(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2005-275661
(P2005-275661A)
(43)公開日　平成17年10月6日(2005.10.6)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330F	5B043
G06T 7/00	G06F 15/00	330E	5B085
	G06T 7/00	530	

審査請求 未請求　請求項の数 5　OL　（全 28 頁）

(21)出願番号　特願2004-86364(P2004-86364)
(22)出願日　平成16年3月24日(2004.3.24)

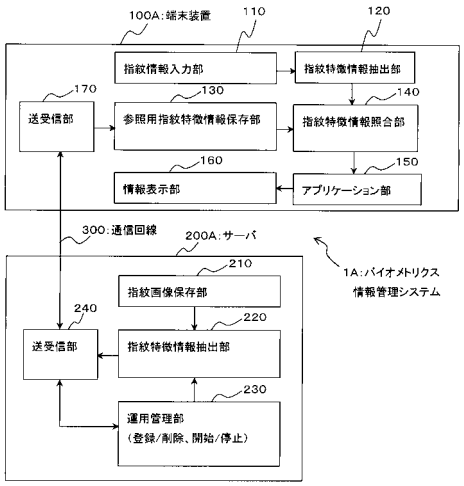
（出願人による申告）平成１５年度、総務省、「ユビキタスネットワーク制御・管理技術の研究開発」委託研究、産業再生法第３０条の適用を受ける特許出願

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100092978
弁理士　真田　有
(72)発明者　新崎　卓
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　仙波　聡史
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Fターム(参考)　5B043 AA04 AA09 BA02 CA10 DA04
FA02 FA03 FA08 GA02
5B085 AE08 AE23 AE25 AE26 BA06

(54)【発明の名称】バイオメトリクス情報管理システムおよびバイオメトリクス情報管理サーバ

(57)【要約】
【課題】端末装置の変更時や端末装置の利用者の変更時に利用者が出頭したり管理者等が立ち会ったりすることなく正規のバイオメトリクス特徴情報を端末装置に対して登録できるようにして、端末装置の利用者や管理者の利便性を大幅に向上させる。
【解決手段】サーバ２００Ａにおいて、保存部２１０に、端末装置１００Ａにおける個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報が予め保存され、端末装置１００Ａの変更時や端末装置１００Ａの利用者の変更時には、保存部２１０に保存されている登録用バイオメトリクス情報から、端末装置１００Ａにおける個人認証機能に応じた特徴情報が抽出され、その特徴情報が、通信手段２４０，３００，１７０を通じ、端末装置１００Ａにおける参照用特徴情報保存部１３０に保存・登録される。
【選択図】図１



【特許請求の範囲】
【請求項１】
バイオメトリクス情報による個人認証機能を有する端末装置と、
該端末装置の運用を管理するためのサーバと、
該端末装置と該サーバとの間で情報をやり取りすべく該端末装置と該サーバとの間を通信可能に接続しうる通信手段とをそなえ、
該端末装置が、
該端末装置のユーザが照合用バイオメトリクス情報を入力するための入力部と、
該入力部から入力された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、
前記ユーザの参照用特徴情報を予め保存する参照用特徴情報保存部と、
該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成され、
該サーバが、
該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、
該登録用バイオメトリクス情報保存部に保存されている前記登録用バイオメトリクス情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、
該特徴情報抽出部によって抽出された特徴情報を、該通信手段を通じて該端末装置に送信し、該端末装置における該参照用特徴情報保存部に、前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴とする、バイオメトリクス情報管理システム。
【請求項２】
バイオメトリクス情報による個人認証機能を有する端末装置と、
該端末装置の運用を管理するためのサーバと、
該端末装置と該サーバとの間で情報をやり取りすべく該端末装置と該サーバとの間を通信可能に接続しうる通信手段とをそなえ、
該端末装置が、
該端末装置のユーザが照合用バイオメトリクス情報を入力するための入力部と、
変換コードを予め保存する変換コード保存部と、
該入力部から入力された前記照合用バイオメトリクス情報に対し、該変換コード保存部に保存される前記変換コードを用いて所定の変換処理を施す照合用バイオメトリクス情報変換部と、
該照合用バイオメトリクス情報変換部によって変換された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、
前記ユーザの参照用特徴情報を予め保存する参照用特徴情報保存部と、
該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成され、
該サーバが、
該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、
該登録用バイオメトリクス情報保存部に保存されるべき前記登録用バイオメトリクス情報に対し、所定の変換コードを用いて所定の変換処理を施す登録用バイオメトリクス情報変換部と、
該登録用バイオメトリクス情報変換部によって変換された前記登録用バイオメトリクス情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、

前記所定の変換コードと前記該特徴情報抽出部によって抽出された特徴情報とを、該通信手段を通じて該端末装置に送信し、それぞれ、該端末装置における該変換コード保存部および該参照用特徴情報保存部に、前記変換コードおよび前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴とする、バイオメトリクス情報管理システム。

【請求項３】

該端末装置が、さらに、

該端末装置固有の端末識別情報を管理し、前記端末識別情報を、該通信手段を通じて該サーバに送信する端末識別情報管理部をそなえて構成され、

該サーバが、さらに、

端末識別情報と当該端末識別情報で特定される端末装置で用いられる特徴情報のデータ形式との対応関係を管理し、該端末装置から送信されてきた前記端末識別情報に対応するデータ形式に応じた特徴情報を前記個人認証機能に応じた特徴情報として抽出するように該特徴情報抽出部による抽出動作を管理する端末識別情報／データ形式対応管理部をそなえて構成されていることを特徴とする、請求項１記載のバイオメトリクス情報管理システム。

【請求項４】

照合用バイオメトリクス情報を入力するための入力部と、該入力部から入力された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、参照用特徴情報を予め保存する参照用特徴情報保存部と、該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成された、バイオメトリクス情報による個人認証機能を有する端末装置の運用を、通信手段を介して管理するためのサーバであって、

該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、

該登録用バイオメトリクス情報保存部に保存されている前記登録用バイオメトリクス情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、

該特徴情報抽出部によって抽出された特徴情報を、該通信手段を通じて該端末装置に送信し、該端末装置における該参照用特徴情報保存部に、前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴とする、バイオメトリクス情報管理サーバ。

【請求項５】

照合用バイオメトリクス情報を入力するための入力部と、変換コードを予め保存する変換コード保存部と、該入力部から入力された前記照合用バイオメトリクス情報に対し、該変換コード保存部に保存される前記変換コードを用いて所定の変換処理を施す照合用バイオメトリクス情報変換部と、該照合用バイオメトリクス情報変換部によって変換された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、参照用特徴情報を予め保存する参照用特徴情報保存部と、該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成された、バイオメトリクス情報による個人認証機能を有する端末装置の運用を、通信手段を介して管理するためのサーバであって、

該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、

該登録用バイオメトリクス情報保存部に保存されるべき前記登録用バイオメトリクス情報に対し、所定の変換コードを用いて所定の変換処理を施す登録用バイオメトリクス情報変換部と、

該登録用バイオメトリクス情報変換部によって変換された前記登録用バイオメトリクス

情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、

前記所定の変換コードと前記該特徴情報抽出部によって抽出された特徴情報とを、該通信手段を通じて該端末装置に送信し、それぞれ、該端末装置における該変換コード保存部および該参照用特徴情報保存部に、前記変換コードおよび前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴とする、バイオメトリクス情報管理サーバ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、例えば、企業等において、バイオメトリクス情報による個人認証機能を有する携帯電話等の端末装置を従業員に貸与して利用させるような場合に、上記端末装置の運用（より具体的には上記端末装置に登録されるバイオメトリクス情報）を管理するためのシステムおよびサーバに関する。

【背景技術】

【０００２】

近年、携帯電子情報端末〔例えばＰＤＡ（Ｐersonal Ｄigital Ａssistant）〕や携帯電話などの携帯型端末装置は、極めて多機能化している。その機能としては、従来の電子手帳や電話としての機能のみならず、有線や無線のネットワークを介して電子情報や画像情報を送受信する機能や、さらには、銀行決済機能，電子商取引機能，株取引機能などもそなえられ、その携帯型端末装置には大量の個人情報が保存されるようになっている。

【０００３】

これに伴い、上述のような携帯型端末におけるセキュリティ性能の向上の要求が極めて高くなっており、セキュリティを確保するために、従来、プッシュボタンやキーボード等から入力される暗証番号やパスワードによる個人認証（端末装置のユーザが予め登録されたユーザ本人であることの認証）や、ＩＤ（ＩＤentification）カードによる個人認証などが採用されている。しかし、暗証番号／パスワードやＩＤカードは盗用される危険性が高く、銀行決済機能，電子商取引機能，株取引機能等を持ち歩ける便利さに対してセキュリティ面の対応がおろそかになっている。このため、より信頼性の高い安全な個人認証を実現することが強く望まれている。

【０００４】

このような要望に応じ、近年、携帯電話等の携帯端末装置にも、より高い精度で個人の特定が可能な、バイオメトリクス情報（生体情報）による個人認証機能が搭載され始めている。バイオメトリクス情報による個人認証は、信頼性が高く、上述の要望に応えられるものと考えられる。特に、バイオメトリクス情報として指紋画像を用いた場合には利便性も高い（例えば下記特許文献１参照）。なお、バイオメトリクス情報としては、指紋画像以外に、虹彩パターン画像，顔画像，掌紋画像，血管パターン画像，網膜パターン画像，音声パターン画像，署名画像などを用いることができる。

【０００５】

ここで、図１８を参照しながら、バイオメトリクス情報（ここでは指紋画像）による個人認証機能を有する、一般的な端末装置の機能構成、特に個人認証機能に係る構成について説明する。図１８は、その構成を示すブロック図である。

図１８に示す端末装置１００は、指紋画像による個人認証機能を実現すべく、指紋情報入力部１１０，指紋特徴情報抽出部１２０，参照用指紋特徴情報保存部１３０，指紋特徴情報照合部１４０，アプリケーション部１５０および情報表示部１６０をそなえて構成されている。

【０００６】

指紋情報入力部（入力部）１１０は、端末装置１００のユーザが照合用バイオメトリクス情報としての照合用指紋画像を入力するためのものである。この指紋情報入力部１１０としては、例えば静電容量式指紋センサや光学式指紋センサが用いられ、この指紋センサ

により、ユーザ（被認証者）の指から指紋画像（指紋センサの採取面に接触しうる隆線と同採取面に接触しない谷線とから成る紋様の画像）が採取される。

【０００７】

指紋特徴情報抽出部（照合用特徴情報抽出部）１２０は、指紋情報入力部１１０から入力された照合用指紋画像から照合用指紋特徴情報を抽出するもので、具体的には、上述のごとく採取された指紋画像の前景である隆線像から、特徴点（分岐点や端点）の位置情報などを特徴情報として抽出するものである。

参照用指紋特徴情報保存部（参照用特徴情報保存部）１３０は、端末装置１００のユーザの参照用指紋特徴情報を予め保存するものである。

【０００８】

指紋特徴情報照合部（照合部）１４０は、指紋特徴情報抽出部１２０によって抽出された照合用指紋特徴情報と参照用指紋特徴情報保存部１３０に保存されている参照用指紋特徴情報とを比較・照合することにより、指紋画像を入力したユーザ（被認証者）が予め登録されている本人であるか否かの判定、つまり個人認証を行なうものである。

アプリケーション部１５０は、指紋特徴情報照合部１４０によって、指紋画像を入力したユーザ（被認証者）が予め登録されている本人であると判定された場合（本人であることが認証された場合）に起動され、各種アプリケーションプログラムを実行するものであり、情報表示部１６０は、アプリケーション部１５０の動作に伴い、ユーザの個人情報を含む各種情報を表示するものである。

【０００９】

上述のように構成された端末装置１００では、この端末装置１００を起動したり、この端末装置１００に保存された個人情報を表示したり、その個人情報を用いた各種アプリケーションプログラムを実行したりする際には、まず、ユーザが指紋情報入力部１１０から指紋画像を入力する。

そして、入力された指紋画像から、指紋特徴情報抽出部１２０により照合用指紋特徴情報（特徴点情報等）が抽出され、指紋特徴情報照合部１４０において、抽出された照合用指紋特徴情報と参照用指紋特徴情報保存部１３０に予め保存されている参照用指紋特徴情報とが比較・照合され、指紋画像を入力したユーザ（被認証者）が予め登録されている本人であるか否かの判定、つまり個人認証が実行される。

【００１０】

その個人認証の結果、指紋画像を入力したユーザ（被認証者）が予め登録されている本人であると判定されると、アプリケーション部１５０が起動され、各種アプリケーションプログラムが実行される。これに伴って、ユーザの個人情報を含む各種情報が情報表示部１６０において表示される。

ところで、企業等において、携帯電話やＰＤＡなどの携帯型端末装置を従業員に貸与して利用させる際、その端末装置は、複数の従業員によって共有利用されるか、もしくは、複数の従業員によって引き継がれながら利用される。その際、企業等から従業員に貸与される携帯型端末装置が、上述のような指紋画像（バイオメトリクス情報）による個人認証機能を有する端末装置１００である場合、その端末装置１００の利用者（従業員）が替わる都度、その端末装置１００の参照用指紋特徴情報保存部１３０に登録・保存されている参照用指紋特徴情報を書き換える登録作業を行なう必要がある。つまり、各端末装置１００についての登録者の管理、特に正規の利用者の登録を管理することが必須となる。

【００１１】

その際、通常、端末装置１００の参照用指紋特徴情報保存部１３０に参照用指紋特徴情報を登録すべき利用者（登録者）本人が、その登録を行なう部署（窓口等）に出頭し、スーパーユーザ等の管理者の立会いの下で、指紋画像を指紋センサから入力する。そして、指紋センサによって採取された指紋画像から、参照用指紋特徴情報が抽出され、その参照用指紋特徴情報が、端末装置の参照用指紋特徴情報保存部に登録されることになる。

【特許文献１】特開２００３－２７４００７号公報

【発明の開示】

【発明が解決しようとする課題】
【００１２】
上述のように、企業等において、バイオメトリクス情報による個人認証機能を有する携帯型端末装置を従業員に貸与して利用させる場合、各従業員の利用する携帯型端末装置を変更したり、携帯型端末装置の利用者を他の従業員に変更したりする際には、従業員は、一々、登録部署に出向き管理者の立会いの下で、上述のような登録処理を行なわなければならず、従業員にとっても管理者にとっても極めて面倒である。
【００１３】
また、その際、セキュリティ上、正規のユーザに対する登録許可の付与や、正規のユーザが登録を完了するまでの監視や、携帯型端末装置の利用停止時のデータ削除（参照用指紋特徴情報の削除）などの運用管理が必要である。
人事異動等の時期には、上述のような登録処理を速やかに行なう必要があり、利用者（従業員）の出頭や管理者の立会いを伴う従来の運用管理手法は現実的ではない。
【００１４】
このため、従業員が自分の指紋画像の登録処理を一度だけ行なっておけば、利用する携帯型端末装置の変更や携帯型端末装置の利用者の変更に際し、利用者が出頭したり管理者等が立ち会ったりすることなく、正規の指紋特徴情報（バイオメトリクス特徴情報）を携帯型端末装置に対して登録できるような仕組みの開発が望まれている。
さらに、現状では、携帯型端末装置に搭載されている照合アルゴリズム（上記指紋特徴情報照合部１４０での照合方式）は、機種毎に異なっているため、利用する携帯型端末装置を変更する際、その携帯型端末装置の機種も変わる場合には、その機種の照合アルゴリズムに対応したデータ形式のバイオメトリクス特徴情報（指紋特徴情報）を抽出するために、どうしても利用者が出頭し管理者立会いの下でバイオメトリクス情報の採取を行なわなければならない。このため、上述のような場合であっても、利用者が出頭したり管理者等が立ち会ったりすることなく、変更後の機種の照合アルゴリズムに対応したデータ形式のバイオメトリクス特徴情報を変更後の携帯型端末装置に登録できるようにすることも望まれている。
【００１５】
本発明は、このような課題に鑑み創案されたもので、端末装置の変更時や端末装置の利用者の変更時に利用者が出頭したり管理者等が立ち会ったりすることなく正規のバイオメトリクス特徴情報を端末装置に対して登録できるようにするとともに、端末装置の変更時にその端末装置の機種が変わる場合にも利用者が出頭したり管理者等が立ち会ったりすることなくその機種の照合アルゴリズムに対応したデータ形式のバイオメトリクス特徴情報を変更後の端末装置に登録できるようにして、端末装置の利用者や管理者の利便性を大幅に向上させることを目的としている。
【課題を解決するための手段】
【００１６】
上記目的を達成するために、本発明のバイオメトリクス情報管理システム（請求項１）は、バイオメトリクス情報による個人認証機能を有する端末装置と、該端末装置の運用を管理するためのサーバと、該端末装置と該サーバとの間で情報をやり取りすべく該端末装置と該サーバとの間を通信可能に接続しうる通信手段とをそなえ、該端末装置が、該端末装置のユーザが照合用バイオメトリクス情報を入力するための入力部と、該入力部から入力された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、前記ユーザの参照用特徴情報を予め保存する参照用特徴情報保存部と、該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成され、該サーバが、該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、該登録用バイオメトリクス情報保存部に保存されている前記登録用バイオメトリクス情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、該

特徴情報抽出部によって抽出された特徴情報を、該通信手段を通じて該端末装置に送信し、該端末装置における該参照用特徴情報保存部に、前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴としている。

【００１７】

このようなバイオメトリクス情報管理システムにおいて、該端末装置が、さらに、該端末装置固有の端末識別情報を管理し、前記端末識別情報を、該通信手段を通じて該サーバに送信する端末識別情報管理部をそなえて構成され、該サーバが、さらに、端末識別情報と当該端末識別情報で特定される端末装置で用いられる特徴情報のデータ形式との対応関係を管理し、該端末装置から送信されてきた前記端末識別情報に対応するデータ形式に応じた特徴情報を前記個人認証機能に応じた特徴情報として抽出するように該特徴情報抽出部による抽出動作を管理する端末識別情報／データ形式対応管理部をそなえて構成されていてもよい（請求項３）。

【００１８】

また、本発明のバイオメトリクス情報管理システム（請求項２）は、上述と同様の端末装置，サーバおよび通信手段をそなえ、該端末装置が、該端末装置のユーザが照合用バイオメトリクス情報を入力するための入力部と、変換コードを予め保存する変換コード保存部と、該入力部から入力された前記照合用バイオメトリクス情報に対し、該変換コード保存部に保存される前記変換コードを用いて所定の変換処理を施す照合用バイオメトリクス情報変換部と、該照合用バイオメトリクス情報変換部によって変換された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、前記ユーザの参照用特徴情報を予め保存する参照用特徴情報保存部と、該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成され、該サーバが、該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、該登録用バイオメトリクス情報保存部に保存されるべき前記登録用バイオメトリクス情報に対し、所定の変換コードを用いて所定の変換処理を施す登録用バイオメトリクス情報変換部と、該登録用バイオメトリクス情報変換部によって変換された前記登録用バイオメトリクス情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、前記所定の変換コードと前記該特徴情報抽出部によって抽出された特徴情報とを、該通信手段を通じて該端末装置に送信し、それぞれ、該端末装置における該変換コード保存部および該参照用特徴情報保存部に、前記変換コードおよび前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴としている。

【００１９】

一方、本発明のバイオメトリクス情報管理サーバ（請求項４）は、照合用バイオメトリクス情報を入力するための入力部と、該入力部から入力された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、参照用特徴情報を予め保存する参照用特徴情報保存部と、該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成された、バイオメトリクス情報による個人認証機能を有する端末装置の運用を、通信手段を介して管理するためのサーバであって、該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、該登録用バイオメトリクス情報保存部に保存されている前記登録用バイオメトリクス情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、該特徴情報抽出部によって抽出された特徴情報を、該通信手段を通じて該端末装置に送信し、該端末装置における該参照用特徴情報保存部に、前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴としている。

【００２０】

また、本発明のバイオメトリクス情報管理サーバ（請求項５）は、照合用バイオメトリ

クス情報を入力するための入力部と、変換コードを予め保存する変換コード保存部と、該入力部から入力された前記照合用バイオメトリクス情報に対し、該変換コード保存部に保存される前記変換コードを用いて所定の変換処理を施す照合用バイオメトリクス情報変換部と、該照合用バイオメトリクス情報変換部によって変換された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、参照用特徴情報を予め保存する参照用特徴情報保存部と、該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成された、バイオメトリクス情報による個人認証機能を有する端末装置の運用を、通信手段を介して管理するためのサーバであって、該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、該登録用バイオメトリクス情報保存部に保存されるべき前記登録用バイオメトリクス情報に対し、所定の変換コードを用いて所定の変換処理を施す登録用バイオメトリクス情報変換部と、該登録用バイオメトリクス情報変換部によって変換された前記登録用バイオメトリクス情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、前記所定の変換コードと前記該特徴情報抽出部によって抽出された特徴情報とを、該通信手段を通じて該端末装置に送信し、それぞれ、該端末装置における該変換コード保存部および該参照用特徴情報保存部に、前記変換コードおよび前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴としている。

【発明の効果】

【００２１】

上述した本発明では、端末装置の利用者（従業員等）は、管理者等の立会いの下で最初に１回だけ登録処理を行ない、自身のバイオメトリクス情報（生データ）を、バイオメトリクス情報管理サーバの登録用バイオメトリクス情報保存部に予め登録・保存しておく。そして、端末装置の変更時や端末装置の利用者の変更時には、バイオメトリクス情報管理サーバにおいて、登録用バイオメトリクス情報保存部に保存されている登録用バイオメトリクス情報から、端末装置における個人認証機能に応じた特徴情報が抽出され、その特徴情報が、通信手段を通じ、端末装置における参照用特徴情報保存部に、参照用特徴情報として保存・登録される。

【００２２】

これにより、端末装置の変更時や端末装置の利用者の変更時に、利用者が出頭したり管理者等が立ち会ったりすることなく、正規のバイオメトリクス特徴情報を端末装置に対して登録することができ、端末装置の利用者のみならず管理者の利便性が大幅に向上する。

また、端末装置の変更時にその端末装置の機種が変わる場合には、その機種の照合アルゴリズムに対応したデータ形式のバイオメトリクス特徴情報を抽出して変更後の端末装置の参照用特徴情報保存部に保存・登録することができるので、端末装置の利用者や管理者の利便性をより高めることができる。

【発明を実施するための最良の形態】

【００２３】

以下、図面を参照して本発明の実施の形態を説明する。

〔１〕第１実施形態の説明

図１は本発明の第１実施形態としてのバイオメトリクス情報管理システム（端末装置およびサーバ）の機能構成を示すブロック図で、この図１に示すように、第１実施形態のバイオメトリクス情報管理システム１Ａは、端末装置１００Ａ，サーバ２００Ａおよび通信回線３００をそなえて構成されている。

【００２４】

端末装置１００Ａは、バイオメトリクス情報（本実施形態では指紋画像）による個人認証機能を有するもので、具体的には携帯電話，ＰＤＡ等の携帯型端末装置である。

サーバ２００Ａは、端末装置１００Ａの運用（より具体的には、端末装置１００Ａに登録される、後述の参照用指紋特徴情報）を管理するバイオメトリクス情報管理サーバとし

て機能するもので、その機能は、実際には、後述するごとくパーソナルコンピュータ等で所定のアプリケーションプログラム（バイオメトリクス情報管理プログラム）を実行することにより実現される。

【００２５】

通信回線（通信手段）３００は、端末装置１００Ａとサーバ２００Ａとの間で情報をやり取りすべく端末装置１００Ａとサーバ２００Ａとの間を通信可能に接続するためのものである。端末装置１００Aが携帯電話であれば、通常の携帯電話回線を通信回線３００として用いることができる。また、端末装置１００AがＰＤＡ等であれば、通常の携帯電話回線のほか無線ＬＡＮ（Local Area Network）や有線の一般電話回線などを通信回線３００として用いることができる。さらに、端末装置１００Ａおよびサーバ２００Ａがいずれも赤外線通信機能をそなえている場合には、その赤外線通信機能を通信回線３００として用いることもできる。また、端末装置１００Ａとサーバ２００Ａとを通信可能に接続する専用のコネクタおよびケーブルがある場合には、これらのコネクタおよびケーブルを通信回線３００として用いることもできる。

【００２６】

そして、端末装置１００Ａは、指紋情報入力部（入力部）１１０，指紋特徴情報抽出部（照合用特徴情報抽出部）１２０，参照用指紋特徴情報保存部（参照用特徴情報保存部）１３０，指紋特徴情報照合部（照合部）１４０，アプリケーション部１５０，情報表示部１６０および送受信部（通信手段）１７０をそなえて構成されている。ここで、指紋情報入力部１１０，指紋特徴情報抽出部１２０，参照用指紋特徴情報保存部１３０，指紋特徴情報照合部１４０，アプリケーション部１５０および情報表示部１６０は、図１８を参照しながら上述した端末装置１００におけるものと同様のものであるので、その詳細な説明は省略する。送受信部１７０は、通信回線３００を通じて外部と情報（各種データ）のやり取りを行なうためのもので、携帯電話やＰＤＡなどに通常そなえられている基本的な通信機能である。本実施形態の端末装置１００Ａは、この送受信部１７０を用いて、サーバ２００Ａと情報のやり取りを行なうようになっている。

【００２７】

また、サーバ２００Ａは、指紋画像保存部（登録用バイオメトリクス情報保存部）２１０，指紋特徴情報抽出部（特徴情報抽出部）２２０，運用管理部２３０および送受信部（通信手段）２４０をそなえて構成されている。

ここで、指紋画像保存部２１０は、端末装置１００Ａにおける個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報そのもの、即ち本実施形態では登録用指紋画像そのもの（生データ）を予め保存するものである。本実施形態においては、端末装置１００Ａの利用者（従業員等）は、管理者等の立会いの下で最初に１回だけ、自身の指紋画像の登録処理を行ない、その指紋画像の生データをバイオメトリクス情報管理サーバ２００Ａの指紋画像保存部２１０に予め登録・保存しておく。

【００２８】

指紋特徴情報抽出部２２０は、指紋画像保存部２１０に保存されている指紋画像情報から、端末装置１００Ａにおける個人認証機能（照合アルゴリズム）に応じた指紋特徴情報（登録データ／参照用指紋特徴情報）を抽出するものである。

運用管理部２３０は、端末装置１００Ａに対する登録データ（参照用指紋特徴情報）の登録／削除等の管理を行なうもので、特に、登録時には、指紋特徴情報抽出部２２０によって抽出された指紋特徴情報を、送受信部２４０および通信回線３００を通じて端末装置１００Ａに送信し、この端末装置１００Ａにおける参照用特徴情報保存部１３０に、参照用指紋特徴情報（登録データ）として保存させるものである。

【００２９】

送受信部２４０は、通信回線３００を通じて外部と情報（各種データ）のやり取りを行なうためのもので、パーソナルコンピュータなどに一般的にそなえられている機能で、本実施形態のサーバ２００Ａは、この送受信部２４０を用いて、端末装置１００Ａと情報のやり取りを行なうようになっている。

次に、図２に示すフローチャート（ステップＳ１１～Ｓ１４）を参照しながら、上述のごとく構成されたシステム１Ａやサーバ２００Ａの動作について説明する。

【００３０】

サーバ２００Ａにおいて、端末装置１００Ａの利用者（従業員等）は、管理者等の立会いの下で最初に１回だけ自身の指紋画像の登録処理を行ない、その指紋画像の生データを指紋画像保存部２１０に予め登録・保存させる。つまり、サーバ２００Ａは、指紋センサ（図示省略）から入力される登録用指紋画像の生データを読み込み（ステップＳ１１）、指紋画像保存部２１０に予め登録・保存する（ステップＳ１２）。

【００３１】

サーバ２００Ａを用いて端末装置１００Ａの新たな利用者の参照用指紋特徴情報を端末装置１００Ａに登録する際には、まず、サーバ２００Ａにおいて、指紋画像保存部２１０に予め登録・保存されている、その利用者についての指紋画像が読み出され、読み出された指紋画像から、指紋特徴情報抽出部２２０によって、端末装置１００Ａにおける個人認証機能（照合アルゴリズム）に応じた指紋特徴情報（登録データ／参照用指紋特徴情報）が抽出される（ステップＳ１３）。この後、抽出された指紋特徴情報が、サーバ２００Ａから送受信部２４０および通信回線３００を通じて端末装置１００Ａに送信される（ステップＳ１４）。端末装置１００Ａにおいては、送受信部２４０で受信された指紋特徴情報が、参照用指紋特徴情報として参照用指紋特徴情報保存部１３０に登録・保存される。

【００３２】

そして、端末装置１００Ａを起動したり、端末装置１００Ａに保存された個人情報を表示したり、その個人情報を用いた各種アプリケーションプログラムを実行したりする際には、図１８に示した端末装置１００と同様、まず、利用者が指紋情報入力部１１０から指紋画像を入力し、入力された指紋画像から、指紋特徴情報抽出部１２０により照合用指紋特徴情報（特徴点情報等）が抽出される。

【００３３】

この後、指紋特徴情報照合部１４０において、抽出された照合用指紋特徴情報と、上述のごとくサーバ２００Ａから参照用指紋特徴情報保存部１３０に登録された参照指紋特徴情報とが比較・照合され、指紋画像を入力したユーザ（被認証者）が予め登録されている本人であるか否かの判定、つまり個人認証が実行される。その個人認証の結果、指紋画像を入力した利用者（被認証者）が予め登録されている本人であると判定されると、アプリケーション部１５０が起動され、各種アプリケーションプログラムが実行される。これに伴って、ユーザの個人情報を含む各種情報が情報表示部１６０において表示される。

【００３４】

このように、第１実施形態のバイオメトリクス情報管理システム１Ａやサーバ２００Ａによれば、端末装置１００Ａの利用者（従業員等）は、管理者等の立会いの下で最初に１回だけ登録処理を行なって自身の指紋画像（生データ）をサーバ２００Ａの指紋画像保存部２１０に予め登録・保存しておくだけで、端末装置１００Ａの変更時や端末装置１００Ａの利用者の変更時には、利用者が出頭したり管理者等が立ち会ったりすることなく、正規の指紋特徴情報を端末装置１００Ａに対して登録することができ、端末装置１００Ａの利用者のみならず管理者の利便性が大幅に向上する。

【００３５】

また、端末装置１００Ａの変更時にその端末装置１００Ａの機種が変わる場合には、その機種の照合アルゴリズムに対応したデータ形式の指紋特徴情報を抽出して変更後の端末装置１００Ａの参照用指紋特徴情報保存部１３０に保存・登録することができるので、端末装置１００Ａの利用者や管理者の利便性をより高めることができる。

さらに、バイオメトリクス情報である指紋画像をサーバ２００Ａ側で一括管理することにより、端末装置１００Aにおける参照用指紋特徴情報の登録／削除や、参照用指紋特徴情報（登録データ）の抽出・作成をサーバ２００A側で一括管理することができ、管理者の利便性を高めることができる。

【００３６】

〔２〕第２実施形態の説明

図３は本発明の第２実施形態としてのバイオメトリクス情報管理システム（端末装置およびサーバ）の機能構成を示すブロック図で、この図３に示すように、第２実施形態のバイオメトリクス情報管理システム１Ｂは、端末装置１００Ｂ，サーバ（バイオメトリクス情報管理サーバ）２００Ｂおよび通信回線３００をそなえて構成されている。なお、図３において既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

【００３７】

第２実施形態の端末装置１００Ｂには、図１に示した端末装置１００Ａの構成にさらにデータ形式管理部１８０が追加されている。このデータ形式管理部１８０は、指紋特徴情報照合部１４０で用いられる指紋特徴情報のデータ形式（つまりは照合アルゴリズム）を管理し、サーバ２００Ｂから保存部１３０に参照用指紋特徴情報を登録・保存する際に、そのデータ形式に関する情報を、送受信部１７０および通信回線３００を通じてサーバ２００Ｂに送信するものである。なお、このとき、そのデータ形式に関する情報とともに、端末装置１００Ｂに搭載されている指紋センサ（入力部）１１０の種別情報も併せてサーバ２００Ｂに送信してもよい。

【００３８】

また、第２実施形態のサーバ２００Ｂにおいては、第１実施形態のサーバ２００Ａと同様に構成されているが、この第２実施形態のサーバ２００Ｂにおいては、サーバ２００Ａの運用管理部２３０に代えて運用管理部２３１がそなえられるとともに、データ形式管理部２５０が追加されている。ここで、運用管理部２３１は、上述した第１実施形態の運用管理部２３０と同様の機能を果たすほか、第２実施形態では、送受信部２４０により端末装置１００Ｂからデータ形式に関する情報を受信すると、データ形式管理部２５０を以下のように動作させるものである。その際、データ形式管理部２５０は、端末装置１００Ｂから送信されてきたデータ形式に応じた指紋特徴情報（登録データ／参照用指紋特徴情報）を指紋特徴情報抽出部２２０によって抽出させるように、この指紋特徴情報抽出部２２０の抽出動作を管理する。

【００３９】

次に、図４に示すフローチャート（ステップＳ２１～Ｓ２５）を参照しながら、上述のごとく構成されたシステム１Ｂやサーバ２００Ｂの動作について説明する。

サーバ２００Ｂにおいても、第１実施形態のサーバ２００Ａと同様、端末装置１００Ｂの利用者は、管理者等の立会いの下で最初に１回だけ自身の指紋画像の登録処理を行ない、その指紋画像の生データを指紋画像保存部２１０に予め登録・保存させる（ステップＳ２１，Ｓ２２）。

【００４０】

サーバ２００Ｂを用いて端末装置１００Ｂの新たな利用者の参照用指紋特徴情報を端末装置１００Ｂに登録する際には、まず、データ形式管理部１８０で管理されているデータ形式に関する情報が、端末装置１００Ｂ側から送受信部１７０および通信回線３００を通じてサーバ２００Ｂに送信・通知されるとともに（ステップＳ２３）、サーバ２００Ｂにおいては、指紋画像保存部２１０に予め登録・保存されている、登録すべき利用者についての指紋画像が読み出される。

【００４１】

そして、読み出された指紋画像から、指紋特徴情報抽出部２２０によって、端末装置１００Ｂから通知されたデータ形式（つまり端末装置１００Ｂに搭載された照合アルゴリズム）に応じた指紋特徴情報（登録データ／参照用指紋特徴情報）が抽出される（ステップＳ２４）。この後、抽出された指紋特徴情報が、サーバ２００Ｂから送受信部２４０および通信回線３００を通じて端末装置１００Ｂに送信される（ステップＳ２５）。端末装置１００Ｂにおいては、送受信部２４０で受信された指紋特徴情報が、参照用指紋特徴情報として参照用指紋特徴情報保存部１３０に登録・保存される。なお、端末装置１００Ｂでの個人認証動作については、上述した端末装置１００Ａの動作と同様であるので、その説

明は省略する。

【００４２】

このように、第２実施形態のバイオメトリクス情報管理システム１Ｂやサーバ２００Ｂによれば、第１実施形態と同様の効果が得られるほか、この第２実施形態のシステム１Ｂでは、端末装置１００Ｂの個人認証機能で利用される指紋特徴情報のデータ形式が端末装置１００Ｂからサーバ２００Ｂに通知され、サーバ２００Ｂにおいて、通知されたデータ形式の指紋特徴情報、即ち端末装置１００Ｂにおける照合アルゴリズム向けの指紋特徴情報を抽出し、端末装置１００Ｂに登録することができる。従って、端末装置１００Ｂ毎に照合アルゴリズム（指紋特徴情報のデータ形式）が異なっている場合でも、各端末装置１００Ｂの照合アルゴリズム（指紋特徴情報のデータ形式）に応じた指紋特徴情報を間違うことなく確実に抽出して登録することができる。

【００４３】

〔３〕第３実施形態の説明

図５は本発明の第３実施形態としてのバイオメトリクス情報管理システム（端末装置およびサーバ）の機能構成を示すブロック図で、この図５に示すように、第３実施形態のバイオメトリクス情報管理システム１Ｃは、端末装置１００Ｃ，サーバ（バイオメトリクス情報管理サーバ）２００Ｃおよび通信回線３００をそなえて構成されている。なお、図５において既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

【００４４】

第３実施形態の端末装置１００Ｃには、図１に示した端末装置１００Ａの構成にさらに端末ＩＤ管理部（端末識別情報管理部）１８１が追加されている。この端末ＩＤ管理部１８１は、端末装置２００Ｃ固有の端末ＩＤ（端末識別情報；例えば端末装置２００Ｃ毎に登録されているシリアルナンバー）を管理し、サーバ２００Ｃから保存部１３０に参照用指紋特徴情報を登録・保存する際に、その端末ＩＤを、送受信部１７０および通信回線３００を通じてサーバ２００Ｃに送信するものである。

【００４５】

また、第３実施形態のサーバ２００Ｃにおいては、第１実施形態のサーバ２００Ａと同様に構成されているが、この第３実施形態のサーバ２００Ｃにおいては、サーバ２００Ａの運用管理部２３０に代えて運用管理部２３２がそなえられるとともに、端末ＩＤ／データ形式対応管理部（端末識別情報／データ形式対応管理部）２５１が追加されている。ここで、運用管理部２３２は、上述した第１実施形態の運用管理部２３０と同様の機能を果たすほか、第３実施形態では、送受信部２４０により端末装置１００Ｃから端末ＩＤを受信すると、端末ＩＤ／データ形式対応管理部２５１を以下のように動作させるものである。

【００４６】

この端末ＩＤ／データ形式対応管理部２５１は、端末ＩＤと各端末ＩＤで特定される端末装置１００Ｃで用いられる指紋特徴情報のデータ形式（つまりは照合アルゴリズム）とを対応付けるための参照テーブル（図７，図８参照）を有しており、この参照テーブルを用いて端末ＩＤとデータ形式との対応関係を管理している。そして、送受信部２４０により端末装置１００Ｃから端末ＩＤを受信すると、端末ＩＤ／データ形式対応管理部２５１は、その端末ＩＤで上記参照テーブルを検索し、その端末ＩＤに対応付けられたデータ形式を読み出し、読み出されたデータ形式に応じた指紋特徴情報（登録データ／参照用指紋特徴情報）を指紋特徴情報抽出部２２０によって抽出させるように、この指紋特徴情報抽出部２２０の抽出動作を管理する。

【００４７】

次に、図６に示すフローチャート（ステップＳ３１～Ｓ３６）を参照しながら、上述のごとく構成されたシステム１Ｃやサーバ２００Ｃの動作について説明する。

サーバ２００Ｃにおいても、第１実施形態のサーバ２００Ａと同様、端末装置１００Ｃの利用者は、管理者等の立会いの下で最初に１回だけ自身の指紋画像の登録処理を行ない

、その指紋画像の生データを指紋画像保存部２１０に予め登録・保存させる（ステップＳ３１，Ｓ３２）。

【００４８】

サーバ２００Ｃを用いて端末装置１００Ｃの新たな利用者の参照用指紋特徴情報を端末装置１００Ｃに登録する際には、まず、端末ＩＤ管理部１８１で管理されている端末ＩＤが、端末装置１００Ｃ側から送受信部１７０および通信回線３００を通じてサーバ２００Ｃに送信・通知される（ステップＳ３３）。

サーバ２００Ｃにおいては、送受信部２４０により端末装置１００Ｃから端末ＩＤを受信すると、端末ＩＤ／データ形式対応管理部２５１により、その端末ＩＤで上記参照テーブルが検索され、その端末ＩＤに対応付けられたデータ形式が読み出されるとともに（ステップＳ３４）、指紋画像保存部２１０に予め登録・保存されている、登録すべき利用者についての登録用指紋画像が読み出される。そして、読み出された登録用指紋画像から、指紋特徴情報抽出部２２０によって、参照テーブルから読み出されたデータ形式（つまり端末装置１００Ｃに搭載された照合アルゴリズム）に応じた指紋特徴情報（登録データ／参照用指紋特徴情報）が抽出される（ステップＳ３５）。

【００４９】

この後、抽出された指紋特徴情報が、サーバ２００Ｃから送受信部２４０および通信回線３００を通じて端末装置１００Ｃに送信される（ステップＳ３６）。端末装置１００Ｃにおいては、送受信部２４０で受信された指紋特徴情報が、参照用指紋特徴情報として参照用指紋特徴情報保存部１３０に登録・保存される。なお、端末装置１００Ｃでの個人認証動作については、上述した端末装置１００Ａの動作と同様であるので、その説明は省略する。

【００５０】

ここで、図７および図８に、第３実施形態の端末ＩＤ／データ形式対応管理部２５１にそなえられる上記参照テーブルの一例および他例をそれぞれ示す。図７に示す参照テーブルでは、端末ＩＤ（000001,000002,000003,000004,000005）と、各端末ＩＤによって特定される端末装置１００Ｃで採用されているバイオメトリクス方式および照合ソフトウェア形式（つまり照合アルゴリズム／バイオメトリクス特徴情報のデータ形式）とが対応付けられている。また、図８に示す参照テーブルでは、端末ＩＤ（000001,000002,000003,000004,000005）と、各端末ＩＤによって特定される端末装置１００Ｃで採用されているバイオメトリクス方式およびバイオメトリクス情報のデータ形式とが対応付けられるとともに、さらに、各端末装置１００Ｃに搭載されている指紋センサ（入力部）１１０の種別情報が対応付けられている。なお、図７および図８では、本システム１Ｃにおいて、バイオメトリクス情報として指紋画像，顔画像、虹彩画像のいずれかを用いる端末装置１００Ｃが混在して利用される場合の参照テーブル例が示されている。このため、図７および図８に示す参照テーブルでは、バイオメトリクス方式として指紋，顔，虹彩といった情報が登録されている。

【００５１】

このように、第３実施形態のバイオメトリクス情報管理システム１Ｃやサーバ２００Ｃによれば、第１実施形態と同様の効果が得られるほか、この第３実施形態のシステム１Ｃでは、端末装置１００Ｃの端末ＩＤが端末装置１００Ｃからサーバ２００Ｃに通知され、サーバ２００Ｃにおいて、通知された端末ＩＤに対応付けられたデータ形式の指紋特徴情報、即ち端末装置１００Ｃにおける照合アルゴリズム向けの指紋特徴情報を抽出し、端末装置１００Ｃに登録することができる。従って、第２実施携帯と同様、端末装置１００Ｃ毎に照合アルゴリズム（指紋特徴情報のデータ形式）が異なっている場合でも、各端末装置１００Ｃの照合アルゴリズム（指紋特徴情報のデータ形式）に応じた指紋特徴情報を間違うことなく確実に抽出して登録することができる。

【００５２】

〔４〕第４実施形態の説明

図９は本発明の第４実施形態としてのバイオメトリクス情報管理システム（端末装置お

よびサーバ）の機能構成を示すブロック図で、この図９に示すように、第４実施形態のバイオメトリクス情報管理システム１Ｄは、端末装置１００Ｄ，サーバ（バイオメトリクス情報管理サーバ）２００Ｄおよび通信回線３００をそなえて構成されている。なお、図９において既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

【００５３】

第４実施形態の端末装置１００Ｄは、図５に示した端末装置１００Ｃと同様に構成されるとともに、この第４実施形態では、通信回線３００および送受信部１７０を通じてサーバ２００Ｄにより遠隔制御される被遠隔制御機能を有している。

また、第４実施形態のサーバ２００Ｄは、第３実施形態のサーバ２００Ｃと同様に構成されているが、この第４実施形態のサーバ２００Ｄにおいては、サーバ２００Ｃの運用管理部２３２に代えて運用管理部２３３がそなえられるとともに、送受信部２４０および通信回線３００を通じて端末装置１００Ｄを遠隔制御する遠隔制御機能がそなえられている。この遠隔制御機能により、サーバ２００Ｄの運用管理部２３３は、端末装置１００Ｄにおける参照用指紋特徴情報（登録データ）の登録／削除、および、端末装置１００Ｄの利用開始／利用停止を遠隔制御することができるようになっている。

【００５４】

次に、図１０～図１３に示すフローチャートを参照しながら、上述のごとく構成されたシステム１Ｄの遠隔制御動作について説明する。

図１０はシステム１Ｄの特徴情報登録時における遠隔制御動作を説明するためのフローチャート（ステップＳ４１～Ｓ４７）で、遠隔制御によって参照用指紋特徴情報の登録を行なう際には、図１０に示すように、まず、サーバ２００Ｄと端末装置１００Ｄとの間で相互認証を行なう（ステップＳ４１）。その相互認証の方法としては、公開鍵方式に基づく相互認証，秘密情報による相互認証，ＩＤ（識別情報）による装置認証などが挙げられる。なお、相互認証に失敗した場合には、サーバ２００Ｄにおいてエラー通知が行なわれる。

【００５５】

相互認証完了後、サーバ２００Ｄから登録対象の端末装置１００Ｄに通信回線３００を通じて登録コマンドが発行され（ステップＳ４２）、この登録コマンドを受けた端末装置１００Ｄ側からは、端末ＩＤ管理部１８１で管理されている端末ＩＤが、送受信部１７０および通信回線３００を通じてサーバ２００Ｄに送信・通知される（ステップＳ４３）。

これ以降は、第３実施形態と同様、サーバ２００Ｄにおいて、端末ＩＤ／データ形式対応管理部２５１により、端末装置１００Ｄから通知された端末ＩＤで上記参照テーブルが検索され、その端末ＩＤに対応付けられたデータ形式が読み出されるとともに（ステップＳ４４）、指紋画像保存部２１０に予め登録・保存されている、登録すべき利用者についての指紋画像が読み出される。そして、読み出された指紋画像から、指紋特徴情報抽出部２２０によって、参照テーブルから読み出されたデータ形式（つまり端末装置１００Ｄに搭載された照合アルゴリズム）に応じた指紋特徴情報（登録データ／参照用指紋特徴情報）が抽出される（ステップＳ４５）。

【００５６】

この後、抽出された指紋特徴情報が、サーバ２００Ｄから送受信部２４０および通信回線３００を通じて端末装置１００Ｄに送信される（ステップＳ４６）。端末装置１００Ｄにおいては、送受信部２４０で受信された指紋特徴情報が、参照用指紋特徴情報として参照用指紋特徴情報保存部１３０に登録・保存される（ステップＳ４７）。なお、端末装置１００Ｄでの個人認証動作については、上述した端末装置１００Ａの動作と同様であるので、その説明は省略する。

【００５７】

図１１はシステム１Ｄの特徴情報削除時における遠隔制御動作を説明するためのフローチャート（ステップＳ５１～Ｓ５３）で、遠隔制御によって参照用指紋特徴情報の削除を行なう際には、図１１に示すように、まず、登録時と同様、サーバ２００Ｄと端末装置１

００Ｄとの間で相互認証を行なってから（ステップＳ５１）、サーバ２００Ｄから登録対象の端末装置１００Ｄに通信回線３００を通じて削除要求コマンドが発行され（ステップＳ５２）、この削除要求コマンドを受けた端末装置１００Ｄにおいて、参照用指紋特徴情報保存部１３０に登録・保存されている参照用指紋特徴情報が削除される（ステップＳ５３）。

【００５８】

図１２はシステム１Ｄの利用開始時における遠隔制御動作を説明するためのフローチャート（ステップＳ６１～Ｓ６３）で、遠隔制御によって端末装置１００Ｄの利用を開始させる際には、図１２に示すように、まず、登録時と同様、サーバ２００Ｄと端末装置１００Ｄとの間で相互認証を行なってから（ステップＳ６１）、サーバ２００Ｄから登録対象の端末装置１００Ｄに通信回線３００を通じて利用開始コマンドが発行され（ステップＳ６２）、この利用開始コマンドを受けた端末装置１００Ｄにおいて、参照用指紋特徴情報保存部１３０に登録・保存されている参照用指紋特徴情報を利用可能（つまり個人認証可能）な状態に切換・設定される（ステップＳ６３）。

【００５９】

図１３はシステム１Ｄの利用停止時における遠隔制御動作を説明するためのフローチャート（ステップＳ７１～Ｓ７３）で、遠隔制御によって端末装置１００Ｄの利用を停止させる際には、図１３に示すように、まず、登録時と同様、サーバ２００Ｄと端末装置１００Ｄとの間で相互認証を行なってから（ステップＳ７１）、サーバ２００Ｄから登録対象の端末装置１００Ｄに通信回線３００を通じて利用停止コマンドが発行され（ステップＳ７２）、この利用停止コマンドを受けた端末装置１００Ｄにおいて、参照用指紋特徴情報保存部１３０に登録・保存されている参照用指紋特徴情報を利用不可（つまり個人認証不可）な状態に切換・設定される（ステップＳ７３）。

【００６０】

このように、第４実施形態のバイオメトリクス情報管理システム１Ｄやサーバ２００Ｄによれば、第１～第３実施形態と同様の効果が得られるほか、この第４実施形態のシステム１Ｄでは、サーバ２００Ｄ側から、端末装置１００Ｄにおける参照用指紋特徴情報（登録データ）の登録／削除、および、端末装置１００Ｄの利用開始／利用停止を遠隔制御することができるので、各端末装置１００Ｄで利用者が指紋特徴情報を登録する必要が全くなくなり、システム運用の管理コストを大幅に削減できるほか、不正登録の可能性が確実に排除され信頼性を高めることができる。

【００６１】

〔５〕第５実施形態の説明

図１４は本発明の第５実施形態としてのバイオメトリクス情報管理システム（端末装置およびサーバ）の機能構成を示すブロック図で、この図１４に示すように、第５実施形態のバイオメトリクス情報管理システム１Ｅは、端末装置１００Ｅ，サーバ（バイオメトリクス情報管理サーバ）２００Ｅおよび通信回線３００をそなえて構成されている。なお、図１４において既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

【００６２】

第５実施形態の端末装置１００Ｅには、第４実施形態の端末装置１００Ｄと同様、通信回線３００および送受信部１７０を通じてサーバ２００Ｅにより遠隔制御される被遠隔制御機能がそなえられるほか、図９に示した端末装置１００Ｄの構成に、さらに変換コード保存部１１１および指紋画像変換部（照合用バイオメトリクス情報変換部）１１２が追加されている。

【００６３】

ここで、変換コード保存部１１１は、所定の変換コードを予め保存するもので、この変換コードは、利用者あるいは管理者によって端末装置１００Ｅ毎に設定される。指紋画像変換部１１２は、指紋情報入力部１１０から入力された照合用指紋画像に対し、変換コード保存部１１１に保存される変換コードを用いて所定の変換処理（指紋画像を歪ませる変

形処理）を施すものである。指紋画像（バイオメトリクス画像）の変形処理とは、所定の関数により指紋画像を変形させる処理のことで、変換コードとは、その関数のパラメータに関するコードである。

【００６４】

この第５実施形態の端末装置１００Ｅにおいて、指紋特徴情報抽出部１２０は、指紋画像変換部１１２によって変換された照合用指紋画像から照合用指紋特徴情報を抽出するようになっている。また、参照用指紋特徴情報保存部１３０には、後述するごとく、端末装置１００Ｅのユーザの参照用指紋特徴情報として、同じ変換コードによって上記変換処理を施された指紋画像から抽出されたものが、サーバ２００Ｅから予め登録・保存されている。そして、指紋特徴情報照合部１４０では、変形処理済み指紋画像から指紋特徴情報抽出部１２０によって抽出された照合用指紋特徴情報と、参照用指紋特徴情報保存部１３０に保存されている参照用指紋特徴情報（サーバ２００Ｅ側で変形処理済み指紋画像から抽出されたもの）とを比較・照合することにより、指紋画像を入力したユーザ（被認証者）が予め登録されている本人であるか否かの判定、つまり個人認証が行なわれるようになっている。

【００６５】

また、第５実施形態のサーバ２００Ｅは、第４実施形態のサーバ２００Ｄと同様に構成され、送受信部２４０および通信回線３００を通じて端末装置１００Ｅを遠隔制御する遠隔制御機能を有しているほか、この第５実施形態のサーバ２００Ｅにおいては、サーバ２００Ｄの運用管理部２３３に代えて運用管理部２３４がそなえられるとともに、指紋画像変換部（登録用バイオメトリクス情報変換部）２１１および端末ＩＤ／データ形式／変換コード対応管理部（端末識別情報／データ形式／変換コード対応管理部）２５２が追加されている。

【００６６】

ここで、運用管理部２３４は、端末装置１００Ｅに対する登録データ（参照用指紋特徴情報）や変換コードの登録／削除等の管理を行なうもので、特に、登録時には、後述するごとく指紋画像に対する変換処理に用いられた変換コードと、後述するごとく指紋特徴情報抽出部２２０によって抽出された指紋特徴情報（登録データ）とを、送受信部２４０および通信回線３００を通じて端末装置１００Ｅに送信し、この端末装置１００Ｅにおける変換コード保存部１１１および参照用特徴情報保存部１３０に、それぞれ保存させるものである。また、運用管理部２３４は、送受信部２４０により端末装置１００Ｅから端末ＩＤを受信すると、端末ＩＤ／データ形式／変換コード対応管理部２５２を以下のように動作させる。

【００６７】

この端末ＩＤ／データ形式／変換コード対応管理部２５２は、端末ＩＤと、各端末ＩＤで特定される端末装置２００Ｃで用いられる指紋特徴情報のデータ形式（つまりは照合アルゴリズム）および変換コードとを対応付けるための参照テーブル（図１６参照）を有しており、この参照テーブルを用いて端末ＩＤとデータ形式および変換コードとの対応関係を管理している。そして、送受信部２４０により端末装置１００Ｅから端末ＩＤを受信すると、端末ＩＤ／データ形式／変換コード対応管理部２５２は、その端末ＩＤで上記参照テーブルを検索し、その端末ＩＤに対応付けられたデータ形式を読み出し、読み出されたデータ形式に応じた指紋特徴情報（登録データ／参照用指紋特徴情報）を指紋特徴情報抽出部２２０によって抽出させるように、この指紋特徴情報抽出部２２０の抽出動作を管理する。なお、端末ＩＤ／データ形式／変換コード対応管理部２５２は、参照用指紋特徴情報および変換コードの登録時に、上記参照テーブル（図１６参照）において、変換コード（登録ユーザ）と、その変換コードを登録した端末装置１００Ｅの端末ＩＤとを対応付けることにより、変換コードと端末ＩＤとの対応関係を管理している。

【００６８】

また、指紋画像変換部２１１は、指紋画像保存部２１０に保存されるべき登録用指紋画像に対し、所定の変換コードを用いて所定の変換処理を施すもので、第５実施形態の指紋

画像保存部２１０には、この指紋画像変換部２１１によって予め変換処理を施された登録用指紋画像（変形処理済み指紋画像）が、その変換処理に用いられた変換コードと対応させて保存されるようになっている。

【００６９】

そして、サーバ２００Ｅにおいて、指紋特徴情報抽出部２２０は、指紋画像保存部２１０に保存されている変形処理済み指紋画像から、端末装置１００Ｅにおける個人認証機能（照合アルゴリズム）に応じた指紋特徴情報（登録データ／参照用指紋特徴情報）を抽出することになる。

また、第５実施形態のサーバ２００Ｅにそなえられた上記遠隔制御機能により、サーバ２００Ｅの運用管理部２３４は、端末装置１００Ｅにおける参照用指紋特徴情報（登録データ）や変換コードの登録／削除、および、端末装置１００Ｅの利用開始／利用停止を遠隔制御することができるようになっている。

【００７０】

次に、図１５に示すフローチャート（ステップＳ８１～Ｓ８７）を参照しながら、上述のごとく構成されたシステム１Ｅやサーバ２００Ｅの動作について説明する。

サーバ２００Ｅにおいて、端末装置１００Ｅの利用者（従業員等）は管理者等の立会いの下で最初に１回だけ自身の指紋画像の読込処理を行なうとともに、変換コードの読込処理が行なわれる（ステップＳ８１）。そして、読み込まれた指紋画像の生データは、指紋画像変換部２１１により、同時に読み込まれた変換コードを用いて変換処理（変形処理）を施され、変換後の指紋画像（変形処理済み指紋画像）が登録用指紋画像として指紋画像保存部２１０に保存されるとともに、変換コードもその指紋画像に対応付けられて保存される（ステップＳ８２）。

【００７１】

サーバ２００Ｅを用いて端末装置１００Ｅの新たな利用者の参照用指紋特徴情報を端末装置１００Ｅに登録する際には、まず、端末ＩＤ管理部１８１で管理されている端末ＩＤが、端末装置１００Ｅ側から送受信部１７０および通信回線３００を通じてサーバ２００Ｅに送信・通知される（ステップＳ８３）。

サーバ２００Ｅにおいては、送受信部２４０により端末装置１００Ｅから端末ＩＤを受信すると、端末ＩＤ／データ形式／変換コード対応管理部２５２により、その端末ＩＤで上記参照テーブルが検索され、その端末ＩＤに対応付けられたデータ形式が読み出されるとともに（ステップＳ８４）、指紋画像保存部２１０に予め登録・保存されている、登録すべき利用者についての登録用指紋画像（変形処理済み指紋画像）が読み出される。そして、読み出された変形処理済み指紋画像から、指紋特徴情報抽出部２２０によって、参照テーブルから読み出されたデータ形式（つまり端末装置１００Ｅに搭載された照合アルゴリズム）に応じた指紋特徴情報（登録データ／参照用指紋特徴情報）が抽出される（ステップＳ８５）。

【００７２】

そして、上述のように抽出された指紋特徴情報と、その指紋特徴情報の抽出元である登録用指紋画像の変形処理に用いられた変換コードとが、サーバ２００Ｅから送受信部２４０および通信回線３００を通じて端末装置１００Ｅに送信される（ステップＳ８６）。端末装置１００Ｅにおいては、送受信部２４０で受信された指紋特徴情報が、参照用指紋特徴情報として参照用指紋特徴情報保存部１３０に登録・保存されるとともに、送受信部２４０で受信された変換コードが変換コード保存部１１１に登録・保存される（ステップＳ８７）。

【００７３】

ここで、図１６に、第５実施形態の端末ＩＤ／データ形式／変換コード対応管理部２５２にそなえられる上記参照テーブルの一例を示す。図１６に示す参照テーブルでは、端末ＩＤ（000001,000002,000003,000004,000005）と、各端末ＩＤによって特定される端末装置１００Ｅで採用されているバイオメトリクス方式および照合ソフトウェア形式（つまり照合アルゴリズム／バイオメトリクス特徴情報のデータ形式）とが対応付けられるとも

に、さらに、各端末装置１００Ｅに登録された変換コード、および、その端末装置１００Ｅの利用者についての登録ユーザ番号が対応付けられている。なお、図１６では、図７，図８に示した参照テーブルと同様、バイオメトリクス情報として指紋画像，顔画像、虹彩画像のいずれかを用いる端末装置１００Ｅが混在して利用されるシステム１Ｅに適用された参照テーブル例が示されている。このため、図１６に示す参照テーブルでは、バイオメトリクス方式として指紋，顔，虹彩といった情報が登録されている。また、図１６に示す参照テーブルでは、端末ＩＤ000001によって特定される端末装置１００Ｅには、複数の利用者（ユーザ）がそれぞれ異なる変換コードで登録されている例が示されている。

【００７４】

次に、図１７に示すフローチャート（ステップＳ９１～Ｓ９５）を参照しながら、端末装置１００Ｅにおける照合動作について説明する。

端末装置１００Ｅを起動したり、端末装置１００Ｅに保存された個人情報を表示したり、その個人情報を用いた各種アプリケーションプログラムを実行したりする際には、端末装置１００Ｅにおいて、まず、利用者が指紋情報入力部１１０から入力した照合用指紋画像を読み込む（ステップＳ９１）。そして、読み込まれた照合用指紋画像に対し、指紋画像変換部１１２により、変換コード保存部１１１に登録されている変換コードを用いて所定の変換処理（変形処理）が施され（ステップＳ９２）、その変形処理された照合用指紋画像から、指紋特徴情報抽出部１２０により照合用指紋特徴情報が抽出される（ステップＳ９３）。

【００７５】

この後、指紋特徴情報照合部１４０において、抽出された照合用指紋特徴情報と、上述のごとくサーバ２００Ｅから参照用指紋特徴情報保存部１３０に登録された参照指紋特徴情報とが比較・照合され（ステップＳ９４）、指紋画像を入力したユーザ（被認証者）が予め登録されている本人であるか否かの判定、つまり個人認証が実行される。ステップＳ９４での比較・照合の結果において所定量以上の一致が見られれば、指紋画像を入力した利用者（被認証者）が予め登録されている本人であると判定され（ステップＳ９５）、アプリケーション部１５０が起動され、各種アプリケーションプログラムが実行される。これに伴って、ユーザの個人情報を含む各種情報が情報表示部１６０において表示される。

【００７６】

このように、第５実施形態のバイオメトリクス情報管理システム１Ｅやサーバ２００Ｅによれば、第１～第４実施形態と同様の効果が得られるほか、この第５実施形態のシステム１Ｅでは、サーバ２００Ｅ側の指紋画像保存部２１０において、利用者の指紋画像が、生データではなく変換コードで所定の変換を施された状態で、つまり変形処理済み指紋画像として保存されるので、万一、指紋画像保存部２１０における指紋画像が漏洩するようなことがあってもその指紋画像を悪用することができず、個人のプライバシーを確実に保護することができる。

【００７７】

また、このとき、端末装置１００Ｅ側では、参照用指紋特徴情報を登録する際に、参照用指紋特徴情報の抽出元である指紋画像に対する変換処理時に用いられた変換コードも変換コード保存部１１１に登録されている。従って、端末装置１００Ｅで個人認証を行なう際には、指紋画像変換部１１２により、変換コード保存部１１１に登録された変換コードを用いて、指紋情報入力部１１０からの照合用指紋画像に対し所定の変換処理を施してから、照合用指紋特徴情報が抽出されるので、問題なく個人認証を行なうことが可能になっている。

【００７８】

なお、第５実施形態では、サーバ２００Ｅにおいて、指紋画像の生データが変換コードを用いて変換処理を施されているが、このサーバ２００Ｅとは別の専用サーバ等において変換コードによる変換処理を行なってから、変換後の指紋画像（変形処理済み指紋画像）を変換コードと対応付けて指紋画像保存部２１０に保存してもよい。

〔６〕その他

なお、本発明は上述した実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々変形して実施することができる。

【００７９】

例えば、上述した実施形態では、バイオメトリクス情報が指紋画像である場合について説明したが、本発明は、これに限定されるものではなく、バイオメトリクス情報としては、指紋画像以外に、虹彩パターン画像，顔画像，掌紋画像，血管パターン画像，網膜パターン画像，音声パターン画像，署名画像などを用いてもよいし、２種類以上のバイオメトリクス情報を組み合わせて用いてもよい。

【００８０】

また、上述した実施形態では、端末装置１００Ａ，１００Ｂ，１００Ｃ，１００Ｄ，１００Ｅが携帯電話，ＰＤＡ等の携帯型端末装置である場合について説明したが、本発明は、これに限定されるものでなく、その他の各種携帯電子情報端末（ノート型パソコン等）や携帯型端末装置のほか、パーソナルコンピュータ等の固定端末装置にも上述と同様に適用され上記実施形態と同様の作用効果を得ることができる。

【００８１】

さらに、上述した実施形態におけるサーバ２００Ａ，２００Ｂ，２００Ｃ，２００Ｄ，２００Ｅは、例えばパーソナルコンピュータ等で所定のアプリケーションプログラム（バイオメトリクス情報管理プログラム）を実行することによって実現される。つまり、上述した指紋画像保存部２１０は、パーソナルコンピュータにおけるハードディスク等によって実現され、上述した指紋画像変換部２１１，指紋特徴情報抽出部２２０，運用管理部２３０～２３４，データ形式管理部２５０，端末ＩＤ／データ形式対応管理部２５１および端末ＩＤ／データ形式／変換コード対応管理部２５２としての機能（各部の全部もしくは一部の機能）は、コンピュータ（ＣＰＵ，情報処理装置，各種端末を含む）が所定のアプリケーションプログラム（バイオメトリクス情報管理プログラム）を実行することによって実現される。

【００８２】

そのプログラムは、例えばフレキシブルディスク，ＣＤ－ＲＯＭ，ＣＤ－Ｒ，ＣＤ－ＲＷ，ＤＶＤ等のコンピュータ読取可能な記録媒体に記録された形態で提供される。この場合、コンピュータはその記録媒体からバイオメトリクス情報管理プログラムを読み取って内部記憶装置または外部記憶装置に転送し格納して用いる。また、そのプログラムを、例えば磁気ディスク，光ディスク，光磁気ディスク等の記憶装置（記録媒体）に記録しておき、その記憶装置から通信回線を介してコンピュータに提供するようにしてもよい。

【００８３】

ここで、コンピュータとは、ハードウエアとＯＳ（オペレーティングシステム）とを含む概念であり、ＯＳの制御の下で動作するハードウエアを意味している。また、ＯＳが不要でアプリケーションプログラム単独でハードウェアを動作させるような場合には、そのハードウェア自体がコンピュータに相当する。ハードウエアは、少なくとも、ＣＰＵ等のマイクロプロセッサと、記録媒体に記録されたプログラムを読み取るための手段とをそなえている。上記バイオメトリクス情報管理ストレージシステム用制御プログラムとしてのアプリケーションプログラムは、上述のようなコンピュータに、指紋画像変換部２１１，指紋特徴情報抽出部２２０，運用管理部２３０～２３４，データ形式管理部２５０，端末ＩＤ／データ形式対応管理部２５１および端末ＩＤ／データ形式／変換コード対応管理部２５２としての機能を実現させるプログラムコードを含んでいる。また、その機能の一部は、アプリケーションプログラムではなくＯＳによって実現されてもよい。

【００８４】

さらに、上記記録媒体としては、上述したフレキシブルディスク，ＣＤ－ＲＯＭ，ＣＤ－Ｒ，ＣＤ－ＲＷ，ＤＶＤ，磁気ディスク，光ディスク，光磁気ディスクのほか、ＩＣカード，ＲＯＭカートリッジ，磁気テープ，パンチカード，コンピュータの内部記憶装置（ＲＡＭやＲＯＭなどのメモリ），外部記憶装置等や、バーコードなどの符号が印刷された印刷物等の、コンピュータ読取可能な種々の媒体を利用することもできる。

【００８５】
〔７〕付記
（付記１）
バイオメトリクス情報による個人認証機能を有する端末装置と、
該端末装置の運用を管理するためのサーバと、
該端末装置と該サーバとの間で情報をやり取りすべく該端末装置と該サーバとの間を通信可能に接続しうる通信手段とをそなえ、
該端末装置が、
該端末装置のユーザが照合用バイオメトリクス情報を入力するための入力部と、
該入力部から入力された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、
前記ユーザの参照用特徴情報を予め保存する参照用特徴情報保存部と、
該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成され、
該サーバが、
該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、
該登録用バイオメトリクス情報保存部に保存されている前記登録用バイオメトリクス情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、
該特徴情報抽出部によって抽出された特徴情報を、該通信手段を通じて該端末装置に送信し、該端末装置における該参照用特徴情報保存部に、前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴とする、バイオメトリクス情報管理システム。
【００８６】
（付記２）
バイオメトリクス情報による個人認証機能を有する端末装置と、
該端末装置の運用を管理するためのサーバと、
該端末装置と該サーバとの間で情報をやり取りすべく該端末装置と該サーバとの間を通信可能に接続しうる通信手段とをそなえ、
該端末装置が、
該端末装置のユーザが照合用バイオメトリクス情報を入力するための入力部と、
変換コードを予め保存する変換コード保存部と、
該入力部から入力された前記照合用バイオメトリクス情報に対し、該変換コード保存部に保存される前記変換コードを用いて所定の変換処理を施す照合用バイオメトリクス情報変換部と、
該照合用バイオメトリクス情報変換部によって変換された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、
前記ユーザの参照用特徴情報を予め保存する参照用特徴情報保存部と、
該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成され、
該サーバが、
該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、
該登録用バイオメトリクス情報保存部に保存されるべき前記登録用バイオメトリクス情報に対し、所定の変換コードを用いて所定の変換処理を施す登録用バイオメトリクス情報変換部と、
該登録用バイオメトリクス情報変換部によって変換された前記登録用バイオメトリクス

情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、

前記所定の変換コードと前記該特徴情報抽出部によって抽出された特徴情報とを、該通信手段を通じて該端末装置に送信し、それぞれ、該端末装置における該変換コード保存部および該参照用特徴情報保存部に、前記変換コードおよび前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴とする、バイオメトリクス情報管理システム。

【００８７】

（付記３）

該端末装置が、さらに、

該照合部で用いられる特徴情報のデータ形式を管理し、前記データ形式を、該通信手段を通じて該サーバに送信するデータ形式管理部をそなえて構成され、

該サーバが、さらに、

該端末装置から送信されてきた前記データ形式に応じた特徴情報を前記個人認証機能に応じた特徴情報として抽出するように該特徴情報抽出部による抽出動作を管理するデータ形式管理部をそなえて構成されていることを特徴とする、付記１または付記２に記載のバイオメトリクス情報管理システム。

【００８８】

（付記４）

該端末装置が、さらに、

該端末装置固有の端末識別情報を管理し、前記端末識別情報を、該通信手段を通じて該サーバに送信する端末識別情報管理部をそなえて構成され、

該サーバが、さらに、

端末識別情報と当該端末識別情報で特定される端末装置で用いられる特徴情報のデータ形式との対応関係を管理し、該端末装置から送信されてきた前記端末識別情報に対応するデータ形式に応じた特徴情報を前記個人認証機能に応じた特徴情報として抽出するように該特徴情報抽出部による抽出動作を管理する端末識別情報／データ形式対応管理部をそなえて構成されていることを特徴とする、付記１記載のバイオメトリクス情報管理システム。

【００８９】

（付記５）

該端末装置が、さらに、

該端末装置固有の端末識別情報を管理し、前記端末識別情報を、該通信手段を通じて該サーバに送信する端末識別情報管理部をそなえて構成され、

該サーバが、さらに、

端末識別情報と当該端末識別情報で特定される端末装置で用いられる特徴情報のデータ形式および変換コードとの対応関係を管理し、該端末装置から送信されてきた前記端末識別情報に対応する変換コードを前記所定の変換コードとして用いて前記登録用バイオメトリクス情報の変換処理を行なうように該登録用バイオメトリクス情報変換部による変換動作を管理するとともに、該端末装置から送信されてきた前記端末識別情報に対応するデータ形式に応じた特徴情報を前記個人認証機能に応じた特徴情報として抽出するように該特徴情報抽出部による抽出動作を管理する端末識別情報／データ形式／変換コード対応管理部をそなえて構成されていることを特徴とする、付記２記載のバイオメトリクス情報管理システム。

【００９０】

（付記６）

該端末装置が、該通信手段を通じて該サーバにより遠隔制御される被遠隔制御機能を有するとともに、

該サーバが、該通信手段を通じて該端末装置を遠隔制御する遠隔制御機能を有していることを特徴とする、付記１～付記５のいずれか一項に記載のバイオメトリクス情報管理シ

ステム。
【００９１】
（付記７）
該サーバが、前記遠隔制御機能により、該端末装置における前記参照用特徴情報もしくは前記変換コードの登録／削除、および、該端末装置の利用開始／利用停止を遠隔制御することを特徴とする、付記６記載のバイオメトリクス情報管理システム。
（付記８）
該端末装置が携帯電子情報端末もしくは携帯電話であり、該端末装置と該サーバとの間の該通信手段として、該端末装置に接続される通信回線が用いられることを特徴とする、付記１～付記７のいずれか一項に記載のバイオメトリクス情報管理システム。
【００９２】
（付記９）
該通信手段として、該端末装置および該サーバのそれぞれにそなえられた赤外線通信機能が用いられることを特徴とする、付記１～付記７のいずれか一項に記載のバイオメトリクス情報管理システム。
（付記１０）
前記バイオメトリクス情報が、指紋画像，虹彩パターン画像，顔画像，掌紋画像，血管パターン画像，網膜パターン画像，音声パターン画像，署名画像のうちの少なくとも一つであることを特徴とする、付記１～付記９のいずれか一項に記載のバイオメトリクス情報管理システム。
【００９３】
（付記１１）
照合用バイオメトリクス情報を入力するための入力部と、該入力部から入力された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、参照用特徴情報を予め保存する参照用特徴情報保存部と、該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成された、バイオメトリクス情報による個人認証機能を有する端末装置の運用を、通信手段を介して管理するためのサーバであって、
該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、
該登録用バイオメトリクス情報保存部に保存されている前記登録用バイオメトリクス情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、
該特徴情報抽出部によって抽出された特徴情報を、該通信手段を通じて該端末装置に送信し、該端末装置における該参照用特徴情報保存部に、前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴とする、バイオメトリクス情報管理サーバ。
【００９４】
（付記１２）
照合用バイオメトリクス情報を入力するための入力部と、変換コードを予め保存する変換コード保存部と、該入力部から入力された前記照合用バイオメトリクス情報に対し、該変換コード保存部に保存される前記変換コードを用いて所定の変換処理を施す照合用バイオメトリクス情報変換部と、該照合用バイオメトリクス情報変換部によって変換された前記照合用バイオメトリクス情報から照合用特徴情報を抽出する照合用特徴情報抽出部と、参照用特徴情報を予め保存する参照用特徴情報保存部と、該照合用特徴情報抽出部によって抽出された前記照合用特徴情報と該参照用特徴情報保存部に保存されている前記参照用特徴情報とを比較・照合して個人認証を行なう照合部とをそなえて構成された、バイオメトリクス情報による個人認証機能を有する端末装置の運用を、通信手段を介して管理するためのサーバであって、

該端末装置における個人認証機能で用いられるものと同一種類の登録用バイオメトリクス情報を予め保存する登録用バイオメトリクス情報保存部と、
該登録用バイオメトリクス情報保存部に保存されるべき前記登録用バイオメトリクス情報に対し、所定の変換コードを用いて所定の変換処理を施す登録用バイオメトリクス情報変換部と、
該登録用バイオメトリクス情報変換部によって変換された前記登録用バイオメトリクス情報から、該端末装置における個人認証機能に応じた特徴情報を抽出する特徴情報抽出部と、
前記所定の変換コードと前記該特徴情報抽出部によって抽出された特徴情報とを、該通信手段を通じて該端末装置に送信し、それぞれ、該端末装置における該変換コード保存部および該参照用特徴情報保存部に、前記変換コードおよび前記参照用特徴情報として保存させる運用管理部とをそなえて構成されていることを特徴とする、バイオメトリクス情報管理サーバ。

【００９５】

（付記１３）

該端末装置の該照合部で用いられる特徴情報のデータ形式を、該端末装置から該通信手段を通じて受信し、受信された前記データ形式に応じた特徴情報を前記個人認証機能に応じた特徴情報として抽出するように該特徴情報抽出部による抽出動作を管理するデータ形式管理部をそなえて構成されていることを特徴とする、付記１１または付記１２に記載のバイオメトリクス情報管理サーバ。

【００９６】

（付記１４）

端末識別情報と当該端末識別情報で特定される端末装置で用いられる特徴情報のデータ形式との対応関係を管理し、該端末装置から該通信手段を通じて送信されてきた端末識別情報に対応するデータ形式に応じた特徴情報を前記個人認証機能に応じた特徴情報として抽出するように該特徴情報抽出部による抽出動作を管理する端末識別情報／データ形式対応管理部をそなえて構成されていることを特徴とする、付記１１記載のバイオメトリクス情報管理サーバ。

【００９７】

（付記１５）

端末識別情報と当該端末識別情報で特定される端末装置で用いられる特徴情報のデータ形式および変換コードとの対応関係を管理し、該端末装置から該通信手段を通じて送信されてきた前記端末識別情報に対応するデータ形式に応じた特徴情報を前記個人認証機能に応じた特徴情報として抽出するように該特徴情報抽出部による抽出動作を管理する端末識別情報／データ形式／変換コード対応管理部をそなえて構成されていることを特徴とする、付記１２記載のバイオメトリクス情報管理サーバ。

【００９８】

（付記１６）

該サーバが、該通信手段を通じて該端末装置を遠隔制御する遠隔制御機能を有していることを特徴とする、付記１１～付記１５のいずれか一項に記載のバイオメトリクス情報管理サーバ。

（付記１７）

該サーバが、前記遠隔制御機能により、該端末装置における前記参照用特徴情報もしくは前記変換コードの登録／削除、および、該端末装置の利用開始／利用停止を遠隔制御することを特徴とする、付記１６記載のバイオメトリクス情報管理サーバ。

【００９９】

（付記１８）

該端末装置と該サーバとの間の該通信手段として、該端末装置に接続される通信回線が用いられることを特徴とする、付記１１～付記１７のいずれか一項に記載のバイオメトリクス情報管理サーバ。

（付記１９）
該通信手段として、該端末装置および該サーバのそれぞれにそなえられた赤外線通信機能が用いられることを特徴とする、付記１１～付記１７のいずれか一項に記載のバイオメトリクス情報管理サーバ。

【０１００】
（付記２０）
前記バイオメトリクス情報が、指紋画像，虹彩パターン画像，顔画像，掌紋画像，血管パターン画像，網膜パターン画像，音声パターン画像，署名画像のうちの少なくとも一つであることを特徴とする、付記１１～付記１９のいずれか一項に記載のバイオメトリクス情報管理サーバ。

【図面の簡単な説明】

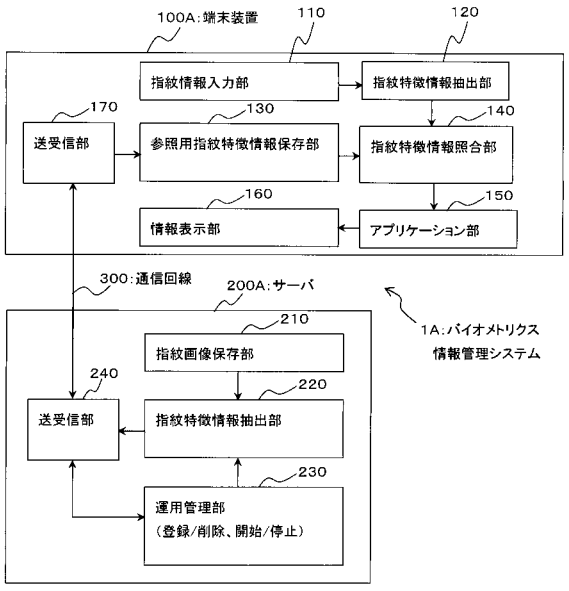
【０１０１】
【図１】本発明の第１実施形態としてのバイオメトリクス情報管理システム（端末装置およびサーバ）の機能構成を示すブロック図である。
【図２】図１に示すシステムの動作を説明するためのフローチャートである。
【図３】本発明の第２実施形態としてのバイオメトリクス情報管理システム（端末装置およびサーバ）の機能構成を示すブロック図である。
【図４】図３に示すシステムの動作を説明するためのフローチャートである。
【図５】本発明の第３実施形態としてのバイオメトリクス情報管理システム（端末装置およびサーバ）の機能構成を示すブロック図である。
【図６】図５に示すシステムの動作を説明するためのフローチャートである。
【図７】第３実施形態の参照テーブルの一例を示す図である。
【図８】第３実施形態の参照テーブルの他例を示す図である。
【図９】本発明の第４実施形態としてのバイオメトリクス情報管理システム（端末装置およびサーバ）の機能構成を示すブロック図である。
【図１０】図９に示すシステムの遠隔制御動作（登録）を説明するためのフローチャートである。
【図１１】図９に示すシステムの遠隔制御動作（削除）を説明するためのフローチャートである。
【図１２】図９に示すシステムの遠隔制御動作（利用開始）を説明するためのフローチャートである。
【図１３】図９に示すシステムの遠隔制御動作（利用停止）を説明するためのフローチャートである。
【図１４】本発明の第５実施形態としてのバイオメトリクス情報管理システム（端末装置およびサーバ）の機能構成を示すブロック図である。
【図１５】図１４に示すシステムの動作を説明するためのフローチャートである。
【図１６】第５実施形態の参照テーブルの一例を示す図である。
【図１７】図１４に示す端末装置における照合動作を説明するためのフローチャートである。
【図１８】バイオメトリクス情報による個人認証機能を有する、一般的な端末装置の機能構成（特に個人認証機能に係る構成）を示すブロック図である。

【符号の説明】

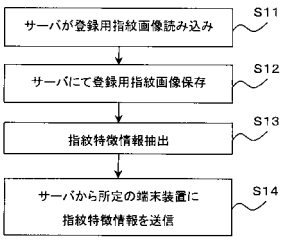
【０１０２】
１Ａ，１Ｂ，１Ｃ，１Ｄ，１Ｅ　バイオメトリクス情報管理システム
１００，１００Ａ，１００Ｂ，１００Ｃ，１００Ｄ，１００Ｅ　端末装置
１１０　指紋情報入力部（入力部）
１１１　変換コード保存部
１１２　指紋画像変換部（照合用バイオメトリクス情報変換部）
１２０　指紋特徴情報抽出部（照合用特徴情報抽出部）
１３０　参照用指紋特徴情報保存部（参照用特徴情報保存部）

１４０　指紋特徴情報照合部（照合部）
１５０　アプリケーション部
１６０　情報表示部
１７０　送受信部（通信手段）
１８０　データ形式管理部
１８１　端末ＩＤ管理部（端末識別情報管理部）
２００Ａ，２００Ｂ，２００Ｃ，２００Ｄ，２００Ｅ　サーバ（バイオメトリクス情報管理サーバ）
２１０　指紋画像保存部（登録用バイオメトリクス情報保存部）
２１１　指紋画像変換部（登録用バイオメトリクス情報変換部）
２２０　指紋特徴情報抽出部（特徴情報抽出部）
２３０，２３１，２３２，２３３，２３４　運用管理部
２４０　送受信部（通信手段）
２５０　データ形式管理部
２５１　端末ＩＤ／データ形式対応管理部（端末識別情報／データ形式対応管理部）
２５２　端末ＩＤ／データ形式／変換コード対応管理部（端末識別情報／データ形式／変換コード対応管理部）
３００　通信回線（通信手段）

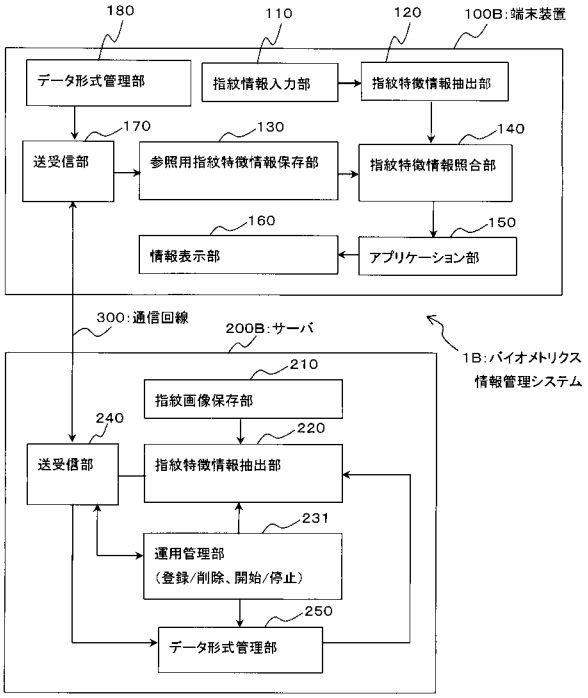
【図１】



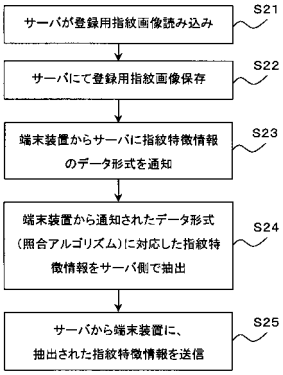
【図２】



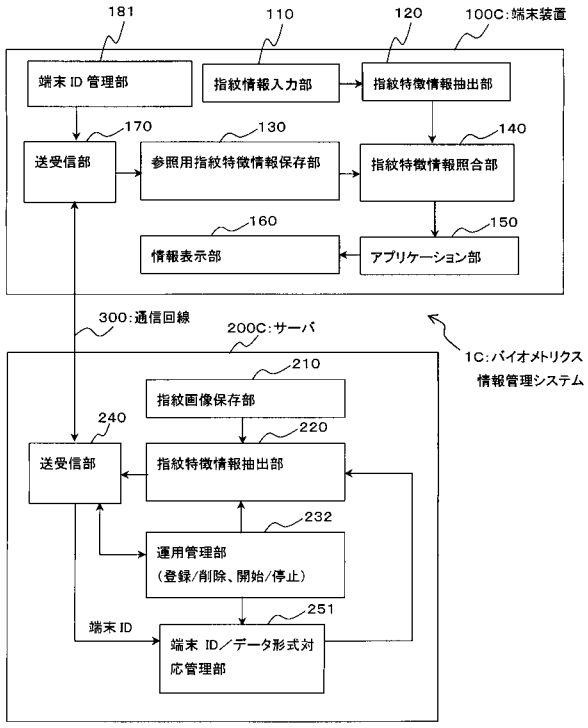
【図３】



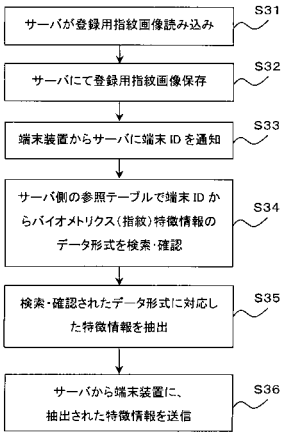
【図４】



【図５】



【図６】



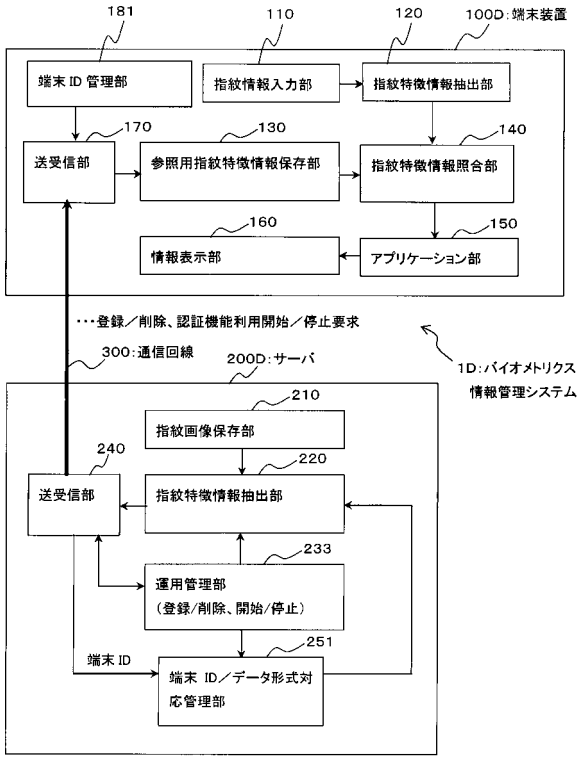
【図７】

端末 ID	バイオメトリクス方式	照合ソフト形式
000001	指紋	PM-A-1
000002	指紋	PM-A-1
000003	指紋	MM-A-1
000004	顔	FA-A-1
000005	虹彩	IR-A-1

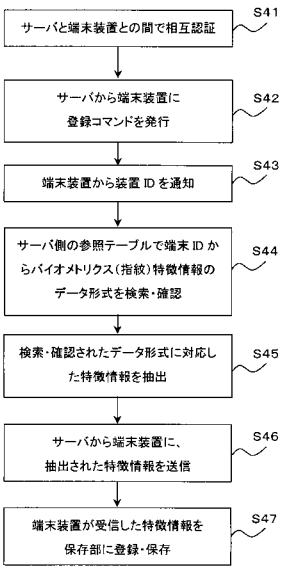
【図８】

端末 ID	バイオメトリクス方式	データ形式	入力センサ
000001	指紋	P-A-1	F0001
000002	指紋	P-A-1	F0002
000003	指紋	M-A-1	F0001
000004	顔	F-A-1	FA0001
000005	虹彩	I-A-1	I0001

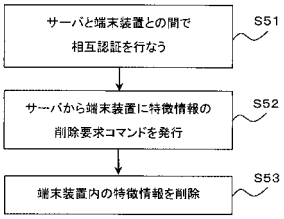
【図９】



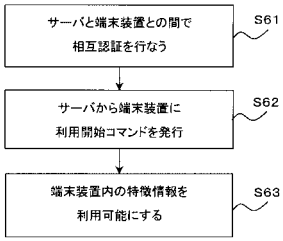
【図１０】



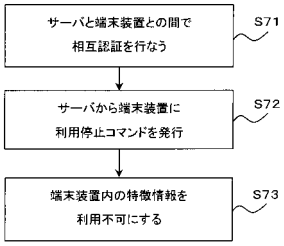
【図１１】



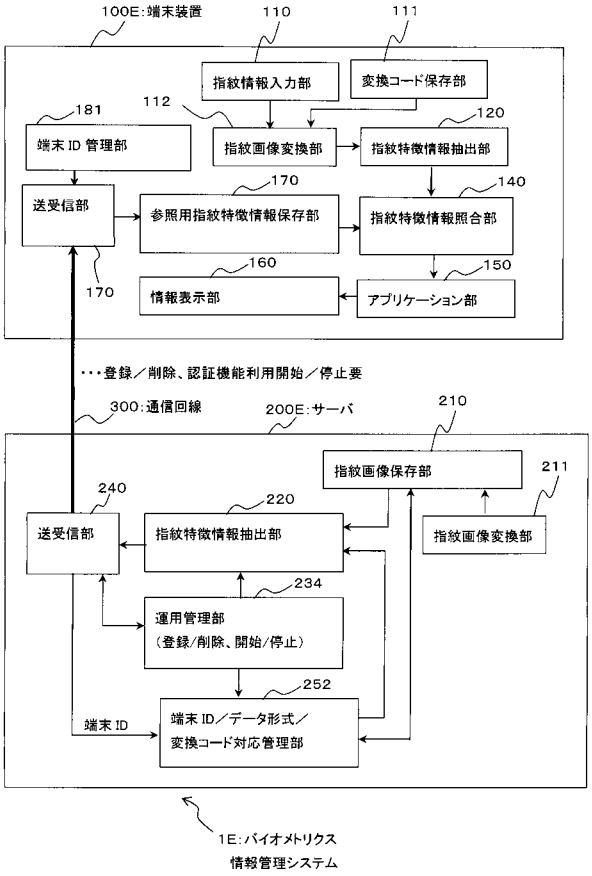
【図１２】



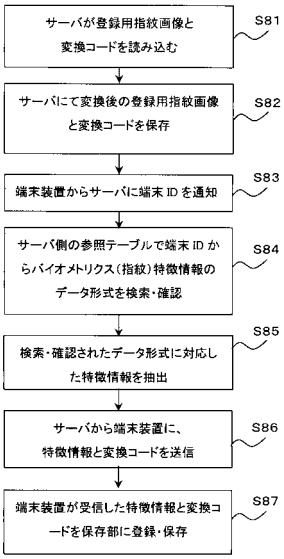
【図１３】



【図１４】



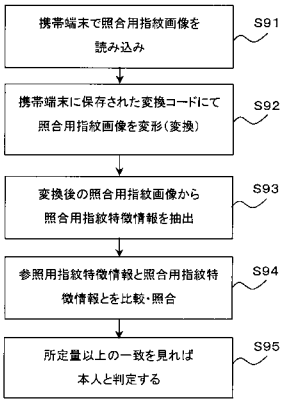
【図１５】



【図１６】

端末 ID	バイオメトリクス方式	照合ソフト形式	登録ユーザ	変換コード
000001	指紋	PM-A-1	1342341	1AD34F6A
			1345677	3A634B6A
			1346686	B6A023DE
			1358902	34A86731
000002	指紋	PM-A-1	2345623	12A53451
000003	指紋	MM-A-1	4564356	653843AE
000004	顔	FA-A-1	2345658	023DE456
000005	虹彩	IR-A-1	2342523	43A734D1

【図１７】



【図１８】