

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2017年6月29日(29.06.2017)



(10) 国際公開番号

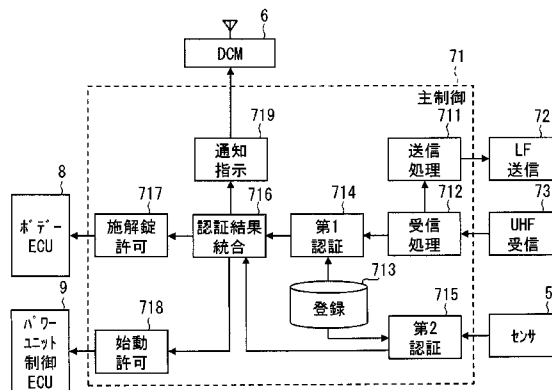
WO 2017/110207 A1

- (51) 国際特許分類:
E05B 49/00 (2006.01) B60R 25/24 (2013.01)
B60R 25/102 (2013.01) B60R 25/25 (2013.01)
- (21) 国際出願番号: PCT/JP2016/079727
- (22) 国際出願日: 2016年10月6日(06.10.2016)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2015-252252 2015年12月24日(24.12.2015) JP
- (71) 出願人: 株式会社デンソー(DENSO CORPORATION) [JP/JP]; 〒4488661 愛知県刈谷市昭和町1丁目1番地 Aichi (JP).
- (72) 発明者: 石川 竜介 (ISHIKAWA Ryusuke); 〒4488661 愛知県刈谷市昭和町1丁目1番地 株式会社デンソー内 Aichi (JP). 呉 昇錫(OH Seung-seok); 〒4488661 愛知県刈谷市昭和町1丁目1番地 株式会社デンソー内 Aichi (JP).
- (74) 代理人: 金 順姫(JIN Shunji); 〒4600003 愛知県名古屋市中区錦2丁目13番19号 瀧定ビル6階 Aichi (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

[続葉有]

(54) Title: VEHICULAR ON-BOARD DEVICE AND AUTHENTICATION SYSTEM

(54) 発明の名称: 車載装置及び認証システム



- 5 Sensor
6 Data communication module (DCM)
8 Body ECU
9 Power unit control ECU
71 Main control
72 LF transmission
73 UHF reception
711 Transmission processing
712 Reception processing
713 Record
714 First authentication
715 Second authentication
716 Authentication result integration
717 Locking and unlocking permission
718 Start permission
719 Notification instruction

(57) Abstract: Provided is a vehicular on-board device that is used in a vehicle and that comprises a first authentication unit (714) to authenticate using code verification via wireless communication with an electronic key, wherein the vehicular on-board device comprises: a second authentication unit (715) that authenticates with a method not using the code verification via wireless communication used by the first authentication unit; and a notification instruction unit (719) that notifies a personal mobile device (3) of a vehicle user that an illegal authentication using wireless communication has been performed on the vehicle when authentication with the first authentication unit 714 was successful but authentication with the second authentication unit 715 was not successful.

(57) 要約: 自車両で用いられて、電子キーとの間で無線通信を介したコード照合によって認証を行う第1認証部(714)を備える車載装置であって、第1認証部で用いる無線通信を介したコード照合以外の方法で認証を行う第2認証部(715)と、第1認証部714で認証が成立したが、第2認証部715で認証が成立しなかった場合に、無線通信を利用した不正な認証が自車に対して行われたことを自車のユーザの個人携帯機(3)へ通知させる通知指示部(719)とを備える。

WO 2017/110207 A1



OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：車載装置及び認証システム

関連出願の相互参照

[0001] 本出願は、2015年12月24日に提出された日本出願番号2015-252252号に基づくもので、ここにその記載内容を援用する。

技術分野

[0002] 本開示は、ユーザに携行される携帯機との間で無線通信を利用した認証を実施する車載装置、及びその車載装置を含む認証システムに関するものである。

背景技術

[0003] 従来、車載装置と電子キーといった携帯機との間で無線通信によるコード照合が成立したことに基づいて、車両ドアの施錠やエンジン始動等の車両制御を可能にする認証システムが知られている。この無線通信が可能となる距離範囲は、車両周辺の近距離に制限されているので、通常、無線通信を利用した認証は、携帯機が車両の近傍に位置する場合に限って可能となる。

[0004] しかしながら、このような認証システムでは、悪意を持った第三者が、中継器を用いて携帯機と車載装置との通信を間接的に実現させることで認証を成立させるリレーアタックが懸念されている。リレーアタックでは、正規のユーザが意図しないにも関わらず、認証を成立させて車両ドアの解錠やエンジン始動等の車両制御を可能にしてしまう。

[0005] これに対して、例えば、特許文献1には、車両（当該車両（subject vehicle）あるいは自車（host vehicle）とも言及される）に搭載された車載装置から送信するリクエスト信号の強度を途中で変化させ、携帯機では、この強度の変化を検出した場合に限って応答することで、リレーアタックを防止する技術が開示されている。

先行技術文献

特許文献

[0006] 特許文献1： J P 2010-185186 A

発明の概要

[0007] しかしながら、特許文献1に開示の技術では、リレーアタックを防止することが可能となったとしても、ユーザは自車に対してリレーアタックが行われたか否かを認知することはできない。自車に対してリレーアタックが行われていることをユーザが認知できない場合、ユーザは自車が盗難の標的になっていることを認知できず、自車盗難に対する防犯を強化することができない。

[0008] 本開示の目的は、無線通信を利用した不正な認証が自車に対して行われたことをユーザが認知できるようにする車載装置及び認証システムを提供することにある。

[0009] 上記目的を達成するために、本開示の一つの観点によれば、車載装置は、車両で用いられて、電子キーとして用いられる携帯機との間での無線通信を介したコード照合によって認証を行う第1認証部を備える車載装置であって、第1認証部で用いる無線通信を介したコード照合以外の方法で認証を行う第2認証部と、第1認証部で認証が成立したが、第2認証部で認証が成立しなかった場合に、無線通信を利用した不正な認証が車両に対して行われたことを車両のユーザの通信端末へ通知させる通知指示部とを備える。

[0010] また、上記目的を達成するために、本開示のもう一つの観点によれば、認証システムは、電子キーとして用いられる携帯機と、車両で用いられて、携帯機との間での無線通信を介したコード照合によって認証を行う第1認証部を備える車載装置であって、第1認証部で用いる無線通信を介したコード照合以外の方法で認証を行う第2認証部と、第1認証部で認証が成立したが、第2認証部で認証が成立しなかった場合に、無線通信を利用した不正な認証が自車に対して行われたことを自車のユーザの通信端末へ通知させる通知指示部とを備える車載装置とを含む。

[0011] 第1認証部で用いる無線通信を介したコード照合で認証が成立したが、これ以外の方法によって第2認証部で認証が成立しなかった場合には、第1認

証部での無線通信を利用した認証が不正に成立したものと言える。よって、通知指示部は、無線通信を介した不正な認証が自転車に対して行われた場合に、このことを自転車のユーザの通信端末へ通知させることができる。また、無線通信を介した不正な認証が自転車に対して行われたことを自転車のユーザの通信端末へ通知させるので、ユーザがこの通信端末から、無線通信を介した不正な認証が自転車に対して行われたことを認知することができる。

図面の簡単な説明

- [0012] 本開示についての上記目的およびその他の目的、特徴や利点は、添付の図面を参照しながら下記の詳細な記述により、より明確になる。
- [図1]第1実施形態の認証システムの概略的な構成の一例を示す図である。
- [図2]電子キーの概略的な構成の一例を示す図である。
- [図3]認証ECUの概略的な構成の一例を示す図である。
- [図4]認証ECUの主制御器の概略的な構成の一例を示す図である。
- [図5]認証ECUの主制御器での認証関連処理の流れの一例を示すフローチャートである。
- [図6]第1認証部と第2認証部との認証結果の組み合わせとそれに対応する処理との対応関係の一例を示す図である。
- [図7]第2実施形態の認証システムの概略的な構成の一例を示す図である。
- [図8]第2実施形態の認証ECUの概略的な構成の一例を示す図である。
- [図9]第2実施形態の認証ECUの主制御器での認証関連処理の流れの一例を示すフローチャートである。
- [図10]変形例の認証ECUの概略的な構成の一例を示す図である。
- [図11]他の変形例の認証ECUの概略的な構成の一例を示す図である。

発明を実施するための形態

- [0013] 図面を参照しながら、開示のための複数の実施形態や変形例を説明する。
- なお、説明の便宜上、複数の実施形態や変形例の間において、それまでの説明に用いた図に示した部分と同一の機能を有する部分については、同一の符号を付し、その説明を省略する場合がある。同一の符号を付した部分につい

ては、他の実施形態や変形例における説明を参照することができる。

[0014] (実施形態 1)

＜認証システム 1 の概略構成＞

以下、本開示の実施形態 1 について図面を用いて説明する。図 1 に示す認証システム 1 は、ユーザに携帯される電子キー 2 及び個人携帯機 3（携帯端末とも言及される）と、車両 HV で用いられるセンサ 5、DCM (Data Communication Module) 6、及び認証 ECU 7 とを含んでいる。この認証システム 1 のうち、電子キー 2 と認証 ECU 7 とを少なくとも含む構成は認証システムに相当する。車両 HV は、当該車両 (subject vehicle) あるいは自車 (host vehicle) とも言及される。

[0015] 認証システム 1 では、センサ 5 で取得するユーザの生体情報によって生体認証を行い、生体認証が成立した場合に、車両 HV のドアの解錠を許可する。また、電子キー 2 と認証 ECU 7 との間で無線通信によってコード照合を行い、無線通信を介したコード照合による認証が成立した場合であって、且つ、生体認証が成立した場合に、車両 HV のドアの施解錠に加え車両 HV の始動を許可する。電子キー 2 及び認証 ECU 7 については後に詳述する。尚、「情報」は、不可算名詞のみならず、可算名詞としても使用され、情報項目と同等である。一つの情報は一つの情報項目と、複数の情報は、複数の情報項目と同等である。

[0016] 個人携帯機 3 は、ユーザが携帯若しくは装着する通信端末であって、DCM 6 と公衆通信回線網を介して通信を行う。個人携帯機 3 の一例としては、多機能携帯電話機、ウェアラブル通信端末等があるが、実施形態 1 では、個人携帯機 3 が多機能携帯電話機である場合を例に挙げて説明を行う。

[0017] センサ 5 は、車両 HV のアウトドアハンドル 4 に設けられており、アウトドアハンドル 4 を握ったユーザから生体情報を取得する接触式の生体認証センサである。センサ 5 の一例としては、接触発光式指紋センサ、静脈認識センサ等があるが、実施形態 1 では、センサ 5 が接触発光式指紋センサであり、センサ 5 で取得する生体情報が指紋情報である場合を例に挙げて説明

を行う。

[0018] センサ5は、車両HVの運転席ドア、助手席ドア、後部座席ドア、トランクルームドアの全てのアウトドアハンドル4に設けられる構成としてもよいし、一部のアウトドアハンドル4に設けられる構成としてもよい。一部のアウトドアハンドル4に設ける場合には、例えば運転席ドアのアウトドアハンドル4に設ける構成とすればよい。

[0019] DCM6は、テレマティクスサービスに用いられる車載通信モジュールであって、公衆通信回線網を介して個人携帯機と通信を行う。

[0020] <電子キー2の概略構成>

続いて、図2を用いて、電子キー2の概略的な構成について説明を行う。図2に示すように電子キー2は、主制御器21（主制御回路とも言及される）、LF受信器22、及びUHF送信器23を備えている。この電子キー2は携帯機に相当する。

[0021] LF受信器22は、アウトドアハンドル4に設けられたLFアンテナを有しており、認証ECU7から送信されてくるLF帯のリクエスト信号をこのLFアンテナを介して受信する。また、LF受信器22は、主制御器21に接続されており、LFアンテナにて受信したリクエスト信号を主制御器21に出力する。

[0022] UHF送信器23は、UHFアンテナを有しており、UHFアンテナを介して認証ECU7へUHF帯の電波にてレスポンス信号を送信する。UHF送信器23は、主制御器21に接続されており、この主制御器21から出力されたレスポンス信号をUHFアンテナから送信する。

[0023] 主制御器21は、CPU、揮発性メモリ、不揮発性メモリ、I/O、及びこれらを接続するバスを備え、不揮発性メモリに記憶された制御プログラムを実行することで各種の処理を実行する。例えば、主制御器21は、認証ECU7から送信されるリクエスト信号に応じた応答信号を送信するなどの応答関連処理等を実行する。

[0024] 主制御器21では、電氣的に書き換え可能な不揮発性メモリに、正規のユ

ーザの車両HVを識別するための車両識別コードが登録されている。主制御器21は、LF受信器22で受信したリクエスト信号の送信元の認証ECU7を搭載した車両HVが正規のユーザの車両であるかコード照合を行う。コード照合は、認証ECU7から受信するリクエスト信号に含まれる車両識別コードと、主制御器21の不揮発性メモリに登録されている車両識別コードとの間で行う。

[0025] そして、主制御器21は、コード照合が成立した場合に、自機器を識別するための電子キー識別コードを含んだレスポンス信号を返信する。電子キー識別コードは、主制御器21の不揮発性メモリに格納しておいたものを読み出して用いる構成とすればよい。

[0026] <認証ECU7の概略構成>

続いて、図3を用いて、認証ECU7の概略的な構成について説明を行う。図3に示すように認証ECU7は、センサ5、DCM6、ボデーECU8、及びパワーユニット制御ECU9と接続されている。一例としては、車載LANによってセンサ5、DCM6、ボデーECU8、及びパワーユニット制御ECU9と認証ECU7とを接続すればよい。この認証ECU7は車載装置に相当する。

[0027] ボデーECU8は、車両HVの各車両ドアの施解錠を制御するための駆動信号を各車両ドアに設けられたドアロックモータに出力することで、各車両ドアの施解錠を行う。また、ボデーECU8には、各車両ドアのアウトードアハンドル4に設けられたタッチセンサが接続されており、各車両ドアのアウトードアハンドルがユーザに触れられたことを検出する。

[0028] パワーユニット制御ECU9は、車両HVの走行駆動源を制御する。走行駆動源としては、エンジン、モータ等がある。パワーユニット制御ECU9は、認証ECU7から走行駆動源の始動許可信号を取得すると、走行駆動源を始動できる始動待機状態とする。例えば、走行駆動源がエンジンの場合を例に挙げると、スタータモータなどが始動できる状態であるエンジン始動待機状態とする。

[0029] また、図3に示すように、認証ECU7は、主制御器71（主制御回路とも言及される）、LF送信器72、UHF受信器73を備えている。

[0030] LF送信器72は、各車両ドアのドアアンテナ10といったLFアンテナを介し、電子キー2にLF帯の電波にてリクエスト信号を送信する。LF帯とは、例えば30kHz～300kHzの周波数帯である。LFアンテナからLF帯の電波で信号を送信できる範囲が、近距離無線通信が可能な近距離無線通信エリアにあたる。リクエスト信号は、コード照合のための電子キー識別コードの送信を要求する信号であって、車両HVを識別するための車両識別コードを含んでいる。ドアアンテナ10は、車両HVの車両ドアのドアハンドルに設けられる。

[0031] LF送信器72は、車室内に設けられた室内アンテナを介して、車室内にもLF帯の電波にてリクエスト信号を送信する構成としてもよい。しかしながら、便宜上、実施形態1では、ドアアンテナ10を介して車室外にリクエスト信号を送信する場合に限って説明を行う。

[0032] UHF受信器73は、UHFアンテナ11を有しており、UHF帯の電波にて電子キー2から送信されてくるレスポンス信号をUHFアンテナ11で受信する。UHF帯とは、例えば300MHz～3GHzの周波数帯である。また、レスポンス信号とは、認証ECU7から送信するリクエスト信号に対して電子キー2から返信される信号である。

[0033] 主制御器71は、揮発性メモリ、不揮発性メモリ、I/O、及びこれらを接続するバスを備え、不揮発性メモリに記憶された制御プログラムを実行することで各種の処理を実行する。主制御器71は、認証に関連する処理（以下、認証関連処理）を実行する。主制御部71については後に詳述する。なお、主制御器71が実行する機能の一部又は全部を、一つ或いは複数のIC等によりハードウェア的に構成してもよい。

[0034] ＜主制御器71の詳細構成＞

図4に示すように、主制御器71は、送信処理部711、受信処理部712、登録器713、第1認証部714、第2認証部715、認証結果統合部

716、施解錠許可部717、始動許可部718、及び通知指示部719を備えている。

[0035] 送信処理部711は、LF送信器72を介してドアアンテナ10から、車両HVの車両識別コードを含むリクエスト信号を送信させる。一例としてリクエスト信号の送信は、車両HVの駐車中に間欠的に行われるものとする。車両識別コードは、車両HVに搭載された認証ECU7の機器IDであってもよい、車両HVの車両IDであってもよい。車両識別コードは、認証ECU7の不揮発性メモリに格納しておいたものを読み出して用いる構成とすればよい。受信処理部712は、リクエスト信号に応答してUHF帯の電波にて電子キー2から送信されてくるレスポンス信号を、UHF受信器73を介して受信する。

[0036] 登録器713は、例えば電氣的に書き換え可能な不揮発性メモリであって、電子キー識別コードのうち、正規のユーザの電子キー2の電子キー識別コードが登録されている。また、正規のユーザの生体情報も登録されている。実施形態1の例では、正規のユーザからセンサ5で取得した指紋情報（以下、正規の指紋情報）が登録されている。

[0037] 第1認証部714は、受信処理部712で受信したレスポンス信号の送信元の電子キー2が正規のユーザの電子キー2であるかコード照合を行う。コード照合は、電子キー2から受信したレスポンス信号に含まれる電子キー識別コードと、登録器713に登録されている電子キー識別コードとの間で行う。そして、両者が一致した場合に、無線通信を介したコード照合による認証が成立したものとする。両者が一致しなかった場合には、認証は不成立となる。

[0038] 第2認証部715は、センサ5で取得した指紋情報が、正規の指紋情報と一致するか照合する指紋認証を行う。指紋認証は、センサ5で取得した指紋情報と、登録器713に登録されている正規の指紋情報との間で行う。そして、両者が一致した場合に、指紋認証が成立したものとする。両者が一致しなかった場合には、認証は不成立となる。

- [0039] 認証結果統合部 716 は、第 1 認証部 714 での認証結果と第 2 認証部 715 での認証結果とを統合して、施解錠許可部 717、始動許可部 718、通知指示部 719 に出力する。
- [0040] 施解錠許可部 717 は、第 1 認証部 714 と第 2 認証部 715 とのいずれか一方でも認証成立であった場合に、車両ドアの施解錠を許可する信号をボデー ECU 8 に送る。この施解錠許可部 717 は解錠許可部に相当する。車両ドアの施解錠が許可された場合、ボデー ECU 8 は、車両ドアのアウトードアハンドル 4 に設けられたタッチセンサへの通電を開始させ、ユーザによるアウトードアハンドル操作を検出可能なスタンバイ状態となる。そして、ユーザがこのタッチセンサに触れたことをボデー ECU 8 で検出した場合に、ボデー ECU 8 が駆動信号をドアロックモータに出力し、車両ドアの施解錠を行う。
- [0041] センサ 5 を車両 H V の各車両ドアに設ける構成とした場合には、施解錠許可部 717 で施解錠を行う車両ドアは、アウトードアハンドル操作を検出した車両ドアに限る構成とすればよい。これによれば、ユーザがアウトードアハンドル 4 に触れた車両ドアに限って施解錠を行うことが可能になる。
- [0042] センサ 5 を車両 H V の運転席の車両ドアに限って設ける構成とした場合には、施解錠許可部 717 で施解錠を行う車両ドアは、車両 H V の全ての車両ドアとする構成とすればよい。運転席の車両ドアのアウトードアハンドル 4 に触れることで車両 H V の全車両ドアの施解錠を行うのは、既存の電子キーシステムの機能と同様であるので、ユーザにとっては馴染みがあり利便性が良い。よって、以上の構成によれば、ユーザにとっての利便性を良好に保ちながら、センサ 5 を車両 H V に設ける数を減らしてコストダウンすることが可能になる。
- [0043] なお、ここでは、施解錠許可部 717 が施解錠の両方を行う構成を示したが、必ずしもこれに限らない。例えば、施錠のみや解錠のみを行う構成としてもよい。
- [0044] 始動許可部 718 は、第 1 認証部 714 と第 2 認証部 715 との両方で認

証成立であった場合に、走行駆動源の始動許可信号をパワーユニット制御ECU9に送る。始動許可信号を取得したパワーユニット制御ECU9は、前述したようにして、走行駆動源を始動待機状態とする。これら施錠許可部717及び始動許可部718は許可部に相当する。

[0045] 通知指示部719は、第1認証部714で認証成立であったが、第2認証部715で認証不成立であった場合に、無線通信を利用した不正な認証が自転車に対して行われたことを、DCM6から個人携帯機3へ通知させる。

[0046] <主制御器71での認証関連処理>

ここで、図5のフローチャートを用いて、認証ECU7の主制御器71での認証関連処理の流れの一例について説明を行う。図5のフローチャートは、車両HVの車両ドアが施錠されたときに開始される。

[0047] 記載されるフローチャートは、複数のセクション（あるいはステップと言及される）を含み、各セクションは、たとえば、S1と表現される。さらに、各セクションは、複数のサブセクションに分割されることができる、一方、複数のセクションが合わさって一つのセクションにすることも可能である。各セクションは、デバイス、あるいは、固有名として、また、構造的な修飾語を伴って、例えば、認証セクションは、認証デバイス、認証器として、言及されることができる。また、セクションは、(i)ハードウェアユニット（例えば、コンピュータ）と組み合わせたソフトウェアのセクションのみならず、(ii)ハードウェア（例えば、集積回路、配線論理回路）のセクションとして、関連する装置の機能を含みあるいは含まずに実現できる。さらに、ハードウェアのセクションは、マイクロコンピュータの内部に含まれることもできる。

[0048] まず、S1では、第2認証部715が、センサ5を介して指紋情報を取得した場合（S1でYES）には、S2に移る。一方、指紋情報を取得していない場合（S1でNO）には、S1の処理を繰り返す。S2では、第2認証部715が、センサ5を介して取得した指紋情報が、正規の指紋情報と一致するか照合する指紋認証を行う。

- [0049] S 3では、送信処理部 7 1 1 が、L F 送信器 7 2 を介してドアアンテナ 1 0 から、車両識別コードを含むリクエスト信号を送信させる。S 4では、受信処理部 7 1 2 が、電子キー 2 からリクエスト信号に応答して送信されてくるレスポンス信号を、U H F 受信器 7 3 を介して受信できた場合（S 4でY E S）には、S 5に移る。一方、受信できなかった場合（S 4でN O）には、S 1 0に移る。
- [0050] S 4の処理では、ドアアンテナ 1 0の通信範囲内に電子キー 2が存在しない場合、若しくは電子キー 2で車両識別コードのコード照合が不成立であった場合に、電子キー 2からのレスポンス信号を受信できなくなる。
- [0051] 受信処理部 7 1 2でのレスポンス信号を受信できたか否かの判断は、リクエスト信号を送信してから所定時間内にレスポンスを受信したか否かによって行う構成とすればよい。所定時間は、リクエスト信号をした電子キー 2がレスポンス信号を送信するまでの時間よりも長い時間であって、任意に設定可能な時間である。また、1 0 0 m s e c ごと等の周期的に複数回リクエスト信号を送信したにも関わらず、レスポンス信号の受信をしなかった場合に、レスポンス信号を受信できなかったと受信処理部 7 1 2で判断する構成としてもよい。
- [0052] S 5では、第 1 認証部 7 1 4 が、受信処理部 7 1 2で受信したレスポンス信号に含まれる電子キー識別コードと、登録器 7 1 3に登録されている電子キー識別コードとのコード照合による認証を行う。
- [0053] S 6では、第 1 認証部 7 1 4でのコード照合による認証が成立した場合（S 6でY E S）には、S 7に移る。一方、コード照合による認証が不成立であった場合（S 6でN O）には、S 1 0に移る。
- [0054] S 7では、S 2において第 2 認証部 7 1 5での指紋認証が成立していた場合（S 7でY E S）には、S 8に移る。一方、指紋認証が不成立であった場合（S 7でN O）には、S 9に移る。
- [0055] S 8では、施解錠許可部 7 1 7が車両H Vの解錠を許可するとともに、始動許可部 7 1 8が車両H Vの始動を許可し、認証関連処理を終了する。S 9

では、リレーアタックといった不正な認証が自車に行われたものとし、施解錠許可部 7 1 7 が車両 H V の解錠を許可しないとともに、始動許可部 7 1 8 が車両 H V の始動を許可しない。また、通知指示部 7 1 9 が、無線通信を利用した不正な認証が自車に対して行われたことを、D C M 6 から個人携帯機 3 へ通知させる。そして、認証関連処理を終了する。

[0056] 通知を受けた個人携帯機 3 では、無線通信を利用した不正な認証が自車に対して行われたことを示す表示及び／又は音声出力を行うことで、無線通信を利用した不正な認証が自車に対して行われたことをユーザに認知させる。通知の一例としては、表示であれば、テキスト表示であってもよいし、アイコン表示であってもよい。音声出力であれば、テキストの読み上げであってもよいし、ブザー音の出力であってもよい。

[0057] S 4 でレスポンス信号を受信できなかった場合、若しくは S 6 でコード照合による認証が不成立であった場合の S 1 0 では、S 2 において第 2 認証部 7 1 5 での指紋認証が成立していた場合（S 1 0 で Y E S）には、S 1 1 に移る。一方、指紋認証が不成立であった場合（S 1 0 で N O）には、S 1 2 に移る。

[0058] S 1 1 では、施解錠許可部 7 1 7 が車両 H V の解錠を許可する一方、始動許可部 7 1 8 は車両 H V の始動を許可せず、認証関連処理を終了する。S 1 2 では、施解錠許可部 7 1 7 が車両 H V の解錠を許可しないとともに、始動許可部 7 1 8 が車両 H V の始動を許可せず、認証関連処理を終了する。

[0059] ここで、図 6 を用いて、第 1 認証部 7 1 4 での無線通信によるコード照合と第 2 認証部 7 1 5 での指紋認証との認証結果の組み合わせとそれに対応する処理との対応関係の一例をまとめる。

[0060] 図 6 に示すように、無線通信によるコード照合と指紋認証とのいずれも成立の場合には、車両 H V の解錠と始動とのいずれも許可される。無線通信によるコード照合が成立したが、指紋認証が不成立の場合には、車両 H V の解錠と始動とのいずれも不許可となるだけでなく、無線通信を利用した不正な認証が自車に対して行われたことが個人携帯機 3 へ通知される。無線通信に

よるコード照合は不成立だが、指紋認証が成立した場合には、車両HVの始動は許可しないが、解錠は許可される。無線通信によるコード照合と指紋認証とのいずれも不成立の場合には、車両HVの解錠と始動とのいずれも不許可となる。

[0061] <実施形態1のまとめ>

第1認証部714での無線通信を介したコード照合で認証が成立したが、第2認証部715での指紋認証が成立しなかった場合には、第1認証部714での無線通信を利用した認証がリレーアタック等によって不正に成立したものと推定できる。これに対して、実施形態1の構成によれば、第1認証部714での無線通信を介したコード照合で認証が成立したが、第2認証部715での指紋認証が成立しなかった場合には、無線通信を介した不正な認証が自転車に対して行われたことを個人携帯機3へ通知させる。よって、ユーザがこの個人携帯機3から、無線通信を介した不正な認証が自転車に対して行われたことを認知することができる。従って、ユーザは車両HVが盗難の標的になっていることを認知でき、例えば車両HVの車輪に盗難防止用のロックをかける等、車両盗難に対する防犯を強化することができる。

[0062] また、実施形態1の構成によれば、第1認証部714での無線通信を介したコード照合で認証が成立しなかったが、第2認証部715での指紋認証が成立した場合には、車両HVの始動は許可しないものの解錠は許可する。これによれば、正規のユーザが車両HVの始動は必要とせず、荷物の積み下ろしを行う場合に、電子キー2を持たなくても車両HVの解錠を行うことが可能になり、利便性が向上する。

[0063] さらに、実施形態1の構成によれば、第1認証部714での無線通信を介したコード照合での認証と、第2認証部715での指紋認証との両方が成立しないと車両HVの始動を許可しないので、2重の認証によって盗難防止の効果が高まる。

[0064] また、センサ5が車両HVのアウトードアハンドル4に設けられているため、ユーザが乗車時の動作を行うだけで第2認証部715での指紋認証を行

うことができる。よって、第2認証部715での認証のための余分な動作をユーザに強いる必要がなく、利便性を損なわない。

[0065] (実施形態2)

実施形態1では、センサ5をアウトドアハンドル4に設ける構成を示したが、必ずしもこれに限らない。例えば、センサ5をスタートストップボタン12に設ける構成（以下、実施形態2）としてもよい。

[0066] <認証システム1a, 認証ECU7a, 主制御器71aの概略構成>

実施形態2の認証システム1aは、図7に示すように、センサ5をアウトドアハンドル4に設ける代わりにスタートストップボタン12に設ける点と、認証ECU7の代わりに認証ECU7aを含む点を除けば、実施形態1の認証システム1と同様である。認証ECU7aは、図8に示すように、主制御器71の代わりに主制御器71a（主制御回路とも言及される）を備える点を除けば、実施形態1の認証ECU7と同様である。

[0067] 主制御器71aは、認証関連処理の処理手順が異なる点を除けば、実施形態1の主制御器71と同様である。主制御器71aは、主制御器71と同様に、送信処理部711、受信処理部712、登録器713、第1認証部714、第2認証部715、認証結果統合部716、施解錠許可部717、始動許可部718、及び通知指示部719を備えている。

[0068] スタートストップボタン12は、車両HVの走行駆動源を始動させるためにユーザが操作するボタンであって、車室内に設けられている。このスタートストップボタン12は始動用入力部に相当する。実施形態2では、センサ5は、スタートストップボタン12を操作したユーザから生体情報を取得する。実施形態2でも、センサ5が接触発光式指紋センサであり、センサ5で取得する生体情報が指紋情報である場合を例に挙げて説明を行う。

[0069] 実施形態2におけるLF送信器72は、近距離無線通信エリアが車両HVの運転席を含むものとする。なお、実施形態2において、センサ5をスタートストップボタン12に設ける理由は、センサ5を車両HVの全車両ドアに設ける構成に比べて、必要となるセンサ5の数を減らすことができるため

ある。

[0070] <主制御器 7 1 a での認証関連処理>

ここで、図 9 のフローチャートを用いて、認証 ECU 7 a の主制御器 7 1 a での認証関連処理の流れの一例について説明を行う。図 9 のフローチャートは、車両 H V の運転席の車両ドアが解錠されて車両ドアが開けられた後、スタートストップボタン 1 2 が操作されたときに開始される。例えば、解錠については第 1 認証部 7 1 4 での無線通信によるコード照合が成立した場合に許可すればよい。

[0071] まず、S 2 1 では、S 3 と同様にして、送信処理部 7 1 1 が、車両識別コードを含むリクエスト信号を送信させる。S 2 2 では、S 4 と同様にして、受信処理部 7 1 2 が、レスポンス信号を受信できた場合（S 2 2 で Y E S）には、S 2 3 に移る。一方、受信できなかった場合（S 2 2 で N O）には、S 3 3 に移る。

[0072] S 2 3 では、S 5 と同様にして、第 1 認証部 7 1 4 がコード照合による認証を行う。S 2 4 では、第 1 認証部 7 1 4 でのコード照合による認証が成立した場合（S 2 4 で Y E S）には、S 2 5 に移る。一方、コード照合による認証が不成立であった場合（S 2 4 で N O）には、S 3 3 に移る。

[0073] なお、第 1 認証部 7 1 4 での無線通信によるコード照合によって解錠を許可する構成とした場合には、S 2 1 ～ S 2 4，及び後述の S 3 3 の処理を省略してもよい。

[0074] S 2 5 では、主制御器 7 1 a が、車両 H V の電源転移を可能にし、S 2 6 に移る。ここで言うところの電源転移とは、車両 H V の電源オフから、アクセサリ（つまり、A C C）電源オン、イグニッション（つまり、I G N）オンまでの電源転移であって、車両 H V の始動の許可は除くものとする。

[0075] S 2 6 では、第 2 認証部 7 1 5 が、センサ 5 を介して指紋情報を取得した場合（S 2 6 で Y E S）には、S 2 7 に移る。一方、指紋情報を取得していない場合（S 2 6 で N O）には、S 3 1 に移る。S 2 7 では、S 2 と同様にして、第 2 認証部 7 1 5 が指紋認証を行う。

- [0076] S 2 8では、第2認証部7 1 5での指紋認証が成立した場合（S 2 8でY E S）には、S 2 9に移る。一方、指紋認証が不成立であった場合（S 2 8でN O）には、S 3 0に移る。
- [0077] S 2 9では、始動許可部7 1 8が車両HVの始動を許可し、認証関連処理を終了する。S 3 0では、リレーアタックといった不正な認証が自車に行われたものとし、始動許可部7 1 8が車両HVの始動を許可しないとともに、通知指示部7 1 9が、無線通信を利用した不正な認証が自車に対して行われたことを、DCM 6から個人携帯機3へ通知させる。そして、認証関連処理を終了する。
- [0078] S 2 6で指紋情報を取得していない場合のS 3 1では、始動許可部7 1 8が車両HVの始動を許可せずに、S 3 2に移る。S 3 2では、認証関連処理の終了タイミングであった場合（S 3 2でY E S）には、認証関連処理を終了する。一方、認証関連処理の終了タイミングでなかった場合（S 3 2でN O）には、S 2 6に戻って処理を繰り返す。ここでの認証関連処理の終了タイミングとは、車両HVからユーザが降車したとき等が挙げられる。車両HVからユーザが降車したことは、車両HVの着座センサでの検出結果、車両HVの室内アンテナから送信するリクエスト信号に対する電子キー2の応答の有無等から主制御器7 1 aが判断すればよい。
- [0079] S 2 2でレスポンス信号を受信できなかった場合、若しくはS 2 4でコード照合による認証が不成立であった場合のS 3 3では、始動許可部7 1 8が車両HVの始動を許可せず、認証関連処理を終了する。
- [0080] 実施形態2では、実施形態1のセンサ5をアウトドアハンドル4に設けるという構成に代えて、センサ5を車室内のスタートストップボタン1 2に設けるという構成を採用している。このような構成を採用した場合であっても、電子キー2を持たなくても車両HVの解錠を行うことが可能になる点の効果を除けば、実施形態1と同様の効果を得ることができる。
- [0081] また、センサ5が車両HVのスタートストップボタン1 2に設けられているため、ユーザが始動時の動作を行うだけで第2認証部7 1 5での指紋認証

を行うことができる。よって、第2認証部715での認証のための余分な動作をユーザに強いる必要がなく、利便性を損なわない。

[0082] (変形例1)

センサ5として接触式の生体認証センサを用いる場合には、ユーザが車両HVへの乗車時若しくは始動時に触れる部材であれば、アウトドアハンドル4及びスタートストップボタン12以外の部材にセンサ5が設けられる構成としてもよい。

[0083] (変形例2)

センサ5として接触式の生体認証センサを用いる構成に必ずしも限らない。例えば、非接触式の生体認証センサを用いる構成としてもよい。一例としては、非接触式の指紋センサ、静脈認識センサを用いる構成とすればよい。他にも、ユーザを撮像した撮像画像から個人認証を行う装置で用いられる撮像装置をセンサ5として用いる構成としてもよい。

[0084] (変形例3)

第2認証部715で行う認証は、第1認証部714で用いる無線通信を介したコード照合以外の方法による認証であれば、必ずしも生体認証でなくてもよい。例えば、個人携帯機3との間での無線通信を介した認証であってもよい。一例を述べると、無線通信規格としてBluetooth（登録商標）を用いる場合には、ペアリング時に用いるPINコードの照合によって第2認証部715が認証を行う構成とすればよい。第2認証部715で個人携帯機3との間での無線通信を介した認証を行う場合には、個人携帯機3と主制御器71との間での通信を仲介するための通信部を認証ECU7がさらに備える構成とすればよい。

[0085] 第2認証部715で行う認証が生体認証でなくても、第1認証部714で用いる無線通信を介したコード照合以外の方法による認証であれば、実施形態1と同様の効果を得ることができる。

[0086] (変形例4)

また、通知指示部719からDCM6を介して通知を受けた個人携帯機3

が行う、無線通信を利用した不正な認証が自転車に対して行われたことを示す表示及び／又は音声出力は、通知の直後であってもよいし、直後でなくてもよい。直後でない場合の構成としては、個人携帯機 3 で通知を受けたことを記録しておき、ユーザが任意のタイミングで通知の内容を確認する構成等がある。

[0087] (変形例 5)

実施形態 1、実施形態 2 では、通信端末として多機能携帯電話機といった個人携帯機 3 を用いる構成を示したが、必ずしもユーザが携帯若しくは装着する通信端末に限らない。例えば、通信端末としてユーザの自宅にある PC、ホームセキュリティ端末等を用いる構成としてもよい。

[0088] (変形例 6)

実施形態 1、2 では、無線通信を利用した不正な認証が自転車に対して行われたことを、通知指示部 719 が DCM 6 から個人携帯機 3 へ通知させる構成を示したが、必ずしもこれに限らない。例えば、ユーザの車両 HV への乗車時に、無線通信を利用した不正な認証が自転車に対して行われたことを、通知指示部 719b が自転車に搭載された表示装置 13 に通知して表示させる構成（以下、変形例 6）としてもよい。

[0089] 以下、本開示の変形例 6 について図面を用いて説明する。変形例 6 の認証 ECU 7b は、図 10 に示すように、通知指示部 719 の代わりに通知指示部 719b を備える点、及び DCM 6 を介して携帯機 3 に通知を行う代わりに表示装置 13 に通知を行う点を除けば、実施形態 1 の認証 ECU 7 と同様である。

[0090] 表示装置 13 は、車両 HV に搭載される表示装置である。表示装置 13 としては、例えばコンビネーションメータ、CID (Center Information Display)、HUD (Head-Up Display) 等がある。

[0091] 通知指示部 719b は、第 1 認証部 714 で認証成立であったが、第 2 認証部 715 で認証不成立であった場合に、無線通信を利用した不正な認証が自転車に対して行われたことを、ユーザの車両 HV の乗車時に、表示装置 13

へ通知する。通知を受けた表示装置 13 は、無線通信を利用した不正な認証が自転車に対して行われたことを表示装置 13 に表示させる。

[0092] ユーザの車両HVの乗車時は、ボデーECU8から得られる車両ドア開閉の信号、着座センサの信号等から通知指示部719bが判断する構成とすればよい。

[0093] 変形例6の構成によれば、無線通信を介した不正な認証が自転車に対して行われたことを、車両HVへの乗車時にユーザが認知することができる。なお、変形例6において、通知指示部719bがDCM6から個人携帯機3への通知も行う構成としてもよい。

[0094] (変形例7)

実施形態1, 2では、車両ドアの施解錠を行うボデーECU8が認証ECU7, 7aと別個に設けられている構成を示したが、必ずしもこれに限らない。例えば、車両ドアの施解錠を行うボデーECU8が認証ECU7, 7aと統合されている構成（以下、変形例7）としてもよい。

[0095] 以下、本開示の変形例7について図面を用いて説明する。変形例7の認証ECU7cは、図11に示すように、施解錠操作部720を備える点を除けば、実施形態1の認証ECU7と同様である。

[0096] 施解錠操作部720は、実施形態1で説明したボデーECU8と同様の処理を行うことで、駆動信号をドアロックモータ14に出力し、車両ドアの施解錠を行う。この施解錠操作部720は解錠操作部に相当する。

[0097] 本開示は、実施例に準拠して記述されたが、本開示は当該実施例や構造に限定されるものではないと理解される。本開示は、様々な変形例や均等範囲内の変形をも包含する。加えて、様々な組み合わせや形態、さらには、それらに一要素のみ、それ以上、あるいはそれ以下、を含む他の組み合わせや形態をも、本開示の範疇や思想範囲に入るものである。

請求の範囲

[請求項1]

車両で用いられて、

電子キーとして用いられる携帯機（２）との間での無線通信を介したコード照合によって認証を行う第１認証部（７１４）を備える車載装置であって、

前記第１認証部で用いる無線通信を介したコード照合以外の方法で認証を行う第２認証部（７１５）と、

前記第１認証部で認証が成立したが、前記第２認証部で認証が成立しなかった場合に、無線通信を利用した不正な認証が前記車両に対して行われたことを前記車両のユーザの通信端末（３）へ通知させる通知指示部（７１９、７１９ｂ）とを備える車載装置。

[請求項2]

請求項１において、

前記車両の始動を許可する始動許可部（７１８）をさらに備え、

前記始動許可部は、前記第１認証部と前記第２認証部との両方で認証が成立しないと前記車両の始動を許可しない車載装置。

[請求項3]

請求項２において、

前記車両のドアの解錠を許可する解錠許可部（７１７）をさらに備え、

前記解錠許可部は、前記第２認証部で認証が成立すれば前記車両のドアの解錠を許可する車載装置。

[請求項4]

請求項３において、

前記車両のドアの解錠を行わせる解錠操作部（７２０）をさらに備える車載装置。

[請求項5]

請求項１～４のいずれか１項において、

前記第２認証部は、生体認証によって認証を行う車載装置。

[請求項6]

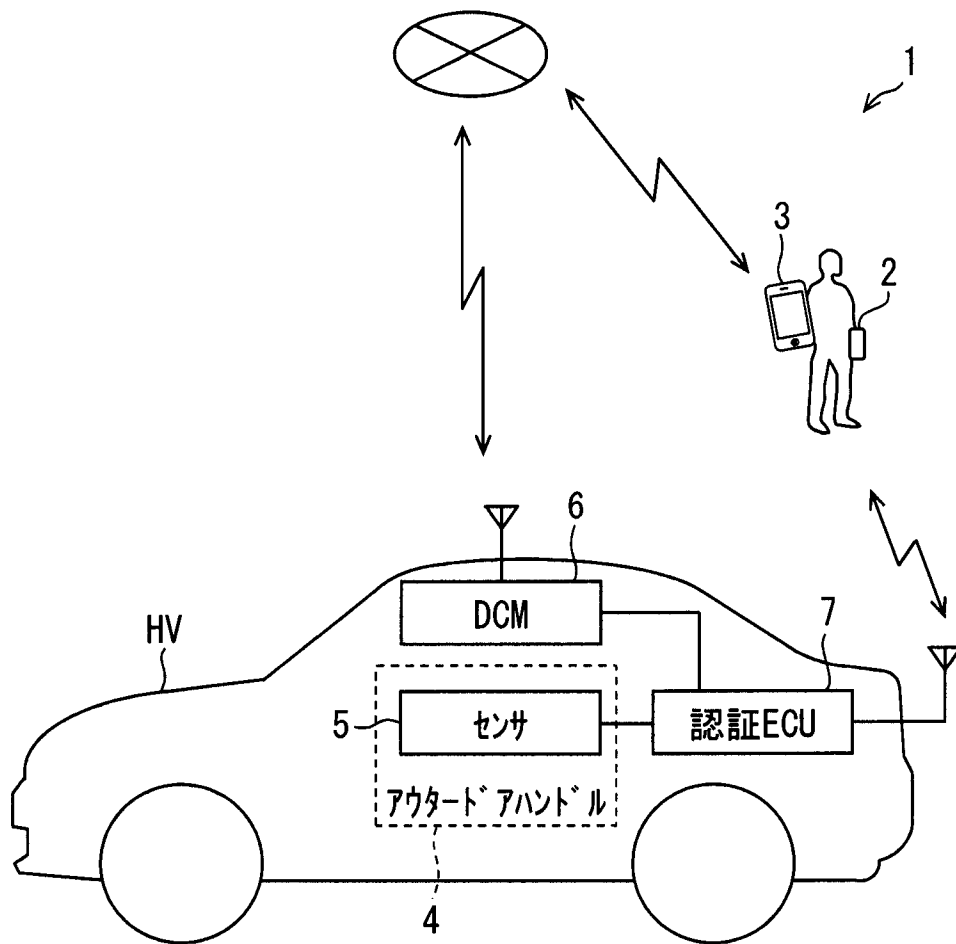
請求項５において、

前記第２認証部は、ユーザが接触するセンサ（５）で取得したこのユーザの生体情報を用いて生体認証を行う車載装置。

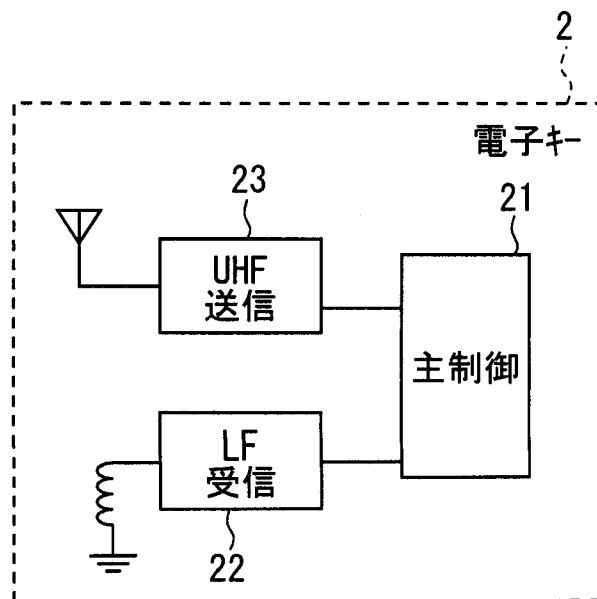
- [請求項7] 請求項6において、
前記第2認証部は、前記車両のアウトドアハンドル（4）に設けられた前記センサで取得したユーザの生体情報を用いて生体認証を行う車載装置。
- [請求項8] 請求項6において、
前記第2認証部は、前記車両の走行駆動源を始動させるためにユーザが操作する始動用入力部（12）に設けられた前記センサで取得したユーザの生体情報を用いて生体認証を行う車載装置。
- [請求項9] 請求項1～8のいずれか1項において、
前記通知指示部は、無線通信を利用した不正な認証が前記車両に対して行われたことを、前記車両のユーザに携帯若しくは装着される前記通信端末へ通知させる車載装置。
- [請求項10] 請求項1～9のいずれか1項において、
前記通知指示部（719）は、無線通信を利用した不正な認証が前記車両に対して行われたことを、テレマティクスサービスに用いる車載通信モジュール（6）を介して、前記車両のユーザの通信端末へ通知させる車載装置。
- [請求項11] 請求項1～9のいずれか1項において、
前記通知指示部（719b）は、無線通信を利用した不正な認証が前記車両に対して行われたことを、前記車両のユーザの前記車両への乗車時に、前記車両に搭載された表示装置（13）に表示させる車載装置。
- [請求項12] 電子キーとして用いられる携帯機（2）と、
車両で用いられて、前記携帯機との間での無線通信を介したコード照合によって認証を行う第1認証部（714）を備える車載装置であって、
前記第1認証部で用いる無線通信を介したコード照合以外の方法で認証を行う第2認証部（715）と、

前記第 1 認証部で認証が成立したが、前記第 2 認証部で認証が成立しなかった場合に、無線通信を利用した不正な認証が前記車両に対して行われたことを前記車両のユーザの通信端末（3）へ通知させる通知指示部（7 1 9，7 1 9 b）とを備える車載装置（7，7 a，7 b，7 c）とを含む認証システム。

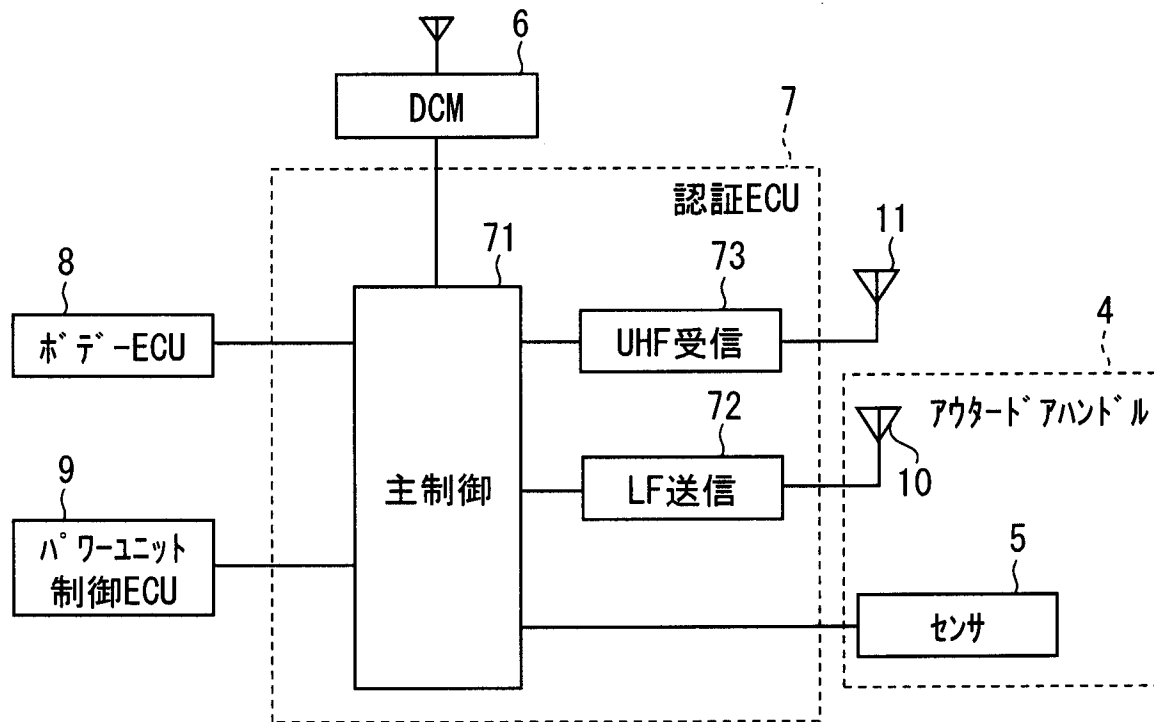
[図1]



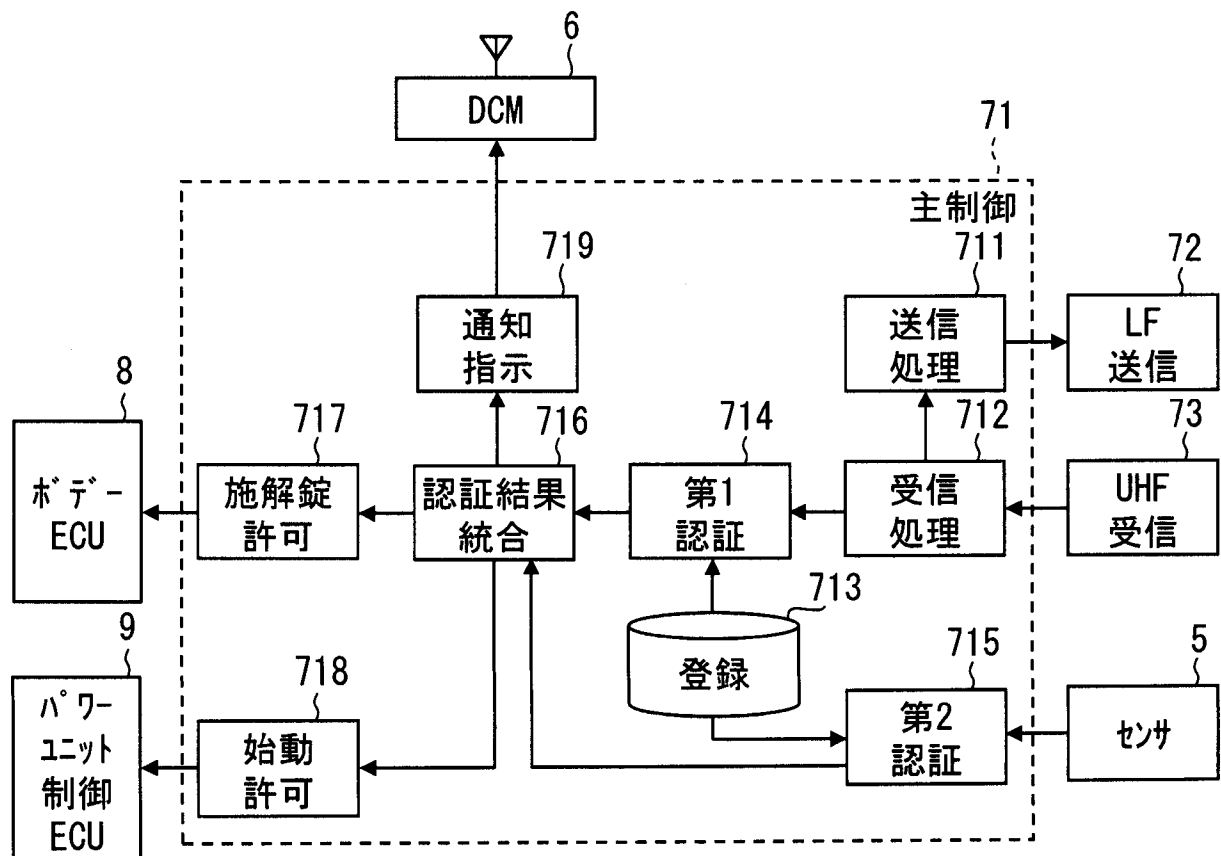
[図2]



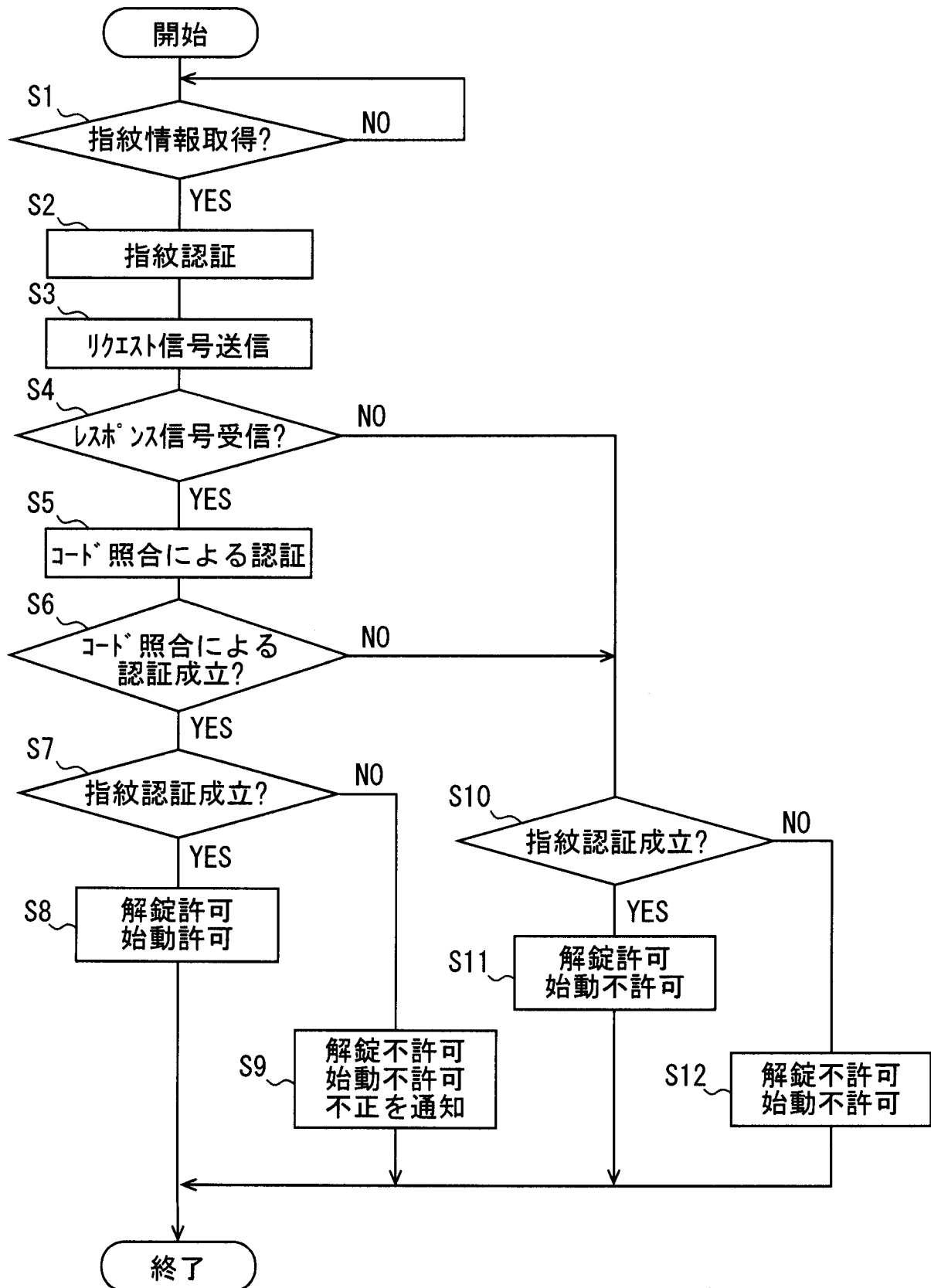
[図3]



[図4]



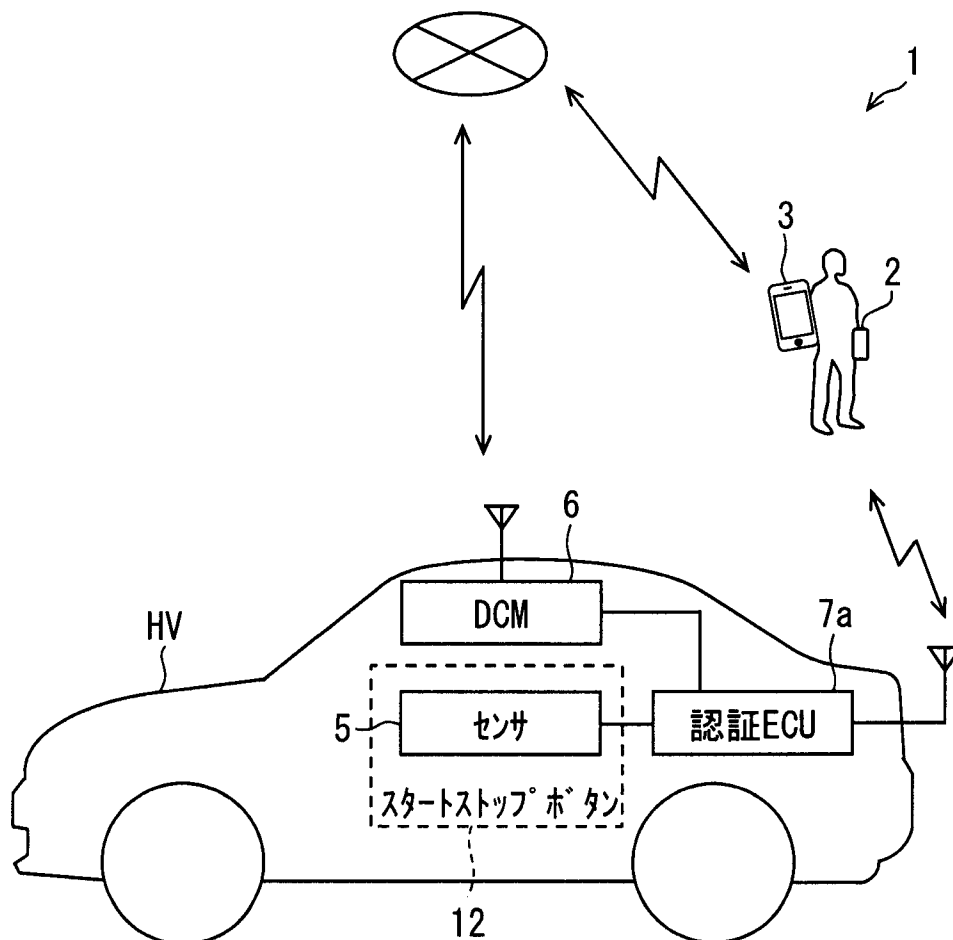
[図5]



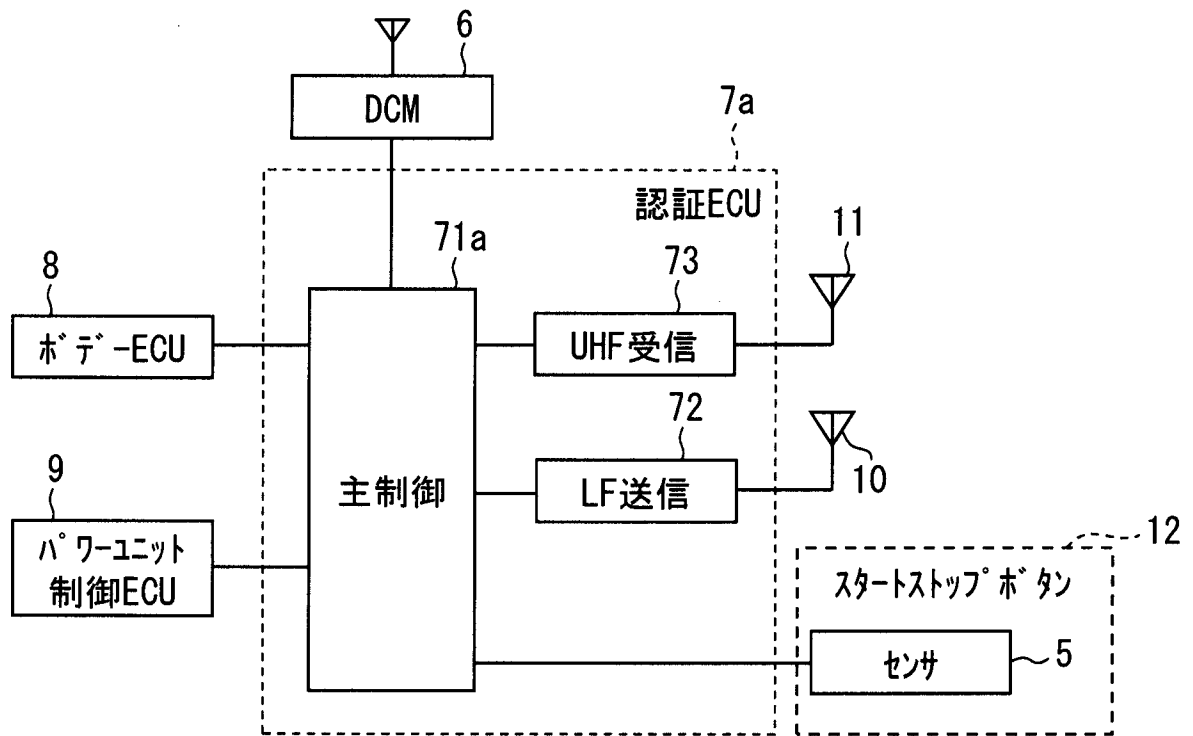
[図6]

無線通信による コード照合	指紋認証	処理
成立	成立	解錠許可, 始動許可
成立	不成立	解錠不許可, 始動不許可, 不正を通知
不成立	成立	解錠許可, 始動不許可
不成立	不成立	解錠不許可, 始動不許可

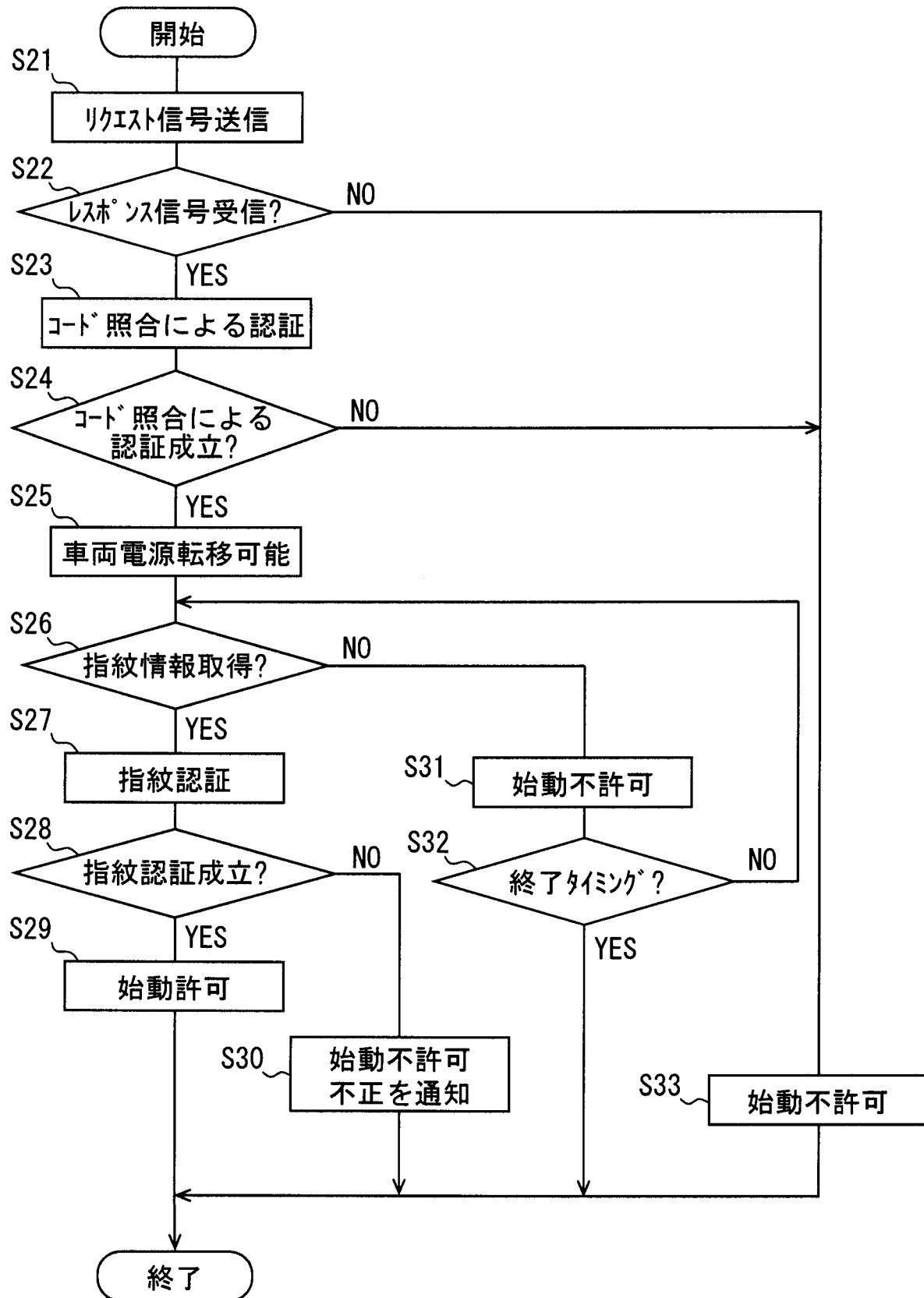
[図7]



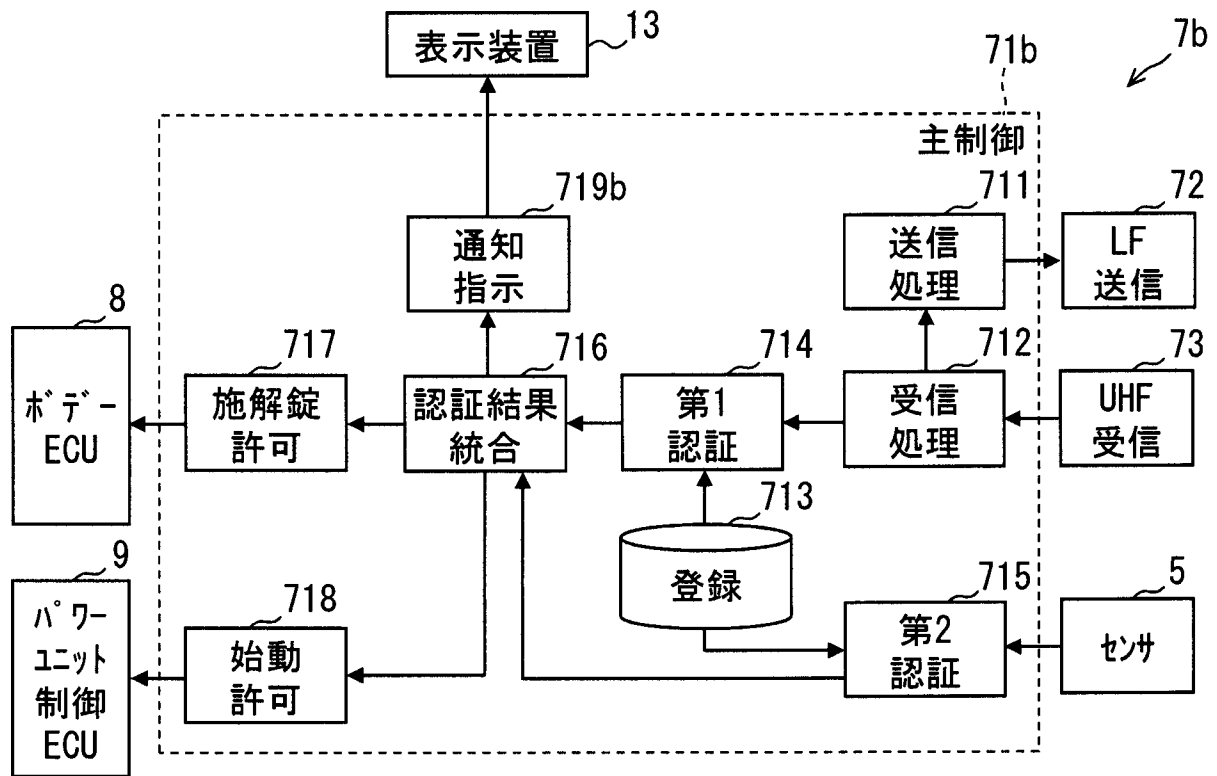
[図8]



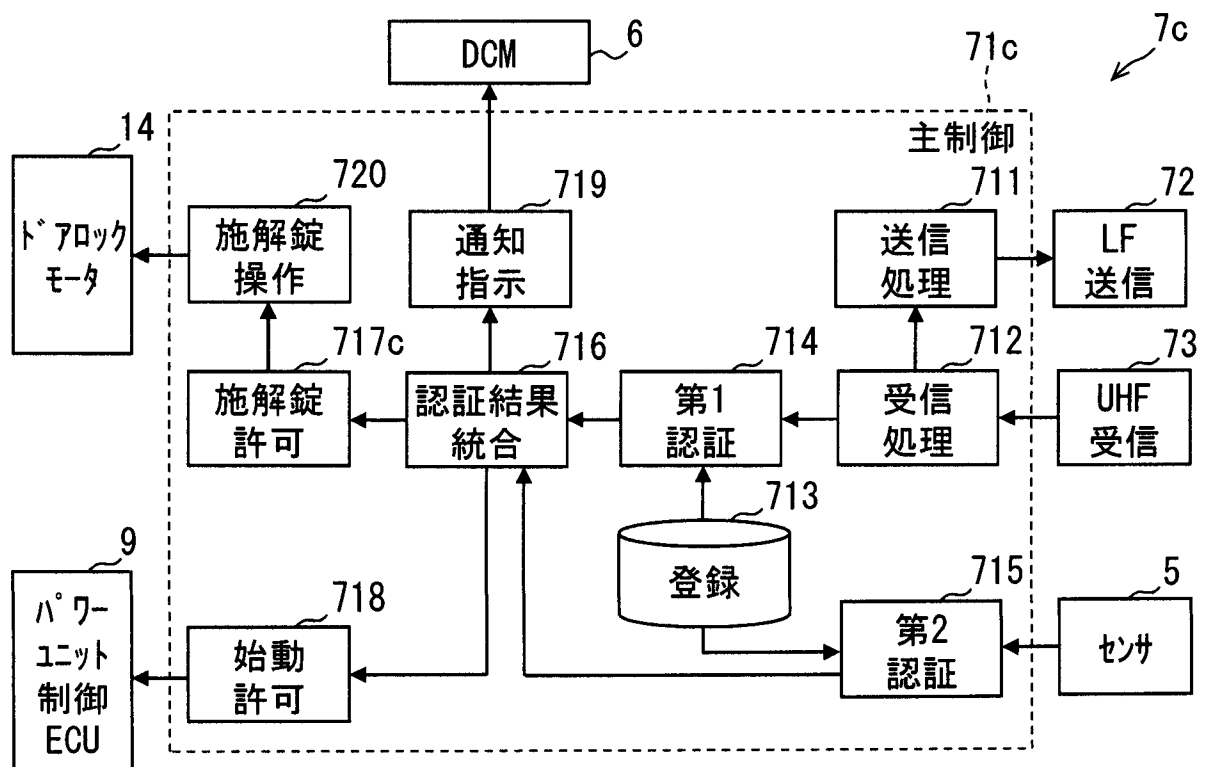
[図9]



[図10]



[図11]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/079727

A. CLASSIFICATION OF SUBJECT MATTER

E05B49/00(2006.01)i, B60R25/102(2013.01)i, B60R25/24(2013.01)i, B60R25/25(2013.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

E05B49/00, B60R25/102, B60R25/24, B60R25/25

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-221960 A (Tokai Rika Co., Ltd.), 08 August 2003 (08.08.2003), paragraphs [0027] to [0093]; fig. 1 to 14 (Family: none)	1-7, 9-12
Y	JP 11-298640 A (Sony Corp.), 29 October 1999 (29.10.1999), paragraphs [0007] to [0015]; fig. 1 to 2 (Family: none)	1-12
Y	JP 2005-273281 A (Teruhiko ISHIGURO), 06 October 2005 (06.10.2005), paragraphs [0035] to [0041]; fig. 1, 7 (Family: none)	1-12

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
02 December 2016 (02.12.16)

Date of mailing of the international search report
13 December 2016 (13.12.16)

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

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/079727

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2009-288944 A (Tokai Rika Co., Ltd.), 10 December 2009 (10.12.2009), paragraphs [0012] to [0030], [0060] to [0068]; fig. 1 (Family: none)	8-11
Y	JP 2014-134082 A (Denso Corp.), 24 July 2014 (24.07.2014), paragraph [0028] (Family: none)	10
Y	JP 2002-302016 A (Nippon Telegraph and Telephone Corp.), 15 October 2002 (15.10.2002), paragraph [0067] (Family: none)	11

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. E05B49/00(2006.01)i, B60R25/102(2013.01)i, B60R25/24(2013.01)i, B60R25/25(2013.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. E05B49/00, B60R25/102, B60R25/24, B60R25/25

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2003-221960 A（株式会社東海理化電機製作所） 2003.08.08, 段落0027-0093、図1-14 (ファミリーなし)	1-7, 9-12
Y	JP 11-298640 A（ソニー株式会社） 1999.10.29, 段落0007-0015、図1-2 (ファミリーなし)	1-12
Y	JP 2005-273281 A（石黒 輝彦）	1-12

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

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

の日の後に公表された文献

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

国際調査を完了した日

02.12.2016

国際調査報告の発送日

13.12.2016

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

兼丸 弘道

2R

5717

電話番号 03-3581-1101 内線 3285

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
	2005. 10. 06, 段落 0 0 3 5 - 0 0 4 1、図 1、7 (ファミリーなし)	
Y	JP 2009-288944 A (株式会社東海理化電機製作所) 2009. 12. 10, 段落 0 0 1 2 - 0 0 3 0、0 0 6 0 - 0 0 6 8、図 1 (ファミリーなし)	8-11
Y	JP 2014-134082 A (株式会社デンソー) 2014. 07. 24, 段落 0 0 2 8 (ファミリーなし)	10
Y	JP 2002-302016 A (日本電信電話株式会社) 2002. 10. 15, 段落 0 0 6 7 (ファミリーなし)	11