(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2020-64541
(P2020-64541A)
(43)公開日　令和2年4月23日(2020.4.23)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/32	(2013.01)	G06F	21/32	5B043
G06F 21/34	(2013.01)	G06F	21/34	5L055
G06T 7/00	(2017.01)	G06T	7/00 510F	
G06Q 20/40	(2012.01)	G06Q	20/40	
G06Q 40/02	(2012.01)	G06Q	40/02	

審査請求 未請求　請求項の数 12　ＯＬ　（全 30 頁）

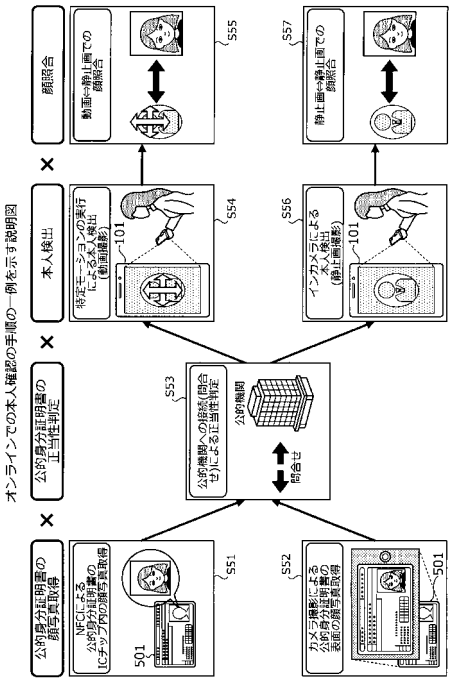
(21)出願番号　特願2018-197278 (P2018-197278)
(22)出願日　平成30年10月19日 (2018.10.19)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100104190
弁理士　酒井　昭徳
(72)発明者　加地　竹志
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　水尾　高暢
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5B043 AA01　AA02　AA09　BA04　CA09
DA05　EA02　GA01
5L055 AA73　BB14

(54)【発明の名称】本人確認プログラム、本人確認方法および情報処理装置

(57)【要約】
【課題】本人確認の手続きにかかる負荷を軽減すること。
【解決手段】情報処理装置１０１は、オンラインでの本人確認を行うにあたり、ＮＦＣ等を利用して、運転免許証５０１に内蔵されたＩＣチップから、顔画像を含む身分証情報を読み取る（ステップＳ５１）。情報処理装置１０１は、読み取った身分証情報に基づき、運転免許証５０１の正当性判定を行う（ステップＳ５３）。ここで、運転免許証５０１が正当であると判定された場合、情報処理装置１０１は、特定モーション（例えば、まばたき）の実行による本人検出を行う（ステップＳ５４）。ここで、本人が検出されると、情報処理装置１０１は、カメラ３０３により撮影された動画と、身分証情報に含まれる顔画像とに基づいて、本人認証（顔照合）を行う（ステップＳ５５）。
【選択図】図５



【特許請求の範囲】
【請求項１】
ユーザの画像を含む個人情報を公的身分証明書から読み取り、
読み取った前記個人情報に基づき、前記公的身分証明書が正当であるか否かを判定し、
前記公的身分証明書が正当であると判定した場合に、ユーザを含む撮影画像を撮影し、
読み取った前記個人情報に含まれる前記ユーザの画像と、撮影した前記ユーザを含む撮影画像とに基づいて、本人認証の結果を出力する、
処理をコンピュータに実行させることを特徴とする本人確認プログラム。
【請求項２】
前記読み取る処理は、
オンラインでの本人確認を要する取引の開始要求を受け付けたことに応じて、ユーザの画像を含む個人情報を公的身分証明書から読み取る、ことを特徴とする請求項１に記載の本人確認プログラム。
【請求項３】
前記読み取る処理は、
前記公的身分証明書に組み込まれたＩＣチップからユーザの画像を含む個人情報を読み取る、ことを特徴とする請求項１または２に記載の本人確認プログラム。
【請求項４】
前記出力する処理は、
本人認証に成功した場合には、本人認証の結果とともに、読み取った前記個人情報に含まれる前記ユーザの画像を出力する、ことを特徴とする請求項３に記載の本人確認プログラム。
【請求項５】
前記公的身分証明書を含む撮影画像を撮影する、処理を前記コンピュータに実行させ、
前記読み取る処理は、
撮影した前記公的身分証明書を含む撮影画像を文字認識処理して、前記公的身分証明書に記載された個人情報を読み取り、
撮影した前記公的身分証明書を含む撮影画像をトリミング処理して、前記公的身分証明書に付されたユーザの画像を取得する、
ことを特徴とする請求項１～４のいずれか一つに記載の本人確認プログラム。
【請求項６】
読み取った前記個人情報に住所情報が含まれる場合、ユーザの現在位置を示す位置情報を取得する、処理を前記コンピュータに実行させ、
前記出力する処理は、
取得した前記位置情報と前記個人情報に含まれる前記住所情報との比較結果にさらに基づいて、本人認証の結果を出力する、ことを特徴とする請求項１～５のいずれか一つに記載の本人確認プログラム。
【請求項７】
前記個人情報に含まれる前記ユーザの画像は、顔画像であり、
前記撮影する処理は、
ユーザを撮影する際に、被写体を表示する画面に、顔を位置付けるガイドを表示する、ことを特徴とする請求項１～６のいずれか一つに記載の本人確認プログラム。
【請求項８】
前記公的身分証明書が正当であると判定した場合に、ユーザを含む動画を撮影し、
読み取った前記個人情報に含まれる前記ユーザの画像と、撮影した前記動画とに基づいて、本人認証を行う、
処理を前記コンピュータに実行させることを特徴とする請求項１～７のいずれか一つに記載の本人確認プログラム。
【請求項９】
前記本人認証を行う処理は、

撮影した前記動画から複数のフレーム画像を選択し、
選択した前記複数のフレーム画像それぞれと、前記個人情報に含まれる前記ユーザの画像とを照合した結果に基づいて、本人認証を行う、
ことを特徴とする請求項８に記載の本人確認プログラム。
【請求項１０】
ユーザを含む動画を撮影中に、モーション指示を出力し、
撮影した前記動画に基づいて、出力した前記モーション指示に対応する動作が行われているか否かを判断する、処理を前記コンピュータに実行させ、
前記本人認証を行う処理は、
前記モーション指示に対応する動作が行われていると判断した場合に、前記個人情報に含まれる前記ユーザの画像と、撮影した前記動画とに基づいて、本人認証を行う、ことを特徴とする請求項８または９に記載の本人確認プログラム。
【請求項１１】
ユーザの画像を含む個人情報を公的身分証明書から読み取り、
読み取った前記個人情報に基づき、前記公的身分証明書が正当であるか否かを判定し、
前記公的身分証明書が正当であると判定した場合に、ユーザを含む撮影画像を撮影し、
読み取った前記個人情報に含まれる前記ユーザの画像と、撮影した前記ユーザを含む撮影画像とに基づいて、本人認証の結果を出力する、
処理をコンピュータが実行することを特徴とする本人確認方法。
【請求項１２】
被写体を撮影するカメラと、
ユーザの画像を含む個人情報を公的身分証明書から読み取る読取部と、
前記読取部が読み取った前記個人情報に基づき、前記公的身分証明書が正当であるか否かを判定する判定部と、
前記判定部が前記公的身分証明書が正当であると判定した場合に、前記カメラにより、ユーザを含む撮影画像を撮影する撮影制御部と、
前記個人情報に含まれる前記ユーザの画像と、前記撮影制御部が撮影した前記ユーザを含む撮影画像とに基づいて、本人認証の結果を出力する出力部と、
を有することを特徴とする情報処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、本人確認プログラム、本人確認方法および情報処理装置に関する。
【背景技術】
【０００２】
例えば、金融機関などでは、犯罪収益移転防止法により、口座開設に際し、犯罪によって得られた資金がマネーロンダリング（資金洗浄）されたり、テロ資金に流用されたりすることなどを防止するため、顧客の本人確認や疑わしい取引の届け出が義務付けられている。
【０００３】
先行技術としては、事業者に提示される身分証明書の画像データを用いて生活者の個人認証を行う情報処理システムがある。例えば、端末装置が、生活者の証明写真を読み取り、読み取った証明写真を情報処理装置に送信し、情報処理装置が、各生活者の証明写真を含む個人情報を記憶する記憶部が記憶している証明写真と、受信した証明写真とが一致するか否かを判定する情報処理システムがある。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１８－３２２３５号公報
【発明の概要】

【発明が解決しようとする課題】
【０００５】
しかしながら、従来技術では、本人確認の手続きに手間や時間がかかる。例えば、口座開設の際に、転送不要郵便（いわゆる、本人限定受取郵便）を利用して本人確認を行う場合、事務手続きが煩雑であり、郵送が必須であるため時間がかかる。
【０００６】
一つの側面では、本発明は、本人確認の手続きにかかる負荷を軽減することを目的とする。
【課題を解決するための手段】
【０００７】
１つの実施態様では、ユーザの画像を含む個人情報を公的身分証明書から読み取り、読み取った前記個人情報に基づき、前記公的身分証明書が正当であるか否かを判定し、前記公的身分証明書が正当であると判定した場合に、ユーザを含む撮影画像を撮影し、読み取った前記個人情報に含まれる前記ユーザの画像と、撮影した前記ユーザを含む撮影画像とに基づいて、本人認証の結果を出力する、本人確認プログラムが提供される。
【発明の効果】
【０００８】
本発明の一側面によれば、本人確認の手続きにかかる負荷を軽減することができる。
【図面の簡単な説明】
【０００９】
【図１】図１は、実施の形態にかかる本人確認方法の一実施例を示す説明図である。
【図２】図２は、本人確認システム２００のシステム構成例を示す説明図である。
【図３】図３は、情報処理装置１０１のハードウェア構成例を示すブロック図である。
【図４】図４は、情報処理装置１０１の機能的構成例を示すブロック図である。
【図５】図５は、オンラインでの本人確認の手順の一例を示す説明図である。
【図６Ａ】図６Ａは、オンラインでの本人確認時の画面の第１の遷移例を示す説明図（その１）である。
【図６Ｂ】図６Ｂは、オンラインでの本人確認時の画面の第１の遷移例を示す説明図（その２）である。
【図６Ｃ】図６Ｃは、オンラインでの本人確認時の画面の第１の遷移例を示す説明図（その３）である。
【図６Ｄ】図６Ｄは、オンラインでの本人確認時の画面の第１の遷移例を示す説明図（その４）である。
【図７Ａ】図７Ａは、オンラインでの本人確認時の画面の第２の遷移例を示す説明図（その１）である。
【図７Ｂ】図７Ｂは、オンラインでの本人確認時の画面の第２の遷移例を示す説明図（その２）である。
【図７Ｃ】図７Ｃは、オンラインでの本人確認時の画面の第２の遷移例を示す説明図（その３）である。
【図７Ｄ】図７Ｄは、オンラインでの本人確認時の画面の第２の遷移例を示す説明図（その４）である。
【図８】図８は、情報処理装置１０１の本人確認支援処理手順の一例を示すフローチャート（その１）である。
【図９】図９は、情報処理装置１０１の本人確認支援処理手順の一例を示すフローチャート（その２）である。
【図１０】図１０は、偽造・変造検証処理の具体的処理手順の一例を示すフローチャートである。
【図１１】図１１は、検証サーバ２０１の偽造・変造検証処理手順の一例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】
以下に図面を参照して、本発明にかかる本人確認プログラム、本人確認方法および情報処理装置の実施の形態を詳細に説明する。
【００１１】
（実施の形態）
図１は、実施の形態にかかる本人確認方法の一実施例を示す説明図である。図１において、情報処理装置１０１は、オンラインでの本人確認を支援するコンピュータである。ここで、本人確認とは、取引を行う際に、相手方が本人であることに間違いがないことを確認することである。
【００１２】
取引には、例えば、事業者（犯罪収益移転防止法における特定事業者など）との間で行われる取引のほか、公的機関に対して行われる申請、手続きなどが含まれてもよい。また、オンラインでの本人確認とは、インターネットなどの通信回線に接続されたコンピュータ（例えば、情報処理装置１０１）を利用して行われる本人確認である。
【００１３】
例えば、金融機関での口座開設の際には、本人確認を行う必要がある。金融機関の窓口に出向くことなく本人確認を行う手段としては、本人限定受取郵便を利用するものがある。ところが、本人限定受取郵便は、事務手続きが煩雑であり、郵送が必須となるため時間（例えば、１週間程度）や費用（例えば、数百円程度）がかかる。
【００１４】
そこで、本実施の形態では、オンラインでの本人確認を実現することで、本人確認の手続きにかかる負荷を軽減する本人確認方法について説明する。以下、情報処理装置１０１の処理例について説明する。
【００１５】
（１）情報処理装置１０１は、ユーザの画像を含む個人情報を公的身分証明書（図１の例では、公的身分証明書１１０）から読み取る。公的身分証明書からの個人情報の読み取りは、例えば、本人確認を行う際に行われる。本人確認は、例えば、オンラインでの本人確認を要する取引に応じて行われる。公的身分証明書とは、人の身分を証明するためのものであり、官公庁や学校、会社、団体などによって発行される文書である。
【００１６】
公的身分証明書としては、例えば、運転免許証、個人番号カード、パスポート、在留カードなどがある。また、ユーザの画像は、公的身分証明書により身分が証明されたユーザの画像であり、例えば、ユーザの顔画像である。また、公的身分証明書には、個人情報を記録するＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）が内蔵されているものがある。
【００１７】
例えば、運転免許証のＩＣチップには、氏名、生年月日、住所、顔写真、免許証交付年月日、有効期間、免許証番号などの個人情報が記録されている。また、運転免許証のＩＣチップには、運転免許証の発行者（例えば、警察）の公開鍵や電子署名が記録されている。ＩＣチップに記録された情報は、近距離無線通信により読み取ることができる。
【００１８】
近距離無線通信とは、通信距離が数センチから数メートル程度の無線通信である。近距離無線通信としては、例えば、ＮＦＣ（Ｎｅａｒ　Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ）を利用した通信が挙げられる。
【００１９】
具体的には、例えば、情報処理装置１０１は、公的身分証明書１１０に組み込まれたＩＣチップから、ユーザの画像を含む個人情報を読み取る。例えば、公的身分証明書１１０が運転免許証の場合には、氏名、生年月日、住所、顔写真、公開鍵、電子署名などを含む情報が個人情報として読み取られる。
【００２０】
（２）情報処理装置１０１は、読み取った個人情報に基づき、公的身分証明書１１０が

正当であるか否かを判定する。すなわち、情報処理装置１０１は、公的身分証明書１１０が本物であるか偽物であるかの真贋判定を行う。公的身分証明書１１０の正当性の判定には、例えば、ＰＫＩ（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）を利用した偽造・変造検証を用いることができる。

【００２１】

偽造・変造検証とは、文書（例えば、公的身分証明書１１０）が偽造や変造されたものではないことを検証する処理である。ＰＫＩを利用した公的身分証明書１１０の偽造・変造検証では、例えば、公的身分証明書１１０のＩＣチップ内の電子署名を用いて改ざんが検知される。なお、偽造・変造検証の処理は、情報処理装置１０１とは異なる他のコンピュータ（例えば、後述の図２に示す検証サーバ２０１）で行われることにしてもよい。

【００２２】

（３）情報処理装置１０１は、公的身分証明書１１０が正当であると判定した場合に、ユーザを含む画像（撮影画像）を撮影する。具体的には、例えば、情報処理装置１０１は、公的身分証明書１１０が正当であると判定した場合に、撮影機能を起動して、ユーザの顔を含む画像を撮影し、撮影した画像を取得する。

【００２３】

ここで、撮影機能とは、画像（静止画または動画）を撮影する機能であり、例えば、後述の図３に示すような情報処理装置１０１のカメラ３０３により実現される。撮影対象のユーザは、本人確認の対象となるユーザである。すなわち、公的身分証明書１１０が正当であると判定されると、本人確認の対象となるユーザ自身が、情報処理装置１０１の撮影機能を利用して、顔画像を撮影する。これにより、本人確認の対象となるユーザの顔画像を得ることができる。

【００２４】

（４）情報処理装置１０１は、読み取った個人情報に含まれるユーザの画像と、撮影したユーザを含む撮影画像とに基づいて、本人認証の結果を出力する。ここで、本人認証とは、資格（例えば、サービス提供を受ける資格）を持つ者であることを主張するユーザの真正性を確認することである。

【００２５】

具体的には、例えば、情報処理装置１０１は、撮影画像から顔を検出し、当該撮影画像から顔画像を抽出する。つぎに、情報処理装置１０１は、個人情報に含まれる顔画像と、抽出した顔画像とを照合して照合率を算出する。照合率は、画像同士の類似度合いを示す指標値である。なお、顔照合処理は、情報処理装置１０１とは異なる他のコンピュータ（例えば、後述の図２に示す照合サーバ２０２）で行われることにしてもよい。

【００２６】

つぎに、情報処理装置１０１は、算出した照合率が、あらかじめ決められた閾値以上であれば、認証成功とする。一方、情報処理装置１０１は、算出した照合率が閾値未満であれば、認証失敗とする。そして、情報処理装置１０１は、本人認証の結果（顔照合結果）を出力する。

【００２７】

本人認証の結果の出力先は、例えば、取引先のコンピュータであってもよい。これにより、取引先の事業者等に対して、本人認証の結果を提供することができる。取引先の事業者等は、本人認証の結果から、相手方が本人であることに間違いがないかの本人確認を行うことができる。

【００２８】

また、情報処理装置１０１は、後述の図３に示すような情報処理装置１０１のディスプレイ３０５に、本人認証の結果を一旦表示し、その後のユーザの操作入力に応じて、本人認証の結果を取引先のコンピュータに送信することにしてもよい。

【００２９】

また、情報処理装置１０１は、上記（２）において公的身分証明書１１０が正当ではないと判定した場合、本人認証の結果として、公的身分証明書１１０が正当でないために本

人認証を行うことができない旨の情報を出力することにしてもよい。この場合は、本人確認できないこととなる。

【００３０】

このように、情報処理装置１０１によれば、公的身分証明書１１０から読み取った個人情報に基づき、公的身分証明書１１０の正当性を確認することができる。また、情報処理装置１０１によれば、撮影機能を起動して撮影されたユーザを含む撮影画像を、正当性が確認された公的身分証明書１１０から読み取られた顔画像と照合して、本人認証を行うことができる。

【００３１】

これにより、オンラインでの本人確認を実現して、本人確認の手続きにかかる負荷を軽減することができる。例えば、本人認証に成功すれば、正当な公的身分証明書１１０から読み取られた顔画像の人物と、本人確認の対象となるユーザとが一致するといえるため、本人であることに間違いがないことを確認することができる。一方、本人認証に失敗すれば、正当な公的身分証明書１１０から読み取られた顔画像の人物と、本人確認の対象となるユーザとが一致しないといえるため、本人確認できないこととなる。

【００３２】

（本人確認システム２００のシステム構成例）

つぎに、図１に示した情報処理装置１０１を含む本人確認システム２００のシステム構成例について説明する。本人確認システム２００は、例えば、オンラインでの本人確認を要する取引を行うシステムに適用される。

【００３３】

図２は、本人確認システム２００のシステム構成例を示す説明図である。図２において、本人確認システム２００は、情報処理装置１０１と、検証サーバ２０１と、照合サーバ２０２と、事業者サーバ２０３と、を含む。本人確認システム２００において、情報処理装置１０１、検証サーバ２０１、照合サーバ２０２および事業者サーバ２０３は、有線または無線のネットワーク２１０を介して接続される。ネットワーク２１０は、例えば、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）、インターネットなどである。

【００３４】

ここで、情報処理装置１０１は、本人確認システム２００のユーザが使用するコンピュータである。ユーザは、例えば、事業者と取引を行う者である。情報処理装置１０１は、例えば、スマートフォン、タブレットＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）などである。

【００３５】

検証サーバ２０１は、公的身分証明書の偽造・変造検証処理を実行するコンピュータである。照合サーバ２０２は、顔照合処理を実行するコンピュータである。なお、顔照合処理は、例えば、Ｗｅｂ ＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）により実現されることにしてもよい。

【００３６】

事業者サーバ２０３は、オンラインでの本人確認を要する取引を行う事業者のコンピュータである。事業者は、例えば、犯罪収益移転防止法における特定事業者（金融機関、クレジットカード事業者など）であってもよく、また、地方公共団体などの公的機関であってもよい。

【００３７】

なお、図２の例では、事業者サーバ２０３を１台のみ表記したが、これに限らない。例えば、事業者サーバ２０３は、オンラインでの本人確認を要する取引を行う事業者ごとに設けられる。また、検証サーバ２０１および照合サーバ２０２は、１つのサーバにより実現されることにしてもよい。

【００３８】

（情報処理装置１０１のハードウェア構成例）

つぎに、情報処理装置１０１のハードウェア構成例について説明する。

【００３９】

図３は、情報処理装置１０１のハードウェア構成例を示すブロック図である。図３において、情報処理装置１０１は、ＣＰＵ３０１と、メモリ３０２と、カメラ３０３と、通信Ｉ／Ｆ３０４と、ディスプレイ３０５と、入力装置３０６と、読取装置３０７と、ＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）ユニット３０８と、を有する。また、各構成部はバス３００によってそれぞれ接続される。

【００４０】

ここで、ＣＰＵ３０１は、情報処理装置１０１の全体の制御を司る。メモリ３０２は、例えば、ＲＯＭ、ＲＡＭおよびフラッシュＲＯＭなどを有する。具体的には、例えば、フラッシュＲＯＭやＲＯＭが各種プログラムを記憶し、ＲＡＭがＣＰＵ３０１のワークエリアとして使用される。メモリ３０２に記憶されるプログラムは、ＣＰＵ３０１にロードされることで、コーディングされている処理をＣＰＵ３０１に実行させる。

【００４１】

カメラ３０３は、画像（静止画または動画）を撮影して画像データを出力する撮影装置である。カメラ３０３は、例えば、ディスプレイ３０５側に搭載されるインカメラや、ディスプレイ３０５の背面側に搭載されるアウトカメラである。

【００４２】

通信Ｉ／Ｆ３０４は、通信回線を通じてネットワーク２１０に接続され、ネットワーク２１０を介して他の装置（例えば、図２に示した検証サーバ２０１、照合サーバ２０２、事業者サーバ２０３）に接続される。そして、通信Ｉ／Ｆ３０４は、ネットワーク２１０と自装置内部とのインターフェースを司り、他の装置からのデータの入出力を制御する。

【００４３】

ディスプレイ３０５は、カーソル、アイコンあるいはツールボックスをはじめ、文書、画像、機能情報などのデータを表示する。ディスプレイ３０５は、例えば、被写体を表示する画面として機能することができる。ディスプレイ３０５としては、例えば、液晶ディスプレイ、有機ＥＬ（Ｅｌｅｃｔｒｏｌｕｍｉｎｅｓｃｅｎｃｅ）ディスプレイなどを採用することができる。

【００４４】

入力装置３０６は、文字、数字、各種指示などの入力のためのキーを有し、データの入力を行う。入力装置３０６は、キーボードやマウスなどであってもよく、また、タッチパネル式の入力パッドやテンキーなどであってもよい。読取装置３０７は、近距離無線通信によりデータの読み取りを行う装置である。例えば、読取装置３０７は、ＮＦＣのリーダライタ装置である。

【００４５】

ＧＰＳユニット３０８は、ＧＰＳ衛星からの電波を受信し、情報処理装置１０１の位置情報を出力する。情報処理装置１０１の位置情報は、例えば、緯度、経度などの地球上の１点を特定する情報である。また、情報処理装置１０１は、ＤＧＰＳ（Ｄｉｆｆｅｒｅｎｔｉａｌ　ＧＰＳ）により、ＧＰＳユニット３０８から出力される位置情報を補正することにしてもよい。また、衛星として、例えば、準天頂衛星システムの衛星を用いることにしてもよい。

【００４６】

なお、情報処理装置１０１は、上述した構成部のほかに、例えば、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）、可搬型記録媒体Ｉ／Ｆ、マイクロホン、スピーカなどを有することにしてもよい。また、図２に示した検証サーバ２０１、照合サーバ２０２および事業者サーバ２０３については、例えば、ＣＰＵ、メモリ、通信Ｉ／Ｆ、ＨＤＤ、可搬型記録媒体Ｉ／Ｆなどのハードウェア構成により実現される。

【００４７】

（情報処理装置１０１の機能的構成例）

図４は、情報処理装置１０１の機能的構成例を示すブロック図である。図４において、情報処理装置１０１は、受付部４０１と、読取部４０２と、判定部４０３と、撮影制御部４０４と、認証部４０５と、出力部４０６と、を含む。具体的には、例えば、受付部４０１～出力部４０６は、図３に示したメモリ３０２に記憶されたプログラムをＣＰＵ３０１に実行させることにより、または、通信Ｉ／Ｆ３０４により、その機能を実現する。各機能部の処理結果は、例えば、メモリ３０２に記憶される。

【００４８】

受付部４０１は、オンラインでの本人確認を要する取引の開始要求を受け付ける。オンラインでの本人確認を要する取引は、例えば、金融機関における口座開設や住所変更などである。具体的には、例えば、受付部４０１は、図３に示した入力装置３０６を用いたユーザの操作入力により、オンラインでの本人確認を要する取引の開始要求を受け付ける。また、受付部４０１は、図２に示した事業者サーバ２０３から受信することにより、オンラインでの本人確認を要する取引の開始要求を受け付けることにしてもよい。

【００４９】

読取部４０２は、ユーザの画像を含む個人情報を公的身分証明書から読み取る。公的身分証明書は、例えば、運転免許証、個人番号カード、パスポート、在留カードなどである。具体的には、例えば、読取部４０２は、オンラインでの本人確認を要する取引の開始要求を受け付けた場合に、図３に示した読取装置３０７により、公的身分証明書に組み込まれたＩＣチップから、身分証情報を読み取る。

【００５０】

身分証情報は、公的身分証明書により身分が証明されたユーザの画像を含む個人情報である。身分証情報には、例えば、氏名、生年月日、住所、顔画像、公開鍵、電子署名などが含まれる。顔画像は、ユーザの画像である。公開鍵は、公的身分証明書の発行者（例えば、公的機関）の公開鍵である。

【００５１】

電子署名は、公的身分証明書の発行者の秘密鍵を用いて生成された電子署名である。より詳細に説明すると、例えば、電子署名は、ハッシュ関数を用いて身分証情報（氏名、生年月日、住所、顔画像）から生成されたハッシュ値を、発行者の秘密鍵を用いて暗号化することにより生成される。

【００５２】

なお、情報処理装置１０１は、複数の公的身分証明書の中から、個人情報を読み取る公的身分証明書の選択を受け付けることにしてもよい。この場合、読取部４０２は、選択された公的身分証明書から、ユーザの画像を含む個人情報を読み取る。

【００５３】

判定部４０３は、読み取られた個人情報に基づき、公的身分証明書が正当であるか否かを判定する。ここで、公的身分証明書の正当性の判定には、例えば、ＰＫＩを利用した公的身分証明書の偽造・変造検証を用いることができる。

【００５４】

具体的には、例えば、判定部４０３は、読み取られた身分証情報に含まれる公開鍵および電子署名を取得する。つぎに、判定部４０３は、取得した公開鍵および電子署名を添付した身分証情報（氏名、生年月日、住所、顔画像）を、図２に示した検証サーバ２０１に送信する。すなわち、情報処理装置１０１は、検証サーバ２０１に対して、公的身分証明書の偽造・変造検証を依頼する。

【００５５】

検証サーバ２０１は、情報処理装置１０１から公開鍵および電子署名が添付された身分証情報を受信すると、ハッシュ関数を用いて、身分証情報のハッシュ値を生成する。そして、検証サーバ２０１は、身分証情報に添付された公開鍵を用いて、身分証情報に添付された電子署名を復号する。

【００５６】

つぎに、検証サーバ２０１は、生成した身分証情報のハッシュ値と、電子署名を復号し

て得られたハッシュ値とを比較する。ここで、ハッシュ値が一致する場合、検証サーバ２０１は、公的身分証明書が本物である、すなわち、偽造されていないと判定する。一方、ハッシュ値が一致しない場合、検証サーバ２０１は、公的身分証明書が偽物である、すなわち、偽造されていると判定する。

【００５７】

そして、検証サーバ２０１は、公的身分証明書が偽造されているか否かを示す検証結果を情報処理装置１０１に送信する。判定部４０３は、検証サーバ２０１からの検証結果が偽造されていないことを示す場合、公的身分証明書が正当であると判定する。一方、検証サーバ２０１からの検証結果が偽造されていることを示す場合、判定部４０３は、公的身分証明書が正当ではないと判定する。

【００５８】

撮影制御部４０４は、公的身分証明書が正当であると判定された場合に、撮影機能を起動して、ユーザを含む撮影画像を撮影する制御を行う。撮影対象のユーザは、本人確認の対象となるユーザである。以下の説明では、本人確認の対象となるユーザを「対象ユーザ」と表記する場合がある。

【００５９】

具体的には、例えば、撮影制御部４０４は、公的身分証明書が正当であると判定された場合に、自装置の撮影機能を起動して、図３に示したカメラ３０３により、対象ユーザを含む撮影画像を撮影する。この際、撮影制御部４０４は、対象ユーザを含む静止画を撮影してもよく、また、対象ユーザを含む動画を撮影してもよい。

【００６０】

また、撮影制御部４０４は、対象ユーザを撮影する際に、被写体を表示する画面に、顔を位置付けるガイドを表示することにしてもよい。被写体を表示する画面は、例えば、図３に示したディスプレイ３０５に表示される。ガイドは、画面上での顔の位置を示す図形であってもよく、文字や記号を組み合わせたものであってもよい。

【００６１】

これにより、ユーザは、例えば、ディスプレイ３０５に表示されるガイドに従って、被写体を表示する画面上での顔の位置を合わせることで、自身の顔画像を簡単に撮影することができる。以下の説明では、被写体を表示する画面を「ファインダ画面」と表記する場合がある。

【００６２】

認証部４０５は、読み取られた個人情報に含まれるユーザの画像と、撮影された対象ユーザを含む撮影画像とに基づいて、本人認証を行う。具体的には、例えば、認証部４０５は、読み取られた身分証情報に含まれる顔画像と、撮影された対象ユーザを含む撮影画像とを、図２に示した照合サーバ２０２に送信する。

【００６３】

すなわち、情報処理装置１０１は、照合サーバ２０２に対して、身分証情報に含まれる顔画像と、対象ユーザを含む撮影画像とに基づく顔照合を依頼する。照合サーバ２０２は、情報処理装置１０１から身分証情報に含まれる顔画像と、対象ユーザを含む撮影画像とを受信すると、撮影画像から顔を検出し、当該撮影画像から顔画像を抽出する。

【００６４】

つぎに、照合サーバ２０２は、身分証情報に含まれる顔画像と、抽出した顔画像とを照合して照合率を算出する。この際、照合サーバ２０２は、算出した照合率に基づいて、他人受入率をあわせて算出することにしてもよい。他人受入率とは、本人ではないのに本人と認識してしまう割合のことである。なお、照合率や他人受入率を算出する技術としては、既存のいかなる技術を用いることにしてもよい。

【００６５】

そして、照合サーバ２０２は、算出した照合率（または、照合率および他人受入率）を情報処理装置１０１に送信する。認証部４０５は、照合サーバ２０２から照合率（または、照合率および他人受入率）を受信すると、受信した照合率が、閾値α以上であるか否か

を判断する。閾値αは、任意に設定可能であり、例えば、８０［％］程度の値に設定される。

【００６６】

ここで、照合率が閾値α以上であれば、認証部４０５は、認証成功とする。一方、照合率が閾値α未満であれば、認証部４０５は、認証失敗とする。なお、ここでは、照合サーバ２０２に対して顔照合を依頼する場合を例に挙げて説明したが、これに限らない。例えば、認証部４０５が、顔照合処理を実行することにしてもよい。

【００６７】

また、対象ユーザを含む動画が撮影された場合には、認証部４０５は、個人情報に含まれるユーザの画像と、撮影された対象ユーザを含む動画とに基づいて、本人認証を行うことにしてもよい。具体的には、例えば、認証部４０５は、撮影された動画から複数のフレーム画像を選択する。

【００６８】

複数のフレーム画像を選択するアルゴリズムは、任意に設定可能である。例えば、認証部４０５は、動画から、複数のフレーム画像を、ランダムに選択してもよいし、１枚置きに選択してもよいし、顔が検出されたものを選択してもよい。

【００６９】

つぎに、認証部４０５は、選択した複数のフレーム画像それぞれと、身分証情報に含まれる顔画像とを照合した結果に基づいて、本人認証を行う。より詳細に説明すると、例えば、認証部４０５は、複数のフレーム画像のうちの少なくともいずれかのフレーム画像の照合率が閾値α以上の場合に、認証成功としてもよい。

【００７０】

これにより、画像（静止画）を１枚撮影して本人認証を行う場合に比べて、認証精度を高めることができる。例えば、本人であるにもかかわらず、顔の写り方が悪い画像であったために照合率が低くなって認証失敗となるといったことを防ぐことができる。

【００７１】

あるいは、認証部４０５は、複数のフレーム画像それぞれと顔画像とを照合して得られるすべての照合率が閾値α以上の場合に、認証成功としてもよい。これにより、他人であるにもかかわらず、たまたま照合率が高くなって認証成功となるといったことを防ぐことができる。

【００７２】

また、認証部４０５は、読み取られた個人情報に住所情報が含まれる場合、ユーザ（対象ユーザ）の現在位置を示す位置情報を取得することにしてもよい。そして、認証部４０５は、取得した位置情報と個人情報に含まれる住所情報との比較結果にさらに基づいて、本人認証を行うことにしてもよい。

【００７３】

具体的には、例えば、認証部４０５は、読み取られた身分証情報に住所が含まれる場合、図３に示したＧＰＳユニット３０８により、自装置の位置情報を、ユーザの現在位置を示す位置情報として取得する。つぎに、認証部４０５は、身分証情報に含まれる住所が示す位置と、取得した位置情報が示すユーザの現在位置との距離を算出する。

【００７４】

なお、距離の算出は、情報処理装置１０１とは異なる外部サーバで行うことにしてもよい。例えば、認証部４０５が、身分証情報に含まれる住所と、ユーザの現在位置を示す位置情報とを外部サーバに送信することにより、距離の算出を依頼することにしてもよい。

【００７５】

そして、認証部４０５は、算出した距離が閾値β以下であるか否かを判断する。閾値βは、任意に設定可能であり、例えば、数十メートル程度の値に設定される。ここで、距離が閾値β以下の場合、認証部４０５は、公的身分証明書の住所付近にユーザが存在すると判定する。一方、距離が閾値βより大きい場合、認証部４０５は、公的身分証明書の住所付近にユーザが存在しないと判定する。

【００７６】
そして、認証部４０５は、照合率が閾値α以上であり、かつ、公的身分証明書の住所付近にユーザが存在すると判定した場合に、認証成功としてもよい。一方、照合率が閾値α以上であっても、公的身分証明書の住所付近にユーザが存在しないと判定した場合には、認証部４０５は、認証失敗としてもよい。
【００７７】
これにより、公的身分証明書のユーザの画像を利用した顔照合だけでなく、公的身分証明書の住所を利用した現在位置確認により、本人認証を行うことができる。
【００７８】
出力部４０６は、本人認証の結果を出力する。出力部４０６の出力形式としては、例えば、メモリ３０２への記憶、通信Ｉ／Ｆ３０４による他のコンピュータへの送信、ディスプレイ３０５への表示、不図示のプリンタへの印刷出力などがある。
【００７９】
具体的には、例えば、出力部４０６は、後述の図６Ｄに示すような認証結果画面ＳＣ９をディスプレイ３０５に表示することにしてもよい。認証結果画面ＳＣ９は、本人認証の結果を示す画面である。これにより、情報処理装置１０１のユーザ（対象ユーザ）に対して、本人認証の結果を示すことができる。
【００８０】
また、出力部４０６は、本人認証の結果を、事業者サーバ２０３に送信することにしてもよい。これにより、オンラインでの本人確認を要する取引先に対して、本人認証の結果を通知することができる。取引先の事業者は、例えば、本人認証の結果から、相手方が本人であることに間違いがないかの本人確認を行うことができる。この際、本人認証の結果だけを事業者に提示すればよいため、事業者側に個人情報を提示することなく、本人確認を行わせることができる。
【００８１】
ただし、出力部４０６は、本人認証に成功した場合、本人認証の結果とともに、読み取られた個人情報に含まれるユーザの画像を出力することにしてもよい。具体的には、例えば、出力部４０６は、本人認証に成功した場合、本人認証の結果とともに、身分証情報に含まれる顔画像を、事業者サーバ２０３に送信することにしてもよい。
【００８２】
これにより、取引先の事業者に対して、正当（本物）であると判定された公的身分証明書に記録された顔画像を提供することができる。例えば、取引を行うにあたり、事業者がユーザの個人情報（顔画像）を要求する場合などに、ユーザが個人情報（顔画像）を手入力するなどの手間を省くことができる。
【００８３】
また、出力部４０６は、公的身分証明書が正当ではないと判定された場合、公的身分証明書が正当ではないことを示す判定結果を出力することにしてもよい。具体的には、例えば、出力部４０６は、公的身分証明書が正当でないために、本人認証を行うことができないことを示す情報を出力することにしてもよい。
【００８４】
また、出力部４０６は、公的身分証明書が正当であると判定された場合に、撮影機能を起動して動画を撮影中に、モーション指示を出力することにしてもよい。この際、出力部４０６は、複数のモーション指示の中からランダムに選択したモーション指示を出力することにしてもよい。
【００８５】
ここで、モーション指示とは、被写体に対して、特定のモーション（動作）を行うよう指示するものである。モーション指示は、例えば、ファインダ画面に表示される画像や、不図示のスピーカからの音声によって行われる。特定のモーションとしては、例えば、まばたき、口の開閉、うなずき、顔振りなどが挙げられる。
【００８６】

これにより、対象ユーザに対して、まばたき、口の開閉、うなずき、顔振りなどのモーションを行うよう指示することができる。なお、モーション指示の出力例については、図６Ｄを用いて後述する。

【００８７】

また、認証部４０５は、撮影された対象ユーザを含む動画に基づいて、出力されたモーション指示に対応する動作が行われているか否かを判断することにしてもよい。例えば、特定のモーションが「まばたき」であれば、認証部４０５は、撮影された動画に基づいて、「まばたき」が行われているか否かを判断する。

【００８８】

より詳細に説明すると、例えば、認証部４０５は、『眼を開けた状態⇒眼を閉じた状態⇒眼を開けた状態』の画像が順に検出されると、「まばたき」が行われていると判断する。また、例えば、特定のモーションが「顔振り」であれば、認証部４０５は、撮影された動画に基づいて、『左向き⇒正面⇒右向き⇒正面』の順に顔が動いていれば、「顔振り」が行われていると判断する。なお、被写体が特定のモーション（動作）を行っているか否かを動画から判断する技術としては、既存のいかなる技術を用いることにしてもよい。

【００８９】

そして、認証部４０５は、モーション指示に対応する動作が行われているか否かの判断結果にさらに基づいて、本人認証を行うことにしてもよい。具体的には、例えば、認証部４０５は、モーション指示に対応する動作が行われていると判断した場合に、身分証情報に含まれる顔画像と対象ユーザを含む撮影画像とに基づく本人認証を行う。一方、モーション指示に対応する動作が行われていないと判断した場合には、認証部４０５は、本人認証は行わないことにしてもよい。

【００９０】

これにより、モーション指示に対応する動作が行われなければ、本人認証のフェーズに移行しないことになるため、例えば、公的身分証明書の顔写真を撮影して対象ユーザの撮影画像とするなどの不正行為を防ぐことができる。また、モーション指示をランダムに選択して出力することで、例えば、出力されるモーション指示を予測しにくくして、モーション指示に応じた動画が事前に用意されるのを防ぐことができる。

【００９１】

なお、情報処理装置１０１は、モーション指示の出力、および、モーション指示に対応する動作が行われているか否かの判断を、モーション指示を変更しながら複数回繰り返し行うことにしてもよい。

【００９２】

上述した説明では、読取部４０２が、読取装置３０７により、公的身分証明書に組み込まれたＩＣチップから、身分証情報を読み取る場合を例に挙げて説明したが、これに限らない。例えば、情報処理装置１０１が読取装置３０７を有していない、あるいは、何らかの理由により読取装置３０７を使用できない場合がある。

【００９３】

この場合、撮影制御部４０４は、公的身分証明書を含む撮影画像を撮影する制御を行うことにしてもよい。読取部４０２は、撮影された公的身分証明書を含む撮影画像を文字認識処理して、公的身分証明書に記載された個人情報を読み取る。具体的には、例えば、読取部４０２は、ＯＣＲ（Ｏｐｔｉｃａｌ　Ｃｈａｒａｃｔｅｒ　Ｒｅａｄｅｒ）で、公的身分証明書を含む撮影画像を文字認識し、公的身分証明書に記載された氏名、生年月日、住所などの個人情報を読み取る。

【００９４】

また、読取部４０２は、撮影された公的身分証明書を含む撮影画像をトリミング処理して、公的身分証明書に付されたユーザの画像を取得する。ここで、トリミング処理とは、画像の一部を切り出す加工処理のことである。具体的には、例えば、読取部４０２は、撮影画像から顔写真部分を検出し、検出した顔写真部分を切り出すことにより、公的身分証明書に付された顔画像（顔写真）を取得する。

【００９５】
これにより、ＮＦＣ等を利用して個人情報を読み取ることができない場合は、公的身分証明書を含む撮影画像を画像処理して、ユーザの画像を含む個人情報を読み取ることができる。ＮＦＣを利用できない場合とは、例えば、情報処理装置１０１が読取装置３０７を有していない、何らかの理由により読取装置３０７を使用できない、公的身分証明書にＩＣが組み込まれていない場合などである。
【００９６】
ただし、この場合、公的身分証明書の正当性の判定に、ＰＫＩを利用した公的身分証明書の偽造・変造検証を用いることができない。そこで、判定部４０３は、例えば、読み取られた個人情報に含まれる住所に基づいて、公的身分証明書が正当であるか否かを判定することにしてもよい。
【００９７】
具体的には、例えば、判定部４０３は、ユーザ（対象ユーザ）の現在位置を示す位置情報を取得する。そして、判定部４０３は、取得した位置情報と個人情報に含まれる住所との比較結果に基づいて、公的身分証明書が正当であるか否かを判定することにしてもよい。
【００９８】
より詳細に説明すると、例えば、判定部４０３は、ＧＰＳユニット３０８により、自装置の位置情報を、ユーザの現在位置を示す位置情報として取得する。つぎに、判定部４０３は、個人情報に含まれる住所が示す位置と、取得した位置情報が示すユーザの現在位置との距離を算出する。
【００９９】
そして、判定部４０３は、算出した距離が閾値β以下であるか否かを判断する。ここで、距離が閾値β以下の場合、判定部４０３は、公的身分証明書が正当であると判定する。一方、距離が閾値βより大きい場合、判定部４０３は、公的身分証明書が正当ではないと判定する。
【０１００】
すなわち、公的身分証明書の住所付近にユーザが存在すれば、公的身分証明書の記載内容が偽造されたものではないと判断して、公的身分証明書が正当であると判定する。これにより、ＮＦＣ等を利用して個人情報を読み取ることができない場合であっても、公的身分証明書の正当性を判定することができる。
【０１０１】
なお、上述したトリミング処理は、公的身分証明書に組み込まれたＩＣチップに、氏名、生年月日、住所、公開鍵などの情報は記録されているものの、顔画像が記録されていない場合に適用することにしてもよい。これにより、運転免許証に付された顔写真などを利用して、本人認証に用いるユーザの画像（顔画像）を取得することができる。
【０１０２】
また、上述した説明では、情報処理装置１０１は、公的身分証明書が正当であると判定した場合に、ユーザを含む画像を撮影することにしたが、これに限らない。例えば、情報処理装置１０１は、公的身分証明書の正当性の判定を行う前に、ユーザを含む撮影画像を撮影することにしてもよい。この場合、情報処理装置１０１は、例えば、公的身分証明書が正当であると判定した場合に、正当な公的身分証明書から読み取った顔画像とカメラ３０３で撮影した撮影画像とに基づき、本人認証を行うことにしてもよい。
【０１０３】
（オンラインでの本人確認の手順）
つぎに、図５を用いて、オンラインでの本人確認の手順について説明する。ここでは、公的身分証明書として「運転免許証」を例に挙げて説明する。
【０１０４】
図５は、オンラインでの本人確認の手順の一例を示す説明図である。図５において、まず、情報処理装置１０１は、読取装置３０７により、運転免許証５０１に組み込まれたＩ

Ｃチップから身分証情報を読み取る（ステップＳ５１）。身分証情報には、例えば、氏名、生年月日、住所、顔画像（顔写真）、公開鍵などが含まれる。

【０１０５】

なお、運転免許証５０１のＩＣチップに顔画像が記録されていない場合には、情報処理装置１０１は、カメラ３０３により撮影された運転免許証５０１を含む撮影画像をトリミング処理して、運転免許証５０１の顔画像（顔写真）を取得する（ステップＳ５２）。

【０１０６】

つぎに、情報処理装置１０１は、身分証情報に基づき、公的機関（例えば、検証サーバ２０１）に問い合わせることにより、運転免許証５０１の正当性判定を行う（ステップＳ５３）。ここで、運転免許証５０１が正当であると判定された場合、情報処理装置１０１は、特定モーションの実行による本人検出を行う（ステップＳ５４）。

【０１０７】

ここで、特定モーションの実行による本人検出とは、カメラ３０３により撮影された動画に基づいて、モーション指示に対応する動作が行われているか否かを判断する処理である。モーション指示に対応する動作が行われていれば、本人が検出される。モーション指示に対応する動作が行われていなければ、本人は検出されない。

【０１０８】

ここで、本人が検出されると、情報処理装置１０１は、カメラ３０３により撮影された動画と、身分証情報に含まれる顔画像（または、ステップＳ５２において取得した顔画像）とに基づいて、本人認証（顔照合）を行う（ステップＳ５５）。

【０１０９】

また、運転免許証５０１が正当であると判定された場合に、情報処理装置１０１は、インカメラによる本人検出を行うことにしてもよい（ステップＳ５６）。ここで、インカメラによる本人検出とは、カメラ３０３（ディスプレイ３０５側に搭載されるインカメラ）により、対象ユーザを含む静止画を撮影することである。

【０１１０】

この場合、情報処理装置１０１は、カメラ３０３により撮影された静止画と、身分証情報に含まれる顔画像（または、ステップＳ５２において取得した顔画像）とに基づいて、本人認証（顔照合）を行う（ステップＳ５７）。

【０１１１】

（オンラインでの本人確認時の操作画面の遷移例）

つぎに、オンラインでの本人確認時に、情報処理装置１０１が、ユーザの操作入力に応じてディスプレイ３０５に表示する画面の遷移例について説明する。以下の説明では、操作画面に表示されているボックス、ボタン等をユーザが選択する操作として、タップ操作を行う場合を例に挙げて説明する。

【０１１２】

図６Ａ～図６Ｄは、オンラインでの本人確認時の画面の第１の遷移例を示す説明図である。図６Ａにおいて、書類確認方法選択画面ＳＣ１は、公的身分証明書の確認方法を選択する操作画面である。書類確認方法選択画面ＳＣ１において、ボタン６０１をタップすると、暗証番号入力画面ＳＣ２に遷移する。ここでは、公的身分証明書として、運転免許証を例に挙げて説明する。

【０１１３】

暗証番号入力画面ＳＣ２は、運転免許証の暗証番号１および暗証番号２を入力する操作画面である。暗証番号１および暗証番号２は、運転免許証の取得時または更新時に設定される暗証番号（４桁の数字）である。暗証番号入力画面ＳＣ２において、運転免許証の暗証番号１および暗証番号２を入力し、ボタン６０３をタップすると、入力された暗証番号１および暗証番号２の検証が行われる。

【０１１４】

なお、運転免許証の正しい暗証番号は、例えば、身分証情報と対応付けてメモリ３０２に記憶されていてもよく、また、身分証情報をキーにして公的機関（警察のサーバ）に問

い合わせることにしてもよい。

【０１１５】

ここで、入力された暗証番号１および暗証番号２が正しければ、ＮＦＣ読取画面ＳＣ３に遷移する。なお、暗証番号の検証に失敗すると、検証失敗を示す画面（不図示）に遷移する。暗証番号入力画面ＳＣ２はスキップして、書類確認方法選択画面ＳＣ１からＮＦＣ読取画面ＳＣ３に遷移することにしてもよい。

【０１１６】

ＮＦＣ読取画面ＳＣ３は、運転免許証に組み込まれたＩＣチップから、身分証情報を読み取るための操作画面である。ユーザが装置本体の裏側に運転免許証をタッチすると、読取装置３０７により、顔画像を含む身分証情報が読み取られる。

【０１１７】

顔画像を含む身分証情報が読み取られると、当該身分証情報に基づき、運転免許証の正当性が判定される。運転免許証の正当性の判定には、例えば、ＰＫＩを利用した運転免許証の偽造・変造検証が用いられる。運転免許証の偽造・変造検証が完了すると、検証結果画面ＳＣ４に遷移する。

【０１１８】

検証結果画面ＳＣ４は、運転免許証の偽造・変造検証の検証結果（検証成功）を示す操作画面である。なお、運転免許証の偽造・変造検証に失敗すると、検証失敗を示す画面（不図示）に遷移する。検証結果画面ＳＣ４には、運転免許証のＩＣチップから読み取られた身分証情報に含まれる氏名、生年月日、住所、顔画像が表示される。検証結果画面ＳＣ４において、ボタン６０４をタップすると、現在位置確認画面ＳＣ５に遷移する。

【０１１９】

現在位置確認画面ＳＣ５は、ユーザの現在位置に関する確認結果（確認成功）を示す操作画面である。なお、ユーザの現在位置の確認に失敗すると、確認失敗を示す画面（不図示）に遷移する。現在位置確認画面ＳＣ５には、マップ６０５と、現在地６０６と、読取結果住所位置６０７とが表示されている。マップ６０５は、運転免許証のＩＣチップから読み取られた身分証情報に含まれる住所付近の地図である。

【０１２０】

現在地６０６は、情報処理装置１０１のユーザの現在位置を示す。読取結果住所位置６０７は、運転免許証のＩＣチップから読み取られた身分証情報に含まれる住所を示す。また、マップ６０５内のマークＭ１は、身分証情報に含まれる住所を示す。マークＭ２は、ユーザの現在位置を示す。

【０１２１】

マップ６０５を表示するための地図情報は、例えば、メモリ３０２にあらかじめ記憶されていてもよく、また、情報処理装置１０１とは異なる外部サーバ（地図情報提供サービスを行うサーバなど）から取得されることにしてもよい。

【０１２２】

ここでは、距離が閾値β以下であり、運転免許証の住所付近にユーザが存在すると判定された場合を想定する。マップ６０５においても、マークＭ１，Ｍ２はほぼ一致している。この場合、現在位置確認画面ＳＣ５において、ボタン６０８をタップすると、認証画面ＳＣ６に遷移する。

【０１２３】

認証画面ＳＣ６は、顔照合により本人認証を行うことを知らせる操作画面である。認証画面ＳＣ６において、ボタン６０９をタップすると、カメラ３０３の撮影機能が起動されて動画の撮影が開始され、本人検出画面ＳＣ７に遷移する。

【０１２４】

本人検出画面ＳＣ７は、特定モーションの実行による本人検出を行う操作画面である。本人検出画面ＳＣ７には、ファインダ画面６１０とともにモーション指示６１１が表示されている。また、ファインダ画面６１０には、顔を位置付けるガイド６１２が表示されている。モーション指示６１１は、被写体に対して、顔振り（頭を横に振る）を行うよう指

示するものである。
【０１２５】
本人検出画面ＳＣ７によれば、ユーザは、ファインダ画面６１０を見ながら、ガイド６１２に従って顔の位置を合わせつつ、モーション指示６１１に対応する動作を行うことができる。ここで、モーション指示６１１に対応する動作、すなわち、顔振り（頭を横に振る）が行われると、認証中画面ＳＣ８に遷移する。
【０１２６】
なお、本人検出画面ＳＣ７において、モーション指示６１１に対応する動作が行われなければ、認証失敗を示す画面（不図示）に遷移する。
【０１２７】
認証中画面ＳＣ８は、顔照合による本人認証を行っていることを示す画面である。本人認証では、例えば、カメラ３０３により撮影された動画のうちの少なくともいずれかのフレーム画像（例えば、対象ユーザが正面を向いている画像）と、身分証情報に含まれる顔画像との照合が行われる。顔照合による本人認証が完了すると、認証結果画面ＳＣ９に遷移する。
【０１２８】
認証結果画面ＳＣ９は、顔照合による本人認証の結果（認証成功）を示す操作画面である。認証結果画面ＳＣ９には、照合率（単位：％）と他人受入率とが表示されている。なお、顔照合による本人認証に失敗すると、認証失敗を示す画面（不図示）に遷移する。
【０１２９】
認証結果画面ＳＣ９において、ボタン６１３をタップすると、本人認証の結果（認証成功）が、取引先の事業者サーバ２０３に送信されて、取引が開始される。図示は省略するが、認証結果画面ＳＣ９には、各種パラメータ（照合率、他人受入率）の説明を表示することにしてもよい。
【０１３０】
これにより、オンラインでの本人確認を実現して、金融機関における口座開設等のオンラインでの本人確認を要する取引を円滑に行うことができる。
【０１３１】
つぎに、図６Ａに示した書類確認方法選択画面ＳＣ１において、ボタン６０２がタップされた場合の画面の遷移例について説明する。
【０１３２】
図７Ａ～図７Ｄは、オンラインでの本人確認時の画面の第２の遷移例を示す説明図である。図７Ａにおいて、書類選択画面ＳＣ１０は、カメラ３０３で撮影する公的身分証明書を選択する操作画面である。書類選択画面ＳＣ１０において、ボタン７０１をタップすると、運転免許証が選択される。書類選択画面ＳＣ１０において、ボタン７０２をタップすると、個人番号カードが選択される。書類選択画面ＳＣ１０において、ボタン７０３をタップすると、在留カードが選択される。
【０１３３】
ここでは、書類選択画面ＳＣ１０において、ボタン７０１がタップされ、公的身分証明書として運転免許証が選択された場合を例に挙げて説明する。書類選択画面ＳＣ１０において、ボタン７０１がタップされると、撮影書類確認画面ＳＣ１１に遷移する。
【０１３４】
撮影書類確認画面ＳＣ１１は、カメラ３０３で撮影する公的身分証明書の選択結果の確認を促す操作画面である。撮影書類確認画面ＳＣ１１において、ボタン７０４をタップすると、書類選択画面ＳＣ１０に遷移して、公的身分証明書の選択をやり直すことができる。撮影書類確認画面ＳＣ１１において、ボタン７０５をタップすると、撮影画面ＳＣ１２に遷移する。
【０１３５】
撮影画面ＳＣ１２は、公的身分証明書を撮影するための操作画面（ファインダ画面）である。撮影画面ＳＣ１２において、運転免許証を表示して、ボタン７０６をタップすると

、カメラ３０３の撮影機能が起動されて運転免許証が撮影され、撮影結果確認画面ＳＣ１３に遷移する。

【０１３６】

撮影結果確認画面ＳＣ１３は、カメラ３０３により撮影された運転免許証を含む撮影画像の確認を促す操作画面である。撮影結果確認画面ＳＣ１３において、ボタン７０７をタップすると、書類選択画面ＳＣ１０に遷移して、公的身分証明書の選択をやり直すことができる。撮影結果確認画面ＳＣ１３において、ボタン７０８をタップすると、運転免許証の正当性判定が開始される。

【０１３７】

ここでは、カメラ３０３により撮影された運転免許証を含む撮影画像から読み取られた個人情報に含まれる住所に基づいて、運転免許証が正当であるか否かを判定する場合を想定する。ここで、運転免許証が正当であると判定されると、認証画面ＳＣ１４に遷移する。一方、運転免許証が正当ではないと判定されると、検証失敗を示す画面（不図示）に遷移する。

【０１３８】

認証画面ＳＣ１４は、顔照合により本人認証を行うことを知らせる操作画面である。認証画面ＳＣ６において、ボタン７０９をタップすると、カメラ３０３の撮影機能が起動されて動画の撮影が開始され、本人検出画面ＳＣ１５に遷移する。

【０１３９】

本人検出画面ＳＣ１５は、特定モーションの実行による本人検出を行う操作画面である。本人検出画面ＳＣ１５には、ファインダ画面７１０とともにモーション指示７１１が表示されている。また、ファインダ画面７１０には、顔を位置付けるガイド７１２が表示されている。モーション指示７１１は、被写体に対して、顔振り（頭を横に振る）を行うよう指示するものである。

【０１４０】

ここで、モーション指示７１１に対応する動作、すなわち、顔振り（頭を横に振る）が行われると、認証中画面ＳＣ１６に遷移する。一方、モーション指示７１１に対応する動作が行われなければ、認証失敗を示す画面（不図示）に遷移する。

【０１４１】

認証中画面ＳＣ１６は、顔照合による本人認証を行っていることを示す画面である。顔照合による本人認証が完了すると、認証結果画面ＳＣ１７に遷移する。認証結果画面ＳＣ１７は、顔照合による本人認証の結果（認証成功）を示す操作画面である。認証結果画面ＳＣ１７には、照合率（単位：％）と他人受入率とが表示されている。なお、顔照合による本人認証に失敗すると、認証失敗を示す画面（不図示）に遷移する。

【０１４２】

認証結果画面ＳＣ１７において、ボタン７１３をタップすると、本人認証の結果（認証成功）が、取引先の事業者サーバ２０３に送信されて、取引が開始される。これにより、オンラインでの本人確認を実現して、金融機関における口座開設等のオンラインでの本人確認を要する取引を円滑に行うことができる。

【０１４３】

（情報処理装置１０１の本人確認支援処理手順）

つぎに、図８および図９を用いて、情報処理装置１０１の本人確認支援処理手順について説明する。本人確認支援処理は、例えば、オンラインでの本人確認を要する取引の開始要求に応じて実行される。

【０１４４】

図８および図９は、情報処理装置１０１の本人確認支援処理手順の一例を示すフローチャートである。図８のフローチャートにおいて、まず、情報処理装置１０１は、読取装置３０７により、公的身分証明書に組み込まれたＩＣチップから、顔画像を含む身分証情報を読み取る（ステップＳ８０１）。

【０１４５】

つぎに、情報処理装置１０１は、読み取った身分証情報に基づき、公的身分証明書の偽造・変造検証処理を行う（ステップＳ８０２）。偽造・変造検証処理の具体的な処理手順については、図１０を用いて後述する。

【０１４６】

つぎに、情報処理装置１０１は、公的身分証明書の偽造・変造検証の検証結果が、検証成功を示す結果であるか否かを判断する（ステップＳ８０３）。ここで、検証失敗を示す結果の場合（ステップＳ８０３：Ｎｏ）、情報処理装置１０１は、公的身分証明書が正当でないことを示す検証結果（ＮＧ）を出力して（ステップＳ８０４）、本フローチャートによる一連の処理を終了する。

【０１４７】

一方、検証成功を示す結果の場合（ステップＳ８０３：Ｙｅｓ）、情報処理装置１０１は、公的身分証明書が正当であることを示す検証結果（ＯＫ）を出力する（ステップＳ８０５）。つぎに、情報処理装置１０１は、ユーザの現在位置を示す位置情報を取得する（ステップＳ８０６）。

【０１４８】

なお、図６Ｂに示した検証結果画面ＳＣ４は、公的身分証明書が正当であることを示す検証結果（ＯＫ）を表示する画面の一例である。

【０１４９】

つぎに、情報処理装置１０１は、読み取った身分証情報に含まれる住所と、取得したユーザの現在位置を示す位置情報とに基づいて、公的身分証明書の住所付近にユーザが存在するか否かを判定する（ステップＳ８０７）。ここで、住所付近にユーザが存在しない場合（ステップＳ８０７：Ｎｏ）、情報処理装置１０１は、公的身分証明書の住所付近にユーザが存在しないことを示す判定結果（ＮＧ）を出力して（ステップＳ８０８）、本フローチャートによる一連の処理を終了する。

【０１５０】

一方、住所付近にユーザが存在する場合（ステップＳ８０７：Ｙｅｓ）、情報処理装置１０１は、公的身分証明書の住所付近にユーザが存在することを示す判定結果（ＯＫ）を出力して（ステップＳ８０９）、図９に示すステップＳ９０１に移行する。

【０１５１】

なお、図６Ｃに示した現在位置確認画面ＳＣ５は、公的身分証明書の住所付近にユーザが存在することを示す判定結果（ＯＫ）を表示する画面の一例である。

【０１５２】

図９のフローチャートにおいて、まず、情報処理装置１０１は、カメラ３０３の撮影機能を起動して、対象ユーザを含む動画を撮影する（ステップＳ９０１）。つぎに、情報処理装置１０１は、カメラ３０３により動画を撮影中に、モーション指示を出力する（ステップＳ９０２）。

【０１５３】

そして、情報処理装置１０１は、カメラ３０３により撮影した動画に基づいて、出力したモーション指示に対応する動作が行われているか否かを判断する（ステップＳ９０３）。ここで、モーション指示に対応する動作が行われていない場合（ステップＳ９０３：Ｎｏ）、情報処理装置１０１は、ステップＳ９０８に移行する。

【０１５４】

一方、モーション指示に対応する動作が行われている場合（ステップＳ９０３：Ｙｅｓ）、情報処理装置１０１は、撮影した動画から、対象ユーザを含むフレーム画像を選択する（ステップＳ９０４）。そして、情報処理装置１０１は、身分証情報に含まれる顔画像と、選択したフレーム画像とに基づいて、顔照合処理を行う（ステップＳ９０５）。

【０１５５】

なお、ステップＳ９０５の顔照合処理は、例えば、照合サーバ２０２に対して顔照合を依頼することにより行われる。ただし、情報処理装置１０１において顔照合処理を実行することにしてもよい。

【０１５６】
つぎに、情報処理装置１０１は、顔照合処理により得られた照合率が閾値α以上であるか否かを判断する（ステップＳ９０６）。ここで、照合率が閾値α以上の場合（ステップＳ９０６：Ｙｅｓ）、情報処理装置１０１は、認証成功を示す顔認証結果（ＯＫ）を出力して（ステップＳ９０７）、本フローチャートによる一連の処理を終了する。
【０１５７】
なお、図６Ｄに示した認証結果画面ＳＣ９は、認証成功を示す顔認証結果（ＯＫ）を表示する画面の一例である。
【０１５８】
一方、照合率が閾値α未満の場合（ステップＳ９０６：Ｎｏ）、情報処理装置１０１は、認証失敗を示す顔認証結果（ＮＧ）を出力して（ステップＳ９０８）、本フローチャートによる一連の処理を終了する。
【０１５９】
これにより、オンラインでの本人確認を実現することができる。なお、情報処理装置１０１は、ステップＳ８０７～Ｓ８０９の処理は実行しないことにしてもよい。
【０１６０】
つぎに、図１０を用いて、図８に示したステップＳ８０２の偽造・変造検証処理の具体的な処理手順について説明する。
【０１６１】
図１０は、偽造・変造検証処理の具体的処理手順の一例を示すフローチャートである。図１０のフローチャートにおいて、まず、情報処理装置１０１は、ステップＳ８０１において読み取った身分証情報に含まれる公開鍵および電子署名を取得する（ステップＳ１００１）。
【０１６２】
つぎに、情報処理装置１０１は、取得した公開鍵および電子署名を添付した身分証情報（氏名、生年月日、住所、顔画像）を検証サーバ２０１に送信する。（ステップＳ１００２）。そして、情報処理装置１０１は、検証サーバ２０１から検証結果を受信したか否かを判断する（ステップＳ１００３）。
【０１６３】
ここで、情報処理装置１０１は、検証サーバ２０１から検証結果を受信するのを待つ（ステップＳ１００３：Ｎｏ）。そして、情報処理装置１０１は、検証サーバ２０１から検証結果を受信した場合（ステップＳ１００３：Ｙｅｓ）、偽造・変造検証処理を呼び出したステップに戻る。
【０１６４】
これにより、検証サーバ２０１に公的身分証明書の偽造・変造検証を依頼して、公的身分証明書の正当性を判定することが可能となる。
【０１６５】
（検証サーバ２０１の偽造・変造検証処理手順）
つぎに、図１１を用いて、検証サーバ２０１の偽造・変造検証処理手順について説明する。
【０１６６】
図１１は、検証サーバ２０１の偽造・変造検証処理手順の一例を示すフローチャートである。図１１のフローチャートにおいて、まず、検証サーバ２０１は、情報処理装置１０１から、公開鍵および電子署名が添付された身分証情報を受信したか否かを判断する（ステップＳ１１０１）。
【０１６７】
ここで、検証サーバ２０１は、身分証情報を受信するのを待つ（ステップＳ１１０１：Ｎｏ）。そして、検証サーバ２０１は、身分証情報を受信した場合（ステップＳ１１０１：Ｙｅｓ）、ハッシュ関数を用いて、身分証情報のハッシュ値を生成する（ステップＳ１１０２）。

【０１６８】
つぎに、検証サーバ２０１は、身分証情報に添付された公開鍵を用いて、身分証情報に添付された電子署名を復号する（ステップＳ１１０３）。そして、検証サーバ２０１は、生成した身分証情報のハッシュ値と、電子署名を復号して得られたハッシュ値とを比較する（ステップＳ１１０４）。
【０１６９】
つぎに、検証サーバ２０１は、ハッシュ値が一致するか否かを判断する（ステップＳ１１０５）。ここで、ハッシュ値が一致する場合（ステップＳ１１０５：Ｙｅｓ）、検証サーバ２０１は、公的身分証明書が偽造されていないことを示す検証結果（ＯＫ）を情報処理装置１０１に送信して（ステップＳ１１０６）、本フローチャートによる一連の処理を終了する。
【０１７０】
一方、ハッシュ値が一致しない場合（ステップＳ１１０５：Ｎｏ）、検証サーバ２０１は、公的身分証明書が偽造されていることを示す検証結果（ＮＧ）を情報処理装置１０１に送信して（ステップＳ１１０７）、本フローチャートによる一連の処理を終了する。これにより、公的身分証明書が偽造されているか否かを検証することができる。
【０１７１】
以上説明したように、実施の形態にかかる情報処理装置１０１によれば、ユーザの画像（例えば、顔画像）を含む個人情報を公的身分証明書から読み取り、読み取った個人情報に基づき、公的身分証明書が正当であるか否かを判定することができる。
【０１７２】
これにより、オンラインでの本人確認を行うにあたり、ＰＫＩを利用した公的身分証明書の偽造・変造検証（真贋検証）などを行って、公的身分証明書の正当性を確認することができる。
【０１７３】
また、情報処理装置１０１によれば、公的身分証明書が正当であると判定した場合に、撮影機能を起動して、対象ユーザを含む撮影画像を撮影し、読み取った個人情報に含まれるユーザの画像と、撮影した対象ユーザを含む撮影画像とに基づいて、本人認証の結果を出力することができる。
【０１７４】
これにより、カメラ３０３により撮影された対象ユーザを含む撮影画像を、正当性が確認（保証）された公的身分証明書から読み取られた顔画像と照合して、本人認証を行うことができる。また、本人認証に成功すれば、正当な公的身分証明書から読み取られた顔画像の人物と対象ユーザとが一致するといえるため、本人であることに間違いがないことを確認することができる。
【０１７５】
また、情報処理装置１０１によれば、オンラインでの本人確認を要する取引の開始要求を受け付けたことに応じて、ユーザの画像を含む個人情報を公的身分証明書から読み取ることができる。これにより、金融機関の口座開設やネットショッピングなどの取引を行う際に、オンラインで本人確認を行うことができる。
【０１７６】
また、情報処理装置１０１によれば、公的身分証明書に組み込まれたＩＣチップから、ＮＦＣ等によりユーザの画像を含む個人情報を読み取ることができる。これにより、公的身分証明書の記載内容が書き替えられていたり、顔写真がすり替えられていたりしても、公的身分証明書の正当性を確認することができる。
【０１７７】
また、情報処理装置１０１によれば、本人認証に成功した場合には、本人認証の結果とともに、読み取った個人情報に含まれるユーザの画像を出力することができる。これにより、取引先の事業者などに対して、正当性が確認（保証）された公的身分証明書から読み取られた顔画像を提供することができる。例えば、取引を行うにあたり、事業者がユーザ

の個人情報（顔画像）を要求する場合などに、ユーザが個人情報（顔画像）を手入力するなどの手間を省くことができる。

【０１７８】

また、情報処理装置１０１によれば、公的身分証明書を含む撮影画像を撮影し、撮影した公的身分証明書を含む撮影画像を文字認識処理して、公的身分証明書に記載された個人情報を読み取ることができる。また、情報処理装置１０１によれば、撮影した公的身分証明書を含む撮影画像をトリミング処理して、公的身分証明書に付されたユーザの画像を取得することができる。

【０１７９】

これにより、ＮＦＣ等を利用して個人情報を読み取ることができない場合は、公的身分証明書を含む撮影画像を画像処理して、ユーザの個人情報（氏名、生年月日、住所、顔画像など）を読み取ることができる。

【０１８０】

また、情報処理装置１０１によれば、読み取った個人情報に住所情報が含まれる場合、対象ユーザの現在位置を示す位置情報を取得し、取得した位置情報と、読み取った個人情報に含まれる住所情報との比較結果にさらに基づいて、本人認証の結果を出力することができる。

【０１８１】

これにより、顔照合の結果だけでなく、公的身分証明書の住所付近に対象ユーザが存在するか否かによって、本人認証を行うことができる。例えば、オンラインでの本人確認は、自宅（本籍地）付近で行うという条件を課して、本人確認の精度の向上を図ることができる。

【０１８２】

また、情報処理装置１０１によれば、対象ユーザを撮影する際に、被写体を表示する画面に、顔を位置付けるガイドを表示することができる。これにより、対象ユーザが顔画像を簡単に撮影可能となり、公的身分証明書から読み取られた個人情報に含まれる顔画像と比較する適切な撮影画像を得ることができる。

【０１８３】

また、情報処理装置１０１によれば、公的身分証明書が正当であると判定した場合に、撮影機能を起動して、ユーザを含む動画を撮影し、読み取った個人情報に含まれるユーザの画像と、撮影した動画とに基づいて、本人認証を行うことができる。

【０１８４】

これにより、動画に含まれる任意のフレーム画像を用いて顔照合することが可能となり、画像（静止画）を１枚撮影して本人認証を行う場合に比べて認証精度を高めることができる。例えば、本人であるにもかかわらず、顔の写り方が悪い画像であったために照合率が低くなって認証失敗となるといったことを防ぐことができる。

【０１８５】

また、情報処理装置１０１によれば、撮影した動画から複数のフレーム画像を選択し、選択した複数のフレーム画像それぞれと、個人情報に含まれる顔画像とを照合した結果に基づいて、本人認証を行うことができる。これにより、他人であるにもかかわらず、たまたま照合率が高くなって認証成功となるといったことを防ぐことができる。

【０１８６】

また、情報処理装置１０１によれば、対象ユーザを含む動画を撮影中に、モーション指示を出力し、撮影した動画に基づいて、出力したモーション指示に対応する動作が行われているか否かを判断することができる。そして、情報処理装置１０１によれば、モーション指示に対応する動作が行われていると判断した場合に、個人情報に含まれる顔画像と、撮影した動画とに基づいて、本人認証を行うことができる。

【０１８７】

これにより、被写体が対象ユーザ本人である、すなわち、実物の人間であることを確認した上で、顔照合を行うことができる。このため、例えば、本人ではない第三者が公的身

分証明書に付された顔写真を撮影した撮影画像を使って、顔照合を行うなどの不正行為を防ぐことができる。

【０１８８】

また、情報処理装置１０１によれば、複数のモーション指示の中からランダムに選択したモーション指示を出力することができる。これにより、出力されるモーション指示を予測しにくくして、モーション指示に応じた動画（例えば、隠し撮りした本人の動画）が事前に用意されるのを防ぐことができる。

【０１８９】

これらのことから、情報処理装置１０１によれば、オンラインでの本人確認を実現して、本人確認の手続きにかかる負荷を軽減することができ、ひいては、オンラインでの本人確認を要する取引を円滑に行うことができる。

【０１９０】

例えば、本人限定受取郵便を利用する場合に比べて、煩雑な事務手続きが不要なため、事業者やユーザの手間を削減することができるとともに、郵送が不要なため本人確認に要する時間を短縮することができる。また、オンラインでの本人確認を行うにあたり、事業者側に個人情報を提供しなくてもよいため、事業者側での個人情報の管理負荷を軽減できるとともに、個人情報の漏洩防止を図ることができる。

【０１９１】

なお、本実施の形態で説明した本人確認方法は、予め用意されたプログラムをパーソナル・コンピュータやワークステーション等のコンピュータで実行することにより実現することができる。本人確認プログラムは、ハードディスク、フレキシブルディスク、ＣＤ（Ｃｏｍｐａｃｔ Ｄｉｓｃ）－ＲＯＭ、ＭＯ（Ｍａｇｎｅｔｏ－Ｏｐｔｉｃａｌ ｄｉｓｋ）、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ）、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）メモリ等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。また、本人確認プログラムは、インターネット等のネットワークを介して配布してもよい。

【０１９２】

上述した実施の形態に関し、さらに以下の付記を開示する。

【０１９３】

（付記１）ユーザの画像を含む個人情報を公的身分証明書から読み取り、

読み取った前記個人情報に基づき、前記公的身分証明書が正当であるか否かを判定し、

前記公的身分証明書が正当であると判定した場合に、ユーザを含む撮影画像を撮影し、

読み取った前記個人情報に含まれる前記ユーザの画像と、撮影した前記ユーザを含む撮影画像とに基づいて、本人認証の結果を出力する、

処理をコンピュータに実行させることを特徴とする本人確認プログラム。

【０１９４】

（付記２）前記読み取る処理は、

オンラインでの本人確認を要する取引の開始要求を受け付けたことに応じて、ユーザの画像を含む個人情報を公的身分証明書から読み取る、ことを特徴とする付記１に記載の本人確認プログラム。

【０１９５】

（付記３）前記読み取る処理は、

前記公的身分証明書に組み込まれたＩＣチップからユーザの画像を含む個人情報を読み取る、ことを特徴とする付記１または２に記載の本人確認プログラム。

【０１９６】

（付記４）前記出力する処理は、

本人認証に成功した場合には、本人認証の結果とともに、読み取った前記個人情報に含まれる前記ユーザの画像を出力する、ことを特徴とする付記３に記載の本人確認プログラム。

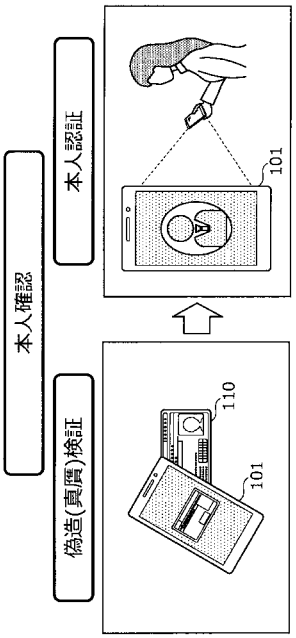
【０１９７】

（付記５）前記公的身分証明書を含む撮影画像を撮影する、処理を前記コンピュータに実行させ、
前記読み取る処理は、
撮影した前記公的身分証明書を含む撮影画像を文字認識処理して、前記公的身分証明書に記載された個人情報を読み取り、
撮影した前記公的身分証明書を含む撮影画像をトリミング処理して、前記公的身分証明書に付されたユーザの画像を取得する、
ことを特徴とする付記１～４のいずれか一つに記載の本人確認プログラム。
【０１９８】
（付記６）読み取った前記個人情報に住所情報が含まれる場合、ユーザの現在位置を示す位置情報を取得する、処理を前記コンピュータに実行させ、
前記出力する処理は、
取得した前記位置情報と前記個人情報に含まれる前記住所情報との比較結果にさらに基づいて、本人認証の結果を出力する、ことを特徴とする付記１～５のいずれか一つに記載の本人確認プログラム。
【０１９９】
（付記７）前記個人情報に含まれる前記ユーザの画像は、顔画像であり、
前記撮影する処理は、
ユーザを撮影する際に、被写体を表示する画面に、顔を位置付けるガイドを表示する、ことを特徴とする付記１～６のいずれか一つに記載の本人確認プログラム。
【０２００】
（付記８）前記公的身分証明書が正当であると判定した場合に、ユーザを含む動画を撮影し、
読み取った前記個人情報に含まれる前記ユーザの画像と、撮影した前記動画とに基づいて、本人認証を行う、
処理を前記コンピュータに実行させることを特徴とする付記１～７のいずれか一つに記載の本人確認プログラム。
【０２０１】
（付記９）前記本人認証を行う処理は、
撮影した前記動画から複数のフレーム画像を選択し、
選択した前記複数のフレーム画像それぞれと、前記個人情報に含まれる前記ユーザの画像とを照合した結果に基づいて、本人認証を行う、
ことを特徴とする付記８に記載の本人確認プログラム。
【０２０２】
（付記１０）ユーザを含む動画を撮影中に、モーション指示を出力し、
撮影した前記動画に基づいて、出力した前記モーション指示に対応する動作が行われているか否かを判断する、処理を前記コンピュータに実行させ、
前記本人認証を行う処理は、
前記モーション指示に対応する動作が行われていると判断した場合に、前記個人情報に含まれる前記ユーザの画像と、撮影した前記動画とに基づいて、本人認証を行う、ことを特徴とする付記８または９に記載の本人確認プログラム。
【０２０３】
（付記１１）前記モーション指示を出力する処理は、
複数のモーション指示の中からランダムに選択したモーション指示を出力する、ことを特徴とする付記１０に記載の本人確認プログラム。
【０２０４】
（付記１２）前記ユーザを含む撮影画像を撮影する処理は、
前記公的身分証明書が正当であると判定した場合に、撮影機能を起動して、ユーザを含む撮影画像を撮影する、ことを特徴とする付記１～１１のいずれか一つに記載の本人確認プログラム。

【０２０５】
（付記１３）ユーザの画像を含む個人情報を公的身分証明書から読み取り、
読み取った前記個人情報に基づき、前記公的身分証明書が正当であるか否かを判定し、
前記公的身分証明書が正当であると判定した場合に、ユーザを含む撮影画像を撮影し、
読み取った前記個人情報に含まれる前記ユーザの画像と、撮影した前記ユーザを含む撮影画像とに基づいて、本人認証の結果を出力する、
処理をコンピュータが実行することを特徴とする本人確認方法。
【０２０６】
（付記１４）被写体を撮影するカメラと、
ユーザの画像を含む個人情報を公的身分証明書から読み取る読取部と、
前記読取部が読み取った前記個人情報に基づき、前記公的身分証明書が正当であるか否かを判定する判定部と、
前記判定部が前記公的身分証明書が正当であると判定した場合に、前記カメラにより、ユーザを含む撮影画像を撮影する撮影制御部と、
前記個人情報に含まれる前記ユーザの画像と、前記撮影制御部が撮影した前記ユーザを含む撮影画像とに基づいて、本人認証の結果を出力する出力部と、
を有することを特徴とする情報処理装置。
【符号の説明】
【０２０７】
１０１　情報処理装置
１１０　公的身分証明書
２００　本人確認システム
２０１　検証サーバ
２０２　照合サーバ
２０３　事業者サーバ
２１０　ネットワーク
３００　バス
３０１　ＣＰＵ
３０２　メモリ
３０３　カメラ
３０４　通信Ｉ／Ｆ
３０５　ディスプレイ
３０６　入力装置
３０７　読取装置
３０８　ＧＰＳユニット
４０１　受付部
４０２　読取部
４０３　判定部
４０４　撮影制御部
４０５　認証部
４０６　出力部

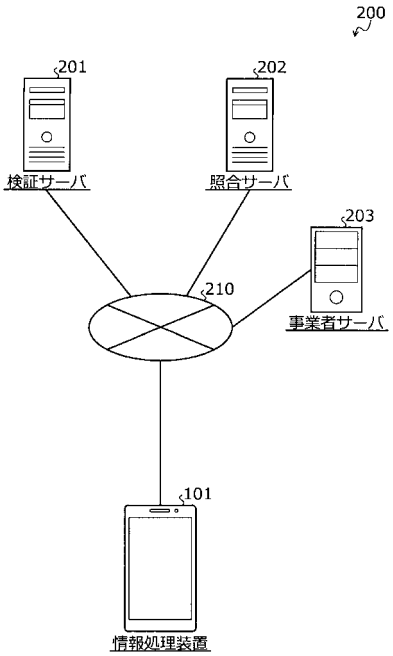
【図１】

実施の形態にかかる本人確認方法の一実施例を示す説明図



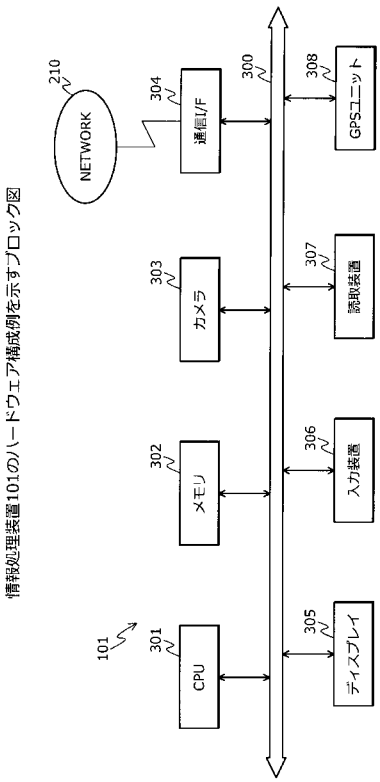
【図２】

本人確認システム200のシステム構成例を示す説明図



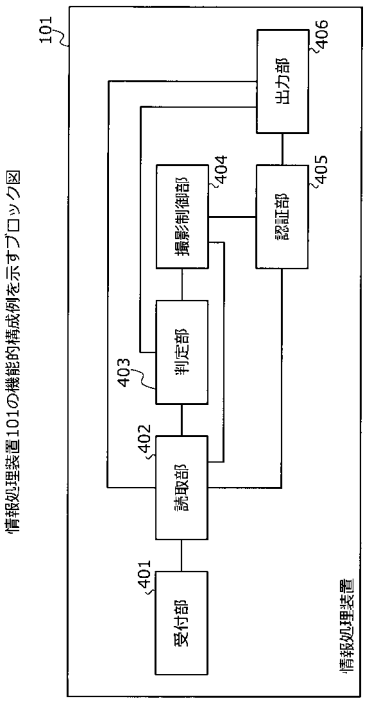
【図３】

情報処理装置101のハードウェア構成例を示すブロック図

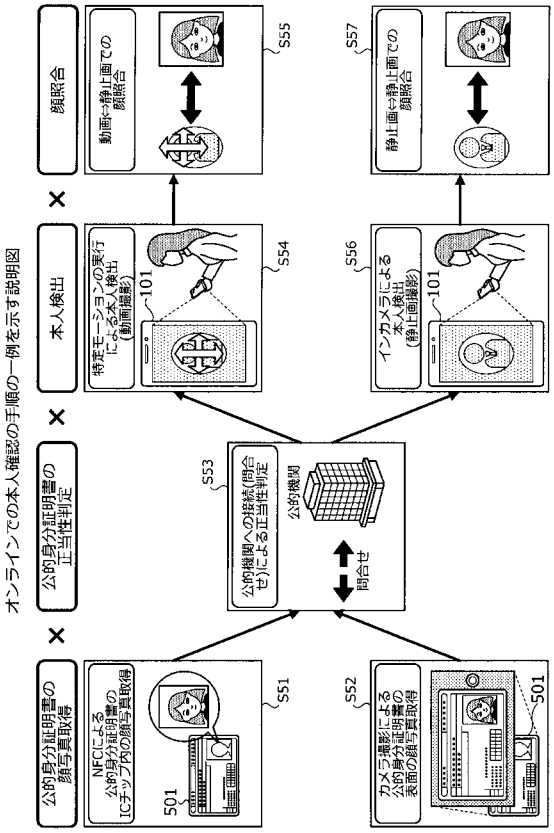


【図４】

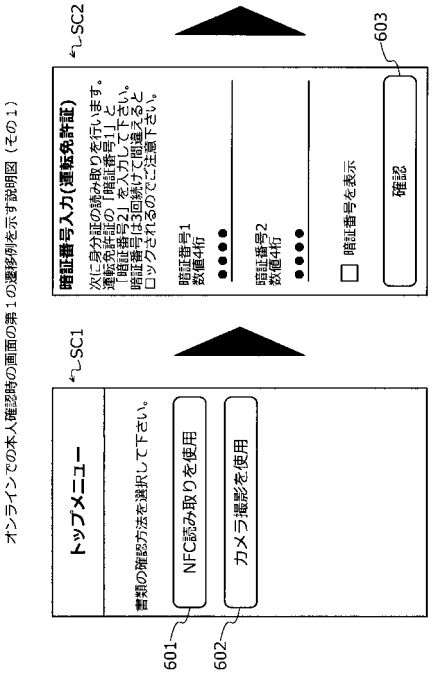
情報処理装置101の機能的構成例を示すブロック図



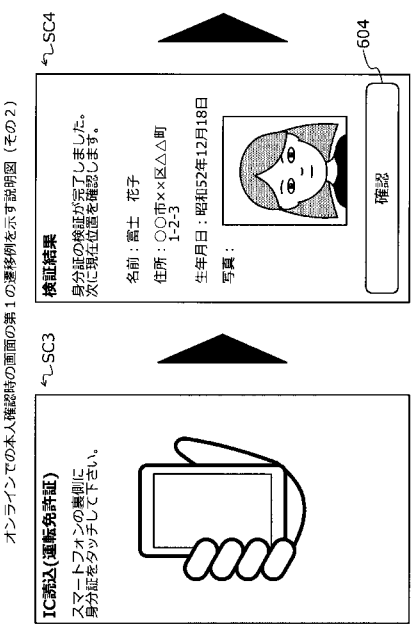
【図５】



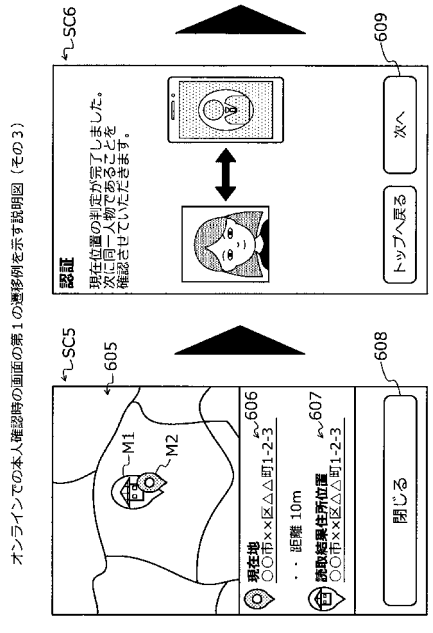
【図６Ａ】



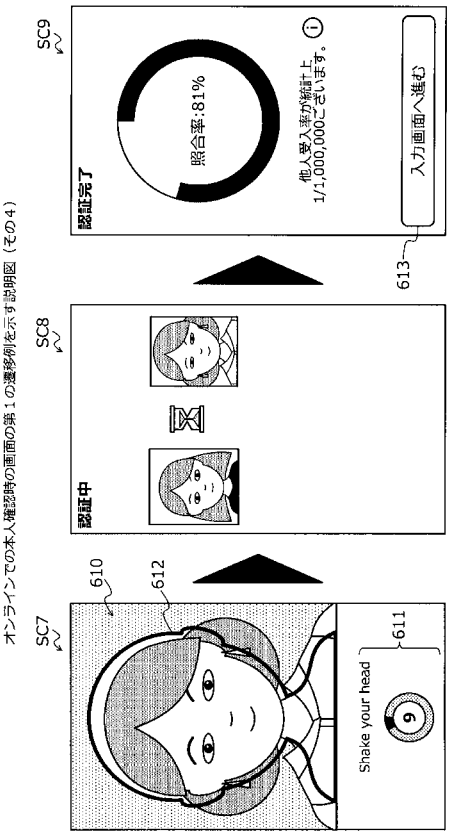
【図６Ｂ】



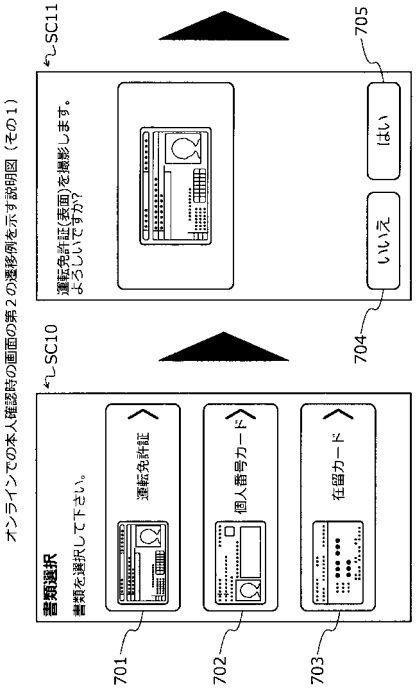
【図６Ｃ】



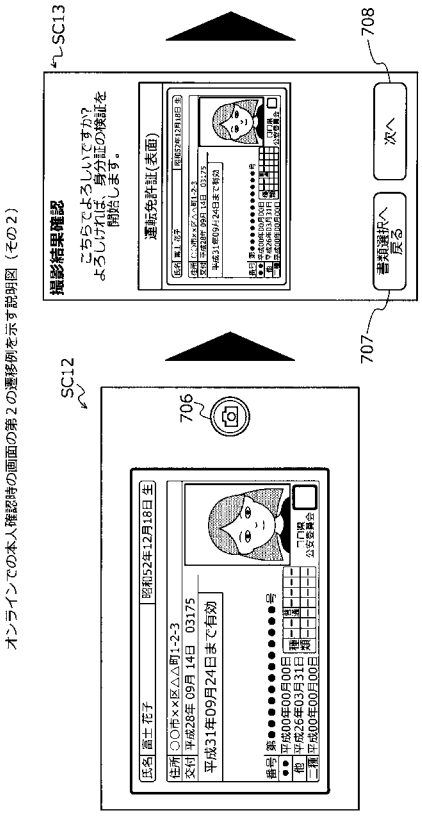
【図６Ｄ】



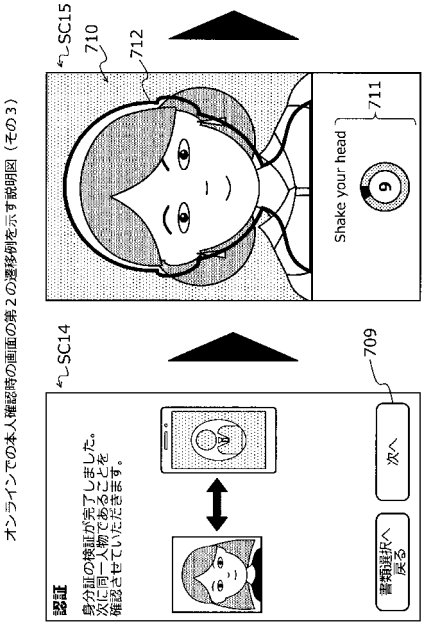
【図７Ａ】



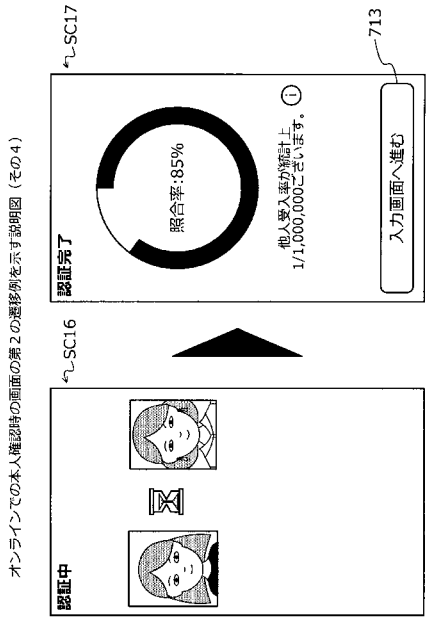
【図７Ｂ】



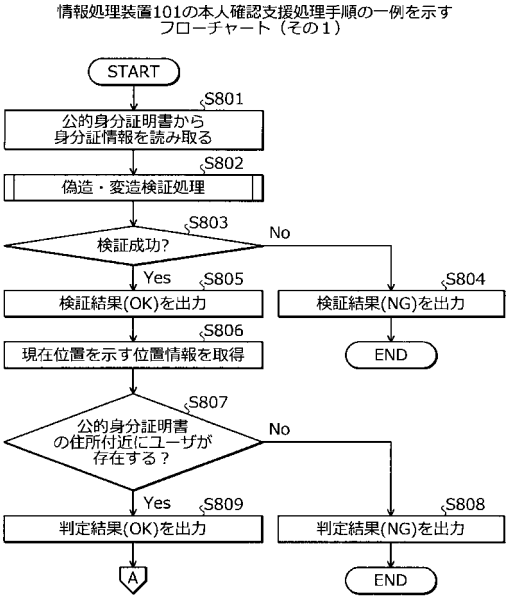
【図７Ｃ】



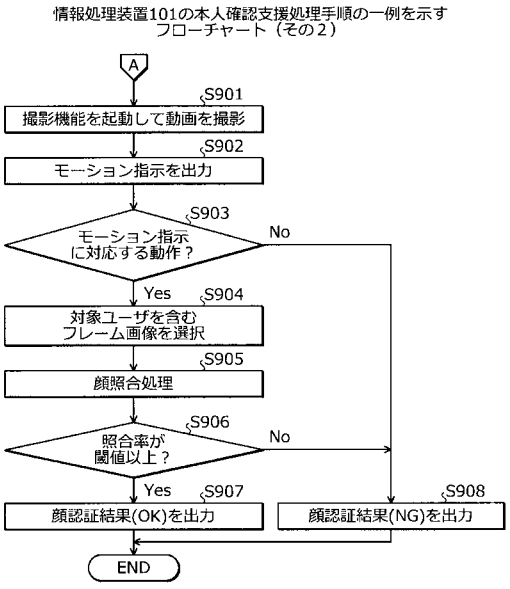
【図７Ｄ】


オンラインでの本人確認時の画面の第２の遷移例を示す説明図（その４）
SC17
713
認証完了
照合率:85%
他人受入率が約1/1,000,000ございます。
入力画面へ進む
SC16
認証中

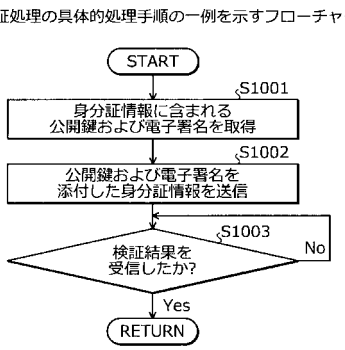
【図８】


情報処理装置101の本人確認支援処理手順の一例を示す
フローチャート（その１）
START
S801
公的身分証明書から
身分証情報を読み取る
S802
偽造・変造検証処理
S803
検証成功?
No
Yes
S805
検証結果(OK)を出力
S804
検証結果(NG)を出力
END
S806
現在位置を示す位置情報を取得
S807
公的身分証明書
の住所付近にユーザが
存在する？
No
Yes
S809
判定結果(OK)を出力
S808
判定結果(NG)を出力
A
END

【図９】


情報処理装置101の本人確認支援処理手順の一例を示す
フローチャート（その２）
A
S901
撮影機能を起動して動画を撮影
S902
モーション指示を出力
S903
モーション指示
に対応する動作？
No
Yes
S904
対象ユーザを含む
フレーム画像を選択
S905
顔照合処理
S906
照合率が
閾値以上？
No
Yes
S907
顔認証結果(OK)を出力
S908
顔認証結果(NG)を出力
END

【図１０】


偽造・変造検証処理の具体的処理手順の一例を示すフローチャート
START
S1001
身分証情報に含まれる
公開鍵および電子署名を取得
S1002
公開鍵および電子署名を
添付した身分証情報を送信
S1003
検証結果を
受信したか?
No
Yes
RETURN

【図１１】

検証サーバ201の偽造・変造検証処理手順の一例を示すフローチャート