

明 細 書

発明の名称： 認証デバイスおよび認証システム

技術分野

[0001] 本発明の実施形態は、認証デバイスおよび認証システムに関する。

背景技術

[0002] 近年、生体情報を用いた本人認証によって機器や電子鍵などのセキュリティを実現するシステムがある。例えば、カメラに着脱可能なレンズは、非常に高価なものがあるため、盗難あるいは第三者による無断使用などを防止する必要がある。このため、従来、レンズに指紋センサを取り付け、指紋による本人認証によってレンズの使用を可能とするものが提案されている。

[0003] しかしながら、従来のレンズに取り付けた指紋センサを用いた本人認証では、セキュリティが強固になる一方で使い勝手が悪くなるという問題がある。例えば、レンズを他人へ一時的に貸与したり譲渡したりする場合、使用者の指紋データの削除および再登録などの手続きを実施しなければならず利便性が低い。また、指紋データが登録済みの使用者（所有者）であっても、レンズの使用または取外しを行う場合には毎回レンズ自体に取り付けた指紋センサに指紋を読み取らせる操作を行う必要があるため、操作性が良いとはいえないことがある。

先行技術文献

特許文献

[0004] 特許文献1：日本国特開2012-159627号公報

発明の概要

発明が解決しようとする課題

[0005] 上記の課題を解決するため、生体情報による本人認証を用いた利便性の良いセキュリティを実現する認証デバイス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

[0006] 実施形態によれば、認証デバイスは、機器本体インターフェースとメモリ

と生体センサとプロセッサとを有する。機器本体インターフェースは、ロック機構を制御する機器本体と通信する。メモリは、ロック機構によるロックを解除する権限を有する登録者の生体情報を記憶する。生体センサは、操作者の生体情報を取得する。プロセッサは、生体センサにより取得する生体情報とメモリが記憶する登録者の生体情報とが同一人物の生体情報と判断した場合、操作者が登録者であることを生体情報で認証したことを機器本体インターフェースにより機器本体へ送信し、ロック機構への制御を促す。

図面の簡単な説明

[0007] [図1]図1は、実施形態に係る認証デバイス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、実施形態に係る認証デバイスにおける制御系の構成例を示すブロック図である。

[図3]図3は、実施形態に係る認証システムにおける第1の登録処理を説明するためのタイミングチャートである。

[図4]図4は、実施形態に係る認証システムにおける第2の登録処理を説明するためのタイミングチャートである。

[図5]図5は、実施形態に係る認証システムにおける第1の認証処理を説明するためのタイミングチャートである。

[図6]図6は、実施形態に係る認証システムにおける第2の認証処理を説明するためのタイミングチャートである。

[図7]図7は、実施形態に係る認証システムにおける第1の一時利用処理を説明するためのタイミングチャートである。

[図8]図8は、実施形態に係る認証システムにおける第2の一時利用処理を説明するためのタイミングチャートである。

[図9]図9は、実施形態に係る認証システムの機器本体における一時利用処理の設定情報に応じた制御動作を説明するためのフローチャートである。

[図10]図10は、実施形態に係る認証システムにおける第1の削除処理を説明するためのタイミングチャートである。

[図11]図 1 1 は、実施形態に係る認証システムにおける第 2 の削除処理を説明するためのタイミングチャートである。

[図12]図 1 2 は、実施形態に係る認証システムにおける第 1 の譲渡処理を説明するためのタイミングチャートである。

[図13]図 1 3 は、実施形態に係る認証システムにおける第 2 の譲渡処理を説明するためのタイミングチャートである。

実施形態

[0008] 以下、実施形態について、図面を参照して説明する。

図 1 は、実施形態に係る認証システムの構成例を示すブロック図である。

図 1 に示すように、認証システムは、情報端末 1、認証デバイス 2、パーツ 4 の脱着が可能な機器本体 3などを有する。認証システムは、指紋の画像（指紋画像）などの生体情報を用いて人物を認証し、生体情報を用いた人物の認証に応じて機器本体 3 又はパーツ 4 の動作を制御するシステムである。

[0009] 情報端末 1 は、認証デバイス 2 と通信可能な情報処理装置である。例えば、情報端末 1 は、スマートフォン、あるいは、タブレット P C などの携帯端末である。情報端末 1 は、認証デバイス 2 に通信接続し、認証デバイス 2 に対して動作指示を供給するものであれば良い。

[0010] 認証デバイス 2 は、人物（操作者）の生体情報を取得し、取得した生体情報に基づいて人物の認証を行う。認証デバイス 2 は、生体認証のために設計されたデバイスであり、情報端末 1 および機器本体 3 とは別の筐体で構成される。認証デバイス 2 は、通信接続する情報端末 1 または機器本体 3 からの要求に応じて生体認証を実行する。

[0011] 機器本体 3 は、データ処理および通信などの機能を実現する電子機器を含む機器である。例えば、機器本体 3 は、制御用の電子機器を具備するカメラである。本実施形態において、機器本体 3 は、パーツ 4 としてのレンズが脱着可能なカメラであるものとする。機器本体 3 としてのカメラは、取り付けられたパーツ 4 としてのレンズと電氣的に接続してレンズが具備する制御チップから識別情報（パーツ I D）などを含むレンズ情報を取得する。また、

カメラなどの機器本体 3 は、レンズなどのパーツ 4 が取り付け可能な構成を有し、取り付けられたレンズなどのパーツ 4 をロックするロック機構（後述する）を具備する。機器本体（カメラ） 3 は、ロック機構によるロックが解除された状態において人的な操作によってレンズ 4 が取り外せるようになっている。

[0012] 次に、実施形態に係る認証システムにおける情報端末 1 の構成について説明する。

図 1 に示すように、情報端末 1 は、制御部 11、通信部およびユーザインターフェース（UI） 13 を有する。

制御部 11 は、プロセッサ、各種メモリおよびインターフェースを有する。制御部 11 は、プロセッサがメモリに記憶したプログラムを実行することによりインターフェースを介して接続された各部を制御する。本実施形態において、制御部 11 は、メモリにインストールした専用のアプリケーションプログラムをプロセッサが実行することにより、認証デバイスへの動作指示を実行する。

[0013] 通信部 12 は、認証デバイス 2 と通信するための通信インターフェース（認証デバイスインターフェース）である。通信部 12 は、無線通信であっても良いし、有線通信であっても良い。例えば、通信部 12 は、有線又は無線の LAN（Local Area Network）接続をサポートするものであり、Ethernet（登録商標）、Wi-Fi、BLE、LTE（登録商標）などの様々な通信規格に準拠した有線または無線のインターフェースを採用することができる。

[0014] ユーザインターフェース 13 は、ユーザが入力する情報を取得したりユーザに情報を報知したりするものである。UI 13 は、例えば、操作部としてのタッチパネルを有する表示装置である。また、UI 13 としては、音声を出力するスピーカあるいは音声を入力するマイクなどを具備するものであっても良い。

[0015] 次に、実施形態に係る認証システムにおける機器本体（カメラ） 3 およびパーツ（レンズ） 4 の構成例について説明する。

機器本体 3 は、機器本体（例えば、カメラ）の本来の構成に加えて、図 1 に示すように、制御部 3 1、接続インターフェース 3 1 a、通信部 3 2、ユーザインターフェース（UI） 3 3、および、ロック機構 3 4 を有する。

[0016] 制御部 3 1 は、プロセッサ、各種メモリおよびインターフェースを有する。制御部 3 1 は、プロセッサがメモリに記憶したプログラムを実行することによりインターフェースを介して接続された各部を制御する。例えば、制御部 3 1 は、認証デバイス 2 へ生体認証を要求したり認証デバイス 2 からの生体認証の結果を受けたりする。制御部 3 1 は、ロック機構 3 4 を制御することによりパーツ 4 を取外し可能としたり取外し不可としたりする。

[0017] 制御部 3 1 は、接続インターフェース 3 1 a を介してパーツ 4 と電氣的に接続する。接続インターフェース 3 1 a は、パーツ 4 との間でデータの送受信ができるように電氣的に接続するためのインターフェースである。例えば、接続インターフェース 3 1 a は、所定位置に取り付けたパーツ 4 に設けたコネクタと接触するコネクタを含む構成とする。

[0018] 通信部 3 2 は、認証デバイス 2 と通信するための通信インターフェース（認証デバイスインターフェース）である。通信部 3 2 は、無線通信であっても良いし、有線通信であっても良い。例えば、通信部 3 2 は、ブルートゥース（登録商標）などの無線通信のインターフェースで実現される。

[0019] ユーザインターフェース 3 3 は、ユーザが入力する情報を取得したりユーザに情報を報知したりするものである。ユーザインターフェース 3 3 は、例えば、操作部としてのタッチパネルを有する表示装置である。機器本体 3 がカメラであれば、ユーザインターフェース 3 3 は、レンズ 4 を介して撮像部に入力している画像あるいは撮影した画像を表示するタッチパネル付きの表示装置であっても良い。また、ユーザインターフェース 3 3 としては、音声を出力するスピーカあるいは音声を入力するマイクなどを含むものであっても良い。

[0020] ロック機構 3 4 は、機器本体 3 に取り付けられたパーツ 4 を保持する機構である。ロック機構 3 4 は、制御部 3 1 からの制御信号によってパーツ 4 を取外

し可能としたりパーツ4の取外しを不可としたりする。例えば、ロック機構34は、解除ボタン34aを有し、解除ボタン34aを押下げた状態でパーツ4が取り外しできるようにするものとする。この場合、ロック機構34は、制御部31からの制御信号によって、解除ボタン34aを有効（押下可能）としてパーツ4が取外しできるようにしたり、解除ボタン34aを無効（押下不可）としてパーツ4の取外しを不可としたりする。

[0021] また、パーツ4は、パーツ本来の構成に加えて、図1に示すように、制御チップ41および接続インターフェース41aを有する。

制御チップ41は、プロセッサ、各種メモリおよびインターフェースを有する。制御チップ41は、例えば、メモリに保持した当該パーツ（レンズ）の識別情報（パーツID）を含むパーツ（レンズ）情報を機器本体3へ出力する制御を行う。

[0022] パーツ4における制御チップ41のプロセッサは、接続インターフェース41aを介して機器本体3の制御部31と通信するように構成される。接続インターフェース41aは、機器本体3と電氣的に接続するためのインターフェースである。例えば、接続インターフェース41aは、機器本体3の所定位置に取り付けた状態で機器本体3に設けられているコネクタと接触するコネクタである。

[0023] 次に、実施形態に係る認証デバイス2の構成について説明する。

図2は、実施形態に係る認証デバイス2の構成例を示すブロック図である。

図2に示すように、認証デバイス2は、プロセッサ21、ROM22、RAM23、データメモリ24、第1通信部25、第2通信部26、生体センサ27、MPU28およびバッテリー29を有する。

[0024] 認証デバイス2は、例えば、プロセッサ21、ROM22、RAM23、データメモリ24、第1通信部25、第2通信部26、生体センサ27およびMPU28を収納し、生体センサ27を外面に露出させる筐体で形成される。認証デバイス2としての筐体は、生体情報（指先の指紋画像）が読取可

能な生体センサ２７が露出できる大きさであれば小型化が可能であり、例えば、数センチ角程度の大きさで実現できる。

[0025] プロセッサ２１は、認証デバイス２の動作に必要な処理および制御を行う。プロセッサ２１は、例えば、ＲＯＭ２２又はデータメモリ２４に記憶されたプログラムを実行することにより認証デバイス２の各種の処理機能を実現する。プロセッサ２１は、認証デバイス２内の各部を制御する。例えば、プロセッサ２１は、生体センサ２７で取得した生体情報と予めデータメモリ２４に登録されている生体情報とを照合する。

[0026] プロセッサ２１は、例えば、ＣＰＵ（Central Processing Unit）、ＳｏＣ（System on a Chip）、ＤＳＰ（Digital Signal Processor）又はＧＰＵ（Graphics Processing Unit）でもよい。または、プロセッサ２１は、これらの組み合わせであってもよい。

なお、プロセッサ２１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２１は、ハードウェア回路により実行される機能を制御する。

[0027] ＲＯＭ２２は、予め制御用のプログラムおよび制御データなどを記憶する不揮発性のメモリである。ＲＯＭ２２は、製造段階で制御プログラムおよび制御データなどを記憶した状態で認証デバイス２に組み込まれる。即ち、ＲＯＭ２２に記憶される制御プログラムおよび制御データは、予め認証デバイス２の仕様などに応じて組み込まれる。

[0028] ＲＡＭ２３は、揮発性のメモリである。ＲＡＭ２３は、プロセッサ２１の処理中のデータなどを一時的に格納する。例えば、ＲＡＭ２３は、計算用バッファ、受信用バッファおよ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２１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、第１の通信部２５または第２の通信部２６を介して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、第１の通信部２５または第２の通信部２６により送信するメッセージ（レスポンスデ

ータ)などを保持する。

[0029] データメモリ24は、書き換え可能な不揮発性メモリで構成する。データメモリ24は、データを格納するメモリおよび暗号ロジック回路などを含むものであっても良い。データメモリ24は、予め登録された生体情報(ここでは、指紋)や、生体情報から特徴点を抽出したデータを暗号化して記憶する。以下では、生体情報から特徴点を抽出したデータを含めて生体情報という。また、データメモリ24は、セキュアにデータを保持するセキュアエレメントを含む。例えば、データメモリ24のセキュアエレメントは、生体情報を暗号化して記憶する。

[0030] 第1の通信部25は、情報端末1と通信するための通信インターフェース(情報端末インターフェース)である。例えば、第1の通信部25としての通信インターフェースは、有線又は無線のLAN(Local Area Network)接続をサポートする通信規格に準拠した有線または無線のインターフェースを採用することができる。

第2の通信部26は、機器本体3と通信するための通信インターフェース(機器本体インターフェース)である。例えば、第2の通信部26は、例えば、ブルートゥースなどの近距離無線通信によって機器本体3と通信するインターフェースで実現しても良い。

なお、第1の通信部25および第2の通信部26は、1つの通信インターフェースで実現しても良いし、異なる通信インターフェースで実現しても良い。

[0031] 生体センサ27は、ユーザの生体情報を読取るセンサで構成される。生体センサ27は、ユーザの生体情報として手指のいずれかの指から指紋を取得する。なお、生体センサ27は、指紋以外の生体情報を取得するものであってもよく、例えば、指の静脈パターンを画像データとして取得する静脈センサであってもよい。

例えば、生体センサ27としての指紋センサは、ユーザの指から指紋画像を取得する。指紋センサは、テンプレートを生成するための指紋画像を取得

する。例えば、指紋センサは、ＣＣＤセンサなどを備える。また、指紋センサは、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。指紋センサは、指紋画像をＭＰＵ２８に送信する。

[0032] ＭＰＵ２８（Micro Processing Unit）は、生体センサ２７からの生体情報を含むデータを処理する。例えば、ＭＰＵ２８は、生体センサ２７としての指紋センサからの指紋画像を処理する。ＭＰＵ２８は、指紋センサからの指紋画像から特徴点情報（特徴点の座標および特徴量など示す情報）を抽出する。ＭＰＵ２８は、抽出した特徴点情報をプロセッサ２１に送信する。

[0033] また、ＭＰＵ２８は、生体センサ２７からの生体情報の照合処理を行う。例えば、ＭＰＵ２８は、生体センサ２７としての指紋センサからの指紋画像の照合処理を行う。この場合、ＭＰＵ２８は、指紋画像同士の類似度を算出する。ＭＰＵ２８は、算出した類似度をプロセッサ２１に送信する。ここでは、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。

[0034] 例えば、ＭＰＵ２８は、各指紋画像の特徴点情報を抽出する。ＭＰＵ２８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、抽出した特徴点情報同士の類似度を算出する。ＭＰＵ２８は、算出した類似度をプロセッサ２１に送信する。また、ＭＰＵ２８は、テンプレートと指紋画像との照合処理を行う。例えば、ＭＰＵ２８は、テンプレートと指紋画像との類似度を算出しプロセッサ２１に送信してもよい。また、ＭＰＵ２８は、照合の成否をプロセッサ２１に送信してもよい。

バッテリー２９は、認証デバイス２の各部に電力を供給する。バッテリー２９は、例えば、二次電池である。バッテリー２９は、ＵＳＢ端子からの有線による給電としてもよい。

なお、認証デバイス２は、動作状態などを報知する表示器あるいはスピーカなどを具備しても良い。表示器は、例えば、ＬＥＤ（Light Emitting Diode）であっても良いし、小型の表示装置などで実現しても良い。

[0035] 上記のように、認証デバイス２は、プロセッサ２１がＲＯＭ２２又はＮＶ

M 2 4 などに格納されるプログラムを実行することで動作する。本実施形態では、認証デバイス 2 は、生体情報としての指紋による人物の認証を M P U 2 8 によって実現するものとする。ただし、生体情報による人物の認証処理は、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ようにしても良い。

[0036] 以下、実施形態に係る認証デバイス 2 を含む認証システムの動作について説明する。

まず、認証システムにおいて認証デバイス 2 に生体情報を登録する登録処理の第 1 の動作例（第 1 の登録処理）について説明する。

図 3 は、実施形態に係る認証システムにおける第 1 の登録処理を説明するためのタイミングチャートである。

ここで、第 1 の登録処理は、管理者が操作するスマートフォンなどの情報端末 1 からの要求に応じて機器本体 3 に取り付けるパーツ 4 の使用権限を有する者（使用権限者）の生体情報を認証デバイス 2 に登録するものとする。

[0037] まず、管理者は、情報端末 1 のユーザインターフェース 1 3 を操作することにより生体情報の登録を指示する。例えば、管理者は、ユーザインターフェース 1 3 で管理対象を識別する識別情報として、管理対象とするパーツ 4 に付与される識別情報（パーツ I D）を入力し、当該パーツ 4 に対する使用権限者の生体情報の登録を指示する。なお、識別情報は、機器本体の識別情報（機器 I D）を含むものであっても良いし、パーツ I D と機器 I D とを含むものであっても良い。また、管理者は、識別情報と共にユーザ名などの使用権限者（登録者）のユーザ情報を入力するようにしても良い。

[0038] 情報端末 1 の制御部 1 1 は、ユーザインターフェース 1 3 により入力される識別情報を取得し（S T 1 1）、識別情報に対応する生体情報の登録指示を受け付ける。生体情報の登録指示を受け付けると、制御部 1 1 は、通信部 1 2 により認証デバイス 2 と通信接続し、取得した識別情報に対応づけて生体情報を登録することを要求するコマンドを認証デバイス 2 へ送信する（S T 1 2）。ここで、制御部 1 1 は、登録者に対して認証デバイス 2 の生体

ンサ 27 における読取位置に指紋が形成されている指を置くようにユーザインターフェース 13 を用いて案内しても良い。

[0039] 認証デバイス 2 は、第 1 の通信部 25 により情報端末 1 からのコマンドを受信する。認証デバイス 2 のプロセッサ 21 は、情報端末 1 から受信したコマンドが生体情報の登録を要求するコマンドである場合、生体情報の登録処理を実行する。登録処理において、プロセッサ 21 は、生体センサ 27 および MFP 28 を用いて登録者の生体情報としての指紋画像を取得する。

[0040] ここで、生体情報を登録する者（登録者）は、生体センサ 27 における所定の読取位置に指紋が形成されている指を置くものとする。本実施形態において、生体情報の登録対象となる人物（登録者）は、パーツ 4 の使用が許可されるべき人物（例えば所有者）であるものとする。なお、生体情報が登録される登録者は、情報端末 1 を操作している管理者と同一人物であっても良いし、別の人物であっても良い。後者の場合、登録者ではない管理者が情報端末 1 で遠隔操作しながら、登録者に生体情報の登録を実行させるような運用が実現できる。

[0041] 生体センサ 27 は、プロセッサ 21 からの指示に応じて起動する。起動した生体センサ 27 は、所定の読取位置に置かれた人物の指から指紋画像を含む読取画像を取得する（ST13）。生体センサ 27 は、取得した読取画像を MPU 28 に送信する。MPU 28 は、生体センサ 27 から読取画像から指紋画像を取得する。MPU 28 は、取得した指紋画像における特徴点情報を抽出する（ST14）。MPU 28 は、抽出した特徴点情報を登録者の生体情報としてプロセッサ 21 に送信する。

[0042] プロセッサ 21 は、MPU 28 から指紋画像の特徴点情報を取得する。登録者の指紋画像の特徴点情報を取得すると、プロセッサ 21 は、取得した指紋画像の特徴点情報に基づいてテンプレート（生体認証用の特徴点を抽出したデータ）を生成する。例えば、プロセッサ 21 は、所定のアルゴリズムに従って、指紋画像の特徴点情報からテンプレートを生成する。

[0043] ここで、プロセッサ 21 は、指紋画像の特徴点情報を取得した後に、再び

上記の動作を繰り返すようにしても良い。上記の動作を繰り返すことで、プロセッサ 21 は、複数の指紋画像の特徴点情報を取得し、収集した複数の指紋画像の特徴点情報に基づいてテンプレートを生成するようにしても良い。複数の指紋画像の特徴点情報は 1 人の登録者から多少のばらつきをもって収集したものとなるから、複数の指紋画像の特徴点情報に基づくテンプレートは生体認証における精度の向上が期待できるものとなる。

[0044] 生体認証用のテンプレートを生成すると、プロセッサ 21 は、生成したテンプレートを識別情報に対応づけてデータメモリ 24 に保存（登録）する（ST15）。また、プロセッサ 21 は、生成したテンプレートを MPU 28 が具備するメモリに格納するようにしても良い。

[0045] テンプレートを登録すると、プロセッサ 21 は、第 1 通信部 25 を通じて指定された識別情報に対応するテンプレートとして使用権限者（登録者）の生体情報を登録できたことを示すレスポンスを情報端末 1 へ送信する（ST16）。

情報端末 1 の制御部 11 は、通信部 12 を介して認証デバイス 2 から登録が完了したことを示すレスポンスを受信すると、ユーザインターフェース 13 を用いて登録完了を管理者（情報端末 1 の操作者）へ報知する（ST17）。

[0046] また、認証デバイス 2 のプロセッサ 21 は、第 2 通信部 26 を通じて使用権限者の生体情報としてのテンプレートの登録が完了したことを機器本体 3 にも通知する（ST16）。これに対して、機器本体 3 は、通信部 32 により生体情報の登録完了の通知を受信する。機器本体 3 の制御部 31 は、生体情報の登録完了の通知を受けると、パーツ 4 に対する使用権限者の生体情報が登録済みであることを記録する（ST18）。例えば、制御部 31 は、制御部 31 内のメモリにパーツ 4 に対する使用権限者の生体情報が認証デバイス 2 に登録されていることを示す情報を記憶する。制御部 31 は、生体情報が登録済みであることが記録されている場合、パーツ 4 の取外しには本人認証が必要であると判定するようにしても良い。

[0047] 次に、認証システムにおいて認証デバイス2に生体情報を登録する登録処理の第2の動作例（第2の登録処理）について説明する。

図4は、実施形態に係る認証システムにおける第2の登録処理を説明するためのタイミングチャートである。

ここで、第2の登録処理は、ユーザ（使用者）が操作する機器本体3からの要求に応じて機器本体3の利用者となる人物の生体情報を認証デバイス2に生体情報を登録するものとする。機器本体3の制御部31は、取り付けられたパーツ4の制御チップ41からパーツIDを含むパーツ情報を取得する機能および認証デバイス2に生体情報の登録あるいは認証を要求する機能を有するものとする。

[0048] まず、使用者は、パーツ4を取り付けた状態の機器本体3においてユーザインターフェース33を操作することにより生体情報の登録を指示する。生体情報の登録を指示した使用者（登録者）は、認証デバイス2における生体センサ27の読取位置に登録する指紋が形成されている指を置く。

[0049] 機器本体3の制御部31は、取り付けられたパーツ4の制御チップ41と接続インターフェース31aを介して通信し、当該パーツ4の識別情報としてのパーツIDを含むパーツ情報を取得する（ST21）。制御部31は、生体情報の登録が指示された場合にパーツ4の制御チップ41と通信してパーツ情報を取得するようにしても良い。また、制御部31は、パーツ4が取り付けられた際にパーツ情報を取得し、取得したパーツ情報をメモリに保持しておくようにしても良い。この場合、制御部31は、生体情報の登録が指示された場合にメモリに保持しているパーツ情報を読み出すようにすれば良い。

[0050] パーツ情報を取得すると、制御部31は、通信部32により認証デバイス2と通信接続する。制御部31は、認証デバイス2との通信接続が確立すると、取得したパーツIDを含む識別情報に対応づけて使用権限者の生体情報の登録を要求するコマンドを認証デバイス2へ送信する（ST22）。識別情報は、パーツIDと機器本体3の識別情報とを含む情報であって良い。

[0051] 認証デバイス 2 は、第 2 の通信部 2 6 により機器本体 3 からの生体情報の登録を要求するコマンドを受信する。認証デバイス 2 のプロセッサ 2 1 は、機器本体 3 から生体情報の登録を要求するコマンドを受信した場合、上述した S T 1 3 - 1 5 の処理と同様に、生体情報の登録処理を実行する。

[0052] すなわち、プロセッサ 2 1 は、生体センサ 2 7 を用いて登録者の生体情報としての指紋画像を取得する。例えば、プロセッサ 2 1 は、M P U 2 8 などを通じて生体センサ 2 7 を起動させる。プロセッサ 2 1 からの指示に応じて起動した生体センサ 2 7 は、所定の読取位置に置かれた人物の指から指紋画像を含む読取画像を取得する（S T 2 3）。

[0053] 生体センサ 2 7 は、取得した読取画像を M P U 2 8 に送信する。M P U 2 8 は、生体センサ 2 7 から取得する読取画像から指紋画像を抽出し、抽出した指紋画像における特徴点情報を抽出する（S T 2 4）。M P U 2 8 は、抽出した特徴点情報を登録者の生体情報としてプロセッサ 2 1 に送信する。これにより、プロセッサ 2 1 は、M P U 2 8 から指紋画像の特徴点情報を取得する。

[0054] 登録者の指紋画像の特徴点情報を取得すると、プロセッサ 2 1 は、取得した指紋画像の特徴点情報に基づいてテンプレート（生体認証用の特徴点を抽出したデータ）を生成する。ここで、プロセッサ 2 1 は、複数の指紋画像の特徴点情報を取得し、収集した複数の指紋画像の特徴点情報に基づいてテンプレートを生成するようにしても良い。生体認証用のテンプレートを生成すると、プロセッサ 2 1 は、生成したテンプレートを識別情報に対応づけてデータメモリ 2 4 あるいは M P U 2 8 に保存（登録）する（S T 2 5）。

[0055] テンプレートを登録すると、プロセッサ 2 1 は、第 2 通信部 2 6 を通じてパーツ 4 に対する使用権限者の生体情報としてのテンプレートの登録が完了したことを示すレスポンスを機器本体 3 へ送信する（S T 2 6）。

機器本体 3 の制御部 3 1 は、通信部 3 2 を介して認証デバイス 2 から登録が完了したことを示すレスポンスを受信する。制御部 3 1 は、登録が完了したことを示すレスポンスを受信すると、パーツ 4 に対する使用権限者の生体

情報が登録済みであることを記録する（ST28）。例えば、制御部31は、制御部31内のメモリにパーツ4に対する使用権限者の生体情報が認証デバイス2に登録されていることを示す情報を記憶する。制御部31は、生体情報が登録済みであることが記録されている場合、パーツ4の取外しには本人認証が必要であると判定するようにしても良い。

[0056] また、機器本体3の制御部31は、認証デバイス2から生体情報の登録が完了したことを示すレスポンスを受信した場合、ユーザインターフェース33を用いて生体情報の登録完了を報知するようにしても良い。

[0057] 以上のように、実施形態に係る認証システムは、第1または第2の登録処理によって、認証デバイスに機器本体に取り付けられるパーツの使用者の生体情報を登録できる。また、第1の登録処理では、情報端末からの指示によって認証デバイスにパーツの使用権限者（ロックを解除する権限を有する者）の生体情報が登録される。また、第2の登録処理では、機器本体からの指示によって認証デバイスに当該機器本体に装着されているパーツの使用権限者（ロックを解除する権限を有する者）の生体情報が登録される。

[0058] 次に、認証システムにおいて認証デバイス2による生体認証の結果に応じて機器本体3のロック機構34によるロックを制御する認証処理の第1の例（第1の認証処理）について説明する。

図5は、実施形態に係る認証システムにおける第1の認証処理を説明するためのタイミングチャートである。

第1の認証処理は、機器本体3からの要求に応じて認証デバイス2が生体認証を実行し、その生体認証の結果に応じて機器本体3におけるロック機構34によるロックを制御する処理であるものとする。

[0059] 機器本体3の制御部31は、使用者がパーツ4を取り外すための操作としての取外し操作（ロック解除操作）を検知する（ST31）。例えば、制御部31は、使用者がユーザインターフェース33を用いて入力するパーツ4の取外し指示を取外し操作として検知する。また、制御部31は、使用者による解除ボタン34aへの操作を検知し、解除ボタン34aへの操作を取

外し操作として検知するようにしても良い。

[0060] パーツ4の取外し操作を検知した場合、制御部31は、通信部32により認証デバイス2と通信し、認証デバイス2へ生体認証を要求するコマンドを送信する(ST32)。制御部31は、生体認証を要求するコマンドとともに、機器本体3に取り付けられているパーツ4のパーツIDを含む識別情報を送信する。ここで、制御部31は、パーツ4の制御チップ41からパーツIDを取得しても良いし、パーツ4が取り付けられた場合に取得するパーツIDを含むパーツ情報をメモリに保持しておき、メモリに保持しているパーツIDを読み出すようにしても良い。

[0061] なお、本実施形態では、パーツ4に対応する登録者の生体情報を用いて認証するものとするが、機器本体3に対応づけた登録者の生体情報を用いて認証するようにして良い。この場合、識別IDは、機器本体3の識別情報(機器ID)を含むものとすれば良い。また、機器本体3とパーツ4との組み合わせに対応する登録者の生体情報を用いて認証するようにしても良い。この場合、識別IDは、機器IDとパーツIDとを含むものとすれば良い。

[0062] 認証デバイス2は、第2の通信部26により機器本体3からの生体認証を要求するコマンドを受信する。認証デバイス2のプロセッサ21は、機器本体3から生体情報の登録を要求するコマンドを受信した場合、生体センサ27により生体情報としての指紋画像を含む画像を読取る(ST33)。ここで、生体センサ27の読取位置には、操作者(認証対象者)の指が置かれるものとする。また、生体センサ27は、操作者の指が置かれたことを検知して画像の読取を実行するようにしても良い。

[0063] 生体センサ27は、読み取った画像(読取画像)をMPU28に送信する。MPU28は、生体センサ27からの読取画像に含まれる生体情報としての指紋画像を取得する。生体センサ27が読み取った画像から生体情報を取得すると、MPU28は、取得した指紋画像における特徴点情報を抽出する(ST34)。MPU28は、抽出した特徴点情報を操作者の生体情報としてプロセッサ21に送信する。これにより、プロセッサ21は、MPU28

から操作者の指紋画像の特徴点情報を取得する。

[0064] 操作者の指紋画像の特徴点情報を取得すると、プロセッサ21は、操作者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を照合することにより生体認証を行う（ST35）。プロセッサ21は、コマンドと共に受信する識別情報に対応する登録者の生体情報として登録者の指紋画像の特徴点情報を取得する。プロセッサ21は、生体センサ27が読み取った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を照合し、両指紋画像が同一人物のものであるかを判定する認証処理を行う。

[0065] 例えば、プロセッサ21は、今回取得した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をMPU28に入力して類似度を算出させる。プロセッサ21は、MPU28から算出された類似度を取得する。類似度を取得すると、プロセッサ21は、類似度が所定の閾値（同一人物と判定する閾値）を超えているか判定する。類似度が閾値を超えていると、プロセッサ21は、生体センサ27が生体情報を読取った操作者が登録者であると特定、つまり、同一人物の生体情報であると判断する。また、類似度が閾値以下であると、プロセッサ21は、生体センサ27が生体情報を読取った操作者が登録者であると同定できなかったものとする。

[0066] 特徴点情報の照合による生体認証が終了すると、プロセッサ21は、第2通信部26により生体情報としての指紋画像による生体認証の結果を含むレスポンスを機器本体3へ送信する（ST36）。

なお、プロセッサ21は、生体認証の結果を認証デバイス2に設けた表示器で表示するようにしても良い。例えば、プロセッサ21は、生体認証が成功した場合に表示器として青色のLEDを点灯させ、生体認証が失敗した場合に赤色のLEDを点灯させるようにしてもよい。また、プロセッサ21は、成功した場合にLEDを点灯、失敗した場合にLEDを点滅させるようにしても良い。

[0067] 機器本体3の制御部31は、通信部32を介して認証デバイス2から生体認証の結果を示すレスポンスを受信する。制御部31は、認証デバイス2に

よる生体認証の結果に応じてロック機構を制御する動作を実行する（ST37）。例えば、制御部31は、認証デバイス2から生体認証が成功したことを示すレスポンスを受信した場合、ロック機構34によるパーツ4のロックを解除し、パーツ4を取外し可能とする。また、制御部31は、認証デバイス2から生体認証が失敗したことを示すレスポンスを受信した場合、ロック機構34によりパーツ4をロックしたままの状態として、パーツ4が取外しできないように制御する。

[0068] なお、制御部31は、認証デバイス2による生体認証の結果あるいは生体認証の結果に応じたロック機構34の状態をユーザインターフェース33としての表示装置などにより報知するようにしても良い。例えば、制御部31は、生体認証が成功した場合に生体認証が成功した旨またはパーツ4が取外し可能である旨をユーザインターフェース33により報知する。また、制御部31は、生体認証が失敗した場合、生体認証が失敗した旨またはパーツ4が取外し不可である旨をユーザインターフェース33により報知するようにしても良い。

[0069] 次に、認証システムにおいて認証デバイス2による生体認証の結果に応じて機器本体3のロック機構を制御する認証処理の第2の例（第2の認証処理）について説明する。

図6は、認証システムにおける第2の認証処理を説明するためのタイミングチャートである。

ここで、第2の認証処理は、ユーザ（管理者）が操作するスマートフォンなどの情報端末1からの要求に応じて認証デバイス2が生体認証を実行し、その生体認証の結果に応じて機器本体34によるパーツ4のロックを制御する処理であるものとする。

[0070] まず、情報端末1の制御部11は、情報端末1を操作している管理者に対して、機器本体3から取り外したいパーツ4を指示させる（ST41）。例えば、情報端末1の制御部11は、予め登録されているパーツから取外しを行いたいパーツをUI13で選択させる。また、制御部11は、通信先とな

る認証デバイス 2 が通信可能な機器本体を検出し、検出した機器本体に取り付けられているパーツから対象とするパーツを選択させるようにしても良い。また、制御部 11 は、対象となるパーツの識別情報（パーツ ID）を UI 13 などでも直接入力させるようにしても良い。

[0071] また、情報端末 1 の制御部 11 は、パーツ 4 が取り外される機器本体 3 を指示されるようにしても良い。例えば、制御部 11 は、予め登録されている機器本体から対象とする機器本体を選択させるようにしても良いし、通信先となる認証デバイス 2 と通信可能な機器本体から対象とする機器本体を選択させるようにしても良いし、機器本体 3 の識別情報（機器 ID）を直接入力させるようにしても良い。

[0072] 制御部 11 は、機器本体 3 から取り外したいパーツ 4 が指示されると、通信部 12 により認証デバイス 2 と通信し、生体認証を要求するコマンドを認証デバイス 2 へ送信する（ST42）。ここで、制御部 11 は、生体認証を要求するコマンドとともに、指定されたパーツを示す識別情報（パーツ ID）を含む識別情報を送信するものとする。

[0073] なお、本実施形態では、パーツ 4 の使用権限を持つ登録者の生体情報を用いて認証するものとするが、機器本体 3 の使用権限を持つ登録者の生体情報で認証するようにしても良い。この場合、識別情報は、機器本体 3 の識別情報（機器 ID）を含むものとすれば良い。また、機器本体 3 とパーツ 4 との組み合わせに対応する登録者の生体情報を用いて認証するようにしても良い。この場合、識別情報は、機器 ID とパーツ ID とを含むものとすれば良い。

[0074] 認証デバイス 2 は、第 1 の通信部 25 により情報端末 1 からの生体認証を要求するコマンドを受信する。認証デバイス 2 のプロセッサ 21 は、情報端末 1 から生体認証を要求するコマンドを受信した場合、生体センサ 27 を用いて操作者の生体情報としての指紋画像を含む画像を読取る（ST43）。ここで、生体センサ 27 の読取位置には、操作者の指が置かれているものとする。また、生体センサ 27 は、読取位置に指が置かれたことを検知して画像の読取を行うようにしても良い。

- [0075] 生体センサ２７は、読み取った画像（読取画像）をＭＰＵ２８に送信する。ＭＰＵ２８は、生体センサ２７からの読取画像に含まれる生体情報としての指紋画像を取得する。生体センサ２７が読み取った画像から生体情報を取得すると、ＭＰＵ２８は、取得した指紋画像における特徴点情報を抽出する（ＳＴ４４）。ＭＰＵ２８は、抽出した特徴点情報を操作者の生体情報としてプロセッサ２１に送信する。これにより、プロセッサ２１は、ＭＰＵ２８から操作者の指紋画像の特徴点情報を取得する。
- [0076] 操作者の指紋画像の特徴点情報を取得すると、プロセッサ２１は、操作者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を照合することにより生体認証を行う（ＳＴ４５）。プロセッサ２１は、コマンドと共に受信する識別情報に対応する登録者の生体情報としての指紋画像の特徴点情報を取得する。プロセッサ２１は、生体センサ２７が読み取った操作者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を照合し、両指紋画像が同一人物のものであるかを判定する認証処理を行う。
- [0077] 例えば、プロセッサ２１は、今回取得した操作者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をＭＰＵ２８に入力して類似度を算出させる。プロセッサ２１は、ＭＰＵ２８から算出された類似度を取得する。類似度を取得すると、プロセッサ２１は、類似度が所定の閾値（同一人物と判定する閾値）を超えているか判定する。類似度が閾値を超えていると、プロセッサ２１は、生体センサ２７が生体情報を読取った操作者が登録者であると特定、つまり、同一人物の生体情報であると判断する。また、類似度が閾値以下であると、プロセッサ２１は、生体センサ２７が生体情報を読取った操作者が登録者と同定できなかったものとする。
- [0078] 特徴点情報の照合による生体認証が終了すると、プロセッサ２１は、第２の通信部２６により生体情報としての指紋画像による生体認証の結果を示すデータを機器本体３へ送信する（ＳＴ４６）。
- [0079] 機器本体３の制御部３１は、通信部３２を介して認証デバイス２から生体認証の結果を示すデータを受信する。制御部３１は、認証デバイス２による

生体認証の結果に応じてロック機構３４によるロックを制御する動作を実行する（ＳＴ４７）。

[0080] 例えば、制御部３１は、認証デバイス２から生体認証が成功したことを示すレスポンスを受信した場合、ロック機構３４によるパーツ４のロックを解除し、パーツ４を取外し可能とする。また、制御部３１は、認証デバイス２から生体認証が失敗したことを示すレスポンスを受信した場合、ロック機構３４によりパーツ４をロックしたままの状態として、パーツ４が取外しできないように制御する。

[0081] また、プロセッサ２１は、第１の通信部２５により生体情報としての指紋画像による生体認証の結果を示すレスポンスを情報端末１へ送信する（ＳＴ４６）。

情報端末１の制御部１１は、通信部３２を介して認証デバイス２から生体認証の結果を示すレスポンスを受信する。制御部１１は、認証デバイス２による生体認証の結果を報知する（ＳＴ４８）。例えば、制御部１１は、認証デバイス２での生体認証が成功した場合、生体認証が成功した旨またはパーツ４が取外し可能である旨をユーザインターフェース１３により報知する。また、制御部１１は、生体認証が失敗した場合、生体認証が失敗した旨またはパーツ４が取外し不可である旨をユーザインターフェース１３により報知する。

[0082] 以上のように、実施形態に係る認証システムは、生体認証を行う認証デバイスを機器本体および機器本体に取り付けるパーツとは別の外部装置として設け、外部装置としての認証デバイスによる生体認証の結果に応じて機器本体におけるロック機構を制御する運用が可能となる。

[0083] また、第１の認証処理では、機器本体から要求によって認証デバイスが生体認証を行い、その生体認証結果に応じて機器本体がロック機構を制御する。これにより、機器本体がパーツの取外し操作などのロックを解除しようとする操作を検知した場合に認証デバイスでの生体認証を実施するようにできる。

また、第2の認証処理では、情報端末から指示によって認証デバイスが生体認証を行い、その生体認証結果に応じて機器本体がロック機構を制御する。これにより、生体認証を遠隔操作で実施しながら、機器本体によるロック状態を制御することが可能となる。

[0084] 次に、認証システムにおいてパーツ4を一時的に生体認証無しで利用可能とする一時利用設定を行う一時利用処理の第1の例（第1の一時利用処理）について説明する。

図7は、認証システムにおける第1の一時利用処理を説明するためのタイミングチャートである。

一時利用処理は、一時的に生体認証無しでパーツ4の利用（取外し）を可能とする回数などを一時利用設定として設定する処理であるものとする。また、第1の一時利用処理は、機器本体3からの要求に応じて認証デバイス2が生体認証を実行し、その生体認証が成功した場合に一時利用設定を行う処理である。

[0085] 機器本体3の制御部31は、ユーザが指定する一時利用の設定情報を取得する（ST61）。例えば、制御部31は、ユーザの操作に応じて一時利用の設定モードとする。ユーザは、ユーザインターフェース33を用いて、パーツ4を生体認証無しで利用可能（他者が利用可能）とする回数などを一時利用設定として入力する。

[0086] 制御部31は、ユーザが入力した一時利用の設定情報を取得すると、当該ユーザがパーツ4の使用権限者であることを確認するために認証デバイス2へユーザ認証を要求する。制御部31は、通信部32により認証デバイス2と通信し、認証デバイス2へ生体認証を要求するコマンドを送信する（ST62）。ここで、制御部31は、生体認証を要求するコマンドとともに、機器本体3に取り付けられているパーツ4のパーツIDを含む識別情報を送信する。なお、識別情報は、上述した各処理と同様に、機器本体3の識別情報（機器ID）を含むものであっても良いし、機器IDとパーツIDとを含むものであっても良い。

- [0087] 認証デバイス 2 は、第 2 の通信部 2 6 により機器本体 3 からの生体認証を要求するコマンドを受信する。認証デバイス 2 のプロセッサ 2 1 は、機器本体 3 から生体情報の登録を要求するコマンドを受信した場合、生体センサ 2 7 を用いて操作者の生体情報としての指紋画像を含む画像を読取る（S T 6 3）。ここで、生体センサ 2 7 の読取位置には、操作者の指が置かれているものとする。また、生体センサ 2 7 は、操作者の指が置かれたことを検知して画像の読取を実行するようにしても良い。
- [0088] 生体センサ 2 7 は、読み取った画像（読取画像）を M P U 2 8 に送信する。M P U 2 8 は、生体センサ 2 7 からの読取画像に含まれる生体情報としての指紋画像を取得する。生体センサ 2 7 が読み取った画像から生体情報を取得すると、M P U 2 8 は、取得した指紋画像における特徴点情報を抽出する（S T 6 4）。M P U 2 8 は、抽出した特徴点情報を操作者の生体情報としてプロセッサ 2 1 に送信する。これにより、プロセッサ 2 1 は、M P U 2 8 から操作者の指紋画像の特徴点情報を取得する。
- [0089] 操作者の指紋画像の特徴点情報を取得すると、プロセッサ 2 1 は、操作者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を照合することにより生体認証を行う（S T 6 5）。プロセッサ 2 1 は、コマンドと共に受信する識別 I D に基づいてパーツ 4 の使用者である登録者を特定し、特定した登録者の指紋画像の特徴点情報を取得する。プロセッサ 2 1 は、生体センサ 2 7 が読み取った操作者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を照合し、両指紋画像が同一人物のものであるかを判定する認証処理を行う。
- [0090] 例えば、プロセッサ 2 1 は、今回取得した操作者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を M P U 2 8 に入力して類似度を算出させる。プロセッサ 2 1 は、M P U 2 8 から算出された類似度を取得する。類似度を取得すると、プロセッサ 2 1 は、類似度が所定の閾値（同一人物と判定する閾値）を超えているか判定する。類似度が閾値を超えていると、プロセッサ 2 1 は、生体センサ 2 7 が生体情報を読取った操作者が登録者である

と特定、つまり、同一人物の生体情報であると判断する。また、類似度が閾値以下であると、プロセッサ 21 は、生体センサ 27 が生体情報を読取った操作者が登録者と同定できなかったものとする。

[0091] 特徴点情報の照合による生体認証が終了すると、プロセッサ 21 は、第 2 通信部 26 により生体情報としての指紋画像による生体認証の結果を含むレスポンスを機器本体 3 へ送信する (S T 6 6)。なお、プロセッサ 21 は、生体認証の結果を認証デバイス 2 に設けた表示器などで表示するようにしても良い。

[0092] 機器本体 3 の制御部 31 は、通信部 32 を介して認証デバイス 2 から生体認証の結果を示すレスポンスを受信する。制御部 31 は、認証デバイス 2 による生体認証の結果に応じて一時利用設定を実行する (S T 6 7)。例えば、制御部 31 は、認証デバイス 2 から生体認証が成功したことを示すレスポンスを受信した場合、ユーザが入力した一時利用の設定情報を記憶し、一時利用設定を有効とする。また、制御部 31 は、認証デバイス 2 から生体認証が失敗したことを示すレスポンスを受信した場合、入力された一時利用設定を中止し、U 1 3 3 などにより一時利用設定が適用できない旨を報知する。制御する。

[0093] また、一時利用設定は、例えば、設定回数だけ生体認証無しでパーツ 4 の取外しを許可するものである。これは、一時的に (設定回数だけ) 使用権限者以外の他者が当該パーツ 4 を他の機器本体に取り付けて使用することを許容するための制御設定である。この場合、機器本体 3 の制御部 11 は、一時利用設定として、パーツ 4 の取外しを設定回数分だけロック機構 34 によるロックをフリーにするように制御できる。

[0094] 次に、認証システムにおいてパーツ 4 を一時的に生体認証無しで利用可能とする設定を行う一時利用処理の第 2 の例 (第 2 の一時利用処理) について説明する。

図 8 は、認証システムにおける第 2 の一時利用処理を説明するためのタイミングチャートである。

ここで、第2の一時利用処理は、情報端末1からの要求に応じて認証デバイス2が生体認証を実行し、その生体認証が成功した場合に機器本体3によるパーツ4の一時利用設定を行う処理である。

[0095] まず、情報端末1の制御部11は、ユーザインターフェース13を用いて入力される指定のパーツ4に対する一時利用の設定情報を取得する（ST71）。例えば、情報端末1の制御部11は、一時利用設定を行うパーツを選択させ、選択されたパーツに対する一時利用の設定情報をユーザインターフェース13により入力させる。また、情報端末1の制御部11は、一時利用設定を行うパーツ4が取り付けられている機器本体3を選択させた後、一時利用の設定情報を入力させるようにしても良い。

[0096] 制御部11は、一時利用の設定情報を取得すると、通信部12により認証デバイス2と通信し、生体認証を要求するコマンドを認証デバイス2へ送信する（ST72）。ここで、制御部11は、生体認証を要求するコマンドとともに、一時利用設定を行うパーツを示す識別情報（パーツID）を含む識別IDを送信する。なお、識別IDは、機器本体3の識別情報（機器ID）としても良いし、機器IDとパーツIDとを含むものとしても良い。

[0097] 認証デバイス2は、第1の通信部25により情報端末1からの生体認証を要求するコマンドを受信する。認証デバイス2のプロセッサ21は、情報端末1から生体認証を要求するコマンドを受信した場合、生体センサ27により生体情報としての指紋画像を含む画像を読取る（ST73）。ここで、生体センサ27の読取位置には、操作者の指が置かれているものとする。また、生体センサ27は、読取位置に指が置かれたことを検知して画像の読取を行うようにしても良い。

[0098] 生体センサ27は、読み取った画像（読取画像）をMPU28に送信する。MPU28は、生体センサ27からの読取画像に含まれる操作者の生体情報としての指紋画像を取得する。生体センサ27が読み取った画像から生体情報を取得すると、MPU28は、取得した指紋画像における特徴点情報を抽出する（ST74）。MPU28は、抽出した特徴点情報を操作者の生体

情報としてプロセッサ２１に送信する。これにより、プロセッサ２１は、ＭＰＵ２８から操作者の指紋画像の特徴点情報を取得する。

[0099] 操作者の指紋画像の特徴点情報を取得すると、プロセッサ２１は、操作者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を照合することにより生体認証を行う（ＳＴ７５）。プロセッサ２１は、コマンドと共に受信する識別ＩＤに基づいてパーツ４の使用者である登録者を特定し、特定した登録者の指紋画像の特徴点情報を取得する。プロセッサ２１は、生体センサ２７が読み取った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を照合し、両指紋画像が同一人物のものであるかを判定する認証処理を行う。

[0100] 例えば、プロセッサ２１は、今回取得した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をＭＰＵ２８に入力して類似度を算出させる。プロセッサ２１は、ＭＰＵ２８から算出された類似度を取得する。類似度を取得すると、プロセッサ２１は、類似度が所定の閾値（同一人物と判定する閾値）を超えているか判定する。類似度が閾値を超えていると、プロセッサ２１は、生体センサ２７が生体情報を読取った操作者が登録者であると特定、つまり、同一人物の生体情報であると判断する。また、類似度が閾値以下であると、プロセッサ２１は、生体センサ２７が生体情報を読取った操作者が登録者と同定できなかったものとする。

[0101] 生体情報による本人認証を終了すると、プロセッサ２１は、第１の通信部２５により生体情報としての指紋画像による生体認証の結果を示すレスポンスを情報端末１へ送信する（ＳＴ７６）。

これに対して、情報端末１の制御部１１は、通信部３２を介して認証デバイス２から生体認証の結果を示すレスポンスを受信する。

[0102] 生体認証の結果を受信した後、制御部１１は、認証デバイス２での生体認証が成功した場合、認証デバイス２を介して一時利用の設定情報を機器本体３へ送信する（ＳＴ７８）。また、制御部１１は、生体認証が失敗した場合、生体認証が失敗した旨または一時利用設定が不可である旨をユーザインタ

ーフェース 13 により報知する。ここで、制御部 11 は、認証デバイス 2 での生体認証が成功した場合に、生体認証が成功した旨または一時設定を設定する旨をユーザインターフェース 13 により報知するようにしても良い。

[0103] また、認証デバイス 2 での生体認証が成功した後、機器本体 3 の制御部 31 は、情報端末 1 からの一時設定の設定情報を取得する。一時設定の設定情報を取得すると、制御部 31 は、取得した設定情報に基づいてパーツ 4 を一時利用させるための一時利用設定を実行する（ST77）。

[0104] なお、情報端末 1 の制御部 11 は、生体認証を要求するコマンドとともに、一時利用設定の設定情報を送信するようにしても良い。この場合、ST78 の処理を省略し、認証デバイス 2 は、生体認証が成功した場合に一時利用設定の設定情報を機器本体 3 へ送信するようにすれば良い。

[0105] 次に、実施形態に係る認証システムにおける機器本体 3 における一時利用設定に応じたロック機構 34 の制御例について説明する。

図 9 は、機器本体 3 における一時利用設定に応じたロック機構 34 の制御例を説明するためのフローチャートである。

ここでは、一時利用設定としてパーツ 4 を本人認証無しで取り外せる回数（一時利用の許容回数）が設定される場合を想定して説明するものとする。また、制御部 11 は、本人認証無しで取り外した回数（一時利用回数）を制御部 11 内のメモリ上に設定するカウンタ（一時利用カウンタ）によってカウントするものとする。

[0106] 機器本体 3 の制御部 31 は、ユーザがパーツ 4 を取り外すための取外し操作（ロック解除操作）をしたことを検知する（ST81）。パーツ 4 の取外し操作を検知した場合、制御部 31 は、パーツ 4 を取り外すための本人認証が不要であるか否かを判定する（ST82）。例えば、制御部 31 は、一時利用の許容回数が設定されている場合、一時利用カウンタがカウントする一時利用回数が一時利用の許容回数以下であれば、本人認証が不要であると判定する。また、制御部 31 は、一時利用回数が一時利用の許容回数を超えている場合、あるいは、一時利用の許容回数が設定されていない場合、本人認

証が必要であると判定する。

[0107] 本人認証が不要であると判定した場合（ST82、YES）、制御部31は、一時利用カウンタをカウントアップし（ST83）、ロック機構34によるパーツ4のロックを解除し、パーツ4を取外し可能とする（ST84）。これにより、機器本体3は、一時利用回数が一時利用の許容回数内であれば、本人認証無しでパーツ4を取り外せるようにできる。なお、制御部11は、パーツ4が取り外されたことを検知した場合に一時利用カウンタをカウントアップするようにしても良い。

[0108] また、本人認証が必要であると判定した場合（ST82、NO）、制御部31は、通信部32を通じて認証デバイス2へ生体認証を要求する（ST85）。例えば、制御部31は、上述したST32-37と同様な処理によって認証デバイス2による生体認証の結果を取得する。認証デバイス2での生体認証が成功した場合（ST86、YES）、制御部31は、ロック機構34によるパーツ4のロックを解除し、パーツ4を取外し可能とする（ST84）。また認証デバイス2での生体認証が成功した場合（ST86、NO）、制御部31は、ロック機構34でパーツ4をロックしたままの状態とし、本人確認ができないためにパーツ4が取外しできない旨をユーザインターフェース33で報知する（ST87）。

[0109] 以上のような処理によって、認証システムにおける機器本体は、本人認証無しでパーツを取外しできるような一時設定を行うことができ、一時設定の条件内であれば、取り付けられているパーツを本人認証無しで取り外すことを許容するようにできる。この結果、認証システムによれば、機器本体に取り付けられているパーツを一時的に本人認証無しで取り外して、使用権限者以外の人物が使用するようにできる。

[0110] 次に、認証システムにおいて認証デバイス2に登録した生体情報を削除する削除処理の第1の例（第1の削除処理）について説明する。

図10は、認証システムにおける第1の削除処理を説明するためのタイミングチャートである。

ここで、第 1 の削除処理では、ユーザ（管理者）が操作するスマートフォンなどの情報端末 1 からの要求に応じて認証デバイス 2 に登録済みのパーツ 4 に対する使用権限者の生体情報を削除するものとする。

[0111] まず、管理者は、情報端末 1 のユーザインターフェース 1 3 を用いて削除対象となる生体情報に対応する識別情報を指定し、生体情報の削除を指示する。例えば、情報端末 1 の制御部 1 1 は、ユーザインターフェース 1 3 を用いて対象とするパーツを指定させ、当該パーツに対応づけて登録されている生体情報の削除を指示させる。ここで、制御部 1 1 は、生体情報を登録済みのパーツから生体情報を削除するパーツを選択させるようにしても良いし、削除対象とするパーツのパーツ ID を入力させるようにしても良い。この場合、制御部 1 1 は、削除対象となる生体情報に対応する識別情報として、生体情報に対応するパーツを示すパーツ ID を取得するようにすれば良い。

[0112] また、生体情報を機器 ID と対応づけて登録している場合には、制御部 1 1 は、削除対象とする生体情報に対応する機器本体を指定させ、指定された機器本体の機器 ID を削除対象となる生体情報に対応する識別情報としても良い。また、生体情報をユーザ名などのユーザ情報と対応づけて登録している場合には、制御部 1 1 は、削除対象とする生体情報のユーザを指定させ、指定されたユーザのユーザ情報を削除対象となる生体情報に対応する識別情報としても良い。

[0113] 情報端末 1 の制御部 1 1 は、ユーザインターフェース 1 3 で指定される削除対象となる生体情報に対応する識別情報を取得する（ST101）。削除対象とする生体情報に対応する識別情報を取得すると、制御部 1 1 は、通信部 1 2 により認証デバイス 2 と通信し、取得した識別情報に対応する生体情報の削除を要求するコマンドを認証デバイス 2 へ送信する（ST102）。

[0114] 認証デバイス 2 は、第 1 の通信部 2 5 により情報端末 1 からのコマンドを受信する。認証デバイス 2 のプロセッサ 2 1 は、情報端末 1 から受信したコマンドが生体情報の削除を要求するコマンドである場合、生体情報の削除処理を実行する。認証デバイス 2 のプロセッサ 2 1 は、生体情報の削除処理に

において、登録者自身であるかを認証する生体認証を実施する。

[0115] すなわち、プロセッサ 21 は、生体センサ 27 により生体情報としての指紋画像を取得させる。例えば、プロセッサ 21 は、MPU 28 などを通じて生体センサ 27 を起動する。ここで、生体情報の削除は、登録者本人であることが生体認証で確認された場合に実施するものとする。このため、生体情報を削除する者（登録者）は、生体センサ 27 における所定の読取位置に指紋が形成されている指を置くものとする。

なお、生体情報を削除する者（登録者）は、情報端末 1 を操作している管理者と同一人物であっても良いし、別の人物であっても良い。後者の場合、登録者ではない管理者が情報端末 1 で遠隔操作しながら、登録者に生体認証を実行させるような運用が実現できる。

[0116] 生体センサ 27 は、プロセッサ 21 からの指示に応じて起動し、所定の読取位置に置かれた人物の指から指紋画像を含む読取画像を取得する（ST103）。生体センサ 27 は、取得した読取画像を MPU 28 に送信する。MPU 28 は、生体センサ 27 から読取画像から指紋画像を取得し、取得した指紋画像における特徴点情報を抽出する（ST104）。MPU 28 は、抽出した特徴点情報を登録者の生体情報としてプロセッサ 21 に送信する。

[0117] プロセッサ 21 は、MPU 28 から生体センサ 27 で読み取った指紋画像の特徴点情報を取得する。生体センサ 27 が読み取った指紋画像の特徴点情報を取得すると、プロセッサ 21 は、読み取った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を照合することにより生体認証を行う（ST105）。プロセッサ 21 は、コマンドと共に受信する識別情報に対応する登録者の生体情報としての指紋画像の特徴点情報を取得する。プロセッサ 21 は、生体センサ 27 が読み取った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を照合し、類似度が設定した閾値の上か下かによって、両指紋画像が同一人物のものであるか否かを判定する生体認証を行う。

[0118] 生体認証が成功した場合、プロセッサ 21 は、当該登録者の生体情報を削除する（106）。プロセッサ 21 は、データメモリ 24 にテンプレートと

して登録している当該登録者の指紋画像の特徴点情報を削除する。また、プロセッサ 21 は、当該登録者の指紋画像の特徴点情報（生体情報）が無効である旨を書き込むようにしても良い。

- [0119] 指定された識別情報に対応する生体情報（登録者の生体情報）を削除すると、プロセッサ 21 は、第 1 の通信部 25 を通じて指定された識別情報に対応する生体情報を削除したことを示すレスポンスを情報端末 1 へ送信する（ST107）。

情報端末 1 の制御部 11 は、通信部 12 を介して認証デバイス 2 から生体情報の削除が完了したことを示すレスポンスを受信すると、ユーザインターフェース 13 を用いて生体情報の登録完了を管理者（情報端末 1 の操作者）へ報知する（ST108）。

- [0120] また、認証デバイス 2 のプロセッサ 21 は、第 2 の通信部 26 を通じてパーツ 4 の使用権限者の生体情報を削除したことを機器本体 3 にも通知する（ST107）。これに対して、機器本体 3 は、通信部 32 により生体情報が削除された旨の通知を受信する。機器本体 3 の制御部 31 は、生体情報が削除された旨の通知を受けると、パーツ 4 に対する使用権限者の生体情報が削除されたことを記録する（ST109）。

- [0121] 例えば、制御部 31 は、制御部 31 内のメモリにパーツ 4 に対する使用権限者の生体情報が削除済み（使用権限者が未登録）であることを示す情報を記憶する。これにより、制御部 31 は、使用権限者の生体情報が未登録（削除済み）であることが記録されている場合、当該パーツ 4 に対して新たな使用権限者の生体情報が登録可能であると判定するようにできる。

- [0122] 次に、認証システムにおいて認証デバイス 2 に生体情報を削除する削除処理の第 2 の例（第 2 の削除処理）について説明する。

図 11 は、認証システムにおける生体情報の第 2 の削除処理を説明するためのタイミングチャートである。

ここで、第 2 の削除処理では、使用者が操作する機器本体 3 からの要求に応じて認証デバイス 2 に登録されている生体情報を削除するものとする。

- [0123] まず、ユーザは、パーツ 4 を取り付けた状態の機器本体 3 においてユーザインターフェース 3 3 を操作することにより生体情報の削除を指示する。生体情報の削除を指示したユーザ（ここでは登録者であることを想定する）は、認証デバイス 2 における生体センサ 2 7 の読取位置に登録する指紋が形成されている指を置く。
- [0124] 機器本体 3 の制御部 3 1 は、削除対象とする生体情報に対応する識別情報を取得する（S T 1 1 1）。ここでは、削除対象の生体情報に対応する識別情報として、取り付けられているパーツ 4 のパーツ I D を含むパーツ情報を識別情報として取得する。
- [0125] 削除対象とする生体情報に対応する識別情報を取得すると、制御部 3 1 は、取得した識別情報を指定し、指定した識別情報に対応する生体情報の削除を要求するコマンドを通信部 3 2 により通信する認証デバイス 2 へ送信する（S T 1 1 2）。
- [0126] 認証デバイス 2 は、第 2 の通信部 2 6 により機器本体 3 からの生体情報の登録を要求するコマンドを受信する。認証デバイス 2 のプロセッサ 2 1 は、機器本体 3 から生体情報の登録を要求するコマンドを受信した場合、上述した S T 1 0 3 - 1 0 6 と同様な処理によって生体情報の削除を実行する（S T 1 1 3 - 1 1 6）。
- 生体情報を削除すると、プロセッサ 2 1 は、第 2 の通信部 2 6 を通じてパーツ 4 に対する使用権限者の生体情報の削除が完了したことを示すレスポンスを機器本体 3 へ送信する（S T 1 1 7）。
- [0127] 機器本体 3 の制御部 3 1 は、通信部 3 2 を介して認証デバイス 2 から生体情報を削除したことを示すレスポンスを受信する。制御部 3 1 は、生体情報を削除したことを示すレスポンスを受信すると、パーツ 4 に対する使用権限者の生体情報が削除されたことを記録する（S T 1 1 8）。例えば、制御部 3 1 は、制御部 3 1 内のメモリにパーツ 4 に対する使用権限者の生体情報が削除済み（使用権限者が未登録）であることを示す情報を記憶する。制御部 3 1 は、使用権限者の生体情報が未登録（削除済み）であることが記録され

ている場合、当該パーツ 4 に対して新たな使用権限者の生体情報が登録可能であると判定するようにできる。

[0128] 以上のような第 1 および第 2 の削除処理によって、認証システムでは、機器本体の取り付けるパーツに対する使用権限者の生体情報を削除することができ、パーツに対する使用権限者を未登録の状態にすることができる。これにより、認証システムでは、生体情報によってパーツの使用権限者を厳密に管理するだけでなく、生体認証によって本人確認できた使用権限者の生体情報を削除することもでき、パーツに対する使用権限者をリセットして当該パーツ 4 を他者に譲り渡したり第 3 者へ売却したりすることが容易にできる。

[0129] 次に、認証システムにおいて認証デバイス 2 に生体情報が登録されている使用権限を譲渡（パーツを他者に譲渡）する譲渡処理の第 1 の例（第 1 の譲渡処理）について説明する。

図 1 2 は、認証システムにおける第 1 の譲渡処理を説明するためのタイミングチャートである。

使用権限の譲渡は、上述した削除処理と登録処理とを実行することで実現できるが、本実施形態に係る認証システムでは、使用権限の譲渡手続きを一連の処理として実現する譲渡処理を行うことも可能である。第 1 の譲渡処理としては、ユーザ（管理者）が操作するスマートフォンなどの情報端末 1 からの要求に応じて認証デバイス 2 に登録済みのパーツ 4 に対する使用権限を譲渡人（現在の使用権限者）から譲受人（新たな使用権限者）へ譲渡する処理例について説明するものとする。

[0130] まず、管理者は、情報端末 1 のユーザインターフェース 1 3 を用いて譲渡対象となるパーツを示す識別情報を指定し、パーツの譲渡（使用権限の譲渡）を指示する。例えば、情報端末 1 の制御部 1 1 は、ユーザインターフェース 1 3 を用いて譲渡対象とするパーツを指定させ、当該パーツの使用権限の譲渡を指示させる。制御部 1 1 は、生体情報を登録済みのパーツから譲渡するパーツを選択させるようにしても良いし、譲渡対象とするパーツのパーツ ID を入力させるようにしても良い。

[0131] また、生体情報を機器IDと対応づけて登録している場合、制御部11は、譲渡対象とする機器本体を指定させ、指定された機器本体の機器IDを譲渡対象となる生体情報に対応する識別情報としても良い。また、生体情報を使用権限者のユーザ名などのユーザ情報と対応づけて登録している場合には、制御部11は、譲渡対象とするパーツの使用権限者であるユーザを指定させ、指定されたユーザに使用権限が設定されているパーツを譲渡対象としても良い。

[0132] 情報端末1の制御部11は、ユーザインターフェース13で入力される譲渡対象となるパーツを示す識別情報を指定した譲渡処理の実行要求を取得する(ST121)。譲渡対象とするパーツを示す識別情報を取得すると、制御部11は、取得した識別情報が示すパーツの譲渡処理を要求するコマンドを通信部12により通信する認証デバイス2へ送信する(ST122)。

[0133] 認証デバイス2は、第1の通信部25により情報端末1からのコマンドを受信する。認証デバイス2のプロセッサ21は、情報端末1から受信したコマンドがパーツの譲渡を要求するコマンドである場合、まず、譲渡人が登録者自身であることを生体認証で確認する。

すなわち、プロセッサ21は、生体センサ27を用いて譲渡人の生体情報としての指紋画像を取得する(ST123)。例えば、プロセッサ21は、MPU28などを通じて生体センサ27を起動する。ここで、譲渡人は、生体センサ27における所定の読取位置に指紋が形成されている指を置き、プロセッサ21は、生体センサ27で譲渡人の指紋画像を含む読取画像を取得する。

[0134] なお、譲渡人（登録者）は、情報端末1を操作している管理者と同一人物であっても良いし、別の人物であっても良い。後者の場合、譲渡人ではない管理者が情報端末1を操作することにより、登録者に生体認証を実行させるような運用が実現できる。

[0135] 生体センサ27は、プロセッサ21からの指示に応じて起動し、所定の読取位置に置かれた人物の指から指紋画像を含む読取画像を取得する。MPU

28は、生体センサ27から読取画像から指紋画像を取得し、取得した指紋画像における特徴点情報を抽出する(ST124)。MPU28は、抽出した特徴点情報を登録者の生体情報としてプロセッサ21に送信する。

[0136] プロセッサ21は、MPU28が生体センサ27で読み取った指紋画像から抽出した特徴点情報を取得する。生体センサ27が読み取った指紋画像の特徴点情報を取得すると、プロセッサ21は、読み取った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を照合することにより生体認証を行う(ST125)。プロセッサ21は、コマンドと共に受信する識別情報に対応する登録者の生体情報を特定し、特定した登録者の指紋画像の特徴点情報と生体センサ27が読み取った指紋画像の特徴点情報とを照合し、類似度が閾値の上か下かによって、両指紋画像が同一人物のものであるか否かを判定する譲渡人に対する生体認証を行う。

[0137] 譲渡人に対する生体認証が終了すると、プロセッサ21は、第1の通信部25を通じて譲受人が登録者であるか否かを示す生体認証の結果を示すレスポンスを情報端末1へ送信する(ST126)。

これに対して、情報端末1の制御部11は、通信部12を介して認証デバイス2から譲渡人に対する生体認証の結果を示すレスポンスを受信する。生体認証の結果を示すレスポンスを受信すると、制御部11は、譲受人が登録者であることが確認できたか否かを判定する。譲渡人が登録者であることが確認できなかった場合、制御部11は、譲渡人の生体認証が不可であるために譲渡処理を終了する。

[0138] 認証デバイス2による生体認証で譲渡人が登録者であることが確認できた場合、制御部11は、ユーザインターフェース13を用いて管理者に譲渡の実行指示を受け付ける。譲渡の実行指示が入力されると、制御部11は、譲渡の実行を指示するコマンドを認証デバイス2へ送信する(ST127)。また、制御部11は、認証デバイス2に譲渡の実行指示を送信するとともに、ユーザインターフェース13などにより譲受人の生体情報を生体センサに読み取らせる旨の案内を行う。このような案内に応じて、譲受人は、生体セ

ンサ 27 の読取位置に登録用の指紋を有する指を置く。

[0139] 一方、認証デバイス 2 のプロセッサ 21 は、第 1 の通信部 25 により情報端末 1 から譲渡の実行指示を受信すると、生体センサ 27 を用いて譲受人の生体情報としての指紋画像を取得する。例えば、プロセッサ 21 は、MPU 28 などを通じて生体センサ 27 を起動させ、生体センサ 27 は、読取位置に置かれた譲受人の指紋画像を含む読取画像を取得する（ST128）。生体センサ 27 は、取得した読取画像を MPU 28 に送信する。MPU 28 は、生体センサ 27 から読取画像から指紋画像を取得する。MPU 28 は、取得した指紋画像における特徴点情報を抽出する（ST129）。MPU 28 は、抽出した特徴点情報を譲受人の生体情報としてプロセッサ 21 に送信する。

[0140] プロセッサ 21 は、MPU 28 から指紋画像の特徴点情報を取得すると、取得した指紋画像の特徴点情報に基づいてテンプレート（生体認証用の特徴点を抽出したデータ）を生成する。テンプレートを生成すると、プロセッサ 21 は、生成したテンプレートを譲受人の生体情報として当該識別情報に対応づけてデータメモリ 24 に保存（登録）する（ST130）。この場合、プロセッサ 21 は、既に当該識別情報に対応づけて登録されていた譲渡人の生体情報を削除する（ST131）。これにより、当該識別情報に対応して登録される生体情報が譲渡人の生体情報から譲受人の生体情報に書き換えられる。つまり、当該識別情報に対応する登録者の生体情報が譲受人の生体情報となるため、当該識別情報が示すパーツの使用権限の譲渡が完了する。

[0141] 譲渡が完了すると、プロセッサ 21 は、第 1 の通信部 25 を通じて指定された識別情報に対応する使用権限の譲渡（登録者の生体情報の書き換え）が完了したことを示すレスポンスを情報端末 1 へ送信する（ST132）。

情報端末 1 の制御部 11 は、認証デバイス 2 からの譲渡完了を示すレスポンスを通信部 12 により受信する。譲渡完了を示すレスポンスを受信すると、制御部 11 は、使用権限の譲渡が完了したことをユーザインターフェース 33 などにより管理者（情報端末 1 の操作者）へ報知する（ST133）。

[0142] また、譲渡が完了した場合、プロセッサ 2 1 は、第 2 の通信部 2 6 を通じて当該識別情報が示すパーツ 4 が取り付けられている機器本体 3 にも使用権限の譲渡（登録者の生体情報の書き換え）が完了したことを通知する（S T 1 3 2）。

機器本体 3 は、通信部 3 2 によって認証デバイス 2 からの譲渡完了を示す通知を受信する。認証デバイス 2 から譲渡完了の通知を受信すると、機器本体 3 の制御部 3 1 は、取り付けられているパーツ 4 に対する使用権限者の生体情報が変更（譲渡）されたことを記録する（S T 1 3 4）。また、制御部 3 1 は、ユーザインターフェース 3 3 などにより使用権限の譲渡が完了したことを報知するようにしても良い。

[0143] 次に、認証システムにおいて認証デバイス 2 に生体情報が登録される使用権限を譲渡（パーツを他者に譲渡）する譲渡処理の第 2 の例（第 2 の譲渡処理）について説明する。

図 1 3 は、認証システムにおける第 2 の譲渡処理を説明するためのタイミングチャートである。

第 2 の譲渡処理としては、ユーザが操作する機器本体 3 からの要求に応じて認証デバイス 2 に登録済みのパーツ 4 に対する使用権限を譲渡人（現在の使用権限者）から譲受人（新たな使用権限者）へ譲渡する処理例について説明するものとする。

[0144] まず、ユーザは、ユーザインターフェース 3 3 を操作することにより機器本体 3 に取り付けられているパーツ 4 の譲渡（使用権限の譲渡）を指示する。譲渡を指示したユーザ（ここでは登録者であることを想定する）は、認証デバイス 2 における生体センサ 2 7 の読取位置に登録する指紋が形成されている指を置く。

[0145] 機器本体 3 の制御部 3 1 は、ユーザインターフェース 3 3 で入力される譲渡指示に応じて、パーツ 4 を示す識別情報を取得し（S T 1 4 1）、取得した識別情報が示すパーツの譲渡を要求するコマンドを通信部 1 2 により通信する認証デバイス 2 へ送信する（S T 1 4 2）。

[0146] 認証デバイス 2 は、第 1 の通信部 25 により情報端末 1 からのコマンドを受信する。認証デバイス 2 のプロセッサ 21 は、情報端末 1 から受信したコマンドがパーツの譲渡を要求するコマンドである場合、譲渡人が登録者自身であることを生体認証で確認するため、生体センサ 27 を用いて譲渡人の生体情報としての指紋画像を取得する（ST143）。

生体センサ 27 は、プロセッサ 21 からの指示に応じて起動し、所定の読取位置に置かれた人物の指から指紋画像を含む読取画像を取得する。MPU 28 は、生体センサ 27 から読取画像から指紋画像を取得し、取得した指紋画像における特徴点情報を抽出する（ST144）。MPU 28 は、抽出した特徴点情報を登録者の生体情報としてプロセッサ 21 に送信する。

[0147] プロセッサ 21 は、MPU 28 が生体センサ 27 で読み取った指紋画像から抽出した特徴点情報を取得する。生体センサ 27 が読み取った指紋画像の特徴点情報を取得すると、プロセッサ 21 は、読み取った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を照合することにより生体認証を行う（ST145）。プロセッサ 21 は、コマンドと共に受信する識別情報に対応する登録者の生体情報としての登録者の指紋画像の特徴点情報と生体センサ 27 が読み取った指紋画像の特徴点情報とを照合し、両指紋画像が同一人物のものであるか否かを判定する譲渡人に対する生体認証を行う。

[0148] 譲渡人に対する生体認証が終了すると、プロセッサ 21 は、第 2 の通信部 26 を通じて譲受人が現在の登録者として特定、または確認できたか否かを示す生体認証の結果を示すレスポンスを情報端末 1 へ送信する（ST146）。

これに対して、機器本体 3 の制御部 31 は、通信部 32 を介して認証デバイス 2 から譲渡人に対する生体認証の結果を示すレスポンスを受信する。生体認証の結果を示すレスポンスを受信すると、制御部 31 は、生体認証によって譲渡人が現在の登録者であることが確認できなかった場合、制御部 31 は、譲渡人の生体認証が不可であるために譲渡処理を終了する。この場合、制御部 31 は、譲渡人の生体認証が不可のため譲渡が不可である旨の案内を

行うようにしても良い。

[0149] 認証デバイス 2 による生体認証で譲渡人が現在の登録者であることが確認できた場合、制御部 3 1 は、ユーザインターフェース 3 3 を用いて管理者に譲渡の実行指示（譲渡実行の確認）を受け付ける。譲渡の実行指示が入力されると、制御部 3 1 は、譲渡の実行を指示するコマンドを認証デバイス 2 へ送信する（S T 1 4 7）。また、制御部 3 1 は、認証デバイス 2 に譲渡の実行指示を送信するとともに、ユーザインターフェース 3 3 などにより譲受人の生体情報を生体センサ 2 7 に読み取らせる旨の案内を行う。このような案内に応じて、譲受人は、生体センサ 2 7 の読取位置に登録用の指紋を有する指を置く。

[0150] 一方、認証デバイス 2 のプロセッサ 2 1 は、第 2 の通信部 2 6 により機器本体 3 から譲渡の実行指示を受信する。譲渡の実行指示を受けると、プロセッサ 2 1 は、生体センサ 2 7 を用いて譲受人の生体情報としての指紋画像を取得する。例えば、プロセッサ 2 1 は、M P U 2 8 などを通じて生体センサ 2 7 を起動させ、生体センサ 2 7 による読取位置に置かれた譲受人の指紋画像を含む読取画像を行う（S T 1 4 8）。生体センサ 2 7 は、取得した読取画像を M P U 2 8 に送信する。M P U 2 8 は、生体センサ 2 7 から読取画像から指紋画像を取得する。M P U 2 8 は、取得した指紋画像における特徴点情報を抽出する（S T 1 4 9）。M P U 2 8 は、抽出した特徴点情報を譲受人の生体情報としてプロセッサ 2 1 に送信する。

[0151] プロセッサ 2 1 は、M P U 2 8 から指紋画像の特徴点情報を取得すると、取得した指紋画像の特徴点情報に基づいてテンプレート（生体認証用の特徴点を抽出したデータ）を生成する。テンプレートを生成すると、プロセッサ 2 1 は、生成したテンプレートを譲受人の生体情報として当該識別情報に対応づけてデータメモリ 2 4 に保存（登録）する（S T 1 5 0）。この場合、プロセッサ 2 1 は、既に当該識別情報に対応づけて登録されていた譲渡人の生体情報を削除する（S T 1 5 1）。これにより、当該識別情報に対応して登録される生体情報が譲渡人の生体情報から譲受人の生体情報に書き換えら

れる。つまり、当該識別情報に対応する登録者の生体情報が譲受人の生体情報となるため、当該識別情報が示すパーツの使用権限の譲渡が完了する。

[0152] 譲渡が完了すると、プロセッサ21は、第2の通信部26を通じて指定された識別情報に対応する使用権限の譲渡（登録者の生体情報の書き換え）が完了したことを示すレスポンスを機器本体3へ送信する（ST152）。

機器本体3の制御部31は、認証デバイス2からの譲渡完了を示すレスポンスを通信部32により受信する。譲渡完了を示すレスポンスを受信すると、制御部31は、取り付けられているパーツ4に対する使用権限者の生体情報が変更（譲渡）されたことを記録する（ST153）。また、制御部31は、ユーザインターフェース33などにより使用権限の譲渡が完了したことを報知するようにしても良い。

[0153] 以上のような第1および第2の譲渡処理によって、認証システムでは、機器本体の取り付けるパーツに対する使用権限者の生体情報を譲渡人（現在の登録者）の生体情報から譲受人（新たな登録者）の生体情報に書き換えることができる。これにより、認証システムでは、機器本体の取り付けるパーツに対する使用権限を譲渡人から譲受人（新たな登録者）へ譲渡することができる。すなわち、実施形態に係る認証システムでは、パーツの使用権限者を生体情報によって厳密に管理するだけでなく、譲渡人を生体認証で確認した上で登録者の生体情報を譲受人の生体情報に書き換えられるようにすることで、当該パーツに対するセキュリティ性を落とすことなく当該パーツの譲渡を実現できる。

[0154] なお、上述した実施形態では、カメラなどの機器本体に取り付けられたレンズなどのパーツに対するロックを制御する形態について説明したが、認証デバイスによる生体認証で機器本体が備えるロック機構を制御するものは上記例に限定されるものではない。すなわち、上述した実施形態に係る認証システムは、認証デバイスと通信可能な機器が制御できるロック機構であれば、どのようなシステムに適用しても良い。

[0155] 例えば、上述した認証システムは、ロッカーあるいはケースなどのロック

機構を制御するシステムに適用しても良い。具体例としては、介護現場において、介護者が情報端末を操作しながら認証デバイスで被介護者の生体情報を読取らせることにより、被介護者に使用権限が設定されているロッカーの電子錠などのロックを制御するような運用が可能である。このような運用によれば、複介護者が情報端末を用いながら被介護者の動作をサポートすることで、雑な操作が困難な被介護者のロッカーなどを被介護者の生体情報で制御するような運用が実現できる。このような運用によれば、介護者によるサポートを得ながらも生体情報でのセキュリティ性を維持しつつロッカーなどを運用することが可能となる。

[0156] 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。