

(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2008-205548  
(P2008-205548A)

(43) 公開日 平成20年9月4日(2008.9.4)

(51) Int.Cl.	F I	テーマコード (参考)
HO4M 1/67 (2006.01)	HO4M 1/67	5K027
HO4B 7/26 (2006.01)	HO4B 7/26 R	5K067
HO4Q 7/38 (2006.01)	HO4B 7/26 109R	

審査請求 未請求 請求項の数 18 O L (全 17 頁)

(21) 出願番号 特願2007-36030 (P2007-36030)  
(22) 出願日 平成19年2月16日 (2007.2.16)

(71) 出願人 000005821  
松下電器産業株式会社  
大阪府門真市大字門真1006番地  
(74) 代理人 100105647  
弁理士 小栗 昌平  
(74) 代理人 100108589  
弁理士 市川 利光  
(74) 代理人 100119552  
弁理士 橋本 公秀  
(72) 発明者 松本 孝之  
大阪府門真市大字門真1006番 松下電  
器産業株式会社内  
(72) 発明者 斎藤 潤一  
大阪府門真市大字門真1006番 松下電  
器産業株式会社内

最終頁に続く

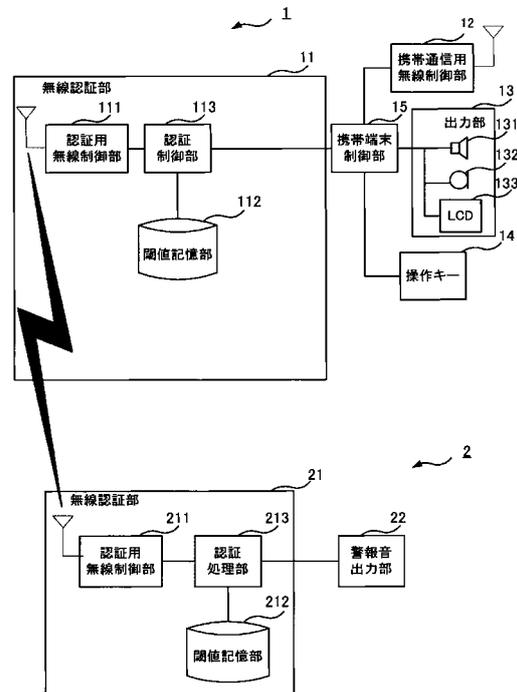
(54) 【発明の名称】 携帯端末装置およびキー

(57) 【要約】

【課題】 携帯端末装置とキーとの間で認証の成否を分ける閾値を電波伝搬環境に応じた値に動的に設定することによって、電波伝搬環境が変わっても、認証の成否を分ける携帯端末装置とキーの距離を一定に保つことができる携帯端末装置またはキーを提供する。

【解決手段】 本発明の携帯端末装置 1 は、キー 2 と無線通信を行う認証用無線制御部 111 と、認証用無線制御部 111 によりキー 2 から受信する無線電波の受信強度を検出する認証制御部 113 と、認証制御部 113 により検出する受信強度がある閾値以上または未満であるかに応じて、所定の処理を実行するよう制御する携帯端末制御部 15 と、任意の時点で認証制御部 113 が検出した受信強度に基づいて、携帯端末制御部 15 が所定の処理を実行すべき前記閾値を設定する閾値設定部 112 と、を備えるものである。

【選択図】 図 2



**【特許請求の範囲】****【請求項 1】**

キーと無線通信を行う無線部と、  
前記無線部により前記キーから受信する無線電波の受信強度を検出する検出部と、  
前記検出部により検出する受信強度がある閾値以上または未満であるかに応じて、所定の処理を実行するよう制御する制御部と、  
任意の時点で前記検出部が検出した受信強度に基づいて、前記制御部が所定の処理を実行すべき前記閾値を設定する閾値設定部と、  
を備える携帯端末装置。

**【請求項 2】**

請求項 1 記載の携帯端末装置であって、  
各種入力操作を受け付ける操作部を備え、  
前記閾値設定部は、前記操作部により前記閾値を設定するための入力操作を受け付けた時点で前記検出部が検出した受信強度に基づいて、前記制御部が所定の処理を実行すべき前記閾値を設定する、  
携帯端末装置。

10

**【請求項 3】**

請求項 1 記載の携帯端末装置であって、  
前記閾値設定部は、一定期間毎に前記検出部が検出する受信強度に基づいて、前記制御部が所定の処理を実行すべき前記閾値を設定する、  
携帯端末装置。

20

**【請求項 4】**

請求項 1 から 3 のいずれか一項に記載の携帯端末装置であって、  
前記閾値設定部は、所定の期間に含まれる複数の任意の各時点で前記検出部が検出した受信強度を平均化し、その平均化した数値を前記制御部が所定の処理を実行すべき前記閾値として設定する、  
携帯端末装置。

**【請求項 5】**

請求項 1 から 3 のいずれか一項に記載の携帯端末装置であって、  
前記閾値設定部は、所定の期間に含まれる複数の任意の各時点で前記検出部が検出した受信強度が、前記制御部が所定の処理を実行すべき前記閾値を再設定する条件を満たす場合、前記複数の任意の各時点で前記検出部が検出した受信強度に基づいて算出される数値を、前記制御部が所定の処理を実行すべき前記閾値として設定する、  
携帯端末装置。

30

**【請求項 6】**

請求項 5 記載の携帯端末装置であって、  
前記閾値設定部は、所定の期間に含まれる先頭の時点と最後の時点それぞれで前記検出部が検出した受信強度の差が所定値以上小さくあるいは大きくなった場合、当該受信強度の差に基づいて算出される数値を、前記制御部が所定の処理を実行すべき前記閾値として設定する、  
携帯端末装置。

40

**【請求項 7】**

請求項 1 から 6 のいずれか一項に記載の携帯端末装置であって、  
前記閾値設定部は、任意の時点で前記検出部が検出した受信強度と、当該受信強度を検出したときの当該携帯端末装置と前記キーとの距離を単位長さとした場合に当該単位長さを基に指定される所定の距離と、に基づいて算出される数値を、前記制御部が所定の処理を実行すべき前記閾値として設定する、  
携帯端末装置。

**【請求項 8】**

請求項 7 記載の携帯端末装置であって、

50

前記閾値設定部は、任意の時点で前記検出部が検出した受信強度と、前記単位長さを基に指定される第1の距離および前記第1の距離よりも長い第2の距離と、に基づいて算出される数値のそれぞれを、前記制御部が所定の処理を実行すべき第1の閾値および第2の閾値として設定し、

前記制御部は、前記検出部により検出する受信強度が前記第1の閾値未満から以上に推移すれば、当該携帯端末装置に備わる各種機能の実行を許可するよう制御し、前記検出部により検出する受信強度が前記第2の閾値以上から未満に推移すれば、当該携帯端末装置に備わる各種機能のうちの少なくとも一つの実行を制限するロック制御部を含む、携帯端末装置。

【請求項9】

10

請求項1から8のいずれか1項に記載の携帯端末装置であって、

前記無線部は、前記制御部が所定の処理を実行すべき前記閾値として前記閾値設定部が設定した数値を前記キーに送信する、  
携帯端末装置。

【請求項10】

請求項9記載の携帯端末装置と無線通信を行う無線部と、

前記無線部により前記携帯端末装置から受信する無線電波の受信強度を検出する検出部と、

前記検出部により検出する受信強度がある閾値未満である場合に報知する報知部と、

前記無線部により前記携帯端末装置から受信した、前記閾値として設定すべき数値を、前記報知部が報知すべき前記閾値として設定する閾値設定部と、  
を備えるキー。

20

【請求項11】

携帯端末装置と無線通信を行う無線部と、

前記無線部により前記携帯端末装置から受信する無線電波の受信強度を検出する検出部と、

前記検出部により検出する受信強度がある閾値未満である場合に報知する報知部と、

任意の時点で前記検出部が検出した受信強度に基づいて、前記報知部が報知すべき前記閾値を設定する閾値設定部と、  
を備えるキー。

30

【請求項12】

請求項11記載のキーであって、

各種入力操作を受け付ける操作部を備え、

前記閾値設定部は、前記操作部により前記閾値を設定するための入力操作を受け付けた時点で前記検出部が検出した受信強度に基づいて、前記報知部が報知すべき前記閾値を設定する、  
キー。

【請求項13】

請求項11記載のキーであって、

前記閾値設定部は、一定期間毎に前記検出部が検出する受信強度に基づいて、前記報知部が報知すべき前記閾値を設定する、  
キー。

40

【請求項14】

請求項11から13のいずれか一項に記載のキーであって、

前記閾値設定部は、所定の期間に含まれる複数の任意の各時点で前記検出部が検出した受信強度を平均化し、その平均化した数値を前記報知部が報知すべき前記閾値として設定する、  
キー。

【請求項15】

請求項11から13のいずれか一項に記載のキーであって、

50

前記閾値設定部は、所定の期間に含まれる複数の任意の各時点で前記検出部が検出した受信強度が、前記報知部が報知すべき前記閾値を再設定する条件を満たす場合、前記複数の任意の各時点で前記検出部が検出した受信強度に基づいて算出される数値を、前記報知部が報知すべき前記閾値として設定する、  
キー。

【請求項 16】

請求項 15 記載のキーであって、

前記閾値設定部は、所定の期間に含まれる先頭の時点と最後の時点それぞれで前記検出部が検出した受信強度の差が所定値以上小さくあるいは大きくなった場合、当該受信強度の差に基づいて算出される数値を、前記報知部が報知すべき前記閾値として設定する、  
キー。

10

【請求項 17】

請求項 11 から 13 のいずれか一項に記載のキーであって、

前記閾値設定部は、任意の時点で前記検出部が検出した受信強度と、当該受信強度を検出したときの当該キーと前記携帯端末装置との距離を単位長さとした場合に当該単位長さを基に指定される所定の距離と、に基づいて算出される数値を、前記報知部が報知すべき前記閾値として設定する、  
キー。

【請求項 18】

請求項 17 記載のキーであって、

前記閾値設定部は、任意の時点で前記検出部が検出した受信強度と、前記単位長さを基に指定される第 1 の距離および前記第 1 の距離よりも長い第 2 の距離と、に基づいて算出される数値のそれぞれを、前記制御部が所定の処理を実行すべき第 1 の閾値および第 2 の閾値として設定し、

20

前記報知部は、前記検出部により検出する受信強度が前記第 1 の閾値未満から以上に推移すれば報知を終了し、前記検出部により検出する受信強度が前記第 2 の閾値以上から未満に推移すれば報知を開始する、  
キー。

【発明の詳細な説明】

【技術分野】

30

【0001】

本発明は、携帯端末装置を置き忘れたときや盗難に遭ったときに、機能の一部あるいは全ての実行を禁止する携帯端末装置および携帯端末装置所有者に警報を発するキーに関する。

【背景技術】

【0002】

近年、携帯電話や PDA、パソコン等の持ち運び可能な電子機器は、広く普及している。しかし、それに伴って置き忘れ等による紛失や盗難に遭う例も多く発生し、他人による不正使用や電話帳など個人情報の漏洩の危険性が増えており、それに伴ってセキュリティを高める技術がますます重要になってきている。

40

【0003】

上記セキュリティを高める技術の一例として、次のようなものが提案されている。すなわち、携帯電話、PDA、あるいはパソコン等の携帯端末装置と、これら携帯端末装置に付属する、携帯端末装置の使用者が携帯可能な形状のキー（無線通信ユニット）と、から構成される使用制限システムである。この使用制限システムにおいて、携帯端末装置は、キーから受信する電波の受信強度がある閾値以上でありかつキーと無線認証している期間中（認証に成功している期間）、携帯端末装置の使用制限を解除し、一方、キーとの距離が離れて受信強度が閾値未満に低下している期間（認証に失敗している期間）、携帯端末装置の使用制限の解除を停止して操作不能にするとともに、同じく受信強度が所定値以下に低下したキーが警報信号を発する（例えば、特許文献 1 参照）。

50

## 【 0 0 0 4 】

また、携帯端末装置およびキーが受信強度の高低を判別するための閾値を複数候補の中から選択できるように構成しておき、選択されたいずれか一つの閾値を基に携帯端末装置およびキーに受信強度の高低を判別させることによって、認証の成否を分ける距離を調整できるようにした携帯端末装置もある。

【特許文献1】特許第2931276号

【発明の開示】

【発明が解決しようとする課題】

## 【 0 0 0 5 】

上記閾値は、ある電波伝搬環境下で、携帯端末装置またはキーが所定距離離れた放射源から放射される電波を受信したときの受信強度であり、例えば、携帯端末装置とキーとの間に電波の伝搬を遮るものがほとんどない（あっても電波の伝播をほとんど妨げない）環境で、電波を放射する放射源から3m、5m、10m離れた地点で計測される受信強度が閾値として設定される。しかしながら、上記の携帯端末装置およびキーは様々な電波伝搬環境下で利用されるため、携帯端末装置またはキーに予め設定された上記閾値によって想定される携帯端末装置とキーの距離が、実際に同じ閾値の受信強度の電波を受信したときの携帯端末装置とキーの距離と必ずしも一致しないことが考えられる。例えば、携帯端末装置またはキーに予め設定された閾値が携帯端末装置とキーの距離10mを想定したものであっても、電波伝搬状況の悪い環境下で携帯端末装置またはキーが同じ閾値の受信強度を受信したときの携帯端末装置とキーの実際の距離は5mである、ことも起こりえる。

## 【 0 0 0 6 】

このため、携帯端末装置またはキーに予め固定的に設定された閾値により受信強度の高低を判別する構成は、その閾値により認証の成否を分けると想定される携帯端末装置とキーの距離を利用者に提示することによって、利便性を高め得るものの、特定の電波伝搬環境下ではかえって、その提示された距離とは異なる距離が認証の成否を分ける距離となってしまう利用者を戸惑わせてしまうことが考えられる。

## 【 0 0 0 7 】

したがって、上記閾値を電波伝搬環境に応じた値に動的に設定することによって、電波伝搬環境が変わっても、認証の成否を分ける携帯端末装置とキーの距離を一定に保つことができる携帯端末装置またはキーが求められている。

## 【 0 0 0 8 】

本発明は、上記事情に鑑みてなされたもので、携帯端末装置とキーとの間で認証の成否を分ける閾値を電波伝搬環境に応じた値に動的に設定することによって、電波伝搬環境が変わっても、認証の成否を分ける携帯端末装置とキーの距離を一定に保つことができる携帯端末装置またはキーを提供することを目的とする。

【課題を解決するための手段】

## 【 0 0 0 9 】

本発明の携帯端末装置は、キーと無線通信を行う無線部と、前記無線部により前記キーから受信する無線電波の受信強度を検出する検出部と、前記検出部により検出する受信強度がある閾値以上または未満であるかに応じて、所定の処理を実行するよう制御する制御部と、任意の時点で前記検出部が検出した受信強度に基づいて、前記制御部が所定の処理を実行すべき前記閾値を設定する閾値設定部と、を備えるものである。

## 【 0 0 1 0 】

本発明のキーは、携帯端末装置と無線通信を行う無線部と、前記無線部により前記携帯端末装置から受信する無線電波の受信強度を検出する検出部と、前記検出部により検出する受信強度がある閾値未満である場合に報知する報知部と、任意の時点で前記検出部が検出した受信強度に基づいて、前記報知部が報知すべき前記閾値を設定する閾値設定部と、を備えるものである。

## 【 0 0 1 1 】

この構成により、受信強度の高低によって無線認証の成否を分けるための閾値をいつで

10

20

30

40

50

も設定することができるため、電波伝搬環境が変わっても、認証の成否を分ける携帯端末装置とキーの距離を一定に保つことができる。

【0012】

また、本発明の携帯端末装置は、各種入力操作を受け付ける操作部を備え、前記閾値設定部が、前記操作部により前記閾値を設定するための入力操作を受け付けた時点で前記検出部が検出した受信強度に基づいて、前記制御部が所定の処理を実行すべき前記閾値を設定する、ものを含む。

【0013】

また、本発明のキーは、各種入力操作を受け付ける操作部を備え、前記閾値設定部が、前記操作部により前記閾値を設定するための入力操作を受け付けた時点で前記検出部が検出した受信強度に基づいて、前記報知部が報知すべき前記閾値を設定する、ものを含む。

10

【0014】

この構成により、利用者が所定の操作を行った時点で受信強度の閾値を設定する構成によって、電波伝搬環境が変わっても、携帯端末装置とキーとを一定の距離離れた状態でその操作を行えば、利用者によって予想される、携帯端末装置による認証の成否を分ける長さ、携帯端末装置が実際に認証処理を行った結果認証の成否を分けることになる距離と、を一致させることができる。

【0015】

また、本発明の携帯端末装置は、前記閾値設定部が、一定期間毎に前記検出部が検出する受信強度に基づいて、前記制御部が所定の処理を実行すべき前記閾値を設定する、ものを含む。

20

【0016】

また、本発明のキーは、前記閾値設定部が、一定期間毎に前記検出部が検出する受信強度に基づいて、前記報知部が報知すべき前記閾値を設定する、ものを含む。

【0017】

この構成により、携帯端末装置とキーの距離がほとんど変化しない場合において、電波伝搬環境が変わっても（例えば、携帯端末装置やキーをカバンやポケットの中に入れることによって、電波伝搬環境が悪くなっても）、認証に成功したあるいは失敗したことを判定するための閾値を自動的に更新し、認証の成否を分ける携帯端末装置とキーとの距離を一定に保つことができる。

30

【0018】

また、本発明の携帯端末装置は、前記閾値設定部が、所定の期間に含まれる複数の任意の各時点で前記検出部が検出した受信強度を平均化し、その平均化した数値を前記制御部が所定の処理を実行すべき前記閾値として設定する、ものを含む。

【0019】

また、本発明のキーは、前記閾値設定部が、所定の期間に含まれる複数の任意の各時点で前記検出部が検出した受信強度を平均化し、その平均化した数値を前記報知部が報知すべき前記閾値として設定する、ものを含む。

【0020】

この構成により、携帯端末装置とキーの距離がほとんど変化しない場合において、電波伝搬環境が変わっても、認証に成功したあるいは失敗したことを判定するための閾値を受信強度の値の変化に応じて自動的に更新し、認証の成否を分ける携帯端末装置とキーとの距離を一定に保つことができる。

40

【0021】

また、本発明の携帯端末装置は、前記閾値設定部が、所定の期間に含まれる複数の任意の各時点で前記検出部が検出した受信強度が、前記制御部が所定の処理を実行すべき前記閾値を再設定する条件を満たす場合、前記複数の任意の各時点で前記検出部が検出した受信強度に基づいて算出される数値を、前記制御部が所定の処理を実行すべき前記閾値として設定する、ものを含む。

【0022】

50

また、本発明のキーは、前記閾値設定部が、所定の期間に含まれる複数の任意の各時点で前記検出部が検出した受信強度が、前記報知部が報知すべき前記閾値を再設定する条件を満たす場合、前記複数の任意の各時点で前記検出部が検出した受信強度に基づいて算出される数値を、前記報知部が報知すべき前記閾値として設定する、ものを含む。

【0023】

この構成により、携帯端末装置とキーの距離がほとんど変化しない場合において、電波伝搬環境が変わっても、認証に成功したあるいは失敗したことを判定するための閾値を受信強度の値の変化に応じて自動的に更新し、認証の成否を分ける携帯端末装置とキーとの距離を一定に保つことができる。

【0024】

また、本発明の携帯端末装置は、前記閾値設定部が、所定の期間に含まれる先頭の時点と最後の時点それぞれで前記検出部が検出した受信強度の差が所定値以上小さくあるいは大きくなった場合、当該受信強度の差に基づいて算出される数値を、前記制御部が所定の処理を実行すべき前記閾値として設定する、ものを含む。

【0025】

また、本発明のキーは、前記閾値設定部が、所定の期間に含まれる先頭の時点と最後の時点それぞれで前記検出部が検出した受信強度の差が所定値以上小さくあるいは大きくなった場合、当該受信強度の差に基づいて算出される数値を、前記報知部が報知すべき前記閾値として設定する、ものを含む。

【0026】

この構成により、携帯端末装置とキーの距離がほとんど変化しない場合において、電波伝搬環境が変わっても、認証に成功したあるいは失敗したことを判定するための閾値を受信強度の値の変化に応じて自動的に更新し、認証の成否を分ける携帯端末装置とキーとの距離を一定に保つことができる。

【0027】

また、本発明の携帯端末装置は、前記閾値設定部が、任意の時点で前記検出部が検出した受信強度と、当該受信強度を検出したときの当該携帯端末装置と前記キーとの距離を単位長さとした場合に当該単位長さを基に指定される所定の距離と、に基づいて算出される数値を、前記制御部が所定の処理を実行すべき前記閾値として設定する、ものを含む。

【0028】

また、本発明のキーは、前記閾値設定部が、任意の時点で前記検出部が検出した受信強度と、当該受信強度を検出したときの当該キーと前記携帯端末装置との距離を単位長さとした場合に当該単位長さを基に指定される所定の距離と、に基づいて算出される数値を、前記報知部が報知すべき前記閾値として設定する、ものを含む。

【0029】

この構成により、利用者は、受信強度を検出したときの携帯端末装置とキーとの距離を基に認証の成否を分ける距離を設定することによって、利用者によって予想される、携帯端末装置とキーの認証の成否を分ける長さと、実際に認証処理を行った結果認証の成否を分けることになる距離と、を一致させつつ、簡易にその距離を調整することができる。

【0030】

また、本発明の携帯端末装置は、前記閾値設定部が、任意の時点で前記検出部が検出した受信強度と、前記単位長さを基に指定される第1の距離および前記第1の距離よりも長い第2の距離と、に基づいて算出される数値のそれぞれを、前記制御部が所定の処理を実行すべき第1の閾値および第2の閾値として設定し、前記制御部が、前記検出部により検出する受信強度が前記第1の閾値未満から以上に推移すれば、当該携帯端末装置に備わる各種機能の実行を許可するよう制御し、前記検出部により検出する受信強度が前記第2の閾値以上から未満に推移すれば、当該携帯端末装置に備わる各種機能のうち少なくとも一つの実行を制限するロック制御部を含む、ものを含む。

【0031】

また、本発明のキーは、前記閾値設定部が、任意の時点で前記検出部が検出した受信強

10

20

30

40

50

度と、前記単位長さを基に指定される第1の距離および前記第1の距離よりも長い第2の距離と、に基づいて算出される数値のそれぞれを、前記制御部が所定の処理を実行すべき第1の閾値および第2の閾値として設定し、前記報知部が、前記検出部により検出する受信強度が前記第1の閾値未満から以上に推移すれば報知を終了し、前記検出部により検出する受信強度が前記第2の閾値以上から未満に推移すれば報知を開始する、ものを含む。

【0032】

この構成により、携帯端末装置により実行可能な各種機能に対する制限、あるいは制限解除タイミングのバリエーションを増やし、また、キーによる報知するバリエーションを増やすことができる。その結果、利用者による携帯端末装置とキーの使い方に適した距離にて携帯端末装置に各種機能の制限および制限解除を、並びにキーに報知制御をさせることができる。

10

【0033】

また、本発明の携帯端末装置は、前記無線部が、前記制御部が所定の処理を実行すべき前記閾値として前記閾値設定部が設定した数値を前記キーに送信する、ものを含む。

【0034】

また、本発明のキーは、本発明の携帯端末装置と無線通信を行う無線部と、前記無線部により前記携帯端末装置から受信する無線電波の受信強度を検出する検出部と、前記検出部により検出する受信強度がある閾値未満である場合に報知する報知部と、前記無線部により前記携帯端末装置から受信した、前記閾値として設定すべき数値を、前記報知部が報知すべき前記閾値として設定する閾値設定部と、を備えるものである。

20

【0035】

この構成により、携帯端末装置によって設定された閾値をキーにも設定することができる。このため、携帯端末装置およびキーそれぞれで閾値設定処理を行う必要がなくなる。

【発明の効果】

【0036】

本発明の携帯端末装置およびキーによれば、携帯端末装置とキーとの間で認証の成否を分ける閾値を電波伝搬環境に応じた値に動的に設定することによって、電波伝搬環境が変わっても、認証の成否を分ける携帯端末装置とキーの距離を一定に保つことができる。

【発明を実施するための最良の形態】

【0037】

以下、本発明の実施の形態の携帯端末装置およびキーについて詳細に説明する。

30

【0038】

(第1実施形態)

まず、本発明の第1実施形態の携帯端末装置およびキーによる、受信強度の閾値を携帯端末装置に設定するときの一例を、図1(a)に示す、受信強度の閾値の設定操作を表す概要図を参照して説明する。なお、以降では、携帯端末装置 - キー間での無線認証に必要な受信強度の閾値を携帯端末装置またはキーに設定することを「キャリブレーション (calibration) 処理を行う」と称する。

【0039】

図1(a)に示す概要図では、携帯端末装置1およびキー2を所持している利用者は、一定の間隔L離れた状態で携帯端末装置とキーを所持しているものとする。図1(a)では、利用者は、携帯端末装置1を手に、キー2をカバンの中に、それぞれ所持している場合を図示している。利用者は、キャリブレーション処理を行いたい場合、携帯端末装置1の操作パネルにより所定の操作行ったりや特定のボタンを押下すると、携帯端末装置1は、操作パネルにより行われたその操作を検出したことをトリガーとして、その時点でキー2から受信している電波の受信強度を受信強度の閾値として設定する。この処理によって、結果的に、携帯端末装置1は、携帯端末装置1とキー2との距離Lを認証の成否を分ける距離とすることになる。

40

【0040】

このように、利用者がキャリブレーション処理を行うために所定の操作を行った任意の

50

時点で受信強度の閾値を携帯端末装置 1 に設定する構成によって、電波伝搬環境が変わっても、利用者によって予想される、携帯端末装置 1 による認証の成否を分ける長さ、携帯端末装置 1 が実際に認証処理を行った結果認証の成否を分ける距離 L と、を一致させることができる。

【0041】

図 2 に、本発明の第 1 実施形態の携帯端末装置およびキーの機能ブロック図を示す。本発明の第 1 実施形態の携帯端末装置 1 は、無線認証部 11、携帯通信用無線制御部 12、出力部 13、操作キー 14、携帯端末制御部 15、を含んで構成される。また、本発明の第 1 実施形態のキー 2 は、無線認証部 21、警報音出力部 22 を含んで構成される。

【0042】

携帯端末装置 1 の無線認証部 11 において、認証用無線制御部 111 は、アンテナを介して、RFID (Radio Frequency Identification: 無線周波数識別) で使用される短距離通信用の電波や UWB (Ultra Wide Band: 超広帯域無線) 等を用いて、ペアリング処理により携帯端末装置 1 と対に設定したキー 2 の識別コード信号が含まれる搬送波の送受信を所定の通信プロトコルに基づき制御する。認証用無線制御部 111 には、増幅回路、変調回路、復調回路、エンコード回路、デコード回路などの回路が含まれる。認証制御部 113 は、無線通信で使用される電波の受信強度 (例えば、復調回路に入力される電波の電圧や、デコード回路によりデコードされたデータの誤り率などを基に算出される) を計測するとともに、その受信強度が閾値記憶部 112 に記憶された数値以上か未満かを判別する。認証制御部 113 は、計測した受信強度が閾値記憶部 112 に記憶された数値以上であれば、続いて、デコードされたデータに含まれるキー 2 の識別 ID をキー 2 との間で行ったペアリング処理によって予め取得しておいた識別 ID と比較し、一致すればキー 2 との認証に成功したことを通知する使用制限解除信号を携帯端末制御部 115 に出力し、一致しなければキー 2 との認証に失敗したことを通知する使用制限要求信号を携帯端末制御部 115 に出力する。一方、認証制御部 113 は、計測した受信強度が閾値記憶部 112 に記憶された数値未満であれば、キー 2 との認証に失敗したことを通知する使用制限要求信号を携帯端末制御部 115 に出力する。

【0043】

携帯端末制御部 115 は、認証制御部 113 から使用制限要求信号を通知されている期間中、携帯端末装置 1 により実行可能な各種機能に対して、その機能の実行に制限を加える。携帯端末制御部 115 による制限の例としては、携帯電話用基地局との間の無線通信処理を制御する携帯通信用無線制御部 12 にその通信処理の一部あるいは全てを行わせないように制御したり、出力部 13 のうちのスピーカ 131 に音を出力させないように、マイク 132 に收音させないように、LCD 133 に表示させないように制御したり、操作キー 14 に入力操作を受け付けないように制御したり、などが挙げられる。また、携帯端末制御部 115 は、キャリブレーション処理を携帯端末装置 1 に実行させることが割り当てられた操作を操作キー 14 により入力されたことを検出すると、キャリブレーション処理を行うことを要求するキャリブレーション要求信号を認証制御部 113 に出力する。

【0044】

認証制御部 113 は、携帯端末制御部 115 からキャリブレーション要求信号を入力すると、その信号を入力した時点以降で計測した受信強度の値を閾値記憶部 112 に出力し、閾値記憶部 112 に記憶させる。なお、キー 2 から受信する電波のうちで、認証制御部 113 が受信強度を計測する上で好ましいものとしては、キー 2 との認証成功後にキー 2 から受信する含む電波、特に、レスポンス信号を含む電波が好ましい。このレスポンス信号を説明するために、携帯端末装置 1 とキー 2 との間で無線認証のために送受信される信号について具体的に説明する。

【0045】

携帯端末装置 1 は、キー 2 からキー 2 の識別 ID を受信すると、キー 2 から受信した識別 ID と、携帯端末装置 1 が記憶するペアリングされた識別 ID と、が一致すると判定し次第、これらの識別 ID が一致した旨 (つまり、一定距離以内にペアリングされた携帯端

10

20

30

40

50

未装置 1 が存在する旨) をキー 2 に通知して、認証モードに移行することになる。キー 2 は、携帯端末装置 1 から通知がない場合にはキー 2 の識別 ID を定期的に送信し続け、一方携帯端末装置 1 は、キー 2 から受信した識別 ID が一致するまで、キー 2 からの信号を受信し続ける(待ち受けモード)。

【0046】

キー 2 は、識別 ID が一致した旨を携帯端末装置 1 から通知されると、以後携帯端末装置 1 との間でチャレンジアンドレスポンス方式を用い、周期的に認証を行う。具体的には、キー 2 は、識別 ID が一致した旨を通知する信号を携帯端末装置 1 から受信すると、チャレンジリクエストを携帯端末装置 1 へ送信し、チャレンジリクエストを受信した携帯端末装置 1 は、乱数を発生させて生成したチャレンジ信号をキー 2 へ送信し、チャレンジ信号を受信したキー 2 は、このチャレンジ信号に対して暗号化処理を行って生成したレスポンス信号を携帯端末装置 1 へ送信し、レスポンス信号を受信した携帯端末装置 1 は、復号化したレスポンス信号とチャレンジ信号とが一致すると認証に成功したと判断し、復号化したレスポンス信号とチャレンジ信号とが不一致だと認証に失敗したと判断する。キー 2 は、認証に成功した場合には、所定の時間間隔で上記の処理を再度行い、一方、認証に失敗した場合には、待ち受けモードに移行して識別 ID の送信を開始する。

10

【0047】

レスポンス信号は、携帯端末装置が識別 ID によってキーを識別した後、携帯端末装置がそのキーから最初に受信する信号であり、携帯端末装置がペアのキーからのみ受信可能なものである。このため、認証制御部 113 は、レスポンス信号を搬送する電波の受信強度の値を閾値記憶部 112 に出力し、閾値記憶部 112 に記憶させることによって、ペアのキー 2 から送信される電波の受信強度のみをキャリブレーション処理に用いることが可能となる(つまり、他の携帯端末利用者が所持しているキーからの電波が、キャリブレーション処理に用いられることはない)。

20

【0048】

また、キー 2 の無線認証部 21 において、認証用無線制御部 211 は、アンテナを介して、RFID (Radio Frequency Identification: 無線周波数識別) で使用される短距離通信の電波や UWB (Ultra Wide Band: 超広帯域無線) 等を用いて、ペアリング処理によりキー 2 と対に設定した携帯端末装置 1 の識別コード信号が含まれる搬送波の送受信を所定の通信プロトコルに基づき制御する。認証用無線制御部 211 には、増幅回路、変調回路、復調回路、エンコード回路、デコード回路などの回路が含まれる。認証処理部 213 は、無線通信で使用される電波の受信強度(例えば、復調回路に入力される電波の電圧や、デコード回路によりデコードされたデータの誤り率などを基に算出される)を計測するとともに、その受信強度が閾値記憶部 212 に記憶された数値以上か未満かを判別する。認証処理部 213 は、計測した受信強度が閾値記憶部 212 に記憶された数値以上であれば、続いて、デコードされたデータに含まれる携帯端末装置 1 の識別 ID の識別(チェック)を携帯端末装置 1 との間で行ったペアリング処理によって予め取得しておいた識別 ID と比較し、一致すれば携帯端末装置 1 との認証に成功したことを通知する警報解除信号を警報音出力部 22 に出力し、一致しなければ携帯端末装置 1 との認証に失敗したことを通知する警報要求信号を警報音出力部 22 に出力する。一方、認証処理部 213 は、計測した受信強度が閾値記憶部 212 に記憶された数値未満であれば、携帯端末装置 1 との認証に失敗したことを通知する警報要求信号を警報音出力部 22 に出力する。

30

40

【0049】

警報音出力部 22 は、スピーカによって構成され、認証処理部 213 から警報要求信号を入力すると、警報音の出力を開始する。

【0050】

以上、本発明の第 1 実施形態の携帯端末装置およびキーによれば、利用者がキャリブレーション処理を行うために所定の操作を行った時点で受信強度の閾値を携帯端末装置に設定する構成によって、電波伝搬環境が変わっても、携帯端末装置とキーとを一定の距離離れた状態で再度キャリブレーション処理を行えば、利用者によって予想される、携帯端末

50

装置による認証の成否を分ける長さ、携帯端末装置が実際に認証処理を行った結果認証の成否を分けることになる距離と、を一致させることができる。

【0051】

なお、キャリアレーション処理において、計測した受信強度の値を閾値として記憶させるようにしたが、これに限るものではなく、計測した受信強度を利用して算出した別の数値を閾値として記憶させるようにしてもよい。すなわち、図1(a)に示す、受信強度の閾値の設定操作を表す概要図では、携帯端末装置1は、一定の間隔L離れたキーから受信した電波の受信強度を閾値として設定することによって認証の成否を分ける距離をLと見なすようにしたが、図1(b)に示す、受信強度の閾値の設定操作を表す別の概要図では、一定の間隔L離れたキーから受信した電波の受信強度に対して $1/K^2$  (Kは実数)を乗算した数値を閾値として設定することによって認証の成否を分ける距離を $K \times L$ と見なすようにした。この閾値の設定手法は、電波の電磁界強度が、伝搬する距離の二乗に反比例して減衰することを利用したものである。実数Kは、キャリアレーション処理を行ったときの携帯端末装置1とキー2の距離に応じて利用者が設定する数値である。

10

【0052】

携帯端末装置1は、キー2から受信した電波の受信強度を計測するのみであり、携帯端末装置1とキー2の距離Lを計測しているわけではない。しかし、携帯端末装置1は、上記の閾値の設定手法では、携帯端末装置1とキー2の距離Lを単位長さ(その単位長さの数値は計測付加)として認識し、その単位長さを基に表される距離 $L'$  ( $L' = K \times L$ )を認証の成否を分ける距離として見なしている。この構成により、利用者は、キャリアレーション処理を携帯端末装置に行わせたときの携帯端末装置とキーとの距離(単位長さL)を基に認証の成否を分ける距離 $L'$ を設定することによって、利用者によって予想される、携帯端末装置による認証の成否を分ける長さ、携帯端末装置が実際に認証処理を行った結果認証の成否を分けることになる距離と、を一致させつつ、簡易にその距離を調整することができる。

20

【0053】

さらに、一定の間隔L離れたキー2から受信した電波の受信強度に対して $1/K^2$  (Kは実数)を乗算した数値を閾値として設定する、上記の閾値の設定手法により、携帯端末装置1は、複数の閾値を記憶し、キー2から受信する電波の受信強度がそのうちの一つの閾値以上から同閾値未満に推移すれば携帯端末装置1により実行可能な各種機能に対して制限を加え、一方、キー2から受信する電波の受信強度が別の閾値未満から同閾値以上に推移すれば各種機能に加えていた制限を解除するようにしてもよい。図1(c)に示す、受信強度の閾値の設定操作を表す別の概要図では、携帯端末装置1は、閾値として、一定の間隔L離れたキーから受信した電波の受信強度(第1の閾値。図1(c)の内側の円が、認証の成否を分ける境界)と、一定の間隔L離れたキー2から受信した電波の受信強度に対して $1/K^2$  (Kは実数)を乗算して算出した閾値(第2の閾値。図1(c)の外側の円が、認証の成否を分ける境界)と、を記憶している。携帯端末装置1は、キー2から受信する電波の受信強度が第2の閾値以上から第2の閾値未満に推移すれば(つまりキー2が外側の円の「内」から「外」に移動すれば)、携帯端末装置1により実行可能な各種機能に対して制限を加え、キー2から受信する電波の受信強度が第1の閾値未満から第1の閾値以上に推移すれば(つまりキー2が内側の円の「外」から「内」に移動すれば)、各種機能に加えていた制限を解除する。

30

40

【0054】

この構成により、携帯端末装置により実行可能な各種機能に対する制限、あるいは制限解除タイミングのバリエーションを増やし、その結果、利用者による携帯端末装置とキーの使い方に適した距離にて携帯端末装置に各種機能の制限、あるいは制限解除をさせることができる。

【0055】

なお、本発明の第1実施形態では、携帯端末装置1がキャリアレーション処理を行うことを指示する操作を利用者から受け付け、携帯端末装置1が閾値を記憶するように記載し

50

たが、キー 2 に操作キーを設け、キー 2 がキャリブレーション処理を行うことを指示する操作を利用者から受け付け、閾値記憶部 2 1 2 に閾値を記憶する構成としてもよい。また、キー 2 に操作キーを設けなくても、キー 2 は、キャリブレーション処理を行った携帯端末装置から設定された閾値を認証用無線制御部 2 1 1 を介して受信し、受信した閾値を閾値記憶部 2 1 2 に記憶するようにしてもよい。この構成により、キーでも、携帯端末装置と同様に閾値を設定することができる。

#### 【 0 0 5 6 】

( 第 2 実施形態 )

図 3 に、本発明の第 2 実施形態の携帯端末装置およびキーの機能ブロック図を示す。本発明の第 2 実施形態の携帯端末装置 1 は、無線認証部 1 1 にタイマー 1 1 4 が含まれている点

10

#### 【 0 0 5 7 】

認証制御部 1 1 3 は、一定時間を計時する度にその旨を通知するタイマー 1 1 4 からその通知信号を入力すると、その通知信号を入力した時点以降で計測した受信強度の値を閾値記憶部 1 1 2 に出力し、閾値記憶部 1 1 2 に記憶させる。

#### 【 0 0 5 8 】

以上、本発明の第 2 実施形態の携帯端末装置およびキーによれば、携帯端末装置とキーの距離がほとんど変化しない場合において、電波伝搬環境が変わっても（例えば、携帯端末装置やキーをカバンやポケットの中に入れることによって、電波伝搬環境が悪くなっても）、認証に成功したあるいは失敗したことを判定するための閾値を自動的に更新し、認証の成否を分ける携帯端末装置とキーとの距離を一定に保つことができる。

20

#### 【 0 0 5 9 】

なお、キャリブレーション処理において、計測した受信強度の値を閾値として記憶させるようにしたが、これに限るものではなく、第 1 実施形態において図 1 ( b )、図 1 ( c ) を参照して説明したように、ある単位長さで計測した受信強度を利用して、その単位長さの実数倍の距離を認証の成否を分ける距離として調整する別の数値を閾値として記憶させるようにしてもよい。

#### 【 0 0 6 0 】

なお、本発明の第 2 実施形態では、携帯端末装置 1 が一定時間間隔でキャリブレーション処理を行い、携帯端末装置 1 が閾値を記憶するように記載したが、キー 2 にタイマーを設け、キー 2 が一定時間間隔でキャリブレーション処理を行い、閾値記憶部 2 1 2 に閾値を記憶する構成としてもよい。また、キー 2 にタイマーを設けなくても、キー 2 は、キャリブレーション処理を行った携帯端末装置から設定された閾値を認証用無線制御部 2 1 1 を介して受信し、受信した閾値を閾値記憶部 2 1 2 に記憶するようにしてもよい。この構成により、キーでも、携帯端末装置と同様に閾値を設定することができる。

30

#### 【 0 0 6 1 】

( 第 3 実施形態 )

図 4 に、本発明の第 3 実施形態の携帯端末装置およびキーの機能ブロック図を示す。本発明の第 3 実施形態の携帯端末装置 1 は、無線認証部 1 1 に受信強度記憶部 1 1 5 および閾値算出部 1 1 6 が含まれている点

40

#### 【 0 0 6 2 】

受信強度記憶部 1 1 5 は、認証制御部 1 1 3 が計測した受信強度を入力し、入力した順に一定時間間隔でその受信強度を記憶する。閾値算出部 1 1 6 は、受信強度記憶部 1 1 5 に時系列順に記憶された受信強度の値から、閾値記憶部 1 1 2 に記憶させるべき閾値を算出し、その閾値を閾値記憶部 1 1 2 に出力する。以降、閾値算出部 1 1 6 による閾値算出例を説明する。図 5 に、受信強度とその受信強度を基に算出した閾値の関係を示す。

50

## 【0063】

図5(a)に示す受信強度とその受信強度を基に算出した閾値の関係では、閾値算出部116は、閾値記憶部112に受信強度が4つ記憶されたときにそれらの受信強度の平均値を算出し、その平均値を以降の閾値として設定している。具体的には、時刻t1から時刻t4の期間では、認証制御部113は時刻t1以前の受信強度を平均化した閾値をもとに受信電界の高低を判別しており、時刻t5から時刻t8の期間では、認証制御部113は時刻t1から時刻t4の期間の受信強度を平均化した閾値をもとに受信電界の高低を判別しており、時刻t8以降の期間では、認証制御部113は時刻t5から時刻t8の期間の受信強度を平均化した閾値をもとに受信電界の高低を判別している。

## 【0064】

また、図5(b)に示す受信強度とその受信強度を基に算出した閾値の関係の別の例では、閾値算出部116は、受信強度の変化量を算出し、ある値以上受信強度が変化すれば、その受信強度の変化分だけ閾値を変化させるものである。具体的には、閾値算出部116は、受信強度記憶部115に連続して記憶されている受信強度が10dBm以上変化すれば閾値を増減するように設定されており、時刻t5の受信強度が時刻t4の受信強度と比べて10dBm以上減少していることを検出すると、時刻t5以前の閾値よりも10dBm減少させた数値を時刻t5以降の閾値とし、認証制御部113はその閾値をもとに受信電界の高低を判別している。

## 【0065】

以上、本発明の第3実施形態の携帯端末装置によれば、携帯端末装置とキーの距離がほとんど変化しない場合において、電波伝搬環境が変わっても、認証に成功したあるいは失敗したことを判定するための閾値を受信強度の値の変化に応じて自動的に更新し、認証の成否を分ける携帯端末装置とキーとの距離を一定に保つことができる。

## 【0066】

なお、キャリブレーション処理において、算出した受信強度の値を閾値として記憶させるようにしたが、これに限るものではなく、第1実施形態において図1(b)、図1(c)を参照して説明したように、ある単位長さで算出した受信強度を利用して、その単位長さの実数倍の距離を認証の成否を分ける距離として調整する別の数値を閾値として記憶させるようにしてもよい。

## 【0067】

なお、本発明の第3実施形態では、携帯端末装置1がある条件にて算出した電界強度を基にキャリブレーション処理を行い、携帯端末装置1が閾値を記憶するように記載したが、キー2に受信強度記憶部および閾値算出部を設け、キー2がある条件にて算出した電界強度を基にキャリブレーション処理を行い、閾値記憶部212に閾値を記憶する構成としてもよい。また、キー2に受信強度記憶部および閾値算出部を設けなくても、キー2は、キャリブレーション処理を行った携帯端末装置から設定された閾値を認証用無線制御部211を介して受信し、受信した閾値を閾値記憶部212に記憶するようにしてもよい。この構成により、キーでも、携帯端末装置と同様に閾値を設定することができる。

## 【産業上の利用可能性】

## 【0068】

本発明の携帯端末装置およびキーによれば、携帯端末装置とキーとの間で認証の成否を分ける閾値を電波伝搬環境に応じた値に動的に設定することによって、電波伝搬環境が変わっても、認証の成否を分ける携帯端末装置とキーの距離を一定に保つことができるという効果を奏し、携帯端末装置を置き忘れたときや盗難に遭ったときに、機能の一部あるいは全ての実行を禁止する携帯端末装置および携帯端末装置所有者に警報を発するキーに関して有用である。

## 【図面の簡単な説明】

## 【0069】

【図1】(a)受信強度の閾値の設定操作を表す概要図 (b)受信強度の閾値の設定操作を表す別の概要図 (c)受信強度の閾値の設定操作を表す別の概要図

10

20

30

40

50

【図2】本発明の第1実施形態の携帯端末装置およびキーの機能ブロック図

【図3】本発明の第2実施形態の携帯端末装置およびキーの機能ブロック図

【図4】本発明の第3実施形態の携帯端末装置およびキーの機能ブロック図

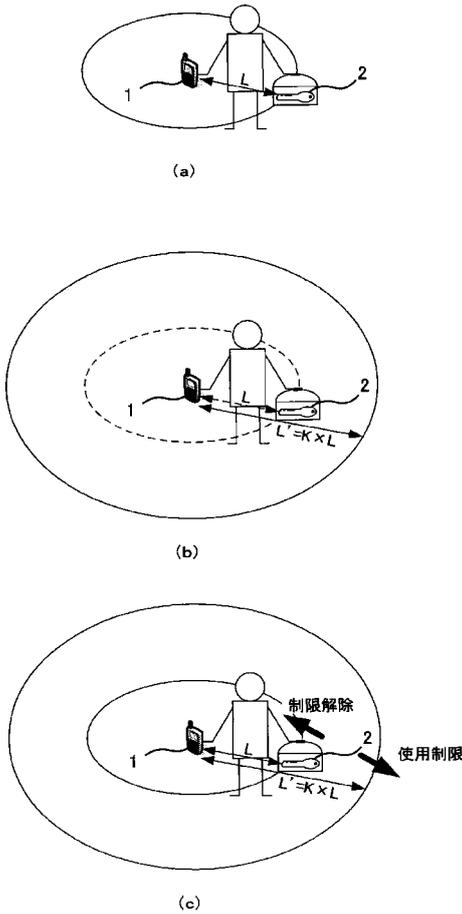
【図5】(a)受信強度とその受信強度を基に算出した閾値の関係の一例 (b)受信強度とその受信強度を基に算出した閾値の関係の別の例

【符号の説明】

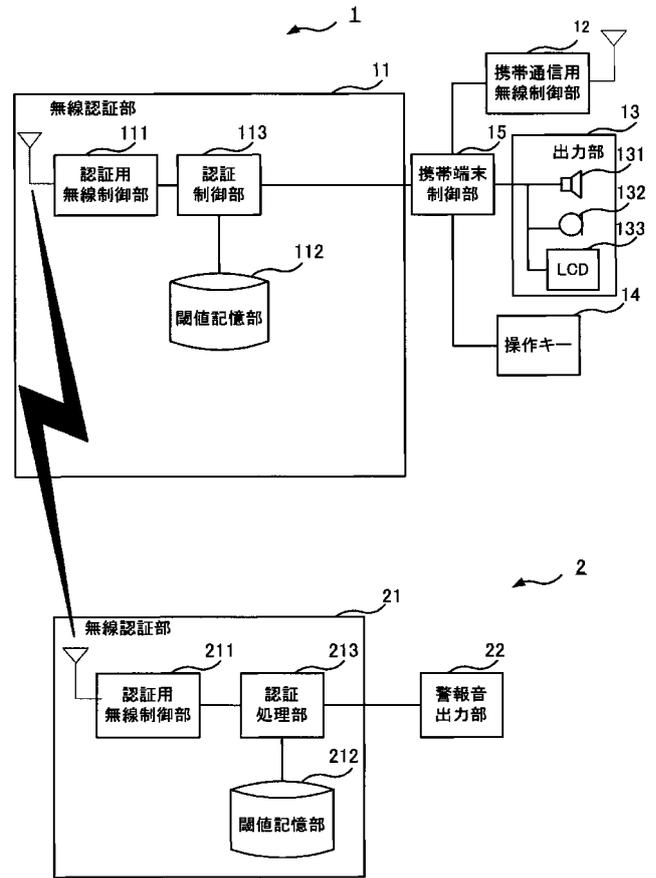
【0070】

- |       |            |    |
|-------|------------|----|
| 1     | 携帯端末装置     |    |
| 1 1   | 無線認証部      |    |
| 1 1 1 | 認証用無線制御部   | 10 |
| 1 1 2 | 閾値記憶部      |    |
| 1 1 3 | 認証制御部      |    |
| 1 1 4 | タイマー       |    |
| 1 1 5 | 受信強度記憶部    |    |
| 1 1 6 | 閾値算出部      |    |
| 1 2   | 携帯通信用無線制御部 |    |
| 1 3   | 出力部        |    |
| 1 3 1 | スピーカ       |    |
| 1 3 2 | マイク        |    |
| 1 3 3 | L C D      | 20 |
| 1 4   | 操作キー       |    |
| 1 5   | 携帯端末制御部    |    |
| 2     | キー         |    |
| 2 1   | 無線認証部      |    |
| 2 1 1 | 認証用無線制御部   |    |
| 2 1 2 | 閾値記憶部      |    |
| 2 1 3 | 認証処理部      |    |
| 2 2   | 警報音出力部     |    |

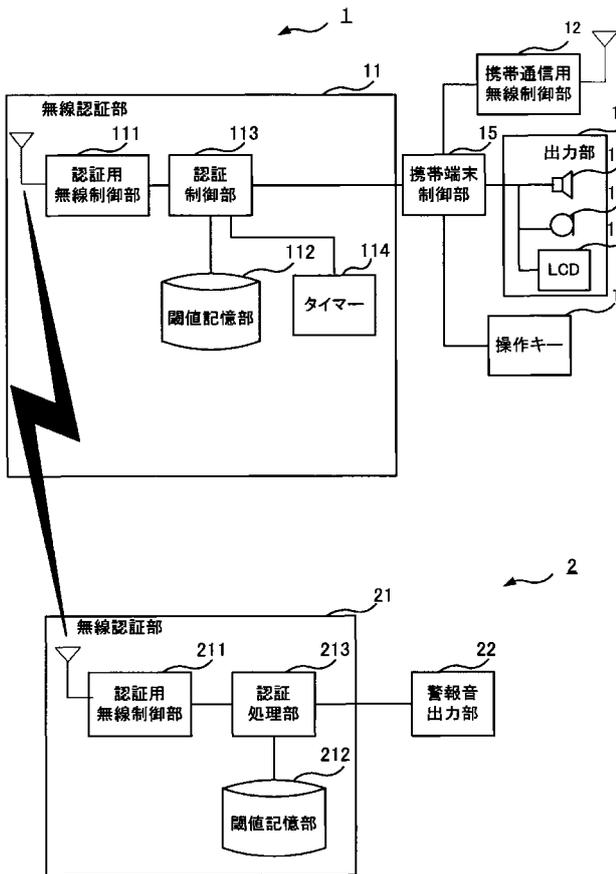
【図1】



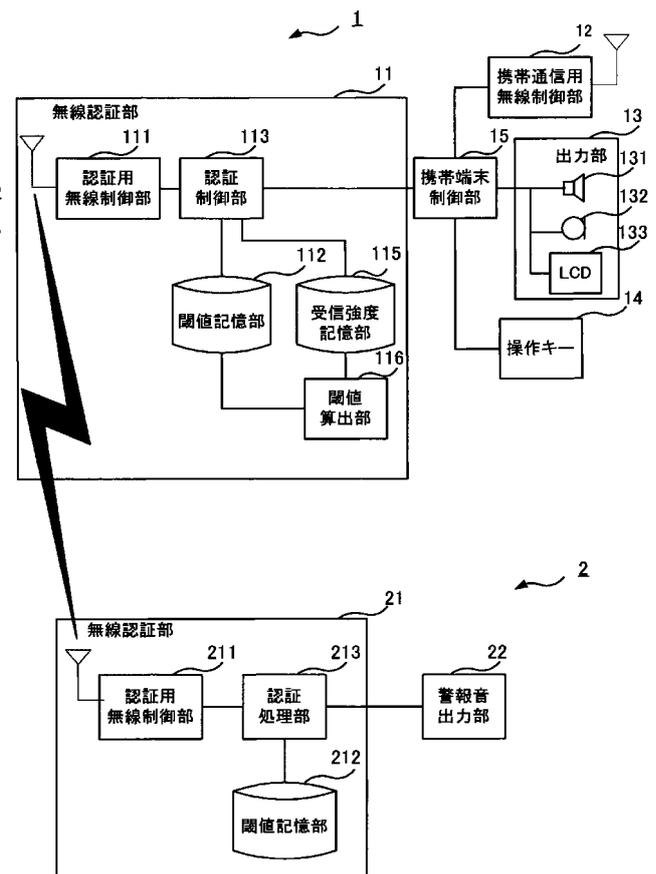
【図2】



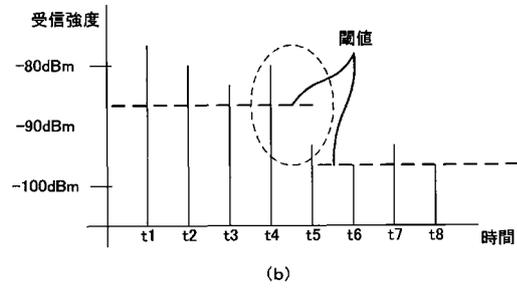
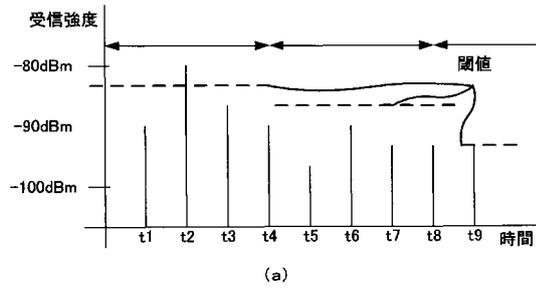
【図3】



【図4】



【 図 5 】



---

フロントページの続き

(72)発明者 渡邊 崇士

大阪府門真市大字門真 1 0 0 6 番 松下電器産業株式会社内

Fターム(参考) 5K027 AA11 BB09 HH11

5K067 AA32 BB04 DD44 EE02 EE03 EE35 FF25 HH22