明　細　書

発明の名称 ： 携帯可能電子装置およびＩＣカード

技術分野

[0001]　本発明の実施形態は、携帯可能電子装置およびＩＣカードに関する。

背景技術

[0002]　従来、携帯可能電子装置としてのＩＣカードには、パスワードを用いて人物認証を行う機能を有するものがある。例えば、ＩＣカードには、アプリケーションプログラム（以下、アプリケーション）に依存しない共通のパスワードが登録されたり、アプリケーション毎に設定されるパスワードが登録されたりすることがある。近年、ＩＣカードは、多用途化が進み、複数のパスワードを登録されるものが多くなってきている。

[0003]　ＩＣカードは、パスワード照合として、ユーザが入力するパスワードと登録されているパスワードとが一致するか否かを照合する。複数のパスワードや認証方法が登録されている場合、ＩＣカードのユーザは、使用目的ごとの複数のパスワード等を記憶しておき、当該ＩＣカードの使用目的に応じたパスワードを入力する必要がある。一方、ユーザの利便性を考慮して、１つのＩＣカードに単一のパスワードだけを登録するように運用すると、セキュリティが低くなってしまう。

先行技術文献

特許文献

[0004] 特許文献1：日本国特開２００７－１５７００２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に、本発明は、生体認証を用いて利便性を高めながらセキュリティを向上できる携帯可能電子装置およびＩＣカードを提供する。

課題を解決するための手段

[0006] 実施形態によれば、携帯可能電子装置は、生体センサと、通信インターフェースと、第１メモリと、第２メモリと、プロセッサと、を有する。生体センサは、人物の生体情報を取得する。通信インターフェースは、上位装置と通信する。第１メモリは、登録者の生体情報を記憶する。第２メモリは、パスワードを記憶する。プロセッサは、通信インターフェースにより上位装置から受信する生体認証を要求するコマンドに応じて生体センサが取得する生体情報と第１メモリが記憶する生体情報とによる生体認証を実行し生体認証が成功した場合に第２メモリが記憶するパスワードの照合状態を照合済とする。

図面の簡単な説明

[0007] [図1]図１は、実施形態に係る携帯可能電子装置としてのＩＣカードの構成例を示すブロック図である。

[図2]図２は、実施形態に係る携帯可能電子装置としてのＩＣカードによる照合コマンドに対する処理例を説明するためのフローチャートである。

[図3]図３は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される照合コマンドの例を示す図である。

[図4]図４は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される照合コマンドの例を示す図である。

[図5]図５は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される照合コマンドの例を示す図である。

[図6]図６は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される照合コマンドにおける第１パラメータの設定例を示す図である。

[図7]図７は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される照合コマンドにおける第２パラメータの設定例を示す図である。

[図8]図８は、実施形態に係る携帯可能電子装置としてのＩＣカードにおける複数のパスワードの照合状態（照合結果）を格納するテーブルの例を示す図である。

[図9]図９は、実施形態に係る携帯可能電子装置としてのＩＣカードによる照

合コマンドに対するパスワード照合の処理例を説明するためのフローチャートである。

[図10]図１０は、実施形態に係る携帯可能電子装置としてのＩＣカードにおける複数のパスワードの管理情報を格納するテーブルの例を示す図である。

[図11]図１１は、実施形態に係る携帯可能電子装置としてのＩＣカードによるバイナリ読出コマンドに対する処理例を説明するためのフローチャートである。

[図12]図１２は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給されるバイナリ読出コマンドの例を示す図である。

[図13]図１３は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給されるバイナリ読出コマンドにおける第１パラメータの設定例を示す図である。

[図14]図１４は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される照合コマンドにおける第２パラメータの設定例を示す図である。

[図15]図１５は、実施形態に係る携帯可能電子装置としてのＩＣカードにおけるデータ（ＥＦ）の管理情報を格納するテーブルの例を示す図である。

[図16]図１６は、実施形態に係る携帯可能電子装置としてのＩＣカードにおけるデータ（ＥＦ）の構成例を示す図である。

[図17]図１７は、実施形態に係る携帯可能電子装置としてのＩＣカードによる照合コマンドに対する処理例を説明するためのフローチャートである。

[図18]図１８は、実施形態に係る携帯可能電子装置としてのＩＣカードにおいて指紋登録データに紐づけたパスワードを示す情報を格納するテーブルの例を示す図である。

[図19]図１９は、実施形態に係る携帯可能電子装置としてのＩＣカードにおける複数のパスワードの管理情報を格納するテーブルの例を示す図である。

[図20]図２０は、実施形態に係る携帯可能電子装置としてのＩＣカードによる照合コマンドに対する処理例を説明するためのフローチャートである。

[図21]図２１は、実施形態に係る携帯可能電子装置としてのＩＣカードにお

ける複数のパスワードの管理情報を格納するテーブルの例を示す図である。

[図22]図２２は、実施形態に係る携帯可能電子装置としてのＩＣカードによる照合コマンドに対する処理例を説明するためのフローチャートである。

[図23]図２３は、実施形態に係る携帯可能電子装置としてのＩＣカードにおけるＩＥＦ毎に登録される指紋登録データの管理情報を格納するテーブルの例を示す図である。

[図24]図２４は、実施形態に係る携帯可能電子装置としてのＩＣカードによる特定コマンドに対する生体認証を含む処理例を説明するためのフローチャートである。

[図25]図２５は、実施形態に係る携帯可能電子装置としてのＩＣカードによる特定コマンドに対する生体認証を含む処理例を説明するためのフローチャートである。

[図26]図２６は、実施形態に係る携帯可能電子装置としてのＩＣカードによる図２５に示す処理の第１の変形例を説明するためのフローチャートである。

[図27]図２７は、実施形態に係る携帯可能電子装置としてのＩＣカードによる図２５に示す処理の第２の変形例を説明するためのフローチャートである。

[図28]図２８は、実施形態に係る携帯可能電子装置としてのＩＣカードによる図２５に示す処理の第３の変形例を説明するためのフローチャートである。

[図29]図２９は、実施形態に係る携帯可能電子装置としてのＩＣカードによる図２５に示す処理の第４の変形例を説明するためのフローチャートである。

[図30]図３０は、実施形態に係る携帯可能電子装置としてのＩＣカードによる図２５に示す処理の第５の変形例を説明するためのフローチャートである。

[図31]図３１は、実施形態に係る携帯可能電子装置としてのＩＣカードによ

る図２５に示す処理の第６の変形例を説明するためのフローチャートである。

[図32]図３２は、実施形態に係る携帯可能電子装置としてのＩＣカードによる図２５に示す処理の第７の変形例を説明するためのフローチャートである。

実施形態

[0008] 以下、実施形態について、図面を参照しつつ説明する。

まず、実施形態に係る携帯可能電子装置としてのＩＣカード１の構成について説明する。

図１は、実施形態に係る携帯可能電子装置としてのＩＣカード１の構成例を示すブロック図である。

ＩＣカード１は、外部装置から供給される電力により活性化する（動作可能な状態になる）携帯可能電子装置の一例である。ＩＣカード１は、上位装置からのコマンドに応じて処理を実行する。本実施形態において、携帯可能電子装置としてのＩＣカード１は、生体情報を用いて認証を実行する機能を有するものとする。例えば、ＩＣカード１は、スマートカードとも称される。また、ＩＣカード１は、携帯可能電子装置の他の例としてのスマートフォンなどのモバイル端末が備える１つの機能に置き換えて実施しても良い。

[0009] 実施形態に係る携帯可能電子装置としてのＩＣカード１は、人物から取得する生体情報を用いた生体照合によって人物を認証する生体認証機能を有する。実施形態では、ＩＣカード１は、生体情報の一例としての指紋を用いた指紋照合によって人物を認証する生体（指紋）認証機能を有するものとして説明する。ただし、実施形態に係る携帯可能電子装置としてのＩＣカード１が備える生体認証機能は、指紋による生体照合に限定されるものではない。例えば、ＩＣカード１で例示される携帯可能電子装置は、指紋以外の生体情報によって生体認証を行うものであっても良い。

[0010] 図１に示す構成例において、ＩＣカード１は、本体Ｃを有する。本体Ｃは、例えば、プラスチックなどによりカード状に形成される。ＩＣカード１は

、本体Ｃ内に制御部１１としてのモジュールＭ、生体照合部１２およびＬＥＤ１３などを備える。例えば、モジュールＭは、１つ又は複数のＩＣチップに通信インターフェースが接続された状態で一体的に形成される。制御部１１としてのモジュールＭは、ＭＰＵ３１および生体センサ３２を有する生体照合部１２、および、ＬＥＤ１３に接続された状態で本体Ｃに設けられる。

[0011] 図１に示す構成例において、制御部１１を構成するモジュールＭは、プロセッサ２１、ＲＯＭ２２、ＲＡＭ２３、データメモリ２４および通信インターフェース２５を有する。 プロセッサ２１は、種々の処理を実行する回路を含む。プロセッサ２１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）である。プロセッサ２１は、ＩＣカード１全体の制御を司る。プロセッサ２１は、ＲＯＭ２２あるいはデータメモリ２４に記憶されているプログラムを実行することにより、種々の処理機能を実現する。ただし、後述するプロセッサ２１が実行する各種の機能のうち一部又は全部は、ハードウエア回路により実現されるようにしても良い。

[0012] ＲＯＭ２２は、プログラムメモリとして機能する不揮発性のメモリである。ＲＯＭ２２は、予め制御用のプログラムおよび制御データなどが記憶される。ＲＯＭ２２は、製造段階で制御プログラムや制御データなどが記憶された状態でＩＣカード１内に組み込まれるものである。ＲＯＭ２２に記憶される制御プログラムや制御データは、予め当該ＩＣカード１の仕様に応じて組み込まれる。例えば、ＲＯＭ２２には、外部装置（カードリーダライタ）から受信するコマンドに応じた処理をプロセッサ２１が実行するためのプログラムが記憶される。

[0013] ＲＡＭ２３は、ワーキングメモリとして機能する揮発性のメモリである。また、ＲＡＭ２３は、プロセッサ２１が処理中のデータなどを一時保管するバッファとしても機能する。例えば、ＲＡＭ２３は、通信インターフェース２５を介して外部装置との間で送受信するデータを一時保管する通信バッファとして機能する。

[0014] データメモリ２４は、データの書き込みおよび書換えが可能な不揮発性の

メモリである。データメモリ２４は、例えば、ＥＥＰＲＯＭ（登録商標）（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）などで構成する。データメモリ２４には、当該ＩＣカード１の運用用途に応じたプログラムや種々のデータが書き込まれる。データメモリ２４には、プログラムファイルあるいはデータファイルなどが定義され、それらのファイルに制御プログラムや種々のデータが書き込まれる。また、データメモリ２４は、一部又は全部の領域が耐タンパー性を有し、セキュアにデータが格納できる。

[0015] データメモリ２４は、正当な利用者（登録者）の生体情報（認証データ）を記憶する第１メモリとパスワード照合を行うためのパスワード登録データを記憶する第２メモリとを含む。また、データメモリ２４は、後述する各種のテーブルを記憶する。

[0016] 例えば、第１メモリとしてのデータメモリ２４は、生体認証を実行するためのデータとして登録者の生体情報（生体登録データ）を記憶する。ＩＣカード１が指紋による生体認証を実行する場合、データメモリ２４は、登録者の指紋データ（指紋登録データ）を記憶する。登録者の指紋データは、生体センサ３２としての指紋センサで取得する指紋情報と照合するための指紋画像又は指紋の特徴データである。また、データメモリ２４には、１人の登録者に対して複数の指ごとに指紋データを登録して良い。また、１つのＩＣカード１を複数の利用者が使用する場合、データメモリ２４には、正当な利用者である複数の登録者の指紋データを登録するようにしても良い。

[0017] 通信インターフェース２５は、通信制御部とインターフェース部とを有し、通信部を構成する。通信インターフェース２５は、当該ＩＣカード１に対して電源電力およびコマンドを供給する上位装置と通信するためのインターフェースである。通信インターフェース２５は、外部装置のインターフェースに対応した通信方式による通信機能を実現する。また、通信インターフェース２５は、複数の通信方式（例えば、接触通信と非接触通信）をサポートするものとして構成しても良い。

[0018] 当該ＩＣカード１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、外部装置と接触して通信する通信部を構成する。この場合、通信インターフェース２５は、外部装置のカードリーダライタに設けられたコンタクト部と物理的かつ電気的に接触するコンタクト部を備え、コンタクト部を介した信号の送受信を制御する通信制御回路などにより構成される。

[0019] また、当該ＩＣカード１が非接触型の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、外部装置のカードリーダライタと非接触（無線）で通信する通信部を構成する。この場合、通信インターフェース２５は、電波の送受信を行うアンテナを備え、アンテナから送信する電波を生成するための変調回路およびアンテナが受信した電波から信号を生成するための復調回路などにより構成される。

[0020] 生体照合部１２は、ＭＰＵ３１および生体センサ３２を有し、制御部１１としてのモジュールＭに接続される。また、生体照合部１２は、ＭＰＵ３１が生体（指紋）照合による生体認証を実行するための認証用プログラムなどを記憶するメモリも有する。

[0021] 生体センサ３２は、生体情報としての指紋情報を取得する生体情報取得部の一例である。本実施形態において、生体センサ３２は、利用者の指紋情報（指紋画像）を読み取る指紋センサである。生体センサ３２としての指紋センサは、指紋を読み取るセンサがＩＣカード１の本体Ｃの表面に露出するように設けられ、露出したセンサ部分に翳された人物の指の指紋を読み取る。なお、生体センサ３２は、指紋センサに限定されるものではなく、指紋以外の生体情報を取得するものであっても良い。

[0022] ＭＰＵ３１は、生体認証用のプログラムを実行することにより生体センサ３２が取得する生体情報としての指紋情報を用いた生体認証を実行する。例えば、ＭＰＵ３１は、生体センサ３２としての指紋センサが読み取った画像から指紋画像を抽出し、指紋センサが読み取った画像から抽出した指紋画像とデータメモリ２４に登録している登録者の指紋画像（又は指紋の特徴デー

タ）とを照合するにより指紋認証を実行する。

[0023] なお、図１に示す構成例では、プロセッサ２１とは別に設けたＭＰＵ３１が生体（指紋）照合による生体認証を実行する構成としたが、プロセッサ２１が生体認証を実行するようにしても良い。プロセッサ２１に生体認証を実行させる場合、生体センサ３２が読み取った生体情報がプロセッサ２１へ供給されるようにすれば良い。例えば、プロセッサ２１は、生体センサ３２としての指紋センサから供給される画像から指紋情報を抽出し、抽出した指紋情報とデータメモリ２４に登録している登録者の指紋情報とを照合するようにすれば良い。

[0024] ＬＥＤ１３は、発光素子を有する。ＬＥＤ１３は、制御部１１の制御によって発光素子の発光状態が制御される。ＬＥＤ１３は、例えば、点灯状態が本体Ｃの表面において視認できる状態で本体Ｃに設けられる。

[0025] 次に、本実施形態に係るＩＣカード１の動作について説明する。

実施形態に係るＩＣカード１は、国際規格などで標準化されたＩＣカードに用いられる既存の通信プロトコルに準じて動作する機能を有する。また、ＩＣカード１は、生体センサ３２が取得する生体情報を用いた生体認証機能、および、パスワード照合による認証機能を有する。ＩＣカード１は、パスワード照合に用いる少なくとも１つ以上のパスワードデータを記憶（保持）する。実施形態に係るＩＣカード１は、パスワード照合の一部又は全部を生体認証に書き換えることが可能な機能を有する。

[0026] 以下、ＩＣカード１において、生体認証が成功した場合に一部又は全部のパスワードの照合状態（照合結果）を照合済（照合成功、照合ＯＫ）の状態に書き換えるための幾つかの動作例について説明する。

図２は、ＩＣカード１が照合コマンドを受信した場合の処理例とＩＣカード１における生体認証の成功に応じて全てのパスワードの照合結果を照合済に置き換える処理例とを示すフローチャートである。

[0027] ＩＣカード１は、上位装置からの電源電力の供給を受けて起動し、上位装置からのコマンドが受信可能な状態となる。ＩＣカード１のプロセッサ２１

は、通信インターフェース２５を介して上位装置からの所定のフォーマットで構成されるコマンドを受信し、受信したコマンドで要求された処理を実行する。

[0028] 図２に示すように、ＩＣカード１のプロセッサ２１は、通信インターフェース２５を介して上位装置からのコマンドを受信した場合（Ｓ１１、ＹＥＳ）、受信したコマンドが照合を要求する照合コマンドであるか否かを判断する（Ｓ１２）。ここで、上位装置からＩＣカード１に供給されるコマンドは、予め規定されている規格に準じて構成されるものとする。ＩＣカード１のプロセッサ２１は、ＲＯＭ２２又はデータメモリ２４に記憶されているプログラムを実行することにより、規格に準じて構成されるコマンドを解釈し、コマンドに応じた処理を実行する。

[0029] 本実施形態において、プロセッサ２１は、受信したコマンドが照合コマンドでない場合（Ｓ１２、ＮＯ）、当該コマンドで指定されたコマンド処理を実行する（Ｓ１３）。他のコマンド処理の一例としては、バイナリデータ読出コマンドに対する処理について後で説明する。

受信したコマンドが照合コマンドである場合（Ｓ１２、ＹＥＳ）、プロセッサ２１は、受信した照合コマンドが処理内容を示す情報として指定するパラメータをチェックし、パラメータで指定される内容の処理を実行する。

[0030] 図３乃至５は、上位装置からＩＣカード１に供給される照合コマンドの構成例を示す図である。

本実施形態において、上位装置からＩＣカード１に供給されるコマンドは、図３乃至５に示すように、「ＣＬＡ」、「ＩＮＳ」、Ｐ１」、「Ｐ２」、「Ｌｃ」、および、「Ｄａｔａ」を並べたフォーマットで構成されるものとする。「ＣＬＡ」および「ＩＮＳ」は、コマンドの内容を示す。例えば、照合コマンドは、図３乃至５に示すように、「ＣＬＡ」「ＩＮＳ」が「００」「２０」となる。また、「Ｐ１」および「Ｐ２」は、「ＣＬＡ」および「ＩＮＳ」で示されるコマンドに応じた意味が定義されるパラメータである。「Ｌｃ」は、「Ｄａｔａ」に格納されるデータの長さを示し、「Ｄａｔａ」は

、添付されるデータを示す。

[0031] 図６は、照合コマンドにおける第１のパラメータである「Ｐ１」の意味を示す図である。

図６に示す例では、照合コマンドにおける「Ｐ１」が「００」である場合、当該照合コマンドがパスワード照合を要求するコマンドであることを示す。例えば、図５に示す照合コマンドは、「Ｐ１」が「００」であるため、パスワード照合を要求するコマンドであることを示す。図５に示すコマンドでは、「Ｄａｔａ」に「Ｌｃ」が示す長さ（サイズ）のパスワードデータ（入力パスワードデータ）が格納される。

[0032] また、図６では、照合コマンドにおける「Ｐ１」が「０１」である場合、当該照合コマンドが指紋情報の入力および照合（生体認証）を要求するコマンドであることを示す。例えば、図３および図４に示す照合コマンドは、「Ｐ１」が「０１」であるため、生体認証を要求するコマンドであることを示す。

[0033] 図６に例示するような定義に従って、プロセッサ２１は、照合コマンドがパスワード照合を指定するものであるか否かを判断する（Ｓ１４）。ここでは、プロセッサ２１は、照合コマンドにおけるパラメータ「Ｐ１」が「００」であるか否かによりパスワード照合であるか否かを判断するものとする。

受信した照合コマンドのＰ１が「００」である場合、つまり、照合コマンドがパスワード照合を要求するコマンドである場合（Ｓ１４、ＹＥＳ）、プロセッサ２１は、パスワード照合を実行する（Ｓ１５）。パスワード照合の処理については、後で詳細に説明する。

[0034] 受信した照合コマンドのＰ１が「００」でない場合、つまり、照合コマンドがパスワード照合を要求するコマンドでない場合（Ｓ１４、ＮＯ）、プロセッサ２１は、照合コマンドが生体（指紋）認証を要求するものであるか否かを判断する（Ｓ１６）。

受信した照合コマンドのＰ１が「００」でも「０１」でもない場合、つまり、照合コマンドがパスワード照合も生体認証も指定していない場合（Ｓ１

６、ＮＯ）、プロセッサ２１は、照合コマンドによる照合方法の指定が不明（Ｐ１の値が異常）であると判定する。この場合、プロセッサ２１は、照合コマンドにおけるＰ１の値が異常であることを示すエラー通知を含むステータスワードを生成し、生体したステータスワードを当該コマンドに対する応答として上位装置へ送信し（Ｓ１７）、次のコマンド受信待ち状態となる。

[0035] 受信した照合コマンドのＰ１が「０１」である場合、つまり、照合コマンドが生体照合を要求するコマンドである場合（Ｓ１６、ＹＥＳ）、プロセッサ２１は、生体認証の結果を反映させるパスワード（生体認証の成功に応じて照合済とするパスワード）を特定する。ここでは、プロセッサ２１は、当該照合コマンドにおける第２のパラメータであるＰ２の値に基づいて生体認証の認証結果を反映させるパスワードを特定するものとする。

[0036] 図７は、照合コマンドにおける第２のパラメータである「Ｐ２」の意味を示す図である。

図７に示す設定例では、照合コマンドにおける「Ｐ１」が「００」である場合、「Ｐ２」に格納される値が生体認証の成功に応じて照合状態（照合結果）を照合済（照合成功、ＯＫ）とするパスワードを示す情報となる。

[0037] 図７に示す定義に従えば、ＩＣカード１は、上位装置から受信する「Ｐ１」が「０１」のコマンド（生体認証を要求する照合コマンド）における「Ｐ２」が「ＦＦ」である場合、生体認証の成功に応じて全てのパスワードに対する照合結果を照合済（照合成功、照合ＯＫ）にセットされるものと解釈する。つまり、図３に示すような「Ｐ２」が「ＦＦ」である照合コマンドを受信した場合、ＩＣカード１は、生体認証の成功に応じて全てのパスワードに対する照合結果を照合済にセットする処理を実行する。

[0038] また、生体認証を要求する照合コマンドにおける「Ｐ２」が「ＦＥ」である場合、ＩＣカード１は、生体認証が成功すると生体照合が成功した生体情報（指紋登録データ）に紐づけられたパスワードに対する照合結果を照合済（照合成功、照合ＯＫ）にセットするものと解釈する。つまり、図４に示すような「Ｐ２」が「ＦＥ」である照合コマンドを受信した場合、ＩＣカード

１は、生体認証の成功に応じて生体照合に用いた指紋登録データに紐づけられたパスワードに対する照合結果を照合済にセットする処理を実行する。

[0039] また、生体認証を要求する照合コマンドにおける「Ｐ２」が特殊値（例えば、「ＦＦ」および「ＦＥ」）以外の値である場合、Ｐ２の値が生体認証の成功に応じて照合結果を照合済とするパスワードを示す値（ＩＥＦ：Ｉｎｔｅｒｎａｌ　Ｅｌｅｍｅｎｔａｒｙ　Ｆｉｌｅ）であるものと解釈する。つまり、生体認証を要求する照合コマンドにおける「Ｐ２」がパスワードを示す値（ＩＥＦ：Ｉｎｔｅｒｎａｌ　Ｅｌｅｍｅｎｔａｒｙ　Ｆｉｌｅ）である場合、ＩＣカード１は、生体認証の成功に応じて指定されたパスワード（ＩＥＦ）に対する照合結果を照合済（照合成功、照合ＯＫ）にセットするものと解釈する。

[0040] ここで、プロセッサ２１は、図７に例示する定義に従って動作するものとする。この場合、プロセッサ２１は、受信した照合コマンドのＰ２が「ＦＦ」である場合に生体認証の成功に応じて全てのパスワードの照合結果を照合済とするものと判断する。つまり、受信した照合コマンドのＰ１が「０１」で、かつ、Ｐ２が「ＦＦ」ある場合（Ｓ１８、ＹＥＳ）、プロセッサ２１は、生体認証の成功に応じて全てのパスワードの照合結果を照合済とするものと解釈し、生体照合部１２に生体情報の入力および生体照合を実行させる（Ｓ２０、Ｓ２１）。

[0041] 例えば、プロセッサ２１は、データメモリ２４に登録されている登録者の指紋データ（指紋登録データ）を生体照合部１２へ送信し、生体照合部１２に生体センサ３２による指紋データ（入力指紋データ）の入力および指紋登録データと入力指紋データとの照合とを指示する。生体照合部１２のＭＰＵ３１は、プロセッサ２１の制御によって供給される指紋登録データを保持し、生体センサ３２による指紋データの入力を行う（Ｓ２０）。生体センサ３２が指紋データを入力すると、ＭＰＵ３１は、生体センサ３２が取得した指紋データ（入力指紋データ）と指紋登録データとを照合し（Ｓ２１）、その照合結果をプロセッサ２１へ供給する。

[0042] プロセッサ２１は、生体照合部１２からの照合結果に応じて生体認証が成功したか否かを判断する。また、プロセッサ２１は、ＬＥＤ１３を生体認証の結果に応じて点灯させる。例えば、プロセッサ２１は、生体照合部１２における生体情報の入力および生体照合を実行中には生体認証が実行中であることを示す点灯状態でＬＥＤ１３を点灯させる。さらに、プロセッサ２１は、生体認証が成功した場合には生体認証が成功したことを示す点灯状態でＬＥＤ１３を点灯させ、生体認証が失敗した場合には生体認証が失敗したことを示す点灯状態でＬＥＤ１３を点灯させる。

[0043] 生体照合部１２での生体照合による生体認証が失敗した場合（Ｓ２２、ＹＥＳ）、プロセッサ２１は、照合失敗（ＮＧ）を示すステータスワードを生成し、生成したステータスワードを照合コマンドの送信元である上位装置へ送信する（Ｓ２３）。

生体照合部１２での生体照合による生体認証が成功した場合（Ｓ２２、ＹＥＳ）、プロセッサ２１は、全てのパスワード（ＩＥＦ）に対して照合結果が照合済み（成功、ＯＫ）であることを示す情報（フラグ）を記憶する（Ｓ２４）。

[0044] 図８は、パスワードに対する照合結果（照合状態）を記録するパスワード照合の照合状態テーブルの構成例を示す図である。

図８に示す例は、全てのパスワードに対する照合状態が照合済みであることを示す情報を照合状態テーブルに記憶した状態を示す。図８に示すような照合状態テーブルは、データメモリ２４又はＲＡＭ２３に設けられる。例えば、プロセッサ２１は、図８に示すような照合状態テーブルをデータメモリ２４に設け、生体照合部１２による生体照合による生体認証が成功した場合に照合状態テーブルにある全てのパスワードに対する照合結果（照合状態）を照合済であることを示す情報にセットする。

[0045] 生体認証を要求する照合コマンドの第２パラメータ（Ｐ２）が「ＦＦ」である場合、プロセッサ２１は、生体照合部１２による生体照合が成功すると（Ｓ２２、ＹＥＳ）、全てのパスワードに対して照合結果が照合済（照合成

功）であることを示す情報（フラグ）を記憶する（Ｓ２４）。生体認証の成功に応じて全てのパスワードに対する照合結果を照合済とした後、プロセッサ２１は、当該照合コマンドの送信元である上位装置へ正常終了を示すステータスワードを送信し（Ｓ２５）、照合コマンドに対する一連の処理を終了する。

[0046] 次に、図２に示すＳ１５の処理としてのパスワード照合処理について説明する。

図９は、ＩＣカード１におけるパスワード照合処理の処理例を説明するためのフローチャートである。

上述したように、図２に示す処理において、受信した照合コマンドにおける第１パラメータ（Ｐ１）が「００」である場合（Ｓ１４、ＹＥＳ）、プロセッサ２１は、パスワード照合処理を実行する（Ｓ１５）。

[0047] 図９に示すパスワード照合処理の処理例において、プロセッサ２１は、受信したパスワード照合を要求する照合コマンドにおける第２パラメータ（Ｐ２）で指定されるＩＥＦが存在するか否かを判定する（Ｓ３１）。ＩＥＦは、データメモリ２４に記憶されるパスワードを格納するファイルである。プロセッサ２１は、受信したパスワード照合を要求する照合コマンドが指定するＩＥＦが存在するか否かにより指定されたパスワードが存在するか否かを判定する。

[0048] 図１０は、パスワードを管理するパスワード管理テーブルの例を示す図である。

図１０に示す例において、パスワード管理テーブルには、ＩＥＦごとに、パスワード登録データ、長さ情報、リトライカウンタ、および、リトライカウンタの初期値が対応づけて記憶される。ＩＥＦは、パスワード（ＩＥＦ）を示す識別情報（ＩＤ）としての番号で特定される。パスワード登録データは、予め登録されるパスワードデータである。長さ情報は、パスワード登録データとして格納されるパスワードデータの長さを示す。

[0049] リトライカウンタは、対応するパスワードを用いてパスワード照合が実行

可能な残り回数（リトライ数）を示す値を格納する。リトライカウンタの初期値は、対応するパスワードによる照合の上限値を示す。リトライカウンタは、リセットされると上限値であるリトライカウンタの初期値がセットされ、照合が失敗するごとにカウントダウンされるカウンタである。リトライカウンタは、対応するパスワードによる照合状態が照合成功となった場合に初期値に戻される。ただし、リトライカウンタが０である場合、当該ＩＣカード１は、ロック状態となるため、パスワード照合などによってリトライカウンタを初期値に戻すことはできなくなる。

[0050] 受信した照合コマンドで指定されるＩＥＦが存在しない場合（Ｓ３１、ＮＯ）、プロセッサ２１は、指定されたＩＥＦ（パスワード）が無いことを示すステータスワードを生成し、生成したステータスワードを当該照合コマンドの送信元である上位装置へ送信する（Ｓ３２）。指定されたＩＥＦが無いことを示すステータスワードを送信した場合、プロセッサ２１は、次のコマンドの入力待ち状態となる。

[0051] 受信した照合コマンドで指定されるＩＥＦが存在する場合（Ｓ３１、ＹＥＳ）、プロセッサ２１は、受信した照合コマンドが指定するＩＥＦがロック状態ではないか否かを判定する（Ｓ３３）。プロセッサ２１は、図１０に示すようなパスワード管理テーブルに格納されるリトライカウンタの値に基づいてコマンドで指定されたパスワード（ＩＥＦ）がロック状態であるか否かを判断する。例えば、プロセッサ２１は、指定されたＩＥＦに対応するリトライカウンタが０であれば当該ＩＥＦがロック状態であると判断する。

[0052] 照合コマンドで指定されたＩＥＦがロック状態である場合（Ｓ３３、ＹＥＳ）、プロセッサ２１は、ロック状態を示すステータスワードを生成し、生成したステータスワードを当該照合コマンドの送信元である上位装置へ送信する（Ｓ３４）。指定されたＩＥＦがロック状態であることを示すステータスワードを送信した場合、プロセッサ２１は、次のコマンドの入力待ち状態となる。

[0053] 照合コマンドで指定されるＩＥＦがロック状態でない（アンロック状態で

ある）場合（Ｓ３３、ＹＥＳ）、プロセッサ２１は、当該照合コマンドのＤａｔａに格納されるパスワードデータ（入力パスワード）と当該照合コマンドが指定するＩＥＦのパスワードデータ（パスワード登録データ）とを照合する（Ｓ３５）。入力パスワードと指定ＩＥＦのパスワード登録データとが一致する場合、プロセッサ２１は、当該照合コマンドが要求するパスワード照合が成功したものと判断する。また、入力パスワードと指定ＩＥＦのパスワード登録データとが一致しない場合、プロセッサ２１は、当該照合コマンドが要求するパスワード照合が失敗したものと判断する。

[0054] パスワード照合が失敗した場合（Ｓ３６、ＮＯ）、プロセッサ２１は、指定ＩＥＦに対するリトライカウンタをカウントダウンすることでリトライ数を改めてセットし、照合結果を示す情報（フラグ）を未照合の状態にリセットする（Ｓ３７）。さらに、プロセッサ２１は、パスワード照合が失敗したことを示すステータスワードを照合コマンドの送信元である上位装置へ送信し（Ｓ３８）、次のコマンド受信待ちの状態となる。

[0055] パスワード照合が成功した場合（Ｓ３６、ＹＥＳ）、プロセッサ２１は、指定ＩＥＦに対するリトライカウンタを初期値にすることでリトライ数を初期値にリセットし、照合結果を示す情報（フラグ）を照合済（照合成功）の状態にセットする（Ｓ３９）。さらに、プロセッサ２１は、パスワード照合が成功したことを示すステータスワードを照合コマンドの送信元である上位装置へ送信し（Ｓ４０）、次のコマンド受信待ちの状態となる。

[0056] 次に、ＩＣカード１におけるコマンド処理の一例としてのバイナリデータの読出を要求するバイナリ読出コマンドに対するコマンド処理（データ読出処理）について説明する。 図１１は、ＩＣカード１によるコマンド処理の一例としてのバイナリ読出コマンドに対するデータ読出処理を説明するためのフローチャートである。

上述したような図２に示す処理において、受信したコマンドが照合コマンドでない場合（Ｓ１２、ＮＯ）、プロセッサ２１は、受信したコマンドに応じたコマンド処理を実行する（Ｓ１３）。図１１に示す処理例では、受信し

たコマンドがバイナリデータの読出を要求するバイナリ読出コマンドであった場合の処理例を示す。

[0057] 図１２は、バイナリ読出コマンドの構成例を示す図である。また、図１３は、バイナリ読出コマンドにおける第１のパラメータ（Ｐ１）の構成例を示す図である。図１４は、バイナリ読出コマンドにおける第２のパラメータ（Ｐ２）の構成例を示す図である。

図１２に示すように、バイナリ読出コマンドは、「ＣＬＡ」「ＩＮＳ」が「００」「Ｂ０」となる。また、バイナリ読出コマンドの「Ｐ１」は、読出対象となるバイナリデータを示す値を格納する。図１３に示す例において、バイナリ読出コマンドの「Ｐ１」には、読出対象となるデータが格納されるファイル（ＥＦ：Ｅｌｅｍｅｎｔａｒｙ　Ｆｉｌｅ）を示す値が格納される。バイナリ読出コマンドの「Ｐ２」は、読出対象となるアドレスを示す値を格納する。図１４に示す例において、バイナリ読出コマンドの「Ｐ２」には、「Ｐ１」で指定されるＥＦにおける読出位置を示すアドレス（相対アドレス）が格納される。

[0058] 図１５は、データを格納するＥＦの管理情報を記憶するＥＦ管理テーブルの例を示す図である。また、図１６は、データメモリ２４におけるＥＦの構成例を示す図である。

図１５に示すようなＥＦ管理テーブルは、例えば、データメモリ２４に記憶される。ＥＦ管理テーブルでは、各ＥＦに対して、サイズ、物理アドレス、読み出しアクセス権、書き込みアクセス権などを示すデータが格納される。サイズは、当該ＥＦにおける実データのサイズを示す。物理アドレスは、当該ＥＦの実データが格納されるデータメモリ２４における場所（書込み開始位置）を示す。

[0059] 読み出しアクセス権は、当該ＥＦに対するデータの読み出し権限を示す情報が記憶される。例えば、読み出しアクセス権において、「００」は、当該ＥＦのデータに対するアクセスがフリーであることを示す。「０ｘ」は、当該ＥＦのデータにアクセスするにはＩＥＦ（０ｘ）に格納される認証情報に

よる照合が成功したことが必要であることを示す。ここで、番号（ＩＤ）がｘｘのＩＥＦをＩＥＦ（ｘｘ）と示すものとする。

[0060] 図１５に示すようなＥＦ管理テーブルでは、当該ＥＦに対する読み出しアクセス権、書き込みアクセス権を示す情報が記憶される。読み出しアクセス権が「０１」であるＥＦのデータを読み出すには、ＩＥＦ（０１）のパスワードによるパスワード照合の照合結果が照合済であることが必要であることを示す。読み出しアクセス権が「０１」、「０２」、「０３」、「０４」であるＥＦは、ＩＥＦ（０１）、ＩＥＦ（０２）、ＩＥＦ（０３）、ＩＥＦ（０４）のパスワードの照合結果が照合済であることがデータを読み出すための条件（権限）として必要であることを示し、「００」は、当該ＥＦのデータに対するアクセスがフリーであることを示す。

[0061] 書き込みアクセス権が「０４」であるＥＦのデータを読み出すには、ＩＥＦ（０４）のパスワードによるパスワード照合の照合結果が照合済であることが必要であることを示す。書き込みアクセス権が「０１」、「０２」、「０３」、「０４」であるＥＦは、ＩＥＦ（０１）、ＩＥＦ（０２）、ＩＥＦ（０３）、ＩＥＦ（０４）のパスワードの照合結果が照合済であることがデータを書き込むための条件（権限）として必要であることを示し、「００」は、当該ＥＦのデータに対するアクセスがフリーであることを示す。

[0062] また、ＥＦは、図１６に示すように、図１５に示すようなＥＦ管理テーブルで指定される物理アドレスに実データが記憶される。例えば、図１６に示すアドレス「１０００ｈ」に記憶される「実データ１」は、図１５に示すＥＦ「０１」（データ番号が「０１」のＥＦ）のサイズが「１００ｈ」のデータであり、読み出しアクセス権が「００」で、書き込みアクセス権が「０４」であることを意味する。

[0063] 図１１に示す処理例において、受信したコマンドがバイナリ読出コマンドでない場合（Ｓ５１、ＮＯ）、プロセッサ２１は、受信したコマンドに応じたコマンド処理を実行する（Ｓ５２）。受信したコマンドがバイナリ読出コマンドである場合（Ｓ５１、ＹＥＳ）、プロセッサ２１は、受信したバイナ

リ読出コマンドの「Ｐ１」および「Ｐ２」に格納された値に応じてデータの読出処理を実行する。

[0064] すなわち、バイナリ読出コマンドを受信した場合（Ｓ５１、ＹＥＳ）、プロセッサ２１は、当該コマンドで指定される読出対象とするデータのファイル（ＥＦ）が存在するか否かを判定する（Ｓ５３）。バイナリ読出コマンドで指定されたＥＦが存在しない場合（Ｓ５３、ＮＯ）、プロセッサ２１は、指定されたデータ（ＥＦ）が存在しないことを示すステータスワードを当該コマンドの送信元である上位装置へ送信し（Ｓ５４）、次のコマンドの受信待ち状態となる。

[0065] 受信したバイナリ読出コマンドで指定されたデータ（ＥＦ）が存在する場合（Ｓ５３、ＹＥＳ）、プロセッサ２１は、指定されたＥＦに対する読み出しアクセス権を確認する（Ｓ５５）。例えば、プロセッサ２１は、指定されたＥＦに対する読み出しアクセス権を図１５に示すようなＥＦ管理テーブルに格納されている情報を参照して確認する。

[0066] バイナリ読出コマンドで指定されたＥＦに対する読み出しアクセス権を満たしていない場合（Ｓ５６、ＮＯ）、プロセッサ２１は、バイナリ読出コマンドで指定されたＥＦからのデータの読出しが不可であると判断する。この場合、プロセッサ２１は、指定されたＥＦのデータを読み出す権限（アクセス権）がないことを示すステータスワードを当該バイナリ読出コマンドの送信元である上位装置へ送信し（Ｓ５７）、次のコマンドの受信待ち状態となる。

[0067] また、バイナリ読出コマンドで指定されたＥＦに対するアクセス権を満たしている場合（Ｓ５６、ＹＥＳ）、プロセッサ２１は、当該コマンドで指定されたＥＦのデータを読み出す（Ｓ５８）。例えば、プロセッサ２１は、ＥＦ管理テーブルに格納された情報を参照し、当該コマンドで相対アドレスとして指定される読出開始位置から当該ＥＦのデータを読み出す。データを読み出すと、プロセッサ２１は、読み出したデータと正常終了を示す情報とを含むステータスワードをバイナリ読出コマンドの送信元である上位装置へ送

信し（Ｓ５９）、次のコマンドの受信待ち状態となる。

[0068] 以上の処理がＩＣカード１において生体認証が成功した場合に全てのパスワードの照合結果を照合済（照合成功）の状態とする処理例である。以上の処理によれば、生体照合の要求に応じて生体認証が成功すると、当該ＩＣカード１に登録されているパスワードに対する照合結果を一律に照合済（照合成功）とすることでき、パスワード照合を簡単な処理でセキュリティ性が高い生体認証に置き換えることができる。また、上述した処理例によれば、ＩＣカードは、生体認証だけでなく、パスワード照合も行えるようにすることで、生体認証機能に不具合が発生した場合であっても、パスワードでの照合を行うことができる。

[0069] 次に、ＩＣカード１における生体認証が成功した場合に生体認証に用いた登録済みの生体情報（指紋登録データ）に紐づいたパスワードの照合結果を照合済の状態にする処理について説明する。

図１７は、ＩＣカード１における生体認証が成功した場合に生体認証に用いた指紋登録データに紐づいたパスワードの照合結果を照合済にセットする処理例を示すフローチャートである。

上述したような図２に示す処理において、受信した照合コマンドのＰ１が「０１」で、かつ、Ｐ２が「ＦＥ」である場合（Ｓ１９、ＹＥＳ）、プロセッサ２１は、図３に示すように、生体認証が成功した場合に指紋登録データに紐づいたパスワードに対する照合結果を照合済にする処理を行う。

[0070] 図１８は、生体認証としての指紋照合に用いる登録者の生体情報としての指紋登録データにパスワードを紐づけた対応パスワードの設定テーブルの例を示す図である。

図１８に示す例では、対応パスワードの設定テーブルにおいて、１つの指紋登録データに複数のパスワード（ＩＥＦ）が紐づけられている。図１８に示す例によれば、指紋登録データを用いた生体認証が成功した場合、ＩＥＦ（０１）のパスワードとＩＥＦ（０３）のパスワードとが照合済（照合成功）の状態とされる。なお、図１８に示すような対応パスワードの設定テーブ

ルにおいて、指紋登録データに対して全てのパスワードを紐づけるようにすれば、当該指紋登録データを用いた生体認証が成功した場合に全てのパスワードの照合結果を照合済とするようにすることもできる。

[0071] すなわち、受信した照合コマンドのＰ１が「０１」で、かつ、Ｐ２が「ＦＥ」である場合（Ｓ１７、ＹＥＳ）、プロセッサ２１は、図１８に示すように、対応するパスワードが設定されている指紋登録データを用いた生体認証を生体照合部１２に実行させる（Ｓ６１、Ｓ６２）。

[0072] 例えば、プロセッサ２１は、データメモリ２４において対応パスワードを紐づけた状態で登録されている登録者の指紋データ（指紋登録データ）を生体照合部１２へ送信し、生体照合部１２に生体センサ３２による指紋データ（入力指紋データ）の入力および指紋登録データと入力指紋データとの照合とを指示する。生体照合部１２のＭＰＵ３１は、生体センサ３２により指紋データの入力し（Ｓ６１）、生体センサ３２で入力した指紋データ（入力指紋データ）と指紋登録データとを照合し（Ｓ６２）、その照合結果をプロセッサ２１へ供給する。

[0073] プロセッサ２１は、生体照合部１２からの照合結果に応じて生体認証が成功したか否かを判断する。また、プロセッサ２１は、ＬＥＤ１３を生体認証の結果に応じて点灯させる。例えば、プロセッサ２１は、生体照合部１２における生体情報の入力および生体照合を実行中には生体認証が実行中であることを示す点灯状態でＬＥＤ１３を点灯させる。さらに、プロセッサ２１は、生体認証が成功した場合には生体認証が成功したことを示す点灯状態でＬＥＤ１３を点灯させ、生体認証が失敗した場合には生体認証が失敗したことを示す点灯状態でＬＥＤ１３を点灯させる。

[0074] 生体照合部１２での生体照合による生体認証が失敗すると（Ｓ６３、ＮＯ）、プロセッサ２１は、生体認証の失敗（照合ＮＧ）を示すステータスワードを生成し、生成したステータスワードを照合コマンドの送信元である上位装置へ送信し（Ｓ６４）、次のコマンドの受信待ち状態となる。

[0075] 生体照合部１２での生体照合による生体認証が成功すると（Ｓ６３、ＹＥ

Ｓ）、プロセッサ２１は、当該生体認証に用いた指紋登録データに紐づけられているパスワード（ＩＥＦ）に対して照合結果が照合済（照合成功、ＯＫ）であることを示す情報（フラグ）を記憶する（Ｓ６５）。

[0076] 図１９は、図１８に示す指紋登録データに紐づけられたパスワードに対する照合結果を照合済（照合成功、ＯＫ）とした場合の照合状態テーブルの例を示す図である。

図１９に示す例では、ＩＥＦ（０１）とＩＥＦ（０３）とが照合状態が照合済となっており、それら以外のＩＥＦに対する照合状態が未照合となっている。図１８に示すテーブルを参照すれば、プロセッサ２１は、図１８に示す指紋登録データを用いた生体認証に成功した場合、当該指紋登録データに紐づけられているＩＥＦ（０１）とＩＥＦ（０３）との照合状態を照合済みにセットする。

[0077] すなわち、受信した照合コマンドの第２パラメータ（Ｐ２）が「ＦＥ」である場合、プロセッサ２１は、生体照合部１２による生体照合が成功すると、生体照合に用いた生体登録データに紐づけられているパスワードの照合結果を照合済（照合成功）にセットする。生体認証の成功に応じて指紋登録データに紐づくパスワードの照合結果を照合済とした後、プロセッサ２１は、当該照合コマンドの送信元である上位装置へ正常終了を示すステータスワードを送信し（Ｓ６６）、次のコマンドの受信待ち状態となる。

[0078] 以上の処理によれば、ＩＣカードは、生体照合を要求する照合コマンドに応じて生体認証を実行し、生体認証が成功した場合に当該生体認証に用いた生体登録情報（指紋登録データ）に紐づけられたパスワードの照合結果を照合済（照合成功）の状態とする。これにより、ＩＣカードは、生体照合の要求に応じた生体認証が成功すると、生体登録情報に紐づいたパスワードに対する照合結果を照合済（照合成功）とすることでき、生体登録情報に紐づけたパスワードの照合をセキュリティ性が高い生体認証に置き換えることができる。また、上述した処理例によれば、ＩＣカードは、生体認証だけでなく、パスワード照合も行えるようにすることで、生体認証機能に不具合が発生

した場合であっても、パスワードでの照合を行うことができる。

[0079] 次に、ＩＣカード１における生体認証が成功した場合に照合コマンドにおいて指定されたＩＥＦのパスワードの照合結果を照合済の状態にする処理について説明する。

図２０は、図２に示す処理において、ＩＣカード１における生体認証が成功した場合にコマンドで指定されたパスワードに対する照合結果を照合済にセットする処理例を示すフローチャートである。

上述したような図２に示す処理において、受信した照合コマンドのＰ１が「０１」で、かつ、Ｐ２が「ＦＦ」および「ＦＥ」以外の値である場合（Ｓ１９、ＮＯ）、プロセッサ２１は、受信した照合コマンドのＰ２で指定されるＩＥＦが存在するか否かを判断する（Ｓ７１）。Ｐ２で指定されるＩＥＦが存在しない場合（Ｓ７１、ＮＯ）、プロセッサ２１は、指定されたＩＥＦが存在しないことを示すステータスワードをコマンドの送信元である上位装置へ送信し（Ｓ７２）、次のコマンド待ち状態となる。

[0080] 生体認証を要求する照合コマンドのＰ２で指定されるＩＥＦが存在する場合（Ｓ７１、ＹＥＳ）、プロセッサ２１は、受信した照合コマンドで指定されるＩＥＦに対応して登録されている指紋登録データを用いた生体認証を実行する。

[0081] プロセッサ２１は、指定されたＩＥＦに対応する指紋登録データを生体照合部１２へ送信し、生体センサ３２による指紋データの入力および指紋登録データと入力指紋データとの照合とを生体照合部１２に指示する。生体照合部１２のＭＰＵ３１は、生体センサ３２により指紋データの入力し（Ｓ７３）、生体センサ３２で入力した指紋データ（入力指紋データ）とプロセッサ２１から指定される指紋登録データとを照合し（Ｓ７４）、その照合結果をプロセッサ２１へ供給する。

[0082] プロセッサ２１は、生体照合部１２からの照合結果に応じて生体認証が成功したか否かを判断する（Ｓ７５）。また、プロセッサ２１は、ＬＥＤ１３を生体認証の結果に応じて点灯させる。例えば、プロセッサ２１は、生体照

合部１２における生体情報の入力および生体照合を実行中には生体認証が実行中であることを示す点灯状態でＬＥＤ１３を点灯させる。さらに、プロセッサ２１は、生体認証が成功した場合には生体認証が成功したことを示す点灯状態でＬＥＤ１３を点灯させ、生体認証が失敗した場合には生体認証が失敗したことを示す点灯状態でＬＥＤ１３を点灯させる。

[0083] 指定されたＩＥＦに対応する指紋登録データを用いた生体認証が失敗すると（Ｓ７５、ＮＯ）、プロセッサ２１は、指定されたＩＥＦのパスワードに対する照合結果を示す情報を未照合の状態にリセットし（Ｓ７６）、生体認証の失敗（照合ＮＧ）を示すステータスワードを照合コマンドの送信元である上位装置へ送信し（Ｓ７７）、次のコマンドの受信待ち状態となる。

[0084] 例えば、図２１は、パスワードに対する照合結果を照合済（照合成功、ＯＫ）とした場合の照合状態テーブルの例を示す図である。

受信した照合コマンドのＰ２で指定されるＩＥＦがＩＥＦ（０１）である場合、プロセッサ２１は、ＩＥＦ（０１）に対応する指紋登録データを用いた生体認証が失敗すると、図２１に示す照合状態テーブルのように、ＩＥＦ（０１）の照合状態が未照合の状態にリセットする。

[0085] 指定されたＩＥＦに対応する指紋登録データを用いた生体認証が成功した場合（Ｓ７５、ＹＥＳ）、プロセッサ２１は、指定されたＩＥＦのパスワードに対する照合結果を照合済（照合成功、ＯＫ）であることを示す情報（フラグ）にセットする（Ｓ７８）。例えば、受信した照合コマンドのＰ２で指定されるＩＥＦがＩＥＦ（０２）である場合にＩＥＦ（０２）に対応する指紋登録データを用いた生体認証が成功すると、プロセッサ２１は、図２１に示す照合状態テーブルのように、ＩＥＦ（０２）の照合状態を照合済であることを示す値である「０１」にセットする。

[0086] 生体認証の成功に応じて指定されたＩＥＦのパスワードの照合結果を照合済とした後、プロセッサ２１は、当該照合コマンドの送信元である上位装置へ正常終了を示すステータスワードを送信し（Ｓ７９）、次のコマンドの受信待ち状態とする。

[0087] 次に、ＩＣカード１がパスワードを格納するＩＥＦごとに照合処理のリトライ回数に対する上限値を設定する場合について説明する。

図２３は、ＩＥＦごとに登録する生体登録データを管理するための管理テーブル（登録データの管理テーブル）の構成例を示す図である。

図２３に示す例において、登録データの管理テーブルでは、パスワードを格納するＩＥＦごとに、指紋登録データ、長さ、リトライカウンタ、および、リトライカウンタの初期値を記憶する。図２３に示すようなテーブルによって、指紋登録データとパスワードとがペアで登録される。これにより、ＩＣカード１は、コマンドで指定されたＩＥＦ（ＩＤ）のパスワードと対になる指紋登録データを用いて生成認証を実行し、その生体認証の成功に応じて対となるパスワードの照合結果を照合済みとすることができる。

[0088] また、図２３に示す管理テーブルでは、ＩＥＦに対応する指紋登録データごとにリトライカウンタを設定する。リトライカウンタは、対応する指紋登録データによる生体認証が実行可能な残りの照合回数を示す。リトライカウンタは、許容される照合回数（照合失敗の回数）の上限値が初期値として設定され、照合が失敗するごとにカウントダウンされるものとする。これにより、リトライカウンタは、指紋登録データによる生体認証が実行可能な残りの照合回数（リトライ数）を示す値が格納される。

[0089] また、リトライカウンタは、対となる生体登録データ（指紋登録データ）とパスワードとで共通の値としても良い。対となる生体登録データとパスワードとで共通のリトライカウンタとする場合、図２３に示す登録データの管理テーブルに記憶される生体登録データを用いた生体照合の残り回数を示すリトライカウンタは、対となるパスワードに対するパスワード照合の残り回数（対となるパスワードに対するリトライカウンタ）と共通化される。

[0090] 例えば、対となる生体登録データとパスワードとでリトライカウンタを共通化する場合、パスワード照合が失敗すると、当該パスワードと対となる生体登録データに対応するリトライカウンタもカウントダウンされる。また、生体登録データを用いた生体認証が失敗すると、当該生体登録データと対と

なるパスワードに対応するリトライカウンタもカウントダウンされる。

[0091] また、リトライカウンタは、対となる生体登録データとパスワードとでそれぞれ別の値としても良い。この場合、登録データの管理テーブルにおける生体登録データを用いた生体照合の残り回数は、対となるパスワードに対するパスワード照合の残り回数とは別々にカウントされる値となる。

[0092] 例えば、対となる生体登録データとパスワードとでリトライカウンタを別々の値で管理する場合、パスワード照合が失敗すると、当該パスワードに対応するリトライカウンタはカウントダウンされるが、当該パスワードと対となる生体登録データに対応するリトライカウンタは更新されない。また、生体登録データを用いた生体認証が失敗すると、当該生体登録データに対するリトライカウンタはカウントダウンされるが、当該生体登録データと対となるパスワードに対応するリトライカウンタは更新（カウントダウン）されない。

[0093] また、対となる生体登録データとパスワードとでリトライカウンタを別々の値で管理する場合、プロセッサ２１は、対となる生体登録データ又はパスワードの何れか一方のリトライカウンタが０になる（リトライ数が上限値を超える）と、対となる生体登録データおよびパスワードの両方をロック状態するようにしても良い。これにより、ＩＣカードは、パスワード照合のリトライ回数が上限値を超えると、当該パスワードと対となる生体登録データによる生体認証もロック状態とすることができ、生体登録データによる生体認証のリトライ数が上限値を超えると、当該生体登録データと対となるパスワードによるパスワード照合もロック状態とすることができる。

[0094] なお、ＩＣカード１の運用によっては、対となる生体登録データとパスワードとでリトライカウンタを別々の値で管理する場合であっても、プロセッサ２１は、対となる生体登録データおよびパスワードについて、それぞれ別々にロック状態を制御するようにしても良い。すなわち、ＩＣカードは、パスワード照合のリトライ回数が上限値を超えた場合であっても、当該パスワードと対となる生体登録データのリトライカウンタが上限値を超えていなけ

れば生体登録データによる生体認証はロック状態としないようにしても良い。この場合、ＩＣカード１は、生体登録データによる生体認証が成功すると、対となるパスワードに対応するリトライカウンタもリセットするようにしても良い。

[0095] また、ＩＣカードは、生体登録データによる生体認証のリトライ数が上限値を超えた場合であっても、当該生体登録データと対となるパスワードのリトライカウンタが上限値を超えていなければ当該パスワードによるパスワード照合もロック状態としないようにしても良い。この場合も、ＩＣカード１は、パスワード照合が成功すると、対となる生体登録データに対応するリトライカウンタもリセットするようにしても良い。

[0096] 図２２に示す処理例において、コマンドで指定されたＩＥＦが存在する場合（Ｓ８１、ＹＥＳ）、プロセッサ２１は、指定されるＩＥＦに対応する指紋登録データがロック状態でるか否かを判定する（Ｓ８３）。例えば、プロセッサ２１は、図２３に示すような登録データの管理テーブルにおいて、指定されたＩＥＦに対応する指紋登録データに対するリトライカウンタが０であるか否かによりロック状態であるか否かを判定する。

[0097] 指定されたＩＥＦに対応する生体認証のリトライカウンタが０である場合、つまり、ロック状態である場合（Ｓ８３、ＹＥＳ）、プロセッサ２１は、ロック状態であることを示すステータスワードをコマンドの送信元である上位装置へ送信し（Ｓ８４）、次のコマンドの受信待ち状態となる。

[0098] 指定されたＩＥＦに対応する生体認証のリトライカウンタが０でない場合、つまり、ロック状態でない場合（Ｓ８３、ＮＯ）、プロセッサ２１は、当該ＩＥＦに対応する指紋登録データを用いた生体認証を実行する。プロセッサ２１は、指定されたＩＥＦに対応する指紋登録データを生体照合部１２へ送信し、生体センサ３２による指紋データの入力および指紋登録データと入力指紋データとの照合とを生体照合部１２に指示する。生体照合部１２のＭＰＵ３１は、生体センサ３２により指紋データの入力し（Ｓ８５）、生体センサ３２で入力した指紋データ（入力指紋データ）とプロセッサ２１から指

定される指紋登録データとを照合し（Ｓ８６）、その照合結果をプロセッサ２１へ供給する。

[0099] プロセッサ２１は、生体照合部１２からの照合結果に応じて生体認証が成功したか否かを判断する。また、プロセッサ２１は、ＬＥＤ１３を生体認証の結果に応じて点灯させる。例えば、プロセッサ２１は、生体照合部１２における生体情報の入力および生体照合を実行中には生体認証が実行中であることを示す点灯状態でＬＥＤ１３を点灯させる。さらに、プロセッサ２１は、生体認証が成功した場合には生体認証が成功したことを示す点灯状態でＬＥＤ１３を点灯させ、生体認証が失敗した場合には生体認証が失敗したことを示す点灯状態でＬＥＤ１３を点灯させる。

[0100] 指定されたＩＥＦに対応する指紋登録データを用いた生体認証が失敗すると（Ｓ８７、ＮＯ）、プロセッサ２１は、指定されたＩＥＦに対応する指紋登録データを用いた生体認証のリトライカウンタをカウントダウンする（Ｓ８８）。また、プロセッサ２１は、当該ＩＥＦのパスワードに対する照合結果を示す情報を未照合の状態にリセットし（Ｓ８９）、生体認証の失敗（照合ＮＧ）を示すステータスワードを照合コマンドの送信元である上位装置へ送信し（Ｓ９０）、次のコマンドの受信待ち状態となる。

[0101] 指定されたＩＥＦに対応する指紋登録データを用いた生体認証が成功した場合（Ｓ８７、ＹＥＳ）、プロセッサ２１は、当該コマンドで指定されたＩＥＦに対応する指紋登録データを用いた生体認証のリトライカウンタをリセットすることによりリトライカウンタの値を初期値にする（Ｓ９１）。また、プロセッサ２１は、生体認証の成功に応じて当該コマンドで指定されたＩＥＦのパスワードに対する照合結果を照合済（照合成功、ＯＫ）であることを示す情報（フラグ）にセットする（Ｓ９２）。生体認証の成功に応じて指定されたＩＥＦのパスワードの照合結果を照合済とした後、プロセッサ２１は、当該照合コマンドの送信元である上位装置へ正常終了を示すステータスワードを送信し（Ｓ９３）、次のコマンドの受信待ち状態とする。

[0102] 以上の処理によれば、ＩＣカードは、生体照合を要求する照合コマンドに

応じて指定されたＩＥＦに対応する生体（指紋）登録データを用いて生体認証を実行し、生体認証が成功した場合に当該ＩＥＦのパスワードの照合結果を照合済（照合成功）とする。これにより、ＩＣカードは、指定したＩＥＦのパスワード照合をセキュリティ性が高い生体認証に置き換えることができる。この結果、生体認証に用いる指紋登録データとパスワードとを対で管理でき、指定するパスワードの照合を予めペアに設定した生体情報による生体認証に置き換えることができる。

[0103] また、上述の処理例によれば、生体登録データごとに生体認証のリトライカウンタを設定でき、生体登録データごとに生体認証を制限できる。生体登録データごとに設ける生体認証のリトライカウンタは、対となるパスワードによるパスワード照合に対するリトライカウンタと共通化することで、対となるパスワードと生体登録データとを１組の認証データとして認証回数を制限することができる。

[0104] また、生体登録データごとに設ける生体認証のリトライカウンタは、対応するパスワードによるパスワード照合に対するリトライカウンタと別々に設けることもできる。この場合、ＩＣカードは、対となるパスワードと生体登録データとの何れか一方のリトライカウンタが認証回数の上限を超えた場合、対となるパスワードと生体登録データとの両方をロック状態する制御が可能である。

[0105] 次に、照合コマンド以外の特定コマンドを受信した場合に生体認証を実行する処理例について説明する。

上述した処理例では、生体認証を要求する照合コマンドを受信した場合に生体認証の成功をパスワードの照合結果に反映させる処理について説明した。ただし、ＩＣカード１は、照合コマンド以外の特定コマンドを受信した場合に生体認証を実行するようにしても良い。ここで、実施形態に係る携帯可能電子装置としてのＩＣカード１が生体認証を実行する特定コマンドとして初期応答後の最初に受信したコマンド（第１コマンド）およびセレクトコマンドを受信した場合に、コマンドの処理に先立って生体認証を行う場合につ

いて説明する。

[0106] 図２４は、ＩＣカード１がセレクトコマンドを受信した場合に生体認証を実行する処理例を説明するためのフローチャートである。

まず、ＩＣカード１は、上位装置との通信を開始する場合、上位装置からの電源電力の供給を受けて起動する。ＩＣカード１のプロセッサ２１は、上位装置から供給される電力によって起動した後、上位装置に対して初期応答を通信インターフェース２５を介して送信する（Ｓ１０１）。

[0107] プロセッサ２１は、初期応答を送信した直後に自己診断処理として生体（指紋）センサ３２が正常に動作するかをチェックする（Ｓ１０２）。自己診断処理により指紋センサ３２が正常に動作しないことを確認した場合、プロセッサ２１は、指紋センサ３２の自己診断結果として指紋センサが異常であることを記憶する（Ｓ１０４）。また、自己診断処理により指紋センサ３２が正常に動作すること確認した場合、プロセッサ２１は、指紋センサ３２の自己診断結果として指紋センサが正常であることを記憶する（Ｓ１０５）。例えば、プロセッサ２１は、ＲＡＭ２３又はデータメモリ２４に指紋センサ３２の自己診断結果を記憶する。

[0108] ＩＣカード１のプロセッサ２１は、初期応答後（自己診断後）、コマンドの受信待ち状態となる（Ｓ１０６）。この状態において上位装置からコマンドを受信した場合（Ｓ１０６、ＹＥＳ）、プロセッサ２１は、受信したコマンドがセレクトコマンドであるか否かを判定する（Ｓ１０７）。受信したコマンドがセレクトコマンドでない場合（Ｓ１０７、ＮＯ）、プロセッサ２１は、Ｓ１１４へ進み、受信したコマンドに応じたコマンド処理を実行する。

[0109] 受信したコマンドがセレクトコマンドである場合（Ｓ１０７、ＹＥＳ）、プロセッサ２１は、自己診断処理で指紋センサ３２が正常であったか否かを判定する（Ｓ１０９）。自己診断処理で指紋センサ３２が異常であった場合（Ｓ１０９、ＮＯ）、プロセッサ２１は、Ｓ１１４へ進み、受信したコマンド（セレクトコマンド）に応じた処理を実行する。

[0110] 自己診断処理で指紋センサ３２が正常であった場合（Ｓ１０９、ＹＥＳ）

、プロセッサ２１は、Ｓ１１４へ進み、データメモリ２４に登録されている指紋登録データを用いた生体認証を実行する。プロセッサ２１は、指紋登録データを生体照合部１２へ送信し、生体センサ３２による指紋データの入力および指紋登録データと入力指紋データとの照合とを生体照合部１２に指示する。この場合、プロセッサ２１は、ＬＥＤ１３を生体（指紋）照合中であることを示す点灯状態で点灯させる。

[0111] 生体照合部１２のＭＰＵ３１は、生体センサ３２により指紋データの入力し（Ｓ１１０）、生体センサ３２で入力した指紋データ（入力指紋データ）とプロセッサ２１から指定される指紋登録データとを照合し（Ｓ１１１）、その照合結果をプロセッサ２１へ供給する。

[0112] プロセッサ２１は、生体照合部１２の照合結果に基づいて生体認証の成否を判定する。プロセッサ２１は、ＬＥＤ１３を生体認証の結果に応じて点灯させる。例えば、プロセッサ２１は、生体認証が成功した場合には生体認証が成功したことを示す点灯状態でＬＥＤ１３を点灯させ、生体認証が失敗した場合には生体認証が失敗したことを示す点灯状態でＬＥＤ１３を点灯させる。

[0113] 生体認証（照合）が成功した場合（Ｓ１１２、ＹＥＳ）、プロセッサ２１は、生体認証の認証結果を反映させるパスワードの照合結果を照合済にセットする（Ｓ１１３）。例えば、プロセッサ２１は、生体認証の成功に応じて全てのパスワードの照合結果を照合済にセットする。また、プロセッサ２１は、セレクトコマンドが選択されるＤＦの配下にあるＩＥＦのパスワードの照合結果を照合済にセットするようにしても良い。プロセッサ２１は、生体認証（照合）の成功に応じてパスワードの照合結果を照合済にセットした後、当該コマンドで要求されるコマンド処理を実行する（Ｓ１１４）。

[0114] また、生体認証（照合）が失敗した場合（Ｓ１１２、ＮＯ）、プロセッサ２１は、パスワードの照合結果を変更することなく、受信したコマンドに応じたコマンド処理を実行する（Ｓ１１４）。

コマンド処理が終了すると、プロセッサ２１は、コマンド処理の実行結果

を示すステータスワードを上位装置へ送信し（Ｓ１１５）、次のコマンド待ち状態となる。

[0115] 以上の処理によれば、ＩＣカードは、セレクトコマンドを受信した場合に生体認証を実行し、生体認証が成功すればパスワードの照合結果を照合済とする処理を実行する。これにより、ＩＣカードは、上位装置から生体認証を要求する照合コマンドを受信しなくてもセレクトコマンドを受信した場合に生体認証を実行することができる。これにより、生体認証あるいはパスワード照合を上位装置からＩＣカードへ供給する処理を省略でき、さらに生体認証によるセキュリティの向上を望める。

[0116] 次に、照合コマンド以外の特定コマンドを受信した場合に生体認証を実行し、生体認証が成功しなければコマンド処理を実行しないようにする処理例について説明する。

図２５乃至３２は、ＩＣカード１が特定コマンドを受信した場合に実行する生体認証が成功しなければコマンド処理を実行しない処理例を説明するためのフローチャートである。

図２５は、照合コマンド以外の特定のコマンドとして、初期応答後の最初のコマンド（第１コマンド）を受信した場合に生体認証を実行するものする。

[0117] まず、ＩＣカード１は、上位装置からの電源電力の供給を受けて起動する。ＩＣカード１のプロセッサ２１は、上位装置から供給される電力によって起動した後、上位装置に対して初期応答を通信インターフェース２５を介して送信する（Ｓ１２１）。

[0118] 初期応答後、ＩＣカード１のプロセッサ２１は、初期応答後（自己診断後）、コマンドの受信待ち状態となる。ただし、プロセッサ２１は、初期応答後に図２４のＳ１０２－Ｓ１０５で説明したような生体（指紋）センサ３２の自己診断処理を実行しても良い。

[0119] コマンドの受信待ち状態において上位装置からのコマンドを受信した場合（Ｓ１２２、ＹＥＳ）、プロセッサ２１は、受信したコマンドが初期応答後

の最初のコマンドであるか否かを判定する（Ｓ１２３）。ここで、初期応答後の最初のコマンド（第１コマンド）は、生体認証を行う特定コマンドとする。受信したコマンドが第１コマンドでない場合（Ｓ１２３、ＮＯ）、プロセッサ２１は、Ｓ１２９へ進み、受信したコマンドに応じたコマンド処理を実行する。

[0120] 受信したコマンドが第１コマンドである場合（Ｓ１２３、ＹＥＳ）、プロセッサ２１は、データメモリ２４に登録されている指紋登録データを用いた生体認証を実行する。プロセッサ２１は、指紋登録データを生体照合部１２へ送信し、生体センサ３２による指紋データの入力および指紋登録データと入力指紋データとの照合とを生体照合部１２に指示する。このような生体認証を実行中において、プロセッサ２１は、ＬＥＤ１３を生体（指紋）照合中であることを示す点灯状態で点灯させる。

[0121] 生体照合部１２のＭＰＵ３１は、生体センサ３２により指紋データの入力し（Ｓ１２５）、生体センサ３２で入力した指紋データ（入力指紋データ）とプロセッサ２１から指定される指紋登録データとを照合し（Ｓ１２６）、その照合結果をプロセッサ２１へ供給する。プロセッサ２１は、生体照合部１２の照合結果に基づいて生体認証の成否を判定する。また、プロセッサ２１は、ＬＥＤ１３を生体認証の結果に応じて点灯させる。例えば、プロセッサ２１は、生体認証が成功した場合には生体認証が成功したことを示す点灯状態でＬＥＤ１３を点灯させ、生体認証が失敗した場合には生体認証が失敗したことを示す点灯状態でＬＥＤ１３を点灯させる。

[0122] 生体認証（照合）が成功した場合（Ｓ１２７、ＹＥＳ）、プロセッサ２１は、生体認証の成功に応じてパスワードの照合結果を照合済にセットする処理を行う（Ｓ１２８）。生体認証の成功に応じてパスワードの照合結果を照合済にセットした後、プロセッサ２１は、当該コマンドで要求されるコマンド処理を実行する（Ｓ１２９）。コマンド処理が終了すると、プロセッサ２１は、コマンド処理の実行結果を示すステータスワードを上位装置へ送信し（Ｓ１３０）、次のコマンド待ち状態となる。

[0123] 生体認証（照合）が失敗した場合（Ｓ１２７、ＮＯ）、プロセッサ２１は、当該コマンド処理を実行せずに、次のコマンド待ち状態となる。この場合、プロセッサ２１は、受信したコマンドに対する応答として生体認証が成功しなかったためにコマンドが実行できなかったことを示すステータスワードを上位装置へ送信するようにしても良い。

なお、初期応答後の最初のコマンドによって実行した生体認証が成功しなかった場合、プロセッサ２１は、次に受信するコマンドも特定コマンドとしてＳ１２５の処理へ進み、生成認証を実行するようにしても良い。

[0124] 図２６は、図２５に示す処理の第１の変形例としての処理の流れを示すフローチャートである。

図２６に示す処理は、図２５の処理例と同様に、照合コマンド以外の特定のコマンドとして、初期応答後の最初のコマンド（第１コマンド）を受信した場合に生体認証を実行する処理である。ただし、図２６に示す処理は、生体認証が失敗した場合に再度生体認証を実行する点が図２５に示す処理例と異なる。

[0125] すなわち、図２６に示す処理例において、ＩＣカード１のプロセッサ２１は、生体認証（照合）が失敗した場合、Ｓ１２５へ戻り、生体センサ３２による指紋データの入力を改めて実行し（Ｓ１２５）、生体センサ３２が改めて入力した指紋データ（入力指紋データ）とプロセッサ２１から指定される指紋登録データとの生体照合を再度実行する（Ｓ１２６）。

[0126] なお、図２６に示す処理例において、プロセッサ２１は、指紋データの入力および照合を連続して実行する回数が所定上限回数を超える場合に、Ｓ１３０へ進み、受信したコマンドに対する応答として生体認証が成功しなかったためにコマンドが実行できなかったことを示すステータスワードを上位装置へ送信するようにしても良い。

以上のような第１の変形例によれば、ＩＣカード１は、生体センサ３２による指紋データの入力に不具合があった場合に、再度の指紋データの入力および照合を行えるようになる。

[0127] 図２７は、図２５に示す処理の第２の変形例としての処理の流れを示すフローチャートである。

図２７は、照合コマンド以外の特定のコマンドとしてセレクトコマンドを受信した場合に生体認証を実行する処理例を示す。ただし、図２７に示す処理は、照合コマンド以外の特定のコマンドをセレクトコマンドする点以外は図２５に示す処理例と同様である。

[0128] すなわち、図２７に示す処理例において、ＩＣカード１のプロセッサ２１は、受信したコマンドがセレクトコマンドである場合（Ｓ１２４、ＹＥＳ）、Ｓ１２５へ進み、データメモリ２４に登録されている指紋登録データを用いた生体認証を実行する。また、受信したコマンドがセレクトコマンド以外のコマンドである場合（Ｓ１２４、ＮＯ）、プロセッサ２１は、Ｓ１２９へ進み、受信したコマンドに応じた処理を実行する。

以上のような第２の変更例によれば、ＩＣカード１は、セレクトコマンドを受信した場合に生体認証を実行するようにすることができる。

[0129] 図２８は、図２５に示す処理の第３の変形例としての処理の流れを示すフローチャートである。

図２８は、図２７の処理例と同様に、照合コマンド以外の特定のコマンドとしてセレクトコマンドを受信した場合に生体認証を実行する処理例を示す。ただし、図２８に示す処理は、生体認証が失敗した場合に再度生体認証を実行する点が図２７に示す処理例と異なる。

[0130] すなわち、図２８に示す処理例において、ＩＣカード１のプロセッサ２１は、セレクトコマンドを受信した後に実行する生体認証（照合）が失敗した場合（Ｓ１２７、ＮＯ）、Ｓ１２５へ戻り、生体センサ３２による指紋データの入力を改めて実行し（Ｓ１２５）、生体センサ３２が改めて入力した指紋データ（入力指紋データ）とプロセッサ２１から指定される指紋登録データとの生体照合を再度実行する（Ｓ１２６）。

[0131] なお、図２８に示す処理例において、プロセッサ２１は、指紋データの入力および照合を連続して実行する回数が所定上限回数を超える場合に、Ｓ１

３０へ進み、生体認証が成功しなかったためにセレクトコマンドが実行できなかったことを示すステータスワードを生体認証の失敗を示すステータスワードを上位装置へ送信するようにしても良い。

以上のような第３の変形例によれば、ＩＣカード１は、セレクトコマンドを受信した場合に生体認証を実行するようにすることができ、さらに、生体センサ３２による指紋データの入力に不具合があった場合には再度の指紋データの入力および照合を行えるようになる。

[0132] また、図２９乃至３２は、図２５乃至２８に示す処理のさらなる変形例としての第４乃至７の変形例を示すフローチャートである。例えば、図２９は、図２５に示す処理の第４の変形例であり、図２５に示す処理におけるＳ１２８の処理を省略した場合の処理例を示す。図３０は、図２５に示す処理の第５の変形例であり、図２６に示す処理におけるＳ１２８の処理を省略した場合の処理例を示す。図３１は、図２５に示す処理の第６の変形例であり、図２７に示す処理におけるＳ１２８の処理を省略した場合の処理例を示す。図３２は、図２５に示す処理の第７の変形例であり、図２８に示す処理におけるＳ１２８の処理を省略した場合の処理例を示す。

[0133] すなわち、ＩＣカード１は、図２６乃至３２に示すように、生体認証（照合）が成功した場合にパスワードの照合結果を照合済にセットする処理を省略するようにしても良い。この場合、ＩＣカードは、第１コマンドあるいはセレクトコマンドなどの特定コマンドを受信した場合、生体認証（照合）が成功した場合にコマンド処理を実行でき、生体認証（照合）が失敗した場合にはコマンド処理を実行しないようにすることができる。

[0134] 以上の処理によれば、ＩＣカードは、初期応答後の最初のコマンド又はセレクトコマンドなどの特定コマンドを受信した場合に生体認証を実行し、生体認証が成功すればコマンド処理を実行し、生体認証が失敗すれば当該コマンドに対するコマンド処理を実行しないようにする。これにより、ＩＣカードは、第１コマンドやセレクトコマンドなどの特定コマンドを受信した場合に実行する生体認証が成功しなければ、コマンド処理を実行しないようにす

ることができる。

[0135] また、ＩＣカードは、初期応答後の最初のコマンド又はセレクトコマンドなどの特定コマンドを受信した場合に実行する生体認証が成功すればパスワードの照合結果を照合済にセットしてコマンド処理を実行するようにできる。これにより、ＩＣカードは、特定コマンドに応じて実行する生体認証が成功すればパスワードの照合結果を照合済にセットすることでき、コマンド処理の高速化を図ることができる。

[0136] 上述の各実施形態で説明した機能は、ハードウエアを用いて構成するに留まらず、ソフトウエアを用いて各機能を記載したプログラムをコンピュータに読み込ませて実現することもできる。また、各機能は、適宜ソフトウエア、ハードウエアのいずれかを選択して構成するものであっても良い。

[0137] 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。

請求の範囲

[請求項1] 人物の生体情報を取得する生体センサと、

上位装置と通信する通信インターフェースと、

登録者の生体情報を記憶する第１メモリと、

パスワードを記憶する第２メモリと、

前記通信インターフェースにより上位装置から受信する生体認証を要求するコマンドに応じて前記生体センサが取得する生体情報と前記第１メモリが記憶する生体情報とによる生体認証を実行し、前記生体認証が成功した場合に前記第２メモリが記憶するパスワードの照合状態を照合済とするプロセッサと、

を有する携帯可能電子装置。

[請求項2] 前記プロセッサは、前記生体認証が成功した場合に前記第２メモリに記憶した全てのパスワードの照合状態を照合済とする、

請求項１に記載の携帯可能電子装置。

[請求項3] 前記プロセッサは、前記生体認証が成功した場合に前記第２メモリに記憶したパスワードのうち前記生体認証に用いた前記第１メモリが記憶する生体情報に紐づけられているパスワードに対する照合状態を照合済の状態とする、

請求項１に記載の携帯可能電子装置。

[請求項4] 前記プロセッサは、前記生体認証が成功した場合に前記第２メモリに記憶したパスワードのうち前記コマンドで指定されたパスワードの照合状態を照合済とする、

請求項１に記載の携帯可能電子装置。

[請求項5] 前記第１メモリは、前記第２メモリが記憶するパスワードに対応づけた生体情報を記憶し、

前記プロセッサは、前記第１メモリが記憶する生体情報のうち前記コマンドで指定されたパスワードに対応する生体情報を用いて生体照合を実行させる、

請求項１に記載の携帯可能電子装置。

[請求項6] 前記プロセッサは、前記第２メモリが記憶するパスワードに対するリトライ数と前記第２メモリが記憶するパスワードに対応する前記第１メモリが記憶する生体情報に対するリトライ数とを共通のリトライ数として管理する、

請求項５に記載の携帯可能電子装置。

[請求項7] 前記プロセッサは、前記第２メモリが記憶するパスワードに対応するリトライ数と前記第２メモリが記憶するパスワードに対応する前記第１メモリが記憶する生体情報に対するリトライ数とをそれぞれ別々に管理する、

請求項５に記載の携帯可能電子装置。

[請求項8] 前記プロセッサは、前記第１メモリが記憶する生体情報に対するリトライ数と前記第２メモリが記憶するパスワードに対応するリトライ数との何れか一方がリトライ上限数を超えた場合に生体情報による生体認証およびパスワードの照合を両方をロックする、

請求項７に記載の携帯可能電子装置。

[請求項9] 前記プロセッサは、前記通信インターフェースにより上位装置から生体認証を要求する照合コマンドを受信した場合に生体認証を実行する、

請求項１乃至８の何れか１項に記載の携帯可能電子装置。

[請求項10] 前記プロセッサは、前記通信インターフェースにより上位装置から特定コマンドを受信した場合に生体認証を実行する、

請求項１乃至８の何れか１項に記載の携帯可能電子装置。

[請求項11] 前記特定コマンドは、前記通信インターフェースにより初期応答を出力した後に最初に受信するコマンドである、

請求項１０に記載の携帯可能電子装置。

[請求項12] 前記特定コマンドは、アプリケーション選択コマンドである、

請求項１０に記載の携帯可能電子装置。

[請求項13] 前記プロセッサは、前記通信インターフェースにより初期応答を出力した後に前記生体センサの自己診断を実行し、前記生体センサの自己診断結果が正常の場合に生体認証を実施する、

請求項１０に記載の携帯可能電子装置。

[請求項14] 前記プロセッサは、前記特定コマンドを受信した場合に実行する生体認証が成功しなければ前記特定コマンドが要求する処理を実行しない、

請求項１０に記載の携帯可能電子装置。

[請求項15] 前記プロセッサは、前記特定コマンドを受信した場合に実行する生体認証が成功しない場合、前記生体センサにより改めて生体情報を取得し、前記生体センサが改めて取得した生体情報と前記第１メモリが記憶する生体情報とによる生体認証を再度実行する、

請求項１０に記載の携帯可能電子装置。

[請求項16] 点灯状態が制御されるＬＥＤを有し、

前記プロセッサは、前記生体認証の結果に応じてＬＥＤの表示状態を制御する、

請求項１乃至１５の何れか１項に記載の携帯可能電子装置。

[請求項17] 前記生体センサは、指紋情報を取得する指紋センサである、

請求項１乃至１６の何れか１項に記載の携帯可能電子装置。

[請求項18] 人物の生体情報を取得する生体センサと、

上位装置と通信する通信インターフェースと、登録者の生体情報を記憶する第１メモリと、パスワードを記憶する第２メモリと、前記通信インターフェースにより上位装置から受信する生体認証を要求するコマンドに応じて前記生体センサが取得する生体情報と前記第１メモリが記憶する生体情報とによる生体認証を実行し、前記生体認証が成功した場合に前記第２メモリが記憶するパスワードの照合状態を照合済とするプロセッサと、を有するモジュールと、

前記生体センサと前記モジュールとを接続した状態を保持する本体

と、

を有するＩＣカード。