(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 22 日(22.06.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/104352 A1

(51) 国際特許分類:
E05B 49/00 (2006.01) *H04M 1/00* (2006.01)
B60R 25/24 (2013.01) *H04Q 9/00* (2006.01)

(21) 国際出願番号: PCT/JP2016/084439

(22) 国際出願日: 2016 年 11 月 21 日(21.11.2016)

(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 2015-242992 2015 年 12 月 14 日(14.12.2015) 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: 三林 浩徳(MITSUBAYASHI Hironori); 〒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).

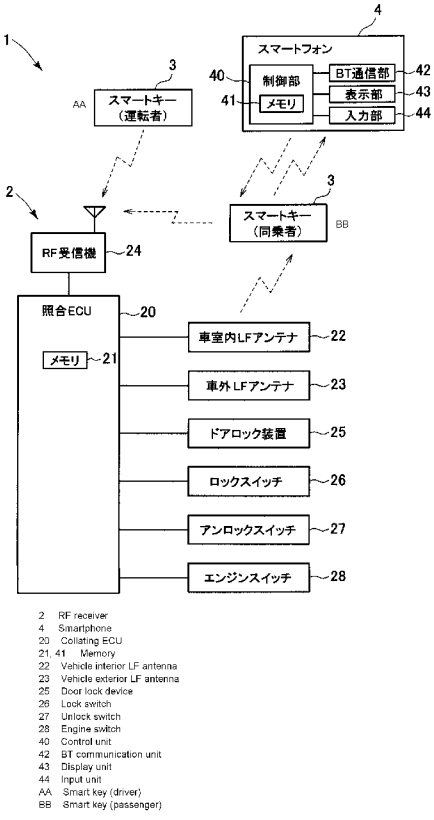
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, 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,

[続葉有]

(54) **Title**: VEHICLE CONTROL SYSTEM

(54) 発明の名称 : 車両制御システム



2 RF receiver
4 Smartphone
20 Collating ECU
21, 41 Memory
22 Vehicle interior LF antenna
23 Vehicle exterior LF antenna
25 Door lock device
26 Lock switch
27 Unlock switch
28 Engine switch
40 Control unit
42 BT communication unit
43 Display unit
44 Input unit
AA Smart key (driver)
BB Smart key (passenger)

(57) **Abstract**: A vehicle control system comprises a vehicular on-board device (2) and a key (3). On the basis of the vehicle being locked by a first key, a confirmation unit (S1-S3, S11-S13, 20, 22, 24) of the vehicular on-board device confirms the presence of a second key, different from the first key, inside a vehicle. A key authentication unit (S23, S24, S32, S33, S41-S43, 30) authenticates that a key user is an authorized user. A validity control unit (S4-S6, S14-S16, S31, S32, 20) of the vehicular on-board device disables functionality of an authorization unit (20) with respect to the second key when the second key is present inside the vehicle and authentication of the second key has failed. The validity control unit enables the functionality of the authorization unit with respect to the second key when the second key is present inside the vehicle and authentication of the second key succeeds.

(57) 要約: 車両制御システムは、車載装置（２）とキー（３）を備える。車載装置の確認部（Ｓ１～Ｓ３、Ｓ１１～Ｓ１３、２０、２２、２４）は、第１キーにより車両が施錠されたことに基づいて、第１キーとは別の第２キーが車室内に有るか否かを確認する。キーの認証部（Ｓ２３、Ｓ２４、Ｓ３２、Ｓ３３、Ｓ４１～Ｓ４３、３０）は、キーを使用するユーザが正規ユーザであることの認証を行う。車載装置の効力制御部（Ｓ４～Ｓ６、Ｓ１４～Ｓ１６、Ｓ３１、Ｓ３２、２０）は、第２キーが車室内に有り、かつ、第２キーに対する認証が失敗であるときには、第２キーに対する許可部（２０）の機能を無効化する。効力制御部は、第２キーが車室内に有り、かつ、第２キーに対する認証が成功であるときには、第２キーに対する許可部の機能を有効化する。

WO 2017/104352 A1

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 ： 車両制御システム

関連出願の相互参照

[0001] 本出願は、２０１５年１２月１４日に出願された日本出願番号２０１５－２４２９９２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、車両に搭載された車載装置とユーザに携帯されるキーとの間の無線通信に基づいて車両に対する所定操作を許可する車両制御システムに関するものである。

背景技術

[0003] 従来、車両に搭載された車載装置とユーザに携帯されるキーとの間の無線通信に基づいて車両の施開錠やエンジン始動といった車両に対する所定操作を許可する車両制御システムが知られている。

[0004] 車両制御システムに関して、特許文献１には、携帯機（キー）が停車後の車内に存在することを示す存在情報を取得した場合には、携帯機からの返信電磁波の受信に基づいて車両に対して所定操作を許可する許可手段の機能を少なくとも一時的に無効化する技術が開示されている。

[0005] 特許文献１の技術によれば、携帯機と車両との間の通信によりドアの施開錠を行う際に、電磁波の車内漏出による携帯機の車内閉じ込みを抑制できるとしている。

先行技術文献

特許文献

[0006] 特許文献1：特開２０１４－２１８８５９号公報

発明の概要

[0007] ところで、キーを車室内に残した状態で別のキーにより車両を施錠した場合、セキュリティ性向上のため、車室内のキーによる車両操作を無効にする構成が考えられる。しかし、この構成を採用した場合、例えば、キーを持つ

同乗者を車室内に残した状態で、運転者が降車して運転者が持つキーで車両を施錠した場合には、同乗者のキーは無効となってしまい、同乗者による車両操作ができないという場合がある。

[0008] 本開示は、キーを車室内に残した状態で別のキーにより車両が施錠された場合、セキュリティ性を確保しつつ、車室内に正規ユーザが居る場合にはその正規ユーザに対してはキーによる車両操作を可能とする車両制御システムを提供することを目的とする。

[0009] 本開示の一態様によれば、車両制御システムは、車両に搭載された車載装置と、車両のユーザに携帯され車載装置との間で無線通信可能なキーとを備える。車載装置は、許可部と、確認部と、効力制御部と、を備える。キーは、認証部と、送信部と、を備える。

[0010] 許可部は、キーとの無線通信に基づいて車両に対する所定操作を許可する。認証部は、キーを使用するユーザが正規ユーザであることの認証を行う。送信部は、認証の結果に応じた認証結果信号を車載装置に送信する。

[0011] キーは第１キーと、第１キーとは別の第２キーを有する。確認部は、第１キーにより車両が施錠されたことに基づいて、第２キーとの車室内での無線通信を試みることで第２キーが車室内に有るか否かを確認する。効力制御部は、確認部により第２キーが車室内に有ることが確認され、かつ、第２キーに対する認証結果信号が、認証が失敗であることを示すときには、第２キーに対する許可部の機能を無効化する。効力制御部は、確認部により第２キーが車室内に有ることが確認され、かつ、第２キーに対する認証結果信号が、認証が成功であることを示すときには、第２キーに対する許可部の機能を有効化する。

[0012] 本開示の一態様によれば、車両の施錠に用いられた第１キーとは別の第２キーが車室内に有る場合に、第２キーを使用するユーザが正規ユーザであるとの認証が成功したときには、第２キーに対する許可部の機能を有効化する。

[0013] したがって、車室内に正規ユーザが居る場合には認証が成功したことを条

件としてその正規ユーザはキーによる車両操作が可能となる。また、認証が失敗のときには、第２キーに対する許可部の機能を無効化するので、正規ユーザが車室内に残っていない状況で第２キーを用いて車両操作が行われてしまうのを抑制できる。つまり、セキュリティ性を確保できる。

図面の簡単な説明

[0014] 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。図面において、

[図1]車両制御システムの構成図であり、

[図2]スマートキーの構成図であり、

[図3]第１実施形態における照合ＥＣＵが実行する処理のフローチャートであり、

[図4]第１実施形態におけるスマートキーの制御部が実行する処理のフローチャートであり、

[図5]車室内のスマートキーを無効化してから、スマートキーとスマートフォンとの間でユーザ認証を自動で行い、認証成功の場合には無効化を解除する処理を示したタイミングチャートであり、

[図6]第２実施形態における照合ＥＣＵが実行する処理のフローチャートであり、

[図7]第２実施形態におけるスマートキーの制御部が実行する処理のフローチャートであり、

[図8]車室内のスマートキーを無効化する前に、スマートキーとスマートフォンとの間でユーザ認証を自動で行い、認証失敗の場合には無効化し、認証成功の場合には有効のままにする処理を示したタイミングチャートであり、

[図9]第３実施形態における照合ＥＣＵが実行する処理のフローチャートであり、

[図10]第３実施形態におけるスマートキーの制御部が実行する処理のフローチャートであり、

[図11]車室内のスマートキーを無効化した後、スマートキーとスマートフォンとの間のユーザ認証を手動で行い、認証成功の場合には無効化を解除する処理を示したタイミングチャートであり、

[図12]スマートキー及びスマートフォンを携帯する同乗者を車室内に残した状態で、運転者が降車して、運転者のスマートキーで車両ドアを施錠した場面を示した図である。

発明を実施するための形態

[0015] （第１実施形態）

以下、本開示の第１実施形態を図面を参照しつつ説明する。

[0016] 図１に示す車両制御システム１は車載装置２とスマートキー３とスマートフォン４とを備えている。

[0017] 車両制御システム１は、車載装置２とスマートキー３との双方向通信に基づいて、車両１００（図１２参照）に対する所定操作、具体的には車両ドアの施開錠やエンジン始動を許可する電子キーシステム（いわゆるスマートエントリーシステム）として構成されている。また、車両制御システム１は、スマートキー３からの一方向通信に基づいて車両ドアの施開錠を行うＲＫＥ（Ｒｅｍｏｔｅ　Ｋｅｙｌｅｓｓ　Ｅｎｔｒｙ）にも対応している。

[0018] 車載装置２は、車両１００に搭載されて、車室内ＬＦ（Ｌｏｗ　Ｆｒｅｑｕｅｎｃｙ）アンテナ２２、車外ＬＦアンテナ２３、ＲＦ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ）受信機２４、ドアロック装置２５、ロックスイッチ２６、アンロックスイッチ２７、エンジンスイッチ２８及びこれらが接続された照合ＥＣＵ２０（ＥＣＵ：Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ）を備えている。

[0019] 車室内ＬＦアンテナ２２及び車外ＬＦアンテナ２３は車両１００に複数箇所に配置されて、その配置位置に応じた範囲に返信を要求する信号をＬＦ帯（例えば１２５ｋＨｚ）の電波として送信するアンテナである。以下では、アンテナ２２、２３から送信される信号をＬＦ信号という。ＬＦ信号は、車室内や車両１００の周辺に存在するスマートキー３を探索するための信号で

ある。車室内ＬＦアンテナ２２は車室内にＬＦ信号を送信する。車外ＬＦアンテナ２３は、車両１００の周辺（例えば車両１００から１ｍ～２ｍ程度の範囲）にＬＦ信号を送信する。

[0020] ＲＦ受信機２４は、スマートキー３からＲＦ帯の電波（例えば３００～４００ＭＨｚの電波）として送信された信号（以下、ＲＦ信号という）を受信する装置である。

[0021] ドアロック装置２５は、各ドアごとに設けられてドアを施錠するロック機構とそのロック機構を施錠側に作動させたり、開錠側に作動させたりするモータとを含んで構成される。

[0022] ロックスイッチ２６は、例えば車両１００の各ドアの車外側に設けられたドアハンドル付近に設けられ、ドアのロック（施錠）を車載装置２（照合ＥＣＵ２０）に指示するための、ユーザにより操作が行われるスイッチ（例えばプッシュスイッチ）である。

[0023] アンロックスイッチ２７は、例えば車両１００の各ドアの車外側に設けられたドアハンドル付近に設けられ、ドアのアンロック（開錠）を車載装置２（照合ＥＣＵ２０）に指示するための、ユーザにより操作が行われるスイッチである。アンロックスイッチ２７は、例えばドアハンドルへのユーザのタッチ（接触）を検出するセンサ（例えば静電容量センサ）として構成される。

[0024] なお、ロックスイッチ２６及びアンロックスイッチ２７は、単一のスイッチ（例えばプッシュスイッチ）で兼用しても良い。この場合、照合ＥＣＵ２０は、ドアが施錠されている時にスイッチの操作があった場合には、アンロックの指示があったものとして処理を行い、反対に、ドアが開錠されている時にスイッチの操作があった場合には、ロックの指示があったものとして処理を行う。

[0025] エンジンスイッチ２８は、車室内の運転席周辺のインストルメントパネル部に設けられ、車両１００のエンジンの始動を車載装置２に指示するための、ユーザにより操作が行われるスイッチ（例えばプッシュスイッチ）である

。

[0026] 照合ＥＣＵ２０は、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成され、電子キーシステムに関する各種処理を実行する制御装置である。照合ＥＣＵ２０には、ＲＯＭ、ＲＡＭ等の、各種情報を記憶したメモリ２１が設けられている。このメモリ２１には、照合ＥＣＵ２０が実行する処理のプログラムや、スマートキー３が正規のスマートキーであることの認証に用いられる照合用データ（マスターＩＤコード）等が記憶されている。また、スマートキー３は複数（図１では２つ）設けられており、メモリ２１には、各スマートキー３のＩＤ（識別情報）が登録されている。

[0027] 照合ＥＣＵ２０の処理の概要を説明すると、ユーザが車両１００に乗車する場面では、照合ＥＣＵ２０は、車外ＬＦアンテナ２３に、車両１００の周辺にＬＦ信号を送信させる。照合ＥＣＵ２０は、ＬＦ信号に応答してスマートキー３から送信されたＲＦ信号をＲＦ受信機２４が受信した場合には、そのＲＦ信号に含まれた照合用データ（ＩＤコード）と、照合ＥＣＵ２０が持つ照合用データ（マスターＩＤコード）とを照合し、照合成功した場合にドアを開錠許可状態（アンロックスイッチ２７のスタンバイ状態）にする。その後、照合ＥＣＵ２０は、アンロックスイッチ２７が操作された場合に、ドアロック装置２５にドアを開錠させる。

[0028] また、照合ＥＣＵ２０は、車両１００のエンジンを始動させる場面では、エンジンスイッチ２８が操作されたことに基づいて、車室内ＬＦアンテナ２２にＬＦ信号を送信させる。照合ＥＣＵ２０は、そのＬＦ信号に応答するＲＦ信号をＲＦ受信機２４が受信した場合には、上記と同様に照合を行い、照合成功した場合にエンジンＥＣＵ（図示外）にエンジン始動を指示する。

[0029] また、照合ＥＣＵ２０は、ユーザが車両１００から降車する場面では、ロックスイッチ２６が操作されたことに基づいて、ＬＦアンテナ２２、２３に車両１００の周辺及び車室内にＬＦ信号を送信させる。そして、照合ＥＣＵ２０は車外に送信したＬＦ信号に基づいて上記照合が成功した場合にはドアロック装置２５にドアを施錠させる。

[0030] 一方、照合ＥＣＵ２０は、車外に送信したＬＦ信号に基づく照合は失敗し、且つ、車室内に送信したＬＦ信号に基づく照合は成功した場合には、スマートキー３が車室内に置かれたままの可能性があるとして、ドアの施錠を中止して、ブザー等で警告を行う。

[0031] また、照合ＥＣＵ２０は、ＲＫＥシステムに関する処理として、スイッチ３５、３６（図２参照）の操作に基づいてスマートキー３から送信されたＲＦ信号をＲＦ受信機２４が受信した場合には、受信信号がロックを指示する信号かアンロックを指示する信号かを判別し、その判別結果に応じてドアを施錠したり開錠したりする。

[0032] なお、スマートキー３から送信されるＲＦ信号には、スマートキー３のＩＤが含まれている。照合ＥＣＵ２０は、ＲＦ信号に含まれたＩＤにより、登録された複数のスマートキー３のうちどのスマートキー３によって車両操作が行われたのかを特定可能である。

[0033] 以上が照合ＥＣＵ２０が実行する処理の概要であるが、後にフローチャートを参照してさらに詳しく説明する。

[0034] 次に、スマートキー３の構成を説明する。スマートキー３は、車両１００のユーザに携帯されるものである。本実施形態では、スマートキー３は２つ設けられており、一方のスマートキー３は車両１００の運転者に携帯され、他方のスマートキー３は同乗者に携帯されている。

[0035] 図２に示すように、スマートキー３は、ＬＦ受信部３２、ＲＦ送信部３３、ＢＴ通信部３４、ロックスイッチ３５、アンロックスイッチ３６及びこれらが接続された制御部３０を備えている。

[0036] ＬＦ受信部３２は、車載装置２から送信されたＬＦ信号を受信する部分である。ＲＦ送信部３３は、制御部３０から出力された送信信号をＲＦ帯の電波（ＲＦ信号）としてスマートキー３の周辺に送信する部分である。ＲＦ送信部３３による信号の送信範囲は、例えばスマートキー３から１０ｍ～３０ｍ程度に設定されている。

[0037] ＢＴ通信部３４は、Ｂｌｕｅｔｏｏｔｈ（登録商標）の通信機能を有した

周囲の無線通信機（本実施形態ではスマートフォン４）と、Ｂｌｕｅｔｏｏｔｈ（登録商標）の通信方式に則って無線通信を行う装置である。ＢＴ通信部３４の通信範囲（通信距離）は例えばスマートキー３から数ｍ～数十ｍの範囲に設定されている。なお、Ｂｌｕｅｔｏｏｔｈ（登録商標）により無線通信を行うには、通信を行う両通信機間でペアリングをする必要がある。

[0038] ロックスイッチ３５及びアンロックスイッチ３６は、スマートキー３の筐体から露出する形で設けられ、車両ドアのロック（ロックスイッチ３５の場合）又はアンロック（アンロックスイッチ３６の場合）を指示するための、ユーザにより操作が行われるスイッチ（例えばプッシュスイッチ）である。

[0039] 制御部３０は、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成され、電子キーシステムに関する各種処理を実行する部分である。制御部３０は、ＲＯＭ、ＲＡＭ等の、各種情報を記憶したメモリ３１が設けられている。このメモリ３１には、制御部３０が実行する処理のプログラムや、スマートキー３が正規のスマートキーであることの認証に用いられる照合用データや、スマートキー３のＩＤ等が記憶されている。

[0040] さらに、メモリ３１には、スマートキー３を使用するユーザが正規ユーザであることを認証するためのデータ（以下、ユーザ認証用データという）が記憶されている。このユーザ認証は、スマートキー３とスマートフォン４との間で行われる認証である。ユーザ認証は、言い換えると、スマートキー３が、スマートフォン４を携帯するユーザに携帯されている又はそのユーザの支配下にある状態にあることの認証である。

[0041] 制御部３０が実行する処理の概要を説明すると、制御部３０は、車載装置２からのＬＦ信号をＬＦ受信部３２が受信した場合には、受信したＬＦ信号に応答する信号を生成して、その信号をＲＦ信号としてＲＦ送信部３３に送信させる。

[0042] また、制御部３０は、ＲＫＥシステムに関する処理として、ロックスイッチ３５が操作された場合には、車両ドアの施錠を指示するＲＦ信号をＲＦ送信部３３に送信させる。また、制御部３０は、アンロックスイッチ３６が操

作された場合には、車両ドアの開錠を指示するＲＦ信号をＲＦ送信部３３に送信させる。なお、制御部３０は、ＲＦ信号に、メモリ３１に記憶された照合用データや自身のＩＤを含める。

[0043] 以上が制御部３０が実行する処理の概要であるが、後にフローチャートを参照してさらに詳しく説明する。

[0044] 次に、スマートフォン４の構成を説明する。スマートフォン４は、車両１００の正規ユーザに携帯され、無線により通話が可能な通話機能を有した公知の携帯電話である。以下では、スマートフォン４は、車両１００の同乗者に携帯されているとして説明する。スマートフォン４は、ＢＴ通信部４２、表示部４３、入力部４４及びこれらが接続された制御部４０を備えている。

[0045] ＢＴ通信部４２は、Ｂｌｕｅｔｏｏｔｈ（登録商標）の通信機能を有した周囲の無線通信機と、Ｂｌｕｅｔｏｏｔｈ（登録商標）の通信方式に則って無線通信を行う通信装置である。ＢＴ通信部４２の通信範囲は例えばスマートフォン４から数ｍ～数十ｍの範囲に設定されている。なお、ＢＴ通信部３４、４２の通信範囲は、車室内程度の範囲とするのが好ましい。

[0046] 車室内に対して通信範囲があまりに広いと、同乗者が車室内に残っていない場合であっても、車室内に存在するスマートキー３と、車外の同乗者が携帯するスマートフォン４との間でユーザ認証が成功してしまう可能性があり、同乗者が車室内に残っている場合にスマートキー３を有効化するという趣旨に反してしまうためである。

[0047] 表示部４３は例えば液晶ディスプレイであり各種情報を表示する。入力部４４は、ユーザによる電話番号等の入力操作を受け付ける部分である。入力部４４は、表示部４３に表示される入力画面へのタッチ操作を検出するセンサであったり、可動操作部及びその可動操作部への操作を検出するセンサであったりする。

[0048] 制御部４０は、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成され、通話機能に関する処理を実行したり、ＢＴ通信部４２を制御したりする。制御部４０は、ＲＯＭ、ＲＡＭ等の、各種情報を記憶したメモリ４１が設けられている。この

メモリ４１には、制御部４０が実行する処理のプログラム等が記憶されている。

[0049] さらに、メモリ４１には、スマートキー３との間でスマートキー３のユーザ認証を行うためのユーザ認証用データが記憶されている。そのユーザ認証用データは、スマートキー３のメモリ３１に記憶されたユーザ認証用データと照合するためのデータである。スマートキー３とスマートフォン４とは、ＢＴ通信部３４、４２間の無線通信に基づいて、スマートキー３のユーザ認証が可能に構成されている。

[0050] ここで、図１２は、同乗者を車室内に残した状態で、運転者が降車して、運転者が携帯するスマートキー３で車両ドアを施錠した場面を示している。同乗者は、運転者のスマートキー３（第１キー）とは別のスマートキー３（第２キー）を携帯している。また、同乗者は、スマートキー３のユーザ認証が可能なスマートフォン４も携帯している。この場面では、降車した運転者が戻ってこない場合には、同乗者が、自身が携帯するスマートキー３で車両１００を操作する必要がある。

[0051] 一方で、仮に同乗者が存在せず、スマートキー３を車室内に残した状態で、運転者が別のスマートキー３で車両を施錠した場合には、車室内のスマートキー３を有効のままにしておくと、不正に車室内にアクセスした侵入者はそのスマートキー３を用いて車両１００を盗難するおそれがある。そこで、車両制御システム１は、スマートキー３を車室内に残した状態で、別のスマートキー３で車両１００が施錠される場面では、同乗者が車室内に居る場合には車室内のスマートキー３を有効とし、同乗者が居ない場合にはスマートキー３を無効とするように作用する。

[0052] 以下では、車載装置２、スマートキー３及びスマートフォン４が実行する、車室内に残っているスマートキー３に対する車両操作機能を状況に応じて無効化したり有効化したりする処理を説明する。先ず、図３、図５を参照して車載装置２の処理を説明する。図５は図１２の場面を想定したタイミングチャートである。また、図５においては、車室内に残っているスマートキー

３（ＢＴ通信部３４）及びスマートフォン４（ＢＴ通信部４２）は双方向通信が可能に予めペアリングが行われているものとする。

[0053] なお、スマートキー３及びスマートフォン４の間の初めてのペアリングは、スマートキー３及びスマートフォン４に対するユーザの操作に基づいて行われる。一回でもペアリングが行われたスマートキー３及びスマートフォン４の組は、以降は、ＢＴ通信部３４、４２の通信可能範囲に接近した時にユーザ操作が無くても自動的にペアリングが行われるとしても良いし、２回目以降のペアリングにおいてもユーザ操作を必要としても良い。

[0054] 照合ＥＣＵ２０は、図３の処理を開始すると、スマートキー３により車両１００の施錠操作が行われたか否かを判断する（Ｓ１）。この施錠操作は、車載装置２からのＬＦ信号に応答してスマートキー３から送信されるＲＦ信号に基づく施錠操作と、ロックスイッチ３５（図２参照）の操作によりスマートキー３から送信されるＲＦ信号に基づく施錠操作（ＲＫＥロック）の両方を含む。また、スマートキー３にメカニカルキーが備えられている場合には、そのメカニカルキーを車両ドアの外面に設けられるキーシリンダに挿入することにより行われる施錠操作も、Ｓ１の処理における施錠操作に含まれる。一方、車室内に設けられたノブ操作による施錠操作は、Ｓ１の処理における施錠操作には含まれない。図５では、運転者が携帯するＩＤ＝１のスマートキー３でＲＫＥロックが行われた例を示している。

[0055] 車両施錠操作が無い場合には（Ｓ１：Ｎｏ）、車両施錠操作が有るまで待機する。車両施錠操作がある場合には（Ｓ１：Ｙｅｓ）、車両施錠操作に用いられたスマートキー３とは別のスマートキー３が車室内に残っているか否かを確認するための車室内照合を行う（Ｓ２）。

[0056] 具体的には、図５に示すように、照合ＥＣＵ２０は、車室内ＬＦアンテナ２２に指示をして、車室内にＬＦ信号を送信させる。この際、ＬＦ信号に、ＬＦ信号を受信したスマートキー３にスマートフォン４との間でユーザ認証を実施するよう要求する認証要求データを、含ませる。Ｓ２では、送信したＬＦ信号に応答するＲＦ信号をＲＦ受信機２４が受信した場合には、受信し

たＲＦ信号に含まれている照合用データと、照合ＥＣＵ２０が保有する照合用データとを照合する。

[0057] 次に、車室内照合の結果を確認して（Ｓ３）、照合失敗の場合、つまり、スマートキー３からのＲＦ信号の受信が無い場合又はＲＦ信号を受信したが照合が失敗した場合には、車室内にスマートキー３が存在しないとして、図３の処理を終了する。

[0058] 一方、車室内照合が成功した場合には、車室内に、施錠操作に用いられたスマートキー３とは別のスマートキー３が存在するとして、その車室内キー３に対する車両操作の機能を無効化する（Ｓ４）。

[0059] 具体的には、Ｓ２の車室内照合の際に受信したＲＦ信号に含まれたＩＤを、無効のキーＩＤとしてメモリ２１に保持しておく。以降、無効のキーＩＤを有したＲＦ信号を受信したとしても、このＲＦ信号を無視し、車両操作を許可しない。図５では、ＩＤ＝２のスマートキー３が車室内に存在しており、そのスマートキー３を無効する例を示している。

[0060] また、車両制御システム１にイモビライザーが備えられている場合には、無効化したスマートキー３に対してはイモビライザーに基づく車両操作も無効とする。なお、イモビライザーとは、車両に備えられた電波発生装置にキーを近づけると、電波発生装置から発生した電波によりキーに備えられたトランスポンダに電力を発生させて、その発生電力によりキーから車両に照合用データを送信させることで、車両側でキーの照合を行い、照合成功の場合にエンジン始動を許可するというものである。これによれば、キーのバッテリが切れたとしても、エンジン始動が可能となる。

[0061] 次に、無効化したスマートキー３から、該スマートキー３のユーザ認証が成功した時に送信される有効化要求のＲＦ信号を受信したか否かを判断する（Ｓ５）。有効化要求の受信が無い場合には（Ｓ５：Ｎｏ）、図３の処理を終了する。この場合には、車室内キー３に対する無効化を維持する。

[0062] 一方、有効化要求を受信した場合には（Ｓ５：Ｙｅｓ）、無効化したキー３（図５の例ではＩＤ＝２のキー）の無効化を解除つまり有効化する（Ｓ６

）。その後、図３の処理を終了する。

[0063] なお、照合ＥＣＵ２０は、車室内のスマートキー３を無効化した場合に、無効化したスマートキー３以外のスマートキー３（つまり有効のスマートキー）により車両操作（車両ドアの施開錠やエンジン始動）が有った時にも、無効化したスマートキー３に対する無効化を解除する。

[0064] 次に、図４、図５を参照してスマートキー３及びスマートフォン４の処理を説明する。スマートキー３の制御部３０は、図４の処理を開始すると、図３のＳ２で車載装置２から送信される認証要求データを含んだＬＦ信号を受信したか否かを判断する（Ｓ２１）。受信が無い場合には（Ｓ２１：Ｎｏ）、図４の処理を終了する。

[0065] 認証要求データを含んだＬＦ信号を受信した場合には（Ｓ２１：Ｙｅｓ）、車室内にスマートキー３が存在することを示したＲＦ信号をＲＦ受信部３３に送信させることで、ＬＦ信号の受信に対する応答を行う（Ｓ２２）。ここで送信するＲＦ信号は、自身のＩＤ及び、車載装置２側でキー３を認証するための照合用データを含んだ信号である。この応答により、施錠操作に用いられたスマートキー３とは別のスマートキー３が車室内に残っていることを車載装置２側に認識させることができる。そして、図３のＳ４の処理により車室内キーの無効化処理が行われる。

[0066] 次に、制御部３０は、ＢＴ通信部３４を用いた無線通信により、スマートフォン４に対して（言い換えるとスマートフォン４のＢＴ通信部４２宛に）ユーザ認証依頼を行う（Ｓ２３）。このユーザ認証依頼は、認証要求データを含んだＬＦ信号の受信をトリガとして行われ、言い換えるとユーザの操作が無くても自動で行われる処理である。

[0067] ユーザ認証依頼を行った後、ＢＴ通信部３４、４２間の無線通信に基づいてスマートキー３のユーザ認証を行う（Ｓ２４）。具体的には、制御部３０のメモリ３１に記憶されたユーザ認証用データと、スマートフォン４のメモリ４１に記憶されたユーザ認証用データとの照合を行う。その照合は、スマートキー３側で行っても良いし、スマートフォン４側で行っても良い。例え

ばスマートフォン４側で照合を行う場合には、スマートキー３が保有するユーザ認証用データをスマートフォン４に送信する。スマートフォン４（制御部４０）は、自身が保有するユーザ認証用データと、スマートキー３からの認証用データとを照合する。スマートフォン４は、その照合が成功した場合には、ユーザ認証が成功したことを示す信号をスマートキー３に送信する。

[0068] ユーザ認証は以下のように行っても良い。すなわち、スマートフォン４は、例えばスマートキー３からのユーザ認証依頼及びユーザ認証用データを受信した場合に、表示部４３にパスワードの入力を促すメッセージを表示させる。その後、入力部４４によりパスワードが入力された場合には、そのパスワードと、スマートキー３から送信されたユーザ認証用データ（パスワード）とを照合することで、ユーザ認証を実施しても良い。

[0069] または、スマートフォン４は、表示部４３にパスワードの入力を促すメッセージを表示させた後、入力部４４によりパスワードが入力された場合には、そのパスワードをスマートキー３に送信する。スマートキー３は、スマートフォン４から送信されたパスワードと、自身が保有するユーザ認証用データ（パスワード）とを照合することで、ユーザ認証を行っても良い。

[0070] なお、Ｓ２３のユーザ認証依頼及びＳ２４のユーザ認証は、ＢＴ通信部３４、４２間で予めペアリングが行われて無線通信可能な状態にある場合に成立する処理である。反対に、スマートキー３とスマートフォン４とが、ＢＴ通信部３４、４２の通信範囲外に位置していたり、通信範囲内に位置していたとしてペアリングが行われていなかったりした場合つまり無線通信可能な状態にない場合には、ユーザ認証は失敗となる。

[0071] 制御部３０は、スマートフォン４との間のユーザ認証が成功したか否かを判断する（Ｓ２５）。ユーザ認証が失敗した場合には（Ｓ２５：Ｎｏ）、図４の処理を終了する。この場合には、スマートフォン４が車室内に存在しない状況や、車室内に存在したとしても予めペアリングが行われていない状況等を想定している。

[0072] 一方、ユーザ認証が成功した場合には（Ｓ２５：Ｙｅｓ）、ＲＦ送信部３

３に、有効化を要求するＲＦ信号を送信させる（Ｓ２６）。このとき、ＲＦ信号に、自身のＩＤを含める。これにより、図３のＳ６の処理により無効化が解除される。その後、図４の処理を終了する。

[0073] 図５の例では、ＩＤ＝２のスマートキーが無効化された後、そのスマートキーとスマートフォンとの間でユーザ認証が行われて、ユーザ認証が成功となる。そして、スマートキーから車載装置に有効化要求が送信される例を示している。

[0074] このように、本実施形態では、照合ＥＣＵ２０は、スマートキー３により車両施錠操作があった場合には、車室内に別のスマートキー３が存在するかを確認し、存在する場合にユーザ認証の結果を待たずに直ちに車室内のスマートキー３に対する車両操作機能を無効化する。そして、無効化した後、ユーザ認証が成功したことを確認できた時に無効化を解除する。

[0075] これによれば、車両施錠操作がされた車両に正規ユーザが残っていた場合には、この正規ユーザが携帯するスマートキー３及びスマートフォン４との間でユーザ認証が行われることで、スマートキー３を有効にすることができる。よって、車室内に残った正規ユーザは、自身が携帯するスマートキー３によってエンジン始動といった車両操作を行うことができる。

[0076] また、車室内に正規ユーザが居ない状態でスマートキー３が存在する場合には、スマートキー３のユーザ認証が失敗となり、スマートキー３を無効にできる。これにより、車室内に不正に侵入した侵入者が居たとしても、その侵入者により車室内のスマートキー３を用いて車両操作が行われてしまうのを抑制でき、セキュリティ性を確保できる。

[0077] また、本実施形態では、スマートキー３とスマートフォン４とが無線通信可能な状態にあることを条件として、ＬＦ信号の受信をトリガとしてスマートキー３のユーザ認証が自動で開始するので、ユーザの操作負担を軽減できる。

[0078] なお、スマートキーにより車両施錠操作が行われた場合には警戒モードに移行して、警戒モード中は車両盗難を防ぐためにスマートキーを用いずに車

両ドアが開けられた時に警報を発するシステムがある。警報が鳴った場合には、スマートキーにより車両操作が行われたことを条件に警報を停止させることができる。

[0079] このシステムを採用した場合、車両施錠操作が行われた際に車室内に別のスマートキー及び同乗者が残っていて、同乗者が内側から車両ドアを開けると警報が鳴ってしまう。このとき、車室内のスマートキーが有効になっていると、そのスマートキーにより車両操作（施開錠等）を行うことで警報を停止させることができる。

[0080] （第２実施形態）

次に、本開示の第２実施形態を上記実施形態と異なる部分を中心に説明する。本実施形態は、施錠操作に用いられたスマートキーとは別のスマートキーが車室内に存在する場合には、ユーザ認証の結果を待ってスマートキーの有効化、無効化を制御する実施形態である。本実施形態では、照合ＥＣＵ２０及び制御部３０が実行する処理が第１実施形態と異なっており、それ以外は第１実施形態と同じである。

[0081] 図６、図８を参照して、照合ＥＣＵ２０が実行する処理から説明する。照合ＥＣＵ２０は、図６の処理を開始すると、図５のＳ１、Ｓ２の処理と同様に、スマートキー３による車両施錠操作の有無を判断し（Ｓ１１）、車両施錠操作が有った場合には（Ｓ１１：Ｙｅｓ）、車室内に別のスマートキー３が存在するか否かを確認するために車室内ＬＦアンテナ２２にＬＦ信号を送信させる（Ｓ１２）。Ｓ１２では、５のＳ２の処理と同様に、ＬＦ信号に、ユーザ認証を実施するよう要求する認証要求データを含ませる。

[0082] 次に、Ｓ１２で送信したＬＦ信号に応答するＲＦ信号の受信の有無を判断する（Ｓ１３）。ＲＦ信号の受信が無い場合には（Ｓ１３：Ｎｏ）、車室内にスマートキー３が存在しないとして、図６の処理を終了する。

[0083] これに対して、ＲＦ信号を受信した場合には（Ｓ１３：Ｙｅｓ）、受信したＲＦ信号に、有効化を要求するデータと、無効化を要求するデータのどちらが含まれているかを判断することで、スマートキー３の認証の結果を確認

する（Ｓ１４）。ＲＦ信号に有効化要求のデータが含まれている場合つまりユーザ認証が成功の場合には、車室内のスマートキー３に対する車両操作機能を有効のままにする（Ｓ１５）。その後、図６の処理を終了する。図８の「ユーザ認証結果ＯＫ」の部分には、車室内のスマートキーを有効化する場合を示している。

[0084] 一方、ＲＦ信号に無効化要求データが含まれている場合つまりユーザ認証が失敗の場合には、車室内のスマートキー３に対する車両操作機能を無効化する（Ｓ１６）。その後、図６の処理を終了する。図８の「ユーザ認証結果ＮＧ」の部分には、車室内のスマートキーを無効化する場合を示している。

[0085] 次に、図７、図８を参照して、制御部３０（スマートキー３）が実行する処理を説明する。制御部３０は、図７の処理を開始すると、図６のＳ１２で車載装置２から送信される認証要求データを含んだＬＦ信号を受信したか否かを判断する（Ｓ３１）。受信していない場合には（Ｓ３１：Ｎｏ）、図７の処理を終了する。

[0086] ＬＦ信号を受信した場合には（Ｓ３１：Ｙｅｓ）、図４のＳ２３～Ｓ２５と同様に、ＢＴ通信部３４、４２間の無線通信に基づいてスマートキー３からスマートフォン４にユーザ認証依頼を行った後、ユーザ認証を行う（Ｓ３２、Ｓ３３、Ｓ３４）。

[0087] ユーザ認証が成功した場合には（Ｓ３４：Ｙｅｓ）有効化を要求するデータを含んだＲＦ信号を送信する（Ｓ３５）。ユーザ認証が失敗した場合には（Ｓ３４：Ｎｏ）無効化を要求するデータを含んだＲＦ信号を送信する（Ｓ３６）。その後、図７の処理を終了する。なお、Ｓ３４では、スマートフォン４へのユーザ認証依頼に対してスマートフォン４から応答が無い場合にも、ユーザ認証が失敗したと判断する。

[0088] このように、本実施形態によっても、第１実施形態と同様の効果を得ることができる。

[0089] （第３実施形態）

次に、本開示の第３実施形態を上記実施形態と異なる部分を中心に説明す

る。本実施形態は、スマートキーが無効化になった後に、ユーザによる手動操作をトリガとしてスマートキーとスマートフォン間のユーザ認証を行い、そのユーザ認証が成功した場合には無効化を解除する実施形態である。

[0090] 図１のスマートフォン４は、入力部４４を用いてユーザ認証の開始を要求する入力操作が可能に構成されている。ユーザによって、ユーザ認証の開始を要求する入力操作が行われた場合には、制御部４０は、ＢＴ通信部４２を用いて、スマートキー３に対してユーザ認証の開始を要求する信号を送信する。

[0091] 以下、図９～図１１を参照して、照合ＥＣＵ２０及び制御部３０が実行する処理を説明する。図９、図１０の処理は、車室内のスマートキー３が無効化状態の時に実行されることを想定している。すなわち、図９の処理は、例えば図３においてＳ５の処理が否定判断された後に続けて実行され、又は図６においてＳ１６の処理の後に続けて実行される。また、図１０の処理は、例えば図４においてＳ２５の処理が否定判断された後に続けて実行され、又は図７においてＳ３６の処理の後に続けて実行される。

[0092] 先ず、制御部３０が実行する処理から説明する。制御部３０は、図１０の処理を開始すると、スマートフォン４からの、ユーザ認証の開始を要求する信号の受信の有無を判断する（Ｓ４１）。受信が無い場合には（Ｓ４１：Ｎｏ）、受信が有るまで待機する。ＢＴ通信部３４がスマートフォン４からの信号を受信した場合には（Ｓ４１：Ｙｅｓ）、図４のＳ２３～Ｓ２５と同様に、ＢＴ通信部３４、４２間の無線通信に基づいてスマートキー３からスマートフォン４にユーザ認証依頼を行った後、ユーザ認証を行う（Ｓ４２、Ｓ４３、Ｓ４４）。ユーザ認証が成功した場合には（Ｓ４４：Ｙｅｓ）有効化を要求するＲＦ信号を送信する（Ｓ４５）。ユーザ認証が失敗した場合には（Ｓ４４：Ｎｏ）図７の処理を終了する。

[0093] 次に、照合ＥＣＵ２０が実行する処理を説明する。照合ＥＣＵ２０は、図９の処理を開始すると、図１０のＳ４５でスマートキー３から送信される有効化要求信号を受信したか否かを判断する（Ｓ３１）。受信が無い場合には

（Ｓ３１：Ｎｏ）、受信が有るまで待機する。有効化要求信号を受信した場合には（Ｓ３１：Ｙｅｓ）、スマートキー３の無効化を解除する（Ｓ３２）。その後、図９の処理を終了する。なお、図１１のタイミングチャートでは、第２実施形態の方法によりスマートキーを無効化した後に、図９、図１０の処理により無効化を解除した例を示している。

[0094] このように本実施形態によれば、例えば車室内に同乗者が残っているがスマートキー３とスマートフォン４とが通信可能範囲まで接近していなかったり、接近していたとしてもペアリングが未実施であるとして第１、第２実施形態の処理により車室内のスマートキー３が無効になったとしても、スマートキー３が無効になっていることを気付いた同乗者が手動でユーザ認証を開始させることができるので、事後的に当該スマートキー３を有効にすることができる。

[0095] 本開示において、例えばスマートフォン以外の、正規ユーザに携帯される通信機能を有した携帯装置を用いて、車室内スマートキーのユーザ認証を行っても良い。また、上記実施形態では、Ｂｌｕｅｔｏｏｔｈ（登録商標）の通信に基づいてスマートキーのユーザ認証を行う例を示したが、他の無線通信規格（例えば、赤外線通信、無線ＬＡＮ、ＮＦＣ（Ｎｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ）等）や有線通信に基づいて、ユーザ認証を行っても良い。

[0096] また、スマートキーとスマートフォンとの通信が成立したことをもって、スマートキーのユーザ認証が成功したと判定しても良い。この場合、上記実施形態の例では、スマートキーのＢＴ通信部とスマートフォンのＢＴ通信部とがペアリングされた状態にある場合にユーザ認証の成功とし、ペアリングされた状態にない場合にユーザ認証の失敗とする。これによれば、ペアリングしたうえでスマートキー及びスマートフォンが相互に保有するユーザ認証用データの照合を行う必要がないので、スマートキーを使用するユーザが正規ユーザであるか否かを簡易に判定できる。

[0097] また、スマートキーに、ユーザ認証のための秘密情報を入力する入力部を

設けて、ユーザの操作に基づいて入力部から入力された情報と、スマートキーに予め記憶された秘密情報とを照合し、照合成功した場合にユーザ認証の成功としても良い。この場合、スマートキーにもともと備えられているロックスイッチ及びアンロックスイッチを、秘密情報を入力する入力部として兼用しても良い。

[0098] この場合、例えば、ユーザ認証を行う際には、ユーザにロックスイッチ及びアンロックスイッチを操作させて、その操作パターンが特定の操作パターンに一致する場合に、ユーザ認証の成功とする。例えば、ロックスイッチの操作を１、アンロックスイッチの操作を０、秘密情報を１０１１としたときには、ロックスイッチ、アンロックスイッチ、ロックスイッチ、ロックスイッチの順に操作された場合に、ユーザ認証が成功となる。

[0099] また、スマートキーに、ユーザの生体情報（指紋、声等）を入力する入力部と、正規ユーザの生体情報（指紋、声等）を記憶する記憶部とを設ける。そして、入力部から入力された生体情報と、記憶部に記憶された生体情報との照合により、ユーザ認証を行っても良い。

[0100] なお、上記実施形態において照合ＥＣＵ２０が許可部に相当する。図３のＳ１～Ｓ３、図６のＳ１１～Ｓ１３の処理を実行する照合ＥＣＵ２０、車室内ＬＦアンテナ２２及びＲＦ受信機２４が確認部に相当する。図４のＳ２３、Ｓ２４、図７のＳ３２、Ｓ３３、図１０のＳ４１～Ｓ４３の処理を実行する制御部３０が認証部に相当する。図４のＳ２５、Ｓ２６、図７のＳ３４～Ｓ３６、図１０のＳ４４、Ｓ４５の処理を実行する制御部３０及びＲＦ送信部３３が送信部に相当する。図３のＳ４～Ｓ６、図６のＳ１４～Ｓ１６、図９のＳ３１、Ｓ３２の処理を実行する照合ＥＣＵ２０が効力制御部に相当する。図４のＳ２６、図７のＳ３５、Ｓ３６、図１０のＳ４５で送信される有効化要求の信号又は無効化要求の信号が認証結果信号に相当する。スマートフォン４が携帯装置に相当する。図３のＳ２、図６のＳ１２で送信されるＬＦ信号が確認用信号に相当する。

[0101] 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（１００）に搭載された車載装置（２）と、

前記車両のユーザに携帯され前記車載装置との間で無線通信可能なキー（３）と、を備え、

前記車載装置は、

前記キーとの無線通信に基づいて前記車両に対する所定操作を許可する許可部（２０）を備え、

前記キーは、

前記キーを使用するユーザが正規ユーザであることの認証を行う認証部（Ｓ２３、Ｓ２４、Ｓ３２、Ｓ３３、Ｓ４１～Ｓ４３、３０）と、

前記認証の結果に応じた認証結果信号を前記車載装置に送信する送信部（Ｓ２５、Ｓ２６、Ｓ３４～Ｓ３６、Ｓ４４、Ｓ４５、３０、３３）と、を備え、

前記キーは、第１キーと、前記第１キーとは別の第２キーを有しており、

前記車載装置は、

前記第１キーにより前記車両が施錠されたことに基づいて、第２キーとの車室内での無線通信を試みることで前記第２キーが車室内に有るか否かを確認する確認部（Ｓ１～Ｓ３、Ｓ１１～Ｓ１３、２０、２２、２４）と、

前記確認部により前記第２キーが車室内に有ることが確認され、かつ、前記第２キーに対する前記認証結果信号が、前記認証が失敗であることを示すときには前記第２キーに対する前記許可部の機能を無効化し、前記確認部により前記第２キーが車室内に有ることが確認され、かつ、前記第２キーに対する前記認証結果信号が、前記認証が成功であることを示すときには前記第２キーに対する前記許可部の機能を有効化する効力制御部（Ｓ４～Ｓ６、Ｓ１４～Ｓ１６、Ｓ３１、Ｓ３

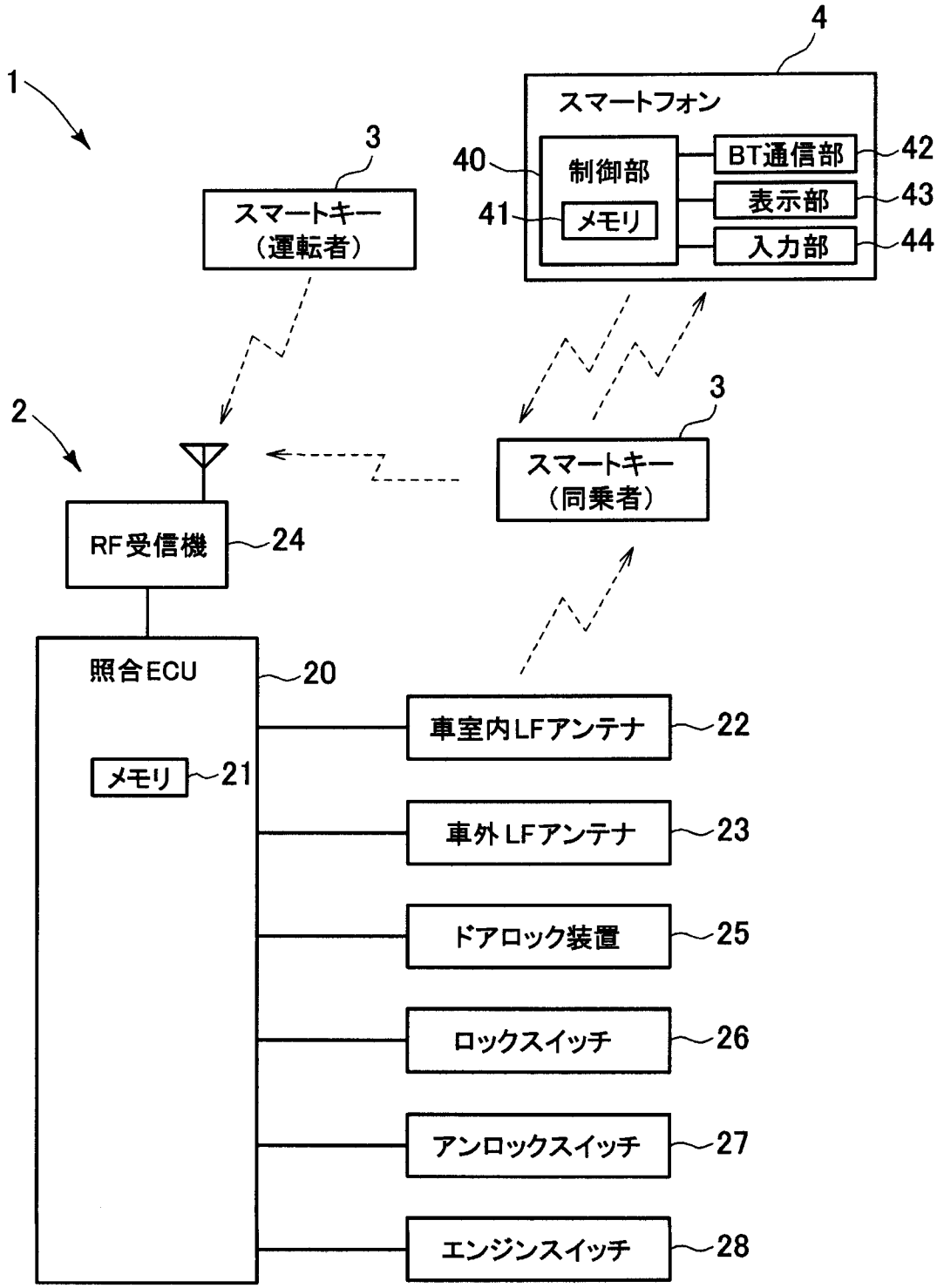
２、２０）と、を備える車両制御システム。

[請求項2] 前記認証部は、正規ユーザに携帯される通信機能を有する携帯装置（４）との間の通信に基づき前記認証を行う請求項１に記載の車両制御システム。

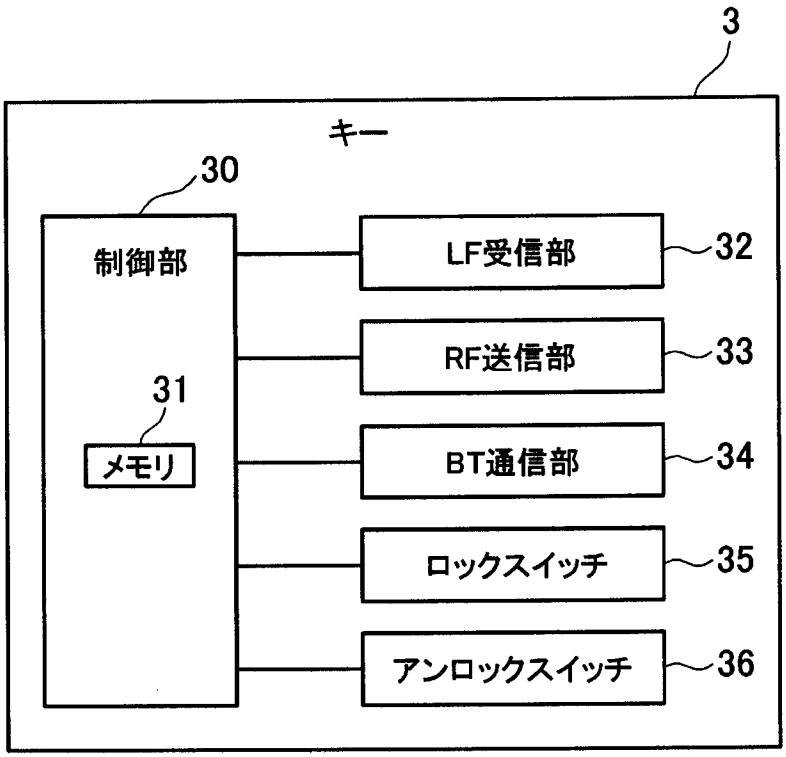
[請求項3] 前記確認部は、前記第１キーにより前記車両が施錠されたことに基づいて、前記第２キーの有無の確認用信号を車室内に送信し、その確認用信号に応答して前記第２キーから送信される応答信号の有無に基づいて車室内における前記第２キーの有無を判定し、

前記認証部（Ｓ２３、Ｓ２４、Ｓ３２、Ｓ３３、３０）は前記確認用信号を受信したことをトリガとして前記携帯装置との間で前記認証を開始する請求項２に記載の車両制御システム。

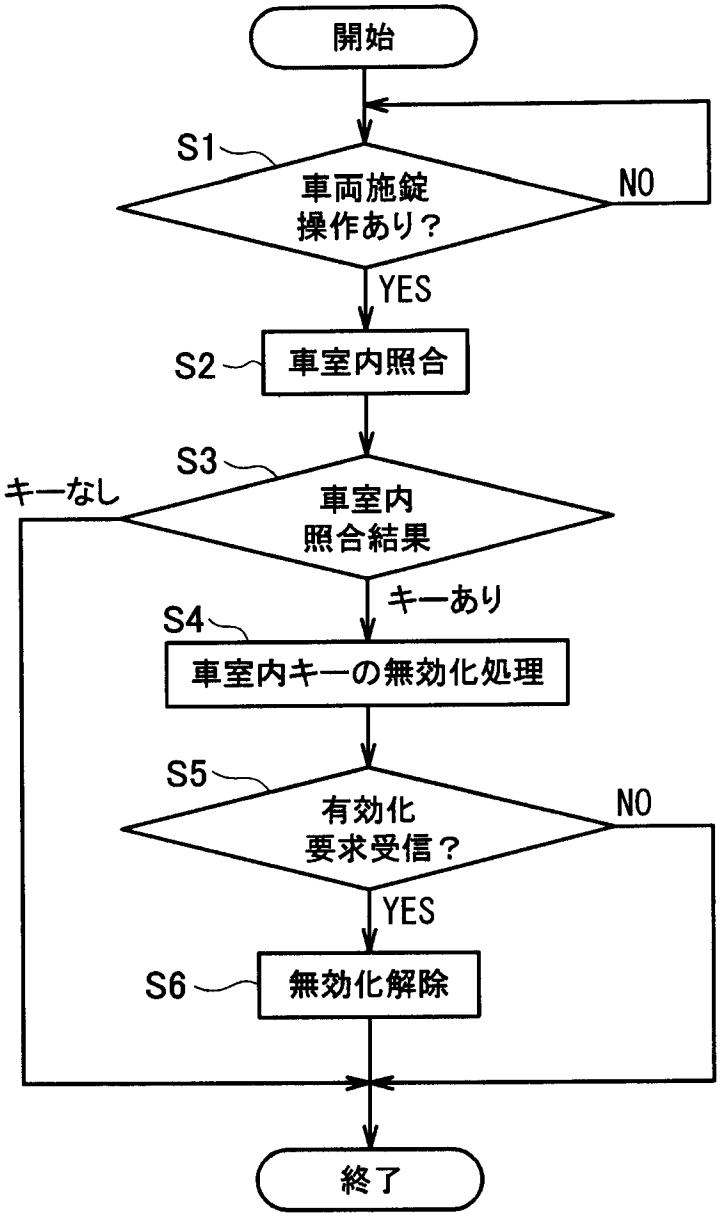
[図1]


1
2
3
スマートキー
（運転者）
4
スマートフォン
40
制御部
41
メモリ
BT通信部
表示部
入力部
42
43
44
3
スマートキー
（同乗者）
RF受信機
24
照合ECU
20
メモリ
21
車室内LFアンテナ
22
車外LFアンテナ
23
ドアロック装置
25
ロックスイッチ
26
アンロックスイッチ
27
エンジンスイッチ
28

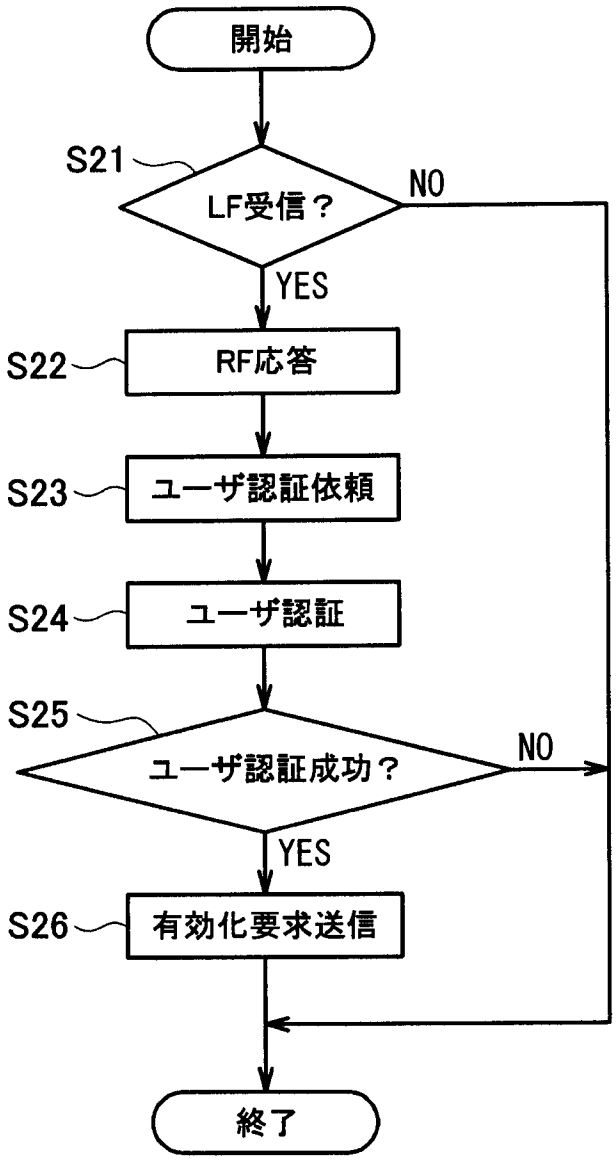
[図2]


3
キー
30
制御部
31
メモリ
LF受信部
32
RF送信部
33
BT通信部
34
ロックスイッチ
35
アンロックスイッチ
36

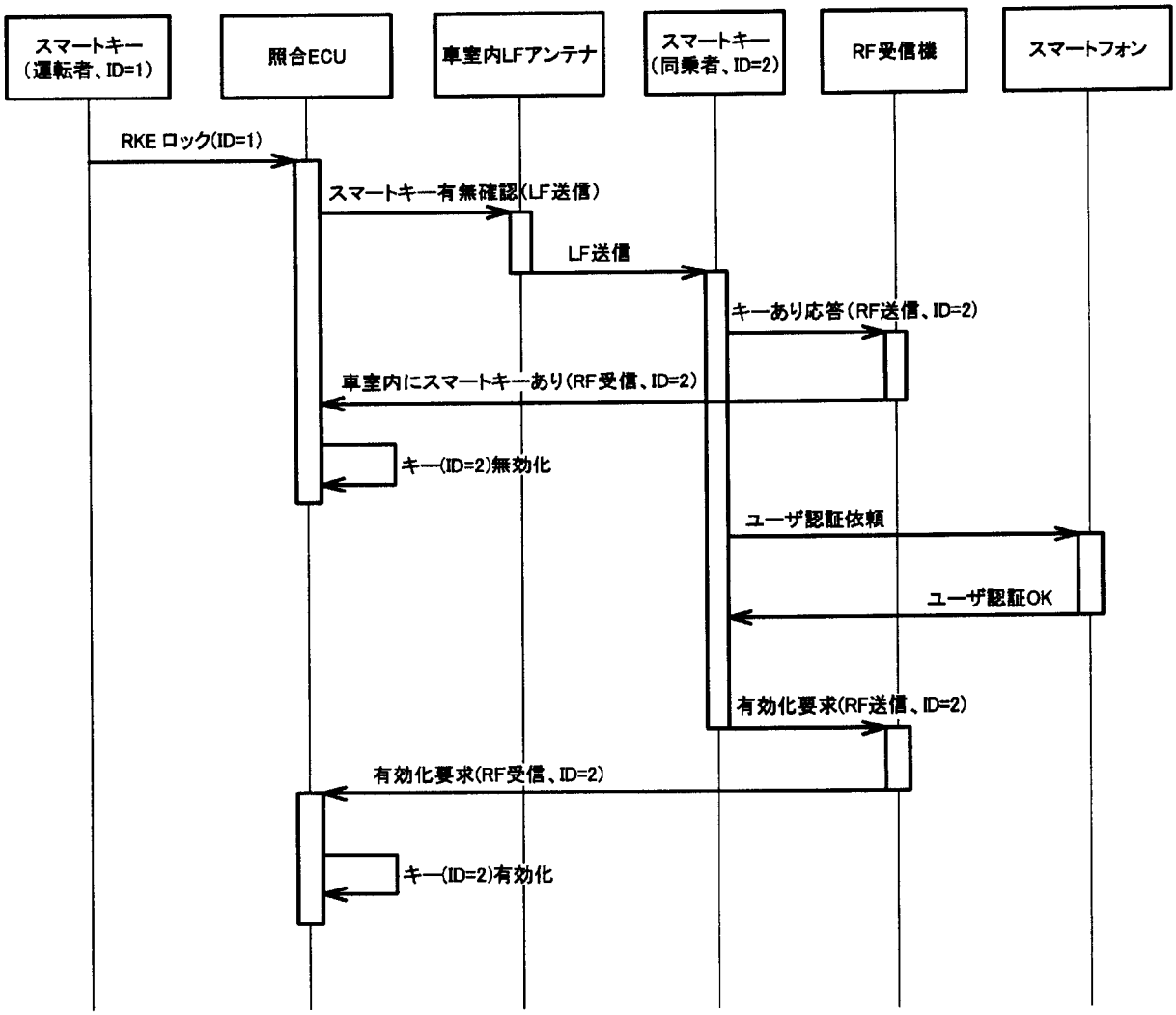
[図3]


開始
S1
車両施錠
操作あり？
NO
YES
S2
車室内照合
S3
キーなし
車室内
照合結果
キーあり
S4
車室内キーの無効化処理
S5
有効化
要求受信？
NO
YES
S6
無効化解除
終了

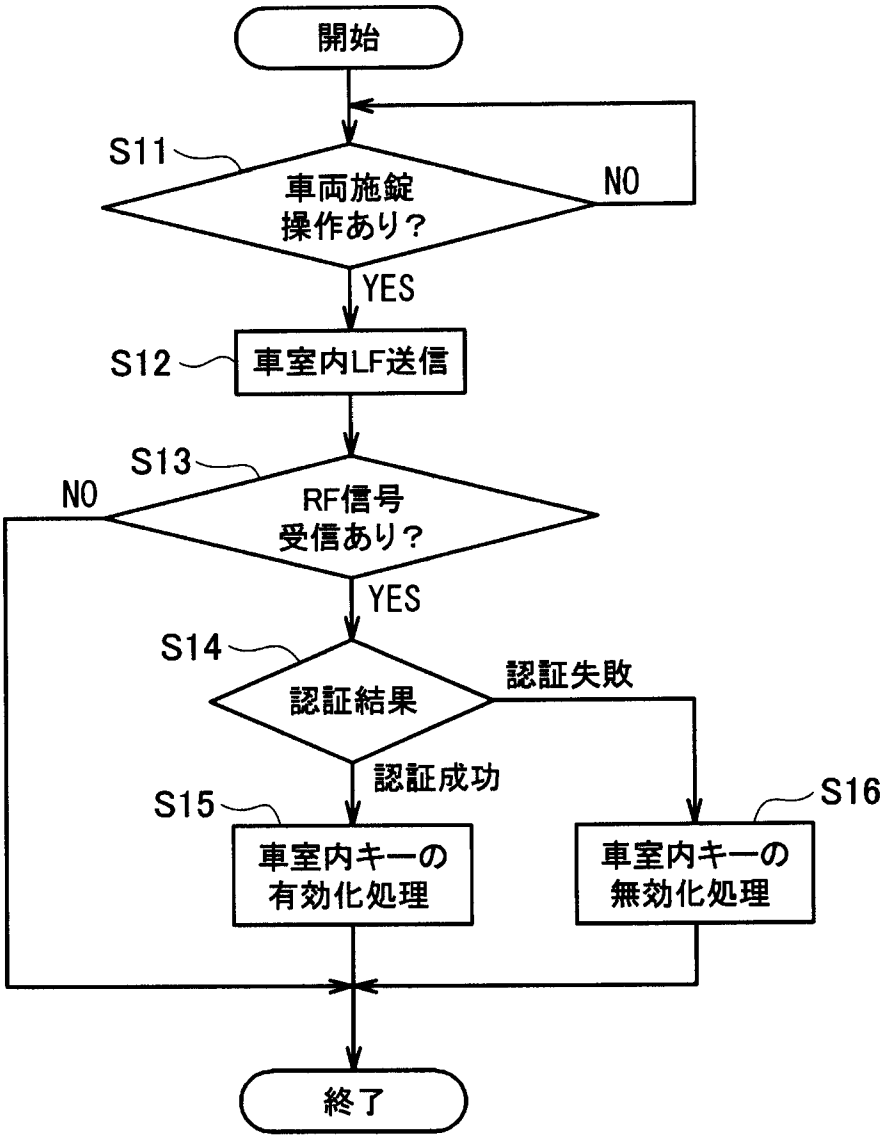
[図4]


開始
S21
LF受信？
NO
YES
S22
RF応答
S23
ユーザ認証依頼
S24
ユーザ認証
S25
ユーザ認証成功？
NO
YES
S26
有効化要求送信
終了

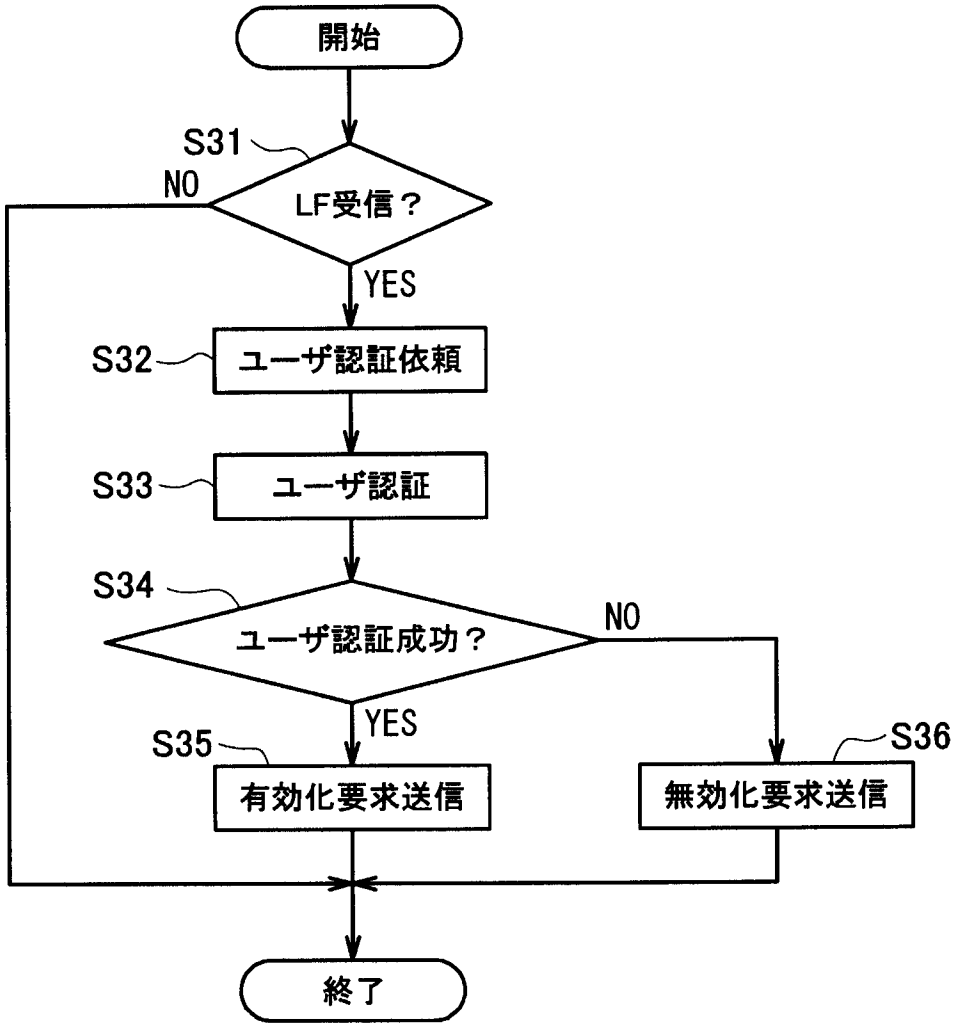
[図5]


スマートキー
(運転者、ID=1)
照合ECU
車室内LFアンテナ
スマートキー
(同乗者、ID=2)
RF受信機
スマートフォン
RKE ロック(ID=1)
スマートキー有無確認(LF送信)
LF送信
キーあり応答(RF送信、ID=2)
車室内にスマートキーあり(RF受信、ID=2)
キー(ID=2)無効化
ユーザ認証依頼
ユーザ認証OK
有効化要求(RF送信、ID=2)
有効化要求(RF受信、ID=2)
キー(ID=2)有効化

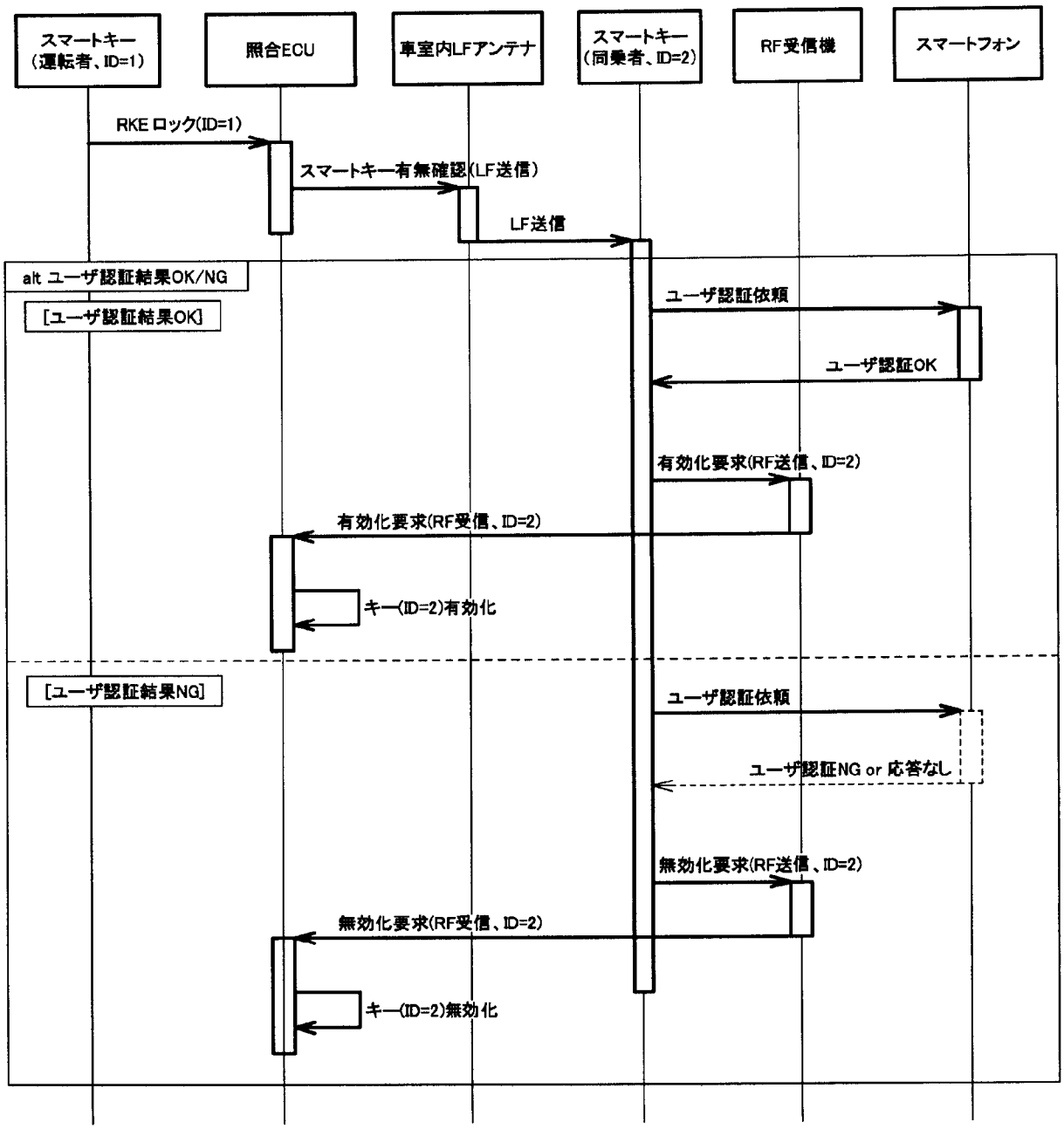
[図6]


開始
S11
車両施錠
操作あり？
NO
YES
S12
車室内LF送信
S13
NO
RF信号
受信あり？
YES
S14
認証結果
認証失敗
認証成功
S15
S16
車室内キーの
有効化処理
車室内キーの
無効化処理
終了

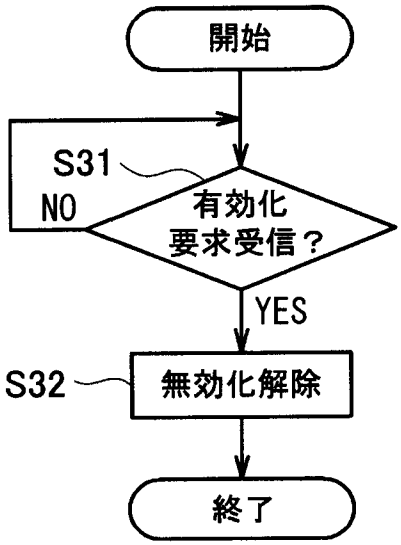
[図7]


開始
S31
NO
LF受信？
YES
S32
ユーザ認証依頼
S33
ユーザ認証
S34
ユーザ認証成功？
NO
YES
S35
有効化要求送信
S36
無効化要求送信
終了

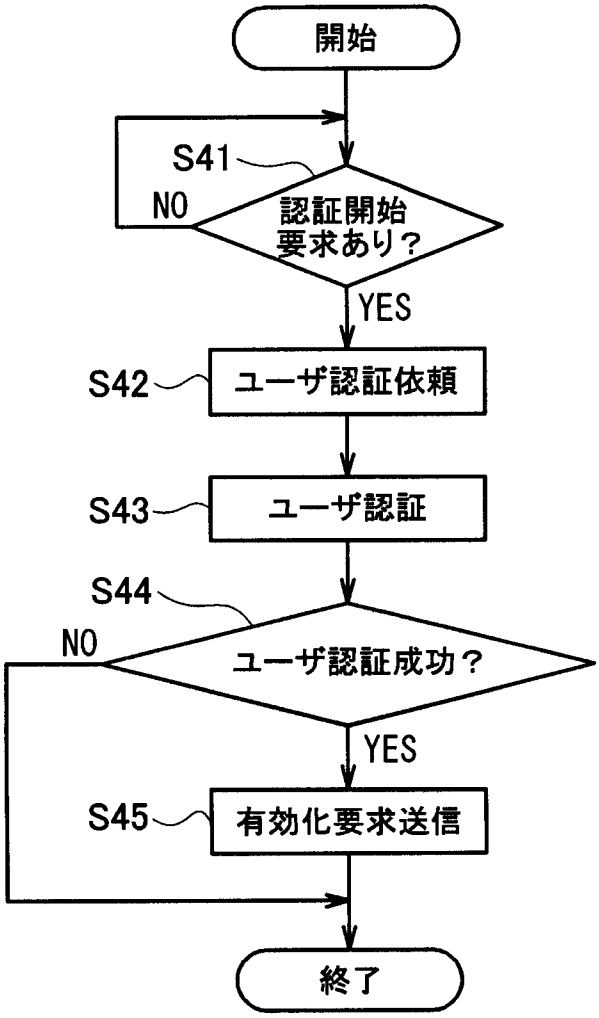
[図8]


スマートキー
(運転者、ID=1)
照合ECU
車室内LFアンテナ
スマートキー
(同乗者、ID=2)
RF受信機
スマートフォン
RKE ロック(ID=1)
スマートキー有無確認(LF送信)
LF送信
alt ユーザ認証結果OK/NG
[ユーザ認証結果OK]
ユーザ認証依頼
ユーザ認証OK
有効化要求(RF送信、ID=2)
有効化要求(RF受信、ID=2)
キー(ID=2)有効化
[ユーザ認証結果NG]
ユーザ認証依頼
ユーザ認証NG or 応答なし
無効化要求(RF送信、ID=2)
無効化要求(RF受信、ID=2)
キー(ID=2)無効化

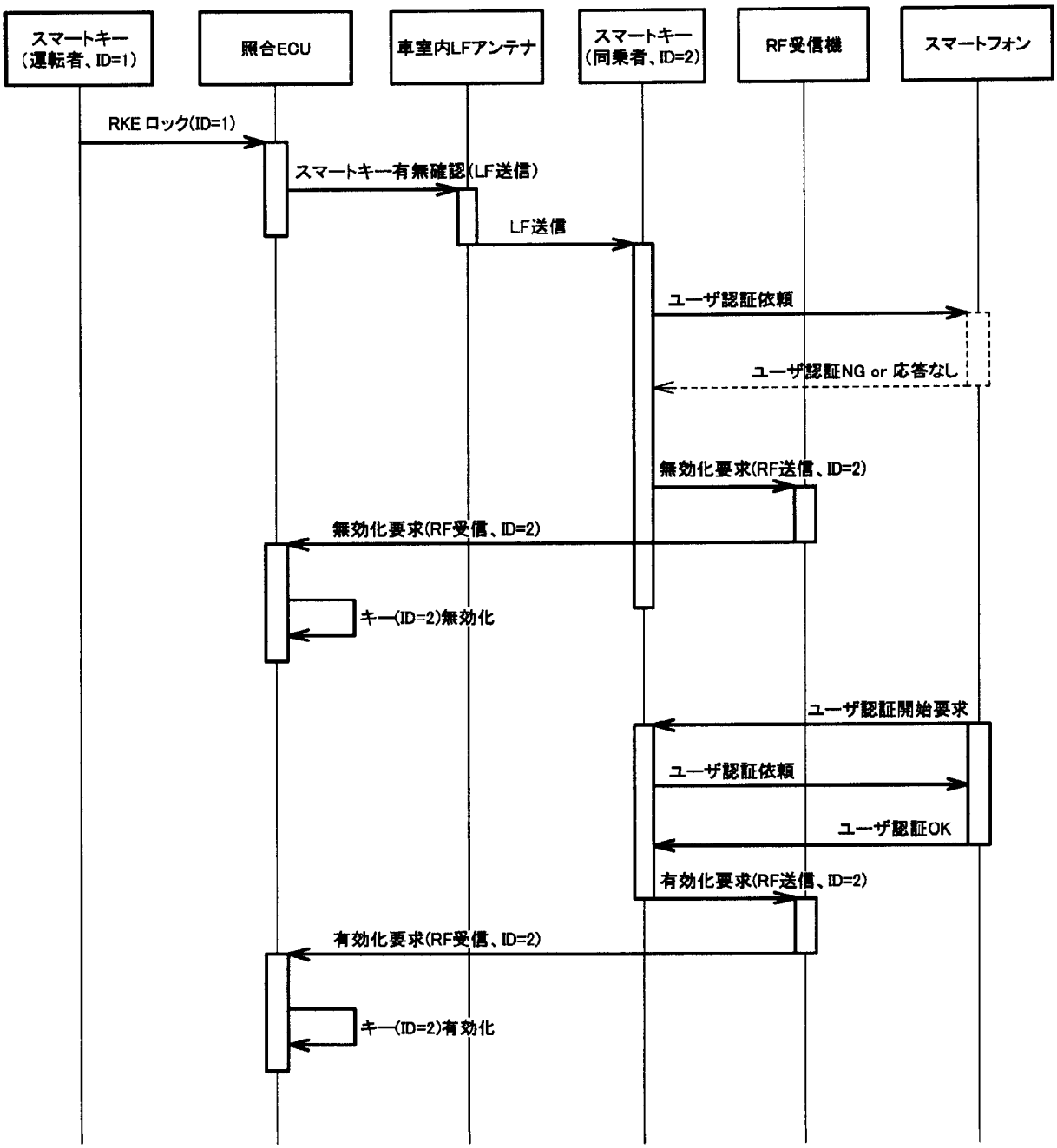
[図9]


開始
S31
NO
有効化
要求受信？
YES
S32
無効化解除
終了

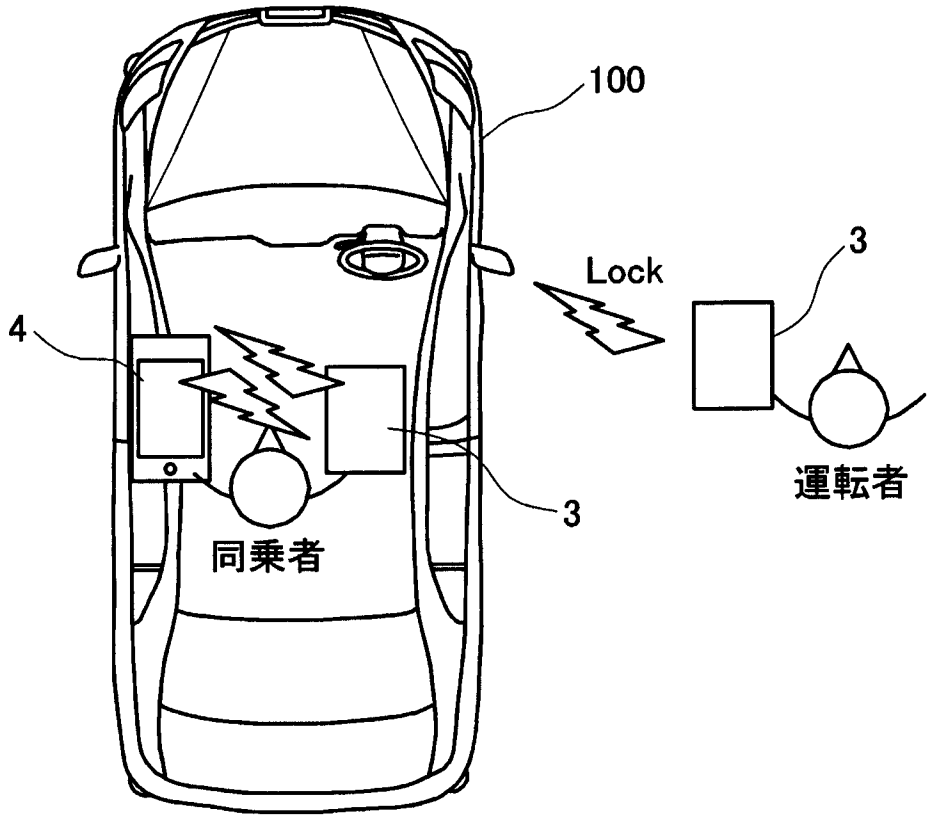
[図10]


開始
S41
NO
認証開始
要求あり？
YES
S42
ユーザ認証依頼
S43
ユーザ認証
S44
NO
ユーザ認証成功？
YES
S45
有効化要求送信
終了

[図11]


スマートキー
(運転者、ID=1)
照合ECU
車室内LFアンテナ
スマートキー
(同乗者、ID=2)
RF受信機
スマートフォン
RKE ロック(ID=1)
スマートキー有無確認(LF送信)
LF送信
ユーザ認証依頼
ユーザ認証NG or 応答なし
無効化要求(RF送信、ID=2)
無効化要求(RF受信、ID=2)
キー(ID=2)無効化
ユーザ認証開始要求
ユーザ認証依頼
ユーザ認証OK
有効化要求(RF送信、ID=2)
有効化要求(RF受信、ID=2)
キー(ID=2)有効化

[図12]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/084439

A. CLASSIFICATION OF SUBJECT MATTER
E05B49/00(2006.01)i, *B60R25/24*(2013.01)i, *H04M1/00*(2006.01)i, *H04Q9/00*(2006.01)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)
E05B49/00-49/04, B60R25/24, H04M1/00, H04Q9/00

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	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

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 4389838 B2 (Toyota Motor Corp.), 24 December 2009 (24.12.2009), entire text; all drawings & US 2006/0255911 A1 entire text; all drawings	1-3
A	JP 2014-152458 A (Calsonic Kansei Corp.), 25 August 2014 (25.08.2014), entire text; all drawings (Family: none)	1-3

☐ 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
31 January 2017 (31.01.17)	07 February 2017 (07.02.17)

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

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０８４４３９

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, B60R25/24(2013.01)i, H04M1/00(2006.01)i, H04Q9/00(2006.01)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.　E05B49/00-49/04, B60R25/24, H04M1/00, H04Q9/00

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

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１７年
日本国実用新案登録公報	１９９６－２０１７年
日本国登録実用新案公報	１９９４－２０１７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 4389838 B2（トヨタ自動車株式会社）2009.12.24, 全文，全図 & US 2006/0255911 A1, 全文，全図	1-3
A	JP 2014-152458 A（カルソニックカンセイ株式会社）2014.08.25, 全文，全図（ファミリーなし）	1-3

☐　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	国際調査報告の発送日
３１．０１．２０１７	０７．０２．２０１７

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
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）　２Ｒ　９３１９
家田　政明
電話番号　０３－３５８１－１１０１　内線　３２８５