(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2004-252964
(P2004-252964A)
(43)公開日　平成16年9月9日(2004.9.9)

| (51)Int.Cl.[7] | F I | | テーマコード（参考） |
|---|---|---|---|
| G06F 17/60 | G06F 17/60 | 140 | 2C032 |
| G09B 29/00 | G06F 17/60 | 506 | 5J104 |
| H04L 9/32 | G06F 17/60 | 510 | |
| | G09B 29/00 | A | |
| | H04L 9/00 | 673D | |

審査請求 未請求　請求項の数 9　OL　（全 17 頁）　最終頁に続く

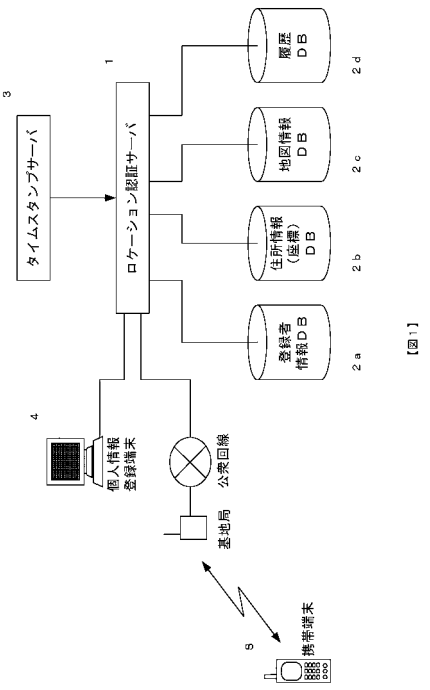
(21)出願番号　特願2004-19229 (P2004-19229)
(22)出願日　平成16年1月28日 (2004.1.28)
(31)優先権主張番号　特願2003-20654 (P2003-20654)
(32)優先日　平成15年1月29日 (2003.1.29)
(33)優先権主張国　日本国 (JP)

(71)出願人　597062650
技研商事インターナショナル株式会社
愛知県名古屋市東区主税町二丁目３０番地
(74)代理人　100093104
弁理士　船津　暢宏
(74)代理人　100092772
弁理士　阪本　清孝
(72)発明者　松本　芳典
東京都千代田区　霞ヶ関三丁目５番１号
霞ヶ関１ＨＦビル４Ｆ　技研商事インターナショナル株式会社内

Ｆターム(参考)　2C032 HB03 HB05 HB22 HB25 HD13
5J104 KA17 KA18 KA19 MA01 PA02
PA10

(54)【発明の名称】ロケーション証明システム

(57)【要約】
【課題】　本発明は、携帯端末の所有者本人及び物品の位置（ロケーション）及び日時を証明するロケーション証明システムを提供する。
【解決手段】　ロケーション認証サーバは、携帯端末５から送信された生体データと登録者情報ＤＢ２ａに登録された生体データを用いて本人認証を行い、携帯端末５の位置通知機能を利用して位置を特定し、住所情報ＤＢ２ｂで特定した位置情報から住所情報を取得し、更に地図情報ＤＢ２ｃから対応する地図情報を取得し、タイムスタンプサーバ３から日時情報を取得し、携帯端末ユーザの位置及び日時をこれらデータで証明するロケーション証明書を生成するとするロケーション証明システムである。
【選択図】　図１



【図１】

【特許請求の範囲】
【請求項１】
ユーザの携帯端末の識別番号を含むユーザに関する情報及び生体データをユーザ毎に記憶する登録者情報データベースと、位置情報に対応付けて住所情報を記憶する住所情報データベースと、携帯端末を用いたユーザのアクセスを位置及び日時で記録する履歴データベースとに接続され、
携帯端末から送信された携帯端末の識別番号、生体データ及び位置情報を受信する通信部と、
受信した生体データについて、前記登録者情報データベースを参照して前記携帯端末の識別番号に対応して予め記憶されている生体データと比較し、両生体データが一致するか否かの個人認証の処理を実行し、
前記個人認証の処理によって両生体データが一致する場合に、前記携帯端末から受信した位置情報について、前記住所情報データベースを参照して前記位置情報を住所情報に変換する処理を実行し、
前記携帯端末からのアクセスを前記履歴データベースに記録する処理を実行し、
日時情報を発行するタイムスタンプサーバから日時情報を取得して、ユーザの位置を住所及び前記日時情報により証明するロケーション証明書を生成する処理を実行する制御部と、
前記生成されたロケーション証明書を記憶する記憶部とを備えたロケーション認証サーバを有することを特徴とするロケーション証明システム。
【請求項２】
ロケーション認証サーバは、地図情報を記憶する地図情報データベースに接続され、
制御部は、携帯端末から受信した位置情報について、前記地図情報データベースを参照して前記位置情報に該当する地図情報を取得する処理を実行し、ロケーション証明書を生成する際に、ユーザの位置を住所、対応する地図情報、及び日時情報により証明するロケーション証明書を生成する処理を実行することを特徴とする請求項１記載のロケーション証明システム。
【請求項３】
ユーザに関する情報には、ユーザが指定したロケーション証明書の送付先が含まれ、
ロケーション認証サーバの制御部は、ユーザからのロケーション証明書発行の要求を、通信部を介して受信すると、登録者情報データベースを参照して当該ユーザのロケーション証明書の送付先を読み込み、当該送付先に記憶部に記憶されたロケーション証明書を、前記通信部を介して送信することを特徴とする請求項１又は２記載のロケーション証明システム。
【請求項４】
ロケーション認証サーバは、ウェブサーバの機能を備え、
制御部は、携帯端末からのロケーション証明書の閲覧要求を、通信部を介して受信すると、個人認証のための生体データの入力を促す画面を表示出力し、
携帯端末から入力されて送信された生体データについて個人認証が為され、両生体データが一致すると、記憶部に記憶された当該ユーザのロケーション証明書のリストを前記携帯端末の表示画面に表示出力し、
前記携帯端末から当該リストの中からロケーション証明書の項目が選択されると、選択されたロケーション証明書を閲覧可能に前記携帯端末の表示画面に表示出力することを特徴とする請求項１乃至３のいずれか記載のロケーション証明システム。
【請求項５】
ロケーション認証サーバの制御部は、携帯端末からユーザのロケーション証明書のリストの中から複数のロケーション証明書の項目が選択されると、選択された複数のロケーション証明書における住所情報を一つの地図情報上に点でプロットして当該点を時系列に接続する線を描画した表示画面に表示出力することを特徴とする請求項４記載のロケーション証明システム。

【請求項６】
生体データとして、指紋、声紋、虹彩、血流及びサインのデータを用いたことを特徴とする請求項１乃至５のいずれか記載のロケーション証明システム。
【請求項７】
ユーザの携帯端末の識別番号を含むユーザに関する情報及びＩＣカードの識別子をユーザ毎に記憶する登録者情報データベースと、位置情報に対応付けて住所情報を記憶する住所情報データベースと、地図情報を記憶する地図情報データベースと、携帯端末を用いたユーザのアクセスを位置及び日時で記録する履歴データベースとに接続され、
携帯端末でＩＣカードの識別子が読み取られ、前記携帯端末から送信された携帯端末の識別番号、ＩＣカードの識別子及び位置情報を受信する通信部と、
受信したＩＣカードの識別子について、前記登録者情報データベースを参照して前記携帯端末の識別番号に対応して予め記憶されているＩＣカードの識別子と比較し、両ＩＣカードの識別子が一致するか否かの個人認証の処理を実行し、
前記個人認証の処理によって両ＩＣカードの識別子が一致する場合に、前記携帯端末から受信した位置情報について、前記住所情報データベースを参照して前記位置情報を住所情報に変換する処理を実行し、
前記地図情報データベースを参照して前記位置情報に該当する地図情報を取得する処理を実行し、
前記携帯端末からのアクセスを前記履歴データベースに記録する処理を実行し、
日時情報を発行するタイムスタンプサーバから日時情報を取得して、ユーザの位置を住所、対応する地図情報及び前記日時情報により証明するロケーション証明書を生成する処理を実行する制御部と、
前記生成されたロケーション証明書を記憶する記憶部とを備えたロケーション認証サーバを有することを特徴とするロケーション証明システム。
【請求項８】
ユーザの携帯端末の識別番号を含むユーザに関する情報及び生体データをユーザ毎に記憶する登録者情報データベースと、物品名と当該物品に付与されたＩＣタグの識別子の情報を記憶する物品情報データベースと、位置情報に対応付けて住所情報を記憶する住所情報データベースと、地図情報を記憶する地図情報データベースと、携帯端末を用いたユーザのアクセスを位置及び日時で記録する履歴データベースとに接続され、
携帯端末でＩＣタグの識別子が読み取られ、前記携帯端末から送信された携帯端末の識別番号、生体データ、位置情報及びＩＣタグの識別子を受信する通信部と、
受信した生体データについて、前記登録者情報データベースを参照して前記携帯端末の識別番号に対応して予め記憶されている生体データと比較し、両生体データが一致するか否かの個人認証の処理を実行し、
前記個人認証の処理によって両生体データが一致する場合に、前記携帯端末から受信した位置情報について、前記住所情報データベースを参照して前記位置情報を住所情報に変換する処理を実行し、
前記地図情報データベースを参照して前記位置情報に該当する地図情報を取得する処理を実行し、
受信したＩＣタグの識別子について、前記物品情報データベースを参照して前記ＩＣタグの識別子に該当する物品名を取得する処理を実行し、
前記携帯端末からのアクセスを前記履歴データベースに記録する処理を実行し、
日時情報を発行するタイムスタンプサーバから日時情報を取得して、物品名、ユーザ及び物品の位置を住所、対応する地図情報及び前記日時情報により証明するロケーション証明書を生成する処理を実行する制御部と、
前記生成されたロケーション証明書を記憶する記憶部とを備えたロケーション認証サーバを有することを特徴とするロケーション証明システム。
【請求項９】
ロケーション認証サーバにおける通信部は、携帯端末から定期的に位置情報を受信し、

ロケーション認証サーバにおける制御部は、定期的に受信した位置情報に基づいて、地図情報に、当該位置情報をプロットして線で結ぶ処理を実行し、物品の移動経路をトレースした地図情報を用いてロケーション証明書を生成する処理を実行することを特徴とする請求項８記載のロケーション証明システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、携帯端末の保有者の位置（ロケーション）を証明するシステムに係り、特に、本人と認証した上でその本人の現在及び過去における位置を証明するロケーション証明システムに関する。

【背景技術】

【０００２】

従来、携帯電話機のＧＰＳ（Global Positioning System）機能を用いてその携帯電話機の位置を知ることができるシステムはあった。

尚、携帯電話機の位置情報を知ることができるシステムの先行技術には、平成１４年２月２８日公開の特開２００２－６４８５３「対象者の所在地確認方法及びその確認システム」（出願人：エヌイーシーアメニプランテクス株式会社、発明者：小林賢司）がある。

【０００３】

この発明は、対象者に装着された移動端末から一定間隔で測位衛星から得られた現在位置情報及び対象者認証コードを、基地局を介して固定端末に送信し、移動端末で異常があれば基地局経由で固定端末に通知することによって、高齢者が事故に遭遇した場合に迅速に身元確認及び事故の発生場所の確認を行うものである。

【０００４】

【特許文献１】特開２００２－６４８５３号公報　（第４頁－第６頁、図１）

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、上記従来の携帯電話機の位置を知ることができるシステムでは、携帯電話機自体の位置を知ることはできるものの、その保有者が確実に携帯電話機と共にその場所にいることまでも証明するものではなく、所有者本人の位置を証明できないという問題点があった。

【０００６】

本発明は上記実情に鑑みて為されたもので、携帯端末の所有者本人及び所持する物品の位置（ロケーション）及び日時を証明するロケーション証明システム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】

【０００７】

本発明は、ロケーション証明システムにおいて、位置情報を通知する機能を備える携帯端末から送信された携帯端末の識別番号、生体データ及び位置情報を受信し、生体データからユーザの個人認証を行い、認証されれば位置情報から当該ユーザの位置を特定し、ユーザの位置及び日時を証明するロケーション証明書を生成するロケーション認証サーバを有することを特徴とする。

【０００８】

本発明は、上記ロケーション証明システムにおいて、ロケーション認証サーバが、携帯端末のユーザからのアクセスがあると、個人認証の処理、位置特定の処理を行い、地図情報データベースから対応する地図情報を取得し、その地図情報を用いて、ユーザの現在位置及び日時を証明するロケーション証明書を生成することを特徴とする。

【０００９】

本発明は、上記ロケーション証明システムにおいて、携帯端末からロケーション証明書の閲覧要求があると、ロケーション認証サーバが、ロケーション証明書のリストを表示出

力し、リストの項目が選択されると、選択された項目に対応するロケーション証明書を閲覧可能としたことを特徴とする。

【００１０】

本発明は、上記ロケーション証明システムにおいて、携帯端末からユーザのロケーション証明書のリストから複数の項目が選択されると、ロケーション認証サーバが、複数項目の住所情報を一つの地図情報上にプロットして時系列に接続する線を描画した表示画面を表示出力することを特徴とする。

【００１１】

本発明は、ロケーション証明システムにおいて、生体データの代わりに携帯端末で読み取られたＩＣカードの識別子を用いて個人認証を行い、認証されれば位置情報から当該ユーザの位置を特定し、ユーザの位置及び日時を証明するロケーション証明書を生成するロケーション認証サーバを有することを特徴とする。

【００１２】

本発明は、ロケーション証明システムにおいて、生体データで個人認証を行い、認証されれば携帯端末で読み取られたＩＣタグの識別子で物品を特定し、位置情報から当該ユーザの位置を特定し、ユーザ及び物品の位置及び日時を証明するロケーション証明書を生成するロケーション認証サーバを有することを特徴とする。

【００１３】

本発明は、上記ロケーション証明システムにおいて、定期的に受信した位置情報に基づいて、地図情報に、当該位置情報をプロットして線で結ぶ処理を実行し、物品の移動経路をトレースした地図情報を用いてロケーション証明書を生成するロケーション認証サーバを有することを特徴とする。

【発明の効果】

【００１４】

本発明によれば、位置情報を通知する機能を備える携帯端末から送信された携帯端末の識別番号、生体データ及び位置情報を受信し、生体データからユーザの個人認証を行い、認証されれば位置情報から当該ユーザの位置を特定し、ユーザの位置及び日時を証明するロケーション証明書を生成するロケーション認証サーバを有するロケーション証明システムとしているので、携帯端末のユーザ本人の位置及び日時を証明できる効果がある。

【００１５】

本発明によれば、ロケーション認証サーバが、携帯端末のユーザからのアクセスがあると、個人認証の処理、位置特定の処理を行い、地図情報データベースから対応する地図情報を取得し、その地図情報を用いて、ユーザの現在位置及び日時を証明するロケーション証明書を生成する上記ロケーション証明システムとしているので、ユーザの現在位置及び日時を、地図情報を用いて容易に証明できる効果がある。

【００１６】

本発明によれば、携帯端末からロケーション証明書の閲覧要求があると、ロケーション認証サーバが、ロケーション証明書のリストを表示出力し、リストの項目が選択されると、選択された項目に対応するロケーション証明書を閲覧可能とした上記ロケーション証明システムとしているので、ユーザの過去の特定日時における位置を容易に証明できる効果がある。

【００１７】

本発明によれば、携帯端末からユーザのロケーション証明書のリストから複数の項目が選択されると、ロケーション認証サーバが、複数項目の住所情報を一つの地図情報上にプロットして時系列に接続する線を描画した表示画面を表示出力する上記ロケーション証明システムとしているので、ユーザの過去の特定期間における位置を容易に証明できる効果がある。

【００１８】

本発明によれば、生体データの代わりに携帯端末で読み取られたＩＣカードの識別子を用いて個人認証を行い、認証されれば位置情報から当該ユーザの位置を特定し、ユーザの

位置及び日時を証明するロケーション証明書を生成するロケーション認証サーバを有するロケーション証明システムとしているので、ＩＣカードを用いてユーザ本人の位置及び日時を証明できる効果がある。

【００１９】

本発明によれば、生体データで個人認証を行い、認証されれば携帯端末で読み取られたＩＣタグの識別子で物品を特定し、位置情報から当該ユーザの位置を特定し、ユーザ及び物品の位置及び日時を証明するロケーション証明書を生成するロケーション認証サーバを有するロケーション証明システムとしているので、ユーザ本人及び物品の位置及び日時を証明できる効果がある。

【００２０】

本発明によれば、定期的に受信した位置情報に基づいて、地図情報に、当該位置情報をプロットして線で結ぶ処理を実行し、物品の移動経路をトレースした地図情報を用いてロケーション証明書を生成するロケーション認証サーバを有する上記ロケーション証明システムとしているので、物品の移動経路を容易に把握できる効果がある。

【発明を実施するための最良の形態】

【００２１】

本発明の実施の形態について図面を参照しながら説明する。

本発明の実施の形態に係るロケーション証明システムは、生体情報（生体データ）を用いて本人認証を行い、携帯端末の位置通知機能を利用して位置を特定し、携帯端末保有者（ユーザ）の位置及び日時を証明するロケーション証明書を生成するものであり、携帯端末の保有者は希望する場所及び日時に自己のロケーションを容易に証明できるものである。

【００２２】

また、本発明の実施の形態に係るロケーション証明システムは、生体情報を用いて本人認証を行い、携帯端末の位置通知機能を利用して位置を特定し、携帯端末保有者の位置及び日時を履歴情報として記録し、携帯端末の保有者からの要求により過去の特定期間におけるロケーションを証明するロケーション証明書を生成するものであり、携帯端末の保有者は希望する場所及び日時に自己のロケーションを容易に証明できるものである。

【００２３】

本発明の実施の形態に係るロケーション証明システム（本システム）の構成について図１を参照しながら説明する。図１は、本発明の実施の形態に係るロケーション証明システムの構成ブロック図である。

本発明の実施の形態に係るロケーション証明システム（本システム）は、図１に示すように、ロケーション認証サーバ１と、登録者情報ＤＢ２ａと、住所情報ＤＢ２ｂと、地図情報ＤＢ２ｃと、履歴ＤＢ２ｄと、タイムスタンプサーバ３と、個人情報登録端末４と、携帯端末５とを基本的に有している。

【００２４】

本システムにおける各部を具体的に説明する。

ロケーション認証サーバ１には、登録者情報ＤＢ２ａ、住所情報ＤＢ２ｂ、地図情報ＤＢ２ｃ及び履歴ＤＢ２ｄにアクセス可能に接続され、タイムスタンプサーバ３から正確な時刻情報を取得する。

また、ロケーション認証サーバ１は、公衆回線を介して携帯端末５と接続可能となっている。

また、ロケーション認証サーバ１には、個人情報登録端末４が接続されている。

実際には、携帯端末５は複数存在するものであり、個人情報登録端末４も複数備えるようにしてもよい。

【００２５】

ロケーション認証サーバ１の基本的な機能は、主に、携帯端末の保有者の登録機能、携帯端末の保有者の位置認証機能、ロケーション証明書の生成・発行機能がある。これら機能については本システムの動作で具体的に説明する。

【００２６】
登録者情報ＤＢ（データベース）２ａは、個人情報登録端末４から入力された登録者の情報を記憶するデータベースである。登録される個人情報としては、携帯端末の識別番号（例えば携帯電話の番号等）、氏名、性別、年齢、所属する企業名、所属、企業住所等があり、更に個人毎に本人認証を行うためのバイオメトリックスデータ（生体データ）が記憶されている。
また、登録者情報ＤＢ２ａに、ロケーション証明書の発行形態も登録しておくことも可能である。例えば、発行形態を紙媒体とするか又は電子媒体にするかが登録される。
【００２７】
バイオメトリックスデータには、指紋、声紋、虹彩、血流、サイン等のデータがある。
バイオメトリックスデータは、登録者個人で異なる形態としてもよい。例えば、Ａさんは指紋データをバイオメトリックスデータとし、Ｂさんは声紋データをバイオメトリックスデータとしてもよい。
また、登録者が複数のバイオメトリックスデータを利用できるようにしてもよい。例えば、Ｃさんは指紋と声紋の両方のバイオメトリックスデータが登録されており、いずれかを任意に使い分けられるようにすることも考えられる。
【００２８】
住所情報（座標）ＤＢ（データベース）２ｂは、携帯端末５から通知された位置情報（座標情報）を住所情報に変換するためのデータベースである。従って、住所情報ＤＢ２ｂ内には、座標データに対する住所データがテーブル形式等で記憶されている。
【００２９】
地図情報ＤＢ（データベース）２ｃは、携帯端末５の保有者の位置を視覚的に表現するための地図データが記憶されている。
地図情報ＤＢ２ｃは、ロケーション認証サーバ１から座標情報又は住所情報の入力を受けると、該当する地図部分のデータをロケーション認証サーバ１に出力する。
【００３０】
履歴ＤＢ２ｄは、登録者に対するロケーション認証を行った履歴を記憶するデータベースである。
履歴ＤＢ２ｄには、携帯端末の識別番号、年月日、時刻、経度、緯度、住所、企業名、対象者名、行動内容等が記録される。
【００３１】
タイムスタンプサーバ３は、公正を担保する第三者機関によって運用されるサーバであり、ロケーション認証サーバ１に正確な年月日、時刻を付与するサーバである。
具体的には、ロケーション認証サーバ１がタイムスタンプサーバ３に現在時刻（年月日を含む）を問い合わせると、タイムスタンプサーバ３が現在の時刻をロケーション認証サーバ１に出力し、ロケーション認証サーバ１は正確な現在時刻を得るものである。
公正を担保するため第三者機関のタイムスタンプサーバ３を利用しているが、イントラネットでの利用を想定する場合には、ロケーション認証サーバ１内で年月日、時刻を付与するようにしてもよい。
【００３２】
個人情報登録端末４は、ロケーション認証サーバ１に個人情報を登録するための端末（コンピュータ）である。
個人情報の登録は、バイオメトリックスのデータタイプで異なり、指紋であれば登録者に出向いてもらい、個人情報登録端末に接続された指紋読み取り装置を用いて指紋の入力を行う。入力された登録者の指紋データはロケーション認証サーバ１に出力され、その登録者に対応付けて登録者情報ＤＢ２ａに登録される。無論、登録者は、登録前に免許証等で本人を確認して登録作業に入ることになる。
【００３３】
また、声紋であれば登録者がマイクから音声を入力し、登録者情報ＤＢ２ａに登録する。この場合、本人認証を容易にするために、特定のワードを登録し、認証時にも同じワー

ドを利用するようにしてもよい。

【００３４】

また、虹彩であればデジタルカメラで撮影し、登録者情報ＤＢ２ａに登録する。血流であれば、専用の測定装置を用いて測定し、登録者情報ＤＢ２ａに血流のデータが登録される。サインであれば、ペン入力装置からサインを直接読み込むか、用紙に書かれたサインをスキャナで読み取って、登録者ＤＢ２ａに登録する。

【００３５】

携帯端末５は、位置情報通知機能と個人認証機能を備えた端末である。端末としては、高性能携帯電話機、高性能ＰＨＳ、ＰＤＡ（個人情報端末）、ノートＰＣ（パソコン）等が考えられる。

位置情報通知機能としては、一般的にＧＰＳ（Global Positioning System）機能、その他の位置検出機能を備えた端末が考えられる。

個人認証機能としては、指紋読み取り装置、音声入力装置（マイク）、虹彩撮影装置（デジタルカメラ）、血流測定装置、サイン読み取り装置のいずれか又は複数を備えた端末が考えられる。

【００３６】

携帯端末５から個人認証のためのバイオメトリックスデータが入力されると、携帯端末５の識別番号と共にロケーション認証サーバ１に送信され、ロケーション認証サーバ１で本人認証が為されて、携帯端末５の位置情報がロケーション認証サーバ１に取り込まれることになる。

尚、通常、携帯端末５から入力されたバイオメトリックスデータは、セキュリティを考慮して暗号化されて送付され、ロケーション認証サーバ１で受信後、復号される。

【００３７】

次に、本システムのロケーション認証サーバ１の内部構成について、図２を参照しながら説明する。図２は、ロケーション認証サーバの内部構成を示す構成ブロック図である。

ロケーション認証サーバ１は、図２に示すように、通信部１１と、記憶部１２と、制御部１３とから基本的に構成されている。

【００３８】

通信部１１は、公衆回線（インターネット、携帯電話網）を介してユーザの携帯端末とデータ送受信を行う。

また、通信部１１は、専用線等で接続されているタイムスタンプサーバ３とのデータ送受信を行うものである。

【００３９】

記憶部１２は、制御部１３で起動される処理プログラムを格納している。

また、記憶部１２は、携帯端末５からアクセスがあった場合に、携帯端末５に表示させる表示画面のデータを記憶している。

尚、記憶部１２は、ハードディスク等の記憶装置で構成される。

【００４０】

制御部１３は、ロケーション認証サーバ１全体の制御を行うものであり、ＣＰＵ（Central Processing Unit）、主メモリ（図示せず）等で構成される。

また、制御部１３は、記憶部１２に格納された処理プログラムが主メモリにロードされると、ユーザ登録、本人認証、位置認証、タイムスタンプ取得、ロケーション証明書生成・発行、履歴記憶の処理を実行させる処理手段を実現させるものである。

【００４１】

また、制御部１３は、データを一時蓄える主メモリ（ＲＡＭ）を備えている。

具体的には、制御部１３は、携帯端末６からの指示に基づいて、記憶部１２に格納されたプログラムを読み出して各手段を起動し、携帯端末５からの指示に応じた処理を実行させる。

【００４２】

次に、制御部１３によって実現される各手段の概要について説明する。

登録手段は、登録者の個人情報（登録者のバイオメトリックスデータを含む）を登録者情報ＤＢ２ａに登録する処理を実行する。

本人認証手段は、通信部１１を介して入力された登録者のバイオメトリックスデータと登録者ＤＢ２ａに登録されたバイオメトリックスデータとを携帯端末の識別番号をキーとして照合し、登録者本人であるか否かを判別し、本人である場合に、登録者ＤＢ２ａから当該本人の個人情報を読み込み、ロケーション証明書生成・発行手段に出力する。

【００４３】

位置認証手段は、携帯端末５が通知した位置情報（座標情報）を、通信部１１を介して入力し、住所情報ＤＢ２ｂを参照して現在位置の住所情報（住所データ）に変換し、続いて地図情報ＤＢ２ｃから当該位置情報又は住所情報に相当する地図データを読み込み、現在位置の住所情報、地図データ等をロケーション証明書生成・発行手段に出力する。

【００４４】

タイムスタンプ取得手段は、入力されたバイオメトリックスデータで本人認証が為されると、タイムスタンプサーバ３にアクセスして、日時のデータの取得要求を、通信部１１を介して送信し、受信した日時のデータをロケーション証明書生成・発行手段に出力する。

【００４５】

ロケーション証明書生成・発行手段は、本人認証手段から認証された個人情報を入力し、位置認証手段から現在位置の住所情報、地図データ等を入力し、タイムスタンプ取得手段から日時データを入力し、これら情報及びデータからロケーション証明書を作成（生成）する手段である。

作成されたロケーション証明書は特定のメールアドレスに添付ファイルで送信して発行する。メールアドレスへの送信の代わりに、ロケーション証明書を書面で送付して発行してもよい。

【００４６】

また、ロケーション証明書生成・発行手段は、登録者からのロケーション証明書発行の要求を、通信部１１を介して入力すると、履歴記憶手段から履歴情報を読み込んでロケーション証明書を作成する。この作成されたロケーション証明書もメールアドレス又は特定の住所に送付して発行する。

【００４７】

履歴記憶手段は、上記各手段で取得されたデータの内容を履歴情報として日時と共に履歴ＤＢ２ｄに記憶する。履歴情報としては、登録者の個人情報、登録者からのアクセス日時、緯度経度の位置情報、住所情報、地図データ等がある。

【００４８】

次に、本システムの動作について説明する。

まず、本システムのロケーション認証のサービスを受けることを希望する者は、個人情報登録端末４から個人情報の登録を行う。個人情報登録端末４は、専用のオペレータが入力・登録作業を行うことになる。

登録の際には、登録者は、個人情報登録端末４に出向いて、本人を確認できるもの、例えば運転免許証を持参して、本人を確認することが行われる。更に、登録者は本人のバイオメトリックスデータを入力装置から入力することになる。

個人情報登録端末４から入力された登録者のデータは、ロケーション認証サーバ１に出力され、登録者情報ＤＢ２ａに登録者に対応付けられて記憶される。

【００４９】

上記の例では、個人情報登録端末４から本サービスを受けようとする本人を登録する操作が為されたが、携帯電話等の携帯端末５から簡易にユーザ登録を行えるようにしてもよい。

例えば、携帯電話等の携帯端末５からロケーション認証サーバ１のウェブサイトにアクセスし、ユーザの新規登録を選択して、ユーザ登録に必要な情報（氏名、年齢、性別、住所等の情報）を入力し、バイオメトリックスデータを登録すると、当該ユーザにはユーザ

ＩＤとパスワードの割り当を行う。以降、本サービスを受けようとする登録者は、当該ウェブサイトにユーザＩＤとパスワードを用いてログインする。

尚、登録されたデータは、登録者情報ＤＢ２ａに記憶され、その時、ユーザの携帯端末５の識別番号も同時に記憶される。

【００５０】

次に、本システムにおけるロケーション認証処理を説明する。

本システムにおいて、ロケーション証明書発行の態様は、大別すると、二通りの方法がある。

第１の方法は、登録者が現在いる場所を証明してもらうために、ロケーション認証サーバ１にアクセスしてロケーション証明書の発行を要求する方法である。

第２の方法は、登録者は携帯端末５を利用する際に、バイオメトリックスによる個人認証を行うようにし、その後に、ロケーション認証サーバ１に対して過去の履歴におけるロケーション証明書の発行を要求する方法がある。

【００５１】

第１の方法であるならば、ロケーション認証サーバ１は、独立したウェブサーバであれば機能する。携帯端末５は、ウェブサーバのロケーション認証サーバ１にアクセスしてロケーション認証を要求することになる。

第２の方法であるならば、ロケーション認証サーバ１は、通信事業者（キャリア）又はインターネットプロバイダーの通信システムに組み込まれている必要がある。携帯端末５を使用した通話（ＩＰ電話を含む）、メール送受信、ウェブ閲覧等の通常の通信機能を実現しつつ、ロケーション認証も同時に行う必要があるためである。

【００５２】

次に、第１の方法によるロケーション証明書発行処理について図３を参照しながら説明する。図３は、本発明の実施の形態に係るロケーション認証システムにおけるロケーション証明書発行処理を示すフローチャートである。

図３に示すように、携帯端末５からロケーション認証サーバ１にアクセスがある（Ｓ１）と、続いて、携帯端末５に備えられたバイオメトリックスデータの入力装置からバイオメトリックスデータを入力する。図３では、バイオメトリックスデータとして声紋を用いているので、マイクから入力された音声（声紋）がロケーション認証サーバ１に入力され、一時記憶される（Ｓ２）。

【００５３】

次に、ロケーション認証サーバ１では、入力・記憶したバイオメトリックスデータと登録者情報ＤＢ２ａに記憶されている登録者のバイオメトリックスデータとを照合する（Ｓ３）。この照合に際して、携帯端末５の識別番号をキーとして登録者情報ＤＢ２ａを参照し、該当する登録されたバイオメトリックスデータを読み込み、携帯端末５から入力されたバイオメトッリクデータとの比較を行う。

【００５４】

そして、両バイオメトリックスデータが一致するか否かを判断して登録者であるか否かを判断する（Ｓ４）。登録者として認められない場合（Ｎｏの場合）、登録者と認められなかった旨を携帯端末５に通知して処理を終了する。ここで、処理を終了せずに、処理Ｓ２に戻って、声紋の入力をやり直すようにしてもよい。

【００５５】

登録者として認められる場合（Ｙｅｓの場合）、携帯端末５が通知した位置情報から住所情報ＤＢ２ｂを参照して、位置情報（座標情報）から現在位置の住所を取得する（Ｓ６）。

続いて、地図情報ＤＢ２ｃから位置情報（又は住所情報）から該当する地図データを取得する（Ｓ７）。

【００５６】

次に、対象の登録者の氏名、登録者の関連情報、現在位置の住所、現在位置の地図等に基づいてロケーション証明書を作成し、タイムスタンプサーバ３からの年月日及び時刻（

日時）を当該ロケーション証明書に記録して生成し、発行する（Ｓ８）。
そして、履歴ＤＢ２ｄに履歴を記録して（Ｓ９）、処理を終了する。
【００５７】
上記例では、ロケーション証明書に日時を記録するようにしているが、処理Ｓ６の前処理で、タイムスタンプサーバ３に時刻を要求して時刻を取得し、処理８で全てのデータをまとめ上げてロケーション証明書を一度に作成するようにしてもよい。
【００５８】
次に、第２の方法によるロケーション証明書発行処理について説明する。
第２の方法では、携帯端末５が通話、電子メールの送受信、ウェブサイトの閲覧等のキャリア（通信事業者）に対して行う際に、個人認証を行う。ここで、電子メールの送受信、ウェブサイトの閲覧であれば、キャリアではなく、インターネットプロバイダーで個人認証することも可能である。
この個人認証で本人と認められると、ロケーション認証サーバ１は、タイムスタンプサーバ３に時刻情報を要求し、タイムスタンプサーバ３から時刻情報（年月日及び時刻）を受け取る。
【００５９】
更に、ロケーション認証サーバ１は、携帯端末５の位置情報通知機能によって通知された位置情報（緯度・経度）から住所情報ＤＢ２ｂを検索して住所を取得する。
その後、ロケーション認証サーバ１は、履歴ＤＢ２ｄに年月日、時刻、緯度・経度、住所、企業名、対象者名、行動内容（例えば、電子メールの受信）を記憶する。
そして、携帯端末５による通話等が為され、通信処理が終了する。
【００６０】
その後、登録者から携帯端末５を用いてロケーション認証サーバ１にロケーション証明書発行の要求手続があると、ロケーション認証サーバ１は、その要求内容に従って、履歴ＤＢ２ｄから必要な情報を読み出し、ロケーション証明書を作成して発行する。
尚、このロケーション証明書の発行要求を行う際にも、登録者はバイオメトリックスを用いて個人認証を行う。
【００６１】
登録者からのロケーション認証サーバ１へのロケーション証明書の発行要求の例としては、特定の年月日、時間帯を指定して、当該登録者の一連の位置履歴を証明書として発行することを要求することが考えられる。また、別の例としては、特定の年月日、特定の時刻の一つ又は複数のロケーションについて証明書の発行を要求することも考えられる。
【００６２】
また、ロケーション証明書には、地図情報ＤＢ２ｃを参照して該当する地図を取得し、その地図を貼り付けるようにしてもよい。
更に、ロケーション証明書には、改竄防止としてドキュメントに書き換え不能の処理を施すものである。
【００６３】
また、携帯電話機の表示画面でロケーション証明書を閲覧できるようにすることも考えられる。また、携帯電話機の表示画面でのロケーション証明書の閲覧に際して、地図を表示させ、当該地図内に移動をトレースした表示画面を生成することも考えられる。この場合、ロケーション認証サーバ１は、ウェブサーバの機能を備えているものとする。
【００６４】
次に、携帯電話機の画面上でロケーション証明書を閲覧する方法について図５を参照しながら説明する。図５は、ロケーション認証サーバにおけるロケーション証明書の閲覧処理を示すフローチャートである。
登録者は、携帯電話の携帯端末を用いてロケーション認証サーバ１のウェブサイトにアクセスする。このサイトへのログインには、ロケーション認証サーバ１は、ユーザＩＤとパスワードの入力を促す画面を表示し、ユーザＩＤとパスワードの入力を確認する（Ｓ１１）と、登録者情報ＤＢ２ａ参照して、ユーザＩＤに対してパスワードが正当であるかど

うか、つまり、正当な登録者であるかどうかを判断する（Ｓ１２）。

【００６５】

処理Ｓ１２の判断によって、正当な登録者であれば（Ｙｅｓの場合）、更に登録者情報ＤＢ２ａを参照して登録してある生体認証方法を選択する（Ｓ１３）。

尚、サイトへのログインにユーザＩＤとパスワードの入力を不要とし、携帯端末５の識別番号によって登録者情報ＤＢ２ａを参照し、登録してある生体認証方法をロケーション認証サーバ１が選択するようにしてもよい。

【００６６】

次に、ロケーション認証サーバは、生体データの入力を促す画面を表示し、選択された認証方法によって生体データが入力されたかどうか判断し（Ｓ１４）、選択された認証方法で生体データが入力されると（Ｙｅｓの場合）、登録者情報ＤＢ２ａを参照し、登録してある生体データと比較して一致するか否かを判断する（Ｓ１５）。

【００６７】

入力された生体データが登録者のものであれば（Ｙｅｓの場合）、本人認証が為されたことになり、ロケーション認証サーバは、登録者のロケーション履歴のリストを表示する（Ｓ１７）。

【００６８】

表示されたリストから登録者が特定日時のロケーション証明書の項目を選択すると、選択されたロケーションの証明書を表示して（Ｓ１７）、ロケーション証明書を閲覧可能とする。

尚、ロケーション証明書の発行の際には、位置情報又は住所情報から地図を表示し、その地図上に証明するロケーションをプロットするようにしてもよい。更に、リストから複数のロケーション証明書の項目を選択した場合、プロットしたロケーションの複数の点を時系列に接続する線を描画して表示画面に表示出力するようにしてもよい。

【００６９】

本システムによれば、携帯端末５の保有者が携帯端末５に設けられた生体データ入力装置を用いて個人認証を行い、本人と認められれば、ロケーション認証サーバは携帯端末５から通知された位置情報を基に住所を特定し、タイムスタンプサーバ３から日時を取得して履歴を記憶すると共に、ロケーション証明書を生成して発行するようにしているので、携帯端末５の保有者本人の位置を証明できる効果がある。

【００７０】

尚、本システムは、例えば、営業日報に添付される証明書、若しくは、配送業者における配達記録の証明書を発行するのに利用可能である。

【００７１】

次に、第２の方法を実現するシステムについて図４を参照しながら説明する。図４は、本発明の第２の実施の形態に係るロケーション証明システムの構成ブロック図である。尚、図１のシステムと同様の構成部分には、同一の符号を付している。

【００７２】

以下、図１のシステムとの相違点を中心に説明する。

キャリアサーバ３０は、携帯端末５を用いた通信サービスを行う通信事業者が管理し、携帯端末５による通話制御機能、電子メールの送受信制御機能、ブラウザ機能等を備えている。

キャリアサーバ３０は、携帯端末５からアクセスがあると、正規のユーザであることを認証して、ロケーション認証サーバ１′に携帯端末５の番号と生体データとを出力する。そして、当該携帯端末５を用いた「行動内容（電子メールの送信、受信、通話等）」を示すデータをロケーション認証サーバ１′に出力する。

【００７３】

ロケーション認証サーバ１′の構成は、図２に示したロケーションサーバ１とほぼ同様である。

ロケーション認証サーバ１′は、キャリアサーバ３０を有する通信事業者によって管理

される。
ロケーション認証サーバ１′は、キャリアサーバ３０から携帯端末５の番号と生体データとが入力されると、生体認証を行って、キャリアサーバ３０を介して位置情報を取得して住所に変換し、タイムスタンプサーバ３からタイムスタンプを取得し、更にキャリアサーバ３０から「行動内容」の入力を受けて、履歴ＤＢ２ｄに記憶する。
尚、ロケーション認証サーバ１′は、キャリアサーバ３０と一体に構成されてもよい。
【００７４】
次に、別の実施の形態（第３の実施の形態）に係るロケーション証明システムについて説明する。
携帯電話機にＩＣタグ読み取り装置、ＩＣカードリーダ等の読み取り装置を備えるものである。ＩＣタグとは、非接触の無線ＩＣタグで、ＩＣタグ読み取り装置で、ＩＣタグのＩＤ（識別子）を読み込むようになっている。また、ＩＣカードリーダは、ＩＣタグ読み取り装置と同様の機能を備えており、非接触型のＩＣカードリーダもある。
【００７５】
また、ロケーション認証サーバ１は、携帯電話機の携帯端末の位置情報の管理及びロケーション証明書の生成・発行又は閲覧を行うと共に、読み取られたＩＣタグ、ＩＣカードの情報で物品（商品）又はサービスを特定し、その物品等の追跡も行い、登録者又は当該物品の管理者等の要求によって追跡画面を作成し、携帯端末の表示画面に表示させる。
【００７６】
尚、生体認証の代わりに、ＩＣカードを読み取らせて本人認証とすることも考えられる。
この場合、登録者情報ＤＢ２ａにはユーザ毎にＩＣカードのＩＤを記憶しておき、ＩＣカードのＩＤが携帯端末５から入力されると、その携帯端末５の識別番号をキーとして登録者情報ＤＢ２ａを参照し、識別番号に対応するＩＣカードのＩＤを読み込み、携帯端末から入力されたＩＤと比較し、一致すれば本人（個人）が認証されたことになるものである。
【００７７】
また、ＩＣタグをレンタカーの一部に取り付け、利用を開始する前に、ＩＣタグのＩＤを読み込み、利用を終了する時に、再度ＩＣタグのＩＤを読み込むようにすれば、レンタカーの移動経路を追跡することが可能となる。この処理については、以下に説明する。
【００７８】
次に、ロケーション証明システムにおけるＩＣタグの処理について図６を参照しながら説明する。図６は、ロケーション証明システムにおけるＩＣタグの処理を示すフローチャートである。尚、図６の処理は、図３における処理Ｓ８の代わりに実行されるものである。つまり、生体データによる本人認証を行った上で、位置情報から住所情報を取得し、該当する地図情報を取得した状態から図６の処理が為されるものである。
【００７９】
また、図６の処理を実行するためには、ロケーション証明システムに、ＩＣタグが付された物品に関する物品情報ＤＢが設けられている。物品情報ＤＢには、物品に付されたＩＣタグの識別子（ＩＤ）と当該物品の名称が対応付けられて記憶されている。
【００８０】
図６に示すように、携帯電話機ではＩＣタグのＩＤを読み込んで、そのＩＤを携帯端末の識別番号と共にロケーション認証サーバに送信するようになっているので、ロケーション認証サーバは、入力されたＩＣタグのＩＤを読み取り、物品情報ＤＢを参照してＩＤに対応する物品名を特定する（Ｓ３１）。
【００８１】
次に、携帯電話機のＧＰＳ機能を用いて位置情報を取得する（Ｓ３２）。続いて、地図情報に取得した位置情報をプロットし、プロットした点を順に結ぶ線を描画し、データを保存する（Ｓ３３）。そして、再度、ＩＣタグのＩＤの入力があるか否か判断し（Ｓ３４）、再度ＩＣタグのＩＤの入力があれば（Ｙｅｓの場合）、処理を終了し、再度ＩＣタグ

のＩＤの入力がなければ（Ｎｏの場合）、処理Ｓ３２に戻り、処理Ｓ３２，Ｓ３３を繰り返す。このようにして位置情報は定期的に取得される。尚、データの保存に際し、タイムスタンプサーバから日時情報を取得して共に保存するようにしてもよい。

【００８２】

このようにして、ＩＣタグのＩＤが読み取られて、携帯電話機によってロケーションの登録が為されると、携帯電話機のＧＰＳ機能によってＩＣタグが付された物品の移動経路が地図情報上にプロットされ、再度ＩＣタグのＩＤを読み込むと、物品の利用を終了したとして、移動経路のプロットを停止するようになっている。

尚、上記プロットした点を取得した順（時系列）に結ぶ線が地図情報上に描画されると、物品の移動経路をトレースするものとなる。

【００８３】

既に、本人認証、住所情報取得、地図情報取得が為され、その地図情報上に移動経路のプロット及びトレース線の描画が為された状態で、タイムスタンプサーバからはプロット毎に日時情報を取得して、それらのデータを統一してロケーション証明書を生成することになる。

【００８４】

これにより、ＩＣタグが貼付された物品の移動経路を容易に判別できる。この場合、移動経路を確認するのは、利用者本人というより、レンタカー等の物品を貸し出す事業者となる。当該事業者は、貸し出した物品の移動状況を容易に管理できるものである。

【産業上の利用可能性】

【００８５】

本発明は、携帯端末の所有者本人、更に所持する物品のロケーション及び日時を証明するロケーション証明システムに好適である。

【図面の簡単な説明】

【００８６】

【図１】本発明の実施の形態に係るロケーション証明システムの構成ブロック図である。

【図２】ロケーション認証サーバの内部構成を示す構成ブロック図である。

【図３】本発明の実施の形態に係るロケーション認証システムにおけるロケーション証明書発行処理を示すフローチャートである。

【図４】本発明の第２の実施の形態に係るロケーション証明システムの構成ブロック図である。

【図５】ロケーション認証サーバにおけるロケーション証明書の閲覧処理を示すフローチャートである。

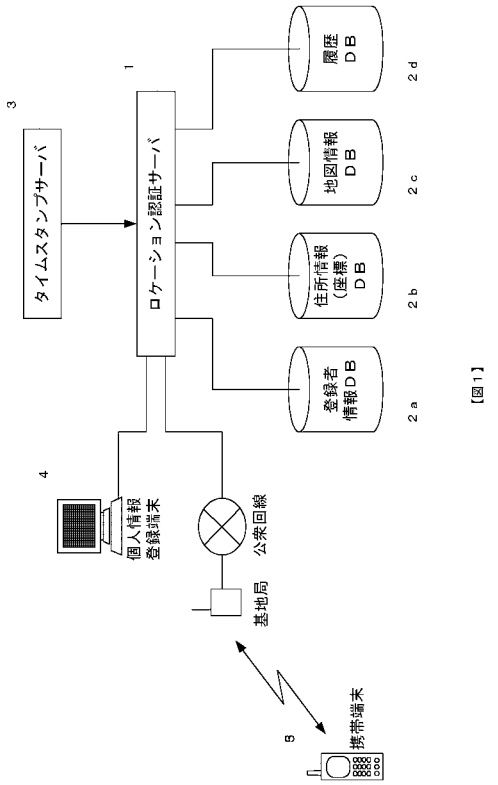
【図６】ロケーション証明システムにおけるＩＣタグの処理を示すフローチャートである。

【符号の説明】

【００８７】

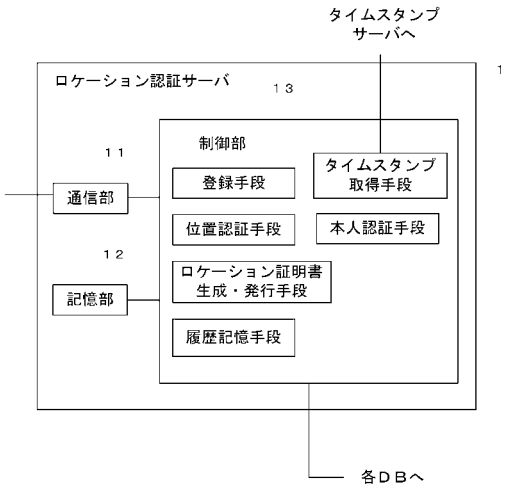
１，１′…ロケーション認証サーバ、　２ａ…登録者情報ＤＢ、　２ｂ…住所情報ＤＢ、　２ｃ…地図情報ＤＢ、　２ｄ…履歴ＤＢ、　３…タイムスタンプサーバ、　４…個人情報登録端末、　５…携帯端末

【図１】



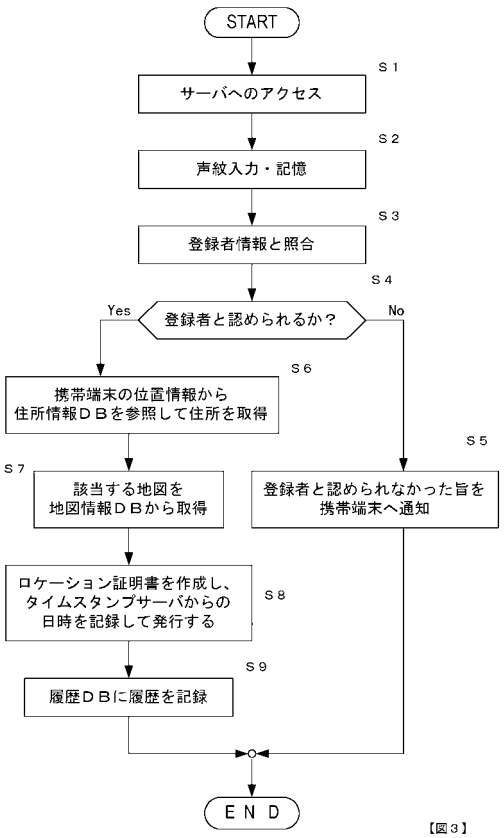

【図１】

【図２】



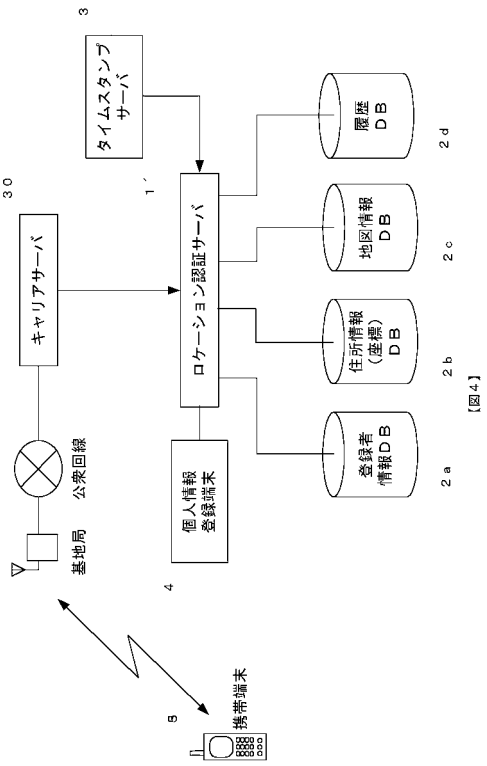

【図２】

【図３】



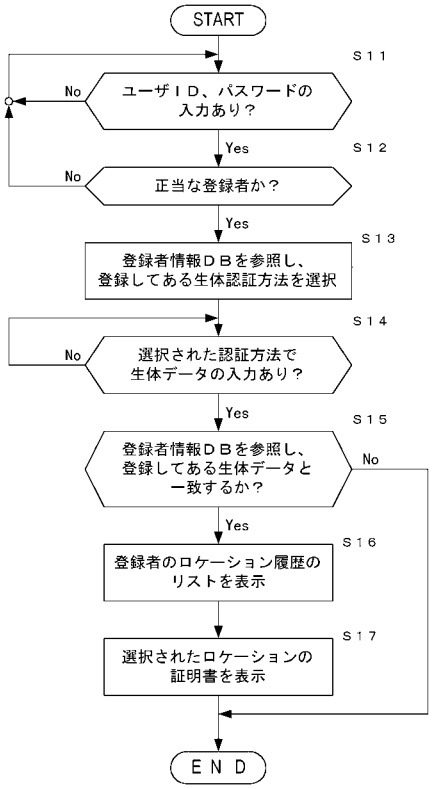

【図３】

【図４】



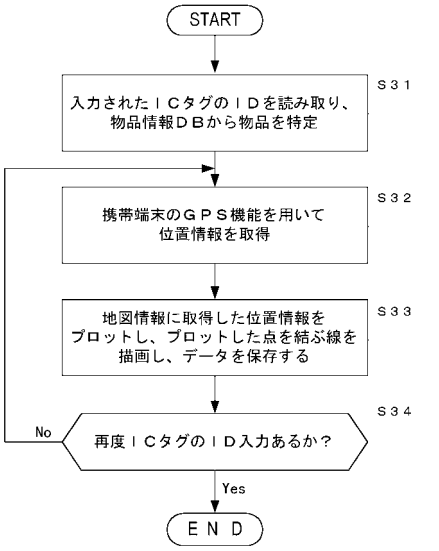

【図４】

【図５】


START
S11
No
ユーザＩＤ、パスワードの
入力あり？
Yes
S12
No
正当な登録者か？
Yes
S13
登録者情報ＤＢを参照し、
登録してある生体認証方法を選択
S14
No
選択された認証方法で
生体データの入力あり？
Yes
S15
登録者情報ＤＢを参照し、
登録してある生体データと
一致するか？
No
Yes
S16
登録者のロケーション履歴の
リストを表示
S17
選択されたロケーションの
証明書を表示
ＥＮＤ

【図５】

【図６】


START
S31
入力されたＩＣタグのＩＤを読み取り、
物品情報ＤＢから物品を特定
S32
携帯端末のＧＰＳ機能を用いて
位置情報を取得
S33
地図情報に取取得した位置情報を
プロットし、プロットした点を結ぶ線を
描画し、データを保存する
S34
No
再度ＩＣタグのＩＤ入力あるか？
Yes
ＥＮＤ

【図６】

フロントページの続き

| (51)Int.Cl.[7] | FI | テーマコード（参考） |
|---|---|---|
| | H04L 9/00 675Z | |