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

特許第4041478号
(P4041478)

(45)発行日　平成20年1月30日(2008.1.30)　(24)登録日　平成19年11月16日(2007.11.16)

(51)Int.Cl.			F I		
H04M	1/67	(2006.01)	H04M	1/67	
H04M	1/725	(2006.01)	H04M	1/725	
H04Q	7/38	(2006.01)	H04B	7/26	109R

請求項の数 8　(全 33 頁)

(21)出願番号　特願2004-195063(P2004-195063)
(22)出願日　平成16年6月30日(2004.6.30)
(65)公開番号　特開2006-20006(P2006-20006A)
(43)公開日　平成18年1月19日(2006.1.19)
審査請求日　平成17年11月30日(2005.11.30)

(73)特許権者　501431073
ソニー・エリクソン・モバイルコミュニケーションズ株式会社
東京都港区港南１丁目８番１５号
(74)代理人　100122884
弁理士　角田　芳末
(74)代理人　100113516
弁理士　磯山　弘信
(72)発明者　伊東　克俊
東京都港区港南１丁目８番１５号　ソニー・エリクソン・モバイルコミュニケーションズ株式会社内

最終頁に続く

(54)【発明の名称】通信システム及び通信端末装置

(57)【特許請求の範囲】
【請求項１】
通信端末装置と、その通信端末装置と所定の無線通信方式で無線通信が可能な無線キー装置とで構成され、前記通信端末装置と前記無線キー装置との通信状態に応じて、前記通信端末装置の機能制限に関するモード、又はその機能制限に関する告知のモードが設定される通信システムにおいて、
前記所定の無線通信方式は、無線接続された２台の機器の間で間欠的に無線通信を行う無線通信方式であり、
前記通信端末装置及び前記無線キー装置は、
前記所定の無線通信方式で無線通信を行う通信回路と、
前記通信回路での通信状態を制御する制御部と、
前記通信回路での無線通信状況又は無線通信距離を判定又は推定する判定手段と、
をそれぞれ備え、
前記通信端末装置と前記無線キー装置とが無線接続され、それぞれの通信回路で間欠的に無線通信を行う通信状態が設定され無線接続が維持された状況で、
前記判定手段で判定又は推定された結果が、前記通信回路を介した無線通信により、前記特定の相手に通知されるとともに、前記特定の相手から送信された判定又は推定結果が受信され、
前記制御部は、前記受信した結果と、前記判定手段での判定状況又は推定状況との組み合わせに基づいて、前記機能制限に関するモード又はその機能制限に関する告知のモード

の設定を変化させる
通信システム。
【請求項２】
特定の相手との所定の無線通信方式での無線通信状態に応じて、機能制限に関するモード、又はその機能制限に関する告知のモードを設定する通信端末装置において、
前記所定の無線通信方式は、無線接続された２台の機器の間で、間欠的に無線通信を行う無線通信方式であり、
前記所定の無線通信方式で無線通信を行う通信回路と、
前記通信回路での通信状態を制御する制御部と、
前記通信回路での無線通信状況又は無線通信距離を判定又は推定する判定手段と、
を備え、
前記通信回路により前記特定の相手と間欠的に無線通信を行う通信状態が設定され、無線接続が維持された状況で、
前記判定手段で判定又は推定された結果が、前記通信回路を介した無線通信により、前記特定の相手に通知されるとともに、前記特定の相手から送信された判定又は推定結果が受信され、
前記制御部は、前記受信した結果と、前記判定手段での判定状況又は推定状況との組み合わせに基づいて、前記機能制限に関するモード又はその機能制限に関する告知のモードの設定を変化させる
通信端末装置。
【請求項３】
請求項２記載の通信端末装置において、
前記通信回路が受信した信号の受信電界強度が、前記判定手段における判定又は推定に使用される
通信端末装置。
【請求項４】
請求項３記載の通信端末装置において、
前記受信電界強度の判定値の変動の差分に基づいて、無線通信状況又は無線通信距離が判定又は推定される
通信端末装置。
【請求項５】
特定の相手との所定の無線通信方式での無線通信状態に応じて、機能制限に関するモード、又はその機能制限に関する告知のモードを設定する通信端末装置において、
前記所定の無線通信方式は、無線接続された２台の機器の間で、間欠的に無線通信を行う無線通信方式であり、
前記所定の無線通信方式で無線通信を行う通信回路と、
前記通信回路での通信状態を制御する制御部と、
前記通信回路が受信した信号パケットの検出状況に基づいて、前記通信回路での無線通信状況又は無線通信距離を判定又は推定する判定手段と、
を備え、
前記通信回路により前記特定の相手と間欠的に無線通信を行う通信状態が設定され、無線接続が維持された状況で、前記判定手段における所定状況の判定又は推定がある場合に、前記制御部が、前記機能制限に関するモード、又はその機能制限に関する告知のモードの設定を変化させる
通信端末装置。
【請求項６】
請求項５記載の通信端末装置において、
前記判定手段での判定又は推定結果に基づいて、前記通信回路から送信させるパケット数が変化する
通信端末装置。

【請求項７】
請求項２記載の通信端末装置において、
前記判定手段での判定状況が所定以上変化した場合にだけ、前記制御部に判定結果が通知され、前記制御部が前記モードの設定を行う
通信端末装置。
【請求項８】
通信端末装置と、その通信端末装置と所定の無線通信方式で無線通信が可能な無線キー装置とで構成され、前記通信端末装置と前記無線キー装置との通信状態に応じて、前記通信端末装置の機能制限に関するモード、又はその機能制限に関する告知のモードが設定される通信システムにおいて、
前記所定の無線通信方式は、無線接続された２台の機器の間で間欠的に無線通信を行う無線通信方式であり、
前記通信端末装置及び前記無線キー装置は、
前記所定の無線通信方式で無線通信を行う通信回路と、
前記通信回路での通信状態を制御する制御部と、
前記通信回路が受信した信号パケットの検出状況に基づいて、前記通信回路での無線通信状況又は無線通信距離を判定又は推定する判定手段と、
を備え、
前記通信回路により前記特定の相手と間欠的に無線通信を行う通信状態が設定され、無線接続が維持された状況で、前記判定手段における所定状況の判定又は推定がある場合に、前記制御部が、前記機能制限に関するモード、又はその機能制限に関する告知のモードの設定を変化させる
通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えば、携帯電話端末の如き通信端末装置と、その端末装置の動作を規制する無線キー装置とで構成されるものに適用して好適な通信システム、及びその通信システムを構成する通信端末装置に関する。
【背景技術】
【０００２】
近年、利用者が常時所持して携帯する通信端末装置の１つである携帯電話端末は、本来の機能である無線電話機能以外に、各種機能が内蔵されて多機能化される傾向にある。
【０００３】
例えば、静止画や動画の撮影を行うカメラ機能、音楽データの録音・再生機能、テレビジョン放送の視聴機能などが、内蔵されたものがある。
【０００４】
また、近年急速に普及している非接触型のＩＣカードとしての機能を内蔵した携帯電話端末も開発されている。この非接触型のＩＣカードは、交通機関の乗車券、会員証や社員証、店での代金決済手段用のカード等として利用され、近接したリーダ・ライタとの間で無線通信を行って、認証処理を行うので、磁気カードなどに比べて使い勝手がよい。なお、携帯端末にＩＣカード機能部を組み込む場合には、ＩＣカード機能部が必ずしもカード型の形状をしているとは限らない。
【０００５】
ところで、このように多機能化された携帯電話端末は、その端末を紛失した際に、端末が備える各種機能を悪用されるのを防止するために、何らかのセキュリティを確保する処理が行うことが好ましい。特に、ＩＣカード機能部が内蔵された端末の場合には、ＩＣカード機能として記憶した個人情報が不正に読み出されたり、或いはＩＣカード機能を利用した不正な決済などが行われる可能性があるため、不正使用を防止する機能の必要性が高い。例えば特許文献１、２には、携帯電話端末と対になる無線カードを用意して、その無

線カードから定期的に認証要求を無線送信して、その認証要求に対する照合がとれない場合に、携帯電話端末の機能を制限することについての記載がある。
【特許文献１】特開２００１－３５２５７９号公報
【特許文献２】特開２００１－３５８８２７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
ところが、特許文献１、２に記載のように、携帯電話端末に、その端末の機能制限を行うための専用の認証処理を行うための通信回路や、認証処理手段を設けるようにすると、端末の構成が複雑化する問題がある。このような機能制限用の無線通信を行う場合に、従来からある各種無線通信方式をそのまま適用できれば、携帯端末の低コスト化に貢献する。
【０００７】
しかしながら、従来からある各種無線通信方式をそのままセキュリティ確保用に使用することを考えた場合、機能制限が必ずしも有効には機能しない場合が想定される。即ち、従来からある一般的な無線通信方式は、その無線システムで与えられたスペックの中で、出来るだけ良好に相手の端末と無線通信を行うのが基本である。このため、例えば携帯電話端末とその端末の機能制限を行う無線カードを用意し、両者の距離が数ｍ程度以上離れた場合に、携帯電話端末の機能を制限させるように想定してシステムを組んでも、実際には携帯電話端末と無線カードとの間で無線通信が出来なくなる距離を一義的に定めるのは困難であり、通信環境が良好な場合には、かなり距離が離れてから、機能制限がかかったり、逆に通信環境が劣悪な場合には、携帯電話端末と無線カードとが近接していても、無線通信できなく、機能制限がかかることが想定され、実用化する上での問題が多々あった。
【０００８】
また、携帯電話端末と対で使用される無線カード等の無線機器は、日常使用する上で極力手間がかからないことが好ましいが、実際には携帯電話端末と認証用のデータなどを常時やり取りしていると、比較的大きな電力消費が発生してしまうので、電池の充電や交換が頻繁に必要で、認証用の装置として作動させる上で、手間がかかってしまう問題があった。
【０００９】
本発明はかかる点に鑑みてなされたものであり、携帯電話端末の如き通信端末装置のセキュリティ制御を行う処理を、他の通信装置との無線通信状況に応じて行う場合に、セキュリティ制御のモード設定などが、低消費電力で良好に行えるようにすることを目的とする。
【課題を解決するための手段】
【００１０】
本発明は、通信端末装置と無線キー装置との通信状態に応じて、通信端末装置の機能を制限に関するモード、又はその機能制限に関する告知のモードが設定される場合に、通信端末装置及び無線キー装置は、通信回路での無線通信状況又は無線通信距離を判定又は推定する判定手段を備えて、通信端末装置と無線キー装置とが無線接続されて、それぞれの通信回路で間欠的に無線通信を行う通信状態が設定され、無線接続が維持された状況で、判定手段で判定又は推定された結果が、通信回路を介した無線通信により、特定の相手に通知されるとともに、特定の相手から送信された判定又は推定結果が受信され、制御部は、前記受信した結果と、判定手段での判定状況又は推定状況との組み合わせに基づいて、機能制限に関するモード又はその機能制限に関する告知のモードの設定を変化させるようにしたものである。
また本発明は、特定の相手との所定の無線通信方式での無線通信状態に応じて、機能制限に関するモード、又はその機能制限に関する告知のモードが設定される場合に、通信端末装置及び無線キー装置は、通信回路での無線通信状況又は無線通信距離を通信回路が受

信した信号パケットの検出状況に基づいて判定又は推定する判定手段を備えて、通信端末装置と無線キー装置とが無線接続されて、通信回路により特定の相手と間欠的に無線通信を行う通信状態が設定され、無線接続が維持された状況で、判定手段における所定状況の判定又は推定がある場合に、制御部が、機能制限に関するモード、又はその機能制限に関する告知のモードの設定を変化させるようにしたものである。

【００１１】

このようにしたことで、通信端末装置と無線キー装置と間での無線接続が行われて、なお且つ間欠的に送受信される状況での、無線通信状況又は無線通信距離が変化した場合に、そのことが判定又は推定されて、機能制限に関するモードの設定又は機能制限に関する告知のモードの設定を変化させることができ、無線通信方式で決められた無線通信処理状態には変化がなくても、機能制限に関するモード等を変化させることができる。

【発明の効果】

【００１２】

本発明によると、無線通信方式で決められた無線通信処理状態には変化がなくても、無線通信状況又は無線通信距離の変化で、機能制限に関するモード等を変化させることができる。従って、通信端末装置と無線キー装置との間で、機能制限に関するモードなどのデータを直接やり取りしなくても、無線通信処理状態の設定と、その設定された無線通信処理状態での通信中の無線通信状況又は無線通信距離の変化で、機能制限に関するモード等を適正に設定できるようになる。このため、例えば通信端末装置と無線キー装置との間が数ｍ以上離れた場合に、機能制限に関するモードを変化させて、機能制限させたり、その機能制限が行われることの告知を行うことが、無線通信状況などから簡単かつ確実に行えるようになる。機能制限に関するモードなどのデータを直接やり取りしないので、低消費電力で処理が行える。

【００１３】

この場合、判定手段で判定又は推定した結果を、通信回路を介した無線通信で、通信相手に通知するとともに、その通信相手から送信された判定又は推定結果を受信して、その受信した結果と、判定手段での判定状況又は推定状況との組み合わせに基づいて、機能制限に関するモード又はその機能制限に関する告知のモードの設定を変化させるようにしたことで、より精度良く通信端末装置と無線キー装置との間の距離変化などを検出できるようになり、より良好なモード設定が行えるようになる。

【００１４】

また、判定手段で判定又は推定する処理は、通信回路が受信した信号の受信電界強度であることで、受信電界強度の測定で、簡単に無線通信状況又は無線通信距離を判定（推定）できるようになる。

【００１５】

また、受信電界強度の判定値の変動の差分に基づいて、無線通信状況又は無線通信距離を判定又は推定するようにしたことで、相対的な無線通信状況から判定でき、良好に判定できるようになる。

【００１６】

また、判定手段で判定又は推定する処理は、通信回路が受信した信号パケットの検出状況であることで、受信パケットのエラーレートなどから簡単に無線通信状況又は無線通信距離を判定（推定）できるようになる。

【００１７】

また、この信号パケットの検出状況を処理に使用する場合に、判定又は推定した受信結果に基づいて、送信させるパケット数を変化させることで、相手側ではそのパケット数から簡単に無線通信状況を判定（推定）できるようになる。

【００１８】

さらに、判定手段での判定状況が所定以上変化した場合にだけ、制御手段に判定結果を通知して、制御手段がモードの設定の処理を行うようにしたことで、制御手段が介在するのを、モード変化に関係した制御処理が行われる場合だけにすることができ、例えば、通

信端末装置と無線キー装置との間で定常的に無線通信が行われていても、両者の距離などに変化がない場合には、制御手段が機能制限のモードに関係した制御処理を行う必要がなく、制御手段の負担を軽減でき、低消費電力化につながる。

【発明を実施するための最良の形態】

【００１９】

以下、本発明の第１の実施の形態を、図１～図３０を参照して説明する。

本例においては、携帯電話端末装置と無線通信を行う無線キー装置を用意して、携帯電話端末装置のセキュリティロックを、両者の無線通信状態で行うように行うようにしたものである。

【００２０】

図１は、本例の装置の例を示した図である。携帯電話端末装置１０とは別体の無線キー装置５０を用意する。この例では、無線キー装置５０は携帯電話端末装置１０よりも小型に構成してあり、例えばネックストラップ５０ａで利用者の首に下げるなど、利用者が常時身につけられる小型形状としてある。無線キー装置５０には、発光部５５と操作部５９（図１では押しボタン形状としてある）が配置してあり、また携帯電話端末装置１０と接続させるための端子部５６が用意してある。

【００２１】

携帯電話端末装置１０としては、ここでは一般的な携帯電話端末の形状の例を示してあり、無線電話通信用のアンテナ１１、スピーカ１４、マイクロフォン１５、表示部１６、操作部（操作キー）１７、発光部２２などが配置してある。また、無線キー装置５０と接続させるための端子部２３が用意してある。この端子部２３は、携帯電話端末装置１０が充電器や各種外部機器と接続するために用意された既存の端子を使用してもよい。また、表示部１６での表示として、例えば以下に説明するセキュリティが確保された状態で作動中であることを示すセキュリティ表示１６ａや、そのセキュリティ機能で動作が制限されたセキュリティロックがかかったことを示す表示（図示せず）を行うようにしてもよい。

【００２２】

次に、本例の携帯電話端末装置１０の構成例を、図２を参照して説明する。本例の携帯電話端末装置１０は、無線電話用の基地局と無線通信を行うための無線電話通信用アンテナ１１を備え、そのアンテナ１１が無線電話通信用の通信回路１２に接続してあり、制御部１９の制御で、基地局との間で無線通信を行うようにしてある。通信回路１２で通話用の通信を行う際には、受信した音声データを音声データ処理部１３に供給して音声データの受信処理を行ってからスピーカ１４に供給して出力させ、また、マイクロフォン１５が拾って音声データ処理部１３で処理された送信用の音声データを通信回路１２に供給して送信させる。

【００２３】

この携帯電話端末装置１０は、液晶ディスプレイなどで構成された表示部１６と、操作キーなどで構成された操作部１７を備える。表示部１６には、メール文、ウェブにアクセスさせた画面などを表示させることができ、操作部１７は、電話番号やメール文などの入力操作や、各種モード設定などが行える。なお、後述する近距離用の通信回路３２での通信処理が行われていて、その通信状態が、通信相手との接続処理を行う接続モードである場合に、操作部１７を構成するいずれかのキーなどが操作されたことを制御部１９が検出すると、強制的に相手に対して応答を求める信号（ページ信号）を送信する処理が行われる構成としてある。この具体的な処理例については後述する。

【００２４】

端末装置１０内の各ブロックは、制御ライン２５を介して制御部１９などと接続してあり、またデータライン２６を介してデータ転送を行える構成としてあり、メモリ１８に必要なデータを記憶させるようにしてある。このメモリ１８には、携帯電話端末として必要なデータだけでなく、後述するＩＣカード機能部４０で必要なデータについても記憶させてもよい。また、セキュリティ機能を実現するプログラムや、そのセキュリティ機能を実行する上で必要なデータの保持を、このメモリ１８で行う。

【００２５】
また、この端末装置１０への電話回線を介した着信や、各種警告を行うために、端末そのものを振動させる振動モータなどで構成される振動部２１と、発光ダイオードなどで構成される発光部２２とを備え、制御部１９の制御で、振動や発光を行う。これらの振動部２１や発光部２２は、携帯電話端末として着信などを知らせる告知手段として使用されるが、セキュリティ機能で必要な警告手段としても使用するようにしてある。なお、セキュリティ機能で必要な警告手段として、音を鳴らす場合には、スピーカ１４などから警告音を出力させてもよい。
【００２６】
そして本例の携帯電話端末１０は、電話通信用の通信回路１２とは別に、近距離無線通信用の通信回路３２を備え、接続されたアンテナ３１を介して、例えば数ｍから最大でも百ｍ程度の比較的狭い範囲内の相手と無線通信を行う（但し後述する無線キー装置と通常時に通信を行う際には通信可能範囲を狭くする処理をしてある）。ここでは、例えばBluetooth（商標）と称される近距離用の無線通信方式を適用してある。この近距離無線通信では、例えばハンズフリー通話用のヘッドセットと通信を行ったり、或いは、パーソナルコンピュータ装置と通信を行って、コンピュータ装置からのデータ通信を、携帯電話端末装置１０を介して行ったり、様々な用途が想定されている。無線通信に使用される周波数帯域としては、例えば２ＧＨｚ帯が使用されて、通信回路１２での無線電話通信とは干渉しない周波数帯又は変調方式としてあり、通信回路１２での無線電話通信と、近距離無線通信用の通信回路３２での通信とを同時に行うことができるようにしてある。
【００２７】
本例の場合には、この近距離通信用の通信回路３２を使って、無線キー装置５０と無線通信を行う。但し、同じ通信方式の通信機器であれば、無線キー装置５０以外の装置（ヘッドセット、パーソナルコンピュータ装置等）とも無線通信が可能である。また、セキュリティ機能を実行する場合には、通信回路３２で無線通信を行う無線キー装置５０が、特定の１台の装置に限定され、その装置の識別ＩＤなどが予めメモリ１８などに登録されている。この無線キー装置５０についての登録情報については、利用者は修正できないようにしてもよい。
【００２８】
通信回路３２内で送信信号を増幅する送信アンプ３３は、制御部１９などの制御で送信電力が複数段階に設定されるようにしてあり、無線キー装置５０と無線接続された状態では、その複数段階の中の低い送信電力を設定するようにしてある。無線キー装置５０以外の機器と接続された状態では、比較的高い段階の送信電力を設定するようにしてある。なお、後述するヘッドセットのように、無線キー装置としての機能が組み込まれた機器と無線接続された場合には、そのときの相手の機器の動作状態（即ち無線キー装置としてだけ作動しているのか、或いは組合された別の機能が作動しているのか否か）によって、送信電力が設定される。
【００２９】
また本例の通信回路３２内には、受信電界強度測定部３４を備え、通信回路３２で受信した信号の受信電界強度（ＲＳＳＩ）を測定して、受信電力値を得るようにしてある。この受信電界強度測定部３４で測定された受信電力値は、通信回路３２内で、無線通信状況又は無線通信距離を判定又は推定する判定に使用される。従って、本例の場合には、通信回路３２が、無線通信状況又は無線通信距離を判定又は推定する判定手段を備えることになる。
【００３０】
また本例の携帯電話端末３０は、非接触ＩＣカード機能部４０を備える。この非接触ＩＣカード機能部４０は、アンテナ４２が接続された課金データ制御部４１を有し、リーダ・ライタとの間で、数cm程度の非常に近接した距離での近接無線通信を行う。この近接無線通信を行う際には、リーダ・ライタ側からの電波を受信して得られる電力で、課金データ制御部４１を作動させることも可能であるが、本例においては携帯電話端末１０内の電

源回路２４から供給される電源で、課金データ制御部４１を作動させるようにしてある。

【００３１】

課金データ制御部４１は、ＩＣカード機能を実行する際に、課金や認証に必要なデータをメモリ１８（又は課金データ制御部４１内の図示しないメモリ）から読み出して、リーダ・ライタと近接無線通信でやり取りを行う。例えば、交通機関の乗車券として機能させる場合には、乗車券（定期券）として有効な区間、有効期間、或いは乗車券として引き落とすことが可能なチャージ金額などのデータや、この端末（ＩＣカード）の所持者に関する個人情報などを、課金データ制御部４１がリーダ・ライタに送って、課金処理や認証処理を行うようにしてある。社員証、会員証、代金決済用のカード、クレジットカードなどとして使用する場合には、それらの認証に必要な情報についても、やり取りされる。

【００３２】

さらに本例の携帯電話端末装置１０は、端子部２３を備え、図示しない各種周辺機器やデータ処理装置などを、この端子２３を使用して直接接続できる構成としてある。この場合、携帯電話端末装置１０内の各部に電源を供給する二次電池などが内蔵された電源回路２４から、端子部２３で接続された外部の機器にも電源を供給できる構成としてある。例えば、図１に破線の矢印Ｊで示すように、無線キー装置５０の端子部５６を、この携帯電話端末装置１０の端子部２３に直接接続させた場合に、携帯電話端末装置１０内の電源回路２４から、無線キー装置５０内の二次電池に充電電流を供給して、充電させることができるようにしてある。また、携帯電話端末装置１０の端子部２３に無線キー装置５０が直接接続された場合には、携帯電話端末装置１０の制御部１９がそのことを検出して、直接接続時のセキュリティ処理（例えば後述する近距離無線通信をしないで実行されるセキュリティ処理）を行うようにしてある。

【００３３】

次に、本例の携帯電話端末装置１０と無線通信を行う、無線キー装置５０の構成について、図３を参照して説明する。本例の無線キー装置５０は、近距離無線通信用の通信回路５２を備え、接続されたアンテナ５１を介して、例えば数ｍから最大でも百ｍ程度の比較的狭い範囲内の相手と無線通信を行う（但し携帯電話端末装置１０と通常時に通信を行う際には通信可能範囲を狭くする処理をしてある）。ここでは、携帯電話端末装置１０側が備えている近距離無線通信方式であるBluetooth方式を、無線キー装置５０も適用してある。通信回路５２で無線通信を行う相手は、登録された特定の１台の携帯電話端末装置１０に限定され、その装置の識別ＩＤなどが予め登録されている。この携帯電話端末装置１０についての登録情報については、利用者は修正できないようにしてもよい。

【００３４】

通信回路５２での無線通信については、制御部５３の制御で実行される。この場合、通信回路５２内で送信信号を増幅する送信アンプ５２ａは、制御部５３などの制御で送信電力が複数段階に設定されるようにしてあり、携帯電話端末装置１０と無線接続された状態では、複数段階の中の低い送信電力を設定するようにしてある。但し、無線キー装置５０に配置された操作部５９（図１に示したボタン形状の操作部など）が操作されたことを制御部５３が検出した場合には、一時的に送信アンプ５２ａで送信電力を高くして、強制的に相手に認識させる信号（ページ信号など）の送信処理を行うようにしてある。

【００３５】

本例の通信回路５２内には、受信電界強度測定部５２ｂを備え、通信回路５２で受信した信号の受信電界強度（ＲＳＳＩ）を測定して、受信電力値を得るようにしてある。この受信電界強度測定部５２ｂで測定された受信電力値は、通信回路５２内で、無線通信状況又は無線通信距離を判定又は推定する判定に使用される。従って、本例の場合には、通信回路５２が、無線通信状況又は無線通信距離を判定又は推定する判定手段を備えることになる。

【００３６】

本例の無線キー装置５０は、警告音を出力させるスピーカ５４ａが接続された警告音生成部５４と、発光ダイオードなどで構成される発光部５５とを備え、制御部５３の制御で

、警告音の出力や振動や発光を行う。これらの警告音生成部５４や発光部５５は、セキュリティ機能で必要な警告手段として使用する。また、発光部５５は、携帯電話端末装置１０と無線通信を行ってセキュリティ機能を作動させている状態で、現在のセキュリティモードを表示させる表示手段としても機能するようにしてある。具体的には、例えば、発光部５５が緑色で点滅しているとき、通常モードであることを表示し、赤色で点滅しているとき、警告モードであることを表示し、機能制限モードであるとき、何も点灯させないようにする等の表示の切替で、セキュリティモードを表示させる表示手段としても機能させる。このセキュリティモードを表示させる表示手段は、液晶ディスプレイなどを使用して、文字や図形などでモードが直接判る表示を行うようにしてもよい。また、振動で警告する警告手段としてもよい。

【００３７】

制御部５３と各部との間は制御ライン５８で接続してあり、制御部５３の制御で、通信回路５２での無線通信や、警告音生成部５４や発光部５５での動作などが実行される。

【００３８】

また、本例の無線キー装置５０は、端子部５６を備え、この端子５６を使用して携帯電話端末装置１０が直接接続できる構成としてある。この接続時には、無線キー装置５０内の制御部５３が、携帯電話端末装置１０内の制御部１９とデータ転送を直接行って、近距離無線通信をしないで直接接続時のセキュリティ処理を行うようにしてある。また、無線キー装置５０内の電源回路５７に内蔵された二次電池の充電残量が少ない場合には、携帯電話端末装置１０側から供給される充電電流で、電源回路５７内の二次電池を充電させることができるようにしてある。

【００３９】

このように構成される携帯電話端末装置１０と無線キー装置５０とを使用する際には、例えば図４に示すように、利用者は無線キー装置５０を常時身に付けておくことで、その利用者が携帯電話端末装置１０を使用する際には、機能が制限されないようにしてある（後述する通常モード）。そして、利用者は無線キー装置５０を常時身に付けた状態のままで、携帯電話端末装置１０をどこかに置いて、携帯電話端末装置１０からある程度の距離離れた場合に、無線キー装置５０から警告動作が行われ（後述する警告モード）、その警告動作が行われた状態で、携帯電話端末装置１０に近づかないでいると、携帯電話端末装置１０の機能が制限される状態となる（後述する機能制限モード）。なお、警告モードでの警告動作については、携帯電話端末装置１０側でだけ行うようにしてもよい。或いは、無線キー装置５０と携帯電話端末装置１０の双方で警告モードでの警告動作を行うようにしてもよい。

【００４０】

機能制限モードで携帯電話端末装置１０の機能が制限される状態としては、例えば、携帯電話端末装置１０の全ての機能を停止させても良いが（但しセキュリティ機能に関係した通信は制限させない）、端末装置１０が備える機能の内の一部だけの機能を停止させてもよい。具体的には、例えば非接触ＩＣカード機能部４０を使用した処理だけを制限させるようにしてもよい。また、携帯電話端末装置１０のアドレス帳閲覧やメール閲覧などの個人情報の表示などを制限させてもよい。また、無線電話としての発信を制限させて、着信だけができるようにしてもよい。この発信制限時には、警察などの緊急通報用の電話番号だけは発信規制しないようにしてもよい。また、無線電話装置としての機能だけを制限させて、非接触ＩＣカード機能部４０を使用した処理については制限させないようにしてもよい。

【００４１】

なお、ここまで説明した無線キー装置５０は、セキュリティ機能だけを行う専用の装置として構成させたが、他の機能を有する装置に、無線キー装置としての機能を組み込むようにしてもよい。例えば携帯電話端末装置１０とBluetooth方式の無線通信を行って、いわゆるハンズフリー通話を行うためのヘッドセットに、無線キー装置を組み込むようにしてもよい。

【００４２】
図５は、この無線キー付ヘッドセットの構成例を示した図である。本例の無線キー付ヘッドセット６０は、近距離無線通信用の通信回路６２を備え、接続されたアンテナ６１を介して、例えば数ｍから最大でも百ｍ程度の比較的狭い範囲内の相手と無線通信を行う。ここでは、携帯電話端末装置１０側が備えている近距離無線通信方式と同じ方式であるBluetooth方式を、無線キー付ヘッドセットの通信回路６２も適用してある。通信回路６２で無線通信を行う相手は、登録された特定の１台の携帯電話端末装置１０に限定され、その装置の識別ＩＤなどが予め登録されている。但し、ヘッドセットだけを使用する際には、通信回路６２で無線通信を行う相手を制限しないようにしてもよい。
【００４３】
通信回路６２での無線通信については、制御部６３の制御で実行される。この場合、通信回路６２内で送信信号を増幅する送信アンプ６２ａは、制御部６３などの制御で送信電力が設定されるようにしてある。
【００４４】
通信回路６２でヘッドセット用の通信（即ち通話用音声データの通信）を行う際には、受信した音声データを音声データ処理部６６に供給して音声データの受信処理を行ってからスピーカ６７に供給して出力させ、また、マイクロフォン６８が拾って音声データ処理部６６で処理された送信用の音声データを通信回路６２に供給して送信させる。
【００４５】
本例の通信回路６２内には、受信電界強度測定部６２ｂを備え、通信回路６２で受信した信号の受信電界強度（ＲＳＳＩ）を測定して、受信電力値を得るようにしてある。この受信電界強度測定部５２ｂで測定された受信電力値は、通信回路６２内で、無線通信状況又は無線通信距離を判定又は推定する判定に使用される。従って、本例の場合には、通信回路６２が、無線通信状況又は無線通信距離を判定又は推定する判定手段を備えることになる。
【００４６】
また本例の無線キー付ヘッドセット６０は、操作キーなどで構成された操作部６４と、メモリ６５と、発光部７０を備える。発光部７０はセキュリティ機能に関する警告手段として使用されるとともに、ヘッドセットとして機能させる際の動作状態の表示手段としても使用される。これらのヘッドセット６０内の各部は、制御ライン７３を介して制御データのやり取りが行えるとともに、データライン７４を介して音声データなどのやり取りが行える。
【００４７】
また、本例の無線キー付ヘッドセット６０は、端子部７１を備え、この端子７１を使用して携帯電話端末装置１０が直接接続できる構成としてある。この接続時には、無線キー付ヘッドセット６０内の制御部６３が、携帯電話端末装置１０内の制御部１９とデータ転送を直接行って、近距離無線通信をしないで直接音声データの転送やセキュリティ処理を行うようにしてある。また、無線キー付ヘッドセット６０内の電源回路７２に内蔵された二次電池の充電残量が少ない場合には、携帯電話端末装置１０側から供給される充電電流で、電源回路７２内の二次電池を充電させることができるようにしてある。
【００４８】
このような無線キー付ヘッドセット６０を用意した場合には、例えば図６に示すように、無線キー付ヘッドセット６０を装着した利用者が、カバンの中などに入ったままの携帯電話端末装置１０と無線通信を行って、いわゆるハンズフリー通話ができるとともに、無線キー装置としての機能を利用することで、無線キー付ヘッドセット６０と携帯電話端末装置１０との位置関係（距離）により、警告動作や機能制限動作を行う。即ち、無線キー付ヘッドセット６０から携帯電話端末装置１０がある程度の距離離れた場合に、無線キー付ヘッドセット６０又は携帯電話端末装置１０（或いは双方）から警告動作が行われ（後述する警告モード）、その警告動作が行われた状態で、携帯電話端末装置１０に近づかないでいると、携帯電話端末装置１０の機能が制限される状態となる（後述する機能制限モ

ード）。

【００４９】

次に、このような構成の携帯電話端末装置１０と無線キー装置５０を用意して、セキュリティ処理を行う場合の、基本的な処理例を、図７～図１９を参照して説明する。なお、以下の説明では無線キー装置５０を使うものとして説明するが、無線キー付ヘッドセット６０を使った場合のセキュリティ処理も、基本的には同様である。

【００５０】

まず、図７を参照して、セキュリティ処理のモードについて説明すると、本例の場合には、携帯電話端末装置１０の機能を制限しない通常モードＭ１と、携帯電話端末装置１０と無線キー装置５０との距離が離れるなどで、その通常モードから外れることを警告する警告モードＭ２と、警告モードから通常モードに戻らない場合に（即ち携帯電話端末装置１０と無線キー装置５０との距離が離れたままである場合に）、携帯電話端末装置１０の機能を制限する機能制限モードＭ３とが用意してある。

【００５１】

これらのモードの遷移としては、図７に矢印で示すように、通常モードＭ１から警告モードＭ２への変化、警告モードＭ２から機能制限モードＭ３への変化があり、また機能制限モードＭ３となった状態で、無線キー装置５０が携帯電話端末装置１０に近づくと、通常モードＭ１に戻る。さらに、警告モードＭ２となって警告動作が行われている状態で、無線キー装置５０が携帯電話端末装置１０に近づくと、通常モードＭ１に戻る。

【００５２】

本例の場合、これらのセキュリティモードは、携帯電話端末装置１０と無線キー装置５０との間での無線通信方式であるBluetooth方式で用意された通信モードと関連を持たせてある。即ち、図８に本例の無線通信方式（Bluetooth方式）での通信モードを示すと、携帯電話端末装置１０と無線キー装置５０の両者で、相手の機器を認証させて無線接続させる接続モードＭ１１があり、その接続モードＭ１１で相互に認証が完了して接続が行われると、実際にペイロードデータの転送が行われるデータ転送モードＭ１２となる。データ転送モードＭ１２でのデータ転送が完了すると、低消費電力通信モードＭ１３に移行する。この低消費電力通信モードＭ１３では、両者の無線通信が、データ転送モードＭ１２での通信周期よりも長い周期で間欠的に行われ、両者の無線接続を維持する状態となる。このように間欠通信を行う周期が長いことで、データ転送モードＭ１２で作動している場合よりも、通信に要する消費電力を小さくすることができ、低消費電力となる。なお、ここでの低消費電力とは、通信周期の間引きから低消費電力になることを示しており、後述する送信電力を下げる処理とは直接関係がない（但し後述するように低消費電力モード中には送信電力を下げる処理を行うようにしてある）。

【００５３】

この低消費電力通信モードＭ１３の状態で、両者間でのデータ転送を再開させる場合には接続モードＭ１１に戻り、接続モードＭ１１で通信を再開させる処理が行われて、実際にデータ転送が行われるデータ転送モードＭ１２となる。低消費電力通信モードＭ１３で無線接続が維持された状態では、接続モードＭ１１での接続処理が比較的簡単に行われ、無線接続をやり直す場合に比べて、データ転送モードＭ１２でのデータ転送の再開が迅速に行える。

【００５４】

また、接続モードＭ１１でいずれかの通信相手と接続処理が行われない場合（或いは接続できない場合）には、それぞれの機器は、スタンバイモードＭ１４に移行する。このスタンバイモードＭ１４となった機器は、非常に長い周期での間欠受信又は送信を行って、相手となる通信機器が存在するかをサーチする処理を行う。なお、スタンバイモードＭ１４となった機器は、ユーザ操作などの何らかの契機となる処理がないと、接続モードＭ１１に戻らないようにしてもよい。また、２台の機器間で通信を行っている間は、２台の機器は、基本的に同じモードが設定されるようにしてある。即ち、少なくとも接続モードＭ１１とデータ転送モードＭ１２と低消費電力モードＭ１３は、２台の機器間で同期して移

行するモードである。

【００５５】

ここで、本例の場合には、図８に示すように、携帯電話端末装置１０と無線キー装置５０との間で、低消費電力通信モードＭ１３で通信している状態のとき、セキュリティモードとして通常モードＭ１を設定し、低消費電力通信モードＭ１３から接続モードＭ１１に通信モードが移行したことを契機として、警告モードが開始される。警告モードから機能制限モードに移行する処理の詳細については後述するが、セキュリティモードが機能制限モードＭ３となると、接続モードＭ１１，データ転送モードＭ１２，スタンバイモードＭ１４である間は、機能制限モードＭ３のままとする。データ転送モードＭ１２から低消費電力通信モードＭ１３に移行した場合にだけ、セキュリティモードが機能制限モードＭ３から通常モードＭ１に戻るようにしてある。

【００５６】

次に、携帯電話端末装置１０と無線キー装置５０のそれぞれで、セキュリティモードが選定される処理を、図９を参照して説明する。このセキュリティモード選定処理は、例えばそれぞれの機器の制御部１９，５３の制御で実行される。まず、現在の通信モードが、低消費電力通信モードであるか否か判断される（ステップＳ１）。ここで、低消費電力通信モードである場合には、制御部内に用意されるステートタイマをリセットし（ステップＳ２）、セキュリティモードを通常モードに設定し（ステップＳ３）、通常モードとしての処理（即ち機能を制限しないモード）として作動させる（ステップＳ４）。なお、ステートタイマは時間の経過でカウントアップするタイマである。

【００５７】

また、ステップＳ１で低消費電力通信モードでないと判断した場合には、直前（現在）のセキュリティモードが通常モードであるか否か判断し（ステップＳ５）、通常モードである場合には、制御部内に用意されるステートタイマをスタートさせ（ステップＳ６）、警告モードの開始を設定させ（ステップＳ７）、警告モードとしての警告動作を実行させる（ステップＳ８）。なお、携帯電話端末装置１０と無線キー装置５０のいずれか一方だけで警告動作を行う構成となっている場合には、他方の装置では、この警告モード中には特に処理を行わない。

【００５８】

そして、ステップＳ５で直前（現在）のセキュリティモードが通常モードでないと判断した場合には、ステップＳ６で起動させたステートタイマのカウント値が、予め決められた値ＴＨを超えたか否か判断する（ステップＳ９）。カウント値が所定値ＴＨ１を超えるまでは、ステップＳ８の警告モードのままとし、カウント値が所定値ＴＨ１を超えた場合には、セキュリティモードを警告モードに変化させる（ステップＳ１０）。ステートタイマのカウント値が、カウント開始から所定値ＴＨ１を越えるまでの時間は、例えば、数秒から数十秒程度の時間とする。

【００５９】

次に、携帯電話端末装置１０と無線キー装置５０のそれぞれで、各通信モードでの通信状態の具体的な例を、図１０以降を参照して説明する。まず、接続モードで携帯電話端末装置１０と無線キー装置５０とが相手の認証処理を行う例を説明する。Bluetooth方式で無線通信を行う場合には、通信を行う２台の機器の内の一方の通信装置がマスタ機器となり、他方の通信装置がスレーブ機器となる。Bluetooth方式のシステム上は、いずれの機器がマスタ、スレーブになっても良いが、本例の場合、携帯電話端末装置１０と無線キー装置５０との間で無線通信を行う場合には、無線キー装置５０がマスタとなり、携帯電話端末装置１０がスレーブとなるようにしてある。

【００６０】

スレーブとなった機器（ここでは携帯電話端末装置１０）は、接続モードのとき、マスタを探すスキャン処理を行う。図１０は、このスキャン処理時の動作例を示したフローチャートである。スキャン処理時には、一定期間連続受信して、マスタからの信号を探す処理を行う（ステップＳ１１）。そのスキャン処理で、セキュリティ処理を行う相手である

無線キー装置５０のＩＤ番号が付与された信号（ページ信号）を受信したか否か判断する（ステップＳ１２）。ここで、無線キー装置５０のＩＤ番号が付与された信号を受信できない場合には、アイドル処理に移って一定期間待機した後に（ステップＳ１３）、ステップＳ１１に戻って、スキャン処理を繰り返し行う。

【００６１】

そして、ステップＳ１２で無線キー装置５０のＩＤ番号が付与されたページ信号を受信できたと判断した場合には、そのページ信号に対する応答信号を送信し（ステップＳ１４）、マスタと接続処理を行って、通信状態に移行（即ちデータ転送モードに移行）する（ステップＳ１６）。

【００６２】

また、マスタとなった機器（ここでは無線キー装置５０）は、接続モードが開始したとき、スタンバイタイマをスタートさせ（ステップＳ２１）、所定期間、決められたチャンネルでページ信号を送信する（ステップＳ２２）。このときのページ信号には、例えば自機に設定されたＩＤ番号を付与するとともに、通信相手のＩＤ番号を付与する。そして、そのページ信号の送信後にスレーブからの応答があるか否か判断し（ステップＳ２３）、応答がない場合には、スタンバイタイマのカウント値が決められた時間ＴＨ２を越えたか否か判断する（ステップＳ２４）。スタンバイタイマのカウント値が決められた時間ＴＨ２を越えていない場合には、アイドル処理に移って一定期間待機した後に（ステップＳ２５）、ステップＳ２２に戻って、ページ信号の送信処理を繰り返し行う。

【００６３】

そして、ステップＳ２３でスレーブからの応答があると判断した場合には、スレーブとの接続処理を行って、通信状態に移行（即ちデータ転送モードに移行）する（ステップＳ２７）。また、ステップＳ２４で、スタンバイタイマのカウント値が決められた時間ＴＨ２を越えた場合には、スタンバイ状態となり（ステップＳ２８）、ここでのスレーブとの接続を試みる処理を中止する。

【００６４】

図１２は、図１０のフローチャートの処理が行われているマスタとなった機器（無線キー装置５０）と、図１１のフローチャートの処理が行われているスレーブとなった機器（携帯電話端末装置１０）との通信状態の例を示した図である。図１２（ａ）は、マスタ（無線キー装置５０）のページ信号の送信タイミングとアイドル期間を示し、図１２（ｂ）は、スレーブ（携帯電話端末装置１０）の受信（スキャン）タイミングとアイドル期間を示したものである。図１２に示すように、送信側のアイドル期間と受信側のアイドル期間は異なり、受信側でいずれかのタイミングで送信されるページ信号を受信できるようにしてある。

【００６５】

図１３は、この図１２の処理をシーケンス図で示したものである。図１３に示すように、無線キー装置５０からは間欠的にページ信号の送信（タイミングＴ１１，Ｔ１２，Ｔ１３）が行われる。ここで、ページ信号に対するレスポンスがあると（タイミングＴ１４）、さらに２台の機器間でレスポンスの相互のやり取りがあり（タイミングＴ１５，Ｔ１６）、その後、無線接続を行うコネクション信号の相互のやり取りが行われて（タイミングＴ１７，Ｔ１８）、データ転送モードに移行する。

【００６６】

次に、本例の各機器がデータ転送モードに移行した場合の処理例を、図１４のフローチャートを参照して説明する。データ転送モードに移行すると、そのデータ転送が行われるチャンネルでの認証処理が行われ（ステップＳ３１）、その認証が正しく完了したか否か判断される（ステップＳ３２）。ここで認証処理が完了しない場合には、接続処理に戻る。

【００６７】

そして、ステップＳ３２での接続処理が完了した場合には、通常はデータ転送が行われるが、本例のセキュリティ処理のための通信時には、データ転送を行わず、直接、低消費

電力モードに移行する処理が行われる（ステップＳ３３）。そして、低消費電力モードに移行できるか否か判断し（ステップＳ３４）、低消費電力モードに移行できる状態である場合には、低消費電力モードのスニフ状態に設定する。低消費電力モードに移行できない場合には、接続処理に戻る。なお、ステップＳ３３での低消費電力モードに移行する処理を行う際には、例えば、双方の通信回路３２，５２内の送信アンプを、

【００６８】

図１５は、図１４のフローチャートで示した通信状態の例を示したシーケンス図である。即ち、データ転送モードで、認証などを行うために相互にパケットの伝送を行い（タイミングＴ２１，Ｔ２２，Ｔ２３，Ｔ２４）、その認証が完了してから、低消費電力モードに移行するためのデータ（スニフモードリクエスト）をマスタ（無線キー装置５０）から送り（タイミングＴ２５）、その了解を受信することで（タイミングＴ２６）、双方の機器が低消費電力モード（スニフモード）に移行する。

【００６９】

図１６は、低消費電力モード（スニフモード）での、スレーブ（携帯電話端末装置１０）での処理例を示したフローチャートである。その処理を説明すると、スニフモードとなると、まずタイマをスタートさせ（ステップＳ４１）、マスタからの信号を受信するスキャン処理を行う（ステップＳ４２）。そのスキャン処理で、セキュリティ処理を行う相手である無線キー装置５０のＩＤ番号が付与された信号（ページ信号）を受信したか否か判断する（ステップＳ４３）。ここで、無線キー装置５０のＩＤ番号が付与された信号を受信した場合には、そのページ信号に対する応答信号を送信し（ステップＳ４４）、ステップＳ４１でスタートさせたタイマをリセットさせ（ステップＳ４５）、アイドル期間に移る（ステップＳ４６）。一定期間のアイドル期間が経過すると、ステップＳ４２のスキャン処理に戻る。ここで、本例の場合には、ステップＳ４６でのアイドル期間（通信が行われない期間）を、比較的長い期間に設定してあるとともに、マスタ側でのアイドル期間と同期させるようにしてある。

【００７０】

そして、ステップＳ４３で無線キー装置５０のＩＤ番号が付与された信号を受信できないと判断した場合には、ステップＳ４１でスタートさせたタイマが、所定値Ｔ　ＳＶを越えたか否か判断し（ステップＳ４７）、所定値Ｔ　ＳＶを越えていない場合には、ステップＳ４６のアイドル処理に移る。そして、ステップＳ４７で所定値Ｔ　ＳＶを越えたと判断された場合、通信モードを接続モードに変化させる（ステップＳ４８）。通信モードを接続モードに変化させる際には、送信アンプの送信電力を高く変化させてもよい。

【００７１】

図１７は、低消費電力モード（スニフモード）での、マスタ（無線キー装置５０）での処理例を示したフローチャートである。その処理を説明すると、スニフモードとなると、まずタイマをスタートさせ（ステップＳ５１）、ページ信号を所定期間送信する処理を行う（ステップＳ５２）。このページ信号の送信後に、セキュリティ処理を行う相手（携帯電話端末装置１０）からの応答を受信したか否か判断する（ステップＳ５３）。ここで、応答信号を受信した場合には、ステップＳ５１でスタートさせたタイマをリセットさせ（ステップＳ５４）、アイドル期間に移る（ステップＳ５５）。一定期間のアイドル期間が経過すると、ステップＳ５２のページ信号送信処理に戻る。ここで、本例の場合には、ステップＳ５５でのアイドル期間（通信が行われない期間）を、比較的長い期間に設定するとともに、スレーブ側でのアイドル期間と同期させるようにしてある。

【００７２】

そして、ステップＳ５３で携帯電話端末装置１０からの応答を受信できないと判断した場合には、ステップＳ５１でスタートさせたタイマが、所定値Ｔ　ＳＶを越えたか否か判断し（ステップＳ５６）、所定値Ｔ　ＳＶを越えていない場合には、ステップＳ５５のアイドル処理に移る。そして、ステップＳ５６で所定値Ｔ　ＳＶを越えたと判断された場合、通信モードを接続モードに変化させる（ステップＳ５７）。通信モードを接続モードに変化させる際には、送信アンプの送信電力を高く変化させてもよい。

【００７３】
図１８は、低消費電力モード（スニフモード）での、両機器での通信タイミングを示したシーケンス図である。この図１８に示すように、マスタでのスニフ処理が行われるタイミング（オンと記載された部分）と、スレーブでのスニフ処理が行われるタイミングとはほぼ一致する。即ち、マスタからポーリングパケットが送信されるタイミング（Ｔ３１，Ｔ３３，Ｔ３５，Ｔ３７）と、スレーブでその受信が行われる期間とが一致し、各ポーリングパケットがスレーブで受信されて、その応答（タイミングＴ３２，Ｔ３４，Ｔ３６，Ｔ３８）についても、マスタ側で受信される。このように間欠的な双方向の通信が行われていることで、低消費電力モードが維持され、マスタとスレーブ間の無線接続状態が維持される。

【００７４】
なお、通信モードがスタンバイ状態になった場合には、例えば図１９のフローチャートに示した処理が行われる。即ち、スタンバイ状態になると、起動タイマに起動させる期間を設定させ（ステップＳ６１）、その起動タイマをスタートさせ（ステップＳ６２）、通信回路をスリープ状態とする（ステップＳ６３）。その後、起動タイマが設定した期間が経過すると、通信回路を起動させて（ステップＳ６４）、接続処理を実行して、接続できる機器があるかの処理に移る。

【００７５】
ここまで説明した処理が実行されることで、携帯電話端末装置１０と無線キー装置５０との間での、近距離無線通信が行われ、携帯電話端末装置１０と無線キー装置５０とが近接した状態で良好に無線通信できる場合には、携帯電話端末装置１０と無線キー装置５０とが低消費電力モードで無線接続された状態に維持される。この低消費電力モードで無線接続された状態では、いわゆるペイロードとなるデータの転送は行われず、無線接続を維持させるための信号が間欠的に送受信されるだけであり、アイドル期間を適切に選定することで、非常に少ない消費電力で、通信が行える。従って、本例のセキュリティ処理を行うことによる消費電力を、少なくすることができ、携帯電話端末装置１０と無線キー装置５０の双方の電池持続時間を長時間化することができる。特に、出来るだけ小型に構成させたい無線キー装置に、大きな効果がある。

【００７６】
そして、携帯電話端末装置１０については、既に携帯電話端末に組み込まれた例が多数あるBluetooth方式の近距離無線通信方式を適用して、セキュリティ処理を行うようにしたので、既存のBluetooth方式の近距離無線通信回路を備えた携帯電話端末の制御構成などを若干変更するだけで、本例のセキュリティ処理が実現可能であり、簡単に良好なセキュリティ機能が実現できる。

【００７７】
ここまで説明した処理は、本例のセキュリティ処理を行う上での基本的な処理であるが、ここで本例においては、携帯電話端末装置１０と無線キー装置５０との間で、低消費電力モードで通信を行って、無線接続されている状態で、以下の処理を行って、より良好にセキュリティモード設定が行えるようにしてある。即ち、低消費電力モードで通信を行っている状態では、基本的な通信処理としては、図１６、図１７のフローチャートに示した通信処理が行われるが、本例においては、受信電界強度についても判断して、その判断結果をセキュリティモード選択する上での判断材料の一つとして利用した処理を行う。なお、以下の説明では、携帯電話端末装置１０をスレーブ、無線キー装置５０をマスタとした例で説明してあるが、携帯電話端末装置１０がマスタ、無線キー装置５０がスレーブであってもよい。

【００７８】
図２０は、スレーブ（携帯電話端末装置１０）が低消費電力モード（スニフモード）で、受信電界強度（受信電力）を測定しながら処理を行う例を示したフローチャートである。この処理は、基本的にBluetooth通信処理を実行する通信回路３２，５２内での処理で実行されるものである。また、測定された受信電力に基づいて通信状態を判定するために

、これらの通信回路内には、受信電力と比較するための第１の閾値ＴＨ１と第２の閾値ＴＨ２が設定してある（ＴＨ１＞ＴＨ２）。この第１の閾値ＴＨ１は、例えば携帯電話端末装置１０と無線キー装置５０との間の距離が数ｍ（例えば３ｍ程度）である場合の平均的な受信電力値とする。第２の閾値ＴＨ２は、例えば携帯電話端末装置１０と無線キー装置５０との間の距離がより長い距離（例えば７ｍ程度）である場合の平均的な受信電力値とする。さらに、通信状態のステートとして、「良」、「警告」、「不良」の３つのステートを設定して記憶できるようにしてある。

【００７９】

図２０に基づいて処理を説明すると、スニフモードとなると、まずタイマをスタートさせ（ステップＳ２０１）、ステートとして「良」を設定し（ステップＳ２０２）、マスタからの信号を受信するスキャン処理を行う（ステップＳ２０３）。そのスキャン処理で、セキュリティ処理を行う相手である無線キー装置５０のＩＤ番号が付与された信号（ページ信号）を受信したか否か判断する（ステップＳ２０４）。ここで、無線キー装置５０のＩＤ番号が付与された信号を受信した場合には、そのページ信号に対する応答信号を送信し（ステップＳ２０５）、ステップＳ２０１でスタートさせたタイマをリセットさせ（ステップＳ２０６）、受信電界強度測定部３４で測定した受信電界強度（受信電力）を測定する（ステップＳ２０７）。

【００８０】

その後、測定した受信電力値のフィルタ処理を行って平均化を行い（ステップＳ２０８）、その平均化された受信電力値が、予め設定されている第１の閾値ＴＨ１より大きいか否か判断する（ステップＳ２０９）。第１の閾値ＴＨ１より大きい場合には、ステートとして「良」を設定する（ステップＳ２１０）。また、第１の閾値ＴＨ１を越えていない場合には、受信電力値が、予め設定されている第２の閾値ＴＨ２より大きいか否か判断する（ステップＳ２１１）。第２の閾値ＴＨ２より大きい場合には、ステートとして「警告」を設定する（ステップＳ２１２）。第２の閾値ＴＨ２を越えていない場合には、ステートとして「不良」を設定する（ステップＳ２１３）。

【００８１】

これらのステートの更新が行われると、アイドル期間に移る（ステップＳ２１４）。一定期間のアイドル期間が経過すると、ステップＳ２０３のスキャン処理に戻る。ここで、本例の場合には、ステップＳ２１４でのアイドル期間（通信が行われない期間）を、比較的長い期間に設定してあるとともに、マスタ側でのアイドル期間と同期させるようにしてある。

【００８２】

そして、ステップＳ２０４で無線キー装置５０のＩＤ番号が付与された信号を受信できないと判断した場合には、ステップＳ２０１でスタートさせたタイマが、所定値Ｔ　ＳＶを越えたか否か判断し（ステップＳ２１５）、所定値Ｔ　ＳＶを越えていない場合には、このときの受信電力値を０として（ステップＳ２１６）、ステップＳ２０８のフィルタ処理を行って平均化を行い、ステップＳ２０９以降のステート判定処理に移る。

【００８３】

そして、ステップＳ２１５で所定値Ｔ　ＳＶを越えたと判断された場合、ステートとして「不良」を設定した上で（ステップＳ２１７）、通信モードを接続モードに変化させる（ステップＳ２１８）。通信モードを接続モードに変化させる際には、送信アンプの送信電力を高く変化させてもよい。

【００８４】

図２１は、低消費電力モード（スニフモード）での、マスタ（無線キー装置５０）での処理例を示したフローチャートである。その処理を説明すると、スニフモードとなると、まずタイマをスタートさせ（ステップＳ２２１）、ページ信号を所定期間送信する処理を行う（ステップＳ２２２）。このページ信号の送信後に、セキュリティ処理を行う相手（携帯電話端末装置１０）からの応答を受信したか否か判断する（ステップＳ２２３）。ここで、応答信号を受信した場合には、ステップＳ２２１でスタートさせたタイマをリセッ

トさせ（ステップＳ２２４）、受信電界強度測定部５２ｂで測定した受信電界強度（受信電力）を測定する（ステップＳ２２５）。

【００８５】

その後、測定した受信電力値のフィルタ処理を行って平均化を行い（ステップＳ２２６）、その平均化された受信電力値が、予め設定されている第１の閾値ＴＨ１より大きいか否か判断する（ステップＳ２２７）。第１の閾値ＴＨ１より大きい場合には、ステートとして「良」を設定する（ステップＳ２２８）。また、第１の閾値ＴＨ１を越えていない場合には、受信電力値が、予め設定されている第２の閾値ＴＨ２より大きいか否か判断する（ステップＳ２２９）。第２の閾値ＴＨ２より大きい場合には、ステートとして「警告」を設定する（ステップＳ２３０）。第２の閾値ＴＨ２を越えていない場合には、ステートとして「不良」を設定する（ステップＳ２３１）。

【００８６】

これらのステートの更新が行われると、アイドル期間に移る（ステップＳ２３２）。一定期間のアイドル期間が経過すると、ステップＳ２２２のページ信号送信処理に戻る。ここで、本例の場合には、ステップＳ２３２でのアイドル期間（通信が行われない期間）を、比較的長い期間に設定してあるとともに、スレーブ側でのアイドル期間と同期させるようにしてある。

【００８７】

そして、ステップＳ２２３で携帯電話端末装置１０からの応答を受信できないと判断した場合には、ステップＳ２２１でスタートさせたタイマが、所定値Ｔ　ＳＶを越えたか否か判断し（ステップＳ２３３）、所定値Ｔ　ＳＶを越えていない場合には、このときの受信電力値を０として（ステップＳ２３４）、ステップＳ２２６のフィルタ処理を行って平均化を行い、ステップＳ２２７以降のステート判定処理に移る。

【００８８】

そして、ステップＳ２３３で所定値Ｔ　ＳＶを越えたと判断された場合、ステートとして「不良」を設定した上で（ステップＳ２３５）、通信モードを接続モードに変化させる（ステップＳ２３６）。通信モードを接続モードに変化させる際には、送信アンプの送信電力を高く変化させてもよい。

【００８９】

図２２は、図２０、図２１の処理で設定されたステートに基づいて、セキュリティモードを設定する処理例を示したフローチャートである。まず、現在のステートが「良」であるか否か判断する（ステップＳ２４１）。現在のステートが「良」である場合には、セキュリティモードとして通常モードを設定して（ステップＳ２４２）、通常モードで作動させる（ステップＳ２４３）。

【００９０】

また、現在のステートが「良」でない場合には、現在のステートが「警告」であるか否か判断する（ステップＳ２４４）。現在のステートが「警告」である場合には、直前のセキュリティモードが機能制限モードであるか否か判断する（ステップＳ２４５）。直前のセキュリティモードが機能制限モードでない場合には、セキュリティモードとして警告モードを設定して（ステップＳ２４６）、警告モードで作動させる（ステップＳ２４７）。

【００９１】

また、ステップＳ２４４で現在のステートが「警告」でない場合には、セキュリティモードとして機能制限モードを設定して（ステップＳ２４８）、機能制限モードで作動させる（ステップＳ２４９）。ステップＳ２４５で機能制限モードであると判断した場合には、そのままステップＳ２４９の機能制限モードで作動させる。

【００９２】

このようにして、受信電界強度の測定に基づいた処理を行うことで、通信モードが低消費電力モードで変化しない状況（即ち低消費電力モードで接続されたままの状態）であっても、携帯電話端末装置１０と無線キー装置５０との間の距離や通信環境に変化があると、セキュリティモードが警告モードや機能制限モードに変化して、セキュリティ処理を良

好に行える。また、警告モードや機能制限モードであっても、無線接続が維持された状態となる場合があるため、その場合には通信状態が良好になって通常モードに戻る処理が迅速に行える。

【００９３】

なお、通信回路３２，５２内で判定されたステートの状態に基づいて、セキュリティモードの設定は、制御ブロック１９，５３側で行われるが、ステートの状態の制御部への報告は、例えば図２３に示す処理で行うようにしてもよい。即ち、通信回路内で受信電力をモニタして（ステップＳ２５１）、その結果でステートの状態が変化したか否か判断する（ステップＳ２５２）。そして、ステートの状態が変化しない場合には、状態を制御部に報告しない。ステートの状態が変化した場合には、制御部（ＣＰＵ）への割り込み処理で、ステートの状態変化を通知する（ステップＳ２５３）。このようにすることで、セキュリティモードに関連した制御部での処理を最小限に抑えることができ、低消費電力化に貢献する。

【００９４】

或いは、図２４に示すように、例えば携帯電話端末装置１０の場合、制御部１９側に受信電界強度測定部１９ａを設けて、近距離通信回路３２での受信電力を、電話通信用の通信回路１２側での間欠受信に同期して処理して、制御部１９が電話通信用の間欠通信処理のために起動している間に、ステートの状態判定とセキュリティモードの設定処理を行うようにしてもよい。

【００９５】

また、ここまで説明した図２０～図２２の処理では、測定された受信レベルの絶対値に基づいてステートを設定するようにしたが、受信レベルの変動の差分からステートを設定するようにしてもよい。即ち、基本的には受信レベルが、通信相手との距離に対応するが、実際には距離だけでなく、障害物の有無・種類によっても大きく変動する。このため、受信レベルだけで距離そのものを厳密に判定（推定）することは不可能である。

【００９６】

ここで、受信電力と２台の機器間の無線通信距離を図２５に示すように、距離に対する減衰量はほぼ一定であり、同一速度で端末装置１０と無線キー装置５０との距離が離れていくと、受信強度の変化量はほぼ一定となる。従って、前回測定した受信強度との差を測定して、

・変化量が継続的にマイナス（レベルが下がっている）の場合には、端末装置と無線キー装置との距離が離れていると判断して、警告モード或いは機能制限モードに移行させる。
・変化量が継続的にプラス（レベルが上がっている）の場合には、端末装置と無線キー装置との距離が近づいていると判断して、警告モード或いは機能制限モードを解除させる。

【００９７】

測定した受信強度ＲＳＳＩの差は、例えば以下のように求める。

ΔＲＳＳＩ［ｎ］＝filter（ＲＳＳＩ［ｎ］－ＲＳＳＩ［ｎ－Ｍ］）

但し、filterは過去の値を平均化するか、又は低域通過フィルタを通過させた処理を示し、Ｍは想定する移動速度と受信強度ＲＳＳＩのサンプル速度に応じて決定される。

【００９８】

図３０は、この受信強度との差分による処理と、受信強度の絶対値による処理を組み合わせた場合の処理例を示したフローチャートである。この図３０は、スレーブの例を示してあるが、マスタ側も同様に適用できる。

【００９９】

図３０に基づいて説明すると、スニフモードとなると、まずタイマをスタートさせ（ステップＳ２９１）、ステートとして「良」を設定し（ステップＳ２９２）、マスタからの信号を受信するスキャン処理を行う（ステップＳ２９３）。そのスキャン処理で、セキュリティ処理を行う相手である無線キー装置５０のＩＤ番号が付与された信号（ページ信号）を受信したか否か判断する（ステップＳ２９４）。ここで、無線キー装置５０のＩＤ番号が付与された信号を受信した場合には、そのページ信号に対する応答信号を送信し（ス

テップＳ２９５）、ステップＳ２９１でスタートさせたタイマをリセットさせ（ステップＳ２９６）、受信電界強度測定部３４で測定した受信電界強度（受信電力）を測定する（ステップＳ２９７）。

【０１００】

その後、測定した受信電力値のフィルタ処理を行って平均化を行い（ステップＳ２９８）、さらに受信電力の差分を判断する（ステップＳ２９９）。そして、ステップＳ２９８で平均化された受信電力値が、予め設定されている第１の閾値ＴＨ１より大きいか否か判断する（ステップＳ３００）。第１の閾値ＴＨ１より大きい場合には、ステップＳ２９９で判断した差分が－ＴＨｄより小さいか否か判断する（ステップＳ３０１）。ここで、－ＴＨｄより小さい値である場合には、２台の距離が遠ざかっていると判断して、警告モードに移行しやすいように、第１の閾値ＴＨ１を増加させる（ステップＳ３０２）。そして、ステートとして「良」を設定する（ステップＳ３０３）。

【０１０１】

また、ステップＳ３００で第１の閾値ＴＨ１を越えていない場合には、受信電力値が、予め設定されている第２の閾値ＴＨ２より大きいか否か判断する（ステップＳ３０５）。第２の閾値ＴＨ２より大きい場合には、ステートとして「警告」を設定する（ステップＳ３０６）。第２の閾値ＴＨ２を越えていない場合には、ステップＳ２９９で判断した差分がＴＨｄより大きいか否か判断する（ステップＳ３０７）。ここで、ＴＨｄより大きい値である場合には、２台の距離が近づいていると判断して、通常モードに移行しやすいように、第１の閾値ＴＨ１を減少させる（ステップＳ３０８）。そして、ステートとして「不良」を設定する（ステップＳ３０９）。

【０１０２】

これらのステートの更新が行われると、アイドル期間に移る（ステップＳ３０４）。一定期間のアイドル期間が経過すると、ステップＳ２９３のスキャン処理に戻る。

【０１０３】

そして、ステップＳ２９４で無線キー装置５０のＩＤ番号が付与された信号を受信できないと判断した場合には、ステップＳ２９１でスタートさせたタイマが、所定値Ｔ　ＳＶを越えたか否か判断し（ステップＳ３９１）、所定値Ｔ　ＳＶを越えていない場合には、このときの受信電力値を０として（ステップＳ３９２）、ステップＳ２９８のフィルタ処理を行って平均化を行い、ステップＳ２９９での差分検出とそれ以降のステート判定処理に移る。

【０１０４】

そして、ステップＳ３９１で所定値Ｔ　ＳＶを越えたと判断された場合、ステートとして「不良」を設定した上で（ステップＳ３９３）、通信モードを接続モードに変化させる（ステップＳ３９４）。

【０１０５】

この図３０に示すように処理されることで、そのときの通信状況に応じた補正が行われながら、ステートの判断が行われる。

【０１０６】

また、ここまでの説明では、携帯電話端末装置１０と無線キー装置５０のそれぞれで個別にステートを設定して、セキュリティモードを設定するようにしたが、それぞれで検出されたステートの状態を、無線通信で相手に送信して、それぞれでセキュリティモードを選定する際に、自らのステートと、通信で報告されたステートとを組み合わせて、セキュリティモードを設定するようにしてもよい。

【０１０７】

図２６は、この場合の処理例を示したフローチャートである。まず、受信電力を測定し（ステップＳ２６１）、その測定でステートが変化したか否か判断する（ステップＳ２６２）。ここで、変化があった場合には、相手に送信するパケットに、ステート変化を報告するデータを付加する（ステップＳ２６３）。このステート変化を報告するデータとしては、ステートが３種類であるので、２ビットあればよい。

【０１０８】
そして、そのステート変化を報告するデータが付加されたパケット、或いはステート変化を報告するデータが付加されていないパケットを送信する（ステップＳ２６４）。その後、自局側でも、受信パケットを解析し（ステップＳ２６５）、ステート変化を報告するデータが付加されている場合には、そのデータから相手の状態を判断する（ステップＳ２６６）。

【０１０９】
図２７は、このようにして得た双方のステートから、セキュリティモードを設定する例を示した図である。即ち、例えば通常モードである場合（ステップＳ２７１）には、自局のステートが良でなくなるとともに、相手のステートが良でなくなると、警告モードにする（ステップＳ２７２）。さらに、警告モードの状態で、自局のステートが不良になり、相手のステートも不良になると、機能制限モードにする（ステップＳ２７３）。また、機能制限モードの状態で、自局のステートが良になり、相手のステートも良になると、通常モードにする（ステップＳ２７１）。

【０１１０】
或いは、図２８に示すように、処理してもよい。即ち、例えば通常モードである場合（ステップＳ２８１）には、自局のステートと相手のステートの何れか一方が良でなくなると、警告モードにする（ステップＳ２８２）。さらに、警告モードの状態で、自局のステートが不良になり、相手のステートも不良になると、機能制限モードにする（ステップＳ２８３）。また、機能制限モードの状態で、自局のステートが良になり、相手のステートも良になると、通常モードにする（ステップＳ２８１）。この図２８の例の場合には、警告モードに入るのが早くなる。

【０１１１】
状態変化の通知としては、例えば図２９に示すように処理できる。即ち、マスタから間欠送信されるパケット（poll）に状態変化のデータを付加し、スレーブからは、そのパケットに対する返送（ＡＣＫ）に状態変化のデータを付加する。

【０１１２】
次に、本発明の第２の実施の形態を、図３１～図３７を参照して説明する。本実施の形態においては、上述した第１の実施の形態と同様に、携帯電話端末装置１０と無線キー装置５０を用意して、セキュリティ処理を行うようにしたものであり、その基本的な処理については第１の実施の形態と同様である。そして第１の実施の形態の場合には、低消費電力モードの場合に、受信電界強度に基づいてセキュリティモードを設定するようにしたが、本実施の形態の場合には、受信パケットの検出状況に基づいて、通信状況又は通信距離を判定（推定）して、セキュリティモードを設定するようにした。その他の処理については、第１の実施の形態と同じである。

【０１１３】
受信パケットの検出処理について、図３１を参照して説明すると、低消費電力モード（スニフモード）では、図３１（ａ）に示すように無線キー装置からスニフスロットがオンのタイミングになると、複数のパケットが送信され、図３１（ｂ）に示すように携帯端末装置からその応答のパケットが送信される。それぞれで受信されたパケットは、通信回路内でエラー検出処理が行われ、エラー無しのパケットが受信成功と判断される。図３１の例では、全てのパケットの伝送に成功した例であるが、例えば図３２に示すように、通信状態が悪い場合には、×印をつけたパケットの受信に失敗する状況もある。この通信状況の悪化は、通信距離にほぼ比例するため、このことを利用して、通信状況又は通信距離を判定又は推定するようにしたものである。

【０１１４】
図３３は、本例でのスレーブ（携帯電話端末装置１０）が低消費電力モード（スニフモード）で、受信電界強度（受信電力）を測定しながら処理を行う例を示したフローチャートである。この処理は、基本的にBluetooth通信処理を実行する通信回路３２，５２内での処理で実行されるものである。この例でも、測定された受信電力に基づいて通信状態を

判定するために、これらの通信回路内には、受信電力と比較するための第１の閾値ＴＨ１と第２の閾値ＴＨ２が設定してある（ＴＨ１＞ＴＨ２）。この第１の閾値ＴＨ１は、例えば携帯電話端末装置１０と無線キー装置５０との間の距離が数ｍ（例えば３ｍ程度）である場合の平均的なパケットエラーレート値とする。第２の閾値ＴＨ２は、例えば携帯電話端末装置１０と無線キー装置５０との間の距離がより長い距離（例えば７ｍ程度）である場合の平均的なパケットエラーレート値とする。さらに、通信状態のステートとして、「良」、「警告」、「不良」の３つのステートを設定して記憶できるようにしてある。

【０１１５】

図３３に基づいて処理を説明すると、スニフモードとなると、まずタイマをスタートさせ（ステップＳ３１１）、ステートとして「良」を設定し（ステップＳ３１２）、マスタからの信号を受信するスキャン処理を行う（ステップＳ３１３）。そのスキャン処理で、セキュリティ処理を行う相手である無線キー装置５０のＩＤ番号が付与された信号（ページ信号）を受信したか否か判断する（ステップＳ３１４）。ここで、無線キー装置５０のＩＤ番号が付与された信号を正しく受信した場合には、そのページ信号に対する応答信号を送信し（ステップＳ３１５）、ステップＳ３１１でスタートさせたタイマをリセットさせ（ステップＳ３１６）、パケットエラーレートＰＥＲを０とする（ステップＳ３１７）。

【０１１６】

その後、検出されたパケットエラーレートＰＥＲのフィルタ処理を行って平均化を行い（ステップＳ３１８）、その平均化されたパケットエラーレート値が、予め設定されている第１の閾値ＴＨ１より小さいか否か判断する（ステップＳ３１９）。第１の閾値ＴＨ１より小さい場合には、ステートとして「良」を設定する（ステップＳ３２０）。また、第１の閾値ＴＨ１より小さくない場合には、パケットエラーレート値が、予め設定されている第２の閾値ＴＨ２より小さいか否か判断する（ステップＳ３２２）。第２の閾値ＴＨ２より小さい場合には、ステートとして「警告」を設定する（ステップＳ３２３）。第２の閾値ＴＨ２より小さくない場合には、ステートとして「不良」を設定する（ステップＳ３２４）。

【０１１７】

これらのステートの更新が行われると、アイドル期間に移る（ステップＳ３２１）。一定期間のアイドル期間が経過すると、ステップＳ３１３のスキャン処理に戻る。ここで、本例の場合には、ステップＳ３１３でのアイドル期間（通信が行われない期間）を、比較的長い期間に設定してあるとともに、マスタ側でのアイドル期間と同期させるようにしてある。

【０１１８】

そして、ステップＳ３２５で無線キー装置５０のＩＤ番号が付与された信号を受信できないと判断した場合には、ステップＳ３１１でスタートさせたタイマが、所定値Ｔ　ＳＶを越えたか否か判断し（ステップＳ３２５）、所定値Ｔ　ＳＶを越えていない場合には、このときのパケットエラーレートを１として（ステップＳ３２６）、ステップＳ３１８のフィルタ処理を行って平均化を行い、ステップＳ３１９以降のステート判定処理に移る。

【０１１９】

そして、ステップＳ３２５で所定値Ｔ　ＳＶを越えたと判断された場合、ステートとして「不良」を設定した上で（ステップＳ３２７）、通信モードを接続モードに変化させる（ステップＳ３２８）。通信モードを接続モードに変化させる際には、送信アンプの送信電力を高く変化させてもよい。

【０１２０】

図３４は、低消費電力モード（スニフモード）での、マスタ（無線キー装置５０）での本例での処理例を示したフローチャートである。その処理を説明すると、スニフモードとなると、まずタイマをスタートさせ（ステップＳ３３１）、ページ信号を所定期間送信する処理を行う（ステップＳ３３２）。このページ信号の送信後に、セキュリティ処理を行う相手（携帯電話端末装置１０）からの応答を受信したか否か判断する（ステップＳ３３

３）。ここで、応答信号を受信した場合には、ステップＳ３３４でスタートさせたタイマをリセットさせ（ステップＳ３３４）、パケットエラーレートを０とする（ステップＳ３３５）。

【０１２１】

その後、検出されたパケットエラーレートＰＥＲのフィルタ処理を行って平均化を行い（ステップＳ３３６）、その平均化されたパケットエラーレート値が、予め設定されている第１の閾値ＴＨ１より小さいか否か判断する（ステップＳ３３７）。第１の閾値ＴＨ１より小さい場合には、ステートとして「良」を設定する（ステップＳ３３８）。また、第１の閾値ＴＨ１より小さくない場合には、パケットエラーレート値が、予め設定されている第２の閾値ＴＨ２より小さいか否か判断する（ステップＳ３４０）。第２の閾値ＴＨ２より小さい場合には、ステートとして「警告」を設定する（ステップＳ３４１）。第２の閾値ＴＨ２より小さくない場合には、ステートとして「不良」を設定する（ステップＳ３４２）。

【０１２２】

これらのステートの更新が行われると、アイドル期間に移る（ステップＳ３３９）。一定期間のアイドル期間が経過すると、ステップＳ３３２のページ信号送信処理に戻る。ここで、本例の場合には、ステップＳ３３９でのアイドル期間（通信が行われない期間）を、比較的長い期間に設定してあるとともに、スレーブ側でのアイドル期間と同期させるようにしてある。

【０１２３】

そして、ステップＳ３３３で携帯電話端末装置１０からの応答を受信できないと判断した場合には、ステップＳ３３１でスタートさせたタイマが、所定値Ｔ　ＳＶを越えたか否か判断し（ステップＳ３４３）、所定値Ｔ　ＳＶを越えていない場合には、このときのパケットエラーレートを１として（ステップＳ３４４）、ステップＳ３３６のフィルタ処理を行って平均化を行い、ステップＳ３３７以降のステート判定処理に移る。

【０１２４】

そして、ステップＳ３４３で所定値Ｔ　ＳＶを越えたと判断された場合、ステートとして「不良」を設定した上で（ステップＳ３４５）、通信モードを接続モードに変化させる（ステップＳ３４６）。通信モードを接続モードに変化させる際には、送信アンプの送信電力を高く変化させてもよい。

【０１２５】

図３３、図３４の処理で設定されたステートに基づいて、セキュリティモードを設定する処理としては、例えば既に説明した図２２の処理が適用できる。このようにして、パケットエラーレートに基づいた処理を行うことで、受信電界強度の測定に基づいて処理する第１の実施の形態の場合と同様に、セキュリティ処理を良好に行える。

【０１２６】

なお、ここまでの例では、パケットエラーレートで判断するようにしたが、送信側でステートに基づいて１単位のスニフスロット内で送信させるパケット数を変化させて、そのパケット数を受信側で検出して、同様の判断を行うようにしてもよい。即ち、受信したパケット数をＮとすると、図３５に示すように、通常モードのとき（ステップＳ３６１）、受信できたパケット数がステート良のパケット数Ｎより少なくなると、警告モードとする（ステップＳ３６２）。警告モードで受信できたパケット数がステート良のパケット数Ｎを越えると、通常モードに戻す。そして、警告モードで受信できたパケット数が、警告ステートのパケット数Ｎより少なくなると、機能制限モードとする（ステップＳ３６３）。機能制限モードで、ステート良のパケット数Ｎが検出されると、通常モードに戻す。

【０１２７】

このようにパケット数を制限させることで、例えば図３６に示すように、携帯電話端末装置１０と無線キー装置５０との間で、スニフスロットの期間に送信されるパケット数が変化するようになる。

【０１２８】

図３７は、送信させるパケット数を選定する処理例を示したフローチャートである。まず、受信判定を行い（ステップＳ３７１）、ステート状態タイマをリセットし（ステップＳ３７２）、現在のステートがいずれであるか判断する（ステップＳ３７３）。ここで、ステートが良である場合には、通常のパケット数で送信させる（ステップＳ３７４）。また、ステートが警告である場合には、ステート状態タイマの値が所定値ＴＷを越えているか否か判断し（ステップＳ３７５）、越えている場合には通常のパケット数で送信させ（ステップＳ３７６）、越えていない場合には、制限されたパケット数で送信させる（ステップＳ３７７）。

【０１２９】

また、ステートが不良である場合には、ステート状態タイマの値が所定値ＴＢを越えているか否か判断し（ステップＳ３７８）、越えている場合には通常のパケット数で送信させ（ステップＳ３７９）、越えていない場合には、制限されたパケット数で送信させる（ステップＳ３８０）。

【０１３０】

このようにして送信させるパケット数を変化させることで、パケットにステートを知らせるデータを付加しなくても、相手にステートを知らせることができ、効率のよいセキュリティ処理が行える。

【０１３１】

なお、上述した各実施の形態では、携帯電話端末１０に、Bluetooth方式などの近距離無線通信手段を内蔵させて、その近距離無線通信手段をセキュリティモード作動用に使用したが、例えば、携帯電話端末１０には、近距離無線通信手段を内蔵させず、外付けで携帯電話端末１０に近距離無線通信手段を接続させるようにしてもよい。即ち、例えば無線キー装置に相当する装置を２個用意して、その２個の無線キー装置の内の一方を、携帯電話端末１０に接続させて、その２個の無線キー装置での通信モードによって、セキュリティモードを設定させてもよい。

【０１３２】

また、ここまで説明した実施の形態では、携帯電話端末にBluetooth方式の通信回路を内蔵させて、その通信回路で無線キー装置と無線通信を行うようにしたが、その他の無線通信方式で、無線キー装置と無線通信を行うようにしてもよい。即ち、無線通信方式として、少なくとも、通信する双方の装置間でデータ転送可能とする第１の通信モードと、無線接続された状態のままで、第１の通信モードでの通信よりも少ない周期で双方の装置間で無線通信を行う第２の通信モードとを有した方式であれば、上述した実施の形態と同様の処理が可能であり、適用可能である。

【０１３３】

また、Bluetooth方式の場合には、通信を行う一方がマスタとなり、他方がスレーブとなるが、上述した無線キー装置側をマスタとし携帯端末側をスレーブとするのは一例であり、逆でもよい。また、通信途中で、マスタとスレーブを入れ替えるようにしてもよい。

【０１３４】

また、上述した実施の形態では、携帯電話端末装置のセキュリティ確保処理に適用したが、その他の携帯型の端末装置のセキュリティ確保を、同様の処理で適用してもよい。

【０１３５】

また、無線キー装置についても、上述した実施の形態では専用のキー装置として構成した例としたが、Bluetooth方式などで通信可能な端末装置（例えばＰＤＡ装置など）に、本発明のキー装置として機能させるプログラムをインストールして、キー装置として機能するようにしてもよい。

【図面の簡単な説明】

【０１３６】

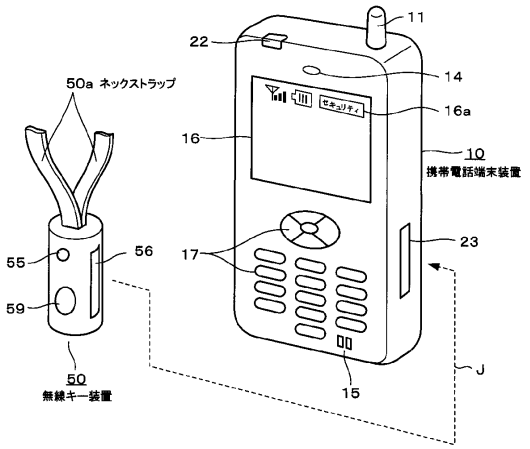
【図１】本発明の第１の実施の形態によるシステム構成例を示した斜視図である。

【図２】本発明の第１の実施の形態による通信端末装置の構成例を示したブロック図である。

【図３】本発明の第１の実施の形態による無線キー装置の構成例を示したブロック図である。
【図４】本発明の第１の実施の形態による使用例を示した説明図である。
【図５】本発明の第１の実施の形態による無線キー装置の変形例（ヘッドセットと一体化させた例）を示したブロック図である。
【図６】図５の例の使用例を示した説明図である。
【図７】本発明の第１の実施の形態によるセキュリティモードの設定例を示した説明図である。
【図８】本発明の第１の実施の形態による通信モードによるセキュリティモードの遷移例を示した説明図である。
【図９】本発明の第１の実施の形態によるモード選定処理例を示したフローチャートである。
【図１０】本発明の第１の実施の形態によるスキャン処理例を示したフローチャートである。
【図１１】本発明の第１の実施の形態によるページ送信処理例を示したフローチャートである。
【図１２】本発明の第１の実施の形態によるページ送信とスキャンの処理状態の例を示したタイミング図である。
【図１３】本発明の第１の実施の形態による接続状態の例を示したシーケンス図である。
【図１４】本発明の第１の実施の形態による低消費電力移行処理例を示したフローチャートである。
【図１５】本発明の第１の実施の形態による通信状態メッセージの伝送例を示したシーケンス図である。
【図１６】本発明の第１の実施の形態による携帯端末での通信処理例を示したフローチャートである。
【図１７】本発明の第１の実施の形態による無線キー装置での通信処理例を示したフローチャートである。
【図１８】本発明の第１の実施の形態によるスニフ状態での伝送例を示したシーケンス図である。
【図１９】本発明の第１の実施の形態によるスタンバイ状態での処理例を示したフローチャートである。
【図２０】本発明の第１の実施の形態によるスニフモードでのスレーブの受信電界強度に基づいた処理例を示したフローチャートである。
【図２１】本発明の第１の実施の形態によるスニフモードでのマスタの受信電界強度に基づいた処理例を示したフローチャートである。
【図２２】本発明の第１の実施の形態によるモード選定処理例を示したフローチャートである。
【図２３】本発明の第１の実施の形態による制御部の割り込み処理例を示したフローチャートである。
【図２４】制御部に受信電界強度測定部を設けた場合の構成例を示したブロック図である。
【図２５】受信電力と装置（デバイス）間の距離の変化例を示した説明図である。
【図２６】本発明の第１の実施の形態による状況判定結果を送信する場合の処理例を示したフローチャートである。
【図２７】本発明の第１の実施の形態によるモード変化例を示した説明図である。
【図２８】本発明の第１の実施の形態によるモード変化例（変形例）を示した説明図である。
【図２９】本発明の第１の実施の形態によるモードの通知例を示した説明図である。
【図３０】本発明の第１の実施の形態によるスニフモードでの受信電界強度とその差分に基づいた処理例を示したフローチャートである。

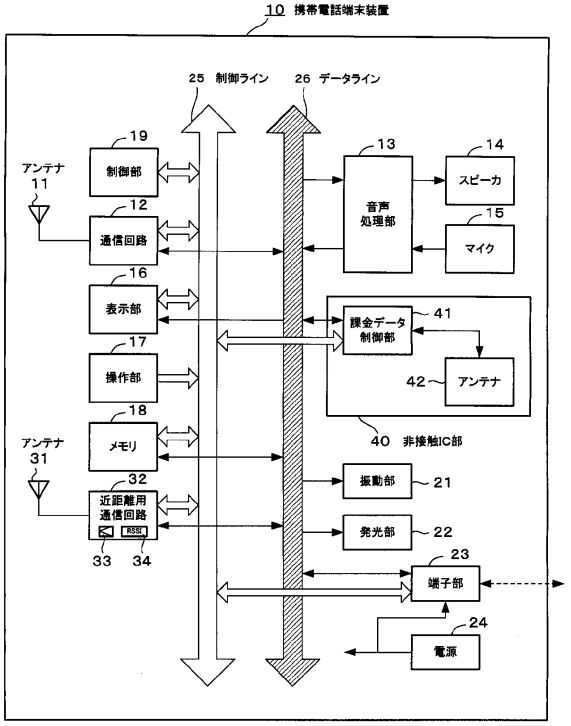
【図３１】本発明の第２の実施の形態によるパケット伝送処理例を示したタイミング図である。
【図３２】本発明の第２の実施の形態によるパケット伝送処理例（エラーがある場合の例）を示したタイミング図である。
【図３３】本発明の第２の実施の形態によるスニフモードでのスレーブの処理例を示したフローチャートである。
【図３４】本発明の第２の実施の形態によるスニフモードでのマスタの処理例を示したフローチャートである。
【図３５】本発明の第２の実施の形態によるモード遷移例を示したフローチャートである。
【図３６】本発明の第２の実施の形態による送信パケット数制限時の伝送処理例を示したタイミング図である。
【図３７】本発明の第２の実施の形態による送信パケット数制限処理例を示したフローチャートである。
【符号の説明】
【０１３７】
１０…携帯電話端末装置、１１…アンテナ、１２…無線電話用通信回路、１３…音声処理部、１４…スピーカ、１５…マイクロフォン、１６…表示部、１７…操作部、１８…メモリ、１９…制御部、２１…振動部、２２…発光部、２３…端子部、２４…電源回路、２５…制御ライン、２６…データライン、３１…アンテナ、３２…近距離無線通信回路、３３…送信アンプ、３４…受信電界強度測定部、４０…非接触ＩＣカード機能部、４１…課金データ制御部、４２…アンテナ、５０…無線キー装置、５１…アンテナ、５２…近距離無線通信回路、５２ａ…送信アンプ、５２ｂ…受信電界強度測定部、５３…制御部、５４…振動部、５５…発光部、５６…端子部、５７…電源回路、５８…制御ライン、５９…操作部、６０…無線キー付ヘッドセット、６１…アンテナ、６２…近距離無線通信回路、６２ａ…送信アンプ、６２ｂ…受信電界強度測定部、６３…制御部、６４…操作部、６５…メモリ、６６…音声処理部、６７…スピーカ、６８…マイクロフォン、６９…振動部、７０…発光部、７１…端子部、７２…電源回路、７３…制御ライン、７４…データライン

【図１】

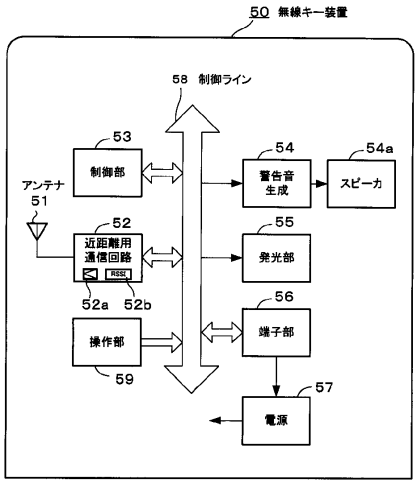


装置例

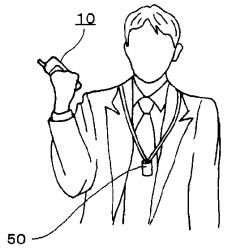
【図２】



【図３】

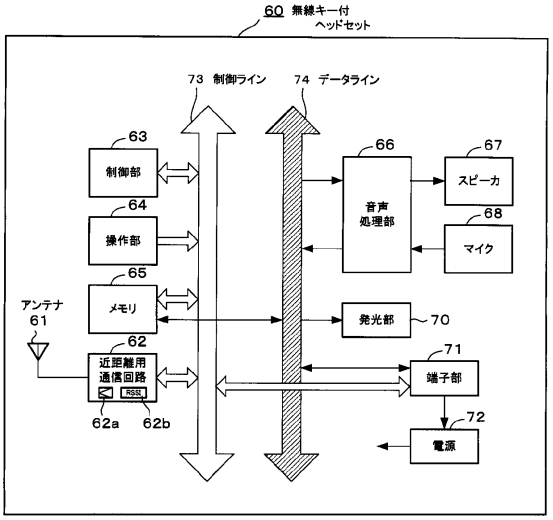


【図４】



使用例

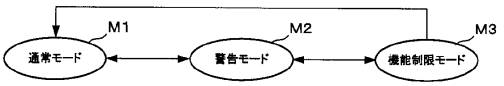
【図５】



【図６】

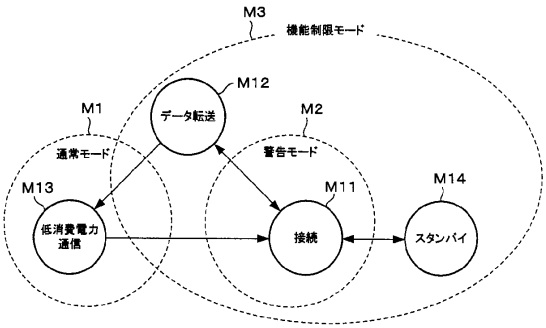
使用例

【図７】



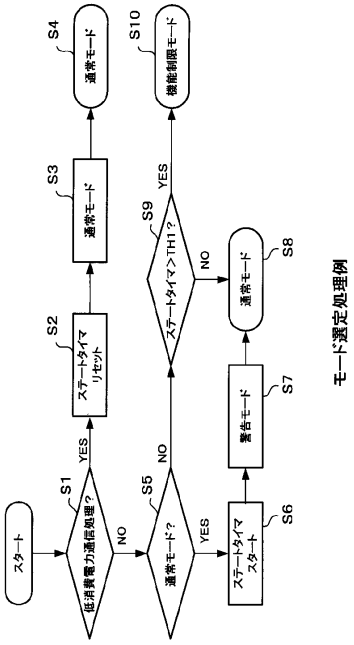
セキュリティ機能モード遷移例

【図８】



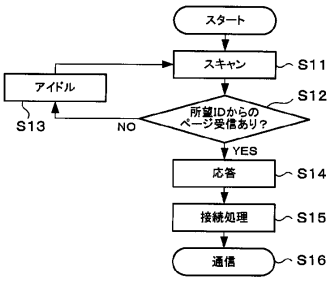
モード遷移例

【図９】



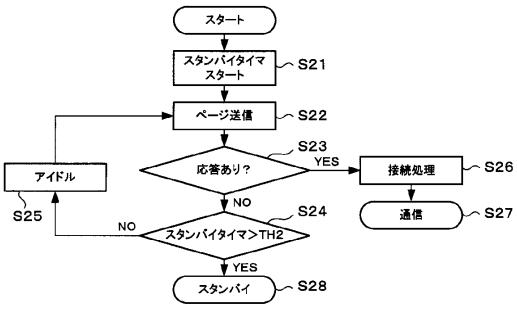
モード選定処理例

【図１０】



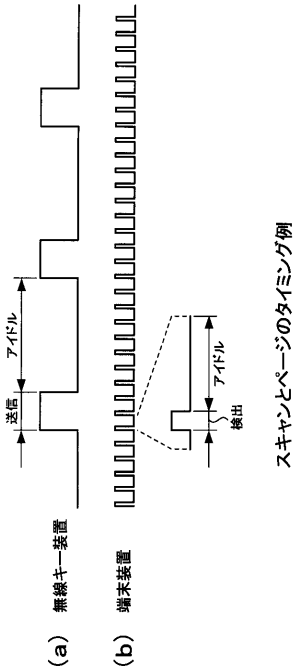
スキャン処理例

【図１１】

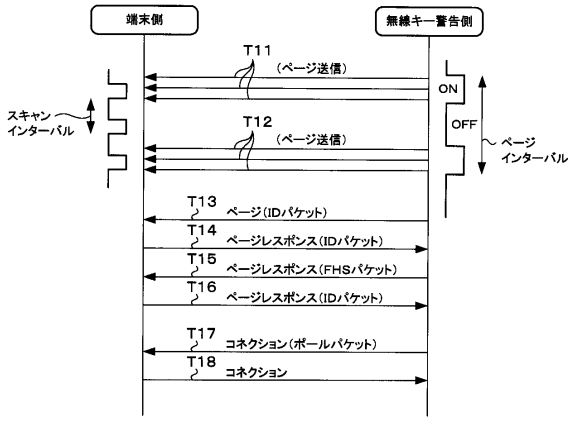


ページ送信処理例

【図１２】

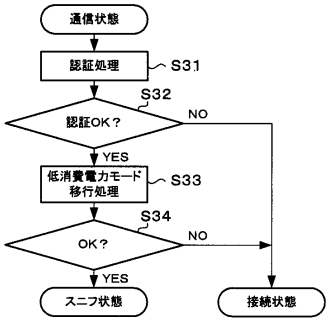


【図１３】



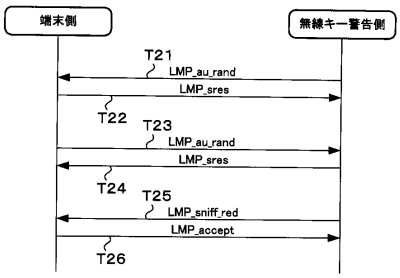
接続状態メッセージシーケンス

【図１４】



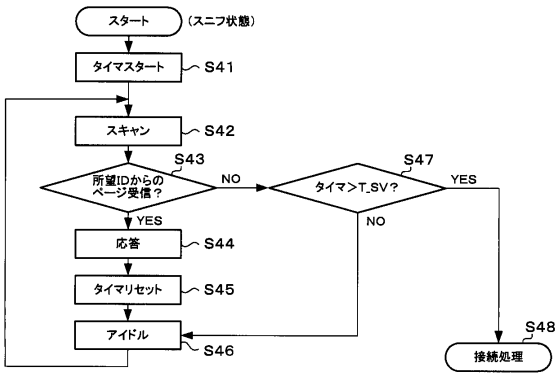
低消費電力移行処理例

【図１５】



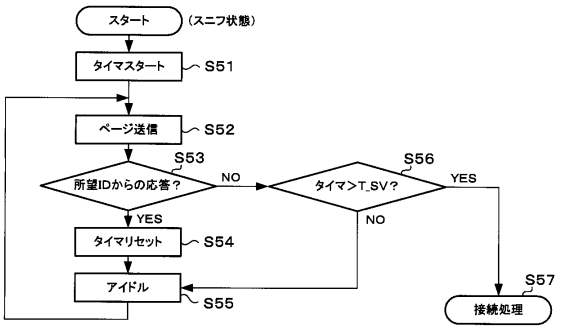
通信状態メッセージシーケンスの例

【図１６】



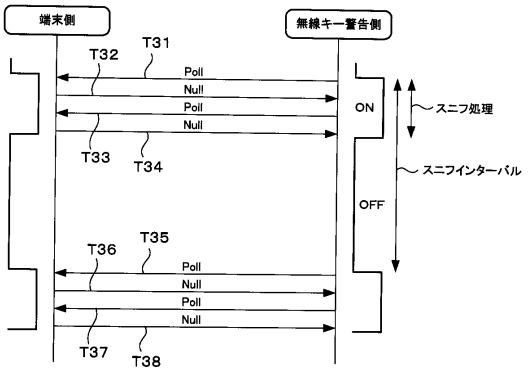
携帯端末での処理例

【図１７】



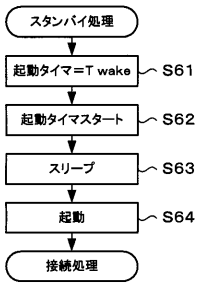
無線キーでの処理例

【図１８】



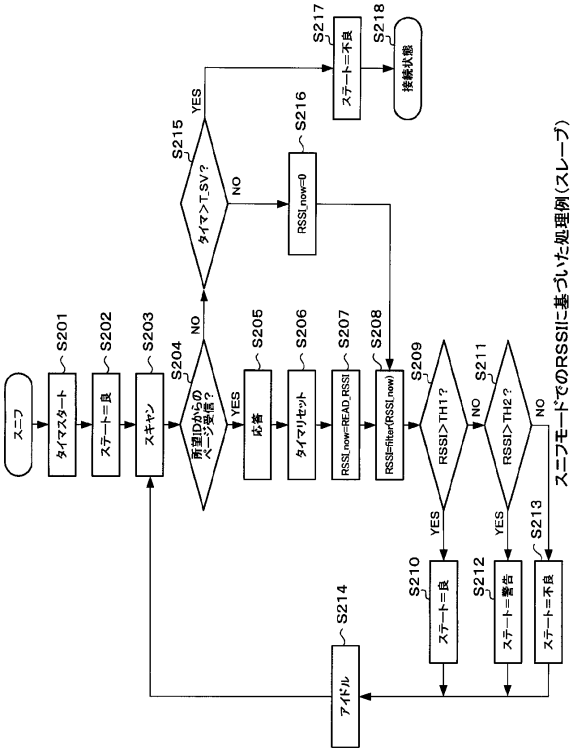
スニフ状態のシーケンス

【図１９】

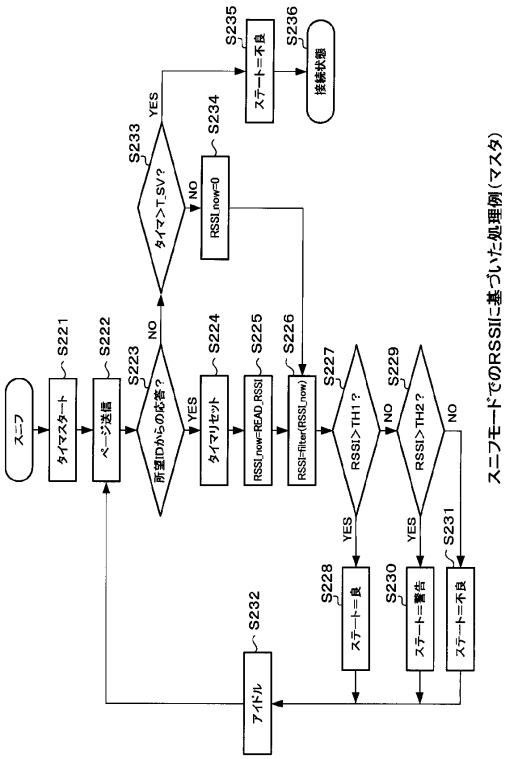


スタンバイ処理例

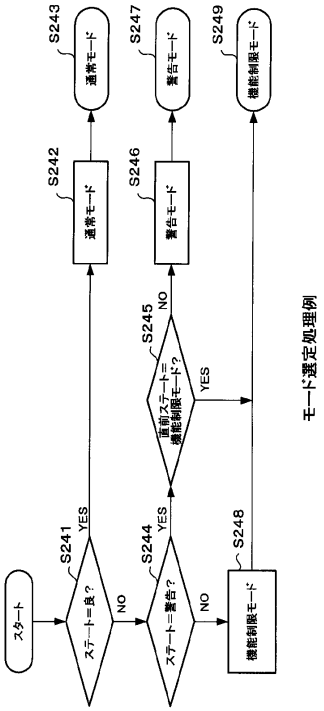
【図２０】



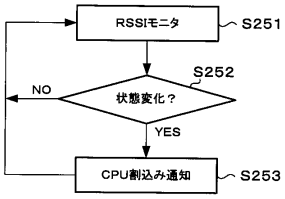
【図２１】



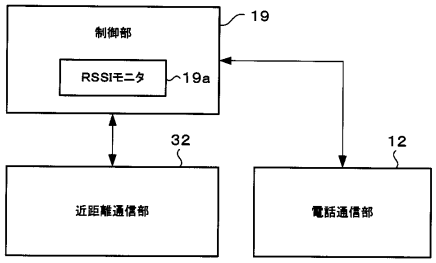
【図２２】



【図２３】

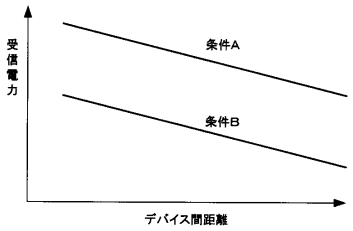


【図２４】



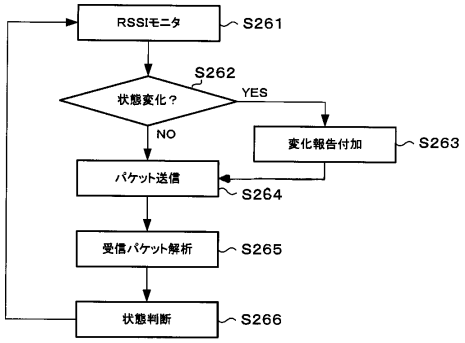
制御部にRSSIモニタを実装させた例

【図２５】

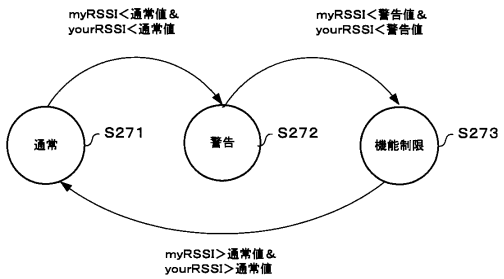


受信電力とデバイス間距離の例

【図２６】

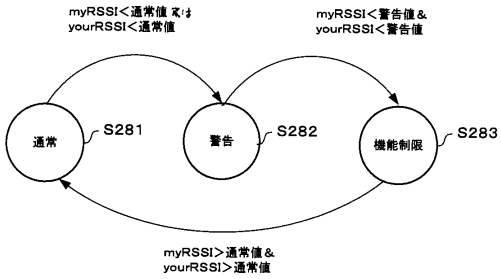


【図２７】



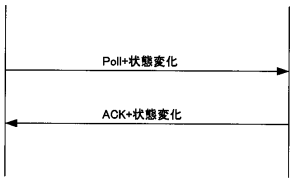
モード変化例

【図２８】



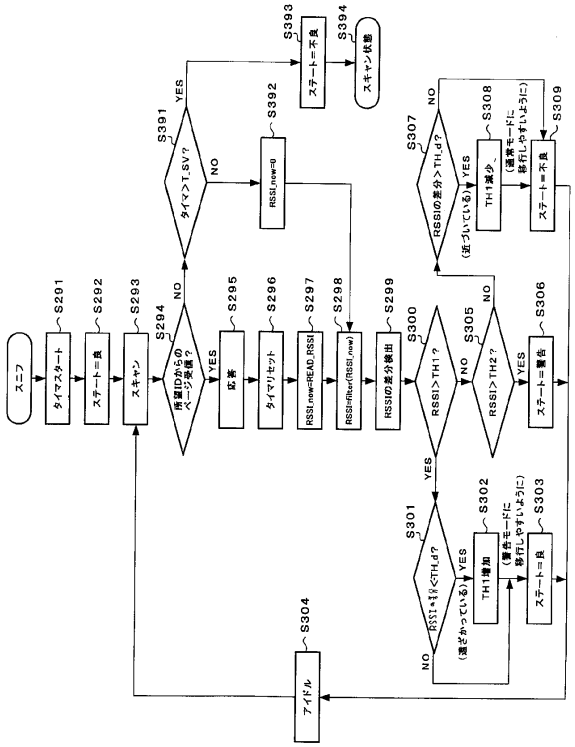
モード変化例

【図２９】

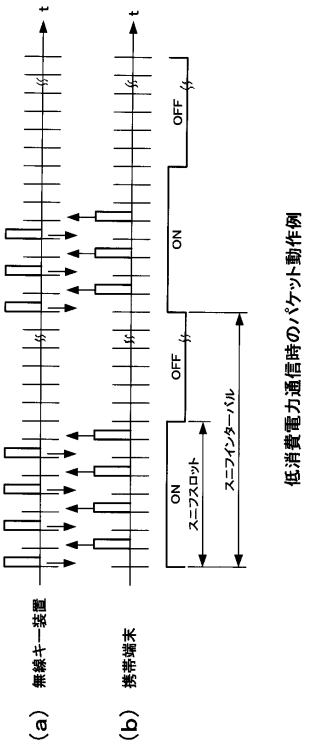


状態変化の通知例

【図３０】

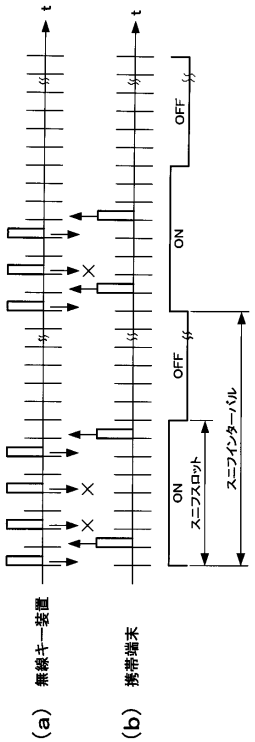


【図３１】



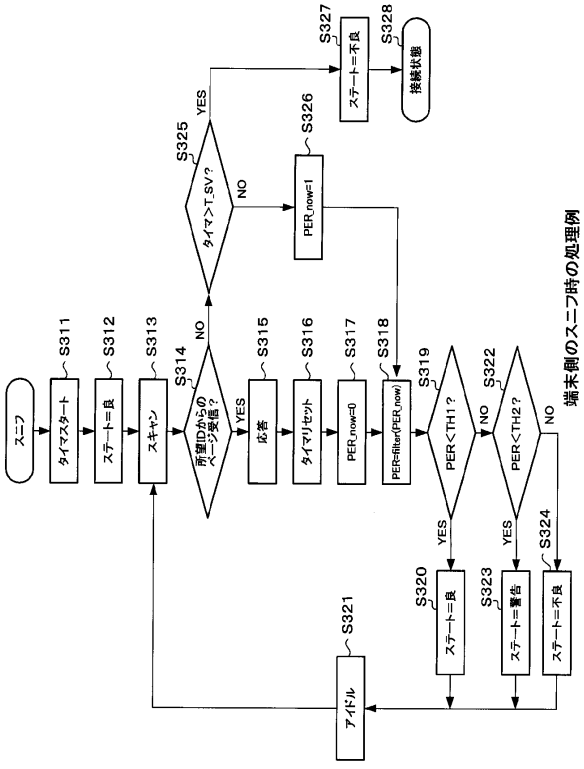
低消費電力通信時のパケット動作例

【図３２】



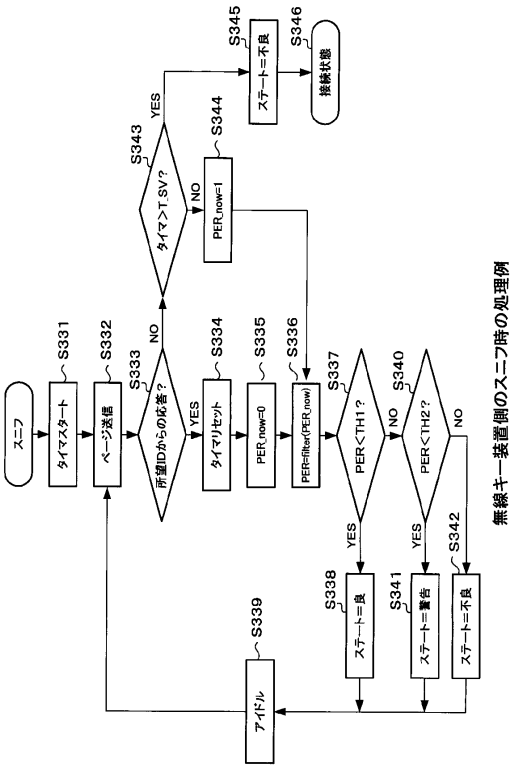
エラーがある場合の低消費電力通信時のパケット動作例

【図３３】



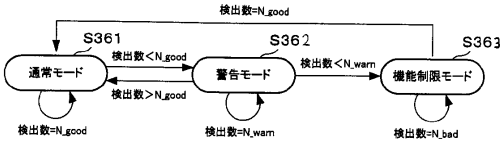
端末側のスニフ時の処理例

【図３４】



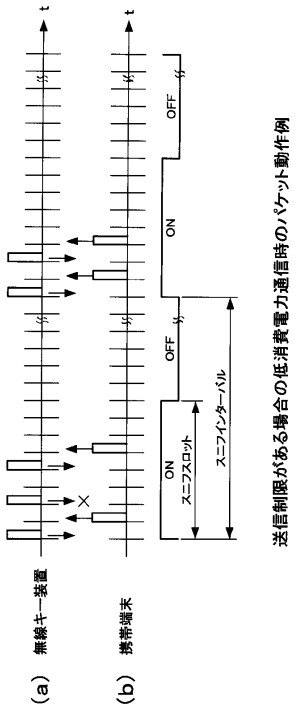
無線キー装置側のスニフ時の処理例

【図３５】



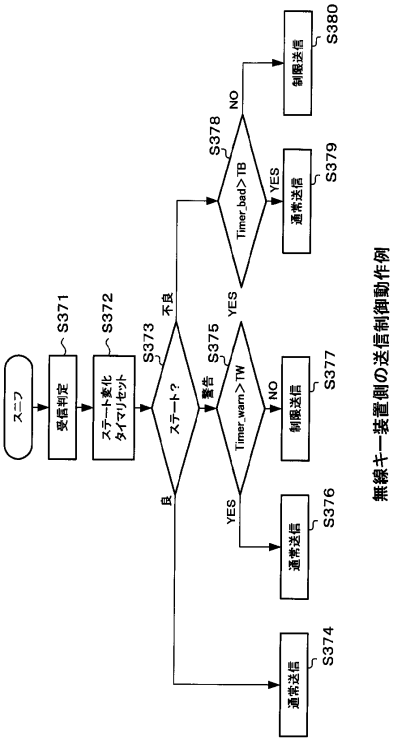
モード遷移の例

【図３６】



送信制限がある場合の低消費電力通信時のパケット動作例

【図３７】



無線キー装置側の送信制御動作例

フロントページの続き

(72)発明者　安田　光義
東京都港区港南１丁目８番１５号　ソニー・エリクソン・モバイルコミュニケーションズ株式会社内
(72)発明者　名取　誠
東京都港区港南１丁目８番１５号　ソニー・エリクソン・モバイルコミュニケーションズ株式会社内
(72)発明者　吉村　司
東京都港区港南１丁目８番１５号　ソニー・エリクソン・モバイルコミュニケーションズ株式会社内
(72)発明者　余越　稔
東京都港区港南１丁目８番１５号　ソニー・エリクソン・モバイルコミュニケーションズ株式会社内
(72)発明者　板垣　竹識
東京都港区港南１丁目８番１５号　ソニー・エリクソン・モバイルコミュニケーションズ株式会社内

審査官　西脇　博志

(56)参考文献　特開２００３－０８７３６８（ＪＰ，Ａ）
特開平１１－０８８４９９（ＪＰ，Ａ）
特開平０３－２２９３９７（ＪＰ，Ａ）
特開平０６－０９３７６５（ＪＰ，Ａ）
特開平０６－２１５２８１（ＪＰ，Ａ）
特開平０８－０４４９７５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｍ　　１／００－１／８２