(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-143325
(P2010-143325A)
(43)公開日　平成22年7月1日(2010.7.1)

(51)Int.Cl.		F I		テーマコード（参考）
B60R 25/04	(2006.01)	B60R 25/04	608	
B60R 25/10	(2006.01)	B60R 25/10	619	

審査請求 有　請求項の数 2　ＯＬ　（全 9 頁）

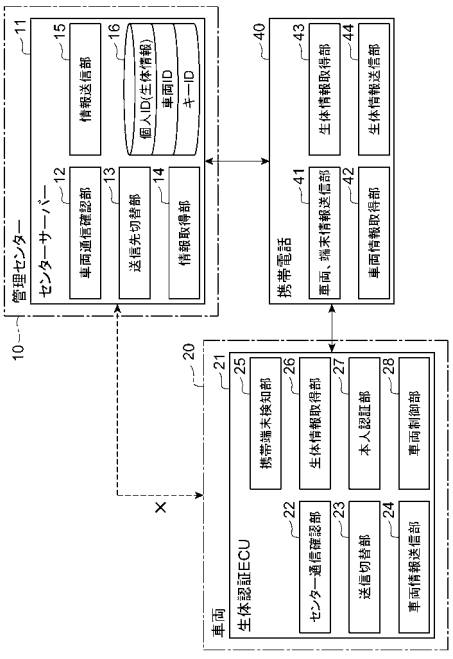
(21)出願番号　特願2008-321112 (P2008-321112)
(22)出願日　平成20年12月17日 (2008.12.17)

（特許庁注：以下のものは登録商標）
１．Ｂｌｕｅｔｏｏｔｈ

(71)出願人　000003207
トヨタ自動車株式会社
愛知県豊田市トヨタ町１番地
(74)代理人　100088155
弁理士　長谷川　芳樹
(74)代理人　100113435
弁理士　黒木　義樹
(74)代理人　100116920
弁理士　鈴木　光
(72)発明者　滝沢　良
愛知県豊田市トヨタ町１番地　トヨタ自動車株式会社内

(54)【発明の名称】車両用生体認証システム

(57)【要約】
【課題】管理センターとの通信圏外に停車した場合であっても、生体認証を行うことが可能な車両用生体認証システムを提供することを目的とする。
【解決手段】管理センター１０から出力された認証用データを受信する受信手段４３を備えた携帯端末４０と、管理センター１０との通信が不可能である場合に、携帯端末４０を介して認証用データを取得し、当該取得した認証用データを用いて本人認証を行う車載機２１と、を備える構成とする。車載機２１は、管理センター１０との通信圏外に車両２０が停車している場合に、携帯端末４０を介して、管理センター１０から出力された認証用データを取得する。これにより、車載機２１は、携帯端末４０を介して取得した認証用データを利用して、本人認証を行う。
【選択図】図２



【特許請求の範囲】
【請求項１】
データ管理を行う管理センターに予め登録された認証用データを用い、当該認証用データと認証対象者の生体情報とを比較して本人認証を行う車両用生体認証システムにおいて、
前記管理センターから出力された前記認証用データを受信する受信手段を備えた携帯端末と、
車両の停車時に前記携帯端末が移動した場合に、前記携帯端末を介して前記認証用データを取得し、当該取得した認証用データを用いて本人認証を行う車載機と、を有することを特徴とする車両用生体認証システム。
【請求項２】
前記車載機は、当該車載機と前記管理センターとの通信が不可能である場合に、前記携帯端末を介して前記認証データを取得し、当該取得した認証用データを用いて本人認証を行う請求項１記載の車両用生体認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車両用生体認証システムに関する。
【背景技術】
【０００２】
従来、このような分野の技術として、認証用生体データを予め管理センター（認証サーバ）に登録し、登録された認証用生体データと、ユーザー（認証対象者）から送信される生体情報とを照合して本人認証を行うことで、ドアロックの開錠を制御するものが知られている（例えば特許文献１）。
【特許文献１】特開２００５－３６５２３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、管理センターが認証用生体データを保持し、認証用生体データを車両（車載機）にダウンロードして生体認証を行う構成において、管理センターとの通信圏外に車両が停止している場合には、管理センターから車載機に認証用生体データをダウンロードすることができないため、生体認証を行うことができないという問題があった。
【０００４】
本発明は、このような課題を解決するために成されたものであり、管理センターとの通信圏外に停車した場合であっても、生体認証を行うことが可能な車両用生体認証システムを提供することを目的とする。
【課題を解決するための手段】
【０００５】
本発明による車両用生体認証システムは、データ管理を行う管理センターに予め登録された認証用データを用い、当該認証用データと認証対象者の生体情報とを比較して本人認証を行う車両用生体認証システムにおいて、管理センターから出力された認証用データを受信する受信手段を備えた携帯端末と、車両の停車時に前記携帯端末が移動した場合に、携帯端末を介して認証用データを取得し、当該取得した認証用データを用いて本人認証を行う前記車載機と、を有することを特徴としている。
【０００６】
このような車両用生体認証システムによれば、管理センターから出力された認証用データを受信する受信手段を備えた携帯端末と、車両の停車時に携帯端末が移動した場合に、携帯端末を介して認証用データを取得し、当該取得した認証用データを用いて本人認証を行う車載機と、を備える構成であるため、携帯端末を介して、管理センターから出力された認証用データを取得することができる。これにより、車載機は、携帯端末を介して取得

した認証用データを利用して、本人認証を行うことができる。すなわち、車載機と管理センターとの通信が不可能であるか否かに関わらず、携帯端末を介して取得した認証用データを利用して、本人認証を行うことができる。

【０００７】

また、車載機は、当該車載機と前記管理センターとの通信が不可能である場合に、携帯端末を介して認証データを取得し、当該取得した認証用データを用いて本人認証を行うことが好ましい。これにより、車両が管理センターと通信不可能なエリアに停車し、且つ、携帯端末が通信圏内に移動可能である場合（携帯端末が車外に移動した場合）に、携帯端末を介して取得した認証用データを利用して、本人認証を行うことができる。

【発明の効果】

【０００８】

本発明の車両用生体認証システムによれば、車外に移動可能な携帯端末を介して、認証用データを取得して、生体認証を行うことができる。これにより、車両が管理センターとの通信圏外に停車した場合でも、携帯端末を介して取得した認証用データを用いて、生体認証を行うことができる。

【発明を実施するための最良の形態】

【０００９】

以下、本発明による車両用生体認証システムの好適な実施形態について図面を参照しながら説明する。なお、図面の説明において同一または相当要素には同一の符号を付し、重複する説明は省略する。図１は、本発明の実施形態に係る車両用生体認証システムを示す概略図、図２は、本発明の実施形態に係る車両用生体認証システムを示すブロック構成図である。

【００１０】

図１に示す車両用生体認証システムは、例えば、車両２０のドアロックの施錠・開錠の制御、エンジン始動許可制御に適用される認証システムであり、ユーザーＡの生体情報を用いて本人認証を行うシステムである。この車両用生体認証システムでは、データ管理を行う管理センター１０から認証用データを取得し、当該認証用データとユーザーＡの生体情報とを照合することで、本人認証を行う。

【００１１】

なお、本人認証に用いられる生体情報としては、車室カメラや車外カメラによって取得した顔画像情報や虹彩情報、ドアノブによって取得した指紋情報や静脈情報、歩行信号検知装置によって取得した歩行パターン情報、エンジンスタートスイッチによって取得した指紋情報や静脈情報が挙げられる。その他の生体的特徴に関する情報を取得して、本人認証を行ってもよい。

【００１２】

本システムの管理センター１０には、認証用データを記憶するセンターサーバー１１が設けられている。センターサーバー１１は、演算処理を行うＣＰＵ、記憶部となるＲＯＭ及びＲＡＭ、入力信号回路、出力信号回路、電源回路などにより構成されている。また、センターサーバー１１は、通信ネットワークに接続され、車両２０の車載機（生体認証ＥＣＵ２１）及び携帯電話４０と通信可能な構成とされている。

【００１３】

センターサーバー１１は、認証用データ記憶部１６を備えている。認証用データ記憶部１６には、本人認証に用いられる認証用データを記憶するデータベース（ＤＢ）が構築され、車両を識別するための車両ＩＤ、車両のキー（電子キー）を識別するためのキーＩＤ、個人（ユーザーＡ）を識別するための個人ＩＤ、携帯端末を識別するための携帯端末ＩＤ、個人の生体情報に関するデータなどが、認証用データとして予め登録されている。

【００１４】

ここで、本実施形態の車両用生体認証システムでは、管理センター１０と車両２０との間の通信が不可能である場合に、移動可能な携帯電話４０に認証用データを転送可能な構成とされている。図２に示すように、管理センター１０のセンターサーバー１１には、車

両通信確認部１２、送信先切替部１３、情報取得部１４、情報送信部１５、認証用データ記憶部１６が構築されている。

【００１５】

車両通信確認部１２は、車両２０との通信が可能であるか否かを判定する判定手段として機能し、定期的に車両２０との通信状態を確認する。車両通信確認部１２は、例えば、センターサーバー１１から車両２０の生体認証ＥＣＵ２１へ応答要求信号を送信し、生体認証ＥＣＵ２１から応答信号が返信された場合に、通信可能である判定する。

【００１６】

送信先切替部１３は、管理センター１０と車両２０との通信状態に応じて、データの送信先を切り換える機能を有している。送信先切替部１３は、例えば、管理センター１０と車両２０との通信が不可能である場合に、データの送信先を車両２０から携帯電話４０へ切り換えることができる。

【００１７】

情報取得部１４は、携帯電話４０や車両２０と通信して、車両２０から出力された車両ＩＤ、携帯電話４０から出力された携帯端末ＩＤ（キーＩＤ）を取得するものである。

【００１８】

情報送信部１５は、車両ＩＤや携帯端末ＩＤに紐付いた（関連付けられた）生体情報（認証用データ）を、携帯電話４０（又は、車両２０）に送信するものである。

【００１９】

携帯電話４０は、認証対象者であるユーザーＡの携帯電話である。携帯電話４０は、通話機能、メール送受信機能、ネットワーク接続機能、撮像機能などを有する。また、携帯電話４０は、演算処理を行うＣＰＵ、記憶部となるＲＯＭ及びＲＡＭ、入力信号回路、出力信号回路、電源回路などを備える構成とされている。携帯電話４０には、車両、端末情報送信部４１、車両情報取得部４２、生体情報取得部４３、生体情報送信部４４が構築されている。

【００２０】

また、携帯電話４０は、センターサーバー１１と通信可能である共に、車両２０と通信可能な構成とされている。携帯電話４０と車両２０との間の通信方式としては、ブルートゥース（Bluetooth）、赤外線などのアドホック（ad hoc）通信、人体通信、メール添付などが挙げられる。

【００２１】

車両情報取得部４２は、車両２０から出力された車両ＩＤを受信する機能を有する。車両、端末情報送信部４１は、受信した車両ＩＤを管理センター１０に送信すると共に、携帯電話４０を識別するための携帯端末ＩＤ（キーＩＤ）を管理センター１０に送信する機能を有している。

【００２２】

生体情報取得部４３は、管理センター１０から出力された認証用データ（予め登録された生体情報）を受信する本発明の受信手段として機能するものである。また、携帯電話の記憶部は、生体情報取得部４３によって取得した認証用データを記憶する記憶手段として機能する。生体情報送信部４４は、管理センター１０から受信した認証用データを車両２０へ送信する機能を有する。

【００２３】

本実施形態の車両用生体認証システムが適用される車両２０の車載機は、生体認証に関する制御を司る電子制御ユニット（以下、「生体認証ＥＣＵ」という。）２１を備えている。

【００２４】

生体認証ＥＣＵ２１は、演算処理を行うＣＰＵ、記憶部となるＲＯＭ及びＲＡＭ、入力信号回路、出力信号回路、電源回路などにより構成されている。生体認証ＥＣＵ２１では、記憶部に記憶されたプログラムを実行することで、センター通信確認部２２、送信切替部２３、車両情報送信部２４、携帯端末検知部２５、生体情報取得部２６、本人認証部２

７、車両制御部２８が構築される。また、生体認証ＥＣＵ２１は、センターサーバー１１と通信可能であると共に、携帯電話４０と通信可能な構成とされている。

【００２５】

センター通信確認部２２は、エンジンＯＦＦ時に管理センター１０との通信状態を確認するものである。センター通信確認部２２は、例えばエンジンＥＣＵから、エンジン停止を報知する信号を受信すると、センターサーバー１１との通信が可能であるか否かの判定を行う。

【００２６】

送信切替部２３は、管理センター１０と車両２０との通信状態に応じて、データの送信先を切り換える機能を有している。送信先切替部２３は、例えば、管理センター１０と車両２０との通信が不可能である場合に、データの送信先を管理センター１０から携帯電話４０へ切り換えることができる。車両情報送信部２４は、車両４０を識別するための車両ＩＤを携帯電話４０に送信するものである。

【００２７】

携帯端末検知部２５は、車両２０のユーザーＡ（認証対象者）が携帯している携帯電話４０を検出するものである。また、携帯端末検知部２５は、車両２０のキー（キーＩＤ）を検出するキー検知部として機能する。

【００２８】

生体情報取得部２６は、管理センター１０から出力された認証用データを取得するものである。生体情報取得部２６は、携帯電話４０を介して、管理センター１０から出力された認証用データを受信する受信手段として機能する。

【００２９】

本人認証部２７は、管理センター１０から出力された認証用データと、ユーザーＡの生体情報とを比較して、本人認証を行う生体認証手段として機能する。生体認証ＥＣＵ２１は、ユーザーＡの生体情報を検出可能な生体情報検出手段と電気的に接続され、生体情報検出手段によって、検出されたユーザーＡの生体情報を取得可能な構成とされている。

【００３０】

生体情報検出手段としては、ドアノブに設けられた指紋／静脈検出センサー、エンジンスタートスイッチに設けられた指紋／静脈検出センサー、車両側部に設けられ、ユーザーＡの歩行パターンを検出する歩行信号検出センサー、ユーザーＡの顔画像、虹彩情報を検出する車載カメラなどが挙げられる。

【００３１】

本人認証部２７は、ユーザーＡの乗車動作（ドア開閉、乗車、エンジンＳＷＯＮなど）に合わせて生体認証を実施する。本人認証部２７は、生体情報検出手段によって、検出された生体情報と、認証用データとを比較して生体認証を実施する。

【００３２】

車両制御部２８は、本人認証部２７による認証結果に応じて、ドアロック制御、エンジン始動許可制御などを実行する。車両制御部２８は、ユーザーＡが車両２０を運転可能なユーザーであると認証された場合に、ドアロックの開錠、エンジン始動許可を行う。車両制御部２８は、例えば、ドアロック制御装置、エンジンＥＣＵに指令信号を送信して、ドアロックの開錠、エンジン始動許可を指示する。

【００３３】

また、生体認証ＥＣＵ２１の記憶部には、携帯端末ＩＤに関連付けられたユーザーＡのドライバーポジション（シート位置）などに関する情報が記憶されている。また、車両制御部２８では、ドライバーポジションに関する情報に基づいて、シート位置の調整を指示する指令信号を送信する。

【００３４】

次に、本実施形態に係る車両用生体認証システムの動作について説明する。図３は、本発明の実施形態に係る車両用生体認証システムで実行される動作手順を示すフローチャートである。なお、ステップをＳと略記する。

【００３５】
まず、車両２０と管理センター１０との通信状態を確認する（Ｓ１）。センターサーバー１１の車両通信確認部１２は、定期的に、車両２０との通信が途絶しているか否かを判定する。生体認証ＥＣＵ２１のセンター通信確認部２２は、管理センター１０との通信が途絶しているか否かを判定する。車両２０と管理センター１０との通信が途絶している場合には、ステップ２に進み、車両２０との通信が途絶していない場合には、ステップ５に進む。例えば、車両２０が管理センター１０との通信圏外に停車している場合には、ステップ２に進む。
【００３６】
ステップ２では、車両２０から携帯電話４０へ車両ＩＤを送信する。具体的には、生体認証ＥＣＵ２１の送信切替部２３は、データの送信先を携帯電話４０に変更し、車両情報送信部２４は、車両ＩＤを携帯電話４０へ送信する。
【００３７】
続く、ステップ３では、車両ＩＤ、携帯端末ＩＤを携帯電話４０から管理センター１０へ送信する。携帯電話４０は、車両情報取得部４２によって、車両２０から出力された車両ＩＤを受信する。車両、端末情報送信部４１は、携帯端末ＩＤ、及び受信した車両ＩＤを管理センター１０へ送信する。センターサーバー１１の情報取得部１４は、携帯電話４０から出力さえた携帯端末ＩＤ及び車両ＩＤを取得する。
【００３８】
次に、センターサーバー１１の送信先切替部１３は、認証用データの送信先を携帯電話４０に変更し、情報送信部１５は、車両ＩＤ、携帯端末ＩＤに関連付けられた認証用データ（生体情報）を携帯電話４０に送信する。携帯電話４０の生体情報取得部４３は、センターサーバー１１から出力された認証用データを受信する（Ｓ４）。受信した認証用データは、携帯電話４０の記憶部に記憶される。
【００３９】
続くステップ５では、キー信号を検知したか否かを判定する。具体的には、生体認証ＥＣＵ２１の携帯端末検知部２５は、ドライバーとなるユーザーＡの携帯電話４０を検知したか否かを判定する。携帯電話４０の携帯端末ＩＤ（電子キーとして鍵情報）を検出した場合には、キー信号を検知したと判定し、ステップ６に進む。キー信号を検知したと判定しなかった場合には、キー信号の検知を待って、ステップ６に進む。
【００４０】
ステップ６では、検知したキー信号に登録されているドライバー（ユーザーＡ）の認証用データを管理センター１０又は携帯電話４０からダウンロードする。すなわち、生体認証ＥＣＵ２１の生体情報取得部２６は、管理センター１０と車両２０との通信が可能である場合には、センターサーバー１１の情報送信部１５から出力された認証用データを、携帯電話４０を介さずに取得し、管理センター１０と車両２０との通信が不可能である場合には、携帯電話４０を介して、認証用データを取得する。
【００４１】
次に、ステップ７では、車載機の生体認証ＥＣＵ２１では、本人認証部２７によって、生体認証を実施する。続く、ステップ８では、生体認証ＥＣＵ２１の車両制御部２８は、認証結果に応じて、指令信号を送信し、ドアロックの開錠、ドライバーポジションの再生、エンジン始動許可を行う。
【００４２】
続く、ステップ９では、生体認証ＥＣＵ２１は、ダウンロードした認証用データ、生体情報を消去する。
【００４３】
このような車両用生体認証システムでは、管理センター１０から出力された認証用データを受信する生体情報取得部４３を備えた携帯電話４０と、管理センター１０との通信が不可能である場合に、携帯電話４０を介して認証用データを取得し、当該取得した認証用データを用いて本人認証を行う車載機（生体認証ＥＣＵ２１）と、を備える構成であるた

め、管理センター１０との通信圏外に車両２０が停車している場合であっても、携帯電話４０を介して、管理センター１０から出力された認証用データを取得することができる。これにより、車載機の生体認証ＥＣＵ２１では、携帯電話４０を介して取得した認証用データを利用して、本人認証を行うことができる。

【００４４】

次に、図４を参照して、本発明の他の実施形態に係る車両用生体認証システムの動作手順について説明する。なお、他の実施形態に係る装置構成は、図２に示すものと同様である。

【００４５】

他の実施形態に係る車両用生体認証システムでは、車両２０のドライバーが降車する際に、管理センター１０と車両２０との通信状態を確認し、通信途絶が確認された場合に、生体情報、及び暗号鍵（暗号を含む鍵情報）を、携帯電話４０に送信しておく。

【００４６】

管理センター１０との通信圏内において、携帯電話４０から管理センター１０に各種情報を送信する。送信される各種情報は、ドライバーの生体情報、車両２０の車両ＩＤ、携帯電話の携帯端末ＩＤ、キーＩＤなどである。管理センター１０は、携帯電話４０から出力された各種情報を受信して、予め登録された認証用データと照合して本人認証を行う。

【００４７】

管理センター１０では、認証結果に関する情報を暗号化する。携帯電話４０では暗号化された認証結果をダウンロードする。次回乗車時において、暗号化された認証結果が、携帯電話４０から車両２０へ送信される。車両２０の生体認証ＥＣＵ２１において、暗号解除することで本人認証を行う。

【００４８】

以下、図４のフローチャートに沿って、説明する。まず、生体認証ＥＣＵ２１の生体情報取得部２６によって、ドライバーの生体情報を取得する（Ｓ２１）。次に、車両２０において、暗号鍵（「秘密鍵」と「公開鍵」）を作成する（Ｓ２２）。車両２０の生体認証ＥＣＵ２１は、暗号鍵（情報）として、秘密鍵情報及び公開鍵情報を作成する。

【００４９】

次に、車両２０から携帯電話４０へ車両ＩＤ、生体情報、公開鍵情報を送信する（Ｓ２３）。ここでは、生体認証ＥＣＵ２１の車両情報送信部２４は、車両ＩＤ、生体情報、公開鍵情報を、携帯電話４０に送信する。

【００５０】

続いて、携帯電話４０の情報を取得して、管理センター１０によって生体認証を実施する（Ｓ２４）。具体的には、携帯電話４０の車両情報取得部４２は、生体認証ＥＣＵ２１から出力された車両ＩＤ、生体情報、公開鍵情報を受信する。車両、端末情報送信部４１は、携帯端末ＩＤ、車両ＩＤ、生体情報、公開鍵情報を管理センター１０に送信する。管理センター１０は、携帯端末ＩＤ、車両ＩＤ、生体情報、公開鍵情報を受信し、受信した情報と、認証用データ記憶部１６に予め記憶されている認証用データと比較することで、本人認証を行う。

【００５１】

次に、センターサーバー１１は、認証結果を暗号化処理し、暗号化された認証結果に関する情報を携帯電話４０に送信する（Ｓ２５）。携帯電話４０では、受信した認証結果に関する情報を記憶部に記憶する。

【００５２】

続いて説明するステップ２６からステップ２９において実行される処理は、次回乗車時に、車載機によって実行される認証処理に関するものである。まず、ステップ２６では、キー信号を検知したか否かを判定する。具体的には、生体認証ＥＣＵ２１の携帯端末検知部２５は、ドライバーとなるユーザーＡの携帯電話４０を検知したか否かを判定する。携帯電話４０の携帯端末ＩＤ（電子キーとして鍵情報）を検出した場合には、キー信号を検知したと判定し、ステップ２７に進む。キー信号を検知したと判定しなかった場合には、

キー信号の検知を待って、ステップ２７に進む。

【００５３】

ステップ２７では、検知したキー信号に登録されているドライバー（ユーザーＡ）の認証用データを携帯電話４０からダウンロードする。すなわち、生体認証ＥＣＵ２１の生体情報取得部２６は、携帯電話４０を介して、認証用データを取得する。

【００５４】

ステップ２８では、車両２０側で秘密鍵により暗号解除を行う。具体的には、生体認証ＥＣＵ２１は、暗号化された認証結果に関する情報について、秘密鍵情報を用いて暗号解除を行うことで、本人認証を行う。

【００５５】

続く、ステップ２９では、解読された認証結果に応じて、ドアロックの解除、ドライバーポジションの再生、エンジン始動許可などの制御処理を実行する。

【００５６】

このような他の実施形態に係る車両用生体認証システムにあっても、携帯電話４０を介して、暗号化された認証結果に関するデータ（認証用データ）を取得することができるため、車両２０が管理センター１０との通信圏外に停車している場合であっても、生体認証を行うことができる。

【００５７】

以上、本発明をその実施形態に基づき具体的に説明したが、本発明は、上記実施形態に限定されるものではない。なお、上記実施形態では、携帯端末を携帯電話４０として説明しているが、その他の通信可能な端末、車外への移動可能な外部端末でもよい。また、携帯端末として、通信機能を有する鍵などであってもよい。

【００５８】

なお、上記実施形態では、センターサーバー１１の車両通信確認部１２は、定期的に、車両２０との通信が途絶えているか否かを判定しているが、センターサーバー１１と車両２０との間の通信の可否に関わらず、携帯端末に認証用データを送信する構成としてもよい。この構成の場合には、センターサーバー１１が定期的に車両２０との通信状態を確認する必要がないため、システムの簡略化を図ることができる。

【図面の簡単な説明】

【００５９】

【図１】本発明の実施形態に係る車両用生体認証システムを示す概略図である。

【図２】本発明の実施形態に係る車両用生体認証システムを示すブロック構成図である。

【図３】本発明の実施形態に係る車両用生体認証システムの動作手順を示すフローチャートである。

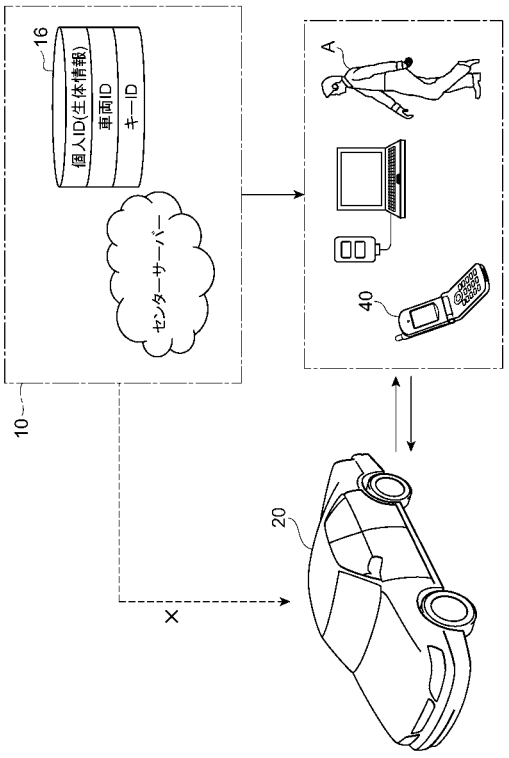
【図４】本発明の他の実施形態に係る車両用生体認証システムの動作手順を示すフローチャートである。

【符号の説明】

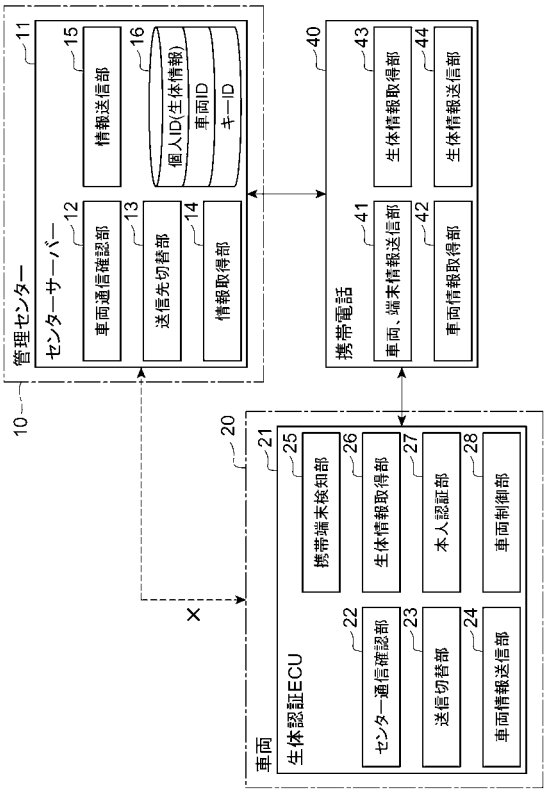
【００６０】

１０…管理センター、１１…センターサーバー、１２…車両通信確認部、１３…送信先切替部、１４…情報取得部、１５…情報送信部、１６…認証用データ記憶部、２０…車両、２１…生体認証ＥＣＵ、２２…センター通信確認部、２３…送信切替部、２４…車両情報送信部、２５…携帯端末検知部、２６…生体情報取得部、２７…本人認証部、２８…車両制御部、４０…携帯電話（携帯端末）、４１…車両・端末情報送信部、４２…車両情報取得部、４３…生体情報取得部、４４…生体情報送信部、Ａ…ユーザー（認証対象者）。

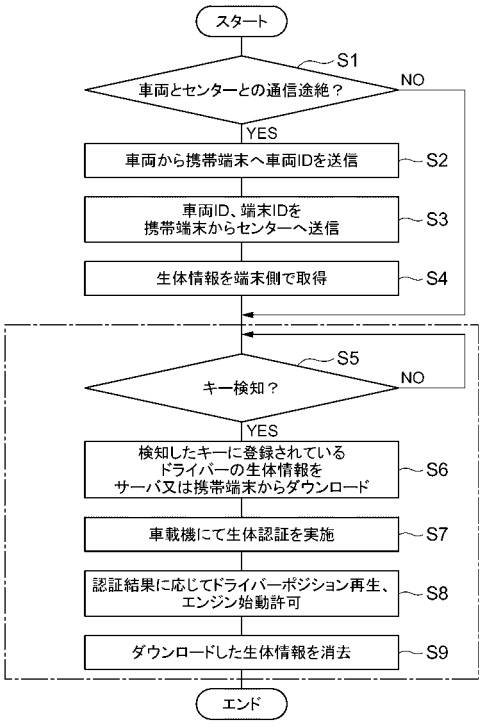
【図１】


16
個人ID(生体情報)
車両ID
キーID
センターサーバー
10
A
40
20
×

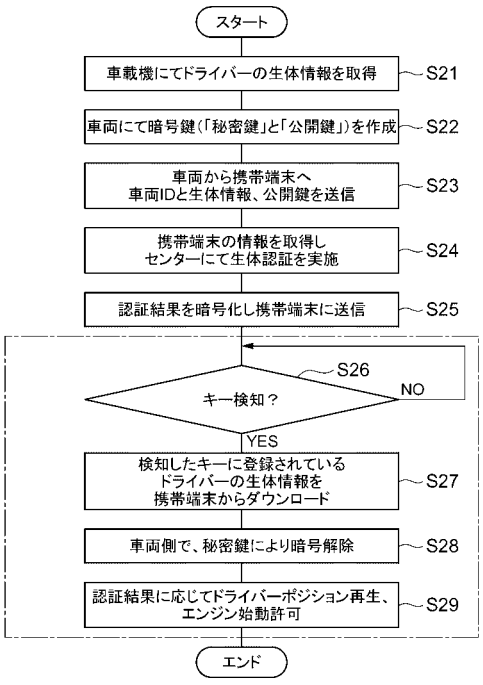
【図２】


管理センター
センターサーバー
11
15
情報送信部
16
個人ID(生体情報)
車両ID
キーID
12
車両通信確認部
13
送信先切替部
14
情報取得部
10
40
携帯電話
43
生体情報取得部
44
生体情報送信部
41
車両、端末情報送信部
42
車両情報取得部
20
車両
生体認証ECU
21
25
携帯端末検知部
26
生体情報取得部
27
本人認証部
28
車両制御部
22
センター通信確認部
23
送信切替部
24
車両情報送信部
×

【図３】


スタート
S1
車両とセンターとの通信途絶？
NO
YES
車両から携帯端末へ車両IDを送信
S2
車両ID、端末IDを
携帯端末からセンターへ送信
S3
生体情報を端末側で取得
S4
S5
キー検知？
NO
YES
検知したキーに登録されている
ドライバーの生体情報を
サーバ又は携帯端末からダウンロード
S6
車載機にて生体認証を実施
S7
認証結果に応じてドライバーポジション再生、
エンジン始動許可
S8
ダウンロードした生体情報を消去
S9
エンド

【図４】


スタート
車載機にてドライバーの生体情報を取得
S21
車両にて暗号鍵(「秘密鍵」と「公開鍵」)を作成
S22
車両から携帯端末へ
車両IDと生体情報、公開鍵を送信
S23
携帯端末の情報を取得し
センターにて生体認証を実施
S24
認証結果を暗号化し携帯端末に送信
S25
S26
キー検知？
NO
YES
検知したキーに登録されている
ドライバーの生体情報を
携帯端末からダウンロード
S27
車両側で、秘密鍵により暗号解除
S28
認証結果に応じてドライバーポジション再生、
エンジン始動許可
S29
エンド