

明 細 書

発明の名称：

携帯可能な認証デバイス、ＩＣカードおよび認証システム

技術分野

[0001] 本発明の実施形態は、携帯可能な認証デバイス、ＩＣカードおよび認証システムに関する。

背景技術

[0002] 従来、医療機器などの利用者を制限する必要がある機器を運用するためのシステムとして、予め設定（指定）された人物または有資格者だけに機器（以下、利用制限機器と称する）の操作を許可する認証システムがある。従来の認証システムでは、利用制限機器または利用制限機器に接続したサーバなどの上位装置に登録された人物であることを確認できた場合に、利用制限機器の利用を許可する。

[0003] しかしながら、利用制限機器でユーザ認証を行う場合には、ユーザ認証を行うためのハードウェアを利用制限機器に設けなければならない。また、生体認証などでユーザ認証を行う場合、利用制限機器または利用制限機器の上位装置が、全ての登録者の生体情報などをセキュアに管理しなければならないという問題がある。

[0004] 一方、指紋認証を行うＩＣカードが実用化されている。ＩＣカードでは、セキュアに生体情報を管理でき、セキュリティ性が高い生体認証を実現している。しかしながら、従来のＩＣカードは、ユーザの生体情報と登録者との生体認証の結果を出力するだけであり、登録者が機器本体の利用権限を持っているか否かを確認することができない。

先行技術文献

特許文献

[0005] 特許文献１：日本国特開平１１－１３４３０２公報

発明の概要

発明が解決しようとする課題

[0006] 上記の課題を解決するため、機器の利用権限を有する人物であることを生体認証で認証した結果を前記機器へ供給できる携帯可能な認証デバイス、ＩＣカードおよび認証システムを提供する。

課題を解決するための手段

[0007] 実施形態によれば、認証デバイスは、センサと通信インターフェースとメモリとプロセッサとを備える。センサは、生体情報を取得する。通信インターフェースは、機器と通信する。メモリは、生体認証に用いる登録者の生体情報の特徴点情報（テンプレート）と登録者が利用権限を有する機器を示す管理情報とを記憶する。プロセッサは、センサが生体情報を取得したユーザが前記通信インターフェースにより通信する機器の利用権限を有する登録者であることを認証し、認証の結果を通信インターフェースにより通信する機器へ送信する。

図面の簡単な説明

[0008] [図1]図1は、実施形態に係る携帯可能な認証デバイスとしてのＩＣカードおよびＩＣカードを含む認証システムの構成例を示すブロック図である。

[図2]図2は、実施形態に係るＩＣカードが保持するデータの第1の構成例を示す図である。

[図3]図3は、実施形態に係るＩＣカードが保持するデータの第1の構成例を示す図である。

[図4]図4は、実施形態に係るＩＣカードが保持するデータの第1の構成例を示す図である。

[図5]図5は、実施形態に係るＩＣカードが保持するデータの第2の構成例を示す図である。

[図6]図6は、実施形態に係るＩＣカードが保持するデータの第2の構成例を示す図である。

[図7]図7は、実施形態に係るＩＣカードが保持するデータの第2の構成例を示す図である。

[図8]図8は、実施形態に係るＩＣカードが保持するデータの第３の構成例を示す図である。

[図9]図9は、実施形態に係るＩＣカードおよびＩＣカードを含む認証システムの動作例を示すタイミングチャートである。

[図10]図10は、実施形態の変形例に係るＩＣカードが保持するデータの構成例を示す図である。

実施形態

[0009] 以下、実施形態について、図面を参照して説明する。

実施形態に係るＩＣカードなどの携帯可能電子装置は、ユーザから取得する生体情報を用いてセキュアに人物の認証処理を行う携帯可能な認証デバイスである。本実施形態において、ＩＣカードは、人物の指紋の画像（指紋画像）を取得する生体センサとしての指紋センサを具備し、指紋センサで取得する指紋画像を用いて認証処理を行う。

[0010] 図1は、実施形態に係るＩＣカード2を含む認証システム10の構成例を示す。

図1が示すように、認証システム10は、ＩＣカード2と複数種類の利用制限機器1（1A、1B、1C、…）とを含むシステムである。利用制限機器1は、特定の人物に対して利用が許可される機器である。例えば、利用制限機器1は、予め設定した人物に対して利用が許可されるものであっても良いし、特定の資格を有する人物に対して利用が許可されるものであっても良い。

[0011] 利用制限機器1は、携帯可能な認証デバイスとしてのＩＣカード2と通信する機能を有する。利用制限機器1は、ＩＣカード2によって自機の利用が許可されている人物であることが認証された場合、当該人物による利用が可能となる装置である。利用制限機器1は、予め設定した人物が操作可能となる医療機器などであっても良いし、有資格者である場合に操作可能となる装置であっても良い。

図1に示す構成例において、利用制限機器1は、プロセッサ11、ＲＯＭ

１２、ＲＡＭ１３、データメモリ１４、リーダライタ１５および処理部１６を有する。

プロセッサ１１は、各部の制御および各種の処理などを実行する。プロセッサ１１は、例えば、ＣＰＵ（central processing unit）である。プロセッサ１１は、ＲＯＭ１１またはデータメモリ１４に記憶されたプログラムを実行することにより各部の制御および各種の処理を実現する。

[0012] ＲＯＭ１２は、書き換え不可のデータを保存する不揮発性メモリである。ＲＯＭ１２は、プログラムまたは制御データなどを記憶する。ＲＡＭ１３は、データを一時的に記憶する揮発性メモリである。

データメモリ１４は、書き換え可能な不揮発性のメモリである。データメモリ１４は、ＨＤＤ（ハードディスクドライブデータ）あるいはＳＳＤ（ソリッドステートドライブ）などで実現される。

[0013] リーダライタ１５は、ＩＣカード２と通信接続するためのインターフェースである。リーダライタ１５は、ＩＣカード２に対して電源供給、クロック供給、リセット制御、データの送受信が行う。リーダライタ１５は、ＩＣカード２の通信方式に応じたインターフェースにより構成される。

[0014] 例えば、ＩＣカード２が接触型のＩＣカードである場合、リーダライタ１５は、ＩＣカード２のコンタクト部と物理的かつ電氣的に接続するための接触部などにより構成される。また、ＩＣカード２が非接触型のＩＣカードである場合、リーダライタ１５は、ＩＣカード２との無線通信を行うためのアンテナ及び通信制御部などにより構成される。

[0015] 処理部１６は、ＩＣカード２によって利用が許可された場合に処理を実行するものである。例えば、処理部１６は、ＩＣカード２において予め設定された人物であることが認証された場合に処理を実行するものであっても良いし、ＩＣカード２において所定の資格を有する人物であることが認証された場合に処理を実行するものであっても良い。具体例として、処理部１６は、医療行為を実行または補助するための処理機構を含むものであっても良いし、運転（操作）免許を有する人物（有資格者）の操作に応じて駆動する駆動

機構を含むものであっても良い。

[0016] 次に、ＩＣカード２の構成について説明する。

ＩＣカード２は、生体情報による認証（生体認証）を実行する機能を有する携帯可能な認証デバイスである。実施形態に係る認証システムにおいて、ＩＣカード２は、利用制限機器１のリーダライタ１５から供給される電力によって動作し、リーダライタ１５からのコマンドに従って処理を実行する。また、ＩＣカード２は、リーダライタ１５からのコマンドに対する処理結果を示すレスポンスをリーダライタ１５へ供給する。

[0017] 図１に示す構成例において、ＩＣカード２は、プラスチックなどで形成されたカード状の本体Ｃを有する。ＩＣカード２は、本体Ｃ内にモジュールＭおよびモジュールＭに接続された生体センサ（指紋センサ）２７を内蔵する。モジュールＭは、ＩＣチップＣａ、通信インターフェース２５およびＭＰＵ２６が接続された状態で一体的に形成され、ＩＣカード２の本体Ｃ内に埋設される。

[0018] さらに、ＩＣチップＣａは、プロセッサ２１、ＲＯＭ２２、ＲＡＭ２３及びデータメモリ２４などを備える。プロセッサ２１は、データバスなどを介してＲＯＭ２２、ＲＡＭ２３、データメモリ２４、通信インターフェース２５およびＭＰＵ２６に接続する。ＭＰＵ２６は、データバスなどを介して生体センサ２７に接続する。

なお、ＩＣカード２は、図１が示すような構成の他に必要に応じた構成を具備したり、ＩＣカード２から特定の構成が除外されたりしてもよい。

[0019] プロセッサ２１は、ＩＣカード２全体の制御を司る制御部として機能する。プロセッサ２１は、ＲＯＭ２２またはデータメモリ２４に記憶される制御プログラム及び制御データに基づいて種々の処理を行う。例えば、プロセッサ２１は、ＲＯＭ２２に記憶されているプログラムを実行することにより、ＩＣカード２の動作制御またはＩＣカード２の運用形態に応じた種々の処理を行う。

[0020] 例えば、プロセッサ２１は、プログラムを実行することにより、ＩＣカー

ド 2 内の各部の制御及び情報処理を実現するプロセッサであればよい。

なお、プロセッサ 2 1 がプログラムを実行することにより実現する各種の機能のうちの一部は、ハードウェア回路により実現されるものであっても良い。この場合、プロセッサ 2 1 は、ハードウェア回路により実行される機能を制御する。

[0021] ROM 2 2 は、予め制御用のプログラム及び制御データなどを記憶する不揮発性のメモリである。ROM 2 2 は、製造段階で制御プログラム及び制御データなどを記憶した状態で IC カード 2 に組み込まれる。例えば、ROM 2 2 に記憶される制御プログラム及び制御データは、予め IC カード 2 の仕様などに応じて組み込まれる。

[0022] RAM 2 3 は、揮発性のメモリである。RAM 2 3 は、プロセッサ 2 1 の処理中のデータなどを一時的に格納する。例えば、RAM 2 3 は、計算用バッファ、受信用バッファ及び送信用バッファとして機能する。計算用バッファは、プロセッサ 2 1 が実行する種々の演算処理の結果などを一時的に保持する。受信用バッファは、通信インターフェース 2 5 を介してリーダライタ 1 5 から受信するコマンドデータなどを保持する。送信用バッファは、通信インターフェース 2 5 を介してリーダライタ 1 5 へ送信するメッセージ（レスポンスデータ）などを保持する。

[0023] データメモリ 2 4 は、フラッシュ ROM などのデータの書き込み及び書換えが可能な不揮発性のメモリにより構成される。データメモリ 2 4 は、IC カード 2 の運用用途に応じて制御プログラム、アプリケーション及び種々のデータを格納する。例えば、データメモリ 2 4 では、プログラムファイル及びデータファイルなどが作成される。作成された各ファイルは、制御プログラム及び種々のデータなどが書き込まれる。

[0024] また、データメモリ 2 4 は、生体（指紋）認証の辞書データとして登録者の生体情報から得られる生体情報の特徴点情報（テンプレート）2 4 a を記憶する。生体情報の特徴点情報 2 4 a は、例えば、登録者の生体情報から抽出される特徴量としての特徴点情報である。データメモリ 2 4 には、登録者

ごとの生体情報の特徴点情報 24 a が記憶される。ＩＣカード 2 は、特定の 1 人の登録者に対する生体情報の特徴点情報 24 a を登録するものであっても良いし、複数の登録者に対応する複数の生体情報の特徴点情報 24 a (24 a 1、24 a 2、42 a 3、…) を登録するようにしても良い。

[0025] また、データメモリ 24 は、利用者（登録者）が使用できる利用制限機器 1 を示す管理テーブル 24 b を有する。管理テーブル 24 b は、生体情報の特徴点情報 24 a が登録される登録者に対して利用が許可されている利用制限機器との関係を示す情報が記憶される。管理テーブル 24 b は、登録者と利用制限機器の利用権限との関係を示すデータを格納するものであれば良い。例えば、管理テーブル 24 b は、登録者ごとに利用可能な利用制限機器を示す情報を格納しても良いし、利用制限機器ごとに利用権限を有する登録者を示す情報を格納しても良いし、複数の登録者と複数の利用制限機器の利用権限との対応づけを示す情報を格納しても良い。また、管理テーブル 24 b は、登録者が有する資格と各種の資格に対する利用制限機器の利用権限とを対応づけて記憶するようにしても良い。

[0026] 通信インターフェース 25 は、リーダライタ 15 とデータを送受信するためのインターフェースである。すなわち、通信インターフェース 25 は、リーダライタ 15 を通じて利用制限機器 1 とデータを送受信するためのインターフェースである。

[0027] ＩＣカード 2 が接触型のＩＣカードとして実現される場合、通信インターフェース 25 は、リーダライタ 15 と物理的かつ電氣的に接触して信号の送受信を行うための通信制御部とコンタクト部とにより構成される。例えば、ＩＣカード 2 は、コンタクト部を介してリーダライタ 15 からの動作電源及び動作クロックの供給を受けて活性化される。

[0028] ＩＣカード 2 が非接触型のＩＣカードとしての実現される場合、通信インターフェース 25 は、リーダライタ 15 との無線通信を行うための変復調回路などの通信制御部とアンテナとにより構成される。例えば、ＩＣカード 2 は、アンテナ及び変復調回路などを介してリーダライタ 15 からの電波を受

信する。ＩＣカード２は、その電波から図示しない電源部により動作電源及び動作クロックを生成して活性化する。

[0029] 生体センサ２７は、操作者の生体情報を取得する。生体センサ２７は、例えば、指紋センサである。生体センサ２７としての指紋センサは、操作者の指から指紋画像を取得する。生体センサ２７としての指紋センサは、ＣＣＤセンサなどを備える。また、指紋センサ２７は、電気容量の変化を検出するセンサなどを備えるものであってもよい。指紋センサ２７は、指紋画像をＭＰＵ２６に送信する。

以下、本実施形態では、一例としてＩＣカード２が接触型のＩＣカードである場合を想定して説明するものとするが、ＩＣカード２が非接触型のＩＣカードであっても同様に実現可能なものである。また、生体センサ２７は、指紋センサであるものとし、ＩＣカード２が利用制限機器１のリーダライタ１５にセットされた状態でユーザの指が指紋センサの読取位置に置けるようにするものとする。

[0030] ＭＰＵ２６（Micro Processing Unit）は、指紋センサ２７からの指紋画像を処理する。ＭＰＵ２６は、プロセッサ、ＲＡＭおよびＲＯＭなどを含む構成を有する。本実施形態で説明するＭＰＵ２６が実現する処理は、ＩＣチップＣａ内のプロセッサ２１がＲＯＭ２２およびＲＡＭ２３などを用いて実現できるものである。このため、以下の説明するＭＰＵ２６の実行する処理は、プロセッサ２１が実行するようにしても良い。

[0031] ＭＰＵ２６は、指紋センサ２７からの指紋画像から特徴点情報（特徴点の座標及び特徴量など示す情報）を抽出する。ＭＰＵ２６は、抽出した特徴点情報をプロセッサ２１に送信する。上述したような指紋センサ２７が取得する指紋画像から特徴点情報を抽出する処理は、プロセッサ２１が実施するようにしても良い。

[0032] プロセッサ２１は、ＭＰＵ２６から送信される指紋センサ２７で取得した指紋画像から抽出した特徴点情報とデータメモリ２４などに登録されている指紋画像の特徴点情報とを照合する。例えば、プロセッサ２１は、所定のア

ルゴリズムに従って、指紋画像同士の類似度として、指紋センサ 27 で取得した指紋画像から抽出した特徴点情報と登録されている指紋画像の特徴点情報との類似度を算出する。ここで、類似度は、高いほど指紋画像同士の類似性が高いことを示す指標である。

プロセッサ 21 は、データメモリ 24 などに登録されている指紋画像の特徴点情報を読み込んで保持する。プロセッサ 21 は、MPU 26 から送られる特徴点情報とプロセッサ 21 内に保持した特徴点情報とを照合して両者の類似度を算出する。

類似度を算出すると、プロセッサ 21 は、照合処理（認証処理）として、算出した類似度と認証用の閾値とを比較することにより認証の成否を判定する。例えば、プロセッサ 21 は、算出した類似度が認証用の閾値以上であれば同一人物である（認証成功）とし、類似度が認証用の閾値未満であれば同一人物と認めない（認証失敗）とすることにより認証処理の結果を得る。

[0033] なお、指紋センサ 27 が取得した指紋画像と登録されている指紋画像との照合処理は、MPU 26 が実施しても良い。例えば、MPU 26 は、照合処理によって指紋センサ 27 で取得した指紋画像と登録されている指紋画像と類似度を算出し、算出した類似度をプロセッサ 21 に送信するようにしても良い。また、MPU 26 は、算出した類似度と認証用の閾値とを比較することにより認証の成否をプロセッサ 21 に送信するようにしてもよい。

[0034] なお、ICカード 2 は、プロセッサ 21 からの制御に従って種々の情報を表示する表示部を具備するものであっても良い。例えば、表示部は、プロセッサ 21 からの制御に従って点灯するライト（例えば、LED（Light Emitting Diode）ライト）などであってもよい。

[0035] 次に、実施形態に係る携帯可能な認証デバイスとしての ICカード 2 が記憶する情報について説明する。

上述した構成例によれば、ICカード 2 は、データメモリ 24 において、登録者ごとの生体情報の特徴点情報 24 a と管理テーブル 24 b と記憶する。上述したように、ICカード 2 は、1 人の登録者の生体情報の特徴点情報

24 a を登録するようにしても良いし、複数の登録者に対する生体情報の特徴点情報 24 a 1、24 a 2、…を登録するようにしても良い。また、管理テーブル 24 b は、登録者と利用権限を有する利用制限機器との関係を示す情報を記憶するものであれば良い。

[0036] 以下、実施形態に係る携帯可能な認証デバイスとしての IC カード 2 に登録する登録者の生体情報の特徴点情報 24 a と管理テーブル 24 b との構成例について説明する。ここでは、具体例として、3 人の登録者（ユーザ 1、ユーザ 2、ユーザ 3）と 3 つの利用制限機器（機器 A、機器 B、機器 C）とがある場合を想定して説明するものとする。

[0037] 図 2 乃至図 4 は、個々のユーザ（登録者）ごとに発行する IC カード 2 における登録者の生体情報の特徴点情報 24 a と管理テーブル 24 b との構成例を示す図である。

図 2 は、ユーザ 1 に対して発行される IC カード（ユーザ 1 用の IC カード）2 における登録者の生体情報の特徴点情報 24 a と管理テーブル 24 b との例を示す。図 3 は、ユーザ 2 に対して発行される IC カード（ユーザ 2 用の IC カード）2 における登録者の生体情報の特徴点情報 24 a と管理テーブル 24 b との例を示す。図 4 は、ユーザ 3 に対して発行される IC カード（ユーザ 3 用の IC カード）2 における登録者の生体情報の特徴点情報 24 a と管理テーブル 24 b との例を示す。

[0038] 図 2 に示す例において、IC カード 2 のデータメモリ 24 には、ユーザ 1 の生体認証用の辞書データである登録者の生体情報の特徴点情報 24 a とユーザ 1 が利用権限を有している利用制限機器 1 を示す情報を格納する管理テーブル 24 b とが記憶される。図 2 に示す管理テーブル 24 b では、登録者の生体情報の特徴点情報 24 a を用いて生体認証が可能なユーザ 1 が機器 A と機器 C との利用権限を有することが示される。

[0039] 図 3 に示す例において、IC カード 2 のデータメモリ 24 には、ユーザ 2 の生体認証用の辞書データである生体情報の特徴点情報 24 a とユーザ 2 が利用権限を有している利用制限機器 1 を示す情報を格納する管理テーブル 2

4 b とが記憶される。図 3 に示す管理テーブル 2 4 b では、生体情報の特徴点情報 2 4 a を用いて生体認証が可能なユーザ 2 が機器 B と機器 C との利用権限を有することが示される。

[0040] 図 4 に示す例において、IC カード 2 のデータメモリ 2 4 には、ユーザ 3 の生体認証用の辞書データである生体情報の特徴点情報 2 4 a とユーザ 3 が利用権限を有している利用制限機器 1 を示す情報を格納する管理テーブル 2 4 b とが記憶される。図 3 に示す管理テーブル 2 4 b では、生体情報の特徴点情報 2 4 a を用いて生体認証が可能なユーザ 3 が機器 A と機器 C との利用権限を有することが示される。

[0041] 図 2 乃至図 4 に示す例によれば、個々のユーザ（登録者）が所持する IC カード 2 に、所持者であるユーザの生体情報の特徴点情報 2 4 a と、当該ユーザが利用可能な機器を示す情報とを登録する。これにより、所持者である登録者に対する生体認証だけでなく、当該登録者（ユーザ）が利用可能な機器を確認できる IC カード 2 を提供できる。例えば、各ユーザに ID カードなどとして生体認証機能付きの IC カードを発行する運用とする場合、図 2 乃至図 4 に示すような登録者の生体情報の特徴点情報 2 4 a と管理テーブル 2 4 b とを IC カード 2 に登録すれば、後述するような IC カード 2 における利用機器の確認とユーザの生体認証とを実現できる。

[0042] 図 5 乃至図 7 は、個々の利用制限機器ごとに発行する IC カード 2 における登録者の生体情報の特徴点情報 2 4 a と管理テーブル 2 4 b との構成例を示す図である。

図 5 は、機器 A に対して発行される IC カード（機器 A 用の IC カード）2 における登録者の生体情報の特徴点情報 2 4 a と管理テーブル 2 4 b との例を示す。図 6 は、機器 B に対して発行される IC カード（機器 B 用の IC カード）2 における登録者の生体情報の特徴点情報 2 4 a と管理テーブル 2 4 b との例を示す。図 7 は、機器 C に対して発行される IC カード（機器 C 用の IC カード）2 における登録者の生体情報の特徴点情報 2 4 a と管理テーブル 2 4 b との例を示す。

- [0043] 図5に示す例において、ICカード2のデータメモリ24には、機器Aの利用権限を有するユーザ1の生体情報の特徴点情報24a1およびユーザ2の生体情報の特徴点情報24a2とともに、機器Aの利用権限を有するユーザを示す情報を格納する管理テーブル24bとが記憶される。図5に示す管理テーブル24bでは、機器Aの利用権限を有するユーザが、生体情報の特徴点情報24a1のユーザ1と生体情報の特徴点情報24a2のユーザ2とであることが示される。
- [0044] 図6に示す例において、ICカード2のデータメモリ24には、機器Bの利用権限を有するユーザ2の生体情報の特徴点情報24a2とともに、機器Bの利用権限を有するユーザを示す情報を格納する管理テーブル24bとが記憶される。図6に示す管理テーブル24bでは、機器Bの利用権限を有するユーザが、生体情報の特徴点情報24a2のユーザ2であることが示される。
- [0045] 図7に示す例において、ICカード2のデータメモリ24には、機器Cの利用権限を有するユーザ1の生体情報の特徴点情報24a1、ユーザ2の生体情報の特徴点情報24a2およびユーザ3の生体情報の特徴点情報24a3とともに、機器Cの利用権限を有するユーザを示す情報を格納する管理テーブル24bとが記憶される。図7に示す管理テーブル24bでは、機器Cの利用権限を有するユーザが、生体情報の特徴点情報24a1のユーザ1と生体情報の特徴点情報24a2のユーザ2と生体情報の特徴点情報24a3のユーザ3とであることが示される。
- [0046] 図5乃至図7に示す例によれば、個々の利用制限機器ごとに発行（設定）するICカード2に、当該利用制限機器が利用可能なユーザと各ユーザの生体情報の特徴点情報とが登録される。これにより、各登録者に対する生体認証だけでなく、当該機器を利用可能なユーザを確認できるICカード2を提供できる。例えば、利用制限機器ごとにICカードを発行する運用とする場合、図5乃至図7に示すような登録者の生体情報の特徴点情報24aと管理テーブル24bとを各機器用のICカード2に登録すれば、後述するような

ＩＣカード２における利用機器の確認とユーザの生体認証とを実現できる。

[0047] 図８は、１つのシステムに対して発行するＩＣカード２における登録者の生体情報の特徴点情報２４ａと管理テーブル２４ｂとの構成例を示す図である。

図８は、３つの機器Ａ、Ｂ、Ｃを有するシステム全体に対して発行されるＩＣカード（マスタ用のＩＣカード）２における登録者の生体情報の特徴点情報２４ａと管理テーブル２４ｂとの例を示す。

図８に示す例において、ＩＣカード２のデータメモリ２４には、３人分の生体情報の特徴点情報２４ａ１、２４ａ２、２４ａ３と、３つの各機器に対して利用権限を有するユーザを示す情報を格納する管理テーブル２４ｂとが記憶される。

[0048] 図８に示す生体情報の特徴点情報２４ａ１、２４ａ２、２４ａ３は、それぞれユーザ１、ユーザ２、ユーザ３の生体認証用の辞書データである。また、図８に示す管理テーブル２４ｂでは、機器Ａの利用権限を有するユーザがユーザ１とユーザ２とであり、機器Ｂの利用権限を有するユーザがユーザ２とであり、機器Ｃの利用権限を有するユーザがユーザ１とユーザ２とユーザ３とであることが示される。

[0049] 図８に示す例によれば、複数の利用制限機器を含むシステム全体に対して発行（設定）するＩＣカード２に、それぞれ利用制限機器が利用可能なユーザと各ユーザの生体情報の特徴点情報とが登録される。これにより、複数の登録者に対する生体認証だけでなく、複数の機器について各機器が利用可能なユーザを確認できる１つのＩＣカード２を提供できる。例えば、複数の利用制限機器を含むシステム全体で１つのＩＣカードを発行する運用とする場合、図８に示すような登録者の生体情報の特徴点情報２４ａと管理テーブル２４ｂとをＩＣカード２に登録すれば、後述するようなＩＣカード２における利用機器の確認とユーザの生体認証とを実現できる。

[0050] なお、実施形態においては、利用制限機器を利用するごとにＩＣカード２による生体認証で人物認証を行うものであるから、図２乃至４の構成を有す

るＩＣカード、図５乃至７の構成を有するＩＣカード、図８の構成を有するＩＣカードを、それぞれ発行する運用としても良い。例えば、図２乃至４に示すような個人ごとのＩＣカードだけでなく、図８に示すようにシステム全体のＩＣカード（マスタ用のＩＣカード）を発行することで、個々のユーザ用のＩＣカードに不具合が生じた場合あるいは個々のユーザ用のＩＣカード紛失した場合にも、マスタ用のＩＣカードで利用制限機器を利用することができるような運用が実現できる。

[0051] 次に、実施形態に係る携帯可能な認証デバイスとしてのＩＣカード２を含む認証システム１０の動作例について説明する。

図９は、実施形態に係る認証システム１０の動作例について説明するためのタイミングチャートである。

ある利用制限機器１を利用しようとするユーザは、生体（指紋）認証を行うＩＣカード２を利用制限機器１のリーダライタ１５にセットする。利用制限機器１は、リーダライタ１５にセットされたＩＣカード２へ動作用の電力を供給する（ＳＴ１０）。ＩＣカード２は、通信インターフェース２５を介してリーダライタ１５から供給される電力を受けて活性化（起動）する（ＳＴ１１）。

[0052] ＩＣカード２のプロセッサ２１は、リーダライタ１５からの電力によって起動すると、初期応答をリーダライタ１５へ送信する。リーダライタ１５は、セットされたＩＣカード２へ動作用の電力を供給するとともに、ＩＣカード２からの初期応答を受信する。初期応答を受信すると、リーダライタ１５は、ＩＣカード２との相互認証を行って通信状態を確立する。利用制限機器１のプロセッサ１１は、リーダライタ１５を介したＩＣカード２との通信状態が確立すると、当該利用制限機器１の識別情報としての機器ＩＤを送信するとともに、ＩＣカード２におけるユーザの認証を要求するコマンドを送信する（ＳＴ１２）。

[0053] 利用制限機器の機器ＩＤを受信すると、ＩＣカード２のプロセッサ２１は、受信した機器ＩＤが示す利用制限機器１の利用権限を有する人物の生体情

報の特徴点情報が当該ＩＣカード２に登録されているかを確認する（ＳＴ１３）。プロセッサ２１は、管理テーブル２４ｂを参照して、当該機器１Ｄの利用制限機器に対して利用権限を有する人物の生体情報が登録されているか否かを確認することにより、当該利用制限機器１が当該ＩＣカード２を用いて利用可能な機器であるか否かを判断する（ＳＴ１４）。

[0054] 例えば、受信した機器１Ｄの機器に対する利用権限を有する人物の生体情報が登録されている場合、プロセッサ２１は、当該ＩＣカード２がセットされた利用制限機器１が利用可能な機器であるとする。また、受信した機器１Ｄの機器に対する利用権限を有する人物の生体情報が登録されていない場合、プロセッサ２１は、当該ＩＣカード２がセットされた利用制限機器１が利用できない機器であるとする。

[0055] すなわち、利用制限機器１の利用権限を有する登録者がＩＣカード２に登録されていないと判断した場合（ＳＴ１４、ＮＯ）、プロセッサ２１は、利用制限機器１が利用不可な機器である旨を利用制限機器１へ応答する（ＳＴ２０）。この場合、ＩＣカード２がセットされた利用制限機器１は、上述のような利用不可な機器である旨の応答を受けて処理部１６による処理を実行不可な状態とする。

[0056] 利用制限機器１の利用権限を有する登録者がＩＣカード２に登録されていると判断した場合（ＳＴ１４、ＹＥＳ）、プロセッサ２１は、ＭＰＵ２６を通じて生体センサとしての指紋センサ２７を起動させ、指紋センサ２７によりユーザの生体情報としての指紋画像を取得させる（ＳＴ１５）。ここで、ユーザは、認証に用いる指紋がある指を指紋センサ２７の読取位置に置くものとする。また、ＭＰＵ２６は、指紋センサ２７の読取位置に指が置かれたのを検知して指紋センサ２７によって指紋画像を読取るようにしても良い。

[0057] 指紋センサ２７が指紋画像を取得すると、プロセッサ２１およびＭＰＵ２６は、取得した指紋画像を用いて生体（指紋）認証を行う（ＳＴ１６）。例えば、ＭＰＵ２６は、指紋センサ２７が取得した指紋画像から特徴点情報を抽出し、抽出した特徴点情報をプロセッサ２１に送信する。これにより、プ

ロセッサ 21 は、MPU 26 から指紋センサ 27 で読み取ったユーザの指紋画像の特徴点情報を取得する。

[0058] 指紋画像の特徴点情報を取得すると、プロセッサ 21 は、取得したユーザの指紋画像の特徴点情報とデータメモリ 24 に登録している登録者の指紋画像の特徴点情報とを照合する。プロセッサ 21 は、ユーザの指紋画像の特徴点情報と登録者の指紋画像の特徴点情報との類似度を算出し、算出した類似度が認証用の閾値以上であるか否かによりユーザが登録者であるか否かを判定する。

[0059] 指紋認証によってユーザが登録者であると認められた場合（生体認証が成功した場合）、プロセッサ 21 は、登録者と一致したユーザ（つまり、登録者）が機器 1D で示される利用制限機器 1 の利用権限を有するか否かを判定する（ST17）。ユーザが当該利用制限機器 1 の利用権限を有する登録者であると認証された場合（ST17、YES）、プロセッサ 21 は、指紋センサ 27 に指を置いたユーザが機器 1D で示される利用制限機器 1 を利用できる登録者であることが認証された旨を通信インターフェース 25 により利用制限機器 1 のリーダライタ 15 へ応答する（ST18）。

[0060] リーダライタ 15 によってユーザが登録者であることが認証された旨の応答を IC カード 2 から受信した場合、利用制限機器 1 のプロセッサ 11 は、処理部 16 の動作を許可し、ユーザが要求する処理を実行可能な状態とする（ST19）。この場合、利用制限機器 1 のプロセッサ 11 は、IC カード 2 における認証の結果によって利用を許可したユーザを示す情報とともに、当該ユーザが実行した利用内容を示す履歴情報をメモリ 14 に記録する（ST20）。

[0061] また、ユーザが当該利用制限機器 1 の利用権限を有する登録者であると判定できなかった場合（ST17、NO）、プロセッサ 21 は、利用権限を有するユーザであることが確認できなかった旨、又は、利用制限機器 1 が利用不可である旨を利用制限機器 1 へ応答とする（ST21）。

[0062] ユーザが登録者であることが認証できなかった旨、又は、利用制限機器 1

が利用不可な機器である旨の応答をＩＣカード２から受信した場合、利用制限機器１のプロセッサ１１は、処理部１６の動作を不可として、当該ユーザが利用制限機器１を利用できない状態とする（ＳＴ２２）。この場合、利用制限機器１のプロセッサ１１は、ＩＣカード２における認証の結果によって利用を不可とした旨の履歴情報をメモリ１４に記録するようにしても良い。

[0063] 以上のような処理によれば、生体センサを具備する携帯可能な認証デバイスとしてのＩＤカードは、利用制限機器との通信接続した場合、当該ＩＣカードに登録されている登録者が当該利用制限機器の利用権限を有するかを確認し、ユーザが利用制限機器の利用権限を有する登録者であることを生体センサが取得する生体認証によって確認する。

[0064] これにより、利用制限機器または利用制限機器の上位装置が各ユーザの利用権限を管理しなくても、ＩＣカードが、利用権限がない人物による利用を防止でき、かつ、生体認証によってユーザが利用権限を有する人物であることを確認できる。この結果として、ＩＣカードが、機器の利用確認を確実に行えるとともに、生体認証によるなりすまし防止できるため、利用権限がある人物の確実な利用制限機器の使用が実現できる。

[0065] 例えば、利用制限機器が処理部で医療行為（医療処理）を行う医療機器である場合、ＩＣカードは、ユーザの当該機器に対する利用権限の確認と、ユーザが利用権限を有する登録者（患者又は特定の操作者）本人であることを生体情報で確認する生体認証とを実行する。これにより、ＩＣカードが、利用制限機器に対して利用権限がある人物との生体認証が成功した場合に利用制限機器による医療処理を実行することを許可することでき、登録者に対応づけられた正しい利用制限機器による医療処理を確実に提供するようにできる。

[0066] （変形例）

上述した実施形態では、ＩＣカードに生体情報の特徴点情報が登録されている登録者が機器ＩＤで特定される機器の利用権限を有するか否かを確認したが、機器ＩＤで特定される機器を利用する資格を登録者が有しているか否

かを確認するようにしても良い。この場合、ＩＣカード２の管理テーブル２４ｂには、登録者が有する資格を示す情報と各利用制限機器の利用が許可される資格を示す情報が記憶される。

以下、上述した実施形態の変形例として、ユーザが有する資格に基づいて利用制限機器が利用可能な否かを確認する例について説明する。

なお、変形例に係る認証システム１０は、管理テーブル２４ｂ以外の構成は上述した実施形態と同様な構成で実現できるため、詳細な説明を省略するものとする。

[0067] 図１０は、資格情報を基に利用制限機器の利用権限を確認する場合のＩＣカード２における登録者の生体情報の特徴点情報２４ａと管理テーブル２４ｂとの構成例を示す図である。

図１０に示す構成例において、ＩＣカード２のデータメモリ２４には、３人分の生体情報の特徴点情報２４ａ１、２４ａ２、２４ａ３と、第１テーブル２４ｂ１および第２テーブル２４ｂ２からなる管理テーブル２４ｂとが記憶される。第１テーブル２４ｂ１は、各利用制限機器（機器Ａ、Ｂ、Ｃ）を利用する場合に必要な資格を示す情報が格納される。第２テーブル２４ｂ２は、各登録者（ユーザ１、２、３）が有する資格を示す情報が格納される。

[0068] 図１０に示す例によれば、機器Ａは、利用に必要な資格が α であることが第１テーブル２４ｂ１から判別でき、資格 α を有するユーザがユーザ１とユーザ３であることが第２テーブル２４ｂ２から判別できる。つまり、図１０に示すＩＣカード２のプロセッサ２１は、管理テーブル２４ｂを参照することにより、ユーザ１およびユーザ３が機器Ａの利用権限を有することが特定できる。

[0069] 図１０に示す例において、機器Ｂは、利用に必要な資格が β であることが第１テーブル２４ｂ１から判別でき、資格 β を有するユーザがユーザ２であることが第２テーブル２４ｂ２から判別できる。つまり、図１０に示すＩＣカード２のプロセッサ２１は、管理テーブル２４ｂを参照することにより、ユーザ２が機器Ｂの利用権限を有することが特定できる。

[0070] 図10に示す例において、機器Cは、利用に必要な資格が α 又は β であることが第1テーブル24b1から判別でき、資格 α を有するユーザがユーザ1およびユーザ3で資格 β を有するユーザがユーザ3であることが第2テーブル24b2から判別できる。つまり、図10に示すICカード2のプロセッサ21は、管理テーブル24bを参照することにより、ユーザ1、2、3が機器Cの利用権限を有することが特定できる。

[0071] また、変形例に係る認証システムは、上述した図9に示す処理と同様な流れで同様な処理が実現できる。ただし、図9におけるST13の処理は、上述したように、図10に示すような管理テーブル24bに登録される情報を参照して、ICカードがセットされた利用制限機器が利用可能な機器であるかを登録者の資格に基づいて確認するようにすればよい。

以上のような変形例によれば、複数の登録者に対する生体認証だけでなく、各登録者が有する資格に基づいて各機器が利用可能なユーザを確認できる携帯可能な認証デバイスとしてのICカードを提供できる。

[0072] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。