

明 細 書

発明の名称： 認証システム、方法及びプログラム

技術分野

[0001] 本発明は、認証システム、方法及びプログラムに関する。

背景技術

[0002] 顔認証を用いたサービスの普及が始まっている。例えば、空港における各種手続き（例えば、チェックイン、荷物預け入れ、セキュリティチェック等）に顔認証の適用が始まっている。

[0003] 例えば、特許文献1には、チェックインから搭乗に至る一連の手続きの流れをセキュリティブース内において旅客自身によりセルフで実施する構成が開示されている。特許文献1に開示された技術では、空港内に設置されたネットワークカメラにより旅客のトレーサビリティチェックが行われる。当該トレーサビリティチェックでは、空港内の任意の場所のネットワークカメラにより撮影された旅客の画像と、本人認証情報として記憶された旅客の顔画像を含む画像とが照合される。ネットワークカメラ設置場所の位置情報と撮影された画像のタイムスタンプとにより旅客の行動が追跡管理される。

先行技術文献

特許文献

[0004] 特許文献1：国際公開第2005/055151号

発明の概要

発明が解決しようとする課題

[0005] 上述のように、空港内の各種手続きに顔認証システムを適用することが始まっている。ここで、空港利用者のうち全ての利用者が顔認証システムを利用している訳ではなく、一定割合の利用者は顔認証システムを利用していないのが現状である。そのため、各種手続きに設置される全ての端末を顔認証対応とすることはできない。

[0006] そこで、手続きが行われる各エリアに設定された端末が、顔認証機能によ

る手続きと顔認証によらない手続きの両方に対応することが考えられる。即ち、顔認証機能と従来手続き機能の双方を備えたハイブリッド端末を設置することが考えられる。この場合、顔認証システム利用者は端末（ハイブリッド端末）の前を通り過ぎれば手続きが終了するが、顔認証システム非利用者はパスポート等を用いた本人認証を同じ端末で行うことになる。

[0007] このような対応（２つの機能を備えるハイブリッド端末の導入）によりシステム利用者と非利用者の混在に対応できるが、同じ端末にシステム利用者と非利用者が並ぶことになり顔認証システムの利便性が損なわれているといった側面もある。

[0008] 本発明は、利用者の利便性を向上させることに寄与する、認証システム、方法及びプログラム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、生体認証機能又は非生体認証機能によりサービスの提供が可能な少なくとも１以上の第１の端末と、それぞれが、生体認証機能と非生体認証機能の切り替えが可能であって、生体認証機能又は非生体認証機能によりサービスの提供が可能な、複数の第２の端末と、前記少なくとも１以上の第１の端末及び前記複数の第２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、前記少なくとも１以上の第１の端末における生体認証機能の利用率を計算し、前記計算された利用率に基づき前記複数の第２の端末のうち少なくとも１台以上の端末の動作モードを決定する、認証システムが提供される。

[0010] 本発明の第２の視点によれば、生体認証機能又は非生体認証機能によりサービスの提供が可能な少なくとも１以上の第１の端末と、それぞれが、生体認証機能と非生体認証機能の切り替えが可能であって、生体認証機能又は非生体認証機能によりサービスの提供が可能な、複数の第２の端末と、前記少なくとも１以上の第１の端末及び前記複数の第２の端末と接続されたサーバ装置と、を含む認証システムにおいて、前記少なくとも１以上の第１の端末における生体認証機能の利用率を計算し、前記計算された利用率に基づき前

記複数の第2の端末のうち少なくとも1台以上の端末の動作モードを決定する方法が提供される。

- [0011] 本発明の第3の視点によれば、生体認証機能又は非生体認証機能によりサービスの提供が可能な少なくとも1以上の第1の端末と、それぞれが、生体認証機能と非生体認証機能の切り替えが可能であって、生体認証機能又は非生体認証機能によりサービスの提供が可能な、複数の第2の端末と、前記少なくとも1以上の第1の端末及び前記複数の第2の端末と接続されたサーバ装置に搭載されたコンピュータに、前記少なくとも1以上の第1の端末における生体認証機能の利用率を計算する処理と、前記計算された利用率に基づき前記複数の第2の端末のうち少なくとも1台以上の端末の動作モードを決定する処理と、を実行させるためのプログラムを記録する、コンピュータ読取可能な記録媒体が提供される。

発明の効果

- [0012] 本発明の各視点によれば、利用者の利便性を向上させることに寄与する、認証システム、方法及びプログラムが提供される。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

- [0013] [図1]一実施形態の概要を説明するための図である。
[図2]第1の実施形態に係る認証システムの概略構成の一例を示す図である。
[図3]第1の実施形態に係る第1の端末の処理構成の一例を示す図である。
[図4]第1の実施形態に係る第2の端末の処理構成の一例を示す図である。
[図5]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6]動作モード決定部の動作を説明するための図である。
[図7]第1の実施形態に係る認証システムの動作の一例を示すシーケンス図である。
[図8]第2の実施形態に係る認証システムの概略構成の一例を示す図である。
[図9]第2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10]サーバ装置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

- [0014] 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。
- [0015] 一実施形態に係る認証システムは、少なくとも1以上の第1の端末101と、複数の第2の端末102と、サーバ装置103と、を含む（図1参照）。第1の端末101は、生体認証機能又は非生体認証機能によりサービスの提供が可能な端末である。第2の端末102は、それぞれが、生体認証機能と非生体認証機能の切り替えが可能であって、生体認証機能又は非生体認証機能によりサービスの提供が可能な端末である。サーバ装置103は、第1の端末101及び複数の第2の端末102と接続されたサーバである。サーバ装置103は、少なくとも1以上の第1の端末101における生体認証機能の利用率を計算する。サーバ装置103は、計算された利用率に基づき複数の第2の端末102のうち少なくとも1台以上の端末の動作モードを決定する。
- [0016] 上記認証システムでは、サーバ装置103が第1の端末101における生体認証の利用状況を把握する。サーバ装置103は、当該把握した生体認証の利用状況に応じて第2の端末102の動作モードを決定する。具体的には、サーバ装置103は、生体認証が多く利用されている状況では生体認証設定によりサービスを提供する第2の端末102の数を多くする。対して、サーバ装置103は、生体認証の利用状況が低調であれば生体認証設定により

サービスを提供する第２の端末１０２の数を少なくする。このような対応により、後段端末である第２の端末１０２の動作モードが最適化されシステムのスループットが上昇する。その結果、システムの利便性が向上する。

[0017] 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。

[0018] [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。

[0019] [システムの構成]

図２は、第１の実施形態に係る認証システムの概略構成の一例を示す図である。図２を参照すると、認証システムには、複数の第１の端末１０－１～１０－３と、複数の第２の端末２０－１～２０－３と、サーバ装置３０と、が含まれる。なお、図２に示す構成は例示であって、端末の数等を限定する趣旨ではない。

[0020] 以降の説明において、第１の端末１０－１～１０－３を区別する特段の理由がない場合には、単に「第１の端末１０」と表記する。他の要素についても同様に、ハイフンの前の符号により当該要素を代表して表記する。

[0021] 第１の端末１０とサーバ装置３０は有線又は無線の通信手段により通信可能に構成されている。第２の端末２０とサーバ装置３０も同様に通信可能に構成されている。

[0022] 第１の端末１０のそれぞれは、予め定められた手続きを行うように構成されている。例えば、第１の端末１０はチェックイン手続きを行うように構成されている。

[0023] 第２の端末２０のそれぞれは、上記第１の端末にて行われる手続きの後段の手続きを行うように構成されている。即ち、第２の端末２０は、第１の端末１０の後段に設置され、第１の端末１０とは異なる手続きを行うように構成されている。例えば、第２の端末２０は、チェックイン手続きが終了した利用者のセキュリティチェックに関する処理を行うように構成されている。

[0024] 第１の端末１０と第２の端末２０は、その動作モードを切り替え可能に構

成されている。具体的には、第1の端末10と第2の端末20は、顔認証による手続きを行う設定（以下、顔認証設定と表記する）と、顔認証を用いない従来型の手続きを行う設定（以下、非顔認証設定と表記する）と、が切り替え可能に構成されている。即ち、第1の端末10と第2の端末20は、顔認証機能と非顔認証機能（従来型の機能）の切り替えが可能であって、いずれかの機能を使って利用者にサービスを提供する。

[0025] 例えば、第1の端末10は、チェックイン手続きを行う端末であると想定する。この場合、顔認証設定の第1の端末10は、面前の利用者の生体情報（顔画像）を取得し、当該取得された生体情報から特徴量（複数の特徴量からなる特徴ベクトル）を生成する。その後、第1の端末10は、利用者が提示するパスポートのIC（Integrated Circuit）チップから対応する生体情報（顔画像）を取得し、当該顔画像から特徴量を生成する。第1の端末10は、上記2つの特徴量の照合（1対1照合）を行う。第1の端末10は、当該照合に成功すると、利用者の生体情報（又は特徴量）、利用者を一意に識別するID（Identifier）等を管理サーバ（図示せず）に送信する。管理サーバは、受信した情報を用いて利用者に顔認証サービスを提供する。

[0026] 一方、非顔認証設定の第1の端末10は、航空会社の職員が操作する端末として動作する。即ち、非顔認証設定の第1の端末10は、職員がパスポートを確認し、面前の利用者が正しいパスポートを所持していると判断した場合に、搭乗券を発行する端末として動作する。

[0027] 例えば、第2の端末20は、セキュリティチェックに関する処理を行う端末であると想定する。この場合、顔認証設定の第2の端末20は、金属探知等のゲートによりセキュリティチェックが完了した利用者の顔画像を取得し、当該取得された顔画像から特徴量を生成する。第2の端末20は、当該生成した特徴量を管理サーバに送信する。管理サーバは、取得した特徴量とデータベース（第1の端末10から送信される情報を記憶するデータベース）に格納された特徴量を用いた照合（1対N照合；Nは正の整数、以下同じ）を行う。管理サーバは、照合結果（照合により特定された利用者のID）を

第2の端末20に送信する。第2の端末20は、セキュリティチェックを通過した利用者を上記送信されたIDにより管理する。

[0028] 一方、非顔認証設定の第2の端末20は、担当職員が操作する端末として動作する。非顔認証設定の第2の端末20は、担当職員がセキュリティチェックを通過した利用者の情報等を入力する端末として動作する。

[0029] 上記管理サーバの機能はサーバ装置30に実装されていてもよいし、サーバ装置30とは異なる装置に実装されていてもよい。なお、管理サーバにて実行される照合（1対1照合、1対N照合）に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、管理サーバは、照合対象の生体情報（被照合対象の特徴ベクトル）と登録側の生体情報（特徴ベクトル）間のユークリッド距離等を類似度として算出し、当該類似度に対する閾値処理等により上記照合を行う。

[0030] サーバ装置30は、認証システムのスループット、即ち、単位時間あたりの処理件数が最大化されるように後段端末（第2の端末20）の動作モードを切り替える装置である。

[0031] [システムの概略動作]

続いて、図2を参照しつつ、第1の実施形態に係る認証システムの概略動作を説明する。

[0032] 第1の端末10のそれぞれは、自装置にて処理した利用者の数を含む「処理情報」をサーバ装置30に通知する。より具体的には、顔認証設定で動作している第1の端末10は、単位時間（例えば、10分、1時間）に当該設定によりサービスを提供した利用者の数（顔認証処理数）をサーバ装置30に通知する。非顔認証設定で動作している第1の端末10は、単位時間に当該設定によりサービスを提供した利用者の数（非顔認証処理数）をサーバ装置30に通知する。

[0033] サーバ装置30は、第1の端末群（顔認証設定の第1の端末10、非顔認証設定の第1の端末10）から通知される処理情報に基づき、単位時間あたりの顔認証利用率を計算する。具体的には、サーバ装置30は、下記の式（

1) により顔認証利用率を計算する。

[0034] [数 1]

$$\text{顔認証利用率} = \text{顔認証処理総数} / (\text{顔認証処理総数} + \text{非顔認証処理総数}) \\ \dots (1)$$

[0035] 式(1)において、顔認証処理総数は、複数の第1の端末10のうち顔認証機能によりサービスを提供している第1の端末10が単位時間あたりに処理した利用者数(顔認証処理数)の総数である。同様に、非顔認証処理総数は、複数の第1の端末10のうち非顔認証機能によりサービスを提供している第1の端末10が単位時間あたりに処理した利用者数(非顔認証処理数)の総数である。即ち、サーバ装置30は、複数の第1の端末10それぞれから取得した処理情報を集計し、顔認証利用率を計算する。

[0036] サーバ装置30は、計算された顔認証利用率に基づき、第2の端末群(顔認証設定の第2の端末20、非顔認証設定の第2の端末20)に含まれる各端末の動作モード(顔認証設定、非顔認証設定)を決定し、切り替える。

[0037] 具体的には、サーバ装置30は、顔認証利用率が高ければ、顔認証設定にて動作する第2の端末20の数を増やす。あるいは、サーバ装置30は、顔認証利用率が低ければ、顔認証設定にて動作する第2の端末20の数を減らす。

[0038] 例えば、図2において、第1の端末10における手続きを顔認証にて完了した利用者を灰色にて示す。サーバ装置30は、第1の端末10を通過した利用者のうち顔認証を利用した利用者の数が多ければ、第1の端末群に続く第2の端末群でも顔認証の利用が多くなると想定し、顔認証設定の第2の端末20の数を増やす。この場合、極端な例では、顔認証利用率が100%であれば第2の端末群に従来型の手続きに対応した端末が設置されている必要はなく、サーバ装置30は、第2の端末群のすべてを顔認証設定にすることができる。

[0039] 対して、サーバ装置30は、第1の端末群を通過した利用者のうち顔認証を利用した利用者の数が少なければ、第1の端末群に続く第2の端末群でも

顔認証の利用が少ないと想定し、顔認証設定の第2の端末20の数を減らす。この場合、極端な例では、顔認証利用率が0%であれば第2の端末群に顔認証の手続きに対応した端末が設置されている必要はなく、サーバ装置30は、第2の端末群のすべてを非顔認証設定にすることができる。

[0040] なお、利用者の利便性を考慮して、第2の端末群の近傍に、各利用者（顔認証システム利用者、顔認証システム非利用者）が利用可能な端末番号等を案内する掲示板（デジタルサイネージ等）を設置するのが望ましい。あるいは、デジタルサイネージに顔認証機能を実装して利用者の利便性を高めてもよい。例えば、面前の利用者が顔認証システムの利用者（管理サーバにID登録された利用者）であると判明した場合には、デジタルサイネージは、当該利用者が向かうべき第2の端末20を表示（指示）してもよい。この場合、サーバ装置30は、デジタルサイネージに対し、第2の端末20のそれぞれの動作モードを通知する。

[0041] 続いて、認証システムに含まれる各装置の詳細について説明する。

[0042] [第1の端末]

図3は、第1の実施形態に係る第1の端末10の処理構成の一例を示す図である。図3を参照すると、第1の端末10は、通信制御部201と、端末機能実現部202と、処理情報生成部203と、記憶部204と、を備える。

[0043] 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。具体的には、通信制御部201は、サーバ装置30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30に向けてデータを送信する。

[0044] 端末機能実現部202は、第1の端末10に割り当てられた機能を実現する手段である。具体的には、第1の端末10がチェックイン端末として動作する場合には、端末機能実現部202は、当該チェックインに関する処理を実行する。

[0045] 端末機能実現部202は、顔認証設定で動作する場合には、当該顔認証に

関する処理を実行する。具体的には、端末機能実現部 202 は、面前の利用者の顔画像を取得したり、特徴量を計算したりする。また、端末機能実現部 202 は、非顔認証設定で動作する場合には、担当職員による情報入力を受け付け、当該受け付けた情報を処理する。

[0046] 端末機能実現部 202 は、第 1 の端末 10 に割り当てられる機能に応じて変化するので、当該機能の実現に関するより詳細な説明を省略する。

[0047] 端末機能実現部 202 は、利用者の手続きを処理するたびに処理内容を処理情報生成部 203 に通知する。例えば、端末機能実現部 202 は、利用者のチェックイン手続きが終了すると、その際の動作モード（顔認証設定、非顔認証設定）と共に手続き完了の旨を処理情報生成部 203 に通知する。

[0048] 処理情報生成部 203 は、サーバ装置 30 に通知する「処理情報」を生成する手段である。処理情報生成部 203 は、所定期間ごとに端末機能実現部 202 が利用者の手続きを処理した数をカウントする。処理情報生成部 203 は、上記所定期間が経過するたびにカウントした利用者数を含む「処理情報」をサーバ装置 30 に送信する。より具体的には、処理情報生成部 203 は、端末の設定モード（顔認証設定、非顔認証設定）と利用者の処理数を含む「処理情報」をサーバ装置 30 に送信する。

[0049] 記憶部 204 は、第 1 の端末 10 の動作に必要な情報を記憶する手段である。

[0050] [第 2 の端末]

複数の第 2 の端末 20 は、少なくとも 1 以上の第 1 の端末 10 の後段に設置された端末である。つまり、第 2 の端末 20 は、第 1 の端末 10 による手続き（サービス）が終了した利用者を対象にしてサービスを提供する端末である。

[0051] 図 4 は、第 1 の実施形態に係る第 2 の端末 20 の処理構成の一例を示す図である。図 4 を参照すると、第 2 の端末 20 は、通信制御部 301 と、端末機能実現部 302 と、動作モード切り替え部 303 と、記憶部 304 と、を備える。

[0052] 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。具体的には、通信制御部 301 は、サーバ装置 30 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 30 に向けてデータを送信する。

[0053] 端末機能実現部 302 は、第 2 の端末 20 に割り当てられた機能を実現する手段である。具体的には、第 2 の端末 20 がセキュリティチェックに関する端末として動作する場合には、端末機能実現部 302 は当該セキュリティチェックに関する処理を実行する。なお、端末機能実現部 302 は、第 1 の端末 10 の端末機能実現部 202 と同様に、第 2 の端末 20 に割り当てられる機能に応じて変化するので、当該機能の実現に関するより詳細な説明を省略する。

[0054] 動作モード切り替え部 303 は、サーバ装置 30 から受信する「設定切り替え通知」に従い、端末機能実現部 302 の動作モードを切り替える手段である。動作モード切り替え部 303 は、サーバ装置 30 から「顔認証設定」が通知された場合には、端末機能実現部 302 に「顔認証設定」で動作するように指示する。同様に、動作モード切り替え部 303 は、サーバ装置 30 から「非顔認証設定」が通知された場合には、端末機能実現部 302 に「非顔認証設定」で動作するように指示する。

[0055] 記憶部 304 は、第 2 の端末 20 の動作に必要な情報を記憶する手段である。

[0056] なお、第 1 の端末 10 の動作モード設定は任意の方法で行うことができる。例えば、管理者等が、第 1 の端末 10 の設定メニューを変更して動作モードを入力してもよい。あるいは、サーバ装置 30 が第 1 の端末 10 に動作モードを通知してもよい。

[0057] [サーバ装置]

図 5 は、第 1 の実施形態に係るサーバ装置 30 の処理構成の一例を示す図である。図 5 を参照すると、サーバ装置 30 は、通信制御部 401 と、顔認証利用率計算部 402 と、動作モード決定部 403 と、記憶部 404 と、を

備える。

- [0058] 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。具体的には、通信制御部401は、第1の端末10、第2の端末20からデータ（パケット）を受信する。また、通信制御部401は、第1の端末10、第2の端末20に向けてデータを送信する。
- [0059] 顔認証利用率計算部402は、顔認証利用率を計算する手段である。顔認証利用率計算部402は、複数の第1の端末10それぞれから送信されてくる処理情報を集計し、単位時間あたりの顔認証利用率を計算する。具体的には、顔認証利用率計算部402は、第1の端末10から送信されてくる処理情報の動作モードに基づき、各端末の処理数を「顔認証処理数」、「非顔認証処理数」のいずれかに分類する。
- [0060] その後、顔認証利用率計算部402は、各端末の処理数を動作モードごとに加算し、顔認証処理総数、非顔認証処理総数を計算し、これらの計算された総数を上述の式（1）に当てはめ顔認証利用率を計算する。顔認証利用率計算部402は、当該計算された顔認証利用率を動作モード決定部403に引き渡す。
- [0061] 動作モード決定部403は、上記計算された顔認証利用率に基づき第2の端末20の動作モードを決定する手段である。具体的には、動作モード決定部403は、複数の第2の端末20のうち少なくとも1台以上の端末の動作モードを決定する。例えば、動作モード決定部403は、顔認証利用率が高ければ顔認証設定で動作する第2の端末20の数が多くなるように第2の端末20の動作モードを決定する。対して、動作モード決定部403は、顔認証利用率が低ければ非顔認証設定で動作する第2の端末20の数が多くなるように第2の端末20の動作モードを決定する。
- [0062] 例えば、動作モード決定部403は、顔認証利用率と顔認証設定で動作させる第2の端末20の数を対応付けたテーブル情報を参照して、第2の端末20の動作モードを決定する。例えば、動作モード決定部403は、図6に示すようなテーブル情報を参照し、顔認証利用率に応じて顔認証設定で動作

する第2の端末20の数を決定する。図6の例では、顔認証利用率が90%以上であれば、顔認証設定で動作する第2の端末20の台数はA1台に設定される。なお、図6の例において、 $A1 > A2 > A3$ とする。

[0063] 動作モード決定部403は、顔認証利用率に従い顔認証設定で動作する第2の端末20の数を決定すると、動作モードを変更する第2の端末20を決定する。具体的には、動作モード決定部403は、顔認証設定で動作する第2の端末20の台数を増やす場合には、非顔認証設定で動作している第2の端末20から増加分（変更分）の台数を選択する。動作モード決定部403は、当該選択された第2の端末20に対して動作モードの変更指示を行う。上記の例では、動作モード決定部403は、選択された第2の端末20に対して顔認証設定で動作するように設定切り替え通知を送信する。

[0064] このように、顔認証利用率計算部402は、少なくとも1以上の第1の端末10における顔認証機能の利用率を計算する。さらに、動作モード決定部403は、当該計算された利用率に基づき複数の第2の端末20のうち顔認証機能によりサービスを提供する端末の台数を決定する。より詳細には、動作モード決定部403は、顔認証利用率に基づき、複数の第2の端末20のうち顔認証機能と非顔認証機能の切り替えが必要な端末を選択し、当該選択された第2の端末20に対して設定切り替え通知を送信する。

[0065] [システムの動作]

続いて、第1の実施形態に係る認証システムの動作について説明する。図7は、第1の実施形態に係る認証システムの動作の一例を示すシーケンス図である。

[0066] 第1の端末10は、単位時間あたりの利用者処理数（顔認証により処理した利用者の数、従来型の処理により処理した利用者の数）を含む処理情報を生成する（ステップS01）。

[0067] 第1の端末10は、生成した処理情報をサーバ装置30に送信する（ステップS02）。

[0068] このように、複数の第1の端末10のそれぞれは、単位時間あたりに顔認

証機能によりサービスを提供した利用者の数、又は、非顔認証機能によりサービスを提供した利用者の数を含む処理情報を生成する。また、複数の第1の端末10のそれぞれは、処理情報をサーバ装置30に送信する。

[0069] サーバ装置30は、第1の端末10から取得した処理情報を集計し、単位時間あたりに処理された顔認証利用者の総数（顔認証処理総数）、非顔認証利用者の総数（非顔認証処理総数）を計算する。サーバ装置30は、これらの総数を用いて顔認証利用率を計算する（ステップS03）。

[0070] サーバ装置30は、顔認証利用率に基づき、第2の端末20の動作モードを決定する（ステップS04）。具体的には、サーバ装置30は、顔認証利用率が高ければ顔認証設定で動作する第2の端末20の数を多くする。

[0071] サーバ装置30は、動作モードの切り替え対象となる第2の端末20に対して設定切り替え通知を送信する（ステップS05）。

[0072] 設定切り替え通知を受信すると、第2の端末20は、当該通知に従い自装置の設定（顔認証設定、従来型処理設定）を切り替える（ステップS06）。

[0073] 以上のように、第1の実施形態に係る認証システムでは、サーバ装置30が、第1の端末10における顔認証の利用状況を把握する。サーバ装置30は、当該把握した顔認証の利用状況に応じて第2の端末群（複数の第2の端末20）に属する第2の端末20の動作モードを決定する。具体的には、サーバ装置30は、顔認証が多く利用されている状況では顔認証設定によりサービスを提供する第2の端末20の数を多くする。対して、サーバ装置30は、顔認証の利用状況が低調であれば顔認証設定によりサービスを提供する第2の端末20の数を少なくする。即ち、サーバ装置30は、システムの上流に位置する前段端末（第1の端末10）における顔認証（生体認証）の利用状況に応じてシステムの下流に位置する後段端末（第2の端末20）における動作モード（生体認証を有効、生体認証を無効）を動的に切り替える。時間帯や季節等に応じてシステム利用者の属性（顔認証利用者、非利用者）の割合が大きく変化したとしても、上記切り替えにより後段端末の動作モー

ドが最適化されシステムのスループットを上昇させることができる。システムのスループットが上昇する結果、認証システムの利便性が向上する。

[0074] [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。

[0075] 第1の実施形態では、第1の端末10から通知される「処理情報」に基づき第2の端末20の動作モードを決定することを説明した。第2の実施形態では、フィールドに設置されたカメラ装置から得られる情報に基づき第2の端末20の動作モードを決定することを説明する。

[0076] 図8は、第2の実施形態に係る認証システムの概略構成の一例を示す図である。図8を参照すると、認証システムには、カメラ装置40-1~40-K（Kは正の整数、以下同じ）と、第2の端末20と、サーバ装置30と、が含まれる。

[0077] カメラ装置40は、フィールド内（例えば、空港内）の各所に設置される。カメラ装置40は、サーバ装置30と有線又は無線の通信手段により通信可能に構成されている。

[0078] カメラ装置40のそれぞれは、フィールド内を撮像した画像をサーバ装置30に送信する。サーバ装置30は、取得したフィールド画像を解析し、当該解析の結果に基づき第2の端末20の動作モードを切り替える。

[0079] 例えば、サーバ装置30は、フィールド内に不審者（図8において灰色にて図示した人物）を発見した場合、第2の端末20の動作モードを非顔認証設定に切り替える。サーバ装置30は、不審者を発見した場合には、第2の端末20が自動で動作（無人で動作）するのではなく、職員等の操作が必要な非顔認証設定に切り替える。このような切り替えにより、フィールド内（空港内）のセキュリティ強化を実現する。即ち、サーバ装置30は、非顔認証設定で動作する第2の端末20を増やす（あるいは、全ての第2の端末20を非顔認証設定とする）ことで、フィールド内の監視体制を強化する。

[0080] あるいは、サーバ装置30は、フィールド画像を解析することで身体障害者や妊婦等、職員のサポートが必要な人物を発見した場合に第2の端末20

の動作モードを非顔認証設定に切り替えてもよい。即ち、サーバ装置30は、身体障害者等を発見した場合には、非顔認証設定で動作する第2の端末20の数を増加させてもよい。

[0081] あるいは、サーバ装置30は、フィールド画像を解析することで各手続きエリア（例えば空港の場合、保安検査エリアや搭乗エリア）の混雑状況を算出し、算出した混雑状況に基づいて第2の端末20の動作モードを切り替えてもよい。

[0082] 続いて、第2の実施形態に係る認証システムに含まれるサーバ装置30の詳細について説明する。なお、カメラ装置40には、汎用のWeb（ウェブ）カメラ等を用いることができる。また、第2の端末20に関しては第1の実施形態にて説明した構成、機能と同一とすることができる。そのため、これらの装置に関する詳細な説明を省略する。

[0083] [サーバ装置]

図9は、第2の実施形態に係るサーバ装置30の処理構成（処理モジュール）の一例を示す図である。図9を参照すると、サーバ装置30は、通信制御部401と、動作モード決定部403と、記憶部404と、画像解析部405と、を備える。

[0084] 図5及び図9を比較すると、第2の実施形態では、顔認証利用率計算部402に変えて画像解析部405が追加されている。

[0085] 画像解析部405は、カメラ装置40から取得したフィールド画像を解析し、その結果を動作モード決定部403に通知する手段である。

[0086] 例えば、画像解析部405は、フィールド内に不審者が存在するか否かに関する解析を実行する。この場合、画像解析部405は、取得したフィールド画像から人物の抽出を行い、当該抽出した人物の顔領域を抽出する。画像解析部405は、抽出した顔領域（顔画像）から特徴量（複数の特徴量からなる特徴ベクトル）を算出する。画像解析部405は、当該算出した特徴量と予め格納されたリスト（不審者の特徴量が記載されたブラックリスト）の特徴量を比較し、算出した特徴量がブラックリストに登録されているか否か

を確認する。

- [0087] 画像解析部405は、フィールド画像から算出した特徴量（フィールド内を移動する人物の特徴量）がブラックリストに登録されていれば、不審者が存在する旨を「画像解析結果」として動作モード決定部403に通知する。あるいは、画像解析部405は、複数の不審者を確認した場合には、不審者の数を「画像解析結果」として動作モード決定部403に通知してもよい。
- [0088] 画像解析部405は、例えば、身体障害者や妊婦がフィールド内に存在するか否かに関する解析を実行してもよい。この場合、画像解析部405は、フィールド画像から人物の全身画像を抽出する。具体的には、画像解析部405は、フィールド画像から人物の全身を含む領域（全身領域）を検出する。その後、画像解析部405は、検出された全身領域をフィールド画像から切り出すことにより、全身画像を抽出する。
- [0089] 画像解析部405は、当該抽出した全身画像と予め用意されたテンプレートと比較して身体障害者等の検出を行う。あるいは、画像解析部405は、機械学習により生成された学習モデルを用いて身体障害者等の検出を行ってもよい。例えば、ラベルが付与された身体障害者等の画像を教師データとして多数用意し、当該教師データを用いて学習モデルが生成される。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。
- [0090] 画像解析部405は、フィールド内に身体障害者等を検出した場合には、その旨を「画像解析結果」として動作モード決定部403に通知する。あるいは、画像解析部405は、複数の身体障害者等を検出した場合には、その数を「画像解析結果」として動作モード決定部403に通知してもよい。
- [0091] 動作モード決定部403は、画像解析部405から取得した画像解析結果に基づき、第2の端末20における動作モードを切り替える手段である。
- [0092] 例えば、動作モード決定部403は、フィールド内に不審者や身体障害者

等が存在していれば、非顔認証設定で動作する第2の端末20の数を増やす。あるいは、動作モード決定部403は、全ての第2の端末20の動作モードを非顔認証設定としてもよい。

[0093] あるいは、動作モード決定部403は、不審者や身体障害者等の数に応じて第2の端末20の動作モードを決定してもよい。例えば、動作モード決定部403は、不審者等の数が増加するに従い非顔認証設定で動作する第2の端末20の数を増加させてもよい。

[0094] 以上のように、第2の実施形態に係る認証システムでは、カメラ装置40から取得したフィールド画像を解析することで空港内のセキュリティを強化したり、身体障害者等に適したサービスを提供したりすることができる。

[0095] 続いて、認証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10は、サーバ装置30のハードウェア構成の一例を示す図である。

[0096] サーバ装置30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10に例示する構成を備える。例えば、サーバ装置30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。

[0097] 但し、図10に示す構成は、サーバ装置30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30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30に含まれるプロセッサ311等の数も図10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30に含まれていてもよい。

[0098] 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。

[0099] 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。

[0100] 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。

[0101] 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。

[0102] サーバ装置30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。

[0103] なお、第1の端末10、第2の端末20もサーバ装置30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30と相違する点はないので説明を省略する。第1の端末10、第2の端末20は、必要に応じてカメラ装置（カメラモジュール）等を備えていればよい。

[0104] [変形例]

なお、上記実施形態にて説明した認証システムの構成、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。

[0105] 例えば、第1の実施形態では、認証システムに複数の第1の端末10が含まれる場合を例にとり説明を行ったが、認証システムには1台以上の第1の端末10が含まれていればよい。認証システムに1台の第1の端末10が含まれる場合には、当該第1の端末10はハイブリッド型の端末とすればよい。つまり、当該第1の端末10は、設定変更を必要とせず、顔認証機能によるサービス提供と非顔認証機能によるサービス提供の両方が可能に構成されている。第1の端末10は、単位時間における顔認証処理数、非顔認証処理数を計算し、サーバ装置30に報告する。サーバ装置30は、これらの処理数を用いて顔認証利用率を計算すればよい。

[0106] 上記実施形態では、利用者の生体情報として「顔、顔画像」を用いる場合について説明したが、本願開示にて利用可能な生体情報は「顔」に限定されない。本願開示では、虹彩等の他の生体情報を利用することができる。

[0107] 第1の実施形態では、前段端末（第1の端末10）における顔認証の利用状況を把握するための指標として顔認証利用率を用いる場合について説明したが他の指標により上記利用状況の把握が行われてもよい。例えば、第1の端末10における非顔認証利用率（従来型の手続きによりサービスが提供された利用者の割合）が計算されてもよい。顔認証利用率と非顔認証利用率は表裏一体の関係にあるので、非顔認証利用率は実質的に顔認証利用率と捉えることができる。

[0108] 第1の実施形態では、第2の端末20を後段の端末として説明したがシステム構成によっては第2の端末20が前段の端末として動作する場合もあり得る。この場合、第2の端末20に第1の端末10の機能が含まれていればよい。つまり、第2の端末20に、「処理情報生成部203」に相当する処理モジュールを実装し、第2の端末20から処理情報をサーバ装置30に送信する。サーバ装置30は、第2の端末20から送信される処理情報に基づ

き顔認証利用率（第2の端末20における顔認証の利用状況）を計算し、その後段端末の動作モードを決定すればよい。

- [0109] 上記実施形態では、顔認証設定又は非顔認証設定によりサービスを提供する端末を例にとり説明を行ったが、端末は、上記2つの設定に加え、顔認証及び非顔認証の両方でサービスを提供するハイブリット端末の設定が可能であってもよい。即ち、第1の実施形態における第1の端末10、第2の端末20、第2の実施形態における第2の端末20は、顔認証設定、非顔認証設定、ハイブリット設定の3つの動作モードが切り替え可能であってもよい。
- [0110] 第1の実施形態では、図6に示すようなテーブル情報により顔認証設定で動作する第2の端末20の台数を決定する場合について説明したが、当該台数の決定は所定の関数等を用いて決定されてもよい。例えば、顔認証利用率を入力、顔認証設定で動作する第2の端末20の台数を出力とする関数を予め定義し、当該関数を用いて顔認証設定で動作する第2の端末20の台数が決定されてもよい。
- [0111] あるいは、顔認証利用率ごとの最適な顔認証設定で動作する第2の端末20の台数を予め教師データとして用意し、当該教師データを用いて構築された学習モデルを用いて顔認証設定で動作する第2の端末20の台数が算出されてもよい。上記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。
- [0112] サーバ装置30は、第1の端末群における顔認証利用率に基づき、第1の端末群の設定を変更してもよい。
- [0113] コンピュータの記憶部に端末動作決定プログラムをインストールすることにより、コンピュータをサーバ装置30として機能させることができる。また、端末動作決定プログラムをコンピュータに実行させることにより、コンピュータにより端末動作決定方法を実行することができる。
- [0114] 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。

[0115] 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。

[0116] 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、空港内の認証システムなどに好適に適用可能である。

[0117] 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]

生体認証機能又は非生体認証機能によりサービスの提供が可能な少なくとも 1 以上の第 1 の端末（10、101）と、

それぞれが、生体認証機能と非生体認証機能の切り替えが可能であって、生体認証機能又は非生体認証機能によりサービスの提供が可能な、複数の第 2 の端末（20、102）と、

前記少なくとも 1 以上の第 1 の端末（10、101）及び前記複数の第 2 の端末（20、102）と接続されたサーバ装置（30、103）と、

を含み、

前記サーバ装置（30、103）は、

前記少なくとも 1 以上の第 1 の端末（10、101）における生体認証機能の利用率を計算し、

前記計算された利用率に基づき前記複数の第 2 の端末（20、102）の

うち少なくとも1台以上の端末の動作モードを決定する、認証システム。

[付記2]

前記サーバ装置(30、103)は、前記複数の第2の端末(20、102)のうち生体認証機能によりサービスを提供する端末の台数を決定する、請求項1に記載の認証システム。

[付記3]

前記サーバ装置(30、103)は、
前記利用率に基づき、前記複数の第2の端末(20、102)のうち生体認証機能と非生体認証機能の切り替えが必要な端末を選択し、前記選択された第2の端末(20、102)に対して設定切り替え通知を送信する、付記1又は2に記載の認証システム。

[付記4]

複数の前記第1の端末(10、101)が含まれ、
前記複数の第1の端末(10、101)のそれぞれは、単位時間あたりに生体認証機能によりサービスを提供した利用者の数、又は、非生体認証機能によりサービスを提供した利用者の数を含む処理情報を生成する、付記1乃至3のいずれかに記載の認証システム。

[付記5]

前記複数の第1の端末(10、101)のそれぞれは、前記処理情報を前記サーバ装置(30、103)に送信する、付記4に記載の認証システム。

[付記6]

前記サーバ装置(30、103)は、前記複数の第1の端末(10、101)それぞれから取得した処理情報を集計し、前記利用率を計算する、付記5に記載の認証システム。

[付記7]

前記サーバ装置(30、103)は、前記複数の第1の端末(10、101)のうち生体認証機能によりサービスを提供している第1の端末(10、101)が単位時間あたりに処理した利用者数の総数と、前記複数の第1の

端末（１０、１０１）のうち非生体認証機能によりサービスを提供している第１の端末（１０、１０１）が単位時間あたりに処理した利用者数の総数と、に基づき前記利用率を計算する、付記６に記載の認証システム。

[付記８]

前記サーバ装置（３０、１０３）は、前記生体認証機能によりサービスを提供した利用者数の総数を、前記生体認証機能によりサービスを提供した利用者数の総数と前記非生体認証機能によりサービスを提供した利用者の総数の和で除算することで前記利用率を計算する、付記７に記載の認証システム。

[付記９]

前記複数の第２の端末（２０、１０２）は、前記少なくとも１以上の第１の端末（１０、１０１）の後段に設置された端末である、付記１乃至８のいずれか一に記載の認証システム。

[付記１０]

前記少なくとも１以上の第１の端末（１０、１０１）は、チェックイン手続きに関する処理を実行する端末である、付記１乃至９のいずれか一に記載の認証システム。

[付記１１]

前記複数の第２の端末（２０、１０２）は、セキュリティチェックに関する処理を実行する端末である、付記１乃至１０のいずれか一に記載の認証システム。

[付記１２]

生体認証機能又は非生体認証機能によりサービスの提供が可能な少なくとも１以上の第１の端末（１０、１０１）と、

それぞれが、生体認証機能と非生体認証機能の切り替えが可能であって、生体認証機能又は非生体認証機能によりサービスの提供が可能な、複数の第２の端末（２０、１０２）と、

前記少なくとも１以上の第１の端末（１０、１０１）及び前記複数の第２

の端末（２０、１０２）と接続されたサーバ装置（３０、１０３）と、
を含む認証システムにおいて、
前記少なくとも１以上の第１の端末（１０、１０１）における生体認証機能の利用率を計算し、
前記計算された利用率に基づき前記複数の第２の端末（２０、１０２）のうち少なくとも１台以上の端末の動作モードを決定する方法。

[付記１３]

生体認証機能又は非生体認証機能によりサービスの提供が可能な少なくとも１以上の第１の端末（１０、１０１）と、

それぞれが、生体認証機能と非生体認証機能の切り替えが可能であって、生体認証機能又は非生体認証機能によりサービスの提供が可能な、複数の第２の端末（２０、１０２）と、

前記少なくとも１以上の第１の端末（１０、１０１）及び前記複数の第２の端末（２０、１０２）と接続されたサーバ装置（３０、１０３）に搭載されたコンピュータ（３１１）に、

前記少なくとも１以上の第１の端末（１０、１０１）における生体認証機能の利用率を計算する処理と、

前記計算された利用率に基づき前記複数の第２の端末（２０、１０２）のうち少なくとも１台以上の端末の動作モードを決定する処理と、

を実行させるためのプログラムを記録する、コンピュータ読取可能な記録媒体。

なお、付記１２の形態及び付記１３の形態は、付記１の形態と同様に、付記２の形態～付記１１の形態に展開することが可能である。

[0118] 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

- [0119] 10、10-1～10-3、101 第1の端末
20、20-1～20-3、102 第2の端末
30、103 サーバ装置
40、40-1～40-K カメラ装置
201、301、401 通信制御部
202、302 端末機能実現部
203 処理情報生成部
204、304、404 記憶部
303 動作モード切り替え部
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 顔認証利用率計算部
403 動作モード決定部
405 画像解析部