

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7363982号
(P7363982)

(45)発行日 令和5年10月18日(2023.10.18)

(24)登録日 令和5年10月10日(2023.10.10)

(51)国際特許分類		F I	
G 0 6 F	21/32 (2013.01)	G 0 6 F	21/32
G 0 6 Q	30/06 (2023.01)	G 0 6 Q	30/06
G 0 6 Q	20/40 (2012.01)	G 0 6 Q	20/40

請求項の数 4 (全39頁)

(21)出願番号	特願2022-115243(P2022-115243)	(73)特許権者	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22)出願日	令和4年7月20日(2022.7.20)	(74)代理人	100168310 弁理士 高橋 幹夫
(62)分割の表示	特願2022-21876(P2022-21876)の分割	(72)発明者	平本 憲由 東京都港区芝五丁目7番1号 日本電気株式会社内
原出願日	令和3年5月31日(2021.5.31)	(72)発明者	奥村 太一 東京都港区芝五丁目7番1号 日本電気株式会社内
(65)公開番号	特開2022-184831(P2022-184831 A)	(72)発明者	阿久津 樹輝 東京都港区芝五丁目7番1号 日本電気株式会社内
(43)公開日	令和4年12月13日(2022.12.13)	審査官	岸野 徹
審査請求日	令和4年7月20日(2022.7.20)		

最終頁に続く

(54)【発明の名称】 認証端末、認証端末の制御方法及びプログラム

(57)【特許請求の範囲】

【請求項1】

所定エリアに滞在する複数の滞在者が所持する複数の端末それぞれから前記複数の滞在者それぞれのIDを取得する、取得部と、

被認証者の生体情報を取得する、生体情報取得部と、

前記被認証者の生体情報と前記複数の滞在者それぞれのIDを含む認証要求を、複数の利用者それぞれのIDと生体情報を対応付けて記憶する、サーバ装置に送信する、認証要求部と、

を備える、認証端末。

【請求項2】

前記認証要求部は、前記被認証者の生体情報が取得されたことに応じて、前記認証要求を前記サーバ装置に送信する、請求項1に記載の認証端末。

【請求項3】

コンピュータが、

所定エリアに滞在する複数の滞在者が所持する複数の端末それぞれから前記複数の滞在者それぞれのIDを取得し、

被認証者の生体情報を取得し、

前記被認証者の生体情報と前記複数の滞在者それぞれのIDを含む認証要求を、複数の利用者それぞれのIDと生体情報を対応付けて記憶する、サーバ装置に送信する、認証端末の制御方法。

【請求項 4】

認証端末に搭載されたコンピュータに、
 所定エリアに滞在する複数の滞在者が所持する複数の端末それぞれから前記複数の滞在者それぞれのIDを取得する処理と、
 被認証者の生体情報を取得する処理と、
 前記被認証者の生体情報と前記複数の滞在者それぞれのIDを含む認証要求を、複数の利用者それぞれのIDと生体情報を対応付けて記憶する、サーバ装置に送信する処理と、
 を実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明は、システム、サーバ装置、認証方法及び記憶媒体に関する。

【背景技術】

【0002】

近年、生体認証を用いたサービスの普及が始まっている。

【0003】

例えば、特許文献1には、店舗内の所定処理（商品購入の決済処理など）に用いる来店者の識別情報の特定精度を高めることができる、と記載されている。特許文献1に記載の店舗管理装置は、店舗に来店する来店者の顔認証により本人確認を行うときに、来店者の携帯する端末装置と通信を行う。店舗管理装置は、複数の登録済顧客の中から来店者に対応する登録済顧客を選択し、来店者に対応する登録済顧客の生体情報の集合と、店舗内における所定処理の実行タイミングにおいて新たに取得した来店者の生体情報と、を用いて認証を行う。店舗管理装置は、当該認証によって、来店者を所定処理（商品購入時の決済処理など）の対象者として特定する。

20

【0004】

特許文献2には、商品およびサービスの購入における電子マネー決済の安全性と利便性を両立させる、と記載されている。特許文献2に記載の生体認証装置は、ユーザを識別するCIDと顔画像を取得する。生体認証装置は、在店者の顔画像群をあらかじめダウンロードしておき、これらの顔画像群と得られた顔画像を照合することにより、ユーザを認証する。認証に成功したとき、生体認証装置はユーザが購入する商品の料金の決済を決済装置に要求し、決済装置により決済許可されたとき、商品の購入を許可する。

30

【先行技術文献】

【特許文献】

【0005】

【文献】国際公開第2019/181364号

特開2019-067075号公報

【発明の概要】

【発明が解決しようとする課題】

【0006】

上述のように、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。このような生体認証を利用したシステムでは、小売店等に生体認証用の端末を設置し、当該端末から生体情報がサーバに送信される。サーバは、取得した生体情報とデータベースに記憶された生体情報を用いた照合処理を実行し、利用者の特定を行う。

40

【0007】

ここで、生体認証を用いたサービスの規模が大きくなると、類似した生体情報（例えば、顔画像又は顔画像から生成された特徴量）が数多くデータベースに登録されることになる。データベースに登録された生体情報（即ち、照合対象となる生体情報）の数が多くなると、認証精度が低下する。

【0008】

本発明は、生体認証の精度向上に寄与する、システム、サーバ装置、認証方法及び記憶

50

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、複数の利用者それぞれのIDと生体情報を対応付けて記憶する、サーバ装置と、少なくとも1以上の認証端末と、を含み、前記少なくとも1以上の認証端末は、所定エリアに滞在する少なくとも1以上の滞在者のIDを記憶するIDリストを保持すると共に、被認証者の認証が必要になると、前記被認証者の生体情報と前記IDリストを含む認証要求を前記サーバ装置に送信し、前記サーバ装置は、前記複数の利用者それぞれのIDから前記IDリストに含まれるIDを抽出し、前記抽出されたIDに対応する生体情報と前記認証要求に含まれる生体情報を用いた生体認証を実行する、システムが提供される。

10

【0010】

本発明の第2の視点によれば、複数の利用者それぞれのIDと生体情報を対応付けて記憶する、第1のサーバ装置と、所定エリアに滞在する滞在者のIDを前記第1のサーバ装置に通知する、デバイスと、少なくとも1以上の認証端末と、を含み、前記第1のサーバ装置は、前記複数の利用者のIDのうち前記通知されたIDに対応する生体情報を前記少なくとも1以上の認証端末に通知し、前記少なくとも1以上の認証端末は、前記通知された生体情報を生体情報リストに記憶し、被認証者の認証が必要になると、前記被認証者の生体情報と前記生体情報リストに記憶された生体情報を用いた生体認証を実行する、システムが提供される。

20

【0011】

本発明の第3の視点によれば、複数の利用者それぞれのIDと生体情報を対応付けて記憶する、記憶部と、所定エリアに滞在する少なくとも1以上の滞在者のIDを記憶するIDリストを保持する認証端末から、被認証者の生体情報と前記IDリストを含む認証要求を受信する、受信部と、前記複数の利用者それぞれのIDから前記IDリストに含まれるIDを抽出し、前記抽出されたIDに対応する生体情報と前記認証要求に含まれる生体情報を用いた生体認証を実行する、認証部と、を備える、サーバ装置が提供される。

【0012】

本発明の第4の視点によれば、複数の利用者それぞれのIDと生体情報を対応付けて記憶する、サーバ装置において、所定エリアに滞在する少なくとも1以上の滞在者のIDを記憶するIDリストを保持する認証端末から、被認証者の生体情報と前記IDリストを含む認証要求を受信し、前記複数の利用者それぞれのIDから前記IDリストに含まれるIDを抽出し、前記抽出されたIDに対応する生体情報と前記認証要求に含まれる生体情報を用いた生体認証を実行する、認証方法が提供される。

30

【0013】

本発明の第5の視点によれば、複数の利用者それぞれのIDと生体情報を対応付けて記憶する、サーバ装置に搭載されたコンピュータに、所定エリアに滞在する少なくとも1以上の滞在者のIDを記憶するIDリストを保持する認証端末から、被認証者の生体情報と前記IDリストを含む認証要求を受信する処理と、前記複数の利用者それぞれのIDから前記IDリストに含まれるIDを抽出する処理と、前記抽出されたIDに対応する生体情報と前記認証要求に含まれる生体情報を用いた生体認証を実行する処理と、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。

40

【発明の効果】

【0014】

本発明の各視点によれば、生体認証の精度向上に寄与する、システム、サーバ装置、認証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】

【0015】

【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。

50

- 【図 2】図 2 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 3】図 3 は、第 1 の実施形態に係るサインージと認証端末の配置を説明するための図である。
- 【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 の実施形態に係るサーバ装置の処理構成の一例を示す図である。
- 【図 7】図 7 は、第 1 の実施形態に係る会員情報データベースの一例を示す図である。
- 【図 8】図 8 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 9】図 9 は、第 1 の実施形態に係るサインージの処理構成の一例を示す図である。
- 【図 10】図 10 は、第 1 の実施形態に係る認証端末の処理構成の一例を示す図である。 10
- 【図 11】図 11 は、第 1 の実施形態に係る入店者リストの一例を示す図である。
- 【図 12】図 12 は、第 1 の実施形態に係る端末の処理構成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システムの動作の一例を示すシーケンス図である。
- 【図 14】図 14 は、第 1 の実施形態に係る変形例の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 2 の実施形態に係るサーバ装置の処理構成の一例を示す図である。
- 【図 16】図 16 は、第 2 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 17】図 17 は、第 2 の実施形態に係る入店者リストの一例を示す図である。
- 【図 18】図 18 は、第 2 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。 20
- 【図 19】図 19 は、第 2 の実施形態に係る変形例 2 の認証システムの概略構成の一例を示す図である。
- 【図 20】図 20 は、第 2 の実施形態に係る変形例 2 の認証端末の処理構成の一例を示す図である。
- 【図 21】図 21 は、第 2 の実施形態に係る変形例 2 の店舗サーバの処理構成の一例を示す図である。
- 【図 22】図 22 は、本願開示に係るサーバ装置のハードウェア構成の一例を示す図である。
- 【図 23】図 23 は、本願開示の変形例に係る認証端末の動作を説明するための図である。 30
- 【図 24】図 24 は、本願開示の変形例に係る認証端末の動作を説明するための図である。
- 【図 25】図 25 は、本願開示の変形例に係る認証端末の動作を説明するための図である。
- 【図 26】図 26 は、本願開示の変形例に係るサインージの配置を説明するための図である。
- 【図 27】図 27 は、本願開示の変形例に係る店舗サーバの処理構成の一例を示す図である。
- 【図 28】図 28 は、本願開示の変形例に係る解析部の動作を説明するための図である。
- 【図 29】図 29 は、本願開示の変形例に係る解析部の動作を説明するための図である。
- 【図 30】図 30 は、本願開示の変形例に係る入店者リストの一例を示す図である。
- 【図 31】図 31 は、本願開示の変形例に係る店舗サーバの処理構成の一例を示す図である。 40
- 【図 32】図 32 は、本願開示の変形例に係る動線情報提供部の動作を説明するための図である。
- 【図 33】図 33 は、本願開示の変形例に係る動線情報提供部の動作を説明するための図である。
- 【図 34】図 34 は、本願開示の変形例に係る認証端末の動作を説明するための図である。
- 【発明を実施するための形態】
- 【0016】

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。

【0017】

一実施形態に係るシステムは、サーバ装置101と、少なくとも1以上の認証端末102と、を含む（図1参照）。サーバ装置101は、複数の利用者それぞれのIDと生体情報を対応付けて記憶する。少なくとも1以上の認証端末102は、所定エリアに滞在する少なくとも1以上の滞在者のIDを記憶するIDリストを保持する。少なくとも1以上の認証端末102は、被認証者の認証が必要になると、被認証者の生体情報とIDリストを含む認証要求をサーバ装置101に送信する。サーバ装置101は、複数の利用者それぞれのIDからIDリストに含まれるIDを抽出し、抽出されたIDに対応する生体情報と認証要求に含まれる生体情報を用いた生体認証を実行する。

10

【0018】

上述のように、生体認証によって登録側の生体情報の数が増えると、認証精度が悪化する。とりわけ、登録された利用者の数が数千万人規模となると、誤認証（本人拒否、他人受け入れ）が発生する可能性がある。また、利用者の数が大規模になると、認証センター側のリソースが不足する懸念があり、サーバ台数の増加等が必要になる。あるいは、サーバの増強等を行わないと、生体認証の結果を得るまでに時間が長くなる可能性もある。

20

【0019】

このような問題に対し、一実施形態に係るシステムは、所定エリア（例えば、店舗内）に滞在している利用者（将来的に被認証者となる利用者；潜在的な被認証者）に割り当てられているIDを認証端末102の内部に蓄積しておく。認証端末102は、所定エリアに滞在している利用者のうち生体認証が必要となった利用者の生体情報を取得すると共に、当該生体情報と内部に蓄積されたID（少なくとも1以上のIDを含むリスト）をサーバ装置101に送信する。サーバ装置101は、事前に登録された利用者のIDのうちIDリストに記載されているIDを抽出する。即ち、サーバ装置101は、事前に登録された利用者のうち所定エリアに滞在している利用者のIDを抽出する。サーバ装置101は、当該抽出されたIDに対応する生体情報を登録側の生体情報、認証要求に含まれる生体情報を照合側の生体情報に設定し、生体認証（照合処理）を実行する。

30

【0020】

上記のようなシステム構成、動作とすることで、生体認証における登録側の生体認証の数が減少し、誤認証の発生を防止できる。即ち、同じ時間帯に店舗に入店（滞在）している利用者数（入店者数）は、事前に登録された利用者数（会員数）よりも大幅に少なく、1対N照合（Nは正の整数、以下同じ）におけるNが小さくなる。その結果、誤認証の発生が防止される。また、登録側の生体情報の数Nが減ることで、認証センターに対するリソースの要求が上昇することもなく、生体認証に要するコストを低減できる。また、上記Nが減ることで、生体認証の結果を得るまでの時間が長くなることもない（システムのスループットが低下することもない）。

40

【0021】

また、認証端末102は、所定エリア（店舗内）に滞在している利用者の生体認証が必要となったタイミングで、滞在者のIDリストを含む認証要求をサーバ装置101に送信している。このような認証端末102の動作によって、サーバ装置101が無駄な処理を実行することがなくなる（サーバ装置101のリソースを浪費することがなくなる）。ここで、店舗に入店した利用者の全員が何らかの消費行動（生体認証が必要となる行動）を行うとも限らない。このような消費行動を起こさない利用者に関する処理は不要である。一実施形態に係るシステムでは、利用者が所定エリアに進入しても、当該進入者の端末からIDを取得することに留まり、認証センター（サーバ装置101）では何らの動作を行

50

わない。当該システムでは、滞在者の認証が必要となったタイミングで、認証センター（サーバ装置 101）に生体認証を依頼する。その結果、サーバ装置 101 による不要な動作が抑制され、サーバ装置 101 のリソースを浪費したり処理速度の低下を招いたりすることがない。

【0022】

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。

【0023】

[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。

【0024】

[システムの構成]

図2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2に示すように、認証システムには、認証センター、サービス事業者が含まれる。

【0025】

認証センターは、サービス事業者に生体認証サービスを提供する。認証センターには、サーバ装置10が含まれる。サーバ装置10は、生体認証を行うサーバである。サーバ装置10が、上記認証センターの主たる機能を実現する。サーバ装置10は、少なくとも、複数の利用者それぞれのIDと生体情報を対応付けて記憶する。

【0026】

サービス事業者は、生体認証を用いたサービスを提供する。サービス事業者により提供される生体認証を用いたサービスとして、小売店等での代金決済サービスが例示される。あるいは、レンタルビデオ店における代金決済に生体認証が用いられてもよい。第1の実施形態では、サービス事業者はレンタルビデオ店を営業する事業者として説明を行う。

【0027】

図2に示すように、サービス事業者には、サイネージ20と、複数の認証端末30-1、30-2と、が含まれる。なお、以降の説明において、複数の認証端末30-1、30-2を区別する特段の理由がない場合には、単に「認証端末30」と表記する。

【0028】

図2に示すように、サービス事業者に設置された端末（サイネージ20、認証端末30）は相互に通信可能に構成されると共に、各端末はサーバ装置10と通信が可能に構成されている。例えば、サーバ装置10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。

【0029】

図2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台以上のサーバ装置10が含まれていてもよい。また、サービス事業者には、少なくとも1台以上の認証端末30が含まれていればよい。

【0030】

サイネージ20は、図3に示すように、店舗（レンタルビデオ店）の出入口付近に設置される装置（デバイス）である。サイネージ20は、店舗に来店した顧客を歓迎するようなメッセージを表示したりイベント情報等のメッセージを表示したりする。

【0031】

認証端末30は、店舗の各所に設置される。例えば、認証端末30は、商品陳列棚の間に設置される。利用者は、認証端末30を用いて代金の決済を行う。代金決済は主に生体認証（顔認証）により行われる。認証端末30は、所謂、セルフレジスタとして動作する。

【0032】

利用者の生体情報には、例えば、顔、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から計算されるデータ（特徴量）が例示される。あるいは、利用者の生体情報は、顔画像、指紋画像等の画像データであってもよい。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。第1の実施形態では、生体情報は、人の顔画像又は顔画像から生成された特徴量とする。

10

20

30

40

50

【 0 0 3 3 】

[動作概略]

続いて、第 1 の実施形態に係る認証システムの動作概略について説明する。

【 0 0 3 4 】

< 利用者登録 >

店舗（レンタルビデオ店）を利用する利用者は、事前に登録（会員登録、利用者登録）をする必要がある。

【 0 0 3 5 】

利用者は、所持する端末 4 0 を操作して、サーバ装置 1 0 にアクセスする。利用者は、自身の生体情報（例えば、顔画像）、個人情報（例えば、氏名、年齢、性別、住所等）、代金決済のための口座情報（例えば、銀行口座、クレジットカード情報等）をサーバ装置 1 0 に入力する（図 4 参照）。

10

【 0 0 3 6 】

端末 4 0 は、生体情報、個人情報、口座情報等を含む「利用者登録要求」をサーバ装置 1 0 に送信する。

【 0 0 3 7 】

生体情報等を取得すると、サーバ装置 1 0 は、利用者（会員）を識別するための会員 ID（IDentifier）を生成する。サーバ装置 1 0 は、生成した会員 ID、上記取得した生体情報、個人情報、口座情報を対応付けて会員情報データベースに記憶する。

【 0 0 3 8 】

また、サーバ装置 1 0 は、生成した会員 ID を、利用者に払い出す。具体的には、サーバ装置 1 0 は、会員 ID を含む応答（利用者登録要求に対する応答）を端末 4 0 に送信する。

20

【 0 0 3 9 】

端末 4 0 は、受信した会員 ID を記憶する。

【 0 0 4 0 】

< 店舗訪問 >

利用者（会員）は、端末 4 0 を所持して店舗を訪れる。店舗の出入り口に設置されたサイネージ 2 0 は、端末 4 0 と通信を行う。例えば、端末 4 0 とサイネージ 2 0 は、Z i g B e e（登録商標）、B l u e t o o t h（登録商標）等の無線通信（とりわけ、近距離無線通信）によって相互に通信を行う（図 5 参照）。

30

【 0 0 4 1 】

サイネージ 2 0 は、定期的又は所定のタイミングで「会員 ID 送信要求」を送信する。サイネージ 2 0 を中心とした所定範囲に利用者（端末 4 0）が到達すると、端末 4 0 は、会員 ID 送信要求を受信する。

【 0 0 4 2 】

当該要求に応じて、端末 4 0 は、サーバ装置 1 0 から払い出された会員 ID をサイネージ 2 0 に送信する。

【 0 0 4 3 】

サイネージ 2 0 は、端末 4 0 から会員 ID を取得すると、当該取得した会員 ID を含む「会員入店通知」を店舗内の各認証端末 3 0 に送信する。なお、図 5 では、認証端末 3 0 - 1 ~ 3 0 - 3 に会員入店通知が送信されるように記載されているが、実際には、認証端末 3 0 - 4 ~ 3 0 - 6 にも当該通知は送信される。

40

【 0 0 4 4 】

各認証端末 3 0 は、会員入店通知に含まれる会員 ID を取り出す。各認証端末 3 0 は、取り出した会員 ID を「入店者リスト」に追加する。入店者リストは、店内に滞在している利用者（会員）の会員 ID からなるリスト（ID リスト）である。例えば、3 人の利用者が入店していれば、3 つの会員 ID が入店者リストに記載される。

【 0 0 4 5 】

利用者は、店内を移動し、レンタルを希望する商品を選択する。利用者は、選択した商

50

品を手を持って認証端末30の前に移動する。なお、利用者が向かう認証端末30は、認証端末30-1~30-6のうちいずれでもよい。図5の例では、利用者は、商品を持って認証端末30-3の前に移動している。

【0046】

認証端末30は、利用者(人)を検出すると、商品代金の決済に係る処理を実行する。認証端末30は、面前の利用者の生体情報(顔画像)を取得する。認証端末30は、取得した顔画像から特徴量を生成する。

【0047】

認証端末30は、当該生成した特徴量(生体情報)と入店者リストを含む「認証要求」をサーバ装置10に送信する。

【0048】

認証要求を受信すると、サーバ装置10は、生体認証を実行する。

【0049】

はじめに、サーバ装置10は、入店者リストに記載された会員IDをキーとして会員情報データベースを検索する。検索の結果、入店している利用者のエントリが抽出される。例えば、3万人の会員が利用者登録し、店内に3人の会員が滞在している場合には、当該3人の会員に対応する会員IDから3つのエントリが抽出される。

【0050】

次に、サーバ装置10は、認証要求に含まれる生体情報と、上記抽出されたエントリに含まれる生体情報と、を用いた生体認証(照合処理)を実行する。より詳細には、サーバ装置10は、1対N照合を実行する。

【0051】

サーバ装置10は、生体認証に成功すると、生体認証に成功した利用者(認証成功と判定された被認証者; 認証成功者)の会員IDを含む肯定応答を認証要求の送信元である認証端末30に送信する。

【0052】

サーバ装置10は、生体認証に失敗すると、その旨を示す否定応答を認証端末30に送信する。

【0053】

認証端末30は、認証結果(認証成功、認証失敗)を受信し、当該認証結果に応じた処理を行う。

【0054】

認証失敗を受信した場合には、認証端末30は、面前の利用者(被認証者)に対して会員登録されていない旨を通知する。あるいは、認証端末30は、店員が待機している案内所に向かわせるようなメッセージを表示してもよい。

【0055】

認証成功を受信した場合には、認証端末30は、代金決済のための処理を行う。具体的には、認証端末30は、商品(レンタルビデオ等)に付されたバーコード、2次元コード等を読み取ることによって、商品を特定する。

【0056】

認証端末30は、特定した商品から代金を計算し、商品名(レンタルビデオのタイトル)や代金等の情報を含む決済情報と利用者(認証成功者)の会員IDを含む「決済要求」をサーバ装置10に送信する。

【0057】

サーバ装置10は、決済要求に含まれる会員IDをキーとして会員情報データベースを検索し、対応するエントリから口座情報を読み出す。サーバ装置10は、読み出した口座情報(銀行口座、クレジットカード情報等)と決済情報に含まれる商品代金を用いた決済処理を行う。

【0058】

サーバ装置10は、決済処理の結果(決済成功、決済失敗)を認証端末30に送信する。

10

20

30

40

50

【 0 0 5 9 】

認証端末 3 0 は、決裁処理の結果に応じた処理を行う。例えば、決済失敗であれば、認証端末 3 0 は、店員が待機している案内所に向かわせるようなメッセージを出力してもよいし、現金による決済を促してもよい。決済成功であれば、認証端末 3 0 は、決済が完了した旨を利用者に通知すればよい。

【 0 0 6 0 】

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。

【 0 0 6 1 】

[サーバ装置]

図 6 は、第 1 の実施形態に係るサーバ装置 1 0 の処理構成（処理モジュール）の一例を示す図である。図 6 を参照すると、サーバ装置 1 0 は、通信制御部 2 0 1 と、利用者登録部 2 0 2 と、認証部 2 0 3 と、決済部 2 0 4 と、記憶部 2 0 5 と、を備える。

10

【 0 0 6 2 】

通信制御部 2 0 1 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 2 0 1 は、認証端末 3 0 からデータ（パケット）を受信する。また、通信制御部 2 0 1 は、認証端末 3 0 に向けてデータを送信する。通信制御部 2 0 1 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 2 0 1 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 2 0 1 を介して他の装置とデータの送受信を行う。通信制御部 2 0 1 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。

20

【 0 0 6 3 】

利用者登録部 2 0 2 は、上述の利用者登録を実現する手段である。利用者登録部 2 0 2 は、端末 4 0 から「利用者登録要求」を受信する。利用者登録部 2 0 2 は、端末 4 0 から取得した顔画像（生体情報）から特徴量（複数の特徴量からなる特徴ベクトル）を生成する。

【 0 0 6 4 】

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、利用者登録部 2 0 2 は、顔画像から目、鼻、口等を特徴点として抽出する。その後、利用者登録部 2 0 2 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。

30

【 0 0 6 5 】

また、利用者登録部 2 0 2 は、利用者（会員）を識別するための会員 ID を生成する。会員 ID は、会員登録された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、利用者登録部 2 0 2 は、利用者登録要求を処理するたびに一意な値を採番し会員 ID としてもよい。

【 0 0 6 6 】

利用者登録部 2 0 2 は、上記生成された会員 ID、特徴量（生体情報）、個人情報、口座情報に対応づけて会員情報データベースに記憶する（図 7 参照）。なお、図 7 に示す会員情報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、生体情報として「顔画像」が会員情報データベースに登録されていてもよい。

40

【 0 0 6 7 】

生体情報等を会員情報データベースに記憶すると、利用者登録部 2 0 2 は、生成した会員 ID を利用者に通知する。具体的には、利用者登録部 2 0 2 は、会員 ID を含む応答（利用者登録要求に対する応答）を端末 4 0 に送信する。

【 0 0 6 8 】

認証部 2 0 3 は、サービス事業者（認証端末 3 0）から送信される認証要求を処理する手段である。図 8 を参照しつつ、認証部 2 0 3 の動作を説明する。

【 0 0 6 9 】

50

認証要求を受信すると、認証部 203 は、認証要求に含まれる「入店者リスト」を取り出す（ステップ S101）。

【0070】

認証部 203 は、入店者リストに記載された少なくとも 1 以上の会員 ID をキーとして会員情報データベースを検索し、対応するエントリを特定する（ステップ S102）。

【0071】

認証部 203 は、認証要求に含まれる生体情報（特徴量）を照合対象に設定し、上記特定された少なくとも 1 以上のエントリに登録された生体情報との間で照合処理を行う（ステップ S103）。より具体的には、認証部 203 は、認証要求から取り出した特徴量を照合対象に設定し、会員情報データベースに登録されている複数の特徴量のうちの一部の特徴量との間で 1 対 N 照合を実行する。

10

【0072】

なお、同じ時間帯に入店している利用者の数は少数であるので、上記照合処理における「N」もまた少数となる。例えば、3 万人の会員の情報が会員情報データベースに登録されていても店舗に滞在している会員の数が「3」であれば、上記 N は「3」となる。

【0073】

上記照合処理において、認証部 203 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。

20

【0074】

類似度が所定の値以上の特徴量が存在しなければ（ステップ S104、N o 分岐）、認証部 203 は、認証結果を「認証失敗」に設定する（ステップ S105）。

【0075】

類似度が所定の値以上の特徴量が存在すれば（ステップ S104、Y e s 分岐）、認証部 203 は、認証結果を「認証成功」に設定する（ステップ S106）。

【0076】

認証部 203 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）。

【0077】

認証失敗の場合には、認証部 203 は、その旨を示す否定応答を認証端末 30 に送信する。

30

【0078】

認証成功の場合には、認証部 203 は、その旨を示す肯定応答を認証端末 30 に送信する。肯定応答を送信する場合、認証部 203 は、会員 ID によって絞り込まれたエントリのうち照合対象との類似度が最も高い生体情報を持つエントリの会員 ID を含む肯定応答を認証端末 30 に送信する。あるいは、認証部 203 は、類似度が最も高い生体情報を持つエントリの個人情報（例えば、氏名）をさらに含む肯定応答を認証端末 30 に送信してもよい。

【0079】

このように、認証部 203 は、複数の利用者（会員）それぞれの ID から入店者リスト（ID リスト）に含まれる ID を抽出する。認証部 203 は、当該抽出された ID に対応する生体情報と認証要求に含まれる生体情報を用いた生体認証を実行する。また、認証部 203 は、生体認証に成功すると、認証成功者の ID を認証要求の送信元である認証端末 30 に通知する。

40

【0080】

決済部 204 は、認証端末 30 から受信する「決済要求」を処理する手段である。決済部 204 は、決済要求から会員 ID を取り出す。決済部 204 は、当該会員 ID をキーとして会員情報データベースを検索し、対応するエントリを特定する。

【0081】

50

決済部 204 は、特定したエントリから口座情報を読み出す。決済部 204 は、当該口座情報と決済要求に含まれる決済情報を用いて決済処理を行う。決済部 204 は、口座情報に記載された銀行口座、クレジットカード口座に対して決済情報に含まれる代金の引き落とし等を要求する。

【0082】

決済部 204 による決済処理は当業者にとって明らかであり、かつ、本願開示の趣旨とも異なるのでさらなる詳細な説明を省略する。

【0083】

記憶部 205 は、サーバ装置 10 の動作に必要な情報を記憶する手段である。記憶部 205 には、会員情報データベースが構築される。

10

【0084】

[サイネージ]

サイネージ 20 は、少なくとも 1 以上の滞在者（所定エリアに滞在する滞在者；店舗への入店者）が所持する端末 40 から当該少なくとも 1 以上の滞在者の ID を取得するデバイスである。

【0085】

図 9 は、第 1 の実施形態に係るサイネージ 20 の処理構成（処理モジュール）の一例を示す図である。図 9 を参照すると、サイネージ 20 は、通信制御部 301 と、会員検出部 302 と、メッセージ出力部 303 と、記憶部 304 と、を備える。

【0086】

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、認証端末 30 からデータ（パケット）を受信する。また、通信制御部 301 は、認証端末 30 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。

20

【0087】

また、通信制御部 301 は、近距離無線通信によって、利用者の所持する端末 40 とも通信を行う。

【0088】

会員検出部 302 は、サイネージ 20 の近傍の会員（利用者）を検出する手段である。会員検出部 302 は、定期的又は所定のタイミングで「会員 ID 送信要求」を近距離無線通信によって送信する。

30

【0089】

会員 ID 送信要求は近距離無線通信によって送信されるので、端末 40 を持つ利用者とサイネージ 20 の間の距離が長いと、端末 40 は当該要求を受信できない。図 5 の例では、サイネージ 20 は、入店した利用者の端末 40 が会員 ID 送信要求を受信できる位置に配置される。

【0090】

会員検出部 302 は、当該要求を受信した端末 40 から会員 ID を含む応答（会員 ID 送信要求に対する応答）を受信する。

40

【0091】

会員検出部 302 は、端末 40 から会員 ID を取得すると、当該会員 ID を含む「会員入店通知」を店舗内の各認証端末 30 に送信（一斉送信；ブロードキャスト）する。

【0092】

このように、会員検出部 302 は、来店した利用者が所持する端末 40 と近距離無線通信によって通信することで、来店者（店舗の滞在者）の会員 ID を取得する。会員検出部 302 は、店舗内（所定エリア）に設置された複数の認証端末 30 それぞれに、当該取得した少なくとも 1 以上の滞在者の会員 ID を通知する。

【0093】

50

メッセージ出力部 303 は、種々のメッセージを出力する手段である。例えば、メッセージ出力部 303 は、会員検出部 302 が会員を検出すると（会員の入店を検出すると）、当該会員の入店を歓迎するメッセージ等を出力する。

【0094】

メッセージ出力部 303 は、液晶パネル等の表示デバイスにメッセージを表示してもよいし、スピーカー等の音響デバイスによってメッセージを出力してもよい。

【0095】

記憶部 304 は、サイネージ 20 の動作に必要な情報を記憶する手段である。

【0096】

[認証端末]

認証端末 30 は、被認証者の生体情報を取得する端末（装置、デバイス）である。

【0097】

図 10 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 10 を参照すると、認証端末 30 は、通信制御部 401 と、入店者リスト管理部 402 と、生体情報取得部 403 と、認証要求部 404 と、決済要求部 405 と、記憶部 406 と、を備える。

【0098】

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、サーバ装置 10 からデータ（パケット）を受信する。また、通信制御部 401 は、サーバ装置 10 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。

【0099】

入店者リスト管理部 402 は、入店者リストを管理する手段である。入店者リスト管理部 402 は、会員入店通知をサイネージ 20 から受信すると、当該通知に含まれる会員 ID を入店者リストに追記する。

【0100】

図 11 は、第 1 の実施形態に係る入店者リストの一例を示す図である。図 11 に示すように、入店者リストは、会員の入店日時と会員 ID を対応付けて記憶する。このように、店舗（所定エリア）に配置された認証端末 30 は、店舗に滞在する滞在者の会員 ID を記憶する入店者リスト（ID リスト）を保持する。

【0101】

生体情報取得部 403 は、カメラを制御し、利用者の生体情報（顔画像）を取得する手段である。生体情報取得部 403 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。生体情報取得部 403 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。

【0102】

なお、生体情報取得部 403 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、生体情報取得部 403 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、生体情報取得部 403 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。

【0103】

生体情報取得部 403 は、抽出した顔画像を認証要求部 404 に引き渡す。

【0104】

認証要求部 404 は、サーバ装置 10 に対して利用者の認証を要求する手段である。認証要求部 404 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）の生体情報と入店者リストを含む認証要求をサーバ装置 10 に送信する。

【0105】

10

20

30

40

50

認証要求部 4 0 4 は、生体情報取得部 4 0 3 から生体情報（顔画像）を取得すると、当該顔画像から特徴量を生成する。認証要求部 4 0 4 は、生成した特徴量、入店者リスト、端末 I D を含む認証要求をサーバ装置 1 0 に送信する。

【 0 1 0 6 】

端末 I D は、各店舗の認証端末 3 0 を識別するための I D である。端末 I D には、認証端末 3 0 の M A C（Media Access Control）アドレスや I P（Internet Protocol）アドレスを用いることができる。

【 0 1 0 7 】

認証要求部 4 0 4 は、サーバ装置 1 0 から認証結果（認証成功、認証失敗）を受信する。

【 0 1 0 8 】

サーバ装置 1 0 からの応答が「否定応答」の場合（認証失敗の場合）には、認証要求部 4 0 4 は、その旨を利用者（被認証者）に通知する。例えば、認証要求部 4 0 4 は、会員登録されていないことを被認証者（認証端末 3 0 の前に立つ利用者）に通知する。あるいは、認証要求部 4 0 4 は、店員のいる案内所等に向かうように被認証者に通知する。あるいは、認証要求部 4 0 4 は、認証失敗者（認証失敗と判定された被認証者）に会員登録を促すメッセージ等を出力してもよい。

【 0 1 0 9 】

サーバ装置 1 0 からの応答が「肯定応答」の場合（認証成功の場合）には、認証要求部 4 0 4 は、当該応答に含まれる会員 I D を取り出す。認証要求部 4 0 4 は、当該取り出した会員 I D を決済要求部 4 0 5 に引き渡す。

【 0 1 1 0 】

決済要求部 4 0 5 は、認証成功者の代金決済に関する要求を行う手段である。決済要求部 4 0 5 は、任意の手段によって商品（例えば、レンタルビデオ）を特定する。例えば、決済要求部 4 0 5 は、レンタルビデオに貼り付けられているタグ、バーコード、2 次元コードによって商品を特定する。

【 0 1 1 1 】

決済要求部 4 0 5 は、特定した商品に基づいて利用者に請求する代金を計算し、決済情報を生成する。決済要求部 4 0 5 は、当該生成した決済情報、会員 I D 及び端末 I D を含む「決済要求」をサーバ装置 1 0 に送信する。

【 0 1 1 2 】

決済要求部 4 0 5 は、サーバ装置 1 0 から決済結果（決済成功、決済失敗）を取得する。決済要求部 4 0 5 は、決済結果に応じた処理を行う。

【 0 1 1 3 】

例えば、決済成功であれば、決済要求部 4 0 5 は、決済が完了した旨を利用者に通知する。決済失敗であれば、決済要求部 4 0 5 は、その旨を利用者に通知すると共に店員の元に向かうように指示する。

【 0 1 1 4 】

このように、決済要求部 4 0 5 は、認証成功者の会員 I D を用いて当該認証成功者にサービス（商品代金決済サービス）を提供する。

【 0 1 1 5 】

記憶部 4 0 6 は、認証端末 3 0 の動作に必要な情報を記憶する。

【 0 1 1 6 】

[端末]

端末 4 0 は、スマートフォン、携帯電話機、ゲーム機、タブレット等の携帯端末装置である。但し、端末 4 0 をこれらの例示に限定する趣旨ではない。本願開示における「端末」は、人が所持可能な任意の機器とすることができる。

【 0 1 1 7 】

図 1 2 は、第 1 の実施形態に係る端末 4 0 の処理構成（処理モジュール）の一例を示す図である。図 1 2 を参照すると、端末 4 0 は、通信制御部 5 0 1 と、利用者登録要求部 5 0 2 と、会員 I D 送信部 5 0 3 と、記憶部 5 0 4 と、を備える。

10

20

30

40

50

【 0 1 1 8 】

通信制御部 5 0 1 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 5 0 1 は、サーバ装置 1 0 からデータ（パケット）を受信する。また、通信制御部 5 0 1 は、サーバ装置 1 0 に向けてデータを送信する。通信制御部 5 0 1 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 5 0 1 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 5 0 1 を介して他の装置とデータの送受信を行う。

【 0 1 1 9 】

また、通信制御部 5 0 1 は、近距離無線通信によって、店舗の出入り口等に設置されたサイネージ 2 0 とも通信を行う。

10

【 0 1 2 0 】

利用者登録要求部 5 0 2 は、利用者の会員登録を実現する手段である。利用者の操作に応じて、利用者登録要求部 5 0 2 は、生体情報（顔画像）、個人情報（氏名等）、口座情報（銀行口座等）を取得する。

【 0 1 2 1 】

利用者登録要求部 5 0 2 は、取得した生体情報、個人情報、口座情報を含む利用者登録要求をサーバ装置 1 0 に送信する。

【 0 1 2 2 】

利用者登録要求部 5 0 2 は、会員 ID を含む応答を受信すると、当該会員 ID を記憶部 5 0 4 に記憶する。

20

【 0 1 2 3 】

会員 ID 送信部 5 0 3 は、会員 ID をサイネージ 2 0 に送信する手段である。会員 ID 送信部 5 0 3 は、「会員 ID 送信要求」を受信すると、記憶部 5 0 4 に格納された会員 ID を含む応答をサイネージ 2 0 に送信する。例えば、会員 ID 送信部 5 0 3 は、Bluetooth（登録商標）等の近距離無線通信手段を用いて会員 ID 送信要求に対する応答を送信する。

【 0 1 2 4 】

記憶部 5 0 4 は、端末 4 0 の動作に必要な情報を記憶する手段である。

【 0 1 2 5 】

[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、利用者登録に関する動作の説明は省略する。図 1 3 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。

30

【 0 1 2 6 】

サイネージ 2 0 は、会員 ID 送信要求の応答から会員 ID を取得する（ステップ S 0 1 ）。

【 0 1 2 7 】

サイネージ 2 0 は、当該取得した会員 ID を含む会員入店通知を各認証端末 3 0 に送信する（ステップ S 0 2 ）。

【 0 1 2 8 】

各認証端末 3 0 は、取得した会員 ID を入店者リストに記載する（会員 ID をリストに記載；ステップ S 0 3 ）。

40

【 0 1 2 9 】

認証端末 3 0 は、面前に利用者（被認証者）を検出すると、生体情報を取得する（ステップ S 0 4 ）。

【 0 1 3 0 】

認証端末 3 0 は、生体情報、入店者リスト及び端末 ID を含む認証要求をサーバ装置 1 0 に送信する（ステップ S 0 5 ）。

【 0 1 3 1 】

サーバ装置 1 0 は、会員情報データベースから入店者リストに記載された会員 ID のエ

50

ントリを抽出する（ステップS06）。

【0132】

サーバ装置10は、認証要求に含まれる生体情報と抽出されたエントリの生体情報を用いた生体認証を実行する（ステップS07）。

【0133】

サーバ装置10は、認証結果を認証端末30に送信する（ステップS08）。

【0134】

認証端末30は、認証結果に応じた処理を行う（ステップS09）。認証失敗であれば、認証端末30は、その旨を利用者に通知する。認証成功であれば、認証端末30は、代金決済に関する処理を実行する（決済要求を送信する）。

【0135】

[第1の実施形態に係る変形例]

上記第1の実施形態では、サイネージ20が利用者の端末40から会員IDを取得することを説明した。しかし、店舗にサイネージ20は設置されていなくともよい。サイネージ20に代わって、店舗の各所に設置された認証端末30が、端末40から会員IDを取得してもよい。

【0136】

具体的には、認証端末30は、サイネージ20の会員検出機能を包含していればよい。この場合、認証端末30は、図14に示すように、会員検出部407を備えていればよい。会員検出部407の基本的な動作は、サイネージ20の会員検出部302の動作と同一とすることができるので詳細な説明は省略する。

【0137】

また、第1の実施形態に係る変形例の認証端末30が備える通信制御部401は、Bluetooth（登録商標）等の近距離無線通信に対応していればよい。

【0138】

会員検出部407は、会員ID送信要求に対する応答によって会員IDを取得すると、当該取得した会員IDを自装置の入店者リスト管理部402に引き渡す。また、会員検出部407は、会員IDを含む「会員入店通知」を他の認証端末30に向けて送信する。

【0139】

例えば、図5において、サイネージ20が店頭（出入口）に設置されていない場合を考える。この場合、例えば、認証端末30-1が会員IDを取得すると、当該会員IDを含む会員入店通知を他の認証端末30-2～30-6に送信する。

【0140】

このように、店頭にサイネージ20が設置されていなくとも、各認証端末30が近距離無線通信によって会員IDを取得することで、店内に滞在している入店者リストが作成される。入店者リストが作成可能であるので、サーバ装置10は、会員IDを利用した認証対象の絞り込みが実現できる。

【0141】

以上のように、第1の実施形態に係る認証システムでは、端末40から店舗のエッジデバイス（サイネージ20、認証端末30）に会員IDが送信される。また、生体認証が必要となると、認証端末30は、店内に滞在している利用者の会員IDを含むリストと共に被認証者の生体情報をクラウド側（認証センター；サーバ装置10）に送信し、生体認証の実行を依頼する。サーバ装置10は、取得したリストを用いて店内に滞在している利用者を絞り込み、当該絞り込んだ利用者を登録側に設定し、生体認証を実行する。会員IDによって利用者が絞り込まれるので、高い精度の生体認証が実現できる。また、第1の実施形態に係る認証システムでは、利用者の入店時に対象を絞り込むのではなく、生体認証が必要なタイミング（即ち、代金決済が必要なタイミング）で対象の絞り込みを行っている。このような対応によって、サーバ装置10は、何らの消費行動を起こさず退店した利用者に関する処理を実行する必要がなくなる。その結果、サーバ装置10のリソースを浪費することや生体認証のスループット低下を招来することがない。

10

20

30

40

50

【 0 1 4 2 】

また、利用者の観点からは、生体情報という取り扱いの難しい個人情報を持ち歩くことなく、生体認証の利便性を享受できるという利点がある。さらに、生体認証によって決済が行えるので、通常の決済時に必要となるようなパスワード入力等の煩雑な操作が不要となる。さらに、利用者は、店舗に入店する際には、所持する端末 4 0 の近距離無線通信機能を有効にするなど、利用者と端末 4 0 の接点を増やすことができる。

【 0 1 4 3 】

また、生体認証を利用するサービス事業者の観点からは、サイネージ 2 0 が端末 4 0 から会員 ID を取得し、認証端末 3 0 は当該会員 ID を共有すれば足り、より多くの機器や複雑な処理が不要であるという利点がある。即ち、第 1 の実施形態に係る認証システムは、サービス事業者側の負担や考慮事項が少ないという利点がある。

【 0 1 4 4 】

[第 2 の実施形態]

続いて、第 2 の実施形態について図面を参照して詳細に説明する。

【 0 1 4 5 】

第 1 の実施形態では、クラウド側（認証センター；サーバ装置 1 0）が生体認証を実行することを説明した。しかし、当該生体認証はローカル側（エッジ側；店舗側）で実行されてもよい。

【 0 1 4 6 】

なお、第 2 の実施形態に係る認証システムの構成は第 1 の実施形態と同一とすることができるので図 2 に相当する説明を省略する。また、第 2 の実施形態に係るサイネージ 2 0 の処理構成も第 1 の実施形態と同一とすることができ、その説明を省略する。

【 0 1 4 7 】

以下、第 1 の実施形態と第 2 の実施形態の相違点を中心に説明する。

【 0 1 4 8 】

第 2 の実施形態に係るサイネージ 2 0 は、利用者の端末 4 0 から会員 ID を取得すると、当該会員 ID を店舗内の認証端末 3 0 に送信するのではなく、サーバ装置 1 0 に送信する。即ち、サイネージ 2 0 は、店舗（所定エリア）に滞在する滞在者の会員 ID をサーバ装置 1 0 に通知する。

【 0 1 4 9 】

より具体的には、サイネージ 2 0 の会員検出部 3 0 2 は、端末 4 0 から会員 ID を取得すると、当該会員 ID と店舗 ID を含む会員入店通知をサーバ装置 1 0 に送信する。

【 0 1 5 0 】

なお、店舗 ID は、認証システムに参加しているサービス事業者を一意に識別するための情報である。例えば、図 2 において、サービス事業者 A とサービス事業者 B には異なる店舗 ID が設定される。

【 0 1 5 1 】

また、端末 ID や店舗 ID は、サーバ装置 1 0 と端末（サイネージ 2 0、認証端末 3 0）の間において任意の方法によって共有される。例えば、システム管理者が端末 ID、店舗 ID を決定し当該決定された端末 ID をサーバ装置 1 0 に設定する。また、システム管理者は、当該決定された端末 ID をサービス事業者に通知する。サービス事業者は、通知された端末 ID を端末（サイネージ 2 0、認証端末 3 0）に設定する。

【 0 1 5 2 】

図 1 5 は、第 2 の実施形態に係るサーバ装置 1 0 の処理構成（処理モジュール）の一例を示す図である。図 1 5 を参照すると、第 2 の実施形態に係るサーバ装置 1 0 は、第 1 の実施形態に係るサーバ装置 1 0 の認証部 2 0 3 に替えて、生体情報通知部 2 0 6 を備える。

【 0 1 5 3 】

生体情報通知部 2 0 6 は、複数の利用者の ID のうちサイネージ 2 0 から通知された会員 ID に対応する生体情報を認証端末 3 0 に通知する手段である。

【 0 1 5 4 】

会員入店通知を受信すると、生体情報通知部 206 は、会員入店通知に含まれる会員 ID をキーとして会員情報データベースを検索し、対応するエントリを特定する。生体情報通知部 206 は、特定したエントリの生体情報（取得した会員 ID に対応する生体情報）をサイネージ 20 が設置された店舗の各認証端末 30 に通知する。

【0155】

具体的には、生体情報通知部 206 は、特定したエントリの生体情報（特徴量）と会員 ID を含む「生体情報通知」を各認証端末 30 に送信する。

【0156】

なお、生体情報通知部 206 は、店舗 ID に基づき会員入店通知の送信元となる店舗及び当該店舗に設置された複数の認証端末 30 を特定する。具体的には、生体情報通知部 206 は、店舗 ID と認証端末 30 の端末 ID を対応付けて記憶するテーブル情報を参照することで生体情報通知の送信先となる認証端末 30 を把握する。

10

【0157】

生体情報通知部 206 は、送信先として特定された各認証端末 30 に向けて「生体情報通知」を送信する。即ち、サーバ装置 10 は、会員入店通知の受信に応じて、対応する会員の生体情報を少なくとも 1 以上の認証端末 30 に送信する。

【0158】

図 16 は、第 2 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 16 を参照すると、第 2 の実施形態に係る認証端末 30 は、第 1 の実施形態に係る認証端末 30 の認証要求部 404 に替えて、認証部 408 を備える。

20

【0159】

入店者リスト管理部 402 は、生体情報通知を受信すると、当該通知に記載された会員 ID と生体情報を入店者リストに記載する（図 17 参照）。このように、各認証端末 30 は、サーバ装置 10 から取得した生体情報（入店者の生体情報）を内部に蓄積する。換言すれば、認証端末 30 は、サーバ装置 10 から通知された生体情報を入店者リスト（生体情報リスト）に記憶し、店内に滞在している利用者の生体情報を蓄積する。

【0160】

認証端末 30 は、代金決済の際、利用者の生体情報を取得し、生体認証を実行する。具体的には、認証部 408 は、生体情報取得部 403 から被認証者の生体情報を取得すると、入店者リストに記載された生体情報と生体情報取得部 403 から取得した生体情報を用いた生体認証を実行する。即ち、認証部 408 は、被認証者の認証が必要になると、生体情報取得部 403 により取得された生体情報とリスト（入店者リスト）に記憶された生体情報を用いた生体認証を実行する。

30

【0161】

なお、認証部 408 の基本的な動作は、第 1 の実施形態で説明した認証部 203 の動作と同一とすることができるので、認証部 408 に関するより詳細な説明を省略する。

【0162】

認証部 408 は、生体認証に成功すると、認証成功者の会員 ID を決済要求部 405 に引き渡す。決済要求部 405 は、会員 ID と決済情報を含む決済要求をサーバ装置 10 に送信する。

40

【0163】

例えば、図 5 の例では、サイネージ 20 は、端末 40 を所持する利用者の会員 ID を含む会員入店通知をサーバ装置 10 に送信する。サーバ装置 10 は、当該会員 ID に対応する生体情報を会員情報データベースから読み出し、認証端末 30 - 1 ~ 30 - 6 に通知する（生体情報通知を送信する）。

【0164】

各認証端末 30 は、通知された生体情報と会員 ID を対応付けて記憶する。

【0165】

図 5 に示すように、利用者が認証端末 30 - 3 を利用して代金決済を行う場合、認証端末 30 - 3 は、内部に蓄積された生体情報を用いた生体認証を実行し、利用者の会員 ID

50

を特定する。認証端末 30 は、特定した会員 ID と決済情報を含む決済要求をサーバ装置 10 に送信する。

【0166】

[システムの動作]

続いて、第 2 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。図 18 は、第 2 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。

【0167】

サイネージ 20 は、会員 ID 送信要求の応答から会員 ID を取得する (ステップ S11)。

【0168】

サイネージ 20 は、当該取得した会員 ID を含む会員入店通知をサーバ装置 10 に送信する (ステップ S12)。

【0169】

サーバ装置 10 は、会員入店通知に含まれる会員 ID に対応する会員の生体情報を特定する (ステップ S13)。

【0170】

サーバ装置 10 は、特定した生体情報と会員 ID を含む生体情報通知を各認証端末 30 に送信する (ステップ S14)。

【0171】

各認証端末 30 は、取得した会員 ID 及び生体情報を入店者リストに記載する (ステップ S15)。

【0172】

認証端末 30 は、面前に利用者 (被認証者) を検出すると、生体認証を実行する (ステップ S16)。認証端末 30 は、内部に蓄積された入店者の生体情報を用いて生体認証を実行する。

【0173】

認証端末 30 は、生体認証に成功すると、被認証者の会員 ID を含む決済要求をサーバ装置 10 に送信する (ステップ S17)。

【0174】

サーバ装置 10 は、決済情報及び口座情報を用いた決済処理を実行する (ステップ S18)。

【0175】

[第 2 の実施形態に係る変形例 1]

上記第 2 の実施形態では、会員が入店したタイミングで会員 ID がサーバ装置 10 に送信され、サーバ装置 10 が当該会員 ID に対応する生体情報を各認証端末 30 に通知することを説明した。しかし、会員 ID は、認証端末 30 にて生体認証が必要となったタイミング (代金決済のタイミング) でサーバ装置 10 に送信されてもよい。例えば、サイネージ 20 は、端末 40 から会員 ID を取得すると当該取得した会員 ID を「入店者リスト」を用いて管理する。

【0176】

認証端末 30 は、決済が必要になると (生体認証の実行が必要になると)、「入店者リスト送信要求」をサイネージ 20 に送信する。サイネージ 20 は、当該要求を受信すると、入店者リストをサーバ装置 10 に送信する。

【0177】

サーバ装置 10 は、入店者リストに記載された会員 ID に対応する生体情報を会員情報データベースから読み出し、会員 ID と生体情報を含む生体情報通知を認証端末 30 に送信する。

【0178】

認証端末 30 は、生体情報通知に記載された生体情報を登録側の生体情報に設定し、生体認証を実行することで、面前の利用者を特定する。認証端末 30 は、特定した利用者の

10

20

30

40

50

会員IDを含む決済要求をサーバ装置10に送信する。

【0179】

このように、生体認証をエッジ側（店舗側、サービス事業者側）で実行する場合であっても、生体認証が必要なタイミング、即ち、代金決済のタイミングで会員IDがサーバ装置10に送信されてもよい。サーバ装置10は、会員IDによって店内に滞在している会員を絞り込み、絞り込んだ会員の生体情報を認証端末30に通知してもよい。

【0180】

[第2の実施形態に係る変形例2]

上記第2の実施形態では、入店した会員の生体情報は認証端末30に蓄積され、当該認証端末30が生体認証を実行する場合について説明した。ここで、サーバ装置10（クラウド側）から店舗側（エッジ側）に送信される生体情報は、各認証端末30が記憶するのではなく、各店舗に設置された店舗サーバが記憶してもよい。

10

【0181】

具体的には、図19に示すように、各店舗に店舗サーバ50が設置され、店舗側の端末（サイネージ20、認証端末30）と店舗サーバ50が接続されていてもよい。店舗サーバ50は、サーバ装置10と接続される。なお、店舗サーバ50は、サーバ装置10を「第1のサーバ装置」とすれば「第2のサーバ装置」となる。

【0182】

サーバ装置10は、会員入店通知を受信すると、受信した会員IDに対応する生体情報及び会員IDを含む「生体情報通知」を店舗サーバ50に送信する。

20

【0183】

店舗サーバ50は、受信した会員ID、生体情報を入店者リストに記憶する。

【0184】

認証端末30は、生体認証が必要な場合、被認証者の生体情報を店舗サーバ50に送信する。より具体的には、認証端末30は、代金決済が必要な場合に、被認証者の生体情報を含む認証要求を店舗サーバ50に送信する。店舗サーバ50は、蓄積された生体情報（入店者リストに記載された生体情報）と認証端末30から取得した生体情報を用いた生体認証を実行する。

【0185】

店舗サーバ50は、生体認証に成功すると認証成功者の会員IDを認証端末30に送信する。認証端末30は、会員IDと決済情報を含む決済要求をサーバ装置10に送信する。認証端末30は、当該決済要求を、店舗サーバ50を介してサーバ装置10に送信してもよいし、直接、サーバ装置10に送信してもよい。

30

【0186】

なお、第2の実施形態に係る変形例2において、サイネージ20が端末IDをサーバ装置10に送信し、当該端末IDに対応する生体情報が店舗サーバ50に送信されるタイミングは利用者の決済時であってもよい。

【0187】

第2の実施形態に係る変形例2の各装置の処理構成について説明する。

【0188】

サーバ装置10に関しては、図15を参照して説明した処理構成と同一とすることができる。生体情報通知部206は、生体情報通知を店舗サーバ50に向けて送信すればよい。

40

【0189】

サイネージ20に関しては、図9を参照して説明した処理構成と同一とすることができる。会員検出部302は、店舗サーバ50を介して会員入店通知をサーバ装置10に送信してもよいし、直接、当該通知をサーバ装置10に送信してもよい。

【0190】

認証端末30に関しては、図20に示すような構成とすることができる。図20に示すように、第2の実施形態に係る変形例2の認証端末30は、入店者リスト管理部402を備えていなくともよい。認証要求部404は、被認証者の生体情報を含む認証要求を店舗

50

サーバ50に送信し、店舗サーバ50から認証成功者の会員IDを取得する。

【0191】

図21は、第2の実施形態に係る変形例2の店舗サーバ50の処理構成（処理モジュール）の一例を示す図である。図21に示すように、店舗サーバ50は、通信制御部601と、入店者リスト管理部602と、認証部603と、記憶部604と、を備える。

【0192】

なお、店舗サーバ50に含まれる各処理モジュールの基本的な動作は、既に説明した同じ名称の処理モジュールの動作と同一とすることができるので、詳細な説明を省略する。

【0193】

例えば、入店者リスト管理部602は、サーバ装置10から生体情報通知を受信し、店内に滞在している利用者（会員）の会員ID、生体情報を入店者リストに追記する。また、認証部603は、認証端末30からの認証要求を処理し、生体認証に成功すると、認証成功者の会員IDを認証端末30に通知する。

【0194】

このように、認証システムは、認証端末30に代わりサーバ装置10から生体情報を受信する店舗サーバ50をさらに含んでもよい。この場合、認証端末30は、被認証者の生体情報を含む認証要求を店舗サーバ50に送信する。店舗サーバ50は、サーバ装置10から受信した生体情報と認証要求に含まれる生体情報を用いた生体認証を実行する。

【0195】

なお、第2の実施形態においても、認証端末30がサイネージ20の機能を備えていてもよい。第2の実施形態においても、サイネージ20に替わり認証端末30が会員IDを利用者の端末40から取得してもよい。認証端末30は、取得した会員IDをサーバ装置10に送信してもよい。

【0196】

以上のように、第2の実施形態に係るシステムでは、店舗に入店した利用者の会員IDはサーバ装置10に送信される。サーバ装置10は、会員IDから対応する利用者の生体情報を特定し、当該特定した生体情報をエッジ側（サービス事業者側）に通知する。エッジ側では、通知された生体情報を内部に蓄積し、生体認証に利用する。第2の実施形態によっても、会員IDによって生体認証の対象が絞り込まれるので、生体認証の精度が向上する。

【0197】

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、サーバ装置10のハードウェア構成の一例を示す図である。

【0198】

サーバ装置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、サーバ装置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。

【0199】

但し、図22に示す構成は、サーバ装置10のハードウェア構成を限定する趣旨ではない。サーバ装置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、サーバ装置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がサーバ装置10に含まれていてもよい。

【0200】

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

10

20

30

40

50

もよい。プロセッサ 3 1 1 は、オペレーティングシステム (O S ; Operating System) を含む各種プログラムを実行する。

【 0 2 0 1 】

メモリ 3 1 2 は、 R A M (Random Access Memory)、 R O M (Read Only Memory)、 H D D (Hard Disk Drive)、 S S D (Solid State Drive) 等である。メモリ 3 1 2 は、 O S 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。

【 0 2 0 2 】

入出力インターフェイス 3 1 3 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。

10

【 0 2 0 3 】

通信インターフェイス 3 1 4 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 3 1 4 は、 N I C (Network Interface Card) 等を備える。

【 0 2 0 4 】

サーバ装置 1 0 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 3 1 2 に格納されたプログラムをプロセッサ 3 1 1 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。

20

【 0 2 0 5 】

なお、サイネージ 2 0、認証端末 3 0、端末 4 0、店舗サーバ 5 0 もサーバ装置 1 0 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サーバ装置 1 0 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 3 0 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。

【 0 2 0 6 】

情報処理装置であるサーバ装置 1 0 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サーバ装置 1 0 の機能が実現できる。また、サーバ装置 1 0 は、当該プログラムにより認証方法を実行する。

30

【 0 2 0 7 】

[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。

【 0 2 0 8 】

上記実施形態では、端末 4 0 は、サイネージ 2 0 等からの要求に応じて会員 I D をサイネージ 2 0 等に通知することを説明した。しかし、端末 4 0 が、近距離無線通信によってサイネージ 2 0 等に通知する情報は会員 I D に限定されない。例えば、端末 4 0 は、会員 I D に加え、生体情報 (例えば、顔画像) を店舗端末 (サイネージ 2 0、認証端末 3 0) に通知してもよい。この場合、例えば、認証端末 3 0 は、会員 I D と生体情報に対応付けて記憶する。認証端末 3 0 は、端末 4 0 から取得した生体情報と面前の被認証者の生体情報を用いた生体認証を実行し、対応する会員 I D を特定する。認証端末 3 0 は、特定した会員 I D をサーバ装置 1 0 に送信し、決済処理を要求してもよい。

40

【 0 2 0 9 】

サーバ装置 1 0 は、会員 I D、生体情報、個人情報、口座情報等に加え、各利用者に発行されたクーポン (例えば、商品代金の割引) や特典 (例えば、誕生日月に使用可能なポイント) に関する情報 (以下、特典情報と表記する) を記憶していてもよい。サーバ装置 1 0 は、生体認証によって利用者を特定すると、当該特定された利用者の特典情報を自動

50

的に適用して決済処理を行ってもよい。あるいは、サーバ装置 10 は、生体認証によって特定された利用者の特典情報を認証端末 30 に通知してもよい。認証端末 30 は、サーバ装置 10 から通知された特典情報の適用可否を認証成功者（認証成功と判定された被認証者）に問い合わせてもよい（図 23 参照）。あるいは、利用者が複数の特典情報（複数種類の特典情報）を所持している場合には、認証端末 30 は、いずれの特典情報を選択して適用するか認証成功者に問い合わせてもよい（図 24 参照）。認証端末 30 は、利用者がクーポンや特典を使用する意思を示した場合に、クーポン等の適用をしてもよい。このように、本願開示の認証システムは、クーポンや特典活用のパーソナライズサービスを提供してもよい。

【0210】

あるいは、サーバ装置 10 にクーポンや特典に関する特定情報が記憶されているのではなく、利用者の端末 40 に特典情報が記憶されていてもよい。端末 40 は、会員 ID と共に特典情報をサイネージ 20 や認証端末 30 に送信してもよい。認証端末 30 は、生体認証によって特定された利用者がクーポン、特典を保持していれば、当該クーポン等を自動的に適用してもよいし、利用者の意思（クーポン使用、クーポン不使用）に応じた処理をしてもよい。このように、本願開示の認証システムは、クーポンや特典の使用忘れを防止でき、利用者にその利便性を感じ取ってもらうことで、店舗の継続的なリピート使用を促す。

【0211】

認証端末 30 の入店者リスト管理部 402 や店舗サーバ 50 の入店者リスト管理部 602 は、入店者リストに登録されてから所定時間経過したエントリを削除してもよい。具体的には、入店者リスト管理部 402 は、店内で商品等を選択するのに十分な時間経過していると判断できる利用者のエントリ（会員 ID、生体情報）を削除して、入店者リストのサイズを適切に保ってもよい。あるいは、入店者リスト管理部 402 は、生体認証に成功した利用者のエントリ（会員 ID、生体情報）を削除してもよい。生体認証の成功に応じてエントリを削除した場合には、入店者リスト管理部 402 は、削除したエントリ（会員 ID）を含む「エントリ削除通知」を他の認証端末 30 に送信してもよい。当該通知を受信した認証端末 30 は、自装置で管理している入店者リストから上記削除されたエントリを削除する。

【0212】

認証端末 30 は、入店から所定時間経過することで入店者リストからエントリが削除された利用者に配慮した対応を行ってもよい。例えば、認証端末 30 は、生体認証の結果が認証失敗の場合、「入店から長時間経過したため入店記録が削除された可能性があります。会員 ID とパスワードを入力して下さい。」といった内容の GUI（Graphical User Interface）を表示してもよい（図 25 参照）。このように、認証端末 30 は、入店から一定時間経過することでエントリが削除された利用者が商品代金の決済を行う際（生体認証を受ける際）には、利用者に会員 ID、パスワード（パスコード）等の入力を求めてもよい。なお、パスワードにより本人認証が行われる場合には、サーバ装置 10 の会員情報データベースは、会員 ID とパスワードを対応付けて記憶しておく。

【0213】

あるいは、店舗の入口と出口が異なる場合、出口で検出された利用者の会員 ID が入店者リストから削除されてもよい。この場合、図 26 に示すように、店舗の出口にサイネージ 21 が設置されている。サイネージ 21 の会員検出部 302 は、近距離無線通信によって利用者の端末 40 から会員 ID を取得すると、当該利用者は退店したと判断する。会員検出部 302 は、当該取得した会員 ID を含む「会員退店通知」を認証端末 30 に送信する。会員退店通知を受信した認証端末 30 は、当該通知に記載された会員 ID に対応する入店者リストのエントリを削除する。

【0214】

図 26 に示すようにサイネージ 21 が設置されている場合には、例えば、店舗サーバ 50 は、店舗内の状況を正確に把握することができる。より具体的には、図 26 に示す構成

10

20

30

40

50

において、入口に設置されたサイネージ 2 0 は会員入店通知を店舗サーバ 5 0 に送信する。対して、出口に設置されたサイネージ 2 1 は会員退店通知を店舗サーバ 5 0 に送信する。店舗サーバ 5 0 の入店者リスト管理部 6 0 2 は、2 つの通知により店舗に滞在している利用者を正確に把握できる。

【0215】

さらに、店舗サーバ 5 0 は、認証端末 3 0 による認証要求を用いることで、店内にて消費行動をした利用者か消費行動をしない利用者か判定することもできる。具体的には、店舗サーバ 5 0 は、認証要求の対象となった利用者は消費行動を行い、認証要求の対象とならず退店した利用者（会員退店通知に含まれる会員 ID の利用者）は消費行動をしていない利用者として判断できる。あるいは、店舗サーバ 5 0 は、所定時間経過したことによって、

10

【0216】

店舗サーバ 5 0 は、上記判定した利用者の種別（消費行動をした利用者、消費行動をしていない利用者）を用いて、機会ロス率を計算してもよい。この場合、店舗サーバ 5 0 は、図 2 7 に示すように、解析部 6 0 5 を備える。解析部 6 0 5 は、入店者リストや認証端末 3 0 からの認証要求（又は認証処理の結果）を解析することで、各種の指標等を計算する手段である。解析部 6 0 5 は、例えば、一日の入店者総数に対する消費行動をしなかった利用者の割合を計算してもよい。具体的には、解析部 6 0 5 は、来店者数（入店者数）に対する消費行動をしていない利用者数の割合を「機会ロス率」として計算する。店舗サーバ 5 0 の解析部 6 0 5 は、入店した利用者のうち生体認証の結果が認証成功とならなかった利用者の割合を機会ロス率として計算する。このように、店舗サーバ 5 0 は、所定期間における、所定エリアに滞在した滞在者数に対する生体認証の結果が成功とならなかった滞在者数を機会ロス率として計算する。例えば、1 日に来店した利用者数（滞在者総数）が 1 0 0 であって、生体認証に成功していない利用者数（消費行動をしていない利用者数）が 3 0 であれば、機会ロス率は 3 0 % と計算される。解析部 6 0 5 は、計算した機会ロス率を店舗の運営者等に提示する。例えば、解析部 6 0 5 は、図 2 8 に示すような、1 日あたりの機会ロス率を店舗運営者等に提示する。

20

【0217】

また、店舗サーバ 5 0 は、利用者の属性（例えば、性別、年齢）ごとの機会ロス率を計算してもよい。この場合、解析部 6 0 5 は、入店した利用者の会員 ID をサーバ装置 1 0 に送信し、当該会員 ID に対応する利用者の個人情報（性別、年齢等）を取得する。解析部 6 0 5 は、取得した個人情報（属性情報；性別、年齢）と会員 ID を対応付けて管理することで、年代ごとの機会ロス率、性別ごとの機会ロス率を計算することができる。このように、店舗サーバ 5 0 は、利用者の会員 ID から導出可能な属性情報ごとの機会ロス率を計算してもよい（図 2 9 参照）。なお、図 2 9 には、年代別の機会ロス率を記載している。なお、機会ロス率を算出する際の利用者の属性には、上記性別、年齢以外にも種々の属性が考えられる。例えば、店舗サーバ 5 0 は、会員グレード、所定期間内（例えば、1 週間、1 ヶ月）における商品購入金額ごとの機会ロス率を計算してもよい。

30

【0218】

なお、機会ロス率の計算や属性ごとの機会ロス率の計算は、サーバ装置 1 0 にて行われてもよい。このように、本願開示の認証システムは、利用者の店舗利用率（機会ロス率）を計算し、サービス事業者にとって有益な情報を提供してもよい。

40

【0219】

サーバ装置 1 0 や店舗サーバ 5 0 は、利用者の端末 4 0 と近距離無線通信によって通信成功した認証端末 3 0 の実績（履歴）を管理することで、利用者の動線を算出することができる。利用者の動線を算出するためには、認証端末 3 0 のそれぞれが近距離無線通信に対応している必要がある。認証端末 3 0 は、近距離無線通信によって利用者を検出すると、当該利用者の端末 4 0 から取得した会員 ID を店舗サーバ 5 0 に送信する。

【0220】

店舗サーバ 5 0 の入店者リスト管理部 6 0 2 は、会員 ID の送信元である認証端末 3 0

50

を時系列で管理する。例えば、店舗サーバ50は、図30に示すような入店者リストを保持する。入店者リスト管理部602は、会員IDの送信元の認証端末30の端末IDを動線フィールドに追記する。なお、図30では、理解の容易のため、認証端末30の符号を端末IDとして記載している。図30を参照すると、入店者リストの2番目に記載された利用者は、認証端末30-1、30-2、30-5、30-6の順で会員IDが取得されているので、図3に示す店舗レイアウトの奥まで行かず真ん中の通路を通過して出入口に向かっているのが分かる。このように、近距離無線通信に対応した認証端末30（エッジデバイス）を店内に複数配置することで、最も購買に貢献する経路（ゴールデンルート）及び陳列棚を特定できたり、利用者が寄り付きにくい場所を特定できたりする。店舗を運営するサービス事業者は、そのような結果を解析することで、店内レイアウトを見直すことができる。

10

【0221】

なお、サービス事業者が動線に関する情報を提供するには、図31に示すように、店舗サーバ50は、動線情報提供部606を備える。動線情報提供部606は、サービス事業者の管理者等からの要求に応じて、入店者リストの動線フィールドから動線を読み出し、提供する。より具体的には、動線情報提供部606は、各ルート（動線）の数を集計し、その結果を提示する。図30の例では、中央通路を経由した時計回りの動線（2番目、3番目の2つのエントリが該当）の本数が「2」、上側通路を通過して奥まで到達した動線（1番目のエントリ）の本数が「1」、下側通路を通過して奥まで到達した動線（4番目のエントリ）の本数が「1」といった結果が提示される。

20

【0222】

サーバ装置10や店舗サーバ50は、動線情報の提供の際に利用者の属性情報（個人情報）を利用してもよい。例えば、動線情報提供部606は、性別や年齢ごとの動線を算出してもよい。この場合、店舗サーバ50は、サーバ装置10から入店者の個人情報（属性情報；年齢、性別等）を取得する。当該取得した個人情報を活用して、動線情報提供部606は、性別ごとの動線（動線の数）や年代ごとの動線の情報を管理者等に提供してもよい。例えば、動線情報提供部606は、図32に示すような、属性ごとの動線に関する情報を店舗運営者等に提示する。なお、図32に示す動線IDは、利用者が取り得る動線を識別するためのIDである。例えば、受付端末30-1、受付端末30-2、受付端末30-3を経由するような動線には「動線1」のようなIDが割り当てられる。

30

【0223】

あるいは、動線情報提供部606は、動線ごとの機会ロス率を計算してもよい。動線情報提供部606は、動線ごとの入店者数を計算すると共に、動線ごとの認証成功とならなかった人数を計算する。動線情報提供部606は、入店者数に対する認証成功とならない人数の割合を計算することで機会ロス率を計算する。この場合、例えば、動線情報提供部606は、図33に示すような、動線ごとの機会ロス率に関する情報を店舗運営者等に提示する。

【0224】

例えば、動線情報提供部606は、20代から30代の女性は「動線1」を移動することが多いが、機会ロス率が「50%」と高いといった情報を店舗運営者等に提示できる。さらに、動線情報提供部606は、動線1に置かれた20代～30代の女性向け商品を変更することで機会ロス率を減らせる可能性があることを提案することができる。あるいは、動線情報提供部606は、「動線3」を移動する50代男性は少ないが、機会ロス率も「5%」と低いといった情報を店舗運営者等に提示できる。そこで、例えば、動線情報提供部606は、動線3における50代男性向けの商品は維持しつつも、他の世代向けの商品は入れ替えたほうが良いことを提案する。

40

【0225】

このように、本願開示に係る認証システムは、動線解析サービスを提供してもよい。即ち、店舗に設置された複数の認証端末30のそれぞれは、利用者（店舗の滞在者）が所持する端末40から会員IDを取得すると、当該会員IDを店舗サーバ50に通知する。店

50

舗サーバ50は、通知された会員IDと会員IDの送信元である認証端末30の端末IDに基づいて滞在者の動線を算出する。その際、店舗サーバ50は、利用者の属性ごとの動線情報を算出してもよい。

【0226】

サーバ装置10や店舗サーバ50は、利用者の属性情報と購買情報を分析してもよい。例えば、サーバ装置10は、性別や年齢ごとの売れ筋商品等を解析結果として算出してもよい。

【0227】

このように、本願開示の変形例では、長い時間に亘り認証に成功せず削除された会員IDや属性、動線（移動ルート）、入店時の時間帯、会員情報の有無等を解析することで、

10

有益な情報を店舗運営者等に提供することができる。

【0228】

上記実施形態では会員IDが各装置間で送受信されることを説明した。しかし、会員IDに替えて、端末番号が各装置（サイネージ20、端末40、認証端末30、サーバ装置10）間で送受信されてもよい。即ち、サーバ装置10は、端末番号を会員IDとして扱ってもよい。この場合、サーバ装置10は、端末番号、生体情報、口座情報等を対応付けて記憶すればよい。

【0229】

端末40を所持せず入店した利用者や近距離無線通信に対応していない端末40（近距離無線通信の機能を有効にしていない端末40）を所持する利用者を考慮した対応が行われてもよい。例えば、生体認証に失敗した場合、認証端末30は、「会員IDを取得できなかった可能性があります。会員IDと生年月日又は電話番号を入力して下さい」といったGUIを表示してもよい（図34参照）。即ち、会員IDによる認証対象の絞り込み（データベースのエントリの絞り込み）ができなかった場合、生体認証に替えてパスワード認証が行われてもよい。あるいは、端末40を所持していない利用者は、その旨を店員に申告（端末忘れを申告）し、店員からの指示に基づいて会員ID、パスワード（生年月日、電話番号等のパスワードに類する情報）をサーバ装置10に入力してもよい。

20

【0230】

あるいは、サイネージ20は、人感センサー等を用いて周囲の利用者を検出してもよい。サイネージ20は、人感センサーを用いて利用者を検出できたにも関わらず、会員ID送信要求に対する応答を受信できない場合には、当該利用者に対して端末40の近距離無線通信機能を有効にするように促してもよい。即ち、所定エリア（店舗内）に近づいても近距離無線通信機能（例えば、Bluetooth（登録商標））オフになっている場合、利用者の端末40の近距離無線通信機能を有効にすることを促すメッセージが出力されてもよい。あるいは、サイネージ20は、上記近距離無線通信を有効にすることを促すメッセージを自装置に表示してもよい。

30

【0231】

上記実施形態では、サービス事業者としてレンタルビデオ店を例にとり説明した。しかし、本願開示の認証システムは他の業種にも適用できることは勿論である。例えば、宿泊業に対して本願開示を適用することもできる。この場合、ホテル又はホテルの敷地が「所定エリア」に設定され、認証端末30は、チェックインカウンター等に設置されたチェックイン端末に相当する。あるいは、駅や空港が「所定エリア」に設定されてもよい。この場合、改札機やゲート装置が認証端末30に相当する。例えば、駅の出入口付近にサイネージ20が設置され、当該サイネージ20が乗客の端末40からIDを取得すればよい。あるいは、スタジアム（野球場、サッカー場）のようなイベント会場やビル等が「所定エリア」に設定されていてもよい。スタジアムやビルの出入口付近にサイネージ20や当該サイネージ20と同等の機能を備えるタブレットが設置され、当該サイネージ20等が、来場者の会員IDや社員のID（社員番号等）を端末40から取得してもよい。サイネージ20等が取得したIDを用いて上記入店者リストに相当するリスト（イベント会場の近くにいる観客のリスト、出勤しようとしている社員のリスト）が生成されてもよい。

40

50

【 0 2 3 2 】

第2の実施形態では、エッジ側（店舗側）で生体認証を実行する場合を説明した。換言すれば、サーバ装置10は生体認証を実行しない場合について説明した。しかし、第2の実施形態であってもサーバ装置10は、生体認証を実行してもよい。例えば、第2の実施形態に係るサーバ装置10は、サービス事業者に応じて生体認証を実行するか否かを決定してもよい。例えば、図2において、サーバ装置10は、サービス事業者Aから認証要求を受信した場合には生体認証を実行し、サービス事業者Bから会員入店通知を受信した場合には対応する生体情報をサービス事業者Bに通知してもよい。

【 0 2 3 3 】

上記実施形態では、サイネージ20は店舗の出入口付近に設置されることを説明した。しかし、サイネージ20は、店舗の他の場所（例えば、店舗の中央）に設置されてもよい。サイネージ20は、店舗の滞在者が通過する場所の近辺に設置されていけばよい。また、店舗に設置されるサイネージ20の数も「1」に限定されず、複数のサイネージ20が店舗に設置されていてもよい。

10

【 0 2 3 4 】

上記実施形態では、サイネージ20は、会員IDを認証端末30に通知することを説明した。しかし、サイネージ20が入店者リストを生成し、当該リストを認証端末30に配布してもよい。即ち、サイネージ20は、利用者の入店のたびに入店者リストを更新し、当該更新された入店者リストを認証端末30に送信してもよい。

【 0 2 3 5 】

上記実施形態では、サイネージ20が会員の入店を検出する場合について説明した。しかし、当該会員の検出は、他のデバイスによって行われてもよい。例えば、出入口付近に設置された監視カメラに通信機能（近距離無線通信による通信機能）を持たせ、監視カメラが会員IDを認証端末30に通知してもよい。

20

【 0 2 3 6 】

上記実施形態では、Bluetooth（登録商標）のような近距離無線通信によって端末40とサイネージ20が会員IDを送受信する場合について説明した。しかし、会員IDの送受信は他の方法によって行われてもよい。例えば、交通系IC（Integrated Circuit）カードに用いられているようなRFID（Radio Frequency Identification）技術を用いて会員IDが送受信されてもよい。あるいは、利用者は、会員IDがエンコードされた2次元コード等をサイネージ20に読み込ませることで、会員IDが店舗側に送信されてもよい。

30

【 0 2 3 7 】

上記実施形態では、端末40が会員ID送信要求に応じて会員IDをサイネージ20に送信する場合について説明した。しかし、端末40は、近距離無線通信を用いて、定期的又は所定のタイミングで端末IDをサイネージ20に送信してもよい。具体的には、利用者は、端末40にインストールされたアプリケーション（端末IDを送信し顔決済を行うためのアプリケーション）を起動し、端末IDを定期的に送信する状態に設定し入店すればよい。このように、サイネージ20は、会員ID送信要求を送信しなくとも、近距離無線通信によって端末IDを取得することができる。

40

【 0 2 3 8 】

上記実施形態では、サーバ装置10の内部に会員情報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、サーバ装置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「会員検出部（会員検出手段）」、「入店者リスト管理部（入店者リスト管理手段）」、「認証部（認証手段）」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けばよい。

【 0 2 3 9 】

サーバ装置10は、利用者登録の際、利用者の身元を確認してもよい。具体的には、サーバ装置10は、利用者の生体情報、個人情報等と共に、生体情報が記載された身元確認

50

書類（例えば、パスポート、免許証等）を取得する。サーバ装置 10 は、身元確認書類の生体情報と利用者から取得した生体情報を用いた 1 対 1 照合を実行する。サーバ装置 10 は、当該照合に成功した場合に、利用者登録を行ってもよい。

【0240】

上記実施形態では、顔画像から生成された特徴量が会員情報データベースに記憶される場合について説明したが、特徴量は当該データベースに記憶されていなくともよい。特徴量に代えて顔画像が会員情報データベースに登録され、サーバ装置 10 は、認証要求を処理するたびに、登録顔画像から特徴量を生成してもよい。

【0241】

各装置（サーバ装置 10、サイネージ 20、認証端末 30、店舗サーバ 50）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。

10

【0242】

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。

【0243】

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。

20

【0244】

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、会員登録された利用者を認証する認証システムなどに好適に適用可能である。

【0245】

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。

30

[付記 1]

複数の利用者それぞれの ID と生体情報に対応付けて記憶する、サーバ装置と、少なくとも 1 以上の認証端末と、を含み、

前記少なくとも 1 以上の認証端末は、所定エリアに滞在する少なくとも 1 以上の滞在者の ID を記憶する ID リストを保持すると共に、被認証者の認証が必要になると、前記被認証者の生体情報と前記 ID リストを含む認証要求を前記サーバ装置に送信し、

前記サーバ装置は、前記複数の利用者それぞれの ID から前記 ID リストに含まれる ID を抽出し、前記抽出された ID に対応する生体情報と前記認証要求に含まれる生体情報を用いた生体認証を実行する、システム。

40

[付記 2]

前記サーバ装置は、前記生体認証に成功すると、認証成功者の ID を前記認証要求の送信元である前記認証端末に通知し、

前記認証端末は、前記認証成功者の ID を用いて前記認証成功者にサービスを提供する、付記 1 に記載のシステム。

[付記 3]

前記少なくとも 1 以上の滞在者が所持する端末から前記少なくとも 1 以上の滞在者の ID を取得する、デバイスをさらに含み、

前記デバイスは、前記取得した ID を、前記少なくとも 1 以上の認証端末に通知し、

50

前記認証端末は、前記通知された I D を前記 I D リストに記憶する、付記 1 又は 2 に記載のシステム。

[付記 4]

前記デバイスは、前記端末と近距離無線通信によって通信することで、前記少なくとも 1 以上の滞在者の I D を取得する、付記 3 に記載のシステム。

[付記 5]

前記デバイスは、前記所定エリアに設置された複数の前記認証端末それぞれに、前記少なくとも 1 以上の滞在者の I D を通知する、付記 3 又は 4 に記載のシステム。

[付記 6]

前記少なくとも 1 以上の認証端末は、前記端末と近距離無線通信によって通信することで、前記少なくとも 1 以上の滞在者の I D を取得する、付記 1 又は 2 に記載のシステム。

10

[付記 7]

前記サーバ装置は、前記複数の利用者それぞれの I D、生体情報及び特典情報を対応付けて記憶し、前記生体認証に成功すると、前記認証成功者の I D と前記特典情報を前記認証要求の送信元である前記認証端末に通知し、

前記認証端末は、前記通知された特典情報の適用可否を前記認証成功者に問い合わせる、付記 2 に記載のシステム。

[付記 8]

複数の利用者それぞれの I D と生体情報に対応付けて記憶する、第 1 のサーバ装置と、所定エリアに滞在する滞在者の I D を前記第 1 のサーバ装置に通知する、デバイスと、少なくとも 1 以上の認証端末と、

20

を含み、

前記第 1 のサーバ装置は、前記複数の利用者の I D のうち前記通知された I D に対応する生体情報を前記少なくとも 1 以上の認証端末に通知し、

前記少なくとも 1 以上の認証端末は、前記通知された生体情報を生体情報リストに記憶し、被認証者の認証が必要になると、前記被認証者の生体情報と前記生体情報リストに記憶された生体情報を用いた生体認証を実行する、システム。

[付記 9]

前記第 1 のサーバ装置は、前記通知された I D に対応する生体情報と共に前記デバイスから通知された I D を前記少なくとも 1 以上の認証端末に通知し、

30

前記少なくとも 1 以上の認証端末は、前記通知された I D と生体情報を前記生体情報リストに記憶する、付記 8 に記載のシステム。

[付記 10]

前記少なくとも 1 以上の認証端末に替わり前記第 1 のサーバ装置から前記生体情報を受信する、第 2 のサーバ装置をさらに含み、

前記少なくとも 1 以上の認証端末は、前記被認証者の生体情報を含む認証要求を前記第 2 のサーバ装置に送信し、

前記第 2 のサーバ装置は、前記第 1 のサーバ装置から受信した生体情報と前記認証要求に含まれる生体情報を用いた生体認証を実行する、付記 8 又は 9 に記載のシステム。

[付記 11]

40

前記第 2 のサーバ装置は、所定期間における、前記所定エリアに滞在した滞在者数に対する前記生体認証の結果が成功とならなかった滞在者数を機会ロス率として計算する、付記 10 に記載のシステム。

[付記 12]

前記認証端末は、前記滞在者の I D を取得すると、前記取得した I D を前記第 2 のサーバ装置に通知し、

前記第 2 のサーバ装置は、前記通知された I D の送信元の端末 I D により前記滞在者の動線を算出する、付記 10 に記載のシステム。

[付記 13]

複数の利用者それぞれの I D と生体情報に対応付けて記憶する、記憶部と、

50

所定エリアに滞在する少なくとも1以上の滞在者のIDを記憶するIDリストを保持する認証端末から、被認証者の生体情報と前記IDリストを含む認証要求を受信する、受信部と、

前記複数の利用者それぞれのIDから前記IDリストに含まれるIDを抽出し、前記抽出されたIDに対応する生体情報と前記認証要求に含まれる生体情報を用いた生体認証を実行する、認証部と、

を備える、サーバ装置。

[付記14]

複数の利用者それぞれのIDと生体情報に対応付けて記憶する、サーバ装置において、所定エリアに滞在する少なくとも1以上の滞在者のIDを記憶するIDリストを保持する認証端末から、被認証者の生体情報と前記IDリストを含む認証要求を受信し、

前記複数の利用者それぞれのIDから前記IDリストに含まれるIDを抽出し、前記抽出されたIDに対応する生体情報と前記認証要求に含まれる生体情報を用いた生体認証を実行する、認証方法。

[付記15]

複数の利用者それぞれのIDと生体情報に対応付けて記憶する、サーバ装置に搭載されたコンピュータに、

所定エリアに滞在する少なくとも1以上の滞在者のIDを記憶するIDリストを保持する認証端末から、被認証者の生体情報と前記IDリストを含む認証要求を受信する処理と、

前記複数の利用者それぞれのIDから前記IDリストに含まれるIDを抽出する処理と、前記抽出されたIDに対応する生体情報と前記認証要求に含まれる生体情報を用いた生体認証を実行する処理と、

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。

【0246】

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op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】

【0247】

10 サーバ装置

20 サイネージ

21 サイネージ

30 認証端末

30-1 認証端末

30-2 認証端末

30-3 認証端末

30-4 認証端末

30-5 認証端末

30-6 認証端末

40 端末

50 店舗サーバ

101 サーバ装置

102 認証端末

201 通信制御部

202 利用者登録部

203 認証部

204 決済部

10

20

30

40

50

- 2 0 5 記憶部
- 2 0 6 生体情報通知部
- 3 0 1 通信制御部
- 3 0 2 会員検出部
- 3 0 3 メッセージ出力部
- 3 0 4 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 入店者リスト管理部
- 4 0 3 生体情報取得部
- 4 0 4 認証要求部
- 4 0 5 決済要求部
- 4 0 6 記憶部
- 4 0 7 会員検出部
- 4 0 8 認証部
- 5 0 1 通信制御部
- 5 0 2 利用者登録要求部
- 5 0 3 会員ID送信部
- 5 0 4 記憶部
- 6 0 1 通信制御部
- 6 0 2 入店者リスト管理部
- 6 0 3 認証部
- 6 0 4 記憶部
- 6 0 5 解析部
- 6 0 6 動線情報提供部

10

20

【図面】

【図1】

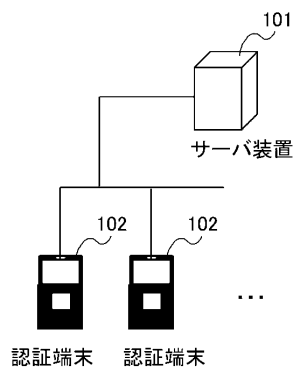


FIG.1

【図2】

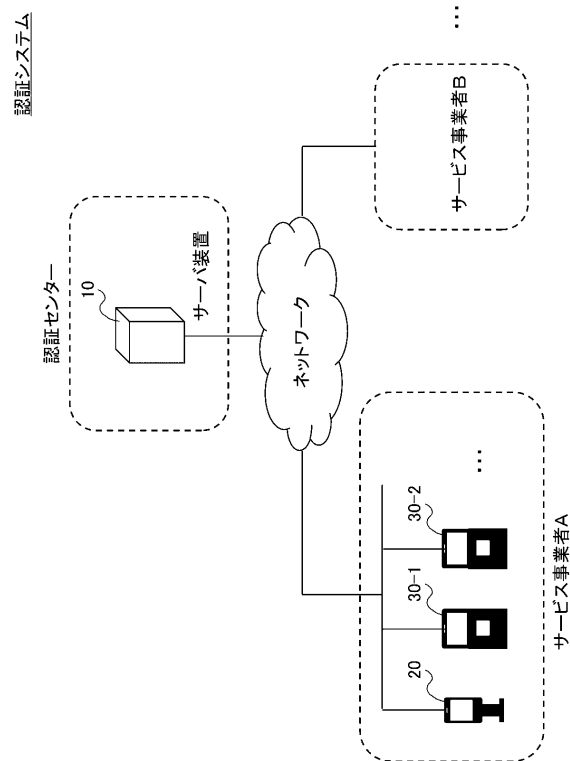


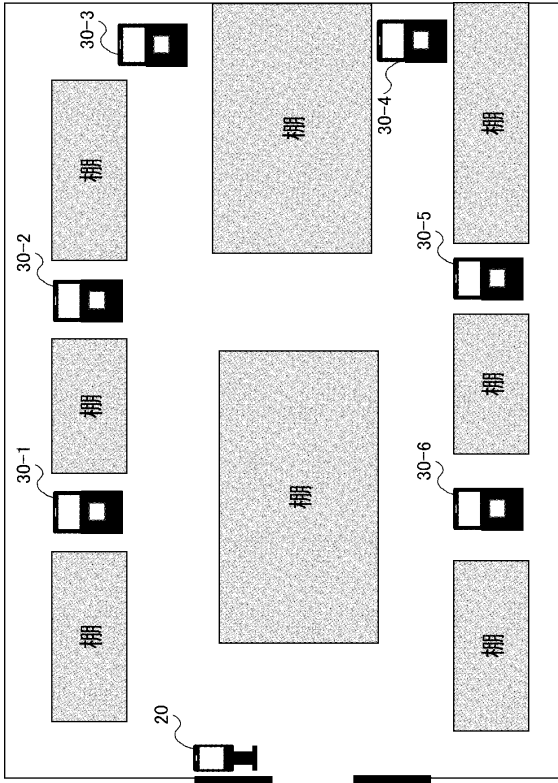
FIG.2

30

40

50

【図3】



【図4】

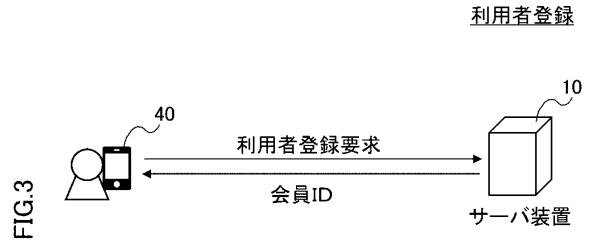
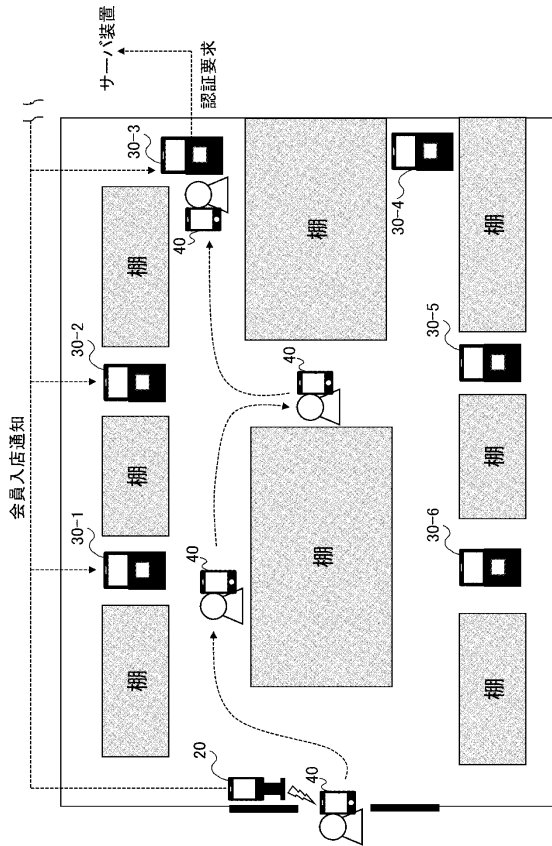


FIG.4

【図5】



【図6】

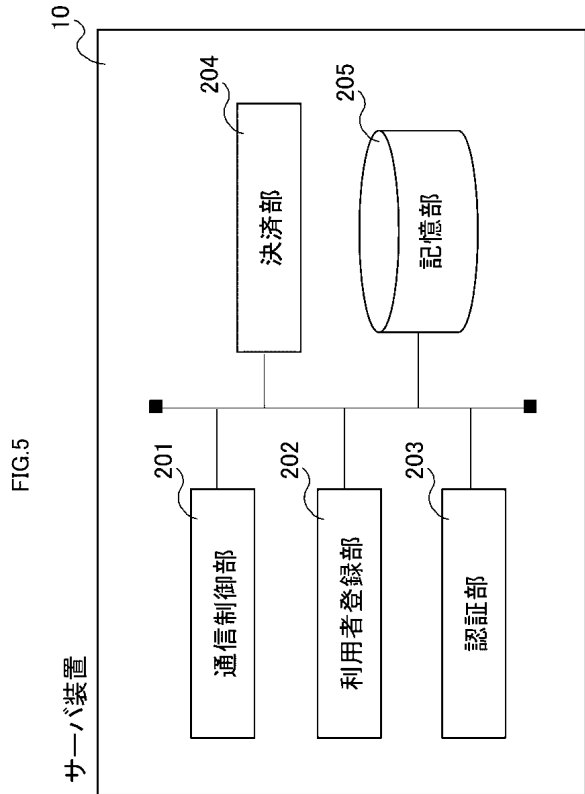


FIG.6

10

20

30

40

50

【図7】

会員情報データベース

会員ID	生体情報 (特徴量)	口座情報	個人情報		
			氏名	年齢	性別
ID01	FV01	AC01	NM11	51	女
ID02	FV02	AC02	NM12	52	男
...

FIG.7

【図8】

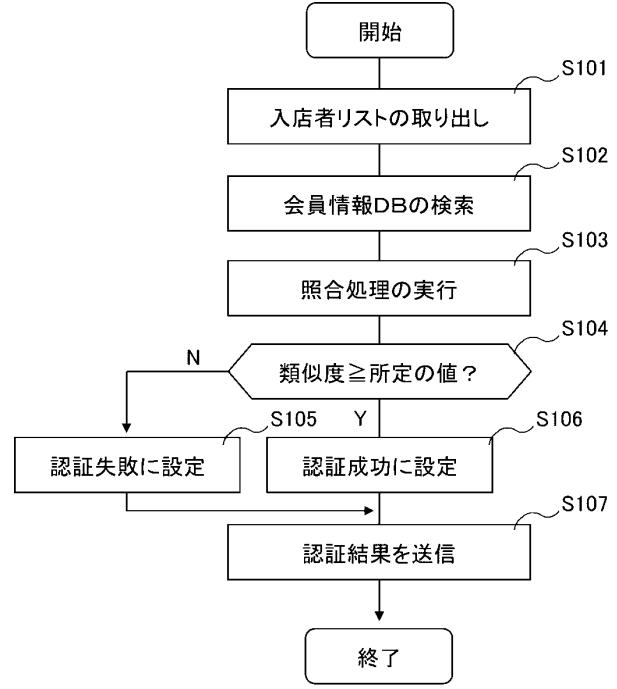


FIG.8

【図9】

20

サインページ

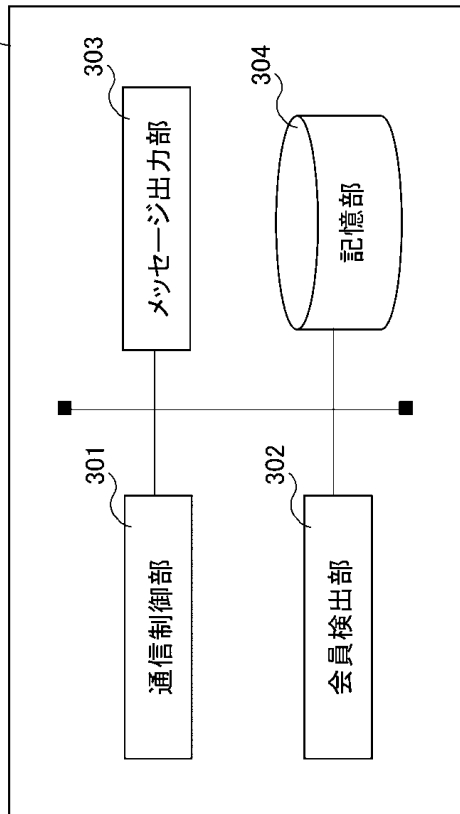


FIG.9

【図10】

30

認証端末

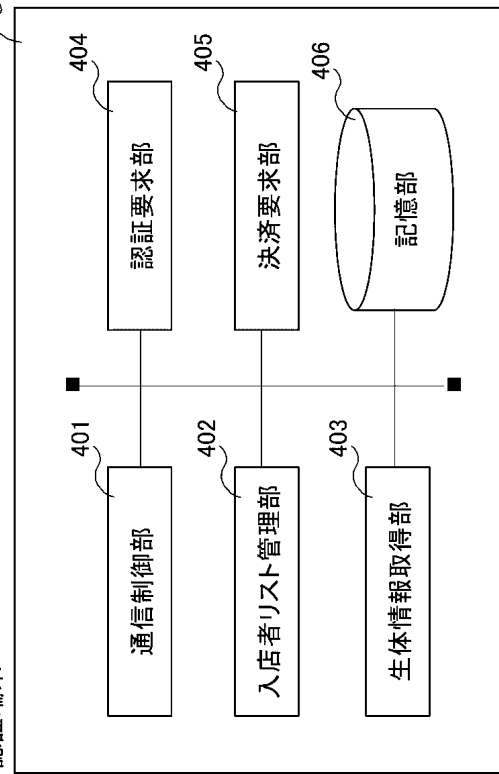


FIG.10

10

20

30

40

50

【図 1 1】

入店者リスト

入店日時	会員ID
Y1/M1/D1 H1:M1:S1	ID11
Y1/M1/D1 H1:M1:S2	ID12
Y1/M1/D1 H2:M2:S2	ID13
Y1/M1/D1 H2:M2:S3	ID14
⋮	⋮

FIG.11

【図 1 3】

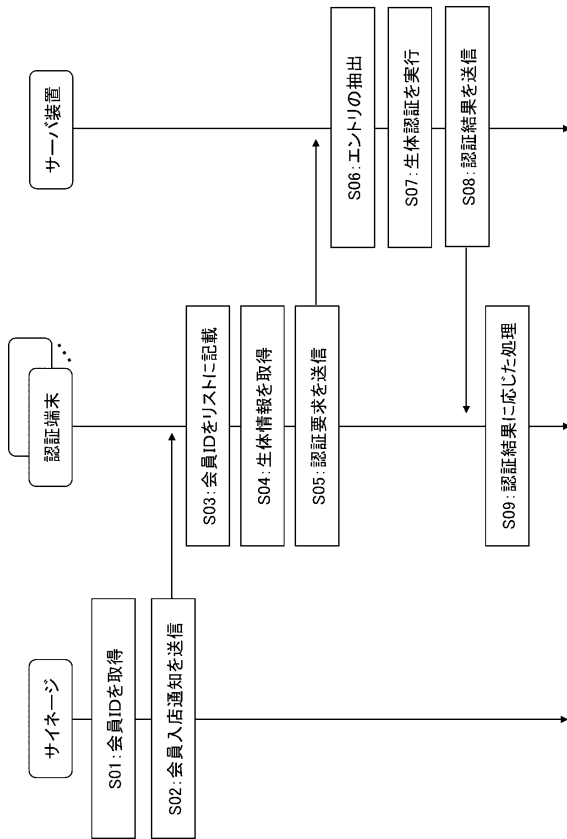


FIG.13

【図 1 2】

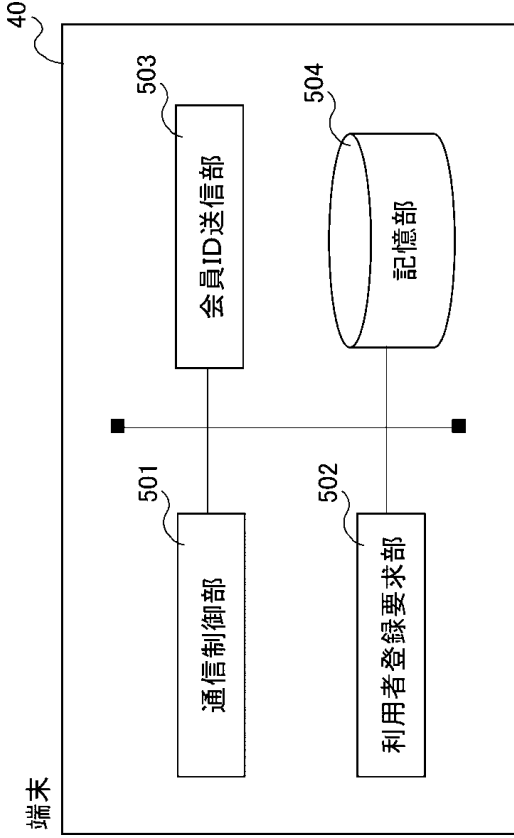


FIG.12

【図 1 4】

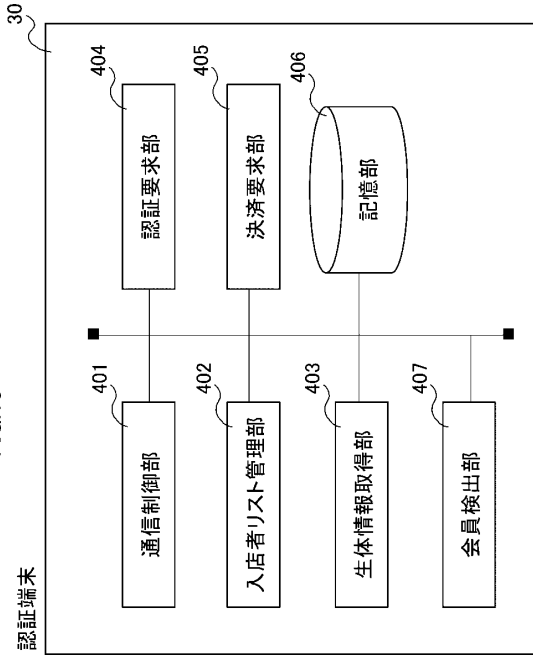
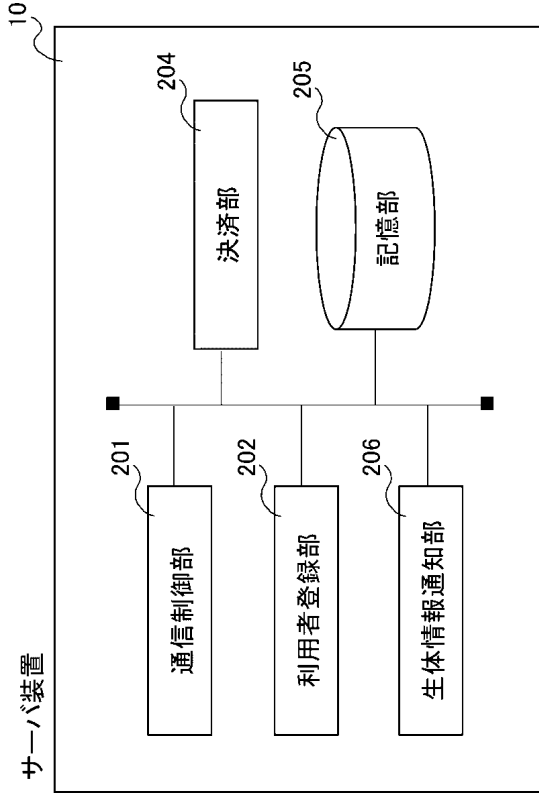
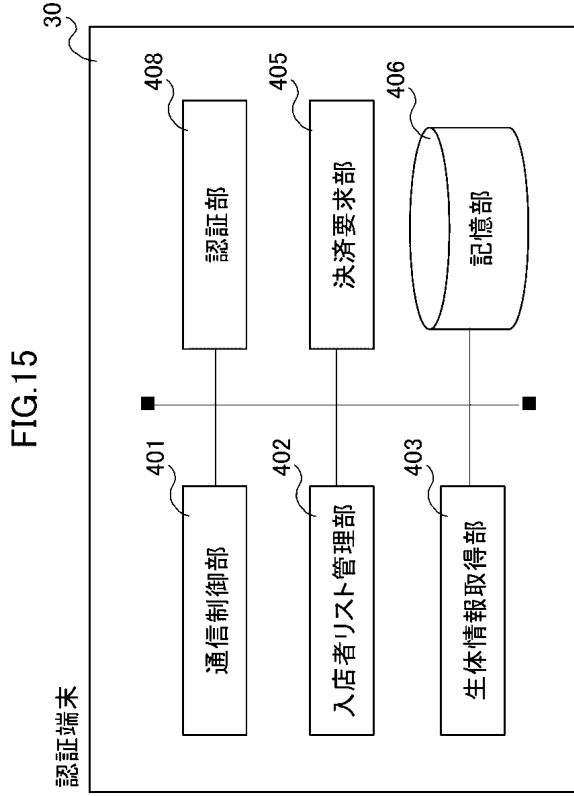


FIG.14

【図 15】



【図 16】



【図 17】

入店者リスト

入店日時	会員ID	生体情報
Y2/M1/D1 H1:M1:S1	ID21	FV21
Y2/M1/D1 H1:M1:S2	ID22	FV22
Y2/M1/D1 H2:M2:S2	ID23	FV23
Y2/M1/D1 H2:M2:S3	ID24	FV24
⋮	⋮	⋮

FIG.17

【図 18】

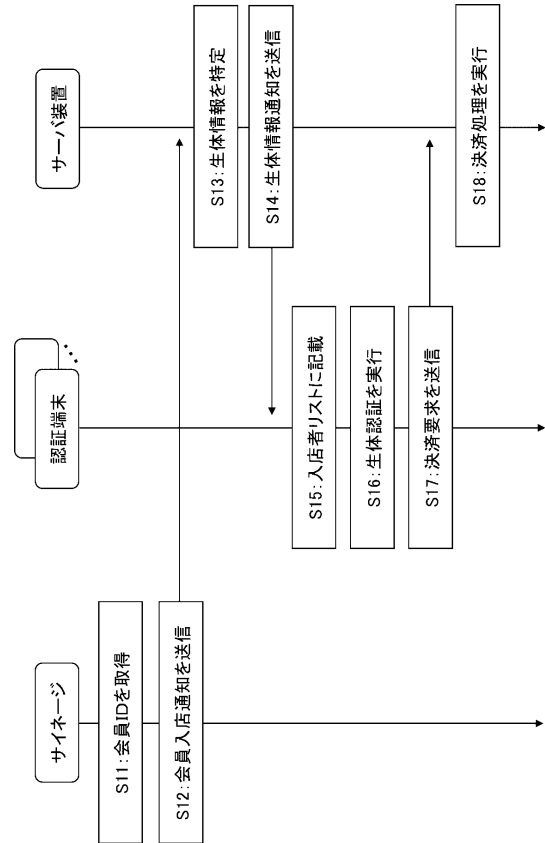


FIG.18

【図 19】

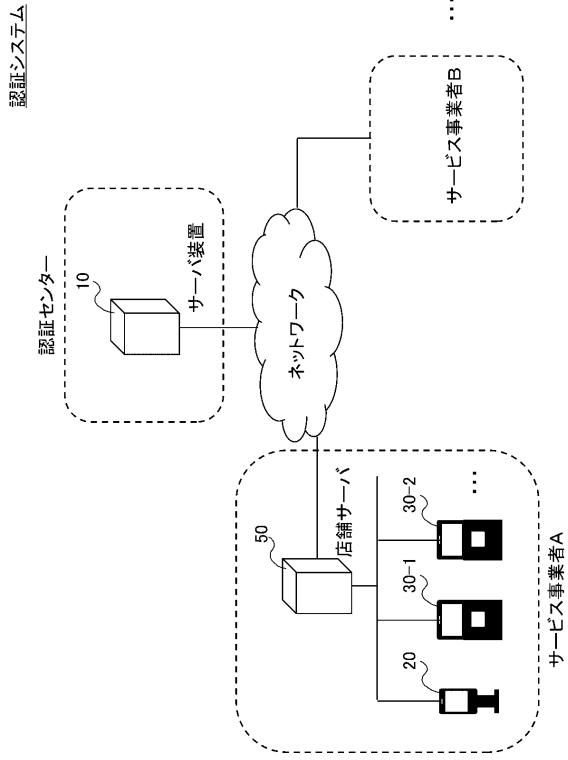


FIG.19

【図 20】

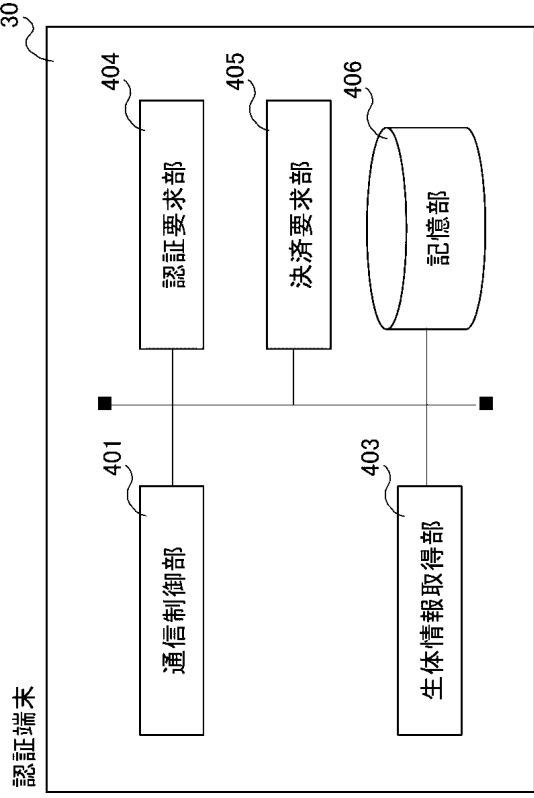


FIG.20

【図 21】

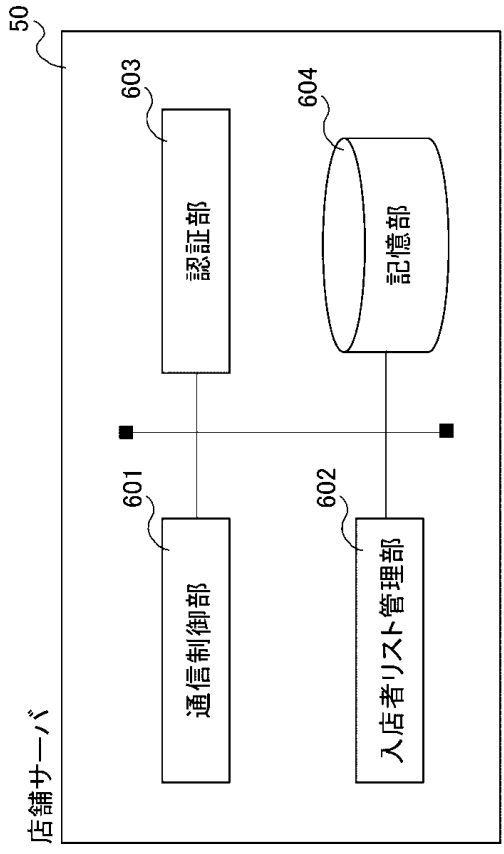


FIG.21

【図 22】

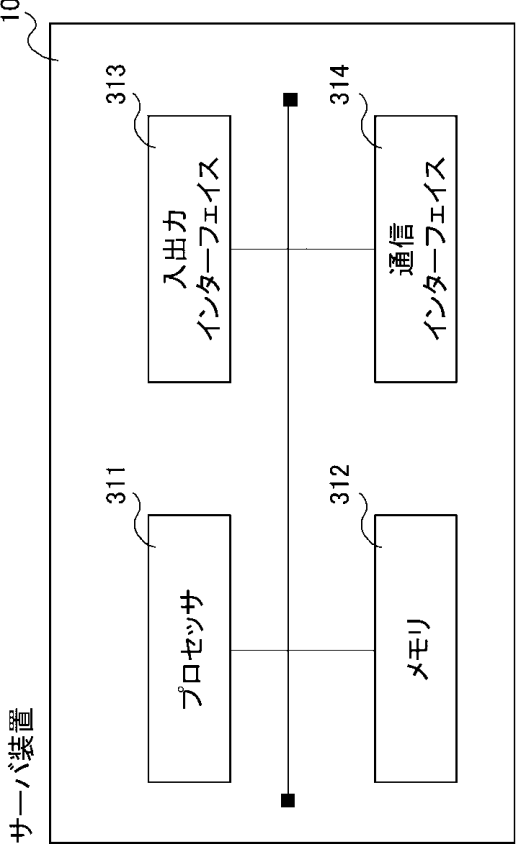


FIG.22

【図 2 3】

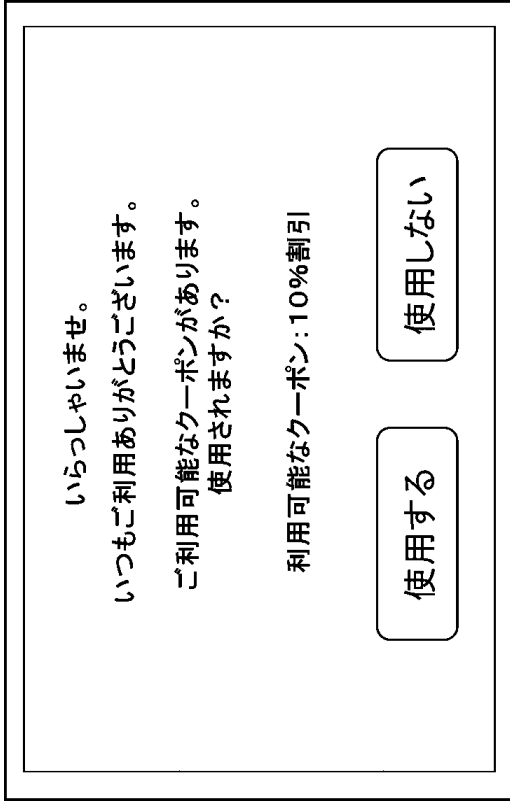


FIG.23

【図 2 4】

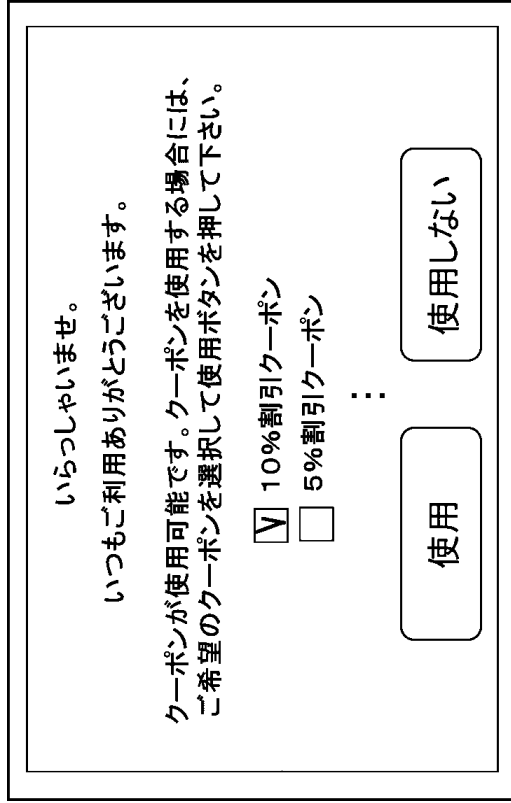


FIG.24

【図 2 5】

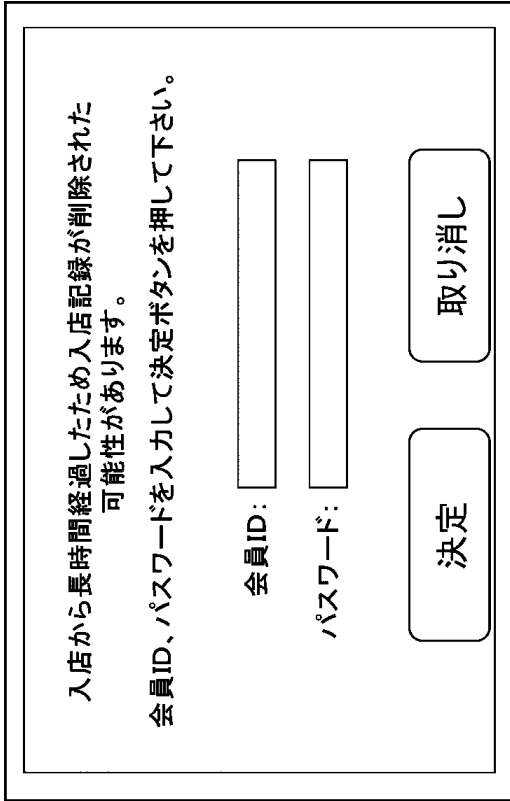


FIG.25

【図 2 6】

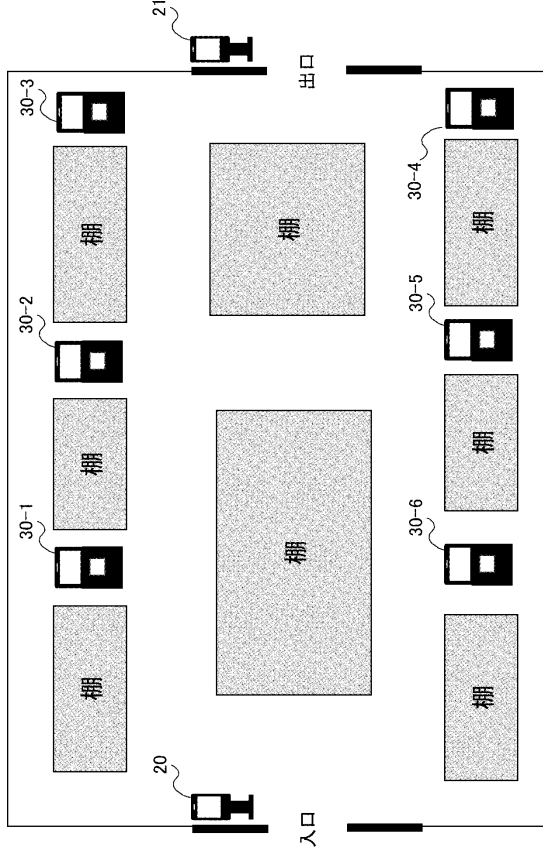
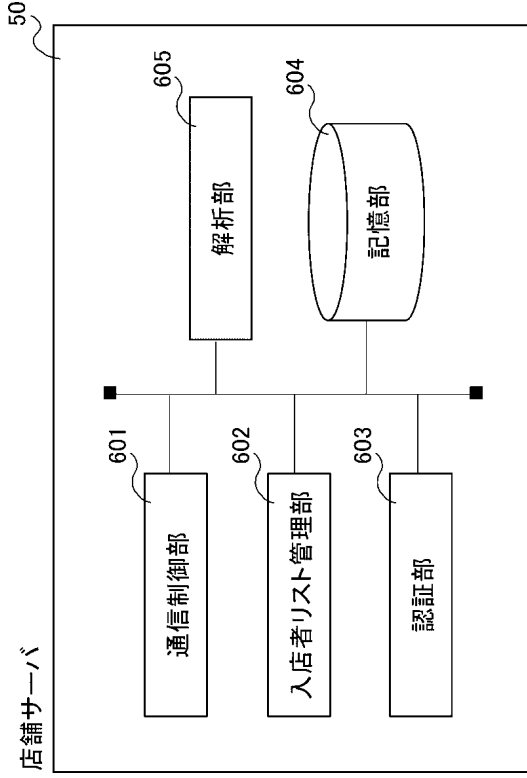


FIG.26

【図 27】



【図 28】

日付	機会ロス率
Y2/M2/D1	L1%
Y2/M2/D2	L2%
Y2/M2/D3	L3%
Y2/M2/D4	L4%
⋮	⋮

FIG.27

FIG.28

【図 29】

日付	機会ロス率	
	10代	20代
Y2/M2/D1	L11%	L12%
Y2/M2/D2	L21%	L22%
Y2/M2/D3	L31%	L32%
Y2/M2/D4	L41%	L42%
⋮	⋮	⋮

FIG.29

【図 30】

入店日時	会員ID	生体情報	入店者リスト
			動線
Y2/M1/D1 H1: M1: S1	ID21	FV21	30-1:30-2:30-3
Y2/M1/D1 H1: M1: S2	ID22	FV22	30-1:30-2:30-5:30-6
Y2/M1/D1 H2: M2: S2	ID23	FV23	30-1:30-2:30-5:30-6
Y2/M1/D1 H2: M2: S3	ID24	FV24	30-6:30-5:30-2:30-1
⋮	⋮	⋮	⋮

FIG.30

10

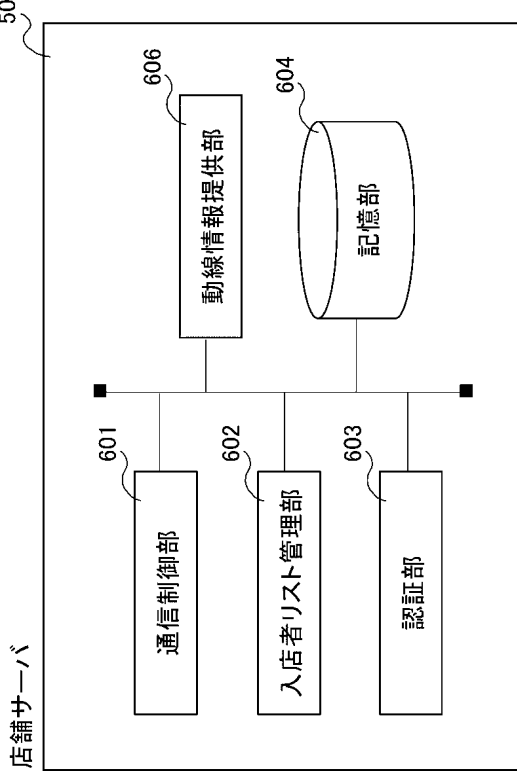
20

30

40

50

【図 3 1】



【図 3 2】

FIG.31

動線ID	動線数	
	10代	20代
動線 1	10本	30本
動線 2	30本	50本
動線 3	33本	40本
動線 4	40本	42本
...

FIG.32

【図 3 3】

動線ID	機会ロス率
動線 1	L5%
動線 2	L6%
動線 3	L7%
動線 4	L8%
...	...

FIG.33

【図 3 4】

会員IDを取得できなかった可能性があります。
 会員IDと、生年月日又は電話番号を入力して決定ボタンを押して下さい。

会員ID:

生年月日:

電話番号:

FIG.34

フロントページの続き

- (56)参考文献 特開2007-299214(JP,A)
特開2009-100334(JP,A)
特開2012-027657(JP,A)
特開2019-032803(JP,A)
特開2009-230267(JP,A)
特開2008-071366(JP,A)
米国特許出願公開第2019/0295344(US,A1)
国際公開第2018/110012(WO,A1)
- (58)調査した分野 (Int.Cl., DB名)
G06F 21/32
G06Q 30/06
G06Q 20/40