

明 細 書

発明の名称：

位置特定システム、位置特定装置、位置特定方法、位置特定プログラム及びコンピュータで読み取り可能な記録媒体並びに記録した機器

技術分野

[0001] 本発明は、位置特定システム、位置特定装置、位置特定方法、位置特定プログラム及びコンピュータで読み取り可能な記録媒体並びに記録した機器に関する。

背景技術

[0002] 従来、移動端末や物体等の位置を検出・測定する技術として、GPS (Global Positioning System) を用いた位置測定が知られている。また、GPS電波が透過しにくい屋内での測位も可能な手段として、基地局やアクセスポイント等との無線通信の状況によって位置を測定するものが知られている。

[0003] このような屋内における一般的な位置測定の方法としては、Wi-Fi測位、基地局測位、音波測位、Bluetooth測位 (BLEビーコン)、可視光測位、カメラ画像測位、気圧測位、PDR (Pedestrian Dead-Reckoning)、地磁気測位、GPS、IMES (Indoor Messaging System) 等、様々な方法がある。これらのうち、スマートフォン端末等を取り出すことなくタッチレスに端末自身を測位できる物理的な利用方法として、気圧、PDR、地磁気、無線、光を用いるものが挙げられる。

[0004] また、一般的な位置を測定するアルゴリズムとして、電波や光の強度を測定する三角測量、周期的な電波や光を対象物との通信角度や時間を測定するTOF、相対性理論に基づいた原子時計等の精度の高い複数の装置の位置情報から測定する方法、加速度、ジャイロ、地磁気等のセンサから移動の方向と速度を推計するPDR、環境特有の物理情報を予めデータベース化してマッチング処理から位置測定を行ういわゆるフィンガープリンティング法等が知られている (特許文献1、特許文献2、非特許文献1)。

[0005] 位置測定には、これら物理的な利用方法とアルゴリズムを組み合わせで利用していることが多い。これらの無線通信には、基地局や端末等が周期的に発信するビーコン信号を受信することにより、ビーコン領域への端末の出入りを検知するという手法がある。このビーコン信号として、極めて少ない消費電力で通信可能で低コスト、汎用的なBLE (Bluetooth Low Energy) 規格によるBLEビーコンがある。BLEビーコンは、無線規格の中でも極めて低消費で汎用的である。このBLEビーコンを用いてスマートフォン端末等を持って移動している人を一人ずつ高速かつ高精度に捕捉・区別・認識できると、単なるロケーション判定のためだけでなく、鍵の代わりに近づくだけで開錠できたり必要な支払いを済ませられたり等、認証に付随する行動をタッチレスで自動化できると思われる。このため、位置精度を向上しようと試みられている（特許文献3、4）。

例えば、支払いの認証にかかわるセキュリティのために、ビーコン基地局と端末をそれぞれ承認する仕組みも開発されている（特許文献5）。しかしながら、位置の測定とは連動できていないため、支払い者を特定するために、レジマシーン等に顔を表示する等して商品を渡す等の相手を手動で特定している。その他にも、NFCや2次元バーコード等で支払い端末の認証を行う等の手法も提案されているが、いずれもタッチレスに位置測定と支払いとを連動するセキュリティ手法は報告されていない。

先行技術文献

特許文献

[0006] 特許文献1：特開2008-104029号公報

特許文献2：特表2012-521557号公報

特許文献3：特開2015-200504号公報

特許文献4：特開2017-17491号公報

特許文献5：特表2017-501620号公報

非特許文献

[0007] 非特許文献1：He, Suining, Tianyang Hu, and S-H. Gary Chan. "Contour-b

ased trilateration for indoor fingerprinting localization.” Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, ACM, 2015.

発明の概要

発明が解決しようとする課題

- [0008] 本発明の目的の一は、屋内においても位置検出を安定的に行うことのできる位置特定システム、位置特定装置、位置特定方法、位置特定プログラム及びコンピュータで読み取り可能な記録媒体並びに記録した機器を提供することにある。

課題を解決するための手段及び発明の効果

- [0009] 本発明の第1の側面に係る位置特定システムによれば、位置を特定する対象となる個人が携帯する個人携帯端末と、前記個人携帯端末の位置を特定する位置特定装置とを備える位置特定システムであって、前記個人携帯端末は、前記位置特定装置に対し、位置の特定に用いる位置特定信号を発信するための個人端末側発信部と、前記個人端末側発信部を制御する個人端末側制御部とを備え、前記位置特定装置は、前記個人端末側発信部が発信した位置特定信号を受信するための、前記個人携帯端末から第一距離だけ離間された第一位置に配置された複数の第一位置特定側受信部と、前記第一位置と異なる位置であって、前記第一距離よりも長い第二距離だけ前記個人携帯端末から離間された第二位置に配置された複数の第二位置特定側受信部と、前記複数の第一位置特定側受信部及び第二位置特定側受信部でそれぞれ受信した位置特定信号の強度差に基づいて、前記個人携帯端末の位置を特定するための位置特定側演算部とを備えることができる。上記構成により、位置特定信号の強度差を利用することで、個人端末側発信部が発する位置特定信号を受信する複数の位置特定側受信部での信号強度のばらつきを低減することが可能となり、個人携帯端末の位置を正確にかつ短時間に測定することが可能となる。
- [0010] また、本発明の第2の側面に係る位置特定システムによれば、上記構成に

加えて、前記位置特定側演算部は、前記複数の第一位置特定側受信部で受信した位置特定信号の電波強度と、前記複数の第二位置特定側受信部で受信した位置特定信号の電波強度との差と、予め設定された閾値との大小を比較する条件式を算出して、前記個人携帯端末の位置を特定するよう構成できる。

[0011] さらに、本発明の第3の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記位置特定側演算部は、前記複数の第一位置特定側受信部で受信した位置特定信号の電波強度の平均値と、前記複数の第二位置特定側受信部で受信した位置特定信号の電波強度の平均値との差と、予め設定された閾値との大小を比較する条件式を算出して、前記個人携帯端末の位置を特定するよう構成できる。

[0012] さらにまた、本発明の第4の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記個人端末側制御部は、前記個人携帯端末が前記位置特定装置に一定距離（例えば10mや100mなど）以内に接近したことを検出して、前記個人端末側発信部が前記位置特定装置に対し位置特定信号を発信するよう制御できる。上記構成により、個人携帯端末を携帯する個人が位置特定装置に近づく前に、個人端末側発信部が位置特定装置に対して位置特定信号を発信するよう制御することが可能となり、個人携帯端末と位置特定装置との間でスムーズな位置特定動作が実行可能となる。

[0013] さらにまた、本発明の第5の側面に係る位置特定システムによれば、上記何れかの構成に加えて、さらに前記位置特定装置から一定距離（例えば10mや100mなど）以上離れた位置に設置された、前記個人端末側発信部による前記位置特定装置への位置特定信号の発信動作を起動させる起動信号を、前記個人携帯端末に向けて発信するための起動信号発信機を備えることができる。上記構成により、個人携帯端末を携帯する個人が位置特定装置に接近する前段階で予め個人端末側発信部を起動させることが可能となり、個人携帯端末と位置特定装置との間でスムーズな位置特定動作が実行可能となる。

[0014] さらにまた、本発明の第6の側面に係る位置特定システムによれば、上記

何れかの構成に加えて、前記個人端末側発信部と前記位置特定側受信部とが、双方向通信可能であり、前記位置特定側演算部が、前記位置特定側受信部で前記個人端末側発信部と通信を行うことにより、前記個人携帯端末の認証を行うよう構成できる。上記構成により、個人携帯端末を携帯する個人を認証することが可能となり、個人を区別した位置検出が可能となる。

[0015] さらにまた、本発明の第7の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記個人携帯端末が、さらに、予め付与された固有の識別情報を保持するための個人端末側記憶部を備えており、前記個人端末側制御部が、前記個人端末側発信部で前記位置特定側受信部と通信を行う際に、前記個人端末側記憶部に保持された固有の識別情報と、該識別情報毎に固有の一回のみ使用可能なワンタイムパスワードを発行可能であり、前記位置特定側演算部が、前記位置特定側受信部で前記個人端末側発信部から受信した前記識別情報及びワンタイムパスワードを認証するよう構成できる。

[0016] さらにまた、本発明の第8の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記個人携帯端末が、さらに、時刻に関する情報を生成するための個人端末側時刻部を備えており、前記個人端末側記憶部が、前記個人携帯端末と位置特定装置との間で予め交換された、該個人携帯端末に付与された識別情報に固有の共通鍵と、前記ワンタイムパスワードの生成に利用する所定の関数を保持しており、前記位置特定装置が、さらに、前記個人携帯端末に付与された識別情報と、該識別情報毎に固有の共通鍵とを関連付けて保持するための位置特定側記憶部と、時刻に関する情報を生成するための位置特定側時刻部を備えており、前記個人携帯端末が、前記位置特定装置に前記識別情報及びワンタイムパスワードを送信するに際して、前記個人端末側制御部が、前記ワンタイムパスワードを発行する際の発行時刻に関する情報を前記個人端末側時刻部で取得し、前記個人端末側記憶部に保持された所定の関数に適用し、さらに前記個人端末側記憶部に保持された共通鍵でもって暗号化して、前記ワンタイムパスワードを発行するよう構成しており、前記位置特定側演算部が、前記位置特定側受信部で、前記個人端末側発

信部から前記識別情報及びワンタイムパスワードを受信する際の受信時刻を、前記位置特定側時刻部より取得すると共に、受信した前記識別情報から、該識別情報に対応する共通鍵を前記位置特定側記憶部より探索し、得られた共通鍵を用いて前記ワンタイムパスワードを復号化し、関数化された発行時刻に関する情報を取得し、一の受信時刻において取得された発行時刻に関する情報と、前記一の受信時刻に関する情報との差分を、別の受信時刻において取得された発行時刻に関する情報と、前記別の受信時刻に関する情報との差分と比較して、その差が所定の時間内であれば、前記個人携帯端末を認証し、所定の時間内でなければ、前記個人携帯端末を認証しないよう構成できる。

[0017] さらにまた、本発明の第9の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記位置特定側演算部が、前記一の受信時刻において取得された発行時刻に関する情報と、前記一の受信時刻に関する情報との差分を認証基準情報として前記位置特定側記憶部に保存し、別の受信時刻において取得された発行時刻に関する情報と、前記別の受信時刻に関する情報との差分を、前記位置特定側記憶部に保存された認証基準情報と比較することで、前記個人携帯端末の認証を行うよう構成できる。上記構成により、認証基準情報を保持して、逐次得られるデータをこの認証基準情報と比較することで、一連の通信において取得されたデータの認証を容易に行うことが可能となる。

[0018] さらにまた、本発明の第10の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記位置特定側記憶部に保存された認証基準情報を、一定時間（例えば1分や10分、1時間など）経過後に削除するよう構成できる。上記構成により、新たな通信を行う際は別途、認証の基準となる認証基準情報を取得し直すようにすることで、なりすましを防止し、一層セキュリティを高めることが可能となる。

[0019] さらにまた、本発明の第11の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記位置特定側演算部が、前記個人携帯端末を認

証した場合に、決済を行うよう構成できる。

- [0020] さらにまた、本発明の第12の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記位置特定装置がさらに、前記位置特定側演算部で測定された前記個人携帯端末の位置に応じて、前記個人携帯端末を携帯する個人の移動を規制する動作を制御するための位置特定側制御部を備えることができる。上記構成により、個人携帯端末を携帯する個人を認識しながら、この者の位置に応じて、その移動を制御することが可能となる。
- [0021] さらにまた、本発明の第13の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記位置特定装置が、個人携帯端末を携帯する個人の通過を規制する開閉式の扉部を有するゲートであり、前記位置特定側制御部が、前記扉部の開閉を制御することができる。上記構成により、個人の認識と位置検出によって、個人携帯端末を携帯する個人の通過を規制するゲートの扉部の開閉の可否を判断できる。
- [0022] さらにまた、本発明の第14の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記個人端末側発信部及び位置特定側受信部との通信の方式を、BLE、RFID又はWi-Fiとすることができる。
- [0023] さらにまた、本発明の第15の側面に係る位置特定システムによれば、上記何れかの構成に加えて、前記個人携帯端末が、公共交通機関の乗車券として機能し、前記位置特定装置が、前記個人携帯端末を携帯する個人の乗車券の認証と決済を行うよう構成できる。
- [0024] さらにまた、本発明の第16の側面に係る位置特定システムによれば、上記何れかの構成に加えて、位置を特定する対象となる個人が携帯する個人携帯端末と、前記個人携帯端末の位置を特定する位置特定装置とを備える位置特定システムであって、前記個人携帯端末は、前記位置特定装置に対し、双方向通信を行うための個人端末側発信部と、前記個人端末側発信部を制御するための個人端末側制御部と、予め付与された固有の識別情報と、前記個人携帯端末と位置特定装置との間で予め交換された、該個人携帯端末に付与された識別情報に固有の共通鍵と、前記ワンタイムパスワードの生成に利用す

る所定の関数とを保持するための個人端末側記憶部と、時刻に関する情報を生成するための個人端末側時刻部とを備え、前記位置特定装置は、前記個人端末側発信部と双方向通信を行うための位置特定側受信部と、前記位置特定側受信部で前記個人端末側発信部と通信を行うことにより、前記個人携帯端末の認証を行うための前記位置特定側演算部と、前記個人携帯端末に付与された識別情報と、該識別情報毎に固有の共通鍵とを関連付けて保持するための位置特定側記憶部と、時刻に関する情報を生成するための位置特定側時刻部とを備え、前記個人端末側制御部が、前記個人端末側発信部で前記位置特定側受信部と通信を行う際に、前記個人端末側記憶部に保持された固有の識別情報と、該識別情報毎に固有の一回のみ使用可能なワンタイムパスワードを発行可能であり、前記位置特定側演算部が、前記位置特定側受信部で前記個人端末側発信部から受信した前記識別情報及びワンタイムパスワードを認証するよう構成しており、前記個人携帯端末が、前記位置特定装置に前記識別情報及びワンタイムパスワードを送信するに際して、前記個人端末側制御部が、前記ワンタイムパスワードを発行する際の発行時刻に関する情報を前記個人端末側時刻部で取得し、前記個人端末側記憶部に保持された所定の関数に適用し、さらに前記個人端末側記憶部に保持された共通鍵でもって暗号化して、前記ワンタイムパスワードを発行するよう構成しており、前記位置特定側演算部が、前記位置特定側受信部で、前記個人端末側発信部から前記識別情報及びワンタイムパスワードを受信する際の受信時刻を、前記位置特定側時刻部より取得すると共に、受信した前記識別情報から、該識別情報に対応する共通鍵を前記位置特定側記憶部より探索し、得られた共通鍵を用いて前記ワンタイムパスワードを復号化し、関数化された発行時刻に関する情報を取得し、一の受信時刻において取得された発行時刻に関する情報と、前記一の受信時刻に関する情報との差分を、別の受信時刻において取得された発行時刻に関する情報と、前記別の受信時刻に関する情報との差分と比較して、その差が所定の時間内であれば、前記個人携帯端末を認証し、所定の時間内でなければ、前記個人携帯端末を認証しないよう構成できる。上記構成

により、個人携帯端末を携帯する個人を認証することが可能となり、個人を区別した位置検出が可能となる。

[0025] さらにまた、本発明の第17の側面に係る位置特定装置によれば、位置を特定する対象となる個人が携帯する個人携帯端末の位置を特定する位置特定装置であって、前記個人携帯端末が前記位置特定装置に対し、個人端末側発信部から発信した、位置の特定に用いる位置特定信号を受信するための、前記個人携帯端末から第一距離だけ離間された第一位置に配置された複数の第一位置特定側受信部と、前記第一位置と異なる位置であって、前記第一距離よりも長い第二距離だけ前記個人携帯端末から離間された第二位置に配置された複数の第二位置特定側受信部と、前記複数の第一位置特定側受信部及び第二位置特定側受信部でそれぞれ受信した位置特定信号の強度差に基づいて、前記個人携帯端末の位置を特定するための位置特定側演算部とを備えることができる。上記構成により、位置特定信号の強度差を利用することで、個人端末側発信部が発する位置特定信号を受信する複数の位置特定側受信部での信号強度のばらつきを低減することが可能となり、個人携帯端末の位置を正確にかつ短時間に測定することが可能となる。

[0026] さらにまた、本発明の第18の側面に係る位置特定方法によれば、位置を特定する対象となる個人が携帯する個人携帯端末と、前記個人携帯端末の位置を特定する位置特定装置とを備える位置特定システムにおいて、前記個人携帯端末の位置を特定する位置特定方法であって、個人携帯端末を携帯する個人が前記位置特定装置に一定距離以内に接近したことを、前記個人携帯端末が検出して、個人端末側制御部が個人端末側発信部の起動させる工程と、前記個人携帯端末が、個人端末側発信部から、前記位置特定装置に対し、位置の特定に用いる位置特定信号を発信する工程と、前記位置特定装置が、前記個人端末側発信部が発信した位置特定信号を、前記個人携帯端末から第一距離だけ離間された第一位置に配置された複数の第一位置特定側受信部と、前記第一位置と異なる位置であって、前記第一距離よりも長い第二距離だけ前記個人携帯端末から離間された第二位置に配置された複数の第二位置特定

側受信部で、それぞれ受信する工程と、前記複数の第一位置特定側受信部及び第二位置特定側受信部でそれぞれ受信した位置特定信号の強度差に基づいて、位置特定側演算部が前記個人携帯端末の位置を特定する工程とを含むことができる。これにより、位置特定信号の強度差を利用することで、個人端末側発信部が発する位置特定信号を受信する複数の位置特定側受信部での信号強度のばらつきを低減することが可能となり、個人携帯端末の位置を正確にかつ短時間に測定することが可能となる。

[0027] さらにまた、本発明の第19の側面に係る位置特定方法によれば、上記に加えて、さらに、前記個人端末側発信部が位置特定信号を発信する工程に先立ち、前記個人端末側発信部が、前記位置特定側受信部に対し、個人端末側記憶部に保持された固有の識別情報と、該識別情報毎に固有の一回のみ使用可能なワンタイムパスワードを送信する工程と、前記位置特定側演算部が、前記識別情報及びワンタイムパスワードに基づいて、前記個人携帯端末の認証を行う工程を含んでおり、前記個人携帯端末が、前記位置測定機に前記識別情報及びワンタイムパスワードを送信する工程は、前記個人端末側制御部が、前記ワンタイムパスワードを発行する際の発行時刻に関する情報を個人端末側時刻部で取得し、前記個人端末側記憶部に保持された所定の関数に適用し、さらに前記個人端末側記憶部に保持された共通鍵でもって暗号化して、前記ワンタイムパスワードを発行するものであり、前記位置特定側演算部が、前記識別情報及びワンタイムパスワードに基づいて、前記個人携帯端末の認証を行う工程は、前記位置測定側演算部が、前記位置測定側通信部で、前記個人端末側発信部から前記識別情報及びワンタイムパスワードを受信する際の受信時刻を、位置測定側時刻部より取得すると共に、受信した前記識別情報から、該識別情報に対応する共通鍵を前記位置測定側記憶部より探索し、得られた共通鍵を用いて前記ワンタイムパスワードを復号化し、関数化された発行時刻に関する情報を取得し、一の受信時刻において取得された発行時刻に関する情報と、前記一の受信時刻に関する情報との差分を、別の受信時刻において取得された発行時刻に関する情報と、前記別の受信時刻に関

する情報との差分と比較して、その差が所定の時間内であれば、前記個人携帯端末を認証し、所定の時間内でなければ、前記個人携帯端末を認証しないものとできる。これにより、個人携帯端末を携帯する個人を認証することが可能となり、個人を区別した位置検出が可能となる。

[0028] さらにまた、本発明の第20の側面に係る位置特定プログラムによれば、位置を特定する対象となる個人が携帯する個人携帯端末と、前記個人携帯端末の位置を特定する位置特定装置とを備える位置特定システムにおいて、前記個人携帯端末の位置を特定する位置特定プログラムであって、個人携帯端末を携帯する個人が前記位置特定装置に一定距離以内に接近したことを、前記個人携帯端末が検出して、個人端末側制御部が個人端末側発信部の起動させる機能と、前記個人携帯端末が、個人端末側発信部から、前記位置特定装置に対し、位置の特定に用いる位置特定信号を発信する機能と、前記位置特定装置が、前記個人端末側発信部が発信した位置特定信号を、前記個人携帯端末から第一距離だけ離間された第一位置に配置された複数の第一位置特定側受信部と、前記第一位置と異なる位置であって、前記第一距離よりも長い第二距離だけ前記個人携帯端末から離間された第二位置に配置された複数の第二位置特定側受信部で、それぞれ受信する機能と、前記複数の第一位置特定側受信部及び第二位置特定側受信部でそれぞれ受信した位置特定信号の強度差に基づいて、位置特定側演算部が前記個人携帯端末の位置を特定する機能とをコンピュータに実現させることができる。これにより、位置特定信号の強度差を利用することで、個人端末側発信部が発する位置特定信号を受信する複数の位置特定側受信部での信号強度のばらつきを低減することが可能となり、個人携帯端末の位置を正確にかつ短時間に測定することが可能となる。

[0029] また第21の側面に係るコンピュータで読み取り可能な記録媒体又は記録した機器は、上記プログラムを格納するものである。記録媒体には、CD-ROM、CD-R、CD-RWやフレキシブルディスク、磁気テープ、MO、DVD-ROM、DVD-RAM、DVD-R、DVD+R、DVD-R

W、DVD+RW、Blu-ray（登録商標）、HDDVD（AOD）等の磁気ディスク、光ディスク、光磁気ディスク、半導体メモリその他のプログラムを格納可能な媒体が含まれる。またプログラムには、上記記録媒体に格納されて配布されるものの他、インターネット等のネットワーク回線を通じてダウンロードによって配布される形態のものも含まれる。さらに記録媒体にはプログラムを記録可能な機器、例えば上記プログラムがソフトウェアやファームウェア等の形態で実行可能な状態に実装された汎用もしくは専用機器を含む。さらにまたプログラムに含まれる各処理や機能は、コンピュータで実行可能なプログラムソフトウェアにより実行してもよいし、各部の処理を所定のゲートアレイ（FPGA、ASIC、DSP）等のハードウェア、又はプログラムソフトウェアとハードウェアの一部の要素を実現する部分的ハードウェアモジュールとが混在する形式で実現してもよい。

図面の簡単な説明

[0030] [図1] BLE発信機と受信機との距離を測定する様子を示す概念図である。

[図2] BLE発信機から同一の距離離間させたBLE 1～4の電波強度の時間変化を示すグラフである。

[図3] BLEビーコンを用いた位置特定方法の一例を示す模式図である。

[図4] BLEビーコンを用いた短時間での三角測量方法を示す模式図である。

[図5] スマートフォン端末等をBLE発信機とし、BLE受信機を2か所に配置する例を示す概念図である。

[図6] 図5の例において、BLE受信機の電波強度差から求めた発信機の存在エリアの例を示す概念図である。

[図7] スマートフォン端末等をBLE発信機とし、BLE受信機を3か所に配置する例を示す概念図である。

[図8] 図7の例において、BLE受信機の電波強度差から求めた発信機の存在エリアの例を示す概念図である。

[図9] BLE発信機から一定距離離れた1つのBLE受信機の電波強度示すヒストグラムである。

[図10] B L E 発信機から異なる距離離れた 2 つの B L E 受信機の電波強度差を示すヒストグラムである。

[図11] 実施形態 1 に係る位置特定システムを示す模式図である。

[図12] B L E 発信機から異なる距離離れた 4 つの B L E 受信機を 2 か所に配置し、各箇所において電波強度を平均化したものの差を示すヒストグラムである。

[図13] B L E 発信機と、複数の B L E 受信機を 3 か所に配置した例を示す模式図である。

[図14] 図 1 3 において、複数の B L E 受信機の電波強度を平均化したものの差から求めた B L E 発信機の存在エリアの例を示す模式図である。

[図15] B L E 発信機の存在エリアを限定することで、B L E 発信機の位置特定をする例を示す模式図である。

[図16] ユーザの通過経路上に通過判定エリアを二か所設けた例を示す模式図である。

[図17] 図 1 6 のユーザの通過経路を規定するゲートを設置した例を示す模式図である。

[図18] 実施形態 1 に係る位置特定システムの機能ブロック図である。

[図19] 位置特定システムのブロック図である。

[図20] 実施形態 2 に係る位置特定システムを示す模式図である。

[図21] 図 2 0 の配置例において、B L E 発信機の電波強度差から求めた B L E 受信機の存在エリアを示す模式図である。

[図22] 実施形態 2 において、スマートフォン端末等を B L E 受信機とし、B L E 発信機を 3 か所に配置した例を示す模式図である。

[図23] 図 2 2 の配置例において、B L E 発信機の電波強度差から求めた B L E 受信機の存在エリアの例を示す模式図である。

[図24] 実施形態 3 に係る位置特定システムを示す模式図である。

[図25] スマートフォン端末等を B L E 受信機とし、複数の B L E 発信機を 3 か所に配置した例を示す模式図である。

[図26]図25の配置例において、BLE発信機の電波強度を平均化したものの差から求めたBLE受信機の存在エリアの例を示す模式図である。

[図27]BLE受信機の存在エリアを限定してBLE発信機の位置特定をする例を示す模式図である。

[図28]ユーザの通過経路上に通過判定エリアを二か所設けた例を示す模式図である。

[図29]認証の3要素を示す模式図である。

[図30]暗号化された時間を送り認証する様子を示す模式図である。

[図31]実施形態4に係る認証システムの機能ブロック図である。

[図32]実施例1に係る事後支払いシステムを示す概略図である。

[図33]図32の事後支払いシステムによる事後支払いの手順を示すフローチャートである。

[図34]事後支払いシステムの詳細な構成図である。

[図35]図35Aは位置特定装置の外観構成例を示す斜視図、図35Bは変形例に係る位置特定装置の外観構成例を示す斜視図である。

[図36]図36Aは位置特定装置の平面図、図36Bは図36AのXXXVIB-XXXVIB線における断面図である。

[図37]位置特定装置の位置特定側制御部を示すブロック図である。

[図38]事業者用管理端末を用いた事後支払いシステムへの登録処理の流れを示すフロー図である。

[図39]事後支払いシステムにおける、個人携帯端末を用いた本システムへの登録処理の流れを示すフロー図である。

[図40]事後支払いシステムによる個人携帯端末から事業者サービスを申請する処理の流れを示すフロー図である。

[図41]事後支払いシステムによる管理サーバシステムで、与信状況の変化を監視維持のための処理の流れを示すフロー図である。

[図42]事後支払いシステムによる、利用者による位置特定装置利用時の処理の流れを示すフロー図である。

[図43]位置特定の手順を示すフローチャートである。

[図44]位置特定装置による個人携帯端末の位置特定における位置特定装置の処理の流れを示すフローチャートである。

[図45]位置特定装置による個人携帯端末の位置特定時における電波強度算出の処理の流れを示すフローチャートである。

[図46]位置特定装置による個人携帯端末の位置特定時における電波強度算出の処理の流れを示すフローチャートである。

[図47]B L E 受信機の電波強度から基準値を求める処理の流れを示すフローチャートである。

[図48]位置特定装置による個人携帯端末の位置特定を行う処理の流れを示すフロー図である。

[図49]暗号化・復号における個人携帯端末の処理の流れを示すフローチャートである。

[図50]暗号化・復号における個人携帯端末の処理の流れを示すフローチャートである。

[図51]暗号化・復号における位置特定装置の認証処理の流れを示すフローチャートである。

[図52]暗号化・復号における位置特定装置の認証処理の流れを示すフローチャートである。

[図53]暗号化・復号における位置特定装置の認証処理の流れを示すフローチャートである。

[図54]暗号化・復号における位置特定装置の認証処理の流れを示すフローチャートである。

[図55]暗号化・復号における位置特定装置の認証なりすまし否認の処理の流れを示すフローチャートである。

[図56]改札機に見立てて実験を行った場合の様子を示す写真である。

[図57]改札機に見立てて実験を行った場合の様子を示す写真である。

[図58]位置特定認証システムを示す概略図である。

[図59]位置特定認証システムを示す概略図である。

発明を実施するための形態

- [0031] 以下、図面に基づいて実施形態を詳細に説明する。なお、以下の説明では、必要に応じて特定の方向や位置を示す用語（例えば、「上」、「下」、及びそれらの用語を含む別の用語）を用いるが、それらの用語の使用は図面を参照した発明の理解を容易にするためであって、それらの用語の意味によって本発明の技術的範囲が制限されるものではない。また、複数の図面に表れる同一符号の部分は同一もしくは同等の部分又は部材を示す。なお、本明細書において「備える」とは、別部材として備えるもの、一体の部材として構成するものの何れをも含む意味で使用する。
- [0032] さらに以下に示す実施形態は、本発明の技術思想を具体化するための位置特定システム、位置特定装置、位置特定方法、位置特定プログラム及びコンピュータで読み取り可能な記録媒体並びに記録した機器を例示するものであって、本発明を以下に限定するものではない。また、以下に記載されている構成部品の寸法、材質、形状、その相対的配置等は、特定の記載がない限り、本発明の範囲をそのみに限定する趣旨ではなく、例示することを意図したものである。また、一の実施の形態、実施例において説明する内容は、他の実施の形態、実施例にも適用可能である。また、図面が示す部材の大きさや位置関係等は、説明を明確にするため、誇張していることがある。
- [0033] なお本明細書において「スマートフォン端末」や「スマートフォン」というとき、スマートフォンに限らず、タブレットやWIFIルータ、携帯音楽プレーヤー等、通信機能を有する端末を含む意味で使用する。
- [0034] 本発明の実施形態においては、スマートフォン端末等を持って移動しているユーザの位置を短時間で高精度に認識する。これによって、例えば公共交通機関の乗車券や、コンサートのチケット等を、スマートフォン端末等のアプリで実現する場合に、従来は自動改札機や入場ゲートにスマートフォン端末をタッチさせる必要があった。しかしながら、利用者にとってはタッチさせる動作が必要となるため、例えば荷物を持ったり子供を抱えている場合、

あるいは身体障害者等、タッチ動作ができない場合にはゲートの開門が行えないという問題があった。これに対して本実施形態に係る位置特定システムにおいては、無線による通信で位置検出を行うことにより、自動改札機や入場ゲートを通過したことをタッチレスで検出することが可能となる。また、後述する通りユーザの認証機能を組み合わせることで、入場、退場の管理や自動決済も可能となる。例えば、スーパーマーケットやコンビニエンスストアの決済等にも適用できる。

(BLEを用いた距離測定方法)

[0035] 初めに、BLEビーコン、BLEビーコンを用いた距離測定方法、BLEビーコンを用いた位置特定方法、本発明の一実施形態に係る位置特定方法について説明をした後、本発明の一実施形態に係る一方向通信における認証方式を説明する。

(BLEビーコン)

[0036] まず、BLEビーコンについて説明する。BLEビーコンは、Bluetooth 4.0以降の規格で規定されており、BLEはBluetooth Low Energyを意味する。BLEは2.4GHz帯域で通信をするが、通信モードにはブロードキャストモードとコネクションモードの二つがある。ブロードキャストモードでは、あるBLEデバイスから別の不特定のBLEデバイスに対して一方的にデータをオープンに送信する。この通信方式では、発信する際の電波強度は時間的にある程度一定である。またコネクションモードでは、あるBLEデバイスと別のBLEデバイスとの間で相互にデータをプライベートに送受信する。この通信方式では、送信先のデバイスで一定の電波強度になるように、電波強度を時間的に変動させている。どちらの通信方式も、一定時間（例えば数msや数十ms）毎にごくわずか（例えばサブmsなど）な時間のみ発信することで、消費電力を大幅に低下させている。

(BLEビーコンを用いた距離測定方法)

[0037] 次に、BLEビーコンを用いた一般的な距離測定方法を説明する。ここで、BLE発信機としてBLEビーコンを、BLE受信機としてスマートフォ

ン端末を用いて、距離を測定する様子を図1に示す。BLE発信機から出力されたブロードキャストモードの電波信号は、時間的に電波強度が一定（例えば平均的には−43 dBmなど）であり、距離が離れるごとに電波強度が減衰する。このため、BLE発信機から出力される電波強度を、電波信号に乗せて送信しつつ、受信電波強度RSSI（Received Signal Strength Indication）を測定することで、電波強度の減衰（伝搬損失）が判明し、これに基づいて測定距離も計算できる。ここで、伝搬損失と距離との関係式を数1に示す。

[0038] [数1]

$$L = 10 \log_{10} d^n$$

（L：伝搬損失 [dB]、d：測定距離 [m]、n：減衰指数）

[0039] 減衰指数nは、真空中であれば2であるが、実環境においては2以上の値を取りうる。数1によれば、測定距離が2倍になれば、得られるRSSIが6 dBm以上減少することが判る。ただ、実際には利用するスマートフォン端末等の送受信アンテナのゲインが安定しないこと等から、電波強度は安定しないと考えられる。

[0040] 図2は、BLE発信機からほぼ同一の距離（例えば1 m）だけ離間させた4つのBLE受信機BLE1～4の電波強度を、時間軸で示したものである。ここでは各BLE受信機が、データをおよそ4 ms毎に取得している。この図から、数百ms程度の時間のうちにも、電波強度が20 dB程度変動することが判る。これは、BLEの発信電波強度及び受信電波強度の時間的な測定変動によるものであり、これでは正確な電波強度を測定することができない。このため、通常は1分程度といった十分な時間を取って、同じ地点で電波を受信し続け、得られたRSSIを平均化することで時間的に安定した伝搬損失の値を得、これに基づいて測定距離を求めている。この方法では、高速に距離を正確に測定することはできない。

（BLEビーコンを用いた位置特定方法）

[0041] 次に、BLEビーコンを用いた位置特定方法について説明する。ここで、

BLEビーコンを用いた一般的な三角測量の例を図3に示す。この図において、3つのBLEビーコン発信機からの信号を十分な時間、スマートフォン端末等のBLE受信機で受信し、数1より求めた距離を各端末で測定することで、正確な位置を測定することができる。各BLEビーコン発信機で測定した距離を円で描くことで、円弧が一致した点Xが得られる。例えば、各BLEビーコン発信機からの信号に発信電力として -40 dBm ずつとして送信し、受信したスマートフォンがそれぞれから受信した電力が -51 dBm 、 -55 dBm 、 -46 dBm だった場合、それぞれ伝搬損失は、 11 dB 、 15 dB 、 6 dB 、とわかる減衰指数が電波吸収などがほとんどない場合は $n=2$ 、となるので、それよりそれぞれの半径を求めることができ、円弧を描くことができる。この点Xが、BLE受信機の存在する地点となる。ただ、短時間では正確に距離測定ができないため、位置が測定できないことがある。

[0042] また、BLEビーコンを用いた短時間での三角測量を図4に示す。図3と同様に3つのBLEビーコン発信機を配置した状態において、各BLEビーコン発信機からの信号を短時間、スマートフォン端末等のBLE受信機で受信して、数1より求めた距離を各端末から測定しようとする、正確な距離を測定できない。そのため、各BLEビーコン発信機から測定した距離の円を描くと、図4に示すように距離を示す円同士の重なりが大きくなって、一致した点が生まれない。このため、BLE受信機の存在する地点がわからなくなってしまう。

[0043] 以上は、BLEを用いて距離や位置を特定乃至検出する方法について説明したが、位置検出等には、BLEに限らず、他のBluetooth規格やWi-Fi、RFID (Radio Frequency Identifier)、iMESH、超音波、ZigBee等、他の無線通信規格を用いることもできる。しかしながら、他の無線通信規格においても上述したBLEと同様に、短時間で高精度に検出することは困難であり、実用的な使用に耐えうるものではなかった。例えば、電車の改札機の通過をタッチレスで検出するには、近接する他の利用

者との区別や、隣接して設置された改札機との区別が必要であることから、40cm以下の測定誤差が求められる。また利用者の歩行速度に鑑みると、位置特定は100ms以下での処理が必要となる。さらに、スマートフォン端末等が利用者のカバンや服のポケットの中等にある場合を考慮し、BLE発信機から発信される電波強度とBLE受信機で得られるRSSIの差が、必ずしも空間中の伝搬損失に限らないということも考慮する必要がある。これらの処理速度や位置精度は、改札機や入場ゲートへの適用に限らず、例えばスーパーマーケットやコンビニエンスストアのレジにおける決済等においても同様に求められる。

〔実施形態1〕

[0044] このように、従来の方法ではユーザが携帯するスマートフォン端末等をBLE受信機として位置特定を行おうとしても、精度と処理速度の点で実用的ではなかった。そこで、本発明の実施形態1に係る位置特定方法では、実環境に適応可能な位置精度と処理速度を実現すべく、スマートフォン端末等をBLE受信機でなくBLE発信機とし、さらにBLE受信機を複数台、異なる位置に配置している。これによって、BLE受信機の電波強度差から位置を特定して、実環境に対応した実用的な検出精度と検出速度を実現できる。この結果、スマートフォン端末等を持って移動しているユーザを、一人ずつ高速に、かつ高精度に捕捉、区別、認識することが可能となった。また認証に付随する行動をタッチレスで自動化でき、行動把握も可能となる。例えば、レジや改札機において、支払うべきユーザが移動していても、誤認識なく特定することが可能となる。

[0045] スマートフォン端末等をBLE発信機とし、BLE受信機を2か所に配置する例を図5に示す。この場合、スマートフォン端末等がカバンや服のポケット等の中であって、そのすぐ外側における出力電波強度がスマートフォン端末等の出力電波強度と異なっても、BLE受信機の電波強度差は変わらない。またこれにより、BLE発信機の発信電波強度の時間的な測定変動を吸収できるため、正確な電波強度測定に寄与する。

[0046] また図6は、スマートフォン端末等をBLE発信機とし、BLE受信機を2か所に配置した場合に、BLE受信機の電波強度差から求めた発信機の存在エリアの例を示している。BLE受信機の電波強度差から求められた発信機の存在エリアは、アポロニウスの円もしくは直線を描く。これは、電波強度が対数で表されるため、電波強度の差が一定（例えば10dB）の場合、距離における比が一定（例えば10倍など）とみなせるからである。ただし、一つの円もしくは直線だけでは、必ずしもBLE発信機の存在エリアを限定できない。

[0047] ここで、スマートフォン端末等をBLE発信機とし、BLE受信機を3か所に配置した場合を図7に、またこの場合にBLE受信機の電波強度差から求めたBLE発信機の存在エリアの例を図8に、それぞれ示す。この場合、アポロニウスの円もしくは直線は3つ描かれることになる。このアポロニウスの円を描くことで、一致した点Xが生まれ、この点Xが当該BLE発信機の存在する地点となる。ただし、直線が一つだけ描かれるとBLE発信機の位置が確定しない。必ず位置を特定できるような配置とする条件は、4つ以上のBLE受信機を、それにより描かれる四角形の辺においていずれも平行とならないように、配置することである。

[0048] もしくは、図6のように、BLE発信機の存在エリアが、例えば直径40cm等、必要なサイズ以下である場合、その位置に存在するとして位置特定をすることもできる。例えば、2か所に配置したBLE発信機から、異なる距離分を離間させてBLE受信機を配置する。このBLE受信機で受信した電波強度の差が、ある閾値（例えば、10dB）以上であることを条件として、BLE発信機の存在エリアは、BLE受信機の電波強度差から計算して描かれるアポロニウスの円の内側の全体エリアとなる。これを利用して存在位置を特定してもよい。

[0049] 図2のように、BLE発信機（例えば-43dBmの平均電波強度で出力している）から一定距離（例えば1m）離れた1つのBLE受信機で検出される電波強度のヒストグラムを、図9に示す。このグラフによれば、BLE

受信機は30 dB程度変動し、標準偏差が5.85程度であった。このように電波強度の変動が非常に大きく、最大値と最小値との差も大きいため、このような電波強度から距離を演算しても、同様に変動が大きくなる。

[0050] 一方で、BLE発信機（例えば-43 dBmの平均電波強度で出力している）から異なる距離（例えば1 m、3 m）だけ離れた2つのBLE受信機の電波強度差（近距離と短距離でのそれぞれ単一受信機の電波強度差分布）のヒストグラムを、図10に示す。標準偏差は6.21程度であった。一般に、BLE発信機から近いBLE受信機の方が、遠い側のBLE受信機の方よりも電波強度は大きい値となるが、一部逆転していることが判る。このように、電波強度差の変動が大きく、大小関係も崩れていることが判る。

[0051] また一般に、2つの理想的な正規分布ヒストグラムを描く同じ確率分布どうしの差を求めると、標準偏差が $\sqrt{2}$ 倍程度となることが知られている。これに対し図10の標準偏差は、図9の標準偏差から $\sqrt{2}$ 倍より小さい広がりとなっている。このことから、BLEの発信電波強度の時間的な測定変動を吸収し、多少、正確な電波強度測定に寄与していることが判る。ただし、図10の標準偏差の広がりがより小さくないと、高速かつ高精度な位置特定は実現できない。

[0052] そこで、BLEの受信電波強度の時間的な測定変動を吸収させる。図2から判る通り、BLE発信機から一定距離（例えば1 mなど）を離間させた4つのBLE受信機の電波強度の変動は、ほぼ独立に変動していることが判る。一般的に、独立したn個の理想的な正規分布ヒストグラムを描く同じ確率分布どうしの平均を求めると、標準偏差が $1/\sqrt{n}$ 倍程度となることが知られている。このため、同じ位置に複数のBLE受信機を配置し、そこで得られる複数のBLE受信機の電波強度を平均化することで、BLEの受信電波強度の時間的な測定変動を低減できると期待される。

[0053] スマートフォン端末等をBLE発信機とし、複数のBLE受信機を2か所に配置した場合の例を図11に示す。例えば、各位置に2台のBLE受信機を配置して、計4つのBLE受信機を配置した場合、その4つのBLE受信

機の強度を平均化すると、そのヒストグラムから求まる標準偏差は、2.63程度となる。この値は、BLE発信機から一定距離（例えば1mなど）だけ離れた1つのBLE受信機の、電波強度のヒストグラムから求まる標準偏差の、およそ1/2となっていることが確認できる。これにより、BLEの受信電波強度の時間的な測定変動を低減できることが判る。

[0054] またBLE発信機（例えば-43dBmの平均電波強度で出力）から異なる距離（例えば1m、3m）離れた4つのBLE受信機を2か所に配置し、それぞれの箇所において電波強度を平均化したものの差のヒストグラムを、図12に示す。このグラフによれば、図10等と比べ、電波強度変動が小さくなり、大小関係も是正されていることが判る。また標準偏差は2.85程度であった。このように、BLE発信機から異なる距離離れた複数のBLE受信機を2か所に配置し、それぞれの箇所において電波強度を平均化したものの差を取ることで、BLEの発信電波強度及び受信電波強度の時間的な測定変動を十分低減できることが判る。

[0055] ここで図13に、スマートフォン端末等をBLE発信機とし、複数のBLE受信機を3か所に配置した場合の例を示す。また図14に、図13のBLE発信機とBLE受信機を配置した例において、複数のBLE受信機の電波強度を平均化したものの差から求めたBLE発信機の存在エリアの例を示している。この場合、アポロニウスの円もしくは直線は3つ描かれることになる。このアポロニウスの円を描くことで、一致した点Xが生まれ、この点Xが当該BLE発信機の存在する地点となる。ただし、直線が一つだけ描かれるとBLE発信機の位置が確定しない。ここで、必ず位置を特定できるような配置とする条件は、4つ以上のBLE受信機を、それにより描かれる四角形の辺においていずれも平行とならないように、配置することである。

[0056] あるいは、BLE発信機の存在エリアが、例えば直径40cm等、必要なサイズ以下である場合には、その位置に存在するとして位置特定をすることもできる。図15は、BLE発信機の存在エリアを限定して利用することで、BLE発信機の位置特定をする例を示している。条件を調整することによ

り、BLE発信機の存在エリアが、スマートフォン端末等を持って移動しているユーザを一人ずつ高精度に区別する範囲（例えば直径40cm以下の円内）となるように設定することができる。例えば、2か所に配置したBLE発信機から、異なる距離（例えば2m）離れたそれぞれの箇所において、複数のBLE受信機の電波強度を平均化したものの差が、ある閾値（例えば10dB）以上であることを条件に、BLE発信機の存在エリアは、複数のBLE受信機の電波強度を平均化したものの差から計算して描かれるアポロニウスの円の内側の全体エリアとなる。

[0057] ただ、例えば、レジや改札機において支払いを行う場合、誤ってBLE発信機のいないエリアにいると判断されると問題が発生する。そこで、これを誤認識と定義する。一般に誤認識の確率自体を低くする必要があるところ、支払い等高精度な認識が必要な場面においては、誤認識をさらに低減するための工夫が必要となる。このため、支払い等の高精度な認証が必要な場面で誤認識をさらに低くするための工夫の例を図16に示す。図16のように、ユーザの通過判定エリアを二か所設け、その両方を一定時間差（例えば0.5秒～2秒など）でユーザが通過した場合のみ認証することで、誤認識をさらに低くすることができる。つまり、たまたま片方のユーザの通過判定エリアに近づき、認証されてしまってももう一つのユーザの通過判定エリアが認証されない限り、通過したと判断されない。

[0058] なお、ここで図15の配置を利用することもできる。つまり、通過時の前半のユーザの通過判定エリアを設定する際には、図15のように、2か所に配置したBLE発信機から異なる距離（例えば2m）離れたそれぞれの箇所において、複数のBLE受信機の電波強度を平均化したものの差が、ある閾値以上であることを条件とする判定方法を用いる。また、通過時の後半のユーザの通過判定エリアを設定する際には、図15とは逆の、2か所に配置した、BLE発信機から異なる距離離れたそれぞれの箇所において複数のBLE受信機の電波強度を平均化したものの差が、ある閾値（例えば10dB）以上であることを条件とする判定を用いることで利用できる。

- [0059] 図17は、図16のユーザの通過を制限するための工夫を示している。図17のように、ユーザの通過経路を規定するためのゲートとして自動改札機を設置する。
- [0060] なお、図16や図17のようなユーザの通過判定エリアを設定するにあたり、BLE発信機から異なる距離（例えば2m）だけ離間させて複数のBLE受信機を2か所に配置することもできる。ここでは、それぞれの箇所において複数のBLE受信機の電波強度を平均化したものの差が、ある閾値（例えば10dB）以上であることを条件に、BLE発信機の位置特定ができる。例えば、図15のような配置を利用することで、ユーザの通過判定のために使う2か所の複数のBLE受信機を共用できる。
- [0061] なお、実際には電波強度を、例えば、図8や図14のようなBLE発信機の存在エリアである3つのアポロニウスの円や直線が一致した点を描くとは限らない。このため、3つ以上のアポロニウスの円や直線を用意し、最も誤差が小さくなるような位置を、BLE発信機の位置として推定することが望ましい。ここでいう誤差は、例えば、距離や電波強度における最小二乗法を用いてもよいし、非線形最小二乗法等の他の回帰計算を用いてもよい。
- [0062] これらの結果、例えば使用するBLE受信機を配置一か所につき4つ利用し、このようなBLE受信機を複数の場所に配置することで、95%以上の確率でBLE発信機の存在エリアで認識が確認でき、誤認識は0.0%以下となる。また、測定時間は平均10ms以下で測定できる。このため、本実施形態で高速かつ高精度な位置特定ができる。この結果、リアルタイムに利用者の位置検出を行うことが可能となる。
- [0063] このように、BLE発信機から異なる距離だけ離間させた複数のBLE受信機を、2か所以上に配置する。そして、それぞれの箇所においてBLE受信機で受信した信号の電波強度を平均化したものの差を取り、図6や図8、図12、図14等のように位置を特定する。これによって、BLEの発信電波強度及び受信電波強度の時間的な測定変動を十分低減して、BLE発信機の位置特定を高速かつ高精度に行えるようになる。また、これによりスマー

トフォン端末等を持って移動しているユーザを個別に高速かつ高精度に捕捉、区別、認識することが可能となり、認証に付随する行動をタッチレスで自動化できるようになる。

(位置特定システムの機能ブロック図)

[0064] ここで、位置特定システムの機能ブロック図を図18に示す。この図に示す位置特定システム100は、位置を特定する対象となる個人が携帯する個人携帯端末10と、この個人携帯端末10の位置を特定する位置特定装置20を備える。

[0065] 個人携帯端末10は、個人端末側発信部11と、個人端末側制御部12を備える。個人端末側発信部11は、位置特定装置20と通信を行うための部材である。具体的には、個人端末側発信部11は、位置特定装置20に対し、位置の特定に用いる位置特定信号を発信する。また個人端末側制御部12は、個人端末側発信部11を制御する。

[0066] 位置特定装置20は、位置特定側受信部21と、位置特定側演算部25を備える。位置特定側受信部21は、個人端末側発信部11が発信した位置特定信号を受信するための部材であり、複数の第一位置特定側受信部22A、22Bと、複数の第二位置特定側受信部23A、23Bを備える。第一位置特定側受信部22は、個人携帯端末10から第一距離だけ離間された第一位置に並んで配置されている。また第二位置特定側受信部23は、第一位置と異なる位置であって、第一距離よりも長い第二距離だけ個人携帯端末10から離間された第二位置に、並んで配置されている。

[0067] さらに位置特定側演算部25は、複数の第一位置特定側受信部22A、22B及び第二位置特定側受信部23A、23Bでそれぞれ受信した位置特定信号の強度差に基づいて、個人携帯端末10の位置を特定する。これにより、位置特定信号の強度差を利用することで、個人端末側発信部11が発する位置特定信号を受信する複数の位置特定側受信部での信号強度のばらつきを低減することが可能となり、個人携帯端末10の位置を正確にかつ短時間に測定することが可能となる。

[0068] 位置特定側演算部 25 は、複数の第一位置特定側受信部 22 A、22 B で受信した位置特定信号の電波強度と、複数の第二位置特定側受信部 23 A、23 B で受信した位置特定信号の電波強度との差と、予め設定された閾値との大小を比較する条件式を算出して、個人携帯端末 10 の位置を特定する。例えば、電波強度の差が、予め設定された閾値（例えば 10 dB）より大きいかを比較する条件式を算出する。

[0069] あるいは、第一位置や第二位置に複数台配置された位置特定側受信部で平均化することにより、信号強度のばらつきを抑制することもできる。この場合、位置特定側演算部 25 は、複数の第一位置特定側受信部 22 A、22 B で受信した位置特定信号の電波強度の平均値と、複数の第二位置特定側受信部 23 A、23 B で受信した位置特定信号の電波強度の平均値との差と、予め設定された閾値との大小を比較する条件式を算出して、個人携帯端末 10 の位置を特定する。

（個人端末側発信部 11 の自動起動機能）

[0070] 以上の構成では、個人携帯端末 10 を発信機として利用している。ここでは BLE で通信することにより、消費電力を抑制できる。ただ、スマートフォン端末の BLE 機能を常時 ON させておくことは、利用者側でバッテリー消費を抑えたい場合には抵抗を生じることが考えられる。このため、利用者によってはスマートフォン端末の BLE 機能を OFF としたいケースが考えられる。上述した位置特定システムの利用時においては、スマートフォン端末の BLE 機能を ON しておくことが必須であり、例えば位置特定システムを地下鉄などの公共交通機関の乗車券として利用する場合は、自動改札機に近づく前に利用者が自身のスマートフォン端末を操作し、BLE 機能を手動で ON させなければならない、手間がかかる。

[0071] そこで、BLE 機能等の個人端末側発信部 11 を、利用者が位置特定装置 20 に接近する前に自動で起動させる、自動起動機能を備えてもよい。例えば、個人携帯端末 10 を携帯する個人が位置特定装置 20 に一定距離以内に接近したことを、個人端末側制御部 12 で検出して、自動的に BLE 機能を

ONさせて、個人端末側発信部11を起動し、個人端末側発信部11が位置特定装置20に対し位置特定信号を発信するよう制御する。これにより、個人携帯端末10を携帯する個人が位置特定装置20に近付く前に、個人端末側発信部11が位置特定装置20に対して位置特定信号を発信するよう制御することが可能となり、個人携帯端末10と位置特定装置20との間でスムーズな位置特定動作が実行可能となる。

[0072] また、BLEビーコン信号発信をスマートフォン端末等に行わせることもできる。例えばBLEビーコンを駅の入口などに設置し、このBLEビーコンから利用者の携帯端末に向けて発信しておくことで、その信号を受信したスマートフォン端末等が自動的にBLEビーコン信号（例えば、利用者の携帯端末のID情報を含んだ位置測定のための信号）を発信する。また、別の構成として、携帯端末が有するGPS機能を用いて、駅などの特定の施設に近づいたら、自動的に信号を発信するように構成してもよい。この場合は、ジオフェンス機能等を利用できる。

（起動信号発信機90）

[0073] あるいは、個人端末側発信部11を起動させるための部材を設置してもよい。具体的には、位置特定装置20から一定距離以上離れた位置に起動信号発信機を設置する。起動信号発信機は、個人端末側発信部11による位置特定装置20への位置特定信号の発信動作を起動させる起動信号を、個人携帯端末10に向けて発信する。これにより、個人携帯端末10を携帯する個人が位置特定装置20に接近する前段階で予め個人端末側発信部11を起動させることが可能となり、個人携帯端末10と位置特定装置20との間でスムーズな位置特定動作が実行可能となる。例えば地下鉄などの公共交通機関の乗車券に利用する場合は、駅の入口や改札口の近傍など、利用者が自動改札機である位置特定装置20に近付く前に通るであろう場所に、起動信号発信機を設置する。このような例を図19に示す。ここでは、鉄道の駅の入口に、それぞれ起動信号発信機90を設置している。起動信号発信機90は、利用者USRのスマートフォン端末のBLE機能をONにすると共に、位置特

定信号の発信動作を開始させる。このように、利用者U S Rが自動改札機等の位置特定装置20に向かう経路上に予め起動信号発信機90を設置しておくことにより、利用者U S Rが自動改札機などの位置特定装置20に接近する前に、位置特定信号の発信動作を開始させることができ、位置特定装置20に接近した状態では、位置特定信号を位置特定装置20側で検出して、スマートフォン端末の位置特定を実行することが可能となる。

[0074] また同様に、自動改札機などの位置特定装置20を通過した後は、利用者U S Rの経路上に別途、終了信号発信機を設置してB L E機能をO F Fにするようにしてもよい。例えば駅の改札内や、あるいは改札の外で駅の出口等に終了信号発信機を設置することで、B L E機能による電力消費を低減することが可能となる。また終了信号発信機は、起動信号発信機と共通化してもよい。例えば駅の入口に配置した起動信号発信機でもって、駅の構内に向かう方向に移動するスマートフォン端末等についてはB L E機能をO Nさせ、駅の構内から離れる方向に移動するスマートフォン端末等についてはB L E機能をO F Fさせる。このような起動信号発信機や終了信号発信機は、B L Eビーコン等が利用できる。

[0075] なお、G P Sを利用してスマートフォン端末等の個人携帯端末10の位置を特定できる場合は、G P Sでもって個人携帯端末10の位置を特定するようにしてもよい。この場合に、G P Sを利用できない屋内にスマートフォン端末等が入った場合に、これを検知して自動的にB L E機能をO Nにすると共に、位置特定信号の発信を開始するように構成してもよい。

[0076] このように、B L E機能のO N／O F Fを自動で切り替える機能を組み合わせることで、タッチレスでの認証、決済という本実施形態の位置特定システムの利便性を損なうことなく、非利用時にはB L EをO F Fしたままとすることも可能となって、利用者の利便性が一層向上する。

[実施形態2]

[0077] 以上の例では、ユーザの携行するスマートフォン端末等の携帯機器をB L E発信機として利用する例について説明したが、本発明はこの構成に限られ

ない。例えば、ユーザの携行するスマートフォン端末等の携帯機器をＢＬＥ受信機として、所定の位置に配置された複数のＢＬＥ発信機との間で通信を行うことにより、携帯機器の位置検出を行うように構成してもよい。このような例を実施形態２に係る位置特定システムとして、図２０に示す。この図に示す位置特定システムは、スマートフォン端末等をＢＬＥ受信機とし、ＢＬＥ発信機を２か所に配置した場合の例を示している。

[0078] 上述した例では、スマートフォン端末側を発信機として利用し、かつ受信器を複数個所に複数台設置することで、複数台で受信機感度のばらつきを低減すると共に、複数個所の差によって発信機の電波強度のばらつきを低減している（キャンセルアウト）。これに対して本実施形態では逆に、スマートフォン端末側を受信機として利用しつつ、発信器を複数個所に複数台設置しており、発信機同士の差を取ることで受信機の感度をキャンセルアウトしている。すなわち、受信機側又は発信機側の少なくとも一方を複数台とすることで、発信機側のアンプのばらつき（電波強度のばらつき）や、受信機側のアンプのばらつき（受信感度のばらつき）を低減して、キャンセルアウトの効果を発揮させている。なお、発信機の電波強度のばらつきは、一台ではさほど低減できない。これに対して複数台を設けることで、その箇所ごとに平均化することで、ある程度ばらつきを低減できる。

[0079] 図２１は、図２０の配置例において、ＢＬＥ発信機の電波強度差から求めたＢＬＥ受信機の存在エリアの例を示している。ＢＬＥ受信機の電波強度差から求められたＢＬＥ受信機の存在エリアは、アポロニウスの円もしくは直線を描く。ただし、一つの円もしくは直線だけでは、必ずしもＢＬＥ発信機の存在エリアを限定できない。

[0080] 一方図２２は、スマートフォン端末等をＢＬＥ受信機とし、ＢＬＥ発信機を３か所に配置した場合の例を示している。また図２３は、図２２の配置例において、ＢＬＥ発信機の電波強度差から求めたＢＬＥ受信機の存在エリアの例を示している。この場合、アポロニウスの円もしくは直線は３つ描かれることになる。このアポロニウスの円を描くことで、一致した点Ｘが生まれ

、この点Xが当該BLE受信機の存在する地点となる。ただし、直線が一つだけ描かれると、BLE受信機の位置が確定しない。必ず位置を特定できるような配置とする条件は、4つ以上のBLE発信機を、それにより描かれる四角形の辺においていずれも平行とならないように配置することである。

[0081] もしくは、図21のように、BLE受信機の存在エリアが、例えば直径40cm等、必要なサイズ以下である場合、その位置に存在するとして位置特定をすることもできる。例えば、2か所に配置したBLE受信機から異なる距離離れたBLE発信機の電波強度差が、ある閾値以上であることを条件とする。この条件下において、BLE受信機の存在エリアは、BLE発信機の電波強度差から計算して描かれるアポロニウスの円の内側の全体エリアとなるため、これを利用してもよい。

〔実施形態3〕

[0082] 上記の例では、複数の異なる箇所に配置された各BLE発信機は一台とした構成を示したが、本発明はこの構成に限られず、複数の異なる箇所に配置されるBLE発信機を、複数台とすることもできる。このような例を実施形態3に係る位置特定システムとして図24に示す。図24は、スマートフォン端末等をBLE受信機とし、複数のBLE発信機を2か所に配置した場合の例を示している。例えば、4つのBLE発信機を配置した場合、その4つのBLE発信機の強度を平均化すると、そのヒストグラムから求まる標準偏差は、BLE受信機から一定距離離れた1つのBLE発信機の電波強度のヒストグラムから求まる標準偏差のおよそ $1/2$ となっていることが確認できる。これにより、BLEの発信電波強度の時間的な測定変動を低減できることが判る。

[0083] 図25は、スマートフォン端末等をBLE受信機とし、複数のBLE発信機を3か所に配置した場合の例を示している。また図26は、スマートフォン端末等をBLE受信機とし、複数のBLE発信機を3か所に配置した場合に複数のBLE発信機の電波強度を平均化したものの差から求めたBLE受信機の存在エリアの例を示している。この場合、アポロニウスの円もしくは

直線は3つ描かれることになる。このアポロニウスの円を描くことで、一致した点Xが生まれ、この点Xが当該BLE受信機の存在する地点となる。ただし、直線が一つだけ描かれるとBLE受信機の位置が確定しない。必ず位置を特定できるような配置とする条件は、4つ以上のBLE発信機を、それにより描かれる四角形の辺においていずれも平行とならないように、配置することである。

[0084] もしくは、BLE受信機の存在エリアが、例えば直径40cm等、必要なサイズ以下である場合には、その位置に存在するとして位置を特定することもできる。図27は、BLE受信機の存在エリアを限定してBLE発信機の位置を特定する様子を示している。条件を調整することにより、BLE受信機の存在エリアが、スマートフォン端末等を持って移動しているユーザを一人ずつ高精度に区別する（例えば直径40cm以下）。例えば、2か所に配置したBLE受信機から異なる距離だけ離間させて複数のBLE発信機を配置する。これら複数のBLE発信機のそれぞれの箇所において、各BLE発信機の電波強度を平均化したものの差が、ある閾値以上であることを条件に、BLE受信機の存在エリアは、複数のBLE発信機の電波強度を平均化したものの差から計算して描かれるアポロニウスの円の内側の全体エリアとなる。

[0085] なお、複数のBLE受信機の受信電波強度が同じように検出できるように電波強度にオフセットを設定してもよい。また、BLE発信機から遠い側のBLE受信機を、近い側のBLE受信機から十分遠くに設置することにより、複数の近いBLE受信機に共通な遠い側のBLE受信機として扱ってもよい。これによっても、スマートフォン端末等を持って移動しているユーザを一人ずつ高速かつ高精度に捕捉、区別、認識することで、認証に付随する行動をタッチレスで自動化できるようにできる。

[0086] ただし、例えばレジや改札機において支払う場合、誤ってBLE受信機のないエリアにいると判断されると問題が発生する。これを誤認識と定義する。誤認識の確率自体を低くする必要があるところ、支払い等高精度な認識

が必要な場面においては誤認識を一層低減させるための工夫が必要となる。

図28は、支払い等高精度な認証が必要な場面で誤認識をさらに低くするための工夫の例を示している。図28のように、ユーザの通過判定エリアを二か所設け、その両方を一定時間差でユーザが通過した場合のみ認証することで、誤認識をさらに低くすることができる。つまり、たまたま片方のユーザの通過判定エリアに近づき、認証されてしまったとしても、他方のユーザの通過判定エリアが認証されない限り、通過したと判断されない。なお、これは図27の配置を利用してもよい。つまり、通過時の前半のユーザの通過判定エリアを設定する際には、図27のように、2か所に配置した、BLE受信機から異なる距離離れたそれぞれの箇所において複数のBLE発信機の電波強度を平均化したものの差が、ある閾値以上であることを条件にする判定方法を用いる。一方、通過時の後半のユーザの通過判定エリアを設定する際には、図27とは逆に、2か所に配置した、BLE受信機から異なる距離離れたそれぞれの箇所において、複数のBLE発信機の電波強度を平均化したものの差が、ある閾値以上であることを条件にする判定方法を利用できる。ただし、BLE送信機を複数配置するような上記の例の場合、BLE受信機は測定された電波強度結果、もしくはその電波強度から位置特定を行った結果等を、位置特定システムに通知する仕組みが別途必要となる。

[0087] なお、実際には電波強度を、例えば、図23や図26のようなBLE発信機の存在エリアである3つのアポロニウスの円や直線が一致した点を描くとは限らない。このため、3つ以上のアポロニウスの円や直線を用意し、最も誤差が小さくなるような位置をBLE受信機の位置として推定することが望ましい。これらの結果、実施形態1と同様に実施形態2でも、BLEの受信電波強度及び発信電波強度の時間的な測定変動を十分低減して、BLE受信機の位置特定が高速かつ高精度にできる。

[0088] 以上の実施形態1～3では、BLEを用いて距離や位置を特定乃至検出する方法について説明した。ただ本発明は、BLEに限らず、他の無線通信規格、例えばBLEでない他のBluetooth規格やWi-Fi、RFI

D、IMES、超音波、ZigBee、あるいは光通信等を用いてもよい。このような無線通信を用いることで、GPSを用いることなく、すなわち屋内においても安定的な位置特定が実現される。

(一方向通信における認証方法)

[0089] 一方で、認証を伴う位置特定には、別途セキュリティに関する問題が発生する。なぜなら、他人や他の装置が位置を成りすますと、例えばレジや改札機において必要な支払いをせずに目的を果たすことができってしまう。そこで次に、本発明の他の実施形態に係る一方向通信における認証方式について説明する。

[0090] まず、認証を行う方法としては、様々な手法が提案されている。ここで認証の3要素を図29に示す。一般的な認証方法として用いられる、例えばIDやパスワードは、利用者が知っている知識を利用している、知識情報の一つである。知識情報としては、IDやパスワードの他に、PIN番号や秘密の質問（一部所持情報と被る）等が挙げられる。

[0091] 次に、ドアのロック解除等で利用されているICカードは、利用者が所持していることを利用している、所持情報の一つである。所持情報としては、ICカードの他に、ワンタイムパスワードやUSBトークン、SMS認証、E-mail認証、ボイスコール、スマホアプリ認証、暗号表認証等が挙げられる。

[0092] さらに、指紋認証等は、利用者自身の特徴を利用した生体情報の一つである。生体情報としては、指紋認証の他、顔認証や虹彩認証、網膜認証、静脈認証等が挙げられる。

[0093] これらの知識情報、所持情報、生体情報といった情報を、認証をすることで、他者のなりすましをも防ぐ。また、これらの情報を複数組み合わせ、2段階認証や多要素認証等とすることで、高いセキュリティを確保することが可能である。

[0094] 現状利用されているこれらの認証方法において、非接触に手間なくセキュアに個人の認証を行うものは提案されていない。例えば、あるユーザが車の

ドアノブを触ったりすることで開錠をする方法はあるが、これは非接触ではない。また、あるユーザがＩＣカードをかざしたりスマートフォン端末等でＱＲコードやバーコード等のシンボルを読み取ることで支払いを行ったりする方法もある。これらの方法は接触ではないが、読み取りのためにＩＣカードやＱＲコード等を読み取り機に近接させる必要があり、ユーザにはポケットから取り出したり、かざすといった動作が必要となって、手間がかかる。さらに、鍵となる無線機器をあるユーザが携帯しつつ、自動ドアに接近することで開錠する方法においては、位置があいまいとなるため、仮に複数のユーザがいた場合、どのユーザを認証したかを識別することが困難となり、セキュアとは言えない。

[0095] そこでユーザの位置情報と組み合わせて利用する方法が考えられる。つまり、非接触に手間なくセキュアに個人の認証を行うことと、認証を受けようとする端末やＩＣカード等を持っている個人を特定することには、何らかの位置情報と切り離せない関係にあることが判る。

[0096] このような位置情報を測定する方法は複数考えられるが、位置情報を非接触に手間なく行う場合、電波等の無線や光、音等の空気中を伝搬できる物理的な媒体を利用する。屋外であればＧＰＳ等の相対性理論を用いた測定を行うことで、少数の位置特定装置２０で広範囲高精度な位置特定を行うこともできる。しかしながら、屋内においては様々な周波数における障害物が存在するため、多数の位置特定装置２０が必要になる。特に、セキュリティを確保するためにユーザの位置特定を行うためには、４０ｃｍ程度の精度が必要となる。このため、位置特定装置２０の設置間隔もより近いほうがよく、設置数が多くなりやすい。位置特定を行うにあたり、これらの多数の位置特定装置２０の一部及び全部と通信する必要が出るため、多数の通信路を確保しなくてはならない。このため、位置情報を得るには、多数の通信路を確保する必要がある。

[0097] 一方で、位置情報を測定したいユーザは複数いることが普通なため、単純な双方向通信を行おうとすれば、多対多の双方向通信を行うこととなる。こ

れでは、人数×位置特定装置20数だけ通信路を確保する必要が生じることとなって、通信周波数帯域が不足する懸念がある。

[0098] そこで、ユーザが持つ認証を受けようとする端末やICカード等、一台当たりの使用できる通信帯域を一つや二つ等に制限すること、もしくは位置特定装置20当たりの使用できる通信帯域を一つや二つ等に制限する等、一对多の双方向通信を行う対策が考えられる。

[0099] しかしながら、この場合はセキュリティの確保が困難になる。例えば、ユーザが持つ認証を受けようとする端末やICカード等が出す一意のID及び相当するものを含む信号を用いて、位置を特定した時点で位置特定と位置情報の認証が完了する。このため、ID及び相当するものを暗号化しなければならない。ところが、常に同じ暗号鍵を用いて暗号化手順を踏んでいた場合、暗号化されたID及び相当するものも常に一定のものとなってしまう、なりすましを受けやすい。つまり、暗号化されたID及び相当するもの自身を複製して発信することで、成りすましが可能となり得る。

[0100] これに対しては、通信の度に暗号鍵を変えたり、暗号化の手順を変えたりする等の方法が考えられる。しかし、この方法は本発明の実施形態においては、利用できない。なぜなら、一般に双方向通信を行う通信端末の間で、暗号鍵や暗号化手順の変更タイミングを同期、失敗時の調整等を行いながら安定的な通信を行っているところ、同じID及び相当するものがある通信帯域中を伝搬した場合には、一度通信が失敗した後に全体的な同期を取るために非常に時間がかかり得るからである。この結果、一度通信が失敗した通信端末は、なかなか通信を回復できない。

[0101] そこで、本実施形態においては、多対多での通信を行う場合の通信方法として、一方向通信を採用している。ここでは、ユーザが携行する、認証を受けようとする端末やICカード等から位置特定装置20側に一方向に通信を行い、その情報を基に位置特定装置20とユーザの携行する認証を受けようとする端末やICカード等との位置特定を行う。あるいは逆に、位置特定装置20側から、ユーザの認証を受けようとする端末等に一方向通信を行い、

その情報を基にこれらの位置特定を行う。例えば、BLEで通信を行う場合は、BLEビーコンで一方向通信を行うことができる。このような一対一あるいは一対多の一方向通信においては、毎回ワンタイムパスワードを発行することで、セキュリティの問題を解決できる。

- [0102] なお、位置情報を測定する方法は、本実施形態に限定されない。例えば、ユーザが持つ認証を受けようとする端末やICカード等が出す一意のID及び相当するものに対し、毎回ワンタイムパスワードとなるものを追加して送信するだけで、その信号を用いて位置を特定しつつ、そのワンタイムパスワードを認証することで、複数の位置特定装置20において受信の度ごとに位置特定と位置情報の認証を完了させられる。この信号は一度しか利用できないために、盗まれても二度目の認証はされない。また、複数の位置特定装置20のいずれかで受信が失敗しても、直後から受信を行うことができるため、非常に安定的な通信が行える。

(ワンタイムパスワード)

- [0103] ところで、既存のワンタイムパスワードには、上記の仕様を満たすものが存在しなかった。現在利用されているワンタイムパスワードとして、(1) ハッシュチェーン型；(2) 時刻同期型；(3) チャレンジ型；(4) トランザクション型等が存在している。

- [0104] (1) ハッシュチェーン型とは、ハッシュ関数等、一方向性関数を用いたものである。ハッシュ関数とは、ある数値からある数値を求める関数であるが、一般に、求まった数値から元の数値を特定することができない。このため、ハッシュ関数のような一方向性関数を繰り返し適応することで、必要個数のパスワード列を作成できる。このパスワード列を逆から有効時間ごとにワンタイムパスワードとして利用する。仮にこのパスワードを知ったとしても、有効時間後の次のパスワードを求めることはできない。また、パスワード列は無限に生成することはできない。

- [0105] (2) 時刻同期型とは、時刻から求めるトークンを用いて認証するものである。認証を受ける装置と認証する装置の内部で、同じアルゴリズムを用い

て、時刻からトークンを求めて、一致するかどうかで認証する。仮に、それぞれの装置間で時刻が少しずれていたとしても、認証する装置がその時間のずれを検知して、認証を受ける装置用の自身の時刻を修正しつつ、認証を行う。これにより、常に同期した時刻で認証が行える。ただし、同期をするためには、トークンの更新時間を、例えば一分とし、時間のずれを、例えば1秒等といった時間範囲で許容するため、ms単位等での修正は不可能である。

[0106] (3) チャレンジ型とは、認証する装置から出された問題（チャレンジ）に対して、認証を受ける装置が回答（レスポンス）を行うものである。回答を複製されるのを避けるため、通常同じ問題が出された場合、以前とは異なる回答となるような仕組みが組み込まれている。なお、このチャレンジ型は、双方向通信を前提としている。

[0107] (4) トランザクション型とは、事前にパスワードのリストを用意しておき、認証の度に一つずつ利用するものである。一つのパスワードは一度しか利用できない。このパスワードのリストを無限に生成することはできない。

[0108] 次に、多対多の一方向通信におけるセキュリティに必要な要件として、（1）一方向通信に利用可能；（2）無限回利用可能；（3）位置特定等に必要な高速性を有する；という3点を満たすものが必要である。しかしながら、現在発明利用されているワンタイムパスワード方式では、いずれもこれらの条件をすべて満たすことができない。

[0109] そこで、本実施形態においては、暗号化された時間を送ることでこの問題を解決している。すなわち、ある確立された通信環境においては、送信側と受信側との時間差が概ね一定であることを利用して、送受信の時間差を確認することにより、通信の真偽を判定するよう構成している。具体的には、個人携帯端末が、位置特定装置にデータを送信する際、識別情報とワンタイムパスワードを送信する。このとき個人携帯端末では、ワンタイムパスワードを発行する際に、発行時刻を取得し、この発行時刻の情報を共通鍵でもって暗号化して、ワンタイムパスワードを発行する。この識別情報とワンタイム

パスワードを、個人携帯端末は位置特定装置に送信する。

- [0110] 一方で、位置特定装置側では、個人端末側発信部から識別情報とワンタイムパスワードを受信すると共に、この際の受信時刻を、位置特定側時刻部より取得する。そして受信した識別情報から、この識別情報に対応する共通鍵を位置特定側記憶部より探索し、得られた共通鍵を用いてワンタイムパスワードを復号化して、関数化された発行時刻に関する情報を取得する。これによって、ワンタイムパスワード発行時の発行時刻（言い換えると個人携帯端末側での送信時刻）に関する情報と、受信時刻に関する情報を取得できるので、これらの差分を取得する。
- [0111] このようにして、送られるデータのパスワード発行時刻と受信時刻の差分、すなわち送信時から受信時までの時間差をデータ通信毎に測定する。一般に、送信側と受信側が一定の通信環境下に置かれている場合、通信環境が短時間に大きく変動することは考え難い。例えば、スマートフォン端末を持った利用者が駅の自動改札機を通過する際、BLEで通信する速度は、この利用者が自動改札機を通過するまでの間においては一定と想定することができる。
- [0112] このように、データ通信毎（例えばパケット毎）に、通信に要する時間が一定であれば、送信時から受信時までの時間差は一定になる。その一方で、不正に自動改札機を通過しようとする不正利用者が、別の正規の利用者であるかのように振る舞う、なりすましなどの不正アクセスを考える。この場合は、一般に、なりそうまそうとする正規利用者が、実際に不正利用者の近くにいるとは考え難く、遠隔地からインターネット等の通信経路を用いてアクセスすると考えられるところ、この場合の送信時と受信時との時間差は、正規利用者の時間差とは異なる（例えば時間がより長くなる）と思われる。
- [0113] このような想定に基づいて、データ通信毎に送信時と受信時の時間差を測定し、これが一定であれば、正しく通信が行われており、一定でない場合は、なりすましなどの不正アクセスが疑われる。この結果、送信時刻を暗号化して送信し、送受信の時間差をモニタすることで、時間差が大きく異なった

場合に不正アクセスと判別できるので、個人携帯端末の認証を行うことが可能となる。

[0114] また、このような個人携帯端末の認証は、位置特定装置に接近する度に毎回行う。例えばスマートフォン端末を持った利用者が自動改札機を通過する度毎に行う。これによって、自動改札機の設置された環境毎に通信速度が異なっているとしても、環境毎に送受信の時間差が測定されるため、正しく認証される。このため、一旦取得した時間差の情報は、一定時間経過後に消去することが好ましい。

[0115] 例えば、あるタイミング（好ましくはデータ通信の最初の段階）の受信時刻において取得した発行時刻と、取得された受信時刻との差分を認証基準情報として、位置特定側記憶部等に保存しておく。そして保存してから一定時間は、この認証基準情報を標準の送受信の時間差として認証を行う。すなわち、一連の通信データについて、受信時刻と発行時刻との差分を、認証基準情報と比較し、同一もしくはほぼ同じと見なせるレベルであれば、認証を行い、差が大きい場合は、認証しない。これによって、スムーズな認証を行うことができる。そして、一定時間経過後は、認証基準情報を削除することで、新たに通信を行う際は、再度、新たな認証基準情報を取得して書き換えることで、一時的になりすましに成功した場合でも、次の認証時にはこれを排除することが可能となって、一層セキュリティを向上できる。

[0116] ここで、暗号化された時間を送り、認証する様子を図30に示す。例えば、アリスとボブが一方向通信を行うとする。事前に、アリスとボブは安全な方法でアリスが持つ認証を受けようとする端末等が出す一意のID等の識別情報と、それとセットとなる暗号鍵を、アリスとボブとの間で共有しておく。アリスが持つ認証を受けようとする端末等が出す一意のID等に、その端末等の持っている時刻を、例えばUNIX時間等の1970年からの時間に、例えばms単位で暗号化し、ID等とその暗号化された時間が一体となった信号としてアリスはボブに送信を行う。受信したボブは、受信したID等を基に、解読のための暗号鍵を検索し、その暗号鍵を用いて暗号化された時

間を復号し、受信した時刻との差を求める。そして、次のタイミングに受信した信号に対して同様な処理を行い、先ほどの復号された時間と受信した時刻との差が一致するかどうかを確認する。一致する場合は、アリスからの信号と認証し、一致しない場合は、認証しない。以降、これを繰り返す。なお、基準とする信号は何時の時点のものでもよい。

[0117] もしくは、受信したボブは、受信したID等を基に、解読のための暗号鍵を検索し、その暗号鍵を用いて暗号化された時間を復号し、受信した時刻と一緒に記録しておく。そして、次のタイミングに受信した信号に対して同様な処理を行い、復号された時間どうしの差と受信した時刻どうしの差が一致するかどうかを確認する。一致する場合は、アリスからの信号と認証し、一致しない場合は、認証しない。以降、これを繰り返す。なお、基準とする信号はいつのものでもよい。

[0118] なお実装に当たっては、例えば1ms以下といった、ある閾値以下の誤差は許容するが、数秒といった単位での時刻差は認めない、等の処理を付加してもよい。

[0119] この方法を用いることで、この信号は一度しか利用できないために、盗まれても二度目の認証はされない。また、複数の位置特定装置20のいずれかで受信が失敗しても、直後から受信を行えるため、受信後に認証を行うことができ、非常に安定的な認証が行える。

[0120] 特に、通信データが盗まれた場合、暗号化された時間と受信のタイミングとが異なるため、二度目の認証がされないだけでなく、仮にアナログ回路を用いる等、高速に単純な信号複製が行われたとしても、同じ信号を二回以上受け取った時点でなりすましが判明する。もしくは、単純な信号複製があった場合、近くで発信を行っているユーザすべての信号を複製してしまうため、一か所に複数人がいるように位置特定が行われてしまうため、なりすましが判明する。

[0121] なお、IDのビット数は、例えば40ビット等でよい。40ビットはおおよそ1兆人分のIDを用意することができるため、一意に設定することができる。

る。また、IDはOSI参照モデルのどのレイヤーでもよい。また、時間のビット数は、例えば48ビット等でよい。48ビットは4000年間程度をマイクロ秒で表現できるだけの空間がある。

[0122] なお、暗号化をする前に、時間を予測できない形に表現を変えてもよいし、パディング処理等をしてよい。また暗号化としては、例えば3DESやAES等の共通鍵暗号を利用してもよいし、楕円暗号等の公開鍵暗号を利用してもよい。さらに、時間をms単位に変換するにあたり、1970年からの時間をmsで測定してもよいし、秒単位で測定した時間にms単位を付加してもよい。

[0123] また時間は、必ずしも1970年からの時間と一致している必要はなく、誤差を許容する仕組みとしている。ただし、あまりも時間がずれている場合、セキュリティ面で問題となる。仮に、アリスとボブが本実施形態に係る方法を用いて一方向通信を行い、アリスが発信する信号間隔はランダムとし、イブが攻撃者であるとする。この場合、イブがアリスの発信信号とその信号の発信タイミングのセットを記録し、イブが同じ発信信号をその信号の発信タイミングで発信した場合、ボブはアリスであるかどうかを区別できない。このため、信号を発信し続けている間となるような、例えば10秒程度以下で一致している必要がある。そのため、適宜、時刻サーバとの同期等も行うことが望ましい。

[0124] さらに、一定時間（例えば一日など）ごとにスマートフォン端末等を異なる本人認証する仕組みがあってもよい。なお、この一定時間（例えば一日など）が経過した後、本人認証を促す文章等を提示してもよいし、あるいは一定時間（例えば追加して一日など）は有効としてもよい。

〔実施形態4〕

[0125] なお、本実施形態に係る一方向通信における認証方法は、位置特定を必要としない一般的な一方向の信号にも利用できる。つまり、一方向通信の一種であるBLEビーコンや、業務無線等においてセキュアに暗号化された認証方式として利用することができる。ここで実施形態4として、位置特定を必

要としない認証システムの機能ブロック図を 図 3 1 に示す。この図に示す認証システム 4 0 0 は、位置を特定する対象となる個人が携帯する個人携帯端末 1 0 と、個人携帯端末 1 0 の位置を特定する位置特定装置 2 0 とを備える。個人携帯端末 1 0 は、個人端末側発信部 1 1 と、個人端末側制御部 1 2 と、個人端末側記憶部 1 3 と、個人端末側時刻部 1 4 を備える。個人端末側発信部 1 1 は、位置特定装置 2 0 に対し、双方向通信を行う。個人端末側制御部 1 2 は、個人端末側発信部 1 1 を制御する。個人端末側記憶部 1 3 は、予め付与された固有の識別情報と、個人携帯端末 1 0 と位置特定装置 2 0 との間で予め交換された、該個人携帯端末 1 0 に付与された識別情報に固有の共通鍵と、ワンタイムパスワードの生成に利用する所定の関数とを保持する。個人端末側時刻部 1 4 は、時刻に関する情報を生成する。

[0126] 一方、位置特定装置 2 0 は、位置特定側受信部 2 1 と、位置特定側演算部 2 5 と、位置特定側記憶部 2 6 と、位置特定側時刻部 2 7 を備える。位置特定側受信部 2 1 は、個人端末側発信部 1 1 と双方向通信を行う。位置特定側演算部 2 5 は、位置特定側受信部 2 1 で個人端末側発信部 1 1 と通信を行うことにより、個人携帯端末 1 0 の認証を行う。位置特定側記憶部 2 6 は、個人携帯端末 1 0 に付与された識別情報と、該識別情報毎に固有の共通鍵とを関連付けて保持する。位置特定側時刻部 2 7 は、時刻に関する情報を生成する。

[0127] 個人端末側制御部 1 2 は、個人端末側発信部 1 1 で位置特定側受信部 2 1 と通信を行う際に、個人端末側記憶部 1 3 に保持された固有の識別情報と、該識別情報毎に固有の一回のみ使用可能なワンタイムパスワードを発行する。また位置特定側演算部 2 5 は、位置特定側受信部 2 1 で個人端末側発信部 1 1 から受信した識別情報及びワンタイムパスワードを認証する。

[0128] 個人携帯端末 1 0 が、位置特定装置 2 0 に識別情報及びワンタイムパスワードを送信するに際して、個人端末側制御部 1 2 が、ワンタイムパスワードを発行する際の発行時刻に関する情報を個人端末側時刻部 1 4 で取得し、個人端末側記憶部 1 3 に保持された所定の関数に適用し、さらに個人端末側記

憶部 13 に保持された共通鍵でもって暗号化して、ワンタイムパスワードを発行する。

[0129] 一方で位置特定側演算部 25 は、位置特定側受信部 21 で、個人端末側発信部 11 から識別情報及びワンタイムパスワードを受信する際の受信時刻を、位置特定側時刻部 27 より取得する。そして、受信した識別情報から、該識別情報に対応する共通鍵を位置特定側記憶部 26 より探索し、得られた共通鍵を用いてワンタイムパスワードを復号化し、関数化された発行時刻に関する情報を取得する。さらに、取得された発行時刻に関する情報を、取得された受信時刻に関する情報と比較し、差分を取得する。すなわち、受信時刻から送信時刻を引いた、通信に要する時間に関する情報を取得する。次に、別のタイミングで同様の処理を行って送受信に要した時間を取得して、先の送受信に要した時間と同じであれば、正しい通信が行われていると判定し、この個人携帯端末を認証する。一方で、送受信に要する時間が、先の時間と大きく異なっている場合は、不正アクセスと判断して認証しない。これにより、個人携帯端末 10 を携帯する個人を認証することが可能となり、個人を区別した位置検出が可能となる。

[0130] なお、送受信に要する時間は、通信環境が一定で変化しないと想定できる場合は、各通信で同じ時間となる。ただし、個人携帯端末や位置特定装置、サーバ等の各機器が有する時刻情報は、世界時計や時刻サーバに従って時刻を修正しているが、これらの時刻には多少のずれがある。そのため、各個人携帯端末や位置特定装置が有する時刻は、本来的に完全には一致していない。ここで、仮に機器間に 100ms 程度の誤差がある場合を考える。時間差がこれだけあると、遠隔地からのなりすましが可能となってしまう。遠隔地といえども、通信には数十ms しかかからない場合が多い。仮に遠隔地で、ユーザ A の個人携帯端末の発信情報を勝手に盗んで、他の地点で同様の発信を行うと、なりすませてしまう。これを阻止するためには、数ms 程度でも誤差を許容しないことが考えられる。

[0131] そこで本実施形態においては、上述の通り通信毎に送受信に要する時間を

認証基準情報として保持し、この値との比較で認証を行うようにしている。遠隔地からの通信では、通信網での渋滞等によって時間差のブレが発生する。その一方で、現地にいるユーザAの個人携帯端末から位置特定装置への通信は光速に近い高速のため、通信路上での通信時間のブレが、ほぼ発生しない。この結果、なりすましを効果的に阻止することが可能となる。ただし、他者がこの発信タイミングとデータを記録等して、保持することにより、タイミング良く発信を行うことができれば、なりすましてしまう可能性がある。このため、絶対的な時間差の制限を加えることが好ましい。例えば、絶対的な時間差として1秒以内や100ms以内といった基準時間差を設定して制限を加える方法が挙げられる。自動改札機の場合は、後述の通り自動改札機側で受信した時刻と、復号化した時刻（すなわち個人携帯端末側の送信時刻）との時間差を取得できるので、この時間差が予め設定された基準時間差よりも大きい場合は、当該データを破棄することでなりすましを回避できる。

[0132] 本実施形態に係る一方向通信における認証方法によれば、一般的な双方向通信時の公開鍵暗号等を用いる認証方法よりも高速な認証が可能となる。また、一般に多数のユーザと通信を行う業務無線等でよく利用される一方向通信の暗号化は、事前に決めた共通鍵で暗号化されている場合が多い。その場合、共通鍵は通信機器内に埋め込まれている。このため、ある通信機器で共通鍵が漏れてしまった場合には、セキュリティ問題が全体に波及し易い。これに対して本実施形態では通信機器ごとに異なった共通鍵を提供してもよいので、このようなセキュリティ問題の影響を受け難い。つまり、高度な位置情報がなくとも、ドアノブを触る方法や、ICカード、スマートフォン端末等でQRコードを読み取る方法や、BLEビーコン等を用いる方法で、開錠や支払いを行う際に、本実施形態に係る一方向通信における認証方法を利用して認証することも可能である。これにより、スマートフォン端末等を携行して移動しているユーザを、一人ずつ高速かつ高精度に捕捉、区別し、非接触に手間なくセキュアに個人認証することで、認証に付随する行動をタッチ

レスで自動化できるようにできる。

- [0133] なお、セキュリティが不要な場合、BLE発信機には演算部等は不要である。また本実施形態のように位置特定のためや認証のために発信する信号は、通信帯域を圧迫させる可能性がある。このため、必要な領域や範囲、時間等に限って発信することが産業発展のためには非常に望ましい。以下、本実施形態の例示的な実施例を説明する。

[実施例1]

(事後支払いシステム)

- [0134] 実施例1では、駅の改札機において利用者が個人携帯端末10を取り出すことなく利用できる例について説明する。なお、同様な事後支払いシステムをバス等の公共交通機関に適応することも可能である。鉄道やバス等の事後支払いシステムの概略を図32に、フローチャートを図33に、それぞれ示す。図32に示す事後支払いシステムは、登録支払管理システム及び利用管理システムを有する管理サーバと、改札機を設置した駅と、利用者の保有する個人携帯端末10と、鉄道会社とで構成される。なお、ここでは利用者が鉄道等を利用後に料金を支払う事後支払いの例を説明するが、本発明は事後支払いに限らず、前払いや同時決済にも利用可能である。

- [0135] この事後支払いシステムによる事後支払いの手順を、図33のフローチャートに基づいて説明する。まずステップS3301において、利用者の個人携帯端末10に、改札チケットの事後支払いを行うための専用のアプリを予めインストールしておく。またこの専用アプリに個人情報、例えば氏名や支払用のクレジットカード番号などを登録しておく。

- [0136] 次にステップS3302において、個人携帯端末10から専用アプリによりID共通鍵(例えば3DES等)を登録サーバの登録支払管理システム側に送信する。またステップS3303において、必要なタイミングでクレジットカード情報を登録支払管理システムがクレジットカード会社との間で認証する。さらにステップS3304において、入力された個人情報を個人情報サーバに保管する。さらにまたステップS3305において、ID共通鍵

利用期間リストを、登録支払管理システムから利用管理システムに送信する。

- [0137] 次にステップS 3 3 0 6において、利用者が鉄道会社を利用する際に、改札機を通過するタイミングで、改札機端末同期処理を行う。そしてステップS 3 3 0 7において、改札接近時に個人携帯端末1 0から、位置特定装置2 0である自動改札機に対しB L E発信を行う。
- [0138] 次にステップS 3 3 0 7において、位置特定システムを稼働させて、個人携帯端末1 0の位置特定を行う。さらにステップS 3 3 0 8において、利用管理システムに位置特定した結果を送信する。
- [0139] 最後にステップS 3 3 0 9において、管理サーバから個人携帯端末1 0に対し、請求や支払、O Dデータの提出等を行う。
- [0140] 次に事後支払いシステムの詳細な構成図を図3 4に示す。この図に示す事後支払いシステムは、管理サーバシステム3 0と、事業者用管理システム4 0と、管理端末5 0と、位置特定装置2 0と、個人携帯端末1 0と、金融機関6 0と、時刻配信サーバ7 0で構成される。各部材は、通信機能を備えており、通信ネットワークを介して相互に接続されている。例えばW A NやL A N、セルラー通信網、W i - F i、B l u e t o o t h、インターネット等のネットワークを介して通信する。なお、双方向通信の場合は、公開鍵暗号や共通鍵暗号を用いて暗号化、電子証明書、電子署名を行うことができる。そのために必要な鍵の生成、保存等を、それぞれの部材が有する演算部と記憶部、必要に応じてI D・暗号鍵データベースとで行う。また必要に応じて、認証局の認証も利用できる。なお、一般的な演算部やセンサ、その他の処理は、ソフトウェアで実装されていてもよいし、ハードウェアで実装されていてもよい。例えば、C P U等で実行させるソフトウェアで実現されていてもよいし、L S IやA S I C、F P G A等のハードウェアで実現されていてもよい。また、一般的なメモリ等の記憶装置は必要に応じてそれぞれの構成要素に含まれるものとする。例えば、R O M、フラッシュメモリ、H D D、S Dカード等の不揮発性の記録媒体と、R A M、レジスタ等の揮発性の記

録媒体とによって実現されていてもよい。このように、本明細書において〇〇演算部というとき、演算部はコンピュータやサーバなどのハードウェアで構成する他、ソフトウェアとして実現させる構成としてもよい。またハードウェアで構成する場合は、CPUやLSI、ASIC等の演算処理装置を利用できる。同様に本明細書において〇〇記憶部という場合は、ハードディスクや不揮発性の半導体メモリ等が利用できる。

- [0141] 本実施例では、事業者用管理システム40は、例えば鉄道会社のIT管理担当部署等に設置してもよい。また管理端末50は、駅等に設置してもよい。位置特定装置20を自動改札機とし、複数設置してもよい。なお、事業者用管理システム40、管理端末50は、より構成要素を少なくしたより簡易なものでもよい。また、個人携帯端末10は、複数のセンサが構成要素としてあってもよい。なお、バスにおいて利用する場合、管理端末50はバスの事業所等に設置してよく、位置特定装置20はバス内に設置してよい。また、通信をインターネットでする代わりに、SDカード（商品名）等が必要なデータのやり取りをしてもよい。

（管理サーバシステム30）

- [0142] 管理サーバシステム30は、サーバ側通信部31と、サーバ側演算部32と、サーバ側記憶部33と、サーバ側利用情報データベースと、サーバ側個人情報データベースと、サーバ側ID・暗号鍵データベースで構成されるサーバ群であり、一台もしくは複数台のサーバからなっている。管理サーバシステム30は、全体と接続されているものであり、本実施例の全体システムを統括するものである。管理サーバシステム30は、個人のデータを登録し、さらに個人と位置特定装置20を利用する事業者間のサービス利用を中継するものである。また、個人のデータの中に支払い情報が含まれる場合、利用者が利用した事業者のサービス利用料を提供された事業者のサービス利用料表に基づき、利用者の支払い手段から徴収する。また、金融機関60と通信を行い、与信審査や認証の確認を登録時及び随時行う。その結果を個人携帯端末10や管理端末50、位置情報認証装置等に通知できる。それぞれの

サーバ側データベースは、複数の異なるデータ保存場所に存在していてもよい。なお、個人携帯端末10からの通信は極力常時接続されないといけませんが、事業者及びその他のシステムとは必ずしも常時接続されている必要はなく、少なくとも2種類以上のサーバに分けて安定性を考慮した運用方法が望ましい。なおサーバ側利用情報データベース、サーバ側個人情報データベース、サーバ側ID・暗号鍵データベースは、個別のサーバとする他、統合することもできる。あるいは、サーバ側記憶部33に組み込んでもよい。

- [0143] サーバ側ID・暗号鍵データベースは、管理サーバシステム30に送られてきた個人携帯端末10の一意的IDとセットとなる暗号鍵、利用場所、利用期間等を保存し、管理端末50や位置特定装置20へ配信する。なお、入出場記録を含んでもよい。また暗号鍵は、3DESやAES暗号等の共通鍵暗号でもよいし、RSAやDSA、楕円暗号等の公開鍵暗号でもよい。なお、BLEビーコンにおいては、3DESのように短いビット数が望ましく、共通鍵暗号のように計算コストが低いものが望ましいが、扱えるビット数に応じて暗号方式はより安全性が高く計算コストが比較的高くないものに徐々に移行することが望ましい。

(事業者用管理システム40)

- [0144] 事業者用管理システム40は、事業者側通信部41と、事業者側演算部42と、事業者側入出力部43と、事業者側利用情報データベースと、事業者側記憶部44とを備える。事業者用管理システム40は、管理サーバシステム30に登録されている利用者から利用申請を受け付けて、その事業者の行っているサービス等を利用者が利用することで得られる収入や利用情報を得られるシステムである。なお、事業者は提供するサービスに応じて、その利用者に対して位置特定装置20の利用場所、利用期間等を指定することができる。また、事業者が提供するサービスに基づいて利用者から利用料を徴収する場合、事業者は事業者用管理システム40を通じて、サービス利用料表を管理サーバシステム30に提供する。また、利用者からの許諾がある範囲で、事業者が提供するサービスの範囲を超えて利用者情報を得ることができ

得る。同様に、利用者からの許諾がある範囲で、管理サーバシステム 30 が解析した利用者情報を得ることができ得る。なお、例えば、事業者側入出力部 43 はなくてもよいし、他のシステムと接続されて利用されていてもよい。

(管理端末 50)

[0145] 管理端末 50 は、管理端末側利用情報データベースと、管理端末側時刻部 54 と、管理端末側 ID・暗号鍵データベースと、管理端末側通信部 51 と、管理端末側演算部 52 と、管理端末側入出力部 53 と、管理端末側記憶部 55 を備える。管理端末 50 は、主に位置特定装置 20 の管理と管理サーバシステム 30 と位置特定装置 20 との中継とが目的であり、位置特定装置 20 に必要な、管理端末側時刻部 54 と、管理端末側 ID・暗号鍵データベースとを一時的に保持し、位置特定装置 20 に配信する。また、位置特定装置 20 から上がってくる利用情報を、管理端末側利用情報データベースに記録し、管理サーバシステム 30 に送信することができる。また、個人情報のデータベースの中に支払い情報が含まれる場合、与信審査や認証の確認結果を受信し、管理端末側 ID・暗号鍵データベースに記録したり、位置情報認証装置等に通知したりできる。これにより、管理サーバシステム 30 が停止していても、管理端末 50 以下で運用が可能である。なお、この管理端末 50 は、複数台の位置特定装置 20 を管理することを主眼としているため、管理端末 50 の機能を、一台又は複数台の位置特定装置 20 に委譲してもよい。

[0146] 管理端末 50 には、他に 2 つの役割がある。一つは、位置特定装置 20 の通過データを集計する役割である。例えば、当駅にはどこの駅からの利用客が多いのかを分析し、今後の列車ダイヤを組んで行く上での参考データとする。このような通過データを利用情報データベースに蓄積し、例えば 5 分単位等で集計して管理サーバシステム 30 に送信してもよい。管理サーバシステム 30 及び管理端末 50 では、この情報を使って駅の混雑情報、集中度の算出や旅客流動調査を行ってもよい。

[0147] もう一つの役割は、利用者へのサービスである。具体的には、利用者の入

出場記録の確認と整合性の修正等を行う。この際、カメラ、マイク等の入出力装置を使ってセンターの係員が対話しながら対応をしてもよく、同時に障害時の対応や、新企画券の案内、販売等もできる。

[0148] また管理端末側時刻部54は、例えばms単位よりも高精度に時刻をカウントできればよい。ここで、必ずしも正確な時刻ではなくてもいいが、例えば1分以下程度で一致している必要がある。そのため、一般的な時刻配信サーバ70を利用する等して、できるだけ時刻を修正しておくことが望ましい。時刻のずれが大きい場合は、端末や装置管理者にエラーとして修正を促すこともできる。

[0149] なお、通信装置は、Bluetooth送受信機能を利用して、個人携帯端末10の状態を確認してもよいし、個人携帯端末10への駅の接近を知らせてもよい。

[0150] なお、キセル対策等のために、位置特定装置20から送られてきた入出記録を管理端末側記憶部55や管理端末側ID・暗号鍵データベースに保持したり、管理サーバシステム30に送ったりしてもよいし、位置特定装置20からの参照にこたえてもよい。

[0151] また、管理端末側入出力部53に画像取り込み部を設けてもよい。画像取り込み部は、位置特定装置20が取得したユーザと位置から、その後の位置特定を、例えばBLEビーコンから画像に切り替えてもよく、その情報を位置特定装置20に伝えてもよいし、個人携帯端末10からの、例えば、BLEビーコンの発信を停止させてもよい。

(位置特定装置20)

[0152] 位置特定装置20は、位置特定側通信部21Aと、位置特定側制御部28と、位置特定側演算部25と、位置特定側ID・暗号鍵データベースと、位置特定側時刻部27とを備える。位置特定装置20は、個人携帯端末10の位置を、高速かつ高精度に位置特定・認証を行うことで、個人携帯端末10をわざわざ取り出したりすることなく通過できるようにする。なお、サービス提供に必要な支払いがある場合は、事後に自動的に金融機関60とのやり

取りにより行われる。また、与信審査や認証の確認結果を受信し、位置特定側 I D ・暗号鍵データベースに記録することができる。

[0153] 位置特定側通信部 21A は、位置特定側受信部 21 として機能する。位置特定側制御部 28 は、位置特定側演算部 25 で測定された個人携帯端末 10 の位置に応じて、個人携帯端末 10 を携帯する個人の移動を規制する動作を制御する。これにより、個人携帯端末 10 を携帯する個人を認識しながら、この者の位置に応じて、その移動を制御することが可能となる。ここで位置特定装置 20 は、例えば個人携帯端末 10 を携帯する個人の通過を規制する開閉式の扉部 29 を有するゲート型の自動改札機とすることができる。この場合は、位置特定側制御部 28 が、扉部 29 の開閉を制御する。これにより、個人の認識と位置検出によって、個人携帯端末 10 を携帯する個人の通過を規制する自動改札機の扉部 29 の開閉の可否を判断できる。

[0154] 位置特定側記憶部 26 は、自機を動かすためのソフトウェアや、自機が設置された駅の識別情報や、自機の識別情報、表示部用の表示情報を保持している。なお、各駅間（又は利用距離ごと）の料金が記憶された料金テーブル、各駅間の距離等を格納していてもよい。

[0155] 位置特定装置 20 の外観構成例を図 35A に、平面図を図 36A に、図 36A の XXXV I B - XXXV I B 線における断面図を図 36B に、それぞれ示す。これらの図に示す位置特定装置 20 は、自動改札機である。この自動改札機は、一对の区画板 24 を略平行姿勢で離間させている。一对の区画板 24 を構成する区画板 24A、24B のそれぞれは、剛体として電波を透過可能な、例えば樹脂等で構成されており、必要に応じてその一部を、電波を透過しない金属で構成してもよい。なお本発明者が試作した位置特定装置 20 の大きさは、高さ 90 cm、横幅 75 cm、奥行き 180 cm とした。

[0156] 位置特定装置 20 は、図 36A に示すように、一对の区画板 24A、24B の間で、利用者の動線に沿って通過判定エリア DA と通過判定エリア DB を画定している。ここでは、図において右側を自動改札機の入口として、通過判定エリア DA を入口側に、また通過判定エリア DB を自動改札機の出口

側に、それぞれ配置している。なお、通過判定エリアD Aを出口側に、通過判定エリアD Bを入口側にしてもよく、また入口と出口を規定せず、双方向に利用者が移動することを許容する場合も、同様である。

[0157] 通過判定エリアD Aの近傍に、位置特定側受信部2 1を設置し、通過判定エリアD Aに利用者が存在するか、あるいは存在しないかを、この位置特定側受信部2 1で判定する。このため通過判定エリアD Aの近傍には、位置特定側受信部2 1を構成する第一位置特定側受信部2 2、第二位置特定側受信部2 3として、BLEビーコン受信機2 1 1 1、2 1 1 2、2 1 1 3、2 1 1 4を設置している。ここでは第一位置特定側受信部2 2 A、2 2 Bとして、BLEビーコン受信機2 1 1 1、2 1 1 2を、区画板2 4 Aに隣接して設けている。また第二位置特定側受信部2 3 A、2 3 Bとして、BLEビーコン受信機2 1 1 3、2 1 1 4を、区画板2 4 Bに隣接して設けている。

[0158] 同様に、通過判定エリアD Bの近傍には、位置特定側受信部2 1として、BLEビーコン受信機2 1 1 5、2 1 1 6、2 1 1 7、2 1 1 8を設置している。ここでは第一位置特定側受信部2 2 A、2 2 Bとして、BLEビーコン受信機2 1 1 5、2 1 1 6を、区画板2 4 Aに隣接して設けている。また第二位置特定側受信部2 3 A、2 3 Bとして、BLEビーコン受信機2 1 1 7、2 1 1 8を、区画板2 4 Bに隣接して設けている。

[0159] 図3 6 Aの平面図に示すように、BLEビーコン受信機2 1 1 1、2 1 1 2の組を中心とする同心円形状の通過判定エリアとして、通過判定エリアD A 1を規定する。またBLEビーコン受信機2 1 1 3、2 1 1 4の組を中心とする同心円形状の通過判定エリアとして、通過判定エリアD A 2を規定する。さらにBLEビーコン受信機2 1 1 1、2 1 1 2の組、及びBLEビーコン受信機2 1 1 3、2 1 1 4の組を結ぶ線分の中点を中心とする同心円形状の通過判定エリアとして、通過判定エリアD Aを規定する。同様に、BLEビーコン受信機2 1 1 5、2 1 1 6の組を中心とする同心円形状の通過判定エリアとして、通過判定エリアD B 1を規定する。またBLEビーコン受信機2 1 1 7、2 1 1 8の組を中心とする同心円形状の通過判定エリアとし

て、通過判定エリアDB2を規定する。さらにBLEビーコン受信機2115、2116の組、及びBLEビーコン受信機2117、2118の組を結ぶ線分の中点を中心とする同心円形状の通過判定エリアとして、通過判定エリアDBを規定する。このように、通過判定エリアDAは通過判定エリアDA1、DA2も含む広い範囲を示し、また通過判定エリアDBも通過判定エリアDB1、DB2も含む広い範囲を示す。

[0160] このように複数のBLEビーコン受信機でもって、通過判定エリアを規定し、個人携帯端末10とBLE通信を行い、個人携帯端末10の位置を特定する。通過判定エリアDAと通過判定エリアDA1と通過判定エリアDA2を利用することで、自動改札機に侵入した個人携帯端末10の位置特定が実現される。また自動改札機内を進んだ個人携帯端末10の位置特定には、通過判定エリアDBと通過判定エリアDB1と通過判定エリアDB2を利用する

(通過判定エリアDA、DB)

[0161] 通過判定エリアDA、DBは、BLEビーコン受信機2111～2114の平均と、BLEビーコン受信機2115～2118の平均との差と、予め設定された閾値との大小を比較する条件式を算出して、個人携帯端末10の位置を特定する。例えば、BLEビーコン受信機2111、2112の組とBLEビーコン受信機2115、2116の組との距離が2000mmで、BLEビーコン受信機2111、2112の組とBLEビーコン受信機2113、2114の組との距離が600mmのとき、通過判定エリアDAでは、BLEビーコン受信機2111～2114の平均が、BLEビーコン受信機2115～2118の平均よりも10dB大きい。逆に通過判定エリアDBでは、BLEビーコン受信機2111～2114の平均が、BLEビーコン受信機2115～2118の平均よりも10dB小さい。

(通過判定エリアDA1、DA2、DB1、DB2)

[0162] また通過判定エリアDA1は、BLEビーコン受信機2111、2112の組と、BLEビーコン受信機2115～2118の平均との差と、予め設

定された閾値との大小を比較する条件式を算出して、個人携帯端末10の位置を特定する。例えば通過判定エリアDA1では、BLEビーコン受信機2111～2112の平均が、BLEビーコン受信機2115～2118の平均よりも10dB大きい。また通過判定エリアDA2では、BLEビーコン受信機2113～2114の平均が、BLEビーコン受信機2115～2118の平均よりも10dB大きい。同様に通過判定エリアDB1は、BLEビーコン受信機2115、2116の組と、BLEビーコン受信機2111～2114の平均との差と、予め設定された閾値との大小を比較する条件式を算出して、個人携帯端末10の位置を特定する。例えば通過判定エリアDB1では、BLEビーコン受信機2115～2116の平均が、BLEビーコン受信機2111～2114の平均よりも10dB大きい。また通過判定エリアDB2では、BLEビーコン受信機2117～2118の平均が、BLEビーコン受信機2111～2114の平均よりも10dB大きい。

[0163] このように、通過判定エリアDAに加えて、さらに図36Aの平面図及び図36Bの垂直断面図に示すように、通過判定エリアDA1、DA2を設定して、個人携帯端末10の位置を検出する。また通過判定エリアDBに対しても、同様に通過判定エリアDB1、DB2を設定する。通過判定エリアの大きさや位置をどのように設定するかは、BLEビーコン受信機の位置や、各BLEビーコン受信機で検出される電波強度の平均差による。対象の通過判定エリアにおいて、これらの設定された電波強度平均差より得られる電波強度差が大きいかどうかに基づいて、通過判定エリア内に個人携帯端末10が位置しているか否かを判定する。

[0164] なお、例えば通過判定エリアDAを基準とし、BLEビーコン受信機2111～2114の強度に大きな偏りがあった場合、例えばBLEビーコン受信機2111、2112で検出された電波強度の平均が、BLEビーコン受信機2113、2114の平均より一定以上の差があった場合は、偏りがあると判定し、この場合はBLE発信機があるであろう電波が強い方を利用する。例えば、BLEビーコン受信機2111、2112の電波強度平均と、

BLEビーコン受信機2115～2118の電波強度平均とが一定以上の電波強度平均差か否かに基づいて、通過判定エリアDA1に個人携帯端末10が位置するか否かを判定する。

[0165] また通過判定エリアDAについては、図36Bの垂直断面図に示すように、その形状が球状のため、ゲートの中央付近では高さDHが最大となり、広い通過判定エリアDAを確保できる一方で、区画板24A、24Bに近づくにつれ、高さ方向の幅が狭くなり、区画板24A、24Bの付近では通過判定エリアDAの外縁が点状となって、高さ方向の領域が狭くなる結果、この領域での位置検出の精度が低下する。このため、自動改札機のゲート間の中央でなく壁面すなわち区画板24A、24Bに沿って進む利用者や、個人携帯端末10を手を持つなどしてゲートの壁面側に位置させている利用者の位置検出に際しては、通過判定エリアDAよりも通過判定エリアDA1やDA2を利用することが好ましい。例えば通過判定エリアDA1の高さDH1は、通過判定エリアDAとは逆に区画板24A、24Bに近づくほど大きくなり、区画板24A、24Bの位置で最大となるため、区画板24A、24Bの近傍領域における位置検出には好適である。この場合において、例えば通過判定エリアDA1について、BLEビーコン受信機2111と2112の平均が、BLEビーコン受信機2113と2114の平均より10dB以上大きければ、BLEビーコン受信機2111～2114をBLEビーコン受信機2111～2112に変更して位置検出を行う。なお、BLEビーコン受信機2111とBLEビーコン受信機2115との間の距離が十分大きければ、BLEビーコン受信機2111とBLEビーコン受信機2115との距離、BLEビーコン受信機2111とBLEビーコン受信機2117との距離は、強度で見た場合にあまり変わらないので、差の対象としてはBLEビーコン受信機2115～2118のままでよい。以上は通過判定エリアDA1の例であるが、通過判定エリアDA2、DB1、DB2なども同様である。

[0166] なお、改札機の外側エリアを金属で覆うと、電波は一般的に金属を超えて

伝搬することができないため、通過判定エリアD A 1の外側にはみ出たエリアからの電波を検出することはできなくなる。これを利用すれば、通過判定エリアの外縁を規制することができる。例えば、多数の改札機を横並びに設置している場合、隣接する改札機を利用する利用者の個人携帯端末の位置を誤って測定してしまうことがないように、遮断することが可能となる。

[0167] このようにして、二枚の一对の区画板24 A、24 Bの間に、通過判定エリアD Aと通過判定エリアD Bという異なる検出領域を設定して、個人携帯端末10がどの位置にあるかをリアルタイムに検出できる。特に通過判定エリアD Aと通過判定エリアD Bを、自動改札機（ゲート）の入口側と出口側にそれぞれ離間して設けることで、個人携帯端末10を持つ利用者がゲートに入ったこと、ゲートから出ようとするのを、それぞれ検出できるようになり、ゲートの通過の有無を判別できるようになる。なお、ゲートが入口側と出口側を特定しない双方向への移動を許容する場合も、同様である。また、ゲートの左右を確定する区画板24にそれぞれ位置検出側受信部21を設置し、この間に検出領域を画定することにより、区画板24の間を通過したか否かを確実に検出できるようになる。特に自動改札機などでは、一般に多数のゲートが横並びに配置されているため、検出する位置が図36 Aにおいて上下方向にずれて、隣接する別のゲートを通過したと誤認識されてしまうと、正しい管理ができなくなる。このため、第一位置特定側受信部22と第二位置特定側受信部23との間に検出領域を設定して、この間に設定した検出領域の通過を検出するようにして、このような隣接するゲート間の誤認識のおそれを低減している。

[0168] さらに、自動改札機には多数の利用者が次々と通過するため、動線方向に並んだ個人携帯端末10をそれぞれ正確に識別する必要がある。このため、自動改札機の一箇所に検出領域を設定するのではなく、入口側と出口側にそれぞれ異なる検出領域を設定して、特定の利用者が自動改札機内で移動したことを追跡するようにして、このような誤検出を抑制している。加えて、利用者の位置検出を短時間に逐次行うことでも、移動する利用者間で誤検出を抑

制できる。また図36Aの例では入口側と出口側に、それぞれ通過判定エリアDA、通過判定エリアDBを設けた例を説明しているが、自動改札機あたりに設定する通過判定エリアの数は2個に限らず、3個以上としてもよい。例えば通過判定エリアDAと通過判定エリアDBの間に、中間通過判定エリアを設けてもよい。これによって、さらに利用者の検出精度を向上させることができる。

[0169] 加えて、利用者の位置検出を短時間に逐次行うことでも、移動する利用者間で誤検出を抑制できる。すなわち、個人携帯端末10を持つ利用者が連続して自動改札機に侵入する際、認証の時間間隔が長いと、別人の通過と誤認識される事態も考えられる。このため、利用者の歩行速度も考慮して認証の時間間隔を設定する。

[0170] 個人携帯端末10の認証とは別に、利用者の移動を検出するセンサを設置してもよい。例えば各区画板24は、区画板24同士の間を通過する利用者の動線に沿って、光電センサや赤外線センサを配置して、利用者の移動を監視してもよい。一般に自動改札機等の位置特定装置は、利用者の通過を監視するセンサを備えており、これを利用できる。例えばスマートフォン端末等の個人携帯端末を持たない者が、自動改札機を通過しようとした際に、これを物理的に検出して、扉部29を閉塞する等の動作を行うことができる。

[0171] なお、第一位置特定側受信部22Aと第一位置特定側受信部22Bとの距離は、第一位置特定側受信部22と第二位置特定側受信部23の距離よりも短くする。好ましくは、第一位置特定側受信部22Aと第一位置特定側受信部22Bとは、隣接させるように配置する。隣接して設置されたBLEビーコン受信機2111とBLEビーコン受信機2112との距離は、例えば5mm～50mmとする。

(位置特定側制御部28)

[0172] 位置特定装置20の位置特定側制御部28の機能を、図37のブロック図に示す。この図に示す位置特定側制御部28は、第1表示部28Aと、第2表示部28Bと、扉部29と、通過センサ部210とを備える。また位置特

定側制御部 28 は、従来型の切符や IC カードの読み取り、書き込みを行うためのリーダライタ 28 C を備えていてもよい。位置特定装置 20 は、例えば図 35 A において A 方向への利用者の通過を制御する。第 1 表示部 28 A は、既存の自動改札機等の目立つ位置に設けられている、利用者の通過やエラー、子供料金の判別等を表示させる表示灯等が該当する。また第 2 表示部 28 B は、チケットを投入したり IC カードをかざす部分に設けられた、引き落とし料金や残高などを表示させる液晶ディスプレイや有機 EL ディスプレイ等が該当する。扉部 29 は、利用者の持つ個人携帯端末 10 に対して行われた処理の結果に応じて、解放状態又は閉止状態に制御される。

[0173] また、通過センサ部 210 は、例えば位置特定装置 20 の通路側の側面に複数設けられている。例えば図 35 B に示す変形例に係る自動改札機 20 B では、通過センサ部 210 として、区画板 24 A、24 B に 5 つの通過センサ 2101 ~ 2105 を設けた例を示している。これらの通過センサ 2101 ~ 2105 は、自動改札機 20 B により形成された通路内の利用者を検出する。通過センサ 2101 ~ 2105 は、例えば赤外線センサや、光センサ、超音波センサ等で実現される。通過センサ 2101 ~ 2105 は、対向する補器に設けられた通過センサ部と連携して、通路内の利用者を検出する透過型のものであってもよいし、あるいは自身に設けられた通過センサと連携して、通路内の利用者を検出する反射型のものであってもよい。また発信する波の強度の変化を検出してもよいし、位相の変化を検出してもよい。これにより身長を測定してもよく、身長がある一定以下の利用者や荷物を通過させる機能を追加してもよい。一方で、個人携帯端末 10 を認証できなかった場合に検知された人物がいた場合に、身長等から不正利用と判断することもできる。

[0174] なお図 35 B に示す自動改札機 20 B は、例えば第 1 表示部 28 A と、第 2 表示部 28 B と、扉部 29 と、リーダライタ 28 C と、通過センサ 2101 ~ 2105 を備える。自動改札機 20 B は、図中、A 方向への利用者の通過を制御する。第 1 表示部 28 A および第 2 表示部 28 B は、各種情報を表

示する。扉部 29 は、個人携帯端末 10 に対して行われた認証処理の結果に応じて開放状態または閉止状態に制御される。

[0175] リーダライタ 28C は、既存の切符や IC カードの読み取りに対応した部材であり、例えばアンテナ 28C1 と、通信部 28C2 とを備える。通信部 28C2 は、コントローラや、変調部、復調部等を備える。コントローラは、変調部および復調部を制御する。変調部は、コマンドを所定の周波数帯を有する電波に重畳させて、その電波をアンテナ 28C1 に発信させる。また復調部は、アンテナ 28C1 を介して取得した電波に含まれる情報を復調し、復調した情報（コマンド）を制御装置に出力する。

[0176] 位置特定側演算部 25 は、BLE ビーコン受信機を用いて個人携帯端末 10 の位置を特定しつつ、位置特定側時刻部 27 と ID・暗号鍵データベースの情報に基づき、本人認証及び支払能力認証を行うことで、位置特定認証を行う。この判定結果に基づき、利用者の通過を許可、又は禁止する制御を実行する。利用者の通過を許可する制御を行う場合、位置特定側制御部 28 は、扉部 29 を解放状態にさせたり、第 1 表示部 28A に通過の許可を示す情報を表示させたりする。利用者の通過を禁止する制御をする場合、位置特定側制御部 28 は、扉部 29 を閉止状態にさせたり、第 1 表示部 28A に通過の禁止を示す情報を表示させたりする。また、位置特定側演算部 25 によりエラー処理が実行された場合、エラー処理として位置特定側制御部 28 は、扉部 29 を閉止状態にさせたり、第 1 表示部 28A にエラー処理に関する情報を表示させたりする。エラー処理に関する情報とは、例えば、位置特定が実行できなかった場合や個人認証ができない場合、支払能力を認証できない場合である。なお、入場記録が確認できない場合も含めてもよい。また位置特定装置 20 は、位置特定側演算部 25 の判定結果に応じて所定の音や音声を出力したり、音声の入力から位置特定側演算部 25 で応答して、エラー処理等を解決したりするために、音入出力部を備えてもよい。また位置特定装置 20 は、キセル対策等のために、入出記録を管理端末 50 や管理サーバシステム 30 に送信してもよい。

[0177] なお、管理端末50から利用者の位置情報を画像で追跡可能な場合は、その個人携帯端末10を認証し、画像と連携して通過させてもよいし、位置特定装置20での位置情報の認証を停止してもよい。また、第1表示部28Aや第2表示部28Bを省略することもできる。

(個人携帯端末10)

[0178] 個人携帯端末10は、位置特定や認証の対象となる利用者が携行する個人所有の通信端末である。個人携帯端末10は、図34に示すように、個人端末側通信部11Aと、個人端末側制御部12と、個人端末側時刻部14と、個人端末側記憶部13と、個人端末側入出力部15と、個人端末側演算部16とを備える。

[0179] 個人端末側時刻部14は、時刻に関する情報を生成する。ここでは個人携帯端末10側の時計が該当する。なお個人端末側時刻部14は、個人端末側演算部16等の他の部材と統合したり、個人端末側演算部16等に組み込んでもよい。

[0180] 個人端末側記憶部13は、各種の情報を保持するための記憶部材であり、不揮発性の半導体メモリやハードディスク等が利用できる。ここでは、固有の識別情報や固有の共通鍵、ワンタイムパスワードの生成に利用する関数等を保持している。

[0181] 個人端末側入出力部15は、個人携帯端末10の入出力を行う部材であり、キーボードやマウス、コンソール、マイク等の入力デバイス、ディスプレイやスピーカー等の出力デバイス、あるいは入出力を兼用したタッチパネル等のマン／マシンインターフェースが利用できる。

[0182] 個人端末側演算部16は、各種の演算や処理を行う部材であり、スマートフォン端末のSoCやパーソナルコンピュータのCPU、あるいはASIC等が利用できる。なお、個人端末側制御部12は個人端末側演算部16と統合してもよい。

[0183] この個人携帯端末10は、管理サーバシステム30に登録を行い、また管理サーバシステム30を通じて位置特定装置20を利用する事業者サービス

の提供を申請することができる。このために必要な支払いを、例えばクレジットカードやデビットカード、プリペイドカード、キャッシュカード等の情報を管理サーバシステム30に登録する。さらに、位置特定装置20を利用するにあたり必要な、個人携帯端末10の一意なIDと、そのIDとセットとなる暗号鍵を生成、発行することができる。なお、事業者からのサービス提供に応じて事業者の指定する位置特定装置20の利用場所、利用期間等を入力装置に表示することができる。なお、スマートフォン端末等でなく、個人情報等の登録及び管理サーバシステム30と設定後はBLEビーコンを発信するだけの小型の端末でもよく、位置特定装置20周辺でのみ発信してもよい。

[0184] 個人端末側通信部11Aは、外部機器と通信を行うための部材である。個人端末側通信部11Aでもって個人携帯端末10は、LTEや3G/4G/5G、CDMA、WIMAX、WiFi（いずれも商品名）等、規格化された通信規格や独自の通信規格に従って、外部機器と通信を行うことができる。また個人端末側通信部11Aは、個人端末側発信部11として機能する。個人端末側通信部11Aは、BLEビーコン発信装置を備えている。さらに、GPS装置やBLEビーコン受信装置を備えていてもよい。個人携帯端末10は、BLEビーコンを発信することで位置特定装置20を通過することができる。なお個人携帯端末10は、GPS装置やBLEビーコン受信機能を用いて管理端末50及び位置特定装置20への接近を感知した場合、BLEビーコンを発信してもよいし、離れた場合は、BLEビーコンの発信を停止してもよい。

[0185] また個人端末側通信部11Aに、無線LANや移動体通信等の無線通信機能を持たせることもできる。この無線通信機能はインターネット等のネットワークと接続できる。また、個人端末側表示部や個人端末側入力部を持たせてもよい。さらに、加速度センサ等を持たせてもよいし、地場測定装置を持たせてもよいし、画像入力装置を持ってもよい。位置特定装置20を通過した個人携帯端末10は、加速度、ジャイロ、地磁気等のセンサから移動

の方向と速度を推計するPDR、環境特有の物理情報を予めデータベース化してマッチング処理から位置特定を行う、いわゆるフィンガープリンティング法等組み合わせることで、その後の位置を特定してもよい。これにより、より精度を向上することが出来る。地図アプリや屋内地図データの提供を受けることで、屋内での地図案内を行ってもよいし、個人端末側入出力部に表示してもよい。また、本実施例のような改札機に利用する場合には、乗換案内アプリと連動させて、乗車位置や時間、駅構内の案内、利用料金の確認等に利用してもよい。また、それらの移動経路情報を管理サーバシステム30に送信して利用情報に登録してもよい。

(金融機関60)

- [0186] 金融機関60は、クレジットカード会社や銀行等、与信審査機能、クレジットカード番号発行機能、支払い機能等をもつ。金融機関60は、管理サーバシステム30に登録されたユーザの支払い登録の与信審査を行う。これらの情報を管理サーバシステム30と連携することで、管理サーバシステム30は、ユーザの登録やID・暗号鍵データベースの更新、ユーザからの支払いや事業者への支払いを行う。

(事業者用管理端末50を用いた事後支払いシステムへの登録処理)

- [0187] 本実施例における、事業者用管理端末50を用いた事後支払いシステムへの登録処理の流れを示すフロー図を、図38に示す。このフロー図は、事業者用管理端末50が事業者側入出力部43とインターネット接続が可能な事業者側通信部41がある場合等で、かつ必要な場合を示している。なお、不必要、もしくは不可能な場合は、事業者用管理端末50と接続可能な別途同等機能を持つ別の端末を利用して事前に設定するものとして、本フローを適応するものとする。事業者用管理端末50は、インターネット等を利用することで、本システムへの登録処理アプリをインストールすることができる。もしくは、インターネット上で登録処理を行うことができるものとする。もしくは、登録処理アプリがインストールされている専用端末として用いてもよい。事業者用管理端末50は、常時、管理サーバシステム30の認証局の

電子証明書を確認し、安全性を確認して接続することが望ましい。事業者用管理端末50は、例えば、銀行口座等の支払い情報を管理サーバシステム30に登録する。また、事業者用管理端末50は、事業者が提供するサービスに基づいて利用者から利用料を徴収するためのサービス利用料表を管理サーバシステム30に送付する。なお、このサービス利用料表は、利用者が判るIDと利用料が判る形で、事後に送付してもよい。管理サーバシステム30は事業者用管理システム40に一意的な事業者IDを発行し、事業者用管理システム40に付与する。事業者用管理システム40は、IDとセットとなるような暗号鍵を発行し、安全な形で管理サーバシステム30に送付する。管理サーバシステム30と事業者用管理システム40は、それぞれを記憶装置に保存する。先に管理端末50及び位置特定装置20を設置していてもよいし、後に設置していてもよいし、同時並行で設置していてもよい。管理端末50及び位置特定装置20と接続が終わった管理サーバシステム30は設置場所を登録する。また、この設置場所の情報を事業者用管理システム40に通知する。管理サーバシステム30は、これらの情報を記憶装置に保存する。

なお、管理サーバシステム30の認証を得ながら他の事業者用管理システム40へとアカウントを移動できるようにしてもよい。

[0188] 図39は、本実施例に係る事後支払いシステムにおける、個人携帯端末10を用いた本システムへの登録処理の流れを示すフロー図である。このフロー図は、個人携帯端末10がスマートフォン端末等の入出力装置とインターネット接続が可能な通信装置がある場合等で、かつ必要な場合を示している。なお、不必要、もしくは不可能な場合は、個人携帯端末10と接続可能な別途同等機能を持つ別の端末を利用して事前に設定するものとして、本フローを適応するものとする。個人携帯端末10は、インターネット等を利用することで、本システムへの登録処理アプリをインストールすることができる。もしくは、インターネット上で登録処理を行うことができるものとする。もしくは、登録処理アプリがインストールされている専用端末として用いて

もよい。個人携帯端末１０は、随時、管理サーバシステム３０の認証局の電子証明書を確認し、安全性を確認して接続することが望ましい。個人携帯端末１０は、例えば、クレジットカード等の支払い情報を管理サーバシステム３０に登録する。この際、クレジットカードの与信審査に必要となる、名前や住所等の情報も登録する。この登録情報は、管理サーバシステム３０の個人情報データベースに安全な形で保存する。この情報をもとに与信審査を行う。この与信審査の結果の通知を受け、その与信審査の結果を個人情報データベースに保存する。与信審査を通過した場合、管理サーバシステム３０は個人携帯端末１０に一意的なＩＤを発行、個人携帯端末１０に付与する。個人携帯端末１０は、ＩＤとセットとなるような暗号鍵を発行し、安全な形で管理サーバシステム３０に送付する。個人携帯端末１０は、このＩＤ・暗号鍵を記憶装置に保存する。管理サーバシステム３０は、これらの情報を個人情報データベース及びＩＤ・暗号鍵データベースに保存する。なお、例えば、利用者がクレジットカード等を紛失した場合等にも一時的に利用者の情報を無効にできる。

[0189] なお、与信審査を通過できなかった場合は、登録ができず、別のクレジットカード等で申請をすることができる。なお、管理サーバシステム３０の認証を得ながら他の個人携帯端末１０へとアカウントを移動できるようにしてもよい。

[0190] 本実施例に係る事後支払いシステムによる個人携帯端末１０から事業者サービスを申請する処理の流れを示すフロー図を、図４０に示す。個人携帯端末１０は、利用したい事業者のサービスを登録することができる。例えば、一部の事業者とは契約を結んでもよいし、一部の事業者とは事前の契約を結ぶことで自動的もしくは任意に利用できるようにしてもよいし、申請を省略できるようにしてもよい。個人携帯端末１０は、管理サーバシステム３０に申請をすることで、必要な事業者サービスを申請する。管理サーバシステム３０は、その情報を事業者用管理システム４０に通知・申請をし、事業者に可否を尋ねる。事業者が拒否をした場合は、管理サーバシステム３０に通知

する。管理サーバシステム 30 は、個人携帯端末 10 に申し込みが拒否された旨を伝え、個人携帯端末 10 は以降のステップに進めない。なお、事業者用管理システム 40 で自動的に可否を決定することができるようにしていてもよい。

[0191] 事業者が申し込みを許可した場合、事業者用管理システム 40 は、事業者 ID、位置特定装置 20 が認可してよい認可期間、及び、通過を許可する設置場所等を管理サーバシステム 30 に通知する。ただし、基本的には、事業者用管理システム 40 は、自身が管理する位置特定装置 20 に関する設置場所とその認可期間を指定することができる。管理サーバシステム 30 は、個人携帯端末 10 に申し込みが許可されたことを通知してもよい。管理サーバシステム 30 は、事業者用管理システム 40 に通知を許可された設置場所に存在する、位置特定装置 20 に申請した利用者の ID・暗号鍵、及び、認可期間を設定する。これは、管理端末 50 を通して設定されてもよい。設定が完了すると、位置特定装置 20、及び、もしくは、管理端末 50 から設定完了通知を管理サーバシステム 30 に通知する。設定完了通知を受け取った管理サーバシステム 30 は、個人携帯端末 10 及び事業者用管理システム 40 に、設定完了を通知してもよい。

[0192] 本実施例に係る事後支払いシステムによる管理サーバシステム 30 で、与信状況の変化を監視維持のための処理の流れを示すフロー図を、図 41 に示す。管理サーバシステム 30 は、与信状況の変化を監視するために、与信情報に変化がない限り、金融機関 60 に与信審査の状況を定期的に確認する。金融機関 60 から与信審査結果を受け、管理サーバシステム 30 は、ID・暗号鍵データベースを更新する。変化があった場合、必要に応じて事業者用管理システム 40 と、管理端末 50 と、位置特定装置 20 とに通知する。この場合、ID・暗号鍵データベースの差分を送付してもよいし、全データを送付してもよい。これによりクレジットカード等の与信 NG を受けた ID は事後支払いを必要とする位置認証装置を通過できなくなる。また、管理サーバシステム 30 は、個人携帯端末 10 にクレジットカード等の否認を通知し

てもよい。なお、新たなクレジットカード等の登録を促してもよい。

[0193] 本実施例に係る事後支払いシステムによる、利用者による位置特定装置 20 利用時の処理の流れを示すフロー図を図 42 に示す。個人携帯端末 10 は、位置特定装置 20 の近くにある管理端末 50 や位置特定装置 20 の通信装置として設置されている BLE 発信機の信号を受信することにより、もしくは GPS により事前に設定されている位置特定装置 20 の設置位置付近に接近することで BLE ビーコン信号を発信する。もしくは、常に発信をしてもよいし、接近によってその発信頻度を上げることで低消費電力を維持してもよい。発信する BLE ビーコン信号には少なくとも ID を付与する。位置特定装置 20 は、その ID を付与された BLE ビーコン信号の発信源の位置特定及び認証を行う。なお、BLE ビーコン信号は暗号化されていてもよいし、管理端末 50 及び位置特定装置 20 が復号してもよい。位置特定の結果、通過させた場合、通過認証を個人携帯端末 10 に通知してもよい。また、事業者用管理システム 40 に通知してもよい。また、その利用履歴を管理端末 50 に通知してもよい。なお、位置特定及び暗号化・復号のフローについては、後で説明する。

[0194] 位置特定装置 20 は、利用履歴を定期的に管理サーバシステム 30 に通知する。なお、管理端末 50 を介してもよいし、管理端末 50 が位置特定装置 20 の代わりに実行してもよい。精算時まで決められた機関の利用履歴を事業者用管理システム 40 と、個人携帯端末 10 とに通知する。事後支払いがある場合、金額清算を行う。精算時に、管理サーバシステム 30 は、請求費用を算出し、請求費用を金融機関 60 に請求し、金融機関 60 から支払われる支払いのうち、例えば、手数料等を除いた部分を事業者に支払い、その利用情報や支払い結果を、事業者用管理システム 40 を通じて通知する。なお、事業者用管理システム 40 を通じて通知しなくてもよい。また、利用者には、個人携帯端末 10 を通じて利用支払情報を通知する。もしくは、Web サイトや SNS を通じて通知してもよいし、他のインターネット媒体や紙媒体を通じて通知してもよいし、クレジットカード等の会社を通じて通知す

ることで、直接管理サーバシステム30から通知しなくてもよい。

(位置特定の手順)

[0195] 次に、位置特定の手順について、図43のフローチャートに基づいて説明する。図43は、位置特定装置20による個人携帯端末10の位置特定における個人携帯端末10の処理の流れを示している。個人携帯端末10は、位置特定装置20の近くにある管理端末50や位置特定装置20の通信装置として設置されているBLE発信機の信号を受信することにより、もしくはGPS電波を受信することにより位置を求め、位置特定装置20が存在するエリアに接近することを検知し、BLEビーコンを発信する。もしくは、常に発信をしてもよいし、接近によってその発信頻度を上げることで低消費電力を維持してもよい。このエリアは、例えば、半径10mでもよいし、半径100mでもよい。そして、このエリアの離脱を検知し、BLEビーコンの発信を停止してもよい。

[0196] 位置特定装置20による個人携帯端末10の位置特定における位置特定装置20の処理の流れを図44のフローチャートに示す。位置特定装置20は、位置特定側受信部21にある、例えば図35Aに示した8つの各BLEビーコン受信機等で、BLEビーコン電波を受信する。各BLEビーコン受信機では、BLEビーコン電波にあるID等と、その電波強度を測定する。同一IDの電波強度について、後述する基準値を算出し、その差が閾値以上か否かを求める。その差が閾値以上であれば、その基準値が大きいエリアに当該IDを持つ個人携帯端末10が存在すると判定される。また、その差が閾値以上でなければ、当該IDを持つ個人携帯端末10がどのエリアにも存在しないと判定される。なお、電波強度の算出方法については後述する。

[0197] 図45は、位置特定装置20による個人携帯端末10の位置特定時における電波強度算出の処理の流れを示すフローチャートである。本実施例のBLEビーコン信号の電波強度は、BLEビーコン信号の受信強度の履歴情報に基づいて電波強度を算出してもよい。例えば、図の上段に示したBLEビーコン受信機の装置Aと装置Bは、p秒毎に得られた電波強度を取り扱う際に

、各受信タイミングでの値のみを用いるのではなく、一定時間毎（図45の例では q 秒毎）に、単数もしくは複数のタイミングでの電波強度の情報が含まれる所定の期間（図45の例では r 秒間。 $p \leq q \leq r$ ）のデータに基づいて平均値を求め、BLEビーコン受信機毎の電波強度とする。

[0198] 図46は、位置特定装置20による個人携帯端末10の位置特定時における電波強度算出の処理の流れを示すフローチャートである。なお、BLEビーコン信号の電波強度は、BLEビーコン信号の受信強度の履歴情報に基づいて電波強度を算出してもよい。例えば、図の上段に示したBLEビーコン受信機の装置Aと装置Bは、 p 秒毎に得られた電波強度を取り扱うが、データが追加されるタイミングに各装置が同時に更新されとは限らない。このため、それぞれの装置毎に同様の処理を行う。つまり、一定時間毎（図46の例では q 回更新毎）に、単数もしくは複数のデータ更新毎での電波強度の情報が含まれる所定の期間（図46の例では r 回更新毎。 $p \leq q \leq r$ ）のデータに基づいて平均値を求め、BLEビーコン受信機毎の電波強度とする。なお、あるIDについて、任意の一定時間後までに通信がなかった場合、溜まっている過去のデータを削除してもよい。

（BLE受信機の電波強度から基準値を求める手順）

[0199] 次に、BLE受信機の電波強度から基準値を求める手順を、図47を参照しながら説明する。図47は、BLE受信機の電波強度から基準値を求める処理の流れを示すフローチャートである。先ほどまで説明された電波強度の測定方法を用いて、各BLE受信機で測定された電波強度とし、以下、同一IDにおいて説明する。なお、本実施例では複数条件を組み合わせた判定方法が説明されているが、これらの条件を任意の組み合わせで判定してもよい。また位置特定は、本実施例の基礎となる知見で説明されるような様々な配置があり、本実施例は一例として説明している。ここでは、図36A、図36Bで示した位置特定装置20における、通過判定エリアDA、DA1、DA2、DB、DB1、DB2を用いて説明を行う。

[0200] ここでは、個人携帯端末10をBLE発信機として、位置特定装置20を

BLE受信機として、BLE通信を行い、個人携帯端末10がどの位置にあるのかを、予め設定された複数の通過判定エリア内にあるか否かを順次判定することにより、決定する。複数の通過判定エリアとは、例えば図36Aに示す通過判定エリアDA、DA1、DA2、DB、DB1、DB2等である。これら複数の通過判定エリアに対して、どのような順序で判定を行うかについては、処理速度や精度に応じて適宜設定可能である。例えば最初に通過判定エリアDA内にあるか否かを判定し、通過判定エリアDA内と判定した場合には処理を終了する。一方通過判定エリアDA外と判定した場合は、通過判定エリアDB内か否かを判定する。あるいは、通過判定エリアDA内外の判定において誤差が大きい場合は、通過判定エリアDA1内か否か、あるいは通過判定エリアDA2内か否かの判定に進めてもよい。

[0201] 以下、特定の通過判定エリアの内外を判定する一手順として、通過判定エリアDA内に個人携帯端末10が位置しているか否かを判定する手順を、図47のフローチャートに基づいて説明する。まずステップS4701において、個人携帯端末10が、BLE受信機であるBLEビーコン受信機2111～2118とそれぞれBLE通信を行い、各BLE受信機でIDと電波強度を検知する。

[0202] 次にステップS4702で、検知された電波強度に対し、検査エリアAに相当するBLEビーコン受信機2111～2114の平均と、検査エリアBに相当するBLEビーコン受信機2115～2118の平均を算出し、その差が所定の閾値以上か否かを判定する。所定の閾値は、ノイズの多さなどの使用環境や用いる電波の強度等に応じて適宜設定される。ここでは、閾値を10dBとしている。そして平均値の差が閾値以上の場合は、ステップS4708に進んで、当該IDに相当する個人携帯端末10は、平均値が大きい検査エリアA、すなわち通過判定エリアDA内に存在すると判定して処理を終了する。

[0203] 一方ステップS4702で、平均値の差が閾値以上でない場合は、ステップS4703に進み、検査エリアA（ここではBLEビーコン受信機2111

1～2114)内で、電波強度の最大値と最小値が所定の閾値以上(例えば10dB以上)であれば、平均値の演算対象から最小値を除く処理を行う。これにより、BLEビーコン受信機間で電波強度のばらつきが大きすぎる場合に、特に、BLEビーコンは本来より-30dBmなど非常に低い電波強度を時たま出力することがあるため、異常値を除去できる利点を得られる。

[0204] その上でステップS4704に進み、再度ステップS4702と同様に、BLEビーコン受信機2111～2114の平均と、BLEビーコン受信機2115～2118の平均を算出し、その差が所定の閾値以上か否かを判定する。そして平均値の差が閾値以上の場合は、ステップS4708に進んで、当該IDに相当する個人携帯端末10が通過判定エリアDA内に存在すると判定して処理を終了する。

[0205] 一方ステップS4704でも、平均値の差が閾値以上でない場合は、ステップS4705に進み、検査エリアA1(通過判定エリアDA1に相当するBLEビーコン受信機2111～2112)と検査エリアA2(通過判定エリアDA2に相当するBLEビーコン受信機2113～2114)で、電波強度の平均値の差が所定の閾値(例えば10dB)以上であれば、平均値が大きい方(BLEビーコン受信機2111～2112、又はBLEビーコン受信機2113～2114のいずれか)を選択する。これは、個人携帯端末10が近い方が電波強度の平均値が大きいため、その値を基に判定することを意味する。

[0206] その上でステップS4706に進み、選択されたBLEビーコン受信機2111～2112又はBLEビーコン受信機2113～2114の平均と、BLEビーコン受信機2115～2118の平均を算出し、その差が所定の閾値(例えば10dB)以上か否かを判定する。そして平均値の差が閾値以上の場合は、同じくステップS4708に進んで、当該IDに相当する個人携帯端末10は、通過判定エリアDA1又はDA2内に存在すると判定して処理を終了する。これにより、個人携帯端末10がゲートの中央でなく区画板24A、24Bのいずれかに接近している場合でも、検出が可能となる。

- [0207] 一方で、ステップS 4 7 0 6でも平均値の差が閾値以上でない場合は、ステップS 4 7 0 7に進み、当該IDの個人携帯端末10は通過判定エリアDA（及びDA1、DA2のいずれにも）に存在しないと判定する。
- [0208] 同様の手順で、通過判定エリアDB（あるいはDB1、DB2）についても判定を行う。さらに、この判定をより高精度に行うフローについて説明する。
- [0209] 位置特定装置20による個人携帯端末10の位置特定を行う処理の流れを図48のフロー図に示す。先ほど得られたエリアに存在するかどうかの判定結果を、ここでは、エリア判定と称する。図48に示す通り、データ処理更新毎にデータが追加されるが、一定時間毎（図48の例ではq回更新毎）に、単数もしくは複数のデータ更新毎での電波強度の情報が含まれる所定の期間（図48の例ではr回更新毎。 $p \leq q \leq r$ ）のデータに基づいて、r個中にp個以上で○と判定されれば更新後も○と判定できる。これは、本システムにおいて、誤判定が非常に低い場合に利用できるが、本発明は誤判定が0.0%とできることから、十分信頼性をもって判断することができることに起因している。なお、あるIDについて、任意の一定時間後までに通信がなかった場合、溜まっている過去のデータを削除してもよい。
- [0210] これらを設定することにより、図36Aのようなエリアを検知することができる。例えば、直径40cm～60cm程度の球に近似したエリアを認識することができる。これにより、個人携帯端末10を保持する高さとして、一般成人のポケットや手提げカバンからながらスマホ（非推奨）の高さとなるような高さをおおよそカバーすることができる。なお、子供等を対象にするためにも、BLE受信機を同一高さに8つつける以外に、異なる高さにも8つ同様につけて位置特定をしてもよい。

（暗号化・復号の手順）

- [0211] 次に、暗号化・復号のフローについて、図49を参照しながら説明する。図49は、暗号化・復号における個人携帯端末10の処理の流れを示すフローチャートである。個人携帯端末10は、事前に、例えば、個人情報やクレ

ジットカード等の、本人認証及びその個人携帯端末10の装置認証を行う。この装置認証には、例えばソフトウェアでのライセンス設定による一台限りとしてもよいし、起動を制限してもよい。これにより個人携帯端末10に一意的なIDが付与される。個人携帯端末10及びその設定端末は、一意なIDとセットとなる暗号鍵を設定することができる。この暗号鍵は、3DESやAES等の共通鍵暗号を利用してよいし、楕円暗号等の公開鍵暗号を利用してよい。この暗号鍵は、安全な方法で管理サーバシステム30のID・暗号鍵データベースにIDとセットで保存される。

[0212] 図50は、暗号化・復号における個人携帯端末10の処理の流れの一例を示すフローチャートである。まずステップS5001において、個人携帯端末10は、稼働時、個人携帯端末10の時間を、例えば、ms単位等の48ビットで、取得し、パディング処理をする。このパディング処理は、いわゆる銀行送金等で利用されるワンタイムパスワードでも利用されるような、時刻から求められる方程式を用いるもの等である。このため、時刻とこのデータからパディング処理内容を攻撃者が推測できるものではない。

[0213] 次にステップS5002において、事前に用意した当該IDとセットとなる暗号鍵で、このパディング処理された時間を暗号化する。そしてステップS5003において、IDと暗号化された時間を送付する。このようにして、認証を受ける被認証機器である個人携帯端末は、送信時の時刻を暗号化して、IDと共に、認証を行う認証装置側に送信する。

(送受信の時間差の一致)

[0214] 図51は、暗号化・復号における位置特定装置20の認証処理の流れの一例を示すフローチャートである。位置特定装置20が認証を行うため、まずステップS5101において、個人携帯端末等の認証を受けようとする装置から送られてくるID（識別情報）と、暗号化された時刻を、位置特定装置20で受信する。次にステップS5102において、認証を行う位置特定装置20は、認証対象の装置のIDから暗号鍵を検索して、当該IDと共に送られた暗号化された時刻を復号化する。そしてステップS5103において

、ID毎に設定されている、時間情報 i (ID) が定義済みか否かを判定する。ここで未だ定義されていない場合は、ステップS5104に進み、 i (ID) を定義する。 i (ID) の定義方法は複数あるが、例えば受信した時刻と復号化した時刻（すなわち被認証機器側の送信時刻）との時間差を求める。 i (ID) が定義されると、ステップS5101に戻って処理を繰り返す。すなわち、新たにIDや暗号化された時刻の受信を行う。一方、 i (ID) が定義済みの場合は、ステップS5105に進み、受信した時刻と復号化した時刻との時間差が i (ID) と一致するかどうかを判定し、一致する場合はステップS5106において認証を行う。一致しない場合は、認証を行わず、ステップS5101に戻って処理をくり繰す。この操作を繰り返すことで、繰り返し認証を行うことができる。なお、必要回数で止める処理でもよいし、リアルタイムな位置特定等で連続的な認証が不可欠な場合は、繰り返してもよい。

（送受信の時間差が所定範囲内）

[0215] 上述した方法では、送信時刻と受信時刻の時間差が一致する場合に認証を行う手順を説明した。ただ、時間差 i (ID) はms単位の精度で一致しない場合がある。例えば送信時刻を規定する被認証機器側と、受信時刻を規定する認証装置側とで、時間がずれていることもある。このため、このような多少の時間の誤差を許容できる認証方法を、以下図52のフローチャートに基づいて説明する。

[0216] 図52は、暗号化・復号における位置特定装置20の認証処理の流れの他の例を示すフローチャートである。まずステップS5201において、認証を行う位置特定装置20で、認証されようとする装置から送られてくるIDと暗号化された時刻を受信する。次にステップS5202において、位置特定装置20は、受信したIDから暗号鍵を検索し、当該IDと共に送られてくる暗号化された時間を復号化する。そしてステップS5203において、ID毎に設定されている時間情報 i (ID) が定義されているか否かを判定する。ここで未だ未定義の場合はステップS5204に進み、時間情報 i (

ID)を定義する。定義方法は複数考えられるが、例えば受信した時刻と復号化した時刻との時間差を求める。このようにして時間情報 i (ID) が定義されると、ステップ S 5 2 0 1 に戻って処理を繰り返す。すなわち、新たに ID や暗号化された時刻を受信する。

- [0217] 一方、ステップ S 5 2 0 3 において i (ID) が定義済みの場合は、ステップ S 5 2 0 5 に進み、新たに受信した時刻と復号化した時刻との時間差が i (ID) との差が任意の設定値、例えば T 秒以下か否かを判定する。そして一致する場合は、ステップ S 5 2 0 6 において認証を行う。この操作を繰り返すことで、繰り返し認証を行うことができる。なお、必要回数で止める処理でもよいし、リアルタイムな位置特定等で連続的な認証が不可欠な場合は、繰り返してもよい。

(送信時刻と受信時刻)

- [0218] 以上は、時間情報 i (ID) に基づいて認証を行う手順について説明したが、認証の基準となる情報は複数用いてもよい。例えば受信した時刻を示す時間情報 i (ID) と、復号化された時刻、すなわち送信時刻を示す時間情報 j (ID) を用いて認証してもよい。このような認証方法を変形例として、図 5 3 に基づいて説明する。

- [0219] 図 5 3 は、暗号化・復号における位置特定装置 2 0 の認証処理の流れを示すフローチャートである。まずステップ S 5 3 0 1 において、位置特定装置 2 0 が認証を行うため、認証されようとする装置から送られてくる ID と暗号化された時刻を受信する。次にステップ S 5 3 0 2 において、位置特定装置 2 0 が受信した ID から暗号鍵を検索し、当該 ID と共に送られる暗号化された時刻を復号化する。そしてステップ S 5 3 0 3 において、ID 毎に設定されている時間情報 i (ID)、 j (ID) が定義されているか否かを判定し、未だ定義されていない場合はステップ S 5 3 0 4 において、これら時間情報 i (ID)、 j (ID) を定義する。例えば、受信した時刻を i (ID)、復号化した時間を j (ID) として定義し、ステップ S 5 3 0 1 に戻って処理を繰り返す。すなわち、新たな ID と暗号化された時刻を受信する

。

[0220] 一方、ステップS5303において $i(ID)$ 、 $j(ID)$ が定義済みの場合は、ステップS5305に進み、受信した時刻と $i(ID)$ 、復号化した時刻と $j(ID)$ との差をそれぞれ取得し、これらの差が一致するかどうかを判定する。一致する場合は、ステップS5305において認証を行う。一方、位置しない場合は認証せず、ステップS5301に戻って処理を繰り返す。このような手順を繰り返すことで、繰り返し認証を行うことができる。なお、必要回数で止める処理でもよいし、リアルタイムな位置特定等で連続的な認証が不可欠な場合は、繰り返してもよい。

[0221] 以上の方法では、 $i(ID)$ と $j(ID)$ との差が一致する場合に認証を行っているが、上述の通り、完全一致を求める必要はなく、ある程度の誤差を許容して、同程度の値が得られている場合は認証を行うように構成してもよい。このような例を変形例として、図54のフローチャートに基づいて説明する。

[0222] 図54は、変形例に係る暗号化・復号における位置特定装置20の認証処理の流れを示すフローチャートである。この例では、受信した時刻の時間差と、復号化した時刻の時間差を用いて認証を行っている。すなわち、あるIDについて受信した時刻を $i(ID)$ 、復号化した時間を $j(ID)$ として求める。そして $i(ID)$ 、 $j(ID)$ が定義されている場合に、受信した時刻と $i(ID)$ 、復号化した時間と $j(ID)$ とのそれぞれの差がms単位の精度で一致しない場合を検出することで、認証の判定を行う。具体的に、位置特定装置20が認証を行う手順を、図54に基づいて説明する。

[0223] まずステップS5401において、位置特定装置20が個人携帯端末等の認証対象の装置から、IDと、暗号化された時間を受信する。次にステップS5402において、位置特定装置20が、送られてくるIDから暗号鍵を検索し、当該IDと共に送られてくる暗号化された時間を復号化する。次にステップS5403において、 $i(ID)$ 、 $j(ID)$ が定義済みか否かを判定する。ここで、未だ $i(ID)$ 、 $j(ID)$ が定義されていない場合は

、ステップS 5 4 0 4において、受信した時刻を i (I D)、復号化した時間を j (I D) として定義した後、ステップS 5 4 0 1に戻って処理を繰り返す。すなわち、新たに I D や時刻を受信する。

- [0224] 一方、ステップS 5 4 0 3において、 i (I D)、 j (I D) が定義済みである場合は、ステップS 5 4 0 5に進み、受信した時刻と i (I D)、復号化した時間と j (I D) とのそれぞれが任意の設定値 T 秒以下で一致する可否を判定する。一致する場合は、ステップS 5 4 0 6に進んで認証を行う。一方、一致しない場合は認証を行わないで、待機状態となる。すなわち、ステップS 5 4 0 1に戻って処理を繰り返す。これによって、認証を行うことができる。なお、繰り返す回数を必要回数に限定して処理を止める処理としてもよい。あるいは、リアルタイムな位置特定等で連続的な認証が不可欠な場合は、処理を無限に繰り返してもよい。さらに上述の通り、 i (I D)、 j (I D) を所定時間経過後に初期化することもできる。これによって、認証の基準となる i (I D)、 j (I D) を一定時間毎に更新することによって、一度なりすましに成功したとしても、永続的になりすましを継続することはできなくなるので、更にセキュリティを向上できる。

(なりすましの検知方法)

- [0225] 次に、なりすましの検知方法を説明する。基本的には、信号をコピーしても、受信してから送信するまでに数 $m s$ 以上かかると、上記までの認証方法で認証されないため、問題にはならないが、数 $m s$ 以上かからない場合があるため、その対策を説明する。

- [0226] 図 5 5 は、暗号化・復号における位置特定装置 2 0 の認証なりすまし否認の処理の流れを示すフローチャートである。図 5 3、及び図 5 4 で説明したような方法を用いて認証する場合、復号化した時間が j (I D) より新しい場合は今までと同様の手順を踏むことができる。図 5 5 では、図 5 3 に対応した説明をしているが、図 5 4 に対応した方法でもよい。ただし、復号化した時間が j (I D) より新しくない場合、つまり何らかの信号をコピーした信号であった場合、 j (I D) より新しい信号は作成できないため、 I D の

なりすましがあるため、IDを一時停止することでなりすましを回避できる。

[0227] 図56及び図57は、改札機に見立てて実験を行った場合の様子を示している。左に示す画像が実験中の画像であり、右上に示す図はその認証の様子を示している。図56では、左に示す画像の画面奥にユーザがおり、右上に示す図では画面奥に数msごとに「○」が表示されており位置特定認証ができていたことが確認できる。この表示の確率は一回あたり95%以上であり、上記説明した処理を行うことで10cm程度移動する間に認証できる確率は $1 - 10^{-17}$ 程度とすることができている。同時に、一回あたり誤認識する確率は0.0%である。同様に図57では、画面手前を認証できていることが判る。なお、逆方向の利用者の通過については位置が逆となる操作を行うことで制御できる。

[0228] 本実施例における改札機に、既存の切符やICカードを読み取りや処理するための装置があってもよいし、そのためのネットワーク接続があってもよいし、本実施例のシステムと連携して利用してもよいし、独立な支払方法として扱ってもよい。

[0229] なお、本実施例では複合的な機能を持つスマートフォン端末等を用いるため、ICカードを交換する等といった不正乗車も防ぐことができる。ただし、利用の際には、例えば、端末等毎にアプリ利用のライセンス認証を必要とする。この場合、利用者は、端末等を変える際には古い端末からライセンスを停止し、新しい端末でライセンスを利用できるような手続きをとる必要がある。例えば、登録サイト等で手続きをしてもよいし、新しい端末の該当アプリに入力するIDとパスワード等を記入してログインする際に、古い端末の該当アプリから自動的にログアウトされて利用できなくなってもよい。また、例えば、管理装置等で、個人携帯端末IDが入場済みかどうかを判断することで、別の支払い方法と連動しても不正乗車を防ぐことができる。

[0230] なお、信号の発信や受信は、BLEビーコンには限定されない。例えばBLE通信、すなわちBLEの発信と受信でも実現可能である。ただし、この

場合は一部手順が異なる。BLE通信はBLEビーコンよりも利用可能な通信帯域が広い利点を得られる。また信号の種別もBLEに限られず、Wi-Fi、RFID、IMES、ZigBee等、既知の規格化された無線通信に用いられる信号も適宜利用できる。さらに、電波信号に限られず、超音波や光通信等の媒質を利用してもよい。

[実施例2]

(事後支払いシステム全般)

[0231] 次に実施例2として、コンビニエンスストアやスーパーマーケット等の販売店において、利用者が個人携帯端末10を取り出すことなく、決済可能な例について説明する。なお、実施例1と同様の点については説明を省略し、異なる点のみについて説明する。

[0232] 従来、コンビニや洋服店等の販売店においてRFID等を商品に設置することで、もしくは、カメラ等で監視することにより、利用者が購入しようとする商品の合計金額を知る手段はあったが、支払いをするにはレジを利用したり、2次元バーコードを利用したりする等手間があった。そこで、本実施例の位置特定認証技術を用いることで利便性を向上することができる。

[0233] 例えば、事業者は、管理端末50をコンビニに設置し、位置特定装置20を出口等に設置する。この位置特定装置20にはRFIDタグの読み取り装置を設置しておく。また、商品には、RFIDタグを付けておく。RFIDタグには金額情報や紐付く情報が記録されている。利用者は、管理サーバシステム30を通じて事業者と利用契約を結ぶ。これにより、利用者は、どの位置特定装置20をいつ利用することができるかが登録される。利用者は、個人携帯端末10を保持しながら、買い物によって商品が入った袋を持ちながら、販売店出口の位置特定装置20を通過する。位置特定装置20は、利用者の持つ個人携帯端末10の位置特定・認証を行いつつ、RFIDタグの読み取りを行って合計金額を計算し、利用者に事後請求を行う。

[0234] これにより、利用者はレジに並ぶことなく、そのまま商品を持ち帰ることができる。また、事業者は、利用者と支払いのやり取りをすることを極端に

減らすことができる。

[0235] なお、RFIDの代わりに、入店した利用者をカメラで追跡、かごや袋に入れた商品を認識してその利用者の支払うべき合計金額をもとめてもよい。また、利用者は、最初に位置特定装置20を通過しておいて、事後に支払ってもよい。

[0236] なお、位置測定装置20の代わりにレジなどにBluetoothのみを設置して代用してもよい。この場合、高精度な位置測定ではないものの、従来程度の精度の位置測定精度はでき、本実施形態に係る認証技術を用いて本人認証は可能となる。例えば、レジの画面等に決済・承認ボタンなどを表示させて、利用者に押させることで決済させてもよい。また、4桁の数字を入れる等した上で決済させても良い。この場合は、レジ装置がタブレットなどの装置とアプリで構成されるようなものであってもよい。さらに、商品の認識はRFIDタグやカメラ等で商品を認識する構成に限らず、従来のバーコード入力等であってもよい。この場合は、事業者側ではレジに店員の配置が必要となるものの、現金管理の必要性がなくなり、また利用者にとって手間なく決済が完了する利便性が得られるといったメリットがある。

[0237] また、店舗内にBLE受信機を設置することにより、従来のような精度、もしくは本位置測定技術のような高精度な位置測定を設置し、顧客のスマートフォンの発信するBLE電波を利用して顧客等の動線分析を行っても良い。

[実施例3]

(事後支払いシステム全般) (無線充電)

[0238] 実施例3では、無線充電において利用者が個人携帯端末10を取り出すことなく利用できる例について説明する。なお、実施例1、2と同様の点については説明を省略し、異なる点のみについて説明する。

[0239] スマートフォン端末等に無線にて充電する方法が研究開発されており、実際に充電が可能となっている。例えば、Cotaというワイヤレス充電システムは、最大10mまで、1Wで充電することができる。これを駅等に複数

設置することで、歩きながら対応スマートフォンを充電することができるようになる。しかし、充電している人物を特定しなければ充電料金を請求することができない。そこで、本実施例の位置特定認証技術を用いることで歩きながら利用者を特定・認証し、利用者は事後支払いを行うことができる。

- [0240] 例えば、事業者は、位置特定装置20をワイヤレス充電システム周辺に設置しておく。また、利用者がインストールしている個人携帯端末10の位置特定・認証用のアプリには、充電量を測定する機能を有している。利用者は、事前に事業者と管理サーバシステム30を経由して契約しておく。利用者は、充電したい個人携帯端末10を保持し、ワイヤレス充電システム周辺に移動する。位置特定装置20は、利用者の個人携帯端末10を位置特定・認証を行うことで、支払能力を確認し、その個人携帯端末10に向けてワイヤレス充電システム用の電波を発信、充電することができる。個人携帯端末10は、位置特定・認証アプリを通じて充電量を測定し、充電量を算出することができ、管理サーバシステム30に通知することができる。管理サーバシステム30は、利用者にワイヤレス充電システムの利用料を請求することができる。これにより利用者も事業者も利便性が向上する。

[実施例4]

(事後支払いシステム全般) (ドライブスルー)

- [0241] 実施例4では、ドライブスルーにおいて利用者が現金やクレジットカード、個人携帯端末10を取り出すことなく利用できる例について説明する。なお、実施例1～3と同様の点については説明を省略し、異なる点のみについて説明する。
- [0242] 従来、ドライブスルーにおいて、商品を受け取ったのちに、現金やクレジットカード、個人携帯端末10等での支払いが必要であったが、支払いの手間があった。そこで、本実施例の位置特定認証技術を用いることで車に居ながらにして、事業者は利用者を特定・認証でき、利用者は事後支払を行うことができる。
- [0243] 例えば、位置特定装置20をドライブスルーに設置しておく。利用者は、

事前に事業者と管理サーバシステム30を経由して契約しておく。事業者は、利用者の注文時、もしくは、商品引き渡し時に位置特定装置20を用いて利用者の個人携帯端末10の位置特定・認証を行い、利用料を請求する。これにより利用者も支払いのための手間が減るため、利便性が向上する。また、事業者も支払いのための手間が減るため利便性が向上する。

なお、実施形態4においても、位置測定装置20の代わりにBluetoothのみを設置して代用してもよい。この場合の構成は上述した実施形態2と同様のものが利用でき、詳細説明を省略する。

[実施例5]

(事後支払いシステム+認証) (車の認識とショッピングの連携)

[0244] 実施例5では、車で付属駐車場に止めてショッピングを行う際に利用者が現金やクレジットカード、個人携帯端末10を取り出すことなくショッピングを利用しつつ、駐車時に発券されていた駐車カードを受け取ったり、もしくはショッピング時にレジで渡したりせず、出庫時に当該駐車カードを出庫ゲートで機械等に読み込ませなくても出庫できるシステム例について説明する。なお、実施例1～4と同様の点については説明を省略し、異なる点のみについて説明する。

[0245] 従来、ショッピングを行う際にレジで駐車カードを渡すことでショッピングの合計額に応じて駐車料金をディスカウントするシステムがあった。また、駐車場に入庫する際に駐車カードの発券と同時に車のナンバープレート撮影することで、駐車場から出庫する際に駐車カードを出庫ゲートで読み込ませることなく自動的にゲートが開いて出庫することができた。しかしながらこのシステムでは、入庫時に駐車カードを受け取り、かつショッピング時に毎回レジで駐車カードを提示する必要がある等、様々な手間があった。

[0246] これに対して、本実施例の位置特定認証技術を用いることで、入庫時に駐車カードを受け取る必要が必ずしもなかったり、ショッピング時にレジで支払いの手間が必要なかったり、同時に駐車カードを提示する必要がなかったりなど、利用者は入庫から出庫まで駐車カードや支払いを意識せずに利用す

ることができるようになる。また事業者も、レジでの支払い作業と駐車カードの確認作業が不要となる。

[0247] 例えば、位置測定装置 20 を入庫・出庫ゲート、各店舗のレジに設置しておく。利用者は、事前に事業者と管理サーバシステム 30 を経由して契約しておく。事業者は、利用者の入出庫時、レジでの決済時に位置測定装置 20 を用いて利用者の個人携帯端末 10 の位置測定・認証を行い、利用料を請求しつつ、入出庫時の駐車カードの授受をなくす。これにより、利用者も事業者も金銭や駐車カードの授受やレジでの処理が減るため、利便性が向上する。

[0248] なお、実施形態 5 においても、位置測定装置 20 の代わりにレジなどに Bluetooth のみを設置して代用してもよい。この場合の構成は上述した実施形態 2 等と同様のものが利用でき、詳細説明を省略する。

[実施例 6]

(事後支払いシステム全般) (バス・タクシーの支払い)

[0249] 実施例 6 では、バス・タクシーの支払いにおいて利用者が現金やクレジットカード、個人携帯端末 10 を取り出すことなく利用できる例について説明する。なお、実施例 1～5 と同様の点については説明を省略し、異なる点のみについて説明する。

[0250] 従来、バスやタクシーは降車時に現金やクレジットカード、ICカード、個人携帯端末 10 等での支払いが必要であったが、支払いの手間があった。そこで、本実施例の位置特定認証技術を用いることで利便性を向上することができる。

[0251] 例えば、事業者は、管理端末 50 をバスの主要な事業場等に設置しておき、バス内の乗降場所に位置特定装置 20 を設置しておく。利用者は、乗車時に位置特定装置 20 を通過し、位置特定装置 20 は、利用開始場所を記録しておく。利用者が、降車時にバス内のゲートを通過する際に、位置特定装置 20 は、位置特定・認証を行うことで個人携帯端末 10 をもつ利用者を通させ、降車場所も記録しておく。事業者は、このデータを事業場の管理端末

50を通じて管理サーバシステム30に通知する。管理サーバシステム30は、利用者ごとの利用記録と料金表から利用者にバスの利用料を事後請求できる。なお、バスの乗り降りを知らせるアプリと連携して、GPS情報等からその乗降タイミングを利用者に知らせてもよい。

[0252] また、タクシーの場合は、事業者は、車内の運転席に管理端末50を設置し、車内の客席の位置を特定できるように位置特定装置20を設置する。利用者は、乗車時に位置特定装置20を通過し、位置特定装置20は、利用開始場所・時間を記録しておく。利用者が降車時に、タクシー内でドライバーが請求を行い、利用者が複数いる場合、請求されたい利用者が支払いを行うことができる。ドライバーは管理端末50を用いて位置特定・認証結果を確認し、請求されたい支払い者の座席にある個人携帯端末10から請求を行うことができる。

[0253] なお、位置測定装置20の代わりにスマートフォン等を設置して代用してもよい。この場合高精度な位置測定自体はできないが従来程度の精度の位置測定精度はでき、本特許技術を用いて本人認証のみはできるため、スマートフォンの画面等に決済・承認ボタンなどのようなものを表示させて、利用者に押させることで決済させることができてもよいし、場合によって4桁の数字を入れる等した上で決済させても良い。

[0254] なお、支払い請求額は事前に料金表を設定しておき、乗車距離や乗車時間から自動的に請求されるようにしてもよいし、特別料金処理等を請求時に設定することもできる。

[実施例7]

(事後支払いシステム全般) (駐車場でのゲートロックをスマホで支払い)

[0255] 実施例7は、駐車場での支払いにおいて利用者が支払いの手間なく利用できる例について説明する。なお、実施例1～6と同様の点については説明を省略し、異なる点のみについて説明する。

[0256] 従来、駐車場等において、利用者は自分の車のロックを事前に解除するか、出場時に支払う必要があったが、手間があった。そこで、本実施例の位置

特定認証技術を用いることで利便性を向上することができる。

[0257] 例えば、位置特定装置20を各駐車場スペースの該当位置に設置しておく。利用者は車内から個人携帯端末10を用いてアプリ等から自分の車のロック解除を申請する。位置特定装置20は、利用者の個人携帯端末10を位置特定・認証をすることにより、該当位置の利用者の車のロックを解除することができる。

[0258] もしくは、位置特定装置20を駐車場の出場位置に設置しておく。利用者が車に乗りながら駐車場を出場する場合、位置特定装置20は利用者の個人携帯端末10を位置特定・認証を行うことで出場を許可し、出場場所のバーを上げる。

[0259] 事業者は事後にクレジットカードからの支払いを請求することができる。

[実施例8]

(事前支払いシステム全般) (イベントや映画館等の事前事後購入後のシステム、スキーリフト、船の乗車)

[0260] 実施例8では、事前に購入したチケット確認を自動化する例について説明する。なお、実施例1～7と同様の点については説明を省略し、異なる点のみについて説明する。

[0261] 従来、映画館や野外でのフェスティバル等チケットを購入後、そのチケットを印刷し、また、そのチケットを担当者に確認してもらったり、もしくは入出場時に機械で確認したり、するため手間がかかりやすく、結果として行列ができ、時間がかかっていた。そこで、本実施例の位置特定認証技術を用いることで利便性を向上することができる。

[0262] 例えば、位置特定装置20を映画館やアミューズメントパーク、イベント会場、スキーのリフトの入場ゲート、船の乗降所等に設置する。図58のように、利用者は、映画館やアミューズメントパーク、イベント、スキー会社、船運航会社等のサイトや代理店サイト等で映画館やアミューズメントパーク、イベント、スキーリフト利用、船乗車の予約を事前に行い、インストールしている位置特定認証アプリに2次元バーコードで予約情報を移行、もし

くは、事業者の予約アプリから予約後に自動的にインストールしている位置特定認証アプリに予約情報を移行する。図59のように、利用者は、個人携帯端末10を用いて位置特定装置20で位置特定・認証を受けることで通過しつつ、支払う。なお、事前に事業者が設定した料金を事後に支払ってもよい。

- [0263] また、事前に既存のインターネットや店舗等の支払い方法で支払った後、2次元バーコードや個人携帯端末10の位置情報認証アプリの自動起動等の方法でその個人携帯端末10の位置情報認証アプリにその支払った情報を移行する。情報を受け取った個人携帯端末10は、管理サーバシステム30にその情報を送る。管理サーバシステム30は、事業会社にその情報を照合する。事業者用管理システム40は、照合確認を行って確認した後、そこから利用者に許可された位置特定装置20の場所や利用期間等を生成し、管理サーバシステム30にその情報を送信する。

[実施例9]

(事前支払いシステム全般) (ホテル)

- [0264] 実施例9では、事前にホテル予約した部屋の鍵を自動的に解錠する例について説明する。なお、実施例1～8と同様の点については説明を省略し、異なる点のみについて説明する。
- [0265] 従来、ホテルを予約してもホテルを利用する際には、チェックインが必要であった。自動化されていても省略できないこのチェックインは、個人情報を再度記入したり支払いを行ったりすることで本人確認を行う必要があった。そこで、本実施例の位置特定認証技術を用いることで利便性を向上することができる。
- [0266] 例えば、事業者であるホテルは、位置特定装置20をホテルの各客室入り口に設置し、施錠システムと連携する。利用者は、ホテルのサイトや代理店サイト等でホテルの予約を行い、インストールしている位置特定認証アプリに2次元バーコードで予約情報を移行、もしくは、ホテルの予約アプリから予約後に自動的にインストールしている位置特定認証アプリに予約情報を移

行する。利用者は、個人携帯端末 10 を用いて予約したホテルの客室入り口に設置された位置特定装置 20 に接近することで、位置特定・認証を受けることで通過しつつ、位置特定装置 20 の場所及び時間があった場合、位置特定装置 20 によってドアが解錠される。支払いは事前の予約時に払ってもよいし、利用終了後等の事後に支払ってもよい。この支払いは、本システムで利用してもよいし、ほかの支払いシステムを利用してもよい。

[0267] なお、位置情報認証端末及び管理端末 50 は、管理サーバシステム 30 に解錠した情報を送る。管理サーバシステム 30 は、事業会社に事業者用管理システム 40 を通じてその情報を通知する。

[0268] これにより、従来必要であった鍵をフロントに預けたりする手間もなくすることができる。

[実施例 10]

(支払いを含むシステム) (認証システム、位置特定装置 20 をマンションやオフィス、会議室等の入退室管理に必要な入出場、もしくは車のドア)

[0269] 実施例 10 では、個人携帯端末 10 を認証することにより付随する行動を自動化する例について説明する。なお、実施例 1～9 と同様の点については説明を省略し、異なる点のみについて説明する。

[0270] 従来、入退室管理等において個人認証は IC カードをタッチしたり、指紋認証をしたりする等、手間があった。そこで、本実施例の位置特定認証技術を用いることで利便性を向上することができる。そこで、本実施例の位置特定認証技術を用いることで利便性を向上することができる。

[0271] 例えば、事業者は、位置特定装置 20 をマンションやオフィス、会議室等の入退室管理に必要な入出場、もしくは車のドアに設置しておく。また、利用者が位置特定装置 20 のどの場所・どの期間で利用していいかを事業者が設定しておく。利用者は、個人携帯端末 10 を用いて位置特定装置 20 で位置特定・認証を受けることで、許可された場所・期間で入退室可能となる。

[0272] 位置特定装置 20 及び管理端末 50 は、管理サーバシステム 30 を経由して入退室の情報を事業者用管理システム 40 に通知することができる。これ

により、例えば、マンションのオートロック解除等がより高速に解除できたり手間が減ったりする。また、社員の勤怠管理を行うことができる。また、会議室予約等として利用できる。また、セキュリティゾーンを設定することができる。なお、時間的に変更可能なセキュリティゾーンを設定することもできる。

[0273] また、車のドアを触ることなく、もしくは、遠隔で鍵を解除する作業なく、近づくだけで開錠することができる。この場合、運転席に座るユーザに応じたミラーや座席の角度を変更させることが出来るほか、発信すべきコメントを変更出来る等、ホスピタリティをあげることが出来る。特にシェアリングカーなどでの認証の手間を大幅に削減出来る。

[0274] さらに、以上のシステムにおいて、認証と位置特定を分離してもよい。すなわち、位置特定のみを行い、認証を行わないシステムや、逆に認証のみを行い、位置特定を行わないシステムを構築することもできる。

[実施例 11]

(支払いを含む認証システム) (認証システム、PC、ATM)

[0275] 実施例 11 では、個人携帯端末 10 を認証することにより本人認証をより簡素化する例について説明する。なお、実施例 1 ~ 10 と同様の点については説明を省略し、異なる点のみについて説明する。

[0276] 従来、ATM等において本人認証は暗証番号を入力したり、静脈認証をしたりする等、手間があった。そこで、本実施例の位置特定認証技術を用いることで利便性を向上することができる。

[0277] 例えば、PCやATM等、本人認証が必要な装置に位置特定装置 20 を設置しておく。また、利用者が位置特定装置 20 のどの場所・どの期間で利用していいかを本人もしくは事業者が本人認証をした上で設定しておく。利用者は、個人携帯端末 10 を用いて位置特定装置 20 で位置特定・認証を受けることで、許可された場所・期間で本人認証を受けられ、PCに近づくだけでログインができたり、ATMの操作を完了させたりすることができる。PCにおいて、ネット上の購入などに必要なクレジットカード情報の入力等を

省いて購入することが出来るし、ＡＴＭにおいてはお金を引き出したり出来る。なお、ＡＴＭにおいて、利用者に応じて発信するコメントを変更してもよい。

- [0278] また、従来の顔認証では誤認識等が課題であるため単独技術ではより多くの人数では対応出来ない場合があり、電話番号の入力やＩＣカードの認識などの手間が掛かる物との組み合わせが必要であった。これに対し本実施形態においては、個人携帯端末１０と組み合わせることで手間なく顔認証を実施することが出来、入国審査や病院等での受付などで手間なく利用することが出来るようになる。このように、顔認証技術や指紋認証技術など、一つの端末で複数のセキュリティとの組み合わせが可能となる。

[実施例１２]

（位置特定のみ）（自立走行ロボット（ドローン等）、屋内地図、座席指定、（三角測量））

- [0279] 実施例１２では、個人携帯端末１０を認証することにより付随する行動を自動化する例について説明する。なお、実施例１～１１と同様の点については説明を省略し、異なる点のみについて説明する。

- [0280] 従来、ドローン等の自立走行ロボットは自己の位置を特定するために、ＧＰＳを用いて測定したり、ＰＤＲを用いたりする等して推定をしてきたが、あまり精度は高くなかった。また、周囲の画像から三角測定をして位置推定を行ってきたが、カメラを複数台用意する必要があり、必ずしも簡易ではなかった。そこで、本実施例の位置特定技術を用いることで利便性を向上することができる。そこで、本実施例の位置特定技術を用いることで利便性を向上することができる。

- [0281] 図２５は、スマートフォン端末等をＢＬＥ受信機とし、複数のＢＬＥ発信機を３か所に配置した場合の例を示している。例えば、図２５に示すように、位置を特定したい空間に、ＢＬＥ発信機を３か所の限らず複数個所設置し、一か所につき複数台設置する。このように設置することにより、ＢＬＥ受信機は一か所につき複数台のＢＬＥ発信機の電波を受信することができる。

この電波の電波強度を平均化することにより、時間的に安定した電波強度を得られる。このため、複数個所のBLE発信機の設置位置を3次元情報で知っておけば、BLE受信機自身の位置を3点測定のとらえで平面上、もしくは、空間上で知ることができる。

[0282] 図24は、スマートフォン端末等をBLE受信機とし、複数のBLE発信機を2か所に配置した場合の例を示している。もしくは、図24に示すように複数のBLE発信機を2か所に限らず複数個所に設置し、図27のようにある2つのBLE発信機か所を選択して、BLE受信機の存在エリアを、例えば10cm等、十分小さくなるような強度差を得ることで自身の位置を特定することができる。これにより、BLE受信機を取り付けるだけで、容易に位置を特定することができる。

[0283] 以上のように本発明の実施形態によれば、レジや改札機において利用者がスマートフォン端末等を取り出すことなく支払いができる。特にスマートフォン端末等を持って移動している人を一人ずつ高速にかつ高精度に捕捉・区別し、非接触に手間なくセキュアに個人の認証することで、認証に付随する行動をタッチレスで自動化することができる。また本発明の一般的かつ特定の態様は、システム、方法及びコンピュータプログラムを用いて実装され、又はシステム、方法及びコンピュータプログラムの組み合わせを用いて実現され得る。

[実施例13]

(本人認証および位置測定) (イベント入場)

[0284] 実施例13では、個人携帯端末10を認証することによりイベント受付を自動化する例について説明する。なお、実施例1～12と同様の点については説明を省略し、異なる点のみについて説明する。

[0285] 従来、セミナーや展示会、説明会等のビジネスセミナーや、映画館や演劇、音楽フェス等の文化イベント、遊園地や野球場などの大型商業施設などでの、入場には時間が掛かった。これは、参加者リストが印刷された紙から探して受付をするのに時間が掛かったり、参加者がQRコードを表示するのに

時間が掛かったり、紙チケットをもぎるのに時間が掛かったり、入場ゲートにQRコードを読み込ませたり紙チケットを入れるのに時間が掛かったり、したためで参加者および主催者にとって手間や人員、時間を割く必要があった。そこで、本実施例の本人認証技術や位置測定技術を用いることで利便性を向上することが出来る。

[0286] 例えば、ビジネスセミナーや文化イベントの受付にBLE受信機付きのタブレット等を等設置しておく。利用者のスマートフォンにはイベント参加用アプリをインストールしておき、タブレットにはイベント受付アプリをインストールしておく。BLE受信機があれば、従来程度の精度の位置測定は可能である。無料でも有料でもイベントに参加したい参加者は参加者用アプリをインストールしておき、またイベント参加登録を済ませておく。これにより、当日イベントに参加するときに近づいた参加者から順に当該タブレット等に名前等を表示させることが出来るようになる。例えば、利用者に名前を言ってもらうだけで、受付担当者はごく少数表示されたイベント参加者名から簡単に探して受付を完了させることが出来る。また、参加者名をタップすることで受付処理をする場合、未受付の参加者のみを表示させ続けることが出来る。これにより、従来よりも高速に受付を完了できるため、受付担当者の人数を減らすことが出来る。あるいは、無料のイベント等、決済機能や認証機能が不要な場合は、参加者自身に受付用のタブレットに表示された自身の名前等をタップして消し込んでもらうことで受付を済ますように構成してもよい。この場合は必要に応じて担当者呼び出す等として、さらに受付担当者を減らすことが可能となる。

[0287] なお、有料の場合、当日参加する前に決済をしてもいいし、クレジットカードを登録するなどして当日参加した時点で決済をしてもいいし、後日請求しても良い。

[0288] また、展示会や大型の文化イベント、大型商業施設などに位置測定装置20を設置しておくこともできる。これにより上記のような方法において無料でも有料でも自動的に参加者の本人認証と位置測定を実現するため、無人で

対応することが出来る。

産業上の利用可能性

[0289] 本発明の実施形態や実施例に係る位置特定システム、位置特定装置、位置特定方法、位置特定プログラム及びコンピュータで読み取り可能な記録媒体並びに記録した機器によれば、例えばレジや改札機において利用者がスマートフォン端末等を取り出すことなく支払いができるシステムに好適に利用できる。

符号の説明

[0290] 100、400…位置特定システム
10…個人携帯端末
11…個人端末側発信部
11A…個人端末側通信部
12…個人端末側制御部
13…個人端末側記憶部
14…個人端末側時刻部
15…個人端末側入出力部
16…個人端末側演算部
20…位置特定装置
20B…自動改札機
21…位置特定側受信部
21A…位置特定側通信部
210…通過センサ部
2101～2105…通過センサ
2111～2118…BLEビーコン受信機
22、22A、22B…第一位置特定側受信部
23、23A、23B…第二位置特定側受信部
24、24A、24B…区画板
25…位置特定側演算部

2 6 …位置特定側記憶部
2 7 …位置特定側時刻部
2 8 …位置特定側制御部 ; 2 8 A …第 1 表示部 ; 2 8 B …第 2 表示部 ; 2 8
C …リーダライタ ; 2 8 C 1 …アンテナ ; 2 8 C 2 …通信部
2 9 …扉部
3 0 …管理サーバシステム
3 1 …サーバ側通信部
3 2 …サーバ側演算部
3 3 …サーバ側記憶部
4 0 …事業者用管理システム
4 1 …事業者側通信部
4 2 …事業者側演算部
4 3 …事業者側入出力部
4 4 …事業者側記憶部
5 0 …管理端末
5 1 …管理端末側通信部
5 2 …管理端末側演算部
5 3 …管理端末側入出力部
5 4 …管理端末側時刻部
5 5 …管理端末側記憶部
6 0 …金融機関
7 0 …時刻配信サーバ
9 0 …起動信号発信機
U S R …利用者
D A、D A 1、D A 2、D B、D B 1、D B 2 …通過判定エリア