

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4789092号  
(P4789092)

(45) 発行日 平成23年10月5日(2011.10.5)

(24) 登録日 平成23年7月29日(2011.7.29)

(51) Int.Cl.	F I	
<b>G06K 17/00 (2006.01)</b>	G06K 17/00	Z E C F
<b>G06F 21/20 (2006.01)</b>	G06F 15/00	3 3 O G
<b>G06K 19/07 (2006.01)</b>	G06K 17/00	L
<b>G06K 19/10 (2006.01)</b>	G06K 17/00	T
<b>G06F 21/24 (2006.01)</b>	G06K 19/00	H

請求項の数 6 (全 29 頁) 最終頁に続く

(21) 出願番号 特願2008-145098 (P2008-145098)  
 (22) 出願日 平成20年5月7日(2008.5.7)  
 (62) 分割の表示 特願2002-584251 (P2002-584251)  
         の分割  
         原出願日 平成14年4月17日(2002.4.17)  
 (65) 公開番号 特開2009-3927 (P2009-3927A)  
 (43) 公開日 平成21年1月8日(2009.1.8)  
         審査請求日 平成20年6月5日(2008.6.5)  
 (31) 優先権主張番号 特願2001-118795 (P2001-118795)  
 (32) 優先日 平成13年4月17日(2001.4.17)  
 (33) 優先権主張国 日本国(JP)

特許権者において、権利譲渡・実施許諾の用意がある。

(73) 特許権者 500552386  
 株式会社モビリティ  
 東京都港区虎ノ門1-16-9 双葉ビル  
 3F  
 (72) 発明者 榊原 辰彦  
 東京都渋谷区恵比寿西2丁目8番5号 高  
 麗羅ビル8F  
 (72) 発明者 春日 一郎  
 東京都八王子市上柚木3丁目10番3号-  
 410  
 審査官 梅沢 俊

最終頁に続く

(54) 【発明の名称】 携帯電話、Rバッジ、受信装置

(57) 【特許請求の範囲】

【請求項1】

R F I D インターフェースを有する携帯電話であって、当該携帯電話のスイッチを押すことで生成されるトリガ信号又はリーダライタから送信されるトリガ信号を、当該携帯電話の所有者が第三者による閲覧や使用を制限し、保護することを希望する被保護情報に対するアクセス要求として受け付ける受付手段と、前記トリガ信号に应答して、Rバッジに対して要求信号を送信する送信手段と、前記Rバッジより識別情報を受け取って、該受け取った識別情報と当該携帯電話に予め記録してある識別情報との比較を行う比較手段と、前記比較手段による比較結果に応じて前記受付手段で受け付けた前記アクセス要求を許可または禁止するアクセス制御手段とを備え、前記アクセス制御手段は、当該比較手段で前記アクセス要求を許可するという比較結果が得られた場合は、前記アクセス要求から所定時間が経過するまでは前記被保護情報へのアクセスを許可することを特徴とする携帯電話。

【請求項2】

前記被保護情報は、プリペイドカード、キャッシュカード、デビットカード、クレジットカード、定期券、乗車券、電子マネー、鍵、会員権、診察券、健康保険証、身分証明書、アミューズメント施設のチケット、公共施設のチケット、社員証、学生証、通行証、各種証明書発行用カード、図書館の貸出カード、入退室管理カードのうち少なくとも1つに記録されたデータであることを特徴とする請求項1記載の携帯電話。

【請求項3】

請求項 1 記載の携帯電話であって、アプリケーションプログラムやデバイスドライバをインターネットを經由してダウンロードして新たな機能を追加および/または更新する手段を有することを特徴とする携帯電話。

【請求項 4】

前記新たな機能はプリペイドカード、キャッシュカード、デビットカード、クレジットカード、定期券、乗車券、電子マネー、アミューズメント施設のチケット、公共施設のチケットのうち少なくとも1つであることを特徴とする請求項 3 記載の携帯電話。

【請求項 5】

請求項 4 記載の携帯電話との間で送受信するための R F I D インターフェースを有し、個別情報の発信要求を前記携帯電話に発信する発信手段と、前記携帯電話から受信した個別情報が要求した個別情報であるか否かを判断する判断手段とを有し、前記判断手段で受信した判断情報が、前記要求した個別情報であると判断されたときに、前記携帯電話との間で処理を行うことを特徴とする受信装置。

10

【請求項 6】

請求項 1 乃至 4 のいずれか 1 つに記載の携帯電話との間で送受信するための R F I D インターフェースを有し、前記携帯電話からの要求に応じて前記識別情報を送信する手段を有することを特徴とする R バッジ。

【発明の詳細な説明】

【技術分野】

【0001】

20

本発明は R F I D インターフェースを利用した情報保護技術に関するものである。

【背景技術】

【0002】

近年、市場には膨大な数の磁気カードが流通している。一例として、クレジットカード、キャッシュカード、プリペイドカード、社員証や学生証、通行証、各種証明書発行用カード、図書館の貸出カード、入退室管理カードなどがあげられる。これらのカードは特定の目的ごとに提供されているため、場合によっては外出時に何枚ものカードを携帯しなければならない。しかしながら、カードの枚数によっては非常にかさばる上に、必要なときに必要なカードをすぐに取り出しにくいなどの問題がある。

【0003】

30

これに対する対応策として、複数のカードを可能な限り1枚にまとめる方法が考えられる。たとえば、金融機関のキャッシュカードをクレジットカードとしても利用できるようにしたカードが、デビットカードとして実用化されている。デビットカードの所有者は、店舗備え付けの端末にカードを挿入して暗証番号を入力するだけで、現金を持ち歩かずに商品を購入することができる。

【0004】

しかしながら、決済時にテンキーを使って自分で暗証番号を入力しなければならず、暗証番号漏洩の不安を拭いきれないことが普及の妨げとなっている。また、デビットカードでは磁気ストライプを利用しているため、紛失や盗難事故の際に改竄されやすいという問題もある。事実、磁気ストライプに記録されたデータを読み取り、偽造カードにコピーして使用する「スキミング」と呼ばれる被害が近年になって急増している。

40

【0005】

こうしたカードの改竄や不正使用が増えている現状を背景に、磁気カードから I C カードに切り替える動きが各業界において本格化しつつある。周知のように、I C カードとはプラスチック製のカードに I C チップを埋め込んだもので、磁気カードに比べて偽造が難しいという利点がある。また、データ記録容量が極めて大きいため、複数のカードを1枚にまとめた多目的カードを比較的容易に製造することができるという利点もある。

【0006】

しかしながら、従来のクレジットカードなど個人情報と金銭的価値の両方が付帯するカードの場合、所有者以外の第三者に不正使用された場合の被害は甚大である。一方、金銭的

50

な価値がありながら匿名性の高いカード（プリペイドカードなど）では、紛失や盗難事故の際に所有者の手元に戻ってくる可能性が極めて低いという欠点がある。さらに、金銭的な価値はなくとも個人情報が多く記録されたカード（住民カードや保健医療カードなど）であればプライバシー保護の観点からさまざまな問題が危惧される。

#### 【0007】

そこで、携帯電話、PHS、携帯情報端末（PDA）、ノートパソコンなどの携帯端末に多目的ICカードを統合したり、複数のICカードの機能を搭載したり、あるいは搭載可能な仕組み（ICカードとしての機能を実行するためのソフトを所定のサーバ等にダウンロード可能な形態で提供し、そのソフトをダウンロードする、あるいはこのようなソフトが搭載された、カード用専用チップを装着する等）を用意するなどし、この端末に対してセキュリティ対策を施す方法が検討されている。ICカードには大きく分けて接触型と非接触型の2種類があり、カードに記録されたデータを利用するには接触型の場合は専用の端末（以下、「リーダライタ」と呼ぶ）にカードを挿入しなければならないが、非接触型ではその必要がなく、リーダライタにかざすだけでよい。したがって、携帯端末をパスワードで保護し、端末にあらかじめ記録されたパスワードと所有者が入力するパスワードとが一致した場合にのみICカードの機能を利用できるようにする方式が考えられる。しかしながら、このような方式ではカード機能を利用するたびに端末にパスワードを入力しなければならない煩わしさがあり、リーダライタにかざすだけでよいという非接触型ICカードの利点が半減してしまう。また、パスワード自体は所有者個人を特定する手段にはならず、何らかの理由でパスワードが漏洩した場合に、悪意の拾得者が不正入手したパスワードを利用して端末にアクセスする可能性もある。

#### 【0008】

あるいは、携帯端末の紛失時に通常の電話機を利用して遠隔地から携帯端末を緊急制御する方法も考えられる。すなわち、プッシュボタン操作によって生成される信号を利用して携帯端末の不正使用を防止するものである。しかしながら、この方法では遠隔操作に対応した基地局の存在が不可欠になるため、確実に不正使用を防止するという意味では不十分である。

#### 【発明の開示】

#### 【発明が解決しようとする課題】

#### 【0009】

本発明は上記課題に鑑みてなされたものであり、その目的とするところは、個人情報や金銭的価値のある情報を統合して管理する場合に当該情報の第三者による不正使用を確実に防止するための情報保護システムを提供することにある。

#### 【0010】

本発明の他の目的は、かかる情報保護システムを実現するための情報保護方法を提供することにある。

#### 【課題を解決するための手段】

#### 【0011】

本発明の第1の態様によれば、RFIDインターフェースを有する携帯電話であって、当該携帯電話のスイッチを押すことで生成されるトリガ信号又はリーダライタから送信されるトリガ信号を、当該携帯電話の所有者が第三者による閲覧や使用を制限し、保護することを希望する被保護情報に対する前記アクセス要求として受け付ける受付手段と、前記トリガ信号にตอบสนองして、Rバッジに対して要求信号を送信する送信手段と、前記Rバッジより識別情報を受け取って、該受け取った識別情報と当該携帯電話に予め記録してある識別情報との比較を行う比較手段と、前記比較手段による比較結果に応じて前記受付手段で受け付けた前記アクセス要求を許可または禁止するアクセス制御手段とを備え、前記アクセス制御手段は、当該比較手段で前記アクセス要求を許可するという比較結果が得られた場合は、前記アクセス要求から所定時間が経過するまでは前記被保護情報へのアクセスを許可することを特徴とする携帯電話が得られる。

#### 【0012】

上記携帯電話において、前記被保護情報は、例えば、プリペイドカード、キャッシュカード、デビットカード、クレジットカード、定期券、乗車券、電子マネー、鍵、会員権、診察券、健康保険証、身分証明書、アミューズメント施設のチケット、公共施設のチケット、社員証、学生証、通行証、各種証明書発行用カード、図書館の貸出カード、入退室管理カードなどに記録されたデータであってよい。

【0013】

また、上記携帯電話はアプリケーションプログラムやデバイスドライバをインターネットを経由してダウンロードして新たな機能を追加および/または更新する手段を有することが好ましい。

【0014】

前記新たな機能とは、例えば、プリペイドカード、キャッシュカード、デビットカード、クレジットカード、定期券、乗車券、電子マネー、アミューズメント施設のチケット、公共施設のチケットなどである。

【0015】

また、本発明の第2の形態によれば、前記携帯電話との間で送受信するためのRFIDインターフェースを有し、個別情報の発信要求を前記携帯電話に発信する発信手段と、前記携帯電話から受信した個別情報が要求した個別情報であるか否かを判断する判断手段とを有し、前記判断手段で受信した判断情報が、前記要求した個別情報であると判断されたときに、前記携帯電話との間で処理を行うことを特徴とする受信装置が得られる。

【0016】

さらに、本発明の第3の形態によれば、前記携帯電話との間で送受信するためのRFIDインターフェースを有し、前記携帯電話からの要求に応じて前記識別情報を送信する手段を有することを特徴とするRバッジが得られる。

【発明の効果】

【0017】

以上詳細に説明したように、本発明では、携帯端末に定期券・クレジットカード・運転免許書などの個人情報を携帯端末に登録することができる。

【0018】

また、携帯端末に一意に割り振られる識別情報をもとに携帯端末の利用状況の履歴を取ることが確実に行われ悪用を防ぐことができる。

【0019】

さらに、携帯端末が悪意を持つ第三者に渡っても、対応するレッドバッジ（ICチップ）などがない限り悪用できない。

【0020】

また、これにより、利用した覚えのない料金を支払う必要がない。

【0021】

或いは、携帯端末に記憶されている個人データの流出を防ぐことが可能になる。

【0022】

また、非接触ICチップとも送受信ができ、携帯端末からICカードの識別を行うこともできる。さらに、書き込みが行え、容易にRFIDシステムが構築できる。

【発明を実施するための最良の形態】

【0023】

以下、本発明の実施形態を図面を参照して説明する。

【0024】

図1は、本発明の一実施形態による情報保護システムの概要を示すブロック図である。この情報保護システムは、第1のICアセンブリ130と第2のICアセンブリ140とで構成される。第1のICアセンブリは、中央処理装置（CPU）131と、無線通信インタフェース部132と、照合用データ記録部133と、トリガ信号受信部134と、被保護情報記録部135とを備えている。同様に、第2のICアセンブリ140は、CPU141と、無線通信インタフェース部142と、照合用データ記録部143とを備えている

10

20

30

40

50

。また、第1および第2のICアセンブリ130および140は、各アセンブリに必要なアプリケーションプログラムや制御プログラム、オペレーティングシステム(OS)、デバイスドライバなどが格納された図示しない読取専用メモリ(ROM)やランダムアクセスメモリ(RAM)を含む。

【0025】

第1のICアセンブリ130および第2のICアセンブリ140は、無線を利用して互いにデータの送受信が可能ないように構成されている。この場合、本願明細書において使用する「無線通信」という用語は、金属端子による電気的な接触を使用せずに行う通信全般を意味し、一例として、非接触自動識別システム(RFID: Radio Frequency Identification)で用いられている電磁結合方式、電磁誘導方式、マイクロ波方式、光方式の無線通信があげられる。また、米国特許第6,211,799号(特開平11-225119号)に開示されているような人体を介して電力と情報を伝送するための方法による通信も本願明細書における「無線通信」に包含されるものとする。

10

【0026】

CPU131は、第1のICアセンブリ130の各構成要素を制御し、CPU141は第2のICアセンブリ140の各構成要素を制御する。無線通信インタフェース部132および142は、それぞれが送信機能と受信機能の両方を有する。この無線通信インタフェース部132および142は、たとえばRFID技術において用いられているようなアンテナやコイルなどを有し、互いにデータの送受信を行うものである。

20

【0027】

RFIDにはさまざまな変調方式や周波数、通信プロトコルを利用したものがあるが、本発明は特定の方式に限定されるものではなく、どのような方式を利用してもよい。ICアセンブリに設けられる無線通信インタフェース部の数にも特に制限はなく、必要に応じて異なる変調方式で機能する無線通信インタフェース部を複数設けるようにしてもよい。なお、汎用性の観点から見ると、非接触型ICカードの分野で標準規格化が進められている仕様に準拠するなどの方式を採用すると好ましい。日本においては、次世代ICカードシステム研究会(the Next Generation IC Card System Study Group)やICカードシステム利用促進協議会(Japan IC Card System Application Council)が標準化活動を行っている。また、すでに確立されている国際規格として、ISO/IEC10536、ISO/IEC14443、ISO/IEC15693がある。このような規格に準拠した無線通信インタフェース部132および142とすることで、より一層汎用的かつ実用性の高い情報保護システムを構築できる可能性がある。

30

【0028】

照合用データ記録部133および143には、第1および第2のICアセンブリの照合を行うためのデータが記録されている。この照合用データが所定の条件を満たした場合に限り、被保護情報記録部135へのアクセス、例えば被保護情報記録部135に格納されたデータやプログラムへのアクセスが許可される。照合用データとは、ICアセンブリの所有者を一意に特定するためのデータであり、その内容は特に限定されるものではない。たとえばCPUの固有記号や製品番号、クレジットカード番号、これらの一意的データを複数組み合わせ合わせたものや、さらにこれを暗号化したものなどを照合用データとして利用することができる。被保護情報とは、個人情報や金銭的価値のある情報など、ICアセンブリの所有者が第三者による閲覧や使用を制限し、保護することを希望する情報またはデータであれば、どのような情報またはデータであってもよい。一例として、クレジットカード、キャッシュカード、プリペイドカード、各種会員権、診察券、健康保険証、身分証明書、公共施設のチケットなど従来のカード類に記録されたデータの他、電子マネーや電子取引情報、私的な住所録やドキュメント、画像データなど、さまざまなものが考えられる。

40

【0029】

図2に、ICアセンブリ130へのアクセス要求に対してのICアセンブリ130のCP

50

U 1 3 1における認証処理を表すフローチャートを示す。

【 0 0 3 0 】

無線通信インタフェース部 1 3 2 は、トリガ信号受信部 1 3 4 と接続され、後述するトリガ信号を受信する。CPU 1 3 1 は、トリガ信号受信部 1 3 4 でトリガ信号が受信されないときは、ICアセンブリ 1 3 0 に対するアクセス要求は無しと判定し、トリガ信号が受信された場合はアクセス要求有りとして判定する (S 1 1)。トリガ信号が検出された場合、CPU 1 3 0 は、無線通信インタフェース 1 3 2 を通じて、当該トリガ信号に回答して第2のICアセンブリ 1 4 0 に対して照合用データの送信を要求する要求信号を送信する (S 1 2)。第2のICアセンブリ 1 4 0 は、この要求信号に回答して、自己の照合用データ記録部 1 4 3 に格納された照合用データを第1のICアセンブリに送信する。CPU 1 3 1 は、無線通信インタフェース 1 3 2 を通じて照合用データが受信されたか否かを判定し (S 1 3)、受信しない場合はアクセスを拒否する (S 1 4)。照合用データが受信された場合、CPU 1 3 1 は、第2のICアセンブリ 1 4 0 から受信した照合用データとICアセンブリ 1 3 0 の照合用データ記録部 1 3 3 に格納された照合用データとの比較処理を開始させる (S 1 5)。この例では、この比較は、比較部 1 3 6 によって行われる。

10

【 0 0 3 1 】

比較部 1 3 6 における比較の結果、所定の条件が満たされたか否かを判定する。この例では、ICアセンブリ 1 4 0 から受信したデータとIC照合用データとが一致するか否かを判定し (S 1 6)、一致した場合には、CPU 1 3 1 は、アクセスを許可し (S 1 7)、被保護情報記録部から必要な情報を抽出する。一方、所定の条件が満たされなかった場合は、CPU 1 3 1 は被保護情報記録部 1 3 5 に格納されたデータへのアクセスを禁止する (S 1 4)。

20

【 0 0 3 2 】

照合用データ記録部 1 3 3、1 4 3、被保護情報記録部 1 3 5 などの記録部は、たとえばICチップなどの記録素子で実現される。なお、図1に示す例では照合用データの比較を第1のICアセンブリ 1 3 0 において行ったが、第2のICチップアセンブリ 1 4 0 側で比較を行うことも可能である。この場合、比較を行った後に第2のICアセンブリ 1 4 0 から第1のICアセンブリ 1 3 0 に比較の結果を無線通信にて通知し、CPU 1 3 1 は当該比較の結果に応じて被保護情報記録部 1 3 5 へのアクセスを許可するか否かを判断する。あるいは、第1のICアセンブリ 1 3 0 と第2のICアセンブリ 1 4 0 の両方に比較部を設け、異なる照合用データをやり取りして双方で所定の条件が満たされた場合にのみ被保護情報記録部 1 3 5 へのアクセスが可能となるような形態にしてもよい。特に後者のような二重照合形態にすることで、被保護情報記録部 1 3 5 に格納されたデータを一層確実に保護することができる。

30

【 0 0 3 3 】

上述した第1および第2のICアセンブリは、周知の半導体製造技術を用いて製造可能なものであるが、本発明は半導体による集積回路に限定されるものではない。たとえば、光電子集積回路 (OEIC) やバイオ系チップを用いて第1および/または第2のICアセンブリを製造してもよい。このようにして製造したICアセンブリは、小型チップとしてさまざまな物体に埋め込むことが可能なものである。以上、本発明の目的において、ICアセンブリを装飾品や衣類など所有者の身近におくことが可能な物体に埋め込んだものを「Rバッジ」と総称する。また、個人情報や金銭的価値の付帯する情報を携帯端末に統合したものを「多目的携帯端末」と総称する。

40

【 0 0 3 4 】

次に、図3を参照すると、第1のICアセンブリを多目的携帯端末 300 の形で実現し、第2のICアセンブリをRバッジ 400 の形で実現した例が示されている。多目的携帯端末 300 はスイッチ 301 を備え、端末の所有者がスイッチ 301 を押すことでトリガ信号が生成される。トリガ信号受信部 1 3 4 (図1) は、トリガ信号を受信すると、無線通信インタフェース部 1 3 2 に対して第2のICアセンブリとの間での通信を開始するよう

50

指示する。これ以降の照合動作については図1を参照して説明したとおりである。このようにすることで、多目的携帯端末とRバッジとの間で照合用データを照合し、照合の結果が所定の条件を満たした場合に限って多目的携帯端末を使用可能とすることができる。

【0035】

図4は、自動改札機に非接触型ICカード用のリーダライタ150を設け、このリーダライタから送信される信号(プリチャージ信号)をトリガ信号として利用した例を示している。この場合、リーダライタから発信される信号は、周知のRFIDシステムにおいて利用されている信号と同様のものである。利用者が多目的携帯端末300を自動改札機に近づけると、リーダライタ150から発信されるプリチャージ信号に应答して多目的携帯端末300がRバッジ400との通信を開始する。これ以降の照合動作については図1を参照して説明したとおりである。利用者は多目的携帯端末を自動改札機に近づけるだけで、改札を通ることができるという利点がある。自動改札機に限らず、金融機関のATMや公衆電話など、決済や金銭の移動を伴う行為に関わる多くの設備に同様の方式を応用することが可能である。

10

【0036】

また、照合結果が所定の条件を満たした後所定時間が経過する前に被保護情報へのアクセスがなされた場合はそれを許可し、この所定時間が経過した後の場合はアクセスを禁止するようにしてもよい。この場合、例えば、ICアセンブリ130または140のいずれか一方または両方にタイマを設けることで、上述のような所定時間が経過したか否かを検出することが可能となる。このような方法をとることで、ICアセンブリ130と140との間の距離が通信可能距離よりも長い場合であっても本発明を実現することが可能である。

20

【0037】

以下、多目的携帯端末300に乗車券を統合して自動改札機を通過する場合を例に説明する。なお、この例では、多目的携帯端末300(ICアセンブリ30)とICアセンブリ140との間の通信可能距離が10cmであるものとする。通常の自動改札機においては、多目的端末300を手で保持した状態で自動改札機のリーダライタ150に近づけて認証を行う。ICアセンブリ140が例えば指輪に実装されているのであれば、多目的端末300内のICアセンブリと指輪との間隔は10cmよりより短いので、問題なく認証を行うことができる。しかし、ICアセンブリ140が帽子あるいはイヤリングに実装されている場合、ICアセンブリ130とICアセンブリ140との間の距離は、通常は10cmよりも長くなり、認証を行うことができなくなる。

30

【0038】

このような場合、多目的携帯端末300を帽子あるいはイヤリングに近づけてICアセンブリ130とICアセンブリ140との距離を10cm以下としたうえで、ICアセンブリ140とICアセンブリ130との間での認証を行わせる。この動作は、例えば図3の例では、多目的携帯端末300を帽子またはイヤリングの近傍に持っていった状態で、多目的携帯端末300のスイッチ301を押してトリガ信号を発信させることにより認証を行う。

40

【0039】

また、図4の例では、リーダライタ150から発信されるプリチャージ信号に应答可能な範囲内に多目的携帯端末300がある状態で、多目的端末300を耳元に近づけて帽子又はイヤリングに実装されたICアセンブリ140との距離を10cm以下とすることで、認証を行い、携帯端末300に記録された乗車券のデータを利用可能とすることができる。このように、タイマを設けて一定のタイムラグを許容することで、ICアセンブリ130とICアセンブリ140とを実際に使用するときの距離が比較的長い場合であっても、通信可能距離の短い通信方式を採用することが可能になる。

【0040】

また、携帯端末に保存された情報を、専用のサーバにバックアップしたり、仕様内容のログファイルを保存することにより、それらの情報を必要に応じてダウンロードし、紛失前

50

の状態に復帰できるようにしてもよい。

【0041】

更に、所有者はICカードをそのまま使うかICカード機能を内蔵した携帯端末として使うかを選択することができる。さらに、ICアセンブリ130に周知のGPS機能を内蔵させることで、ICアセンブリ130を紛失したようなときにも被保護情報記録部135に記録されたデータに対する保護性を一層高めることができる。

【0042】

次に、本発明を端末等に適用した実施の形態を以下の“第1の実施の形態”～“第7の実施の形態”を例にとって詳細に説明する。

【0043】

第1の実施の形態における携帯端末10は、図5に示すように、電波認識方式でデータの送受信を行う送受信部20と、RAMやROMなどからなるメモリ30と、CPU（中央制御処理装置）などからなる制御部40から概略構成される。

【0044】

電波認識方式とは、RFIDなどに代表される送受信方式で、電気的な接続を行わずにデータが送受信されるもので、電磁結合・電磁誘導・マイクロ波・光などを利用したものである。

【0045】

この携帯端末10は、携帯電話、PHS、PDA（携帯情報端末）、ノートパソコンなどの端末である。電波認識方式で送受信するインターフェースを、以下、RFIDインターフェースと呼ぶ。

【0046】

制御部40は送受信部20やメモリ30に接続して、送受信部20やメモリ30を制御する。

【0047】

送受信部20には、発信部（或いは、送信部）と受信部を兼ね備えたもので、アンテナ22を介してRFIDインターフェースを備えた記録素子などからデータを読み取る機能や、記録素子などにデータを書き込む機能、或いは、RFIDインターフェースを備えた読取装置にデータを発信する機能などを備える。

【0048】

記録素子とは、ICチップなどである。以下、記録素子をICチップとして説明する。

【0049】

また、送受信部20は、通信制御用ICなどからなる通信制御用部21とアンテナ22などから構成される。ここでは、通信制御用部21を通信制御用ICとして以下説明する。

【0050】

さらに、送受信部20の通信制御用IC21は制御部40と接続され、制御部40からデータを読み込むためのコマンドを受け取りアンテナを介してデータを送受信するものである。

【0051】

メモリ30は制御部40と接続され、データを格納する部分や、OS（オペレーティングシステム）や通信制御用IC21を制御するデバイスドライバなどの制御プログラム、さらに、アプリケーションプログラムなどを備えている。

【0052】

RFIDインターフェースには、さまざまな変調方式・周波数・通信プロトコル等がある。そこで、図6に示すように、それぞれに対応した、通信制御用IC21やアンテナを用意し、さらに、通信制御用IC21を制御するデバイスドライバなどの制御プログラムを携帯端末10に複数用意して必要に応じて選択可能なように構成することもできる。

【0053】

また、標準化の観点からすると、密着型としてISO/IEC10536、近接型としてISO/IEC14443、近傍型としてISO/IEC15693のRFIDインター

10

20

30

40

50



フェースを備えることが好ましい。また、キャリア周波数としては、125kHz～400kHz、4.9152MHz、13.56MHz、2.45GHzのものが考えられる。

【0054】

また、RFIDインターフェースには、例えば、一方を体に装着し一方を手を持つと人体を通して送受信することが可能なものもある。このように、伝導性のあるものを媒介して送受信をおこなう機能を持たせることもできる。

【0055】

さらに、上述したものに限らず、必要に応じて他の方式のRFIDインターフェースの組み込みが可能である。

10

【0056】

また、携帯端末10には、図7のブロック図に示すように、各RFIDインターフェースに対応した送受信部20と、この各RFIDインターフェースを利用するためのデバイスドライバ(制御プログラム)31とを複数用意し、OS(オペレーティングシステム)などからなるシステム管理部32上でさまざまなアプリケーションプログラム33を動作させることができ多種多様な機能を持たせることが可能である。さらに、必要に応じて、アプリケーションプログラム33で利用するデータを格納するデータ格納部34を持つ。

【0057】

さらに、このアプリケーションプログラム33やデバイスドライバ31は、インターネットなどのネットワークからダウンロードして、新たな機能の追加や、更新することが可能である。

20

【0058】

また、ICカードにも、前述したRFIDインターフェースと同様の構成を備えている。図8に示すように、ICカード50にはICチップ51がアンテナ22と接続されている。

【0059】

記録素子であるICチップ51には、通信制御用IC21とCPUなどからなる制御部40とメモリ30を備え、アンテナ22を介してデータの送受信を行う。メモリ30は制御部40と接続され、データをメモリに格納する部分や、通信制御用IC21を制御するソフトウェアを備えている。さらに、OSを備えるようにしても良い。

30

【0060】

あるいは、通信制御する部分を集積回路とすることも可能である。

【0061】

また、図示しないが、あらゆる装置に前述したRFIDインターフェースの送受信部20を組み込むことができ、RFIDインターフェースでデータの送受信を行う機能を持たせることが可能である。

【0062】

次に、送受信部20の送受信を行う仕組みについて、電磁誘導を使って送受信する例について具体的に説明する。

【0063】

ここでは、図9に示すように、送受信部20を受信部20'と発信部(送信部)20"とに分けて説明する。

40

【0064】

まず、受信部20'では、通信制御用IC21には、制御部40から読み取りのコマンドを受けてデータの読み取りを開始する読み取り制御部211と、受信したデータを制御部40'に渡すデータ受信部212とを備える。

【0065】

読み取り制御部211は、制御部40'から読み取りのコマンドを受け取ると発信要求としてパルス発生してアンテナ22'から送出する機能を備える。また、データ受信部212は、発信部20"からのデータをアンテナ22'で受信するとデータをデコー

50

ドして制御部 40' に渡す機能を備える。

【0066】

発信部 20" には、電磁誘導によるキャパシティを蓄える蓄電部 213 と、データを送信するデータ送信部 214 と備える。

【0067】

蓄電部 213 は、アンテナ 22" で受信部 20' から発信要求としてパワーパルスを受け取ると蓄電する機能を備える。また、データ送信部 214 では、蓄電部 213 に蓄えられたエネルギーを電源としてアンテナ 22" からデータを発信する機能を備える。

【0068】

また、発信部 20" に、電源が接続される構成になっている場合には、パワーパルスを受信信号としてのみ利用し、蓄電部 213 を備えない構成とすることも可能である。

10

【0069】

送受信部 20 は、受信部 20' と発信部（送信部）20" の双方の機能を兼ね備えるものである。

【0070】

次に、本実施の形態の動作をフローチャートに従って説明する。

【0071】

ここでは、RFID インターフェースを備えた IC カードや装置からデータを受信する場合を例に、携帯端末 10 の受信の動作を図 10 のフローチャートを用いて説明する。

【0072】

20

まず、RFID インターフェースを備えた IC カードや装置などの近くに携帯端末 10 を持って行く。RFID インターフェースを備えた IC カードや装置と携帯端末 10 とが送受信可能な距離は、密着型か、近接型か、近傍型かによって違う。密着型か、近接型か、近傍型かは目的により使い分けられ、アプリケーションプログラムで選択されたデバイスドライバを用いて送受信を行う（S100）。アプリケーションプログラムからデバイスドライバに読み取りのシステムコールを呼び出すと、デバイスドライバから通信制御用 IC 21 に読み取りのコマンドが送られる（S101）。通信制御用 IC 21 は、読み取りのコマンドを受け取ると読み取り制御部 211 を介してアンテナ 22（22'）より発信要求としてパワーパルスを発生する。

【0073】

30

IC カードや装置は、発信要求としてパワーパルスを受け取り、電磁誘導で発生した電流は蓄電部 213 に蓄える（S200）。蓄電部 213 に蓄えられた電力を使用してデータをアンテナ 22" から発信する（S201）。

【0074】

携帯端末 10 は、アンテナ 22（22'）を介してデータを受信し（S103）、データ受信部 212 を介してデコードされたデータは、デバイスドライバからアプリケーションプログラムに渡される。

【0075】

次に、RFID インターフェースを備えた IC カードや装置などにデータを発信する場合を例に、携帯端末 10 の発信の動作を図 11 のフローチャートを用いて説明する。

40

【0076】

IC カードや装置では通信制御用 IC 21 に読み取りのコマンドを送る（S210）と、IC カードや装置の通信制御用 IC 21 は、読み取りのコマンドを受け取ると読み取り制御部 211 を介してアンテナ 22（22'）より発信要求としてパワーパルスを発生する（S211）。

【0077】

携帯端末 10 は、発信要求としてパワーパルスを受け取ると（S110）、それを CPU の割り込み信号として利用し、データをアンテナ 22（22"）から発信する（S111）。あるいは、電磁誘導で発生した電流を蓄電部 213 に蓄え、蓄電部 213 に蓄えられた電力を利用してデータを発信しても良い。

50

【 0 0 7 8 】

ICカードや装置は、アンテナ 2 2 ( 2 2 ' ) を介してデータを受信する ( S 2 1 2 ) 。

【 0 0 7 9 】

ここでは、携帯端末 1 0 には送受信部に受信部の機能と発信部 ( 送信部 ) の機能を備えたものについて説明したが、受信部の機能が発信部 ( 送信部 ) の機能かいずれかを一方のみを備えたものでも良い。

【 0 0 8 0 】

また、ここでは電磁誘導による例について説明したが、データを受信する側から発信要求としてポーリングしてデータを受信するようにしても良い。

【 0 0 8 1 】

さらに、送受信部 2 0 は携帯端末 1 0 に脱着可能なユニットとし ( 例えば、カード型ユニットなど ) 、さまざまな R F I D インターフェースを装着することが可能である。

【 0 0 8 2 】

あるいは、記録素子には半導体以外のものを利用して IC チップと同様の機能をもつもので構成するようにしても良い。

【 0 0 8 3 】

以上、説明したように R F I D インターフェースを備えた携帯端末 1 0 を利用して、ICカード 5 0 とデータの送受信を行うことができる。さらに、R F I D インターフェースを備えた装置ともデータの送受信を行うことができる。

【 0 0 8 4 】

また、携帯端末 1 0 で IC カード 5 0 や装置に記憶されている固有のデータを読み込むと、アプリケーションを起動することも可能である。例えば、IC カード 5 0 の情報を読み込むとインターネットに接続する。あるいは、R F I D インターフェースを組み込んだ装置から情報を読み込むと、説明書などを表示することもできる。

【 0 0 8 5 】

第 2 の実施の形態では、携帯端末 1 0 に ( IC カードで行われている ) 定期券・乗車券・クレジットカード・鍵などの機能を内蔵させる個別情報システムについて説明する。ここでは、クレジットカードなどカード機能を携帯端末 1 0 に内蔵させる場合を例に説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

【 0 0 8 6 】

他の実施の形態における個別情報

システム 1 1 は、図 1 2 に示すように、携帯端末 1 0 と R F I D インターフェースの送受信部 2 0 ' ( 受信部 ) を組み込んだ受信装置 6 0 とで概略構成される。

【 0 0 8 7 】

受信装置 6 0 は、送受信部 2 0 ' と制御部 4 0 ' が設けられ、携帯端末 1 0 から個別情報を読み取る機能を備えている。この受信装置 6 0 に携帯端末 1 0 を近づけて個別情報を読み取るようにするため、送受信部 2 0 ' には、近接型を使用することが好ましい。

【 0 0 8 8 】

携帯端末 1 0 は、図 1 3 に示すように、メモリ 3 0 上のデータ格納部 3 4 に個別情報 3 4 0 を記憶する。ここでは、個別情報 3 4 0 としてカード情報を記憶している例について説明する。

【 0 0 8 9 】

個別情報 3 4 0 には、複数のカード情報 ( 例えば、図 1 3 の A、B、C ) を記憶することも可能でその中から利用するカードを選択する機能を備える。さらに、カードに応じたアプリケーションプログラム 3 3 を複数用意し、各カードに応じた機能を持たせることが可能である。

【 0 0 9 0 】

以下、個別情報 3 4 0 をカード情報と置き換えて説明する。

【 0 0 9 1 】

次に、本実施の形態の動作を図 1 4 のフローチャートに従って説明する。

10

20

30

40

50

## 【 0 0 9 2 】

携帯端末 1 0 で、利用するカードを選択して ( S 1 2 0 )、携帯端末 1 0 を受信装置 6 0 に近づける。受信装置 6 0 では、例えば、受信装置 6 0 に設けられている読み取りスイッチの押下によって、カード情報 3 4 0 の読み取り指示を受け取ると、読み取りコマンドを送受信部 2 0 に送る ( S 2 2 0 )。そこで、送受信部 2 0 から指定されているカードのカード情報 3 4 0 ( 個別情報 ) の発信要求 ( パワーパルスなど ) を携帯端末 1 0 に発信する ( S 2 2 1 )。

## 【 0 0 9 3 】

携帯端末 1 0 では、カード情報 3 4 0 の発信要求を受け取ると選択されているカード情報 3 4 0 を発信する ( S 1 2 2 )。受信装置 6 0 では、受信したカード情報 3 4 0 が、要求したカード情報であれば処理を続行するが ( S 2 2 4 )、要求したカード情報でない場合はエラー終了する ( S 2 2 5 )。

10

## 【 0 0 9 4 】

本実施の形態では、携帯端末 1 0 にカード機能を持たせる場合について説明したが、定期券や乗車券の機能を持たせることも可能である。この場合には、受信装置 6 0 の送受信部 2 0 には、多少離れた位置から読み取り可能なように近接型を利用することが好ましい。

## 【 0 0 9 5 】

また、携帯端末 1 0 に鍵の機能を持たせることも可能である。この場合には、受信装置 6 0 の送受信部 2 0 には、やや離れた位置から読み取り可能なように近傍型または近接型を利用することが好ましい。

20

## 【 0 0 9 6 】

また、電子マネー・クレジットカード・会員権・診察券・健康保健所・身分証明書・アミューズメント施設のチケット類の機能を持たせることも可能である。

## 【 0 0 9 7 】

さらに、個別情報 3 4 0 は、携帯端末 1 0 の固体それぞれを識別する識別情報を利用することもできる。

## 【 0 0 9 8 】

さらにまた、携帯端末 1 0 を買い換えるなど置き換えをする場合には、携帯端末 1 0 に記録されている電子マネー・クレジットカード・会員権などを管理する管理会社にインターネットなどを介して置き換えを通知する。そこで、古い携帯端末 1 0 では利用できないようにし、新しい携帯端末 1 0 にその情報をダウンロードして利用するようにすることも可能である。

30

## 【 0 0 9 9 】

以上、説明したように、携帯端末 1 0 に、複数の機能を兼ね備えるようにすることが可能である。

## 【 0 1 0 0 】

第 3 の実施の形態では、識別情報を記憶する IC チップを利用して携帯端末 1 0 の使用者を識別する使用者識別システムについて説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

## 【 0 1 0 1 】

いつも身に付けているものや身近におくものに IC チップを埋め込んだものを総称して、以下、レッドバッジと呼ぶ。

40

## 【 0 1 0 2 】

第 3 の実施の形態における使用者識別システム 1 2 は、図 1 5 に示すように、携帯端末 1 0 と識別情報を記憶する携帯記録素子とで概略構成される。以下、携帯記録素子として IC チップ 5 1 とアンテナ 2 2 を組み込んだレッドバッジ 7 0 を例に説明する。

## 【 0 1 0 3 】

ここで、IC チップ 5 1 を内蔵したレッドバッジ 7 0 の例について説明する。レッドバッジ 7 0 は、第 1 のタイプとして、図 1 6 に示すように、指輪・イヤリング等の本体をアンテナ 2 2 として本来の目的と共用し、それに IC チップ 5 1 が備えられるタイプがある。

50

## 【0104】

第2のタイプとして、図17に示すように、ネクタイピン等の本体61にICチップ51とアンテナ22が内蔵される。或いは、図18に示すように、カフスポタン・バッジ・ブローチ・ペンダント・コンタクトレンズ等の本体62にICチップ51とアンテナ22が内蔵されたものなど身につけるものに内蔵されるタイプがある。

## 【0105】

他にも、財布・パスケース等の本体にICチップ51とアンテナ22が内蔵される。筆記用具・ライター等の本体にICチップ51とアンテナ22が内蔵されたものなど身近におくものに内蔵されるタイプがある。

## 【0106】

以上、例に挙げたものだけでなく、様々なものにICチップ51を内蔵することができアンテナ22の形状も多様である。

## 【0107】

また、図19に示すように、レッドバッジ70に内蔵されたICチップ51には、識別情報をメモリ30の識別情報記憶部35に格納する。識別情報記憶部35はROMなど書換不可能な記録素子で構成されることが望ましい。また、識別情報350は一意に識別できるように割り振ったものである。識別情報350はレッドバッジ70の製造時に、一意となるように書き込むようにしても良い。

## 【0108】

また、携帯端末10の近傍に複数の第三者のレッドバッジ70が存在する場合を考慮すると、携帯端末10とレッドバッジ70は、近接していないと識別情報350が読み取れないようにするほうが望ましい。近接とは、使用している携帯端末10と、使用者が衣類につけるなど身につけた状態のレッドバッジ70とが送受信可能な程度である。

## 【0109】

以上の条件を考慮に入れると、レッドバッジ70には、近接型または密着型のICチップを使用することが好ましい。さらに、レッドバッジ70と携帯端末10との送受信可能な範囲は数十センチメートル以下であることが望まれる。

## 【0110】

次に、本実施の形態の動作をフローチャートに従って説明する。

## 【0111】

識別情報350を登録する動作について、図20のフローチャートを用いて説明する。以下、フローチャートではレッドバッジ70をRバッジとする。

## 【0112】

まず、携帯端末10にレッドバッジ70の識別情報350を登録するための登録モードにする(S130)。この登録モードにする際には、暗証番号やバイオメトリックス(アイリス、声紋、指紋など)を入力しないと登録モードにならないようにし、第三者では登録できないようにする。登録モードになると、読み取り開始のコマンドを制御部40から通信制御用IC21に送信するとアンテナ22から発信要求(パワーパルスなど)を発信してレッドバッジ70の読み取りを開始する(S131)。

## 【0113】

ここで、携帯端末10のタイマーに所定の時間tを設定する(S132)。そこで、時間tが経過するまで(S134)、レッドバッジ70から識別情報350を受信したか繰り返しチェックする(S133)。

## 【0114】

時間tが経過しても、レッドバッジ70から識別情報350の受信が完了しない場合は、携帯端末10の画面上にエラーメッセージを表示する(S135)。或いは、受信した識別情報がすでに登録済みの識別情報の場合には、携帯端末10の画面上にエラーメッセージを表示する(S135)。

## 【0115】

受信した識別情報350が登録済みの識別情報でない場合は、識別情報350を携帯端末

10

20

30

40

50

10のメモリ30に格納して登録する。

【0116】

携帯端末10を使用する際に、近傍にあるレッドバッジ70の識別情報350を確認する動作について、図21のフローチャートを用いて説明する。図21のフローチャートで説明するデフォルトモード1は、操作を開始しレッドバッジ70の識別情報350が読み込まれたときに解除されるもので、通常操作を行っていない状態とする。また、デフォルトモード2は、いたずらされている可能性があるため、解除には暗証番号やバイオメトリックスなどを入力して本人である確認をする必要がある状態として以下説明する。

【0117】

まず、携帯端末10を使用する者がキー入力などの携帯端末10を使用するための初動作を行った時点で、制御部40のCPUには割り込みが発生する(S150)。割り込みが発生すると、読み取り開始のコマンドを制御部40から通信制御用IC21に送られる。通信制御用IC21は、読み取り開始のコマンドを受け取るとアンテナ22から発信要求を発信して読み取りを開始する。

10

【0118】

ここで、制御部40はタイマーに所定の時間t1を設定し(S151)、レッドバッジ70から発信した識別情報350を受信したかチェックする(S152)。時間t1が経過するまで識別情報350の受信したかを繰り返しチェックする(S153)。時間t1が経過しても、レッドバッジ70から識別情報350の受信が完了しない場合は、デフォルトモード1を設定する(S162)。

20

【0119】

識別情報350の受信が完了した場合は、受信した識別情報がメモリ30に予め登録されている識別情報と比較し、該当するものがある場合には、登録済みのレッドバッジ70が近くにあるので携帯端末10の利用が可能である(S154)。該当するものがない場合には、登録済みのレッドバッジ70ではない。そこで、登録されてない識別情報の受信回数が指定の回数より少ない場合は、デフォルトモード1を設定する(S162)が、登録されてない識別情報の受信回数が指定の回数より多い場合は、デフォルトモード2を設定する(S163)。

【0120】

登録されている識別情報を受信した場合には(S154)、さらに、所定の時間t2をタイマーに設定する(S156)。時間t2が経過するまでに(S158)、通話・メール受信・インターネットのアクセスなどの処理を開始しなかった場合は(S207)、デフォルトモード1を設定する(S162)。

30

【0121】

時間t2が経過するまでに(S158)、開始した通話・メール受信・インターネットのアクセスなどの処理が終了した場合は(S157)、所定の時間t3をタイマーに設定する(S159)。時間t3が経過するまでに(S161)、通話・メール受信・インターネットのアクセスなどの次の処理を開始した場合には(S160)、レッドバッジ70の読み込みをすることはなく、引き続き作業を行うことができる。一つの作業が終了するたびにt3が起動され(S159)、t3以内に次の作業が開始されないときは(S161)

40

【0122】

図21のフローチャートでは、携帯端末10を利用する初動作に伴って発生した割り込み処理で、近傍にあるレッドバッジ70の識別情報を確認する処理について説明したが、携帯端末10を使用する際に、この割り込みの処理と同時に使用者の操作に応じた処理が平行して実行される。

【0123】

また、デフォルトモード2の場合には、機能を停止し予め設定した動作をする。例えば、着信音を最大にして警告を発する。或いは、ダイヤルロックにすることも可能である。

【0124】

50

デフォルトモードは各携帯端末10の出荷時に設定されているが、購入後それぞれに応じた動作を使用者が任意に設定することができる。また、セキュリティレベルに応じて、携帯端末10を利用する前には暗証番号を必ず入力しなければ使用できないようにするなど、使用者で変更可能である。

【0125】

また、識別情報350の受信は、操作時の割り込み処理を使った例について説明したが、携帯端末10からポーリングをしてレッドバッジ70から識別情報350を受信し、定期的にレッドバッジ3の有り無しを確認することも可能である。

【0126】

さらに、図22に示す使用者識別システム12'のように、第2の実施の形態で説明したように、携帯端末10に定期券・乗車券・クレジットカード・鍵などの機能を内蔵させ、その機能を受信装置60で受け取る場合に、まず、携帯端末10の使用者が正当な使用者かをレッドバッジ70で確認を取るようにすることも可能である。

10

【0127】

以上、説明したようにレッドバッジに組み込んだ携帯記録素子の識別情報を確認して携帯端末10の使用を可能にすることができ、正当な使用者にのみ使用を許可することができる。

【0128】

第4の実施の形態では、携帯端末10でICチップなどの記録素子にデータを書き込む機能について説明する。前述の実施の形態と同一のものには同一符号を付して詳細な説明を省略する。

20

【0129】

第4の実施の形態における携帯記録素子書込システム13は、図23に示すように、携帯端末10と記録素子51とアンテナ22を組み込んだICカード50とで概略構成される。ここでは、記録素子51とアンテナ22を組み込んだICカード50にデータを書き込む場合を例に説明する。

【0130】

記録素子51は、識別情報350を記録しているものである。

【0131】

次に、本実施の形態の動作を図24のフローチャートに従って説明する。

30

【0132】

まず、携帯端末10で書き込みモードの選択をした時点で、制御部40のCPUには割り込みが発生する(S170)。割り込みが発生すると、読み取り開始のコマンドを制御部40から通信制御用IC21に送られる。通信制御用IC21では読み取り開始のコマンドを受け取るとアンテナ22から読み取り要求(パワーパルスなど)を発信してICカード50に登録されている識別情報350の読み取りを開始する。

【0133】

ここで、携帯端末10の制御部40はタイマーに所定の時間t1を設定し(S171)、ICカード50から発信した識別情報350を受信したかチェックする(S172)。時間t1が経過するまで識別情報350の受信を繰り返しチェックを行い(S173)、時間t1が経過しても、ICカード50から識別情報350の受信が完了しない場合は、カードの認識不能の表示を行う(S180)。

40

【0134】

識別情報350の受信が完了した場合は、受信した識別情報がメモリ30に予め登録されている識別情報と比較して、該当するものがある場合には(S174)、登録済みのICカード50であるとする。該当するものがない場合には(S174)、登録済みのICカード50ではないので書込不可の表示をする(S181)。

【0135】

登録済みのICカード50の場合は、まず、書込カウンタCを設定する(S175)。書込処理(S176)を行い正常に書込処理が終了しない場合は(S177)、書込カウ

50

ンターCが0になるまで(S178)、再度書込処理(S176)をする。書込カウンタ  
ーCが0になっても書き込みができない場合は書込不良を表示する(S182)。

【0136】

正常に書き込みが終了すると書込終了を表示する(S179)。

【0137】

以上、説明したように、RFIDインターフェースを備えた携帯端末10では、受信した  
デジタルチケットなどのデジタル情報をICカード50に書き込むことが可能である。ま  
た、携帯端末10を利用してインターネットなどの銀行からキャッシングしてICカード  
50に書き込むことも可能である。

【0138】

さらに、図25に示す携帯記録素子書込システム13'のように、ICカード50に書き  
込みを行う際、第3の実施の形態で説明したように携帯端末10の利用者が正当な使用者  
かをレッドバッジ70で確認を取るようにすることも可能である。

【0139】

これにより、正当な携帯端末10の利用者のみICカード50に書き込みが行える。

【0140】

第5の実施の形態では、インターネットなどの回線を利用して携帯端末10やICカード  
50の利用状況を管理する第1の利用管理システムについて説明する。前述の実施の形態  
と同一のものには同一符号を伏して詳細な説明を省略する。

【0141】

第5の実施の形態における利用管理システム14は、図26に示すように、携帯端末10  
やICカード50などの記録素子とRFIDインターフェースの送受信部を組み込んだ装  
置90と管理サーバ100とが通信回線110を介して接続される。さらに、通信回線1  
10には、銀行の端末やネットバンクなどの金融機関120が接続される構成になっても  
良い。

【0142】

この携帯端末10やICカード50などの記録素子には、各個体が一意に識別できる識別  
情報350が書換不可能に記録されている。また、携帯端末10には、RFIDインター  
フェースの送受信部20を備え、識別情報350を発信する機能を備える。さらに、携帯  
端末10には、通信回線送信部25を備え、通信回線を介してインターネットなどに接続  
する機能を備えている。

【0143】

ここでは、装置90は、自動販売機にRFIDインターフェースの送受信部を組み込んだ  
ものを例に説明する。装置90より、RFIDインターフェースを備える携帯端末10や  
ICカード50などと送受信することが可能で、代金を携帯端末10やICカード50に  
記録されているプリペイドカードやキャッシュカードなどから代金を受領する機能を備え  
ている。

【0144】

また、装置90には、管理サーバ100と通信回線110を介して送受信を行うサーバ接  
続部80を備える。さらに、装置90には、装置毎に割り振られる装置番号91を記録し  
ている。

【0145】

管理サーバ100は、携帯端末10やICカード50の識別情報350とその利用情報と  
をともに通信回線110を介して受信し、利用内容を表す利用情報を管理する管理部を備  
える。

【0146】

通信回線110は、専用回線やインターネットなどである。情報管理の信頼性の観点から  
、セキュリティの確保されているものが好ましい。

【0147】

次に、本実施の形態の動作を携帯端末10を例に、図27のフローチャートと図28の携

10

20

30

40

50



帯端末10の画面の遷移図に従って説明する。

【0148】

まず、携帯端末10では、図28の画面の遷移図に示すように、メニューからプリペイドカードのモード1000～商品購入モード1001～自動販売機モード1002を選択する(S300)。ここで、識別情報350を携帯端末10のRFIDインターフェースから自動販売機90に発信すると、携帯端末10には、個人認証中の画面1003が表示される(S301)。以下、自動販売機90と携帯端末10とは、RFIDインターフェースで送受信されるものとする。

【0149】

自動販売機90では、識別情報350を受け取ると、携帯端末10の識別情報350と自動販売機90の装置番号91とを管理サーバ100にサーバ接続部80から送信して、残高確認及びブラックリストとの照合を行う(S400)。管理サーバ100では、識別番号350から携帯端末10の所有者の個人データをチェックする。さらに、ブラックリストのチェックを行う(S500)。

10

【0150】

あるいは、一度受信したブラックリストを自動販売機90に記憶しておき、自動販売機90でチェックを行うようにすることも可能である。これにより、管理サーバ100との送受信の時間に要する時間を短縮し、利便性を高めることも可能である。

【0151】

以下、自動販売機90と管理サーバ100とは、サーバ接続部80から送受信されるものとする。

20

【0152】

自動販売機90では、管理サーバ100でのチェック結果より個人データ及びブラックリストに問題がある場合は(S400)、携帯端末10に購入不可を発信する。携帯端末10には使用不能を表す画面1007を表示する(S302)。

【0153】

また、個人データ及びブラックリストに問題が無ければ(S400)、携帯端末10に購入許可を発信する。携帯端末10には商品の選択画面1004を表示する(S303)。

【0154】

自動販売機90で商品を選択すると(S401)、自動販売機90から携帯端末10に商品代金の引き落としデータが送られる(S402)。携帯端末10では、代金減算処理が行われ、処理中の画面1005が表示される(S304)。さらに、このとき携帯端末10から代金引き落としの処理が正常に行われなかった場合には(S402)、利用情報としてNGの通知が自動販売機90から管理サーバ100に送信され、個人データまたはブラックリストが更新される(S501)。

30

【0155】

自動販売機90では、携帯端末10から代金引き落としの処理が正常に行われたが(S402)、商品の払い出しが正常に行われなかった場合には(S403)、利用情報としてNGの通知を自動販売機90から管理サーバ100に送信され、正常に動作しなかった自動販売機90の装置番号91が記録される(S502)。

40

【0156】

また、携帯端末10から代金引き落としの処理が正常に行われ(S402)、さらに、商品の払い出しが正常に行われた場合には(S403)、購入処理完了を自動販売機90から携帯端末10に発信する。携帯端末10では残金が画面1006に表示される。(S305)。さらに、利用情報として購入情報が自動販売機90から管理サーバ100に送信され、履歴として記録される(S503)。

【0157】

ここでは、携帯端末10について説明したがICカード50でも同様に行うことができる。

【0158】

50

また、自動販売機 90 から商品が正常に払い出しされなかった場合には、携帯端末 10 の通信回線送信部 25 より通信回線 110 を介して管理サーバ 100 に接続して、携帯端末 10 の識別番号 350 と自動販売機 90 を利用した利用情報とをともに、装置番号 91 よりどの自動販売機 90 を利用したかが確認でき、代金の払い戻しを受けることも可能である。

【0159】

さらに、自動販売機 90 の装置番号 91 を携帯端末 10 の R F I D インターフェースの送受信部 20 を介して受信し、利用情報と携帯端末 10 の識別情報 350 と装置番号 91 とを、携帯端末 10 の通信回線送信部 25 より通信回線 110 を介して管理サーバ 100 に送信することも可能である。

10

【0160】

ここでは、携帯端末 10 をプリペイドカードとして利用した場合について説明したが、携帯端末 10 をキャッシュカード・デビットカード・ポイントカード・スマートカードクレジットカードなどとして利用した場合でも同様に行える。

【0161】

また、ここでは情報はセキュリティ上、暗号化されて管理サーバに送信されることが好ましい。

【0162】

以上、説明したように、携帯端末 10 に一意に割り振られる識別情報 350 と利用情報を関連付けて管理することにより携帯端末 10 の利用履歴をとることができる。

20

【0163】

携帯端末 10 に G P S ( G l o b a l P o s i t i o n i n g S y s t e m ) 機能を備え、位置情報を取得して携帯端末 10 の位置を正確に把握することにより、装置番号 91 とを比較することで不正利用を防ぐことが可能である。

【0164】

さらに、図 29 に示す利用管理システム 14' のように、携帯端末 10 を使用する際、第 3 の実施の形態で説明したように携帯端末 10 の使用者が正当な使用者かをレッドバッジ 70 で確認を取るようにすることも可能である。

【0165】

これにより、正当な携帯端末 10 の利用者のみ携帯端末 10 を使用することができる。

30

【0166】

第 6 の実施の形態では、インターネットなどの回線を利用して携帯端末 10 や I C カード 50 にキャッシュカードやプリペイドカードの機能を登録する第 2 の利用管理システムについて説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

【0167】

第 6 の実施の形態における利用管理システム 15 は、図 30 に示すように、携帯端末 10 や I C カード 50 と R F I D インターフェースの送受信部 20 を組み込んだ装置 90' と管理サーバ 100 とが通信回線 110 を介して接続される。さらに、通信回線 110 には、銀行の端末やネットバンクなどの金融機関 120 が接続される。

40

【0168】

装置 90' は、R F I D インターフェースの送受信部 20 を備えたプリペイド購入機 90' とし、携帯端末 10 や I C カード 50 に対して、プリペイドカードの残高の書換が行われるものを例に説明する。さらに、装置 90' には、装置毎に割り振られる装置番号 91 を記録している。

【0169】

次に、本実施の形態の動作を図 31 のフローチャートと図 32 の携帯端末 10 の画面の遷移図に従って説明する。

【0170】

まず、携帯端末 10 では、図 32 の画面の遷移図に示すように、メニューからプリペイド

50

カードのモード1100～現金加算モード1101を選択する(S310)。ここで、識別情報350をRFIDインターフェースで携帯端末10からプリペイド購入機90'に発信すると、携帯端末10には、個人認証中の画面1102が表示される(S311)。

【0171】

プリペイド購入機90'では、識別情報350を受け取ると、携帯端末10の識別情報350をサーバ接続部80から管理サーバ100に送信して、残高確認及びブラックリストとの照合を行う(S410)。管理サーバ100では、識別番号350から携帯端末10の所有者の個人データをチェックする。さらに、ブラックリストのチェックを行う(S510)。以下、プリペイド購入機90'と管理サーバ100とは、サーバ接続部80から送受信されるものとする。

10

【0172】

プリペイド購入機90'では、個人データ及びブラックリストに問題がある場合は(S410)、携帯端末10に加算不可を発信する。携帯端末10では加算不能を表す画面1106を表示する(S312)。

【0173】

また、個人データあるいはブラックリストに問題が無ければ(S410)、携帯端末10に購入許可を発信する。携帯端末10には加算金額の選択画面1103を表示する(S313)。プリペイド購入機90'では、加算金額が選択される(S411)と携帯端末10に加算金額のデータを送る(S412)。

【0174】

ここで、指定された金額が金融機関120に残高があるかを確認し(S412)、不足の場合は、携帯端末10に残金不足を発信して残金不足のエラー画面1107を表示する(S314)。不足に問題がない場合は、加算処理が行われ、処理中の画面1104が表示される(S315)。さらに、このとき携帯端末10から加算処理が正常に行われなかった場合には(S413)、利用情報としてNGの通知が管理サーバ100に送信され、個人データにエラーが記録される(S511)。さらに、携帯端末10には加算処理異常のエラー画面1008が表示される(S316)。

20

【0175】

携帯端末10から加算処理が正常に行われた場合には(S413)、残高が携帯端末10の画面1108に表示され(S317)、利用情報として加算情報とプリペイド購入機90'の装置番号91とが管理サーバ100に送信され履歴として記録される(S512)。

30

【0176】

また、銀行などの金融機関120から引き落として携帯端末10に加算処理をする例について説明したが、プリペイド購入機90'に現金を投入して携帯端末10に加算処理をすることも可能である。

【0177】

さらに、自動販売機90をプリペイドカード購入機90'として利用することも可能である。

【0178】

ここでは、携帯端末10をプリペイドカードとして利用した場合について説明したが、キャッシュカード・デビットカード・クレジットカード・会員権・診察券・健康保健所・身分証明書・アミューズメント施設のチケット類などでも同様におこなうことが可能である。

40

【0179】

また、本実施の形態では、RFIDインターフェースをもつ専用機90'を例に説明したが、金融機関120から通信回線110を介して直接引き落として携帯端末10に加算処理をし、さらに、管理サーバ100へ携帯端末10の識別情報350と利用情報と送信するようにすることもできる。

【0180】

50

各種クレジット会社との通信回線 110 を介して送受信することにより、クレジットカードの機能を携帯端末 10 に追加することも可能である。

【0181】

以上、説明したように、携帯端末 10 にカードなどの機能を持たせることができ、さらに、識別番号 350 から携帯端末 10 に登録されている全ての利用状況を管理することができる。

【0182】

さらに、図 33 に示す利用管理システム 15' のように、携帯端末 10 に加算処理をする際に、第 3 の実施の形態で説明したように携帯端末 10 の使用者が正当な使用者がをレッドバッジ 70 で確認を取るようにすることも可能である。

10

【0183】

これにより、正当な携帯端末 10 の利用者のみ携帯端末 10 に加算処理をすることができる。

【0184】

第 7 の実施の形態では、RFID インターフェースを持つ携帯端末 10 同士の送受信について説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

【0185】

図 34 に示すように、携帯端末 10 と携帯端末 10 とを近づけることにより RFID インターフェースを使用して送受信を行うことが可能である。例えば、デジタルマネー・着メ

20

ロ・待ち受け画面などのデジタル情報を相手側の携帯端末 10 に渡すことが可能である。

【図面の簡単な説明】

【0186】

【図 1】本発明の一実施形態による情報保護システムの概要を示すブロック図である。

【図 2】IC アセンブリへのアクセス要求に対しての IC アセンブリの CPU における認証処理を表すフローチャートである。

【図 3】多目的携帯端末と R バッジの説明図である。

【図 4】自動改札機に非接触型 IC カード用のリーダライタを設けた例の説明図である。

【図 5】RFID インターフェースを備えた携帯端末の構成を表す図である。

【図 6】複数の RFID インターフェースを備えた携帯端末の構成を表す図である。

30

【図 7】携帯端末のソフトウェアの構成を表す図である。

【図 8】IC カードの構成を表す図である。

【図 9】電磁誘導による送受信の仕組みを示す図である。

【図 10】データを受信の動作を表すフローチャートである。

【図 11】データを発信の動作を表すフローチャートである。

【図 12】個別情報システムの構成を表す図である。

【図 13】携帯端末に個別情報が格納されているようすを示す図である。

【図 14】個別情報システムの動作を示すフローチャートである。

【図 15】使用者識別システムの構成を表す図である。

【図 16】レッドバッジの例を表す図である。

40

【図 17】レッドバッジの例を表す図である。

【図 18】レッドバッジの例を表す図である。

【図 19】レッドバッジの IC チップの構成を表す図である。

【図 20】識別情報を登録する動作を表すフローチャートである。

【図 21】識別情報より利用可能かを判断する動作を表すフローチャートである。

【図 22】レッドバッジを個別情報システムで利用した図である。

【図 23】携帯記録素子書込システムの構成を表す図である。

【図 24】携帯記録素子書込システムの動作を示すフローチャートである。

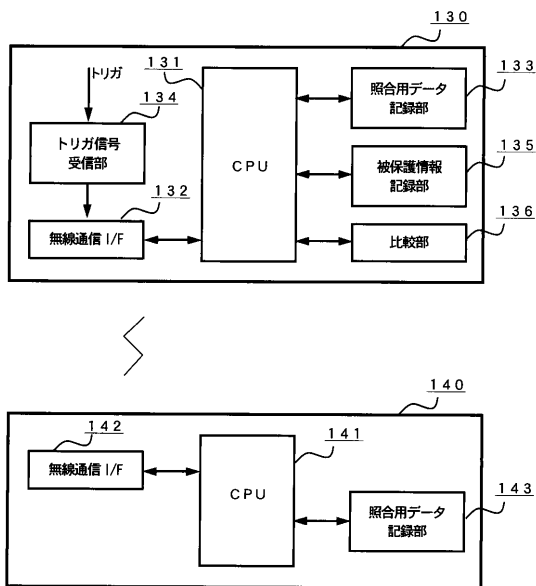
【図 25】携帯記録素子書込システムでレッドバッジを利用した図である。

【図 26】管理システムの第 1 の構成を表す図である。

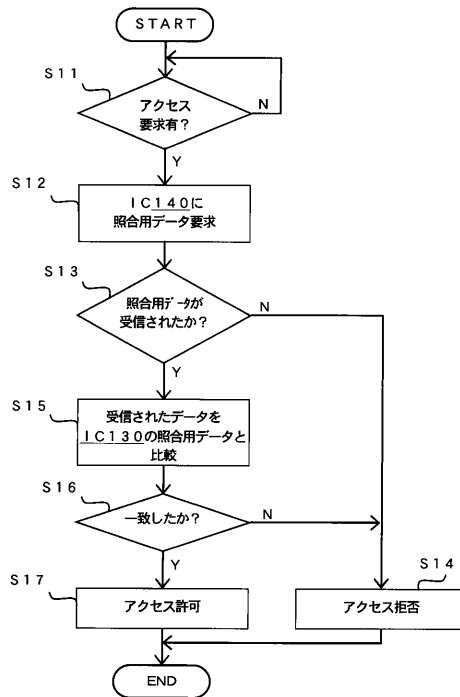
50

- 【図 27】 利用管理システムの第 1 の動作を表す図である。
- 【図 28】 携帯端末に表示される画面の例である。
- 【図 29】 第 1 の利用管理システムでレッドバッジを利用した図である。
- 【図 30】 利用管理システムの第 2 の構成を表す図である。
- 【図 31】 利用管理システムの第 2 の動作を表す図である。
- 【図 32】 携帯端末に表示される画面の例である。
- 【図 33】 第 2 の利用管理システムでレッドバッジを利用した図である。
- 【図 34】 携帯端末の間で送受信の行われる様子を示す図である。

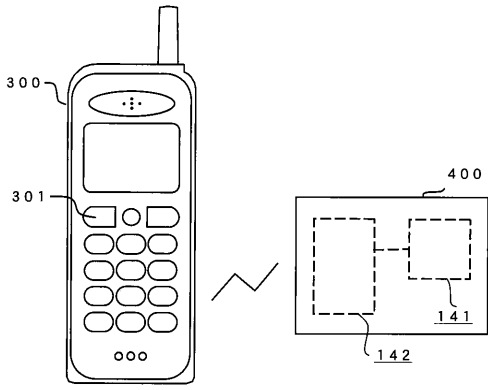
【図 1】



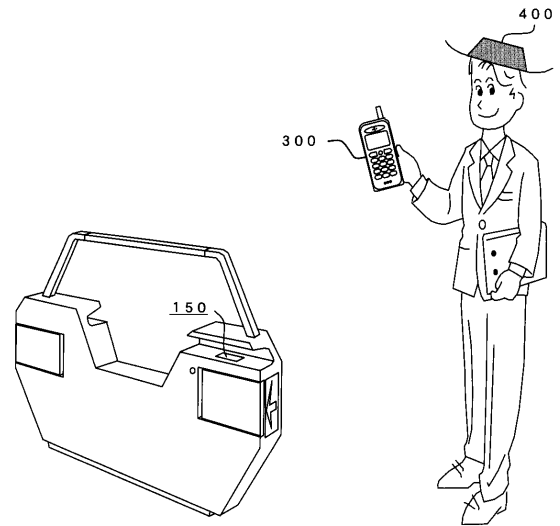
【図 2】



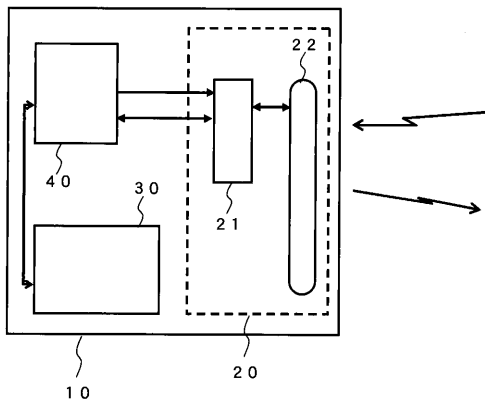
【図3】



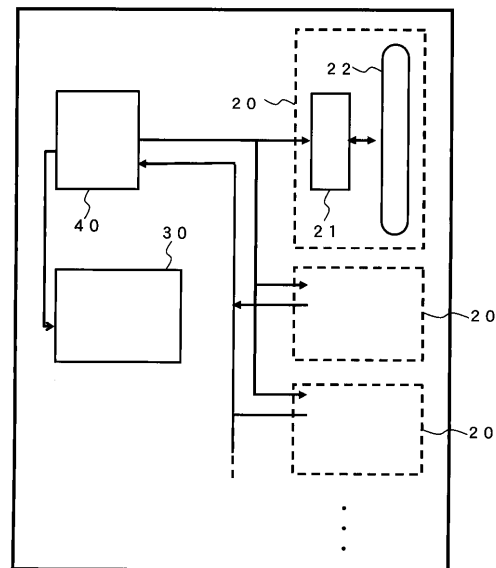
【図4】



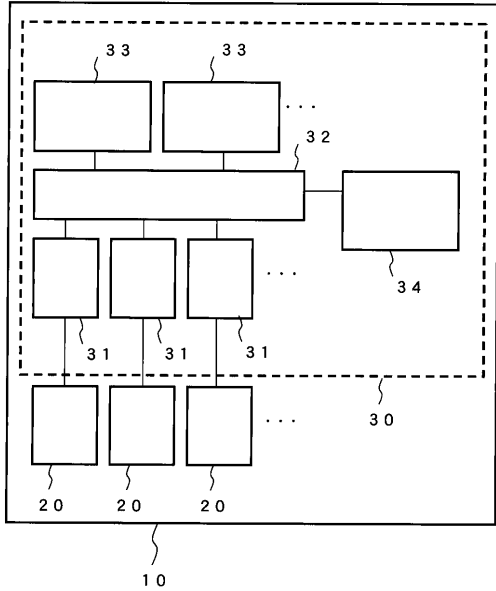
【図5】



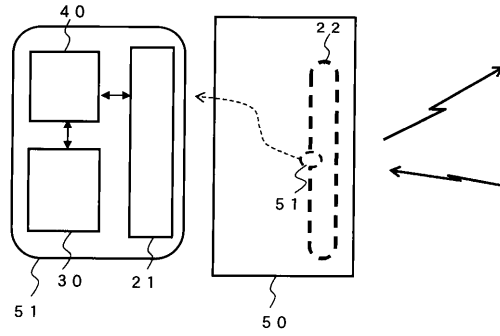
【図6】



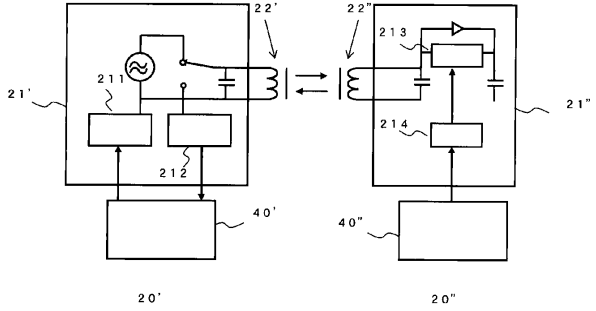
【図7】



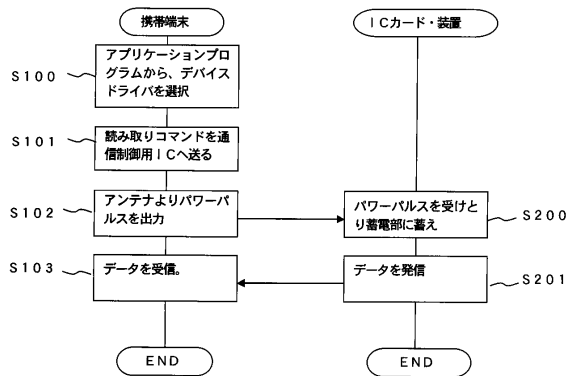
【図8】



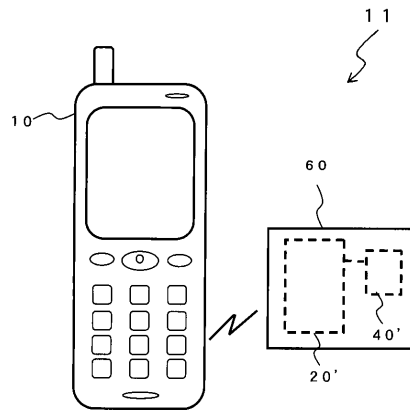
【図9】



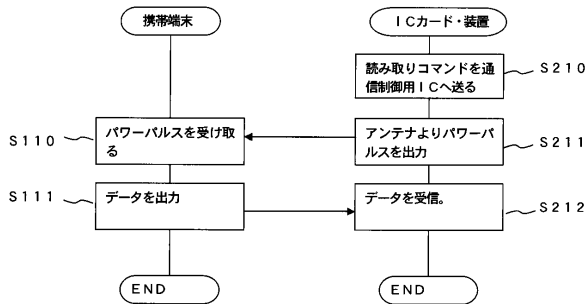
【図10】



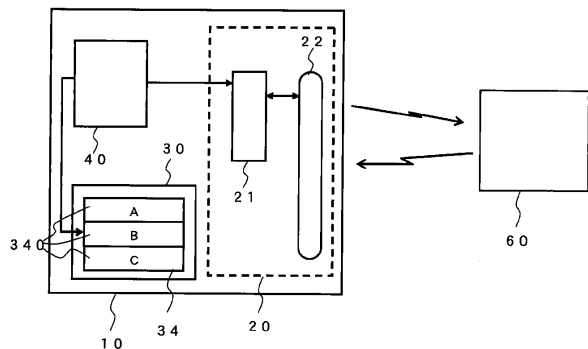
【図12】



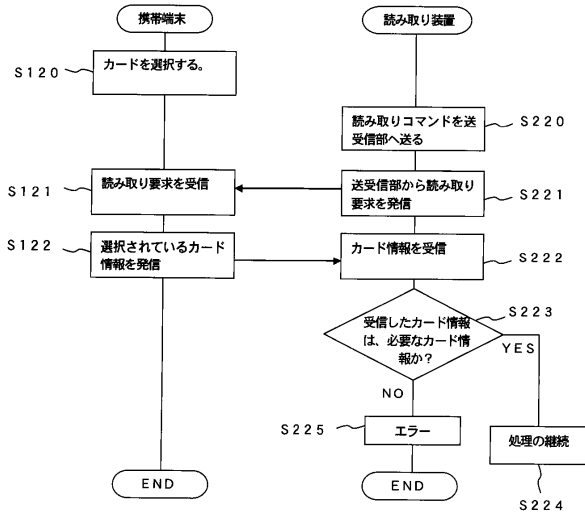
【図11】



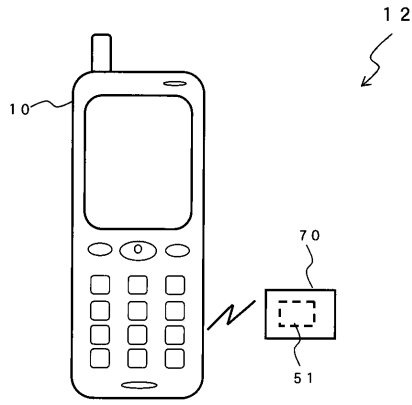
【図13】



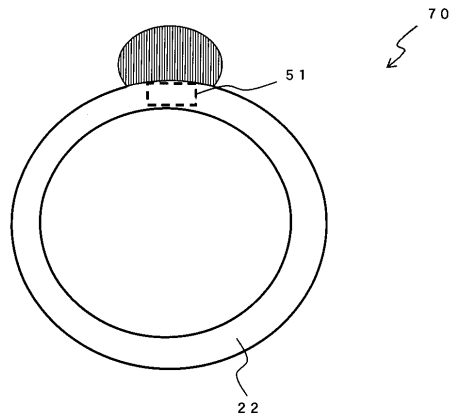
【図14】



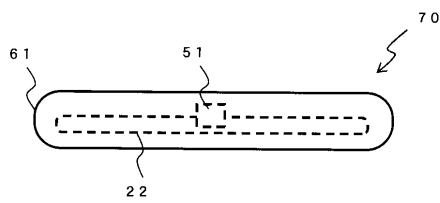
【図15】



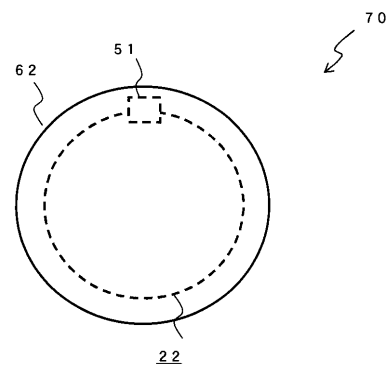
【図16】



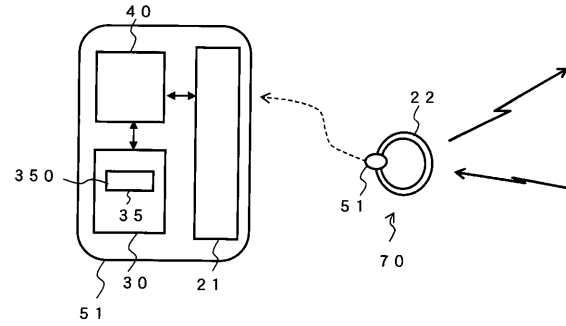
【図17】



【図18】

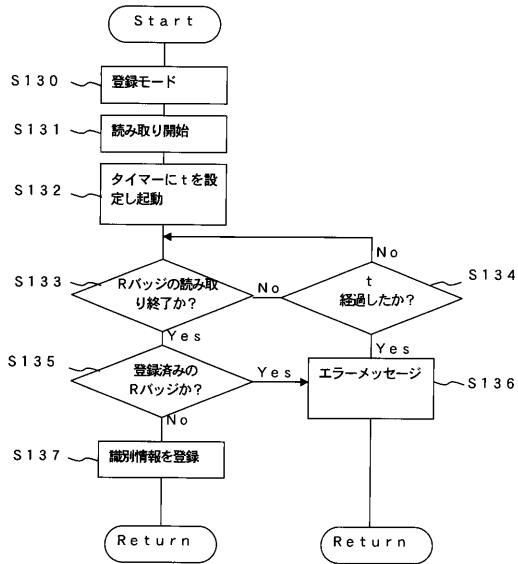


【図19】

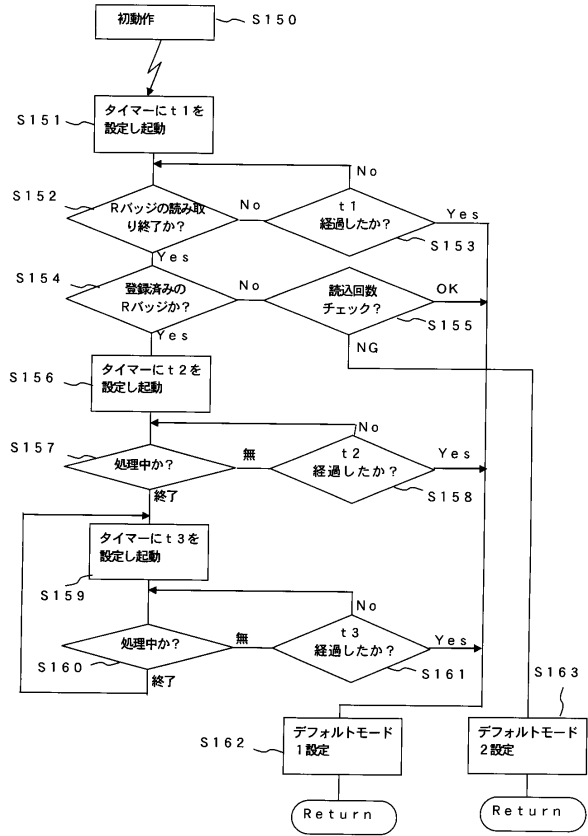




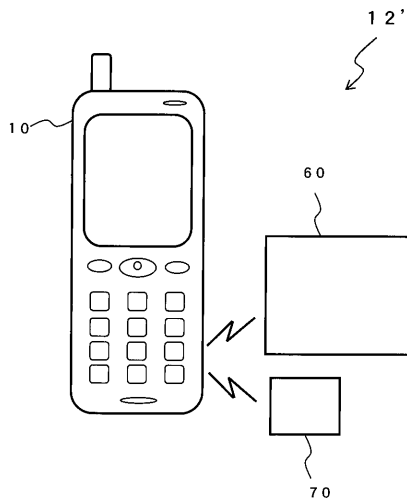
【図20】



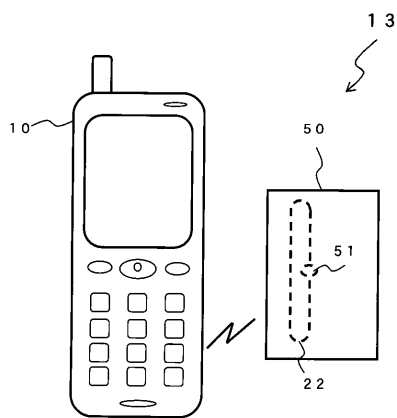
【図21】



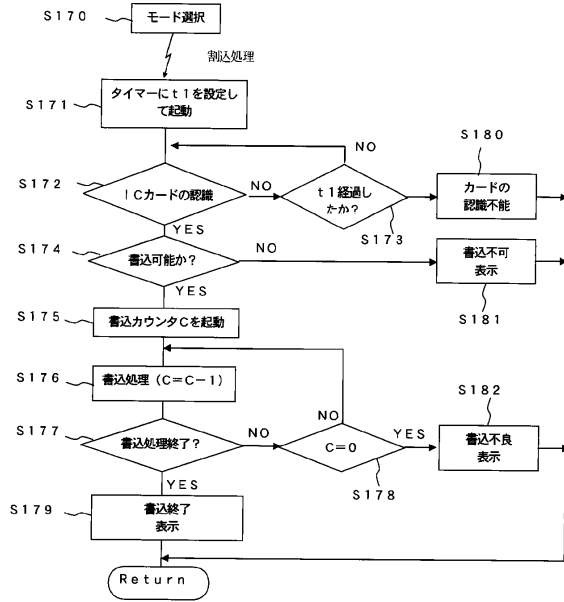
【図22】



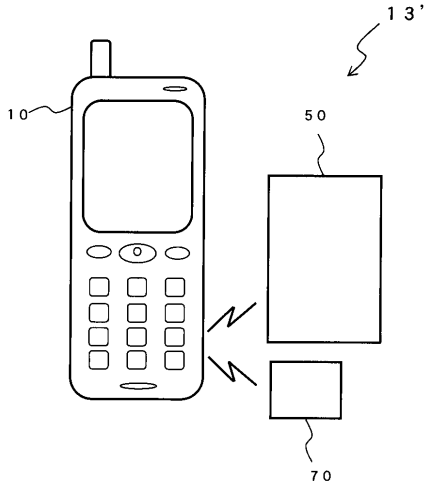
【図23】



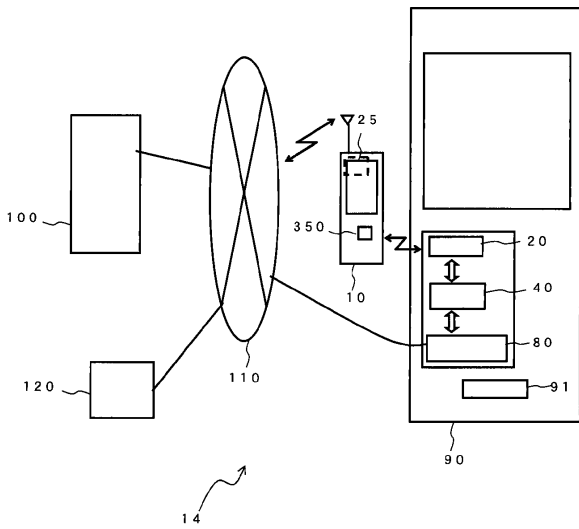
【図24】



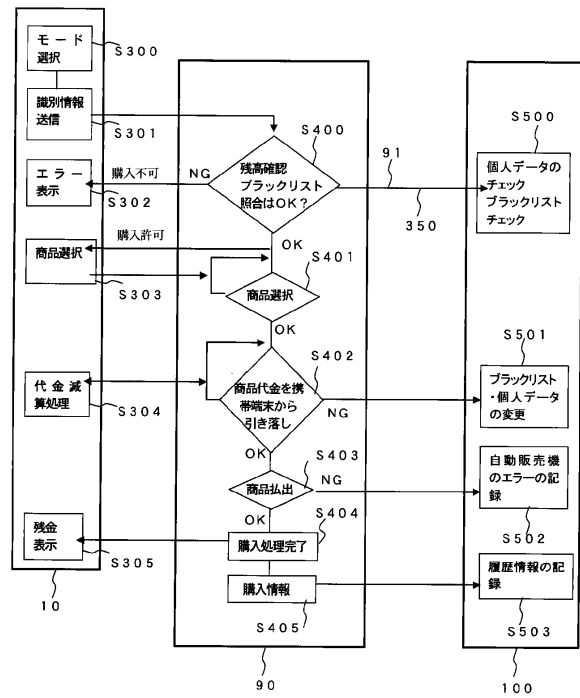
【図25】



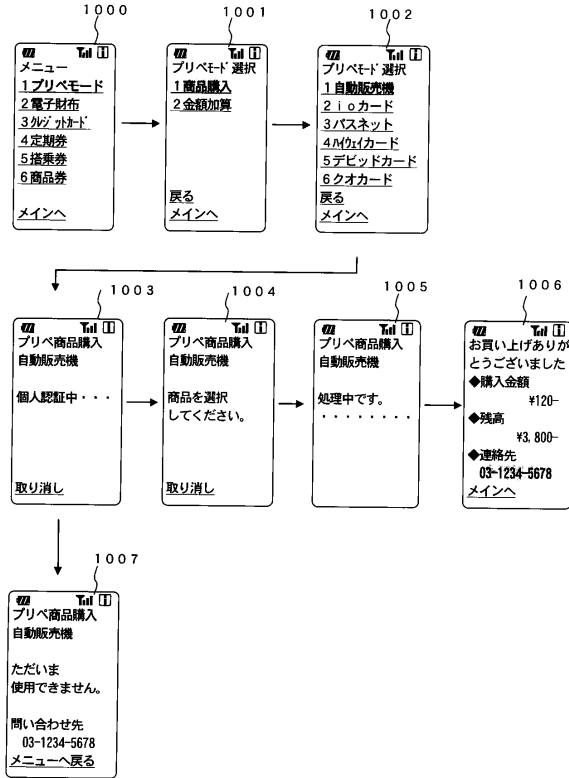
【図26】



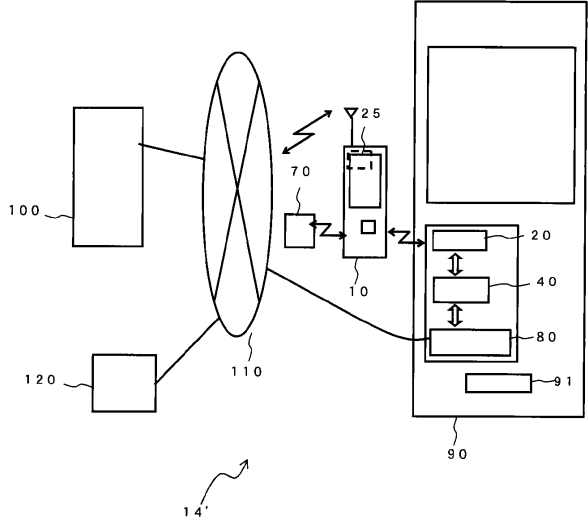
【図27】



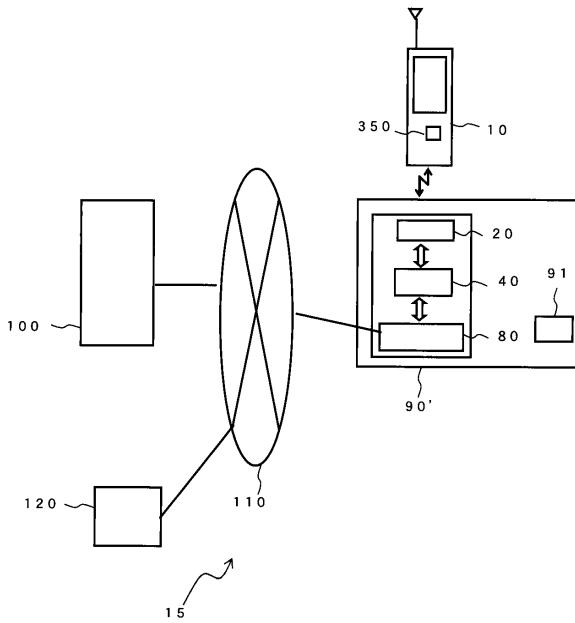
【図28】



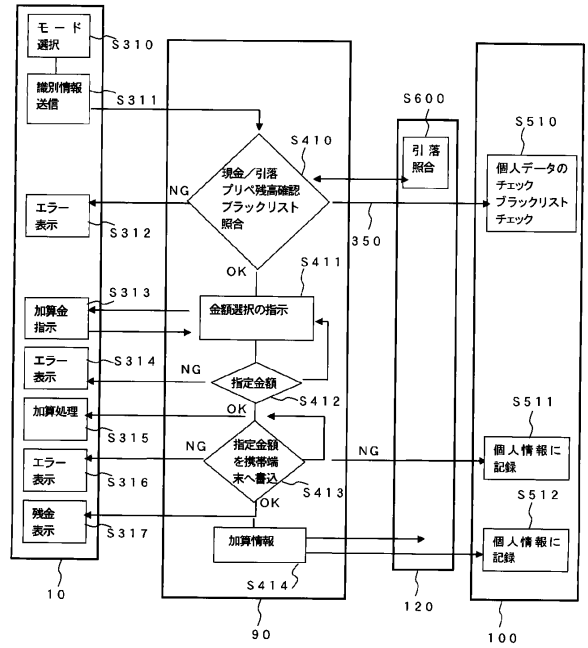
【図29】



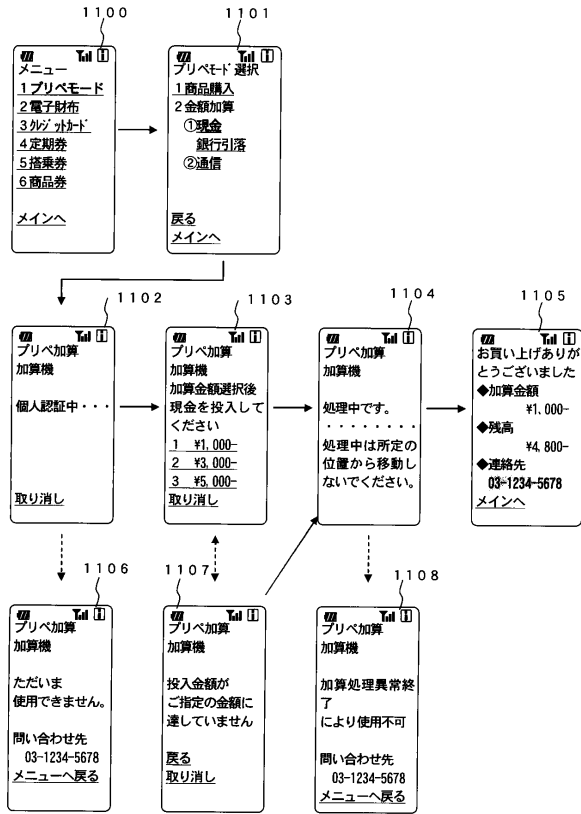
【図30】



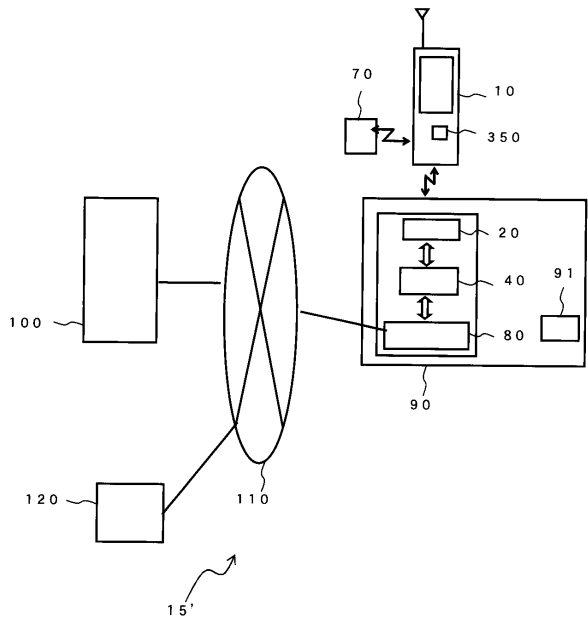
【図31】



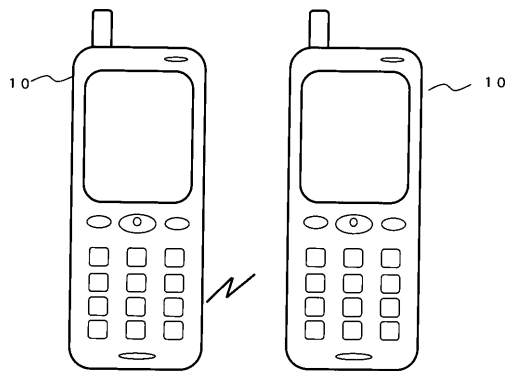
【図32】



【図33】



【図34】



## フロントページの続き

(51) Int.Cl.		F I
<i>H 0 4 W</i>	<i>12/06 (2009.01)</i>	<i>G 0 6 K 19/00 R</i>
<i>H 0 4 W</i>	<i>12/02 (2009.01)</i>	<i>G 0 6 F 12/14 5 3 0 C</i>
<i>H 0 4 W</i>	<i>84/10 (2009.01)</i>	<i>G 0 6 F 12/14 5 6 0 Z</i>
<i>H 0 4 W</i>	<i>8/24 (2009.01)</i>	<i>H 0 4 Q 7/00 1 8 3</i>
<i>H 0 4 M</i>	<i>1/727 (2006.01)</i>	<i>H 0 4 Q 7/00 1 8 1</i>
<i>H 0 4 M</i>	<i>11/00 (2006.01)</i>	<i>H 0 4 Q 7/00 6 2 9</i>
<i>H 0 4 L</i>	<i>9/32 (2006.01)</i>	<i>H 0 4 Q 7/00 1 5 3</i>
		<i>H 0 4 M 1/727</i>
		<i>H 0 4 M 11/00 3 0 2</i>
		<i>H 0 4 L 9/00 6 7 3 A</i>

- (56)参考文献 特開平04 - 306760 (JP, A)  
 特開平03 - 060543 (JP, A)  
 特開2000 - 306005 (JP, A)

## (58)調査した分野(Int.Cl., DB名)

G 0 6 K 1 7 / 0 0  
 G 0 6 F 2 1 / 2 0  
 G 0 6 F 2 1 / 2 4  
 G 0 6 K 1 9 / 0 7  
 G 0 6 K 1 9 / 1 0  
 H 0 4 L 9 / 3 2  
 H 0 4 M 1 / 7 2 7  
 H 0 4 M 1 1 / 0 0  
 H 0 4 W 8 / 2 4  
 H 0 4 W 1 2 / 0 2  
 H 0 4 W 1 2 / 0 6  
 H 0 4 W 8 4 / 1 0