(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2007-255075
(P2007-255075A)
(43)公開日　平成19年10月4日(2007.10.4)

(51)Int.Cl.		F I			テーマコード（参考）
E05B 49/00	(2006.01)	E05B	49/00	J	2E250
H04Q 7/38	(2006.01)	H04B	7/26	109R	5K067
H04B 7/26	(2006.01)	H04B	7/26	M	
B60R 25/00	(2006.01)	B60R	25/00	606	
B60R 25/04	(2006.01)	B60R	25/04	608	

審査請求 未請求　請求項の数 8　ＯＬ　（全 29 頁）

(21)出願番号　特願2006-81260(P2006-81260)
(22)出願日　平成18年3月23日(2006.3.23)

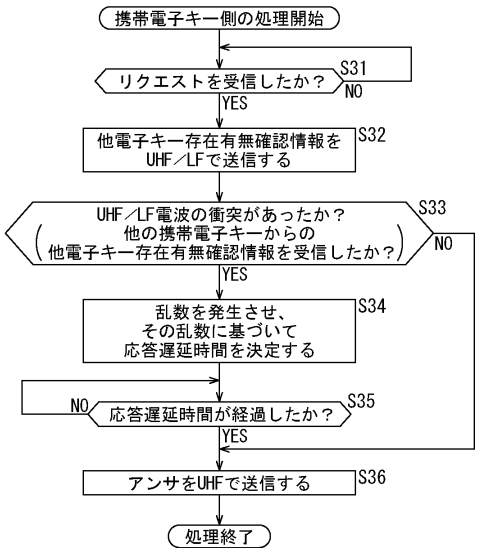
(71)出願人　000002945
オムロン株式会社
京都市下京区塩小路通堀川東入南不動堂町
８０１番地
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　樫山　正人
京都市下京区塩小路通堀川東入南不動堂町
８０１番地　オムロン株式会社内
(72)発明者　植田　雄祐
京都市下京区塩小路通堀川東入南不動堂町
８０１番地　オムロン株式会社内

Ｆターム(参考)　2E250 AA21 BB08 BB43 CC20 FF27
FF35 FF36 HH01 JJ03 KK03
LL00 LL01
5K067 AA32 BB21 EE02 EE16 HH36

(54)【発明の名称】無線通信システムおよび方法、並びに、携帯無線通信装置および方法

(57)【要約】
【課題】正常な認証通信を実現させるようにする。
【解決手段】例えば、携帯電子キーは、ＥＣＵからのリクエストを受信すると、他電子キー存在有無確認情報を送信し（Ｓ３１ＹＥＳ，Ｓ３２）、その受信を試みる。携帯電子キーは、自身からの他電子キー存在有無確認情報以外に、他の携帯電子キーからの他電子キー存在有無確認情報を受信した場合（Ｓ３３ＹＥＳ）、自身を含めて複数の携帯電子キーがＥＣＵの通信圏内に存在すると判断して、次のような処理を実行する。即ち、携帯電子キーは、乱数を発生させ、その乱数に基づいて応答遅延時間を決定し、その応答遅延時間経過後に、アンサをＥＣＵに送信する（Ｓ３４乃至Ｓ３６）。本発明は、車両の盗難防止システムに適用可能である。
【選択図】図１７

図17



【特許請求の範囲】
【請求項１】
複数の携帯無線通信装置のうちの所定の１台が固定無線通信装置により認証される無線通信システムにおいて、
前記固定無線通信装置は、認証を行うためのリクエストを送信し、
前記複数の携帯無線通信装置のうちの前記リクエストを受信した１台以上の携帯無線通信装置のそれぞれは、
前記リクエストを受信した他の携帯無線通信装置の存在有無を確認するための確認情報を送信し、
自身の前記確認情報のみを受信したと判断した場合、前記リクエストに対するアンサを前記固定無線通信装置に送信し、
自身の前記確認情報のみならず、他の携帯無線通信装置からの確認情報も受信したと判断した場合、所定の設定手法に基づいて応答遅延時間を設定し、その応答遅延時間が経過したときに、前記リクエストに対するアンサを前記固定無線通信装置に送信し、
前記固定無線通信装置は、前記リクエストを受信した１台以上の前記携帯無線通信装置のうちの少なくとも１台からの前記アンサを受信した場合、そのアンサを送信した携帯無線通信装置の認証を行う
無線通信システム。
【請求項２】
複数の携帯無線通信装置のうちの所定の１台が固定無線通信装置により認証される無線通信システムの無線通信方法において、
前記固定無線通信装置は、認証を行うためのリクエストを送信し、
前記複数の携帯無線通信装置のうちの前記リクエストを受信した１台以上の携帯無線通信装置のそれぞれは、
前記リクエストを受信した他の携帯無線通信装置の存在有無を確認するための確認情報を送信し、
自身の前記確認情報のみを受信したと判断した場合、前記リクエストに対するアンサを前記固定無線通信装置に送信し、
自身の前記確認情報のみならず、他の携帯無線通信装置からの確認情報も受信したと判断した場合、所定の設定手法に基づいて応答遅延時間を設定し、その応答遅延時間が経過したときに、前記リクエストに対するアンサを前記固定無線通信装置に送信し、
前記固定無線通信装置は、前記リクエストを受信した１台以上の前記携帯無線通信装置のうちの少なくとも１台からの前記アンサを受信した場合、そのアンサを送信した携帯無線通信装置の認証を行う
無線通信方法。
【請求項３】
固定無線通信装置により認証されるＮ台（Ｎは２以上の整数値）の携帯無線通信装置のうちの所定の１台において、
前記固定無線通信装置から送信された、認証を行うためのリクエストを受信する第１の受信手段と、
前記第１の受信手段に受信された前記リクエストに対するアンサを生成する第１の生成手段と、
前記第１の生成手段により生成された前記アンサを前記固定無線通信装置に送信する第１の送信手段と、
前記第１の受信手段に前記リクエストが受信された場合、前記リクエストを受信した他の携帯無線通信装置の存在有無を確認するための確認情報を生成する第２の生成手段と、
前記第２の生成手段により生成された前記確認情報を送信する第２の送信手段と、
前記確認情報を受信する第２の受信手段と、
前記第２の送信手段から送信された前記確認情報のみが前記第２の受信手段に受信されたと判断した場合、前記第１の送信手段から前記アンサを前記固定無線通信装置に送信さ

せ、前記第２の送信手段から送信された前記確認情報のみならず、他の携帯無線通信装置からの確認情報も前記第２の受信手段に受信されたと判断した場合、所定の設定手法に基づいて応答遅延時間を設定し、その応答遅延時間が経過したときに、前記第１の送信手段から前記アンサを前記固定無線通信装置に送信させる制御を行う送信制御手段と
を備える携帯無線通信装置。
【請求項４】
前記送信制御手段は、
前記第２の送信手段から送信された前記確認情報が前記第２の受信手段に正常に受信された場合、前記第２の送信手段から送信された前記確認情報のみが前記第２の受信手段に受信されたと判断し、
それ以外の場合、前記第２の送信手段から送信された前記確認情報のみならず、前記他の携帯無線通信装置からの確認情報も前記第２の受信手段に受信されたと判断する
請求項３に記載の携帯無線通信装置。
【請求項５】
前記固定無線通信装置は、車両に搭載されており、前記リクエストをＬＦ（Low Frequency）で送信し、
複数の前記携帯無線通信装置は、前記車両のドアの施錠解除とエンジン始動許可との少なくとも一方を指示するための携帯電子キーであり、前記アンサをＵＨＦ（Ultra High Frequency）で送信し、
前記第２の送信手段は、前記ＬＦ用の送信回路で構成され、前記確認情報を前記ＬＦで送信し、
前記第２の受信手段と前記第１の受信手段とは、共通の前記ＬＦ用の受信回路で構成され、共通の前記ＬＦ用の受信回路は、前記ＬＦの形態で送信されてくる前記確認情報または前記リクエストを受信し、
前記第１の送信手段は、前記ＵＨＦ用の送信回路で構成され、前記アンサを前記ＵＨＦで送信する
請求項３に記載の携帯無線通信装置。
【請求項６】
前記固定無線通信装置は、車両に搭載されており、前記リクエストをＬＦ（Low Frequency）で送信し、
複数の前記携帯無線通信装置は、前記車両のドアの施錠解除とエンジン始動許可との少なくとも一方を指示するための携帯電子キーであり、前記アンサをＵＨＦ（Ultra High Frequency）で送信し、
前記第１の受信手段は、前記ＬＦ用の受信回路で構成され、前記ＬＦの形態で送信されてくる前記リクエストを受信し、
前記第１の送信手段と前記第２の送信手段は、共通の前記ＵＨＦ用の送信回路で構成され、前記確認情報または前記アンサを前記ＵＨＦで送信し、
前記第２の受信手段は、前記ＵＨＦ用の受信回路で構成され、前記ＵＨＦの形態で送信されてくる前記確認情報を受信する
請求項３に記載の携帯無線通信装置。
【請求項７】
前記第１の生成手段は、前記他の携帯無線通信装置からの確認情報も前記第２の受信手段に受信されたと前記送信制御手段により判断された場合、他の携帯無線通信装置の存在を示す情報を含めた前記アンサを生成する
請求項３に記載の携帯無線通信装置。
【請求項８】
固定無線通信装置により認証される複数の携帯無線通信装置のうちの所定の１台の無線通信方法において、
前記固定無線通信装置から送信された、認証を行うためのリクエストを受信すると、
前記リクエストを受信した他の携帯無線通信装置の存在有無を確認するための確認情報

を送信し、
自身の前記確認情報のみを受信したと判断した場合、前記リクエストに対するアンサを前記固定無線通信装置に送信し、
自身の前記確認情報のみならず、他の携帯無線通信装置からの確認情報も受信したと判断した場合、所定の設定手法に基づいて応答遅延時間を設定し、その応答遅延時間が経過したときに、前記リクエストに対するアンサを前記固定無線通信装置に送信する
ステップを含む無線通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線通信システムおよび方法、並びに、携帯無線通信装置および方法に関し、特に、複数の携帯無線通信装置が固定無線通信装置の通信圏内に存在しても正常な認証通信を実現できる、無線通信システムおよび方法、並びに、携帯無線通信装置および方法に関する。
【背景技術】
【０００２】
従来の車両の盗難防止システムは、車両に搭載されたＥＣＵ（Electronic Control Unit：電子制御装置）と、その車両を運転するユーザが携帯する携帯電子キーとから構成されている（例えば特許文献１や２参照）。
【０００３】
この場合、ＥＣＵは、携帯電子キーと認証通信を行い、その認証に成功すると、車両のドアの施錠解除やエンジン始動のために必要な処理を実行する。
【特許文献１】特開２００３－２０８３５号公報
【特許文献２】特開平０９－２７９９１７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、近年、予備用または複数ユーザ用として、１台の車両（ＥＣＵ）に対して複数の携帯電子キーが配布される場合がある。このような場合、複数の携帯電子キーがＥＣＵの通信圏内に存在するとき、例えば一人のユーザが複数の携帯電子キーを所持したまま車両に近づいたときや、例えば携帯電子キーを１つずつ所持する複数のユーザが同時に車両に近づいたようなときには、次のような問題が発生する。
【０００５】
即ち、ＥＣＵと携帯電子キーとの間での認証通信においては、ＥＣＵのリクエストに対する携帯電子キーのアンサとして、所定の送信フレームが送信される。従って、複数の携帯電子キーがＥＣＵの通信圏内に存在するときには、複数の携帯電子キーからの各送信フレームがＥＣＵにおいて電波衝突を起こすことになる。その結果、正常な認証通信が行えない、即ち、正常な通信が確立できない、という問題が発生する。
【０００６】
このような問題は、車両の盗難防止システムのみならず、複数の携帯無線通信装置のうちの所定の１台が固定無線通信装置により認証される無線通信システム全体において発生し得る。
【０００７】
本発明は、このような状況に鑑みてなされたものであり、複数の携帯無線通信装置が固定無線通信装置の通信圏内に存在しても、正常な認証通信を実現させるようにするものである。
【課題を解決するための手段】
【０００８】
本発明の一側面の無線通信システムおよび方法は、複数の携帯無線通信装置のうちの所定の１台が固定無線通信装置により認証される無線通信システムおよび方法であって、前

記固定無線通信装置は、認証を行うためのリクエストを送信し、前記複数の携帯無線通信装置のうちの前記リクエストを受信した１台以上の携帯無線通信装置のそれぞれは、前記リクエストを受信した他の携帯無線通信装置の存在有無を確認するための確認情報を送信し、自身の前記確認情報のみを受信したと判断した場合、前記リクエストに対するアンサを前記固定無線通信装置に送信し、自身の前記確認情報のみならず、他の携帯無線通信装置からの確認情報も受信したと判断した場合、所定の設定手法に基づいて応答遅延時間を設定し、その応答遅延時間が経過したときに、前記リクエストに対するアンサを前記固定無線通信装置に送信し、前記固定無線通信装置は、前記リクエストを受信した１台以上の前記携帯無線通信装置のうちの少なくとも１台からの前記アンサを受信した場合、そのアンサを送信した携帯無線通信装置の認証を行う。

【０００９】

固定無線通信装置は、例えば車両に搭載されたＥＣＵにより構成される。携帯無線通信装置は、例えば車両を運転するユーザが携帯する携帯電子キーにより構成される。

【００１０】

これにより、固定無線通信装置の通信圏内に複数の携帯無線通信装置が存在しても、複数の携帯無線通信装置同士がそのことを認識し、各アンサの送信タイミングをずらすようにしたので、電波衝突が固定無線通信装置で発生しなくなり、その結果、正常な認証通信が実現される。

【００１１】

本発明の一側面の携帯無線通信装置は、固定無線通信装置により認証されるＮ台（Ｎは２以上の整数値）の携帯無線通信装置のうちの所定の１台であって、前記固定無線通信装置から送信された、認証を行うためのリクエストを受信する第１の受信手段と、前記第１の受信手段に受信された前記リクエストに対するアンサを生成する第１の生成手段と、前記第１の生成手段により生成された前記アンサを前記固定無線通信装置に送信する第１の送信手段と、前記第１の受信手段に前記リクエストが受信された場合、前記リクエストを受信した他の携帯無線通信装置の存在有無を確認するための確認情報を生成する第２の生成手段と、前記第２の生成手段により生成された前記確認情報を送信する第２の送信手段と、前記確認情報を受信する第２の受信手段と、前記第２の送信手段から送信された前記確認情報のみが前記第２の受信手段に受信されたと判断した場合、前記第１の送信手段から前記アンサを前記固定無線通信装置に送信させ、前記第２の送信手段から送信された前記確認情報のみならず、他の携帯無線通信装置からの確認情報も前記第２の受信手段に受信されたと判断した場合、所定の設定手法に基づいて応答遅延時間を設定し、その応答遅延時間が経過したときに、前記第１の送信手段から前記アンサを前記固定無線通信装置に送信させる制御を行う送信制御手段とを備える。

【００１２】

固定無線通信装置は、例えば車両に搭載されたＥＣＵにより構成される。携帯無線通信装置は、例えば車両を運転するユーザが携帯する携帯電子キーにより構成される。

【００１３】

第１の受信手段は、例えばＬＦ用の受信回路で構成される。第１の送信手段は、例えばＵＨＦ用の送信回路で構成される。前記第２の受信手段は、例えばＬＦ用の受信回路で構成される。第２の送信手段は、例えばＵＨＦ用またはＬＦ用の送信回路で構成される。第２の受信手段は、例えばＵＨＦ用またはＬＦ用の受信回路で構成される。第１の生成手段、第２の生成手段、および、送信制御手段は、信号処理を行う回路や、ソフトウエアとしての信号処理を実行するコンピュータ等で構成される。

【００１４】

これにより、固定無線通信装置の通信圏内に複数の携帯無線通信装置が存在しても、複数の携帯無線通信装置同士がそのことを認識し、各アンサの送信タイミングをずらすようにしたので、電波衝突が固定無線通信装置で発生しなくなり、その結果、正常な認証通信が実現される。

【００１５】

前記送信制御手段は、前記第２の送信手段から送信された前記確認情報が前記第２の受信手段に正常に受信された場合、前記第２の送信手段から送信された前記確認情報のみが前記第２の受信手段に受信されたと判断し、それ以外の場合、前記第２の送信手段から送信された前記確認情報のみならず、前記他の携帯無線通信装置からの確認情報も前記第２の受信手段に受信されたと判断することができる。

【００１６】

これにより、送信制御手段を簡素に構成できる。即ち、送信制御手段が回路で構成されている場合には、その回路規模を縮小できる。また、ソフトウエアを実行するコンピュータで探知手段が構成されている場合には、そのソフトウエアの規模を縮小できる。

【００１７】

前記固定無線通信装置は、車両に搭載されており、前記リクエストをＬＦ（Low Frequency）で送信し、複数の前記携帯無線通信装置は、前記車両のドアの施錠解除とエンジン始動許可との少なくとも一方を指示するための携帯電子キーであり、前記アンサをＵＨＦ（Ultra High Frequency）で送信し、前記第２の送信手段は、前記ＬＦ用の送信回路で構成され、前記確認情報を前記ＬＦで送信し、前記第２の受信手段と前記第１の受信手段とは、共通の前記ＬＦ用の受信回路で構成され、共通の前記ＬＦ用の受信回路は、前記ＬＦの形態で送信されてくる前記確認情報または前記リクエストを受信し、前記第１の送信手段は、前記ＵＨＦ用の送信回路で構成され、前記アンサを前記ＵＨＦで送信することができる。

【００１８】

これにより、確認情報を受信するための受信回路を新たに設ける必要がなくなる。

【００１９】

前記固定無線通信装置は、車両に搭載されており、前記リクエストをＬＦ（Low Frequency）で送信し、複数の前記携帯無線通信装置は、前記車両のドアの施錠解除とエンジン始動許可との少なくとも一方を指示するための携帯電子キーであり、前記アンサをＵＨＦ（Ultra High Frequency）で送信し、前記第１の受信手段は、前記ＬＦ用の受信回路で構成され、前記ＬＦの形態で送信されてくる前記リクエストを受信し、前記第１の送信手段と前記第２の送信手段は、共通の前記ＵＨＦ用の送信回路で構成され、前記確認情報または前記アンサを前記ＵＨＦで送信し、前記第２の受信手段は、前記ＵＨＦ用の受信回路で構成され、前記ＵＨＦの形態で送信されてくる前記確認情報を受信することができる。

【００２０】

これにより、認証通信が終了されるまでの処理時間を短縮でき、システム全体の応答を早くすることができる。

【００２１】

前記第１の生成手段は、前記他の携帯無線通信装置からの確認情報も前記第２の受信手段に受信されたと前記送信制御手段により判断された場合、他の携帯無線通信装置の存在を示す情報を含めた前記アンサを生成することができる。

【００２２】

これにより、かかるアンサを受信した固定無線通信装置側でも、その通信圏内に複数の携帯無線通信装置が存在することを容易に認識できるようになる。

【００２３】

本発明の一側面の無線通信方法は、固定無線通信装置により認証される複数の携帯無線通信装置のうちの所定の１台の無線通信方法であって、前記固定無線通信装置から送信された、認証を行うためのリクエストを受信すると、前記リクエストを受信した他の携帯無線通信装置の存在有無を確認するための確認情報を送信し、自身の前記確認情報のみを受信したと判断した場合、前記リクエストに対するアンサを前記固定無線通信装置に送信し、自身の前記確認情報のみならず、他の携帯無線通信装置からの確認情報も受信したと判断した場合、所定の設定手法に基づいて応答遅延時間を設定し、その応答遅延時間が経過したときに、前記リクエストに対するアンサを前記固定無線通信装置に送信する。

【００２４】

これにより、固定無線通信装置の通信圏内に複数の携帯無線通信装置が存在しても、複数の携帯無線通信装置同士がそのことを認識し、各アンサの送信タイミングをずらすようにしたので、電波衝突が固定無線通信装置で発生しなくなり、その結果、正常な認証通信が実現される。

【００２５】

上記において、アンサと確認情報とが同じであっても構わない。この場合には、第１の生成手段と第２の生成手段が同じであっても良く、第１の送信手段と第２の送信手段が同じであっても良く、さらには第１の受信手段と第２の受信手段が同じであっても良い。リクエストを受信した後に送信されたアンサが、そのアンサの送信を行った携帯電子キーによって正常に受信できなかった場合には、所定の設定方法によって設定された応答遅延時間の経過後に2回目のアンサを送信するような構成としても良い。

【発明の効果】

【００２６】

以上のごとく、本発明によれば、複数の携帯無線通信装置のうちの所定の１台が固定無線通信装置により認証される無線通信システムを実現できる。特に、かかる無線通信システムにおいて、複数の携帯無線通信装置が固定無線通信装置の通信圏内に存在しても、正常な認証通信が実現できる。

【００２７】

また、最初の認証通信においてはどの携帯電子キーとの通信を優先するかは定めていないため、通信圏内に携帯電子キーが１台しか存在しない場合には、最初の通信で認証ができるので、時間を短くすることができる。即ち、認証のための時間を短くできると共に正常に認証通信ができる。

【発明を実施するための最良の形態】

【００２８】

図１は、本発明が適用される無線通信システムの一実施の形態としての車両盗難防止システムの構成例を示している。

【００２９】

図１の例では、車両盗難防止システムは、車両１に固定無線通信装置として搭載されたＥＣＵ１１と、携帯無線通信装置としてのＮ個（Ｎは２以上の整数値）の携帯電子キー２－１乃至２－Ｎとから構成されている。

【００３０】

なお、以下、携帯電子キー２－１乃至２－Ｎのそれぞれを個々に区別する必要がない場合、それらをまとめて携帯電子キー２と称する。また、携帯電子キー２の数量は、一般的に「台」を用いないが、携帯電子キー２は携帯無線通信装置の一実施の形態であることを強調するため、本明細書では「台」を用いるとする。

【００３１】

ＥＣＵ１１は、携帯電子キー２－１乃至２－Ｎのうちの１台と認証通信を行い、その認証に成功したとき、車両１のドアの解錠やエンジン始動のために必要な処理（以下、ドアのアンロック処理等と称する）を実行する。

【００３２】

しかしながら、上述したように、携帯電子キー２－１乃至２－Ｎのうちの２台以上がＥＣＵ１１の通信圏内に存在する場合、その２台以上の携帯電子キー２から送信フレームがＥＣＵ１１に対してそれぞれほぼ同時に送信されてくる。その結果、それらの送信フレームがＥＣＵ１１において衝突してしまい、認証通信ができなくなってしまう、即ち、正常な通信が確立できなくなってしまうという問題が発生する。

【００３３】

そこで、本発明人は、この問題を解決可能な２つの手法を発明した。以下、この２つの手法を区別するためそれぞれ、データ衝突検知方式、および、事前調停方式と称する。なお、各方式の呼称の由来については、後述する各方式の詳細を説明していくことで明らかになると思われるため、ここでは説明を省略する。

【００３４】
なお、本発明で用いている語句「リクエスト」とは、固定無線通信装置（本実施の形態ではＥＣＵ１１）から送信される無線信号であって、通信圏内に存在する携帯無線通信装置（本実施の形態では携帯電子キー２）がこの「リクエスト」を受信したことに基づいて、携帯無線通信装置が信号を送信するようにさせる機能を有する無線信号である。また、語句「アンサ」とは、前記「リクエスト」を受信したことに基づいて、携帯無線通信装置から送信される無線信号である。「アンサ」の機能は、単に受信した事を示す機能であっても良いし、固定無線通信装置に対して何らかの動作を要求または実施させるものでも良い。「アンサ」には、各無線通信装置のID、携帯無線通信装置の位置情報、車両や固定無線通信装置に対する動作を求めるコードなどが含まれても良い。
【００３５】
（データ衝突検知方式）
【００３６】
はじめに、図２乃至図１３を参照して、データ衝突検知方式について説明する。
【００３７】
なお、以下の説明では、説明の簡略上、携帯電子キー２－１乃至２－Ｎのうちの２台、例えば携帯電子キー２－１，２－３がＥＣＵ１１の通信圏内に存在する場合を例として、それらの動作を説明していく。ただし、携帯電子キー２－１乃至２－Ｎのうちの任意の２台以上がＥＣＵ１１の通信圏内に存在する場合の動作も、基本的に以下の動作と同様になる。
【００３８】
例えば図２に示されるように、ＥＣＵ１１は、認証を行うためのリクエストＬＦ１を、ＬＦ（Low Frequency）の形態で定期的に送信している。
【００３９】
この場合、ＥＣＵ１１の通信圏内に存在する携帯電子キー２－１，２－３のそれぞれは、リクエストＬＦ１を受信すると、例えば図３に示されるように、各アンサＵＨＦ１－１，ＵＨＦ１－３のそれぞれを、ＵＨＦ（Ultra High Frequency）の形態でＥＣＵ１１に対して送信する。
【００４０】
すると、図３に示されるように、ＥＣＵ１１において、アンサＵＨＦ１－１，１－３の電波衝突が発生することになる。
【００４１】
そこで、このような電波衝突をＥＣＵ１１側で検知できるように、データ衝突検知方式では、ＥＣＵ１１からのリクエストに対するアンサは、別の携帯電子キー２のアンサと混合した場合に自身の識別が可能な構成を有している。この場合、ＥＣＵ１１は、各携帯電子キー２の各アンサの各構成を予め把握しておくことで、電波衝突が発生したこと、即ち、アンサが混合されていることを判定でき、混合であると判定した場合には、所定の方法によって優先付けされた携帯電子キー２の１台１台に対して個別通信を行い、その個別通信の結果に基づいてその所定の１台の認証を行うことが可能になる。或いは、ＥＣＵ１１は、混合であると判定した場合には、混合された受信信号からアンサを送信してきた複数の携帯電子キー２を特定し、所定の方法によって優先付けされた携帯電子キー２の１台１台に対して個別通信を行い、その個別通信の結果に基づいてその所定の１台の認証を行うことが可能になる。
【００４２】
即ち、データ衝突検知方式で使用される携帯電子キー２のアンサは、別の携帯電子キー２のアンサと混合した場合に自身の識別が可能な構成を有していれば、任意の構成で構わない。ただし、本実施の形態のアンサを構成する送信フレームとしては、図４に示されるようなフレーム２１が採用されている。
【００４３】
フレーム２１は、電波衝突をＥＣＵ１１側に検出させるためのビット列３１と、自身を

アンサとして利用する携帯電子キー２のＩＤ（Identification）とを含むように構成されている。なお、以下、フレーム２１を特に衝突検知フレーム２１と称する。また、この呼称に伴い、ビット列３１を特に衝突検知ビット列３１と称する。

【００４４】

Ｎ台の携帯電子キー２－１乃至２－Ｎが存在する場合、ひとつの携帯電子キー２についての衝突検知フレーム２１の衝突検知ビット列３１は、Ｎビットで構成される。この場合、Ｎビットのうちの、所定の１ビットのみが“１”となり、他のビットは皆“０”となるように定義されている。ただし、１台の携帯電子キー２についての“１”となるビットは、その他の全ての携帯電子キー２についての“１”となるビットの全てと重複されないように定義される。

【００４５】

具体的には例えばＮ＝４である場合、即ち、４台の携帯電子キー２－１乃至２－４が存在する場合、図５に示されるように、携帯電子キー２－１についての衝突検知フレーム２１－１は、「０００１」と定義された衝突検知ビット列３１－１と、携帯電子キー２－１のＩＤ１とを含むように構成される。

【００４６】

携帯電子キー２－２についての衝突検知フレーム２１－２は、「００１０」と定義された衝突検知ビット列３１－２と、携帯電子キー２－２のＩＤ２とを含むように構成される。

【００４７】

携帯電子キー２－３についての衝突検知フレーム２１－３は、「０１００」と定義された衝突検知ビット列３１－３と、携帯電子キー２－３のＩＤ３とを含むように構成される。

【００４８】

携帯電子キー２－４についての衝突検知フレーム２１－４は、「１０００」と定義された衝突検知ビット列３１－４と、携帯電子キー２－４のＩＤ４とを含むように構成される。

【００４９】

この場合、携帯電子キー２－１乃至２－４のうちの１台のみがＥＣＵ１１の通信圏内に存在するときには、ＥＣＵ１１は、リクエスト（図２の例ではリクエストＬＦ１）に対するアンサとして、衝突検知フレーム２１－１乃至２１－４のうちの１つのみを受信することになる。その際、衝突検知フレーム２１－１乃至２１－４のうちの何れがＥＣＵ１１において受信されても、衝突検知ビット列３１を構成する４ビットのうちの１ビットのみが“１”となる。即ち、ＥＣＵ１１は、受信された衝突検知ビット列３１を構成する４ビットのうちの１ビットのみが“１”であることを確認することで、電波衝突は発生していないと認定することができる。

【００５０】

これに対して、上述した図３に示されるように、２台の携帯電子キー２－１，２－３がＥＣＵ１１の通信圏内に存在するときには、図６に示されるように、携帯電子キー２－１，２－３のそれぞれは、リクエストに対するアンサとして、衝突検知フレーム２１－１，２１－３のそれぞれをほぼ同時に送信することになる。その結果、図３を用いて上述したように、ＥＣＵ１１において衝突検知フレーム２１－１，２１－３は電波衝突を起こすので、ＥＣＵ１１にとっては、図６のフレーム４１をアンサとして受信することになる。

【００５１】

以下、ＥＣＵ１１にアンサとして受信されたフレームを、受信衝突検知フレームと称する。即ち、図６の例では、フレーム４１が、受信衝突検知フレームとなる。

【００５２】

この場合、受信衝突検知フレーム４１のうちの、衝突検知フレーム２１の衝突検知ビット列３１の配置位置に対応する位置のビット列４２（以下、受信衝突検知ビット列４２と称する）を構成する４ビットのうちの２ビットが“１”となる。

【００５３】
具体的には例えば、衝突検知フレーム２１－１，２１－３のそれぞれが、携帯電子キー２－１，２－３のそれぞれによりＡＳＫ（Amplitude Shift Keying）方式で変調されて、アンサＵＨＦ１－１，１－３のそれぞれとして送信されたとする。
【００５４】
なお、リクエストＬＦ１を携帯電子キー２－１，２－３が受信するまでの時間の違い、即ち、距離の違いは無視できるように、信号処理されるとする。また、携帯電子キー２－１，２－３がリクエストＬＦ１を受信してから、アンサＵＨＦ１－１，１－３を返信するまでの時間は設計的には同一であるので、同一であるとする。
【００５５】
このような前提の下では、衝突検知フレーム２１－１の衝突検知ビット列３１－１と、衝突検知フレーム２１－２の衝突検知ビット列３１－２とのそれぞれの変調信号は、それぞれ図７の一番上と中央とのそれぞれに示される信号になる。従って、電波衝突によりこれらの変調信号が合成され、その結果、図７の一番下に示される変調信号がＥＣＵ１１に受信される。従って、ＥＣＵ１１は、この変調信号を復調することで、図６に示される受信衝突検知ビット列４２、即ち、「０１０１」を検出する。
【００５６】
このようにして、ＥＣＵ１１は、受信衝突検知ビット列４２を構成する４ビットのうちの２ビットが“１”であることを確認することで、電波衝突が発生していると認定することができる。
【００５７】
図示はしないが、同様に、携帯電子キー２－１乃至２－４のうちの任意の２台がＥＣＵ１１の通信圏内に存在する場合には、受信衝突検知ビット列を構成する４ビットのうちの２ビットが“１”となる。また、携帯電子キー２－１乃至２－４のうちの任意の３台がＥＣＵ１１の通信圏内に存在する場合には、受信衝突検知ビット列を構成する４ビットのうちの３ビットが“１”となる。さらにまた、携帯電子キー２－１乃至２－４の４台全てがＥＣＵ１１の通信圏内に存在する場合には、受信衝突検知ビット列を構成する４ビットの全てが“１”となる。
【００５８】
即ち、携帯電子キー２－１乃至２－Ｎのうちの任意のＫ台（Ｋは１乃至Ｎのうちの何れかの整数値）がＥＣＵ１１の通信圏内に存在する場合には、受信衝突検知ビット列を構成するＮビットのうちのＫビットが“１”となる。
【００５９】
従って、ＥＣＵ１１は、受信衝突検知ビット列を構成するＮビットのうちの２ビット以上が“１”であることを確認することで、電波衝突が発生していると認定することができる。
【００６０】
さらに、ＥＣＵ１１は、携帯電子キー２－１乃至２－Ｎのそれぞれについての衝突検知ビット列３１－１乃至３１－Ｎの各構成を予め把握していれば、即ち、それぞれの“１”となるビットの各位置を予め把握していれば、受信衝突検知ビット列における“１”の位置を確認することで、携帯電子キー２－１乃至２－Ｎのうちの何れがその通信圏内に存在するのかを認識することができる。そして、ＥＣＵ１１は、通信圏内に存在すると認識した１以上の携帯電子キー２を、認証通信を行うべき候補（以下、認証候補）としてそれぞれ特定できる。
【００６１】
具体的には例えば、図６の例では、ＥＣＵ１１は、受信衝突検知ビット列４２である「０１０１」のうちの先頭から２ビット目の“１”を検出することで、携帯電子キー２－３を認証候補として特定できる。同様に、ＥＣＵ１１は、この「０１０１」のうちの先頭から４ビット目の“１”を検出することで、携帯電子キー２－１を認証候補として特定できる。

【００６２】
その後、ＥＣＵ１１は、認証候補として特定された携帯電子キー２－１，２－３の中から所定の１台を認証相手として決定し、その認証相手と個別通信することでその認証を行うことができる。
【００６３】
この場合、認証候補の中から認証相手を決定する決定手法は特に限定されないが、例えば本実施の形態では、携帯電子キー２－１乃至２－Ｎのそれぞれには優先順位が予め決められており、その優先順位に従って認証相手が決定する、という手法が採用されているとする。
【００６４】
具体的には例えば、携帯電子キー２－１乃至２－Ｎの順番で優先順位が決定されているとする。この場合、ＥＣＵ１１は、認証候補である携帯電子キー２－１，２－３のうちの優先順位の高い方、即ち本実施の形態では携帯電子キー２－１を認証相手として決定する。そして、ＥＣＵ１１は、例えば図８に示されるように、携帯電子キー２－１との認証通信を行う。
【００６５】
即ち、ＥＣＵ１１は、携帯電子キー２－１を個別に認証するためのリクエスト（以下、このようなリクエストを特に個別リクエストと称する）ＬＦ２－１を、携帯電子キー２－１に対して送信する。即ち、個別リクエストＬＦ２－１は、携帯電子キー２－１のみが応答するように設定されている。換言すると、個別リクエストを構成するフレームは、認証相手のみが応答するように設定されていれば、その形態は特に限定されない。具体的には例えば、ここでは、個別リクエストＬＦ２－１は、携帯電子キー２－１のみが応答すればよいので、携帯電子キー２－１についての図５の衝突検知フレーム２１－１と等価なフレームを採用することができる。
【００６６】
この場合、携帯電子キー２－１は、個別リクエストＬＦ２－１に対するアンサＵＨＦ２－１を、ＥＣＵ１１に対して送信する。このとき、携帯電子キー２－３は、上述したように、個別リクエストＬＦ２－１を受信しても応答しない。
【００６７】
ＥＣＵ１１は、アンサＵＨＦ２－１を受信した場合、携帯電子キー２－１の認証に成功したとして、ドアのアンロック処理等を実行する。
【００６８】
これに対して、例えば図９に示されるように、携帯電子キー２－１からのアンサＵＨＦ２－１を受信できなかった場合、ＥＣＵ１１は、携帯電子キー２－１の認証に失敗したとして、次の優先順位の携帯電子キー２－３を認証相手として決定し、例えば同図に示されるように、携帯電子キー２－３との認証通信を行う。
【００６９】
即ち、ＥＣＵ１１は、個別リクエストＬＦ２－３を、携帯電子キー２－３に対して送信する。即ち、個別リクエストＬＦ２－３は、携帯電子キー２－３のみが応答するように設定されている。具体的には例えば、上述した図８の例とあわせるならば、個別リクエストＬＦ２－３は、携帯電子キー２－３についての図５の衝突検知フレーム２１－３と等価なフレームを採用することができる。
【００７０】
この場合、携帯電子キー２－３は、個別リクエストＬＦ２－３に対するアンサＵＨＦ２－３を、ＥＣＵ１１に対して送信する。このとき、携帯電子キー２－１は、上述したように、個別リクエストＬＦ２－３を受信しても応答しない。
【００７１】
ＥＣＵ１１は、個別リクエストＵＨＦ２－３を受信すると、携帯電子キー２－３の認証に成功したとして、ドアのアンロック処理等を実行する。
【００７２】

なお、図示はしないが、ＥＣＵ１１は、アンサＵＨＦ２－３を仮に受信できなかった場合、即ち、通信圏内に存在する携帯電子キー２－１，２－３からのアンサＵＨＦ２－１，２－３を仮に何れも受信できなかった場合、ドアのアンロック処理等の実行を禁止する。

【００７３】

このように、本実施の形態では、優先順位が高い順に個別通信による認証通信を行うようにしたので、優先順位の高い携帯電子キー２をユーザが所持することで、それだけ認証通信の処理時間を短縮させることができる。

【００７４】

また、所定の携帯電子キー２との認証通信に失敗した場合、さらに、次の優先順位の他の携帯電子キー２との認証通信を試みるようにしたので、より一段と確実な認証通信が実現される。

【００７５】

以上説明したデータ衝突検知方式を採用した車両盗難防止システムがアンロック処理等を実行するまでの一連の処理は、例えば、図１０と図１１とに示されるフローチャートに従って実行される。即ち、図１０は、ＥＣＵ１１側の処理例を説明するフローチャートであり、図１１は、１台の携帯電子キー２の処理例を説明するフローチャートである。

【００７６】

図１０のステップＳ１において、ＥＣＵ１１は、リクエストをＬＦで送信する。

【００７７】

ステップＳ２において、ＥＣＵ１１は、アンサとしてのＵＨＦを受信したか否かを判定する。

【００７８】

携帯電子キー２－１乃至２－Ｎの何れもがＥＣＵ１１の通信圏外に存在する場合、ステップＳ２においてＮＯであると判定されて、処理はステップＳ１に戻されそれ以降の処理が繰り返される。即ち、携帯電子キー２－１乃至２－Ｎのうちの少なくとも１台がＥＣＵ１１の通信圏内に進入してくるまで、ＥＣＵ１１は、リクエストとしてのＬＦを定期的に送信している。あるいは携帯電子キー２の所有者が車両１に接近した事を検知した場合、ＥＣＵ１１は、リクエストとしてのＬＦを送信するようにしても良い。

【００７９】

その後、携帯電子キー２－１乃至２－Ｎのうちの少なくとも１台がＥＣＵ１１の通信圏内に進入してきた場合、アンサとしてのＵＨＦを送信してくることになるので（後述する図１１のステップＳ１２参照）、即ち、上述した衝突検知フレームを送信してくることになるので、ＥＣＵ１１は、それらの混合信号（ただし、携帯電子キー２が１台のみ存在する場合にはその衝突検知フレーム自体）を受信衝突検知フレームとして受信することになる。これにより、ステップＳ２においてＹＥＳであると判定されて、処理はステップＳ３に進む。

【００８０】

ステップＳ３において、ＥＣＵ１１は、ＵＨＦ電波の衝突があったか否かを判定する。

【００８１】

上述したように、受信衝突検知フレームの受信衝突検知ビット列を構成するＮビットのうちの１ビットのみが“１”であることは、ＵＨＦ電波の衝突は発生していないことを意味する。従って、このことを確認した場合には、ＥＣＵ１１は、ステップＳ３において、ＮＯであると判定して、ステップＳ１０において、ドアのアンロック処理等を実行する。これにより、ＥＣＵ１１側の処理は終了となる。即ち、図１０の例では、受信衝突検知ビット列を構成するＮビットのうちの１ビットのみが“１”であること、即ち、ステップＳ３の処理でＮＯであると判定されることが、認証の成功の一条件とされており、その条件が満たされると、ドアのアンロック処理等が実行される。

【００８２】

これに対して、上述したように、受信衝突検知ビット列を構成するＮビットのうちの２ビット以上が“１”であることは、ＵＨＦ電波の衝突が発生していることを意味する。従

って、このことを確認した場合には、ＥＣＵ１１は、ステップＳ３において、ＹＥＳであると判定して、次のようなステップＳ４以降の処理を実行する。

【００８３】

即ち、ステップＳ４において、ＥＣＵ１１は、受信衝突検知ビット列における２つ以上の“１”とそれらの配置位置とを確認することで、複数の携帯電子キー２の存在を確認し、それらを認証候補に設定する。

【００８４】

具体的には例えば、上述した図５の例の衝突検知ビット列２１－１乃至２１－４がアンサとして利用されている場合、受信衝突検知ビット列を構成する４ビットのうちの最後尾から上位方向にＭ（Ｍは１乃至４のうちの何れかの整数値）ビット目が“１”であるときには、携帯電子キー２－Ｍが認証候補に認定される。

【００８５】

ステップＳ５において、ＥＣＵ１１は、認証候補の中で優先度の一番高い携帯電子キー２を認証相手に決定する。

【００８６】

ステップＳ６において、ＥＣＵ１１は、認証相手に対して、個別リクエストをＬＦで送信する。

【００８７】

ステップＳ７において、ＥＣＵ１１は、認証相手からアンサを受信したか否かを判定する。

【００８８】

認証相手からアンサとしてのＵＨＦが送信されてきた場合（後述する図１１のステップＳ１４の処理が実行された場合）、ＥＣＵ１１は、そのアンサを受信することで、ステップＳ７においてＹＥＳであると判定して、ステップＳ１０において、ドアのアンロック処理等を実行する。これにより、ＥＣＵ１１側の処理は終了となる。即ち、図１０の例では、電波衝突を起こした各アンサを送信した複数の携帯電子キー２が認証候補に設定され、さらに、それらの認証候補の中から優先順位が高いものが認証相手として決定され、その認証相手に対して個別リクエストが送信される。この場合、この個別リクエストに対するアンサが受信されること、即ち、ステップＳ７の処理でＹＥＳであると判定されることが、認証の成功の一条件とされており、その条件が満たされると、ドアのアンロック処理等が実行される。

【００８９】

これに対して、認証相手からのアンサが送信されてこなかった等の理由で、そのアンサの受信ができなかった場合、ＥＣＵ１１は、ステップＳ７においてＮＯであると判定して、ステップＳ８において、その認証相手を認証候補から除外する。

【００９０】

ステップＳ９において、ＥＣＵ１１は、認証候補が存在するか否かを判定する。

【００９１】

即ち、ステップＳ８の処理が何度か繰り返された結果、ステップＳ４の処理で設定された認証候補の全てが除外されてしまったような場合、ステップＳ９においてＮＯであると判定されて、ＥＣＵ１１側の処理が終了となる。

【００９２】

なお、図示はしないが、ステップＳ９においてＮＯであると判定された場合、処理を終了させずに、処理をステップＳ１に戻して、それ以降の処理を繰り返させるようにすることも可能である。即ち、ＥＣＵ１１は、認証に失敗したときには、ドアのアンロック処理等の実行を禁止して、その後、定期的なリクエストを再度送信するようにすることも可能である。

【００９３】

これに対して、認証候補がまだ１以上存在する場合には、処理はステップＳ５に戻され、それ以降の処理が繰り返される。即ち、残っている認証候補の中で優先度が最も高い携

帯電子キー２が新たな認証相手となり、その新たな認証相手についてのステップＳ５乃至Ｓ１０の処理が実行される。

【００９４】

このようなＥＣＵ１１側の処理に対する携帯電子キー２側の処理例は、図１１のフローチャートに示されるようになる。

【００９５】

即ち、図１１のステップＳ１１において、携帯電子キー２は、リクエストを受信したか否かを判定する。

【００９６】

上述した図１０のステップＳ１の処理でＥＣＵ１１からリクエストが送信されてきた場合、携帯電子キー２は、それを受信することで、ステップＳ１１においてＹＥＳであると判定し、ステップＳ１２において、図４の衝突検知フレーム２１を含むアンサをＵＨＦでＥＣＵ１１に対して送信する。

【００９７】

なお、図４の衝突検知フレーム２１を含むアンサと記述したのは、上述した例では衝突検知フレーム２１自身がアンサとされたが、アンサの構成は、衝突検知フレーム２１を含めば、上述した例に特に限定されないからである。即ち、例えば、ＩＤの後に別のデータを付加したフレームをアンサとして採用することもできる。

【００９８】

このようにしてステップＳ１２の処理が実行された場合、または、ステップＳ１１の処理でリクエストを受信していないと判定され場合、処理はステップＳ１３に進む。

【００９９】

ステップＳ１３において、携帯電子キー２は、個別リクエストを受信したか否かを判定する。

【０１００】

上述した図１０のステップＳ６の処理でＥＣＵ１１から個別リクエストが送信されてきた場合、携帯電子キー２は、それを受信することで、ステップＳ１３においてＹＥＳであると判定し、ステップＳ１４において、アンサをＵＨＦでＥＣＵ１１に対して送信する。

【０１０１】

このようにしてステップＳ１４の処理が実行された場合、または、ステップＳ１３の処理で個別リクエストを受信していないと判定され場合、処理はステップＳ１１に戻され、それ以降の処理が繰り返される。

【０１０２】

以上の図１０と図１１との処理の関係の具体例を示すと、図１２と図１３とのそれぞれに示されるようになる。即ち、図１２は、上述した図２、図３、および図８を用いて説明した動作例を、図１０と図１１とに対応させた場合のフローチャートを示している。一方、図１３は、上述した図２、図３、および図９を用いて説明した動作例のうちの図９の部分を、図１０と図１１とに対応させた場合のフローチャートを示している。即ち、上述した図２、図３、および図９の動作例のうちの図２および図３の部分、即ち、ステップＳ７の判定処理の直前までの処理例は図１２にも示されているため、図１３では省略されている。

【０１０３】

なお、図１２と図１３の説明は、上述した図２、図３、図８、および図９を用いた説明の繰り返しになるので、ここでは省略する。

【０１０４】

以上説明したように、データ衝突検知方式では、別の携帯電子キー２のアンサと混合した場合に自身の識別が可能な構成を有するアンサが使用されるので、ＥＣＵ１１の通信圏内に存在する複数の携帯電子キー２からの各アンサによって電波衝突がＥＣＵ１１で発生しても、ＥＣＵ１１側で、その発生の検知ができるので、正常な認証通信が実現される。さらに、図４の構成のようなアンサを使用すれば、ＥＣＵ１１側で、受信衝突検知ビット

の“１”の配置位置を確認することで、複数の携帯電子キー２のそれぞれを認識できるようになり、より一段と適切な認証通信が実行できるようになる。

【０１０５】

（事前調停方式）

【０１０６】

次に、図１４乃至図１８を参照して、事前調停方式について説明する。

【０１０７】

なお、以下の事前調停方式の説明でも、上述したデータ衝突検知方式の説明とあわせるために、携帯電子キー２－１乃至２－Ｎのうちの２台、例えば携帯電子キー２－１，２－３がＥＣＵ１１の通信圏内に存在する場合を例として、それらの動作を説明していく。ただし、携帯電子キー２－１乃至２－Ｎのうちの任意の２台以上がＥＣＵ１１の通信圏内に存在する場合の動作も、基本的に以下の動作と同様になる。

【０１０８】

例えば、図２を用いて上述したＥＣＵ１１の動作、即ち、リクエストＬＦ１を定期的に送信するといった動作自体は、事前調停方式でも行われるとする。

【０１０９】

ただし、事前調停方式では、ＥＣＵ１１の通信圏内に存在する携帯電子キー２－１，２－３のそれぞれは、リクエストＬＦ１を受信すると、そのアンサをＥＣＵ１１に対して返す前に、例えば図１４に示されるように、電波衝突の原因となる他の携帯電子キー２が存在するか否かを確認するための情報ＬＦ／ＵＨＦ３－１，３－３のそれぞれを送信する。なお、以下、電波衝突の原因となる他の携帯電子キー２が存在するか否かを確認するための情報を、他電子キー存在有無確認情報と称する。さらに、それを省略して単に確認情報と称する場合もある。

【０１１０】

そして、携帯電子キー２－１，２－３のそれぞれは、自身が送信した確認情報ＬＦ／ＵＨＦ３－１，ＬＦ／ＵＨＦ３－３の受信を試みる。

【０１１１】

なお、図１４において、確認情報の符号をＬＦ／ＵＨＦ３－１，ＬＦ／ＵＨＦ３－３と記述しているのは、確認情報の空間中の伝送形態は、特に限定されず、一例として、ＬＦを採用することもできるし、ＵＨＦを採用することもできるからである。

【０１１２】

また、確認情報をＬＦで送信する場合には、携帯電子キー２は、ＬＦ送受信回路（例えば後述する図２０のＬＦ用送信回路７２やＬＦ用受信回路７４）を搭載する必要がある。ただし、確認情報の受信用のＬＦ受信回路は、ＥＣＵ１１からのリクエストＬＦ１の受信用のＬＦ受信回路と併用することもできる。

【０１１３】

これに対して、確認情報をＵＨＦで送信する場合には、携帯電子キー２は、ＥＣＵ１１からのリクエストＬＦ１の受信用のＬＦ受信回路（例えば後述する図２０のＬＦ用受信回路７４）とは別に、確認情報の受信用のＵＨＦ受信回路（例えば後述する図２０のＵＨＦ用受信回路７８）を新たに搭載する必要がある。ただし、この場合、ＥＣＵ１１によりドアのアンロック処理等が実行されるまでの応答時間が、確認情報をＬＦで送信する場合と比較して短縮できる、という効果を奏することが可能になる。また、確認情報の送信用のＵＨＦ送信回路は、ＥＣＵ１１に対するアンサ（例えば後述する図１５のアンサＵＨＦ４－１，ＵＨＦ４－３）の送信用のＵＨＦ送信回路（例えば後述する図２０のＵＨＦ用送信回路７６）と併用することもできる。

【０１１４】

ところで、図示はしないが、仮に１台の携帯電子キー２のみしか存在しない場合には、その携帯電子キー２は、自身が送信した確認情報のみを正常に受信することができる。従って、このような場合、その携帯電子キー２は、他の携帯電子キー２は存在しないと認定して、ＥＣＵ１１に対してアンサとしてのＵＨＦを直ちに送信する。

【０１１５】
これに対して、図１４の例では、携帯電子キー２－１においては、自身が送信した確認情報ＬＦ／ＵＨＦ３－１のみならず、他の携帯電子キー２－３が送信した確認情報ＬＦ／ＵＨＦ３－３も受信されることになる。即ち、確認情報ＬＦ／ＵＨＦ３－１，ＬＦ／ＵＨＦ３－３による電波衝突が発生することになる。図示はしないが、さらに他の携帯電子キー２が存在する場合にも、同様に電波衝突が発生することになる。そこで、携帯電子キー２－１は、自身が送信した確認情報ＬＦ／ＵＨＦ３－１以外に、さらに他の携帯電子キー２が送信した確認情報（図１４の例では確認情報ＬＦ／ＵＨＦ３－３）も受信した場合、他の携帯電子キー２が存在すると認定する。なお、自身が送信した確認情報ＬＦ／ＵＨＦ３－１以外に、さらに他の携帯電子キー２が送信した確認情報も受信した場合とは、自身以外の確認情報を実際に受信した場合の他、自身が送信した確認情報ＬＦ／ＵＨＦ３－１を正常に受信できなかった場合も含む。
【０１１６】
同様に、携帯電子キー２－３においては、自身が送信した確認情報ＬＦ／ＵＨＦ３－３のみならず、他の携帯電子キー２－１が送信した確認情報ＬＦ／ＵＨＦ３－１も受信されることになる。即ち、確認情報ＬＦ／ＵＨＦ３－３，ＬＦ／ＵＨＦ３－１による電波衝突が発生することになる。図示はしないが、さらに他の携帯電子キー２が存在する場合にも、同様に電波衝突が発生することになる。そこで、携帯電子キー２－３は、自身が送信した確認情報ＬＦ／ＵＨＦ３－３以外に、さらに他の携帯電子キー２が送信した確認情報（図１４の例では確認情報ＬＦ／ＵＨＦ３－１）も受信した場合、他の携帯電子キー２が存在すると認定する。なお、自身が送信した確認情報ＬＦ／ＵＨＦ３－３以外に、さらに他の携帯電子キー２が送信した確認情報も受信した場合とは、自身以外の確認情報を実際に受信した場合の他、自身が送信した確認情報ＬＦ／ＵＨＦ３－３を正常に受信できなかった場合も含む。
【０１１７】
このようにして、携帯電子キー２－１，２－３のそれぞれは、両者の確認情報ＬＦ／ＵＨＦ３－３，３－１をそれぞれ受信すること（自身からの確認情報ＬＦ／ＵＨＦ３－１，３－３を正常に受信できなかったことも含む）になるので、そのことから、複数の携帯電子キー２の存在をそれぞれ認定することができる。
【０１１８】
ここで注目すべき点は、他の携帯電子キー２からの確認情報の受信の有無（自身からの確認情報を正常に受信できなかったか否かも含む）だけで、複数の携帯電子キー２の存在を認定できる点である。この点により、確認情報自体は、特別なフレームを用いる必要は無くなり、任意のフレーム、例えば通常のアンサ用のフレームを用いることが可能になる。あるいは、図６、図７で説明した受信衝突検知フレームを採用する事によっても、複数の携帯電子キー２の存在を認定でき、さらにはどの携帯電子キー２なのかも特定が可能である。
【０１１９】
このようにして、携帯電子キー２－１，２－３のそれぞれは、複数の携帯電子キー２の存在をそれぞれ認定すると、ＥＣＵ１１に対するアンサを直ちに返さずに、例えば図１５に示されるように、アンサＵＨＦ４－１，ＵＨＦ４－３のそれぞれを、応答時間をそれぞれずらした上でＥＣＵ１１に対して送信する。
【０１２０】
この場合の応答時間をずらす手法は特に限定されないが、例えば本実施の形態では、各携帯電子キー２は、それぞれ乱数を発生させ、各乱数に基づいてアンサの応答遅延時間をそれぞれ決定し、各応答遅延時間が経過した時点でアンサをそれぞれ送信する、といった手法が採用されているとする。ただし、応答遅延時間の最大時間は、携帯電子キー２の総数Ｎに応じて予め決定されており、発生される乱数の最大値も、その応答遅延時間の最大時間に応じて予め決定されているとする。
【０１２１】

あるいは、予め応答遅延時間を各携帯電子キー２に設定しておいても良い。さらに、この設定の時期は任意であり、例えば製造メーカの出荷段階で設定しても良い。また、その設定手法も特に限定されず、例えば、オーナ用の携帯電子キー２は最優先とし、応答遅延時間が最小と設定しておき、スペアの携帯電子キー２は２番目の優先順位のように設定する、といった手法も採用可能である。この設定内容は、携帯電子キー２の制御回路内のメモリ等に書き込んでおくことで実現できる。

【０１２２】

なお、本実施の形態では、そのアンサを構成するフレームの所定の領域には、複数の携帯電子キー２の存在を示す情報（以下、複数存在情報と称する）が記述されるとする。これにより、ＥＣＵ１１側でも、その所定の領域を確認することで、その通信範囲内に携帯電子キー２が複数台存在するのか否かを容易に認識できるようになる。

【０１２３】

また、ＥＣＵ１１は、携帯電子キー２の総数Ｎに応じた待ち時間を設けて、例えば上述した応答遅延時間の最大時間に対応する待ち時間を設けて、複数の携帯電子キー２からのアンサをそれぞれ受信できるようにする。そして、例えば、ＥＣＵ１１は、最初のアンサを受信したとき、認証は成功したとして、ドアのアンロック処理等を実行するようにする。

【０１２４】

以上説明した事前調停方式を採用した車両盗難防止システムがアンロック処理等が実行するまでの一連の処理は、例えば図１６と図１７とに示されるフローチャートに従って実行される。即ち、図１６は、ＥＣＵ１１側の処理例を説明するフローチャートであり、図１７は、１台の携帯電子キー２の処理例を説明するフローチャートである。

【０１２５】

図１６のステップＳ２１において、ＥＣＵ１１は、リクエストをＬＦで送信する。

【０１２６】

ステップＳ２２において、ＥＣＵ１１は、アンサとしてのＵＨＦを受信したか否かを判定する。

【０１２７】

ステップＳ２２において、アンサとしてのＵＨＦを受信していないと判定した場合、ＥＣＵ１１は、ステップＳ２３において、待ち時間を経過したか否かを判定する。

【０１２８】

ステップＳ２３において、待ち時間を経過していないと判定された場合、処理はステップＳ２２に戻され、それ以降の処理が繰り返される。即ち、待ち時間が経過するまでの間、アンサとしてのＵＨＦが送信されてこない限り、ステップＳ２２とＳ２３のループ処理が繰り返される。そして、待ち時間が経過すると、ステップＳ２３においてＹＥＳであると判定されて、処理はステップＳ２１に戻され、それ以降の処理が繰り返される。

【０１２９】

これに対して、待ち時間が経過するまでの間に、アンサとしてのＵＨＦが送信されてきて（後述する図１７のステップＳ３６参照）、ＥＣＵ１１に受信されると、ステップＳ２２においてＹＥＳであると判定され、認証が成功したとして、処理はステップＳ２４に進む。そして、ステップＳ２４において、ＥＣＵ１１は、ドアのアンロック処理等を実行する。これにより、ＥＣＵ１１側の処理は終了となる。

【０１３０】

このようなＥＣＵ１１側の処理に対する携帯電子キー２側の処理例は、図１７のフローチャートに示されるようになる。

【０１３１】

即ち、ステップＳ３１において、携帯電子キー２は、リクエストを受信したか否かを判定する。

【０１３２】

ステップＳ３１において、リクエストを受信していないと判定された場合、処理はステ

ップＳ３１に戻され、それ以降の処理が繰り返される。即ち、ＥＣＵ１１からリクエストが送信してくるまでの間、ステップＳ３１の判定処理が繰り返される。

【０１３３】

上述した図１６のステップＳ２１の処理でＥＣＵ１１からリクエストが送信されてきた場合、携帯電子キー２は、それを受信することで、ステップＳ３１においてＹＥＳであると判定し、ステップＳ３２において、他携帯電子キー存在有無情報をＵＨＦ／ＬＦで送信する。

【０１３４】

即ち、図１７の例では、他携帯電子キー存在有無情報の伝送形態はＵＨＦまたはＬＦとされている。ただし、上述したように、他携帯電子キー存在有無情報の伝送形態は、特にＵＨＦとＬＦとに限定されない。

【０１３５】

ステップＳ３３において、携帯電子キー２は、ＵＨＦ／ＬＦ電波の衝突があったか否かを判定する。

【０１３６】

自身が送信した他携帯電子キー存在有無情報のみが正常に受信された場合、携帯電子キー２は、ステップＳ３３において、ＵＨＦ／ＬＦ電波の衝突はなかったと判定し、ステップＳ３６において、アンサをＵＨＦでＥＣＵ１１に対して送信する。これにより、携帯電子キー２側の処理は終了となる。

【０１３７】

これに対して、自身が送信した他携帯電子キー存在有無情報のみならず、他の携帯電子キー２からの他携帯電子キー存在有無情報が受信された場合（自身が送信した他携帯電子キー存在有無情報が正常に受信されなかった場合含む）、携帯電子キー２は、ステップＳ３３において、ＵＨＦ／ＬＦ電波の衝突があったと判定し、ステップＳ３４において、乱数を発生させ、その乱数に基づいて応答遅延時間を決定する。

【０１３８】

そして、ステップＳ３５において、携帯電子キー２は、応答遅延時間が経過したか否かを判定する。

【０１３９】

ステップＳ３５において、応答遅延時間がまだ経過していないと判定された場合、処理は再びステップＳ３５に戻される。即ち、応答遅延時間が経過するまでの間、ステップＳ３５の判定処理が繰り返される。

【０１４０】

そして、応答遅延時間が経過すると、ステップＳ３５においてＹＥＳであると判定されて、処理はステップＳ３６に進む。ステップＳ３６において、携帯電子キー２は、アンサをＵＨＦでＥＣＵ１１に対して送信する。これにより、携帯電子キー２側の処理は終了となる。

【０１４１】

以上の図１６と図１７との処理の関係の具体例を示すと、図１８に示されるようになる。即ち、図１８は、上述した図２、図１４、および図１５を用いて説明した動作例を、図１６と図１７とに対応させた場合のフローチャートを示している。

【０１４２】

なお、図１８の説明は、上述した図２、図１４、および、図１５を用いた説明の繰り返しになるので、ここでは省略する。

【０１４３】

以上説明したように、事前調停方式では、ＥＣＵ１１の通信圏内に複数の携帯電子キー２が存在しても、複数の携帯電子キー２は、他携帯電子キー存在有無情報をそれぞれ送信することで、他の携帯電子キー２が存在することを認識でき、さらに、そのような認識をしたときには、各アンサの送信タイミングをずらすようにしたので、電波衝突自体がＥＣＵ１１において発生しなくなり、その結果、正常な認証通信が実現される。

【０１４４】
ところで、上述した一連の処理（或いはそのうちの一部分の処理）、例えば上述した図１０，図１１，図１５，図１６のフローチャートのうちの少なくとも一部に従った処理は、ハードウエアにより実行させることもできるし、ソフトウエアにより実行させることもできる。
【０１４５】
その一連の処理（或いはそのうちの一部分の処理）をハードウエアにより実行させる場合には、ＥＣＵ１１と携帯電子キー２とのそれぞれは、例えば図１９，２０のそれぞれに示されるように構成することができる。即ち、図１９，２０のそれぞれは、ＥＣＵ１１と携帯電子キー２のそれぞれのハードウエア構成例を示している。
【０１４６】
図１９の例では、ＥＣＵ１１は、ＬＦ用送信回路５１、ＵＨＦ用受信回路５３、制御回路５５、および電源回路５９を含むように構成されている。
【０１４７】
また、ＥＣＵ１１の制御回路５５には、ドアノブセンサ５６とエンジン始動許可スイッチ５７（以下、図１９の記載にあわせて、エンジン始動許可ＳＷ５７と称する）とが接続されている。
【０１４８】
ドアノブセンサ５６は、車両のドアノブを操作するためにこのドアノブ又はその付近に接近又は接触したユーザの身体（例えば手や指）を検出する例えば近接スイッチである。また、エンジン始動許可ＳＷ５７は、車両のエンジンを始動操作するために、例えば運転席に着座したユーザの身体（例えば腕や足）を検出する例えば近接スイッチである。本実施の形態では、これらのドアノブセンサ５６やエンジン始動許可ＳＷ５７が、上述したドアのアンロック処理等を実行するためのトリガを形成する。即ち、ドアノブセンサ５６やエンジン始動許可ＳＷ５７の検出信号（出力信号）が、上述した図１０のステップＳ１０や図１６のステップＳ２４の処理開始のトリガとなる。
【０１４９】
ここで、ドアノブセンサ５６の代わりに、或いはドアノブセンサ５６に加えて、他のセンサ（例えば、ドアノブ作動センサ）を設けてもよい。ドアノブ作動センサは、ドアノブが引かれると検出信号を出力するなんらかのセンサである。また、エンジン始動許可ＳＷ５７としては、運転席の運転操作（エンジンの始動操作含む）を行うための操作具類が配置された各所に、運転者の腕や足を検出するための近接センサを設けてもよい。また、ドアのアンロック処理等を実行するためのトリガを形成するための別の検出手段として、車両に既設のセンサ（例えば、ドアの開閉を検出するドア開閉センサ）を利用してもよい。
【０１５０】
また、ＥＣＵ１１の制御回路５５には、ＬＦ用送信回路５１が接続されている。このＬＦ用送信回路５１にはまた、アンテナ５２が接続されている。即ち、ＬＦ用送信回路５１は、制御回路５５から提供されたリクエスト等の情報を、ＬＦの形態でアンテナ５２から送信する。
【０１５１】
また、ＥＣＵ１１の制御回路５５には、ＵＨＦ用受信回路５３が接続されている。このＵＨＦ用受信回路５３にはまた、アンテナ５４が接続されている。即ち、ＵＨＦ用受信回路５３は、携帯電子キー２からＵＨＦの形態で送信されてくるアンサを、アンテナ５４を介して受信して適当な形態に変換した上で制御回路５５に提供する。
【０１５２】
さらにまた、ＥＣＵ１１の制御回路５５には、モータ５８が接続されている。モータ５８は、車両ドアの錠装置の駆動源であるモータ、即ちドアロックアクチュエータである。
【０１５３】
制御回路５５は、図示はしないが例えば、各種情報を記憶する記憶部と、ＥＣＵ１１全体の制御や必要な情報処理を行うマイクロコンピュータ等を含むように構成される。ここ

で、図示せぬ記憶部は、例えば書き込み消去可能な不揮発性のメモリ、より具体的には例えば、ＥＥＰＲＯＭ（Electrically Erasable Programmable Read-only Memory）よりなる。

【０１５４】

この制御回路５５が、上述した図１０や図１６のフローチャートに従った処理を主に実行する。なお、これらの処理のうちの図１０のステップＳ１０や図１６のステップＳ２４の処理、即ち、ドアのアンロック処理等については、例えば次のような処理となる。即ち、例えばドアノブセンサ５６の検出信号が入力されると、制御回路５５は、アンテナ５２からリクエストＬＦ１を送信する。そして携帯電子キー２からのアンサＵＨＦを受信できた場合には、モータ５８を駆動してドアの解錠を行う。また例えば、エンジン始動許可ＳＷ５７の検出信号が入力されると、アンテナ５２からリクエストＬＦ１を送信する。そして携帯電子キーからのアンサＵＨＦを受信できた場合には、制御回路５５は、エンジン始動許可を出力する。

【０１５５】

電源回路５９は、車両に搭載されたバッテリー（図示省略）を入力電源として、必要な電圧変換や電圧の安定化処理等を行う回路を有するものであり、ＥＣＵ１１の電力消費要素に基本的に常に電源供給を行っている。ここに、電力消費要素とは、図１９の例では、ＬＦ用送信回路５１、ＵＨＦ用受信回路５３、および制御回路５５のことをいう。

【０１５６】

このような図１９の例のＥＣＵ１１に対して、図２０の例の携帯電子キー２は、アンテナ７１乃至電池８０を含むように構成されている。

【０１５７】

ＬＦ用送信回路７２は、制御回路７９から提供された情報を、ＬＦの形態でアンテナ７１から送信する。ここに、制御回路７９から提供された情報とは、事前調停方式で利用される確認情報（他電子キー存在有無確認情報）をいう。即ち、データ衝突検知方式が採用されている場合、または、事前調停方式が採用されているが確認情報はＵＨＦで送信される場合には、アンテナ７１とＬＦ用送信回路７２とは省略可能である。

【０１５８】

ＬＦ用受信回路７４は、アンテナ７３に受信されたＬＦを、適当な形態の情報に変換して制御回路７９に提供する。ここに、アンテナ７３にＬＦの形態で受信される情報とは、ＥＣＵ１１からのリクエスト、または、事前調停方式が採用されている場合に携帯電子キー２自身や他の携帯電子キー２からＬＦの形態で送信された確認情報をいう。

【０１５９】

ＵＨＦ用送信回路７６は、制御回路７９から提供された情報を、ＵＨＦの形態でアンテナ７５から送信する。ここに、制御回路７９から提供された情報とは、ＥＣＵ１１に対するアンサ、または、事前調停方式で利用される確認情報をいう。

【０１６０】

ＵＨＦ用受信回路７８は、アンテナ７７に受信されたＵＨＦを、適当な形態の情報に変換して制御回路７９に提供する。ここに、アンテナ７３にＵＨＦの形態で受信される情報とは、事前調停方式が採用されている場合に携帯電子キー２自身や他の携帯電子キー２からＵＨＦの形態で送信された確認情報をいう。即ち、データ衝突検知方式が採用されている場合、または、事前調停方式が採用されているが確認情報はＬＦで送信される場合には、アンテナ７７とＵＨＦ用受信回路７８とは省略可能である。

【０１６１】

以上の内容をまとめると、データ衝突検知方式が採用されている場合には、アンテナ７３およびＬＦ用受信回路７４、並びに、アンテナ７５およびＵＨＦ用送信回路７６を含めば足りる。即ち、この場合、アンテナ７１およびＬＦ用送信回路７２、並びに、アンテナ７７およびＵＨＦ用受信回路７８は省略可能である。

【０１６２】

また、事前調停方式が採用され、確認情報がＬＦで送信される場合には、アンテナ７１

およびＬＦ用送信回路７２、アンテナ７３およびＬＦ用受信回路７４、並びに、アンテナ７５およびＵＨＦ用送信回路７６を含めば足りる。即ち、この場合、アンテナ７７およびＵＨＦ用受信回路７８は省略可能である。

【０１６３】

これに対して、事前調停方式が採用され、確認情報がＵＨＦで送信される場合には、アンテナ７３およびＬＦ用受信回路７４、アンテナ７５およびＵＨＦ用送信回路７６、並びにアンテナ７７およびＵＨＦ用受信回路７８を含めば足りる。即ち、この場合、アンテナ７１およびＬＦ用送信回路７２は省略可能である。

【０１６４】

制御回路７９は、図示はしないが例えば、各種情報を記憶する記憶部と、携帯電子キー２全体の制御や必要な情報処理を行うマイクロコンピュータ等を含むように構成される。ここで、図示せぬ記憶部は、例えば書き込み消去可能な不揮発性のメモリ、より具体的には例えば、ＥＥＰＲＯＭよりなる。この制御回路７９が、上述した図１１や図１７のフローチャートに従った処理を主に実行する。

【０１６５】

電池８０は、携帯電子キー２の電力消費要素に基本的に常に電源供給を行っている。ここに、電力消費要素とは、図２０の例では、ＬＦ用送信回路７２、ＬＦ用受信回路７４、ＵＨＦ用送信回路７６、ＵＨＦ用受信回路７８、および制御回路７９のことをいう。

【０１６６】

以上、上述した一連の処理（或いはそのうちの一部分の処理）をハードウエアにより実行させる場合の一実施の形態について説明した。

【０１６７】

一方、上述した一連の処理（或いはそのうちの一部分の処理）をソフトウエアにより実行させる場合には、ＥＣＵ１１若しくはその一部分、携帯電子キー２若しくはその一部分は、例えば、図２１に示されるようなコンピュータで構成することができる。

【０１６８】

図２１において、ＣＰＵ（Central Processing Unit）１０１は、ＲＯＭ（Read Only Memory）１０２に記録されているプログラム、または記憶部１０８からＲＡＭ（Random Access Memory）１０３にロードされたプログラムに従って各種の処理を実行する。ＲＡＭ１０３にはまた、ＣＰＵ１０１が各種の処理を実行する上において必要なデータなども適宜記憶される。

【０１６９】

ＣＰＵ１０１、ＲＯＭ１０２、およびＲＡＭ１０３は、バス１０４を介して相互に接続されている。このバス１０４にはまた、入出力インタフェース１０５も接続されている。

【０１７０】

入出力インタフェース１０５には、キーボード、マウスなどよりなる入力部１０６、ディスプレイなどよりなる出力部１０７、ハードディスクなどより構成される記憶部１０８、および、モデム、ターミナルアダプタなどより構成される通信部１０９が接続されている。通信部１０９は、インターネットを含むネットワークを介して他の装置との通信処理を行う。さらにまた、通信部１０９は、図示せぬアンテナを介してＥＣＵ１１と携帯電子キー２との間の送受信処理も行う。

【０１７１】

入出力インタフェース１０５にはまた、必要に応じてドライブ１１０が接続され、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどよりなるリムーバブルメディア１１１が適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部１０８にインストールされる。

【０１７２】

一連の処理をソフトウエアにより実行させる場合には、そのソフトウエアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパ

ーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【０１７３】

このようなプログラムを含む記録媒体は、図２１に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フロッピディスクを含む）、光ディスク（ＣＤ－ＲＯＭ(Compact Disk-Read Only Memory),ＤＶＤ(Digital Versatile Disk)を含む）、光磁気ディスク（ＭＤ（Mini-Disk）を含む）、もしくは半導体メモリなどよりなるリムーバブルメディア（パッケージメディア）１１１により構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM１０２や、記憶部１０８に含まれるハードディスクなどで構成される。

【０１７４】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、その順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１７５】

また、本発明が適用されるシステムは、上述した車両盗難防止システムのみならず、複数の携帯無線通信装置のうちの所定の１台が固定無線通信装置により認証される無線通信システムであれば足りる。なお、ここに、システムとは、複数の処理装置や処理部により構成される装置全体を表すものである。

【０１７６】

例えば、固定無線通信装置は、上述した例ではＥＣＵ１１として車両１（四輪車や二輪車）に搭載されたが、その他例えば、小型飛行機などの乗物、機械、機器、建造物又は設備などに搭載可能である。また、認証後の動作は、上述した例ではドアのアンロック処理等が採用されたが、その他例えば、ドア以外のトランクや盗難防止装置等の開錠又は施錠、或いはエンジン以外の搭載物の稼働又はその稼働許可などの各種動作を採用することができる。ここに、エンジン以外の搭載物としては、例えば、モータ等の駆動源、トランスミッションなどの駆動機構、エアコン、オーディオ、ナビゲーションシステム、照明等があり得る。

【図面の簡単な説明】

【０１７７】

【図１】本発明が適用される無線通信システムとしての車両の盗難防止システムの構成例を示す図である。

【図２】本発明が適用されるデータ衝突検知方式による無線通信システムの動作を説明する図である。

【図３】本発明が適用されるデータ衝突検知方式による無線通信システムの動作を説明する図である。

【図４】本発明が適用されるデータ衝突検知方式で利用される送信フレームの構造例を説明する図である。

【図５】本発明が適用されるデータ衝突検知方式で利用される送信フレームの構造例を説明する図である。

【図６】本発明が適用されるデータ衝突検知方式において、ＥＣＵが電波衝突を検知する原理を説明する図である。

【図７】本発明が適用されるデータ衝突検知方式において、ＥＣＵが電波衝突を検知する原理を説明する図である。

【図８】本発明が適用されるデータ衝突検知方式による無線通信システムの動作を説明する図である。

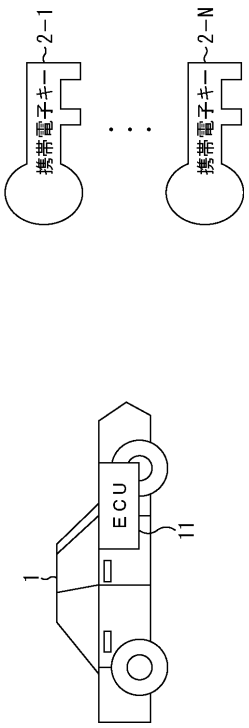
【図９】本発明が適用されるデータ衝突検知方式による無線通信システムの動作を説明する図である。

【図１０】本発明が適用されるデータ衝突検知方式によるＥＣＵ側の処理例を説明するフローチャートである。

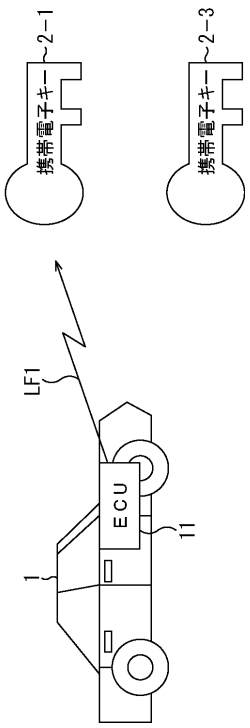
【図１１】本発明が適用されるデータ衝突検知方式による携帯電子キー側の処理例を説明するフローチャートである。
【図１２】図１０と図１１との処理の関係の具体例を示す図である。
【図１３】図１０と図１１との処理の関係の具体例を示す図である。
【図１４】本発明が適用される事前調停方式による無線通信システムの動作を説明する図である。
【図１５】本発明が適用される事前調停方式による無線通信システムの動作を説明する図である。
【図１６】本発明が適用される事前調停方式によるＥＣＵ側の処理例を説明するフローチャートである。
【図１７】本発明が適用される事前調停方式による携帯電子キー側の処理例を説明するフローチャートである。
【図１８】図１６と図１７との処理の関係の具体例を示す図である。
【図１９】本発明が適用される固定無線通信装置としてのＥＣＵの構成例を示すブロック図である。
【図２０】本発明が適用される携帯無線通信装置としての携帯電子キーの構成例を示すブロック図である。
【図２１】本発明が適用される固定無線通信装置の全部若しくは一部分または携帯無線通信装置の全部若しくは一部分のハードウエア構成の別の例を示すブロック図である。
【符号の説明】
【０１７８】
１　車両
２－１乃至２－Ｎ　携帯電子キー
１１　ＥＣＵ
２１　衝突検知フレーム
３１　衝突検知ビット列
４１　受信衝突検知フレーム
４２　受信衝突検知ビット列
５１　ＬＦ用送信回路
５２　アンテナ
５３　ＵＨＦ用受信回路
５４　アンテナ
５５　制御回路
５６　ドアノブセンサ
５７　エンジン始動許可ＳＷ
５８　モータ
５９　電源回路
７１　アンテナ
７２　ＬＦ用送信回路
７３　アンテナ
７４　ＬＦ用受信回路
７５　アンテナ
７６　ＵＨＦ用送信回路
７７　アンテナ
７８　ＵＨＦ用受信回路
７９　制御回路
８０　電池
１０１　ＣＰＵ
１０２　ＲＯＭ
１０３　ＲＡＭ

１０４　バス
１０５　入出力インタフェース
１０６　入力部
１０７　出力部
１０８　記憶部
１０９　通信部
１１０　ドライブ
１１１　リムーバブルメディア

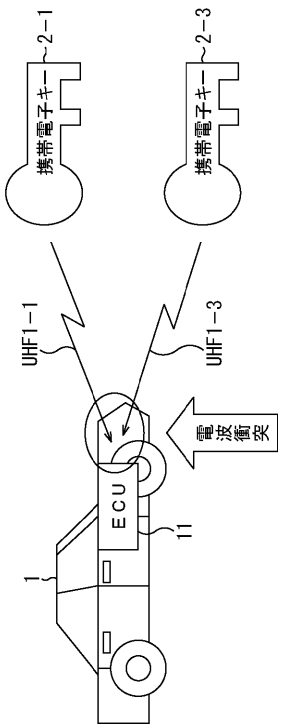
【図１】
図1



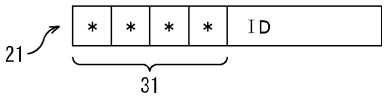
【図２】
図2



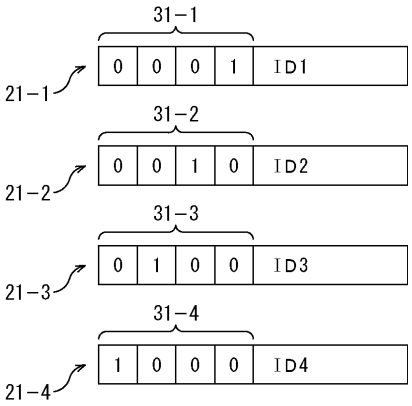
【図３】
図3



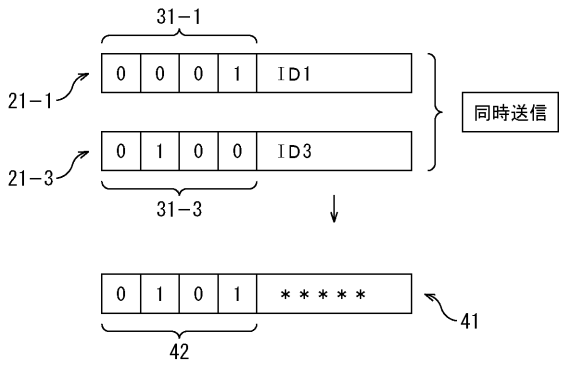
【図４】
図4



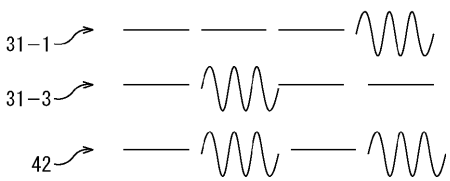
【図５】
図5



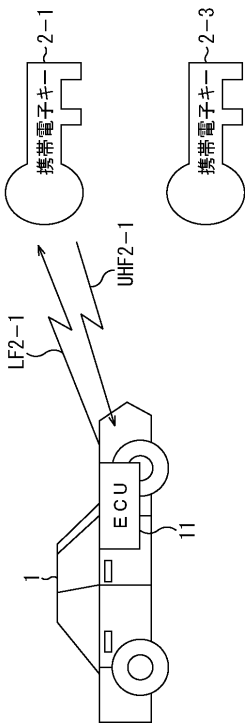
【図６】
図6



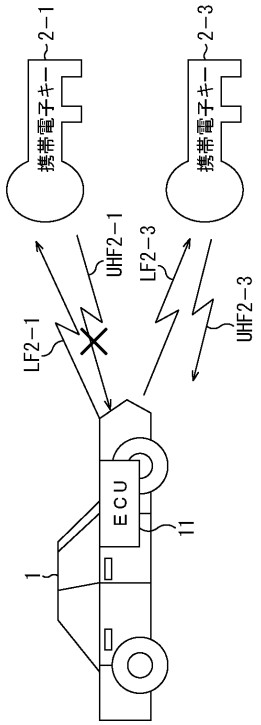
【図７】
図7



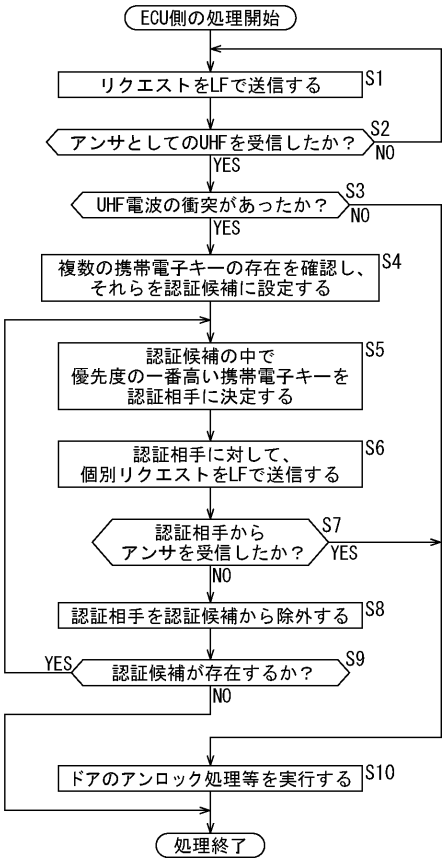
【図８】
図8



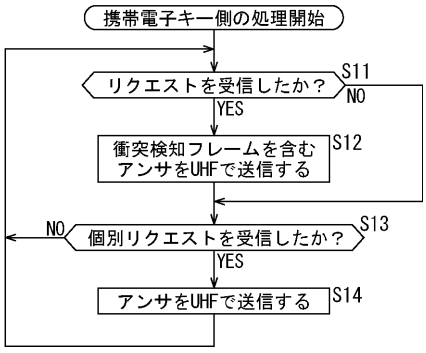
【図９】
図9



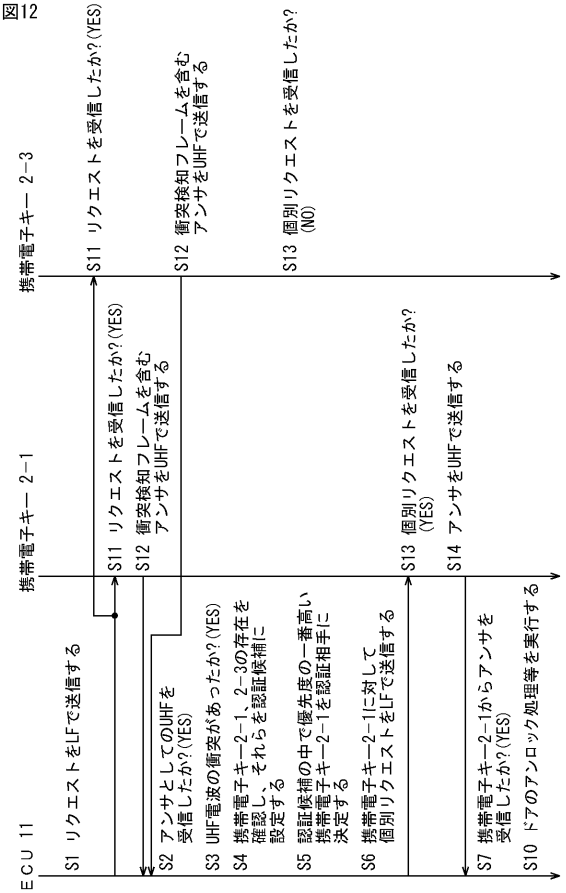
【図１０】
図10



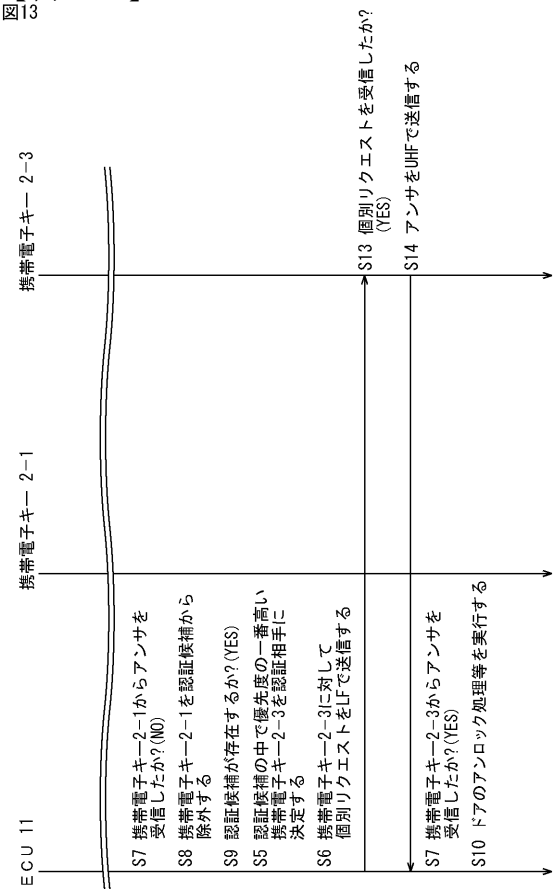
【図１１】
図11



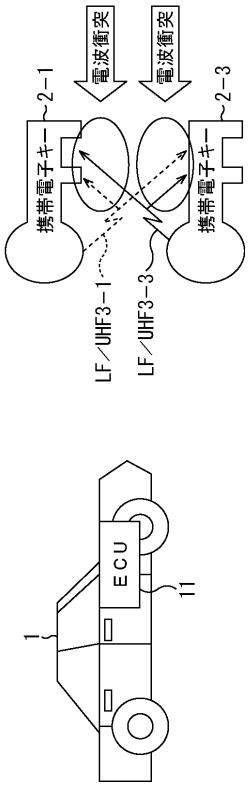
【図１２】
図12



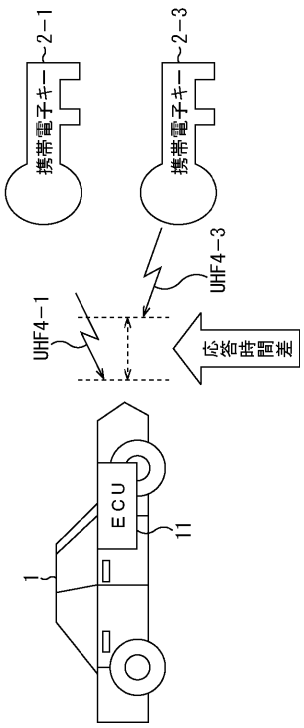
【図１３】
図13



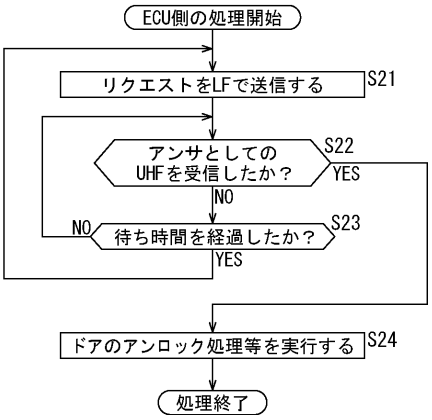
【図１４】
図14



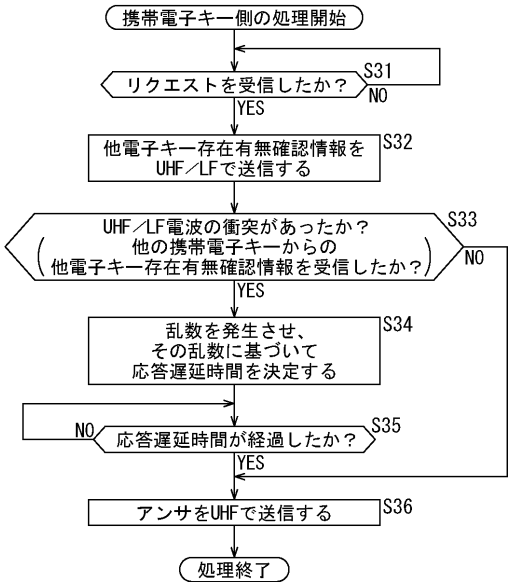
【図１５】
図15



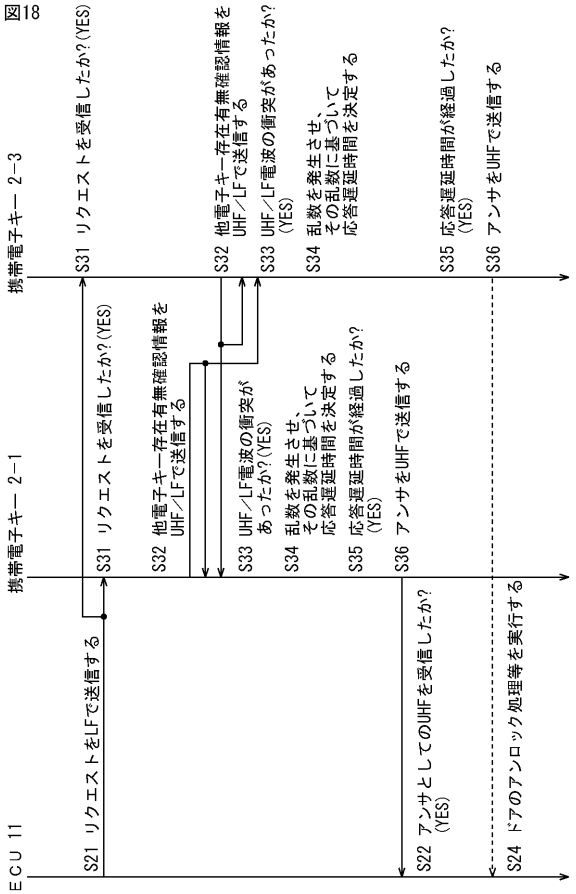
【図１６】
図16



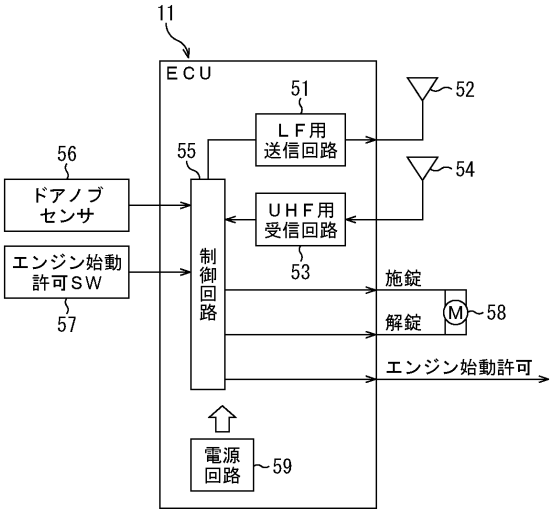
【図１７】
図17



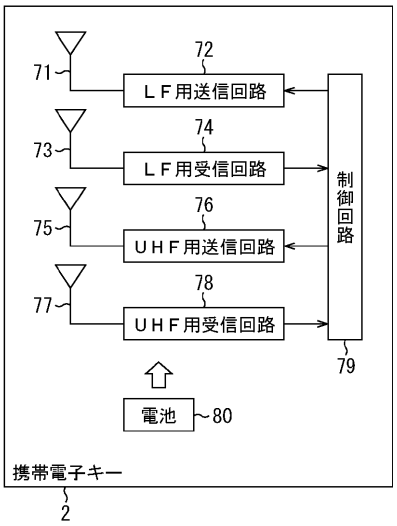
【図１８】
図18



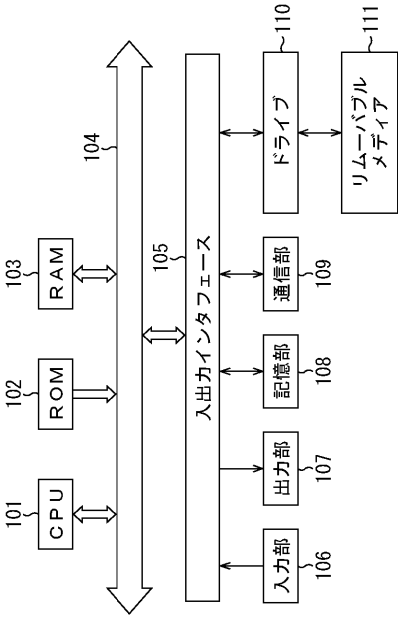
【図１９】
図19



【図２０】
図20



【図２１】
図21


CPU
101
ROM
102
RAM
103
104
105
入出力インタフェース
入力部
106
出力部
107
記憶部
108
通信部
109
ドライブ
110
リムーバブル
メディア
111