

(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2006-20006

(P2006-20006A)

(43) 公開日 平成18年1月19日(2006.1.19)

(51) Int. Cl.			F I		テーマコード (参考)
H04M	1/67	(2006.01)	H04M	1/67	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 8 O L (全 34 頁)

(21) 出願番号	特願2004-195063 (P2004-195063)	(71) 出願人	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 Wビル
(22) 出願日	平成16年6月30日 (2004.6.30)	(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

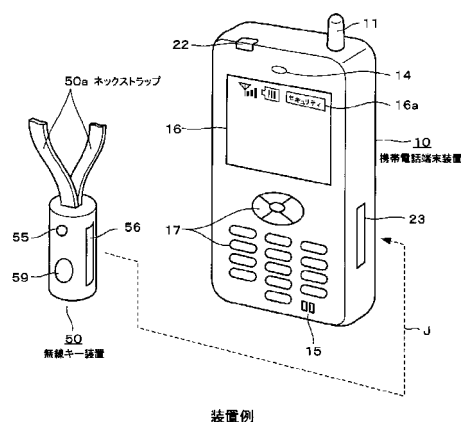
(54) 【発明の名称】 通信システム及び通信端末装置

(57) 【要約】

【課題】 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。

【解決手段】 通信端末装置10と無線キー装置50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を設定する場合に、通信端末装置及び無線キー装置は、通信手段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、それぞれの通信手段で間欠的に無線通信を行う通信状態が設定されて、無線接続が維持された状態で、判定手段で所定の状況の判定又は推定がある場合に、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ようにした。

【選択図】 図1



【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る通信システムであり、

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を設定する通信システムにおいて、

前記所定の無線通信方式として、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状態が用意された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手段と、

前記通信手段での通信状態を制御する制御手段と、

前記通信手段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が備え、

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て、それぞれの通信手段で間欠的に無線通信を行う通信状態が設定されて、無線接続が維持された状況で、前記判定手段で所定の状況の判定又は推定がある場合に、前記機能を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

通信システム。

【請求項 2】

所定の無線通信方式で特定の相手との無線通信状態に応じて、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として、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状態が用意された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手段と、

前記通信手段での通信状態を制御する制御手段と、

前記通信手段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、

前記通信手段で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て、無線接続が維持された状況で、前記判定手段で所定の状況の判定又は推定がある場合に、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制御手段とを備えた

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、

前記判定手段で判定又は推定した結果を、前記通信手段を介した無線通信で、前記特定の相手に通知するとともに、前記特定の相手から送信された判定又は推定結果を受信し、

前記制御手段は、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 4】

請求項 2 記載の通信端末装置において、

前記判定手段で判定又は推定する処理は、前記通信手段が受信した信号の受信電界強度である

通信端末装置。

【請求項 5】

請求項 4 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を判定又は推定する

通信端末装置。

10

20

30

40

50

【請求項 6】

請求項 2 記載の通信端末装置において、

前記判定手段で判定又は推定する処理は、前記通信手段が受信した信号パケットの検出状況である

通信端末装置。

【請求項 7】

請求項 6 記載の通信端末装置において、

前記判定手段で判定又は推定した結果に基づいて、前記通信手段から送信させるパケット数を変化させる

通信端末装置。

10

【請求項 8】

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、前記制御手段に判定結果を通知して、前記制御手段が前記モードの設定の処理を行う

通信端末装置。

【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。

20

【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。

30

【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。

40

【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

50

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を設定する場合に、通信端末装置及び無線キー装置は、通信手段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、それぞれの通信手段で間欠的に無線通信を行う通信状態が設定されて、無線接続が維持された状況で、判定手段で所定の状況の判定又は推定がある場合に、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出来るようになる。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、通信手段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、通信手段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、通信手段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処理を使用する場合に、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、制御手段が介入するのを、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、

10

20

30

40

50

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に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

10

20

30

40

50

通信用の通信回路 3 2 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 3 2 を使って、無線キー装置 5 0 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 5 0 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 3 2 で無線通信を行う無線キー装置 5 0 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 1 8 などに登録されている。この無線キー装置 5 0 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 3 2 内で送信信号を増幅する送信アンプ 3 3 は、制御部 1 9 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 5 0 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 5 0 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 3 2 内には、受信電界強度測定部 3 4 を備え、通信回路 3 2 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 3 4 で測定された受信電力値は、通信回路 3 2 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 3 2 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 3 0 は、非接触 IC カード機能部 4 0 を備える。この非接触 IC カード機能部 4 0 は、アンテナ 4 2 が接続された課金データ制御部 4 1 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 4 1 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 1 0 内の電源回路 2 4 から供給される電源で、課金データ制御部 4 1 を作動させるようにしてある。

【0031】

課金データ制御部 4 1 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 1 8（又は課金データ制御部 4 1 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 4 1 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 1 0 は、端子部 2 3 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 2 3 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 1 0 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 2 4 から、端子部 2 3 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 5 0 の端子部 5 6 を、この携帯電話端末装置 1 0 の端子部 2 3 に直接接続させた場合に、携帯電話端末装置 1 0 内の電源回路 2 4 から、無線キー装置 5 0 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 1 0 の端子部 2 3 に無線キー装置 5 0 が直

10

20

30

40

50

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

10

【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

20

【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。

30

40

【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

50

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、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】

10

20

30

40

50

本例の通信回路 6 2 内には、受信電界強度測定部 6 2 b を備え、通信回路 6 2 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 5 2 b で測定された受信電力値は、通信回路 6 2 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 6 2 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 6 0 は、操作キーなどで構成された操作部 6 4 と、メモリ 6 5 と、発光部 7 0 を備える。発光部 7 0 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 6 0 内の各部は、制御ライン 7 3 を介して制御データのやり取りが行えらるとともに、データライン 7 4 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 6 0 は、端子部 7 1 を備え、この端子 7 1 を使用して携帯電話端末装置 1 0 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 6 0 内の制御部 6 3 が、携帯電話端末装置 1 0 内の制御部 1 9 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 6 0 内の電源回路 7 2 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 1 0 側から供給される充電電流で、電源回路 7 2 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 6 0 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 6 0 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 1 0 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 6 0 と携帯電話端末装置 1 0 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 6 0 から携帯電話端末装置 1 0 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 6 0 又は携帯電話端末装置 1 0 (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 1 0 に近づかないでいると、携帯電話端末装置 1 0 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 1 0 と無線キー装置 5 0 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 1 9 を参照して説明する。なお、以下の説明では無線キー装置 5 0 を使うものとして説明するが、無線キー付ヘッドセット 6 0 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 1 0 の機能を制限しない通常モード M 1 と、携帯電話端末装置 1 0 と無線キー装置 5 0 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 M 2 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 1 0 と無線キー装置 5 0 との距離が離れたままである場合に)、携帯電話端末装置 1 0 の機能を制限する機能制限モード M 3 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 M 1 から警告モード M 2 への変化、警告モード M 2 から機能制限モード M 3 への変化があり、また機能制限モード M 3 となった状態で、無線キー装置 5 0 が携帯電話端末装置 1 0 に近づくと、通常モード M 1 に戻る。さらに、警告モード M 2 となって警告動作が行われている状態で、無線キー装置 5 0 が携帯電話端末装置 1 0 に近づくと、通常モード M 1 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）。 10

【0053】

この低消費電力通信モードM13の状態、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。 20

【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。 30

【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。 40

【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 50

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。

10

20

30

40

50

【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。 10

【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。 20

【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、 30

【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。 40

【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 50

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 S 4 4）、ステップ S 4 1 でスタートさせたタイマをリセットさせ（ステップ S 4 5）、アイドル期間に移る（ステップ S 4 6）。一定期間のアイドル期間が経過すると、ステップ S 4 2 のスキャン処理に戻る。ここで、本例の場合には、ステップ S 4 6 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 S 4 3 で無線キー装置 5 0 の I D 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 S 4 1 でスタートさせたタイマが、所定値 T S V を越えたか否か判断し（ステップ S 4 7）、所定値 T S V を越えていない場合には、ステップ S 4 6 のアイドル処理に移る。そして、ステップ S 4 7 で所定値 T S V 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 S 4 8）。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。

10

【0071】

図 1 7 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 5 0）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 S 5 1）、ページ信号を所定期間送信する処理を行う（ステップ S 5 2）。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 1 0）からの応答を受信したか否か判断する（ステップ S 5 3）。ここで、応答信号を受信した場合には、ステップ S 5 1 でスタートさせたタイマをリセットさせ（ステップ S 5 4）、アイドル期間に移る（ステップ S 5 5）。一定期間のアイドル期間が経過すると、ステップ S 5 2 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 S 5 5 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。

20

【0072】

そして、ステップ S 5 3 で携帯電話端末装置 1 0 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 S 5 1 でスタートさせたタイマが、所定値 T S V を越えたか否か判断し（ステップ S 5 6）、所定値 T S V を越えていない場合には、ステップ S 5 5 のアイドル処理に移る。そして、ステップ S 5 6 で所定値 T S V 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 S 5 7）。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。

30

【0073】

図 1 8 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 1 8 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（T 3 1, T 3 3, T 3 5, T 3 7）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 T 3 2, T 3 4, T 3 6, T 3 8）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。

40

【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 1 9 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 S 6 1）、その起動タイマをスタートさせ（ステップ S 6 2）、通信回路をスリープ状態とする（ステップ S 6 3）。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 S 6 4）、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 1 0 と無線キー装置 5 0

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れ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 3 m 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 7 m 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

10

20

30

40

50

）、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より大きい場合にか
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より大きい場合にか否か判断する
（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。

10

【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。

20

【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）。

30

【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より大きい場合にか否か判断する
（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）。

40

【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

50

た場合には、ステップ S 2 2 1 でスタートさせたタイマが、所定値 T S V を越えたか否か判断し（ステップ S 2 3 3）、所定値 T S V 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 S 2 3 4）、ステップ S 2 2 6 のフィルタ処理を行って平均化を行い、ステップ S 2 2 7 以降のステート判定処理に移る。

【0088】

そして、ステップ S 2 3 3 で所定値 T S V 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 S 2 3 5）、通信モードを接続モードに変化させる（ステップ S 2 3 6）。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 2 2 は、図 2 0、図 2 1 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 S 2 4 1）。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 S 2 4 2）、通常モードで作動させる（ステップ S 2 4 3）。

【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 S 2 4 4）。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 S 2 4 5）。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 20

【0091】

ードとして機能制限モードを設定して（ステップ S 2 4 8）、機能制限モードで作動させる（ステップ S 2 4 9）。ステップ S 2 4 5 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 S 2 4 9 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 1 0 と無線キー装置 5 0 との間の距離や通信環境に変化があると 30、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 3 2、5 2 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 1 9、5 3 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 2 3 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 S 2 5 1）、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 S 2 5 2）。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 40 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 S 2 5 3）。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 2 4 に示すように、例えば携帯電話端末装置 1 0 の場合、制御部 1 9 側に受信電界強度測定部 1 9 a を設けて、近距離通信回路 3 2 での受信電力を、電話通信用の通信回路 1 2 側での間欠受信に同期して処理して、制御部 1 9 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。

10

20

30

40

50

【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。

$$\Delta \text{RSSI} [n] = \text{filter} (\text{RSSI} [n] - \text{RSSI} [n-M])$$

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より大きいかな否か判断する（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より小さいかな否か判断する（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より大きいかな否か判断する（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より大きいかな否か判断する（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。

10

【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】

20

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、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

30

【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、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、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）。

40

【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、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S

50

283)。また、機能制限モードの状態、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。この通信状態の悪化は、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 S 3 1 8)、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 T H 1 より小さいか否か判断する(ステップ S 3 1 9)。第 1 の閾値 T H 1 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 S 3 2 0)。また、第 1 の閾値 T H 1 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 T H 2 より小さいか否か判断する(ステップ S 3 2 2)。第 2 の閾値 T H 2 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 S 3 2 3)。第 2 の閾値 T H 2 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 S 3 2 4)。

【0 1 1 7】

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 S 3 2 1)。一定期間のアイドル期間が経過すると、ステップ S 3 1 3 のスキャン処理に戻る。ここで、本例の場合には、ステップ S 3 1 3 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。

【0 1 1 8】

そして、ステップ S 3 2 5 で無線キー装置 5 0 の I D 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 S 3 1 1 でスタートさせたタイマが、所定値 T S V を越えたか否か判断し(ステップ S 3 2 5)、所定値 T S V 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 S 3 2 6)、ステップ S 3 1 8 のフィルタ処理を行って平均化を行い、ステップ S 3 1 9 以降のステート判定処理に移る。

【0 1 1 9】

そして、ステップ S 3 2 5 で所定値 T S V 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 S 3 2 7)、通信モードを接続モードに変化させる(ステップ S 3 2 8)。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。

【0 1 2 0】

図 3 4 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 5 0)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 S 3 3 1)、ページ信号を所定期間送信する処理を行う(ステップ S 3 3 2)。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 1 0)からの応答を受信したか否か判断する(ステップ S 3 3 3)。ここで、応答信号を受信した場合には、ステップ S 3 3 4 でスタートさせたタイマをリセットさせ(ステップ S 3 3 4)、パケットエラーレートを 0 とする(ステップ S 3 3 5)。

【0 1 2 1】

その後、検出されたパケットエラーレート P E R のフィルタ処理を行って平均化を行い(ステップ S 3 3 6)、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 T H 1 より小さいか否か判断する(ステップ S 3 3 7)。第 1 の閾値 T H 1 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 S 3 3 8)。また、第 1 の閾値 T H 1 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 T H 2 より小さいか否か判断する(ステップ S 3 4 0)。第 2 の閾値 T H 2 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 S 3 4 1)。第 2 の閾値 T H 2 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 S 3 4 2)。

【0 1 2 2】

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 S 3 3 9)。一定期間のアイドル期間が経過すると、ステップ S 3 3 2 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 S 3 3 9 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。 10

【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。 20

【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ようになる。 30

【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T_W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）。 40

【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T_B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）。 40

【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 50

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。

10

【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。

20

【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。

30

【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。

40

【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。

50

【図 1 4】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 1 5】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 1 6】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 1 7】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 1 8】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 1 9】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 2 0】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 2 1】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 2 2】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 2 3】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 2 4】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 2 5】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 2 6】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 2 7】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 2 8】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 2 9】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 3 0】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 3 1】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 3 2】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 3 3】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 3 4】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 3 5】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 3 6】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 3 7】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】

【0 1 3 7】

1 0…携帯電話端末装置、1 1…アンテナ、1 2…無線電話用通信回路、1 3…音声処理部、1 4…スピーカ、1 5…マイクロフォン、1 6…表示部、1 7…操作部、1 8…メモリ、1 9…制御部、2 1…振動部、2 2…発光部、2 3…端子部、2 4…電源回路、2

10

20

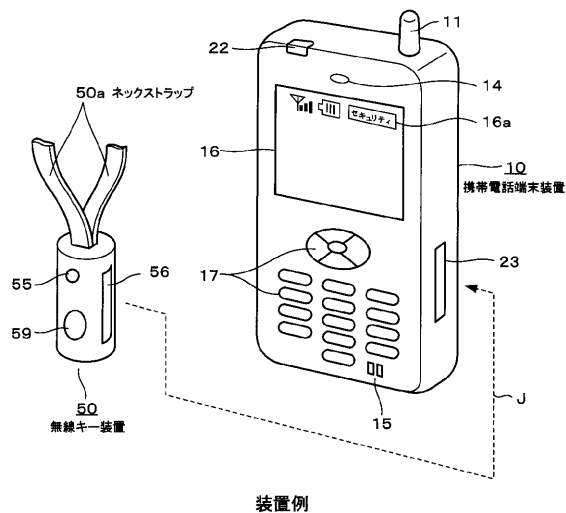
30

40

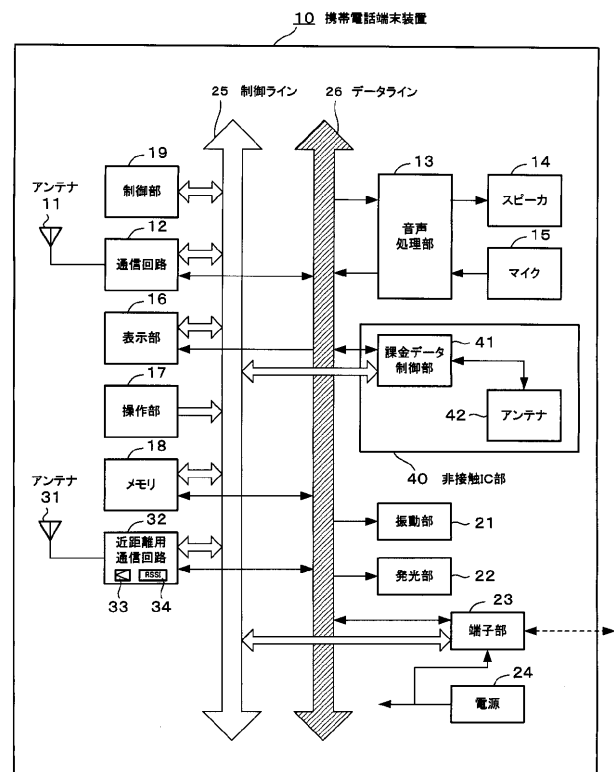
50

5…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

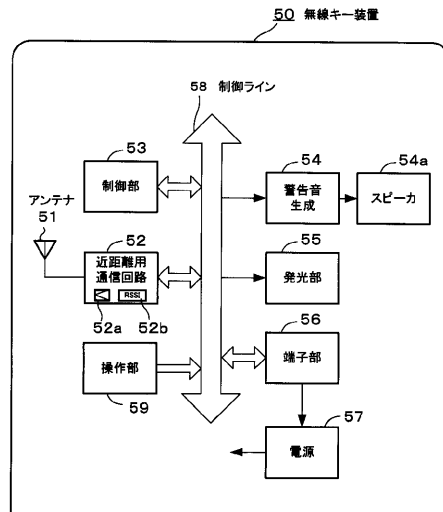
【図1】



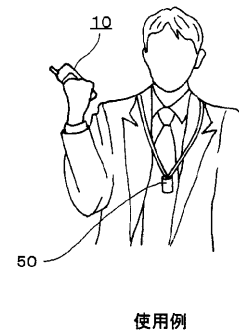
【図2】



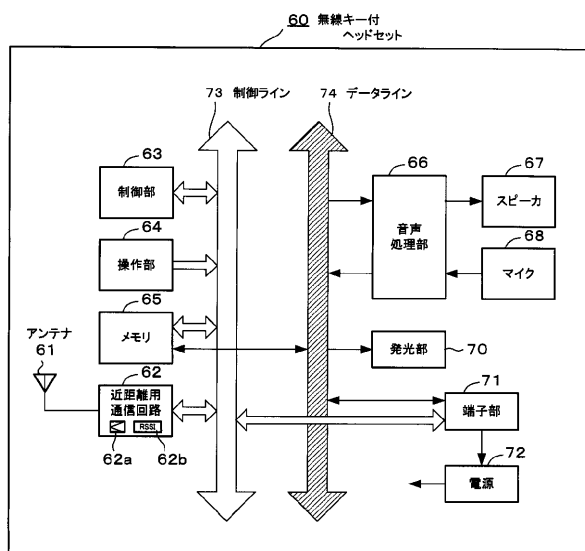
【 図 3 】



【図 4】



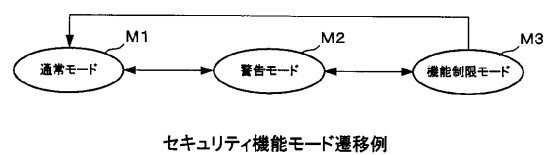
【図 5】



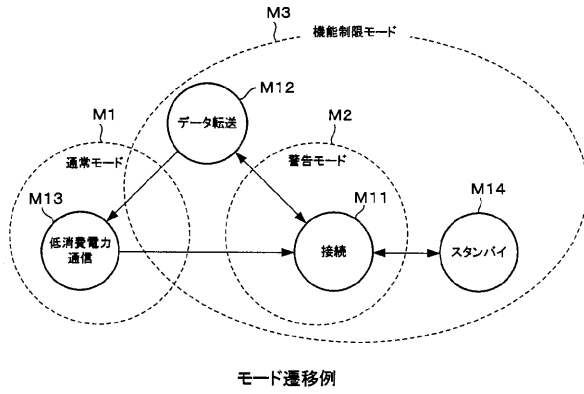
【図 6】



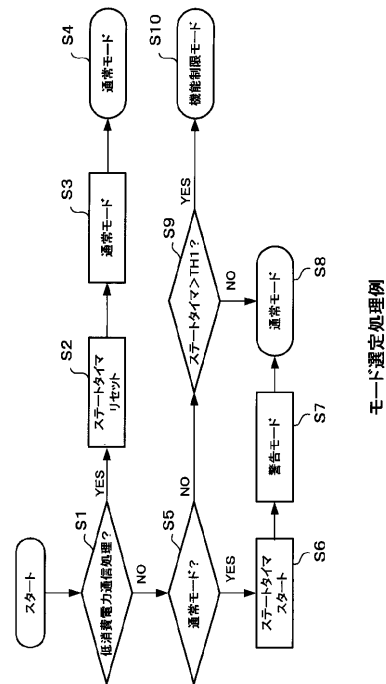
【图 7】



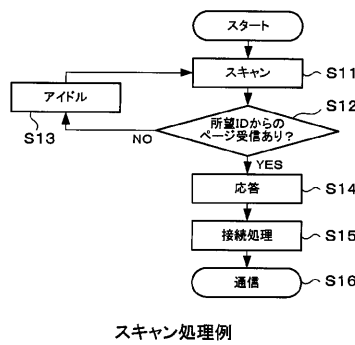
【図 8】



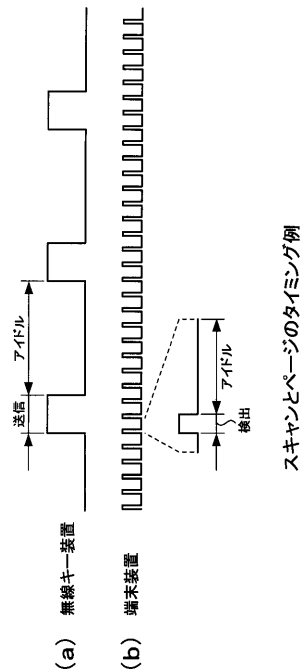
【図 9】



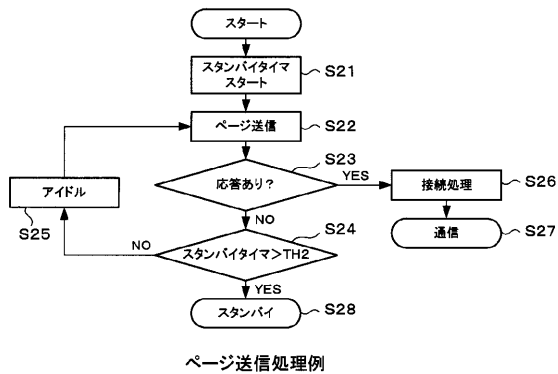
【図 10】



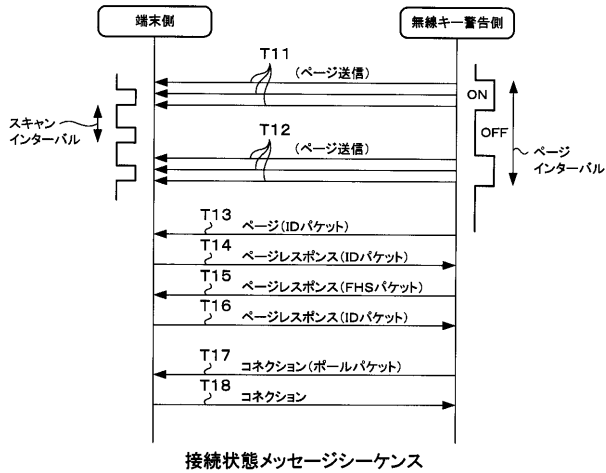
【図 12】



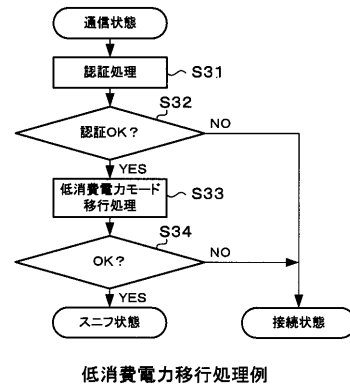
【図 11】



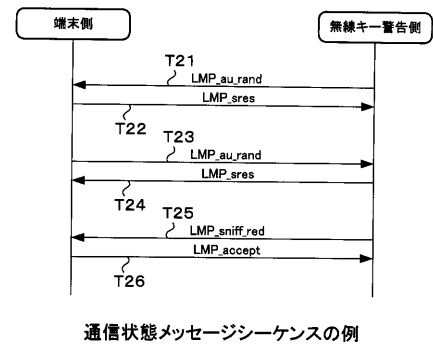
【図 13】



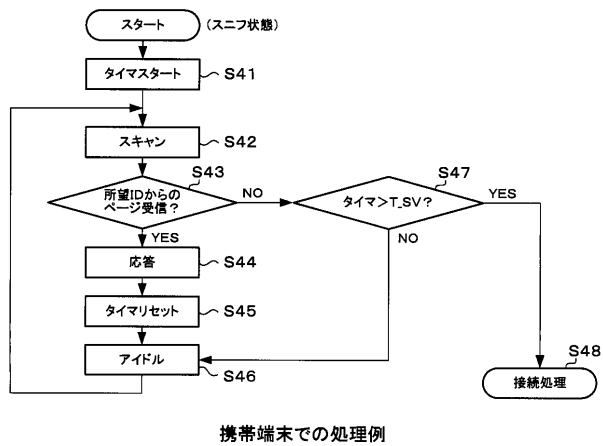
【図 14】



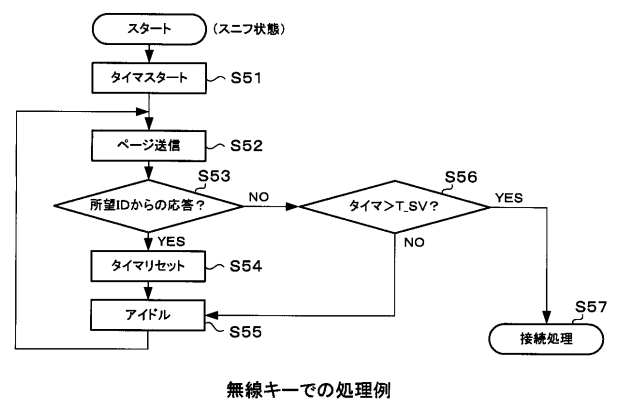
【図 15】



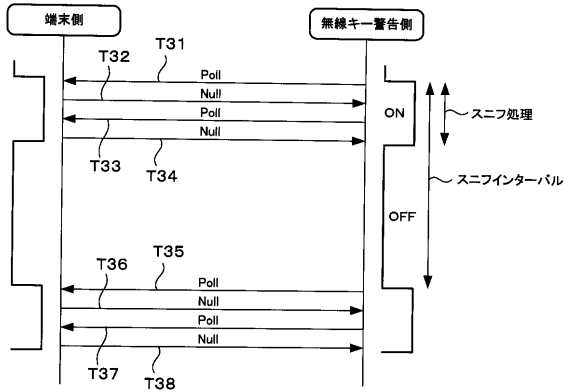
【図 16】



【図 17】

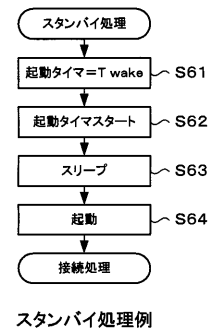


【図 18】



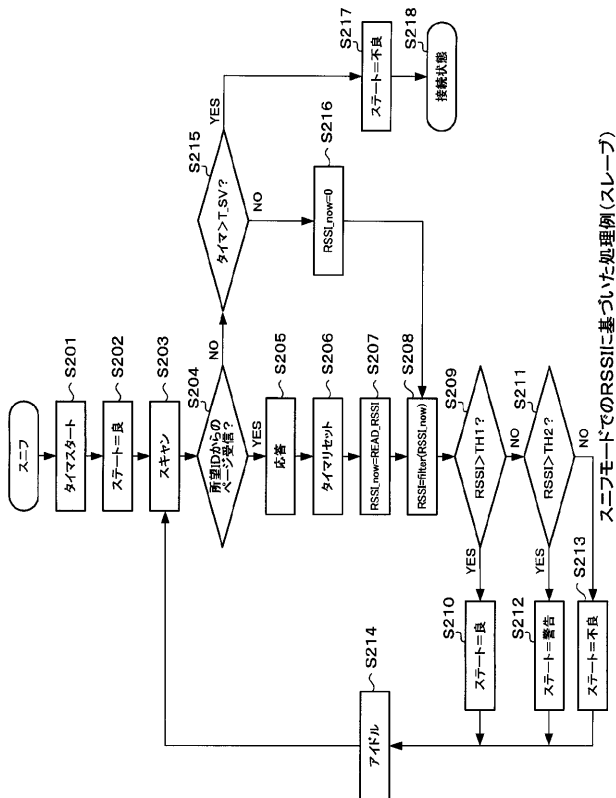
スニフ状態のシーケンス

【図 19】

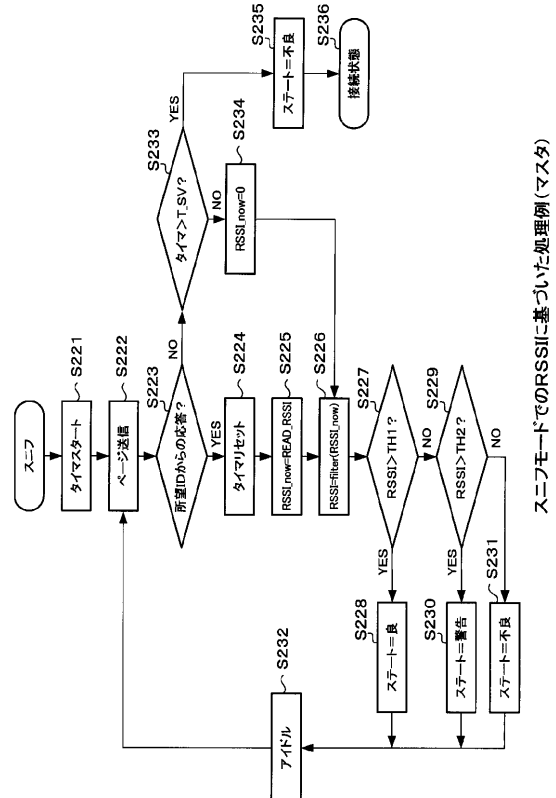


スタンバイ処理例

【図 20】

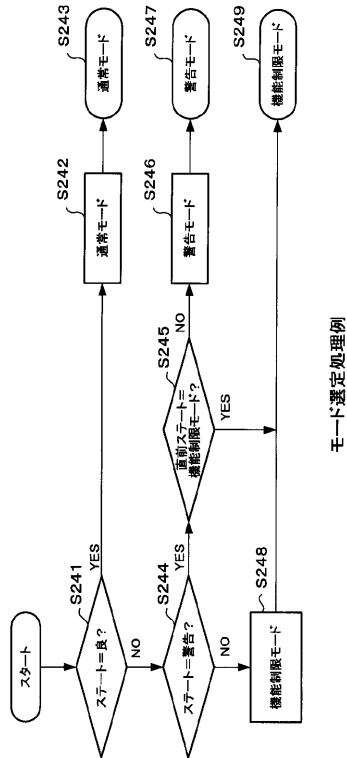


【図 21】

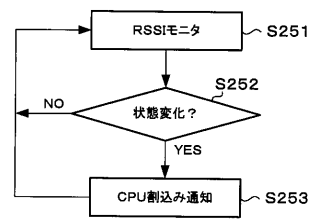


スニフモードでのRSSIに基づいた処理例(マスター)

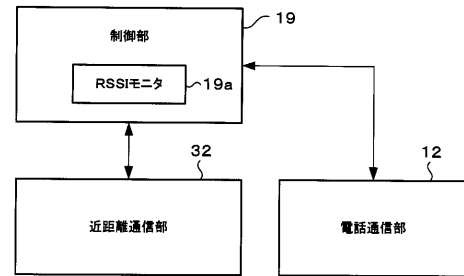
【図 2 2】



【図 2 3】

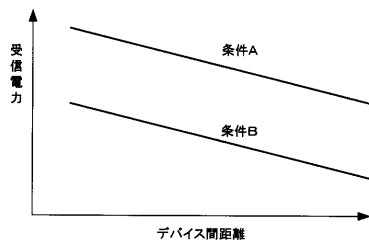


【図 2 4】



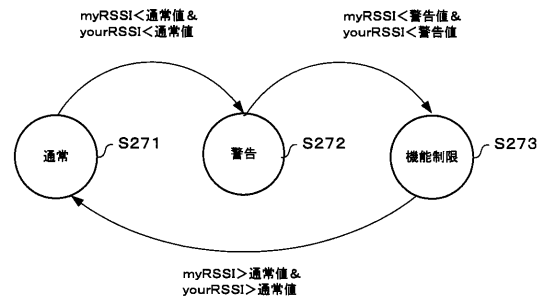
制御部にRSSIモニタを実装させた例

【図 2 5】



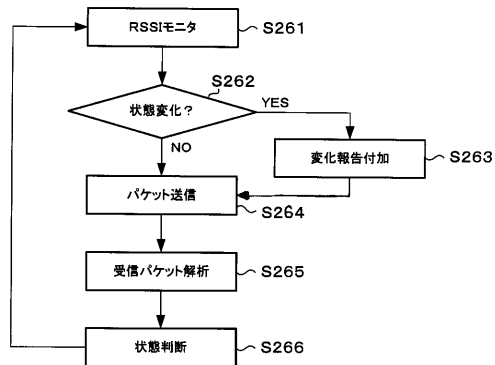
受信電力とデバイス間距離の例

【図 2 7】

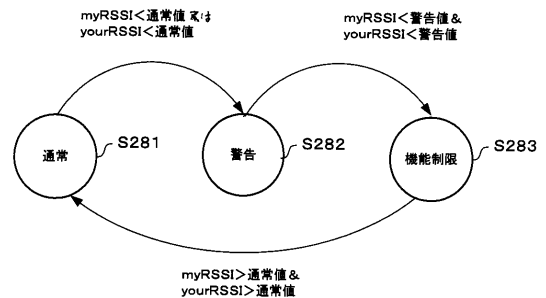


モード変化例

【図 2 6】

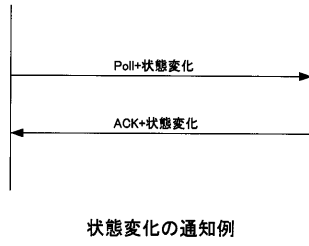


【図 2 8】

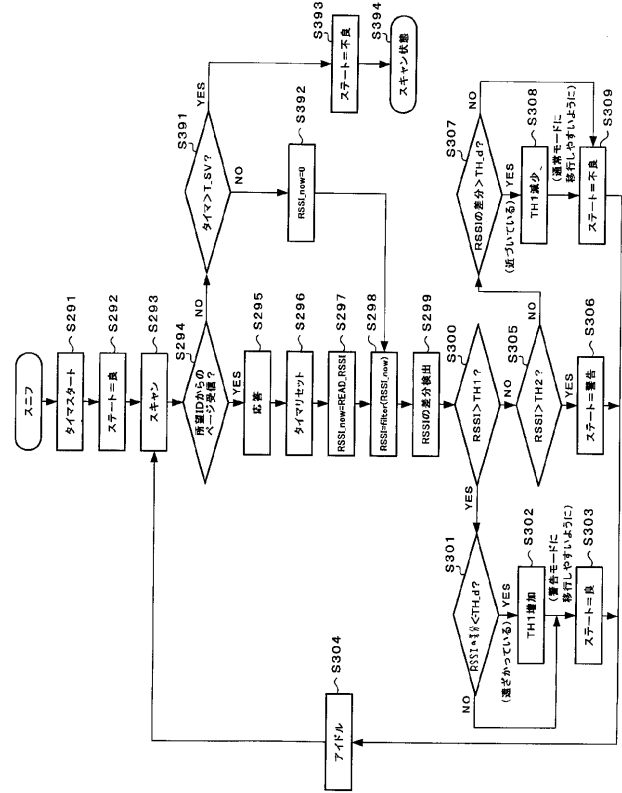


モード変化例

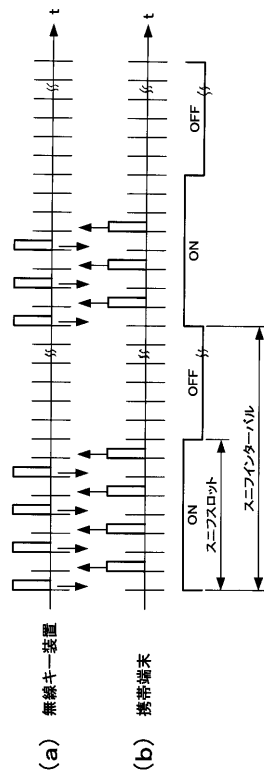
【図 29】



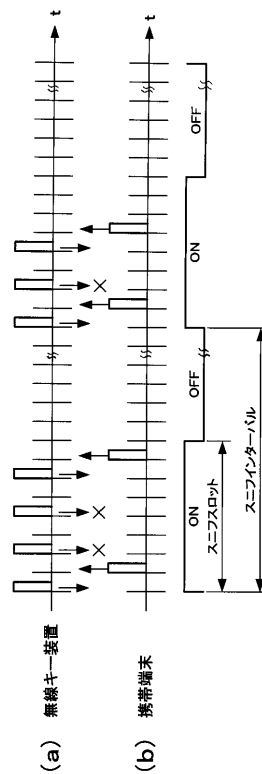
【図 30】



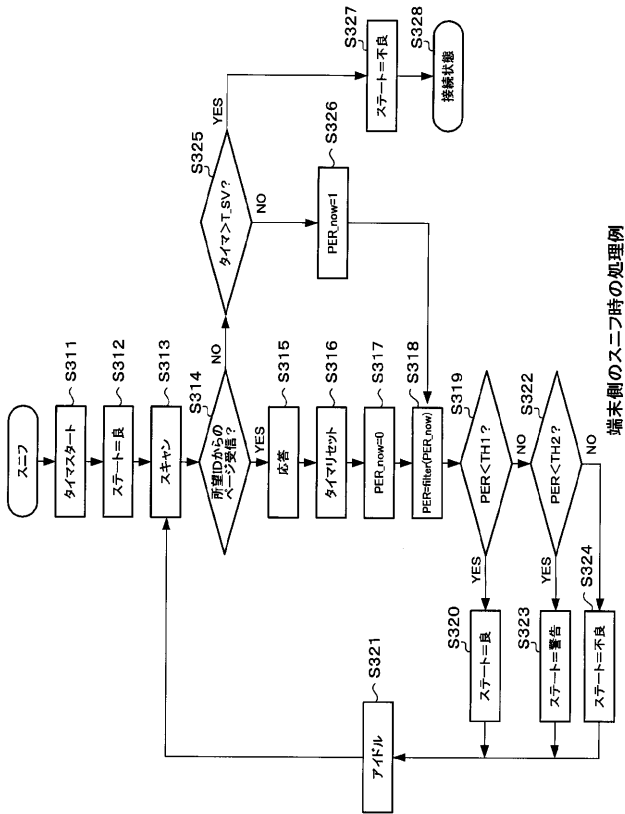
【図 31】



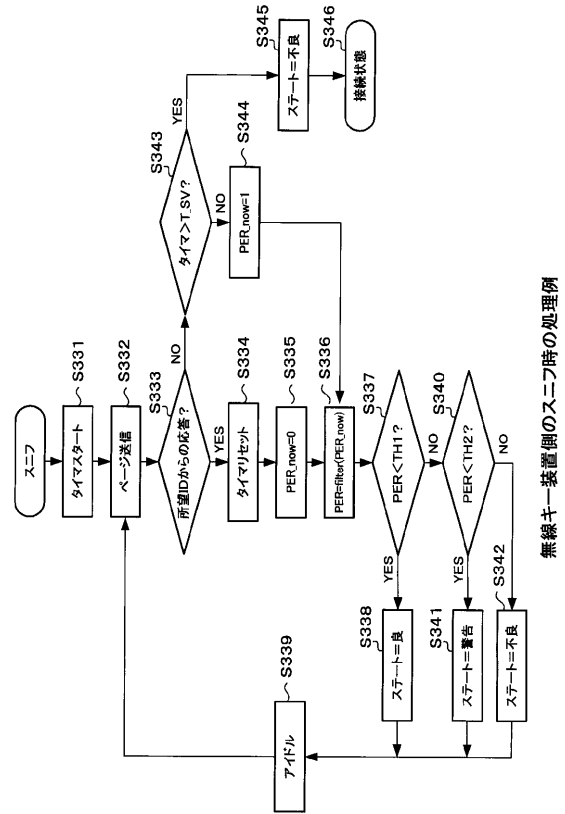
【図 32】



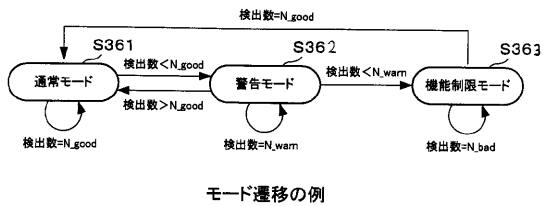
【図 3 3】



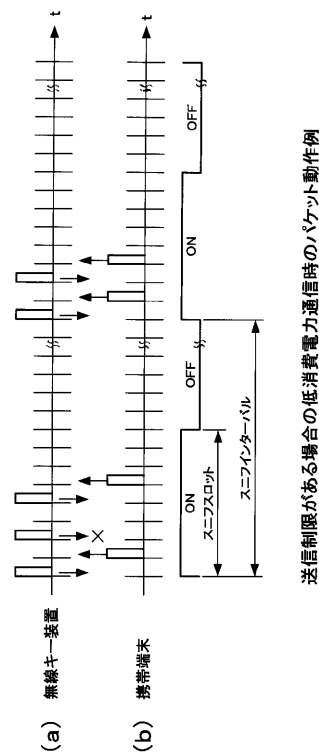
【図 3 4】



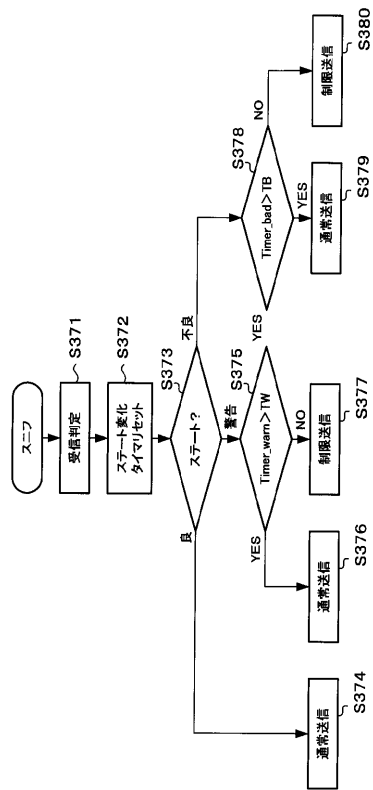
【図 3 5】



【図 3 6】



【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

Fターム(参考) 5K027 AA11 BB09 CC08 HH11 HH23 MM03
5K067 AA32 BB04 DD27 DD51 EE03 EE35 FF02 GG01 GG11 HH21