

(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2009-31877

(P2009-31877A)

(43) 公開日 平成21年2月12日(2009.2.12)

(51) Int.Cl. F I テーマコード (参考)
G06K 19/10 (2006.01) G06K 19/00 S 5B035
G06K 19/07 (2006.01) G06K 19/00 H

審査請求 有 請求項の数 10 O L (全 15 頁)

(21) 出願番号	特願2007-192655 (P2007-192655)	(71) 出願人	000197366
(22) 出願日	平成19年7月24日 (2007.7.24)		NECアクセステクニカ株式会社
		(74) 代理人	100079164
			弁理士 高橋 勇
		(72) 発明者	石田 博通
			静岡県掛川市下俣800番地 NECア
			クセステクニカ株式会社内
		Fターム(参考)	5B035 AA06 AA14 BB09 CA08 CA11
			CA12 CA23 CA38

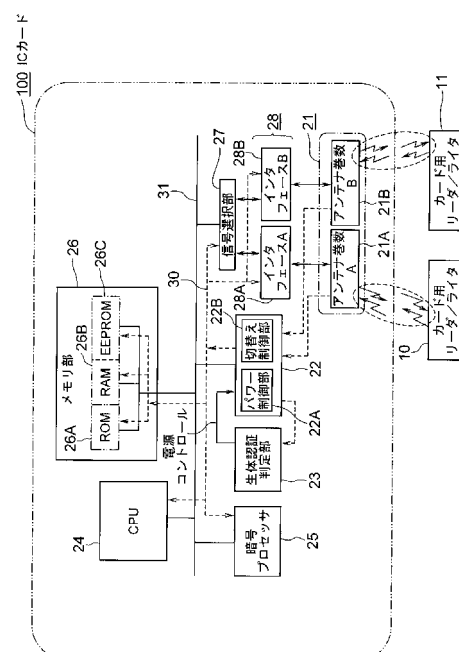
(54) 【発明の名称】 非接触ICカード、携帯端末装置、起動制御方法、および起動制御プログラム

(57) 【要約】

【課題】 本人専用にするため高セキュリティを前提に、マルチRFインタフェース対応で複数アプリケーション機能を統合して利便性の向上したICカード等を提供する。

【解決手段】 カード用リーダ／ライタ10、11が作る電磁界を介して非接触で電力供給を受け前記カード用リーダ／ライタ10、11との間で通信をおこなう機能を備えた非接触ICカード100であって、前記電磁界の無線周波数等の異なるRFインタフェース形式が複数種類ある場合に、その何れかのRFインタフェース形式を備えた前記カード用リーダ／ライタ11に接近したとき正常に動作するための複数のアンテナ構造体21と、このアンテナ構造体21からの電力供給を受けて生体認証による本人確認を行なう生体認証判定部23、及び前記生体認証判定部23が本人認証した場合のみ構成各機能部への電力を供給する制御を行なう電力供給制御部とを備えて構成される。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

カード用リーダ／ライタにより形成される電磁界を介して非接触で電力供給を受けると共に前記カード用リーダ／ライタとの間で相互に通信を行う機能を備えた非接触 I C カードであって、

前記電磁界の無線周波数等の異なる R F インタフェース形式が複数種類ある場合に、その何れかの R F インタフェース形式を備えた前記カード用リーダ／ライタに接近したとき正常に動作するための複数のアンテナ構造体と、前記アンテナ構造体からの電力供給を受けて生体認証による本人確認を行なう生体認証判定部及び前記アンテナ構造体からの電力供給を受けかつ前記生体認証判定部が本人認証した場合に他の各構成機能部への電力供給制御を行う電力供給制御部とを、備えたことを特徴とする非接触 I C カード。

10

【請求項 2】

前記請求項 1 に記載の非接触 I C カードにおいて、

前記アンテナ構造体を複数の巻き線から成る巻き線構造とすると共に、この巻き線構造の前記アンテナ構造体に当該巻線を切替え制御する巻線切替制御部を併設し、

前記アンテナ構造体がマルチ R F インタフェース形式に対応する複数のアンテナ特性を形成するように、前記巻線切替制御部が、前記アンテナ構造体の前記複数の巻き線を接続し又は遮断する巻線切替え制御機能を備えていることを特徴とした非接触 I C カード。

【請求項 3】

前記請求項 1 又は 2 に記載の非接触 I C カードにおいて、

20

前記電力供給制御部に暗証番号検出判定部を併設し、前記生体認証判定部での認証が失敗した場合でも、別に使用者から入力される暗証番号が前記暗証番号検出判定部によって正規であると判定された場合には、当該判定結果に基づいて前記電力供給制御部が作動し前記各機能部への電力供給を行う構成としたことを特徴とする非接触 I C カード。

【請求項 4】

前記請求項 1 乃至 3 の何れか 1 つに記載の非接触 I C カードにおいて、

前記電力供給制御部に不正操作ロック部を併設し、前記生体認証判定部での認証が失敗した場合には、前記不正操作ロック部が機能して前記生体認証判定部と前記電力供給制御部を稼働させないように不正操作ロック状態に設定することを特徴とした非接触 I C カード。

30

【請求項 5】

前記請求項 4 に記載の非接触 I C カードにおいて、

前記不正操作ロック部が、事前に設定された前記不正操作ロック状態を外部から解除指令が入力された場合に解除するロック状態解除機能を備えていることを特徴とした非接触 I C カード。

【請求項 6】

前記請求項 1 乃至 5 の何れか 1 つに記載の非接触 I C カードにおいて、

前記電力供給制御部にタイマ監視部を併設し、前記生体認証判定部での生体認証確立後、前記タイマ監視部は一定時間だけ前記電力供給制御部を通電可能にすることを特徴とした非接触 I C カード。

40

【請求項 7】

前記請求項 1 乃至 6 の何れか 1 つに記載の非接触 I C カードにおいて、

前記複数のアンテナ構造体の内、一つのアンテナ構造体が前記生体認証判別部、暗証番号検出判定部、及び不正操作ロック部の一又は二以上の生体認証判別部等に専用に電力を供給する構成とし、他のアンテナ構造体を前記電力供給制御部を介して前記生体認証判定部等以外の他の各構成機能部に電力を供給すると共に前記カード用リーダ／ライタと通信する構成としたことを特徴とする非接触 I C カード。

【請求項 8】

前記請求項 1 乃至 7 の何れか 1 つに記載の非接触 I C カードに含まれる I C チップを含むカード片を携帯端末本体に着脱自在に搭載し、

50

前記携帯端末本体が予め備えているテンキー、音声送話機、画像撮像機等の情報入力機能を利用して暗証番号及び生体情報を入力するようにし、これにより前記ＩＣチップを含むカード片が備えている前記認証機能を利用して本人認証処理を行なう構成としたことを特徴とする携帯端末装置。

【請求項９】

カード用リーダ／ライタにより形成される電磁界を介して非接触で電力を受給する電力供給制御部を備え、生体認証による本人確認を行なう生体認証判定部と、前記リーダ／ライタとの間で相互に通信を行う相互通信機能とを備えた非接触ＩＣカードにあって、

前記電力供給制御部が前記生体認証判定部等により電力を供給し他のカード機能部には電力供給を禁止する本人認証工程と、

前記生体認証判定部が本人認証した場合に同時に当該生体認証判定部が他のカード機能部に対する給電許可信号を前記電力供給制御部に送出する給電許可信号送出工程と、

前記給電許可信号に付勢されて機能し前記電力供給制御部から前記生体認証判定部を除く前記他のカード機能部へ電力を供給する電力供給工程と、
を備えたことを特徴とする非接触ＩＣカード用起動制御方法。

【請求項１０】

カード用リーダ／ライタにより形成される電磁界を介して非接触で電力を受給する電力供給制御部を備え、生体認証による本人確認を行なう生体認証判定部と前記カード用リーダ／ライタとの間で相互に通信をおこなう機能を備えた非接触ＩＣカードにあって、

前記電力供給制御部は前記生体認証判定部等により電力を供給し、他のカード機能部には電力供給を禁止する本人認証処理、

前記生体認証判定部が本人認証した場合に給電許可信号を前記電力供給制御部に送出する給電許可信号送出処理、

前記給電許可信号に付勢されて機能し前記電力供給制御部から前記生体認証判定部を除く前記他のカード機能部へ電力供給を行う電力供給処理、
をコンピュータに実行させるように構成したことを特徴とするカード起動制御プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、非接触ＩＣカードに係り、特に生体認証機能とマルチＲＦインタフェースを備えた非接触ＩＣカード及びその機能を取込んだ携帯端末装置に関する。

【背景技術】

【０００２】

近年、磁気カードについてはスキミングや偽造キャッシュカード等の不正引出しが問題になる一方で、非接触ＩＣカードおよびその機能を取込んだ携帯端末装置は、ＩＣチップへの不正データの書き込みや内部データの読み出し改ざん等のリスクが暗号機能などのセキュリティ機能により極めて少なく、その普及が加速している。

【０００３】

電子マネー「Ｅｄｙ（エディ）」やＪＲが発行する「Ｓｕｉｃａ（スイカ）」、「ＩＣＯＣＡ（イコカ）」などの非接触認証（ＲＦＩＤ：Radio Frequency IDentification）技術を利用した各種非接触ＩＣカード、あるいは携帯電話会社がサービスする「おサイフケータイ」などの電子マネー機能を有する携帯端末装置等がそれである（ここで、Ｅｄｙ，Ｓｕｉｃａ，ＩＣＯＣＡ，おサイフケータイ，は登録商標である）。

【０００４】

これらＩＣカード或いは携帯端末装置は、安全性を高めるための高度な暗号技術を扱えるＩＣチップを搭載して、カード用リーダ／ライタとの間で相互の認証やデータの読み出し書き込みを行なっている。例えば、「Ｆｅｌｉｃａ（登録商標）」（某先行メーカーの開発技術）などでは、非接触カードとカード用リーダ／ライタ間の通信の傍受を防ぐため共通鍵暗号方式を採用しており、一定程度、安全である。更にセキュリティレベルを上げるた

10

20

30

40

50

め公開鍵暗号方式を使用する方式もある。

【0005】

そのため、ICチップに保存された秘密鍵が解読される危険性も零ではないが、磁気カードに比べて内部データが改ざんされたりするリスクは極めて少なく、カードのコピーやクローンを作り出すことも極めて困難である。

【0006】

しかし、これらが盗難や紛失により所有者以外の他人の手に渡ってしまった場合には、これらカード等には正当な所有者か否かを確認する本人認証機能が無いため、他人でも容易に本人に成りすまして使用できるという危険性がある。

【0007】

この危険性を解消するため、例えば、本人に固有の生体情報（指紋、虹彩、顔、静脈等）を認証する生体認証機能をICカードに搭載し、成りすましの危険を防ぐ工夫も公開され、そのとき生体認証機能を動作させる電力を圧電素子から得る提案もなされている（例えば特許文献1）。

【0008】

また一方、ICカードを利用するサービスが多様化するにつれ、夫々のサービスに対応した多数のICカードを携帯しなければならない不便さも目立ってきた。電子マネー機能を有する携帯端末装置等においても、サービスを提供する提供主体により、無線周波数などRF（Radio Frequency：無線）インタフェース形式の違い、サービスレベル、セキュリティ技術（暗号化のアルゴリズム）等の異なるタイプが存在しており、ユーザとしては複数のICカードや携帯端末装置を所持しなければならないという問題がある。

【0009】

これまで進められてきた1枚のカードで複数のアプリケーションないしサービスを扱えるマルチアプリケーション対応の技術開発は、無線周波数などのRFインタフェース形式は一つのものであった。非接触型ICカードといっても、通信距離（無線周波数に依存する）の違いにより密着型（低周波）、近接型（短波）、近傍型（中波）、又は遠隔型（マイクロ波）といった異なったタイプの方式が存在し、サービス毎に使い分けが行なわれている。これら無線周波数などのRFインタフェース形式が異なるサービスをも、1枚のカードに統合できれば利便性は向上する。

【0010】

そのため、通信距離が異なる複数のサービスで利用するため、複数のアンテナとRFインタフェースをカードに備えた構成とし、通信距離が長くなることによるセキュリティ低下をサービスに使用できるメモリ領域を限定する等で防ぐ工夫が既に公開されている。ただし、この場合、生体認証などの認証機能は付いていない（例えば特許文献2）。

【特許文献1】特開2005-202505号公報

【特許文献2】特開2006-320541号公報

【発明の開示】

【発明が解決しようとする課題】

【0011】

上述したように、これまでの非接触ICカードやその機能を取込んだ携帯端末装置は、例えば盗難や紛失などにより他人の手に渡ってしまった場合に簡単に本人に成りすまして使用できるというセキュリティ上の問題を抱えていた。また、サービスが多様化するにつれ、RFインタフェース形式の違い等から複数のICカードや携帯端末装置を携帯しなければならない不便さも目立ってきた。

【0012】

〔発明の目的〕

本発明は、上記問題点に鑑み、RFインタフェース形式の異なるサービスにも高いセキュリティ機能の下に使用できるようにし、これによって利便性の向上を図った非接触ICカード、携帯端末装置、起動制御方法、および起動制御プログラムを提供することを、その目的とする。

10

20

30

40

50

【課題を解決するための手段】

【0013】

上記目的を達成するため、本発明に係る非接触ＩＣカードは、カード用リーダ／ライタにより形成される電磁界を介して非接触で電力供給を受けると共に前記カード用リーダ／ライタとの間で相互に通信を行う機能を備え、前記電磁界の無線周波数等の異なるＲＦインタフェース形式が複数種類ある場合に、その何れかのＲＦインタフェース形式を備えた前記カード用リーダ／ライタに接近したとき正常に動作するための複数のアンテナ構造体と、前記アンテナ構造体からの電力供給を受けて生体認証による本人確認を行なう生体認証判定部及び前記アンテナ構造体からの電力供給を受けかつ前記生体認証判定部が本人認証した場合に他の各構成機能部への電力供給制御を行う電力供給制御部とを備えたことを特徴とする。

10

【0014】

又、上記目的を達成するため、本発明に係る携帯端末装置は、前述した非接触ＩＣカードに含まれるＩＣチップを含むカード片を携帯端末本体に着脱自在に搭載し、前記携帯端末本体が予め備えているテンキー、音声送話機、画像撮像機等の情報入力機能を利用して暗証番号及び生体情報を入力するようにし、これにより前述したＩＣチップを含むカード片が備えている前記認証機能を利用して本人認証処理を行なう構成としたことを特徴とする。

【0015】

更に、上記目的を達成するため、本発明に係るカード起動制御方法は、カード用リーダ／ライタが作る電磁界を介して非接触で電力を受給する電力供給制御部を備え、生体認証による本人確認を行なう生体認証判定部と前記カード用リーダ／ライタとの間で相互に通信をおこなう機能を備えた非接触ＩＣカードにあって、前記電力供給制御部は前記生体認証判定部等により電力を供給し、他のカード機能部には電力供給を禁止する本人認証工程と、前記生体認証判定部が本人認証した場合に給電許可信号を前記電力供給制御部に送出する給電許可信号送出工程と、前記給電許可信号に付勢されて機能し前記電力供給制御部から前記生体認証判定部を除く前記他のカード機能部へ電力供給を行う電力供給工程とを備えたことを特徴とする。

20

【0016】

更に又、上記目的を達成するため、本発明に係るカード起動制御プログラムは、カード用リーダ／ライタが作る電磁界を介して非接触で電力を受給する電力供給制御部を備え、生体認証による本人確認を行なう生体認証判定部と前記リーダ／ライタとの間で相互に通信をおこなう機能を備えた非接触ＩＣカードにおいて、前記電力供給制御部は前記生体認証判定部等により電力を供給し他のカード機能部には電力供給を禁止する本人認証処理と、前記生体認証判定部が本人認証した場合に給電許可信号を前記電力供給制御部に送出する給電許可信号送出処理と、前記給電許可信号に付勢されて機能し前記電力供給制御部から前記生体認証判定部を除く前記他のカード機能部へ電力供給を行う電力供給処理とをコンピュータに実行させるように構成したことを特徴とする。

30

【発明の効果】

【0017】

以上のように、本発明によると、ＩＣカードの所持者が本人であることを認証されることを前提として無線周波数等のＲＦインタフェースの異なるＩＣカードの統合化を成し得るようにしたので、多様化するカードの一元化によって管理面や携帯面の利便性が向上すると同時にカードの盗難や紛失などに際しても高い安全性が得られるという従来にない優れた非接触ＩＣカード、携帯端末装置、起動制御方法、および起動制御プログラムを提供することができる。

40

【発明を実施するための最良の形態】

【0018】

〔第１の実施形態〕

以下、本発明の第１実施形態を図１乃至図４に基づいて説明する。

50

最初に、本実施形態の基本的な構成について説明し、その後、本実施形態全体を具体的に説明する。

【0019】

まず、図1において、符号100は非接触ICカードを示し、符号10, 11は前述した非接触ICカード100の使用時に当該非接触ICカード100に対応して配置されるカード用リーダ／ライタを示す。非接触ICカード100は、カード用リーダ／ライタ10, 11により形成される電磁界を介して非接触で電力供給を取り込む機能を有し、更に当該カード用リーダ／ライタ10, 11との間で相互に通信を行う機能を備えている。

【0020】

この非接触ICカード100は、上述した電磁界の無線周波数等の異なるRFインタフェース形式が複数種類ある場合、その何れかのRFインタフェース形式を備えた前記カード用リーダ／ライタ10, 11に接近したとき正常に動作するための複数のアンテナ構造体21と、このアンテナ構造体21からの電力供給により作動して生体認証による本人確認を行なう生体認証判定部23と、前述したアンテナ構造体21からの電力供給を受けかつ前記生体認証判定部23が本人認証した場合のみ各機能部への電力を供給制御する電力供給制御部としてのパワー制御部22Aとを備えている。

【0021】

ここで、前述したアンテナ構造体21は本実施形態では複数の巻き線から成る巻線構造によって形成されている。そして、この巻き線構造の前記アンテナ構造体21には、前述した巻き線構造を必要に応じて切り替える切替え制御部（巻線切替制御部）22Bが併設されている。即ち、前述したアンテナ構造体21がマルチRFインタフェース形式に対応する複数のアンテナ特性を形成するように、前述した切替え制御部22Bが前記アンテナ構造体21の前述した巻き線構造の接続制御および切断（遮断）制御を実行する制御機能を備えた構成となっている。符号22は主制御部を示す。この主制御部22は、本第1実施形態では前述したパワー制御部22Aと切替え制御部（巻線切替制御部）22Bとを主たる構成要素として構成されている。

【0022】

これを更に詳述する。

図1は、上述したように非接触ICカード（以下「本ICカード」と呼ぶ）100のブロック構成図である。

【0023】

本ICカード100は、RFインタフェース形式の違うカード用リーダ／ライタ10, 11の通信距離内にあるとどちらとも通信できるように構成されている。ここで、図1には、同時に両方のカード用リーダ／ライタ10, 11と通信しているように表示しているが、カード用リーダ／ライタ10, 11に対してはサービスに依存しており、その設置状況も多様であり、必要に応じて又は外部からの指令によりどちらか一方のカード用リーダ／ライタ10又は11に対して通信を許容するように構成してもよい。

【0024】

本ICカード100は、前述したように、カード用リーダ／ライタ10, 11から供給される電磁波を受けるアンテナ構造体21（具体的には複数のアンテナ21A, 21B）と、このアンテナ21A, 21Bからの交流電流を整流して電力を得かつ供給制御を行なう電力供給制御部として機能するパワー制御部22と、パワー制御部22から一次電源を得て本人認証を行なう生体認証判定部23とを備えている。この生体認証判定部23での本人認証で本人が確認されると、生体認証判定部23は直ちに機能してパワー制御部22に必要な各構成ユニットへの電源供給を許可し、その後、所定の認証手順に準拠してICカードの認証手続きが開始される。

ここで、前記アンテナ21Aは巻数Aのアンテナコイルにより構成され、前記アンテナ21Bは巻数Bのアンテナコイルにより構成されている（図1参照）。

【0025】

更に、本ICカード100は、各種情報処理を行なうCPU24と、暗号化された認証

処理を行なう暗号プロセッサ 25 と、処理プログラムを保管する ROM 26 A と、処理作業領域としての RAM 26 B と、予め登録された個人情報や暗号化方式に用いられる鍵情報を保管する EEPROM 26 C を含むメモリ部 26 と、カード用リーダ／ライタ 10, 11 との情報の入出力を無線通信で行なうための RF インタフェース部 28 0 及び使用する無線によって信号を切替える信号選択部 27 とを備えている。

【0026】

次に、本 IC カード 100 の上記構成各部の機能を説明する。

まず、生体認証判定部 23 は、指紋、虹彩、顔、静脈、網膜、声紋、筆跡、および音声等何らかの個人固有の情報を生体情報入力部（図示せず）から受け取り、この個人固有の情報と予めカードに登録され記憶されている個人情報とを照合する生体認証により、本人確認を行なう機能を備えている。そして、本人確認に成功した場合のみ、次に述べるパワー制御部 22 A の電力供給を許可する許可信号を送る。これによって、本人以外の他人がカードを不正に使用しようとしても電力供給が遮断されカードが動作しないので紛失・盗難等に対する安全性が高まる。

【0027】

パワー制御部 22 A は、アンテナ構造体 21 から得た交流電力を整流して直流電力に変換し、先ず生体認証判定部 23 に給電するが、それ以外の本 IC カードの各機能部へは給電を遮断する機能を有している。前述の生体認証判定部 23 からの本人認証結果である給電許可信号が送られない限り、電力を他には供給しないという形態で電力供給を制御している。本人認証が成されない場合は、この制御機能によって、一切、本 IC カード 100 とカード用リーダ／ライタ 10, 11 間の情報のやり取りはできないので、安全性が高まる。

【0028】

CPU 24 は、本人認証が完了し電力供給がなされて各構成機能部が動作を始めると、先ず、カード用リーダ／ライタ 10 からの IC カード 100 に対する起動要求信号に対応するインタフェース 28 A を経由して受信し、メモリ部 26 と協働して情報処理を行ない、応答を再びインタフェース 28 A 経由でカード用リーダ／ライタ 10 側へ通知する。非接触 IC カード 100 とカード用リーダ／ライタ 10 間の制御手順は、標準化された暗号化認証処理手順によって行う。ここで、カード用リーダ／ライタ 10, 11 に対応してインタフェース 28 A, 28 B が装備され、このインタフェース 28 A とインタフェース 28 B とにより、インタフェース 28 が構成されている。

【0029】

暗号プロセッサ 25 は、本 IC カード 100 とカード用リーダ／ライタ 10 間で取り交わされる標準化された暗号化認証処理を専用に行う。IC カード 100 とカード用リーダ／ライタ 10, 11 とは、各々正当に発行され又は設置されたものであることを相互に認証する形態となっている。

【0030】

メモリ部 26 は、処理プログラムを保管する ROM 26 A、処理作業領域として RAM 26 B、予め登録された個人情報や暗号化方式に用いられる鍵情報を保管する EEPROM 26 C を備え、CPU 24 や暗号プロセッサ 25 と協働して処理した各種情報を保持する。

【0031】

次に、複数の無線周波数に対応する上述した複数のアンテナ構造体 21 について説明する。

図 2 (a) に、アンテナ構造体 21 のカード内部の構造を他の要素と共に模式的に示したものを示す。ここで、アンテナ構造体 21 には、前述したように切替え制御部（巻線切替え制御部）22 B が併設され、この切替え制御部 22 B によって巻線を切替えることにより、複数の無線周波数に対応したアンテナ特性を設定し得るように構成されている。

図 2 (b) は、アンテナ 21 A, 21 B とこれらを接続し又は遮断制御する切替え制御部（巻線切替制御部）22 B の構成を示す。例えば、巻線数 10, 50, 100 ターンの

10

20

30

40

50

巻き線から、スイッチ S W 1 とスイッチ S W 2 を共に閉じることによって、160ターンの巻線特性のアンテナ特性を得る。また、スイッチ S W 1 のみ閉じることによって60ターンの巻線特性のアンテナ特性が得られる。

【0032】

(動作説明)

次に、本第1実施形態の動作、特に初期の生体認証を中心にしたカード起動制御動作について説明する。

【0033】

生体認証を行うために、先ず、パワー制御部(電力供給制御部)22は生体認証判定部23のみに電力を供給し、カードの他の各構成機能部には電力供給を禁止するように機能する(本人認証工程)。

10

【0034】

続いて、生体認証判定部23が本人認証した場合のみ電力供給許可信号をパワー制御部22に送出する(給電許可信号送出工程)。この電力供給許可信号によりパワー制御部22から生体認証判定部23を除くカードの他の機能部へ電力供給を行う(電力供給工程)。その後、カード用リーダ/ライタ10、11との間で準拠している認証手順による相互認証を行なう認証工程に入る。

【0035】

次に、本第1実施形態の上記動作を図3に基づいて更に詳細に説明する。

図3は、カード用リーダ/ライタ10、11からのアンテナ給電を受けて行う本ICカード100の起動制御動作を示すフローチャートである。

20

【0036】

本ICカード100を起動状態に設定し(ステップS101)、当該本ICカード100をカード用リーダ/ライタ10、11に近づけると、本ICカード100はカード用リーダ/ライタ10、11から電磁波を検出する(ステップS102)。パワー制御部22はアンテナ21からの交流電流を整流し直流電力を得た後(ステップS103)、本人認証動作に入る(認証動作工程)。

【0037】

この認証動作工程では、先ず、生体認証判定部23のみを起動させて(ステップS104)、生体認証モード状態に設定し、生体認証モードに入っていることを利用者へ報知(ステップS105)する。これを報知する手段については、鳴音、振動、LEDや表示等、可能な何れかの手段(例えば鳴音発信)にて行う。

30

【0038】

ここで、生体認証とは、一般的な指紋、虹彩、顔、静脈、網膜、声紋、筆跡、および音声等の個人の特徴を、体質的に捉えた生体情報を使用して本人である証を検出するものである。そして、予め装備された前記個人の何れかの特徴を検出する手段(図示せず)から、本人確認のための生体情報が入力されたかどうかを判定し(ステップS106)、生体情報の検出がされない場合は、予め決められた時間(N)に至るまで監視し(ステップS109)、タイマ値をカウントアップ(ステップS107)して生体情報の入力があるまで待ち続ける。定められた時間経過後はタイムアウトして(ステップS110)、初期状態へ移行する。

40

【0039】

生体情報が入力された場合は、予め登録されている本人の生体情報データとの認証判定を行い(ステップS108)、その認証結果が異なる場合も初期状態へ移行する。以上が「本人認証工程」である。

【0040】

次に、生体認証結果から本人確認が出来た場合(S111)は、生体認証判定部23からパワー制御部22に対して給電許可(ステップS113)が行われ、給電許可信号が送出される(給電許可信号送出工程)。

そして、この給電許可信号に基づいてパワー制御部22においては、CPU24、暗号

50

プロセッサ 25, メモリ部 26, インタフェース 28A, 28B等の各ユニットへの通電を行い(電力供給工程)、本 ICカード 100とカード用リーダ/ライタ 10, 11間の通常の暗号による相互認証処理を行なわれる(ステップ S114)。本人確認が出来ない場合(ステップ S110)には、初期状態へ移行する。

【0041】

ここで、上述した本人認証工程、給電許可信号送出工程、及び電力供給工程の各工程については、その各処理内容をプログラム化して、コンピュータに実行させるように構成してもよい。

【0042】

次に、カード用リーダ/ライタ 10, 11と ICカード 100間の信号制御を、図 4に基づいて説明する。この図 4は、カード用リーダ/ライタ 10, 11と ICカード 100との間の信号制御シーケンス図である。

【0043】

マスタ側として動作するリーダ/ライタ 10は、一定間隔での問合せ要求である応答待ち信号を、無線搬送波と共にスレーブ側として動作する ICカード 100に送る。

ICカード 100側では、この無線搬送波をアンテナ構造体 21で受信し整流して直流電力を得、生体認証判定部 23だけを起動して生体認証処理を行い、本人確認が完了した場合にパワー制御部 22に給電許可信号を与え、本 ICカード 100の他の CPUなどの機能部を起動し、マスタ側であるカード用リーダ/ライタ 10, 11へ通常行なう相互認証処理を開始する為の応答信号を返すことによってマスタ側へ通知する。これに対して、マスタ側は、ACK(了解)信号を返信して通常の暗号化処理による相互認証処理シーケンスへ移行する。

【0044】

ここで、相互認証処理とは、ICカード 100とカード用リーダ/ライタ 10, 11が共に不正なものではなく正規のものであることを何らかの方法で認証する処理をいう。

【0045】

〔第1実施形態の効果〕

この第1の実施形態では、上述したように、アンテナ巻線 21Aおよびパワー制御部 22Aを稼働させて先ず生体認証判定部 23だけを起動して生体認証処理を行い、本人確認が完了した場合にパワー制御部 22Aによって他の構成各部への給電許可を与えるようにしたので、ICカード 100の所持者が本人であることを認証されることを前提として、無線周波数等の RFインタフェースの異なる内容の ICカードを統合化して一の ICカード 100にしたものが有効に機能する構成とした。このため、この第1の実施形態によると、この多様化した ICカードの一元化によって管理面や携帯面の利便性が向上すると同時にカードの盗難や紛失などに際しても高い安全性が得られるという従来にない優れた非接触 ICカードを提供することができる。

【0046】

即ち、上記第1の実施形態によると、以下に示す効能を奏する。

第一の効果として、カードの所持者が本人であることを認証しない限りカードとして一切動作しないので、カードの盗難、紛失などに際して高い安全性が得られる。第二の効果として、無線周波数等の RFインタフェースの異なる ICカードの統合化までが可能になり、多様化するカードの一元化によって管理面や携帯面の利便性が向上する。

【0047】

〔第2の実施形態〕

次に、本発明の第2の実施形態を図5に基づいて説明する。

この図5に示す第2の実施形態は、前述した第1の実施形態における前述したパワー制御部(電力供給制御部) 22Aに、暗証番号検出判定部 23Aを併設し ICカード 200とした点に特徴を有する。

【0048】

そして、前述した ICカード 200における本人認証において、何らかの異変によって

本人確認が適切に出来ない場合には、そのときに備えてバックアップとして上述した暗証番号検出判定部 2 3 A を設けてあるので、この第 2 実施形態では、生体認証の失敗を暗証番号の入力で回避するようにした。

【0049】

この場合、前述したパワー制御部（電力供給制御部）2 2 A には、別に併設されたメモリに前述した暗証番号検出判定部 2 3 A から入力される本人の暗証番号と同一の暗証番号が予め記憶されている。そして、パワー制御部 2 2 A に前述した暗証番号が入力された場合には、直ちにこれに対応して機能し、前述した生体認証によって本人確認が成された場合と同様に、前述したパワー制御部 2 2 A から他の構成各部へ、給電許可を与えるようにした。

10

その他の構成、およびその作用効果については、前述した第 1 の実施形態の場合と同一となっている。

【0050】

〔第 3 の実施形態〕

次に、本発明の第 3 の実施形態を図 6 乃至図 7 に基づいて説明する。

この図 6 乃至図 7 に示す第 3 の実施形態は、前述した第 1 又は第 2 の実施形態の構成要素に加えて、不正操作ロック機能部 2 3 B を設けた点に特徴を有する。

【0051】

これは、前述した生体認証判定部 2 3 による本人認証が確認出来なかった場合は不正に第三者の手に渡った可能性があることから、かかる場合には、この不正操作ロック機能部 2 3 B を機能させて以後の IC カード 3 0 0 の動作を不可能にする「セキュリティロック状態」を設定するようにしたものである。

20

【0052】

即ち、本第 3 実施形態にあつては、前述したパワー制御部（電力供給制御部）2 2 A に不正操作ロック部 2 3 B を併設し、前記生体認証判定部 2 3 での本人認証が失敗した場合には、前記不正操作ロック部 2 3 B が機能して前記生体認証判定部 2 3 と前記パワー制御部 2 2 A を稼働させないように不正操作ロック状態に設定することを特徴とする。

ここで、上記不正操作ロック部 2 3 B は、外部から解除指令が入力された場合には事前に設定された前記不正操作ロック状態を解除するロック状態解除機能を備えている。

【0053】

30

そして、前述したセキュリティロック状態となった本 IC カード 3 0 0 を再度カード用リーダ／ライタ 1 0, 1 1 へ近づけても本 IC カード 3 0 0 が使用できないようにするには、具体的には、生体認証判定部 2 3 や暗証番号検出判定部 2 3 A 等への電力供給の遮断状態を保持したり、或いはパワー制御部 2 2 A からの電力供給の遮断状態を保持する機能を供えることで、実現できる。

このセキュリティロック機能としては、その解除を何らかの方法で可能なように構成する場合と、その解除を一切許さないように構成する場合と、の二種類の方法がとることができる。

【0054】

更に又、交通機関等での使用を目的として、本人認証確立後の一定時間だけを通電可能とするタイマ監視機能部 2 3 C をパワー制御部 2 2 A に併設し、これにより不正に使用されないようにしてもよい。

40

【0055】

図 7 に、本第 3 の実施形態における動作説明用のフローチャートを示す。

この図 7 は、前述した第 1 実施形態では、その動作フローチャート（図 3 参照）のステップ S 1 1 2 が初期状態に戻るのに対し、この本第 3 の実施形態では、ステップ S 1 1 2 が「セキュリティロック状態」になる点を除いて前述した図 3 の動作フローチャートと全く同一となっている。

【0056】

その他の構成およびその作用効果は、前述した第 1 実施形態の場合と同一となっている

50

。

【0057】

〔第4の実施形態〕

次に、本発明の第4の実施形態を図8に基づいて説明する。

この図8に示す第4の実施形態は、前述した第1の実施形態におけるカード用リーダ／ライタ10、11を一体化してカード用リーダ／ライタ12とすると共にアンテナA（アンテナ巻線21A）とアンテナB（アンテナ巻線21B）とを完全に分離した点に特徴を有する。ここで、符号23Nは、前述した第2乃至第3の各実施形態における本人認証系を本実施形態では総て装備して成る生体認証判別部等を示す。

【0058】

この図8において、本第4実施形態におけるの非接触ICカード400は、上述したように、1つのアンテナ巻線21Aを生体認証判別部等23Nに専用に給電Aとして電力供給する構成（一次系電源）と、他のアンテナ巻線21Bをパワー制御部22Aを介して生体認証判定部等23N以外のカードの機能部に給電Bとして電力を供給する構成（二次系電源）とを備えている。更に、前述した他のアンテナ巻線21Bによって前記カード用リーダ／ライタ12と相互通信が実行されるように構成されている。

【0059】

この場合、カード用リーダ／ライタ12は、一次系電源としてアンテナ巻線21Aに電力供給するための無線電波Aを出力しており、同時に、前述した各実施形態の場合と同様に、情報通信をアンテナ巻線21Bを介して無線電波Bを使って実行するように構成されている。

【0060】

ここで、本第4実施形態にあつては、図8に開示した上記生体認証判別部等23Nは、前述した第2実施形態の図5に開示した生体認証判定部23及び暗号番号検出判定部23A、第3実施形態の図6に開示した暗証番号検出判定部23A、不正操作ロック部23、及びタイマ監視機能部23Cをも包含するように構成されている。そして、この生体認証判別部等23Nを中心とした一次系電源と、生体認証判定部等23N以外のカードの機能部に電力供給する二次系電源との電力供給系を、相互に完全に分離することによって、更にセキュリティレベルを上げられるという利点がある。

その他の基本的な構成およびその作用効果については、前述した第1実施形態の場合と同一となっている。

【0061】

〔第5の実施形態〕

次に、本発明の第5の実施形態を説明する。

この第5実施形態は、上述した第1乃至第4の各実施形態に係る非接触ICカード100、200、300、又は400を構成するICチップを含むカード片を携帯端末本体（図示せず）側に着脱自在に搭載するように構成し、この携帯端末本体側に予め装備したマルチRF対応のアンテナ構造体と一体になって、前述した非接触ICカードの場合と同様の機能を当該携帯端末装置に形成したことを特徴とする。

【0062】

この場合、携帯端末自体が電源を有するので、その電源を利用し、或いはテンキーなどの入力機能を利用して暗証番号を入力したりすることができる。更に、携帯端末に備えられているカメラの撮像機能を顔や指紋等の生体情報入力部として使用し、又、当該携帯端末に備えられている音声送話機を音声の生体情報入力部として利用することもできる。このため、上述した各実施形態における非接触ICカード単体に比べて、当該携帯端末には文字、音声、画像等の情報入力機能が豊富に備わっているので、本人認証機能の実現はより容易である。

その他のICチップの構成およびその作用効果については、前述した各実施形態の場合と同一となっている。

【0063】

上述した各実施形態にあっては、以上のように構成され機能するので、以下に示す効果を得ることができる。

第一の効果として、カードの所持者が本人であることを認証しない限りカードとして一切動作しないので、カードの盗難、紛失などに際して高い安全性が得られる。

第二の効果として、無線周波数等の R F インタフェースの異なる I C カードの統合化までが可能となり、多様化するカードの一元化によって管理面や携帯面の利便性が向上する。

【 0 0 6 4 】

更に、本人であるにもかかわらず、本人認証が万一失敗した場合でも、本人であれば使えるよう予備の認証機能としての暗証番号検出判定部 2 3 A を備えることにより、利便性を更に増すことができる。また、上記各実施形態によると、セキュリティロック機能およびタイマ監視機能を設ける等により、その用途に応じてきめ細かく安全性の向上を図ることが可能となった。

【図面の簡単な説明】

【 0 0 6 5 】

【図 1】本発明の第 1 実施形態に係る I C カードの構成を示すブロック図である。

【図 2】図 1 に開示した I C カードのアンテナ構造体及び巻線切替え制御部を示す模式的説明図である。

【図 3】図 1 に開示した I C カードの起動制御を示すフローチャート図である。

【図 4】図 1 に開示した I C カードとカード用リーダ／ライタ間の信号シーケンス図である。

【図 5】本発明の第 2 実施形態に係る I C カードの構成を示すブロック図である。

【図 6】本発明の第 3 実施形態に係る I C カードの構成を示すブロック図である。

【図 7】図 6 に開示した I C カードの起動制御を示すフローチャート図である。

【図 8】本発明の第 4 実施形態に係る I C カードの構成を示すブロック図である。

【符号の説明】

【 0 0 6 6 】

1 0, 1 1, 1 2 カード用リーダ／ライタ

1 0 0, 2 0 0, 3 0 0, 4 0 0 非接触 I C カード

2 1 アンテナ構造体

2 1 A アンテナ（アンテナ巻線 A）

2 1 B アンテナ（アンテナ巻線 B）

2 2 主制御部

2 2 A パワー制御部（電力供給制御部）

2 2 B 切替え制御部（巻線切替制御部）

2 3 生体認証判定部

2 3 A 暗証番号検出判定部

2 3 B 不正操作ロック機能部

2 3 N 生体認証判別部等

2 4 C P U （プロセッサ）

2 5 暗号プロセッサ

2 6 メモリ部

2 6 A R O M

2 6 B R A M

2 6 C E E P R O M

2 7 信号選択部

2 8 R F インタフェース部

2 8 A R F インタフェース A

2 8 B R F インタフェース B

3 0 給電線

10

20

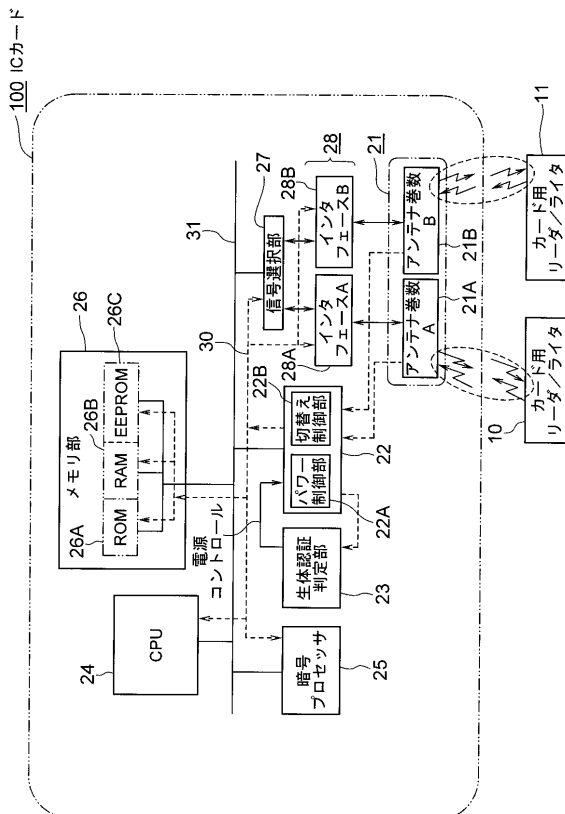
30

40

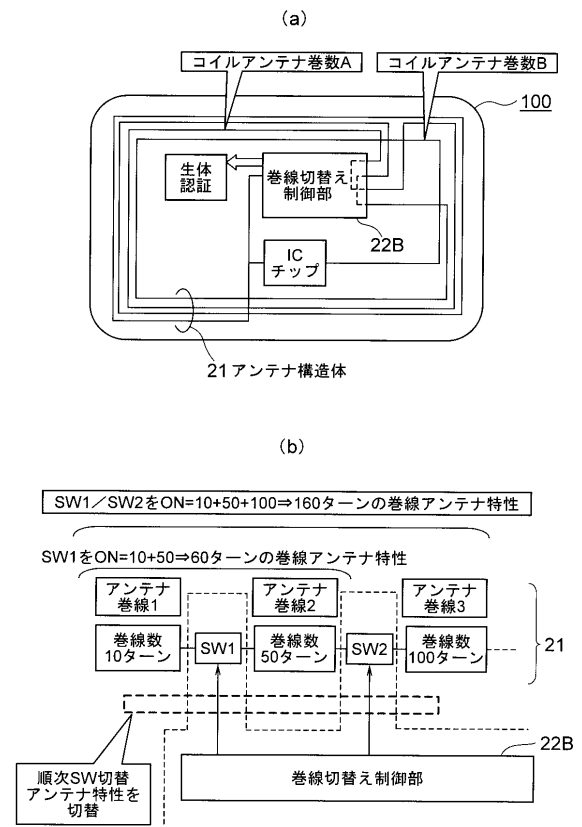
50

3 1 信号バス

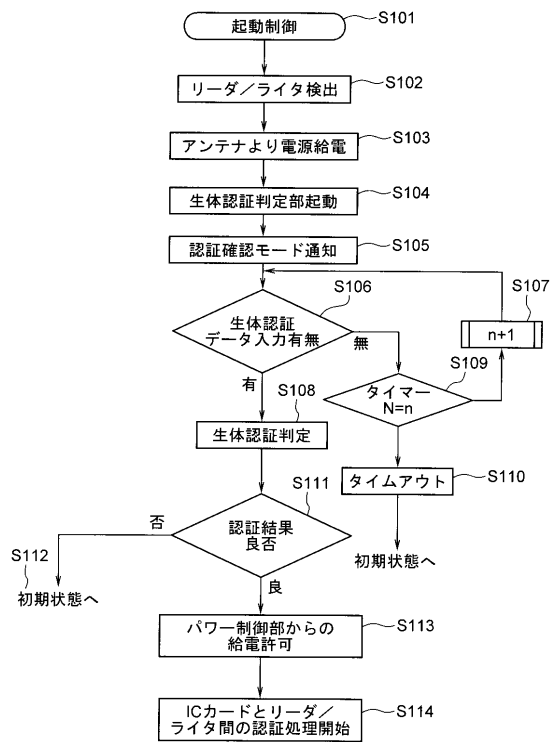
【図 1】



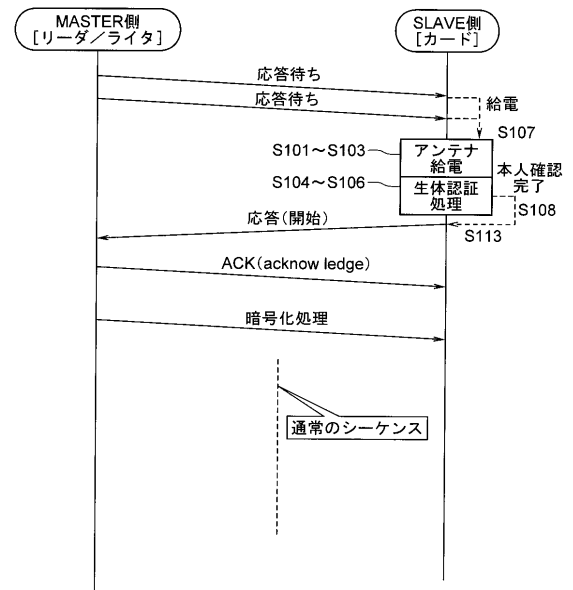
【図 2】



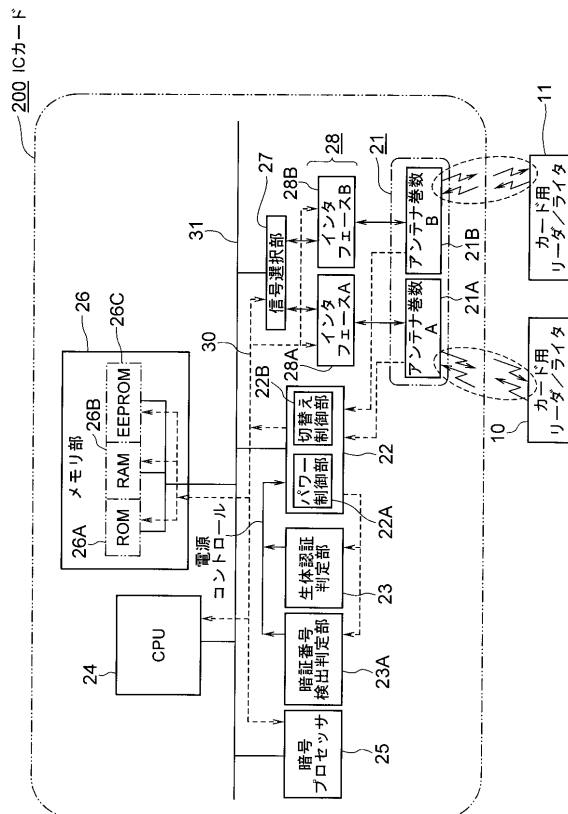
【図 3】



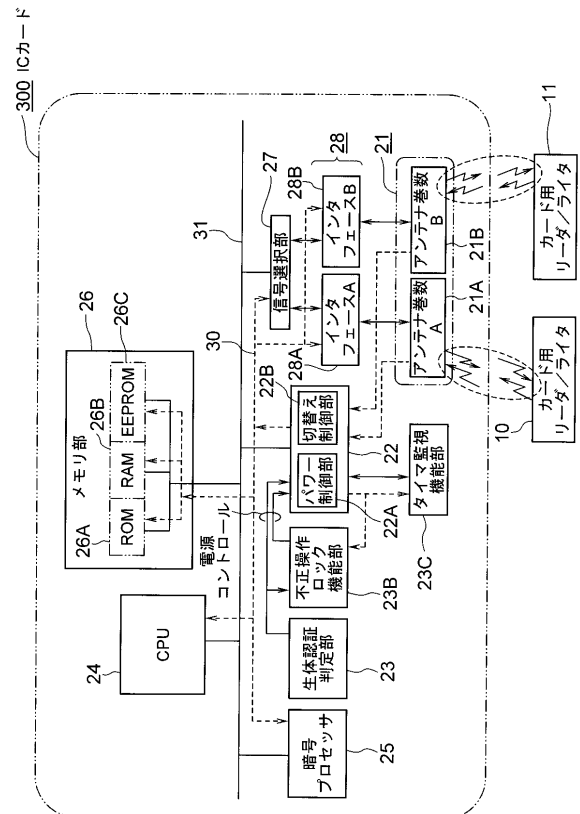
【図 4】



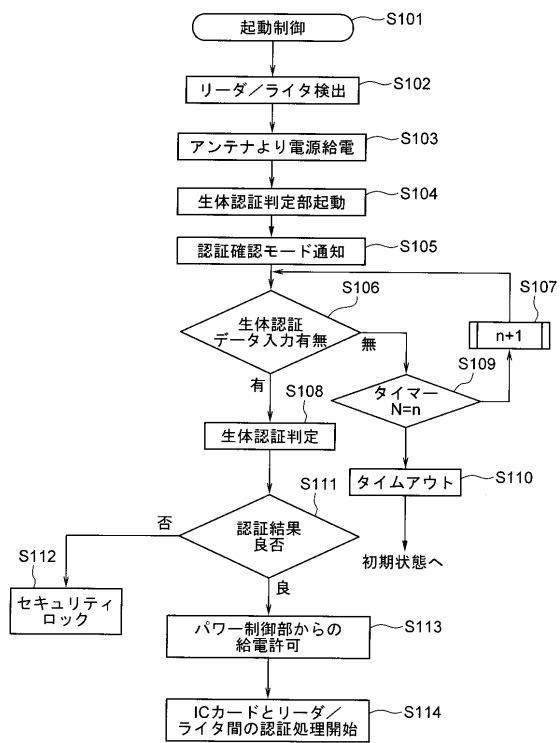
【図 5】



【図 6】



【図 7】



【図 8】

