

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7298733号
(P7298733)

(45)発行日 令和5年6月27日(2023.6.27)

(24)登録日 令和5年6月19日(2023.6.19)

(51)国際特許分類 F I
G 0 6 F 21/32 (2013.01) G 0 6 F 21/32
G 0 6 Q 50/26 (2012.01) G 0 6 Q 50/26

請求項の数 13 (全33頁)

(21)出願番号	特願2022-31425(P2022-31425)	(73)特許権者	000004237
(22)出願日	令和4年3月2日(2022.3.2)		日本電気株式会社
(62)分割の表示	特願2021-566965(P2021-566965))の分割		東京都港区芝五丁目7番1号
原出願日	令和2年9月11日(2020.9.11)	(74)代理人	100109313
(65)公開番号	特開2022-82548(P2022-82548A)		弁理士 机 昌彦
(43)公開日	令和4年6月2日(2022.6.2)	(74)代理人	100149618
審査請求日	令和4年3月2日(2022.3.2)		弁理士 北嶋 啓至
		(72)発明者	大谷 巧
			東京都港区芝五丁目7番1号
			日本電気株式会社内
		(72)発明者	笹本 武史
			東京都港区芝五丁目7番1号
			日本電気株式会社内
		(72)発明者	井上 淳一
			東京都港区芝五丁目7番1号
			最終頁に続く

(54)【発明の名称】 サーバ装置、システム、サーバ装置の制御方法及びコンピュータプログラム

(57)【特許請求の範囲】

【請求項1】

複数の端末のうちの予め定められた一つの端末から取得した被認証者の生体情報を用いたパスポートの正当性判定に成功した場合に、パスポートの正当性判定に成功した被認証者に対応するトークンIDを発行するトークン生成部と、

複数の端末のうち、前記一つの端末以外の端末から、当該端末により取得された被認証者の生体情報を含む認証要求を受信する、受信部と、
受信された認証要求に応じて被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行う、認証部と、

前記生体認証に成功した被認証者である認証成功者ごとに、パスポート情報、予め登録された生体情報、及び、搭乗予約情報が関連付けられた認証成功者に対応するトークンIDと、前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する、記憶部と、

を備える、サーバ装置。

【請求項2】

前記記憶部が記憶する前記認証結果詳細情報は、前記認証要求の送信元を識別する端末IDをさらに含み、

少なくとも予め登録された利用者の生体情報、端末ID、及び、当該端末IDに対応する端末により取得された生体情報を含む認証結果検証情報を生成する、検証情報生成部をさらに備える、請求項1に記載のサーバ装置。

10

20

【請求項 3】

前記認証結果詳細情報は、前記生体認証により認証成功と判定された際の類似度に関する情報を含む、請求項 2 に記載のサーバ装置。

【請求項 4】

前記検証情報生成部は、前記認証結果詳細情報を解析し、前記認証結果検証情報を生成するか否かを判定する、請求項 2 に記載のサーバ装置。

【請求項 5】

前記検証情報生成部は、認証成功と判定された際の類似度に基づいて、前記認証結果検証情報を生成するか否かを決定する、請求項 3 に記載のサーバ装置。

【請求項 6】

前記検証情報生成部は、前記認証結果詳細情報に含まれる前記類似度が第 1 の閾値よりも小さい場合に、前記認証結果検証情報を生成する、請求項 5 に記載のサーバ装置。

【請求項 7】

認証成功者についての前記認証結果詳細情報は、前記認証要求の送信元の端末ごとに、当該端末により取得された生体情報を用いた前記生体認証により認証成功と判定された場合に生成され、前記生体認証により認証成功と判定された際の類似度に関する情報を含み、

前記検証情報生成部は、認証成功者について複数の前記認証結果詳細情報が生成されている場合に、それら認証結果詳細情報に含まれている類似度のうち、最も大きい第 1 類似度と 2 番目に値の大きい第 2 類似度の差分が、第 2 の閾値よりも小さい場合に、前記認証結果検証情報を生成する、請求項 5 に記載のサーバ装置。

【請求項 8】

認証成功者についての前記認証結果詳細情報は、前記認証要求の送信元の端末ごとに、当該端末により取得された生体情報を用いた前記生体認証により認証成功と判定された場合に生成され、前記生体認証により認証成功と判定された際の類似度に関する情報を含み、

前記検証情報生成部は、認証成功者について複数の前記認証結果詳細情報が生成されている場合に、それら認証結果詳細情報に含まれている類似度を要素とする時系列データに対する統計処理の結果に基づいて、前記認証結果詳細情報を生成するか否かを決定する、請求項 5 に記載のサーバ装置。

【請求項 9】

前記検証情報生成部は、前記認証結果検証情報を、空港又は航空会社の職員が使用する職員端末に送信する、請求項 2 乃至請求項 8 のいずれか一項に記載のサーバ装置。

【請求項 10】

前記検証情報生成部は、定期的又は所定のタイミングで前記認証結果詳細情報を解析し、生成する必要があると判定された前記認証結果検証情報と共に、対応する認証成功者のフライトに関する情報を前記職員端末に送信する、請求項 9 に記載のサーバ装置。

【請求項 11】

複数の端末と、

複数の前記端末と接続された請求項 1 に記載のサーバ装置と、
を備える、システム。

【請求項 12】

サーバ装置が、

複数の端末のうちの予め定められた一つの端末から取得した被認証者の生体情報を用いたパスポートの正当性判定に成功した場合に、パスポートの正当性判定に成功した被認証者に対応するトークン ID を発行し、

複数の端末のうち、前記一つの端末以外の端末から、当該端末により取得された被認証者の生体情報を含む認証要求を受信し、
受信された認証要求に応じて被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行い、

前記生体認証に成功した被認証者である認証成功者ごとに、パスポート情報、予め登録された生体情報、及び、搭乗予約情報が関連付けられた認証成功者に対応するトークン ID

10

20

30

40

50

Dと、前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する、サーバ装置の制御方法。

【請求項 13】

サーバ装置に搭載されたコンピュータに、
複数の端末のうちの予め定められた一つの端末から取得した被認証者の生体情報を用いたパスポートの正当性判定に成功した場合に、パスポートの正当性判定に成功した被認証者に対応するトークンIDを発行する処理と、

複数の端末のうち、前記一つの端末以外の端末から、当該端末により取得された被認証者の生体情報を含む認証要求を受信する処理と、
受信された認証要求に応じて被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行う処理と、

前記生体認証に成功した被認証者である認証成功者ごとに、パスポート情報、予め登録された生体情報、及び、搭乗予約情報が関連付けられた認証成功者に対応するトークンIDと、前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する処理と

を実行させるためのコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、サーバ装置、システム、サーバ装置の制御方法及び記憶媒体に関する。

【背景技術】

【0002】

空港や港等において出入国審査が行われる。当該出入国審査の担当官は、パスポートに貼付された顔写真と面前の人物の顔を比較し、パスポートの顔画像と面前の人物の顔が一致する場合に当該人物の出入国を許可する。

【0003】

上記出入国審査の手続きを、生体認証を用いて行うことに関する技術開発が行われている。

【0004】

例えば、特許文献1に記載された移動監視方法は、パブリックエリアからセキュアエリアへの人の移動経路における第一のポイントで、個人のバイオメトリクスデータおよび関連身元確認データを取得する。当該移動監視方法は、セキュアエリアにおける第二のポイントで、個人のバイオメトリクスデータおよび関連身元確認データを取得する。当該移動監視方法は、第二のポイントにおいて取得された身元確認データを、第二のポイントで取得されたものと比較する。さらに、当該移動監視方法は、整合性がある場合には、この整合性のある身元確認データについて、第一のポイントで取得された関連イメージを、第二のポイントで取得された関連イメージと比較する。

【0005】

特許文献2には、精度改善施策の効果を事前に推定し、管理者へ提示できる技術を提供する、と記載されている。

【先行技術文献】

【特許文献】

【0006】

【文献】特表2007-506159号公報
特開2014-081796号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

特許文献1、2に開示されたように、生体認証に関する種々の技術開発が行われている。しかしながら、生体認証の精度には限界があり一定比率の誤認証（他人受入、本人拒否

10

20

30

40

50

）が生じ得る。空港における手続きにおいて誤認証が発生すると、当該誤認証の修正に時間を要したり、利用者が誤った搭乗機に搭乗したまま外国に出国してしまったりする。

【０００８】

本発明は、生体認証における誤認証（とりわけ、他人受入）の発生を検出可能とすることに寄与する、サーバ装置、システム、サーバ装置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、複数の端末のうち被認証者の生体情報を取得した端末から、前記被認証者の生体情報を含む認証要求を受信する、受信部と、前記被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行う、認証部と、前記生体認証に成功した認証成功者について、前記予め登録された生体情報と、前記認証要求を処理した際の詳細を含む情報であって前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する、記憶部と、を備える、サーバ装置が提供される。

10

【００１０】

本発明の第２の視点によれば、複数の端末と、前記複数の端末と接続されたサーバ装置と、を含み、前記サーバ装置は、前記複数の端末のうち被認証者の生体情報を取得した端末から、前記被認証者の生体情報を含む認証要求を受信する、受信部と、前記被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行う、認証部と、前記生体認証に成功した認証成功者について、前記予め登録された生体情報と、前記認証要求を処理した際の詳細を含む情報であって前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する、記憶部と、を備える、システムが提供される。

20

【００１１】

本発明の第３の視点によれば、サーバ装置において、複数の端末のうち被認証者の生体情報を取得した端末から、前記被認証者の生体情報を含む認証要求を受信し、前記被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行い、前記生体認証に成功した認証成功者について、前記予め登録された生体情報と、前記認証要求を処理した際の詳細を含む情報であって前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する、サーバ装置の制御方法が提供される。

30

【００１２】

本発明の第４の視点によれば、サーバ装置に搭載されたコンピュータに、複数の端末のうち被認証者の生体情報を取得した端末から、前記被認証者の生体情報を含む認証要求を受信する処理と、前記被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行う処理と、前記生体認証に成功した認証成功者について、前記予め登録された生体情報と、前記認証要求を処理した際の詳細を含む情報であって前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する処理と、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。

40

【発明の効果】

【００１３】

本発明の各視点によれば、生体認証における誤認証（とりわけ、他人受入）の発生を検出可能とすることに寄与する、サーバ装置、システム、サーバ装置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】一実施形態の概要を説明するための図である。

50

【図 2】第 1 の実施形態に係る搭乗手続きシステムの概略構成の一例を示す図である。

【図 3】第 1 の実施形態に係るチェックイン端末の処理構成の一例を示す図である。

【図 4】第 1 の実施形態に係るシステム登録部の動作を説明するための図である。

【図 5】第 1 の実施形態に係るシステム登録部の処理構成の一例を示す図である。

【図 6】第 1 の実施形態に係る搭乗ゲート装置の処理構成の一例を示す図である。

【図 7】第 1 の実施形態に係る認証要求の一例を示す図である。

【図 8】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 9】第 1 の実施形態に係るトークン ID 情報データベースの一例を示す図である。

【図 10】第 1 の実施形態に係る業務情報データベースの一例を示す図である。

【図 11】第 1 の実施形態に係る認証結果データベースの一例を示す図である。

【図 12】第 1 の実施形態に係る検証情報生成部の動作を説明するための図である。

【図 13】第 1 の実施形態に係る検証情報生成部の動作を説明するための図である。

【図 14】第 1 の実施形態に係る搭乗手続きシステムの動作の一例を示すシーケンス図である。

【図 15】第 2 の実施形態に係る検証情報生成部の動作を説明するための図である。

【図 16】サーバ装置のハードウェア構成の一例を示す図である。

【図 17】本願開示の変形例に係るサーバ装置の動作を説明するための図である。

【図 18】本願開示の変形例に係る職員端末の動作を説明するための図である。

【図 19】本願開示の変形例に係る職員端末の動作を説明するための図である。

【図 20】本願開示の変形例に係る職員端末の動作を説明するための図である。

【図 21】本願開示の変形例に係るサーバ装置の処理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】

一実施形態に係るサーバ装置 100 は、受信部 101 と、認証部 102 と、記憶部 103 と、を備える（図 1 参照）。受信部 101 は、複数の端末のうち被認証者の生体情報を取得した端末から、被認証者の生体情報を含む認証要求を受信する。認証部 102 は、被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行う。記憶部 103 は、生体認証に成功した認証成功者について、予め登録された生体情報と認証結果詳細情報を対応付けて記憶する。認証結果詳細情報は、認証要求の送信元である端末により取得された生体情報を含む。

【0017】

サーバ装置 100 は、端末からの認証要求を処理するたびに、その結果（履歴）の詳細を記憶する。当該履歴情報を用いることで、サーバ装置 100 は、空港等の職員が認証結果に誤認証（とりわけ、他人受入に係る誤認証）が含まれているか否か検証するための認証結果検証情報を生成することができる。当該情報は、職員等に提供され、職員は、当該情報に基づいて生成された表示を確認することで他人受入の発生を検出できる。ここで、認証結果検証情報には、認証に使われた 2 種類の生体情報（例えば、登録顔画像、取得顔画像）に加え、取得顔画像を取得した端末の ID を含ませることもできる。職員等は、当該端末の ID に基づいて誤認証が発生した端末を特定することができるので、他人受入の発生に伴う問題、矛盾を迅速に解決できる。

【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2は、第1の実施形態に係る搭乗手続きシステムの概略構成の一例を示す図である。第1の実施形態に係る搭乗手続きシステムは、空港における一連の手続き（荷物預け入れ、セキュリティチェック等）を生体認証にて実現するシステムである。図2に示す搭乗手続きシステムは、例えば、入出国の管理局等の公的機関や当該公的機関から業務の委託を受けた受託者により運営される。

10

【0021】

なお、本願開示において、「搭乗手続き」は、チェックインから航空機に搭乗するまでに行われる一連の手続きを示す。

【0022】

図2を参照すると、搭乗手続きシステムには、チェックイン端末10、手荷物預け機11、旅客通過システム12、ゲート装置13、搭乗ゲート装置14と、サーバ装置20、職員端末30と、が含まれる。

【0023】

チェックイン端末10、手荷物預け機11、旅客通過システム12、ゲート装置13及び搭乗ゲート装置14は空港に設置された端末（タッチポイント）である。これらの端末は、ネットワークを介してサーバ装置20と接続されている。図2に示すネットワークは、空港の構内通信網を含むLAN（Local Area Network）、WAN（Wide Area Network）、移動体通信網等により構成されている。接続方式は、有線方式に限らず、無線方式でもよい。

20

【0024】

サーバ装置20は、空港会社等の施設内に設置されている。あるいは、サーバ装置20はネットワーク上のクラウドに設置されたサーバであってもよい。

【0025】

職員端末30は、空港や航空会社の職員等により使用される端末である。搭乗手続きシステムには1台の職員端末30が含まれていてもよいし、複数の職員端末30が含まれていてもよい。

30

【0026】

職員端末30は、図2に示すような据え置き型のコンピュータであってもよいし、携帯電話、スマートフォン、タブレット、ノートパソコンのような携帯型端末であってもよい。職員端末30は、職員が使用する端末であればどのような形式、形態であってもよい。

【0027】

なお、図2に示す構成は例示であって、搭乗手続きシステムの構成を限定する趣旨ではない。搭乗手続きシステムには、図示していない装置等が含まれていてもよい。

【0028】

利用者の搭乗手続きは、図2に示す各端末により行われる。具体的には、利用者が出国する際の一連の手続きは、5か所に設置された端末にて順次実施される。図2に示す搭乗手続きシステムでは、利用者の搭乗手続きは生体情報を用いた認証（生体認証）により実現される。

40

【0029】

本願開示における生体情報は、顔画像、指紋画像、虹彩画像、指の静脈画像、掌紋画像、手のひらの静脈画像等である。あるいは、生体情報は、人の声を記憶した音声データ（声紋）であってもよい。生体情報は、1つであっても複数であってもよい。なお、本願開示における「生体情報」の文言は、生体の全部又は一部を含む画像データ、音声データ及び当該画像から抽出される特徴量を意味するものとする。

50

【0030】

生体認証による搭乗手続きを希望する利用者（システム利用者）は、空港に到着すると、チェックイン端末10を操作して「チェックイン手続き」を行う。システム利用者は、紙の航空券、搭乗情報が記載された二次元バーコード、eチケットの控えを表示する携帯端末等をチェックイン端末10に提示する。チェックイン端末10は、チェックイン手続きが終了すると、搭乗券を出力する。なお、搭乗券には、紙媒体の搭乗券と電子媒体の搭乗券が含まれる。

【0031】

チェックイン手続きが終了した利用者であって、生体認証による搭乗手続きを希望するシステム利用者は、チェックイン端末10を用いてシステム登録を行う。具体的には、システム利用者は、取得した搭乗券とパスポートをチェックイン端末10に読み込ませる。また、チェックイン端末10は、システム利用者の生体情報（例えば、顔画像）を取得する。

10

【0032】

チェックイン端末10は、これら（搭乗券、パスポート、生体情報）に関する情報をサーバ装置20に送信する。

【0033】

サーバ装置20は、チェックイン端末10から取得した情報の正当性を確認する。具体的には、サーバ装置20は、提示されたパスポートの正当性を確認する。当該確認を終了すると、サーバ装置20はシステム利用者の登録を行う。具体的には、サーバ装置20は、当該システム登録された利用者の搭乗手続きに用いられるトークンを発行する。

20

【0034】

発行されたトークンは、トークンID（Identifier）により識別される。搭乗手続きに必要な情報（例えば、生体情報、搭乗手続きに必要な業務情報等）はトークンIDを介して対応付けられる。即ち、「トークン」は、システム利用者の登録と共に発行され、当該登録されたシステム利用者が生体情報を利用した搭乗手続きを受けるための識別情報である。トークン（トークンID）が発行されると、システム利用者は、生体認証を用いた搭乗手続きを利用することができる。

【0035】

トークンの生成に応じて、サーバ装置20は、トークンID情報データベースと業務情報データベースのそれぞれにエントリを追加する。

30

【0036】

トークンID情報データベースは、生成されたトークンの詳細情報を記憶するデータベースである。当該データベースは、少なくともトークンIDと生体情報（顔画像、特徴量）を対応付けて記憶する。サーバ装置20は、トークンID情報データベースを参照し生体認証を実行する。

【0037】

業務情報データベースは、業務情報を記憶するデータベースである。業務情報データベースは、トークンIDと業務情報を対応付けて記憶する。業務情報は、端末が手続き（業務）を進める際に必要となる情報である。

40

【0038】

トークンが発行されたシステム利用者が、端末に到着すると、当該端末にて生体情報（例えば、顔画像）が取得される。端末は、顔画像を含む認証要求をサーバ装置20に送信する。

【0039】

なお、本願開示において、「端末」と表記した場合には、サーバ装置20に生体情報を含む認証要求を送信する装置、デバイス等を意味する。図2の例では、手荷物預け機11、旅客通過システム12、ゲート装置13、搭乗ゲート装置14が「端末」に相当する。あるいは、チェックイン手続きも生体認証により行われる場合には、チェックイン端末10も「端末」に相当する。

50

【0040】

サーバ装置20は、端末から取得した生体情報とシステム登録された生体情報を用いた生体認証を行う。生体認証に成功すると、サーバ装置20は、その旨を示す肯定応答を端末に送信する。肯定応答には、端末が手続きを進める際に必要となる業務情報が含まれる。生体認証に失敗すると、サーバ装置20は、その旨を示す否定応答を端末に送信する。

【0041】

サーバ装置20は、各端末から受信した認証要求を処理した際の詳細情報を記憶、管理する。具体的には、サーバ装置20は、認証結果データベースを用いて、上記詳細等を記憶する。認証結果データベースの詳細は後述する。

【0042】

認証成功を受信した端末は、取得した業務情報に基づき利用者の搭乗手続きを行う。例えば、端末は、必要に応じてゲート等を開き、利用者の通過を許可する。認証失敗を受信した端末は、その旨を被認証者に通知する。

【0043】

サーバ装置20は、認証結果データベースに記憶された認証処理の結果（詳細情報）を解析し、空港や航空会社の職員等が生体認証の結果のなかに誤認証（とりわけ、他人受入に関する誤認証）が含まれているか否かを検証するための認証結果検証情報を生成する。サーバ装置20は、当該生成された認証結果検証情報を職員端末30に提供する。

【0044】

職員は、認証結果検証情報に基づいて生成される表示に基づいて、他人受入が発生したか否かを検証する。他人受入が発生していれば、職員は、他人受入の発生により生じる矛盾等を解消する。

【0045】

続いて、各装置の概略構成、機能等を説明する。

【0046】

チェックイン端末10は、空港内のチェックインロビーに設置されている。上述のように、利用者は、チェックイン端末10を用いて生体認証を用いた搭乗手続きを実現するためのシステム登録を行う。また、システム利用者は、チェックイン端末10を操作してチェックイン手続きを行う。即ち、チェックイン端末10は、利用者が操作することによって、チェックイン手続きを行うためのセルフ端末でもある。チェックイン端末10は、C U S S（Common Use Self Service）端末とも称される。利用者は、チェックイン手続きを完了すると、手荷物の預け場所あるいは保安検査場へ移動する。

【0047】

手荷物預け機11は、空港内の手荷物カウンタ（有人カウンタ）の隣接領域あるいはチェックイン端末10の近傍領域に設置されている。手荷物預け機11は、利用者が操作することにより、航空機内に持ち込まない手荷物を預ける手続（手荷物預け手続）を行うためのセルフ端末である。手荷物預け機11は、C U B D（Common Use Bag Drop）端末とも称される。利用者は、手荷物預け手続を完了すると、保安検査場へ移動する。なお、利用者が、手荷物を預けない場合には、手荷物預け手続は省略される。

【0048】

旅客通過システム12は、空港内の保安検査場の入口に設置されているゲート装置である。旅客通過システム12は、P R S（Passenger Reconciliation System）とも称され、保安検査場の入口において利用者の通過可否を判定するシステムである。利用者は、旅客通過システム12を通過した後に保安検査手続を完了すると、出国審査場へ移動する。

【0049】

ゲート装置13は、空港内の出国審査場に設置されている。ゲート装置13は、利用者の出国審査手続を自動的に行う装置である。利用者は、出国審査手続を完了すると、免税店や搭乗ゲートが設けられている出国エリアに移動する。

【0050】

搭乗ゲート装置14は、出国エリアの搭乗ゲートごとに設置された通行制御装置である

10

20

30

40

50

。搭乗ゲート装置 1 4 は、出国審査（生体情報を用いた審査）の一連の手続きにおける最終段のゲート装置である。搭乗ゲート装置 1 4 は、A B G（Automated Boarding Gate s）端末とも称される。搭乗ゲート装置 1 4 は、利用者が搭乗ゲートから搭乗可能な航空機の搭乗者であることを確認する。利用者は、搭乗ゲート装置 1 4 を通過すると、航空機に搭乗し、第 2 国へ向けて出国する。

【0051】

なお、図 2 に示す各装置（チェックイン端末 1 0、手荷物預け機 1 1、旅客通過システム 1 2、ゲート装置 1 3、搭乗ゲート装置 1 4）による生体認証を用いた搭乗手続きは一例であって、手続きに使用される装置を限定する趣旨ではない。例えば、上記装置とは異なる装置が搭乗手続きに使用されてもよいし、上記各装置のうち一部の装置が手続きに使用されてなくともよい。例えば、ゲート装置 1 3 が搭乗手続きシステムに含まれていなくともよい。

10

【0052】

サーバ装置 2 0 は、上記搭乗手続きを支援、管理するためのサーバ装置である。サーバ装置 2 0 は、トークン I D を管理する。具体的には、サーバ装置 2 0 は、トークン I D の発行や無効化を行う。また、サーバ装置 2 0 は、空港内の各種端末からの認証要求を処理する。

【0053】

続いて、第 1 の実施形態に係る搭乗手続きシステムに含まれる各装置の詳細について説明する。以降の説明では、生体情報として利用者の「顔画像」や「顔画像から生成された特徴量」を例にとり説明を行う。

20

【0054】

〔チェックイン端末〕

上述のように、チェックイン端末 1 0 は、システム利用者に対して、チェックイン手続きとシステム登録に関する操作を提供する装置である。

【0055】

図 3 は、第 1 の実施形態に係るチェックイン端末 1 0 の処理構成（処理モジュール）の一例を示す図である。図 3 を参照すると、チェックイン端末 1 0 は、通信制御部 2 0 1 と、システム登録部 2 0 2 と、トークン発行要求部 2 0 3 と、メッセージ出力部 2 0 4 と、チェックイン実行部 2 0 5 と、記憶部 2 0 6 と、を含む。

30

【0056】

通信制御部 2 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 2 0 1 は、サーバ装置 2 0 からデータ（パケット）を受信する。また、通信制御部 2 0 1 は、サーバ装置 2 0 に向けてデータを送信する。通信制御部 2 0 1 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 2 0 1 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 2 0 1 を介して他の装置とデータの送受信を行う。

【0057】

システム登録部 2 0 2 は、生体認証による搭乗手続きを希望する利用者のシステム登録を行う手段である。例えば、システム登録部 2 0 2 は、チェックイン手続きの終了後に、利用者が「顔画像を用いた搭乗手続き」を希望するか否かを確認するための G U I（Graphical User Interface）を当該利用者に提供する（図 4 参照）。

40

【0058】

利用者が顔画像を用いた搭乗手続きを希望すると、システム登録部 2 0 2 は、G U I を用いて 3 つの情報（搭乗券に記載された情報、パスポートに記載された情報、生体情報）を取得する。

【0059】

システム登録部 2 0 2 は、3 つのサブモジュールを備える。図 5 は、第 1 の実施形態に係るシステム登録部 2 0 2 の処理構成（処理モジュール）の一例を示す図である。図 5 に示すように、システム登録部 2 0 2 は、搭乗券情報取得部 2 1 1 と、パスポート情報取得

50

部 2 1 2 と、生体情報取得部 2 1 3 と、を備える。

【 0 0 6 0 】

搭乗券情報取得部 2 1 1 は、システム利用者が所持する搭乗券に記載された情報（以下、搭乗券情報と表記する）を取得する手段である。搭乗券情報取得部 2 1 1 は、スキャナ等の読取機（図示せず）を制御し、搭乗券情報を取得する。

【 0 0 6 1 】

搭乗券情報には、氏名（姓、名）、エアラインコード、便名、搭乗日、出発地（搭乗空港）、目的地（到着空港）、シート番号、搭乗時間、到着時間等が含まれる。

【 0 0 6 2 】

パスポート情報取得部 2 1 2 は、システム利用者が所持するパスポートに記載された情報（以下、パスポート情報と表記する）を取得する手段である。パスポート情報取得部 2 1 2 は、スキャナ等の読取機を制御し、パスポート情報を取得する。

【 0 0 6 3 】

パスポート情報には、顔画像（以下、パスポート顔画像と表記する）、氏名、性別、国籍、パスポート番号、パスポート発行国等が含まれる。

【 0 0 6 4 】

生体情報取得部 2 1 3 は、システム利用者の生体情報を取得する手段である。生体情報取得部 2 1 3 は、カメラを制御し、システム利用者の顔画像を取得する。例えば、生体情報取得部 2 1 3 は、常時又は定期的に撮影する画像中に顔を検出すると、利用者の顔を撮影してその顔画像を取得する。

【 0 0 6 5 】

生体情報取得部 2 1 3 は、顔画像を撮影する前に、メッセージ出力部 2 0 4 を介して顔画像の撮影に関する案内メッセージを表示するのが望ましい。例えば、生体情報取得部 2 1 3 は、「お客様の顔画像を撮影し、システムに登録いたします。登録された顔画像は、搭乗完了後にシステムから削除されます」といったメッセージを表示する。

【 0 0 6 6 】

システム登録部 2 0 2 は、取得した 3 つの情報（搭乗券情報、パスポート情報、生体情報）をトークン発行要求部 2 0 3 に引き渡す。

【 0 0 6 7 】

図 3 に示すトークン発行要求部 2 0 3 は、サーバ装置 2 0 に対してトークンの発行を要求する手段である。トークン発行要求部 2 0 3 は、搭乗券情報、パスポート情報及び生体情報（顔画像）を含むトークン発行要求を生成する。トークン発行要求部 2 0 3 は、生成したトークン発行要求をサーバ装置 2 0 に送信する。

【 0 0 6 8 】

トークン発行要求部 2 0 3 は、サーバ装置 2 0 から取得した応答（トークン発行要求に対する応答）をメッセージ出力部 2 0 4 に引き渡す。

【 0 0 6 9 】

メッセージ出力部 2 0 4 は、種々のメッセージを出力する手段である。例えば、メッセージ出力部 2 0 4 は、サーバ装置 2 0 から取得した応答に応じたメッセージを出力する。

【 0 0 7 0 】

トークンの発行に成功した旨の応答（肯定応答）を受信した場合には、メッセージ出力部 2 0 4 は、その旨を出力する。例えば、メッセージ出力部 2 0 4 は、「今後の手続きは顔認証により行うことができます」といったメッセージを出力する。

【 0 0 7 1 】

トークンの発行に失敗した旨の応答（否定応答）を受信した場合には、メッセージ出力部 2 0 4 は、その旨を出力する。例えば、メッセージ出力部 2 0 4 は、「申し訳ありません。顔認証による手続きは行えません。有人のブースに向かってください」といったメッセージを出力する。

【 0 0 7 2 】

チェックイン実行部 2 0 5 は、利用者のチェックイン手続きを行う手段である。チェッ

10

20

30

40

50

クイン実行部 205 は、利用者が提示した航空券に基づいて座席の選択等のチェックイン手続きを実行する。例えば、チェックイン実行部 205 は、航空券に記載された情報を DCS (Departure Control System) に送信し、当該 DCS から搭乗券に記載する情報を取得する。なお、チェックイン実行部 205 の動作は既存のチェックイン端末の動作と同一とすることができるのでより詳細な説明を省略する。

【0073】

記憶部 206 は、チェックイン端末 10 の動作に必要な情報を記憶する手段である。

【0074】

〔搭乗ゲート装置〕

図 6 は、第 1 の実施形態に係る搭乗ゲート装置 14 の処理構成（処理モジュール）の一例を示す図である。図 6 を参照すると、搭乗ゲート装置 14 は、通信制御部 301 と、生体情報取得部 302 と、認証要求部 303 と、メッセージ出力部 304 と、機能実現部 305 と、記憶部 306 と、を含む。

【0075】

通信制御部 301 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 20 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 20 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。

【0076】

生体情報取得部 302 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。生体情報取得部 302 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像する。生体情報取得部 302 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。

【0077】

なお、生体情報取得部 302 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 302 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 302 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。

【0078】

生体情報取得部 302 は、抽出した顔画像を認証要求部 303 に引き渡す。

【0079】

認証要求部 303 は、サーバ装置 20 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 303 は、自装置の識別子（以下、端末 ID と表記する）、上記取得した顔画像等を含む認証要求を生成する（図 7 参照）。端末 ID には MAC (Media Access Control address) アドレス、IP (Internet Protocol) アドレス等を用いることができる。認証要求部 303 は、生成した認証要求をサーバ装置 20 に送信する。

【0080】

サーバ装置 20 は、認証要求に含まれる端末 ID を確認することで、認証要求の送信元である端末を一意に特定できる。また、サーバ装置 20 は、端末 ID に基づいて端末の種類（手荷物預け機 11、旅客通過システム 12、ゲート装置 13、搭乗ゲート装置 14）を特定することもできる。なお、端末 ID は、システムに含まれる各端末とサーバ装置 20 の間で共有される。例えば、システム管理者等が端末 ID を決定し、当該決定された端末 ID を各端末に入力してもよい。また、システム管理者は、端末 ID と端末の種類を対応付けたテーブル情報等をサーバ装置 20 に入力してもよい。

【0081】

認証要求部 303 は、認証要求に対するサーバ装置 20 からの応答を受信する。認証要求部 303 は、サーバ装置 20 から取得した応答をメッセージ出力部 304 と機能実現部

10

20

30

40

50

305に引き渡す。

【0082】

メッセージ出力部304は、種々のメッセージを出力する手段である。例えば、メッセージ出力部304は、サーバ装置20から取得した認証結果（認証成功、認証失敗）に応じたメッセージを出力する。

【0083】

機能実現部305は、搭乗ゲート装置14の機能を実現する手段である。機能実現部305は、認証成功者（認証成功と判定された被認証者）に関する手続きを実現する。機能実現部305は、取得した業務情報から利用者（認証成功者）が搭乗可能な航空機の便番号を特定する。機能実現部305は、当該特定された便番号と自装置に割り当てられた便番号が一致する場合に、上記認証成功者のゲート通過を許可する。なお、機能実現部305の動作は既存の搭乗ゲート装置の動作と同一とすることができるので詳細な説明を省略する。また、当該搭乗ゲート装置14から搭乗する航空機の航空会社に勤務する職員が、搭乗ゲート装置14に必要な便番号を割り当て（入力）すればよい。

10

【0084】

機能実現部305は、認証成功者のゲート通過を許可した場合には、その旨をサーバ装置20に通知する。

【0085】

記憶部306は、搭乗ゲート装置14の動作に必要な情報を記憶する手段である。

【0086】

20

〔他の端末〕

搭乗手続きシステムに含まれる他の端末（手荷物預け機11、旅客通過システム12、ゲート装置13）の基本的な処理構成は、図6に示す搭乗ゲート装置14の処理構成と同一とすることができるので詳細な説明を省略する。いずれの端末も、システム利用者の生体情報（顔画像）を取得し、当該取得した生体情報を用いた認証をサーバ装置20に要求する。認証に成功すると、各端末に割り当てられた機能が実行される。また、各端末は、認証結果（認証成功、認証失敗）に応じた表示（メッセージ）を出力する。

【0087】

〔サーバ装置〕

図8は、第1の実施形態に係るサーバ装置20の処理構成（処理モジュール）の一例を示す図である。図8を参照すると、サーバ装置20は、通信制御部401と、トークン生成部402と、データベース管理部403と、認証部404と、検証情報生成部405、記憶部406と、を含む。

30

【0088】

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、チェックイン端末10からデータ（パケット）を受信する。また、通信制御部401は、チェックイン端末10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、端末から被認証者の生体情報を取得する、「取得部」としての機能を備える。あるいは、通信制御部401は、被認証者の生体情報を含む認証要求を受信する「受信部」、当該認証要求に対する応答を送信する「送信部」としての機能を有する。

40

【0089】

トークン生成部402は、チェックイン端末10からのトークン生成要求に応じてトークンを生成する手段である。その際、トークン生成部402は、利用者が提示したパスポートの正当性に関する判定を行う。

【0090】

具体的には、トークン生成部402は、チェックイン端末10にパスポートを提示した人物と、当該パスポートの発行を受けた人物と、が同一人物か否かを判定する。当該判定

50

を実行するため、トークン生成部 402 は、トークン生成要求に含まれる顔画像（システム利用者の顔画像）とパスポート情報に含まれるパスポート顔画像を抽出する。トークン生成部 402 は、これら 2 つの顔画像が実質的に一致するか否かを判定する。

【0091】

トークン生成部 402 は、上記 2 枚の顔画像の照合（1対1照合）を実行する。トークン生成部 402 は、2 つの画像それぞれから特徴ベクトルを算出する。トークン生成部 402 は、当該 2 つの画像の類似度（例えば、ユークリッド距離）を算出し、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。例えば、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）、トークン生成部 402 は、2 つの顔画像は同一人物によるものと判定する。

10

【0092】

トークン生成部 402 は、生体情報を用いたパスポートの正当性判定に成功すると、トークンを発行する。例えば、トークン生成部 402 は、処理時の日時やシーケンス番号等に基づいて固有な値をトークン ID として生成する。

【0093】

トークン生成部 402 は、トークン（トークン ID）を生成すると、チェックイン端末 10 に対して肯定応答（トークン発行）を送信する。トークン生成部 402 は、トークン ID の生成に失敗すると、チェックイン端末 10 に対して否定応答（トークン非発行）を送信する。

【0094】

トークン生成部 402 は、トークン ID の生成（発行）に成功すると、生成したトークン ID、搭乗券情報、パスポート情報、顔画像（システム利用者の顔画像）をデータベース管理部 403 に引き渡す。

20

【0095】

データベース管理部 403 は、サーバ装置 20 に構築されたデータベースを管理する手段（管理部）である。

【0096】

サーバ装置 20 は、トークン ID 情報データベース、業務情報データベースと、認証結果データベースと、を備える。

【0097】

トークン ID 情報データベースは、少なくともトークン ID と利用者の生体情報を対応付けて記憶する。図 9 は、トークン ID 情報データベースの一例を示す図である。図 9 を参照すると、トークン ID 情報データベースは、トークン ID、登録顔画像、特徴量、トークン発行時刻及びトークン発行デバイス名等を記憶するフィールドを有する。

30

【0098】

上述のように、トークン ID は一時的に発行される識別子である。利用者が搭乗ゲート装置 14 での手続きを終えると、当該トークン ID は無効にされる。即ち、トークン ID は、永続的に使用される識別子ではなく、有効期間（ライフサイクル）を有するワンタイム ID である。

【0099】

登録顔画像は、システム利用者の顔画像である。例えば、登録顔画像は、チェックイン端末 10 が撮像した利用者の顔画像であってもよいし、パスポート顔画像であってもよい。特徴量は、顔画像から生成される特徴ベクトルである。トークン発行時刻は、サーバ装置 20 がトークン ID を発行した時刻である。デバイス名は、トークン ID の発行の契機となった登録顔画像の取得元のデバイス名（例えば、チェックイン端末 10）である。

40

【0100】

業務情報データベースは、利用者の搭乗手続きを行う際に必要な情報（業務情報）を管理するデータベースである。図 10 は、業務情報データベースの一例を示す図である。図 10 を参照すると、業務情報データベースは、トークン ID、搭乗者名、出発地、目的地、エアラインコード、便番号、運行年月日等を記憶するフィールドを有する。業務情報デ

50

データベースは、上記フィールドに加え、シート番号、国籍、旅券番号、姓、名、生年月日及び性別等を記憶するフィールドを有していてもよい。業務情報データベースは、所定の業務（各タッチポイントで行われる手続き業務）に必要な業務情報をトークンIDごとに記憶している。

【0101】

業務情報データベースに格納される上記情報は、搭乗券情報及びパスポート情報から取得される。

【0102】

データベース管理部403は、トークン生成部402からトークンIDを取得すると（トークンIDが発行されると）、上記2つのデータベースに新規エントリを追加する。データベース管理部403は、各データベースのフィールドに設定値を設定する。例えば、データベース管理部403は、登録顔画像から特徴量を生成し、当該生成した特徴量をトークンID情報データベースに登録する。なお、設定値を設定できないフィールドに関しては、データベース管理部403は、初期値（デフォルト値）を設定してもよい。

【0103】

認証部404は、生体認証を行う手段である。認証部404は、端末から取得された認証要求を処理する。認証部404は、被認証者の生体情報と予めトークンID情報データベースに登録された複数の利用者それぞれの生体情報を用いた生体認証を行う。

【0104】

具体的には、認証部404は、複数の端末のうち被認証者の生体情報を取得した端末からの認証要求を、トークンID情報データベースを参照して処理する。認証要求には、被認証者の生体情報が含まれる。認証部404は、認証要求に含まれる生体情報とトークンID情報データベースに登録された生体情報を用いた照合処理（1対N照合）を実行する。

【0105】

認証部404は、端末（手荷物預け機11、旅客通過システム12、ゲート装置13、搭乗ゲート装置14）から取得した顔画像から特徴量を生成する。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、認証部404は、顔画像から目、鼻、口等を特徴点として抽出する。その後、認証部404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し、複数の特徴量からなる特徴ベクトルを生成する。

【0106】

認証部404は、当該生成した特徴量（特徴ベクトル）を照合側の特徴量、トークンID情報データベースに記憶された特徴量を登録側の特徴量にそれぞれ設定する。

【0107】

認証部404は、照合側の特徴量と登録側の複数の特徴量それぞれとの間の類似度（スコア）を計算する。当該類似度には、カイ二乗距離やユークリッド距離等を用いることができる。なお、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。

【0108】

認証部404は、トークンID情報データベースに登録された複数の特徴量（有効な特徴量）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認証に成功したと判断する。

【0109】

認証に成功すると、認証部404は、類似度の最も高い特徴量に対応するトークンIDを特定する。認証部404は、特定されたトークンIDをキーとして業務情報データベースを検索し、対応するエントリを特定する。

【0110】

認証部404は、認証結果を端末に送信する（認証要求に応答する）。

【0111】

認証に成功した場合には、認証部404は、記業務情報データベースから特定されたエントリ（トークンID、業務情報）を含む肯定応答を端末に送信する。

10

20

30

40

50

【0112】

認証に失敗した場合には、認証部404は、認証失敗を示す否定応答を端末に送信する。

【0113】

続いて、認証結果データベースについて説明する。上述のように、各端末からの認証要求が処理された際の詳細情報は、認証結果データベースに記憶される。認証結果データベースは、生体認証に成功した認証成功者について、予め登録された生体情報と、認証要求が処理された際の詳細を含む情報（以下、認証結果詳細情報と表記する）と、を対応づけて記憶する。

【0114】

図11は、認証結果データベースの一例を示す図である。図11に示すように、認証結果データベースは、トークンIDごと（認証成功者ごと）に、登録顔画像と少なくとも1以上の認証結果詳細情報を記憶する。認証結果詳細情報には、認証要求の送信元を識別する端末ID、認証要求に含まれる取得顔画像（端末により取得された顔画像）、認証成功と判定された際の類似度（スコア）等が含まれる。

10

【0115】

なお、図11では、理解の容易のため、端末IDとして図2に示す各端末に割り当てられた符号を用いている。また、図11に示す認証結果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、認証結果データベースは、認証に成功した日時（認証時刻）等を記憶してもよい。

【0116】

認証成功の結果が得られた場合には、認証部404は、認証結果データベースを更新する。具体的には、被認証者のトークンIDが認証結果データベースに登録されていないければ、認証部404は、新たなエントリを当該データベースに追加するとともに、認証処理の詳細を書き込む。被認証者のトークンIDが認証結果データベースに登録されていれば、認証部404は、対応するエントリの認証結果詳細情報フィールドに認証処理の結果を書き込む。

20

【0117】

なお、空港における搭乗手続きの順番は予め定まっているため、認証結果データベースに記憶される端末IDにも順序が存在する。例えば、図2の例では、通常の手続きでは手荷物預け機11、旅客通過システム12、ゲート装置13、搭乗ゲート装置14の順で手続が行われる。従って、上記各端末の順番で認証処理の詳細が認証結果データベースに記憶されることになる。なお、手荷物預け機11における手続きは必須なものではないため、当該端末による認証結果は認証結果データベースに記憶されないこともある。

30

【0118】

検証情報生成部405は、上述の認証結果検証情報を生成する手段である。検証情報生成部405は、少なくとも登録顔画像、端末ID及び端末により取得された取得顔画像を含む認証結果検証情報を生成する。検証情報生成部405により生成された認証結果検証情報は、空港や航空会社の職員等に提供される。

【0119】

例えば、検証情報生成部405は、生成した認証結果検証情報を職員端末30に送信する。職員端末30は、受信した認証結果検証情報に基づいて、図12に示すような表示（GUI）を生成する。職員端末30は、認証結果データベースに記憶されたエントリ（認証成功者）の登録顔画像と少なくとも1以上の取得顔画像を同時に確認できるような表示を行う。また、職員端末30は、端末IDに基づいて、取得顔画像を取得した端末の名称等を合わせて表示する。

40

【0120】

なお、検証情報生成部405は、職員（職員端末30）からの要求に応じて認証結果検証情報を生成し、職員端末30に送信する。職員は、図12に示すような表示を確認し、他人受入の誤認証が発生していないと判断した場合には次ボタンを押下する。職員端末30は、次ボタンの押下検出に応じて、サーバ装置20に新たな認証結果検証情報の送信を

50

依頼する。

【0121】

新たな依頼を受信すると、検証情報生成部405は、認証結果データベースの次のエントリから認証結果検証情報を生成し、職員端末30に送信する。

【0122】

登録顔画像と取得顔画像を比較し、これらの顔画像が異なる人物から撮像された顔画像であると考えられる場合には、職員等は、他人受入が発生したと判断する。この場合、職員等は、トークンIDをサーバ装置20に入力し誤認証当事者に関する詳細な情報（例えば、氏名、航空会社、便番号等）を取得する。職員等は、得られた詳細情報に基づいて、上記誤認証当事者のもとに向かい適切な対応を行う。具体的には、職員等は、誤認証当事者が所持するパスポート等を確認し、誤認証により生じた矛盾等を修正する。

10

【0123】

あるいは、職員端末30は、誤認証当事者の詳細情報を得るためのボタン等を表示してもよい（図13参照）。職員端末30は、職員等が詳細情報の提示を求めた場合（詳細情報ボタンが押下された場合）、その旨をサーバ装置20に通知する。サーバ装置の検証情報生成部405は、当該通知に応じて、トークンIDをキーとして業務情報データベースを検索する。検証情報生成部405は、検索の結果により特定されたエントリの氏名、エアラインコード、便番号等を職員端末30に送信する。職員端末30は、得られた情報を表示する。あるいは、検証情報生成部405は、誤認証当事者（職員等を選択された旅客）に関する端末の通過履歴を、認証結果データベースを参照して生成し、職員端末30に送信してもよい。職員端末30は、当該通過履歴を表示してもよい。

20

【0124】

なお、同じ認証成功者について、複数の認証結果詳細情報が記憶されている場合には、検証情報生成部405は、複数の認証結果詳細情報それぞれに対応する、端末ID及び取得顔画像を含む認証結果検証情報を生成する。職員端末30は、このような認証結果検証情報を用いて図12、図13に示すような表示（GUI）を生成することができる。

【0125】

記憶部406は、サーバ装置20の動作に必要な各種情報を記憶する。記憶部406には、トークンID情報データベース、業務情報データベース、認証結果データベースが構築される。

30

【0126】

〔職員端末〕

職員端末30は、液晶パネル等の表示デバイス、タッチパネル等の操作デバイスを備え、情報出力機能及び情報入力機能を備えていればよい。職員端末30は、市販されているコンピュータ等により実現可能であり、内部の処理構成等は当業者にとって明らかであるからその説明を省略する。

【0127】

〔システム動作〕

続いて、第1の実施形態に係る搭乗手続きシステムの動作を説明する。図14は、第1の実施形態に係る搭乗手続きシステムの動作の一例を示すシーケンス図である。図14を用いて利用者の認証処理を実行する際の動作及びその後の動作を説明する。システム登録に関する動作の説明は省略する。

40

【0128】

端末（手荷物預け機11、旅客通過システム12、ゲート装置13、搭乗ゲート装置14のいずれか）は、利用者（被認証者）の顔画像を取得し、認証要求をサーバ装置20に送信する（ステップS01）。

【0129】

サーバ装置20は、認証要求に含まれる顔画像から特徴量を生成し、トークンID情報データベースを用いた認証処理を実行する（ステップS02）。

【0130】

50

認証に成功すると（ステップ S 0 3、Y e s 分岐）、サーバ装置 2 0 は、照合処理により得られたトークン I D をキーとして業務情報データベースを検索（ステップ S 0 4）する。

【0131】

認証に失敗すると（ステップ S 0 3、N o 分岐）、サーバ装置 2 0 は、ステップ S 0 5 以降の処理を実行する。

【0132】

サーバ装置 2 0 は、認証結果（認証成功、認証失敗）を端末（タッチポイント）に送信する（ステップ S 0 5）。

【0133】

端末は、サーバ装置 2 0 から取得した認証結果に応じた表示を行う（ステップ S 0 6）。また、端末は、認証結果に応じて利用者の搭乗手続きを実行する。当該動作についての説明は省略する。各端末は、割り当てられた機能を実行すればよい。

【0134】

職員端末 3 0 は、誤認証（他人受入）発生を検証するための情報を提供するようにサーバ装置 2 0 に依頼する（ステップ S 1 1）。

【0135】

サーバ装置 2 0 は、認証結果データベースを参照して認証結果検証情報を生成する。サーバ装置 2 0 は、生成した認証結果検証情報を職員端末 3 0 に送信する（ステップ S 1 2）。

【0136】

職員端末 3 0 は、認証結果検証情報に基づいて誤認証発生を検証するための G U I を表示する（ステップ S 1 3）。

【0137】

以上のように、第 1 の実施形態に係る搭乗手続きシステムは、被認証者の認証に成功すると、認証処理（認証結果）の詳細を認証結果データベースに記憶する。サーバ装置 2 0 は、職員等からの要請に応じて当該データベースを参照し、職員等が誤認証（他人受入）の発生を検証するための認証結果検証情報を生成する。当該認証結果検証情報には、登録顔画像と取得顔画像に加え、認証処理の発生契機となった端末の端末 I D が含まれる。そのため、職員端末 3 0 は、複数の端末（手荷物預け機 1 1 等の端末）のいずれで他人受入が発生したか特定することができる。併せて、職員端末 3 0 は、他人受入の当事者に関する詳細な情報（例えば、搭乗便番号、航空会社等）を職員に提示できるので、職員は迅速に適切な処置を行うことができる。

【0138】

〔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。

【0139】

第 1 の実施形態では、認証結果データベースに記憶された各エントリを情報提供の対象（認証結果検証情報の生成対象）としている。しかし、このような対応であると、認証結果データベースに数多くのエントリが含まれる場合、職員等による他人受入の検証に多大な労力を要することになる。

【0140】

第 2 の実施形態では、職員の労力を軽減するため、認証結果検証情報の生成対象とするエントリを絞り込む場合について説明する。

【0141】

第 2 の実施形態に係る搭乗手続きシステムの概略構成は第 1 の実施形態と同一とすることができるので図 2 に相当する説明を省略する。同様に、第 2 の実施形態に係るサーバ装置 2 0、端末の処理構成は、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。

【0142】

10

20

30

40

50

以下、第1及び第2の実施形態の相違点について説明する。

【0143】

第2の実施形態に係る検証情報生成部405は、生体認証の結果のうち他人受入が発生している可能性の高い認証結果に関して認証結果検証情報を生成する。検証情報生成部405は、他人受入が発生している可能性の低い認証結果（認証結果データベースのエントリ）については、認証結果検証情報の生成対象から除外する。

【0144】

検証情報生成部405は、情報提供の際、又は、情報提供に備えて事前に、認証結果データベースの各エントリ（認証成功者）について認証結果検証情報を生成するか否かを判定する。より具体的には、検証情報生成部405は、認証結果詳細情報を解析し、認証結果データベースの各エントリについて認証結果検証情報の生成対象とするか否かを判定する。

10

【0145】

例えば、検証情報生成部405は、各エントリに含まれる少なくとも1以上の認証結果詳細情報のなかに、誤認証（他人受入）の可能性が高い情報が含まれている場合、当該情報を含むエントリを情報提供の対象に設定する。換言すれば、誤認証が発生した可能性が低い認証結果詳細情報だけを含むエントリに関しては、検証情報生成部405は、認証結果検証情報の生成対象とはしない。

【0146】

例えば、検証情報生成部405は、端末からの認証要求を処理する際に用いられた類似度に基づいて、各エントリを認証結果検証情報の生成対象とするか否かを判定する。検証情報生成部405は、認証結果詳細情報に含まれる類似度が所定の閾値よりも小さい場合、当該認証結果詳細情報を含むエントリを認証結果検証情報の生成対象とする。

20

【0147】

図11の例では、トークンIDが「ID11」の認証成功者に関し、認証結果詳細情報1の類似度S11が、閾値TH1よりも小さい場合に、当該認証成功者に関する認証結果検証情報が生成される。この場合、認証には成功しているが、その確度が低く、当該認証成功者に関する認証結果は誤認証の蓋然性が高いためである。

【0148】

あるいは、検証情報生成部405は、認証結果データベースの各エントリに記載された類似度（複数の認証結果詳細情報それぞれに含まれる類似度）を要素とする時系列データに基づいて、認証結果検証情報を生成するか否かを判定してもよい。より具体的には、検証情報生成部405は、上記時系列データに対する統計処理の結果に基づいて上記判定を行ってもよい。

30

【0149】

例えば、検証情報生成部405は、前後の類似度において変化率が所定の閾値よりも大きい場合に、対応するエントリを認証結果検証情報の生成対象に設定する。

【0150】

例えば、認証成功者Aに関し、認証処理の結果により得られた類似度をグラフ化すると図15（a）の通りとする。認証成功者Bに関し、類似度をグラフ化すると図15（b）の通りとする。なお、図15に示す点線は、認証成功と判断される閾値TH2の値を示す。即ち、図15に示すプロットされた各類似度は認証成功と判定される閾値TH2よりも大きい。

40

【0151】

図15の2つのグラフを比較すると、図15（a）に関して、類似度（スコア）は高い値で安定している（類似度間の変化率は小さい）。当該事実、4回の認証処理において計算された類似度は同程度であることを示し、各端末において同一人物の顔画像が取得された可能性が高いことを示す。

【0152】

対して、図15（b）に関しては、3回目から4回目の認証結果において、類似度の変化率が大きい。当該事実、登録顔画像と4回目の認証処理に使われた取得顔画像の類似

50

度は認証成功を判定する閾値TH2よりも大きい、3回目の認証処理で使われた取得顔画像と4回目の認証処理で使われた取得顔画像は別人の顔画像であることを示唆する。従って、検証情報生成部405は、認証成功者Bに関する認証には他人受入が発生している蓋然性が高いと判定し、認証結果詳細情報の生成対象に設定する。

【0153】

あるいは、検証情報生成部405は、各エントリに記載された特徴量の時系列データに関する「ばらつき」に基づいて認証結果詳細情報の生成要否を判定してもよい。具体的には、検証情報生成部405は、時系列データのばらつきを示す指標（分散、標準偏差）を計算する。検証情報生成部405は、計算されたばらつきを示す指標（分散、標準偏差）が所定の閾値よりも大きい場合に、対応するエントリを認証結果詳細情報の生成対象に設定する。

10

【0154】

あるいは、検証情報生成部405は、認証処理時に計算された複数の類似度のうち最も値の大きい類似度（第1類似度）とその次に値の大きい類似度（第2類似度；第1類似度＞第2類似度）を使って認証結果詳細情報の生成要否を判定してもよい。なお、この場合、認証部404は、上記2つの類似度を認証結果データベースに記憶する。

【0155】

検証情報生成部405は、認証結果データベースの各エントリの認証結果詳細情報に関して、第1類似度と第2の類似度の差分が閾値TH3よりも小さい場合に、当該エントリを認証結果検証情報の生成対象に設定する。

20

【0156】

ここで、第1類似度と第2類似度の差が大きいという事実は、被認証者と2番目に似ていると判定された人物の顔は被認証者（本人）の顔に似ていないことを示す。対して、第1類似度と第2の類似度の差が小さいという事実は、被認証者と2番目に似ていると判定された人物の顔は被認証者の顔に似ていることを示す。例えば、被認証者が双子の場合であって、双方の顔画像が登録されている場合には、本人の顔画像による類似度（第1類似度）と双子の他の顔画像による類似度（第2類似度）の差は小さくなる。

【0157】

上記事実を利用し、検証情報生成部405は、2つの類似度の差分が所定の閾値よりも小さい認証は他人受入発生蓋然性が高い結果であると判定する。

30

【0158】

あるいは、検証情報生成部405は、顔画像から生成された特徴量に基づく顔画像間の類似度とは異なる指標等に基づいて認証結果詳細情報の生成要否を判定してもよい。生体認証において誤認証（他人受入）の発生は、照合側及び登録側の「顔」が似ていることに起因する。より正確には、目や鼻の位置、これら特徴点間の距離が同程度であると、他人同士の顔であっても誤認証（他人受入）が発生し得る。ここで、空港における搭乗手続きシステムでは、チェックイン時に登録顔画像がサーバ装置20に入力され、その後、比較的短い時間で端末（搭乗ゲート装置14等）が生体認証をサーバ装置20に依頼することになる。このような短い期間に、被認証者の髪型、眼鏡着用の有無、服装等が変化することは想定し難い。検証情報生成部405は、このような空港における生体認証の特徴、特質を利用して、認証結果詳細情報の生成要否を判定してもよい。

40

【0159】

より具体的には、検証情報生成部405は、特徴量を用いた手法とは異なる手法により2枚の画像の類似度を計算する。例えば、検証情報生成部405は、2枚の顔画像に写る人物の髪型が異なれば類似度に低い値を設定する。あるいは、検証情報生成部405は、一方の顔画像には眼鏡が写っており、他方の顔画像に眼鏡が写っていなければ類似度に低い値を設定する。あるいは、検証情報生成部405は、2枚の顔画像に写る人物の服装が異なれば類似度に低い値を設定する。検証情報生成部405は、上記のような方法により計算された類似度が閾値TH4よりも低い場合に、他人受入発生蓋然性が高いと判定する。即ち、検証情報生成部405は、特徴量に基づく類似度とは異なる手法により算出さ

50

れた画像間の類似度に基づいて、認証結果詳細情報の生成要否を判定してもよい。

【0160】

なお、髪型の類似度判定に関し、検証情報生成部405は、顔上部の領域の面積を比較してもよいし、当該領域の形状を利用してもよい。また、眼鏡着用の有無に関し、検証情報生成部405は、テンプレートマッチング等の手法を用いて判定してもよい。服装の同一性判定に関し、検証情報生成部405は、顔領域以外の領域の周波数解析結果を用いてもよい。サーバ装置は、顔領域以外の領域の模様、テクスチャーが異なるか否かに応じて衣服の同一性を判定してもよい。

【0161】

検証情報生成部405は、上記の方法又は他の方法により誤認証が発生している蓋然性の高い認証結果（エントリ）を認証結果検証情報の生成対象とする。即ち、誤認証（他人受入）が発生している可能性が低いと判定された認証結果に関しては、図12や図13に示すような表示は行われたい。換言すれば、職員等は、誤認証が発生している蓋然性の高い認証結果（登録顔画像、取得顔画像）を検証すればよい。

【0162】

以上のように、第2の実施形態に係るサーバ装置20は、職員等に情報提供を行う際、他人受入が発生している蓋然性の高い認証結果（認証結果詳細情報）から認証結果検証情報を生成する。このように、サーバ装置20は、誤認証が発生している蓋然性の高い認証結果に関する情報を絞り込んで職員等に情報提供を行うので、提供された情報の確認を行う職員の負担を軽減することができる。

【0163】

続いて、搭乗手続き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16は、サーバ装置20のハードウェア構成の一例を示す図である。

【0164】

サーバ装置20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16に例示する構成を備える。例えば、サーバ装置20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。

【0165】

但し、図16に示す構成は、サーバ装置20のハードウェア構成を限定する趣旨ではない。サーバ装置20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、サーバ装置20に含まれるプロセッサ311等の数も図16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がサーバ装置20に含まれていてもよい。

【0166】

プロセッサ311は、例えば、CPU（Central Processing Unit）、MPU（Micro Processing Unit）、DSP（Digital Signal Processor）等のプログラマ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。

【0167】

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。

【0168】

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。

【0169】

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。

【0170】

サーバ装置20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。

10

【0171】

なお、チェックイン端末10、搭乗ゲート装置14、職員端末30等もサーバ装置20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サーバ装置20と相違する点はないので説明を省略する。チェックイン端末10等は、カメラ等を備えていればよい。

【0172】

サーバ装置20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サーバ装置20の機能が実現できる。また、サーバ装置20は、当該プログラムによりサーバ装置の制御方法を実行する。

20

【0173】

[変形例]

なお、上記実施形態にて説明した搭乗手続きシステムの構成、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。

【0174】

上記実施形態では、利用者のチェックイン手続きの後にシステム登録がされることを説明したが、チェックイン手続きの前にシステム登録がなされてもよい。この場合、チェックイン手続きの前に搭乗券は発行されていないので、サーバ装置20は、搭乗券に替えて航空券の情報を用いてシステム登録すればよい。

30

【0175】

上記実施形態では、チェックイン端末10にてシステム登録（生体認証を用いた搭乗手続きを実現するための登録）を行う場合について説明した。しかし、システム登録は、チェックイン端末10以外の装置、端末にて行われてもよい。例えば、システム登録専用の装置が空港に設置されてもよいし、手荷物預け機11、旅客通過システム12等の端末（タッチポイント）でシステム登録が行われてもよい。

【0176】

上記実施形態では、一連の搭乗手続きが生体認証により行われる場合について説明したが、一部の手続きが生体認証により行われてもよい。例えば、図2において、手荷物預け機11にてシステム登録がされ、手荷物預け入れ以降の手続き（保安検査等）が生体認証により行われてもよい。換言するならば、一連の搭乗手続きのうち一部の手続きに関しては有人のブース等にて実施されてもよい。

40

【0177】

上記実施形態では、サーバ装置20が3つのデータベースを備える場合について説明した。しかし、サーバ装置20に構築される、トークンID情報データベース、業務情報データベース、認証結果データベースは、サーバ装置20とは異なるデータベースサーバに構築されていてもよい。即ち、搭乗手続きシステムには、上記実施形態にて説明した各種手段（例えば、トークン生成手段）等が含まれていればよい。

【0178】

50

上記実施形態では、認証要求には顔画像が含まれる場合について説明したが、認証要求には顔画像から生成された特徴量が含まれていてもよい。この場合、サーバ装置 20 は、認証要求から取り出した特徴量とトークン ID 情報データベースに登録された特徴量を用いて認証要求を処理すればよい。

【0179】

第 2 の実施形態では、サーバ装置 20 は、類似度等により認証結果を選別し、他人受入発生に関する検証対象を絞り込んでいる。上記説明した選別方法は例示であって、サーバ装置 20（検証情報生成部 405）は、他の条件等に基づいて絞り込みを行ってもよい。例えば、サーバ装置 20 は、認証成功者の座席等級（最上級客席、上級客室、普通客席）に基づいて、認証結果検証情報の生成対象を絞り込んでもよい。例えば、サーバ装置 20 は、座席等級がファーストクラスの旅客に限って他人受入発生に関する検証対象としてもよい。この場合、職員は、ファーストクラスの乗客（航空会社等がトラブルを避けたい乗客）に関する誤認証の発生を注意深く監視することができる。

10

【0180】

あるいは、サーバ装置 20 は、認証結果データベースに格納された端末 ID の順序に基づいて、認証結果検証情報の生成可否を判定してもよい。上述したように、空港における手続きは、その順番が予め定められている。そこで、サーバ装置 20 は、当該予め定められた順番とは異なる順番で生体認証が行われたことが記録されているエン트리に関しては、誤認証が発生している蓋然性が高いと判断し、認証結果検証情報の生成対象としてもよい。例えば、検証情報生成部 405 は、ゲート装置 13 における認証の後に手荷物預け機 11 における認証が発生（記録）されているエン트리に関しては、認証結果検証情報の生成対象と判定してもよい。通常、ゲート装置 13 の後に手荷物預け機 11 にて認証が行われることは想定できないためである。

20

【0181】

サーバ装置 20 は、第 2 の実施形態にて説明したように、職員等からの指示に基づいて認証結果検証情報による情報提供を行うだけでなく、定期的又は所定のタイミングにて上記情報提供を自発的に行ってもよい。例えば、サーバ装置 20（検証情報生成部 405）は、定期的又は所定のタイミングにて、認証結果データベースに記憶された認証結果（認証結果詳細情報）を解析し、認証結果検証情報の送信可否を決定する。具体的には、サーバ装置 20 は、第 2 の実施形態にて説明した方法又は他の方法により、上記送信可否を決定する。サーバ装置 20 は、認証結果検証情報の送信が必要と判断した場合、その旨を職員端末 30 に報知（通知、警告）する。その際、サーバ装置 20 は、他人受入発生の当事者の氏名やフライトに関する情報を職員端末 30 に通知してもよい。具体的には、サーバ装置 20 は、図 17 に示すような表示が生成可能なデータを職員端末 30 に送信してもよい。

30

【0182】

図 17 に示すような表示に接した職員は、表示された旅客のもとに向かい誤認証（他人受入）が真に発生しているか否かを確認する。他人受入が発生していれば、職員は、当該他人認証により生じた矛盾を修正する。例えば、職員は、サーバ装置 20 に記憶されたデータの修正等を行う。なお、職員は、図 17 に示されるように、各端末で取得された顔画像を見比べることができるので、どの端末で誤認証が発生したか特定することができる。例えば、搭乗ゲート装置 14 にて取得された取得顔画像が他の取得顔画像と異なっていれば、職員等は、搭乗ゲート装置 14 で他人受入が発生したと判断できる。

40

【0183】

このように、サーバ装置 20 の検証情報生成部 405 は、定期的又は所定のタイミングで認証結果詳細情報を解析し、認証結果検証情報の送信可否を決定してもよい。検証情報生成部 405 は、生成する必要があると判定された認証結果検証情報と共に、対応する認証成功者のフライトに関する情報を職員端末に送信してもよい。

【0184】

サーバ装置 20 は、他人受入発生の蓋然性が高いと判断した認証結果から当該認証に使

50

われた顔画像を取得した端末を特定し、特定した端末の情報を職員等に通知してもよい。例えば、図15(b)の例では、4回目の認証処理(例えば、搭乗ゲート装置14からの認証要求に関する処理)にて他人受入発生の蓋然性が高いと判定される。そこで、サーバ装置20は、搭乗ゲート装置14における認証時に他人受入の発生した可能性が高い旨を職員に通知する。

【0185】

上記実施形態では、サーバ装置20は、1人の旅客(認証成功者)の認証結果検証情報を職員端末30に送信することを説明した。しかし、サーバ装置20は、複数の旅客の認証結果検証情報をまとめて職員端末30に送信してもよい。例えば、サーバ装置20は、図11に示す認証データベースに記載されたエントリのうち複数のエントリそれぞれに対応した認証結果検証情報を生成し、職員端末30に送信してもよい。職員端末30は、取得した情報から図18に示すような一覧表示を行ってもよい。

10

【0186】

あるいは、サーバ装置20は、認証時に用いられた類似度等に従い、他人受入が発生している蓋然性が高いか否かを示すフラグが付与された認証結果検証情報を職員端末30に送信してもよい。職員端末30は、図19に示すように、当該フラグを参照して他人受入が発生している可能性の高い結果を強調するような表示をしてもよい。なお、図19では、灰色に着色されたエントリは他人受入が発生している蓋然性の高いエントリを示す。

【0187】

あるいは、職員端末30は、図18、図19に示す表示に接した職員がエントリを選択すると、図12や図13に示すような表示(顔画像を含む表示)を行ってもよい。あるいは、職員端末30は、顔画像に加え、認証成功者の氏名、エアラインコード、便番号等を併せて表示してもよい。

20

【0188】

上記実施形態では、図12、図13を参照しつつ、1つの画面に1つのエントリに関する認証結果検証対象を表示する場合について説明した。しかし、1つの画面に複数のエントリに関する認証結果検証対象(認証成功者の認証結果)が表示されていてもよい(図20参照)。

【0189】

上記実施形態では、類似度等に基づいて他人受入の発生確率が高い認証結果を特定する場合について説明した。しかし、当該特定は、機械学習により生成された学習モデルを用いて行われてもよい。具体的には、システム管理者等は、多数の他人受入発生時のデータ(取得顔画像、登録顔画像)を収集する。システム管理者等は、当該収集したデータに認証失敗に関するラベルを付与して教師データを生成する。システム管理者等は、当該教師データを学習器に入力し、学習モデル(分類モデル)を生成する。サーバ装置20に、当該学習モデルが実装される。サーバ装置20は、2枚の顔画像を学習モデルに入力し、判定結果(他人受入発生、非発生)を得る。サーバ装置20は、判定結果が「他人受入発生」の場合に、対応するエントリを情報提供の対象としたり職員にアラートを出す対象としたりしてもよい。なお、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。

30

40

【0190】

上記実施形態では、顔画像及び顔画像から生成された特徴量を「生体情報」として扱い、システムの動作等を説明した。しかし、顔画像等に替えて他の情報が「生体情報」として用いられてもよい。例えば、声紋認証が用いられる場合には、事前に登録された声紋情報(音声データ)が再生されることで、他人受入の発生が検出されてもよい。

【0191】

上記実施形態では、類似度や類似度を要素とする時系列データに基づいて認証結果検証情報の生成要否を判定する場合について説明した。サーバ装置20は、上記説明した複数

50

の方法を組み合わせ、認証結果検証情報の生成可否を判定してもよい。例えば、サーバ装置 20 は、複数の判定方法それぞれについて、認証結果検証情報の生成可否を判定する。サーバ装置 20 は、得られた複数の判定結果のうち少なくとも 1 つが「生成必要」であれば対応するエントリから認証結果検証情報を生成してもよい。あるいは、サーバ装置 20 は、複数の判定結果に対する統計処理の結果に基づいて認証結果検証情報の生成可否を決定してもよい。例えば、サーバ装置 20 は、「生成必要」と判定された数が所定の閾値よりも大きい場合に、対応するエントリから認証結果検証情報を生成してもよい

【0192】

上記実施形態では、サーバ装置 20 は、職員端末 30 を介して認証結果検証情報を職員等に提供する場合について説明した。しかし、サーバ装置 20 は、自装置の表示デバイス等を用いて上記情報提供を行ってもよい。あるいは、サーバ装置 20 は、職員等が駐在している管理室等に設置されたダッシュボード等を介して上記情報提供を行ってもよい。

【0193】

チェックイン端末 10 等とサーバ装置 20 の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。搭乗券情報やパスポート情報には個人情報が含まれ、当該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。

【0194】

サーバ装置 20 は、職員等に認証結果データベースの検索機能を提供してもよい。例えば、サーバ装置 20 は、他人受入が発生している可能性の高い認証結果を検索するような「検索部 407」を備えていてもよい（図 21 参照）。検索部 407 は、職員端末 30 等から検索条件を取得する。検索部 407 は、当該条件に合致する認証結果を検索し、検索結果を返信する。例えば、検索部 407 は、職員等からの情報入力に基づいて、認証成功者の類似度の差分（第 1 類似度と第 2 類似度の差分）が所定の閾値以下のエントリ（認証結果）を検索する。

【0195】

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。

【0196】

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、組み合わせで用いてもよい。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。

【0197】

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、空港等における搭乗手続きシステムなどに好適に適用可能である。但し、本願開示の適用先は空港の手続きに限定されず、本願開示は複数の手続きを要するシステムに適用可能である。例えば、イベント会場等の入退場制御において本願開示を適用することもできる。例えば、サーバ装置 20 が、イベント会場における認証履歴を解析し、誤認証が強く疑われる結果についてはその旨をイベント主催者等に通知してもよい。

【0198】

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〕

複数の端末のうち被認証者の生体情報を取得した端末から、前記被認証者の生体情報を含む認証要求を受信する、受信部と、

10

20

30

40

50

前記被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行う、認証部と、

前記生体認証に成功した認証成功者について、前記予め登録された生体情報と、前記認証要求を処理した際の詳細を含む情報であって前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する、記憶部と、

を備える、サーバ装置。

[付記 2]

前記記憶部が記憶する前記認証結果詳細情報は、前記認証要求の送信元を識別する端末 ID をさらに含み、

少なくとも前記予め登録された生体情報、前記端末 ID 及び前記端末により取得された生体情報を含む認証結果検証情報を生成する、生成部をさらに備える、付記 1 に記載のサーバ装置。

10

[付記 3]

前記認証結果詳細情報は、前記生体認証により認証成功と判定された際の類似度を含む、付記 2 に記載のサーバ装置。

[付記 4]

前記生成部は、前記認証結果詳細情報を解析し、前記認証結果検証情報を生成するか否かを判定する、付記 3 に記載のサーバ装置。

[付記 5]

前記生成部は、前記類似度に基づいて、前記認証結果検証情報を生成するか否かを決定する、付記 4 に記載のサーバ装置。

20

[付記 6]

前記生成部は、前記認証結果詳細情報に含まれる類似度が第 1 の閾値よりも小さい場合に、前記認証結果検証情報を生成する、付記 5 に記載のサーバ装置。

[付記 7]

前記生成部は、最も大きい第 1 類似度と 2 番目に値の大きい第 2 類似度の差分が、第 2 の閾値よりも小さい場合に、前記認証結果検証情報を生成する、付記 5 又は 6 に記載のサーバ装置。

[付記 8]

前記生成部は、

30

同じ認証成功者に関して、複数の前記認証結果詳細情報が記憶されている場合、

前記複数の認証結果詳細情報それぞれに含まれる類似度を要素とする時系列データに対する統計処理の結果に基づいて、前記認証結果詳細情報を生成するか否かを決定する、付記 5 乃至 7 のいずれかに記載のサーバ装置。

[付記 9]

前記生成部は、前記認証結果検証情報を、空港又は航空会社の職員が使用する職員端末に送信する、付記 2 乃至 8 のいずれかに記載のサーバ装置。

[付記 10]

前記生成部は、定期的又は所定のタイミングで前記認証結果詳細情報を解析し、生成する必要があると判定された前記認証結果検証情報と共に、対応する認証成功者のフライトに関する情報を前記職員端末に送信する、付記 9 に記載のサーバ装置。

40

[付記 11]

前記生体情報は、顔画像又は前記顔画像から抽出された特徴量である、付記 1 乃至 10 のいずれかに記載のサーバ装置。

[付記 12]

複数の端末と、

前記複数の端末と接続されたサーバ装置と、

を含み、

前記サーバ装置は、

前記複数の端末のうち被認証者の生体情報を取得した端末から、前記被認証者の生体情

50

報を含む認証要求を受信する、受信部と、

前記被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行う、認証部と、

前記生体認証に成功した認証成功者について、前記予め登録された生体情報と、前記認証要求を処理した際の詳細を含む情報であって前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する、記憶部と、

を備える、システム。

[付記 13]

サーバ装置において、

複数の端末のうち被認証者の生体情報を取得した端末から、前記被認証者の生体情報を含む認証要求を受信し、

前記被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行い、

前記生体認証に成功した認証成功者について、前記予め登録された生体情報と、前記認証要求を処理した際の詳細を含む情報であって前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する、サーバ装置の制御方法。

[付記 14]

サーバ装置に搭載されたコンピュータに、

複数の端末のうち被認証者の生体情報を取得した端末から、前記被認証者の生体情報を含む認証要求を受信する処理と、

前記被認証者の生体情報と予め登録された複数の利用者それぞれの生体情報を用いた生体認証を行う処理と、

前記生体認証に成功した認証成功者について、前記予め登録された生体情報と、前記認証要求を処理した際の詳細を含む情報であって前記認証要求の送信元である端末により取得された生体情報を含む認証結果詳細情報と、を対応付けて記憶する処理と、

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。

【0199】

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 Scope 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】

【0200】

10 チェックイン端末

11 手荷物預け機

12 旅客通過システム

13 ゲート装置

14 搭乗ゲート装置

20、100 サーバ装置

30 職員端末

101 受信部

102、404 認証部

103、206、306、406 記憶部

201、301、401 通信制御部

202 システム登録部

203 トークン発行要求部

204、304 メッセージ出力部

10

20

30

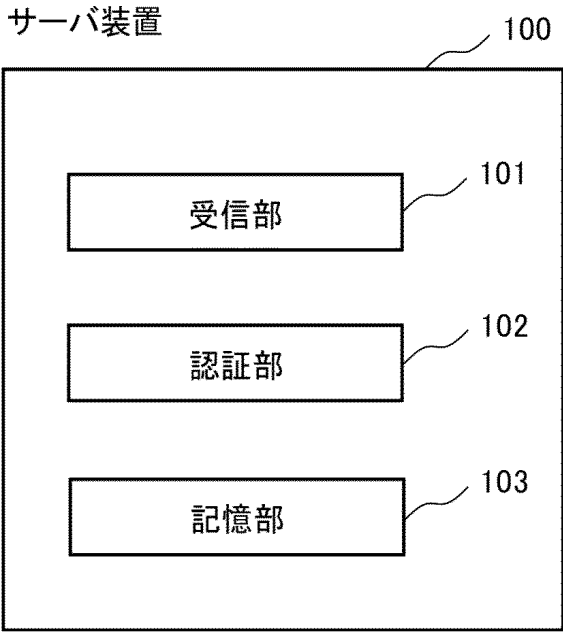
40

50

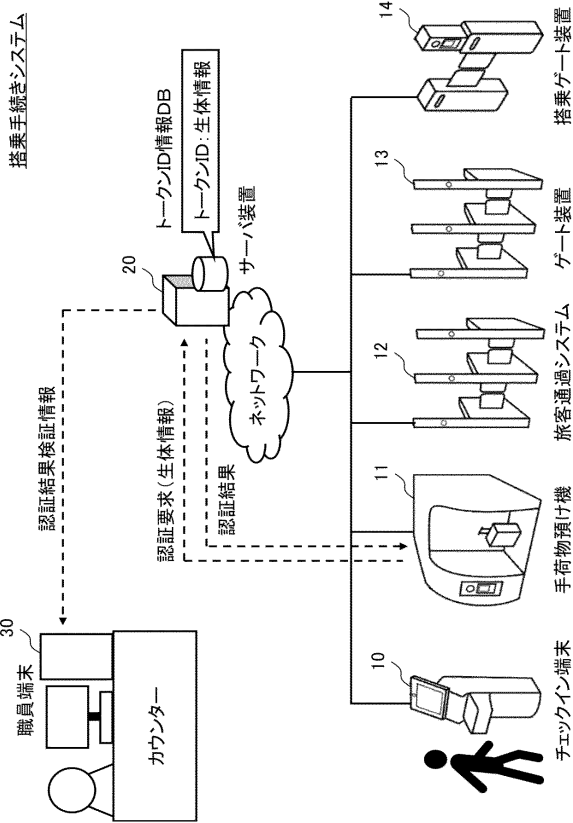
- 205 チェックイン実行部
- 211 搭乗券情報取得部
- 212 パスポート情報取得部
- 213、302 生体情報取得部
- 303 認証要求部
- 305 機能実現部
- 311 プロセッサ
- 312 メモリ
- 313 入出力インターフェイス
- 314 通信インターフェイス
- 402 トークン生成部
- 403 データベース管理部
- 405 検証情報生成部
- 407 検索部

【図面】

【図1】



【図2】



10

20

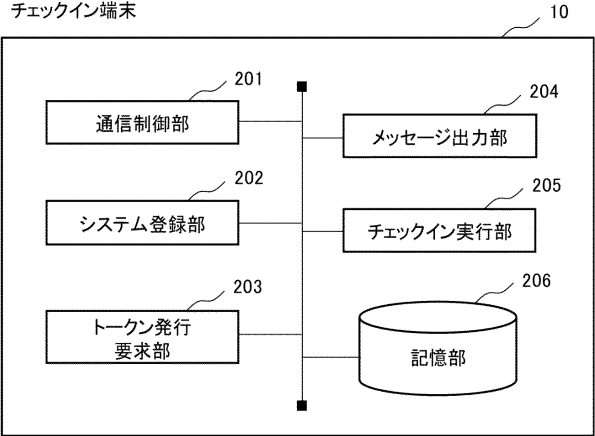
30

40

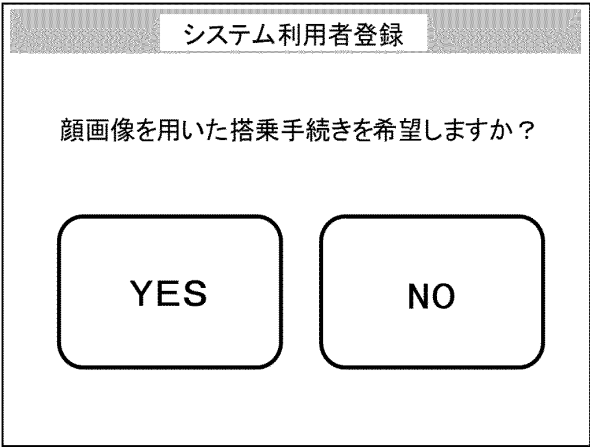
50

【図 3】

チェックイン端末

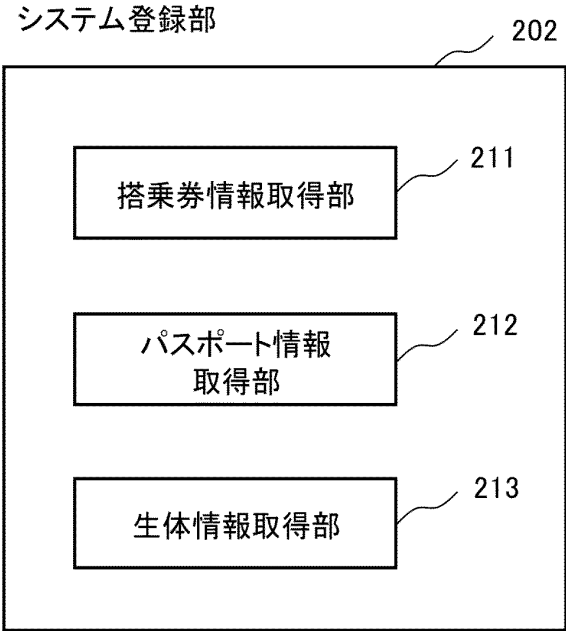


【図 4】



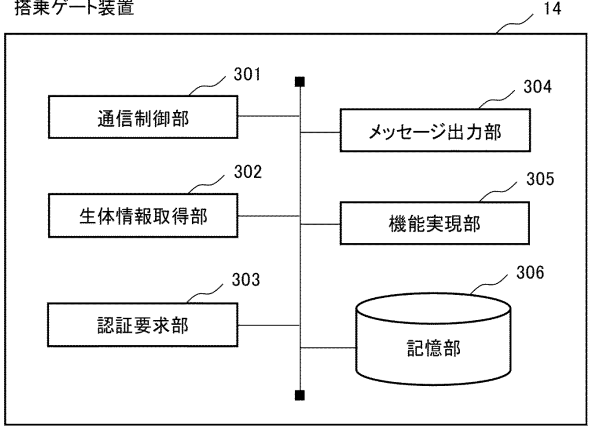
【図 5】

システム登録部



【図 6】

搭乗ゲート装置



10

20

30

40

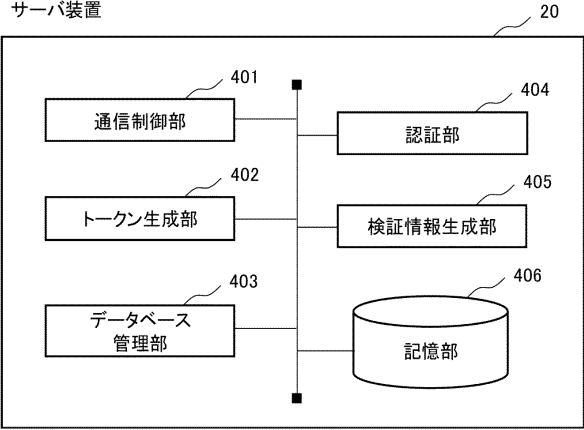
50

【図 7】

端末ID	生体情報	...
------	------	-----

認証要求

【図 8】



10

【図 9】

トークンID情報データベース

トークンID	登録顔画像	特徴量	発行時刻	デバイス名	...
ID01	F01	Fv01	12:01:01	D1	...
ID02	F02	Fv02	12:02:02	D2	...
ID03	F03	Fv03	12:03:03	D3	...
⋮	⋮	⋮	⋮	⋮	⋮

【図 10】

業務情報データベース

トークンID	搭乗者名	出発地	目的地	エリアインコード	便番号	運行年月日	...
ID01	AAA	A1	B1	C1	AA1	2020/1/20	...
ID02	BBB	A2	B2	C2	AA2	2020/1/20	...
ID03	CCC	A3	B3	C3	AA3	2020/1/20	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

20

30

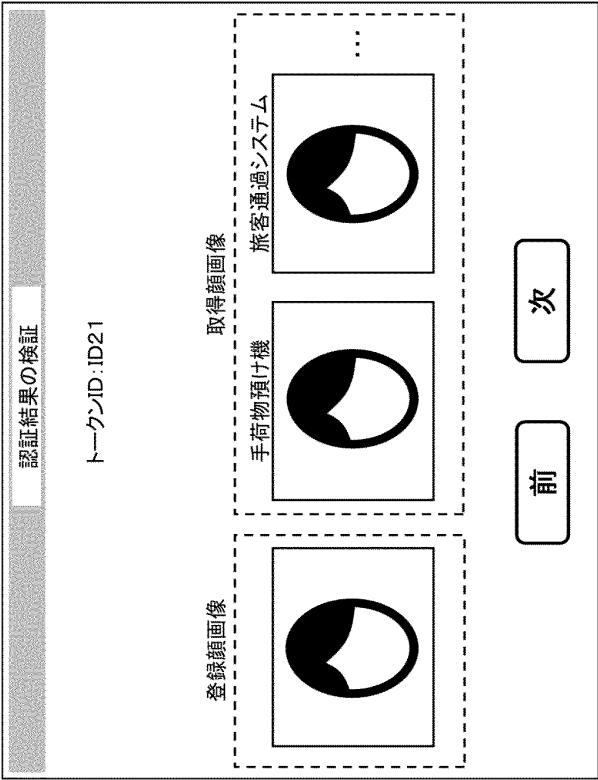
40

50

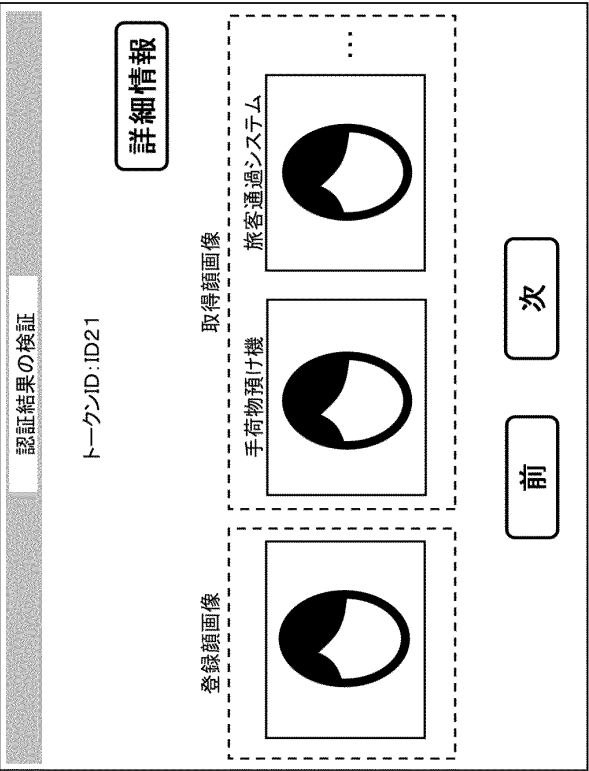
【図 1 1】

認証結果データベース			
トークンID	登録顔画像	認証結果詳細情報 1	
		端末ID	類似度
ID11	F11	11	oF11
ID12	F12	11	oF12
ID13	F13	11	oF13
...	...	...	...
		認証結果詳細情報 2	
		端末ID	類似度
...	...	12	oF21
...	...	12	oF22
...	...	12	oF23
...	...	...	...

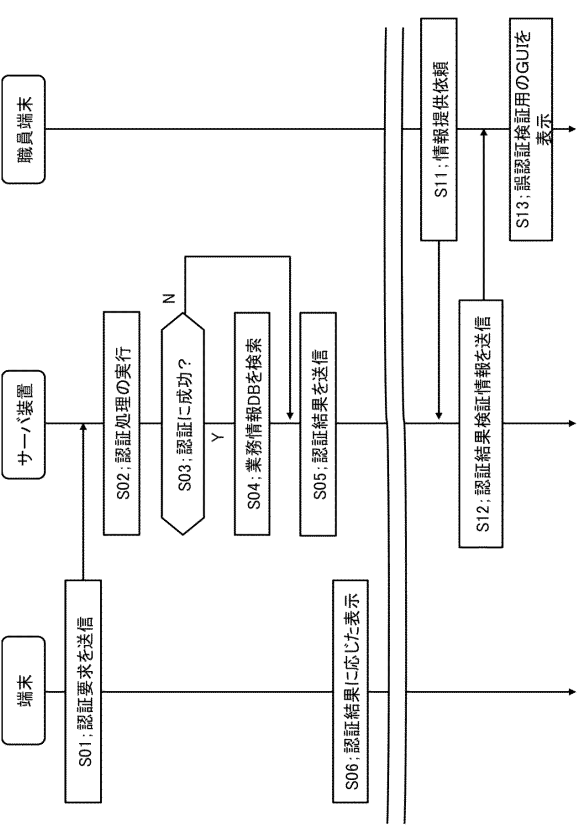
【図 1 2】



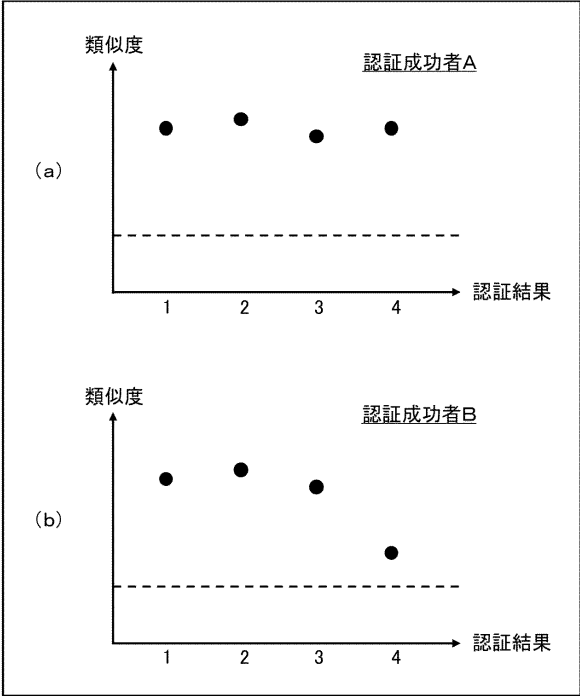
【図 1 3】



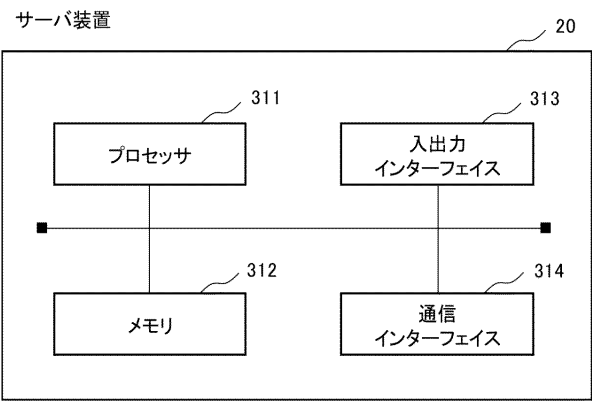
【図 1 4】



【図 1 5】



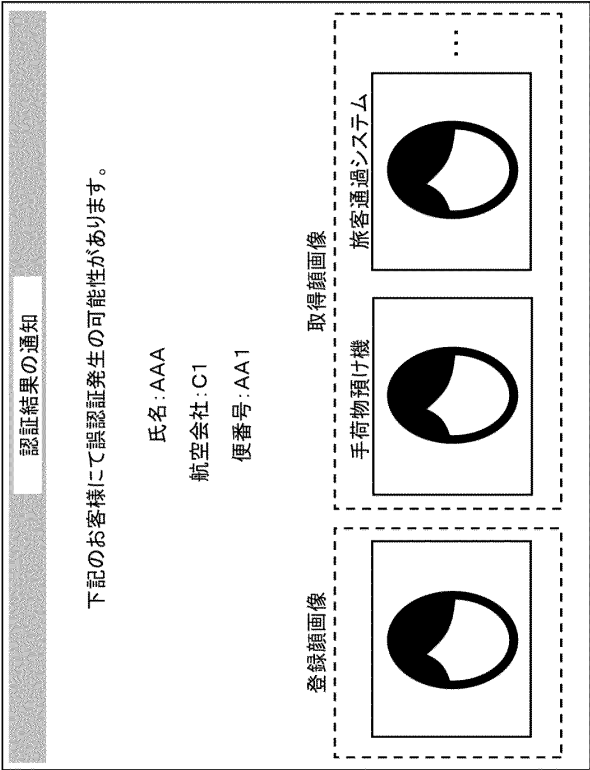
【図 1 6】



10

20

【図 1 7】



【図 1 8】

Figure 18 is a table showing authentication results. The table has four columns: 'トークンID' (Token ID), '認証結果詳細情報1' (Authentication Result Detailed Information 1), '認証結果詳細情報2' (Authentication Result Detailed Information 2), and '類似度' (Similarity Degree). The rows are indexed by 'トークンID' from ID11 to ID19, and by '類似度' from S21 to S29. The '認証結果詳細情報1' column contains '端末ID' (Terminal ID) and '類似度' (Similarity Degree). The '認証結果詳細情報2' column contains '端末ID' (Terminal ID) and '類似度' (Similarity Degree).

トークンID	認証結果詳細情報1		認証結果詳細情報2	
	端末ID	類似度	端末ID	類似度
ID11	11	S11	12	S21
ID12	11	S12	12	S22
ID13	11	S13	12	S23
ID14	11	S14	12	S24
ID15	11	S15	12	S25
ID16	11	S16	12	S26
ID17	11	S17	12	S27
ID18	11	S18	12	S28
ID19	11	S19	12	S29
...	...	...	...	...

30

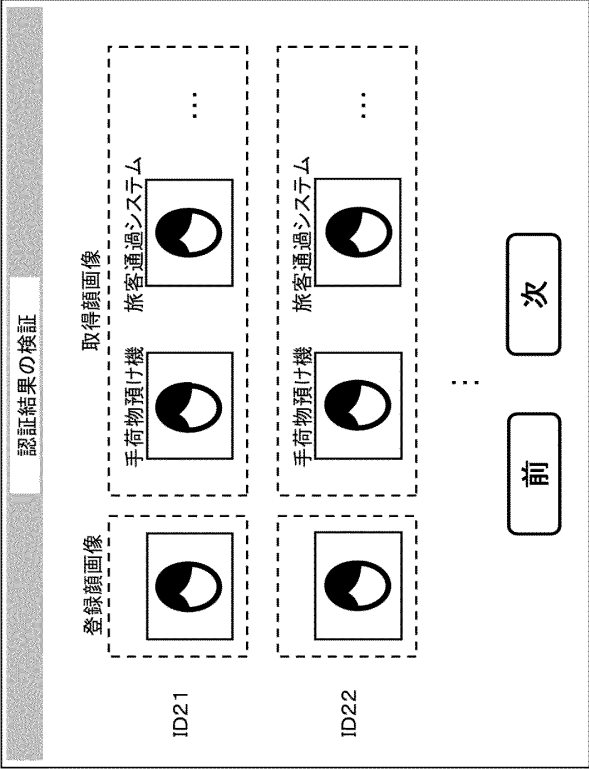
40

50

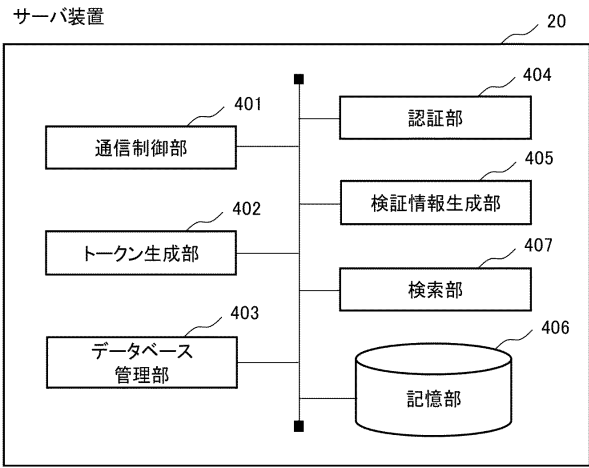
【図 19】

認証結果の検証					
トークンID	認証結果詳細情報1		認証結果詳細情報2		...
	端末ID	類似度	端末ID	類似度	
ID11	11	S11	12	S21	...
ID12	11	S12	12	S22	...
ID13	11	S13	12	S23	...
ID14	11	S14	12	S24	...
ID15	11	S15	12	S25	...
ID16	11	S16	12	S26	...
ID17	11	S17	12	S27	...
ID18	11	S18	12	S28	...
ID19	11	S19	12	S29	...
...	...	...	...	...	...

【図 20】



【図 21】



10

20

30

40

50

フロントページの続き

日本電気株式会社内

審査官 宮司 卓佳

- (56)参考文献 特開 2002-140306 (JP, A)
特開 2015-049602 (JP, A)
特表 2020-504363 (JP, A)
特開 2004-078686 (JP, A)
特開 2018-045340 (JP, A)
- (58)調査した分野 (Int.Cl., DB名)
G06F 21/32
G06Q 50/26