

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第5633233号
(P5633233)

(45) 発行日 平成26年12月3日(2014.12.3)

(24) 登録日 平成26年10月24日(2014.10.24)

(51) Int.Cl. F I
HO4M 1/67 (2006.01) HO4M 1/67

請求項の数 8 (全 18 頁)

<p>(21) 出願番号 特願2010-176537 (P2010-176537) (22) 出願日 平成22年8月5日(2010.8.5) (65) 公開番号 特開2012-39313 (P2012-39313A) (43) 公開日 平成24年2月23日(2012.2.23) 審査請求日 平成25年6月13日(2013.6.13)</p>	<p>(73) 特許権者 000002897 大日本印刷株式会社 東京都新宿区市谷加賀町一丁目1番1号 (74) 代理人 110000958 特許業務法人 インテクト国際特許事務所 (74) 代理人 100083839 弁理士 石川 泰男 (74) 代理人 100120189 弁理士 奥 和幸 (72) 発明者 山田 真生 東京都新宿区市谷加賀町一丁目1番1号 大日本印刷株式会社内 審査官 永田 義仁</p>
---	--

最終頁に続く

(54) 【発明の名称】 端末装置、携帯電話機、動作管理方法及び動作管理プログラム等

(57) 【特許請求の範囲】

【請求項1】

R F I D タグに記憶されたデータの読み取り及び登録を非接触で行う端末装置であって、

R F I D タグに記憶された識別情報を読み取り、登録する登録手段と、
 端末装置の使用を制限するセキュリティモードを開始する開始手段と、
 前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在する R F I D タグを検索し、当該 R F I D タグに記憶された識別情報を読み取る通信手段と、

前記登録された識別情報から、前記通信手段によって読み取られた識別情報が所定の数量検索された場合に、前記セキュリティモードを終了する終了手段と、

予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了手段と、

前記所定の数量に満たなかった場合であって予め定められる第2の数量に達した場合に、前記暗証番号の入力を要求する要求手段と、
 を備えることを特徴とする端末装置。

【請求項2】

R F I D タグに記憶されたデータの読み取り及び登録を非接触で行う端末装置であって、

R F I D タグに記憶された識別情報を読み取り、前記読み取られた識別情報に対応する

10

20

点数を付与する登録手段と、

端末装置の使用を制限するセキュリティモードを開始する開始手段と、

前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するRFIDタグを検索し、当該RFIDタグに記憶された識別情報を読み取る通信手段と、

前記通信手段によって読み取られた全ての識別情報に対応する点数の合計が、所定の点数に達した場合に、前記セキュリティモードを終了する終了手段と、

予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了手段と、

前記所定の点数に満たなかった場合であって予め定められる第2の点数に達した場合に、前記暗証番号の入力を要求する要求手段と、

を備えることを特徴とする端末装置。

【請求項3】

請求項1に記載の端末装置であって、

前記端末装置は携帯電話機であり、

前記RFIDタグは、前記携帯電話機のユーザが携行する物品に貼付されており、

前記通信手段は、前記ユーザが携行する物品に貼付されたRFIDタグに記憶された識別情報を読み取り、

前記終了手段は、前記登録された識別情報から、前記通信手段によって読み取られた前記ユーザが携行する物品に貼付されたRFIDタグに記憶された識別情報が所定の数量検索された場合に、前記セキュリティモードを終了することを特徴とする携帯電話機。

【請求項4】

請求項2に記載の端末装置であって、

前記端末装置は携帯電話機であり、

前記RFIDタグは、前記携帯電話機のユーザが携行する物品に貼付されており、

前記通信手段は、前記ユーザが携行する物品に貼付されたRFIDタグに記憶された識別情報を読み取り、

前記終了手段は、前記通信手段によって読み取られた全ての識別情報に対応する点数の合計が、所定の点数に達した場合に、前記セキュリティモードを終了することを特徴とする携帯電話機。

【請求項5】

RFIDタグに記憶されたデータの読み取り及び登録を非接触で行う端末装置における動作管理方法であって、

RFIDタグに記憶された識別情報を読み取り、登録する登録工程と、

端末装置の使用を制限するセキュリティモードを開始する開始工程と、

前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するRFIDタグを検索し、当該RFIDタグに記憶された識別情報を読み取る通信工程と、

前記登録された識別情報から、前記通信工程によって読み取られた識別情報が所定の数量検索された場合に、前記セキュリティモードを終了する終了工程と、

予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了工程と、

前記所定の数量に満たなかった場合であって予め定められる第2の数量に達した場合に、前記暗証番号の入力を要求する要求工程と、

を有することを特徴とする動作管理方法。

【請求項6】

RFIDタグに記憶されたデータの読み取り及び登録を非接触で行う端末装置における動作管理方法であって、

RFIDタグに記憶された識別情報を読み取り、前記読み取られた識別情報に対応する点数を付与する登録工程と、

10

20

30

40

50

端末装置の使用を制限するセキュリティモードを開始する開始工程と、
前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するRFIDタグを検索し、当該RFIDタグに記憶された識別情報を読み取る通信工程と、

前記通信工程によって読み取られた全ての識別情報に対応する点数の合計が、所定の点数に達した場合に、前記セキュリティモードを終了する終了工程と、

予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了工程と、

前記所定の点数に満たなかった場合であって予め定められる第2の点数に達した場合に、前記暗証番号の入力を要求する要求工程と、

を有することを特徴とする動作管理方法。

10

【請求項7】

RFIDタグに記憶されたデータの読み取り及び登録を非接触で行う端末装置に含まれるコンピュータを、

RFIDタグに記憶された識別情報を読み取り、登録する登録手段、

端末装置の使用を制限するセキュリティモードを開始する開始手段、

前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するRFIDタグを検索し、当該RFIDタグに記憶された識別情報を読み取る通信手段

、
前記登録された識別情報から、前記通信手段によって読み取られた識別情報が所定の数量検索された場合に、前記セキュリティモードを終了する終了手段、

20

予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了手段、及び、

前記所定の数量に満たなかった場合であって予め定められる第2の数量に達した場合に、前記暗証番号の入力を要求する要求手段として機能させることを特徴とする動作管理プログラム。

【請求項8】

RFIDタグに記憶されたデータの読み取り及び登録を非接触で行う端末装置に含まれるコンピュータを、

RFIDタグに記憶された識別情報を読み取り、前記読み取られた識別情報に対応する点数を付与する登録手段、

30

端末装置の使用を制限するセキュリティモードを開始する開始手段、

前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するRFIDタグを検索し、当該RFIDタグに記憶された識別情報を読み取る通信手段

、
前記通信手段によって読み取られた全ての識別情報に対応する点数の合計が、所定の点数に達した場合に、前記セキュリティモードを終了する終了手段、

予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了手段、及び、

前記所定の点数に満たなかった場合であって予め定められる第2の点数に達した場合に、前記暗証番号の入力を要求する要求手段として機能させることを特徴とする動作管理プログラム。

40

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、端末装置、携帯電話機、動作管理方法及び動作管理プログラム等に関するものであり、より詳細には、例えば、簡便な方法で確実に装置の動作を管理することができる端末装置、動作管理方法及び動作管理プログラム等の技術分野に関する。

【背景技術】

【0002】

50

近年、CPUやメモリ等のデバイスの小型化及び高機能化によって、様々な機能を備える携帯電話機、PDA、ノートパソコン等の携帯型端末装置が普及し利用されている。

【0003】

かかる携帯型端末装置は、その携帯性から盗難に遭いやすく、また、置忘れ等紛失しやすいため、当該携帯型端末装置が容易に第三者の手に渡ってしまう虞がある。そして、携帯型端末装置が第三者にわたってしまうと、当該携帯電話機を第三者に使用されてしまったり、当該携帯型端末装置に記憶された機密情報や個人情報が第三者に知られてしまう等、携帯型端末装置のユーザに甚大な被害を与えてしまう。そこで、このような問題点を回避するために、携帯型端末装置には、一般的にセキュリティモード（ロック機構）が備えられている。

10

【0004】

セキュリティモードは、上述した携帯電話機等が備える様々な機能（通話機能、メール機能、ブラウジング機能、電話帳機能、及びスケジュール帳等）の第三者による使用を制限するための機能であり、例えば携帯電話機のユーザの操作に基づいて実行されるものである。このセキュリティモードが実行されると、携帯電話機は、操作部からの入力信号を受け付けられないため（すなわち、当該入力信号を無効とする。）、当該携帯電話機が備える上記機能を実行することができない。そして、例えば、操作部から入力される情報（例えば、数字や文字等）が、予め設定された暗証番号と一致した場合に、上記携帯電話機は、上記セキュリティモードを解除するようになっている。

【0005】

また、特許文献1では、ロック機能を備えた携帯型通信装置において、外部の通信装置の遠隔操作によって、かかるロック機能を作動可能とする技術が開示されている。

20

【先行技術文献】

【特許文献】

【0006】

【特許文献1】特開平11-32369号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

しかしながら、上記セキュリティモードを解除するためには上記暗証番号を入力しなければならず、例えば、暗証番号を忘れてしまった場合には、かかるセキュリティモードを解除することができなくなってしまう。また、特許文献1に記載された技術では、セキュリティモードの実行及び解除に外部の通信装置の遠隔操作が必要になり、ユーザに当該通信装置の遠隔操作という特別な動作を要求してしまう。

30

【0008】

そこで、本発明は、上記問題点を鑑みてなされたものであり、その目的の一例は、簡便な方法で装置の動作を管理することができる端末装置、携帯電話機、動作管理方法及び動作管理プログラム等の技術分野に関する。

【課題を解決するための手段】

【0009】

上記課題を解決するため、請求項1に記載の発明は、RFIDタグに記憶されたデータの読み取り及び登録を非接触で行う端末装置であって、RFIDタグに記憶された識別情報を読み取り、登録する登録手段と、端末装置の使用を制限するセキュリティモードを開始する開始手段と、前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するRFIDタグを検索し、当該RFIDタグに記憶された識別情報を読み取る通信手段と、前記登録された識別情報から、前記通信手段によって読み取られた識別情報が所定の数量検索された場合に、前記セキュリティモードを終了する終了手段と、予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了手段と、前記所定の数量に満たなかった場合であって予め定められる第2の数量に達した場合に、前記暗証番号の入力を要求する要求手段

40

50

と、を備えることを特徴とする。

【0010】

従って、簡便な方法で確実に端末装置のセキュリティモードを終了することができ、ユーザの生活状況に応じて、端末装置のセキュリティモードを終了することができる。

【0011】

請求項2に記載の発明は、R F I Dタグに記憶されたデータの読み取り及び登録を非接触で行う端末装置であって、R F I Dタグに記憶された識別情報を読み取り、前記読み取られた識別情報に対応する点数を付与する登録手段と、端末装置の使用を制限するセキュリティモードを開始する開始手段と、前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するR F I Dタグを検索し、当該R F I Dタグに記憶された識別情報を読み取る通信手段と、前記通信手段によって読み取られた全ての識別情報に対応する点数の合計が、所定の点数に達した場合に、前記セキュリティモードを終了する終了手段と、予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了手段と、前記所定の点数に満たなかった場合であって予め定められる第2の点数に達した場合に、前記暗証番号の入力を要求する要求手段と、を備えることを特徴とする。

10

【0012】

従って、端末装置のユーザが常に携帯する物品を所有している場合に、端末装置のセキュリティモードを終了することができる。

【0015】

請求項3に記載の発明は、請求項1に記載の端末装置であって、前記端末装置は携帯電話機であり、前記R F I Dタグは、前記携帯電話機のユーザが携帯する物品に貼付されており、前記通信手段は、前記ユーザが携帯する物品に貼付されたR F I Dタグに記憶された識別情報を読み取り、前記終了手段は、前記登録された識別情報から、前記通信手段によって読み取られた前記ユーザが携帯する物品に貼付されたR F I Dタグに記憶された識別情報が所定の数量検索された場合に、前記セキュリティモードを終了することを特徴とする。請求項4に記載の発明は、請求項2に記載の端末装置であって、前記端末装置は携帯電話機であり、前記R F I Dタグは、前記携帯電話機のユーザが携帯する物品に貼付されており、前記通信手段は、前記ユーザが携帯する物品に貼付されたR F I Dタグに記憶された識別情報を読み取り、前記終了手段は、前記通信手段によって読み取られた全ての識別情報に対応する点数の合計が、所定の点数に達した場合に、前記セキュリティモードを終了することを特徴とする。

20

30

【0016】

従って、携帯電話機のユーザが常に携帯する物品を所有している場合に、携帯電話機のセキュリティモードを終了することができる。

【0017】

請求項5に記載の発明は、R F I Dタグに記憶されたデータの読み取り及び登録を非接触で行う端末装置における動作管理方法であって、R F I Dタグに記憶された識別情報を読み取り、登録する登録工程と、端末装置の使用を制限するセキュリティモードを開始する開始工程と、前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するR F I Dタグを検索し、当該R F I Dタグに記憶された識別情報を読み取る通信工程と、前記登録された識別情報から、前記通信工程によって読み取られた識別情報が所定の数量検索された場合に、前記セキュリティモードを終了する終了工程と、予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了工程と、前記所定の数量に満たなかった場合であって予め定められる第2の数量に達した場合に、前記暗証番号の入力を要求する要求工程と、を有することを特徴とする。請求項6に記載の発明は、R F I Dタグに記憶されたデータの読み取り及び登録を非接触で行う端末装置における動作管理方法であって、R F I Dタグに記憶された識別情報を読み取り、前記読み取られた識別情報に対応する点数を付与する登録工程と、端末装置の使用を制限するセキュリティモードを開始する開始工程と、前

40

50

記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するRFIDタグを検索し、当該RFIDタグに記憶された識別情報を読み取る通信工程と、前記通信工程によって読み取られた全ての識別情報に対応する点数の合計が、所定の点数に達した場合に、前記セキュリティモードを終了する終了工程と、予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了工程と、前記所定の点数に満たなかった場合であって予め定められる第2の点数に達した場合に、前記暗証番号の入力を要求する要求工程と、を有することを特徴とする。

【0018】

請求項7に記載の発明は、RFIDタグに記憶されたデータの読み取り及び登録を非接触で行う端末装置に含まれるコンピュータを、RFIDタグに記憶された識別情報を読み取り、登録する登録手段、端末装置の使用を制限するセキュリティモードを開始する開始手段、前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するRFIDタグを検索し、当該RFIDタグに記憶された識別情報を読み取る通信手段、前記登録された識別情報から、前記通信手段によって読み取られた識別情報が所定の数量検索された場合に、前記セキュリティモードを終了する終了手段、予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了手段、及び、前記所定の数量に満たなかった場合であって予め定められる第2の数量に達した場合に、前記暗証番号の入力を要求する要求手段として機能させることを特徴とする。請求項8に記載の発明は、RFIDタグに記憶されたデータの読み取り及び登録を非接触で行う端末装置に含まれるコンピュータを、RFIDタグに記憶された識別情報を読み取り、前記読み取られた識別情報に対応する点数を付与する登録手段、端末装置の使用を制限するセキュリティモードを開始する開始手段、前記セキュリティモードが実行されている間、データの通信が可能な通信範囲内に存在するRFIDタグを検索し、当該RFIDタグに記憶された識別情報を読み取る通信手段、前記通信手段によって読み取られた全ての識別情報に対応する点数の合計が、所定の点数に達した場合に、前記セキュリティモードを終了する終了手段、予め設定された暗証番号と、外部から入力される暗証番号とが一致した場合に前記セキュリティモードを終了させる第2の終了手段、及び、前記所定の点数に満たなかった場合であって予め定められる第2の点数に達した場合に、前記暗証番号の入力を要求する要求手段として機能させることを特徴とする。

【発明の効果】

【0019】

以上のように、本発明によれば、端末装置は、登録されたRFIDタグの識別情報から、読み取られた識別情報が所定の数量検索された場合に、前記セキュリティモードを終了するように構成したので、簡便な方法で確実に端末装置のセキュリティモードを終了することができる。

【図面の簡単な説明】

【0020】

【図1】本実施形態に係るセキュリティシステムの全体構成の一例を示すブロック図である。

【図2】携帯電話機1内の機能ブロックの一例を示す概念図である。

【図3】本実施形態のセキュリティシステムSにおける携帯電話機1のCPUの動作を示す状態チャート図である。

【図4】本実施形態の登録状態における表示画面の遷移例を示す図である。

【図5】本実施形態の管理状態における表示画面の遷移例を示す図である。

【図6】本実施形態の管理状態における表示画面の遷移例を示す図である。

【図7】本実施形態の暗証番号の入力を促す表示画面を示す図である。

【発明を実施するための形態】

【0021】

以下、本発明を実施するための最良の実施形態について、図面に基づいて説明する。な

10

20

30

40

50

お、以下に説明する実施の形態は、携帯電話機（端末装置の一例）におけるセキュリティシステムに対して本願を適用した場合の実施形態である。

【0022】

[1. セキュリティシステムの構成及び機能]

先ず、図1を参照して、本実施形態に係るセキュリティシステムの構成及び機能について説明する。

【0023】

ここで、以下に説明するセキュリティシステムの構成及び動作概要は、例えば、ICタグ（RFIDタグ）リーダ機能を有する携帯電話機が実行するセキュリティモードが適用されるセキュリティシステムに対して本願を適用した場合の実施形態である。

10

【0024】

なお、このセキュリティモードとは、携帯電話機のユーザ以外の者が、携帯電話機等が備える様々な機能（通話機能、メール機能、ブラウジング機能、電話帳機能、及びスケジュール帳等）の操作を行うことを防止するために、かかる携帯電話機の操作（例えば、キー操作等）をロック（無効化）するための機能である。そして、当該ユーザの操作に基づき、又は一定期間キー操作がされない場合に、携帯電話機に記憶されたプログラム（後述するセキュリティモード専用アプリ）の制御により、上記セキュリティモードが実行されるようになっている。

【0025】

さらに本実施形態におけるセキュリティシステムは、携帯電話機の周囲に、当該携帯電話機のユーザが携行する物品（RFIDタグが貼付）が所定の数だけ存在した場合には、当該携帯電話機の周囲に当該ユーザが存在する（ユーザが携帯電話機を手に行っている）ものとみなして、上記セキュリティモードを解除するものである。

20

【0026】

また、このセキュリティシステムでは、携帯電話機の操作部から入力される情報（例えば、数字や文字等）が、予め設定された暗証番号と一致した場合に、上記携帯電話機は、セキュリティモードを解除するようになっている。

【0027】

図1は、本実施形態に係るセキュリティシステムの全体構成の一例を示すブロック図である。

30

【0028】

図1に示すように、セキュリティシステムSは、携帯電話機1（本願の端末装置の一例）と、携帯電話機1のユーザが携行する物品としての財布2、手帳3及び腕時計4のそれぞれにRFIDタグ2A、3A及び4Aが貼付されている。

【0029】

この携帯電話機1とRFIDタグ2A、3A及び4Aとは、詳しくは後述するが、携帯電話機1に備えられるリーダライタ機能によって相互にデータの読取りが可能となっている。

【0030】

なお、図1の例では、説明の便宜上、携帯電話機1のユーザが携行する物品（財布2、手帳3及び腕時計4）は3つ示されているがこれに限定されるものではない。また、携帯電話機1は、利用者毎に多数存在するようによい。

40

【0031】

[1-1. 携帯電話機1の構成及び機能]

携帯電話機1は、アンテナ、スピーカ、マイク、操作キー、ディスプレイの他、CPU（本実施形態における登録手段、開始手段、通信手段、終了手段、第2の終了手段、及び要求手段の一例）、RAM、ROM（各種データ及び携帯電話機1の動作を担うプログラムを予め記録）、記憶部等から構成された制御装置により構成されている。

【0032】

図2は、携帯電話機1内の機能ブロックの一例を示す概念図である。

50

【0033】

図2に示すように、携帯電話機1は、一般的な外部通信制御機能（例えば、W-CDMA又はCDMA2000の通信方式による）、ディスプレイ機能（例えば、液晶ディスプレイ等）、操作部（例えばキーボード、テンキー、タッチパネル等であり、オペレータ等からの操作指示を受け付け、その指示内容を指示信号としてCPUに出力する）、ブラウザ機能（URLを指定することで所定のサーバにアクセスして所定の情報を受ける（例えば、http（Hyper Text Transfer Protocol）による））、メーラ機能（例えば、メーラをユーザインタフェースとして、他の携帯電話機又はサーバ等との間でネットワークを介したデータの送受信を行う。）、携帯アプリ（携帯電話機の利用者が携帯電話機上で実行したい作業を実施する機能を直接的に有するソフトウェア）等を有している。なお、携帯電話機1におけるこれらの機能は公知であるため詳しい説明を省略する。

10

【0034】

また、本実施形態の携帯電話機1は、アンテナ及び通信制御部等を備え、上述したRFIDタグ2A、3A及び4Aとの間でデータ通信を可能とするリーダライタ機能を有している。

【0035】

このリーダライタ機能は、データの通信が可能な通信範囲内で、RFIDタグに対して、当該RFIDタグを駆動させるために必要な電力伝送と所定の通信規格に応じたデータ伝送（例えば、データの返信を要求する信号等の送受信等を行い、RFIDタグから送信されるデータを非接触で（無線通信方式により）読み取るようになっている。

20

【0036】

この通信範囲は、携帯電話機1とRFIDタグとの間で上記データの通信が可能な距離を示しており、上記通信規格に応じて定められている。具体的には、ISO/IEC18000-2（135KHz以下の無線通信方式）では上記通信範囲は数cm～1.0m、ISO/IEC18000-3（13.56MHzの無線通信方式）では上記通信範囲は数cm～数10cm（以下、これらを「近距離用通信方式」と総称する。）、ISO/IEC18000-4（950MHz帯の無線通信方式）では上記通信範囲は10mまで、ISO/IEC18000-5（2.45GHz帯の無線通信方式）では上記通信範囲は2.0mまで（以下、これらを「遠距離用通信方式」と総称する。）、と定められている。

【0037】

本実施形態における携帯電話機1のCPUは、上記通信規格を任意に切り替えることができるようになっており、かかる切り替え動作によって、通信距離を設定することができる。

30

【0038】

すなわち、携帯電話機1のCPUは、近距離用通信方式に切り替えることにより、携帯電話機1から比較的近い範囲（即ち、上記通信範囲が数cm～1.0m等）に存在するRFIDタグとの間で上記データの通信が可能となる。また、携帯電話機1のCPUは、遠距離用通信方式に切り替えることにより、携帯電話機1から比較的遠い範囲（即ち、上記通信範囲が10m等）に存在するRFIDタグとの間で上記データの通信が可能となる。

【0039】

また、この通信範囲は、携帯電話機1から送信される上記信号の電界強度に応じて変化する。具体的には、例えば、通信制御部が所定の通信規格（例えば、ISO/IEC18000-2）に応じて、RFIDタグとの間で上記データの通信を行う場合を考える。

40

【0040】

上述したように、当該通信規格における通信範囲は数cm～1.0mであるが、携帯電話機1から送信される上記信号の電界強度がより強い場合には、当該通信範囲は1.0mに近い値へ、かかる電界強度が弱い場合には、当該通信範囲は数cmに近い値へと変化するようになっている。

【0041】

本実施形態における携帯電話機1のCPUは、上記電界強度を任意に変化させることが

50

できるようになっている。

【0042】

このようにして、本実施形態における携帯電話機1のCPUは、通信規格又は電界強度を任意に切り替えることができるようになっており、かかる切り替え動作によって、通信距離を設定することができる。

【0043】

さらに、本実施形態における携帯電話機1は、上記携帯アプリの一例としてセキュリティモード専用アプリを有している。このセキュリティモード専用アプリは、上述したセキュリティシステムを実現するためのアプリケーションである。

【0044】

具体的には、所定の期間が経過した場合（例えば、携帯電話機のユーザの操作に基づき又は一定期間キー操作がされない場合）に、セキュリティモード専用アプリが起動され、当該アプリの制御のもと、携帯電話機1のCPUは、上述したセキュリティモードを実行する。

【0045】

同時に、携帯電話機1のCPUは、通信制御部を介して、上記通信範囲内に存在する当該RFIDタグに記憶された識別情報を検索し、かかる識別情報を読み取るべく、上記データの返信を要求する信号を送信する（すなわち、ポーリングを行う）。

【0046】

そして、携帯電話機のCPU1は、予め登録された識別情報から、上記読み取られた識別情報が所定の数量検索された場合には、上記セキュリティモードを終了するようになっている。

【0047】

なお、携帯機器としては、例えば、携帯電話機、PDA、ポータブルプレイヤー等を適用可能であるが、本実施形態においては、携帯電話機1を適用する。

【0048】

[1-2. RFIDタグ2Aの構成及び機能]

RFIDタグ2Aは、図示しないアンテナ等を備えるインターフェース、ROM (Read Only Memory)、RAM (Random Access Memory)、EEPROM、CPU (Central Processing Unit)等を備えて構成されている。インターフェースは、上述したデータ等を送受信するための入出力ポート(port)であり、CPUは、インターフェースを介して、上述した携帯電話機1等と交信する。EEPROMは、不揮発性半導体メモリの一種であり、記憶領域に記憶されているデータを消去し、何度でも再記憶ができるPROM (Programmable Rom)である。さらに、EEPROMは、上述した識別情報等を格納(記憶)する。この識別情報は、当該RFIDタグ2A自体を他のRFIDタグから識別するための識別情報であり、例えば、RFIDタグの製造業者等によって、製造時点に予め記憶されている。

【0049】

以上のように構成したRFIDタグ2Aでは、携帯電話機1のCPUから送信されるデータの返信を要求する信号を受信すると、上記アンテナに当該信号に基づく電圧が誘起され、その誘起電圧が上記CPUに供給される。上記CPUは、上記電圧に基づく電源の供給により起動され、上記信号を受信すると、EEPROM等に記憶されたデータ(例えば、識別情報等)を上記アンテナを介して、上記通信範囲内の携帯電話機1へ、上記通信規格に応じて送信する。

【0050】

[2. セキュリティシステムSにおける携帯電話機1のCPUの動作]

次に、図3～図7を用いて、本実施形態のセキュリティシステムSにおける携帯電話機1のCPUの動作について説明する。

【0051】

図3は、本実施形態のセキュリティシステムSにおける携帯電話機1のCPUの動作を

10

20

30

40

50

示すステートチャート図である。

【 0 0 5 2 】

図 3 に示すステートチャート図は、携帯電話機 1 の CPU 1 の動作状態の遷移を記述したものであり、待機状態、登録状態、探索状態及び管理状態が存在する。

【 0 0 5 3 】

そして、各状態に遷移する際に共通の動作（アクション）がある場合には各状態の entry / に、また、この状態にある間継続的に行われる動作は do / に、また、この状態から他の状態に遷移する際に共通の動作がある場合には exit / に、それぞれ記述される。

【 0 0 5 4 】

携帯電話機 1 の CPU は、電源が投入されると、待機状態となる。かかる待機状態では、例えば上述した携帯電話機等が備える様々な機能を実行するための指示（以下、「割り込みイベント」とする。）が入力された場合、携帯電話機 1 の CPU は、当該指示にかかる機能を実行する（割り込み待ち）ようになっている。即ち、待機状態では、携帯電話機 1 の CPU は、割り込み待ちの状態にある。

10

【 0 0 5 5 】

また、携帯電話機 1 の CPU は、待機状態に入る時、タイマ 0 割り込みカウンタ、及びタイマ 1 割り込みカウンタをスタートさせる。

【 0 0 5 6 】

このタイマ 0 割り込みカウンタとは、所定の期間毎に所定の割り込みイベント（携帯電話機 1 が実行する動作）を発生（実行）させるためのタイマであり、割り込みイベント毎に所定の期間が設定されている。そして、このカウンタが、上記所定の期間をカウント（計数）した場合には、携帯電話機 1 の CPU は、当該所定の期間に対応する割り込みイベントを実行するようになっている。

20

【 0 0 5 7 】

以下、本実施形態においては、割り込みイベントの種類を、タイマ 0 割り込み、タイマ 1 割り込みと識別し、割り込みイベントに設定されるカウンタを、タイマ 0 割り込みカウンタ、タイマ 1 割り込みカウンタとする。

【 0 0 5 8 】

そして、本実施形態においては、タイマ 0 割り込みに対応する所定の時間は 1 秒（S）に設定されており、携帯電話機 1 の CPU は、待機状態から 1 秒経過した後は、登録状態へ遷移するようになっている。

30

【 0 0 5 9 】

また、本実施形態においては、タイマ 1 割り込みに対応する所定の時間は 60（S）に設定されており、携帯電話機 1 の CPU は、待機状態から 60 秒経過した後は、探索状態へ遷移するようになっている。

【 0 0 6 0 】

また、この割り込みイベントには優先順位を付けることもでき、携帯電話機 1 の CPU は、かかる優先順位に応じて割り込みイベントを実行するようになっている。また、本実施形態の携帯電話機 1 の CPU は、操作ボタンが押下された場合には、これら割り込みイベントに優先させて、当該押下された操作ボタンに対応するイベントを実行する。

40

【 0 0 6 1 】

図 3 に示すステートチャートでは、携帯電話機 1 の CPU は、タイマ 0 割り込みを、タイマ 1 割り込みより優先させて実行し、かかるタイマ 0 割り込みが実行された後に、タイマ 1 割り込みを実行する。

【 0 0 6 2 】

このようにタイマ 0 割り込み、及びタイマ 1 割り込みは常に動作しており、カウントアップして設定値に達すると、割り込み要求を出力し、0 からカウントアップを再開する。

【 0 0 6 3 】

例えば、タイマ 0 割り込みを 1 秒、タイマ 1 割り込みを 60 秒に設定することにより、スムーズな登録（待ち時間 1 秒）とリーズナブルなセキュリティ（離れてから 60 秒後にセキ

50

ュリティモード（ロック）開始）を実現できる。

【0064】

図3の説明に戻り、携帯電話機1のCPUは、タイマ0割込みカウンタが1秒経過したことをカウントした場合には、登録状態へ遷移する。

【0065】

以下、本実施形態の登録状態について、図4を用いて説明する。

【0066】

図4は、本実施形態の登録状態における表示画面の遷移例を示す図である。

【0067】

この登録状態とは、携帯電話機1に、携帯電話機1のユーザが携行する物品に貼付されるRFIDタグの識別情報を登録するための処理をいう。

【0068】

具体的には、携帯電話機1のCPUは登録状態に遷移すると、通信制御部を介して、携帯電話機1から比較的近い範囲（即ち、上記通信範囲が数cm～10cm等）に存在するRFIDタグに記憶された識別情報を読み取るべく、近距離用通信方式に切り替えて、又は弱い電界強度に切り替えて、上記データの返信を要求する信号を送信する。

【0069】

そして、携帯電話機1のCPUは、RFIDタグに記憶された識別情報を読み取った場合には、読み取った識別情報を記憶部に記憶するか否かを選択させる画面を、例えばディスプレイに表示する（図4（A））。

【0070】

図4（A）には、RFIDタグを読み取ったことを示すコメントとして、「IDを検出しました。登録しますか？」が、また、かかる登録の可否を決定する操作ボタンとして、「はい」及び「いいえ」が表示されている。

【0071】

そして、ユーザの操作部の操作により「はい」が選択されると、携帯電話機1のCPUは、登録されるRFIDタグの情報（RFIDタグが貼付された物品の名称及び当該物品を持ち歩く頻度等）を登録するための画面を表示する（図4（B））。

【0072】

図4（B）には、RFIDタグが貼付された物品の名称を入力するための入力部、当該物品を持ち歩く頻度を入力するためのラジオボタン、及び登録指示ボタン及びキャンセルボタンが表示されている。

【0073】

そして、ユーザによる操作部の操作により、当該物品の名称及び当該物品を持ち歩く頻度が入力され、登録指示ボタンが押下されると（図4（C）及び（D））、携帯電話機1のCPUは、当該物品の名称及び当該物品を持ち歩く頻度を登録する（図4（E））。

【0074】

図4（E）には、携帯電話機1のCPUが、当該物品の名称及び当該物品を持ち歩く頻度を登録したことを示す画面が表示されている。

【0075】

そして、ユーザの操作により図4（E）に示される終了ボタンが押下された場合には、携帯電話機1のCPUは、待機状態へと遷移する（図3の待機命令）。

【0076】

図3の説明に戻り、携帯電話機1のCPUは、タイマ1割込みカウンタが60秒経過したことをカウントした場合には、探索状態へ遷移する。この探索時間は省電力化のため、所定時間経過毎に行うことが好ましい。

【0077】

以下、本実施形態の探索状態について説明する。

【0078】

この探索状態とは、携帯電話機1のCPUによって上記セキュリティモードが実行され

10

20

30

40

50

、携帯電話機 1 の周囲に存在する R F I D タグを検索している状態をいう。

【 0 0 7 9 】

そして、上述したように、携帯電話機 1 の C P U は、通信範囲内に存在する携帯電話機
のユーザが携行する物品に貼付される R F I D タグから読み取った識別情報と、この登録
された識別情報を照合し、一致した場合にはセキュリティモードを解除するようになって
いる。

【 0 0 8 0 】

具体的には、携帯電話機 1 の C P U は探索状態に遷移すると、通信制御部を介して、携
帯電話機 1 から比較的遠い範囲（即ち、上記通信範囲が 1 0 c m ~ 1 . 0 m 等）に存在す
る R F I D タグに記憶された識別情報を読み取るべく、遠距離用通信方式に切り替えて、
又は強い電界強度に切り替えて、上記データの返信を要求する信号を送信する。

10

【 0 0 8 1 】

そして、携帯電話機 1 の C P U は、R F I D タグに記憶された識別情報を読み取った場
合には、すでに登録された識別情報の中に、当該読み取られた識別情報が存在するか否か
を検索する。

【 0 0 8 2 】

そして、例えば、前記登録された識別情報から、この読み取られた識別情報が所定の数
量検索された場合には、携帯電話機 1 の C P U は、セキュリティモードを終了するよう
になっている。この所定の数量は任意に設定することができる。

【 0 0 8 3 】

具体的には、例えば、前記登録された識別情報として、ユーザの携行する財布に貼付さ
れた R F I D タグの識別情報、時計に貼付された R F I D タグの識別情報、及びベルトに
貼付された R F I D の識別情報があるとす。そして、探索状態において、携帯電話機 1
の C P U が、ユーザの携行する財布に貼付された R F I D タグの識別情報、時計に貼付さ
れた R F I D タグの識別情報を読み取った場合には、携帯電話機 1 の C P U は、セキュリ
ティモードを終了する（すなわち、上記所定の数量として 2 ）。

20

【 0 0 8 4 】

そして、携帯電話機 1 の C P U は、セキュリティモードを終了すると、上記信号の送信
を停止し、待機状態へ遷移する。

【 0 0 8 5 】

また、携帯電話機 1 の C P U は、タイマ 0 割込みカウンタが 1 秒経過したことをカウン
トした場合には、登録状態へ遷移するようになっている。

30

【 0 0 8 6 】

図 3 の説明に戻り、登録状態においてユーザの操作により図 4（E）に示されるメニ
ューボタンが押下された場合、又は待機状態において例えば図示しないメニュー画面にお
いてメニューボタンが押下された場合には、携帯電話機 1 の C P U は、管理状態へ遷移する
。

【 0 0 8 7 】

以下、本実施形態の管理状態について、図 5 及び図 6 を用いて説明する。

【 0 0 8 8 】

図 5 及び図 6 は、本実施形態の管理状態における表示画面の遷移例を示す図である。

40

【 0 0 8 9 】

この管理状態とは、登録状態において登録された R F I D タグの情報の変更を行うため
の処理をいう。

【 0 0 9 0 】

具体的には、携帯電話機 1 の C P U は、管理状態に遷移すると、登録状態において登録
された R F I D タグの情報の変更を行うためのメニュー画面を表示する（図 5（A））。

【 0 0 9 1 】

そして、ユーザの操作部の操作によって登録リスト変更・削除ボタンが押下されると、
携帯電話機 1 の C P U は、すでに登録された R F I D タグの情報を変更削除するための画

50

面を表示する（図5（B））。

【0092】

ここで、カーソル（破線で囲まれた矩形部）により登録されたRFIDタグ（RFIDタグが貼付された物品の名称）が選択されると、携帯電話機1のCPUは、選択されたRFIDタグの情報を変更するための画面を表示する（図5（C））。

【0093】

この画面は、RFIDタグが貼付された物品の名称及び当該物品を持ち歩く頻度を変更するための操作画面である。携帯電話機1のユーザは、操作部の操作によって、RFIDタグが貼付された物品の名称及び当該物品を持ち歩く頻度を変更することができ、さらに、変更ボタンを押下すると、携帯電話機1のCPUは、かかる変更を記憶部に記憶する（図5（D））。

10

【0094】

また、メニュー画面（図5（A））において、携帯電話機1のユーザは、操作部の操作によって、新規ID登録ボタンを押下すると、携帯電話機1のCPUは、登録状態へ遷移する。

【0095】

また、メニュー画面（図5（A）、図6（A））において、携帯電話機1のユーザは、操作部の操作によって、ロック解除設定・変更ボタンを押下すると、携帯電話機1のCPUは、セキュリティレベルを変更するための操作画面を表示する（図6（B））。

【0096】

20

本実施形態における携帯電話機1のCPUは、読み取られたユーザの携行する物品に貼付されたRFIDタグの識別情報に対応する点数を付与し、記憶する。そして、携帯電話機1のCPUは、探索状態（すなわち、セキュリティモード実行時）において、読み取られた全てのRFIDタグの識別情報に対応する点数の合計が、所定の点数に達した場合に、セキュリティモードを終了するようにしてもよい。すなわち、携帯電話機1のCPUは、セキュリティモードを終了させるための所定の点数を設定し、かかる所定の点数に応じて当該セキュリティモードを終了するようになっている。

【0097】

本実施形態では、この所定の点数をセキュリティレベルとしている。即ち、換言すれば、セキュリティレベルとは、セキュリティモードを解除するために必要なユーザの携行する物品に貼付されたRFIDタグの数や種類を設定するための値をいう。

30

【0098】

具体的には、上述した登録状態において、携帯電話機1のユーザが、RFIDタグが貼付された物品を持ち歩く頻度を設定したが、かかる頻度に応じて所定の点数が設定されている。

【0099】

具体的には、例えば、携帯電話機1のCPUは、「ほとんどいつも」に設定された場合には3点を、「わりとしょっちゅう」に設定された場合には2点を、「たまに」に設定された場合には1点を、それぞれ設定するようになっている。

【0100】

40

そして、携帯電話機1のCPUは、セキュリティレベルに応じて、セキュリティモードを終了させるための所定の点数（即ち、上記頻度に応じた所定の点数の合計）を設定し、かかる所定の点数に応じて当該セキュリティモードを終了する。

【0101】

具体的には、携帯電話機1のCPUは、セキュリティレベルが高に設定された場合には上記所定の点数は5点以上に、セキュリティレベルが中に設定された場合には上記所定の点数は3点以上に、セキュリティレベルが低に設定された場合には上記所定の点数は1点以上に設定するようになっている（図6（B）（C））。

【0102】

また、携帯電話機1のCPUは、前記登録された識別情報から読み取られた識別情報が

50

所定の数量検索されなかった場合、又は、読み取られた全てのRFIDタグの識別情報に対応する点数の合計が所定の点数に達しない場合には、暗証番号の入力を促し、入力された暗証番号と予め設定された暗証番号とが一致した場合にセキュリティモードを終了するようにしてもよい。

【0103】

この場合、上述した所定の数量よりも小さい値を第2の数量とし、携帯電話機1のCPUは、当該所定の数量に達しないが、この第2の数量に達した場合には、暗証番号の入力を促し、入力された暗証番号と予め設定された暗証番号とが一致した場合にセキュリティモードを終了するようにしてもよい。

【0104】

この第2の数量は任意に設定することができる。

【0105】

また、上述した所定の点数よりも小さい値を第2の点数とし、携帯電話機1のCPUは、当該所定の数量に達しないが、この第2の点数に達した場合には、暗証番号の入力を促し、入力された暗証番号と予め設定された暗証番号とが一致した場合にセキュリティモードを終了するようにしてもよい。

【0106】

この第2の点数は任意に設定することができる。

【0107】

図7は、本実施形態の暗証番号の入力を促す表示画面を示す図である。

【0108】

図7(A)には、ユーザの操作部の操作により暗証番号(PINコード)が入力される入力部と、入力を確定するためのボタンであるOKボタンが表示されている。

【0109】

ユーザの操作部の操作により暗証番号が入力され、入力された暗証番号と予め設定された暗証番号とが一致した場合には、携帯電話機1のCPUは、セキュリティモードを終了するようになっている。

【0110】

なお、以上説明した実施形態は特許請求の範囲に係る発明を限定するものではない。そして、上記実施形態の中で説明されている構成の組み合わせ全てが発明の課題解決に必須の手段であるとは限らない。

【0111】

また、図3に示す状態チャートに対応するプログラムをフレキシブルディスク又はハードディスク等の記録媒体に記録しておき、或いはネットワークNTを介して取得して記憶しておき、これらを汎用のマイクロコンピュータ等に読み出して実行させることにより、当該マイクロコンピュータ等を上記実施形態に係る携帯電話機1のCPUが示す動作と同様に機能させることも可能である。

【0112】

以上説明したように、携帯電話機1のCPUは、携帯電話機1のユーザが携行する物品に貼付されるRFIDタグの識別情報を登録し、セキュリティモードが実行されている間、登録された識別情報から、通信範囲内に存在する携帯電話機のユーザが携行する物品に貼付されるRFIDタグから読み取った識別情報が所定の数量検索された場合に、前記セキュリティモードを終了するように構成したため、携帯電話機1のCPUは、携帯電話機1のユーザの手を煩わせることなく、簡便な方法で確実にセキュリティモードを終了することができる。

【0113】

また、携帯電話機1のCPUは、セキュリティモードを終了させるための所定の点数を設定し、かかる所定の点数に応じて当該セキュリティモードを終了するように構成したため、携帯電話機1のユーザが常に携行する物品を所有している場合に、簡便な方法で確実にセキュリティモードを終了することができる。

10

20

30

40

50

【0114】

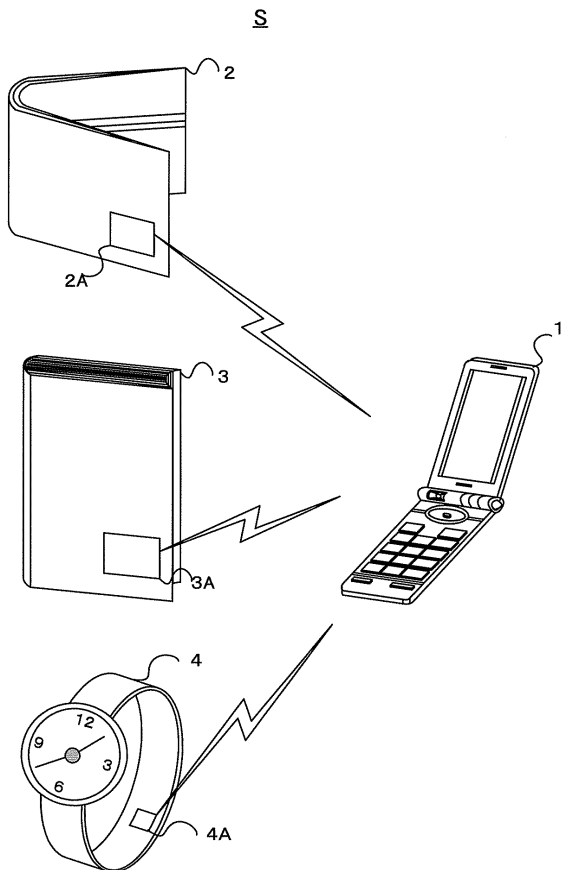
また、携帯電話機 1 の CPU は、前記登録された識別情報から読み取られた識別情報が所定の数量検索されなかった場合、又は、読み取られた全ての RFID タグの識別情報に対応する点数の合計が所定の点数に達しない場合には、暗証番号の入力を促し、入力された暗証番号と予め設定された暗証番号とが一致した場合にセキュリティモードを終了するように構成したため、携帯電話機 1 のユーザの生活状況に応じて、セキュリティモードを終了することができる。即ち、携帯電話機 1 のユーザが携行する頻度が高いものを所有していた場合にはセキュリティモードを終了することができる。

【符号の説明】

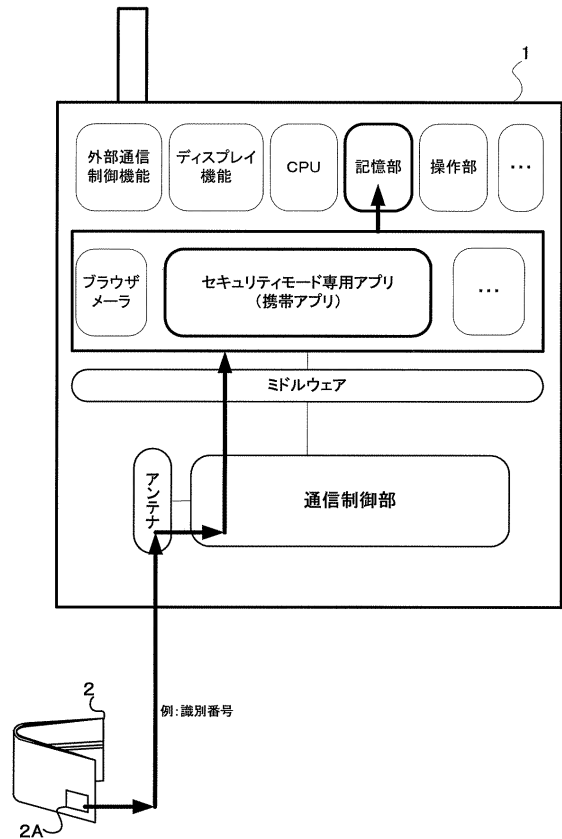
【0115】

- 1 携帯電話機
- 2 財布
- 2 A RFID タグ
- 3 手帳
- 3 A RFID タグ
- 4 腕時計
- 4 A RFID タグ
- S セキュリティシステム

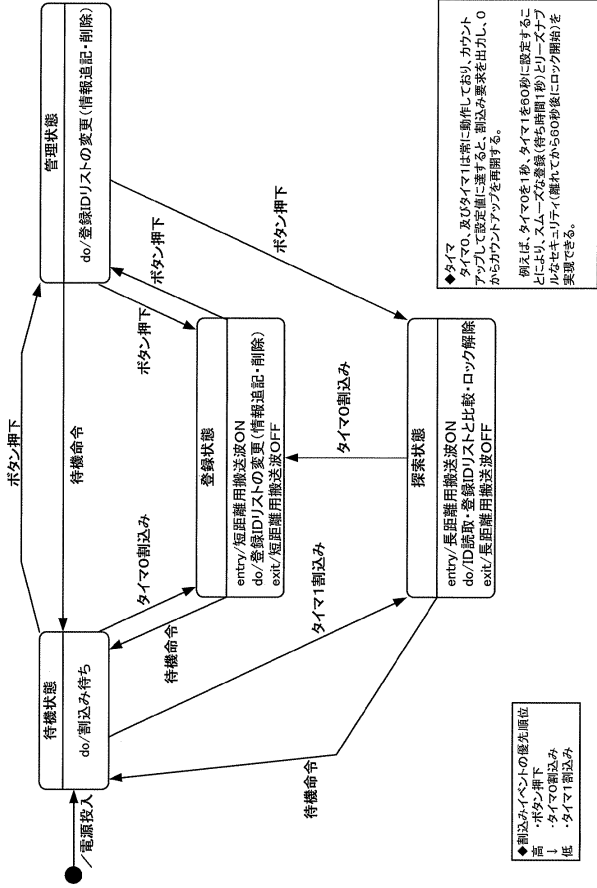
【図 1】



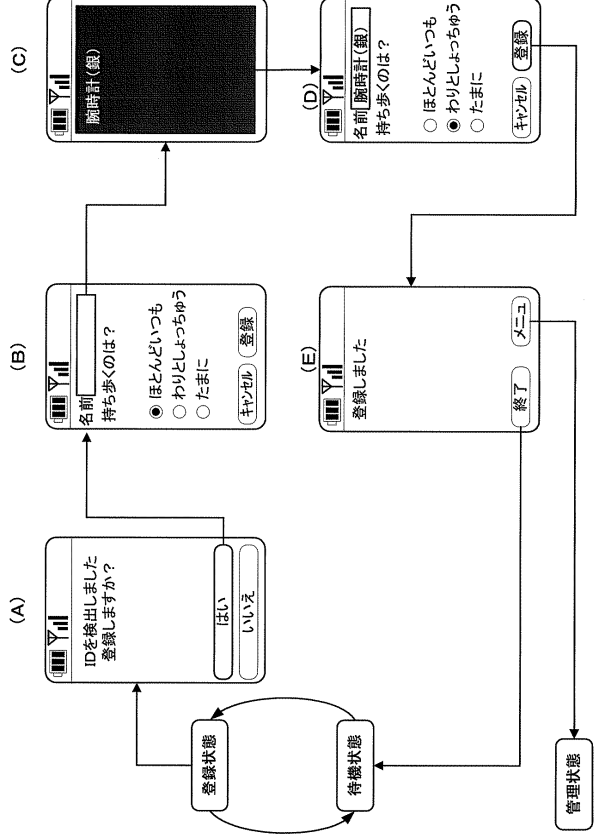
【図 2】



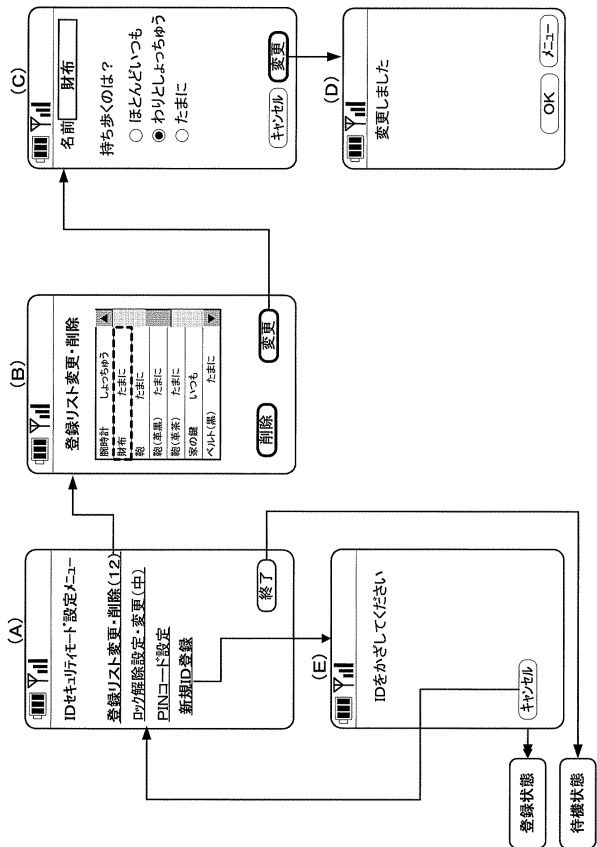
【図 3】



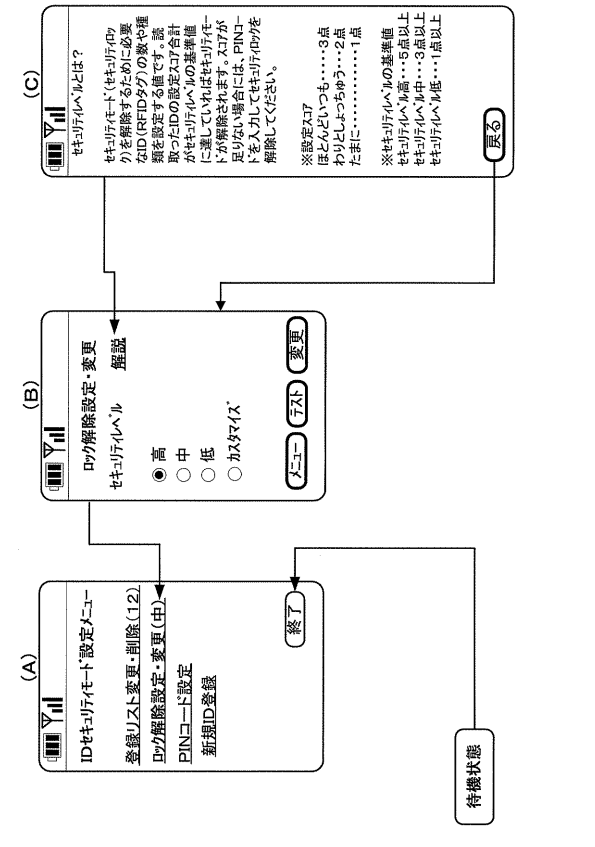
【図 4】



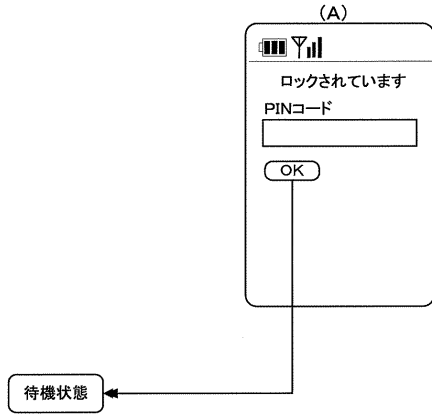
【図 5】



【図 6】



【図7】



フロントページの続き

(56)参考文献 特開2005-352710(JP,A)
特表2007-528524(JP,A)
特開2006-178591(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06K 17/00
H04M 1/00
H04M 1/24 - 1/82
H04M 99/00