(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2013-236318
(P2013-236318A)
(43)公開日　平成25年11月21日(2013.11.21)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
B60R 25/01	(2013.01)	H04L	9/00	601E	
B60R 25/04	(2013.01)	B60R	25/00	606	
B60R 25/10	(2013.01)	B60R	25/04	608	
		B60R	25/10	617	

審査請求 未請求　請求項の数 6　OL　（全 20 頁）

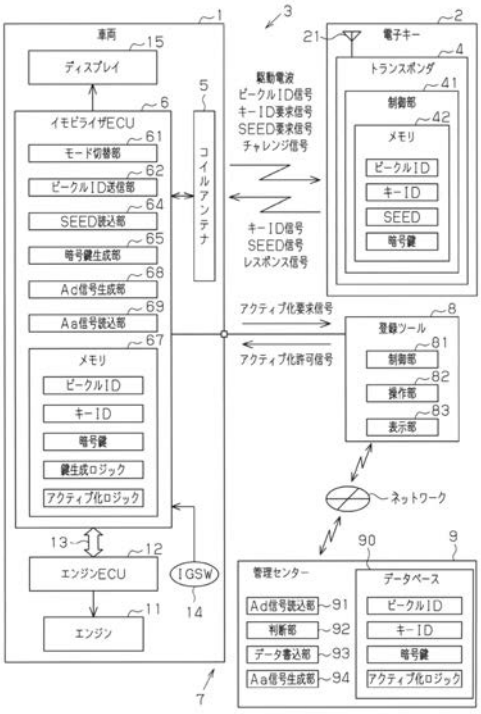
(21)出願番号　特願2012-108546 (P2012-108546)
(22)出願日　平成24年5月10日 (2012.5.10)

(71)出願人　000003551
株式会社東海理化電機製作所
愛知県丹羽郡大口町豊田三丁目２６０番地
(74)代理人　100068755
弁理士　恩田　博宣
(74)代理人　100105957
弁理士　恩田　誠
(72)発明者　長江　敏広
愛知県丹羽郡大口町豊田三丁目２６０番地
株式会社東海理化電機製作所内
(72)発明者　河合　英樹
愛知県丹羽郡大口町豊田三丁目２６０番地
株式会社東海理化電機製作所内

最終頁に続く

(54)【発明の名称】携帯機登録システム

(57)【要約】
【課題】セキュリティ性が高い携帯機登録システムを提供する。
【解決手段】車両１との間で同じ暗号鍵を持ち合い、当該暗号鍵を使用して暗号化通信が行なわれる電子キー２を車両１のイモビライザＥＣＵ６に登録する携帯機登録システムは、イモビライザＥＣＵ６が、電子キー２から送信されるＩＤコード信号に含まれるＳＥＥＤコードから、鍵生成ロジックを使用して暗号鍵を生成し、これを登録する。イモビライザＥＣＵ６は、登録した暗号鍵のアクティブ化を要求する信号を管理センター９に送る。管理センター９は、受信した暗号鍵の自身への登録がなければ、これを登録するとともに当該登録した暗号鍵のアクティブ化を許可する信号をイモビライザＥＣＵ６に送る。イモビライザＥＣＵ６は、アクティブ化を許可する信号を受信して初めて暗号鍵を使用した暗号化通信が許可される。
【選択図】図１



【特許請求の範囲】
【請求項１】
通信対象との間で同じ暗号鍵を持ち合い、前記通信対象の制御装置との間で前記暗号鍵を使用して暗号化通信が行なわれる携帯機を前記制御装置に登録する携帯機登録システムにおいて、
前記制御装置には、前記通信対象に固有の第１の識別情報及び外部から取り込まれる鍵生成コードから暗号鍵を生成する鍵生成ロジックが記憶され、
前記携帯機には、前記暗号鍵を生成する際に使用する前記携帯機に固有の暗号鍵生成コードと、前記鍵生成ロジックを使用して生成される前記暗号鍵とが記憶され、
前記制御装置は、前記携帯機の登録処理として、前記携帯機との無線通信を通じて前記第１の識別情報を登録される前記携帯機に書き込むとともに、前記携帯機に記憶された前記暗号鍵生成コードを取り込んで、当該鍵生成コードから自身に記憶された前記鍵生成ロジックを使用して前記暗号鍵を生成し、生成した当該暗号鍵を記憶するものであって、
前記制御装置及び前記第１の識別情報を管理する管理センターは、両者間における信号の暗号化及び暗号化の解読に使用する前記第１の識別情報に固有のアクティブ化ロジックを記憶し、
前記制御装置は、前記第１の識別情報を含むアクティブ化要求信号を管理センターに送り、
前記管理センターは、前記制御装置が記憶した前記暗号鍵を使用しての前記暗号化通信を許可する旨示す前記アクティブ化ロジックを用いて暗号化したアクティブ化許可信号を前記制御装置に送り、
前記制御装置は、前記アクティブ化許可信号を受信した場合に、当該アクティブ化許可信号を前記アクティブ化ロジックを用いて解読するとともに、自身が記憶した前記暗号鍵を使用しての前記暗号化通信を許可する携帯機登録システム。
【請求項２】
通信対象との間で同じ暗号鍵を持ち合い、前記通信対象の制御装置との間で前記暗号鍵を使用して暗号化通信が行なわれる携帯機を前記制御装置に登録する携帯機登録システムにおいて、
前記制御装置には、前記通信対象に固有の第１の識別情報及び外部から取り込まれる鍵生成コードから暗号鍵を生成する鍵生成ロジックが記憶され、
前記携帯機には、前記暗号鍵を生成する際に使用する前記携帯機に固有の暗号鍵生成コードと、前記鍵生成ロジックを使用して生成される前記暗号鍵とが記憶され、
前記制御装置は、前記携帯機の登録処理として、前記携帯機との無線通信を通じて前記第１の識別情報を登録される前記携帯機に書き込むとともに、前記携帯機に記憶された前記暗号鍵生成コードを取り込んで、当該鍵生成コードから自身に記憶された前記鍵生成ロジックを使用して前記暗号鍵を生成し、生成した当該暗号鍵を記憶するものであって、
前記制御装置は、記憶した前記暗号鍵と前記第１の識別情報とを対応付けたアクティブ化要求信号を管理センターに送り、
前記管理センターは、受信したアクティブ化要求信号に含まれる前記暗号鍵の自身に対する登録の有無を確認し、登録がない場合には、当該暗号鍵を前記第１の識別情報に対応付けて登録するとともに、当該暗号鍵を使用しての前記暗号化通信を許可する旨示すアクティブ化許可信号を前記制御装置に送り、
前記制御装置は、記憶した前記暗号鍵を使用しての前記アクティブ化許可信号を受信した場合に、当該記憶した前記暗号鍵を使用しての前記暗号化通信を許可する携帯機登録システム。
【請求項３】
通信対象との間で同じ暗号鍵を持ち合い、前記通信対象の制御装置との間で前記暗号鍵を使用して暗号化通信が行なわれる携帯機を前記制御装置に登録する携帯機登録システムにおいて、
前記制御装置には、前記通信対象に固有の第１の識別情報及び外部から取り込まれる鍵

生成コードから暗号鍵を生成する鍵生成ロジックが記憶され、
前記携帯機には、前記暗号鍵を生成する際に使用する前記携帯機に固有の暗号鍵生成コードと、前記鍵生成ロジックを使用して生成される前記暗号鍵とが記憶され、
前記制御装置は、前記携帯機の登録処理として、前記携帯機との無線通信を通じて前記第１の識別情報を登録される前記携帯機に書き込むとともに、前記携帯機に記憶された前記暗号鍵生成コードを取り込んで、当該鍵生成コードから自身に記憶された前記鍵生成ロジックを使用して前記暗号鍵を生成し、生成した当該暗号鍵を記憶するものであって、
前記制御装置及び前記第１の識別情報を管理する管理センターは、両者間における信号の暗号化及び暗号化の解読に使用する前記第１の識別情報に固有のアクティブ化ロジックを記憶し、
前記制御装置は、記憶した前記暗号鍵と前記第１の識別情報とを対応付けたアクティブ化要求信号を管理センターに送り、
前記管理センターは、受信したアクティブ化要求信号に含まれる前記暗号鍵の自身に対する登録の有無を確認し、登録がない場合には、当該暗号鍵を前記第１の識別情報に対応付けて登録するとともに、当該暗号鍵を使用しての前記暗号化通信を許可する旨示す前記アクティブ化ロジックを用いて暗号化されたアクティブ化許可信号を前記制御装置に送り、
前記制御装置は、記憶した前記暗号鍵を使用しての前記アクティブ化許可信号を受信した場合に、当該アクティブ化許可信号を前記アクティブ化ロジックを用いて解読するとともに、自身が記憶した前記暗号鍵を使用しての前記暗号化通信を許可する携帯機登録システム。
【請求項４】
請求項１又は３に記載の携帯機登録システムにおいて、
前記制御装置は、前記アクティブ化ロジックを用いて暗号化したアクティブ化要求信号を送信し、
前記管理センターは、前記アクティブ化ロジックを用いて暗号化された前記アクティブ化要求信号を解読する携帯機登録システム。
【請求項５】
請求項１～４のうちいずれか一項に記載の携帯機登録システムにおいて、
前記制御装置及び前記携帯機は、前記暗号鍵に加えて、前記携帯機に固有の第２の識別情報を使用して前記暗号化通信を行うものであって、
前記制御装置は、前記鍵生成コードとともに前記第２の識別情報を取り込み、これを記憶し、当該記憶した第２の識別情報を前記アクティブ化要求信号に含ませて送信し、
前記管理センターは、前記暗号鍵の有無に加えて、前記第２の識別情報の登録の有無を確認し、これら前記暗号鍵及び前記第２の識別情報の登録がない場合に、当該暗号鍵及び第２の識別情報を前記第１の識別情報に対応付けて登録するとともに、前記アクティブ化要求信号に前記第２の識別情報を使用しての前記暗号化通信を許可する旨を含ませる携帯機登録システム。
【請求項６】
請求項１～５のうちいずれか一項に記載の携帯機登録システムにおいて、
前記制御装置と前記管理センターとの通信は、報知手段を備えるツールを介して行われるものであって、
前記管理センターは、前記アクティブ化許可信号を送信できない場合には、その旨示すアクティブ化不可信号を送信し、
前記ツールは、前記アクティブ化不可信号を受信した場合に、前記報知手段を介して前記アクティブ化許可信号を送信できない旨報知する携帯機登録システム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、携帯機を通信対象の制御装置に登録する携帯機登録システムに関する。

【背景技術】
【０００２】
従来、車両のユーザにより所持される携帯機と車両との間で暗号化通信を行い、認証が成立することに基づいて、ドアの施解錠やエンジンの始動停止等を行う携帯機システムが知られている。そして、このような携帯機システムでは、セキュリティ性を維持するために、携帯機と車両との間の通信を保護する必要がある。このため、携帯機システムでは、携帯機と車両との間で暗号通信が行われている（例えば、特許文献１参照）。暗号通信では、通信内容が暗号化されるので、秘匿性に優れる。
【０００３】
上記暗号通信の暗号方式としては、共通鍵暗号方式が採用される。共通鍵暗号方式では、暗号化と復号に同一の暗号鍵を使用する。このため、携帯機と車両との両方に同一の暗号鍵を持たせておく必要がある。携帯機及び車両への暗号鍵の登録は、携帯機を車両の制御装置に登録する過程で行われる。制御装置は、携帯機から無線送信された識別情報と自身に記憶された識別情報との照合によって携帯機との認証を行う。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００９－３０２８４８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ところで、携帯機を制御装置に登録する携帯機登録システムにおいては、制御装置と携帯機との間で紐付けがなければ、どの携帯機を持ってきても制御装置に登録が可能となり、ユーザ以外の携帯機が制御装置に登録されるおそれがある。この場合、ユーザ以外の携帯機を使用することにより携帯機システムを動作させることができるのでセキュリティ性が低い。
【０００６】
この発明は、こうした実情に鑑みてなされたものであり、その目的は、セキュリティ性が高い携帯機登録システムを提供することにある。
【課題を解決するための手段】
【０００７】
上記課題を解決するために、請求項１に記載の発明は、通信対象との間で同じ暗号鍵を持ち合い、前記通信対象の制御装置との間で前記暗号鍵を使用して暗号化通信が行なわれる携帯機を前記制御装置に登録する携帯機登録システムにおいて、前記制御装置には、前記通信対象に固有の第１の識別情報及び外部から取り込まれる鍵生成コードから暗号鍵を生成する鍵生成ロジックが記憶され、前記携帯機には、前記暗号鍵を生成する際に使用する前記携帯機に固有の暗号鍵生成コードと、前記鍵生成ロジックを使用して生成される前記暗号鍵とが記憶され、前記制御装置は、前記携帯機の登録処理として、前記携帯機との無線通信を通じて前記第１の識別情報を登録される前記携帯機に書き込むとともに、前記携帯機に記憶された前記暗号鍵生成コードを取り込んで、当該鍵生成コードから自身に記憶された前記鍵生成ロジックを使用して前記暗号鍵を生成し、生成した当該暗号鍵を記憶するものであって、前記制御装置及び前記第１の識別情報を管理する管理センターは、両者間における信号の暗号化及び暗号化の解読に使用する前記第１の識別情報に固有のアクティブ化ロジックを記憶し、前記制御装置は、前記第１の識別情報を含むアクティブ化要求信号を管理センターに送り、前記管理センターは、前記制御装置が記憶した前記暗号鍵を使用しての前記暗号化通信を許可する旨示す前記アクティブ化ロジックを用いて暗号化したアクティブ化許可信号を前記制御装置に送り、前記制御装置は、前記アクティブ化許可信号を受信した場合に、当該アクティブ化許可信号を前記アクティブ化ロジックを用いて解読するとともに、自身が記憶した前記暗号鍵を使用しての前記暗号化通信を許可することを要旨とする。

【０００８】
同構成によれば、管理センターから送信されるアクティブ化許可信号は、第１の識別情報に固有のアクティブ化ロジックを使用して暗号化されているので、アクティブ化の許可をうけるべき当事者、すなわち先の第１の識別情報と同じ第１の識別情報を有する制御装置でのみ解読可能である。このため、他の制御装置ではアクティブ化許可信号の解読は不可、換言すればアクティブ化は許可されないので、セキュリティ性が高い。
【０００９】
請求項２に記載の発明は、通信対象との間で同じ暗号鍵を持ち合い、前記通信対象の制御装置との間で前記暗号鍵を使用して暗号化通信が行なわれる携帯機を前記制御装置に登録する携帯機登録システムにおいて、前記制御装置には、前記通信対象に固有の第１の識別情報及び外部から取り込まれる鍵生成コードから暗号鍵を生成する鍵生成ロジックが記憶され、前記携帯機には、前記暗号鍵を生成する際に使用する前記携帯機に固有の暗号鍵生成コードと、前記鍵生成ロジックを使用して生成される前記暗号鍵とが記憶され、前記制御装置は、前記携帯機の登録処理として、前記携帯機との無線通信を通じて前記第１の識別情報を登録される前記携帯機に書き込むとともに、前記携帯機に記憶された前記暗号鍵生成コードを取り込んで、当該鍵生成コードから自身に記憶された前記鍵生成ロジックを使用して前記暗号鍵を生成し、生成した当該暗号鍵を記憶するものであって、前記制御装置は、記憶した前記暗号鍵と前記第１の識別情報とを対応付けたアクティブ化要求信号を管理センターに送り、前記管理センターは、受信したアクティブ化要求信号に含まれる前記暗号鍵の自身に対する登録の有無を確認し、登録がない場合には、当該暗号鍵を前記第１の識別情報に対応付けて登録するとともに、当該暗号鍵を使用しての前記暗号化通信を許可する旨示すアクティブ化許可信号を前記制御装置に送り、前記制御装置は、記憶した前記暗号鍵を使用しての前記アクティブ化許可信号を受信した場合に、当該記憶した前記暗号鍵を使用しての前記暗号化通信を許可することを要旨とする。
【００１０】
同構成によれば、管理センターは、受信した暗号鍵の登録がない場合のみ、アクティブ化許可信号を送る。すなわち、管理センターは、暗号鍵の登録があればアクティブ化許可信号を送らない。制御装置は、アクティブ化許可信号を受信しなければ、例え暗号鍵を記憶していても携帯機との間で暗号化通信を行うことができない。このため、携帯機は、複数の制御装置との間で暗号化通信を行うことができないので、セキュリティ性が高い。
【００１１】
請求項３に記載の発明は、通信対象との間で同じ暗号鍵を持ち合い、前記通信対象の制御装置との間で前記暗号鍵を使用して暗号化通信が行なわれる携帯機を前記制御装置に登録する携帯機登録システムにおいて、前記制御装置には、前記通信対象に固有の第１の識別情報及び外部から取り込まれる鍵生成コードから暗号鍵を生成する鍵生成ロジックが記憶され、前記携帯機には、前記暗号鍵を生成する際に使用する前記携帯機に固有の暗号鍵生成コードと、前記鍵生成ロジックを使用して生成される前記暗号鍵とが記憶され、前記制御装置は、前記携帯機の登録処理として、前記携帯機との無線通信を通じて前記第１の識別情報を登録される前記携帯機に書き込むとともに、前記携帯機に記憶された前記暗号鍵生成コードを取り込んで、当該鍵生成コードから自身に記憶された前記鍵生成ロジックを使用して前記暗号鍵を生成し、生成した当該暗号鍵を記憶するものであって、前記制御装置及び前記第１の識別情報を管理する管理センターは、両者間における信号の暗号化及び暗号化の解読に使用する前記第１の識別情報に固有のアクティブ化ロジックを記憶し、前記制御装置は、記憶した前記暗号鍵と前記第１の識別情報とを対応付けたアクティブ化要求信号を管理センターに送り、前記管理センターは、受信したアクティブ化要求信号に含まれる前記暗号鍵の自身に対する登録の有無を確認し、登録がない場合には、当該暗号鍵を前記第１の識別情報に対応付けて登録するとともに、当該暗号鍵を使用しての前記暗号化通信を許可する旨示す前記アクティブ化ロジックを用いて暗号化されたアクティブ化許可信号を前記制御装置に送り、前記制御装置は、記憶した前記暗号鍵を使用しての前記アクティブ化許可信号を受信した場合に、当該アクティブ化許可信号を前記アクティブ化

ロジックを用いて解読するとともに、自身が記憶した前記暗号鍵を使用しての前記暗号化通信を許可することを要旨とする。

【００１２】

同構成によれば、管理センターは、受信した暗号鍵の登録がない場合のみ、アクティブ化許可信号を送る。すなわち、管理センターは、暗号鍵の登録があればアクティブ化許可信号を送らない。制御装置は、アクティブ化許可信号を受信しなければ、例え暗号鍵を記憶していても携帯機との間で暗号化通信を行うことができない。また、アクティブ化許可信号は、アクティブ化ロジックを使用して暗号化されているので、アクティブ化の許可をうけるべき当事者、すなわち先の第１の識別情報と同じ第１の識別情報を有する制御装置でのみ解読可能である。このため、他の制御装置ではアクティブ化許可信号の解読は不可、換言すればアクティブ化は許可されない上、携帯機は、複数の制御装置との間で暗号化通信を行うことができないので、セキュリティ性が高い。

【００１３】

請求項４に記載の発明は、請求項１又は３に記載の携帯機登録システムにおいて、前記制御装置は、前記アクティブ化ロジックを用いて暗号化したアクティブ化要求信号を送信し、前記管理センターは、前記アクティブ化ロジックを用いて暗号化された前記アクティブ化要求信号を解読することを要旨とする。

【００１４】

同構成によれば、アクティブ化ロジックを有するものでなければ、第１の識別情報と暗号鍵とが対応付けられているアクティブ化要求信号を解読することができない。従って、第１の識別情報及び暗号鍵が外部に漏れることを抑制することができるので、よりセキュリティ性が高まる。

【００１５】

請求項５に記載の発明は、請求項１～４のうちいずれか一項に記載の携帯機登録システムにおいて、前記制御装置及び前記携帯機は、前記暗号鍵に加えて、前記携帯機に固有の第２の識別情報を使用して前記暗号化通信を行うものであって、前記制御装置は、前記鍵生成コードとともに前記第２の識別情報を取り込み、これを記憶し、当該記憶した第２の識別情報を前記アクティブ化要求信号に含ませて送信し、前記管理センターは、前記暗号鍵の有無に加えて、前記第２の識別情報の登録の有無を確認し、これら前記暗号鍵及び前記第２の識別情報の登録がない場合に、当該暗号鍵及び第２の識別情報を前記第１の識別情報に対応付けて登録するとともに、前記アクティブ化要求信号に前記第２の識別情報を使用しての前記暗号化通信を許可する旨を含ませることを要旨とする。

【００１６】

同構成によれば、管理センターには、第１の識別情報に対応付けられた状態で、暗号鍵、及び第２の識別情報が登録されている。このため、携帯機を紛失した場合でも、管理センターに登録されている情報から制御装置に該当する携帯機を製造することができる。

【００１７】

請求項６に記載の発明は、請求項１～５のうちいずれか一項に記載の携帯機登録システムにおいて、前記制御装置と前記管理センターとの通信は、報知手段を備えるツールを介して行われるものであって、前記管理センターは、前記アクティブ化許可信号を送信できない場合には、その旨示すアクティブ化不可信号を送信し、前記ツールは、前記アクティブ化不可信号を受信した場合に、前記報知手段を介して前記アクティブ化許可信号を送信できない旨報知することを要旨とする。

【００１８】

同構成によれば、アクティブ化が許可されない場合、その旨報知手段から報知されるので、制御装置と携帯機との間の登録作業を行う作業者は、アクティブ化が許可されなかったことを認識しやすい。

【発明の効果】

【００１９】

本発明によれば、セキュリティ性が高い携帯機登録システムを提供することができる。

【図面の簡単な説明】
【００２０】
【図１】電子キー登録システムの概略構成を示すブロック図。
【図２】電子キー登録システムの製造を示す図。
【図３】電子キー登録システムの登録を示す図。
【図４】電子キー登録システムの登録作業を示すシーケンスチャート。
【図５】電子キー登録システムの追加キーの製造を示す図。
【図６】電子キー登録システムの交換ＥＣＵの製造を示す図。
【発明を実施するための形態】
【００２１】
以下、本発明にかかる電子キー登録システムを車両に具体化した一実施形態について図１～図６を参照して説明する。
図１に示すように、車両１には、例えば近距離無線通信（通信距離が約数ｃｍの無線通信）によって電子キー２とＩＤ照合を実行するイモビライザシステム３が設けられている。電子キー２には、ＩＤタグ、いわゆるトランスポンダ４が設けられている。イモビライザシステム３は、車両１のコイルアンテナ５から送信される駆動電波によりトランスポンダ４が起動した際、このトランスポンダ４から送信されるキーＩＤ信号を基にＩＤ照合を行うシステムである。なお、車両１が通信対象に相当する。また、イモビライザシステム３が電子キーシステムとして機能する。
【００２２】
車両１には、イモビライザシステム３のコントロールユニットとしてイモビライザＥＣＵ６が設けられている。イモビライザＥＣＵ６には、エンジン１１の動作を制御するエンジンＥＣＵ１２が車内ＬＡＮ１３を介して接続されている。イモビライザＥＣＵ６のメモリ６７には、車両１と組をなす電子キー２のキーＩＤが登録されている。イモビライザＥＣＵ６には、ＬＦ（Ｌｏｗ　Ｆｒｅｑｕｅｎｃｙ）帯、及びＨＦ（Ｈｉｇｈ　Ｆｒｅｑｕｅｎｃｙ）帯の電波を送受信するコイルアンテナ５が接続されている。コイルアンテナ５は、磁界成分により電波を送信する磁界アンテナが採用されており、キーシリンダに設けられている。なお、イモビライザＥＣＵ６が制御装置に相当する。
【００２３】
電子キー２のトランスポンダ４には、通信動作を制御する制御部４１が設けられている。この制御部４１のメモリ４２には、電子キー２に固有のキーＩＤ（トランスポンダコード）が登録されている。トランスポンダ４には、ＬＦ帯、及びＨＦ帯の電波を送受信する送受信アンテナ２１が設けられている。
【００２４】
イモビライザＥＣＵ６は、電子キー２がキーシリンダに挿入されたことを検出すると、コイルアンテナ５から駆動電波を断続的に送信する。乗車したユーザがエンジン１１を始動する際には、電子キー２をキーシリンダに挿入して、回動操作を行う。このとき、トランスポンダ４は、コイルアンテナ５から送信される駆動電波を送受信アンテナ２１で受信すると、駆動電波を電源として起動する。トランスポンダ４は、起動状態に切り換わると、自身に登録されたキーＩＤを含むキーＩＤ信号を送受信アンテナ２１から送信する。イモビライザＥＣＵ６は、トランスポンダ４から送信されたキーＩＤ信号をコイルアンテナ５で受信すると、キーＩＤ信号に含まれるキーＩＤと自身のメモリ６７に記憶されている使用の許可された（許可フラグがたてられている）キーＩＤとのＩＤ照合（イモビライザ照合）を実行する。イモビライザＥＣＵ６は、ＩＤ照合の結果をメモリ６７へ記憶する。なお、本例では、許可フラグをたてることをアクティブ化といい、当該アクティブ化の詳細については後述する。
【００２５】
キーシリンダ内には、電子キー２の回動位置を検出するイグニッションスイッチ（ＩＧＳＷ）１４が設けられている。イグニッションスイッチ１４がエンジンスタート位置まで操作されると、エンジンＥＣＵ１２は、イモビライザＥＣＵ６にＩＤ照合が成立している

か否かを確認する。エンジンＥＣＵ１２は、イモビライザＥＣＵ６からＩＤ照合の結果を取得し、その結果が照合成立を示すものであるとき、エンジン１１への点火制御及び燃料噴射制御を開始し、エンジン１１を始動させる。

【００２６】

イモビライザＥＣＵ６は、電子キー２のキーＩＤを確認するコード照合の他に、チャレンジレスポンス認証も実行する。チャレンジレスポンス認証は、車両１が例えば乱数コードとしてチャレンジコードを電子キー２に送信してレスポンスを演算させ、車両１が自ら演算するレスポンスコードと、電子キー２から受信したレスポンスコードとが一致するか否かによる認証である。本例のイモビライザＥＣＵ６とトランスポンダ４との認証には、共通の暗号鍵を用いる共通鍵暗号方式が採用されている。電子キー２及びイモビライザＥＣＵ６は、それぞれに登録された暗号鍵を使用してチャレンジコードからレスポンスコードを演算する。

【００２７】

トランスポンダ４のメモリ４２には、車両１に固有の識別情報であるビークルＩＤ（ＶＩＤ）と、暗号鍵Ｋを生成する際に使用するＳＥＥＤコード（ＳＣ）と、認証に用いる暗号鍵Ｋとが記憶されている。

【００２８】

イモビライザＥＣＵ６のメモリ６７には、車両１に固有の識別情報であるビークルＩＤ（ＶＩＤ）と、認証に用いる暗号鍵Ｋと、暗号鍵Ｋを生成する際に使用する鍵生成ロジックｆと、電子キー２のキーＩＤとが記憶されている。また、メモリ６７には、ビークルＩＤ、キーＩＤ及び暗号鍵Ｋ等を暗号化するアクティブ化ロジックｇが記憶されている。アクティブ化ロジックｇは、ビークルＩＤに対応する固有のものである。このアクティブ化ロジックｇは、アクティブ化の過程で使用される。

【００２９】

イモビライザシステム３には、電子キー２をイモビライザＥＣＵ６に登録する電子キー登録システム７が含まれる。電子キー登録システム７は、電子キー２と、イモビライザＥＣＵ６との間で無線通信を行い、互いに固有の情報を登録するシステムである。電子キー登録システム７は、イモビライザＥＣＵ６に対して、アクティブ化を許可する管理センター９を備える。管理センター９は、ビークルＩＤに対し、キーＩＤ、暗号鍵Ｋ、及びアクティブ化ロジックｇが対応付けられた状態で保存するデータベース９０を備える。図２に示すように、データベース９０には、初め車両１に固有のビークルＩＤ及びアクティブ化ロジックｇのみが保存されている。イモビライザＥＣＵ６は、製造される際、データベース９０に保存されているビークルＩＤ及びアクティブ化ロジックｇがメモリ４２に記憶される。なお、データベース９０へのキーＩＤ及び暗号鍵Ｋの書き込みは、アクティブ化の過程で行われる。また、図２中に示す（－）は、キーＩＤ等が登録されていないこと、すなわちブランクであることを示す。

【００３０】

図１に示すように、電子キー登録システム７は、イモビライザＥＣＵ６に電子キー２を登録するための登録ツール８を備える。登録ツール８は、車両１に接続して使用される。登録ツール８は、イモビライザＥＣＵ６の動作モードを通常モードと登録モードとの間で切り替える。登録モードとされたイモビライザＥＣＵ６は、電子キー２との間で無線通信を行い、自身に固有の情報（ビークルＩＤ（ＶＩＤ－Ａ））を電子キー２に登録させるとともに、電子キー２に固有の情報（キーＩＤ（Ｋｙ－Ａ）、暗号鍵Ｋ（Ｋ－Ａ））を登録する。そして、イモビライザＥＣＵ６は、アクティブ化要求信号を生成し、これを登録ツール８に送る。登録ツール８には、登録ツール８を制御する制御部８１と、ユーザによる登録操作を検出する操作部８２と、登録動作を表示する表示部８３とが設けられている。登録ツール８は、ユーザに操作されて登録モードに設定されると、イモビライザＥＣＵ６の動作モードを登録モードに変更する旨示す登録信号を車両１に出力する。また、登録ツール８は、イモビライザＥＣＵ６からアクティブ化要求信号を受信すると、当該アクティブ化要求信号をネットワークを介して管理センター９に送る。登録ツール８は、管理セン

ター９からアクティブ化許可信号を受信すると、当該アクティブ化許可信号をイモビライザＥＣＵ６に送る。なお、アクティブ化要求信号（Ａｃｔｉｖｅ ｄｅｍａｎｄ 以下、Ａｄ信号）及びアクティブ化許可信号（Ａｃｔｉｖｅ ａｐｐｒｏｖａｌ、以下Ａａ信号）については、後述するアクティブ化の過程で説明する。

【００３１】

イモビライザＥＣＵ６には、動作モードを切り替えるモード切替部６１が設けられている。モード切替部６１は、登録ツール８から登録信号が入力されると、動作モードを通常モードから登録モードに切り替える。モード切替部６１は、登録モードに切り替えた後、イモビライザＥＣＵ６と登録ツール８との接続が解除された場合に、動作モードを通常モードに切り替える。通常モードのイモビライザＥＣＵ６は、電子キー２との間で、通常の認証、すなわちＩＤ照合を行う。

【００３２】

イモビライザＥＣＵ６には、登録する電子キー２にビークルＩＤを送信するビークルＩＤ送信部６２が設けられている。イモビライザＥＣＵ６の動作モードが登録モードに切り替えられると、ビークルＩＤ送信部６２は、メモリ６７に記憶されたビークルＩＤを含ませたビークルＩＤ信号をコイルアンテナ５から電子キー２に送信する。

【００３３】

また、イモビライザＥＣＵ６には、電子キー２に記憶されている暗号鍵Ｋを生成するためにＳＥＥＤコードを読み込むＳＥＥＤ読込部６４が設けられている。イモビライザＥＣＵ６は、ＳＥＥＤコードを要求するＳＥＥＤ要求信号をコイルアンテナ５から送信する。電子キー２は、ＳＥＥＤ要求信号を受信すると、ＳＥＥＤコードを含むＳＥＥＤ信号を生成し、この生成した信号を送信する。ＳＥＥＤ読込部６４は、コイルアンテナ５を介して受信されるＳＥＥＤ信号からＳＥＥＤコードを取り出す。

【００３４】

また、イモビライザＥＣＵ６には、暗号鍵Ｋを生成する暗号鍵生成部６５が設けられている。暗号鍵生成部６５は、ＳＥＥＤ読込部６４が取得したＳＥＥＤコードからメモリ６７に記憶されている鍵生成ロジックｆを使用して暗号鍵Ｋを生成する。

【００３５】

また、イモビライザＥＣＵ６には、Ａｄ信号を生成するアクティブ化要求信号生成部（以下、Ａｄ信号生成部）６８が設けられている。Ａｄ信号生成部６８は、メモリ６７に記憶されているアクティブ化ロジックｇを使用してキーＩＤ、暗号鍵Ｋ、及びアクティブ化の許可を要求するコードを暗号化させたＡｄ信号を生成する。

【００３６】

管理センター９は、Ａｄ信号を読み込むアクティブ化要求信号読込部（以下、Ａｄ信号読込部）９１と、アクティブ化を許可するか否かを判断する判断部９２と、データベース９０のデータを更新するデータ書込部９３と、アクティブ化許可信号生成部（以下、Ａａ信号生成部）９４とを備える。

【００３７】

管理センター９がＡｄ信号を受信すると、Ａｄ信号読込部９１は、データベース９０に保存されているアクティブ化ロジックｇのいずれかを使用して、Ａｄ信号に含まれるビークルＩＤ、キーＩＤ、暗号鍵Ｋ、及びアクティブ化を要求するコードを読み込む。判断部９２は、Ａｄ信号読込部９１において読み込んだアクティブ化の許可を要求するコードの有無を判断するとともに、当該コードが有ると判断される場合には、データベース９０を参照して受信したキーＩＤ及び暗号鍵Ｋが登録されているか否か判断する。データ書込部９３は、判断部９２において受信したキーＩＤ及び暗号鍵Ｋが登録されていないと判断された場合に、当該受信したキーＩＤ及び暗号鍵Ｋを同じく受信したビークルＩＤと対応するようにデータベース９０に書き込む。Ａａ信号生成部９４は、データ書込部９３において、キーＩＤ及び暗号鍵Ｋがデータベース９０に書き込まれた場合に、ビークルＩＤ、キーＩＤ、暗号鍵Ｋ、及びアクティブ化を許可するコードをビークルＩＤと対応するアクティブ化ロジックｇで暗号化させたＡａ信号を生成する。管理センター９は、Ａａ信号生成

部９４において生成されたＡａ信号をネットワークを介して登録ツール８に送る。

【００３８】

イモビライザＥＣＵ６には、受信したＡａ信号を読み込み、メモリ６７に登録されているキーＩＤ及び暗号鍵Ｋに許可フラグをたてるアクティブ化許可信号読込部（以下、Ａａ信号読込部）６９が設けられている。Ａａ信号読込部６９は、メモリ６７に保存されているアクティブ化ロジックｇを使用して、Ａａ信号に含まれるビークルＩＤ、キーＩＤ、暗号鍵Ｋ、及びアクティブ化を許可するコードを読み込む。そして、読み込んだキーＩＤ及び暗号鍵Ｋがメモリ６７に登録されている場合には、これらキーＩＤ及び暗号鍵Ｋに許可フラグをたてる（アクティブ化）。キーＩＤ及び暗号鍵Ｋは、アクティブ化されることにより使用可能となる。これにより、イモビライザＥＣＵ６は、アクティブ化されたキーＩＤ及び暗号鍵Ｋを有する電子キー２との間におけるＩＤ照合が可能になる。

【００３９】

次に、イモビライザＥＣＵ６への電子キー２の登録作業について図２～図６を参照して説明する。

車両１は、多種多様な部品で構成される。このため、各部品は、部品工場で製造された後、組付工場に集められ、そこで車両１に組付けられる。すなわち、イモビライザＥＣＵ６、及び電子キー２は、それぞれ、部品工場で製造された後、組付工場へと集められ、組付ラインにて車両に組付けられる。そして、イモビライザＥＣＵ６に対する電子キー２の登録作業が行われる。

【００４０】

まず、登録作業前の部品工場における製造作業について説明する。図２に示すように、イモビライザＥＣＵ６は、ビークルＩＤ（ＶＩＤ－Ａ）、鍵生成ロジックｆ、及びアクティブ化ロジックｇ（ｇ－Ａ）がメモリ６７に記憶された状態で製造される。ビークルＩＤ（ＶＩＤ－Ａ）及びアクティブ化ロジックｇ（ｇ－Ａ）は、データベース９０に記憶されているものである。これらは、イモビライザＥＣＵ６に固有のものである。鍵生成ロジックｆは、製造されるイモビライザＥＣＵ６全てに共通するものである。一方、電子キー２は、キーＩＤ（Ｋｙ－Ａ）と、ＳＥＥＤコード（ＳＣ－Ａ）と、当該ＳＥＥＤコードから鍵生成ロジックｆを使用して生成された暗号鍵Ｋ（Ｋ－Ａ）とがメモリ４２に記憶された状態で製造される。なお、ＳＥＥＤコード（ＳＣ－Ａ）は、電子キー２に固有のものである。

【００４１】

次に、組付工場における電子キー２の登録作業について説明する。図３に示すように、本例の電子キー登録システム７では、イモビライザＥＣＵ６がビークルＩＤ（ＶＩＤ－Ａ）を含むビークルＩＤ信号を送信する。電子キー２は、イモビライザＥＣＵ６からのビークルＩＤ信号を受信すると、この信号に含まれるビークルＩＤ（ＶＩＤ－Ａ）を登録する。また、電子キー２はＳＥＥＤコード（ＳＣ－Ａ）を含むＳＥＥＤコード信号を送信する。イモビライザＥＣＵ６は、ＳＥＥＤコード信号に含まれるＳＥＥＤコードを一時的にメモリ６７記憶するとともに、当該ＳＥＥＤコード（ＳＣ－Ａ）から鍵生成ロジックｆを使用して暗号鍵Ｋ（Ｋ－１）を生成し、これをメモリ６７に記憶する。このように、電子キー２とイモビライザＥＣＵ６は、予め紐付けされている（対応している）のではなく、組付工場における登録作業を経て初めて紐付けされる。

【００４２】

ここで、図４及び図５に示されるシーケンスチャートに従って電子キー２の登録処理手順について詳細に説明する。図４に示すように、登録ツール８は、ユーザによって操作されて登録モードに設定されると、登録信号をイモビライザＥＣＵ６に出力する（ステップＳ１）。イモビライザＥＣＵ６は、登録信号を受信すると、動作モードを登録モードに切り替える（ステップＳ２）。

【００４３】

そして、イモビライザＥＣＵ６は、メモリ６７に記憶されたビークルＩＤ（ＶＩＤ－Ａ）を含ませたビークルＩＤ信号をコイルアンテナ５から電子キー２に送信する（ステップ

Ｓ３）。電子キー２は、ビークルＩＤ信号を受信すると、ビークルＩＤ信号に含まれるビークルＩＤ（ＶＩＤ－Ａ）をメモリ４２に書き込む（ステップＳ４）。

【００４４】

イモビライザＥＣＵ６は、ステップＳ３のビークルＩＤの送信に続いて、キーＩＤの送信を要求するキーＩＤ要求信号をコイルアンテナ５から送信する（ステップＳ５）。

電子キー２は、キーＩＤ要求信号を受信すると、これに対する応答としてメモリ４２に記憶されたキーＩＤ（Ｋｙ－Ａ）を含むキーＩＤ信号を送信する（ステップＳ６）。

【００４５】

イモビライザＥＣＵ６は、キーＩＤ信号を受信すると、当該信号に含まれるキーＩＤ（Ｋｙ－Ａ）をメモリ６７に書き込む（ステップＳ７）。

イモビライザＥＣＵ６は、ステップＳ５のキーＩＤ要求信号の送信に続いて、ＳＥＥＤコードの送信を要求するＳＥＥＤ要求信号をコイルアンテナ５から送信する（ステップＳ８）。

【００４６】

電子キー２は、ＳＥＥＤ要求信号を受信すると、これに対する応答としてメモリ４２に記憶されたＳＥＥＤコード（ＳＣ－Ａ）を含むＳＥＥＤ信号を送信する（ステップＳ９）。

【００４７】

イモビライザＥＣＵ６は、ＳＥＥＤ信号を受信すると、当該信号に含まれるＳＥＥＤコード（ＳＣ－Ａ）から鍵生成ロジックｆを使用して暗号鍵Ｋ（Ｋ－Ａ）を生成する（ステップＳ１０）。すなわち、イモビライザＥＣＵ６は、電子キー２から暗号鍵Ｋ（Ｋ－Ａ）を直接取得するのではなく、ＳＥＥＤコード（ＳＣ－Ａ）を取得することで暗号鍵Ｋ（Ｋ－Ａ）を生成する。なお、ＳＥＥＤコード（ＳＣ－Ａ）は、一時的にメモリ６７に記憶される。続いて、イモビライザＥＣＵ６は、生成した暗号鍵Ｋ（Ｋ－Ａ）をメモリ６７に記憶する（ステップＳ１１）。

【００４８】

続いて、図５に示すように、イモビライザＥＣＵ６は、自身に登録されたキーＩＤ及び暗号鍵Ｋを使用してのＩＤ照合の許可（アクティブ化）を得るべく、アクティブ化要求信号（Ａｄ信号）を登録ツール８に送信する（ステップＳ１２）。Ａｄ信号を受信した登録ツール８は、ネットワークを介してこのＡｄ信号を管理センター９へ送信する（ステップＳ１３）。

【００４９】

管理センター９は、Ａｄ信号を受信すると、アクティブ化ロジックｇを使用して、ビークルＩＤ、キーＩＤ、暗号鍵Ｋ、及びアクティブ化の許可を要求するコードを得る（ステップＳ１４）。次に、管理センター９は、受信したキーＩＤ及び暗号鍵Ｋがデータベース９０に登録されているか否かを判断する（ステップＳ１５）。キーＩＤ及び暗号鍵Ｋがデータベース９０に登録されていなければ、管理センター９は、これらキーＩＤ及び暗号鍵Ｋが同じく受信したビークルＩＤと対応するようにデータベース９０に書き込む（ステップＳ１６）。そして、管理センター９は、ネットワークを介してアクティブ化許可信号（Ａａ信号）を登録ツール８へ送信する（ステップＳ１７）。

【００５０】

Ａａ信号を受信した登録ツール８は、接続されているイモビライザＥＣＵ６に、受信したＡａ信号を送信する（ステップＳ１８）。イモビライザＥＣＵ６は、Ａａ信号を受信すると、アクティブ化ロジックｇを使用して、ビークルＩＤ、キーＩＤ、暗号鍵Ｋ、及びアクティブ化を許可するコードを得る（ステップＳ１９）。イモビライザＥＣＵ６は、アクティブ化を許可するコードを得ると、同じく受信したキーＩＤ及び暗号鍵Ｋに許可フラグをたてる（アクティブ化）（ステップＳ２０）。こうして、イモビライザＥＣＵ６は、自身に登録されたキーＩＤ及び暗号鍵Ｋを使用しての電子キー２とのＩＤ照合が可能となる。

【００５１】

なお、図６に示すように、ステップＳ１５において、キーＩＤ及び暗号鍵Ｋがデータベース９０に登録されている場合には、管理センター９は、キーＩＤ及び暗号鍵Ｋをデータベース９０への書き込みをせずに、アクティブ化ができない旨示すアクティブ化不可信号（ｎＡａ信号）を登録ツール８へ送信する（ステップＳ２１）。ｎＡａ信号を受信した登録ツール８は、表示部８３にアクティブ化が不可である旨示す表示を行う（ステップＳ２２）。

【００５２】

このように、電子キー２が既にデータベース９０に登録されている場合には、その電子キー２のキーＩＤ及び暗号鍵Ｋはアクティブ化されない。すなわち、イモビライザＥＣＵ６は、登録されていてもアクティブ化されていないキーＩＤ及び暗号鍵Ｋを使用してＩＤ照合を行うことができない。これにより、電子キー２は、複数のイモビライザＥＣＵ６に対してＩＤ照合を行うことができないので、セキュリティ性が高い。また、表示部８３の視認を通じて、これら一連の登録作業を行う作業者が、電子キー２が既にデータベース９０に登録されていることを認識することができる。

【００５３】

次に、車両出荷後に、電子キー２を紛失等して電子キー２を補給する場合、及びイモビライザＥＣＵ６が故障等してイモビライザＥＣＵ６を交換する場合について説明する。

図３に示すように、管理センター９のデータベース９０には、アクティブ化されたビークルＩＤ、キーＩＤ、暗号鍵Ｋ、及びアクティブ化ロジックｇが対応付けられて保存されている。このため、ビークルＩＤ又はキーＩＤがわかれば、これに対応する情報をデータベース９０から読み込むことにより、ＩＤ照合が可能とされた状態の電子キー２及びイモビライザＥＣＵ６を容易に製造することができる。このため、先に説明した特別な登録作業は必要ない。

【００５４】

以上、説明した実施形態によれば、以下の効果を奏することができる。

（１）イモビライザＥＣＵ６は、登録したキーＩＤ及び暗号鍵Ｋを使用してＩＤ照合を行う旨許可するアクティブ化許可信号を受信した場合に、キーＩＤ及び暗号鍵Ｋに許可フラグを立てるようにした。そして、イモビライザＥＣＵ６は、許可フラグがたててあるキーＩＤ及び暗号鍵Ｋを使用してのＩＤ照合のみ許可するようにした。すなわち、許可フラグのないキーＩＤ及び暗号鍵Ｋを使用してのＩＤ照合はできない。これにより、電子キー２は、複数のイモビライザＥＣＵ６に対してＩＤ照合を行うことができないので、イモビライザシステム３のセキュリティ性が高い。

【００５５】

また、管理センター９を介した登録作業が行われないと、キーＩＤ及び暗号鍵Ｋのアクティブ化が行われない。従って、仮に登録前の電子キー２又はイモビライザＥＣＵ６が市場に流出しても、当該流出した電子キー２又はイモビライザＥＣＵ６は、管理センター９を介した登録作業を行うことができない。この点からも、イモビライザシステム３のセキュリティ性は高い。

【００５６】

（２）電子キー２とイモビライザＥＣＵ６は、予め紐付けされているのではなく、組付工場における登録作業を経て初めて紐付けされる。すなわち、電子キー２は、どのイモビライザＥＣＵ６に対しても登録可能である。逆にイモビライザＥＣＵ６は、どの電子キー２に対しても登録可能である。これにより、電子キー２とイモビライザＥＣＵ６とが組付工場にセットで納入される必要はない。また、登録作業時における作業者の負担も小さい。

【００５７】

（３）アクティブ化要求信号及びアクティブ化許可信号をビークルＩＤに固有のアクティブ化ロジックで暗号化した。同じビークルＩＤをもつ当事者である管理センター９及びイモビライザＥＣＵ６以外におけるアクティブ化要求信号及びアクティブ化許可信号の解読は不可である。これにより、アクティブ化要求信号及びアクティブ化許可信号に含まれ

るビークルＩＤ、キーＩＤ、暗号鍵Ｋが外部に漏れることが抑制される。

【００５８】

（４）イモビライザＥＣＵ６と管理センター９との通信は、表示部８３を備える登録ツール８を介して行うようにした。また、管理センター９は、アクティブ化要求信号に含まれるキーＩＤ及び暗号鍵Ｋの少なくとも一つがデータベース９０に登録されている場合に、アクティブ化が許可できない旨示すアクティブ化不可信号を送信するようにした。そして、登録ツール８は、アクティブ化不可信号を受信した場合に、表示部８３を通じてアクティブ化が許可できない旨を表示するようにした。これにより、一連の登録作業を行う作業者が、表示部８３の視認を通じて、電子キー２が既にデータベース９０に登録されていることを容易に認識することができる。

【００５９】

なお、上記実施形態は、これを適宜変更した以下の形態にて実施することができる。

・上記実施形態において、アクティブ化要求信号にキーＩＤを含ませなくてもよい。すなわち、管理センター９は、データベース９０において暗号鍵Ｋの登録の有無のみ確認し、登録がなければ当該暗号鍵Ｋを登録するとともに、アクティブ化許可信号を送信する。このようにしても、電子キー２は、複数のイモビライザＥＣＵ６との間におけるＩＤ照合が許可されないので、セキュリティ性が高い。また、アクティブ化要求信号に暗号鍵を含ませなくてもよい。すなわち、管理センター９は、データベース９０においてビークルＩＤのみ登録し、その後アクティブ化許可信号を送信する。このようにしても、アクティブ化許可信号は、アクティブ化ロジックｇにより暗号化されているので、セキュリティ性が高い。

【００６０】

・上記実施形態において、管理センター９は、必ずしも暗号鍵Ｋの登録の有無を確認しなくてもよい。この場合、管理センター９は、アクティブ化許可信号をアクティブ化ロジックｇで暗号化する必要がある。このように構成した場合、アクティブ化許可信号は、アクティブ化許可信号を受信するべきイモビライザＥＣＵ６でのみ解読可能である。このため、仮に他のイモビライザＥＣＵでアクティブ化許可信号を受信しても、当該受信したアクティブ化許可信号の解読は不能である。従って、他のイモビライザＥＣＵとそれに登録された電子キーとの間における無線通信はアクティブ化されないので、セキュリティ性が高い。

【００６１】

・上記実施形態において、アクティブ化要求信号及びアクティブ化許可信号は、必ずしもアクティブ化ロジックで暗号化されている必要はない。また、アクティブ化ロジックで暗号化されているのは、アクティブ化要求信号及びアクティブ化許可信号のどちらか一方であってもよい。このようにしても、電子キー２は、複数のイモビライザＥＣＵ６との間におけるＩＤ照合が許可されないので、セキュリティ性が高い。

【００６２】

・上記実施形態において、イモビライザＥＣＵ６と管理センター９との通信は、必ずしも登録ツール８を介して行う必要はない。すなわち、イモビライザＥＣＵ６と管理センター９との通信は、他のツールを介して行ってもよいし、直接行ってもよい。このようにしても、電子キー２は、複数のイモビライザＥＣＵ６との間におけるＩＤ照合が許可されないので、セキュリティ性が高い。

【００６３】

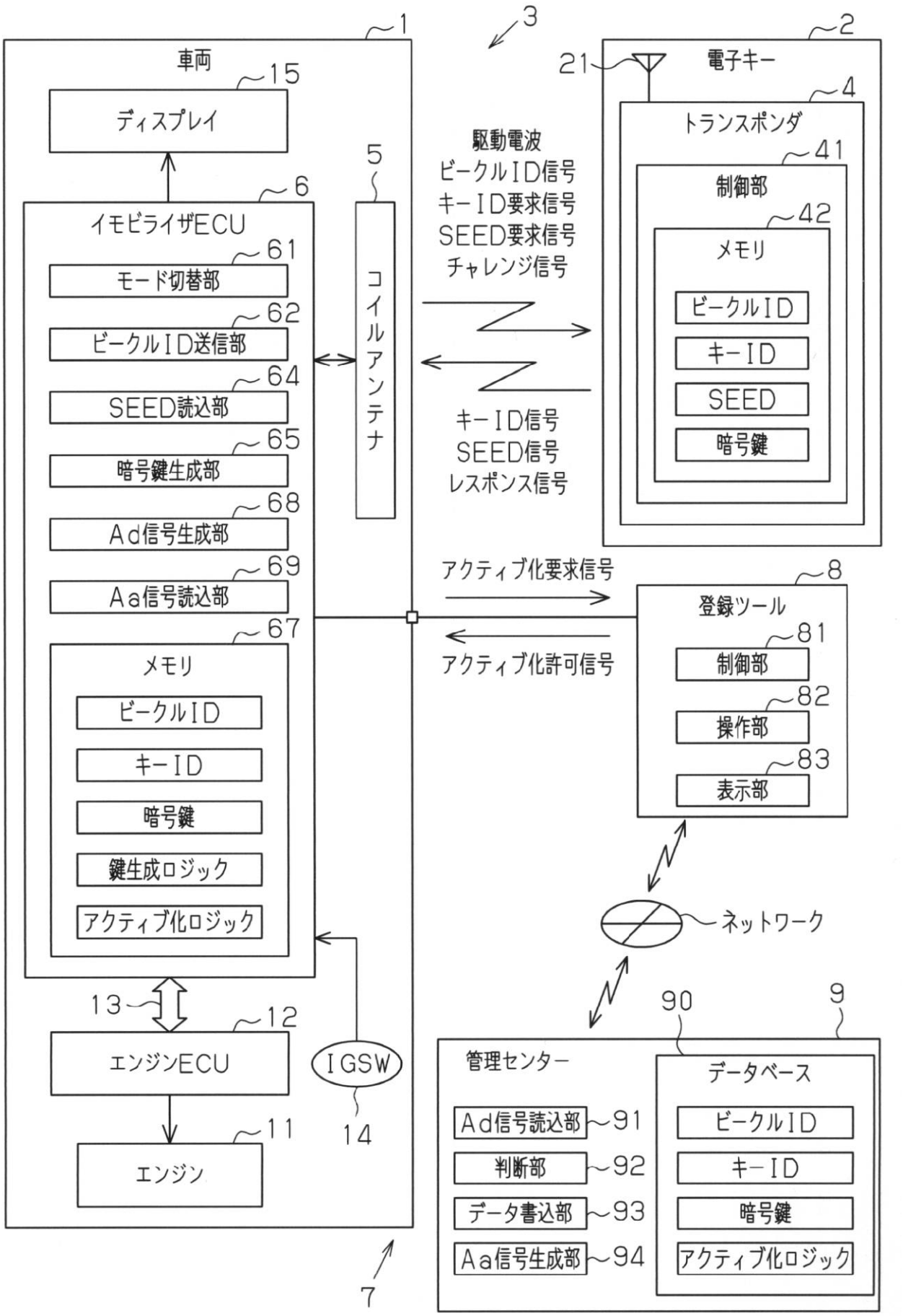
・上記実施形態において、登録ツール８は、アクティブ化許可信号を受信した場合に表示部８３にその旨表示してもよい。このようにすれば、登録作業者が、アクティブ化が許可されたことを容易に認識することができる。

【００６４】

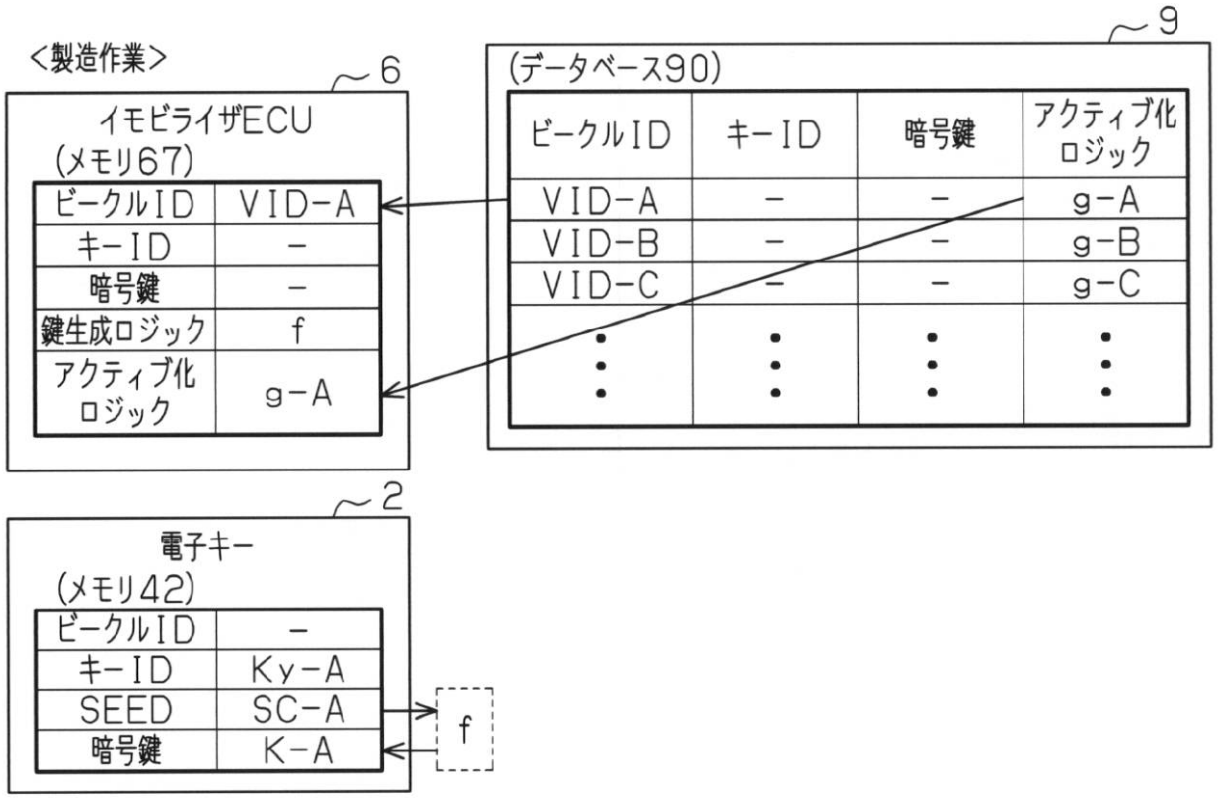
・上記実施形態において、アクティブ化が不可であることを報知する報知手段としては、表示部８３に限らず種々の形態をとることができる。例えば、音による報知でもよいし、光りや振動による報知であってもよい。

【００６５】
・上記実施形態において、電子キー２は、ビークルＩＤの登録後ＳＥＥＤコードを削除してもよい。ＳＥＥＤコードが削除されると、イモビライザＥＣＵ６への登録ができなくなるので、一つの電子キー２が複数のイモビライザＥＣＵ６に登録されることを抑制することができる。
【００６６】
・上記実施形態において、イモビライザＥＣＵ６は、登録作業後に鍵生成ロジックｆ自体を削除してもよい。このようにすれば、イモビライザＥＣＵ６に別の電子キーが登録されることを防ぐことができる。また、鍵生成ロジックｆ自体が外部に漏れることを防ぐことができる。なお、鍵生成ロジックｆを削除せずとも、登録作業後に使用を禁止すれば、イモビライザＥＣＵ６に別の電子キーが登録されることを防ぐことができる。
【００６７】
・上記実施形態では、キーシリンダに電子キー２を挿入するタイプのイモビライザシステム３に本発明を適用したが、車両１から送信される電波によって作られる通信エリアに電子キーが進入することで、自動的に通信が行なわれるタイプの電子キーシステムに適用してもよい。
【００６８】
・上記実施形態では、車両１から駆動電波を受信して起動した電子キー２が無線信号を送信するイモビライザシステム３に本発明を適用したが、電子キー２に設けられたスイッチを操作することにより、車両１に向けて無線信号を送信する、いわゆるワイヤレスシステムに適用してもよい。
【００６９】
・上記実施形態では、車両１の電子キーシステムに本発明を採用したが、住宅等の建物の電子キーシステムに本発明を採用してもよい。
【符号の説明】
【００７０】
１…車両、２…電子キー、３…イモビライザシステム、４…トランスポンダ、５…コイルアンテナ、６…イモビライザＥＣＵ、７…電子キー登録システム、８…登録ツール、９…管理センター、１１…エンジン、１２…エンジンＥＣＵ、１３…車内ＬＡＮ、１４…イグニッションスイッチ（ＩＧＳＷ）、２１…送受信アンテナ、４１…制御部、４２…メモリ、６１…モード切替部、６２…ビークルＩＤ送信部、６４…ＳＥＥＤ読込部、６５…暗号鍵生成部、６７…メモリ、６８…アクティブ化要求信号生成部、６９アクティブ化許可信号読込部、８１…制御部、８２…操作部、８３…表示部、９０…データベース、９１…アクティブ化要求信号読込部、９２…判断部、９３…データ書込部、９４…アクティブ化許可信号生成部。

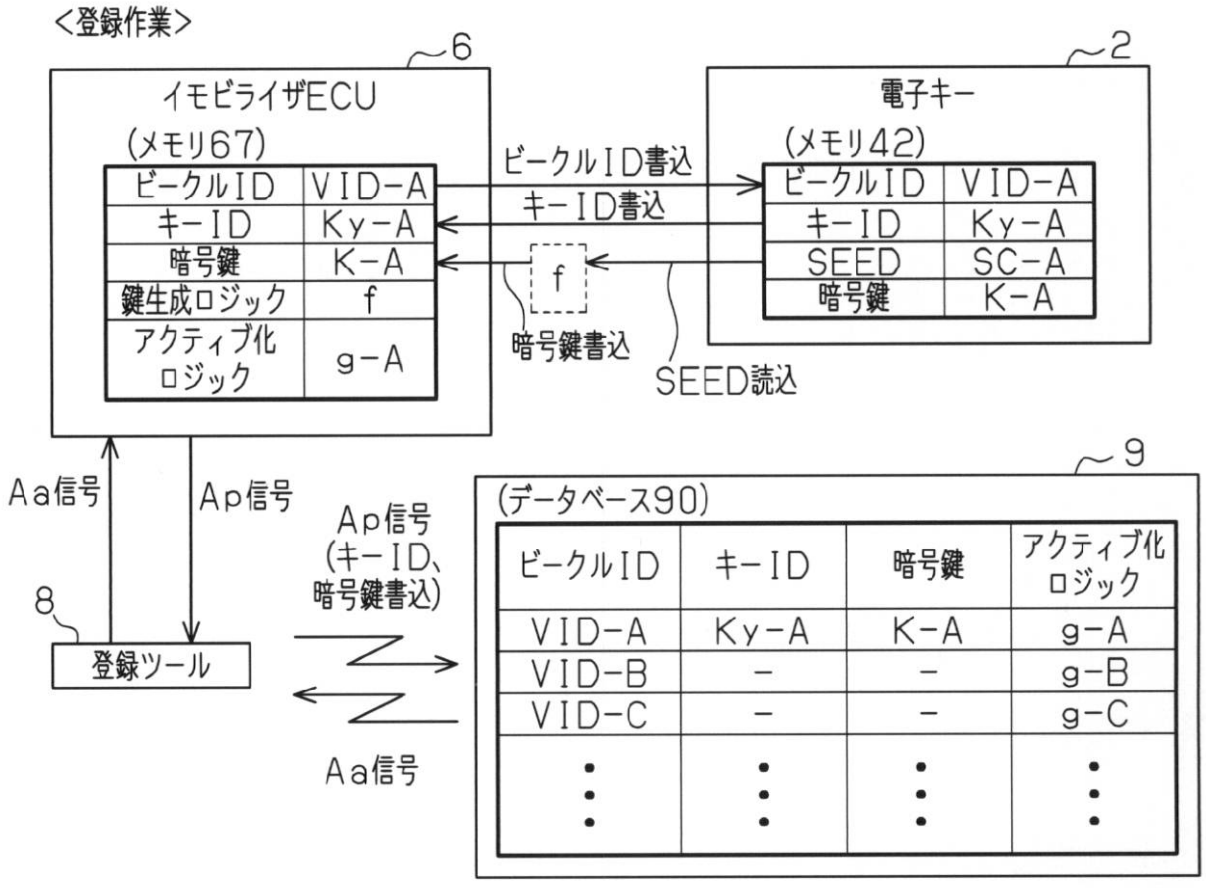
【図１】


1
車両
15
ディスプレイ
6
イモビライザECU
61
モード切替部
62
ビークルID送信部
64
SEED読込部
65
暗号鍵生成部
68
Ad信号生成部
69
Aa信号読込部
67
メモリ
ビークルID
キーID
暗号鍵
鍵生成ロジック
アクティブ化ロジック
5
コイルアンテナ
13
12
エンジンECU
11
エンジン
IGSW
14
7
3
駆動電波
ビークルID信号
キーID要求信号
SEED要求信号
チャレンジ信号
キーID信号
SEED信号
レスポンス信号
2
21
電子キー
4
トランスポンダ
41
制御部
42
メモリ
ビークルID
キーID
SEED
暗号鍵
アクティブ化要求信号
アクティブ化許可信号
8
登録ツール
81
制御部
82
操作部
83
表示部
ネットワーク
90
9
管理センター
データベース
Ad信号読込部
91
判断部
92
データ書込部
93
Aa信号生成部
94
ビークルID
キーID
暗号鍵
アクティブ化ロジック

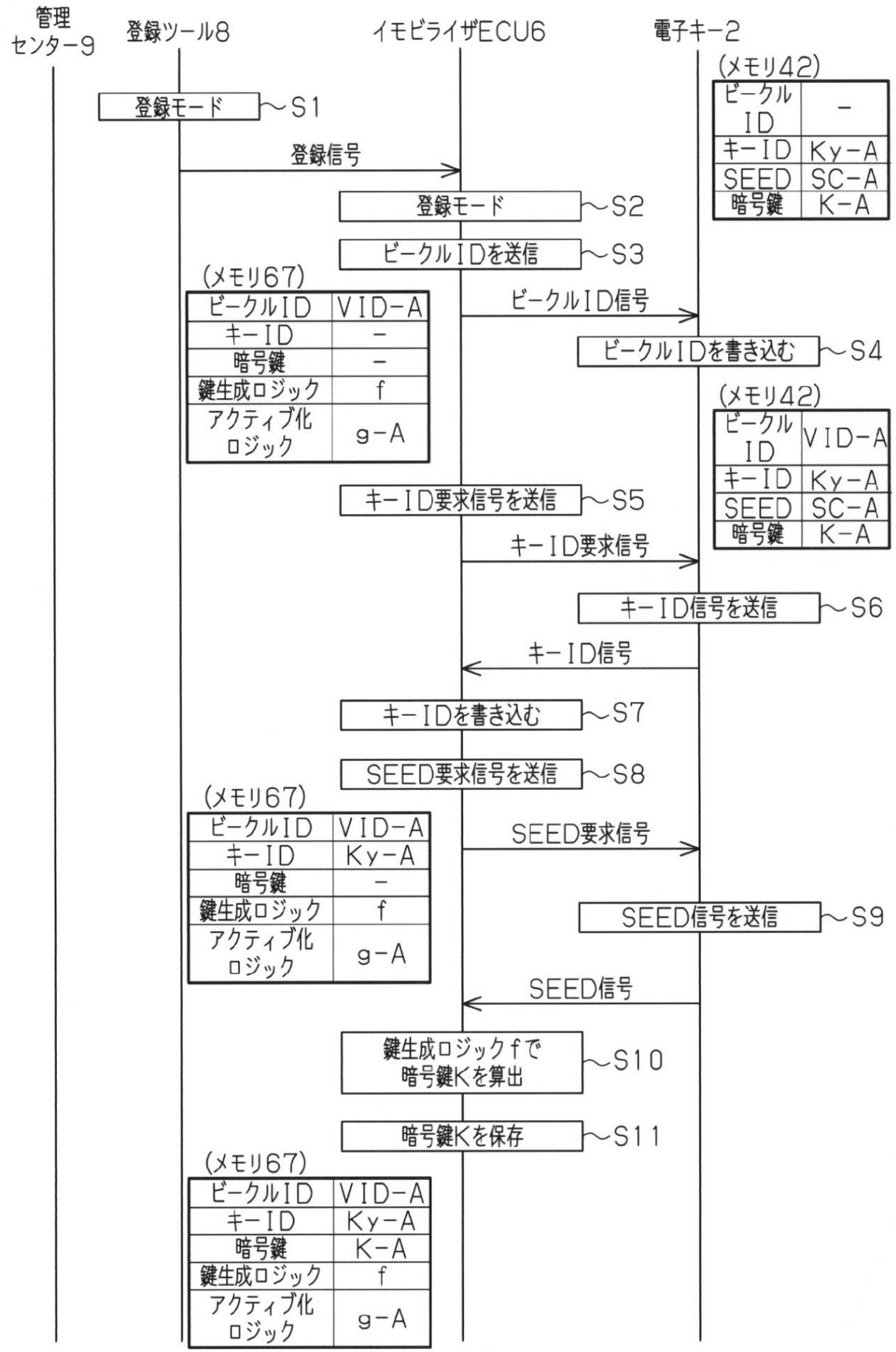
【図２】


<製造作業>
6
イモビライザECU
(メモリ67)
ビークルID VID-A
キーID -
暗号鍵 -
鍵生成ロジック f
アクティブ化ロジック g-A
9
(データベース90)
ビークルID
キーID
暗号鍵
アクティブ化ロジック
VID-A - - g-A
VID-B - - g-B
VID-C - - g-C
2
電子キー
(メモリ42)
ビークルID -
キーID Ky-A
SEED SC-A
暗号鍵 K-A
f

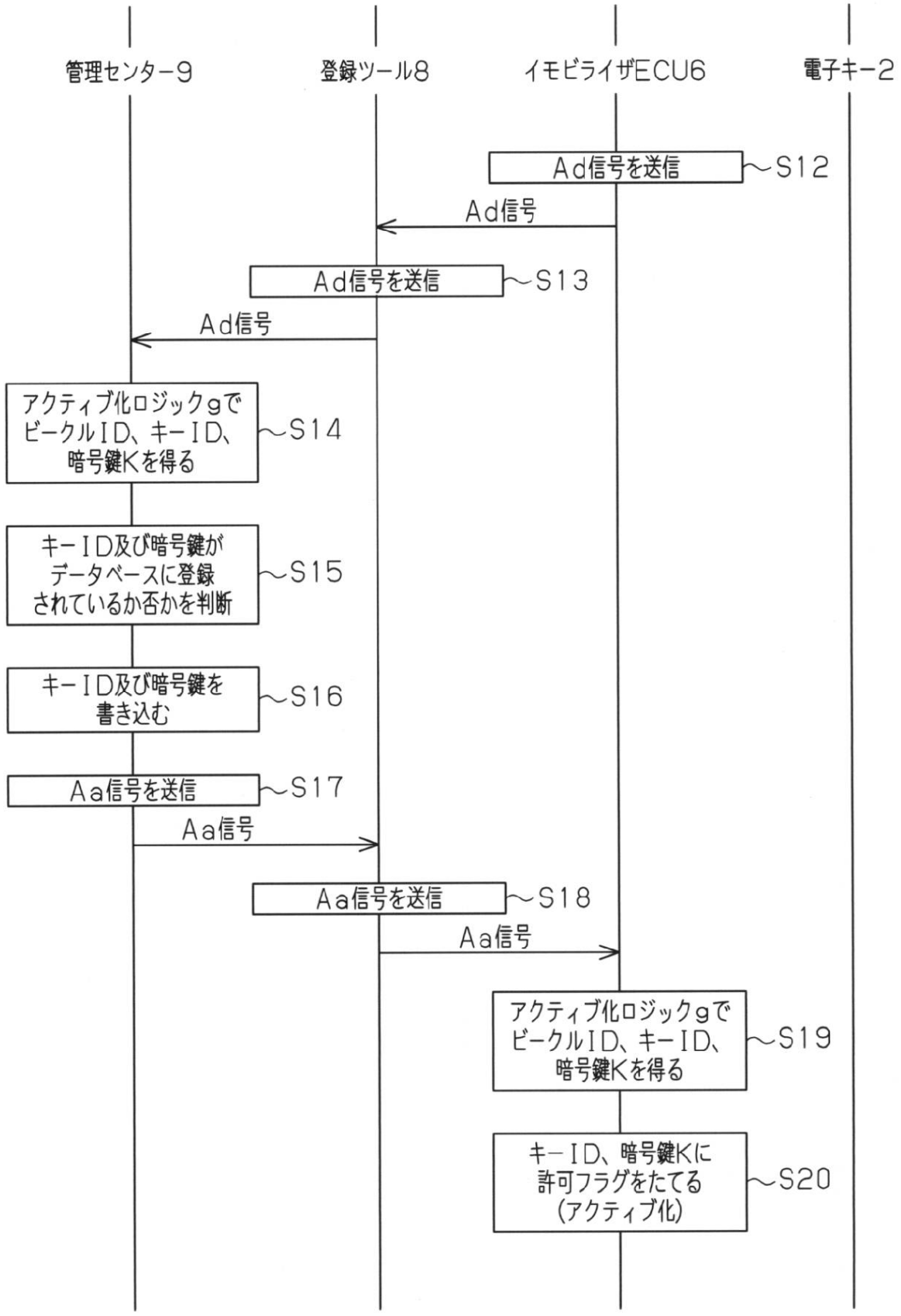
【図３】


<登録作業>
6
イモビライザECU
(メモリ67)
ビークルID VID-A
キーID Ky-A
暗号鍵 K-A
鍵生成ロジック f
アクティブ化ロジック g-A
2
電子キー
(メモリ42)
ビークルID VID-A
キーID Ky-A
SEED SC-A
暗号鍵 K-A
ビークルID書込
キーID書込
f
暗号鍵書込
SEED読込
Aa信号
Ap信号
8
登録ツール
Ap信号
(キーID、暗号鍵書込)
Aa信号
9
(データベース90)
ビークルID
キーID
暗号鍵
アクティブ化ロジック
VID-A Ky-A K-A g-A
VID-B - - g-B
VID-C - - g-C

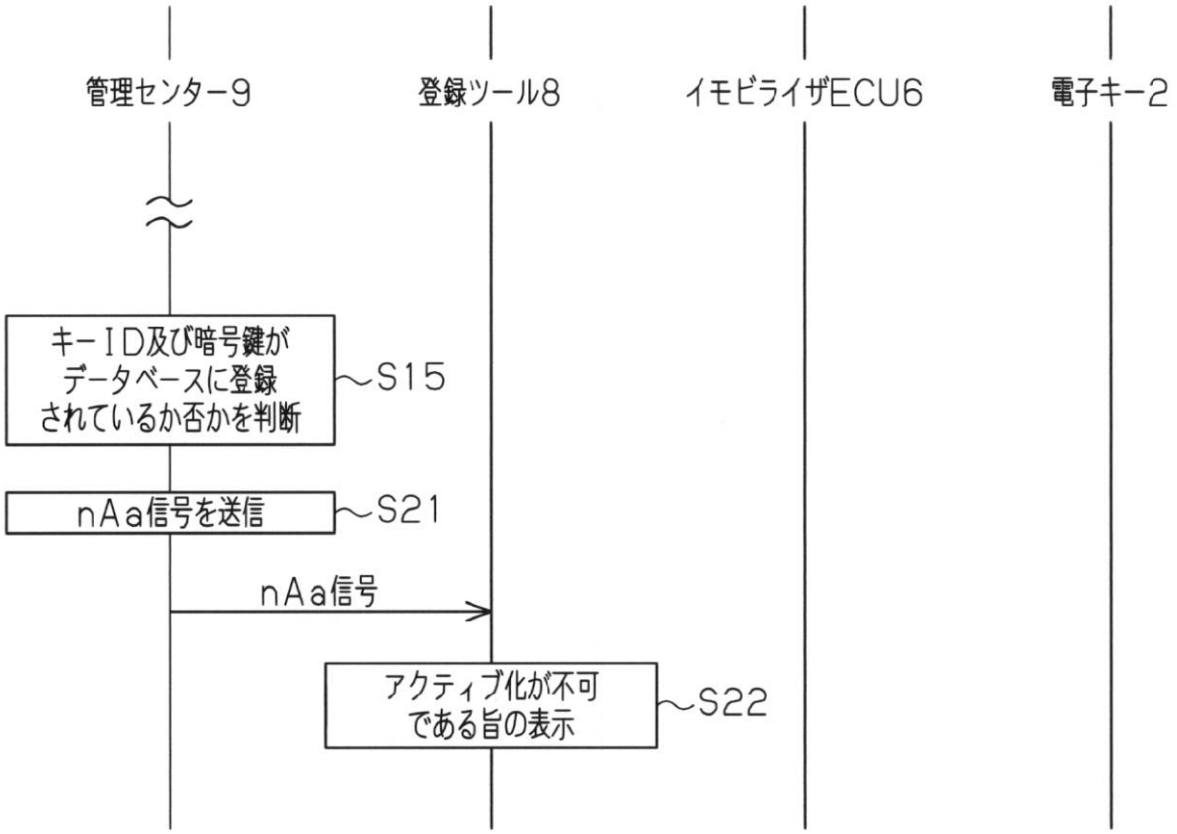
【図４】


管理センター9
登録ツール8
イモビライザECU6
電子キー2
(メモリ42)
ビークルID | －
キーID | Ky-A
SEED | SC-A
暗号鍵 | K-A
登録モード
S1
登録信号
登録モード
S2
ビークルIDを送信
S3
(メモリ67)
ビークルID | VID-A
キーID | －
暗号鍵 | －
鍵生成ロジック | f
アクティブ化ロジック | g-A
ビークルID信号
ビークルIDを書き込む
S4
(メモリ42)
ビークルID | VID-A
キーID | Ky-A
SEED | SC-A
暗号鍵 | K-A
キーID要求信号を送信
S5
キーID要求信号
キーID信号を送信
S6
キーID信号
キーIDを書き込む
S7
SEED要求信号を送信
S8
(メモリ67)
ビークルID | VID-A
キーID | Ky-A
暗号鍵 | －
鍵生成ロジック | f
アクティブ化ロジック | g-A
SEED要求信号
SEED信号を送信
S9
SEED信号
鍵生成ロジックfで暗号鍵Kを算出
S10
暗号鍵Kを保存
S11
(メモリ67)
ビークルID | VID-A
キーID | Ky-A
暗号鍵 | K-A
鍵生成ロジック | f
アクティブ化ロジック | g-A

【図５】


管理センター9
登録ツール8
イモビライザECU6
電子キー2
Ad信号を送信
S12
Ad信号
Ad信号を送信
S13
Ad信号
アクティブ化ロジックgで
ビークルID、キーID、
暗号鍵Kを得る
S14
キーID及び暗号鍵が
データベースに登録
されているか否かを判断
S15
キーID及び暗号鍵を
書き込む
S16
Aa信号を送信
S17
Aa信号
Aa信号を送信
S18
Aa信号
アクティブ化ロジックgで
ビークルID、キーID、
暗号鍵Kを得る
S19
キーID、暗号鍵Kに
許可フラグをたてる
(アクティブ化)
S20

【図６】


管理センター9
登録ツール8
イモビライザECU6
電子キー2
キーID及び暗号鍵が
データベースに登録
されているか否かを判断
S15
nAa信号を送信
S21
nAa信号
アクティブ化が不可
である旨の表示
S22

フロントページの続き

(72)発明者　江川　哲也
愛知県丹羽郡大口町豊田三丁目２６０番地　株式会社東海理化電機製作所内
(72)発明者　岩下　明暁
愛知県丹羽郡大口町豊田三丁目２６０番地　株式会社東海理化電機製作所内
(72)発明者　河村　大輔
愛知県丹羽郡大口町豊田三丁目２６０番地　株式会社東海理化電機製作所内
(72)発明者　林　政樹
愛知県丹羽郡大口町豊田三丁目２６０番地　株式会社東海理化電機製作所内

Ｆターム(参考) 5J104 AA16　EA04　EA15　EA16　JA03　MA05　NA02　NA37