

(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
2024年2月8日(08.02.2024)



(10) 国際公開番号

WO 2024/029285 A1

(51) 国際特許分類:

G06F 21/35 (2013.01) E05B 49/00 (2006.01)
B60R 25/24 (2013.01)

(21) 国際出願番号: PCT/JP2023/025564

(22) 国際出願日: 2023年7月11日(11.07.2023)

(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 2022-124932 2022年8月4日(04.08.2022) 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: 浅井 健太郎 (ASAI Kentaro); 〒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). 戸川 英史 (TOGAWA Hideshi); 〒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). 松

下 傑 (MATSUSHITA Suguru); 〒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). 坂本 浩二 (SAKAMOTO Koji); 〒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).

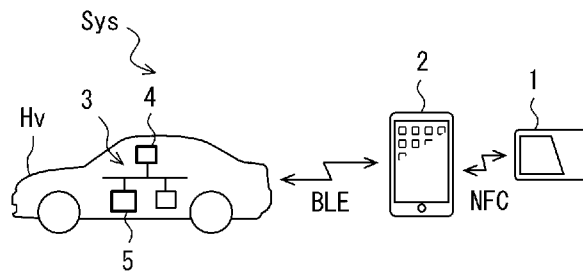
(74) 代理人: 矢作 和行, 外 (YAHAGI Kazuyuki et al.); 〒4600003 愛知県名古屋市中区錦2丁目13番19号 瀧定ビル3階 Aichi (JP).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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,

(54) Title: USER AUTHENTICATION METHOD, USER AUTHENTICATION DIGITAL KEY SYSTEM, AND MOBILE DEVICE PROGRAM

(54) 発明の名称: ユーザ認証方法、ユーザ認証デジタルキーシステム、携帯デバイス用プログラム

図1



(57) Abstract: A mobile device (2) establishes an NFC link with a card key (1) by the card key (1) being laid on the back surface part thereof. Further, the mobile device (2) is configured to be capable of performing BLE communication with a vehicle (Hv). The mobile device (2) plays the role of transferring a challenge code transmitted from the vehicle (Hv) by a BLE link to the card key (1) by NFC. The card key (1), when having received the challenge code from the mobile device (2), generates a response code from the challenge code using a vehicle key code saved in the card, and returns the response code to the mobile device (2). The mobile device (2) transfers the response code received by NFC to the vehicle (Hv) by BLE, thereby authenticating the user.

(57) 要約: 携帯デバイス(2)は、その背面部にカードキー(1)が重ねられることにより、カードキー(1)とNFCリンクを確立する。また、携帯デバイス(2)は車両(Hv)とBLE通信を実施可能に構成されている。携帯デバイス(2)は、車両(Hv)からBLEリンクで送信されるチャレンジコードを、NFCでカードキー(1)に転送する役割を担う。カードキー(1)は、携帯デバイス(2)よりチャレンジコードを受信すると、カード内部に保存されている車両鍵コードを用いてチャレンジコードからレスポンスコードを生成し、携帯デバイス(2)に返送する。携帯デバイス(2)が、NFCで受信したレスポンスコードをBLEで車両(Hv)に転送することで、ユーザ認証が行われる。

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))

明 細 書

発明の名称：

ユーザ認証方法、ユーザ認証デジタルキーシステム、携帯デバイス用プログラム

関連出願の相互参照

[0001] この出願は、2022年8月4日に日本に出願された特許出願第2022-124932号を基礎としており、基礎の出願の内容を、全体的に、参照により援用している。

技術分野

[0002] 本開示は、携帯デバイスとの無線通信によってユーザを認証する技術に関する。

背景技術

[0003] 特許文献1には、サーバが発行するトークン（使い捨ての鍵コード）を用いて車両が携帯デバイスを認証し、開錠／施錠などの車両制御を実施するシステムが開示されている。特許文献1における携帯デバイスは、スマートフォンなどのインターネット接続可能に構成された、ユーザによって携帯されるデバイスである。特許文献1に開示のように、携帯デバイスを車両の鍵として使用することができれば、ユーザは車両の使用に際し、専用の電子キーを所持する必要がなくなり、利便性がよくなる。

[0004] また、特許文献2には、携帯デバイスに固定の（使い捨てではない）鍵コードを保存しておくことにより、携帯デバイスを専用キーのように使用可能なスマートエントリーシステムも開示されている。なお、スマートエントリーシステムとは、専用キー／携帯デバイスが車載装置と自動的に無線通信による認証処理を行うことによって、ユーザが専用キー／携帯デバイスを操作することなく、ドアの開錠／施錠などの車両制御を行うシステムである。当該システムは、パッシブエントリー／パッシブスタート（Passive Entry / Passive Start：PEPS）システムなどとも呼ばれうる。

先行技術文献

特許文献

[0005] 特許文献1：特許2021-37889号公報

特許文献2：特開2020-100994号公報

発明の概要

[0006] 特許文献1に開示のように、サーバから携帯デバイスに鍵コードを配信するサーバベースのシステムでは、サーバ維持のための費用が発生しうる。一方、特許文献2に開示されるように、携帯デバイスそのものに、使い捨てではない／繰り返し利用可能な鍵コードを保存する構成では、ハッキングによって鍵コードが盗まれないよう、セキュリティソフトウェアの定期的なアップデートが必要となる。すなわち、スマートフォンそのものに鍵コードを保存する構成では、セキュリティ性確保のための費用が発生しうる。

[0007] 本開示は、上記の検討又は着眼点に基づいて成されたものであり、その目的の1つは、セキュリティを確保しつつ、システム維持のための費用を抑制可能なユーザ認証方法、ユーザ認証デジタルキーシステム、携帯デバイス用プログラムを提供することにある。

[0008] ここに開示されるユーザ認証方法は、通信可能距離が0.5m以上となる方式の無線通信である第1通信と、第1通信よりも通信可能距離が短い方式である第2通信と、を実施可能に構成されている携帯デバイスで使用されるアプリケーションであるデジタルキーアプリと、第1通信を実施可能に構成されてあって、ユーザ認証に使用される第1の鍵コードが保存された第1記憶装置を備える認証ユニットと、第2通信を実施可能に構成されてあって、第1の鍵コードと同じ値または関連する第2の鍵コードが保存された第2記憶装置を備えるキーモジュールと、によって実施されるユーザ認証方法であって、認証ユニットが、ユーザ認証のための第1データを、第1通信にてデジタルキーアプリに送信することと、デジタルキーアプリが、第1通信にて第1データを受信したことに基づき、キーモジュールと第2通信を実施することで、第1データと第2の鍵コードを用いて生成される第2データを取得

することと、デジタルキーアプリが、第2データを第1通信にて認証ユニットに送信することと、認証ユニットが、デジタルキーアプリから受信する第2データを用いて、ユーザ認証を実施することと、を含む。

[0009] 上記構成によれば、携帯デバイスは、キーモジュールと認証ユニットの通信を中継する装置として機能する。携帯デバイス自体には鍵コードは保存されていないため、携帯デバイスが紛失／ハッキングされた場合であっても、鍵コードが流出する恐れを低減できる。また、ユーザ側の鍵コードは、キーモジュールに保存されているため、デジタルキーサーバは省略可能となる。つまり、セキュリティを確保しつつ、システム維持のための費用を抑制可能となる。

[0010] 本開示のユーザ認証デジタルキーシステムは、通信可能距離が0.5 m以上となる方式の無線通信である第1通信と、第1通信よりも通信可能距離が短い方式である第2通信と、を実施可能に構成されている携帯デバイスで使用するアプリケーションであるデジタルキーアプリと、第2通信で携帯デバイスと通信可能に構成されているキーモジュールと、を含むユーザ認証デジタルキーシステムであって、デジタルキーアプリは、認証ユニットから第1通信にて送信される、ユーザ認証のための第1データを受信する第1データ受信部と、第1データ受信部が第1通信にて第1データを受信したことに基づき、キーモジュールに向けて、第1データを含むデータセットを第2通信にて送信する第1データ転送部と、を備え、キーモジュールは、ユーザ認証に使用される鍵コードが保存されたモジュール内記憶部と、デジタルキーアプリから第2通信にて第1データを受信したことに基づいて、モジュール内記憶部に保存されている鍵コードを用いて第1データから第2データを生成し、第2通信にて返送する応答回路と、を備え、デジタルキーアプリは、さらに、第2通信にてキーモジュールから返送されてくる第2データを受信する第2データ受信部と、第2データを第1通信にて認証ユニットに送信する第2データ送信部と、を備える。

[0011] 上記ユーザ認証デジタルキーシステムは、上記ユーザ認証方法を実施する

携帯デバイスとキーモジュールを要素とするシステムである。上記ユーザ認証デジタルキーシステムに依れば、上記ユーザ認証方法と同様の理由により、セキュリティを確保しつつ、システム維持のための費用を抑制可能となる。

[0012] 本開示の携帯デバイス用プログラムは、通信可能距離が0.5 m以上となる方式の無線通信である第1通信と、第1通信よりも通信可能距離が短い方式である第2通信と、を実施可能に構成されている携帯デバイスが備えるプロセッサに、認証ユニットから第1通信にて送信される、ユーザ認証のための第1データを受信することと、第1通信にて認証ユニットから第1データを受信したことに基づき、ユーザ認証に使用される鍵コードが登録されているキーモジュールと第2通信を実施することで、第1データと鍵コードを用いて生成される第2データを取得することと、第2データを第1通信にて認証ユニットに送信することと、を実行させるための命令を含む。

[0013] 上記携帯デバイス用プログラムは、第1通信及び第2通信可能に構成された一般的な携帯デバイスを、上記ユーザ認証法を実施する携帯デバイスとして機能させるためのプログラムである。

[0014] なお、請求の範囲に記載した括弧内の符号は、一つの態様として後述する実施形態に記載の具体的手段との対応関係を示すものであって、本開示の技術的範囲を限定するものではない。また、本開示は、鍵コード／車両の利用状況を管理するサーバであるデジタルキーサーバの設置を任意の要素とするものであって、デジタルキーサーバの導入を禁止するものではない。本開示は、デジタルキーサーバを含むシステム／方法に対しても適用可能である。

図面の簡単な説明

[0015] [図1]車両用デジタルキーシステムの全体像を説明するための図である。

[図2]カードキーの構成を示すブロック図である。

[図3]携帯デバイスの構成を示すブロック図である。

[図4]車載システムの構成を示すブロック図である。

[図5]BLE認証の概略的な流れを示すフローチャートである。

[図6]ユーザがB L E 認証を利用して車両を開錠する際の各デバイスの作動を説明するためのシーケンス図である。

[図7]携帯デバイスにおけるレスポンスコードの取得方法の変形例を示すシーケンス図である。

[図8]携帯デバイスにおける車両鍵コードの管理方法の変形例を説明するためのシーケンス図である。

[図9]カード認証サーバとの協働により携帯デバイスがN F Cで通信している相手の正当性を検証する構成を説明するためのフローチャートである。

[図10]携帯デバイスの機能ブロック図である。

[図11]チャレンジコードを受信した際にカードキーと通信不能である場合の携帯デバイスの作動を説明するためのフローチャートである。

[図12]カードキーとの接続維持時間にも基づいて応答停止状態に移行する制御態様を説明するためのフローチャートである。

発明を実施するための形態

[0016] 以下、本開示の実施形態について図を用いて説明する。図1は、車両用デジタルキーシステムS y sの概略的な構成の一例を示す図である。図1に示すように車両用デジタルキーシステムS y sは、カードキー1と、携帯デバイス2と、車載システム3と、を含む。車載システム3は、車両H vに搭載されたセンサ、モータ、及びE C U (Electronic Control Unit) を主体として構成されているシステムであって、車両H vのロック機構の状態（施錠／開錠）を制御する。車載システム3は、認証E C U 4と、統合E C U 5とを備える。

[0017] 車両H vは、個人によって所有される4輪自動車であってよい。本実施形態におけるユーザとは、車両H vの所有者（オーナー）、又はその家族などであってよい。車両H vは、外部充電可能な、いわゆるプラグインハイブリッド車といった、電動車であってよい。電動車の概念には、電気自動車の他、ハイブリッド車、及び燃料電池車も含まれる。尚、ハイブリッド車は動力源としてエンジンとモータを備える車両である。他の態様として車両H vは

、エンジン車であってもよい。以下の説明における前後、左右、上下の各方向は、基準方向に関する注釈がない場合には（つまり基本的には）、車両Hvを基準として規定される。

[0018] <全体概要>

携帯デバイス2と認証ECU4はそれぞれ、Bluetooth（登録商標） Low Energy（以降、BLE）に準拠した無線通信であるBLE通信を実施可能に構成されている。本開示におけるBLE信号とはBLE規格に準拠した無線信号を指す。携帯デバイス2と認証ECU4は、互いにペアリング処理がなされている。携帯デバイス2は、認証ECU4の通信エリア内に存在することに基づいて認証ECU4と通信接続する。

[0019] 以下では認証ECU4が携帯デバイス2との通信におけるマスターとして振る舞い、携帯デバイス2がスレーブとして振る舞うように設定されている場合について説明する。認証ECU4は携帯デバイス2からのアドバタイズ packetsを受信することで、携帯デバイス2との通信接続を確立し、車両Hvの周辺に携帯デバイス2（ひいてはユーザ）が存在することを検出する。アドバタイズ packetsは、自分自身の存在を他のデバイスに通知（すなわちアドバタイズ）するための信号である。尚、他の態様として、携帯デバイス2が認証ECU4との通信におけるマスターとして動作するように設定されていても良い。

[0020] また、携帯デバイス2とカードキー1は、近接場通信（NFC：Near Field Communication）を実施可能に構成されている。NFCは、通信可能距離が数cmから10cm程度となる通信を指す。NFCは、非接触通信／タッチ通信／略接触通信／超近距離通信などと呼ぶこともできる。NFCは、BLE通信よりも通信可能な距離が十分に小さい通信方式に相当する。通信可能な距離が十分に小さい通信方式とは、通信可能距離が10分の1以下となる通信方式を指す。NFCの規格は、ISO/IEC 18092（NFCIP-1）、ISO/IEC 21481（NFCIP-2）、ISO/IEC 14443、又はISO/IEC 18092といった、任意の規格であってもよい。NFCは、Type-F規格に適合するものであっても良いし、Type-

A又はType-B規格に適合するものであってもよい。Type-F規格は、NFCIP-1、JIS X 6319-4等で定められた方式であって、いわゆるFeliCa（登録商標）に相当する。なお、携帯デバイス2とカードキー1との通信は、セキュアエレメントを用いて実施されることが好ましい。

[0021] 携帯デバイス2は、NFCリーダ／ライタとしての機能を備え、定期的に／特定のイベントが生じた場合に、ポーリングコマンドを送信することで、カードキー1との通信接続を試行する。ポーリングコマンドは、通信可能範囲内にカードキー1が存在するか否かを調べるためのコマンドである。携帯デバイス2の裏面など、携帯デバイス2においてNFC通信用のアンテナが設けられている部分にカードキー1が重ねられている場合、携帯デバイス2はカードキー1との通信可能となりうる。

[0022] 携帯デバイス2は、カードキー1とのNFC通信に際し、データの返送を要求する側の端末、すなわちリーダ／アクティブデバイスとして動作する。また、カードキー1は、携帯デバイス2から受信したデータの内容に応じた信号を返送する、パッシブデバイスとして構成されている。具体的には、カードキー1は、携帯デバイス2から送信される信号の受信電力で駆動し、応答信号を生成及び返送する。

[0023] <カードキー1について>

カードキー1は、車両鍵コードが登録されたICカード（例えばクレジットカード）である。カードキー1がキーモジュールに相当する。キーモジュールは、車両鍵コードが保存された、携帯デバイス2とNFC通信可能な物体である。

[0024] 本開示における車両鍵コードは、車両Hvを利用するための電子的な鍵としてのコードである。車両鍵コードは、認証ECU4が、車両Hvを操作しようとしている人物の正当性、つまり、正規のユーザであることを確認するためのデータと解することができる。車両鍵コードは、128ビット又は256ビットなど、所定の長さを有する。車両鍵コードは、車両Hvとカードキー1の組み合わせ毎に異なる。車両鍵コードは、1つの局面においては、

パスワード又はP I N (Personal Identification Number) などといった、秘密の番号と解することができる。番号の概念には、数字以外の文字又は記号を組み合わせた文字列も含まれうる。また、車両鍵コードは、クレジットカード番号をもとに生成されたコードであってもよい。車両鍵コードは、クレジットカード番号と有効期限を連結させたビット列を所定のハッシュ関数に入力して得られるコードであっても良い。

[0025] 車両鍵コードは、車両 I D とユーザ I D を結合した値を所定のハッシュ関数に入力して得られる出力値であってもよい。車両 I D は車両ごとに割り当てられる固有の識別番号であって、車両識別コード (V I N : Vehicle Identification Number) などである。尚、車両鍵コードは、ユーザが登録した所定文字数のパスワードそのもの、又は、当該パスワードを所定のハッシュ関数に入れた値であっても良い。

[0026] 車両鍵コードは、車載 H M I (Human Machine Interface) に対するユーザ操作に基づいて認証 E C U 4 が発行しうる。クレジットカードへの車両鍵コードへの書き込みは、車載システム 3 が備える N F C 通信機のライタ機能を用いて実現される。なお、車両鍵コードの発行機能は、携帯デバイス 2 が備えていても良い。クレジットカードなどのキーモジュールの素材への車両鍵コードの書き込みも、携帯デバイス 2 を用いて実施可能に構成されても良い。その他、車両鍵コードは、所定のサーバによって発行され、携帯デバイス 2 又は認証 E C U 4 を介してクレジットカードに書き込まれても良い。クレジットカードが備える記憶装置に車両鍵コードが書き込まれることにより、本開示のカードキー 1 / キーモジュールとして機能する。なお、カードキー 1 に登録されている車両鍵コードと同一のコードは、認証 E C U 4 にも登録されている。

[0027] カードキー 1 は、図 2 に示すように、N F C アンテナ 1 1 と I C (Integrated Circuit) チップ 1 2 を含む。I C チップ 1 2 は、高周波回路 1 3、電源回路 1 4、R O M (Read Only Memory) 1 5、フラッシュメモリ 1 6、R A M (Random Access Memory) 1 7、C P U (Central Processing Unit) 1 8

を備える。ＩＣチップ１２が応答回路に相当する。

[0028] ＮＦＣアンテナ１１は、ＮＦＣで使用される周波数帯の電波を受信するための導体素子である。ＮＦＣアンテナ１１は、ループアンテナあるいはアンテナコイルである。ＮＦＣアンテナ１１は、ＩＣチップ１２の高周波回路１３と接続されている。ＮＦＣアンテナ１１は、携帯デバイス２とのデータの送受信に供される。また、ＮＦＣアンテナ１１は、携帯デバイス２から受信した信号に応じた電力をＩＣチップ１２に供給する役割を担う。

[0029] 高周波回路１３は、ベースバンド信号から高周波信号への変換及び逆変換にかかる処理を実施する回路モジュールである。ここでの高周波とは、ＮＦＣで使用される周波数帯（例えば１３．５６ＭＨｚ）と解されて良い。高周波回路１３は、ＮＦＣアンテナ１１で受信した高周波信号に対して復調等の受信処理を施し、受信データとしてＣＰＵ１８に出力する。また、高周波回路１３は、ＣＰＵ１８から入力されたデータを変調してＮＦＣアンテナ１１に出力し、無線送信させる。

[0030] 電源回路１４は、ＮＦＣアンテナ１１から入力される電力を、ＣＰＵ１８の駆動等に適した電圧に変換する回路モジュールである。ＲＯＭ１５には、ＯＳ（Operating System）又はアプリケーションなどといった、カードキー１向けのプログラムが格納されている、読み出し専用の記憶媒体である。フラッシュメモリ１６は、書き換え可能な不揮発性の記憶装置である。フラッシュメモリ１６は、車両鍵コードが保存されている記憶領域であるカード内格納部１６１を備える。カード内格納部１６１が第２記憶装置及びモジュール内記憶部に相当する。カード内格納部１６１に保存されている車両鍵コードが第２の鍵コードに相当する。ＲＡＭ１７は、書き換え可能な揮発性メモリである。

[0031] ＣＰＵ１８は、各種演算処理を行う演算コアである。ＣＰＵ１８等の回路は、ポーリングコマンドなど、ＮＦＣアンテナ１１が所定値以上の強度を有するＮＦＣ信号を受信したことに基づいて起動する。

[0032] ＣＰＵ１８は、携帯デバイス２から受信した信号に応じた応答を返送する

ための処理を実施する。CPU 18は、携帯デバイス2から通信要求を受信したことに基づいて、携帯デバイス2と通信接続／相互認証にかかるコマンド／データの送受信を実施する。

[0033] また、CPU 18は、携帯デバイス2からチャレンジコードを含むNFC信号を受信すると、チャレンジコードとカード内格納部161に保存されている車両鍵コードからレスポンスコードを生成する。CPU 18によるレスポンスコードの生成は、後述する認証ECU4が検証コードを生成するときと同じ方法で（換言すれば同じ生成関数を用いて）実施される。CPU 18は、生成したレスポンスコードをNFCで携帯デバイス2に返送する処理を行う。つまり、カードキー1は、チャレンジコードを受信すると、応答信号として、受信したチャレンジコードを車両鍵コードで暗号化したレスポンスコードを生成して返送するように構成されている。チャレンジコード及びレスポンスコードの送受信は、NDEF（NFC Data Exchange Format）で実施されても良い。レスポンスコードは、ユーザの正当性を証明するために認証ECU4に提出されるコードであるため、提出用認証コードと呼ぶこともできる。レスポンスコードが第2データに相当する。

[0034] <携帯デバイス2について>

携帯デバイス2は、BLE通信機能及びNFC機能を備えた、携帯可能かつ汎用的な情報処理端末である。携帯デバイス2は、スマートフォン又はウェアラブルデバイスであってよい。ウェアラブルデバイスは、ユーザの身体に装着されて使用される通信デバイスである。ウェアラブルデバイスは、リストバンド型、腕時計型、指輪型、メガネ型、イヤホン型など、多様な形状であってよい。本開示の携帯デバイス2は、スマートフォンなどの主機と、ウェアラブルデバイスなどの子機とに分けて実現されていても良い。

[0035] 携帯デバイス2は、図3に示すようにデバイス制御部20、ディスプレイ21、タッチパネル22、BLE通信部23、NFC通信部24、及びセルラー通信部25を備える。図中のCOMは通信部（通信モジュール）を表している。

- [0036] デバイス制御部20は、携帯デバイス2全体の動作を制御するモジュールである。デバイス制御部20は、デバイスプロセッサ201、メモリ202、ストレージ203等を備えた、コンピュータとして構成されている。デバイスプロセッサ201は、CPUであってよい。メモリ202は、RAMなどの揮発性記憶媒体である。ストレージ203は、フラッシュメモリ等の不揮発性の記憶媒体を含む構成である。また、デバイス制御部20は、アプリケーションソフトウェアとしてデジタルキーアプリ（以降、DKアプリ）204を備える。DKは、Digital Keyの略である。
- [0037] ディスプレイ21は、液晶ディスプレイ又は有機ELディスプレイであってよい。ディスプレイ21はデバイス制御部20からの入力信号に応じた画像を表示する。タッチパネル22は、静電容量式のタッチパネルであって、ディスプレイ21に積層されている。タッチパネル22は携帯デバイス2が備える入力装置である。
- [0038] BLE通信部23は、BLE通信を実施するための通信モジュールである。NFC通信部24はNFC用の通信モジュールである。本開示では、携帯デバイス2がカードキー1などのNFC媒体と通信可能な部位をカード読取位置と称する。携帯デバイス2におけるカード読取位置は、筐体の背面部、すなわちディスプレイ21の反対側に設けられていてよい。カード読取位置はNFC用のアンテナが形成されている部分に対応する。カード読取位置は、カードセット位置／NFC可能位置などと呼ぶこともできる。
- [0039] セルラー通信部25は、セルラー通信を実施するための通信モジュールである。本開示におけるセルラー通信とは、LTE（Long Term Evolution）／4G、5Gなど、移動体通信事業者が提供する携帯電話回線を利用した無線通信を指す。各種通信モジュールは、通信方式に応じたアンテナ、送受信回路、及びマイクロコンピュータを備えうる。
- [0040] DKアプリ204は、ユーザの認証、認証ECU4との通信、及びカードキー1との通信等をセキュアに行うためのアプリである。DKアプリ204は、ストレージ203などにインストールされている。

[0041] 本開示の「DKアプリ」との記載は、当該アプリケーションを実行する装置、デバイス制御部、携帯デバイス、又は、デバイスプロセッサと読み替えられてよい。同様に、以降における主語／目的語としての「携帯デバイス」との記載は、DKアプリ、デバイス制御部、又はデバイスプロセッサと読み替えられてよい。DKアプリ204が携帯デバイス用プログラムに相当する。

[0042] DKアプリ204は、ディスプレイ21、タッチパネル22、BLE通信部23、及び、NFC通信部24の作動を制御する。DKアプリ204は、BLE通信部23及びNFC通信部24の動作状態（アクティブ／非アクティブ）を切り替える。

[0043] なお、BLE通信部23がアクティブな状態とは、認証ECU4と通信するための機能が稼働している状態に相当する。アクティブ状態には、待受状態が含まれて良い。BLE通信部23が非アクティブな状態とは、BLE信号を受信できない状態であって、受信機能がオフに設定された状態に相当する。NFC通信部24がアクティブな状態とは、カードキー1と通信可能な状態であって、ポーリングコマンド又は疎通確認のためのコマンドを定期送信する状態に相当する。NFC通信部24が非アクティブな状態とは、カードキー1と通信不能な状態であって、通信接続／接続維持のためのコマンドの送信を停止している状態に相当する。NFC通信部24が非アクティブな状態は、NFC通信部24の電源をオフにした状態であってもよい。

[0044] また、DKアプリ204は、認証ECU4とBLE通信のリンク（コネクション）が確立したことに基づいて、認証ECU4とBLEによるデータ通信を実行する。DKアプリ204は、認証ECU4からBLE通信にて、チャレンジコードを受信した場合、カードキー1と通信することでカードキー1からレスポンスコードを取得する。そして、当該レスポンスコードをBLE通信にて認証ECU4に返送する。このように本実施形態における携帯デバイス2／DKアプリ204は、認証ECU4とカードキー1との通信を中継するデバイスとして振る舞いうる。

[0045] また、デバイス制御部20は、DKアプリ204の機能として、車両Hvのステータスを確認する画面である車両状態確認画面を表示可能に構成されていてもよい。車両状態確認画面は、ガソリン／バッテリーの残量、窓及びドアの開閉状態、施錠状態、又は車内温度などを示す画面であってよい。

[0046] さらに、デバイス制御部20は、車両Hvが備える電装設備の一部を遠隔操作可能に構成されていても良い。デバイス制御部20は、タッチパネル22に対するユーザ操作に基づき、車両Hvの施錠／開錠、空調装置のオン／オフ、窓の開閉、又はハザードランプの消灯を指示する無線信号を送信する。便宜上、車両Hvを施錠するための指示信号を施錠指示信号と称する。

[0047] 尚、携帯デバイス2は、BLE通信機能及びNFC機能を備える限りにおいて、車両Hvの電子キーとしての専用デバイスであるスマートキーであってもよい。スマートキーは、車両Hvの購入時に、車両Hvとともにオーナーに譲渡されるデバイスである。スマートキーは車両Hvの付属物の1つと解することができる。スマートキーは、扁平な直方体型、扁平な楕円体型（いわゆるフォブタイプ）、又はカード型など、多様な形状を採用可能である。スマートキーは、車両用携帯機、キーフォブ、アクセスキーなどと呼ばれる。

[0048] <車載システム3の構成について>

車載システム3は、図4に示すように、認証ECU4、統合ECU5、BLE通信機61、NFC通信機62、生体認証センサ63、ドアハンドルスイッチ64、ドアロックモータ65、走行用電源66、及び車載ディスプレイ67を備える。

[0049] 認証ECU4は、BLE通信機61、NFC通信機62、生体認証センサ63、ドアハンドルスイッチ64のそれぞれと専用の信号線で接続されている。また、認証ECU4は、統合ECU5及び車載ディスプレイ67と、車両内ネットワークNwを介して相互通信可能に接続されている。ドアロックモータ65及び走行用電源66は、統合ECU5と通信可能に接続している。車両内ネットワークNwは、車両Hv内に構築されている通信ネットワー

クである。車両内ネットワークNwの規格としては、多様な規格を採用可能である。図4に示す装置同士の接続形態は一例であって、具体的な装置同士の接続態様は適宜変更可能である。ドアハンドルスイッチ64は、統合ECU5と接続されていても良いし、車両内ネットワークNwを介して認証ECU4及び統合ECU5と接続されていてもよい。

[0050] 認証ECU4は、車両Hvにアクセスしようとしている人物が正規のユーザであるか否かの判定、すなわちユーザ認証を実行するECUである。認証ECU4が認証ユニットに相当する。認証ECU4は、コンピュータを用いて実現されている。すなわち、認証ECU4は、プロセッサ41、メモリ42、ストレージ43、入出力回路(I/O)44、及びこれらの構成を接続するバスラインなどを備えている。プロセッサ41は、CPU又はGPUなどといった、演算コアである。メモリ42は、RAMなどの揮発性メモリである。ストレージ43は、フラッシュメモリ等の不揮発性の記憶媒体を含む構成である。

[0051] ストレージ43は、車両鍵コードが保存されている記憶領域である車両鍵記憶部431を備える。車両鍵記憶部431が第1記憶装置に相当する。車両鍵記憶部431に保存されている車両鍵コードが第1の鍵コードに相当する。ストレージ43には、プロセッサ41によって実行される車両用認証プログラムが格納されている。プロセッサ41は、車両用認証プログラムを実施することにより、後述する各機能部の機能が実現される。プロセッサ41が車両用認証プログラムを実行することは、当該プログラムに対応するユーザ認証方法が実行されることに相当する。入出力回路44は、他装置と通信するための回路モジュールである。

[0052] ユーザ認証にかかる認証ECU4の作動の詳細は別途後述する。認証ECU4は、ユーザの認証状態(認証済み／未認証)を示す信号を、定期的に統合ECU5に入力する。本開示では、ユーザ認証が成功したことを示す信号を認証成功信号と称する。認証ECU4は、ユーザ認証が失敗した場合、ユーザ認証が失敗したことを示す認証失敗信号を統合ECU5に出力しても良

い。

[0053] 統合ECU5は、認証ECU4によるユーザ認証が成功していることを条件として、車両Hvへのユーザの操作内容に応じた車両制御を実施するECUである。統合ECU5は、車両制御として、車両Hvのアンロック／ロック、走行用電源66のオン／オフ切替などを実施する。

[0054] 統合ECU5は、ユーザ認証済みの状態においてドアハンドルスイッチ64が押下されたことに基づいて、車両Hvの各ドアに設けられたドアロックモータ65に向けて開錠指示信号を出力する。これにより統合ECU5は、各ドアのロック機構を施錠状態から開錠状態に切り替える。また、統合ECU5は、ユーザ認証済みの状態において、スタートスイッチが押下されたことに基づいて、走行用電源66をオフからオンに切り替える。さらに、統合ECU5はユーザ認証済みの状態においてユーザの施錠操作を検出したことに基づいて車両Hvを施錠する。

[0055] ユーザ認証済みの状態とは、ユーザ認証が成功している状態である。統合ECU5は、認証ECU4からの入力信号に基づいてユーザ認証済みの状態であるか否かを判断可能である。統合ECU5は、認証成功信号が入力されてから所定時間の間は、ユーザ認証済みとみなして作動してよい。統合ECU5は、認証成功信号から入力されている間のみ、ユーザ認証済みの状態と判定するように構成されていてもよい。

[0056] なお、ユーザ認証は後述するようにユーザ操作をトリガとして実行されてもよい。認証ECU4は、開錠操作等をトリガとしてユーザ認証処理を実施し、当該認証が成功したに基づいて統合ECU5が車両Hvを開錠してもよい。また、各種車両制御の実行条件には車両Hvに対するユーザ／携帯デバイス2の位置が含まれていても良い。施錠及び開錠にかかる制御は、車室外の所定距離以内に携帯デバイス2／ユーザが存在することを条件として実行されても良い。走行用電源のオンは、車室内に携帯デバイス2／ユーザが存在することが確認できていることを条件として実行されても良い。なお、統合ECU5は認証ECU4と一体化されていてもよい。車載システム3

内における機能配置は適宜変更可能である。

[0057] BLE通信機61はBLE通信を実施するための通信モジュールである。BLE通信機61は、認証ECU4からの制御信号に基づいて動作する。BLE通信機61は、携帯デバイス2から受信したデータ及び携帯デバイス2からの信号の受信状況に関するデータを、認証ECU4に提供する。また、BLE通信機61は、認証ECU4から入力されたデータを携帯デバイス2に向けて送信する。BLE通信機61は認証ECU4の筐体内に設けられていても良い。つまり、BLE通信機61は、認証ECU4に組み込まれていてもよい。また、車載システム3は複数のBLE通信機61を備えていても良い。

[0058] NFC通信機62は、NFC通信を実施するための通信モジュールである。NFC通信機62は、車両Hvの外面部と、車内の運転席付近に配置される。外面部におけるNFC通信機62の設置箇所としては、運転席側のBピラー／Cピラー／サイドミラー／外側ドアハンドルなどを採用可能である。複数のNFC通信機62のそれぞれの動作状態は、認証ECU4によって制御される。なお、NFC通信機62は任意の要素であって省略されてもよい。

[0059] 生体認証センサ63は、ユーザ認証に使用可能なユーザの生体情報を読み取るセンサである。ユーザ認証に使用可能なユーザの生体情報とは、指紋、静脈パターン、顔画像、虹彩パターン、又は声などであってよい。車載システム3は、生体認証センサ63として、指紋リーダ、静脈スキャナ、カメラ、及びマイクの何れか1種類、又は複数種類のセンサを備えうる。なお、指紋リーダは、指紋情報を読み取る装置であって、複数の電極が形成する静電容量の分布パターン、又は、当該分布パターンに基づいて定まる特徴点の分布パターンを示すデータを認証ECU4に出力する。静脈スキャナは、赤外線を用いて手又は指の静脈パターンを読み取る装置である。

[0060] 車載システム3は、車外指紋リーダと車内指紋リーダを備えていてよい。車外指紋リーダは、運転席用の外側ドアハンドルといった、車両Hvの外面

部に設けられた指紋リーダである。車外用指紋リーダは、車外に存在するユーザが車両Hvを施錠したり開錠したりするために供される。車内指紋リーダは、ステアリングホイール又はインストゥルメントパネルといった、車内の運転席周りに配置された指紋リーダである。生体認証センサ63は、認証ECU4の指示に基づいて起動し、認証対象とする人物（ターゲット）の生体情報を取得する。そして、取得できたターゲットの生体情報を示すデータである観測生体データを認証ECU4に出力する。なお、生体認証センサ63は任意の要素であって省略されてもよい。

[0061] ドアハンドルスイッチ64は、ユーザが車両Hvのドアを開錠及び施錠するための操作を検出するためのタッチセンサ／プッシュスイッチである。ドアハンドルスイッチ64は、車両Hvの外側ドアハンドルまたその近傍に設けられていてよい。なお、車載システム3は、ユーザの施錠／開錠操作を検出するためのセンサとして、ドア下モーションセンサを備えていても良い。ドア下モーションセンサは、ドア下の所定領域に向けて赤外線／超音波を送信することによってドア下に足がかざされたことを検出するセンサである。

[0062] ドアロックモータ65は、ドアのロック機構の状態（施錠、開錠）を切り替えるためのモータである。ドアロックモータ65はドアごとに設けられている。走行用電源66は、車両Hvが走行するための電源であって、車両がエンジン車である場合にはイグニッション電源を指す。車両Hvが電動車である場合、走行用電源66とはシステムメインリレーを指す。

[0063] 車載ディスプレイ67は、車両Hvに搭載された表示装置であって、液晶ディスプレイ又は有機ELディスプレイを用いて実現されている。車載ディスプレイ67は、インストゥルメントパネルの車幅方向の中央領域、又は、運転席の正面領域に配置されていてよい。車載ディスプレイ67は、車外の路面／サイドウィンドウに画像を投影するプロジェクタであっても良い。

[0064] なお、車載システム3は、上記以外にも多様なECU及びセンサを備える。認証ECU4及び統合ECU5には、多様な信号が入力される。認証ECU4及び統合ECU5は、スタートスイッチ、ブレーキペダルセンサ、シフ

トポジションセンサ、カーテシスイッチ、及び着座センサといった、多様なセンサの出力信号を受信しうる。スタートスイッチは、走行用電源66のオンオフを切り替えるためのプッシュスイッチであって、車内の運転席周りに配置されている。ブレーキペダルセンサは、ユーザによるブレーキペダルの踏み込み量／踏み込み力を示す信号を出力するセンサである。シフトポジションセンサはシフトの設定位置を示す信号を出力するセンサである。カーテシセンサは、ドアの開閉状態を示す信号を出力するセンサであって、ドアごとに配置されている。着座センサは座席に人間が座っているか否かを検出するセンサであって、少なくとも運転席に設けられている。

[0065] <BLE認証処理について>

認証ECU4は、BLE通信機61との協働により、BLE通信によるユーザ認証処理であるBLE認証処理を実施する。なお、携帯デバイス2及びカードキー1はユーザに紐づく。そのため、認証ECU4が車両鍵コードを用いて通信相手（携帯デバイス2／カードキー1）の正当性を検証すること、すなわち携帯デバイス2／カードキー1を認証することは、ユーザを認証することに相当する。本開示におけるユーザ認証は、適宜、デバイス認証又はコード認証と読み替えられてよい。

[0066] BLE認証処理は、前述の通りチャレンジレスポンス方式であって実施されうる。無線認証処理は、図5に示すように、ステップS11～S14を含んでいてよい。図5に示す各ステップの実行主体は何れも認証ECU4である。なお、システム全体の作動としては、携帯デバイス2がチャレンジコードを受信するステップ、受信したチャレンジコードを携帯デバイス2がカードキー1に転送するステップ、及び携帯デバイス2がカードキー1からレスポンスコードを受信して認証ECU4に返送するステップなどが存在しうる。

[0067] ステップS11は、携帯デバイス2に向けて、BLEにてチャレンジコードを送信するステップである。チャレンジコードは、予め用意された乱数表を用いて生成される所定長の乱数であってよい。チャレンジコードは、認証

ＥＣＵ４が備える現在時刻情報（いわゆるシステム時刻）をＳＥＥＤとして用いて生成された乱数であっても良い。チャレンジコードは多様な方法で決定されうる。チャレンジコードを含むデータセットが第１データに相当する。

[0068] ステップＳ１２は、認証ＥＣＵ４に保存されている車両鍵コードと、携帯デバイス２に送信したチャレンジコードとを用いて所定の手順により検証コードを生成するステップである。検証コードは、レスポンスコードの正当性、ひいては車両Ｈｖを利用しようとしている人物の正当性を検証するためのコードである。検証コードは、検証用認証コードと呼ぶこともできる。

[0069] ステップＳ１３は、携帯デバイス２から送信されるレスポンスコードを受信するステップである。ステップＳ１４は、携帯デバイス２から返送されてきたレスポンスコードと検証コードとを照らし合わせるステップである。認証ＥＣＵ４は、検証コードと受信したレスポンスコードが一致している場合に、認証ＥＣＵ４はユーザ認証成功と判定する。

[0070] なお、コード照合処理（Ｓ１４）の内容は、受信したレスポンスコードを、認証ＥＣＵ４に保存されている車両鍵コードを用いて復号することによって、元のチャレンジコードが得られるか否かを判定する処理であってもよい。その場合、検証コードの生成ステップ（Ｓ１２）は省略されてもよい。また、無線通信によるユーザ認証方法は、チャレンジレスポンス方式に限定されず、多様な方法を採用可能である。

[0071] 認証ＥＣＵ４は多様なタイミング／条件で上記のＢＬＥ認証処理を実行しうる。認証ＥＣＵ４は、ＢＬＥ通信機６１と携帯デバイス２との通信接続が確立したことをトリガとしてＢＬＥ認証処理を実行してもよい。認証ＥＣＵ４は、ＢＬＥ通信機６１と携帯デバイス２とが通信接続している間、所定の周期でＢＬＥ認証処理を実施するように構成されていても良い。

[0072] また、認証ＥＣＵ４は、所定の認証イベントを検出したことに基づいて、ＢＬＥ認証処理のための通信を実施してもよい。認証イベントとしては、施錠操作、開錠操作、始動操作、ドア閉、ブレーキ踏込などである。施錠操作

は、走行用電源 6 6 がオフ且つ全てのドアが閉じられた状態でドアハンドルスイッチ 6 4 をタッチする行為を指す。開錠操作は、走行用電源 6 6 がオフ且つ全てのドアが閉じられた状態で外側ドアハンドルをタッチする行為、又は、ドア下に足をかざす行為であってよい。始動操作とは、ブレーキペダルを踏み込んだ状態で、スタートスイッチを押下する行為を指す。ドア閉は、ドアを閉じる行為を指す。認証 E C U 4 は、車両 H v に搭載されている種々のセンサからの入力信号に基づいて、各種ユーザの行為を検出する。なお、上記ユーザ行為の検出機能は、統合 E C U 5 が備えていても良い。認証 E C U 4 は統合 E C U 5 から要求に基づいてユーザ認証を実施するように構成されていても良い。携帯デバイス 2 との通信リンクの確立も認証イベントに含めることができる。

[0073] <その他の方式の認証処理について>

本実施形態の認証 E C U 4 は、より好適な例として、N F C を用いたユーザ認証である N F C 認証処理又は、生体情報を用いたユーザ認証である生体認証処理を実施可能に構成されている。N F C 認証処理又は生体認証処理は、B L E 認証が失敗した場合、又は、B L E 認証が不能である場合のバックアップ（つまり代替認証手段）に相当する。

[0074] N F C 認証処理は、携帯デバイス 2 を介さずに、車両 H v がカードキー 1 と直接的に通信することにより、カードキー 1 からレスポンスコードを受信する方式に相当する。B L E 認証処理と N F C 認証処理は、認証 E C U 4 にとって直接的な通信相手となるデバイス及び通信方式が異なるだけである。N F C 認証の手順は、概略的には B L E 認証と同様であってよい。生体認証処理は、生体認証センサ 6 3 から受信する観測生体データと、事前にストレージ 4 3 に登録されているユーザの生体情報とを比較することで、ターゲットがユーザかどうかを判定する処理である。

[0075] <デバイス位置の判定>

車両用認証プログラムは、ユーザ認証を実施するためのプログラムに加えて、デバイス位置を判定するプログラムであるデバイス位置確認プログラム

を含んでいてもよい。つまり認証ECU4は、デバイス位置を判定する機能も備える。本開示におけるデバイス位置とは、車両に対する携帯デバイス2の位置を指す。携帯デバイス2はユーザによって携帯されるものであるため、デバイス位置を判定することはユーザの位置を判定することに相当する。

[0076] 認証ECU4は、BLE通信機61から取得する携帯デバイス2からの信号の受信強度に基づいてデバイス位置を判定しても良い。また、認証ECU4は、携帯デバイス2と双方向通信を実施することで測距値を算出し、当該測距値を用いて車両Hvから所定距離（例えば1.5m）以内にユーザが存在するか否かを判定してもよい。測距値は、BLE通信機61から携帯デバイス2までの距離を示すパラメータであって、電波の飛行時間（ToF: Time of Flight）に対応しうる。

[0077] なお、車載システム3が、アンカーとして複数のBLE通信機61を備える場合、複数のBLE通信機61のそれぞれで観測される受信強度／測距値と、各BLE通信機61の搭載位置情報を用いて、車両Hvに対するデバイス位置座標を算出してもよい。デバイス位置座標の算出は、GPS及び位置推定の技術分野における3点測位あるいは多点測位と同様の手法により実施可能である。認証ECU4は、エリア判定を行うものであってもよいし、デバイス位置座標を算出するものであっても良い。エリア判定とは、車外遠方、車外近傍、車内といった、車両Hvに事前に設定されている複数のエリア／ゾーンの何れかに携帯デバイス2が存在するかを判定することを指す。

[0078] <BLE認証の流れについて>

ユーザがBLE認証を利用して車両Hvにアクセスする場合には、携帯デバイス2のカード読取位置にカードキー1を重ねた状態で車両Hvに接近し、ドアハンドルスイッチ64を押下／タッチするといった一連のアクションが想定される。以下、上記一連のアクションに付随する認証ECU4及び携帯デバイス2及びカードキー1の作動について図6を用いて説明する。

[0079] まず、前提として携帯デバイス2は、カードキー1と通信接続していない

場合には、定期的に、N F C 通信部 2 4 から所定のポーリングコマンドを送信する（S 2 1）。ユーザが携帯デバイス 2 のカード読取位置にカードキー 1 を重ねると、カードキー 1 は、N F C 通信部 2 4 から発せられる電磁界をもとに起動し（S 2 2）、携帯デバイス 2 との N F C 通信リンクを確立する（S 2 3）。N F C 通信リンクが確立している状態とは、相互認証が完了している状態と解する事ができる。本開示では、携帯デバイス 2 のカード読取位置にカードキー 1 を重ねるユーザのアクションを重ね合わせ操作と称する。携帯デバイス 2 は、N F C 通信部 2 4 がカードキー 1 から応答信号を受信したことに基づいて重ね合わせ操作を検出する。

[0080] 携帯デバイス 2 は、カードキー 1 と通信接続したことに基づいて、カードキー 1 と通信可能であることをユーザに通知する（S 2 4）。当該通知は、所定の通知音／効果音をスピーカから出力したり、ディスプレイ 2 1 に所定のアイコン／メッセージを表示したりすることで実現されうる。

[0081] 携帯デバイス 2 は、カードキー 1 と N F C 通信可能となった時刻であるカード接続時刻をストレージ 2 0 3 あるいはメモリ 2 0 2 に記録しても良い。カード接続時刻は、携帯デバイス 2 のカード読取位置にカードキー 1 が重ねられた時刻に対応する。なお、本実施形態の携帯デバイス 2 は、カードキー 1 と N F C 通信可能となった場合には、定期的にカードキー 1 と疎通確認のための信号（コマンド）を送受信することにより、接続状態を維持する。換言すれば、携帯デバイス 2 は、カードキー 1 と N F C 通信可能な状態が維持されているか否かを定期的に確認する。本開示ではステップ S 2 1 ～ S 2 4 を、デバイスキー接続シーケンスとも称する。

[0082] 一方、認証 E C U 4 は、デバイスキー接続シーケンスとは独立して、車両ーデバイス接続シーケンスを実施する。認証 E C U 4 は、定期的にスキャン処理を実施してよい（S 2 5）。スキャン処理は、携帯デバイス 2 を検出するための処理である。スキャン処理は、B L E 規格に準拠した方式で実施されてよい。認証 E C U 4 はパッシブスキャン方式にて車両 H v の周辺に存在する携帯デバイス 2 を探索してよい。なお、認証 E C U 4 は、スキャン要

求の送信を伴うアクティブスキャン方式によって携帯デバイス2を探索しても良い。2種類のスキャン方式はシーンによって使い分けられても良い。駐車中の待機シーンにおいては、認証ECU4はパッシブスキャン方式で携帯デバイス2を探索する。一方、認証ECU4は、ドアハンドルスイッチ64の押下などの所定のイベントを検出した時にはアクティブスキャン方式で携帯デバイス2を探索しても良い。スキャン処理は、所定の認証イベントが発生したことに基づいて実施されても良い。

[0083] 認証ECU4はスキャン処理によって携帯デバイス2を発見できた場合には(S25A YES)、携帯デバイス2とBLE通信リンクを確立する(S26)。なお、認証ECU4が携帯デバイス2とBLE通信可能となる場合とは、ユーザが車両Hvの近くに接近した場合に対応しうる。本開示ではステップS25~26を車両ーデバイス接続シーケンスとも称する。

[0084] その後、認証ECU4は、ドアハンドルスイッチ64からの入力信号に基づきユーザによって開錠操作が行われたことを検出すると、チャレンジコードを含むBLE信号を携帯デバイス2に送信する(S31A)。また、認証ECU4は、携帯デバイス2に向けて送信したチャレンジコードと、認証ECU4にローカル保存されている車両鍵コードを用いて検証コードを生成する(S32)。

[0085] 携帯デバイス2は、認証ECU4からチャレンジコードを受信すると(S31B)、当該コードをNFC通信でカードキー1に転送する(S33A)。チャレンジコードを含む信号は、レスポンスコードの生成を要求する信号として機能しうる。チャレンジコードを含む信号は、認証要求信号と呼ぶことができる。ステップS33Aにおける携帯デバイス2は、BLE規格に準拠した認証要求信号を、NFC規格に準拠した信号に変換してカードキー1に送信する構成に相当する。

[0086] カードキー1は、NFCで携帯デバイス2からチャレンジコードを受信すると(S33B)、当該チャレンジコードと、カード内格納部161に保存されている車両鍵コードを用いてレスポンスコードを生成する(S34)。

そして、カードキー 1 は、自分で生成したレスポンスコードを N F C で携帯デバイス 2 に送信する (S 3 5 A) 。

[0087] 携帯デバイス 2 は、カードキー 1 からレスポンスコードを受信すると (S 3 5 B) 、当該コードを B L E 通信で認証 E C U 4 に転送する (S 3 6 A) 。レスポンスコードを含む信号は、ユーザ認証にかかる認証 E C U 4 からの要求に応答する信号であるため、認証応答信号と呼ぶこともできる。ステップ S 3 6 A における携帯デバイス 2 は、N F C 規格に準拠した認証応答信号を、B L E 規格に準拠した信号に変換して認証 E C U 4 に送信する構成に相当する。

[0088] 認証 E C U 4 は、携帯デバイス 2 からレスポンスコードを受信すると (S 3 6 B) 、当該受信したレスポンスコードと、ステップ S 3 2 で事前に生成しておいた検証コードとが一致するか否かを判定する (S 3 7) 。認証 E C U 4 にとっての通信相手が、カードキー 1 と接続された携帯デバイス 2 である場合には、2 つのコードは一致するはずである。また、カードキー 1 と接続された携帯デバイス 2 が車両 H v 周辺に存在することは車両 H v を使用しようとしている人物がユーザであるとの推定が働く。よって、認証 E C U 4 は、受信したレスポンスコードが検証コードと一致する場合には、ユーザ認証を成功と判定する。一方、認証 E C U 4 は、受信したレスポンスコードが検証コードと一致しない場合には、ユーザ認証を失敗と判定する。なお、認証 E C U 4 はチャレンジコードを送信してから所定の応答待機時間が経過してもレスポンスコードを受信できなかった場合にも、認証失敗と判定しうる。本開示ではステップ S 3 1 A ~ S 3 7 を B L E 認証シーケンスとも称する。

[0089] 認証 E C U 4 は、ステップ S 3 7 でのコード照合が完了すると、認証結果を示す信号を統合 E C U 5 に送信する。仮に統合 E C U 5 は、認証成功信号が入力された場合には、車両 H v を開錠する。なお、統合 E C U 5 は、認証失敗信号が入力された場合には、車載ディスプレイ 6 7 に、B L E 認証が失敗したことを示す画像である認証失敗画像を表示してもよい。また、統合 E

C U 5 は、所定の B L E 信号を携帯デバイス 2 に送信することにより、携帯デバイス 2 のディスプレイ 2 1 に認証失敗画像を表示させても良い。当該構成によればユーザは、携帯デバイス 2 を用いた無線認証、換言すれば B L E 認証が失敗したことを認識可能となる。

[0090] <上記構成の効果について>

上記説明の通り、本実施形態における B L E 認証処理は、認証 E C U 4 が携帯デバイス 2 を介してカードキー 1 と通信する方式に相当する。携帯デバイス 2 は、カードキー 1 と認証 E C U 4 との通信を中継する役割を担う。

[0091] 携帯デバイス 2 には、車両鍵コードが保存されていないため、携帯デバイス 2 のカード読取位置にカードキー 1 が重ねられていない場合、携帯デバイス 2 は車両鍵コードにもアクセスできない。また、カードキー 1 が携帯デバイス 2 から離れている場合、カードキー 1 はインターネットなどの広域ネットワークから物理的に切り離された状態となる。

[0092] 故に、カード読取位置にカードキー 1 が重ねられていない場合には、仮に携帯デバイス 2 がハッキングされた場合であっても、車両鍵コードが盗まれることはない。つまり、車両鍵コードがハッキングによって盗まれる恐れを低減可能となる。またカードキー 1 が携帯デバイス 2 のカード読取位置から離れた態様でユーザに所持／保管されている状況においては、リレーアタック等によってユーザ以外の人物である第 3 者が車両 H v とカードキー 1 の通信を不正に成立させることは困難である。

[0093] また、カード読取位置にカードキー 1 が重ねられた状態においては、携帯デバイス 2 は、特許文献 2 に開示のパッシブエントリ／パッシブスタート（P assive Entry / Passive Start : P E P S）システムを実現するための専用キーと同様に機能する。すなわち、ユーザは、携帯デバイス 2 を操作することなく、車両 H v の開錠又は施錠、電源オンなどを実施可能となる。

[0094] 本実施形態の構成によれば、ユーザの都合／判断に応じてカード読取位置とカードキー 1 を重ねたり離したりすることで、B L E 認証機能の有効／無効を変更できる。そのため、ユーザの利便性とセキュリティ性を両立可能と

なる。ユーザは車両Hvを使う時間帯、及び、相対的に盗難のリスクが低い環境に駐車している場合には、カード読取位置にカードキー1を重ねた状態を維持することで利便性を高めることができる。また、夜間や、商業施設／レストランの駐車場など、盗難のリスクが高いシーンにおいては、ユーザはカード読取位置からカードキー1を離しておくことにより、リレーアタックによって車両Hvが盗難される恐れを低減できる。

[0095] 加えて、本実施形態の構成では、携帯デバイス2を車両Hvの鍵として機能させるために、携帯デバイス2がデジタルキーサーバとデータ通信を実施する必要がない。本実施形態の構成によればデジタルキーサーバを省略可能となる。ひいては、デジタルキーサーバの維持費及びセキュリティ対策費が不要となる。よって、システム全体としての維持費等を低減可能となる。なお、デジタルキーサーバは、携帯デバイス2に車両Hvを使用するための一時的な認証鍵を配信するサーバである。

[0096] また、携帯デバイス2及び認証ECU4は、車両Hvの開錠等に際してデジタルキーサーバとデータ通信を実施する必要がないため、セルラー通信の圏外などにおいても、ユーザは携帯デバイス2を車両Hvの鍵として利用可能となる。さらに、本実施形態の構成によれば携帯デバイス2及び認証ECU4は、セルラー通信機能を備えなくともよいといった利点を有する。

[0097] また、上記構成によれば、認証ECU4は、特許文献2に開示されるような、携帯デバイス2自身が車両鍵コードを保持している場合と同様の機能を備えていれば良い。特許文献2に開示の構成に対し、車載システム3については特別なハードウェア／ソフトウェアを追加する必要がない。つまり、本実施形態の構成によれば車載システム3の製造コストの増大を抑制しつつ、セキュリティを高めることが可能となる。

[0098] 上記構成によれば、カードキー1の内部でレスポンスコードが生成されるため、車両鍵コードが通信ラインに乗らない。すなわち、車両鍵コードの登録時以外において、車両鍵コードがデバイス間で送受信されるシーンが発生しない。よって、後述する変形例(1)として述べる構成よりも、高いセキ

セキュリティを実現可能となる。

[0099] また、比較構成としては、上記のBLE認証を備えずに、NFC認証のみに対応している車載システムも考えられる。当該比較構成では、ユーザは、車両を利用するたびにカバン又はポケットからカードキー1を取り出して、車両のNFC通信部にかざす必要がある。そのような課題に対し、本実施形態の構成によれば、携帯デバイス2のカード読取位置にカードキー1を重ねておけば、カードキー1を取り出すことなく、開錠等を実施可能となるといった利点を有する。

[0100] また、本実施形態の構成では、車両HvがNFC通信機62を備える事により、バックアップ手段として、NFC認証も実施可能に構成されている。当該構成によれば、携帯デバイス2の電池切れ、BLE通信機61の不調、又はBLE通信部23の不調などによってBLE認証が実施できない場合でも、ユーザは車両Hvを利用可能となる。

[0101] 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、以降で述べる種々の変形例も本開示の技術的範囲に含まれる。また、本開示の構成は、下記以外にも要旨を逸脱しない範囲内で種々変更されてよい。下記の種々の補足や変形例などは、技術的な矛盾が生じない範囲において適宜組み合わせて実施されてよい。以上で述べた部材と同一の機能を有する部材については、同一の符号を付し、その説明を省略することがある。また、構成の一部のみに言及している場合、他の部分については上記説明が適用されてよい。

[0102] <変形例(1)>

上述した実施形態ではカードキー1がレスポンスコードを生成して携帯デバイス2に送信する態様を例示したが、携帯デバイス2がレスポンスコードを取得する方法はこれに限定されない。図7に示すように携帯デバイス2自身が、カードキー1から車両鍵コードを受信し、レスポンスコードを生成してもよい。図7に示すシーケンスは、図6のステップS31B～S35Bの代替処理であって、携帯デバイス2はカードキー1とNFC通信可能な状態

となっていることを条件として実行される。

[0103] 図7に示すステップS41は、携帯デバイス2が認証ECU4からBLEでチャレンジコードを受信したか否かを判定するステップである。認証ECU4とのBLE接続している間、ステップS41は定期的の実施されうる。なお、図7に示すステップS42A以降のシーケンスは、携帯デバイス2が認証ECU4からBLEでチャレンジコードを受信したことをトリガとして実行されても良い。

[0104] 携帯デバイス2は、認証ECU4からチャレンジコードを受信すると（S41 YES）、カードキー1に対して、車両鍵要求信号をNFCで送信する（S42A）。車両鍵要求信号は、車両鍵コードを送信するように要求するNFC信号である。カードキー1は、携帯デバイス2から車両鍵送信用要求信号を受信すると、カード内格納部161に保存されている車両鍵コードを読み出し（S43）、NFCで携帯デバイス2に送信する（S44A）。

[0105] 携帯デバイス2は、カードキー1から車両鍵コードを受信すると（S44B）、受信した車両鍵コードを用いてレスポンスコードを生成する（S45）。また、携帯デバイス2は、レスポンスコードの生成が完了次第、カードキー1から受信した車両鍵コードのデータをデバイス内から削除する（S46）。携帯デバイス2は、レスポンスデータの生成後、1秒以内にメモリ202に保持されている車両鍵コードを削除してよい。なお、携帯デバイス2は、カードキー1に受信した車両鍵コードは、RAMなどの一時メモリに保存しか保存できないように制限されていてもよい。その後、携帯デバイス2は、レスポンスコードをBLEで認証ECU4に送信する（S47）。

[0106] 上記の構成は、1つの局面において、カードキー1に車両鍵コードを書き込んでおき、レスポンスコードを生成する必要が有るときのみ、携帯デバイス2がカードキー1から車両鍵コードを読み出す構成に相当する。当該構成によっても、携帯デバイス2が車両鍵コードを保持している時間を一時的に限定できるため、携帯デバイス2に車両鍵コードを常時保存する構成に比べてセキュリティを高めることができる。

[0107] <変形例（２）>

上記変形例（１）のさらなる変形例として、図８に示すように携帯デバイス２は、チャレンジコードの受信有無に関わらずに、カードキー１と通信接続したタイミングでカードキー１から車両鍵コードを取得し、一定時間保存するように構成されていても良い。図８のステップＳ５１は、カードキー１と通信接続したか否かを判定するステップである。ステップＳ５２Ａは、携帯デバイス２がカードキー１とＮＦＣ通信可能となったことに基づいて、カードキー１に車両鍵要求信号を送信するステップである。カードキー１は、前述の通り、車両鍵要求信号を受信したことに基づいて（Ｓ５２Ｂ）、カード内格納部１６１から車両鍵コードを読み出して（Ｓ５３）、携帯デバイス２に送信する（Ｓ５４Ａ）。

[0108] ステップＳ５５は、携帯デバイス２が、カードキー１から受信した車両鍵コードをメモリ２０２に保存するとともに、保存時刻を記録するステップである。ステップＳ５６は、保存時刻からの経過時間が所定の保管時間を超過したか否かを判定するステップである。保管時間は、３０秒、１分、又は３分など、５分以下に設定されることが好ましい。当該変形例において、携帯デバイス２は保管期限切れとなった車両鍵コードを自動的に削除する（ステップＳ５７）。

[0109] 上記構成によれば、携帯デバイス２は、認証ＥＣＵ４からチャレンジコードを受信した際、カードキー１とＮＦＣ通信する必要がなくなるため、速やかにレスポンスコードを返送可能となる。よって、ユーザにとっては、車両の操作に対するシステムの応答性が高まるため、利便性が向上しうる。また、携帯デバイス２が車両鍵コードを保持している状態は一時的であるため、携帯デバイス２に車両鍵コードを常時保存する構成に比べてセキュリティを高めることができる。なお、携帯デバイス２は車両鍵コードをメモリ４２から削除後においては、前述のステップＳ４１～Ｓ４７を実施するように構成されていても良い。

[0110] <変形例（３）>

変形例（１）、（２）のさらなる変形例として、携帯デバイス２は、カードキー１から車両鍵コードを使用回数の制限付きで受信して保存するように構成されていても良い。使用回数が制限された車両鍵コードとは、一定回数使用可能な車両鍵コードに相当する。当該構成によれば、一時的に携帯デバイス２のカード読取位置からカードキー１が外れた状態においても、携帯デバイス２はレスポンスコードを生成及び返送可能となる。また、携帯デバイス２に保存されている車両鍵コードには使用可能回数が設定されているため、携帯デバイス２のみを所持する第３者が車両Ｈｖを無制限に使用することを防ぐことができる。

[0111] <変形例（４）>

変形例（１）～（３）のさらなる変形例として、認証ＥＣＵ４は、車両鍵コードそのものではなく、車両鍵コードをもとに生成した一時鍵コードを用いて、検証コードを生成するように構成されていてもよい。一時鍵コードは、車両鍵コードに認証処理実行時の日時情報を組み合わせたコードであってよい。それに合わせて、カードキー１は、携帯デバイス２からの車両鍵送信要求に対し、カード内格納部１６１に保存されている車両鍵コードに日時情報を組み合わせてなる一時鍵コードを返送してもよい。携帯デバイス２は、カードキー１から受信した一時鍵コードを用いてレスポンスコードを生成し、認証ＥＣＵ４に返送すればよい。

[0112] なお、一般的なクレジットカードは時計機能を備えない。カードキー１は、携帯デバイス２から日時情報を受信すればよい。携帯デバイス２は、車両鍵送信要求として、現在の日時情報を含むＮＦＣ信号を送信してもよい。当該構成によればカードキー１は、カードキー１自身が時計機能を備えていなくとも、携帯デバイス２の日時情報をもとに一時鍵コードを生成可能となる。

[0113] また、認証ＥＣＵ４と携帯デバイス２とでは時刻に数分～１０分程度のずれが生じていることが起こりうる。つまり、時刻情報を構成する要素のうち、分（ｍｍ）や秒（ｓｓ）の値は、デバイス間で相違することが起こりうる。

。そのような事情から、一時鍵コードの生成に使用する日時情報は、年月日に加えて10時や15時といった時刻までの情報、つまり、YYYY-MM-DDThhを示すデータとすることが好ましい。YYYY-MM-DDは年月日を示し、hhは何時かを示す。DDとhhの間にあるTは区切り文字である。

[0114] また、一時鍵コードの生成には、日時情報の代わりに／並列的に、それぞれのデバイスの位置座標を用いられてもよい。その場合カードキー1は、携帯デバイス2から位置情報を取得すればよい。なお、位置座標が1秒ずれている場合、距離としては約40mずれる。ユーザが車両Hvを使用する場合、車両Hvから6m以内にはユーザが存在することが期待できる。故に、整数秒までの位置情報は、認証ECU4と携帯デバイス2とで一致していることが期待できる。そのため、一時鍵コードの生成に整数秒までの位置情報を用いる場合であっても、認証ECU4がBLE認証に使用する一時鍵コードと、カードキー1が携帯デバイス2に返送する一時鍵コードは一致し、認証成功となりうる。

[0115] 本変形例(4)に開示の構成によれば、本当の車両鍵コードは携帯デバイス2に送信されないため、変形例(1)～(3)の構成よりもセキュリティを高めることができる。また、仮に一時鍵コードが盗まれた場合であっても、一定時間後／別の場所では当該一時鍵コードは無効となりうる。よって、車両用デジタルキーシステムSysのセキュリティを高めることができる。

[0116] <変形例(5)>

カードキー1がクレジットカードである場合、携帯デバイス2はカード認証サーバと通信することで、当該カードの正真性及び有効性を検証可能である。カード認証サーバは、クレジットカードの発行会社が管理するサーバであって、クレジットカードの正真性及び有効期限をチェックするサーバである。当該着想に基づき、携帯デバイス2は、図9に示すようにカードキー1とNFC通信可能となった際、カード認証サーバと通信することで、NFCで通信接続しているカードの正真性及び有効期限をチェックしても良い。N

F Cで通信接続しているカードが第2通信接続デバイスに相当する。

[0117] 図9に示すステップS 6 1は、カードキー1としてのクレジットカードとN F Cで通信接続したか否かを判定するステップである。また、ステップS 6 2は、携帯デバイス2がカードキー1とN F C通信可能となったことに基づいて、カード認証サーバに向けて、認証依頼を送信するステップである。認証依頼として送信するデータセットは、クレジットカード番号と有効期限が含まれてよい。カード認証サーバへの認証依頼は、セルラー通信によって実施されうる。

[0118] ステップS 6 3は、カード認証サーバからカード自体の認証結果を受信するステップである。携帯デバイス2はカード認証サーバから認証O Kとの回答を受信した場合には（S 6 4 Y E S）、当該カードキー1との通信接続を維持する（S 6 5）。これにより、携帯デバイス2は、カードキー1へチャレンジコードの送信や、車両鍵送信要求の送信といった、B L E認証のための後続処理を実施可能となる。

[0119] 一方、携帯デバイス2はカード認証サーバから認証失敗との回答を受信した場合には（S 6 4 N O）、当該カードキー1との通信接続を終了する（S 6 6）。ステップS 6 6は、通信を切断するのではなく、後続の処理を実施しないように一時的に設定を変更するステップであってもよい。

[0120] なお、クレジットカードの認証が失敗となるケースとしては、カード自体が偽造されたものである場合や、有効期限が切れている場合、カードの管理会社によって無効化されている場合である。カードが無効化されている場合には、紛失届け出がなされている場合や、不正利用の疑いが検知されている場合である。

[0121] 上記の構成によれば、偽造／紛失／盗難されたカードキー1を用いて第3者が車両H vを使用する恐れを低減できる。また、クレジットカードのセキュリティ機能を利用するため、車両用デジタルキーシステムS y sとしては新たに専用のサーバを設置する必要もない。よって、コストアップを抑制しつつ、セキュリティを高めることが可能となる。

[0122] <変形例（６）>

携帯デバイス２は、図１０に示すように、カードキー１と通信可能な状態であるか否かを判定する判定部Ｆ４を備えていてもよい。カードキー１と通信可能な状態とは、カードキー１がカード読取位置に重ねられている状態に対応する。カードキー１と通信可能か否かは、ポーリングコマンド又は特定のコマンドをＮＦＣ通信部２４から送信させ、カードキー１からの応答を受信できるか否かに基づいて判断可能である。カードキー１と通信可能な状態であるか否かは、フラグ等で管理されうる。

[0123] また、携帯デバイス２は、判定部Ｆ４の判定結果に応じて、チャレンジコードを受信した際の応答を変更しても良い。図１１に示すように、携帯デバイス２は、認証ＥＣＵ４からのチャレンジコードを受信した際（Ｓ７１　ＹＥＳ）、判定部Ｆ４はカードキー１と通信可能であるかどうかを判定する（Ｓ７２）。ここで携帯デバイス２は、カードキー１と通信可能である場合には、チャレンジコードの転送など、レスポンスコードの取得にかかる後続処理を実施する（Ｓ７３）。

[0124] 一方、携帯デバイス２は、チャレンジコードを受信した際に（Ｓ７１　ＹＥＳ）、カードキー１と通信不能である場合には（Ｓ７２　ＮＯ）、認証ＥＣＵ４に向けて認証不可通知を送信する（Ｓ７４）。認証不可通知は、レスポンスコードを返送できないことを示す特定コード（エラーコード）を含むＢＬＥ信号である。また、携帯デバイス２は、認証不可通知を送信するとともに、ステップＳ７５としてユーザ通知処理を実施してもよい。

[0125] ステップＳ７５としてのユーザ通知処理は、ユーザにＰＥＰＳ機能が利用できないこと／カードキー１をカード読取位置にかざす必要があることをユーザに通知する処理である。当該ユーザ通知処理は、携帯デバイス２が備えるバイブレータを所定パターンで振動させこと／所定パターンの通知音を出力すること／ディスプレイ２１に所定のメッセージを表示することで実現されうる。当該構成によれば、ユーザは、携帯デバイス２にカードキー１を重ね合わせることを忘れたことなどに気が付きやすくなる。

[0126] なお、認証E C U 4もまた、認証不可通知を受信した場合、B L E認証が不能であることをユーザに通知する処理を実施しても良い。当該通知は、車載ディスプレイ67への画像表示又はヘッドライトの明滅などを用いて実施されうる。認証E C U 4は、携帯デバイス2から認証不可通知を受信した場合、別の認証手段を使用することを提案するガイド画像を車載ディスプレイ67に表示しても良い。認証E C U 4は、携帯デバイス2から認証不可通知を受信したことに基づいてN F C通信機62を起動させた後に、N F C認証の利用をユーザに提案しても良い。また、認証E C U 4は、携帯デバイス2から認証不可通知を受信したことに基づいて生体認証センサ63を起動させた後に、生体認証の利用をユーザに提案しても良い。B L E認証が不能であることの通知、又は、別の認証方式の利用の案内などが臨時制御に相当する。

[0127] 認証E C U 4は、携帯デバイス2から認証不可通知を受信した場合に限らず、携帯デバイス2とB L E通信接続できていない状態においてユーザの開錠操作又は施錠操作等を検知した場合にも、上記代替認証手段の利用を提案する処理を実施しても良い。当該構成によればB L E認証失敗／不作動によってユーザを混乱させる恐れを低減できる。また、認証E C U 4は、B L E認証が実施できないと判定している場合にのみ、N F C通信機62又は生体認証センサ63といった代替認証用のデバイスを起動するように構成されていても良い。当該構成によれば、駐車中等における消費電力を低減できる。

[0128] なお、図10に示すチャレンジコード受信部F1は、認証E C U 4からB L E通信にてチャレンジコードを受信する処理を行うソフトウェア／ハードウェアモジュールである。チャレンジコード受信部F1が第1データ受信部に相当する。レスポンスコード取得部F2は、カードキー1との通信によって、レスポンスコードを取得する構成である。ここでの取得には、カードキー1から受信することのほか、カードキー1から受信した車両鍵コードを用いて自分自身で生成することも含まれる。チャレンジコード転送部F2aは、チャレンジコードをN F Cにてカードキー1に転送する処理を実施するモ

ジュールであり、変形例（２）等によっては省略されうる。チャレンジコード転送部 F 2 a が第 1 データ転送部に相当する。レスポンスコード受信部 F 2 b は、N F C にてカードキー 1 からレスポンスコードを受信する処理を実施するモジュールであり、変形例（２）等によっては省略されうる。レスポンスコード受信部 F 2 b が第 2 データ受信部に相当する。レスポンスコード送信部 F 3 は、B L E 通信にてレスポンスコードを認証 E C U 4 に送信する構成である。レスポンスコード送信部 F 3 が第 2 データ送信部に相当する。

[0129] <変形例（７）>

携帯デバイス 2 は、図 1 2 に示すようにカードキー 1 と通信可能となっている状態が一定時間以上継続された場合には、レスポンスコードを返送しない、応答停止状態に移行するように構成されていても良い。応答停止状態は、一時的に N F C 通信機能を停止させた状態、あるいは、N F C 通信機能は維持するもののレスポンスコードの取得にかかる処理を実施しない状態に相当する。

[0130] 具体的には携帯デバイス 2 はカードキー 1 と通信可能となった際（S 8 1 Y E S）、その時点での時刻をカード接続時刻として記録する（S 8 2）。そして、カードキー 1 と通信可能な状態が継続している間は、カード接続時刻から所定の応答ロック時間が経過したか否かを判定する（S 8 3）。ステップ S 8 3 は、携帯デバイス 2 はカードキー 1 と通信可能である状態が継続している時間である接続維持時間が所定値を超過したか否かを判定するステップに相当する。

[0131] 応答ロック時間は、５分又は１５分などであってよい。応答ロック時間は、１時間や３時間などであってもよい。応答ロック時間の設定値は、ユーザがタッチパネル 2 2 を介して自由に設定可能に構成されていても良い。応答ロック時間が短いほどセキュリティは向上しうる。

[0132] カード接続時刻からの経過時間が応答ロック時間を超過した場合（S 8 3 Y E S）、携帯デバイス 2 は、応答停止状態に移行する（S 8 4）。携帯デバイス 2 は、N F C 通信機 6 2 を非アクティブ状態に遷移させてもよい。

また、携帯デバイス2は、NFC通信機62をアクティブ状態にしたまま、ソフトウェア的にカードキー1との通信を終了／停止してもよい。

[0133] 応答停止状態に以降後、携帯デバイス2は所定の解除操作が行われたことを検出すると、通常状態に復帰する(S86)。通常状態は、カードキー1と通信可能な状態に相当する。解除操作は、DKアプリ204に設けられた所定の解除ボタンを選択する操作であってもよいし、カード読取位置にカードキー1を重ね直す操作であってもよい。これらの操作はタッチパネル22からの信号、あるいは、NFC通信部24から信号に基づいて検出可能である。また、解除操作は、携帯デバイス2を振る行為であってもよい。当該行為は携帯デバイス2に設けられた加速度センサの出力から検出可能である。

[0134] 上記構成によれば、ユーザが携帯デバイス2のカード読取位置にカードキー1を長時間重ねたままであったとしても、車両Hvが不正に使用される恐れを低減できる。

[0135] <変形例(8)>

車載システム3と携帯デバイス2との通信規格としては、BLE以外にも、Bluetooth Classicや、Wi-Fi(登録商標)、UWB-IR(Ultra Wide Band - Impulse Radio)、EnOcean(登録商標)など、多様なものを採用可能である。車載システム3と携帯デバイス2との通信方式は、LF-UHF併用方式であってもよい。LF-UHF併用方式は、125kHzや134kHzなどのLF(Low Frequency)帯の電波と、315MHzや、920MHzなどのUHF(Ultra High Frequency)帯の電波を併用して双方向通信を行う方式である。LF-UHF併用方式は、車載システム3から携帯デバイス2への信号送信にはLF帯の電波を用い、携帯デバイス2から車載システム3への信号送信にはUHF帯の電波を用いる方式であってもよい。

[0136] 携帯デバイス2と車載システム3とは、近距離通信可能に構成されていればよい。ここでの近距離通信とは、実質的な通信可能距離が、0.5m以上であって、1m/10m/20m/100m程度となる方式の通信を指す。上述したBLEやWi-Fi等が近距離通信を実現する通信方式に相当する

。上記実施形態におけるBLE通信との記載は、UWB通信やWi-Fi通信、近距離通信などに置き換え可能である。なお、通信可能距離は通信可能な距離の最大値であることから最大通信距離と呼ぶこともできる。

[0137] <変形例（9）>

上記実施形態では、クレジットカードをキーモジュールとして機能させる態様について述べたが、キーモジュールの実施形態はこれに限定されない。キーモジュールは、クレジットカード以外の、NFC機能を備えたICカードであってもよい。また、キーモジュールは、タグや、キーリング／キーチェーン（いわゆるキーホルダ）、ストラップなど、カード以外の形態を有していても良い。キーモジュールは、指輪やリストバンドなどのウェアラブルデバイスであってもよい。またMNFCは、電磁誘導方式／パッシブ型のRFID（radio frequency identification）の一種と解することができる。カードキー1は、NFCタグ、あるいは、RFIDタグと呼ぶこともできる。カードキー1と携帯デバイス2との通信方式が第2通信の方式に相当する。第2通信方式は、通信可能距離が0.5m未満、より好ましくは0.1m程度となる方式であることが好ましい。通信距離が短いほど、カードキー1と携帯デバイス2が不用意に通信するおそれを低減でき、セキュリティを高めることができる。なお、第2通信方式は赤外線通信であっても良い。また、第2通信方式は人体通信であってもよい。キーモジュールは、ハッキング／ウイルス感染による車両鍵コードの盗難／流出の恐れを低減するために、セルラー通信機能を備えない装置／アクセサリ／道具であることが好ましい。キーモジュールに保存されている車両鍵コードは、認証ECU4に保存されている車両鍵コードと互いに関連付けられていればよく、必ずしも同じ値である必要はない。つまり第1の鍵コードと第2の鍵コードは、互いに関連付けられていることを条件として、異なる値であってもよい。認証成功と判断する条件は、鍵コードの特性に応じて設計されればよい。

[0138] <変形例（10）>

車両Hvは、会社組織が保有する社用車や、公的機関が保有する公用車で

あってもよい。車両H vが社用車や公用車である場合には、当該車両H vを管理する組織に属する人物がユーザとなりうる。車両H vは、貸出サービスに供される車両（いわゆるレンタカー）であってもよいし、カーシェアリングサービスに供される車両（いわゆるシェアカー）であってもよい。車両H vが上記サービスに供される車両（以下、サービス車両）である場合には、それらのサービスの利用契約を行っており、且つ、サービスの利用予約等に基づき、一時的に当該車両H vを利用する権限を有する人物がユーザとなりうる。また、本開示は車両だけでなく、建物や施設用の電子キーシステムにも適用可能である。

[0139] <付言（１）>

本開示には以下の技術的思想も含まれる。また、以下の技術的思想は、ユーザ認証デジタルキーシステムや携帯デバイス用プログラムなどにも適宜適用可能である。

[0140] [技術的思想１]

通信可能距離が0.5 m以上となる方式の無線通信である第１通信と、前記第１通信よりも通信可能距離が短い方式である第２通信と、を実施可能に構成されている携帯デバイス（２）で使用されるアプリケーションであるデジタルキーアプリ（２０４）と、

前記第１通信を実施可能に構成されてあって、ユーザ認証に使用される鍵コードが保存された第１記憶装置（４３１）を備える認証ユニット（４）と、

前記第２通信を実施可能に構成されてあって、前記鍵コードが保存された第２記憶装置（１６１）を備えるキーモジュール（１）と、によって実施されるユーザ認証方法であって、

前記認証ユニットが、所定の認証イベントを検出したことに基づいて又は定期的に、前記ユーザ認証のための第１データを、前記第１通信にて前記デジタルキーアプリに送信すること（Ｓ１１）、

前記デジタルキーアプリが、前記第１通信にて前記第１データを受信した

ことに基づき、前記キーモジュールと前記第 2 通信を実施することで、前記第 1 データと前記鍵コードを用いて生成される第 2 データを取得すること（S 3 5 B、S 4 5）、

前記デジタルキーアプリが、前記第 2 データを前記第 1 通信にて前記認証ユニットに送信すること（S 3 6 A）、

前記認証ユニットが、前記デジタルキーアプリから受信する前記第 2 データと、前記第 1 記憶装置に保存されている前記鍵コードと、前記第 1 データとを用いて、前記ユーザ認証を実施すること（S 1 4、S 3 7）、を含むユーザ認証方法。

[0141] [技術的思想 2]

技術的思想 1 に記載のユーザ認証方法であって、

前記デジタルキーアプリが前記第 2 データを取得するための工程／方法として、

前記デジタルキーアプリが、前記認証ユニットから前記第 1 データを受信したことに基づいて、前記キーモジュールに対し、前記第 1 データを含むデータセットを前記第 2 通信にて送信すること（S 3 3 A）と、

前記キーモジュールが、前記デジタルキーアプリから前記第 1 データを受信したことに基づいて、前記第 2 記憶装置に保存されている前記鍵コードを用いて前記第 1 データから前記第 2 データを生成し、前記第 2 通信にて返送すること（S 3 5 A）と、

前記デジタルキーアプリが、前記第 2 通信にて前記キーモジュールから返送されてくる前記第 2 データを受信すること（S 3 5 B）と、を含むユーザ認証方法。

[0142] [技術的思想 3]

技術的思想 1 に記載のユーザ認証方法であって、

前記デジタルキーアプリが前記第 2 データを取得するための工程／方法として、

前記デジタルキーアプリは、前記認証ユニットから前記第 1 データを受信

したことに基づいて、前記キーモジュールに対し、前記鍵コードを送信するように要求する信号である鍵要求信号を前記第2通信にて送信すること（S42A）と、

前記キーモジュールが、前記鍵要求信号を受信したことに基づいて、前記第2記憶装置に保存されている前記鍵コードを、前記第2通信にて前記デジタルキーアプリに送信すること（S44A）と、

前記デジタルキーアプリが、前記キーモジュールから前記第2通信にて受信した前記鍵コードを用いて、前記第1データから前記第2データを生成すること（S45）と、を含むユーザ認証方法。

[0143] [技術的思想4]

技術的思想3に記載のユーザ認証方法であって、

前記デジタルキーアプリが、前記第2通信にて受信した前記第2の鍵コードを前記第2データの生成後は速やかに前記携帯デバイスの内部から削除すること（S46）を含むユーザ認証方法。

[0144] [技術的思想5]

技術的思想1から4の何れか1つに記載のユーザ認証方法であって、

前記デジタルキーアプリが、前記携帯デバイスに搭載されているセンサからの入力信号に基づき、所定の重ね合わせ操作が行われたことを検出することと、

前記デジタルキーアプリが、前記重ね合わせ操作が行われたことを検出したことに基づいて前記キーモジュールと通信接続すること、を含むユーザ認証方法。

[0145] [技術的思想6]

技術的思想1から5の何れか1つに記載のユーザ認証方法であって、

前記デジタルキーアプリが、前記キーモジュールと通信可能かどうかを判断すること（S72）と、

前記デジタルキーアプリが、前記認証ユニットから前記第1データを受信した際に、前記キーモジュールと通信不能である場合には、前記認証ユニッ

トに向けて所定のエラーコードを含む信号を前記第 1 通信にて返送すること（S 7 4）と、

前記認証ユニットは、前記デジタルキーアプリから前記エラーコードを含む信号を受信したことに基づいて所定の臨時制御を実施することと、を含むユーザ認証方法。

[0146] [技術的思想 7]

技術的思想 1 から 6 の何れか 1 つに記載のユーザ認証方法であって、
前記ユーザ認証のためのステップとして、

前記認証ユニットが、前記第 1 記憶装置に保存されている前記鍵コードを用いて、前記第 2 データの生成と同様の方式により、前記デジタルキーアプリに送信した前記第 1 データから第 3 データを生成すること（S 1 2）と、

前記認証ユニットが、前記第 3 データと前記第 2 データを比較し、両者が一致することを条件として前記ユーザ認証が成功したと判定することと、を含むユーザ認証方法。

[0147] [技術的思想 8]

技術的思想 1 から 7 の何れか 1 つに記載のユーザ認証方法であって、

前記デジタルキーアプリが、前記第 2 通信で接続しているデバイスである第 2 通信接続デバイスの正当性を検証するための通信を、所定のサーバと実施すること（S 6 2）と、

前記デジタルキーアプリが、前記サーバにて前記第 2 通信接続デバイスの正当性が肯定されていることを条件として、前記第 2 データを取得するための処理を開始すること（S 6 5）と、を含むユーザ認証方法。

[0148] [技術的思想 9]

技術的思想 8 に記載のユーザ認証方法であって、

前記デジタルキーアプリが、前記サーバにて前記第 2 通信接続デバイスの正当性が構成されていない場合には、前記第 2 データを取得するための処理を実行しないこと（S 6 6）と、を含むユーザ認証方法。

[0149] [技術的思想 1 0]

技術的思想 1 から 9 の何れか 1 つに記載のユーザ認証方法であって、
前記デジタルキーアプリが、前記キーモジュールと前記第 2 通信を開始してからの経過時間である接続維持時間を計測すること（S 8 2）と、
前記デジタルキーアプリが、前記接続維持時間が所定の応答ロック時間を超えたことに基づいて、前記第 2 データを前記認証ユニットに送信しない応答停止状態に移行すること（S 8 4）と、を含むユーザ認証方法。

[0150] [技術的思想 1 1]

技術的思想 1 0 に記載のユーザ認証方法であって、
前記デジタルキーアプリが、前記携帯デバイスに搭載されているセンサからの入力信号に基づき、所定の解除操作が行われたことを検出すること（S 8 5）と、
前記デジタルキーアプリが、前記解除操作が行われたことを検出したことに基づいて前記応答停止状態から通常状態に復帰すること（S 8 6）と、を含むユーザ認証方法。

[0151] [技術的思想 1 2]

技術的思想 1 から 1 1 の何れか 1 つに記載のユーザ認証方法であって、
前記第 2 通信は、N F C（Near Field Communication）であるユーザ認証方法。

[0152] [技術的思想 1 3]

技術的思想 1 から 1 2 の何れか 1 つに記載のユーザ認証方法であって、
前記キーモジュールは、クレジットカードであるユーザ認証方法。

[0153] <付言（2）>

本開示に示す種々のフローチャートは何れも一例であって、フローチャートを構成するステップの数や、処理の実行順は適宜変更可能である。また、本開示に記載の装置、システム、並びにそれらの手法は、コンピュータプログラムにより具体化された一つ乃至は複数の機能を実行するようにプログラムされたプロセッサを構成する専用コンピュータにより、実現されてもよい。本開示に記載の装置及びその手法は、専用ハードウェア論理回路を用いて

実現されてもよい。本開示に記載の装置及びその手法は、コンピュータプログラムを実行するプロセッサと一つ以上のハードウェア論理回路との組み合わせにより構成された一つ以上の専用コンピュータにより、実現されてもよい。プロセッサ（演算コア）としては、CPUや、MPU、GPU、DFP（Data Flow Processor）などを採用可能である。携帯デバイス2／認証ECU4が備える機能の一部又は全部は、システムオンチップ（SOC：System-on-Chip）、IC、及びFPGA（Field-Programmable Gate Array）の何れかを用いて実現されていてもよい。ICの概念には、ASIC（Application Specific Integrated Circuit）も含まれる。また、各デバイスで使用されるコンピュータプログラムは、コンピュータにより実行されるインストラクションとして、コンピュータ読み取り可能な非遷移有形記録媒体（non-transitory tangible storage medium）に記憶されていればよい。プログラムの記録媒体としては、HDD（Hard-disk Drive）やSSD（Solid State Drive）、フラッシュメモリ、ROM等を採用可能である。コンピュータを携帯デバイス2／認証ECU4／カードキー1として機能させるためのプログラム、このプログラムを記録した半導体メモリ等の非遷移的実態的記録媒体等の形態も本開示の範囲に含まれる。また、車両鍵コードを書き込み可能な記憶領域が設けられたクレジットカードや、クレジットカードに車両鍵コードを書き込み可能に構成されたNFCライタなども本開示に含まれる。

請求の範囲

[請求項1] 通信可能距離が0.5 m以上となる方式の無線通信である第1通信と、前記第1通信よりも通信可能距離が短い方式である第2通信と、を実施可能に構成されている携帯デバイス(2)で使用されるアプリケーションであるデジタルキーアプリ(204)と、

 前記第1通信を実施可能に構成されてあって、ユーザ認証に使用される第1の鍵コードが保存された第1記憶装置(431)を備える認証ユニット(4)と、

 前記第2通信を実施可能に構成されてあって、前記第1の鍵コードと同じ値または関連する第2の鍵コードが保存された第2記憶装置(161)を備えるキーモジュール(1)と、によって実施されるユーザ認証方法であって、

 前記認証ユニットが、前記ユーザ認証のための第1データを、前記第1通信にて前記デジタルキーアプリに送信すること(S11)と、

 前記デジタルキーアプリが、前記第1通信にて前記第1データを受信したことに基づき、前記キーモジュールと前記第2通信を実施することで、前記第1データと前記第2の鍵コードを用いて生成される第2データを取得すること(S35B、S45)と、

 前記デジタルキーアプリが、前記第2データを前記第1通信にて前記認証ユニットに送信すること(S36A)と、

 前記認証ユニットが、前記デジタルキーアプリから受信する前記第2データを用いて、前記ユーザ認証を実施すること(S14、S37)と、を含むユーザ認証方法。

[請求項2] 請求項1に記載のユーザ認証方法であって、

 前記デジタルキーアプリが前記第2データを取得するための工程として、

 前記デジタルキーアプリが、前記認証ユニットから前記第1データを受信したことに基づいて、前記キーモジュールに対し、前記第1デ

ータを含むデータセットを前記第2通信にて送信すること（S33A）と、

前記キーモジュールが、前記デジタルキーアプリから前記第1データを受信したことに基づいて、前記第2の鍵コードを用いて前記第1データから前記第2データを生成し、前記第2通信にて返送すること（S35A）と、

前記デジタルキーアプリが、前記第2通信にて前記キーモジュールから返送されてくる前記第2データを受信すること（S35B）と、を含むユーザ認証方法。

[請求項3]

請求項1に記載のユーザ認証方法であって、

前記デジタルキーアプリが前記第2データを取得するための工程として、

前記デジタルキーアプリが、前記認証ユニットから前記第1データを受信したことに基づいて、前記キーモジュールに対し、前記第2の鍵コードを送信するように要求する信号である鍵要求信号を前記第2通信にて送信すること（S42A）と、

前記キーモジュールが、前記鍵要求信号を受信したことに基づいて、前記第2の鍵コードを前記第2通信にて前記デジタルキーアプリに送信すること（S44A）と、

前記デジタルキーアプリが、前記キーモジュールから前記第2通信にて受信した前記第2の鍵コードを用いて、前記第1データから前記第2データを生成すること（S45）と、を含むユーザ認証方法。

[請求項4]

請求項3に記載のユーザ認証方法であって、

前記デジタルキーアプリが、前記第2通信にて受信した前記第2の鍵コードを前記第2データの生成後は速やかに前記携帯デバイスの内部から削除すること（S46）を含むユーザ認証方法。

[請求項5]

請求項1に記載のユーザ認証方法であって、

前記デジタルキーアプリが、前記携帯デバイスに搭載されているセ

ンサからの入力信号に基づき、所定の重ね合わせ操作が行われたことを検出することと、

前記デジタルキーアプリが、前記重ね合わせ操作が行われたことを検出したことに基づいて前記キーモジュールと通信接続すること、を含むユーザ認証方法。

- [請求項6] 請求項 1 から 5 の何れか 1 項に記載のユーザ認証方法であって、
- 前記デジタルキーアプリが、前記キーモジュールと通信可能かどうかを判断すること（S 7 2）と、
- 前記デジタルキーアプリが、前記認証ユニットから前記第 1 データを受信した際に、前記キーモジュールと通信不能である場合には、前記認証ユニットに向けて所定のエラーコードを含む信号を前記第 1 通信にて返送すること（S 7 4）と、
- 前記認証ユニットは、前記デジタルキーアプリから前記エラーコードを含む信号を受信したことに基づいて所定の臨時制御を実施することと、を含むユーザ認証方法。

- [請求項7] 請求項 1 から 5 の何れか 1 項に記載のユーザ認証方法であって、
- 前記ユーザ認証のためのステップとして、
- 前記認証ユニットが、前記第 1 の鍵コードを用いて、前記第 2 データの生成と同様の方式により、前記デジタルキーアプリに送信した前記第 1 データから第 3 データを生成すること（S 1 2）と、
- 前記認証ユニットが、前記第 3 データと前記第 2 データを比較することにより前記ユーザ認証を行うことと、を含むユーザ認証方法。

- [請求項8] 請求項 1 から 5 の何れか 1 項に記載のユーザ認証方法であって、
- 前記デジタルキーアプリが、前記第 2 通信で通信接続している前記キーモジュールの正当性を検証するための通信を、所定のサーバと実施すること（S 6 2）と、
- 前記デジタルキーアプリが、前記サーバにて前記キーモジュールの正当性が肯定されていることを条件として、前記第 2 データを取得す

るための処理を開始すること（S 6 5）と、を含むユーザ認証方法。

[請求項9]

請求項 8 に記載のユーザ認証方法であって、

前記デジタルキーアプリが、前記サーバにて前記キーモジュールの正当性が肯定されていない場合には、前記第 2 データを取得するための処理を実行しないこと（S 6 6）と、を含むユーザ認証方法。

[請求項10]

請求項 1 から 5 の何れか 1 項に記載のユーザ認証方法であって、

前記デジタルキーアプリが、前記キーモジュールと前記第 2 通信を開始してからの経過時間である接続維持時間を計測すること（S 8 2）と、

前記デジタルキーアプリが、前記接続維持時間が所定の応答ロック時間を超えたことに基づいて、前記第 2 データを前記認証ユニットに送信しない応答停止状態に移行すること（S 8 4）と、を含むユーザ認証方法。

[請求項11]

請求項 1 0 に記載のユーザ認証方法であって、

前記デジタルキーアプリが、前記携帯デバイスに搭載されているセンサからの入力信号に基づき、所定の解除操作が行われたことを検出すること（S 8 5）と、

前記デジタルキーアプリが、前記解除操作が行われたことを検出したことに基づいて前記応答停止状態から通常状態に復帰すること（S 8 6）と、を含むユーザ認証方法。

[請求項12]

請求項 1 から 5 の何れか 1 項に記載のユーザ認証方法であって、

前記第 1 通信は、Bluetooth Low Energy、Bluetooth Classic、Wi-Fi、Ultra Wide Band - Impulse Radio、EnOcean、及び L F - U H F 併用方式のいずれかであり、

前記第 2 通信は、N F C（Near Field Communication）であるユーザ認証方法。

[請求項13]

請求項 1 から 5 の何れか 1 項に記載のユーザ認証方法であって、

前記キーモジュールは、クレジットカードであるユーザ認証方法。

[請求項14] 通信可能距離が0.5 m以上となる方式の無線通信である第1通信と、前記第1通信よりも通信可能距離が短い方式である第2通信と、を実施可能に構成されている携帯デバイス(2)で使用されるアプリケーションであるデジタルキーアプリ(204)と、

前記第2通信で前記携帯デバイスと通信可能に構成されているキーモジュール(1)と、を含むユーザ認証デジタルキーシステムであって、

前記デジタルキーアプリは、

認証ユニットから前記第1通信にて送信される、ユーザ認証のための第1データを受信する第1データ受信部(F1)と、

前記第1データ受信部が前記第1通信にて前記第1データを受信したことに基づき、前記キーモジュールに向けて、前記第1データを含むデータセットを前記第2通信にて送信する第1データ転送部(F2a)と、を備え、

前記キーモジュールは、

前記ユーザ認証に使用される鍵コードが保存されたモジュール内記憶部と、

前記デジタルキーアプリから前記第2通信にて前記第1データを受信したことに基づいて、前記モジュール内記憶部に保存されている前記鍵コードを用いて前記第1データから第2データを生成し、前記第2通信にて返送する応答回路(12)と、を備え、

前記デジタルキーアプリは、さらに、

前記第2通信にて前記キーモジュールから返送されてくる前記第2データを受信する第2データ受信部(F2b)と、

前記第2データを前記第1通信にて前記認証ユニットに送信する第2データ送信部(F3)と、を備えるユーザ認証デジタルキーシステム。

[請求項15] 前記第1通信は、Bluetooth(登録商標) Low Energy、Bluetooth

Classic、Wi-Fi、Ultra Wide Band - Impulse Radio、EnOcean、及び L F - U H F 併用方式のいずれかであり、

前記第 2 通信は、N F C (Near Field Communication) である、請求項 1 4 に記載のユーザ認証デジタルキーシステム。

[請求項16] 前記キーモジュールは、クレジットカードである、請求項 1 4 又は 1 5 に記載のユーザ認証デジタルキーシステム。

[請求項17] 通信可能距離が 0. 5 m 以上となる方式の無線通信である第 1 通信と、前記第 1 通信よりも通信可能距離が短い方式である第 2 通信と、を実施可能に構成されている携帯デバイス (2) が備えるプロセッサ (2 0 1) に、

認証ユニット (4) から前記第 1 通信にて送信される、ユーザ認証のための第 1 データを受信すること (S 3 1 B) と、

前記第 1 通信にて前記認証ユニットから前記第 1 データを受信したことに基づき、前記ユーザ認証に使用される鍵コードが登録されているキーモジュール (1) と前記第 2 通信を実施することで、前記第 1 データと前記鍵コードを用いて生成される第 2 データを取得すること (S 3 5 B、S 4 5) と、

前記第 2 データを前記第 1 通信にて前記認証ユニットに送信すること (S 3 6 A) と、を実行させるための命令を含む携帯デバイス用プログラム。

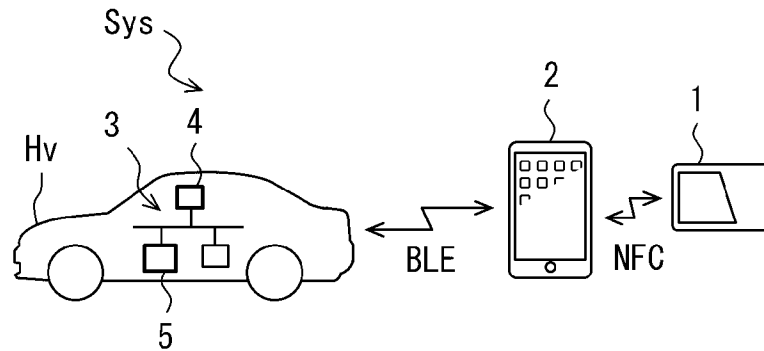
[請求項18] 前記第 1 通信は、Bluetooth Low Energy、Bluetooth Classic、Wi-Fi、Ultra Wide Band - Impulse Radio、EnOcean、及び L F - U H F 併用方式のいずれかであり、

前記第 2 通信は、N F C (Near Field Communication) である、請求項 1 7 に記載の携帯デバイス用プログラム。

[請求項19] 前記キーモジュールは、クレジットカードである、請求項 1 7 又は 1 8 に記載の携帯デバイス用プログラム。

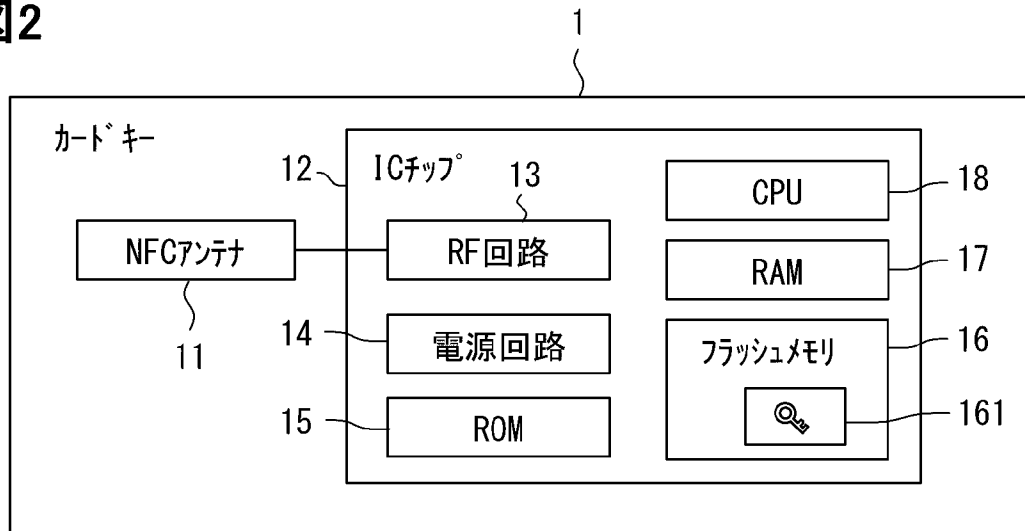
[図1]

図1



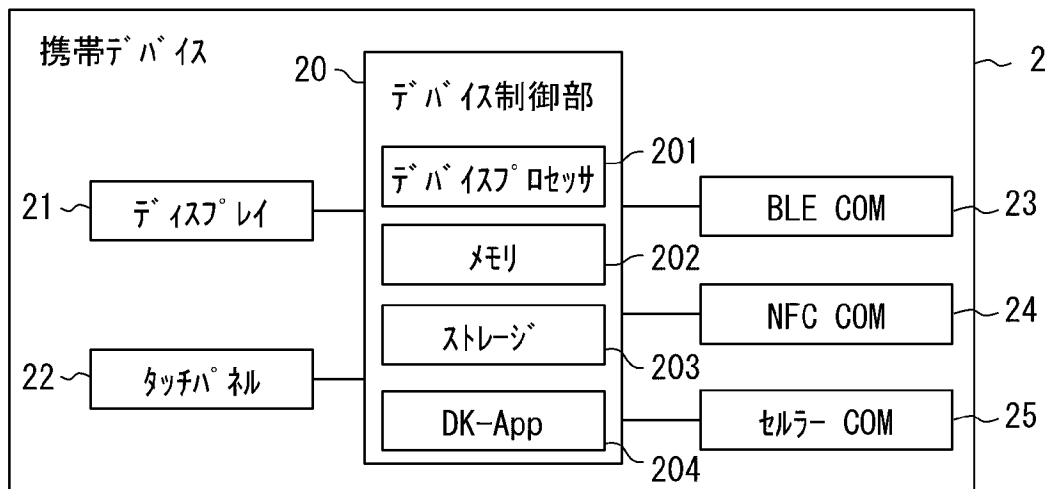
[図2]

図2



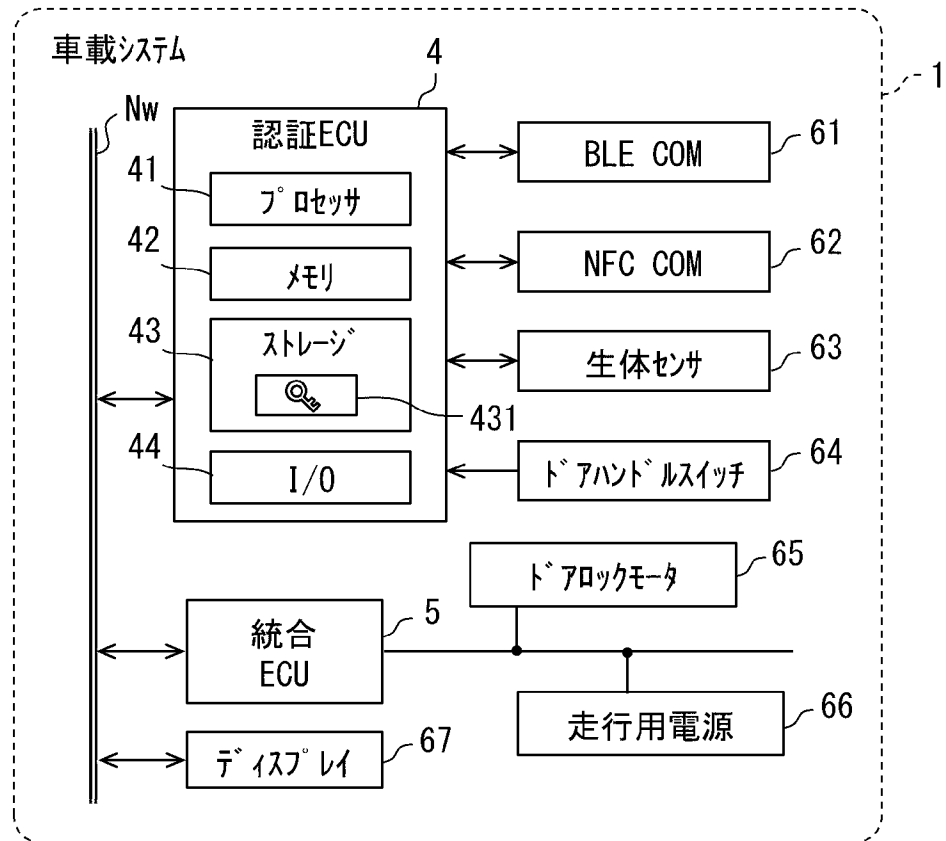
[図3]

図3



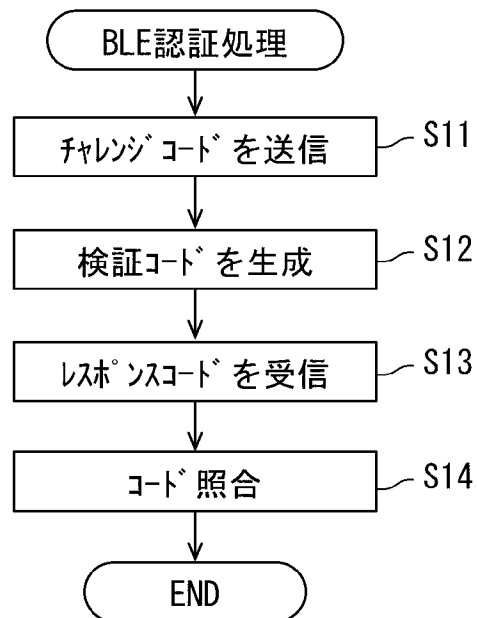
[図4]

図4



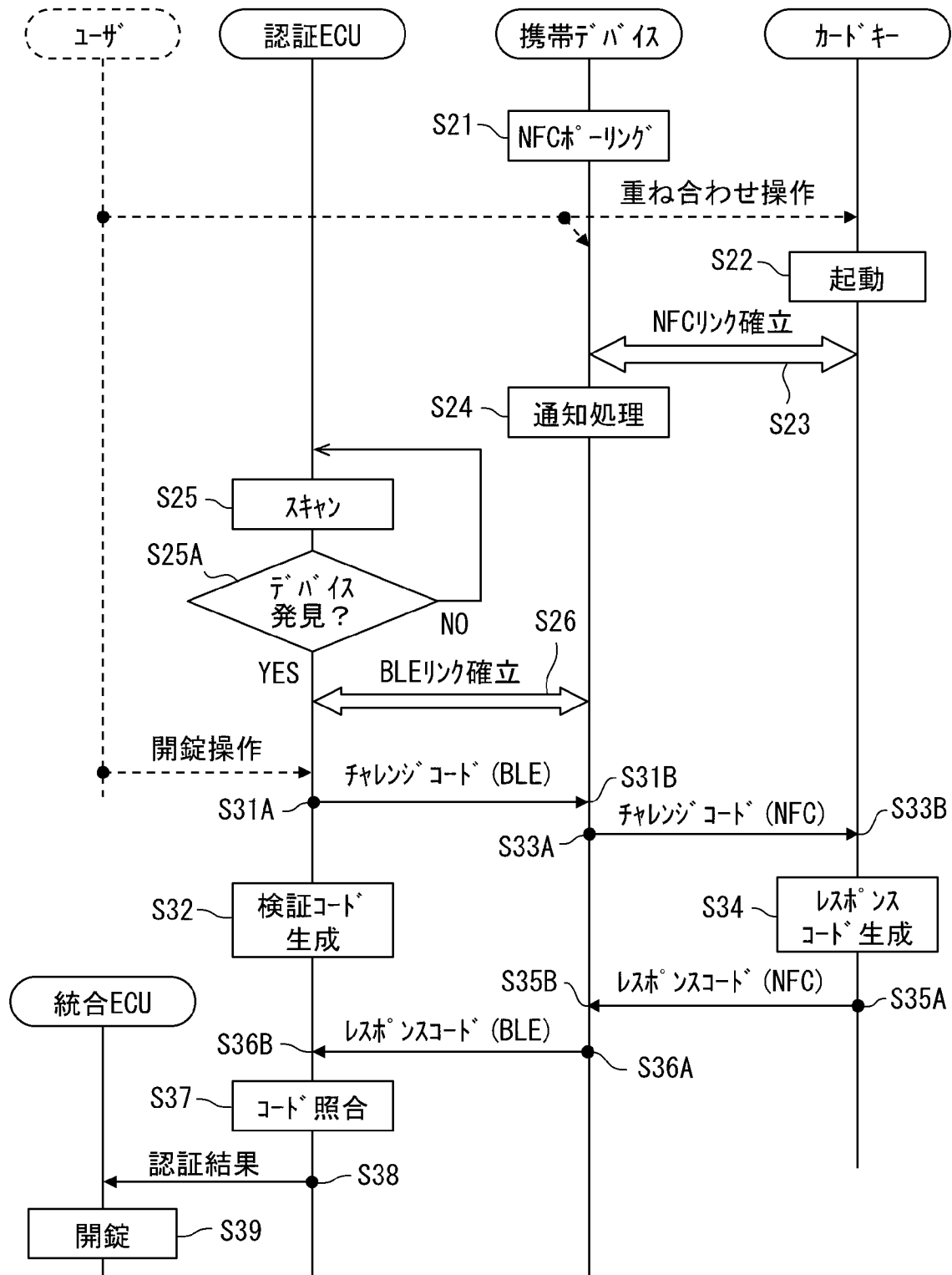
[図5]

図5



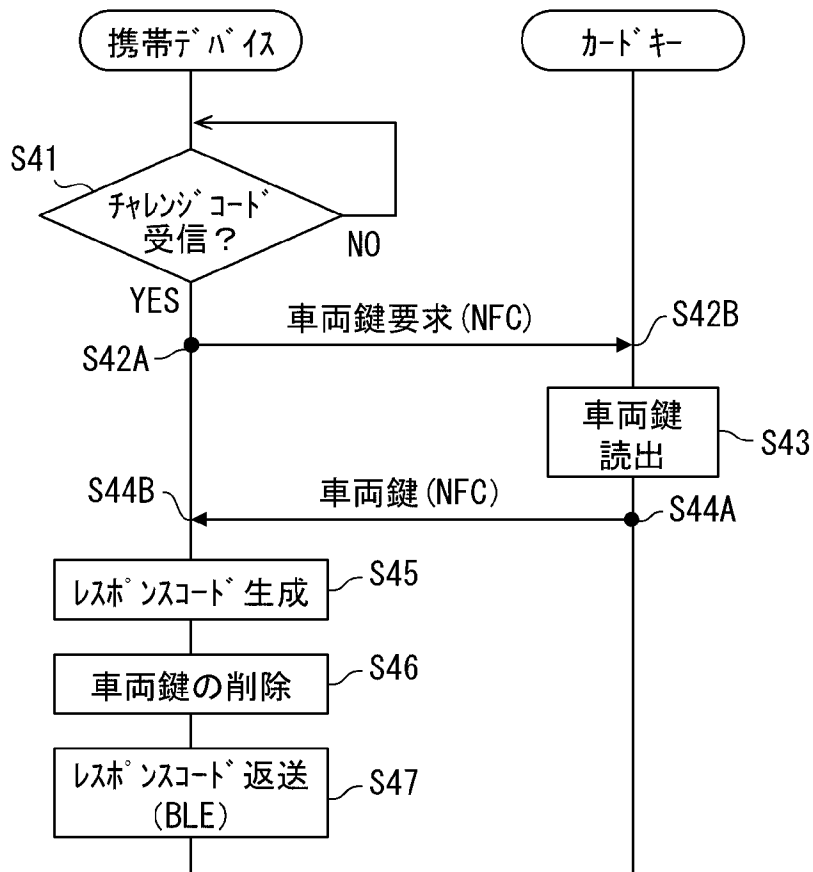
[図6]

図6



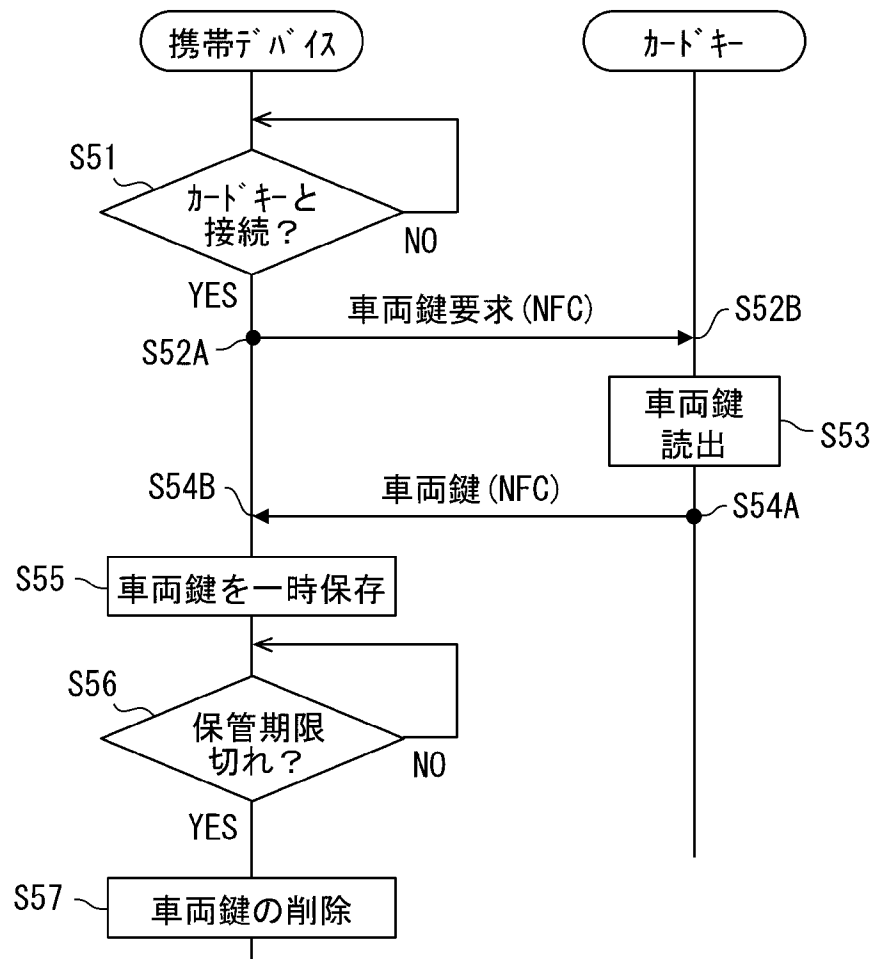
[図7]

図7



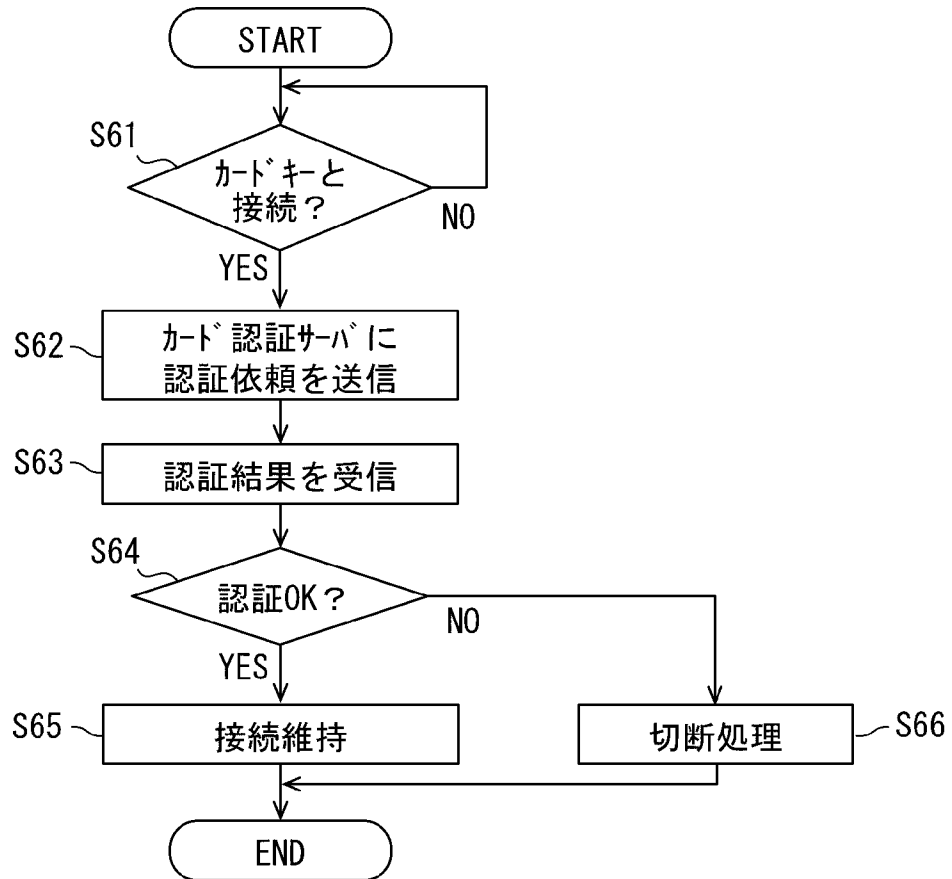
[図8]

図8



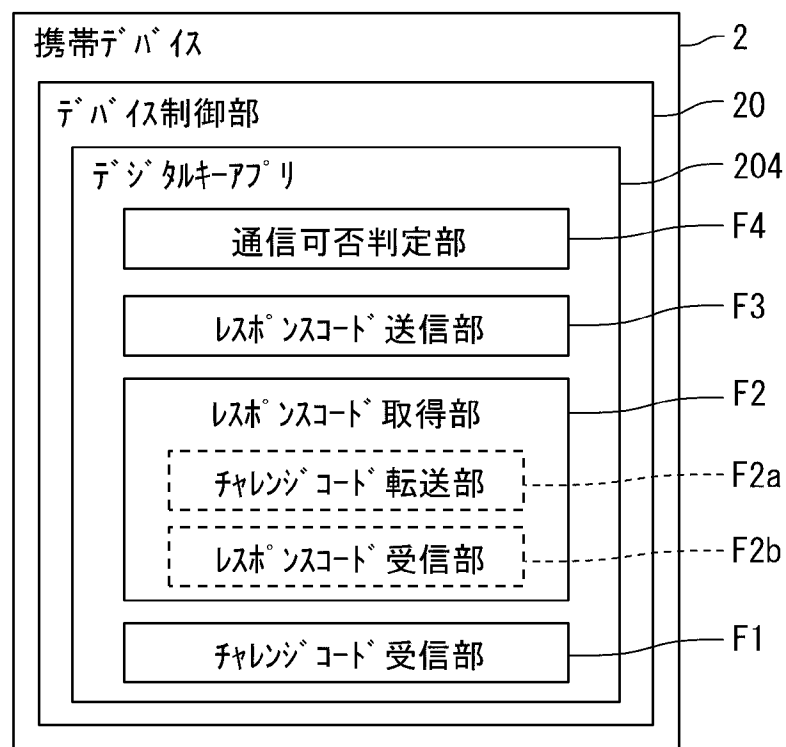
[図9]

図9



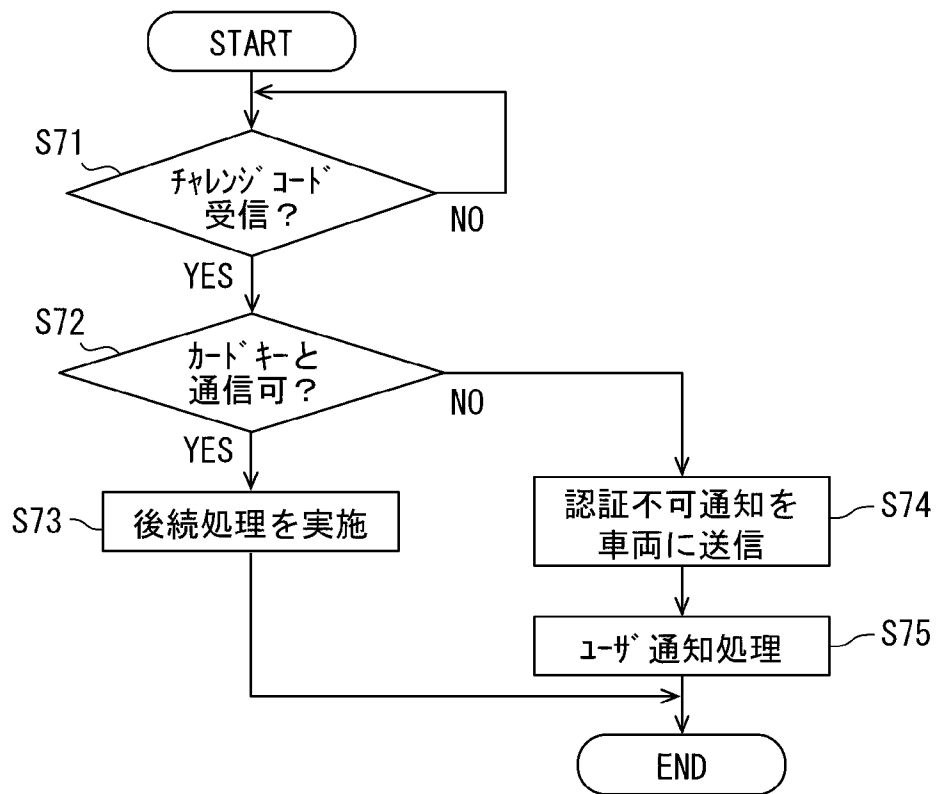
[図10]

図10



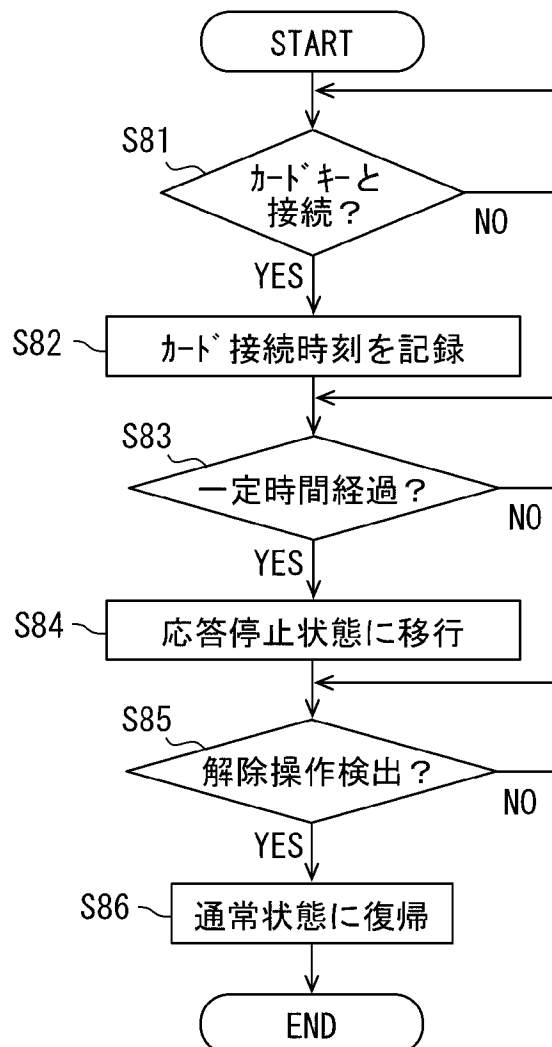
[図11]

図11



[図12]

図12



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/025564

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/35**(2013.01)i; **B60R 25/24**(2013.01)i; **E05B 49/00**(2006.01)i

FI: G06F21/35; B60R25/24; E05B49/00 K

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)

G06F21/35; B60R25/24; E05B49/00

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 1971-2023

Registered utility model specifications of Japan 1996-2023

Published registered utility model applications of Japan 1994-2023

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 2021-105834 A (TOKAI RIKA CO LTD) 26 July 2021 (2021-07-26) paragraph [0013]	1-19
A	JP 2021-147959 A (TOKAI RIKA CO LTD) 27 September 2021 (2021-09-27) paragraphs [0018]-[0037]	1-19
A	JP 2015-103048 A (TOPPAN PRINTING CO LTD) 04 June 2015 (2015-06-04) paragraphs [0031]-[0048]	1-19



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

19 September 2023

Date of mailing of the international search report

26 September 2023

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)

3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915

Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/025564

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2021-105834	A	26 July 2021	US 2021/0203658 A1 paragraph [0014] DE 102020133908 A CN 113068185 A	
JP	2021-147959	A	27 September 2021	(Family: none)	
JP	2015-103048	A	04 June 2015	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/35(2013.01)i; B60R 25/24(2013.01)i; E05B 49/00(2006.01)i FI: G06F21/35; B60R25/24; E05B49/00 K										
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）） G06F21/35; B60R25/24; E05B49/00										
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										
<table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2023年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2023年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2023年</td> </tr> </table>			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2023年	日本国実用新案登録公報	1996 - 2023年	日本国登録実用新案公報	1994 - 2023年
日本国実用新案公報	1922 - 1996年									
日本国公開実用新案公報	1971 - 2023年									
日本国実用新案登録公報	1996 - 2023年									
日本国登録実用新案公報	1994 - 2023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 2021-105834 A（株式会社東海理化電機製作所）26.07.2021（2021 - 07 - 26） 段落0013	1-19								
A	JP 2021-147959 A（株式会社東海理化電機製作所）27.09.2021（2021 - 09 - 27） 段落0018-0037	1-19								
A	JP 2015-103048 A（凸版印刷株式会社）04.06.2015（2015 - 06 - 04） 段落0031-0048	1-19								
☐ 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。										
<table border="0"> <tr> <td> * 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技术水準を示すもの “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 </td> <td> “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 </td> </tr> </table>			* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技术水準を示すもの “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						
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技术水準を示すもの “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 19.09.2023	国際調査報告の発送日 26.09.2023									
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） 金沢 史明 5S 4538 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/JP2023/025564

引用文献			公表日	パテントファミリー文献	公表日
JP	2021-105834	A	26.07.2021	US 2021/0203658 A1 段落0014 DE 102020133908 A CN 113068185 A	
JP	2021-147959	A	27.09.2021	(ファミリーなし)	
JP	2015-103048	A	04.06.2015	(ファミリーなし)	