

(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
2024年6月13日(13.06.2024)



(10) 国際公開番号

WO 2024/122002 A1

(51) 国際特許分類:
G06F 21/32 (2013.01)

(21) 国際出願番号: PCT/JP2022/045180

(22) 国際出願日: 2022年12月7日(07.12.2022)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 Tokyo (JP).

(72) 発明者: 新宮 由久 (SHINGU Yoshihisa); 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP). 太田 知秀 (OTA Tomohide); 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP). 柳澤 一精 (YANAGISAWA Issei); 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP). 四分一 大助 (SHIBUICHI Daisuke); 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: ▲高 ▼橋 幹夫 (TAKAHASHI Mikio); 〒2520137 神奈川県相模原市緑区二本松2-5-25 ユニゾン国際特許事務所 Kanagawa (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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,

(54) Title: TERMINAL, SYSTEM, METHOD FOR CONTROLLING TERMINAL, AND STORAGE MEDIUM

(54) 発明の名称: 端末、システム、端末の制御方法及び記憶媒体

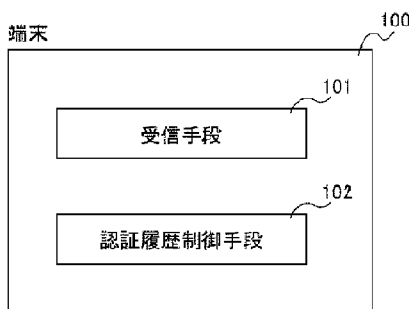


FIG.1

- 100 Terminal
101 Reception means
102 Authentication history control means

(57) Abstract: The present invention provides a terminal for achieving management or the like of an authentication history at a service provider selected by a user. The terminal comprises a reception means and an authentication history control means. The reception means receives an authentication success notification from a service server of a service provider that is selected by a user from among a plurality of service providers and has successfully executed biometric authentication of the user. The authentication history control means performs control relating to the history of successful biometric authentication at the service provider in response to reception of the authentication success notification.

(57) 要約: 利用者が選択したサービス提供者における認証履歴の管理等を実現する端末を提供する。端末は、受信手段と、認証履歴制御手段と、を備える。受信手段は、複数のサービス提供者のなかから利用者が選択したサービス提供者であって、当該利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信する。認証履歴制御手段は、認証成功通知の受信に応じて、サービス提供者において成功した生体認証の履歴に関する制御を行う。

DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS,
IT, LT, LU, LV, MC, ME, 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： 端末、システム、端末の制御方法及び記憶媒体 技術分野

[0001] 本発明は、端末、システム、端末の制御方法及び記憶媒体に関する。

背景技術

[0002] 生体認証に関する技術が存在する。

[0003] 例えば、特許文献 1 には、複数の認証端末を含む認証システムにおける利便性を向上させるサーバ装置を提供する、と記載されている。特許文献 1 のサーバ装置は、取得部と、認証部と、を備える。取得部は、認証成功と判定するための条件を含む認証ルールを取得する。認証部は、第 1 の端末から送信された第 1 の認証要求に応じて第 1 の生体認証を行い、第 2 の端末から送信された第 2 の認証要求に応じて、認証ルールを用いる第 2 の生体認証を行う。

[0004] 特許文献 2 には、一ユーザあたりの認証端末の占有時間を極力抑えながら、複数のサービス運営者が生体認証端末を利用できるようにする、と記載されている。特許文献 2 の認証装置は、認証テーブルと、受付手段と、認証手段と、通知手段と、を備える。認証テーブルは、各ユーザの識別情報、および、ユーザが所有するユーザ端末の連絡先を含む個人情報に対応づけて管理する。受付手段は、ユーザからユーザ識別情報および認証情報を受け付ける。認証手段は、ユーザから入力された認証情報と、認証するための基準となる基準認証情報とを比較し、その比較結果に基づき本人認証を行う。通知手段は、認証テーブルを参照し、ユーザに対応するユーザ端末に対して、本人認証の結果を通知する。

先行技術文献

特許文献

[0005] 特許文献1：国際公開第 2 0 2 2 / 1 7 6 0 4 2 号

特許文献2：特開 2 0 0 6 - 1 4 6 4 5 6 号公報

発明の概要

発明が解決しようとする課題

- [0006] 近年、生体認証を用いた様々なサービスの提供が始まっている。ここで、個人情報保護、プライバシー保護の観点から生体認証に用いる認証情報や認証結果等を利用者自身が管理したいという要望がある。具体的には、利用者が、複数のサービス提供者のなかから生体認証を受けるサービス提供者を選択し、当該選択したサービス提供者における認証履歴等を管理、確認したいという要望がある。
- [0007] なお、当該要望は、特許文献1や特許文献2に開示された技術を適用しても実現されない。特許文献1や特許文献2は、利用者が複数のサービス提供者のなかからサービス提供者を選択するような認証システムを開示していない。
- [0008] 本発明は、利用者が選択したサービス提供者における認証履歴の管理等を実現することに寄与する、端末、システム、端末の制御方法及び記憶媒体を提供することを主たる目的とする。

課題を解決するための手段

- [0009] 本発明の第1の視点によれば、複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信する、受信手段と、前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う、認証履歴制御手段と、を備える、端末が提供される。
- [0010] 本発明の第2の視点によれば、複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバと、前記利用者が所持する端末と、を含み、前記端末は、前記サービスサーバから、認証成功通知を受信する、受信手段と、前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う、認証履歴制御手段と、を備える、システ

ムが提供される。

[0011] 本発明の第3の視点によれば、端末において、複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信し、前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う、端末の制御方法が提供される。

[0012] 本発明の第4の視点によれば、端末に搭載されたコンピュータに、複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信する処理と、前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う処理と、を実行させるためのプログラムを記憶する、コンピュータ読取可能な記憶媒体が提供される。

発明の効果

[0013] 本発明の各視点によれば、利用者が選択したサービス提供者における認証履歴の管理等を実現することに寄与する、端末、システム、端末の制御方法及び記憶媒体が提供される。なお、本発明の効果は上記に限定されない。本発明により、当該効果の代わりに、又は当該効果と共に、他の効果が奏されてもよい。

図面の簡単な説明

[0014] [図1]図1は、一実施形態の概要を説明するための図である。

[図2]図2は、一実施形態の動作の一例を示すフローチャートである。

[図3]図3は、第1の実施形態に係る認証システムの概略構成の一例を示す図である。

[図4]図4は、第1の実施形態に係る認証システムの動作を説明するための図である。

[図5]図5は、第1の実施形態に係る認証システムの動作を説明するための図である。

[図6]図6は、第1の実施形態に係る認証システムの動作を説明するための図である。

[図7]図7は、第1の実施形態に係る認証システムの動作を説明するための図である。

[図8]図8は、第1の実施形態に係る制御サーバの処理構成の一例を示す図である。

[図9]図9は、第1の実施形態に係るアカウント管理データベースの一例を示す図である。

[図10]図10は、第1の実施形態に係る端末の表示の一例を示す図である。

[図11]図11は、第1の実施形態に係るサービスサーバの処理構成の一例を示す図である。

[図12]図12は、第1の実施形態に係る利用者管理データベースの一例を示す図である。

[図13]図13は、第1の実施形態に係る認証部の動作の一例を示すフローチャートである。

[図14]図14は、第1の実施形態に係る認証端末の処理構成の一例を示す図である。

[図15]図15は、第1の実施形態に係る端末の処理構成の一例を示す図である。

[図16]図16は、第1の実施形態に係る端末の表示の一例を示す図である。

[図17]図17は、第1の実施形態に係る認証履歴管理データベースの一例を示す図である。

[図18]図18は、第1の実施形態に係る端末の表示の一例を示す図である。

[図19]図19は、第1の実施形態に係る端末の表示の一例を示す図である。

[図20]図20は、第1の実施形態に係る端末の表示の一例を示す図である。

[図21]図21は、第1の実施形態に係る認証システムの動作の一例を示すシーケンス図である。

[図22]図22は、本願開示に係る制御サーバのハードウェア構成の一例を示す図である。

す図である。

[図23]図23は、本願開示の変形例に係る端末の表示の一例を示す図である。

[図24]図24は、本願開示の変形例に係る端末の表示の一例を示す図である。

発明を実施するための形態

[0015] はじめに、一実施形態の概要について説明する。なお、この概要に付記した図面参照符号は、理解を助けるための一例として各要素に便宜上付記したものであり、この概要の記載はなんらの限定を意図するものではない。また、特段の釈明がない場合には、各図面に記載されたブロックはハードウェア単位の構成ではなく、機能単位の構成を表す。各図におけるブロック間の接続線は、双方向及び単方向の双方を含む。一方向矢印については、主たる信号（データ）の流れを模式的に示すものであり、双方向性を排除するものではない。なお、本明細書及び図面において、同様に説明されることが可能な要素については、同一の符号を付することにより重複説明が省略され得る。

[0016] 一実施形態に係る端末100は、受信手段101と、認証履歴制御手段102と、を備える（図1参照）。受信手段101は、複数のサービス提供者のなかから利用者が選択したサービス提供者であって、当該利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信する（図2のステップS1）。認証履歴制御手段102は、認証成功通知の受信に応じて、サービス提供者において成功した生体認証の履歴に関する制御を行う（ステップS2）。

[0017] 利用者は、複数のサービス提供者のなかからサービスの提供を受けたいサービス提供者を選択する。当該選択に応じて、生体認証に使われる認証情報の原本が上記選択されたサービス提供者に提供される。サービス提供者のサービスサーバは、認証情報を使って利用者の認証に成功すると、当該認証成功の事実及び詳細を通知する認証成功通知を端末100に送信する。端末100は、当該認証成功通知の受信に応じて、生体認証の履歴に関する制御を

行う。例えば、端末１００は、利用者による認証履歴の閲覧を可能にする。このように、端末１００は、利用者が複数のサービス提供者のなかから選択したサービス提供者における認証履歴の管理等を実現する。認証履歴等を確認することで、利用者は、身に覚えのない不正な生体認証の実施等を発見できる。

[0018] 以下に具体的な実施形態について、図面を参照してさらに詳しく説明する。

[0019] [第１の実施形態]

第１の実施形態について、図面を用いてより詳細に説明する。

[0020] [システムの構成]

図３は、第１の実施形態に係る認証システム（情報処理システム）の概略構成の一例を示す図である。図３に示すように、認証システムには、複数のサービス提供者Ａ～Ｃ、認証センターが含まれる。

[0021] サービス提供者は、生体認証を用いて利用者にサービスを提供する事業者である。本願開示に係る認証システムは、様々な業種、業界に属するサービス提供者が生体認証を用いてサービスを提供することを前提とする。なお、サービス提供者により提供されるサービスは、有償無償を問わない。

[0022] 例えば、マンション等の賃貸住宅サービスを提供する事業者、従業員の勤務先である事業者（利用者の勤務先）、コンサート等のイベントを提供する事業者、航空機等の交通手段を運営する事業者等がサービス提供者として例示される。あるいは、宿泊サービスを提供する事業者、小売店等の事業者、金融サービスを提供する事業者、教育事業者等も本願開示のサービス提供者に含まれる。また、サービス提供者は、民間事業者に限らない。自治体等の公的機関がサービス提供者であってもよい。

[0023] 認証センターは、複数のサービス提供者それぞれの生体認証に関する制御、管理等を行う。利用者（一般消費者）に対して生体認証を用いたサービスを提供する事業者（サービス提供者）は、認証センターと契約を締結する必要がある。

- [0024] 認証センターは、制御サーバ10を備える。制御サーバ10は、認証センターの主たる機能を実現する。制御サーバ10は、認証センターの建物内に設置されていてもよいし、ネットワーク（クラウド）上に設置されたサーバであってもよい。
- [0025] 上述のように、サービス提供者は、生体認証を用いたサービスを利用者に提供する。例えば、利用者がオフィスに出勤する際やマンションに帰宅する際に生体認証が行われ、正当な資格を有する利用者（社員、住民）がオフィス等に入ることができる。あるいは、イベント会場等におけるチケット確認、ホテルにおけるチェックイン手続き、空港における出入国手続き等において生体認証が行われる。このようなサービス（手続き）においても正当な資格を有する利用者にサービスが提供される。あるいは、小売店等での決済手続きが生体認証を用いて行われる。
- [0026] 図3に示すように、各サービス提供者は、サービスサーバ20と、少なくとも1以上の認証端末30と、を備える。サービス提供者が備える装置（サービスサーバ20、認証端末30）は相互に通信可能に接続される。具体的には、サービスサーバ20と認証端末30は、有線又は無線の通信手段により接続される。
- [0027] サービスサーバ20は、ネットワークを介して制御サーバ10と接続されている。サービスサーバ20は、サービス提供者の建物に設置されていてもよいし、クラウド上に設置されていてもよい。
- [0028] サービスサーバ20は、利用者にサービスを提供する際に必要な情報を記憶する。具体的には、サービスサーバ20は、各サービス提供者が生体認証を用いたサービスを提供する際に必要な業務情報と、生体認証に必要な情報と、を記憶する。サービスサーバ20は、利用者管理データベースを用いて、業務情報と生体認証に必要な情報を記憶する。利用者管理データベースの詳細は後述する。
- [0029] 例えば、利用者が勤務する企業のサービスサーバ20は、利用者（従業員）の氏名、生年月日、社員番号、所属部署、勤務地等の情報を業務情報とし

て記憶する。また、イベントを主催するイベント会社のサービスサーバ20は、イベント参加者が購入したチケットに関する情報を業務情報として記憶する。さらに、小売店等のサービスサーバ20は、代金決済に必要なクレジットカード情報（決済情報）等を業務情報として記憶する。

[0030] サービスサーバ20が記憶する生体認証に必要な情報の詳細は後述する。

[0031] 認証端末30は、サービスの提供を受ける利用者のインターフェイスとなる装置である。認証端末30は、各サービス提供者それぞれのサービス提供場所に設置される。より具体的には、認証端末30は、利用者が実際に訪れる店舗等に設置される。

[0032] 認証端末30は、サービス提供者の業種等に応じた機能、形態を備える。例えば、職場やイベント会場に設置された認証端末30は、利用者（被認証者）の通行を制限するゲートを備えたゲート装置とすることができる。また、小売店に設置された認証端末30には、タブレット型の端末を用いることができる。

[0033] なお、図3は例示であって、本願開示の認証システムの構成等を限定する趣旨ではない。例えば、認証センターには2台以上の制御サーバ10が含まれていてもよい。また、認証システムには、少なくとも1以上のサービス提供者が参加していればよい。さらに、各サービス提供者は、少なくとも1台以上のサービスサーバ20と、少なくとも1台以上の認証端末30と、を備えていればよい。

[0034] [概略動作]

続いて、第1の実施形態に係る認証システムの概略動作について説明する。

[0035] <アカウント生成>

サービス提供者からサービスの提供を希望する利用者は、システムにアカウントを生成する必要がある。具体的には、利用者は、所持する端末40を操作して、制御サーバ10にアクセスする（図4参照）。

[0036] 利用者は、制御サーバ10が提供するWEB（ウェブ）ページ等において

、ログイン情報（例えば、ログインID、パスワード）、氏名、生年月日、連絡先等を入力する。制御サーバ10は、ログイン情報等を取得すると、当該利用者を識別するためのIDを生成する。なお、以降の説明において、制御サーバ10が生成したIDを「システムID」と表記する。制御サーバ10は、生成したシステムID、ログイン情報等に対応付けてアカウント管理データベースに記憶する。アカウント管理データベースの詳細は後述する。

[0037] ＜生体情報登録＞

生体認証を用いてサービスの提供を受けることを希望する利用者は、自身の生体情報を端末40に登録する必要がある。

[0038] ここで、生体認証を用いたサービスの提供には、生体情報から生成された認証情報が事前にサービス提供者に登録されている必要がある。例えば、顔認証を用いてサービスが提供される際には、顔画像から生成された特徴量（特徴ベクトル）が認証情報として事前に登録されている必要がある。あるいは、指紋認証を用いてサービスが提供される際には、指紋画像から生成された特徴量が認証情報として事前に登録されている必要がある。

[0039] 以降の説明において、顔画像や指紋画像のように、認証情報を生成する際の原本（基礎）となる情報を「原本生体情報」と表記する。また、原本生体情報から生成され、事前に登録される特徴量を「登録認証情報」と表記する。

[0040] システムアカウント生成を完了した利用者は、原本生体情報（例えば、顔画像）を所持する端末40に登録する必要がある。端末40は、GUI（Graphical User Interface）等を用いて原本生体情報を取得する。端末40は、取得した原本生体情報（例えば、顔画像）を内部に記憶する。このように、端末40は、生体認証に用いられる認証情報の原本となる原本生体情報を記憶する。

[0041] ＜サービスの選択＞

システム登録（システムアカウント作成）及び原本生体情報の登録を行った利用者は、生体認証サービスの提供を受けたいサービス提供者を選択する

。利用者は、認証システムに参加している複数のサービス提供者（認証センターと契約しているサービス提供者）のなかからサービスの提供を受けたいサービス提供者を選択する。

[0042] 制御サーバ10は、認証システムに参加しているサービス提供者の情報を記憶する。例えば、制御サーバ10は、サービス提供者の名称、業種、所在地等を記憶する。制御サーバ10は、複数のサービス提供者それぞれの情報を保持すると共に、利用者によるサービス提供者の選択を可能とする。

[0043] 利用者が端末40を操作してポータルサイト上にて所定の動作を行うと、制御サーバ10は、利用者が希望するサービス（サービス提供者）の選択を可能とするGUI等を端末40に表示する。制御サーバ10は、GUIを用いて利用者が希望するサービス（生体認証サービス）を取得する。

[0044] <利用者登録>

利用者が選択したサービス提供者を取得すると、制御サーバ10は、当該選択されたサービス提供者が、生体認証を用いたサービスを利用者に提供可能とする「利用者登録」に関する制御を実行する。

[0045] 具体的には、制御サーバ10は、利用者の端末40に格納された原本生体情報を上記選択されたサービス提供者が取得するための制御を行う。サービス提供者は、取得した原本生体情報から登録認証情報を生成し、当該生成した登録認証情報と業務情報を対応付けることで利用者にサービスを提供する準備が整う。

[0046] 利用者は、端末40を操作して制御サーバ10にアクセスし、当該利用者のポータルサイトにログインする。利用者がポータルサイト上で所定の操作（例えば、サービス提供者の選択ボタンの押下）を行うと、制御サーバ10は、サービス提供者の一覧を含むGUIを端末40に表示する。

[0047] サービス提供者が選択されると、制御サーバ10は、利用者に対して原本生体情報の提供を要求する。具体的には、制御サーバ10は、「原本提供要求」を利用者の端末40に送信する（図5のステップS01参照）。

[0048] 原本提供要求を受信すると、端末40は、利用者の原本生体情報（例えば

、顔画像）を制御サーバ１０に送信する（ステップＳ０２）。

[0049] 制御サーバ１０は、利用者のシステムＩＤ、取得した原本生体情報、個人特定情報等を利用者が選択したサービス提供者に通知する。なお、個人特定情報は、利用者を特定するための情報である。個人特定情報として、利用者の氏名、又は、氏名と生年月日の組み合わせが例示される。

[0050] 制御サーバ１０は、システムＩＤ、原本生体情報及び個人特定情報等を含む「利用者登録要求」を利用者が選択したサービス提供者のサービスサーバ２０に送信する（ステップＳ０３）。

[0051] 利用者登録要求を受信したサービスサーバ２０は、取得した個人特定情報を用いて利用者管理データベースを検索し、利用者登録（生体認証を用いたサービスの提供）を希望する利用者を特定する。サービスサーバ２０は、特定された利用者のエントリにシステムＩＤ、原本生体情報から得られる登録認証情報（例えば、特徴量）を記憶する。

[0052] サービスサーバ２０は、利用者登録の結果（利用者登録に成功、失敗）を含む応答を制御サーバ１０に送信する（ステップＳ０４）。

[0053] なお、制御サーバ１０は、利用者登録要求をサービスサーバ２０に送信したタイミング、又は当該要求に対する応答を受信したタイミングにおいて、利用者から取得した原本生体情報（例えば、顔画像）を削除する。また、サービスサーバ２０は、登録認証情報（例えば、特徴量）を生成すると、制御サーバ１０から取得した原本生体情報を削除する。

[0054] ＜サービスの提供＞

サービスの選択を完了した利用者は、サービスの提供を受けるためサービス提供者を訪れる。例えば、利用者は、オフィス、遊園地、イベント会場、小売店等自身で選択したサービスの提供を受けるサービス提供者の施設、店舗等を訪れる。

[0055] 認証端末３０は、サービスの提供を受ける利用者（被認証者）の生体情報を取得する。例えば、認証端末３０は、被認証者を撮影し、原本生体情報に対応する生体情報（例えば、顔画像）を取得する。認証端末３０は、取得し

た顔画像を含む認証要求をサービスサーバ20に送信する（図6参照）。なお、認証端末30は、必要に応じて、生体情報と共に他の情報（例えば、購入商品名、購入商品の代金等）をサービスサーバ20に送信する。あるいは、認証端末30は、生体情報（個人を特定するための情報、ID）と共に認証処理に使用される情報（例えば、クレジットカード情報）をサービスサーバ20に送信してもよい。

[0056] サービスサーバ20は、取得した顔画像から照合用の認証情報を生成する。例えば、サービスサーバ20は、照合用の顔画像から特徴量を生成する。サービスサーバ20は、当該生成された照合用の認証情報（以下、照合認証情報と表記する）と、利用者管理データベースに登録された登録認証情報と、を用いた照合処理（1対N照合；Nは正の整数、以下同じ）を実行する。

[0057] サービスサーバ20は、照合処理により利用者管理データベースに登録された利用者（被認証者）を特定する。

[0058] サービスサーバ20は、特定された利用者の業務情報を用いて当該利用者の認証を行う。例えば、社員の勤務先企業のサービスサーバ20は、被認証者が自社の社員であってオフィスに入場する資格を備えていれば「認証成功」と判定する。あるいは、イベント会場に設置されたサービスサーバ20は、被認証者が購入したチケットが有効であれば「認証成功」と判定する。あるいは、小売店に設置されたサービスサーバ20は、被認証者が購入した商品等の代金決済に成功すると「認証成功」と判定する。

[0059] なお、サービス提供者には、2種類のサービス事業者が存在する。

[0060] 第1のサービス提供者は、原則として、被認証者の認証に成功しても登録認証情報（特徴量）等を保持し続けるサービス提供者である。例えば、利用者の勤務先企業やマンション管理会社等が第1のサービス提供者として例示される。これらのサービス提供者は、利用者の認証（オフィス、マンション等への入退場）に成功しても利用者管理データベースに記憶された登録認証情報等を削除しない。あるいは、事前登録されたクレジットカード情報等を用いて商品代金の顔決済に関するサービスを提供する小売店も第1のサービ

ス提供者として例示される。当該小売店は、クレジットカード情報と登録認証情報を対応付けて記憶し続ける。

[0061] 第2のサービス提供者は、原則として、被認証者の認証に成功すると登録認証情報（特微量）等を削除するサービス提供者である。例えば、イベントを開催するイベント会社等が第2のサービス提供者として例示される。当該イベント会社は、利用者の認証に成功すると（購入チケットを用いて利用者がイベント会場に入場すると）、利用者管理データベースに記憶された登録認証情報を削除する。

[0062] なお、同じサービス提供者であっても、利用者に提供するサービスの内容によっては登録認証情報を記憶し続けたり、登録認証情報を削除したりする。例えば、遊園地等を運営する事業者は、1日の使用に限定されるチケットを販売する。この場合、当該事業者は、第2のサービス提供者となる。上記事業者が、所定期間に亘り遊園地等に入場できるチケット（例えば、年間チケット）も販売する場合、第1のサービス提供者となる。この場合、事業者は、年間チケットの期限が到来するまで登録認証情報を保持し続ける。

[0063] サービスサーバ20は、認証結果（認証成功、認証失敗）を認証端末30に送信する。

[0064] 認証端末30は、認証結果に応じた処理を実行する。例えば、認証成功を受信すると、オフィスに設置された認証端末30は、ゲートを開き被認証者の通行を許可する。あるいは、イベント会場に設置された認証端末30は、認証成功を受信すると、被認証者のゲート通過を許可する。あるいは、小売店に設置された認証端末30は、認証成功を受信すると、商品の決済が終了した旨を被認証者に通知する。

[0065] <認証成功の通知>

また、サービスサーバ20は、被認証者の認証に成功すると、その旨を利用者に通知する。サービスサーバ20は、認証結果の詳細を、制御サーバ10を介して利用者が所持する端末40に通知する。具体的には、被認証者の認証に成功すると、サービスサーバ20は、認証成功者（認証成功と判定さ

れた被認証者）のシステムID、認証処理の詳細情報及び認証情報の状態を含む認証成功通知を制御サーバ10に送信する（図7参照）。

[0066] 認証処理の詳細情報には、例えば、認証日時、認証場所、提供サービスの詳細（例えば、購入商品名、支払金額等）が含まれる。

[0067] 例えば、被認証者の勤務先のサービスサーバ20は、認証成功者の出勤日時、オフィス名を提供サービスの詳細として生成する。あるいは、例えば、小売店のサービスサーバ20は、認証成功者の来店日時、店舗、購入商品、支払金額等を提供サービスの詳細として生成する。

[0068] 認証情報の状態には、認証処理後における認証成功者の登録認証情報（特徴量）の状態（保持、削除）が設定される。

[0069] 例えば、被認証者の勤務先のような第1のサービス提供者のサービスサーバ20は、認証情報の状態に「認証情報保持」を設定する。あるいは、イベント会社のような第2のサービス提供者のサービスサーバ20は、認証情報の状態に「認証情報削除」を設定する。

[0070] 制御サーバ10は、認証成功通知を受信する。制御サーバ10は、認証成功通知に含まれるシステムIDをキーとしてアカウント管理データベースを検索し、対応するエントリ（利用者）を特定する。制御サーバ10は、特定した利用者の端末40にサービスサーバ20から受信した認証成功通知を送信（転送）する。

[0071] 端末40は、受信した認証成功通知に基づいて認証履歴を生成する。また、端末40は、認証成功通知を受信するたびに、当該通知の受信事実を利用者に通知する。例えば、端末40は、ポップアップ等の手段により認証成功通知に含まれる内容（認証処理の詳細、認証情報の状態）を表示する。

[0072] あるいは、端末40は、所定のボタン（履歴確認ボタン）が押下されると、認証履歴を表示する。利用者は、認証履歴を確認することで、不正利用の有無等を確認できる。

[0073] このように利用者が事前に選択したサービス提供者が当該利用者の認証に成功すると、当該認証成功の事実が利用者に通知される。なお、サービスサ

サーバ20は、上記説明したように、制御サーバ10を介して認証成功通知を端末40に送信してもよいし、制御サーバ10を介さずに直接、認証成功通知を端末40に送信してもよい。この場合、サービスサーバ20は、業務情報を取得する際、利用者の連絡先（端末40が受信可能なメールアドレス等）を取得すればよい。

[0074] 続いて、第1の実施形態に係る認証システムに含まれる各装置の詳細について説明する。

[0075] [制御サーバ]

図8は、第1の実施形態に係る制御サーバ10の処理構成（処理モジュール）の一例を示す図である。図8を参照すると、制御サーバ10は、通信制御部201と、アカウント管理部202と、事業者管理部203と、サービス選択制御部204と、利用者登録制御部205と、記憶部206と、を備える。

[0076] 通信制御部201は、他の装置との間の通信を制御する手段である。例えば、通信制御部201は、サービスサーバ20からデータ（パケット）を受信する。また、通信制御部201は、サービスサーバ20に向けてデータを送信する。通信制御部201は、他の装置から受信したデータを他の処理モジュールに引き渡す。通信制御部201は、他の処理モジュールから取得したデータを他の装置に向けて送信する。このように、他の処理モジュールは、通信制御部201を介して他の装置とデータの送受信を行う。通信制御部201は、他の装置からデータを受信する受信部としての機能と、他の装置に向けてデータを送信する送信部としての機能と、を備える。

[0077] アカウント管理部202は、利用者のアカウントを管理する手段である。アカウント管理部202は、利用者が端末40を操作して、所定のホームページ等にアクセスすると、当該利用者のアカウントを生成するために必要な情報を取得する。

[0078] 具体的には、アカウント管理部202は、ログイン情報、氏名、生年月日、連絡先（例えば、端末40が受信可能なメールアドレス）等の個人情報を

取得する。ログイン情報等を取得すると、アカウント管理部202は、当該利用者を識別するためのシステムIDを生成する。システムIDは、利用者を一意に識別できる情報であればどのような情報であってもよい。例えば、アカウント管理部202は、アカウント生成のたびに一意な値を採番しシステムIDとしてもよい。

[0079] アカウント管理部202は、生成されたシステムID、ログイン情報、氏名等を対応付けてアカウント管理データベースに記憶する（図9参照）。なお、図9に示すアカウント管理データベースは例示であって、記憶する項目等を限定する趣旨ではない。例えば、アカウント生成日時等がアカウント管理データベースに記憶されていてもよい。

[0080] また、アカウント管理部202は、利用者の端末40からポータルサイトにログインするためのログイン情報取得する。アカウント管理部202は、ログイン情報を使った認証を行う。

[0081] 事業者管理部203は、認証システムに参加するサービス提供者（サービス事業者）を管理する手段である。事業者管理部203は、各サービス提供者の職員等からシステム登録する事業者情報（サービス提供者の名称、業種、所在地、サービスサーバ20のアドレス等）を取得する。

[0082] 例えば、事業者管理部203は、事業者情報等を入力するためのインターフェイスを各サービス提供者に提供してもよい。あるいは、各サービス提供者は、事業者情報等が格納されたUSB（Universal Serial Bus）メモリ等を認証センターに送付してもよい。事業者管理部203は、認証センターの職員等から事業者情報等取得してもよい。

[0083] 事業者管理部203は、事業者情報等取得したサービス提供者についてのID（事業者ID）を生成する。事業者管理部203は、当該生成された事業者ID、取得した事業者情報等に対応付けて記憶する。

[0084] サービス選択制御部204は、利用者による生体認証サービス（サービス提供者）の選択を制御する手段である。サービス選択制御部204は、生体認証を用いたサービスを提供する複数のサービス提供者のなかから、利用者

がサービスの提供を受けたいサービス提供者を選択することを可能とする。

[0085] 利用者が端末40を操作してポータルサイトにログインし、当該ポータルサイト上で所定の動作を行うと、サービス選択制御部204は、例えば、図10に示すようなGUIを端末40に表示する。

[0086] 上記GUIを表示する際、サービス選択制御部204は、利用者が選択済のサービス提供者と未選択なサービス提供者を区別可能な表示を行う。図10の例では、サービス事業者を示すアイコンの右上にチェックが入ったサービス提供者は既に選択されたサービス提供者を示し、チェックが入っていないサービス提供者は未選択なサービス提供者を示す。

[0087] なお、サービス選択制御部204は、図10に示すようなGUIを表示するために事業者情報及びアカウント管理データベースに登録された情報を用いる。具体的には、サービス選択制御部204は、事業者情報を参照し、認証センターと契約を締結しているサービス提供者の一覧を生成する。また、サービス選択制御部204は、アカウント管理データベースの選択サービスフィールドを参照し、利用者が選択済のサービス提供者（サービス提供者の事業者ID）を取得する。

[0088] また、サービス選択制御部204は、サービス提供者の一覧を表示する際、各サービス提供者のより詳細な情報（例えば、業種、提供するサービス、店舗の場所等）も併せて利用者に提供してもよい。

[0089] サービス選択制御部204は、利用者が選択したサービス提供者の情報（例えば、利用者登録が希望されたサービス提供者の事業者ID）を利用者登録制御部205に引き渡す。

[0090] 利用者登録制御部205は、制御サーバ10による「利用者登録」を制御する手段である。利用者登録制御部205は、利用者により選択されたサービス提供者が生体認証を用いたサービスを当該利用者に提供可能とする「利用者登録」を制御する。

[0091] 利用者がサービス提供者を選択すると、利用者登録制御部205は、利用者が所持する端末40に「原本提供要求」を送信する。利用者登録制御部2

０５は、端末４０から利用者の原本生体情報（例えば、顔画像）を受信する。

[0092] 利用者登録制御部２０５は、利用者のシステムＩＤ、原本生体情報及び個人特定情報等を含む利用者登録要求を、利用者が選択したサービスに対応するサービス提供者のサービスサーバ２０に送信する。

[0093] なお、利用者登録制御部２０５は、アカウント管理データベースからシステムＩＤ及び個人特定情報（例えば、氏名又は氏名と生年月日の組み合わせ）を取得する。

[0094] 利用者登録制御部２０５は、利用者登録要求に対する応答（肯定応答、否定応答）を受信する。

[0095] 肯定応答（利用者登録に成功）を受信した場合、利用者登録制御部２０５は、利用者が選択したサービス提供者の事業者ＩＤをアカウント管理データベースに登録する。また、肯定応答を受信した場合、利用者登録制御部２０５は、選択されたサービス提供者に関する利用者登録に成功した旨を利用者に通知する。

[0096] 否定応答（利用者登録に失敗）を受信した場合、利用者登録制御部２０５は、その旨を利用者に通知する。

[0097] 記憶部２０６は、制御サーバ１０の動作に必要な情報を記憶する手段である。

[0098] [サービスサーバ]

図１１は、第１の実施形態に係るサービスサーバ２０の処理構成（処理モジュール）の一例を示す図である。図１１を参照すると、サービスサーバ２０は、通信制御部３０１と、業務情報管理部３０２と、利用者登録制御部３０３と、認証部３０４と、記憶部３０５と、を備える。

[0099] 通信制御部３０１は、他の装置との間の通信を制御する手段である。例えば、通信制御部３０１は、制御サーバ１０からデータ（パケット）を受信する。また、通信制御部３０１は、制御サーバ１０に向けてデータを送信する。通信制御部３０１は、他の装置から受信したデータを他の処理モジュール

に引き渡す。通信制御部３０１は、他の処理モジュールから取得したデータを他の装置に向けて送信する。このように、他の処理モジュールは、通信制御部３０１を介して他の装置とデータの送受信を行う。通信制御部３０１は、他の装置からデータを受信する受信部としての機能と、他の装置に向けてデータを送信する送信部としての機能と、を備える。

[0100] 業務情報管理部３０２は、サービス提供者が業務の提供に必要な業務情報に関する管理、制御を行う手段である。

[0101] 業務情報管理部３０２は、任意の手段を用いて自社、自組織のサービス提供に必要な業務情報を取得する。例えば、利用者の勤務先企業の業務情報管理部３０２は、従業員の氏名、生年月日、社員番号、所属部署、勤務地等の情報を業務情報として取得する。

[0102] 業務情報管理部３０２は、サービス提供者の職員等から上記業務情報を取得してもよいし、ホームページ等の手段を用いて利用者から直接、業務情報を取得してもよい。

[0103] 業務情報管理部３０２は、利用者管理データベースを用いて業務情報を管理する。

[0104] なお、業務情報管理部３０２のより詳細な説明は省略する。個別のサービスにおける業務情報の詳細やその取得方法は、本願開示の趣旨とは異なるためである。

[0105] 利用者登録制御部３０３は、サービス提供者による利用者登録を制御する手段である。利用者登録制御部３０３は、制御サーバ１０から受信した利用者登録要求を処理する。

[0106] 利用者登録要求を受信すると、利用者登録制御部３０３は、当該利用者登録要求に含まれる個人特定情報（例えば、氏名）をキーとして利用者管理データベースを検索し、対応する利用者（エントリ）を特定する。

[0107] 対応する利用者が利用者管理データベースに登録されていると、利用者登録制御部３０３は、取得した原本生体情報（例えば、顔画像）から登録認証情報を生成する。例えば、顔画像を取得した場合、利用者登録制御部３０３

は、自社で採用する顔認証アルゴリズムに対応した特徴量（特徴ベクトル）を登録認証情報として生成する。

[0108] 特徴量の生成処理に関しては既存の技術を用いることができるので、その詳細な説明を省略する。例えば、利用者登録制御部 303 は、顔画像から目、鼻、口等を特徴点として抽出する。その後、利用者登録制御部 303 は、特徴点それぞれの位置や各特徴点間の距離を特徴量として計算し、複数の特徴量からなる特徴ベクトル（顔画像を特徴づけるベクトル情報）を生成する。

[0109] 登録認証情報（例えば、特徴量）が生成されると、利用者登録制御部 303 は、システム ID、生成された登録認証情報（特徴量）及び業務情報を対応付けて利用者管理データベースに記憶する（図 12 参照）。

[0110] なお、図 12 に示す利用者管理データベースは例示であって、記憶する項目等を限定する趣旨ではない。例えば、利用者登録の日時等が利用者管理データベースに登録されていてもよい。

[0111] 利用者登録が正常に終了すると、利用者登録制御部 303 は、利用者登録に成功した旨を示す肯定応答を制御サーバ 10 に送信する。なお、利用者登録制御部 303 は、登録認証情報（例えば、特徴量）を生成し、当該生成された登録認証情報を利用者管理データベースに登録すると、制御サーバ 10 から取得した原本生体情報を削除する。

[0112] 利用者登録が正常に終了しなければ、利用者登録制御部 303 は、利用者登録に失敗した旨を示す否定応答を制御サーバ 10 に送信する。例えば、制御サーバ 10 から受信した個人特定情報（例えば、氏名）が利用者管理データベースに登録されていない場合や原本生体情報から有効な登録認証情報が生成できない場合等に、否定応答が制御サーバ 10 に送信される。

[0113] 認証部 304 は、被認証者の生体認証を行う手段である。

[0114] 図 13 は、第 1 の実施形態に係る認証部 304 の動作の一例を示すフローチャートである。図 13 を参照して、認証部 304 の動作を説明する。

[0115] 認証端末 30 から認証要求を受信すると、認証部 304 は、生体情報を用

いた照合処理を実行する（ステップS 1 0 1）。

[0116] 具体的には、認証部3 0 4は、認証要求に含まれる生体情報から照合認証情報を生成する。例えば、顔画像を取得すると、認証部3 0 4は、自社で採用している顔認証アルゴリズムに対応した特徴量を生成する。認証部3 0 4は、生成した照合認証情報（特徴量）と、利用者管理データベースに登録された登録認証情報（特徴量）と、を用いた照合処理を実行する。

[0117] 具体的には、認証部3 0 4は、照合対象の特徴量（特徴ベクトル）と登録側の複数の特徴量それぞれとの間の類似度を計算する。当該類似度には、カイ二乗距離やユークリッド距離等を用いることができる。なお、距離が離れているほど類似度は低く、距離が近いほど類似度が高い。

[0118] 類似度が所定の値以上の特徴量が存在しなければ、認証部3 0 4は、照合処理に失敗したと判定する。類似度が所定の値以上の特徴量が存在すれば、認証部3 0 4は、照合処理に成功したと判定する。照合処理に成功すると、利用者管理データベースに登録された複数のエントリのうち最も類似度が高い特徴量（登録認証情報）を持つエントリの利用者が被認証者として特定される。

[0119] 照合処理に失敗すると（ステップS 1 0 2、N o分岐）、認証部3 0 4は、処理を終了する。この場合、認証部3 0 4は、認証に失敗した旨を認証端末3 0に通知してもよい。あるいは、認証部3 0 4は、顔認証の健全性を確認するため、照合処理に失敗した事実及び照合処理の詳細をログとして記憶してもよい。

[0120] 照合処理に成功すると（ステップS 1 0 2、Y e s分岐）、認証部3 0 4は、照合処理により特定された被認証者の業務情報を用いて当該被認証者にサービスの提供が可能か否か判定する。認証部3 0 4は、業務情報によるサービス提供可否の判定を行う（ステップS 1 0 3）。

[0121] 例えば、社員の勤務先企業のサービスサーバ2 0の認証部3 0 4は、被認証者が自社の社員であってオフィスに入場する資格を備えていれば、サービスの提供が可能と判定する。あるいは、イベント会社のサービスサーバ2 0

は、被認証者が購入したチケットが有効であれば、サービスの提供が可能と判定する。あるいは、小売店等のサービスサーバ20の認証部304は、クレジットカード情報等を用いた商品代金の決済に成功した場合に、サービスの提供が可能と判定する。

[0122] なお、各サービス提供者における業務情報を用いた認証処理に関するより詳細な説明を省略する。各サービス提供者に特有な処理は本願開示の趣旨とは異なるためである。

[0123] サービスの提供が不可な場合（ステップS104、No分岐）、認証部304は、認証結果に「認証失敗」を設定する（ステップS105）。

[0124] サービスの提供が可能な場合（ステップS104、Yes分岐）、認証部304は、認証結果に「認証成功」を設定する（ステップS106）。

[0125] 認証部304は、認証結果（認証成功、認証失敗）を認証端末30に送信する（ステップS107）。

[0126] 認証失敗の場合には、認証部304は、その旨を示す否定応答を認証端末30に送信する。

[0127] 認証成功の場合には、認証部304は、その旨を示す肯定応答を認証端末30に送信する。その際、認証部304は、必要に応じて、利用者にサービスを提供するために必要な情報を含む肯定応答を認証端末30に送信する。上記住民票発行の例では、住民票を発行（印刷）するために必要な情報が認証端末30に送信される。

[0128] また、認証成功の場合には、認証部304は、必要に応じて利用者管理データベースの更新を行う（データベースの更新；ステップS108）。より具体的には、認証部304は、認証処理の内容に応じて、少なくとも認証成功者の登録認証情報を削除する。

[0129] 例えば、認証部304は、被認証者の入退（オフィスへの出勤、マンションへの帰宅等）に関する認証処理の場合には特段の処理を行わない（登録認証情報を削除しない）。あるいは、クレジットカード情報を使って被認証者が購入した商品の決済を行った場合にも、認証部304は、特段の処理を行

わない。

[0130] このように、認証成功者の登録認証情報を削除しない場合には、認証部 304 は、認証情報の状態に「認証情報保持」を設定する。

[0131] 被認証者が購入チケットを利用してイベント会場等に入場した場合には、認証部 304 は、当該被認証者の登録認証情報を削除する（対応する利用者管理データベースのエントリを削除する）。この場合、認証部 304 は、認証情報の状態に「認証情報削除」を設定する。

[0132] 登録認証情報を削除するか否かは、利用者に提供されるサービスに応じて予め定められている。あるいは、業務情報に含まれる情報に基づいて登録認証情報（登録認証情報を含むエントリ）の削除が決定されてもよい。例えば、利用者の購入したチケットが「年間パスポート」のような繰り返し使えるチケットの場合には、認証部 304 は、登録認証情報を削除しない。

[0133] 認証成功の場合には、認証部 304 は、認証成功通知を制御サーバ 10 に送信する（ステップ S109）。

[0134] 具体的には、認証部 304 は、被認証者（照合処理により特定された利用者）のシステム ID、認証処理の詳細情報及び認証情報の状態を含む認証成功通知を制御サーバ 10 に送信する。

[0135] 認証部 304 は、照合処理により特定されたエントリ（利用者管理データベースのエントリ）から上記システム ID を取得する。

[0136] 認証部 304 は、認証端末 30 から受信した認証要求を処理した日時から認証日時を生成し、当該認証端末 30 の設置場所から認証場所を生成する。また、認証部 304 は、業務情報を使った認証処理の内容から提供サービスの詳細を生成する。

[0137] 例えば、被認証者が勤務先に出勤した場合、認証部 304 は、「認証日時＝2022年11月7日、08：30」、「認証場所＝本社ビル」、「提供サービスの詳細＝出勤」といった内容を含む認証処理の詳細情報を生成する。あるいは、被認証者が小売店で商品を購入した場合、認証部 304 は、「認証日時＝2022年11月7日、13：00」、「認証場所＝駅前店」、

「提供サービスの詳細＝栄養ドリンク購入、３００円」といった内容の認証処理の詳細情報を生成する。

[0138] なお、利用者が退職した、利用者がマンションから退去した、年間パスポートの有効期限が経過した等が発生すると、利用者管理データベースから対応する利用者のエントリが削除される。この場合、当該利用者の認証に成功することはないので、利用者管理データベースの更新や認証成功通知の送信が行われることはない。

[0139] 記憶部３０５は、サービスサーバ２０の動作に必要な情報を記憶する手段である。

[0140] [認証端末]

図１４は、第１の実施形態に係る認証端末３０の処理構成（処理モジュール）の一例を示す図である。図１４を参照すると、認証端末３０は、通信制御部４０１と、提供サービス制御部４０２と、認証要求部４０３と、記憶部４０４と、を備える。

[0141] 通信制御部４０１は、他の装置との間の通信を制御する手段である。例えば、通信制御部４０１は、サービスサーバ２０からデータ（パケット）を受信する。また、通信制御部４０１は、サービスサーバ２０に向けてデータを送信する。通信制御部４０１は、他の装置から受信したデータを他の処理モジュールに引き渡す。通信制御部４０１は、他の処理モジュールから取得したデータを他の装置に向けて送信する。このように、他の処理モジュールは、通信制御部４０１を介して他の装置とデータの送受信を行う。通信制御部４０１は、他の装置からデータを受信する受信部としての機能と、他の装置に向けてデータを送信する送信部としての機能と、を備える。

[0142] 提供サービス制御部４０２は、利用者に提供するサービスに関する制御を実行する手段である。提供サービス制御部４０２は、認証端末３０に割り当てられた機能を実現する。

[0143] 提供サービス制御部４０２は、利用者がサービスの享受を希望すると、当該利用者（被認証者）の生体情報（例えば、顔画像）を取得する。例えば、

提供サービス制御部402は、定期的又は所定のタイミングにおいて自装置の前方を撮像する。提供サービス制御部402は、取得した画像に人の顔画像が含まれるか否かを判定し、顔画像が含まれる場合には取得した画像データから顔画像を抽出する。

[0144] なお、提供サービス制御部402による顔画像の検出処理や顔画像の抽出処理には既存の技術を用いることができるので詳細な説明を省略する。例えば、提供サービス制御部402は、CNN（Convolutional Neural Network）により学習された学習モデルを用いて、画像データの中から顔画像（顔領域）を抽出してもよい。あるいは、提供サービス制御部402は、テンプレートマッチング等の手法を用いて顔画像を抽出してもよい。

[0145] 提供サービス制御部402は、取得した生体情報（例えば、顔画像）を認証要求部403に引き渡す。

[0146] 認証要求部403は、サービスサーバ20に対して被認証者の認証を要求する手段である。認証要求部403は、被認証者の認証が必要になると、被認証者（認証端末30の面前の利用者）の生体情報を含む認証要求をサービスサーバ20に送信する。

[0147] 認証要求部403は、サービスサーバ20から認証結果（認証成功、認証失敗）を受信する。認証要求部403は、受信した認証結果を提供サービス制御部402に引き渡す。

[0148] 例えば、利用者の勤務先に設置された認証端末30の提供サービス制御部402は、認証成功を受信すると、ゲートを開き被認証者の入場を許可する。

[0149] 認証失敗を受信した場合、提供サービス制御部402は、予め定められたメッセージ等を出力してもよい。

[0150] なお、各サービス提供者の認証端末30に含まれる提供サービス制御部402に関するより詳細な説明は省略する。提供サービス制御部402による認証端末30の機能実現は、本願開示の趣旨とは異なるためである。

[0151] 記憶部404は、認証端末30の動作に必要な情報を記憶する手段である

。

[0152] [端末]

図15は、第1の実施形態に係る端末40の処理構成（処理モジュール）の一例を示す図である。図15を参照すると、端末40は、通信制御部501と、アカウント生成制御部502と、原本情報取得部503と、サービス選択部504と、認証履歴制御部505と、記憶部506と、を備える。

[0153] 通信制御部501は、他の装置との間の通信を制御する手段である。例えば、通信制御部501は、制御サーバ10からデータ（パケット）を受信する。また、通信制御部501は、制御サーバ10に向けてデータを送信する。通信制御部501は、他の装置から受信したデータを他の処理モジュールに引き渡す。通信制御部501は、他の処理モジュールから取得したデータを他の装置に向けて送信する。このように、他の処理モジュールは、通信制御部501を介して他の装置とデータの送受信を行う。通信制御部501は、他の装置からデータを受信する受信部としての機能と、他の装置に向けてデータを送信する送信部としての機能と、を備える。

[0154] 通信制御部501は、複数のサービス提供者それぞれの生体認証に関する管理を行う、制御サーバ10からの要求に応じて、記憶部506に記憶された原本生体情報を、制御サーバ10を介して利用者が選択したサービス提供者のサービスサーバ20に送信する。また、通信制御部501は、複数のサービス提供者のなかから利用者が選択したサービス提供者であって、当該利用者の生体認証に成功したサービス提供者のサービスサーバ20から、直接的又は間接的に認証成功通知を受信する。

[0155] アカウント生成制御部502は、利用者によるアカウント生成を制御する手段である。アカウント生成制御部502は、利用者の操作に応じて、制御サーバ10が提供する所定のWEBページ等にアクセスする。

[0156] アカウント生成制御部502は、利用者の操作に応じて、当該WEBページに、ログイン情報、氏名、生年月日、連絡先等を入力する。

[0157] 原本情報取得部503は、利用者の生体情報（原本生体情報）を取得する

手段である。原本情報取得部503は、利用者の操作に応じて、原本生体情報（例えば、顔画像）を取得するためのGUI等を表示する。例えば、原本情報取得部503は、図16に示すようなGUIを用いて原本生体情報を取得する。

[0158] 原本情報取得部503は、取得した原本生体情報（例えば、顔画像）を記憶部506に格納する。その際、原本情報取得部503は、取得した原本生体情報に暗号化、コード化等を施し、当該暗号化された原本生体情報を記憶部506に記憶してもよい。即ち、利用者が所持する端末40は、暗号化された原本生体情報を保持してもよい。暗号化された原本生体情報は、原本生体情報が制御サーバ10に送信される際に復号されてもよい。あるいは、暗号化された原本生体情報を復号するための情報（例えば、共通鍵）が端末40と制御サーバ10の間で共有され、制御サーバ10が暗号化された原本生体情報を復号してもよい。

[0159] なお、端末40は、原則として、利用者の原本生体情報（例えば、顔画像）を削除しない。即ち、端末40は、利用者からの明確な指示がなければ記憶部506に記憶された原本生体情報を削除しない。

[0160] サービス選択部504は、利用者による生体認証サービスの選択を可能とする手段である。サービス選択部504は、利用者の操作に応じて、制御サーバ10が提供するポータルサイトにログインする。サービス選択部504は、制御サーバ10が提供するGUIを用いて利用者が選択したサービス提供者の情報を制御サーバ10に送信する。

[0161] サービス選択部504は、制御サーバ10から原本提供要求を受信する。当該要求を受信すると、サービス選択部504は、記憶部506に記憶された原本生体情報を制御サーバ10に送信する。原本生体情報は、制御サーバ10を介して、利用者が選択したサービス提供者のサービスサーバ20に送信される。

[0162] 認証履歴制御部505は、利用者の認証履歴に関する制御を実行する手段である。認証履歴制御部505は、制御サーバ10から受信する認証成功通

知を処理する。認証履歴制御部505は、認証成功通知の受信に応じて、サービス提供者において成功した生体認証の履歴に関する制御を行う。

[0163] 認証成功通知には、サービス提供者が成功した認証処理の詳細情報と、サービス提供者が生体認証に用いる認証情報の状態と、が含まれる。

[0164] 認証履歴制御部505は、認証成功通知に含まれる認証処理の詳細情報及び認証情報の状態を認証履歴管理データベースに記憶する（図17参照）。認証履歴制御部505は、認証処理の詳細情報及び認証情報の状態を認証履歴管理データベースに記憶することで、利用者の生体認証に関する履歴を生成する。なお、図17に示す認証履歴管理データベースは例示であって、記憶する項目等を限定する趣旨ではない。

[0165] また、認証成功通知を受信すると、認証履歴制御部505は、利用者（端末40の所有者）の認証が行われた事実を当該利用者に通知する。例えば、認証履歴制御部505は、認証成功通知を受信するたびに、図18に示すようなポップアップ通知を用いて利用者の認証に関する情報を表示する。即ち、認証履歴制御部505は、認証成功通知を受信するたびに、認証処理の詳細情報及び認証情報の状態を含むメッセージを表示する。

[0166] あるいは、認証履歴制御部505は、利用者が所定の動作を行うと（例えば、認証履歴ボタンを押下すると）、認証履歴管理データベースに記憶された認証履歴の一覧を表示する（図19参照）。即ち、認証履歴制御部505は、利用者の所定の操作に応じて、認証履歴管理データベースに記憶された生体認証に関する履歴の表示を行う。

[0167] なお、認証履歴制御部505は、認証履歴の一覧表示を行う際、図19に示すように、認証処理の詳細情報を表示してもよいし、図20に示すように認証処理の詳細情報に加えて認証情報の状態を表示してもよい。

[0168] 記憶部506は、端末40の動作に必要な情報を記憶する手段である。記憶部506は、生体認証に用いられる認証情報の原本となる原本生体情報を記憶する。なお、例えば、原本生体情報は顔画像であり、認証情報は顔画像から生成された特徴量である。

[0169] [システムの動作]

続いて、第1の実施形態に係る認証システムの動作について説明する。なお、アカウント生成等に関する動作の説明は省略する。図21は、第1の実施形態に係る認証システムの動作の一例を示すシーケンス図である。

[0170] 認証端末30から認証要求を受信すると、サービスサーバ20は、認証処理を実行する（ステップS21）。

[0171] 被認証者の認証に成功すると、サービスサーバ20は、認証成功通知を制御サーバ10に送信する（ステップS22）。

[0172] 制御サーバ10は、認証成功通知を認証成功者の端末40に転送する（ステップS23）。

[0173] 端末40は、認証処理が行われた事実（認証に成功した事実及びその詳細）を利用者に通知する（認証の事実を通知；ステップS24）。

[0174] 続いて、第1の実施形態に係る変形例について説明する。

[0175] <第1の実施形態に係る変形例1>

利用者は、所定のコードを用いてサービス提供者を選択してもよい。例えば、数多くのサービス提供者のなかから利用者が容易にサービス選択者を指定可能とする管理コードが使用されてもよい。例えば、制御サーバ10は、図10に示されたアイコンの一覧において、利用者が所定のアイコンを選択すると、管理コードの入力を求めるGUIを表示する。制御サーバ10は、利用者が入力した管理コードに対応するサービス提供者を当該利用者により選択されたサービス提供者として扱う。

[0176] あるいは、制御サーバ10は、利用者が入力する管理コードをパスワードのように扱ってもよい。具体的には、利用者がサービス提供者を選択すると、制御サーバ10は、当該選択されたサービス提供者の管理コードの入力を利用者に求める。制御サーバ10は、利用者が入力した管理コードと、選択されたサービス提供者の予め定められた管理コードと、が一致した場合、利用者によるサービス提供者の選択を受け入れてもよい。換言すれば、制御サーバ10は、上記2つの管理コードが一致しない場合、利用者によるサービ

ス提供者の選択を拒否する。

[0177] <第1の実施形態に係る変形例2>

上記実施形態では、利用者登録の際、サービス提供者（サービスサーバ20）は個人特定情報を用いて利用者を特定する場合について説明した。しかし、当該利用者の選択は、サービス提供者が利用者（顧客）を管理するID（以下、個別IDと表記する）を用いて行われてもよい。

[0178] 具体的には、利用者がサービス提供者を選択すると、制御サーバ10は、当該利用者のシステムIDが埋め込まれたリダイレクト用URL（Uniform Resource Locator）を端末40に送信する。当該リダイレクト用URLは、利用者が選択したサービス提供者のポータルサイト（アカウント）へログインするためのURLである。

[0179] 受信したリダイレクト用URLに従って、利用者がサービス提供者のログインページにログインすると、サービスサーバ20は、当該利用者の個別ID（ログインID）とリダイレクト用URLに埋め込まれたシステムIDを取得する。

[0180] サービスサーバ20は、取得した個別IDを用いて利用者管理データベースを検索し、対応するエントリ（利用者）を特定する。サービスサーバ20は、特定したエントリにシステムIDを記憶する。

[0181] このように、システムIDが埋め込まれたリダイレクト用URLが使用されて、利用者登録が実現されてもよい。

[0182] 以上のように、第1の実施形態に係る認証システムは、利用者の端末40に格納された原本生体情報は、当該利用者が選択したサービス提供者のサービスサーバ20に提供される。サービスサーバ20は、当該利用者の原本生体情報から登録認証情報を生成し、当該生成した登録認証情報と業務情報に対応付けて記憶することで、利用者に生体認証を用いたサービスの提供を可能とする。利用者がサービス提供者から生体認証サービスを受けると、サービスサーバ20は、制御サーバ10を介して認証成功通知を利用者の端末40に送信する。認証成功通知の受信に応じて、端末40は、サービス提供者

にて生体認証が行われた事実をポップアップ通知したり、過去の認証結果の一覧を表示したりする。利用者は、当該ポップアップ通知や認証履歴の一覧表示により、不正な生体認証が行われていないか検証できる。換言すれば、利用者は、ポップアップ通知や認証履歴の一覧表示により不正な生体認証を発見できる。

[0183] 続いて、認証システムを構成する各装置のハードウェアについて説明する。図22は、制御サーバ10のハードウェア構成の一例を示す図である。

[0184] 制御サーバ10は、情報処理装置（所謂、コンピュータ）により構成可能であり、図22に例示する構成を備える。例えば、制御サーバ10は、プロセッサ311、メモリ312、入出力インターフェイス313及び通信インターフェイス314等を備える。上記プロセッサ311等の構成要素は内部バス等により接続され、相互に通信可能に構成されている。

[0185] 但し、図22に示す構成は、制御サーバ10のハードウェア構成を限定する趣旨ではない。制御サーバ10は、図示しないハードウェアを含んでもよいし、必要に応じて入出力インターフェイス313を備えていなくともよい。また、制御サーバ10に含まれるプロセッサ311等の数も図22の例示に限定する趣旨ではなく、例えば、複数のプロセッサ311が制御サーバ10に含まれていてもよい。

[0186] プロセッサ311は、例えば、CPU（Central Processing Unit）、MPU（Micro Processing Unit）、DSP（Digital Signal Processor）等のプログラマブルなデバイスである。あるいは、プロセッサ311は、FPGA（Field Programmable Gate Array）、ASIC（Application Specific Integrated Circuit）等のデバイスであってもよい。プロセッサ311は、オペレーティングシステム（OS；Operating System）を含む各種プログラムを実行する。

[0187] メモリ312は、RAM（Random Access Memory）、ROM（Read Only Memory）、HDD（Hard Disk Drive）、SSD（Solid State Drive）等である。メモリ312は、OSプログラム、アプリケーションプログラム、各種

データを格納する。

[0188] 入出力インターフェイス 313 は、図示しない表示装置や入力装置のインターフェイスである。表示装置は、例えば、液晶ディスプレイ等である。入力装置は、例えば、キーボードやマウス等のユーザ操作を受け付ける装置である。

[0189] 通信インターフェイス 314 は、他の装置と通信を行う回路、モジュール等である。例えば、通信インターフェイス 314 は、NIC (Network Interface Card) 等を備える。

[0190] 制御サーバ 10 の機能は、各種処理モジュールにより実現される。当該処理モジュールは、例えば、メモリ 312 に格納されたプログラムをプロセッサ 311 が実行することで実現される。また、当該プログラムは、コンピュータが読み取り可能な記憶媒体に記録することができる。記憶媒体は、半導体メモリ、ハードディスク、磁気記録媒体、光記録媒体等の非トランジエント (non-transitory) なものとすることができる。即ち、本発明は、コンピュータプログラム製品として具現することも可能である。また、上記プログラムは、ネットワークを介してダウンロードするか、あるいは、プログラムを記憶した記憶媒体を用いて、更新することができる。さらに、上記処理モジュールは、半導体チップにより実現されてもよい。

[0191] なお、サービスサーバ 20、認証端末 30、端末 40 等も制御サーバ 10 と同様に情報処理装置により構成可能であり、その基本的なハードウェア構成は制御サーバ 10 と相違する点はないので説明を省略する。例えば、認証端末 30 は、被認証者を撮影するためのカメラ装置を備えていればよい。

[0192] 情報処理装置である制御サーバ 10 は、コンピュータを搭載し、当該コンピュータにプログラムを実行させることで制御サーバ 10 の機能が実現できる。また、制御サーバ 10 は、当該プログラムにより制御サーバ 10 の制御方法を実行する。同様に、情報処理装置である端末 40 は、コンピュータを搭載し、当該コンピュータにプログラムを実行させることで端末 40 の機能が実現できる。また、端末 40 は、当該プログラムにより端末 40 の制御方

法を実行する。

[0193] [変形例]

なお、上記実施形態にて説明した認証システムの構成、動作等は例示であって、システムの構成等を限定する趣旨ではない。

[0194] 上記実施形態では、利用者によるサービス提供者の選択と、当該選択に伴う原本生体情報の提供（オプトイン）について説明した。制御サーバ10や端末40は、当該オプトインしたサービス提供者の情報を図10に示すように、サービス提供者のアイコンにチェックを入れることで利用者が識別可能としている。制御サーバ10及び端末40は、オプトインしたサービス提供者から登録認証情報を削除するオプアウトを可能としてもよい。この場合、制御サーバ10は、図10において、利用者が選択済のサービス提供者（オプトインされたサービス提供者）を選択すると、当該選択されたサービス提供者のサービスサーバ20に対して、利用者のシステムIDを含む利用者登録解除要求を送信する。サービスサーバ20は、システムIDに対応する利用者の登録認証情報等を削除する。

[0195] サービスサーバ20（認証部304）は、業務情報を用いたサービス提供可否の判定に失敗した場合には、当該失敗の事実を被認証者（照合処理により特定された被認証者）に通知してもよい。その際、認証部304は、認証に失敗した原因も併せて被認証者に通知してもよい。例えば、認証部304は、「オフィスに入場する権限がない」、「クレジットカードによる決済に失敗した」、「チケットが無効」等の理由を被認証者に通知してもよい。この場合、認証部304は、被認証者のシステムIDと認証失敗の理由を含む認証失敗通知を制御サーバ10に送信する。制御サーバ10は、システムIDを用いて被認証者の端末40を特定し、当該特定された端末40に認証失敗通知を送信する。認証失敗通知を受信すると、端末40は、利用者に認証に失敗した理由を通知する。例えば、端末40は、図23に示すようなポップアップ通知により認証に失敗した理由を利用者に通知する。あるいは、端末40は、認証失敗通知を使って認証履歴を生成してもよい。この場合、端

末40は、利用者の操作に応じて、図24に示すように認証失敗時の原因を表示してもよい。

[0196] 上記実施形態では、人の「顔」を生体情報の例にとり認証システムの動作を説明した。しかし、本願開示の認証システムは、他の種類の生体情報を用いることもできる。例えば、指紋、声紋、静脈、網膜、瞳の虹彩の模様（パターン）といった個人に固有の身体的特徴を備えるデータが用いられてもよい。即ち、利用者の生体情報は、利用者の身体的特徴を情報として含むものであればよい。

[0197] 利用者の端末40は、制御サーバ10から原本提供要求を受信するたびに、原本生体情報（例えば、顔画像）をサービス提供者に送信することについての同意を利用者から取得してもよい。具体的には、原本提供要求を受信すると、端末40のサービス選択部504は、GUI等を用いて原本生体情報（例えば、顔画像）の提供可否を取得する。サービス選択部504は、原本生体情報の提供に関する利用者の同意が得られると、内部に記憶された原本生体情報を制御サーバ10に送信する。

[0198] 上記実施形態では、制御サーバ10の内部にアカウント管理データベースが構成される場合について説明したが、当該データベースは外部のデータベースサーバ等に構築されてもよい。即ち、制御サーバ10の一部の機能は別のサーバに実装されていてもよい。より具体的には、上記説明した「サービス選択制御部（サービス選択制御手段）」等がシステムに含まれるいずれかの装置に実装されていればよい。

[0199] 各装置（制御サーバ10、サービスサーバ20、認証端末30）間のデータ送受信の形態は特に限定されないが、これら装置間で送受信されるデータは暗号化されていてもよい。これらの装置間では、生体情報等が送受信され、これらの情報を適切に保護するためには、暗号化されたデータが送受信されることが望ましい。

[0200] 上記説明で用いた流れ図（フローチャート、シーケンス図）では、複数の工程（処理）が順番に記載されているが、実施形態で実行される工程の実行

順序は、その記載の順番に制限されない。実施形態では、例えば各処理を並行して実行する等、図示される工程の順番を内容的に支障のない範囲で変更することができる。

[0201] 上記の実施形態は本願開示の理解を容易にするために詳細に説明したものであり、上記説明したすべての構成が必要であることを意図したものではない。また、複数の実施形態について説明した場合には、各実施形態は単独で用いてもよいし、組み合わせて用いてもよい。例えば、実施形態の構成の一部を他の実施形態の構成に置き換えることや、実施形態の構成に他の実施形態の構成を加えることも可能である。さらに、実施形態の構成の一部について他の構成の追加、削除、置換が可能である。

[0202] 上記の説明により、本発明の産業上の利用可能性は明らかであるが、本発明は、生体認証サービスを提供する情報処理システムなどに好適に適用可能である。

[0203] 上記の実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

[付記 1]

複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信する、受信手段と、

前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う、認証履歴制御手段と、

を備える、端末。

[付記 2]

前記認証成功通知には、前記サービス提供者が成功した認証処理の詳細情報と、前記サービス提供者が生体認証に用いる認証情報の状態と、が含まれ、

前記認証履歴制御手段は、前記認証処理の詳細情報及び前記認証情報の状態を記憶することで、前記利用者の生体認証に関する履歴を生成する、付記

1 に記載の端末。

[付記 3]

前記認証履歴制御手段は、前記認証成功通知を受信するたびに、前記認証処理の詳細情報及び前記認証情報の状態を含むメッセージを表示する、付記 2 に記載の端末。

[付記 4]

前記認証履歴制御手段は、前記利用者の所定の操作に応じて、前記記憶された生体認証に関する履歴の表示を行う、付記 3 に記載の端末。

[付記 5]

前記生体認証に用いられる前記認証情報の原本となる原本生体情報を記憶する、記憶手段と、

前記複数のサービス提供者それぞれの生体認証に関する管理を行う、制御サーバからの要求に応じて、前記記憶された原本生体情報を、前記制御サーバを介して前記利用者が選択したサービス提供者のサービスサーバに送信する、送信手段と、

をさらに備える、付記 2 乃至 4 のいずれか一項に記載の端末。

[付記 6]

前記原本生体情報は顔画像であり、前記認証情報は前記顔画像から生成された特徴量である、付記 5 に記載の端末。

[付記 7]

複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバと、前記利用者が所持する端末と、

を含み、

前記端末は、

前記サービスサーバから、認証成功通知を受信する、受信手段と、

前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う、認証履歴制御手段と、

を備える、システム。

[付記 8]

前記複数のサービス提供者それぞれの生体認証に関する管理を行う、制御サーバをさらに含み、

前記受信手段は、前記制御サーバを介して、前記認証成功通知を受信する、付記 7 に記載のシステム。

[付記 9]

端末において、

複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信し、

前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う、端末の制御方法。

[付記 10]

端末に搭載されたコンピュータに、

複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信する処理と、

前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う処理と、

を実行させるためのプログラムを記憶する、コンピュータ読取可能な記憶媒体。

[0204] なお、引用した上記の先行技術文献の各開示は、本書に引用をもって繰り込むものとする。以上、本発明の実施形態を説明したが、本発明はこれらの実施形態に限定されるものではない。これらの実施形態は例示にすぎないということ、及び、本発明のスコップ及び精神から逸脱することなく様々な変形が可能であるということは、当業者に理解されるであろう。即ち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし

得る各種変形、修正を含むことは勿論である。

符号の説明

- [0205] 1 0 制御サーバ
- 2 0 サービスサーバ
- 3 0 認証端末
- 4 0 端末
- 1 0 0 端末
- 1 0 1 受信手段
- 1 0 2 認証履歴制御手段
- 2 0 1 通信制御部
- 2 0 2 アカウント管理部
- 2 0 3 事業者管理部
- 2 0 4 サービス選択制御部
- 2 0 5 利用者登録制御部
- 2 0 6 記憶部
- 3 0 1 通信制御部
- 3 0 2 業務情報管理部
- 3 0 3 利用者登録制御部
- 3 0 4 認証部
- 3 0 5 記憶部
- 3 1 1 プロセッサ
- 3 1 2 メモリ
- 3 1 3 入出力インターフェイス
- 3 1 4 通信インターフェイス
- 4 0 1 通信制御部
- 4 0 2 提供サービス制御部
- 4 0 3 認証要求部
- 4 0 4 記憶部

- 5 0 1 通信制御部
- 5 0 2 アカウント生成制御部
- 5 0 3 原本情報取得部
- 5 0 4 サービス選択部
- 5 0 5 認証履歴制御部
- 5 0 6 記憶部

請求の範囲

- [請求項1] 複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信する、受信手段と、
- 前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う、認証履歴制御手段と、
- を備える、端末。
- [請求項2] 前記認証成功通知には、前記サービス提供者が成功した認証処理の詳細情報と、前記サービス提供者が生体認証に用いる認証情報の状態と、が含まれ、
- 前記認証履歴制御手段は、前記認証処理の詳細情報及び前記認証情報の状態を記憶することで、前記利用者の生体認証に関する履歴を生成する、請求項1に記載の端末。
- [請求項3] 前記認証履歴制御手段は、前記認証成功通知を受信するたびに、前記認証処理の詳細情報及び前記認証情報の状態を含むメッセージを表示する、請求項2に記載の端末。
- [請求項4] 前記認証履歴制御手段は、前記利用者の所定の操作に応じて、前記記憶された生体認証に関する履歴の表示を行う、請求項3に記載の端末。
- [請求項5] 前記生体認証に用いられる前記認証情報の原本となる原本生体情報を記憶する、記憶手段と、
- 前記複数のサービス提供者それぞれの生体認証に関する管理を行う、制御サーバからの要求に応じて、前記記憶された原本生体情報を、前記制御サーバを介して前記利用者が選択したサービス提供者のサービスサーバに送信する、送信手段と、
- をさらに備える、請求項2乃至4のいずれか一項に記載の端末。
- [請求項6] 前記原本生体情報は顔画像であり、前記認証情報は前記顔画像から生成された特徴量である、請求項5に記載の端末。

- [請求項7] 複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバと、
- 前記利用者が所持する端末と、
- を含み、
- 前記端末は、
- 前記サービスサーバから、認証成功通知を受信する、受信手段と、
- 前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う、認証履歴制御手段と、
- を備える、システム。
- [請求項8] 前記複数のサービス提供者それぞれの生体認証に関する管理を行う、制御サーバをさらに含み、
- 前記受信手段は、前記制御サーバを介して、前記認証成功通知を受信する、請求項7に記載のシステム。
- [請求項9] 端末において、
- 複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信し、
- 前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う、端末の制御方法。
- [請求項10] 端末に搭載されたコンピュータに、
- 複数のサービス提供者のなかから利用者が選択したサービス提供者であって、前記利用者の生体認証に成功したサービス提供者のサービスサーバから、認証成功通知を受信する処理と、
- 前記認証成功通知の受信に応じて、前記サービス提供者において成功した生体認証の履歴に関する制御を行う処理と、
- を実行させるためのプログラムを記憶する、コンピュータ読取可能な記憶媒体。

[図1]

端末

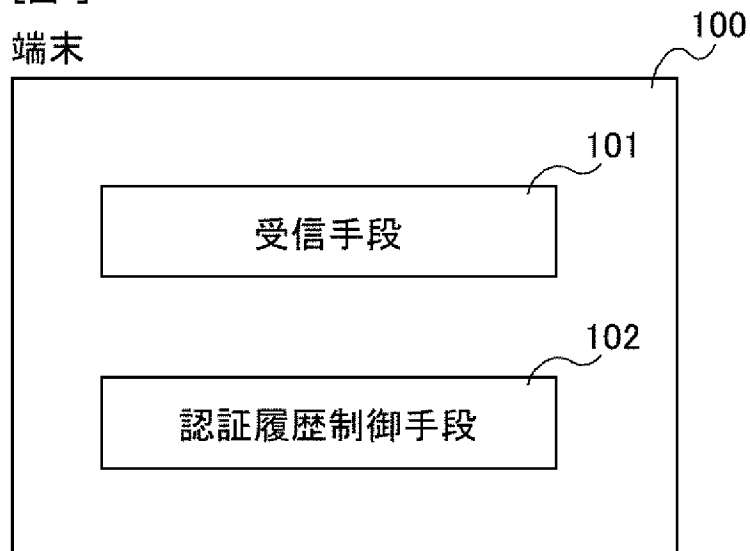


FIG.1

[図2]

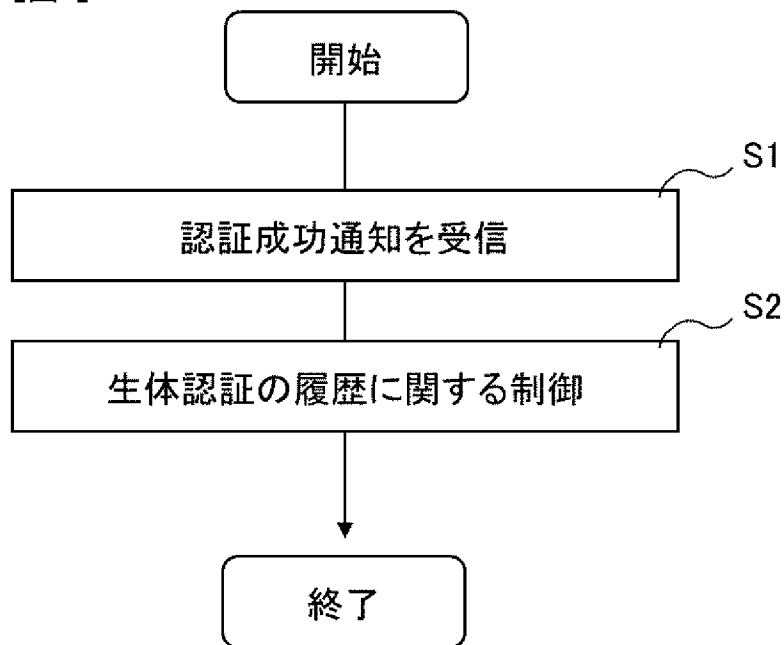


FIG.2

[図3]

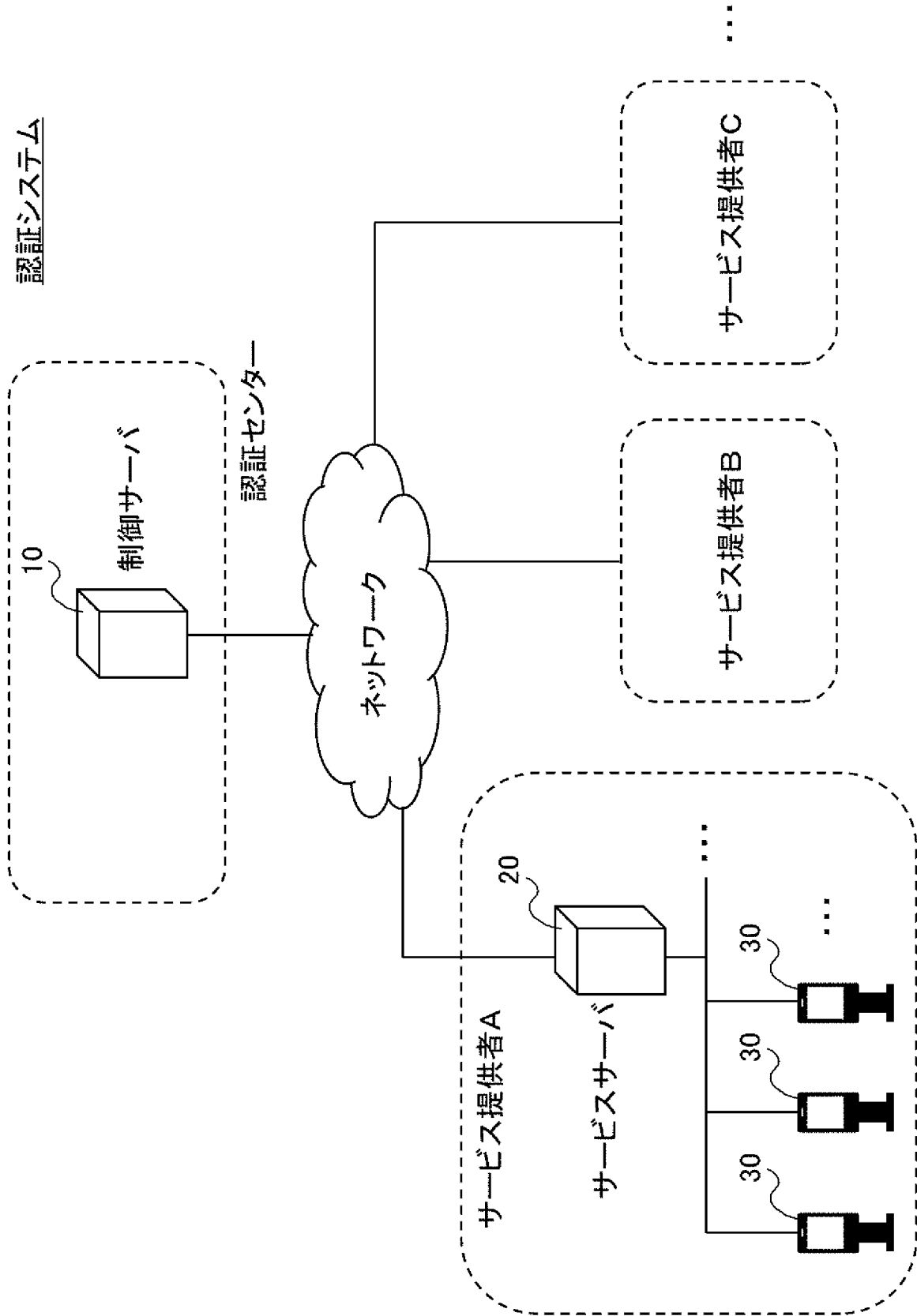


FIG.3

[図4]



FIG.4

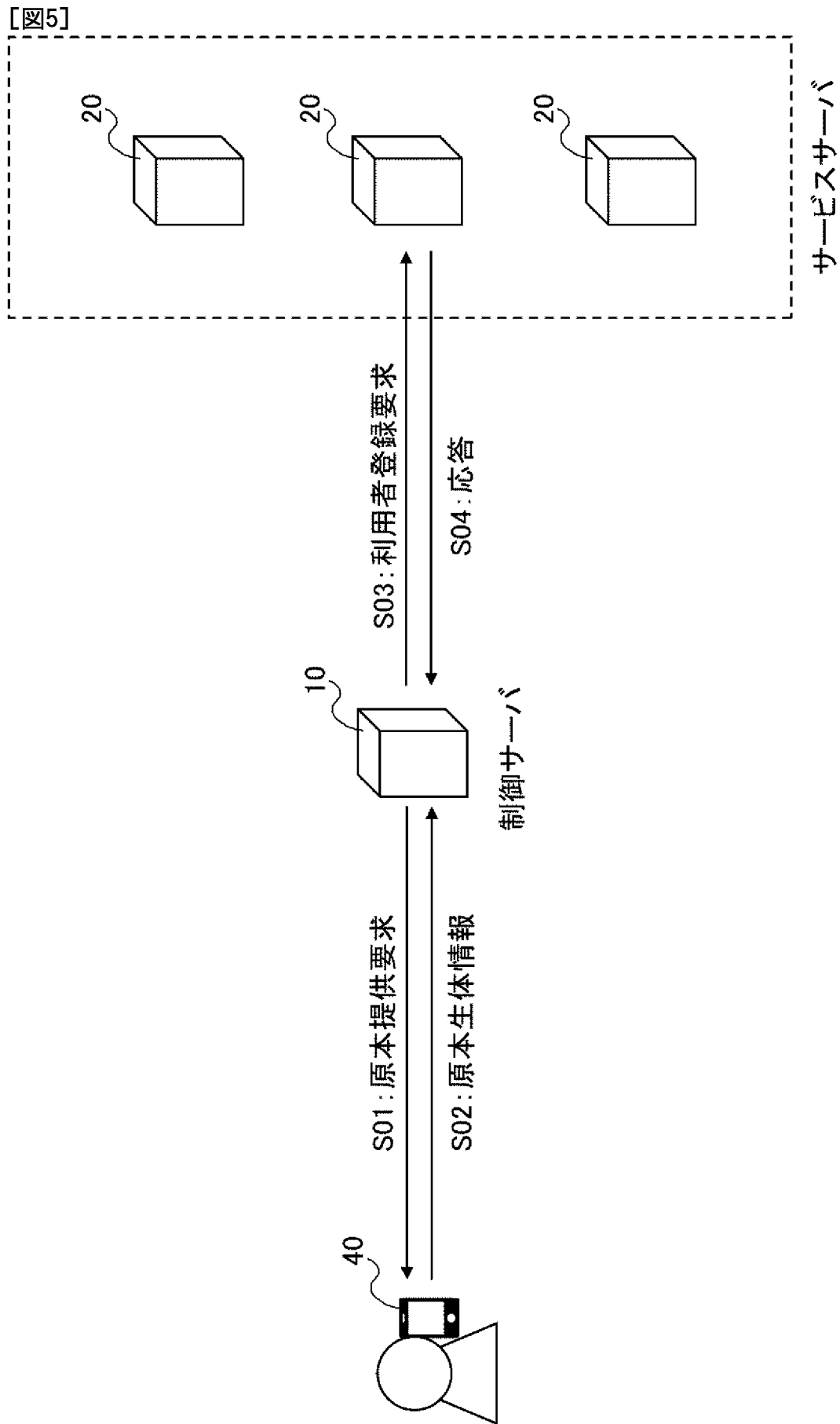


FIG.5

[図6]

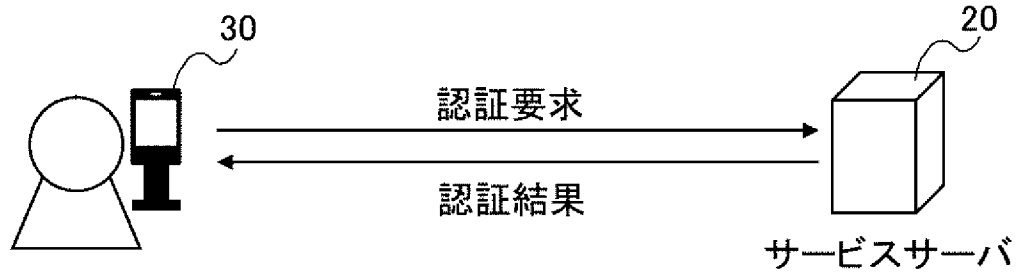


FIG.6

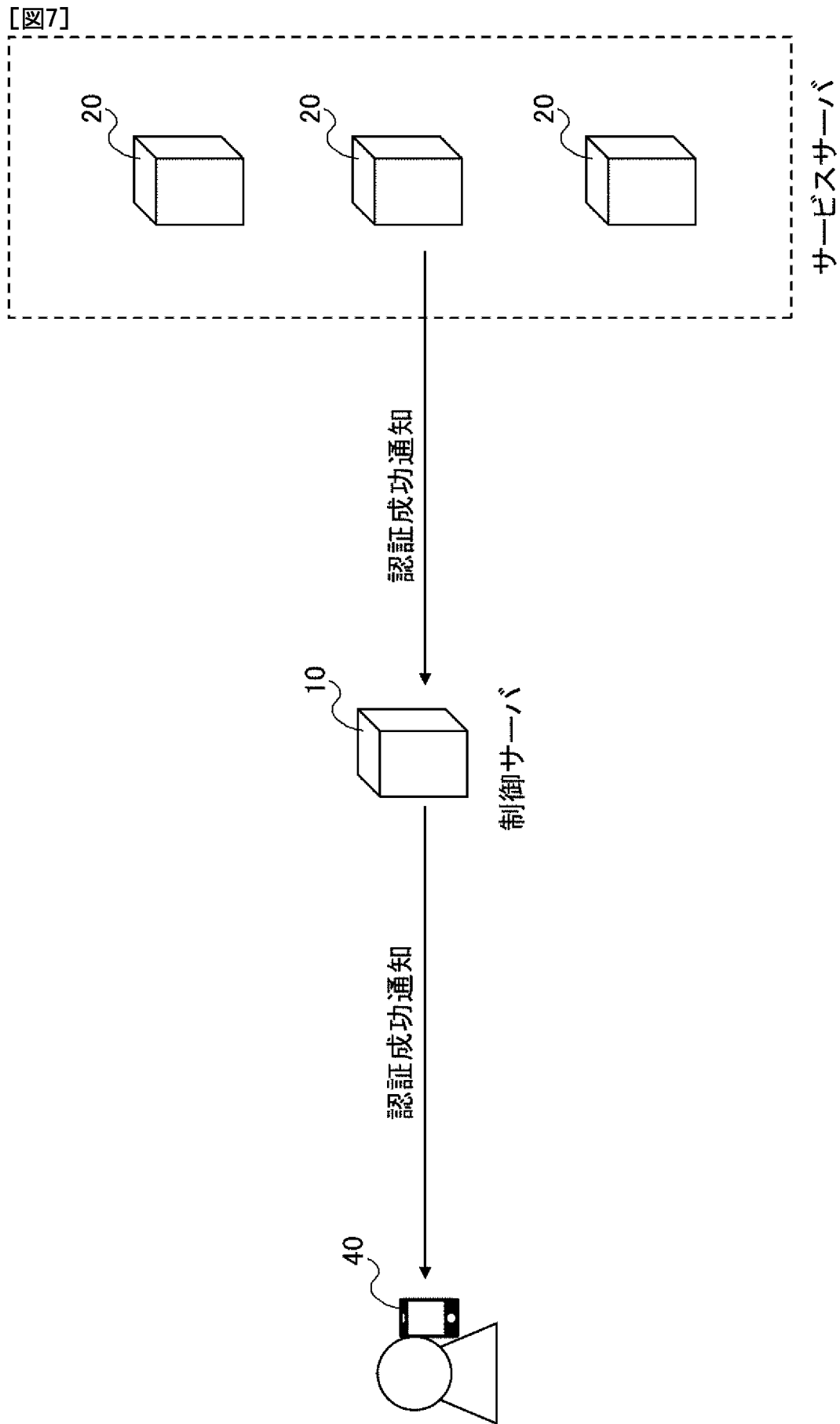


FIG.7

[図8]

制御サーバ

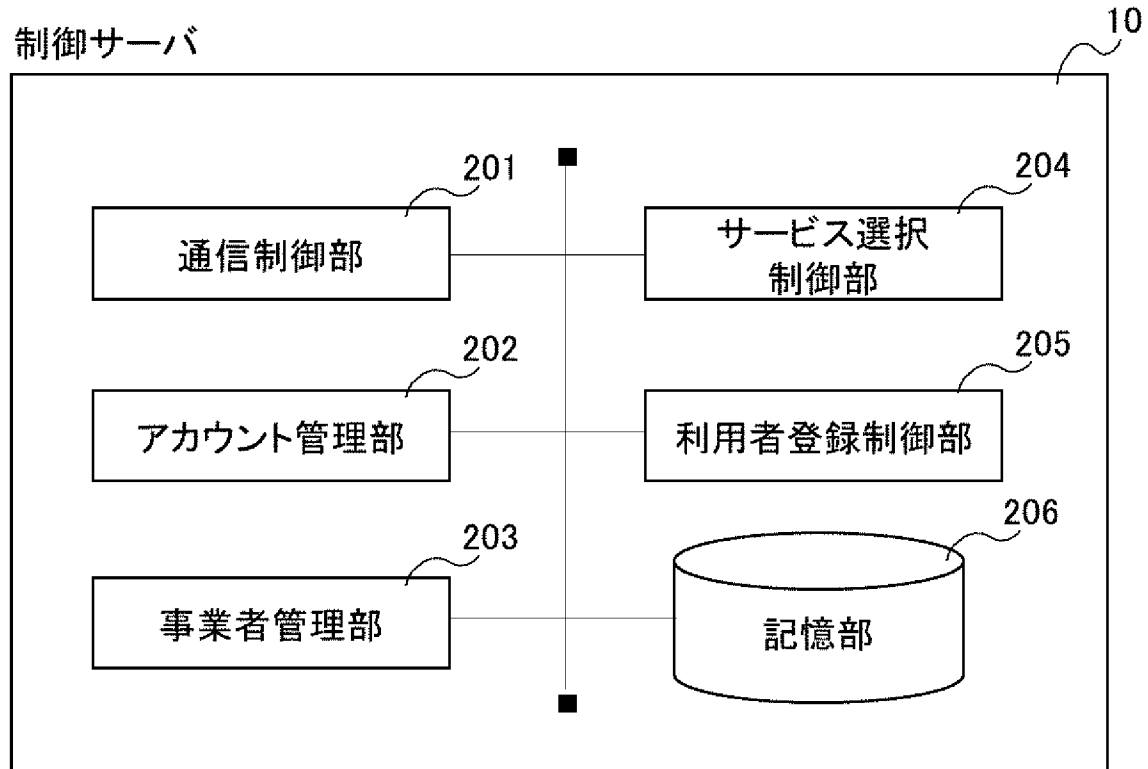


FIG.8

[図9]

アカウント管理データベース

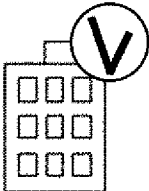
システムID	ログイン情報	氏名	選択サービス	...
uID01	(ID01,PW01)	NM01	sID01,sID02,...	...
uID02	(ID02,PW02)	NM02	sID03,sID04,...	...
⋮	⋮	⋮	⋮	⋮

FIG.9

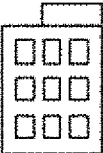
[図10]

サービスの選択

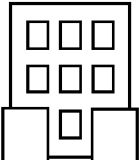
生体認証サービスを受ける事業者を
選択して下さい。



企業A



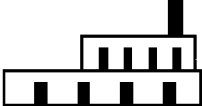
企業B



市役所



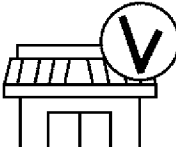
コンサート



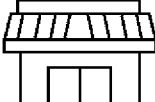
航空券



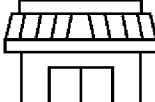
切符



小売店A



小売店B



小売店C

FIG.10

[図11]

サービスサーバ

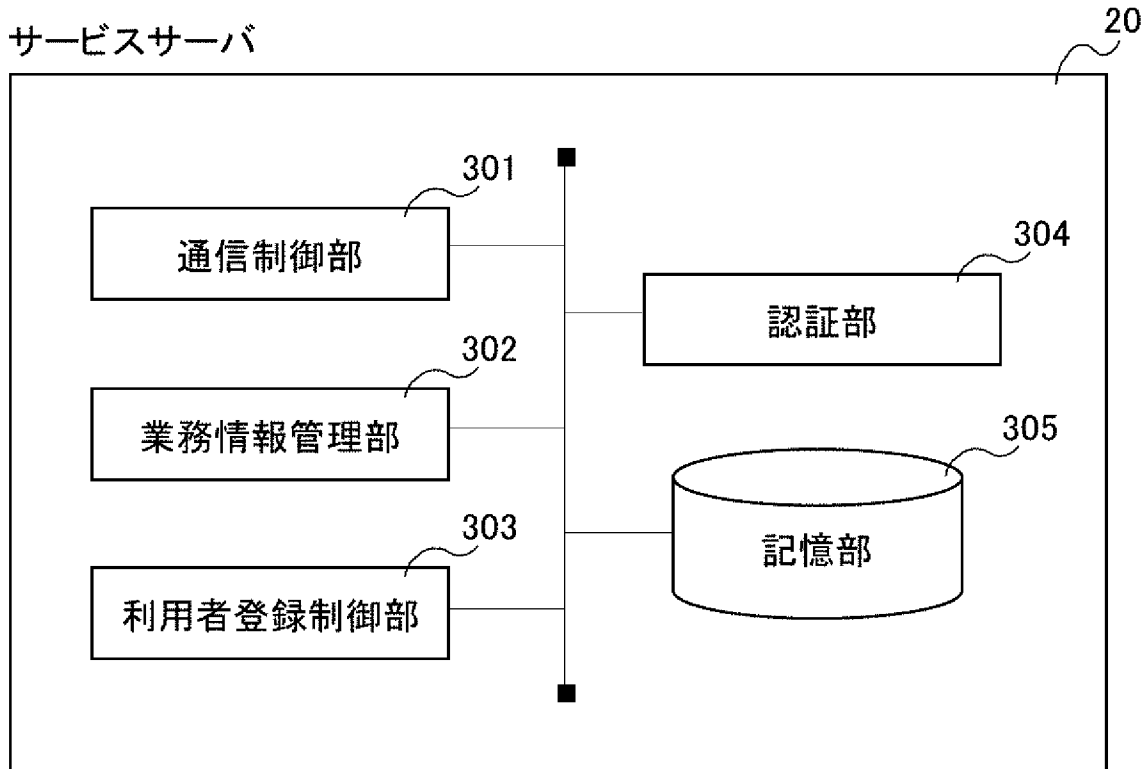


FIG.11

[図12]

利用者管理データベース

システムID	登録認証情報	業務情報	...
uID11	FV11	GI11	...
uID12	FV12	GI12	...
⋮	⋮	⋮	⋮

FIG.12

[図13]

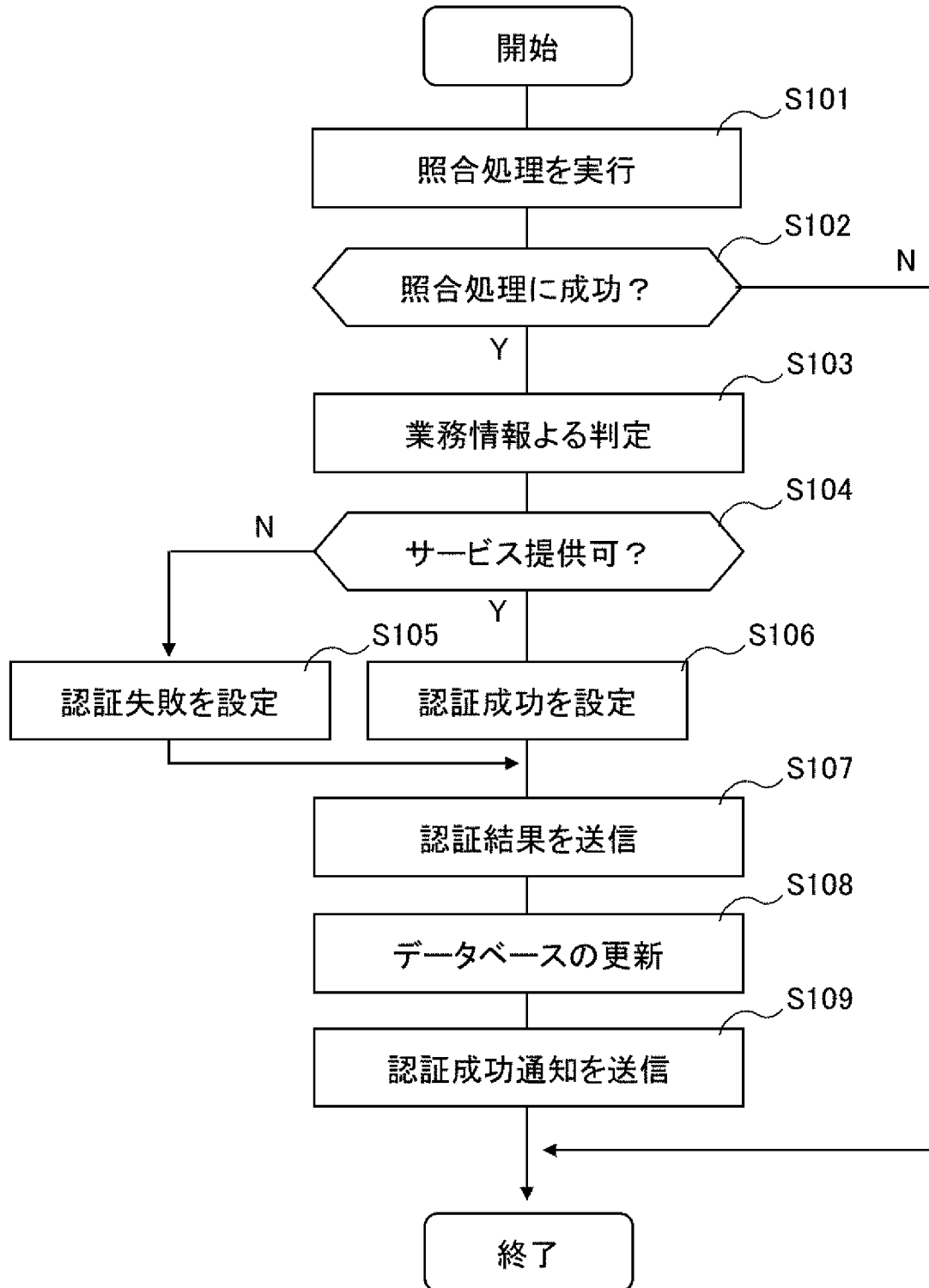


FIG.13

[図14]

認証端末

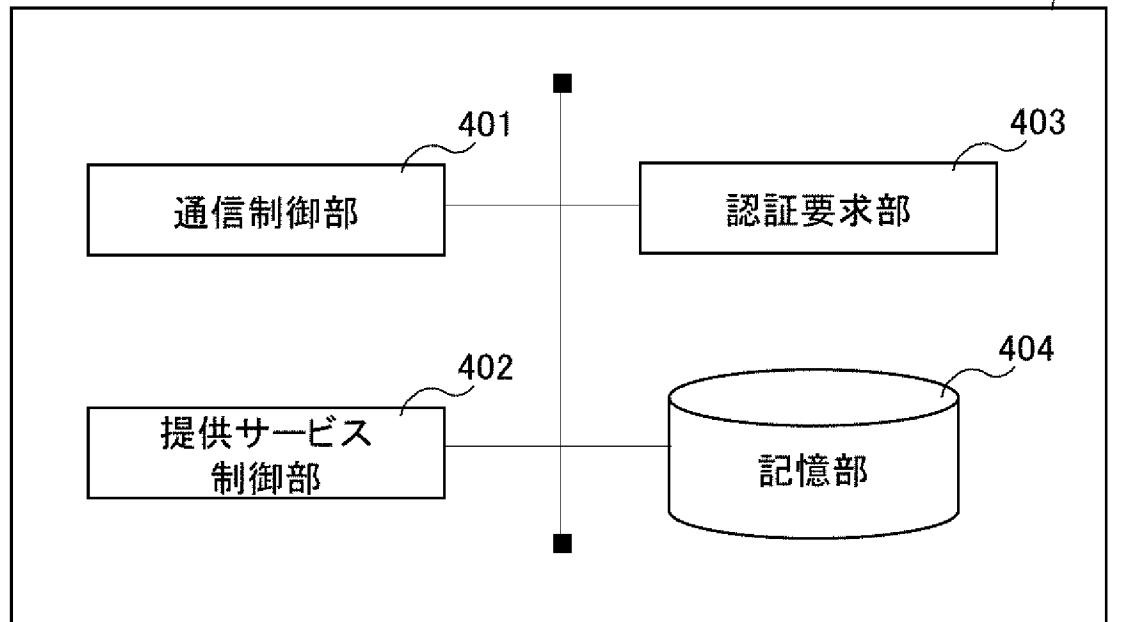


FIG.14

[図15]

端末

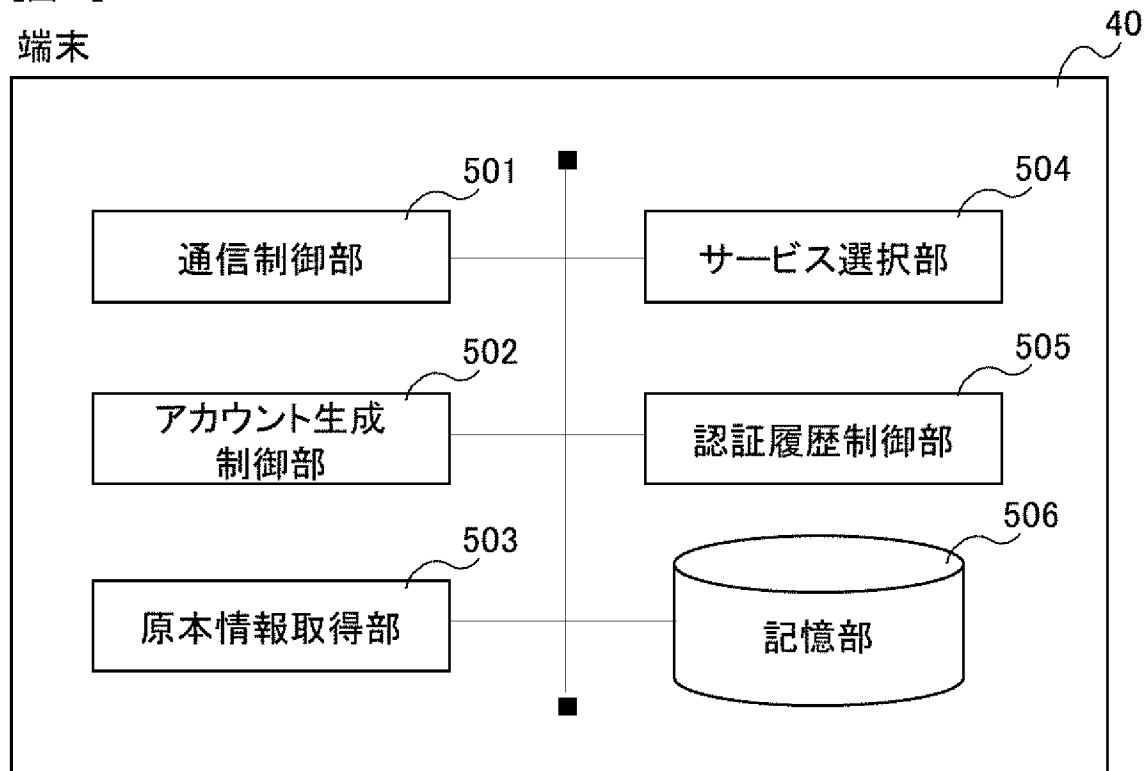
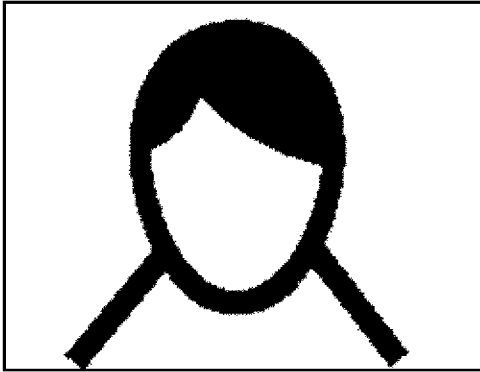


FIG.15

[図16]

生体情報の登録

生体認証に利用する顔画像を取得します。
撮影ボタンを押して下さい。



撮影

キャンセル

FIG.16

図17
認証履歴管理データベース

認証日時	認証場所	認証処理の詳細	認証情報の状態	...
DATE01	本社ビル	出勤	維持	...
DATE02	本社ビル	退社	維持	...
DATE03	コンサートホール	入場	削除	...
⋮	⋮	⋮	⋮	⋮

FIG.17

[図18]

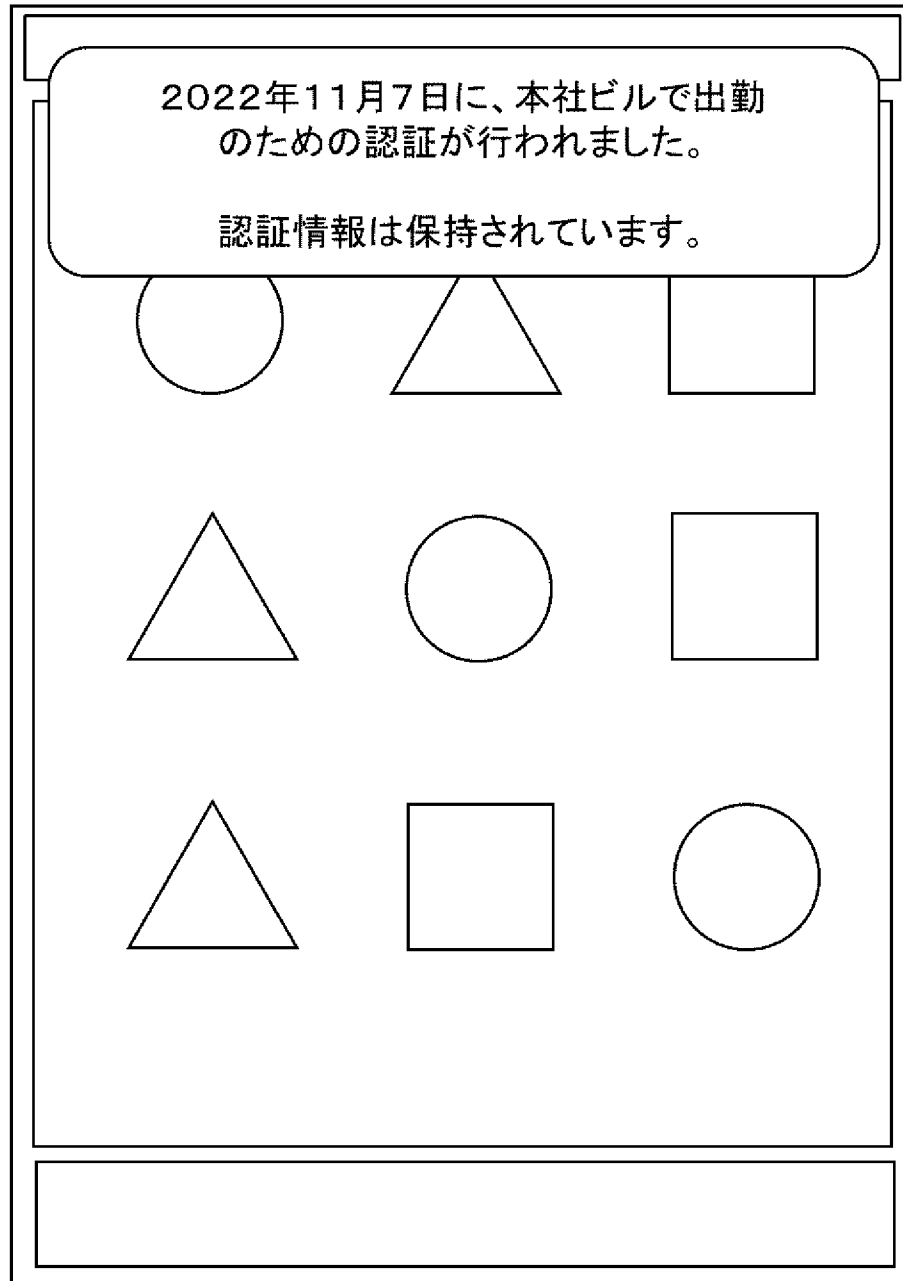


FIG.18

[図19]

認証履歴	
認証日時: DATE01 認証場所: 本社ビル 認証処理の詳細: 出勤	
認証日時: DATE02 認証場所: 本社ビル 認証処理の詳細: 退社	
認証日時: DATE03 認証場所: コンサートホール 認証処理の詳細: 入場	
⋮	

FIG.19

[図20]

認証履歴	
認証日時: DATE01 認証場所: 本社ビル 認証処理の詳細: 出勤 認証情報の状態: 維持	
認証日時: DATE02 認証場所: 本社ビル 認証処理の詳細: 退社 認証情報の状態: 維持	
認証日時: DATE03 認証場所: コンサートホール 認証処理の詳細: 入場 認証情報の状態: 削除	
⋮	

FIG.20

[図21]

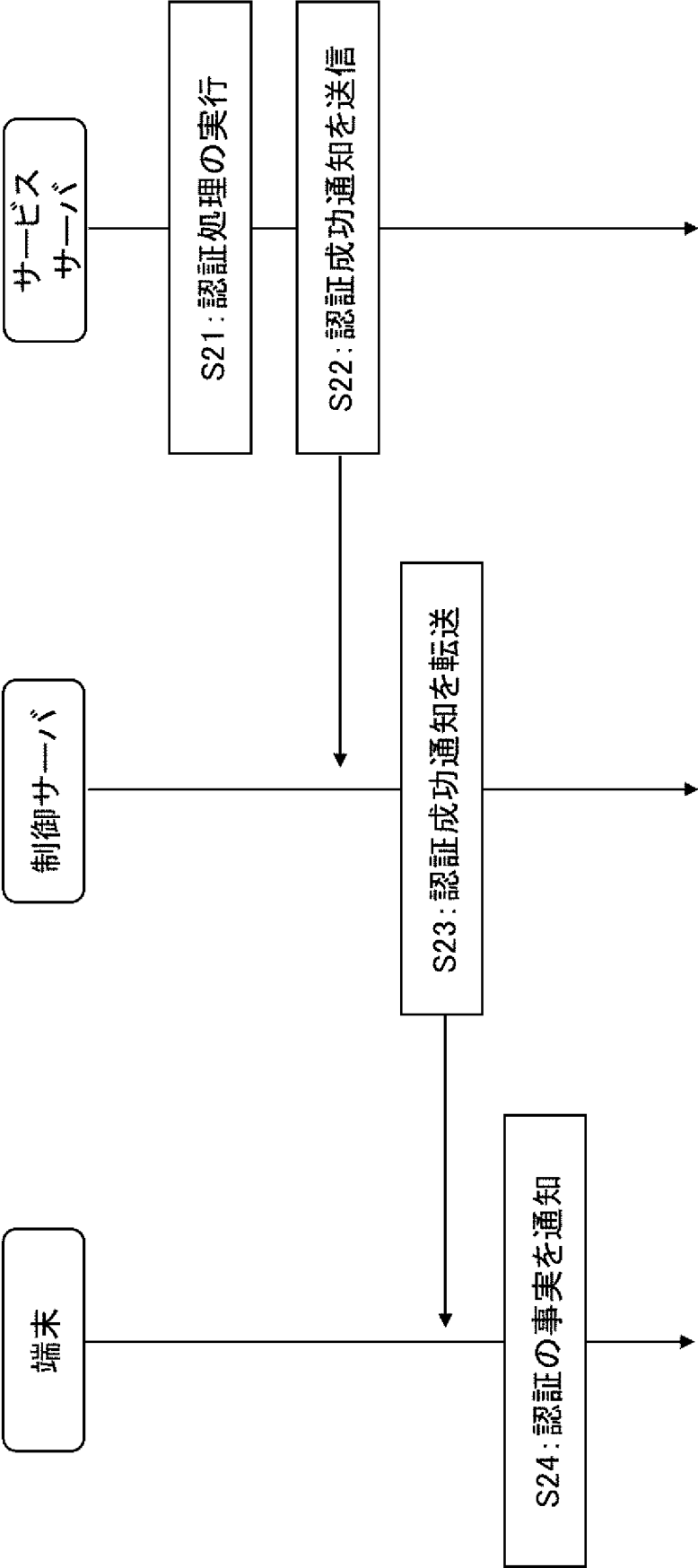


FIG.21

[図22]

制御サーバ

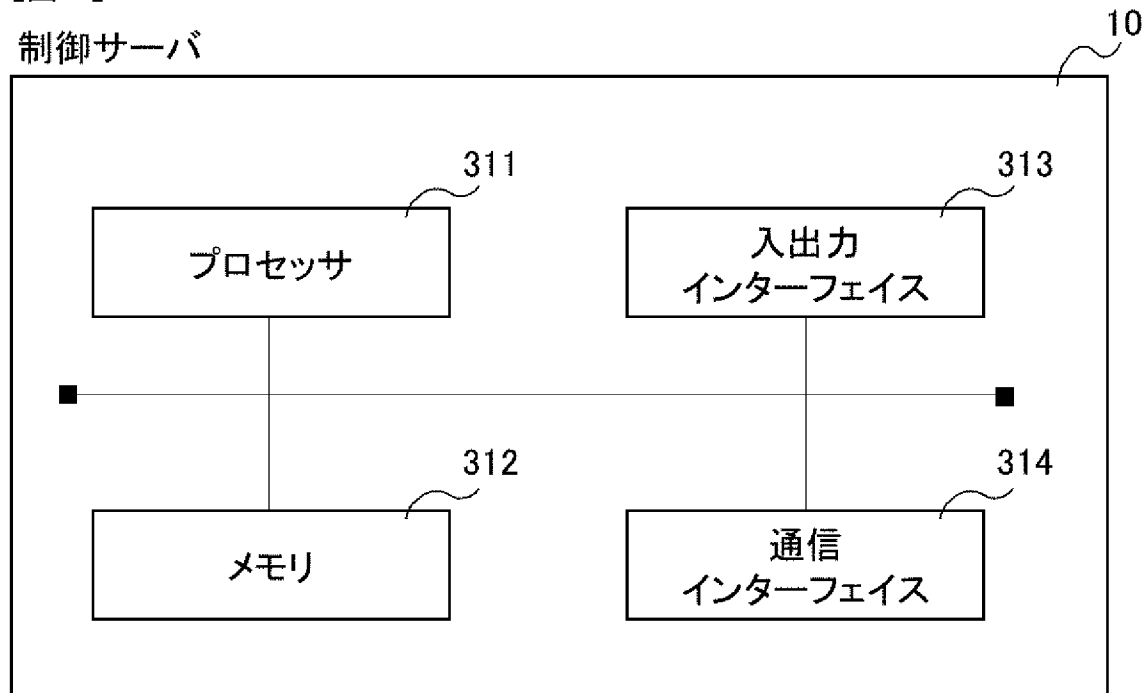


FIG.22

[図23]

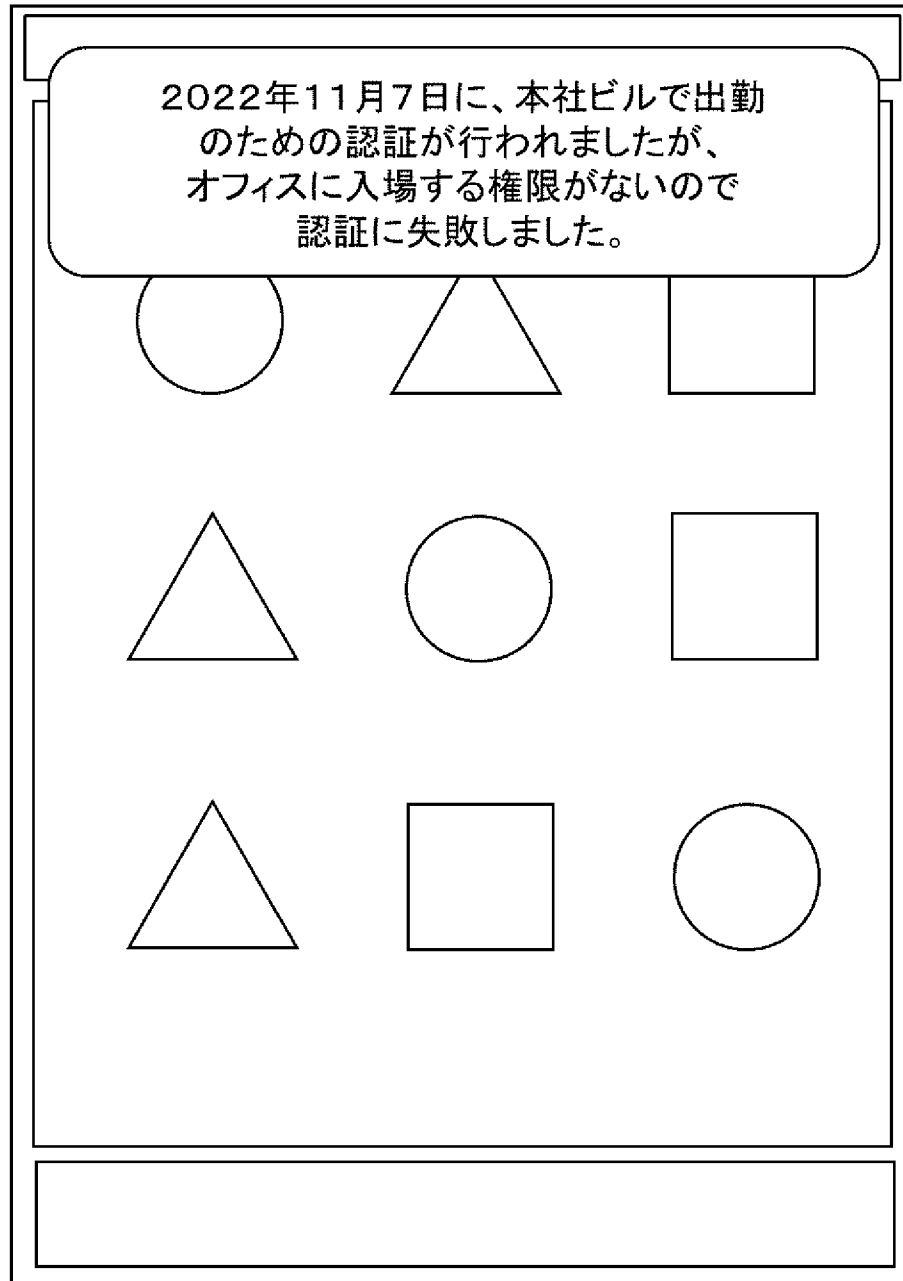


FIG.23

[図24]

認証履歴	
認証日時: DATE01 認証場所: 本社ビル 認証処理の詳細: 出勤 認証情報の状態: 維持	
認証日時: DATE02 認証場所: 本社ビル 認証処理の詳細: 退社 認証情報の状態: 維持	
認証日時: DATE03 認証場所: コンサートホール 認証結果: 失敗 認証失敗の原因: チケットが無効	
⋮	

FIG.24

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2022/045180

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/32**(2013.01)i

FI: G06F21/32

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)

G06F21/32

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 1971-2023

Registered utility model specifications of Japan 1996-2023

Published registered utility model applications of Japan 1994-2023

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 5950318 B1 (BRAINY INC.) 13 July 2016 (2016-07-13) paragraphs [0016], [0031], [0040], [0046], [0047], [0108], [0142], [0143]	1, 7-10
A	paragraphs [0016], [0031], [0040], [0046], [0047], [0108], [0142], [0143]	2-6
A	WO 2021/214969 A1 (NEC CORP.) 28 October 2021 (2021-10-28) abstract	1-10
A	JP 2010-049568 A (KPE INC.) 04 March 2010 (2010-03-04) claim 1, paragraph [0001]	1-10
A	JP 2005-284701 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 13 October 2005 (2005-10-13) claim 1	1-10



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

31 January 2023

Date of mailing of the international search report

14 February 2023

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)

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/JP2022/045180

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	5950318	B1	13 July 2016	US 2018/0189773 A1 paragraphs [0034], [0049], [0058], [0064], [0065], [0126], [0160], [0161] WO 2017/037913 A1 CN 108027951 A	
WO	2021/214969	A1	28 October 2021	(Family: none)	
JP	2010-049568	A	04 March 2010	(Family: none)	
JP	2005-284701	A	13 October 2005	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/32(2013.01)i FI: G06F21/32										
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）） G06F21/32 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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2023年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2023年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2023年</td> </tr> </table> 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）			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2023年	日本国実用新案登録公報	1996 - 2023年	日本国登録実用新案公報	1994 - 2023年
日本国実用新案公報	1922 - 1996年									
日本国公開実用新案公報	1971 - 2023年									
日本国実用新案登録公報	1996 - 2023年									
日本国登録実用新案公報	1994 - 2023年									
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 5950318 B1（プレイニー株式会社）13.07.2016（2016 - 07 - 13） 段落[0016], [0031], [0040], [0046]-[0047], [0108], [0142]-[0143]	1, 7-10								
A	段落[0016], [0031], [0040], [0046]-[0047], [0108], [0142]-[0143]	2-6								
A	WO 2021/214969 A1（日本電気株式会社）28.10.2021（2021 - 10 - 28） 要約	1-10								
A	JP 2010-049568 A（K P E株式会社）04.03.2010（2010 - 03 - 04） 請求項1, 段落[0001]	1-10								
A	JP 2005-284701 A（松下電器産業株式会社）13.10.2005（2005 - 10 - 13） 請求項1	1-10								
☐ 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、一般的技术水準を示すもの “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 31.01.2023		国際調査報告の発送日 14.02.2023								
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） 宮司 卓佳 5S 9555 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/JP2022/045180

引用文献			公表日	パテントファミリー文献	公表日
JP	5950318	B1	13.07.2016	US 2018/0189773 A1 段落[0034], [0049], [0058], [0064]-[0065], [0126], [0160]-[0161] WO 2017/037913 A1 CN 108027951 A	
WO	2021/214969	A1	28.10.2021	(ファミリーなし)	
JP	2010-049568	A	04.03.2010	(ファミリーなし)	
JP	2005-284701	A	13.10.2005	(ファミリーなし)	