(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
2020年5月22日(22.05.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/100929 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G06F 21/31* (2013.01)
B60R 25/24 (2013.01)

(21) 国際出願番号： PCT/JP2019/044488

(22) 国際出願日： 2019年11月13日(13.11.2019)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

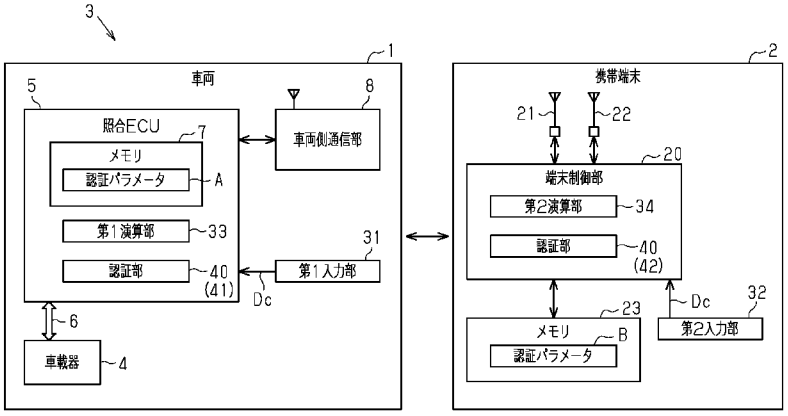
(30) 優先権データ：
特願 2018-214331 2018年11月15日(15.11.2018) JP

(71) 出願人: 株式会社東海理化電機製作所(**KABUSHIKI KAISHA TOKAI RIKA DENKI SEISAKUSHO**) [JP/JP]; 〒4800195 愛知県丹羽郡大口町豊田三丁目２６０番地 Aichi (JP). 国立研究開発法人産業技術総合研究所(**NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL SCIENCE AND TECHNOLOGY**) [JP/JP]; 〒1008921 東京都千代田区霞が関１－３－１ Tokyo (JP).

(72) 発明者: 竹内 恭平 (**TAKEUCHI Kyohei**); 〒4800195 愛知県丹羽郡大口町豊田三丁目２６０番地 株式会社東海理化電機製作所内 Aichi (JP). 岸本 耕平(**KISHIMOTO Kohei**); 〒4800195 愛知県丹羽郡大口町豊田三丁目２６０番地 株式会社東海理化電機製作所内 Aichi (JP). 岩下 明暁(**IWASHITA Hiroaki**); 〒4800195 愛知県丹羽郡大口町豊田三丁目２６０番地 株式会社東海理化電機製作所内 Aichi (JP). 古原 和邦(**KOBARA**

(54) **Title:** AUTHENTICATION SYSTEM AND AUTHENTICATION METHOD

(54) 発明の名称： 認証システム及び認証方法



1 Vehicle
2 Portable terminal
4 Onboard device
5 Verification ECU
7, 23 Memory
8 Vehicle-side communication unit
20 Terminal control unit
31 First input unit
32 Second input unit
33 First computing unit
34 Second computing unit
40 Authentication unit
A, B Authentication parameters

(57) **Abstract:** Provided is an authentication system (3) which performs authentication between a portable terminal (2) and a communication counterpart (1) by radio and permits activation of the communication counterpart on the basis of the result of authentication. The authentication system (3) is provided with: a first input unit (31) and a second input unit (32) which are provided at mutually separate locations and into which authentication information used for authentication can be input; a first computing unit (33) which performs computation on the basis of the authentication information input into

WO 2020/100929 A1

［続葉有］

Kazukuni); 〒1350064 東京都江東区青海２－３－２６ 国立研究開発法人産業技術総合研究所内 Tokyo (JP).

(74) 代理人：恩田 誠, 外 (**ONDA Makoto** et al.); 〒5008731 岐阜県岐阜市大宮町二丁目１２番地１ Gifu (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能)：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

添付公開書類：

— 国際調査報告（条約第21条(3)）

---

the first input unit (31) and a communication counterpart-side authentication parameter registered in the communication counterpart (1); a second computing unit (34) which performs computation on the basis of the authentication information input into the second input unit (32) and a portable terminal-side authentication parameter registered in the portable terminal (2); and authentication units (40 to 42) which, if the authentication information has been input into the first input unit (31), perform authentication on the basis of the result of computation by the first computing unit (33) and the portable terminal-side authentication parameter, and which, if the authentication information has been input into the second input unit (32), performs authentication on the basis of the result of computation by the second computing unit (34) and the communication counterpart-side authentication parameter.

(57) 要約：携帯端末（２）と通信相手（１）との間で無線を通じて認証を行い、その認証結果に基づき通信相手の作動を許可する認証システム（３）は、互いに別の場所に設けられ、認証に用いられる認証情報を入力可能な第１入力部（３１）及び第２入力部（３２）と、第１入力部（３１）に入力された認証情報及び通信相手（１）に登録された通信相手側認証パラメータを基に演算を行う第１演算部（３３）と、第２入力部（３２）に入力された認証情報及び携帯端末（２）に登録された携帯端末側認証パラメータを基に演算を行う第２演算部（３４）と、第１入力部（３１）に認証情報が入力された場合、第１演算部（３３）の演算結果及び携帯端末側認証パラメータを基に認証を行い、第２入力部（３２）に認証情報が入力された場合、第２演算部（３４）の演算結果及び通信相手側認証パラメータを基に認証を行う認証部（４０～４２）と、を備える。

明　細　書

発明の名称 ： 認証システム及び認証方法

技術分野

[0001]　本発明は、携帯端末とその通信相手との間で無線を通じて認証を行う認証システム及び認証方法に関する。

背景技術

[0002]　従来、車両の制御を行うために、ユーザに所持される携帯端末と車両に搭載される車載機との間の無線通信を通じて認証を行う認証システムが知られている。認証システムとしては、スマート照合システムが知られている。スマート照合システムのＩＤ照合（スマート照合）では、携帯端末が、車載機からの送信電波に自動で応答して車載機と無線通信を行う。

[0003]　この種のスマート照合システムに関して、中継器を使用した不正行為が存在する。このような不正行為では、例えば携帯端末が車載機から遠い場所に位置する場合に、中継器が、携帯端末から車載機への通信を中継する。

[0004]　特許文献１は、車両に設けられた入力部に入力された認証情報を用いて認証を行う認証システムを開示する。認証システムは、入力部に入力された認証情報が予め登録された認証情報と一致するか否かを判定する。

先行技術文献

特許文献

[0005] 特許文献1：特開２０１０－１９５０６１号公報

発明の概要

[0006]　スマート照合システムに特許文献１の認証システムが適用された場合、スマート照合システムは、ユーザに認証情報の認証を課してセキュリティ性を向上させることができる。しかし、この種の認証システムでは、予め決められた入力部へ認証情報を入力する作業が認証の度に必要となり、ユーザにとって利便性が悪くなってしまうという問題があった。

[0007]　本開示の一側面の認証システムは、携帯端末とその通信相手との間で無線

を通じて認証を行い、その認証結果に基づき前記通信相手の作動を許可する認証システムであって、互いに別の場所に設けられ、前記認証に用いられる認証情報を入力可能な第１入力部及び第２入力部と、前記第１入力部に入力された前記認証情報及び前記通信相手に登録された通信相手側認証パラメータを基に演算を行う第１演算部と、前記第２入力部に入力された前記認証情報及び前記携帯端末に登録された携帯端末側認証パラメータを基に演算を行う第２演算部と、前記第１入力部に前記認証情報が入力された場合、前記第１演算部の演算結果及び前記携帯端末側認証パラメータを基に前記認証を行い、前記第２入力部に前記認証情報が入力された場合、前記第２演算部の演算結果及び前記通信相手側認証パラメータを基に前記認証を行う認証部と、を備える。

[0008] 本開示の他の側面の認証方法は、携帯端末とその通信相手との間で無線を通じて認証を行い、その認証結果に基づき前記通信相手の作動を許可する認証方法であって、互いに別の場所に設けられた第１入力部及び第２入力部の少なくとも一方に入力された前記認証に用いられる認証情報を受け取ることと、前記第１入力部に入力された前記認証情報、及び前記通信相手に登録された通信相手側認証パラメータを基に演算を行うことと、前記第２入力部に入力された前記認証情報、及び前記携帯端末に登録された携帯端末側認証パラメータを基に演算を行うことと、前記第１入力部に前記認証情報が入力された場合、前記通信相手側認証パラメータを基に演算した演算結果及び前記携帯端末側認証パラメータを基に前記認証を行い、前記第２入力部に前記認証情報が入力された場合、前記携帯端末側認証パラメータを基に演算した演算結果及び前記通信相手側認証パラメータを基に前記認証を行うことと、を備える。

発明の効果

[0009] 本発明の目的は、セキュリティ性及び利便性の両立を可能とした認証システム及び認証方法を提供することにある。

図面の簡単な説明

[0010] [図1]第１実施形態における認証システムの構成を示すブロック図。

[図2]第１入力部に認証情報が入力された場合の認証の流れを示すフロー図。

[図3]第２入力部に認証情報が入力された場合の認証の流れを示すフロー図。

[図4]第２実施形態における認証システムの構成を示すブロック図。

[図5]第２実施形態における認証の流れを示すフロー図。

[図6]第３実施形態における認証システムの構成を示すブロック図。

発明を実施するための形態

[0011] ＜第１実施形態＞

通信相手の制御を行うための認証を行う認証システム及び認証方法の第１実施形態について、図１～図３を用いて説明する。

[0012] 第１実施形態では、認証システム３は、通信相手として車両１に適用されている。認証システム３は、車両１および携帯端末２を備える。車両１は、車載機器４、照合ＥＣＵ（Electronic Control Unit）５、および車両側通信部８を含む。例えば、車載機器４は、ドアロック装置、エンジン、又はこれらの両方を含む。認証システム３は、その認証結果に基づき、車載機器４の作動を許可又は実行する。携帯端末２は、電話機能を有し、近距離無線通信を用いて車両１と通信可能な高機能携帯電話であることが好ましい。一例では、認証システム３は、車両１からの近距離無線通信を契機に近距離無線通信によってＩＤ照合を実行する近距離無線照合システムである。例えば、近距離無線通信は、ブルートゥース（Bluetooth：登録商標）通信である。

[0013] 照合ＥＣＵ５は、ＩＤ照合を行うように構成されている。照合ＥＣＵ５は、車内の通信線６を通じて車載機器４に接続されている。通信線６は、例えばＣＡＮ（Controller Area Network）またはＬＩＮ（Local Interconnect Network）からなる。

[0014] 照合ＥＣＵ５は、データを書き込み及び書き替え可能なメモリ７を含む。メモリ７は、車両１に登録された少なくとも１つの携帯端末２の電子キーＩＤを保存している。一例では、ＩＤ照合は、電子キーＩＤの正否を確認する電子キーＩＤ照合である。認証システム３では、電子キーＩＤ照合の成立は

、車載機器４の作動を許可又は実行するための複数の条件のうちの一条件である。

[0015] メモリ７は、車両１及び携帯端末２の間の認証で用いる認証パラメータＡを保存している。認証システム３では、認証パラメータＡを用いた認証の成立が、車載機器４の作動を許可又は実行するための複数の条件のうちの一条件である。なお、認証パラメータＡが通信相手側認証パラメータに相当する。

[0016] 車両側通信部８は、携帯端末２との間で近距離無線通信を行う。例えば、車両側通信部８は、近距離無線通信として、携帯端末２との間でＢＬＥ（Bluetooth Low Energy）通信を行う。近距離無線通信において、携帯端末２がマスタであり、車両１がスレーブである。他の例では、近距離無線通信において、携帯端末２がスレーブであり、車両１がマスタでもよい。車両側通信部８は、車両１の近傍エリアに定期的にアドバタイズメッセージを送信する。

[0017] 携帯端末２は、携帯端末２の作動を制御する端末制御部２０と、携帯端末２においてネットワーク通信を行なうネットワーク通信モジュール２１と、携帯端末２において近距離無線通信を行う端末通信部２２と、データを書き込み及び書き換え可能なメモリ２３と、を備えている。例えば、端末通信部２２は、近距離無線通信としてＢＬＥ通信を行う。

[0018] メモリ２３は、携帯端末２の電子キーＩＤ、及び認証パラメータＢを保存している。一例では、携帯端末２は、携帯端末２を車両１に登録（電子キー登録）する際に、携帯端末２の電子キーＩＤをネットワーク通信を通じてサーバ（図示略）から取得する。携帯端末２は、取得された携帯端末２の電子キーＩＤを、無線通信を介して車両１に登録する。認証パラメータＢは、車両１と携帯端末２との間の認証に使用される。なお、認証パラメータＢが携帯端末側認証パラメータに相当する。

[0019] 一例では、携帯端末２の端末制御部２０は、携帯端末２において認証システム３の作動を管理するユーザインタフェースアプリケーション（図示略）を実装している。端末制御部２０は、ユーザインタフェースアプリケーショ

ンを用いて、車両１への携帯端末２の登録（電子キー登録）、車両ドアの施解錠操作、車両１のエンジンの始動操作、または任意の２つ以上の組み合わせを含む種々の処理を実行する。

[0020] 携帯端末２が車両１からのアドバタイズメッセージを受信して携帯端末２と車両１との間で近距離無線通信の接続が確立されると、携帯端末２は、車両１と相互に近距離無線通信を行って自動的にＩＤ照合を実行する。例えば、携帯端末２の電子キー登録が完了し、かつ車両１と携帯端末２との間で近距離無線通信の接続が確立している場合、電子キーＩＤが照合ＥＣＵ５と端末制御部２０との間で送受信されて電子キーＩＤの照合を行う。なお、これら一連のＩＤ照合では、ユーザが携帯端末２を操作することなく、また、ユーザが車両１を操作することなく自動的に処理が実行される。

[0021] 認証システム３は、車両１及び携帯端末２の間の通信を通じて認証パラメータＡ及び認証パラメータＢを用いた認証を行う。認証システム３は、ユーザによって入力された認証情報Ｄｃを受け取り、入力された認証情報Ｄｃ、認証パラメータＡ、及び認証パラメータＢに基づいて認証の判定を行う。例えば、認証情報Ｄｃは、認証システム３に予め登録しておいたパスワードである。なお、認証システム３は、ＩＤ照合の前、ＩＤ照合の後、及びＩＤ照合の途中のいずれのタイミングでこのような認証を実施してもよい。

[0022] 一例では、車両１は、データ入力可能な第１入力部３１を含む。例えば、第１入力部３１は、車両１の室内に設けられたカーナビゲーションシステム、車外ドアハンドル、車外ドアハンドルのロックボタン、車両１の室外に設けられたその他の入力装置、またはこれら任意の２つ以上の組み合わせを含む。携帯端末２は、データ入力可能な第２入力部３２を含む。例えば、第２入力部３２は、携帯端末２のタッチパネルディスプレイである。他の例では、第１入力部３１は、車両１とは別個に設けられてもよく、また、第２入力部３２は、携帯端末２とは別個に設けられてもよい。また他の例では、第１入力部３１及び第２入力部３２は、指紋センサや虹彩センサ、カメラでもよい。

[0023] 車両１は、第１入力部３１に入力された認証情報Ｄｃ及び認証パラメータＡを基に演算を行う第１演算部３３を含む。例えば、第１演算部３３は、車両１の照合ＥＣＵ５に設けられている。第１演算部３３は、第１入力部３１に入力された認証情報Ｄｃ及び認証パラメータＡを用いて所定の演算式（演算アルゴリズム）により演算された演算結果Ａ´を求める。

[0024] 携帯端末２は、第２入力部３２に入力された認証情報Ｄｃ及び認証パラメータＢを基に演算を行う第２演算部３４を含む。例えば、第２演算部３４は、携帯端末２の端末制御部２０に設けられている。第２演算部３４は、第２入力部３２に入力された認証情報Ｄｃ及び認証パラメータＢを用いて所定の演算式（演算アルゴリズム）により演算された演算結果Ｂ´を求める。

[0025] 認証システム３は、車両１及び携帯端末２の間の認証を実行する認証部４０を備えている。認証部４０は、第１入力部３１に認証情報Ｄｃが入力された場合、第１演算部３３の演算結果及び認証パラメータＡを基に認証を行い、第２入力部３２に認証情報Ｄｃが入力された場合、第２演算部３４の演算結果及び認証パラメータＢを基に認証を行う。一例では、認証部４０は、照合ＥＣＵ５に設けられた認証部４１と、端末制御部２０に設けられた認証部４２とを含む。第１入力部３１に認証情報Ｄｃが入力された場合、認証部４１，４２は、第１演算部３３の演算結果Ａ´及び認証パラメータＢを基に認証を行う。一方、認証部４１，４２は、第２入力部３２に認証情報Ｄｃが入力された場合、第２演算部３４の演算結果Ｂ´及び認証パラメータＡを基に認証を行う。

[0026] 認証に用いられる認証情報Ｄｃは、例えば電子キー登録時に設定される。また、認証パラメータＡ及び認証パラメータＢは、電子キー登録時に、認証情報Ｄｃに紐付けられて生成され、車両１及び携帯端末２にそれぞれ登録される。さらに、演算結果Ａ´，Ｂ´を求める演算式（演算アルゴリズム）は、例えば電子キー登録時に、照合ＥＣＵ５及び端末制御部２０のユーザインターフェースアプリケーションに付与されている。

[0027] 一例では、認証部４１，４２は、第１入力部３１に認証情報Ｄｃが入力さ

れた場合、演算結果Ａ´及び認証パラメータＢの一致を確認する。また、認証部４１，４２は、第２入力部３２に認証情報Ｄｃが入力された場合、演算結果Ｂ´及び認証パラメータＡの一致を確認する。

[0028] 次に、図２及び図３を用いて、第１実施形態の認証システムの作用及び効果について説明する。まず、図２を用いて認証において第１入力部３１に認証情報Ｄｃが入力された場合を説明する。

[0029] 図２に示すように、ステップＳ１０１において、車両１の照合ＥＣＵ５は、携帯端末２との近距離通信の接続を確立するために、車両側通信部８からアドバタイズメッセージを車両１の近傍エリアに定期的に送信する。携帯端末２の端末制御部２０は、車両１の近傍エリアに進入し、アドバタイズメッセージを受信すると、車両側通信部８との間で車両１との近距離通信の接続を開始する。

[0030] ステップＳ１０２において、車両１及び携帯端末２は、アドバタイズメッセージに連なる一連の通信接続の処理に従って動作し、機器認証（例えばアドレス認証等）が成立すると、自動で通信接続する。両者の通信接続は、携帯端末２が車両１との近距離無線通信の範囲外へ移動するまで継続される。

[0031] ステップＳ１０３において、車両１及び携帯端末２は、近距離通信の接続が確立されると、電子キーＩＤの正否を確認するＩＤ照合を開始する。ＩＤ照合には、電子キーＩＤの送受信が含まれる。照合ＥＣＵ５は、ＩＤ照合が不成立の場合、車両１の作動を禁止する。照合ＥＣＵ５は、ＩＤ照合が成立した場合、認証情報Ｄｃを用いた認証を開始する。

[0032] ステップＳ１０４において、照合ＥＣＵ５は、ＩＤ照合が成立した場合、第１入力部３１へのデータ入力を受け付ける。このとき、照合ＥＣＵ５は、認証情報Ｄｃの入力要求をユーザに通知し、第１入力部３１に認証情報Ｄｃを入力させる。例えば、認証情報Ｄｃの入力要求は、音声または表示等によってユーザに通知される。照合ＥＣＵ５は、第１入力部３１へ認証情報Ｄｃが入力された場合、ステップＳ１０５へ移行する。照合ＥＣＵ５は、第１入力部３１及び第２入力部３２のどちらにも認証情報Ｄｃが入力されなかった

場合、処理を終了する。

[0033] ステップＳ１０５において、照合ＥＣＵ５の第１演算部３３は、第１入力部３１へ入力された認証情報Ｄｃ及び認証パラメータＡを基に演算を行い演算結果Ａ´を求める。第１入力部３１の演算結果Ａ´は、メモリ７に書き込み保存される。

[0034] ステップＳ１０６において、認証部４１は、送信の度に値の異なる乱数からなるチャレンジコードを生成する。認証部４１は、生成されたチャレンジコードを含むチャレンジ信号を、携帯端末２へ送信する。

[0035] ステップＳ１０７において、認証部４１は、演算結果Ａ´を用いてチャレンジコードを演算して、車両１側のレスポンスコードを生成する。

ステップＳ１０８において、端末制御部２０の認証部４２は、チャレンジ信号を受信すると、携帯端末２に登録された認証パラメータＢを用いてチャレンジ信号に含まれるチャレンジコードを演算して、携帯端末２側のレスポンスコードを生成する。

[0036] ステップＳ１０９において、認証部４２は、生成した携帯端末２側のレスポンスコードを含むレスポンス信号を、車両１へ送信する。

ステップＳ１１０において、認証部４１は、携帯端末２からレスポンス信号を受信すると、車両１側及び携帯端末２側のレスポンスコードが一致しているか否かを確認する。認証部４１は、車両１側及び携帯端末２側のレスポンスコードが一致している場合、認証が成立したと判定する。一方、認証部４１は、車両１側及び携帯端末２側のレスポンスコードが一致しない場合、認証を不成立と判定する。

[0037] 認証パラメータＡ，Ｂと、演算結果Ａ´，Ｂ´との関係について説明する。ここでは、第１演算部３３及び第２演算部３４の演算式（演算アルゴリズム）の一例として、排他的倫理和（ＸＯＲ）が用いられる。すなわち、第１入力部３１に認証情報Ｄｃが入力された場合、第１演算部３３は、「Ａ　ＸＯＲ　Ｄｃ」を、演算結果Ａ´として算出する。なお、「Ａ　ＸＯＲ　Ｄｃ」は、認証パラメータＡ及び認証情報Ｄｃの排他的倫理和を示す。第１入力

部３１に正規の認証情報Ｄｃが入力された場合、「Ａ　ＸＯＲ　Ｄｃ＝Ｂ」の関係が成り立つようになっている。すなわち、演算結果Ａ´及び認証パラメータＢが一致する。演算結果Ａ´及び認証パラメータＢが一致する場合、演算結果Ａ´を用いて演算したレスポンスコードは、認証パラメータＢを用いて演算したレスポンスコードと一致する。また、第２入力部３２に認証情報Ｄｃが入力された場合、第２演算部３４は、「Ｂ　ＸＯＲ　Ｄｃ」を、演算結果Ｂ´として算出する。なお、「Ｂ　ＸＯＲ　Ｄｃ」は、認証パラメータＢ及び認証情報Ｄｃの排他的倫理和を示す。第２入力部３２に正規の認証情報Ｄｃが入力された場合、「Ｂ　ＸＯＲ　Ｄｃ＝Ａ」の関係が成り立つようになっている。すなわち、演算結果Ｂ´及び認証パラメータＡが一致する。演算結果Ｂ´及び認証パラメータＡが一致する場合、演算結果Ｂ´を用いて演算したレスポンスコードは、認証パラメータＡを用いて演算したレスポンスコードと一致する。つまり、第１演算部３３の演算式は、正規な認証情報Ｄｃおよび認証パラメータＡを用いて演算された場合に認証パラメータＢと一致する演算結果Ａ´を生成するように構成される。第２演算部３４の演算式は、正規な認証情報Ｄｃおよび認証パラメータＢを用いて演算された場合に認証パラメータＡと一致する演算結果Ｂ´を生成するように構成される。

[0038] ステップＳ１１１において、照合ＥＣＵ５は、認証が成立したと判定された場合、車載機器４の作動を許可する。例えば、照合ＥＣＵ５は、ドアロックの施解錠やエンジンの始動を許可する。

[0039] 次に、図３を用いて、第２入力部３２へ認証情報Ｄｃが入力された場合について説明する。

図３に示すように、ステップＳ２０１において、車両１及び携帯端末２が近距離通信接続され、かつＩＤ照合が成立すると、端末制御部２０は、ステップＳ２０２へ移行する。

[0040] ステップＳ２０２において、端末制御部２０は、第２入力部３２へのデータ入力を受け付ける。このとき、端末制御部２０は、ユーザインタフェース

アプリケーションにより、ユーザへ認証情報Ｄｃの入力要求を通知し、第２入力部３２へ認証情報Ｄｃを入力させる。端末制御部２０は、第２入力部３２へ認証情報Ｄｃが入力された場合、ステップＳ２０３へ移行する。なお、端末制御部２０は、照合ＥＣＵ５によって認証の処理が終了されるまで、第２入力部３２への入力を受け付ける。

[0041] ステップＳ２０３において、端末制御部２０の第２演算部３４は、第２入力部３２へ入力された認証情報Ｄｃ及び認証パラメータＢを基に演算を行い演算結果Ｂ´を求める。演算結果Ｂ´は、メモリ２３に保存される。

[0042] ステップＳ２０４において、端末制御部２０は、第２入力部３２に認証情報Ｄｃの入力があったことを通知するアック信号を、車両１へ送信する。

ステップＳ２０５において、認証部４１，４２は、演算結果を用いた認証を開始する。演算結果を用いた認証とは、図２のステップＳ１０６～Ｓ１１１に相当する。ここでは、認証部４２は、演算結果Ｂ´を用いて演算した携帯端末２側のレスポンスコードを含むレスポンス信号を車両１へ送信する。認証部４１は、認証パラメータＡを用いて演算した車両１側のレスポンスコードと、携帯端末２側のレスポンスコードとが一致するかを確認する。認証部４１は、車両１側のレスポンスコードが携帯端末２側のレスポンスコードと一致する場合、認証が成立したと判定する。

[0043] このように、本例では、認証システム３は、第１入力部３１と、第２入力部３２と、第１入力部３１に入力された認証情報Ｄｃ及び認証パラメータＡを基に演算結果Ａ´を求める第１演算部３３と、第２入力部３２に入力された認証情報Ｄｃ及び認証パラメータＢを基に演算結果Ｂ´を求める第２演算部３４とを備えた。また、認証システム３は、第１入力部３１に認証情報Ｄｃが入力された場合、演算結果Ａ´及び認証パラメータＢを基に認証を行い、第２入力部３２に認証情報Ｄｃが入力された場合、演算結果Ｂ´及び認証パラメータＡを基に認証を行う認証部４０を備えた。この構成によれば、認証の過程において、ユーザに認証情報Ｄｃを入力させるので、正規の認証情報Ｄｃを知らない第三者に認証を成立されることがない。さらに、ユーザに

とっては、第１入力部３１及び第２入力部３２のどちらか一方に認証情報Ｄｃを入力すればよいので、予め決められた入力部に入力が必要な場合と比較して利便性が向上する。したがって、セキュリティ性及び利便性の両立が可能となる。

[0044] 一例では、認証部４０は、第１入力部３１に認証情報Ｄｃが入力された場合、演算結果Ａ´と、認証パラメータＢとの一致を確認する。また、認証部４０は、第２入力部３２に認証情報Ｄｃが入力された場合、演算結果Ｂ´と、認証パラメータＡとの一致を確認する。この構成によれば、認証の成立のためには、車両１側及び携帯端末２側の双方に決められた演算式で演算を行う必要がある。したがって、セキュリティ性の向上に寄与する。

[0045] また、これら演算結果Ａ´，Ｂ´と認証パラメータＡ，Ｂとの一致を確認する際に、それぞれを用いて演算した車両１側及び携帯端末２側のレスポンスコードの一致を確認する構成とした。この構成によれば、演算結果Ａ´，Ｂ´及び認証パラメータＡ，Ｂを車両１及び携帯端末２の間で送受信する必要がないため、セキュリティ性の向上に寄与する。

[0046] 一例では、第１入力部３１は、車両１に設けられ、第２入力部３２は、携帯端末２に設けられた。この構成によれば、車両１側及び携帯端末２側のどちらかへの認証情報Ｄｃの入力により、車両１を作動させることができる。これは、ユーザの利便性の向上に寄与する。

[0047] ＜第２実施形態＞

次に、認証システム及び認証方法の第２実施形態について、図４及び図５を用いて説明する。第２実施形態では、互いに異なる複数の認証情報を有している点で、第１実施形態と異なる。従って、第１実施形態と同一の部材構成については、同一の符号を付し、その詳細な説明を省略し、異なる部分のみ詳述する。

[0048] 図４に示すように、車両１は、車載機器４として用いられるドアロック装置１０及びエンジン１１を含む。また、車両１は、ドアロック装置１０を制御するボディＥＣＵ１２と、エンジン１１を制御するエンジンＥＣＵ１３と

、を含む。これらＥＣＵは、車内の通信線６を通じて照合ＥＣＵ５と接続されている。

[0049] 車両１は、車両ドア１４と、該車両ドア１４に設けられかつ車両ドア１４の開閉を操作するための車外ドアハンドル１５と、を含む。ドアロック装置１０は、車両ドア１４を施解錠するように構成された機械的な機構である。車外ドアハンドル１５は、タッチセンサ１６と、ロックボタン１７と、を含む。タッチセンサ１６は、ドア解錠するときなどのトリガとして車外ドアハンドル１５に対するユーザのタッチ操作を検出する。ロックボタン１７は、ドア施錠するときなどのトリガとして車外ドアハンドル１５に対するユーザのタッチ操作を検出する。ボディＥＣＵ１２は、ＩＤ照合が成立し、かつ認証が成立しているときに、タッチセンサ１６及びロックボタン１７の検出信号を基に、ドアロック装置１０の作動を制御する。ドアロック装置１０の作動が車両１の第１の作動に該当する。

[0050] 車両１は、エンジン１１の電源遷移を操作するためのエンジンスイッチ１８を含む。エンジンスイッチ１８は、例えばプッシュ式のスイッチでもよい。エンジンＥＣＵ１３は、所定の条件下でエンジンスイッチ１８が操作されることでエンジン１１の遷移を制御する。なお、エンジン１１の始動の所定の条件とは、ＩＤ照合が成立していること、認証が成立していること、車両１のブレーキペダル（図示略）が踏まれていること、車両１のトランスミッションがパーキングレンジに入っていること、及びこれらの２つ以上の組み合わせが挙げられる。エンジン１１の遷移が車両１の第２の作動に該当する。

[0051] 一例では、認証部４０は、前述の認証として、車両操作の機能（車両ドア１４の施解錠操作、車両１の電源遷移操作）ごとに第１認証又は第２認証を行う。認証部４０は、第１認証又は第２認証において異なる演算処理を行う。本例の場合、車両ドア１４の施解錠操作の際に第１認証が実行され、車両１の電源遷移操作の際に第２認証が実行される。認証部４１は、第１認証を行う第１認証部４１ａと、第２認証を行う第２認証部４１ｂとを有している

。また、認証部４２は、第１認証を行う第１認証部４２ａと、第２認証を行う第２認証部４２ｂとを有している。

[0052] 車両１のメモリ７は、第１認証で用いられる第１認証パラメータＡ１と、第２認証で用いられる第２認証パラメータＡ２とを保存している。また、携帯端末２のメモリ２３は、第１認証で用いられる第１認証パラメータＢ１と、第２認証で用いられる第２認証パラメータＢ２とを保存している。

[0053] 認証情報Ｄｃは、互いに異なる第１認証情報Ｄｃ１と、第２認証情報Ｄｃ２とを含む。第１認証情報Ｄｃ１は、第１認証に用いられる。第２認証情報Ｄｃ２は、第２認証に用いられる。第１認証パラメータＡ１及び第１認証パラメータＢ１は、第１認証情報Ｄｃ１に紐づけられて生成されている。また、第２認証パラメータＡ２及び第２認証パラメータＢ２は、第２認証情報Ｄｃ２に紐づけられて生成されている。

[0054] 第１演算部３３は、第１入力部３１に認証情報Ｄｃが入力されると、認証情報Ｄｃ及び第１認証パラメータＡ１を基に演算した演算結果Ａ１´と、認証情報Ｄｃ及び第２認証パラメータＡ２を基に演算した演算結果Ａ２´とを求める。第２演算部３４は、第２入力部３２に認証情報Ｄｃが入力されると、認証情報Ｄｃ及び第１認証パラメータＢ１を基に演算した演算結果Ｂ１´と、認証情報Ｄｃ及び第２認証パラメータＢ２を基に演算した演算結果Ｂ２´とを求める。

[0055] 第１認証部４１ａ，４２ａは、演算結果Ａ１´及び第１認証パラメータＢ１、又は演算結果Ｂ１´及び第１認証パラメータＡ１が一致する場合に、第１認証を成立と判定する。第２認証部４１ｂ，４２ｂは、演算結果Ａ２´及び第２認証パラメータＢ２、又は演算結果Ｂ２´及び第２認証パラメータＡ２が一致する場合に、第２認証を成立と判定する。ここで、第１入力部３１に第１認証情報Ｄｃ１が入力された場合、演算結果Ａ１´及び第１認証パラメータＢ１が一致する。また、第２入力部３２に第１認証情報Ｄｃ１が入力された場合、演算結果Ｂ１´及び第１認証パラメータＡ１が一致する。また、第１入力部３１に第２認証情報Ｄｃ２が入力された場合、演算結果Ａ２´

及び第２認証パラメータＢ２が一致する。さらに、第２入力部３２に第２認証情報Ｄｃ２が入力された場合、演算結果Ｂ２´及び第２認証パラメータＡ２が一致する。

[0056] 次に、図５を用いて、第２実施形態の認証システムの作用及び効果を説明する。ここでは、第１入力部３１に認証情報Ｄｃが入力された場合について説明する。

図５に示すように、ステップＳ３０１において、ＩＤ照合が完了すると、認証の処理が開始される。

[0057] ステップＳ３０２において、照合ＥＣＵ５は、第１入力部３１に認証情報Ｄｃが入力されると、ステップＳ３０３へ移行する。

ステップＳ３０３において、第１演算部３３は、認証情報Ｄｃ及び第１認証パラメータＡ１を用いて所定の演算式により演算結果Ａ１´を求める。また、第１演算部３３は、認証情報Ｄｃ及び第２認証パラメータＡ２を用いて所定の演算式により演算結果Ａ２´を求める。

[0058] ステップＳ３０４において、認証部４１は、送信の度に値の異なる乱数からなるチャレンジコードを生成する。認証部４１は、チャレンジコードを含むチャレンジ信号を、携帯端末２へ送信する。

[0059] ステップＳ３０５において、第１認証部４１ａは、演算結果Ａ１´を用いてチャレンジコードを演算して、車両１側の第１レスポンスコードを生成する。また、第２認証部４１ｂは、演算結果Ａ２´を用いてチャレンジコードを演算して、車両１側の第２レスポンスコードを生成する。

[0060] ステップＳ３０６において、チャレンジ信号を受信すると、第１認証部４２ａは、第１認証パラメータＢ１を用いてチャレンジコードを演算して、携帯端末２側の第１レスポンスコードを生成する。また、第２認証部４２ｂは、第２認証パラメータＢ２を用いてチャレンジコードを演算して、携帯端末２側の第２レスポンスコードを生成する。

[0061] ステップＳ３０７において、第１認証部４２ａ及び第２認証部４２ｂは、携帯端末２側の第１レスポンスコード及び第２レスポンスコードを、車両１

へ送信する。

ステップＳ３０８において、第１認証部４１ａは、車両１側及び携帯端末２側の第１レスポンスコードが一致するか否かを判定する。ステップＳ３０２で、第１入力部３１に第１認証情報Ｄｃ１が入力された場合は、演算結果Ａ１´及び第１認証パラメータＢ１が一致するので、車両１側及び携帯端末２側の第１レスポンスコードも一致する。車両１側及び携帯端末２側の第１レスポンスコードが一致する場合、第１認証部４１ａは、第１認証が成立したと判定する。照合ＥＣＵ５は、第１認証が成立した場合、ステップＳ３０８へ移行する。一方、照合ＥＣＵ５は、第１認証が不成立の場合、ステップＳ３０７へ移行する。

[0062] ステップＳ３０９において、第２認証部４１ｂは、車両１側及び携帯端末２側の第２レスポンスコードが一致するか否かを判定する。ステップＳ３０２で、第１入力部３１に第２認証情報Ｄｃ２が入力された場合は、演算結果Ａ２´及び第２認証パラメータＢ２が一致するので、車両１側及び携帯端末２側の第２レスポンスコードも一致する。車両１側及び携帯端末２側の第２レスポンスコードが一致する場合、第２認証部４１ｂは、第２認証が成立したと判定する。照合ＥＣＵ５は、第２認証が成立した場合、ステップＳ３０９へ移行する。一方、照合ＥＣＵ５は、第２認証が不成立の場合、処理を終了する。

[0063] ステップＳ３１０において、第１認証が成立した場合、照合ＥＣＵ５は、ボディＥＣＵ１２にドアロック装置１０の作動を許可する。これにより、ボディＥＣＵ１２は、タッチセンサ１６及びロックボタン１７の検出信号を基に、ドアロック装置１０の作動を制御する。

[0064] ステップＳ３１１において、第２認証が成立した場合、照合ＥＣＵ５は、エンジンＥＣＵ１３にエンジン１１の始動を許可する。これにより、エンジンＥＣＵ１３は、所定の条件下でエンジンスイッチ１８が操作されることでエンジン１１の始動を制御する。

[0065] なお、本例において、第２入力部３２に認証情報Ｄｃが入力された場合、

第２演算部３４によって演算結果Ｂ１´，Ｂ２´が演算される。そして、上述のチャレンジ信号及びレスポンス信号の送受信によって、演算結果Ｂ１´及び第１認証パラメータＡ１の一致を確認することで、第１認証が行われ、演算結果Ｂ２´及び第２認証パラメータＡ２の一致を確認することで第２認証が行われる。

[0066] このように、本例では、認証情報Ｄｃに、互いに異なる第１認証情報Ｄｃ１及び第２認証情報Ｄｃ２が含まれている。また、第１認証情報Ｄｃ１を基に第１認証が許可された場合、照合ＥＣＵ５は、車両１のドアロック装置１０の作動を許可し、第２認証情報Ｄｃ２を基に第２認証が許可された場合、照合ＥＣＵ５は、車両１のエンジン１１の始動を許可する。この構成によれば、第１認証及び第２認証の成立には、それぞれ異なる第１認証情報Ｄｃ１及び第２認証情報Ｄｃ２が入力される必要がある。すなわち、認証システム３は、車両１のドアロック装置１０を作動させるときと、エンジン１１を遷移させるときとで、別の認証情報Ｄｃを入力させる。第１認証情報Ｄｃ１及び第２認証情報Ｄｃ２の一方だけでは、車両１の全ての作動が許可されないので、セキュリティ性の向上に寄与する。また、例えば携帯端末２のユーザインタフェースアプリケーションなどを用いて、車両１を遠隔で操作する場合に、誤操作を抑制できる。

[0067] ＜第３実施形態＞

次に、認証システムの第３実施形態を、図６を用いて説明する。第３実施形態についても第１実施形態と異なる部分のみ詳述する。

[0068] 図６に示すように、認証システム３は、認証パラメータＡ，Ｂを新たな値に更新するパラメータ更新部５０を備えている。パラメータ更新部５０は、パラメータ更新部５１と、パラメータ更新部５２と、を含む。パラメータ更新部５１は、照合ＥＣＵ５に設けられ、認証パラメータＡを更新する。パラメータ更新部５２は、端末制御部２０に設けられ、認証パラメータＢを更新する。パラメータ更新部５１，５２は、認証が成立した場合に、認証パラメータＡ，Ｂを更新する。

[0069] パラメータ更新部５１，５２は、例えば車両１及び携帯端末２に複数の認証パラメータを有する場合、複数の認証パラメータのうちのいずれかの認証パラメータを基に認証が成立した際に、全ての認証パラメータを更新する。仮に、車両１及び携帯端末２が、例えば第１認証に用いられる第１認証パラメータＡ１，Ｂ１及び第２認証に用いられる第２認証パラメータＡ２，Ｂ２を有すると仮定する。この場合、パラメータ更新部５１，５２は、第１認証及び第２認証のいずれかが成立した際に、第１認証パラメータＡ１，Ｂ１及び第２認証パラメータＡ２，Ｂ２の全てを更新する。

[0070] このように、本例では、認証システム３は、認証が成立した場合に、車両１側の認証パラメータＡ及び携帯端末２側の認証パラメータＢを新たな値に更新するパラメータ更新部を備えた。この構成によれば、認証のたびに認証パラメータＡ，Ｂを更新できるので、セキュリティ性の向上に寄与する。

[0071] なお、本実施形態は、以下のように変更して実施することができる。本実施形態及び以下の変更例は、技術的に矛盾しない範囲で互いに組み合わせて実施することができる。

・各実施形態において、第１演算部３３及び第２演算部３４の演算式（演算アルゴリズム）は、排他的倫理和に限定されず、加法や減法を用いたり、乗法や除法を用いたり、べき乗を計算したり、楕円曲線状の点を計算したりするものでもよい。認証パラメータＡ，Ｂから認証情報Ｄｃが推測されないように演算式を設定することで、認証情報Ｄｃの秘匿性を確保できる。

[0072] ・第３実施形態において、更新される認証パラメータは、認証に用いられた認証パラメータだけとしてもよいし、前回更新されてから一定の期間が経った認証パラメータを更新することとしてもよい。

[0073] ・第２実施形態において、第１認証及び第２認証を、関連付けて行ってもよい。例えば、第１認証の成立後、一定時間以内のみ第２認証を実行する態様としてもよい。

・第２実施形態において、複数の認証情報Ｄｃは、２つに限定されず、３つ以上であってもよく、複数であればいくつでもよい。これは、仕様に応じ

て適宜変更可能である。

[0074] ・各実施形態において、認証情報Ｄｃは、英数記号を用いたパスワードでもよいし、暗証番号でもよいし、象形パターンでもよいし、ユーザの生体情報であってもよいし、これらの組み合わせであってもよい。なお、生体情報には、指紋、顔、静脈、掌形、虹彩、網膜などが含まれる。

[0075] ・各実施形態において、第１入力部３１及び第２入力部３２に入力される認証情報Ｄｃは、異なっていてもよい。例えば、認証情報Ｄｃがパスワード及び生体情報である場合、第１入力部３１にはパスワードが入力され、第２入力部３２には、生体情報が入力されるようにしてもよい。この場合、車両１及び携帯端末２にパスワード用及び生体情報用の認証パラメータが設けられて認証が行われればよい。

[0076] ・各実施形態において、第１入力部３１に正規の認証情報Ｄｃが入力された場合、認証パラメータＡを演算して得られた演算結果Ａ´と、認証パラメータＢとが一致してもよい。また、第２入力部３２に正規の認証情報Ｄｃが入力された場合、認証パラメータＢを演算して得られた演算結果Ｂ´と、認証パラメータＡとが一致してもよい。さらに、認証パラメータＡ及び認証パラメータＢは、認証情報Ｄｃを共通鍵とした平文及び暗号文の関係であってもよい。

[0077] ・各実施形態において、第１演算部３３及び第２演算部３４の演算式は、それぞれ異なっていてもよいし、同じでもよい。

・各実施形態において、認証情報Ｄｃは、電子キー登録後の任意のタイミングで、変更可能であり、例えば認証が成立した場合に、ユーザの操作により認証情報Ｄｃを変更してもよい。なお、認証情報Ｄｃが変更されると、認証情報Ｄｃに紐付けられた認証パラメータＡ，Ｂも変更される。

[0078] ・各実施形態において、演算結果及び認証パラメータの認証の際に、認証部４２がチャレンジコードを生成し、認証部４２がレスポンスコードの一致を確認する態様としてもよい。

[0079] ・各実施形態において、車両１及び携帯端末２の認証は、片方向認証でも

よいし、相互認証でもよい。相互認証では、例えば、車両１から携帯端末２へチャレンジコードを送信し、双方で生成したレスポンスコードの一致を車両１で確認するとともに、携帯端末２から車両１へチャレンジコードを送信し、双方で生成したレスポンスコードの一致を携帯端末２で確認する。

[0080] ・各実施形態において、認証部４０は、演算結果及び認証パラメータを単に比較することにより、これらの一致を確認してもよい。

・各実施形態において、演算結果及び認証パラメータを暗号化した暗号文を用いてこれらの一致を確認してもよいし、演算結果及び認証パラメータをハッシュ化したハッシュ値を用いてこれらの一致を確認してもよい。なお、ハッシュ値は、チャレンジコード及び演算結果と、チャレンジコード及び認証パラメータとをそれぞれハッシュ化したものでもよいし、演算結果及び認証パラメータをそれぞれハッシュ化したものでもよい。

[0081] ・各実施形態において、車両１側及び携帯端末２側で求めた演算値の一致を確認する場合、演算結果Ａ´及び認証パラメータＢ、演算結果Ｂ´及び認証パラメータＡが一致することは、構成要素から省略できる。すなわち、演算結果Ａ´，Ｂ´及び認証パラメータＡ，Ｂを用いて認証情報Ｄｃの正否が判定できればよい。

[0082] ・各実施形態において、認証の成立可否の判定は、車両１及び携帯端末２のどちらで行ってもよい。

・各実施形態において、近距離無線通信は、ブルートゥース通信に限定されず、他の通信方式に変更してもよい。

[0083] ・各実施形態において、携帯端末２は、高機能携帯電話に限定されず、種々の端末であってもよい。例えば、車両１の電子キーでもよい。

・各実施形態において、通信相手は、車両１に限定されず、例えば宿泊施設のドア、コインパーキングのゲート機、宅配ボックスのロッカーなど、他の部材に適用されてもよい。

[0084] 明細書及び／又は特許請求の範囲に開示された全ての特徴は、当初の開示の目的のために、ならびに、実施形態及び／又は特許請求の範囲における特

徴の組み合わせから独立して特許請求の範囲に記載の発明を限定する目的のために、互いに別個にかつ独立して開示されることを意図したものである。全ての数値範囲又は構成要素の集合を表す記載は、当初の開示の目的のため、ならびに特許請求の範囲に記載の発明を限定する目的のために、特に数値範囲の限定として、全ての可能な中間値又は中間的構成要素を開示するものである。

[0085] 上記実施形態では、照合ＥＣＵ、端末制御部、演算部、認証部、およびパラメータ更新部の各々は、１つ以上の専用回路または１つ以上のプロセッサを用いて構成することができる。また、車両１および携帯端末２の各々には、１つ以上のプロセッサに接続されたメモリ（コンピュータ読み取り可能な非一時的記憶媒体）が設けられてもよい。メモリは、１つ以上のプロセッサによって実行可能な命令群を含む１つ以上のプログラムを記憶してもよい。命令群は、それらが実行されたときに、本開示による鍵情報生成処理をプロセッサに実行させる。たとえば、プログラムは、図２に示すシーケンスのステップ１０１～ステップ１１１の処理、図３に示すシーケンスのステップ２０１～ステップ２０５の処理、図５に示すシーケンスのステップ３０１～ステップ３１１の処理をプロセッサに実行させる命令群を含む。従って、本開示により、このようなプログラムを記憶したコンピュータ読み取り可能な非一時的記憶媒体を提供することもできる。

符号の説明

[0086] １…車両、１０…ドアロック装置、１１…エンジン、２…携帯端末、２０…端末制御部、３…認証システム、３１…第１入力部、３２…第２入力部、３３…第１演算部、３４…第２演算部、４…車載機器、４０…認証部、４１…認証部、４２…認証部、５…照合ＥＣＵ、５０…パラメータ更新部、Ａ…認証パラメータ、Ｂ…認証パラメータ、Ｄｃ…認証情報。

請求の範囲

[請求項1] 携帯端末と通信相手との間で無線を通じて認証を行い、その認証結果に基づき前記通信相手の作動を許可する認証システムであって、

互いに別の場所に設けられ、前記認証に用いられる認証情報を入力可能な第１入力部及び第２入力部と、

前記第１入力部に入力された前記認証情報及び前記通信相手に登録された通信相手側認証パラメータを基に演算を行う第１演算部と、

前記第２入力部に入力された前記認証情報及び前記携帯端末に登録された携帯端末側認証パラメータを基に演算を行う第２演算部と、

前記第１入力部に前記認証情報が入力された場合、前記第１演算部の演算結果及び前記携帯端末側認証パラメータを基に前記認証を行い、前記第２入力部に前記認証情報が入力された場合、前記第２演算部の演算結果及び前記通信相手側認証パラメータを基に前記認証を行う認証部と、を備える認証システム。

[請求項2] 前記認証部は、

前記第１入力部に前記認証情報が入力された場合、前記認証として、前記第１演算部の演算結果と前記携帯端末側認証パラメータとの一致を確認し、

前記第２入力部に前記認証情報が入力された場合、前記認証として、前記第２演算部の演算結果と前記通信相手側認証パラメータとの一致を確認する、請求項１に記載の認証システム。

[請求項3] 前記第１入力部は、前記通信相手に設けられ、

前記第２入力部は、前記携帯端末に設けられている、請求項１又は請求項２に記載の認証システム。

[請求項4] 前記認証情報は、互いに異なる第１認証情報及び第２認証情報を含み、

前記認証部は、前記第１認証情報を基に前記認証を行う第１認証と、前記第２認証情報を基に前記認証を行う第２認証とを実行し、

前記第１認証が成立した場合、前記通信相手の第１の作動を許可し、前記第２認証が成立した場合、前記通信相手の第２の作動を許可する、請求項１から請求項３のうちいずれか一項に記載の認証システム。

[請求項5] 前記認証部による前記認証が成立した場合に、前記通信相手側認証パラメータ及び前記携帯端末側認証パラメータを新たな値に更新するパラメータ更新部をさらに備える請求項１から請求項４のうちいずれか一項に記載の認証システム。

[請求項6] 携帯端末とその通信相手との間で無線を通じて認証を行い、その認証結果に基づき前記通信相手の作動を許可する認証方法であって、

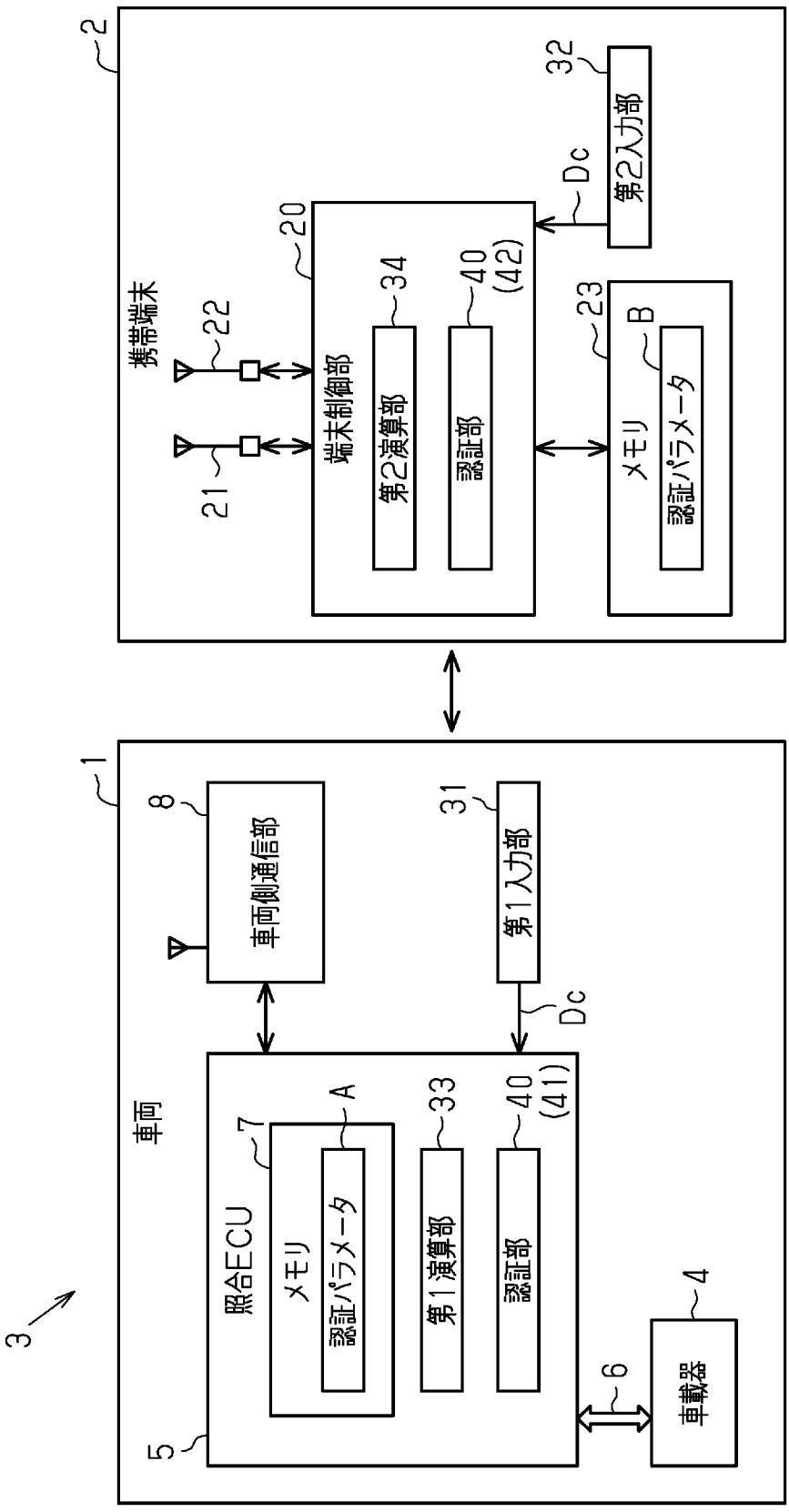
互いに別の場所に設けられた第１入力部及び第２入力部の少なくとも一方に入力された前記認証に用いられる認証情報を受け取ることと、

前記第１入力部に入力された前記認証情報、及び前記通信相手に登録された通信相手側認証パラメータを基に演算を行うことと、

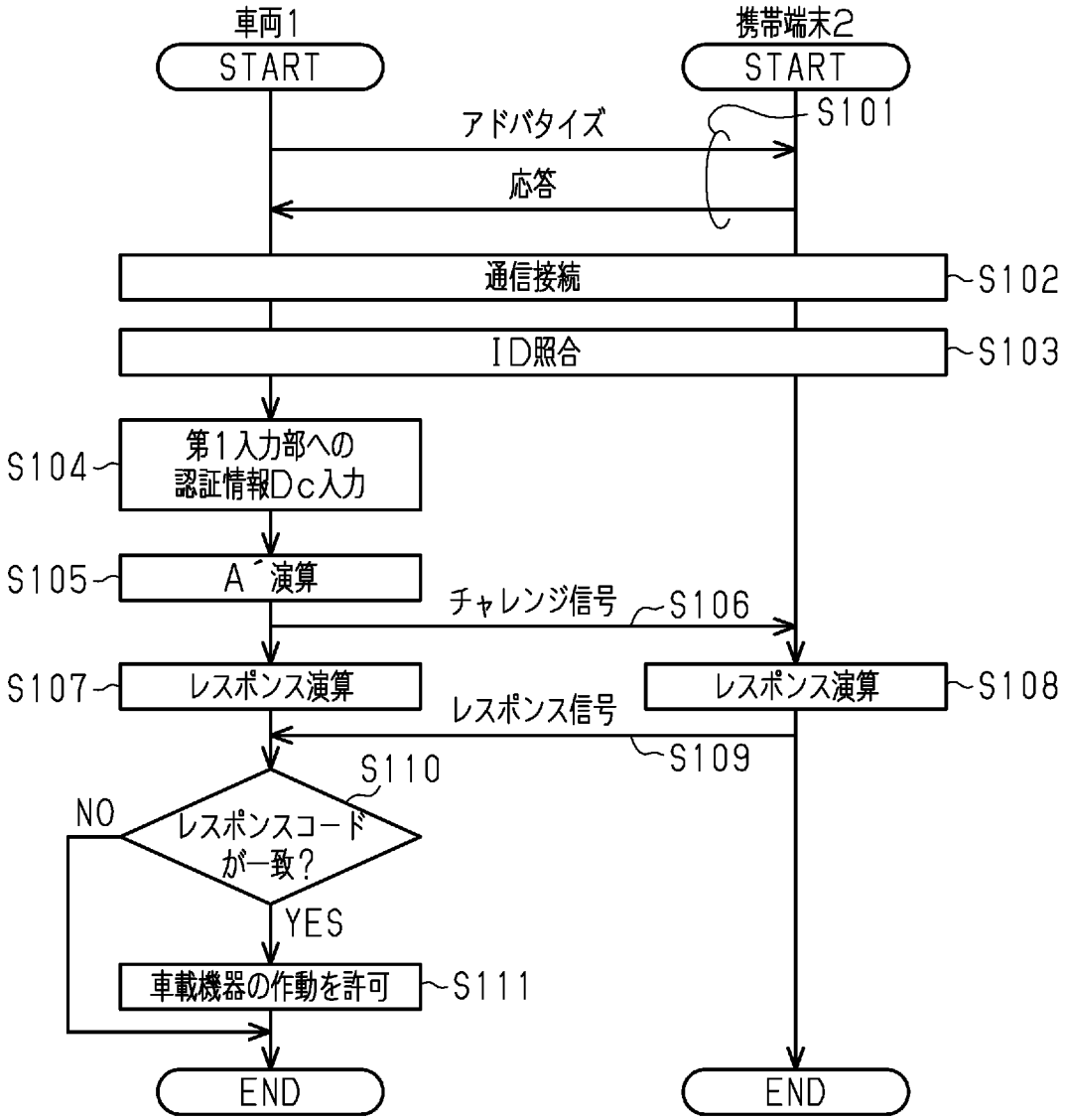
前記第２入力部に入力された前記認証情報、及び前記携帯端末に登録された携帯端末側認証パラメータを基に演算を行うことと、

前記第１入力部に前記認証情報が入力された場合、前記通信相手側認証パラメータを基に演算した演算結果及び前記携帯端末側認証パラメータを基に前記認証を行い、前記第２入力部に前記認証情報が入力された場合、前記携帯端末側認証パラメータを基に演算した演算結果及び前記通信相手側認証パラメータを基に前記認証を行うことと、を備える認証方法。

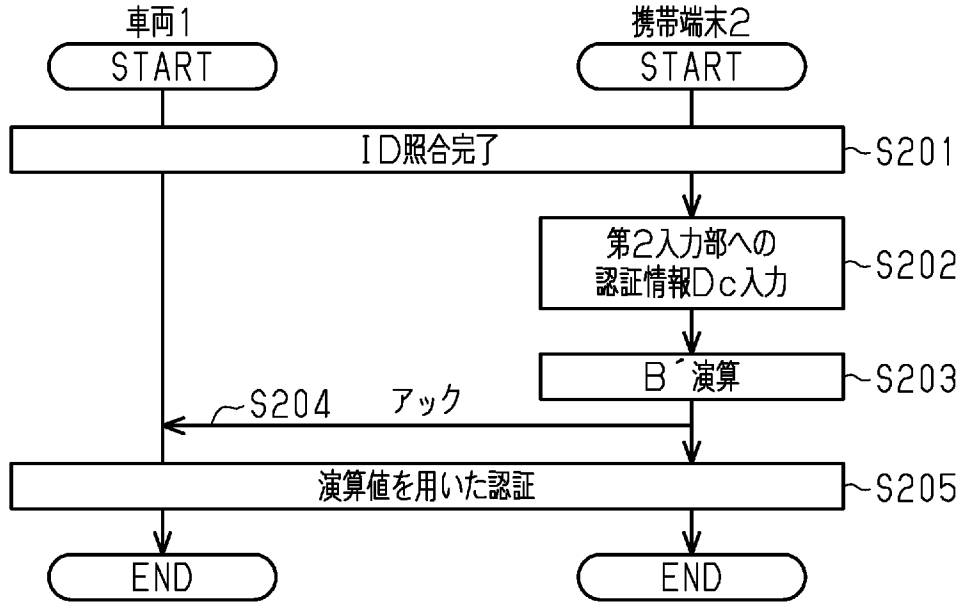
[図1]


2
携帯端末
22
21
20
端末制御部
第2演算部
34
認証部
40
(42)
32
第2入力部
Dc
23
B
メモリ
認証パラメータ
1
車両
8
車両側通信部
31
第1入力部
Dc
照合ECU
7
メモリ
A
認証パラメータ
第1演算部
33
認証部
40
(41)
5
6
車載器
4
3

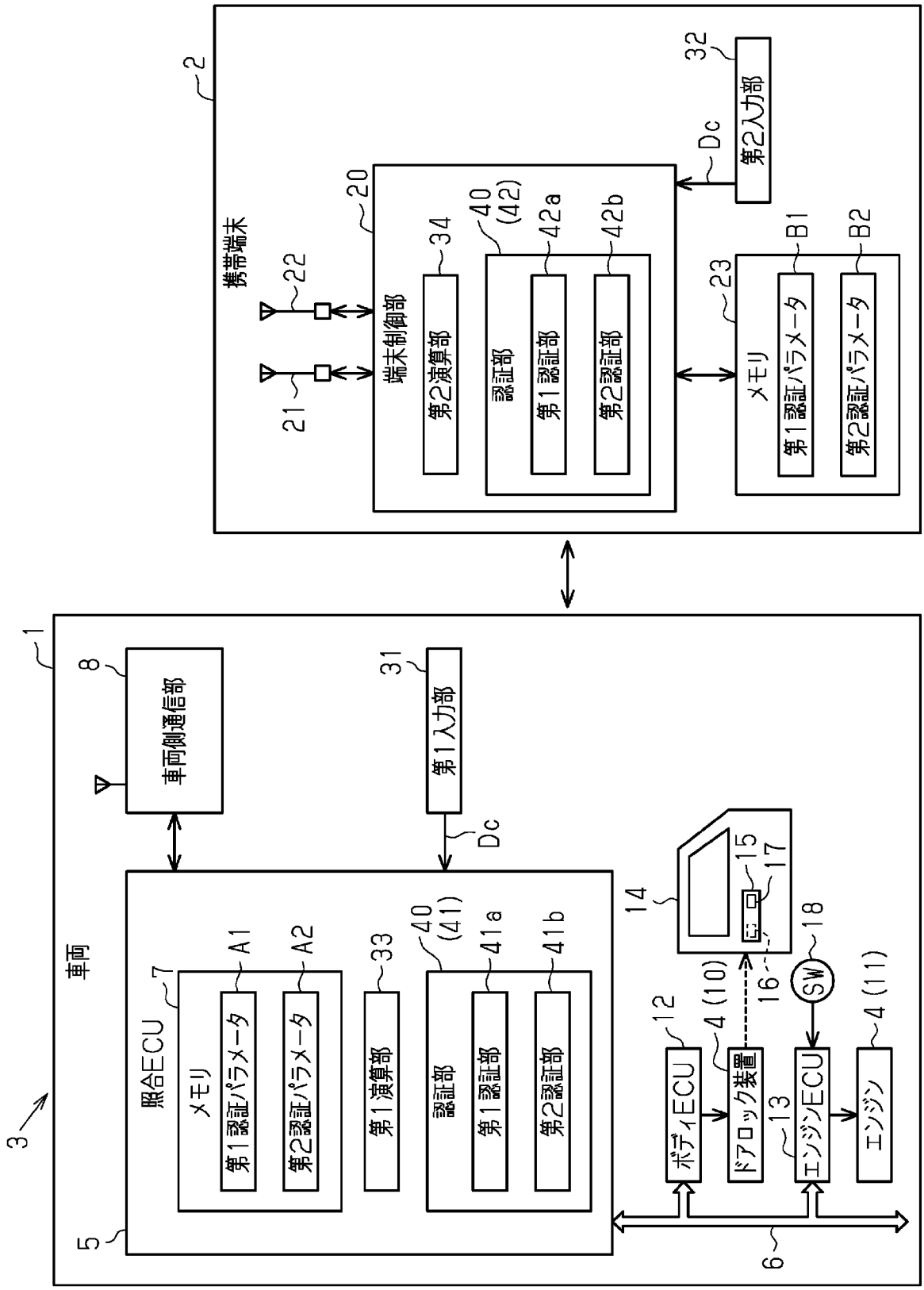
[図2]


車両1
START
携帯端末2
START
S101
アドバタイズ
応答
通信接続
S102
ID照合
S103
S104
第1入力部への
認証情報Dc入力
S105
A´演算
チャレンジ信号
S106
S107
レスポンス演算
レスポンス演算
S108
レスポンス信号
S109
S110
NO
レスポンスコード
が一致?
YES
車載機器の作動を許可
S111
END
END

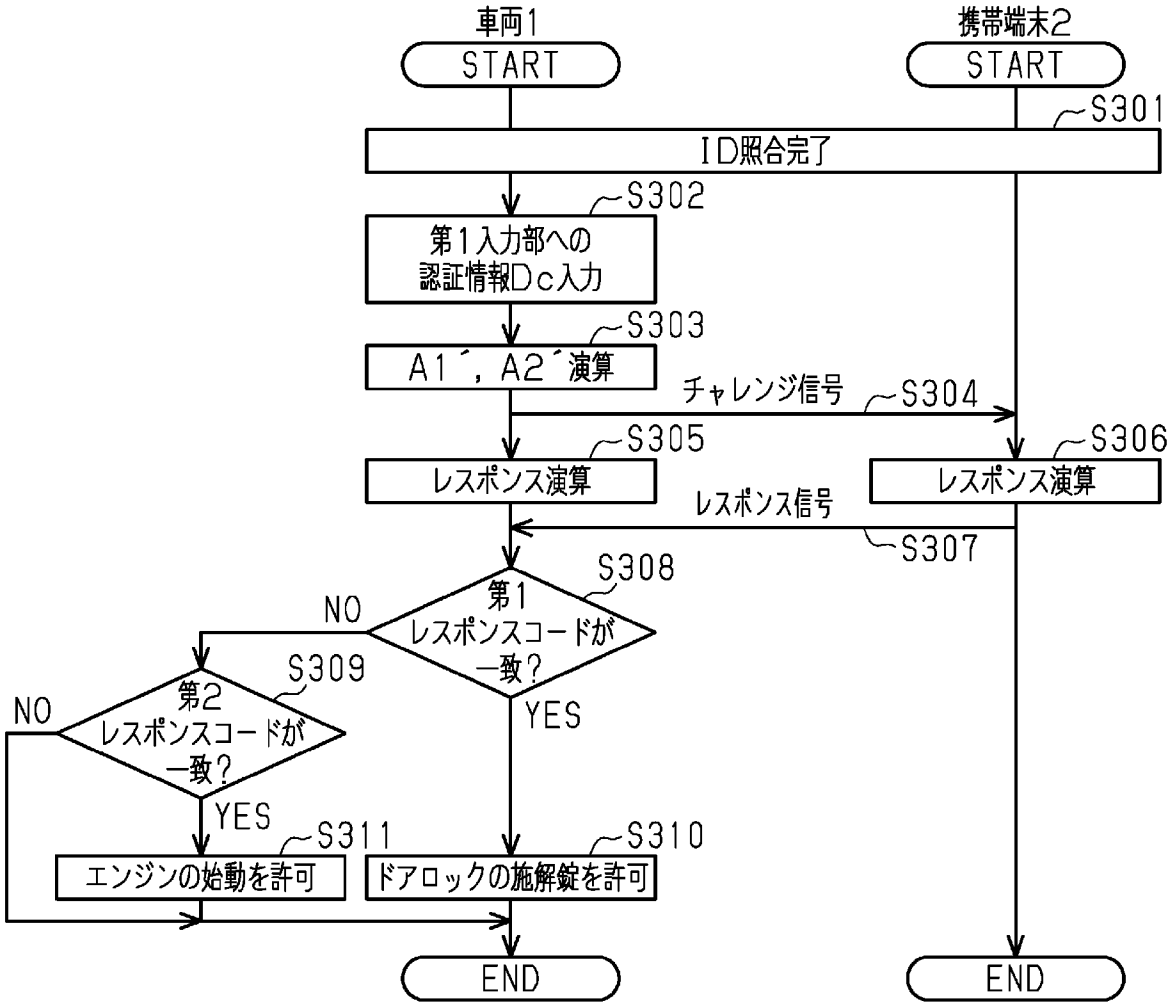
[図3]


車両1
START
携帯端末2
START
ID照合完了
S201
第2入力部への
認証情報Dc入力
S202
B´演算
S203
S204
アック
演算値を用いた認証
S205
END
END

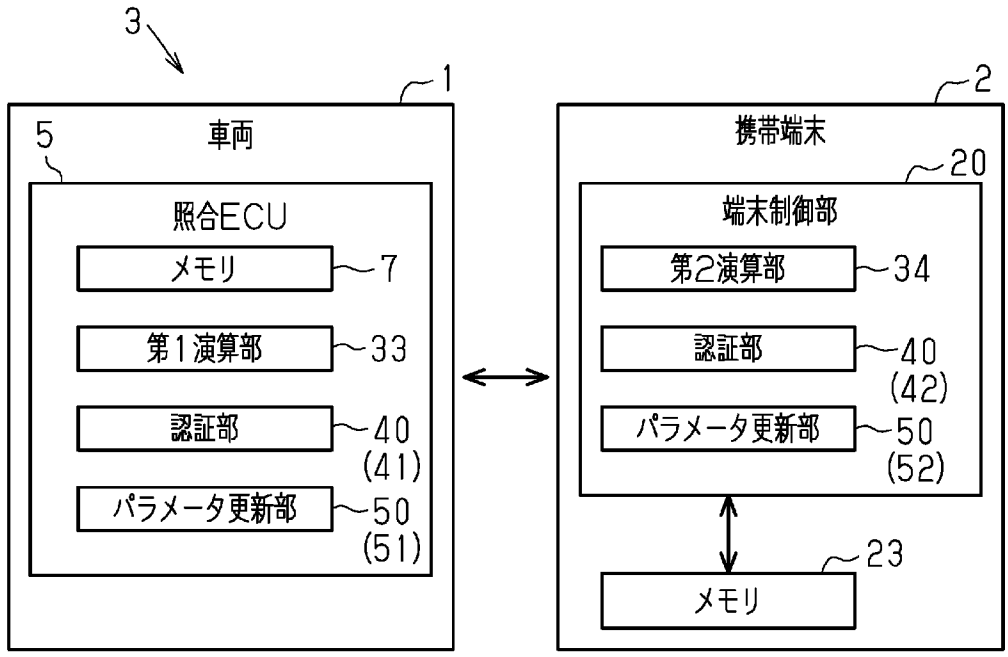
[図4]


2
携帯端末
22
21
20
端末制御部
第2演算部
34
40
(42)
認証部
第1認証部
42a
第2認証部
42b
32
第2入力部
Dc
23
メモリ
第1認証パラメータ
B1
第2認証パラメータ
B2
1
車両
8
車両側通信部
31
第1入力部
Dc
3
5
照合ECU
メモリ
第1認証パラメータ
A1
第2認証パラメータ
A2
7
第1演算部
33
40
(41)
認証部
第1認証部
41a
第2認証部
41b
14
15
17
SW
18
16
4 (10)
ドアロック装置
12
ボディECU
13
エンジンECU
4 (11)
エンジン
6

[図5]


車両1
携帯端末2
START
START
S301
ID照合完了
S302
第1入力部への
認証情報Dc入力
S303
A1´, A2´演算
チャレンジ信号
S304
S305
レスポンス演算
S306
レスポンス演算
レスポンス信号
S307
S308
第1
レスポンスコードが
一致?
NO
YES
S309
第2
レスポンスコードが
一致?
NO
YES
S311
エンジンの始動を許可
S310
ドアロックの施解錠を許可
END
END

[図6]


3
1
2
5
車両
携帯端末
20
照合ECU
端末制御部
メモリ
7
第2演算部
34
第1演算部
33
認証部
40
(41)
認証部
40
(42)
パラメータ更新部
50
(51)
パラメータ更新部
50
(52)
23
メモリ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/044488

A. CLASSIFICATION OF SUBJECT MATTER
H04L 9/32(2006.01)i; B60R 25/24(2013.01)i; G06F 21/31(2013.01)i
FI: H04L9/00 67511; G06F21/31; B60R25/24

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)
H04L9/32; B60R25/24; G06F21/31

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2012-193499 A (MITSUBISHI ELECTRIC CORP.) 11.10.2012 (2012-10-11)	1-6
A	JP 2017-076874 A (TOKAIRIKA, CO., LTD.) 20.04.2017 (2017-04-20)	1-6
A	WO 2005/041474 A1 (THE FOUNDATION FOR THE PROMOTION OF INDUSTRIAL SCIENCE) 06.05.2005 (2005-05-06)	1-6
A	JP 2005-252702 A (COMSQUARE CO., LTD.) 15.09.2005 (2005-09-15)	1-6

☐ 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	Date of mailing of the international search report
30 January 2020 (30.01.2020)	10 February 2020 (10.02.2020)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2019/044488

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2012-193499 A	11 Oct. 2012	DE 102011080435 A1	
JP 2017-076874 A	20 Apr. 2017	(Family: none)	
WO 2005/041474 A1	06 May 2005	US 2007/0061572 A1 CN 1871810 A KR 10-2006-0073647 A	
JP 2005-252702 A	15 Sep. 2005	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2019/044488

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/32(2006.01)i; B60R 25/24(2013.01)i; G06F 21/31(2013.01)i
FI: H04L9/00 675A; G06F21/31; B60R25/24

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））

H04L9/32; B60R25/24; G06F21/31

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	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０年

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

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2012-193499 A (三菱電機株式会社) 11.10.2012 (2012-10-11)	1-6
A	JP 2017-076874 A (株式会社東海理化電機製作所) 20.04.2017 (2017-04-20)	1-6
A	WO 2005/041474 A1 (財団法人生産技術研究奨励会) 06.05.2005 (2005-05-06)	1-6
A	JP 2005-252702 A (株式会社コムスクエア) 15.09.2005 (2005-09-15)	1-6

☐ 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抵触するものではなく、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	国際調査報告の発送日
30.01.2020	10.02.2020

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
田中　啓介 5S 3453
電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2019/044488

引用文献	公表日	パテントファミリー文献	公表日
JP 2012-193499 A	11.10.2012	DE 102011080435 A1	
JP 2017-076874 A	20.04.2017	（ファミリーなし）	
WO 2005/041474 A1	06.05.2005	US 2007/0061572 A1	
		CN 1871810 A	
		KR 10-2006-0073647 A	
JP 2005-252702 A	15.09.2005	（ファミリーなし）	