(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3768325号
(P3768325)
(45)発行日　平成18年4月19日(2006.4.19)　(24)登録日　平成18年2月10日(2006.2.10)

(51)Int.Cl.　　F I
H04M 1/66 (2006.01)　　H04M 1/66
H04Q 7/38 (2006.01)　　H04B 7/26　109S

請求項の数 3　(全 16 頁)

(21)出願番号　特願平9-97610
(22)出願日　平成9年4月15日(1997.4.15)
(65)公開番号　特開平10-290285
(43)公開日　平成10年10月27日(1998.10.27)
審査請求日　平成13年1月15日(2001.1.15)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　濱松　美博
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

審査官　吉村　博之

最終頁に続く

(54)【発明の名称】通信端末装置

(57)【特許請求の範囲】

【請求項１】

識別情報を含む制御情報を記憶したカードと、該カードを脱着自在であり、かつ前記カードの制御情報に基づいて通信を行う本体とを備えた通信端末装置において、

前記本体は、

電源オンもしくは電源オフする電源ボタンと、

電源投入により通信を行う通信手段と、

前記カードの脱着状態を検出する脱着検出手段と、

前記脱着検出手段からの検出信号に基づいて該カードの装着を確認するＣＰＵと、

前記ＣＰＵにより前記カードの装着状態が検出された場合に前記カードに記憶された識別情報を含む制御情報を記憶する記憶手段と、

前記記憶手段に記憶された識別情報とあらかじめ記憶された識別情報とを照合し、その照合により一致が得られた場合にのみ前記電源ボタンの電源オン操作による電源投入を許可し、かつ、前記脱着検出手段及びＣＰＵにより前記カードの抜き取りが検出された場合にのみ前記通信手段による通信を許可する制御手段と、

を有したことを特徴とする通信端末装置。

【請求項２】

前記脱着検出手段及びＣＰＵにより前記カードの抜き取りが検出された場合に前記電源ボタンによる電源オフ操作の有無を判断し、その判断により電源オフ操作有りという判断結果が得られた場合に前記記憶手段に記憶された識別情報を含む制御情報を消去する制御

手段を有したことを特徴とする請求項１に記載の通信端末装置。
【請求項３】
前記カードは、外部通信機器について前記本体での使用可否を示す情報をあらかじめ記憶しており、
前記脱着検出手段及びＣＰＵにより前記カードの装着状態が検出された場合に前記カードに記憶された前記使用可否を示す情報を読み出し、その読み出された情報に従って本体自身に接続された外部通信機器の使用可否を判断し、その判断により使用可であるという判断結果が得られた場合に前記接続された外部通信機器を用いた通信を許可する制御手段を有したことを特徴とする請求項１または２に記載の通信端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、通信端末装置に関し、詳細には、ＩＣ（集積回路）カードの情報を用いて通信を行う携帯電話機，自動車電話機等の通信端末装置に関するものである。
【０００２】
【従来の技術】
図１３は、例えば特開平７－２０３０８号公報による従来の通信端末装置を示すブロック図である。図１３に示した通信端末装置においては、本体である本体４１が、アンテナ４６，このアンテナ４６に接続された無線通信を行う無線送信部４７および無線受信部４８，この無線受信部４８の無線チャネルを設定する局部周波数発振部４９，無線送信や局部周波数発振を制御する論理制御部・記憶部５０，操作者の正否の旨を表示する表示部５１，電源を供給する電源部５２，磁気カード装着部５５の磁気カード読取部５６を介して磁気カード４２に接続される読取Ｉ／Ｏ部５３，操作を指示するキー操作部５４により構成される。なお、磁気カード４２は、磁気データ（加入者個別データや個人暗証番号）を記憶した情報記憶部５７を有している。
【０００３】
つぎに、動作について説明する。図１３に示した通信端末装置では、本体４１の磁気カード装着部５５に磁気カード４２が挿入されると、磁気カード読取部５６により磁気データが読み取られ、その磁気データはさらに論理制御部・記憶部５０に転送される。このとき、操作者によるキー操作部５４のキー操作により暗証番号が入力され、その入力暗証番号と磁気データに含まれる暗証番号とが一致した場合には、無線電話の接続が可能になる。
【０００４】
なお、カードを用いて通信を行う近似技術として、例えば特開平６－２９６１６１号公報，同２９６１６２号公報がある。これら公報には、ＩＣカードの抜き取りを消費電力により検出し、ＩＣカードが抜き取られた際に通話を中止するという技術が開示されている。
【０００５】
【発明が解決しようとする課題】
上記公報のように従来例による通信端末装置は、磁気カードやＩＣカードなどのカードを本体に装着した状態で通信機能を果たすようにした構成なので、携帯中に、その通信端末装置が盗難されたり紛失した場合にはそのまま使用可能な状態で第三者に渡っていた。それゆえ、永久的に使用可能な状態が続いてしまうことから、第三者による乱用や悪用が放置されるという問題があった。
【０００６】
この発明は、上述した従来例による問題を解消するため、カードと本体との同時盗難や紛失を回避して、第三者による乱用や悪用による不正使用を有効に防止することが可能な通信端末装置を得ることを目的とする。
【０００７】
【課題を解決するための手段】
上述した課題を解決し、目的を達成するため、この発明に係る通信端末装置は、識別情報を含む制御情報を記憶したカードと、カードを脱着自在であり、かつカードの制御情報

に基づいて通信を行う本体とを備えた通信端末装置において、本体は、電源オンもしくは電源オフする電源ボタンと、電源投入により通信を行う通信手段と、カードの脱着状態を検出する脱着検出手段と、脱着検出手段からの検出信号に基づいてカードの装着を確認するＣＰＵと、ＣＰＵによりカードの装着状態が検出された場合にカードに記憶された識別情報を含む制御情報を記憶する記憶手段と、記憶手段に記憶された識別情報とあらかじめ記憶された識別情報とを照合し、その照合により一致が得られた場合にのみ前記電源ボタンの電源オン操作による電源投入を許可し、かつ、前記脱着検出手段及びＣＰＵにより前記カードの抜き取りが検出された場合にのみ通信手段による通信を許可する制御手段と、を有したことを特徴とする。

【０００８】

この発明によれば、本体においてＣＰＵによりカードの装着状態が検出された場合にカードに記憶された識別情報を含む制御情報を記憶手段により記憶し、記憶手段に記憶された識別情報とあらかじめ記憶された識別情報とを照合し、その照合により一致が得られた場合にのみ電源ボタンの電源オン操作による電源投入を許可し、かつ、前記脱着検出手段及びＣＰＵによりカードの抜き取りが検出された場合にのみ通信手段による通信を許可するようにしたので、使用時の段階で本体とカードとは別々に携帯され、本体とカードとを同時に盗難もしくは紛失するような事態が未然に防止され、これによって、本体だけでは電源投入ができず、不正使用を有効に防止することが可能である。

つぎの発明に係る通信端末装置は、上記の発明において、脱着検出手段及びＣＰＵによりカードの抜き取りが検出された場合に電源ボタンによる電源オフ操作の有無を判断し、その判断により電源オフ操作有りという判断結果が得られた場合に記憶手段に記憶された識別情報を含む制御情報を消去する制御手段を有したことを特徴とする。

この発明によれば、カードの抜き取りが検出された場合に電源ボタンによる電源オフ操作があると、カードから読み出して記憶しておいた識別情報を含む制御情報を消去するようにしたので、電源オフ後の本体の再使用ができなくなり、これによって、本体だけでは再使用ができないなどのように不正使用を有効に防止することが可能である。

【０００９】

つぎの発明に係る通信端末装置は、上記の発明において、カードは、外部通信機器について本体での使用可否を示す情報をあらかじめ記憶しており、脱着検出手段及びＣＰＵによりカードの装着状態が検出された場合にカードに記憶された使用可否を示す情報を読み出し、その読み出された情報に従って本体自身に接続された外部通信機器の使用可否を判断し、その判断により使用可であるという判断結果が得られた場合に接続された外部通信機器を用いた通信を許可する制御手段を有したことを特徴とする。

この発明によれば、カードの装着状態が検出された場合にカードに記憶された外部通信機器について本体での使用可否を示す情報に従って本体自身に接続された外部通信機器の使用可否を判断し、その判断により使用可であるという判断結果が得られた場合に接続された外部通信機器を用いた通信を許可するようにしたので、外部通信機器を接続しただけでは通信が行えず、これによって、外部通信機器を用いた不正使用を有効に防止することが可能である。

【００２１】

【発明の実施の形態】

以下に添付図面を参照して、この発明に係る通信端末装置の好適な実施の形態を詳細に説明する。

【００２２】

（実施の形態１）

図１はこの発明の実施の形態１による通信端末装置の内部構成を示すブロック図である。図１に示した通信端末装置は、ＩＣカード１と本体２Ａとの組合わせで構成されている。

【００２３】

ＩＣカード１は、各種の情報が記憶されたメモリ部１１と、メモリ部１１に接続された外部接続端子１２とを備えている。メモリ部１１は、ＩＤコードなどのように本体２Ａが通

信機能を果たすための情報を記憶している。外部接続端子１２は、ＩＣカード１が後述する本体２Ａのスロット部２１に挿入された際に、そのスロット部２１内に設けられた接続端子２１２に電気的に接続される。

【００２４】

本体２Ａは、ＩＣカード１を脱着（装着または脱装）するためのスロット部２１を備えている。スロット部２１は、ＩＣカード１が収容される収容空間２１１、収容空間２１１の内部に設けられＩＣカード１の外部接続端子１２に接続する接続端子２１２、および、接続端子２１２に付設され感圧センサ，電流センサ等により構成されてＩＣカード１の装着状態，脱装状態を検出する脱着検出部２１３を備えている。

【００２５】

スロット部２１の接続端子２１２には、ＩＣカード１のメモリ部１１に記憶されている情報を読取るＩ／Ｏ部２２が接続されている。Ｉ／Ｏ部２２は、ＩＣカード１のメモリ部１１から読取った情報が書込まれるＲＡＭ部２３を介してＣＰＵ部２４に接続されている。スロット部２１の脱着検出部２１３は、ＣＰＵ部２４に直接接続されている。ＲＡＭ部２３には、ＣＰＵ部２４に接続した電源のバックアップ部２５が設けられている。

【００２６】

また、本体２Ａは、通信の基本構造である送受信部２７、送受信部２７への通電を電源のオン／オフにより制御する電源ボタン２８、およびアンテナ３０を備えている。送受信部２７，電源ボタン２８は、ＣＰＵ部２４に接続されている。さらに、本体２Ａは、ダイヤル入力などのように通信を指示するキー操作部２９と、通信状態などの情報を可視表示する表示部３１とを備えている。なお、本体２Ａは、マイクやスピーカを有しているが、説明を簡略にするため、図示およびその説明を省略する。

【００２７】

つぎに、通信端末装置の形状について説明する。図２はこの発明の実施の形態１による通信端末装置の外観形状を示す外観斜視図である。通信端末装置において、本体２Ａは、矩形状に形成され、上面に表示部３１，電源ボタン２８，キー操作部２９を配置させている。この本体２Ａは、内部にＲＡＭ部２３，ＣＰＵ部２４を搭載させるとともに、底面にＩＣカード１の脱着を行うためのスロット部２１を設けている。

【００２８】

つぎに、動作について説明する。図３は実施の形態１による動作を説明するフローチャートである。図１および図２に示した通信端末装置では、ＩＣカード１，本体２Ａを使用して通信を行う場合、まず使用者がＩＣカード１を本体２Ａのスロット部２１に装着する必要がある。ＩＣカード１の装着状態は、スロット部２１の脱着検出部２１３によって検出され、その検出信号がＣＰＵ部２４に送信される。ＣＰＵ部２４は、この検出信号を受け付けることでＩＣカード１の挿入（装着状態）を確認する（ステップＳ１１）。

【００２９】

続いて、ＣＰＵ部２４は電源ボタン２８のオン操作を受け入れる。すなわち、ＣＰＵ部２４は、本体２ＡへのＩＣカード１の装着が完了してから、電源投入を許可するように制御する。この後、使用者により電源ボタン２８がオン操作されると、ＣＰＵ部２４は、そのオン操作を受け付け（ステップＳ１２）、送受信部２７への通電を指示する（ステップＳ１３）。すなわち、本体２Ａ内の各ユニットに電源が投入され、アンテナ３０を通じて外部との通信準備が整うことになる。

【００３０】

ところが、ＩＣカード１が装着されない場合には（ステップＳ１１）、本体２Ａのみを入手した者が不正使用しようとしても、本体２Ａの脱着検出部２１３によってＩＣカード１の最初からの脱装状態が検出されることから、電源ボタン２８がオン操作されても、ＣＰＵ部２４により本体２Ａの送受信部２７への通電が拒否される。すなわち、本体２Ａに電源が投入されないため、通信が不可能となる。

【００３１】

以上説明したように、この実施の形態１によれば、本体２ＡにおいてＩＣカード１の装着

状態が検出された場合に電源ボタン２８の電源オン操作による電源投入を許可するようにしたので、ＩＣカード１が本体２Ａの電源投入時以外には必要なくなって、使用時でも本体２ＡとＩＣカード１とを別々に携帯することが可能になることから、本体２ＡとＩＣカード１とを同時に盗難もしくは紛失するような事態が減少し、これによって、本体２Ａだけでは電源投入ができないなどのように不正使用を有効に防止することが可能である。

【００３２】

なお、許可された使用者の間で複数の本体２…を共有して使用する場合、各使用者がもつＩＣカード１毎に電話番号やサービス情報を与えておけば、各本体２…に固有の電話番号やサービス制限を固定させる必要がなくなるので、正当な使用者がＩＣカード１さえ持っていれば、共有対象となるすべての本体２を使用することが可能である。

【００３３】

（実施の形態２）

さて、前述した実施の形態１は、ＩＣカードを本体に装着した場合にのみ本体の電源投入を許可するようにしていたが、以下に説明する実施の形態２のように、電源投入後はＩＣカードを抜き取ってから通信を行うようにしてもよい。この実施の形態２は、前述の実施の形態１による構成を適用していることから、構成の図示およびその説明を省略し、動作についての説明では図１に示した番号と同様の番号を用いて説明する。

【００３４】

ここでは、動作についてのみ説明する。図４は実施の形態２による動作を説明するフローチャートである。実施の形態２による通信端末装置では、ＩＣカード１，本体２Ａを使用して通信を行う場合、まず使用者がＩＣカード１を本体２Ａのスロット部２１に装着する必要がある。ＩＣカード１の装着状態は、スロット部２１の脱着検出部２１３によって検出され、その検出信号がＣＰＵ部２４に送信される。ＣＰＵ部２４は、この検出信号を受け付けることでＩＣカード１の挿入（装着状態）を確認する（ステップＳ２１）。

【００３５】

このようにしてＩＣカード１が本体２Ａに装着されると、そのＩＣカード１のメモリ部１１に記憶されているＩＤデータを含む制御情報がメモリ部１１から読み出され、本体２Ａ内のＲＡＭ部２３に格納される（ステップＳ２２）。したがって、ＩＣカード１が装着されていないと、ＩＤデータを含む制御情報の読み出しが行えないため、以降、通信はもちろん電源投入さえも行えないことになる。

【００３６】

続いて、ＣＰＵ部２４は、ＲＡＭ部２３に格納されたＩＤデータの正当性を確認するため、そのＩＤデータとＣＰＵ部２４自身があらかじめ記憶しているＩＤデータとを照合して、一致か、それとも不一致かを判断する（ステップＳ２３）。その結果、一致が確認された場合にのみ、ＣＰＵ部２４は電源ボタン２８のオン操作を受け入れる。すなわち、ＣＰＵ部２４は、ＩＤデータの正当性を確認してから、電源投入を許可するように制御する。

【００３７】

この後、使用者により電源ボタン２８がオン操作されると、ＣＰＵ部２４は、そのオン操作を受け付け（ステップＳ２４）、内部への通電を指示する（ステップＳ２５）。すなわち、本体２Ａ内の各ユニットに電源が投入される。ところが、この段階では、まだアンテナ３０を通じて外部との通信準備が整わず、続いてＩＣカード１の脱着状態が確認される（ステップＳ２６）。

【００３８】

すなわち、脱着検出部２１３によりＩＣカード１の脱着状態が検出される。その際、ＩＣカード１が装着状態で検出された場合には通信準備が整わないものとして、ＩＣカード１が抜き取られるまでは通信は不許可となる（ステップＳ２８）。一方、ＩＣカード１が脱装状態で検出された場合には通信準備が整ったものとして、通信が許可される（ステップＳ２７）。

【００３９】

なお、ＩＤの不一致（ステップＳ２３）やＩＤ一致後の電源未投入（ステップＳ２４）の

際には、通信不許可として処理が終了する（ステップＳ２８）。

【００４０】

以上説明したように、実施の形態２によれば、本体２ＡにおいてＩＣカード１の脱装状態が検出された場合に通信を許可するようにしたので、使用時の段階で本体２ＡとＩＣカード１とは別々に携帯され、本体２ＡとＩＣカード１とを同時に盗難もしくは紛失するような事態が未然に防止され、これによって、本体２Ａだけでは電源投入ができないなどのように不正使用を有効に防止することが可能である。

【００４１】

また、本体２Ａに装着されたＩＣカード１のＩＤデータと本体２Ａにあらかじめ記憶された識別情報とを照合し、その照合により一致が得られ、かつＩＣカード１の脱装状態が検出された場合にのみ、通信を許可するようにしたので、使用時の段階で本体２ＡとＩＣカード１とは別々に携帯され、適合するＩＣカード１と本体２Ａとの双方を入手しない限り使用できず、これによって、不正使用を有効に防止することが可能である。

【００４２】

（実施の形態３）

さて、前述の実施の形態１，２では、通信を開始するに当たってのセキュリティを具体化したものであったが、以下に説明する実施の形態３のように、通信が一旦終了すると、その段階で通信を許可するための情報をすべて抹消するようにしてもよい。

【００４３】

この実施の形態３は、前述の実施の形態１による構成を適用していることから、構成の図示およびその説明を省略し、動作についての説明では図１に示した番号と同様の番号を用いて説明する。

【００４４】

ここでは、動作についてのみ説明する。図５は実施の形態３による動作を説明するフローチャートである。この実施の形態３において、実施の形態２による通信が行われている場合には、ＩＣカード１から読み出したＩＤ情報などの制御情報がＲＡＭ部２３に格納済みとなる。

【００４５】

実施の形態２による通信は、ＩＣカード１の脱装状態が条件となっていることから、ＩＣカード１が脱装された状態で実施される。また、実施の形態１，２において、ＩＣカード１の装着で電源投入が許可されることから、この実施の形態３の前提が実施の形態１，２であれば、本体２が動作中のときにはＩＣカード１が装着状態となる。

【００４６】

このため、実施の形態２を前提とした場合、通信中であればステップＳ３１においてＩＣカード１の脱装状態が確認され（ステップＳ３１）、続くステップＳ３２において電源ボタン２８によるオフ操作が検出される。また、実施の形態１，２を前提とした場合には、通信中でなければ、ステップＳ３１においてその時の脱着検出部２１３の検出状態からＩＣカード１の脱着状態が判断される。

【００４７】

いずれにしても、ＩＣカード１が抜き取られていない場合、すなわちＩＣカード１の装着状態が保持されているのであれば（ステップＳ３１）、電源の切断は許可されず、現状が保持されたまま処理は終了する。

【００４８】

一方、ＩＣカード１が抜き取られ、ＩＣカード１の脱装状態が確認された場合には（ステップＳ３１）、電源の切断が許可されるので、その後、電源ボタン２８が電源オフ操作されると（ステップＳ３２）、ＲＡＭ部２３に記憶されているＩＣカード１の制御情報がすべて消去される（ステップＳ３３）。

【００４９】

以上説明したように、実施の形態３によれば、本体２ＡにおいてＩＣカード１の脱装状態が検出された場合に電源ボタン２８による電源オフ操作があると、ＩＣカード１から読み

出してＲＡＭ部２３に記憶しておいた制御情報を消去するようにしたので、その制御情報がなくなることで電源オフ後の本体２Ａの再使用ができなくなり、これによって、本体２Ａだけでは再使用ができないなどのように不正使用を有効に防止することが可能である。

【００５０】

（実施の形態４）

さて、前述した実施の形態１～３は、ＩＣカードの脱着状態に従って本体の動作を決定していたが、以下に説明する実施の形態４のように、ＩＣカードと本体との両方が意志に反して第三者の手に渡った場合にも、時間的に期限を与えることで不正使用による被害を最小限を抑えるようにしてもよい。

【００５１】

まず、構成について説明する。図６はこの発明の実施の形態４による通信端末装置の内部構成を示すブロック図である。実施の形態４による通信端末装置は、本体２ＢとＩＣカード１との組み合わせで構成される。本体２Ｂは、全体的には図１に示した本体２Ａと同様の構成を有することから、同様のユニットには同様の番号を付し、その説明を省略する。

【００５２】

本体２Ｂにおいては、前述のＣＰＵ部２４に時刻を測定して現時刻を得る時刻測定部３２が設けられており、この追加構成が本体２Ａと構成上で相違する。なお、ＩＣカード１については共通とするが、制御情報の中に、ＩＣカード１の有効期限が時間的な情報として含まれている。この情報を以下に時間的有効期限情報と称する。この時間的有効期限情報は、図６に示した如く、ＩＣカード１のメモリ部１１にあらかじめ記憶されている。

【００５３】

つぎに、動作について説明する。図７は実施の形態４による動作を説明するフローチャートである。前述の実施の形態２と同様に、本体２Ｂのスロット部２１にＩＣカード１が装着されると（ステップＳ４１）、ＩＣカード１のメモリ部１１に記憶されている時間的有効期限情報を含む制御情報が本体２ＢのＲＡＭ部２３に格納される（ステップＳ４２）。

【００５４】

ＣＰＵ部２４は、ＲＡＭ部２３に格納された時間的有効期限情報と時刻測定部３２から得られる時刻データとを比較して、ＩＣカード１による通信が有効か、それとも無効かを判断する（ステップＳ４３）。すなわち、時間的有効期限情報が現時刻よりも先（未来）の期限を表していた場合には、ＩＣカード１による通信は有効として許可される（ステップＳ４４）。

【００５５】

一方、時間的有効期限情報が現時刻よりも以前（過去）の期限を表していた場合には、ＩＣカード１による通信は無効として不許可となる（ステップＳ４５）。なお、このステップＳ４３からの判定では、ＲＡＭ部２３に書込まれた制御情報内のＩＤデータとＣＰＵ部２４があらかじめ記憶しているＩＤデータとの照合一致を前提条件としてもよい。

【００５６】

以上説明したように、実施の形態４によれば、本体２ＢにおいてＩＣカード１の装着状態が検出された場合にＩＣカード１に記憶された期限情報と本体２Ｂで測定した時刻情報との比較から時間的有効可否を判断し、その判断により時間的に有効であるという判断結果が得られた場合に通信を許可するようにしたので、本体２ＢとＩＣカード１とを同時に盗難もしくは紛失するような事態が生じてもその使用に時間的制限が与えられ、これによって、永続的な不正使用を有効に防止することが可能である。

【００５７】

なお、この実施の形態４では、前述の実施の形態２を組み合わせて、ステップＳ４３で有効の判断が下された後に、電源ボタン２８の電源オン操作と、ＩＣカード１の抜き取りとを条件としてもよい。

【００５８】

（実施の形態５）

さて、前述した実施の形態１～３は、ＩＣカードの脱着状態に従って本体の動作を決定し

ていたが、以下に説明する実施の形態５のように、ＩＣカードと本体との両方が意思に反して第三者の手に渡った場合にも、回数的に期限を与えることで不正使用による被害を最小限を抑えるようにしてもよい。

【００５９】

まず、構成について説明する。図８はこの発明の実施の形態５による通信端末装置の内部構成を示すブロック図である。実施の形態５による通信端末装置は、本体２ＣとＩＣカード１との組み合わせで構成される。本体２Ｃは、全体的には図１に示した本体２Ａと同様の構成を有することから、同様のユニットには同様の番号を付し、その説明を省略する。

【００６０】

本体２Ｃにおいては、前述のＣＰＵ部２４にレジスタ３３が設けられ、そのレジスタ３３には、ＩＣカード１の使用回数を制限するための値すなわち回数比較データがあらかじめ記憶される。この追加構成が本体２Ａと構成上で相違する。

【００６１】

なお、ＩＣカード１については共通とするが、制御情報の中に、ＩＣカード１の有効期限が回数的な情報として含まれている。この情報を以下に回数的有効期限情報と称する。この回数的有効期限情報は、図８に示した如く、ＩＣカード１のメモリ部１１に記憶され、ＩＣカード１を一回使用する度に更新される。すなわち、この回数的有効期限情報は使用の度に１ずつ減算される値を示すものである。

【００６２】

つぎに、動作について説明する。図９は実施の形態５による動作を説明するフローチャートである。前述の実施の形態２と同様に、本体２Ｃのスロット部２１にＩＣカード１が装着されると（ステップＳ５１）、ＩＣカード１のメモリ部１１に記憶されている回数的有効期限情報を含む制御情報が本体２ＣのＲＡＭ部２３に格納される（ステップＳ５２）。

【００６３】

ＣＰＵ部２４は、ＲＡＭ部２３に格納された回数的有効期限情報とレジスタ３３にあらかじめ記憶しておいた回数比較データとを比較して、ＩＣカード１による通信が有効か、それとも無効かを判断する（ステップＳ５３）。すなわち、回数的有効期限情報に基づく回数が“０”（回数比較データの値）に到達していなければ、今回の使用を含めて１回以上の使用残数があることから、今回の１回分が減算されてから（ステップＳ５４）、ＩＣカード１による通信は有効として許可される（ステップＳ５５）。

【００６４】

一方、回数的有効期限情報に基づく回数が“０”に到達していれば、今回の使用を含めて１回も使用残数がないことから、ＩＣカード１による通信は無効として不許可となる（ステップＳ５６）。なお、このステップＳ５３からの判定では、ＲＡＭ部２３に書込まれた制御情報内のＩＤデータとＣＰＵ部２４があらかじめ記憶しているＩＤデータとの照合一致を前提条件としてもよい。

【００６５】

以上説明したように、実施の形態５によれば、本体２ＣにおいてＩＣカード１の装着状態が検出された場合に、ＩＣカード１の使用の度に減算されてＩＣカード１に記憶された回数的有効期限情報と本体２Ｃに予め記憶された回数比較データとの比較から回数的有効可否を判断し、その判断により回数的に有効であるという判断結果が得られた場合に通信を許可するようにしたので、本体２ＣとＩＣカード１とを同時に盗難もしくは紛失するような事態が生じてもその使用に回数的制限が与えられ、これによって、永続的な不正使用を有効に防止することが可能である。

【００６６】

なお、この実施の形態５では、前述の実施の形態２を組み合わせて、ステップＳ４３で有効の判断が下された後に、電源ボタン２８の電源オン操作と、ＩＣカード１の抜き取りとを条件としてもよい。

【００６７】

（実施の形態６）

さて、前述した実施の形態５は、回数的有効期限情報をカウントダウン式に行うようにしていたが、以下に説明する実施の形態６のように、回数的有効期限情報をカウントアップ式に行うようにしてもよい。

【００６８】

この実施の形態６は、回数的有効期限情報の扱い方が前述の実施の形態５と異なる他は、すべて同様となることから、以下に動作についてのみ説明する。この実施の形態６において、回数的有効期限情報は使用の度に１ずつ加算される値を示し、回数比較データは予め指定された回数（指定回数）を示す。

【００６９】

図１０は実施の形態６による動作を説明するフローチャートである。前述の実施の形態２と同様に、本体２ＣのスロットＩＣカード１が装着されると（ステップＳ６１）、ＩＣカード１のメモリ部１１に記憶されている回数的有効期限情報を含む制御情報が本体２ＣのＲＡＭ部２３に格納される（ステップＳ６２）。

【００７０】

ＣＰＵ部２４は、ＲＡＭ部２３に格納された回数的有効期限情報とレジスタ３３にあらかじめ記憶しておいた回数比較データとを比較して、ＩＣカード１による通信が有効か、それとも無効かを判断する（ステップＳ６３）。すなわち、回数的有効期限情報に基づく回数が指定回数＋１に到達していなければ、指定回数を超えておらず、今回の使用を含めて１回以上の使用残数があることから、今回の１回分が加算されてから（ステップＳ６４）、ＩＣカード１による通信は有効として許可される（ステップＳ６５）。

【００７１】

一方、回数的有効期限情報に基づく回数が指定回数＋１に到達していれば、今回の使用を含めて１回も使用残数がないことから、ＩＣカード１による通信は無効として不許可となる（ステップＳ６６）。なお、このステップＳ６３からの判定では、ＲＡＭ部２３に書込まれた制御情報内のＩＤデータとＣＰＵ部２４があらかじめ記憶しているＩＤデータとの照合一致を前提条件としてもよい。

【００７２】

以上説明したように、実施の形態６によれば、本体２ＣにおいてＩＣカード１の装着状態が検出された場合に、ＩＣカード１の使用の度に加算されてＩＣカード１に記憶された回数的有効期限情報と本体２Ｃに予め記憶された回数比較データとの比較から回数的有効可否を判断し、その判断により回数的に有効であるという判断結果が得られた場合に通信を許可するようにしたので、本体２ＣとＩＣカード１とを同時に盗難もしくは紛失するような事態が生じてもその使用に回数的制限が与えられ、これによって、永続的な不正使用を有効に防止することが可能である。

【００７３】

なお、この実施の形態６では、前述の実施の形態２を組み合わせて、ステップＳ４３で有効の判断が下された後に、電源ボタン２８の電源オン操作と、ＩＣカード１の抜き取りとを条件としてもよい。

【００７４】

（実施の形態７）

さて、前述した実施の形態１～６は、ＩＣカードの脱装状態や制御情報に従って本体の通信機能に対する制御を行うものであったが、以下に説明する実施の形態７のように、ブースタなどの外部通信機器を接続させて通信を行う場合にもＩＣカードの制御情報に従って行うようにしてもよい。

【００７５】

なお、この実施の形態７は、基本構成を実施の形態１の構成としていることから、以下に外部通信機器とのシステム構成と動作上の説明のみ行うものとする。

【００７６】

図１１はこの発明の実施の形態７による通信端末装置とオプション機器（外部通信機器）とのシステム構成を示す構成図である。実施の形態７による通信端末装置は、本体２Ｄと

ＩＣカード１との組み合わせで構成される。本体２Ｄは、全体的には図１に示した本体２Ａと同様の構成を有することから、その説明を省略する。図１１に示すように、本体２Ｄには、図示せぬコネクタを通じてブースタ３のようなオプション機器が接続されている。このブースタ３には、さらに無線通信を行うためのアンテナ４が接続されてる。

【００７７】

つぎに、動作について説明する。図１２は実施の形態７による動作を説明するフローチャートである。前提として、ＩＣカード１のメモリ部１１には、オプション機器使用可否情報があらかじめ記憶されている。このオプション機器使用可否情報は、本体２Ｄに対して使用可能なオプション機器と使用不能なオプション機器とを判断させる情報である。

【００７８】

前述の実施の形態２と同様に、本体２Ｄのスロット部２１にＩＣカード１が装着されると（ステップＳ７１）、ＩＣカード１のメモリ部１１に記憶されているオプション機器使用可否情報を含む制御情報が本体２ＤのＲＡＭ部２３に格納される（ステップＳ７２）。ＣＰＵ部２４は、ＲＡＭ部２３に格納されたオプション機器使用可否情報を解析して、現在図１１に示した如く接続されたブースタ３による通信が有効か、それとも無効かを判断する（ステップＳ７３）。

【００７９】

その結果、オプション機器使用可否情報によりブースタ３の使用が認められていれば、ブースタ３による通信は有効として許可される（ステップＳ７４）。一方、オプション機器使用可否情報によりブースタ３の使用が認められていなければ、ブースタ３による通信は無効として不許可となる（ステップＳ７５）。なお、このステップＳ７３からの判定では、ＲＡＭ部２３に書込まれた制御情報内のＩＤデータとＣＰＵ部２４があらかじめ記憶しているＩＤデータとの照合一致を前提条件としてもよい。

【００８０】

以上説明したように、実施の形態７によれば、本体２ＤにおいてＩＣカード１の装着状態が検出された場合にＩＣカード１に記憶されたブースタ３の如く外部通信機器について本体２Ｄでの使用可否を示す情報に従って本体自身に接続された外部通信機器の使用可否を判断し、その判断により使用可であるという判断結果が得られた場合に接続された外部通信機器を用いた通信を許可するようにしたので、外部通信機器を接続しただけでは通信が行えず、これによって、外部通信機器を用いた不正使用を有効に防止することが可能である。

【００８１】

なお、この実施の形態７では、前述の実施の形態２を組み合わせて、ステップＳ４３で有効の判断が下された後に、電源ボタン２８の電源オン操作と、ＩＣカード１の抜き取りとを条件としてもよい。

【００８２】

【発明の効果】

以上説明したように、この発明によれば、本体においてＣＰＵによりカードの装着状態が検出された場合にカードに記憶された識別情報を含む制御情報を記憶手段により記憶し、記憶手段に記憶された識別情報とあらかじめ記憶された識別情報とを照合し、その照合により一致が得られた場合にのみ電源ボタンの電源オン操作による電源投入を許可し、かつ、前記脱着検出手段及びＣＰＵによりカードの抜き取りが検出された場合にのみ通信手段による通信を許可するようにしたので、使用時の段階で本体とカードとは別々に携帯され、本体とカードとを同時に盗難もしくは紛失するような事態が未然に防止され、これによって、本体だけでは電源投入ができず、不正使用を有効に防止することが可能な通信端末装置が得られるという効果を奏する。

つぎの発明によれば、カードの抜き取りが検出された場合に電源ボタンによる電源オフ操作があると、カードから読み出して記憶しておいた識別情報を含む制御情報を消去するようにしたので、電源オフ後の本体の再使用ができなくなり、これによって、本体だけでは再使用ができないなどのように不正使用を有効に防止することが可能な通信端末装置が

得られるという効果を奏する。

【００８３】

つぎの発明によれば、カードの装着状態が検出された場合にカードに記憶された外部通信機器について本体での使用可否を示す情報に従って本体自身に接続された外部通信機器の使用可否を判断し、その判断により使用可であるという判断結果が得られた場合に接続された外部通信機器を用いた通信を許可するようにしたので、外部通信機器を接続しただけでは通信が行えず、これによって、外部通信機器を用いた不正使用を有効に防止することが可能な通信端末装置が得られるという効果を奏する。

【図面の簡単な説明】

【図１】　この発明の実施の形態１による通信端末装置の内部構成を示すブロック図である。

【図２】　この発明の実施の形態１による通信端末装置の外観形状を示す外観斜視図である。

【図３】　実施の形態１による動作を説明するフローチャートである。

【図４】　実施の形態２による動作を説明するフローチャートである。

【図５】　実施の形態３による動作を説明するフローチャートである。

【図６】　この発明の実施の形態４による通信端末装置の内部構成を示すブロック図である。

【図７】　実施の形態４による動作を説明するフローチャートである。

【図８】　この発明の実施の形態５による通信端末装置の内部構成を示すブロック図である。

【図９】　実施の形態５による動作を説明するフローチャートである。

【図１０】　実施の形態６による動作を説明するフローチャートである。

【図１１】　この発明の実施の形態７による通信端末装置と外部通信機器とのシステム構成を示す構成図である。

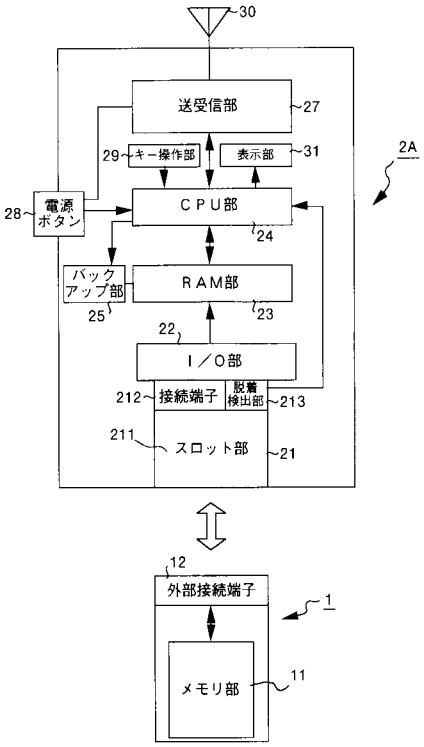
【図１２】　実施の形態７による動作を説明するフローチャートである。

【図１３】　従来例による通信端末装置の構成を示すブロック図である。

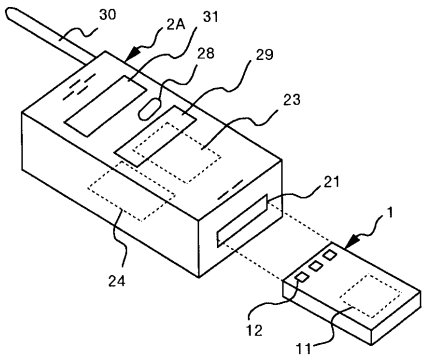
【符号の説明】

１　ＩＣカード、２Ａ，２Ｂ，２Ｃ，２Ｄ　本体、３　ブースタ、１１　メモリ部、２３　ＲＡＭ部、２４　ＣＰＵ部、２７　送受信部、２８　電源ボタン、３２　時刻測定部、３３　レジスタ、２１３　脱着検出部。

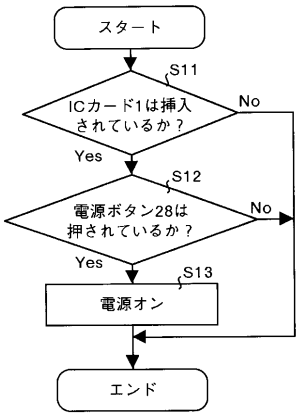
【図１】


30
送受信部
27
29
キー操作部
表示部
31
2A
28
電源ボタン
ＣＰＵ部
24
バックアップ部
25
ＲＡＭ部
23
22
Ｉ／Ｏ部
212
接続端子
脱着検出部
213
211
スロット部
21
12
外部接続端子
1
メモリ部
11

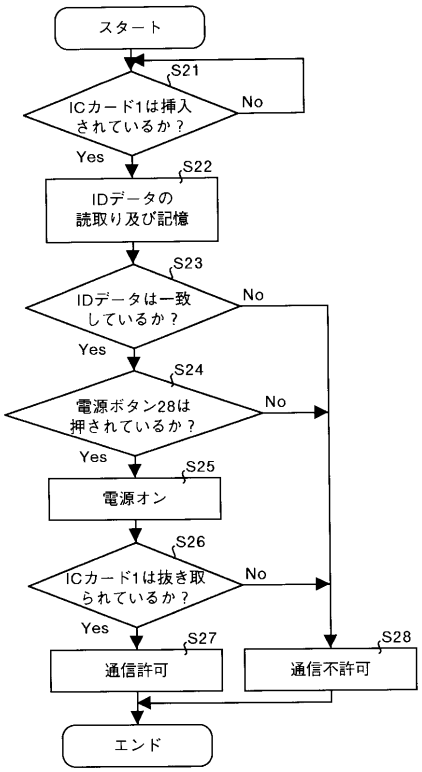
【図２】


30
2A
31
28
29
23
21
1
24
12
11

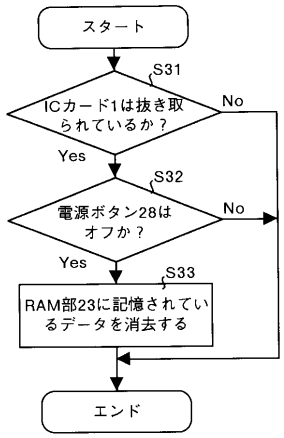
【図３】


スタート
S11
ICカード1は挿入されているか？
No
Yes
S12
電源ボタン28は押されているか？
No
Yes
S13
電源オン
エンド

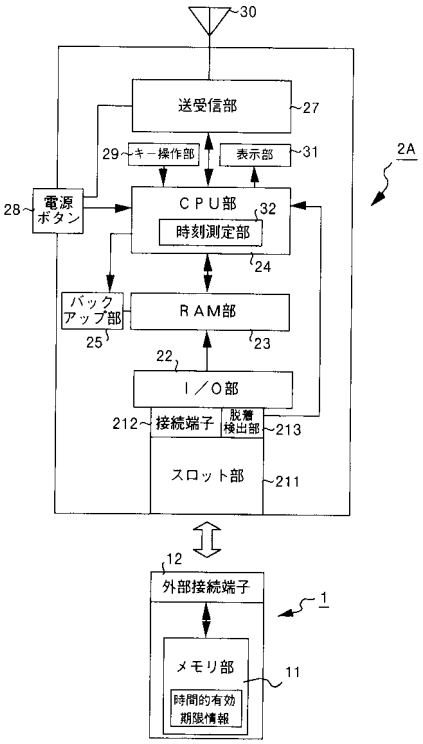
【図４】


スタート
S21
ICカード1は挿入されているか？
No
Yes
S22
IDデータの読取り及び記憶
S23
IDデータは一致しているか？
No
Yes
S24
電源ボタン28は押されているか？
No
Yes
S25
電源オン
S26
ICカード1は抜き取られているか？
No
Yes
S27
通信許可
S28
通信不許可
エンド

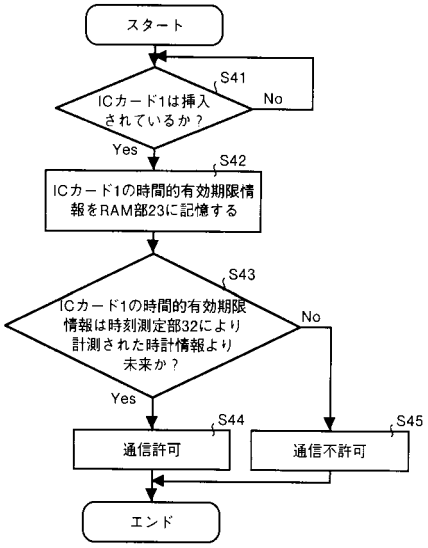
【図５】


スタート
S31
ICカード1は抜き取られているか？
No
Yes
S32
電源ボタン28はオフか？
No
Yes
S33
RAM部23に記憶されているデータを消去する
エンド

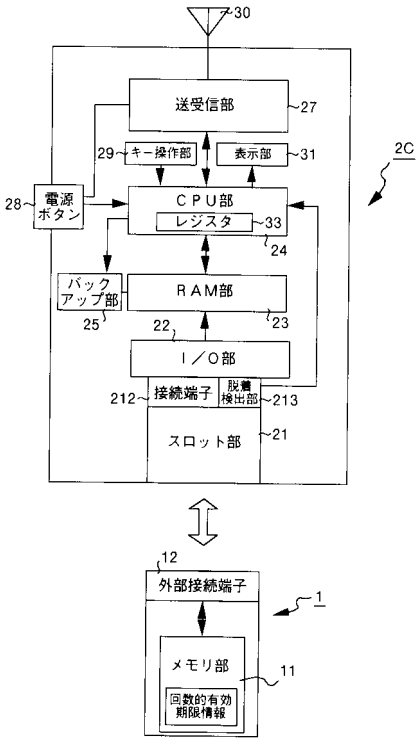
【図６】


30
送受信部
27
29
キー操作部
表示部
31
2A
28
電源ボタン
CPU部
32
時刻測定部
24
バックアップ部
25
RAM部
23
22
I／O部
212
接続端子
脱着検出部
213
スロット部
211
12
外部接続端子
1
メモリ部
11
時間的有効期限情報

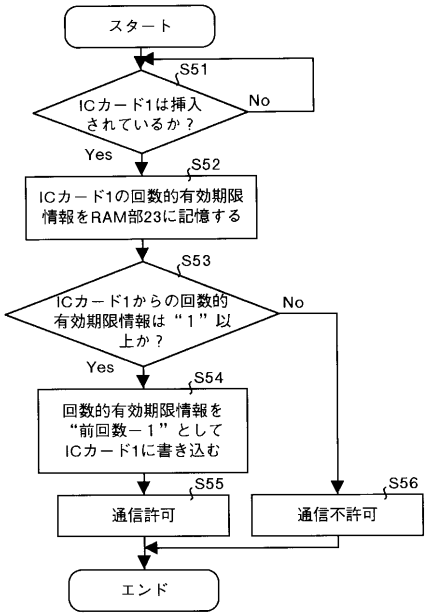
【図７】


スタート
S41
ICカード1は挿入されているか？
No
Yes
S42
ICカード1の時間的有効期限情報をRAM部23に記憶する
S43
ICカード1の時間的有効期限情報は時刻測定部32により計測された時計情報より未来か？
No
Yes
S44
通信許可
S45
通信不許可
エンド

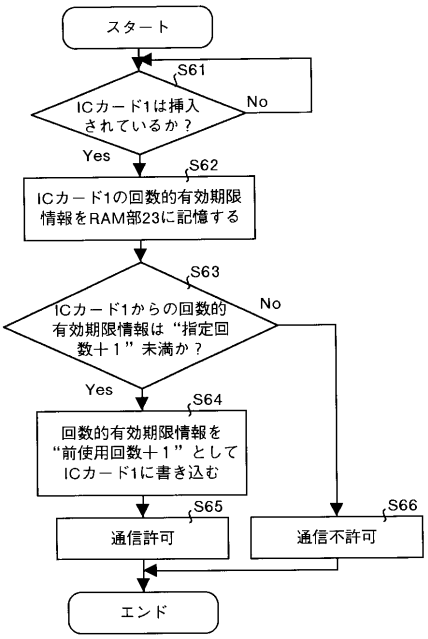
【図８】


30
送受信部
27
29
キー操作部
表示部
31
2C
28
電源ボタン
CPU部
レジスタ
33
24
バックアップ部
25
RAM部
23
22
I／O部
212
接続端子
脱着検出部
213
スロット部
21
12
外部接続端子
1
メモリ部
11
回数的有効期限情報

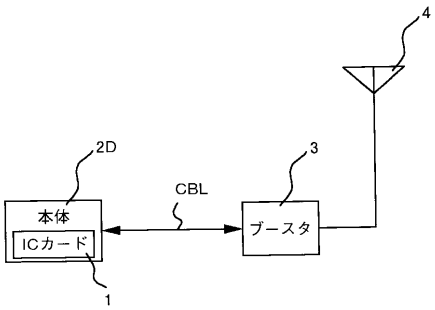
【図９】



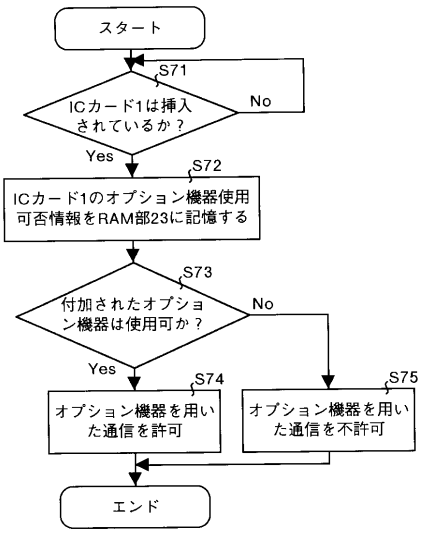
【図１０】



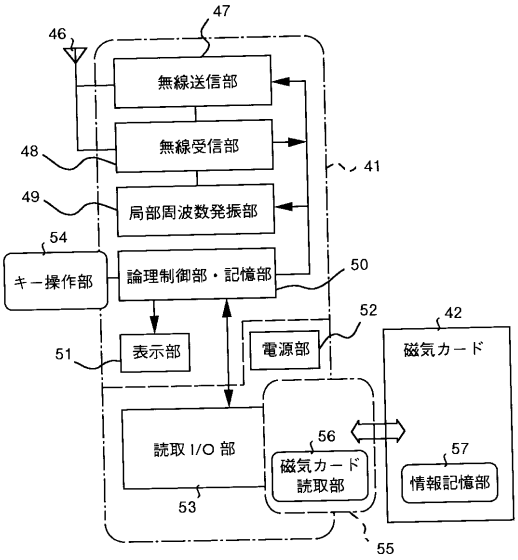
【図１１】



【図１２】



【図１３】


47
46
無線送信部
無線受信部
48
41
49
局部周波数発振部
54
キー操作部
論理制御部・記憶部
50
52
42
磁気カード
51
表示部
電源部
読取 I/O 部
56
57
磁気カード
読取部
情報記憶部
53
55

フロントページの続き

(56)参考文献 特開平０４－０１４９１６（ＪＰ，Ａ）
特開昭６４－０８１４５７（ＪＰ，Ａ）
特開平０８－２５１６４１（ＪＰ，Ａ）
特開平０３－２８６６５９（ＪＰ，Ａ）
特開昭６３－０３３０４６（ＪＰ，Ａ）
特開平０８－１２５７２１（ＪＰ，Ａ）
特開平０９－０８４１３７（ＪＰ，Ａ）
特開昭６２－０３６９２７（ＪＰ，Ａ）
実開昭６１－１９９９６０（ＪＰ，Ｕ）
特開平０９－０９８４８０（ＪＰ，Ａ）
特開平０８－１６７９２７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04M 1/66