

明 細 書

発明の名称： 情報処理装置、情報処理方法及び記録媒体

技術分野

[0001] 本発明は、情報処理装置、情報処理方法及び記録媒体に関する。

背景技術

[0002] 特許文献1には、カメラで撮像されたユーザの顔画像とデータベースに予め記憶されている登録者の顔画像とを照合し、その照合結果に基づいてユーザを認証する認証装置が開示されている。当該認証装置は、顔照合の照合結果が照合一致である場合に、ユーザに対して予め設定されたセキュリティ権限に関するレベル値と所定の閾値とを更に対比することによって、最終的な認証可否の判定を行う。そして、当該認証装置は、ユーザが両方の判定条件を満たさないとき、電子錠を施錠状態に制御する。

先行技術文献

特許文献

[0003] 特許文献1：特開2006-336364号

発明の概要

発明が解決しようとする課題

[0004] しかし、特許文献1には、認証不可である場合に認証不可の理由又は対処方法を通知することは開示されていない。このため、認証装置がユーザを認証不可であると判定した場合の状況把握が困難となる虞がある。

[0005] そこで、本発明は、上述の問題に鑑み、認証装置がユーザを認証不可であると判定した場合の状況把握を容易にする情報処理装置、情報処理方法及び記録媒体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

[0006] 本発明の一観点によれば、管理対象の利用を要求するユーザから取得された生体情報と複数の登録者の各々の登録生体情報とを照合する照合部と、前記複数の登録者のうちの照合結果が照合一致である登録者が前記管理対象の

利用権限を有するか否かを判定する判定部と、前記照合部における前記照合結果が照合不一致である場合には第1エラー情報を出力し、前記判定部において前記照合結果が照合一致である登録者が前記利用権限を有していないと判定された場合には前記第1エラー情報とは異なる第2エラー情報を出力する出力部と、を備える情報処理装置が提供される。

[0007] 本発明の他の観点によれば、管理対象の利用を要求するユーザから取得された生体情報と複数の登録者の各々の登録生体情報とを照合する照合処理を行うステップと、前記複数の登録者のうちの照合結果が照合一致である登録者が前記管理対象の利用権限を有するか否かを判定する判定処理を行うステップと、前記照合処理における前記照合結果が照合不一致である場合には第1エラー情報を出力し、前記判定処理において前記照合結果が照合一致である登録者が前記利用権限を有していないと判定された場合には前記第1エラー情報とは異なる第2エラー情報を出力するステップと、を備える情報処理方法が提供される。

[0008] 本発明の更に他の観点によれば、コンピュータに、管理対象の利用を要求するユーザから取得された生体情報と複数の登録者の各々の登録生体情報とを照合する照合処理を行うステップと、前記複数の登録者のうちの照合結果が照合一致である登録者が前記管理対象の利用権限を有するか否かを判定する判定処理を行うステップと、前記照合処理における前記照合結果が照合不一致である場合には第1エラー情報を出力し、前記判定処理において前記照合結果が照合一致である登録者が前記利用権限を有していないと判定された場合には前記第1エラー情報とは異なる第2エラー情報を出力するステップと、を実行させるためのプログラムが記録された記録媒体が提供される。

発明の効果

[0009] 本発明によれば、認証装置がユーザを認証不可であると判定した場合の状況把握を容易にする情報処理装置、情報処理方法及び記録媒体を提供することができる。

図面の簡単な説明

[0010] [図1]第1実施形態における生体認証システムの全体構成例を示すブロック図である。

[図2]第1実施形態における認証情報データベースが記憶する情報の一例を示す図である。

[図3]第1実施形態における人物属性情報データベースが記憶する情報の一例を示す図である。

[図4]第1実施形態におけるオプトイン情報データベースが記憶する情報の一例を示す図である。

[図5]第1実施形態におけるオプトイン情報を説明する図である。

[図6]第1実施形態における拡張情報データベースが記憶する情報の一例を示す図である。

[図7]第1実施形態における施設ごとの拡張項目を説明する図である。

[図8]第1実施形態における認証サーバのハードウェア構成例を示すブロック図である。

[図9]第1実施形態における管理サーバのハードウェア構成例を示すブロック図である。

[図10]第1実施形態における入退場制御装置のハードウェア構成例を示すブロック図である。

[図11]第1実施形態における業務端末のハードウェア構成例を示すブロック図である。

[図12]第1実施形態における生体認証システムの処理の一例を示すフローチャートである。

[図13]第1実施形態における生体認証システムの処理の一例を示すフローチャートである。

[図14]第1実施形態における入退場制御装置が表示する画面の一例を示す図である。

[図15]第1実施形態における入退場制御装置が表示する画面の一例を示す図である。

[図16]第2実施形態における情報処理装置の構成例を示すブロック図である。

発明を実施するための形態

[0011] 以下、図面を参照して、本発明の例示的な実施形態を説明する。図面において同様の要素又は対応する要素には同一の符号を付し、その説明を省略又は簡略化することがある。

[0012] [第1実施形態]

図1は、生体認証システム1の全体構成例を示すブロック図である。図1に示されるように、生体認証システム1は、認証サーバ10、管理サーバ20、入退場制御装置30及び業務端末40を備えるコンピュータシステムである。各装置は、LAN (Local Area Network) やインターネット等のネットワークNWに接続されている。

[0013] 本実施形態における生体認証システム1は、例えば、オフィスビル、テーマパーク、ホテル及びイベント会場等の各種施設への入退場のための本人確認、空港・海港・国境における入出国のための本人確認、行政機関における本人確認、決済処理における本人確認等に適用され得る。

[0014] 認証サーバ10は、管理サーバ20からの認証要求に応じて認証処理を実行する情報処理装置（サーバコンピュータ）である。具体的には、認証サーバ10は、本システムの加盟店の施設において撮像された顔画像（あるいは特徴量）と、認証情報データベース11に予め登録された登録顔画像（あるいは特徴量）との照合処理を実行し、その照合結果に基づいてユーザの認証を行う。

[0015] また、認証サーバ10は、照合処理の照合結果が照合一致である場合に、ユーザが管理対象である施設の利用権限を有する人物か否かを判定する。なお、本実施形態における「照合一致」の語句は、照合処理における照合スコアが所定の閾値以上であることを意味するものとする。「照合不一致」の語句は、照合スコアが閾値未満であることを意味するものとする。

[0016] そして、認証サーバ10は、ユーザが管理対象である施設の利用権限を有

する人物であると判定した場合には、対象施設における入退場、サービスの利用、商品の購入やサービスの利用に対する決済等を許可する。なお、認証サーバ10は、ユーザが（A）顔照合の照合結果が照合不一致、（B）対象施設に関する利用権限を有していない、のいずれかに該当する場合には、（A）・（B）のそれぞれに対応するエラー情報をユーザに対して出力する。なお、当該エラー情報には、ユーザにエラーに対する対処を促す案内情報も含まれる。詳細については後述する。

[0017] また、認証サーバ10は、認証情報データベース11、人物属性情報データベース12、オプトイン情報データベース13及び拡張情報データベース14等のデータベースを有する。なお、認証サーバ10が備えるデータベースは、これらに限定されない。

[0018] 認証情報データベース11は、登録者の生体情報を記憶するデータベースである。本実施形態における“生体情報”の語句は、顔画像及び顔画像から抽出される特徴量を意味するものとするが、生体情報は顔画像及び顔特徴量に限られない。生体情報としては、虹彩画像、指紋画像、掌紋画像及び耳介画像等を用いてもよい。

[0019] 図2は、認証情報データベース11が記憶する情報の一例を示す図である。ここでは、認証情報データベース11は、パーソンID、認証ID、登録顔画像及び特徴量をデータ項目として含んでいる。パーソンIDは、登録者ごとに固有な識別子である。パーソンIDは、ユーザが生体認証システム1に生体情報を登録する際に発行される。認証IDは、パーソンIDの発行を決定した認証処理を特定する識別子である。例えば、認証IDは認証処理を実行した日時やパーソンIDの発行順序に基づいて設定され得る。

[0020] 人物属性情報データベース12は、登録者の人物属性情報を記憶するデータベースである。図3は、人物属性情報データベース12が記憶する情報の一例を示す図である。ここでは、人物属性情報データベース12は、パーソンID、氏名、性別、年齢及び住所をデータ項目として含んでいる。また、人物属性情報データベース12は、複数の拡張情報外部キーをデータ項目と

して含んでいる。拡張情報外部キーは、加盟店の業務システム（例えば、ホテルの宿泊予約システム、テーマパークのチケット販売システム等）から登録者についての業務情報を取得するために用いられる。取得された業務情報は、後述する拡張情報データベース 14 において拡張情報として記憶・管理される。

[0021] オプトイン情報データベース 13 は、認証基盤である認証サーバ 10 を利用する複数の加盟店のうち、ユーザが生体情報の利用を許諾（opt-in）した加盟店に関する情報（以下、「オプトイン情報」と呼ぶ。）を記憶するデータベースである。オプトイン情報は、例えばユーザが生体認証システム 1 における登録画面（不図示）に表示されている加盟店一覧の中から任意に加盟店を指定することで作成され得る。

[0022] 図 4 は、オプトイン情報データベース 13 が記憶する情報の一例を示す図である。ここでは、オプトイン情報データベース 13 は、パーソン ID、企業コード、加盟店コード及びサービス ID をデータ項目として含んでいる。企業コードは、企業ごとに固有な識別子である。加盟店コードは、同一企業に属する加盟店（以下、単に「施設」ともいう。）ごとに固有な識別子である。サービス ID は、加盟店において利用するサービス内容を示す識別子である。例えば、施設が“カジノ”である場合には、パスポート等の写真付き公的証明書の顔画像に基づいた本人確認サービス、施設への入場時から退場時までに所定の時間制限がある場合には、入場時からの経過時間を計測するサービス等をそれぞれ異なるサービス ID により区別する。

[0023] 図 5 は、オプトイン情報を説明する図である。ここでは、複数の登録者のパーソン ID と、複数の加盟店（ホテル／テーマパーク／カジノ／フィットネスジム）における顔認証サービスの利用可否が表形式で示されている。図 5 において、例えば、パーソン ID が“1000123”である登録者は“ホテル”、“テーマパーク”、“カジノ”及び“フィットネスジム”の 4 つの施設について顔認証サービスを利用することを許諾している。

[0024] 一方、パーソン ID が“1000125”の登録者は、ホテルとカジノの

2つの加盟店について顔認証サービスを利用することを許諾している。すなわち、後者は、“ホテル”及び“カジノ”についての利用権限を有するが、“テーマパーク”及び“フィットネスジム”についての利用権限を有していない。認証サーバ10は、登録者のパーソナルIDに基づいてオプトイン情報データベース13を参照することにより、登録者が対象の加盟店に関する利用権限を有するか否かを判定できる。

[0025] 拡張情報データベース14は、各施設に対する登録者の利用権限の有無を詳細に判定するために使用される拡張情報を記憶するデータベースである。図6は、拡張情報データベース14が記憶する情報の一例を示す図である。ここでは、拡張情報データベース14は、拡張情報ID、施設ID、施設区分及び拡張項目をデータ項目として含んでいる。拡張情報IDは、拡張情報ごとに固有な識別子であり、上述した拡張情報外部キーに対応する。施設IDは、加盟店の施設ごとに固有な識別子である。施設区分は、施設の種類を示す区分である。拡張項目は、施設ごとに定義されるデータ項目である。

[0026] 図7は、施設ごとの拡張項目を説明する図である。ここでは、施設として“ホテル”、“テーマパーク”、“カジノ”及び“フィットネスジム”の4つが例示され、各施設に複数の拡張項目が対応付けられている。施設が“ホテル”の場合には、拡張項目として予約チャンネルID、予約番号、部屋番号、人数、宿泊予定日、チェックイン日時、チェックアウト日時が含まれている。これらの拡張項目は、上述したパーソナルID及びオプトイン情報によって登録者ごとに取得できる。このため、ユーザが認証を要求した日にユーザの宿泊予約が存在しない場合には、ユーザはホテルの利用権限を有しないと判定される。

[0027] また、施設が“テーマパーク”の場合には、拡張項目としてチケット種別、チケットID、有効期間、入場日時が含まれている。チケット種別は、例えば年間チケット、当日チケット、回数券等である。したがって、チケット種別や有効期間等を考慮することにより、ユーザが認証を要求した日にテーマパークへの入場権限を有するか否かを詳細に判定できる。

- [0028] また、施設が“カジノ”の場合には、拡張項目としてトークンID、初回入場時、滞在時間合計が含まれている。トークンIDは、パーソンIDとは別に、カジノにおいてパスポート等の顔写真付きの公的証明書の提示及び認証を条件として初回入場時に発行される識別子である。したがって、施設が“カジノ”である場合には、ユーザに対してトークンIDが発行されていることや、滞在時間合計が所定の制限時間を超えていないことを入場条件に含めることができる。
- [0029] そして、施設が“フィットネスジム”の場合には、拡張項目として会員種別及び有効期間が含まれている。会員種別は、レギュラー会員、ナイト会員、平日会員、ゲスト会員等の種別である。有効期間は、会員証の有効期間である。したがって、施設が“フィットネスジム”である場合には、ユーザが認証を要求した日付及び時間帯が会員種別や有効期間の条件を満たすか否かを入場条件に含めることができる。
- [0030] 管理サーバ20は、PC (Personal Computer)、サーバ等のコンピュータであり、例えば複数の加盟店（施設）の各々に対応して設けられる。例えば、ホテルの業務システムを管理する管理サーバ20と、テーマパークの業務システムを管理サーバ20は、互いに独立している。
- [0031] 入退場制御装置30は、施設においてユーザの入退場を制御する装置である。入退場制御装置30としては、施設の出入口に設置されるゲート装置や、部屋のドアの電子錠を制御する装置等が挙げられる。
- [0032] 業務端末40は、施設の管理者、職員又は認証対象者であるユーザが使用する端末装置である。業務端末40としては、業務内容に応じて、PC、タブレット端末及びKIOSK端末等の各種端末が用いられる。業務端末40は、例えば、ユーザが自身で操作し、生体情報、人物属性情報及びオプトイン情報を登録及び更新する際にも使用され得る。
- [0033] 続いて、図8乃至図11を参照しながら、生体認証システム1における各装置のハードウェア構成を説明する。
- [0034] 図8は、認証サーバ10のハードウェア構成例を示すブロック図である。

同図に示すように、認証サーバ１０は、演算、制御及び記憶を行うコンピュータとして、ＣＰＵ（Central Processing Unit）１０１、ＲＡＭ（Random Access Memory）１０２、ＲＯＭ（Read Only Memory）１０３、ＨＤＤ（Hard Disk Drive）１０４、通信Ｉ／Ｆ（Interface）１０５、表示装置１０６及び入力装置１０７を備える。ＣＰＵ１０１、ＲＡＭ１０２、ＲＯＭ１０３、ＨＤＤ１０４、通信Ｉ／Ｆ１０５、表示装置１０６及び入力装置１０７は、バス、配線、駆動装置等を介して相互に接続される。

[0035] ＣＰＵ１０１は、ＲＯＭ１０３及びＨＤＤ１０４に記憶されたプログラムに従って所定の動作を行うとともに、認証サーバ１０の各部を制御する機能を有するプロセッサである。ＲＡＭ１０２は、揮発性記憶媒体から構成され、ＣＰＵ１０１の動作に必要な一時的なメモリ領域を提供する。ＲＯＭ１０３は、不揮発性記憶媒体から構成され、認証サーバ１０の動作に用いられるプログラム等の必要な情報を記憶する。ＨＤＤ１０４は、不揮発性記憶媒体から構成され、管理サーバ２０等から取得したデータの一時記憶、登録者の顔画像及び特徴量の記憶、認証サーバ１０の動作プログラム等の記憶等を行う記憶装置である。

[0036] 通信Ｉ／Ｆ１０５は、イーサネット（登録商標）、Ｗｉ－Ｆｉ（登録商標）、４Ｇ等の規格に基づく通信インターフェースであり、他の装置との通信を行うためのモジュールである。

[0037] 表示装置１０６は、動画、静止画、文字等を表示する液晶ディスプレイ、ＯＬＥＤ（Organic Light Emitting Diode）ディスプレイ等であって、ユーザへの情報の提示に用いられる。

[0038] 入力装置１０７は、キーボード、ポインティングデバイス、ボタン等であって、認証サーバ１０の管理者による操作を受け付ける。表示装置１０６及び入力装置１０７は、タッチパネルとして一体に形成されていてもよい。

[0039] 図９は、管理サーバ２０のハードウェア構成例を示すブロック図である。同図に示すように、管理サーバ２０は、ＣＰＵ２０１、ＲＡＭ２０２、ＲＯＭ２０３、ＨＤＤ２０４、通信Ｉ／Ｆ２０５、表示装置２０６及び入力装置

207を備える。CPU201、RAM202、ROM203、HDD204、通信I/F205、表示装置206及び入力装置207は、バス、配線、駆動装置等を介して相互に接続される。

[0040] 図10は、入退場制御装置30のハードウェア構成例を示すブロック図である。同図に示すように、入退場制御装置30は、CPU301、RAM302、ROM303、HDD304、通信I/F305、表示装置306、入力装置307、媒体読取装置308、生体情報取得装置309及び開閉部材310を有している。

[0041] 媒体読取装置308は、ユーザが所持するカード、チケット及び電子機器等の各種の記録媒体を読み取り、記録媒体に記録された情報を取得する装置である。媒体読取装置308は、例えば、コードリーダー、イメージスキャナ、非接触IC(Integrated Circuit)リーダー、OCR(Optical Character Reader)装置等により構成され、その読取部にかざされた各種の記録媒体から情報を取得する。

[0042] 生体情報取得装置309は、生体情報としてユーザの顔画像を取得する装置である。生体情報取得装置309は、例えば、装置の前に立つユーザの顔を撮像するデジタルカメラであり、ユーザの顔を撮像する。

[0043] 開閉部材310は、入退場制御装置30におけるユーザの本人確認に成功した場合に、CPU301による制御に従って、待機時においてユーザの通行を遮る閉鎖状態から、ユーザの通行を許可する開放状態へ移行する。開閉部材310の方式は、特に限定されるものではなく、例えば、通路の片側又は両側から設けられたフラッパーが開閉するフラッパーゲート、3本のバーが回転するターンスタイルゲート等である。

[0044] 図11は、業務端末40のハードウェア構成例を示すブロック図である。同図に示すように、業務端末40は、CPU401、RAM402、ROM403、HDD404、通信I/F405、表示装置406、入力装置407、媒体読取装置408及び生体情報取得装置409を有している。

[0045] なお、図8乃至図11に示されているハードウェア構成は一例であり、こ

れら以外の装置が追加されていてもよく、一部の装置が設けられていなくてもよい。また、一部の装置が同様の機能を有する別の装置に置換されていてもよい。また、本実施形態の一部の機能がネットワークNWを介して他の装置により提供されてもよく、本実施形態の機能が複数の装置に分散されて実現されてもよい。

[0046] 続いて、図12乃至図15を参照しながら、本実施形態における生体認証システム1の動作について説明する。

[0047] 図12は、生体認証システム1の処理の一例を示すフローチャートである。この処理は、ユーザが生体認証システム1に対して、生体情報、人物属性情報及びオプティン情報の登録又は更新を行う際に実行される。

[0048] ここでは、ユーザが各施設に設けられた業務端末40から管理サーバ20を介して認証サーバ10にアクセスして、各種情報の登録又は更新を行う場合を例として説明する。なお、各種情報の登録又は更新を行える装置は、業務端末40のみに限られない。ユーザがユーザ端末（不図示）からネットワークNWを介して生体認証システム1のWEBサイトにアクセスして、各種情報の登録・更新を行うことも可能である。

[0049] 先ず、認証サーバ10は、業務端末40から管理サーバ20を介してリクエストデータを受信すると、当該リクエストデータが生体情報の登録要求か否かを判定する（ステップS101）。

[0050] ここで、認証サーバ10は、リクエストデータが生体情報の登録要求であると判定した場合には（ステップS101、YES）、処理はステップS102へ移行する。

[0051] これに対し、認証サーバ10は、リクエストデータが生体情報の登録要求ではないと判定した場合（ステップS101、NO）には、処理はステップS111へ移行する。

[0052] ステップS102において、認証サーバ10は、管理サーバ20を介して、業務端末40の表示装置406に生体情報、人物属性情報及びオプティン情報の登録画面を表示させる。登録画面においては、ユーザは、入力装置4

07の操作によって、登録生体情報と、施設ごとの利用権限とを設定できるものとする。

[0053] 次に、業務端末40は、登録画面の表示中に、生体情報取得装置409によりユーザの顔画像を撮像すると（ステップS103）、撮像した顔画像を認証サーバ10へ送信する。

[0054] 次に、認証サーバ10は、業務端末40において撮像された顔画像を受信すると、顔画像から特徴量を算出し（ステップS104）、登録者であるユーザに対して固有なパーソンIDを発行する（ステップS105）。なお、パーソンIDの発行前に、特徴量に基づいて認証情報データベース11を検索し、ユーザの顔画像が未登録であることを確認してもよい。また、登録に際し、パスポートや免許証等から顔画像を読み取り、読み取った顔画像と撮像された顔画像とを照合して、本人確認をしてもよい。

[0055] 次に、認証サーバ10は、ユーザの生体情報である顔画像及び特徴量を認証情報データベース11に登録する（ステップS106）。

[0056] 次に、認証サーバ10は、ユーザが業務端末40の表示装置406に表示された登録画面の入力フォームにおいて入力した人物属性情報を取得すると（ステップS107）、取得した人物属性情報をパーソンIDと関連付けて人物属性情報データベース12に登録する（ステップS108）。また、人物属性情報の取得方法は、ステップS107のように登録画面上で入力された情報を取得する方法に限られない。例えば、ユーザの人物属性情報を記録している記録媒体（2次元バーコード、磁気カード、旅券、ICカード等）を光学的に又は電磁的に読み取ってもよい。これは、生体情報やオプトイン情報についても同様である。

[0057] 次に、認証サーバ10は、ユーザが登録画面の入力フォームにおいて入力したオプトイン情報を取得すると（ステップS109）、取得したオプトイン情報をパーソンIDと関連付けてオプトイン情報データベース13に登録し（ステップS110）、処理を終了する。

[0058] ステップS111において、認証サーバ10は、業務端末40の表示装置

406に生体情報、人物属性情報及びオプトイン情報の更新画面を表示させる。更新画面においては、ユーザは、入力装置407の操作によって、データベースに登録済みの登録生体情報と、施設ごとの利用権限とをそれぞれ変更する情報を入力できるものとする。

[0059] 次に、業務端末40は、更新画面の表示中に、生体情報取得装置409によりユーザの顔画像を撮像すると（ステップS112）、撮像した顔画像を認証サーバ10へ送信する。

[0060] 次に、認証サーバ10は、業務端末40において撮像された顔画像を受信すると、顔画像から特徴量を算出する（ステップS113）。次に、認証サーバ10は、撮影顔画像（あるいは特徴量）と認証情報データベース11に記憶されている登録顔画像（あるいは登録特徴量）との顔照合を実行する（ステップS114）。

[0061] 次に、認証サーバ10は、顔照合の照合結果に基づいてユーザのパーソンIDを特定する（ステップS115）。具体的には、認証サーバ10は、複数の登録者のうち、ステップS114における照合スコアが所定の閾値以上である登録者のパーソンIDを特定する。なお、複数人の登録者の各々の照合スコアが閾値以上である場合には、複数のパーソンIDが特定されてもよいし、照合スコアが最も高い登録者のパーソンIDのみを特定してもよい。

[0062] 次に、認証サーバ10は、ユーザが業務端末40に表示された更新画面の入力フォームにおいて入力した人物属性情報を取得すると（ステップS116）、取得した人物属性情報とパーソンIDに基づいて人物属性情報データベース12に記憶されている人物属性情報を更新する（ステップS117）。なお、ユーザが人物属性情報の変更を希望していない場合には、ステップS116及びステップS117の処理は省略される。また、ステップS107の場合と同様に、人物属性情報の取得方法は、更新画面上で入力された情報を取得する方法に限られない。

[0063] 次に、認証サーバ10は、ユーザが更新画面の入力フォームにおいて入力したオプトイン情報を取得すると（ステップS118）、取得したオプトイ

ン情報とパーソンIDに基づいてオプトイン情報データベース13に記憶されているオプトイン情報を更新し（ステップS119）、処理を終了する。
なお、ユーザがオプトイン情報の変更を希望していない場合には、ステップS118及びステップS119の処理は省略される。

[0064] 図13は、生体認証システム1の処理の一例を示すフローチャートである。
この処理は、例えば、ユーザが加盟店の施設において施設の利用（入退場、決済等）を要求した際に実行される。ここでは、加盟店の施設に設置された入退場制御装置30においてユーザが施設への入場を要求する場合を例として説明する。

[0065] 先ず、入退場制御装置30は、生体情報取得装置309によりユーザの顔画像を撮像すると（ステップS201）、撮像した顔画像を管理サーバ20経由で認証サーバ10へ送信する。

[0066] 次に、認証サーバ10は、入退場制御装置30において撮像された顔画像を受信すると、顔画像から特徴量を算出する（ステップS202）。次に、認証サーバ10は、撮影顔画像（あるいは特徴量）と認証情報データベース11に記憶されている登録顔画像（あるいは登録特徴量）との顔照合を実行する（ステップS203）。

[0067] 次に、認証サーバ10は、顔照合の照合結果に基づいてユーザがパーソンIDの登録者であるか否かを判定する（ステップS204）。

[0068] ここで、認証サーバ10が、ユーザが登録者であると判定した場合（ステップS204、YES）、処理はステップS205へ移行する。

[0069] これに対し、認証サーバ10が、ユーザが登録者ではないと判定した場合（ステップS204、NO）、処理はステップS207へ移行する。

[0070] ステップS205において、認証サーバ10は、認証情報データベース11を参照してユーザとの照合結果が照合一致である登録者のパーソンIDを特定する。

[0071] そして、認証サーバ10は、特定したパーソンIDに基づいて人物属性情報データベース12、オプトイン情報データベース13及び拡張情報データ

ベース 14 をそれぞれ検索し、登録者に関する人物属性情報、オプトイン情報及び拡張情報を取得する（ステップ S 206）。その後、処理はステップ S 208 へ移行する。

[0072] ステップ S 207 において、認証サーバ 10 は、顔照合の結果（照合不一致）に基づいて入退場制御装置 30 の表示装置 306 に顔照合エラーを示す案内画面を表示させる。

[0073] 図 14 は、入退場制御装置 30 が表示する画面の一例を示す図である。ここでは、顔照合エラーを示すエラーメッセージ（「お客様の生体情報（顔画像）は、認証システムに登録されていません。」）が案内画面に表示されている。これにより、ユーザは認証不可の理由を知ることができる。

[0074] また、同画面には、顔照合エラーに対してユーザが対処する方法を示す案内メッセージ（「当施設において顔認証サービスを利用される場合には、サービスカウンタにて生体情報を登録してください。」）も併せて表示されている。これにより、ユーザは認証不可の状況把握を容易に行えるだけでなく、認証不可の状況を解消するための対処方法も知ることができる。

[0075] なお、図 14 に示すエラーメッセージは一例に過ぎず、対処方法も様々である。例えば、入退場制御装置 30 における表示画面が案内画面から生体情報の登録画面に遷移し、その場で生体情報を登録できる構成にしてもよい。また、後続のユーザの認証処理を妨げないように、ゲート（入退場制御装置 30）の近傍に設置されているセルフ端末（例えば業務端末 40）に登録画面を連携表示させるシステム構成にしてもよい。これらの場合には、ユーザはサービスカウンタに赴かなくても済む利点がある。

[0076] ステップ S 208 において、認証サーバ 10 は、オプトイン情報及び拡張情報に基づいて、ユーザとの照合結果が照合一致である登録者が施設を利用できる人物であるか否かを判定する。ここでは、認証サーバ 10 が、登録者が施設を利用できる人物であると判定した場合（ステップ S 208、YES）、処理はステップ S 209 へ移行する。

[0077] これに対し、認証サーバ 10 が、登録者が施設を利用できる人物ではない

と判定した場合（ステップS 2 0 8、N O）、処理はステップS 2 1 0へ移行する。

[0078] ステップS 2 0 9において、認証サーバ1 0は、認証成功時の処理を実行し（ステップS 2 0 9）、処理を終了する。具体的には、認証サーバ1 0は、登録者と同一人物であると認証したユーザを施設内へ入場させるために、管理サーバ2 0を介して入退場制御装置3 0に対して開閉部材3 1 0を開放させる制御を行わせる。

[0079] ステップS 2 1 0において、認証サーバ1 0は、入退場制御装置3 0の表示装置3 0 6にユーザが施設の利用権限を有していないことを示す案内画面を表示させる。

[0080] 図1 5は、入退場制御装置3 0が表示する画面の一例を示す図である。ここでは、ユーザが施設の利用権限を有していないことを示すエラーメッセージ（「お客様は、顔認証サービスの利用対象リストに当施設を登録していません。」）が案内画面に表示されている。これにより、ユーザは認証不可の理由を知ることができる。

[0081] また、同画面には、利用権限のエラーに対してユーザが対処する方法を示す案内メッセージ（「当施設において顔認証サービスを利用される場合には、サービスカウンタにて利用対象リストを更新してください。」）も併せて表示されている。これにより、ユーザは認証不可の状況把握を容易に行えるだけでなく、認証不可の状況を解消するための対処方法も知ることができる。

[0082] なお、図1 5に示すエラーメッセージは一例に過ぎず、対処方法も様々である。例えば、入退場制御装置3 0における表示画面が案内画面から利用対象リストの更新画面に遷移し、その場で利用対象リストを更新できる構成にしてもよい。また、後続のユーザの認証処理を妨げないように、ゲート（入退場制御装置3 0）の近傍に設置されているセルフ端末（例えば業務端末4 0）に更新画面を連携表示させるシステム構成にしてもよい。これらの場合には、ユーザはサービスカウンタに赴かなくても済む利点がある。

[0083] 以上により、本実施形態によれば、認証サーバ10は、管理対象（例えば施設）の利用を要求したユーザと登録者との照合処理における照合結果が照合不一致である場合には登録者でないことを示す第1エラー情報（顔照合エラー）を出力し、利用権限の判定処理において登録者が管理対象の利用権限を有していないと判定された場合には第1エラー情報とは異なり、利用権限無しを示す第2エラー情報（利用権限エラー）を出力する。すなわち、認証サーバ10がユーザを認証不可であると判定した場合には、ユーザに対して認証不可の理由及び理由に応じた対処方法が通知される。これにより、ユーザは顔認証サービスへの登録状況や顔認証サービスの利用対象施設の登録状況を容易に把握することができる。また、ユーザは認証不可の認証結果に容易に対処できる。

[0084] [第2実施形態]

図16は、第2実施形態における情報処理装置100の構成例を示すブロック図である。情報処理装置100は、照合部100A、判定部100B及び出力部100Cを備える。照合部100Aは、管理対象の利用を要求するユーザから取得された生体情報と複数の登録者の各々の登録生体情報とを照合する。判定部100Bは、複数の登録者のうちの照合結果が照合一致である登録者が管理対象の利用権限を有するか否かを判定する。出力部100Cは、照合部100Aにおける照合結果が照合不一致である場合には第1エラー情報を出力し、判定部100Bにおいて照合結果が照合一致である登録者が管理対象の利用権限を有していないと判定された場合には第1エラー情報とは異なる第2エラー情報を出力する。本実施形態によれば、認証装置がユーザを認証不可であると判定した場合の状況把握を容易にできる。

[0085] [変形実施形態]

本発明は、上述の実施形態に限定されることなく、本発明の趣旨を逸脱しない範囲において適宜変更可能である。例えば、いずれかの実施形態の一部の構成を他の実施形態に追加した例や、他の実施形態の一部の構成と置換した例も、本発明の実施形態である。

- [0086] 上述の実施形態においては、エラー情報が認証対象者であるユーザに対して提示される情報である場合について説明したが、エラー情報の提示先はユーザのみに限られない。例えば、認証対象者ではない、施設の管理者に対して認証不可の理由及び対処方法を提示してもよい。また、ユーザと管理者の両方に対してエラー情報を提示してもよい。これにより、ユーザにエラー情報を提示する場合と同様の効果を奏する。すなわち、管理者はユーザの顔認証サービスへの登録状況や顔認証サービスの利用対象施設の登録状況を容易に把握することができる。この結果、管理者は認証サーバ10がユーザを認証不可とした認証結果に容易に対処できる。
- [0087] 上述の実施形態においては、ユーザが施設を利用する場合について説明したが、利用権限は施設に関する利用権限のみに限られない。例えば、会社の備品を管理するシステムの場合には、社員ごとに備品の利用権限（使用権限）を定めることで、顔認証によって備品の貸し出し管理を行うことができる。同様に、利用権限には、データベースへのアクセス権限等も含み得る。
- [0088] 上述の実施形態においては、認証サーバ10が照合処理、判定処理及び出力処理の機能を備えるシステム構成について説明した。しかし、認証サーバ10の機能の一部又は全部を他の装置（管理サーバ20、入退場制御装置30及び業務端末40等）が備えてもよい。例えば、認証サーバ10がユーザの生体情報及びオプトイン情報等を一元管理している場合に、各施設の入退場制御装置30等が認証サーバ10のデータベースを参照することで照合処理や判定処理を実行するシステム構成にしてもよい。
- [0089] 上述の実施形態の機能を実現するように該実施形態の構成を動作させるプログラムを記録媒体に記録させ、該記録媒体に記録されたプログラムをコードとして読み出し、コンピュータにおいて実行する処理方法も各実施形態の範疇に含まれる。すなわち、コンピュータ読取可能な記録媒体も各実施形態の範囲に含まれる。また、上述のプログラムが記録された記録媒体はもちろん、そのプログラム自体も各実施形態に含まれる。
- [0090] 該記録媒体としては例えばフロッピー（登録商標）ディスク、ハードディ

スク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性メモリカード等を用いることができる。また該記録媒体に記録されたプログラム単体で処理を実行しているものに限らず、他のソフトウェア、拡張ボードの機能と共同して、ＯＳ上で動作して処理を実行するものも各実施形態の範疇に含まれる。

[0091] 上述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うるが、以下には限られない。

[0092] (付記１)

管理対象の利用を要求するユーザから取得された生体情報と複数の登録者の各々の登録生体情報とを照合する照合部と、

前記複数の登録者のうちの照合結果が照合一致である登録者が前記管理対象の利用権限を有するか否かを判定する判定部と、

前記照合部における前記照合結果が照合不一致である場合には第１エラー情報を出力し、前記判定部において前記照合結果が照合一致である登録者が前記利用権限を有していないと判定された場合には前記第１エラー情報とは異なる第２エラー情報を出力する出力部と、

を備える情報処理装置。

[0093] (付記２)

前記第１エラー情報は、前記照合不一致を示す情報を含む、

付記１に記載の情報処理装置。

[0094] (付記３)

前記第２エラー情報は、前記ユーザが前記利用権限を有していないことを示す情報を含む、

付記１又は２に記載の情報処理装置。

[0095] (付記４)

前記第１エラー情報は、前記生体情報の登録を促す情報を含む、

付記１乃至３のいずれかに記載の情報処理装置。

[0096] (付記５)

前記第 2 エラー情報は、前記利用権限の登録を促す情報を含む、
付記 1 乃至 4 のいずれかに記載の情報処理装置。

[0097] (付記 6)

前記第 1 エラー情報及び前記第 2 エラー情報は、前記ユーザに対して提示される情報である、

付記 1 乃至 5 のいずれかに記載の情報処理装置。

[0098] (付記 7)

前記第 1 エラー情報及び前記第 2 エラー情報は、前記ユーザとは異なる管理者に対して提示される情報である、

付記 1 乃至 5 のいずれかに記載の情報処理装置。

[0099] (付記 8)

前記登録生体情報と複数の施設の各々に関する前記利用権限とを前記登録者ごとに関連付けて記憶する記憶部、

を更に備える付記 1 乃至 7 のいずれかに記載の情報処理装置。

[0100] (付記 9)

前記登録生体情報及び前記施設ごとの前記利用権限を設定する設定部と、
前記登録者ごとに固有な識別子を発行し、設定された前記登録生体情報と前記利用権限とを前記識別子により関連付けて前記記憶部に登録する制御部と、

を更に備える付記 8 に記載の情報処理装置。

[0101] (付記 10)

前記生体情報は、顔画像、虹彩画像、指紋画像、耳介画像及び掌紋画像のいずれかである、

付記 1 乃至 9 のいずれかに記載の情報処理装置。

[0102] (付記 11)

管理対象の利用を要求するユーザから取得された生体情報と複数の登録者の各々の登録生体情報とを照合する照合処理を行うステップと、

前記複数の登録者のうちの照合結果が照合一致である登録者が前記管理対

象の利用権限を有するか否かを判定する判定処理を行うステップと、

前記照合処理における前記照合結果が照合不一致である場合には第１エラー情報を出力し、前記判定処理において前記照合結果が照合一致である登録者が前記利用権限を有していないと判定された場合には前記第１エラー情報とは異なる第２エラー情報を出力するステップと、

を備える情報処理方法。

[0103] (付記１２)

コンピュータに、

管理対象の利用を要求するユーザから取得された生体情報と複数の登録者の各々の登録生体情報とを照合する照合処理を行うステップと、

前記複数の登録者のうちの照合結果が照合一致である登録者が前記管理対象の利用権限を有するか否かを判定する判定処理を行うステップと、

前記照合処理における前記照合結果が照合不一致である場合には第１エラー情報を出力し、前記判定処理において前記照合結果が照合一致である登録者が前記利用権限を有していないと判定された場合には前記第１エラー情報とは異なる第２エラー情報を出力するステップと、

を実行させるためのプログラムが記録された記録媒体。

符号の説明

[0104] NW・・・ネットワーク

１・・・生体認証システム

１０・・・認証サーバ

１１・・・認証情報データベース

１２・・・人物属性情報データベース

１３・・・オプトイン情報データベース

１４・・・拡張情報データベース

２０・・・管理サーバ

３０・・・入退場制御装置

４０・・・業務端末

100 . . . 情報処理装置

100A . . . 照合部

100B . . . 判定部

100C . . . 出力部