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

特許第5360192号
(P5360192)

(45)発行日　平成25年12月4日(2013.12.4)　(24)登録日　平成25年9月13日(2013.9.13)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/20	131E
G06F 21/32	(2013.01)	G06F	21/20	132
G06K 17/00	(2006.01)	G06K	17/00	T
G06K 19/10	(2006.01)	G06K	17/00	V
		G06K	19/00	R

請求項の数 16　(全 15 頁)

(21)出願番号　特願2011-503631 (P2011-503631)
(86)(22)出願日　平成21年3月13日(2009.3.13)
(86)国際出願番号　PCT/JP2009/054938
(87)国際公開番号　WO2010/103663
(87)国際公開日　平成22年9月16日(2010.9.16)
審査請求日　平成23年9月21日(2011.9.21)

(73)特許権者　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　100087480
弁理士　片山　修平
(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

審査官　田中　慎太郎

最終頁に続く

(54)【発明の名称】個人認証システムおよび個人認証方法

(57)【特許請求の範囲】
【請求項１】
利用者の個人情報を明かさずに行われた申請に応じて提供した匿名ＩＤに対応させて照合用生体情報を記憶する認証サーバと、
利用者の生体情報を取得する生体センサと、
電子記憶媒体に記憶された匿名ＩＤを取得し、前記生体センサによって取得された生体情報とともに前記認証サーバに送信する端末と、を備え、
前記認証サーバは、前記生体センサによって取得された生体情報が前記匿名ＩＤに対応する照合用生体情報との間で所定の一致が得られた場合に、前記電子記憶媒体に記憶された個人情報へのアクセスに必要な情報を前記端末に送信することを特徴とする個人認証システム。
【請求項２】
前記電子記憶媒体は、ファイアウォールによって前記匿名ＩＤにかかるアプリケーション領域と前記個人情報にかかるアプリケーション領域との間のアクセスが禁止されたマルチアプリカードであることを特徴とする請求項１記載の個人認証システム。
【請求項３】
前記認証サーバは、前記端末が前記電子記憶媒体の個人情報へのアクセスに必要な情報として、個人情報アクセスＰＩＮを記憶することを特徴とする請求項１または２記載の個人認証システム。
【請求項４】

前記電子記憶媒体は、個人情報として、利用者ＩＤおよび管理サーバアクセスキーを記憶し、
前記端末は、前記電子記憶媒体の個人情報へのアクセスに必要な情報を前記認証サーバから受信した場合に、前記利用者ＩＤおよび前記管理サーバアクセスキーを読み込むことによって、個人情報管理サーバに記憶された前記利用者の個人情報にアクセス可能であることを特徴とする請求項１～３のいずれかに記載の個人認証システム。
【請求項５】
前記電子記憶媒体は、個人情報を記憶する個人情報領域に、所定の形式で算出された匿名ＩＤのハッシュ値を記憶し、
前記端末は、前記匿名ＩＤとともに前記ハッシュ値を前記認証サーバに送信することを特徴とする請求項１～４のいずれかに記載の個人認証システム。
【請求項６】
前記端末は、前記電子記憶媒体において前記個人情報を記憶する個人情報領域および前記匿名ＩＤを記憶する匿名ＩＤ領域の少なくとも一方の所定の形式で算出されたハッシュ値を他方に添付して確認可能であることを特徴とする請求項１～５のいずれかに記載の個人認証システム。
【請求項７】
前記電子記憶媒体は、前記ファイアウォールによって互いにアクセスが禁止された複数のアプリケーション領域に、異なるサービスの個人情報を格納し、
前記匿名ＩＤは、前記異なるサービスの個人情報のそれぞれに対して設定されていることを特徴とする請求項１～６のいずれかに記載の個人認証システム。
【請求項８】
前記認証サーバは、前記異なるサービスに対して異なる照合用生体情報を記憶していることを特徴とする請求項７記載の個人認証システム。
【請求項９】
利用者の個人情報を明かさずに行われた申請に応じて提供した匿名ＩＤに対応させて照合用生体情報を認証サーバに記憶するステップと、
生体センサにより利用者の生体情報を取得するステップと、
端末を用いて、電子記憶媒体に記憶された匿名ＩＤを取得し、前記生体センサによって取得された生体情報とともに前記認証サーバに送信するステップと、
前記生体センサによって取得された生体情報が前記匿名ＩＤに対応する照合用生体情報との間で所定の一致が得られた場合に、前記電子記憶媒体に記憶された個人情報へのアクセスに必要な情報を前記認証サーバから前記端末に送信するステップと、を含むことを特徴とする個人認証方法。
【請求項１０】
前記電子記憶媒体は、ファイアウォールによって前記匿名ＩＤにかかるアプリケーション領域と前記個人情報にかかるアプリケーション領域との間のアクセスが禁止されたマルチアプリカードであることを特徴とする請求項９記載の個人認証方法。
【請求項１１】
前記認証サーバは、前記端末が前記電子記憶媒体の個人情報へのアクセスに必要な情報として、個人情報アクセスＰＩＮを記憶することを特徴とする請求項９または１０記載の個人認証方法。
【請求項１２】
前記電子記憶媒体は、個人情報として、利用者ＩＤおよび管理サーバアクセスキーを記憶し、
前記電子記憶媒体の個人情報へのアクセスに必要な情報を前記端末が前記認証サーバから受信した場合に、前記端末を用いて前記利用者ＩＤおよび前記管理サーバアクセスキーを読み込むことによって、個人情報管理サーバに記憶された前記利用者の個人情報にアクセスするステップを含むことを特徴とする請求項９～１１のいずれかに記載の個人認証方法。

【請求項１３】
前記電子記憶媒体は、個人情報を記憶する個人情報領域に、所定の形式で算出された匿名ＩＤのハッシュ値を記憶し、
前記端末を用いて、前記匿名ＩＤとともに前記ハッシュ値を前記認証サーバに送信するステップを含むことを特徴とする請求項９～１２のいずれかに記載の個人認証方法。
【請求項１４】
前記電子記憶媒体において前記個人情報を記憶する個人情報領域および前記匿名ＩＤを記憶する匿名ＩＤ領域の少なくとも一方の所定の形式で算出されたハッシュ値を他方に添付して確認するステップを含むことを特徴とする請求項９～１３のいずれかに記載の個人認証方法。
【請求項１５】
前記電子記憶媒体は、前記ファイアウォールによって互いにアクセスが禁止された複数のアプリケーション領域に、異なるサービスの個人情報を格納し、
前記匿名ＩＤは、前記異なるサービスの個人情報のそれぞれに対して設定されていることを特徴とする請求項９～１４のいずれかに記載の個人認証方法。
【請求項１６】
前記認証サーバは、前記異なるサービスに対して異なる照合用生体情報を記憶していることを特徴とする請求項１５記載の個人認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子記憶媒体技術および生体認証技術を連携させた個人認証システムおよび個人認証方法に関する。
【背景技術】
【０００２】
従来の電子記憶媒体および生体認証の連携技術では、電子記憶媒体内に個人情報および生体情報を記憶しておき、生体情報で本人確認を行った後で個人情報へのアクセスを許可するという技術が開示されている（例えば、特許文献１参照）。
【０００３】
また、認証サーバに個人情報と生体情報を記憶しておき、送られてきた生体情報が本人のものであることおよび本人の生体情報であることを確認した場合に情報へのアクセスを許可する技術が開示されている（例えば、特許文献２参照）。
【０００４】
【特許文献１】特開昭６１－１９９１６２号公報
【特許文献２】国際公開第２００１／０４２９３８号
【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，上記技術では、個人情報および生体情報を１つの媒体で管理することが要求される。特に電子記憶媒体（例えばＩＣカード）は実際の記憶者（利用者）のものではなく、ＩＣカードの所有母体から記憶者に貸与されているものである。ＩＣカードに生体情報を記憶した場合は、所有母体がＩＣカードのライフサイクル（登録、発行、停止および廃棄）を厳密に管理する必要があるため、カードのように散逸しやすいものに生体情報を入れた場合には管理が煩雑になる。また、ＩＣカードの脆弱性が露呈した場合は、個人情報と生体情報の両方を危険に晒すことになる。
【０００６】
本発明は上記課題に鑑みなされたものであり、個人情報および生体情報の安全性を向上させることができる個人認証システムおよび個人認証方法を提供することを目的とする。
【課題を解決するための手段】
【０００７】

上記課題を解決するために、明細書開示の個人認証システムは、利用者の個人情報を明かさずに行われた申請に応じて提供した匿名ＩＤに対応させて照合用生体情報を記憶する認証サーバと、利用者の生体情報を取得する生体センサと、電子記憶媒体に記憶された匿名ＩＤを取得し生体センサによって取得された生体情報とともに認証サーバに送信する端末と、を備え、認証サーバは、生体センサによって取得された生体情報が匿名ＩＤに対応する照合用生体情報との間で所定の一致が得られた場合に、電子記憶媒体に記憶された個人情報へのアクセスに必要な情報を端末に送信するものである。

【０００８】

上記課題を解決するために、明細書開示の個人認証方法は、利用者の個人情報を明かさずに行われた申請に応じて提供した匿名ＩＤに対応させて照合用生体情報を認証サーバに記憶するステップと、生体センサにより利用者の生体情報を取得するステップと、端末を用いて電子記憶媒体に記憶された匿名ＩＤを取得し生体センサによって取得された生体情報とともに認証サーバに送信するステップと、生体センサによって取得された生体情報が匿名ＩＤに対応する照合用生体情報との間で所定の一致が得られた場合に電子記憶媒体に記憶された個人情報へのアクセスに必要な情報を認証サーバから端末に送信するステップと、を含むものである。

【発明の効果】

【０００９】

明細書開示の個人認証システムおよび個人認証方法によれば、電子記憶媒体と認証サーバとに、本人確認に必要な情報を分散して管理することができる。それにより、個人情報および生体情報の安全性を向上させることができる。

【図面の簡単な説明】

【００１０】

【図１】実施例１に係る個人認証システムの構成を説明するためのブロック図である。
【図２】ＩＣカードへの個人情報の登録方法の流れを記載した例である。
【図３】ＩＣカードを発行する手順について説明するための図である。
【図４】実施例２に係る個人認証システムの構成を説明するためのブロック図である。
【図５】実施例３に係る個人認証システムの構成を説明するためのブロック図である。
【図６】実施例３の変形例に係る個人認証システムの構成を説明するためのブロック図である。
【図７】実施例４に係る個人認証システムの構成を説明するためのブロック図である。
【図８】ハッシュ値の作成工程を説明するための図である。
【図９】実施例４の変形例に係る個人認証システムの構成を説明するためのブロック図である。
【図１０】ハッシュ値の作成工程を説明するための図である。
【図１１】複数の個人情報を記憶したＩＣカードを説明するための図である。
【図１２】実施例５に係る個人認証システムの構成を説明するためのブロック図である。
【図１３】実施例５の変形例に係る個人認証システムの構成を説明するためのブロック図である。
【図１４】各実施例に係るＩＣカード端末および生体情報認証サーバの機器構成図である。

【発明を実施するための最良の形態】

【００１１】

以下、図面を参照しつつ、本発明の実施例について説明する。

【実施例１】

【００１２】

図１は、実施例１に係る個人認証システムの構成を説明するためのブロック図である。本実施例においては、電子記憶媒体の一例としてＩＣカードを用いる。図１で説明されるように、実施例１に係る個人認証システムは、ＩＣカード端末１００と生体情報認証サーバ２００とがネットワークを介して通信可能に接続された構成を有する。この場合のネッ

トワークとして、公衆回線網、インターネット、イントラネット等の通信網を用いることができる。

【００１３】

ＩＣカード端末１００は、生体センサ１１０、カードリーダ１２０、生体認証部１３０、およびＩＣカード認証部１４０を備える。生体センサ１１０は、ユーザの生体情報を取得するセンサである。本実施例においては、生体センサ１１０の一例として、指紋センサを用いる。カードリーダ１２０は、後述するＩＣカード３００から情報を読み取り、ＩＣカード３００に情報を書き込むための装置である。カードリーダ１２０は、接触型リーダでもよく、非接触型リーダであってもよい。

【００１４】

生体認証部１３０は、通信機能部１３１、生体情報入力部１３２、生体情報処理部１３３、相互認証機能部１３４、および匿名ＩＤアクセス機能部１３５として機能する。ＩＣカード認証部１４０は、通信機能部１４１、相互認証機能部１４２、ＰＩＮ入力機能部１４３、および個人情報アクセス部１４４として機能する。ここで、「ＰＩＮ」とは、Personal Identification Number（暗証番号）のことである。生体情報認証サーバ２００は、データベースに匿名ＩＤ情報、生体情報、およびＩＣカードＰＩＮを記憶する。このとき、生体認証サーバは、匿名ＩＤ情報、生体情報、およびＩＣカードＰＩＮをネットワーク等を介して物理的に分離して管理してもよい。また、生体情報、ＩＣカードＰＩＮは暗号化して保存してもよい。

【００１５】

本実施例に係る個人認証システムにおいて使用されるＩＣカード３００は、複数のアプリケーション領域を有するマルチアプリカードである。ＩＣカード３００は、ファイアウォールによって互いにアクセスが禁止されたアプリケーション領域を複数備える。ファイアウォールの例として、属性情報に従ってメモリへのアクセス許可を行う属性制御方式、ページ番号と論理アドレスとでアクセス許可を行うページ管理方式、仮想マシンがＡＰ（アプリケーション）のプログラムを解釈実行する仮想マシン方式等を用いることができる。なお、属性情報とは、読み出し専用、読み書き可能、実行可能、アクセス不可等の属性を表わす。ページとは、メモリ上でのＡＰの論理的配置を表わす単位のことである。

【００１６】

本実施例においては、ＩＣカード３００は、所定のアプリケーション領域に匿名ＩＤ情報部３１０を備え、他のアプリケーション領域に個人情報部３２０を備える。匿名ＩＤ情報部３１０は、相互認証機能部３１１および匿名ＩＤ情報記憶部３１２として機能する。個人情報部３２０は、相互認証機能部３２１、ＰＩＮロック機能部３２２、および個人情報記憶部３２３として機能する。

【００１７】

図２は、ＩＣカード３００への個人情報の登録方法の流れを記載した例である。図２においては、一例として、生体情報認証サーバ２００を管理する生体認証サーバサービスプロバイダと、ＩＣカード３００を発行するＩＣカード発行サービスプロバイダとが独立している例が記載されている。なお、ＩＣカード発行サービスプロバイダの下に、最終的なサービスを提供するプロバイダが１または複数存在していてもよい。

【００１８】

利用者は、プリペイド方式により利用権を購入し（ステップＳ１）、個人情報を明かすことなく匿名のＩＤ申請を行う（ステップＳ２）。生体認証サーバサービスプロバイダは、匿名ＩＤを提供するとともに、証明書を発行する（ステップＳ３）。また、生体認証サーバサービスプロバイダは、利用者から登録用の生体データの提供を受け（ステップＳ４）、提供を受けた生体データを生体情報認証サーバ２００に登録する（ステップＳ５）。次に、利用者は、証明書を受け取り、匿名ＩＤを受け取るとともに、連絡用としてメールアドレス等の通信手段を生体認証サーバサービスプロバイダに提供する（ステップＳ６）。

【００１９】

その後、利用者は、ＩＣカード発行サービスプロバイダにＩＣカード３００の発行申請を行う（ステップＳ７）とともに、個人情報をＩＣカード発行サービスプロバイダに提供する（ステップＳ８）。ＩＣカード発行サービスプロバイダは、ＩＣカード３００に利用者の個人情報およびＩＤを書き込む（ステップＳ９）。次に、ＩＣカード発行サービスプロバイダは、ＩＣカード３００を発行し、匿名ＩＤアクセスＰＩＮを発行し、個人情報アクセスＰＩＮを発行する（ステップＳ１０）。

【００２０】

次に、利用者は、ＩＣカード発行サービスプロバイダを介して、匿名ＩＤアクセスＰＩＮを用いて自身の匿名ＩＤをＩＣカード３００に登録する（ステップＳ１１）。次に、生体認証サーバサービスプロバイダは、個人情報にアクセスするためのＰＩＮを生体情報認証サーバ２００に登録する（ステップＳ１２）。以上の流れによって、生体情報が生体情報認証サーバ２００に登録されるとともに、ＩＣカード３００に個人情報が登録される。

【００２１】

図３は、ＩＣカード３００を発行する手順について説明するための図である。図３において、ＩＣカード業者はＩＣカードを製造する業者（０次発行者）であり、ＩＣカード発行サービス業者はＩＣカード３００の個人情報部３２０のフォーマット仕様を作成する業者（１次発行者）であり、認証サービス業者は匿名ＩＤ情報部３１０のフォーマット仕様を作成する業者である。

【００２２】

図３で説明されるように、ＩＣカード業者は、初期設定によってカードフォーマットを作成して輸送鍵を設定することによって、ＩＣカード３００をマルチアプリカード仕様に設定する（ステップＳ２１）。次に、ＩＣカード発行サービス業者は、個人情報部３２０用に、ＩＣカード３００のカードフォーマット仕様を設定する（ステップＳ２２）。また、認証サービス業者は、匿名ＩＤ情報部３１０用に、ＩＣカード３００のカードフォーマット仕様を設定する（ステップＳ２３）。

【００２３】

次に、ＩＣカード発行サービス業者は、ＩＣカード３００にカードアプリケーションを書き込むことによって、ＩＣカード３００内に個人情報部３２０を作成する（ステップＳ２４）。また、認証サービス業者は、ＩＣカード３００にカードアプリケーションを書き込むことによって、匿名ＩＤ情報部３１０を作成する（ステップＳ２５）。次に、ＩＣカード発行サービス業者は、ＩＣカード３００を発行する（ステップＳ２６）。

【００２４】

以上のように、ＩＣカードの製造業者と、個人情報部３２０を設定する業者と、匿名ＩＤ情報部３１０を設定する業者と、を独立させることが可能である。それにより、個人情報の安全性が向上する。

【００２５】

続いて、図１を参照しつつ、実施例１に係る個人認証システムの動作について説明する。まず、生体センサ１１０は、利用者の生体情報を取得する。生体センサ１１０によって取得された生体情報は、生体情報入力部１３２によって生体情報処理部１３３に入力される。生体情報処理部１３３は、生体情報を照合用のデータに変換する。

【００２６】

次に、相互認証機能部１３４は、ＩＣカードリーダ１２０を介して、ＩＣカード３００の相互認証機能部３１１と相互認証を行う。相互認証が完了すれば、匿名ＩＤアクセス機能部１３５は、匿名ＩＤ情報記憶部３１２から利用者の匿名ＩＤ情報を読み取る。通信機能部１３１は、利用者の匿名ＩＤおよび生体情報を生体情報認証サーバ２００に送信する。

【００２７】

生体情報認証サーバ２００は、受信した生体情報の照合を行う。この場合、生体情報認証サーバ２００は、登録済みの匿名ＩＤ利用者に対応する生体情報と所定の一致を確認し、登録済みの匿名ＩＤ利用者の生体情報であると判断した場合には、ＩＣカードＰＩＮを

ＩＣカード端末１００に送信する。このときＰＩＮを暗号化して送ってもよい。
【００２８】
通信機能部１４１は、生体情報認証サーバ２００からＩＣカードＰＩＮを受信する。それにより、相互認証機能部１４２は、ＩＣカード３００の相互認証機能部３２１と相互認証を行う。相互認証が完了すれば、ＰＩＮ入力機能部１４３は、ＩＣカード３００のＰＩＮロック機能部３２２にＩＣカードＰＩＮの情報を入力する。生体情報認証サーバ２００から受信したＩＣカードピンとＩＣカード３００に記憶されたＩＣカードピンとが一致すれば、ＰＩＮロック機能部３２２は、ＰＩＮロックを解除する。次に、個人情報アクセス部１４４は、ＩＣカード３００の個人情報記憶部３２３から個人情報を読み取る。以上の動作によって、利用者は、自身の個人情報にアクセスすることができる。
【００２９】
本実施例によれば、個人情報と生体情報とをＩＣカード３００と生体情報認証サーバ２００とに分離して記憶することができる。それにより、生体情報認証サーバ２００に記憶してある生体情報の匿名化を図ることができる。また、機微情報である生体情報を散逸しやすいカード媒体に記憶するのではなく生体情報認証サーバ２００で記憶することによって、認証用生体情報のライフサイクル管理を適確に行うことができる。
【００３０】
また、利用者がＩＣカード３００を紛失した場合にＩＣカード３００を再発行する場合においても、カード内に生体情報が記憶されていないため利用者が再度生体情報の登録に出向く必要がない。したがって、カードに必要な情報を入力することによって、郵送でカードを再発行することができる。
【００３１】
また、分散して情報を記憶することによって、ＩＣカード３００の脆弱性が発見された場合に、個人情報（カード情報）および生体情報の両方を危険にさらすことがない。また、ＩＣカード３００およびＩＣカード端末１００が個人情報および生体情報を分離して扱う構造を有しているため、匿名性を記憶することができる。
【００３２】
なお、ＩＣカード端末１００は、パーソナルコンピュータに接続された装置であってもよく、独立して動作するものであってもよい。また、ＩＣカード端末１００とＩＣカード３００との間に、セキュアメッセージング等の手段で通信経路の安全を確保してもよい。さらに、ＳＳＬ（Secure Socket Layer）等の暗号化通信手段を用いてＩＣカード端末１００と生体情報認証サーバ２００との間の通信を行ってもよい。
【実施例２】
【００３３】
実施例２においては、ＩＣカード内の個人情報へのアクセスが許可された場合に、個人情報管理サーバに記憶された個人情報にアクセス可能とする例について説明する。
【００３４】
図４は、実施例２に係る個人認証システムの構成を説明するためのブロック図である。図４においては、個人情報管理サーバ４００がさらに備わっている。また、ＩＣカード３００の代わりにＩＣカード３００ａが記載されている。ＩＣカード３００ａがＩＣカード３００と異なる点は、個人情報部３２０の代わりに個人情報部３２０ａが備わり、カード利用者ＩＤ記憶部３２４および管理サーバアクセスキー記憶部３２５がさらに備わっている点である。
【００３５】
本実施例においては、ＰＩＮロックが解除された場合に、個人情報アクセス機能部１４４は、個人情報記憶部３２３にアクセスすることができる。この場合、個人情報アクセス機能部１４４は、個人情報記憶部３２３を介して、カード利用者ＩＤ記憶部３２４からカード利用者ＩＤを読み取るとともに、管理サーバアクセスキー記憶部３２５から管理サーバアクセスキーを読み取る。
【００３６】

次に、通信機能部１４１は、カード利用者ＩＤおよび管理サーバアクセスキーを個人情報管理サーバ４００に送信する。それにより、利用者は、個人情報管理サーバ４００に記憶された個人情報にＩＣカード端末１００を介してアクセスすることができる。

【００３７】

本実施例によれば、生体情報認証サーバ２００と個人情報管理サーバ４００とに本人確認に必要な情報を分散しておくことができる。それにより、個人情報および生体情報の安全性を向上させることができる。また、個人情報管理サーバ４００に個人情報を記憶しておくことができる。それにより、ＩＣカード３００を紛失した場合においても、個人情報の漏洩が防止される。

【実施例３】

【００３８】

複数の生体情報認証サーバサービスを設定しようとすれば、複数のサービスから１つのサービスを選択可能な技術が必要となる。そこで、実施例３においては、生体情報認証サーバサービスプロバイダリストをＩＣカードに持たせる。

【００３９】

図５は、実施例３に係る個人認証システムの構成を説明するためのブロック図である。実施例３に係る個人認証システムが実施例２に係る個人認証システムと異なる点は、ＩＣカード３００ａの代わりにＩＣカード３００ｂを用いる点である。

【００４０】

図５において説明されるように、ＩＣカード３００ｂがＩＣカード３００ａと異なる点は、サービスリスト部３３０がさらに設けられている点である。サービスリスト部３３０は、相互認証機能部３３１および対応サービスリスト記憶部３３２として機能する。対応サービスリスト記憶部３３２は、複数の生体情報認証サーバサービスの一覧を記憶している。また、サービスリスト部３３０は、ファイアウォールによって、個人情報部３２０および匿名ＩＤ情報部３１０との間で相互アクセスが禁止されている。

【００４１】

本実施例においては、相互認証機能部１３４と相互認証機能部３３１との間の相互認証が完了した場合に、ＩＣカード端末１００は、対応サービスリスト記憶部３３２から複数の生体情報認証サーバサービスを読み出す。例えば、ＩＣカード端末１００は、ディスプレイに複数の生体情報認証サーバサービスを一覧として表示し、利用者にいずれかのサービスを選択させてもよい。それにより、利用者は、複数の生体情報認証サーバサービスから所望のサービスを選択することができる。

【００４２】

（変形例）

図６は、実施例３の変形例に係る個人認証システムの構成を説明するためのブロック図である。本変形例においては、ＩＣカード端末がサービスリストを記憶する。本変形例に係る個人認証システムが実施例２に係る個人認証システムと異なる点は、ＩＣカード端末１００の代わりにＩＣカード端末１００ｃが備わっている点である。図６において説明されるように、ＩＣカード端末１００ｃがＩＣカード端末１００と異なる点は、対応サービスリスト記憶部１４５がさらに備わっている点である。対応サービスリスト記憶部１４５は、複数の生体情報認証サーバサービスの一覧を記憶している。

【００４３】

本実施例においては、ＩＣカード端末１００ｃは、対応サービスリスト記憶部１４５から複数の生体情報認証サーバサービスを読み出す。その後、ＩＣカード端末１００ｃは、ディスプレイに複数の生体情報認証サーバサービスを一覧として表示し、利用者にいずれかのサービスを選択させてもよい。それにより、利用者は、複数の生体情報認証サーバサービスから所望のサービスを選択することができる。

【実施例４】

【００４４】

ＩＣカード３００内部での個人情報領域と匿名ＩＤ領域との分離の完全性を保障するた

めに、所定の形式で算出された匿名ＩＤのハッシュ値を個人情報領域に記憶してもよい。

【００４５】

図７は、実施例４に係る個人認証システムの構成を説明するためのブロック図である。実施例４に係る個人認証システムが実施例２に係る個人認証システムと異なる点は、ＩＣカード３００ａの代わりにＩＣカード３００ｄを用いる点および生体情報認証サーバ２００の代わりに生体情報認証サーバ２００ｄを用いる点である。

【００４６】

図７において説明されるように、ＩＣカード３００ｄは、個人情報部３２０の代わりに個人情報部３２０ｄを備える。個人情報部３２０ｄは、匿名ＩＤハッシュ値記憶部３２６をさらに備える。匿名ＩＤハッシュ値記憶部３２６は、所定の形式で算出された匿名ＩＤのハッシュ値を記憶する。また、生体情報認証サーバ２００ｄは、匿名ＩＤハッシュ値を記憶する。

【００４７】

本実施例においては、ＩＣカード端末１００から匿名ＩＤを生体情報認証サーバ２００ｄに送信する際に、匿名ＩＤハッシュ値が同時に送信される。生体情報認証サーバ２００ｄは、記憶している匿名ＩＤハッシュ値と受信した匿名ＩＤハッシュ値とが一致する場合に、生体認証を行う。それにより、ＩＣカード３００ｄ内における匿名ＩＤ情報部３１０と個人情報部３２０ｄとの分離の完全性を保障することができる。

【００４８】

図８は、ハッシュ値の作成工程を説明するための図である。匿名ＩＤに対して所定のハッシュ関数処理を施すことによって、匿名ＩＤをハッシュ化することができる。このハッシュ化された匿名ＩＤを匿名ＩＤハッシュ値記憶部３２６に記憶することによって、ハッシュ値を個人情報部３２０ｄに記憶させることができる。ハッシュ関数には、ＭＤ５、ＳＨＡ－１、ＳＨＡ－２５６、ＳＨＡ－５１２等を用いてもよい。また、Request for Comments: 2104で定義されるHMAC(Keyed-Hashing for Message Authentication code)等の方式を用いてハッシュ値（ダイジェスト値）を生成してもよい。

【００４９】

（変形例）

ＩＣカード３００内部での個人情報領域と匿名ＩＤ領域との分離の完全性を保障するために、所定の形式で算出された個人情報のハッシュ値を匿名ＩＤ情報部に記憶してもよい。

【００５０】

図９は、実施例４の変形例に係る個人認証システムの構成を説明するためのブロック図である。本変形例に係る個人認証システムが実施例２に係る個人認証システムと異なる点は、ＩＣカード３００ａの代わりにＩＣカード３００ｅを用いる点および生体情報認証サーバ２００の代わりに生体情報認証サーバ２００ｅを用いる点である。

【００５１】

図９において説明されるように、ＩＣカード３００ｅは、匿名ＩＤ情報部３１０の代わりに匿名ＩＤ情報部３１０ｅを備える。匿名ＩＤ情報部３１０ｅは、個人情報ハッシュ値記憶部３１３をさらに備える。個人情報ハッシュ値記憶部３１３は、所定の形式で算出された個人情報のハッシュ値を記憶する。また、生体情報認証サーバ２００ｅは、個人情報のハッシュ値を記憶する。

【００５２】

本実施例においては、ＩＣカード端末１００から匿名ＩＤを生体情報認証サーバ２００ｅに送信する際に、個人情報ハッシュ値が同時に送信される。生体情報認証サーバ２００ｅは、記憶している個人情報ハッシュ値と受信した個人情報ハッシュ値とが一致する場合に、生体認証を行う。それにより、ＩＣカード３００ｅ内における匿名ＩＤ情報部３１０ｅと個人情報部３２０ａとの分離の完全性を保障することができる。

【００５３】

図１０は、ハッシュ値の作成工程を説明するための図である。個人情報部３２０ａに記

憶された個人情報に対して所定のハッシュ関数処理を施すことによって、個人情報をハッシュ化することができる。このハッシュ化された個人情報を個人情報ハッシュ値記憶部３１３に記憶することによって、ハッシュ値を匿名ＩＤ情報部３１０ｅに記憶させることができる。

【実施例５】

【００５４】

複数のサービスプロバイダによる個人情報がＩＣカード内に記憶されていてもよい。図１１は、複数の個人情報を記憶したＩＣカードを説明するための図である。図１１で説明されるように、ＩＣカードは、ファイアウォールによって互いにアクセスが禁止された各領域に、複数の個人情報の各々を記憶していてもよい。この場合、ＩＣカードは、複数のサービスプロバイダによる個人情報を記憶することができる。

【００５５】

図１２は、実施例５に係る個人認証システムの構成を説明するためのブロック図である。実施例５に係る個人認証システムが実施例２に係る個人認証システムと異なる点は、ＩＣカード３００ａの代わりにＩＣカード３００ｆを用いる点および生体情報認証サーバ２００の代わりに生体情報認証サーバ２００ｆを用いる点である。

【００５６】

ＩＣカード３００ｆは、複数の個人情報部３２０ｆ，３２０ｇを備える。各個人情報部３２０ｆ，３２０ｇは、互いに異なる個人情報を記憶している。また、ＩＣカード３００ｆは、匿名ＩＤ情報記憶部３１２に、各個人情報に対応した匿名ＩＤを記憶している。また、生体情報認証サーバ２００ｆは、各個人情報に対応して、匿名ＩＤ情報、生体情報、およびＩＣカードＰＩＮを記憶している。それにより、ＩＣカード３００ｇと生体情報認証サーバ２００ｇとの間で、匿名ＩＤとＩＣカードＰＩＮとを１対１で対応させることができる。

【００５７】

利用者は、対応サービスリスト記憶部３３２に記憶されたサービスリストから所望のサービスを選択することによって、所望の個人情報にアクセスすることができる。なお、個人情報にアクセスするまでの動作は実施例１と同様であるので、説明を省略する。

【００５８】

（変形例）

なお、匿名ＩＤと利用者の各指の指紋情報とを１対１で対応させてもよい。図１３は、実施例５の変形例に係る個人認証システムの構成を説明するためのブロック図である。本変形例に係る個人認証システムが実施例５に係る個人認証システムと異なる点は、ＩＣカード３００ｆの代わりにＩＣカード３００ｇを用いる点および生体情報認証サーバ２００ｆの代わりに生体情報認証サーバ２００ｇを用いる点である。

【００５９】

ＩＣカード３００ｇがＩＣカード３００ｆと異なる点は、サービスリスト部３３０の代わりにサービスリスト部３３０ｇを備える点である。サービスリスト部３３０は、対応サービスリスト記憶部３３２ｇを備え、複数のサービスを各指に対応させて記憶している。

【００６０】

生体情報認証サーバ２００ｇは、利用者の各指の生体情報を照合用生体情報として記憶し、各照合用生体情報とサービスリスト記憶部３３２ｇに記憶されたサービスリストとを対応させている。

【００６１】

利用者は、対応サービスリスト記憶部３３２ｇに記憶されたサービスリストから所望のサービスを選択し、対応する指を生体センサ１１０に取得させることによって、所望の個人情報にアクセスすることができる。なお、個人情報にアクセスするまでの動作は実施例１と同様であるので、説明を省略する。

【００６２】

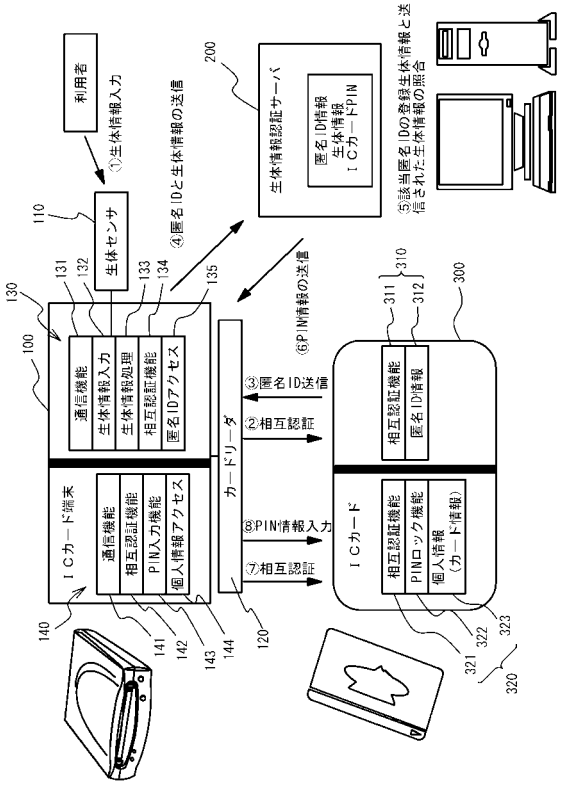
（機器構成）

図１４は、上記各実施例に係るＩＣカード端末１００および生体情報認証サーバ２００の機器構成図である。図１４で説明されるように、ＩＣカード端末１００は、ＣＰＵ（中央演算処理装置）１０１、ＲＡＭ（ランダムアクセスメモリ）１０２、ＲＯＭ（リードオンリメモリ）１０３、入出力インタフェース１０４、ＬＡＮインタフェース１０５等を備える。各機器は、バスによって接続されている。ＣＰＵ１０１がＲＯＭ１０３等に記憶されているプログラムを実行することによって、ＩＣカード端末１００に、生体認証部１３０、およびＩＣカード認証部１４０が実現される。

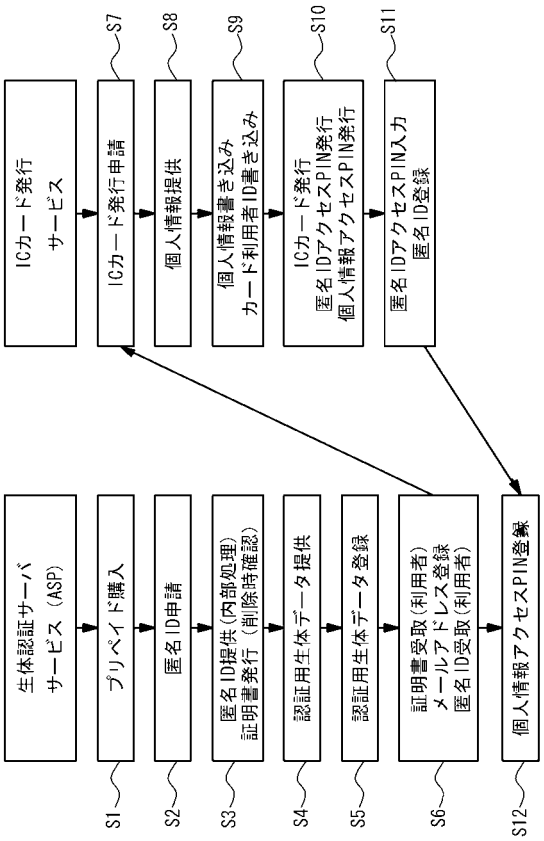
【００６３】

生体情報認証サーバ２００は、ＣＰＵ（中央演算処理装置）２０１、ＲＡＭ（ランダムアクセスメモリ）２０２、ＨＤＤ（ハードディスクドライブ）２０３、入出力インタフェース２０４、ＬＡＮインタフェース２０５等を備える。各機器は、バスによって接続されている。ＣＰＵ１０１がＨＤＤ２０３等に記憶されているプログラムを実行することによって、生体情報認証サーバ２００が実現される。

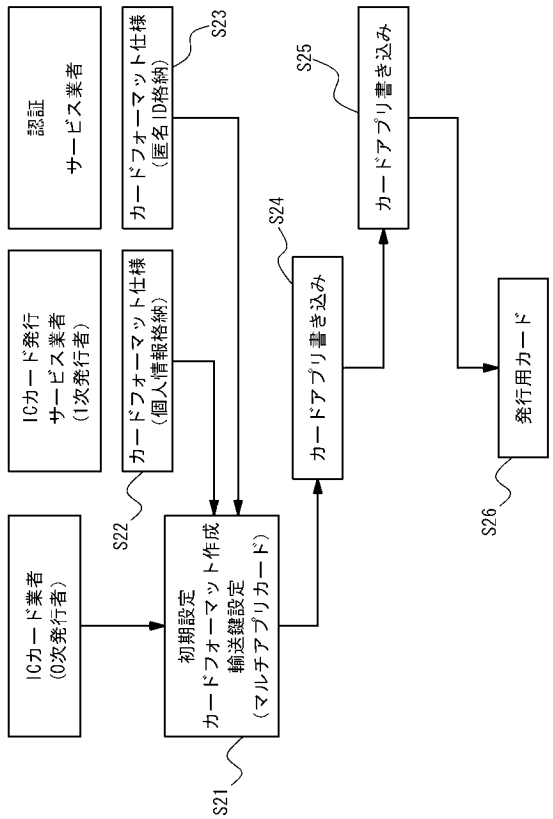
【図１】



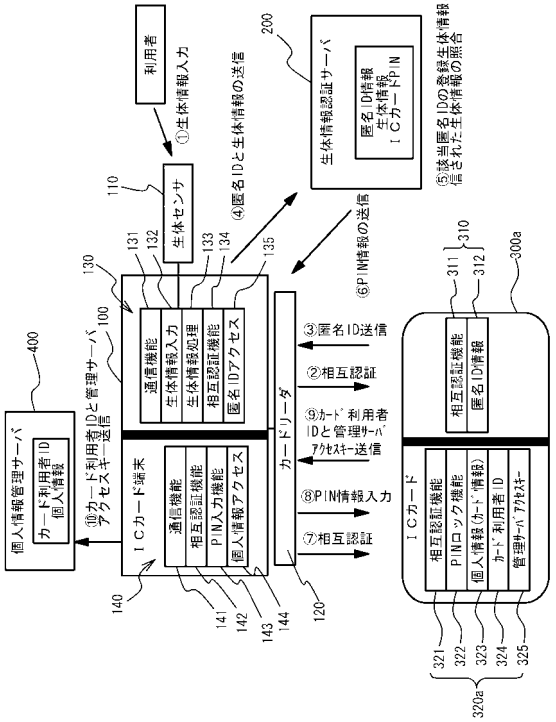
【図２】



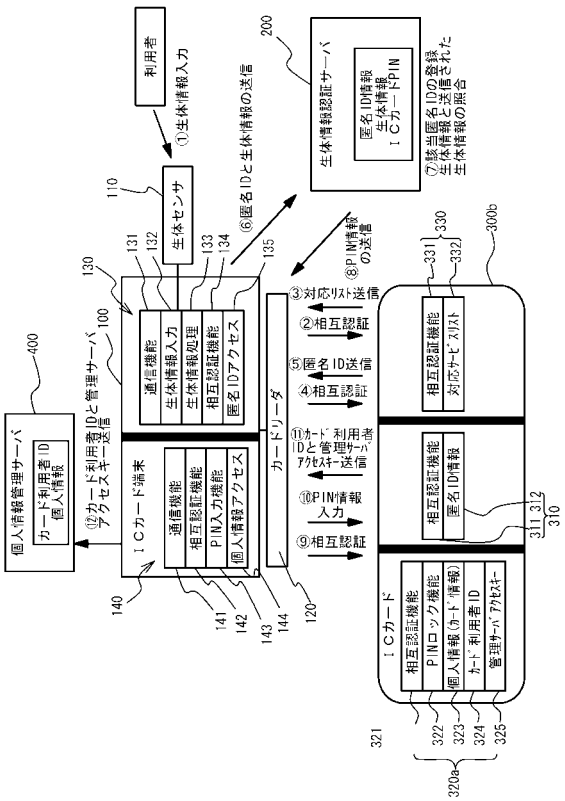
【図３】


認証
サービス業者
ICカード発行
サービス業者
（1次発行者）
カードフォーマット仕様
（匿名ID格納）
S23
S25
カードアプリ書き込み
S24
カードフォーマット仕様
（個人情報格納）
S22
ICカード業者
（0次発行者）
初期設定
カードフォーマット作成
輸送鍵設定
（マルチアプリカード）
カードアプリ書き込み
発行用カード
S21
S26

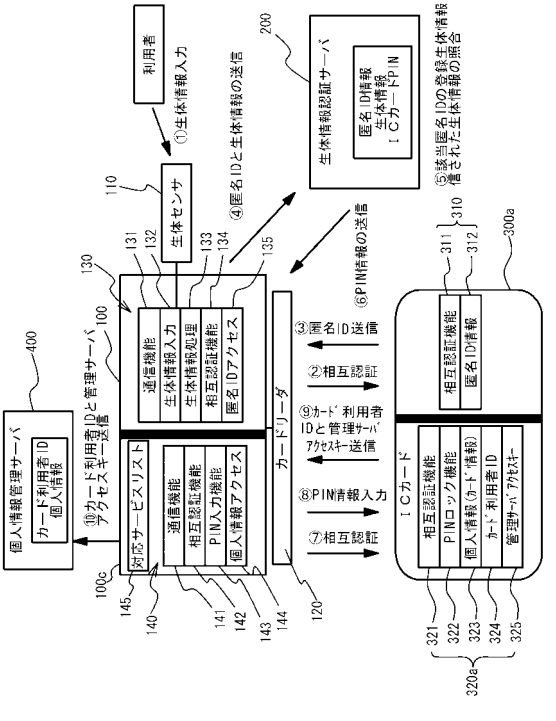
【図４】


利用者
①生体情報入力
生体センサ
110
200
生体情報認証サーバ
匿名ID情報
生体情報
ICカードPIN
④匿名IDと生体情報の送信
⑥PIN情報の送信
⑤該当匿名IDの登録生体情報と送信された生体情報の照合
130
131
132
133
134
135
100
通信機能
生体情報入力
生体情報処理
相互認証機能
匿名IDアクセス
カードリーダ
③匿名ID送信
②相互認証
⑨ｶｰﾄﾞ利用者IDと管理サーバアクセスキー送信
⑧PIN情報入力
⑦相互認証
400
個人情報管理サーバ
カード利用者ID
個人情報
⑩カード利用者IDと管理サーバアクセスキー送信
ICカード端末
通信機能
相互認証機能
PIN入力機能
個人情報アクセス
140
141
142
143
144
120
310
311
312
300a
ICカード
相互認証機能
匿名ID情報
PINロック機能
個人情報（ｶｰﾄﾞ情報）
カード利用者ID
管理サーバアクセスキー
321
322
323
324
325
320a

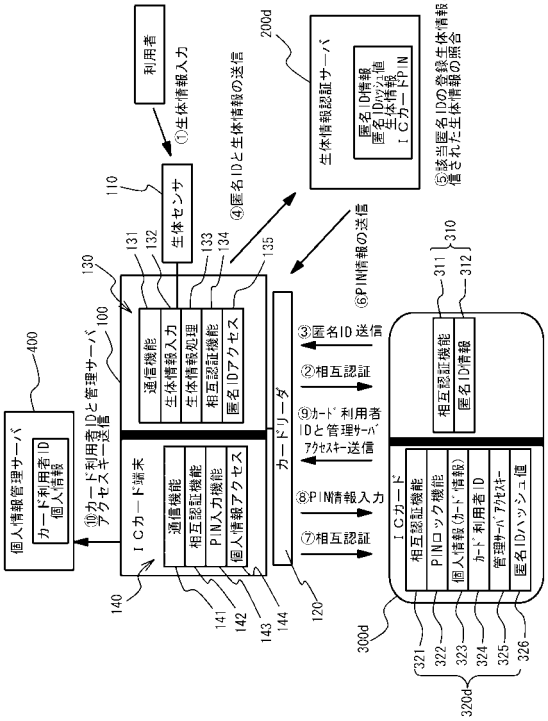
【図５】


利用者
①生体情報入力
生体センサ
110
200
生体情報認証サーバ
匿名ID情報
生体情報
ICカードPIN
⑥匿名IDと生体情報の送信
⑧PIN情報の送信
⑦該当匿名IDの登録生体情報と送信された生体情報の照合
130
131
132
133
134
135
100
通信機能
生体情報入力
生体情報処理
相互認証機能
匿名IDアクセス
カードリーダ
③対応リスト送信
②相互認証
⑤匿名ID送信
④相互認証
⑪ｶｰﾄﾞ利用者IDと管理サーバアクセスキー送信
⑩PIN情報入力
⑨相互認証
400
個人情報管理サーバ
カード利用者ID
個人情報
⑫カード利用者IDと管理サーバアクセスキー送信
ICカード端末
通信機能
相互認証機能
PIN入力機能
個人情報アクセス
140
141
142
143
144
120
330
331
332
300b
相互認証機能
対応カードリスト
相互認証機能
匿名ID情報
311
312
310
ICカード
相互認証機能
PINロック機能
個人情報（ｶｰﾄﾞ情報）
カード利用者ID
管理サーバアクセスキー
321
322
323
324
325
320a

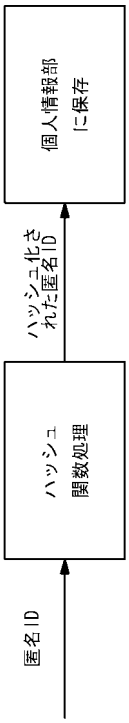
【図６】


利用者
①生体情報入力
生体センサ
110
200
生体情報認証サーバ
匿名ID情報
生体情報
ICカードPIN
④匿名IDと生体情報の送信
⑥PIN情報の送信
⑤該当匿名IDの登録生体情報と送信された生体情報の照合
130
131
132
133
134
135
100
通信機能
生体情報入力
生体情報処理
相互認証機能
匿名IDアクセス
カードリーダ
③匿名ID送信
②相互認証
⑨ｶｰﾄﾞ利用者IDと管理サーバアクセスキー送信
⑧PIN情報入力
⑦相互認証
400
個人情報管理サーバ
カード利用者ID
個人情報
⑩カード利用者IDと管理サーバアクセスキー送信
対応サービスリスト
100c
ICカード端末
通信機能
相互認証機能
PIN入力機能
個人情報アクセス
145
140
141
142
143
144
120
310
311
312
300a
ICカード
相互認証機能
匿名ID情報
PINロック機能
個人情報（ｶｰﾄﾞ情報）
カード利用者ID
管理サーバアクセスキー
321
322
323
324
325
320a

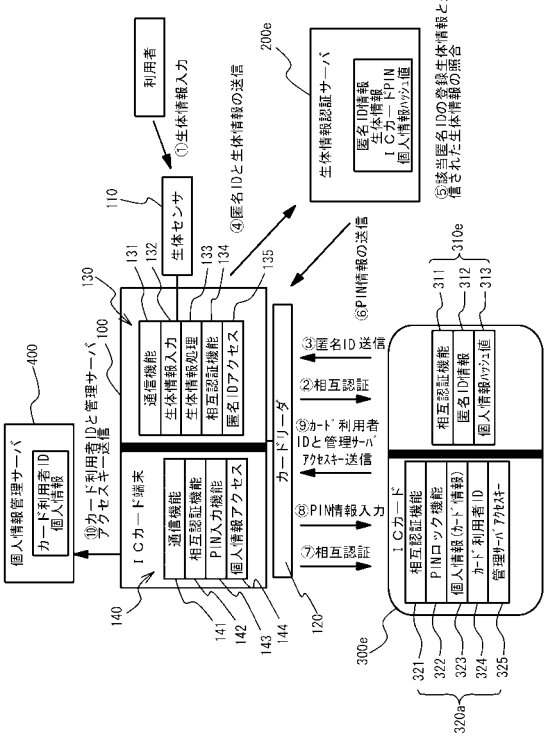
【図７】


利用者
①生体情報入力
生体センサ
④匿名IDと生体情報の送信
生体情報認証サーバ
匿名ID情報
匿名ID(ハッシュ値)
ICカードPIN
⑤該当匿名IDの登録生体情報と送信された生体情報の照合
⑥PIN情報の送信
③匿名ID送信
②相互認証
⑨カード利用者IDと管理サーバアクセスキー送信
⑧PIN情報入力
⑦相互認証
カードリーダ
ICカード端末
通信機能
生体情報入力
生体情報処理
相互認証機能
匿名IDアクセス
PIN入力機能
個人情報アクセス
ICカード
相互認証機能
PINロック機能
個人情報(カード情報)
カード利用者ID
管理サーバアクセスキー
匿名IDハッシュ値
匿名ID情報
⑩カード利用者IDと管理サーバアクセスキー送信
個人情報管理サーバ
カード利用者ID
個人情報
100
110
120
130
131
132
133
134
135
140
141
142
143
144
200d
300d
310
311
312
320d
321
322
323
324
325
326
400

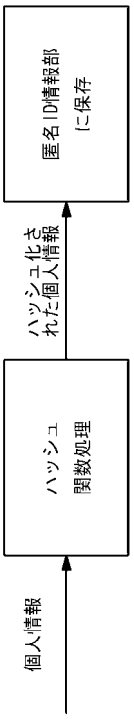
【図８】


匿名ID
ハッシュ関数処理
ハッシュ化された匿名ID
個人情報部に保存

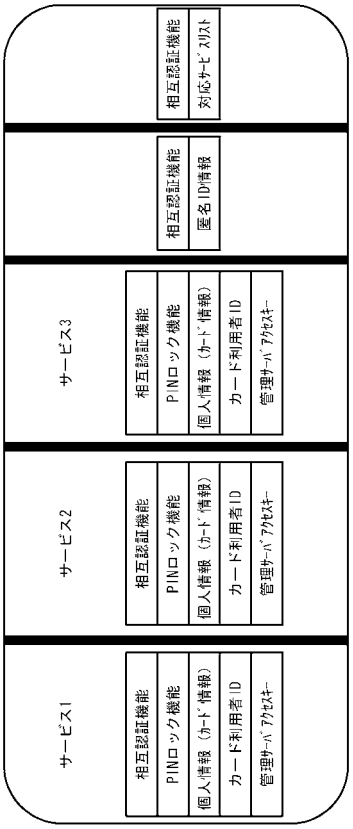
【図９】


利用者
①生体情報入力
生体センサ
④匿名IDと生体情報の送信
生体情報認証サーバ
匿名ID情報
生体情報
ICカードPIN
個人情報ハッシュ値
⑤該当匿名IDの登録生体情報と送信された生体情報の照合
⑥PIN情報の送信
③匿名ID送信
②相互認証
⑨カード利用者IDと管理サーバアクセスキー送信
⑧PIN情報入力
⑦相互認証
カードリーダ
ICカード端末
通信機能
生体情報入力
生体情報処理
相互認証機能
匿名IDアクセス
PIN入力機能
個人情報アクセス
ICカード
相互認証機能
PINロック機能
個人情報(カード情報)
カード利用者ID
管理サーバアクセスキー
匿名ID情報
個人情報ハッシュ値
⑩カード利用者IDと管理サーバアクセスキー送信
個人情報管理サーバ
カード利用者ID
個人情報
100
110
120
130
131
132
133
134
135
140
141
142
143
144
200e
300e
310e
311
312
313
320e
321
322
323
324
325
400

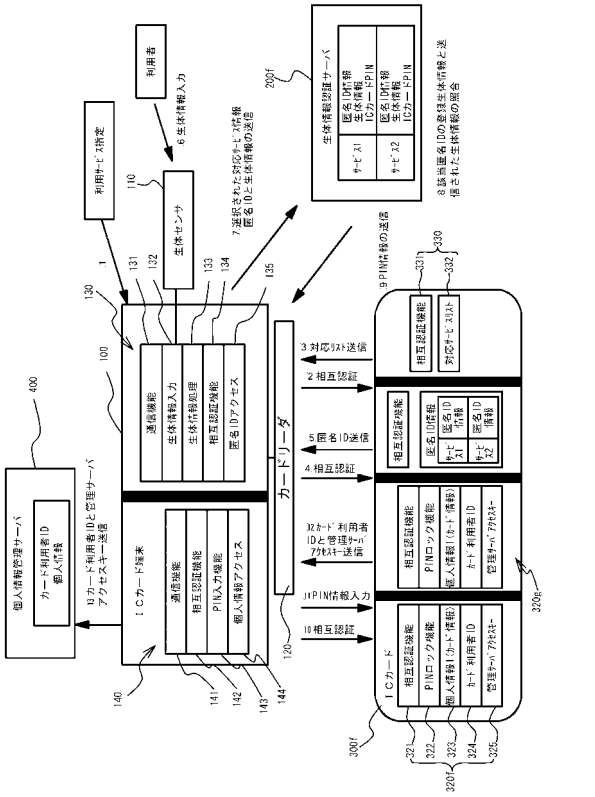
【図１０】


個人情報
ハッシュ関数処理
ハッシュ化された個人情報
匿名ID情報部に保存

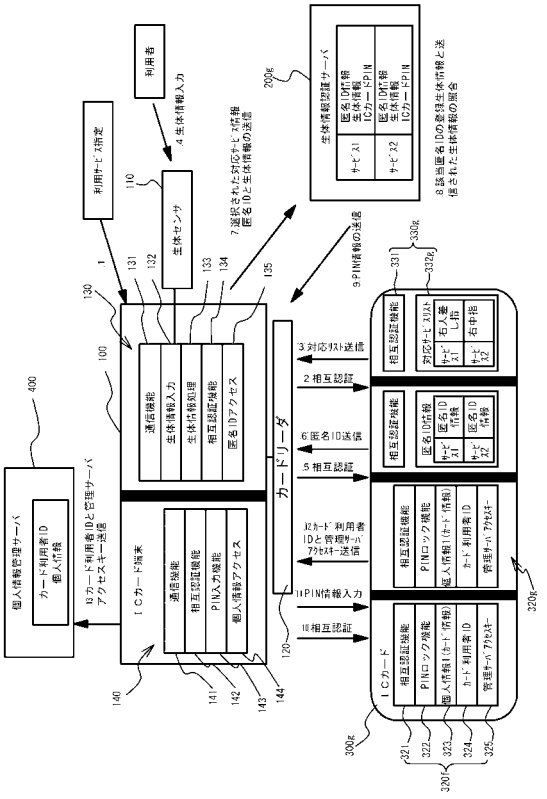
【図１１】



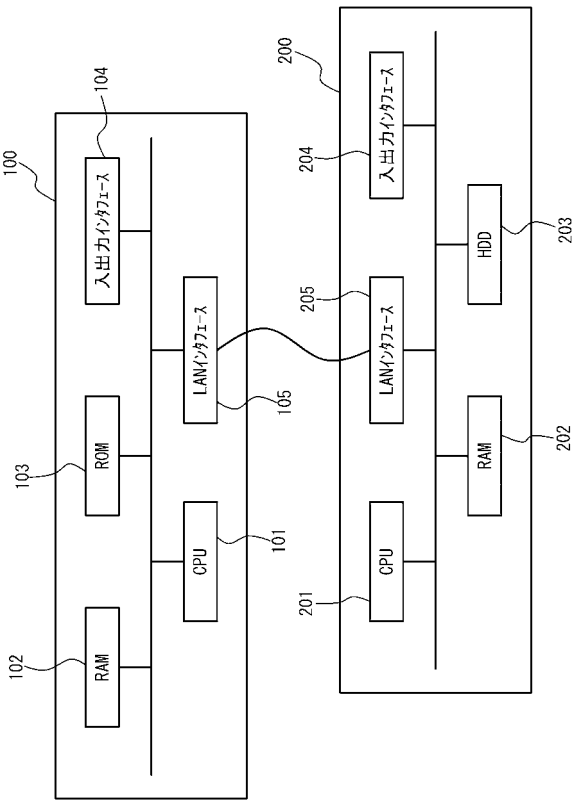
【図１２】



【図１３】



【図１４】



フロントページの続き

(56)参考文献 特開２００９－００９４２７（ＪＰ，Ａ）
特開２００６－０７３０２９（ＪＰ，Ａ）
特開２００８－２５１０２１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／３２
Ｇ０６Ｋ　１７／００
Ｇ０６Ｋ　１９／１０