(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2007-19746
(P2007-19746A)
(43)公開日　平成19年1月25日(2007.1.25)

(51)Int.Cl.			F I			テーマコード（参考）
H04M	1/66	(2006.01)	H04M	1/66		5K027
H04M	1/725	(2006.01)	H04M	1/725		5K067
H04Q	7/38	(2006.01)	H04B	7/26	109R	

審査請求 未請求　請求項の数 6　OL　（全 10 頁）

(21)出願番号　特願2005-197843 (P2005-197843)
(22)出願日　平成17年7月6日 (2005.7.6)

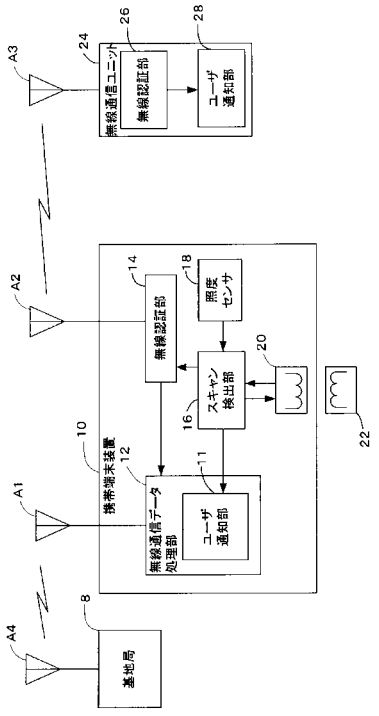
(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100115107
弁理士　高松　猛
(74)代理人　100108589
弁理士　市川　利光
(74)代理人　100119552
弁理士　橋本　公秀
(72)発明者　田苗　弘
神奈川県横浜市都筑区佐江戸町６００番地
パナソニックモバイルコミュニケーションズ株式会社内

Ｆターム(参考)　5K027 AA11 BB09 CC08 FF12 FF22 FF25 HH26 MM03 MM11 MM15

最終頁に続く

(54)【発明の名称】非接触ＩＣを備えた携帯端末装置

(57)【要約】
【課題】　携帯端末装置における非接触ＩＣの不正スキャンを防止する。
【解決手段】　無線通信認証システムは、無線通信データ処理部１２、無線認証部１４、スキャン検出部１６、照度センサ１８、及び非接触ＩＣ２０を含む携帯端末装置１０と、無線認証部２６及びユーザ通知部２８を含む無線通信ユニット２４とから構成される。照度センサ１８は携帯端末装置の周囲の照度を測定する。暗い場所に携帯端末装置が置かれている状況下で、外部のスキャナにより非接触ＩＣがスキャンされ、非接触ＩＣ２０に起電力が発生すると、スキャン検出部１６は、当該起電力によって非接触ＩＣ２０がスキャンされたことを検出し、ユーザ通知部１１によりユーザにその旨を通知するとともに、無線認証部１４を介して、無線通信ユニット２４に通知する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
非接触ＩＣと、
当該非接触ＩＣがスキャンされたことを検出するスキャン検出部と、
前記スキャン検出部により前記非接触ＩＣがスキャンされたことが検出されたとき、スキャンの事実をユーザに通知するユーザ通知部と、
を備える携帯端末装置。
【請求項２】
請求項１記載の携帯端末装置であって、
前記スキャン検出部は、前記非接触ＩＣがスキャンされたとき、当該非接触ＩＣが発生する起電力を検出する携帯端末装置。
【請求項３】
請求項１または２記載の携帯端末装置であって、
周囲の照度を検知する照度センサを更に備え、
当該照度センサにより検知された周囲の照度が所定値以下のとき、前記ユーザ通知部はスキャンの事実をユーザに通知する携帯端末装置。
【請求項４】
請求項１ないし３のいずれか１項記載の携帯端末装置であって、
前記ユーザ通知部は、スピーカ、発光装置、バイブレータの少なくともいずれか一つより構成される携帯端末装置。
【請求項５】
請求項１ないし４のいずれか１項記載の携帯端末装置であって、
当該携帯端末装置の電源がオフのときに前記非接触ＩＣがスキャンされると、緊急割込より、電源がオンにされる携帯端末装置。
【請求項６】
無線通信ユニットと、当該無線通信ユニットと無線認証を行う携帯端末装置と、を備える無線通信認証システムであって、
前記携帯端末装置は、非接触ＩＣと、当該非接触ＩＣがスキャンされたことを検出するスキャン検出部と、前記無線通信ユニットへ認証信号及び前記スキャンの事実を示す通知信号を送信する無線認証部と、を備え、
前記無線通信ユニットは、前記携帯端末装置の無線認証部からの前記認証信号及び前記通知信号を受信する無線認証部と、前記通知信号に基づきスキャンの事実をユーザに通知するユーザ通知部と、を備える無線通信認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、非接触ＩＣを備えた携帯端末装置に関し、特に非接触ＩＣの不正な読取りを防止し得る技術に関する。
【背景技術】
【０００２】
近年、携帯電話等の携帯端末装置に保存された個人情報等の情報流出を防止する技術が検討されてきている。このような状況に鑑み、置き忘れや盗難により該装置が所有者又は使用者の手元から離れたとき、装置そのものを使用不能にすると共に装置が一定距離以上離れたことを警告可能な携帯端末装置の無線通信ユニット、使用制限装置が提案されている（例えば、特許文献１参照）。
【０００３】
図４は、無線認証を使用した携帯端末装置及び無線ユニットからなる無線通信認証システムの全体構成を説明するブロック図である。このシステムにおいては、無線通信ユニット５の無線認証部６と携帯端末装置１の無線認証部２は、予め関連付けされた認証ＩＤを所有し、アンテナＡ６、Ａ７間の無線通信を利用してお互いが１対１の関係性を有するこ

とを把握することで常時無線認証する方法を採用している。

【０００４】

携帯端末装置１の無線認証部２がアンテナＡ６、Ａ７間の無線通信の電波減衰量を測定し、無線通信ユニット５と携帯端末装置１の通信距離を求め、距離に応じて認証か非認証かを判断し、携帯端末装置１の無線通信通話部３に使用制限をかけるか否か判断がなされる。

【０００５】

無線通信ユニット５と携帯端末装置１が一定距離以内にあれば、携帯端末装置１は所有者が管理可能な場所に存在すると判断し、使用制限をかけない。無線通信ユニット５と携帯端末装置１が一定距離以上ならば、携帯端末装置１は所有者の管理可能な場所に存在していないと判断し、使用制限をかける。無線通信ユニット５と携帯端末装置１が一定距離以上離れたとき、無線通信ユニット５は、スピーカ等のユーザ通知部７を使用してユーザに警告する。

【特許文献１】特開平１１－８８４９９号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

ところで、昨今の携帯端末装置においては、図４に示したように非接触ＩＣ２０が搭載されているものが多い。非接触ＩＣは、種々の回路が半導体集積回路化されて、チップ上に形成され、構成されている。この非接触ＩＣ２０内には、携帯端末装置のユーザの口座情報や決済情報等個人情報が記憶されており、外部のスキャナ２２によって、そのような個人情報の読み書きが行なわれる。このような構成を採用することにより、決済等種々の手続きを簡略化することができる。

【０００７】

しかしながら、携帯端末装置に内蔵された非接触ＩＣは、ユーザの気づかない間に第三者によりスキャンされ、個人情報が流出、漏洩される危険性がある。特に、混雑した人ごみの中や、ユーザの不注意時をついて、携帯端末装置１がユーザの手元、管理可能な場所にあるにもかかわらず、悪意ある第三者によって非接触ＩＣ内の情報が読込まれる（スキャンされる）問題が存在する。

【課題を解決するための手段】

【０００８】

本発明は、携帯端末装置に内蔵された非接触ＩＣ内の情報が、ユーザの気づかない間に第三者によりスキャンされる危険を防止し得る携帯端末装置を提供する。

【０００９】

本発明の携帯端末装置は、非接触ＩＣと、当該非接触ＩＣがスキャンされたことを検出するスキャン検出部と、前記スキャン検出部により前記非接触ＩＣがスキャンされたことが検出されたとき、スキャンの事実をユーザに通知するユーザ通知部と、を備える。前記スキャン検出部は、前記非接触ＩＣがスキャンされたとき、当該非接触ＩＣが発生する起電力を検出するものであってもよい。

【００１０】

この構成により、携帯端末装置に内蔵された非接触ＩＣが、混雑した人ごみやユーザの不注意をついてユーザの気づかない間に第三者によりスキャンされる危険を防止し得る携帯端末装置が実現される。

【００１１】

また、周囲の照度を検知する照度センサを更に携帯端末装置に設け、当該照度センサにより検知された周囲の照度が所定値以下のとき、前記ユーザ通知部はスキャンの事実をユーザに通知するように構成してもよい。

【００１２】

携帯端末装置が鞄やポケットの中のような暗い場所に置かれているとき、特に不正なスキャンがされやすい。そこで上記の構成により、特にそのような場所に置かれているとき

ユーザに通知することにより、ユーザの注意を喚起することができる。また、正当なスキャンは明るい場所でされることが多いので、正当なスキャンがなされている場合にも余計な通知がなされてしまうことを抑制することができる。

【００１３】

また、前記ユーザ通知部を、スピーカ、発光装置、バイブレータの少なくともいずれか一つより構成することができる。

【００１４】

さらに、携帯端末装置の電源がオフのときに前記非接触ＩＣがスキャンされると、緊急割込より、電源がオンにされるよう携帯端末装置を構成してもよい。

【００１５】

この構成により、たとえ携帯端末装置の電源がオフであっても、緊急割り込みで電源を起動するので、携帯端末装置に内蔵された非接触ＩＣが悪意ある第三者によりスキャンされる危険を抑制することができる。この構成は、携帯端末装置の電源がオフであっても起動する非接触ＩＣの場合、特に有用である。

【００１６】

更に本発明は、無線通信ユニットと、当該無線通信ユニットと無線認証を行う携帯端末装置と、を備える無線通信認証システムであって、前記携帯端末装置は、非接触ＩＣと、当該非接触ＩＣがスキャンされたことを検出するスキャン検出部と、前記無線通信ユニットへ認証信号及び前記スキャンの事実を示す通知信号を送信する無線認証部と、を備え、前記無線通信ユニットは、前記携帯端末装置の無線認証部からの前記認証信号及び前記通知信号を受信する無線認証部と、前記通知信号に基づきスキャンの事実をユーザに通知するユーザ通知部と、を備える。

【００１７】

このような無線通信認証システムにおいて、無線通信ユニットが携帯端末装置からの通知信号を受け、ユーザに非接触ＩＣがスキャンされた事実を通知する。無線通信ユニットにおいては、携帯端末装置の動作状態とは別に独立した動作状態を維持できる。従って、携帯端末装置がスリープモード、省電力モードの如き通常の動作モードとは異なっていても、ユーザにスキャンの事実を通知することができる。また、携帯端末装置と協同して、または単独でそのような通知をなすことのより、ユーザにより注意を喚起させることができる。

【発明の効果】

【００１８】

本発明の携帯端末装置、無線通信認証システムによれば、携帯端末装置の非接触ＩＣに対する第三者のスキャンをユーザに容易に知らしめることができるため、非接触ＩＣ内の情報をより確実に保護し得る。

【発明を実施するための最良の形態】

【００１９】

以下、本発明の実施形態である携帯端末装置及び無線通信ユニットを含む無線通信認証システムについて、図面を参照して説明する。

【００２０】

図１は、本実施形態の携帯端末装置１０及び無線通信ユニット２４より構成される無線通信認証システムのブロック図である。携帯端末装置１０は携帯電話、ＰＤＡ（Personal Digital Assistant）等の携帯電子機器より構成される。一方、無線通信ユニット２４は、一般的にユーザが常時身に付けるキー、キーホルダー、バッジ、カード等の形態に構成されたものであるが、特にその形態は限定されない。このシステムにおいては、携帯端末装置１０と無線通信ユニット２４の間で無線認証が行われ、無線認証が成功している間のみ、携帯端末装置１０はその使用制限が解除され、使用可能となるが、無線認証が途切れると、携帯端末装置１０に使用制限がかかり、機能の一部または全てが使用不可となる。

【００２１】

本発明においては、アンテナを内蔵し、微弱な電波を利用して外部のスキャナ（リーダ

／ライタ）と交信する非接触式ＩＣ２０が携帯端末装置１０に搭載されている。悪意ある第三者が非接触ＩＣをスキャンしようとした場合に、本人、周囲の人、スキャンした第三者へ聞こえる音を鳴らし、これによってこれらの人々の注意を喚起し、悪意ある第三者によるスキャンを抑制することができる。

【００２２】

携帯端末装置１０は、無線通信データ処理部１２と、無線認証部１４と、スキャン検出部１６と、照度センサ１８と、非接触ＩＣ２０と、アンテナＡ１と、アンテナＡ２とを備える。

【００２３】

非接触ＩＣ２０は、種々の回路が半導体集積回路化されて、チップ上に形成され、構成されている。この非接触ＩＣ２０内には、携帯端末装置のユーザの口座情報や決済情報等個人情報が記憶されており、外部のスキャナによって、そのような個人情報の読み書きが行なわれる。このような構成を採用することにより、決済等種々の手続きを簡略化することができる。非接触ＩＣ２０は、ＩＣカード、ＩＣチップ、ＩＣタグ、ＲＦＩＤ（Radio Frequency Identification）等種々の呼び方があるが、既存のものが使用可能であり、特にその構成は限定されない。

【００２４】

無線通信ユニット２４は、無線認証部２６と、ユーザ通知部２８と、アンテナＡ３とを含む。携帯端末装置１０のアンテナＡ２と無線通信ユニット２４のアンテナＡ３を介して無線認証部１４、無線認証部２６は所定の認証信号を用いて無線認証を行なう。このシステムにおいては、無線通信ユニット５の無線認証部６と携帯端末装置１の無線認証部２は、予め関連付けされた認証ＩＤを所有し、アンテナＡ２、Ａ３間の無線通信を利用してお互いが１対１の関係性を有することを把握することで常時無線認証する方法を採用している。

【００２５】

携帯端末装置１０の無線認証部１４がアンテナＡ２、Ａ３間の無線通信の電波減衰量を測定し、無線通信ユニット２４と携帯端末装置１０の通信距離を求め、距離に応じて認証か非認証かを判断し、携帯端末装置１０の無線通信データ処理部１２に使用制限をかけるか否か判断がなされる。

【００２６】

無線通信ユニット２４と携帯端末装置１０が一定距離以内にあれば、携帯端末装置１０はユーザが管理可能な場所に存在すると判断し、使用制限をかけない。無線通信ユニット２４と携帯端末装置１０が一定距離以上離れているならば、携帯端末装置１０はユーザの管理可能な場所に存在していないと判断し、使用制限をかける。また、無線通信ユニット２４と携帯端末装置１０が一定距離以上離れたとき、無線通信ユニット２４は、スピーカ等のユーザ通知部２８を使用してユーザに警告する。

【００２７】

次に、携帯端末装置１０側の説明を行なう。悪意ある第三者が、自らの所有するスキャナ２２を用いて非接触ＩＣ２０内の情報を読込もうとしたとき、スキャナ２２側で発生する電磁波により非接触ＩＣ２０内部に起電力を生じる。この起電力によって非接触ＩＣ２０は動作する。このとき使用制限が無線通信データ処理部１２に対してかかっていなければ、非接触ＩＣ２０は正常に動作する。そして、スキャン検出部１６は、非接触ＩＣ２０の起電力を検知し、無線通信データ処理部１２のユーザ通知部１１が、第三者のスキャンに対する警告をユーザに通知する。ユーザ通知部１１は警告音を発するスピーカや、警告を振動によって通知するバイブレータ、警告を視覚的に発するＬＥＤの如き発光装置等により構成されるが、警告を通知できるものならばその構成は限定されない。

【００２８】

スキャン検出部１６は、非接触ＩＣ２０内部の起電力をトリガーとして、非接触ＩＣ２０が第三者のスキャナ２２によりスキャンされたことを検出し、無線認証部１４及び無線通信データ処理部１２に対し、通知する。この通知によって、無線認証部１４は、無線通

信データ処理部１２に対して使用を制限する使用制限信号を与えるとともに、アンテナＡ３を介して無線通信ユニット２４に、第三者のスキャナ２２によりスキャンされたことを示す旨の通知信号を認証信号とともに送信する。

【００２９】

また、本実施形態の携帯端末装置１０は、照度センサ１８を更に有する。照度センサ１８は、携帯端末装置１０の周囲の明るさ（照度、輝度等）を検知し、明るさ（照度）が所定値以下である場合、携帯端末装置１０が暗い場所（暗所）に存在することを示す信号を、スキャン検出部１６に与える。この信号が与えられているときのみ、スキャン検出部１６はユーザ通知部１１を起動可能状態にすることができる。

【００３０】

一般に、カバンの内部、ポケットの内側等の所定の暗所に携帯端末装置１０が存在している場合において、第三者による不正なスキャンが行なわれる場合が多い。一方、カバンから取り出した時など、携帯端末装置１０が明るい場所に存在している場合は、不正なスキャンが行なわれる場合は少ない。そこで、照度センサ１８が、携帯端末装置１０が暗所にあることを示す信号をスキャン検出部１６へ与えた場合のみ、スキャン検出部１６はユーザ通知部１１を起動可能状態に設定することができる。これにより、明るい場所で正常なスキャンが行なわれる場合においてもユーザ通知部１１が作動することを防止することができる。もちろん照度センサ１８は必要に応じて設けられ、必須の構成ではない。また、上述の照度の所定値も状況に応じて可変とする構成にしてもよい。

【００３１】

また、第三者によるスキャンの通知を受けたスキャン検出部１６は、非接触ＩＣ２０に使用制限信号を与え、非接触ＩＣ２０の使用を制限し、読み出し不可状態にするような構成にすることもできる。これによって、非接触ＩＣ２０からスキャナ２２によって情報が読み出されることを防止することができる。

【００３２】

また、アンテナＡ１は、携帯端末装置の基地局８のアンテナＡ４と音声通信、メール通信等通常の無線通信を行なうために用いられる。そこで、アンテナＡ１、アンテナＡ４、基地局８を介して、通常の無線通信によって携帯端末装置１０と無線通信ユニット２４との間で、予め登録された緊急連絡先にメールを発信し、情報のやりとりをすることによって、不正なアクセスであるか否かを判断してもよい。

【００３３】

また、携帯端末装置１０の電源がオフであっても、緊急割り込みで電源を起動する機能をもつ、例えばスイッチング回路（図示なし）を携帯端末装置１０に設けてもよい。これによって、たとえ携帯端末装置１０の電源がオフであっても、非接触ＩＣ２０が第三者によりスキャンされるときに緊急割込機能が作用し、電源をオンにし、携帯端末装置１０を起動して警告機能を実行するような構成にすることもできる。この構成は、携帯端末装置１０が省電力モードの如きスリープ状態にある場合にも応用され得る。一般的に非接触ＩＣ２０は、携帯端末装置１０の電源オン・オフの状態、動作モードに拘わらず外部のスキャナ２２等から電力を受け取ることで動作可能である。

【００３４】

次に無線通信ユニットの説明を行なう。無線通信ユニット２４は、無線認証部２６及びユーザ通知手段２８を含む。無線認証部２６が、携帯端末装置１０側における第三者の不正なスキャンの通知を受けると、ユーザ通知部２８が動作し、その旨をユーザに知らせる。ユーザ通知部２８もユーザ通知部１１と同様、警告音を発するスピーカや、警告を振動によって通知するバイブレータ、警告を視覚的に発するＬＥＤの如き発光装置等により構成されるが、警告を通知できるものならばその構成は限定されない。このとき、携帯端末装置１０のユーザ通知部１１が動作しないように制御することも可能である。また逆に、携帯端末装置１０のユーザ通知部１１が動作する場合は、無線通信ユニット２４のユーザ通知部２８が動作しないよう制御することも可能である。

【００３５】

また、たとえ携帯端末装置１０が省電力モードの如きスリープ状態であっても、非接触ＩＣ２０が第三者によりスキャンされたとき、アンテナＡ２、Ａ３間の無線認証によって、無線通信ユニット２４のユーザ通知部が動作するような構成を採用することもできる。

【００３６】

図２は、携帯端末装置１０と無線通信ユニット２４を身体に装着したユーザ４０に対し、第三者が接近して情報をスキャンしようとする状況を説明する図である。悪意のある第三者３８がスキャナ２２を用いて携帯端末装置１０の非接触スキャンしようとした場合、非接触ＩＣ２０には起電力を生じる。この起電力をトリガーとして、携帯端末装置１０は、警告等の通知機能を発揮することによって不正なスキャンを防止する。

【００３７】

携帯端末装置１０の無線通信データ処理部１２が省電カモードで動作していて音を鳴らせない場合、無線通信データ処理部１２は、スキャン検出部１６から出力されたスキャン通知信号を割込信号とみなして電源を起動し、携帯端末装置１０から警告音を鳴らすような構成にしてもよい。

【００３８】

また、無線通信ユニット２４は、携帯端末装置１０と無線通信ユニット２４との間でやりとりされる無線認証通信によって、上述したように、携帯端末装置１０と同時に、又は単独で通知機能を発揮する。特に無線通信ユニット２４は、ユーザ４０の視聴覚器官に近い位置に装着されていることが多いので、ユーザに対しよりわかりやすく通知をすることができる。これによって、不正スキャンの抑制が向上する。

【００３９】

すなわち、携帯端末装置１０の警告だけでなく、スキャン検出部１６がスキャン通知信号を無線認証部１４へ出力し、アンテナＡ２、Ａ３間の無線通信を利用して無線通信ユニット２４へ送信する。そして、無線通信ユニット２４の無線認証部２６がこの受信した通知信号をユーザ通知部２８へ出力し、無線通信ユニット２４も警告を通知する。さらに、携帯端末装置１０と無線通信ユニット２４が同時に警告通知を発してもよい。

【００４０】

図３は、本実施形態の携帯端末装置１０の制御フローを説明するフローチャートである。まず、携帯端末装置１０の非接触ＩＣ２０内部に、外部からの何らかのスキャンにより起電力が発生したとき（ステップＳ１；ＹＥＳ）、照度センサ１８が、装置が暗所に存在するか否かを判断する（ステップＳ２）。暗所でない場合（ステップＳ２；ＮＯ）、本実施形態では特に処理を行なわず、通常の制御へ移行する。一方、暗所である場合（ステップＳ２；ＹＥＳ）、照度センサ１８は、所定の照度以下の環境に携帯端末装置１０が存在する旨を示す信号をスキャン検出部１６へ与える（ステップＳ３）。そして、スキャン検出部１６は、非接触ＩＣ２０を非作動状態にする（ステップＳ４）。

【００４１】

さらに、スキャン検出部１６は、無線認証部１４に対し、無線通信ユニット２４へ暗所でのスキャンがなされた旨の通知信号を送信するよう命ずる（ステップＳ５）。ついで、図示せぬスピーカより警告音を発し、ユーザに対し、暗所でのスキャンがなされたことを通知する（ステップＳ６）。

【００４２】

以上説明したように、本発明においては、外部のスキャナにより、非接触ＩＣに対し何らかのスキャンがなされたとき、携帯端末装置はユーザにその旨を通知する。従って、ユーザは、そのようなスキャンにいち早く気づくことができ、不正なスキャンであった場合は迅速に対応することができる。

【００４３】

また、必要に応じて無線通信ユニットも、携帯端末装置といっしょに又は、単独で通知をなすことができる。このような構成はユーザに対する通知をより確実ならしめることに寄与する。

【００４４】

さらに本実施形態の携帯端末装置は照度センサを有し、周囲が一定照度より暗い場合のみに、上述の通知機能を発揮するような構成を有するため、不正でない正当なスキャンの場合にも通知がなされてしまうという事態を減らすことができる。

【００４５】

以上、本発明の各種実施形態を説明したが、本発明は前記実施形態において示された事項に限定されず、明細書の記載、並びに周知の技術に基づいて、当業者がその変更・応用することも本発明の予定するところであり、保護を求める範囲に含まれる。

【産業上の利用可能性】

【００４６】

本発明の携帯端末装置、無線通信認証システムによれば、携帯端末装置の非接触ＩＣに対する第三者のスキャンをユーザに容易に知らしめることができるため、非接触ＩＣ内の情報をより確実に保護し得る。

【図面の簡単な説明】

【００４７】

【図１】本発明の携帯端末装置及び無線通信ユニットを含む無線通信認証システムの１実施形態の構成を説明するブロック図。

【図２】携帯端末装置と無線通信ユニットを身体に装着したユーザと、携帯端末装置をスキャンしようとする第三者を示す図。

【図３】実施形態の携帯端末装置の制御フローを説明するフローチャート。

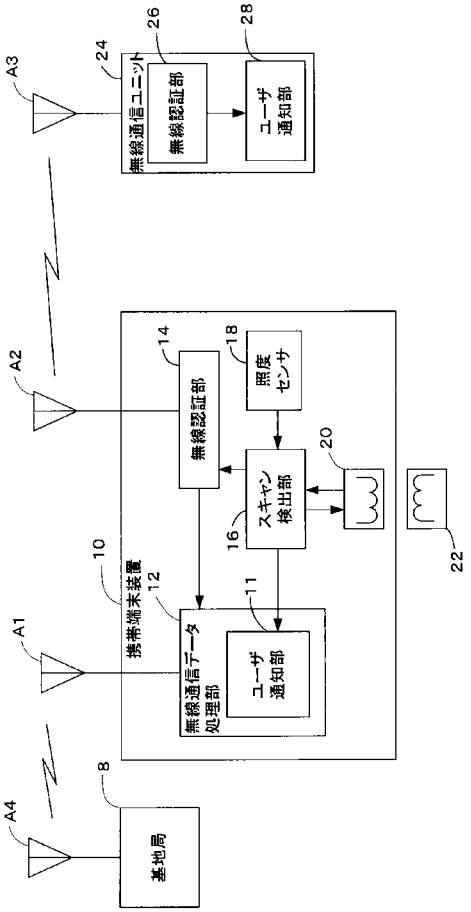
【図４】従来の無線認証を使用した無線通信認証システムの全体構成を説明するブロック図。

【符号の説明】

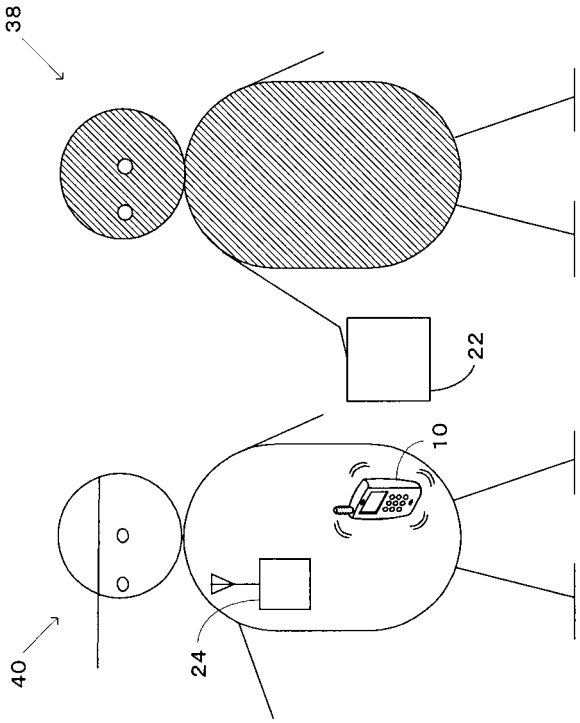
【００４８】

１０　携帯端末装置
１１　ユーザ通知部
１２　無線通信データ処理部
１４　無線認証部
１６　スキャン検出部
１８　照度センサ
２０　非接触ＩＣ
２２　スキャナ
２４　無線通信ユニット
２６　無線認証部
２８　ユーザ通知部

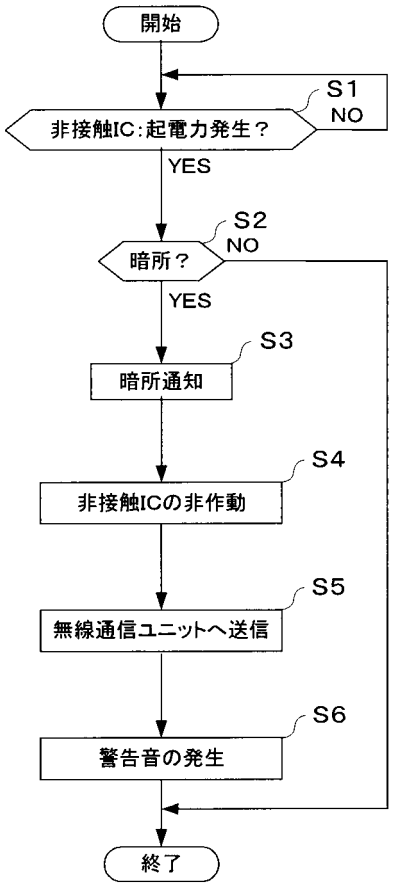
【図１】


A3
24
無線通信ユニット
26
無線認証部
28
ユーザ通知部
A2
14
無線認証部
18
照度センサ
20
スキャン検出部
16
22
10
携帯端末装置
12
11
A1
無線通信データ処理部
ユーザ通知部
8
A4
基地局

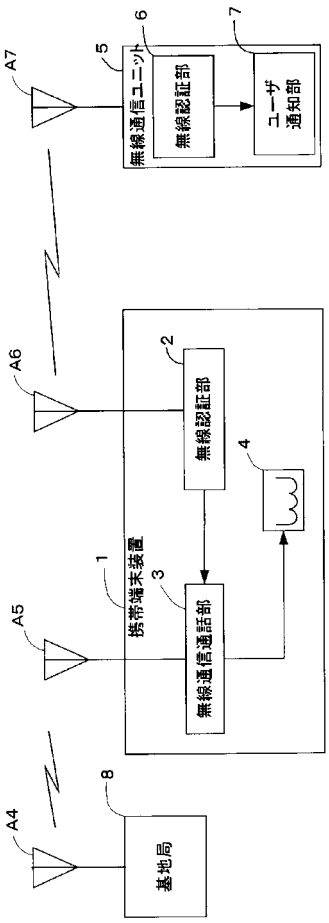
【図２】


38
22
10
40
24

【図３】


開始
S1
非接触IC:起電力発生？
NO
YES
S2
暗所？
NO
YES
S3
暗所通知
S4
非接触ICの非作動
S5
無線通信ユニットへ送信
S6
警告音の発生
終了

【図４】


A7
5
無線通信ユニット
6
無線認証部
7
ユーザ通知部
A6
2
無線認証部
4
1
携帯端末装置
3
無線通信通話部
A5
A4
8
基地局

フロントページの続き

Ｆターム(参考) 5K067 AA32 BB04 EE02 EE10 EE39 FF24 FF25 FF28 HH22 KK13
KK15