

(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2020-4044

(P2020-4044A)

(43) 公開日 令和2年1月9日(2020.1.9)

(51) Int.Cl.	F I	テーマコード (参考)
G 0 6 F 21/32 (2013.01)	G O 6 F 21/32	2 E 2 5 O
E O 5 B 49/00 (2006.01)	E O 5 B 49/00	R
B 6 O R 25/25 (2013.01)	B 6 O R 25/25	
G O 6 F 21/60 (2013.01)	G O 6 F 21/60	3 2 O

審査請求 未請求 請求項の数 5 O L (全 9 頁)

(21) 出願番号	特願2018-122229 (P2018-122229)	(71) 出願人	000003551
(22) 出願日	平成30年6月27日 (2018. 6. 27)		株式会社東海理化電機製作所
		(74) 代理人	100105957
			弁理士 恩田 誠
		(74) 代理人	100068755
			弁理士 恩田 博宣
		(72) 発明者	野畑 直樹
			愛知県丹羽郡大口町豊田三丁目2 6 O 番地
			株式会社東海理化電機製作所内
		F ターム (参考)	2E250 AA21 BB05 BB08 BB29 BB46
			CC16 DD06 DD09 EE10 FF08
			FF23 FF27 FF36 HH01 JJ03
			JJ05

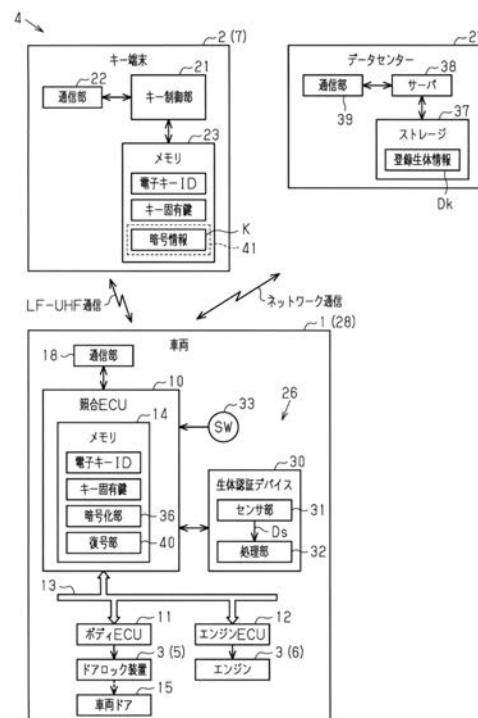
(54) 【発明の名称】 認証システム及び認証方法

(57) 【要約】

【課題】登録生体情報の取り扱いのセキュリティ性向上を可能にした認証システム及び認証方法を提供する。

【解決手段】データセンター27のストレージ37には、車両1において実施される生体認証の解となる登録生体情報Dkが保管される。この登録生体情報Dkは、暗号化されている。生体認証デバイス30で生体認証を行う場合、データセンター27から登録生体情報Dkを取得する。このとき、復号部40は、キー端末2から暗号情報Kを取得し、この暗号情報Kにより登録生体情報Dkを復号する。生体認証デバイス30は、センサ部31で取得した生体情報Dsと、復号された登録生体情報Dkとを用い、生体認証を実行する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

ユーザから生体情報を取得し、当該生体情報を用いた認証が成立する場合に作動対象物の作動が許可又は実行される認証システムであって、

前記認証を行う場合に、認証の解として暗号化された登録生体情報を、キー端末に格納されている暗号情報により復号して、前記認証を実施可能にする復号部を備えた認証システム。

【請求項 2】

認証の解となる前記登録生体情報の登録にあたり、前記キー端末に格納された暗号情報を基に前記登録生体情報を暗号化し、その暗号化登録生体情報をストレージに保存しておく暗号化部を備える

請求項 1 に記載の認証システム。

【請求項 3】

前記キー端末は、前記作動対象物と無線による ID 照合が可能なキーであり、

前記作動対象物は、前記キー端末との間の ID 照合が成立するとともに、前記生体情報を用いた認証が成立した場合に、作動が許可又は実行される

請求項 1 又は 2 に記載の認証システム。

【請求項 4】

前記登録生体情報を復号する前記暗号情報は、その格納先として設けられたメモリにおいてセキュアな領域に格納されている

請求項 1 ～ 3 のうちいずれか一項に記載の認証システム。

【請求項 5】

ユーザから生体情報を取得し、当該生体情報を用いた認証が成立する場合に作動対象物の作動が許可又は実行される認証方法であって、

前記認証を行う場合に、認証の解として暗号化された登録生体情報を、キー端末に格納されている復号情報により復号して、前記認証を実施可能にする認証方法。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、生体情報を用いた認証を行う認証システム及び認証方法に関する。

【背景技術】**【0002】**

従来、ユーザから生体情報を取得し、この生体情報の正否を確認することによりユーザ認証を行う認証システムが周知である（特許文献 1 等参照）。認証に用いる生体情報は、例えば指紋、静脈、網膜等がある。この種の認証システムは、車両のみならず、種々のサービスへの使用が検討されている。

【先行技術文献】**【特許文献】****【0003】**

【特許文献 1】 特開 2000-352245 号公報

【発明の概要】**【発明が解決しようとする課題】****【0004】**

ところで、生体認証は、ユーザから取得した生体情報と、事前に登録しておいた生体認証（登録生体認証）とを比較する認証態様となっている。このため、事前登録した生体認証情報が更新されないまま長期間使用された状態をとっていると、第三者による生体情報の盗難に晒される可能性が高くなり、セキュリティ性の面で問題があった。

【0005】

本発明の目的は、登録生体情報の取り扱いのセキュリティ性向上を可能にした認証システム及び認証方法を提供することにある。

10

20

30

40

50

【課題を解決するための手段】

【0006】

前記問題点を解決する認証システムは、ユーザから生体情報を取得し、当該生体情報を用いた認証が成立する場合に作動対象物の作動が許可又は実行される構成であって、前記認証を行う場合に、認証の解として暗号化された登録生体情報を、キー端末に格納されている暗号情報により復号して、前記認証を実施可能にする復号部を備えた。

【0007】

本構成によれば、生体認証の解として用いられる登録生体情報が暗号化されて保管される。このため、仮に登録生体情報が盗難に遭っても、登録生体情報を復号するのに必要な暗号情報を知らなければ、登録生体情報を使用することができない。よって、登録生体情報の取り扱いのセキュリティ性を向上することが可能となる。

10

【0008】

前記認証システムにおいて、認証の解となる前記登録生体情報の登録にあたり、前記キー端末に格納された暗号情報を基に前記登録生体情報を暗号化し、その暗号化登録生体情報をストレージに保存しておく暗号化部を備えることが好ましい。この構成によれば、ユーザが所持を管理するキー端末を利用して登録生体情報を暗号化するので、復元に遭い難い登録生体情報とすることが可能となる。

【0009】

前記認証システムにおいて、前記キー端末は、前記作動対象物と無線によるID照合が可能なキーであり、前記作動対象物は、前記キー端末との間のID照合が成立するとともに、前記生体情報を用いた認証が成立した場合に、作動が許可又は実行されることが好ましい。この構成によれば、ID照合及び生体認証の両方が成立しないと作動対象物の作動が許可又は実行されないので、作動対象物の不正使用に対するセキュリティ性を確保することが可能となる。

20

【0010】

前記認証システムにおいて、前記登録生体情報を復号する前記暗号情報は、その格納先として設けられたメモリにおいてセキュアな領域に格納されていることが好ましい。この構成によれば、暗号情報をメモリから不正に読み出すことができなくなるので、登録生体情報の復号に必要となる暗号情報が盗難され難くなる。よって、登録生体情報の不正取得に対するセキュリティ性を確保するのに有利となる。

30

【0011】

前記問題点を解決する認証方法は、ユーザから生体情報を取得し、当該生体情報を用いた認証が成立する場合に作動対象物の作動が許可又は実行される方法であって、前記認証を行う場合に、認証の解として暗号化された登録生体情報を、キー端末に格納されている復号情報により復号して、前記認証を実施可能にする。

【発明の効果】

【0012】

本発明によれば、登録生体情報の取り扱いのセキュリティ性を向上することができる。

【図面の簡単な説明】

【0013】

40

【図1】一実施形態の認証システムの構成図。

【図2】登録生体情報を暗号化して保管する際の手順を示すフローチャート。

【図3】生体認証の手順を示すフローチャート。

【発明を実施するための形態】

【0014】

以下、認証システム及び認証方法の一実施形態を図1～図3に従って説明する。

図1に示すように、車両1は、キー端末2と無線によるID照合を行って車載装置3の作動を実行又は許可する電子キーシステム4を備える。電子キーシステム4は、車両1からの通信を契機に狭域無線によりID照合（スマート照合）を実行するキー操作フリーシステムである。車載装置3は、例えばドアロック装置5やエンジン6などがある。キー端

50

末 2 は、主にキー機能を有した端末、いわゆる電子キー 7 である。

【0015】

車両 1 は、I D 照合を行う照合 E C U (Electronic Control Unit) 1 0 と、車載電装品の電源を管理するボディ E C U 1 1 と、エンジン 6 を制御するエンジン E C U 1 2 とを備える。これら E C U は、車内の通信線 1 3 を介して電気接続されている。通信線 1 3 は、例えば C A N (Controller Area Network) や L I N (Local Interconnect Network) である。照合 E C U 1 0 のメモリ 1 4 には、車両 1 に登録された電子キー 7 の電子キー I D と、I D 照合の認証時に使用するキー固有鍵とが登録されている。ボディ E C U 1 1 は、車両ドア 1 5 の施解錠を切り替えるドアロック装置 5 を制御する。

【0016】

キー固有鍵を用いた認証は、例えばチャレンジレスポンス認証である。この認証は、公開鍵暗号又は共通鍵暗号のどちらでもよい。公開鍵暗号は、暗号鍵と復号鍵とで異なる鍵情報を用い、復号鍵が秘密鍵となった暗号である。共通鍵暗号は、暗号と復号とで同じ鍵情報を用いる暗号である。

【0017】

車両 1 は、車両 1 における通信を実行する通信部 1 8 を備える。通信部 1 8 は、電子キー 7 との狭域通信の他に、ネットワーク通信が可能となっている。通信部 1 8 は、電子キー 7 との通信を、例えば L F (Low Frequency) - U H F (Ultra High Frequency) の双方向通信 (スマート通信) により実行する。この場合、車両 1 → 電子キー 7 の通信が L F 通信であることが好ましく、電子キー 7 → 車両 1 の通信が U H F 通信であることが好ましい。

【0018】

電子キー 7 は、電子キー 7 の作動を制御するキー制御部 2 1 と、電子キー 7 において通信を実行する通信部 2 2 と、データ書き込み及び読み出しが可能なメモリ 2 3 とを備える。通信部 2 2 は、狭域無線を通じて車両 1 の通信部 1 8 と無線通信を実行する。メモリ 2 3 には、電子キー 7 が持つ固有の電子キー I D 及びキー固有鍵が書き込み保存されている。

【0019】

車両 1 は、待機状態の電子キー 7 を起動させるためにウェイク信号を通信部 1 8 から定期的に L F 送信する。電子キー 7 は、通信部 1 8 から送信されたウェイク信号を受信すると、待機状態から起動状態に切り替わり、車両 1 にアック信号を U H F 送信する。照合 E C U 1 0 は、電子キー 7 から送信されたアック信号を受信して通信の確立を認識すると、I D 照合 (スマート照合) を実行する。スマート照合には、電子キー 7 に登録された電子キー I D の正否を確認するキー I D 照合や、所定の暗号鍵を用いたチャレンジレスポンス認証等がある。

【0020】

車両 1 は、ユーザから取得した生体情報 D s を認証する生体認証機能 (認証システム 2 6) を備える。本例の認証システム 2 6 の認証方式は、生体情報 D s として指紋情報の正否を認証する指紋認証である。また、生体認証は、車両 1 (作動対象物 2 8) の作動を許可又は実行する際に成立が課される 1 条件である。本例の認証システム 2 6 は、生体認証の解 (正解値) である登録生体情報 D k を、電子キー 7 の暗号情報 K により暗号化してデータセンター 2 7 に保管しておき、生体認証時、この暗号化登録生体情報 D k をデータセンター 2 7 から取得して復号し、生体認証を実行する。

【0021】

認証システム 2 6 は、車両 1 において生体認証の処理を実行する生体認証デバイス 3 0 を備える。生体認証デバイス 3 0 は、ユーザの生体情報 D s を取得するセンサ部 3 1 と、センサ部 3 1 で取得した生体情報 D s を認証する処理部 3 2 とを備える。センサ部 3 1 は、車載用の認証システム 2 6 の場合、例えば車両 1 の運転席に配設されたエンジンスイッチ 3 3 のノブ (図示略) に設けられることが好ましい。この場合、エンジンスイッチ 3 3 のノブの押圧操作時、ノブを押すユーザの指から、押し操作と同時にセンサ部 3 1 でユー

10

20

30

40

50

ザの生体情報Ds（指紋情報）を取得することができる。処理部32は、取得した生体情報Dsの正否を確認することにより、生体認証を実行する。

【0022】

認証システム26は、生体認証の解となる登録生体情報Dkを暗号化する暗号化部36を備える。暗号化部36は、照合ECU10に設けられている。暗号化部36は、登録生体情報Dkが事前登録されるにあたり、登録生体情報Dkを暗号化する。暗号化部36は、暗号化された登録生体情報Dk、すなわち暗号化登録生体情報Dkを、ネットワーク通信を通じてデータセンター27に送信し、データセンター27のストレージ37に格納する。

【0023】

データセンター27は、前述のストレージ37と、データセンター27の作動を制御するサーバ38と、データセンター27においてネットワーク通信を行う通信部39とを備える。サーバ38は、車両1から送信された暗号化登録生体情報Dkを通信部39で受診すると、これをストレージ37に格納する。また、サーバ38は、車両1から暗号化登録生体情報送信要求を通信部39で受信すると、ストレージ37に格納されている暗号化登録生体情報Dkを、車両1に通知する。

【0024】

認証システム26は、暗号化登録生体情報Dkを復号する復号部40を備える。復号部40は、照合ECU10に設けられている。復号部40は、生体認証時、データセンター27に対し暗号化登録生体情報送信要求をネットワーク送信し、ストレージ37に格納されている暗号化登録生体情報Dkを取得する。また、復号部40は、電子キー7のメモリ23のセキュアな領域41から暗号情報Kを取得し、この暗号情報Kを基に、ストレージ37から取得した暗号化登録生体情報Dkを復号する。

【0025】

処理部32は、復号した登録生体情報Dkを基に、生体認証を実行する。本例の処理部32は、センサ部31からユーザの生体情報Dsを取得した場合、この生体情報Dsと、取得した復号した登録生体情報Dkとを比較することにより、生体認証を実行する。そして、処理部32は、生体認証の認証結果を、照合ECU10等の他の車載ECUに出力する。

【0026】

次に、図2及び図3を用いて、本実施形態の認証システム26の作用及び効果について説明する。

〔生体認証の解となる生体情報の登録〕

まず、図2を用いて、生体認証の解となる登録生体情報Dkをデータセンター27のストレージ37に登録する手順を説明する。この登録生体情報Dkの登録（登録モード）は、例えば車両1や電子キー7等において、所定の登録操作が実施された場合に開始される。登録操作は、車両1の場合、車内のカーナビゲーションシステムを操作する態様が想定され、電子キー7の場合、電子キー7に設けられた各種ボタンを規定の順序及び回数で操作する態様が想定される。

【0027】

ステップ101において、暗号化部36は、認証システム26が登録生体情報Dkの登録モードに切り替わった場合、電子キー7から暗号情報Kを取得する。暗号情報Kは、生体認証の解として登録しておく登録生体情報Dkを暗号化するのに必要な情報である。

【0028】

ここで、例えば暗号方式が暗号と復号とで異なる鍵となる公開鍵暗号の場合、暗号化部36は、暗号情報Kとして「復号鍵」を電子キー7から取得する。復号鍵は、秘密鍵である。この場合、暗号化部36は、暗号情報Kの取得を、電子キーシステム4のハード構成を用いて実施する。ここでは、まず暗号化部36は、暗号情報Kの通知要求（暗号情報通知要求）を、通信部18からLF電波によって電子キー7に送信する。電子キー7は、車両1から送信された暗号情報通知要求を通信部22で受信すると、メモリ23（セキュア

10

20

30

40

50

な領域 4 1) に格納されている暗号情報 K を読み出し、これを通信部 2 2 から U H F 電波によって送信する。

【0029】

また、例えば暗号方式が暗号と復号とで同じである共通鍵暗号の場合、暗号化部 3 6 は、暗号情報 K として共通の「暗号鍵」を取得する。この場合も、暗号化部 3 6 は、暗号鍵を電子キー 7 から取得する。

【0030】

ステップ 1 0 2 において、暗号化部 3 6 は、生体認証の解とすべき登録生体情報 D k を、センサ部 3 1 から取得する。本例の場合、登録生体情報 D k の登録操作開始の旨を音声や表示により通知してセンサ部 3 1 を操作させ、このときにセンサ部 3 1 によって検出されるセンサ出力を、登録生体情報 D k として取得する。

10

【0031】

ステップ 1 0 3 において、暗号化部 3 6 は、取得した登録生体情報 D k を、電子キー 7 から取得した暗号情報 K (復号鍵) で暗号化する。これにより、暗号化部 3 6 は、暗号化登録生体情報 D k を生成する。

【0032】

ステップ 1 0 4 において、暗号化部 3 6 は、暗号化した登録生体情報 D k (暗号化登録生体情報 D k) を、ネットワーク通信を通じてデータセンター 2 7 に送信する。本例の場合、データセンター 2 7 のサーバ 3 8 は、車両 1 から暗号化登録生体情報 D k を受信すると、車両 1 と対応付けた状態で暗号化登録生体情報 D k をストレージ 3 7 に保管する。これにより、ストレージ 3 7 に保管される暗号化登録生体情報 D k が、車両 1 と一対一対応で保管される。以上により、事前の暗号化登録生体情報 D k の登録作業が完了する。

20

【0033】

[生体認証時の作動]

続いて、図 3 を用いて、生体認証の具体的な作動の手順について説明する。生体認証は、例えば車両電源の遷移操作 (エンジン始動操作) を行う際にユーザに課された認証の場合、エンジン 6 をかけようとしてブレーキペダルを踏み込んだときにセンサ部 3 1 が起動して、認証の作動が開始される。

【0034】

ステップ 2 0 1 において、復号部 4 0 は、データセンター 2 7 (ストレージ 3 7) から、暗号化登録生体情報 D k を取得する。本例の場合、復号部 4 0 は、暗号化登録生体情報 D k の送信を要求する暗号化登録生体情報送信要求を、ネットワーク通信を通じてデータセンター 2 7 に送信する。この暗号化登録生体情報送信要求には、例えば車両 1 の識別情報 (車体番号等) や、暗号化登録生体情報 D k の通知を要求するコマンド等が含まれる。サーバ 3 8 は、復号部 4 0 から送信された暗号化登録生体情報要求を受信すると、同要求に含まれる車両 1 の識別情報から、対応する暗号化登録生体情報 D k を読み出し、これを、ネットワーク通信を通じて車両 1 に送信する。

30

【0035】

ステップ 2 0 2 において、復号部 4 0 は、暗号化登録生体情報 D k を復号するのに必要な暗号情報 K を取得する。本例の場合、復号部 4 0 は、暗号情報 K を車両 1 に送信することを要求する暗号情報送信要求を、電子キーシステム 4 の通信網を介して、車両 1 に登録された電子キー 7 に対して送信 (L F 送信) する。電子キー 7 は、車両 1 から送信された暗号情報送信要求を受信すると、メモリ 2 3 (セキュアな領域 4 1) に登録されている暗号情報 K を読み出し、これを通信部 2 2 から電子キーシステム 4 の通信網を介して送信 (U H F 送信) する。復号部 4 0 は、電子キー 7 から送信された暗号情報 K を通信部 1 8 で受信することにより、暗号情報 K を取得する。なお、暗号方式が公開鍵暗号の場合、暗号情報 K として「復号鍵」を取得し、暗号方式が共通鍵暗号の場合、暗号情報 K として「暗号鍵」を取得する。

40

【0036】

ステップ 2 0 3 において、復号部 4 0 は、データセンター 2 7 から取得した暗号化登録

50

生体情報 D k を、電子キー 7 から取得した暗号情報 K を基に復号する。本例の場合、復号部 4 0 は、暗号情報 K としての復号鍵や暗号鍵により、暗号化登録生体情報 D k を復号する。復号部 4 0 は、復号した登録生体情報 D k を、生体認証デバイス 3 0（処理部 3 2）に出力する。

【0037】

ステップ 2 0 4 において、処理部 3 2 は、センサ部 3 1 で検出した生体情報 D s を、認証対象の生体情報 D s として取得する。すなわち、車両 1 を操作（エンジン 6 を始動させたい）したいユーザがエンジンスイッチ 3 3 を操作したときにセンサ部 3 1 で検出した生体情報 D s を、認証対象の生体情報 D s として取得する。

【0038】

ステップ 2 0 5 において、処理部 3 2 は、認証対象の生体情報 D s と、復号により取得した登録生体情報 D k とを比較し、これらが一致するか否かを判定する。このとき、これらが一致すれば、ステップ 2 0 6 に移行し、これらが一致しなければ、ステップ 2 0 8 に移行する。

【0039】

ステップ 2 0 6 において、処理部 3 2 は、認証対象の生体情報 D s と、復号後の登録生体情報 D k とが一致すれば、生体認証を成立とする。処理部 3 2 は、生体認証が成立する場合、生体認証成立通知を照合 E C U 1 0 に出力する。

【0040】

ステップ 2 0 7 において、照合 E C U 1 0 は、生体認証デバイス 3 0（処理部 3 2）から生体認証成立通知を入力することを契機に、サービスの提供、すなわち車両電源の遷移操作（エンジン始動操作）を許可する。例えば、照合 E C U 1 0 は、車内に位置する電子キー 7 との間でスマート照合（室内スマート照合）が成立することを確認するとともに、生体認証も成立することを確認すると、車両 1 の作動を許可又は実行する。よって、例えばブレーキペダルを踏み込み操作しながらエンジンスイッチ 3 3 が押圧操作されると、エンジン 6 が始動される。

【0041】

ステップ 2 0 8 において、処理部 3 2 は、認証対象の生体情報 D s と、復号後の登録生体情報 D k とが一致しなければ、生体認証を不成立とする。このため、仮に室内スマート照合が成立していても、生体認証が成立しないことによって、エンジン 6 の始動操作が許可されない。よって、第三者による車両盗難に対するセキュリティ性を確保することが可能となる。

【0042】

さて、本例の場合、生体認証の解として用いられる登録生体情報 D k が暗号化されて保管される。このため、仮に登録生体情報 D k が盗難に遭っても、登録生体情報 D k を復号するのに必要な暗号情報 K を知らなければ、登録生体情報 D k を使用することができない。よって、登録生体情報 D k の取り扱いのセキュリティ性を向上することができる。

【0043】

認証の解となる登録生体情報 D k の登録にあたり、電子キー 7 に格納された暗号情報 K を基に登録生体情報 D k が暗号化され、その暗号化登録生体情報 D k がストレージ 3 7 に保管される。よって、ユーザが所持を管理する電子キー 7 を利用して登録生体情報 D k を暗号化するので、復元に遭い難い登録生体情報 D k とすることが可能となる。

【0044】

電子キー 7 は、車両 1 と無線による I D 照合が可能なキーである。また、車両 1 は、電子キー 7 との間の I D 照合（スマート照合）が成立しつつ、生体認証が成立した場合に、作動が許可又は実行される。よって、I D 照合及び生体認証の両方が成立しないと車両 1 の作動が許可又は実行されないため、車両 1 の不正使用に対するセキュリティ性を確保することができる。

【0045】

登録生体情報 D k を復号する暗号情報 K は、その格納先として設けられたメモリ 2 3 に

10

20

30

40

50

においてセキュアな領域 4 1 に格納されている。これにより、暗号情報 K をメモリ 2 3 から不正に読み出すことができなくなるので、登録生体情報 D k の復号に必要な暗号情報 K が盗難され難くなる。よって、登録生体情報 D k の不正取得に対するセキュリティ性を確保することができる。

【0046】

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

・暗号化登録生体情報 D k の登録作業は、車両 1 を介して行われることに限定されない。例えば、キー端末 2（電子キー 7）をデータセンター 2 7 に直接接続して、暗号化登録生体情報 D k の登録を実施してもよい。

10

【0047】

・生体認証の開始は、ブレーキペダルが踏み込まれたときに限定されず、例えば車両ドア 1 5 の開閉を検出してユーザが乗車したときなど、種々のどのタイミングに変更してもよい。

【0048】

・車両 1 の識別情報は、例えば車体番号など、車両 1（作動対象物 2 8）を識別できるパラメータであればよい。

・暗号情報 K は、暗号化登録生体情報 D k を復号できるものであればよい。

【0049】

・暗号情報 K の保存先は、セキュアな領域 4 1 に限定されず、種々のメモリ領域が適用できる。

20

・暗号処理や復号処理は、車両 1（照合 ECU 1 0）で行われることに限らず、例えば電子キー 7 やデータセンター 2 7 など、他の場所で実施されてもよい。

【0050】

・暗号化登録生体情報 D k の格納先は、ストレージ 3 7 に限定されず、データ保存が可能な媒体であればよい。

・登録生体情報 D k は、データセンター 2 7 に保管されることに限定されず、他の保管先を採用してもよい。また、登録生体情報 D k は、車両 1 外に保管されることに限定されず、車両 1 内の格納先に保管されてもよい。

【0051】

30

・電子キーシステム 4 は、電子キー 7 を照合できるシステムであれば、種々の態様のシステムに変更可能である。

・電子キーシステム 4 で使用する電波の周波数や通信方式は、種々の態様のものに適宜変更することができる。

【0052】

・生体情報 D s は、指紋情報に限定されず、生体認証の種類に応じて、他のパラメータに適宜変更できる。

・作動対象物 2 8 は、車両 1 に限定されず、他の機器、装置、設備等に変更してもよい。

【0053】

40

・キー端末 2 は、電子キー 7 に限定されず、キー機能を有している端末であればよい。また、キー端末 2 は、例えば高機能携帯電話としてもよい。

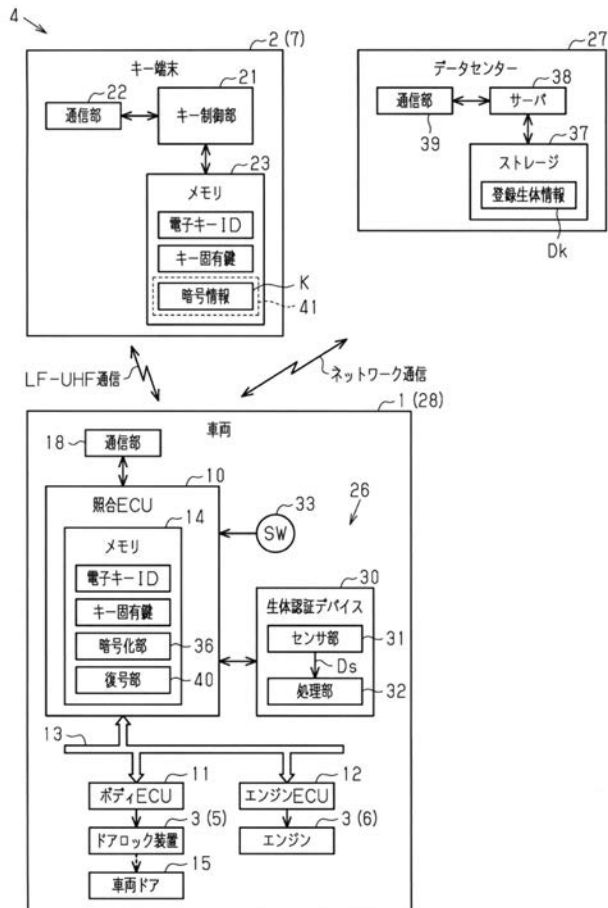
・認証システム 2 6 は、車載用に限定されず、他の対象物に適用されてもよい。

【符号の説明】

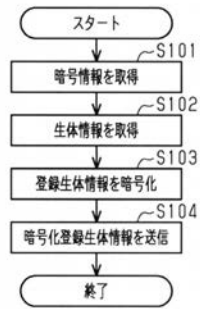
【0054】

1…車両、2…キー端末、7…電子キー、23…メモリ、26…認証システム、28…作動対象物、36…暗号化部、37…ストレージ、40…復号部、41…セキュアな領域、D s…生体情報、D k…登録生体情報（暗号化登録生体情報）、X…暗号情報。

【図 1】



【図 2】



【図 3】

