

明 細 書

発明の名称： 端末、システム、端末の制御方法及び記憶媒体

技術分野

[0001] 本発明は、端末、システム、端末の制御方法及び記憶媒体に関する。

背景技術

[0002] 生体認証や当該生体認証を用いたサービスの提供に関する技術が存在する。

[0003] 例えば、特許文献 1 には、生体認証の精度向上に寄与する、システム、サーバ装置、認証方法及び記憶媒体を提供する、と記載されている。特許文献 1 のシステムは、サーバ装置と、少なくとも 1 以上の認証端末と、を含む。サーバ装置は、複数の利用者それぞれの ID と生体情報を対応付けて記憶する。少なくとも 1 以上の認証端末は、所定エリアに滞在する少なくとも 1 以上の滞在者の ID を記憶する ID リストを保持する。少なくとも 1 以上の認証端末は、被認証者の認証が必要になると、被認証者の生体情報と ID リストを含む認証要求をサーバ装置に送信する。サーバ装置は、複数の利用者それぞれの ID から ID リストに含まれる ID を抽出し、抽出された ID に対応する生体情報と認証要求に含まれる生体情報を用いた生体認証を実行する。

[0004] 特許文献 2 には、ポイントが付与された利用者の利便性を向上させる、認証サーバを提供する、と記載されている。特許文献 2 の認証サーバは、利用者登録部と、ポイント管理部と、データベースと、を備える。利用者管理部は、利用者を一意に定める第 1 の ID と、利用者の生体認証に用いる生体情報を取得する。ポイント管理部は、生体認証の結果を用いて利用者にサービスを提供するサービス事業者が利用者に付与した第 1 のポイントと利用者にオンラインサービスを提供するオンライン事業者が利用者に付与した第 2 のポイントの管理を行う。データベースは、第 1 の ID 、生体情報、第 1 及び第 2 のポイントの合算値と、を対応付けて記憶する。

先行技術文献

特許文献

[0005] 特許文献1：特許第7036300号公報

特許文献2：国際公開第2022/137954号

発明の概要

発明が解決しようとする課題

[0006] 特許文献1や特許文献2に開示されたシステムでは、生体認証を用いたサービスの提供を受ける利用者の生体情報や生体情報を用いたサービスの提供に必要な情報をサーバに登録する必要がある。ここで、サーバが、当該生体情報を用いたサービスの提供に必要な情報をどのようにして取得するのが問題になる。

[0007] 例えば、生体情報を用いたサービスの提供に必要な情報として、空港会社（空港運営会社）や航空会社のシステムが管理する情報（例えば、会員IDや搭乗券情報）等が例示される。サーバがこれらの情報を空港会社等のシステムから取得する場合、空港会社側のシステムが情報提供に対応する必要がある。ここで、生体情報を用いたサービスの提供に必要な情報は多岐に亘り、各情報を保持するシステムの変更等には大きなコストが発生する。その結果、生体認証を用いたサービスの普及が妨げられる。

[0008] 本発明は、生体認証を用いたサービスの提供に必要な情報のシステム登録を容易に実現することに寄与する、端末、システム、端末の制御方法及び記憶媒体を提供することを主たる目的とする。

課題を解決するための手段

[0009] 本発明の第1の視点によれば、利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得する、取得手段と、前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求をサーバ装置に送信する、送信手段と、を備える、端末が提供される。

[0010] 本発明の第2の視点によれば、サーバ装置と、利用者が所持する端末と、を含み、前記端末は、前記利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得し、前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求を前記サーバ装置に送信し、前記サーバ装置は、前記トークン登録要求の受信に応じて、前記利用者の生体情報及び業務情報を対応付けて第1のデータベースに記憶する、システムが提供される。

[0011] 本発明の第3の視点によれば、端末において、利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得し、前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求をサーバ装置に送信する、端末の制御方法が提供される。

[0012] 本発明の第4の視点によれば、端末に搭載されたコンピュータに、利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得する処理と、前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求をサーバ装置に送信する処理と、を実行させるためのプログラムを記憶する、コンピュータ読取可能な記憶媒体が提供される。

発明の効果

[0013] 本発明の各視点によれば、生体認証を用いたサービスの提供に必要な情報のシステム登録を容易に実現することに寄与する、端末、システム、端末の制御方法及び記憶媒体が提供される。なお、本発明の効果は上記に限定されない。本発明により、当該効果の代わりに、又は当該効果と共に、他の効果が奏されてもよい。

図面の簡単な説明

[0014] [図1]図1は、一実施形態の概要を説明するための図である。

[図2]図2は、一実施形態の動作を説明するためのフローチャートである。

[図3]図3は、第1の実施形態に係る情報処理システムの概略構成の一例を示

す図である。

[図4]図4は、第1の実施形態に係る情報処理システムの動作を説明するための図である。

[図5]図5は、第1の実施形態に係る端末にインストールされたアプリケーションを説明するための図である。

[図6]図6は、第1の実施形態に係る端末の表示の一例を示す図である。

[図7]図7は、第1の実施形態に係る端末の表示の一例を示す図である。

[図8]図8は、第1の実施形態に係る情報処理システムの動作を説明するための図である。

[図9]図9は、第1の実施形態に係る情報処理システムの動作を説明するための図である。

[図10]図10は、第1の実施形態に係る端末の処理構成の一例を示す図である。

[図11]図11は、第1の実施形態に係るトークン制御部の動作の一例を示すフローチャートである。

[図12]図12は、第1の実施形態に係る空港端末の処理構成の一例を示す図である。

[図13]図13は、第1の実施形態に係る空港端末の表示の一例を示す図である。

[図14]図14は、第1の実施形態に係るサーバ装置の処理構成の一例を示す図である。

[図15]図15は、第1の実施形態に係る利用者管理データベースの一例を示す図である。

[図16]図16は、第1の実施形態に係るトークン制御部の動作の一例を示すフローチャートである。

[図17]図17は、第1の実施形態に係る認証部の動作の一例を示すフローチャートである。

[図18]図18は、第1の実施形態に係るテーブル情報の一例を示す図である

。

[図19]図19は、第1の実施形態に係る認証端末の処理構成の一例を示す図である。

[図20]図20は、第1の実施形態に係る情報処理システムの動作の一例を示すシーケンス図である。

[図21]図21は、第1の実施形態に係る情報処理システムの動作の一例を示すシーケンス図である。

[図22]図22は、第2の実施形態に係る端末の表示の一例を示す図である。

[図23]図23は、第3の実施形態に係る行動履歴管理データベースの一例を示す図である。

[図24]図24は、第3の実施形態に係るサーバ装置の処理構成の一例を示す図である。

[図25]図25は、本願開示に係る端末のハードウェア構成の一例を示す図である。

発明を実施するための形態

[0015] はじめに、一実施形態の概要について説明する。なお、この概要に付記した図面参照符号は、理解を助けるための一例として各要素に便宜上付記したものであり、この概要の記載はなんらの限定を意図するものではない。また、特段の釈明がない場合には、各図面に記載されたブロックはハードウェア単位の構成ではなく、機能単位の構成を表す。各図におけるブロック間の接続線は、双方向及び単方向の双方を含む。一方向矢印については、主たる信号（データ）の流れを模式的に示すものであり、双方向性を排除するものではない。なお、本明細書及び図面において、同様に説明されることが可能な要素については、同一の符号を付することにより重複説明が省略され得る。

[0016] 一実施形態に係る端末100は、取得手段101と、送信手段102と、を備える（図1参照）。取得手段101は、利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得する（図2のステップS1）。送信手段102は

、取得された業務情報と利用者の生体情報を含むトークン登録要求をサーバ装置に送信する（ステップS2）。

[0017] 端末100は、生体認証を用いたサービスの享受に必要な業務情報を自装置（スマートフォン）にインストールされたアプリケーションから取得する。端末100は、当該取得した業務情報と利用者の生体情報をサーバ装置に送信し、トークンの登録を依頼する。このような構成を採用することで、サービス提供者のシステムが集中管理しているような業務情報を、当該システムからサーバ装置に送信する必要がない。その結果、各サービス提供者のシステムの大幅変更等を伴うことなく、生体認証を用いたサービスの提供に必要な情報のシステム登録が容易に実現される。

[0018] 以下に具体的な実施形態について、図面を参照してさらに詳しく説明する。

[0019] [第1の実施形態]

第1の実施形態について、図面を用いてより詳細に説明する。

[0020] [システムの構成]

図3は、第1の実施形態に係る情報処理システム（認証システム）の概略構成の一例を示す図である。図3に示す情報処理システムには、サーバ装置10と、複数の認証端末20-1～20-4と、空港端末30と、が含まれる。

[0021] なお、以降の説明において、認証端末20-1～20-4を区別する特段の理由がない場合には、単に「認証端末20」と表記する。

[0022] サーバ装置10は、生体認証を用いたサービスを空港利用者に提供する装置である。サーバ装置10は、任意の団体等により運営される。例えば、空港会社、航空会社、国や自治体等の公的機関、空港会社や公的機関等から委託を受けた民間企業等がサーバ装置10を運営する。

[0023] サーバ装置10は、空港内に設置されていてもよいし、ネットワーク上のクラウドに設置されていてもよい。

[0024] 認証端末20は、生体認証を用いたサービスの享受を受ける利用者のイン

ターフェイスとなる端末（タッチポイント）である。利用者に生体認証を用いたサービスを提供する事業者（サービス提供者）は、提供するサービスに応じた認証端末 20 を空港内の各所に設置する。利用者は、認証端末 20 を介して生体認証を用いたサービスの提供を受ける。

[0025] 例えば、認証端末 20-1 は、売店等に設置される POS（Point of Sale）端末である。例えば、空港会社が売店等に認証端末 20-1（POS 端末）を設置する。例えば、空港会社は、認証端末 20-1 を介して自社の会員（以下、空港会員とも表記する）に生体認証を用いた決済サービスを提供する。例えば、認証端末 20-1 は、顔決済に関する制御等を実行する。

[0026] 認証端末 20-2 は、例えば、ラウンジ等に設置された受付端末である。例えば、空港会社が、ラウンジの出入口（受付）に認証端末 20-2（受付端末）を設置する。例えば、空港会社は、自社の会員（空港会員）に対してラウンジの無料利用を許可する。例えば、認証端末 20-2 は、生体認証により特定された利用者がラウンジを無料利用する資格を備えているか否かをラウンジの受付で待機する職員等に通知する。

[0027] 認証端末 20-3 は、例えば、空港内のロビー等に設置されたデジタルサイネージである。例えば、航空会社が発着ロビー等に認証端末 20-3（デジタルサイネージ）を設置する。例えば、航空会社は、自社の会員（以下、航空会員とも表記する）に対して種々の情報を提供する。例えば、認証端末 20-3 は、生体認証により特定された利用者に対して搭乗ゲートの場所を案内したり、観光地に関する情報提供を行ったりする。

[0028] 認証端末 20-4 は、例えば、搭乗口ごとに設置されたゲート装置である。例えば、航空会社が認証端末 20-4（ゲート装置）を設置する。認証端末 20-4 は、生体認証により特定された利用者が航空機に搭乗する資格を備えていなければ当該利用者の通行を拒否する。

[0029] 空港端末 30 は、空港内に設置された端末である。利用者は、空港端末 30 を操作して、チェックイン手続き等を行う。また、空港端末 30 は、利用者のトークン登録に関する機能を備える。具体的には、空港端末 30 は、利

用者のトークン登録（トークン発行）をサーバ装置１０に要求する。トークンに関する詳細は後述する。

[0030] 利用者は、端末４０を所持する。端末４０には種々のアプリケーションがインストールされている。例えば、空港会社の会員が使用するエアポートアプリケーションや航空会社の会員が使用するエアラインアプリケーションが端末４０にはインストールされている。

[0031] 利用者は、エアポートアプリケーションを用いて空港会社が提供する様々なサービスや特典を享受する。例えば、利用者は、エアポートアプリケーションを用いて、空港会社と提携するホテルの予約、フライト情報の確認等を行う。あるいは、利用者は、エアポートアプリケーションを使ってクレジットカード情報等を空港会社のシステムに登録する。利用者は、登録されたクレジットカード情報を使って買い物（例えば、オンラインショッピング）を行うことができる。

[0032] また、利用者は、エアラインアプリケーションを用いて、航空券の購入、チェックイン手続き等を行う。例えば、利用者は、エアラインアプリケーションを用いて搭乗券を管理する。

[0033] さらに、端末４０は、上述のトークン登録に関する機能を備える。

[0034] 図３に示す情報処理システムに含まれる各装置（サーバ装置１０、認証端末２０等）は、ネットワークを介して相互に通信可能に構成されている。例えば、サーバ装置１０と認証端末２０は、有線又は無線の通信手段により接続され、相互に通信が可能となるように構成されている。

[0035] 図３は例示であって、本願開示の情報提供システムの構成等を限定する趣旨ではない。例えば、情報処理システムには２台以上のサーバ装置１０が含まれていてもよい。また、情報処理システムに含まれる認証端末２０の数は４に限定されない。情報処理システムには、少なくとも１以上の認証端末２０が含まれていればよい。

[0036] また、図３に示す認証端末２０は例示であって、認証端末２０の設置主体や設置目的等を限定する趣旨ではない。空港には、ＰＯＳ端末、受付端末、

デジタルサイネージ、ゲート装置以外の用途に使われる認証端末 20 が設置されていてもよい。あるいは、空港会社が設置するデジタルサイネージと航空会社が設置するデジタルサイネージとが混在していてもよい。

[0037] システムの概略動作]

続いて、情報処理システムの概略動作について説明する。

[0038] <トークン登録>

上述のように、空港端末 30 及び端末 40 は、トークン登録に関する機能を備える。

[0039] トークンは、サーバ装置 10 が利用者に生体認証を用いたサービスを提供する際に必要な情報であって、システムに登録される情報である。具体的には、トークンは、利用者の生体情報と業務情報の組み合わせから構成され、サーバ装置 10 のデータベースに記憶される。

[0040] なお、生体情報には、例えば、顔、指紋、声紋、静脈、網膜、瞳の虹彩の模様（パターン）といった個人に固有の身体的特徴から計算されるデータ（特徴量）が例示される。あるいは、生体情報は、顔画像、指紋画像等の画像データであってもよい。生体情報は、利用者の身体的特徴を情報として含むものであればよい。本願開示では、人の「顔」に関する生体情報（顔画像又は顔画像から生成された特徴量）を用いる場合について説明する。

[0041] 業務情報は、サービス提供者（例えば、空港会社、航空会社）が利用者にサービスを提供する際に必要な情報である。業務情報は、サービス提供者や当該サービス提供者から提供されるサービスの種類に応じて異なる。

[0042] 例えば、空港会員に顔決済サービスが提供される場合には、空港会社の会員 ID が業務情報となる。なお、以降の説明において、空港会社の会員 ID を「空港会員 ID」と表記する。あるいは、空港会員にラウンジの無料利用サービスが提供される場合にも、空港会員 ID が業務情報となる。

[0043] あるいは、航空会員に有益な情報が提供される場合、航空会社の会員 ID や搭乗券情報が業務情報となる。なお、以降の説明において、航空会社の会員 ID を「航空会員 ID」と表記する。あるいは、利用者が認証端末 20 -

4 を通過して航空機に搭乗する際には、搭乗券情報が業務情報となる。

- [0044] 利用者は、空港にて生体認証を用いたサービスの提供を受ける前に、トークンをシステムに登録する必要がある。具体的には、利用者は、空港内に設置された空港端末 30 又は所持する端末 40 を用いてトークンの登録をサーバ装置 10 に要求する。
- [0045] はじめに、利用者が空港端末 30 を用いてトークンの登録をサーバ装置 10 に要求する場合について説明する。
- [0046] 利用者がトークン登録（トークン発行）を希望すると、空港端末 30 は、当該利用者の生体情報を取得する。例えば、空港端末 30 は、面前の利用者を撮影し、顔画像を取得する。
- [0047] また、空港端末 30 は、利用者の所持する身分証明書から生体情報を取得する。具体的には、空港端末 30 は、パスポート、運転免許証、マイナンバーカード等の IC（Integrated Circuit）が搭載された身分証明書から顔画像を取得する。
- [0048] 空港端末 30 は、利用者を撮影することで得られた生体情報と、身分証明書から取得した生体情報と、を用いた本人確認を実行する。空港端末 30 は、2 つの生体情報（顔画像）を用いた本人確認（1 対 1 認証）を実行する。
- [0049] 本人確認に成功すると、空港端末 30 は、生体認証を用いたサービスの提供に必要な業務情報を取得する。例えば、空港端末 30 は、空港会社の会員情報（空港会員 ID）、航空会社の会員情報（例えば、航空会員 ID）、搭乗券情報（搭乗券から得られる情報）等を利用者から取得する。
- [0050] 空港端末 30 は、利用者の生体情報（例えば、撮影により得られた顔画像又は身分証明書から読み出した顔画像）と業務情報を含む「トークン登録要求」をサーバ装置 10 に送信する（図 4 参照）。
- [0051] トークン登録要求を受信すると、サーバ装置 10 は、当該トークン登録要求に含まれる生体情報及び業務情報を用いてトークンを登録（発行）する。サーバ装置 10 は、空港端末 30 から取得した情報（生体情報、業務情報）を利用者管理データベースに登録する。なお、サーバ装置 10 がトークンを

記憶する利用者管理データベースの詳細は後述する。

- [0052] サーバ装置 10 は、トークン登録要求に対する処理結果を空港端末 30 に通知する。トークンの登録に成功すると、サーバ装置 10 は、その旨を示す肯定応答を空港端末 30 に送信する。トークンの登録に失敗すると、サーバ装置 10 は、その旨を示す否定応答を空港端末 30 に送信する。
- [0053] 空港端末 30 は、トークン登録要求の結果を利用者に通知する。
- [0054] 続いて、利用者が端末 40 を用いてトークンの登録をサーバ装置 10 に要求する場合について説明する。
- [0055] 上述のように、利用者の端末 40 には種々のアプリケーションがインストールされている。例えば、上述のエアポートアプリケーションやエアラインアプリケーション等が端末 40 にインストールされている。
- [0056] また、利用者は、トークンの登録を管理、制御するためのアプリケーションを当該端末 40 にインストールする。利用者は、例えば、アプリケーションストア等からトークン制御アプリケーションをダウンロードして端末 40 にインストールする。
- [0057] 例えば、図 5 に示すように、端末 40 には、トークン制御アプリケーション、エアポートアプリケーション、エアラインアプリケーション等の各種アプリケーションがインストールされている。端末 40 にインストールされたアプリケーションは、相互にデータの送受信が可能に構成されている。
- [0058] トークン制御アプリケーションは、他のアプリケーションと連携が可能である。具体的には、トークン制御アプリケーションは、他のアプリケーションからデータを受信したり、他のアプリケーションにデータを送信したりできる。
- [0059] ここで、端末 40 にインストールされたアプリケーションは、自アプリケーションの実行に必要な情報を記憶し、管理する。例えば、エアポートアプリケーションは、利用者の空港会員 ID を管理し、記憶する。あるいは、エアラインアプリケーションは、利用者の航空会員 ID、搭乗券情報等を管理し、管理する。

- [0060] エアポートアプリケーション、エアラインアプリケーション等は、利用者が生体認証を用いたサービスの享受を希望した場合、当該希望するサービスに応じた業務情報をトークン制御アプリケーションに送信する。例えば、利用者が空港の売店にて顔決済により商品購入を希望した場合、エアポートアプリケーションは、空港会員IDをトークン制御アプリケーションに送信する。
- [0061] あるいは、エアポートアプリケーション、エアラインアプリケーションは、利用者に対して提案可能な生体認証を用いたサービスが存在する場合、当該提案可能なサービスを利用者に案内する。エアラインアプリケーション等は、利用者が提案されたサービスの享受を希望した場合、当該希望するサービスに応じた業務情報をトークン制御アプリケーションに送信する。
- [0062] 例えば、エアラインアプリケーションは、航空会社のシステムから搭乗券を取得した場合、生体認証でゲート装置を通過することを提案する。エアポートアプリケーションは、航空会社の係員等に搭乗券等をはじめとした書類（媒体）を提示することなくゲート装置を通過して航空機に搭乗できることを利用者に案内する。なお、以降の説明において、搭乗券等を提示することなくゲート装置を通過することを「顔パス」と表記する。利用者が提案を受け入れると、エアラインアプリケーションは、搭乗券情報をトークン制御アプリケーションに送信する。
- [0063] 他のアプリケーションから業務情報を取得すると（他のアプリケーションからプッシュ通知を受信すると）、トークン制御アプリケーションは、利用者の生体情報を取得する。例えば、トークン制御アプリケーションは、所謂、自撮りにより利用者を撮影し、利用者の顔画像を取得する。
- [0064] その後、トークン制御アプリケーションは、利用者の所持する身分証明書から生体情報を取得する。トークン制御アプリケーションは、パスポート、運転免許証、マイナンバーカード等のICチップから顔画像を読み出す。
- [0065] トークン制御アプリケーションは、2つの生体情報を用いた本人確認（1対1認証）を実行する。

[0066] 本人確認に成功すると、トークン制御アプリケーションは、個人情報を第三者（サーバ装置１０）に提供することに対する同意を取得する。例えば、トークン制御アプリケーションは、図６や図７に示すようなＧＵＩ（Graphic al User Interface）を用いて個人情報（生体情報及び業務情報）の第三者提供に対する利用者の同意を取得する。

[0067] なお、図６は、トークン制御アプリケーションがエアポートアプリケーションから顔決済用の業務情報を取得した場合のＧＵＩの一例である。図７は、トークン制御アプリケーションがエアラインアプリケーションから顔パス用の業務情報を取得した場合のＧＵＩの一例である。

[0068] 生体情報及び業務情報の第三者提供に対する利用者の同意を取得すると、トークン制御アプリケーションは、利用者の生体情報と業務情報を含む「トークン登録要求」をサーバ装置１０に送信する（図８参照）。

[0069] サーバ装置１０は、空港端末３０から受信したトークン登録要求と同様に、端末４０から受信したトークン登録要求を処理する。サーバ装置１０は、トークン登録要求の処理結果（トークン登録成功、トークン登録失敗）を端末４０に通知する。サーバ装置１０は、トークン登録要求に対する応答（肯定応答、否定応答）を端末４０に送信する。

[0070] 端末４０（トークン制御アプリケーション）は、トークン登録要求の結果を利用者に通知する。

[0071] このように、端末４０は、利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得する。端末４０は、当該取得された業務情報と利用者の生体情報を含むトークン登録要求をサーバ装置１０に送信する。サーバ装置１０は、トークン登録要求の受信に応じて、利用者の生体情報及び業務情報に対応付けて第１のデータベース（利用者管理データベース）に記憶する。

[0072] ＜サービスの提供＞

利用者は、認証端末２０を介して生体認証を用いたサービスの提供を受ける。生体認証を用いたサービスの享受を希望する利用者は、例えば、認証端

末20の前に移動する。

- [0073] 認証端末20は、サービス提供者の従業員等又は利用者の操作（指示）に応じて利用者の生体情報を取得する。あるいは、認証端末20は、自動的に面前の利用者の生体情報を取得する。
- [0074] 例えば、利用者が顔決済によって商品の購入を希望した場合、認証端末20-1（POS端末）は、売店の店員又は利用者（商品購入者）の操作に応じて、利用者を撮影し顔画像を取得する。あるいは、利用者がラウンジへの入場を希望した場合、認証端末20-2（受付端末）は、ラウンジの受付に待機する職員等の操作に応じて、利用者を撮影し顔画像を取得する。
- [0075] あるいは、認証端末20-3（デジタルサイネージ）や認証端末20-4（ゲート装置）は、自装置の面前に利用者を検出すると、当該利用者を撮影して顔画像を取得する。
- [0076] 認証端末20は、取得した生体情報と端末IDを含む「認証要求」をサーバ装置10に送信する（図9参照）。
- [0077] 端末IDは、認証端末20を識別するためのIDである。端末IDには、認証端末20のMAC（Media Access Control）アドレスやIP（Internet Protocol）アドレスを用いることができる。
- [0078] なお、端末IDは、サーバ装置10と各認証端末20の間において任意の方法によって共有される。例えば、システム管理者が端末IDを決定し当該決定された端末IDをサーバ装置10に設定する。また、システム管理者は、当該決定された端末IDを各認証端末20に設定する。
- [0079] 認証要求を受信したサーバ装置10は、認証要求に含まれる生体情報と利用者管理データベースに登録された生体情報を用いた生体認証を実行する。サーバ装置10は、これらの生体情報を用いた照合処理（1対N照合、Nは正の整数。以下同じ）を実行し、被認証者を特定する。
- [0080] また、サーバ装置10は、認証要求に含まれる端末IDを用いて認証要求の送信元である認証端末20を特定する（認証端末20の種類を特定する）。サーバ装置10は、特定された認証端末20に対応する業務情報（照合処

理により特定された被認証者の業務情報）を認証端末 20 に送信する。

[0081] 例えば、認証端末 20-1（POS 端末）や認証端末 20-2（受付端末）から認証要求を受信した場合、サーバ装置 10 は、空港会社の空港会員 ID を認証端末 20-1 に通知する。

[0082] あるいは、認証端末 20-3（デジタルサイネージ）から認証要求を受信した場合、サーバ装置 10 は、航空会員 ID 又は搭乗券情報を認証端末 20-3 に送信する。あるいは、認証端末 20-4（ゲート装置）から認証要求を受信した場合、サーバ装置 10 は、搭乗券情報等を認証端末 20-4 に通知する。

[0083] サーバ装置 10 は、認証要求に対する応答を認証端末 20 に送信する。

[0084] 具体的には、照合処理に成功し、且つ、認証端末 20 に対応した業務情報が利用者管理データベースに登録されている場合、サーバ装置 10 は、認証成功を示す肯定応答を認証端末 20 に送信する。より詳細には、サーバ装置 10 は、認証要求の送信元である認証端末 20 に対応する業務情報を含む肯定応答を認証端末 20 に送信する。

[0085] 照合処理に失敗した場合、又は、認証端末 20 に対応した業務情報が利用者管理データベースに登録されていない場合、サーバ装置 10 は、認証失敗を示す否定応答を認証端末 20 に送信する。

[0086] 否定応答（認証失敗）を受信した場合、認証端末 20 は、その旨を利用者や職員等に通知する。

[0087] 肯定応答（認証成功）を受信した場合、認証端末 20 は、サーバ装置 10 から取得した業務情報を用いて利用者にサービスを提供する。

[0088] 例えば、認証端末 20-1（POS 端末）は、サーバ装置 10 から取得した空港会員 ID と決済情報（利用者が購入した商品の商品名、購入金額）を空港会社のシステム（図示せず）に送信する。空港会社のシステム（自社の会員に種々のサービスを提供するシステム）は、空港会員 ID を用いて商品購入者を特定し、当該特定された商品購入者のクレジットカード情報と決済情報を用いて決済処理を行う。

- [0089] あるいは、認証端末20-2（受付端末）は、サーバ装置10から取得した空港会員IDを空港会社システムに送信する。空港会社システムは、空港会員IDに紐付けて記憶された会員情報（例えば、会員の氏名等）を認証端末20-2に送信する。認証端末20-2は、取得した会員情報と共に被認証者は空港会社の会員である旨を職員等に通知する。職員は、被認証者のラウンジ無料利用を許可する。
- [0090] あるいは、認証端末20-3（デジタルサイネージ）は、サーバ装置10から取得した航空会員IDを航空会社システム（図示せず）に送信し、対応する会員情報を取得する。認証端末20-3は、取得した会員情報を用いた情報提供（例えば、利用者が搭乗予定の航空機に関するフライト情報）を表示する。あるいは、認証端末20-3は、サーバ装置10から取得した搭乗券情報に基づいた情報提供を行う。例えば、認証端末20-3は、利用者が搭乗する航空機の搭乗ゲートの場所を表示する。
- [0091] あるいは、認証端末20-4（ゲート装置）は、サーバ装置10から取得した搭乗券情報を用いて、利用者が認証端末20-4の先に駐機している航空機に搭乗できる権限を備えているか否か判定する。認証端末20-4は、自装置にて搭乗可否を判定している航空機に対応する搭乗券情報をサーバ装置10から取得した場合には、ゲートを開き利用者の通行を許可する。認証端末20-4は、自装置にて搭乗可否を判定している航空機に対応する搭乗券情報をサーバ装置10から取得できない場合には、ゲートを閉じ利用者の通行を拒否する。
- [0092] このように、サーバ装置10は、被認証者の生体情報を含む認証要求を認証端末20から受信する。サーバ装置10は、受信した認証要求に含まれる生体情報と利用者管理データベースに記憶された生体情報を用いた照合処理により被認証者を特定する。サーバ装置10は、利用者管理データベースに記憶された、被認証者の少なくとも1以上の業務情報のうち認証端末20に対応する業務情報を当該認証端末20に送信する。
- [0093] 続いて、第1の実施形態に係る情報処理システムに含まれる各装置の詳細

について説明する。

[0094] [端末]

端末40には、スマートフォン、携帯電話機、ゲーム機、タブレット等の携帯端末装置やコンピュータ（パーソナルコンピュータ、ノートパソコン）等が例示される。

[0095] 図10は、第1の実施形態に係る端末40の処理構成（処理モジュール）の一例を示す図である。図10を参照すると、端末40は、通信制御部201と、トークン制御部202と、記憶部203と、を備える。

[0096] 通信制御部201は、他の装置との間の通信を制御する手段である。例えば、通信制御部201は、サーバ装置10からデータ（パケット）を受信する。また、通信制御部201は、サーバ装置10に向けてデータを送信する。通信制御部201は、他の装置から受信したデータを他の処理モジュールに引き渡す。通信制御部201は、他の処理モジュールから取得したデータを他の装置に向けて送信する。このように、他の処理モジュールは、通信制御部201を介して他の装置とデータの送受信を行う。通信制御部201は、他の装置からデータを受信する受信部としての機能と、他の装置に向けてデータを送信する送信部としての機能と、を備える。

[0097] トークン制御部202は、端末40におけるトークンに関する制御を行う手段である。具体的には、トークン制御部202は、トークンの登録をサーバ装置10に要求する。トークン制御部202は、上述のトークン制御アプリケーションを実現するモジュールである。

[0098] トークン制御部202は、利用者が空港内外で生体認証を用いたサービスの提供を受けるために必要なトークンの登録をサーバ装置10に要求する。

[0099] トークン制御部202は、利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得する、取得手段としての機能を備える。また、トークン制御部202は、取得された業務情報と利用者の生体情報を含むトークン登録要求をサーバ装置に送信する、送信手段としての機能を備える。

- [0100] 図 1 1 は、第 1 の実施形態に係るトークン制御部 2 0 2 の動作の一例を示すフローチャートである。図 1 1 を参照し、トークン制御部 2 0 2 の動作を説明する。
- [0101] トークン制御部 2 0 2 は、他のアプリケーションから業務情報を受信する（ステップ S 1 0 1）。具体的には、トークン制御部 2 0 2 は、他のアプリケーションからのプッシュ通知により業務情報を取得する。
- [0102] 例えば、トークン制御部 2 0 2 は、エアポートアプリケーションから空港会員 I D を取得する。あるいは、トークン制御部 2 0 2 は、エアラインアプリケーションから航空会員 I D を取得する。
- [0103] トークン制御部 2 0 2 は、例えば、D e e p L i n k と称されるアプリケーション連携手法を用いて、業務情報を取得する。あるいは、トークン制御部 2 0 2 は、予め定められた A P I （Application Programming Interface）を用いて業務情報を取得してもよい。例えば、トークン制御部 2 0 2 は、トークン制御アプリケーションが定める A P I を用いて、他のアプリケーションから業務情報を受信する。
- [0104] 業務情報を受信すると、トークン制御部 2 0 2 は、本人確認用の生体情報を取得する（ステップ S 1 0 2）。具体的には、トークン制御部 2 0 2 は、利用者を撮影することで当該利用者の顔画像を取得する。
- [0105] さらに、トークン制御部 2 0 2 は、利用者が所持する身分証明書から生体情報を取得する。例えば、トークン制御部 2 0 2 は、パスポート、運転免許証、マイナンバーカード等の身分証明書に搭載された I C チップから顔画像を取得する。トークン制御部 2 0 2 は、N F C （Near Field Communication）により I C チップと通信を行い、当該 I C チップに格納された顔画像を取得する。
- [0106] トークン制御部 2 0 2 は、本人確認を実行する（ステップ S 1 0 3）。具体的には、トークン制御部 2 0 2 は、利用者を撮影することで得られた顔画像と、身分証明書の I C チップから読み出した顔画像と、を用いた本人確認を行う。トークン制御部 2 0 2 は、2 つの生体情報が実質的に一致するか否

かを判定し本人確認を行う。

[0107] トークン制御部202は、撮影により取得した顔画像と身分証明書から取得した顔画像のそれぞれから特徴量を生成する。

[0108] なお、特徴量の生成処理に関しては既存の技術を用いることができるので、その詳細な説明を省略する。例えば、トークン制御部202は、顔画像から目、鼻、口等を特徴点として抽出する。その後、トークン制御部202は、特徴点それぞれの位置や各特徴点間の距離を特徴量として計算する（複数の特徴量からなる特徴ベクトルを生成する）。

[0109] 次に、トークン制御部202は、当該生成された2つの特徴量を用いた認証処理（1対1認証）を実行する。具体的には、トークン制御部202は、2つの特徴量を用いて対応する顔画像間の類似度を算出する。トークン制御部202は、当該算出した類似度に対する閾値処理の結果に基づき、2つの画像が同一人物の顔画像か否かを判定する。なお、当該類似度には、カイニ乗距離やユークリッド距離等を用いることができる。距離が離れているほど類似度は低く、距離が近いほど類似度が高い。

[0110] 類似度が所定の値よりも大きければ（距離が所定の値よりも短ければ）、トークン制御部202は、本人確認成功と判定する。類似度が所定の値以下であれば、トークン制御部202は、本人確認失敗と判定する。

[0111] なお、トークン制御部202は、利用者が実在していることを証明する「ライブネス認証」を実行してもよい。具体的には、トークン制御部202は、撮影により得られた顔画像と身分証明書から読み出した顔画像を用いた認証（照合）に成功した後に、利用者に所定動作の指示を行い利用者（被認証者）が指示に従っているか否かを判定する。例えば、トークン制御部202は、「右目を閉じて下さい」といった指示を行い、利用者が指示に従っているか否かに応じて、利用者が実在していることを判定する。

[0112] 本人確認に失敗すると（ステップS104、No分岐）、トークン制御部202は、トークン登録に関する処理を終了する。この場合、トークン制御部202は、本人確認に失敗したことを理由にトークンが登録（発行）でき

ない旨を利用者に通知してもよい。

- [0113] 本人確認に成功すると（ステップS 1 0 4、Y e s 分岐）、トークン制御部 2 0 2 は、個人情報の第三者提供に対する利用者の同意を取得する（ステップS 1 0 5）。
- [0114] トークン制御部 2 0 2 は、取得した業務情報の種類（内容）や業務情報の提供元のアプリケーションに応じたG U I を用いて利用者の同意を取得する。例えば、トークン制御部 2 0 2 は、図 6 や図 7 に示すG U I を用いて個人情報の第三者提供に関する利用者の同意を取得する。
- [0115] 個人情報（生体情報及び業務情報）の提供に関する同意が得られない場合（ステップS 1 0 6、N o 分岐）、トークン制御部 2 0 2 は、トークン登録に関する処理を終了する。この場合、トークン制御部 2 0 2 は、個人情報を第三者に提供しなければトークンが登録できない旨を利用者に通知してもよい。
- [0116] 個人情報の提供に関する同意が得られた場合（ステップS 1 0 6、Y e s 分岐）、トークン制御部 2 0 2 は、トークン登録要求をサーバ装置 1 0 に送信する（ステップS 1 0 7）。トークン制御部 2 0 2 は、利用者の生体情報（例えば、撮影により得られた顔画像又は身分証明書から読み出した顔画像）と業務情報を含む「トークン登録要求」をサーバ装置 1 0 に送信する。
- [0117] トークン制御部 2 0 2 は、トークン登録要求に対する応答（肯定応答、否定応答）を受信する（ステップS 1 0 8）。
- [0118] トークン制御部 2 0 2 は、トークン登録要求の結果に応じた処理を実行する（ステップS 1 0 9）。
- [0119] 肯定応答（トークン登録成功）を受信した場合、トークン制御部 2 0 2 は、例えば、空港内外で生体認証を用いたサービスの提供を受けることができる旨を利用者に通知する。
- [0120] 否定応答（トークン登録失敗）を受信した場合、トークン制御部 2 0 2 は、例えば、トークンの登録に失敗した旨を利用者に通知する。
- [0121] なお、図 1 1 を参照しつつ、トークン制御部 2 0 2 は、生体認証による本

人確認の実行（ステップS 1 0 3）の後に個人情報の第三者提供に対する同意を取得（ステップS 1 0 5）する場合について説明した。しかし、トークン制御部2 0 2は、個人情報の第三者提供に対する同意を取得した後に、生体認証による本人確認を実行してもよい。例えば、トークン制御アプリケーションはエアラインアプリケーションから搭乗券情報を受信する。当該搭乗券情報の受信に応じて、トークン制御アプリケーション（トークン制御部2 0 2）は、取得した搭乗券情報の利用目的を明示しつつ、生体情報と搭乗券情報を外部サーバに提供することに対する利用者の同意を取得する。同意を取得した後に、トークン制御アプリケーションは、利用者の生体情報を用いた本人確認を実行する。

[0122] このように、トークン制御部2 0 2は、トークン登録要求をサーバ装置1 0に送信する前に、利用者の個人情報（業務情報及び生体情報）を第三者提供することに対する利用者の同意を取得する、同意取得手段としての機能を備える。さらに、トークン制御部2 0 2は、利用者から取得した生体情報と当該利用者が所持する身分証明書から取得した生体情報を用いた本人確認を実行する、本人確認手段としての機能を備える。トークン制御部2 0 2は、トークン登録を希望する利用者の本人確認に成功した後に、トークン登録要求をサーバ装置1 0に送信する。

[0123] 記憶部2 0 3は、端末4 0の動作に必要な情報を記憶する手段である。

[0124] なお、エアポートアプリケーションやエアラインアプリケーション等を実現するための処理モジュールに関する詳細な説明は省略する。トークン制御アプリケーションとは異なる他のアプリケーションに関する詳細は、本願開示の趣旨とは異なるためである。

[0125] [空港端末]

図1 2は、第1の実施形態に係る空港端末3 0の処理構成（処理モジュール）の一例を示す図である。図1 2を参照すると、空港端末3 0は、通信制御部3 0 1と、トークン制御部3 0 2と、記憶部3 0 3と、を備える。

[0126] 通信制御部3 0 1は、他の装置との間の通信を制御する手段である。例え

ば、通信制御部301は、サーバ装置10からデータ（パケット）を受信する。また、通信制御部301は、サーバ装置10に向けてデータを送信する。通信制御部301は、他の装置から受信したデータを他の処理モジュールに引き渡す。通信制御部301は、他の処理モジュールから取得したデータを他の装置に向けて送信する。このように、他の処理モジュールは、通信制御部301を介して他の装置とデータの送受信を行う。通信制御部301は、他の装置からデータを受信する受信部としての機能と、他の装置に向けてデータを送信する送信部としての機能と、を備える。

[0127] トークン制御部302は、空港端末30におけるトークンに関する制御を行う手段である。トークン制御部302は、生体情報を用いた本人確認を行う。トークン制御部302の本人確認に関する動作は、端末40のトークン制御部202の本人確認に関する動作と同一とすることができるので説明を省略する。

[0128] トークン制御部302は、業務情報を利用者から取得する。例えば、トークン制御部302は、GUIを用いて業務情報（例えば、空港会員ID）を取得する。

[0129] あるいは、トークン制御部302は、業務情報を端末40から取得する。例えば、トークン制御部302は、GUIを用いて業務情報を取得する。例えば、トークン制御部302は、生体認証を用いて提供可能なサービスの一覧を表示する。利用者は、表示された一覧のなかから希望するサービスを選択する。例えば、利用者は、「顔決済での商品購入」を選択する。

[0130] トークン制御部302は、利用者が選択したサービスに応じた業務情報を取得する。例えば、トークン制御部302は、図13に示すようなGUIを使って業務情報を取得する。

[0131] 図13に示すGUIに接した利用者は、端末40を操作して、空港端末30が指示するアプリケーションを起動する。利用者は、起動したアプリケーションにおいて所定の操作を行う。端末40は、利用者の操作に応じて、業務情報が変換された2次元バーコードを表示する。例えば、エアポートアプ

リケーションは、空港会員IDに基づいて生成された2次元バーコードを表示する。

[0132] 図13に示すGUIにおいて、「決定」ボタンが押下された場合、トークン制御部302は、利用者が提示する2次元バーコードを読み取り、業務情報を取得する。

[0133] トークン制御部302は、利用者の生体情報と業務情報を含むトークン登録要求をサーバ装置10に送信する。トークン制御部302は、トークン登録要求に対する応答（トークン登録成功、トークン登録失敗）に応じた処理を実行する。

[0134] 記憶部303は、空港端末30の動作に必要な情報を記憶する手段である。

[0135] [サーバ装置]

図14は、第1の実施形態に係るサーバ装置10の処理構成（処理モジュール）の一例を示す図である。図14を参照すると、サーバ装置10は、通信制御部401と、トークン制御部402と、認証部403と、記憶部404と、を備える。

[0136] 通信制御部401は、他の装置との間の通信を制御する手段である。例えば、通信制御部401は、認証端末20からデータ（パケット）を受信する。また、通信制御部401は、認証端末20に向けてデータを送信する。通信制御部401は、他の装置から受信したデータを他の処理モジュールに引き渡す。通信制御部401は、他の処理モジュールから取得したデータを他の装置に向けて送信する。このように、他の処理モジュールは、通信制御部401を介して他の装置とデータの送受信を行う。通信制御部401は、他の装置からデータを受信する受信部としての機能と、他の装置に向けてデータを送信する送信部としての機能と、を備える。

[0137] トークン制御部402は、サーバ装置10におけるトークンに関する制御を行う手段である。トークン制御部402は、端末40又は空港端末30から受信するトークン登録要求を処理する。

- [0138] トークン登録要求を受信すると、トークン制御部402は、当該トークン登録要求に含まれる生体情報及び業務情報を利用者管理データベースに登録する（図15参照）。図15に示すように、利用者管理データベースは、利用者のユーザID、生体情報（特徴量）及び業務情報を対応付けて記憶する。
- [0139] 図15に示すように、利用者管理データベースは、取得した業務情報を永続的に記憶する業務情報と、一時的に記憶する業務情報に分類して記憶する。例えば、空港会員IDや航空会員IDは永続的に記憶される業務情報であり、搭乗券情報は一時的に記憶（例えば、登録から24時間に限り記憶）される業務情報である。
- [0140] システム管理者等は、各業務情報をいずれの記憶方式に分類するか決定し、サーバ装置10に設定する。システム管理者等は、業務情報の内容（性質）等を考慮して記憶方式を決定すればよい。例えば、空港会員ID等は繰り返し使用される業務情報であるが、搭乗券情報は利用者が航空機に搭乗することで使用が終了する業務情報である。システム管理者等は、これらの状況を考慮して各業務情報の記憶方式を決定する。
- [0141] 図15に示す利用者管理データベースは例示であって、記憶する項目等を限定する趣旨ではない。例えば、生体情報として「顔画像」が利用者管理データベースに登録されていてもよい。
- [0142] 図16は、第1の実施形態に係るトークン制御部402の動作の一例を示すフローチャートである。図16を参照し、トークン制御部402の動作を説明する。
- [0143] トークン登録要求を受信すると、トークン制御部402は、トークン登録要求に含まれる生体情報（顔画像）の品質を判定する（ステップS201）。
- [0144] 具体的には、トークン制御部402は、受信した顔画像が認証用途に足りる十分な品質を備えているか否かを判定する。例えば、トークン制御部402は、予め用意された学習モデルを用いて顔画像の品質を判定する。トークン

制御部402は、学習モデルに顔画像を入力し、判定結果を取得する。

- [0145] なお、当該学習モデルは、画像データ（顔画像）にラベル（品質；良い、悪い）が付与された数多くの教師データを用いた機械学習により得られる。学習モデルの生成には、サポートベクタマシン、ブースティングやニューラルネットワーク等の任意のアルゴリズムを用いることができる。なお、上記サポートベクタマシン等のアルゴリズムは公知の技術を使用することができるので、その説明を省略する。
- [0146] 顔画像の品質が悪いと（ステップS202、No分岐）、トークン制御部402は、トークンの登録に失敗したと判定する。この場合、トークン制御部402は、トークン登録失敗を示す否定応答をトークン登録要求の送信元に送信する（ステップS203）。
- [0147] 顔画像の品質が良いと（ステップS202、Yes分岐）、トークン制御部402は、トークンの登録を希望する利用者のエントリが利用者管理データベースに存在するか否かを判定する。
- [0148] 具体的には、トークン制御部402は、トークン登録要求に含まれる生体情報と利用者管理データベースに記憶された生体情報を用いた照合処理（1対N照合；Nは正の整数、以下同じ）を実行する（ステップS204）。
- [0149] トークン制御部402は、トークン登録要求に含まれる顔画像から特徴量を生成する。トークン制御部402は、当該生成した特徴量（特徴ベクトル）を照合側の特徴量、利用者管理データベースに登録された特徴量を登録側の特徴量にそれぞれ設定する。
- [0150] トークン制御部402は、照合側の特徴量と登録側の複数の特徴量それぞれの間の類似度を計算する。なお、当該類似度には、カイニ乗距離やユークリッド距離等を用いることができる。距離が離れているほど類似度は低く、距離が近いほど類似度が高い。
- [0151] トークン制御部402は、利用者管理データベースに登録された複数の特徴量のうち、照合対象の特徴量との間の類似度が所定の値以上の特徴量が存在すれば、照合処理に成功したと判断する。そのような特徴量が存在しなけ

れば、トークン制御部402は、照合処理に失敗したと判断する。

[0152] 照合処理に失敗すると（ステップS205、No分岐）、トークン制御部402は、利用者管理データベースに新たなエントリを追加する（ステップS206）。

[0153] その後、トークン制御部402は、利用者を識別するためのユーザIDを生成する。なお、ユーザIDは、利用者を一意に識別できる情報であればどのような情報であってもよい。例えば、トークン制御部402は、エントリの追加のたびに一意な値を採番しユーザIDとしてもよい。

[0154] トークン制御部402は、追加したエントリに、ユーザID、生体情報（特徴量）及び業務情報を記憶する（ステップS207）。

[0155] 照合処理に成功すると（ステップS205、Yes分岐）、トークン制御部402は、照合処理により特定されたエントリ（類似度が最も高い生体情報が記憶されたエントリ）に、業務情報を記憶する（ステップS208）。

[0156] 利用者管理データベースにトークンを登録すると、トークン制御部402は、トークン登録要求の送信元（空港端末30、端末40）に対してトークン登録成功を通知する。具体的には、トークン制御部402は、トークン登録成功を示す肯定応答をトークン登録要求の送信元に送信する（ステップS209）。

[0157] なお、トークン制御部402は、利用者管理データベースに登録された業務情報を削除する機能を有する。トークン制御部402は、定期的又は所定のタイミングで利用者管理データベースにアクセスする。トークン制御部402は、当該データベースの各エントリ（トークン）に一時的に記憶された業務情報うち、登録から所定時間経過（例えば、24時間経過）している業務情報を削除する。

[0158] 認証部403は、認証端末20を介してサービスの提供を受けようとする利用者（被認証者）を認証する手段である。認証部403は、空港内外に設置された各認証端末20（タッチポイント）から受信する認証要求を処理する。

- [0159] 図17は、第1の実施形態に係る認証部403の動作の一例を示すフローチャートである。図17を参照し、認証部403の動作を説明する。
- [0160] 認証要求には、被認証者の生体情報と端末IDが含まれる。
- [0161] 認証部403は、認証要求に含まれる生体情報と利用者管理データベースに記憶された生体情報を用いた照合処理（1対N照合；Nは正の整数、以下同じ）を実行する（ステップS301）。
- [0162] なお、認証部403による照合処理は、トークン制御部402による照合処理と同一とすることができるので詳細な説明を省略する。
- [0163] 照合処理に失敗すると（ステップS302、No分岐）、認証部403は、被認証者の認証に失敗した旨を示す否定応答を認証端末20に送信する（ステップS303）。
- [0164] 照合処理に成功すると（ステップS302、Yes分岐）、認証部403は、認証要求に含まれる端末IDを用いて認証要求の送信元である認証端末20（認証端末20の種類；例えば、POS端末、受付端末、デジタルサイネージ、ゲート装置等）を特定する。
- [0165] 例えば、認証部403は、認証端末20の種類と当該認証端末20が業務の提供に必要とする業務情報に対応付けて記憶するテーブル情報を参照し、認証端末20に応じた業務情報を特定する（図18参照）。なお、図18において、理解の容易のため、端末IDには図3に示す各認証端末20の種類を表記している。
- [0166] 認証部403は、利用者管理データベースから、当該特定された認証端末20に応じた業務情報の読み出しを試みる（ステップS304）。
- [0167] 認証端末20に応じた業務情報が利用者管理データベースから読み出せない場合（ステップS305、No分岐）、認証部403は、被認証者の認証に失敗したと判定する。この場合、認証部403は、被認証者の認証に失敗した旨を示す否定応答を認証端末20に送信する（ステップS303）。
- [0168] 認証端末20に応じた業務情報が利用者管理データベースから読み出せた場合（ステップS305、Yes分岐）、認証部403は、被認証者の認証

に成功したと判定する。この場合、認証部403は、被認証者の認証に成功した旨を示す肯定応答を認証端末20に送信する（ステップS306）。その際、認証部403は、利用者管理データベースから読み出した業務情報を含む肯定応答を認証端末20に送信する。

[0169] 記憶部404は、サーバ装置10の動作に必要な各種情報を記憶する。記憶部404には、利用者管理データベースが構築される。

[0170] [認証端末]

図19は、第1の実施形態に係る認証端末20の処理構成（処理モジュール）の一例を示す図である。図19を参照すると、認証端末20は、通信制御部501と、生体情報取得部502と、認証要求部503と、機能実現部504と、記憶部505と、を備える。

[0171] 通信制御部501は、他の装置との間の通信を制御する手段である。例えば、通信制御部501は、サーバ装置10からデータ（パケット）を受信する。また、通信制御部501は、サーバ装置10に向けてデータを送信する。通信制御部501は、他の装置から受信したデータを他の処理モジュールに引き渡す。通信制御部501は、他の処理モジュールから取得したデータを他の装置に向けて送信する。このように、他の処理モジュールは、通信制御部501を介して他の装置とデータの送受信を行う。通信制御部501は、他の装置からデータを受信する受信部としての機能と、他の装置に向けてデータを送信する送信部としての機能と、を備える。

[0172] 生体情報取得部502は、カメラ（図示せず）を制御し、利用者の生体情報を取得する手段である。例えば、生体情報取得部502は、例えば、売店の職員等の操作に応じて面前の利用者を撮影する。あるいは、生体情報取得部502は、定期的又は所定のタイミングにおいて自装置の前方を撮影する。生体情報取得部502は、取得した画像に人の顔画像が含まれるか否かを判定し、顔画像が含まれる場合には取得した画像データから顔画像を抽出する。

[0173] なお、生体情報取得部502による顔画像の検出処理や顔画像の抽出処理

には既存の技術を用いることができるので詳細な説明を省略する。例えば、生体情報取得部502は、CNN (Convolutional Neural Network) により学習された学習モデルを用いて、画像データの中から顔画像（顔領域）を抽出してもよい。あるいは、生体情報取得部502は、テンプレートマッチング等の手法を用いて顔画像を抽出してもよい。

[0174] 生体情報取得部502は、抽出した顔画像を認証要求部503に引き渡す。

[0175] 認証要求部503は、サーバ装置10に対して面前の利用者に関する認証を要求する手段である。認証要求部503は、取得した顔画像及び端末IDを含む認証要求を生成し、サーバ装置10に送信する。

[0176] 認証要求部503は、認証要求に対する応答（肯定応答、否定応答）をサーバ装置10から受信する。認証要求部503は、受信した応答を機能実現部504に引き渡す。

[0177] 機能実現部504は、各認証端末20に割り当てられた機能を実現する手段である。各認証端末20の機能実現部504に関する詳細な動作の説明は省略する。各認証端末20の動作は本願開示の趣旨とは異なるためである。

[0178] 記憶部505は、認証端末20の動作に必要な情報を記憶する手段である。

[0179] [システム動作]

続いて、第1の実施形態に係る情報処理システムの動作を説明する。図20は、第1の実施形態に係る情報処理システムの動作の一例を示すシーケンス図である。図20を参照し、端末40からトークン登録要求が送信される場合の情報処理システムの動作を説明する。

[0180] 端末40は、自装置にインストールされているアプリケーションから業務情報を取得し、当該取得した業務情報等を含むトークン登録要求をサーバ装置10に送信する（ステップS01）。

[0181] サーバ装置10は、トークン登録要求の受信に応じて、トークンを登録する（ステップS02）。

- [0182] サーバ装置１０は、トークン登録処理の結果（トークン登録成功、トークン登録失敗）を端末４０に送信する（ステップＳ０３）。
- [0183] 端末４０は、受信した結果（トークン登録成功、トークン登録失敗）に応じた処理を実行する（ステップＳ０４）。
- [0184] なお、利用者は、端末４０や空港端末３０を用いて、何度もトークン登録をサーバ装置１０に要求できる。例えば、利用者は、端末４０を用いて空港会員ＩＤに関するトークンの登録をサーバ装置１０に要求する。その後、利用者は、空港端末３０を用いて航空会員ＩＤに関するトークンの登録をサーバ装置１０に要求してもよい。
- [0185] 図２１は、第１の実施形態に係る情報処理システムの動作の一例を示すシーケンス図である。図２１を参照し、認証処理が行われる際の情報処理システムの動作を説明する。
- [0186] 認証端末２０は、利用者の生体情報を取得し、当該取得した生体情報を含む認証要求をサーバ装置１０に送信する（ステップＳ１１）。
- [0187] サーバ装置１０は、認証要求に含まれる生体情報と、利用者管理データベースに含まれる生体情報及び業務情報と、を用いた認証処理を実行する（ステップＳ１２）。
- [0188] サーバ装置１０は、認証結果（認証成功、認証失敗）を認証端末２０に送信する（ステップＳ１３）。
- [0189] 認証端末２０は、受信した認証結果（認証成功、認証失敗）に応じた処理を実行する（ステップＳ１４）。
- [0190] 続いて、第１の実施形態に係る変形例について説明する。
- [0191] <変形例>
- 上記実施形態では、サーバ装置１０は、認証要求を送信する認証端末２０の設置主体に関する業務情報を、当該認証端末２０に送信する場合について説明した。しかし、サーバ装置１０が送信する業務情報は、認証端末２０の設置主体に関する業務情報に限定されない。
- [0192] 例えば、空港会社が設置した認証端末２０－１（ＰＯＳ端末）から認証要

求を受信した場合、サーバ装置 10 は、空港会員 ID に替えて又は加えて航空会員 ID を当該認証端末 20-1 に送信してもよい。認証端末 20-1 は、生体認証に成功した被認証者の航空会員 ID を受信することで、当該被認証者は航空会社の会員であることを把握する。この場合、認証端末 20-1 は、航空会社の会員に対して、商品代金の割引を行う等の特典を付与することができる。

[0193] このように、第 1 の実施形態に係る情報処理システムでは、認証端末 20 の設置主体に依らず、サーバ装置 10 に予め設定された業務情報が認証端末 20 に送信される。その結果、異なる事業者（サービス提供者）間の業務提携等が容易に実現できる。

[0194] 例えば、空港会社 A と航空会社 B が業務提携をした場合を考える。空港会社 A は、複数の航空会社のうち航空会社 B の利用者（会員）を優遇するようなシステムを容易に構築できる。例えば、航空会社 B の会員が売店で商品を購入すると特典が付与される場合、サーバ装置 10 は、認証端末 20-1 からの認証要求に成功すると、航空会社 B の航空会員 ID を当該認証端末 20-1 に送信すればよい。あるいは、航空会社 B の会員にもラウジンの無料利用を認める場合、サーバ装置 10 は、認証端末 20-2（受付端末）からの認証要求を処理した際、当該航空会社 B の航空会員 ID を認証端末 20-2 に送信すればよい。

[0195] このような複数のサービス提供者に跨がった生体認証サービスの提供を実現するためには、システム管理者等は、図 18 に示すテーブル情報を書き換えればよい（テーブル情報を再設定すればよい）。

[0196] このように、サーバ装置 10 は、第 1 の事業者の第 1 の ID を業務情報として含むトークン登録要求を受信したことに応じて、利用者の生体情報と第 1 の ID を対応付けて利用者管理データベースに記憶する。さらに、サーバ装置 10 は、第 2 の事業者の第 2 の ID を業務情報として含むトークン登録要求を受信したことに応じて、当該利用者の生体情報、第 1 の ID 及び第 2 の ID を対応付けて利用者管理データベースに記憶する。

- [0197] 以上のように、第１の実施形態に係る端末４０は、生体認証を用いたサービスの享受に必要な業務情報を自装置（例えば、スマートフォン）にインストールされたアプリケーションから取得する。端末４０は、当該取得した業務情報と利用者の生体情報をサーバ装置１０に送信し、トークンの登録を依頼する。第１の実施形態に係る情報処理システムは、個人が所持する端末４０に分散して記憶されている業務情報を、トークン制御アプリケーションを介してシステム（サーバ装置１０）に登録する。そのため、サービス提供者のシステムが集中管理している業務情報をサーバ装置１０に送信する必要がない。その結果、生体認証を用いたサービスの提供に必要な情報のシステム登録が容易に実現される。
- [0198] サービス提供者が利用者に対して生体認証を用いた種々のサービスを提供する際、各サービスに応じた業務情報（例えば、会員情報）をどのような方法を使ってシステムに登録するのが問題になる。当該問題に対し、第１の実施形態に係る情報処理システムでは、端末４０に分散されて格納されている業務情報をトークン制御アプリケーションが収集し、当該収集した業務情報をサーバ装置１０に登録する。このような構成を採用することで、生体認証を用いた新規なサービスを容易に開始できる。即ち、近年、個人情報に対する利用者の意識の高まりからスマートフォン等に必要情報が登録される傾向にある。当該傾向は今後も継続すると予想される。スマートフォン等の端末４０から生体認証を用いたサービスに必要な業務情報が取得されれば、大掛かりなシステム連携等を実施しなくても生体認証に必要な情報をシステムに登録することが可能になる。
- [0199] また、第１の実施形態に係るサーバ装置１０は、利用者の生体情報を介して、各サービス提供者の情報（例えば、会員ＩＤ等の情報）を連携して記憶する。即ち、各サービス提供者の会員情報（会員ＩＤ）は、各システムから独立しつつ結合している「疎結合」の状態にある。サーバ装置１０は、このような会員情報（会員ＩＤ）を疎結合な状態で記憶することで、各サービス提供者間の連携を容易に実現できる。具体的には、システム管理者等が図１

8に示すようなテーブル情報を書き換えることで、各サービス提供者間の連携が容易に実現される。サーバ装置10は、認証処理に成功した際、書き換えられたテーブル情報に従って認証端末20（サービス提供者により設置されたデバイス）に当該サービス提供者と連携している他のサービス提供者の会員情報を送信すればよい。

[0200] [第2の実施形態]

続いて、第2の実施形態について図面を参照して詳細に説明する。

[0201] 第1の実施形態では、端末40にインストールされたアプリケーションが、トークン制御アプリケーションに対して業務情報を通知（プッシュ通知）する場合について説明した。第2の実施形態では、トークン制御アプリケーションが、他のアプリケーションに対して業務情報の提供を要求する場合について説明する。

[0202] なお、第2の実施形態に係る情報処理システムの構成は第1の実施形態と同一とすることができるので図3に相当する説明を省略する。また、第2の実施形態に係るサーバ装置10等の処理構成も第1の実施形態と同一とすることができるので、その説明を省略する。

[0203] 以下、第1の実施形態と第2の実施形態の相違点を中心に説明する。

[0204] 端末40は、利用者に提供可能な生体認証を用いたサービスの一覧を表示し、当該一覧表示されたサービスのなかから利用者が享受を希望するサービスを取得する。端末40は、自装置にインストールされたアプリケーションのなかから上記取得したサービス（利用者が選択したサービス）の提供に必要な業務情報を取得する。

[0205] 具体的には、端末40のトークン制御部202は、利用者が所定の動作を行うと、自装置にインストールされたアプリケーションから得られる業務情報を用いて利用者に提供可能なサービス（生体情報を用いたサービス）の一覧を表示する。

[0206] その際、トークン制御部202は、端末40にインストールされているアプリケーションの情報を取得する。例えば、トークン制御部202は、OS

(Operating System) から端末 40 にインストールされているアプリケーションの名称、バージョン等の情報を取得する。

- [0207] 次に、トークン制御部 202 は、端末 40 にインストールされているアプリケーションから得られる業務情報と利用者に提供可能なサービスに対応付けて記憶するテーブル情報を参照する。トークン制御部 202 は、当該テーブル情報を参照し、他のアプリケーションから得られる業務情報を使って利用者に提供可能なサービスの一覧を生成する。
- [0208] トークン制御部 202 は、生成したサービスの一覧を用いて図 22 に示すような GUI を表示する。トークン制御部 202 は、GUI を用いて利用者が享受を希望するサービスの情報を取得する。
- [0209] トークン制御部 202 は、利用者が希望するサービスに必要な業務情報を記憶するアプリケーションに対して、業務情報の提供を要求する。トークン制御部 202 は、Deep Link や API 等を用いて他のアプリケーションから必要な業務情報を取得する。
- [0210] 業務情報を取得すると、トークン制御部 202 は、利用者の本人確認を実行する。トークン制御部 202 は、利用者を撮影することで得られる顔画像と身分証明書から得られる顔画像を用いた本人確認を実行する。
- [0211] 本人確認に成功すると、トークン制御部 202 は、個人情報（生体情報及び業務情報）の第三者提供に対する利用者の同意を取得する。トークン制御部 202 は、図 6 や図 7 に類似する GUI を使って利用者の同意を取得する。
- [0212] 利用者の同意が得られると、トークン制御部 202 は、生体情報及び業務情報を含むトークン登録要求をサーバ装置 10 に送信する。
- [0213] なお、第 2 の実施形態においても、第 1 の実施形態と同様に、トークン制御部 202 は、個人情報の第三者提供に対する同意を取得した後に、利用者の生体情報を用いた本人確認を実行してもよい。この場合、トークン制御部 202 は、図 22 に示すような一覧表示画面において、個人情報の第三者提供に対する利用者の同意を取得してもよい。例えば、トークン制御部 202 は

、「第三者提供される生体情報」と、提供可能なサービスごとの「第三者提供される業務情報」及び「個人情報（生体情報、業務情報）の利用目的」を併せて表示してもよい。

[0214] 以上のように、第2の実施形態に係る端末40は、自装置にインストールされたアプリケーションから収集可能な業務情報に基づいて提供可能なサービスの一覧を利用者に提示する。端末40は、利用者が選択したサービスに応じた業務情報をアプリケーションから取得し、当該取得した業務情報をサーバ装置10に登録する。第2の実施形態においても、生体認証を用いたサービスの提供に必要な情報のシステム登録が容易に実現される。

[0215] [第3の実施形態]

続いて、第3の実施形態について図面を参照して詳細に説明する。

[0216] 第3の実施形態では、サーバ装置10が、利用者の行動履歴をサービス事業者等に提供する場合について説明する。

[0217] なお、第3の実施形態に係る情報処理システムの構成は第1及び第2の実施形態と同一とすることができるので図3に相当する説明を省略する。

[0218] 以下、第1の実施形態乃至第3の実施形態の相違点を中心に説明する。

[0219] 第3の実施形態に係る認証部403は、認証要求の受信に応じて実行した認証処理の詳細を行動履歴管理データベースに記憶する。認証部403は、認証処理の詳細を記憶することで利用者の行動履歴を生成する。

[0220] 例えば、認証部403は、生体認証に成功した日時、被認証者が使用した認証端末20に関する情報（例えば、設置場所や種類）等を行動履歴管理データベースに記憶する（図23参照）。あるいは、認証部403は、認証端末20から生体情報に加えて決済情報のような付随情報を取得できる場合には、当該付随情報も併せて行動履歴管理データベースに記憶する。

[0221] 認証部403は、被認証者の認証に成功すると、当該被認証者のユーザIDをキーとして行動履歴管理データベースを検索する。検索に成功すると、認証部403は、当該検索により特定されたエントリに行動履歴を記憶する。

- [0222] 検索に失敗すると、認証部403は、行動履歴管理データベースに新たなエントリを追加する。認証部403は、当該追加したエントリに、利用者のユーザIDと、利用者管理データベースに記憶された業務情報のうちサービス提供者が利用者を管理するIDに相当する情報を記憶する。図15に示す利用者管理データベースの例では、認証部403は、空港会社の会員ID（空港会員ID）と航空会社の会員ID（航空会員ID）を行動履歴管理データベースに記憶する。さらに、認証部403は、利用者の行動履歴を上記追加されたエントリに記憶する。
- [0223] 認証部403は、図23の行動履歴管理データベースに示されるような行動履歴を生成する。なお、図23に示す行動履歴管理データベースは例示であって、記憶する項目等を限定する趣旨ではない。
- [0224] 図24は、第3の実施形態に係るサーバ装置10の処理構成（処理モジュール）の一例を示す図である。図24を参照すると、第1の実施形態に係るサーバ装置10の構成に情報提供制御部405が追加されている。
- [0225] 情報提供制御部405は、システムに参加するサービス提供者等からの要求に基づいて利用者の行動に関する情報を提供する手段である。情報提供制御部405は、行動履歴管理データベースに記憶された行動履歴を用いて提供情報を生成し、当該生成された提供情報を出力する。
- [0226] 情報提供制御部405は、サービス提供者からの情報提供に関する要求を取得する。例えば、情報提供制御部405は、サービス提供者の担当者等がアクセス可能なポータルサイト等を用いてサービス提供者からの情報提供に関する要求を取得する。
- [0227] 情報提供制御部405は、サービス提供者から行動履歴を知りたい利用者のIDを取得する。例えば、空港会社は、自社の会員であって行動履歴を知りたい利用者のID（IDのリスト）をポータルサイトに入力する。
- [0228] 情報提供制御部405は、取得したID（IDリスト）をキーとして行動履歴管理データベースを検索し、対応するエントリを特定する。情報提供制御部405は、特定したエントリの行動履歴フィールドに記憶された行動履歴

歴をサービス提供者に提供する。

[0229] 以上のように、第3の実施形態に係るサーバ装置10は、被認証者の生体認証に成功すると、少なくとも認証端末20に関する情報を用いて当該被認証者の行動履歴を生成する。サーバ装置10は、被認証者の第1のID、第2のID及び生成された行動履歴を対応付けて行動履歴管理データベース（第2のデータベース）に記憶する。サーバ装置10は、第1の事業者から第1のIDを取得すると、当該第1のIDに対応する利用者の行動履歴を行動履歴管理データベースから読み出し、読み出した行動履歴を第1の事業者に提供する。その結果、複数のサービス事業者が関わる行動履歴が容易に収集される。即ち、第3の実施形態に係るサーバ装置10から提供される情報を活用することで、複数の事業者に跨がったデータの分析が可能になる。例えば、空港会社と鉄道会社は、MaaS（Mobility as a Service）の観点からのデータ分析が行える。なお、複数の事業者は互いに連携していてもよいし、連携していなくてもよい。

[0230] 続いて、情報処理システムを構成する各装置のハードウェアについて説明する。図25は、端末40のハードウェア構成の一例を示す図である。

[0231] 端末40は、情報処理装置（所謂、コンピュータ）により構成可能であり、図25に例示する構成を備える。例えば、端末40は、プロセッサ311、メモリ312、入出力インターフェイス313及び通信インターフェイス314等を備える。上記プロセッサ311等の構成要素は内部バス等により接続され、相互に通信可能に構成されている。

[0232] 但し、図25に示す構成は、端末40のハードウェア構成を限定する趣旨ではない。端末40は、図示しないハードウェアを含んでもよいし、必要に応じて入出力インターフェイス313を備えていなくともよい。また、端末40に含まれるプロセッサ311等の数も図25の例示に限定する趣旨ではなく、例えば、複数のプロセッサ311が端末40に含まれていてもよい。

[0233] プロセッサ311は、例えば、CPU（Central Processing Unit）、MPU（Micro Processing Unit）、DSP（Digital Signal Processor）等のプ

ログラムブルなデバイスである。あるいは、プロセッサ311は、FPGA (Field Programmable Gate Array)、ASIC (Application Specific Integrated Circuit) 等のデバイスであってもよい。プロセッサ311は、オペレーティングシステム(OS; Operating System)を含む各種プログラムを実行する。

[0234] メモリ312は、RAM (Random Access Memory)、ROM (Read Only Memory)、HDD (Hard Disk Drive)、SSD (Solid State Drive) 等である。メモリ312は、OSプログラム、アプリケーションプログラム、各種データを格納する。

[0235] 入出力インターフェイス313は、図示しない表示装置や入力装置のインターフェイスである。表示装置は、例えば、液晶ディスプレイ等である。入力装置は、例えば、キーボードやマウス等のユーザ操作を受け付ける装置である。

[0236] 通信インターフェイス314は、他の装置と通信を行う回路、モジュール等である。例えば、通信インターフェイス314は、NIC (Network Interface Card) 等を備える。

[0237] 端末40の機能は、各種処理モジュールにより実現される。当該処理モジュールは、例えば、メモリ312に格納されたプログラムをプロセッサ311が実行することで実現される。また、当該プログラムは、コンピュータが読み取り可能な記憶媒体に記録することができる。記憶媒体は、半導体メモリ、ハードディスク、磁気記録媒体、光記録媒体等の非トランジエント (non-transitory) なものとすることができる。即ち、本発明は、コンピュータプログラム製品として具現することも可能である。また、上記プログラムは、ネットワークを介してダウンロードするか、あるいは、プログラムを記憶した記憶媒体を用いて、更新することができる。さらに、上記処理モジュールは、半導体チップにより実現されてもよい。

[0238] なお、サーバ装置10等も端末40と同様に情報処理装置により構成可能であり、その基本的なハードウェア構成は端末40と相違する点はないので

説明を省略する。

[0239] 情報処理装置である端末40は、コンピュータを搭載し、当該コンピュータにプログラムを実行させることで端末40の機能が実現できる。また、端末40は、当該プログラムにより端末40の制御方法を実行する。

[0240] [変形例]

なお、上記実施形態にて説明した情報処理システムの構成、動作等は例示であって、システムの構成等を限定する趣旨ではない。

[0241] 上記実施形態では、空港における認証システムを例にとり本願開示の情報処理システムの動作を説明した。しかし、本願開示の情報処理システムは、空港以外の施設を対象としてもよい。例えば、情報処理システムは、ターミナル駅等の大規模な駅における認証システムを対象としてもよい。あるいは、情報処理システムは、イベント会場等の認証システムを対象としてもよい。

[0242] 上記実施形態では、国内線の離着陸が行われる空港を例にとり本願開示の情報処理システムについて説明した。しかし、本願開示の情報処理システムは、国際線の離着陸が行われる空港を対象としてもよい。この場合、利用者は、端末40に格納されたパスポート情報を業務情報としてサーバ装置10に登録すればよい。

[0243] 上記実施形態では、トークン制御アプリケーション以外のアプリケーションの例として、エアポートアプリケーションやエアラインアプリケーションを例にとり説明を行った。しかし、端末40にインストールされたアプリケーションをこれらのアプリケーションに限定する趣旨ではないことは当然である。トークン制御アプリケーションは、端末40にインストールされた任意のアプリケーションから業務情報を取得することができる。例えば、トークン制御アプリケーションは、鉄道会社の会員が用いるトレインアプリケーションから業務情報を取得してもよい。

[0244] 上記実施形態では、システム管理者が各業務情報の記憶方式（永続的に記憶、一時的に記憶）をサーバ装置10に設定する場合について説明した。当

該記憶方式の選択は、利用者自身によって行われてもよい。例えば、端末40は、図6や図7に示すGUIによって個人情報の第三者提供に関する利用者の同意を取得する際、利用者が業務情報の記憶方式を選択可能としてもよい。

[0245] 第2の実施形態において、端末40にインストールされたアプリケーションから得られる業務情報を使って提供可能なサービスの一覧表示が利用者に提供されることを説明した（図22参照）。しかし、端末40は、システムとして利用者に提供可能なサービス（生体認証を用いたサービス）の一覧を生成しGUIを表示してもよい。また、利用者が端末40にインストールされていないアプリケーションから取得可能な業務情報に用いられるサービスを選択した場合、端末40は、当該インストールされていないアプリケーションのインストールを利用者に促してもよい。例えば、エアラインアプリケーションから取得可能な搭乗情報を用いた「搭乗ゲートの顔パス」が選択され、端末40に当該エアラインアプリケーションがインストールされていない場合、端末40は、エアラインアプリケーションのインストールを促す。なお、システムとして利用者に提供可能なサービスの一覧を利用者に提示する場合であっても、第2の実施形態で説明したように、端末40は、個人情報の第三者提供に対する利用者の同意を取得した後に、生体情報を利用した本人確認を実行してもよい。

[0246] あるいは、端末40は、自装置にインストールされたアプリケーションのバージョンが古く適切な業務情報を取得できない場合等に、アプリケーションのバージョンアップを利用者に促してもよい。

[0247] 上記実施形態では、トークン発行時（トークン登録時）の生体情報に関する品質確認をサーバ装置10が実施する場合について説明した。当該品質確認は、空港端末30や端末40にて実行されてもよい。

[0248] 上記実施形態では、顔画像に係る生体情報がサーバ装置10と認証端末20の間で送受信される場合について説明した。しかし、顔画像から生成された特徴量が上記装置間で送受信されてもよい。この場合、受信側のサーバ装

置 1 0 が、受信した特徴量を利用し、その後の処理に当該受信した特徴量を活用してもよい。あるいは、利用者管理データベースに記憶される生体情報は特徴量であってもよいし顔画像であってもよい。顔画像が記憶されている場合には、必要に応じて顔画像から特徴量が生成されればよい。あるいは、顔画像と特徴量の両方が利用者管理データベースに記憶されていてもよい。

[0249] 上記実施形態では、サーバ装置 1 0 の内部に利用者管理データベースが構成される場合について説明したが、当該利用者管理データベースは外部のデータベースサーバ等に構築されてもよい。即ち、サーバ装置 1 0 等の一部の機能は別のサーバに実装されていてもよい。より具体的には、上記説明した「トークン制御部（トークン制御手段）」等がシステムに含まれるいずれかの装置に実装されていけばよい。

[0250] 各装置（サーバ装置 1 0、端末 4 0 等）間のデータ送受信の形態は特に限定されないが、これら装置間で送受信されるデータは暗号化されていてもよい。これらの装置間では、生体情報等が送受信され、個人情報を適切に保護するためには、暗号化されたデータが送受信されることが望ましい。

[0251] 上記説明で用いた流れ図（フローチャート、シーケンス図）では、複数の工程（処理）が順番に記載されているが、実施形態で実行される工程の実行順序は、その記載の順番に制限されない。実施形態では、例えば各処理を並行して実行する等、図示される工程の順番を内容的に支障のない範囲で変更することができる。

[0252] 上記の実施形態は本願開示の理解を容易にするために詳細に説明したものであり、上記説明したすべての構成が必要であることを意図したものではない。また、複数の実施形態について説明した場合には、各実施形態は単独で用いてもよいし、組み合わせて用いてもよい。例えば、実施形態の構成の一部を他の実施形態の構成に置き換えることや、実施形態の構成に他の実施形態の構成を加えることも可能である。さらに、実施形態の構成の一部について他の構成の追加、削除、置換が可能である。

[0253] 上記の説明により、本発明の産業上の利用可能性は明らかであるが、本発

明は、利用者に生体認証を用いたサービスを提供する情報処理システムなどに好適に適用可能である。

[0254] 上記の実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

[付記 1]

利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得する、取得手段と、

前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求をサーバ装置に送信する、送信手段と、

を備える、端末。

[付記 2]

前記トークン登録要求を前記サーバ装置に送信する前に、前記業務情報及び生体情報を第三者提供することに対する前記利用者の同意を取得する、同意取得手段をさらに備える、付記 1 に記載の端末。

[付記 3]

前記利用者から取得した生体情報と前記利用者が所持する身分証明書から取得した生体情報を用いた本人確認を実行する、本人確認手段をさらに備える、

前記送信手段は、前記本人確認に成功した後に、前記トークン登録要求を前記サーバ装置に送信する、付記 2 に記載の端末。

[付記 4]

前記取得手段は、

前記利用者に提供可能な生体認証を用いたサービスの一覧を表示し、前記一覧表示されたサービスのなかから前記利用者が享受を希望するサービスを取得し、

前記自装置にインストールされたアプリケーションのなかから前記取得したサービスの提供に必要な業務情報を取得する、付記 3 に記載の端末。

[付記 5]

サーバ装置と、
利用者が所持する端末と、
を含み、
前記端末は、

前記利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得し、前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求を前記サーバ装置に送信し、

前記サーバ装置は、

前記トークン登録要求の受信に応じて、前記利用者の生体情報及び業務情報を対応付けて第 1 のデータベースに記憶する、システム。

[付記 6]

前記サーバ装置は、

第 1 の事業者の第 1 の ID を前記業務情報として含む前記トークン登録要求を受信したことに応じて、前記利用者の生体情報と前記第 1 の ID を対応付けて前記第 1 のデータベースに記憶し、

第 2 の事業者の第 2 の ID を前記業務情報として含む前記トークン登録要求を受信したことに応じて、前記利用者の生体情報、前記第 1 の ID 及び前記第 2 の ID を対応付けて前記第 1 のデータベースに記憶する、付記 5 に記載のシステム。

[付記 7]

前記サーバ装置は、

被認証者の生体情報を含む認証要求を認証端末から受信し、

前記受信した認証要求に含まれる生体情報と前記第 1 のデータベースに記憶された生体情報を用いた照合処理により前記被認証者を特定し、前記第 1 のデータベースに記憶された、前記被認証者の少なくとも 1 以上の業務情報のうち前記認証端末に対応する業務情報を前記認証端末に送信する、付記 6

に記載のシステム。

[付記 8]

前記サーバ装置は、

前記被認証者の生体認証に成功すると、少なくとも前記認証端末に関する情報を用いて前記被認証者の行動履歴を生成し、前記被認証者の前記第 1 の ID、前記第 2 の ID 及び前記生成された行動履歴を対応付けて第 2 のデータベースに記憶する、付記 7 に記載のシステム。

[付記 9]

前記サーバ装置は、

前記第 1 の事業者から前記第 1 の ID を取得すると、前記第 1 の ID に対応する利用者の行動履歴を前記第 2 のデータベースから読み出し、前記読み出した行動履歴を前記第 1 の事業者に提供する、付記 8 に記載のシステム。

[付記 10]

前記生体情報は、顔画像又は前記顔画像から生成された特徴量である、付記 5 乃至 9 のいずれか一項に記載のシステム。

[付記 11]

端末において、

利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得し、

前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求をサーバ装置に送信する、端末の制御方法。

[付記 12]

端末に搭載されたコンピュータに、

利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得する処理と、

前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求をサーバ装置に送信する処理と、

を実行させるためのプログラムを記憶する、コンピュータ読取可能な記憶

媒体。

[0255] なお、引用した上記の先行技術文献の各開示は、本書に引用をもって繰り込むものとする。以上、本発明の実施形態を説明したが、本発明はこれらの実施形態に限定されるものではない。これらの実施形態は例示にすぎないということ、及び、本発明のスコップ及び精神から逸脱することなく様々な変形が可能であるということは、当業者に理解されるであろう。即ち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得る各種変形、修正を含むことは勿論である。

符号の説明

[0256] 10 サーバ装置
20 認証端末
20-1 認証端末
20-2 認証端末
20-3 認証端末
20-4 認証端末
30 空港端末
40 端末
100 端末
101 取得手段
102 送信手段
201 通信制御部
202 トークン制御部
203 記憶部
301 通信制御部
302 トークン制御部
303 記憶部
311 プロセッサ
312 メモリ

- 3 1 3 入出力インターフェイス
- 3 1 4 通信インターフェイス
- 4 0 1 通信制御部
- 4 0 2 トークン制御部
- 4 0 3 認証部
- 4 0 4 記憶部
- 4 0 5 情報提供制御部
- 5 0 1 通信制御部
- 5 0 2 生体情報取得部
- 5 0 3 認証要求部
- 5 0 4 機能実現部
- 5 0 5 記憶部

請求の範囲

- [請求項1] 利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得する、取得手段と、
- 前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求をサーバ装置に送信する、送信手段と、
- を備える、端末。
- [請求項2] 前記トークン登録要求を前記サーバ装置に送信する前に、前記業務情報及び生体情報を第三者提供することに対する前記利用者の同意を取得する、同意取得手段をさらに備える、請求項1に記載の端末。
- [請求項3] 前記利用者から取得した生体情報と前記利用者が所持する身分証明書から取得した生体情報を用いた本人確認を実行する、本人確認手段をさらに備え、
- 前記送信手段は、前記本人確認に成功した後に、前記トークン登録要求を前記サーバ装置に送信する、請求項2に記載の端末。
- [請求項4] 前記取得手段は、
- 前記利用者に提供可能な生体認証を用いたサービスの一覧を表示し、前記一覧表示されたサービスのなかから前記利用者が享受を希望するサービスを取得し、
- 前記自装置にインストールされたアプリケーションのなかから前記取得したサービスの提供に必要な業務情報を取得する、請求項3に記載の端末。
- [請求項5] サーバ装置と、
- 利用者が所持する端末と、
- を含み、
- 前記端末は、
- 前記利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取

得し、前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求を前記サーバ装置に送信し、

前記サーバ装置は、

前記トークン登録要求の受信に応じて、前記利用者の生体情報及び業務情報を対応付けて第1のデータベースに記憶する、システム。

[請求項6]

前記サーバ装置は、

第1の事業者の第1のIDを前記業務情報として含む前記トークン登録要求を受信したことに応じて、前記利用者の生体情報と前記第1のIDを対応付けて前記第1のデータベースに記憶し、

第2の事業者の第2のIDを前記業務情報として含む前記トークン登録要求を受信したことに応じて、前記利用者の生体情報、前記第1のID及び前記第2のIDを対応付けて前記第1のデータベースに記憶する、請求項5に記載のシステム。

[請求項7]

前記サーバ装置は、

被認証者の生体情報を含む認証要求を認証端末から受信し、

前記受信した認証要求に含まれる生体情報と前記第1のデータベースに記憶された生体情報を用いた照合処理により前記被認証者を特定し、前記第1のデータベースに記憶された、前記被認証者の少なくとも1以上の業務情報のうち前記認証端末に対応する業務情報を前記認証端末に送信する、請求項6に記載のシステム。

[請求項8]

前記サーバ装置は、

前記被認証者の生体認証に成功すると、少なくとも前記認証端末に関する情報を用いて前記被認証者の行動履歴を生成し、前記被認証者の前記第1のID、前記第2のID及び前記生成された行動履歴を対応付けて第2のデータベースに記憶する、請求項7に記載のシステム。

[請求項9]

前記サーバ装置は、

前記第1の事業者から前記第1のIDを取得すると、前記第1のID

Dに対応する利用者の行動履歴を前記第2のデータベースから読み出し、前記読み出した行動履歴を前記第1の事業者を提供する、請求項8に記載のシステム。

[請求項10] 前記生体情報は、顔画像又は前記顔画像から生成された特徴量である、請求項5乃至9のいずれか一項に記載のシステム。

[請求項11] 端末において、
利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得し、
前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求をサーバ装置に送信する、端末の制御方法。

[請求項12] 端末に搭載されたコンピュータに、
利用者が生体認証を用いたサービスの提供を受けるために必要な業務情報を、自装置にインストールされたアプリケーションから取得する処理と、
前記取得された業務情報と前記利用者の生体情報を含むトークン登録要求をサーバ装置に送信する処理と、
を実行させるためのプログラムを記憶する、コンピュータ読取可能な記憶媒体。