

(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
2019年5月23日(23.05.2019)



(10) 国際公開番号

WO 2019/098205 A1

- (51) 国際特許分類:
G06F 21/31 (2013.01) *G06T 7/00* (2017.01)
G06F 21/32 (2013.01)
- (21) 国際出願番号: PCT/JP2018/042024
- (22) 国際出願日: 2018年11月13日(13.11.2018)
- (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 2017-220360 2017年11月15日(15.11.2017) JP
- (71) 出願人: NECソリューションイノベータ株式会社(NEC SOLUTION INNOVATORS,

LTD.) [JP/JP]; 〒1368627 東京都江東区新木場一丁目18番7号 Tokyo (JP).

- (72) 発明者: 山田 栄子(YAMADA, Eiko); 〒1368627 東京都江東区新木場一丁目18番7号 NECソリューションイノベータ株式会社内 Tokyo (JP). 奥村 明俊(OKUMURA, Akitoshi); 〒1368627 東京都江東区新木場一丁目18番7号 NECソリューションイノベータ株式会社内 Tokyo (JP). 星野 隆道(HOSHINO, Takamichi); 〒1368627 東京都江東区新木場一丁目18番7号 NECソリューションイノベータ株式会社内 Tokyo (JP).

(54) **Title:** AUTHENTICATION DEVICE, AUTHENTICATION METHOD, AND COMPUTER-READABLE RECORDING MEDIUM

(54) 発明の名称: 認証装置、認証方法、及びコンピュータ読み取り可能な記録媒体

[図1]

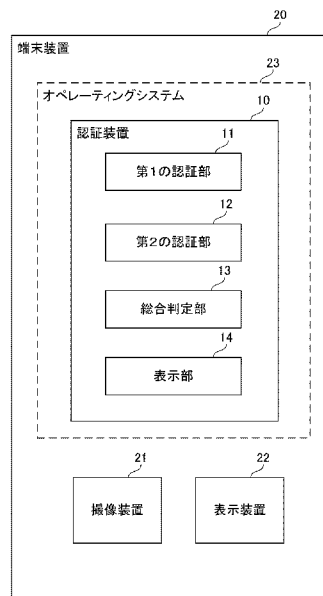


FIG. 1:
10 Authentication device
11 First authentication unit
12 Second authentication unit
13 Overall determination unit
14 Display unit
20 Terminal device
21 Imaging device
22 Display device
23 Operating system

(57) **Abstract:** This authentication device 10 is provided to a portable terminal device 20 provided with an imaging device 21. The authentication device 10 is provided with: a first authentication unit 11 which performs authentication by checking facial image data of the face of a user photographed by the imaging device 21 of the terminal device 20, against facial authentication data stored in the terminal device 20; a second authentication unit 12 which performs authentication using second authentication data which is stored in the terminal device 20, and which is formed from characteristics other than

(74) 代理人: 特許業務法人ブライタス(BRIGHTAS IP ATTORNEYS); 〒1040061 東京都中央区銀座1丁目19番12号 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, JP, 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, 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:

— 国際調査報告 (条約第21条(3))

facial characteristics; an overall determination unit 13 which determines whether the user corresponds to a pre-registered person, on the basis of the authentication result from the first authentication unit 11, and the authentication result from the second authentication unit 12; and a display unit 14 which displays, on a screen of the terminal device 20, the result of the determination performed by the overall determination unit 13.

(57) 要約: 認証装置10は、撮像装置21を有する携帯型の端末装置20に備えられている。認証装置10は、端末装置20に保持されている顔認証用データに、端末装置20の撮像装置21によって撮影されたユーザの顔の顔画像データを照合して、認証を行う、第1の認証部11と、端末装置20に保持されている、顔以外の特徴による第2の認証用データを用いて、認証を行う、第2の認証部12と、第1の認証部11による認証結果と第2の認証部12による認証結果とに基づいて、ユーザが予め登録されている人物と一致するかどうか判定する、総合判定部13と、総合判定部13による判定の結果を、端末装置20の画面に表示させる、表示部14と、を備えている。

明 細 書

発明の名称：

認証装置、認証方法、及びコンピュータ読み取り可能な記録媒体

技術分野

[0001] 本発明は、本人確認を行うための認証装置、認証方法、及びこれらを実現するためのプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

背景技術

[0002] 近年、人気の高いコンサートといった大規模イベントにおいて、チケットを買占めて、高額で売買するといった違法転売行為が問題となっている。このようなチケットの違法転売行為に対する対策として、イベント会場では、チケットの購入者と来場者とが、同一人物であることを確認する、本人確認作業が行なわれている。

[0003] 本人確認作業の一例として、一部の来場者に対し、抜き打ちで、購入時に登録された氏名と、来場者の提示する身分証明書の氏名とが、一致しているかどうかを確認する、といった方法が採られている。しかしながら、大規模イベントでは、来場者の数も数万人規模となるため、上記方法では、十分な本人確認を行なうことは困難である。

[0004] そこで、最近、大規模イベントにおいては、本人確認のため、例えば、非特許文献１に開示されている顔認証を用いたシステムが利用される。非特許文献１で開示されたシステムは、イベント入場者制御システム、顔画像管理システム、及び会場で用いられる認証用端末装置等で構成されている。そして、具体的には、非特許文献１で開示されたシステムは以下に示す処理を実行する。

[0005] 最初に、チケット購入者が、自身の顔画像、氏名等の個人情報、ＩＤ番号等を、イベント入場者制御システムに送信すると、イベント入場者制御システムは、送信されてきた、顔画像及び個人情報等を登録する。次いで、顔画

像管理システムは、登録された顔画像から、顔の特徴量を生成し、生成した特徴量を、個人のID番号と紐付けて、認証用データとして登録する。

[0006] 続いて、イベント当日に、チケット購入者が、会場に入場する際に、設置されているカードリーダを介してチェックインすると、イベント入場者制御システムは、チケット購入者のID番号を特定し、特定したID番号を顔画像管理システムに送信する。これにより、顔画像管理システムは、送信されてきたIDが紐付けられている認証用データを、認証用端末装置に送信する。

[0007] その後、会場に待機しているスタッフが、カメラ付の認証用端末装置を用いて、来場したチケット購入者の顔を撮影すると、認証用端末装置は、撮影された顔画像を、送信されてきた認証用データに照合して、顔認証を実行する。

[0008] 認証が成功した場合は、認証用端末装置は、画面上に、認証が成功した旨を表示するので、スタッフは、来場したチケット購入者の入場を許可する。このように、非特許文献1に開示されたシステムを用いれば、チケットの購入者と来場者との一致性を簡単に確かめることができ、違法な転売行為を防ぐことができる。

先行技術文献

非特許文献

[0009] 非特許文献1: Okumura, A., Hoshino, T., Handa, S. and Nishiyama, Y.: Identity Verification of Ticket Holders at Large-scale Events Using Face Recognition, IPSJ Transactions on Consumer Devices & Systems, Vol.7 No.2 (2017/5/25)

発明の概要

発明が解決しようとする課題

[0010] しかしながら、非特許文献1で開示されたシステムでは、顔画像管理システムは、来場者毎に、認証用端末に対して認証用データを送信する必要がある

る。このため、特に大規模なイベントでは、顔画像管理システムから認証用端末へのデータ量が著しく増加するため、通信回線が混雑し、認証処理が遅延してしまうという問題が発生する。

[0011] 一方、このような問題は、顔画像管理システムの処理速度を高め、大容量の回線を利用すれば解消できるとも考えられるが、この場合は、通信コスト及びシステムの設置コストが増大するという問題が発生する。

[0012] また、非特許文献 1 で開示されたシステムを採用した場合は、イベントの規模が大きくなり、来場者の数が増加するほど、必要な認証用端末の数も増加する。このため、この点からも、システムの設置コストは増大してしまう。

[0013] また、顔画像管理システムが認証用端末に送信する各来場者の認証用データは、顔の特徴量を特定するデータであり、個人データである。このような個人データを、イベント当日に、通信回線を介して、送信することは、個人情報漏洩の観点から好ましくはない。

[0014] 本発明の目的の一例は、上記問題を解消し、顔画像を用いた認証処理に要するコストの低減と、個人情報の漏洩の抑制とを図り得る、認証装置、認証方法、及びコンピュータ読み取り可能な記録媒体を提供することにある。

課題を解決するための手段

[0015] 上記目的を達成するため、本発明の一側面における認証装置は撮像装置を有する携帯型の端末装置に備えられる認証装置であって、

前記端末装置に保持されている顔認証用データに、前記端末装置の前記撮像装置によって撮影されたユーザの顔の顔画像データを照合して、認証を行う、第 1 の認証部と、

前記端末装置に保持されている、顔以外の特徴による第 2 の認証用データを用いて、認証を行う、第 2 の認証部と、

前記第 1 の認証部による認証結果と前記第 2 の認証部による認証結果とに基づいて、前記ユーザが予め登録されている人物と一致するかどうか判定する、総合判定部と、

前記総合判定部による判定の結果を、前記端末装置の画面に表示させる、表示部と、

を備えていることを特徴とする。

[0016] また、上記目的を達成するため、本発明の一側面における認証方法は、撮像装置を有する携帯型の端末装置を用いた認証方法であって、

(a) 前記端末装置に保持されている顔認証用データに、前記端末装置の前記撮像装置によって撮影されたユーザの顔の顔画像データを照合して、認証を行う、ステップと、

(b) 前記端末装置に保持されている、顔以外の特徴による第2の認証用データを用いて、認証を行う、ステップと、

(c) 前記(a)のステップによる認証結果と前記(b)のステップによる認証結果とに基づいて、前記ユーザが予め登録されている人物と一致するかどうか判定する、ステップと、

(d) 前記(c)のステップによる判定の結果を、前記端末装置の画面に表示させる、ステップと、

を有することを特徴とする。

[0017] 更に、上記目的を達成するため、本発明の一側面におけるコンピュータ読み取り可能な記録媒体は、撮像装置を有する携帯型の端末装置を構成する、コンピュータによって認証を行うためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記コンピュータに、

(a) 前記端末装置に保持されている顔認証用データに、前記端末装置の前記撮像装置によって撮影されたユーザの顔の顔画像データを照合して、認証を行う、ステップと、

(b) 前記端末装置に保持されている、顔以外の特徴による第2の認証用データを用いて、認証を行う、ステップと、

(c) 前記(a)のステップによる認証結果と前記(b)のステップによる認証結果とに基づいて、前記ユーザが予め登録されている人物と一致するか

どうか判定する、ステップと、

(d) 前記(c)のステップによる判定の結果を、前記端末装置の画面に表示させる、ステップと、

を実行させる命令を含む、プログラムを記録していることを特徴とする。

発明の効果

[0018] 以上のように、本発明によれば、顔画像を用いた認証処理に要するコストの低減と個人情報の漏洩の抑制とを図ることができる。

図面の簡単な説明

[0019] [図1]図1は、本発明の実施の形態における認証装置の構成を示すブロック図である。

[図2]図2は、本発明の実施の形態における認証装置を用いた認証の手順を説明する図である。

[図3]図3は、本発明の実施の形態における認証装置の動作を示すフロー図である。

[図4]図4は、本発明の実施の形態における認証装置を実現するコンピュータの一例を示すブロック図である。

発明を実施するための形態

[0020] (実施の形態)

以下、本発明の実施の形態における認証装置、認証方法、及びプログラムについて、図1～図4を参照しながら説明する。

[0021] [装置構成]

最初に、図1を用いて、本実施の形態における認証装置の構成について説明する。図1は、本発明の実施の形態における認証装置の構成を示すブロック図である。

[0022] 図1に示す本実施の形態における認証装置10は、例えば、イベント等において、本人確認を行うための認証を行うために用いられる。図10に示すように、認証装置10は、撮像装置21を有する携帯型の端末装置20に備えられている。また、図1に示すように、認証装置10は、第1の認証部1

１と、第２の認証部１２と、総合判定部１３と、表示部１４とを備えている。

[0023] 第１の認証部１１は、端末装置２０に保持されている顔認証用データに、端末装置２０の撮像装置２１によって撮影されたユーザの顔の顔画像データを照合して、認証を行う。第２の認証部１２は、端末装置２０に保持されている、顔以外の特徴による第２の認証用データを用いて、認証を行う。

[0024] 総合判定部１３は、第１の認証部１１による認証結果と第２の認証部１２による認証結果とに基づいて、ユーザが予め登録されている人物と一致するかどうか判定する。表示部１４は、総合判定部１３による判定の結果を、端末装置２０の画面に表示させる。

[0025] このように、本実施の形態では、撮像装置２１を備えた携帯型の端末装置２０によって認証を行うことができ、端末装置２０としてユーザ自身の端末装置を用いることができる。このため、認証を行う側において認証用端末を用意しなくても良く、認証対象となる人の数が増加しても、認証用のシステムの設置コストの増加は抑制される。また、認証に用いられる顔認証用データ及び第２の認証用データは、端末装置２０に保持されているので、個人情報の漏洩が抑制されると共に、通信コストの増加も抑制される。つまり、本実施の形態によれば、顔画像を用いた認証処理に要するコストの低減と、個人情報の漏洩の抑制とが図られる。

[0026] ここで、本実施の形態における認証装置１０の構成についてより具体的に説明する。図１に示すように、本実施の形態では、認証装置１０は、端末装置２０を構成するコンピュータで実行される、プログラムによって構築されている。具体的には、このプログラムは、認証装置１０のオペレーティングシステム２３上で動作するプログラムである。本実施の形態では、オペレーティングシステム２３上でプログラムを実行することにより、認証装置１０が構築される。

[0027] また、後述するように、プログラムは、イベントの主催者等によって管理されているサーバ装置３０（後述の図２参照）から送信されてくる。更に、

プログラムには、顔認証用データと第2の認証用データとが予め付加されており、プログラムが実行されると、これらのデータは、端末装置20のメモリ等の記憶装置に保持される。

[0028] また、本実施の形態において、第2の認証用データとしては、特定の日時を含むデータが挙げられる。この場合、第2の認証部12は、第2の認証用データに、第1の認証部によって認証が行われた日時を照合することによって、認証を行う。

[0029] 更に、第2の認証用データとしては、指定された位置（例えば、イベント会場の位置）の座標を含むデータも挙げられる。この場合、第2の認証部12は、第2の認証用データに、撮像装置21によってユーザ40の顔が撮影されたときの端末装置20の位置の座標を照合することによって、認証を行う。

[0030] 加えて、第2の認証用データとしては、指定された端末装置20の識別子を含むデータも挙げられる。この場合、第2の認証部12は、第2の認証用データに、端末装置20に付与されている識別子を照合することによって、認証を行う。

[0031] また、第2の認証用データとしては、特定の画像データを含むデータも挙げられる。この場合、第2の認証部12は、端末装置20の撮像装置21によって撮影された画像から、ユーザの顔以外の部分の画像を抽出し、第2の認証用データに、抽出した画像を照合することによって、認証を行う（後述する図2についての説明を参照）。特定の画像としては、イベントの主催者が指定したイラスト、図形、ロゴ等の画像が挙げられる。

[0032] また、第2の認証用データは、上述した、特定の日時、指定された位置の座標、指定された端末装置20の識別子、及び特定の画像データのうち、2つ以上を組み合わせて得られたデータであっても良い。

[0033] 続いて、図2を用いて、本実施の形態における認証装置10を用いた認証の手順について説明する。図2は、本発明の実施の形態における認証装置を用いた認証の手順を説明する図である。また、以下においては、認証装置1

0が、コンサート等のイベントにおける本人認証に用いられる場合を例に挙げて説明する。

[0034] 図2に示すように、まず、イベントへの参加を希望するユーザ40は、自宅等のイベント会場以外の場所において、端末装置20を用いて、自身のユーザ情報（名前、住所、電話番号等）と、端末装置20の撮像装置21で撮影した自身の顔の画像データ（以下「顔画像データ」と表記する）とをサーバ装置30に送信する。

[0035] サーバ装置30は、ユーザ情報及び顔画像データを受信すると、受信したユーザ情報を登録する。また、サーバ装置30は、受信した顔画像データから、特徴量を抽出し、抽出した特徴量を用いて顔認証用データを作成し、作成した顔認証用データも登録する。

[0036] そして、イベント当日、イベント会場において、ユーザ40が、端末装置20を介して、ユーザ情報を送信して、サーバ装置30に認証を求める。これにより、サーバ装置30は、送信されてきたユーザ情報が登録されているかどうかを判定する。ユーザ情報が登録されていると、サーバ装置30は、認証装置10を構築するためのプログラムに、登録されている顔認証用データと予め設定されている第2の認証用データとを付加し、これらのデータが付加されたプログラムを、端末装置20に送信する。

[0037] 端末装置20でプログラムが受信されると、端末装置20のオペレーティングシステム23は、受信されたプログラムをインストールし、これを実行する。これにより、オペレーティングシステム23上に、認証装置10が構築される。また、プログラムに予め付加されている、顔認証用データと第2の認証用データとは、端末装置20のメモリ等の記憶装置に保持される。

[0038] その後、ユーザ40が、顔認証のために、端末装置20の撮像装置21を用いて顔を撮影すると、認証装置10において、第1の認証部11、及び第2の認証部12による認証が行われ、更に、総合判定部13による総合判定が行われる。その後、認証の結果が、表示部14によって、表示装置22の画面上に表示される。そして、イベント会場にいる係員50は、認証が許可

されている場合は、ユーザ４０の入場を許可し、認証が許可されていない場合は、ユーザ４０の入場を許可しない。なお、図２において、５１は、第２の認証部１２による認証に使われる図形であり、これについては後述する。

[0039] [装置動作]

次に、本実施の形態における認証装置１０の動作について図３を用いて説明する。図３は、本発明の実施の形態における認証装置の動作を示すフロー図である。以下の説明においては、適宜図１及び図２を参酌する。また、本実施の形態では、認証装置１０を動作させることによって、認証方法が実施される。よって、本実施の形態における認証方法の説明は、以下の認証装置１０の動作説明に代える。

[0040] まず、前提として、図２で示したように、イベント当日、イベント会場において、ユーザ４０が、端末装置２０を介して、ユーザ情報を送信して、サーバ装置３０に認証を求めるとする。また、これに対応して、サーバ装置３０は、顔認証用データと第２の認証用データとが付加されたプログラムを、端末装置２０に送信し、更に、端末装置２０において、このプログラムが実行され、認証装置１０が構築されているとする。

[0041] 図３に示すように、まず、ユーザ４０が、撮像装置２１を用いて、自身の顔を撮影すると、第１の認証部１１は、撮像装置２１が出力した顔画像データを取得し、取得した顔画像データを、顔認証用データに照合して認証を実行する（ステップＡ１）。

[0042] 具体的には、第１の認証部１１は、顔画像データから、ユーザ４０の顔の部分の特徴量を抽出し、抽出した特徴量と顔認証用データで特定される特徴量とを比較し、両者の一致率を算出する。そして、第１の認証部１１は、一致率が閾値以上となる場合は、認証を許可する。

[0043] 次に、第２の認証部１２は、端末装置２０に保持されている第２の認証用データを用いて、認証を行う（ステップＡ２）。

[0044] ここで、第２の認証用データが、イベントの主催者が指定した図形の画像データである場合を例に挙げてステップＡ２を説明する。この場合において

は、イベント会場において、ユーザ40が自身の顔を撮影する場所は指定されており、指定された場所の壁には、指定された図形（図2の例では★）が描かれている。

[0045] そして、ユーザ40は、図2に示すように、壁の図形51が背景に表示されるように自身の顔を撮影する。この結果、顔画像データには、図形51の画像も含まれるので、第2の認証部12は、顔画像データから、図形51の画像を抽出する。そして、第2の認証部12は、抽出した図形51の画像と、第2の認証用データの画像との一致率を求め、求めた一致率が閾値以上となる場合は、認証を許可する。

[0046] 次に、総合判定部13は、ステップA1における認証結果と、ステップA2における認証結果とに基づいて、ユーザ40が予め登録されている人物と一致するかどうかを判定する（ステップA3）。ステップA3では、総合判定部13は、例えば、ステップA1及びA2の両方において認証が許可されている場合に、ユーザ40は予め登録されている人物と一致すると判定する。

[0047] ステップA3の判定の結果、ユーザ40が予め登録されている人物と一致する場合は、表示部14は、表示装置22の画面上に、認証を許可する旨を表示する（ステップA4）。この場合、図2に示したように、イベント会場にいる係員50は、ユーザ40の入場を許可する。

[0048] 一方、ステップA3の判定の結果、ユーザ40が予め登録されている人物と一致しない場合は、表示部14は、表示装置22の画面上に、認証を許可しない旨を表示する（ステップA5）。この場合、図2に示したように、イベント会場にいる係員50は、ユーザ40の入場を許可しない。

[0049] [実施の形態における効果]

以上のように本実施の形態では、イベントの主催者側で顔認証用の端末を用意する必要がない。また、イベントのために大容量の回線を用意したり、イベント会場に、認証用データを受信したりするためのシステムを設置する必要がない。このため、本実施の形態によれば、顔画像を用いた認証処理に

要するコストの低減が図られる。また、イベント会場において、認証用データの通信を行う必要もないため、個人情報の漏洩も抑制できる。更に、本実施の形態では、顔認証だけでなく、顔以外の特徴による認証も行われるため、いっそう厳密な本人確認が可能となるため、不正な入場を確実に抑制できる。

[0050] また、本実施の形態における認証装置 10 は、イベント会場における来場者の本人確認以外の用途にも利用できる。例えば、認証装置 10 は、特定の部屋への入室時の本人確認、特定の建物、施設、飛行機の搭乗口への入場時の本人確認等に用いられても良い。

[0051] 更に、本実施の形態では、表示部 14 は、認証を許可する旨の表示の代わりに、特定の二次元コードを表示しても良い。この態様は、特定の二次元コードで開閉する入場ゲートが設置されている場合に有用である。

[0052] また、本実施の形態では、認証装置 10 を構成するプログラムは、ステップ A4 又は A5 の実行後に、自身が削除されるように構成されていても良い。これにより、第 3 者による悪用が抑制される。

[0053] [プログラム]

本実施の形態におけるプログラムは、コンピュータに、図 4 に示すステップ A1 ～ A5 を実行させるプログラムであれば良い。このプログラムをコンピュータにインストールし、実行することによって、本実施の形態における認証装置 10 と認証方法とを実現することができる。この場合、コンピュータのプロセッサは、第 1 の認証部 11、第 2 の認証部 12、総合判定部 13、及び表示部 14 として機能し、処理を行なう。また、コンピュータとしては、スマートフォン、タブレット型端末といった端末装置を構成するコンピュータが挙げられる。

[0054] ここで、本実施の形態におけるプログラムを実行することによって、認証装置 10 を実現するコンピュータの一例について図 4 を用いて説明する。図 4 は、本発明の実施の形態における認証装置を実現するコンピュータの一例を示すブロック図である。

- [0055] 図4に示すように、コンピュータ110は、CPU111と、メインメモリ112と、記憶装置113と、入力インターフェイス114と、表示コントローラ115と、データリーダ／ライタ116と、通信インターフェイス117とを備える。これらの各部は、バス121を介して、互いにデータ通信可能に接続される。また、コンピュータ110は、CPU111に加えて、又はCPU111に代えて、GPU (Graphics Processing Unit)、又はFPGA (Field-Programmable Gate Array) を備えていても良い。
- [0056] CPU111は、記憶装置113に格納された、本実施の形態におけるプログラム（コード）をメインメモリ112に展開し、これらを所定順序で実行することにより、各種の演算を実施する。メインメモリ112は、典型的には、DRAM (Dynamic Random Access Memory) 等の揮発性の記憶装置である。
- [0057] また、本実施の形態におけるプログラムは、上述したようにネットワークを介して送信されてきても良いし、コンピュータ読み取り可能な記録媒体120に格納された状態で提供されても良い。
- [0058] また、記憶装置113の具体例としては、ハードディスクドライブの他、フラッシュメモリ等の半導体記憶装置が挙げられる。入力インターフェイス114は、CPU111と、キーボード及びマウスといった入力機器118との間のデータ伝送を仲介する。表示コントローラ115は、ディスプレイ装置119と接続され、ディスプレイ装置119での表示を制御する。
- [0059] データリーダ／ライタ116は、CPU111と記録媒体120との間のデータ伝送を仲介し、記録媒体120からのプログラムの読み出し、及びコンピュータ110における処理結果の記録媒体120への書き込みを実行する。通信インターフェイス117は、CPU111と、他のコンピュータとの間のデータ伝送を仲介する。
- [0060] また、記録媒体120の具体例としては、CF (Compact Flash (登録商標)) 及びSD (Secure Digital) 等の汎用的な半導体記憶デバイス、フレキシブルディスク (Flexible Disk) 等の磁気記録媒体、又はCD-ROM (Co

mpact Disk Read Only Memory)などの光学記録媒体が挙げられる。

[0061] なお、本実施の形態における認証装置10は、一部がプログラムで実現され、残りの部分がハードウェアで実現されていてもよい。

[0062] 上述した実施の形態の一部又は全部は、以下に記載する(付記1)～(付記18)によって表現することができるが、以下の記載に限定されるものではない。

[0063] (付記1)

撮像装置を有する携帯型の端末装置に備えられる認証装置であって、

前記端末装置に保持されている顔認証用データに、前記端末装置の前記撮像装置によって撮影されたユーザの顔の顔画像データを照合して、認証を行う、第1の認証部と、

前記端末装置に保持されている、顔以外の特徴による第2の認証用データを用いて、認証を行う、第2の認証部と、

前記第1の認証部による認証結果と前記第2の認証部による認証結果とに基づいて、前記ユーザが予め登録されている人物と一致するかどうか判定する、総合判定部と、

前記総合判定部による判定の結果を、前記端末装置の画面に表示させる、表示部と、

を備えていることを特徴とする認証装置。

[0064] (付記2)

当該認証装置が、前記端末装置を構成するコンピュータで実行されるプログラムによって構築されており、

前記プログラムには、前記顔認証用データ及び前記第2の認証用データが、予め付加されている、

付記1に記載の認証装置。

[0065] (付記3)

前記第2の認証用データが、特定の日時を含み、

前記第2の認証部が、前記第2の認証用データに、前記第1の認証部によ

って認証が行われた日時を照合することによって、認証を行う、
付記 1 または 2 に記載の認証装置。

[0066] (付記 4)

前記第 2 の認証用データが、指定された位置の座標を含み、
前記第 2 の認証部が、前記第 2 の認証用データに、前記撮像装置によって
前記ユーザの顔が撮影されたときの前記端末装置の位置の座標を照合すること
によって、認証を行う、付記 1 ～ 3 のいずれかに記載の認証装置。

[0067] (付記 5)

前記第 2 の認証用データが、指定された端末装置の識別子を含み、
前記第 2 の認証部が、前記第 2 の認証用データに、前記端末装置に付与さ
れている識別子を照合することによって、認証を行う、
付記 1 ～ 4 のいずれかに記載の認証装置。

[0068] (付記 6)

前記第 2 の認証用データが、特定の画像データを含み、
前記第 2 の認証部が前記端末装置の前記撮像装置によって撮影された画像
から、前記ユーザの顔以外の部分の画像を抽出し、前記第 2 の認証用データ
に、抽出した前記画像を照合することによって、認証を行う、
付記 1 ～ 5 のいずれかに記載の認証装置。

[0069] (付記 7)

撮像装置を有する携帯型の端末装置を用いた認証方法であって、
(a) 前記端末装置に保持されている顔認証用データに、前記端末装置の前
記撮像装置によって撮影されたユーザの顔の顔画像データを照合して、認証
を行う、ステップと、
(b) 前記端末装置に保持されている、顔以外の特徴による第 2 の認証用デ
ータを用いて、認証を行う、ステップと、
(c) 前記 (a) のステップによる認証結果と前記 (b) のステップによる
認証結果とに基づいて、前記ユーザが予め登録されている人物と一致するか
どうか判定する、ステップと、

(d) 前記(c)のステップによる判定の結果を、前記端末装置の画面に表示させる、ステップと、
を有することを特徴とする認証方法。

[0070] (付記8)

前記(a)～(d)のステップが、前記端末装置を構成するコンピュータによって実行され、前記端末装置が、前記顔認証用データ及び前記第2の認証用データを保持している、
付記7に記載の認証方法。

[0071] (付記9)

前記第2の認証用データが、特定の日時を含み、
前記(b)のステップにおいて、前記第2の認証用データに、前記(a)のステップによって認証が行われた日時を照合することによって、認証を行う、
付記7または8に記載の認証方法。

[0072] (付記10)

前記第2の認証用データが、指定された位置の座標を含み、
前記(b)のステップにおいて、前記第2の認証用データに、前記撮像装置によって前記ユーザの顔が撮影されたときの前記端末装置の位置の座標を照合することによって、認証を行う、
付記7～9のいずれかに記載の認証方法。

[0073] (付記11)

前記第2の認証用データが、指定された端末装置の識別子を含み、
前記(b)のステップにおいて、前記第2の認証用データに、前記端末装置に付与されている識別子を照合することによって、認証を行う、
付記7～10のいずれかに記載の認証方法。

[0074] (付記12)

前記第2の認証用データが、特定の画像データを含み、
前記(b)のステップにおいて、前記端末装置の前記撮像装置によって撮

影された画像から、前記ユーザの顔以外の部分の画像を抽出し、前記第 2 の認証用データに、抽出した前記画像を照合することによって、認証を行う、付記 7 ～ 11 のいずれかに記載の認証方法。

[0075] (付記 13)

撮像装置を有する携帯型の端末装置を構成する、コンピュータによって認証を行うためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記コンピュータに、

(a) 前記端末装置に保持されている顔認証用データに、前記端末装置の前記撮像装置によって撮影されたユーザの顔の顔画像データを照合して、認証を行う、ステップと、

(b) 前記端末装置に保持されている、顔以外の特徴による第 2 の認証用データを用いて、認証を行う、ステップと、

(c) 前記 (a) のステップによる認証結果と前記 (b) のステップによる認証結果とに基づいて、前記ユーザが予め登録されている人物と一致するかどうか判定する、ステップと、

(d) 前記 (c) のステップによる判定の結果を、前記端末装置の画面に表示させる、ステップと、

を実行させる命令を含む、プログラムを記録しているコンピュータ読み取り可能な記録媒体。

[0076] (付記 14)

前記 (a) ～ (d) のステップが、前記端末装置を構成するコンピュータによって実行され、前記端末装置が、前記顔認証用データ及び前記第 2 の認証用データを保持している、

付記 13 に記載のコンピュータ読み取り可能な記録媒体。

[0077] (付記 15)

前記第 2 の認証用データが、特定の日時を含み、

前記 (b) のステップにおいて、前記第 2 の認証用データに、前記 (a)

のステップによって認証が行われた日時を照合することによって、認証を行う、

付記 1 3 または 1 4 に記載のコンピュータ読み取り可能な記録媒体。

[0078] (付記 1 6)

前記第 2 の認証用データが、指定された位置の座標を含み、

前記 (b) のステップにおいて、前記第 2 の認証用データに、前記撮像装置によって前記ユーザの顔が撮影されたときの前記端末装置の位置の座標を照合することによって、認証を行う、

付記 1 3 ～ 1 5 のいずれかに記載のコンピュータ読み取り可能な記録媒体。

[0079] (付記 1 7)

前記第 2 の認証用データが、指定された端末装置の識別子を含み、

前記 (b) のステップにおいて、前記第 2 の認証用データに、前記端末装置に付与されている識別子を照合することによって、認証を行う、

付記 1 3 ～ 1 6 のいずれかに記載のコンピュータ読み取り可能な記録媒体。

[0080] (付記 1 8)

前記第 2 の認証用データが、特定の画像データを含み、

前記 (b) のステップにおいて、前記端末装置の前記撮像装置によって撮影された画像から、前記ユーザの顔以外の部分の画像を抽出し、前記第 2 の認証用データに、抽出した前記画像を照合することによって、認証を行う、
付記 1 3 ～ 1 7 のいずれかに記載のコンピュータ読み取り可能な記録媒体。

[0081] 以上、実施の形態を参照して本願発明を説明したが、本願発明は上記実施の形態に限定されるものではない。本願発明の構成や詳細には、本願発明の Scope 内で当業者が理解し得る様々な変更をすることができる。

[0082] この出願は、2017 年 11 月 15 日に提出された日本出願特願 2017-220360 を基礎とする優先権を主張し、その開示の全てをここに取り込む。

産業上の利用可能性

[0083] 以上のように、本発明によれば、顔画像を用いた認証処理に要するコスト

の低減と個人情報の漏洩の抑制とを図ることができる。本発明は、イベント等における来場者の本人確認、特定の部屋への入室時の本人確認、特定の建物、施設、飛行機の搭乗口への入場時の本人確認に有用である。

符号の説明

- [0084] 1 0 認証装置
 - 1 1 第1の認証部
 - 1 2 第2の認証部
 - 1 3 総合判定部
 - 1 4 表示部
- 2 0 端末装置
 - 2 1 撮像装置
 - 2 2 表示装置
 - 2 3 オペレーティングシステム
- 3 0 サーバ装置
- 4 0 ユーザ
- 5 0 イベント会場の係員
 - 5 1 第2の認証用の図形
- 1 1 0 コンピュータ
 - 1 1 1 CPU
 - 1 1 2 メインメモリ
 - 1 1 3 記憶装置
 - 1 1 4 入力インターフェイス
 - 1 1 5 表示コントローラ
 - 1 1 6 データリーダ／ライタ
 - 1 1 7 通信インターフェイス
 - 1 1 8 入力機器
 - 1 1 9 ディスプレイ装置
 - 1 2 0 記録媒体

1 2 1 バス

請求の範囲

- [請求項1] 撮像装置を有する携帯型の端末装置に備えられる認証装置であって、
- 、
- 前記端末装置に保持されている顔認証用データに、前記端末装置の前記撮像装置によって撮影されたユーザの顔の顔画像データを照合して、認証を行う、第1の認証部と、
- 前記端末装置に保持されている、顔以外の特徴による第2の認証用データを用いて、認証を行う、第2の認証部と、
- 前記第1の認証部による認証結果と前記第2の認証部による認証結果とに基づいて、前記ユーザが予め登録されている人物と一致するかどうか判定する、総合判定部と、
- 前記総合判定部による判定の結果を、前記端末装置の画面に表示させる、表示部と、
- を備えていることを特徴とする認証装置。
- [請求項2] 当該認証装置が、前記端末装置を構成するコンピュータで実行されるプログラムによって構築されており、
- 前記プログラムには、前記顔認証用データ及び前記第2の認証用データが、予め付加されている、
- 請求項1に記載の認証装置。
- [請求項3] 前記第2の認証用データが、特定の日時を含み、
- 前記第2の認証部が、前記第2の認証用データに、前記第1の認証部によって認証が行われた日時を照合することによって、認証を行う、
- 、
- 請求項1または2に記載の認証装置。
- [請求項4] 前記第2の認証用データが、指定された位置の座標を含み、
- 前記第2の認証部が、前記第2の認証用データに、前記撮像装置によって前記ユーザの顔が撮影されたときの前記端末装置の位置の座標を照合することによって、認証を行う、請求項1～3のいずれかに記

載の認証装置。

[請求項5] 前記第2の認証用データが、指定された端末装置の識別子を含み、
前記第2の認証部が、前記第2の認証用データに、前記端末装置に付与されている識別子を照合することによって、認証を行う、
請求項1～4のいずれかに記載の認証装置。

[請求項6] 前記第2の認証用データが、特定の画像データを含み、
前記第2の認証部が前記端末装置の前記撮像装置によって撮影された画像から、前記ユーザの顔以外の部分の画像を抽出し、前記第2の認証用データに、抽出した前記画像を照合することによって、認証を行う、
請求項1～5のいずれかに記載の認証装置。

[請求項7] 撮像装置を有する携帯型の端末装置を用いた認証方法であって、
(a) 前記端末装置に保持されている顔認証用データに、前記端末装置の前記撮像装置によって撮影されたユーザの顔の顔画像データを照合して、認証を行う、ステップと、
(b) 前記端末装置に保持されている、顔以外の特徴による第2の認証用データを用いて、認証を行う、ステップと、
(c) 前記(a)のステップによる認証結果と前記(b)のステップによる認証結果とに基づいて、前記ユーザが予め登録されている人物と一致するかどうか判定する、ステップと、
(d) 前記(c)のステップによる判定の結果を、前記端末装置の画面に表示させる、ステップと、
を有することを特徴とする認証方法。

[請求項8] 前記(a)～(d)のステップが、前記端末装置を構成するコンピュータによって実行され、前記端末装置が、前記顔認証用データ及び前記第2の認証用データを保持している、
請求項7に記載の認証方法。

[請求項9] 前記第2の認証用データが、特定の日時を含み、

前記（b）のステップにおいて、前記第2の認証用データに、前記（a）のステップによって認証が行われた日時を照合することによって、認証を行う、

請求項7または8に記載の認証方法。

[請求項10]

前記第2の認証用データが、指定された位置の座標を含み、

前記（b）のステップにおいて、前記第2の認証用データに、前記撮像装置によって前記ユーザの顔が撮影されたときの前記端末装置の位置の座標を照合することによって、認証を行う、

請求項7～9のいずれかに記載の認証方法。

[請求項11]

前記第2の認証用データが、指定された端末装置の識別子を含み、

前記（b）のステップにおいて、前記第2の認証用データに、前記端末装置に付与されている識別子を照合することによって、認証を行う、

請求項7～10のいずれかに記載の認証方法。

[請求項12]

前記第2の認証用データが、特定の画像データを含み、

前記（b）のステップにおいて、前記端末装置の前記撮像装置によって撮影された画像から、前記ユーザの顔以外の部分の画像を抽出し、前記第2の認証用データに、抽出した前記画像を照合することによって、認証を行う、

請求項7～11のいずれかに記載の認証方法。

[請求項13]

撮像装置を有する携帯型の端末装置を構成する、コンピュータによって認証を行うためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記コンピュータに、

（a）前記端末装置に保持されている顔認証用データに、前記端末装置の前記撮像装置によって撮影されたユーザの顔の顔画像データを照合して、認証を行う、ステップと、

（b）前記端末装置に保持されている、顔以外の特徴による第2の認

証用データを用いて、認証を行う、ステップと、

(c) 前記 (a) のステップによる認証結果と前記 (b) のステップによる認証結果とに基づいて、前記ユーザが予め登録されている人物と一致するかどうか判定する、ステップと、

(d) 前記 (c) のステップによる判定の結果を、前記端末装置の画面に表示させる、ステップと、

を実行させる命令を含む、プログラムを記録しているコンピュータ読み取り可能な記録媒体。

[請求項14] 前記 (a) ～ (d) のステップが、前記端末装置を構成するコンピュータによって実行され、前記端末装置が、前記顔認証用データ及び前記第2の認証用データを保持している、請求項13に記載のコンピュータ読み取り可能な記録媒体。

[請求項15] 前記第2の認証用データが、特定の日時を含み、前記 (b) のステップにおいて、前記第2の認証用データに、前記 (a) のステップによって認証が行われた日時を照合することによって、認証を行う、請求項13または14に記載のコンピュータ読み取り可能な記録媒体。

[請求項16] 前記第2の認証用データが、指定された位置の座標を含み、前記 (b) のステップにおいて、前記第2の認証用データに、前記撮像装置によって前記ユーザの顔が撮影されたときの前記端末装置の位置の座標を照合することによって、認証を行う、請求項13～15のいずれかに記載のコンピュータ読み取り可能な記録媒体。

[請求項17] 前記第2の認証用データが、指定された端末装置の識別子を含み、前記 (b) のステップにおいて、前記第2の認証用データに、前記端末装置に付与されている識別子を照合することによって、認証を行う、

請求項 1 3 ～ 1 6 のいずれかに記載のコンピュータ読み取り可能な記録媒体。

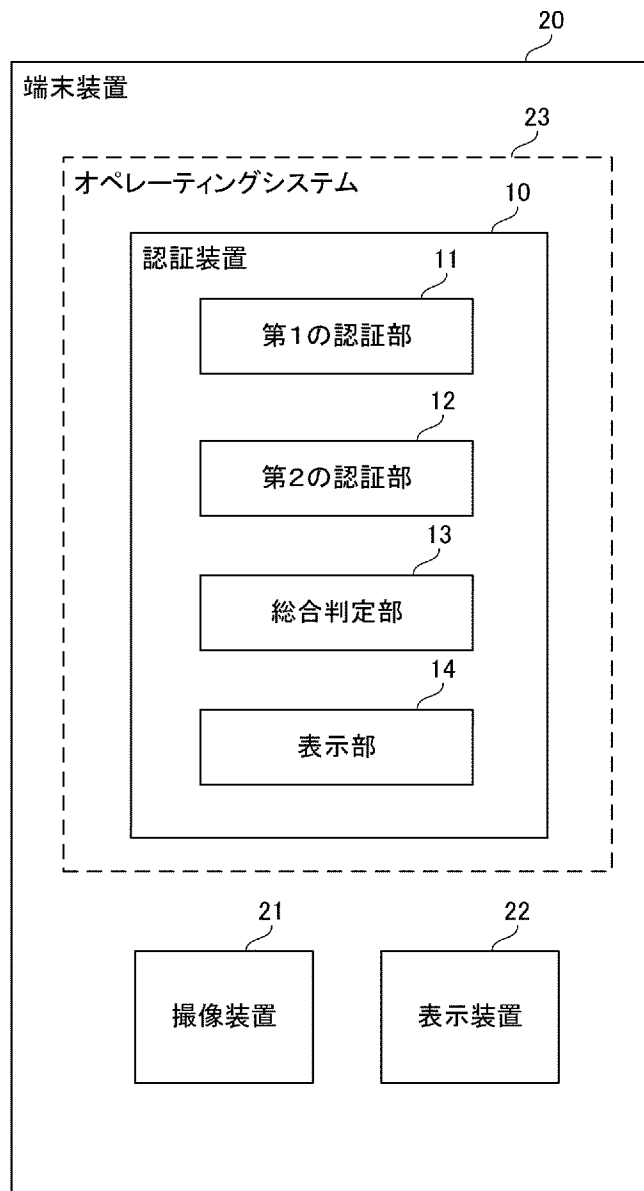
[請求項18]

前記第 2 の認証用データが、特定の画像データを含み、

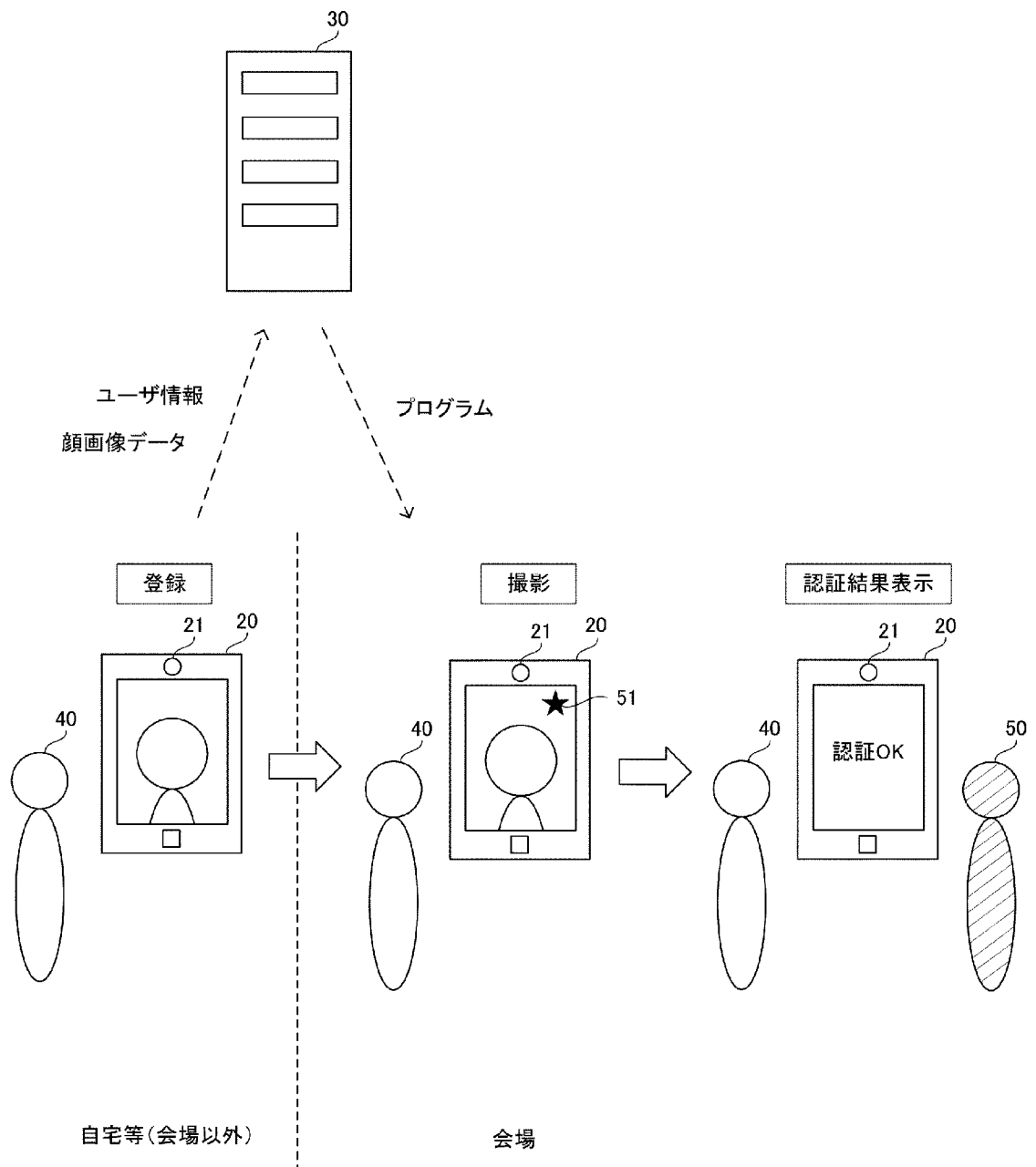
前記 (b) のステップにおいて、前記端末装置の前記撮像装置によって撮影された画像から、前記ユーザの顔以外の部分の画像を抽出し、前記第 2 の認証用データに、抽出した前記画像を照合することによって、認証を行う、

請求項 1 3 ～ 1 7 のいずれかに記載のコンピュータ読み取り可能な記録媒体。

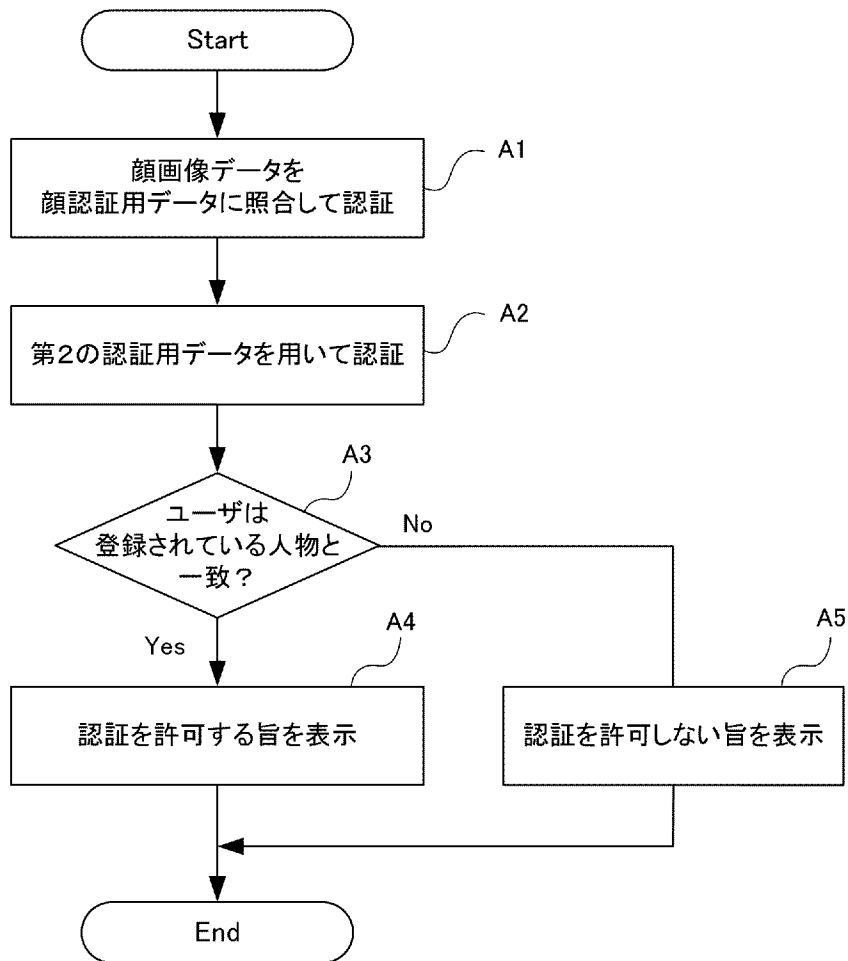
[図1]



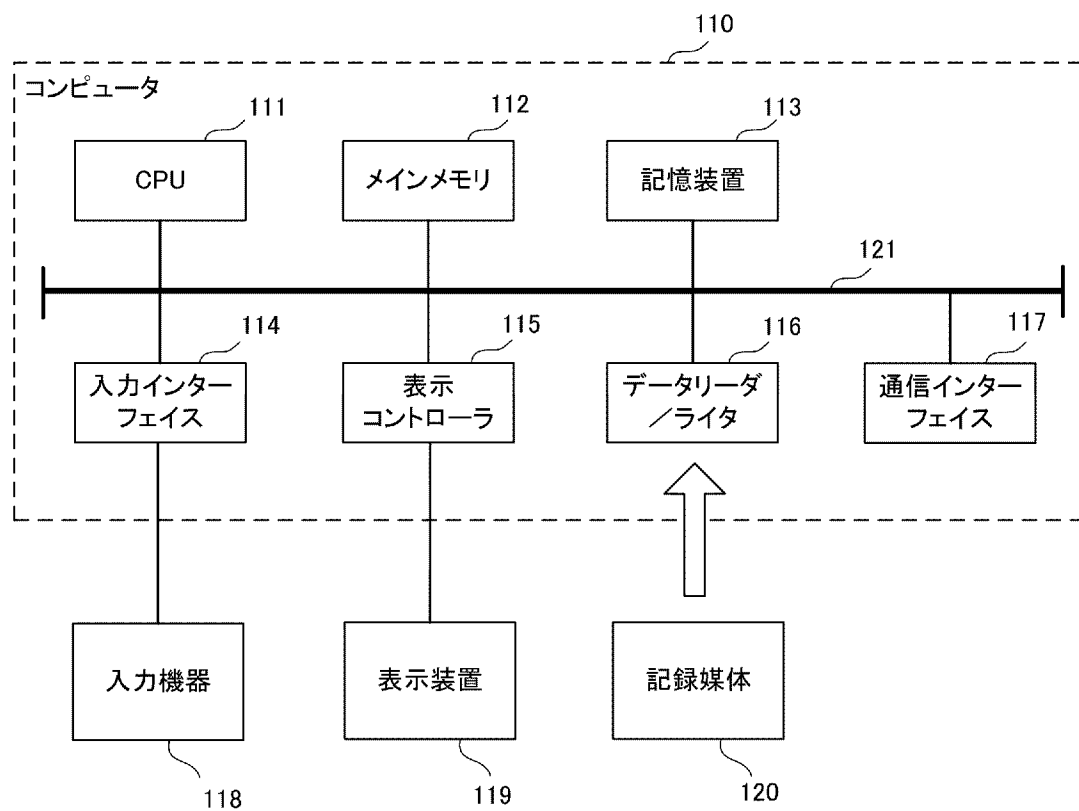
[図2]



[図3]



[図4]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/042024

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F21/31 (2013.01) i, G06F21/32 (2013.01) i, G06T7/00 (2017.01) i

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. G06F21/31, G06F21/32, G06T7/00

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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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	JP 2017-182326 A (NASC INTERNATIONAL CO., LTD.) 05 October 2017, paragraphs [0056]-[0091], [0098], fig. 1, 3-12 (Family: none)	1-2, 5, 7-8, 11, 13-14, 17
Y		3-4, 6, 9-10, 12, 15-16, 18
Y	JP 6050920 B1 (ASUHA CO., LTD.) 21 December 2016, paragraphs [0053]-[0116], fig. 1-7 & US 2018/0165433 A1, paragraphs [0077]-[0140], fig. 1-7	3-4, 6, 9-10, 12, 15-16, 18

☒ 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
06 February 2019 (06.02.2019)

Date of mailing of the international search report
19 February 2019 (19.02.2019)

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

International application No.

PCT/JP2018/042024

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2016/125603 A1 (SONY CORP.) 11 August 2016, paragraphs [0075]-[0110], fig. 6-8 & US 2017/0352197 A1, paragraphs [0103]-[0138], fig. 6-8 & EP 3255591 A1	6, 12, 18
A	JP 2015-103198 A (CANON MARKETING JAPAN INC., etc.) 04 June 2015 (Family: none)	1-18
A	JP 2004-118783 A (MITSUBISHI ELECTRIC CORP.) 15 April 2004 (Family: none)	1-18
P, X	JP 2018-060354 A (TECHFIRM KK) 12 April 2018, paragraphs [0021]-[0074], fig. 1-7 (Family: none)	1-5, 7-11, 13-17

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F21/31(2013.01)i, G06F21/32(2013.01)i, G06T7/00(2017.01)i

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））

Int.Cl. G06F21/31, G06F21/32, G06T7/00

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	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019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 2017-182326 A（ナスクインターナショナル株式会社） 2017.10.05, 段落[0056]-[0091], [0098], 第1, 3-12 図	1-2, 5, 7-8, 11, 13-14, 17
Y	（ファミリーなし）	3-4, 6, 9-10, 12, 15-16, 18
Y	JP 6050920 B1（アスハ株式会社）2016.12.21, 段落[0053]-[0116], 第1-7 図 & US 2018/0165433 A1, 段落[0077]-[0140], 第1-7 図	3-4, 6, 9-10, 12, 15-16, 18

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矛盾するものではなく、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

06.02.2019

国際調査報告の発送日

19.02.2019

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

田中 啓介

5 S

3 4 5 3

電話番号 03-3581-1101 内線 3546

C (続き) . 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
Y	WO 2016/125603 A1 (ソニー株式会社) 2016.08.11, 段落 [0075]-[0110], 第 6-8 図 & US 2017/0352197 A1, 段落 [0103]-[0138], 第 6-8 図 & EP 3255591 A1	6, 12, 18
A	JP 2015-103198 A (キャノンマーケティングジャパン株式会社 他) 2015.06.04 (ファミリーなし)	1-18
A	JP 2004-118783 A (三菱電機株式会社) 2004.04.15 (ファミリーなし)	1-18
P, X	JP 2018-060354 A (テックファーム株式会社) 2018.04.12, 段落 [0021]-[0074], 第 1-7 図 (ファミリーなし)	1-5, 7-11, 13- 17