(19)日本国特許庁(JP)　　(12)公開特許公報(A)　　(11)公開番号
特開2022-103695
(P2022-103695A)
(43)公開日　令和4年7月8日(2022.7.8)

(51)国際特許分類　　FI
G06F 21/31 (2013.01)　　G06F 21/31
G06F 21/62 (2013.01)　　G06F 21/62

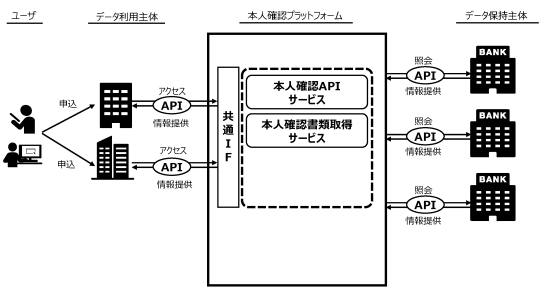
審査請求　未請求　請求項の数　18　　ＯＬ　（全24頁）

(21)出願番号　特願2020-218482(P2020-218482)
(22)出願日　令和2年12月28日(2020.12.28)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100110928
弁理士　速水 進治
(72)発明者　矢澤 賢一郎
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　鈴木 遼一
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　竹内 鉄兵
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　猪股 知仁
最終頁に続く

(54)【発明の名称】　本人確認情報利用システム、管理装置、本人確認情報利用方法、管理方法及びプログラム

(57)【要約】
【課題】あるサービスの利用を開始する際に必要となる本人確認の作業を効率化する。
【解決手段】本発明の本人確認情報利用システムは、データ保持主体が保持する本人確認情報がデータ利用主体に提供される前に、その本人確認情報をユーザに提示し、内容の確認を促すステップを実行する。そして、ユーザにより確認された本人確認情報がデータ利用主体に提供される。このような本人確認情報利用システムによれば、古い内容のまま放置された本人確認情報がデータ利用主体に提供される不都合を効果的に抑制することができる。
【選択図】図１



【特許請求の範囲】
【請求項１】
複数のユーザの本人確認情報を記憶するデータ保持主体の装置と、前記データ保持主体の装置とデータ利用主体の装置との間で行われる前記本人確認情報の受け渡しを管理する管理装置とを有し、
前記データ保持主体の装置は、
前記管理装置から送信された遷移情報に基づきログイン画面に遷移してきたエンドユーザの端末と通信し、ログイン情報の受信及び前記ログイン情報に基づく認証処理を行う認証手段と、
前記認証処理で認証に成功した場合、ログインしたユーザの前記本人確認情報を記憶手段から読み出し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促す確認手段と、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記管理装置に送信する本人確認情報送信手段と、
を有し、
前記管理装置は、
前記データ保持主体の装置から受信した前記本人確認情報を、前記データ利用主体の装置に送信する中継手段を有する本人確認情報利用システム。
【請求項２】
前記確認手段は、前記本人確認情報が表示されるとともに、前記本人確認情報の一部が隠された情報確認画面を前記エンドユーザの端末に表示させる請求項１に記載の本人確認情報利用システム。
【請求項３】
前記確認手段は、前記エンドユーザの端末に出力された前記本人確認情報の変更を受付け、
前記本人確認情報送信手段は、前記確認手段により前記本人確認情報の変更が受付けられた場合、変更後の前記本人確認情報を前記管理装置に送信する請求項１又は２に記載の本人確認情報利用システム。
【請求項４】
前記管理装置は、
前記データ保持主体の装置から受信した前記本人確認情報を自装置の不揮発性記憶装置に保存せず、前記データ保持主体の装置と前記データ利用主体の装置との間の中継を行う請求項１から３のいずれか１項に記載の本人確認情報利用システム。
【請求項５】
前記管理装置は、
前記本人確認情報を提供可能な前記データ保持主体の一覧を示す一覧情報を前記データ利用主体の装置に送信する一覧情報送信手段と、
前記一覧情報で示される一覧の中から選択された前記データ保持主体を示す選択情報を前記データ利用主体の装置から受信すると、選択された前記データ保持主体の装置にログインするための前記ログイン画面に前記エンドユーザの端末を遷移させるための前記遷移情報を出力する遷移情報送信手段と、
を有する請求項１から４のいずれか１項に記載の本人確認情報利用システム。
【請求項６】
前記遷移情報送信手段は、複数の前記データ保持主体が選択されたことを示す前記選択情報を受信すると、選択された複数の前記データ保持主体の装置各々にログインするための複数の前記ログイン画面に前記エンドユーザの端末を遷移させるための複数の前記遷移情報を出力し、
前記管理装置は、
複数の前記データ保持主体の装置各々から前記本人確認情報を受信した場合、複数の前記本人確認情報が互いに一致するか否か判定する判定手段をさらに有する請求項５に記載の

本人確認情報利用システム。
【請求項７】
前記判定手段は、
複数の前記本人確認情報が互いに一致しない場合、複数の前記本人確認情報の中から信頼度が最も高いものを決定し、決定した前記本人確認情報を前記データ利用主体の装置に送信させる請求項６に記載の本人確認情報利用システム。
【請求項８】
前記判定手段は、
複数の前記本人確認情報が互いに一致しない場合、複数の前記本人確認情報の送信元である複数の前記データ保持主体の装置にその旨を通知する請求項６又は７に記載の本人確認情報利用システム。
【請求項９】
データ保持主体の装置にログインするためのログイン画面にエンドユーザの端末を遷移させるための遷移情報を出力する遷移情報送信手段と、
前記遷移情報に基づき前記ログイン画面に遷移してきた前記エンドユーザの端末が前記ログイン画面を介して前記データ保持主体の装置へのログインに成功した場合、ログインしたユーザの前記本人確認情報を前記データ保持主体の装置から受信し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促す確認手段と、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記データ利用主体の装置に送信する中継手段と、
を有する管理装置。
【請求項１０】
前記確認手段は、前記本人確認情報が表示されるとともに、前記本人確認情報の一部が隠された情報確認画面を前記エンドユーザの端末に表示させる請求項９に記載の管理装置。
【請求項１１】
前記データ保持主体の装置から受信した前記本人確認情報を自装置の不揮発性記憶装置に保存せず、前記データ保持主体の装置と前記データ利用主体の装置との間の中継を行う請求項９又は１０に記載の管理装置。
【請求項１２】
本人確認情報を提供可能なデータ保持主体の一覧を示す一覧情報をデータ利用主体の装置に送信する一覧情報送信手段をさらに有し、
前記遷移情報送信手段は、
前記一覧情報で示される一覧の中から選択された前記データ保持主体を示す選択情報を前記データ利用主体の装置から受信すると、選択された前記データ保持主体の装置にログインするための前記ログイン画面に前記エンドユーザの端末を遷移させるための前記遷移情報を出力する請求項９から１１のいずれか１項に記載の管理装置。
【請求項１３】
前記遷移情報送信手段は、複数の前記データ保持主体が選択されたことを示す前記選択情報を受信すると、選択された複数の前記データ保持主体の装置各々にログインするための複数の前記ログイン画面に前記エンドユーザの端末を遷移させるための複数の前記遷移情報を出力し、
前記確認手段は、前記エンドユーザの端末が複数の前記ログイン画面各々を介して複数の前記データ保持主体の装置各々へのログインに成功した場合、ログインしたユーザの前記本人確認情報を複数の前記データ保持主体の装置各々から受信し、前記エンドユーザの端末に出力して、複数の前記データ保持主体の装置各々から受信した複数の前記本人確認情報の確認を促し、
複数の前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された複数の前記本人確認情報が互いに一致するか否か判定する判定手段をさらに有する請求項１２に記載の管理装置。
【請求項１４】

前記判定手段は、
複数の前記本人確認情報が互いに一致しない場合、複数の前記本人確認情報の中から信頼度が最も高いものを決定し、決定した前記本人確認情報を前記データ利用主体の装置に送信させる請求項１３に記載の管理装置。
【請求項１５】
前記判定手段は、
複数の前記本人確認情報が互いに一致しない場合、複数の前記本人確認情報の送信元である複数の前記データ保持主体の装置にその旨を通知する請求項１３又は１４に記載の管理装置。
【請求項１６】
複数のユーザの本人確認情報を記憶するデータ保持主体の装置と、前記データ保持主体の装置とデータ利用主体の装置との間で行われる前記本人確認情報の受け渡しを管理する管理装置とを有する本人確認情報利用システムにより実行され、
前記データ保持主体の装置は、
前記管理装置から送信された遷移情報に基づきログイン画面に遷移してきたエンドユーザの端末と通信し、ログイン情報の受信及び前記ログイン情報に基づく認証処理を行い、
前記認証処理で認証に成功した場合、ログインしたユーザの前記本人確認情報を記憶手段から読み出し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促し、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記管理装置に送信し、
前記管理装置は、
前記データ保持主体の装置から受信した前記本人確認情報を、前記データ利用主体の装置に送信する本人確認情報利用方法。
【請求項１７】
コンピュータが、
データ保持主体の装置にログインするためのログイン画面にエンドユーザの端末を遷移させるための遷移情報を出力し、
前記遷移情報に基づき前記ログイン画面に遷移してきた前記エンドユーザの端末が前記ログイン画面を介して前記データ保持主体の装置へのログインに成功した場合、ログインしたユーザの前記本人確認情報を前記データ保持主体の装置から受信し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促し、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記データ利用主体の装置に送信する管理方法。
【請求項１８】
コンピュータを、
データ保持主体の装置にログインするためのログイン画面にエンドユーザの端末を遷移させるための遷移情報を出力する遷移情報送信手段、
前記遷移情報に基づき前記ログイン画面に遷移してきた前記エンドユーザの端末が前記ログイン画面を介して前記データ保持主体の装置へのログインに成功した場合、ログインしたユーザの前記本人確認情報を前記データ保持主体の装置から受信し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促す確認手段、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記データ利用主体の装置に送信する中継手段、
として機能させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、本人確認情報利用システム、管理装置、本人確認情報利用方法、管理方法及びプログラムに関する。
【背景技術】

【０００２】
所定の事業者が提供する所定のサービスの利用を開始する際には、本人確認が必要となる場合がある。例えば、銀行、証券会社等で口座を開設する際等が例示される。
【０００３】
非特許文献１は、本人確認の作業をオンラインで効率的に行う技術を開示している。当該技術では、ある銀行の口座を保有しているユーザがある証券会社で口座を開設する際の本人確認を、その銀行で管理されている本人確認情報と、ユーザより提示された本人確認情報との照合で実現する。
【０００４】
関連する技術が、特許文献１に開示されている。特許文献１は、身元確認依頼サーバと、身元確認基盤サーバと、複数の携帯端末通信事業者の身元保証サーバとを有する身元確認システムを開示している。
【０００５】
身元確認依頼サーバは、ユーザ端末からのリクエストを受け付けて、身元確認基盤サーバに当該ユーザ端末のユーザの身元確認依頼を送信する。そして、身元確認依頼サーバは、身元保証サーバが行った認証結果のアドレス情報を受信し、当該アドレス情報を用いて認証結果を取得する。
【０００６】
身元確認基盤サーバは、いずれかの身元保証サーバの選択指示をユーザ端末から受け付ける。そして、身元確認基盤サーバは、選択指示で選択された身元保証サーバからのリクエストに基づいて、第１のパスワードを生成し、生成した第１のパスワードを携帯端末に送信するとともに、ユーザ端末から入力された第２のパスワードと第１のパスワードが一致するか否かを認証する。
【０００７】
身元保証サーバは、通信サービスを提供する各携帯端末のユーザのユーザ情報を記憶している。そして、身元保証サーバは、第１のパスワードと第２のパスワードとが一致する場合、ユーザ端末から入力されたユーザ情報を、上記記憶するユーザ情報を参照して認証し、認証結果を身元確認結果として記憶する。そして、身元保証サーバは、記憶された認証結果のアドレス情報を、身元確認基盤サーバを介して身元確認依頼サーバに送信する。
【先行技術文献】
【特許文献】
【０００８】
【特許文献１】特開２０１２－２０８８５６号公報
【非特許文献】
【０００９】
【非特許文献１】"本人確認サポート（個人）ＡＰＩサービスとそのユースケースのご紹介"、［online］、２０１９年７月１１日、三菱ＵＦＪ銀行、［２０２０年１１月２０日検索］、インターネット＜https://developer.portal.bk.mufg.jp/node/3874＞
【発明の概要】
【発明が解決しようとする課題】
【００１０】
非特許文献１の技術を利用することで、本人確認の作業が効率化する。しかし、本発明者らは、以下の課題を見出した。
【００１１】
各ユーザの本人確認情報は不変でなく、引っ越し、転職、電話番号の変更等の各種要因に起因して変化し得る。そして、銀行等に登録されている本人確認情報が更新されず、古い内容のまま放置される場合がある。例えば証券会社の口座開設時の本人確認においてこのような古い内容のまま放置された本人確認情報を利用し、ユーザより提示された本人確認情報と照合すると、当然エラーが発生する。非特許文献１の技術で実現される本人確認の仕組みをよく理解していないユーザは、なぜエラーになったのか理解できず、解決手段が

見いだせない。結果、本人確認の作業に要する時間や労力が多大になってしまう。なお、ここでは話を理解しやすくするため銀行及び証券会社の例に基づき説明したが、本発明の課題はこれらの分野に限定されるものではない。

【００１２】

本発明は、あるサービスの利用を開始する際に必要となる本人確認の作業を効率化することを課題とする。

【課題を解決するための手段】

【００１３】

本発明によれば、

複数のユーザの本人確認情報を記憶するデータ保持主体の装置と、前記データ保持主体の装置とデータ利用主体の装置との間で行われる前記本人確認情報の受け渡しを管理する管理装置とを有し、

前記データ保持主体の装置は、

前記管理装置から送信された遷移情報に基づきログイン画面に遷移してきたエンドユーザの端末と通信し、ログイン情報の受信及び前記ログイン情報に基づく認証処理を行う認証手段と、

前記認証処理で認証に成功した場合、ログインしたユーザの前記本人確認情報を記憶手段から読み出し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促す確認手段と、

前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記管理装置に送信する本人確認情報送信手段と、

を有し、

前記管理装置は、

前記データ保持主体の装置から受信した前記本人確認情報を、前記データ利用主体の装置に送信する中継手段を有する本人確認情報利用システムが提供される。

【００１４】

また、本発明によれば、

データ保持主体の装置にログインするためのログイン画面にエンドユーザの端末を遷移させるための遷移情報を出力する遷移情報送信手段と、

前記遷移情報に基づき前記ログイン画面に遷移してきた前記エンドユーザの端末が前記ログイン画面を介して前記データ保持主体の装置へのログインに成功した場合、ログインしたユーザの前記本人確認情報を前記データ保持主体の装置から受信し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促す確認手段と、

前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記データ利用主体の装置に送信する中継手段と、

を有する管理装置が提供される。

【００１５】

また、本発明によれば、

複数のユーザの本人確認情報を記憶するデータ保持主体の装置と、前記データ保持主体の装置とデータ利用主体の装置との間で行われる前記本人確認情報の受け渡しを管理する管理装置とを有する本人確認情報利用システムにより実行され、

前記データ保持主体の装置は、

前記管理装置から送信された遷移情報に基づきログイン画面に遷移してきたエンドユーザの端末と通信し、ログイン情報の受信及び前記ログイン情報に基づく認証処理を行い、

前記認証処理で認証に成功した場合、ログインしたユーザの前記本人確認情報を記憶手段から読み出し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促し、

前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記管理装置に送信し、

前記管理装置は、

前記データ保持主体の装置から受信した前記本人確認情報を、前記データ利用主体の装置

に送信する本人確認情報利用方法が提供される。
【００１６】
また、本発明によれば、
コンピュータが、
データ保持主体の装置にログインするためのログイン画面にエンドユーザの端末を遷移させるための遷移情報を出力し、
前記遷移情報に基づき前記ログイン画面に遷移してきた前記エンドユーザの端末が前記ログイン画面を介して前記データ保持主体の装置へのログインに成功した場合、ログインしたユーザの前記本人確認情報を前記データ保持主体の装置から受信し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促し、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記データ利用主体の装置に送信する管理方法が提供される。
【００１７】
また、本発明によれば、
コンピュータを、
データ保持主体の装置にログインするためのログイン画面にエンドユーザの端末を遷移させるための遷移情報を出力する遷移情報送信手段、
前記遷移情報に基づき前記ログイン画面に遷移してきた前記エンドユーザの端末が前記ログイン画面を介して前記データ保持主体の装置へのログインに成功した場合、ログインしたユーザの前記本人確認情報を前記データ保持主体の装置から受信し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促す確認手段、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記データ利用主体の装置に送信する中継手段、
として機能させるプログラムが提供される。
【発明の効果】
【００１８】
本発明によれば、あるサービスの利用を開始する際に必要となる本人確認の作業が効率化する。
【図面の簡単な説明】
【００１９】
【図１】本実施形態の本人確認情報利用システムの概要を説明するための図である。
【図２】本実施形態の本人確認情報利用システムの処理の流れの一例を説明するための図である。
【図３】本実施形態の本人確認情報利用システムで実現される画面遷移の一例を説明するための図である。
【図４】本実施形態の管理装置の機能ブロック図の一例である。
【図５】本実施形態のデータ保持主体の装置の機能ブロック図の一例である。
【図６】本実施形態の装置のハードウエア構成の一例を示す図である。
【図７】本実施形態の管理装置の機能ブロック図の一例である。
【図８】本実施形態の本人確認情報利用システムの処理の流れの一例を説明するための図である。
【図９】本実施形態のデータ保持主体の装置の機能ブロック図の一例である。
【図１０】本実施形態の管理装置の機能ブロック図の一例である。
【図１１】本実施形態の管理装置の機能ブロック図の一例である。
【発明を実施するための形態】
【００２０】
以下、本発明の実施の形態について、図面を用いて説明する。尚、すべての図面において、同様な構成要素には同様の符号を付し、適宜説明を省略する。
【００２１】

＜第１の実施形態＞
「概要」
まず、図１を用いて、本実施形態の本人確認情報利用システムの概要を説明する。
【００２２】
図示するデータ利用主体及びデータ保持主体は、利用開始時に本人確認が必要となるサービスを提供する主体である。データ利用主体及びデータ保持主体は、例えば銀行、証券会社等であり、利用開始時に本人確認が必要となるサービスは例えば口座開設等である。なお、ここでの例示はあくまで一例であり、これらに限定されない。
【００２３】
本人確認プラットフォームは、データ利用主体とデータ保持主体との間で行われる本人確認情報の受け渡しを管理する。データ利用主体の装置と本人確認プラットフォームは、例えば所定のＡＰＩを介してデータ連携を行うことができる。また、データ保持主体の装置と本人確認プラットフォームは、例えば所定のＡＰＩを介してデータ連携を行うことができる。
【００２４】
本実施形態の本人確認情報利用システムは、データ保持主体が保持する本人確認情報がデータ利用主体に提供される前に、その本人確認情報をユーザに提示し、内容の確認を促すステップを実行する。そして、ユーザにより確認された本人確認情報がデータ利用主体に提供される。
【００２５】
このような本人確認情報利用システムによれば、古い内容のまま放置された本人確認情報がデータ利用主体に提供される不都合を効果的に抑制することができる。これにより、古い内容の本人確認情報が送受信されることにより生じる不都合（ユーザより提示された本人確認情報との照合におけるエラー等）を抑制できる。結果、あるサービスの利用を開始する際に必要となる本人確認の作業が効率化する。
【００２６】
「本人確認情報利用システムの機能構成」
次に、図２を用いて、本実施形態の本人確認情報利用システムの構成を詳細に説明する。
管理装置１０は、図１で示した本人確認プラットフォームに対応する。データ保持主体の装置２０は、図１で示したデータ保持主体が管理・使用する装置である。データ利用主体の装置３０は、図１で示したデータ利用主体が管理・使用する装置である。エンドユーザの端末４０は、図１で示したユーザが管理・使用する装置であり、スマートフォン、タブレット端末、パーソナルコンピュータ、スマートウォッチ、携帯電話等が例示される。
【００２７】
まず、（１）として示すように、エンドユーザの端末４０とデータ利用主体の装置３０が通信し、エンドユーザの端末４０からデータ利用主体の装置３０にサービス開始申し込みが送信される。当該送信を実現する一例として、ウェブページやアプリケーションを介した処理が例示されるが、これらに限定されない。
【００２８】
図３に、エンドユーザの端末４０に表示される画面の一例を示す。図３の（１）乃至（８）、（１１）は、データ利用主体の装置３０から提示された画面であり、図３の（９）及び（１０）は、データ保持主体の装置２０から提示された画面である。なお、図３の画面はあくまで一例であり、各画面で表示される内容、各画面の表示順、各画面を表示するか否か等は、本発明の作用効果を実現できる範囲内で変更可能である。
【００２９】
当該図においては、データ利用主体及びデータ保持主体は銀行、証券会社等であり、利用開始時に本人確認が必要となるサービスは口座開設であることを前提とする。図３の（１）の画面において口座開設のボタンが操作されると、サービス開始申し込みがエンドユーザの端末４０からデータ利用主体の装置３０に送信される。
【００３０】

次に、図２の（２）として示すように、サービス開始申し込みを受け付けたデータ利用主体の装置３０は、本人確認情報を提供可能なデータ保持主体の装置２０の一覧のリクエストを管理装置１０に送信する。

【００３１】

例えば、図３の（６）に示すような本人確認方法を選択する画面において「データ保持主体の装置２０が保持する本人確認情報を利用した本人確認」をユーザが選択（図中、銀行ＡＰＩ連携のボタンを操作）し、その後、図３の（７）に示すような利用規約にユーザが同意（図中、許諾のボタンを操作）したことに応じて、データ利用主体の装置３０は上記リクエストを管理装置１０に送信してもよい。なお、一例として、図３の（６）及び（７）の画面は、図３の（２）乃至（５）の画面で各種手続きが行われた後に表示される。

【００３２】

次に、図２の（３）として示すように、管理装置１０は、本人確認情報を提供可能なデータ保持主体の装置２０の一覧をデータ利用主体の装置３０に送信する。

【００３３】

例えば、予め、本人確認情報の送受信が可能な主体の組み合わせが決まっており（銀行Ａと銀行Ｂとの間では本人確認情報の送受信が可、銀行Ａと銀行Ｃとの間では本人確認情報の送受信が不可等）、その組み合わせを示す組み合わせ情報が管理装置１０に登録されている。そして、管理装置１０は、当該組み合わせ情報に基づき、（２）のリクエストを送信してきたデータ利用主体の装置３０に本人確認情報を提供可能なデータ保持主体の装置２０を特定し、その一覧をデータ利用主体の装置３０に送信する。

【００３４】

次に、図２の（４）として示すように、データ利用主体の装置３０は、本人確認情報を提供可能なデータ保持主体の一覧をエンドユーザの端末４０に送信する。結果、図３の（８）に示すように、エンドユーザの端末４０に、本人確認情報を提供可能なデータ保持主体の一覧が表示される。

【００３５】

次に、エンドユーザの端末４０は、上記一覧の中から１つを選択するユーザ入力を受付ける。なお、以下の実施形態で、ここで２つ以上を選択できる例を説明する。ユーザは、一覧の中から、自身の本人確認情報が登録されている主体（例：口座を既に有する銀行等）を選択する。すると、図２の（５）として示すように、選択内容を示す情報が、エンドユーザの端末４０からデータ利用主体の装置３０に送信される。

【００３６】

次に、図２の（６）として示すように、データ利用主体の装置３０は、図２の（５）で受信した選択内容を示す情報を管理装置１０に送信する。

【００３７】

次に、図２の（７）として示すように、管理装置１０は、選択されたデータ保持主体の装置２０にログインするためのログイン画面にエンドユーザの端末４０を遷移（リダイレクト）させるための遷移情報をデータ利用主体の装置３０に送信する。次に、図２の（８）として示すように、データ利用主体の装置３０は、図２の（７）で受信した遷移情報をエンドユーザの端末４０に送信する。エンドユーザの端末４０は、受信した遷移情報に基づき、データ保持主体の装置２０にログインするためのログイン画面に遷移する。結果、図３の（９）に示すように、エンドユーザの端末４０に、データ保持主体の装置２０のログイン画面が表示される。なお、ここでは、エンドユーザの端末４０を選択されたデータ保持主体の装置２０のログイン画面にリダイレクトできればよく、その実現手段はここで例示したものに限定されない。

【００３８】

次に、図２の（９）として示すように、エンドユーザの端末４０は、ユーザが入力したログイン情報（ＩＤ（identifier）、パスワード等）をデータ保持主体の装置２０に送信する。

【００３９】

次に、ログインに成功した場合、図２の（１０）として示すように、データ保持主体の装置２０は、データ保持主体の装置２０に記憶されているそのユーザの本人確認情報を読み出し、エンドユーザの端末４０に出力して、本人確認情報の確認を促す。

【００４０】

例えば、図３の（１０）に示すような情報確認画面がエンドユーザの端末４０に表示される。なお、当該情報確認画面において、本人確認情報の一部が隠されてもよい。例えば、「日本太●、東京都●●区・・・」等のように、文字の一部が伏字になっていてもよい。これにより、当該情報を盗み見られたり、不正に取得されたりする不都合を抑制できる。

【００４１】

また、当該情報確認画面において、本人確認情報の内容が現在の内容と異なる場合、変更を促す旨がユーザに通知されてもよい。そして、当該情報確認画面において、本人確認情報の変更ができてもよい。すなわち、表示された情報確認情報が古い内容のままであった場合、ユーザは、当該情報確認画面から本人確認情報を変更する操作を行うことができてもよい。データ保持主体の装置２０は、当該情報確認画面から本人確認情報を変更する操作を受付けると、入力内容に基づき、自装置に記憶されているそのユーザの本人確認情報を更新する。そして、データ保持主体の装置２０は、変更後の本人確認情報をエンドユーザの端末４０に出力して、本人確認情報の確認を促す。

【００４２】

次に、本人確認情報が正しいことがユーザにより確認された場合（図３の（１０）の確認ボタンに対する操作がなされた場合）、図２の（１１）として示すように、エンドユーザの端末４０はその旨を示す入力情報をデータ保持主体の装置２０に送信する。

【００４３】

その後、図２の（１２）として示すように、データ保持主体の装置２０は、本人認証済通知を管理装置１０に送信する。そして、管理装置１０は、図２の（１３）として示すように、その本人認証済通知をエンドユーザの端末４０に送信する。

【００４４】

その後、図２の（１４）として示すように、エンドユーザの端末４０は、データ利用主体の装置３０に本人情報取得要求を送信する。次いで、データ利用主体の装置３０は、図２の（１５）として示すように、受信した本人情報取得要求を管理装置１０に送信する。そして、管理装置１０は、図２の（１６）として示すように、本人確認情報のリクエストをデータ保持主体の装置２０に送信する。

【００４５】

データ保持主体の装置２０は、管理装置１０からの本人確認情報のリクエストを受信すると、図２の（１７）として示すように、ユーザにより確認された本人確認情報を管理装置１０に送信する。なお、情報確認画面において本人確認情報が変更された場合、データ保持主体の装置２０は、変更後の本人確認情報を管理装置１０に送信する。

【００４６】

次に、図２の（１８）として示すように、管理装置１０は、受信した本人確認情報をデータ利用主体の装置３０に送信する。管理装置１０は、受信した本人確認情報を自装置の不揮発性記憶装置に保存せず、単にデータ保持主体の装置２０とデータ利用主体の装置３０との間の中継だけを行うことが好ましい。本人確認情報を不要に多くの場所に記憶させることを回避することで、本人確認情報が漏洩したり、不正に取得されたりする不都合を抑制できる。また、データ保持主体は、安心して、自身が管理している本人確認情報を外部に提供できる。また、管理装置１０は、データ保持主体の装置２０から受信した本人確認情報のフォーマットを統一フォーマットに変換した後、フォーマット変換後の本人確認情報をデータ利用主体の装置３０に送信してもよい。統一フォーマットの詳細は特段制限されない。例えば生年月日の統一フォーマットは「ＹＹＹＹ－ＭＭ－ＤＤ」等としてもよい。この場合、「１９９０年１月１日」や「１９９００１０１」等のフォーマットで表された生年月日は、「１９９０－０１－０１」に変換される。

【００４７】

なお、データ利用主体の装置３０は、図２の（１９）として示すように、エンドユーザの端末４０から本人確認情報を取得する。例えば、図３の（１１）に示すような本人確認書類を撮影する画面をエンドユーザの端末４０に表示させ、当該画面から本人確認情報を取得する。なお、図２の（１９）の処理のタイミングは任意であり、特段制限されない。

【００４８】

そして、データ利用主体の装置３０は、データ保持主体の装置２０から受信した本人確認情報と、エンドユーザの端末４０から受信した本人確認情報とを照合する処理を行う。当該照合処理は、２つの本人確認情報をオペレータに向けて提示し、オペレータによる確認作業を促すとともに、照合結果の入力を受付ける処理であってもよいし、コンピュータが２つの本人確認情報の照合を行うものであってもよい。

【００４９】

なお、装置間で送受信される各種情報を、サービス開始申し込みを行ったユーザに紐付ける手段は特段制限されず、周知のあらゆる手段を採用することができる。

【００５０】

「管理装置１０の機能構成」

次に、図４の機能ブロック図を用いて、管理装置１０の機能構成を説明する。図示するように、管理装置１０は、一覧情報送信部１１と、遷移情報送信部１２と、中継部１３とを有する。

【００５１】

一覧情報送信部１１は、本人確認情報を提供可能なデータ保持主体の装置２０の一覧を示す一覧情報をデータ利用主体の装置３０に送信する。

【００５２】

遷移情報送信部１２は、一覧情報で示される一覧の中から選択されたデータ保持主体の装置２０を示す選択情報をデータ利用主体の装置３０から受信すると、選択されたデータ保持主体の装置２０にログインするためのログイン画面にエンドユーザの端末４０を遷移させるための遷移情報を出力する。

【００５３】

中継部１３は、データ保持主体の装置２０から受信した本人確認情報を、データ利用主体の装置３０に送信する。なお、中継部１３は、データ保持主体の装置２０から受信した本人確認情報を自装置の不揮発性記憶装置に保存せず、データ保持主体の装置２０とデータ利用主体の装置３０との間の中継を行うことが好ましい。

【００５４】

「データ保持主体の装置２０の機能構成」

次に、図５の機能ブロック図を用いて、データ保持主体の装置２０の機能構成を説明する。図示するように、データ保持主体の装置２０は、認証部２１と、確認部２２と、本人確認情報送信部２３とを有する。データ保持主体の装置２０は、複数のユーザの本人確認情報を記憶している。

【００５５】

認証部２１は、管理装置１０から送信された遷移情報に基づきログイン画面に遷移してきたエンドユーザの端末４０と通信し、ログイン情報の受信及びログイン情報に基づく認証処理を行う。

【００５６】

確認部２２は、認証処理で認証に成功した場合、ログインしたユーザの本人確認情報を記憶手段から読み出し、エンドユーザの端末４０に出力して、本人確認情報の確認を促す。確認部２２は、本人確認情報が表示されるとともに、本人確認情報の一部が隠された情報確認画面をエンドユーザの端末４０に表示させることができる。また、確認部２２は、エンドユーザの端末４０に出力された本人確認情報の変更を受付けることができてもよい。

【００５７】

本人確認情報送信部２３は、本人確認情報を確認した旨の確認情報をエンドユーザの端末４０から受信すると、確認された本人確認情報を管理装置１０に送信する。確認部２２に

より本人確認情報の変更が受け受けられた場合、本人確認情報送信部２３は、変更後の本人確認情報を管理装置１０に送信する。

【００５８】

「装置のハードウエア構成」

本人確認情報利用システムを構成する各装置のハードウエア構成の一例を説明する。本人確認情報利用システムは、管理装置１０と、データ保持主体の装置２０とを有する。本人確認情報利用システムは、さらにデータ利用主体の装置３０を有してもよい。また、本人確認情報利用システムは、さらにエンドユーザの端末４０を有してもよい。

【００５９】

図６は、各装置のハードウエア構成例を示す図である。各装置が備える各機能部は、任意のコンピュータのＣＰＵ（Central Processing Unit）、メモリ、メモリにロードされるプログラム、そのプログラムを格納するハードディスク等の記憶ユニット（あらかじめ装置を出荷する段階から格納されているプログラムのほか、ＣＤ（Compact Disc）等の記憶媒体やインターネット上のサーバ等からダウンロードされたプログラムをも格納できる）、ネットワーク接続用インターフェイスを中心にハードウエアとソフトウエアの任意の組合せによって実現される。そして、その実現方法、装置にはいろいろな変形例があることは、当業者には理解されるところである。

【００６０】

図６に示すように、各装置は、プロセッサ１Ａ、メモリ２Ａ、入出力インターフェイス３Ａ、周辺回路４Ａ、バス５Ａを有する。周辺回路４Ａには、様々なモジュールが含まれる。通知システムは、周辺回路４Ａを有さなくてもよい。なお、各装置は物理的及び／又は論理的に分かれた複数の装置で構成されてもよいし、物理的及び論理的に一体となった１つの装置で構成されてもよい。前者の場合、各装置を構成する複数の装置各々が上記ハードウエア構成を備えることができる。

【００６１】

バス５Ａは、プロセッサ１Ａ、メモリ２Ａ、周辺回路４Ａ及び入出力インターフェイス３Ａが相互にデータを送受信するためのデータ伝送路である。プロセッサ１Ａは、例えばＣＰＵ、ＧＰＵ（Graphics Processing Unit）などの演算処理装置である。メモリ２Ａは、例えばＲＡＭ（Random Access Memory）やＲＯＭ（Read Only Memory）などのメモリである。入出力インターフェイス３Ａは、入力装置、外部装置、外部サーバ、外部センサ等から情報を取得するためのインターフェイスや、出力装置、外部装置、外部サーバ等に情報を出力するためのインターフェイスなどを含む。入力装置は、例えばキーボード、マウス、マイク等である。出力装置は、例えばディスプレイ、スピーカ、プリンター、メーラ等である。プロセッサ１Ａは、各モジュールに指令を出し、それらの演算結果をもとに演算を行うことができる。

【００６２】

「作用効果」

本実施形態の本人確認情報利用システムは、データ保持主体が保持する本人確認情報がデータ利用主体に提供される前に、その本人確認情報をユーザに提示し、内容の確認を促すステップを実行する。そして、ユーザにより確認された本人確認情報がデータ利用主体に提供される。

【００６３】

このような本人確認情報利用システムによれば、古い内容のまま放置された本人確認情報がデータ利用主体に提供される不都合を効果的に抑制することができる。これにより、古い内容の本人確認情報が送受信されることにより生じる不都合（ユーザより提示された本人確認情報との照合におけるエラー等）を抑制できる。結果、あるサービスの利用を開始する際に必要となる本人確認の作業が効率化する。

【００６４】

また、本実施形態の本人確認情報利用システムは、データ保持主体が保持する本人確認情報をユーザに提示し、内容の確認を促す処理において、本人確認情報が表示されるとも

に、本人確認情報の一部が隠された情報確認画面をエンドユーザの端末に表示させることができる。これにより、当該情報を盗み見られたり、不正に取得されたりする不都合を抑制できる。

【００６５】

また、本実施形態の本人確認情報利用システムにおいては、データ保持主体が保持する本人確認情報をユーザに提示し、内容の確認を促すステップにおいて、本人確認情報の変更を受付けることができる。そして、変更を受付けた場合、変更後の本人確認情報をデータ保持主体の装置からデータ利用主体の装置に送信することができる。上記ステップにおいて本人確認情報の変更を行うことができるので、ユーザは、別途ページを開いて本人確認情報を変更したり、変更後に再度それまで行ったサービス利用開始のための手続きを最初からやり直したりする手間を回避できる。

【００６６】

また、本実施形態の本人確認情報利用システムにおいては、管理装置１０は、データ保持主体の装置から受信した本人確認情報を自装置の不揮発性記憶装置に保存せず、単にデータ保持主体の装置２０とデータ利用主体の装置３０との間の中継だけを行うことができる。本人確認情報を不要に多くの場所に記憶させることを回避することで、本人確認情報が漏洩したり、不正に取得されたりする不都合を抑制できる。また、データ保持主体は、安心して、自身が管理している本人確認情報を外部に提供できる。

【００６７】

＜第２の実施形態＞

本実施形態の本人確認情報利用システムは、データ利用主体の装置３０に本人確認情報を提供可能な複数のデータ保持主体の装置２０の中から複数を選択可能な点で、第１の実施形態と異なる。例えば図３の（８）に示す画面において、ユーザは複数のデータ保持主体を選択できる。

【００６８】

本実施形態の管理装置１０の機能ブロック図の一例は、図７で示される。図示するように、管理装置１０は、一覧情報送信部１１と、遷移情報送信部１２と、中継部１３と、判定部１４とを有する。

【００６９】

遷移情報送信部１２は、複数のデータ保持主体が選択されたことを示す選択情報を受信すると（図２の（６））、選択された複数のデータ保持主体の装置２０各々にログインするための複数のログイン画面にエンドユーザの端末４０を遷移させるための複数の遷移情報を出力する（図２の（７））。

【００７０】

結果、エンドユーザの端末４０は、選択された複数のデータ保持主体各々のログイン画面にリダイレクトされる。そして、ユーザは、各ログイン画面を介してログイン情報の入力等を行う（図２の（９））。そして、ログインに成功した場合、各データ保持主体の装置２０は、第１の実施形態で説明したように本人確認情報をエンドユーザの端末４０に出力し（図２の（１０））、その後、確認された本人確認情報を管理装置１０に送信する（図２の（１３））。

【００７１】

判定部１４は、複数のデータ保持主体の装置２０各々から本人確認情報を受信した場合、複数の本人確認情報が互いに一致するか否か判定する。そして、複数の本人確認情報が互いに一致しない場合、判定部１４は、複数の本人確認情報の送信元である複数のデータ保持主体の装置２０にその旨を通知する。これにより、データ保持主体の装置２０は、自装置が管理する情報が間違っている可能性があることを認識できる。

【００７２】

また、複数の本人確認情報が互いに一致しない場合、判定部１４は、複数の本人確認情報の中から信頼度が最も高いものを決定し、決定した本人確認情報をデータ利用主体の装置３０に送信させることができる（図２の（１４））。なお、複数の本人確認情報が互いに

一致する場合、判定部１４は、その本人確認情報をデータ利用主体の装置３０に送信させる。

【００７３】

例えば、データ保持主体の装置２０から受信した本人確認情報は、情報の更新日を示す情報を含んでもよい。そして、判定部１４は、更新日が最新の本人確認情報を、信頼度が最も高いものとして決定してもよい。

【００７４】

その他、データ保持主体の装置２０から受信した本人確認情報は、上述した本人確認情報の確認処理（図３の（９）の処理）を行った最新日を示す情報を含んでもよい。そして、判定部１４は、確認処理を行った最新日が最新の本人確認情報を、信頼度が最も高いものとして決定してもよい。

【００７５】

その他、データ保持主体の装置２０から受信した本人確認情報は、上述した本人確認情報の確認処理（図３の（９）の処理）を行った回数を示す情報を含んでもよい。そして、判定部１４は、確認処理を行った回数が最大の本人確認情報を、信頼度が最も高いものとして決定してもよい。

【００７６】

本実施形態の本人確認情報利用システムのその他の構成は、第１の実施形態と同様である。

【００７７】

以上、本実施形態の本人確認情報利用システムによれば、第１の実施形態と同様の作用効果が実現される。また、本実施形態の本人確認情報利用システムによれば、複数のデータ保持主体の装置２０から本人確認情報を収集し、それらの内容が互いに一致しない場合には、その中の信頼度が最も高いものを、データ利用主体の装置３０に送信させることができる。これにより、古い内容のまま放置された本人確認情報がデータ利用主体に提供される不都合を効果的に抑制することができる。

【００７８】

また、本実施形態の本人確認情報利用システムによれば、複数のデータ保持主体の装置２０から収集した本人確認情報の内容が互いに一致しない場合、管理装置１０は、複数の本人確認情報の送信元である複数のデータ保持主体の装置２０にその旨を通知することができる。これにより、データ保持主体の装置２０は、自装置が管理する情報が間違っている可能性があることを認識できる。

【００７９】

＜第３の実施形態＞

「概要」

本実施形態の本人確認情報利用システムは、上述したユーザが本人確認情報を確認する処理（図２の（１０）、図３（１０）の画面提示）を、データ保持主体の装置２０でなく管理装置１０が行う点で、第１の実施形態と異なる。

【００８０】

「本人確認情報利用システムの機能構成」

次に、図８を用いて、本実施形態の本人確認情報利用システムの構成を詳細に説明する。（１）から（９）までの処理の流れは、第１の実施形態で説明した図２の（１）から（９）までの処理の流れと同じである。すなわち、図３の（９）に示すように、ユーザにより選択されたデータ保持主体の装置２０にログインするためのログイン画面をエンドユーザの端末４０に表示させ、ログイン処理を実行するまでは、第１の実施形態の処理の流れと同じである。

【００８１】

データ保持主体の装置２０へのログインに成功した場合、図８の（１０）として示すように、データ保持主体の装置２０は、本人認証済通知を管理装置１０に送信する。その後、管理装置１０は、図８（１１）として示すように、本人確認情報のリクエストをデータ保

持主体の装置２０に送信する。データ保持主体の装置２０は、管理装置１０からのリクエストを受信すると、図８の（１２）として示すように、データ保持主体の装置２０に記憶されているそのユーザの本人確認情報を読み出し、読み出した本人確認情報を管理装置１０に送信する。

【００８２】

次いで、管理装置１０は、図８の（１３）として示すように、データ保持主体の装置２０から受信した本人確認情報をエンドユーザの端末４０に出力して、本人確認情報の確認を促す。例えば、管理装置１０は、図３の（１０）に示すような情報確認画面を生成し、エンドユーザの端末４０に表示させる。なお、当該情報確認画面において、本人確認情報の一部が隠されてもよい。例えば、「日本太●、東京都●●区・・・」等のように、文字の一部が伏字になっていてもよい。これにより、当該情報を盗み見られたり、不正に取得されたりする不都合を抑制できる。

【００８３】

また、当該情報確認画面において、本人確認情報の内容が現在の内容と異なる場合、変更を促す旨がユーザに通知されてもよい。そして、当該情報確認画面において本人確認情報を変更する入力を行う旨が入力されると、管理装置１０は、データ保持主体の装置２０の画面（本人確認情報を変更するための画面）にエンドユーザの端末４０を遷移（リダイレクト）させてもよい。また、当該情報確認画面において、本人確認情報の内容が現在の内容と異なる場合、別のデータ保持主体を選択し直す画面を呼び出すことができてもよい。当該画面を呼び出す入力がなされた場合、その旨が管理装置１０からデータ利用主体の装置３０に通知される。そして、図８の（４）として示すように、データ利用主体の装置３０が本人確認情報を提供可能なデータ保持主体の一覧をエンドユーザの端末４０に送信する処理以降が行われる。

【００８４】

次に、本人確認情報が正しいことがユーザにより確認された場合、図８の（１４）として示すように、エンドユーザの端末４０はその旨を示す入力情報を管理装置１０に送信する。

【００８５】

その後、図８の（１５）として示すように、管理装置１０は、ユーザにより確認された本人確認情報をデータ利用主体の装置３０に送信する。なお、管理装置１０は、（１２）で受信した本人確認情報をデータ利用主体の装置３０に送信してもよいし、（１４）の入力情報を受信した後、再度、データ保持主体の装置２０から本人確認情報を受信し直し、新たに受信した本人確認情報をデータ利用主体の装置３０に送信してもよい。管理装置１０は、データ保持主体の装置２０から受信した本人確認情報を自装置の不揮発性記憶装置に保存せず、単にデータ保持主体の装置２０とデータ利用主体の装置３０との間の中継だけを行うことが好ましい。本人確認情報を不要に多くの場所に記憶させることを回避することで、本人確認情報が漏洩したり、不正に取得されたりする不都合を抑制できる。また、データ保持主体は、安心して、自身が管理している本人確認情報を外部に提供できる。また、管理装置１０は、データ保持主体の装置２０から受信した本人確認情報のフォーマットを統一フォーマットに変換した後、フォーマット変換後の本人確認情報をデータ利用主体の装置３０に送信してもよい。統一フォーマットの詳細は特段制限されない。例えば生年月日の統一フォーマットは「ＹＹＹＹ－ＭＭ－ＤＤ」等としてもよい。この場合、「１９９０年１月１日」や「１９９００１０１」等のフォーマットで表された生年月日は、「１９９０－０１－０１」に変換される。

【００８６】

なお、データ利用主体の装置３０は、図８の（１６）として示すように、エンドユーザの端末４０から本人確認情報を取得する。例えば、図３の（１１）に示すような本人確認書類を撮影する画面をエンドユーザの端末４０に表示させ、当該画面から本人確認情報を取得する。なお、図８の（１６）の処理のタイミングは任意であり、特段制限されない。

【００８７】

そして、データ利用主体の装置３０は、データ保持主体の装置２０から受信した本人確認情報と、エンドユーザの端末４０から受信した本人確認情報とを照合する処理を行う。当該照合処理は、２つの本人確認情報をオペレータに向けて提示し、オペレータによる確認作業を促すとともに、照合結果の入力を受付ける処理であってもよいし、コンピュータが２つの本人確認情報の照合を行うものであってもよい。

【００８８】

「データ保持主体の装置２０の機能構成」

次に、図９の機能ブロック図を用いて、データ保持主体の装置２０の機能構成を説明する。図示するように、データ保持主体の装置２０は、認証部２１と、本人確認情報送信部２３とを有する。

【００８９】

認証部２１は、管理装置１０から送信された遷移情報に基づきログイン画面に遷移してきたエンドユーザの端末４０と通信し、ログイン情報の受信及びログイン情報に基づく認証処理を行う。本人確認情報送信部２３は、認証処理で認証に成功した場合、ログインしたユーザの本人確認情報を記憶手段から読み出し、管理装置１０に送信する。

【００９０】

「管理装置１０の機能構成」

次に、図１０の機能ブロック図を用いて、管理装置１０の機能構成を説明する。図示するように、管理装置１０は、一覧情報送信部１１と、遷移情報送信部１２と、中継部１３と、確認部１５とを有する。

【００９１】

一覧情報送信部１１は、本人確認情報を提供可能なデータ保持主体の装置２０の一覧を示す一覧情報をデータ利用主体の装置３０に送信する。

【００９２】

遷移情報送信部１２は、データ保持主体の装置２０にログインするためのログイン画面にエンドユーザの端末４０を遷移させるための遷移情報を出力する。具体的には、遷移情報送信部１２は、一覧情報で示される一覧の中から選択されたデータ保持主体を示す選択情報をデータ利用主体の装置３０から受信すると、選択されたデータ保持主体の装置２０にログインするためのログイン画面にエンドユーザの端末４０を遷移させるための遷移情報を出力する。

【００９３】

確認部１５は、遷移情報に基づきログイン画面に遷移してきたエンドユーザの端末４０がログイン画面を介してデータ保持主体の装置２０へのログインに成功した場合、ログインしたユーザの本人確認情報をデータ保持主体の装置２０から受信する。そして、確認部１５は、受信した本人確認情報をエンドユーザの端末４０に出力して、本人確認情報の確認を促す。確認部１５は、本人確認情報が表示されるとともに、本人確認情報の一部が隠された情報確認画面をエンドユーザの端末４０に表示させることができる。

【００９４】

中継部１３は、本人確認情報を確認した旨の確認情報をエンドユーザの端末４０から受信すると、確認された本人確認情報をデータ利用主体の装置３０に送信する。なお、中継部１３は、データ保持主体の装置２０から受信した本人確認情報を自装置の不揮発性記憶装置に保存せず、データ保持主体の装置２０とデータ利用主体の装置３０との間の中継を行うことが好ましい。

【００９５】

「装置のハードウエア構成」

本人確認情報利用システムを構成する各装置のハードウエア構成の一例は、第１及び第２の実施形態と同様である。

【００９６】

「作用効果」

本実施形態の本人確認情報利用システムによれ、第１の実施形態と同様の作用効果が実現

される。また、本実施形態の本人確認情報利用システムによれば、上述したユーザが本人確認情報を確認する処理を、データ保持主体の装置２０でなく管理装置１０が行うことができる。これにより、データ保持主体の装置２０の処理負担が軽減される。

【００９７】

＜第４の実施形態＞

本実施形態の本人確認情報利用システムは、データ利用主体の装置３０に本人確認情報を提供可能な複数のデータ保持主体の装置２０の中から複数を選択可能な点で、第３の実施形態と異なる。例えば、例えば図３の（８）に示す画面において、ユーザは複数のデータ保持主体を選択できる。

【００９８】

本実施形態の管理装置１０の機能ブロック図の一例は、図１１で示される。図示するように、管理装置１０は、一覧情報送信部１１と、遷移情報送信部１２と、中継部１３と、判定部１４と、確認部１５とを有する。

【００９９】

遷移情報送信部１２は、複数のデータ保持主体が選択されたことを示す選択情報を受信すると（図８の（６））、選択された複数のデータ保持主体の装置２０各々にログインするための複数のログイン画面にエンドユーザの端末４０を遷移させるための複数の遷移情報を出力する（図８の（７））。

【０１００】

結果、エンドユーザの端末４０は、選択された複数のデータ保持主体各々のログイン画面にリダイレクトされる。そして、ユーザは、各ログイン画面を介してログイン情報の入力等を行う（図８の（９））。そして、ログインに成功した場合、本人認証済通知の送信（図８の（１０））、本人確認情報のリクエストの受信（図８の（１１））を経て、各データ保持主体の装置２０は、第３の実施形態で説明したように本人確認情報を管理装置１０に送信する（図８の（１２））。その後、管理装置１０は、複数のデータ保持主体の装置２０から受信した複数の本人確認情報をエンドユーザの端末４０に出力して、本人確認情報の確認を促す（図８の（１３））。例えば、管理装置１０は、複数の本人確認情報を一覧表示した情報確認画面を生成し、エンドユーザの端末４０に表示させてもよいし、複数の本人確認情報を順次表示する情報確認画面を生成し、エンドユーザの端末４０に表示させてもよいし、その他の構成の情報確認画面を生成し、エンドユーザの端末４０に表示させてもよい。

【０１０１】

判定部１４の構成は、第２の実施形態で説明したものと同じであるので、ここでの説明は省力する。

【０１０２】

本実施形態の本人確認情報利用システムのその他の構成は、第３の実施形態と同様である。

【０１０３】

以上、本実施形態の本人確認情報利用システムによれば、第３の実施形態と同様の作用効果が実現される。また、本実施形態の本人確認情報利用システムによれば、管理装置１０が備える判定部１４により、第２の実施形態と同様の作用効果が実現される。

【０１０４】

以上、図面を参照して本発明の実施形態について述べたが、これらは本発明の例示であり、上記以外の様々な構成を採用することもできる。

【０１０５】

なお、本明細書において、「取得」とは、ユーザ入力に基づき、又は、プログラムの指示に基づき、「自装置が他の装置や記憶媒体に格納されているデータを取りに行くこと（能動的な取得）」、たとえば、他の装置にリクエストまたは問い合わせして受信すること、他の装置や記憶媒体にアクセスして読み出すこと等、および、ユーザ入力に基づき、又は、プログラムの指示に基づき、「自装置に他の装置から出力されるデータを入力すること

（受動的な取得）」、たとえば、配信（または、送信、プッシュ通知等）されるデータを受信すること、また、受信したデータまたは情報の中から選択して取得すること、及び、「データを編集（テキスト化、データの並び替え、一部データの抽出、ファイル形式の変更等）などして新たなデータを生成し、当該新たなデータを取得すること」の少なくともいずれか一方を含む。

【０１０６】

上記の実施形態の一部または全部は、以下の付記のようにも記載されうるが、以下に限られない。

１．　複数のユーザの本人確認情報を記憶するデータ保持主体の装置と、前記データ保持主体の装置とデータ利用主体の装置との間で行われる前記本人確認情報の受け渡しを管理する管理装置とを有し、

前記データ保持主体の装置は、

前記管理装置から送信された遷移情報に基づきログイン画面に遷移してきたエンドユーザの端末と通信し、ログイン情報の受信及び前記ログイン情報に基づく認証処理を行う認証手段と、

前記認証処理で認証に成功した場合、ログインしたユーザの前記本人確認情報を記憶手段から読み出し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促す確認手段と、

前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記管理装置に送信する本人確認情報送信手段と、

を有し、

前記管理装置は、

前記データ保持主体の装置から受信した前記本人確認情報を、前記データ利用主体の装置に送信する中継手段を有する本人確認情報利用システム。

２．　前記確認手段は、前記本人確認情報が表示されるとともに、前記本人確認情報の一部が隠された情報確認画面を前記エンドユーザの端末に表示させる１に記載の本人確認情報利用システム。

３．　前記確認手段は、前記エンドユーザの端末に出力された前記本人確認情報の変更を受付け、

前記本人確認情報送信手段は、前記確認手段により前記本人確認情報の変更が受付けられた場合、変更後の前記本人確認情報を前記管理装置に送信する１又は２に記載の本人確認情報利用システム。

４．　前記管理装置は、

前記データ保持主体の装置から受信した前記本人確認情報を自装置の不揮発性記憶装置に保存せず、前記データ保持主体の装置と前記データ利用主体の装置との間の中継を行う１から３のいずれかに記載の本人確認情報利用システム。

５．　前記管理装置は、

前記本人確認情報を提供可能な前記データ保持主体の一覧を示す一覧情報を前記データ利用主体の装置に送信する一覧情報送信手段と、

前記一覧情報で示される一覧の中から選択された前記データ保持主体を示す選択情報を前記データ利用主体の装置から受信すると、選択された前記データ保持主体の装置にログインするための前記ログイン画面に前記エンドユーザの端末を遷移させるための前記遷移情報を出力する遷移情報送信手段と、

を有する１から４のいずれかに記載の本人確認情報利用システム。

６．　前記遷移情報送信手段は、複数の前記データ保持主体が選択されたことを示す前記選択情報を受信すると、選択された複数の前記データ保持主体の装置各々にログインするための複数の前記ログイン画面に前記エンドユーザの端末を遷移させるための複数の前記遷移情報を出力し、

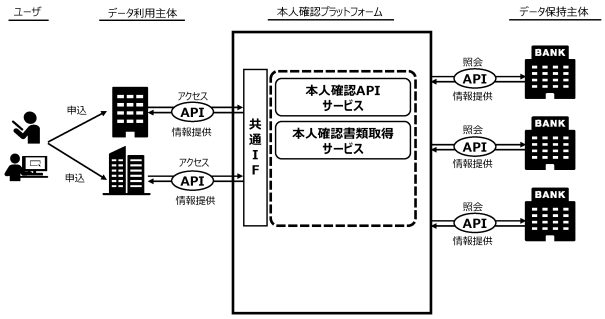
前記管理装置は、

複数の前記データ保持主体の装置各々から前記本人確認情報を受信した場合、複数の前記

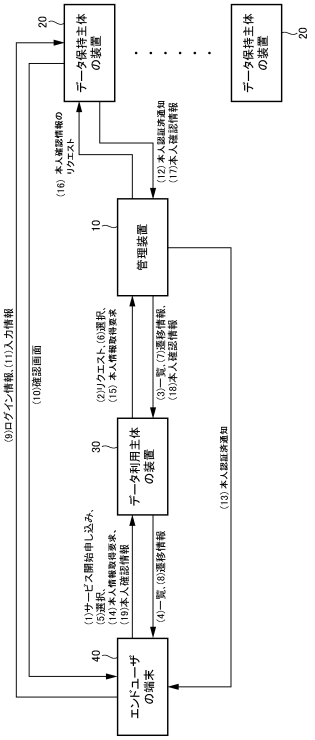
本人確認情報が互いに一致するか否か判定する判定手段をさらに有する５に記載の本人確認情報利用システム。
７．　前記判定手段は、
複数の前記本人確認情報が互いに一致しない場合、複数の前記本人確認情報の中から信頼度が最も高いものを決定し、決定した前記本人確認情報を前記データ利用主体の装置に送信させる６に記載の本人確認情報利用システム。
８．　前記判定手段は、
複数の前記本人確認情報が互いに一致しない場合、複数の前記本人確認情報の送信元である複数の前記データ保持主体の装置にその旨を通知する６又は７に記載の本人確認情報利用システム。
９．　データ保持主体の装置にログインするためのログイン画面にエンドユーザの端末を遷移させるための遷移情報を出力する遷移情報送信手段と、
前記遷移情報に基づき前記ログイン画面に遷移してきた前記エンドユーザの端末が前記ログイン画面を介して前記データ保持主体の装置へのログインに成功した場合、ログインしたユーザの前記本人確認情報を前記データ保持主体の装置から受信し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促す確認手段と、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記データ利用主体の装置に送信する中継手段と、
を有する管理装置。
１０．　前記確認手段は、前記本人確認情報が表示されるとともに、前記本人確認情報の一部が隠された情報確認画面を前記エンドユーザの端末に表示させる９に記載の管理装置。
１１．　前記データ保持主体の装置から受信した前記本人確認情報を自装置の不揮発性記憶装置に保存せず、前記データ保持主体の装置と前記データ利用主体の装置との間の中継を行う９又は１０に記載の管理装置。
１２．　本人確認情報を提供可能なデータ保持主体の一覧を示す一覧情報をデータ利用主体の装置に送信する一覧情報送信手段をさらに有し、
前記遷移情報送信手段は、
前記一覧情報で示される一覧の中から選択された前記データ保持主体を示す選択情報を前記データ利用主体の装置から受信すると、選択された前記データ保持主体の装置にログインするための前記ログイン画面に前記エンドユーザの端末を遷移させるための前記遷移情報を出力する９から１１のいずれかに記載の管理装置。
１３．　前記遷移情報送信手段は、複数の前記データ保持主体が選択されたことを示す前記選択情報を受信すると、選択された複数の前記データ保持主体の装置各々にログインするための複数の前記ログイン画面に前記エンドユーザの端末を遷移させるための複数の前記遷移情報を出力し、
前記確認手段は、前記エンドユーザの端末が複数の前記ログイン画面各々を介して複数の前記データ保持主体の装置各々へのログインに成功した場合、ログインしたユーザの前記本人確認情報を複数の前記データ保持主体の装置各々から受信し、前記エンドユーザの端末に出力して、複数の前記データ保持主体の装置各々から受信した複数の前記本人確認情報の確認を促し、
複数の前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された複数の前記本人確認情報が互いに一致するか否か判定する判定手段をさらに有する１２に記載の管理装置。
１４．　前記判定手段は、
複数の前記本人確認情報が互いに一致しない場合、複数の前記本人確認情報の中から信頼度が最も高いものを決定し、決定した前記本人確認情報を前記データ利用主体の装置に送信させる１３に記載の管理装置。
１５．　前記判定手段は、
複数の前記本人確認情報が互いに一致しない場合、複数の前記本人確認情報の送信元であ

る複数の前記データ保持主体の装置にその旨を通知する１３又は１４に記載の管理装置。
１６．　複数のユーザの本人確認情報を記憶するデータ保持主体の装置と、前記データ保持主体の装置とデータ利用主体の装置との間で行われる前記本人確認情報の受け渡しを管理する管理装置とを有する本人確認情報利用システムにより実行され、
前記データ保持主体の装置は、
前記管理装置から送信された遷移情報に基づきログイン画面に遷移してきたエンドユーザの端末と通信し、ログイン情報の受信及び前記ログイン情報に基づく認証処理を行い、
前記認証処理で認証に成功した場合、ログインしたユーザの前記本人確認情報を記憶手段から読み出し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促し、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記管理装置に送信し、
前記管理装置は、
前記データ保持主体の装置から受信した前記本人確認情報を、前記データ利用主体の装置に送信する本人確認情報利用方法。
１７．　コンピュータが、
データ保持主体の装置にログインするためのログイン画面にエンドユーザの端末を遷移させるための遷移情報を出力し、
前記遷移情報に基づき前記ログイン画面に遷移してきた前記エンドユーザの端末が前記ログイン画面を介して前記データ保持主体の装置へのログインに成功した場合、ログインしたユーザの前記本人確認情報を前記データ保持主体の装置から受信し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促し、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記データ利用主体の装置に送信する管理方法。
１８．　コンピュータを、
データ保持主体の装置にログインするためのログイン画面にエンドユーザの端末を遷移させるための遷移情報を出力する遷移情報送信手段、
前記遷移情報に基づき前記ログイン画面に遷移してきた前記エンドユーザの端末が前記ログイン画面を介して前記データ保持主体の装置へのログインに成功した場合、ログインしたユーザの前記本人確認情報を前記データ保持主体の装置から受信し、前記エンドユーザの端末に出力して、前記本人確認情報の確認を促す確認手段、
前記本人確認情報を確認した旨の確認情報を前記エンドユーザの端末から受信すると、確認された前記本人確認情報を前記データ利用主体の装置に送信する中継手段、
として機能させるプログラム。
【符号の説明】
【０１０７】
１０　管理装置
１１　一覧情報送信部
１２　遷移情報送信部
１３　中継部
１４　判定部
１５　確認部
２０　データ保持主体の装置
２１　認証部
２２　確認部
２３　本人確認情報送信部
３０　データ利用主体の装置
４０　エンドユーザの端末
１Ａ　プロセッサ
２Ａ　メモリ
３Ａ　入出力Ｉ／Ｆ

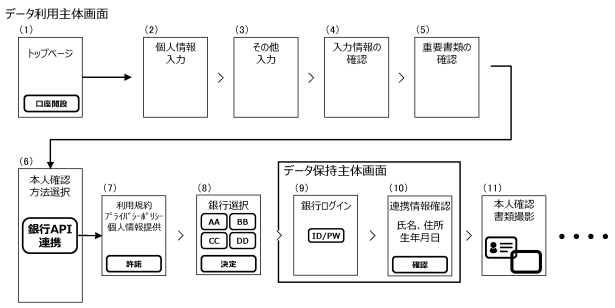
４Ａ　周辺回路
５Ａ　バス
【図面】
【図１】



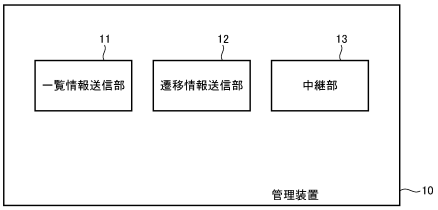
【図２】



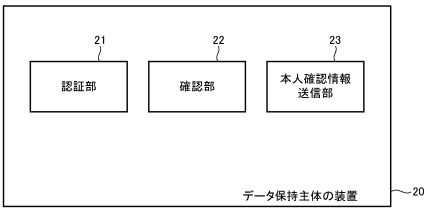
【図３】



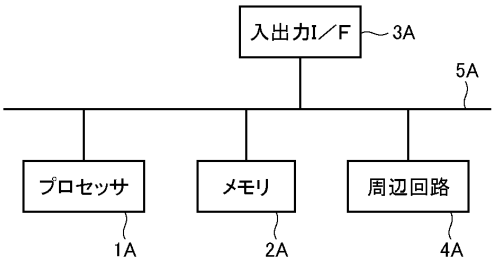
【図４】



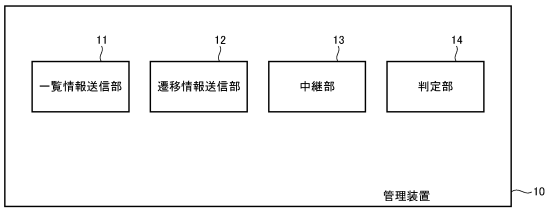
【図５】


21
22
23
認証部
確認部
本人確認情報送信部
データ保持主体の装置
20

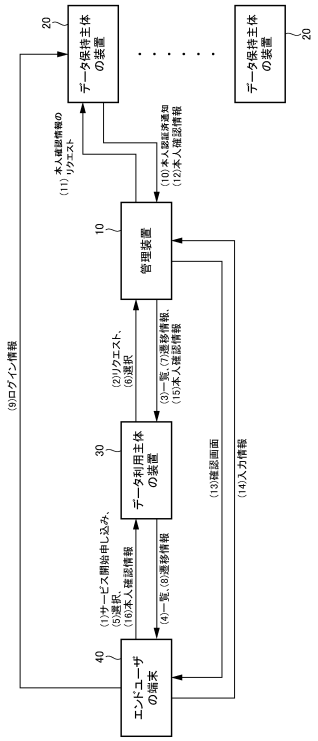
【図６】


入出力I／F
3A
5A
プロセッサ
メモリ
周辺回路
1A
2A
4A

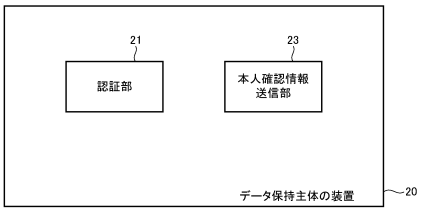
【図７】


11
12
13
14
一覧情報送信部
遷移情報送信部
中継部
判定部
管理装置
10

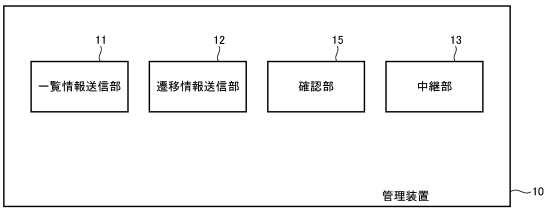
【図８】


20
データ保持主体の装置
20
データ保持主体の装置
本人確認情報のリクエスト
(11)
(10)本人確認済通知
(12)本人確認情報
10
管理装置
(2)リクエスト、
(6)選択、
(3)一覧、(7)遷移情報、
(15)本人確認情報
(9)ログイン情報
30
データ利用主体の装置
(13)確認画面
(14)入力情報
(1)サービス開始申し込み、
(5)選択、
(16)本人確認情報
(4)一覧、(8)遷移情報
40
エンドユーザの端末

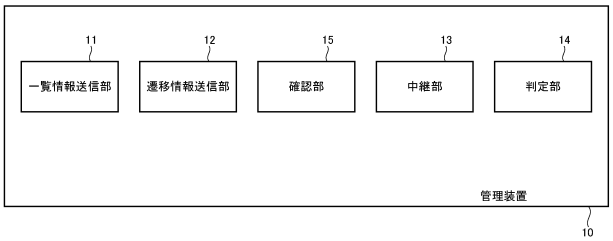
【図９】


21
23
認証部
本人確認情報
送信部
データ保持主体の装置
20

【図１０】


11
12
15
13
一覧情報送信部
遷移情報送信部
確認部
中継部
管理装置
10

【図１１】


11
12
15
13
14
一覧情報送信部
遷移情報送信部
確認部
中継部
判定部
管理装置
10

フロントページの続き

東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者 森山 陽平
東京都港区芝五丁目７番１号 日本電気株式会社内