(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6810568号
(P6810568)

(45)発行日　令和3年1月6日(2021.1.6)　(24)登録日　令和2年12月15日(2020.12.15)

(51)Int.Cl.　F I
G06F 21/32 (2013.01)　G06F 21/32
G06T 7/00 (2017.01)　G06T 7/00　５１０Ｂ

請求項の数 4　(全 16 頁)

(21)出願番号　特願2016-186490(P2016-186490)
(22)出願日　平成28年9月26日(2016.9.26)
(65)公開番号　特開2018-55145(P2018-55145A)
(43)公開日　平成30年4月5日(2018.4.5)
審査請求日　平成31年2月14日(2019.2.14)

前置審査

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000176
一色国際特許業務法人
(72)発明者　高木　琢磨
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　寺田　直人
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　吉田　正人
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内

最終頁に続く

(54)【発明の名称】認証処理システムおよび認証処理方法

(57)【特許請求の範囲】
【請求項１】
認証対象者が入力した当該認証対象者の識別情報をキーに、当該認証対象者に関して登録済みの生体認証用テンプレートの取得要求を、所定の認証サーバに送信すると共に、生体情報リーダーでの前記認証対象者に対する生体情報読み取りを実行し、当該生体情報読み取りの間に前記認証サーバから前記認証対象者の生体認証用テンプレートを取得する処理と、前記生体情報読み取りにより得た生体情報と、前記認証サーバから得た生体認証用テンプレートとに基づく所定の生体認証処理と、を実行する認証処理装置と、
認証対象者の識別情報と、当該認証対象者に関してテンプレート公開型生体認証基盤におけるポリシーに基づいて複数種の生体部位それぞれに複数生成された生体認証用テンプレートと、前記生体認証用テンプレートのうち直近の生体認証処理に使用されたものであることを示すフラグであって、使用対象となった生体部位の種類および当該種類に関して複数存在する生体認証用テンプレートのうち使用対象のもの、に紐付けて設定される直近使用フラグ、を対応付けて格納した認証テーブルを記憶する記憶装置と、前記認証処理装置からの前記取得要求に応じて、当該取得要求が示す前記認証対象者の識別情報をキーに、前記認証テーブルにおける当該認証対象者の生体認証用テンプレートのうち、前記直近使用フラグが設定されているものを検索し、当該検索により、前記認証対象者に関し過去に認証対象となった生体認証用テンプレートを特定し、当該生体認証用テンプレートを、前記認証処理装置に返信する処理と、前記テンプレート公開型生体認証基盤における認証手順に基づき前記認証処理装置と共に前記生体認証処理を実行する処理、を行う演算装置

とを備えた認証サーバと、
を含む認証処理システム。
【請求項２】
前記認証処理装置は、
前記認証サーバから、前記生体認証用テンプレートとして、テンプレート公開型生体認証基盤におけるポリシーに基づいて生成された生体認証用テンプレートを取得し、前記生体認証処理を、前記テンプレート公開型生体認証基盤における認証手順に基づき前記認証サーバと共に実行するものである、
ことを特徴とする請求項１に記載の認証処理システム。
【請求項３】
認証装置が、
認証対象者が入力した当該認証対象者の識別情報をキーに、当該認証対象者に関して登録済みの生体認証用テンプレートの取得要求を、所定の認証サーバに送信すると共に、生体情報リーダーでの前記認証対象者に対する生体情報読み取りを実行し、当該生体情報読み取りの間に前記認証サーバから前記認証対象者の生体認証用テンプレートを取得する処理と、前記生体情報読み取りにより得た生体情報と、前記認証サーバから得た生体認証用テンプレートとに基づく所定の生体認証処理と、を実行し、
認証サーバが、
認証対象者の識別情報と、当該認証対象者に関してテンプレート公開型生体認証基盤におけるポリシーに基づいて複数種の生体部位それぞれに複数生成された生体認証用テンプレートと、前記生体認証用テンプレートのうち直近の生体認証処理に使用されたものであることを示すフラグであって、使用対象となった生体部位の種類および当該種類に関して複数存在する生体認証用テンプレートのうち使用対象のもの、に紐付けて設定される直近使用フラグ、を対応付けて格納した認証テーブルを記憶装置で保持し、前記認証処理装置からの前記取得要求に応じて、当該取得要求が示す前記認証対象者の識別情報をキーに、前記認証テーブルにおける当該認証対象者の生体認証用テンプレートのうち、前記直近使用フラグが設定されているものを検索し、当該検索により、前記認証対象者に関し過去に認証対象となった生体認証用テンプレートを特定し、当該生体認証用テンプレートを、前記認証処理装置に返信する処理と、前記テンプレート公開型生体認証基盤における認証手順に基づき前記認証処理装置と共に前記生体認証処理を実行する処理と、を実行する、
ことを特徴とする認証処理方法。
【請求項４】
前記認証処理装置が、
前記認証サーバから、前記生体認証用テンプレートとして、テンプレート公開型生体認証基盤におけるポリシーに基づいて生成された生体認証用テンプレートを取得し、前記生体認証処理を、前記テンプレート公開型生体認証基盤における認証手順に基づき前記認証サーバと共に実行する、
ことを特徴とする請求項３に記載の認証処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証処理システムおよび認証処理方法に関するものであり、具体的には、生体認証の処理を効率化し、認証処理時間を従来よりも低減可能とする技術に関する。
【背景技術】
【０００２】
金融機関等におけるＡＴＭや、営業店窓口に備わる端末など、顧客等の本人認証処理を必要とする装置が種々存在する。最近では、認証に要する手順を従来よりも低減してユーザビリティを向上させると共に、悪意の第三者による資産窃取などを回避する意味もあり、生体認証システムが広く採用されている。
【０００３】

このような生体認証に関連する従来技術としては、例えば、ユーザ認証処理を生体情報によって処理する為の生体情報入力装置と、ユーザの生体情報を用いた認証処理を行う認証処理部と、ユーザ所望の処理を実行する為の前記入出力装置に対するユーザ認証動作始を検出し、認証動作開始の検出によってユーザ所望の処理準備をバックグラウンドで開始することで、ユーザ認証処理が完了する前にユーザ所望の処理準備が完了し、ユーザ認証完了直後にユーザ所望の処理が実行可能な状態となるよう制御する制御部とを有する認証装置（特許文献１参照）などが提案されている。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２０１１－７６２８８号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

こうした生体認証のシステムでは、認証用の生体情報を顧客各自のＩＣカード等の媒体内に格納・管理する運用が一般的である。この場合、当該媒体の保管や携行、ＡＴＭ等にセットする操作など種々の顧客負担は回避出来ない。また、当該媒体の発行や紛失時の再発行等にかかる金融機関側の負担も回避できない。

【０００６】

また、上述のＡＴＭ等と認証サーバとの間で、生体情報を暗号化するなどしてやりとりして生体認証の処理を実行する場合、顧客から読み取った生体情報と認証サーバにおける全登録者の生体情報との照合手順が必要となる。その結果、認証時間が長くなりがちで、顧客満足度が低下しやすい懸念もある。

【０００７】

そこで本発明の目的は、生体認証の処理を効率化し、認証処理時間を従来よりも低減可能とする技術を提供することにある。

【課題を解決するための手段】

【０００８】

上記課題を解決する本発明の認証処理システムは、認証対象者が入力した当該認証対象者の識別情報をキーに、当該認証対象者に関して登録済みの生体認証用テンプレートの取得要求を、所定の認証サーバに送信すると共に、生体情報リーダーでの前記認証対象者に対する生体情報読み取りを実行し、当該生体情報読み取りの間に前記認証サーバから前記認証対象者の生体認証用テンプレートを取得する処理と、前記生体情報読み取りにより得た生体情報と、前記認証サーバから得た生体認証用テンプレートとに基づく所定の生体認証処理と、を実行する認証処理装置と、認証対象者の識別情報と、当該認証対象者に関してテンプレート公開型生体認証基盤におけるポリシーに基づいて複数種の生体部位それぞれに複数生成された生体認証用テンプレートと、前記生体認証用テンプレートのうち直近の生体認証処理に使用されたものであることを示すフラグであって、使用対象となった生体部位の種類および当該種類に関して複数存在する生体認証用テンプレートのうち使用対象のもの、に紐付けて設定される直近使用フラグ、を対応付けて格納した認証テーブルを記憶する記憶装置と、前記認証処理装置からの前記取得要求に応じて、当該取得要求が示す前記認証対象者の識別情報をキーに、前記認証テーブルにおける当該認証対象者の生体認証用テンプレートのうち、前記直近使用フラグが設定されているものを検索し、当該検索により、前記認証対象者に関し過去に認証対象となった生体認証用テンプレートを特定し、当該生体認証用テンプレートを、前記認証処理装置に返信する処理と、前記テンプレート公開型生体認証基盤における認証手順に基づき前記認証処理装置と共に前記生体認証処理を実行する処理、を行う演算装置を備えた認証サーバを含むことを特徴とする。

【０００９】

また、本発明の認証処理方法は、認証装置が、認証対象者が入力した当該認証対象者の識別情報をキーに、当該認証対象者に関して登録済みの生体認証用テンプレートの取得要

求を、所定の認証サーバに送信すると共に、生体情報リーダーでの前記認証対象者に対する生体情報読み取りを実行し、当該生体情報読み取りの間に前記認証サーバから前記認証対象者の生体認証用テンプレートを取得する処理と、前記生体情報読み取りにより得た生体情報と、前記認証サーバから得た生体認証用テンプレートとに基づく所定の生体認証処理と、を実行し、認証サーバが、認証対象者の識別情報と、当該認証対象者に関してテンプレート公開型生体認証基盤におけるポリシーに基づいて複数種の生体部位それぞれに複数生成された生体認証用テンプレートと、前記生体認証用テンプレートのうち直近の生体認証処理に使用されたものであることを示すフラグであって、使用対象となった生体部位の種類および当該種類に関して複数存在する生体認証用テンプレートのうち使用対象のもの、に紐付けて設定される直近使用フラグ、を対応付けて格納した認証テーブルを記憶装置で保持し、前記認証処理装置からの前記取得要求に応じて、当該取得要求が示す前記認証対象者の識別情報をキーに、前記認証テーブルにおける当該認証対象者の生体認証用テンプレートのうち、前記直近使用フラグが設定されているものを検索し、当該検索により、前記認証対象者に関し過去に認証対象となった生体認証用テンプレートを特定し、当該生体認証用テンプレートを、前記認証処理装置に返信する処理と、前記テンプレート公開型生体認証基盤における認証手順に基づき前記認証処理装置と共に前記生体認証処理を実行する処理と、を実行する、ことを特徴とする。

【発明の効果】

【００１０】

本発明によれば、生体認証の処理を効率化し、認証処理時間を従来よりも低減可能となる。

【図面の簡単な説明】

【００１１】

【図１】本実施形態の認証処理システムを示すネットワーク構成図である。

【図２】本実施形態における認証処理装置のハードウェア構成例を示す図である。

【図３】本実施形態における認証サーバのハードウェア構成例を示す図である。

【図４】本実施形態の認証テーブルのデータ構成例を示す図である。

【図５】本実施形態の生体認証用テンプレートの構成イメージを示す図である。

【図６】本実施形態における認証処理方法のフロー例１を示す図である。

【図７】本実施形態における画面例を示す図である。

【図８】本実施形態における差分計算の実行順序例を示す図である。

【図９】本実施形態における認証処理方法のフロー例２を示す図である。

【発明を実施するための形態】

【００１２】

－－－システム構成－－－

【００１３】

以下に本発明の実施形態について図面を用いて詳細に説明する。図１は、本実施形態の認証処理システム１０に対応したネットワーク構成図である。図１に示す認証処理システム１０は、生体認証の処理を効率化し、認証処理時間を従来よりも低減可能とするコンピュータシステムである。

【００１４】

本実施形態の認証処理システム１０は、認証処理装置１００および認証サーバ２００が、ネットワーク５を介して通信可能に結ばれて構成されたものとなる。

【００１５】

こうした認証処理システム１０を構成する装置のうち、認証処理装置１００は、ＡＴＭや営業店の窓口端末など、金融機関の顧客に関して本人認証を行う装置を想定する。勿論、本人認証を行うべき装置であれば種類は問わない。ここでは一例として、上述の金融機関の顧客を認証対象者とする。また、認証サーバ２００は、上述の金融機関の各顧客に関して、その生体認証用テンプレートを管理し、認証処理装置１００と協働して生体認証の処理を実行するサーバ装置となる。

【００１６】
上述の認証処理装置１００および認証サーバ２００は、いずれも、テンプレート公開型生体認証基盤（参考：特開２０１５－３９１０６号公報）において生体認証処理を行う装置である。従って、本実施形態における生体認証処理は、テンプレート公開型生体認証基盤における認証処理のプロトコルに沿ったものとなる。
【００１７】
上述のテンプレート公開型生体認証基盤を本人認証に適用した場合、ＡＴＭ等で従来から用いられているＩＣチップ内蔵のキャッシュカードなど、生体情報を格納した媒体が不要となる。また、認証サーバ２００からネットワーク５経由で認証処理装置１００に提供される各顧客の生体認証用テンプレートは、数学的にも元の生体情報に戻せないことが証明された、いわゆる不可逆的な情報である。よって、こうした生体認証用テンプレートは漏洩しても当該顧客の生体情報を第三者に知られることは無く、セキュアな環境での生体認証が実行出来ることとなる。
－－－ハードウェア構成－－－
【００１８】
また、本実施形態の認証処理システム１０が含む各装置のハードウェア構成例について説明する。図２は、本実施形態の認証処理装置１００のハードウェア構成例を示す図である。なお、この認証処理装置１００は、具体的にはＡＴＭや営業店端末を想定するが、そうした端末に特有の既存構成（例：ＡＴＭにおける現金搬送機構、現金保管庫など）については説明を省略する。
【００１９】
本実施形態の認証処理装置１００は、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）やハードディスクドライブなど適宜な不揮発性記憶素子で構成される記憶装置１０１、ＲＡＭなど揮発性記憶素子で構成されるメモリ１０３、記憶装置１０１に保持されるプログラム１０２をメモリ１０３に読み出すなどして実行し装置自体の統括制御を行なうとともに各種判定、演算及び制御処理を行なうＣＰＵなどの演算装置１０４、ユーザからのキー入力や音声入力を受け付ける入力装置１０５、処理データの表示を行うディスプレイ等の出力装置１０６、ネットワーク５と接続し他装置との通信処理を担う通信装置１０７、および、顧客の生体部位に対する生体情報の読み取り動作を行う生体情報リーダー１１０を備える。
【００２０】
なお、上述の生体情報リーダー１１０は、例えば、指や掌の静脈センサーや、指紋や虹彩の撮像装置、などを想定する。
【００２１】
また、上述のプログラム１０２には、テンプレート公開型生体認証基盤におけるプロトコルに沿った認証手順を実行するプログラムが含まれる。
【００２２】
続いて図３に、本実施形態の認証サーバ２００のハードウェア構成例を示す。本実施形態の認証サーバ２００は、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）やハードディスクドライブなど適宜な不揮発性記憶素子で構成される記憶装置２０１、ＲＡＭなど揮発性記憶素子で構成されるメモリ２０３、記憶装置２０１に保持されるプログラム２０２をメモリ２０３に読み出すなどして実行し装置自体の統括制御を行なうとともに各種判定、演算及び制御処理を行なうＣＰＵなどの演算装置２０４、および、ネットワーク５と接続し他装置との通信処理を担う通信装置２０５、を備える。
【００２３】
なお、上述の記憶装置２０１には、プログラム２０２に加えて、各顧客の各生体部位に対する生体認証用テンプレートを保管する認証テーブル２２５を格納している。この認証テーブル２２５の具体的なデータ構成例等は後述する。
－－－データ構造例－－－
【００２４】

続いて、本実施形態の認証処理システム１０にて用いるテーブル類について説明する。図４に、本実施形態における認証テーブル２２５の一例を示す。

【００２５】

本実施形態の認証テーブル２２５は、金融機関の顧客から予め取得した生体情報を、上述したテンプレート公開型生体認証基盤のプロトコルに沿って加工し生成した生体認証用テンプレートを蓄積したテーブルである。

【００２６】

そのデータ構造は、金融機関の顧客を一意に特定する顧客ＩＤをキーとして、当該顧客に関して生体認証用テンプレートが登録された生体部位、当該生体部位に関して登録された複数の生体認証用テンプレート、および、直近使用フラグ、といった値を対応付けたレコードの集合体となっている。

【００２７】

なお、生体部位の例としては、右手親指を「Ｒ０１」、右手人差し指を「Ｒ０２」、右手中指を「Ｒ０３」、右手薬指を「Ｒ０４」、右手子指を「Ｒ０５」、とし、同様に、左手親指を「Ｌ０１」、左手人差し指を「Ｌ０２」、左手中指を「Ｌ０３」、左手薬指を「Ｌ０４」、左手子指を「Ｌ０５」、などとしている。

【００２８】

図４の例では、顧客ＩＤ「００００１」の顧客に関しては、右手人差し指「Ｒ０２」と左手人差し指「Ｌ０２」に関して、生体認証用テンプレートが登録済みである。また、顧客ＩＤ「００００２」の顧客に関しては、右手人差し指「Ｒ０２」、左手人差し指「Ｌ０２」、および左手中指「Ｌ０３」に関して、生体認証用テンプレートが登録済みである。

また、生体認証用テンプレートは、認証サーバ２００が、登録用に顧客が指定した各生体部位から得た生体情報に、当該顧客用の秘密鍵を埋め込んだデータと、前述の秘密鍵とペアの公開鍵とをセットにしたものである。勿論、こうした認証用テンプレートの生成手順は、テンプレート公開型生体認証基盤におけるプロトコルに沿ったものである。

【００２９】

なお、生体認証用テンプレートは、図４の認証テーブル２２５の例で示すように、一人の顧客の、複数の生体部位に関して、例えば時期別に複数登録されている（図５参照）。

【００３０】

また、直近使用フラグは、各顧客に関して登録済みの生体認証用テンプレートのうち、直近の生体認証処理に使用された、すなわち、認証処理装置１００にて照合対象となったものに付与したフラグである。

【００３１】

図４の例の場合、顧客ＩＤ「００００１」の顧客に関しては、右手人差し指「Ｒ０２」のレコードに直近使用フラグ「１」が付与されている。よって、この顧客を対象とした直近の生体認証処理では、この右手人差し指「Ｒ０２」の生体認証用テンプレートが使用されたことを示している。同様に、顧客ＩＤ「００００２」の顧客に関しては、左人差し指「Ｌ０２」のレコードに直近使用フラグ「１」が付与されている。よって、この顧客を対象とした直近の生体認証処理では、この左手人差し指「Ｌ０２」の生体認証用テンプレートが使用されたことを示している。

【００３２】

なお、本実施形態の認証テーブル２２５では、上述の直近使用フラグが、生体部位の種類ごとに付与された例を示しているが、生体部位の種類と共に、その生体部位に関する生体認証用テンプレートのうち１つを特定するよう直近使用フラグが付与される形態としてもよい。

－－－フロー例１－－－

【００３３】

以下、本実施形態における認証処理方法の実際手順について図に基づき説明する。以下で説明する認証処理方法に対応する各種動作は、認証処理システム１０を構成する、認証処理装置１００および認証サーバ２００がそれぞれメモリ等に読み出して実行するプログ

ラムによって実現される。そして、このプログラムは、以下に説明される各種の動作を行うためのコードから構成されている。

【００３４】

図６は、本実施形態における認証処理方法のフロー例１を示す図である。ここで、金融機関の顧客が、ＡＴＭ等の認証処理装置１００において、所望の金融取引を行うべく所定指示を入力し、それに応じて認証処理装置１００が当該顧客に対する生体認証の手順を開始したとする。

【００３５】

この場合、認証処理装置１００は、上述の顧客に対して識別情報たる顧客ＩＤの入力画面６００（図７参照）を出力装置１０６で表示する（ｓ１００）。ここでは識別情報の一例として顧客ＩＤを入力させる形態をあげたが、これに限定しない。例えば、当該顧客が金融機関で保持する口座の、店番、科目、口座番号、といった情報を入力させるとしてもよい。

【００３６】

次に、認証処理装置１００は、上述の顧客ＩＤをキーに、当該顧客に関して登録済みの生体認証用テンプレートの取得要求を、認証サーバ２００に送信する（ｓ１０１）。

【００３７】

一方、認証サーバ２００は、上述の取得要求を受信し、当該取得要求が含む顧客ＩＤをキーに、認証テーブル２２５での検索を実行する（ｓ１０２）。

【００３８】

他方、認証処理装置１００は、上述の取得要求の送信（ｓ１０１）と共に、生体情報リーダー１１０での上述の顧客に対する生体情報読み取りを開始する（ｓ１０３）。この生体情報読み取りが行われている間、認証サーバ２００では、上述の検索に伴って、当該顧客ＩＤに対応した顧客の、各生体部位について登録済みの生体認証用テンプレートを特定し、例えば生体部位ごとに認証処理装置１００に返信する（ｓ１０４）。

【００３９】

また、認証処理装置１００は、生体情報読み取りを行っている間、顧客ＩＤをキーにした本人認証用データの要求を認証サーバ２００に送信し、認証サーバ２００から当該顧客に関する本人認証用データを取得する（ｓ１０５）。この本人認証用データは、金融機関における既存の顧客管理システム等が保持するデータで、例えば、顧客ＩＤと紐付いて管理されている、当該顧客が保持する金融取引用口座の情報を想定する。

【００４０】

上述の、顧客の生体部位に対する生体情報読み取りの動作は、例えば１～２秒など秒単位であるケースが多い。一方、顧客ＩＤに基づく生体認証用テンプレートや本人認証用データの取得は、例えば数ミリ秒から数十ミリ秒単位と想定される。よって、ｓ１０３で生体情報読み取りの動作が開始されてから、その動作が完了するまでの間、すなわち生体情報読み取り動作のバックグラウンドで、生体認証用テンプレート等の取得が並行して実行出来る。

【００４１】

ここで、認証処理装置１００は、上述の顧客に関して、認証テーブル２２５に登録済みの複数の生体部位のそれぞれに関して複数登録されている生体認証用テンプレートを、全て取得し、かつ、生体情報リーダー１１０での生体情報読み取りも完了したとする（ｓ１０６）。

【００４２】

この場合、認証処理装置１００は、上述のテンプレート公開型生体認証基盤のプロトコルに基づく、ワインタイムの鍵ペア生成を所定アルゴリズムにより実行し、ワンタイム公開鍵とワンタイム秘密鍵を生成する（ｓ１０７）。

【００４３】

次に、認証処理装置１００は、生体情報リーダー１１０で得た上述の顧客の生体情報に対し、ｓ１０７で生成したワンタイム秘密鍵を所定アルゴリズムにて埋め込んで、これを

秘密鍵データとし、認証サーバ２００から取得した各生体認証用テンプレートとの差分計算を逐一実行する（ｓ１０８）。

【００４４】

この差分計算に際しては、テンプレート公開型生体認証基盤における所定の誤り訂正処理を施すことで、生体情報同士の差は消去されるものとする。

【００４５】

また、上述の差分計算を逐一実行する順序としては、図８にて概念を示すように、認証サーバ２００から得た、例えば右手人差し指と左手人差し指の各生体部位のそれぞれに関する複数の生体認証用テンプレート、すなわちテンプレート１～テンプレート３のうち、各生体部位の間で順次選択した１つの生体認証用テンプレートと、生体情報リーダー１１０にて得た生体情報とワンタイム秘密鍵に基づく秘密鍵データとの照合を、所定結果が得られるまで繰り返し実行するものとする。

【００４６】

上述のｓ１０８の差分計算の結果、各生体認証用テンプレートとの差分計算を行っても差分秘密鍵を生成できなかった場合（ｓ１０９：ｎ）、認証処理装置１００は、認証失敗と判定して処理を終了する。

【００４７】

他方、上述のｓ１０８の差分計算の結果、各生体認証用テンプレートのうちいずれかとの差分計算によって、差分秘密鍵を生成できた場合（ｓ１０９：ｙ）、認証処理装置１００は、上述のワンタイム秘密鍵により上述の本人認証用データに署名を行い、これをサーバ認証用データとし、上述の差分秘密鍵と共に、認証サーバ２００に送信する（ｓ１１０）。

【００４８】

一方、認証サーバ２００は、上述のサーバ認証用データおよび差分秘密鍵を受信し、サーバ認証用データを上述の顧客の公開鍵で復号化して署名検証を実行する（ｓ１１１）。

また、認証サーバ２００は、当該顧客に関して予め保持する公開鍵と上述のワンタイム公開鍵が、差分秘密鍵と対応しているかどうかを検証する（ｓ１１２）。この場合、テンプレート公開型生体認証基盤においては、秘密鍵と公開鍵の関係が「準同型性」という性質を満たす方式を採用しており、この性質を用いることで、差分秘密鍵が、上述の二つの公開鍵に対応する秘密鍵同士の差分と一致しているかを検証することとなる。

【００４９】

認証サーバ２００は、上述のｓ１１１の署名検証およびｓ１１２の検証の結果を、認証処理装置１００に返し（ｓ１１３）、処理を終了する。一方の認証処理装置１００は、この結果を受信して、出力装置１０６に表示し（ｓ１１４）、処理を終了する。

【００５０】

なお、ｓ１０９～ｓ１１４にかかる、認証サーバ２００と認証処理装置１００における処理は、テンプレート公開型生体認証基盤における生体認証の手順に沿った処理となる。

【００５１】

また、上述のフローのうち、ｓ１００において、認証処理装置１００は、上述の顧客に対して識別情報たる顧客ＩＤに加えて、認証対象とする生体部位の指定も受け付ける入力画面を出力装置１０６で表示させるとしてよい。

【００５２】

この場合、ｓ１０１における認証処理装置１００は、上述の顧客ＩＤおよび生体部位の情報をキーに、当該顧客の該当生体部位に関して登録済みの生体認証用テンプレートの取得要求を、認証サーバ２００に送信することとなる。

【００５３】

また、ｓ１０２における認証サーバ２００は、上述の取得要求を受信し、当該取得要求が含む顧客ＩＤおよび生体部位の情報をキーに、認証テーブル２２５での検索を実行する。この検索により、認証サーバ２００は、当該顧客ＩＤに対応した顧客の、指定された各生体部位について登録済みの生体認証用テンプレートを特定し、例えば生体部位ごとに認

証処理装置１００に返信する。以降のステップに関しては上述のフロー例１と同様である。

－－－フロー例２－－－

【００５４】

次に、顧客が特段の指定を行わずとも、当該顧客が過去に認証対象とした生体部位に基づいて、生体認証用テンプレートを特定し、これを用いる例について図に基づき説明する。　図９は、本実施形態における認証処理方法のフロー例２を示す図である。ここでは、生体認証用テンプレートの取得に伴う処理に関して説明する。

【００５５】

この場合、認証サーバ２００は、認証処理装置１００から生体認証用テンプレートの取得要求を受信したとする。

【００５６】

当該認証サーバ２００は、上述の取得要求が含む顧客ＩＤをキーに、認証テーブル２２５における該当顧客の各レコードのうち、直近使用フラグが「１」であるものを特定する（ｓ２００）。なお、認証処理装置１００は、フロー例１と同様、上述の取得要求の送信と共に、生体情報リーダー１１０での上述の顧客に対する生体情報読み取りを開始しているものとする。

【００５７】

次に認証サーバ２００は、上述のｓ２００で特定したレコードが示す生体認証用テンプレート、すなわち過去に認証対象となった生体部位の生体認証用テンプレートを、認証処理装置１００に返信する（ｓ２０１）。

【００５８】

一方、認証処理装置１００は、上述の認証サーバ２００から、上述の顧客に関して直近の過去に認証対象となった生体部位に関する生体認証用テンプレートを取得する（ｓ２０２）。以降、上述のフロー例１における、ｓ１０６～ｓ１１１４と同様の処理を、認証処理装置１００および認証サーバ２００で実行することとなる。

【００５９】

以上、本発明を実施するための最良の形態などについて具体的に説明したが、本発明はこれに限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。

【００６０】

こうした本実施形態によれば、テンプレート公開型生体認証基盤に基づく生体認証処理の特徴である、ＩＣチップ内蔵のキャッシュカードなど、生体情報を格納した媒体の保持・管理等が不要で、なりすまし等のリスクも非常に低いという利点と共に、ＡＴＭなど認証処理装置における認証対象者の生体情報読み取り動作と、認証サーバからの生体認証用テンプレートのダウンロードとを並行して処理することによる、効率的かつ迅速な生体認証処理が可能となる利点がある。認証サーバでは、認証処理装置にて認証対象者から指定された識別情報に基づいて、生体認証用テンプレートを一意に検索し、認証処理装置に返すことが出来る。よって、認証処理装置でも、いわゆる１：１認証を行うことが可能となり、生体認証の処理効率が更に向上することとなる。

【００６１】

また、一人の認証対象者に関して、複数の生体部位に関して、複数の生体認証用テンプレートを登録・管理することで、認証対象者における怪我や経年変化などに対応して、本人認証率と他人拒否率の向上を担保することも出来る。

【００６２】

すなわち、生体認証の処理を効率化し、認証処理時間を従来よりも低減可能となる。

【００６３】

本明細書の記載により、少なくとも次のことが明らかにされる。すなわち、本実施形態の認証処理装置において、前記認証処理装置は、前記認証サーバから、前記生体認証用テンプレートとして、テンプレート公開型生体認証基盤におけるポリシーに基づいて生成された生体認証用テンプレートを取得し、前記生体認証処理を、前記テンプレート公開型生

体認証基盤における認証手順に基づき前記認証サーバと共に実行するものである、としてもよい。

【００６４】

これによれば、ネットワークを介したセキュアな生体認証が効率的かつ迅速に実行可能となる。ひいては、生体認証の処理をより効率化し、認証処理時間を従来よりも低減可能となる。

【００６５】

また、本実施形態の生体認証システムにおいて、前記認証処理装置は、前記認証サーバから前記生体認証用テンプレートを取得するに際し、前記認証対象者における複数の生体部位のそれぞれに関して複数登録されている生体認証用テンプレートを取得するものである、としてもよい。

【００６６】

これによれば、認証対象者の生体部位がケガなどによって認証対象と出来ない状況等であっても、代替部位に関して生体認証が可能となる上、当該生体部位における生体情報の経年変化等にも対応して、本人認証率および他人拒否率を好適なものと出来る。ひいては、生体認証の処理をより効率化し、認証処理時間を従来よりも低減可能となる。

【００６７】

また、本実施形態の生体認証システムにおいて、前記認証処理装置は、前記生体認証処理に際し、前記認証サーバから得た、複数の生体部位のそれぞれに関する複数の生体認証用テンプレートのうち、各生体部位の間で順次選択した１つの生体認証用テンプレートと、前記生体情報読み取りにより得た生体情報との照合を、所定結果が得られるまで繰り返し実行するものである、としてもよい。

【００６８】

これによれば、一人の認証対象者に関して多数の生体部位に複数の生体認証用テンプレートが登録・管理されている状況にも対応して、認証効率を好適に維持し、ひいては、生体認証の処理をより効率化し、認証処理時間を従来よりも低減可能となる。

【００６９】

また、本実施形態の生体認証システムにおいて、前記認証処理装置は、前記生体認証用テンプレートを取得する処理に際し、前記認証対象者が指定した生体部位の情報と、前記認証対象者の識別情報とをキーに、当該認証対象者に関して登録済みの生体認証用テンプレートの取得要求を、前記認証サーバに送信すると共に、生体情報リーダーでの前記認証対象者に対する生体情報読み取りを実行し、当該生体情報読み取りの間に、前記認証サーバから、前記認証対象者の前記指定を受けた生体部位に関する生体認証用テンプレートを取得し、前記生体認証処理に際し、前記生体情報読み取りにより得た生体情報と、前記認証サーバから得た前記生体部位に関する生体認証用テンプレートとに基づく所定の生体認証処理を実行するものである、としてもよい。

【００７０】

これによれば、認証対象者の識別情報のみならず、その生体部位に関しても指定を受け、これに基づく、認証サーバでの生体認証用テンプレートの迅速な特定・読み取りが可能となり、ひいては、生体認証の処理をより効率化し、認証処理時間を従来よりも低減可能となる。

【００７１】

また、本実施形態の生体認証システムにおいて、前記認証処理装置は、前記生体認証用テンプレートを取得する処理に際し、前記認証対象者の識別情報をキーに、当該認証対象者に関して過去に認証対象となった生体部位に関して登録済みの生体認証用テンプレートの取得要求を、前記認証サーバに送信すると共に、生体情報リーダーでの前記認証対象者に対する生体情報読み取りを実行し、当該生体情報読み取りの間に、前記認証サーバから、前記認証対象者の前記過去に認証対象となった生体部位に関する生体認証用テンプレートを取得し、前記生体認証処理に際し、前記生体情報読み取りにより得た生体情報と、前記認証サーバから得た前記過去に認証対象となった生体部位に関する生体認証用テンプレ

ートとに基づく所定の生体認証処理を実行するものである、としてもよい。
【００７２】
これによれば、恐らく今回も認証対象とする確率が高いと推定される、過去に認証対象となった生体部位に関して生体認証用テンプレートを取得することが可能となり、ひいては、生体認証の処理をより効率化し、認証処理時間を従来よりも低減可能となる。
【００７３】
また、本実施形態の生体認証システムにおいて、認証対象者の識別情報と、当該認証対象者に関してテンプレート公開型生体認証基盤におけるポリシーに基づいて生成された生体認証用テンプレートとを対応付けて格納した認証テーブルを記憶する記憶装置と、前記認証処理装置からの前記取得要求に応じて、当該取得要求が示す前記認証対象者の識別情報をキーに前記認証テーブルで検索を実行し、当該検索で特定した生体認証用テンプレートを、前記認証処理装置に返信する処理と、前記テンプレート公開型生体認証基盤における認証手順に基づき前記認証処理装置と共に前記生体認証処理を実行する処理と、を行う演算装置と、を備えた認証サーバを更に含むとしてもよい。
【００７４】
これによれば、テンプレート公開型生体認証基盤に対応した認証サーバと、上述の認証処理装置との間での、認証対象者に関する生体認証の処理を、より効率的なものとし、ひいては、生体認証の処理をより効率化し、認証処理時間を従来よりも低減可能となる。
【００７５】
また、本実施形態の生体認証システムにおいて、前記認証サーバは、前記記憶装置の認証テーブルにおいて、前記認証対象者における複数の生体部位のそれぞれに関して、生体認証用テンプレートを複数保持しており、前記認証処理装置からの前記取得要求に応じて、前記認証対象者における複数の生体部位のそれぞれに関して複数登録されている生体認証用テンプレートを、前記認証テーブルから読み出して認証処理装置に返信するものである、としてもよい。
【００７６】
これによれば、各認証対象者の生体部位がケガなどによって認証対象と出来ない状況等であっても、代替部位に関して生体認証が可能となる上、当該生体部位における生体情報の経年変化等にも対応して、本人認証率および他人拒否率を好適なものと出来る。ひいては、生体認証の処理をより効率化し、認証処理時間を従来よりも低減可能となる。
【００７７】
また、本実施形態の生体認証システムにおいて、前記認証サーバは、前記認証処理装置からの前記取得要求に応じて、当該取得要求が示す、前記認証対象者が指定した生体部位の情報と、前記認証対象者の識別情報とをキーに、当該認証対象者の前記生体部位に関して登録済みの生体認証用テンプレートを、前記認証テーブルから読み出して認証処理装置に返信するものである、としてもよい。
【００７８】
これによれば、認証対象者の識別情報のみならず、その生体部位に関しても指定を受け、これに基づく、認証サーバでの生体認証用テンプレートの迅速な特定・読み取りが可能となり、ひいては、生体認証の処理をより効率化し、認証処理時間を従来よりも低減可能となる。
【００７９】
また、本実施形態の生体認証システムにおいて、前記認証サーバは、認証対象者における所定の生体部位に関して生体認証処理を実行した履歴を、記憶装置にて保持しており、前記認証処理装置からの前記取得要求に応じて、当該取得要求が示す前記認証対象者の識別情報をキーに前記履歴を検索し、当該認証対象者に関して過去に認証対象となった生体部位を特定し、当該生体部位に関して登録済みの生体認証用テンプレートを前記認証テーブルから読み出して認証処理装置に返信するものである、としてもよい。
【００８０】
これによれば、恐らく今回も認証対象とする確率が高いと推定される、過去に認証対象

となった生体部位に関して生体認証用テンプレートを特定し、認証処理装置に提供することが可能となり、ひいては、生体認証の処理をより効率化し、認証処理時間を従来よりも低減可能となる。

【００８１】

また、本実施形態の生体認証方法において、前記認証処理装置が、前記認証サーバから、前記生体認証用テンプレートとして、テンプレート公開型生体認証基盤におけるポリシーに基づいて生成された生体認証用テンプレートを取得し、前記生体認証処理を、前記テンプレート公開型生体認証基盤における認証手順に基づき前記認証サーバと共に実行する、としてもよい。

【００８２】

また、本実施形態の生体認証方法において、前記認証処理装置が、前記認証サーバから前記生体認証用テンプレートを取得するに際し、前記認証対象者における複数の生体部位のそれぞれに関して複数登録されている生体認証用テンプレートを取得する、としてもよい。

【００８３】

また、本実施形態の生体認証方法において、前記認証処理装置が、前記生体認証処理に際し、前記認証サーバから得た、複数の生体部位のそれぞれに関する複数の生体認証用テンプレートのうち、各生体部位の間で順次選択した１つの生体認証用テンプレートと、前記生体情報読み取りにより得た生体情報との照合を、所定結果が得られるまで繰り返し実行する、としてもよい。

【００８４】

また、本実施形態の生体認証方法において、前記認証処理装置が、前記生体認証用テンプレートを取得する処理に際し、前記認証対象者が指定した生体部位の情報と、前記認証対象者の識別情報とをキーに、当該認証対象者に関して登録済みの生体認証用テンプレートの取得要求を、前記認証サーバに送信すると共に、生体情報リーダーでの前記認証対象者に対する生体情報読み取りを実行し、当該生体情報読み取りの間に、前記認証サーバから、前記認証対象者の前記指定を受けた生体部位に関する生体認証用テンプレートを取得し、前記生体認証処理に際し、前記生体情報読み取りにより得た生体情報と、前記認証サーバから得た前記生体部位に関する生体認証用テンプレートとに基づく所定の生体認証処理を実行する、としてもよい。

【００８５】

また、本実施形態の生体認証方法において、前記認証処理装置が、前記生体認証用テンプレートを取得する処理に際し、前記認証対象者の識別情報をキーに、当該認証対象者に関して過去に認証対象となった生体部位に関して登録済みの生体認証用テンプレートの取得要求を、前記認証サーバに送信すると共に、生体情報リーダーでの前記認証対象者に対する生体情報読み取りを実行し、当該生体情報読み取りの間に、前記認証サーバから、前記認証対象者の前記過去に認証対象となった生体部位に関する生体認証用テンプレートを取得し、前記生体認証処理に際し、前記生体情報読み取りにより得た生体情報と、前記認証サーバから得た前記過去に認証対象となった生体部位に関する生体認証用テンプレートとに基づく所定の生体認証処理を実行する、としてもよい。

【００８６】

また、本実施形態の生体認証方法において、認証対象者の識別情報と、当該認証対象者に関してテンプレート公開型生体認証基盤におけるポリシーに基づいて生成された生体認証用テンプレートとを対応付けて格納した認証テーブルを記憶する記憶装置を備えた認証サーバが、前記認証処理装置からの前記取得要求に応じて、当該取得要求が示す前記認証対象者の識別情報をキーに前記認証テーブルで検索を実行し、当該検索で特定した生体認証用テンプレートを、前記認証処理装置に返信する処理と、前記テンプレート公開型生体認証基盤における認証手順に基づき前記認証処理装置と共に前記生体認証処理を実行する処理と、としてもよい。

【００８７】

また、本実施形態の生体認証方法において、前記認証サーバが、前記記憶装置の認証テーブルにおいて、前記認証対象者における複数の生体部位のそれぞれに関して、生体認証用テンプレートを複数保持しており、前記認証処理装置からの前記取得要求に応じて、前記認証対象者における複数の生体部位のそれぞれに関して複数登録されている生体認証用テンプレートを、前記認証テーブルから読み出して認証処理装置に返信する、としてもよい。

【００８８】

また、本実施形態の生体認証方法において、前記認証サーバが、前記認証処理装置からの前記取得要求に応じて、当該取得要求が示す、前記認証対象者が指定した生体部位の情報と、前記認証対象者の識別情報とをキーに、当該認証対象者の前記生体部位に関して登録済みの生体認証用テンプレートを、前記認証テーブルから読み出して認証処理装置に返信する、としてもよい。

【００８９】

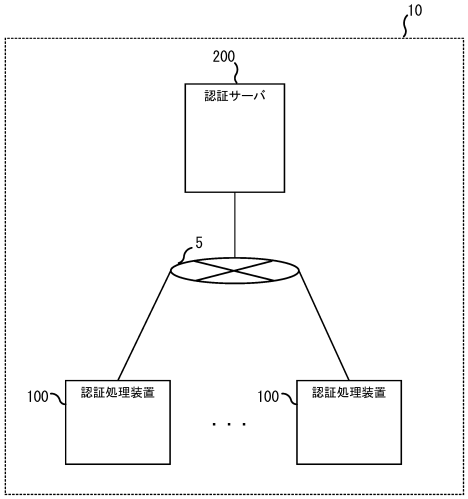
また、本実施形態の生体認証方法において、前記認証サーバが、認証対象者における所定の生体部位に関して生体認証処理を実行した履歴を、記憶装置にて保持しており、前記認証処理装置からの前記取得要求に応じて、当該取得要求が示す前記認証対象者の識別情報をキーに前記履歴を検索し、当該認証対象者に関して過去に認証対象となった生体部位を特定し、当該生体部位に関して登録済みの生体認証用テンプレートを前記認証テーブルから読み出して認証処理装置に返信する、としてもよい。

【符号の説明】

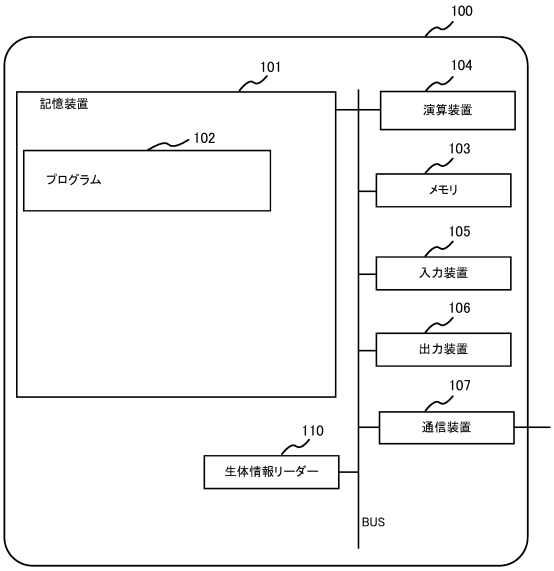
【００９０】

５　ネットワーク
１０　認証処理システム
１００　認証処理装置
１０１　記憶装置
１０２　プログラム
１０３　メモリ
１０４　演算装置
１０５　入力装置
１０６　出力装置
１０７　通信装置
１１０　生体情報リーダー
２００　認証サーバ
２０１　記憶装置
２０２　プログラム
２０３　メモリ
２０４　演算装置
２０５　通信装置
２２５　認証テーブル

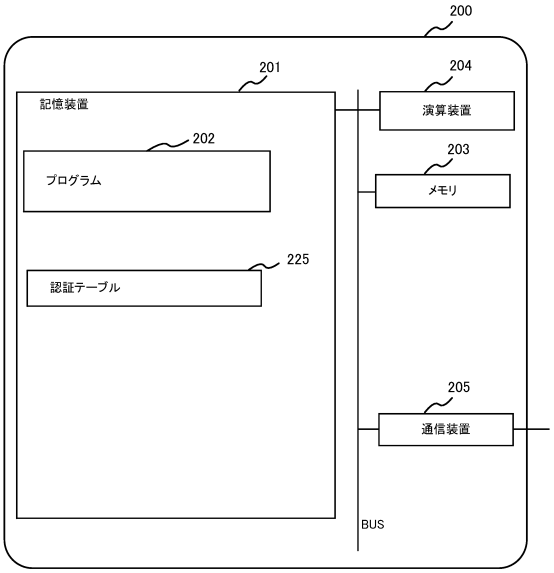
【図１】



【図２】



【図３】

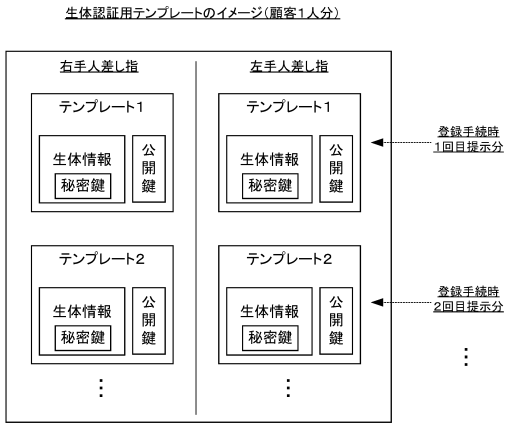


【図４】

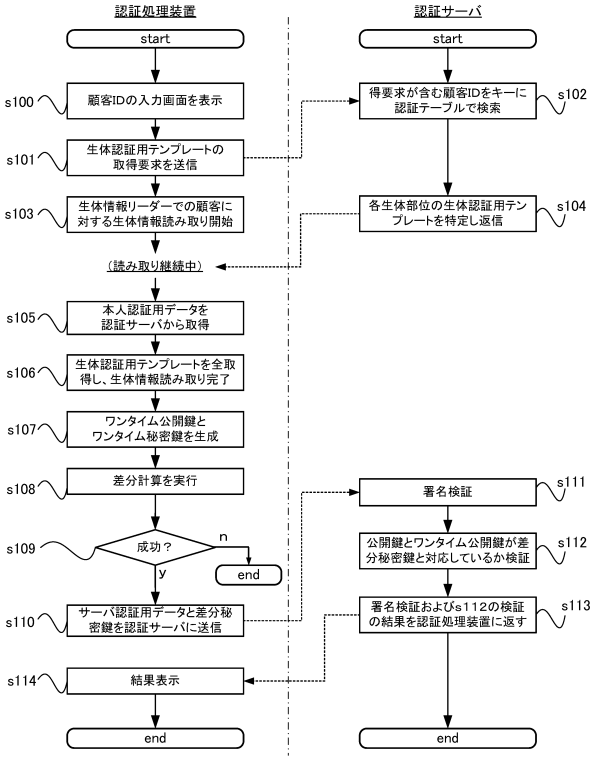
認証テーブル 225

顧客ID	生体部位	テンプレート1	テンプレート2	…	直近使用フラグ	…
00001	R02	＊＊＊＊＊	＊＊＊＊＊	…	1	…
	…	…	…	…	0	…
	L02	＊＊＊＊＊	＊＊＊＊＊	…	0	…
	…	…	…	…	0	…
00002	R02	＊＊＊＊＊	＊＊＊＊＊	…	0	…
	…	…	…	…	0	…
	L02	＊＊＊＊＊	＊＊＊＊＊	…	1	…
	…	…	…	…	0	…
	R03	＊＊＊＊＊	＊＊＊＊＊	…	0	…
	…	…	…	…	0	…
…	…	…	…	…	…	…

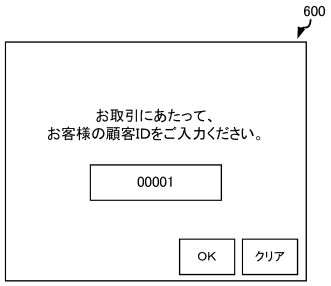
【図５】


生体認証用テンプレートのイメージ（顧客１人分）
右手人差し指
左手人差し指
テンプレート1
テンプレート2
生体情報
秘密鍵
公開鍵
登録手続時
1回目提示分
登録手続時
2回目提示分

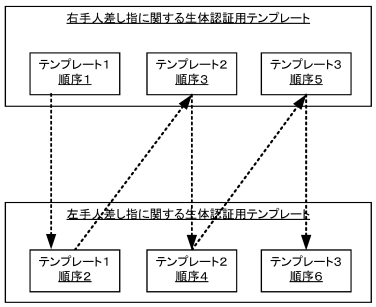
【図６】


認証処理装置
認証サーバ
start
顧客IDの入力画面を表示
生体認証用テンプレートの取得要求を送信
生体情報リーダーでの顧客に対する生体情報読み取り開始
（読み取り継続中）
本人認証用データを認証サーバから取得
生体認証用テンプレートを全取得し、生体情報読み取り完了
ワンタイム公開鍵とワンタイム秘密鍵を生成
差分計算を実行
成功？
n
y
end
サーバ認証用データと差分秘密鍵を認証サーバに送信
結果表示
得要求が含む顧客IDをキーに認証テーブルで検索
各生体部位の生体認証用テンプレートを特定し返信
署名検証
公開鍵とワンタイム公開鍵が差分秘密鍵と対応しているか検証
署名検証およびs112の検証の結果を認証処理装置に返す
s100
s101
s102
s103
s104
s105
s106
s107
s108
s109
s110
s111
s112
s113
s114

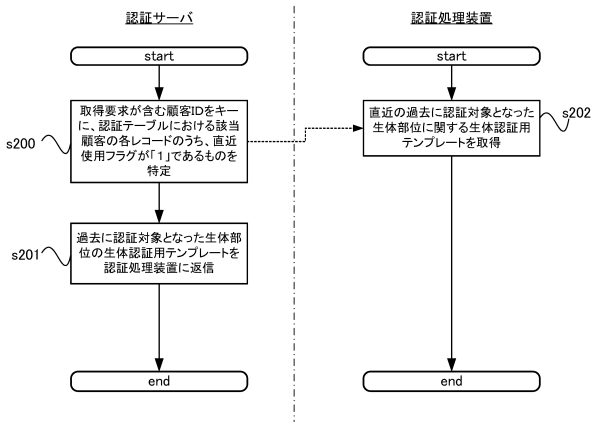
【図７】


600
お取引にあたって、
お客様の顧客IDをご入力ください。
00001
OK
クリア

【図８】


右手人差し指に関する生体認証用テンプレート
テンプレート1
順序1
テンプレート2
順序3
テンプレート3
順序5
左手人差し指に関する生体認証用テンプレート
テンプレート1
順序2
テンプレート2
順序4
テンプレート3
順序6

【図９】


認証サーバ
認証処理装置
start
取得要求が含む顧客IDをキーに、認証テーブルにおける該当顧客の各レコードのうち、直近使用フラグが「1」であるものを特定
過去に認証対象となった生体部位の生体認証用テンプレートを認証処理装置に返信
直近の過去に認証対象となった生体部位に関する生体認証用テンプレートを取得
end
s200
s201
s202

フロントページの続き

審査官　金沢　史明

(56)参考文献　特開２００８－２１７２５７（ＪＰ，Ａ）
特開２０１３－１２２６８０（ＪＰ，Ａ）
特開２０１０－１１３４３３（ＪＰ，Ａ）
特開２０１４－０１６７２６（ＪＰ，Ａ）
特開２０１６－１１５１０８（ＪＰ，Ａ）
特開２００６－００７４６４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３２