工夫されている。つまり、認証時に生体認証機構部 5 0 8 で取得した生体特徴量から新たに前処理データを作成し、この前処理データと生体特徴量から認証データを作成することも理論上可能であるが、本実施形態ではそのようにはせず、I C カード 1 0 5 に記憶しておいた前処理データと生体特徴量により認証データを作成するので、セキュリティが高く保たれている。

【0065】

また、認証制御ミドル 7 0 2 は前処理データを生体認証機構部 5 0 8 内に記憶し、認証データが作成されてから削除するのが良く、認証が必要な際に、随時、前処理データバッファ 7 0 7 から生体認証機構部 5 0 8 に送信する態様が望ましい。つまり、A T M 5 0 1 による取引が終わるまで認証制御ソフト 6 2 2 内の前処理データバッファ 7 0 7 に前処理データを記憶しておくことである。こうすることで、前処理データを I C カード 1 0 5 から送信するよりも、認証制御ソフト 6 2 2 内の前処理データバッファ 7 0 7 から送信した方が早い処理が可能になる、との効果がある。

【0066】

図 9 ~ 1 2 を用いて現金自動取引装置、現金自動預払装置 (A T M) 5 0 1 で I C カード 1 0 5 を使用して I C カード内認証方式による生体認証処理を含む支払取引を実施するときの処理を説明する。

【0067】

図 9 は A T M 5 0 1 の C P U 6 0 1、認証制御ソフト 6 2 2 等 (制御部) が実行し、特に I C カード内認証方式を用いた生体認証処理による A T M 上での取引を示すフローチャート例である。

【0068】

生体認証処理を行う前に、取引選択や暗証番号入力、カード挿入など A T M 5 0 1 での取引を実行するために必要な処理を行う。操作部 5 0 3 に入金、支払、残高照会、振込などの取引選択案内を R O M 6 2 0 より読み出して表示し、利用者から取引の選択を受け付ける (ステップ 9 0 1)。生体認証が必要な取引、例えば支払取引等が選択された場合は操作部 5 0 3 に I C カードを挿入する旨の案内を表示し I C カード 1 0 5 の挿入を促す。利用者によりカード / 明細票機構部 5 0 4 に I C カード 1 0 5 が挿入されるとそれを検知し (ステップ 9 0 2)、カード / 明細票機構部 5 0 4 の I C カード読取部 6 0 3 より I C カード 1 0 5 から口座番号を読み取る。なお、I C カード 1 0 5 は磁気ストライプを備えたものでも良く、そのときは生体情報以外の、口座番号などのデータを I C カード 1 0 5 の磁気ストライプから読み取ることも可能である。

【0069】

次に暗証番号を入力する旨の案内を操作部 5 0 3 に表示する。利用者により操作部 5 0 3 に暗証番号が入力されると、それを検知し (ステップ 9 0 3)、読み取った口座番号と入力された暗証番号とを通信部 6 1 0、6 1 3 を介してサーバ 5 0 2 に送信する。一方、サーバ 5 0 2 の C P U 6 1 1 は、入力された暗証番号を通信部 6 1 0、6 1 3 を介して受信し、入力された暗証番号と事前に記憶部 6 1 2 に登録しておいた口座番号に対応する暗

10

20

30

40

50

証番号との照合を行い、その照合結果をA T M 5 0 1に通信部 6 1 0、6 1 3を介して送信する。A T M 5 0 1は通信部 6 1 0、6 1 3を介して照合結果を受信して、暗証番号の正否をチェックし（ステップ 9 0 4）、入力された暗証番号が正しくなかった場合は、暗証番号の入力回数をカウントする（ステップ 9 0 5）。このときの暗証番号の入力回数が規定回数以内であれば利用者に対し、暗証番号の再入力を促す。暗証番号の入力回数が規定回数を超えていれば、取引を中止する（ステップ 9 0 6）。

【0070】

S 9 0 4において、入力された暗証番号が正しかった場合は、挿入された I C カード 1 0 5が生体認証対象カードであるか否かを判断する（ステップ 9 0 7）。このときの生体認証対象カードとは、生体認証を実施するために必要な情報やプログラムを持つカードである。

10

【0071】

そして、挿入された I C カード 1 0 5が生体認証対象カードではなかった場合は生体認証処理を行わず、続いて支払等の取引を実行する（ステップ 9 1 5）。挿入された I C カード 1 0 5が生体認証対象カードであった場合、生体認証処理の事前準備として認証取引開始処理を行う（ステップ 9 0 8）。認証取引開始処理については後述の図 1 0を用いて詳細に説明する。

【0072】

認証取引開始処理が終了すると、A T M 5 0 1の C P U 6 0 1は認証制御ソフト 6 2 2を R A M 6 2 1に取り込み、展開する。次に A T M 5 0 1の C P U 6 0 1は認証制御アプリ 7 0 1を実行する。それを受けて認証制御アプリ 7 0 1は認証制御ミドル 7 0 2に対し登録情報取得指示を出す。登録情報取得指示を受けた認証制御ミドル 7 0 2は I C カード制御プログラム 7 0 4を実行して、認証制御アプリ 7 0 1から指示された処理に必要な情報（登録者情報）を I C カード 1 0 5から取得する（ステップ 9 0 9）。処理に必要な情報には口座番号、店番、科目などの取引情報や利用者氏名、運転免許証や保険証などの本人確認が可能な証明書の有無といった利用者情報などが含まれる。また、このとき認証制御ミドル 7 0 2は認証制御アプリ 7 0 1に取得を指示された情報の他に、I C カード 1 0 5に予め登録されていた前処理データを取得し、前処理データバッファ 7 0 7に格納する。これは、認証制御アプリ 7 0 1が指定している情報と同時に前処理データも取得することで I C カード 1 0 5にアクセスする回数を減らし、処理時間を向上するためである。このデータは認証制御ミドル 7 0 2に送信され、前処理データバッファ 7 0 7に格納される。このように A T M 5 0 1の C P U 5 0 1が主体になって認証制御ソフト 6 2 2内の各種プログラムを実行してそれぞれの処理を行うが、以下では、説明を簡略化するためにこの過程を省略し、認証制御ミドル 7 0 2を主体として説明する。また、上述してきたように、これらを纏めて制御部（手段）による制御、処理とも言う。

20

30

【0073】

I C カード 1 0 5から登録情報を取得後、認証制御ミドル 7 0 2は生体認証機構部制御プログラム 7 0 3を実行して生体認証処理を行う（ステップ 9 1 0）。即ち、前処理データバッファ 7 0 7に格納された前処理データを生体認証機構部 5 0 8へ送信すると同時に、生体認証機構部 5 0 8に生体情報取得を指示する。この生体認証処理については図 8を用いて説明したが、後述の図 1 1においても詳細に説明する。

40

【0074】

次に生体認証の成否をチェックし（ステップ 9 1 1）、ここで生体認証が失敗だった場合は、生体認証の実施回数をカウントする（ステップ 9 1 2）。このときの生体認証の実施回数が規定回数以内であれば R A M 6 2 1又はプログラムに記憶、格納していた前処理データを生体認証機構部 5 0 8に再送信し、利用者に対し生体認証の再実施を促す。生体認証の実施回数が規定回数を超えていれば、取引を中止する（ステップ 9 1 3）。なお、このとき、R A M 6 2 1に記憶された前処理データ等はセキュリティを高めるため削除する。そして S 9 1 1において、生体認証が成功だった場合は、生体認証処理の事後処理として認証取引終了処理を行う（ステップ 9 1 4）。この認証取引終了処理については後述

50

の図12を用いて詳細に説明する。

【0075】

認証取引終了処理が終了すると、利用者の希望する取引、つまりS901で取引選択された取引を実行する(ステップ915)。具体的には、利用者の希望する取引が支払取引ならば、操作部503により、支払金額の入力を受け付ける。利用者により支払金額入力が行われると、入力された金額及び金額が正しいか否かの確認キー押下を促すメッセージを操作部503に表示する。操作部503の確認キーが押下されると、サーバ502と取引データの通信を行う。通信後、ATM501のCPU601は要求された金額分の紙幣、硬貨を紙幣入金機構部506、硬貨入金機構部507からそれぞれ排出し、カード/明細票機構部504の明細票印字部604に取引データの印字を行わせる。そして、カード/明細票機構部504からICカード105を返却するとともに、取引データを明細票に印字・送出し、取引が終了する(ステップ916)。

10

【0076】

また、利用者の希望する取引が残高照会ならば、サーバ502と取引データの通信を行い、通信後、操作部503に預金又は借入残高を表示する。表示後、利用者に対し、取引を終了したいか、続けて別の取引を実施したいかの案内を行う。取引を終了したい場合には、カード/明細票機構部504からICカード105を返却するとともに、利用者の要望に応じて取引データを明細票に印字・送出し、取引が終了する(ステップ916)。利用者が別の取引実施を希望する場合には、以下の処理を行う。

【0077】

20

残高照会後に続けて、上述の支払取引などの生体認証が必要な取引が希望された場合、再び生体認証を実施して、生体認証が成功した場合にのみ取引を実行する。生体認証を取引ごとに実施することにより、利用者が残高照会で預金・借入残高を確認したがICカード105を受け取らずにATMから離れてしまった場合、第三者により取引が行われてしまう場面も考えられるので、そのような危険を排除し、セキュリティの高いATMシステムを実現することができる。

【0078】

なお、このフローでは、暗証番号入力後に、生体認証を実施しているが、この順番を逆にして、生体認証実施の後に暗証番号を入力させても良い。暗証番号入力を先に実施する場合には、一般的な取引と同様に利用者はカード挿入後、最初の取引選択後すぐに暗証番号を入力するので、その後に生体認証を行っても操作フローが現状に近く装置を扱い易いという利点がある。一方、暗証番号による認証よりも生体認証を先に実施する場合には、もしも本人以外が生体認証を行い生体認証が失敗となり取引を拒否するときに、暗証番号入力を経ずに取引を終了するので無駄な暗証番号照合のためのサーバとの通信をしなくて済み、サーバへの負担を軽減できるという利点がある。

30

【0079】

図10により、図9のS908における認証取引開始処理について説明する。認証制御アプリ701から認証取引開始指示を受けた認証制御ミドル702は、ICカード制御プログラム704を実行して、ICカード105との接続を行う(ステップ1001)。これは前述したようにICカード105からのデータの読み取りを可能な状態にするものである。但し、ICカード105には生体情報に関するデータがなく、ICカード内認証に対応していないICカードの場合は、例えば上述の暗証番号による認証処理のみでもATMでの所望の取引ができるようにするのが望ましく、図9のS902などのカード挿入とほぼ同タイミングでICカード制御プログラム704を認証制御ミドル702以外の他のATMソフトウェアによって実行し、少なくともS908の処理前にICカード105との接続を完了させておく方が良い。

40

【0080】

また、カード/明細票機構部504に挿入されているICカード105には、図1の生体情報登録装置101により予め利用者固有の登録データ及び前処理データが登録されており、ICカード105内で認証を行うための認証プログラム711が搭載、記憶されて

50

いる。この認証プログラム711はICカード105に事前に、また書き換え不可能な形式で書き込まれたアプリケーションであり、ICカードに事前登録された登録データと、ATMの制御部によって得られた認証データとを特定のアルゴリズムに従ってマッチング、照合を行うプログラムである。

【0081】

S1001にてカード／明細票機構部504とICカード105との接続が成功すると、認証制御ミドル702はICカード105に登録されているサポート認証方式（又はサポート認証情報）を取得する（ステップ1002）。サポート認証方式とは、予めICカード105に登録されているもので、認証データや生体特徴量などの情報をどの制御手順で認証処理が実施できるかを一意に決定できる情報である。例えば、指静脈認証では生体認証機構部508内において認証（照合）する装置内認証処理と、ICカード105内において認証するICカード内認証処理をサポートしており、ICカード105からサポート認証方式を取得することで、認証制御手順を切り替え1つの認証制御プログラムで2つの認証方式を可能にしている。

10

【0082】

このサポート認証方式取得のような、ICカードなどに登録された認証方式、認証制御手順を一意に決定する情報を用いて認証制御の手順や方式を切り替える方法は、ATMなどの生体認証装置搭載端末に複数の認証装置（例えば指、手のひらといった静脈認証装置や目の虹彩認証装置など）が搭載されている場合にも、認証制御プログラムの制御方式を切り替えることで複数の生体認証装置の制御に対応できることになる。

20

【0083】

次に、ステップ1002で得た認証方式が、ICカード内認証か否かを判断し（ステップ1003）、ICカード内認証でない場合は取引処理を行わずにICカード105を返却する（ステップ916）。一方、ICカード内認証方式である場合はATM501とICカード105との間の相互認証を行い、認証取引開始処理は終了する（ステップ1004）。相互認証とは、生体認証機構部508にある認証データ作成プログラム709や、ICカード105に搭載された認証プログラム711などが不正なプログラムに改ざんされていないか、ATM501とICカード105とで相互のプログラムの正当性を確認するための処理である。

【0084】

図11により図9のS908の生体認証処理について説明する。図8で説明したように、この生体認証処理は、最終的には、予めICカード105内に記録しておいた登録データと、生体認証処理時に新たに作成した認証データとの認証（照合）を行い、その照合結果を得る処理であり、認証自身の根幹に係る処理はICカード105内で行うことを特徴とする。

30

【0085】

図9のS909においてICカード105よりデータを受信するが、それと共にこの生体認証時には、ICカード105から予め記憶していた前処理データを認証制御ミドル702に送信する。認証制御ミドル702はICカード105に記憶していた前処理データを受信し、前処理データバッファ707に格納する。さらに、前処理データバッファ707に格納されたこの前処理データを生体認証機構部508へ送信する（ステップ1101）。生体認証機構部508は前処理データを受信すると、次にまた並行処理として、利用者の生体情報を読み取る。

40

【0086】

図11のステップ1102～ステップ1105の処理は、図4のステップ404～ステップ407とほぼ同じ処理を実行して生体特徴量を得る。画像センサ607の画像取得可能領域に指が置かれると生体有無検知用照明LED608により物体（指）が置かれたことを検知し（ステップ1102）、物体（指）が生体であるか否かを調べる（ステップ1103）。挿入された物体（指）が生体でなかった場合は、生体認証が失敗となる（ステップ1104）。挿入された物体（指）が生体だった場合は、生体取得用照明LED60

50

9により生体に近赤外線を照射し、画像センサ607で生体画像（指静脈パターン）を取得し、記憶部606に記憶する（ステップ1105）。

【0087】

次に、生体画像（指静脈パターン）から特徴的なデータをあらわす生体特徴量を抽出する（ステップ1106）。そして、認証制御ミドル702の指示で認証データ作成プログラム709を実行することで、図8にて説明した認証データを作成する（ステップ1107）。そして作成された認証データを認証制御ミドル702に送信し、認証データバッファ706に格納する。

【0088】

認証制御ミドル702はICカード制御プログラム704を実行して、認証データバッファ706に格納した認証データをICカード105に送信すると同時にICカード105内の認証プログラム711に生体認証指示を出す（ステップ1108）。一方、ICカード105はカード内に記憶された認証プログラム711を実行して、ICカード105に予め登録された登録データと、上述の認証制御ミドル702の認証データバッファ706に格納された認証データとを照合して生体認証処理を行い、認証結果データを作成する。

10

【0089】

そして、ICカード105は認証結果データを認証制御ミドル702に送信し、認証制御ミドル702は認証制御ミドル702内（ハードとしてはRAM内）の認証結果データバッファ705に格納する。このように認証制御ミドル702が実施する生体認証機構部508とICカード105と間のデータの送受信制御では、生体画像（指静脈パターン）から取得した生体特徴量は生体認証機構部508の外部に出ることがなく、またICカード105に登録されている認証データも外部に出ることがない。よって個人情報が装置の外部に漏洩するのを防ぐことができるので、個人情報の秘匿性が守りセキュリティが向上する。

20

【0090】

認証制御ミドル702は生体認証機構部制御プログラム703を実行して認証結果データバッファ705に格納された認証結果データを生体認証機構部508へ送信すると共に認証結果判定プログラム710に認証結果判定指示を出す。次に認証結果判定プログラム710を実行してICカード105内で行った認証の結果である認証結果データバッファ705に格納された認証結果データから生体認証が成功か失敗かを判断する。ここで出力として、生体認証機構部508は認証が成功した場合は、生体のどの部位で認証が成功したかを認証制御ミドル702に通知する（ステップ1109）。例えば、生体認証の部位が指静脈や、指紋などであれば、どの指（例、右手、中指等）で認証が成功したか、手ひらの静脈であれば右手か左手か、目の虹彩であれば、右目か左目のどちらで認証が成功したかが認証制御ミドル702に通知されることになる。

30

【0091】

認証結果が失敗であった場合は、認証結果判定プログラム710でICカード内認証に失敗した原因を判断し認証制御ミドル702に通知する。原因として、例えば指の置き方が悪かったのか、登録されていた別の指を置いてしまったか、などの情報を付随させて認証制御ミドル702に通知し、それに基づいて認証制御アプリ701によって操作部503にその原因を表示するのが望ましく、これにより操作性の良い装置を提供できる。このように、生体認証機構部508が認証結果を判別する例にて説明したが、ICカード内の認証プログラム711、または、認証結果データを取得した認証制御ミドル702でも認証処理の成否や認証成功部位、認証失敗原因などの認証結果の判別ができる形態でも良い。

40

【0092】

認証制御ミドル702は登録データと認証データとのマッチング、照合結果である判定結果データを認証制御アプリ701へ送信する。認証制御アプリ701は判定結果データが認証失敗であれば、ATM501の操作部503に認証再開始画面を出すなどして、利

50

用者に再度、認証を実施させるようにする。このとき、認証制御ミドル702は、ICカード105の登録情報取得処理で取得した前処理データを前処理データバッファ707に保持し続けるのが望ましく、ICカード105の登録情報取得処理を省略することができるので、認証処理時間が向上する。これは、残高照会から支払取引というような1回の来店で連続した本人確認が必要な取引を行うため複数回の認証処理を実行する場合にも、同様にICカード105から取得した前処理データを前処理データバッファ707から削除しないことで、ICカード105の登録情報取得処理を省略し、連続取引にての認証処理を実行することが可能である。

【0093】

図12により、図9のS914に示す認証取引終了処理について説明する。

10

【0094】

認証制御アプリ701は判定結果データが認証成功であれば、認証制御ミドル702に対して認証取引終了指示を出す。認証制御ミドル702は、ICカード制御プログラム704を実行しICカード105との切断処理を実行する。ICカード105との切断とはICカード105にアクセスすることができなくなる状態である。ICカード105との切断後、認証制御ミドル702からの指示で生体認証装置制御プログラム703は、生体認証機構部508にある生体特徴量など、生体認証に使用した個人情報やそれを元に作成された認証に係わる情報を全て記憶部から削除する。

【0095】

これは個人情報などが外部に漏洩することを防ぎ、セキュリティを向上させるために有効な特徴でもある。生体認証機構508内のデータをクリアした後、認証制御ミドル702は、自身が持つ認証結果データバッファ705、認証データバッファ706、前処理データバッファ707に格納された情報を削除し（連続取引は除く）、情報漏洩を防止している。認証取引終了処理が終了すると、支払金額の入力、サーバ502との通信などを行い、支払取引を終了する。

20

【0096】

以上、図1～4を用いて生体情報の登録処理、図5～12を用いて生体情報の認証処理を説明したように、例えば、ハード的にはCPU601、主記憶部602の制御、処理によって行われ、ソフト的には認証制御ソフト622、認証制御アプリ701、認証制御ミドル702の制御、処理によって生体情報の認証が実行される。よって、上述したとおり、これらを纏めて制御部、制御手段による制御、処理ということが出来るし、また各プログラムの機能をLSI等のハード的にも達成できる。また図7の各種プログラムはその処理に必要なときに初めて起動、実行されるだけでなく、ATM起動時に各プログラムを起動させておき、各処理で必要なプログラムを実行させる方が処理時間は短縮できる。

30

【0097】

また、図3において、前処理データを生体特徴量から作成し、その作成した前処理データと生体特徴量から認証時に使用される登録データを作成する形態にて説明したが、前処理データの作成に関して生体特徴量とは全く関連なく、また独立に作成してもよい。上述したとおり、生体情報の登録時において前処理データは登録データを作成するための暗号鍵（またはアルゴリズム）の機能を有し、生体認証時には認証データを作成するための暗号鍵の機能、役割を有している。従って、生体特徴量から前処理データを作成すれば、即ち利用者それぞれに対応したデータとなりセキュリティの高いデータ作成アルゴリズムを構成できるが、一方、前処理データを生体特徴量とは独立に作成すれば、事前に暗号鍵としての役目である前処理データ自身を作成しておくこともでき、全体として簡易なプログラム構成となるので手間が省け、登録、認証の処理時間が短くなる。

40

【0098】

また、前処理データを生体特徴量から一段階で作成したが、何段階か踏まえた上で作成するようにしてもよい。これにより、第3者が前処理データ作成過程を解析しようとしても、作成過程が複雑なので解析しにくい、また、解析に時間がかかるという効果がある。

【0099】

50

また、前処理データ、登録データ、認証データ（認証失敗時や連続取引時に作成する認証データを含む）は元々利用者の指などの生体特微量（画像パターン含む）から作成、生成された情報であることから、第1、2、…（生体）情報と言うことができる。即ち、これら第1、2…（生体情報）は生体特微量を含んだ概念である生体情報から得られる情報とも言える。

【0100】

以上、本発明のICカード内認証方式ではICカード内に登録された個人を特定できる情報と認証装置で取得した生体情報(生体特微量)そのものは、認証装置搭載端末に取り込まれることがないので、個人情報の秘匿性が守られ、セキュリティの高い生体認証が可能となる。

10

【図面の簡単な説明】

【0101】

【図1】生体情報登録処理システムの概要図の例。

【図2】生体情報登録処理システムのブロック図の例。

【図3】生体情報登録処理の説明図。

【図4】生体情報登録処理のフローチャートの例。

【図5】生体認証処理システムの概要図の例。

【図6】生体認証処理システムのブロック図の例。

【図7】認証制御ソフトウェアの構成図の例。

【図8】生体認証処理の説明図。

20

【図9】ICカード内認証方式を用いた生体認証処理を含む取引のフローチャートの例。

【図10】認証取引開始処理のフローチャートの例。

【図11】生体認証処理のフローチャートの例。

【図12】認証取引終了処理のフローチャートの例。

【符号の説明】

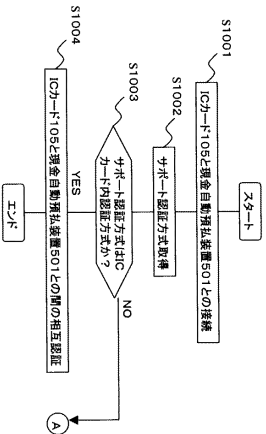
【0102】

101…生体情報登録装置、102…生体情報読取装置、103…ICカード装置、104…登録用端末装置、105…ICカード、201…CPU（生体情報登録装置）、202…主記憶部（生体情報登録装置）、203…ROM（生体情報登録装置）、204…RAM（生体情報登録装置）、205…登録処理プログラム、206…登録データ作成プログラム、207…生体情報読取装置制御プログラム、208…ICカード装置制御プログラム、209…通信制御プログラム、210…画像センサ（生体情報登録装置）、221…CPU（ICカード）、222…記憶部（ICカード）、231…CPU（登録用端末装置）、232…主記憶部（登録用端末装置）、233…生体情報登録装置制御プログラム、501…現金自動預払装置、502…サーバ、503…操作部（現金自動預払装置）、504…カード/明細票機構部、508…生体認証機構部、601…CPU（現金自動預払装置）、602…主記憶部（現金自動預払装置）、607…画像センサ（現金自動預払装置）、611…CPU（サーバ）、612…記憶部（サーバ）、620…ROM（現金自動預払装置）、621…RAM（現金自動預払装置）、622…認証制御ソフトウェア、701…認証制御アプリケーション、702…認証制御ミドルウェア、703…生体認証機構部制御プログラム、704…ICカード制御プログラム、705…認証結果データバッファ、706…認証データバッファ、707…前処理データバッファ、709…認証データ作成プログラム、710…認証結果判定プログラム、711…認証プログラム

30

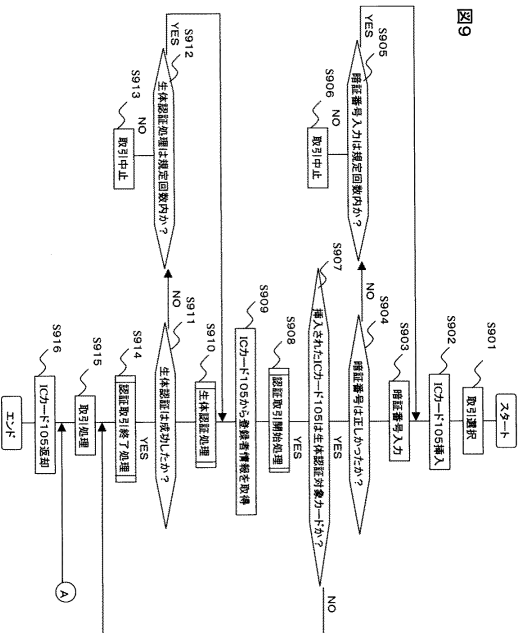
40

図 10



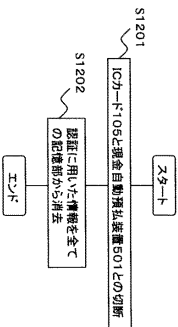
【図 10】

図 9



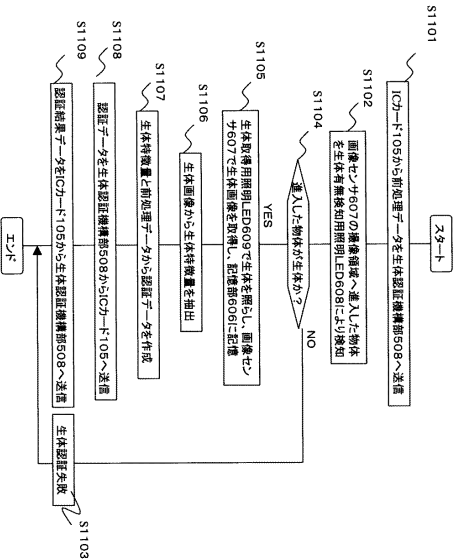
【図 9】

図 12



【図 12】

図 11



【図 11】

フロントページの続き

(51)Int.Cl. F I
G 0 6 T 7/00 (2006.01) G 0 6 T 7/00 5 1 0 B

(72)発明者 山口 章
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

合議体

審判長 丸山 英行

審判官 金丸 治之

審判官 中川 真一

(56)参考文献 特開平10-312459 (JP, A)
特開平11-143833 (JP, A)
国際公開第2004/023999 (WO, A1)
特開2000-181870 (JP, A)

(58)調査した分野(Int.Cl., DB名)
G07D 1/00- 9/04
G06K 17/00