

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7540253号
(P7540253)

(45)発行日 令和6年8月27日(2024.8.27)

(24)登録日 令和6年8月19日(2024.8.19)

(51)国際特許分類 F I
G 0 6 Q 40/02 (2023.01) G 0 6 Q 40/02

請求項の数 4 (全12頁)

(21)出願番号	特願2020-151583(P2020-151583)	(73)特許権者	000002897 大日本印刷株式会社 東京都新宿区市谷加賀町一丁目1番1号
(22)出願日	令和2年9月9日(2020.9.9)	(74)代理人	100096091 弁理士 井上 誠一
(65)公開番号	特開2022-45799(P2022-45799A)	(72)発明者	安達 俊介 東京都新宿区市谷加賀町一丁目1番1号 大日本印刷株式会社内
(43)公開日	令和4年3月22日(2022.3.22)	審査官	宮地 匡人
審査請求日	令和5年7月27日(2023.7.27)		

最終頁に続く

(54)【発明の名称】 本人確認支援装置およびプログラム

(57)【特許請求の範囲】

【請求項1】

ユーザ端末から本人確認用の画像と前記画像の撮影時の前記ユーザ端末の位置情報を受信する受信手段と、

ユーザの住所情報を取得する取得手段と、

本人確認のため、前記ユーザ端末の位置情報と前記ユーザの住所情報を比較する比較手段と、

を有し、

前記比較手段は、さらに、前記ユーザの住所情報を、避けるべき所定の住所群と比較し、
前記比較手段は、前記ユーザ端末の位置情報と前記ユーザの住所情報が一致せず、且つ前記ユーザの住所情報と前記所定の住所群中の全ての住所とが一致しない場合、前記ユーザ端末の位置情報と、前記ユーザの住所情報と、前記所定の住所群中の住所とを地図上で示した表示画面を表示することを特徴とする本人確認支援装置。

10

【請求項2】

前記画像は、本人確認証の画像であることを特徴とする請求項1記載の本人確認支援装置。

【請求項3】

前記比較手段は、GPS情報である前記ユーザ端末の位置情報をテキストに変換し、テキストに変換した前記ユーザ端末の位置情報と、テキストである前記ユーザの住所情報との一致度を、前記ユーザ端末の位置情報のテキストと前記ユーザの住所情報のテキストに基

20

づき算出することを特徴とする請求項 1 または請求項 2 に記載の本人確認支援装置。

【請求項 4】

コンピュータを、
 ユーザ端末から本人確認用の画像と前記画像の撮影時の前記ユーザ端末の位置情報を受信する受信手段と、
 ユーザの住所情報を取得する取得手段と、
 本人確認のため、前記ユーザ端末の位置情報と前記ユーザの住所情報を比較する比較手段と、
 を有し、

前記比較手段は、さらに、前記ユーザの住所情報を、避けるべき所定の住所群と比較し、
 前記比較手段は、前記ユーザ端末の位置情報と前記ユーザの住所情報が一致せず、且つ前記ユーザの住所情報と前記所定の住所群中の全ての住所とが一致しない場合、前記ユーザ端末の位置情報と、前記ユーザの住所情報と、前記所定の住所群中の住所とを地図上で示した表示画面を表示する本人確認支援装置として機能させるためのプログラム。

10

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、本人確認支援装置とそのプログラムに関する。

【背景技術】

【0002】

金融機関では口座開設時に運転免許証等のIDカード（本人確認証）による本人確認が必要であり、これにより特殊詐欺などの犯罪目的で不正に口座開設が行われるのを防いでいる。

20

【0003】

近年、不正な口座開設のためにIDカードを偽造するケースが増えつつあるが、通常の金融機関では、申請者が金融機関に出向いてIDカードを提出し、金融機関側は提出されたIDカードを用いて対面により本人確認するのが一般的である。この場合、IDカードをじっくりと観察でき、申請者の挙動やカードの触感からも不正を感知できる。

【0004】

また特許文献 1 にはIDカードの券面をスキャナで撮影した画像からIDカードの真贋を判定する真贋判定装置が記載されており、提出されたIDカードをスキャナで読取ることIDカードの真贋判定を行うことも可能である。

30

【先行技術文献】

【特許文献】

【0005】

【文献】特開2011-34535号公報

【発明の概要】

【発明が解決しようとする課題】

【0006】

最近では来店不要なオンラインでの口座開設も一般的になってきており、スマートフォン等のカメラでIDカードの券面を撮影し、その画像を金融機関に送ることで本人確認が行われるものもある。この場合、本人確認は対面でなく画像だけで行われるので、不正を防ぐための工夫が望まれている。

40

【0007】

本発明は上記の問題に鑑みてなされたものであり、本人確認を好適に行うことのできる本人確認支援装置等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】

前述した課題を解決するための第 1 の発明は、ユーザ端末から本人確認用の画像と前記画像の撮影時の前記ユーザ端末の位置情報を受信する受信手段と、ユーザの住所情報を取

50

得する取得手段と、本人確認のため、前記ユーザ端末の位置情報と前記ユーザの住所情報を比較する比較手段と、を有し、前記比較手段は、さらに、前記ユーザの住所情報を、避けるべき所定の住所群と比較し、前記比較手段は、前記ユーザ端末の位置情報と前記ユーザの住所情報が一致せず、且つ前記ユーザの住所情報と前記所定の住所群中の全ての住所とが一致しない場合、前記ユーザ端末の位置情報と、前記ユーザの住所情報と、前記所定の住所群中の住所とを地図上で示した表示画面を表示することを特徴とする本人確認支援装置である。

【0009】

本発明では、ユーザ端末から本人確認証の撮影画像など本人確認用の画像を受信した際に、当該画像の撮影時のユーザ端末の位置情報とユーザの住所情報の比較を行う。これらが一致しない場合、ユーザは、撮影環境が比較的整っており且つ自らが慣れた自宅で画像の撮影を行わず、わざわざ外に出て撮影を行っていることになるので、何らかの不正を疑うべき余地があると考え、万全を期すため上記の比較を行って本人確認に利用する。

10

【0010】

また本発明では、犯罪者の住所など、避けるべき住所群をいわゆるブラックリストなどとして予め定めておき、これらの住所とユーザの住所情報を比較して本人確認に利用することで、本人確認の精度を高めることができる。

【0011】

前記画像は、本人確認証の画像であることが望ましい。

本発明は、運転免許証などの本人確認証の画像を送信して口座開設やスマートフォン等の購入の申請を行うような場合に好適に適用することができる。

20

【0012】

また本発明により、担当者がユーザ端末の位置情報等から本人確認を行うのを支援することができる。

【0013】

前記比較手段は、GPS情報である前記ユーザ端末の位置情報をテキストに変換し、テキストに変換した前記ユーザ端末の位置情報と、テキストである前記ユーザの住所情報との一致度を、前記ユーザ端末の位置情報のテキストと前記ユーザの住所情報のテキストに基づき算出することが望ましい。

このように一致度の値を算出することでも、担当者による本人確認を支援することができる。

30

【0014】

第2の発明は、コンピュータを、ユーザ端末から本人確認用の画像と前記画像の撮影時の前記ユーザ端末の位置情報を受信する受信手段と、ユーザの住所情報を取得する取得手段と、本人確認のため、前記ユーザ端末の位置情報と前記ユーザの住所情報を比較する比較手段と、を有し、前記比較手段は、さらに、前記ユーザの住所情報を、避けるべき所定の住所群と比較し、前記比較手段は、前記ユーザ端末の位置情報と前記ユーザの住所情報が一致せず、且つ前記ユーザの住所情報と前記所定の住所群中の全ての住所とが一致しない場合、前記ユーザ端末の位置情報と、前記ユーザの住所情報と、前記所定の住所群中の住所とを地図上で示した表示画面を表示する本人確認支援装置として機能させるためのプログラムである。

40

【発明の効果】

【0015】

本発明により、本人確認を好適に行うことのできる本人確認支援装置等を提供することができる。

【図面の簡単な説明】

【0016】

【図1】本人確認システム1を示す図。

【図2】本人確認支援装置3のハードウェア構成を示す図。

【図3】ユーザ端末5のハードウェア構成を示す図。

50

【図4】本人確認支援装置3の機能構成を示す図。

【図5】IDカード10を示す図。

【図6】本人確認方法の流れを示すフローチャート。

【図7】本人確認方法の流れを示すフローチャート。

【図8】比較処理について説明する図。

【図9】一致度の算出例を説明する図。

【発明を実施するための形態】

【0017】

以下、図面に基づいて本発明の好適な実施形態について詳細に説明する。

【0018】

(1. 本人確認システム1)

図1は本発明の実施形態に係る本人確認支援装置3を有する本人確認システム1を示す図である。

【0019】

本人確認システム1は、口座開設やスマートフォン等の購入の申請時に、申請者(ユーザ)のIDカード10を撮影した撮影画像や本人確認に必要なその他の情報をユーザ端末5から本人確認支援装置3に送信して本人確認を行うためのものであり、本人確認支援装置3とユーザ端末5とをネットワークにより通信可能に接続して構成される。

【0020】

図2は本人確認支援装置3のハードウェア構成を示す図である。本人確認支援装置3は、制御部31、記憶部32、表示部33、通信部34等をバス等で接続して構成されたコンピュータにより実現できる。ただしこれに限ることは無く、適宜様々な構成をとることができる。

【0021】

制御部31はCPU、ROM、RAMなどから構成される。CPUは、記憶部32、ROMなどの記憶媒体に格納された本人確認支援装置3の処理に係るプログラムをRAM上のワークエリアに呼び出して実行する。ROMは不揮発性メモリであり、ブートプログラムやBIOSなどのプログラム、データなどを恒久的に保持している。RAMは揮発性メモリであり、記憶部32、ROMなどからロードしたプログラムやデータを一時的に保持するとともに、制御部31が各種処理を行うために使用するワークエリアを備える。

【0022】

記憶部32はハードディスクドライブやソリッドステートドライブ、フラッシュメモリ等であり、後述する処理に際し本人確認支援装置3が実行するプログラム、プログラム実行に必要なデータ、OSなどが格納される。これらのプログラムやデータは、制御部31により必要に応じて読み出され実行される。また本実施形態では、犯罪者の住所など、避けるべき所定の住所群がいわゆるブラックリストなどとして予め記憶部32に格納されているものとする。

【0023】

表示部33は液晶ディスプレイ等であり、本人確認に係る各種の情報を表示する。

【0024】

通信部34はネットワークを介した通信を媒介する通信インタフェースであり、ユーザ端末5との間で通信を行う。

【0025】

ユーザ端末5はユーザの所持するカメラ付きの端末であり、ユーザのIDカード10を撮影した撮影画像や本人確認に必要なその他の情報を本人確認支援装置3に送信する。ユーザ端末5としては、例えばスマートフォンやタブレット端末等の携帯端末などを用いることができる。

【0026】

図3はユーザ端末5のハードウェア構成を示す図である。図3に示すように、ユーザ端末5は、制御部51、記憶部52、表示部53、入力部54、通信部55、カメラ56、

10

20

30

40

50

音声入出力部 5 7 等をバス等で接続して構成されたコンピュータにより実現できる。ただしこれに限ることは無く、適宜様々な構成をとることができる。

【 0 0 2 7 】

制御部 5 1、記憶部 5 2、通信部 5 5 は上述した制御部 3 1、記憶部 3 2、通信部 3 4 と略同様である。記憶部 5 2 には、ユーザ端末 5 が後述する処理を実行するための専用のアプリケーションプログラムが格納されている。

【 0 0 2 8 】

また表示部 5 3 は液晶パネル等のディスプレイ装置を有し、ユーザ端末 5 に入力を行うための入力部 5 4 としてタッチパネルが設けられている。音声入出力部 5 7 は、音声の入出力に用いるマイクやスピーカーを備える。

【 0 0 2 9 】

カメラ 5 6 は、光学レンズ、CCD (Charge coupled device) や CMOS (Complementary metal-oxide semiconductor) 等の撮像素子、A/D (Analog/Digital) 変換部等から構成されるエリアカメラである。カメラ 5 6 は、光学レンズを介して入力された被写体像を撮像素子により光電変換し、アナログ画像信号を生成する。そして、A/D変換部によりアナログ画像信号をデジタル画像データに変換する。

【 0 0 3 0 】

図 4 は本人確認支援装置 3 の機能構成を示す図である。本人確認支援装置 3 は、受信手段 3 0 1、取得手段 3 0 2、比較手段 3 0 3 等を有する。

【 0 0 3 1 】

受信手段 3 0 1 は、本人確認支援装置 3 の制御部 3 1 が、通信部 3 4 を介してユーザ端末 5 から IDカード 1 0 の撮影画像と IDカード 1 0 の撮影時のユーザ端末 5 の位置情報を受信するものである。

【 0 0 3 2 】

取得手段 3 0 2 は、本人確認支援装置 3 の制御部 3 1 が、ユーザの住所情報を取得するものである。本実施形態では、ユーザの住所情報を本人確認に必要な情報とし、これをユーザ端末 5 から通信部 3 4 を介して受信し、取得する。

【 0 0 3 3 】

比較手段 3 0 3 は、本人確認支援装置 3 の制御部 3 1 が、ユーザ端末 5 の位置情報やユーザの住所情報についての比較を本人確認のために行うものである。この処理の詳細については後述する。

【 0 0 3 4 】

(2 . IDカード 1 0)

IDカード 1 0 は、本実施形態において本人確認に用いる本人確認証である。本人確認証は、金融機関や携帯電話キャリアなどで本人確認に用いられる媒体をいい、例えば運転免許証、マイナンバーカード、在留カード、特別永住者カードなどである。

【 0 0 3 5 】

図 5 (a)、(b) はそれぞれ IDカード 1 0 の表面と裏面を模式的に示す図である。IDカード 1 0 は、略矩形形状のカード基材の表面の所定位置に、カード所持者の住所 1 1 の他、カード所持者の氏名、顔画像、IDカード 1 0 の発行番号などを印刷したものである。また裏面の所定位置には、住所が更新された場合に新住所を書き込む備考欄 2 1 が設けられている。

【 0 0 3 6 】

(3 . 本人確認方法)

図 6 は、本人確認システム 1 で実行される本人確認方法の流れを示すフローチャートである。図 6 の S 1 ~ S 2、S 4 ~ S 5 はユーザ端末 5 の制御部 5 1 がユーザ端末 5 の各部を制御して実行する処理であり、S 3、S 6 ~ S 7 は本人確認支援装置 3 の制御部 3 1 が本人確認支援装置 3 の各部を制御して実行する処理である。

【 0 0 3 7 】

本実施形態では、まずユーザがユーザ端末 5 を操作して記憶部 5 2 に格納された専用の

10

20

30

40

50

アプリケーションプログラムを立ち上げる。すると、ユーザ端末5は表示部53にメニュー画面(不図示)を表示し、メニュー画面でのユーザの選択に応じてカメラ56を起動し、IDカード10の券面を撮影する(S1)。本実施形態では、IDカード10の券面として図5(a)、(b)に示した表面と裏面を撮影する。

【0038】

ここで、IDカード10の撮影画像のデータには、GPS(Global positioning system)などにより得られたIDカード10の撮影時のユーザ端末5の位置情報がEXIF(Exchangeable image file format)情報などとして含まれているものとする。ユーザ端末5は、IDカード10の撮影画像をIDカード10の撮影時のユーザ端末5の位置情報と併せて本人確認支援装置3に送信する(S2)。本人確認支援装置3は、ユーザ端末5からIDカード10の撮影画像とIDカード10の撮影時のユーザ端末5の位置情報を受信する(S3)。

10

【0039】

またユーザはユーザ端末5を操作し、本人確認に必要な情報(本人確認情報という)をユーザ端末5に入力する。ユーザ端末5は本人確認情報の入力を受付け(S4)、本人確認情報を本人確認支援装置3に送信する(S5)。この本人確認情報にはユーザの住所を示す住所情報が含まれるものとし、本人確認支援装置3は、住所情報を含む本人確認情報をユーザ端末5から受信する(S6)。

【0040】

その後、本人確認支援装置3は、本人確認のため、IDカード10の撮影時のユーザ端末5の位置情報やユーザの住所情報についての比較を行う(S7)。

20

【0041】

図7は、S7において実行される比較処理を示すフローチャートである。本実施形態では、S7において、ユーザの住所情報とIDカード10の撮影時のユーザ端末5の位置情報を比較する(S71)とともに、ユーザの住所情報を、本人確認支援装置3の記憶部32に格納された、避けるべき所定の住所群と比較する(S72)。

【0042】

そして、図8(a)に示すように、ユーザの住所情報とIDカード10の撮影時のユーザ端末5の位置情報が一致し、ユーザの住所情報と前記所定の住所群中のいずれかの住所が一致する場合(S73; S71で一致、S72で一致)、ユーザの住所が避けるべき住所であるため本人確認が失敗したとする(S74)。本人確認が失敗した旨は、ユーザ端末5に通知されるとともに、本人確認支援装置3の表示部33にも表示される。なお、ユーザの住所情報とユーザ端末5の位置情報がどの程度近ければ一致とみなすかは適宜設定することができる。これはユーザの住所情報と所定の住所群との比較においても同様である。

30

【0043】

ユーザの住所情報とIDカード10の撮影時のユーザ端末5の位置情報が一致し、ユーザの住所情報と前記所定の住所群中の全ての住所が一致しない場合(S73; S71で一致、S72で不一致)、本人確認が成功したとする(S75)。本人確認が成功した旨は、ユーザ端末5に通知されるとともに、本人確認支援装置3の表示部33にも表示される。

【0044】

またユーザの住所情報とIDカード10の撮影時のユーザ端末5の位置情報が一致せず、ユーザの住所情報と前記所定の住所群中のいずれかの住所が一致する場合(S73; S71で不一致、S72で一致)、ユーザの住所が避けるべき住所であるため本人確認が失敗したとする(S76)。本人確認が失敗した旨は、前記と同様、ユーザ端末5に通知されるとともに、本人確認支援装置3の表示部33にも表示される。

40

【0045】

そして、ユーザの住所情報とIDカード10の撮影時のユーザ端末5の位置情報が一致せず、ユーザの住所情報と前記所定の住所群中の全ての住所が一致しない場合(S73; S71で不一致、S72で不一致)、ユーザは、撮影環境が比較的整っており且つ自らが慣れた自宅で画像の撮影を行わず、わざわざ外に出て撮影を行っていることになるので、ユーザの住所情報とユーザ端末5の位置情報の齟齬には何らかの不正を疑うべき余地がある

50

と考え、表示部 3 3 にアラート（警告）を表示し（S 7 7）、担当者に注意を促す。

【0 0 4 6】

例を挙げると、前記所定の住所群中の住所に住むユーザが、IDカード 1 0 の裏面に所定の住所群中に無い住所を記入し、前記の S 4（図 6 参照）で当該住所を入力している（S 7 2 で不一致となる）が、IDカード 1 0 の撮影は自宅で行っている（S 7 1 で不一致となる）ケースでは、S 7 7 でアラートが表示されることになる。S 7 のフローでは、上記ケースも含め、S 4 で入力した住所が前記所定の住所群中には無いが、IDカード 1 0 の撮影を当該入力した住所以外で行っている場合全般について、アラートが表示される。

【0 0 4 7】

この場合、担当者はユーザの住所情報やIDカード 1 0 の撮影時のユーザ端末 5 の位置情報、IDカード 1 0 の撮影画像等から、本人確認を注意して行う。

10

【0 0 4 8】

図 8（b）は、この時に表示部 3 3 に表示される本人確認用の表示画面の一例である。この例では、地図上でユーザの住所情報 3 3 1、IDカード 1 0 の撮影時のユーザ端末 5 の位置情報 3 3 2、前記所定の住所群中の住所 3 3 3 等が示され、住所情報 3 3 1 や位置情報 3 3 2 が示す場所、住所情報 3 3 1 と位置情報 3 3 2 の近さ、位置情報 3 3 2 と住所 3 3 3 の近さなどを考慮して本人確認の判断を総合的に行い、その後の対応を決めることができる。また住所情報 3 3 1 については、その位置から所定距離の範囲を示す円周 3 3 4 が表示されており、上記の判断の助けとなる。

【0 0 4 9】

20

以上説明したように、本実施形態では、ユーザ端末 5 から本人確認用のIDカード 1 0 の撮影画像を受信した際に、当該撮影画像の撮影時のユーザ端末 5 の位置情報とユーザの住所情報の比較を行う。これらが一致しない場合、ユーザは、撮影環境が比較的整っており且つ自らが慣れた自宅画像の撮影を行わず、わざわざ外に出て撮影を行っていることになるので、何らかの不正を疑うべき点があると考え、万全を期すため上記の比較を行ってこれを本人確認に利用する。

【0 0 5 0】

また本実施形態では、避けるべき住所群をいわゆるブラックリストなどとして予め定めおき、これらの住所とユーザの住所情報を比較して本人確認に利用することで、本人確認の精度を高めることができる。

30

【0 0 5 1】

また本実施形態では、IDカード 1 0 の撮影時のユーザ端末 5 の位置情報とユーザの住所情報が一致しない場合、上記位置情報とユーザの住所情報を地図上で示した表示画面を表示するので、担当者が上記位置情報等から本人確認を行うのを支援することができる。

【0 0 5 2】

しかしながら、本発明は以上の実施形態で説明したものに限らない。例えば本実施形態では口座開設やスマートフォンなどの購入の申請時に本人確認を行う例を説明したが、本人確認の適用場面あるいは適用目的は特に限定されない。

【0 0 5 3】

また、本人確認支援装置 3 は、IDカード 1 0 の撮影時のユーザ端末 5 の位置情報と、避けるべき所定の住所群との比較を行ってもよい。この場合、前述のケース、すなわち、上記所定の住所群中の住所に住むユーザが、IDカード 1 0 の裏面に所定の住所群中に無い住所を記入し、前記の S 4（図 6 参照）で当該住所を入力しているが、IDカード 1 0 の撮影は自宅で行っているケースでは、IDカード 1 0 の撮影時のユーザ端末 5 の位置情報が所定の住所群中の住所と一致することにより不正な申請とみなされ本人確認が失敗となる。

40

【0 0 5 4】

さらに、IDカード 1 0 の撮影時のユーザ端末 5 の位置情報とユーザの住所情報の一致度を算出し、本人確認に用いることもできる。その方法は特に限定されないが、例えば図 9 に示すように、GPS情報として記録されたIDカード 1 0 の撮影時のユーザ端末 5 の位置情報を住所のテキスト情報に変換し、ユーザの住所情報との一致度を見ることができる。例

50

例えば住所が都道府県から番地まで一致する場合、IDカード10の撮影時のユーザ端末5の位置情報とユーザの住所情報が一致(完全一致)するとし、そうでない場合は両者が一致しないとする。

【0055】

後者の場合、ユーザ端末5の位置情報とユーザの住所情報がどの程度一致するかにより一致度を算出し、例えば都道府県から町名まで一致する場合、高い一致度(ほぼ一致)を与え、都道府県しか一致しない場合や、都道府県も一致しない場合、低い一致度(不一致)を与える。前記したアラート(図7のS77参照)においては、これらの一致度に応じた警戒レベルを本人確認支援装置3の表示部33に表示するなどして、担当者による本人確認を支援することができる。

10

【0056】

また本実施形態ではユーザが入力した住所情報を比較に用いているが、その代わりに、S3(図6参照)で受信したIDカード10の撮影画像からIDカード10の表面や裏面に記載された住所をOCR(Optical character recognition)技術により読取って住所情報として取得し、比較に用いてもよい。この場合、IDカード10の表面や裏面に前記した所定の住所群のいずれかの住所が記載されていると、不正な申請とみなされ本人確認が失敗となる。

【0057】

また本実施形態ではIDカード10(本人確認証)の撮影画像を本人確認支援装置3に送信しているが、その他の本人確認用の画像(例えば顔画像など)を本人確認支援装置3に送信する場合にも適用可能である。ただし、本発明は、運転免許証などの本人確認証の画像を送信して各種の申請を行うような場合に好適に適用することができる。

20

【0058】

以上、添付図面を参照して、本発明の好適な実施形態について説明したが、本発明は係る例に限定されない。当業者であれば、本願で開示した技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

【符号の説明】

【0059】

- 1：本人確認システム
- 3：本人確認支援装置
- 5：ユーザ端末
- 10：IDカード
- 301：受信手段
- 302：取得手段
- 303：比較手段

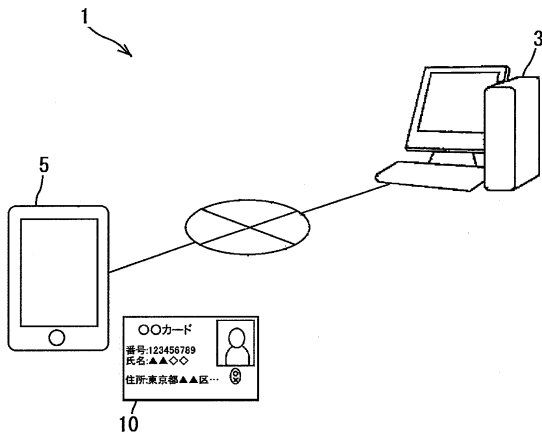
30

40

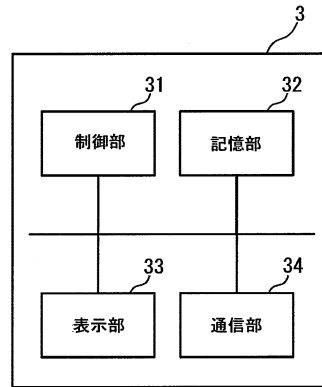
50

【図面】

【図 1】

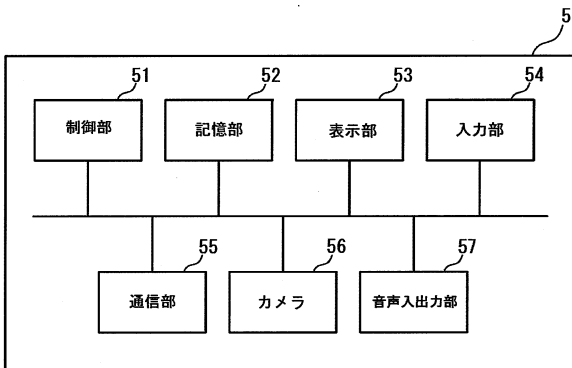


【図 2】

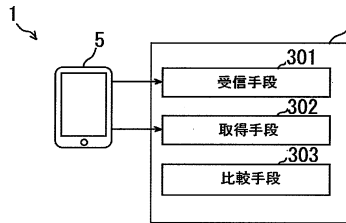


10

【図 3】



【図 4】



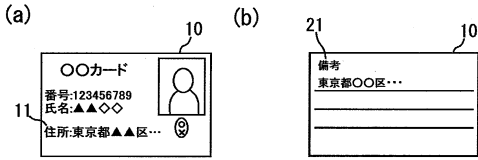
20

30

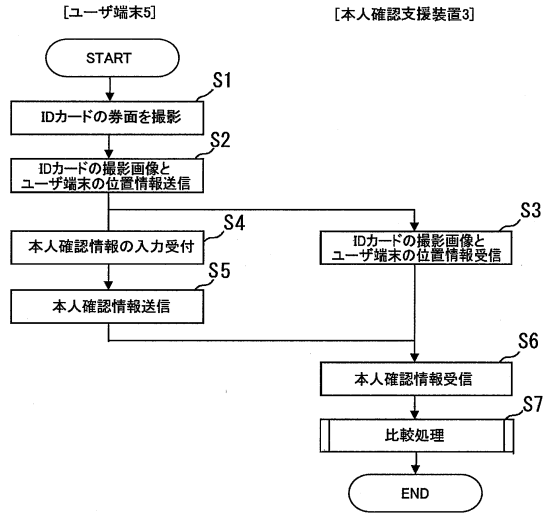
40

50

【図5】

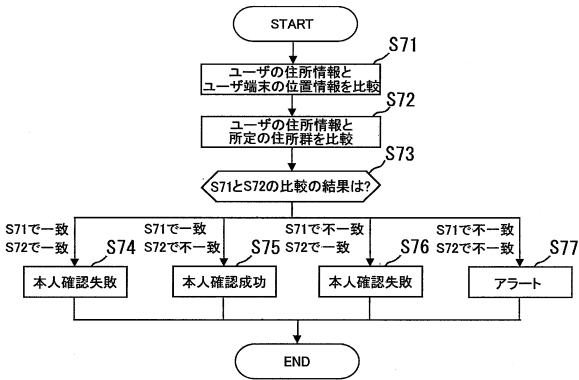


【図6】

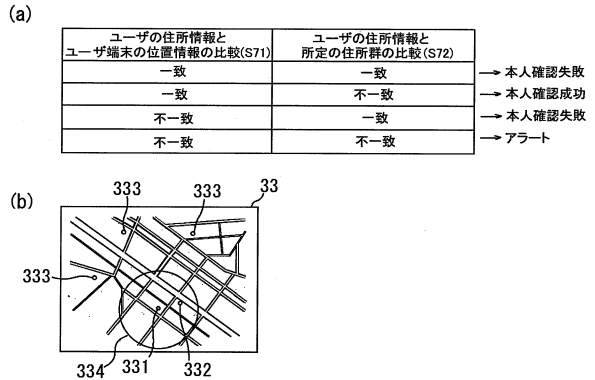


10

【図7】



【図8】



20

30

40

50

【 図 9 】

ユーザの住所情報 : 東京都 ○○区 △△町 1-1-1
ユーザ端末の位置情報 : 東京都 ○○区 △△町 1-1-1 ⇨ 完全一致
ユーザ端末の位置情報 : 東京都 ○○区 △△町 1-1-2 ⇨ ほぼ一致
ユーザ端末の位置情報 : 東京都 □□区 ◇◇ 6-6-6 ⇨ 不一致
ユーザ端末の位置情報 : 大阪府 ▲▲市 ◎◎ 3-3-3 ⇨ 不一致

10

20

30

40

50

フロントページの続き

- (56)参考文献 特開2019-086971(JP,A)
特開2014-127163(JP,A)
特開2020-064541(JP,A)
特開2019-028660(JP,A)
- (58)調査した分野 (Int.Cl., DB名)
G06Q 10/00-99/00