

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2017-208751

(P2017-208751A)

(43) 公開日 平成29年11月24日(2017.11.24)

(51) Int.Cl.	F I	テーマコード (参考)
H04M 9/00 (2006.01)	H04M 9/00	5C087
G08B 25/04 (2006.01)	G08B 25/04	5K038

審査請求 未請求 請求項の数 3 O L (全 11 頁)

(21) 出願番号	特願2016-101165 (P2016-101165)	(71) 出願人	000233491
(22) 出願日	平成28年5月20日 (2016. 5. 20)		株式会社日立システムズ
			東京都品川区大崎一丁目2番1号
		(74) 代理人	110000062
			特許業務法人第一国際特許事務所
		(72) 発明者	周防 壮史
			東京都品川区大崎一丁目2番1号 株式会
			社日立システムズ内
		Fターム(参考)	5C087 AA02 AA03 BB11 BB72 DD03
			DD24 DD36 EE18 FF01 FF02
			FF24 GG02 GG08 GG19 GG66
			GG70 GG83
			5K038 AA06 DD12 DD18 GG02

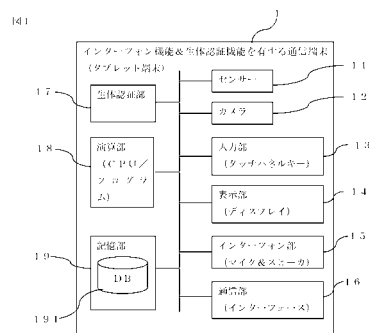
(54) 【発明の名称】 来訪者認証・判定システム

(57) 【要約】

【課題】表示機能、インターフォン機能及び通信機能を有する通信端末を利用して来訪者を認証・判定し、当該認証・判定結果に応じて、通信端末の表示機能、インターフォン機能、通信機能などを制御する技術を提供する。

【解決手段】生体認証部により生成した認証IDと記憶部に格納した来訪者の生体情報をデータ化した認証IDを照合・判定する生体ID照合・判定部と、当該認証ID照合・判定部にて判定した結果に応じて、表示部、インターフォン部、通信部の、各機能の1つ以上をONに制御する制御部と備えた電子機器。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

来訪者認証、表示、インターフォン、通信、の各機能を有する電子機器を備えた来訪者認証・判定システムであって、

前記電子機器は、

来訪者を感知したとき、当該来訪者の生体認証情報を収集するセンサー部と、表示機能を有する表示部と、インターフォン機能を有するインターフォン部と、外部機器との通信機能を有する通信部と、来訪者の生体情報を収集し、当該来訪者の生体認証情報をデータ化し、認証 I D として出力する生体認証部と、来訪者を判定するための来訪者判定情報を I D 認証として格納した記憶部と、前記認証 I D の照合・判定を行う演算部と、を有し、

10

前記演算部は、

前記生体認証部により生成した認証 I D と前記記憶部に格納した来訪者の生体情報をデータ化した認証 I D を照合・判定する生体 I D 照合・判定部と、

当該認証 I D を照合・判定部にて判定した結果に応じて、前記表示部、インターフォン部、通信部の、各機能の 1 つ以上を ON に制御する制御部と、を含む

ことを特徴とする来訪者認証・判定システム。

【請求項 2】

前記制御部は、

前記認証 I D 照合・判定部にて、照合・判定した結果、来訪者に「危険性無」と判定した場合、

20

(1) 前記表示部の表示機能及び／又は前記インターフォン機能を ON する、

(2) 前記表示部の画面にインターフォンのアイコンのみを表示する、

(3) 前記表示部の画面に来訪者に合わせた表札の表示を行う、

の何れか 1 つの制御を行い、

前記認証 I D 照合・判定部にて、照合・判定した結果、照合・判定できず不明とし、来訪者に「危険性有」と判定した場合、

(1) 前記表示部の表示機能及び／又は前記インターフォン機能を OFF する、

(2) 前記表示部の画面に警告表示を行う、

(3) 前記インターフォンのアイコンを表示するもインターフォン機能を停止状態した上で家主に「危険性有」の来訪者が来ている旨を通知する

30

の何れか 1 つの制御を行い、

前記通信部の通信機能を ON し、来訪者の認証 I D を、前記外部機器側に送信する、

ことを特徴とする請求項 1 記載の来訪者認証・判定システム。

【請求項 3】

前記認証 I D 照合・判定部にて、照合・判定した結果、照合・判定できず不明の場合、前記通信部の通信機能を ON し、

前記制御部は、

前記来訪者の認証 I D を、前記外部機器側に送信したとき、

前記外部機器から前記認証 I D の照合・判定結果を受け、当該照合・判定結果に応じて前記表示部、前記インターフォン部、前記通信部の、各機能の 1 つ以上を ON に制御することを特徴とする請求項 2 記載の来訪者認証・判定システム。

40

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、来訪者を認証・判定し、その認証・判定結果に応じて電子機器（通信端末）を制御する来訪者認証・判定システムに関する。

例えば、建造物に設置される通信端末を備えた来訪者認証・判定システムにおいて、来訪者の認証・判定結果を受けて、通信端末の表示機能、インターフォン機能、通信機能の何れか 1 つ以上を制御する来訪者認証・判定システムに関する。

【背景技術】

50

【0002】

一般的に家の門扉や玄関に、郵便配達員や宅配者などの来訪問者に家主を知らせるべき表札や呼出しのためにインターフォン、などが設置されている。表札は誰もが閲覧できる上に、公開情報の扱いとなるため、例えば、Googleのストリートビューからも確認することができる。また、インターフォンは誰でも操作できる。利便性が高い反面、悪意を持った訪問者は、表札の閲覧やインターフォンの操作を悪用される問題がある。

また、表札の閲覧拒否やインターフォン操作禁止などのセキュリティに関する機能が無い。そのため悪意のある訪問者への対策は、個人の対応力に依存している。個人の対応力には限界があるため、悪意を持った訪問者により、何かしらの損害を受ける危険性がある。また、来訪者への対応は在宅者に限定されており、来訪者の対応中に外部の人間への連絡は、困難であり、実際は在宅者のみで来訪者を対応しなければならない。

個人情報の漏洩の防止や防犯等、来訪問者の不便を解消するため、特開2010-39151号公報（特許文献1）に記載の電子表札システムに関する技術がある。この公報には、「訪問者が自身を特定する訪問元識別情報を記憶する非接触型ICカード90を、電子表札100に設けられた訪問元識別情報入力部70に近づけることで、電子表札100がICカード90から訪問元識別情報を読み取り、読み取った訪問元識別情報に基づいて訪問元を識別し、訪問元が表札情報を表示する対象の訪問元である場合には、表示部72に表札情報を表示する。」という記載がある（要約書参照）。

【先行技術文献】

【特許文献】

【0003】

【特許文献1】特開2010-39151号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

特許文献1では、来訪者に関する情報を事前に登録する必要があることを前提としており、来訪者に関する情報がない場合については考慮されていない。また、インターフォンを利用して在宅者だけでなく、信頼のおける外部の人、例えば、家族の協力を得て来訪者を多角的に認証・判定し、その結果に応じた機器の制御を行うことまでは想定されていない。

【0005】

そこで、本発明では、表示機能、インターフォン機能及び通信機能を有する通信端末を利用して来訪者を認証・判定し、当該認証・判定結果に応じて、通信端末の表示機能、インターフォン機能、通信機能などを制御する技術を提供することを目的とする。

例えば、本発明を表札・インターフォン機能を有するシステムに応用した場合には、従来の表札、インターフォンと同等の機能を有し、かつ、セキュリティ機能を備えた技術を提供することを目的とする。

【課題を解決するための手段】

【0006】

上記課題を解決するために、代表的な本発明の来訪者認証・判定システムの一つは、来訪者認証、表示、インターフォン、通信、の各機能を有する電子機器を備えた来訪者認証・判定システムであって、

前記電子機器は、

来訪者を感知したとき、当該来訪者の生体認証情報を収集するセンサー部と、表示機能を有する表示部と、インターフォン機能を有するインターフォン部と、外部機器との通信機能を有する通信部と、来訪者の生体情報を収集し、当該来訪者の生体認証情報をデータ化し、認証IDとして出力する生体認証部と、来訪者を判定するための来訪者判定情報をID認証として格納した記憶部と、前記認証IDの照合・判定を行う演算部、を有し、

前記演算部は、

前記生体認証部により生成した認証IDと前記記憶部に格納した来訪者の生体情報をデ

10

20

30

40

50

ータ化した認証 I D を照合・判定する生体 I D 照合・判定部と、

当該認証 I D 照合・判定部にて判定した結果に応じて、前記表示部、インターフォン部、通信部の、各機能の 1 つ以上を ON に制御する制御部と、を含むことを特徴とする。

【0007】

前記制御部は、

前記認証 I D 照合・判定部にて、照合・判定した結果、来訪者に「危険性無」と判定した場合、前記表示部の表示機能を ON、及び／又は前記インターフォン機能を ON し、来訪者に「危険性有」と判定した場合、前記表示部の表示機能を制御（OFF、）及び／又は前記インターフォン機能を制御（OFF）し、

10

前記認証 I D 照合・判定部にて、照合・判定した結果、照合・判定できず不明とした場合、前記通信部の通信機能を ON し、来訪者の認証 I D を、前記外部機器側に送信する、ことを特徴とする。

【0008】

前記認証 I D 照合・判定部にて、照合・判定した結果、照合・判定できず不明とした場合、前記通信部の通信機能を ON し、

前記制御部は、

前記来訪者の認証 I D を、前記外部機器側に送信したとき、

前記外部機器から前記認証 I D の照合・判定結果を受け、当該照合・判定結果に応じて表示部、インターフォン部、通信部の、各機能の 1 つ以上を ON に制御することを特徴とする。

20

【発明の効果】

【0009】

本発明によれば、個人情報、例えば、表札名の公開範囲を最小限に留めたり、危険性／悪意ある訪問者によるインターフォン操作を防止することができる。また、場合によっては、在宅者以外の人々が訪問者を確認することもできる。これにより、危険性／悪意ある訪問者の来訪そのものを抑止する効果も期待できる。

【図面の簡単な説明】

【0010】

【図 1】図 1 は、本発明の実施例 1 を示すものであり、インターフォン機能及び生体認証機能を有する通信端末の構成例を示すブロック図。

30

【図 2】図 2 は、本発明の生体認証部及び演算部の処理を説明するフローチャート。

【図 3】図 3 は、記憶部に予め登録した認証 I D 及び来訪者情報の一例を示すテーブル。

【図 4】図 4 は、来訪者の照合・判定処理の一例を示すフローチャート。

【図 5】図 5 は、本発明の実施例 2 を示すものであり、通信端末と外部機器（サーバ）との接続関係を示すブロック図。

【図 6】図 6 は、通信端末と外部機器（サーバ）の処理フローを示すフローチャート。

【図 7】図 7 は、受付業務を行うロボットに適用した場合における認証 I D 1911 と来訪者情報 1912 を含むテーブル構成例を示す図。

【図 8】図 8 は、店舗スタッフ業務を行うロボットに適用した場合における認証 I D と来訪者情報を含むテーブル構成例を示す図。

40

【発明を実施するための形態】

【0011】

以下、実施例について図面を用いて説明する。本例では、表札・インターフォン機能、を有する電子表札機器を備えた電子表札システムについて説明する。

【実施例 1】

【0012】

図 1 は、本発明の一実施例を示すものであり、インターフォン機能及び生体認証機能を有する電子表札機器、例えばタブレット端末などの通信端末 1 の構成を示すブロック図である。

50

【0013】

通信端末1は、建造物、例えば、ビル内の居室入口ドア近傍や家の玄関ドアや門扉、などに取り付けられる。

【0014】

また、通信端末1は、センサー11、カメラ12、入力部（タッチパネルキー）13、表示部（ディスプレイ）14、インターフォン部（含マイク、スピーカ）15、通信部（インターフェース）16、生体認証部17、演算部（CPU）18、記憶部19、を有する。

【0015】

センサー11は、人体を感知するセンサーであり、来訪者が通信端末1に近づいたとき、来訪者を感知し、来訪者の生体情報を出力する。

10

【0016】

カメラ12は、例えば、来訪者を撮影する機能を有する。

【0017】

入力部13は、例えば、主との間で情報を伝達するタッチキーである。

【0018】

表示部14は、表示部14の表示機能をONしたとき、主の氏名などを表示し、また、インターフォン部15のインターフォン機能をON状態にしたとき、インターフォンアイコン（操作ボタン）を表示する。

【0019】

インターフォン部15は、来訪者との間で会話を可能とするインターフォン機能を有する。

20

【0020】

通信部（インターフェース）16は、端末1と外部機器、例えばサーバ2との間の通信を行うものである。これにより、インターフォン部15をONしたとき、来訪者との対応者として、インターフォン部15を介して在宅者だけでなく、外部の人間とすることもできる。

【0021】

生体認証部17は、来訪者の生体情報をデータ化、例えば、認証ID化する。

生体認証部17における認証は、既存の静脈認証、指紋認証、網膜認証、顔認証、などの認証技術を利用する。

30

【0022】

演算部18は、各部の動作制御を司り、来訪者（認証ID）の照合・判定機能、及び判定結果に応じた処理を実行（制御）する機能を有する。演算部18は、内部に格納されたプログラムに従って各部の動作を制御し、また、上述した各機能を実行する。

【0023】

記憶部19（データベース191）は、来訪者の認証IDや来訪者情報を記憶する。認証IDや来訪者情報については後述する。記憶部19への各情報登録・更新は、本システムの提供元だけでなく、本システム利用者によっても可能である。記憶部19に登録されている情報は、ID化されているため、個人を特定することはできない。そのため、情報漏洩にリスクは軽減される。ここで、利用者による記憶部19のDB1911に登録された情報／データを他の利用者へ公開する場合は、登録内容に個人を特定できる内容や誹謗中傷などがなくチェックする仕組みを別途用意することも可能である。

40

【0024】

図2は、端末1における生体認証部17及び演算部18の処理を説明するフローチャートである。図2のフローチャートに基づく動作は以下のとおりである。

【0025】

ステップS171：端末1の生体認証部17は、来訪者が端末1に近づいたとき、来訪者を例えば、人体センサーにより検知し、当該来訪者の生体情報、を入手する。

【0026】

50

ステップ S 1 7 2 : 生体認証部 1 7 は、来訪者の生体情報をデータ化、つまり認証 I D 化する。これにより、本システムで使用するデータのみでは、個人を特定することができないようにすることができる。その結果、例えば、本システムで使用するデータが外部に漏洩したとしても、その被害範囲の拡大を阻止することができる。

【 0 0 2 7 】

ステップ S 1 8 1 : 演算部 1 8 は、生体認証部 1 7 の認証 I D を受け、予め記憶部 1 9 に登録した認証 I D を照合し、来訪者の判定を行う。

【 0 0 2 8 】

ステップ S 1 8 2 : ステップ S 1 8 1 による認証・判定結果を元に予め設定した動作を実行する。

10

【 0 0 2 9 】

つまり、認証・判定結果、来訪者に危険性がない、例えば、悪意がないと認証・判定した場合には、表示部 1 4 の表示機能を O N し、表示部 1 4 の画面に主の氏名などを表示し、来訪者に所在を知らせる。あるいは、インターフォン部 1 5 のインターフォン機能を O N し、表示部 1 4 の画面にインターフォンアイコン（操作ボタン）を表示し、主との会話を可能とする。これにより、必要な場合のみ、来訪者に対して表示機能やインターフォン機能を提供することができる。その結果、来訪者によっては、来訪者と接触することなく、来訪者の訪問を拒絶することができる。

【 0 0 3 0 】

来訪者に危険性がある、例えば、悪意があると認証・判定した場合には、表示機能やインターフォン機能を O F F 状態に維持し、その代わりに通信部 1 6 の通信機能を O N し、来訪者の認証 I D を外部のサーバ 2、又は警察や警備会社などに送信し、その旨を通報する。

20

【 0 0 3 1 】

外部機器 2 との通信可能とすることにより、来訪者への対応を在宅者のみでなく、外部の人間、例えば、家族や友人、警察や警備会社の警備員にて本システムにおける機能を担うことができる。

【 0 0 3 2 】

また、悪意ある訪問者により、何等かの被害を受けた場合、その来訪者の生体情報を記憶部 1 9 にデータ（I D）として登録することにより、他の利用者とのデータ共有が可能であり、また、悪意ある訪問者が、本システムを利用している別宅に来訪したとき、悪意ある訪問者であることを即座に判定することができる。このとき、警察へ通報するアクションを事前登録し、被害を未然に防止することも可能である。

30

【 0 0 3 3 】

図 3 は、記憶部 1 9 に予め登録した認証 I D 及び来訪者情報の一例を示すテーブル 1 9 1 ある。

【 0 0 3 4 】

テーブル 1 9 1 は、認証 I D 1 9 1 1、来訪者情報 1 9 1 2、を有する。

【 0 0 3 5 】

認証 I D 1 9 1 1 は、複数の認証 I D、例えば、静脈認証 1 9 1 1 1、指紋認証 1 9 1 1 2、網膜認証 1 9 1 1 3、顔認証 1 9 1 1 4、などの I D である。

40

【 0 0 3 6 】

来訪者情報 1 9 1 2 は、脅威レベル（危険有無／悪意有無） 1 9 1 2 1、種別（職業など） 1 9 1 2 2、状況（作業など） 1 9 1 2 3、などの情報である。

【 0 0 3 7 】

図 4 は、来訪者の照合・判定処理の一例を示すフローチャートである。図 4 のフローチャートに基づく動作は以下のとおりである。

【 0 0 3 8 】

ステップ S 1 8 1 1 : 演算部 1 8 は、来訪者の認証 I D と記憶部 1 9 に登録されている認証 I D を照合する。

50

【0039】

ステップS1812：演算部18は、来訪者の認証IDが記憶部19に登録されているものと一致する認証IDが有るか否かの認証ID有無を判定する。

当該ステップにて、一致する認証IDが有る場合には、ステップS1813に進み、無い（不明）場合には、ステップS182におけるステップS1823に進む。

【0040】

ステップS1813：演算部18は、ステップS1811における認証IDの脅威レベル（悪意有無）を判定する。この判定には、記憶部19の来訪者情報1912を利用する。

【0041】

ステップS1813にて、危険無（悪意無）の場合には、ステップS182におけるステップS1821／S1822に進む。

【0042】

ステップS1821／ステップS1822：演算部18は、表示部14の表示機能をONし、当該表示部の画面に氏名（表札名）を表示、及び／又はインターフォン部15のインターフォン機能をONし、当該表示部の画面にインターフォンアイコン（操作ボタン）を表示する。

【0043】

ステップS1823：演算部18は、通信機能をONし、来訪者の認証IDを、通信部16を介してサーバ2へ送信する。

【0044】

ステップS1824：演算部18は、通信機能をONし、警察や警備会社などへ通報する。

【実施例2】

【0045】

本実施例は、図1におけるインターフォン機能及び生体認証機能を有する通信端末1を、ネットワーク3を介して複数のサーバ2に接続し、通信端末1で認証IDの認証ができない場合、サーバ2側にて代行してもらうものである。図5～図6を参照し、実施例1から変更がある部分、ステップのみ、以下に示す。

【0046】

図5は、通信端末1とサーバ2との接続関係を示すブロック図である。

【0047】

サーバ2は、通信端末1と同様に生体認証及び生体ID照合・判定機能を有する。そして、係る機能を実行する演算部28、通信部26、記憶部29、などを有する。

【0048】

図6は、通信端末1とサーバ2の処理フローを示すフローチャートである。図6のフローチャートに基づく動作は以下のとおりである。

【0049】

ステップS280：サーバ2における演算部28は、通信端末1から送信されてくる来訪者の認証IDを受信する。

【0050】

ステップS281：演算部28は、来訪者の認証IDの照合・判定を行う。この照合・判定は、サーバ2自身が独自に有する認証ID及び来訪者情報を利用する。

【0051】

ステップS283：ステップS281による照合・認証結果を、通信部26を介して通信端末1に送信する。

【0052】

係る実施例によれば、通信端末1で照合・判定できない場合、サーバ2側にて代行することにより、通信端末1のステップS182における動作制御をより確実に実行することができる。

10

20

30

40

50

【0053】

以上述べた実施例によれば、従来の表札・インターフォンと同等の機能を持ち、かつセキュリティ機能を備えたシステムを提供することができる。

【0054】

また、従来の表札・インターフォンの変わりとなる電子表札機器として、例えば、既存のタブレット端末を設置することにより、タブレット画面には必要な場合のみ来訪者に対し家主の名前を表示（表札の機能）し、また、必要な場合のみ来訪者に対しインターフォンの機能を提供することができる。来訪者に対し、悪意があるか否かの判断基準はシステムにて算出する。これにより家主は、システムが悪意を持っていると判定した来訪者と接触することなく、来訪を拒絶することができる。

10

【0055】

また、タブレット端末から外部との通信可能であることから、来訪者への対応を在宅者のみでなく外部の人間が担うことも可能である。また、複数人に対応することも可能である。

来訪者の判定には、生体認証機能を使用する。ただし、生体認証機能により算出した情報は、パスワードではなくIDとして利用し、あらかじめ用意した情報と照合し来訪者を判定する。これにより、本システムで使用するデータのみでは、個人を特定することはできないようにすることで、例え、情報が漏えいしたとしてもその被害範囲が拡大しないようにすることができる。

【0056】

20

また、上記実施例では、インターフォン機能及び生体認識機能を有する通信端末としてタブレット端末を例に挙げて説明したが、これは受付機能を有するロボットに置き換えてもよい。

また、上記実施例では、来訪者に「危険性無」と判定した場合、（１）前記表示部の表示機能及び／又は前記インターフォン機能をONになるように制御しているが、（２）前記表示部にインターフォンのアイコンのみの表示を行うように制御してもよく、また、（３）夫婦別姓、ルームシェア、などに対応できるように来訪者に合わせた表札の表示を行うように制御してもよい。

また、来訪者に「危険性有」と判定した場合、（１）前記表示部の表示機能及び／又は前記インターフォン機能をOFFとなるように制御しているが、（２）前記表示部の画面に警告表示を行うように制御してもよく、また、（３）前記インターフォンのアイコンを表示し、当該インターフォンのインターフォン機能を停止状態した上で家主に「危険性有」の来訪者が来ている旨を通知するような制御を行ってもよい。

30

【実施例3】

【0057】

本実施例は、インターフォン機能を有する通信端末1として、図5に示すタブレットをロボットに置き換え、受付業務用に応用した一例である。つまり、ロボットに上述したような機能を実行する構成を備え、例えば、企業の受け付け業務をロボットで代用する場合には、記憶部19のデータに、認証ID1911に面会の予定(日時、場所、担当者)や来訪者が来たときの処理内容などを登録する。そして、来訪者の生体情報を認証ID化する。これにより、ロボットは、それら情報を必要なタイミング（特定のお客様が来訪したタイミング）で取得し、それらデータを用いた処理を実行することができる。

40

処理の例としては、来訪者を会議室へ誘導したり、打合せ予定の担当者へ連絡するなどである。

【0058】

図7は、本発明を、受付業務を行うロボットに適用した場合における認証ID1911と来訪者情報1912を含むテーブル構成例を示す図である。

認証ID1911は、認証の種類、つまり、静脈認証、指紋認証、網膜認証、顔認証、などを含み、来訪者情報1912は、脅威レベル（悪意有無）、日時、場所、担当者、などの各情報を含む。

50

【実施例 4】

【0059】

本実施例は、インターフォン機能を有する通信端末 1 として、図 5 に示すタブレットをロボットに置き換え、店舗スタッフ業務用に応用した一例である。つまり、ロボットに上述したような機能を実行する構成を備え、例えば、店舗スタッフ業務をロボットで代行する場合、更に詳しくは、アパレル、雑貨、飲食などの店舗にて、店頭立つスタッフ業務にロボットを使用する場合には、記憶部 19 に認証 ID 191 が存在するかの判定を新規顧客／リピータ、の何れかであるかの判定に利用する。

新規顧客であれば、記憶部 29 に認証 ID 191 を新規に登録し、新規顧客向けの処理動作を実行する。リピータであれば、過去の購買情報などを含めた処理動作を実行する。また、記憶部 19 の情報(購買履歴情報などをもとに特定の数値を記録することで、ポイントカードを配布することなく、ポイントカードと同様の仕組みを提供することができる。

10

【0060】

図 8 は、本発明を、店舗スタッフ業務を行うロボットに適用した場合における認証 ID と来訪者情報を含むテーブル構成例を示す図である。

認証 ID 1911 は、認証の種類、つまり、静脈認証、指紋認証、網膜認証、顔認証、などを含み、来訪者情報 1912 は、脅威レベル（悪意有無）、店舗状況、ポイント、購入履歴、などの各情報を含む。

【0061】

なお、上記の各構成、機能、処理部、処理手段等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現されてもよい。

20

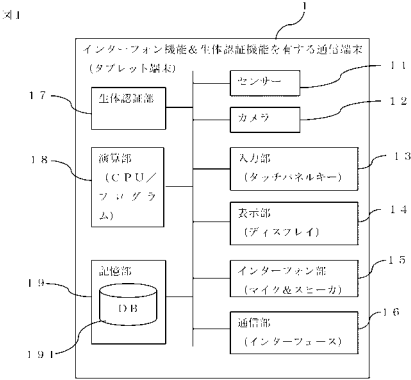
【符号の説明】

【0062】

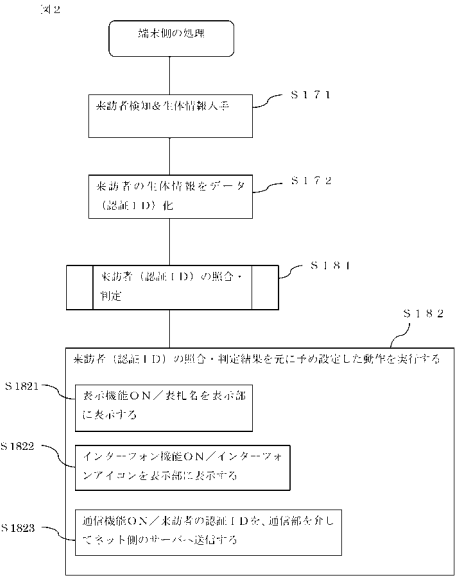
- 1 通信端末（タブレット端末／ロボット）
- 11 センサー
- 12 カメラ
- 13 入力部
- 14 表示部
- 15 インターフォン部
- 16 通信部
- 17 生体認証部
- 18 演算部
- 19 記憶部
- 2 サーバ（外部機器）
- 26 通信部
- 28 演算部
- 29 記憶部
- 3 ネットワーク

30

【図 1】



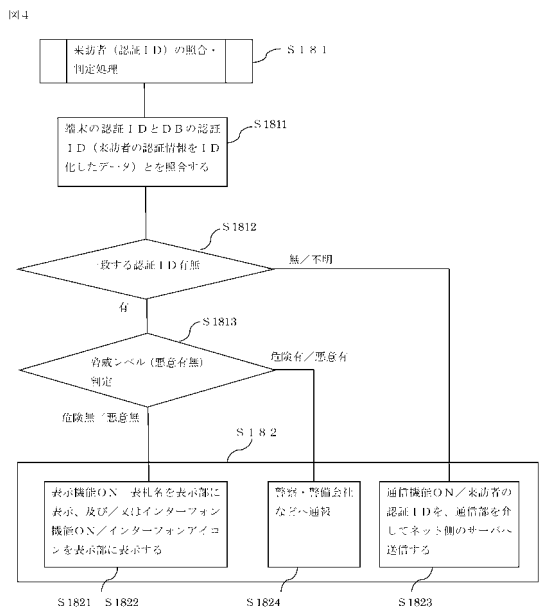
【図 2】



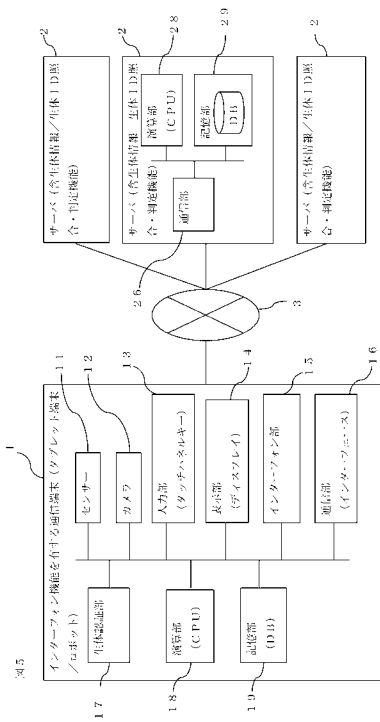
【図 3】

図3は、来訪者情報データベースの構成図である。図3は、1911、1912、1913、1914、1915、1916、1917、1918、1919、1920、1921、1922、1923の各ブロックを含む。1911は来訪者情報、1912は来訪者情報、1913は来訪者情報、1914は来訪者情報、1915は来訪者情報、1916は来訪者情報、1917は来訪者情報、1918は来訪者情報、1919は来訪者情報、1920は来訪者情報、1921は来訪者情報、1922は来訪者情報、1923は来訪者情報。

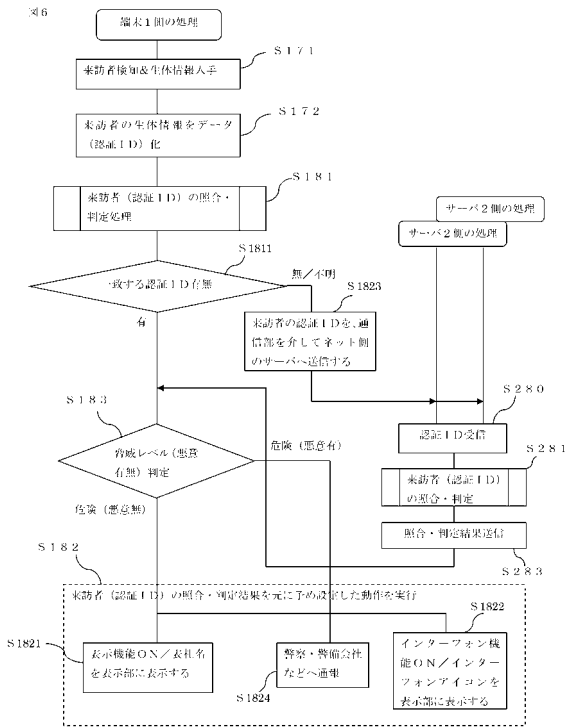
【図 4】



【図 5】



【図 6】



【図 7】

図 7

1911 認識ID				1912 来訪者情報	
静態認識証	指紋認識証	顔認識証	危険レベル (懸念有無)	日時	場所
XXXXXXXX	XXXXXX	XXXXXX	問題なし (懸念無)	2012/4/2 15:00	会議室 A
XXXXXXXX	XXXXXX	XXXXXX	問題なし (懸念無)	2012/4/2 17:00	会議室 B
333	333	333333	問題なし (懸念無)	2012/4/2 17:30	会議室 C

【図 8】

図 8

1911 認識ID				1912 来訪者情報	
静態認識証	指紋認識証	顔認識証	危険レベル (懸念有無)	実行状況	ホスト
XXXXXXXX	XXXXXX	XXXXXX	問題なし (懸念無)	2012/4/2 15:00~16:30 2012/5/3 9:00~9:30	150
XXXXXXXX	XXXXXX	XXXXXX	問題なし (懸念無)	2011/3/3 9:00~10:00 2013/8/8 10:00~12:00 2013/12/1 9:00~9:30	300