(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-155587
(P2006-155587A)
(43)公開日　平成18年6月15日(2006.6.15)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330F	4C038
G06T 1/00	(2006.01)	G06T	1/00	400H	5B035
G06T 7/00	(2006.01)	G06T	7/00	510B	5B043
A61B 5/117	(2006.01)	A61B	5/10	320C	5B047
G06K 19/07	(2006.01)	A61B	5/10	320Z	5B058

審査請求 未請求　請求項の数 12　ＯＬ　（全 33 頁）　最終頁に続く

(21)出願番号　特願2005-298110 (P2005-298110)
(22)出願日　平成17年10月12日 (2005.10.12)
(31)優先権主張番号　特願2004-323807 (P2004-323807)
(32)優先日　平成16年11月8日 (2004.11.8)
(33)優先権主張国　日本国(JP)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100082740
弁理士　田辺　恵基
(72)発明者　佐藤　英雄
東京都品川区北品川６丁目７番３５号ソニー株式会社内

Ｆターム(参考)　4C038 VA04 VA07 VB12 VB13 VC01 VC05
5B035 BA01 BB09 BC01 CA23
5B043 AA09 BA03 CA10 DA05 FA04 GA17

最終頁に続く

(54)【発明の名称】情報処理システム及び情報処理装置

(57)【要約】
【課題】本発明は、使い勝手を格段的に向上させ得る情報処理システムを提案するものである。
【解決手段】第１の情報処理装置と、第２の情報処理装置とによって構成される情報処理システムにおいて、第１の情報処理装置は、生体の所定部位に装着する装着手段と、所定部位における識別対象を生体識別データとして記憶する記憶手段と、装着手段に保持され、近接する通信対象に記憶手段に記憶される生体識別データを送信する通信手段とを設け、第２の情報処理装置は、生体の所定部位を近接させる近接面に近接させられた生体を撮像する撮像手段と、近接面に近接させられた生体に保持される通信対象と通信する通信手段と、撮像手段により撮像された生体画像から生体の識別対象を抽出し、当該抽出した識別対象と、通信対象から通信手段を介して得られる生体識別データに基づく識別対象とに基づいて生体認証する認証手段とを設けるようにした。
【選択図】図３

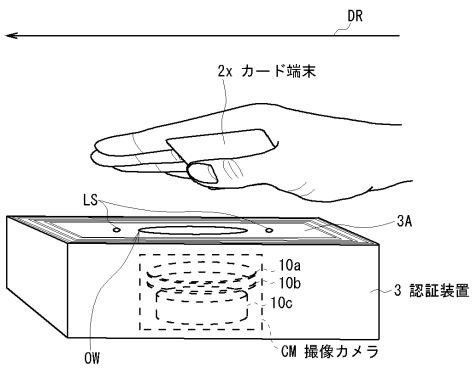

図３　カード端末と認証装置との構成（２）

【特許請求の範囲】
【請求項１】
第１の情報処理装置と、第２の情報処理装置とによって構成される情報処理システムにおいて、
上記第１の情報処理装置は、
生体の所定部位における識別対象を生体識別データとして記憶する記憶手段と、
上記生体に保持されて所定の位置にまで近接され、当該位置に近接された状態で通信する第１の通信手段と
を具え、
上記第２の情報処理装置は、
上記位置に近接された上記生体を生体データとして検出する生体センサと、
上記位置に近接された上記生体に保持される上記第１の通信手段と通信する第２の通信手段と、
上記生体センサで検出された上記生体データから上記所定部位に対応する生体データを抽出する抽出手段と、
上記抽出手段で抽出された上記所定部位に対応する生体データと、上記第１及び第２の通信手段を介して上記第１の情報処理装置から取得した上記生体識別データとに基づいて生体認証する生体認証手段と
を具えることを特徴とする情報処理システム。
【請求項２】
所定の位置に近接された生体を生体データとして検出する生体センサと、
上記位置に近接された上記生体に保持される通信対象と通信する近距離通信手段と、
上記生体センサで検出された上記生体データから上記所定部位における生体データを抽出する抽出手段と、
上記抽出手段で抽出された上記所定部位における生体データと、上記通信対象に登録され、当該通信対象から上記近距離通信手段を介して取得した上記生体識別データとに基づいて照合する生体認証手段と
を具えることを特徴とする情報処理装置。
【請求項３】
上記通信対象を管理する管理サーバに対して所定のネットワークを介して通信するネットワーク通信手段と、
上記ネットワーク通信手段及び上記近距離通信手段を介して上記通信対象と、上記管理サーバとの相互認証を中継する中継手段とをさらに具え、
上記相互認証の結果に応じて上記生体認証手段による照合が行われ、又は上記生体認証手段による照合結果に応じて上記中継手段による上記相互認証の中継が行われる
ことを特徴とする請求項２に記載の情報処理装置。
【請求項４】
上記通信対象に登録された上記生体識別データを対応付けて管理する管理サーバに対して所定のネットワークを介して通信するネットワーク通信手段をさらに具え、
上記生体認証手段は、
上記抽出手段で抽出された上記所定部位における生体データと、上記ネットワーク通信手段を介して上記管理サーバから取得した上記生体識別データと、上記近距離通信手段を介して上記通信対象から取得した上記生体識別データとを相互に照合する
ことを特徴とする請求項２に記載の情報処理装置。
【請求項５】
上記通信対象に登録された上記生体識別データと、当該生体識別データを生成するまでの過程で得られるデータを用いて圧縮データとを対応付けて管理する管理サーバに対して所定のネットワークを介して通信するネットワーク通信手段とをさらに具え、
上記抽出手段は、
上記生体センサで検出された上記生体データから上記所定部位における生体データを抽

出するまでの過程で得られるデータを用いて圧縮データを生成し、
上記生体認証手段は、
上記抽出手段で生成された上記圧縮データと、上記ネットワーク通信手段を介して上記管理サーバから取得した上記圧縮データとを照合する
ことを特徴とする請求項２に記載の情報処理装置。
【請求項６】
上記生体認証手段は、
上記抽出手段で生成された上記圧縮データと、上記ネットワーク通信手段を介して上記管理サーバから取得した上記圧縮データとを照合すると共に、上記抽出手段で抽出された抽出された上記所定部位における生体データと、上記近距離通信手段を介して上記通信対象から取得した上記生体識別データとを照合する
ことを特徴とする請求項５に記載の情報処理装置。
【請求項７】
上記生体に保持される上記通信対象には、光源が設けられ、
上記光源に対する点滅状態を制御する点滅パターンを生成する生成手段と、
上記生成手段において生成された上記点滅パターンを暗号化する暗号化手段と
をさらに具え、
上記生体認証手段は、
上記点滅パターンと、上記位置に近接された上記通信対象における上記光源から上記点滅パターンに従って点滅照射され、当該位置に近接された上記生体を介して上記生体センサで検出された上記生体データの輝度パターンとを照合する
ことを特徴とする請求項２に記載の情報処理装置。
【請求項８】
上記生体識別データは、所定の分割単位のデータとしてそれぞれ分割され、
上記生体認証手段は、
上記分割単位のデータを取得するごとに、上記所定部位における生体データの対応するデータ部分と生体認証し、当該分割単位のデータを取得できなかった場合には、その取得できなかった分割単位のデータから再取得を開始する
ことを特徴とする請求項２に記載の情報処理装置。
【請求項９】
生体の所定部位に装着する装着手段と、
上記所定部位における識別対象を生体識別データとして記憶する記憶手段と、
上記装着手段に保持され、当該装着手段を装着した上記所定部位を近接させた通信対象に対して上記生体識別データを送信する通信手段と
を具え、
上記通信対象では、上記装着手段を装着した状態で近接された上記生体が生体データとして検出される
ことを特徴とする情報処理装置。
【請求項１０】
上記通信対象から供給される信号の受信に応じて誘起する電圧を蓄積する電圧蓄積手段を具え、
上記通信手段は、
上記電圧蓄積手段により蓄積された電圧を起電力として、上記通信対象に対して上記生体識別データを送信する
ことを特徴とする請求項９に記載の情報処理装置。
【請求項１１】
上記装着手段は、
円形状のリング部と、
上記リング部に設けられ、上記所定部位における識別対象に撮像光を照射する光源とからなり、

上記撮像光は、
上記通信対象に近接された上記生体を介して、当該通信対象に設けられた撮像素子に導光される
ことを特徴とする請求項９に記載の情報処理装置。
【請求項１２】
上記撮像光は、上記通信対象から供給される点滅パターンに従って点滅照射し、
上記点滅パターンは、上記撮像光に基づいて順次生成される画像の輝度パターンと比較される
ことを特徴とする請求項９に記載の情報処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理システム及び情報処理装置に関し、例えば生体固有の血管に基づくデータを認証する場合に適用して好適なものである。
【背景技術】
【０００２】
従来、生体固有となる血管の形成パターン（以下、これを血管形成パターンと呼ぶ）に基づいて認証処理を実行する認証装置が提案されている。
【０００３】
この種の認証装置においては、血管に内在する脱酸素化ヘモグロビン（静脈血）又は酸素化ヘモグロビン（動脈血）に近赤外線帯域の光が特異的に吸収されることを利用して登録者の血管を撮像し、この撮像結果として得られる血管画像から血管形成パターン（以下、これを登録血管形成パターンと呼ぶ）を抽出し、これを所定のデータベースに登録しておく。
【０００４】
そして認証装置は、この登録処理と同様にして認証対象者における血管形成パターン（以下、これを認証対象者血管形成パターンと呼ぶ）を抽出し、この認証対象者血管形成パターンを、予めデータベースに登録しておいた複数の登録血管形成パターンと順次照合するようにして、本人(登録者)の有無を判定するようになされている（例えば特許文献１参照）。
【特許文献１】特願２００３－２４２４９２公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながらこのような認証装置においては、認証対象者血管形成パターンに対応する登録血管形成パターンが検出されるまで、複数の登録血管形成パターンを順次照合するため、認証対象者血管形成パターンと照合する処理時間が増大する傾向にあり、ユーザにとっては待ち時間が長くなるという問題があった。
【０００６】
殊に、データベースに登録される登録血管形成パターンが多くなるほど、かかる処理時間は増大する傾向にあることから、ユーザの待ち時間はより長くなるといった結果を招くことになる。
【０００７】
本発明は以上の点を考慮してなされたもので、使い勝手を格段的に向上させ得る情報処理システム及び情報処理装置を提案するものである。
【課題を解決するための手段】
【０００８】
かかる課題を解決するために本発明は、第１の情報処理装置と、第２の情報処理装置とによって構成される情報処理システムであって、第１の情報処理装置には、生体の所定部位における識別対象を生体識別データとして記憶する記憶手段と、生体に保持されて所定

の位置にまで近接され、当該位置に近接された状態で通信する第１の通信手段と　を設け、第２の情報処理装置には、位置に近接された生体を生体データとして検出する生体センサと、位置に近接された生体に保持される第１の通信手段と通信する第２の通信手段と、生体センサで検出された生体データから所定部位に対応する生体データを抽出する抽出手段と、抽出手段で抽出された所定部位に対応する生体データと、第１及び第２の通信手段を介して第１の情報処理装置から取得した生体識別データとに基づいて生体認証する生体認証手段とを設けるようにした。

【０００９】

従ってこの情報処理システムでは、第１の情報処理装置を第２の情報処理装置に近接させるだけで、当該第２の情報処理装置が、このときこの第１の情報処理装置を保持するユーザの生体データを自動的に取得できるため、複数の第１の情報処理装置にそれぞれ記憶される全ての生体識別データをデータベースとして第２の情報処理装置に登録する場合に比して、当該第２の情報処理装置におけるデータベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができ、その処理に費やされる時間を大幅に短縮することができる。

【００１０】

また本発明は、情報処理装置であって、所定の位置に近接された生体を生体データとして検出する生体センサと、その位置に近接された生体に保持される通信対象と通信する近距離通信手段と、生体センサで検出された生体データから所定部位における生体データを抽出する抽出手段と、抽出手段で抽出された所定部位における生体データと、通信対象に登録され、当該通信対象から近距離通信手段を介して取得した生体識別データとに基づいて照合する生体認証手段とを設けるようにした。

【００１１】

従ってこの情報処理装置では、通信対象が近接されるだけで、その通信対象を保持するユーザの生体データを自動的に取得できるため、複数の通信対象にそれぞれ記憶される全ての生体識別データをデータベースとして登録しておく場合に比して、当該データベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができ、その処理に費やされる時間を大幅に短縮することができる。

【００１２】

さらに本発明は、情報処理装置であって、生体の所定部位に装着する装着手段と、所定部位における識別対象を生体識別データとして記憶する記憶手段と、装着手段に保持され、当該装着手段を装着した所定部位を近接させた通信対象に対して生体識別データを送信する通信手段とを設け、当該装着手段を装着した状態で近接された生体が通信対象において生体データとして検出されるようにした。

【００１３】

従ってこの情報処理装置では、所定部位に装着した装着手段を通信対象に近接させるだけで、その通信対象を保持するユーザの生体データが自動的に取得されるため、複数の情報処理装置にそれぞれ記憶される全ての生体識別データをデータベースとして通信対象に登録しておく場合に比して、当該データベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができ、その処理に費やされる時間を大幅に短縮することができる。

【発明の効果】

【００１４】

本発明の情報処理システムによれば、第１の情報処理装置を第２の情報処理装置に近接させるだけで、当該第２の情報処理装置が、このときこの第１の情報処理装置を保持するユーザの生体データを自動的に取得できるようにしたことにより、複数の第１の情報処理装置にそれぞれ記憶される全ての生体識別データをデータベースとして第２の情報処理装置に登録する場合に比して、当該第２の情報処理装置におけるデータベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができるため、その処理に費やされる時間の短縮に応じてユーザの待ち時間を短縮化することができ、か

くして使い勝手を格段的に向上させることができる。
【００１５】
また本発明の情報処理装置によれば、通信対象が近接されるだけで、その通信対象を保持するユーザの生体データを自動的に取得できるようにしたことにより、複数の通信対象にそれぞれ記憶される全ての生体識別データをデータベースとして登録しておく場合に比して、当該データベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができるため、その処理に費やされる時間の短縮に応じてユーザの待ち時間を短縮化することができ、かくして、使い勝手を格段的に向上させることができる。
【００１６】
さらに本発明の情報処理装置によれば、所定部位に装着した装着手段を通信対象に近接させるだけで、その通信対象を保持するユーザの生体データが自動的に取得されるようにしたことにより、複数の情報処理装置にそれぞれ記憶される全ての生体識別データをデータベースとして通信対象に登録しておく場合に比して、当該データベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができるため、その処理に費やされる時間の短縮に応じてユーザの待ち時間を短縮化することができ、かくして使い勝手を格段的に向上させることができる。
【発明を実施するための最良の形態】
【００１７】
以下図面について、本発明の一実施の形態を詳述する。
【００１８】
（１）第１の実施の形態
（１－１）第１の実施の形態による情報処理システムの全体構成
図１において、１は全体として第１の実施の形態による情報処理システムを示し、カード形状でなる複数の端末装置（以下、これをカード端末と呼ぶ）２ｉ（ｉ＝１、２……、Ｎ）と、認証装置３と、カード端末管理サーバ４とによって構成される。
【００１９】
各カード端末２ｉは、所定のサービスの提供対象となるユーザにそれぞれ発行されたものであり、当該ユーザに内在する血管の形成パターン（以下、これを血管形成パターンと呼ぶ）を登録データ（以下、これを登録血管パターンデータと呼ぶ）としてそれぞれ保持している。
【００２０】
一方、認証装置３は、所定の設置箇所に設置されており、サービスを受けようとするユーザが血管形成パターンを登録した正規ユーザ（以下、これを登録者と呼ぶ）本人であるか否かを、各カード端末２ｉにそれぞれ保持されている登録血管パターンデータに基づいて判定するようになされている。なお、この情報処理システム１では、１つの認証装置３を設置する場合であるが、複数の認証装置３を所定の設置箇所に設置するようにしても良い。
【００２１】
他方、カード端末管理サーバ４は、各カード端末２ｉを、当該カード端末２ｉにそれぞれ保持された固有の端末ＩＤ(Identifier)に基づいて管理するようになされている。
【００２２】
この情報処理システム１では、サービスを提供する場合、ユーザはカード端末２ｘ（ｘ＝１、２、……、又はＮ）を認証装置３の所定位置にかざすように近接する。この場合、認証装置３は、カード端末２ｘを近接させたユーザの手における血管形成パターンを取得すると共に、端末ＩＤに基づくカード端末２ｘと、カード端末管理サーバ４との相互認証を中継する。また認証装置３は、この相互認証結果に応じてカード端末２ｘに保持された登録血管パターンデータを取得する。
【００２３】
この状態において認証装置３は、ユーザから取得した血管形成パターンと、カード端末

２ｘから取得した登録血管パターンデータに表される血管形成パターンとを照合することによって登録者本人の有無を判定するようになされている。

【００２４】

このようにこの情報処理システム１では、カード端末２ｘを認証装置３に近接させるだけで、当該認証装置３が、このときこのカード端末２ｘを把持するユーザの血管形成パターンを自動的に取得し、この血管形成パターンと、当該カード端末２ｘに予め登録された血管形成パターンとを照合する。

【００２５】

従ってこの情報処理システム１では、複数のカード端末２ｉにそれぞれ記憶される全ての血管形成パターンをデータベースとして認証装置３に登録する場合に比して、当該認証装置３におけるデータベースから各血管形成パターンを任意の順序で読み出して照合するといった処理を回避することができるため、その処理に費やされる時間を大幅に短縮することができるようになされている。

【００２６】

またこの情報処理システム１では、複数のカード端末２ｉにそれぞれ記憶される全ての血管形成パターンをデータベースとして認証装置３に登録する場合に比して、当該データベースに登録された血管形成パターンが認証装置３の管理者等によって盗用されるといったことを回避することができるため、当該血管形成パターンの信頼性を向上することができるようになされている。

【００２７】

さらにこの情報処理システム１においては、生体の内方に介在する固有構造物の血管を認証対象として選定することによって、生体表面に有する指紋等を認証対象とする場合に比して、生体からの直接的な盗用のみならず第三者による登録者への成りすましをも防止できるようになされている。

【００２８】

（１－２）カード端末及び認証装置の構成

ここで、カード端末２ｘ及び認証装置３の構成を図２及び図３に示す。

【００２９】

このカード端末２ｘには、アンテナコイル（以下、これを端末側アンテナと呼ぶ）ATc_Dと、当該端末側アンテナATc_Dに接続された信号処理部（以下、これを端末側信号処理部と呼ぶ）ICc_D１とが所定位置に内蔵されており、当該端末側信号処理部ICc_D１には、端末ＩＤ及び登録血管パターンデータが登録されている。

【００３０】

この端末側信号処理部ICc_D１は、認証装置３から供給される電磁誘導信号を端末側アンテナATc_Dを介して受信した場合、その受信に応じて誘起される電圧を駆動電圧として起動し、認証装置３及びネットワークＮＴ（図１）を介してカード端末管理サーバ４との間で各種データ授受することによって相互認証する。

【００３１】

また端末側信号処理部ICc_D１は、この相互認証結果に応じて認証装置３から供給される暗号データを用いて登録血管パターンデータを暗号化し、当該暗号化した登録血管パターンデータを端末側アンテナATc_Dを介して認証装置３に送信するようになされている。

【００３２】

一方、この認証装置３は、例えば角筒状でなり、当該認証装置３の筐体には、カード端末２ｘを近接させる面（以下、これを近接面と呼ぶ）３Ａが選定されている。この近接面３Ａには、無色透明のガラス材質でなる開口窓ＯＷが形成され、当該開口窓ＯＷを囲むようにアンテナコイル（以下、これを認証側アンテナと呼ぶ）ATc_rが設けられている。

【００３３】

この認証側アンテナATc_rは、認証装置３の筐体内の所定位置に内蔵された信号処理部（以下、これを認証側信号処理部と呼ぶ）ICc_r１に接続される。認証側信号処理部

ＩＣ$_{cr}$１は、認証側アンテナＡＴ$_{cr}$を介して電磁誘導信号を発信するようになされており、当該電磁誘導信号によって、近接面３Ａに近接されたカード端末２ｘをバッテリーレス状態で起動させ得るようになされている。

【００３４】

かかる構成に加えてこの認証側信号処理部ＩＣ$_{cr}$１には、近接面３Ａに近接させたカード端末２ｘを把持する手の内方における血管を読み取る生体情報読取部ＬＩＲが接続されている。この生体情報読取部ＬＩＲは、開口窓ＯＷの下方に設けられた撮像カメラＣＭ（図３）と、近接面３Ａの所定位置に設けられた１又は２以上の近赤外光光源ＬＳとからなっている。

【００３５】

この実施の形態の場合、カード端末２ｘを把持する手と、近接面３Ａとは所定の位置関係を保って近接するようになされており、例えば、図３に示したように、当該手の指における指腹を、近接面３Ａに対して平行となる状態かつ所定方向ＤＲから対向させた状態で近接するようになされている。

【００３６】

なお、この近接面３Ａに対して手を能動的に近接するようにしても良く、あるいは、所定の位置に配置させるための部材（図示せず）を介して受動的に近接するようにしても良い。また端末側信号処理部ＩＣ$_{CD}$１（図２）に予め記憶されている登録血管パターンデータは、近接面３Ａに対して所定の位置関係にある手から抽出された血管形成パターンを表すデータとなっている。

【００３７】

このようにしてカード端末２ｘを把持した手を近接面３Ａに近接させた場合、認証側信号処理部ＩＣ$_{cr}$１には、カード端末２ｘの起動に応じてそのカード端末２ｘから、相互認証に関するデータが供給される。

【００３８】

この場合、認証側信号処理部ＩＣ$_{cr}$１は、ネットワークＮＴ（図１）を介してカード端末管理サーバ４（図１）に接続し、相互認証に関するネットワークＮＴを介してカード端末管理サーバ４に送信する。また認証側信号処理部ＩＣ$_{cr}$１は、カード端末管理サーバ４から供給される相互認証に関するデータを受信すると、当該データを認証側アンテナＡＴ$_{cr}$を介してカード端末２ｘに送信する。

【００３９】

その一方で、認証側信号処理部ＩＣ$_{cr}$１は、生体情報読取部ＬＩＲを駆動する。この場合、図４において破線で示すように、近赤外光光源ＬＳから撮像空間に発射される近赤外光は、カード端末２ｘを把持する手の指に照射され、当該指に内在する血管を通るヘモグロビンに吸収されると共に血管以外の組織で散乱及び反射してその指から出射する。この出射した近赤外光は、血管を投影する近赤外光（以下、これを血管投影光と呼ぶ）として得られ、この血管投影光が、開口窓ＯＷ（図１）から撮像カメラＣＭの撮像レンズ１０ａ、絞り（図示せず）及び近赤外光透過フィルタ１０ｂを順次介して固体撮像素子１０ｃに入射することとなる。

【００４０】

認証側信号処理部ＩＣ$_{cr}$１は、撮像カメラＣＭを制御して撮像レンズ１０ａの焦点距離及びフォーカス位置を調整すると共に、固体撮像素子１０ｃに入射する血管投影光の光量を調整する。そして認証側信号処理部ＩＣ$_{cr}$１は、固体撮像素子１０ｃの撮像面に結像される血管を所定周期で血管画像信号として生成し、当該血管画像信号から血管形成パターンを抽出する。

【００４１】

また認証側信号処理部ＩＣ$_{cr}$１は、カード端末２ｘと、カード端末管理サーバ４との相互認証の成功した場合、当該成功に応じて所定の暗号鍵を認証側アンテナＡＴ$_{cr}$を介してカード端末２ｘに送信する。そして認証側信号処理部ＩＣ$_{cr}$１は、カード端末２ｘから、この暗号鍵により暗号化された登録血管パターンデータを認証側アンテナＡＴ$_{cr}$

を介して受信すると、これを復号化する。

【００４２】

このようにして認証側信号処理部ＩＣ$_{cr}$１は、撮像対象のユーザから抽出した血管形成パターンと、カード端末２ｘに登録された登録血管パターンデータに表される血管形成パターンとを取得する。

【００４３】

そして認証側信号処理部ＩＣ$_{cr}$１は、これら血管形成パターンを照合し、当該照合結果に応じて登録者本人の有無を判定するようになされている。ちなみにこの判定結果は、この認証装置内に搭載されたサービス提供処理部又はこの認証装置３外に接続されたサービス提供処理部に通知され、当該サービス提供処理部によって所定のサービスが登録者に提供されることとなる。

【００４４】

（１－３）信号処理部の具体的な回路構成

次に、上述した端末側信号処理部ＩＣ$_{CD}$１及び認証側信号処理部ＩＣ$_{cr}$１の具体的な回路構成について説明する。

【００４５】

図５において、カード端末２ｘの端末側信号処理部ＩＣ$_{CD}$１は、この端末側信号処理部ＩＣ$_{CD}$１全体の制御を司るＣＰＵ（（Central Processing Unit）以下、端末側ＣＰＵと呼ぶ）２１に対して、プログラムや各種設定データ等が記憶されたＲＯＭ（Read Only Memory）、ワークメモリとしてのＲＡＭ（Random Access Memory）及び各種パラメータが格納されたＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）からなる内部メモリ２２と、電磁誘導方式に準拠して各種信号を送受信する送受信部２３と、暗号化／復号化部２４と、乱数発生部２５とをそれぞれバス２６を介して相互に接続して構成される。

【００４６】

この送受信部２３は、認証装置３から供給される電磁誘導信号を端末側アンテナＡＴ$_{CD}$を介して受けると、これに応じて誘起される電圧を内蔵バッテリ（図示せず）蓄積するようになされている。この蓄積した電圧は、所定の閾値まで達すると、駆動電圧として各回路部に供給され、この結果、カード端末２ｘが起動することとなる。

【００４７】

この状態において端末側ＣＰＵ２１は、内部メモリ２２のＲＯＭに格納されたプログラム及び設定データに基づいて、起動した旨を通知する起動通知データＤ１を生成する。そして端末側ＣＰＵ２１は、この起動通知データＤ１を送受信部２３及び端末側アンテナＡＴ$_{CD}$を順次介して認証装置３に送信すると共に、各回路部を制御してカード端末管理サーバ４と相互認証するようになされている。

【００４８】

一方、認証装置３の認証側信号処理部ＩＣ$_{cr}$１は、この認証側信号処理部ＩＣ$_{cr}$１全体の制御を司るＣＰＵ（以下、これを認証側ＣＰＵと呼ぶ）３１に対して、プログラムや各種設定データ等が記憶されたＲＯＭ、当該認証側ＣＰＵ３１のワークメモリとしてのＲＡＭ及び各種パラメータが格納されたＥＥＰＲＯＭからなる内部メモリ３２と、電磁誘導方式に準拠して各種信号を送受信する送受信部３３と、暗号化／復号化部３４と、ネットワークインタフェース３５と、生体情報読取部ＬＩＲを駆動制御する駆動制御部３６と、生体情報読取部ＬＩＲでの読取結果から血管形成パターンを抽出するパターン抽出部３７と、認証部３８とをそれぞれバス３９を介して相互に接続して構成される。

【００４９】

この送受信部３３は、電磁誘導信号を認証側アンテナＡＴ$_{cr}$を介して発信するようになされており、当該電磁誘導信号によって起動したカード端末２ｘから送信される起動通知データＤ１を認証側アンテナＡＴ$_{cr}$を介して受信すると、これを認証側ＣＰＵ３１に送出する。

【００５０】

認証側ＣＰＵ３１は、送受信部３３から供給される起動通知データＤ１を受けると、内部メモリ３２のＲＯＭに格納されたプログラム及び設定データに基づいて各回路部を制御し、カード端末２ｘと、カード端末管理サーバ４との相互認証を中継するようになされている。

【００５１】

（１－４）相互認証の中継処理

ここで、かかる認証装置３における相互認証の中継処理を、カード端末２ｘと認証装置３とにおける相互認証とともに詳細に説明する。

【００５２】

実際上、端末側ＣＰＵ２１は、起動に応じて、端末ＩＤをシード（Seed）とするデータ（以下、これをシードデータと呼ぶ）Ｄ２aと、当該シードデータＤ２ａを拡散するデータ（以下、これを拡散データと呼ぶ）Ｄ２ｂとを生成し、これらを乱数発生部２５に送出する。

【００５３】

乱数発生部２５は、シードデータＤ２ａを拡散データＤ２ｂにより拡散することによって乱数パターンのデータ（以下、これを乱数パターンデータと呼ぶ）Ｄ３を生成し、これを暗号化／復号化部２４に送出する。

【００５４】

暗号化／復号化部２４は、この乱数パターンデータＤ３に対して、予め保持している鍵情報を用いて例えばＤＥＳ（Data Encryption Standard）等の所定の暗号化処理を施し、この結果得られる暗号化乱数パターンデータＤ４を送受信部２３及び端末側アンテナAT_{CD}を順次介して認証装置３に送信する。

【００５５】

認証装置３の認証側ＣＰＵ３１は、カード端末２ｘから認証側アンテナAT_{cr}及び送受信部３３を順次介して起動通知データＤ１を受けると、ネットワークインタフェース３５からネットワークＮＴ（図１）を介してカード端末管理装置４に接続する。その後、認証側ＣＰＵ３１は、カード端末２ｘから送信される暗号化乱数パターンデータＤ４を認証側アンテナAT_{cr}及び送受信部３３を順次介して受けると、ネットワークインタフェース３５からカード端末管理装置４に送信する。

【００５６】

カード端末管理装置４では、この暗号化乱数パターンデータＤ４は、当該カード端末管理装置４に保持されている鍵情報を用いて所定の復号化処理が施され、その後に逆拡散処理が施され、カード端末２ｘの端末ＩＤ（シードデータＤ２ａ）が取得される。

【００５７】

この状態においてカード端末管理装置４では、この端末ＩＤ（シードデータＤ２ａ）が当該カード端末管理装置４に保持されているデータベースにある場合には現在の通信相手がカード端末２ｘであるものと判定される一方、当該データベースにない場合には現在の通信相手がカード端末２ｘに成りすましているものと判定され、この判定結果が管理側判定データＤ５として認証装置３に送信される。

【００５８】

またカード端末管理装置４では、カード端末２ｘの端末ＩＤが、拡散データＤ２ｂに対応する拡散データで再び拡散され、当該拡散結果に対して、カード端末２ｘと同一の鍵情報を用いて暗号化処理が施され、この結果得られる暗号化乱数パターンデータＤ６が認証装置３に送信される。

【００５９】

認証装置３の認証側ＣＰＵ３１は、カード端末管理装置４から供給される管理側判定データＤ５及び暗号化乱数パターンデータＤ６をネットワークインタフェース３５を介して受信し、当該管理側判定データＤ５を内部メモリ３２に一時記憶すると共に、暗号化乱数パターンデータＤ６を送受信部３３及び認証側アンテナAT_{cr}を順次介してカード端末２ｘに送信する。

【００６０】
カード端末２ｘの端末側ＣＰＵ２１は、認証装置３から返信される暗号化乱数パターンデータＤ６を端末側アンテナＡＴ$_{CD}$及び送受信部２３を順次介して受けると、暗号化／復号化部２４において、当該暗号化乱数パターンデータＤ６に対して鍵情報を用いて復号化処理を施し、乱数発生部２５において、この復号化処理結果を拡散データＤ２ｂにより逆拡散することによってシードデータＤ７を生成する。
【００６１】
そして端末側ＣＰＵ２１は、このシードデータＤ７に表される端末ＩＤが自己の端末ＩＤと一致した場合には現在の通信相手が認証装置３であるものと判定する一方、当該自己の端末ＩＤと不一致であった場合には現在の通信相手が認証装置３に成りすましているものと判定し、この判定結果を端末側判定データＤ８として、送受信部２３及び端末側アンテナＡＴ$_{CD}$を順次介して認証装置３に送信する。
【００６２】
このようにして認証装置３の認証側ＣＰＵ３１は、カード端末２ｘと認証装置３における相互認証に関する各種データを中継することによって、この相互認証処理結果として管理側判定データＤ５と、端末側判定データＤ８とをそれぞれ取得することができるようになされている。
【００６３】
（１－５）生体認証処理
次に、この生体認証処理を詳細に説明する。
【００６４】
実際上、認証側ＣＰＵ３１は、カード端末２ｘから認証側アンテナＡＴ$_{cr}$及び送受信部３３を順次介して起動通知データＤ１を受けると、駆動制御部３６を介して生体情報取得部ＬＩＲを制御し、当該生体情報取得部ＬＩＲの撮像カメラＣＭ（図３、図４）によって、このとき近接面３Ａ（図３、図４）に近接されるカード端末２ｘを把持する手の指内方の血管を撮像する。
【００６５】
そして認証側ＣＰＵ３１は、パターン抽出部３７において、この撮像結果として得られる血管画像信号Ｓ１に対して、Ａ／Ｄ（Analog/Digital）変換処理、２値化処理、血管線状化処理、分岐点等の特徴点抽出処理などの各種処理を施し、この結果得られる血管形成パターンのデータＤ１０を認証部３８に送出する。
【００６６】
一方、認証側ＣＰＵ３１は、上述のカード端末２ｘと認証装置３における相互認証の中継処理の結果として、当該カード端末２ｘ及び認証装置３から得られた端末側判定データＤ８及び管理側判定データＤ５の判定結果が相互に認証成功を表すものであった場合には、暗号化／復号化部３４において、予め内部メモリ３２に記憶された認証側暗号鍵Ｄ１１に対して、秘密鍵を用いて所定の暗号化処理を施し、当該暗号化された認証側暗号鍵Ｄ１１を送受信部３３及び認証側アンテナＡＴ$_{cr}$を順次介してカード端末２ｘに送信する。
【００６７】
カード端末２ｘの端末側ＣＰＵ２１は、この暗号化された認証側暗号鍵Ｄ１１を送受信部２３及び端末側アンテナＡＴ$_{CD}$を順次介して受信すると、暗号化／復号化部２４において、予め内部メモリ２２に記憶された端末側暗号鍵Ｄ１２に対して、秘密鍵を用いて所定の暗号化処理を施し、当該暗号化された端末側暗号鍵Ｄ１２を送受信部２３及び端末側アンテナＡＴ$_{CD}$を順次介して認証装置３に送信する。
【００６８】
また端末側ＣＰＵ２１は、暗号化／復号化部２４において、暗号化された認証側暗号鍵Ｄ１１に対して、秘密鍵を用いて所定の復号化処理を施す。そして端末側ＣＰＵ２１は、復号化した認証側暗号鍵Ｄ１１を用いて、内部メモリ２２のＥＥＰＲＯＭに登録された登録パターンデータＤ１３を暗号化すると共に、当該認証側暗号鍵Ｄ１１で暗号化された登

録パターンデータＤ１３を、端末側暗号鍵Ｄ１２を用いてさらに暗号化し、当該２重暗号化された登録パターンデータＤ１３を送受信部２３及び端末側アンテナAT_{CD}を順次介して認証装置３に送信する。

【００６９】

認証装置３の認証側ＣＰＵ３１は、暗号化された端末側暗号鍵Ｄ１２を認証側アンテナAT_{cr}及び送受信部３３を順次介して受信すると、暗号化／復号化部３４において、当該暗号化された端末側暗号鍵Ｄ１２に対して、秘密鍵を用いて所定の復号化処理を施す。

【００７０】

また認証側ＣＰＵ３１は、その後にカード端末２ｘから送信される、２重暗号化された登録パターンデータＤ１３を待ち受ける。そして認証側ＣＰＵ３１は、２重暗号化された登録パターンデータＤ１３を受信すると、復号化した端末側暗号鍵Ｄ１２を用いて復号化すると共に、予め内部メモリ３２に記憶された認証側暗号鍵Ｄ１１を用いて復号化し、当該復号化した登録パターンデータＤ１３を認証部３８に送出するようになされている。

【００７１】

このようにして認証側ＣＰＵ３１は、カード端末２ｘに登録された登録パターンデータＤ１３を取得する場合には、認証側暗号鍵Ｄ１１と、端末側暗号鍵Ｄ１２とをカード端末２ｘとの間で相互に受け渡し、これら暗号鍵Ｄ１１、Ｄ１２を用いて登録パターンデータＤ１３を２重暗号化した状態でカード端末２ｘに送信させる。従って、この認証側ＣＰＵ３１では、登録パターンデータＤ１３の送信途中での盗用を強固に防止し、セキュリティ強化を図ることができるようになされている。

【００７２】

認証部３８は、この登録パターンデータＤ１３と、パターン抽出部３７で抽出された血管形成パターンのデータＤ１０とを照合する。そして認証部３８は、これらデータＤ１０、Ｄ１３に表されるこれら血管形成パターンの照合の程度が所定の閾値以上であった場合には、登録者本人であると判定する一方、当該閾値未満であった場合には、第三者であると判定するようになされている。

【００７３】

（１－６）認証処理手順

ここで、かかる認証側ＣＰＵ３１による相互認証の中継処理及び生体認証処理の一連の認証処理（以下、これを第１の認証処理と呼ぶ）は、図６に示す第１の認証処理手順ＲＴ１に従って行われる。

【００７４】

すなわち認証側ＣＰＵ３１は、近接面３Ａに近接されたカード端末２ｘから起動通知データＤ１を受けると、この第１の認証処理手順ＲＴ１をステップＳＰ０において開始し、続くステップＳＰ１において、生体情報読取部ＬＩＲ（図２）を起動し、当該カード端末２ｘを把持する手の指に内在する血管形成パターンの抽出を開始する。

【００７５】

そして認証側ＣＰＵ３１は、ステップＳＰ２において、カード端末２ｘと、カード端末管理サーバ４との相互認証を中継し、続くステップＳＰ３において、当該カード端末２ｘ及びカード端末管理サーバ４から供給される管理側判定データＤ５と、端末側判定データＤ８とに基づいて相互認証が成功したか否かを判定する。

【００７６】

ここで、認証側ＣＰＵ３１は、相互認証が成功したと判定した場合には、次のステップＳＰ４において、自己の認証側暗号鍵Ｄ１１（図５）をカード端末２ｘに送信すると共に、当該カード端末２ｘに保持された端末側暗号鍵Ｄ１２（図５）をカード端末２ｘから取得し、続くステップＳＰ５において、これら認証側暗号鍵Ｄ１１及び端末側暗号鍵Ｄ１２を用いて、カード端末２ｘから２重暗号化された状態で送信される登録血管形成パターンＤ１３を復号化する。

【００７７】

そして認証側ＣＰＵ３１は、次のステップＳＰ６において、ステップＳＰ１で開始する

ことにより取得したユーザの血管形成パターンと、ステップＳＰ５で復号化した登録血管形成パターンＤ１３に表される血管形成パターンとを照合し、続くステップＳＰ７において、当該照合結果に基づいて登録者本人の有無を判定した後、ステップＳＰ８に移ってこの第１の認証処理手順ＲＴ１を終了する。

【００７８】

一方、認証側ＣＰＵ３１は、ステップＳＰ３で相互認証が失敗したと判定した場合には、上述のステップＳＰ４乃至ステップＳＰ７までの各種処理を実行することなく、ステップＳＰ８に移ってこの第１の認証処理手順ＲＴ１を終了する。

【００７９】

このようにして認証側ＣＰＵ３１は、第１の認証処理を実行することができるようになされている。

【００８０】

（１－７）第１の実施の形態による動作及び効果

以上の構成において、この情報処理システム１の認証装置３は、複数のカード端末２ｉ（図１）のうち、近接面３Ａ（図３）に近接されたカード端末２ｘと通信し、当該カード端末２ｘに保持された登録血管形成パターンＤ１３を取得する。

【００８１】

この一方で、認証装置３は、近接面３Ａに近接されたカード端末２ｘを把持する手を撮像し、当該撮像結果から血管形成パターンを抽出する。

【００８２】

そして認証装置３は、これら血管形成パターンに基づいて、このとき近接面３Ａにカード端末２ｘを近接させたユーザが、カード端末２ｘに保持された登録血管形成パターンの登録者であるか否かを認証する。

【００８３】

従ってこの認証装置３では、複数のカード端末２ｉにそれぞれ記憶される全ての血管形成パターンをデータベースとして認証装置３に登録する場合に比して、当該認証装置３におけるデータベースから各血管形成パターンを任意の順序で読み出して照合するといった処理を回避することができるため、当該照合時間を大幅に短縮することができる。

【００８４】

この場合、登録血管形成パターンはカード端末２ｘに保持されているため、血管形成パターンをデータベースとして認証装置３に登録する場合に比して、当該データベースに登録された血管形成パターンが認証装置３の管理者等によって盗用されるといったことを回避することができるため、当該血管形成パターンの信頼性を向上することができるようになされている。

【００８５】

また認証装置３は、カード端末２ｘとカード端末管理サーバ４との相互認証を中継し、当該相互認証が成功したと判定した場合に生体認証を実行することにより、当該カード端末２ｘに保持された登録血管形成パターンを盗用して偽造カード端末に保持するといった成りすましをも回避することができるため、セキュリティの強化をより一段と図ることができる。

【００８６】

以上の構成によれば、複数のカード端末２ｉのうち、近接面３Ａに近接されたカード端末２ｘに保持された登録血管形成パターンＤ１３と、当該カード端末２ｘを把持するユーザから抽出した血管形成パターンとを照合するようにしたことにより、複数のカード端末２ｉ（図１）にそれぞれ記憶される全ての血管形成パターンをデータベースとして認証装置３に登録する場合に比して、照合処理の低減することができるため、当該照合処理の低減を通じてユーザの待ち時間を短縮化することができ、かくして使い勝手を向上することができる。

【００８７】

（２）第２の実施の形態

（２－１）第２の実施の形態による情報処理システムの全体構成

図７において、５１は全体として第２の実施の形態による情報処理システムを示し、指輪型でなる複数の端末装置（以下、これをリング端末と呼ぶ）５２ｉ（ｉ＝１、２、……、Ｎ）と、認証装置５３とによって構成される。

【００８８】

各リング端末５２ｉは、所定のサービスの提供対象となるユーザにそれぞれ配られたものであり、固有の端末ＩＤを、認証装置５３に登録された登録血管形成パターンデータを識別するためのデータとしてそれぞれ保持している。

【００８９】

一方、認証装置５３は、各リング端末５２ｉにそれぞれ保持された端末ＩＤと、登録血管パターンデータとをデータベース化して管理しており、このデータベースの登録血管パターンデータに基づいて、サービスを受けようとするユーザが登録者本人であるか否かを判定するようになされている。なお、この情報処理システム１では、１つの認証装置３を設置する場合を例示してあるが、複数の認証装置３を所定の設置箇所に設置するようにしても良い。

【００９０】

この情報処理システム５１では、サービスを提供する場合、ユーザはリング端末５２ｘ（ｘ＝１、２、……、又はＮ）を装着した部分を認証装置５３の所定位置に近接する。この場合、認証装置５３は、端末ＩＤに基づいてリング端末５２ｘと端末認証（相互認証）すると共に、カード端末２ｘを近接させた装着部分に内在する血管の血管形成パターンを取得する。

【００９１】

そして認証装置５３は、端末認証（相互認証）が成功した場合には、そのカード端末２ｘの端末ＩＤに基づいて、対応する登録血管パターンデータをデータベースから特定し、当該特定した登録血管パターンデータに表される血管形成パターンと、ユーザから取得した血管形成パターンを照合することによって登録者本人の有無を判定するようになされている。

【００９２】

このようにしてこの情報処理システム５１では、リング端末５２ｘを認証装置５３に近接させるだけで、当該認証装置５３が、このときこのリング端末５２ｘを装着したユーザの血管形成パターンを自動的に取得し、これをデータベースに保持された登録血管形成パターンと照合する。

【００９３】

この場合、認証装置５３は、データベースに登録された複数の血管形成パターンのうち、端末認証（相互認証）で用いた端末ＩＤに基づいて対応する登録血管形成パターンを特定してから照合するため、データベースから各血管形成パターンを任意の順序で逐一読み出して照合する場合に比して、その処理負荷を大幅に低減することができ、この結果、ユーザの待ち時間を大幅に短縮することができるようになされている。

【００９４】

なお、この情報処理システム５１は、登録血管パターンデータの管理機能を認証装置５３に設けると共に、当該管理される登録血管パターンデータのなかから対応する登録血管パターンデータを識別するためのデータ（端末ＩＤ）をカード端末５２ｉに登録させた点で、当該登録血管パターンデータの管理機能を設けることなく、個々のカード端末２ｉに登録血管パターンデータを登録させた情報処理システム１（図１）とは相違する。

【００９５】

従ってこの情報処理システム５１では、情報処理システム１に比べると、認証装置５３の管理者によってデータベースの登録血管パターンデータが盗用される可能性は比較的高いが、その反面、カード端末５２ｉから登録血管パターンデータが盗用される可能性は確実になくなる。

【００９６】

またこの情報処理システム５１は、端末認証機能及び生体認証機能を認証装置５３に一括する形態となっているが、この形態は、当該端末認証機能をカード端末管理サーバ４及び生体認証機能を認証装置３に分割していた情報処理システム１（図１）の形態に比して、例えば家庭内等のように比較的小規模なシステムを構築する場合には、特に有用である。

【００９７】

（２－２）リング端末及び認証装置の構成

ここで、リング端末５２ｘ及び認証装置５３の構成を説明する。

【００９８】

リング端末５２ｘは、第１の実施の形態における対応部分に同一の符号を付した図８に示すように、薄厚でなる円形状のリング部５４と、このリング部５４の外周表面に設けられた装飾部５５とからなり、当該リング部５４を介して指に装脱着することができるようになされている。

【００９９】

またこのリング部５４の内部には、リング部５４の形状に対応する端末側アンテナ$ＡＴ_{ＣＤ}$が収納されると共に、当該リング部５４の内周表面には、複数の近赤外光光源ＬＳ（$ＬＳ_{Ａ}$～$ＬＳ_{Ｄ}$）が装飾部５５の近傍に配設されている。そしてこれら端末側アンテナ$ＡＴ_{ＣＤ}$及び近赤外光光源ＬＳは、装飾部５５の内部に収納された端末側信号処理部$ＩＣ_{ＣＤ}$２に接続されている。

【０１００】

この端末側信号処理部$ＩＣ_{ＣＤ}$２は、認証装置５３から供給される電磁誘導信号を端末側アンテナ$ＡＴ_{ＣＤ}$を介して受信した場合、その受信に応じて誘起される電圧を駆動電圧として起動し、予め保持された端末ＩＤを用いて認証装置５３との間で各種データ授受することによって相互認証すると共に、近赤外光光源ＬＳを駆動制御し得るようになされている。なお、この端末側信号処理部$ＩＣ_{ＣＤ}$２の具体的処理内容については後述する。

【０１０１】

一方、認証装置５３は、図２及び図３との対応部分に同一符号を付した図９及び図１０に示すように、第１の実施の形態における認証装置３に比して、近接面３Ａに設けられた近赤外光光源ＬＳを省いた点（ただし、端末側に新たに設けられいる）と、認証側信号処理部$ＩＣ_{ｃｒ}$１に代えて認証側信号処理部$ＩＣ_{ｃｒ}$２を設けた点を除いて、第１の実施の形態における認証装置３と同一構成となっている。

【０１０２】

具体的に認証側信号処理部$ＩＣ_{ｃｒ}$２は、認証側信号処理部$ＩＣ_{ｃｒ}$１における相互認証中継処理に代えて、リング端末５２ｘと直接的に相互認証する相互認証処理を設けた点と、当該認証側信号処理部$ＩＣ_{ｃｒ}$１における生体認証処理に代えて、登録者本人の有無を２手法を用いて判定する生体認証処理（以下、これを２重生体認証処理と呼ぶ）を設けた点が相違点となっている。

【０１０３】

かかる相互認証処理及び２重生体認証処理を、図５との対応部分に同一符号を付した図１１を用いて詳細に説明する。

【０１０４】

（２－３）相互認証処理

リング端末５２ｘの端末側ＣＰＵ６１は、認証装置３から供給される電磁誘導信号を端末側アンテナ$ＡＴ_{ＣＤ}$を介して受信した場合、その受信に応じて誘起される電圧を駆動電圧として起動する。そして端末側ＣＰＵ６１は、第１の実施の形態で上述したように、起動通知データＤ１を端末側アンテナ$ＡＴ_{ＣＤ}$及び送受信部２３を順次介して認証装置５３に送信した後、暗号化乱数パターンデータＤ４を生成して認証装置５３に送信する。

【０１０５】

認証装置３の認証側ＣＰＵ７１は、リング端末５２ｘから供給される起動通知データＤ１を認証側アンテナ$ＡＴ_{ｃｒ}$及び送受信部３３を順次介して受けると、その後にリング端

末５２ｘから供給される暗号化乱数パターンデータＤ４を待ち受ける。

【０１０６】

認証側ＣＰＵ７１は、暗号化乱数パターンデータＤ４を受けた場合、暗号化／復号化部３４において、予め保持されたカード端末２ｘと同一の鍵情報を用いて所定の復号化処理を施した後、乱数発生部７２において、当該復号結果に対して逆拡散処理を施し、この結果得られるリング端末５２ｘの端末ＩＤ（シードデータＤ２ａ）を取得する。

【０１０７】

この状態において認証側ＣＰＵ７１は、この端末ＩＤがハードディスク７３におけるデータベースにある場合には現在の通信相手がリング端末５２ｘであるものと判定する一方、当該データベースにない場合には現在の通信相手がリング端末５２ｘに成りすましているものと判定し、当該判定結果を管理側判定データＤ５として内部メモリ３２に一時的に記憶する。

【０１０８】

また認証側ＣＰＵ７１は、乱数発生部７２において、リング端末５２ｘにおける拡散データＤ２ｂに対応する拡散データで再び端末ＩＤを拡散した後、暗号化／復号化部３４において、当該拡散結果に対して、鍵情報を用いて暗号化処理を施し、この結果得られる暗号化乱数パターンデータＤ６を送受信部３３及び認証側アンテナ$ＡＴ_{cr}$を順次介してリング端末５２ｘに送信する。

【０１０９】

リング端末５２ｘの端末側ＣＰＵ６１は、この暗号化乱数パターンデータＤ６に対して第１の実施の形態と同様にして各種処理を施し、この結果得られるシードデータＤ７に表される端末ＩＤが自己の端末ＩＤと一致した場合には現在の通信相手が認証装置５３であるものと判定する一方、当該自己の端末ＩＤと不一致であった場合には現在の通信相手が認証装置５３に成りすましているものと判定し、この判定結果を端末側判定データＤ８として、送受信部２３及び端末側アンテナ$ＡＴ_{CD}$を順次介して認証装置５３に送信する。

【０１１０】

このようにして認証装置５３の認証側ＣＰＵ７１は、リング端末５２ｘとの間における端末認証（相互認証）結果として管理側判定データＤ５と、端末側判定データＤ８とをそれぞれ取得することができるようになされている。

【０１１１】

（２－４）生体認証処理

次に、２重生体認証処理について説明する。

【０１１２】

実際上、認証側ＣＰＵ７１は、リング端末５２ｘから供給される起動通知データＤ１を受けた場合に、シードデータＤ２０ａ及び拡散データＤ２０ｂを生成する。そして認証側ＣＰＵ７１は、暗号化／復号化部３４において、シードデータＤ２０ａ及び拡散データＤ２０ｂに対して、予め保持している鍵情報を用いて所定の暗号化処理を施し、当該暗号化されたシードデータＤ２０ａ及び拡散データＤ２０ｂを送受信部３３及び認証側アンテナ$ＡＴ_{cr}$を順次介してリング端末５２ｘに送信する。

【０１１３】

一方、リング端末５２ｘの端末側ＣＰＵ６１は、暗号化されたシードデータＤ２０ａ及び拡散データＤ２０ｂを端末側アンテナ$ＡＴ_{CD}$及び送受信部２３を順次介して受けると、暗号化／復号化部２４において、当該暗号化されたシードデータＤ２０ａ及び拡散データＤ２０ｂに対して復号化処理を施す。

【０１１４】

そして端末側ＣＰＵ６１は、乱数発生部２５において、復号化したシードデータＤ２０ａを拡散データＤ２０ｂにより拡散し、近赤外光光源ＬＳの点灯を表す「１」と近赤外光光源ＬＳの非点灯を表す「０」とからなる点滅パターンのデータ（以下、これを点滅パターンデータと呼ぶ）Ｄ２１を生成する。

【０１１５】

この状態において端末側ＣＰＵ６１は、光源駆動部６２において、点滅パターンデータＤ２１に基づいて近赤外光光源ＬＳを点滅させると共に、暗号化／復号化部２４において、当該点滅パターンデータＤ２１に対して、秘密鍵を用いて暗号化処理を施し、当該暗号化された点滅パターンデータＤ２１を送受信部２３及び端末側アンテナ$ＡＴ_{ＣＤ}$を順次介して認証装置５３に送信する。

【０１１６】

認証側ＣＰＵ７１は、リング端末５２ｘから、暗号化された点滅パターンデータＤ２１を認証側アンテナ$ＡＴ_{ｃｒ}$及び送受信部３３を順次介して受けた場合、暗号化／復号化部３４において、当該暗号化された点滅パターンデータＤ２１を復号化し、この結果得られる点滅パターンデータＤ２１を点滅パターン照合部７６に送出する。

【０１１７】

また認証側ＣＰＵ７１は、撮像カメラＣＭも制御し、このとき近接面３Ａ（図１０）に近接されるリング端末５２ｘを装着する指内方の血管を撮像するようになされている。

【０１１８】

ここで、この実施の形態の場合、リング端末５２ｘを装着する手と、近接面３Ａとは所定の位置関係を保って近接するようになされており、例えば、図１０に示したように、所定の指背に装飾部５５が対向するようにリング端末５２ｘを装着し、当該指の指腹を、近接面３Ａに対して平行となる状態かつ所定方向ＤＲから対向させた状態で近接するようになされている。

【０１１９】

なお、この近接面３Ａに対して手を能動的に近接するようにしても良く、あるいは、所定の位置に配置させるための部材（図示せず）を介して受動的に近接するようにしても良い。

【０１２０】

このようにしてリング端末５２ｘを装着する手を近接面３Ａに近接させた場合、図１２において破線で示すように、当該リング端末５２ｘの近赤外光光源ＬＳから発射される近赤外光は、そのリング端末５２ｘを装着する指に照射され、当該指に内在する血管を通るヘモグロビンに吸収されると共に血管以外の組織で散乱及び反射してその指から出射する。この出射した近赤外光は、血管投影光として得られ、この血管投影光が、開口窓ＯＷから撮像カメラＣＭの撮像レンズ１０ａ、絞り（図示せず）及び近赤外光透過フィルタ１０ｂを順次介して固体撮像素子１０ｃに入射し、血管画像信号Ｓ１０ｊ（ｊ＝１、２、……、ｍ）として輝度パターン生成部７４及びパターン抽出部７５に送出される。

【０１２１】

輝度パターン生成部７４は、血管画像信号Ｓ１０ｊにおける輝度状態の変化を検出する。ここで、血管画像信号Ｓ１０ｊにおける輝度状態は、近赤外光光源ＬＳの点滅パターンに対応するものとなっているため、当該近赤外光光源ＬＳが非点灯のときには暗い状態となり、これに対して近赤外光光源ＬＳが点灯のときには明るい状態となっている。

【０１２２】

そして輝度パターン生成部７４は、かかる検出結果に基づいて、血管画像信号Ｓ１０ｊにおける輝度状態が明るい状態を表す「１」と当該輝度状態が暗い状態を表す「０」とからなるパターン（以下、これを輝度パターンと呼ぶ）データＤ３０を生成し、これをパターン抽出部７５及び点滅パターン照合部７６に送出する。

【０１２３】

パターン抽出部７５は、撮像カメラＣＭから供給される血管画像信号Ｓ１０ｊに対してＡ／Ｄ（Analog/Digital）変換処理や血管線状化処理等の各種処理を施した後に２値化処理を施し、２値血管画像のデータを生成する。

【０１２４】

そしてパターン抽出部７５は、輝度パターン生成部７６から供給される輝度パターンデータＤ３０に基づいて、これら２値血管画像のデータのなかから近赤外光光源ＬＳの点灯時に対応する１枚の２値血管画像を選択し、当該選択した２値血管画像から分岐点等の特

徴点抽出し、この結果得られる血管形成パターンのデータＤ１０を認証部７７に送出する。

【０１２５】

点滅パターン照合部７６は、リング端末５２ｘから供給された点滅パターンデータＤ２１と、輝度パターン生成部７４から供給される輝度パターンデータＤ３０との状態（「１」及び「０」の配列状態）を照合することによって、例えば血管形成パターンのフィルムに近赤外光を照射する等といったような巧妙な成りすまし行為を検出するようになされている。

【０１２６】

そして点滅パターン照合部７６は、かかる照合結果が一致した場合には成りすまし行為がないものと判定する一方、当該照合結果が不一致であった場合には成りすまし行為があるものと判定し、この判定結果を点滅パターン判定データＤ３１として認証部７７に送出する。

【０１２７】

一方、認証側ＣＰＵ７１は、上述のリング端末５２ｘとの間における相互認証により得た端末側判定データＤ８及び認証側判定データＤ５の判定結果が相互に認証成功を表すものであった場合には、暗号化／復号化部３４において、予め内部メモリ３２に記憶された認証側暗号鍵Ｄ１１に対して、秘密鍵を用いて所定の暗号化処理を施し、当該暗号化された認証側暗号鍵Ｄ１１を送受信部３３及び認証側アンテナ$ＡＴ_{ｃｒ}$を順次介してリング端末５２ｘに送信する。

【０１２８】

リング端末５２ｘの端末側ＣＰＵ６１は、この暗号化された認証側暗号鍵Ｄ１１を送受信部２３及び端末側アンテナ$ＡＴ_{ＣＤ}$を順次介して受信すると、暗号化／復号化部２４において、予め内部メモリ２２に記憶された端末側暗号鍵Ｄ１２に対して、秘密鍵を用いて所定の暗号化処理を施し、当該暗号化された端末側暗号鍵Ｄ１２を送受信部２３及び端末側アンテナ$ＡＴ_{ＣＤ}$を順次介して認証装置５３に送信する。

【０１２９】

また端末側ＣＰＵ６１は、暗号化／復号化部２４において、暗号化された認証側暗号鍵Ｄ１１に対して、秘密鍵を用いて所定の復号化処理を施す。そして端末側ＣＰＵ６１は、復号化した認証側暗号鍵Ｄ１１を用いて、内部メモリ２２のＥＥＰＲＯＭに記憶された端末ＩＤを暗号化すると共に、当該認証側暗号鍵Ｄ１１で暗号化された端末ＩＤを、端末側暗号鍵Ｄ１２を用いてさらに暗号化し、当該２重暗号化された端末ＩＤを送受信部２３及び端末側アンテナ$ＡＴ_{ＣＤ}$を順次介して認証装置５３に送信する。

【０１３０】

認証装置５３の認証側ＣＰＵ７１は、暗号化された端末側暗号鍵Ｄ１２を認証側アンテナ$ＡＴ_{ｃｒ}$及び送受信部３３を順次介して受信すると、暗号化／復号化部３４において、当該暗号化された端末側暗号鍵Ｄ１２に対して、秘密鍵を用いて所定の復号化処理を施す。

【０１３１】

また認証側ＣＰＵ７１は、その後にリング端末５２ｘから送信される、２重暗号化された端末ＩＤを待ち受ける。そして認証側ＣＰＵ７１は、２重暗号化された端末ＩＤを受信すると、復号化した端末側暗号鍵Ｄ１２を用いて復号化すると共に、予め内部メモリ３２に記憶された認証側暗号鍵Ｄ１１を用いて復号化し、当該復号化した端末ＩＤを認証部７７に送出するようになされている。

【０１３２】

このようにして認証部７７には、かかる端末ＩＤと、点滅パターン照合部７６から供給される点滅パターン判定データＤ３１と、パターン抽出部７５から供給される血管形成パターンのデータＤ１０とがそれぞれ入力されることとなる。

【０１３３】

認証部７７は、点滅パターン判定データＤ３１の判定結果が成りすまし行為がない旨を

表している場合には、端末ＩＤに対応する登録血管形成パターンデータをデータベースから検索し、当該端末ＩＤに対応する登録血管形成パターンデータＲＤをハードディスク７３から読み出す。

【０１３４】

そして認証部７７は、ハードディスク７３から読み出した登録血管形成パターンデータＲＤと、パターン抽出部７５から供給される血管形成パターンのデータＤ１０とに基づいて、登録者本人の有無を判定するようになされている。

【０１３５】

（２－５）認証処理手順

ここで、かかる認証側ＣＰＵ７１による相互認証処理及び２重生体認証処理の一連の認証処理（以下、これを第２の認証処理と呼ぶ）は、図１３に示す第２の認証処理手順ＲＴ２に従って行われる。

【０１３６】

すなわち認証側ＣＰＵ７１は、近接面３Ａに近接されたカード端末２ｘから起動通知データＤ１（図１１）を受けると、この第２の認証処理手順ＲＴ２をステップＳＰ１０において開始し、続くステップＳＰ１１において、リング端末５２ｘと相互認証処理を実行し、続くステップＳＰ１２において、当該相互認証処理結果として得られる管理側判定データＤ５と、端末側判定データＤ８とに基づいて相互認証が成功したか否かを判定する。

【０１３７】

ここで、認証側ＣＰＵ７１は、相互認証が成功したと判定した場合には、次のステップＳＰ１３において、所定のシードデータＤ２０ａ及び拡散データＤ２０ｂ（図１１）を暗号化した状態でリング端末５２ｘに送信する。この場合、リング端末５２ｘでは、これらシードデータＤ２０ａ及び拡散データＤ２０ｂに基づいて点滅パターンデータＤ２１（図１１）が生成され、当該点滅パターンデータＤ２１が暗号化された状態で認証装置５３に送出されると共に、その点滅パターンデータＤ２１に基づいて近赤外光光源ＬＳ（図１２）が点滅される。

【０１３８】

次いで、認証側ＣＰＵ７１は、ステップＳＰ１４において、撮像カメラＣＭ（図１２）を起動し、当該撮像カメラＣＭでの撮像結果（血管撮像信号Ｓ１０ｊ）に基づいて、リング端末５２ｘを把持する手の指に内在する血管形成パターンを抽出する。

【０１３９】

そして認証側ＣＰＵ７１は、次のステップＳＰ１５において、リング端末５２ｘから送信される点滅パターンデータＤ２１に表される点滅パターンと、撮像カメラＣＭで撮像された血管撮像信号Ｓ１０ｊにおける輝度パターンとを照合し、続くステップＳＰ１６において、当該点滅パターン及び輝度パターンが一致すると判定した場合には、ステップＳＰ１７に移る。

【０１４０】

認証側ＣＰＵ７１は、このステップＳＰ１７において、ステップＳＰ１１での相互認証時に得られるリング端末５２ｘの端末ＩＤに対応付けられた登録血管形成パターンデータＲＤをデータベースから特定し、当該端末ＩＤに対応する登録血管形成パターンデータＲＤをハードディスク７３から読み出す。

【０１４１】

そして認証側ＣＰＵ７１は、次のステップＳＰ１８において、この登録血管形成パターンデータＲＤに表される血管形成パターンと、ステップＳＰ１４でユーザから抽出した血管形成パターンとを照合し、続くステップＳＰ１９において、当該照合結果に基づいて登録者本人の有無を判定した後、次のステップＳＰ２０に移ってこの第２の認証処理手順ＲＴ２を終了する。

【０１４２】

一方、認証側ＣＰＵ７１は、ステップＳＰ１２で相互認証が失敗したと判定した場合、又はステップＳＰ１６で点滅パターン及び輝度パターンが一致しないと判定した場合には

、当該ステップＳＰ１９で登録者本人の有無を判定するまでもなく、当該登録者以外の第三者からのアクセスであるため、その後の各種処理を実行せずにステップＳＰ２０に移ってこの認証処理手順ＲＴ２を終了する。

【０１４３】

このようにして認証側ＣＰＵ７１は、第２の認証処理を実行することができるようになされている。

【０１４４】

（２－６）第２の実施の形態による動作及び効果

以上の構成において、この情報処理システム５１の認証装置５３は、複数のリング端末５２ｉ（図７）のうち、近接面３Ａ（図１０）に近接されたリング端末５２ｘと通信して相互認証し、当該リング端末５２ｘに保持された端末ＩＤを取得する。

【０１４５】

そして認証装置５３は、相互認証が成功した場合には、この端末ＩＤに対応する登録血管形成パターンデータＲＤに表される血管形成パターンと、血管画像信号Ｓ１０ｊから抽出した血管形成パターンとを照合し、登録者の有無を判定する。

【０１４６】

従って、この認証装置５３では、当該認証装置３におけるデータベースから各血管形成パターンを任意の順序で逐一読み出して照合するといった処理を回避することができるため、当該照合時間を大幅に短縮することができる。

【０１４７】

またこの認証装置５３は、相互認証の一方で、近接面３Ａに近接されたリング端末５２ｘを装着する手に対して、所定の点滅パターンでリング端末５２ｘの近赤外光光源ＬＳを点滅させると共に、当該手を撮像する。そして認証装置５３は、相互認証が成功した場合には、近赤外光光源ＬＳを点滅させた点滅パターンと、撮像結果として得られる血管画像信号Ｓ１０ｊの輝度パターンとを照合し、当該照合結果に応じて、血管形成パターンに基づく登録者の有無を判定する。

【０１４８】

従ってこの認証装置５３では、第三者による登録者への成りすましを異なる観点から２重にチェックできるため、巧妙な成りすましを回避することができ、セキュリティの強化をより一段と図ることができる。

【０１４９】

以上の構成によれば、相互認証により得られる端末ＩＤを登録血管形成パターンデータの識別子として、複数の登録血管形成パターンデータのなかから対応する登録血管形成パターンデータＲＤを特定し、当該登録血管形成パターンデータＲＤに表される血管形成パターンと、血管画像信号Ｓ１０ｊから抽出した血管形成パターンとに基づいて登録者の有無を判定するようにしたことにより、データベースから各血管形成パターンを任意の順序で逐一読み出して照合するといった処理を回避してその照合処理の低減することができるため、当該照合処理の低減した分だけユーザの待ち時間を短縮化することができ、かくして使い勝手を向上することができる。

【０１５０】

（３）他の実施の形態

上述の第１の実施の形態では端末側（カード端末２ｉ）に登録血管形成パターンデータを登録し、第２の実施の形態では認証側（認証装置５３）に登録血管形成パターンデータを登録し、当該登録された血管形成パターンと、ユーザから抽出した血管形成パターンとが一致したときに登録者と判定するようにした場合について述べたが、本発明はこれに限らず、図２及び図５との対応部分に同一符号を付した図１４に示すように、当該端末装置１０２ｘ及び端末ＩＤを管理する端末管理サーバ１０４の双方に登録血管形成パターンデータを登録し、当該登録された２つの血管形成パターンと、認証装置１０３によってユーザから抽出された血管形成パターンとの３つがそれぞれ一致したときに登録者と判定するようにしても良い。

【０１５１】
この図１４に示す情報処理システム１０１では、第三者は、互いに異なる箇所にそれぞれ登録される登録血管形成パターンデータそれぞれを盗用することは困難であることから、当該登録された登録血管形成パターンデータの一方を第三者のものにすりかえたとしてもこれを検出することができ、この結果、セキュリティの強化をより一段と図ることができる。
【０１５２】
なお、この端末装置１０２ｘは、カード形状又はリング形状のいずれであっても良く、これ以外の形状であっても携帯型のものであれば、他の種々の形状のものを適用することができる。また、近赤外光光源ＬＳは、第１の実施の形態のように認証側に設けられていても良く、第２の実施の形態のように端末側に設けられていても良い。
【０１５３】
ここで、かかる認証装置１０３の認証処理手順を、図１５に示すフローチャートを用いて説明する。
【０１５４】
すなわち認証側ＣＰＵ１３１は、近接面３Ａに近接された端末装置１０２ｘから起動通知データＤ１を受けると、この第３の認証処理手順ＲＴ３をステップＳＰ２０において開始し、続くステップＳＰ２１において、撮像カメラＣＭ（図２）を起動し、このときこの端末装置１０２ｘを把持又は装着している手（指）に内在する血管形成パターンの抽出を開始する。
【０１５５】
そして認証側ＣＰＵ１３１は、ステップＳＰ２２において、端末装置１０２ｘと、端末管理サーバ１０４との相互認証を中継し、続くステップＳＰ２３において、当該端末装置１０２ｘ及び端末管理サーバ１０４から供給される管理側判定データＤ５と、端末側判定データＤ８とに基づいて相互認証が成功したか否かを判定する。
【０１５６】
この相互認証が成功したと判定した場合、認証側ＣＰＵ１３１は、次のステップＳＰ２４において、自己の認証側暗号鍵Ｄ１１（図５）を端末装置１０２ｘに送信すると共に、当該端末装置１０２ｘに保持された端末側暗号鍵Ｄ１２（図５）を端末装置１０２ｘから取得し、続くステップＳＰ２５において、これら認証側暗号鍵Ｄ１１及び端末側暗号鍵Ｄ１２を用いて、端末装置１０２ｘから２重暗号化された状態で送信される登録血管形成パターンＤ１３を復号化する。
【０１５７】
また認証側ＣＰＵ１３１は、ステップＳＰ２６において、ステップＳＰ２４及びＳＰ２５の各種処理と同様にして、端末ＩＤと登録血管形成パターンとの対応付をデータベースとして管理する端末管理サーバ１０４と暗号鍵を相互に交換し、当該端末管理サーバ１０４の暗号鍵及び認証装置１０３の認証側暗号鍵Ｄ１１を用いて、２重暗号化された状態で送信される登録血管形成パターンＤ１３を復号化する。ちなみにこの登録血管形成パターンＤ１３は、端末管理サーバ１０４に登録される複数の登録血管形成パターンのうち、相互認証時に用いられた端末ＩＤに対応するものである。
【０１５８】
そして認証側ＣＰＵ１３１は、次のステップＳＰ２７において、ステップＳＰ２１で開始することにより取得したユーザの血管形成パターンＰＴ１（図１４）と、ステップＳＰ２５で端末装置１０２ｘから取得した登録血管形成パターンＤ１３に表される血管形成パターンＰＴ２（図１４）と、ステップＳＰ２６で端末管理サーバ１０４から取得した登録血管形成パターンＤ１３に表される血管形成パターンＰＴ３（図１４）とを照合し、続くステップＳＰ２８において、当該照合結果に基づいて登録者本人の有無を判定した後、ステップＳＰ２９に移ってこの第３の認証処理手順ＲＴ３を終了する。
【０１５９】
一方、ステップＳＰ２３で相互認証が失敗したと判定した場合、認証側ＣＰＵ１３１は

、上述のステップＳＰ２４乃至ステップＳＰ２８までの各種処理を実行することなく、ステップＳＰ２９に移ってこの第３の認証処理手順ＲＴ３を終了する。

【０１６０】

このようにしてこの認証装置１０３は、端末装置１０２ｘ及び端末管理サーバ１０４に登録された登録血管形成パターンデータと、認証装置１０３によってユーザから抽出された血管形成パターンとに基づいて登録者の有無を判定することができる。

【０１６１】

なお、登録者の有無の判定機能を端末管理サーバ１０４に設けるようにしても、端末装置１０２ｘ及び端末管理サーバ１０４に登録された登録血管形成パターンデータと、認証装置１０３によってユーザから抽出された血管形成パターンとを、当該端末管理サーバ１０４に集めるようにすれば、上述の第３の認証処理手順ＲＴ３と同様の手順で三者相互間の生体認証を実現できる。

【０１６２】

また、別の例として、図１４との対応部分に同一符号を付した図１６に示すように、登録対象の端末装置１０２ｘ及び端末管理サーバ１０４には、登録血管形成パターンデータを登録しておき、管理機能を有する端末管理サーバ１０４には、当該登録血管形成パターンデータに対応付けて、登録血管形成パターンデータを生成するまでの処理過程のデータから生成したハッシュ値を登録しておく。

【０１６３】

そして、認証装置１０３は、端末装置１０２ｘ及び端末管理サーバ１０４に登録された登録血管形成パターンデータを取得し、当該登録血管形成パターンデータに表される血管形成パターンＰＴ２、ＰＴ３同士を照合する。その一方で、認証装置１０３は、このとき端末管理サーバ１０４から取得した登録血管形成パターンデータに対応するハッシュ値Ｈ１も取得し、このハッシュ値Ｈ１と、ユーザから抽出した血管形成パターンのデータを生成するまでの処理過程のデータから生成したハッシュ値Ｈ２とを照合する。

【０１６４】

このようにすれば、第三者は、登録血管形成パターンデータを盗用するのみならず、ハッシュ値生成アルゴリズムや、ハッシュ値Ｈ２がいずれの処理過程で得られたデータを用いて生成したかを知らなければ、成りすましができないことになるため、セキュリティの強化をより一段と図ることができる。

【０１６５】

また、登録血管形成パターンデータと、ユーザから抽出した血管形成パターンのデータとを照合する場合に比して、データ量が少ない分だけ照合処理負荷を低減することができ、ユーザの待ち時間をより一段と短縮化することができる。

【０１６６】

なお、この場合、認証側ＣＰＵ１３１は、図１５との対応部分に同一符号を付した図１７に示す第４の認証処理手順ＲＴ４のように、第３の認証処理手順ＲＴ３におけるステップＳＰ２６及びＳＰ２７に代えて、当該ステップＳＰ２６及びＳＰ２７での取得対象及び照合対象を一部変更したステップＳＰ２６′及びＳＰ２７′を設けるだけで、当該第３の認証処理手順ＲＴ３と同様の処理手順に従って生体認証処理を実行することができる。

【０１６７】

さらに、別の例として、図２及び図５との対応部分に同一符号を付した図１８に示す情報処理システム２０１を適用することもできる。この情報処理システム２０１では、所定の秘密鍵を用いて暗号化された暗号登録血管形成パターンデータＤ１００が端末装置２０２ｘに登録され、当該未暗号化状態における登録血管形成パターンデータのハッシュ値Ｈ１と、秘密鍵ＫＹとが端末ＩＤに対応付けられて端末管理サーバ２０４に登録される。

【０１６８】

この端末装置２０２ｘは、カード形状又はリング形状のいずれであっても良く、これ以外の形状であっても携帯型のものであれば、他の種々の形状のものを適用することができる。また、近赤外光光源ＬＳは、第１の実施の形態のように認証側に設けられていても良

く、第２の実施の形態のように端末側に設けられていても良い。

【０１６９】

認証装置２０３は、この端末装置２０２ｘを近接された場合に、当該端末装置２０２ｘを把持又は装着している手（指）に内在する血管形成パターンの抽出を開始する。一方で、認証装置２０３は、暗号登録血管形成パターンデータＤ１００を端末装置２０２ｘから取得すると共に、当該端末装置２０２ｘの端末ＩＤに対応する登録血管形成パターンデータのハッシュ値Ｈ１と、秘密鍵ＫＹとを端末管理サーバ２０４から取得する。

【０１７０】

そして認証装置２０３は、所定のアルゴリズムに従って、秘密鍵ＫＹを用いて暗号登録血管形成パターンデータＤ１００を復号化すると共に、当該復号化された登録血管形成パターンデータからハッシュ値を生成し、当該生成したハッシュ値（以下、これを比較用ハッシュ値と呼ぶ）と、端末管理サーバ２０４から取得したハッシュ値Ｈ１とを照合する。

【０１７１】

また認証装置２０３は、この照合結果が一致した場合には、ユーザから取得した血管形成パターンＰＴと、復号化した登録血管形成パターンデータに表される血管形成パターンとを照合する。

【０１７２】

このようにこの情報処理システム２０１では、暗号登録血管形成パターンデータＤ１００に対して個別の秘密鍵ＫＹは端末装置２０２ｘに送られないため、この秘密鍵ＫＹが分からなければ、第三者には暗号登録血管形成パターンデータＤ１００から比較用ハッシュ値を求めることは不可能となる。従って、この情報処理システム２０１においては、端末装置２０２ｘ内の暗号登録血管形成パターンデータＤ１００を置き換えた場合等には、一般に、ハッシュ値を用いた最初の照合段階で第三者であることを判定することができるため、登録血管形成パターンを用いて照合する場合に比して、データ量が少ない分だけ照合処理負荷を大幅に低減することができ、ユーザの待ち時間をより一段と短縮化することができる。

【０１７３】

またこの情報処理システム２０１においては、第三者は、互いに異なる箇所にそれぞれ登録される暗号登録血管形成パターンデータＤ１００、秘密鍵ＫＹ及びハッシュ値Ｈ１を盗用することは困難であると共に、これら暗号登録血管形成パターンデータＤ１００及び秘密鍵ＫＹから比較用ハッシュ値を求めることも困難であるため、端末装置２０２ｘ内の暗号登録血管形成パターンデータＤ１００を置き換えたとしてもこれを検出することができ、この結果、セキュリティの強化をより一段と図ることができる。これに加えてこの情報処理システム２０１においては、登録血管形成パターンデータそのものを管理することがないため、外部に対する血管形成パターンの流出等を防止でき、より一段とセキュリティを強化することができる。

【０１７４】

さらにこの情報処理システム２０１においては、登録血管形成パターンデータそのものを管理することがないため、当該登録血管形成パターンデータを管理することによる処理負荷を回避できると共に、その管理する登録血管形成パターンデータの送信処理を回避することができるため、全体として処理パフォーマンスを向上することができる。

【０１７５】

ここで、かかる認証装置２０３の認証処理手順を、図１９に示すフローチャートを用いて説明する。

【０１７６】

すなわち認証側ＣＰＵ２３１は、近接面３Ａに近接された端末装置２０２Ｘから起動通知データＤ１を受けると、この第５の認証処理手順ＲＴ５をステップＳＰ３０において開始し、続くステップＳＰ３１において、撮像カメラＣＭ（図２）を起動し、このときこの端末装置２０２Ｘを把持又は装着している手（指）に内在する血管形成パターンの抽出を開始する。

【０１７７】
そして認証側ＣＰＵ２３１は、ステップＳＰ３２において、端末装置２０２Ｘと、端末管理サーバ２０４との相互認証を中継し、続くステップＳＰ３３において、当該端末装置２０２Ｘ及び端末管理サーバ２０４から供給される管理側判定データＤ５と、端末側判定データＤ８とに基づいて相互認証が成功したか否かを判定する。
【０１７８】
この相互認証が成功したと判定した場合、認証側ＣＰＵ２３１は、次のステップＳＰ３４において、自己の認証側暗号鍵Ｄ１１（図５）を端末装置２０２Ｘに送信すると共に、当該端末装置２０２Ｘに保持された端末側暗号鍵Ｄ１２（図５）を端末装置２０２Ｘから取得し、続くステップＳＰ３５において、これら認証側暗号鍵Ｄ１１及び端末側暗号鍵Ｄ１２を用いて、端末装置２０２Ｘから２重暗号化された状態で送信される暗号登録血管形成パターンＤ１００（図１８）を復号化する。
【０１７９】
また認証側ＣＰＵ２３１は、ステップＳＰ３６において、ステップＳＰ３４及びＳＰ３５の各種処理と同様にして、端末管理サーバ２０４と暗号鍵を相互に交換し、当該端末管理サーバ２０４の暗号鍵及び認証装置２０３の認証側暗号鍵Ｄ１１を用いて、２重暗号化された状態で送信される秘密鍵ＫＹ及びハッシュ値Ｈ１（図１８）を復号化する。ちなみにこの秘密鍵ＫＹ及びハッシュ値Ｈ１は、端末管理サーバ２０４に登録される複数の秘密鍵及びハッシュ値のうち、相互認証時に用いられた端末ＩＤに対応するものである。
【０１８０】
そして認証側ＣＰＵ２３１は、次のステップＳＰ３７において、この秘密鍵ＫＹを用いて、ステップＳＰ３５で端末装置２０２Ｘから取得した暗号登録血管形成パターンデータＤ１００を復号化すると共に、当該復号化された登録血管形成パターンデータから比較用ハッシュ値を生成し、ステップＳＰ３８に移る。
【０１８１】
認証側ＣＰＵ２３１は、このステップＳＰ３８において、ステップＳＰ３７で生成した比較用ハッシュ値と、ステップＳＰ３６で端末管理サーバ２０４から取得したハッシュ値Ｈ１とを照合し、これらが一致しない場合には、ステップＳＰ３７で復号化した登録血管形成パターンデータに表される血管形成パターンと、ステップＳＰ３１で開始することにより取得したユーザの血管形成パターンＰＴ（図１８）とを照合し、続くステップＳＰ３９において、当該照合結果に基づいて登録者本人の有無を判定した後、ステップＳＰ４０に移ってこの第５の認証処理手順ＲＴ５を終了する。
【０１８２】
一方、ステップＳＰ３３で相互認証が失敗したと判定した場合、認証側ＣＰＵ２３１は、上述のステップＳＰ３４乃至ステップＳＰ３９までの各種処理を実行することなく、ステップＳＰ４０に移ってこの第５の認証処理手順ＲＴ５を終了する。
【０１８３】
このようにしてこの認証装置２０３は、互いに異なる箇所にそれぞれ登録される暗号登録血管形成パターンデータＤ１００、秘密鍵ＫＹ及びハッシュ値Ｈ１に基づいて三者相互間の生体認証を実現できる。
【０１８４】
なお、登録者の有無の判定機能を端末管理サーバ２０４に設けるようにしても、端末装置２０２Ｘに登録された暗号登録血管形成パターンデータＤ１００と、認証装置２０３によってユーザから抽出された血管形成パターンＰＴとを、当該端末管理サーバ２０４に集めるようにすれば、上述の第５の認証処理手順ＲＴ５と同様の手順で三者相互間の生体認証を実現できる。
【０１８５】
さらに上述の実施の形態では、登録血管形成パターンデータを電磁誘導方式により送信するデータ送信処理と、当該登録血管形成パターンデータに基づく生体認証処理との具体的な関係については述べなかったが、本発明は、これら処理を図２０に示すような関係で

行うようにする。

【０１８６】

すなわちこの図２０（Ａ）に示すように、端末側は、送信対象の登録血管形成パターンデータＤ１３を所定単位で分割し、当該分割したデータ$Ｄ１３_{k}$（ｋ＝１、２、３、……、ｌ）を順次送信する。一方、認証側は、送信されたデータ$Ｄ１３_{k}$順に、当該データ$Ｄ１３_{k}$と、登録血管形成パターンデータＤ１３の対応するデータ部分とを照合する（生体認証処理）。

【０１８７】

ここで、認証側は、例えば図２０（Ｂ）に示すように、通信エラーによりデータ$Ｄ１３_{2}$を受信できなかった場合には、生体認証処理を中断すると共に、再度データ$Ｄ１３_{2}$から送信すべき旨を端末側に通知する。その後、認証側は、再びデータ$Ｄ１３_{2}$から順次送信されるごとに、当該データ１３_{k}と、登録血管形成パターンデータＤ１３の対応するデータ部分とを照合する。

【０１８８】

このようにすれば、通信エラーが生じるたびに、登録血管形成パターンデータＤ１３の送信及び照合を最初からやりなおす場合に比して、当該送信処理及び照合処理の負荷を低減することができ、ユーザの待ち時間をより一段と短縮化することができる。

【０１８９】

さらに上述の実施の形態においては、カード状の端末装置（第１の実施の形態におけるカード端末２ｉ）又は指に装着可能な端末装置（第２の実施の形態におけるリング端末５２ｉ）を適用するようにした場合について述べたが、端末側信号処理部$ＩＣ_{ＣＤ}$１又は$ＩＣ_{ＣＤ}$２（図２、図８等）と、端末側アンテナ$ＡＴ_{ＣＤ}$（図２、図８等）とが搭載された腕輪、ネックレス、イヤリング、眼鏡等の付属品を適用するようにしても良い。また端末側信号処理部$ＩＣ_{ＣＤ}$１又は$ＩＣ_{ＣＤ}$２（図２、図８等）と、端末側アンテナ$ＡＴ_{ＣＤ}$（図２、図８等）とが搭載された携帯電話機、ＰＤＡ(Personal Digital Assistants)等の携帯型電子機器に適用するようにしても良い。要は、携帯型のものであれば、これを端末装置として採用することができる。

【０１９０】

さらに上述の実施の形態においては、生体における識別対象として指に内在する血管を適用するようにした場合について述べたが、本発明はこれに限らず、例えば生体に内在する神経や、生体に表在する指紋、あるいは声紋や口紋等、この他種々の生体識別対象を適用することができる。因みに、神経を認証対象とする場合には、例えば神経に特異的なマーカを体内に注入し、当該マーカを撮像するようにすれば、上述の実施の形態と同様にして神経を認証対象とすることができる。

【０１９１】

この場合、生体センサとして上述の実施の形態では血管を撮像する撮像カメラＣＭを採用したが、本発明はこれに限らず、適用する生体識別対象に対応するものを適宜採択することができる。また、生体識別対象をパターンとして抽出する手法も、適用する生体識別対象に対応する手法を適宜採択することができる。なお、識別対象として血管を適用する場合に、上述の実施の形態とは異なる構成の生体センサを採択するようにしても良く、パターン抽出部の内容を適宜取捨選択するようにしても良い。

【０１９２】

さらに上述の実施の形態においては、登録血管形成パターンデータ又は端末ＩＤを未暗号化状態で端末側の内部メモリ２２に登録するようにした場合について述べたが、本発明はこれに限らず、当該暗号化した状態において内部メモリ２２に登録しておくようにしても良い。

【０１９３】

さらに上述の実施の形態においては、登録血管形成パターンデータと、ユーザから取得した血管形成パターンのデータとを照合する認証部３８又は７７を認証装置３又は５３に設けるようにした場合について述べたが、本発明はこれに限らず、当該認証装置３又は５

３に代えて、ユーザの血管パターンを抽出する抽出装置を設けると共に、その抽出装置に対してインターネット等の所定のネットワークを介して認証サーバを設け、当該認証サーバに認証部３８の機能を搭載するようにしても良い。これにより、認証装置３又は５３の盗難等による個人データの流出等を未然かつ有効に防止することができ、また認証サーバに登録血管形成パターンデータを一括して格納することにより、登録血管形成パターンデータや認証部の管理等を簡素化することができる。

【０１９４】

さらに上述の実施の形態においては、生体認証処理を実行する前に、相互認証処理を実行するようにした場合について述べたが、本発明はこれに限らず、当該相互認証処理を実行する前に、生体認証処理を実行するようにしても良い。なお、この場合、生体認証処理で用いるためのユーザから抽出する血管形成パターンデータについては、かかる生体認証処理及び相互認証処理の過程での種々のタイミングで抽出することができる。

【０１９５】

さらに上述の第２の実施の形態においては、近赤外光光源ＬＳを点滅させた点滅パターンと、撮像結果として得られる血管画像信号Ｓ１０ｊの輝度パターンとを照合し、当該照合結果に応じて、血管形成パターンに基づく登録者の有無を判定するようにした場合について述べたが、本発明はこれに限らず、当該判定機能を情報処理システム１（図１）又は情報処理システム１０１（図１４）に適用するようにしても良い。なお、この場合、近赤外光光源ＬＳを点滅させる点滅パターンデータについては、認証側におけるシードデータＤ２０ａ及び拡散データＤ２０ｂから端末側で生成するようにしたが、予め点滅パターンデータを端末側で保持していても良い。

【０１９６】

さらに上述の第２の実施の形態においては、複数の端末ＩＤに対応づけられた登録血管形成パターンデータをハードディスク７３に格納した場合について述べたが、本発明はこれに限らず、この他種々のハードディスク以外の記録媒体に記録することができ、またハードディスクに代えてインターネット等の所定のネットワークを介して認証サーバを設け、当該認証サーバに登録血管形成パターンデータを格納するようにしても良い。

【０１９７】

さらに上述の第２の実施の形態においては、端末ＩＤに対応する登録血管形成パターンデータをデータベースから特定した場合について述べたが、本発明はこれに限らず、この他種々の固有となる識別子に登録血管形成パターンデータを対応付け、当該識別子に基づいてデータベースから登録血管形成パターンデータを特定するようにしても良い。

【産業上の利用可能性】

【０１９８】

本発明は、携帯品を用いるユーザにおける登録者の有無を判定する場合に利用可能である。

【図面の簡単な説明】

【０１９９】

【図１】第１の実施の形態による情報処理システムの全体構成を示す略線図である。

【図２】カード端末と認証装置との構成（１）を示す略線図である。

【図３】カード端末と認証装置との構成（２）を示す略線図である。

【図４】近赤外光の光路（１）を示す略線図である。

【図５】第１の実施の形態による端末側信号処理部と認証側認証処理部との具体的な回路構成を示す略線図である。

【図６】第１の認証処理手順を示すフローチャートである。

【図７】第２の実施の形態による情報処理システムの全体構成を示す略線図である。

【図８】リング端末の構成を示す略線図である。

【図９】リング端末と認証装置との構成（１）を示す略線図である。

【図１０】リング端末と認証装置との構成（２）を示す略線図である。

【図１１】第２の実施の形態による端末側信号処理部と認証側認証処理部との具体的な回

路構成を示す略線図である。
【図１２】近赤外光の光路（２）を示す略線図である。
【図１３】第２の認証処理手順を示すフローチャートである。
【図１４】他の実施の形態による生体認証（１）を示す略線図である。
【図１５】第３の認証処理手順を示すフローチャートである。
【図１６】他の実施の形態による生体認証（２）を示す略線図である。
【図１７】第４の認証処理手順を示すフローチャートである。
【図１８】他の実施の形態による生体認証（３）を示す略線図である。
【図１９】第５の認証処理手順を示すフローチャートである。
【図２０】データ送信処理と生体認証処理との関係を示す略線図である。
【符号の説明】
【０２００】
１、５１、１０１、２０１……情報処理システム、２ｉ（ｉ＝１、２、……、Ｎ）、２ｘ……カード端末、５２ｉ（ｉ＝１、２、……、Ｎ）、５２ｘ……リング端末、１０２ｘ、２０２ｘ……端末装置、３、５３、１０３、２０３……認証装置、４……カード端末管理サーバ、１０４、２０４……端末管理サーバ、２１、６１……端末側ＣＰＵ、３１、７１、１３１、２３１……認証側ＣＰＵ、２２、３２……内部メモリ、２３、３３……送受信部、２４、３４……暗号化／復号化部、２５……乱数発生部、３５……ネットワークインタフェース、３６……駆動制御部、３７、７５……パターン抽出部、３８、７７……認証部、７３……ハードディスク、７４……輝度パターン生成部、７６……点滅パターン照合部、ＣＭ……撮像カメラ、ＬＳ……近赤外光光源、AT_{CD}……端末側アンテナ、AT_{cr}……認証側アンテナ、$IC_{CD}1$、$IC_{CD}2$……端末側信号処理部、$IC_{cr}1$、$IC_{cr}2$……認証側信号処理部、ＲＴ１……第１の認証処理手順、ＲＴ２……第２の認証処理手順、ＲＴ３……第３の認証処理手順、ＲＴ４……第４の認証処理手順、ＲＴ５……第５の認証処理手順。

【図１】

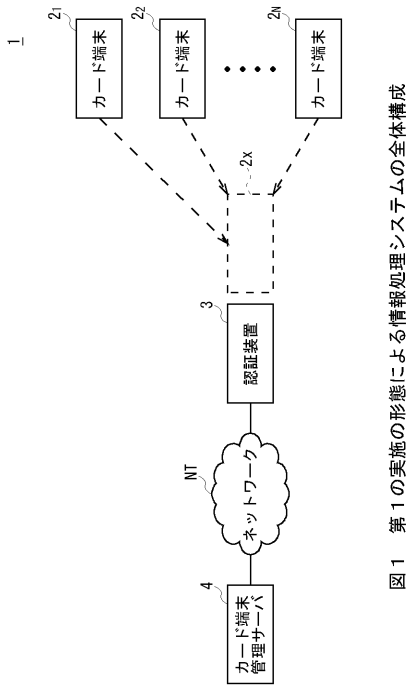

図１　第１の実施の形態による情報処理システムの全体構成

【図２】

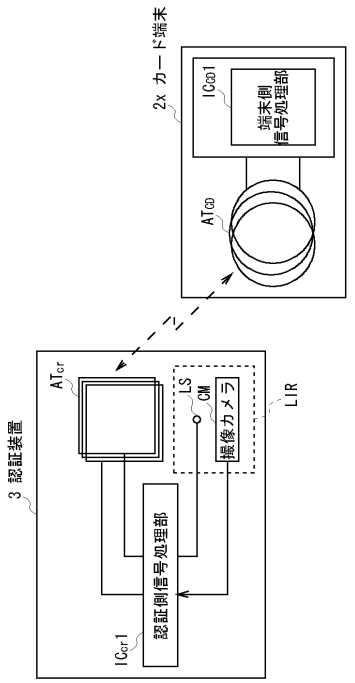

図２　カード端末と認証装置との構成（１）

【図３】

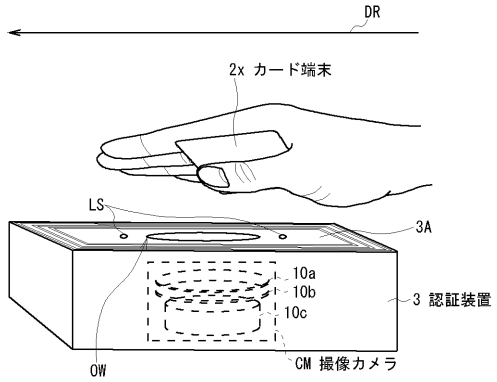

図３　カード端末と認証装置との構成（２）

【図４】

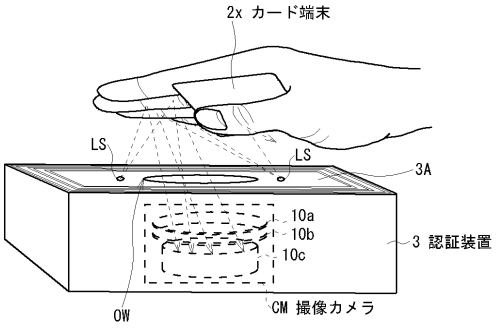

図４　近赤外光の光路（１）

【図５】

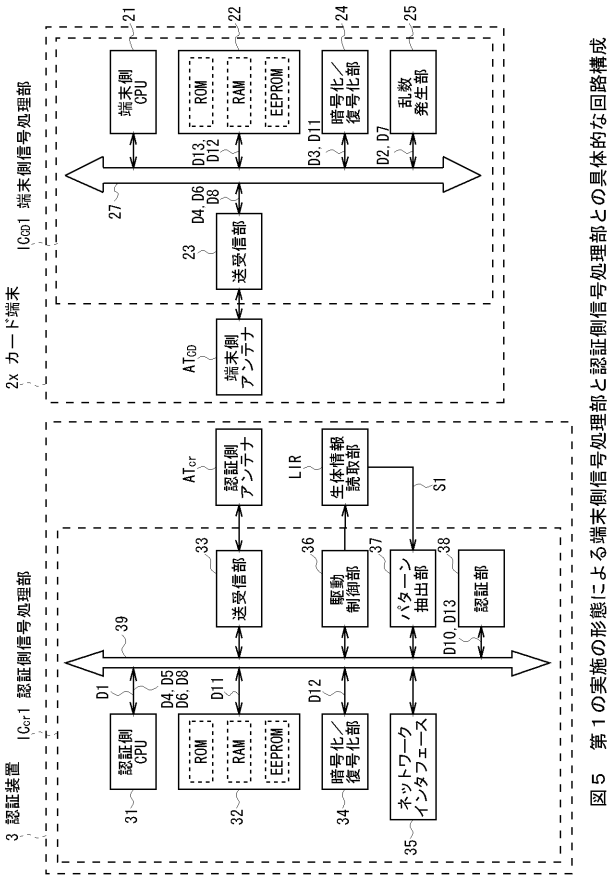

図５　第１の実施の形態による端末側信号処理部と認証側信号処理部との具体的な回路構成

【図６】

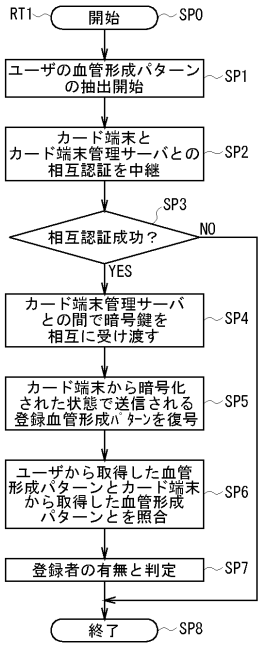

図６　第１の認証処理手順

【図７】

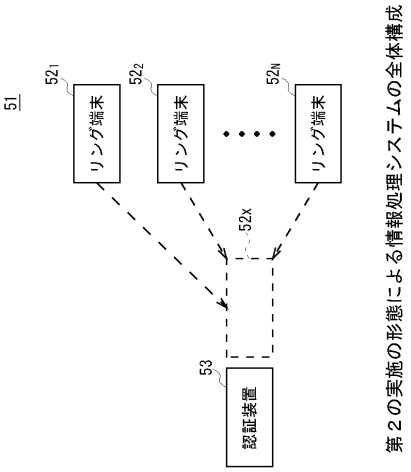

図７　第２の実施の形態による情報処理システムの全体構成

【図８】

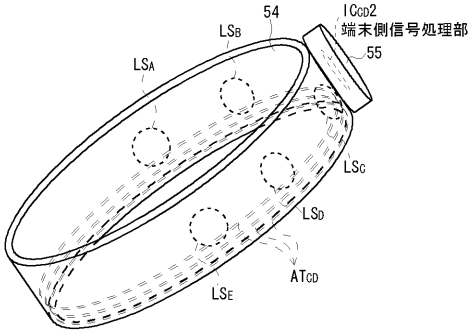

図８　リング端末の構成

【図９】

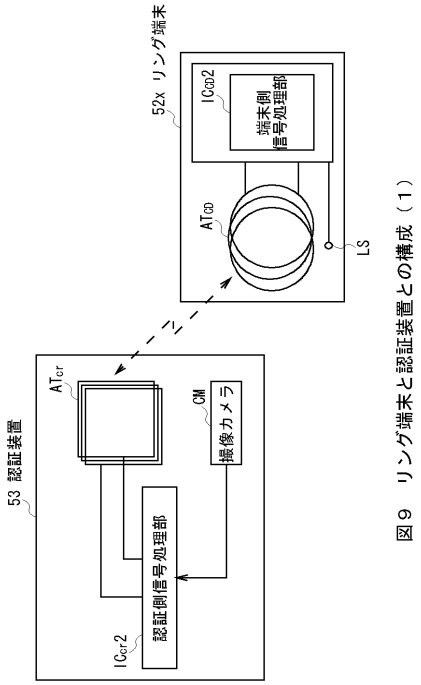

図９　リング端末と認証装置との構成（１）

【図１０】

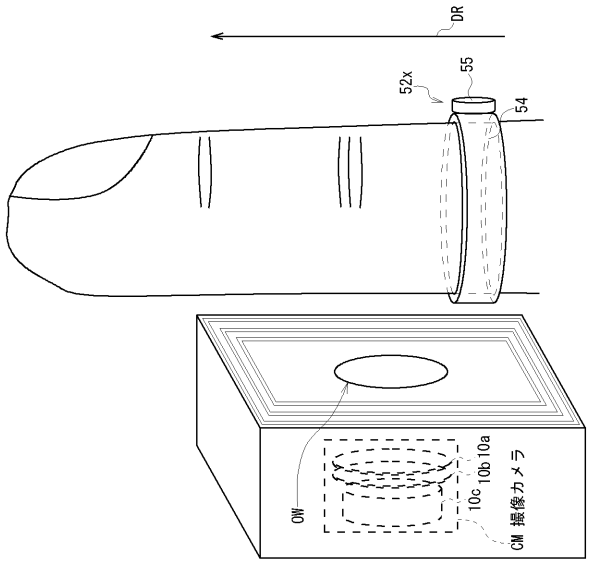

図１０　リング端末と認証装置との構成（２）

【図１１】

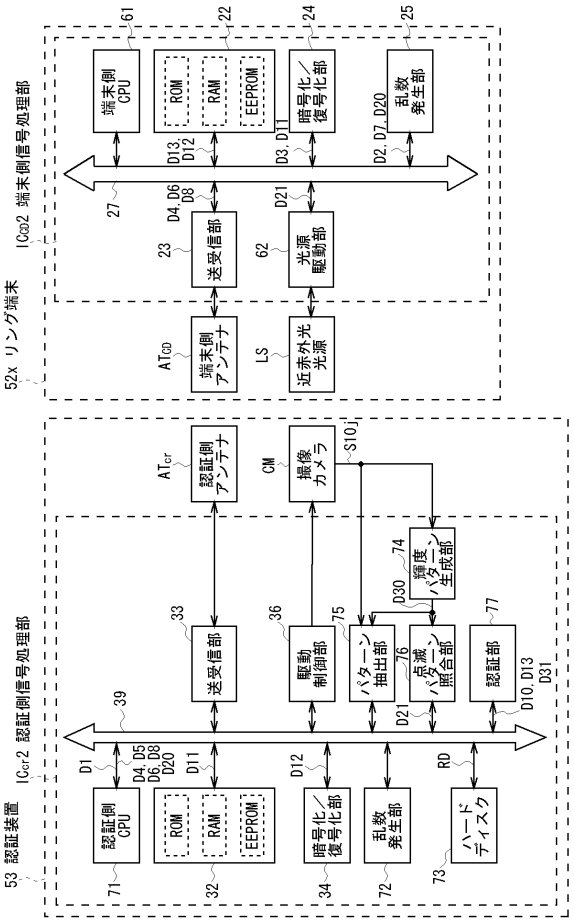

図１１　第２の実施の形態による端末側信号処理部と認証側信号処理部との具体的な回路構成

【図１２】

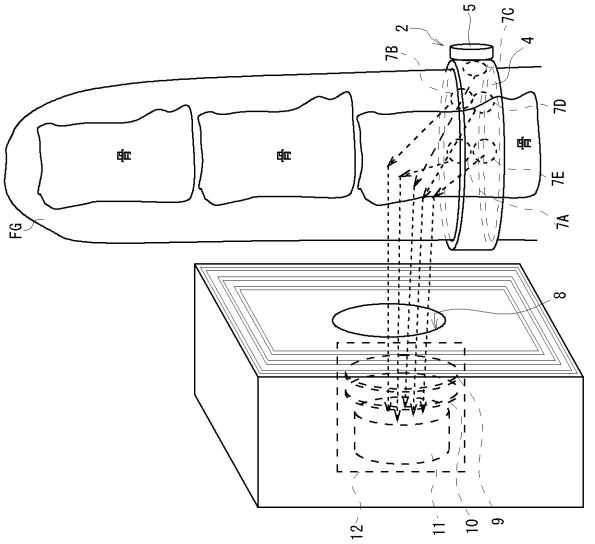

図１２　近赤外光の光路（２）

【図１３】

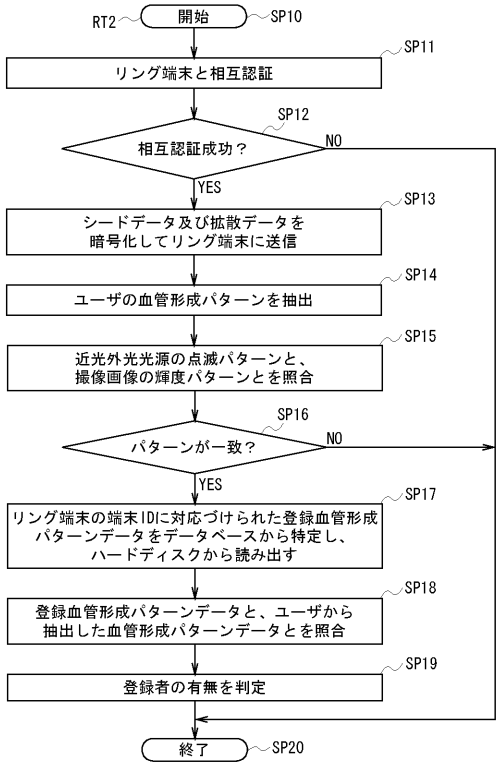

図１３　第２の認証処理手順

【図１４】

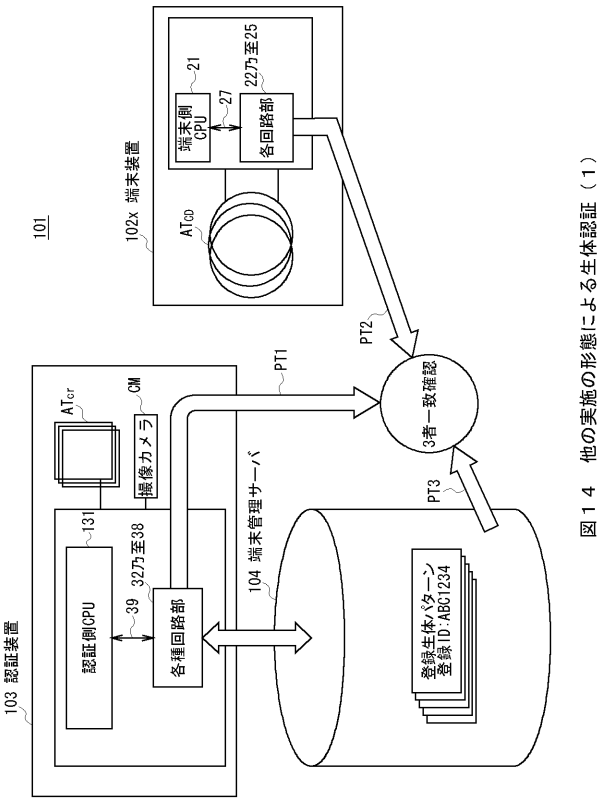

図１４　他の実施の形態による生体認証（１）

【図１５】

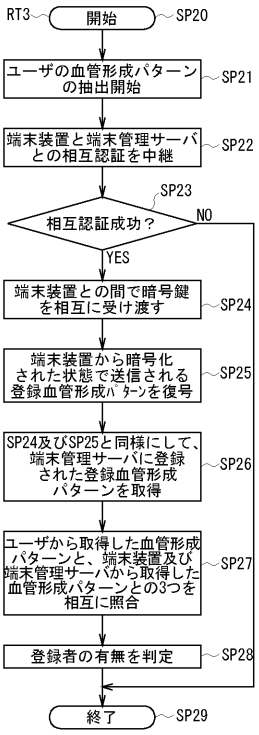

図１５　第３の認証処理手順

【図１６】

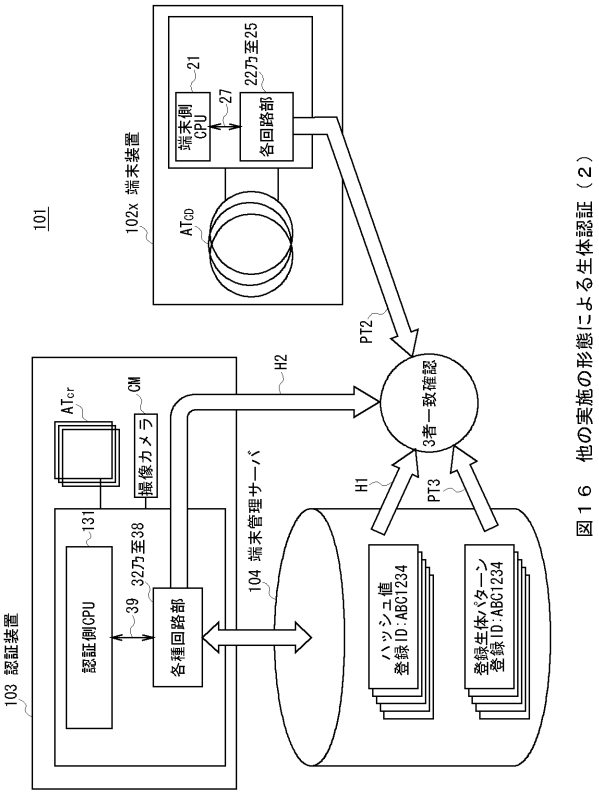

図１６　他の実施の形態による生体認証（２）

【図１７】

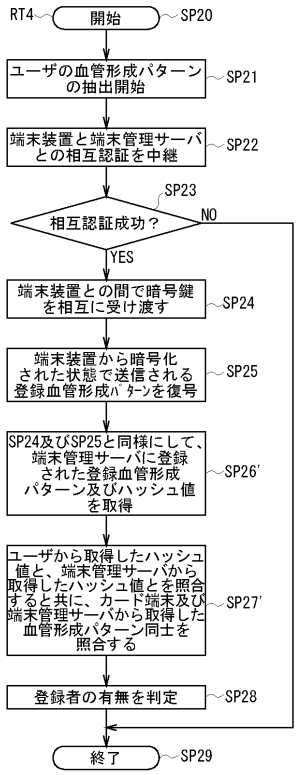

図１７　第４の認証処理手順

【図１８】

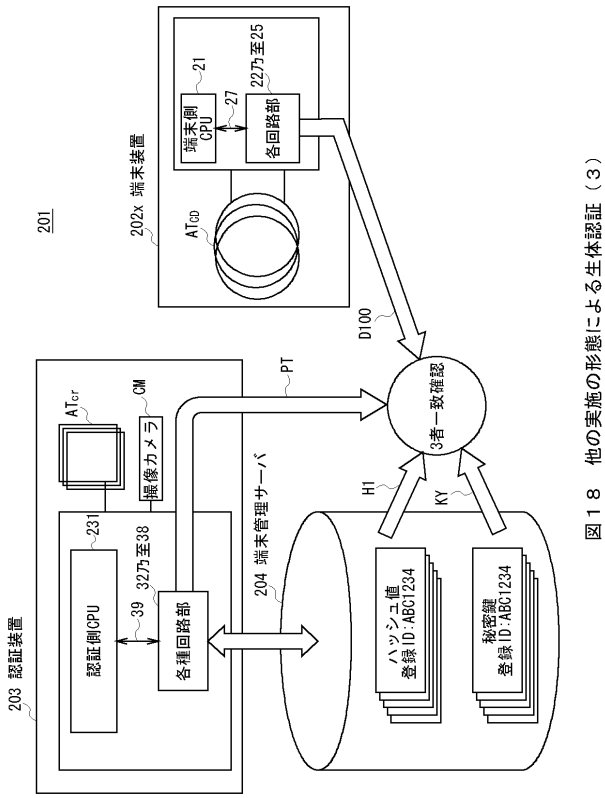

図１８　他の実施の形態による生体認証（３）

【図１９】

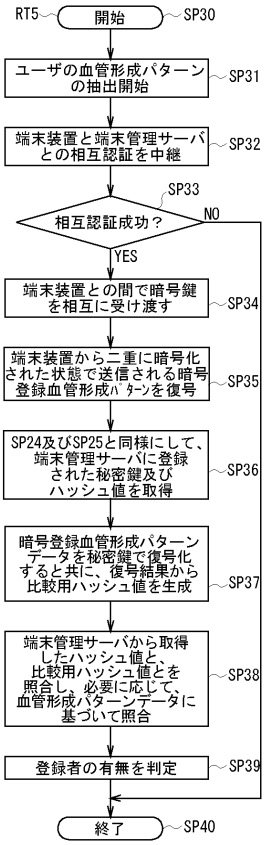

図１９　第５の認証処理手順

【図２０】

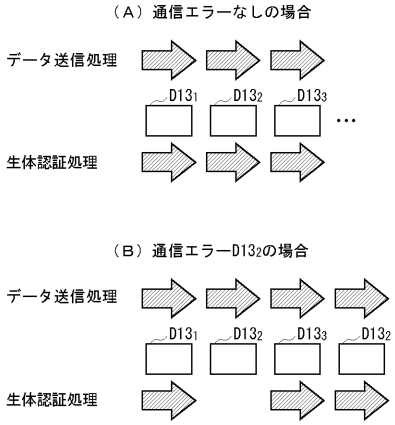

図２０　データ送信と、生体認証との関係

フロントページの続き

(51)Int.Cl.			FI			テーマコード（参考）
G06K 19/10	***(2006.01)***		G06F	15/00	330G	5B285
G06K 19/04	***(2006.01)***		G06K	19/00	H	
G06K 17/00	***(2006.01)***		G06K	19/00	S	
			G06K	19/04		
			G06K	17/00	F	
			G06K	17/00	V	

Fターム(参考) 5B047 AA23 AA25 BA02 BB04 BC05 BC07 BC11 BC12 BC16 CA17
CA19 CB22 DB01 DB03
5B058 CA15 KA01 KA38 KA40
5B285 AA01 BA02 CA41 CA42 CA47 CB06 CB08 CB12 CB15 CB16
CB23 CB44 CB62 CB64 CB74 CB76