(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年7月23日(23.07.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/149136 A1

(51) 国際特許分類:
G06T 7/00 (2017.01) *G06F 21/32* (2013.01)
G06T 7/20 (2017.01) *G06Q 50/10* (2012.01)
G06F 21/31 (2013.01)

(21) 国際出願番号： PCT/JP2019/051070

(22) 国際出願日： 2019年12月26日(26.12.2019)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
特願 2019-004321 2019年1月15日(15.01.2019) JP

(71) 出願人: グローリー株式会社 (**GLORY LTD.**) [JP/JP]; 〒6708567 兵庫県姫路市下手野一丁目３番１号 Hyogo (JP).

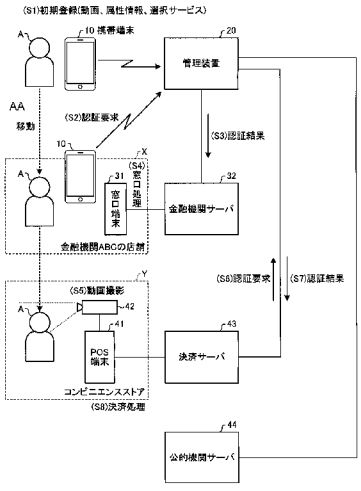
(72) 発明者: 藤田 裕一 (**FUJITA, Yuichi**); 〒6708567 兵庫県姫路市下手野１丁目３番１号 グローリー株式会社内 Hyogo (JP). 西田 繁信 (**NISHIDA, Shigenobu**); 〒6708567 兵庫県姫路市下手野１丁目３番１号 グローリー株式会社内 Hyogo (JP). 國分 亜優美 (**KOKUBUN, Ayumi**); 〒6708567 兵庫県姫路市下手野１丁目３番１号 グローリー株式会社内 Hyogo (JP). 盛脇 荘太郎 (**MORIWAKI, Sotaro**); 〒6708567 兵庫県姫路市下手野１丁目３番１号 グローリー株式会社内 Hyogo (JP).

(74) 代理人: 中辻 史郎, 外 (**NAKATSUJI, Shiro** et al.); 〒1070052 東京都港区赤坂１丁目１４番５号 アークヒルズエグゼクティブタワーＳ３０２ 中辻特許事務所 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) **Title:** AUTHENTICATION SYSTEM, MANAGEMENT DEVICE, AND AUTHENTICATION METHOD

(54) 発明の名称： 認証システム、管理装置及び認証方法



10 Portable terminal
20 Management device
31 Teller terminal
32 Financial institution server
41 POS terminal
43 Payment server
44 Public institution server
S1 Initial registration (moving-image, attribute information, selection service)
S2, S6 Authentication request
S3, S7 Authentication result
S4 Teller processing
S5 Capturing moving-image
S8 Payment processing
X Store of financial institution ABC
Y Convenience store
AA Movement

(57) **Abstract:** In order for personal authentication to be efficiently performed when a user performs various procedures, an authentication system causes a user A to access a management device 20 from a portable terminal 10 and perform initial registration that includes a moving-image of the user A. When the user A receives a service in a store X of a financial institution ABC or a store Y of a convenience store, the management device 20 receives the moving-image of the user A having been imaged in the store, performs an authentication process that corresponds to the type of use, and notifies the store about the result of authentication.

(57) 要約：利用者が各種手続きを行う場合における本人認証を効率良く行うため、認証システムは、利用者Ａに、携帯端末１０から管理装置２０にアクセスして利用者Ａの動画像を含む初期登録を行わせる。利用者Ａが金融機関ＡＢＣの店舗Ｘ又はコンビニエンスストアの店舗Ｙでサービスを受ける場合、管理装置２０は、店舗で撮像された利用者Ａの動画像を受信して利用種別に応じた認証処理を行い、認証結果を店舗に通知する。

WO 2020/149136 A1

［続葉有］

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告(条約第21条(3))

明　細　書

発明の名称 ： 認証システム、管理装置及び認証方法

技術分野

[0001] 本発明は、利用者が各種の手続きを行う場合に、手続きを行う者が利用者本人であることの認証（以下、「本人認証」と言う）を効率良く行うことができる認証システム、管理装置及び認証方法に関する。

背景技術

[0002] 従来、複数の銀行の口座開設の申込を無人で受け付ける銀行口座開設受付端末装置が知られている。例えば、特許文献１に開示された銀行口座開設受付端末装置は、申込者の身分証明書を読み取るとともに該申込者の顔を撮像する。この装置は、撮像した申込者の顔画像と身分証明書により申込者の認証を行う。

[0003] また、複数の認証を組み合わせて認証精度を上げる技術が知られている。例えば、特許文献２に開示された装置では、第１認証部が第１種類の個人認証を行う。第１認証部の個人特徴情報抽出部で得られた被認証者の個人特徴情報に基づいて、カメラ及び照明位置の設定が行われる。その後、第２認証部が、カメラにより撮像された被認証者の撮像画像データに基づいて、第２種類の個人認証を行う。

先行技術文献

特許文献

[0004] 特許文献1：特開２００３－０３０４５２公報

特許文献2：特開２００５－２５８８６０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、上記特許文献１の技術は、新たな銀行口座を開設する場合には利用できるが、口座開設以外のネットバンキングや決済には利用することができない。また、上記特許文献２の技術を用いて複数の認証を組み合わ

せれば、認証精度を高めることができるものの、認証レベルが異なる複数のサービスに対応することができない。

[0006] 例えば、利用者が住所変更を行う場合には、金融機関に対する住所変更届等の手続き、公的機関への転出・転入届け等の手続き、各機関への住所変更等の手続きを行う必要が生ずる。上記特許文献１の技術では、このような手続に対応することができない。利用者は、金融機関、公的機関、その他の機関にそれぞれ赴いて手続きを行わねばならず、かかる手続きに係る労力が過大となっている。また、利用者は、それぞれの手続きにおいて本人認証を個別に行う必要がある。このため、各種の手続きを行う場合の本人認証をいかに効率良く行うかが重要な課題となっている。

[0007] 本発明は、上記従来技術の課題を解決するためになされたものであって、利用者が各種の手続きを行う場合における認証を効率良く行うことができる認証システム、管理装置及び認証方法を提供することを目的とする。

課題を解決するための手段

[0008] 上記の課題を解決するため、本発明は、利用者を認証するための複数の認証情報を管理する認証情報管理手段を有する認証システムであって、所定の利用種別を判定する利用種別判定手段と、前記利用種別判定手段によって判定された利用種別に対応する認証種別を複数の認証種別から選択する認証種別選択手段と、前記認証種別選択手段により選択された認証種別に基づいて前記利用者の認証処理を行う認証処理手段と、前記認証処理手段による前記利用者の認証結果を通知する通知手段とを備える。

[0009] また、本発明は、上記の発明において、前記認証処理手段は、前記利用者の顔部分と該利用者の音声を含む動画像を用いた動的生体認証を少なくとも含む認証処理を行う。

[0010] また、本発明は、上記の発明において、前記動的生体認証は、前記動画像に含まれる前記利用者の顔画像に基づく顔認証処理と、前記動画像に含まれる前記利用者の音声情報に基づく音声認証処理とを含む認証処理を行う。

[0011] また、本発明は、上記の発明において、前記顔認証処理は、前記動画像に

含まれる前記利用者の顔画像と、前記認証情報管理手段により管理された認証情報に含まれる顔画像とを照合する処理である。

[0012] また、本発明は、上記の発明において、前記認証情報管理手段により管理された認証情報は、公的機関により発行された利用者の顔画像を含む証明書に係る情報である。

[0013] また、本発明は、上記の発明において、前記音声認証処理は、前記利用者により発話された音声が示す該利用者に係る属性情報と、前記認証情報管理手段により管理された認証情報に含まれる属性情報とを照合する処理である。

[0014] また、本発明は、上記の発明において、前記音声認証処理は、前記利用者により発話された音声が示すキーワードと、該利用者に対して発話を求めた所定のキーワードとを照合する処理である。

[0015] また、本発明は、上記の発明において、前記音声認証処理は、前記利用者により発話された音声に含まれる該利用者の声紋情報と、前記認証情報管理手段により管理された認証情報に含まれる声紋情報とを照合する処理である。

[0016] また、本発明は、上記の発明において、前記動的生体認証は、前記動画像に含まれる前記利用者の口唇の動きが、該動画像に含まれる前記利用者の音声が示すキーワードと一致するかを認証する口唇認証を含む。

[0017] また、本発明は、上記の発明において、前記認証処理手段における認証処理は、前記利用者が所持する携帯端末と通信可能な管理装置において実行される。

[0018] また、本発明は、上記の発明において、前記認証処理手段における認証処理は、前記利用者が所持する携帯端末において実行される。

[0019] また、本発明は、上記の発明において、前記認証情報管理手段において管理される認証情報は、前記利用者が所持する携帯端末から登録可能である。

[0020] また、本発明は、利用者を認証するための複数の認証情報を管理する認証情報管理手段を有する管理装置であって、所定の利用種別を判定する利用種

別判定手段と、前記利用種別判定手段によって判定された利用種別に対応する認証種別を複数の認証種別から選択する認証種別選択手段と、前記認証種別選択手段により選択された認証種別に基づいて前記利用者の認証処理を行う認証処理手段と、前記認証処理手段による前記利用者の認証結果を通知する通知手段とを備える。

[0021] また、本発明は、利用者を認証するための複数の認証情報を管理する認証情報管理手段を有する認証システムにおける認証方法であって、所定の利用種別を判定する利用種別判定工程と、前記利用種別判定工程によって判定された利用種別に対応する認証種別を複数の認証種別から選択する認証種別選択工程と、前記認証種別選択工程により選択された認証種別に基づいて前記利用者の認証処理を行う認証処理工程と、前記認証処理工程による前記利用者の認証結果を通知する通知工程とを含む。

発明の効果

[0022] 本発明によれば、利用者が各種の手続きを行う場合における認証を効率良く行うことができる。

図面の簡単な説明

[0023] [図1]図１は、実施例１に係る認証システムの概要を示す図である。

[図2]図２は、図１に示した管理装置の構成を示す機能ブロック図である。

[図3]図３は、図２に示した認証情報テーブルの一例を示す図である。

[図4]図４は、図２に示した認証種別管理テーブルの一例を示す図である。

[図5]図５は、図４に示した認証種別５の認証処理を説明するための説明図である。

[図6]図６は、初期登録時の処理手順を示すフローチャートである。

[図7]図７は、初期登録時の携帯端末の画面例（その１）を示す図である。

[図8]図８は、初期登録時の携帯端末の画面例（その２）を示す図である。

[図9]図９は、初期登録時の携帯端末の画面例（その３）を示す図である。

[図10]図１０は、初期登録時の携帯端末の画面例（その４）を示す図である。

[図11]図１１は、本人認証時の処理手順を示すフローチャートである。

[図12]図１２は、実施例２に係る認証システムの概要を示す図である。

[図13]図１３は、図１２に示した管理装置の構成を示す機能ブロック図である。

[図14]図１４は、初期登録時の処理手順を示すフローチャートである。

[図15]図１５は、サービス予約時の処理手順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

[0024] 以下に、添付図面を参照して、本発明に係る認証システム、管理装置及び認証方法の好適な実施例を詳細に説明する。以下に示す実施例１及び２では、クライアント－サーバシステムのサーバ装置として機能する管理装置を用いて認証サービスを提供する場合を示すが、本発明はこれに限定されるものではない。例えば、クラウドシステム上で認証サービスを提供する場合に本発明を適用することもできる。

実施例 1

[0025] ＜実施例１に係る認証システムの概要＞

まず、本実施例１に係る認証システムの概要について説明する。本実施例１に係る認証システムは、動画像を用いた顔認証、音声認識等を利用した本人認証サービスを行う認証システムである。すなわち、利用者があらかじめ顔及び音声を含む動的生体情報を認証システムに登録しておき、この動的生体情報を用いた認証処理を行うことにより、第三者に対して利用者が本人であることを証明することができるシステムである。

[0026] 具体的には、利用者の顔画像を含む公的証明書をあらかじめ認証システムに登録する。例えば、マイナンバーカード又は運転免許証を公的証明書として利用することができる。認証システムは、登録された公的証明書に含まれる顔画像と、例えば携帯端末１０にて撮像された利用者の顔画像とが同一であることを顔認証により認証する。また、認証システムは、利用者の氏名又はキーワードを携帯端末１０の認証アプリ上で発話させ、この音声を音声認識した氏名又はキーワードが公的証明書のキーワードと同一であることを認

証する。また、認証システムは、携帯端末１０の認証アプリ上で発話された音声に含まれる声紋と、あらかじめ登録された利用者の声紋とが同一であることを認証する。また、認証システムは、音声に含まれる各音素と利用者の口、唇の動きとがマッチしているか否かを口唇認証する。認証システムは、このような様々な認証のうちの複数の認証を含む動的生体認証を行うことにより、利用者が本人であるか否かを認証する。

[0027] 例えば、利用者が住所を変更する場合、利用者は、本認証システムで初期登録を行うことにより、各金融機関にて住所変更を行う際の本人認証を効率化することができる。金融機関のみならず、コンビニエンスストアで商品を購入する場合、公的機関での住所変更手続きを行う場合、社員食堂の自動券売機で食券を購入する場合等にも、本人認証を効率化することができる。この際、本認証システムでは、利用者の利用種別に応じて、使用する認証種別を異なるものとすることができる。

[0028] ここで、本実施例１に係る認証システムの概要について図１を用いて具体的に説明する。図１は、本実施例１に係る認証システムの概要を示す図である。ここでは、利用者Ａが自宅等で認証サービスの初期登録を行い、その後に金融機関ＡＢＣの店舗Ｘに移動して認証サービスを受け、引き続きコンビニエンスストアの店舗Ｙに移動して認証サービスを受ける場合について説明する。

[0029] 図１に示す認証システムは、利用者Ａが事前に動画、属性情報、選択サービスを登録することを条件として、該利用者Ａが各種サービスの提供を受ける場合にその利用種別に応じた本人認証を行うシステムである。具体的には、複数の認証種別の中から利用種別に応じた認証種別が選択されて、選択した認証種別の認証処理が行われる。

[0030] 本認証システムの中核をなす管理装置２０は、利用者Ａの携帯端末１０と通信可能である。携帯端末１０は、スマートフォン又はタブレット等の端末装置である。携帯端末１０は、例えば、４Ｇ規格のＬＴＥ（Ｌｏｎｇ Ｔｅｒｍ Ｅｖｏｌｕｔｉｏｎ）通信又はＷｉＦｉ通信により、管理装置２０に

アクセスする。

[0031] 管理装置２０は、ある金融機関の金融機関サーバ３２、ある決済システムの決済サーバ４３、公的機関の公的機関サーバ４４と通信可能に接続されている。金融機関サーバ３２は、利用者の携帯端末１０を用いたインターネットバンキングを可能とするために設けられた管理装置である。決済サーバ４３は、各利用者の電子マネー額などを管理するサーバ装置である。公的機関サーバ４４は、市区町村の住民表などを管理するサーバ装置である。

[0032] 管理装置２０は、利用種別を判定する機能と、判定された利用種別に対応する認証種別を複数の認証種別から選択する機能と、選択された認証種別に基づいて利用者Ａの認証処理を行う機能と、利用者Ａの認証結果を通知する機能とを有する。利用種別に応じた認証とは、利用者Ａの利用シーンに合わせた認証を行うことを意味する。例えば、利用者Ａが金融機関ＡＢＣの店舗Ｘに所在する場合には、該利用者Ａの氏名などの個人情報を発話させるべきではない。このため、管理装置２０は、個人情報を含まないキーワードの発話を含む動画像を用いた認証種別を選択する。一方、利用者Ａが自宅に所在する場合、管理装置２０は、個人情報の発話を含む動画像を用いた認証種別を選択する。また、例えば、利用者Ａがコンビニエンスストアの店舗Ｙで低額な商品を購入する場合には、管理装置２０は、動画像を用いた比較的簡単な認証種別を選択する。一方、利用者Ａが金融機関ＡＢＣの店舗Ｘで高額の出金を行う場合、管理装置２０は、動画像を用いた高精度な認証種別を選択することになる。

[0033] 利用者Ａが認証システムによる認証サービスを受ける場合には、該利用者Ａが所持する携帯端末１０を用いて管理装置２０にアクセスし、初期登録を行う（ステップＳ１）。本実施例１では、携帯端末１０を用いて管理装置２０又は所定のサイトから認証サービスの認証アプリをダウンロードし、この認証アプリを携帯端末１０上で起動して初期登録を行う場合について説明するが、直接管理装置２０にアクセスしてウエブ上で登録しても良い。初期登録においては、利用者の顔画像及び音声を含む動画像、属性情報、選択サー

ビス、銀行口座の口座情報、電子マネーの口座情報、マイナンバー等が登録される。初期登録の詳細な説明については後述する。

[0034] その後、利用者Ａが金融機関ＡＢＣの店舗Ｘに移動して、例えば、口座の住所変更又は新規口座の開設を行う。窓口端末３１を操作する窓口担当者から呼び出された利用者は、携帯端末１０の認証アプリを起動してログイン操作を行い、管理装置２０にアクセスして認証要求を行う（ステップＳ２）。認証要求を受けた管理装置２０は、利用者Ａの認証処理を行う。このとき、管理装置２０は、利用種別に合わせた認証種別を複数の認証種別の中から選択し、この認証種別に対応する動画像を用いた認証処理を行う。認証処理の詳細な説明については後述する。

[0035] 管理装置２０は、認証結果を金融機関ＡＢＣの金融機関サーバ３２に通知する（ステップＳ３）。金融機関サーバ３２は、認証結果が正当である旨の通知を受けたならば、引き続き口座の住所変更又は新規口座の開設等の窓口処理を行う（ステップＳ４）。これにより、金融機関ＡＢＣは、利用者のなりすましを防止しつつ各種の手続きを行うことができる。ここでは利用者Ａの携帯端末１０から管理装置２０に対して認証要求を行う場合を示したが、窓口端末３１に動画像を撮像する機能と認証要求を行う機能とが設けられている場合には、窓口端末３１から管理装置２０に認証要求を行うこともできる。

[0036] その後、利用者Ａがコンビニエンスストアの店舗Ｙに移動して、商品を購入する場合には、店舗ＹのＰＯＳ端末４１に接続されたカメラ４２が利用者Ａの動画像を撮像する（ステップＳ５）。ＰＯＳ端末４１は、この動画像を用いて管理装置２０に認証要求を行う（ステップＳ６）。認証要求を受けた管理装置２０は、利用者Ａの認証処理を行う。このとき、管理装置２０は、利用種別に合わせた認証種別を複数の認証種別の中から選択し、この認証種別に対応する動画像を用いた認証処理を行う。

[0037] 管理装置２０は、認証結果を決済サーバ４３に通知する（ステップＳ７）。決済サーバ４３は、認証結果が正当である旨の通知を受けたならば、電子

マネー又は金融機関ＡＢＣの口座引落等により商品の決済が可能である旨をＰＯＳ端末４１に通知し、ＰＯＳ端末４１において決済処理を行う（ステップＳ８）。このため、例えば利用者Ａの携帯端末１０が電池切れを起こした場合や利用者Ａが携帯端末１０を紛失した場合であっても、該利用者Ａは商品を購入することができる。特に、災害などが発生し、携帯端末１０が使用できない場合でも、利用者Ａの動画を撮像することができれば、利用者Ａは店舗Ｙで商品を購入することが可能となる。なお、金融機関ＡＢＣの場合と同様に、利用者Ａの携帯端末１０を用いて認証要求を行うこともできる。

[0038] 上述してきたように、本実施例１に係る認証システムでは、利用者Ａが、携帯端末１０から管理装置２０にアクセスして利用者の動画像登録を含む初期登録を行う。利用者Ａが金融機関ＡＢＣの店舗Ｘ又はコンビニエンスストアの店舗Ｙでサービスを受ける場合には、管理装置２０に動画像さ送信される。管理装置２０は、利用種別に応じた認証処理を行い、認証結果を店舗に通知する。これにより、利用者Ａが各種の手続きを行う場合における本人認証を効率良く行うことができる。説明の便宜上その詳細な説明を省略したが、市役所等の公的機関の手続きを行う場合には、管理装置２０から公的機関サーバ４４に対して認証結果を通知すれば良い。

[0039] ＜管理装置２０の構成＞

次に、図１に示した管理装置２０の構成について説明する。図２は、図１に示した管理装置２０の構成を示す機能ブロック図である。同図に示すように、管理装置２０は、入力部２１、表示部２２、通信Ｉ／Ｆ部２３、記憶部２４及び制御部２５を有する。

[0040] 入力部２１は、キーボードやマウス等の入力デバイスである。表示部２２は、液晶パネルやディスプレイ装置等の表示デバイスである。通信Ｉ／Ｆ部２３は、携帯端末１０等との通信を行う。

[0041] 記憶部２４は、ハードディスク装置又は不揮発性メモリ等の２次記憶部である。記憶部２４は、認証情報テーブル２４ａ及び認証種別管理テーブル２４ｂを記憶する。認証情報テーブル２４ａは、利用者を一意に識別する利用

者識別情報ごとに、属性情報、認証情報及び共有サービスに係る情報等を含む。属性情報には、利用者の氏名、住所、電話番号等の個人情報が含まれる。認証情報には、利用者の顔及び音声を含む動画像、利用者の虹彩情報等が含まれる。共有サービスに係る情報には、認証システムの適用対象となるシステム種別が含まれる。

[0042] 図３は、図２に示した認証情報テーブル２４ａの一例を示す図である。同図に示すように、利用者ＩＤ「Ａ１２３」には、氏名「田中〇男」、住所「東京都…（以下省略）」、電話番号「０３（１２３４）５６７８」の属性情報が対応付けられている。属性情報には、利用者の氏名のフリガナ、利用者の年齢、利用者の携帯端末１０の電話番号、メールアドレスなどを含めることもできる。

[0043] また、利用者ＩＤ「Ａ１２３」には、顔及び音声を含む動画像等が認証情報として対応付けられている。例えば、初期登録時に利用者に５種類の異なるキーワードを発話させる場合は、各キーワードを発話する利用者の動画像がそれぞれ撮像され、これら５種類の動画像が利用者ＩＤ「Ａ１２３」に対応付けられる。また、利用者ＩＤ「Ａ１２３」に対応付けて、利用者が発話した複数のキーワードが登録される。例えば、携帯端末１０の表示部に「出身学校は？」と表示されて、利用者が「〇〇大学」と発話したならば、音声認識された「〇〇大学」がキーワードとして登録される。また、携帯端末１０の表示部に「母親の名前は？」と表示されて、利用者が「□□子」と発話したならば、音声認識された「□□子」がキーワードとして登録される。

[0044] 同様に、利用者の声紋情報が登録される。携帯端末１０の表示部に所定長の文章を表示してこれを利用者に音読させ、この音声データを解析して取得した該利用者の声紋情報が、認証情報テーブル２４ａに登録される。声紋情報としては、声の音響的な特徴量（周波数特性）と言語的な特徴量（音素の並びの特性）との一方又は双方が取得される。これらの動画像、キーワード、声紋情報は、データそのものを認証情報テーブル２４ａに記憶させることもできるが、ファイルへのリンク情報を記憶させることもできる。説明の便

宜上図示省略したが、利用者の虹彩情報は認証情報として記憶される。

[0045] 図３は、利用者ＩＤ「Ａ１２３」には、金融機関ＡＢＣ、決済システムＤＥＦ、公的システムＧＨＩが共有サービスとして対応付けられた状況を示している。説明の便宜上図示省略したが、金融機関ＡＢＣに関して支店名及び口座番号等を記憶させ、決済システムＤＥＦに関して電子マネーの識別番号を記憶させ、公的システムＧＨＩに関してマイナンバーカードの識別番号を記憶させることができる。

[0046] 同様に、利用者ＩＤ「Ａ４５６」には、氏名「山本△郎」、住所「東京都…（以下省略）」、電話番号「０３（９８７６）５４３２」を含む属性情報と、顔及び音声を含む動画からなる認証情報と、共有サービスに係る情報とが登録されている。この利用者ＩＤ「Ａ４５６」では、決済システムＤＥＦがサービス対象外とされている。

[0047] 認証種別管理テーブル２４ｂは、複数の認証種別にそれぞれ対応する認証処理の組み合わせを示すテーブルである。本実施例１に係る認証システムは、例えば利用者の利用シーン等の利用種別に対応する認証種別を複数の認証種別から選択し、選択した認証種別に基づいて利用者の認証処理を行う。利用種別に対応する認証種別を容易に選択できるようにする必要があることから、あらかじめ複数の認証種別が認証種別管理テーブル２４ｂに登録されている。

[0048] 図４は、図２に示した認証種別管理テーブル２４ｂの一例を示す図である。同図に示すように、認証種別１は、顔認証で認証処理を行う認証種別である。認証種別２は、顔認証と音声認証１（属性）による動的生体認証を行う認証種別である。音声認証１（属性）とは、利用者により発話された音声に含まれる属性情報（例えば、氏名）が利用者の属性情報と一致するか否かを判定する認証処理を意味する。

[0049] 認証種別３は、顔認証と音声認証２（キーワード）による動的生体認証を行う認証種別である。音声認証２（キーワード）とは、携帯端末１０の表示部に利用者しか知らない質問事項を表示し、この質問事項に対する回答を音

声認識した結果にキーワードが含まれているか否かを判定する認証処理を意味する。例えば、携帯端末１０の表示部に「出身学校は？」と表示された場合に、「〇〇大学」と発話されたならば、音声認識された「〇〇大学」が認証情報テーブル２４ａにキーワード登録されているか否かの認証処理が行われる。

[0050] 認証種別４は、顔認証と音声認証３（声紋）による動的生体認証を行う認証種別である。例えば、携帯端末１０の表示部に「下記に示す一文を読んで下さい」と表示し、音読された音声から声紋情報を取得し、この声紋情報が認証情報テーブル２４ａに登録された声紋情報と一致するか否かの認証処理が行われる。

[0051] 認証種別５は、顔認証、音声認証２（キーワード）及び口唇認証による動的生体認証を行う認証種別である。口唇認証とは、利用者が発話した音素と該利用者の口の動きとが一致するか否かを認証する認証処理である。図５は、図４に示した認証種別５の認証処理を説明するための説明図である。同図に示すように、認証種別５の動的生体認証では、動画像に含まれる顔を用いて顔認証処理が行われるとともに、動画像に含まれる音声に基づいて、すでに説明した音声認証（キーワード）が行われる。さらに、動画像を形成する各画像に含まれる口及び唇の動きと音声に含まれる音素との対応関係により、利用者が真に発話しているか否かの認証処理が行われる。これにより、あらかじめ録音した音声を再生する不正を防止することができる。

[0052] 認証種別６は、顔認証、音声認証３（声紋）及び口唇認証による動的生体認証を行う認証種別である。認証種別７は、顔認証、音声認証２（キーワード）、音声認証３（声紋）、口唇認証及び虹彩認証による動的生体認証を行う認証種別である。認証種別７は、個人を正確に特定する高度な個人認証を要する場合に採用される認証種別となる。

[0053] このように、本実施例１では認証種別１～７の７段階の認証種別を設けており、認証種別７に近づくほど認証レベルが高度化している。ここでは認証種別１～７の例を示したが、各認証種別をどのような認証処理の組み合わせ

とするかは自由である。例示した認証処理の他に、指紋認証、掌紋認証などの各種の個人生体情報を組み合わせることもできる。

[0054] 図２の説明に戻ると、制御部２５は、管理装置２０の全体制御を行う。制御部２５は、認証情報管理部２５ａと、初期登録処理部２５ｂと、利用種別判定部２５ｃと、認証種別選択部２５ｄと、認証処理部２５ｅと、認証結果通知部２５ｆとを有する。実際には、これらの機能部に対応するプログラムを図示しないＲＯＭや不揮発性メモリに記憶しておき、これらのプログラムをＣＰＵにロードして実行することにより、認証情報管理部２５ａ、初期登録処理部２５ｂ、利用種別判定部２５ｃ、認証種別選択部２５ｄ、認証処理部２５ｅ及び認証結果通知部２５ｆにそれぞれ対応するプロセスを実行させることになる。

[0055] 認証情報管理部２５ａは、記憶部２４に記憶した認証情報テーブル２４ａを用いて利用者ごとの認証情報を管理する。すでに説明した通り、認証情報テーブル２４ａには、利用者の属性情報、認証情報、共有サービス等が登録されている。認証情報管理部２５ａは、これらの情報の更新処理などを行う。

[0056] 初期登録処理部２５ｂは、利用者が新たに認証システムを利用する場合の初期登録を行う。本実施例１では、新たに認証システムを利用する利用者が、携帯端末１０を用いて管理装置２０又は所定のウエブサーバから所定の認証アプリをダウンロードし、この認証アプリを携帯端末１０で起動する。そして、該認証アプリを通して、運転免許証等の確認書類、利用者の氏名等の属性情報、動画像等の認証情報、共有サービスの登録が行われる。ここでは認証アプリを用いる場合を示したが、ウエブブラウザを用いてＨＴＴＰサーバにアクセスし、ウエブブラウザ上で初期登録を行うこともできる。

[0057] 利用種別判定部２５ｃは、利用者の置かれているシーン等の種別を判定する。例えば、利用者が金融機関の住所変更、口座開設を行う場合、利用種別判定部２５ｃは、利用種別が「金融機関対応」であると判定する。また、例えば、利用者が金融機関において高額送金又は海外送金を行う場合、利用種

別判定部２５ｃは、利用種別が「高額送金」であると判定する。このように、利用者の置かれているシーンに応じた利用種別を判定する。

[0058] 認証種別選択部２５ｄは、利用種別判定部２５ｃにより判定された利用種別に対応する認証種別を選択する。例えば、利用種別判定部２５ｃにより利用種別が「高額送金」であると判定された場合、認証種別選択部２５ｄは、認証レベルの高い認証種別７を選択する。また、例えば、会社の社員食堂の自動券売機において認証種別を選択する場合、認証種別選択部２５ｄは、過去２ヶ月未満の利用がある利用者については簡易な認証処理である認証種別１を選択し、過去２ヶ月以上利用がない利用者については、認証種別２を選択する。また、例えば、認証種別選択部２５ｄは、利用者が自宅に所在する場合には認証種別２を選択し、利用者が自宅に所在しない場合には認証種別３を選択する。利用者が自宅以外に所在しているときに、氏名等の属性情報を発話させることは、個人情報保護の観点から妥当ではないからである。なお、どの利用種別の場合にどの認証種別を選択するかは、図示しないテーブルにあらかじめ記憶することができる。また、深層学習などの技術を用いて選択する設定とすることもできる。

[0059] 認証処理部２５ｅは、認証種別選択部２５ｄにより選択された認証種別に対応する認証処理を行う。例えば、認証種別選択部２５ｄにより認証種別５が選択された場合、認証処理部２５ｅは、利用者の動画像を用いて顔認証処理、音声認証処理（キーワード）、口唇認証処理を含む動的生体認証を行う。顔認証処理、音声認証処理（キーワード）、口唇認証処理の詳細な説明については省略する。

[0060] 認証結果通知部２５ｆは、認証処理部２５ｅによる認証結果を通知する。認証結果の通知先は、携帯端末１０に限定されず、金融機関の窓口端末３１、決済サーバ４３等を通知先とすることもできる。

[0061] ＜初期登録処理＞

次に、管理装置２０による初期登録処理について説明する。図６は、初期登録時の処理手順を示すフローチャートである。図７～図１０は、初期登録

時の携帯端末１０の画面例を示す図である。

[0062] 図６に示すように、初期登録を行う場合には、まず確認書類の登録が行われる（ステップＳ１０１）。具体的には、図７に示した認証アプリの画面において「新規登録」が選択操作されると、図８に示した確認書類の登録画面が表示される。例えば、免許証がカメラ枠内に入るようにして「進む」ボタンが選択操作されたならば、この免許証の画像が確認書類として管理装置２０に送信される。

[0063] その後、属性情報の登録が行われる（ステップＳ１０２）。具体的には、図９に示した属性情報の登録画面が携帯端末１０の表示部に表示される。ここで、図９に示すように、氏名「田中〇男」、住所「東京都…」、電話番号「０３（１２３４）５６７８」と入力されて「進む」ボタンが選択されたならば、入力された属性情報が管理装置２０に送信される。

[0064] その後、動画像の登録が行われる（ステップＳ１０３）。具体的には、利用者の氏名、複数のキーワード（例えば５つ）が順に携帯端末１０の表示部に表示されて、利用者がこれを発話すると、利用者の顔及び音声を含む動画像が撮像されて管理装置２０に送信される。

[0065] その後、共有サービスの登録が行われる（ステップＳ１０４）。具体的には、複数の金融機関、複数の決済システム、複数の公的機関サービスなどのうち、利用者は、認証サービスを利用する金融機関名、決済システム名、公的機関サービス名を入力することになる。例えば、図１０に示すように、金融機関名「ＡＢＣ」、支店名「赤坂」、口座番号「１２３４５６７」のように利用者の口座情報を登録し、電子マネー「ＤＥＦ」、識別番号「１１１１１１１」のように決済システムの識別番号を登録することもできる。

[0066] ＜本人認証時の管理装置２０の処理手順＞

次に、本人認証時の管理装置２０の処理手順について説明する。図１１は、本人認証時の処理手順を示すフローチャートである。ここでは、初期登録が事前に完了するとともに、携帯端末１０の認証アプリでログインが行われているものとする。例えば、携帯端末１０は、認証アプリの表示画面上に初

期登録時に登録された複数のキーワードのうちの一つを表示し、このキーワードを利用者に発話させ、その動画像を撮像する。そして、携帯端末１０は、この動画像を含む情報を管理装置２０に送信して、動画像ログインを行う。

[0067] 図１１に示すように、管理装置２０は、動画像ログインを受け付けたならば（ステップＳ２０１）、利用種別の判定を行う（ステップＳ２０２）。管理装置２０は、例えば、認証アプリを介して、金融機関における高額出金などの状況に関する情報（音声データ、テキスト）を携帯端末１０から取得する。その後、管理装置２０は、携帯端末１０から取得した情報に基づいて、利用種別を判定する。

[0068] その後、管理装置２０は、利用種別に基づいて認証種別を選択する（ステップＳ２０３）。具体的には、管理装置２０は、図４に示した認証種別１～７の中から利用種別に応じた認証種別を選択することになる。認証種別の選択は、あらかじめ設定された利用種別と認証種別の対応関係を示すテーブルを用いて行うことができる。また、管理装置２０は、深層学習を行った学習済モデルを用いて選択することもできる。

[0069] その後、管理装置２０は、選択した認証種別に応じた認証処理を行う（ステップＳ２０４）。例えば、図４に示した認証処理５が選択された場合には、図５に示した顔認証、音声認証（キーワード）及び口唇認証を含む動的生体認証が行われる。その後、認証結果が該当する送信先に通知される（ステップＳ２０５）。

[0070] 上述してきたように、本実施例１に係る認証システムでは、利用者Ａの携帯端末１０から管理装置２０にアクセスして、利用者Ａの動画像を含む初期登録が行われる。利用者Ａが金融機関ＡＢＣの店舗Ｘ又はコンビニエンスストアの店舗Ｙでサービスを受ける場合、利用者Ａを撮像した動画像が管理装置２０に送信される。管理装置２０は、利用種別に応じた認証処理を行い、認証結果を店舗に通知する。これにより、利用者Ａが各種の手続きを行う場合における本人認証を効率良く行うことができる。

[0071] 特に、本実施例１によれば、種別の異なる複数のシステムでの認証を、業態を超えて効率良く行うことができる。また、カードレス化を促進するができる。さらに、認証用の専用機器を携帯端末１０に追加する必要がなく、携帯端末１０にカメラ、マイク、通信機能があれば足りるため、利用範囲の拡大を図ることができる。

[0072] また、本認証システムは、Ｎ人の中から１人を認証する１対Ｎ認証を行う場合に適用することもできる。災害により各利用者が所持するスマートフォンを使えない場合であっても、音声付きの動画が撮像できるタブレットなどの共用端末が１台あれば、これを携帯端末１０として利用者の本人認証を行うことができるため、災害時に極めて有効である。共有システムの組み合わせ次第で、災害時における本人認証により金銭が無くとも商品を購入するよう構成することもできる。

[0073] 上記実施例１では、図４に示した顔認証、音声認証１（属性）、音声認証２（キーワード）、音声認証３（声紋）、口唇認証、虹彩認証を組み合わせた動的生体認証を行う場合を示したが、本発明はこれに限定されるものではなく、自在に各種認証処理を組み合わせることができる。また、指紋認証、掌紋認証などの各種個人認証情報を併用することもできる。

[0074] また、上記実施例１では、各種の認証処理を管理装置２０上で行う場合を示したが、本発明はこれに限定されるものではなく、認証処理を携帯端末１０上で行い、その認証結果を携帯端末１０から管理装置２０に通知することもできる。この場合には、管理装置２０から携帯端末１０に対して認証種別を通知し、この認証種別の通知を受けた携帯端末１０が認証種別に応じた認証処理を行うことになる。

[0075] また、上記実施例１では、あらかじめ初期登録を行う場合を示したが、本発明はこれに限定されるものではなく、初期登録と本人認証を連続して行うこともできる。また、上記実施例１では、利用種別に応じて認証種別を選択する場合を示したが、本発明はこれに限定されるものではなく、利用者の状況に着目して認証種別を選択するよう構成することもできる。また、利用者

と該利用者の家族とを紐付けるよう構成することもできる。さらに、利用者がインバウンド（訪日外国人）である場合に、自国においては低レベルの認証種別を選択し、日本では高いレベルの認証種別を選択するよう構成することもできる。

実施例 2

[0076] ＜実施例２に係る認証システムの概要＞

次に、Ｘ国に所在する利用者がＹ国に入国し、Ｙ国内のサービスを利用する場合における認証システムについて説明する。本実施例では、利用者Ｂがｘ国内で認証サービスの初期登録を行い、その後にＸ国を出国してＹ国に入国し、Ｙ国においてサービスを受ける場合を示している。なお、Ｙ国が日本であるものとする。

[0077] 図１２は、実施例２に係る認証システムの概要を示す図である。同図に示すように、利用者Ｂが認証システムによる認証サービスを受ける場合、利用者Ｂは、該利用者Ｂが所持する携帯端末１００を用いて管理装置１１０にアクセスし、初期登録を行う（ステップＳ１１）。初期登録においては、利用者Ｂの顔画像及び音声を含む動画像、属性情報（氏名、旅券番号、国際免許証番号等）、決済情報（クレジット情報、銀行口座情報、ペイメント手段等）等が登録される。

[0078] その後、利用者Ｂは利用サービス予約を行う（ステップＳ１２）。利用サービス予約では、サービス種別、期間、利用手段等が登録される。例えば、インバウンドが日本において民泊を利用する場合には、サービス種別「民泊」、期間「２０１９年２月１日～２月１０日」、利用手段「二次元バーコード」が登録される。

[0079] 管理装置１１０は、サービス管理会社のサービス管理装置１２０にサービス予約を行う（ステップＳ１３）。サービス管理会社が、該当するサービスを提供できる場合には、サービス管理装置１２０が管理装置１１０に対して許可情報を返信する（ステップＳ１４）。許可情報には、例えば民泊を利用する場合の鍵となる２次元バーコードの情報が含まれる。

[0080] そして、利用者Ｂは、Ｙ国すなわち日本に入国して民泊を利用する場合に、携帯端末１００の認証アプリを起動して管理装置１１０にアクセスし、利用者Ｂの動画像の送信を含むサービス利用要求の処理を行う（ステップＳ１５）。サービス利用要求を受けた管理装置１１０は、受信した動画像を用いて本人認証を行う（ステップＳ１６）。このとき、管理装置１１０は、実施例１に示した動的生体認証を用いた認証処理を行うことができる。その結果、正しく本人認証が行われたならば、管理装置１１０は、サービス許可情報を携帯端末１００に送信する（ステップＳ１７）。サービス許可情報には、例えば民泊の鍵となる二次元バーコードが含まれる。

[0081] 携帯端末１００は、管理装置１１０からサービス許可情報を受信したならば、このサービス許可情報を端末内の記憶部に記憶して（ステップＳ１８）、サービスに利用する（ステップＳ１９）。民泊の場合には、民泊を行う家屋又はマンションの鍵が二次元バーコードで開錠可能な構成とされている。利用者Ｂは、サービス許可情報に含まれる二次元バーコードを用いて家屋又はマンションの鍵を開錠することができる。なお、利用サービス予約で登録した期間経過前に携帯端末１００にアラートが出され（ステップＳ２０）、期間経過後は鍵の開錠を不能とするようになっている。

[0082] 上述してきたように、本実施例２の認証システムでは、訪日外国人が日本国内で効率良く本人認証することができる。このため、訪日外国人は、日本国内で効率的にサービスを受けることが可能となる。例えば、訪日外国人が民泊を利用する場合には、該当する家屋又はマンションに直接赴き、サービス許可情報に含まれる二次元バーコードを用いて開錠することが可能となる。なお、サービスに要した費用は、初期登録時に登録した決済システムから徴収することができる。

[0083] ＜管理装置１１０の構成＞

次に、図１２に示した管理装置１１０の構成について説明する。図１３は、図１２に示した管理装置１１０の構成を示す機能ブロック図である。同図に示すように、管理装置１１０は、入力部１１１、表示部１１２、通信Ｉ／

Ｆ部１１３、記憶部１１４及び制御部１１５を有する。

[0084] 入力部１１１は、キーボードやマウス等の入力デバイスである。表示部１１２は、液晶パネルやディスプレイ装置等の表示デバイスである。通信Ｉ／Ｆ部１１３は、携帯端末１００及びサービス管理装置１２０等との通信を行う。

[0085] 記憶部１１４は、ハードディスク装置又は不揮発性メモリ等の２次記憶部である記憶部１１４は、利用者情報テーブル１１４ａ及びサービス情報管理テーブル１１４ｂを記憶する。利用者情報テーブル１１４ａは、利用者を一意に識別する利用者識別情報ごとに、属性情報、認証情報及び予約サービス情報等を含む。属性情報には、利用者の氏名、旅券番号、電話番号等の個人情報が含まれる。認証情報には、利用者の顔及び音声を含む動画像等が含まれる。予約サービス情報には、利用者が予約したサービスに係る情報が含まれる。サービス情報管理テーブル１１４ｂは、利用者に対して提供可能な各種サービスのサービス管理装置１２０のアクセス先情報などを管理するテーブルである。

[0086] 制御部１１５は、管理装置１１０の全体制御を行う。制御部１１５は、利用者情報管理部１１５ａと、初期登録処理部１１５ｂと、利用サービス予約処理部１１５ｃと、許可情報取得部１１５ｄと、認証処理部１１５ｅと、サービス許可情報通知部１１５ｆとを有する。実際には、これらの機能部に対応するプログラムを図示しないＲＯＭや不揮発性メモリに記憶しておき、これらのプログラムをＣＰＵにロードして実行することにより、利用者情報管理部１１５ａ、初期登録処理部１１５ｂ、利用サービス予約処理部１１５ｃ、許可情報取得部１１５ｄ、認証処理部１１５ｅ及びサービス許可情報通知部１１５ｆにそれぞれ対応するプロセスを実行させることになる。

[0087] 利用者情報管理部１１５ａは、記憶部１１４に記憶した利用者情報テーブル１１４ａを用いて利用者ごとの情報を管理する。すでに説明した通り、利用者情報テーブル１１４ａには、利用者の属性情報、認証情報、予約サービス情報等が登録されている。利用者情報管理部１１５ａは、これらの情報の

更新処理などを行う。

[0088] 初期登録処理部１１５ｂは、利用者が新たに認証システムを利用する場合の初期登録を行う。具体的には、認証アプリを通して、パスポート又は国際免許証等の確認書類、利用者の氏名等の属性情報、動画像等の認証情報、決済情報の登録が行われる。ここでは認証アプリを用いる場合を示したが、ウエブブラウザを用いてＨＴＴＰサーバにアクセスし、ウエブブラウザ上で初期登録を行うこともできる。

[0089] 利用サービス予約処理部１１５ｃは、利用者が利用するサービスの予約を行う。利用サービス予約処理部１１５ｃは、利用サービス種別、期間、利用手段の予約を行う。許可情報取得部１１５ｄは、利用者から予約されたサービスに対応するサービス管理装置１２０から許可情報を取得する。許可情報には、例えば民泊の鍵となる２次元バーコードが含まれる。

[0090] 認証処理部１１５ｅは、動画像を用いた動的生体認証を行う。動的生体認証の詳細については実施例１と同様であるので、その詳細な説明を省略する。サービス許可情報通知部１１５ｆは、利用者の携帯端末１００に対してサービス許可情報を通知する。サービス許可情報には、例えば民泊を利用する場合の鍵となる２次元バーコードが含まれる。

[0091] ＜初期登録処理＞

次に、図１３に示した管理装置１１０による初期登録処理について説明する。図１４は、図１３に示した管理装置１１０による初期登録時の処理手順を示すフローチャートである。同図に示すように、まず属性情報が登録される（ステップＳ３０１）。属性情報には、パスポート又は国際免許証の画像、氏名、旅券番号、電話番号などが含まれる。

[0092] その後、携帯端末１００を用いて顔と音声を含む動画像が撮像され、撮像された動画像が登録される（ステップＳ３０２）。動画像を撮像する場合には、携帯端末１００が、氏名及び複数のキーワードを利用者に発話させ、それぞれの動画像を登録することになる。

[0093] その後、利用者の決済情報が登録される（ステップＳ３０３）。具体的に

は、金融機関の金融機関名、支店名及び口座番号、電子マネーの識別番号などが登録されることになる。

[0094] ＜サービス予約時の管理装置１１０の処理手順＞

次に、サービス予約時の管理装置１１０の処理手順について説明する。図１５は、サービス予約時の管理装置１１０の処理手順を示すフローチャートである。ここでは、初期登録が事前に完了しているものとする。例えば、携帯端末１００は、認証アプリの表示画面上に初期登録時に登録された複数のキーワードのうちの一つを表示し、このキーワードを利用者に発話させ、その動画像を撮像する。そして、携帯端末１００は、この動画像を含む情報を管理装置１１０に送信して、動画像ログインを行う。

[0095] 管理装置１１０は、動画像ログインを受け付けたならば（ステップＳ４０１）、動画像を用いた動的生体情報による認証処理を行う（ステップＳ４０２）。その結果、正当な本人ではないと認証された場合には（ステップＳ４０３；Ｎｏ）、管理装置１１０は、エラー処理を行って（ステップＳ４０４）、処理を終了する。

[0096] これに対して、正当な本人であると認証された場合には（ステップＳ４０３；Ｙｅｓ）、管理装置１１０は、利用サービスの種別（例えば、民泊の利用）を受け付け（ステップＳ４０５）、利用期間を受け付ける（ステップＳ４０６）。

[0097] その後、管理装置１１０は、該当するサービス管理装置１２０にアクセスして許可情報を取得し（ステップＳ４０７）、予約情報を利用者情報テーブル１１４ａに登録して（ステップＳ４０８）、上記一連の処理を終了する。

[0098] ＜サービス処理時の管理装置１１０の処理手順＞

利用者がサービスを受ける場合、管理装置１１０は、サービス予約時と同様にして動画像ログインを受け付ける。その後、管理装置１１０は、動画像を用いた動的生体情報による認証処理を行ない、正当な本人であると認証された場合には、サービス許可情報を携帯端末１００に通知する。

[0099] 上述してきたように、本実施例２の認証システムでは、訪日外国人が日本

国内で効率良く本人認証することができる。このため、訪日外国人は、日本国内で効率的にサービスを受けることが可能となる。例えば、訪日外国人が民泊を利用する場合には、該当する家屋又はマンションに直接赴き、サービス許可情報に含まれる二次元バーコードを用いて開錠することが可能となる。なお、サービスに要した費用は、初期登録時に登録した決済システムから徴収することができる。

[0100] 上記実施例２では、２次元バーコードで開錠可能な民泊を利用する場合を示したが、本発明はこれに限定されるものではなく、近距離無線通信を用いて鍵を開錠する場合にも適用することができる。また、サービス種別は民泊に限定されるものではなく、ホテル予約やカーシェアに利用することもできる。

[0101] また、本人を特定するために、公的証明書から取得した住所に本人限定受け取り郵便物を送付して利用者の本人確認を行い、その郵送物に付した認証用ＵＲＬを記した２次元バーコードなどで利用者を検証サイトに誘導し、再度顔認証、音声認証などを行うことで、より一層なりすましを防止するように構成することもできる。

[0102] 上記の実施例１又は２で図示した各構成は機能概略的なものであり、必ずしも物理的に図示の構成をされていることを要しない。すなわち、各装置の分散・統合の形態は図示のものに限られず、その全部又は一部を各種の負荷や使用状況などに応じて、任意の単位で機能的又は物理的に分散・統合して構成することができる。

産業上の利用可能性

[0103] 本発明に係る認証システム、管理装置及び認証方法は、利用者が各種の手続きを行う場合における本人認証を効率良く行う場合に有用である。

符号の説明

[0104] Ａ、Ｂ　利用者

１０　携帯端末

２０　管理装置

２１　入力部

２２　表示部

２３　通信Ｉ／Ｆ部

２４　記憶部

２４ａ　認証情報テーブル

２４ｂ　認証種別管理テーブル

２５　制御部

２５ａ　認証情報管理部

２５ｂ　初期登録処理部

２５ｃ　利用種別判定部

２５ｄ　認証種別選択部

２５ｅ　認証処理部

２５ｆ　認証結果通知部

３１　窓口端末

３２　金融機関サーバ

４１　ＰＯＳ端末

４２　撮像装置（カメラ）

４３　決済サーバ

４４　公的機関サーバ

１００　携帯端末

１１０　管理装置

１１１　入力部

１１２　表示部

１１３　通信Ｉ／Ｆ部

１１４　記憶部

１１４ａ　利用者情報テーブル

１１４ｂ　サービス情報管理テーブル

１１５　制御部

１１５ａ　利用者情報管理部

１１５ｂ　初期登録処理部

１１５ｃ　利用サービス予約処理部

１１５ｄ　許可情報取得部

１１５ｅ　認証処理部

１１５ｆ　サービス許可情報通知部

１２０　サービス管理装置

請求の範囲

[請求項1] 利用者を認証するための複数の認証情報を管理する認証情報管理手段を有する認証システムであって、

所定の利用種別を判定する利用種別判定手段と、

前記利用種別判定手段によって判定された利用種別に対応する認証種別を複数の認証種別から選択する認証種別選択手段と、

前記認証種別選択手段により選択された認証種別に基づいて前記利用者の認証処理を行う認証処理手段と、

前記認証処理手段による前記利用者の認証結果を通知する通知手段と

を備える認証システム。

[請求項2] 前記認証処理手段は、前記利用者の顔部分と該利用者の音声を含む動画像を用いた動的生体認証を少なくとも含む認証処理を行う請求項１に記載の認証システム。

[請求項3] 前記動的生体認証は、

前記動画像に含まれる前記利用者の顔画像に基づく顔認証処理と、前記動画像に含まれる前記利用者の音声情報に基づく音声認証処理とを含む認証処理を行う請求項２に記載の認証システム。

[請求項4] 前記顔認証処理は、

前記動画像に含まれる前記利用者の顔画像と、前記認証情報管理手段により管理された認証情報に含まれる顔画像とを照合する処理である請求項３に記載の認証システム。

[請求項5] 前記認証情報管理手段により管理された認証情報は、公的機関により発行された利用者の顔画像を含む証明書に係る情報である請求項３又は４に記載の認証システム。

[請求項6] 前記音声認証処理は、

前記利用者により発話された音声が示す該利用者に係る属性情報と、前記認証情報管理手段により管理された認証情報に含まれる属性情

報とを照合する処理である請求項３又は４に記載の認証システム。

[請求項7] 前記音声認証処理は、

前記利用者により発話された音声が示すキーワードと、該利用者に対して発話を求めた所定のキーワードとを照合する処理である請求項３に記載の認証システム。

[請求項8] 前記音声認証処理は、

前記利用者により発話された音声に含まれる該利用者の声紋情報と、前記認証情報管理手段により管理された認証情報に含まれる声紋情報とを照合する処理である請求項３に記載の認証システム。

[請求項9] 前記動的生体認証は、

前記動画像に含まれる前記利用者の口唇の動きが、該動画像に含まれる前記利用者の音声が示すキーワードと一致するかを認証する口唇認証を含む請求項３に記載の認証システム。

[請求項10] 前記認証処理手段における認証処理は、

前記利用者が所持する携帯端末と通信可能な管理装置において実行される請求項１乃至９のいずれか一つに記載の認証システム。

[請求項11] 前記認証処理手段における認証処理は、

前記利用者が所持する携帯端末において実行される請求項１乃至９のいずれか一つに記載の認証システム。

[請求項12] 前記認証情報管理手段において管理される認証情報は、

前記利用者が所持する携帯端末から登録可能である請求項１乃至１１のいずれか一つに記載の認証システム。

[請求項13] 利用者を認証するための複数の認証情報を管理する認証情報管理手段を有する管理装置であって、

所定の利用種別を判定する利用種別判定手段と、

前記利用種別判定手段によって判定された利用種別に対応する認証種別を複数の認証種別から選択する認証種別選択手段と、

前記認証種別選択手段により選択された認証種別に基づいて前記利

用者の認証処理を行う認証処理手段と、

前記認証処理手段による前記利用者の認証結果を通知する通知手段と

を備える管理装置。

[請求項14] 利用者を認証するための複数の認証情報を管理する認証情報管理手段を有する認証システムにおける認証方法であって、

所定の利用種別を判定する利用種別判定工程と、

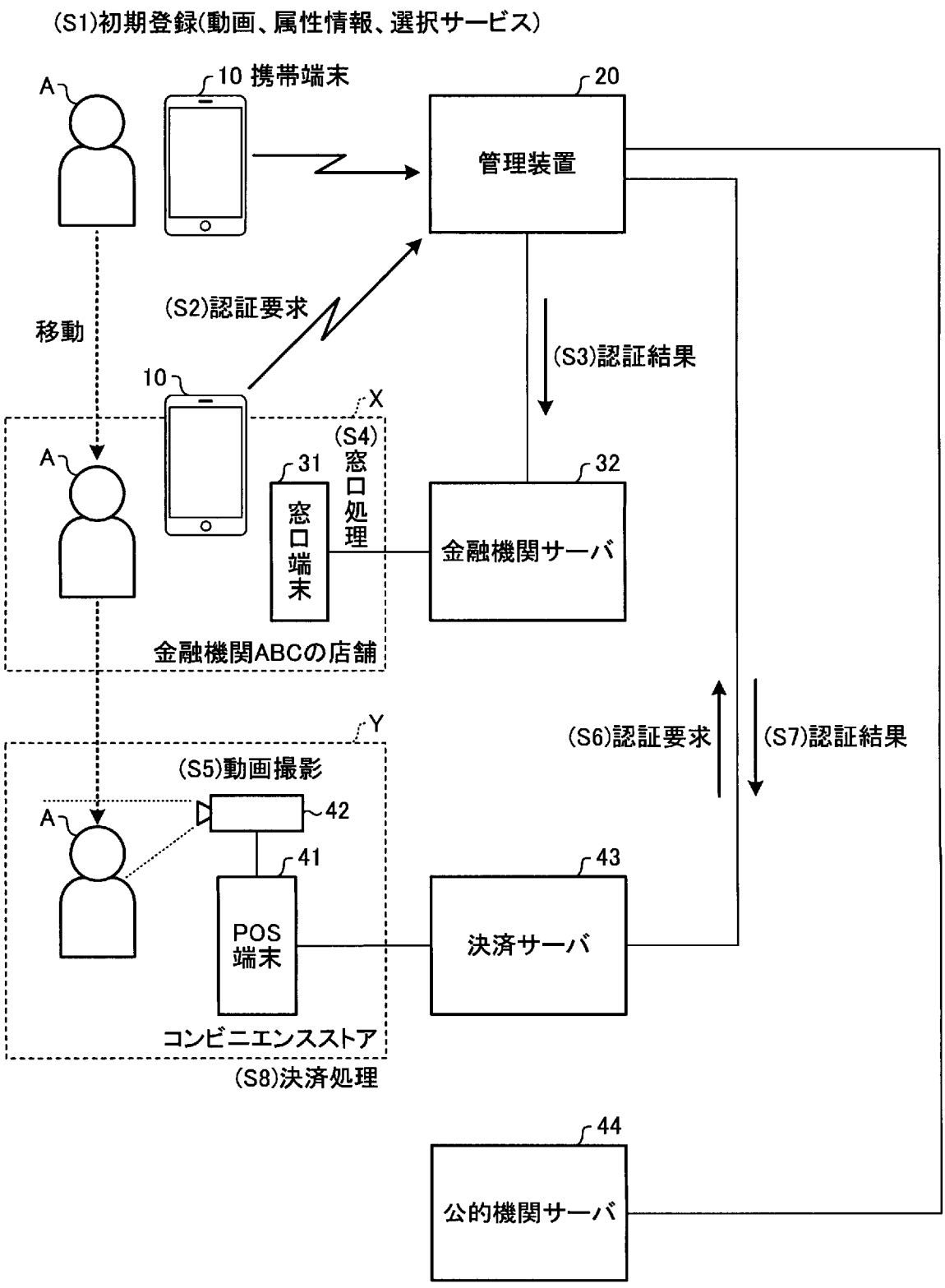
前記利用種別判定工程によって判定された利用種別に対応する認証種別を複数の認証種別から選択する認証種別選択工程と、

前記認証種別選択工程により選択された認証種別に基づいて前記利用者の認証処理を行う認証処理工程と、

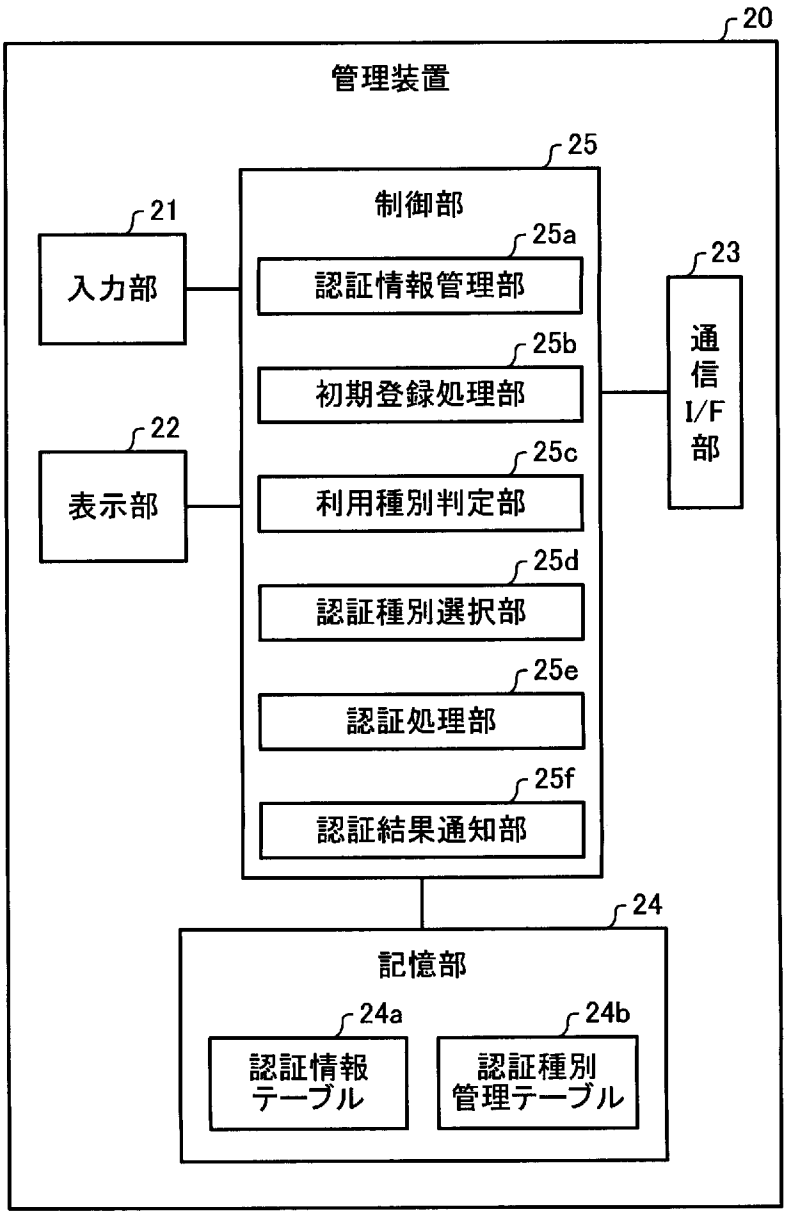
前記認証処理工程による前記利用者の認証結果を通知する通知工程と

を含む認証方法。

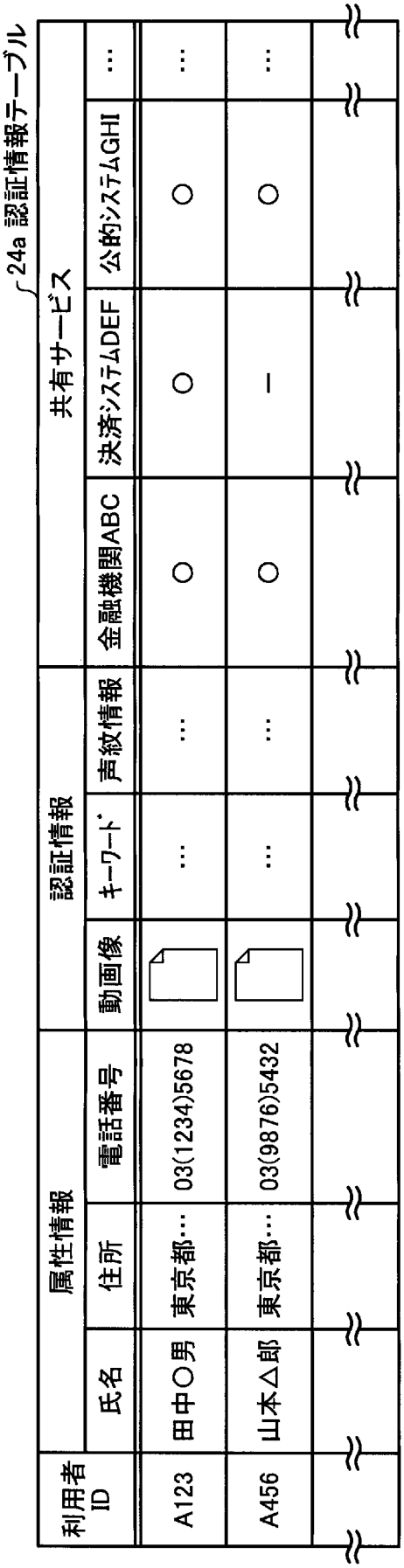
[図1]


(S1)初期登録(動画、属性情報、選択サービス)
A
10 携帯端末
20
管理装置
移動
(S2)認証要求
(S3)認証結果
10
X
(S4)
窓口処理
31
窓口端末
32
金融機関サーバ
金融機関ABCの店舗
Y
(S5)動画撮影
42
41
POS端末
43
決済サーバ
コンビニエンスストア
(S6)認証要求
(S7)認証結果
(S8)決済処理
44
公的機関サーバ

[図2]


20
管理装置
25
制御部
25a
認証情報管理部
25b
初期登録処理部
25c
利用種別判定部
25d
認証種別選択部
25e
認証処理部
25f
認証結果通知部
21
入力部
22
表示部
23
通信I/F部
24
記憶部
24a
認証情報テーブル
24b
認証種別管理テーブル

[図3]

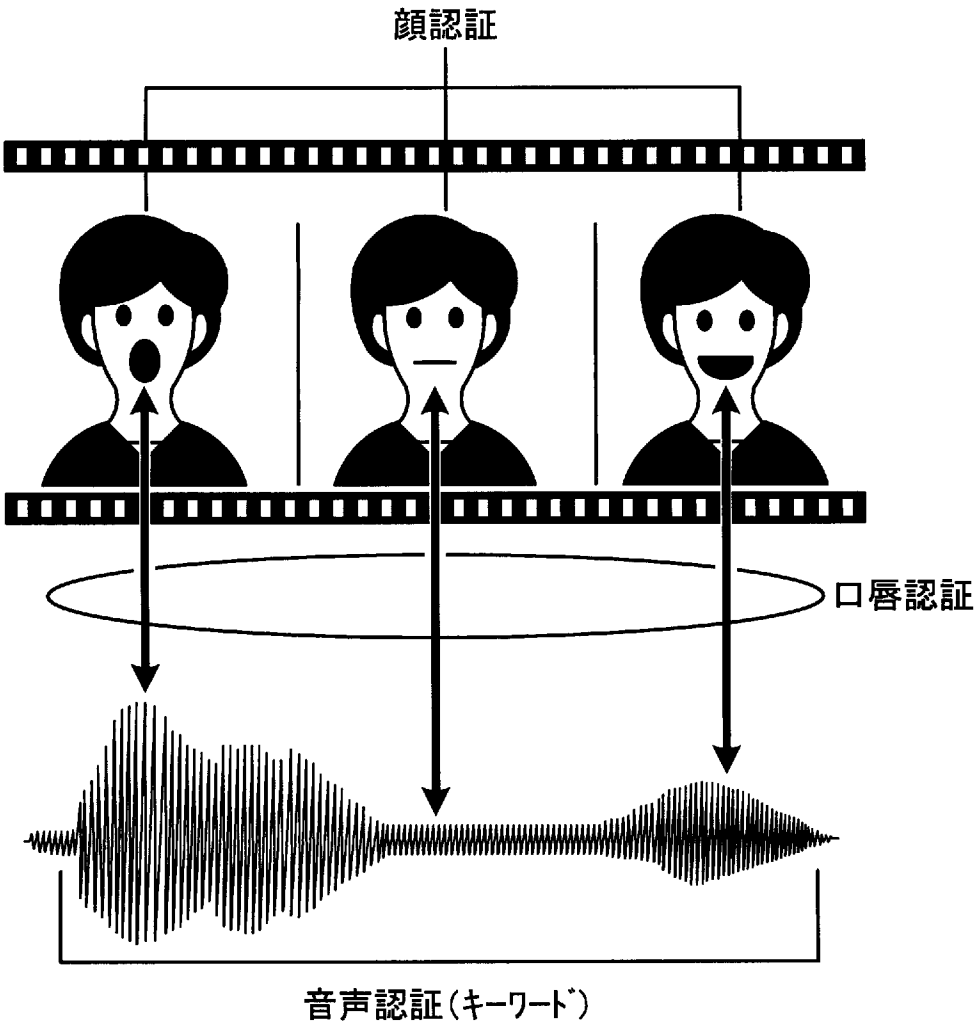

24a 認証情報テーブル
利用者ID
属性情報
氏名
住所
電話番号
認証情報
動画像
キーワード
声紋情報
共有サービス
金融機関ABC
決済システムDEF
公的システムGHI
A123
田中〇男
東京都…
03(1234)5678
…
…
〇
〇
A456
山本△郎
東京都…
03(9876)5432
…
…
〇
－
〇

[図4]

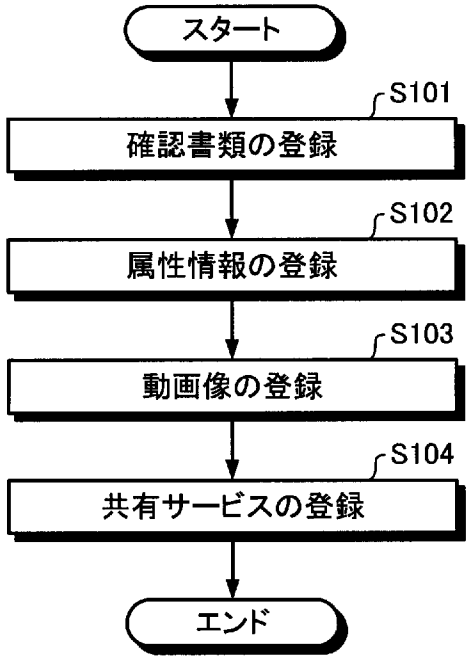
24b 認証種別管理テーブル

認証種別	顔認証	音声認証1（属性）	音声認証2（キーワード）	音声認証3（声紋）	口唇認証	虹彩認証
1	○	－	－	－	－	－
2	○	○	－	－	－	－
3	○	－	○	－	－	－
4	○	－	－	○	－	－
5	○	－	○	－	○	－
6	○	－	－	○	○	－
7	○	－	○	○	○	○

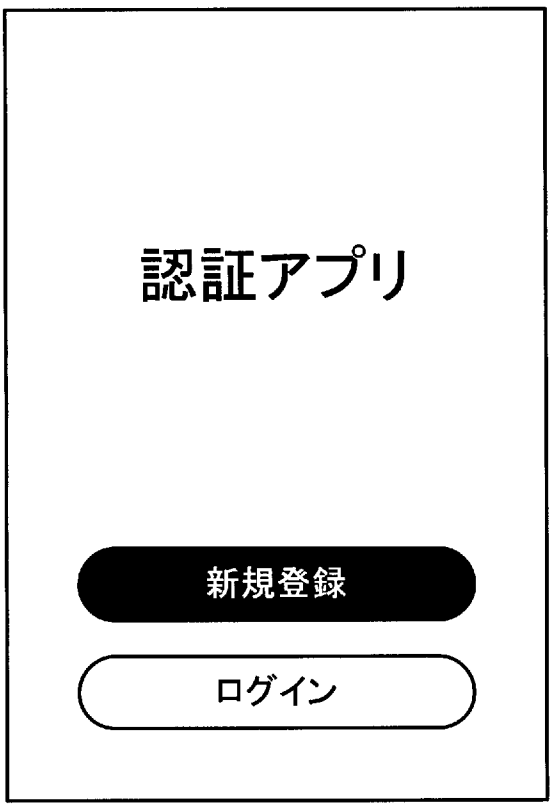
[図5]



[図6]


スタート
S101
確認書類の登録
S102
属性情報の登録
S103
動画像の登録
S104
共有サービスの登録
エンド

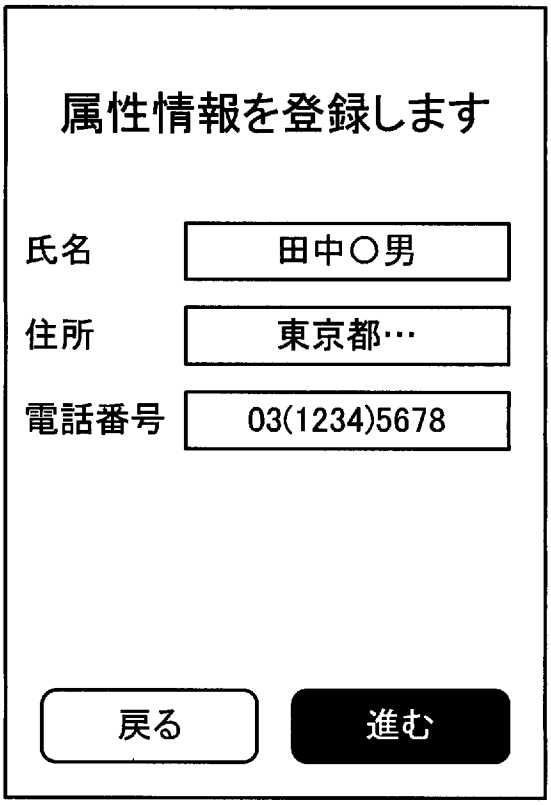
[図7]


認証アプリ
新規登録
ログイン

[図8]


確認書類を登録します
氏名
田中〇男
住所
東京都…
交付
平成 〇〇年 〇〇月 〇〇日 12345
運転免許証
優良
第 123456789000 号
平成 〇〇年 〇〇月 〇〇日
平成 〇〇年 〇〇月 〇〇日
平成 〇〇年 〇〇月 〇〇日
〇〇
公安委員会
戻る
進む

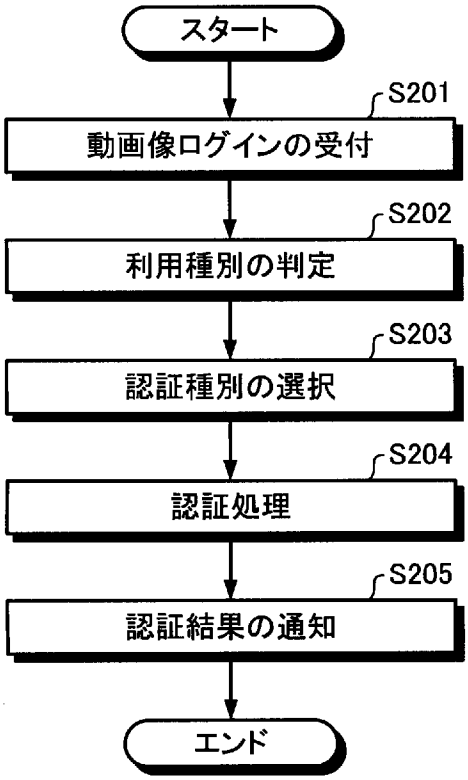
[図9]


属性情報を登録します
氏名
田中〇男
住所
東京都…
電話番号
03(1234)5678
戻る
進む

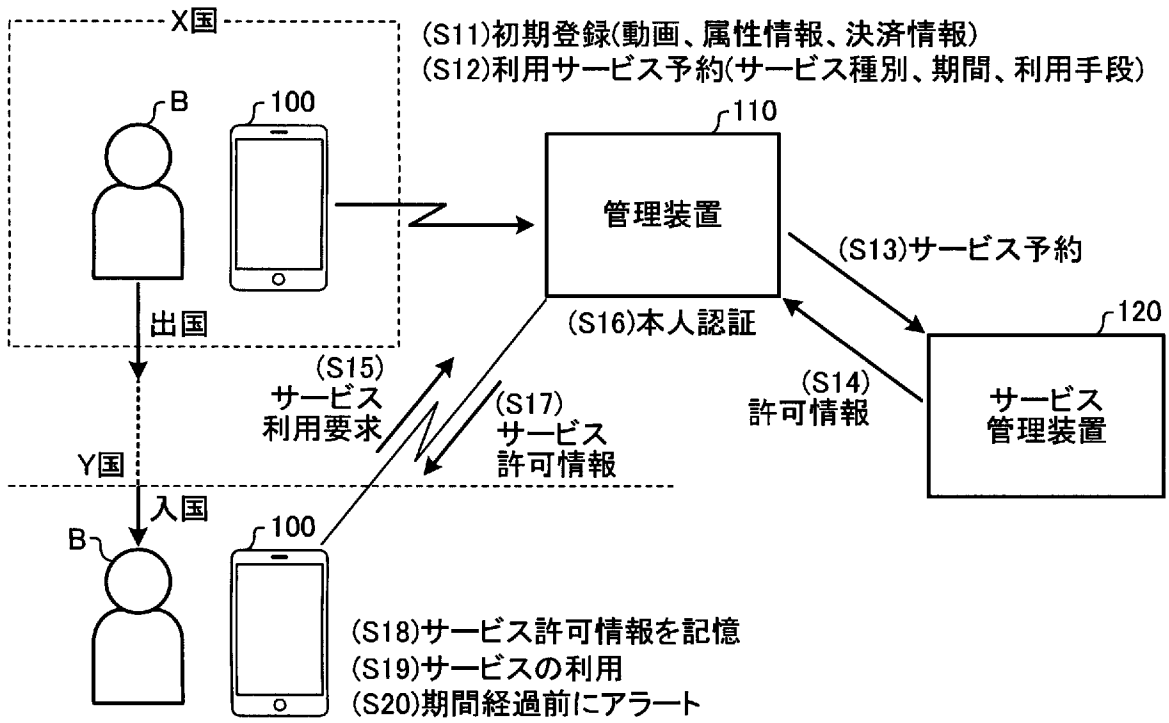
[図10]


共有サービスを登録します
・金融機関
ABC
支店名
赤坂
口座番号
1234567
・電子マネー
DEF
識別番号
1111111

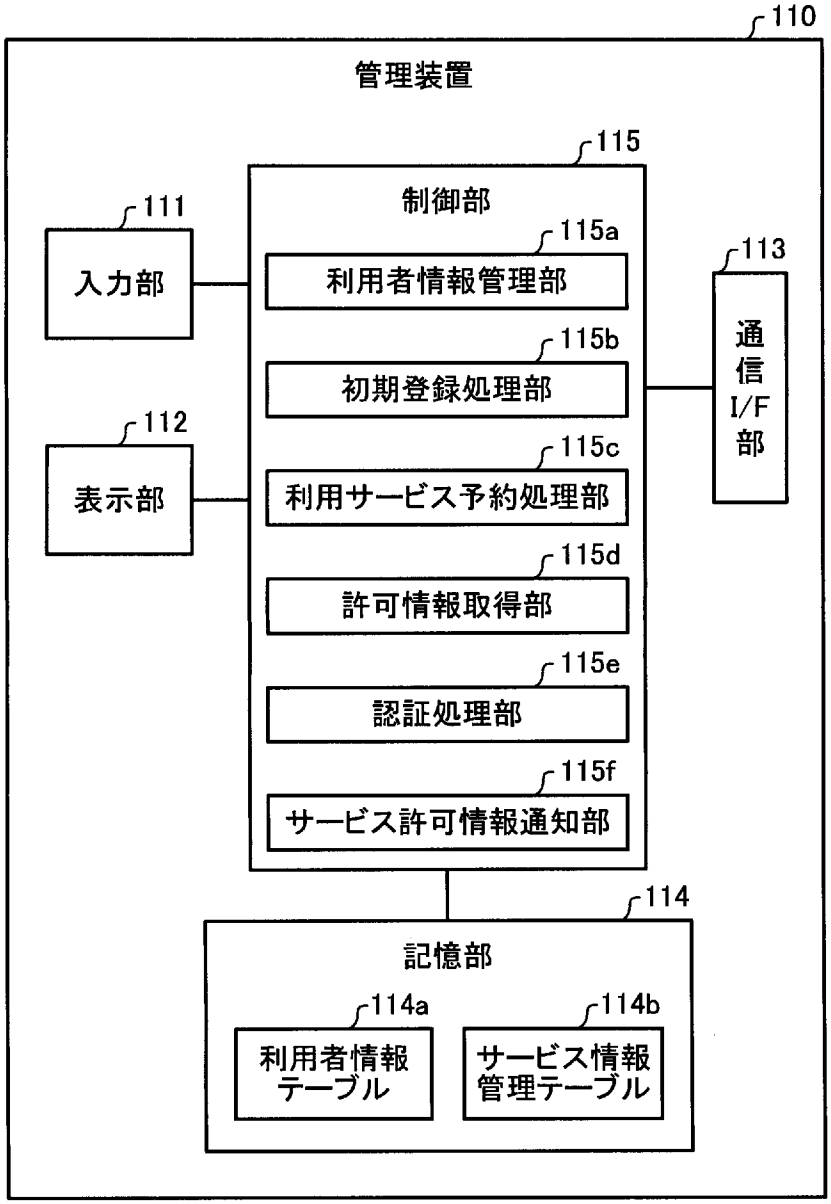
[図11]


スタート
S201
動画像ログインの受付
S202
利用種別の判定
S203
認証種別の選択
S204
認証処理
S205
認証結果の通知
エンド

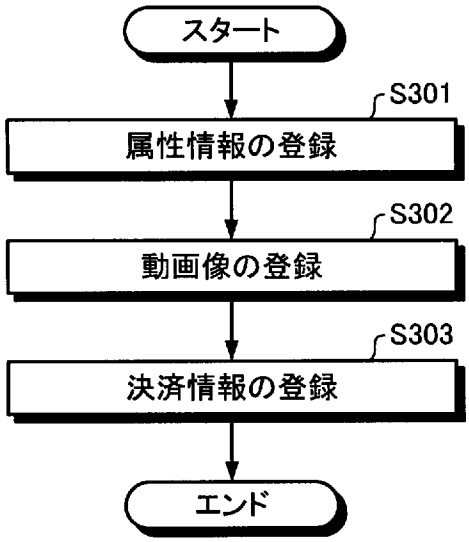
[図12]


X国
B
100
(S11)初期登録(動画、属性情報、決済情報)
(S12)利用サービス予約(サービス種別、期間、利用手段)
110
管理装置
(S13)サービス予約
120
出国
(S16)本人認証
(S15)
サービス
利用要求
(S17)
サービス
許可情報
(S14)
許可情報
サービス
管理装置
Y国
入国
B
100
(S18)サービス許可情報を記憶
(S19)サービスの利用
(S20)期間経過前にアラート

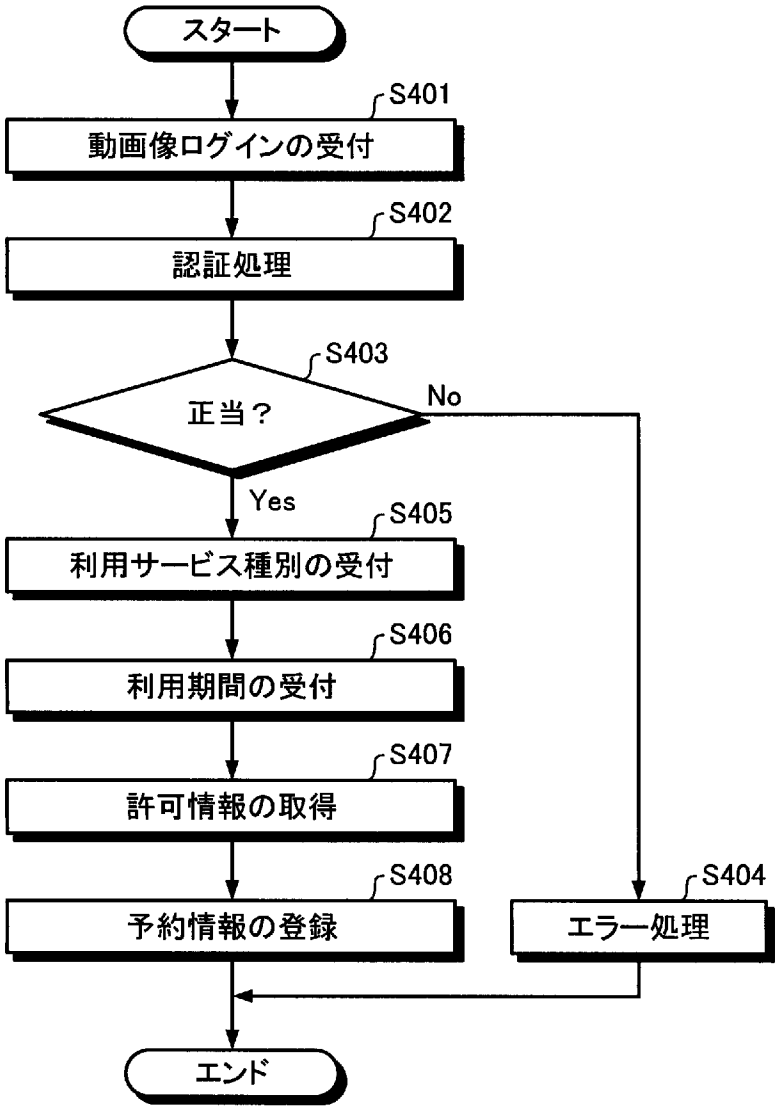
[図13]


110
管理装置
115
制御部
111
入力部
115a
利用者情報管理部
113
通信I/F部
115b
初期登録処理部
112
表示部
115c
利用サービス予約処理部
115d
許可情報取得部
115e
認証処理部
115f
サービス許可情報通知部
114
記憶部
114a
利用者情報テーブル
114b
サービス情報管理テーブル

[図14]



[図15]


スタート
S401
動画像ログインの受付
S402
認証処理
S403
正当？
No
Yes
S405
利用サービス種別の受付
S406
利用期間の受付
S407
許可情報の取得
S408
予約情報の登録
S404
エラー処理
エンド

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/051070

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. G06T7/00(2017.01)i, G06T7/20(2017.01)i, G06F21/31(2013.01)i, G06F21/32(2013.01)i, G06Q50/10(2012.01)i
FI: G06F21/31, G06F21/32, G06T7/20 300B, G06T7/00 P, G06T7/00 510F, G06Q50/10
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int. Cl. G06T7/00, G06T7/20, G06F21/31, G06F21/32, G06Q50/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2020
Registered utility model specifications of Japan 1996-2020
Published registered utility model applications of Japan 1994-2020

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2008-040961 A (TOPPAN PRINTING CO., LTD.) 21 February 2008, paragraphs [0010]-[0023]	1, 10-14 2-9
Y	JP 2004-259255 A (FUJI PHOTO FILM CO., LTD.) 16 September 2004, paragraphs [0025], [0048]-[0054]	2-9
Y	JP 2000-090329 A (OKI SOFTWARE KK) 31 March 2000, paragraphs [0013]-[0020], [0025]	5
Y	JP 2004-139221 A (NTT DOCOMO TOKAI INC.) 13 May 2004, paragraphs [0039]-[0055]	7

☐ Further documents are listed in the continuation of Box C.
☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26.02.2020	10.03.2020
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2019/051070

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
JP 2008-040961 A	21.02.2008	(Family: none)	
JP 2004-259255 A	16.09.2004	US 2004/0151348 A1 paragraphs [0035], [0058]-[0064]	
JP 2000-090329 A	31.03.2000	(Family: none)	
JP 2004-139221 A	13.05.2004	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2019/051070

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06T 7/00(2017.01)i; G06T 7/20(2017.01)i; G06F 21/31(2013.01)i; G06F 21/32(2013.01)i; G06Q 50/10(2012.01)i
FI: G06F21/31; G06F21/32; G06T7/20 300B; G06T7/00 P; G06T7/00 510F; G06Q50/10

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

G06T7/00; G06T7/20; G06F21/31; G06F21/32; G06Q50/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X	JP 2008-040961 A (凸版印刷株式会社) 21.02.2008 (2008-02-21) 段落００１０－００２３	１，１０－１４
Y		２－９
Y	JP 2004-259255 A (富士写真フイルム株式会社) 16.09.2004 (2004-09-16) 段落００２５、００４８－００５４	２－９
Y	JP 2000-090329 A (沖ソフトウェア株式会社) 31.03.2000 (2000-03-31) 段落００１３－００２０，００２５	５
Y	JP 2004-139221 A (株式会社エヌ・ティ・ティ・ドコモ東海) 13.05.2004 (2004-05-13) 段落００３９－００５５	７

☐ Ｃ欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
“A” 特に関連のある文献ではなく、一般的技術水準を示すもの
“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
“O” 口頭による開示、使用、展示等に言及する文献
“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの
“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
“Y” 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
“&” 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
26.02.2020	10.03.2020

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
和平　悠希 5S 5380

電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2019/051070

引用文献	公表日	パテントファミリー文献	公表日
JP 2008-040961 A	21.02.2008	（ファミリーなし）	
JP 2004-259255 A	16.09.2004	US 2004/0151348 A1 段落００３５，００５８－００６４	
JP 2000-090329 A	31.03.2000	（ファミリーなし）	
JP 2004-139221 A	13.05.2004	（ファミリーなし）	