

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4165452号  
(P4165452)

(45) 発行日 平成20年10月15日(2008.10.15)

(24) 登録日 平成20年8月8日(2008.8.8)

(51) Int.Cl.		F I	
<b>HO4M</b>	<b>1/675</b>	<b>(2006.01)</b>	HO4M 1/675
<b>HO4Q</b>	<b>7/38</b>	<b>(2006.01)</b>	HO4Q 7/00 183
			HO4Q 7/00 184

請求項の数 10 (全 16 頁)

(21) 出願番号	特願2004-154022 (P2004-154022)	(73) 特許権者	000004237
(22) 出願日	平成16年5月25日 (2004.5.25)		日本電気株式会社
(65) 公開番号	特開2005-340976 (P2005-340976A)		東京都港区芝五丁目7番1号
(43) 公開日	平成17年12月8日 (2005.12.8)	(74) 代理人	100085235
審査請求日	平成19年4月23日 (2007.4.23)		弁理士 松浦 兼行
		(72) 発明者	片柳 健志
			東京都港区芝5丁目7番1号 日本電気株式会社内
		審査官	吉村 伊佐雄

最終頁に続く

(54) 【発明の名称】 携帯通信端末及びその情報管理方法

(57) 【特許請求の範囲】

【請求項1】

着脱自在なICカードが装着されたとき、そのICカードに記録された固有情報に基づき、環境設定を行って発着信動作が可能とされる携帯通信端末であって、

前記ICカードに記録された固有情報に対応付けて認証用情報及び通信に関連する個別管理情報を記憶する記憶手段と、

装着された前記ICカードが、前記記憶手段に前記固有情報が予め登録されているICカードであるかどうか判定する第1の判定手段と、

前記第1の判定手段により登録されていないICカードであると判定されたときには、予め定められた所定の操作のみ可能で、通常の出着信動作を制限する制限モードに設定すると共に、携帯通信端末管理者へ失敗通知を発信する第1の設定手段と、

前記第1の判定手段により登録されているICカードであると判定されたときには、前記携帯通信端末管理者へ成功通知を発信する成功通知手段と、

前記第1の判定手段により登録されているICカードであると判定されたときには、そのICカードの前記固有情報に対応付けて前記個別管理情報が、前記記憶手段に登録されているかどうか判定する第2の判定手段と、

前記第2の判定手段により前記個別管理情報が登録されていないと判定されたときには、前記記憶手段に記憶されている前記個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モードに設定する第2の設定手段と、

前記第2の判定手段により前記個別管理情報が登録されていると判定されたときには、

10

20

該個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定する第3の設定手段と

を有することを特徴とする携帯通信端末。

【請求項2】

前記第1の判定手段により登録されていないICカードであると判定されたときには、携帯通信端末管理者へ失敗通知を発信する第1の発信手段と、該失敗通知を受信した該携帯通信端末管理者が遠隔操作により予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードに設定する第1の遠隔操作手段とを、前記第1の設定手段に替えて設けると共に、前記第1の判定手段により登録されているICカードであると判定され、かつ、前記第2の判定手段により前記個別管理情報が登録されていないと判定されたときは、前記成功通知を受信した前記携帯通信端末管理者が遠隔操作により前記一般モードに設定する第2の遠隔操作手段を、前記第2の設定手段に替えて設け、前記第1の判定手段により登録されているICカードであると判定され、かつ、前記第2の判定手段により前記個別管理情報が登録されていると判定されたときには、前記成功通知を受信した前記携帯通信端末管理者が遠隔操作により前記ユーザ別モードに設定する第3の遠隔操作手段を、前記第3の設定手段に替えて設けたことを特徴とする請求項1記載の携帯通信端末。

10

【請求項3】

着脱自在なICカードが装着されたとき、そのICカードに記録された固有情報に基づき、環境設定を行って発着信動作が可能とされる携帯通信端末であって、

20

前記ICカードに記録された固有情報に対応付けて認証用情報及び通信に関連する個別管理情報を記憶する記憶手段と、

装着された前記ICカードが、前記記憶手段に前記固有情報が予め登録されているICカードであるかどうか判定する第1の判定手段と、

前記第1の判定手段により登録されていないICカードであると判定されたときには、予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードとする制限モード設定手段と、

前記制限モードにおいて装着された前記ICカードの登録認証を行い、認証が成功したときは、該装着されたICカードの固有情報を前記記憶手段に記憶する第1の認証手段と

30

、前記第1の認証手段により認証が失敗したときに、携帯通信端末管理者へ失敗通知を発信する失敗通知手段と、

前記第1の判定手段により登録されているICカードであると判定されたとき、又は前記第1の認証手段により認証が成功したときは、前記携帯通信端末管理者へ成功通知を発信する成功通知手段と、

前記第1の判定手段により登録されているICカードであると判定されたとき、又は前記第1の認証手段により認証が成功したときは、前記記憶手段に記憶されている前記個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モードに設定する一般モード設定手段と

を有することを特徴とする携帯通信端末。

40

【請求項4】

前記第1の判定手段により登録されているICカードであると判定されたとき、又は前記第1の認証手段により認証が成功したときは、前記記憶手段に、認証が成功したICカードに記録された固有情報に対応付けて前記個別管理情報が記憶されているか否か判定し、前記個別管理情報が記憶されていないと判定されたときには、前記一般モード設定手段により前記一般モードに設定させる第2の判定手段と、前記第2の判定手段により、前記装着されたICカードの固有情報に対応付けて前記個別管理情報が前記記憶手段に記憶されていると判定されたときには、該個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定するユーザ別モード設定手段とを更に有することを特徴とする請求項3記載の携帯通信端末。

50

## 【請求項 5】

前記一般モード設定手段により設定された前記一般モードにおいて、前記装着された IC カードの固有情報に対応付けた前記個別管理情報が前記記憶手段に記憶されているか否かの認証を行い、認証が成功したときは前記ユーザ別モード設定手段によりユーザ別モードに設定させる第 2 の認証手段を更に有することを特徴とする請求項 4 記載の携帯通信端末。

## 【請求項 6】

着脱自在な IC カードが装着されたとき、その IC カードに記録された固有情報に基づき、環境設定を行って発着信動作が可能とされると共に、前記固有情報に対応付けて認証用情報及び通信に関連する個別管理情報が記憶手段に予め記憶されている携帯通信端末の情報管理方法であって、

装着された前記 IC カードの固有情報が、前記記憶手段に予め登録されているかどうか判定する第 1 のステップと、

前記第 1 のステップにより装着された IC カードの固有情報が登録されていないと判定されたときには、予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードに設定すると共に、携帯通信端末管理者へ失敗通知を発信する第 2 のステップと、

前記第 1 のステップにより装着された IC カードの固有情報が登録されていると判定されたときには、前記携帯通信端末管理者へ成功通知を発信する第 3 のステップと、

前記第 1 のステップにより装着された IC カードの固有情報が登録されていると判定されたときには、その IC カードの前記固有情報に対応付けて前記個別管理情報が、前記記憶手段に登録されているかどうか判定する第 4 のステップと、

前記第 4 のステップにより装着された IC カードの前記個別管理情報が登録されていないと判定されたときには、前記記憶手段に記憶されている前記個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モードに設定する第 5 のステップと、

前記第 4 のステップにより装着された IC カードの前記個別管理情報が登録されていると判定されたときには、該個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定する第 6 のステップと

を含むことを特徴とする携帯通信端末の情報管理方法。

## 【請求項 7】

前記第 1 のステップにより装着された IC カードの固有情報が登録されていないと判定されたときには、携帯通信端末管理者へ失敗通知を発信する第 7 のステップと、該失敗通知を受信した該携帯通信端末管理者が遠隔操作により予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードに設定する第 8 のステップとを、前記第 2 のステップに替えて設けると共に、前記第 1 のステップにより装着された IC カードの固有情報が登録されていると判定され、かつ、前記第 4 のステップにより前記個別管理情報が登録されていないと判定されたときには、前記成功通知を受信した前記携帯通信端末管理者が遠隔操作により前記一般モードに設定する第 9 のステップを、前記第 5 のステップに替えて設け、前記第 1 のステップにより装着された IC カードの固有情報が登録されていると判定され、かつ、前記第 4 のステップにより前記個別管理情報が登録されていると判定されたときには、前記成功通知を受信した前記携帯通信端末管理者が遠隔操作により前記ユーザ別モードに設定する第 10 のステップを、前記第 6 のステップに替えて設けたことを特徴とする請求項 6 記載の携帯通信端末の情報管理方法。

## 【請求項 8】

着脱自在な IC カードが装着されたとき、その IC カードに記録された固有情報に基づき、環境設定を行って発着信動作が可能とされると共に、前記固有情報に対応付けて認証用情報及び通信に関連する個別管理情報が記憶手段に予め記憶されている携帯通信端末の情報管理方法であって、

装着された前記 IC カードの固有情報が、前記記憶手段に予め登録されているかどうか

10

20

30

40

50

判定する第 1 のステップと、

前記第 1 のステップにより装着された IC カードの固有情報が登録されていないと判定されたときには、予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードに設定する第 2 のステップと、

前記制限モードにおいて装着された前記 IC カードの登録認証を行い、認証が成功したときは、該装着された IC カードの固有情報を前記記憶手段に記憶する第 3 のステップと、

前記第 3 のステップにより認証が失敗したときに、携帯通信端末管理者へ失敗通知を発信する第 4 のステップと、

前記第 1 のステップにより装着された IC カードの固有情報が登録されていると判定されたとき、又は前記第 3 のステップにより認証が成功したときは、前記携帯通信端末管理者へ成功通知を発信する第 5 のステップと、

前記第 1 のステップにより装着された IC カードの固有情報が登録されていると判定されたとき、又は前記第 3 のステップにより認証が成功したときは、前記記憶手段に記憶されている前記個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モードに設定する第 6 のステップと

を含むことを特徴とする携帯通信端末の情報管理方法。

#### 【請求項 9】

前記第 1 のステップにより装着された IC カードの固有情報が登録されていると判定されたとき、又は前記第 3 のステップにより認証が成功したときは、前記記憶手段に、認証が成功した IC カードに記録された固有情報に対応付けて前記個別管理情報が記憶されているか否か判定し、前記個別管理情報が記憶されていないと判定されたときには、前記第 6 のステップにより前記一般モードに設定させる第 7 のステップと、前記第 7 のステップにより、前記装着された IC カードの固有情報に対応付けて前記個別管理情報が前記記憶手段に記憶されていると判定されたときには、該個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定する第 8 のステップとを更に含むことを特徴とする請求項 8 記載の携帯通信端末の情報管理方法。

#### 【請求項 10】

前記一般モードにおいて、前記装着された IC カードの固有情報に対応付けた前記個別管理情報が前記記憶手段に記憶されているか否かの認証を行い、認証が成功したときは前記第 8 のステップによりユーザ別モードに設定させる第 9 のステップを更に含むことを特徴とする請求項 9 記載の携帯通信端末の情報管理方法。

#### 【発明の詳細な説明】

#### 【技術分野】

#### 【0001】

本発明は携帯通信端末及びその情報管理方法に係り、特に加入者識別モジュール (SIM:Subscriber Identity Module) カードや次世代の加入者識別モジュール (USIM:Universal Subscriber Identity Module) カードなどの電話番号が登録された IC カードを装着することで発着信動作を行う携帯通信端末及びその携帯通信端末の情報管理方法に関する。

#### 【背景技術】

#### 【0002】

携帯電話機、PHS(Personal Handy phone System)、PDA(Personal Digital Assistants:個人向け携帯型情報通信機器)等の携帯端末装置で、通信機能を持ち、情報を管理することが可能な携帯通信端末の中には、加入者の電話番号等の電話に関する情報を、端末に対して着脱自在なSIMカードあるいはUSIMカードに書き込んでおき、そのSIM/USIMカードを携帯通信端末に装着して初めて発着信可能な状態となり、相手端末との通信が可能となる携帯通信端末が知られている。上記のSIMカードは、ヨーロッパで規格化されたGSM(Global System for Mobile communication)の携帯通信端末

10

20

30

40

50

で着脱することが定められたICカードであり、上記のUSIMカードは、第3世代携帯電話の規格のIMT-2000(International Mobile Telecommunication System 2000)で着脱することが定められたICカードである。

【0003】

このような携帯通信端末では、どのSIM/USIMカードが装着されても発着信可能であるため、1人のユーザが1台の携帯通信端末と複数のSIM/USIMカードを所有して、SIM/USIMカードを差し替えることで1台の携帯通信端末をビジネス用とプライベート用などの使い分けが可能となり、あるいは、複数のユーザが各々自分専用のSIM/USIMカードを所有している場合は、携帯通信端末が1台しかなくても、自分専用のSIM/USIMカードを携帯通信端末に装着することにより、通信可能となるので、1台の携帯通信端末を複数のユーザが共用することが可能となり、利便性を向上できる。

10

【0004】

しかしながら、SIM/USIMカードが第三者の手に渡ると、SIM/USIMカードを別の携帯通信端末に入れ替えて装着することで、別の携帯通信端末を使用した通信が可能となってしまう、また、SIM/USIMカードが廃棄されてしまうと、そのSIM/USIMカードに記憶されていた情報が失われてしまう。また、SIM/USIMカードの入れ替えにより、電話番号が変更されるので、本来の所有者が操作ロック用の制御信号を送っても、携帯通信端末を操作ロックすることができない。

【0005】

そこで、SIMカードを携帯通信端末に装着したときに、携帯通信端末がSIMカードから識別コード番号と通報先電話番号とを入力し、識別コード番号がデータ入力手段からのデータと比較されて一致と判定されると、SIMカードの内部情報が読み出され、不一致と判定されると、SIMカードの通報先電話番号を選択して通報先端末に自動的に接続し、SIMカードの内部情報をこの携帯通信端末で表示することなく通報先端末に送信してからSIMカードの内部情報を削除するようにしたセキュリティ方法が知られている(例えば、特許文献1参照)。このセキュリティ方法によれば、SIMカードが盗難等により第三者に使用されたときには、通報先端末に自動的にそのSIMカードの内部情報が転送されるため、内部情報を取得できると共に、そのSIMカードが装着された携帯通信端末は内部情報が表示されずに不正使用を防止できる。

20

30

【0006】

また、SIM/USIMカードが携帯通信端末に装着された際に、SIM/USIMカードからそのカードを識別するための特定の情報を読み出すカード情報読み出し手段と、このカード情報読み出し手段によってSIM/USIMカードから読み出された上記の特定の情報に基づいて当該カードの正当性を判断し、その判断結果に応じて発着信動作を含む端末動作を制御する動作制御手段を具備した携帯通信端末も従来より知られている(例えば、特許文献2参照)。この従来の携帯通信端末によれば、他人によるSIM/USIMカードの使用などで、SIM/USIMカードの正当性が認められなかった場合には、発着信動作を含む端末動作を禁止できる。

【0007】

更に、従来、ICカードの差し替えで複数の電話機を使用する場合、ICカードにカード電話帳データの各電話番号毎の使用回数データ又は最新使用日データの少なくともいずれか一方を記憶することにより、そのICカードを介して一方のカード式電話機で使用した電話番号及び使用履歴を他方のカード式電話機でも使用できるようにした通信端末も知られている(例えば特許文献3参照)。

40

【0008】

【特許文献1】特開2003-264631号公報

【特許文献2】特開2004-064657号公報

【特許文献3】特開2004-088235号公報

【発明の開示】

50

**【発明が解決しようとする課題】****【0009】**

しかるに、上記のSIM/USIMカードが装着されることで発着信動作を行う携帯通信端末では、電話帳データやメールのデータ等の個人情報は、依然として主に携帯通信端末本体へ記録されるため、その携帯通信端末を他人に貸与する場合には、そのデータを消去または秘匿する必要がある。

**【0010】**

また、その携帯通信端末を借用した側としても、返却する場合には自分が使用したデータを端末本体から消去するなどの作業をしなければならず、例えば身内や社用として貸し借りを繰り返したい場合などに非常に手間がかかることになり、折角の利便性を損なっている。更に、ある程度大規模な組織で、そのような運用を行った場合に、今現在、誰が使用しているかを確認することが困難である。

10

**【0011】**

前記特許文献1及び2記載の従来の携帯通信端末では、SIM/USIMカードの不正使用を防止するものであり、上記のように携帯通信端末を本来の使用人と第三者との間で正規に貸し借りする場合には適用できない。更に、前記特許文献3記載のものは、ICカードに携帯電話で使用した電話番号及びその使用履歴に関するデータを記憶させることにより、複数台のカード式電話機を共用できるようにしたものであり、1台の携帯通信端末を複数のユーザ(加入者)が共用するものではない。

**【0012】**

本発明は以上の点に鑑みなされたもので、端末本体に記憶された個人情報を他人から簡単に秘匿し得る携帯通信端末及びその情報管理方法を提供することを目的とする。

20

**【0013】**

また、本発明の他の目的は、その所在を容易に明らかにし得る携帯通信端末及びその情報管理方法を提供することにある。

**【課題を解決するための手段】****【0014】**

上記の目的を達成するため、第1の発明の携帯通信端末は、着脱自在なICカードが装着されたとき、そのICカードに記録された固有情報に基づき、環境設定を行って発着信動作が可能とされる携帯通信端末であって、ICカードに記録された固有情報に対応付けて認証用情報及び通信に関連する個別管理情報を記憶する記憶手段と、装着されたICカードが、記憶手段に固有情報が予め登録されているICカードであるかどうか判定する第1の判定手段と、第1の判定手段により登録されていないICカードであると判定されたときには、予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードに設定すると共に、携帯通信端末管理者へ失敗通知を発信する第1の設定手段と、第1の判定手段により登録されているICカードであると判定されたときには、携帯通信端末管理者へ成功通知を発信する成功通知手段と、第1の判定手段により登録されているICカードであると判定されたときには、そのICカードの固有情報に対応付けて個別管理情報が、記憶手段に登録されているかどうか判定する第2の判定手段と、第2の判定手段により個別管理情報が登録されていないと判定されたときには、記憶手段に記憶されている個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モードに設定する第2の設定手段と、第2の判定手段により個別管理情報が登録されていると判定されたときには、個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定する第3の設定手段とを有する構成としたものである。

30

40

**【0015】**

この発明では、ICカードを入れ替えた時に、その携帯通信端末の管理者に対して失敗通知又は成功通知を行うようにしたため、携帯通信端末の現在の使用者をICカードの固有情報に基づき携帯通信端末の管理者に把握させることができる。また、この発明では、装着されたICカードが、携帯通信端末内の記憶手段に、その固有情報に対応付けて個別管理情報が記録されている場合に限り、個別管理情報に応じた機能の動作を可能とするユ

50

ーザ別モードに設定し、それ以外は個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モード、又は予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードに設定するようにできる。

【0016】

また、上記の目的を達成するため、第2の発明の携帯通信端末は、第1の判定手段により登録されていないICカードであると判定されたときには、携帯通信端末管理者へ失敗通知を発信する第1の発信手段と、失敗通知を受信した携帯通信端末管理者が遠隔操作により予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードに設定する第1の遠隔操作手段とを、第1の設定手段に替えて設けると共に、第1の判定手段により登録されているICカードであると判定され、かつ、第2の判定手段により個別管理情報が登録されていないと判定されたときには、成功通知を受信した携帯通信端末管理者が遠隔操作により一般モードに設定する第2の遠隔操作手段を、第2の設定手段に替えて設け、第1の判定手段により登録されているICカードであると判定され、かつ、第2の判定手段により個別管理情報が登録されていると判定されたときには、成功通知を受信した携帯通信端末管理者が遠隔操作によりユーザ別モードに設定する第3の遠隔操作手段を、第3の設定手段に替えて設けたことを特徴とする。この発明では、携帯通信端末管理者の遠隔操作により制限モード、一般モード又はユーザ別モードに設定することができる。

10

【0017】

また、上記の目的を達成するため、第3の発明の携帯通信端末は、着脱自在なICカードが装着されたとき、そのICカードに記録された固有情報に基づき、環境設定を行って発着信動作が可能とされる携帯通信端末であって、ICカードに記録された固有情報に対応付けて認証用情報及び通信に関連する個別管理情報を記憶する記憶手段と、装着されたICカードが、記憶手段に固有情報が予め登録されているICカードであるかどうか判定する第1の判定手段と、第1の判定手段により登録されていないICカードであると判定されたときには、予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードとする制限モード設定手段と、制限モードにおいて装着されたICカードの登録認証を行い、認証が成功したときは、装着されたICカードの固有情報を記憶手段に記憶する第1の認証手段と、第1の認証手段により認証が失敗したときに、携帯通信端末管理者へ失敗通知を発信する失敗通知手段と、第1の判定手段により登録されているICカードであると判定されたとき、又は第1の認証手段により認証が成功したときは、携帯通信端末管理者へ成功通知を発信する成功通知手段と、第1の判定手段により登録されているICカードであると判定されたとき、又は第1の認証手段により認証が成功したときは、記憶手段に記憶されている個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モードに設定する一般モード設定手段とを有する構成としたものである。

20

30

【0018】

この発明では、ICカードを入れ替えた時に、その携帯通信端末の管理者に対して失敗通知又は成功通知を行うようにしたため、携帯通信端末の現在の使用者をICカードの固有情報に基づき携帯通信端末の管理者に把握させることができる。また、この発明では、装着されたICカードが記憶手段に登録されているICカードであると判定されたとき、又は制限モードにおいて装着されたICカードの登録認証が成功したときは、個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モードに設定することができる。

40

【0019】

また、上記の目的を達成するため、第4の発明の携帯通信端末は、第3の発明の第1の判定手段により登録されているICカードであると判定されたとき、又は第1の認証手段により認証が成功したときは、記憶手段に、認証が成功したICカードに記録された固有情報に対応付けて個別管理情報が記憶されているか否か判定し、個別管理情報が記憶されていないと判定されたときには、一般モード設定手段により一般モードに設定させる第2

50

の判定手段と、第2の判定手段により、装着されたICカードの固有情報に対応付けて個別管理情報が記憶手段に記憶されていると判定されたときには、個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定するユーザ別モード設定手段とを更に有することを特徴とする。

**【0020】**

この発明では、装着されたICカードが記憶手段に登録されているICカードであると判定されたとき、又は制限モードにおいて装着されたICカードの登録認証が成功したときは、装着されたICカードの固有情報に対応付けて個別管理情報が記憶手段に記憶されていると判定されたときに限り、個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定することができる。

10

**【0021】**

また、上記の目的を達成するため、第5の発明の携帯通信端末は、第4の発明の一般モード設定手段により設定された一般モードにおいて、装着されたICカードの固有情報に対応付けた個別管理情報が記憶手段に記憶されているか否かの認証を行い、認証が成功したときはユーザ別モード設定手段によりユーザ別モードに設定させる第2の認証手段を更に有することを特徴とする。この発明では、一般モードで動作していても、認証が成功したときには、ユーザ別モードに設定を切り替えることができる。

**【0022】**

また、上記の目的を達成するため、第6の発明の携帯通信端末の情報管理方法は、着脱自在なICカードが装着されたとき、そのICカードに記録された固有情報に基づき、環境設定を行って発着信動作が可能とされると共に、固有情報に対応付けて認証用情報及び通信に関連する個別管理情報が記憶手段に予め記憶されている携帯通信端末の情報管理方法であって、装着されたICカードの固有情報が、記憶手段に予め登録されているかどうか判定する第1のステップと、第1のステップにより装着されたICカードの固有情報が登録されていないと判定されたときには、予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードに設定すると共に、携帯通信端末管理者へ失敗通知を発信する第2のステップと、第1のステップにより装着されたICカードの固有情報が登録されていると判定されたときには、携帯通信端末管理者へ成功通知を発信する第3のステップと、第1のステップにより装着されたICカードの固有情報が登録されていると判定されたときには、そのICカードの固有情報に対応付けて個別管理情報が、記憶手段に登録されているかどうか判定する第4のステップと、第4のステップにより装着されたICカードの個別管理情報が登録されていないと判定されたときには、記憶手段に記憶されている個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モードに設定する第5のステップと、第4のステップにより装着されたICカードの個別管理情報が登録されていると判定されたときには、個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定する第6のステップとを含むことを特徴とする。

20

30

**【0023】**

この発明では、ICカードを入れ替えた時に、その携帯通信端末の管理者に対して失敗通知又は成功通知を行うようにしたため、携帯通信端末の現在の使用者をICカードの固有情報に基づき携帯通信端末の管理者に把握させることができる。また、この発明では、装着されたICカードが、携帯通信端末内の記憶手段に、その固有情報に対応付けて個別管理情報が記録されている場合に限り、個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定し、それ以外は個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モード、又は予め定められた所定の操作のみ可能で、通常の発着信動作を制限する制限モードに設定するようである。

40

**【0024】**

また、上記の目的を達成するため、第7の発明の携帯通信端末の情報管理方法は、第1のステップにより装着されたICカードの固有情報が登録されていないと判定されたときには、携帯通信端末管理者へ失敗通知を発信する第7のステップと、失敗通知を受信した携帯通信端末管理者が遠隔操作により予め定められた所定の操作のみ可能で、通常の発着

50



信動作を制限する制限モードに設定する第8のステップとを、第6の発明の第2のステップに替えて設けると共に、第1のステップにより装着されたICカードの固有情報が登録されていると判定され、かつ、第4のステップにより個別管理情報が登録されていないと判定されたときには、成功通知を受信した携帯通信端末管理者が遠隔操作により一般モードに設定する第9のステップを、第6の発明の第5のステップに替えて設け、第1のステップにより装着されたICカードの固有情報が登録されていると判定され、かつ、第4のステップにより個別管理情報が登録されていると判定されたときには、成功通知を受信した携帯通信端末管理者が遠隔操作によりユーザ別モードに設定する第10のステップを、第6のステップに替えて設けたことを特徴とする。この発明では、携帯通信端末管理者の遠隔操作により制限モード、一般モード又はユーザ別モードに設定することができる。

10

**【0025】**

また、上記の目的を達成するため、第8の発明の携帯通信端末の情報管理方法は着脱自在なICカードが装着されたとき、そのICカードに記録された固有情報に基づき、環境設定を行って発着信動作が可能とされると共に、固有情報に対応付けて認証用情報及び通信に関連する個別管理情報が記憶手段に予め記憶されている携帯通信端末の情報管理方法であって、装着されたICカードの固有情報が、記憶手段に予め登録されているかどうか判定する第1のステップと、第1のステップにより装着されたICカードの固有情報が登録されていないと判定されたときには、予め定められた所定の操作のみ可能で、通常が発着信動作を制限する制限モードに設定する第2のステップと、制限モードにおいて装着されたICカードの登録認証を行い、認証が成功したときは、装着されたICカードの固有情報を記憶手段に記憶する第3のステップと、第3のステップにより認証が失敗したときに、携帯通信端末管理者へ失敗通知を発信する第4のステップと、第1のステップにより装着されたICカードの固有情報が登録されていると判定されたとき、又は第3のステップにより認証が成功したときは、携帯通信端末管理者へ成功通知を発信する第5のステップと、第1のステップにより装着されたICカードの固有情報が登録されていると判定されたとき、又は第3のステップにより認証が成功したときは、記憶手段に記憶されている個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モードに設定する第6のステップとを含むことを特徴とする。

20

**【0026】**

この発明では、ICカードを入れ替えた時に、その携帯通信端末の管理者に対して失敗通知又は成功通知を行うようにしたため、携帯通信端末の現在の使用者をICカードの固有情報に基づき携帯通信端末の管理者に把握させることができる。また、この発明では、装着されたICカードが記憶手段に登録されているICカードであると判定されたとき、又は制限モードにおいて装着されたICカードの登録認証が成功したときは、個別管理情報の閲覧・操作機能を除く他のすべての機能を自由に使用することが可能な一般モードに設定することができる。

30

**【0027】**

また、上記の目的を達成するため、第9の発明の携帯通信端末の情報管理方法は、第8の発明の第1のステップにより装着されたICカードの固有情報が登録されていると判定されたとき、又は第3のステップにより認証が成功したときは、記憶手段に、認証が成功したICカードに記録された固有情報に対応付けて個別管理情報が記憶されているか否か判定し、個別管理情報が記憶されていないと判定されたときには、第6のステップにより一般モードに設定させる第7のステップと、第7のステップにより、装着されたICカードの固有情報に対応付けて個別管理情報が記憶手段に記憶されていると判定されたときには、個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定する第8のステップとを更に含むことを特徴とする。

40

**【0028】**

この発明では、装着されたICカードが記憶手段に登録されているICカードであると判定されたとき、又は制限モードにおいて装着されたICカードの登録認証が成功したときは、装着されたICカードの固有情報に対応付けて個別管理情報が記憶手段に記憶され

50

ていると判定されたときに限り、個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定することができる。

【 0 0 2 9 】

更に、上記の目的を達成するため、第 1 0 の発明の携帯通信端末の情報管理方法は、一般モードにおいて、装着された IC カードの固有情報に対応付けた個別管理情報が記憶手段に記憶されているか否かの認証を行い、認証が成功したときは第 8 のステップによりユーザ別モードに設定させる第 9 のステップを第 9 の発明に更に含むことを特徴とする。この発明では、一般モードで動作していても、認証が成功したときには、ユーザ別モードに設定を切り替えることができる。

【 発明の効果 】

10

【 0 0 3 0 】

本発明によれば、IC カードを入れ替えた時に、その携帯通信端末の管理者に対して失敗通知又は成功通知を行うことにより、携帯通信端末の現在の使用者を IC カードの固有情報に基づき携帯通信端末の管理者が把握・管理できるようにしたため、携帯通信端末の管理者は現在の携帯通信端末の所在を管理できると共に、盗用等の不正使用をも把握することができる。

【 0 0 3 1 】

また、本発明によれば、装着された IC カードが記憶手段に登録されている IC カードであると判定されたとき、又は制限モードにおいて装着された IC カードの登録認証が成功したときは、装着された IC カードの固有情報に対応付けて個別管理情報が記憶手段に記憶されていると判定されたときに限り、個別管理情報に応じた機能の動作を可能とするユーザ別モードに設定することで、自分固有の個別管理情報は記憶手段に記憶されていても他のユーザが閲覧・操作できないようにしたため、ユーザが自分の IC カードを抜いて他のユーザに携帯通信端末を貸与したり、他のユーザが使用した携帯通信端末を借用する場合のいずれにおいても、携帯通信端末の記憶手段から自分又は他人の個別管理情報を消去するなどの操作を行わなくてよく、手間が省け、使い勝手を従来よりも大幅に向上することができる。

20

【 0 0 3 2 】

また、本発明によれば、社用や身内での貸し借りなどの、複数の人が同一の携帯通信端末を使用する場合に、個人情報保護や各々の設定を保持することができる。

30

【 発明を実施するための最良の形態 】

【 0 0 3 3 】

次に、本発明の実施の形態について図面と共に説明する。図 1 は本発明になる携帯通信端末の一実施の形態のブロック図を示す。図 1 に示す実施の形態は、SIM / USIM カード（すなわち、IC カード）が IC カード挿入部 1 0 に着脱自在な携帯電話機であり、最寄りの基地局（図示せず）から送信された信号は、送受信アンテナ 1 で受信されて無線部 2 に供給されて復調などの処理がなされて制御部 3 に供給され、他方、制御部 3 から出力された信号は無線部 2 で変調などの処理が行われて、所定の周波数帯の送信信号とされ送受信アンテナ 1 を介して最寄りの基地局（図示せず）へ無線送信される。

【 0 0 3 4 】

40

制御部 3 は無線部 2 により復調された信号を供給されたときには、それが音声信号のときにはサウンド 7 に供給して受話音声として発音させ、また、マイク 9 により収音されて音声信号に変換された送話音声信号は、無線部 2 へ供給して変調等の所定の信号処理を行わせる。上記の携帯電話機の通常の通話動作については周知であるので詳しい説明は省略する。

【 0 0 3 5 】

制御部 3 は携帯電話機の各部を統括的に制御する制御回路であり、この制御部 3 によって IC カード挿入部 1 0 に挿入された IC カードが USIM か SIM かを判別して、各部の動作を制御すると共に、USIM の識別情報（IMSI）はメモリ 4 に記憶する。メモリ 4 は、メモリダイヤル及びファンクション機能を設定するための設定画面や制御部 3 の

50

動作用プログラム等を記憶しているメモリである。操作部 6 は複数のキーから構成された入力部であり、制御部 3 では操作部 6 の操作に応じてメモリ 4 から前述の識別情報などを読み出し、表示部 5 上に表示する。

【 0 0 3 6 】

表示部 5 は液晶などを用いた表示パネルからなっており、携帯電話機の状態、時刻等を表示する。サウンダ 7 は音声を放音する部分であり、メモリ 4 に記憶している鳴動パターンの音を鳴動したり、受話音声信号を電気 - 音響変換して発音する。タイマ 8 は時計機能を担当する。マイク 9 は通話の際に送話音声を収音して音響 - 電気変換して音声信号に変換する。ICカード挿入部 10 は、使用者情報や電話番号などの識別情報を含んだICカード (SIM/USIM) を挿入する部分であり、挿入されたICカードの記憶情報を制御部 3 にて読み出し、携帯電話機が動作する。通常、ICカードがICカード挿入部 10 に挿入されていない状態では、携帯電話機は制限された動作しか行うことができない。

10

【 0 0 3 7 】

次に、本実施の形態の動作について、図 2 のフローチャートを併せ参照して説明する。本実施の形態は、各々自分専用のICカードを有するユーザが 1 台の携帯電話機を共用する場合の管理の手間の低減に好適である。まず、本実施の形態の携帯電話機の制御部 3 は電源が投入されると (ステップ S 1)、ICカード挿入部 10 に挿入されたICカードの識別情報がUSIMの識別情報 (IMSI) であるか否かの判別を行う (ステップ S 2)。

【 0 0 3 8 】

20

制御部 3 は、ICカード挿入部 10 に挿入されたICカードの識別情報が、メモリ 4 に予め登録されているUSIMの識別情報 (IMSI) と一致しないとステップ S 2 で判定した場合は、制限モード (SIM/USIM Personalisation) に入る (ステップ S 3)。このステップ S 3 の制限モードにおいてユーザに許可される操作は、3GPP標準動作であるUSIM登録認証、緊急呼の発信に加え、予め登録しておいた管理者番号 (携帯電話管理者の電話番号、メールアドレス等) への発信も許可する。

【 0 0 3 9 】

管理者番号は、この携帯電話機の管理者 (オーナー) の連絡先等であり、これを登録しておくことで所有者を明確に示し各種の通知が行われる通知先として使われる。その他の電話帳等の個人情報に関わるデータに関しては、制限モードでは一切の閲覧・操作を行うことはできない。

30

【 0 0 4 0 】

この制限モードにおいて、SIM/USIM (IMSI) 登録操作を行い、SIM/USIM (IMSI) 登録認証が成功したかどうか判定する (ステップ S 4)。ステップ S 4 の登録認証判定は、例えば携帯電話機本体のメモリ 4 にUSIM登録認証用のパスワードが予め記憶されており、制限モード時にユーザが認証動作を行う際にパスワードの入力が求められ、それに応じて入力したパスワードが記憶されているパスワードと合致するかどうか制御部 3 が比較照合し、合致した場合は登録認証成功、不一致の場合は登録認証失敗と判定される。

【 0 0 4 1 】

40

ステップ S 4 でUSIM登録認証に失敗と判定した場合、認証失敗通知が行われる (ステップ S 6)。この認証失敗通知は前述の管理者番号に対して、電子メール等で通知される。その内容は携帯電話機に挿入されているUSIMのIMSI情報を含んでおり、失敗を通知するものである。これにより、携帯電話機の管理者は、現在の携帯電話機の所在を管理することができる。認証失敗通知後は再びステップ S 3 の制限モードに戻る。制限モードに戻ると、再びSIM/USIM (IMSI) 登録認証操作が可能となる。最初のパスワード入力に失敗する可能性があるため、再度認証のチャンスを与えるためである。入力パスワードが携帯電話機に保存されているパスワードに一致しない限り、ユーザは制限モードでのみしか使用できない。

【 0 0 4 2 】

50

ステップS4での登録認証に成功したときには、挿入されたICカードのIMSIをメモリ4に記録し、認証成功通知を発行する(ステップS5)。従って、以後再びこのICカードを所有するユーザがこの携帯電話機を使用する場合は、ステップS2では、登録されているUSIMとして判断される。また、ステップS2の判定において、ICカード挿入部10に挿入されたICカードの識別情報IMSIが、メモリ4に予め登録されているSIM/USIMの識別情報であることが確認された場合は、制御部3は認証成功通知を発行する(ステップS5)。この認証成功通知は、前述の管理者番号に対して、電子メール等で通知される。その内容は携帯電話機に挿入されているUSIMのIMSI情報を含んでおり、これにより、携帯電話機の管理者は、現在の携帯電話機の利用者を把握・管理することができる。

10

**【0043】**

認証成功通知がされると、制御部3は続いて、メモリ4に個人情報が登録済みであるか判定する(ステップS7)。この個人情報は、挿入されたICカードによって個別に管理する、メモリ4にのみIMSIに対応付けて記憶された個別管理情報(電話帳、メール、発着信履歴等)のことであり、換言すると、ステップS7では後述するユーザ別モードを使用する権限が与えられているICカードが挿入されているのか否かを判定することと同じである。

**【0044】**

個人情報が登録済みでないときには一般モードに移行し(ステップS8)、登録済みであるときには、個人情報を判定する(ステップS10)。ステップS8の一般モードにおいては、携帯電話機の全ての機能を自由に使用することができるが、後述するユーザ別モードでメモリ4に登録された電話帳等の個人情報に関わるデータの閲覧・操作を行うことはできない。

20

**【0045】**

ステップS8で一般モードに移行すると、制御部3は個人情報登録操作の認証を行う(ステップS9)。この個人情報登録操作の認証は、ユーザに対して個人情報登録操作のパスワード入力を促し、これによりユーザが入力したパスワードを、予めメモリ4に記憶されている個人情報登録操作認証用パスワードと一致するか比較照合することで行われる。なお、この個人情報登録操作認証用パスワードは、前記ステップS4におけるUSIM登録認証用パスワードとは異なるパスワードが用意されている。

30

**【0046】**

入力パスワードが上記の個人情報登録操作認証用パスワードと合致せず、個人情報登録認証に失敗すると、一般モードで引き続き動作するが、入力パスワードが上記の個人情報登録操作認証用パスワードと合致し、個人登録認証に成功すると、個人情報登録済みか否か再度判定する(ステップS7)。ステップS9で個人情報登録認証が成功したと判定された場合は、挿入されたICカードが、個別に管理する情報(個人情報)を持つICカードであるものに変更されたので、ステップS7では、個人情報登録済みと判定される。

**【0047】**

制御部3は、ステップS7で個人情報登録済みと判定されたときには、個人情報を判定して(ステップS10)、ユーザ別モードに移行する。ステップS10での個人情報の判定とは、メモリ4に登録されているユーザ別のIMSI情報を判定することであり、IMSI情報を判定することにより、各IMSI情報毎のユーザ別モードが可能となる。

40

**【0048】**

このユーザ別モードの動作は、見た目上一般モードと変わりなく、全ての操作を可能とする。一般モードとの違いは、何かしらの要因によって携帯電話機のメモリ4に個人情報に関わるデータが生成される場合、そのユーザのみが閲覧・操作可能なデータ(IMSIと関連付けられたデータ)として生成されることにある。また、ユーザ別モードでは、例えば電話帳に登録する際に、他人に見られたくないユーザ専用の電話番号か、他人に見られても差し支えない電話番号かを区別して登録できる手段を有する。一般モードでは、ユーザ専用の電話番号登録はできない。

50

## 【 0 0 4 9 】

また、このユーザ別モードでは、携帯電話の各種環境設定もユーザ別のものとして記録される。このユーザ別モードは、細かく分ければユーザAモードS11、ユーザBモードS12、ユーザCモードS13などと分類され、これらのうち、任意のユーザ別モードにおいては、他の全てのユーザ別モードでユーザが登録した個人情報関連データの閲覧・操作は不可能であり、自分のユーザ別モードで登録した個人情報関連データの閲覧・操作のみ可能である。ただし、データを生成する時、またはそのデータを明示的に一般モードで閲覧・操作可能に変更することは可能である。

## 【 0 0 5 0 】

これにより、本実施の形態によれば、例えば以下のような使い方が可能となる。いま、ユーザAがA社、B社、C社の各電話番号を電話帳に登録して使用した携帯電話機を、ユーザBに渡すと、A社、B社、C社の各電話番号が電話帳に表示されるが、ユーザBはC社、D社、E社の電話番号を使用したい場合、A社とB社の電話番号は不要であり、また、D社の電話番号は個人用扱いとしたい場合は、D社の電話番号をユーザB専用電話番号として、ユーザBモードにおいてユーザBの持つICカードのISMIに対応させてメモリ4に登録する。

10

## 【 0 0 5 1 】

そして、ユーザBが自分のICカードを携帯電話機から抜いて、再びユーザAに渡すときに、ユーザBが「A社とB社の電話番号は不要であるので個人扱いに」と注文する。ユーザAが自分が持つICカードを携帯電話機に挿入（装着）して表示部5に電話帳を表示させると、A社、B社、C社、E社の電話番号が見えるので、ユーザAはユーザBの先の注文を受けて、ユーザAモードにてA社とB社の電話番号を自分専用の電話番号として登録すると、ユーザAの持つICカードのISMIに対応させてメモリ4にA社とB社の電話番号が登録される。

20

## 【 0 0 5 2 】

これにより、その後、ユーザAが自分のICカードを携帯電話機から抜いて、再びユーザBに渡した場合、ユーザBが自分が持つICカードを携帯電話機に挿入（装着）して表示部5に電話帳を表示させると、ユーザBモードではC社、D社及びE社の各電話番号だけが表示されることになる。携帯電話機のメモリ4には、A社、B社、C社、D社、E社の各電話番号が登録されているが、そのうち、A社とB社の各電話番号はユーザAのISMIに対応させて登録され、ユーザAモードでのみ表示されるようにされており、D社の電話番号はユーザBのISMIに対応させて登録され、ユーザBモードでのみ表示されるようにされている。

30

## 【 0 0 5 3 】

従来は、携帯電話機に電話帳登録されている全ての電話番号を表示するために、上記の場合は、ユーザに関係なくA社、B社、C社、D社、E社の各電話番号が全て表示されてしまうので、ユーザBは事実上、D社の電話番号を電話帳登録できないし、各ユーザは自分が使うことがない電話番号を含んだ電話帳を使用しなくてはならず、使い勝手が悪いものとなる。

## 【 0 0 5 4 】

これに対し、本実施の形態によれば、上記の場合、制限モードでは表示部には電話帳登録された電話番号は何も表示されず、一般モードでは、C社とE社の各電話番号とが表示され、一般閲覧可能なF社の電話番号を電話帳に登録することも可能である。一方、ユーザ別モードでは、例えばユーザAのICカードを装着すると、A社、B社、C社、E社の各電話番号が表示され、ユーザAが使用する電話番号だけを表示でき、使い勝手を向上できる。また、ユーザ別モードでは、一般閲覧可能な電話番号も電話帳に保存することが可能である。更に、携帯電話機の設定（例えば、着信音、待ち受け等）もユーザ別に登録することが可能である。

40

## 【 0 0 5 5 】

このように、本実施の形態によれば、自分以外のユーザに見せたくないデータをいちい

50

ち削除することや、携帯電話機の環境設定のやり直しといった、SIM/USIMを抜いた携帯電話機を他人に貸与する場合の手間、再度借用した場合の手間を不要にできるため、利便性を大幅に向上することができる。

【0056】

なお、本発明は以上の実施の形態に限定されるものではなく、その他種々の変形例を包含するものである。例えば、ステップS5、S6での通知は自動的に行うのが通常であるが、手動でも差し支えない。また、携帯電話機の管理者（実質所有者）が、SIM/USIMカードによる機能制限（通話エリア、通話時間等）を設定したり、あるいは予め複数設定された機能制限を切り替え可能にしてもよい。また、この設定等は、SIM/USIMカードの入れ替えの連絡を受けた直後に携帯電話機の管理者（実質所有者）の遠隔操作で可能にしてもよい。

10

【0057】

また、SIM/USIMカードによっては、定期的にその携帯通信端末の状態（SIM/USIMカードを交換してからの累積通信料金等）を、所定の連絡先（当該携帯通信端末の名義人、実質所有者等）に通知するようにしてもよい。更に、SIM/USIMカード入れ替え時のカスタマイズは、切り替え時以外に、現在のデータを消去してインターネットに接続し、所定のサーバ装置の所定の記憶エリアから、データを自動ダウンロードするものでもよい。

【0058】

更に、本発明で使用するICカードは、カードに各々のIDが存在しているものであれば何でも使用可能であり、例えば、SDカードにIDを記録したファイルを格納しておき、そのファイルのIDを実施の形態のIMS Iとして使用することができる。また、USMIカードを使用しない2G携帯通信端末（PDC）等に、同じようなカード挿入部を設けて、上記のような個別のIDを持つカードを使って、上記の実施の形態と同様の動作を行わせることも可能である。また、本発明は、上記の実施の形態をコンピュータにより実行させるコンピュータプログラムも含むものである。

20

【図面の簡単な説明】

【0059】

【図1】本発明の一実施の形態の構成図である。

【図2】図1の動作説明用フローチャートである。

30

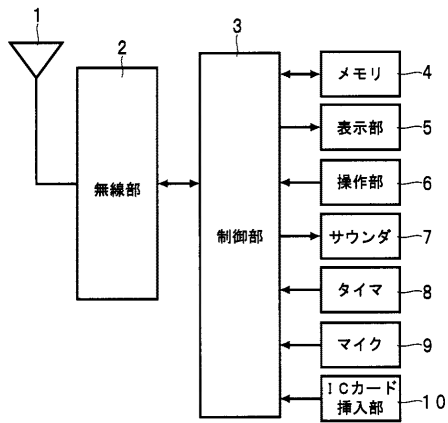
【符号の説明】

【0060】

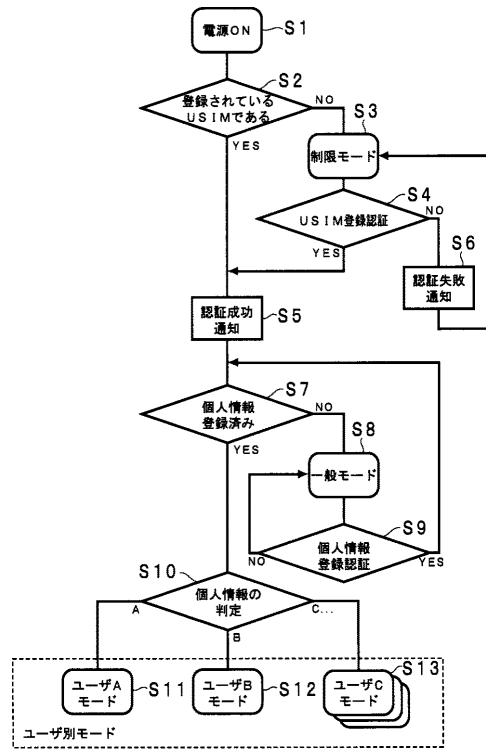
- 2 無線部
- 3 制御部
- 4 メモリ
- 5 表示部
- 6 操作部
- 7 サウンダ
- 8 タイマ
- 9 マイク
- 10 ICカード挿入部

40

【図1】



【図2】



---

フロントページの続き

- (56)参考文献 特開2004-064657(JP,A)  
特開2003-289371(JP,A)  
特開2000-308140(JP,A)  
特開2003-091509(JP,A)  
特開2002-027092(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04M 1/675

H04Q 7/38