(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7512584号
(P7512584)

(45)発行日　令和6年7月9日(2024.7.9)

(24)登録日　令和6年7月1日(2024.7.1)

(51)国際特許分類

Ｇ０６Ｆ　21/32　(2013.01)	Ｇ０６Ｆ	21/32		
Ｇ０６Ｆ　21/33　(2013.01)	Ｇ０６Ｆ	21/33		
Ｇ０９Ｃ　1/00　(2006.01)	Ｇ０９Ｃ	1/00	６４０Ｅ	
Ｈ０４Ｌ　9/32　(2006.01)	Ｈ０４Ｌ	9/32	２００Ｂ	

FI

請求項の数　10　（全29頁）

(21)出願番号　特願2019-206034(P2019-206034)
(22)出願日　令和1年11月14日(2019.11.14)
(65)公開番号　特開2020-87460(P2020-87460A)
(43)公開日　令和2年6月4日(2020.6.4)
審査請求日　令和4年9月27日(2022.9.27)
(31)優先権主張番号　特願2018-213524(P2018-213524)
(32)優先日　平成30年11月14日(2018.11.14)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100106002
弁理士　正林 真之
(74)代理人　100165157
弁理士　芝 哲央
(74)代理人　100120891
弁理士　林 一好
(72)発明者　松田 薫平
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　稲垣 将太
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

最終頁に続く

(54)【発明の名称】　本人認証システム、認証器、プログラム及び本人認証方法

(57)【特許請求の範囲】

【請求項１】

ユーザが所持する撮影部を備えた認証器と、

前記認証器に対して通信可能に接続された本人認証サーバと、

を備えた本人認証システムであって、

前記認証器は、

ユーザの本人確認の際に、本人確認書類に有する顔写真を含む面に対して垂直の撮影方向を含む、前記顔写真を確認可能な複数の異なる撮影方向から前記本人確認書類を撮影した前記本人確認書類の画像である複数の本人確認画像を、前記撮影部から取得する本人確認画像取得手段と、

前記本人確認画像に含まれる顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、照合画像記憶部に記憶させる画像記憶処理手段と、

サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合手段と、

前記顔画像照合手段による照合結果を、前記本人認証サーバに送信する照合結果送信手段と、

を備え、

前記本人認証サーバは、前記照合結果に基づいて、サービスの利用を許可する許可手段を備えること、

を特徴とする本人認証システム。
【請求項２】
ユーザが所持する撮影部を備えた認証器と、
前記認証器に対して通信可能に接続された本人認証サーバと、
を備えた本人認証システムであって、
前記認証器は、
ユーザの本人確認の際に、本人確認書類に有する顔写真を含む面に対して垂直の撮影方向を含む、前記顔写真を確認可能な複数の異なる撮影方向から前記本人確認書類を撮影した前記本人確認書類の画像である複数の本人確認画像を、前記撮影部から取得する本人確認画像取得手段と、
前記本人確認画像取得手段が取得した前記複数の本人確認画像のうち少なくとも１つの前記本人確認画像に含まれる顔写真画像を記憶部に記憶する手段と、
前記記憶する手段により前記記憶部に記憶された、前記本人確認画像に含まれる前記顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、前記本人確認ができたことに応じて前記記憶部から照合画像記憶部に記憶させる画像記憶処理手段と、
サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合手段と、
前記顔画像照合手段による照合結果を、前記本人認証サーバに送信する照合結果送信手段と、
を備え、
前記本人認証サーバは、前記照合結果に基づいて、サービスの利用を許可する許可手段を備えること、
を特徴とする本人認証システム。
【請求項３】
請求項１又は請求項２に記載の本人認証システムにおいて、
前記認証器は、
秘密鍵及び公開鍵からなる鍵ペアを生成する鍵生成手段と、
前記鍵生成手段により生成した前記鍵ペアに含まれる前記公開鍵を、前記本人認証サーバに送信する鍵送信手段と、
を備え、
前記照合結果送信手段は、前記鍵生成手段により生成した前記鍵ペアに含まれる前記秘密鍵で署名した前記照合結果を送信し、
前記本人認証サーバは、
前記公開鍵を受信して記憶部に記憶する鍵記憶手段を備え、
前記許可手段は、受信した前記照合結果を、前記鍵記憶手段が記憶した前記公開鍵で署名検証し、署名検証できた場合に、サービスの利用を許可すること、
を特徴とする本人認証システム。
【請求項４】
請求項３に記載の本人認証システムにおいて、
前記認証器は、前記本人認証サーバに、利用開始要求を送信する要求送信手段を備え、
前記本人認証サーバは、前記利用開始要求を受信したことに応じて、乱数を利用して発生させたチャレンジコードを送信するコード送信手段を備え、
前記認証器の前記照合結果送信手段は、前記顔画像照合手段により照合できた場合に、前記チャレンジコードを前記秘密鍵で署名した前記照合結果を送信すること、
を特徴とする本人認証システム。
【請求項５】
ユーザが所持する、撮影部を備えた認証器であって、
ユーザの本人確認の際に、本人確認書類に有する顔写真を含む面に対して垂直の撮影方向を含む、前記顔写真を確認可能な複数の異なる撮影方向から前記本人確認書類を撮影し

た前記本人確認書類の画像である複数の本人確認画像を、前記撮影部から取得する本人確認画像取得手段と、
前記本人確認画像に含まれる顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、照合画像記憶部に記憶させる画像記憶処理手段と、
サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合手段と、
前記顔画像照合手段による照合結果を、通信可能に接続され本人認証を行う本人認証サーバに送信する照合結果送信手段と、
を備えること、
を特徴とする認証器。
【請求項６】
ユーザが所持する、撮影部を備えた認証器であって、
ユーザの本人確認の際に、本人確認書類に有する顔写真を含む面に対して垂直の撮影方向を含む、前記顔写真を確認可能な複数の異なる撮影方向から前記本人確認書類を撮影した前記本人確認書類の画像である複数の本人確認画像を、前記撮影部から取得する本人確認画像取得手段と、
前記本人確認画像取得手段が取得した前記複数の本人確認画像のうち少なくとも１つの前記本人確認画像に含まれる顔写真画像を記憶部に記憶する手段と、
前記記憶する手段により前記記憶部に記憶された、前記本人確認画像に含まれる前記顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、前記本人確認ができたことに応じて前記記憶部から照合画像記憶部に記憶させる画像記憶処理手段と、
サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合手段と、
前記顔画像照合手段による照合結果を、通信可能に接続され本人認証を行う本人認証サーバに送信する照合結果送信手段と、
を備えること、
を特徴とする認証器。
【請求項７】
ユーザが所持する、撮影部を備えたコンピュータを、
ユーザの本人確認の際に、本人確認書類に有する顔写真を含む面に対して垂直の撮影方向を含む、前記顔写真を確認可能な複数の異なる撮影方向から前記本人確認書類を撮影した前記本人確認書類の画像である複数の本人確認画像を、前記撮影部から取得する本人確認画像取得手段と、
前記本人確認画像に含まれる顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、照合画像記憶部に記憶させる画像記憶処理手段と、
サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合手段と、
前記顔画像照合手段による照合結果を、通信可能に接続され本人認証を行う本人認証サーバに送信する照合結果送信手段と、
して機能させるためのプログラム。
【請求項８】
ユーザが所持する、撮影部を備えたコンピュータを、
ユーザの本人確認の際に、本人確認書類に有する顔写真を含む面に対して垂直の撮影方向を含む、前記顔写真を確認可能な複数の異なる撮影方向から前記本人確認書類を撮影した前記本人確認書類の画像である複数の本人確認画像を、前記撮影部から取得する本人確認画像取得手段と、
前記本人確認画像取得手段が取得した前記複数の本人確認画像のうち少なくとも１つの前

記本人確認画像に含まれる顔写真画像を記憶部に記憶する手段と、
前記記憶する手段により前記記憶部に記憶された、前記本人確認画像に含まれる前記顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、前記本人確認ができたことに応じて前記記憶部から照合画像記憶部に記憶させる画像記憶処理手段と、
サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合手段と、
前記顔画像照合手段による照合結果を、通信可能に接続され本人認証を行う本人認証サーバに送信する照合結果送信手段と、
して機能させるためのプログラム。

【請求項９】
ユーザが所持する撮影部を備えた認証器が、前記認証器に対して通信可能に接続された本人認証サーバを用いた本人認証の前に行うユーザの本人確認の際に、本人確認書類に有する顔写真を含む面に対して垂直の撮影方向を含む、前記顔写真を確認可能な複数の異なる撮影方向から前記本人確認書類を撮影した前記本人確認書類の画像である複数の本人確認画像を、前記撮影部から取得する本人確認画像取得ステップと、
前記認証器が、前記本人確認画像に含まれる顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、照合画像記憶部に記憶させる画像記憶ステップと、
前記認証器が、サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合ステップと、
前記認証器が、前記顔画像照合ステップによる照合結果を、前記本人認証サーバに送信する照合結果送信ステップと、
を含み、
前記本人認証サーバが、前記照合結果に基づいて、サービスの利用を許可する許可ステップを含むこと、
を特徴とする本人認証方法。

【請求項１０】
ユーザが所持する撮影部を備えた認証器が、前記認証器に対して通信可能に接続された本人認証サーバを用いた本人認証の前に行うユーザの本人確認の際に、本人確認書類に有する顔写真を含む面に対して垂直の撮影方向を含む、前記顔写真を確認可能な複数の異なる撮影方向から前記本人確認書類を撮影した前記本人確認書類の画像である複数の本人確認画像を、前記撮影部から取得する本人確認画像取得ステップと、
前記認証器が、前記本人確認画像取得ステップが取得した前記複数の本人確認画像のうち少なくとも１つの前記本人確認画像に含まれる顔写真画像を記憶部に記憶するステップと、
前記認証器が、前記記憶するステップにより前記記憶部に記憶された、前記本人確認画像に含まれる前記顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、前記本人確認ができたことに応じて前記記憶部から照合画像記憶部に記憶させる画像記憶ステップと、
前記認証器が、サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合ステップと、
前記認証器が、前記顔画像照合ステップによる照合結果を、前記本人認証サーバに送信する照合結果送信ステップと、
を含み、
前記本人認証サーバが、前記照合結果に基づいて、サービスの利用を許可する許可ステップを含むこと、
を特徴とする本人認証方法。

【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、本人認証システム、認証器、プログラム及び本人認証方法に関する。
【背景技術】
【０００２】
従来、銀行等において、インターネット等の通信ネットワークを介して、顧客に対していわゆるインターネットバンキングのサービスを提供することが行われている。インターネットバンキングのサービスでは、携帯端末等の顧客が所持する端末を使用して本人であることの確認を行うために、例えば、生体情報を利用したものが考えられている。一例として、免許証等のＩＣカードに記憶された顔画像と、端末の操作者である顧客の顔画像とを用いた顔認証により、本人確認を行う方法が開示されている（例えば、特許文献１）。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開２０１５－８８０８０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
特許文献１に記載のものは、ＩＣカードのチップに記憶された顔画像データを用いるものであるため、情報端末には、ＩＣカードを読み取るためのリーダを備えている必要があった。
また、サービス利用時には、本人確認がされたユーザのみの利用を許容するために、毎回本人認証を行う必要がある。特許文献１に記載のものは、顔画像を用いた顔認証をサーバ側で行っているが、顔画像に代表される生体情報が、サービスを利用する都度、通信回線を介して送信されることになるため、データのセキュリティ性に問題があった。
【０００５】
そこで、本発明は、セキュリティ性を向上させた本人認証システム、認証器、プログラム及び本人認証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】
【０００６】
本発明は、以下のような解決手段により、前記課題を解決する。なお、理解を容易にするために、本発明の実施形態に対応する符号を付して説明するが、これに限定されるものではない。また、符号を付して説明した構成は、適宜改良してもよく、また、少なくとも一部を他の構成物に代替してもよい。
【０００７】
第１の発明は、ユーザが所持する撮影部（３４）を備えた認証器（１）と、前記認証器に対して通信可能に接続された本人認証サーバ（４）と、を備えた本人認証システム（１００）であって、前記認証器は、ユーザの本人確認の際に前記撮影部を介して取得した、本人確認書類（３）の画像である本人確認画像に含まれる顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、照合画像記憶部（３２）に記憶させる画像記憶処理手段（１６ａ）と、サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合手段（１８）と、前記顔画像照合手段による照合結果を、前記本人認証サーバに送信する照合結果送信手段（１９）と、を備え、前記本人認証サーバは、前記照合結果に基づいて、サービスの利用を許可する許可手段（４４）を備えること、を特徴とする本人認証システムである。
第２の発明は、第１の発明の本人認証システム（１００）において、前記認証器（１）に対して通信可能に接続された本人確認サーバ（４）を備え、前記認証器は、前記本人確認書類（３）と、前記顔画像とを、前記本人確認サーバに対して送信することで、前記本人確認サーバに本人確認を依頼する本人確認依頼手段（１４）を備え、前記画像記憶処理手段（１６ａ）は、前記本人確認サーバから本人確認ができた旨を受信した場合に、前記照合画像を、前記照合画像記憶部（３２）に記憶させること、を特徴とする本人認証シス

テムである。
第３の発明は、第１の発明又は第２の発明の本人認証システム（１００）において、前記認証器（１）は、秘密鍵及び公開鍵からなる鍵ペアを生成する鍵生成手段（１６ｂ）と、前記鍵生成手段により生成した前記鍵ペアに含まれる前記公開鍵を、前記本人認証サーバ（４）に送信する鍵送信手段（１６ｂ）と、を備え、前記照合結果送信手段（１９）は、前記鍵生成手段により生成した前記鍵ペアに含まれる前記秘密鍵で署名した前記照合結果を送信し、前記本人認証サーバは、前記公開鍵を受信して記憶部（５３）に記憶する鍵記憶手段（４２）を備え、前記許可手段（４４）は、受信した前記照合結果を、前記鍵記憶手段が記憶した前記公開鍵で署名検証し、署名検証できた場合に、サービスの利用を許可すること、を特徴とする本人認証システムである。
第４の発明は、第３の発明の本人認証システム（１００）において、前記認証器（１）は、前記本人認証サーバ（４）に、利用開始要求を送信する要求送信手段（１７）を備え、前記本人認証サーバは、前記利用開始要求を受信したことに応じて、乱数を利用して発生させたチャレンジコードを送信するコード送信手段（４３）を備え、前記認証器の前記照合結果送信手段（１９）は、前記顔画像照合手段（１８）により照合できた場合に、前記チャレンジコードを前記秘密鍵で署名した前記照合結果を送信すること、を特徴とする本人認証システムである。
第５の発明は、ユーザが所持する、撮影部（３４）を備えた認証器（１）であって、ユーザの本人確認の際に前記撮影部を介して取得した、本人確認書類（３）の画像である本人確認画像に含まれる顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、照合画像記憶部（３２）に記憶させる画像記憶処理手段（１６ａ）と、サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合手段（１８）と、前記顔画像照合手段による照合結果を、通信可能に接続され本人認証を行う本人認証サーバ（４）に送信する照合結果送信手段（１９）と、を備えること、を特徴とする認証器である。
第６の発明は、ユーザが所持する、撮影部（３４）を備えたコンピュータ（１）を、ユーザの本人確認の際に前記撮影部を介して取得した、本人確認書類の画像である本人確認画像に含まれる顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、照合画像記憶部（３２）に記憶させる画像記憶処理手段と、サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合手段と、前記顔画像照合手段による照合結果を、通信可能に接続され本人認証を行う本人認証サーバ（４）に送信する照合結果送信手段と、して機能させるためのプログラム（３１ｃ）である。
第７の発明は、ユーザが所持する撮影部（３４）を備えた認証器（１）が、前記認証器に対して通信可能に接続された本人認証サーバ（４）を用いた本人認証の前に行うユーザの本人確認の際に前記撮影部を介して取得した、本人確認書類（３）の画像である本人確認画像に含まれる顔写真画像と、前記本人確認書類を所持した所持者の顔の画像である顔画像とのうち少なくとも一方である照合画像を、照合画像記憶部（３２）に記憶させる画像記憶ステップと、前記認証器が、サービス利用時に、前記撮影部を介してサービス利用者の顔画像を取得し、前記照合画像記憶部に記憶された前記照合画像と照合する顔画像照合ステップと、前記認証器が、前記顔画像照合ステップによる照合結果を、前記本人認証サーバに送信する照合結果送信ステップと、を含み、前記本人認証サーバが、前記照合結果に基づいて、サービスの利用を許可する許可ステップを含むこと、を特徴とする本人認証方法である。
【発明の効果】
【０００８】
本発明によれば、セキュリティ性を向上させた本人認証システム、認証器、プログラム及び本人認証方法を提供することができる。
【図面の簡単な説明】

【０００９】
【図１】第１実施形態に係る本人認証システムの全体構成を示す図である。
【図２】第１実施形態に係る携帯端末の機能ブロック図である。
【図３】第１実施形態に係る本人認証サーバの機能ブロック図である。
【図４】第１実施形態に係る携帯端末でのサービス開始処理を示すフローチャートである。
【図５】第１実施形態に係る携帯端末での本人確認処理を示すフローチャートである。
【図６】第１実施形態に係る本人認証システムでの本人確認画像処理を示すフローチャートである。
【図７】第１実施形態に係る本人認証システムでの照合画像処理を示すフローチャートである。
【図８】第１実施形態に係る本人認証システムでの本人認証処理を示すフローチャートである。
【図９】図８の続きである。
【図１０】第２実施形態に係る本人認証システムにおける携帯端末の機能ブロック図である。
【図１１】第２実施形態に係る携帯端末での本人確認処理を示すフローチャートである。
【図１２】第２実施形態に係る携帯端末での表示例を示す図である。
【図１３】第２実施形態に係る携帯端末に表示する書類位置ガイド画像の例を示す図である。
【図１４】第２実施形態に係る本人認証システムでの照合画像処理を示すフローチャートである。
【図１５】第２実施形態に係る携帯端末での照合画像の取得処理を示すフローチャートである。
【図１６】第２実施形態に係る携帯端末での表示例を示す図である。
【図１７】第２実施形態に係る本人認証システムでの本人認証処理を示すフローチャートである。
【図１８】図１７の続きである。
【図１９】第２実施形態に係る携帯端末での顔画像の取得処理を示すフローチャートである。
【発明を実施するための形態】
【００１０】
以下、本発明を実施するための形態について、図を参照しながら説明する。なお、これは、あくまでも一例であって、本発明の技術的範囲はこれに限られるものではない。
【００１１】
（第１実施形態）
図１は、第１実施形態に係る本人認証システム１００の全体構成を示す図である。
図２は、第１実施形態に係る携帯端末１の機能ブロック図である。
図３は、第１実施形態に係る本人認証サーバ４の機能ブロック図である。
図１に示す本人認証システム１００は、各種サービスにおける初回のサービス開始時に必要な本人確認を、携帯端末１（認証器）のみによって行い、２回目以降のサービス開始時に必要な本人認証を、携帯端末１のみによって安全に行うためのシステムである。
【００１２】
ここで、各種サービスとは、例えば、銀行での口座開設や各種の銀行業務に係るサービス、カーシェアサービス、不動産の賃貸等に係るサービス等であり、本人確認及び本人認証が必要な様々なサービスをいう。現在、銀行の口座開設等においての本人確認の手段としては、口座開設を申し込んだ申込本人宅に、転送不要郵便を送付することにより行われている。昨今、オンラインでの本人確認を完結させる方法が、金融機関において検討されている。本発明における本人確認とは、口座開設等の金融機関との取引を始めるにあたり、携帯端末等を利用したオンラインでの手続きを可能とするための確認処理をいい、初回のサービス開始の際に必ず行うものである。本人確認では、例えば、運転免許証等の公的

な証明書を用いた確認を行う。他方、本人認証とは、既に本人確認ができている状態であって、２回目以降のサービス開始時等に、なりすまし等を防ぐための確認をいう。

以下において、携帯端末１を使用して、本人確認や本人認証が必要なサービスを開始する場合を例に、本人認証システム１００について説明する。

【００１３】

本人認証システム１００は、携帯端末１と、本人認証サーバ４（本人確認サーバ、本人認証サーバ）とを備える。携帯端末１は、例えば、無線通信の基地局Ｒを介して通信ネットワークＮに接続可能である。また、本人認証サーバ４は、通信ネットワークＮを介して通信可能に接続されている。

本人認証システム１００は、通信ネットワークＮを介して、サービス提供サーバ７に対して接続されている。サービス提供サーバ７は、携帯端末１との間でサービス処理を行うためのサーバである。

【００１４】

携帯端末１は、例えば、サービス提供サーバ７によるサービスの提供を受けようとする者が所有する端末である。以下、サービスの提供を受けようとする者のことを、ユーザという。携帯端末１は、例えば、スマートフォンやタブレットに代表されるコンピュータの機能を併せ持った携帯型の装置である。

図２に示すように、携帯端末１は、制御部１０と、記憶部３０と、カメラ３４（撮影部）と、タッチパネルディスプレイ３５と、通信インタフェース部３９とを備える。

【００１５】

制御部１０は、携帯端末１の全体を制御するＣＰＵ（中央処理装置）である。制御部１０は、記憶部３０に記憶されているオペレーティングシステム（ＯＳ）や各種アプリケーションプログラムを適宜読み出して実行することにより、上述したハードウェアと協働し、各種機能を実行する。

制御部１０は、アプリ起動部１１と、本人確認部１２と、本人認証部１５と、サービス処理部２０とを備える。

【００１６】

アプリ起動部１１は、取引アプリ３１ａを実行した際に、例えば、取引アプリ３１ａに対応して処理を行うサービス提供サーバ７から本人確認済であるか否かによって、本人確認アプリ３１ｂや本人認証アプリ３１ｃ（プログラム）を起動させる。

本人確認部１２は、本人確認処理を行う制御部である。本人確認部１２は、画像取得部１３と、本人確認依頼部１４（本人確認依頼手段）とを備える。

【００１７】

画像取得部１３は、ユーザがカメラ３４を操作して、自身の本人確認書類を撮影することで、本人確認書類の画像である本人確認画像を取得する。ここで、本人確認書類とは、ユーザの顔写真が掲載された、公的に認められた身分証明書である。本人確認書類の一例として、図１には、運転免許証３が示されている。なお、本人確認書類としては、他に、ユーザの顔写真が掲載されたマイナンバーカード等であってもよい。

そして、画像取得部１３は、取得した本人確認画像から顔写真画像を抽出する。その後、画像取得部１３は、抽出した顔写真画像を記憶部３０に記憶させる。

また、画像取得部１３は、ユーザがカメラ３４を操作して、自身の顔を撮影することで、ユーザの顔画像であり、照合に用いる照合画像を取得する。

本人確認依頼部１４は、記憶部３０に記憶された顔写真画像と、取得した照合画像とを、本人認証サーバ４に対して送信し、本人確認を依頼する。

【００１８】

本人認証部１５は、サービスの利用開始時に毎回行う本人認証に関する制御部である。本人認証部１５は、事前処理部１６と、要求送信部１７（要求送信手段）と、顔画像取得照合部１８（顔画像照合手段）と、照合結果送信部１９（照合結果送信手段）とを備える。

事前処理部１６は、本人確認が行えた場合に、１度だけ行う処理である。事前処理部１６は、画像記憶処理部１６ａ（画像記憶処理手段）と、鍵処理部１６ｂ（鍵生成手段、鍵

送信手段）とを備える。

【００１９】

画像記憶処理部１６ａは、本人確認部１２によって本人確認ができた場合に、本人確認部１２の処理で取得した顔画像を、以降に行う本人認証時に照合に用いる照合画像として、照合画像記憶部３２に記憶させる。

鍵処理部１６ｂは、本人認証サーバ４との間での確認で用いる鍵ペアを生成する。鍵ペアは、秘密鍵と公開鍵とからなる。そして、鍵処理部１６ｂは、生成した秘密鍵を、鍵記憶部３３に記憶させる。また、鍵処理部１６ｂは、生成した公開鍵を、本人認証サーバ４に送信する。

【００２０】

要求送信部１７は、サービスの利用開始時に毎回行う処理である利用開始要求を、本人認証サーバ４に対して送信する。利用開始要求は、例えば、サービス提供サーバ７にログインするためのログイン要求であってもよい。

顔画像取得照合部１８は、ユーザ（サービス利用者）がカメラ３４を操作して、自身の顔を撮影することで、ユーザの顔画像を取得する。そして、顔画像取得照合部１８は、取得した顔画像と、照合画像記憶部３２に記憶された照合画像とを照合し、同一人物であるか否かを確認する。

照合結果送信部１９は、顔画像取得照合部１８による照合結果として、利用開始要求を送信することで本人認証サーバ４から受信したチャレンジコードを、鍵記憶部３３に記憶された秘密鍵で署名して、本人認証サーバ４に送信する。

サービス処理部２０は、本人認証サーバ４から受信した署名検証結果が、サービス利用を許可したものである場合に、サービス提供サーバ７との間でサービス処理を行う。

【００２１】

記憶部３０は、制御部１０が各種の処理を実行するために必要なプログラム、データ等を記憶するための半導体メモリ素子等の記憶領域である。

記憶部３０は、プログラム記憶部３１と、照合画像記憶部３２と、鍵記憶部３３とを備える。

プログラム記憶部３１は、各種のアプリケーションプログラム（以下、アプリケーションプログラムのことを、アプリケーション、アプリ、又はプログラム等という。）を記憶する記憶領域である。プログラム記憶部３１は、取引アプリ３１ａと、本人確認アプリ３１ｂと、本人認証アプリ３１ｃとを記憶している。なお、本実施形態では、以下において、取引アプリ３１ａと、本人確認アプリ３１ｂと、本人認証アプリ３１ｃとを用いるものを説明するが、複数のアプリの機能が一体になったアプリを用いるものであってもよい。

【００２２】

取引アプリ３１ａと、本人確認アプリ３１ｂと、本人認証アプリ３１ｃとは、予め携帯端末１にインストールされ、又は、通信ネットワークＮを介して図示しないアプリ配信サーバに対して通信をすることで、携帯端末１にダウンロードされる。

取引アプリ３１ａは、サービス提供サーバ７との間でのサービス処理を行うためのプログラムである。

本人確認アプリ３１ｂは、携帯端末１の制御部１０が実行する本人確認の各種機能を行うためのプログラムである。

本人認証アプリ３１ｃは、携帯端末１の制御部１０が実行する本人認証の各種機能を行うためのプログラムである。

【００２３】

照合画像記憶部３２は、本人認証に用いる画像を、照合画像として記憶する記憶領域である。照合画像記憶部３２には、本人確認ができた場合に、本人確認で使用した顔画像が、照合画像として記憶される。

鍵記憶部３３は、本人認証で用いる秘密鍵を記憶する記憶領域である。鍵記憶部３３には、本人確認ができた場合に、本人認証アプリ３１ｃを実行することによって生成した鍵ペアのうち、秘密鍵が記憶される。

【００２４】
カメラ３４は、撮影装置である。カメラ３４は、インカメラ３４ａと、アウトカメラ３４ｂとを有する。インカメラ３４ａは、携帯端末１のタッチパネルディスプレイ３５の側に有するカメラである。アウトカメラ３４ｂは、携帯端末１の背面側に有するカメラである。
タッチパネルディスプレイ３５は、液晶パネル等で構成される表示部としての機能と、ユーザの指による各種操作入力を行う入力部としての機能とを有する。
通信インタフェース部３９は、通信ネットワークＮを介して各種のサーバとの通信を行うためのインタフェースであり、送信部及び受信部の役割を行う。
【００２５】
図１に戻り、運転免許証３は、カード形状のものであり、上述したように、公的な身分証明書である。運転免許証３の表面には、ユーザ（所持者）の住所、氏名、生年月日と、ユーザの顔写真とを含むユーザの個人情報が記載されている。携帯端末１のユーザは、本人認証システム１００において、自身が所持する運転免許証３等を、携帯端末１を用いて撮影する。
【００２６】
本人認証サーバ４は、サービス開始時に、本人確認及び本人認証を行うサーバである。本人認証サーバ４は、サービスを提供する企業とは異なる企業が有する。なお、本人認証サーバ４は、サービスを提供する企業が有してもよい。
図３に示すように、本人認証サーバ４は、制御部４０と、記憶部５０と、通信インタフェース部５９とを備える。
【００２７】
制御部４０は、本人認証サーバ４の全体を制御するＣＰＵである。制御部４０は、記憶部５０に記憶されているＯＳやアプリケーションプログラムを適宜読み出して実行することにより、上述したハードウェアと協働し、各種機能を実行する。
制御部４０は、本人確認処理部４１と、鍵受信処理部４２（鍵記憶手段）と、コード生成送信部４３（コード送信手段）と、サービス利用許可部４４（許可手段）とを備える。
【００２８】
本人確認処理部４１は、本人確認処理を行う。
具体的には、本人確認処理部４１は、顔画像と、顔写真画像とを、携帯端末１から受信する。そして、本人確認処理部４１は、受信した顔画像と顔写真画像とを照合する。ここで、本人確認処理部４１は、顔画像と顔写真画像との照合結果を、スコアによって示してもよい。例えば、本人確認処理部４１は、画像照合処理を行い、顔写真画像の一致度合いをスコアとして算出する。ここで、スコアは、例えば、０～１００までの数値により表されるものであり、一致度合いが高いほど数値が高い。
その後、本人確認処理部４１は、照合結果を、携帯端末１に送信する。
【００２９】
鍵受信処理部４２は、携帯端末１から本人認証で用いる公開鍵を受信し、受信した公開鍵を鍵記憶部５３に記憶する。
コード生成送信部４３は、利用開始要求を受信したことに応じて、乱数を利用してチャレンジコードを発生させる。また、コード生成送信部４３は、発生させたチャレンジコードを、携帯端末１に送信する。
サービス利用許可部４４は、携帯端末１から受信した署名を検証し、検証できた場合に、サービス利用を許可した署名検証結果を、携帯端末１に送信する。
【００３０】
記憶部５０は、制御部４０が各種の処理を実行するために必要なプログラム、データ等を記憶するためのハードディスク、半導体メモリ素子等の記憶領域である。
記憶部５０は、プログラム記憶部５１と、鍵記憶部５３とを備える。
プログラム記憶部５１は、各種のプログラムを記憶する記憶領域である。プログラム記憶部５１は、本人確認プログラム５１ａと、本人認証プログラム５１ｂとを記憶する。

本人確認プログラム５１ａは、本人認証サーバ４の制御部４０が実行する本人確認処理部４１の機能を行うためのプログラムである。
本人認証プログラム５１ｂは、本人認証サーバ４の制御部４０が実行する鍵受信処理部４２からサービス利用許可部４４までの機能を行うためのプログラムである。
なお、本実施形態では、以下において、本人確認プログラム５１ａと、本人認証プログラム５１ｂとを用いるものを説明するが、２つのプログラムの機能が一体になったプログラムを用いるものであってもよい。
通信インタフェース部５９は、通信ネットワークＮを介してサービス提供サーバ７等の各種サーバ及び携帯端末１との間の通信を行うためのインタフェースである。

【００３１】

ここで、コンピュータとは、制御部、記憶装置等を備えた情報処理装置をいい、携帯端末１及び本人認証サーバ４は、それぞれ制御部、記憶部等を備えた情報処理装置であり、コンピュータの概念に含まれる。

【００３２】

図１に示すサービス提供サーバ７は、サービス処理を行うためのサーバである。図１において、本人認証システム１００は、サービス提供サーバ７を１つのみ記載しているが、サービスごとに複数のサーバを備えてもよい。
なお、サービス提供サーバ７は、図示しないが、制御部、記憶部、通信インタフェース部等を備える。

【００３３】

図１に示す基地局Ｒは、無線通信の基地局であって、携帯端末１が各種のサーバとの間の通信をするための中継を行う。基地局Ｒは、例えば、無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）の基地局や、通信事業者の携帯端末通信網用の基地局である。
通信ネットワークＮは、各種のサーバ間や各種のサーバと基地局Ｒとの間のネットワークであり、インターネット回線や携帯端末通信網等である。

【００３４】

次に、本人認証システム１００の処理について説明する。
図４は、第１実施形態に係る携帯端末１でのサービス開始処理を示すフローチャートである。
まず、サービスを開始したいユーザは、例えば、自身の携帯端末１のタッチパネルディスプレイ３５に表示されている取引アプリ３１ａのアイコン（図示せず）を選択するタップ等のタッチ操作をする。そうすることで、携帯端末１の制御部１０は、取引アプリ３１ａを実行する。

【００３５】

取引アプリ３１ａが実行されると、携帯端末１のタッチパネルディスプレイ３５には、取引アプリ３１ａのメイン画面（図示せず）が表示される。そこで、ユーザがメイン画面からサービス開始のための操作（例えば、メニューを選択する操作）を行うと、図４のステップＳ１０（以下、単に「Ｓ」という。）において、携帯端末１の制御部１０は、サービス開始操作を受け付ける。

【００３６】

次に、Ｓ１１において、制御部１０は、本人確認処理がされているか否かを判断する。一例として、制御部１０は、照合画像記憶部３２を参照して、照合画像が記憶されていれば、本人確認処理がされていると判断する。本人確認処理がされている場合（Ｓ１１：ＹＥＳ）には、制御部１０は、処理をＳ１２に移す。他方、本人確認がされていない場合（Ｓ１１：ＮＯ）には、制御部１０は、処理をＳ１３に移す。
Ｓ１２において、制御部１０は、本人認証処理（後述する図８参照）を行う。その後、制御部１０は、本処理を終了する。
他方、Ｓ１３において、制御部１０は、本人確認処理（後述する図５参照）を行う。その後、制御部１０は、本処理を終了する。

【００３７】

次に、本人確認処理について説明する。
図５は、第１実施形態に係る携帯端末１での本人確認処理を示すフローチャートである。
図６は、第１実施形態に係る本人認証システム１００での本人確認画像処理を示すフローチャートである。
図７は、第１実施形態に係る本人認証システム１００での照合画像処理を示すフローチャートである。
【００３８】
図５のＳ２０において、制御部１０（アプリ起動部１１）は、本人確認アプリ３１ｂを起動させる。
Ｓ２１において、携帯端末１の制御部１０（本人確認部１２）は、本人確認画像処理を行う。
ここで、本人確認画像処理について、図６に基づき説明する。
図６のＳ５０において、携帯端末１の制御部１０（画像取得部１３）は、アウトカメラ３４ｂを起動させ、タッチパネルディスプレイ３５にアウトカメラ３４ｂのスルー画像（撮影範囲の画像）を表示させて、本人確認書類を撮影可能にする。そして、ユーザが、本人確認書類をスルー画像に写り込むようにして、図示しない撮影ボタンをタップすることで、制御部１０は、本人確認画像を取得する。
【００３９】
その際、制御部１０は、まず、本人確認書類として何を撮影するのか（運転免許証３又はマイナンバーカード）を選択するための身分証明書選択画面（図示せず）を表示させ、ユーザに本人確認書類の種類を選択させてもよい。そして、制御部１０は、本人確認書類の種類に応じて、撮影をさせるための案内を変えてもよい。例えば、運転免許証３の場合には、表面と裏面とを撮影する必要がある。他方、マイナンバーカードであれば、表面のみを撮影すれば足りる。
【００４０】
Ｓ５１において、制御部１０（画像取得部１３）は、本人確認画像から顔写真画像を抽出する。制御部１０は、例えば、本人確認画像を解析して、本人確認書類を特定する。そして、制御部１０は、本人確認書類から顔写真の画像位置を特定して、特定した画像位置の画像を抽出する。
Ｓ５２において、制御部１０（画像取得部１３）は、抽出した顔写真画像を、記憶部３０に一時記憶させる。その後、制御部１０は、処理を図５のＳ２２に移す。
【００４１】
図５のＳ２２において、制御部１０（本人確認部１２）は、照合画像処理を行う。
ここで、照合画像処理について、図７に基づき説明する。
図７のＳ６０において、携帯端末１の制御部１０（画像取得部１３）は、インカメラ３４ａを起動させ、タッチパネルディスプレイ３５にインカメラ３４ａのスルー画像を表示させる。そして、ユーザが、自身の顔をスルー画像に写り込むようにして、図示しない撮影ボタンをタップすることで、制御部１０は、照合画像（顔画像）を取得する。
【００４２】
Ｓ６１において、制御部１０（本人確認依頼部１４）は、記憶部３０に一時記憶した顔写真画像と共に、取得した照合画像を、本人認証サーバ４に対して送信する。ここで、記憶部３０に記憶した顔写真画像とは、本人確認画像処理において携帯端末１が取得及び記憶したものである。
Ｓ６２において、本人認証サーバ４の制御部４０（本人確認処理部４１）は、照合画像と、顔写真画像とを、携帯端末１から受信する。
【００４３】
Ｓ６３において、制御部４０（本人確認処理部４１）は、照合画像と顔写真画像とを照合する顔照合処理を行う。制御部４０は、画像照合処理を行い、例えば、照合画像と顔写真画像との一致度合いをスコアとして算出する。
Ｓ６４において、制御部４０（本人確認処理部４１）は、照合結果を、携帯端末１に対

して送信する。その後、制御部４０は、本処理を終了する。
　Ｓ６５において、携帯端末１の制御部１０（本人確認部１２）は、照合結果を受信する。その後、制御部１０は、処理を図５のＳ２３に移す。
【００４４】
　図５のＳ２３において、制御部１０（本人確認部１２）は、照合結果によって認証ができたか否かを判定する。照合結果として得られた、例えば、スコアが閾値以上である場合に、制御部１０は、認証ができたと判定する。認証ができたと判定された場合（Ｓ２３：ＹＥＳ）には、制御部１０は、処理をＳ２４に移す。他方、認証ができたと判定されなかった場合（Ｓ２３：ＮＯ）には、制御部１０は、処理をＳ２９に移す。
【００４５】
　Ｓ２４において、制御部１０は、本人認証アプリ３１ｃを起動させる。
　Ｓ２５において、制御部１０（画像記憶処理部１６ａ）は、本人確認処理で取得した顔画像を、照合画像として照合画像記憶部３２に記憶させる。
　Ｓ２６において、制御部１０（鍵処理部１６ｂ）は、鍵ペアを生成し、生成した鍵ペアのうちの公開鍵を、本人認証サーバ４へ送信する。そうすることで、本人認証サーバ４の制御部４０（鍵受信処理部４２）は、公開鍵を受信し、鍵記憶部５３に受信した公開鍵を記憶させる。
　Ｓ２７において、制御部１０（サービス処理部２０）は、取引アプリ３１ａに対応したサービス提供サーバ７との間でサービス処理を行う。その後、制御部１０は、処理を図４に移し、本処理を終了する。
【００４６】
　他方、Ｓ２９において、制御部１０は、認証エラーの旨を、タッチパネルディスプレイ３５に出力する。その後、制御部１０は、処理を図４に移し、本処理を終了する。
【００４７】
　次に、本人認証処理について説明する。
　図８及び図９は、第１実施形態に係る本人認証システム１００での本人認証処理を示すフローチャートである。
　図８のＳ３０において、携帯端末１の制御部１０（アプリ起動部１１）は、本人認証アプリ３１ｃを起動させる。
　Ｓ３１において、制御部１０（要求送信部１７）は、利用開始要求を、本人認証サーバ４に送信する。
【００４８】
　Ｓ３２において、本人認証サーバ４の制御部４０は、利用開始要求を受信する。
　Ｓ３３において、制御部４０（コード生成送信部４３）は、乱数を発生させてチャレンジコードを生成し、携帯端末１に生成したチャレンジコードを送信する。その後、制御部４０は、本処理を終了する。
　Ｓ３４において、携帯端末１の制御部１０は、チャレンジコードを受信する。
　Ｓ３５において、制御部１０（顔画像取得照合部１８）は、顔画像を取得する。制御部１０は、インカメラ３４ａをアクティブにし、ユーザに自身の顔を撮影させることで、ユーザの顔画像を取得する。
【００４９】
　Ｓ３６において、制御部１０（顔画像取得照合部１８）は、取得したユーザの顔画像と、照合画像記憶部３２に記憶された照合画像とを照合する。この画像を照合する画像照合処理は、本人認証サーバ４が本人確認の際に行ったものと同じロジックのものであってよい。制御部１０は、画像照合処理により、例えば、顔画像と照合画像との一致度合いをスコアとして算出する。
　Ｓ３７において、制御部１０（顔画像取得照合部１８）は、照合できたか否かを判定する。例えば、スコアが閾値以上である場合に、制御部１０は、照合ができたと判定する。照合ができたと判定された場合（Ｓ３７：ＹＥＳ）には、制御部１０は、処理をＳ３８に移す。他方、照合ができたと判定されなかった場合（Ｓ３７：ＮＯ）には、制御部１０は

、処理をＳ３９に移す。
【００５０】
Ｓ３８において、制御部１０（照合結果送信部１９）は、Ｓ３４で受信したチャレンジコードを、鍵記憶部３３に記憶された秘密鍵で署名する。その後、制御部１０は、処理を図９のＳ４０に移す。
他方、Ｓ３９において、制御部１０は、認証エラーの旨を、タッチパネルディスプレイ３５に出力する。その後、制御部１０は、処理を図４に移し、本処理を終了する。
【００５１】
図９のＳ４０において、制御部１０（照合結果送信部１９）は、署名したデータを、本人認証サーバ４に送信する。
Ｓ４１において、本人認証サーバ４の制御部４０は、署名したデータを受信する。
Ｓ４２において、制御部４０は、鍵記憶部５３に有する公開鍵を用いた署名検証処理を行う。公開鍵を用いて署名検証ができた場合に、制御部４０は、本人認証ができたと判定する。
【００５２】
Ｓ４３において、制御部４０は、署名検証ができたか否かを判定する。署名検証ができた場合（Ｓ４３：ＹＥＳ）には、制御部４０は、処理をＳ４４に移す。他方、署名検証ができなかった場合（Ｓ４３：ＮＯ）には、制御部４０は、本処理を終了する。
Ｓ４４において、制御部４０（サービス利用許可部４４）は、署名検証結果を、携帯端末１に送信する。その後、制御部４０は、本処理を終了する。
【００５３】
Ｓ４５において、携帯端末１の制御部１０は、署名検証結果を受信したか否かを判定する。署名検証結果を受信した場合（Ｓ４５：ＹＥＳ）には、制御部１０は、処理をＳ４６に移す。他方、署名検証結果を受信していない場合（Ｓ４５：ＮＯ）には、制御部１０は、処理をＳ４９に移す。なお、署名したデータを送信（Ｓ４０）後、所定時間内に署名検証結果を受信しない場合に、制御部１０は、署名検証結果を受信しなかったと判定してもよい。
Ｓ４６において、制御部１０（サービス処理部２０）は、取引アプリ３１ａに対応したサービス提供サーバ７との間でサービス処理を行う。その後、制御部１０は、処理を図４に移し、本処理を終了する。
【００５４】
他方、Ｓ４９において、制御部１０は、認証エラーの旨を、タッチパネルディスプレイ３５に出力する。その後、制御部１０は、処理を図４に移し、本処理を終了する。
【００５５】
このように、第１実施形態によれば、本人認証システム１００は、以下のような効果がある。
（１）本人確認で取得した顔画像を、携帯端末１に記憶しておき、サービス利用時に都度行う本人認証での照合に、記憶した顔画像である照合画像を用いる。よって、通信ネットワークＮに本人認証で用いる顔画像である生体情報を送信することがなく、セキュリティ性を向上させることができる。つまり、本人確認処理から本人認証処理を一連の処理として、又は、連続した処理として行えることは、セキュリティを高めることになる。また、本人認証のために、再度照合元になる顔画像を取得するものではなく、本人確認で取得した顔画像（照合画像）を流用するので、１度照合用の画像を取得すれば足り、ユーザにとって、より利便性が良いものにできる。
【００５６】
（２）特に、金融機関のオンライン取引に関する本人認証の処理においては、従来からのパスワード認証から、より一層の利便性及びセキュリティ性の向上のため、生体認証へと移行しつつある。生体認証において、例えば、顔画像を用いて照合をする場合には、照合元になる顔画像は、極力、外部に出力（又は送信）したものではなく、携帯端末１の内部にのみ保持した画像を利用することが好ましい。生体認証において、本人の生体情報を

登録する際に、顔画像等の本人データが流用されることがなく、より強固な環境でセキュリティを維持することが可能になる。
（３）本人確認で取得した顔画像は、本人確認ができた場合に、本人認証時の照合用の画像として携帯端末１に記憶させる。よって、顔画像を記憶させる行為を、本人認証時の最初にだけ行うものにできる。
【００５７】
（４）携帯端末１から本人認証サーバ４に対して、秘密鍵で署名した本人認証の照合結果を送信するので、よりセキュリティ性を向上できる。
（５）本人認証サーバ４から携帯端末１に、チャレンジコードを送信し、携帯端末１から本人認証サーバ４には、チャレンジコードを秘密鍵で署名した照合結果を送信するので、本人認証サーバ４では、本人認証を行う携帯端末１の同一性を確保でき、セキュリティ性が向上する。
【００５８】
（第２実施形態）
第２実施形態では、携帯端末を用いてユーザが行う各種の撮影態様について、セキュリティ性を向上させる工夫をしたものを説明する。なお、以降の説明において、上述した第１実施形態と同様の機能を果たす部分には、同一の符号又は末尾に同一の符号を付して、重複する説明を適宜省略する。
【００５９】
図１０は、第２実施形態に係る本人認証システム２００における携帯端末２０１の機能ブロック図である。
本人認証システム２００は、携帯端末２０１を備える。なお、図示しないが、本人認証システム２００では、携帯端末２０１が、図示しない通信ネットワークＮ及び基地局Ｒを介して本人認証サーバ４及びサービス提供サーバ７に対して接続されている（図１参照）。
【００６０】
携帯端末２０１は、制御部２１０と、記憶部２３０と、カメラ３４と、タッチパネルディスプレイ３５と、通信インタフェース部３９とを備える。
制御部２１０は、アプリ起動部１１と、本人確認部２１２と、本人認証部２１５と、サービス処理部２０とを備える。
本人確認部２１２は、画像取得部２１３（本人確認画像取得手段、本人確認用顔画像取得手段）と、本人確認依頼部２１４（本人確認依頼手段）とを備える。
【００６１】
画像取得部２１３は、ユーザがカメラ３４を操作して、自身の本人確認書類を複数回撮影することで、本人確認書類の画像である本人確認画像を取得する。そして、画像取得部２１３は、取得した複数の本人確認画像のうちの１つの画像を、照合に用いる。
また、画像取得部２１３は、ユーザがカメラ３４を操作して、自身の顔を複数回撮影することで、ユーザの顔画像を取得する。そして、画像取得部２１３は、取得した複数の顔画像のうちの１つの画像を、照合に用いる照合画像にする。
【００６２】
（１）本人確認画像の取得について
画像取得部２１３は、本人確認書類の顔写真画像を含む面に対して垂直の撮影方向を含む、顔写真画像を確認可能な複数の異なる撮影方向から本人確認書類を撮影した複数の本人確認画像を取得する。
その際、指定の撮影方向の本人確認画像を取得するべく、画像取得部２１３は、書類位置ガイド画像を、タッチパネルディスプレイ３５に出力してもよい。書類位置ガイド画像は、顔写真を確認可能な撮影方向と、本人確認画像の大きさを含む本人確認書類の配置位置とを指定する画像である。指定の撮影方向とは、本人確認書類の顔写真を確認できる方向である。また、書類位置ガイド画像を出力して撮影させることで、ユーザにその場で、本人確認書類を用いて撮影させ、不正を防ぐものにしている。
【００６３】

具体的には、ユーザは、自身の携帯端末２０１を操作して、書類位置ガイド画像により示されたガイド位置にしたがって、自身の本人確認書類を写しこむ。そして、ユーザがカメラ３４を操作して撮影することで、画像取得部２１３は、本人確認書類の画像である本人確認画像を取得する。

画像取得部２１３は、次に、先ほどとは撮影方向及び配置位置の異なる書類位置ガイド画像を出力して、書類位置ガイド画像にしたがって、ユーザに本人確認画像を取得させる処理を行う。画像取得部２１３は、この書類位置ガイド画像を出力し、ユーザに本人確認書類を撮影させる処理を、複数回繰り返す。そして、画像取得部２１３は、取得した本人確認画像を、記憶部２３０に記憶させる。ここで、画像取得部２１３が出力する書類位置ガイド画像のうちの１つは、本人確認書類の顔写真を含む面に対して垂直の撮影方向である、本人確認書類の正面から本人確認書類を撮影させるためのものである。

【００６４】

そして、画像取得部２１３は、記憶した複数の本人確認画像のうち１つの本人確認画像から顔写真画像を抽出する。その際、画像取得部２１３は、本人確認書類の正面から本人確認書類が撮影されることで得られた本人確認画像を使用して、顔写真画像を抽出するのが望ましい。そのようにすることで、制御部２１０は、例えば、取得した顔写真画像の歪み補正をする等の追加処理を行わずに済み、照合に使用しやすい。その後、画像取得部２１３は、抽出した顔写真画像を記憶部２３０に記憶させる。

さらに、画像取得部２１３は、取得した本人確認画像を、取得時に使用した書類位置ガイド画像に基づいて確認してもよい。画像取得部２１３は、本人確認画像を分析して、例えば、書類位置ガイド画像が示す枠内に、指定の撮影方向から顔写真が掲載された本人確認書類が撮影されていることを確認する。

【００６５】

（２）顔画像の取得について

画像取得部２１３は、少なくともユーザの顔の向きが正面方向である顔画像と、ユーザの顔の向きが正面とは異なる向きである顔画像とを取得する。

その際、ユーザ本人がその場で撮影していることを確認するべく、画像取得部２１３は、撮影の都度、ユーザの顔の向きを指定するガイド情報を出力してもよい。

具体的には、画像取得部２１３は、まず、ガイド情報として、自身の正面の顔を撮影するための顔撮影ガイド画像（指示情報）を、タッチパネルディスプレイ３５に出力させる。ユーザは、自身の携帯端末２０１を操作してインカメラ３４ａを起動させて自身の顔の向きを正面方向にし、顔撮影ガイド画像により示されたガイド位置に収まるようにする。そして、ユーザがカメラ３４を操作して撮影することで、画像取得部２１３は、顔画像を取得する。

【００６６】

画像取得部２１３は、次に、ユーザの顔の向きを変える指示を、例えば、タッチパネルディスプレイ３５に出力させると共に、携帯端末２０１の図示しないスピーカから音声出力する。顔の向きを変えた場合には、ユーザは、タッチパネルディスプレイ３５を視認できないため、音声による指示は有効である。そして、画像取得部２１３は、例えば、カウントダウンを音声出力した上で、撮影タイミングになった時にカメラ３４を制御して、顔画像を取得する。

なお、画像取得部２１３は、ユーザの顔の向きを、例えば、上下左右の方向に変えさせて顔画像を撮影する処理を、複数回行ってもよい。また、画像取得部２１３は、正面方向の顔画像を取得する処理を、途中で行ってもよい。

そして、画像取得部２１３は、取得した顔画像を記憶部２３０に記憶させる。

【００６７】

また、画像取得部２１３は、取得した照合画像が撮影条件を満たしたものであるか、つまり、その前に出力した指示内容にしたがったものであるか否かを確認する。

さらに、画像取得部２１３は、取得した複数の顔画像のうち、例えば、正面から撮影したユーザの顔画像を、照合画像にする。

本人確認依頼部２１４は、記憶部２３０に記憶された顔写真画像と、取得した照合画像とを、本人認証サーバ４に対して送信し、本人確認を依頼する。

【００６８】

本人認証部２１５は、事前処理部１６と、要求送信部１７と、顔画像取得部２１８ａ（指示出力手段、顔画像照合手段、顔画像取得手段、繰り返し手段、画像確認手段）と、顔画像照合部２１８ｂ（顔画像照合手段、照合手段）と、照合結果送信部１９とを備える。

顔画像取得部２１８ａは、ユーザがカメラ３４を操作して、自身の顔を撮影することで、ユーザの顔画像を取得する。

【００６９】

顔画像取得部２１８ａの処理は、画像取得部２１３の顔画像の取得に関する処理と同様である。

顔画像取得部２１８ａは、取得した複数の顔画像が、各々の撮影条件を満たしたものであるか、つまり、その前に出力した指示内容にしたがったものであるか否かを確認する。

顔画像照合部２１８ｂは、顔画像取得部２１８ａにより取得した顔画像と、照合画像記憶部３２に記憶された照合画像とを照合し、同一人物であるか否かを確認する。ここで、顔画像照合部２１８ｂは、ユーザの顔が正面方向である顔画像を、照合画像記憶部３２に記憶された照合画像との照合に用いる画像として選定する。

【００７０】

記憶部２３０は、プログラム記憶部２３１と、照合画像記憶部３２と、鍵記憶部３３とを備える。

プログラム記憶部２３１は、取引アプリ３１ａと、本人確認アプリ２３１ｂと、本人認証アプリ２３１ｃとを記憶している。

本人確認アプリ２３１ｂは、携帯端末２０１の制御部２１０が実行する本人確認の各種機能を行うためのプログラムである。

本人認証アプリ２３１ｃは、携帯端末２０１の制御部２１０が実行する本人認証の各種機能を行うためのプログラムである。

【００７１】

次に、本人認証システム２００の処理について説明する。

サービス開始処理については、第１実施形態（図４）と同様である。

また、本人確認処理における処理の流れは、第１実施形態（図５）と同様である。

この本人確認処理で行う本人確認画像処理について、図１１に基づいて説明する。

図１１は、第２実施形態に係る携帯端末２０１での本人確認処理を示すフローチャートである。

図１２は、第２実施形態に係る携帯端末２０１での表示例を示す図である。

図１３は、第２実施形態に係る携帯端末２０１に表示する書類位置ガイド画像の例を示す図である。

【００７２】

図１１のＳ２５０において、携帯端末２０１の制御部２１０（画像取得部２１３）は、アウトカメラ３４ｂを起動させ、タッチパネルディスプレイ３５にアウトカメラ３４ｂのスルー画像を表示させる。また、制御部２１０は、例えば、図１２（Ａ）に示すような、本人確認書類の正面を撮影方向にした書類位置ガイド画像２５０を、タッチパネルディスプレイ３５に出力する。

図１２（Ａ）に示す書類位置ガイド画像２５０は、本人確認書類を配置させる書類位置領域２５０ａと、撮影ボタン２５０ｂとを含む画像である。また、書類位置ガイド画像２５０は、透過性を有する画像である。これは、アウトカメラ３４ｂのスルー画像と共に出力するためであり、少なくとも書類位置領域２５０ａは、透過性を有する必要がある。

【００７３】

ユーザが、本人確認書類を書類位置領域２５０ａに写り込むように配置して、撮影ボタン２５０ｂをタップすることで、図１１のＳ２５１において、制御部２１０（画像取得部２１３）は、本人確認画像を取得する。そして、制御部２１０は、取得した本人確認画像

を、記憶部２３０に記憶させる。
　Ｓ２５２において、制御部２１０（画像取得部２１３）は、アウトカメラ３４ｂを再度起動させて、タッチパネルディスプレイ３５にアウトカメラ３４ｂのスルー画像を再度表示させる。そして、制御部２１０は、例えば、図１２（Ｂ）に示すような、本人確認書類の側面を含む、本人確認画像の撮影を指示する書類位置ガイド画像２５１を、タッチパネルディスプレイ３５に出力する。
【００７４】
　図１２（Ｂ）に示す書類位置ガイド画像２５１は、本人確認書類を配置させる書類位置領域２５１ａと、撮影ボタン２５１ｂとを含む画像である。また、上述した書類位置ガイド画像２５０と同様に、書類位置ガイド画像２５１は、透過性を有する画像である。書類位置領域２５１ａは、本人確認書類の顔写真が確認でき、かつ、本人確認書類の長辺の厚さが確認できるように、斜め方向からの撮影方向を指示したものである。そのため、書類位置領域２５１ａは、底辺が長い台形状で示している。
　なお、これは、一例であって、例えば、書類位置領域２５１ａは、枠線で示すものではなく、本人確認書類の２つの長辺の位置を線で示すものであってもよい。また、書類位置領域２５１ａは、本人確認書類の短辺の厚さを確認するためのものにしてもよい。
【００７５】
　ユーザが、本人確認書類を書類位置領域２５１ａに写り込むように配置して、撮影ボタン２５１ｂをタップすることで、図１１のＳ２５３において、制御部２１０（画像取得部２１３）は、本人確認画像を取得する。そして、制御部２１０は、取得した本人確認画像を、記憶部２３０に記憶させる。
【００７６】
　Ｓ２５４において、制御部２１０（画像取得部２１３）は、書類位置ガイド画像に基づき、取得した本人確認画像を確認する。
　制御部２１０は、例えば、本人確認書類が書類位置領域２５０ａ内に収まっており、かつ、所定の大きさで本人確認画像が取得できていることや、取得した本人確認画像が、本人確認書類であること（例えば、運転免許証３の表面であること）を確認する。制御部２１０は、この確認を、取得した本人確認画像の全てにおいて行う。また、制御部２１０は、取得した本人確認画像の解像度が所定の条件を満たすか否かを確認する。例えば、手振れ等により、また、光量が不足したりしている場合には、本人確認画像の解像度が所定の条件を満たさなくなる。
【００７７】
　なお、制御部２１０は、本人確認画像の確認により確認ができなかった場合、つまり、本人確認画像としての条件を満たさない場合には、所定のリトライ回数まで再度Ｓ２５０からの処理を行うようにしてもよい。また、制御部２１０は、例えば、所定のリトライ回数を超えた場合には、エラーとして以降の処理を行わないようにしてもよい。
【００７８】
　Ｓ２５５において、制御部２１０（画像取得部２１３）は、本人確認画像から顔写真画像を抽出する。制御部２１０は、例えば、Ｓ２５１で取得した本人確認書類を正面から撮影した本人確認画像から、顔写真画像を抽出する。
　Ｓ２５６において、制御部２１０（画像取得部２１３）は、抽出した顔写真画像を、記憶部２３０に記憶させる。その後、制御部２１０は、次に説明する照合画像処理（図５のＳ２２参照）を行う。
【００７９】
　なお、この例では、まず本人確認書類の正面を撮影方向にした書類位置ガイド画像２５０を出力して撮影してから、異なる撮影方向及び撮影位置の書類位置ガイド画像２５１を出力して撮影させるものを例に説明したが、これに限定されない。複数回の本人確認書類の撮影のうちの１回を、本人確認書類の正面を撮影方向にしたものにすれば、順番は限定されない。また、撮影回数は、２回に限定されるものではなく、３回以上であってもよい。
【００８０】

さらに、本人認証システム２００では、様々な撮影方向及び撮影位置の書類位置ガイド画像を、記憶部２３０に記憶させておいて、制御部２１０は、その中からランダムに書類位置ガイド画像を選択して、出力するようにしてもよい。様々な撮影方向及び撮影位置の書類位置ガイド画像は、例えば、図１３（Ａ）に示す書類位置ガイド画像２６１から図１３（Ｄ）に示す書類位置ガイド画像２６４までである。

【００８１】

図１３（Ａ）に示す書類位置ガイド画像２６１は、本人確認書類の厚みを撮影可能な撮影方向であり、近距離で画面上部に本人確認書類を配置させて撮影させるための書類位置領域２６１ａを含む。

図１３（Ｂ）に示す書類位置ガイド画像２６２は、本人確認書類の厚みを撮影可能な撮影方向であり、近距離で画面下部に本人確認書類を配置させて撮影させるための書類位置領域２６２ａを含む。

他方、図１３（Ｃ）に示す書類位置ガイド画像２６３及び図１３（Ｄ）に示す書類位置ガイド画像２６４は、本人確認書類の厚みを撮影可能な撮影方向であり、遠距離で画面上部又は下部に本人確認書類を配置させて撮影させるための書類位置領域２６３ａ及び２６４ａを含む。

なお、記憶部２３０には、その他、画面中央に書類位置領域を配置させるようにして撮影させる書類位置ガイド画像を記憶してもよい。

【００８２】

また、この例では、複数回、異なる撮影方向から本人確認書類を撮影した後に、本人確認画像を確認するものであるが、これに限定されない。制御部２１０は、本人確認画像を取得した都度、本人確認画像を確認してもよい。また、制御部２１０は、本人確認画像を取得した後、ユーザに本人確認画像を確認させて、ユーザが保存する指示を入力した場合に、取得した本人確認画像を記憶するようにし、ユーザの確認によって取り直しを可能にしてもよい。

【００８３】

次に、本人確認処理で行う照合画像処理について、図１４に基づき説明する。

図１４は、第２実施形態に係る本人認証システム２００での照合画像処理を示すフローチャートである。

図１５は、第２実施形態に係る携帯端末２０１での照合画像の取得処理を示すフローチャートである。

図１６は、第２実施形態に係る携帯端末２０１での表示例を示す図である。

【００８４】

図１４のＳ２６０において、携帯端末２０１の制御部２１０（画像取得部２１３）は、照合画像の取得処理を行う。

ここで、照合画像の取得処理について、図１５に基づき説明する。

図１５のＳ２７０において、制御部２１０（画像取得部２１３）は、インカメラ３４ａを起動させ、タッチパネルディスプレイ３５にインカメラ３４ａのスルー画像を表示させる。そして、制御部２１０は、例えば、図１６（Ａ）に示すような、顔撮影ガイド画像２７０を、タッチパネルディスプレイ３５に出力する。

図１６（Ａ）に示す顔撮影ガイド画像２７０は、ユーザの正面からの顔画像を取得させるためのものである。また、顔撮影ガイド画像２７０は、ユーザ自身の顔の位置を特定する顔位置領域２７０ａを含む画像である。

【００８５】

図１５のＳ２７１において、制御部２１０（画像取得部２１３）は、ユーザの顔画像を取得し、記憶部２３０に記憶させる。顔画像の取得は、ユーザが、自身の顔を顔位置領域２７０ａに写り込むように携帯端末２０１の位置を移動させて、図示しない撮影ボタンをタップすることで、制御部２１０が撮影するように制御して、ユーザの顔画像を取得するようにしてもよい。また、制御部２１０は、顔撮影ガイド画像２７０を出力してから所定時間（例えば、５秒等）を経過後に自動的に撮影するように制御して、ユーザの顔画像を

取得してもよい。さらに、制御部２１０に顔及び目の瞬きを検出する機能を有しておき、制御部２１０が瞬きを検出した後に撮影するように制御して、ユーザの顔画像を取得してもよい。

【００８６】

Ｓ２７２において、制御部２１０（画像取得部２１３）は、ユーザに対して顔の向きを変える指示を出力する。ここで、制御部２１０による指示は、例えば、図１６（Ｂ）に示す顔撮影ガイド画像２７１のように表示するものの他、例えば、図示しないスピーカから音声出力してもよい。図１６（Ｂ）に示す顔撮影ガイド画像２７１は、ユーザに右を向かせるものであるが、ユーザの顔を、例えば、上下左右のいずれかの方向に向かせるものであってもよい。

【００８７】

Ｓ２７３において、制御部２１０（画像取得部２１３）は、顔画像を取得し、記憶部２３０に記憶させる。この撮影では、ユーザの顔の向きが携帯端末２０１のタッチパネルディスプレイ３５に向いていないため、ユーザが図示しない撮影ボタンをタップするのは難しい。そこで、制御部２１０は、撮影条件として、例えば、顔撮影ガイド画像２７１を出力してから所定時間（例えば、５秒等）を音声によりカウントした後に、自動的に撮影するように制御して、ユーザの顔画像を取得してもよい。また、制御部２１０は、顔撮影ガイド画像２７１を出力してから所定時間（例えば、５秒等）内に、顔位置領域２７１ａに顔が写り込んでいることを検出したことに応じて自動的に撮影するように制御して、ユーザの顔画像を取得してもよい。

【００８８】

Ｓ２７４において、制御部２１０（画像取得部２１３）は、取得した顔画像が、対応する指示内容にしたがったものであるか否かを確認する。なお、確認ができなかった場合には、制御部２１０は、以降の処理を行わないようにしてもよい。

Ｓ２７５において、制御部２１０（画像取得部２１３）は、取得した複数の顔画像のうちの１つを照合に用いる照合画像として選定する。制御部２１０は、例えば、Ｓ２７１で取得したユーザの正面からの顔画像を、照合画像として選定する。その後、制御部２１０は、処理を図１４のＳ２６１に移す。

図１４のＳ２６１からＳ２６５までの処理は、第１実施形態（図７）のＳ６１からＳ６５までの処理と同様である。

【００８９】

次に、サービス開始処理で行う本人認証処理について、図１７及び図１８に基づき説明する。

図１７及び図１８は、第２実施形態に係る本人認証システム２００での本人認証処理を示すフローチャートである。

図１７のＳ２３０からＳ２３４までは、第１実施形態（図８）のＳ３０からＳ３４までの処理と同様である。

図１７のＳ２３５において、制御部２１０（顔画像取得部２１８ａ）は、顔画像の取得処理を行う。

【００９０】

ここで、顔画像の取得処理について、図１９に基づき説明する。

図１９のＳ２９０からＳ２９４までの処理は、照合画像の取得処理（図１５参照）のＳ２７０からＳ２７４までの処理と同様である。

なお、この例では、ユーザの顔が正面方向の画像を取得してから、ユーザの顔が右方向に向いた画像を取得するものを説明しているが、本人認証処理をする都度、指示情報を変更するのが好ましい。例えば、ユーザの顔が正面方向の画像を取得するのは、最初である必要はなく、制御部２１０は、先に、ユーザの顔が上下左右のいずれかの方向を向いた画像を取得するための指示を出力し、その後に、ユーザの顔が正面方向の画像を取得するための指示をしてもよい。また、制御部２１０は、指示内容を、記憶部２３０に記憶しておき、前回の指示内容とは異なる指示内容を出力するようにしてもよい。

【００９１】
図１７のＳ２３６において、制御部２１０（顔画像照合部２１８ｂ）は、Ｓ２３５の処理で取得した顔画像と、照合画像記憶部３２に記憶された照合画像とを照合する。制御部２１０（顔画像照合部２１８ｂ）は、照合画像との照合に用いる顔画像として、ユーザの顔が正面方向の画像を選定する。そのようにすれば、照合に用いる顔画像と、照合画像とが、同じユーザの顔が正面方向の画像になるため、照合の精度が高まる。
図１７のＳ２３７から図１８のＳ２４９までの処理は、第１実施形態（図８及び図９）のＳ３７からＳ４９までの処理と同様である。
【００９２】
このように、第２実施形態によれば、本人認証システム２００は、以下のような効果がある。
（１）本人認証処理時に、携帯端末２０１は、指示情報に基づいてユーザの顔の向きを変えさせて、ユーザの顔画像を複数回撮影するものを含むようにした。よって、指示情報にしたがった撮影が必要であり、例えば、予め用意した画像を用いる等の不正行為を防ぐことができる。
また、ユーザの顔の向きを変えた場合には、音声による指示や、自動で撮影をするように工夫をした。よって、ユーザが撮影するための操作をするのが困難な場合にも、対応できるものにでき、利便性に優れたものにできる。
さらに、本人認証の都度、指示内容を異なるものにすることで、毎回の認証時において、不正行為を防ぐことができる。
【００９３】
（２）同様に、本人確認処理時に、携帯端末２０１は、指示情報に基づいてユーザの顔の向きを変えさせて、ユーザの顔画像を複数回撮影するものを含むようにした。よって、本人認証時のみならず本人確認時においても、指示情報にしたがった撮影が必要にあり、予め用意した画像を用いる等の不正行為を防ぐことができる。
【００９４】
（３）本人確認処理時に、携帯端末２０１は、顔写真が確認可能な複数の異なる撮影方向から本人確認書類を撮影して、複数の本人確認画像を得るようにした。そして、複数の本人確認画像のうちの少なくとも１つは、本人確認書類の厚さを確認できるものであるようにした。よって、真の本人確認書類であることを、本人確認画像によって判別できるようになり、セキュリティ性が向上したものにできる。
【００９５】
（４）携帯端末２０１は、本人確認画像を取得するための書類位置ガイド画像を出力させるようにした。そして、書類位置ガイド画像は、顔写真を確認可能な撮影方向と、本人確認画像の大きさを含む本人確認書類の配置位置とを指定する画像であるため、ユーザに書類ガイド画像にしたがって本人確認書類を撮影させることができる。また、撮影方向と配置位置とが指定されているため、その場で本人確認書類を用意して撮影しなければならないものになり、予め用意した画像を用いる等の不正行為を防ぐことができる。
【００９６】
以上、本発明の実施形態について説明したが、本発明は上述した実施形態に限定されるものではない。また、実施形態に記載した効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、実施形態に記載したものに限定されない。なお、上述した実施形態及び後述する変形形態は、適宜組み合わせて用いることもできるが、詳細な説明は省略する。
【００９７】
（変形形態）
（１）各実施形態では、携帯端末が本人確認の際に取得した顔画像を、本人認証の際の照合に用いる画像とするものを例に説明したが、これに限定されない。携帯端末が本人確認の際に取得した本人確認画像から得られた顔写真画像を、本人認証の際の照合に用いる画像としてもよい。しかし、携帯端末が本人確認の際に取得した顔画像は、本人認証の際

に撮影して取得する顔画像と同じインカメラを用いて撮影された画像であり、両者は類似した撮影条件で取得した画像になる。そのため、携帯端末が本人確認の際に取得した顔画像の方が、照合時の精度が良くなる可能性がある。

（２）各実施形態では、本人確認の処理として、本人確認書類から得た顔写真画像と、顔画像とを、本人認証サーバで照合し、照合できた場合に、本人確認ができたものとして説明したがこれに限定されない。本人確認の処理として、他の確認処理を含めてもよい。

【００９８】

（３）各実施形態では、本人確認の処理で行われる本人確認画像処理を、携帯端末のみで行うものを例に説明したが、これに限定されない。携帯端末で行う画像取得以外の処理を、本人確認サーバが行ってもよいし、本人確認サーバが行っている処理を、携帯端末で行ってもよい。例えば、取得した各画像の確認処理を、本人確認サーバで行ってもよい。また、本人確認サーバと、携帯端末との両方で、各画像の確認処理を行ってもよい。

【００９９】

さらに、本人確認画像処理として、本人確認書類による処理の一部を、本人認証サーバで行ってもよい。

具体的には、本人認証サーバの本人確認処理部は、運転免許証を撮影して得られた本人確認画像を、携帯端末から受信する。そして、本人認証サーバの本人確認処理部は、ＯＣＲ（光学式文字認識）によって、本人確認書類に含まれる文字をテキスト化する。その後、本人確認処理部は、テキスト化した文字列を、携帯端末に送信する。携帯端末の本人確認部は、テキスト化した文字列を受信し、タッチパネルディスプレイに文字情報を表示させる。なお、携帯端末は、表示された文字情報を修正する機能を有してもよい。そして、本人認証サーバから取得した文字情報は、例えば、本人確認ができた場合に、サービス提供サーバに対して送信することができる。

このような処理を行うことで、ユーザがサービスを利用する際に必要になる氏名等を、テキスト化された文字情報を用いればよく、ユーザが入力する手間を省くことができる。また、受信した文字情報を携帯端末で修正可能にすることで、誤変換であったり、本人確認書類に記載の氏名や住所が変更になったりした場合であっても、変更箇所のみを変更すればよく、利便性が高いものにできる。

【０１００】

（４）各実施形態では、本人確認画像に含まれる本人確認書類に関して、特段の処理を行っていないが、同じであるかの照合を行ってもよい。また、各処理にて取得した複数の画像について、被写体が同一のものである確認を行ってもよい。

【０１０１】

（５）第２実施形態では、複数の本人確認画像を取得し、正面から撮影した本人確認画像から顔写真画像を抽出するものを例に説明したが、これに限定されない。本人確認書類の厚さが確認できる撮影方向からの撮影により取得した本人確認画像から顔写真画像を抽出してもよい。その場合、例えば、公知の画像補正技術を用いて正面から撮影したような画像に歪みを補正して、顔照合処理に用いる画像にしてもよい。また、この補正技術を用いて、複数の本人確認画像が同一の本人確認書類を撮影した画像であることを確認してもよい。

【０１０２】

（６）第２実施形態では、撮影の際にガイドとなる画像を出力するものを説明した。その際、ガイドとなる画像を出力してから撮影するまでの時間について、特段記載していないが、制御部は、所定の時間内に撮影されなかった場合には、エラーとして以降の処理を行わないようにしてもよい。

【０１０３】

（７）各実施形態での本人確認及び本人認証を行うサービスについては、様々なものが該当する。例えば、銀行業務であれば、口座開設及び口座の紐付け処理や、ＡＴＭを用いた現金引き出し等の処理等に用いることができる。ＡＴＭを用いるものとしては、携帯端末で本人認証を行って、認証された場合にＱＲコード（登録商標）を表示させて、ＡＴＭ

に読み取らせることで、携帯端末を、キャッシュカードの代わりとすることができる。また、窓口での業務で、代理人が本人に代わって行う場合に、本人による本人認証がされたことを証明する情報を代理人が受信等することで、委任状等を予め用意せずに済む。

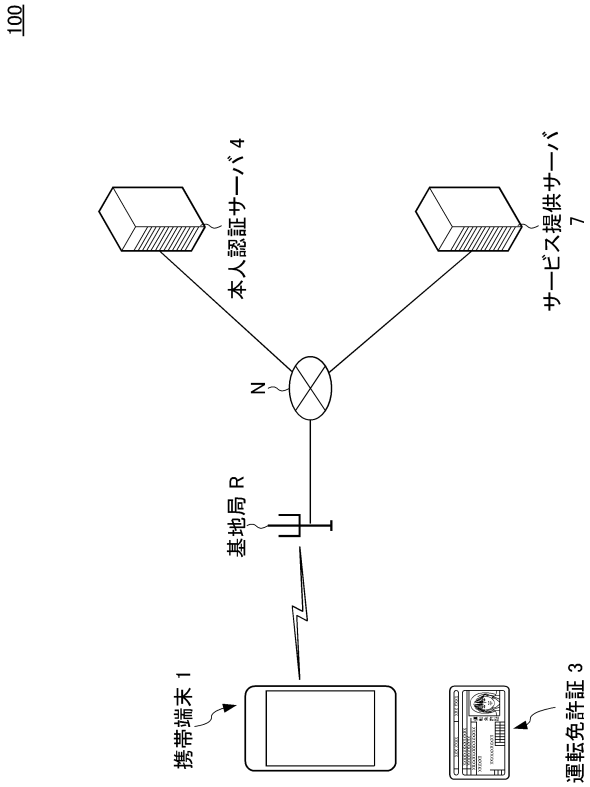
【符号の説明】

【０１０４】

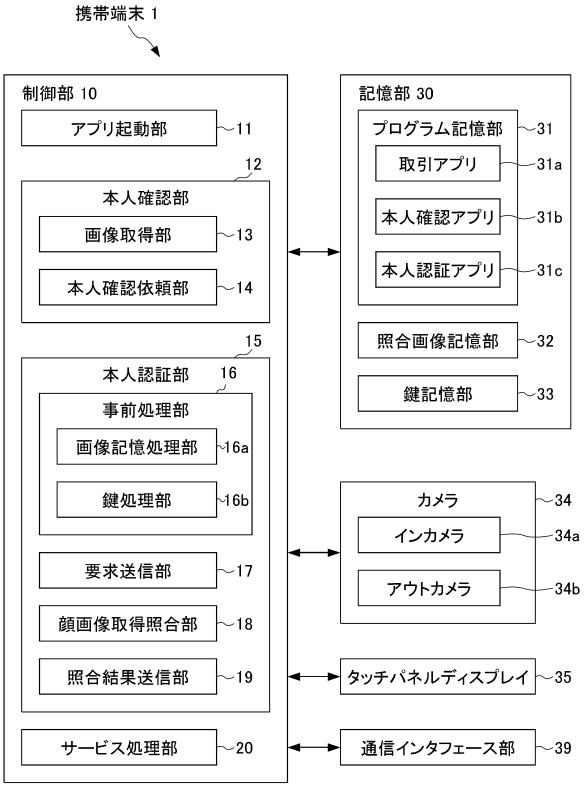
１，２０１　携帯端末
３　運転免許証
４　本人認証サーバ
７　サービス提供サーバ
１０，４０，２１０　制御部
１２，２１２　本人確認部
１３，２１３　画像取得部
１４，２１４　本人確認依頼部
１５，２１５　本人認証部
１６ａ　画像記憶処理部
１６ｂ　鍵処理部
１７　要求送信部
１８　顔画像取得照合部
１９　照合結果送信部
２０　サービス処理部
３０，５０，２３０　記憶部
３１ａ　取引アプリ
３１ｂ，２３１ｂ　本人確認アプリ
３１ｃ，２３１ｃ　本人認証アプリ
３２　照合画像記憶部
３３，５３　鍵記憶部
３４　カメラ
３５　タッチパネルディスプレイ
４１　本人確認処理部
４２　鍵受信処理部
４３　コード生成送信部
４４　サービス利用許可部
１００，２００　本人認証システム
２１８ａ　顔画像取得部
２１８ｂ　顔画像照合部

【図面】

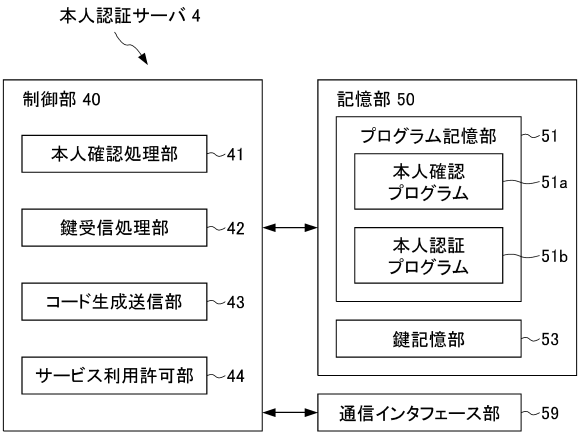
【図１】


100
本人認証サーバ 4
サービス提供サーバ 7
N
基地局 R
携帯端末 1
運転免許証 3

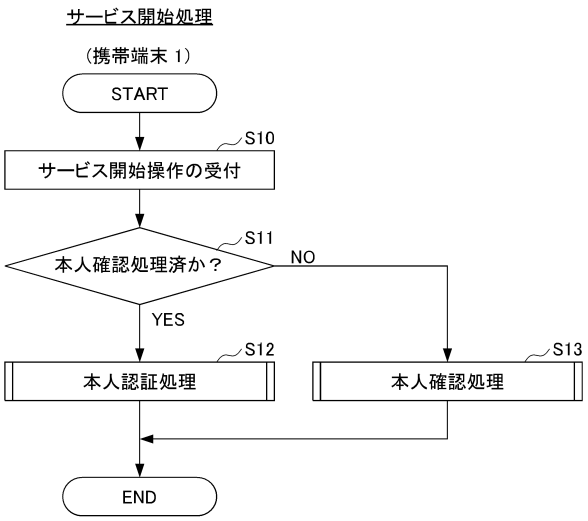
【図２】


携帯端末 1
制御部 10
アプリ起動部 11
12
本人確認部
画像取得部 13
本人確認依頼部 14
15
本人認証部 16
事前処理部
画像記憶処理部 16a
鍵処理部 16b
要求送信部 17
顔画像取得照合部 18
照合結果送信部 19
サービス処理部 20
記憶部 30
プログラム記憶部 31
取引アプリ 31a
本人確認アプリ 31b
本人認証アプリ 31c
照合画像記憶部 32
鍵記憶部 33
カメラ 34
インカメラ 34a
アウトカメラ 34b
タッチパネルディスプレイ 35
通信インタフェース部 39

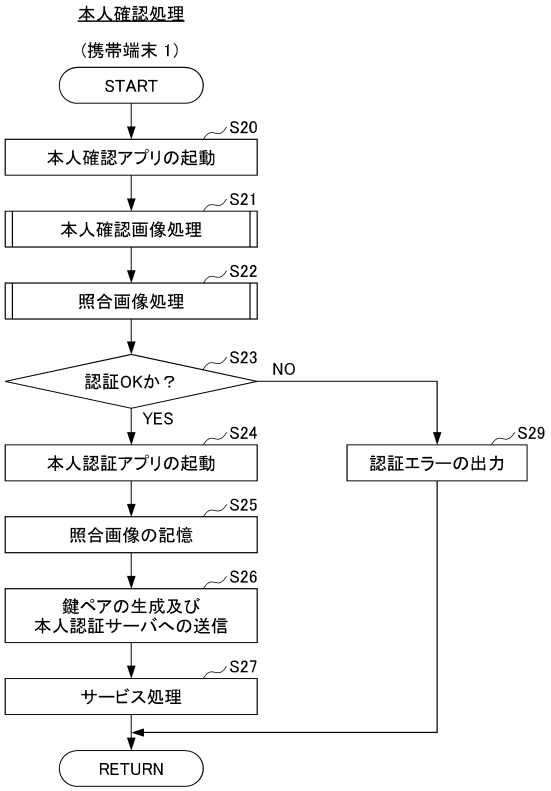
【図３】


本人認証サーバ 4
制御部 40
本人確認処理部 41
鍵受信処理部 42
コード生成送信部 43
サービス利用許可部 44
記憶部 50
プログラム記憶部 51
本人確認プログラム 51a
本人認証プログラム 51b
鍵記憶部 53
通信インタフェース部 59

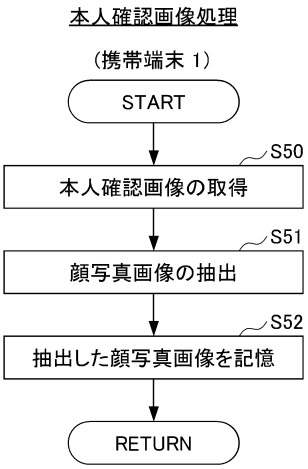
【図４】


サービス開始処理
（携帯端末 1）
START
S10
サービス開始操作の受付
S11
本人確認処理済か？
NO
YES
S12
本人認証処理
S13
本人確認処理
END

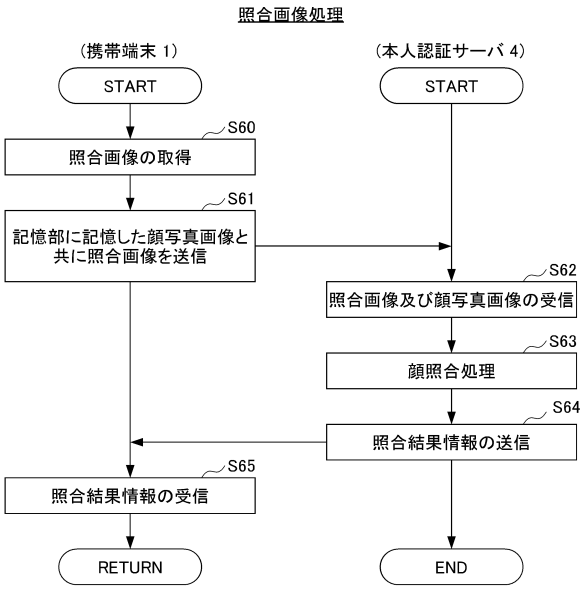
【図５】


本人確認処理
（携帯端末 1）
START
S20
本人確認アプリの起動
S21
本人確認画像処理
S22
照合画像処理
S23
認証OKか？
NO
YES
S24
本人認証アプリの起動
S25
照合画像の記憶
S26
鍵ペアの生成及び
本人認証サーバへの送信
S27
サービス処理
S29
認証エラーの出力
RETURN

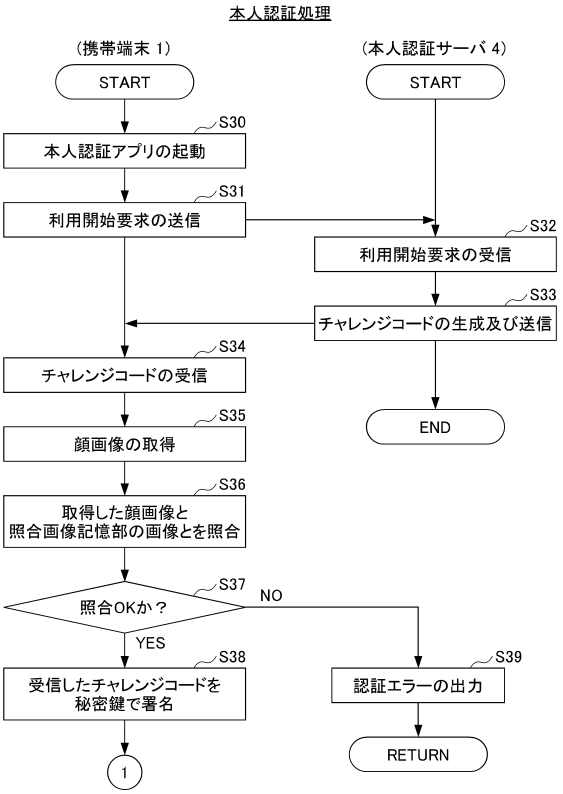
【図６】


本人確認画像処理
（携帯端末 1）
START
S50
本人確認画像の取得
S51
顔写真画像の抽出
S52
抽出した顔写真画像を記憶
RETURN

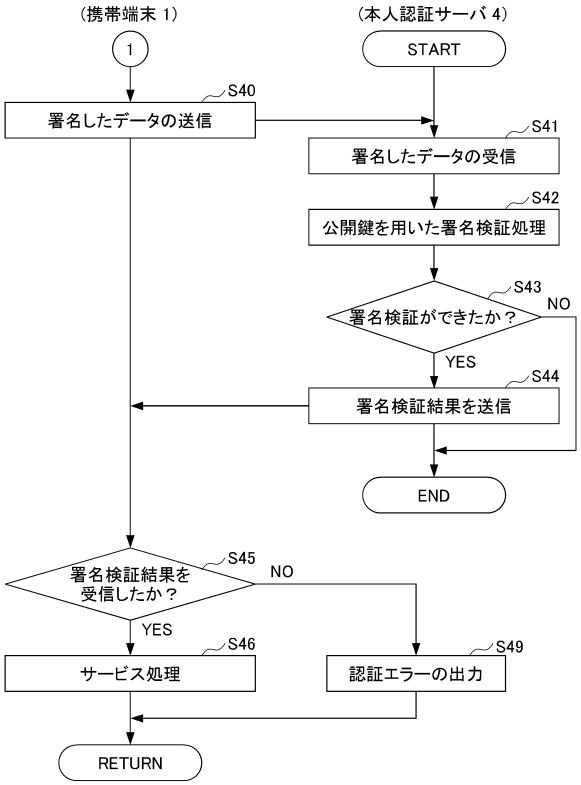
【図７】


照合画像処理
（携帯端末 1）
（本人認証サーバ 4）
START
START
S60
照合画像の取得
S61
記憶部に記憶した顔写真画像と
共に照合画像を送信
S62
照合画像及び顔写真画像の受信
S63
顔照合処理
S64
照合結果情報の送信
S65
照合結果情報の受信
RETURN
END

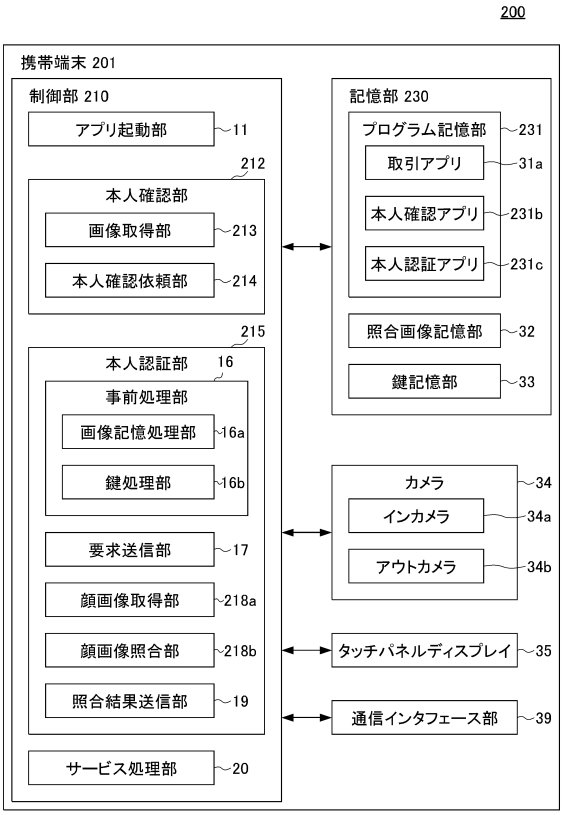
【図８】


本人認証処理
（携帯端末 1）
（本人認証サーバ 4）
START
START
S30
本人認証アプリの起動
S31
利用開始要求の送信
S32
利用開始要求の受信
S33
チャレンジコードの生成及び送信
S34
チャレンジコードの受信
END
S35
顔画像の取得
S36
取得した顔画像と
照合画像記憶部の画像とを照合
S37
照合OKか？
NO
YES
S38
受信したチャレンジコードを
秘密鍵で署名
S39
認証エラーの出力
1
RETURN

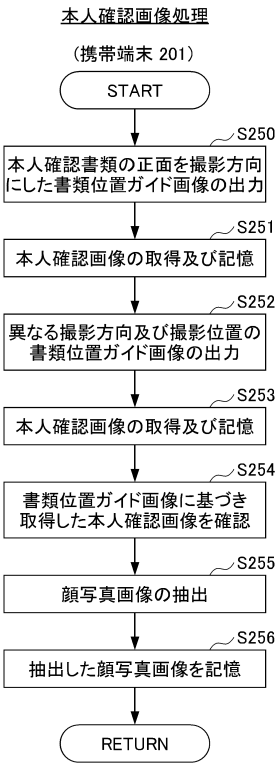
【図９】



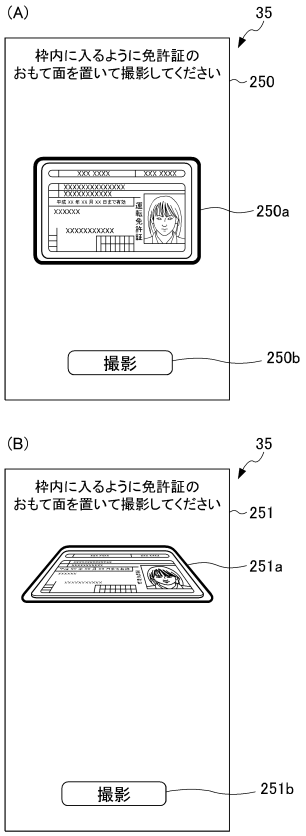
【図１０】



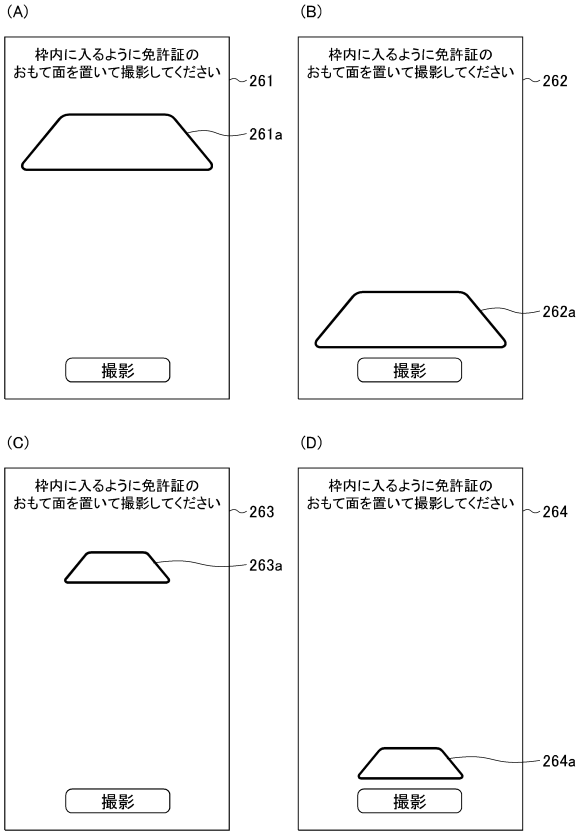
【図１１】



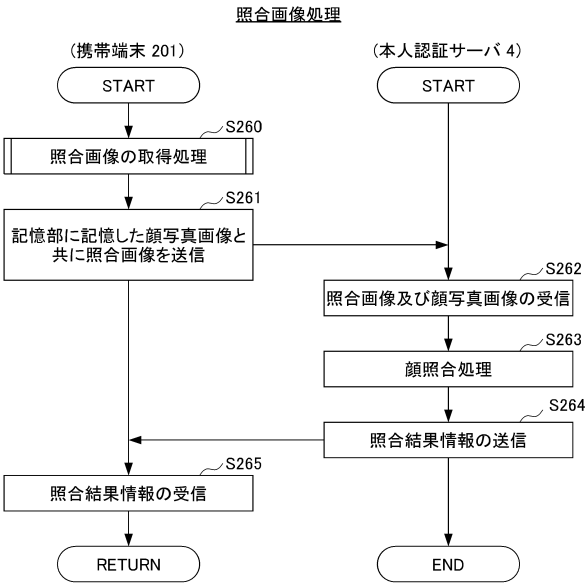
【図１２】



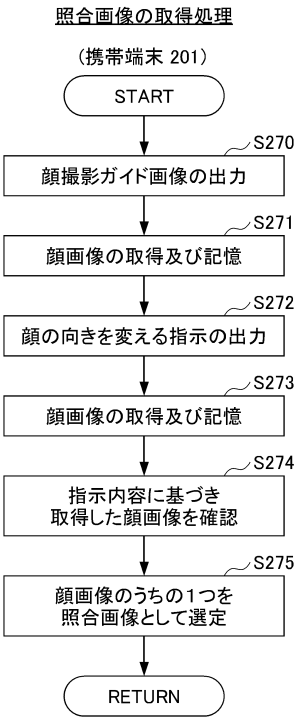
【図１３】



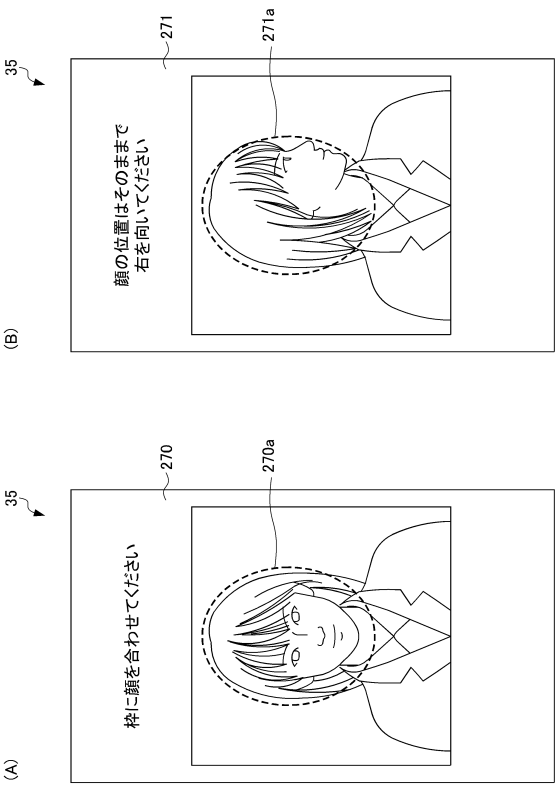
【図１４】



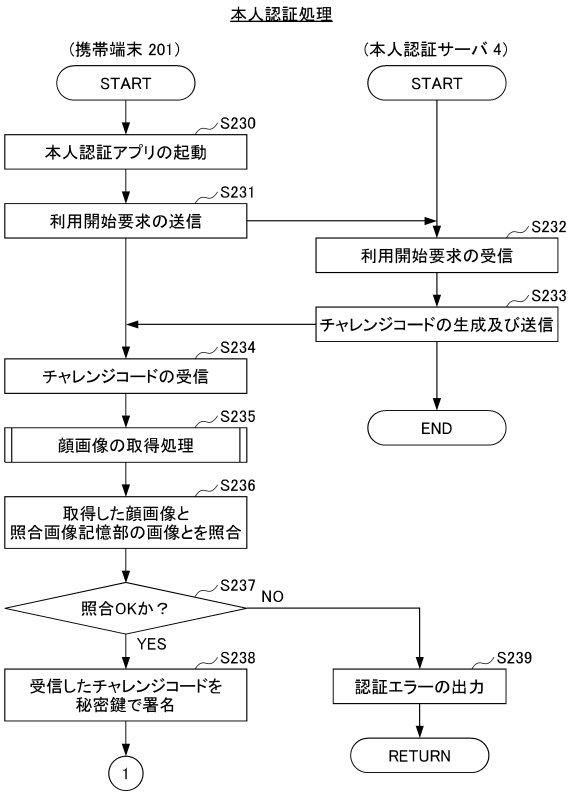
【図１５】



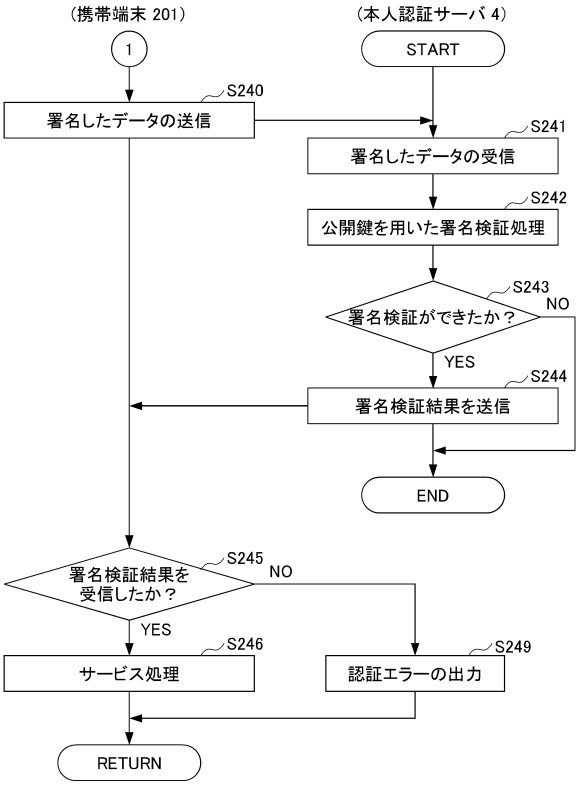
【図１６】



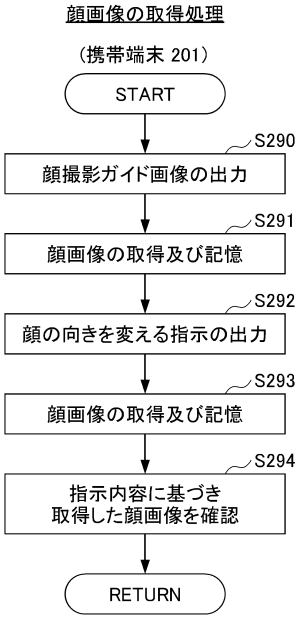
【図１７】


本人認証処理
（携帯端末 201）
（本人認証サーバ 4）
START
START
S230
本人認証アプリの起動
S231
利用開始要求の送信
S232
利用開始要求の受信
S233
チャレンジコードの生成及び送信
END
S234
チャレンジコードの受信
S235
顔画像の取得処理
S236
取得した顔画像と
照合画像記憶部の画像とを照合
S237
照合OKか？
NO
YES
S238
受信したチャレンジコードを
秘密鍵で署名
S239
認証エラーの出力
RETURN
1

【図１８】


（携帯端末 201）
（本人認証サーバ 4）
1
START
S240
署名したデータの送信
S241
署名したデータの受信
S242
公開鍵を用いた署名検証処理
S243
署名検証ができたか？
NO
YES
S244
署名検証結果を送信
END
S245
署名検証結果を
受信したか？
NO
YES
S246
サービス処理
S249
認証エラーの出力
RETURN

【図１９】


顔画像の取得処理
（携帯端末 201）
START
S290
顔撮影ガイド画像の出力
S291
顔画像の取得及び記憶
S292
顔の向きを変える指示の出力
S293
顔画像の取得及び記憶
S294
指示内容に基づき
取得した顔画像を確認
RETURN

フロントページの続き

(72)発明者　木村 雅則
東京都新宿区市谷加賀町一丁目１番１号 大日本印刷株式会社内
審査官　吉田 歩

(56)参考文献　特開２００５－２９３５４４（ＪＰ，Ａ）
国際公開第２００７／０１０５９７（WO，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３２
Ｇ０６Ｆ　２１／３３
Ｈ０４Ｌ　９／３２
Ｇ０９Ｃ　１／００