(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4204133号
(P4204133)

(45)発行日　平成21年1月7日(2009.1.7)　(24)登録日　平成20年10月24日(2008.10.24)

(51)Int.Cl.		F I		
H04B 1/59	(2006.01)	H04B	1/59	
G06K 17/00	(2006.01)	G06K	17/00	F
H04B 5/02	(2006.01)	H04B	5/02	

請求項の数 7　(全 15 頁)

(21)出願番号　特願平11-49678
(22)出願日　平成11年2月26日(1999.2.26)
(65)公開番号　特開2000-252854(P2000-252854A)
(43)公開日　平成12年9月14日(2000.9.14)
審査請求日　平成17年2月4日(2005.2.4)

(73)特許権者　000116024
ローム株式会社
京都府京都市右京区西院溝崎町２１番地
(74)代理人　100085501
弁理士　佐野　静夫
(72)発明者　疋田　純一
京都市右京区西院溝崎町２１番地　ローム株式会社内
(72)発明者　生藤　義弘
京都市右京区西院溝崎町２１番地　ローム株式会社内
(72)発明者　田口　治生
京都市右京区西院溝崎町２１番地　ローム株式会社内

最終頁に続く

(54)【発明の名称】通信システム

(57)【特許請求の範囲】

【請求項１】

管理元が異なる複数の通信用質問器と、前記質問器と個々に通信を行うことが可能である通信用応答器とからなる通信システムにおいて、

前記応答器は、前記質問器との通信において使用される情報が記憶される複数の応答器記憶領域を有する応答器記憶手段を備え、

前記質問器は、質問器記憶手段を備え、

前記応答器は、前記応答器記憶手段に前記質問器で前記応答器を認識するための鍵信号を１つ記憶し、

前記質問器は、前記質問器記憶手段に、前記鍵信号に応じた前記応答器記憶領域を指定する応答器情報を記憶し、

前記質問器は、通信の許可を求める第１の信号を前記応答器に送信し、前記第１の信号を受信した前記応答器は鍵信号を送信し、前記鍵信号を受信した質問器は応答器情報を含む命令信号送信し、前記命令信号を受信した前記応答器は可能信号を送信しかつ応答器情報の指定する記憶領域のみを使用して前記質問器と通信することを特徴とする通信システム。

【請求項２】

前記応答器は、前記質問器から送信される前記第１の信号に特定の演算処理を施す応答器演算手段を備え、前記演算手段によって前記第１の信号に演算処理を施した第２の信号及び前記鍵信号を送信することを特徴する請求項１に記載の通信システム。

【請求項３】
前記質問器は、前記第２の信号に演算処理を施す質問器演算手段を備え、前記応答器から送信された前記第２の信号を照合し前記応答器が適正なものか否かを判別するとともに、前記質問器が適正であるときは、命令信号及び前記第２の信号に演算処理を施した第３の信号を送信することを特徴とする請求項２に記載の通信システム。
【請求項４】
前記応答器は、前記質問器から送信された前記第３の信号を受信し、前記第３の信号を照合し前記質問器が適正なものか否かを判別するとともに、前記質問器が適正であるとき通信を許可する認証手段を有することを特徴とする請求項３に記載の通信システム。
【請求項５】
前記認証手段は、前記命令信号に含まれる応答器情報が適正なものか否かを判別とともに、前記質問器が適正でかつ応答器信号が適正であるとき通信を許可することを特徴とする請求項４に記載の通信システム。
【請求項６】
前記応答器記憶領域の少なくとも１領域が、前記質問器と通信を行う際に前記応答器記憶領域が使用されるとき、前記質問器から与えられる度数変更命令に応じて、前記応答器記憶領域内に記憶されている度数を変更する度数記憶部材によって構成されることを特徴とする請求項１乃至請求項５のいずれかに記載の通信システム。
【請求項７】
前記応答器と前記質問器が非接触で通信を行うことを特徴する請求項１乃至請求項６のいずれかに記載の通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、高周波タグやＩＣカードといった通信用応答器及びこれを用いた通信システムに関するもので、特に、複数のプロバイダの質問器との通信に応じて使用される複数の記憶領域を有する通信用応答器及びこれを用いた通信システムに関する。
【０００２】
【従来の技術】
近年、応答器として使用されるＩＣカード１枚で、多数のプロバイダがそれぞれに管理する複数種類のリーダ・ライタ（質問器）と通信が可能となるような通信システムが提供されている。このような通信システムを実現するために、前記ＩＣカード内に設けられたメモリを区分して、多数のプロバイダがそれぞれに管理する前記リーダ・ライタとの通信のやり取りを行う際にデータを格納するためのメモリとして使用されるように、複数のメモリ領域が前記プロバイダに応じて割り当てられている。このように、１枚のＩＣカードで多数のプロバイダがそれぞれに管理する前記リーダ・ライタと通信を行うことができるので、通信を行う際、現在通信を行っているリーダ・ライタを管理するプロバイダに割り当てられた特定のメモリ領域のみを使用可能とするとともに、それ以外のメモリ領域を使用不可能とする必要がある。
【０００３】
そのため、ＩＣカードには、それぞれのメモリ領域に割り当てられたプロバイダの管理するリーダ・ライタと通信を行うときのみに使用可能とするための暗号鍵が複数記憶されている。そして、この暗号鍵を使用して、ＩＣカード及びリーダ・ライタ間で相互認証処理が行われる。このような相互認証処理を行う非接触通信システムが、特開平１０－３２７１４２号公報に提示されている。
【０００４】
特開平１０－３２７１４２号公報に提示される通信システムでは、図１１のように、ＩＣカード内に記憶されたそれぞれのメモリ領域（エリア）を使用可能にするための前記暗号鍵は、プロバイダ毎に決定される。更に、この暗号鍵によって認証されたリーダ・ライタがアクセスを要求するメモリ領域を判別することができる。一方、リーダ・ライタ側では

、前記暗号鍵によって、ＩＣカードが適正なものか否か判断することができるが、個々のＩＣカードを判別することができない。そのため、リーダ・ライタがＩＣカードを判別するために、予めＩＣカードそれぞれに固有のＩＤ番号を記憶させる。

【０００５】

【発明が決しようとする課題】

しかしながら、特開平１０－３２７１４２号公報で提供されるＩＣカード内のメモリ領域を使用可能にするための暗号鍵は、プロバイダ毎に設定されたものであり、ＩＣカード固有の暗号鍵でない。そこで、本発明は、メモリ領域を使用可能にするための暗号鍵を、ＩＣカード毎に設定し、更に安全性の高い通信用応答器及びこれを用いた通信システムを提供することを目的とする。

【０００６】

又、特開平１０－３２７１４２号公報で提供されるＩＣカード内に記憶されるＩＤ番号は生産時に発行されるものなので、このＩＤ番号をＩＣカードに記憶させると同時に、各プロバイダも同時にそのＩＤ番号を認知させる必要がある。よって、ＩＣカードを生産する毎に、各プロバイダにそのＩＤ番号を認知させなければならないので、この通信システムにおける管理が煩雑となる。

【０００７】

【課題を解決するための手段】

本発明の通信システムは、管理元が異なる複数の通信用質問器と、前記質問器と個々に通信を行うことが可能である通信用応答器とからなる通信システムにおいて、前記応答器は、前記質問器との通信において使用される情報が記憶される複数の応答器記憶領域を有する応答器記憶手段を備え、前記質問器は、質問器記憶手段を備え、前記応答器は、前記応答器記憶手段に前記質問器で前記応答器を認識するための鍵信号を１つ記憶し、前記質問器は、前記質問器記憶手段に、前記鍵信号に応じた前記応答器記憶領域を指定する応答器情報を記憶し、前記質問器は、通信の許可を求める第１の信号を前記応答器に送信し、前記第１の信号を受信した前記応答器は鍵信号を送信し、前記鍵信号を受信した質問器は応答器情報を含む命令信号送信し、前記命令信号を受信した前記応答器は可能信号を送信しかつ応答器情報の指定する記憶領域のみを使用して前記質問器と通信することを特徴とする。

【０００８】

また、前記応答器は、前記質問器から送信される前記第１の信号に特定の演算処理を施す応答器演算手段を備え、前記演算手段によって前記第１の信号に演算処理を施した第２の信号及び前記鍵信号を送信することを特徴する。

【０００９】

また、前記質問器は、前記第２の信号に演算処理を施す質問器演算手段を備え、前記応答器から送信された前記第２の信号を照合し前記応答器が適正なものか否かを判別するとともに、前記質問器が適正であるときは、命令信号及び前記第２の信号に演算処理を施した第３の信号を送信することを特徴とする。

【００１０】

また、前記応答器は、前記質問器から送信された前記第３の信号を受信し、前記第３の信号を照合し前記質問器が適正なものか否かを判別するとともに、前記質問器が適正であるとき通信を許可する認証手段を有することを特徴とする。

【００１１】

また、前記応答器は、前記命令信号に含まれる応答器情報が適正なものか否かを判別とともに、前記質問器が適正かつ前記質問器が適正であるとき通信を許可する認証手段を有することを特徴とする。また、前記認証手段は、前記命令信号に含まれる応答器情報が適正なものか否かを判別とともに、前記質問器が適正でかつ応答器信号が適正であるとき通信を許可することを特徴とする。

【００１２】

また、前記応答器記憶領域の少なくとも１領域が、前記質問器と通信を行う際に前記応

答器記憶領域が使用されるとき、前記質問器から与えられる度数変更命令に応じて、前記応答器記憶領域内に記憶されている度数を変更する度数記憶部材によって構成されることを特徴とする。

【００１３】

また、前記応答器と前記質問器が非接触で通信を行うことを特徴とする。

【００１４】

【発明の実施の形態】

本発明の第１の実施形態について、図面を参照して説明する。図１は、本実施形態における通信システムの構成を示すブロック図である。図２は、本実施形態における通信システムの動作を示すタイムチャートである。尚、以下、ＮＧとは、認証を行ったとき認証する相手が不適正であることを、ＯＫとは認証を行ったとき認証する相手が適正であることを意味する。

【００１５】

図１に示す通信システムは、質問器となるリーダ・ライタ１及びコントローラ２と、応答器となるＩＣカード３とを有する。このような通信システムにおいて、リーダ・ライタ１は、ＩＣカード３と信号の送受信を行う同調回路４と、同調回路４で受信した応答信号を復調するとともに制御回路６より送出される命令信号を変調する変復調回路５と、命令信号を生成する制御回路６と、受信した応答信号に付加された認証信号が制御回路６より送出されるとともに該認証信号によってＩＣカード３の認証を行う認証回路７と、受信した応答信号に付加された認証信号が制御回路６より送出されるとともに該認証信号に所定の演算処理ｆ１（）を行う演算回路８とから構成される。このようなリーダ・ライタ１を制御するとともに通信を行うコントローラ２は、リーダ・ライタ１の制御回路６と信号のやり取りをするとともにリーダ・ライタ１の制御を行う主制御回路９と、ＩＣカード３の所有者のＩＤ及び所有者に関する情報が記憶されたメモリ１０とを有する。

【００１６】

又、ＩＣカード３は、リーダ・ライタ１と信号の送受信を行う同調回路１１と、同調回路１１で同調した信号を整流することによってＩＣカード３の各ブロックに供給する電源電圧を生成する整流回路１２と、同調回路１１で受信した命令信号を復調するとともに制御回路１４より送出される応答信号を変調する変復調回路１３と、応答信号を生成する制御回路１４と、受信した命令信号に付加された認証信号が制御回路１４より送出されるとともに該認証信号によってリーダ・ライタ１の認証を行う認証回路１５と、受信した命令信号に付加された認証信号が制御回路１４より送出されるとともに該認証信号に所定の演算処理ｆ２（）を行う演算回路１６と、所有者の個人情報及びＩＤが記憶されるメモリ１７とから構成される。

【００１７】

更に、このような構成のＩＣカード３は、複数のプロバイダがそれぞれ管理するリーダ・ライタと通信可能であり、メモリ１７内において、それぞれのプロバイダに、アクセスする領域17_1～17_nが振り分けられている。即ち、図３（ａ）のように、プロバイダＡ１の管理するリーダ・ライタ1_1がＩＣカード３と通信可能となったとき、その通信時にＩＣカード３内のメモリ領域17_1の読み出し又は書き込みが行われ、又、図３（ｂ）のように、プロバイダＡ２の管理するリーダ・ライタ1_2がＩＣカード３と通信可能となったとき、その通信時にＩＣカード３内の別の領域となるメモリ領域17_2の読み出し又は書き込みが行われる。

【００１８】

又、メモリ領域17_1～17_nにアクセスするためのＩＤ番号（メモリＩＤとする。）ＩＤ１～ＩＤｎと、プロバイダ側が個々のＩＣカード３を認識するためのＩＤ番号（ユーザーＩＤとする。）ＩＤ０がメモり１７内に記憶されている。このＩＤ番号ＩＤ０～ＩＤｎは、個々のＩＣカード３によって設定されるもので、ユーザーＩＤ　ＩＤ０は、生産時に生産者によって設定され、又、メモリＩＤ　ＩＤ１～ＩＤｎは、各プロバイダによって設定される。即ち、図４のように、ＩＣカード3_1のメモリ１７－１内に記憶するＩＤ番号を

それぞれＩＤ０$_1$及びＩＤ１$_1$～ＩＤｎ$_1$とすると、ＩＣカード３$_2$のメモリ１７－２内に記憶するＩＤ番号はそれぞれＩＤ０$_1$及びＩＤ１$_1$～ＩＤｎ$_1$と異なるＩＤ０$_2$及びＩＤ１$_2$～ＩＤｎ$_2$となる。

【００１９】

更に、図４のように、プロバイダＡが、ＩＣカード３$_1$と通信する際はメモリ領域１７$_1$－１を、ＩＣカード３$_2$と通信する際はメモリ領域１７$_1$－２を使用するとする。このとき、図５のように、プロバイダＡが管理するコントローラ２のメモリ１０は、ＩＣカード３$_1$のユーザーＩＤ　ＩＤ０$_1$とメモリ領域１７$_1$－１のメモリＩＤ　ＩＤ１$_1$とＩＣカード３$_1$のユーザー情報とを、又、ＩＣカード３$_2$のユーザーＩＤ　ＩＤ０$_2$とメモリ領域１７$_1$－２のメモリＩＤ　ＩＤ１$_2$とＩＣカード３$_2$のユーザー情報とを、それぞれ対応させて記憶している。

【００２０】

このような通信システムにおいて、図２のように、リーダ・ライタ１からある一定の期間毎に、ＩＣカード３が認証動作を行うための認証信号（ローリングコード）Ｒｃａが制御回路６で付加された命令信号Ｃａを生成し（ＳＴＥＰ１）、この命令信号Ｃａを変復調回路５で変調して同調回路４よりＩＣカード３へ送信する（ＳＴＥＰ２）。このとき命令信号Ｃａに付加する認証信号Ｒｃａは、任意の信号で、演算回路８で演算ｆ１（）を施した信号でない。

【００２１】

ＩＣカード３が同調回路１１でこの命令信号Ｃａを受信すると、整流回路１２で電源電圧を生成するとともに、変復調回路１３で復調し制御回路１４に送出する。制御回路１４では、命令信号Ｃａより認証信号Ｒｃａを検知して、この認証信号Ｒｃａがリーダ・ライタ１内で演算ｆ１（）が施された信号であるか否かを判別するために認証回路１５に認証信号Ｒｃａを送出する（ＳＴＥＰ３）。今、この認証信号Ｒｃａは演算ｆ１（）が施された信号でないので、認証結果はＮＧとなり、ＩＣカード３はリーダ・ライタ１を認証しない（ＳＴＥＰ４）。

【００２２】

又、このとき同時に、制御回路１４で検知された認証信号Ｒｃａを演算回路１６に送出して演算ｆ２（）を施す（ＳＴＥＰ５）。このように演算回路１６で演算ｆ２（）を施した信号ｆ２（Ｒｃａ）を認証信号Ｒｃｂとして制御回路１４に送出し、リーダ・ライタ１に送信する応答信号Ｒａに付加する。又、制御回路１４では、この応答信号Ｒａに、メモリ１７内に記憶されているユーザーＩＤ　ＩＤ０の情報を付加する（ＳＴＥＰ６）。このように生成された応答信号Ｒａは、変復調回路１３で変調され同調回路１１よりリーダ・ライタ１に送信される（ＳＴＥＰ７）。

【００２３】

リーダ・ライタ１がこの応答信号Ｒａを同調回路４より受け、変復調回路５で復調した後、制御回路６に送出する。制御回路６では、応答信号Ｒａより認証信号Ｒｃｂ及びユーザーＩＤ　ＩＤ０を検知して（ＳＴＥＰ８）、この認証信号ＲｃｂがＩＣカード３内で演算ｆ２（）が施された信号であるか否かを判別するために認証回路７に認証信号Ｒｃｂを送出する。今、この認証信号Ｒｃｂ＝ｆ２（Ｒｃａ）は演算ｆ２（）が施された信号であるので、リーダ・ライタ１はＩＣカード３を認証する（ＳＴＥＰ９）。

【００２４】

このとき、認証結果がＮＧの場合、コントローラ２との通信は行われず、制御回路６で検知された認証信号Ｒｃｂを演算回路８に送出し、演算回路８で演算ｆ１（）を施す。このように認証信号Ｒｃｂに演算ｆ１（）を施した信号ｆ１（Ｒｃｂ）を認証信号Ｒｃｃとして制御回路６に送出する（ＳＴＥＰ１０）。又、認証結果がＯＫとなるとき、制御回路６で検知したユーザーＩＤ　ＩＤ０をコントローラ２の主制御回路９に送出し（ステップ１１）、このユーザーＩＤ　ＩＤ０に対応させてメモリ１０内に記憶したＩＣカード３のメモリ領域１７$_1$を使用可能にするためのメモリＩＤ　ＩＤ１を読み出す（ＳＴＥＰ１２）。そして、コントローラ２は、メモリ１０より読み出したメモリＩＤ　ＩＤ１を、主制御回

路９からリーダ・ライタ１の制御回路６に送出する（ＳＴＥＰ１３）。
【００２５】
今、制御回路６において、認証回路７の認証結果がＯＫであれば、メモリＩＤＩＤ１、認証信号Ｒｃｃ及びメモリ領域17_1を使用することを示す信号を付加した命令信号Ｃｂを、又、認証回路７の認証結果がＮＧのときもしくはメモリ１０内にユーザーＩＤ ＩＤ０が無いときは、認証信号Ｒｃｃを付加した命令信号Ｃｂ’を変復調回路５に送出する（ＳＴＥＰ１４）。このようにして制御回路６より送出された命令信号Ｃｂ，Ｃｂ’を、変復調回路５で変調するとともに、同調回路４より送信する（ＳＴＥＰ１５）。
【００２６】
今、ＩＣカード３の同調回路１１で命令信号Ｃｂを受信すると、整流回路１２で電源電圧を生成するとともに、変復調回路１３で復調し制御回路１４に送出する。制御回路１４では、命令信号Ｃｂより認証信号Ｒｃｃ及びメモリＩＤ ＩＤ１を検知するとともに、リーダ・ライタ１が使用するメモリ領域が領域17_1であることを認識する（ＳＴＥＰ１６）。そして、認証信号Ｒｃｃがリーダ・ライタ１内で演算ｆ１（）が施された信号であるか否かを判別するために認証回路１５に認証信号Ｒｃｃを送出する。尚、図２のタイムチャートには表記していないが、ＩＣカード３が命令信号Ｃｂ’を受信すると、リーダ・ライタ１、コントローラ２、及びＩＣカード３においてＳＴＥＰ３以降の動作を繰り返す。今、命令信号Ｃｂを受信したものとしているので、認証回路１５で認証信号Ｒｃｃによってリーダ・ライタ１が適正か否かを認証する（ＳＴＥＰ１７）。
【００２７】
このとき、認証結果がＯＫの場合、メモリ１７内のメモリ領域17_1のメモリＩＤと比較して、制御回路１４にてリーダ・ライタ１から送信されたメモリＩＤが一致するか否か判断し（ＳＴＥＰ１８）、一致すればＳＴＥＰ２０に移行し、一致しなければＳＴＥＰ１９に移行する。又、ＳＴＥＰ１７で認証結果がＮＧとなるとき、又は、ＳＴＥＰ１８でメモリＩＤが不一致であるとき、制御回路１４で検知された認証信号Ｒｃｃを演算回路１６に送出し、演算回路１６で演算ｆ２（）を施す。このように認証信号Ｒｃｃに演算ｆ２（）を施した信号ｆ２（Ｒｃｃ）を認証信号Ｒｃｄとして制御回路１４に送出し（ＳＴＥＰ１９）、ＳＴＥＰ２０に移行する。
【００２８】
ＳＴＥＰ１８又はＳＴＥＰ１９のような処理動作が終了しＳＴＥＰ２０に移行すると、認証結果がＯＫのときは通信可能であることをリーダ・ライタ１に伝えるための応答信号Ｒｂを、認証結果がＮＧのときは認証信号Ｒｃｄ及びユーザーＩＤ ＩＤ０を付加した応答信号Ｒｂ’を制御回路１４で生成して変復調回路１３に送出する。今、認証信号Ｒｃｃ＝ｆ１（Ｒｃｂ）で且つ、リーダ・ライタ１か送信されるメモリＩＤはＩＤ１でありメモリ領域17_1のメモリＩＤと一致するので、ＳＴＥＰ２０では、通信可能であることをリーダ・ライタ１に伝えるための応答信号Ｒｂを生成する。このように応答信号Ｒｂ，Ｒｂ’が変復調回路１３に送出されると、それぞれ変調されて同調回路１１より送信される（ＳＴＥＰ２１）。
【００２９】
今、リーダ・ライタ１の同調回路４で応答信号Ｒｂを受信すると、変復調回路５で復調し制御回路６に送出する。制御回路６では、応答信号ＲｂよりＩＣカード３内のメモリ領域17_1が開放され、通信可能となったことを認識する（ＳＴＥＰ２２）。尚、図２のタイムチャートには表記していないが、リーダ・ライタ１が応答信号Ｒｂ’を受信すると、リーダ・ライタ１、コントローラ２、及びＩＣカード３においてＳＴＥＰ８以降の動作を繰り返す。
【００３０】
今、応答信号Ｒｂを受信したものとしているので、制御回路６よりコントローラ２の主制御回路９にＩＣカード３と通信可能であることを認識させる（ＳＴＥＰ２３）。コントローラ２がＩＣカード３と通信可能であることを認識すると、リーダ・ライタ１を介してＩＣカード３と相互に通信を行い、この通信を行う際にＩＣカード３のメモリ領域17_1の

データの読み出し又は書き込みを行う（ＳＴＥＰ２４）。

【００３１】

本発明の第２の実施形態について、図面を参照して説明する。図６は、本実施形態における通信システムの構成を示すブロック図である。図７は、本実施形態における通信システムの動作を示すタイムチャートである。尚、本実施形態の通信システムにおいて、図６に示すリーダ・ライタ及びコントローラの内部構造は、図１の通信システム内におけるリーダ・ライタ１及びコントローラ２の内部構造と同様のものとする。又、図６のＩＣカードを構成するブロックにおいて、図１の通信システム内におけるＩＣカード３を構成するブロックと同様のものは、同じ記号を付してその詳細な説明は省略する。

【００３２】

図６に示すＩＣカード３１は、領域18_1～18_nに分割されたメモリ１８と、同調回路１１と、整流回路１２と、変復調回路１３と、制御回路１４と、認証回路１５と、演算回路１６とを有し、又、第１の実施形態におけるＩＣカード３と同様、複数のプロバイダがそれぞれ管理するリーダ・ライタと通信可能であり、メモリ１８内において、それぞれのプロバイダに、アクセスする領域18_1～18_nが振り分けられている。

【００３３】

又、メモリ領域18_1～18_nは、プロバイダ側が個々のＩＣカード３を認識するためのＩＤ番号（認識ＩＤとする。）ＩＤ１ａ～ＩＤｎａと、アクセスするためのＩＤ番号（メモリＩＤとする。）ＩＤ１ｂ～ＩＤｎｂとを有し、この認識ＩＤ ＩＤ１ａ～ＩＤｎａ及びメモリＩＤ ＩＤ１ｂ～ＩＤｎｂがメモり１８内に記憶されている。この認識ＩＤ ＩＤ１ａ～ＩＤｎａ及びメモリＩＤ ＩＤ１ｂ～ＩＤｎｂは、個々のＩＣカード３によって設定されるもので、生産後に各プロバイダにより設定される。

【００３４】

更に、図８のように、プロバイダＢが、ＩＣカード31_1と通信する際はメモリ１８－１の内、領域18_1－１を、ＩＣカード31_2と通信する際はメモリ１８－２の内、領域18_1－２を使用するとする。このとき、図９のように、コントローラ２のメモリ１０は、ＩＣカード31_1の認識ＩＤ ＩＤ１ａ－１とメモリＩＤ ＩＤ１ｂ－１とを、又、ＩＣカード31_2のユーザーＩＤ ＩＤ１ａ－２とメモリＩＤ ＩＤ１ｂ－２とを、それぞれ対応させて記憶している。

【００３５】

このような通信システムの動作について、図７を使用して説明する。尚、図２とと同様の動作は、同様であること示しその詳細な説明は省略する。まず、リーダ・ライタ１において、図２のＳＴＥＰ１及びＳＴＥＰ２と同様の処理をＳＴＥＰ１ａ及びＳＴＥＰ２ａで行い、認証信号Ｒｃ１を付加した命令信号をＣ１をＩＣカード３１に送信する。又、このとき、命令信号Ｃ１には、メモリ領域18_1へのアクセスを希望していることを示す信号も付加されている。

【００３６】

ＩＣカード３１が同調回路１１でこの命令信号Ｃ１を受信すると、ＳＴＥＰ３ａにおいて、制御回路１４でリーダ・ライタ１がメモリ領域18_1へのアクセスを希望していることを認識するとともに、図２のＳＴＥＰ３と同様に、認証回路１５に制御回路１４で検知した認証信号Ｒｃ１を送出する。ＳＴＥＰ４ａ及びＳＴＥＰ５ａにおいて、図２のＳＴＥＰ４及びＳＴＥＰ５と同様の動作を行う。

【００３７】

そして、制御回路１４において、演算回路１６で認証信号Ｒｃ１に基づいて生成された認証信号Ｒｃ２＝ｆ２（Ｒｃ１）及び、メモリ１８より読み出した領域18_1の認識ＩＤ ＩＤ１ａが、応答信号Ｒ１に付加される（ＳＴＥＰ６ａ）。このように生成された応答信号Ｒ１は、変復調回路１３で変調されて同調回路１１よりリーダ・ライタ１に送信される（ＳＴＥＰ７ａ）。

【００３８】

リーダ・ライタ１がこの応答信号Ｒ１を同調回路４より受信すると、ＳＴＥＰ８ａ～１４

ａにおいて、図２のＳＴＥＰ８～１４と同様の動作を行う。即ち、制御回路６で応答信号Ｒ１より認識ＩＤ　ＩＤ１ａ及び認証信号Ｒｃ２を検知し、認証回路７によって認証信号Ｒｃ２に基づいて認証処理を行う。このとき、認証結果がＮＧの場合、コントローラ２との通信が行われずに、ＳＴＥＰ１０ａに移行して演算回路で認証信号Ｒｃ３＝ｆ１（Ｒｃ２）を生成した後、認証信号Ｒｃ３を付加した命令信号Ｃ２’を生成する。又、認証結果がＯＫの場合、ＳＴＥＰ１１ａに移行した後、コントローラ２でメモリ１０内の認識ＩＤ　ＩＤ１ａに対応するメモリＩＤ　ＩＤ１ｂを読み出してリーダ・ライタ１に送出し、認証信号Ｒｃ３及びメモリＩＤ　ＩＤ１ｂを付加した命令信号Ｃ２を生成する。又、認識ＩＤ　ＩＤ１ａがメモリ１０内に存在しないときは、上記した命令信号Ｃ２’が制御回路６で生成される。

【００３９】

このように、命令信号Ｃ２，Ｃ２’が生成されると、この命令信号をＩＣカード３１に送信する（ＳＴＥＰ１５ａ）。今、この認証信号Ｒｃ２＝ｆ２（Ｒｃ１）は演算ｆ２（）が施された信号であるので、リーダ・ライタ１はＩＣカード３１を認証する。よって、命令信号Ｃ２がＩＣカード３１に送信される。

【００４０】

ここで、ＳＴＥＰ１６ａ以降の動作については、図７で使用している記号以外は、図２のＳＴＥＰ１６以降の動作とほぼ同様であるので、以下、簡単に説明する。

【００４１】

今、ＩＣカード３１が命令信号Ｃ２を受信すると、制御回路１４で、命令信号Ｃ２より認証信号Ｒｃ３及びメモリＩＤ　ＩＤ１ｂを検知する（ＳＴＥＰ１６ａ）。尚、第１の実施形態と同様に、ＩＣカード３１が命令信号Ｃ２’を受信すると、リーダ・ライタ１、コントローラ２、及びＩＣカード３１においてＳＴＥＰ３ａ以降の動作を繰り返す。そして、認証回路１５で認証信号Ｒｃ３がリーダ・ライタ１内で演算ｆ１（）が施された信号であるか否かを判別して、リーダ・ライタ１が適正か否かを判断する（ＳＴＥＰ１７ａ）。

【００４２】

このとき、認証結果がＯＫの場合、メモリ領域18_1のメモリＩＤと比較して、制御回路１４にてリーダ・ライタ１から送信されたメモリＩＤが一致するか否か判断し（ＳＴＥＰ１８ａ）、一致すればＳＴＥＰ２０ａに移行し、一致しなければＳＴＥＰ１９ａに移行する。又、ＳＴＥＰ１７ａで認証結果がＮＧの場合、又は、ＳＴＥＰ１８ａでメモリＩＤが不一致であるとき、制御回路１４で検知された認証信号Ｒｃ３を演算回路１６に送出し、演算回路１６で認証信号Ｒｃ４＝ｆ２（Ｒｃ３）を生成して（ＳＴＥＰ１９ａ）、ＳＴＥＰ２０ａに移行する。

【００４３】

ＳＴＥＰ１８ａ又はＳＴＥＰ１９ａのような処理動作が終了しＳＴＥＰ２０ａに移行すると、認証結果がＯＫのときは通信可能であることをリーダ・ライタ１に伝えるための応答信号Ｒ２を、認証結果がＮＧのときは認証信号Ｒｃ４及び認識ＩＤ　ＩＤ１ａを付加した応答信号Ｒ２’を制御回路１４で生成した後、リーダ・ライタ１に送信する（ＳＴＥＰ２１ａ）。今、認証信号Ｒｃ３＝ｆ１（Ｒｃ２）で且つ、リーダ・ライタ１から送信されるメモリＩＤはＩＤ１ｂでありメモリ領域18_1のメモリＩＤと一致するので、ＳＴＥＰ２１ａでは、通信可能であることをリーダ・ライタ１に伝えるための応答信号Ｒ２が送信される。

【００４４】

リーダ・ライタ１が応答信号Ｒ２を受信すると、制御回路６で、応答信号Ｒ２よりＩＣカード３１内のメモリ領域18_1が開放され、通信可能となったことを認識する（ＳＴＥＰ２２ａ）。尚、第１の実施形態と同様に、リーダ・ライタ１が応答信号Ｒ２’を受信すると、リーダ・ライタ１、コントローラ２、及びＩＣカード３１においてＳＴＥＰ８ａ以降の動作を繰り返す。

【００４５】

今、応答信号Ｒ２を受信したものとしているので、制御回路６よりコントローラ２の主制

御回路９にＩＣカード３１と通信可能であることを認識させる（ＳＴＥＰ２３ａ）。コントローラ２がＩＣカード３１と通信可能であることを認識すると、リーダ・ライタ１を介してＩＣカード３１と相互に通信を行い、この通信を行う際にＩＣカード３１のメモリ領域１８_{1}のデータの読み出し又は書き込みを行う（ＳＴＥＰ２４ａ）。

【００４６】

尚、第１及び第２の実施形態において、リーダ・ライタ、ＩＣカードの間で複数回認証動作が行われ、全く認証が行われなかったとき、コントローラにエラーメッセージが送信され、通信が終了される。又、ＩＣカード又はコントローラでＩＤ番号の確認が複数回行われ、いずれも不一致もしくは存在しないと判断されたとき、コントローラにエラーメッセージが送信され、通信が終了される。

【００４７】

本発明の第３の実施形態について、図面を参照して説明する。図１０は、本実施形態における通信システムの構成を示すブロック図である。尚、本実施形態の通信システムにおいて、図１０に示すリーダ・ライタ及びコントローラの内部構造は、図１の通信システム内におけるリーダ・ライタ１及びコントローラ２の内部構造と同様のものとする。又、図１０のＩＣカードを構成するブロックにおいて、図１の通信システム内におけるＩＣカード３を構成するブロックと同様のものは、同じ記号を付してその詳細な説明は省略する。

【００４８】

図１０に示すＩＣカード３２は、領域１９_{1}～１９_{3}に分割されたメモリ１９と、同調回路１１と、整流回路１２と、変復調回路１３と、制御回路１４と、認証回路１５と、演算回路１６とを有する。又、第１の実施形態におけるＩＣカード３と同様、プロバイダＣ１，Ｃ２，Ｃ３がそれぞれ管理するリーダ・ライタと通信可能であり、メモリ１９内において、プロバイダＣ１，Ｃ２，Ｃ３それぞれに、アクセスする領域１９_{1}，１９_{2}，１９_{3}が振り分けられている。

【００４９】

又、プロバイダＣ１がＩＣカード３２を例えばその度数が金銭を表すプリペイドカードとして扱い、メモリ領域１９_{1}内に、使用した度数毎にその度数を表すビット数が減少するようなダウンカウンタ（不図示）が構成されているものする。更に、このダウンカウンタは、制御回路１４からのリセット信号によって初期化される。今、プロバイダＣ１が管理するリーダ・ライタ５０にＩＣカード３２が近接して、第１又は第２の実施形態のような認証動作が行われ、リーダ・ライタ５０及びＩＣカード３２が相互認証した後、メモリ領域１９_{1}が開放されて、コントローラ５１とＩＣカード３２との間でリーダ・ライタ５０を介した通信が可能となったとする。

【００５０】

ＩＣカード３２のユーザーＤが、例えばガソリンスタンドなどで代金を支払うために利用しているようなときの動作について説明する。まず、ダウンカウンタ内に保持されているビット数を読み出すための命令信号が、コントローラ５１内のメモリ（不図示）に記憶しているユーザーＤの残り度数の情報が付加され、この命令信号がコントローラ５１よりリーダ・ライタ５０を介してＩＣカード３２に送信される。このとき、コントローラ５１では、支払い後のユーザーＤの残り度数を演算し主制御回路（不図示）内に記憶する。

【００５１】

ＩＣカード３２にこのような命令信号を受信すると、制御回路１４よりダウンカウンタを読み出し可能とする信号がメモリ領域１９_{1}に送出される。メモリ領域１９_{1}に読み出し可能とする信号が送出されると、ダウンカウンタを読み出し可能とし、制御回路１４でそのビット数がカウントされる。更に、制御回路１４では、命令信号に付加されたコントローラ５１内のメモリに記憶しているユーザーＤの残り度数とダウンカウンタから検知される度数とを比較して一致するか確認する。この度数が一致したとき、一致したことを知らせる応答信号を、リーダ・ライタ５０を介してコントローラ５１に送信する。

【００５２】

コントローラ５１は、この応答信号を受けると、リーダ・ライタ５０を介して、ダウンカ

ウンタ内のビット数を代金分の度数に相当するビット数だけ減少させる命令信号をＩＣカード３２に送信する。このとき、コントローラ５１では、支払い後のユーザーＤの残り度数を演算し主制御回路（不図示）内に記憶する。ＩＣカード３２がこの命令信号を受けると、制御回路１４よりダウンカウンタを書き込み可能とする信号がメモリ領域１９_{1}に送出される。メモリ領域１９_{1}に書き込み可能とする信号が送出されると、ダウンカウンタを書き込み可能とし、ダウンカウンタ内に保持されているビット数のうち、命令信号より検知されるビット数分削除される。

【００５３】

このように度数が削除されると、制御回路１４で削除後のダウンカウンタのビット数が演算され、このビット数に相当する度数の情報が付加された応答信号が、リーダ・ライタ５０を介してコントローラ５１に送信される。コントローラ５１では、主制御回路に記憶した度数と応答信号より検知される度数を比較して一致したとき、一致したことを知らせる命令信号をＩＣカードに送信するとともに、コントローラ５１のメモリにこの度数を記憶させて通信を終了する。

【００５４】

又、ＩＣカード３２とリーダ・ライタ５０が相互認証して通信可能となった後、度数を増加させるためにユーザーＤが入金をしたときの動作を説明する。まず、ダウンカウンタ内に保持されているビット数を読み出すための命令信号に、コントローラ５１内のメモリに記憶しているユーザーＤの残り度数の情報が付加され、この命令信号がコントローラ５１よりリーダ・ライタ５０を介してＩＣカード３２に送信される。

【００５５】

ＩＣカード３２にこのような命令信号を受信すると、制御回路１４よりダウンカウンタを読み出し可能とする信号がメモリ領域１９_{1}に送出される。メモリ領域１９_{1}に読み出し可能とする信号が送出されると、ダウンカウンタを読み出し可能とし、制御回路１４でそのビット数がカウントされる。更に、制御回路１４では、命令信号に付加されたコントローラ５１内のメモリに記憶しているユーザーＤの残り度数とダウンカウンタから検知される度数とを比較して一致するか確認する。この度数が一致したとき、一致したことを知らせる応答信号を、リーダ・ライタ５０を介してコントローラ５１に送信する。

【００５６】

コントローラ５１は、この応答信号を受けると、リーダ・ライタ５０を介して、ダウンカウンタ内のビット数を入金後の度数に相当するビット数に変更させる命令信号をＩＣカード３２に送信する。このとき、コントローラ５１では、入金後のユーザーＤの残り度数を演算し主制御回路内に記憶する。ＩＣカード３２がこの命令信号を受けると、制御回路１４よりダウンカウンタを書き込み可能とする信号がメモリ領域１９_{1}に送出される。メモリ領域１９_{1}に書き込み可能とする信号が送出されると、ダウンカウンタを書き込み可能となる。その後、制御回路１４よりリセット信号が送信され、一旦、初期化される。このように初期化された後、ダウンカウンタ内に保持されているビット数が命令信号より検知されるビット数に相当するまで削除される。

【００５７】

このように度数が変更されると、制御回路１４で変更後のダウンカウンタのビット数が演算され、このダウンカウンタのビット数に相当する度数の情報が付加された応答信号が、リーダ・ライタ５０を介してコントローラ５１に送信される。コントローラ５１では、主制御回路に記憶した度数と応答信号より検知される度数を比較して一致したとき、一致したことを知らせる命令信号をＩＣカードに送信するとともに、コントローラ５１のメモリにこの度数を記憶させて通信を終了する。

【００５８】

以上の実施形態では、ＩＣカードといった非接触で通信を行う通信用応答器を用いて説明したが、このような応答器に限らず、接触して通信を行うような通信用応答器でも良い。尚、接触して通信を行う場合、第１～第３の実施形態のように信号の送受信を行うための同調回路を用いる代わりに、入出力インターフェイスを応答器及び質問器に設けることに

よって、その通信が可能となる。

【００５９】

【発明の効果】

本発明では、より安全性の高い通信システムを形成することができる。

【００６３】

また、少なくとも１つの記憶領域が度数記憶部材によって構成されることにより、プリペイドカードのような、その度数を金銭の代わりとして用いることを目的とした記憶領域を形成することが可能となる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態で使用する通信システムの構成を示すブロック図。

【図２】図１に示す通信システムの動作を示すタイムチャート。

【図３】図１に示す通信システムにおいてリーダ・ライタを管理するプロバイダとＩＣカード内のメモリ領域の関係を示すブロック図。

【図４】図１に示す通信システムで使用するＩＣカードの個々の関係を示すブロック図。

【図５】図１に示す通信システムで使用するコントローラの内部及びメモリ内部の構造を示すブロック図。

【図６】本発明の第２の実施形態で使用する通信システムの構成を示すブロック図。

【図７】図６に示す通信システムの動作を示すタイムチャート。

【図８】図６に示す通信システムで使用するＩＣカードの個々の関係を示すブロック図。

【図９】図６に示す通信システムで使用するコントローラの内部及びメモリ内部の構造を示すブロック図。

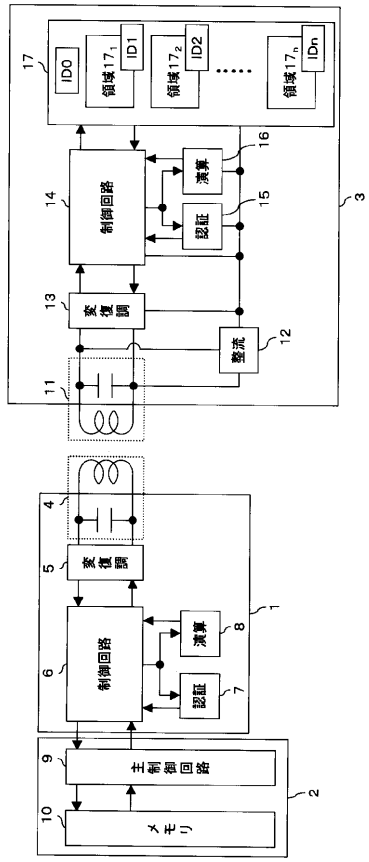
【図１０】本発明の第３の実施形態で使用する通信システムの構成を示すブロック図。

【図１１】従来の通信システムの構成を示すブロック図。

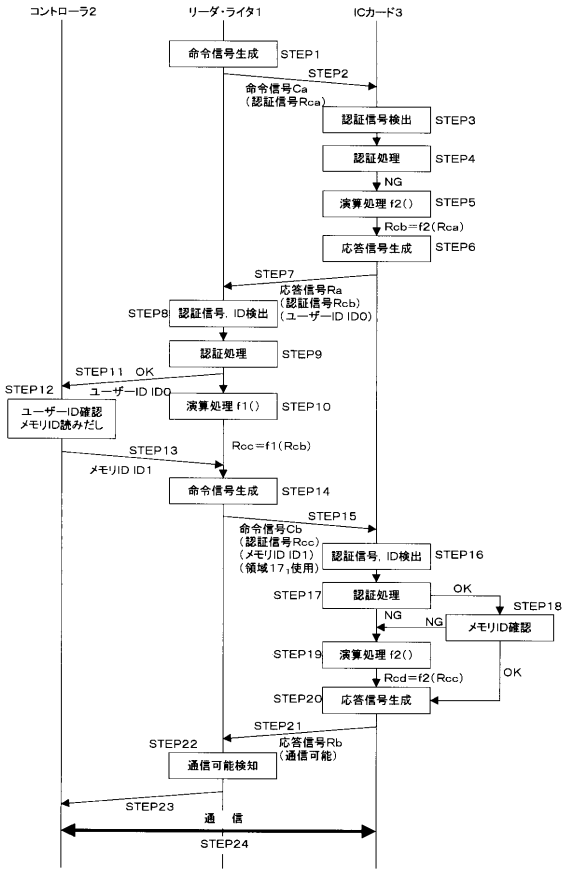
【符号の説明】

１，５０　リーダ・ライタ
２，５１　コントローラ
３，３１，３２　ＩＣカード
４，１１　同調回路
５，１３　変復調回路
６，１４　制御回路
７，１５　認証回路
８，１６　演算回路
９　主制御回路
１０，１７，１８，１９　メモリ
１２　整流回路

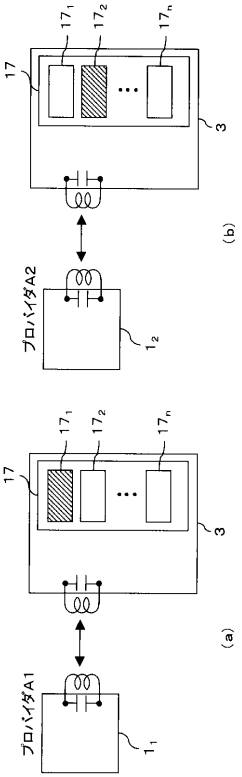
【図１】


17
IDO
領域17₁
ID1
領域17₂
ID2
領域17ₙ
IDn
制御回路
演算
認証
変復調
整流
16
15
14
13
12
11
3
4
5
6
7
8
1
9
10
2
主制御回路
メモリ

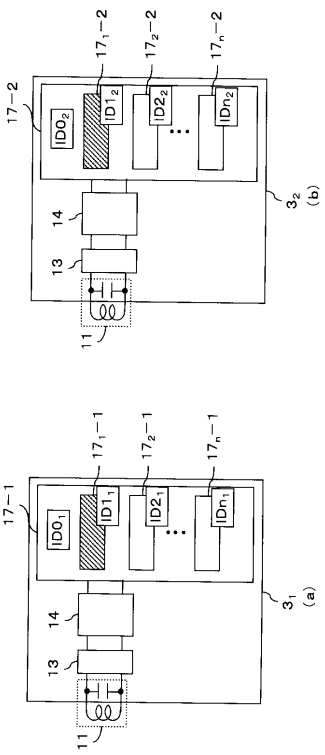
【図２】


コントローラ2
リーダ・ライタ1
ICカード3
命令信号生成 STEP1
STEP2
命令信号Ca
(認証信号Rca)
認証信号検出 STEP3
認証処理 STEP4
NG
演算処理 f2() STEP5
Rcb=f2(Rca)
応答信号生成 STEP6
STEP7
応答信号Ra
(認証信号Rcb)
(ユーザーID IDO)
STEP8 認証信号, ID検出
認証処理 STEP9
STEP11 OK
STEP12
ユーザーID IDO
ユーザーID確認
メモリID読みだし
演算処理 f1() STEP10
Rcc=f1(Rcb)
STEP13
メモリID ID1
命令信号生成 STEP14
STEP15
命令信号Cb
(認証信号Rcc)
(メモリID ID1)
(領域17₁使用)
認証信号, ID検出 STEP16
認証処理 STEP17
OK
STEP18
メモリID確認
NG
NG
STEP19 演算処理 f2()
Rcd=f2(Rcc)
OK
STEP20 応答信号生成
STEP21
STEP22
応答信号Rb
(通信可能)
通信可能検知
STEP23
通 信
STEP24

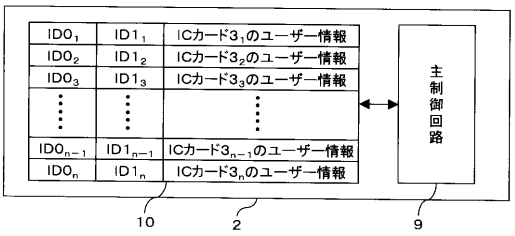
【図３】


17₁
17₂
17ₙ
17
3
(b)
プロバイダA2
1₂
17₁
17₂
17ₙ
17
3
(a)
プロバイダA1
1₁

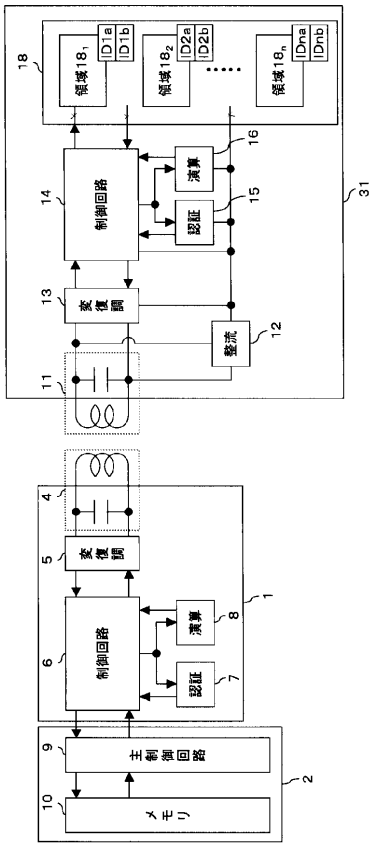
【図４】


17₁−2
17₂−2
17ₙ−2
17−2
IDO₂
ID1₂
ID2₂
IDn₂
3₂
(b)
14
13
11
17₁−1
17₂−1
17ₙ−1
17−1
IDO₁
ID1₁
ID2₁
IDn₁
3₁
(a)
14
13
11

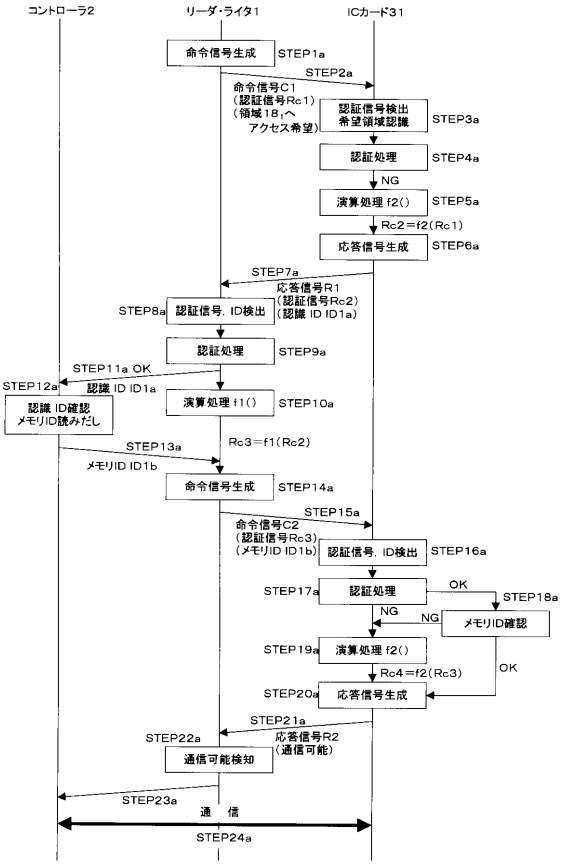
【図５】


ID0$_1$ ID1$_1$ ICカード3$_1$のユーザー情報
ID0$_2$ ID1$_2$ ICカード3$_2$のユーザー情報
ID0$_3$ ID1$_3$ ICカード3$_3$のユーザー情報
ID0$_{n-1}$ ID1$_{n-1}$ ICカード3$_{n-1}$のユーザー情報
ID0$_n$ ID1$_n$ ICカード3$_n$のユーザー情報
主制御回路
10
2
9

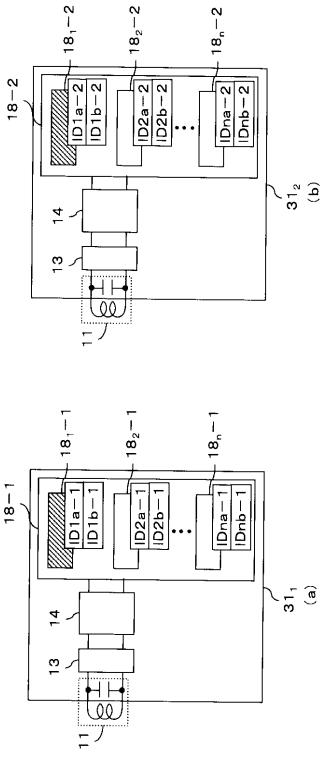
【図６】


18
領域18$_1$
ID1a
ID1b
領域18$_2$
ID2a
ID2b
領域18$_n$
IDna
IDnb
14
制御回路
演算
16
認証
15
31
13
変復調
整流
12
11
4
5
変復調
6
制御回路
演算
8
認証
7
1
9
主制御回路
10
メモリ
2

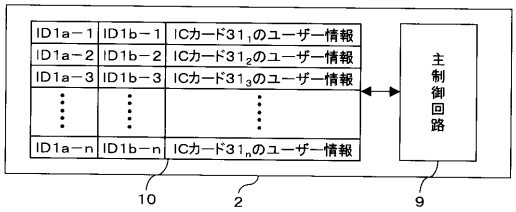
【図７】


コントローラ2
リーダ・ライタ1
ICカード31
命令信号生成
STEP1a
STEP2a
命令信号C1
(認証信号Rc1)
(領域18$_1$へ
アクセス希望)
認証信号検出
希望領域認識
STEP3a
認証処理
STEP4a
NG
演算処理 f2()
STEP5a
Rc2=f2(Rc1)
応答信号生成
STEP6a
STEP7a
応答信号R1
(認証信号Rc2)
(認識 ID ID1a)
STEP8a
認証信号, ID検出
認証処理
STEP9a
STEP11a OK
STEP12a
認識 ID ID1a
認識 ID確認
メモリID読みだし
演算処理 f1()
STEP10a
Rc3=f1(Rc2)
STEP13a
メモリID ID1b
命令信号生成
STEP14a
STEP15a
命令信号C2
(認証信号Rc3)
(メモリID ID1b)
認証信号, ID検出
STEP16a
STEP17a
認証処理
OK
STEP18a
NG
NG
メモリID確認
STEP19a
演算処理 f2()
OK
Rc4=f2(Rc3)
STEP20a
応答信号生成
STEP21a
STEP22a
応答信号R2
(通信可能)
通信可能検知
STEP23a
通 信
STEP24a

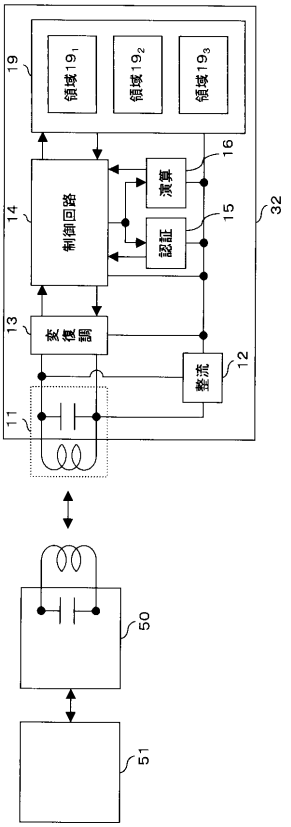
【図８】


18$_1$−2
18$_2$−2
18$_n$−2
18−2
ID1a−2
ID1b−2
ID2a−2
ID2b−2
IDna−2
IDnb−2
31$_2$
(b)
14
13
11
18$_1$−1
18$_2$−1
18$_n$−1
18−1
ID1a−1
ID1b−1
ID2a−1
ID2b−1
IDna−1
IDnb−1
31$_1$
(a)
14
13
11

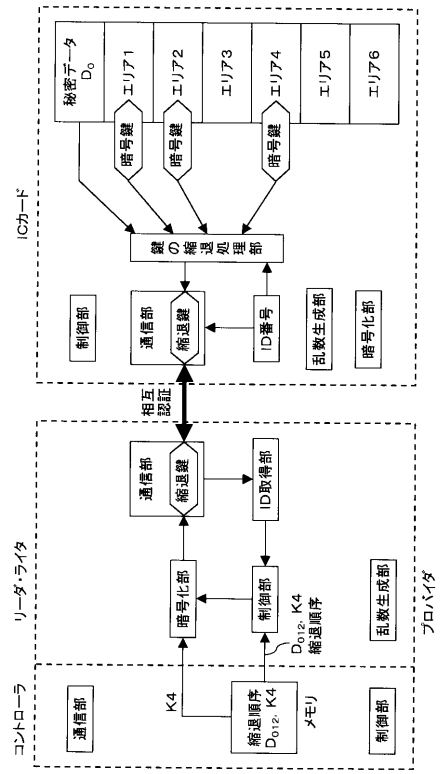
【図９】


ID1a−1
ID1b−1
ICカード31$_1$のユーザー情報
ID1a−2
ID1b−2
ICカード31$_2$のユーザー情報
ID1a−3
ID1b−3
ICカード31$_3$のユーザー情報
ID1a−n
ID1b−n
ICカード31$_n$のユーザー情報
照合回路
10
2
9

【図１０】


19
領域19$_1$
領域19$_2$
領域19$_3$
16
演算
14
制御回路
15
認証
32
13
変復調
12
整流
11
50
51

【図１１】


ICカード
秘密データ D$_0$
エリア1
エリア2
エリア3
エリア4
エリア5
エリア6
暗号鍵
暗号鍵
暗号鍵
鍵の縮退処理部
制御部
通信部
縮退鍵
ID番号
乱数生成部
暗号化部
相互認証
リーダ・ライタ
通信部
縮退鍵
ID取得部
暗号化部
制御部
D$_{012}$, K4
縮退順序
乱数生成部
プロバイダ
コントローラ
通信部
K4
縮退順序 D$_{012}$, K4
メモリ
制御部

フロントページの続き

審査官　藤井　浩

(56)参考文献　特開平１０－３２７１４２（ＪＰ，Ａ）
特開平１０－３０７８９９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04B　1/59
G06K　17/00
G06K　19/07
H04B　5/02