(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2021-131855
(P2021-131855A)
(43)公開日　令和3年9月9日(2021.9.9)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/32	(2013.01)	G06F	21/32	
G06F 21/31	(2013.01)	G06F	21/31	

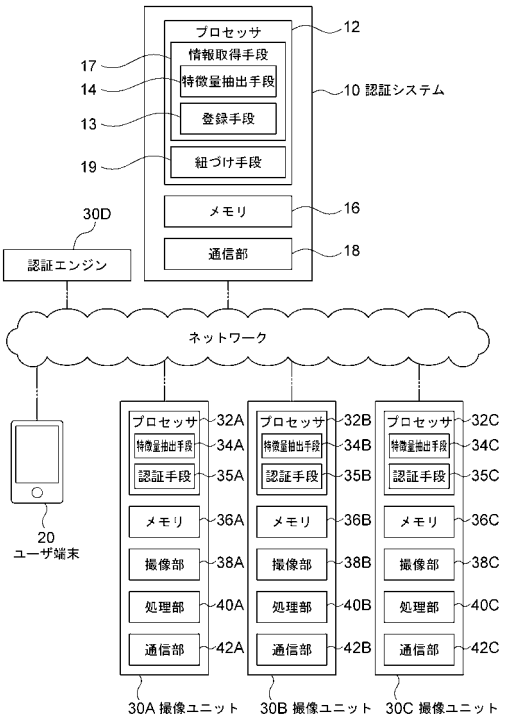
審査請求 有　請求項の数 8　ＯＬ　（全 40 頁）

(21)出願番号　特願2021-15335(P2021-15335)
(22)出願日　令和3年2月2日(2021.2.2)
(62)分割の表示　特願2020-102335(P2020-102335)の分割
原出願日　令和2年6月12日(2020.6.12)
(31)優先権主張番号　特願2020-25377(P2020-25377)
(32)優先日　令和2年2月18日(2020.2.18)
(33)優先権主張国・地域又は機関　日本国(JP)

(71)出願人　520318074
ＤＸＹＺ株式会社
東京都新宿区西新宿６－５－１新宿アイランドタワー４１階
(74)代理人　100131842
弁理士　加島　広基
(72)発明者　中西　聖
東京都新宿区西新宿６－５－１新宿アイランドタワー４１階　ＤＸＹＺ株式会社内
(72)発明者　新宮　由久
東京都新宿区西新宿６－５－１新宿アイランドタワー４１階　ＤＸＹＺ株式会社内

(54)【発明の名称】認証システムおよび情報処理方法

(57)【要約】
【課題】登録された顔画像のデータを、顔認証以外の認証を行う認証エンジンで使用することにより利便性を向上させることができる認証システムおよび情報処理方法を提供する。
【解決手段】ユーザ端末２０から受け付けた情報を用いてユーザの認証を行う認証システム１０は、ユーザ登録時に、ユーザの顔画像データをユーザ端末２０から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をユーザの識別情報としてメモリ１６に記憶させる情報取得手段１７と、顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、メモリ１６に記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段１９とを備えている。
【選択図】図１



【特許請求の範囲】
【請求項１】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる情報取得手段と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う認証手段と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段と、
を備えた、認証システム。
【請求項２】
前記認証手段によりユーザの認証を行う際に、ユーザの顔画像の特徴量と、ユーザの顔画像の特徴量以外の要素とを用いることにより二要素認証を行う、請求項１記載の認証システム。
【請求項３】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる情報取得手段と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像の特徴量に係る情報を各サービス機関の撮像ユニットに送信する送信手段と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段と、
を備えた、認証システム。
【請求項４】
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報は、ユーザが所持するユーザ端末の識別情報、ユーザの顔以外の生体情報から得られる情報、ユーザによりユーザ端末に入力されたコードまたはパスワードからなる群のうち少なくとも何れかを含む、請求項１乃至３のいずれか一項に記載の認証システム。
【請求項５】
サービス機関の認証エンジンの追加を行う旨の指示をユーザ端末から受け付けると、前記紐づけ手段は、追加されたサービス機関の認証エンジンの認証で用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける、請求項１乃至４のいずれか一項に記載の認証システム。
【請求項６】
前記紐づけ手段によるユーザの識別情報の紐づけが行われた後でも、各サービス機関の認証エンジンで用いられるユーザの識別情報はそのまま残される、請求項１乃至５のいずれか一項に記載の認証システム。
【請求項７】
前記情報取得手段は、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出する際に、受け付けたユーザの顔画像データからハッシュ関数により求めたハッシュ値を、このユーザの顔画像の特徴量として抽出する、請求項１乃至６のいずれか一項に記載の認証システム。
【請求項８】

ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる情報取得手段と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う認証手段と、
を備え、
前記認証手段によりユーザの認証を行う際に、ユーザの顔画像の特徴量と、ユーザの顔画像の特徴量以外の要素とを用いることにより二要素認証を行う、認証システム。
【請求項９】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる情報取得手段と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データと、前記メモリに記憶されているユーザの顔画像データとを比較することによってユーザの認証を行う認証手段と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける紐づけ手段と、
を備えた、認証システム。
【請求項１０】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる情報取得手段と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像データを各サービス機関の撮像ユニットに送信する送信手段と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける紐づけ手段と、
を備えた、認証システム。
【請求項１１】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる工程と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける工程と、
を備えた、情報処理方法。
【請求項１２】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、

ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる工程と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像の特徴量に係る情報を各サービス機関の撮像ユニットに送信する工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける工程と、
を備えた、情報処理方法。
【請求項１３】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる工程と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う工程と、
を備え、
前記認証手段によりユーザの認証を行う際に、ユーザの顔画像の特徴量と、ユーザの顔画像の特徴量以外の要素とを用いることにより二要素認証を行う、情報処理方法。
【請求項１４】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる工程と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データと、前記メモリに記憶されているユーザの顔画像データとを比較することによってユーザの認証を行う工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける工程と、
を備えた、情報処理方法。
【請求項１５】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる工程と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像データを各サービス機関の撮像ユニットに送信する工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける工程と、
を備えた、情報処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、認証システムおよび情報処理方法に関する。
【背景技術】
【０００２】
従来、顔データに基づいて認証を行う認証システムとして、入力された入力顔データと、予め登録された登録顔データとを照合して本人認証を行う認証システムが知られている（例えば、特許文献１、２参照）。
【０００３】
特許文献１に記載された認証システムでは、カメラにより撮像された撮像画像中の顔部分の画像を用いて対象人物を認証する。また、特許文献２に記載された認証システムでは、例えば登録される顔画像が４つの場合、２つを精度保証用の顔パターンとし、１つを外乱成分吸収用の顔パターンとし、１つを更新対象用の顔パターンとしている。そして、新たに顔パターンを登録するときには、事前に登録されている４つの顔パターンのうち、新たに登録される顔パターンとの類似度が２番目に低い更新対象用の顔パターンを削除する。すなわち、新たに登録される顔パターンとの類似度が一番低い外乱成分吸収用の顔パターンを残すことにより、環境のばらつきに順応して顔認証を行う。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１９－１９７４２６号公報
【特許文献２】特開２００６－７２５４０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
特許文献１、２に開示される認証システムでは、登録された顔画像のデータを、顔認証以外の認証を行う認証エンジンで使用することができないため不便であるという問題があった。
【０００６】
本発明は、このような点を考慮してなされたものであり、登録された顔画像のデータを、顔認証以外の認証を行う認証エンジンで使用することにより利便性を向上させることができる認証システムおよび情報処理方法を提供することを目的とする。
【課題を解決するための手段】
【０００７】
本発明の認証システムは、ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる情報取得手段と、ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う認証手段と、顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段と、を備えたことを特徴とする。
【０００８】
本発明の認証システムは、ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる情報取得手段と、各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像の特徴量に係る情報を各サービス機関の撮像

ユニットに送信する送信手段と、顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段と、を備えたことを特徴とする。

【０００９】

本発明の認証システムは、ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる情報取得手段と、ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う認証手段と、を備え、前記認証手段によりユーザの認証を行う際に、ユーザの顔画像の特徴量と、ユーザの顔画像の特徴量以外の要素とを用いることにより二要素認証を行うことを特徴とする。

【００１０】

本発明の認証システムは、ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる情報取得手段と、ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データと、前記メモリに記憶されているユーザの顔画像データとを比較することによってユーザの認証を行う認証手段と、顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける紐づけ手段と、を備えたことを特徴とする。

【００１１】

本発明の認証システムは、ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる情報取得手段と、各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像データを各サービス機関の撮像ユニットに送信する送信手段と、顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける紐づけ手段と、を備えたことを特徴とする。

【００１２】

本発明の情報処理方法は、ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる工程と、ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う工程と、顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける工程と、を備えたことを特徴とする。

【００１３】

本発明の情報処理方法は、ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる工程と、各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせる

ために、前記メモリに記憶されている、ユーザの顔画像の特徴量に係る情報を各サービス機関の撮像ユニットに送信する工程と、顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける工程と、を備えたことを特徴とする。

【００１４】

本発明の情報処理方法は、ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる工程と、ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う工程と、を備え、前記認証手段によりユーザの認証を行う際に、ユーザの顔画像の特徴量と、ユーザの顔画像の特徴量以外の要素とを用いることにより二要素認証を行うことを特徴とする。

【００１５】

本発明の情報処理方法は、ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる工程と、ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データと、前記メモリに記憶されているユーザの顔画像データとを比較することによってユーザの認証を行う工程と、顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける工程と、を備えたことを特徴とする。

【００１６】

本発明の情報処理方法は、ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる工程と、各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像データを各サービス機関の撮像ユニットに送信する工程と、顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける工程と、を備えたことを特徴とする。

【発明の効果】

【００１７】

本発明の認証システムおよび情報処理方法によれば、登録された顔画像のデータを、顔認証以外の認証を行う認証エンジンで使用することにより利便性を向上させることができる。

【図面の簡単な説明】

【００１８】

【図１】本発明の実施の形態による認証システムおよび各サービス機関に配置される撮像ユニットの一例を概略的に示す図である。

【図２】図１に示す認証システムによりユーザの顔画像の登録を行う際に実行される処理内容を示すフローチャートである。

【図３】図１に示す認証システムおよび撮像ユニットによりユーザの認証を行う際に実行される処理内容の一例を示すフローチャートである。

【図４】本発明の実施の形態による認証システムおよび各サービス機関に配置される撮像ユニットの他の例を概略的に示す図である。

【図５】図４に示す認証システムによりユーザの顔画像の登録を行う際に実行される処理内容を示すフローチャートである。

【図６】図４に示す認証システムおよび撮像ユニットによりユーザの認証を行う際に実行される処理内容の一例を示すフローチャートである。
【図７】本発明の実施の形態による認証システムおよび各サービス機関に配置される撮像ユニットの更に他の例を概略的に示す図である。
【図８】図７に示す認証システムによりユーザの顔画像の登録を行う際に実行される処理内容を示すフローチャートである。
【図９】図７に示す認証システムおよび撮像ユニットによりユーザの認証を行う際に実行される処理内容の一例を示すフローチャートである。
【図１０】ユーザ端末に表示される初期画面を示す図である。
【図１１】ユーザ端末に表示される登録画面を示す図である。
【図１２】ユーザ端末に表示される登録画面を示す図である。
【図１３】ユーザ端末に表示されるサービス追加画面を示す図である。
【図１４】ユーザ端末に表示される認証履歴の画面を示す図である。
【図１５】ユーザ端末に表示される認証履歴の詳細画面を示す図である。
【図１６】本発明の実施の形態による認証システムおよび各会社に配置される撮像ユニットの更に他の例を概略的に示す図である。
【図１７】本発明の実施の形態による認証システムおよび各会社に配置される撮像ユニットの更に他の例を概略的に示す図である。
【発明を実施するための形態】
【００１９】
以下、図面を参照して本発明の実施の形態について説明する。図１乃至図１５は、本実施の形態に係る認証システムおよび各サービス機関に配置される撮像ユニットを示す図である。
【００２０】
図１に示すように、飲食店、ホテル、交通機関、オフィスビル、集合住宅施設、コンビニエンスストア等の各サービス機関には、ユーザの認証を行う撮像ユニット３０Ａ、３０Ｂ、３０Ｃが配置されている。なお、図１では３つの撮像ユニット３０Ａ、３０Ｂ、３０Ｃが図示されているが、２つまたは４つ以上の撮像ユニットが用いられてもよい。また、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対して、各サービス機関とは別の会社に設置される認証システム１０がインターネット回線等のネットワークを介して通信可能に接続されている。また、ユーザが所持するスマートフォン等のユーザ端末２０は、認証システム１０および各撮像ユニット３０Ａ、３０Ｂ、３０Ｃにインターネット回線等のネットワークを介して通信可能に接続されている。以下、認証システム１０および各撮像ユニット３０Ａ、３０Ｂ、３０Ｃの詳細について説明する。
【００２１】
認証システム１０は例えばコンピュータ等から構成されており、当該認証システム１０は、ＣＰＵ等のプロセッサ１２と、メモリ１６と、通信部１８とを有している。プロセッサ１２は、ユーザ端末２０から受け取った顔画像データに基づいて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量をハッシュ値として抽出する特徴量抽出手段１４と、抽出されたユーザの顔画像の特徴量を登録する登録手段１３とを有している。そして、プロセッサ１２は、メモリ１６に記憶されているプログラムを実行することにより、特徴量抽出手段１４において各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量をハッシュ値として抽出するようになっている。具体的には、特徴量抽出手段１４は、受け付けたユーザの顔画像データから所定のハッシュ関数により求めたハッシュ値を、ユーザの顔画像の特徴量として抽出する。なお、ユーザの顔画像データが同じであっても、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの種類によってユーザの顔画像の特徴量が異なる場合がある。事業会社等のサービス機関が異なると、これらのサービス機関で使用される撮像ユニット３０Ａ、３０Ｂ、３０Ｃの仕様も異なるからである。このため、特徴量抽出手段１４は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎にユーザの顔画像の特徴量を抽出する。すなわち、１つの顔画像データから、各撮像ユニット３０Ａ

、３０Ｂ、３０Ｃに対応する複数のユーザの顔画像の特徴量が抽出される。また、プロセッサ１２は、メモリ１６に記憶されているプログラムを実行することにより、特徴量抽出手段１４により抽出された撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎のユーザの顔画像の特徴量（具体的には、ハッシュ値）を、登録手段１３により、ユーザの識別情報および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けてメモリ１６に記憶させるようになっている。なお、プロセッサ１２により実行されるプログラムはメモリ１６に記憶されているものに限定されることはない。外部装置から認証システム１０に送信されたプログラムや、認証システム１０に着脱自在に装着される記録媒体に記憶されているプログラムをプロセッサ１２が実行することにより、特徴量抽出手段１４および登録手段１３の各々において処理が行われてもよい。また、本実施の形態では、特徴量抽出手段１４および登録手段１３により、情報取得手段１７が構成される。情報取得手段１７は、ユーザ登録時に、ユーザの顔画像データを受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をユーザの識別情報としてメモリ１６に記憶させる。

【００２２】

上述したように、メモリ１６には、特徴量抽出手段１４により抽出されたユーザの顔画像の特徴量（具体的には、ハッシュ値）が、ユーザの識別情報および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けられて記憶されるようになっている。上述したように、特徴量抽出手段１４により抽出されるユーザの顔画像の特徴量は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの種類によって異なる場合がある。このため、特徴量抽出手段１４は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎にユーザの顔画像の特徴量を抽出する。このことにより、特徴量抽出手段１４により抽出されるユーザの顔画像の特徴量も、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに関連付けてメモリ１６に記憶させる必要がある。また、メモリ１６には、ユーザの識別情報と、このユーザにより選択されたサービス機関とが関連付けられて記憶されるようになっている。また、上述したように、メモリ１６は、プロセッサ１２において様々な処理を行わせるためのプログラムを記憶するようになっている。また、プロセッサ１２は、通信部１８によりインターネット回線等のネットワークを介して各サービス機関に配置される撮像ユニット３０Ａ、３０Ｂ、３０Ｃまたはユーザ端末２０と信号の送受信を行うようになっている。

【００２３】

各サービス機関に配置される撮像ユニット３０Ａ、３０Ｂ、３０Ｃの各々は例えばコンピュータ等から構成されており、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃは、ＣＰＵ等のプロセッサ３２Ａ、３２Ｂ、３２Ｃと、メモリ３６Ａ、３６Ｂ、３６Ｃと、撮像部３８Ａ、３８Ｂ、３８Ｃと、処理部４０Ａ、４０Ｂ、４０Ｃと、通信部４２Ａ、４２Ｂ、４２Ｃとを有している。プロセッサ３２Ａ、３２Ｂ、３２Ｃは、撮像部３８Ａ、３８Ｂ、３８Ｃにより撮像されたユーザの顔画像データに基づいてユーザの顔画像の特徴量をハッシュ値として抽出する特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃと、認証手段３５Ａ、３５Ｂ、３５Ｃとを有している。そして、プロセッサ３２Ａ、３２Ｂ、３２Ｃは、メモリ３６Ａ、３６Ｂ、３６Ｃに記憶されているプログラムを実行することにより、特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃにおいてユーザの顔画像の特徴量をハッシュ値として抽出するようになっている。具体的には、特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃは、受け付けたユーザの顔画像データから所定のハッシュ関数により求めたハッシュ値を、ユーザの顔画像の特徴量として抽出する。また、プロセッサ３２Ａ、３２Ｂ、３２Ｃは、メモリ３６Ａ、３６Ｂ、３６Ｃに記憶されているプログラムを実行することにより、認証手段３５Ａ、３５Ｂ、３５Ｃにおいてユーザの認証を行うようになっている。このような処理内容の詳細については後述する。なお、プロセッサ３２Ａ、３２Ｂ、３２Ｃにより実行されるプログラムはメモリ３６Ａ、３６Ｂ、３６Ｃに記憶されているものに限定されることはない。外部装置から撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信されたプログラムや、撮像ユニット３０Ａ、３０Ｂ、３０Ｃに着脱自在に装着される記録媒体に記憶されているプログラムをプロセッサ３２Ａ、３２Ｂ、３２Ｃが実行することにより、特徴量抽出手段３４Ａ、３４Ｂ、

３４Ｃおよび認証手段３５Ａ、３５Ｂ、３５Ｃの各々において様々な処理が行われてもよい。また、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃは、それぞれ、１つのサービス機関に対応するものに限定されない。例えば、撮像ユニット３０Ａが複数のサービス機関に対応するものであってもよい。

【００２４】

また、メモリ３６Ａ、３６Ｂ、３６Ｃは、予め登録されたユーザの識別情報と、このユーザの顔画像の特徴量とを関連付けて記憶するようになっている。また、上述したように、メモリ３６Ａ、３６Ｂ、３６Ｃは、プロセッサ３２Ａ、３２Ｂ、３２Ｃにおいて様々な処理を行わせるためのプログラムを記憶するようになっている。また、撮像部３８Ａ、３８Ｂ、３８Ｃは例えばカメラを有しており、ユーザを撮像することにより当該ユーザの顔画像データを取得するようになっている。

【００２５】

また、処理部４０Ａ、４０Ｂ、４０Ｃは、認証が行われたユーザに対して様々な処理を行うようになっている。例えば、撮像ユニット３０Ａ、３０Ｂ、３０Ｃがオフィスビルや集合住宅施設等に配置されている場合には、処理部４０Ａ、４０Ｂ、４０Ｃは、ユーザの認証が行われた場合に、これらのオフィスビルや集合住宅施設の出入り口等に配置される扉の施錠を解除するようになる。また、撮像ユニット３０Ａ、３０Ｂ、３０Ｃが飲食店、ホテル、交通機関、コンビニエンスストア等に配置されている場合には、これらのサービス機関で料金の支払いを行う際にキャッシュレスによる決済を可能とする。この場合には、撮像ユニット３０Ａ、３０Ｂ、３０Ｃから金融機関やクレジットカード会社のサーバに支払い情報が送信されることにより、ユーザの銀行口座から支払い金額が自動的に引き落とされたりクレジットカードの利用明細に追加されたりするようになる。また、プロセッサ３２Ａ、３２Ｂ、３２Ｃは、通信部４２Ａ、４２Ｂ、４２Ｃによりインターネット回線等のネットワークを介して認証システム１０またはユーザ端末２０と信号の送受信を行うようになっている。

【００２６】

また、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいて、ユーザの顔画像を撮像部３８Ａ、３８Ｂ、３８Ｃにより撮像することによって、このユーザの顔画像の特徴量を各撮像ユニット３０Ａ、３０Ｂ、３０Ｃで登録することができるようになっている。具体的には、ユーザの顔画像の特徴量を各撮像ユニット３０Ａ、３０Ｂ、３０Ｃで登録する際に、ユーザの顔画像が撮像部３８Ａ、３８Ｂ、３８Ｃにより撮像されると、プロセッサ３２Ａ、３２Ｂ、３２Ｃは、撮像部３８Ａ、３８Ｂ、３８Ｃにより撮像されたユーザの顔画像データに基づいて、特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃによりユーザの顔画像の特徴量をハッシュ値として抽出する。そして、この抽出されたユーザの顔画像の特徴量（具体的には、ハッシュ値）がメモリ３６Ａ、３６Ｂ、３６Ｃに記憶される。このようにして、ユーザの顔画像の特徴量が各撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいて登録される。

【００２７】

ユーザ端末２０ではオンラインストア等により顔認証アプリをインストールすることができるようになっている。このような顔認証アプリをインストールすると、ユーザはユーザ端末２０により顔画像データの登録、サービスを利用するサービス機関の登録等を行うことができるようになる。このような顔認証アプリの処理内容については後述する。なお、このような顔認証アプリは認証システム１０から提供されるようになっていてもよく、あるいは認証システム１０とは別のシステムから提供されるようになっていてもよい。

【００２８】

本実施の形態では、認証システム１０および各サービス機関に配置される撮像ユニット３０Ａ、３０Ｂ、３０ＣはＡＰＩ連携（アプリケーション・プログラミング・インターフェース）が行われている。これにより、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃのシステムを、それぞれ独立して構成したものに比べて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃのシステムを容易に構成することができる。

【００２９】

次に、認証システム１０および各撮像ユニット３０Ａ、３０Ｂ、３０Ｃによりユーザの認証を行う際の処理内容について図２、図３および図１０乃至図１２を用いて説明する。

【００３０】

まず、ユーザがユーザ端末２０を用いて顔画像データを認証システム１０に登録する処理について説明する。最初に、ユーザは顔認証アプリをユーザ端末２０にインストールする。このような顔認証アプリの初期画面では図１０に示す画面が表示される。ユーザは、ユーザ端末２０においてこのような顔認証アプリで最初にユーザ登録を行う。具体的には、図１０に示す画面においてアカウントボタンを押すと、図１１に示すようなユーザ登録画面となる。このようなユーザ登録画面において氏名、生年月日、電話番号、メールアドレス、パスワード等の登録情報を入力し、利用規約に同意する欄にチェックを入れた後に登録ボタンを押下すると、図１２に示すような顔画像の撮像画面となる。このような撮像画面でユーザがユーザ端末２０により顔画像を撮像すると、ユーザ登録画面で入力された様々な情報およびユーザの顔画像データがユーザ端末２０から認証システム１０に送信される。このようにして、認証システム１０のプロセッサ１２はユーザ端末２０から顔画像データを受け取る（ＳＴＥＰ１）。また、ユーザ端末２０の識別情報、およびユーザ端末２０に入力されたユーザの氏名、生年月日、電話番号、メールアドレス、パスワード等の登録情報も、認証システム１０のプロセッサ１２はユーザ端末２０から受け取る。また、プロセッサ１２はユーザの識別情報としてユーザＩＤを発行し、この発行されたユーザＩＤをメモリ１６に記憶させる。

【００３１】

次に、認証システム１０のプロセッサ１２は、ユーザ端末２０から受け取った顔画像データに基づいて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応する顔画像の特徴量をハッシュ値として特徴量抽出手段１４により抽出する（ＳＴＥＰ２）。この際に、特徴量抽出手段１４により抽出されるユーザの顔画像の特徴量は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの種類によって異なる場合がある。このため、特徴量抽出手段１４は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎にユーザの顔画像の特徴量を抽出する。また、特徴量抽出手段１４は、ユーザにより予め選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量のみを抽出する。例えば、撮像ユニット３０Ａが設置されるサービス機関についてはユーザが顔画像データを使うことを認めているが、撮像ユニット３０Ｂが設置されるサービス機関についてはユーザが顔画像データを使うことを認めていない場合には、特徴量抽出手段１４は、撮像ユニット３０Ａに対応するユーザの顔画像の特徴量のみを抽出する。なお、上述したように、メモリ１６には、ユーザの識別情報と、このユーザにより選択されたサービス機関とが関連付けられて記憶されるようになっている。そして、プロセッサ１２は、特徴量抽出手段１４により抽出された各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応する顔画像の特徴量を、登録手段１３により認証システム１０のメモリ１６にユーザＩＤ（ユーザの識別情報）および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けて記憶させる（ＳＴＥＰ３）。このようにして、ユーザ端末２０により撮像されたユーザの顔画像の登録が完了する。また、メモリ１６に記憶されたユーザの顔画像の特徴量に係る情報は、認証システム１０から、ユーザにより選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される（ＳＴＥＰ４）。この際に、撮像ユニット３０Ａ、３０Ｂ、３０Ｃには、この撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量が送信される。撮像ユニット３０Ａ、３０Ｂ、３０Ｃは、認証システム１０から送信されたユーザの顔画像の特徴量に係る情報を、ユーザの識別情報に関連付けてメモリ３６Ａ、３６Ｂ、３６Ｃに記憶させる。

【００３２】

次に、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいてユーザの認証を行う処理について説明する。各撮像ユニット３０Ａ、３０Ｂ、３０Ｃが設置されるサービス機関においてユーザの認証が必要となった場合には、まず、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ、３８Ｂ、３８Ｃによりユーザを撮像することによってユーザの顔画像データを取得する（ＳＴＥＰ１１）。また、撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいて、プ

ロセッサ３２Ａ、３２Ｂ、３２Ｃは、取得された顔画像データに基づいて特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃによりユーザの顔画像の特徴量をハッシュ値として抽出する（ＳＴＥＰ１２）。そして、プロセッサ３２Ａ、３２Ｂ、３２Ｃは、特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃにより抽出されたユーザの顔画像の特徴量（具体的には、ハッシュ値）と、メモリ３６Ａ、３６Ｂ、３６Ｃに記憶されているユーザの顔画像の特徴量（具体的には、ハッシュ値）とを比較することによりユーザの認証を行う（ＳＴＥＰ１３）。より詳細に説明すると、特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃにより抽出されたユーザの顔画像の特徴量と、メモリ３６Ａ、３６Ｂ、３６Ｃに記憶されているユーザの顔画像の特徴量との一致率が所定の閾値（例えば、８０％）を超える場合には、認証手段３５Ａ、３５Ｂ、３５Ｃはユーザの認証を行う。なお、上述したように、メモリ３６Ａ、３６Ｂ、３６Ｃには、予め登録されたユーザの識別情報と、このユーザの顔画像の特徴量とが関連付けて記憶されている。

【００３３】

そして、認証手段３５Ａ、３５Ｂ、３５Ｃによりユーザの認証が行われると（ＳＴＥＰ１４の「ＹＥＳ」）、プロセッサ３２Ａ、３２Ｂ、３２Ｃは各処理部４０Ａ、４０Ｂ、４０Ｃによりこの撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するサービスを実施可能とする（ＳＴＥＰ１５）。具体的には、上述したように、撮像ユニット３０Ａ、３０Ｂ、３０Ｃがオフィスビルや集合住宅施設等に配置されている場合には、処理部４０Ａ、４０Ｂ、４０Ｃは、ユーザの認証が行われた場合に、これらのオフィスビルや集合住宅施設の出入り口等に配置される扉の施錠を解除する。また、撮像ユニット３０Ａ、３０Ｂ、３０Ｃが飲食店、ホテル、交通機関、コンビニエンスストア等に配置されている場合には、これらのサービス機関で料金の支払いを行う際にキャッシュレスによる決済を可能とする。なお、キャッシュレスによる決済が行われる場合には、二要素認証が行われるようにしてもよい。その後、撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、サービスの利用状況に係る情報を認証システム１０に送信する（ＳＴＥＰ１７）。このことにより、認証システム１０において各サービス機関におけるサービスの利用状況に係る情報がユーザ毎にメモリ１６に記憶される。

【００３４】

一方、特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃにより抽出されたユーザの顔画像の特徴量が、メモリ３６Ａ、３６Ｂ、３６Ｃに記憶されているユーザの顔画像の特徴量に略一致せず、認証手段３５Ａ、３５Ｂ、３５Ｃによりユーザの認証を行うことができなかった場合には（ＳＴＥＰ１４の「ＮＯ」）、プロセッサ３２Ａ、３２Ｂ、３２Ｃは各処理部４０Ａ、４０Ｂ、４０Ｃによりこの撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するサービスを実施不可とする（ＳＴＥＰ１６）。この場合も、撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、サービスの利用状況に係る情報（具体的には、ユーザが撮像ユニット３０Ａ、３０Ｂ、３０Ｃで認証を行おうとしたが認証されずにサービスを利用できなかったという情報）を認証システム１０に送信する（ＳＴＥＰ１７）。

【００３５】

このような認証方法によれば、ユーザの顔画像の特徴量があるサービス機関の撮像エンジン（例えば、撮像ユニット３０Ａ）で登録されているが、別のサービス機関の撮像エンジン（例えば、撮像ユニット３０Ｂ）で登録されていない場合でも、認証システム１０のメモリ１６および各撮像ユニット３０Ａ、３０Ｂ、３０Ｃのメモリ３６Ａ、３６Ｂ、３６Ｃにこのユーザの顔画像の特徴量を撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けて記憶させておくことにより、ユーザの顔画像の特徴量が登録されていないサービス機関でも撮像部によりユーザの顔画像を撮像することによってユーザの認証を行うことができる。この場合には、複数の撮像ユニットの全てでユーザは顔画像データの登録を行う必要がなくなるので、ユーザの手間を省くことができるようになる。

【００３６】

なお、本実施の形態による認証システム１０や認証方法は図１乃至図３に示すものに限定されることはない。本実施の形態による認証システム１０や認証方法の他の例について

図４乃至図６を用いて説明する。なお、図４に示す認証システム１０や各撮像ユニット３０Ａ、３０Ｂ、３０Ｃについて、図１に示す認証システム１０や各撮像ユニット３０Ａ、３０Ｂ、３０Ｃと同じ構成要素については同じ参照符号を付けてその説明を省略する。

【００３７】

図４に示すように、認証システム１０のプロセッサ１２は、ユーザ端末２０から受け取った顔画像データに基づいて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量をハッシュ値として抽出する特徴量抽出手段１４と、抽出されたユーザの顔画像の特徴量を登録する登録手段１３と、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ～３８Ｃに撮像されたユーザの顔画像の特徴量（具体的には、ハッシュ値）に基づいてユーザの認証を行う認証手段１５とを有している。プロセッサ１２は、メモリ１６に記憶されているプログラムを実行することにより、登録手段１３において特徴量抽出手段１４により抽出されたユーザの顔画像の特徴量（具体的には、ハッシュ値）を、ユーザの識別情報および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けてメモリ１６に記憶させるようになっている。また、プロセッサ１２は、メモリ１６に記憶されているプログラムを実行することにより、認証手段１５において、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ～３８Ｃに撮像されたユーザの顔画像の特徴量（具体的には、ハッシュ値）と、メモリ１６に記憶されている各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量（具体的には、ハッシュ値）とを比較することにより、ユーザの認証を行うようになっている。なお、プロセッサ１２により実行されるプログラムはメモリ１６に記憶されているものに限定されることはない。外部装置から認証システム１０に送信されたプログラムや、認証システム１０に着脱自在に装着される記録媒体に記憶されているプログラムをプロセッサ１２が実行することにより、特徴量抽出手段１４、登録手段１３および認証手段１５の各々において処理が行われてもよい。また、本実施の形態でも、特徴量抽出手段１４および登録手段１３により、情報取得手段１７が構成される。情報取得手段１７は、ユーザ登録時に、ユーザの顔画像データを受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をユーザの識別情報としてメモリ１６に記憶させる。

【００３８】

各サービス機関に配置される撮像ユニット３０Ａ、３０Ｂ、３０Ｃの各々は例えばコンピュータ等から構成されており、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃは、ＣＰＵ等のプロセッサ３２Ａ、３２Ｂ、３２Ｃと、メモリ３６Ａ、３６Ｂ、３６Ｃと、撮像部３８Ａ、３８Ｂ、３８Ｃと、処理部４０Ａ、４０Ｂ、４０Ｃと、通信部４２Ａ、４２Ｂ、４２Ｃとを有している。プロセッサ３２Ａ、３２Ｂ、３２Ｃは、撮像部３８Ａ、３８Ｂ、３８Ｃにより撮像されたユーザの顔画像データに基づいてユーザの顔画像の特徴量をハッシュ値として抽出する特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃを有している。なお、図４に示す例では、プロセッサ３２Ａ、３２Ｂ、３２Ｃは図１に示すような認証手段３５Ａ、３５Ｂ、３５Ｃを有していない。プロセッサ３２Ａ、３２Ｂ、３２Ｃは、メモリ３６Ａ、３６Ｂ、３６Ｃに記憶されているプログラムを実行することにより、特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃにおいてユーザの顔画像の特徴量をハッシュ値として抽出するようになっている。具体的には、特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃは、受け付けたユーザの顔画像データから所定のハッシュ関数により求めたハッシュ値を、ユーザの顔画像の特徴量として抽出する。なお、プロセッサ３２Ａ、３２Ｂ、３２Ｃにより実行されるプログラムはメモリ３６Ａ、３６Ｂ、３６Ｃに記憶されているものに限定されることはない。外部装置から撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信されたプログラムや、撮像ユニット３０Ａ、３０Ｂ、３０Ｃに着脱自在に装着される記録媒体に記憶されているプログラムをプロセッサ３２Ａ、３２Ｂ、３２Ｃが実行することにより、特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃにおいて様々な処理が行われてもよい。また、図４に示す例では、メモリ３６Ａ、３６Ｂ、３６Ｃには、ユーザの顔画像の特徴量が記憶されないようになっている。

【００３９】

図４に示す例でも、認証システム１０および各サービス機関に配置される撮像ユニット３０Ａ、３０Ｂ、３０ＣはＡＰＩ連携（アプリケーション・プログラミング・インターフェース）が行われている。これにより、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃのシステムを、それぞれ独立して構成したものに比べて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃのシステムを容易に構成することができる。

【００４０】

次に、図４に示すような認証システム１０および各撮像ユニット３０Ａ、３０Ｂ、３０ＣによりユーザＵの認証を行う際の処理内容について図５および図６を用いて説明する。

【００４１】

まず、ユーザＵがユーザ端末２０を用いて顔画像データを認証システム１０に登録する処理について説明する。なお、ユーザＵがユーザ端末２０により顔画像を撮像する具体的な方法については既に説明したためここでは省略する。ユーザＵがユーザ端末２０においてこのような顔認証アプリで最初にユーザ登録を行うと、ユーザ登録画面で入力された様々な情報およびユーザＵの顔画像データがユーザ端末２０から認証システム１０に送信される。このようにして、認証システム１０のプロセッサ１２はユーザ端末２０から顔画像データを受け取る（ＳＴＥＰ２１）。また、ユーザ端末２０の識別情報、およびユーザ端末２０に入力されたユーザＵの氏名、生年月日、電話番号、メールアドレス、パスワード等の登録情報も、認証システム１０のプロセッサ１２はユーザ端末２０から受け取る。また、プロセッサ１２はユーザＵの識別情報としてユーザＩＤを発行し、この発行されたユーザＩＤをメモリ１６に記憶させる。

【００４２】

次に、認証システム１０のプロセッサ１２は、ユーザ端末２０から受け取った顔画像データに基づいて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応する顔画像の特徴量をハッシュ値として特徴量抽出手段１４により抽出する（ＳＴＥＰ２２）。この際に、特徴量抽出手段１４により抽出されるユーザＵの顔画像の特徴量は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの種類によって異なる場合があり、特徴量抽出手段１４は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎にユーザＵの顔画像の特徴量を抽出する。また、特徴量抽出手段１４は、ユーザＵにより予め選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザＵの顔画像の特徴量のみを抽出する。そして、プロセッサ１２は、特徴量抽出手段１４により抽出された各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応する顔画像の特徴量を、登録手段１３により認証システム１０のメモリ１６にユーザＩＤ（ユーザＵの識別情報）および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けて記憶させる（ＳＴＥＰ２３）。このようにして、ユーザ端末２０により撮像されたユーザＵの顔画像の登録が完了する。なお、図４に示す例では、メモリ１６に記憶されたユーザＵの顔画像の特徴量に係る情報は、認証システム１０から、ユーザＵにより選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信されない。

【００４３】

次に、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいてユーザの認証を行う処理について説明する。各撮像ユニット３０Ａ、３０Ｂ、３０Ｃが設置されるサービス機関においてユーザＵの認証が必要となった場合には、まず、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ、３８Ｂ、３８ＣによりユーザＵを撮像することによってユーザＵの顔画像データを取得する（ＳＴＥＰ３１）。また、撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいて、プロセッサ３２Ａ、３２Ｂ、３２Ｃは、取得された顔画像データに基づいて特徴量抽出手段３４Ａ、３４Ｂ、３４ＣによりユーザＵの顔画像の特徴量をハッシュ値として抽出する（ＳＴＥＰ３２）。そして、プロセッサ３２Ａ、３２Ｂ、３２Ｃは、特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃにより抽出されたユーザＵの顔画像の特徴量（具体的には、ハッシュ値）を通信部４２Ａ、４２Ｂ、４２Ｃにより認証システム１０のプロセッサ１２に送信する（ＳＴＥＰ３３）。なお、認証システム１０のプロセッサ１２が撮像ユニット３０Ａ、３０Ｂ、３０ＣからユーザＵの顔画像の特徴量に係る情報を受け付ける際に、メモリ１６に記憶されている、ユーザＵにより選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ

のみから送信されたユーザの顔画像の特徴量に係る情報を受け付ける。そして、認証システム１０において、プロセッサ１２は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けたユーザの顔画像の特徴量（具体的には、ハッシュ値）と、メモリ１６に記憶されているユーザの顔画像の特徴量（具体的には、ハッシュ値）とを認証手段１５によって比較することによりユーザの認証を行う（ＳＴＥＰ３４）。より詳細に説明すると、撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けたユーザの顔画像の特徴量と、メモリ１６に記憶されているユーザの顔画像の特徴量との一致率が所定の閾値（例えば、８０％）を超える場合には、認証手段１５はユーザの認証を行う。なお、上述したように、メモリ１６には、予め登録されたユーザの識別情報および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報と、ユーザの顔画像の特徴量とが関連付けて記憶されている。

【００４４】

そして、認証手段１５によりユーザの認証が行われると（ＳＴＥＰ３５の「ＹＥＳ」）、認証結果に係る情報が認証システム１０のプロセッサ１２から通信部１８により撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される（ＳＴＥＰ３６）。そして、認証結果に係る情報を受け取った撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、各処理部４０Ａ、４０Ｂ、４０Ｃによりこの撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するサービスを実施可能とする（ＳＴＥＰ３７）。その後、撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、サービスの利用状況に係る情報を認証システム１０に送信する。このことにより、認証システム１０において各サービス機関におけるサービスの利用状況に係る情報がユーザ毎にメモリ１６に記憶される。

【００４５】

一方、撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けたユーザの顔画像の特徴量が、メモリ１６に記憶されているユーザの顔画像の特徴量に略一致せず、認証手段１５によりユーザの認証を行うことができなかった場合にも（ＳＴＥＰ３５の「ＮＯ」）、認証結果に係る情報が認証システム１０のプロセッサ１２から通信部１８により撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される（ＳＴＥＰ３８）。そして、認証結果に係る情報を受け取った撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは各処理部４０Ａ、４０Ｂ、４０Ｃによりこの撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するサービスを実施不可とする（ＳＴＥＰ３９）。この場合も、撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、サービスの利用状況に係る情報（具体的には、ユーザが撮像ユニット３０Ａ、３０Ｂ、３０Ｃで認証を行おうとしたが認証されずにサービスを利用できなかったという情報）を認証システム１０に送信する。

【００４６】

このような認証方法によれば、ユーザの顔画像の特徴量があるサービス機関の撮像エンジン（例えば、撮像ユニット３０Ａ）で登録されているが、別のサービス機関の撮像エンジン（例えば、撮像ユニット３０Ｂ）で登録されていない場合でも、認証システム１０のメモリ１６にこのユーザの顔画像の特徴量を撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けて記憶させておくことにより、ユーザの顔画像の特徴量が登録されていないサービス機関でも撮像部によりユーザの顔画像を撮像することによってユーザの認証を行うことができる。この場合には、複数の撮像ユニットの全てでユーザは顔画像データの登録を行う必要がなくなるので、ユーザの手間を省くことができるようになる。

【００４７】

また。本実施の形態による認証システム１０や認証方法の更に他の例について図７乃至図９を用いて説明する。なお、図７に示す認証システム１０や各撮像ユニット３０Ａ、３０Ｂ、３０Ｃについて、図１や図４に示す認証システム１０や各撮像ユニット３０Ａ、３０Ｂ、３０Ｃと同じ構成要素については同じ参照符号を付けてその説明を省略する。

【００４８】

図７に示すように、認証システム１０のプロセッサ１２は、ユーザ端末２０から受け取った顔画像データに基づいて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量をハッシュ値として抽出する特徴量抽出手段１４と、抽出されたユーザ

の顔画像の特徴量を登録する登録手段１３と、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ～３８Ｃに撮像されたユーザの顔画像の特徴量（具体的には、ハッシュ値）に基づいてユーザの認証を行う認証手段１５とを有している。プロセッサ１２は、メモリ１６に記憶されているプログラムを実行することにより、登録手段１３において特徴量抽出手段１４により抽出されたユーザの顔画像の特徴量（具体的には、ハッシュ値）を、ユーザの識別情報および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けてメモリ１６に記憶させるようになっている。また、プロセッサ１２は、メモリ１６に記憶されているプログラムを実行することにより、認証手段１５において、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ～３８Ｃに撮像されたユーザの顔画像の特徴量（具体的には、ハッシュ値）と、メモリ１６に記憶されている各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量（具体的には、ハッシュ値）とを比較することにより、ユーザの認証を行うようになっている。なお、プロセッサ１２により実行されるプログラムはメモリ１６に記憶されているものに限定されることはない。外部装置から認証システム１０に送信されたプログラムや、認証システム１０に着脱自在に装着される記録媒体に記憶されているプログラムをプロセッサ１２が実行することにより、特徴量抽出手段１４、登録手段１３および認証手段１５の各々において処理が行われてもよい。また、本実施の形態でも、特徴量抽出手段１４および登録手段１３により、情報取得手段１７が構成される。情報取得手段１７は、ユーザ登録時に、ユーザの顔画像データを受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をユーザの識別情報としてメモリ１６に記憶させる。

【００４９】

各サービス機関に配置される撮像ユニット３０Ａ、３０Ｂ、３０Ｃの各々は例えばコンピュータ等から構成されており、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃは、ＣＰＵ等のプロセッサ３２Ａ、３２Ｂ、３２Ｃと、メモリ３６Ａ、３６Ｂ、３６Ｃと、撮像部３８Ａ、３８Ｂ、３８Ｃと、処理部４０Ａ、４０Ｂ、４０Ｃと、通信部４２Ａ、４２Ｂ、４２Ｃとを有している。なお、図７に示す例では、プロセッサ３２Ａ、３２Ｂ、３２Ｃは図１に示すような特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃおよび認証手段３５Ａ、３５Ｂ、３５Ｃを有していない。また、図７に示す例では、メモリ３６Ａ、３６Ｂ、３６Ｃには、ユーザの顔画像の特徴量が記憶されないようになっている。

【００５０】

図７に示す例でも、認証システム１０および各サービス機関に配置される撮像ユニット３０Ａ、３０Ｂ、３０ＣはＡＰＩ連携（アプリケーション・プログラミング・インターフェース）が行われている。これにより、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃのシステムを、それぞれ独立して構成したものに比べて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃのシステムを容易に構成することができる。

【００５１】

次に、図７に示すような認証システム１０および各撮像ユニット３０Ａ、３０Ｂ、３０Ｃによりユーザの認証を行う際の処理内容について図８および図９を用いて説明する。

【００５２】

まず、ユーザがユーザ端末２０を用いて顔画像データを認証システム１０に登録する処理について説明する。なお、ユーザがユーザ端末２０により顔画像を撮像する具体的な方法については既に説明したためここでは省略する。ユーザがユーザ端末２０においてこのような顔認証アプリで最初にユーザ登録を行うと、ユーザ登録画面で入力された様々な情報およびユーザの顔画像データがユーザ端末２０から認証システム１０に送信される。このようにして、認証システム１０のプロセッサ１２はユーザ端末２０から顔画像データを受け取る（ＳＴＥＰ４１）。また、ユーザ端末２０の識別情報、およびユーザ端末２０に入力されたユーザの氏名、生年月日、電話番号、メールアドレス、パスワード等の登録情報も、認証システム１０のプロセッサ１２はユーザ端末２０から受け取る。また、プロセッサ１２はユーザの識別情報としてユーザＩＤを発行し、この発行されたユーザＩＤをメ

モリ１６に記憶させる。
【００５３】
次に、認証システム１０のプロセッサ１２は、ユーザ端末２０から受け取った顔画像データに基づいて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応する顔画像の特徴量をハッシュ値として特徴量抽出手段１４により抽出する（ＳＴＥＰ４２）。この際に、特徴量抽出手段１４により抽出されるユーザの顔画像の特徴量は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの種類によって異なる場合があり、特徴量抽出手段１４は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎にユーザの顔画像の特徴量を抽出する。また、特徴量抽出手段１４は、ユーザにより予め選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量のみを抽出する。そして、プロセッサ１２は、特徴量抽出手段１４により抽出された各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応する顔画像の特徴量を、登録手段１３により認証システム１０のメモリ１６にユーザＩＤ（ユーザの識別情報）および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けて記憶させる（ＳＴＥＰ４３）。このようにして、ユーザ端末２０により撮像されたユーザの顔画像の登録が完了する。なお、図７に示す例では、メモリ１６に記憶されたユーザの顔画像の特徴量に係る情報は、認証システム１０から、ユーザにより選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信されない。
【００５４】
次に、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいてユーザの認証を行う処理について説明する。各撮像ユニット３０Ａ、３０Ｂ、３０Ｃが設置されるサービス機関においてユーザの認証が必要となった場合には、まず、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ、３８Ｂ、３８Ｃによりユーザを撮像することによってユーザの顔画像データを取得する（ＳＴＥＰ５１）。撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、撮像部３８Ａ、３８Ｂ、３８Ｃにより撮像されたユーザの顔画像データを通信部４２Ａ、４２Ｂ、４２Ｃにより認証システム１０のプロセッサ１２に送信する（ＳＴＥＰ５２）。なお、認証システム１０のプロセッサ１２が撮像ユニット３０Ａ、３０Ｂ、３０Ｃからユーザの顔画像データを受け付ける際に、メモリ１６に記憶されている、ユーザにより選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃのみから送信されたユーザの顔画像データを受け付ける。そして、認証システム１０において、プロセッサ１２は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けた顔画像データに基づいて特徴量抽出手段１４によりユーザの顔画像の特徴量をハッシュ値として抽出する（ＳＴＥＰ５３）。そして、プロセッサ１２は、特徴量抽出手段１４により抽出されたユーザの顔画像の特徴量（具体的には、ハッシュ値）と、メモリ１６に記憶されているユーザの顔画像の特徴量（具体的には、ハッシュ値）とを認証手段１５によって比較することによりユーザの認証を行う（ＳＴＥＰ５４）。より詳細に説明すると、特徴量抽出手段１４により抽出されたユーザの顔画像の特徴量と、メモリ１６に記憶されているユーザの顔画像の特徴量との一致率が所定の閾値（例えば、８０％）を超える場合には、認証手段１５はユーザの認証を行う。なお、上述したように、メモリ１６には、予め登録されたユーザの識別情報および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報と、ユーザの顔画像の特徴量とが関連付けて記憶されている。
【００５５】
そして、認証手段１５によりユーザの認証が行われると（ＳＴＥＰ５５の「ＹＥＳ」）、認証結果に係る情報が認証システム１０のプロセッサ１２から通信部１８により撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される（ＳＴＥＰ５６）。そして、認証結果に係る情報を受け取った撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、各処理部４０Ａ、４０Ｂ、４０Ｃによりこの撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するサービスを実施可能とする（ＳＴＥＰ５７）。その後、撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、サービスの利用状況に係る情報を認証システム１０に送信する。このことにより、認証システム１０において各サービス機関におけるサービスの利用状況に係る情報がユーザ毎にメモリ１６に記憶される。

【００５６】
一方、撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けたユーザの顔画像の特徴量が、メモリ１６に記憶されているユーザの顔画像の特徴量に略一致せず、認証手段１５によりユーザの認証を行うことができなかった場合にも（ＳＴＥＰ５５の「ＮＯ」）、認証結果に係る情報が認証システム１０のプロセッサ１２から通信部１８により撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される（ＳＴＥＰ５８）。そして、認証結果に係る情報を受け取った撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは各処理部４０Ａ、４０Ｂ、４０Ｃによりこの撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するサービスを実施不可とする（ＳＴＥＰ５９）。この場合も、撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、サービスの利用状況に係る情報（具体的には、ユーザが撮像ユニット３０Ａ、３０Ｂ、３０Ｃで認証を行おうとしたが認証されずにサービスを利用できなかったという情報）を認証システム１０に送信する。
【００５７】
このような認証方法によれば、ユーザの顔画像の特徴量があるサービス機関の撮像エンジン（例えば、撮像ユニット３０Ａ）で登録されているが、別のサービス機関の撮像エンジン（例えば、撮像ユニット３０Ｂ）で登録されていない場合でも、認証システム１０のメモリ１６にこのユーザの顔画像の特徴量を撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けて記憶させておくことにより、ユーザの顔画像の特徴量が登録されていないサービス機関でも撮像部によりユーザの顔画像を撮像することによってユーザの認証を行うことができる。この場合には、複数の撮像ユニットの全てでユーザは顔画像データの登録を行う必要がなくなるので、ユーザの手間を省くことができるようになる。
【００５８】
次に、図１乃至図９に示すような認証システム１０において、上述した顔認証サービスが適用されるサービス機関をユーザが増やしたい場合の処理について説明する。ユーザが上述したユーザ登録を行った後、図１０に示すようなユーザ端末２０の初期画面において「サービス追加」のボタンをユーザが指で押すと、図１３に示すようなサービス機関の一覧が表示される。なお、このようなサービス機関の一覧は、予め認証システム１０に登録されたものである。図１３に示すような画面において、未登録サービスのアイコンと登録済サービスのアイコンとは別の色で表示されたり、未登録サービスのアイコンが薄く表示されたりする等により、未登録サービスのアイコンと登録済サービスのアイコンとが区別して表示される。そして、ユーザが未登録サービスのアイコンを指で押すと、追加するサービスの規約が表示される。ユーザがサービスの規約に合意する旨の指示を入力すると、未登録サービスが登録済サービスになる。この際に、認証システム１０において、この登録済サービスに関連するサービス機関がユーザＩＤ（ユーザの識別情報）に関連付けられてメモリ１６に記憶される。その後、ユーザ端末２０には図１２に示すような顔画像の撮像画面が表示される。このような撮像画面でユーザがユーザ端末２０により顔画像を撮像すると、ユーザの顔画像データがユーザ端末２０から認証システム１０に送信される。このようにして、認証システム１０のプロセッサ１２はユーザ端末２０から顔画像データを受け取る。そして、認証システム１０のプロセッサ１２は、ユーザ端末２０から受け取った顔画像データに基づいて、新たなサービス機関の撮像ユニットに対応する顔画像の特徴量をハッシュ値として特徴量抽出手段１４により抽出する。プロセッサ１２は、特徴量抽出手段１４により抽出された新たな撮像ユニットに対応する顔画像の特徴量を、登録手段１３により認証システム１０のメモリ１６にユーザＩＤ（ユーザの識別情報）および新たなサービス機関の撮像ユニットの識別情報に関連付けて記憶させる。このようにして、新たなサービス機関の登録が完了する。なお、後述するようにメモリ１６にユーザの顔画像データが記憶されている場合には、新たなサービス機関をユーザがユーザ端末２０で登録する際に、ユーザ端末２０によりユーザの顔画像を撮像しなくても、メモリ１６に記憶されているユーザの顔画像データに基づいて、新たなサービス機関の撮像ユニットに対応する顔画像の特徴量をハッシュ値として特徴量抽出手段１４により抽出してもよい。また、図１３に示すような画面において、ユーザが登録済サービスを削除することができるよう

になっていてもよい。この場合には、登録済サービスが未登録サービスになる。また、メモリ１６に記憶されている、削除された登録済サービスに係るサービス機関の撮像ユニットに対応するユーザの顔画像の特徴量に係る情報が削除される。

【００５９】

また、ユーザが上述したユーザ登録を行った後、図１０に示すようなユーザ端末２０の初期画面において「認証履歴」のボタンをユーザが指で押すと、図１４に示すような過去の認証履歴情報の一覧（言い換えると、ユーザによるサービス機関の利用状況に係る情報の一覧）がユーザ端末２０に表示されるようになる。より詳細には、認証システム１０のメモリ１６には、ユーザの過去の認証履歴情報がユーザの識別情報に関連付けられて記憶されている。そして、図１０に示すようなユーザ端末２０の初期画面において「認証履歴」のボタンがユーザにより指で押されると、ユーザ端末２０から認証システム１０のプロセッサ１２によりユーザの過去の認証履歴情報を求める信号が送信される。認証システム１０のプロセッサ１２は、ユーザの過去の認証履歴情報を求める信号をユーザ端末２０から受け取ると、メモリ１６に記憶されているこのユーザの識別情報に対応する過去の認証履歴情報を通信部１８によりユーザ端末２０に送信する。このことにより、ユーザ端末２０には、このユーザの過去の認証履歴情報の一覧が表示されるようになる。また、図１４に示すような過去の認証履歴情報の一覧において、ある認証履歴の表示をユーザが指で押すと、図１５に示すようにユーザ端末２０にはこの認証履歴の詳細が表示されるようになる。

【００６０】

また、本実施の形態では、ユーザがユーザ端末２０を用いて認証システム１０におけるユーザの顔認証の特徴量の登録を行う代わりに、ユーザがある撮像ユニット３０Ａ、３０Ｂ、３０Ｃを用いて認証システム１０におけるユーザの顔認証の特徴量の登録を行うようになっていてもよい。具体的には、ある撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいてユーザが登録情報を入力するとともに撮像部３８Ａ、３８Ｂ、３８Ｃによりユーザの顔画像を撮像すると、入力された登録情報およびユーザの顔画像データが撮像ユニット３０Ａ、３０Ｂ、３０Ｃから認証システム１０に送信される。このようにして、認証システム１０のプロセッサ１２は撮像ユニット３０Ａ、３０Ｂ、３０Ｃから顔画像データを受け取る。また、プロセッサ１２は撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け取った登録情報に基づいてユーザの識別情報としてユーザＩＤを発行し、この発行されたユーザＩＤをメモリ１６に記憶させる。

【００６１】

次に、認証システム１０のプロセッサ１２は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け取った顔画像データに基づいて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応する顔画像の特徴量をハッシュ値として特徴量抽出手段１４により抽出する。この際に、特徴量抽出手段１４は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎にユーザの顔画像の特徴量を抽出する。また、特徴量抽出手段１４は、ユーザにより予め選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量のみを抽出する。例えば、撮像ユニット３０Ａが設置されるサービス機関についてはユーザが顔画像データを使うことを認めているが、撮像ユニット３０Ｂが設置されるサービス機関についてはユーザが顔画像データを使うことを認めていない場合には、特徴量抽出手段１４は、撮像ユニット３０Ａに対応するユーザの顔画像の特徴量のみを抽出する。なお、上述したように、メモリ１６には、ユーザの識別情報と、このユーザにより選択されたサービス機関とが関連付けられて記憶されるようになっている。そして、プロセッサ１２は、特徴量抽出手段１４により抽出された各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応する顔画像の特徴量を、登録手段１３により認証システム１０のメモリ１６にユーザＩＤ（ユーザの識別情報）および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けて記憶させる。このようにして、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ、３８Ｂ、３８Ｃにより撮像されたユーザの顔画像の登録が完了する。このような態様では、ユーザがユーザ端末２０を用いなくても認証システム１０におけるユーザの顔認証の特徴量の登録を行

うことができる。

【００６２】

以上のような構成からなる、本実施の形態に係る、認証システム１０により行われる認証方法によれば、ユーザの顔画像データおよびユーザの識別情報を受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に抽出する。そして、抽出された複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎のユーザの顔画像の特徴量に係る情報を、受け付けたユーザの識別情報に関連付けてメモリ１６に記憶させる。このような認証方法によれば、容易に複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃで顔認証を行うことができるようになる。

【００６３】

具体的には、従来でも顔認証を用いた認証エンジンを設けることは一般的に広まっているが、従来技術の認証システムでは、顔データを登録していない認証エンジンでは、顔認証を行うことができなかった。このため、複数の認証エンジンそれぞれで認証を行うためには、ユーザは、複数の認証エンジンそれぞれで顔データを登録する必要があり手間がかかりストレスとなっていた。これに対し、本実施の形態では、ユーザの顔画像の特徴量があるサービス機関の認証エンジン（例えば、撮像ユニット３０Ａ）で登録されているが、別のサービス機関の認証エンジン（例えば、撮像ユニット３０Ｂ）で登録されていない場合でも、認証システム１０のメモリ１６にこのユーザの顔画像の特徴量を撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に記憶させておくことにより、ユーザの顔画像の特徴量が登録されていないサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃでも撮像部３８Ａ、３８Ｂ、３８Ｃによりユーザの顔画像を撮像することによってユーザの認証を行うことができる。この場合には、複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃの全てでユーザは顔画像データの登録を行う必要がなくなるので、ユーザの手間を省くことができるようになる。これにより、顔画像データの登録が面倒で、顔画像データを登録していない撮像ユニットを用いた各種サービスを利用していなかったユーザにも、気軽に各種サービスを利用するように促すことができる。

【００６４】

また、ハッシュ値等のユーザの顔画像の特徴量を抽出してメモリ１６に記憶させる場合には、ユーザの顔画像データ自体をメモリ１６に記憶させる場合と比較して、メモリ１６に記憶されるデータ量を著しく小さくすることができる。これは、ユーザの顔画像データ自体のデータ量と比較して、ユーザの顔画像の特徴量のデータ量が小さいからである。また、この場合にはメモリ１６にユーザの顔画像データ自体が保存されないため、ユーザのプライバシー性をより一層確実に保護することができる。また、ユーザの顔画像の特徴量に係る情報を認証システム１０と各撮像ユニット３０Ａ、３０Ｂ、３０Ｃとの間で送る場合には、ユーザの顔画像データを認証システム１０と各撮像ユニット３０Ａ、３０Ｂ、３０Ｃとの間で送る場合と比較してデータ通信量を著しく小さくすることができる。

【００６５】

また、本実施の形態の認証方法では、上述したように、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出する際に、ユーザの顔画像の特徴量を複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に抽出し、抽出された複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎のユーザの顔画像の特徴量を、登録手段１３によりユーザの識別情報に関連付けてメモリに記憶させる。このときには、特徴量抽出手段１４により抽出されるユーザの顔画像の特徴量が、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの種類によって異なる場合にも対応することができる。なお、複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃで同じプログラムが用いられ、特徴量抽出手段１４により抽出されるユーザの顔画像の特徴量が、撮像ユニット３０Ａ、３０Ｂ、３０Ｃで共通する場合には、ユーザの顔画像の特徴量を複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に抽出しなくてもよい。

【００６６】

また、本実施の形態の認証方法では、上述したように、メモリ１６には、ユーザにより選択されたサービス機関に係る情報がユーザの識別情報に関連付けられて記憶されており

、受け付けたユーザの顔画像データに基づいて、このユーザの顔画像の特徴量を複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に特徴量抽出手段１４により抽出する工程において、メモリ１６に記憶されているユーザにより選択されたサービス機関の撮像ユニットのみに対応するユーザの顔画像の特徴量を特徴量抽出手段１４により抽出する。この場合には、ユーザが選択していないサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像の特徴量はメモリ１６に記憶されないので、セキュリティ性を向上させることができ、ユーザを安心させることができる。また、認証システム１０が統括的に管理する認証エンジンのグループに参加する企業等は、ユーザ端末２０等で顔画像データを登録するだけで、多数の認証エンジンで認証させることができるという顧客利便性の向上を顧客にアピールすることができるようになる。

【００６７】

また、本実施の形態の認証方法では、上述したように、特徴量抽出手段１４は、受け付けたユーザの顔画像データから所定のハッシュ関数により求めたハッシュ値を、このユーザの顔画像の特徴量として複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に抽出する。この場合には、ユーザの顔画像の特徴量としてハッシュ値をメモリ１６に記憶させるので、顔画像データそのものをメモリ１６に記憶させる場合と比較して、メモリ１６に記憶されるデータ量を低減することができる。また、ハッシュ値から顔画像データを復元または推測することは難しく、認証システム１０ではハッシュ値のみを保存するので、ユーザのプライバシー性やセキュリティ性を高めることができる。

【００６８】

なお、本実施の形態では、特徴量抽出手段１４は、受け付けたユーザの顔画像データに基づいて、ユーザの顔画像の特徴量をハッシュ値として複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に抽出することに限定されることはない。特徴量抽出手段１４は、受け付けたユーザの顔画像データに基づいて、ユーザの顔画像の特徴量をハッシュ値とは別の種類の値で複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に抽出するようになっていてもよい。例えば、ユーザの顔画像の特徴量として、顔の各パーツ（目、鼻、耳等）の相対位置や大きさや形等を特徴として抽出するようにしてもよい。この場合でも、ハッシュ値とは別の種類の値のデータ量が顔画像自体のデータ量よりも少ない場合には、メモリ１６に記憶されるデータ量を低減することができる。

【００６９】

また、本実施の形態の認証方法では、上述したように、受け付けたユーザの顔画像データに基づいて、このユーザの顔画像の特徴量を複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に特徴量抽出手段１４により抽出する工程において、ユーザが所持するユーザ端末２０から送信されたユーザの顔画像データに基づいて、このユーザの顔画像の特徴量を複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に特徴量抽出手段１４により抽出する。あるいは、受け付けたユーザの顔画像データに基づいて、このユーザの顔画像の特徴量を複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に特徴量抽出手段１４により抽出する工程において、複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃのうちある撮像ユニットから送信されたユーザの顔画像データに基づいて、このユーザの顔画像の特徴量を複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に特徴量抽出手段１４により抽出してもよい。

【００７０】

また、本実施の形態では、プロセッサ１２により実行される、認証システム１０により認証方法を行うためのプログラムおよびこのプログラムが記録された記録媒体が用いられる。ここで、プロセッサ１２がプログラムを実行することにより、ユーザの顔画像データおよびユーザの識別情報を受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に抽出する。そして、抽出された複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎のユーザの顔画像の特徴量に係る情報を、受け付けたユーザの識別情報に関連付けてメモリ１６に記憶させる。このようなプログラムおよび記録媒体によれば、容易に複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃで顔認証を行うことができるようになる。

【００７１】
また、本実施の形態では、プロセッサ１２を備えた認証システム１０が用いられる。このような認証システム１０では、プロセッサ１２は、プログラムを実行することにより、ユーザの顔画像データおよびユーザの識別情報を受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に抽出する。そして、抽出された複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎のユーザの顔画像の特徴量に係る情報を、受け付けたユーザの識別情報に関連付けてメモリ１６に記憶させる。このような認証システム１０によれば、容易に複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃで顔認証を行うことができるようになる。
【００７２】
なお、本発明による認証方法や認証システムは、上述したような態様に限定されることはなく、様々な変更を加えることができる。
【００７３】
例えば、認証システムとして図１６に示すようなものが用いられてもよい。図１６に示す認証システム５０は、プロセッサ５２と、第１サーバ５６と、第２サーバ５８と、第３サーバ６０とを有している。ここで、各サーバ５６、５８、６０は各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応している。具体的には、第１サーバ５６は撮像ユニット３０Ａに対応しており、第２サーバ５８は撮像ユニット３０Ｂに対応しており、第３サーバ６０は撮像ユニット３０Ｃに対応している。また、図１６では３つの撮像ユニット３０Ａ、３０Ｂ、３０Ｃが図示されているが、２つまたは４つ以上の撮像ユニットが用いられる場合には各撮像ユニットに対応してサーバが認証システム１０に設けられる。また、プロセッサ５２は、サーバ管理手段５２ａと、特徴量抽出手段５４と、登録手段５３と、認証手段５５とを有している。プロセッサ５２の特徴量抽出手段５４、登録手段５３および認証手段５５は、図１、図４、図７に示す認証システム１０のプロセッサ１２の特徴量抽出手段１４、登録手段１３および認証手段１５と略同一の機能を有している。サーバ管理手段５２ａは、各サーバ５６、５８、６０の管理を行うようになっている。
【００７４】
各サーバ５６、５８、６０には、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するユーザの顔画像のデータの特徴量がユーザの識別情報に関連付けられて記憶されている。また、各サーバ５６、５８、６０は、インターネット回線等のネットワークを介して対応する各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに通信可能に接続されている。各サーバ５６、５８、６０は、サーバ管理手段５２ａによりＡＰＩ（アプリケーション・プログラミング・インターフェース）で一括管理可能に構成されている。これにより、各サーバ５６、５８、６０のシステム（プログラム）を、それぞれ独立して構成したものに比べて、各サーバ５６、５８、６０のシステムを容易に構成することができる。また、サーバ管理手段５２ａと、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃが設置されたサービス機関とは、ＡＰＩ連携されている。例えば、サーバ管理手段５２ａのプラットフォームを各サービス機関に開放して、各サービス機関においてもサーバ管理手段５２ａと同じプラットフォームを使用することで、各サービス機関でのサービスを行うためのシステムを容易に構築することができる。
【００７５】
このようなプロセッサ５２および各サーバ５６、５８、６０を有する認証システム５０でも、プロセッサ１２を有する認証システム１０と同様の処理を行うことができる。すなわち、図１６に示す認証システム５０により行われる認証方法によれば、プロセッサ５２は、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を各撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に特徴量抽出手段５４により抽出し、抽出されたユーザの顔画像の特徴量を、登録手段５３によりユーザの識別情報および撮像ユニット３０Ａ、３０Ｂ、３０Ｃに関連付けて各サーバ５６、５８、６０に記憶させる。
【００７６】
また、各サーバ５６、５８、６０に記憶されているユーザの顔画像の特徴量に係る情報

は、各サーバ５６、５８、６０から対応する各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される。このことにより、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいてユーザの認証を行う際に、撮像部３８Ａ、３８Ｂ、３８Ｃによりユーザを撮像することによってユーザの顔画像データを取得し、取得された顔画像データに基づいて特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃによりユーザの顔画像の特徴量を抽出することにより、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃでユーザの認証を行うことができるようになる。その後、撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、サービスの利用状況に係る情報を認証システム１０に送信する。このことにより、認証システム５０において各サービス機関におけるサービスの利用状況に係る情報がユーザ毎に各サーバ５６、５８、６０に記憶される。

【００７７】

ユーザの認証を行う他の方法として、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいてユーザの認証を行う際に、撮像部３８Ａ、３８Ｂ、３８Ｃによりユーザを撮像することによってユーザの顔画像データを取得し、取得された顔画像データに基づいて特徴量抽出手段３４Ａ、３４Ｂ、３４Ｃによりユーザの顔画像の特徴量を抽出する。そして、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃから認証システム５０にユーザの顔画像の特徴量に係る情報が送信される。このことにより、認証手段５５によってユーザの認証を行うことができるようになる。その後、ユーザの認証結果が認証システム５０から元の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される。

【００７８】

ユーザの認証を行う更に他の方法として、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいてユーザの認証を行う際に、撮像部３８Ａ、３８Ｂ、３８Ｃによりユーザを撮像することによってユーザの顔画像データを取得する。そして、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃから認証システム５０にユーザの顔画像データが送信される。そして、プロセッサ５２は、各サーバ５６、５８、６０に送信されたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を特徴量抽出手段５４により抽出し、抽出されたユーザの顔画像の特徴量と、各サーバ５６、５８、６０に記憶されているユーザの顔画像の特徴量とを認証手段５５により比較する。このことにより、認証手段５５によってユーザの認証を行うことができるようになる。その後、ユーザの認証結果が認証システム５０から元の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される。

【００７９】

これらの認証方法によれば、容易に複数の撮像ユニット３０Ａ、３０Ｂ、３０Ｃで顔認証を行うことができるようになる。

【００８０】

また、図１、図４、図７等に示すような認証システム１０において、ユーザ端末２０や各撮像ユニット３０Ａ、３０Ｂ、３０Ｃから送信されたユーザの顔画像データそのものをプロセッサ１２がメモリ１６に記憶させてもよい。

【００８１】

また、上記の例では、各サービス機関に設置される撮像ユニット３０Ａ、３０Ｂ、３０Ｃとは別に認証システム１０、５０が設置される態様が示されているが、各サービス機関に設置される撮像ユニット３０Ａ、３０Ｂ、３０Ｃのうちある撮像ユニットが認証システム１０、５０の機能を兼ねるようになっていてもよい。すなわち、各サービス機関に設置される撮像ユニット３０Ａ、３０Ｂ、３０Ｃのうちある撮像ユニットのプロセッサが、図１、図４、図７等に示す認証システム１０のプロセッサ１２における特徴量抽出手段１４、登録手段１３および認証手段１５と同等の機能を有する特徴量抽出手段、登録手段および認証手段を有していてもよい。

【００８２】

また、更に別の例として、認証システム１０は、ユーザの顔画像データから抽出されるユーザの顔画像の特徴量（具体的には、例えばハッシュ値）と、ユーザの顔画像の特徴量以外の要素（具体的には、例えばユーザ登録時にユーザ端末２０に入力されたパスワード

やユーザ端末２０の識別情報）とを用いることによりユーザの認証を二段階で行ってもよい（二要素認証）。この際に、サービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに必要なセキュリティレベルに応じて、認証に必要な要素を組み合わせてもよい。

【００８３】

また、上述した説明では、ユーザがユーザ端末２０を用いて顔画像データを認証システム１０に登録する際に、ユーザ登録画面において氏名、生年月日、電話番号、メールアドレス、パスワード等の登録情報を入力し、利用規約に同意する欄にチェックを入れた後に登録ボタンを押下するようになっている。また、撮像画面でユーザがユーザ端末２０により顔画像を撮像すると、ユーザ登録画面で入力された様々な情報およびユーザの顔画像データがユーザ端末２０から認証システム１０に送信される。その後、プロセッサ１２はユーザの識別情報としてユーザＩＤを発行し、この発行されたユーザＩＤをメモリ１６に記憶させる。しかしながら、本実施の形態はこのような態様に限定されることはない。他の態様として、ユーザの顔画像データから特徴量抽出手段１４により撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に抽出されるユーザの顔画像の特徴量（具体的には、例えばハッシュ値）そのものがユーザＩＤとして用いられてもよい。この場合、撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎にユーザＩＤ（すなわち、ハッシュ値）が異なるが、認証システム１０のプロセッサ１２は同一ユーザの撮像ユニット３０Ａ、３０Ｂ、３０Ｃ毎に異なる複数のユーザＩＤを互いに紐づけるようになっている。

【００８４】

また、認証システム１０のプロセッサ１２は、ユーザ登録画面で入力された様々な情報とユーザの顔画像データとを受け取った後にユーザの識別情報として発行されたユーザＩＤと、顔認証以外の認証を行う様々なサービス機関の認証エンジン３０Ｄで用いられるユーザＩＤ（ユーザの識別情報）とを紐づけてもよい。すなわち、認証システム１０は、顔認証以外の認証を行うサービス機関の認証エンジン３０Ｄで用いられるユーザＩＤ（ユーザの識別情報）と、メモリ１６に記憶されているユーザの顔画像の特徴量に係るユーザＩＤ（ユーザの識別情報）とを紐づける紐づけ手段１９を更に備えていてもよい。具体的には、顔認証以外の認証を行う様々なサービス機関の認証エンジン３０Ｄで用いられるユーザＩＤとして、ユーザが所持するスマートフォン等のユーザ端末２０の識別情報、ユーザの指紋情報や静脈情報等の生体情報から得られるユーザの識別情報（例えば、ハッシュ値）、ユーザによりスマートフォン等のユーザ端末２０に入力された数桁のコード（具体的には、例えば数字やローマ字を組み合わせたもの）やパスワードが考えられる。この場合には、顔認証以外の認証を行う様々なサービス機関の認証エンジン３０Ｄでユーザが認証を行う際に、ユーザ端末で顔画像を撮像することにより得られるユーザの顔画像データに基づいたユーザＩＤ（具体的には、顔画像データから抽出されるハッシュ値）を代用することができ、よってユーザにとっての利便性を向上させることができる。また、紐づけ手段１９による紐づけが行われた後でも、サービス機関の認証エンジン３０Ｄで用いられるユーザＩＤを残したままとしてもよい。この場合には、クラウドである認証システム１０を用いずにサービス機関の認証エンジン３０Ｄでユーザの認証をスタンドアローンで行う場合にも適切にユーザの認証を行うことができる。

【００８５】

また、サービス機関の種類によって異なる強度の認証が設定されていてもよい。具体的には、例えばサービス機関の認証エンジンとしてユーザが働くオフィスビルや自宅の施錠システムが用いられる場合には、スマートフォン等のユーザ端末２０の識別情報によって扉の施錠が解除されるようないわゆるスマートロックが用いられる。具体的には、ユーザが働くオフィスビルや自宅の施錠システムの扉やその近傍に設置される受信装置にユーザ端末２０を近づけるだけでＢｌｕｅｔｏｏｔｈ（登録商標）の機能によりユーザ端末２０の識別情報が読み取られたり、ユーザ端末２０にインストールされているスマートロックのアプリにより扉の施錠を開錠する指令がユーザにより入力されたりすると、ユーザ端末２０の識別情報に基づいてユーザの認証が行われる。そして、予め登録されているユーザであるという認証が行われると、ユーザが働くオフィスビルや自宅の扉の施錠が解除され

る。一方、サービス機関の認証エンジンとして金融機関の口座への振込システムや決済システムが用いられる場合には、ユーザ端末２０における金融機関サービスや決済サービスへのログイン時に顔認証が必要となり、さらに口座への振込時や決済時には顔認証に加えてＳＭＳ（ショートメッセージサービス）の配信による認証やパスワード入力が必要となる。このように、用途に応じてユーザＩＤの認証の強度を異なるようにすることによって、頻繁に使用するサービス機関の認証エンジンについては認証の強度を低くすることによりユーザの利便性を向上させるとともに金銭等を扱うサービス機関の認証エンジンについては認証の強度を高くすることによりセキュリティ性を向上させることができる。

【００８６】

また、ユーザは、顔認証に係るサービス機関に加えて、顔認証以外の認証を行うサービス機関の追加や削除をユーザ端末２０により図１３に示すような画面で行うことができるようになっていてもよい。すなわち、顔認証に係るサービス機関の一覧に加えて、顔認証以外の認証を行うサービス機関の一覧も予め認証システム１０に登録されている。そして、図１３に示すようなユーザ端末２０の画面において、ユーザが未登録サービスを登録すると、新たに登録されたサービス機関の認証エンジンで用いられるユーザＩＤがメモリ１６に記憶される。また、この際に、既にメモリ１６に記憶されている他のサービス機関のユーザＩＤと、新たに登録されたサービス機関の認証エンジンで用いられるユーザＩＤ（例えば、ユーザ端末２０の識別情報や、新たにサービス機関を登録するときにユーザにより入力された数桁のコードやパスワード等）とが紐づけ手段１９により紐づけられる。この場合には、顔認証以外の認証を行うサービス機関が新たに登録された場合に、ユーザがこのサービス機関の認証エンジンで認証を行う際に、ユーザ端末で顔画像を撮像することにより得られるユーザの顔画像データに基づいたユーザＩＤ（具体的には、顔画像データから抽出されるハッシュ値）を代用することができ、よってユーザにとっての利便性を向上させることができる。また、図１３に示すような画面において、顔認証以外の認証を行うサービス機関が登録済である場合にこの登録済サービスを削除することができるようになっている。この場合には、登録済サービスが未登録サービスになる。また、メモリ１６に記憶されている、削除された登録済サービスに係るサービス機関の認証エンジンに対応するユーザＩＤが削除される。

【００８７】

以上のような態様の認証システム１０によれば、図４乃至図６に示す認証システム１０や図７乃至図９に示す認証システム１０では、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をユーザの識別情報としてメモリ１６に記憶させる情報取得手段１７と、ユーザ認証時に、サービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量または撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けたユーザの顔画像の特徴量と、メモリ１６に記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う認証手段１５と、顔認証以外の認証を行うサービス機関の認証エンジン３０Ｄで用いられるユーザの識別情報と、メモリ１６に記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段１９とを備えている。このような認証システム１０によれば、登録された顔画像のデータ（具体的には、ユーザの顔画像の特徴量）を、顔認証以外の認証を行う認証エンジン３０Ｄで使用することにより利便性を向上させることができる。

【００８８】

また、図１乃至図３に示す認証システム１０では、認証システム１０は、ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をユーザの識別情報としてメモリ１６に記憶させる情報取得手段１７と、各サービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいてユーザの顔画像に基づく認証を行わせるために、メモリ１６に記憶されている、ユーザの顔画像の特徴量に係る情報を各

サービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信する送信手段としての通信部１８と、顔認証以外の認証を行うサービス機関の認証エンジン３０Ｄで用いられるユーザの識別情報と、メモリ１６に記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段１９とを備えている。このような認証システム１０でも、登録された顔画像のデータ（具体的には、ユーザの顔画像の特徴量）を、顔認証以外の認証を行う認証エンジン３０Ｄで使用することにより利便性を向上させることができる。

【００８９】

また、本実施の形態の認証システム１０では、顔認証以外の認証を行うサービス機関の認証エンジン３０Ｄで用いられるユーザの識別情報は、ユーザが所持するユーザ端末の識別情報、ユーザの顔以外の生体情報から得られる情報、ユーザによりユーザ端末に入力されたコードまたはパスワードからなる群のうち少なくとも何れかを含んでいる。

【００９０】

また、本実施の形態の認証システム１０では、サービス機関の認証エンジンの追加を行う旨の指示をユーザ端末から受け付けると、紐づけ手段１９は、追加されたサービス機関の認証エンジンの認証で用いられるユーザの識別情報と、メモリ１６に記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける。

【００９１】

また、本実施の形態の認証システム１０では、紐づけ手段１９によるユーザの識別情報の紐づけが行われた後でも、各サービス機関の認証エンジンで用いられるユーザの識別情報はそのまま残される。

【００９２】

また、図４乃至図６に示す認証システム１０や図７乃至図９に示す認証システム１０による情報処理方法では、ユーザ登録時に、ユーザの顔画像データをユーザ端末２０から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をユーザの識別情報としてメモリ１６に記憶させる工程と、ユーザ認証時に、サービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けたユーザの顔画像の特徴量と、メモリ１６に記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う工程と、顔認証以外の認証を行うサービス機関の認証エンジン３０Ｄで用いられるユーザの識別情報と、メモリ１６に記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける工程と、を備えている。このような情報処理方法によれば、登録された顔画像のデータ（具体的には、ユーザの顔画像の特徴量）を、顔認証以外の認証を行う認証エンジン３０Ｄで使用することにより利便性を向上させることができる。

【００９３】

また、図１乃至図３に示す認証システム１０による情報処理方法では、ユーザ登録時に、ユーザの顔画像データをユーザ端末２０から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をユーザの識別情報としてメモリ１６に記憶させる工程と、各サービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいてユーザの顔画像に基づく認証を行わせるために、メモリ１６に記憶されている、ユーザの顔画像の特徴量に係る情報を各サービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信する工程と、顔認証以外の認証を行うサービス機関の認証エンジン３０Ｄで用いられるユーザの識別情報と、メモリ１６に記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける工程と、を備えている。このような情報処理方法でも、登録された顔画像のデータ（具体的には、ユーザの顔画像の特徴量）を、顔認証以外の認証を行う認証エンジン３０Ｄで使用することにより利便性を向上させることができる。

【００９４】

また、更に別の例として、図１７に示す認証システム１０が用いられてもよい。図１７

に示す認証システム１０や各撮像ユニット３０Ａ、３０Ｂ、３０Ｃについて、図１、図４、図７に示す認証システム１０や各撮像ユニット３０Ａ、３０Ｂ、３０Ｃと同じ構成要素については同じ参照符号を付けてその説明を省略する。

【００９５】

図１７に示すように、認証システム１０のプロセッサ１２は、ユーザ端末２０から受け取った顔画像データを登録する登録手段１３と、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ～３８Ｃに撮像されたユーザの顔画像データに基づいてユーザの認証を行う認証手段１５とを有している。プロセッサ１２は、メモリ１６に記憶されているプログラムを実行することにより、登録手段１３に登録されたユーザの顔画像データを、ユーザの識別情報および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けてメモリ１６に記憶させるようになっている。また、プロセッサ１２は、メモリ１６に記憶されているプログラムを実行することにより、認証手段１５において、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ～３８Ｃに撮像されたユーザの顔画像データと、メモリ１６に記憶されているユーザの顔画像データとを比較することにより、ユーザの認証を行うようになっている。なお、プロセッサ１２により実行されるプログラムはメモリ１６に記憶されているものに限定されることはない。外部装置から認証システム１０に送信されたプログラムや、認証システム１０に着脱自在に装着される記録媒体に記憶されているプログラムをプロセッサ１２が実行することにより、登録手段１３および認証手段１５の各々において処理が行われてもよい。また、本実施の形態では、登録手段１３により情報取得手段１７が構成される。情報取得手段１７は、ユーザ登録時に、ユーザの顔画像データを受け付け、受け付けたユーザの顔画像データをユーザの識別情報としてメモリ１６に記憶させる。

【００９６】

各サービス機関に配置される撮像ユニット３０Ａ、３０Ｂ、３０Ｃの各々は例えばコンピュータ等から構成されており、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃは、ＣＰＵ等のプロセッサ３２Ａ、３２Ｂ、３２Ｃと、メモリ３６Ａ、３６Ｂ、３６Ｃと、撮像部３８Ａ、３８Ｂ、３８Ｃと、処理部４０Ａ、４０Ｂ、４０Ｃと、通信部４２Ａ、４２Ｂ、４２Ｃとを有している。

【００９７】

図１７に示す例でも、認証システム１０および各サービス機関に配置される撮像ユニット３０Ａ、３０Ｂ、３０ＣはＡＰＩ連携（アプリケーション・プログラミング・インターフェース）が行われている。これにより、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃのシステムを、それぞれ独立して構成したものに比べて、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃのシステムを容易に構成することができる。

【００９８】

次に、図１７に示すような認証システム１０および各撮像ユニット３０Ａ、３０Ｂ、３０Ｃによりユーザの認証を行う際の処理内容について簡単に説明する。

【００９９】

まず、ユーザがユーザ端末２０を用いて顔画像データを認証システム１０に登録する処理について説明する。なお、ユーザがユーザ端末２０により顔画像を撮像する具体的な方法については既に説明したためここでは省略する。ユーザがユーザ端末２０においてこのような顔認証アプリで最初にユーザ登録を行うと、ユーザ登録画面で入力された様々な情報およびユーザの顔画像データがユーザ端末２０から認証システム１０に送信される。このようにして、認証システム１０のプロセッサ１２はユーザ端末２０から顔画像データを受け取る。また、ユーザ端末２０の識別情報、およびユーザ端末２０に入力されたユーザの氏名、生年月日、電話番号、メールアドレス、パスワード等の登録情報も、認証システム１０のプロセッサ１２はユーザ端末２０から受け取る。また、プロセッサ１２はユーザの識別情報としてユーザＩＤを発行し、この発行されたユーザＩＤをメモリ１６に記憶させる。

【０１００】

次に、認証システム１０のプロセッサ１２は、ユーザ端末２０から受け取った顔画像データを、登録手段１３により認証システム１０のメモリ１６にユーザＩＤ（ユーザの識別情報）および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報に関連付けて記憶させる。このようにして、ユーザ端末２０により撮像されたユーザの顔画像の登録が完了する。なお、図１７に示す例では、メモリ１６に記憶されたユーザの顔画像データは、認証システム１０から、ユーザにより選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信されない。

【０１０１】

次に、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃにおいてユーザの認証を行う処理について説明する。各撮像ユニット３０Ａ、３０Ｂ、３０Ｃが設置されるサービス機関においてユーザの認証が必要となった場合には、まず、撮像ユニット３０Ａ、３０Ｂ、３０Ｃの撮像部３８Ａ、３８Ｂ、３８Ｃによりユーザを撮像することによってユーザの顔画像データを取得する。撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、撮像部３８Ａ、３８Ｂ、３８Ｃにより撮像されたユーザの顔画像データを通信部４２Ａ、４２Ｂ、４２Ｃにより認証システム１０のプロセッサ１２に送信する。なお、認証システム１０のプロセッサ１２が撮像ユニット３０Ａ、３０Ｂ、３０Ｃからユーザの顔画像データを受け付ける際に、メモリ１６に記憶されている、ユーザにより選択されたサービス機関の撮像ユニット３０Ａ、３０Ｂ、３０Ｃのみから送信されたユーザの顔画像データを受け付ける。そして、認証システム１０において、プロセッサ１２は、撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けた顔画像データと、メモリ１６に記憶されているユーザの顔画像データとを認証手段１５によって比較することによりユーザの認証を行う。より詳細に説明すると、撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けたユーザの顔画像データと、メモリ１６に記憶されているユーザの顔画像データとの一致率が所定の閾値（例えば、８０％）を超える場合には、認証手段１５はユーザの認証を行う。なお、上述したように、メモリ１６には、予め登録されたユーザの識別情報および撮像ユニット３０Ａ、３０Ｂ、３０Ｃの識別情報と、ユーザの顔画像データとが関連付けて記憶されている。

【０１０２】

そして、認証手段１５によりユーザの認証が行われると、認証結果に係る情報が認証システム１０のプロセッサ１２から通信部１８により撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される。そして、認証結果に係る情報を受け取った撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、各処理部４０Ａ、４０Ｂ、４０Ｃによりこの撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するサービスを実施可能とする。その後、撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、サービスの利用状況に係る情報を認証システム１０に送信する。このことにより、認証システム１０において各サービス機関におけるサービスの利用状況に係る情報がユーザ毎にメモリ１６に記憶される。

【０１０３】

一方、撮像ユニット３０Ａ、３０Ｂ、３０Ｃから受け付けたユーザの顔画像データが、メモリ１６に記憶されているユーザの顔画像データに略一致せず、認証手段１５によりユーザの認証を行うことができなかった場合にも、認証結果に係る情報が認証システム１０のプロセッサ１２から通信部１８により撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される（ＳＴＥＰ５８）。そして、認証結果に係る情報を受け取った撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは各処理部４０Ａ、４０Ｂ、４０Ｃによりこの撮像ユニット３０Ａ、３０Ｂ、３０Ｃに対応するサービスを実施不可とする。この場合も、撮像ユニット３０Ａ、３０Ｂ、３０Ｃのプロセッサ３２Ａ、３２Ｂ、３２Ｃは、サービスの利用状況に係る情報（具体的には、ユーザが撮像ユニット３０Ａ、３０Ｂ、３０Ｃで認証を行おうとしたが認証されずにサービスを利用できなかったという情報）を認証システム１０に送信する。

【０１０４】

このような認証方法によれば、ユーザの顔画像データがあるサービス機関の認証エンジン（例えば、撮像ユニット３０Ａ）で登録されているが、別のサービス機関の認証エンジン（例えば、撮像ユニット３０Ｂ）で登録されていない場合でも、認証システム１０のメモリ１６にこのユーザの顔画像データを記憶させておくことにより、ユーザの顔画像データが登録されていないサービス機関でも撮像部によりユーザの顔画像を撮像することによってユーザの認証を行うことができる。この場合には、複数の認証エンジンの全てでユーザは顔画像データの登録を行う必要がなくなるので、ユーザの手間を省くことができるようになる。

【０１０５】

また、図１７に示す認証システム１０でも紐づけ手段１９が設けられている。紐づけ手段１９は、顔認証以外の認証を行うサービス機関の認証エンジン３０Ｄで用いられるユーザの識別情報と、メモリ１６に記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける。このような認証システム１０によれば、登録された顔画像のデータ（具体的には、ユーザの顔画像データ）を、顔認証以外の認証を行う認証エンジン３０Ｄで使用することにより利便性を向上させることができる。

【０１０６】

また、更なる変形例において、図１乃至図３に示すような認証システム１０では、各撮像ユニット３０Ａ、３０Ｂ、３０Ｃの認証手段３５Ａ、３５Ｂ、３５Ｃは、ユーザの顔画像の特徴量ではなくユーザの顔画像データを用いてユーザの認証を行うようになっていてもよい。この場合、認証システム１０で登録されたユーザの顔画像データが各撮像ユニット３０Ａ、３０Ｂ、３０Ｃに送信される。また、この場合、図１乃至図３に示すような認証システム１０の紐づけ手段１９は、顔認証以外の認証を行うサービス機関の認証エンジン３０Ｄで用いられるユーザの識別情報と、メモリ１６に記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける。このような認証システム１０でも、登録された顔画像のデータ（具体的には、ユーザの顔画像の特徴量）を、顔認証以外の認証を行う認証エンジン３０Ｄで使用することにより利便性を向上させることができる。

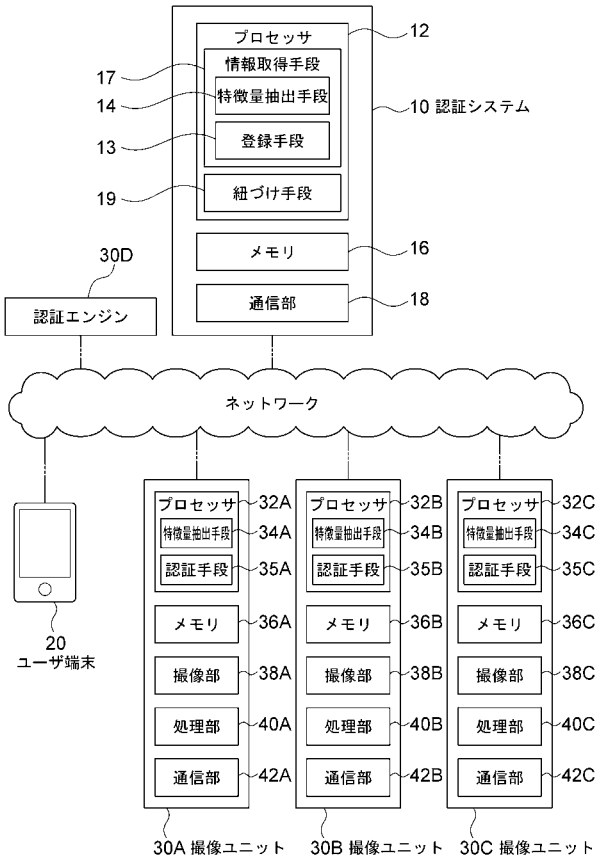
【符号の説明】

【０１０７】

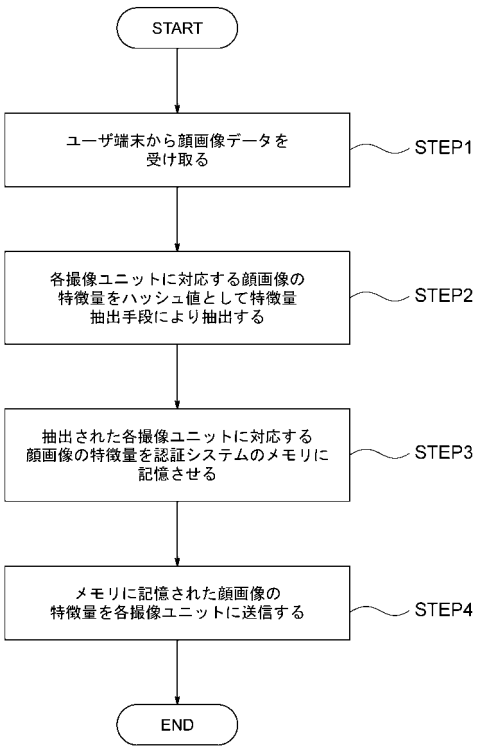
１０　認証システム
１２　プロセッサ
１３　登録手段
１４　特徴量抽出手段
１５　認証手段
１６　メモリ
１７　情報取得手段
１８　通信部
１９　紐づけ手段
２０　ユーザ端末
３０Ａ、３０Ｂ、３０Ｃ　撮像ユニット
３０Ｄ　認証エンジン
３２Ａ、３２Ｂ、３２Ｃ　プロセッサ
３４Ａ、３４Ｂ、３４Ｃ　特徴量抽出手段
３５Ａ、３５Ｂ、３５Ｃ　認証手段
３６Ａ、３６Ｂ、３６Ｃ　メモリ
３８Ａ、３８Ｂ、３８Ｃ　撮像部
４０Ａ、４０Ｂ、４０Ｃ　処理部
４２Ａ、４２Ｂ、４２Ｃ　通信部
５０　認証システム
５２　プロセッサ
５２ａ　サーバ管理手段

５３　登録手段
５４　特徴量抽出手段
５５　認証手段
５６　第１サーバ
５８　第２サーバ
６０　第３サーバ

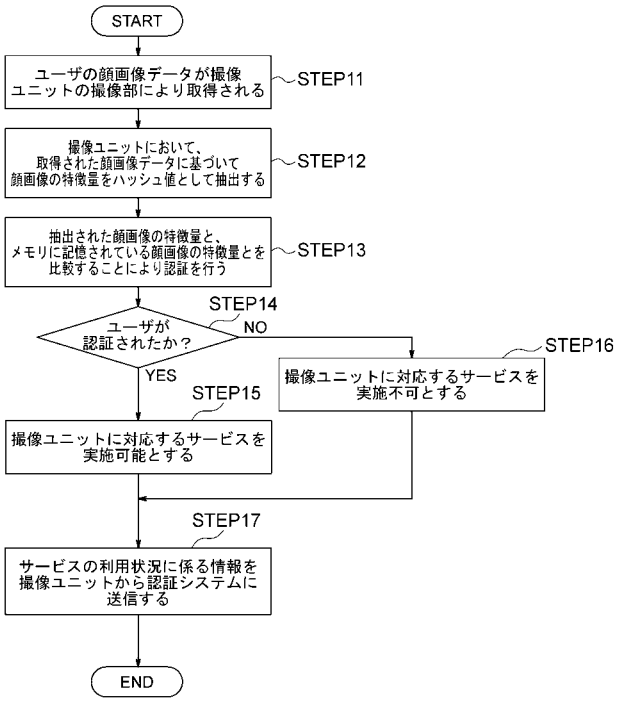
【図１】



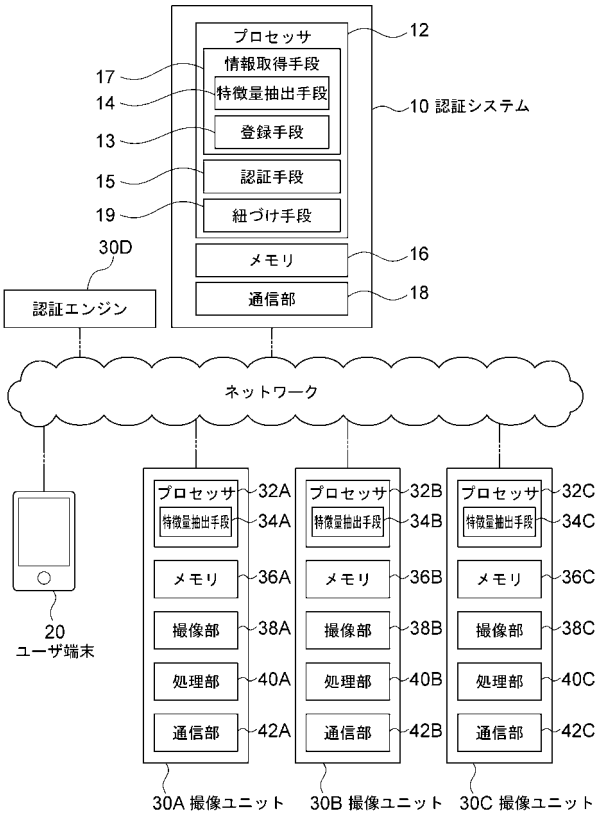
【図２】



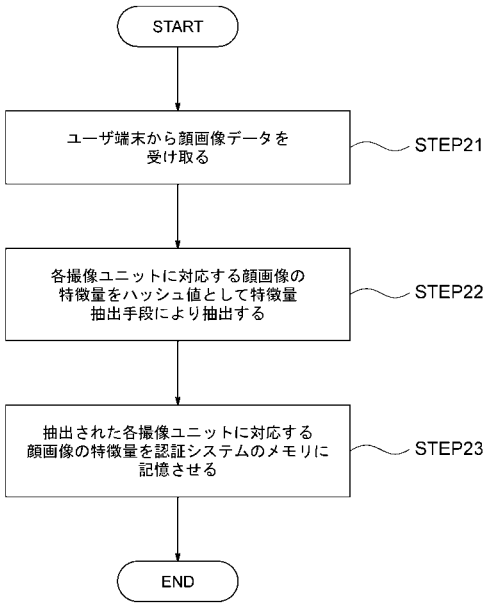
【図３】


START
ユーザの顔画像データが撮像ユニットの撮像部により取得される
STEP11
撮像ユニットにおいて、取得された顔画像データに基づいて顔画像の特徴量をハッシュ値として抽出する
STEP12
抽出された顔画像の特徴量と、メモリに記憶されている顔画像の特徴量とを比較することにより認証を行う
STEP13
STEP14
ユーザが認証されたか？
NO
YES
STEP16
撮像ユニットに対応するサービスを実施不可とする
STEP15
撮像ユニットに対応するサービスを実施可能とする
STEP17
サービスの利用状況に係る情報を撮像ユニットから認証システムに送信する
END

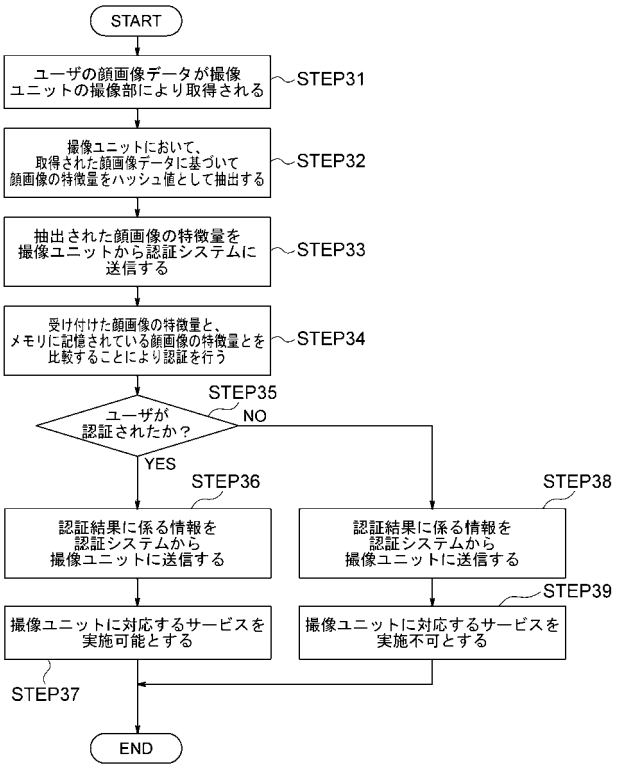
【図４】


プロセッサ
12
情報取得手段
17
特徴量抽出手段
14
登録手段
13
認証手段
15
紐づけ手段
19
10 認証システム
メモリ
16
通信部
18
30D
認証エンジン
ネットワーク
20
ユーザ端末
プロセッサ
32A
特徴量抽出手段
34A
メモリ
36A
撮像部
38A
処理部
40A
通信部
42A
30A 撮像ユニット
32B
34B
36B
38B
40B
42B
30B 撮像ユニット
32C
34C
36C
38C
40C
42C
30C 撮像ユニット

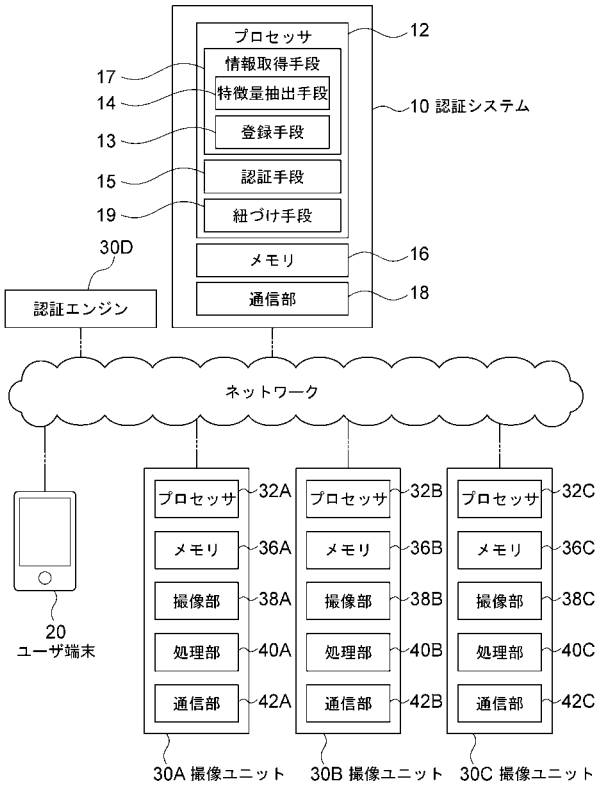
【図５】


START
ユーザ端末から顔画像データを受け取る
STEP21
各撮像ユニットに対応する顔画像の特徴量をハッシュ値として特徴量抽出手段により抽出する
STEP22
抽出された各撮像ユニットに対応する顔画像の特徴量を認証システムのメモリに記憶させる
STEP23
END

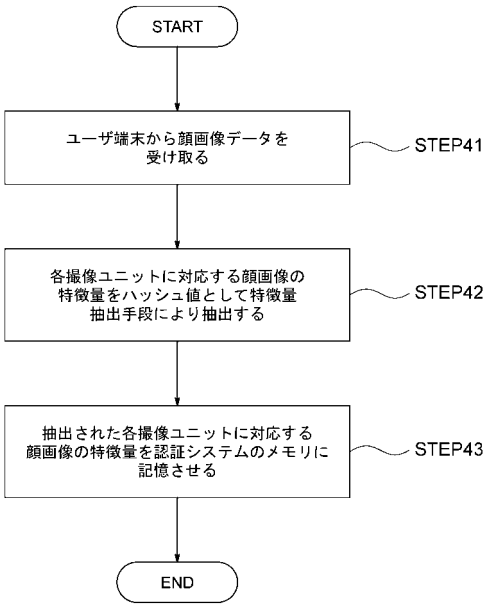
【図６】


START
ユーザの顔画像データが撮像ユニットの撮像部により取得される
STEP31
撮像ユニットにおいて、取得された顔画像データに基づいて顔画像の特徴量をハッシュ値として抽出する
STEP32
抽出された顔画像の特徴量を撮像ユニットから認証システムに送信する
STEP33
受け付けた顔画像の特徴量と、メモリに記憶されている顔画像の特徴量とを比較することにより認証を行う
STEP34
STEP35
ユーザが認証されたか？
NO
YES
STEP36
認証結果に係る情報を認証システムから撮像ユニットに送信する
STEP38
認証結果に係る情報を認証システムから撮像ユニットに送信する
STEP39
撮像ユニットに対応するサービスを実施可能とする
撮像ユニットに対応するサービスを実施不可とする
STEP37
END

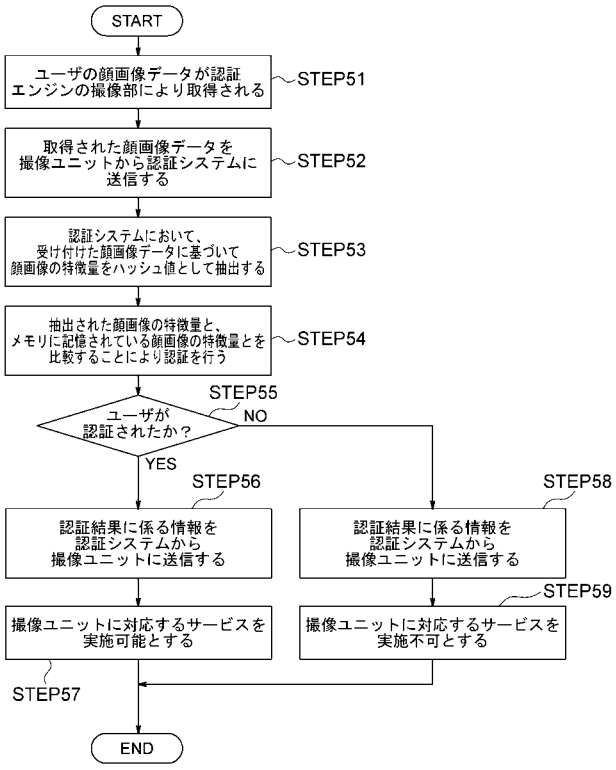
【図７】



【図８】



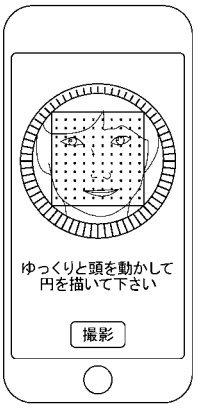
【図９】



【図１０】

【図１１】

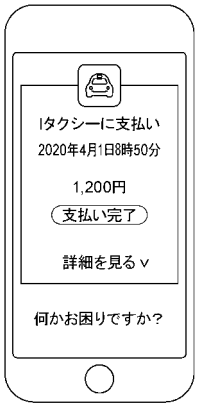
【図１２】



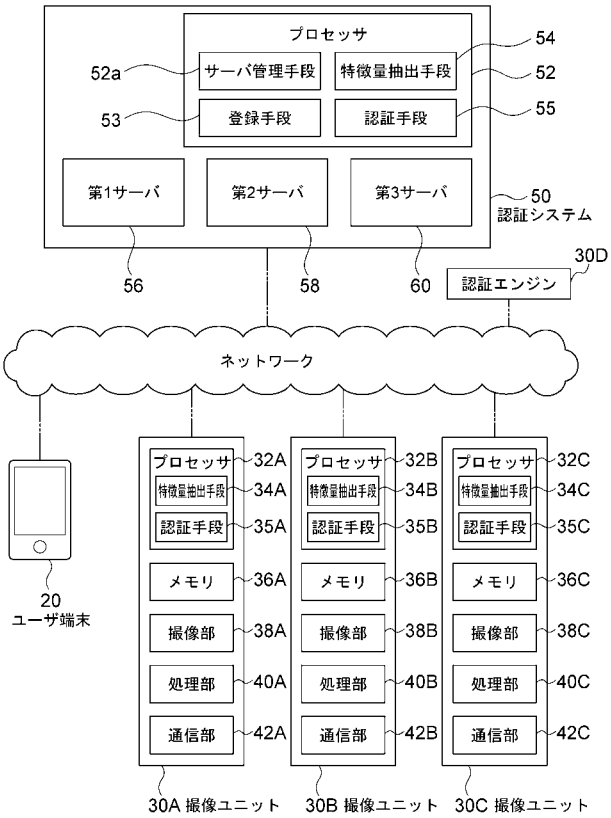
【図１３】

【図１４】

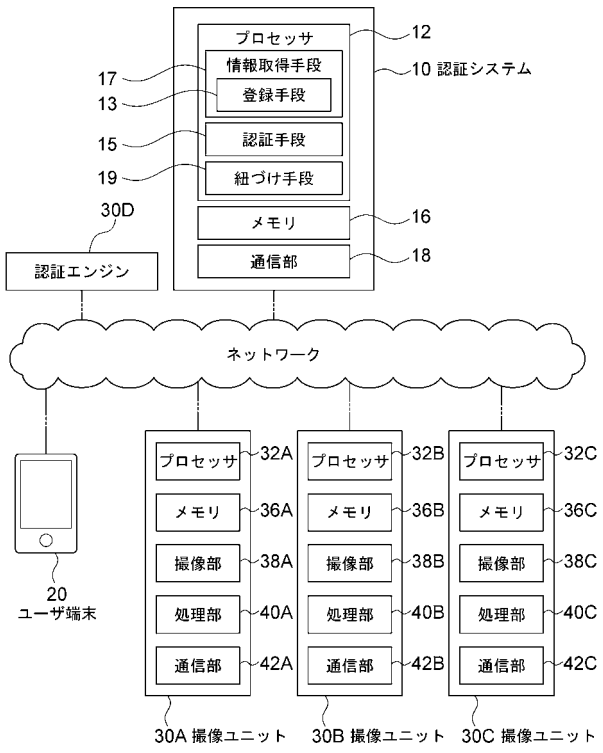
【図１５】



【図１６】



【図１７】



【手続補正書】
【提出日】令和3年2月2日(2021.2.2)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる情報取得手段と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの顔認証を行う認証手段と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われる、認証システム。
【請求項２】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる情報取得手段と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像の特徴量に係る情報を各サービス機関の撮像ユニットに送信する送信手段と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われる、認証システム。
【請求項３】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる情報取得手段と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データと、前記メモリに記憶されているユーザの顔画像データとを比較することによってユーザの認証を行う認証手段と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づけ

る紐づけ手段と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われる、認証システム。
【請求項４】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる情報取得手段と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像データを各サービス機関の撮像ユニットに送信する送信手段と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける紐づけ手段と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われる、認証システム。
【請求項５】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる工程と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける工程と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われる、情報処理方法。
【請求項６】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる工程と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像の特徴量に係る情報を各サービス機関の撮像ユニットに送信する工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づ

ける工程と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われる、情報処理方法。
【請求項７】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる工程と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データと、前記メモリに記憶されているユーザの顔画像データとを比較することによってユーザの認証を行う工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける工程と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われる、情報処理方法。
【請求項８】
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる工程と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像データを各サービス機関の撮像ユニットに送信する工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける工程と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われる、情報処理方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００７
【補正方法】変更
【補正の内容】
【０００７】
本発明の認証システムは、
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる情報取得手段と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データか

ら抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの顔認証を行う認証手段と、

顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段と、

を備え、

サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われることを特徴とする。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正の内容】
【０００８】

本発明の認証システムは、

ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、

ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる情報取得手段と、

各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像の特徴量に係る情報を各サービス機関の撮像ユニットに送信する送信手段と、

顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける紐づけ手段と、

を備え、

サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われることを特徴とする。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】削除
【補正の内容】
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】変更
【補正の内容】
【００１０】

本発明の認証システムは、

ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、

ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる情報取得手段と、

ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データと、前記メモリに記憶されているユーザの顔画像データとを比較することによってユーザの

認証を行う認証手段と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける紐づけ手段と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われることを特徴とする。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正の内容】
【００１１】
本発明の認証システムは、
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムであって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる情報取得手段と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像データを各サービス機関の撮像ユニットに送信する送信手段と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける紐づけ手段と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われることを特徴とする。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
本発明の情報処理方法は、
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる工程と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データから抽出されたユーザの顔画像の特徴量またはサービス機関の撮像ユニットから受け付けたユーザの顔画像の特徴量と、前記メモリに記憶されているユーザの顔画像の特徴量とを比較することによってユーザの認証を行う工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける工程と、
を備え、

サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われることを特徴とする。

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】変更
【補正の内容】
【００１３】
本発明の情報処理方法は、
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データに基づいてこのユーザの顔画像の特徴量を抽出し、抽出されたユーザの顔画像の特徴量に係る情報をメモリに記憶させる工程と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像の特徴量に係る情報を各サービス機関の撮像ユニットに送信する工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像の特徴量に係るユーザの識別情報とを紐づける工程と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われることを特徴とする。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００１４
【補正方法】削除
【補正の内容】
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００１５
【補正方法】変更
【補正の内容】
【００１５】
本発明の情報処理方法は、
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる工程と、
ユーザ認証時に、サービス機関の撮像ユニットから受け付けたユーザの顔画像データと、前記メモリに記憶されているユーザの顔画像データとを比較することによってユーザの認証を行う工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける工程と、
を備え、

サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われることを特徴とする。

【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正の内容】
【００１６】
本発明の情報処理方法は、
ユーザ端末から受け付けた情報を用いてユーザの認証を行う認証システムによる情報処理方法であって、
ユーザ登録時に、ユーザの顔画像データをユーザ端末から受け付け、受け付けたユーザの顔画像データをメモリに記憶させる工程と、
各サービス機関の撮像ユニットにおいてユーザの顔画像に基づく認証を行わせるために、前記メモリに記憶されている、ユーザの顔画像データを各サービス機関の撮像ユニットに送信する工程と、
顔認証以外の認証を行うサービス機関の認証エンジンで用いられるユーザの識別情報と、前記メモリに記憶されているユーザの顔画像データに係るユーザの識別情報とを紐づける工程と、
を備え、
サービス機関の種類によって異なる強度の認証が設定されており、ある種類のサービス機関では前記認証手段による顔認証に基づいてユーザの認証が行われ、別の種類のサービス機関では前記認証手段による顔認証に加えて生体認証以外の情報を用いることによりユーザの認証が行われることを特徴とする。