(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7484095号
(P7484095)

(45)発行日　令和6年5月16日(2024.5.16)

(24)登録日　令和6年5月8日(2024.5.8)

(51)国際特許分類

Ｇ０６Ｑ	*20/40*	*(2012.01)*	Ｇ０６Ｑ	20/40
Ｇ０６Ｆ	*21/30*	*(2013.01)*	Ｇ０６Ｆ	21/30
Ｇ０６Ｆ	*21/32*	*(2013.01)*	Ｇ０６Ｆ	21/32

ＦＩ

請求項の数　6　（全26頁）

(21)出願番号　特願2019-127693(P2019-127693)
(22)出願日　令和1年7月9日(2019.7.9)
(65)公開番号　特開2021-12640(P2021-12640A)
(43)公開日　令和3年2月4日(2021.2.4)
審査請求日　令和4年5月27日(2022.5.27)

(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】　金融取引システム及び金融取引方法

(57)【特許請求の範囲】

【請求項１】

ユーザが所持する、撮影部を備えた携帯端末と、

前記携帯端末に対して通信可能に接続され、本人認証処理を行う本人認証サーバと、

前記携帯端末と、金融取引業務を行う銀行サーバとの各々に対して通信可能に接続され、前記ユーザによる前記銀行サーバを用いた金融取引を仲介する取引仲介サーバと、

を備えた金融取引システムであって、

前記銀行サーバは、口座情報と、前記銀行サーバへのログイン処理に用いる前記ユーザを識別するユーザ識別情報とを対応付けて記憶する口座情報記憶部を備え、

前記取引仲介サーバは、利用者識別情報と、銀行識別情報と、前記ユーザ識別情報とを対応付けて記憶する利用者情報記憶部を備え、

前記携帯端末は、

前記ユーザの本人確認の際に前記撮影部を介して取得した前記ユーザの顔画像を照合画像として、前記取引仲介サーバへのログインに用いる前記利用者識別情報に対応付けて記憶した照合画像記憶部と、

前記利用者識別情報と、前記銀行識別情報との入力を受け付ける入力受付手段と、

前記撮影部を介して前記ユーザの顔画像を取得する画像取得手段と、

前記入力受付手段により受け付けた前記利用者識別情報が、前記照合画像記憶部に記憶されている場合に、前記画像取得手段により取得した前記ユーザの顔画像と、前記照合画像記憶部に記憶された前記照合画像とを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く認証結果を、前記携帯端末に送信する認証結果送信手段を備え、
前記携帯端末は、前記認証結果と、前記利用者識別情報と、前記銀行識別情報とを含む取引要求を、前記取引仲介サーバに対して送信する要求送信手段を備え、
前記取引仲介サーバは、受信した前記利用者識別情報と、前記銀行識別情報とに基づいて、前記利用者情報記憶部を参照して対応する前記ユーザ識別情報を抽出し、前記銀行識別情報に対応する前記銀行サーバに対して、前記認証結果と、前記ユーザ識別情報を含む取引実行要求を送信する実行要求手段を備え、
前記銀行サーバは、前記ユーザ識別情報に対応付けられた前記口座情報を、前記口座情報記憶部を参照して特定し、前記認証結果に基づいて、前記口座情報を用いた取引を許可するか否かを決定する取引決定手段を備える、
金融取引システム。
【請求項２】
請求項１に記載の金融取引システムにおいて、
前記照合画像記憶部は、前記ユーザの顔写真を含む本人確認書類の画像と共に本人確認に用いられた、前記ユーザの顔画像を、前記照合画像として記憶する、
金融取引システム。
【請求項３】
請求項１又は請求項２に記載の金融取引システムにおいて、
前記携帯端末は、本人認証方法の指定を受け付ける認証方法受付手段を備え、
前記携帯端末の前記画像取得手段は、前記認証方法受付手段による前記本人認証方法の指定が顔認証である場合に、前記撮影部を介して前記ユーザの顔画像を取得する、
金融取引システム。
【請求項４】
請求項３に記載の金融取引システムにおいて、
前記携帯端末は、
前記認証方法受付手段による前記本人認証方法の指定が顔認証であって、前記照合画像記憶部に前記照合画像が記憶されていない場合に、前記本人認証サーバに対して、本人確認書類の画像と、前記顔画像とを送信し、本人確認処理を行う本人確認処理手段と、
前記本人認証サーバから本人確認ができた旨を受信した場合に、前記顔画像を前記照合画像として、前記入力受付手段により受け付けた前記利用者識別情報に関連付けて前記照合画像記憶部に記憶させる関連付け手段と、
を備える、
金融取引システム。
【請求項５】
請求項３又は請求項４に記載の金融取引システムにおいて、
前記携帯端末は、取引項目を受け付ける取引項目受付手段を備え、
前記携帯端末の前記認証方法受付手段は、前記取引項目受付手段により受け付けた前記取引項目に応じて、前記本人認証方法の指定を受け付ける、
金融取引システム。
【請求項６】
ユーザが所持する、撮影部を備えた携帯端末が、前記ユーザの顔写真を含む本人確認書類の画像と共に本人確認に用いられた、前記ユーザの本人確認の際に前記撮影部を介して取得した前記ユーザの顔画像を照合画像として、前記携帯端末に対して通信可能に接続され、金融取引業務を行う銀行サーバを用いた金融取引を仲介する取引仲介サーバへのログイン処理に用いる前記ユーザを識別する利用者識別情報に対応付けて記憶した照合画像記憶部を備え、

前記携帯端末が、前記利用者識別情報と、銀行識別情報との入力を受け付ける入力受付ステップと、
前記携帯端末が、前記撮影部を介して前記ユーザの顔画像を取得する画像取得ステップと、
前記携帯端末が、前記入力受付ステップにより受け付けた前記利用者識別情報が、前記照合画像記憶部に記憶されている場合に、前記画像取得ステップにより取得した前記ユーザの顔画像と、前記照合画像記憶部に記憶された前記照合画像とを照合する顔画像照合ステップと、
前記携帯端末が、前記顔画像照合ステップによる照合結果を、前記携帯端末に対して通信可能に接続され、本人認証処理を行う本人認証サーバに送信する照合結果送信ステップと、
前記本人認証サーバが、前記照合結果に基づく認証結果を、前記携帯端末に送信する認証結果送信ステップと、
前記携帯端末が、前記認証結果と、前記利用者識別情報と、前記銀行識別情報とを含む取引要求を、前記取引仲介サーバに対して送信する要求送信ステップと、
前記取引仲介サーバが、受信した前記利用者識別情報と前記銀行識別情報とに基づき、前記銀行サーバへのログイン処理に用いる前記ユーザを識別するユーザ識別情報を、前記利用者識別情報と前記銀行識別情報と前記ユーザ識別情報とを対応付けて記憶する利用者情報記憶部から抽出し、前記銀行識別情報に対応する前記銀行サーバに対して、前記認証結果と、前記ユーザ識別情報とを含む取引実行要求を送信する実行要求ステップと、
前記銀行サーバが、受信した前記ユーザ識別情報に対応付けられた口座情報を、前記口座情報と前記ユーザ識別情報とを対応付けて記憶する口座情報記憶部を参照して特定し、前記認証結果に基づいて前記口座情報を用いた取引を許可するか否かを決定する取引決定ステップと、
を含む、
金融取引方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、金融取引システム及び金融取引方法に関する。
【背景技術】
【０００２】
従来、銀行等の金融機関では、インターネット等の通信ネットワークを介して、顧客にサービスを提供する、いわゆるインターネットバンキングによるサービスの提供が行われている。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厳格に行うことが求められる。そのため、例えば、生体情報を利用することが考えられている。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１参照）。
【０００３】
また、資金移動取引等、本人であることをより厳格に求める取引を行う場合に、ワンタイムパスワードを用いる方法がある。利用者は、携帯端末等の入力画面にワンタイムパスワードを入力し、入力されたワンタイムパスワードが正しい場合に、取引が可能になる。
【先行技術文献】
【特許文献】
【０００４】
【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】
【０００５】

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。

そして、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。そのため、サービスを利用する都度、顔画像に代表される生体情報が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。

【０００６】

また、ワンタイムパスワードを用いるものは、利用者に通知されるまでの手続が煩雑である。そのため、ワンタイムパスワードに代わる本人認証方法が求められていた。

【０００７】

そこで、本発明は、セキュリティ性の高い本人認証方法を用いて金融取引を可能にした金融取引システム、携帯端末、認証モジュール及び金融取引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】

【０００８】

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。

【０００９】

第１の発明は、ユーザが所持する、撮影部（３４）を備えた携帯端末（１）と、前記携帯端末に対して通信可能に接続され、本人認証処理を行う本人認証サーバ（４）と、前記携帯端末に対して通信可能に接続され、金融取引業務を行う銀行サーバ（７）と、を備えた金融取引システム（１００）であって、前記銀行サーバは、口座情報と、ユーザ識別情報とを対応付けて記憶する口座情報記憶部（７７）を備え、前記携帯端末は、前記ユーザの本人確認の際に前記撮影部を介して取得した前記ユーザの顔画像を照合画像として、前記銀行サーバへのログイン処理に用いる前記ユーザ識別情報に対応付けて記憶した照合画像記憶部（３２）と、前記ユーザ識別情報の入力を受け付ける入力受付手段（１１）と、前記撮影部を介して前記ユーザの顔画像を取得する画像取得手段（１７）と、前記入力受付手段により受け付けた前記ユーザ識別情報が、前記照合画像記憶部に記憶されている場合に、前記画像取得手段により取得した前記ユーザの顔画像と、前記照合画像記憶部に記憶された前記照合画像とを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く認証結果を、前記携帯端末に送信する認証結果送信手段（４４）を備え、前記携帯端末は、前記本人認証サーバから受信した前記認証結果と、前記ユーザ識別情報とを含む取引要求を、前記銀行サーバに対して送信する要求送信手段（２０）を備え、前記銀行サーバは、前記ユーザ識別情報に対応付けられた前記口座情報を、前記口座情報記憶部を参照して特定し、前記認証結果に基づいて前記口座情報を用いた取引を許可するか否かを決定する取引決定手段（７１）を備える、金融取引システムである。

第２の発明は、第１の発明の金融取引システム（１００）において、前記携帯端末（１）は、本人認証方法の指定を受け付ける認証方法受付手段（１１）を備え、前記携帯端末の前記画像取得手段（１７）は、前記認証方法受付手段による前記本人認証方法の指定が顔認証である場合に、前記撮影部を介して前記ユーザの顔画像を取得する、金融取引システムである。

第３の発明は、第２の発明の金融取引システム（１００）において、前記携帯端末（１）は、前記認証方法受付手段（１１）による前記本人認証方法の指定が顔認証であって、前記照合画像記憶部（３２）に記憶された前記照合画像が、前記ユーザ識別情報が対応付けられていない場合に、前記入力受付手段（１１）によって受け付けた前記ユーザ識別情報を、前記照合画像に関連付ける関連付け手段（１４）を備える、金融取引システムであ

る。

第４の発明は、第３の発明の金融取引システム（１００）において、前記携帯端末（１）は、前記認証方法受付手段（１１）による前記本人認証方法の指定が顔認証であって、前記照合画像記憶部（３２）に前記照合画像が記憶されていない場合に、前記本人認証サーバ（４）に対して、本人確認書類の画像と、前記顔画像とを送信し、本人確認処理を行う本人確認処理手段（１４）を備え、前記携帯端末の前記関連付け手段（１４）は、前記本人認証サーバから本人確認ができた旨を受信した場合に、前記顔画像を前記照合画像として、前記入力受付手段（１１）により受け付けた前記ユーザ識別情報に関連付けて前記照合画像記憶部に記憶させる、金融取引システムである。

第５の発明は、第２の発明から第４の発明までのいずれかの金融取引システム（１００）において、前記携帯端末（１）は、取引項目を受け付ける取引項目受付手段（１１）を備え、前記携帯端末の前記認証方法受付手段（１１）は、前記取引項目受付手段により受け付けた前記取引項目に応じて、前記本人認証方法の指定を受け付ける、金融取引システムである。

第６の発明は、ユーザが所持する、撮影部（３４）を備えた携帯端末（２０１）と、前記携帯端末に対して通信可能に接続され、本人認証処理を行う本人認証サーバ（４）と、前記携帯端末と、金融取引業務を行う銀行サーバ（７）との各々に対して通信可能に接続され、前記ユーザによる前記銀行サーバを用いた金融取引を仲介する取引仲介サーバ（２０８）と、を備えた金融取引システム（２００）であって、前記銀行サーバは、口座情報と、前記銀行サーバへのログイン処理に用いる前記ユーザを識別するユーザ識別情報とを対応付けて記憶する口座情報記憶部（７７）を備え、前記取引仲介サーバは、利用者識別情報と、銀行識別情報と、前記ユーザ識別情報とを対応付けて記憶する利用者情報記憶部（２８７）を備え、前記携帯端末は、前記ユーザの本人確認の際に前記撮影部を介して取得した前記ユーザの顔画像を照合画像として、前記取引仲介サーバへのログインに用いる前記利用者識別情報に対応付けて記憶した照合画像記憶部（２３２）と、前記利用者識別情報と、前記銀行識別情報との入力を受け付ける入力受付手段（２１１）と、前記撮影部を介して前記ユーザの顔画像を取得する画像取得手段（１７）と、前記入力受付手段により受け付けた前記利用者識別情報が、前記照合画像記憶部に記憶されている場合に、前記画像取得手段により取得した前記ユーザの顔画像と、前記照合画像記憶部に記憶された前記照合画像とを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く認証結果を、前記携帯端末に送信する認証結果送信手段（４４）を備え、前記携帯端末は、前記認証結果と、前記利用者識別情報と、前記銀行識別情報とを含む取引要求を、前記取引仲介サーバに対して送信する要求送信手段（２２０）を備え、前記取引仲介サーバは、受信した前記利用者識別情報と、前記銀行識別情報とに基づいて、前記利用者情報記憶部を参照して対応する前記ユーザ識別情報を抽出し、前記銀行識別情報に対応する前記銀行サーバに対して、前記認証結果と、前記ユーザ識別情報を含む取引実行要求を送信する実行要求手段（２８１）を備え、前記銀行サーバは、前記ユーザ識別情報に対応付けられた前記口座情報を、前記口座情報記憶部を参照して特定し、前記認証結果に基づいて、前記口座情報を用いた取引を許可するか否かを決定する取引決定手段（７１）を備える、金融取引システムである。

第７の発明は、ユーザが所持する、撮影部（３４）を備えた携帯端末（１）であって、前記ユーザの本人確認の際に前記撮影部を介して取得した前記ユーザの顔画像を照合画像として、通信可能に接続され金融取引業務を行う銀行サーバ（７）へのログイン処理に用いる前記ユーザを識別するユーザ識別情報に対応付けて記憶した照合画像記憶部（３２）と、前記ユーザ識別情報の入力を受け付ける入力受付手段（１１）と、前記撮影部を介して前記ユーザの顔画像を取得する画像取得手段（１７）と、前記入力受付手段により受け付けた前記ユーザ識別情報が、前記照合画像記憶部に記憶されている場合に、前記画像取得手段により取得した前記ユーザの顔画像と、前記照合画像記憶部に記憶された前記照合画像とを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、本人認証処理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、前記本人認証サーバから受信した認証結果と、前記ユーザ識別情報とを含む取引要求を、前記銀行サーバに対して送信する要求送信手段（２０）と、を備える、携帯端末である。

第８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である携帯端末（１）で実行する認証モジュール（３１ｃ）であって、前記携帯端末は、前記ユーザの本人確認の際に前記撮影部を介して取得した前記ユーザの顔画像を照合画像として、金融取引業務を行う銀行サーバ（７）へのログイン処理に用いる前記ユーザを識別するユーザ識別情報に対応付けて記憶した照合画像記憶部（３２）と、前記銀行サーバとの間で銀行取引を行うための銀行取引プログラム（３１ａ）と、を備え、前記携帯端末を、前記撮影部を介して前記ユーザの顔画像を取得する画像取得手段と、前記銀行取引プログラムから受け渡された前記ユーザ識別情報が、前記照合画像記憶部に記憶された前記ユーザ識別情報に一致する場合に、前記画像取得手段により取得した前記ユーザの顔画像と、前記照合画像記憶部に記憶された前記照合画像とを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、前記携帯端末に対して通信可能に接続され、本人認証処理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、前記本人認証サーバから受信した認証結果を、前記銀行取引プログラムに受け渡す手段と、して機能させるための認証モジュールである。

第９の発明は、ユーザが所持する、撮影部（３４）を備えた携帯端末（１）が、前記ユーザの本人確認の際に前記撮影部を介して取得した前記ユーザの顔画像を照合画像として、前記携帯端末に対して通信可能に接続され、金融取引業務を行う銀行サーバへのログイン処理に用いる前記ユーザを識別するユーザ識別情報に対応付けて記憶した照合画像記憶部（３２）を備え、前記携帯端末が、前記ユーザ識別情報の入力を受け付ける入力受付ステップと、前記携帯端末が、前記撮影部を介して前記ユーザの顔画像を取得する画像取得ステップと、前記携帯端末が、前記入力受付ステップにより受け付けた前記ユーザ識別情報が、前記照合画像記憶部に記憶されている場合に、前記画像取得ステップにより取得した前記ユーザの顔画像と、前記照合画像記憶部に記憶された前記照合画像とを照合する顔画像照合ステップと、前記携帯端末が、前記顔画像照合ステップによる照合結果を、前記携帯端末に対して通信可能に接続され、本人認証処理を行う本人認証サーバ（４）に送信する照合結果送信ステップと、前記本人認証サーバが、前記照合結果に基づく認証結果を、前記携帯端末に送信する認証結果送信ステップと、前記携帯端末が、前記認証結果と、前記ユーザ識別情報とを含む取引要求を、前記銀行サーバに対して送信する要求送信ステップと、前記銀行サーバが、前記ユーザ識別情報に対応付けられた口座情報を、口座情報と、ユーザ識別情報とを対応付けて記憶する口座情報記憶部（７７）を参照して特定し、前記認証結果に基づいて前記口座情報を用いた取引を許可するか否かを判定する取引判定ステップと、を含む、金融取引方法である。

【発明の効果】

【００１０】

本発明によれば、セキュリティ性の高い本人認証方法を用いて金融取引を可能にした金融取引システム、携帯端末、認証モジュール及び金融取引方法を提供することができる。

【図面の簡単な説明】

【００１１】

【図１】第１実施形態に係る金融取引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及び銀行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取引開始時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表示例を示す図である。

【図６】第１実施形態に係る携帯端末での生体認証による確認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８】第１実施形態に係る携帯端末及び本人認証サーバでの照合画像処理を示すフローチャートである。
【図９】第１実施形態に係る携帯端末及び本人認証サーバでの本人認証処理を示すフローチャートである。
【図１０】図９の続きである。
【図１１】第２実施形態に係る金融取引システムの全体構成を示す図である。
【図１２】第２実施形態に係る携帯端末の機能ブロック図である。
【図１３】第２実施形態に係る取引仲介サーバの機能ブロック図及び利用者情報記憶部の例を示す図である。
【図１４】第２実施形態に係る金融取引システムでの取引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】
【００１２】
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。
【００１３】
（第１実施形態）
図１は、第１実施形態に係る金融取引システム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及び銀行サーバ７の機能ブロック図である。
図１に示す金融取引システム１００は、インターネットバンキングによる金融取引を、携帯端末１を用いて行うシステムである。そして、金融取引システム１００は、特に、振込等の資金移動取引の場合に、高セキュリティの認証である顔画像による生体認証を行うことで、携帯端末１によって安全に取引を行うためのシステムである。
【００１４】
ここで、本発明における本人確認とは、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う。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、なりすまし等を防ぐための確認をいう。
また、以下において、事前にインターネットバンキングの申込がされており、携帯端末１を使用したインターネットバンキングによる金融取引のうち、振込等の資金移動取引を希望する者に対する処理を説明するものである。
そして、以下において、携帯端末１を使用したインターネットバンキングによる金融取引のうち、振込等の資金移動取引を行う際に、顔画像を用いた本人確認又は本人認証を行うものを例に説明する。
【００１５】
金融取引システム１００は、携帯端末１と、本人認証サーバ４と、銀行サーバ７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及び銀行サーバ７は、通信ネットワークＮを介して携帯端末１と通信可能に接続されている。
【００１６】
携帯端末１は、例えば、銀行サーバ７によるサービスの提供を受けようとする者（以下、ユーザともいう。）が所持する端末である。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。
【００１７】
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、入力受付部１１（入力受付手段、認証方法受付手段、取引項目受付手段）と、認証確認処理部１２と、取引要求部２０（要求送信手段）とを備える。
【００１８】
入力受付部１１は、ユーザによる取引を行うための各種の入力を受け付ける。
例えば、入力受付部１１は、インターネットバンキングによる取引を行うために銀行サーバ７にログインするためのログイン情報の入力を受け付ける。ここで、ログイン情報とは、銀行サーバ７に予め登録されたログインＩＤ（ＩＤｅｎｔｉｆｉｃａｔｉｏｎ：ユーザ識別情報）及びパスワードをいう。そして、ログインＩＤ及びパスワードは、口座番号や、暗証番号とは異なるものである。
また、入力受付部１１は、取引項目の指定を受け付ける。取引項目とは、例えば、口座照会、振込等の金融取引に関する項目をいう。
さらに、入力受付部１１は、認証方法（本人認証方法）の選択を受け付ける。認証方法には、例えば、顔画像による生体認証（顔認証）や、ＯＴＰ（ワンタイムパスワード）による認証等がある。
【００１９】
認証確認処理部１２は、入力受付部１１が受け付けた取引項目の指定や認証方法に基づき所定の認証確認の処理を行う。
認証確認処理部１２は、関連付け確認部１３と、本人確認処理部１４（本人確認処理手段、関連付け手段）と、認証ＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）処理部１５とを備える。
【００２０】
関連付け確認部１３は、インターネットバンキングによる取引を行うために銀行サーバ７にログインするためのログインＩＤと、生体認証情報とが関連付けられているか否かを確認する。
本人確認処理部１４は、ログインＩＤと、生体認証情報とが関連付けられていない場合に行う処理である。本人確認処理部１４は、本人確認ＡＰＩ３１ｂにより行われる。
より具体的には、本人確認処理部１４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、本人確認処理部１４は、取得した本人確認画像から顔写真画像を抽出し、抽出した顔写真画像を記憶部３０に記憶させる。
【００２１】
また、本人確認処理部１４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し、取得した照合画像を記憶部３０に記憶させる。
その後、本人確認処理部１４は、記憶部３０に記憶された顔写真画像と照合画像とを、本人認証サーバ４に対して送信し、本人確認を依頼する。
そして、本人確認処理部１４は、本人認証サーバ４から本人確認結果を受信する。
【００２２】
本人認証サーバ４から受信した本人確認結果が照合できたものである場合に、本人確認処理部１４は、記憶部３０に記憶された照合画像を、照合画像記憶部３２に記憶させ、入力受付部１１が受け付けたログインＩＤを、照合画像（生体認証情報）に関連付ける。
また、本人確認処理部１４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、本人確認処理部１４は、生成した秘密鍵を、鍵記憶部３３に記憶させる。また、本人確認処理部１４は、生成した公開鍵を、本人認証サーバ４に送信する。

【００２３】
認証ＡＰＩ処理部１５は、ログインＩＤと、生体認証情報とが関連付けられている場合に行う処理である。認証ＡＰＩ処理部１５は、認証ＡＰＩ３１ｃにより行われる。
認証ＡＰＩ処理部１５は、認証要求部１６と、顔画像取得部１７（画像取得手段）と、顔画像照合部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。
【００２４】
認証要求部１６は、本人認証を行うための要求を、本人認証サーバ４に対して送信する。
顔画像取得部１７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。
顔画像照合部１８は、顔画像取得部１７によって取得した顔画像と、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、顔画像照合部１８により照合ができた場合に、認証要求部１６が認証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、署名データを本人認証サーバ４送信する。
【００２５】
取引要求部２０は、銀行サーバ７に対して、認証結果と、ログインＩＤとを含む取引要求を送信する。
【００２６】
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。
【００２７】
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、銀行取引アプリ３１ａ（銀行取引プログラム）と、本人確認ＡＰＩ３１ｂと、認証ＡＰＩ３１ｃ（認証モジュール）とを記憶している。なお、本実施形態では、以下において、銀行取引アプリ３１ａと、本人確認ＡＰＩ３１ｂと、認証ＡＰＩ３１ｃとを用いるものを説明するが、これに限定されるものではない。
【００２８】
銀行取引アプリ３１ａは、予め携帯端末１にインストールされ、又は、必要に応じて、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。
銀行取引アプリ３１ａは、銀行サーバ７を用いたインターネットバンキング取引を行うためのプログラムである。
本人確認ＡＰＩ３１ｂは、本人確認の機能を行うモジュール（プログラムの一種）である。より具体的には、本人確認ＡＰＩ３１ｂは、主に、本人確認画像を取得し、顔写真画像を抽出するモジュールである。
認証ＡＰＩ３１ｃは、本人認証の機能を行うモジュールである。より具体的には、認証ＡＰＩ３１ｃは、顔画像を取得し、照合画像との比較照合判定を行うモジュールである。
【００２９】
照合画像記憶部３２は、本人認証に用いる顔画像（照合画像）を、ログインＩＤに関連付け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ものと同じ顔画像が、ログインＩＤと関連付けられて記憶される。
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生成した鍵ペアのうち、秘密鍵が記憶される。
【００３０】
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３

４ｂ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。

【００３１】

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、金融取引システム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。

【００３２】

本人認証サーバ４は、本人確認及び本人認証の各処理を行うサーバである。例えば、銀行取引アプリ３１ａによる振込等の資金移動取引を開始する際に、携帯端末１においてインターネットバンキングのログインＩＤと顔画像とが関連付けられていない場合には、本人確認を行う。また、本人認証サーバ４は、２回目以降に銀行取引アプリ３１ａによる振込等の資金移動取引を行う際等、携帯端末１においてインターネットバンキングのログインＩＤと顔画像とが関連付けられている場合には、本人認証を行う。本人認証サーバ４は、例えば、銀行サーバ７を有する銀行等が有してもよいし、銀行等とは異なる認証に関するサービスを提供する企業が有してもよい。この例では、銀行サーバ７とは異なる企業が有するものとして説明する。

【００３３】

図３（Ａ）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。

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と、コード生成送信部４３と、認証結果送信部４４（認証結果送信手段）とを備える。

【００３４】

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。

【００３５】

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、携帯端末１から認証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。

認証結果送信部４４は、携帯端末１から受信した署名データを検証し、検証できた場合には、署名検証結果を、携帯端末１に送信する。

【００３６】

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、本人認証プログラム５１ａを記憶する。
本人認証プログラム５１ａは、本人認証サーバ４の制御部４０が実行する各種機能を行うためのプログラムである。
なお、第１実施形態では、以下において、本人認証プログラム５１ａのみを用いて、本人確認時及び本人認証時の本人認証サーバ４における処理を行うものを説明する。しかし、本人確認時と、本人認証時の本人認証サーバ４における処理を、異なるプログラムを用いて行う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を介して携帯端末１等との間の通信を行うためのインタフェースである。
【００３７】
銀行サーバ７は、金融取引業務、特に銀行業務を行うサーバであり、例えば、携帯端末１との間で通信を行うことでインターネットバンキングを行うためのフロントサーバである。銀行サーバ７は、例えば、図示しない元帳を有する勘定系システムに対して通信可能に接続され、口座情報を取得したり、取引を実行して口座情報（残高等）を更新したりする。
図３（Ｂ）に示すように、銀行サーバ７は、制御部７０と、記憶部７５と、通信インタフェース部７９とを備える。
【００３８】
制御部７０は、銀行サーバ７の全体を制御するＣＰＵである。制御部７０は、記憶部７５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７０は、処理実行部７１（取引決定手段）を備える。
処理実行部７１は、携帯端末１から認証結果と、ログインＩＤとを含む取引要求を受信することで、取引要求に対して許可するか否かを決定し、決定した処理を実行して、取引を成立させる。
【００３９】
記憶部７５は、制御部７０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７５は、プログラム記憶部７６と、口座情報記憶部７７とを備える。
プログラム記憶部７６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７６は、取引プログラム７６ａを記憶する。
取引プログラム７６ａは、銀行サーバ７の制御部７０が実行する各種機能を行うためのプログラムである。
口座情報記憶部７７は、ログインＩＤに対応付けてパスワードと、口座番号、口座名等の口座情報とを記憶する記憶領域である。
通信インタフェース部７９は、通信ネットワークＮを介して携帯端末１等との間の通信を行うためのインタフェースである。
【００４０】
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、本人認証サーバ４及び銀行サーバ７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。
【００４１】
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。

【００４２】
次に、金融取引システム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での取引開始時処理を示すフローチャートである。
図５は、第１実施形態に係る携帯端末１での表示例を示す図である。
まず、携帯端末１を用いてインターネットバンキング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に表示されている銀行取引アプリ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、銀行取引アプリ３１ａを実行する。
【００４３】
銀行取引アプリ３１ａが実行されると、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、タッチパネルディスプレイ３５に、銀行取引アプリ３１ａのログイン画面６０を表示する。図５（ａ）は、ログイン画面６０の例を示す。ユーザは、ログイン画面６０から銀行取引アプリ３１ａで用いるログインＩＤ及びパスワードを入力し、「次へ」のボタンをタップする。
そうすることで、携帯端末１の制御部１０（入力受付部１１）は、ログイン情報の入力を受け付け、銀行サーバ７に対して、ログインＩＤ及びパスワードを送信するログイン処理を行う。
銀行サーバ７の制御部７０では、受信したログインＩＤ及びパスワードによるログイン認証を行い、ログイン認証結果を携帯端末１に送信する。
【００４４】
携帯端末１の制御部１０は、ログイン認証結果を受信し、ログイン認証ができたものである場合に、Ｓ２において、制御部１０は、図５（ｂ）に例示するメニュー画面６１を出力する。メニュー画面６１は、銀行取引アプリ３１ａにおいて実行可能な各種の取引が一覧になったものである。図５（ｂ）は、ログインＩＤに対応する口座情報が１つの口座に関するものである場合の例である。１つのログインＩＤに対応する口座情報が複数の口座についてある場合には、メニュー画面６１に、例えば、複数の口座番号を出力して、取引対象の口座番号をユーザに選択させる。
【００４５】
Ｓ３において、制御部１０は、例えば、銀行取引アプリ３１ａを終了させる操作を受け付けることで、本処理を終了するか否かを判断する。終了する場合（Ｓ３：ＹＥＳ）には、制御部１０は、銀行取引アプリ３１ａの実行を終了することで、本処理を終了する。他方、終了しない場合（Ｓ３：ＮＯ）には、制御部１０は、処理をＳ４に移す。
【００４６】
Ｓ４において、制御部１０（入力受付部１１）は、メニュー画面６１から、例えば、「振込」の取引項目が選択されることで、資金移動取引が選択されたか否かを判断する。資金移動取引が選択された場合（Ｓ４：ＹＥＳ）には、制御部１０は、処理をＳ５に移す。他方、資金移動取引が選択されていない場合（Ｓ４：ＮＯ）には、制御部１０は、処理をＳ６に移す。ここで、資金移動取引が選択されていない場合とは、例えば、入出金明細照会や、残高照会等の口座照会に関する取引項目が選択された場合をいう。また、資金移動取引が選択されていない場合として、住所やパスワードの変更等の各種変更処理を含んでもよい。
【００４７】
Ｓ５において、制御部１０は、図５（ｃ）に例示する認証方法選択画面６２を出力する。認証方法選択画面６２は、認められている認証方法が選択可能に出力されたものである。図５（ｃ）に示す認証方法選択画面６２には、生体認証と、ＯＴＰ（ワンタイムパスワード）による認証とが示されている。その後、制御部１０は、処理をＳ７に移す。
他方、Ｓ６において、制御部１０は、選択された取引項目に対する処理を行う。具体的に、制御部１０は、選択された項目が口座照会に関する取引項目であれば、ログインＩＤと、取引項目の内容を銀行サーバ７に送信することで、銀行サーバ７から取引項目の内容

に即した情報（残高等）を受信して出力する。その後、制御部１０は、処理をＳ２に移す。
【００４８】
Ｓ７において、制御部１０（入力受付部１１）は、生体認証が選択されたか否かを判断する。生体認証が選択された場合（Ｓ７：ＹＥＳ）には、制御部１０は、処理をＳ８に移す。他方、生体認証が選択されなかった場合（Ｓ７：ＮＯ）には、制御部１０は、処理をＳ９に移す。
Ｓ８において、制御部１０（認証確認処理部１２）は、生体認証による確認処理（後述する図６参照）を行う。この実施形態での生体認証は、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得られるユーザの顔画像を用いる。その後、制御部１０は、処理をＳ１０に移す。
【００４９】
他方、Ｓ９において、制御部１０は、他の選択された方法による確認処理を行う。他の選択された方法による確認処理については、説明を省略する。
Ｓ１０において、制御部１０（取引要求部２０）は、確認処理結果（認証結果）と、ログインＩＤと、取引項目の内容とを含む取引要求を、銀行サーバ７に対して送信する。
【００５０】
そして、銀行サーバ７の制御部７０（処理実行部７１）は、受信した取引要求に認証ができたとの確認処理結果を含む場合には、口座情報記憶部７７を参照して口座情報を特定し、取引項目の内容に沿ったデータを携帯端末１に送信する。携帯端末１では、例えば、図５（ｅ）に示す振込詳細設定画面６４を出力する。そして、制御部１０と銀行サーバ７との間の通信により、銀行サーバ７の制御部７０（処理実行部７１）は、取引項目の内容に関する処理を実行する。その後、制御部１０は、取引結果画面（図示せず）を出力後に、処理をＳ２に移す。
他方、受信した取引要求に認証エラーの確認処理結果を含む場合には、制御部１０は、例えば、図５（ｆ）に示す確認結果画面６５を出力する。その後、制御部１０は、処理をＳ２に移す。
【００５１】
次に、生体認証による確認処理について説明する。
図６は、第１実施形態に係る携帯端末１での生体認証による確認処理を示すフローチャートである。
Ｓ２１において、制御部１０（関連付け確認部１３）は、照合画像記憶部３２に記憶されている顔画像（照合画像）に、ログイン処理で用いたログインＩＤが関連付けられているか否かを判断する。ログインＩＤが関連付けられている場合（Ｓ２１：ＹＥＳ）には、制御部１０は、処理をＳ２２に移す。他方、ログインＩＤが関連付けられていない場合（Ｓ２１：ＮＯ）には、制御部１０は、処理をＳ２３に移す。
【００５２】
Ｓ２２において、制御部１０（本人確認処理部１４）は、本人認証処理（後述する図９参照）を行う。その後、制御部１０は、処理を図４のＳ１０に移す。
他方、Ｓ２３において、制御部１０（認証ＡＰＩ処理部１５）は、本人確認処理（後述する図７参照）を行う。その後、制御部１０は、処理を図４のＳ１０に移す。
【００５３】
次に、本人確認処理について説明する。ここでの本人確認処理とは、本人確認書類と、ユーザの顔画像とを撮影して、本人確認書類に有する顔写真画像とユーザの顔画像とを照合する処理と、照合できた場合に、ユーザの顔画像にインターネットバンキングを利用するためのログインＩＤを関連付ける処理とを合わせたものをいう。
図７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８は、第１実施形態に係る携帯端末１及び本人認証サーバ４での照合画像処理を示すフローチャートである。
【００５４】
図７のＳ３１において、制御部１０（本人確認処理部１４）は、照合画像処理を行う。

ここで、照合画像処理について、図８に基づき説明する。
図８のＳ４１において、制御部１０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。
【００５５】
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。
【００５６】
Ｓ４２において、制御部１０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。
Ｓ４３において、制御部１０は、抽出した顔写真画像を、記憶部３０に一時記憶させる。
【００５７】
Ｓ４４において、制御部１０は、今度はインカメラ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。
Ｓ４５において、制御部１０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暗号化して、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、携帯端末１が取得（Ｓ４１）及び記憶（Ｓ４３）したものである。また、顔写真画像及び照合画像は、ユーザの生体情報であるため、暗号化して送信するのが望ましい。そして、暗号化の方式は、特に限定されず、例えば、共通鍵暗号方式を用いてもよいし、他の既知の暗号方式を用いてもよい。
【００５８】
Ｓ４６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。
Ｓ４７において、制御部４０（本人確認処理部４１）は、受信した照合画像と顔写真画像とを復号し、各々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。
Ｓ４８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。
Ｓ４９において、携帯端末１の制御部１０は、照合結果を受信する。その後、制御部１０は、処理を図７のＳ３２に移す。
【００５９】
図７のＳ３２において、制御部１０（本人確認処理部１４）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（Ｓ３２：ＹＥＳ）には、制御部１０は、処理をＳ３３に移す。他方、認証ができたと判定されなかった場合（Ｓ３２：ＮＯ）には、制御部１０は、処理をＳ３９に移す。
【００６０】
Ｓ３３において、制御部１０（本人確認処理部１４）は、本人確認処理で取得した顔画像を、照合画像として、ログイン処理で用いたログインＩＤに関連付ける関連付け処理を行う。その際、制御部１０は、例えば、図５（ｇ）に示す認証情報登録画面６６を出力し、ユーザに処理内容を確認させてもよい。

Ｓ３４において、制御部１０（本人確認処理部１４）は、関連付けがされた照合画像を、照合画像記憶部３２に記憶させる。その結果、照合画像記憶部３２には、照合画像とログインＩＤとが関連付けられて記憶される。

【００６１】

Ｓ３５において、制御部１０（本人確認処理部１４）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。その後、制御部１０は、処理を図４のＳ１０に移す。この処理により、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。

他方、Ｓ３９において、制御部１０は、認証エラーと判定し、処理を図４のＳ１０に移す。

【００６２】

次に、本人認証処理について説明する。ここで、本人認証処理とは、照合画像にログインＩＤとの関連付けがされている場合における資金移動取引処理を行う際の処理をいう。

図９及び図１０は、第１実施形態に係る携帯端末１及び本人認証サーバ４での本人認証処理を示すフローチャートである。

図９のＳ６１において、制御部１０（認証要求部１６）は、認証要求を、本人認証サーバ４に送信する。

【００６３】

Ｓ６２において、本人認証サーバ４の制御部４０は、認証要求を受信する。

Ｓ６３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。

Ｓ６４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。

Ｓ６５において、制御部１０（顔画像取得部１７）は、顔画像を取得する。制御部１０は、図５（ｄ）に例示する撮影画面６３を出力して、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。

【００６４】

Ｓ６６において、制御部１０（顔画像照合部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、当該ログインＩＤに関連付けら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。

Ｓ６７において、制御部１０（顔画像照合部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（Ｓ６７：ＹＥＳ）には、制御部１０は、処理をＳ６８に移す。他方、照合ができたと判定されなかった場合（Ｓ６７：ＮＯ）には、制御部１０は、処理をＳ６９に移す。

【００６５】

Ｓ６８において、制御部１０は、Ｓ６４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１０のＳ７１に移す。

他方、Ｓ６９において、制御部１０は、認証エラーと判定し、処理を図４のＳ１０に移す。

【００６６】

図１０のＳ７１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。

Ｓ７２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。

Ｓ７３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。

【００６７】

Ｓ７４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（Ｓ７４：ＹＥＳ）には、制御部４０は、処理をＳ７５に移す。他方、署名検証ができなかった場合（Ｓ７４：ＮＯ）には、制御部４０は、本処理を終了する。

Ｓ７５において、制御部４０（認証結果送信部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。

【００６８】

Ｓ７６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（Ｓ７６：ＹＥＳ）には、制御部１０は、処理をＳ７７に移す。他方、署名検証結果を受信していない場合（Ｓ７６：ＮＯ）には、制御部１０は、処理をＳ７９に移す。なお、署名したデータを送信（Ｓ７１）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。

Ｓ７７において、制御部１０は、認証できたと判定し、処理を図４のＳ１０に移す。

他方、Ｓ７９において、制御部１０は、認証エラーと判定し、処理を図４のＳ１０に移す。

【００６９】

このように、第１実施形態によれば、金融取引システム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（照合画像）を、インターネットバンキングの利用時に使用するログインＩＤに関連付けて携帯端末１に記憶する。そして、インターネットバンキングの資金移動取引の都度行う本人認証での照合に、ログインＩＤに関連付けて携帯端末１に記憶してある顔画像を用いる。このように、顔画像による本人認証処理を、携帯端末１のみによって行うため、本人認証で用いる顔画像である生体情報を、通信ネットワークＮに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。

また、本人認証のために、照合元になる顔画像を再度取得するものではなく、本人確認で取得した顔画像を流用する。そのため、照合用の画像は、一度取得すれば足り、ユーザにとって、より利便性が良いものにできる。

【００７０】

（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に記憶させたものである。よって、顔画像を記憶させる行為を、生体認証による確認処理を初めて行うときにのみ１回だけ行えばよい。

【００７１】

（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。

【００７２】

（第２実施形態）

第２実施形態では、複数の銀行の銀行サーバと、携帯端末との間を仲介する取引仲介サーバを有するものについて説明する。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。

【００７３】

図１１は、第２実施形態に係る金融取引システムの全体構成を示す図である。

図１２は、第２実施形態に係る携帯端末の機能ブロック図である。

図１３は、第２実施形態に係る取引仲介サーバの機能ブロック図及び利用者情報記憶部の例を示す図である。

【００７４】

図１１に示す金融取引システム２００は、複数の銀行サーバ７と、携帯端末２０１との間で取引を仲介する取引仲介サーバ２０８を用いて、インターネットバンキングによる金融取引を、携帯端末２０１を用いて行うシステムである。そして、金融取引システム２００は、特に、振込等の資金移動取引の場合に、高セキュリティの認証である顔画像による生体認証を行うことで、携帯端末２０１によって安全に取引を行うためのシステムである。

金融取引システム２００は、携帯端末２０１と、本人認証サーバ４と、銀行サーバ７と、取引仲介サーバ２０８とを備える。取引仲介サーバ２０８は、通信ネットワークＮに接続可能である。

【００７５】

図１２に示すように、携帯端末１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、入力受付部２１１（入力受付手段）と、認証確認処理部１２と、取引要求部２２０（要求送信手段）とを備える。

【００７６】

入力受付部２１１は、ユーザによる取引を行うための各種の入力を受け付ける。

例えば、入力受付部２１１は、取引仲介サーバ２０８にログインするためのログイン情報の入力を受け付ける。ここで、ログイン情報とは、取引仲介サーバ２０８に予め登録された利用者ＩＤ（利用者識別情報）及びパスワードをいう。この利用者ＩＤ及びパスワードは、銀行サーバ７にログインするためのログインＩＤ及びパスワードとは異なるものである。

また、入力受付部２１１は、取引項目の指定や、認証方法の選択等を受け付けてもよい。

取引要求部２２０は、取引仲介サーバ２０８に対して、認証結果と、利用者ＩＤと、銀行を識別する識別情報である銀行ＩＤ（銀行識別情報）とを含む取引要求を送信する。

【００７７】

記憶部２３０は、プログラム記憶部２３１と、照合画像記憶部２３２と、鍵記憶部３３とを備える。

プログラム記憶部２３１は、取引仲介アプリ２３１ｄと、本人確認ＡＰＩ３１ｂと、認証ＡＰＩ３１ｃとを記憶している。

取引仲介アプリ２３１ｄは、取引仲介サーバ２０８を利用した銀行サーバ７との間でのインターネットバンキング取引を行うためのプログラムである。

照合画像記憶部２３２は、本人認証に用いる顔画像（照合画像）を、利用者ＩＤに関連付けて記憶する記憶領域である。

【００７８】

取引仲介サーバ２０８は、携帯端末１と銀行サーバ７とを仲介するサーバである。取引仲介サーバ２０８を用いることで、携帯端末１には、自身の保有する複数の銀行の口座情報から、資金残高を把握したりすることができる。

図１３（Ａ）に示すように、取引仲介サーバ２０８は、制御部２８０と、記憶部２８５と、通信インタフェース部２８９とを備える。

【００７９】

制御部２８０は、取引仲介サーバ２０８の全体を制御するＣＰＵである。制御部２８０は、記憶部２８５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２８０は、実行要求部２８１（実行要求手段）を備える。

実行要求部２８１は、携帯端末１から認証結果と、利用者ＩＤと、銀行ＩＤとを含む取引要求を受信することで、ログインＩＤを取得し、銀行サーバ７に対して、認証結果と、ログインＩＤとを含む取引実行要求を送信する。

【００８０】

記憶部２８５は、制御部２８０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２８５は、プログラム記憶部２８６と、利用者情報記憶部２８７とを備える。

プログラム記憶部２８６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２８６は、取引仲介プログラム２８６ａを記憶する。

取引仲介プログラム２８６ａは、取引仲介サーバ２０８の制御部２８０が実行する各種機能を行うためのプログラムである。

【００８１】

利用者情報記憶部２８７は、図１３（Ｂ）に例示するように、利用者ＩＤに対応付けてパスワードと、利用者ＩＤにより特定される利用者の銀行に対応した銀行サーバ７にログインするためのログイン情報（銀行ＩＤ、ログインＩＤ、パスワード）とを記憶する記憶領域である。

通信インタフェース部２８９は、通信ネットワークＮを介して携帯端末１等との間の通信を行うためのインタフェースである。

なお、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、取引仲介サーバ２０８は、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。

【００８２】

次に、金融取引システム２００の処理について、第１実施形態との変更箇所を中心に説明する。

図１４は、第２実施形態に係る金融取引システム２００での取引処理を示すフローチャートである。

この図１４で説明する取引処理の前提として、携帯端末２０１は、本人認証サーバ４との間で既に本人確認処理を行っており、携帯端末２０１の照合画像記憶部２３２には、顔画像（照合画像）と、取引仲介サーバ２０８にログインするための利用者ＩＤとが関連付けられているものとする。そして、取引処理は、生体認証（顔認証）による本人認証結果に基づいて、利用可能な取引を限定するものである。

【００８３】

まず、ユーザは、取引仲介アプリ２３１ｄを起動させるためのアイコン（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２０１の制御部２１０は、取引仲介アプリ２３１ｄを実行する。

取引仲介アプリ２３１ｄが実行されると、携帯端末２０１の制御部２１０は、タッチパネルディスプレイ３５に、取引仲介アプリ２３１ｄのログイン画面（図示せず）を表示する。ユーザは、取引仲介アプリ２３１ｄで用いる利用者ＩＤ及びパスワードを入力する。

そうすることで、図１４のＳ２０１において、携帯端末２０１の制御部２１０（入力受付部２１１）は、ログイン情報の入力を受け付け、取引仲介サーバ２０８に対して、利用者ＩＤ及びパスワード（ＰＷ）を送信するログイン処理を行う。

【００８４】

Ｓ２０２において、取引仲介サーバ２０８の制御部２８０では、受信した利用者ＩＤ及びパスワードによるログイン認証を行い、認証できた場合には、利用者情報記憶部２８７を参照し、利用者ＩＤに対応するログインＩＤ及びパスワードを、各銀行サーバ７に送信する。ここで、利用者ＩＤに対して１つの銀行ＩＤのみが対応付けられている場合には、制御部２１０は、１つの銀行ＩＤに対応する銀行サーバ７に対して、ログインＩＤ及びパスワードを送信する。他方、利用者ＩＤに対して複数の銀行ＩＤが対応付けられている場合には、各銀行ＩＤに対応する銀行サーバ７に対して、銀行ＩＤに対応付けられたログインＩＤ及びパスワードを送信する。

【００８５】
Ｓ２０３において、銀行サーバ７の制御部７０は、受信したログインＩＤ及びパスワードによるログイン認証を行う。そして、認証できた場合には、制御部７０は、ログインＩＤに対応付けられた口座情報を、取引仲介サーバ２０８に送信する。
Ｓ２０４において、取引仲介サーバ２０８の制御部２８０は、口座情報を受信した場合に、口座情報に対応した銀行ＩＤを対応付けて、携帯端末２０１に送信する。
【００８６】
Ｓ２０６及びＳ２０７において、携帯端末２０１の制御部２１０（認証ＡＰＩ処理部１５）は、本人認証サーバ４との間で本人認証処理を行う。この携帯端末２０１と、本人認証サーバ４との本人認証処理は、第１実施形態（図９及び図１０）と同様である。なお、図９のＳ６６に対応する処理において、制御部２１０（顔画像照合部１８）は、取得したユーザの顔画像と、照合画像記憶部２３２に記憶された当該利用者ＩＤに関連付けられた照合画像とを照合する。
【００８７】
Ｓ２０８において、携帯端末２０１の制御部２１０は、受信した情報に基づいて、メニュー画面を生成して出力する。
ここで、本人認証処理により本人の確認ができた場合には、例えば、口座照会処理のような銀行の元帳に対する更新を伴わない参照系の処理と、振込処理のような銀行の元帳に対する更新を行う更新系の処理とを許可する。よって、制御部２１０は、参照系の処理と、更新系の処理とが可能な項目を含むメニュー画面を生成して出力する。
他方、本人認証処理により本人の確認ができなかった場合には、ログイン認証はできているため、例えば、口座照会処理のような銀行の元帳に対する更新を伴わない参照系の処理のみを許可する。
【００８８】
Ｓ２０９において、携帯端末２０１の制御部２１０（取引要求部２２０）は、利用者ＩＤと、銀行ＩＤと、取引項目の内容とを含む取引要求を、取引仲介サーバ２０８に送信する。
Ｓ２１０において、取引仲介サーバ２０８の制御部２８０は、携帯端末１から利用者ＩＤ及び銀行ＩＤを含む取引要求を受信すると、利用者情報記憶部２８７を参照して、対応するログインＩＤを取得する。そして、制御部２８０（実行要求部２８１）は、銀行サーバ７に対して、ログインＩＤと、取引項目の内容とを含む取引実行要求を送信する。
Ｓ２１１において、銀行サーバ７の制御部７０（処理実行部７１）は、取引仲介サーバ２０８からログインＩＤと、取引項目の内容とを含む取引実行要求を受信することで、取引実行処理を行う。
【００８９】
なお、この取引処理は、本人確認が行われ、照合画像に利用者ＩＤが既に関連付けられている場合を例に説明した。照合画像に利用者ＩＤが関連付けられていない場合には、第１実施形態（図７及び図８参照）の本人確認処理と同様の処理を行えばよい。
【００９０】
このように、第２実施形態によれば、金融取引システム２００は、以下のような効果がある。
インターネットバンキング取引において、第１実施形態における携帯端末１が、銀行サーバ７を用いた取引の際に行う顔画像の生体情報を利用した本人認証を、取引仲介サーバ２０８が、携帯端末２０１と、銀行サーバ７との間を仲介して取引をする場合においても、同様の仕組みが適用できる。よって、様々なビジネスサービス取引において、顔画像の生体情報を利用した本人認証を行うことができる。
【００９１】
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。

【００９２】

（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。

【００９３】

（２）各実施形態では、資金移動取引について、生体認証による本人認証を行うものを例に説明したが、これに限定されない。他の照会取引等においても、生体認証による本人認証を行ってもよい。

また、第１実施形態では、認証方法を選択可能にし、複数の認証方法から生体認証による認証方法が選択できるものを例に説明したが、これに限定されない。全てを生体認証による認証方法にしてもよく、そのようにすれば、認証方法選択画面に関連する処理は不要になる。

【００９４】

（３）各実施形態では、本人確認書類による処理を、携帯端末１のみで行う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、銀行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、銀行サーバでは、氏名等の確認も行うことができる。また、受信した文字情報を携帯端末で修正可能にしてもよい。そのようにすることで、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。また、変更箇所の前後の文字情報を含んで銀行サーバに送信すれば、銀行サーバにおいて、不正な修正が行われたか否かを確認できる。

【００９５】

（４）第１実施形態では、インターネットバンキング取引を行うために、携帯端末に銀行取引アプリを記憶させるものを例に説明したが、これに限定されない。例えば、銀行サーバがＷｅｂサーバの機能を有し、携帯端末が有するＷｅｂブラウザを用いるものであってもよい。

（５）第１実施形態では、ユーザが携帯端末のみを用いて行うものを例に説明したが、これに限定されない。例えば、カメラを有さないパーソナルコンピュータ（ＰＣ）によるインターネットバンキング取引をする場合であっても適用できる。その場合、携帯端末には、認証ＡＰＩを有するようにし、ＰＣと、携帯端末との間を連携させて、携帯端末で本人認証を行い、ＰＣでは、銀行取引アプリによる取引アプリ処理を行うようにすればよい。

（６）第１実施形態では、銀行サーバと、本人認証サーバとを別のサーバとして説明したが、これに限定されない。銀行サーバに、本人確認や本人認証の機能を有するようにして、１つのサーバによって実現してもよい。

（７）第１実施形態では、ログイン認証ができた場合に、メニュー画面を出力し、取引項目が指定された後に生体認証を行うものを例に説明した。また、第２実施形態では、ログイン認証ができた場合に、生体認証を行った上で、メニュー画面を出力するものを例に説明した。しかし、これらに限定されるものではない。生体認証を行うタイミングは、取引項目が指定された後であっても、取引項目を指定する前であっても、どちらでもよい。そして、生体認証ができた場合と、できなかった場合とで、許可する取引が異なり、更新系の取引においては、生体認証を必須とすればよい。

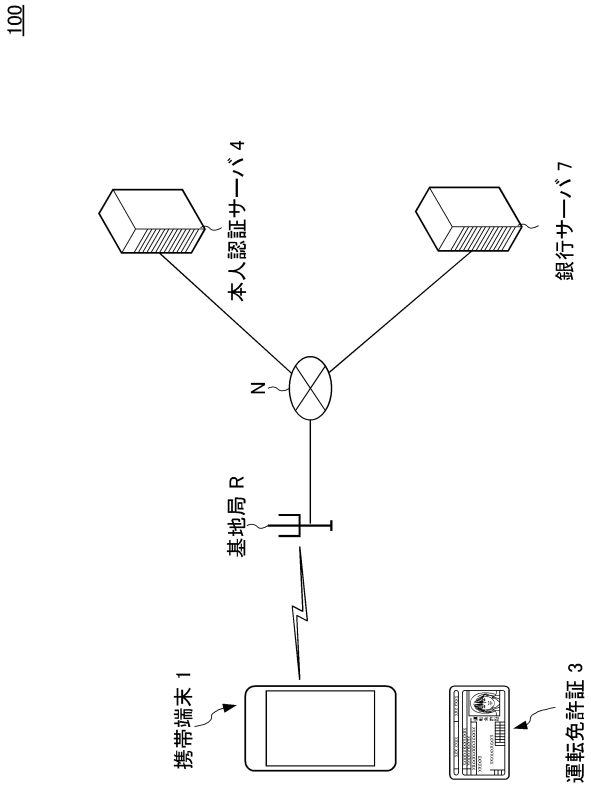
【符号の説明】

【００９６】

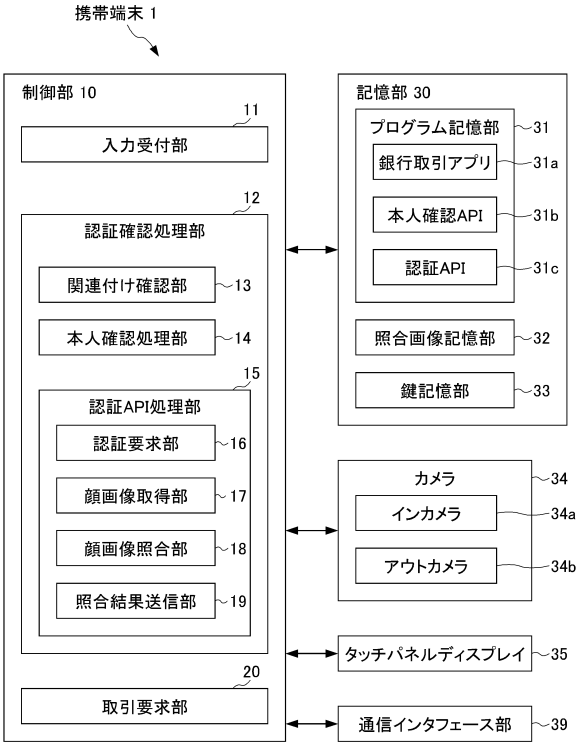
１，２０１　携帯端末
３　運転免許証
４　本人認証サーバ
７　銀行サーバ
１０，４０，７０，２１０，２８０　制御部
１１，２１１　入力受付部
１３　関連付け確認部
１４　本人確認処理部
１５　認証ＡＰＩ処理部
１６　認証要求部
１７　顔画像取得部
１８　顔画像照合部
１９　照合結果送信部
２０，２２０　取引要求部
３０，５０，７５，２３０，２８５　記憶部
３１ａ　銀行取引アプリ
３１ｂ　本人認証ＡＰＩ
３１ｃ　認証ＡＰＩ
３２，２３２　照合画像記憶部
３３，５３　鍵記憶部
３４　カメラ
３５　タッチパネルディスプレイ
４４　認証結果送信部
７１　処理実行部
７７　口座情報記憶部
１００，２００　金融取引システム
２０８　取引仲介サーバ
２３１ｄ　取引仲介アプリ
２８１　実行要求部
２８７　利用者情報記憶部

【図面】

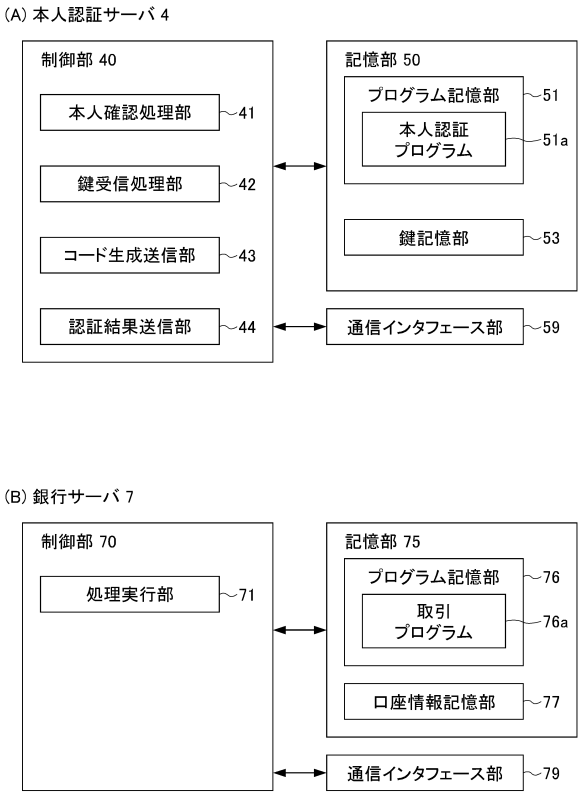
【図１】


100
本人認証サーバ 4
銀行サーバ 7
N
基地局 R
携帯端末 1
運転免許証 3

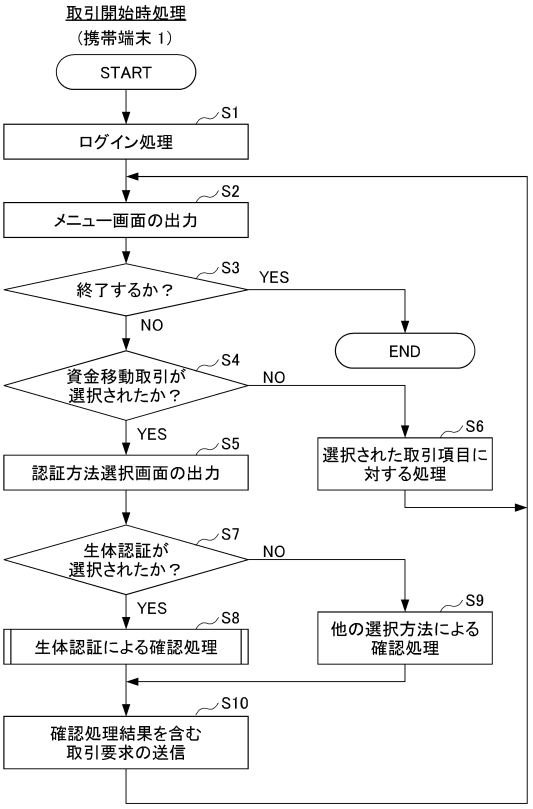
【図２】


携帯端末 1
制御部 10
11
入力受付部
12
認証確認処理部
関連付け確認部 13
本人確認処理部 14
15
認証API処理部
認証要求部 16
顔画像取得部 17
顔画像照合部 18
照合結果送信部 19
20
取引要求部
記憶部 30
プログラム記憶部 31
銀行取引アプリ 31a
本人確認API 31b
認証API 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

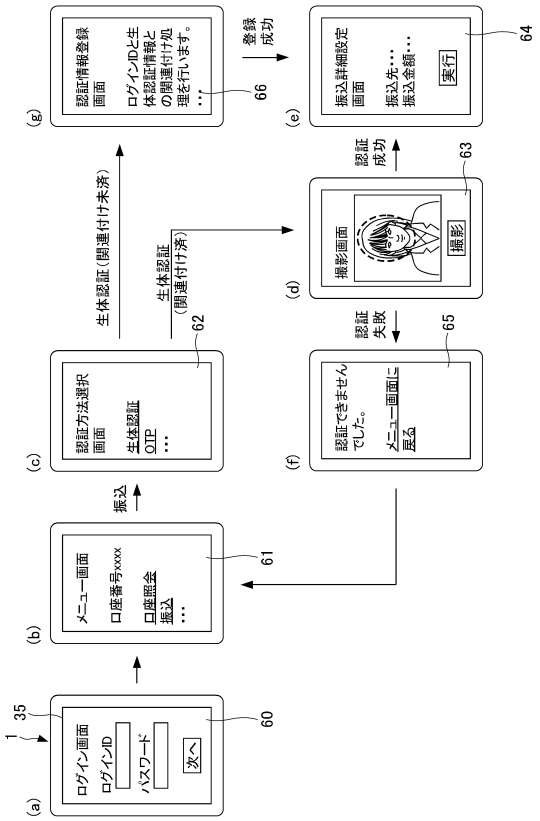
【図３】


(A) 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
認証結果送信部 44
記憶部 50
プログラム記憶部 51
本人認証プログラム 51a
鍵記憶部 53
通信インタフェース部 59
(B) 銀行サーバ 7
制御部 70
処理実行部 71
記憶部 75
プログラム記憶部 76
取引プログラム 76a
口座情報記憶部 77
通信インタフェース部 79

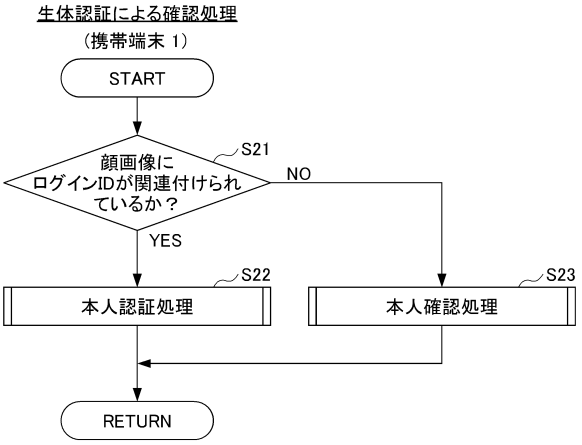
【図４】


取引開始時処理
(携帯端末 1)
START
S1
ログイン処理
S2
メニュー画面の出力
S3
終了するか？
YES
END
NO
S4
資金移動取引が選択されたか？
NO
S6
選択された取引項目に対する処理
YES
S5
認証方法選択画面の出力
S7
生体認証が選択されたか？
NO
S9
他の選択方法による確認処理
YES
S8
生体認証による確認処理
S10
確認処理結果を含む取引要求の送信

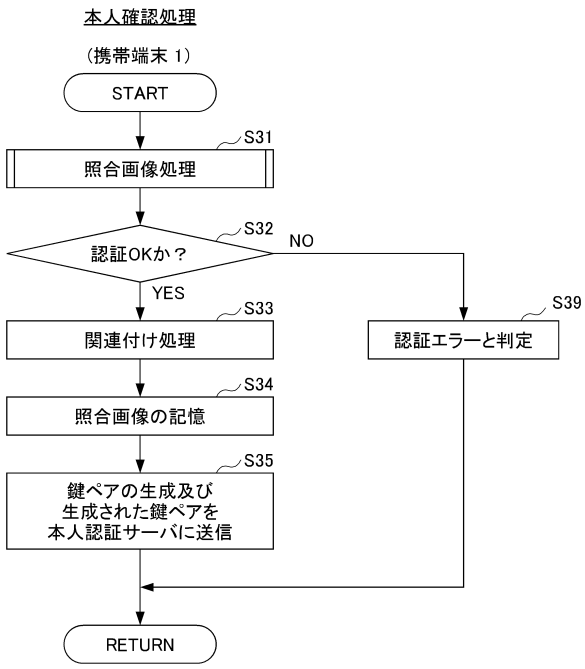
【図５】


(a)
ログイン画面
ログインID
パスワード
次へ
35
60
(b)
メニュー画面
口座番号xxxx
口座照会
振込
…
61
振込
(c)
認証方法選択画面
生体認証
OTP
…
62
生体認証（関連付け済）
生体認証（関連付け未済）
(d)
撮影画面
撮影
63
認証成功
(e)
振込詳細設定画面
振込先…
振込金額…
実行
64
登録成功
(f)
認証できませんでした。
メニュー画面に戻る
65
認証失敗
(g)
認証情報登録画面
ログインIDと生体認証情報との関連付け処理を行います。
…
66

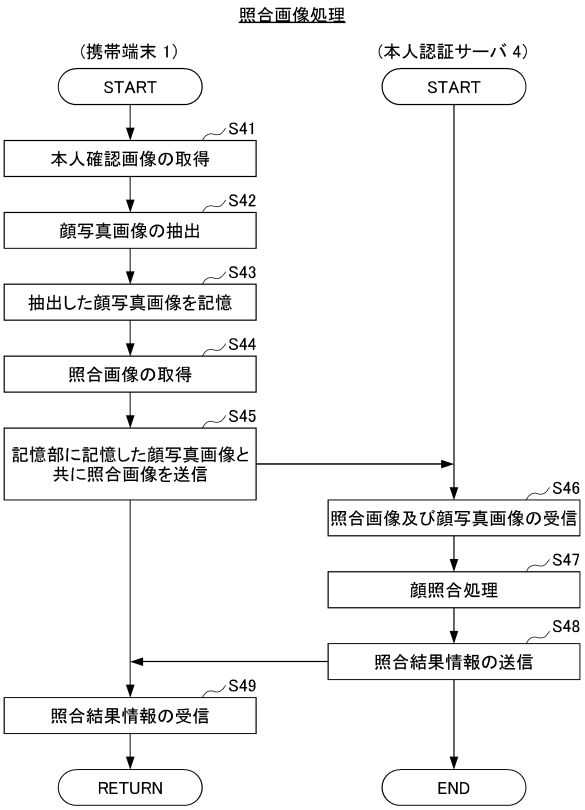
【図６】


生体認証による確認処理
（携帯端末 1）
START
顔画像にログインIDが関連付けられているか？
S21
NO
YES
S22
本人認証処理
S23
本人確認処理
RETURN

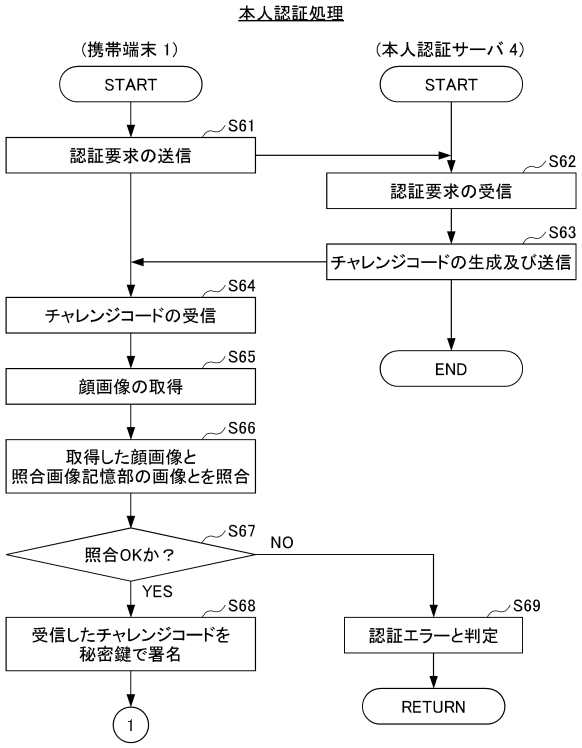
【図７】


本人確認処理
（携帯端末 1）
START
S31
照合画像処理
S32
認証OKか？
NO
YES
S33
関連付け処理
S34
照合画像の記憶
S35
鍵ペアの生成及び生成された鍵ペアを本人認証サーバに送信
S39
認証エラーと判定
RETURN

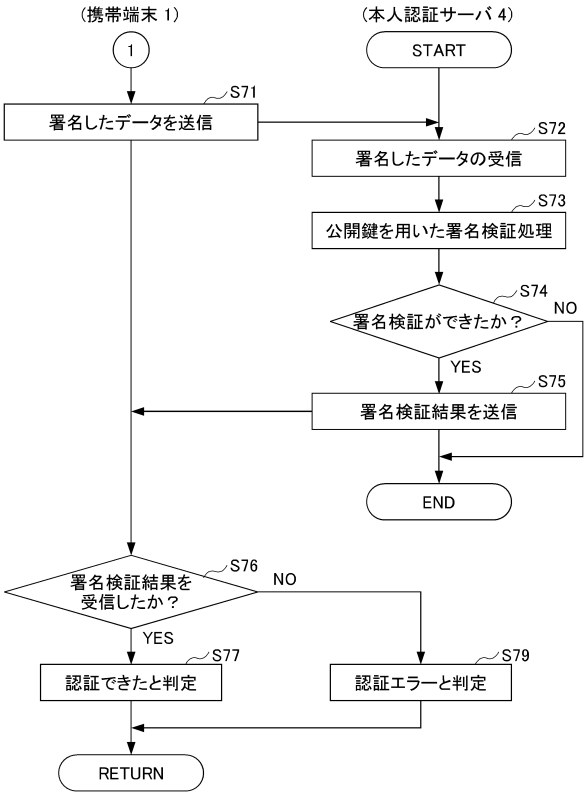
【図８】


照合画像処理
（携帯端末 1）
START
S41
本人確認画像の取得
S42
顔写真画像の抽出
S43
抽出した顔写真画像を記憶
S44
照合画像の取得
S45
記憶部に記憶した顔写真画像と共に照合画像を送信
S49
照合結果情報の受信
RETURN
（本人認証サーバ 4）
START
S46
照合画像及び顔写真画像の受信
S47
顔照合処理
S48
照合結果情報の送信
END

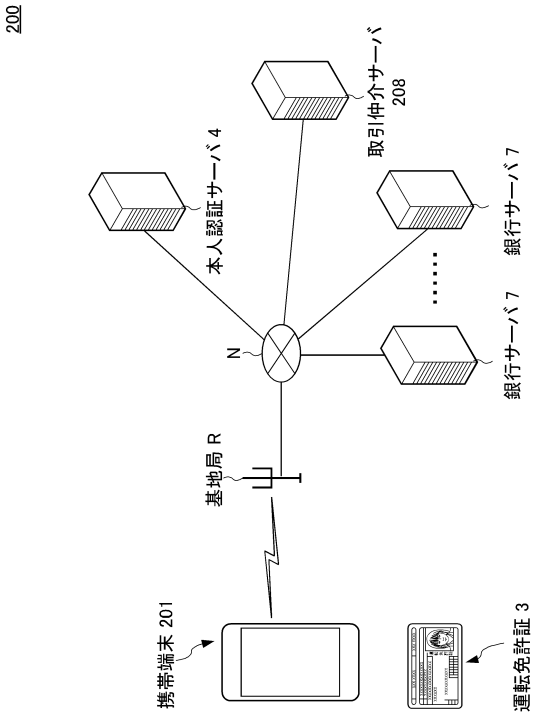
【図９】



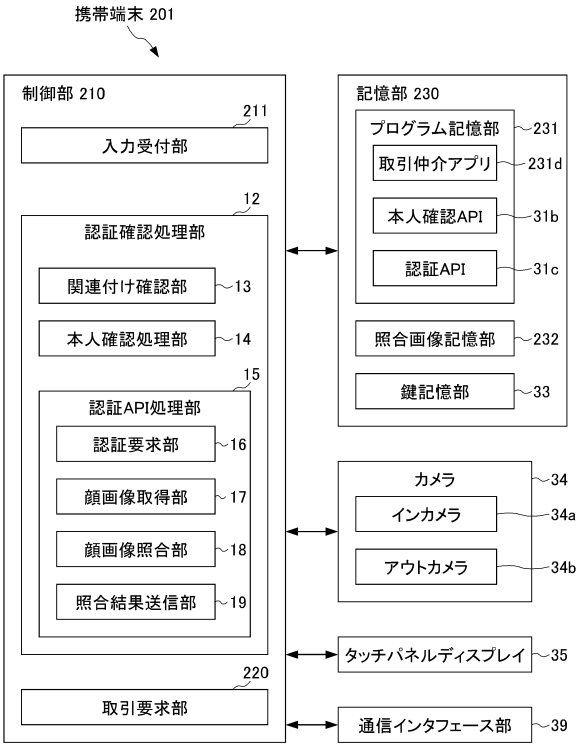
【図１０】



【図１１】

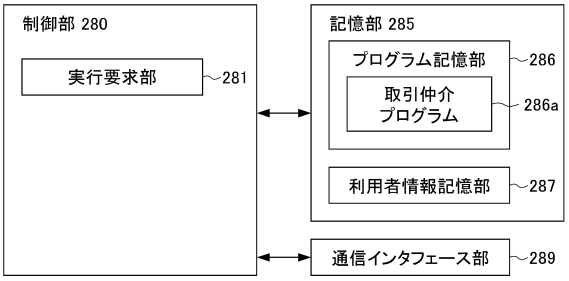


【図１２】



【図１３】

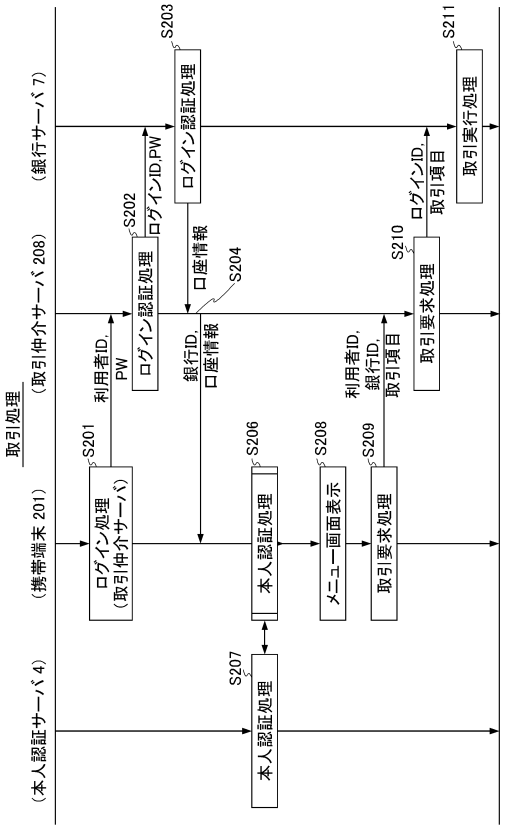
(A) 取引仲介サーバ 208



(B) 利用者情報記憶部 287

利用者ID	パスワード	銀行ID	ログインID	パスワード
ID1001	xxx	A001	U0123	aaa
		B123	B5013	bbb
		X209	X2019	ccc
・・・	・・・	・・・	・・・	・・・
ID1012	yyy	A001	U5823	ppp
・・・	・・・	・・・	・・・	・・・

【図１４】



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　庄司 琴美

(56)参考文献
特開２０１９－０４６０４４（ＪＰ，Ａ）
特開２０１６－１８１８０６（ＪＰ，Ａ）
特開２０１６－０１２３７０（ＪＰ，Ａ）
特開２００４－２４０６４５（ＪＰ，Ａ）
特開２００３－２０８４０７（ＪＰ，Ａ）
特開２０１４－０８５７７８（ＪＰ，Ａ）
特開２０１９－０２８８３７（ＪＰ，Ａ）
特開２００５－０６３０７７（ＪＰ，Ａ）
特開２００４－００５３４５（ＪＰ，Ａ）
特許第６４９９３６９（ＪＰ，Ｂ１）
特開２００７－２９３５９８（ＪＰ，Ａ）
特開２００２－３２９０７７（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００ － ９９／００
Ｇ０６Ｆ　２１／３０ － ２１／４６