

明 細 書

発明の名称：

位置情報認証システム、測位端末、および位置情報取得装置

関連出願の相互参照

[0001] 本出願は、2014年1月21日に出願された日本国特許出願2014-8904号に基づくものであり、ここにその記載内容を参照により援用する。

技術分野

[0002] 本開示は、位置情報を算出するために航法衛星から受信する航法メッセージの認証を行うことができる位置情報認証システム、その認証システムが備える測位端末、位置情報取得装置に関する。

背景技術

[0003] グローバルポジショニングシステム（以下、GPS）などの航法衛星システムが備える航法衛星から衛星電波を受信し、その衛星電波に含まれている航法メッセージを用いて現在位置を算出する測位端末が広く知られている。

[0004] ところが、偽の衛星電波を生成して放送する偽衛星電波生成装置が存在する。この偽衛星電波生成装置を使って、悪意のある者が測位端末に誤った位置を算出させる虞がある。

[0005] そこで、特許文献1に開示されているように、位置情報を算出するために航法衛星から受信する航法メッセージの信頼性を判断するために、その航法メッセージを認証することができる位置情報認証システムが提案されている。

[0006] この位置情報認証システムにより、測位端末は、測位端末自身が受信した航法メッセージが認証センタで認証された航法メッセージであるかどうかを判断できる。測位端末自身が受信した航法メッセージが認証センタで認証された航法メッセージであると判断できれば、その航法メッセージは、航法衛星が送信したものであると判断することができる。

- [0007] 特許文献1の技術により、航法メッセージを受信する測位端末は、信頼性のある現在位置を算出することができる。
- [0008] 本願発明者らは以下を見出した。
- [0009] 測位端末が算出した位置情報の用途としては、その測位端末を所有するユーザが現在位置を知る用途の他に、測位端末が算出した現在位置を示す位置情報を、周囲に送信する用途が考えられる。たとえば、位置情報を、有料駐車区域や有料道路を管理する課金管理装置に送信して、自動的に課金する用途が考えられる。この用途においては、測位端末が信頼性のある現在位置を算出できたとしても、測位端末が、算出した現在位置とは異なる位置を示す位置情報を、その位置情報を受信して課金処理を行う位置情報取得装置に送信してしまうと、正しく課金を行うことができない。
- [0010] このように、測位端末が算出した位置を位置情報取得装置が取得して課金などの所定の処理を行うシステムにおいては、測位端末が位置を正しく算出することができるだけでは十分でない。測位端末は測位端末自身が位置情報を改ざんしない端末であることを示し、位置情報を取得する位置情報取得装置は、測位端末が、位置情報を改ざんしない信頼できる端末であることを判断できる必要がある。

先行技術文献

特許文献

- [0011] 特許文献1：日本国公開特許公報2013-130395号

発明の概要

- [0012] 本開示は、この事情に基づいて成されたものであり、その目的とするところは、測位端末が、位置情報認証システムに対応していることを、その測位端末から位置情報を取得する位置情報取得装置が判断できる位置情報認証システム、その測位端末、位置情報取得装置を提供することにある。
- [0013] 本開示の一態様に係る位置情報認証システムは、航法メッセージを受信し、受信した航法メッセージが認証できる航法メッセージである場合に、その航法メッセージを用いて算出した現在位置を示す位置情報を外部に無線送信

する測位端末と、測位端末が認証に用いるセンタ作成認証データを送信する通信衛星に、そのセンタ作成認証データを送信する認証センタ装置と、測位端末が無線送信した位置情報を受信する位置情報取得装置とを備える。

[0014] 認証センタ装置は、航法衛星システムが備える航法衛星から航法メッセージを含んでいる衛星電波を受信するセンタ側衛星受信部と、暗号キーを作成し、その暗号キーとセンタ側衛星受信部が受信した衛星電波に含まれている航法メッセージとに基づいて、センタ作成認証データを作成するセンタ側認証データ作成部と、センタ側認証データ作成部が作成したセンタ作成認証データを通信衛星に送信する認証データ送信部と、を備える。

[0015] 測位端末は、通信衛星からセンタ作成認証データを受信するとともに、航法衛星から衛星電波を受信する端末側衛星受信部と、認証センタ装置から、暗号キーまたはその暗号キーを作成することができるキー作成データのいずれかであるキー関連データを受信するキー受信部と、キー受信部が受信したキー関連データと、端末側衛星受信部が受信した衛星電波から抽出した航法メッセージとに基づいて端末作成認証データを作成する端末側認証データ作成部と、センタ作成認証データと端末作成認証データとを比較し、一致している場合に端末側衛星受信部が受信した衛星電波に含まれている航法メッセージが認証できたと判断する認証判断部と、キー受信部が認証センタ装置から受信したキー関連データに基づいて、端末側衛星受信部が受信した衛星電波に含まれている航法メッセージが認証できたことを示す認証済みデータを作成する認証済み作成部と、航法メッセージに基づいて算出した位置情報とともに、認証済み作成部が作成した認証済みデータを送信する端末側送信部とを備える。

[0016] 位置情報取得装置は、端末側送信部が送信した位置情報および認証済みデータを通信部から取得する端末データ取得部と、通信部を介して、認証センタ装置からキー関連データを取得するキー取得部と、キー取得部が取得したキー関連データに基づいて、認証済みデータと比較するための認証済み比較データを作成する比較データ作成部と、端末データ取得部が取得した認証済

みデータと比較データ作成部が作成した認証済み比較データとを比較し、一致している場合に、測位端末は正規の測位端末であると判断する端末判断部とを備える。

[0017] 本開示によれば、測位端末は、航法衛星から受信した衛星電波に含まれている航法メッセージの認証を行う。この認証のために、キー受信部は、認証センタ装置がセンタ作成認証データの作成に用いた暗号キーまたはその暗号キーを作成することができるキー作成データであるキー関連データを認証センタ装置から受信している。そして、認証ができた場合には、認証センタ装置から受信したキー関連データを用いて、認証済みであることを示す認証済みデータを作成して、位置情報とともにその認証済みデータを送信している。

[0018] このように、測位端末は、認証済みデータを、認証センタ装置から取得したデータであるキー関連データを用いて作成して位置情報とともに送信する。これにより、測位端末自身が、認証センタ装置との間の通信が可能な、認証センタ装置から信頼された正規の測位端末であることを証明することができる。

[0019] また、その認証済みデータを作成するためのキー関連データは、測位端末自身が受信した衛星電波に含まれている航法メッセージを認証するために認証センタ装置から取得される。よって、認証済みデータを作成するためのデータを別途、認証センタ装置から取得する必要がないので、認証済みデータを作成する処理を簡単にすることができる。

[0020] そして、位置情報とともに認証済みデータを受信した位置情報取得装置は、位置情報取得装置自身も認証センタ装置からキー関連データを取得する。そして、取得したキー関連データに基づいて、認証済みデータと比較するための認証済み比較データを作成する。端末判断部は、この認証済み比較データと、端末データ取得部が取得した認証済みデータとを比較することで、位置情報を送信した測位端末が正規の測位端末であるか否かを判断することができる。

[0021] 本開示の別の一態様に係る測位端末は、航法メッセージを受信し、受信した航法メッセージが認証できる航法メッセージである場合に、その航法メッセージを用いて算出した現在位置を示す位置情報を外部に無線送信する。測位端末は、認証センタ装置が作成し、測位端末における認証に用いるために通信衛星に送信したセンタ作成認証データを通信衛星から受信するとともに、航法衛星システムが備える航法衛星から航法メッセージを含んでいる衛星電波を受信する端末側衛星受信部と、認証センタ装置から、センタ作成認証データを作成するための暗号キーまたはその暗号キーを作成することができるキー作成データのいずれかであるキー関連データを受信するキー受信部と、キー受信部が受信したキー関連データと、端末側衛星受信部が受信した衛星電波から抽出した航法メッセージとに基づいて端末作成認証データを作成する端末側認証データ作成部と、センタ作成認証データと端末作成認証データとを比較し、一致している場合に端末側衛星受信部が受信した衛星電波に含まれている航法メッセージが認証できたと判断する認証判断部と、キー受信部が認証センタ装置から受信したキー関連データに基づいて、端末側衛星受信部が受信した衛星電波に含まれている航法メッセージが認証できたことを示す認証済みデータを作成する認証済み作成部と、航法メッセージに基づいて算出した位置情報とともに、認証済み作成部が作成した認証済みデータを送信する端末側送信部とを備える。

[0022] 本開示の別の一態様に係る位置情報取得装置は、航法メッセージを受信し、受信した航法メッセージが認証できる航法メッセージである場合に、その航法メッセージを用いて算出した現在位置を示す位置情報および受信した航法メッセージが認証できたことを示す認証済みデータを外部に無線送信する測位端末から、位置情報および認証済みデータを受信する。位置情報取得装置は、測位端末が送信した位置情報および認証済みデータを通信部から取得する端末データ取得部と、通信部を介して、認証センタ装置から、測位端末が認証に用いるセンタ作成認証データを作成するために認証センタ装置が用いた暗号キーまたはその暗号キーを作成することができるキー作成データの

いずれかであるキー関連データを取得するキー取得部と、キー取得部が取得したキー関連データに基づいて、認証済みデータと比較するための認証済み比較データを作成する比較データ作成部と、端末データ取得部が取得した認証済みデータと比較データ作成部が作成した認証済み比較データとを比較し、一致している場合に、測位端末は正規の測位端末であると判断する端末判断部とを備える。

[0023] 本開示の位置情報認証システム、その測位端末、位置情報取得装置によれば、測位端末が、位置情報認証システムに対応していることを、その測位端末から位置情報を取得する位置情報取得装置が判断できる。

図面の簡単な説明

[0024] 本開示についての上記および他の目的、特徴や利点は、添付の図面を参照した下記の詳細な説明から、より明確になる。添付図面において

[図1]図1は、実施形態1となる位置情報認証システムの構成図であり、

[図2]図2は、図1の認証センタ処理装置の構成を詳しく示すブロック図であり、

[図3]図3は、図1の車載機の構成を詳しく示すブロック図であり、

[図4]図4は、衛星電波に含まれている航法メッセージと、R A N Dメッセージの関係を示す図であり、

[図5]図5は、車載機の制御部が実行する処理を示すフローチャートであり、

[図6]図6は、図5のステップS4の航法メッセージ認証処理を詳しく示すフローチャートであり、

[図7]図7は、路側機の制御部が実行する処理を示すフローチャートであり、

[図8]図8は、実施形態2における路側機の構成図であり、

[図9]図9は、路側機が備える制御部が実行する事前処理を示すフローチャートであり、

[図10]図10は、路側機が備える制御部が車載機から位置情報等を受信した場合に実行する処理を示すフローチャートである。

発明を実施するための形態

[0025] (実施形態1)

以下、本開示の実施形態を図面に基づいて説明する。図1に示すように、実施形態1の位置情報認証システム1は、認証センタ装置100、本開示の測位端末に相当する車載機200、本開示の位置情報取得装置に相当する路側機300を備える。

[0026] (位置情報認証システム1の概略構成)

認証センタ装置100は、モニタステーション装置110、認証センタ処理装置120、マスタコントロールステーション装置130を備える。なお、以下では、装置、処理装置を省略し、モニタステーション装置110はモニタステーション110、認証センタ処理装置120は認証センタ120、マスタコントロールステーション装置130はマスタコントロールステーション130とする。

[0027] モニタステーション110は、本開示のセンタ側衛星受信部に相当し、航法衛星システムの一つであるGPSが備えるGPS衛星2が送信するGPS電波を受信する。GPS衛星2は本開示の航法衛星に相当し、GPS電波は本開示の衛星電波に相当する。周知のように、GPS電波には航法メッセージが含まれている。モニタステーション110は、受信したGPS電波を復調して航法メッセージを抽出し、認証センタ120へ送る。複数のGPS衛星2からGPS電波を受信した場合には、それぞれのGPS電波から航法メッセージを抽出して、認証センタ120へ送る。

[0028] 認証センタ120は、航法メッセージと暗号キーであるHマトリクスとから、本開示のセンタ作成認証データに相当するパリティデータを作成する。そして、作成したパリティデータを含む信号をマスタコントロールステーション130に送る。また、車載機200や路側機300との間で通信も行う。この認証センタ120の詳細は図2を用いて説明する。

[0029] マスタコントロールステーション130は、本開示の認証データ送信部に相当し、認証センタ120から受信したパリティデータを準天頂衛星（以下、QZS衛星）3に送信する。

[0030] Q Z S 衛星 3 は本開示の通信衛星に相当し、パリティデータを含んだ航法メッセージを地上に向けて放送する。

[0031] 車載機 200 は、航法メッセージ認証型の車載機であり、GPS 衛星 2 から受信した航法メッセージが認証できるかどうかを、Q Z S 衛星 3 から受信した航法メッセージに含まれているパリティデータを用いて認証する。この認証の際に、認証センタ 120 と通信を行う。また、GPS 衛星 2 から受信した航法メッセージを用いて現在位置を算出し、算出した現在位置を示す位置情報を、後述するハッシュ値とともに外部に無線送信する。ハッシュ値は航法メッセージの認証ができたことを示しており、本開示の認証済みデータに相当する。車載機 200 は、図 3、図 5、図 6 を用いて説明する。

[0032] 路側機 300 は、車載機 200 が送信する位置情報を用いた所定のサービスを提供するサービス提供事業者が管理する。上記サービスとしては、たとえば、車載機 200 を搭載した車両が有料駐車区域に駐車した場合や、その車両が有料道路を走行した場合に、その車両の使用者に課金するサービスがある。

[0033] この路側機 300 は通信部 310 と制御部 320 を備える。通信部 310 は、認証センタ 120 が備える通信部 126（図 2 参照）や、車載機 200 が備える通信部 210（図 3 参照）と無線通信を行う。

[0034] 制御部 320 は、CPU、ROM、RAM 等を備えたコンピュータであり、CPU が、RAM の一時記憶機能を利用しつつ ROM に記憶されているプログラムを実行することで通信部 310 を制御する。また、車載機 200 が送信したハッシュ値を通信部 310 を介して取得し、そのハッシュ値に基づいて、車載機 200 が正規の車載機であるか否かを判断する。この判断の際に、認証センタ 120 と通信を行う。

[0035] （認証センタ 120 の詳細構成）

図 2 に示すように、認証センタ 120 は、制御部 122、データ記憶部 124、通信部 126 を備える。

[0036] 制御部 122 は、CPU、ROM、RAM 等を備えたコンピュータであり

、データ記憶部 124、通信部 126 を制御する。また、CPU が、RAM の一時記憶機能を利用しつつ ROM に記憶されているプログラムを実行することで、RAND メッセージ生成部 1221、SEED 値生成部 1222、H マトリクス計算部 1223、パリティ計算部 1224、信号加工部 1225 としての機能を備える。なお、これら、各部 1221～1225 の機能は、特許文献 1 に開示されている機能と同じでよい。また、これらに加え、制御部 122 は、H マトリクス選択部 1226 も備える。この制御部 122 は、本開示のセンタ側認証データ作成部に相当する。

[0037] RAND メッセージ生成部 1221 は、レファランス認証ナビゲーションデータ (RAND: Reference Authentication Navigation Data) を意味しており、モニタステーション 110 から取得する航法メッセージから作成する。

[0038] 図 4 に RAND メッセージと航法メッセージとの関係を示す。周知のように、航法メッセージはサブフレーム 1～5 に分けられ、サブフレーム 4、5 は、それぞれ、1～25 ページを持つ。そして、各サブフレームはワード 1～10 に分けられる。

[0039] RAND メッセージは、サブフレーム 1 のワード 2 に含まれている経過時間 TOW (time of week、本開示の時刻情報に相当)、ワード 8～10 に含まれている TOC、AFO、AF1 が順番に並んでいる。さらに、その後に、アンチスプーフフラグである AS Flag、衛星番号である PRN (Pseudo Random Noise) ID が追加されている。なお、図 4 において、RAND メッセージを構成する各データの後の括弧内に示す数値は、各データのビット数を意味する。

[0040] TOW は 6 秒ごとに変化するので、TOW と PRN ID を含んでいる RAND メッセージは、どの GPS 衛星がいつ送信したかを示すメッセージであると言える。また、TOW が 6 秒ごとに変化し、また、PRN ID を含んでいるので、モニタステーション 110 が受信した GPS 衛星 2 ごと、かつ、6 秒ごとに RAND メッセージを生成する。

[0041] SEED 値生成部 1222 は、PC クロックを入力として唯一の SEED

値を生成する。たとえば、PCクロックを入力として乱数を発生させることで、SEED値を生成する。なお、本実施形態におけるSEED値は36ビットとする。

[0042] Hマトリクス計算部1223は、SEED値生成部1222が生成したSEED値を使い、このSEED値に一对一に対応するHマトリクスを計算する。このHマトリクスは本開示の暗号キーに相当する。また、SEED値が決まればHマトリクスを作成することができるので、SEED値は本開示のキー作成データに相当する。Hマトリクスとしては、周知のハッシュ関数を用いればよく、例えばLDPC (Low Density Parity Check) 符号化を行うためのパリティ検査行列を用いればよい。さらに、パリティ検査行列から決定される生成行列を用いてもよい。

[0043] Hマトリクスは本開示の暗号キーの一例に対応し、HマトリクスまたはSEED値は本開示のキー関連データの一例に相当する。

[0044] パリティ計算部1224は、RANDメッセージ生成部1221が作成したRANDメッセージ、Hマトリクス計算部1223が計算したHマトリクスに基づいて、パリティデータを計算する。すなわち、このHマトリクスをRANDメッセージに乗じることで、パリティデータを計算する。

[0045] 信号加工部1225は、パリティ計算部1224が計算したパリティデータ、および、その計算に使用したRANDメッセージを、QZS衛星3に送信させる航法メッセージに挿入する。そして、挿入済みの航法メッセージをマスタコントロールステーション130に送る。

[0046] さらに、信号加工部1225は、信号の挿入に合わせて、パリティ計算部1224が計算したパリティデータ、パリティデータの計算に用いたRANDメッセージ、Hマトリクス、そのHマトリクスの計算に用いたSEED値をデータ記憶部124に記憶する。

[0047] この信号加工部1225は、RANDメッセージ生成部1221がRANDメッセージを生成するごとに、RANDメッセージとパリティデータをQZS衛星3に送信させる航法メッセージに挿入する。よって、SEED値生

成部 1 2 2 2、Hマトリクス計算部 1 2 2 3、パリティ計算部 1 2 2 4 も、R A N D メッセージ生成部 1 2 2 1 が R A N D メッセージを生成することにより、処理を実行する。

[0048] Hマトリクス選択部 1 2 2 6 は、車載機 2 0 0 から送信されてきた P R N I D、T O W、公開キーを通信部 1 2 6 が受信したときは、データ記憶部 1 2 4 に記憶されているHマトリクスから、受信した P R N I D、T O W に対応するHマトリクスを選択する。そして、選択したHマトリクスを公開キーで暗号化し、暗号化したHマトリクスを、P R N I Dなどを送信した車載機 2 0 0 へ送信する。

[0049] また、路側機 3 0 0 から送信されてきた P R N I D、T O W、公開キーを通信部 1 2 6 が受信したときは、データ記憶部 1 2 4 に記憶されているHマトリクスおよびパリティデータから、受信した P R N I D、T O W に対応するHマトリクスおよびパリティデータを選択する。そして、選択したHマトリクスおよびパリティデータを公開キーで暗号化し、暗号化したHマトリクスおよびパリティデータを、P R N I Dなどを送信した路側機 3 0 0 へ送信する。

[0050] 通信部 1 2 6 は、車載機 2 0 0 が備える通信部 2 1 0、および、路側機 3 0 0 が備える通信部 3 1 0 と通信する。

[0051] マスタコントロールステーション 1 3 0 は、信号加工部 1 2 2 5 が生成した航法メッセージを Q Z S 衛星 3 に送信する。

[0052] Q Z S 衛星 3 は、マスタコントロールステーション 1 3 0 から受信した航法メッセージを地上に向けて放送する。

[0053] (車載機 2 0 0 の構成)

Q Z S 衛星 3 が放送した航法メッセージは、車載機 2 0 0 の衛星受信部 2 3 0 に受信される。この車載機 2 0 0 は、衛星受信部 2 3 0 の他に、通信部 2 1 0、制御部 2 2 0 を備える。

[0054] 通信部 2 1 0 は、受信部 2 1 1 と送信部 2 1 2 を備える。受信部 2 1 1 は、本開示のキー受信部に相当し、送信部 2 1 2 は本開示の端末側送信部に相

当する。通信部 210 は、狭域通信機能と広域通信機能を備えている。狭域通信機能は、たとえば、通信距離が数百メートルである。広域通信機能は、通信距離がたとえば数キロメートルであり、公衆通信回線網の基地局と通信を行うことにより、公衆通信回線網の通信圏内の他の通信機器と通信することができる。狭域通信機能により、路側機 300 の通信部 310 と通信し、広域通信機能により、認証センタ 120 の通信部 126 と通信する。

[0055] 衛星受信部 230 は、本開示の端末側衛星受信部に相当し、GPS 衛星 2、QZS 衛星 3 が送信する電波を一定周期で受信する。

[0056] 制御部 220 は、CPU、ROM、RAM等を備えたコンピュータであり、通信部 210、衛星受信部 230 を制御する。また、CPUが、RAMの一時記憶機能を利用しつつROMに記憶されているプログラムを実行することで、図5に示す処理を実行する。

[0057] 図5に示す処理は、衛星受信部 230 が4つ以上のGPS 衛星 2 からGPS 電波を受信するごとに実行する。4つ以上としているのは、現在位置を算出するには、4つ以上のGPS 衛星 2 からGPS 電波を受信する必要があるからである。

[0058] ステップS2では、GPS 電波に基づいて現在位置を算出する。ステップS4では、航法メッセージ認証処理を実行する。この処理の詳細は図6に示す。

[0059] ステップS42では、QZS 衛星 3 から受信した航法メッセージを、受信部 211 から取得する。

[0060] ステップS44では、ステップS42で取得した航法メッセージから、現在位置の算出に用いた航法メッセージに対応するPRNID、TOW、パリティデータを抽出する。なお、PRNID、TOWは、現在位置の算出に用いた航法メッセージから抽出してもよい。

[0061] ステップS46では、ステップS44で抽出したPRNIDとTOWを公開キーとともに、送信部 212 から認証センタ 120 へ送信する。前述したように、認証センタ 120 は、このPRNIDとTOWより定まるHマトリ

クスを、公開キーにより暗号化して車載機 200 へ送信する。

- [0062] ステップ S 48 では、認証センタ 120 から送信された、暗号化された H マトリクスを受信部 211 から取得する。ステップ S 50 では、ステップ S 48 で取得した、暗号化された H マトリクスを秘密キーで復号する。
- [0063] ステップ S 52 では、ステップ S 46 で送信した PRN ID と同じ PRN ID を航法メッセージに含んでいる GPS 電波から、RAND メッセージを作成する。
- [0064] ステップ S 54 では、ステップ S 52 で作成した RAND メッセージと、ステップ S 50 で復号した H マトリクスとから、比較パリティデータを作成する。ここで作成した比較パリティデータが、本開示の端末作成認証データに相当し、この S 54 は本開示の端末側認証データ作成部に相当する。
- [0065] 続いて本開示の認証判断部に相当するステップ S 56 ~ S 60 を実行する。ステップ S 56 では、ステップ S 54 で作成した比較パリティデータと、ステップ S 44 で抽出したパリティデータが一致するか否かを判断する。
- [0066] ステップ S 50 で復号した H マトリクスは、認証センタ 120 がパリティデータの作成に使用した H マトリクスと同じである。そして、認証センタ 120 のパリティ計算部 1224 は、この H マトリクスと RAND メッセージとに基づいてパリティデータを計算している。
- [0067] よって、ステップ S 54 で作成した比較パリティデータが、ステップ S 44 で抽出したパリティデータと一致する場合、ステップ S 52 で作成した RAND メッセージが、認証センタ 120 が作成した RAND メッセージと同じであると考えることができる。そこで、ステップ S 54 で作成した比較パリティデータと、ステップ S 44 で抽出したパリティデータとが一致する場合、ステップ S 58 に進み、認証成立とする。一方、2つのパリティデータが一致しない場合、ステップ S 60 に進み、認証不成立とする。
- [0068] 説明を図 5 に戻す。ステップ S 4 を実行した後は、本開示認証済み作成部に相当するステップ S 6 ~ S 10 を実行する。ステップ S 6 では、航法メッセージ認証処理の処理結果が、認証成立であったか否かを判断する。

[0069] この判断がN o、すなわち、認証不成立である場合には、図4の処理を終了する。一方、ステップS 6の判断がY e sの場合には、ステップS 8に進む。

[0070] ステップS 8では、位置情報の送信が必要であるか否かを判断する。位置情報の送信が必要である場合としては、たとえば、路側機3 0 0の通信部3 1 0から位置情報の要求信号を受信した場合などがある。また、一定の送信周期で位置情報を送信するようにしてもよい。ステップS 8の判断がN oである場合には、図4の処理を終了する。一方、ステップS 8の判断もY e sとなった場合にはステップS 1 0へ進む。

[0071] ステップS 1 0では、認証センタ1 2 0が作成したデータであるHマトリクスと、パリティデータとを入力キーとしてハッシュ関数からハッシュ値を作成する。このハッシュ値は本開示の認証済みデータに相当する。

[0072] ステップS 1 2では、ステップS 1で算出した現在位置を示す位置情報、ステップS 8で作成したハッシュ値、ステップS 4 4で抽出したP R N I D、T O Wを、送信部2 1 2から路側機3 0 0の通信部3 1 0に送信する。

[0073] (路側機3 0 0の処理)

路側機3 0 0の制御部3 2 0は、周期的に、路側機3 0 0の周囲に位置情報の送信を要求する要求信号を送信する。この要求信号を車載機2 0 0が受信した場合、前述のように、車載機2 0 0は、位置情報、ハッシュ値等を送信する。

[0074] 路側機3 0 0の通信部3 1 0が、車載機2 0 0から位置情報、ハッシュ値等を受信した場合、路側機3 0 0の制御部3 2 0は図7に示す処理を実行する。

[0075] ステップS 7 0では、通信部3 1 0が受信した位置情報、ハッシュ値、P R N I D、T O Wを通信部3 1 0から取得する。このステップS 7 0は本開示の端末データ取得部に相当する。

[0076] ステップS 7 2では、ステップS 7 0で取得したP R N I DとT O Wを公開キーとともに、通信部3 1 0から認証センタ1 2 0へ送信する。なお、こ

の公開キーは路側機 300 が独自に記憶している公開キーであり、車載機 200 が認証センタ 120 へ送信する公開キーとは異なるキーである。

[0077] 前述したように、認証センタ 120 は、この PRNID と TOW より定まる H マトリクスおよびパリティデータを、公開キーにより暗号化して路側機 300 へ送信する。これら H マトリクスおよびパリティデータは、ハッシュ値を作成するための入力キーである。

[0078] ステップ S 74 では、認証センタ 120 から送信された、暗号化された H マトリクスおよびパリティデータを、通信部 310 から取得する。このステップ S 74 は本開示のキー取得部に相当する。

[0079] ステップ S 76 では、ステップ S 74 で取得した、暗号化された H マトリクスおよびパリティデータを秘密キーで復号する。

[0080] ステップ S 78 では、ステップ S 76 で復号した H マトリクスおよびパリティデータを入力キーとして、正規の車載機 200 が使用するものとして予め記憶しているハッシュ関数から比較ハッシュ値を作成する。この比較ハッシュ値は本開示の認証済み比較データに相当し、ステップ S 78 は本開示の比較データ作成部に相当する。

[0081] 続いて、本開示の端末判断部に相当するステップ S 80 ～ S 84 を実行する。ステップ S 80 では、ステップ S 78 で作成した比較ハッシュ値と、ステップ S 70 で取得したハッシュ値が一致するか否かを判断する。

[0082] 2 つのハッシュ値が一致する場合、車載機 200 が送信したハッシュ値も、認証センタ 120 が作成した H マトリクスを入力キーとしていると考えることができる。そこで、2 つのハッシュ値が一致する場合、ステップ S 82 に進み、位置情報、ハッシュ値等を送信した車載機 200 は正規車載機であるとする。一方、2 つのハッシュ値が一致しない場合、ステップ S 84 に進み、位置情報、ハッシュ値等を送信した車載機 200 は不正車載機であるとする。

[0083] 以上、説明した実施形態 1 によれば、車載機 200 は、GPS 衛星 2 から受信した衛星電波に含まれている航法メッセージの認証を行っている (S 4

）。この認証のために、認証センタ 120 がパリティデータの作成に用いた H マトリクスを認証センタ 120 から取得している（S48）。そして、認証ができた場合には、認証センタ 120 から取得した H マトリクスを用いて、認証済みであることを示すためにハッシュ値を作成して（S10）、位置情報とともにそのハッシュ値を送信している（S12）。

[0084] このように、車載機 200 は、認証済みであることを示すデータであるハッシュ値を、認証センタ 120 から取得した H マトリクスを用いて作成して位置情報とともに送信する。これにより、車載機 200 自身が、認証センタ 120 との間の通信が可能な、認証センタ 120 から信頼された正規車載機であることを証明することができる。

[0085] また、そのハッシュ値を作成するための H マトリクスは、車載機 200 自身が受信した衛星電波に含まれている航法メッセージを認証するために認証センタ 120 から取得したものである。よって、ハッシュ値を作成するためのデータを別途、認証センタ 120 から取得する必要がないので、ハッシュ値を作成する処理を簡単にすることができる。

[0086] また、H マトリクスそのものを送信するのではなく、H マトリクスからハッシュ関数を用いて作成したハッシュ値を送信している。ハッシュ関数は不可逆の一方関数であることから、H マトリクスが第三者に知られてしまうことも抑制できる。

[0087] 位置情報とともにハッシュ値を受信した路側機 300 は、路側機 300 自身も認証センタ 120 から H マトリクスを取得し、また、パリティデータも取得する（S74）。これら H マトリクス、パリティデータと、正規の車載機 200 が使用するものとして予め記憶しているハッシュ関数から比較ハッシュ値を作成する（S78）。この比較ハッシュ値と、車載機 200 から取得したハッシュ値とを比較することで、位置情報を送信した車載機 200 が正規車載機であるか否かを判断することができる。

[0088] （実施形態 2）

次に、実施形態 2 を説明する。なお、この実施形態 2 以下の説明において

、それまでに使用した符号と同一番号の符号を有する要素は、特に言及する場合を除き、それ以前の実施形態における同一符号の要素と同一である。また、構成の一部のみを説明している場合、構成の他の部分については先に説明した実施形態を適用することができる。

[0089] 実施形態2では、路側機300Aは、図8に示すように、衛星受信部330を備える。この衛星受信部330は本開示の取得装置側衛星受信部に相当する。また、実施形態2では、制御部320Aの処理が、実施形態1の制御部320と一部相違する。この制御部320Aの処理を図9、図10を用いて説明する。制御部320Aは、図9に示す処理を一定のGPS電波取得周期で実行し、図10に示す処理も、一定周期で実行する。

[0090] 図9は、車載機200から位置情報等を取得する前に行う事前処理である。この図9から説明する。ステップS90では、衛星受信部330が受信したGPS電波に含まれている航法メッセージを、衛星受信部330から取得する。衛星受信部330が複数のGPS衛星2からGPS電波を受信した場合、衛星受信部330が受信したすべてのGPS電波についての航法メッセージを取得する。

[0091] 本開示の電波情報抽出部に相当するステップS92では、ステップS90で取得したすべての航法メッセージから、PRNIDとTOWを抽出する。

[0092] 本開示の電波情報送信処理部に相当するステップS94では、ステップS92で抽出したPRNIDとTOWを公開キーとともに、通信部310から認証センタ120へ送信する。認証センタ120は、このPRNIDとTOWより定まるHマトリクス、パリティデータを、公開キーにより暗号化して路側機300へ送信する。

[0093] ステップS96では、認証センタ120から送信された、暗号化されたHマトリクスおよびパリティデータを、通信部310から取得する。

[0094] ステップS98では、ステップS96で取得した、暗号化されたHマトリクスおよびパリティデータを秘密キーで復号する。このステップS96は本開示のキー取得部に相当する。

- [0095] ステップS 1 0 0では、ステップS 9 8で復号したHマトリクスおよびパリティデータを入力キーとして、正規の車載機2 0 0が使用するものとして予め記憶しているハッシュ関数から比較ハッシュ値を作成する。この比較ハッシュ値は、衛星受信部3 3 0が受信したすべてのGPS電波について作成することになる。
- [0096] ステップS 1 0 2では、比較ハッシュ値テーブルを作成する。この比較ハッシュ値テーブルは、ステップS 1 0 0で作成した比較ハッシュ値と、その比較ハッシュ値の作成に用いたHマトリクス、パリティデータを取得するために認証センタ1 2 0へ送信したPRNID、TOWとの対応関係を示すテーブルである。
- [0097] 次に、図1 0を説明する。ステップS 1 1 0では、車載機2 0 0が図5のステップS 1 2を実行することにより送信する位置情報等のデータを、通信部3 1 0が受信したか否かを判断する。この判断がNoであれば図1 0の処理を終了する。一方、ステップS 1 1 0の判断がYesであればステップS 1 1 2へ進む。
- [0098] ステップS 1 1 2では、通信部3 1 0が車載機2 0 0から受信した位置情報、ハッシュ値、PRNID、TOWを取得する。
- [0099] 続いて、本開示の端末判断部に相当するステップS 1 1 4～S 1 2 0を実行する。ステップS 1 1 4では、図9の事前処理で作成した比較ハッシュ値テーブルに、ステップS 1 1 2で取得したPRNID、TOWがある場合、そのPRNID、TOWに対応する比較ハッシュ値を、今回の比較に用いる比較ハッシュ値に決定する。なお、図9の事前処理では、衛星受信部2 3 0が受信したすべてのGPS電波についての比較ハッシュ値を作成している。そのため、比較ハッシュ値テーブルには、ステップS 1 1 2で取得したPRNID、TOWに対応するハッシュ値が含まれている可能性が高い。しかし、路側機3 0 0の周辺の電波遮蔽物の位置、大きさによっては、車載機2 0 0の衛星受信部2 3 0が受信した衛星電波を、路側機3 0 0の衛星受信部3 3 0が受信できないこともある。この場合には、ステップS 1 1 2で取得し

たPRNID、TOWに対応するハッシュ値が比較ハッシュ値テーブルに含まれていない。ステップS112で取得したPRNID、TOWに対応するハッシュ値が比較ハッシュ値テーブルに含まれていない場合には、図7のステップS72～S78の処理を実行して比較ハッシュ値を作成する。

[0100] ステップS116では、ステップS112で取得したハッシュ値と、ステップS114で決定した比較ハッシュ値が一致するか否かを判断する。

[0101] 2つのハッシュ値が一致する場合、ステップS118に進み、位置情報、ハッシュ値等を送信した車載機200は正規車載機であるとする。一方、2つのハッシュ値が一致しない場合、ステップS120に進み、位置情報、ハッシュ値等を送信した車載機200は不正車載機であるとする。

[0102] 以上、説明した実施形態2によれば、路側機300は衛星受信部230を備えているので、この路側機300の周囲に存在しており、ハッシュ値を路側機300に送信する可能性がある車載機200と同じGPS衛星2から衛星電波を受信することができる。

[0103] 実施形態1では、車載機200からPRNID、TOWを受信し、そのPRNID、TOWを認証センタ120に送信してHマトリクス、パリティデータを取得していた。しかし、実施形態2では、車載機200と同じGPS衛星2から衛星電波を受信することができる。そこで、車載機200からPRNID、TOWを受信するのを待たずに、衛星受信部330が受信した航法メッセージからPRNID、TOWを抽出する。そして、抽出したPRNID、TOWを認証センタ120に送信してHマトリクス、パリティデータを取得して、比較ハッシュ値テーブルを作成する（図9）。

[0104] これにより、車載機200から位置情報等を受信した後は（S110：Yes）、予め作成しておいた比較ハッシュ値テーブルを参照して、車載機200から受信したPRNID、TOWに対応する比較ハッシュ値を決定すればよい（S112、S114）。つまり、車載機200からPRNID、TOWを受信した後に、実施形態1における図7のステップS72～S78の処理を実行しなくて済む可能性が高いので、迅速に正規車載機かどうかの判

断を行うことができる。

[0105] 特に、路側機 300 が、車載機 200 を正規車載機と認定した後に、その認定結果に基づく処理を行う場合であって、車載機 200 が走行している場合には、迅速に正規車載機かどうかの判断を行う必要性が高い。認定結果に基づく処理としては、たとえば、正規車載機であることを、車載機 200 に送信する、あるいは、正規車載機と認定したことに基づいて車両走行路に設けられたゲートを開閉するなどの処理がある。実施形態 2 は、このように、迅速に正規車載機かどうかの判断を行う必要性がある場合に、特に有用である。

[0106] 以上、本開示の実施形態を説明したが、本開示は上述の実施形態に限定されるものではなく、次の変形例も本開示の技術的範囲に含まれ、さらに、下記以外にも要旨を逸脱しない範囲内で種々変更して実施することができる。

[0107] (変形例 1、変形例 2)

たとえば、前述の実施形態では、Hマトリクスとパリティデータをハッシュ関数の入力キーとして、ハッシュ値および比較ハッシュ値を作成していた（認証済み作成部：S10、比較データ作成部：S100）。しかし、これに限られず、ハッシュ関数の入力キーをHマトリクスのみとしてハッシュ値および比較ハッシュ値を作成してもよい（変形例 1）。また、暗号キーであるHマトリクスに代えて、キー作成データであるSEED値をハッシュ関数の入力キーとしてハッシュ値および比較ハッシュ値を作成してもよい（変形例 2）。

[0108] (変形例 3)

また、SEED値からHマトリクスが作成できる。そこで、認証済み作成部、比較データ作成部は、キー関連データとしてSEED値を取得しても、そのSEED値をそのまま入力キーとせず、SEED値からHマトリクスを作成し、そのHマトリクスを入力キーとしてハッシュ値を作成してもよい。

[0109] (変形例 4)

また、認証済み作成部、比較データ作成部は、ハッシュ値を認証済みデー

タ、認証済み比較データとせず、そのハッシュ値の作成に用いたＨマトリクスやＳＥＥＤ値を認証済みデータ、認証済み比較データとしてもよい。

[0110] (変形例５)

実施形態２では、衛星受信部３３０が受信したすべてのＧＰＳ電波についての比較ハッシュ値を作成していたが、衛星受信部３３０が受信したＧＰＳ電波のうちの一部についての比較ハッシュ値を作成してもよい。たとえば、良好に受信できる予め設定された数のＧＰＳ衛星２から受信したＧＰＳ電波に限定して、比較ハッシュ値を作成してもよい。

[0111] (変形例６)

前述の実施形態では、位置情報取得装置として路側機３００、３００Ａを説明したが、これに限られない。位置情報取得装置は、有料駐車場や有料道路の不正利用を取り締まる取り締まり車両に搭載されるなど、移動型の装置であってもよい。

[0112] (変形例７)

前述の実施形態では、測位端末として車載機２００を説明したが、これに限られない。測位端末は、人に携帯される携帯型の端末や、車以外の移動体に搭載される端末であってもよい。

[0113] この出願に記載されるフローチャート、あるいは、フローチャートの処理は、複数のステップ（あるいはセクションと言及される）から構成され、各ステップは、たとえば、Ｓ２と表現される。さらに、各ステップは、複数のサブステップに分割されることができる、一方、複数のステップが合わさって一つのステップにすることも可能である。

[0114] 本実施形態において、制御部１２２内の各部は、制御部１２２の有する機能に着目して、その内部を便宜的に分類したものであり、制御部１２２の内部が、それぞれの部に対応する部分に物理的に区分されていることを意味するものではない。従って、それぞれの「部」は、コンピュータープログラムの一部分としてソフトウェア的に実現することもできるし、ＩＣチップや大規模集積回路によってハードウェア的に実現することもできる。

[0115] 以上、本開示の実施形態、構成、態様を例示したが、本開示に係わる実施形態、構成、態様は、上述した各実施形態、各構成、各態様に限定されるものではない。例えば、異なる実施形態、構成、態様にそれぞれ開示された技術的部を適宜組み合わせて得られる実施形態、構成、態様についても本開示に係わる実施形態、構成、態様の範囲に含まれる。

請求の範囲

[請求項1]

航法メッセージを受信し、受信した航法メッセージが認証できる航法メッセージである場合に、前記航法メッセージを用いて算出した現在位置を示す位置情報を外部に無線送信する測位端末（200）と、

前記測位端末（200）が認証に用いるセンタ作成認証データを送信する通信衛星（3）に、前記センタ作成認証データを送信する認証センタ装置（100）と、

前記測位端末（200）が無線送信した位置情報を受信する位置情報取得装置（300、300A）とを備えた位置情報認証システム（1）であって、

前記認証センタ装置（100）は、

航法衛星システムが備える航法衛星（2）から航法メッセージを含んでいる衛星電波を受信するセンタ側衛星受信部（110）と、

暗号キーを作成し、前記暗号キーと前記センタ側衛星受信部（110）が受信した衛星電波に含まれている航法メッセージとに基づいて、前記センタ作成認証データを作成するセンタ側認証データ作成部（122）と、

前記センタ側認証データ作成部（122）が作成したセンタ作成認証データを前記通信衛星（3）に送信する認証データ送信部（130）と、を備え、

前記測位端末（200）は、

前記通信衛星（3）から前記センタ作成認証データを受信するとともに、前記航法衛星（2）から前記衛星電波を受信する端末側衛星受信部（230）と、

前記認証センタ装置（100）から、前記暗号キーまたは前記暗号キーを作成することができるキー作成データのいずれかであるキー関連データを受信するキー受信部（211）と、

前記キー受信部（211）が受信したキー関連データと、前記端末

側衛星受信部（２３０）が受信した衛星電波から抽出した航法メッセージとに基づいて端末作成認証データを作成する端末側認証データ作成部（Ｓ５４）と、

前記センタ作成認証データと前記端末作成認証データとを比較し、一致している場合に前記端末側衛星受信部（２３０）が受信した衛星電波に含まれている航法メッセージが認証できたと判断する認証判断部（Ｓ５６～Ｓ６０）と、

前記キー受信部（２１１）が前記認証センタ装置（１００）から受信した前記キー関連データに基づいて、前記端末側衛星受信部（２３０）が受信した衛星電波に含まれている航法メッセージが認証できたことを示す認証済みデータを作成する認証済み作成部（Ｓ６～Ｓ１０）と、

前記航法メッセージに基づいて算出した前記位置情報とともに、前記認証済み作成部（Ｓ６～Ｓ１０）が作成した認証済みデータを送信する端末側送信部（２１２）とを備え、

前記位置情報取得装置（３００、３００Ａ）は、

前記端末側送信部（２１２）が送信した前記位置情報および前記認証済みデータを通信部から取得する端末データ取得部（Ｓ７０、Ｓ１１２）と、

前記通信部を介して、前記認証センタ装置（１００）から前記キー関連データを取得するキー取得部（Ｓ７４、Ｓ９６）と、

前記キー取得部（Ｓ７４、Ｓ９６）が取得したキー関連データに基づいて、前記認証済みデータと比較するための認証済み比較データを作成する比較データ作成部（Ｓ７８、Ｓ１００、Ｓ１０２）と、

前記端末データ取得部（Ｓ７０、Ｓ１１２）が取得した認証済みデータと前記比較データ作成部（Ｓ７８、Ｓ１００、Ｓ１０２）が作成した認証済み比較データとを比較し、一致している場合に、前記測位端末（２００）は正規の測位端末であると判断する端末判断部（Ｓ８

0～S 8 4、S 1 1 4～S 1 2 0) とを備える位置情報認証システム。

[請求項2]

請求項 1 において、

前記認証済み作成部 (S 6～S 1 0) は、前記キー受信部 (2 1 1) が受信した前記キー関連データを用いて、ハッシュ関数により前記認証済みデータを作成する位置情報認証システム。

[請求項3]

請求項 2 において、

前記認証済み作成部 (S 6～S 1 0) は、前記端末作成認証データを、前記キー受信部 (2 1 1) が受信した前記キー関連データとともに用いて、前記ハッシュ関数により前記認証済みデータを作成する位置情報認証システム。

[請求項4]

請求項 1～3 のいずれか 1 項において、

前記位置情報取得装置 (3 0 0 A) は、

前記航法衛星 (2) から前記衛星電波を受信する取得装置側衛星受信部 (3 3 0) と、

前記取得装置側衛星受信部が受信した衛星電波から衛星番号および時刻情報を抽出する電波情報抽出部 (S 9 2) と、

前記電波情報抽出部が抽出した衛星番号および時刻情報を周期的に前記通信部から前記認証センタへ送信させる電波情報送信処理部 (S 9 4) とを備え、

前記キー取得部 (S 9 6) は、前記通信部が前記衛星番号および時刻情報を前記認証センタに送信したことに基づいて認証センタから送信される前記キー関連データを、前記通信部から取得し、

前記比較データ作成部 (S 1 0 0、S 1 0 2) は、前記認証済み比較データを作成することに加えて、前記認証済み比較データと、前記衛星番号および時刻情報との対応関係を、前記認証済みデータを受信する前に予め決定しておき、

前記端末判断部 (S 1 1 4～S 1 2 0) は、前記端末データ取得部

(S 7 0、S 1 1 2) が取得した衛星番号および時刻情報と前記対応関係に基づいて定まる認証済み比較データがある場合に、前記認証済み比較データを、前記端末データ取得部 (S 7 0、S 1 1 2) が取得した認証済みデータと比較する位置情報認証システム。

[請求項5]

航法メッセージを受信し、受信した航法メッセージが認証できる航法メッセージである場合に、前記航法メッセージを用いて算出した現在位置を示す位置情報を外部に無線送信する測位端末 (2 0 0) であって、

認証センタ装置 (1 0 0) が作成し、前記測位端末 (2 0 0) における認証に用いるために通信衛星 (3) に送信したセンタ作成認証データを通信衛星 (3) から受信するとともに、航法衛星システムが備える航法衛星 (2) から航法メッセージを含んでいる衛星電波を受信する端末側衛星受信部 (2 3 0) と、

前記認証センタ装置 (1 0 0) から、前記センタ作成認証データを作成するための暗号キーまたは前記暗号キーを作成することができるキー作成データのいずれかであるキー関連データを受信するキー受信部 (2 1 1) と、

前記キー受信部 (2 1 1) が受信したキー関連データと、前記端末側衛星受信部 (2 3 0) が受信した衛星電波から抽出した航法メッセージとに基づいて端末作成認証データを作成する端末側認証データ作成部 (S 5 4) と、

前記センタ作成認証データと前記端末作成認証データとを比較し、一致している場合に前記端末側衛星受信部 (2 3 0) が受信した衛星電波に含まれている航法メッセージが認証できたと判断する認証判断部 (S 5 6 ~ S 6 0) と、

前記キー受信部 (2 1 1) が前記認証センタ装置 (1 0 0) から受信した前記キー関連データに基づいて、前記端末側衛星受信部 (2 3 0) が受信した衛星電波に含まれている航法メッセージが認証できた

ことを示す認証済みデータを作成する認証済み作成部（S 6 ～ S 1 0）と、

前記航法メッセージに基づいて算出した前記位置情報とともに、前記認証済み作成部（S 6 ～ S 1 0）が作成した認証済みデータを送信する端末側送信部（2 1 2）とを備える測位端末。

[請求項6]

航法メッセージを受信し、受信した航法メッセージが認証できる航法メッセージである場合に、前記航法メッセージを用いて算出した現在位置を示す位置情報および受信した航法メッセージが認証できたことを示す認証済みデータを外部に無線送信する測位端末（2 0 0）から、前記位置情報および前記認証済みデータを受信する位置情報取得装置（3 0 0、3 0 0 A）であって、

前記測位端末（2 0 0）が送信した前記位置情報および前記認証済みデータを通信部から取得する端末データ取得部（S 7 0、S 1 1 2）と、

前記通信部を介して、認証センタ装置（1 0 0）から、前記測位端末（2 0 0）が認証に用いるセンタ作成認証データを作成するために前記認証センタ装置（1 0 0）が用いた暗号キーまたは前記暗号キーを作成することができるキー作成データのいずれかであるキー関連データを取得するキー取得部（S 7 4、S 9 6）と、

前記キー取得部（S 7 4、S 9 6）が取得したキー関連データに基づいて、前記認証済みデータと比較するための認証済み比較データを作成する比較データ作成部（S 7 8、S 1 0 0、S 1 0 2）と、

前記端末データ取得部（S 7 0、S 1 1 2）が取得した認証済みデータと前記比較データ作成部（S 7 8、S 1 0 0、S 1 0 2）が作成した認証済み比較データとを比較し、一致している場合に、前記測位端末（2 0 0）は正規の測位端末であると判断する端末判断部（S 8 0 ～ S 8 4、S 1 1 4 ～ S 1 2 0）とを備える位置情報取得装置。