

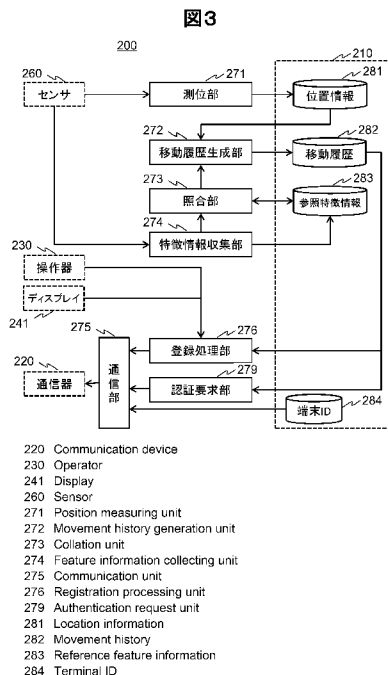


- (51) 国際特許分類:
G06F 21/31 (2013.01) G06F 21/44 (2013.01)
G06F 21/32 (2013.01)
- (21) 国際出願番号: PCT/JP2018/044998
- (22) 国際出願日: 2018年12月6日(06.12.2018)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2017-244152 2017年12月20日(20.12.2017) JP
- (71) 出願人: マクセル株式会社 (MAXELL, LTD.)
[JP/JP]; 〒6188525 京都府乙訓郡大山崎町大山崎小泉1番地 Kyoto (JP).
- (72) 発明者: 嶋田 堅一 (SHIMADA Kenichi);
〒1008280 東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内 Tokyo (JP).

- (74) 代理人: 特許業務法人 武和国際特許事務所 (THE PATENT BODY CORPORATE TAKEWA INTERNATIONAL PATENT OFFICE); 〒1050003 東京都港区西新橋3丁目13番3号 ユニゾ西新橋三丁目ビル Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: TERMINAL DEVICE, PERSONAL AUTHENTICATION SYSTEM, AND PERSONAL AUTHENTICATION METHOD

(54) 発明の名称: 端末機器、本人認証システムおよび本人認証方法



(57) Abstract: Provided is a technology having high levels of safety and convenience for personal authentication through a mobile terminal. A terminal device 200 of the present invention is provided with: a position measuring unit 271 which measures the location of the terminal device 200 at a prescribed time interval and accumulates the measured result as location information; a movement history generation unit 272 which generates a movement history by using the location information during a prescribed period and stores the movement history as movement history information; a registration processing unit 276 which transmits the movement history information to a personal authentication device for registration; and an authentication request unit 279 which performs an authentication request on the personal authentication device 310 by using the movement history information that has been transmitted by the registration processing unit 276 to the personal authentication device 310.

(57) 要約: 携帯端末を介した本人認証において、安全性が高く、さらに利便性の高い技術を提供する。本発明の端末機器200は、所定の時間間隔で端末機器200の位置を測位し、位置情報として蓄積する測位部271と、所定期間の位置情報を用いて移動履歴を生成し、移動履歴情報として記憶する移動履歴生成部272と、移動履歴情報を、本人認証装置に登録のために送信する登録処理部276と、登録処理部276が本人認証装置310に送信後の移動履歴情報を用いて、本人認証装置310に対して認証要求を行う認証要求部279と、を備える。

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 一 国際調査報告(条約第21条(3))

明 細 書

発明の名称： 端末機器、本人認証システムおよび本人認証方法
技術分野

[0001] 本発明は、本人認証技術に関する。特に、ユーザ保有の端末で収集したユーザに係わる履歴情報を用いて本人認証を行う技術に関する。

背景技術

[0002] 携帯端末で取得できる位置情報を用いた本人認証技術がある。例えば、特許文献 1 には、「ユーザの携帯通信機器から、その携帯通信機器の現在位置情報を受信し、その携帯通信機器の移動履歴に関する情報を収集する。そして、この履歴の内容に関する質問を生成し、ユーザに提示する。ユーザから受け取った回答と履歴の内容を比較し、両者間の整合性が確認された場合、本人であると決定する（要約抜粋）。」技術が開示されている。

先行技術文献

特許文献

[0003] 特許文献1：特開 2 0 1 4 - 1 4 9 8 1 1 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 に開示の技術では、端末から取得した移動履歴情報がユーザ本人のものかを確認するために、システム側が質問を作成し、ユーザが回答する方法を採用している。認証に用いるクレデンシャルが自動的に変更されるため、利便性も安全性も高い。しかし、答えの選択肢を選ぶ際にボタン操作を行う必要があり、ユーザにとって、手間がかかる。

[0005] 本発明は、上記事情に鑑みてなされたもので、携帯端末を介した本人認証において、安全性が高く、さらに利便性の高い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、本発明は、端末機器であって、所定の時間間隔

で前記端末機器の位置を測位し、位置情報として蓄積する測位部と、所定期間の前記位置情報を用いて移動履歴を生成し、移動履歴情報として記憶する移動履歴生成部と、前記移動履歴情報を、本人認証装置に登録のために送信する登録処理部と、前記登録処理部が前記本人認証装置に送信後の前記移動履歴情報を用いて、前記本人認証装置に対して認証要求を行う認証要求部と、を備えることを特徴とする端末機器を提供する。

[0007] また、本発明は、端末機器と、認証インタフェース装置と、本人認証装置とを備える本人認証システムであって、前記端末機器は、所定の時間間隔で前記端末機器の位置を測位し、位置情報として蓄積する測位部と、所定期間の前記位置情報を用いて移動履歴を生成し、移動履歴情報として記憶する移動履歴生成部と、前記移動履歴情報を、前記本人認証装置に登録のために送信する登録処理部と、前記登録処理部が前記本人認証装置に送信後の前記移動履歴情報を用いて、前記認証インタフェース装置を介して前記本人認証装置に対して認証要求を行う認証要求部と、を備え、前記本人認証装置は、前記端末機器から送信された前記移動履歴情報を、保管する保管処理部と、前記端末機器から前記認証インタフェース装置を介して前記認証要求を受信した際、当該認証要求に含まれる前記移動履歴が前記保管処理部により保管されているか否かを判別することにより、認証を行い、認証結果を返す認証部と、を備えることを特徴とする本人認証システムを提供する。

[0008] 本発明は、端末機器と、認証インタフェース装置と、本人認証装置とを備える本人認証システムにおける本人認証方法であって、端末機器において移動履歴情報を記憶するとともに、前記本人認証装置に当該移動履歴情報を送信し、当該本人認証装置において認証情報として保管する初期登録ステップと、前記認証インタフェース装置を介して前記移動履歴情報を認証要求として前記本人認証装置に送信し、前記本人認証装置において前記認証情報を用いて認証を受ける認証ステップと、新たに生成した移動履歴情報を、前記認証インタフェース装置を介して前記本人認証装置に送信し、前記本人認証装置において保管されている前記認証情報を当該移動履歴情報によって置き換

える認証情報更新ステップと、を備えることを特徴とする本人認証方法を提供する。

発明の効果

[0009] 本発明によれば、携帯端末を介した本人認証において、安全性が高く、さらに利便性の高い技術を提供できる。上記した以外の課題、構成および効果は、以下の実施形態の説明により明らかにされる。

図面の簡単な説明

[0010] [図1]第一の実施形態の本人認証システムの全体構成図である。

[図2]第一の実施形態の端末機器のハードウェア構成図である。

[図3]第一の実施形態の端末機器の機能ブロック図である。

[図4] (a) および (b) は、それぞれ、第一の実施形態の本人認証装置の機能ブロック図およびハードウェア構成図であり、(c) は、第一の実施形態の店舗機器のハードウェア構成図である。

[図5] (a) は、第一の実施形態の本人認証処理のフローチャートであり、(b) は、第一の実施形態の初期登録処理を説明するための説明図である。

[図6] (a) は、第一の実施形態の店舗認証処理を、(b) は、第一の実施形態の認証情報更新処理を、それぞれ、説明するための説明図である。

[図7] (a) は、第一の実施形態の処理登録処理の、(b) は、第一の実施形態の店舗認証処理および認証情報更新処理の、それぞれフローチャートである。

[図8] (a) ～ (c) は、それぞれ、第一の実施形態の初期登録処理、店舗認証処理および認証情報更新処理の、データの流れを説明するための説明図である。

[図9] (a) ～ (d) は、それぞれ、第一の実施形態の本人認証処理を説明するための説明図である。

[図10] (a) は、第一の実施形態の端末IDの、(b) は、第一の実施形態の移動履歴の、(c) は、第一の実施形態の生体情報の、それぞれ、データ構成を説明するための説明図である。

[図11] (a) ~ (d) は、第一の実施形態の特徴情報を用いた移動履歴生成処理を説明するための説明図である。

[図12] (a) および (b) は、それぞれ、第一の実施形態の移動履歴生成処理のフローチャートおよびタイミングチャートである。

[図13] 第二の実施形態の本人認証システムの全体構成図である。

[図14] (a) および (b) は、それぞれ、第二の実施形態の本人認証装置の機能ブロックおよびハードウェア構成図である。

[図15] 第二の実施形態の認証時のデータの流れを説明するための説明図である。

[図16] (a) は、第三の実施形態の端末機器の機能ブロック図であり、(b) は、第三の実施形態の本人認証装置の機能ブロック図である。

[図17] (a) は、第三の実施形態の基準情報取得処理を、(b) は、認証処理を、それぞれ、説明するための説明図である。

[図18] 第三の実施形態の認証処理のフローチャートである。

発明を実施するための形態

[0011] 以下、図面を参照しながら本発明の実施形態について説明する。以下、本明細書において、同一機能を有するものは、特に断らない限り、同一の符号を付し、繰り返しの説明は省略する。

[0012] <<第一の実施形態>>

本発明の第一の実施形態を説明する。本実施形態の本人認証システムでは、ユーザが保持するモバイル端末やウェアラブル端末などの端末機器の情報をを用いて本人認証を行う。具体的には、所定期間、ユーザの位置情報を収集し、収集した情報から移動履歴情報（以下、単に移動履歴と呼ぶ。）を生成し、本人認証装置（サーバ）と共有する。そして、この共有する移動履歴を認証情報として認証に用いる。このとき、この移動履歴は、正当なユーザが端末機器を保持している間に取得した位置情報から生成される。また、認証情報は、所定のタイミングで、更新する。

[0013] まず、本実施形態の本人認証システム 100 の全体構成を説明する。図 1

は、本実施形態の本人認証システム１００の全体構成図である。本人認証システム１００は、端末機器２００と、プロバイダシステム３００と、を備える。

[0014] プロバイダシステム３００は、プロバイダ等が有する本人認証装置３１０と、各店舗に備えられる店舗機器３３０と、本人認証装置３１０と店舗機器３３０との間でデータ送受信を行う内部ネットワーク（Ｎ／Ｗ）３２０と、を備える。なお、その他、図示はしないが、決済サーバ等を備えていてもよい。

[0015] 図１では、店舗機器３３０は、店舗機器３３１と店舗機器３３２との２つを備える場合を例示するが、店舗機器３３０の数はこれに限定されない。また、以下、本明細書で、特に区別する必要がない場合は、各店舗機器３３１、３３２を、店舗機器３３０で代表する。

[0016] 端末機器２００と、本人認証装置３１０と、は、ネットワーク１０１で直接データを送受信できる。

[0017] [端末機器のハードウェア構成]

まず、端末機器２００について説明する。端末機器２００のハードウェア構成を図２に示す。本図に示すように、端末機器２００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）２０１と、システムバス２０２と、記憶装置２１０と、通信器２２０と、拡張Ｉ／Ｆ２２７と、操作器２３０と、ビデオプロセッサ２４０と、オーディオプロセッサ２５０と、センサ２６０とを備える。

[0018] ＣＰＵ２０１は、端末機器２００全体を制御するマイクロプロセッサユニットである。システムバス２０２はＣＰＵ２０１と端末機器２００内の各動作ブロックとの間でデータ送受信を行うためのデータ通信路である。

[0019] 記憶装置２１０は、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）２１１と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）２１２と、外部メモリインタフェース（Ｉ／Ｆ）２１３と、を備える。

[0020] ＲＯＭ２１１は、オペレーティングシステムなどの基本動作プログラムや

その他の動作プログラムが格納されるメモリである。ROM 211として、例えば、EEPROM (Electrically Erasable and Programmable Read Only Memory) やフラッシュROMのような書き換え可能なROMが用いられる。また、上記プログラムの動作設定値、本実施形態の各機能を実現するために必要な各種のプログラムやデータも記憶される。

[0021] 外部メモリ I/F 213は、メモリカードやその他のメモリ媒体を接続してデータの送受信を行うインタフェースである。

[0022] RAM 212は、基本動作プログラムやその他の動作プログラム実行時のワークエリアである。

[0023] ROM 211及びRAM 212は、CPU 201と一体構成であっても良い。

[0024] なお、ROM 211に記憶された各動作プログラムは、例えば、ネットワーク上の各配信サーバからのダウンロード処理により更新及び機能拡張することができる。

[0025] 通信器 220は、LAN (Local Area Network) 通信器 221と、電話網通信器 222と、端末間通信器 223と、を備える。

[0026] LAN通信器 221はWi-Fi (登録商標) 等による無線接続によりアクセスポイント (AP) 装置を介してネットワーク 101に接続され、ネットワーク 101上の他の装置とデータの送受信を行う。

[0027] 電話網通信器 222は移動体電話通信網の基地局との無線通信により、通話及びデータの送受信を行う。

[0028] 端末間通信器 223は、端末機器 200と、店舗機器 330との間の通信を実現するI/Fである。用いられる通信方式には、例えば、近距離無線通信 (NFC (Near Field Communication))、Bluetooth (登録商標) 等がある。NFCは、数センチからおよそ1メートル程度の極短距離で、NFCチップを搭載した機器間の双方向通信を実現する。例えば、端末機器 200に搭載される電子マネーなどの非接触I

Cチップを利用したサービスに対応する。Bluetooth（登録商標）は、数mから数十m程度の距離の情報機器間で、電波を使い簡易な情報のやりとりを実現する。

[0029] LAN通信器221と、電話網通信器222と、端末間通信器223と、は、それぞれ、符号回路や復号回路、アンテナ等を備える。また、通信器220は、赤外線通信を実現する通信器や、その他の通信器を更に備えていても良い。

[0030] 拡張I/F227は、端末機器200の機能を拡張するためのインタフェース群である。本実施形態では、映像／音声I/F、USB(Universal Serial Bus)I/F等を備える。映像／音声I/Fは、外部映像／音声出力機器からの映像信号／音声信号の入力、外部映像／音声入力機器への映像信号／音声信号の出力、等を行う。USB I/Fは、PC(Personal Computer)等の他の装置と接続してデータの送受信を行う。また、キーボードやその他のUSB機器の接続を行っても良い。

[0031] 操作器230は、端末機器200に対する操作指示の入力を受け付ける。本実施形態では、ディスプレイ241に重ねて配置したタッチパネルおよびボタンスイッチを並べた操作キーを備える。なお、そのいずれか一方のみであっても良い。また、拡張I/F227に接続したキーボード等を用いて端末機器200の操作を行っても良い。また、有線通信又は無線通信により接続された別体の機器を用いて端末機器200の操作を行っても良い。また、タッチパネル機能はディスプレイ241が備えていてもよい。

[0032] ビデオプロセッサ240は、ディスプレイ241と、画像信号プロセッサ242と、カメラ243と、を備える。

[0033] ディスプレイ241は、例えば液晶パネル等の表示デバイスであり、画像信号プロセッサ242で処理した画像データを表示し、端末機器200のユーザに提供する。画像信号プロセッサ242は図示を省略したビデオRAMを備え、ビデオRAMに入力された画像データに基づいてディスプレイ24

1が駆動される。また、画像信号プロセッサ242は、必要に応じてフォーマット変換、メニューやその他のOSD (On-Screen Display) 信号の重畳処理等を行う。カメラ243は、CCD (Charge Coupled Device) やCMOS (Complementary Metal Oxide Semiconductor) センサ等の電子デバイスを用いてレンズから入力した光を電気信号に変換することにより、周囲や対象物を画像データとして取得する撮影装置である。

[0034] オーディオプロセッサ250は、スピーカ251と、音声信号プロセッサ252と、マイク253と、を備える。スピーカ251は、音声信号プロセッサ252で処理した音声信号を端末機器200のユーザに提供する。マイク253は、ユーザの声などを音声データに変換して入力する。

[0035] センサ260は、端末機器200の状態を検出するためのセンサ群である。本実施形態では、例えば、GPS (Global Positioning System) 受信器261と、ジャイロセンサ262と、地磁気センサ263と、加速度センサ264と、照度センサ265と、近接センサ266と、生体情報センサ267と、を備える。

[0036] GPS受信器261は、GPS衛星等の測位衛星からの信号を受信し、位置情報を算出する。加速度センサ264は、端末機器200の加速度を検出する。本実施形態では、端末機器200に設定された機器座標系のx、y、z各軸方向の加速度を検出する。検出される値の単位は、重力加速度を基準とした「G」(1.0Gは約 9.8 m/s^2)である。生体情報センサ267は、例えば、脈波、心拍数等のユーザ209の生体情報を検出する。

[0037] これらのセンサ群により、端末機器200の位置、傾き、方角、動き、及び周囲の明るさ、ユーザ209の生体情報等を検出する。また、端末機器200が、気圧センサ等、圧力センサ他のセンサを更に備えていても良い。なお、上述のように、位置情報は、GPS受信器261により取得する。しかし、GPS電波が入りにくい場所等では、LAN通信器221によりWi-FiのAP装置の位置情報を用いて取得してもよいし、同様に電話網通信器

222により基地局の位置情報及び電話通信電波の伝搬遅延を用いた位置情報取得方法により取得してもよい。また、これらのセンサ群は、必ずしも全てを備えていなくてもよい。

[0038] なお、図2に示す端末機器200の構成例は、本実施形態に必須ではない構成も多数含んでいるが、これらが備えられていない構成であっても本実施形態の効果を損なうことはない。また、デジタル放送受信機能や電子マネー決済機能等、図示していない構成が更に加えられていても良い。

[0039] [端末機器の機能構成]

次に、本実施形態の端末機器200の機能構成について説明する。ここでは、本実施形態の本人認証処理に関する機能に主眼をおいて説明する。

[0040] 図3は、本実施形態の端末機器200の機能ブロック図である。本実施形態の端末機器200は、測位部271と、移動履歴生成部272と、照合部273と、特徴情報収集部274と、通信部275と、登録処理部276と、認証要求部279と、を備える。また、これらの各部が処理を実行するために用いたり、処理の結果得られるデータを格納したりする、位置情報記憶部281と、移動履歴記憶部282と、参照特徴情報記憶部283と、端末ID記憶部284と、を備える。

[0041] 測位部271は、センサ260からの信号を処理し、端末機器200の位置情報を算出する。算出した位置情報は、位置情報記憶部281に記憶する。位置情報は、例えば、センサ260からの信号を取得した時刻に対応づけて記憶される。本実施形態では、例えば、センサ260として、GPS受信器261から受信する位置情報を、そのまま位置情報記憶部281に記憶する。位置情報の記憶は、所定の時間間隔で行う。

[0042] 特徴情報収集部274は、センサ260からの信号を、ユーザ209の特徴情報として収集し、照合部273に受け渡す。また、後述する初期処理として、ユーザ209からの指示に従って、所定期間、特徴情報を収集し、照合時の参照特徴情報として、参照特徴情報記憶部283に記憶する。本実施形態では、特徴情報として、例えば、加速度センサ264が検出した加速度

から算出した情報を用いる。また、生体情報センサ 267 で検出した、脈波、心拍数等を用いてもよい。

[0043] 照合部 273 は、特徴情報収集部 274 から特徴情報を受信すると、参照特徴情報記憶部 283 と照合し、照合結果を移動履歴生成部 272 に出力する。

[0044] 移動履歴生成部 272 は、位置情報記憶部 281 に記憶された位置情報を用いて、移動履歴を生成する。移動履歴情報は、照合部 273 から照合成功を意味する結果を受信したタイミングに同期して生成する。生成の詳細は、後述する。生成した移動履歴は、移動履歴記憶部 282 に記憶される。

[0045] 通信部 275 は、通信器 220 を介した外部装置とのデータの送受信を行う。本実施形態では、所定のタイミングで、移動履歴記憶部 282 に記憶される移動履歴と、端末 ID 記憶部 284 に記憶される端末識別情報（端末 ID）との組を、認証情報として送信する。また、認証結果等の情報を外部から受信する。なお、端末 ID は、各端末機器 200 を一意に識別する識別情報であり、予め各端末機器 200 に付与される。

[0046] 本実施形態では、認証情報は、本人認証装置 310 に登録するために送信される場合と、認証のために送信される場合とがある。登録処理部 276 は、送信する認証情報が、登録のために送信される場合、その旨、通信部 275 に通知する。

[0047] 通信部 275 は、通知を受け、登録のための送信の場合、登録のための送信であることが判別可能なように、ヘッダ情報を生成し、送信データに付加する。以後、登録のために送信される認証情報を登録認証情報と呼ぶ。なお、登録処理部 276 は、送信タイミングにより、または、操作器 230 やディスプレイ 241 を介したユーザ 209 からの指示により、登録のための送信であるか否かを判別する。

[0048] なお、登録処理部 276 は、登録のための送信でない場合、すなわち、認証のための送信である場合は、通信部 275 にその旨、通知してもよいし、何も通知しなくてもよい。

[0049] 認証要求部 279 は、移動履歴記憶部 282 に記憶される移動履歴を用いて、店舗機器 330 を介して本人認証装置 310 に対して認証要求を行う。認証要求は、例えば、店舗機器 330 と、端末間通信を行うことを契機に実行される。

[0050] これらの各機能は、CPU 201 が、ROM 211 に予め保存したプログラムを、RAM 212 にロードして実行することにより実現される。また、位置情報記憶部 281 と、移動履歴記憶部 282 と、参照特徴情報記憶部 283 と、端末 ID 記憶部 284 は、例えば、ROM 211、または、外部メモリ等に設けられる。また、各機能が実行するために必要なデータ、実行中に生成される中間データ、実行の結果生成されるデータも、ROM 211、または、外部メモリ等に格納される。

[0051] [本人認証装置]

次に、本人認証装置 310 のハードウェア構成および機能ブロックを説明する。

[0052] 図 4 (a) は、本人認証装置 310 の機能ブロック図である。本図に示すように、本人認証装置 310 は、通信部 311 と、保管処理部 312 と、認証部 313 と、を備える。また、認証情報を保管する認証情報保管部 314 をさらに備える。

[0053] 図 4 (b) は、本人認証装置 310 のハードウェア構成図である。本人認証装置 310 は、CPU 321 と、メモリ 322 と、記憶装置 323 と、通信器 324 と、を備える情報処理装置である。本実施形態では、通信器 324 として、例えば、LAN 通信器 325 を備える。LAN 通信器 325 は、内部ネットワーク 320 およびネットワーク 101 を介した通信を実現する。

[0054] 通信部 311 は、通信器 324 を介した外部装置とのデータの送受信を制御する。また、本実施形態では、受信した認証情報が、登録認証情報であるか否かを判別する。判別は、受信データのヘッダ情報により行う。そして、登録認証情報と判別された場合、保管処理部 312 に受け渡す。また、その

他の場合、認証部 3 1 3 に受け渡す。

[0055] 保管処理部 3 1 2 は、各端末機器 2 0 0 から送信される、登録認証情報、すなわち、移動履歴と端末 I D との組を、認証情報として認証情報保管部 3 1 4 に保管する。

[0056] 認証部 3 1 3 は、通信部 3 1 1 を介して店舗機器 3 3 0 から認証要求を受信すると、認証を行い、要求元の店舗機器 3 3 0 に認証結果を返信する。本実施形態では、認証要求として、店舗機器 3 3 0 から、移動履歴と端末 I D との組を受信する。認証部 3 1 3 は、受信した移動履歴と端末 I D との組と、認証情報保管部 3 1 4 に保管される認証情報と照合し、認証を行う。両者が一致した場合、認証成功とし、不一致の場合、認証失敗とする。

[0057] 本人認証装置 3 1 0 の各機能は、CPU 3 2 1 が、記憶装置 3 2 3 に格納されたプログラムを、メモリ 3 2 2 にロードして実行することにより実現される。また、認証情報保管部 3 1 4 は、例えば、記憶装置 3 2 3 等に設けられる。

[0058] [店舗機器]

次に、本実施形態の店舗に備えられる店舗機器 3 3 0 について説明する。本実施形態の店舗機器 3 3 0 は、端末機器 2 0 0 から認証要求として、認証情報を受け取ると、本人認証装置 3 1 0 に送信し、認証を受ける。店舗機器 3 3 0 は、図 4 (c) に示すように、CPU 3 4 1 と、メモリ 3 4 2 と、記憶装置 3 4 3 と、通信器 3 4 4 とを備える情報処理装置で構成される。通信器 3 4 4 は、LAN 通信器 3 4 5 と、端末間通信器 3 4 6 と、を備える。

[0059] LAN 通信器 3 4 0 は、本人認証装置 3 1 0 との、内部ネットワーク 3 2 0 を介した通信を実現する。また、端末間通信器 3 4 6 は、端末機器 2 0 0 との間のデータの送受信を実現する。

[0060] [本人認証処理]

次に、本実施形態の本人認証処理の流れを説明する。図 5 (a) は、本実施形態の本人認証処理の流れの概略図である。

[0061] 本図に示すように、本人認証処理では、初期登録処理を行い（ステップ S

1001)、その後、店舗等で店舗機器330を介して店舗認証処理(ステップS1002)として、認証を受ける。店舗認証処理において、認証が成功した場合(ステップS1003; Yes)、認証情報を更新する認証情報更新処理を行う(ステップS1004)。なお、ステップS1003で認証が失敗した場合は、例えば、端末機器200は、ユーザ209にその旨通知し、処理を終了する。以下、各処理について、詳細を説明する。

[0062] 初期登録処理は、図5(b)に示すように、端末機器200から認証情報を本人認証装置310に登録する処理である。初期登録処理は、認証処理を行う前に実行される。本図に示すように、まず、端末機器200において、移動履歴生成部272が、位置情報記憶部281に記憶される位置情報4aから移動履歴5aを生成する。そして、登録処理部276の指示により、生成した移動履歴5aと端末ID1aとの組を、登録認証情報として、ネットワーク101を介して、本人認証装置310に送信する。

[0063] 登録認証情報を受信した本人認証装置310では、保管処理部312が、認証情報保管部314に、移動履歴5aと端末ID1aとを対応づけて、認証情報として登録する。

[0064] なお、初期登録完了後、ユーザ209が、指示を中止の指示をしない限り、測位部271は、位置情報の収集を継続する。

[0065] 店舗認証処理は、図6(a)に示すように、ユーザ209が、店舗等に備えられる店舗機器330(331)において、認証を受ける処理である。ユーザ209は、事前に初期登録処理を行った端末機器200を店舗機器331等にかざすことにより、認証を要求する。ここでは、認証要求部279は、移動履歴5aと、端末ID1aとを、認証情報として店舗機器331に送信する。送信は、例えば、近距離無線通信等の端末間通信を用いて行う。

[0066] 店舗機器331の通信器344は、認証情報を受信すると、内部ネットワーク320を介して本人認証装置310に転送する。そして、本人認証装置310では、認証部313が、認証情報保管部314に登録されている認証情報を用いて認証を行い、結果を店舗機器331に返す。また、店舗機器3

31は、認証結果を送信元の端末機器200に返信する。

[0067] 認証情報更新処理は、店舗機器331を介した認証が成功した場合、本人認証装置310内に保管される認証情報を更新する処理である。ここでは、それまでに収集した位置情報4bを用いて、新たな移動履歴5bを生成する。そして、端末ID1aとともに、店舗機器331を介して、新たな登録認証情報として、本人認証装置310に送信し、認証情報を更新する。

[0068] 図6(b)に示すように、まず、端末機器200において、移動履歴生成部272が、位置情報記憶部281に記憶される位置情報4bから移動履歴5bを生成する。そして、登録処理部276の指示により、生成した移動履歴5bと端末ID1aとの組を、新たな登録認証情報として、店舗機器331に送信する。送信は、例えば、端末間通信により行う。

[0069] なお、登録処理部276は、このように、認証成功後、同じ店舗機器330を介して、新たな移動履歴5bを送信する場合、登録のための送信と判断し、通信部275に通知する。

[0070] 店舗機器331は、受信した新たな登録認証情報を、内部ネットワーク320を介して本人認証装置310に送信する。

[0071] 登録認証情報を受信した本人認証装置310では、保管処理部312が、認証情報保管部314に、移動履歴5bと端末ID1aとを対応づけて、認証情報として登録することにより、認証情報を更新する。保管処理部312は、例えば、同じ端末ID1aに対応づけて登録されている認証情報を抽出し、新たに送信された認証情報で、抽出した認証情報を置き換える。

[0072] 初期登録処理の処理フローを、図7(a)に示す。

[0073] 測位部271は、所定期間、位置情報4aを収集し(ステップS1101)、位置情報記憶部281に記憶する。

[0074] そして、移動履歴生成部272は、生成した位置情報4aから移動履歴5aを生成し(ステップS1102)、移動履歴記憶部282に記憶する。

[0075] ユーザ209からの指示に従って、登録処理部276は、通信部275に、移動履歴5aを、端末ID1aとともに、登録認証情報として、本人認証

装置 310 へ送信させる（ステップ S1103）。このとき、通信部 275 は、送信データに、登録認証情報であることを示すヘッダ情報を付加する。

[0076] 本人認証装置 310 では、保管処理部 312 が、受信した登録認証情報（移動履歴 5a および端末 ID 1a）を、認証情報保管部 314 に格納する（ステップ S1201）。

[0077] 店舗認証処理と、認証情報更新処理との、処理フローを図 7（b）に示す。

[0078] 上述のように、測位部 271 は、位置情報 4b の収集を継続する（ステップ S1301）。

[0079] 位置情報 4b の収集とは独立し、ユーザ 209 が店舗に到着すると、認証要求部 279 は、端末機器 200 から、店舗機器 330 へ、認証情報（移動履歴 5a および端末 ID 1a）を、店舗機器 330 へ送信する（ステップ S1302）。ここで、送信される移動履歴 5a は、初期登録時に、移動履歴記憶部 282 に記憶されているデータである。また、送信は、例えば、端末間通信器 223 を用いて行う。

[0080] 店舗機器 330 では、端末間通信器 346 を介して、認証情報（移動履歴 5a および端末 ID 1a）を受け取り、LAN 通信器 345 を介して、本人認証装置 310 へ送信する（ステップ S1401）。店舗機器 330 から本人認証装置 310 への送信は、例えば、内部ネットワーク 320 を介して行われる。

[0081] 店舗機器 330 から認証情報（移動履歴 5a および端末 ID 1a）を受け取ると（ステップ S1501）、本人認証装置 310 では、認証部 313 が、認証情報保管部 314 に保管されている認証情報と照合し、認証を行う（ステップ S1502）。

[0082] そして、通信部 311 を介して、認証結果を店舗機器 330 に送信する（ステップ S1503）。送信される認証結果は、認証成功または認証失敗のいずれかである。

[0083] 認証結果を受信すると、店舗機器 330 では、認証結果を端末機器に送信

する（ステップS 1 4 0 2）。

[0084] 端末機器 2 0 0 は、認証結果を受信する（ステップS 1 3 0 3）。ここで、認証成功であれば、例えば、決済処理等に移行する。一方、認証失敗であれば、その旨をユーザに通知する。ユーザへの通知は、例えば、メッセージをディスプレイ 2 4 1 に表示するなどにより行う。

[0085] 次に、端末機器 2 0 0 では、ステップS 1 3 0 3 で受信した結果が、認証成功の場合、移動履歴生成部 2 7 2 は、その時点までに収集された位置情報 4 b を用いて、移動履歴 5 b を生成する（ステップS 1 3 0 4）。そして、新たに生成した移動履歴 5 b を、移動履歴記憶部 2 8 2 に記憶するとともに、店舗機器 3 3 0 へ送信する（ステップS 1 3 0 5）。移動履歴 5 b は、端末 I D 1 a とともに、新たな登録認証情報として店舗機器 3 3 0 へ送信される。送信は、端末間通信器 2 2 3、2 4 6 を介して行われる。

[0086] 店舗機器 3 3 0 では、受信した新たな登録認証情報（移動履歴 5 b および端末 I D 1 a）を、本人認証装置 3 1 0 へ送信する（ステップS 1 4 0 4）。

[0087] 本人認証装置 3 1 0 では、保管処理部 3 1 2 が、認証情報保管部 3 1 4 に保管されている認証情報を、新たに受信した登録認証情報で更新する（ステップS 1 5 0 4）。このとき、保管処理部 3 1 2 は、同じ端末 I D 1 a を有する認証情報を抽出し、新たに送信された認証情報に置き換える（上書きする）。

[0088] その後、端末機器 2 0 0 は、ステップS 1 3 0 1 へ戻り、位置情報の収集を継続する。

[0089] 上記の初期登録処理と、店舗認証処理と、認証情報更新処理との、データの流れを、図 8（a）～図 8（c）に示す。

[0090] 図 8（a）に示すように、初期登録処理では、登録認証情報（移動履歴 5 a および端末 I D 1 a）が、直接、本人認証装置 3 1 0 に送信される。

[0091] 初期登録処理以降の処理、すなわち、店舗認証処理および認証情報更新処理では、図 8（b）および図 8（c）に示すように、認証情報（移動履歴 5

aおよび端末ID1a)、または、登録認証情報(移動履歴5bおよび端末ID1a)が、店舗機器330を介して、本人認証装置310に送信される。

- [0092] 本実施形態の本人認証処理を、ユーザ209の動きに沿って、図9(a)～図9(d)を用いて説明する。各店舗が、店舗機器331、332、333、334を備えるものとする。
- [0093] まず、ユーザ209は、図9(a)に示すように、店舗等で本実施形態の本人認証処理を行う前に、初期登録処理を行う。初期登録処理は、例えば、ユーザ209の自宅等で行われる。
- [0094] 初期登録処理を終えると、ユーザ209は、図9(b)に示すように、初期登録処理を行った端末機器200を携帯し、店舗に向かう。そして、端末機器200を、店舗機器331にかざすなどする。これにより、端末機器200は、自身に記憶される移動履歴5aと、端末ID1aとを、認証情報として店舗機器331に送信し、認証を要求する。
- [0095] なお、図9(b)に示すように、ユーザ209は、認証を受ける店舗に到る間も、位置情報の収集を継続する。
- [0096] 店舗機器331は、認証情報を本人認証装置310に送信し、認証を受ける。認証に成功すると、端末機器200は、図9(c)に示すように、先に移動履歴を生成後に蓄積した位置情報から、新たな移動履歴5bを生成する。そして、新たな移動履歴5bを自身の移動履歴記憶部282に記憶するとともに、端末ID1aとともに、登録認証情報として、店舗機器331に送信する。
- [0097] 店舗機器331は、新たな登録認証情報(移動履歴5bおよび端末ID1a)を、本人認証装置310に転送する。そして、本人認証装置310では、端末ID1aに対応づけて登録されている認証情報を更新する。
- [0098] その後、ユーザ209は、別の店舗に行った場合、その店舗の店舗機器332において、図9(d)に示すように、新たに移動履歴記憶部282に記憶された移動履歴5bを用いて、認証要求、認証情報の更新等を行う。

[0099] なお、店舗認証処理の前に、認証要求部 279 は、ユーザ 209 の正当性を確認する処理を行ってもよい。すなわち、端末機器 200 が、本人確認部をさらに備え、本人確認部において、ユーザ 209 が予め登録されたユーザ 209 本人であるか否かを確認し、本人と確認された後、店舗認証処理を行う。

[0100] この場合の本人確認部による本人確認は、例えば、指紋等の生体情報を活用してもよい。また、パスワード等、知識情報を活用してもよい。

[0101] また、上記例では、端末機器 200 は、認証結果を受信後に移動履歴を生成するよう記載したが、移動履歴生成のタイミングは、これに限定されない。移動履歴の生成は、認証処理とは、独立して行ってもよい。例えば、後述するよう、位置情報を収集する毎に、その正当性を判別し、正当であれば、移動情報として蓄積するよう構成してもよい。

[0102] この場合、認証情報として、本人認証装置 310 へ登録済みの移動履歴と、新たに生成し、次に登録予定の移動履歴（更新用移動履歴）とは、区別可能な態様で、移動履歴記憶部 282 に記憶する。

[0103] [データ構成]

ここで、端末機器 200 から本人認証装置 310、店舗機器 330 に送信されるデータの構成を説明する。

[0104] 端末 ID 1a のデータ構成例を図 10（a）に示す。本図に示すように、端末 ID 1a は、端末の型式を特定する型名情報 411 と、シリアル番号 412 と、を備える。なお、端末 ID 1a は、これに限定されない。各端末機器 200 を、一意に特定可能な情報であればよい。また、端末 ID 1a は、例えば、ヘッダ情報として送信データに挿入されてもよい。

[0105] 移動履歴 5a のデータ構成例を図 10（b）に示す。移動履歴 5a は、例えば、所定期間に測位された位置情報の時系列データとする。すなわち、移動履歴 5a は、所定数の位置情報を備える。本図に示すように、移動履歴 5a は、各位置情報について、それぞれ、位置情報を特定する番号 421 と、当該位置情報を取得した日時 422 と、位置情報 423 と、を備える。

[0106] なお、移動履歴 5 a は、これに限定されない。例えば、各位置情報のハッシュ値を計算し、そのハッシュ値の時系列データであってもよい。また、プライバシー保護の観点から、所定のルールのもと、測位された位置情報の遷移の順番を並び替えて移動履歴としてもよい。

[0107] [移動履歴生成処理]

ここで、本実施形態の移動履歴生成処理を説明する。本実施形態では、測位部 2 7 1 が所定期間収集した位置情報から、移動履歴生成部 2 7 2 が、移動履歴を生成する。このとき、本実施形態では、端末機器 2 0 0 の正当なユーザ 2 0 9 が、当該端末機器 2 0 0 を所持している間に収集された位置情報のみを、移動履歴生成に採用する。

[0108] 本実施形態では、正当なユーザ 2 0 9 であるか否かを、予め登録された、ユーザ 2 0 9 の特徴情報を用いて判別する。本実施形態では、特徴情報として、例えば、ユーザの歩調周波数、歩幅、歩行速度等、歩行に関する情報を用いる。これらの情報は、例えば、加速度センサ 2 6 4 で取得した、所定期間の加速度情報から算出する。

[0109] 歩調は、ユーザ 2 0 9 の歩行時の加速度波形の変化から推定する。また、歩幅は、推定した歩調と測位部 2 7 1 が取得した位置情報とを組み合わせで推定する。

[0110] 本実施形態の、特徴情報を用いた移動履歴生成処理の概略を図 1 1 (a) ~ 図 1 1 (c) を用いて説明する。

[0111] 本実施形態では、図 1 1 (a) に示すように、まず、初期処理として、特徴情報収集部 2 7 4 が、予め定めた特徴情報を収集し、照合時の参照特徴情報 5 0 a として、参照特徴情報記憶部 2 8 3 に登録する。

[0112] ここで、登録される参照特徴情報 5 0 a のデータ構成を、図 1 0 (c) に示す。本図に示すように、参照特徴情報 5 0 a は、例えば、歩調周波数 4 3 1 と、歩幅 4 3 2 と、歩行速度 4 3 3 と、を備える。なお、参照特徴情報 5 0 a は、例えば、波形データそのものであってもよい。

[0113] 参照特徴情報 5 0 a を登録後、移動履歴生成部 2 7 2 は、正当なユーザ 2

０９が所持している間に取得された位置情報を用いて移動履歴を生成する。

[0114] 図１１（ｂ）、図１１（ｃ）に示すように、特徴情報収集部２７４は、所定の時間間隔で、特徴情報を取得する。そして、照合部２７３は、取得した特徴情報を、参照特徴情報記憶部２８３に記憶される参照特徴情報５０ａと照合し、整合性の有無を判別する。

[0115] すなわち、整合性があれば、正当なユーザ２０９がこの端末機器２００を保持していると判別し、整合性が無ければ、正当ではないユーザ２０８がこの端末機器２００を保持していると判別する。

[0116] 移動履歴生成部２７２は、照合部２７３の照合結果を用いて、移動履歴を算出する。

[0117] 以下、本実施形態の移動履歴生成処理の流れを説明する。図１２（ａ）は、本実施形態の移動履歴生成処理の処理フローである。本処理は、所定の時間間隔 Δt で実行される。なお、この間、測位部２７１は、 Δt より短い時間間隔で、位置情報を収集し、位置情報記憶部２８１に収集時刻に対応づけて、記憶する。

[0118] まず、特徴情報収集部２７４は、特徴情報を収集する（ステップＳ１６０１）。そして、照合部２７３は、収集した特徴情報と、参照特徴情報記憶部２８３に格納される参照特徴情報５０ａとを照合する（ステップＳ１６０２）。

[0119] 収集した特徴情報と参照特徴情報５０ａとが略一致し、整合性が有る場合、照合部２７３は、正当なユーザ２０９が所持していると判別する。そして、前回の照合結果と比較し、照合結果が変化したか否かを判別する（ステップＳ１６０３）。前回の照合結果から変化した場合、移動履歴生成部２７２に通知する（ステップＳ１６０４）。

[0120] 照合結果の変化の通知を受け取ると、移動履歴生成部２７２は、移動履歴の生成、非生成の状態を反転させ（ステップＳ１６０５）、今回の照合結果を、記憶し、処理を終了する。すなわち、移動履歴を生成していれば、移動履歴の生成を停止し、移動履歴の生成を停止している状態であれば、移動履

歴の生成を開始する。

[0121] このように、本実施形態では、移動履歴生成部 272 は、一度、正当なユーザ 209 が所持していると判別された場合は、次に、正当なユーザ 209 が所持していないと判別されるまでは、移動履歴生成を継続する。また、一旦、正当なユーザ 209 が所持していないと判別された場合は、次に、正当なユーザ 209 が所持していると判別されるまでは、移動履歴の生成を停止する。すなわち、上記ステップ S1605 で説明したように、照合結果の反転に応じて、移動履歴の生成、非生成の状態を反転させる。

[0122] このような、上記の移動履歴の生成、非生成状態の反転を、具体的なタイミングチャートで説明する。図 12 (b) は、照合部 273 による照合タイミング（照合実施、照合不実施）と、照合結果（一致、不一致）と、移動履歴生成、非生成状態の変化の様子を示すタイミングチャートである。

[0123] 上述のように、照合部 273 は、所定の時間間隔 Δt で、取得した特徴情報と、参照用特徴情報との照合を実施する。そして、照合結果に変化があった場合、移動履歴生成部 272 に通知する。

[0124] 図 12 (b) の例では、1 回目および 2 回目の照合結果は、一致を示し、それぞれ、前回の照合結果から変化はない。このため、照合部 273 は、照合結果を移動履歴生成部 272 に通知しない。移動履歴生成部 272 は、通知がないため、そのまま、その状態を継続する。例えば、移動履歴を生成している場合は、そのまま生成を続ける。一方、移動履歴の生成を停止している場合は、そのまま停止状態を継続する。

[0125] ここで、3 回目の照合時、照合結果が不一致を示す。この場合、一致である 2 回目の照合結果から、照合結果が変化したため、照合部 273 は、移動履歴生成部 272 に通知する。移動履歴生成部 272 は、通知を受け、状態を反転させる。すなわち、この場合は、今まで移動履歴を生成していたところ、移動履歴の生成を停止する。

[0126] 4 回目の照合時は、照合結果が一致を示す。この場合、不一致である 3 回目の照合結果から、照合結果が変化したため、照合部 273 は、移動履歴生

成部 272 に通知する。移動履歴生成部 272 は、通知を受け、状態を判定させる。すなわち、この場合は、今まで移動履歴の生成を停止していたところ、移動履歴の生成を開始する。

[0127] 図 12 (b) の例では、3 回目の照合の直前までは、正当なユーザ 209 が保持しているものと判別され、3 回目の照合時から 4 回目の照合の直前までは、正当なユーザ 209 に所持されていないものと判別される。

[0128] 本実施形態の移動履歴生成部 272 は、このように、正当なユーザ 209 が所持していると判別された期間のみ、位置情報から移動履歴を生成する。このため、正当なユーザ 209 である本人による移動履歴を高い精度で収集できる。

[0129] なお、上記実施形態では、特徴情報として、加速度センサ 264 の出力から算出される情報を用いたが、特徴情報は、これに限定されない。例えば、端末機器 200 が、腕時計型機器である場合、図 11 (d) に示すように、例えば、脈波信号であってもよい。脈波信号は、例えば、生体情報センサ 267 として、脈波センサを備え、この脈波センサで取得する。

[0130] 以上説明したように、本実施形態によれば、位置情報から生成された移動履歴であって、ユーザ 209 が予め登録した移動履歴そのものを、ユーザ 209 の本人認証に用いる。このため、端末保持者の固有情報を用いて、本人認証を行うことができる。また、質問を生成したり、質問に答えたりといった処理がないため、本人認証装置 310 側の負担も少なく、端末機器 200 を操作するユーザ 209 の負担や手間も少ない。

[0131] また、この移動履歴は、端末機器 200 の識別情報（端末 ID）に対応づけて、本人認証装置 310 に登録される。このため、例えば、移動履歴情報のみがコピーされ、他の端末から送信されたとしても、認証は成功しない。このため、安全性が高い。

[0132] また、移動履歴は、端末機器 200 を、正当なユーザ 209 が所持していると判断された期間に収集された位置情報を用いて生成される。従って、本人認証に用いる移動履歴の信頼性が高い。

- [0133] また、移動履歴の生成を継続的に行い、所定のタイミングで、本人認証装置 310 に認証情報として登録される移動履歴を更新する。このため、認証情報の漏えいに強いシステムを提供できる。
- [0134] また、上記実施形態では、特に、この認証情報の更新を、店舗機器 330 において、認証後に行う。従って、更新時のデータの送受信は、端末間通信で行われる。一般のネットワークを介した送受信に比べ、端末間通信は、安全性が高い。このような安全性の高い通信を用いて、認証情報の更新を行うため、システム全体としての安全性も高い。
- [0135] このように、本実施形態では、本人である確度の高い位置情報から生成された移動履歴を用いて、本人認証を行う。また、その移動履歴は、事前に本人認証装置 310 に、端末機器 200 を特定する情報とともに登録しておく。さらに、所定のタイミングで認証情報を更新する。これらにより、本実施形態によれば、安全性と利便性とを両立させたシステムを実現できる。
- [0136] なお、本実施形態では、移動履歴の更新を、店舗で本人認証を行った後、店舗機器 330 を用いて行うよう構成されているが、これに限定されない。例えば、所定のタイミングで、ネットワーク 101 を介して、本人認証装置 310 に認証情報を送信し、更新するよう構成してもよい。所定のタイミングは、例えば、予め定めた時間間隔や、所定量の移動履歴が生成される毎、等とする。この場合、送信時は、暗号化するなど、所定のセキュリティ対策を施す。
- [0137] また、移動履歴は、正当なユーザ 209 が保持している間に得られた位置情報（正当な位置情報）が、所定量蓄積される毎に生成してもよい。この場合、最新の移動履歴のみ、更新用移動履歴として記憶しておいてもよい。
- [0138] また、上述のように、店舗機器 330 と端末間通信が可能な時に、不定期に移動履歴を生成する場合、前回の移動履歴生成時に用いた位置情報も含めて、所定量の正当な位置情報を確保してもよい。例えば、前回の移動履歴生成時以降の期間が短く、十分な量の正当な位置情報が蓄積されていない場合などである。また、十分な量の正当な位置情報が蓄積されていない場合は

、新たな移動履歴を生成せず、本人認証装置 310 に保管される認証情報内の移動履歴を更新しなくてもよい。

[0139] また、上記実施形態では、認証情報として、移動履歴とともに、端末 ID を送信し、端末 ID 1a も、本人認証装置 310 で保管しているが、これに限定されない。本人認証装置 310 の認証情報保管部 314 では、移動履歴のみを保管してもよい。この場合は、認証部 313 は、送信元の端末機器 200 によらず、送信された移動履歴が、認証情報保管部 314 に保管されていれば、認証成功とする。

[0140] <<第二の実施形態>>

次に、本発明の第二の実施形態を説明する。第一の実施形態は、各店舗とは独立して、本人認証装置を備える。これに対し、本実施形態では、各店舗、あるいは、店舗グループ毎に、本人認証装置を備える。そして、本人認証に用いる認証情報を、複数の本人認証装置間で分散共有する。

[0141] 以下、本実施形態の本人認証システム 102 について、第一の実施形態と異なる構成に主眼をおいて説明する。

[0142] 本実施形態の本人認証システム 102 の全体構成を図 13 に示す。本実施形態の本人認証システム 102 は、端末機器 200 と、プロバイダシステム 302 と、を備える。そして、プロバイダシステム 302 は、店舗毎に配置される本人認証装置 350 (351、352、353) を備える。各本人認証装置 350 間は、内部ネットワーク 320 で接続される。なお、各本人認証装置 351、352、353 を特に区別する必要がない場合は、本人認証装置 350 で代表する。

[0143] 本実施形態の端末機器 200 は、基本的に第一の実施形態の端末機器 200 と同様の構成を有するため、ここでは、説明を省略する。

[0144] 図 14 (a) は、本実施形態の本人認証装置 350 の機能ブロック図である。また、図 14 (b) は、本実施形態の本人認証装置 350 のハードウェア構成図である。

[0145] 図 14 (b) に示すように、本実施形態の本人認証装置 350 は、第一の

実施形態の本人認証装置 310 の構成に加え、端末間通信器 326 を備える。端末間通信器 326 は、端末機器 200 が備える同名の装置と同様の構成を有する。本実施形態では、店舗において、端末機器 200 とデータの送受信を行うために用いられる。

[0146] また、本実施形態の本人認証装置 350 は、図 14 (a) に示すように、第一の実施形態と同様の機能構成に加え、共有処理部 315 を備える。

[0147] 本実施形態では、上述のように、本人認証装置 350 を複数備える。そして、全ての本人認証装置 350 間で、認証情報を共有する。また、本実施形態では、1 つの認証要求に対する認証を、複数の本人認証装置 350 で行う。そして、所定割合以上、例えば、半数以上の本人認証装置 350 で認証成功と判別された場合、システム全体として認証成功と判断する。

[0148] これを実現するため、共有処理部 315 は、通信部 311 が、受信した認証情報が登録認証情報であるか否かを判別した後、その送信元を判別する。ここでは、送信元が、端末機器 200 であるか、他の本人認証装置 350 であるかを判別する。送信元が端末機器 200 であるか、他の本人認証装置 350 であるかは、例えば、送受信データのヘッダ情報等により判別する。

[0149] そして、受信した認証情報または登録認証情報の送信元が端末機器 200 である場合、保管処理部 312 または認証部 313 に受け渡すだけでなく、他の全ての本人認証装置 350 にも、受信した認証情報または登録認証情報を送信するよう通信部 311 に指示を行う。一方、受信した認証情報または登録認証情報の送信元が他の本人認証装置 350 である場合は、第一の実施形態同様、登録認証情報であるか否かの判別結果に応じて、保管処理部 312 または認証部 313 に受け渡す。

[0150] さらに、認証情報を他の本人認証装置 350 から受け取った場合、共有処理部 315 は、認証部 313 に認証させるとともに、通信部 311 に、認証結果を送信元の本人認証装置 350 に送信させる。

[0151] また、通信部 311 を介して、他の本人認証装置 350 から認証結果を受け取ると、自装置の認証部 313 の認証結果を加え、半数以上の本人認証装

置 3 5 0 で認証成功であるか否かを判別する。そして、半数以上で認証成功であれば、認証成功とし、通信部 3 1 1 から送信元の端末機器 2 0 0 に送信させる。一方、認証成功との認証結果が半数より少ない場合は、認証失敗とし、通信部 3 1 1 から送信元の端末機器 2 0 0 に送信させる。

[0152] 以下、本実施形態の本人認証処理の流れを説明する。

[0153] なお、本実施形態においても、第一の実施形態同様、まず、端末機器 2 0 0 は、本人認証装置 3 5 0 に対し、認証情報を登録する初期登録処理を行う。初期登録処理は、第一の実施形態同様、ネットワーク 1 0 1 を介して、いずれかの本人認証装置 3 5 0 に対して登録認証情報を送信することにより行う。

[0154] このとき、登録認証情報を受信した本人認証装置 3 5 0 は、受信した認証情報（移動履歴 5 a および端末 I D 1 a）を、自身の認証情報保管部 3 1 4 に保管するだけでなく、他の本人認証装置 3 5 0 へ送信する。そして、他の本人認証装置 3 5 0 においても、受信した登録認証情報を、認証情報保管部 3 1 4 に保管する。

[0155] これにより、当該端末機器 2 0 0 の登録認証情報（移動履歴 5 a および端末 I D 1 a）が、全ての本人認証装置 3 5 0 間で共有される。

[0156] 図 1 5 を用いて、本実施形態の認証時のデータの流れを説明する。本図に示すように、端末機器 2 0 0 を保持したユーザ 2 0 9 が、特定の店舗に行き、本人認証装置 3 5 2 に対して認証を要求した場合、すなわち、端末機器 2 0 0 から認証要求を受けた場合、本人認証装置 3 5 2 は、自装置内で認証を行う。

[0157] また、本人認証装置 3 5 2 は、内部ネットワーク 3 2 0 を介して、認証情報（移動履歴 5 a および端末 I D 1 a）を、他の本人認証装置 3 5 1、3 5 3 に送信する。他の本人認証装置 3 5 1、3 5 3 では、それぞれ、認証を行い、認証結果を、内部ネットワーク 3 2 0 を介して、送信元の本人認証装置 3 5 2 に返信する。

[0158] 本人認証装置 3 5 2 では、自身の認証結果と、他の本人認証装置 3 5 1、

３５３から受信した認証結果とを用い、最終的な認証結果を決定し、要求元の端末機器２００に返信する。

[0159] なお、本実施形態では、初期登録処理を、本人認証装置３５０を有する特定の店舗で、端末間通信を用いて行ってもよい。このように構成することで、初期登録処理時の認証情報が端末間通信で送受信される。これにより、さらに安全性が高くなる。

[0160] 本実施形態によれば、第一の実施形態と同様の構成を有する本人認証装置３５０を、複数有する。このため、本実施形態によれば、第一の実施形態と同様の効果が得られる。さらに、本実施形態では、本人認証装置３５０を複数備え、認証情報を共有する。これにより、認証時に複数装置の合意形成を図り、相互検証を行う。従って、信頼性が向上する。

[0161] なお、本実施形態では、半数以上の本人認証装置３５０が認証成功であった場合、認証成功と判別している。しかしながら、認証成功と判別する際の、認証に成功した本人認証装置３５０の割合は、これに限定されず、自由に設定可能である。例えば、全ての本人認証装置３５０で認証成功の場合のみ、認証成功と判別するよう構成してもよい。

[0162] また、上記実施形態では、本人認証装置３５０が、店舗毎に配置される場合を例にあげて説明したが、本構成に限定されない。本人認証装置３５０は、例えば、いくつかの店舗グループ毎に配置されてもよい。

[0163] また、本実施形態においても、第一の実施形態の各種の変形例が適用可能である。

[0164] <<第三の実施形態>>

次に、本発明の第三の実施形態を説明する。本実施形態では、移動履歴の正当性を検証するために、第三者の位置情報を用いる。

[0165] 本実施形態では、第三者の位置情報として、例えば、携帯電話網の基地局１０５の位置情報を用いる。以下、本実施形態について、第一の実施形態と異なる構成に主眼をおいて説明する。

[0166] 本実施形態の本人認証システム１００の全体構成は、第一の実施形態と基

本的に同じである。また、各構成要素のハードウェア構成、機能ブロックも、基本的に第一の実施形態と同じである。ただし、端末機器 200 は、第三者の位置情報を取得する構成を備える。また、本人認証装置 310 は、第三者の位置情報の正当性を判別する構成を備える。

[0167] 図 16 (a) は、本実施形態の端末機器 203 の機能ブロックである。本図に示すように、本実施形態の端末機器 203 は、第一の実施形態の構成に加え、基準情報取得部 277 を備える。基準情報取得部 277 は、測位部 271 が位置情報を取得し、位置情報記憶部 281 に格納するタイミングで、基準位置情報を取得する。そして、測位部 271 が同じタイミングで取得した位置情報に対応づけて、基準情報として、基準情報記憶部 285 に記憶する。

[0168] 基準情報取得部 277 が取得する基準位置情報は、本実施形態では、例えば、上述のように、基地局 105 の情報とする。

[0169] 基準情報取得部 277 は、通信器 220 のうち、電話網通信器 222 を介して、通信時に用いる基地局 105 の情報を、基準位置情報として取得する。取得する基準位置情報は、例えば、基地局 105 の位置情報そのものであってもよいし、基地局を特定する識別情報（基地局 ID）であってもよい。

[0170] 図 17 (a) に示すように、基準情報取得部 277 は、同じタイミングで取得した位置情報 2a と、基準位置情報 40a との組を、基準情報 500a として基準情報記憶部 285 に記憶する。

[0171] なお、基準情報 500 は、所定のタイミングでの生成を繰り返す。従って、位置情報 2 と基準位置情報 40 とを備える基準情報 500 が、複数生成され、基準情報記憶部 285 に記憶される。ここでは、基準情報 500a (40a、2a)、基準情報 500b (40b、2b)、基準情報 500c (40c、2c)、が登録されている場合を例示する。

[0172] 本実施形態では、認証時、図 17 (b) に示すように、認証要求部 279 は、第一の実施形態の認証情報（移動履歴 5a および端末 ID 1a）に加え、基準情報 500 を、店舗機器 330 に送信する。そして、店舗機器 330

は、受信した認証情報と基準情報500とを、本人認証装置310に送信する。

[0173] また、本実施形態の本人認証装置319は、図16(b)に示すように、第一の実施形態の構成に加え、さらに、基準情報検証部316を備える。基準情報検証部316は、基準情報500の正当性を検証する。

[0174] すなわち、基準情報検証部316は、受信した基準情報500内の位置情報2と、対応づけて登録されている基準位置情報40との関係が、合理的なものであるかを検証する。例えば、基準位置情報40aが、基地局105の位置情報である場合、位置情報2aが、基準位置情報40aで特定される基地局105のカバーエリア内であるかを検証する。

[0175] なお、基準位置情報40aが基地局105の基地局IDである場合、当該IDで特定される基地局105のカバーエリア内であるかを検証する。

[0176] なお、各基地局105の位置情報および／または基地局ID等と、カバーエリアとの対応情報は、本人認証装置310で入手可能とする。

[0177] そして、基準情報検証結果がカバーエリア内であると判別された場合のみ、本人認証成功とする。

[0178] 本実施形態の本人認証装置310における、認証処理の流れを図18に沿って説明する。

[0179] まず、第一の実施形態と同様に、認証部313が、受信した認証情報と、認証情報保管部314に保管される認証情報とを照合する（ステップS3101）。

[0180] そして、一致しない場合、認証失敗とし、認証失敗を意味する情報を送信元の端末機器200に返信し（ステップS3106）、処理を終了する。

[0181] 一方一致した場合、基準情報検証部316は、各基準情報500を解析し、その正当性を検証する（ステップS3103）。ここでは、位置情報2が上述のように、基準位置情報40で特定される基地局105のカバーエリア内であるか否かを判別する。そして、全ての基準情報500が、カバーエリア内であれば、正当と判別する（ステップS3104）。

- [0182] ステップS 3 1 0 4 で正当と判別された場合、認証成功を意味する情報を、送信元の端末機器 2 0 0 に返信し（ステップS 3 1 0 5）、処理を終了する。
- [0183] 一方、正当と判別されない場合は、ステップS 3 1 0 6 へ移行する。
- [0184] なお、本実施形態では、基準情報として、携帯電話の基地局 1 0 5 の位置情報を用いたが、基準情報は、これに限定されない。その他のランドマークの位置情報等、端末機器 2 0 0 で取得でき、かつ、本人認証装置 3 1 0 で、当該情報の正当性を判別できる情報であればよい。
- [0185] 本実施形態は、端末機器 2 0 0 および本人認証装置 3 1 0 は、それぞれ、第一の実施形態と同様の構成を有する。このため、第一の実施形態と同様の効果が得られる。さらに、本実施形態の端末機器 2 0 0 は、基準情報を収集し、認証情報とともに、本人認証装置 3 1 0 に送信する。そして、本人認証装置 3 1 0 では、基準情報の正当性も判別する。この基準情報には、例えば、第三者の位置情報を用いる。
- [0186] このため、本実施形態によれば、端末機器 2 0 0 から送信される移動履歴が、実際にユーザ 2 0 9 の移動により得られたものであるか、偽物でないか、を判別できる。従って、より信頼性を向上できる。
- [0187] また、本実施形態においても、第一の実施形態の各種の変形例が適用可能である。
- [0188] 上記実施形態では、測位部 2 7 1 が取得した位置情報から認証情報を生成しているが、認証情報は、これに限定されない。例えば、購買履歴等を用いてもよい。購買履歴は、例えば、購買店舗情報、購買商品情報、購買金額情報等を含んでいてもよい。
- [0189] 本発明は上記の実施形態に限定されるものではなく、様々な変形例が含まれる。例えば、上記した実施形態は、本発明を分かりやすく説明するためのものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある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が可能であり、また、ある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。また、各実施形態の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

[0190] また、上記の各構成、機能、処理部、処理手段等は、それらの一部または全部を、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してもよい。

[0191] また、制御線や情報線は説明上必要と考えられるものを示しており、製品上必ずしも全ての制御線や情報線を示しているとは限らない。実際には殆ど全ての構成が相互に接続されていると考えてもよい。

符号の説明

[0192] 1 a : 端末 I D、2 : 位置情報、2 a : 位置情報、4 a : 位置情報、4 b : 位置情報、5 a : 移動履歴、5 b : 移動履歴、4 0 : 基準位置情報、4 0 a : 基準位置情報、5 0 a : 参照特徴情報、
1 0 0 : 本人認証システム、1 0 1 : ネットワーク、1 0 2 : 本人認証システム、1 0 5 : 基地局、
2 0 0 : 端末機器、2 0 1 : CPU、2 0 2 : システムバス、2 0 3 : 端末機器、2 0 8 : 正当でないユーザ、2 0 9 : 正当なユーザ、2 1 0 : 記憶装置、2 1 1 : ROM、2 1 2 : RAM、2 1 3 : 外部メモリ I / F、2 2 0 : 通信器、2 2 1 : LAN 通信器、2 2 2 : 電話網通信器、2 2 3 : 端末間通信器、2 2 7 : 拡張 I / F、2 3 0 : 操作器、2 4 0 : ビデオプロセッサ、2 4 1 : ディスプレイ、2 4 2 : 画像信号プロセッサ、2 4 3 : カメラ、2 4 6 : 端末間通信器、2 5 0 : オーディオプロセッサ、2 5 1 : スピーカ、2 5 2 : 音声信号プロセッサ、2 5 3 : マイク、2 6 0 : センサ、2 6 1 : GPS 受信器、2 6 2 : ジャイロセンサ、2 6 3 : 地磁気センサ、2 6 4 : 加速度センサ、2 6 5 : 照度センサ、2 6 6 : 近接センサ、2 6 7 : 生体情報センサ、2 7 1 : 測位部、2 7 2 : 移動履歴生成部、2 7 3 : 照合部、2 7 4 : 特徴情報収集部、2 7 5 : 通信部、2 7 6 : 登録処理部、2 7 7 : 基準情報取得部、2 7 9 : 認証要求部、2 8 1 : 位置情報記憶部、2 8 2 : 移動履歴記憶部、2 8 3 : 参照特徴情報記憶部、2 8 4 : 端末 I D 記憶部

、 2 8 5 : 基準情報記憶部、

3 0 0 : プロバイダシステム、 3 0 2 : プロバイダシステム、 3 1 0 : 本人認証装置、 3 1 1 : 通信部、 3 1 2 : 保管処理部、 3 1 3 : 認証部、 3 1 4 : 認証情報保管部、 3 1 5 : 共有処理部、 3 1 6 : 基準情報検証部、 3 1 9 : 本人認証装置、 3 2 0 : 内部ネットワーク、 3 2 1 : CPU、 3 2 2 : メモリ、 3 2 3 : 記憶装置、 3 2 4 : 通信器、 3 2 5 : LAN通信器、 3 2 6 : 端末間通信器、 3 3 0 : 店舗機器、 3 3 1 : 店舗機器、 3 3 2 : 店舗機器、 3 3 3 : 店舗機器、 3 3 4 : 店舗機器、 3 4 0 : LAN通信器、 3 4 1 : CPU、 3 4 2 : メモリ、 3 4 3 : 記憶装置、 3 4 4 : 通信器、 3 4 5 : LAN通信器、 3 4 6 : 端末間通信器、 3 5 0 : 本人認証装置、 3 5 1 : 本人認証装置、 3 5 2 : 本人認証装置、 3 5 3 : 本人認証装置、

4 1 1 : 型名情報、 4 1 2 : シリアル番号、 4 2 2 : 日時、 4 2 3 : 位置情報、 4 3 1 : 歩調周波数、 4 3 2 : 歩幅、 4 3 3 : 歩行速度、

5 0 0 : 基準情報、 5 0 0 a : 基準情報、 5 0 0 b : 基準情報、 5 0 0 c : 基準情報

請求の範囲

[請求項1]

端末機器であって、

所定の時間間隔で前記端末機器の位置を測位し、位置情報として蓄積する測位部と、

所定期間の前記位置情報を用いて移動履歴を生成し、移動履歴情報として記憶する移動履歴生成部と、

前記移動履歴情報を、本人認証装置に登録のために送信する登録処理部と、

前記登録処理部が前記本人認証装置に送信後の前記移動履歴情報を用いて、前記本人認証装置に対して認証要求を行う認証要求部と、を備えること

を特徴とする端末機器。

[請求項2]

請求項1記載の端末機器であって、

前記登録処理部は、前記移動履歴情報とともに、当該端末機器を一意に特定する端末識別情報を、前記本人認証装置に送信し、

前記認証要求部は、前記認証要求に、前記端末識別情報と前記移動履歴情報とを含めること

を特徴とする端末機器。

[請求項3]

請求項1記載の端末機器であって、

当該端末機器のユーザの特徴を示す特徴情報を収集する特徴情報収集部と、

収集した前記特徴情報を、予め保持する正当なユーザの特徴情報である参照特徴情報と照合し、照合結果を出力する照合部と、をさらに備え、

前記移動履歴生成部は、前記照合部が前記照合結果として前記特徴情報と前記参照特徴情報とが一致したことを意味する情報を出力している間に測位された位置情報を用いて、前記移動履歴を生成することを特徴とする端末機器。

- [請求項4] 請求項1記載の端末機器であって、
前記登録処理部は、前記認証要求部の前記認証要求に応じて認証された後、最新の前記移動履歴情報を前記本人認証装置に送信することを特徴とする端末機器。
- [請求項5] 請求項1記載の端末機器であって、
第三者の位置情報を、基準情報として取得する基準情報取得部をさらに備え、
前記認証要求部は、前記認証要求に、前記基準情報もさらに含めること
を特徴とする端末機器。
- [請求項6] 請求項1記載の端末機器であって、
前記認証要求は、近距離無線通信を用いて行うこと
を特徴とする端末機器。
- [請求項7] 端末機器と、認証インタフェース装置と、本人認証装置とを備える本人認証システムであって、
前記端末機器は、
所定の時間間隔で前記端末機器の位置を測位し、位置情報として蓄積する測位部と、
所定期間の前記位置情報を用いて移動履歴を生成し、移動履歴情報として記憶する移動履歴生成部と、
前記移動履歴情報を、前記本人認証装置に登録のために送信する登録処理部と、
前記登録処理部が前記本人認証装置に送信後の前記移動履歴情報を用いて、前記認証インタフェース装置を介して前記本人認証装置に対して認証要求を行う認証要求部と、を備え、
前記本人認証装置は、
前記端末機器から送信された前記移動履歴情報を、保管する保管処理部と、

前記端末機器から前記認証インタフェース装置を介して前記認証要求を受信した際、当該認証要求に含まれる前記移動履歴が前記保管処理部により保管されているか否かを判別することにより、認証を行い、認証結果を返す認証部と、を備えることを特徴とする本人認証システム。

[請求項8]

請求項7記載の本人認証システムであって、

前記保管処理部は、前記端末機器から新たな移動履歴情報を受信する毎に、最新の前記移動履歴情報で、保管されている前記移動履歴情報を上書きすること

を特徴とする本人認証システム。

[請求項9]

請求項7記載の本人認証システムであって、

前記本人認証装置を複数備え、

各前記本人認証装置は、共有処理部を備え、

前記共有処理部は、前記端末機器から送信された前記移動履歴情報および前記認証要求を、他の本人認証装置に送信するとともに、前記他の本人認証装置それぞれから前記認証要求に対する認証結果を受信し、受信した当該認証結果と自身の前記認証部による認証結果とに応じて認証の成否を決定すること

を特徴とする本人認証システム。

[請求項10]

端末機器と、認証インタフェース装置と、本人認証装置とを備える本人認証システムにおける本人認証方法であって、

端末機器において移動履歴情報を記憶するとともに、前記本人認証装置に当該移動履歴情報を送信し、当該本人認証装置において認証情報として保管する初期登録ステップと、

前記認証インタフェース装置を介して前記移動履歴情報を認証要求として前記本人認証装置に送信し、前記本人認証装置において前記認証情報を用いて認証を受ける認証ステップと、

新たに生成した移動履歴情報を、前記認証インタフェース装置を介

して前記本人認証装置に送信し、前記本人認証装置において保管されている前記認証情報を当該移動履歴情報によって置き換える認証情報更新ステップと、を備えること

を特徴とする本人認証方法。

[請求項11]

請求項10記載の本人認証方法であって、

前記端末機器から前記認証インタフェース装置および前記本人認証装置のいずれかに前記移動履歴情報を送信する前に、当該移動履歴情報を生成する移動履歴情報生成ステップを備え、

前記移動履歴情報生成ステップは、

前記端末機器の位置情報を取得する位置情報取得ステップと、

前記端末機器のユーザの正当性を判別する正当性判別ステップと、

前記正当性判別ステップにおいて正当と判別された際に取得された位置情報を前記移動履歴情報に採用する採用移動履歴決定ステップと、を備えること

を特徴とする本人認証方法。

[請求項12]

請求項10記載の本人認証方法であって、

前記認証情報は、送信元の前記端末機器の識別情報である端末識別情報をさらに備え、

前記認証ステップでは、前記認証要求に、当該認証要求の送信元の前記端末機器の前記端末識別情報を含めること

を特徴とする本人認証方法。

[請求項13]

請求項3記載の端末機器であって、

当該端末機器の加速度を検出する加速度センサをさらに備え、

前記特徴情報として、所定期間の前記加速度センサの出力を用いること

を特徴とする端末機器。

[請求項14]

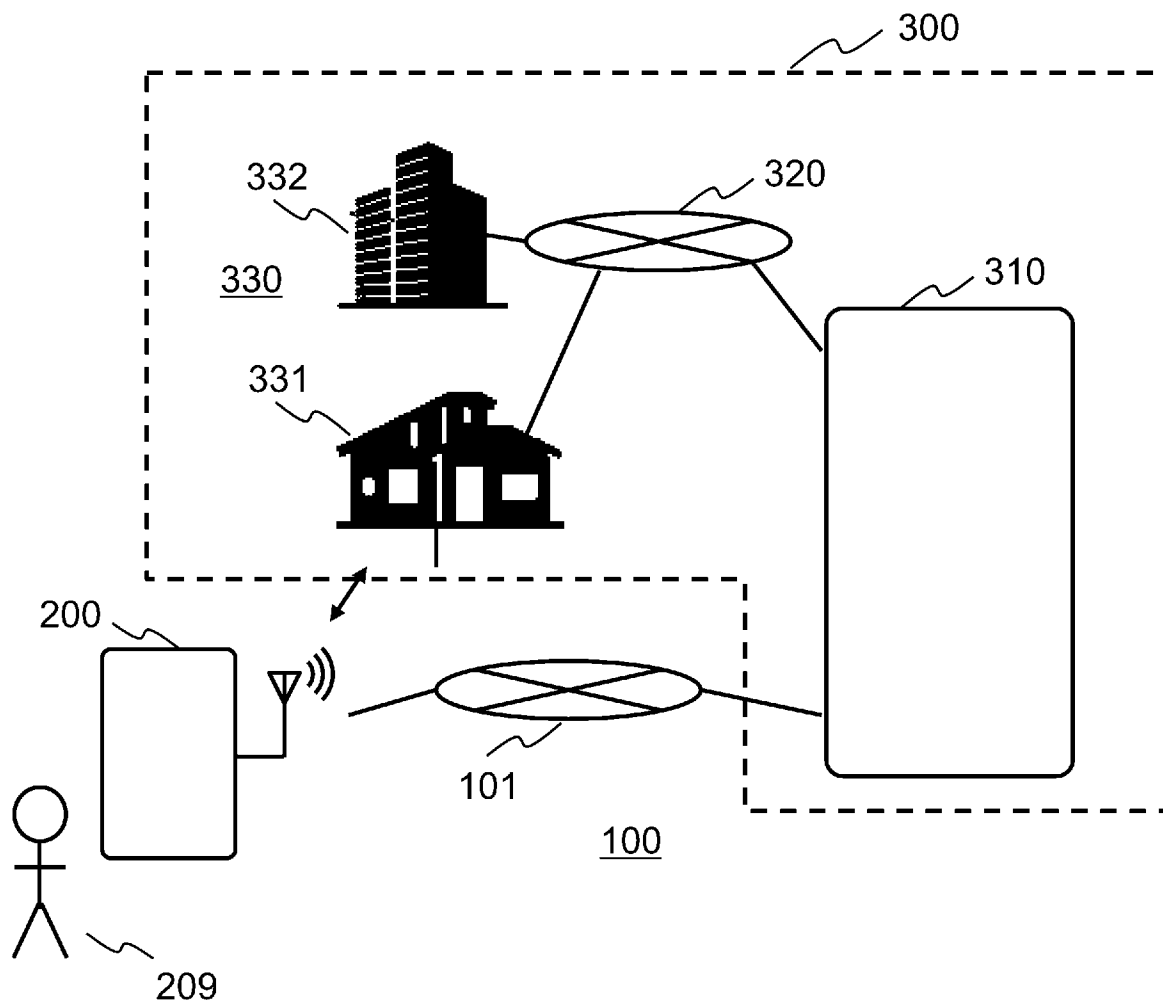
請求項3記載の端末機器であって、

前記ユーザの脈波を検出する脈波センサをさらに備え、

前記特徴情報として、所定期間の前記脈波センサの出力を用いること
と
を特徴とする端末機器。

[図1]

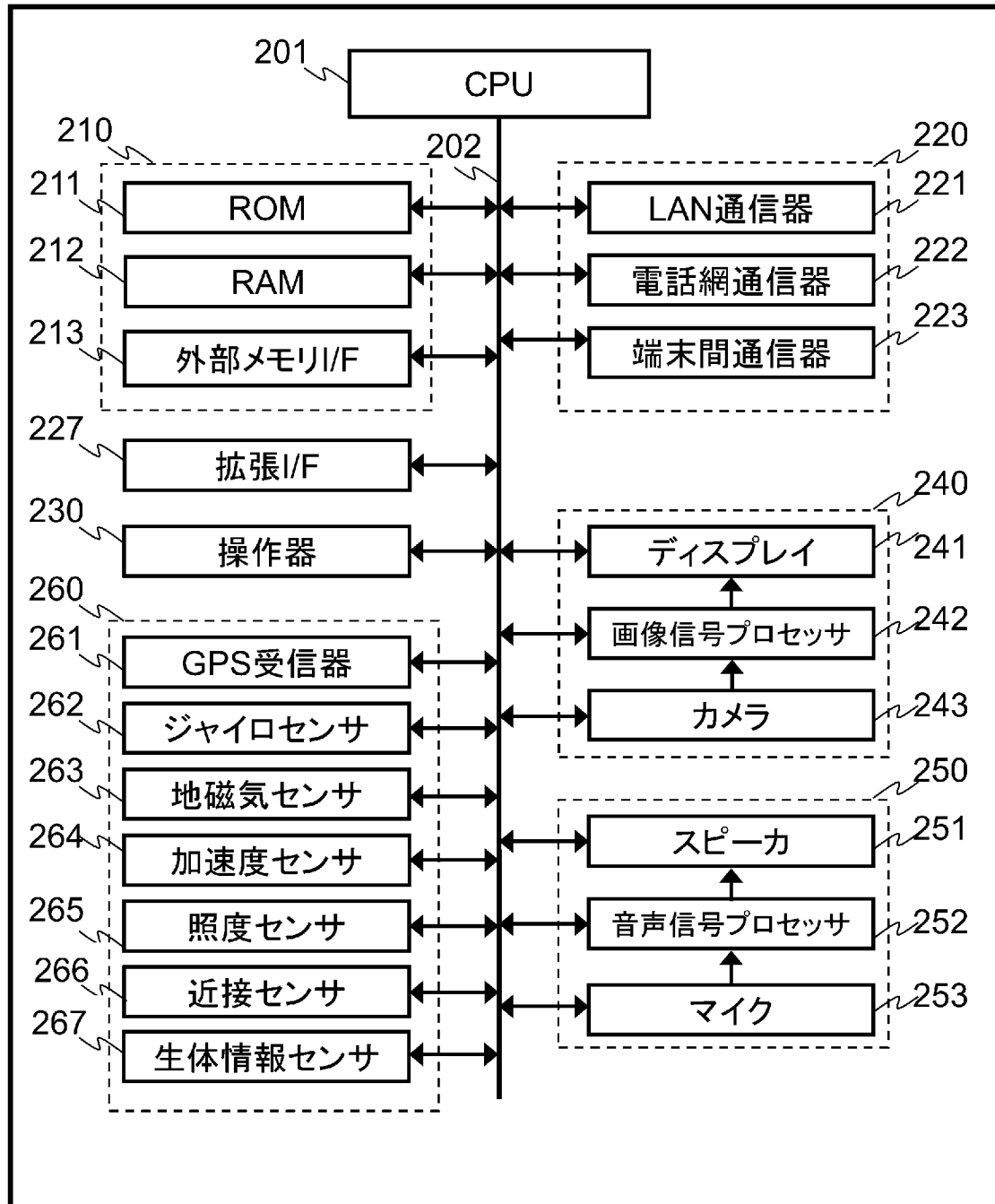
図1



[図2]

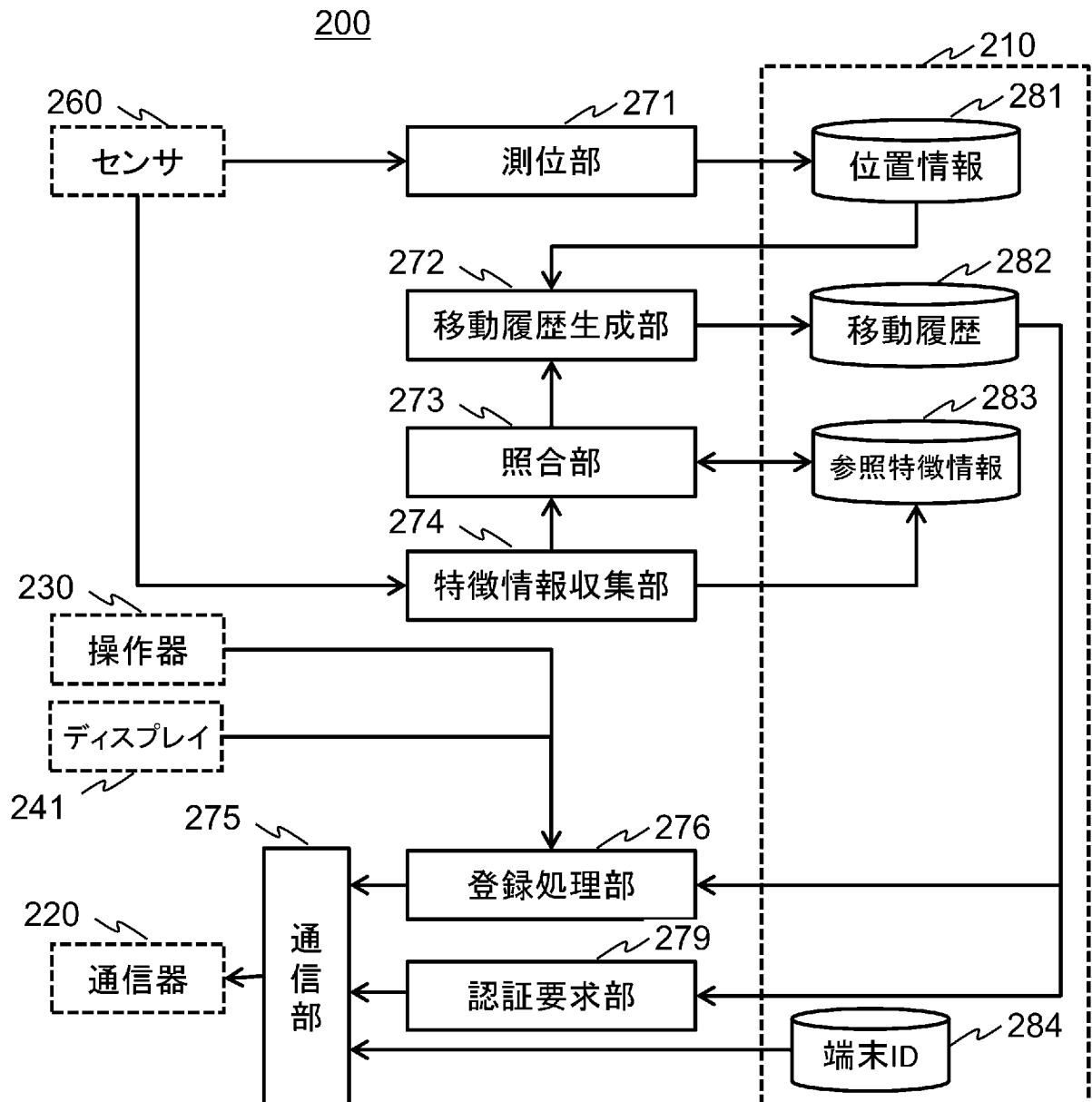
図2

200



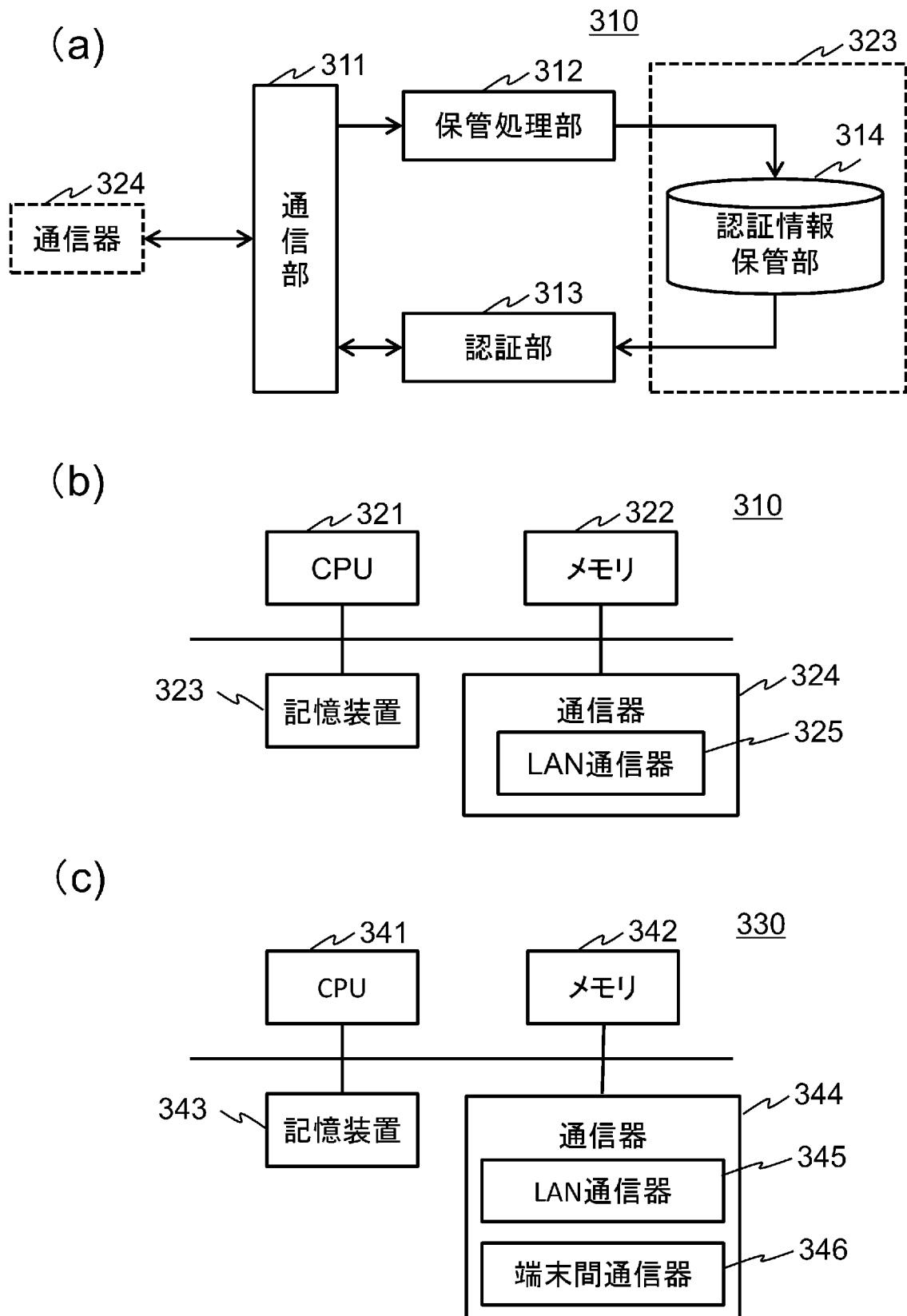
[図3]

図3



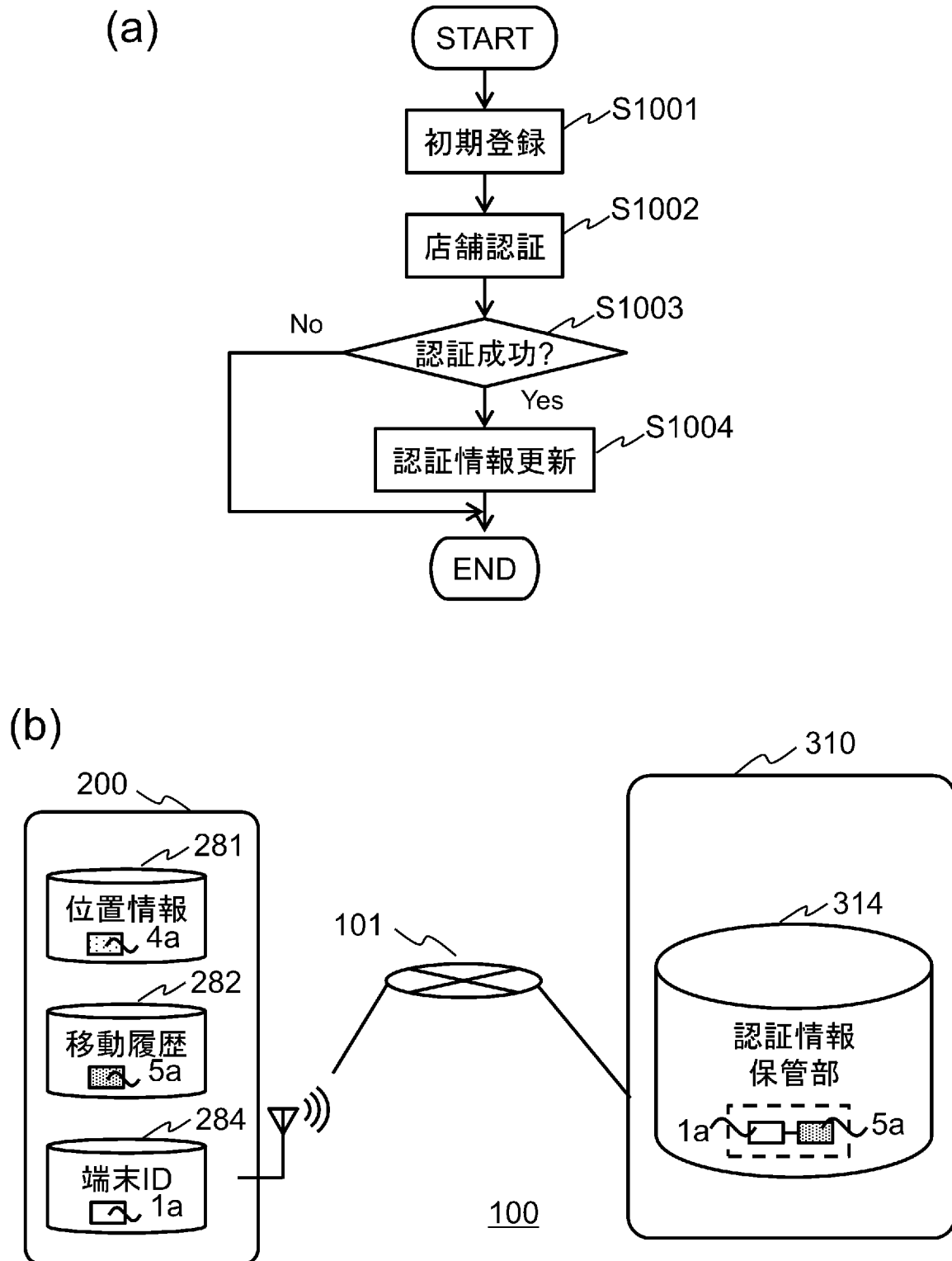
[図4]

図4



[図5]

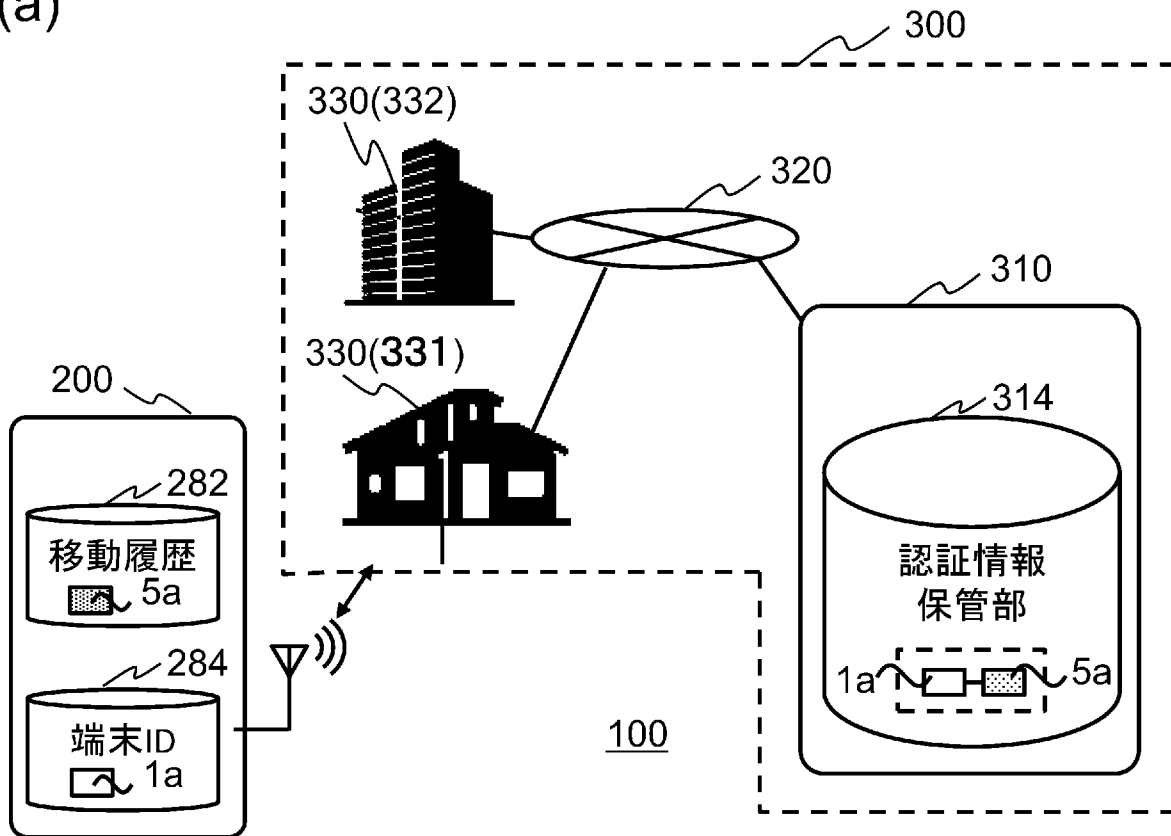
図5



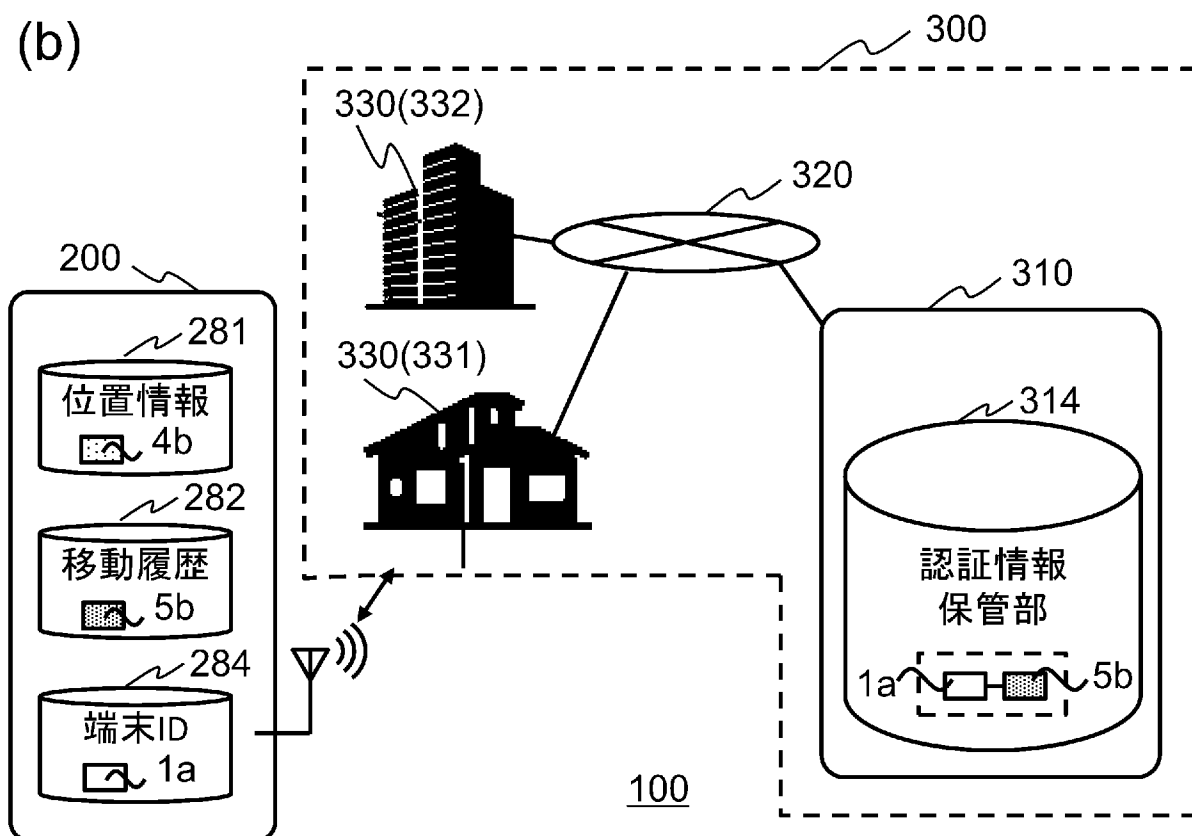
[図6]

図6

(a)



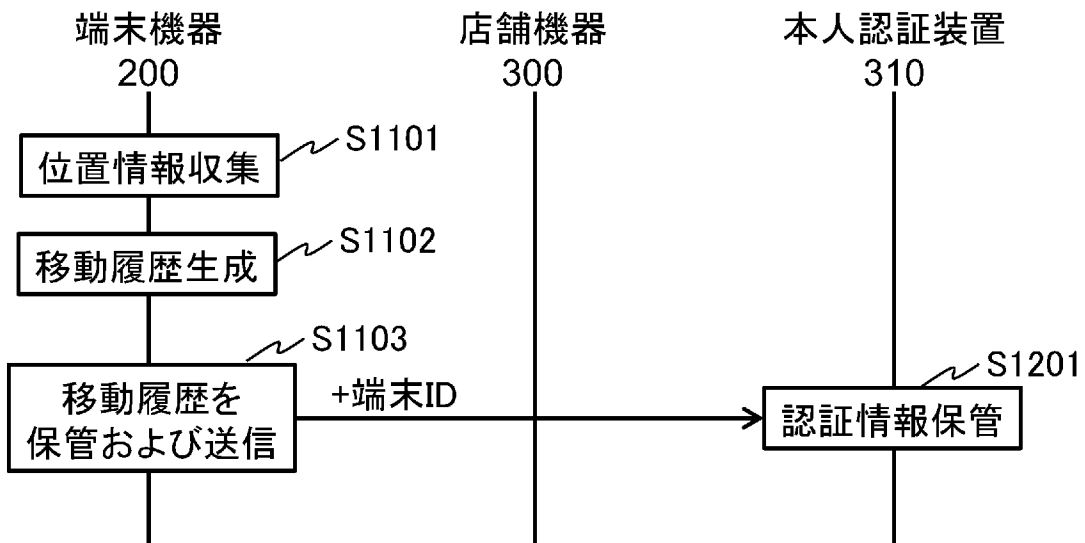
(b)



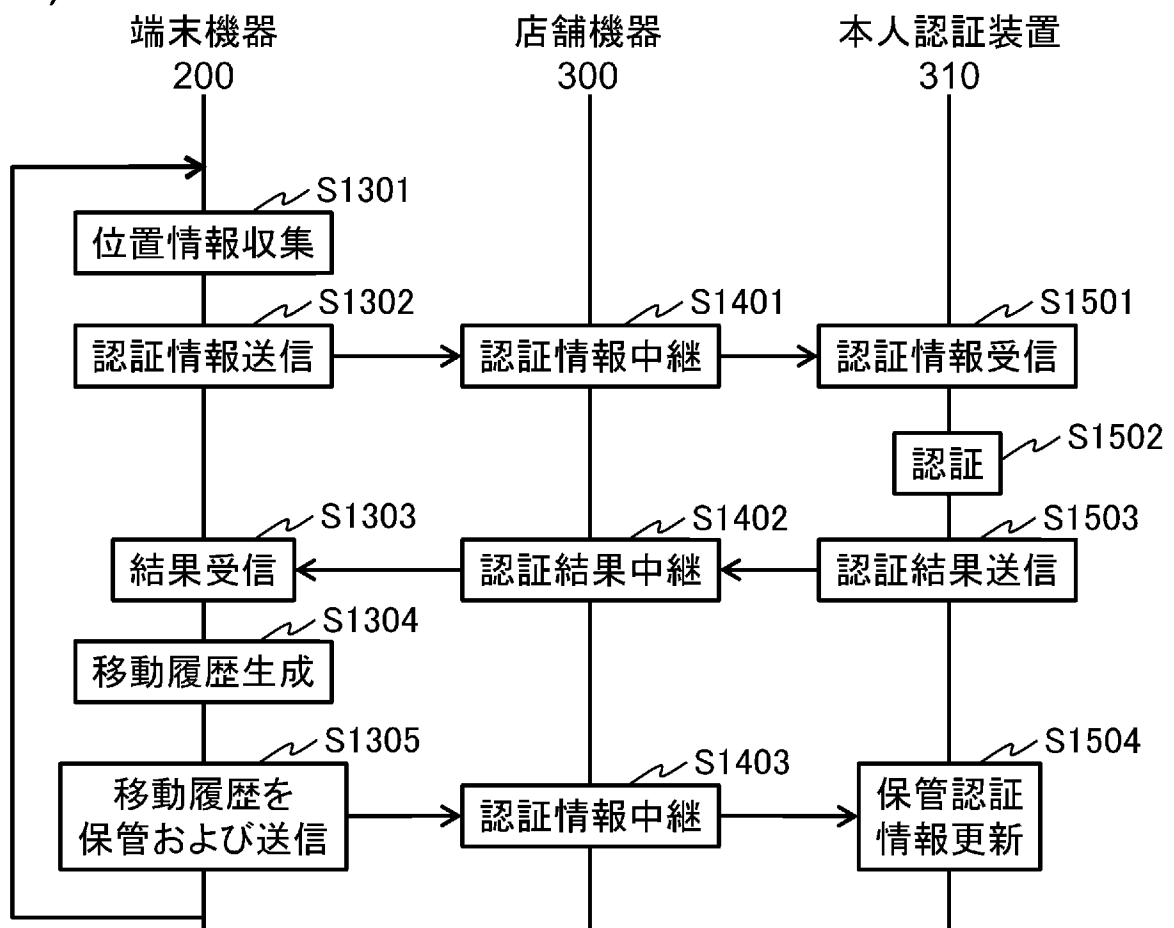
[図7]

図7

(a)



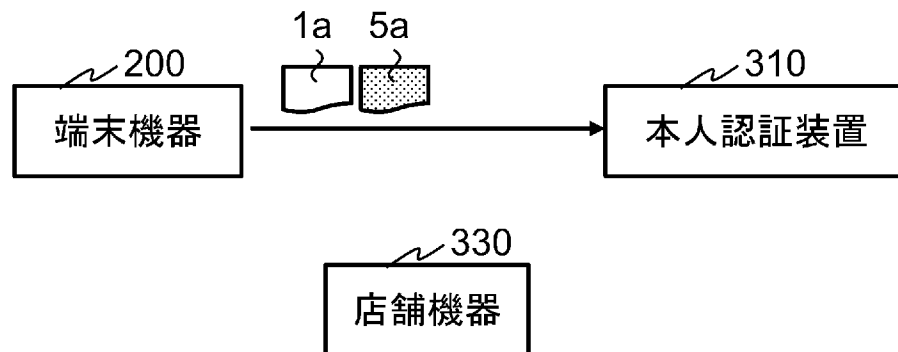
(b)



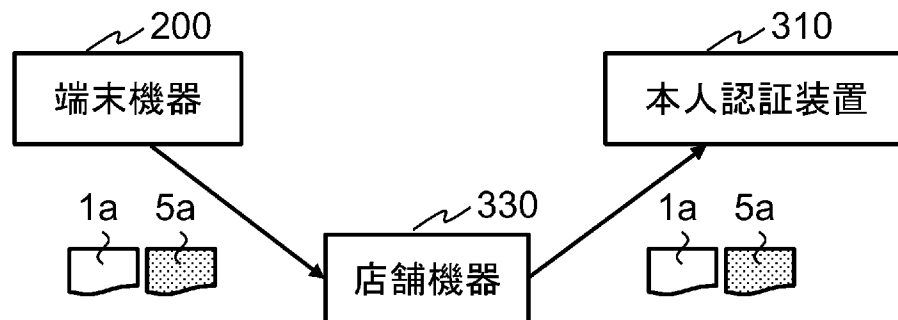
[図8]

図8

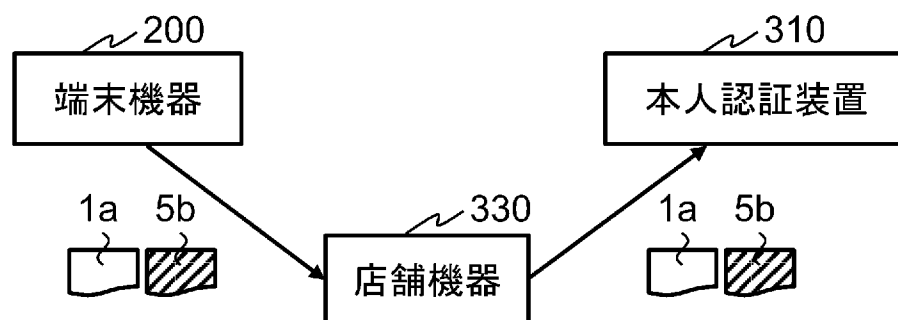
(a)



(b)

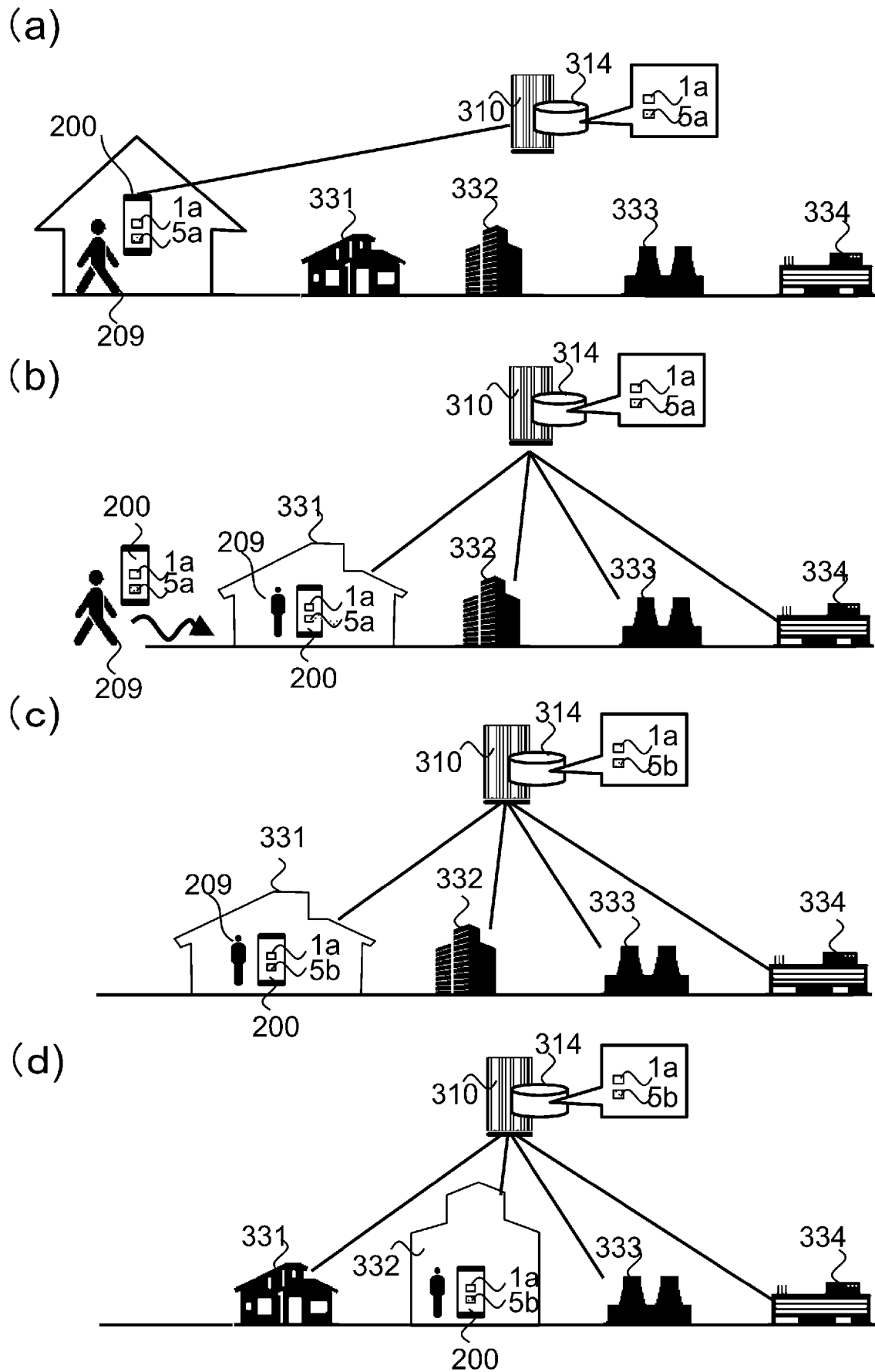


(c)



[図9]

図9



[図10]

図10

(a)

1a

型名 411	シリアル番号 412
xxxxxxxx	*****

(b)

5a

番号 421	日時 422	位置 423
1	2017.11.24 15:00	緯度 36° , 0' , 0" , 経度 135° , 0' , 0"
2	2017.11.24 15:01	緯度 36° , 0' , 2" , 経度 135° , 0' , 1"
3	2017.11.24 15:02	緯度 36° , 0' , 4" , 経度 135° , 0' , 2"
⋮	⋮	⋮

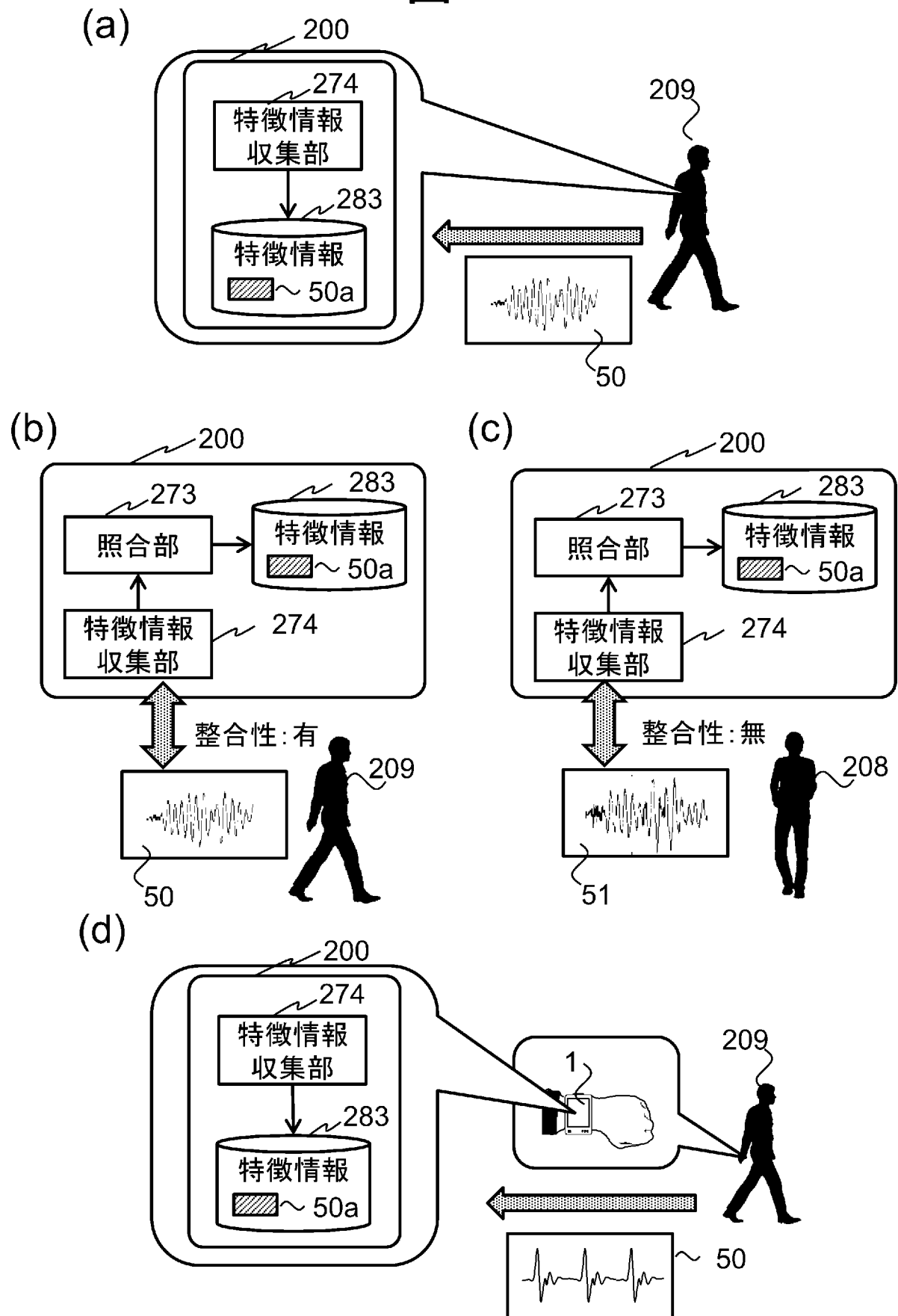
(c)

50a

歩調周波数 431	歩幅 432	歩行速度 433
xxx	yyy	zzz

[図11]

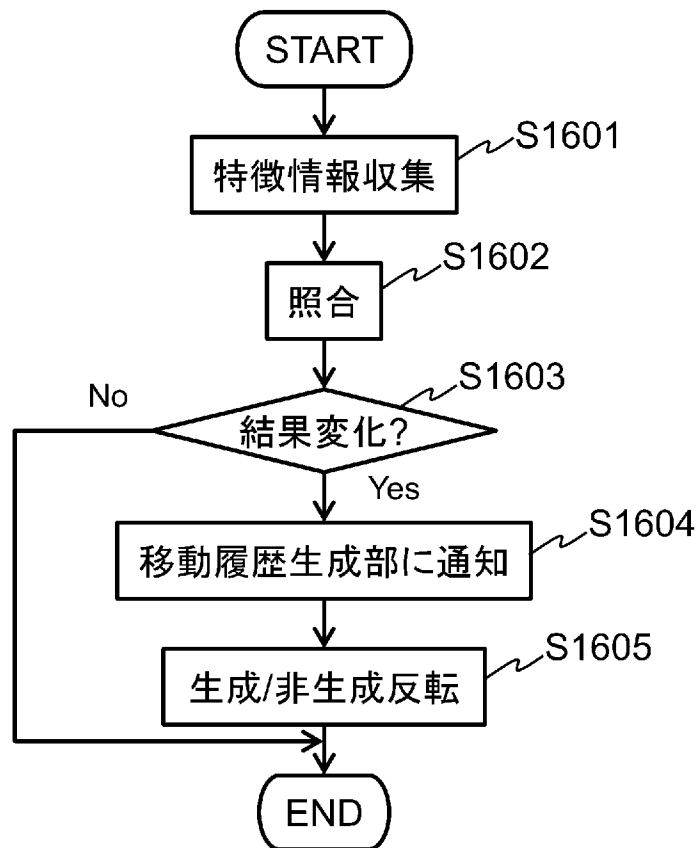
図 11



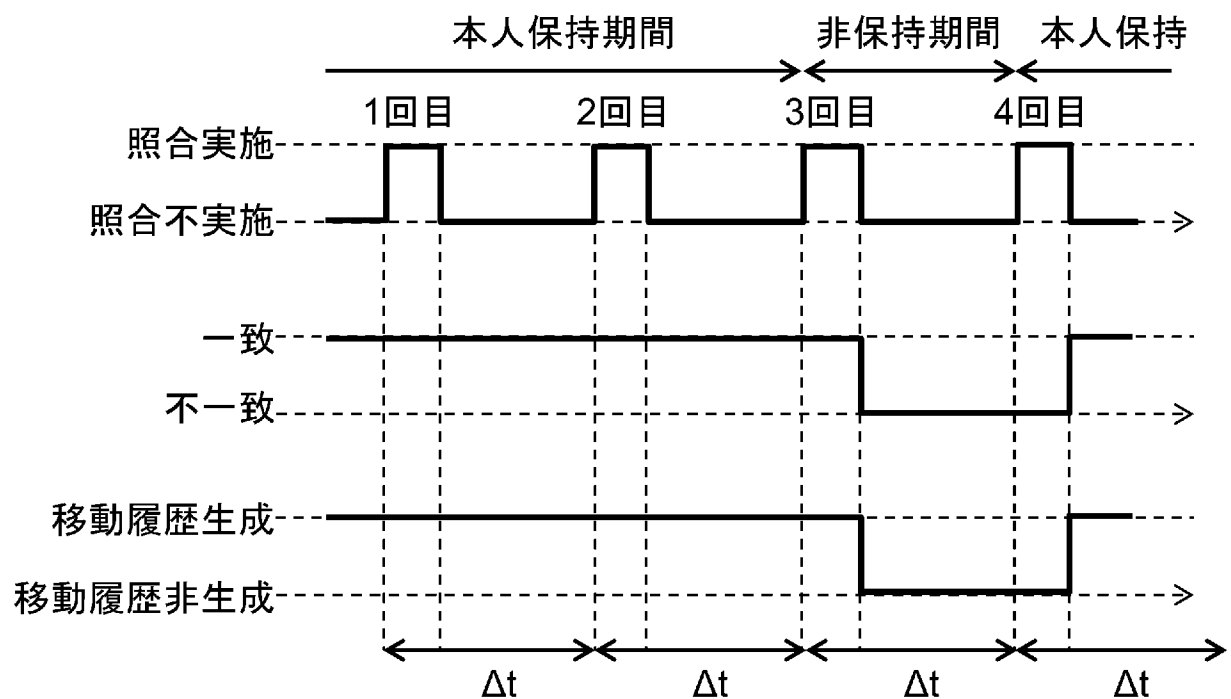
[図12]

図12

(a)

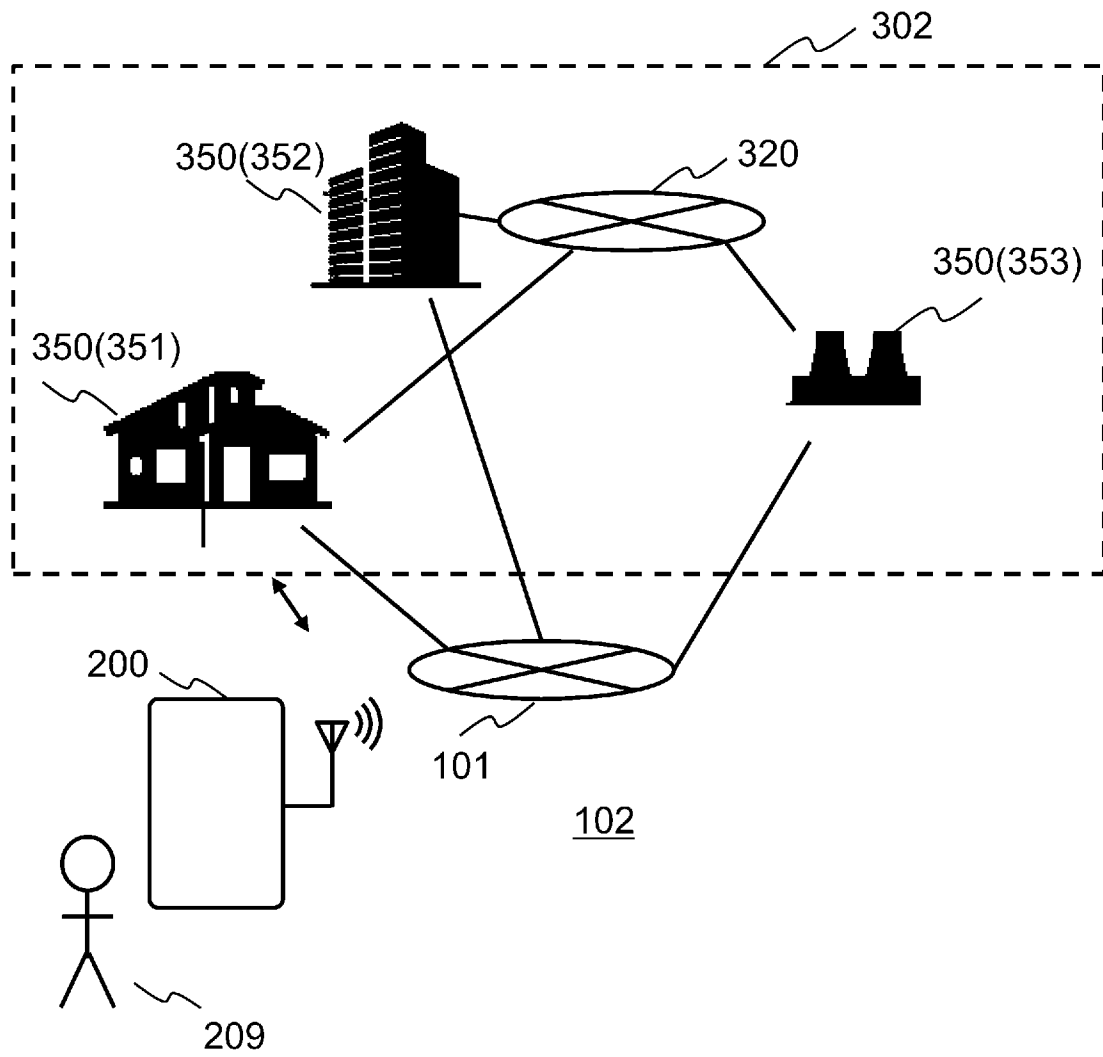


(b)



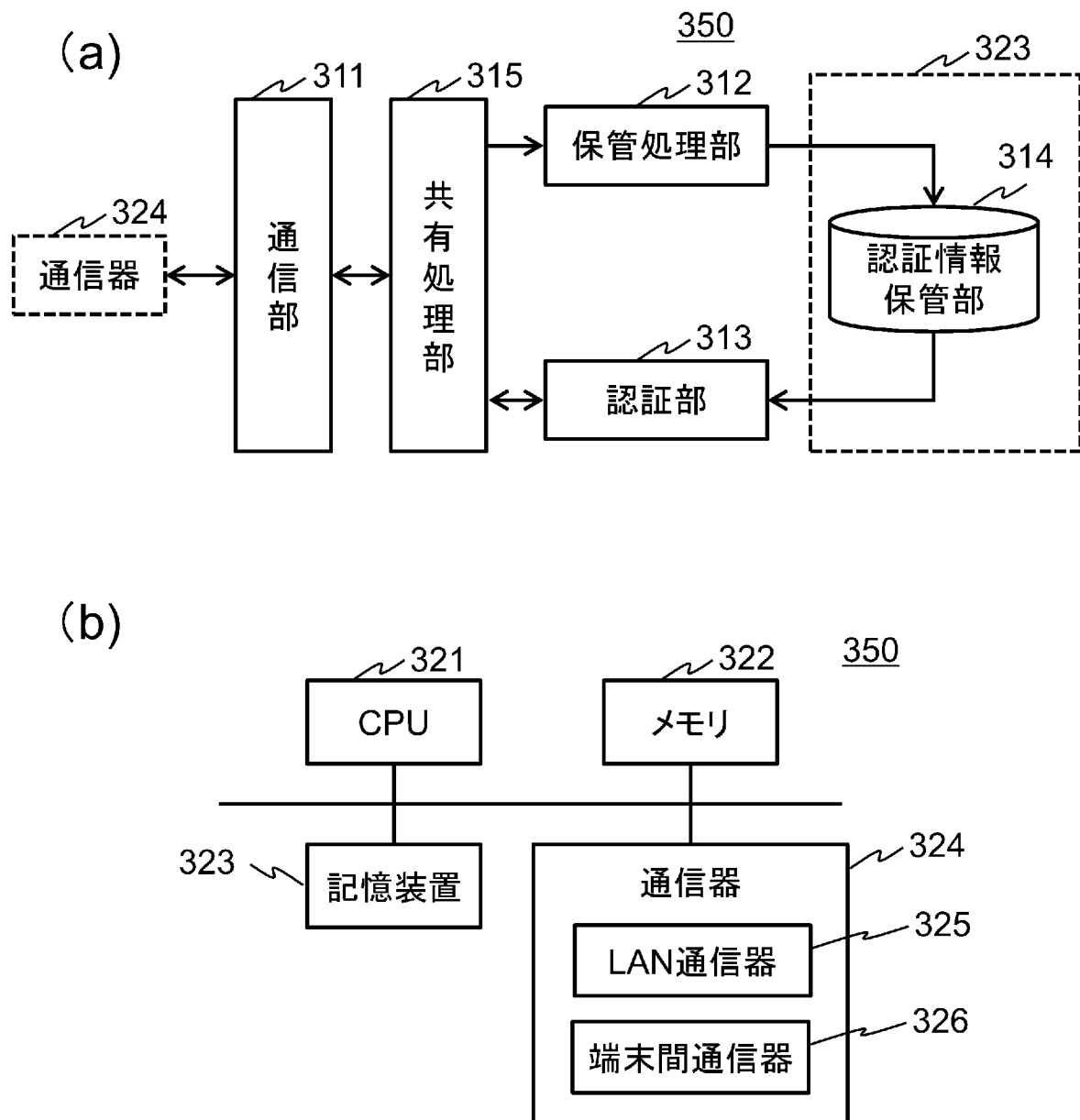
[図13]

図13



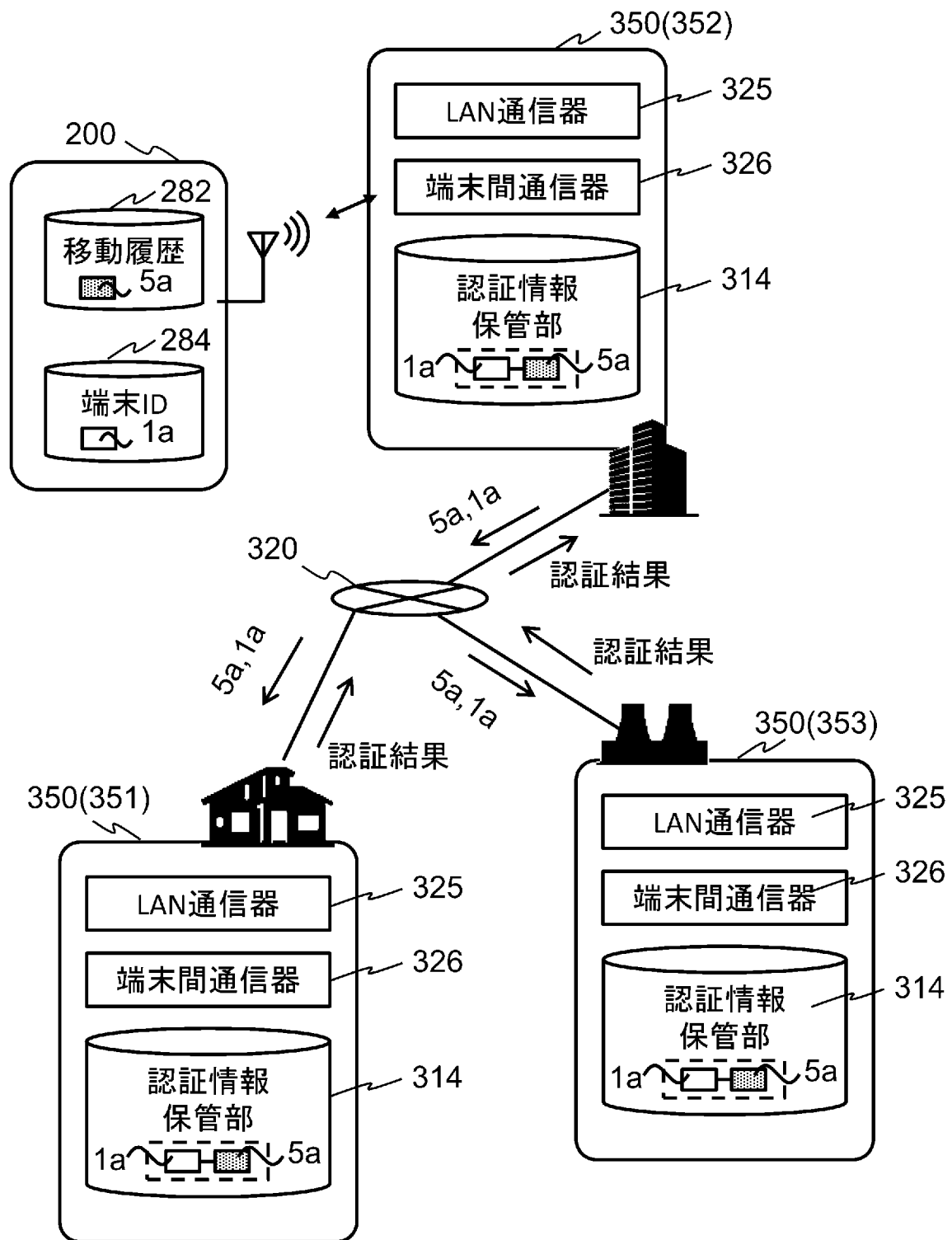
[図14]

図14



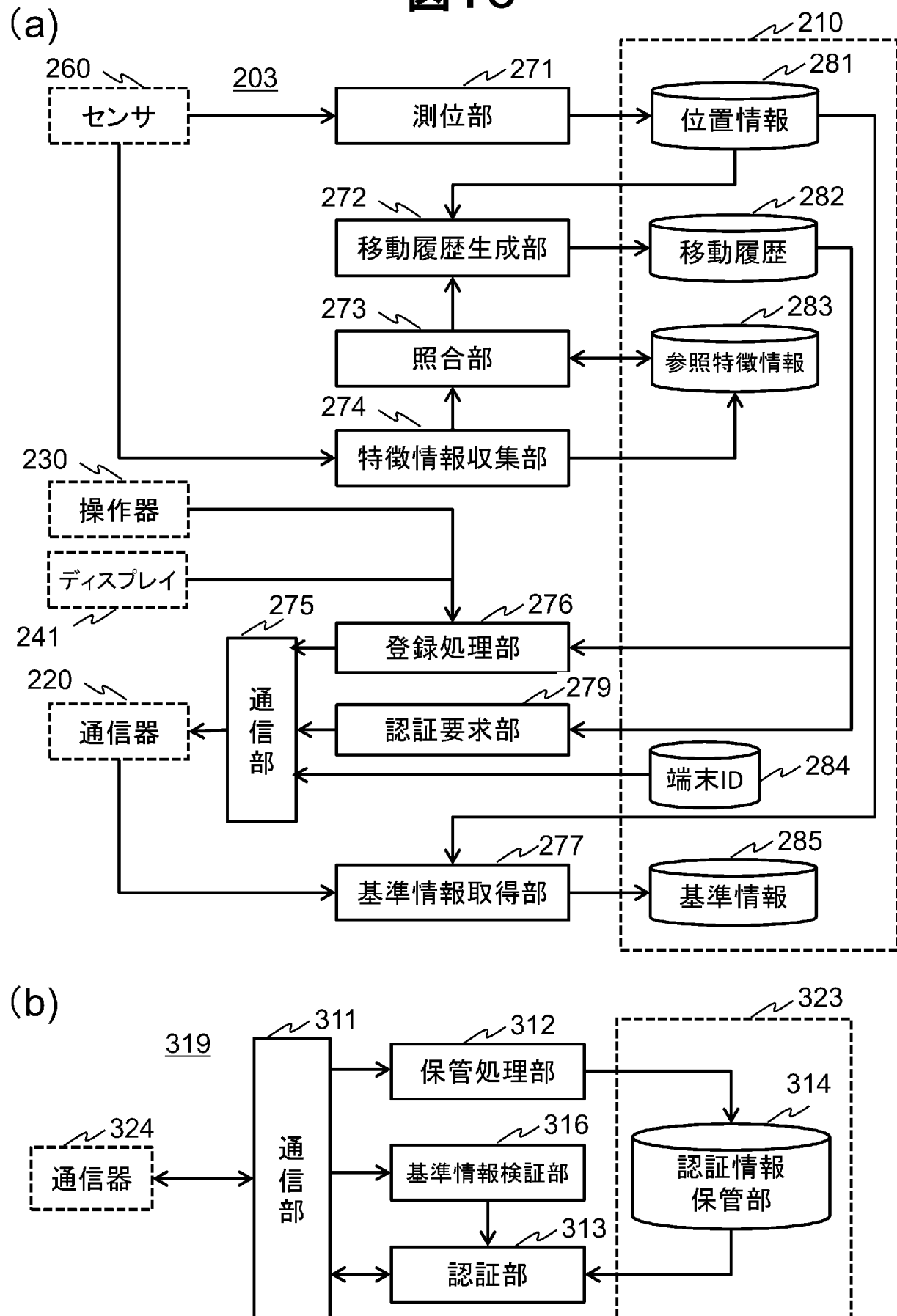
[図15]

図15



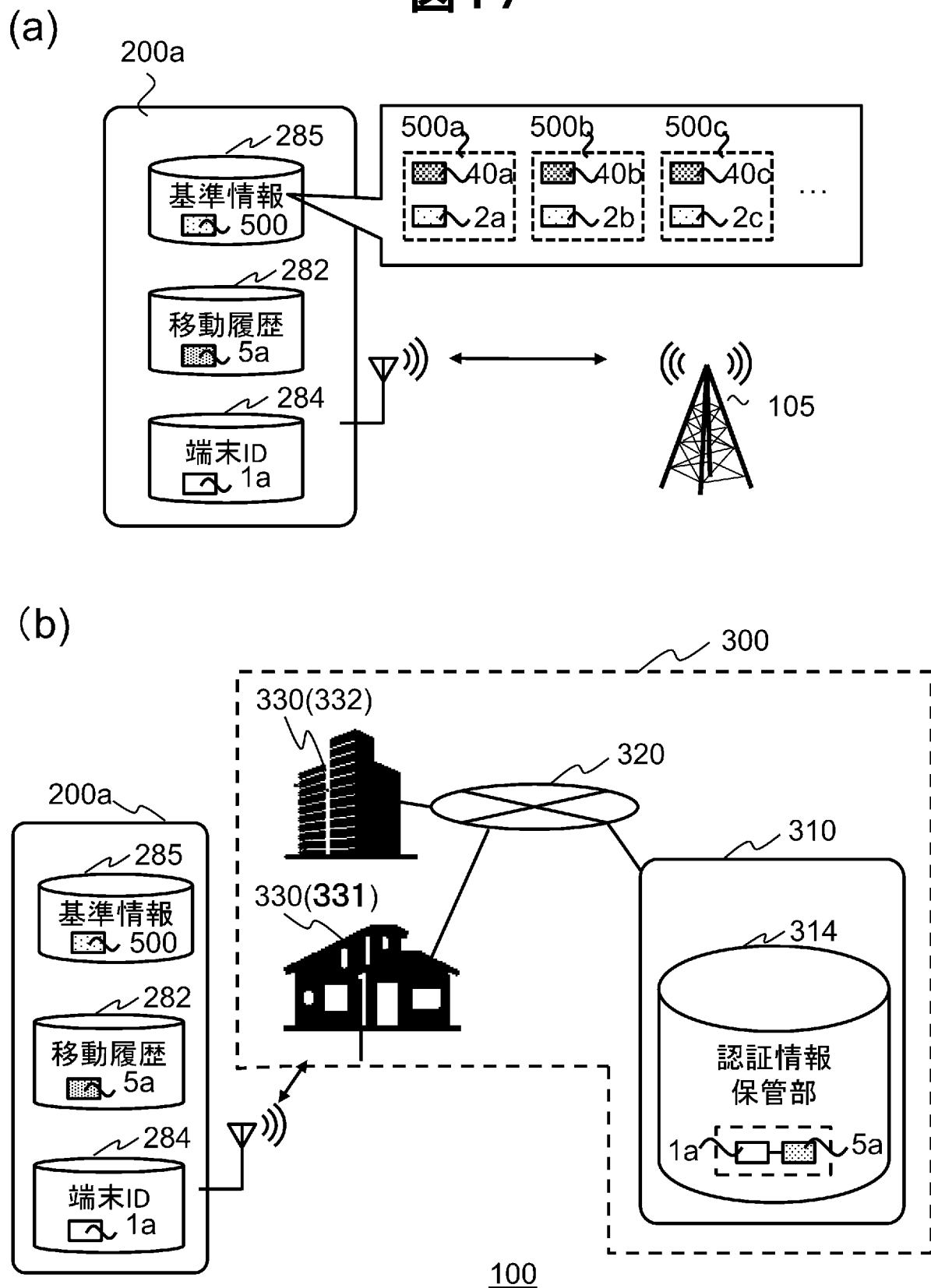
[図16]

図16



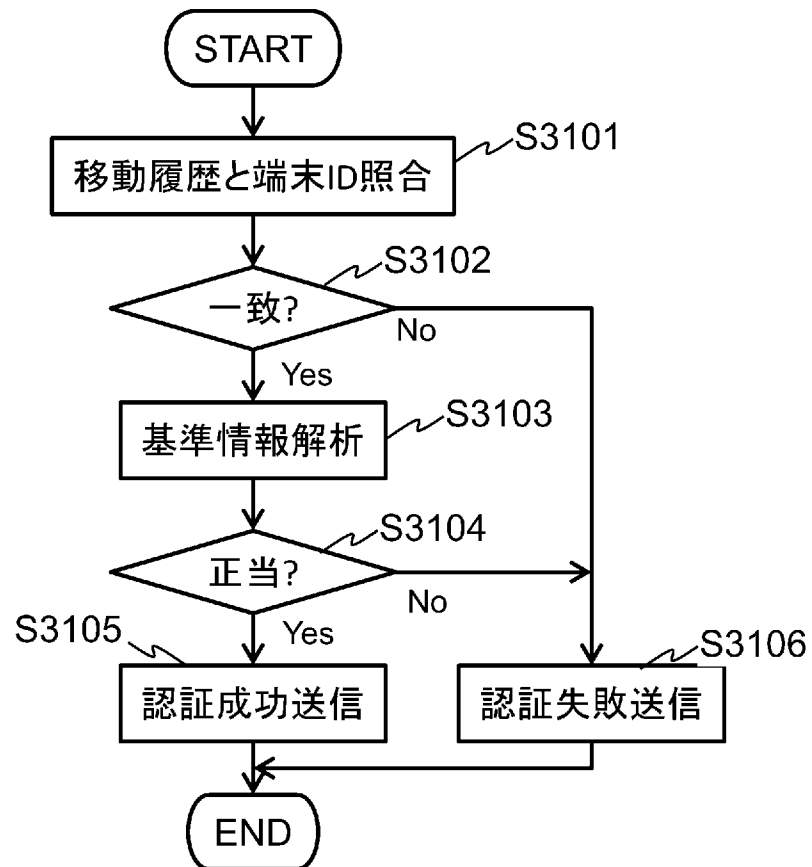
[図17]

図17



[図18]

図18



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/044998

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F21/31 (2013.01) i, G06F21/32 (2013.01) i, G06F21/44 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl. G06F21/31, G06F21/32, G06F21/44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-258845 A (NTT DATA SYSTEMS CORP.) 16 September 2004 (Family: none)	1-14
A	JP 2012-133526 A (PANASONIC CORP.) 12 July 2012 (Family: none)	1-14
A	JP 2010-277190 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 09 December 2010, paragraphs [0041]-[0045], fig. 1-4, 12-13 (Family: none)	1-14
A	WO 2013/073120 A1 (PANASONIC CORP.) 23 May 2013 & US 9171410 B2 & CN 103238155 A	1-14
A	JP 2016-99684 A (INTERMAN CORPORATION) 30 May 2016 (Family: none)	1-14

☐ 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
04 March 2019 (04.03.2019)

Date of mailing of the international search report
12 March 2019 (12.03.2019)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F21/31(2013.01)i, G06F21/32(2013.01)i, G06F21/44(2013.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. G06F21/31, G06F21/32, G06F21/44

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2004-258845 A（株式会社エヌ・ティ・ティ・データ・システムズ）2004.09.16,（ファミリーなし）	1-14
A	JP 2012-133526 A（パナソニック株式会社）2012.07.12,（ファミリーなし）	1-14
A	JP 2010-277190 A（日本電信電話株式会社）2010.12.09, [0041]-[0045], 図 1-4, 12-13（ファミリーなし）	1-14

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

04.03.2019

国際調査報告の発送日

12.03.2019

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

岸野 徹

5 S

3983

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	WO 2013/073120 A1 (パナソニック株式会社) 2013. 05. 23, & US 9171410 B2 & CN 103238155 A	1-14
A	JP 2016-99684 A (インターマン株式会社) 2016. 05. 30, (ファミリーなし)	1-14