(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2004-304294
(P2004-304294A)
(43)公開日　平成16年10月28日(2004.10.28)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04Q	7/38	H04B	7/26	109R	5J104
H04L	9/32	H04L	9/00	673D	5K067

審査請求 未請求　請求項の数 9　OL　（全 13 頁）

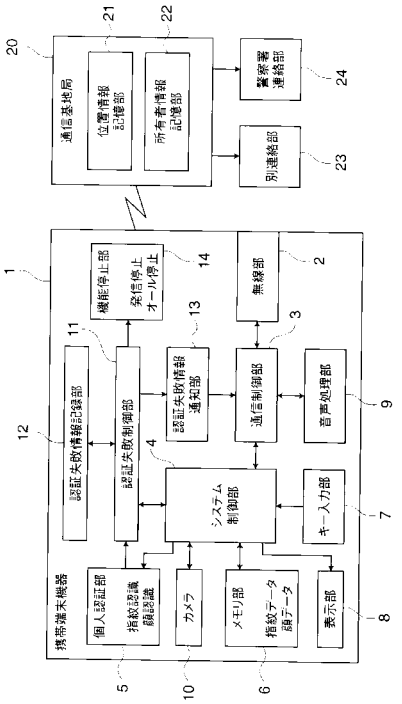
(21)出願番号　特願2003-92095(P2003-92095)
(22)出願日　平成15年3月28日(2003.3.28)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町２２番２２号
(74)代理人　100065248
弁理士　野河　信太郎
(72)発明者　桑島　秀紀
大阪府大阪市阿倍野区長池町２２番２２号
シャープ株式会社内

Fターム(参考)　5J104 AA07 KA01 KA04 KA16 KA17
MA01 NA05 NA27 NA38 PA01
5K067 AA32 EE02 EE10 HH22 HH23

(54)【発明の名称】個人認証機能付き携帯端末機器およびそのシステム

(57)【要約】
【課題】携帯端末機器に個人認証の機能を設けることで、盗難や紛失によって第三者の手に渡った携帯端末機器の第三者による不正使用を防止する。
【解決手段】携帯端末機器に、正規ユーザーの指紋情報を記憶した指紋情報メモリと、指紋センサとを設け、プロセッサにより、指紋センサで読み取った指紋情報が指紋情報メモリに記憶した正規ユーザーの指紋情報と一致するか否かを判定し、不一致であった場合にはその結果を通信基地局に通知する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
通信基地局との双方向通信を行う通信機能を有する携帯端末機器であって、
個人認証情報を記憶する個人認証情報記憶部と、
携帯端末機器の使用者が正規の使用者であるのか否かを識別するための識別情報を入力する識別情報入力部と、
個人認証情報記憶部に記憶された個人認証情報に基づいて、識別情報入力部から入力された識別情報の個人認証を行う個人認証部と、
個人認証部による個人認証の結果、識別情報の個人認証が不成立であった場合には個人認証部の認証結果を通信基地局に通知する通知部を備えてなる個人認証機能付き携帯端末機器。
【請求項２】
個人認証情報記憶部に記憶された個人認証情報が指紋情報からなり、
識別情報入力部が携帯端末機器の使用者の指紋を入力する指紋入力部からなり、
個人認証部が、個人認証情報記憶部に記憶された指紋情報に基づいて、指紋入力部から入力された指紋の個人認証を行う請求項１記載の個人認証機能付き携帯端末機器。
【請求項３】
個人認証情報記憶部に記憶された個人認証情報が顔画像情報からなり、
識別情報入力部が携帯端末機器の使用者の顔を撮像するためのカメラからなり、
個人認証部が、個人認証情報記憶部に記憶された顔画像情報に基づいて、カメラで撮像された顔画像の個人認証を行う請求項１記載の個人認証機能付き携帯端末機器。
【請求項４】
識別情報の個人認証が不成立であった場合にその認証不成立の結果を記憶する認証結果記憶部と、識別情報の個人認証が不成立であった場合の制御を行う認証失敗制御部をさらに備え、
認証失敗制御部は、使用者から発信制御が行われたときに認証結果記憶部に記憶された認証不成立の結果が通信基地局に通知されるよう通知部を制御する請求項１記載の個人認証機能付き携帯端末機器。
【請求項５】
識別情報の個人認証が不成立であった場合にその認証不成立の結果を記憶する認証結果記憶部と、識別情報の個人認証が不成立であった場合の制御を行う認証失敗制御部をさらに備え、
認証失敗制御部は、個人認証の不成立が所定の回数に達したときに認証結果記憶部に記憶された認証不成立の結果が通信基地局に通知されるよう通知部を制御する請求項１記載の個人認証機能付き携帯端末機器。
【請求項６】
通知部により認証結果が通信基地局に通知された後、通信機能の一部または全部を停止する機能停止部をさらに備えてなる請求項１記載の個人認証機能付き携帯端末機器。
【請求項７】
請求項１～６のいずれか１つに記載の携帯端末機器と、その携帯端末機器と双方向通信を行う通信基地局とからなる個人認証機能付き携帯端末機器システムであって、
通信基地局が、携帯端末機器の所有者の氏名、有線電話番号などの所有者情報を記憶する所有者情報記憶部と、携帯端末機器から識別情報の個人認証不成立の結果を受信するとその個人認証不成立の結果を所有者情報記憶部に記憶された所有者情報を参照して所有者に通知する認証結果所有者通知部を備えてなる個人認証機能付き携帯端末機器システム。
【請求項８】
通信基地局が、携帯端末機器から識別情報の個人認証不成立の結果を受信するとその個人認証不成立の結果を所定の機関に通知する認証結果所定機関通知部をさらに備えてなる請求項７記載の個人認証機能付き携帯端末機器システム。
【請求項９】

通信基地局が、識別情報の個人認証不成立の結果を受信したことを認証結果所有者通知部または認証結果所定機関通知部で通知する際、携帯端末機器と通信した通信基地局の位置情報を通知内容に含ませる位置情報付加部をさらに備えてなる請求項７または８記載の携帯端末機器システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、個人認証機能付き携帯端末機器およびそのシステムに関し、さらに詳しくは、携帯端末機器の盗難や紛失が発生した際の第三者による不正使用を防止する個人認証機能付き携帯端末機器およびそのシステムに関する。

【０００２】

【従来の技術】

近年、携帯電話やモバイル機器のような携帯端末機器の普及が進んでおり、利便性が一挙に拡大されてきている。しかし、一方では物理的な接続がなく、持ち運び可能であることから、盗難・紛失などの事態が発生する可能性もある。この場合、盗難・紛失などから第三者に渡った携帯端末機器は、携帯端末機器の所有者の意思に反して不正に使用される可能性がある。

【０００３】

このような第三者の不正使用を防止するため、所有者が携帯端末機器の紛失に気がついた時点で、携帯端末機器の一部あるいはすべての機能を停止する、いわゆる携帯端末機器をロックする技術が知られている（例えば、特許文献１参照）。

【０００４】

この技術では、携帯端末機器以外の通信装置からリモート操作で携帯端末機器の利用をロックするように制御することができる。この技術を用いることにより、紛失した携帯端末機器の第三者による不正使用を防止することができる。

【０００５】

しかしこの技術は、所有者が携帯端末機器の盗難・紛失に気づいた後の対応を前提としている。したがって、携帯端末機器を紛失した時点から紛失に気がつくまでの間は、第三者による不正使用を防止することはできない。すなわち即時性のある対応はできない。

【０００６】

そこで、この即時性を考慮した技術も開発されている（例えば、特許文献２参照）。図８にこの従来技術における携帯端末機器のシステム構成図を示す。

この技術では、携帯端末機器３１とは別に、携帯端末機器３１に対応した位置登録端末機器３２をあらかじめ用意しておく。そして、携帯端末機器３１と共に、位置登録端末機器３２も通信基地局３３に随時、位置情報を通知する。もし、携帯端末機器３１と位置登録端末機器３２の距離が一定距離以上離れれば、通信基地局３３から所有者にその情報を通知する。この手法により、携帯端末機器の盗難・紛失を早急に検知できるため、携帯端末機器の所有者は、この通知をもって速やかに通信基地局に対して、携帯端末機器のロックを行うように手続きすることで、第三者の不正使用を防止することができる携帯端末機器システムを提案している。

【０００７】

【特許文献１】

特開平６－１２５３０５号公報

【特許文献２】

特開平９－１９１３４２号公報

【０００８】

【発明が解決しようとする課題】

しかしながら、携帯端末機器とは別に位置登録端末機器も一緒に持ち運ぶようにした場合には、携帯としての利便性を損ねてしまう。昨今の携帯端末機器は小型軽量化が重要なテーマになっており、この点は大きなマイナス要素である。

【０００９】
また、消費電力との兼ね合いもあるが、携帯端末機器、位置登録端末機器共に、可能な限り位置登録情報を更新したとしても、紛失した携帯端末機器の不正使用の場所が同一通信基地局内であれば、この不正使用を防止することができない。
【００１０】
本発明は、このような事情を考慮してなされたもので、携帯端末機器に個人認証の機能を設けることで、盗難や紛失によって第三者の手に渡った携帯端末機器の第三者による不正使用を防止することを目的とするものである。
【００１１】
【課題を解決するための手段】
本発明は、通信基地局との双方向通信を行う通信機能を有する携帯端末機器であって、個人認証情報を記憶する個人認証情報記憶部と、携帯端末機器の使用者が正規の使用者であるのか否かを識別するための識別情報を入力する識別情報入力部と、個人認証情報記憶部に記憶された個人認証情報に基づいて、識別情報入力部から入力された識別情報の個人認証を行う個人認証部と、個人認証部による個人認証の結果、識別情報の個人認証が不成立であった場合には個人認証部の認証結果を通信基地局に通知する通知部を備えてなる個人認証機能付き携帯端末機器である。
【００１２】
本発明によれば、識別情報入力部から個人認証用の識別情報が入力されると、あらかじめ記憶された個人認証情報に基づいて、入力された識別情報の個人認証が行われる。その結果、識別情報の個人認証が不成立であった場合には、その認証結果が通信基地局に通知される。通信基地局では、その結果に基づいて、該当する携帯端末機器の使用を制限したり、有線電話で所有者に連絡するなど、各種の対策を講ずることが可能となり、これにより、所有者が携帯端末機器の盗難や紛失に気づいていない場合でも、第三者による不正使用を確実に防止することができる。
【００１３】
【発明の実施の形態】
本発明において、個人認証情報記憶部は、個人認証を行うことが可能な情報を記憶できるものであればよく、当該分野で公知の各種の半導体メモリ、磁気記録媒体、光学式記憶媒体などを適用することができる。この個人認証情報記憶部は、小型の携帯端末機器に内蔵可能なものであることが望ましく、その点からはデジタルカメラの記憶媒体などに用いられているカード式メモリなどを適用することが望ましい。
【００１４】
識別情報入力部は、携帯端末機器の使用者が正規の使用者であるのか否かを識別するための識別情報を入力できるものであればよく、当該分野で公知の各種の入力装置を適用することができる。
【００１５】
この識別情報入力部は、携帯端末機器の使用者の指紋を入力する指紋入力部で構成されていてもよい。指紋入力部としては、指紋センサに指を置いたときに、センサ内の電荷の量から指紋の形を判定する半導体式指紋センサなどを適用することができる。また、識別情報入力部は、携帯端末機器の使用者の顔を撮像するためのカメラで構成されていてもよい。カメラとしては、携帯端末機器に内蔵可能な小型のＣＣＤカメラなどを適用することができる。
【００１６】
識別情報入力部を指紋入力部で構成する場合には、個人認証情報記憶部には個人認証情報として指紋情報を記憶させておき、指紋センサで検出した指紋情報を個人認証情報記憶部の指紋情報と比較して個人認証を行う。また、識別情報入力部をカメラで構成する場合には、個人認証情報記憶部には個人認証情報として顔画像情報を記憶させておき、カメラで撮影された顔画像情報を個人認証情報記憶部の顔画像情報と比較して個人認証を行う。
【００１７】

個人認証部は、個人認証情報記憶部に記憶された個人認証情報に基づいて、識別情報入力部から入力された識別情報の個人認証を行うことができるものであればよい。この個人認証部としては、プログラムで作動可能な各種のプロセッサを適用することができる。このプロセッサは、携帯端末機器のプロセッサを適用したものであってもよいし、携帯端末機器とは別のプロセッサを用いたものであってもよい。

【００１８】

通知部は、個人認証部による個人認証の結果、識別情報の個人認証が不成立であった場合にはその認証結果を通信基地局に通知できるものであればよく、当該分野で公知の各種の情報送信装置を適用することができる。この通知部としては、携帯端末機器に内蔵した通常の情報送信に利用する情報送信装置を適用することが望ましい。

【００１９】

以下、図面に示す実施の形態に基づいてこの発明を詳述する。なお、この発明はこれによって限定されるものではなく、各種の変形が可能である。

【００２０】

図１は本発明の個人認証機能付き携帯端末機器システムの構成を示すブロック図である。本携帯端末機器システムは携帯端末機器１と通信基地局２０とで構成される。

【００２１】

携帯端末機器１は、携帯電話やモバイル機器からなり、無線部２、通信制御部３、システム制御部４、個人認証部５、メモリ部６、キー入力部７、表示部８、音声処理部９、カメラ部１０、認証失敗制御部１１、認証失敗情報記録部１２、認証失敗情報通知部１３、および機能停止部１４から構成されている。

【００２２】

通信基地局２０は、位置情報記憶部２１と所有者情報記憶部２２とを有している。また、通信基地局２０には、携帯電話以外の例えば有線電話などにより携帯電話の所有者と連絡をとるための別連絡部２３と、警察署に連絡をとるための警察署連絡部２４とが設けられている。

【００２３】

無線部２は、通信基地局２０との間で無線回線を通じて、通信を行うための電波信号と電気信号をお互い変換する機能を有している。

通信制御部３は、通信を実現するための、いわゆるベースバンド処理回路であり、一般にはモデム機能やチャネルコーディック機能から実現される。

【００２４】

例えば、電波信号受信時、モデムには、通信基地局２０から送られてきた電波信号が、無線部２を介することにより、電気信号（アナログ信号）として変換され、入力される。

【００２５】

モデムは、受信したアナログ信号をデジタル信号に変換して（いわゆる復調）、後段のチャネルコーディックにデジタル信号情報を渡す。チャネルコーディックは、このデジタル信号情報に対して、通信の規格で定められた特定のデジタル処理を行う。なお、本例におけるチャネルコーディックは、音声情報信号とシステム制御信号の分離、結合を行う機能も備えているものと定義する。特定のデジタル処理が終了したら、音声情報信号とシステム制御信号を分離して、音声情報信号は音声処理部９へ、システム制御信号はシステム制御部４へそれぞれ渡す。

【００２６】

また、電波信号送信時には、チャネルコーディックはシステム制御部４からのシステム制御信号と、音声処理部９からの音声情報信号とを結合、さらに、特定のデジタル処理を行ったのち、モデムへ送信デジタル信号として渡す。

モデムは、このデジタル信号をアナログ信号に変換し（変調）、無線部２を介することで電波信号とし、通信基地局２０へ信号を送出する。

【００２７】

通信プロトコルに則する必要な信号のやり取りが通信基地局２０と正常に行われることに

より、携帯端末機器１は通信基地局２０と通信できる、いわば接続された状態となる。
【００２８】
システム制御部４は、いわゆるマイコンや、マイコンが作業を行うため必要な一時記憶部などから構成され、携帯端末機器１のシステム全体の制御を行う。
システム制御部４には、携帯端末機器１の使用者が正規な使用者（以下、正規ユーザーと記載する）かどうかの個人認証を行うことができる個人認証部５、電話アドレス情報やメールなどの情報を記憶しておくメモリ部６、携帯端末機器へ情報を入力するためのキー入力部７、個人情報やシステムの状態などを表示する表示部８、個人認証失敗時にあらかじめ定めておいた処理を携帯端末機器で行うように制御する認証失敗制御部１１、およびカメラ１０が接続されている。
【００２９】
個人認証部５は、番号の組み合わせ等のいわゆるパスワードではなく、指紋や顔情報のような生体情報から個人認証を行う、いわゆるバイオメトリクス認証技術を適用したものである。これは、利便性や、セキュリティのレベルの向上に大きく貢献する。具体的な個人認証の手段としては、本例では指紋認証技術を用いている。これに代えて、カメラ１０などを使用しての顔認証技術を用いてもよい。
【００３０】
指紋認証技術には、指紋センサに指を置いたときに、センサ内の電荷の量から指紋の形を判定する半導体式指紋認証方式など、いくつかの手法があるが、本例では特にこだわらない。
【００３１】
したがって、個人認証部５は、指紋情報を読み取る指紋センサ、特別な正規ユーザー登録方法で正規ユーザーの指紋データを登録、格納するメモリ、指紋センサで読み取られた指紋データと、登録してある正規ユーザーの指紋データとを比較して、正規ユーザーとして識別できるかどうか判断する比較器を備えている。比較器から出力される個人認証結果情報は、認証失敗制御部１１に送られる。
【００３２】
携帯端末機器１は、所有者だけでなく、複数の人数で使用するケースも考えられる。この場合、こちらも特別な正規ユーザー登録方法で、新規ユーザーの指紋データを追加登録してもよい。特別な正規ユーザー登録方法とは、処理フローの説明時に記載（後述）する。
【００３３】
メモリ部６は、携帯端末機器のいわゆるプログラムを格納しているＲＯＭや、電話アドレス情報や、メールなどの情報を記憶しておくことができるＦＲＯＭなどから構成されており、必要に応じてシステム制御部４との間で情報の読み出しや書き込みが行われる。
【００３４】
キー入力部７は、テンキーや各種モードキーなどから構成されており、携帯端末機器の使用者のキー操作を入力情報として、システム制御部４に渡す。
表示部８は、ドットマトリクス構成の液晶パネルおよび各ドライバなどから構成され、キー入力部７から入力された番号などの情報画像や、各種通信モードを表す画像、電話機能の動作状態を示すアイコン画像等、携帯端末機器としての必要な情報が、システム制御部４からの指示により適宜表示される。
【００３５】
音声処理部９は、音声情報信号から実際の音声に変換するためのＤ／Ａコンバータ、フィルタ、スピーカなどを備え、通信制御部３から入力された音声情報を、携帯端末機器の外に実際の音声として出力する。また、実際の音声がマイクから入力されたら、Ａ／Ｄコンバータ、フィルタなどを用いて、音声処理を行った後、音声情報信号（デジタル信号）を通信制御部３に渡す機能を備える。
【００３６】
認証失敗制御部１１は、個人認証失敗時に、携帯端末機器１に対してどのような処理を行うかをまとめたブロックであり、認証失敗情報記録部１２、認証失敗情報通知部１３、機

能停止部１４と接続される。
【００３７】
認証失敗情報記録部１２は、個人認証を何回失敗、あるいは成功したかを記憶する。なお、本例では個人認証部５やメモリ部６とは別に記載しているが、これらに含まれていてもよい。
携帯端末機器１の構成は上記のとおりである。
【００３８】
携帯端末機器１の使用契約時には、あらかじめ通信基地局２０を管理する通信キャリア側へ、正規ユーザーの緊急連絡先などの所有者情報を登録しておく。この所有者情報は所有者情報記憶部２２に記憶されている。通信キャリア側は、携帯端末機器１以外の例えば有線電話などで正規ユーザーに連絡をとるための別連絡部２３を有しており、この別連絡部２３を用い、所有者情報記憶部２２を参照することで、正規ユーザーに連絡することができるようになっている。なお、携帯端末機器の使用契約時と記載したが、もちろんこの時点のみではなく、携帯端末機器システムの適用開始時までに所有者情報を登録すればよい。図７に所有者情報の一例を示す。
【００３９】
以下、上述のように構成された携帯端末機器システムの動作について説明する。最初に、一般的な携帯端末機器の処理フローの一例を図２に示す。
まず、キー入力部７による携帯端末機器１の電源ＯＮ操作が行われると、携帯端末機器起動処理が行われる（ステップＳ１）。この処理は、携帯端末機器自体の起動処理の他、セルサーチ等、通信プロトコルに即した所定の処理も含む。この所定の手続きにより、通信基地局２０との交信を開始し、通信可能な状態に進む（ステップＳ２）。これを本例では待機状態と記載する。
【００４０】
また、待機状態であることを使用者に報知するため、表示部８に適切な情報を表示してもよい。たとえば、携帯端末機器に一般的に内蔵されている時計機能から、現在の時刻を表示する。一般的に、携帯端末機器はこの待機状態のまま使用される。
【００４１】
携帯端末機器１は待機状態である中、使用者のキー操作によって、なんらかの処理要求を受け付けたら（ステップＳ３）、要求に対応した処理を行う（ステップＳ４）。この処理を本例では通常処理と記載する。通常処理とは、たとえば、通話を開始するように操作されたら、システム制御部４は、例えば通信制御部３、無線部２、音声処理部９など通話に必要な機能を用いて通話を行う。また、アドレス情報を表示させるような要求を受け付けたら、システム制御部４は、メモリ部６から必要なデータを読み出し、表示部８に表示させる。通常処理とは、このような一般的な携帯端末機器の処理のことである。
【００４２】
さらに、待機状態である中で、キー入力部７から電源ＯＦＦ操作を受け付けたら（ステップＳ５）、システム制御部４は、携帯端末機器のＯＦＦ処理を行い、電源を切る（ステップＳ６）。
【００４３】
以上が一般的な携帯端末機器の利用形態である。次に、本発明における正規ユーザー登録処理について記載する。図３に正規ユーザー登録処理のフローを示す。
携帯端末機器１が待機状態であるときに（ステップＳ２）、正規ユーザー登録処理を行うように操作すると（ステップＳ７）、携帯端末機器１は正規ユーザー登録処理に進む（ステップＳ８）。特に携帯端末機器１を新規に使用する場合であれば、この処理を行う必要がある。
【００４４】
以下、ステップＳ８の正規ユーザー登録処理について記載する。ここに記載する正規ユーザー登録とは、個人認証処理を行うための前準備であり、さらに個人認証処理とは、携帯端末機器１を操作している使用者が、正規ユーザーであるのか、あるいは不正に使用しよ

うとしている第三者であるのかを、識別、認証する処理のことである。本発明において、この個人認証処理は幾度となく繰り返し実行されることになるので、本処理の操作の利便性は大変重要な課題である。したがって、高度なセキュリティを保ちつつ、かつ利便性を考慮すると、いわゆる煩雑なパスワード入力などではなく、指を指定の場所に置くだけなどの簡易な操作で認証手続きが実行できる指紋認証技術など用いることが望ましい。

【００４５】

正規ユーザー登録を行う際には、第三者によって容易に登録されることを禁止するため、特別な手法をもって行う。「特別な」とは、第三者が容易に推測、実現できない、複雑な手法のことである。たとえば、長いパスワードを用いてもよいし、携帯端末機器１とは別の端末機器を用意して、これと接続しながらではないと正規ユーザー登録を行えないようにしてもよい。長いパスワードや別の端末機器は、常に携帯端末機器と一緒に携帯しておく必要はないが（逆に、容易な携帯性がないほうが望ましい）、所有者はこのパスワードや別の端末機器をきっちりと管理することが重要である。このように正規ユーザー登録処理は、利便性を犠牲にしたほうが、かえってセキュリティの向上につながる。

【００４６】

具体的には、まず、携帯端末機器１に、上述した特別な手法でもって、現在の携帯端末機器の使用者が正規ユーザーであることを認証させる。次に、個人認証部５から正規ユーザーの指紋データを読み取り、そのデータを正規ユーザーの指紋データとして、メモリに格納する。このメモリは携帯端末機器１のメモリ部６を使用してもよいし、個人認証部５内に別途備えておいてもよい。ただし、携帯端末機器１の電源がＯＦＦされても、正規ユーザー登録情報は記憶し続けるものとする。こうしないと、利便性が著しく低下してしまう。正規ユーザー登録処理が完了すれば、携帯端末機器１の待機状態であるステップＳ２に戻る。

【００４７】

なお、複数の人間が本携帯端末機器１を共有して使用するケースも考えられる。この場合は、最初に正規ユーザーとして登録した人の了解のもと、いわば正規ユーザーが携帯端末機器１の管理者としてふるまい、具体的には上記のような特別な手法を用いて新規に正規ユーザーを追加する。

【００４８】

次に、本発明における正規ユーザーの個人認証機能有効処理について記載する。図４に正規ユーザーの個人認証機能有効処理のフローを示す。

正規ユーザーが、携帯端末機器１が待機状態であるときに（ステップＳ２）、すでに正規ユーザー登録処理が行われていれば、個人認証機能を有効あるいは無効にするように操作すると（ステップＳ９）、携帯端末機器１は個人認証機能有効処理に進む（ステップＳ１０）。個人認証機能有効とは、携帯端末機器の使用者が、登録してある正規ユーザーであることを識別、認証した結果でもって、各種通常処理の動作可否を制御するかどうか選択するフラグ（イネーブル）情報である。この情報も、携帯端末機器１の電源がＯＦＦされても記憶し続けるものとする。なお、本発明では、個人認証機能は有効であるのが前提ではあるが、もちろんこのステップＳ１０でその機能を一時的にＯＦＦにすることも選択できる。

【００４９】

次に、本発明の主旨である個人認証機能が有効である場合の携帯端末機器１の動作について記載する。図５に個人認証機能が有効である場合の処理フローを示す。

一般に、携帯電話などの携帯端末機器は、利便性から、通常は、ステップ２の待機状態で使用されるケースがほとんどである。本例では、図３におけるステップＳ８で、正規ユーザーの登録処理を行っている携帯端末機器１の動作が、ステップＳ２の待機状態であるとして、以下記載する。

【００５０】

ここで、携帯端末機器１の使用者が、キー入力部７から通常処理を行うよう操作すると（ステップＳ３）、システム制御部４は、要求された通常処理を行う際に、個人認証が必要

かどうか判断し、もし必要のない通常処理の要求ならば、ステップＳ４の通常処理を直接実行してもかまわない。すなわち、ここで記載した通常処理とは、セキュリティをかける必要のない処理であり、たとえばカレンダー表示やゲームなどが考えられる。このように各通常処理別に、個人認証が必要かどうかを設定できるようにしておくと、正規ユーザーとして登録されていない第三者でも、図４におけるステップＳ１０で個人認証機能の設定変更を行わずに通常処理を利用できるようになるため、利便性が向上する。

【００５１】

ステップＳ３で、個人認証が必要な通常処理の実行要求があった場合には、図４におけるステップＳ１０で、個人認証機能が有効に設定されているか調べる（ステップＳ１１）。そもそも個人認証機能が有効でない場合では、ステップＳ４の要求された通常処理を行う。しかし、個人認証機能が有効である場合は個人認証処理（ステップＳ１２）に進む。個人認証処理は、携帯端末機器１を使用する際に、第三者の不正利用を防止し、正規ユーザーだけ正しく使用できるよう制御するステップである。ステップＳ１２に進んだときは、要求された通常処理を行うには、個人認証が必要であることを示す情報を表示部８に表示してもよい。

【００５２】

個人認証処理は、まず携帯端末機器１の使用者に、認証部５を使用して使用者の指紋情報を入力させる。つぎに、個人認証部５内で、入力された指紋情報が、あらかじめ図３におけるステップＳ８で正規ユーザーとして登録してある指紋情報と一致するか、比較器などを用いて照合、識別する。識別した結果、正規ユーザーか、あるいは登録していない第三者かの情報（個人認証結果情報）を、認証失敗制御部１１に送る。

【００５３】

この段階で、識別した結果が正規ユーザーのものであれば、ステップＳ４に進んで、要求された通常処理を行うが、もし、登録されていない第三者のものであれば、認証失敗制御部１１は認証失敗情報通知部１３を使用して、通信基地局２０に、認証失敗が発生したことを知らせる認証失敗情報を発信、通知する（ステップＳ１３）。

【００５４】

このとき、認証失敗制御部１１は、一度だけの認証結果から、認証失敗と判断するのではなく、たとえば５回連続で認証に失敗するなど、複数回認証に失敗した時点で初めて認証失敗とみなしてステップＳ１３に進んでもよい。この場合、認証に失敗した回数を認証失敗情報記憶部１２に記憶させておく必要がある。何回認証に失敗すれば認証失敗とみなすのかは、携帯端末機器１の使用者が任意に設定できるものとする。

【００５５】

また、認証失敗とみなしても、この状態をすぐ通信基地局２０に通知することはせず、認証失敗状態であることを記憶しておき、この状態の携帯端末機器１から発信の実行が操作された時に、初めて認証失敗情報を基地局に通知するようにしてもよい。

【００５６】

上記のような、複数回の認証確認後に初めて認証失敗の処理を行うことや、発信制御が行われようとしたときに初めて認証失敗の処理を行うことは、おもに誤作動（意図しない連絡）を防ぐことを目的としている。

【００５７】

たとえば、所有者が、認証失敗情報が通信基地局２０に連絡されることなど意図せず、ただ単に携帯端末機器１に格納している情報を知人に見せようとして、同機を手渡す場合などが考えられるが、このときでも、いきなり認証失敗、即通知では、通知する基地局側に負荷がかかる。また、所有者側にも必要ない情報が連絡されることになり、利便性が損なわれてしまう。

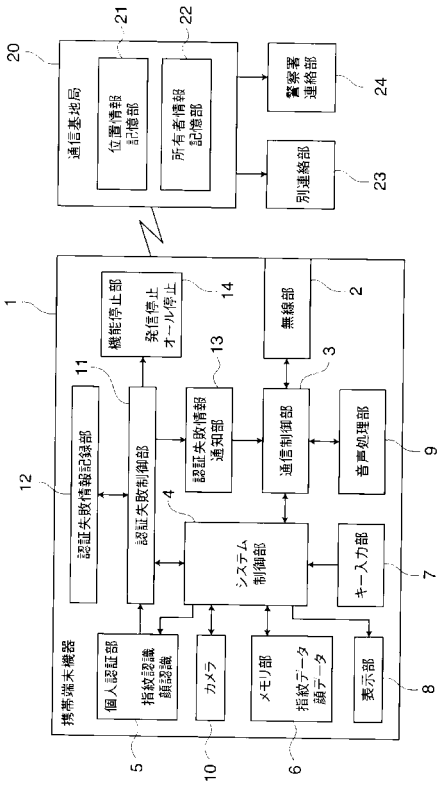
【００５８】

認証失敗と判断した認証失敗制御部１１は、認証失敗情報通知部１３に対して通信基地局２０へ向け、認証失敗情報を通知するよう要求を出力する。認証失敗情報通知部１３は、携帯端末機器１の使用者の操作に関わらず、通信（発信）に必要な機能、すなわち通信制

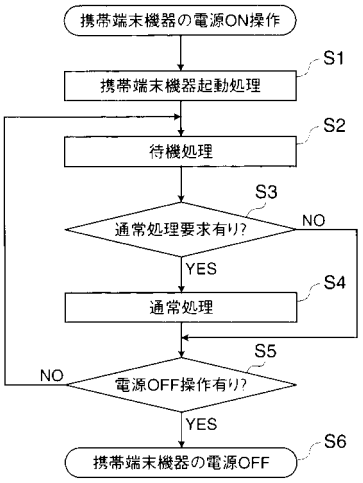
御部３を用いてその情報を通信基地局２０側に通知する。
【００５９】
また、認証失敗制御部１１は、認証失敗と判断したら、携帯端末機器１の一部あるいはすべての機能を制限する、いわゆるロック処理を行ってもよい（ステップＳ１４）。
【００６０】
まず、携帯端末機器１にあらかじめ、認証失敗情報を受け付けた場合、すなわち携帯端末機器１が第三者に不正に使用されようとしていると考えられた場合、携帯端末機器１にどのような機能制限を行うか設定しておく（不図示）。ここで述べる機能制限とは、携帯端末機器１が不正使用されないように、例えば、勝手に通信されないように通信制御部３の動作を停止させたり、メモリ部６の内容を閲覧されないようにしておいたりすることである。機能停止部１４は、認証失敗制御部１１から認証失敗情報を受け付けたら、設定されている上記情報に基づき携帯端末機器１のロックを行う。
【００６１】
たとえば、通常処理４に含まれる通話機能や、アドレス表示機能などの機能をロック（使用できない）するようにする。さらに、この情報を表示部８に表示してもよい。この制御によって、携帯端末機器１が不正使用される前に、確実に即時性をもって携帯端末機器の不正使用を防止することができる。
【００６２】
以下、認証失敗情報を受け取った通信基地局側２０の処理フローを図６に記載する。図５のステップＳ１３で発信された認証失敗情報を受信した通信基地局２０は（ステップＳ１５）、事前に所有者情報記憶部２２に登録してある所有者情報を参照して、携帯端末機器１とは別の別連絡部２３でもって、所有者に認証失敗情報を通知する（ステップＳ１６）。このため、正規ユーザーは紛失、盗難などの発生情報を、即時性をもって得ることができる。また、認証失敗情報を所有者に通知するさいに、位置情報記憶部２１に記憶した通信基地局２０の位置情報を付加してもよい。こうしておけば、紛失した携帯端末機器１の位置情報がわかるため、所有者は携帯端末機器１がどこにあるか、見つけやすくなる効果が得られる。また、単なる紛失ではなく、第三者による盗難かどうかの判断材料のひとつにもなる。
【００６３】
なお、よりセキュリティの向上のため、認証失敗情報を受け付けたら、警察署連絡部２４により（ステップＳ１７）、警察署に通知してもよい（ステップＳ１８）。この警察署へ通知をするか否かは、基本的に携帯端末機器１の正規ユーザーが設定できるようにしておく。また、いつでもその設定を変更できるようにしておく。もし警察署への連絡が必要なければ、通信基地局２０側にそのように設定をしておくこともできる。
【００６４】
このようにして、携帯端末機器に個人認証の機能を設けることにより、盗難や紛失によって第三者の手に渡った携帯端末機器の第三者による不正使用を防止することができる。
【００６５】
【発明の効果】
本発明によれば、携帯端末機器が盗難や紛失により第三者の手に渡った場合でも、第三者による不正使用を確実に防止することができる。また、即時性を持った情報が通信基地局から得られるため、盗難や紛失の発生を正規ユーザーが速やかに知ることができる。さらに、この情報に通信基地局の位置情報が含まれていれば、紛失した携帯端末機器を探す手がかりになり、紛失か盗難かの判断材料とすることができる。
【図面の簡単な説明】
【図１】本発明の個人認証機能付き携帯端末機器システムの構成を示すブロック図である。
【図２】実施形態における携帯端末機器の基本動作状態を示すフローチャートである。
【図３】実施形態における携帯端末機器の正規ユーザー登録処理を示すフローチャートである。

【図４】実施形態における携帯端末機器の個人認証機能有効処理を示すフローチャートである。
【図５】実施形態における携帯端末機器の個人認証機能を用いた処理を示すフローチャートである。
【図６】実施形態における通信基地局側の処理を示すフローチャートである。
【図７】実施形態における通信基地局側の所有者情報の一例である。
【図８】従来例における携帯端末機器のシステム構成図である。
【符号の説明】
１　携帯端末機器
２　無線部
３　通信制御部
４　システム制御部
５　個人認証部
６　メモリ部
７　キー入力部
８　表示部
９　音声処理部
１０　カメラ
１１　認証失敗制御部
１２　認証失敗情報記録部
１３　認証失敗情報通知部
１４　機能停止部
２０　通信基地局
２１　位置情報記憶部
２２　所有者情報記憶部
２３　別連絡部
２４　警察署連絡部

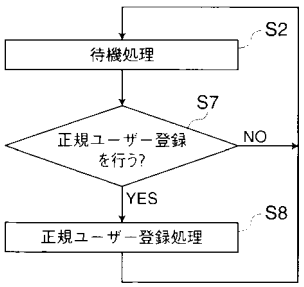
【図１】



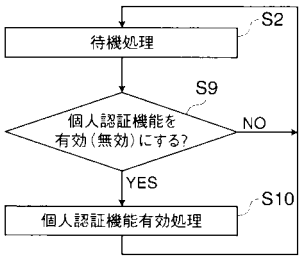
【図２】



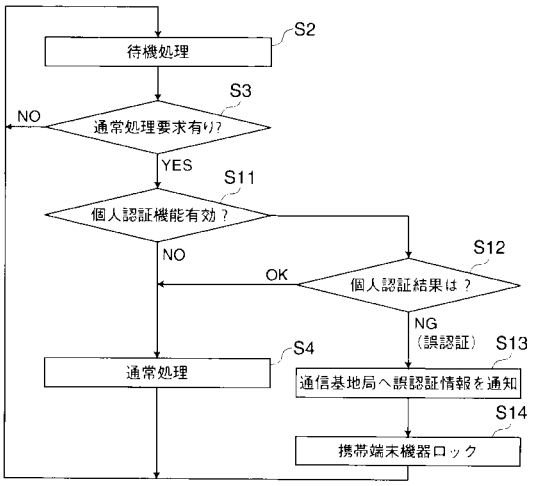
【図３】



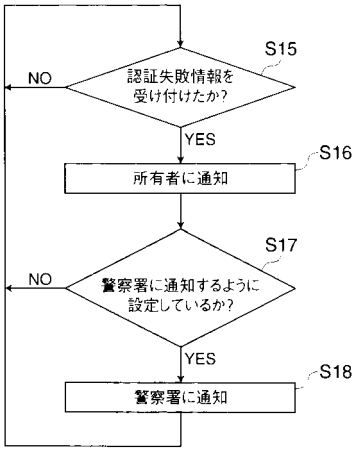
【図４】



【図５】



【図６】



【図７】

ID	01234567
氏名	○○ ××
携帯端末機器連絡番号	090-XXXX-XXXX
緊急連絡先	奈良県大和郡山市XX町XX
別連絡部の連絡番号	0743-XX-XXXX
最新通話(受信)時間	20XX/XX/XX XXhXXmXXs
認証失敗情報受信時間	20XX/XX/XX XXhXXmXXs

【図８】