(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3929888号
(P3929888)
(45)発行日　平成19年6月13日(2007.6.13)　(24)登録日　平成19年3月16日(2007.3.16)

(51)Int.Cl.　　F I
G06K 19/073 (2006.01)　　G06K 19/00 P
G06K 19/07 (2006.01)　　G06K 19/00 N

請求項の数 5　(全 16 頁)

(21)出願番号　特願2002-373565(P2002-373565)
(22)出願日　平成14年12月25日(2002.12.25)
(65)公開番号　特開2004-206331(P2004-206331A)
(43)公開日　平成16年7月22日(2004.7.22)
審査請求日　平成16年6月9日(2004.6.9)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100109900
弁理士　堀口　浩
(72)発明者　小島　健司
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内
(72)発明者　梅澤　健太郎
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内
(72)発明者　三宅　秀享
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内

最終頁に続く

(54)【発明の名称】ＩＣカード

(57)【特許請求の範囲】
【請求項１】
利用時に外部の端末と電気的に接続し、電力供給を受けて所定の処理を行うＩＣカードにおいて、
このＩＣカードに固有の認証情報を記憶する記憶手段と、
利用時に該端末より送信される認証情報を入力する入力手段と、
ソース領域とドレイン領域と該ソース領域および該ドレイン領域との間のチャネル領域とからなる第１層と、該第１層に積層されるトンネル絶縁膜からなる第２層と、該第２層に積層されるゲートからなる第３層とを有し、電力供給されると該チャネル領域の基板界面と該ゲートとの間に高電界を印加し該チャネル領域から該ゲートへ電子を注入し、その後電力供給を受けることなく時間とともに前記ゲートに注入した電子が減少することにより、利用時外のときに電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により該経時変化部の電子量を測定し時間計測中であるか否かを示す信号を出力する経時変化タイマと、
前記入力手段からの認証情報を、前記記憶手段の認証情報と照合し、一致するか一致しないかを判断する判断手段と、
前記判断手段によって一致しないと判断された場合に、前記経時変化部への電力供給を指示するよう制御し、前記経時変化タイマが計測中である場合には、前記所定の処理を行わないように制御する制御手段とを、備えたことを特徴とするＩＣカード。
【請求項２】

利用時に外部の端末と電気的に接続し、電力供給を受けて所定の処理を行うＩＣカードにおいて、
このＩＣカードに固有の認証情報を記憶する記憶手段と、
利用時に該端末より送信される認証情報を入力する入力手段と、
ソース領域とドレイン領域と該ソース領域および該ドレイン領域との間のチャネル領域とからなる第１層と、該第１層に積層されるトンネル絶縁膜からなる第２層と、該第２層に積層されるゲートからなる第３層とを有し、電力供給されると該チャネル領域の基板界面と該ゲートとの間に高電界を印加し該チャネル領域から該ゲートへ電子を注入し、その後電力供給を受けることなく時間とともに前記ゲートに注入した電子が減少することにより、利用時外のときに電力供給を受けずに経時変化する第一経時変化部を有し、該電力供給中に所定の指示により該第一経時変化部の電子量を測定し時間計測中であるか否かを示す信号を出力する第一経時変化タイマと、
前記入力手段からの認証情報を、前記記憶手段の認証情報と照合し、一致するか一致しないかを判断する第一判断手段と、
前記第一判断手段によって一致しないと判断される回数を、少なくとも予め定めた上限値までカウントするカウント手段と、
前記カウント手段でカウントされた回数が上限値になった場合に、前記第一経時変化部への電力供給を指示するよう制御し、前記第一経時変化タイマが計測中である場合には、前記所定の処理を行わないように制御する制御手段とを備えたことを特徴とするＩＣカード。

【請求項３】
利用時外のときにも電力供給を受けずに、前記第一経時変化タイマの経時変化部とは経時変化が異なる第二経時変化部を有し、該電力供給中に所定の指示により該第二経時変化部の電子量を測定し時間計測中であるか否かを示す信号を出力する第二経時変化タイマを更に備え、
前記制御手段は、前記第一判断手段で不正であると判断された都度、前記第二経時変化部への電力供給を指示するようにしたことを特徴とする請求項２記載のＩＣカード。

【請求項４】
利用時外のときにも電力供給を受けずに、前記第一経時変化タイマの経時変化部とは経時変化が異なる第二経時変化部を有し、該電力供給中に所定の指示により該第二経時変化部の電子量を測定し時間計測中であるか否かを示す信号を出力する第二経時変化タイマを更に備え、
この第二経時変化タイマは、前記カウント手段でカウントが開始される時点から所定期間計測するものであることを特徴とする請求項２記載のＩＣカード。

【請求項５】
前記第一経時変化タイマが未計測で、前記第二経時変化タイマが計測中で、前記第一判断手段で正当であると判断されたとき、前記第二経時変化タイマの計測を終了するようにしたことを特徴とする請求項３または４いずれかに記載のＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】
本発明は、接触型で、電池を備えないＩＣカードに係り、特に、所有者の誤入力による不備と他人のなりすましによる不正利用とを考慮したＩＣカード、ＩＣカードの不正利用防止方法、および、プログラムに関する。

【０００２】

【従来の技術】
ＩＣカードは、個人情報をはじめとした重要情報を記録し利用するため、紛失時の正当な所有者以外の者による不正利用を防止する必要がある。このため、一般的なＩＣカードでは、ＩＣカードを利用する際には、ＩＣカードの正当な所有者（これを単に所有者と呼ぶ）を認証するために、ＰＩＮ（Ｐｅｒｓｏｎａｌ Ｉｎｆｏｒｍａｔｉｏｎ Ｎｕｍｂｅｒ

）による認証（これをＰＩＮ認証と呼ぶ）が行われている。通常、正当なＰＩＮの情報はＩＣカード内に記憶されており、所有者はＩＣカードを挿入した端末装置よりＰＩＮを入力し、そのＰＩＮがＩＣカード内で正当なＰＩＮと照合された後、照合結果が端末装置に返される（例えば、特許文献１参照）。

【０００３】

このＰＩＮ認証では、他人のＩＣカードを手に入れた攻撃者が、所有者のＰＩＮを推定し入力することで正当な所有者になりすます恐れがある。このようなＰＩＮ推定攻撃に対する対策としては、不正なＰＩＮが連続して一定回数入力された時点でＩＣカードをロック（これをＩＣカードのＰＩＮロックと呼ぶ）するという方法が行われている。ＰＩＮロックされたＩＣカードには、それ以上ＰＩＮを入力することはできず使用不可能となる。なお、ＰＩＮロックは、システム側で行う方式とＩＣカード側で行う方式とがある。

【０００４】

このようなＰＩＮロックは、不正な攻撃者に対しての対策であったが、所有者も誤って不正なＰＩＮの入力を行ってＰＩＮロックされてしまうことがある。この場合には、システムの管理者などに連絡し面倒な手続を行って、ロックを解除してもらう必要があり、所有者にとって使い勝手が悪かった。

【０００５】

【特許文献１】

特開２０００－７６４０２公報

【０００６】

【発明が解決しようとする課題】

ところで、従来技術で説明したＩＣカードのＰＩＮロックは、ロックする時間を一定時間とすることができれば、正当なユーザには、特に管理者等へ連絡を行って面倒な手続を行うことなく、（しばらくは利用できないが）再び利用できるようになり、また、不正なユーザには、連続的に推定攻撃ができなくなるようになる。従って、ロックする時間を一定時間とすることが望まれていた。

【０００７】

しかしながら、ＰＩＮロックをシステム側で行う方式では、システム側の端末装置を集中管理するサーバ装置によってＰＩＮロックを管理するためのロック管理情報を集中管理しておき、ＰＩＮ認証が行われる都度、管理されるロック管理情報をアクセスして判断する必要があり、処理が重くなる。

【０００８】

そこで、ＰＩＮロックをＩＣカード側で行う方式で実現したいが、ＩＣカード単体時には電力供給を得ることができないので、一定時間を計測することができなかった。なお、電池を内蔵することが考えられるが、これでは、電池が不要なＩＣカードのメリットを生かせない。

【０００９】

本発明は、上記問題点に鑑みなされたものであり、端末装置や処理サーバなどのシステム側に負担をかけず、電力供給の無い状態でも所定期間のＰＩＮロックを実現できるＩＣカード、ＩＣカードの不正利用防止方法、および、プログラムを提供することを目的とする。

【００１０】

【課題を解決するための手段】

本発明は、利用時に外部の端末と電気的に接続し、電力供給を受けて所定の処理を行うＩＣカードにおいて、このＩＣカードに固有の認証情報を記憶する記憶手段と、利用時に該端末より送信される認証情報を入力する入力手段と、利用時外のときにも電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する経時変化タイマと、前記入力手段からの認証情報を、前記記憶手段の認証情報と照合し、一致するか一致しないかを判断する判断手段と、前記判断手段によって一致しないと判断された場合に、前記経時変化タイマへ計測の開始を指示するとともに

、前記経時変化タイマの計測中には、前記所定の処理を行わないように制御する制御手段とを備えた。

【００１１】

また、本発明は、利用時に外部の端末と電気的に接続し、電力供給を受けて所定の処理を行うＩＣカードにおいて、このＩＣカードに固有の認証情報を記憶する記憶手段と、利用時に該端末より送信される認証情報を入力する入力手段と、利用時外のときにも電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する第一経時変化タイマと、前記入力手段からの認証情報を、前記記憶手段の認証情報と照合し、一致するか一致しないかを判断する第一判断手段と、前記第一判断手段によって一致しないと判断される回数を、少なくとも予め定めた上限値までカウントするカウント手段と、前記カウント手段でカウントされた回数が上限値になった場合に、前記第一経時変化タイマへ計測の開始を指示するとともに、前記第一経時変化タイマの計測中には、前記所定の処理を行わないように制御する制御手段とを備えた。

【００１２】

このようにした本発明のＩＣカードは、ＩＣカード側で、一定時間のＰＩＮロックを可能にすることができ、ＩＣカードへのＰＩＮの推定攻撃に対する安全性を確保しつつ、利用者の利便性も確保できる。

【００１３】

【発明の実施の形態】

以下、本発明の実施形態について、図面を参照しつつ詳細に説明する。

【００１４】

図１は、本実施の形態に係る全体システムを示したものであり、ＩＣカード端末１０と、接触型のＩＣカード２０とからなる。なお、ＩＣカード端末１０は、ネットワークを介して、多数のＩＣカード端末１０を集中管理するサーバ等と接続されていて良いことは、勿論である。

【００１５】

接触型のＩＣカード２０は、プラスチックでカード状の定格サイズで形成されたプラスチック部材２５と、所定の論理動作を行うＩＣチップ２２を封止材２３で封止し、このＩＣチップ２２と接続され、外部に露出するＩＣカードインタフェース２１を備えるＩＣモジュール２４とを備え、ＩＣカード端末１０へ挿入中に、ＩＣカード端末１０からの電源供給を受けて、ＩＣチップ２２が動作し、一方、ＩＣカード端末１０へ挿入されない時は動作しないものである。

【００１６】

ＩＣカード端末１０は、ＩＣカード２０を挿入するための挿入部１１と、挿入部１１にＩＣカード２０が挿入された際に、ＩＣカード２０と電気的に接続するＩＣカードインタフェース１３とを備える。ＩＣカードインタフェース１３は、ＩＣカード２０が挿入された際に、ＩＣカード２０のＩＣカードインタフェース２１と対向する位置に配置される。また、ＩＣカード端末１０は、ＩＣカード２０の挿入後、ユーザからのＰＩＮ（Ｐｅｒｓｏｎａｌ ＩＤ Ｎｕｍｂｅｒ）を入力するための入力部１２と、ＩＣカード端末１０の全体の制御を司る制御部１４とを備える。入力部１２、制御部１４、及びＩＣカード２０への電力を供給するための電源Ｖは、ＩＣカードインタフェース１３と接続されている。

【００１７】

このように構成される本システムにおいてＩＣカード２０を利用する際には、まずＩＣカード２０をＩＣカード端末１０へ挿入し、入力部１２からＰＩＮを入力し、この入力されたＰＩＮをＩＣカードインタフェース１３、２１を介し、ＩＣカード２０のＩＣチップ２２へ供給する。ＩＣチップ２２では、供給されたＰＩＮを、ＩＣチップ２２の内部で記憶する正当なＰＩＮと照合する。この照合結果が正しければ、その後、ＩＣカード端末１０からＩＣカード２０へＩＣカードインタフェース１３、２１を介し、コマンドを送信し、ＩＣカード２０は、この命令を解釈し動作する。また、ＩＣカード２０は、ＩＣカード端末１０へ応答、等を行う。

【００１８】
図２は、ＩＣカード２０のＩＣチップ２２の内部構成を示している。
【００１９】
入出力部３１は、ＩＣカードインタフェース２１と内部バス３９とに接続され、このＩＣカード２０がＩＣカード端末１０へ挿入中に、ＩＣカードインタフェース２１を介して得られた電力を電源供給部３８へ供給するとともに、ＩＣカードインタフェース２１を介して受信したコマンドやデータを内部バス３９へ送信するとともに、内部バス３９から受信されるコマンドやデータをＩＣカードインタフェース２１へ送信する。
【００２０】
ＣＰＵ３２は、ＩＣチップ２２の全体を制御するものであり、ＲＯＭ３３に記憶されるプログラムによって、動作する。ＲＯＭ３３には、プログラムの他にこのＩＣカード２０のＰＩＮが記憶されている。このＲＯＭ３３に記憶されるＰＩＮの値を、以後、正当なＰＩＮ、それ以外のＰＩＮの値を不正なＰＩＮと呼ぶことにする。なお、ＰＩＮの変更を許容するＩＣカード２０を提供する場合には、後記のＥＥＰＲＯＭ３５に記憶するようにしても良い。また、ＲＯＭ３３には、更に所定期間中に不正なＰＩＮが入力される回数を制限するための閾値が記憶されている。
【００２１】
ＲＡＭ３４は、ＣＰＵ３２に利用されるワークメモリである。ＥＥＰＲＯＭ３５は、ＣＰＵ３２によって読み書き可能な不揮発性の半導体メモリである。ＥＥＰＲＯＭ３５には、所定期間中に入力される不正なＰＩＮの回数を記憶するための不正カウント数記憶領域を備えている。
【００２２】
電源供給部３８は、入出力部３１と接続され、ＩＣカード端末１０から供給される電力を受け、ＩＣチップ２２内の各部に電源供給を行うものである。
【００２３】
ロック用タイマ３６、及びカウンタ用タイマ３７は、同様な構成で実現され、電源供給を受けることなく経時変化することにより所定期間が経過したか否かを測定するものである。なお、ロック用タイマ３６、及びカウンタ用タイマ３７は、測定する所定期間はそれぞれ固定であり、それぞれ期間が異なっており、ロック用タイマ３６のほうが長い期間カウントできる。ロック用タイマ３６は、後記のＩＣカード２０内で行われる他の処理が行えない（ロック状態）期間を設定するものである。一方、カウンタ用タイマ３７は、不正なＰＩＮをカウントするための期間を設定するものである。
【００２４】
ここで、このロック用タイマ３６及びカウンタ用タイマ３７（以下総称して単にタイマ３６／３７と称す）についてより詳細に説明する。
【００２５】
図３は、タイマ３６／３７の基本概念を示したものである。タイマ３６／３７は、電池などの電力源無く経時変化する経時変化部４１と、この経時変化部４１へ入力信号を入力する入力部４２と、経時変化部４１の状態に基づいて、入力信号に対し変化した出力信号を出力する出力部４３とを備える。ここで、経時変化部４１は、時間とともに状態が変化するものであり、この変化された状態を時間の測定に利用するものである。入力部４２及び出力部４３は、経時変化部４１の状態を確認したいときに用いられる。
【００２６】
図４は、図３のタイマ３６／３７の基本概念を実現する第一の具体例である。
【００２７】
この第一の具体例のタイマは、ソース領域５１と、ドレイン領域５２と、ソース領域５１およびドレイン領域５２との間にチャネル領域５３とからなる第１層と、第１層の上部に積層されるトンネル絶縁膜５４からなる第２層と、第２層の上部に積層されるフローティングゲート５５からなる第３層と、第３層の上部に積層される絶縁膜５６で形成される第４層と、第４層の上部に積層される制御ゲート５７からなる第５層とを備えて形成される

。また、ソース領域５１、及び、ドレイン領域５２には、それぞれソース電極５８とドレイン電極５９とが設けられている。

【００２８】

図５は、図４のタイマ３６／３７が時間経過に伴った状態変化を示した図である。なお、図上、グレーの丸は電子を示しており、白の丸は正孔を示している。

【００２９】

（ａ）は、初期状態を示す図である。タイマ３６／３７は、前処理として、制御ゲート５７からチャネル領域５３の基板介面とフローティングゲート５５の間に高電界を印加し、ＦＮトンネリングによって電子をチャネルからフローティングゲート５５に注入しておく。このとき、チャネル領域５３の基板介面は、反転して正孔が集中し、ソース領域５１とドレイン領域５２との間のチャネル領域５３の基板界面にチャネルが開く。

【００３０】

この（ａ）の状態から、時間経過と共に、フローティングゲート５５の電子が基板界面に直接トンネルし、徐々にチャネル領域５３の基板界面の電界が減少する。（ｂ）は、（ａ）の状態からある時間だけ経過した後の時刻T_1の状態を示しており、（ｃ）は、（ｂ）の状態から更にある時間だけ経過した後の時刻T_2の状態を示しており、（ｄ）は、（ｃ）の状態から更にある時間だけ経過した後の時刻T_3の状態を示している。なお、点線は、電子がその時刻までに直接トンネルにより移動したことを模式的に示している。時刻T_3の（ｄ）の状態では、フローティングゲート５５に注入されていた電子がほとんど抜け、チャネル領域５３の基板界面にチャネルが形成されなくなり、その結果、出力信号が流れなくなる。

【００３１】

図６は、このようなタイマ３６／３７の時間と出力信号との関係を示した図である。時刻T_a（＝０）からT_bの間に直接トンネリングが生じ、最後にはチャネルが消失してノイズレベルまで出力信号が低下する。タイマ３６／３７は、時刻T_a（＝０）からT_b（＝ノイズレベル到達時間）の間の、この経時変化を利用し変化した出力信号を供給するから、この出力信号を受信する側は、例えば、所定期間経過したか否か判断したり、このタイマ３６／３７の状態と出力信号の関係が逐時明確になっている場合には、初期状態からの相対的な時刻を知ることができる。なお、図６上のT_1、T_2、T_3は、図６の（ｂ）、（ｃ）、（ｄ）の状態を示している。

【００３２】

図７は、図３のタイマ３６／３７の基本概念を実現する第二の具体例である。この第二の具体例のタイマ３６／３７は、ソース領域６１と、ドレイン領域６２と、ソース領域６１およびドレイン領域６２との間にチャネル領域６３とからなる第１層と、第１層の上部に積層されるトンネル絶縁膜６４からなる第２層と、第２層の上部に積層されるゲート６５からなる第３層と、第３層の上部にリーク電流を制御するためのＰＮ接合６６とを備えて形成される。また、ソース領域６１、及び、ドレイン領域６２には、それぞれソース電極６８とドレイン電極６９とが設けられている。

【００３３】

タイマ３６／３７の時間経過に伴った状態変化についての説明は、第一の具体例のタイマ３６／３７の説明での直接トンネリングを、ＰＮ接合のリーク電流に置き換えれば第一の具体例と同様なので省略する。

【００３４】

図８は、図３のタイマ３６／３７の基本概念を実現する第三の具体例である。この第三の具体例のタイマ３６／３７は、ソース領域７１と、ドレイン領域７２と、ソース領域７１およびドレイン領域７２との間にチャネル領域７３とからなる第１層と、第１層の上部に積層されるトンネル絶縁膜７４からなる第２層と、第２層の上部に積層されるゲート７５からなる第３層と、第３層の上部にリーク電流を制御するためのショットキー接合７６とを備えて形成される。また、ソース領域７１、及び、ドレイン領域７２には、それぞれソース電極７８とドレイン電極７９とが設けられている。

【００３５】
タイマ３６／３７の時間経過に伴った状態変化についての説明は、第一の具体例のタイマ３６／３７の説明での直接トンネリングを、ＰＮ接合のリーク電流に置き換えれば第一の具体例と同様なので省略する。
【００３６】
以上説明したタイマ３６／３７は、図９に示す接続例のようにして構成し、利用する。
【００３７】
図９（ａ）の例は、タイマ３６／３７の両端に、電源供給部３８から電源供給される時に電圧をかけることが可能なようになっており、電源端８１側には、スイッチ素子８３を介してタイマ３６／３７のソース電極５８／６８／７８が接続され、ＧＮＤ端８２側とは電流計８４を介し、ドレイン電極５９／６９／７９が接続される。スイッチ素子８３は、ＣＰＵ３２からのＯＮ／ＯＦＦ（イネーブル）信号線と接続され、ＯＮ信号時にスイッチがＯＮされ導通する。また、電流計８４は、ＣＰＵ３２へ電流値を出力するよう接続される。
【００３８】
そして、ＩＣチップ２２が動作中にタイマ３６／３７の状態を確認する際には、ＣＰＵ３２がスイッチ素子８３をＯＮにすると、電源端８１－ＧＮＤ端８２間に所定電圧がかかり、タイマ３６／３７を介して流れる電流を電流計８４で測定し、測定された電流値がＣＰＵ３２へ出力されることによって、ＣＰＵ３２は、タイマ３６／３７の状態が分かるようになる。
【００３９】
また、特に図示しないが、タイマ３６／３７は、図５の説明時に記載したように時間を測定する前に、前処理が必要であり、この前処理を行う手段を備えている。タイマ３６／３７は、外部から計測開始の指示を受けると、前処理を行った上で、時間計測を開始する。
【００４０】
上記接続例では、一つのタイマ３６／３７についての例を示したが、複数のタイマ３７を備えるようにしてもよい。複数のタイマ３６／３７の各経時変化部４１の経時変化は、用途に応じて同じであっても、異なっていても良いが、ここでは同じ例を図９（ｂ）に示し説明する。この例は、（ａ）のタイマ３６／３７を複数並列化し、それぞれ出力される電流値を平均化回路８５へ入力し、平均化した電流値を制御回路３４へ出力するようにしたものである。なお、制御回路３４からのＯＮ／ＯＦＦ（イネーブル）信号線もそれぞれのスイッチ素子８３へ接続されて、共通に制御できる。この例では、経時変化部４１の経時変化に多少のばらつきがあっても、平均化することにより、安定したタイマを提供できる。また、特に図示しないが、複数の経時変化部４１の経時変化が異なったものとすると、いろいろな時刻情報が取得できるなどの利点がある。
【００４１】
次に、本チップ２２のＣＰＵ３２上で動作する全体の概略フローについて、図１０を用いて説明する。
【００４２】
ＩＣカード２０がＩＣカード端末１０へ挿入されてから排出までに、まず、必ずＰＩＮ認証を行い、このＰＩＮ認証の結果が正当なＰＩＮと判断されたときに、他の処理が行えるようになっている。ＰＩＮ認証の結果が不正なＰＩＮと判断されたときには、カードを一旦排出するようにする（図の（ａ））、または、カードを排出せずに再度ＰＩＮ認証を行わせるようにする（図の（ｂ））。
【００４３】
次に、このＰＩＮ認証に関する動作について、図１１のフローチャートを用いて詳細に説明する。
【００４４】
まず、ユーザは、ＩＣカード２０をＩＣカード端末１０へ挿入の上、入力部１２から、ＰＩＮを入力する。入力されたＰＩＮは、ＩＣカードインタフェース１３、２１を介して、

ＩＣカード２０の入出力部３１へ入力される。入出力部３１は、ＣＰＵ３２へＰＩＮを送信し、ＣＰＵ３２で動作するプログラムは、ＰＩＮを受信する（S101）。

【００４５】

ＰＩＮを受信すると、まず、ロック用タイマ３６が現在計測中であるか否かを判断する（S102）。これは、ロック用タイマ３６から図９の説明時に説明したようにして電流値を読み取り、この電流値が、ノイズレベルに到達しているか否かを判断すればよい。

【００４６】

もし、計測中であると判断された場合には、ＩＣカード２０は、現在ロック状態であるため、失敗と判断し、端末１０へその旨通知する（S103）。

【００４７】

一方、ロック用タイマ３６が計測中で無いと判断された場合、次にカウンタ用タイマ３７が計測中であるか否かを判断する（S104）。これも、ステップS102と同様の方法で判断すれば良い。

【００４８】

もし、カウンタ用タイマ３７が計測中で無ければ、ＥＥＰＲＯＭ３５の不正カウント数記憶領域に記憶される不正カウンタをリセットし（S105）、カウンタ用タイマ３７の計測を開始させる（S106）。この開始の指示によりカウンタ用タイマ３７は、例えば、上記で説明した第一の具体例のタイマであったとすると、一瞬の間高電圧を印加することにより、フローティングゲートへ電子を蓄え、その後何もしないことにより計測を開始する。

【００４９】

次に、ステップS101で受信したＰＩＮを、ＲＯＭ３３に記憶する正当なＰＩＮと照合する（S107）。

【００５０】

この照合の結果、受信したＰＩＮが正しいＰＩＮであれば、カウンタ用タイマ３７の計測を終了し（S108）、成功と判断し、端末１０へその旨通知する（S109）。なお、ステップS108の終了の処理は、カウンタ用タイマ３７自身の経時変化を終了させたり、カウンタ用タイマ３７の有効／無効フラグを格納する領域をＥＥＰＲＯＭ３５内に設けておき、これによって管理するようなど様々な方法で実現できる。

【００５１】

一方、ＰＩＮ照合の結果、不正なＰＩＮであれば、ＥＥＰＲＯＭ３５の不正カウンタ記憶領域に記憶する不正カウンタの値をインクリメントする（S110）。次に、このインクリメントした不正カウンタの値が、ＲＯＭ３３に格納される閾値か否かを確認する（S111）。

【００５２】

不正カウンタ数格納領域の値が閾値となった場合には、ＩＣカード２０を正規のユーザでないユーザが不正利用している可能性が高いとして、ロック用タイマ３６へ計測を開始させる（S112）。そして、ＩＣカード２０をロック状態に移行させる。なお、この計測の開始も、ステップS106の説明時に記載した方法と同様の方法で行えば良い。そして、ステップS107でのＰＩＮ照合の結果に基づき、失敗と判断し、端末１０へその旨通知する(S113)。

【００５３】

以上のようなＰＩＮ認証に関する動作についてのフローに従う一具体例のタイムチャートは、図１２に示すようになる。なお、ＰＩＮの不正入力の閾値を３とし、カウンタ用タイマ３７が計測する時間をＴ1、ロック用タイマ３６が計測する時間をＴ2とし、Ｔ1＜Ｔ2とする。また、不正ＰＩＮは、入力部１２から不正なＰＩＮが入力されたことを示し、正当ＰＩＮは、入力部１２から正当なＰＩＮが入力されたことを示している。

【００５４】

図１２（ａ）において、初期状態は不正カウンタは不定（何でも良い）、タイマ３６、３７は何れも計測していない状態である。この状態から、まず、最初の不正ＰＩＮが入力されると、ステップS105によって不正カウンタをリセット（０）にし、ステップS106によってカウンタ用タイマ３７が計測を開始し、ステップS110によって不正カウンタがインクリ

メントされ１となる。なお、この状態では、まだ閾値より不正カウンタのほうが小さいのでステップS112は、未だ開始されない。

【００５５】

次に、最初の不正ＰＩＮが入力されてからＴ1までの期間より前に、再度、不正ＰＩＮが入力されたとする。このとき、カウンタ用タイマ３７は計測中であるから、ステップS105、S106の処理はされず、ステップS110によって不正カウンタがインクリメントされ２となる。なお、なお、この状態でも、まだ閾値より不正カウンタのほうが小さいのでステップS112は、未だ開始されない。

【００５６】

次に、最初の不正PINが入力されてからＴ1までの期間より前に、再度、不正ＰＩＮが入力されたとする。このとき、カウンタ用タイマ３７は計測中であるから、ステップS105、S106の処理はされず、ステップS110によって不正カウンタがインクリメントされ３となる。この結果、不正カウンタは閾値と同じになったので、ステップS112が実行される。すなわち、ロック用タイマ３６が計測を開始し、ＩＣカード２０はロック状態となり、以後Ｔ2期間経過するまで継続する。このＴ2期間中は、例え正当なＰＩＮが入力されたとしても、ステップS103で認証処理が終了するようになっており、ロック状態を維持している。

【００５７】

Ｔ2時間経過するとロック用タイマ３６は計測を終了するが、この時より前にカウンタ用タイマ３７も（Ｔ1＜Ｔ2なので）計測を終了しており、上記で述べた初期状態と同様な状態に戻る。なお、不正カウンタの値は、次回のＰＩＮ入力時にステップS105によって必ずリセットされるので、初期状態のときと同様、不定と考えて良い。

【００５８】

一方、図１２（ｂ）は、カウンタ用タイマ３７でカウント中に正当なＰＩＮが受信された場合を示した図である。図１２（ｂ）において、初期状態、最初の不正ＰＩＮ、２回目の不正ＰＩＮは、図１２（ａ）と同様とする。ここで、３回目のＰＩＮの受信時に、正当なＰＩＮが入力されると、ステップS101、S102、S104、S107の順に進み、ステップS107で正しいＰＩＮであると判断され、ステップS108へ進む、ステップS108では、カウンタ用タイマの計測を終了するので、初期状態と同じ状態に戻ることになる。

【００５９】

以上説明したように、本実施の形態のＩＣカードは、電力が供給されない状況でも動作し続けるタイマをロック用タイマとして利用するから、ロック状態後、一定時間後に再びＰＩＮ受信可能状態となる。

【００６０】

また、電力が供給されない状況でも動作し続けるタイマをカウンタ用タイマとして利用するから、最初の不正ＰＩＮの入力後一定時間経過内にロック状態とならなければ、不正カウンタをリセットすることが可能となる。

【００６１】

このようにすることは、正当なユーザが誤って不正ＰＩＮを閾値数以上入力したとしても、一定時間経過するだけで、特に管理者側から何もすることなく再度利用可能になるだけでなく、不正なユーザが不正ＰＩＮを多数入力することによって、正当なＰＩＮを知りえるＰＩＮの推定攻撃に対しても、一定時間経過するまで再度ＰＩＮ入力ができなくなるので、正当なＰＩＮを知るまでに大変時間がかかるようにできる。

【００６２】

また、このＩＣカードを利用可能な端末は、従来のＩＣカード端末と何ら変更無く利用できる利点もある。

【００６３】

次に、上記で説明したＰＩＮ認証の別の変形例に関する動作について、図１３のフローチャートを用いて詳細に説明する。

【００６４】

変形例のＰＩＮ認証のフローチャートは、図１１のＰＩＮ認証のフローチャート上のステ

ップS106の「カウンタ用タイマ計測開始」の位置を、ステップS107の後に移動したものであり、他は特に変更点が無い。このようなＰＩＮ認証の別の変形例によれば、ＰＩＮ照合により、不正ＰＩＮと判断された時に、カウンタ用タイマ３７の計測をはじめから再度開始する。

【００６５】

このようなＰＩＮ認証の別の変形例に従う、一具体例のタイムチャートは、図１４のようになる。なお、図１４の諸条件は、図１２のそれと同様にしてある。

【００６６】

図１４（ａ）および（ｂ）からわかるように、ロック用タイマ３６が計測中で無い状態（不正カウンタが閾値を越えていない場合）では、カウント用タイマ３７の計測時間は、計測開始後、不正ＰＩＮが入力される都度、計測を再度開始し、結果として延長されている。また、図１４（ｂ）左のように、ロック用タイマ３６が計測中で無い状態（不正カウンタが閾値を越えていない場合）で、且つ、カウント用タイマ３７の計測中に、正当なＰＩＮが入力されると、カウント用タイマ３７の計測を終了するようになる。一方、図１４（ｂ）右のように、ロック用タイマ３６が計測中の状態（不正カウンタが閾値を越えている場合）では、不正ＰＩＮ、正当ＰＩＮの何れが入力されても、カウンタ用タイマ３７には、何ら影響を受けない（延長されない）。

【００６７】

以上のような変形例によれば、ロック状態になっていない状態では、最後にＰＩＮ入力を間違ってから所定時間中何もＰＩＮ入力しなければ、所定時間経過後には再度ＰＩＮ入力ができるようになることを保証できる利点を（図１１のフローと比較し）更に備えている。

【００６８】

以上説明したように、本実施の形態のＩＣカードの変形例は、電力が供給されない状況でも動作し続けるタイマをロック用タイマとして利用するから、ロック状態後、一定時間後に再びＰＩＮ受信可能状態となる。

【００６９】

また、電力が供給されない状況でも動作し続けるタイマをカウンタ用タイマとして利用するから、前回の不正ＰＩＮ入力後、一定時間経過していれば、不正カウンタをリセットすることが可能となる。

【００７０】

このようにすることは、正当なユーザが誤って不正ＰＩＮを閾値数以上入力したとしても、一定時間経過するだけで、特に管理者側から何もすることなく再度利用可能になるだけでなく、不正なユーザが不正ＰＩＮを多数入力することによって、正当なＰＩＮを知りえるＰＩＮの推定攻撃に対しても、一定時間経過するまで再度ＰＩＮ入力ができなくなるので、正当なＰＩＮを知るまでに大変時間がかかるようにできる。

【００７１】

また、このＩＣカードを利用可能な端末は、従来のＩＣカード端末と何ら変更無く利用できる利点もある。

【００７２】

【発明の効果】

以上説明したように、本発明によれば、ＩＣカード側で、一定時間のＰＩＮロックを可能にすることができる。これにより、ＩＣカードへのＰＩＮの推定攻撃に対する安全性を確保しつつ、利用者の利便性も確保できる。

【図面の簡単な説明】

【図１】本実施の形態に係る全体システムを示した図。

【図２】ＩＣカード２０のＩＣチップ２２の内部構成を示す図。

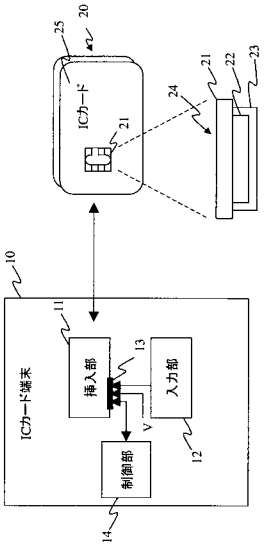
【図３】　タイマ３６／３７の基本概念を示した図。

【図４】　タイマ３６／３７を実現する第一の具体例。

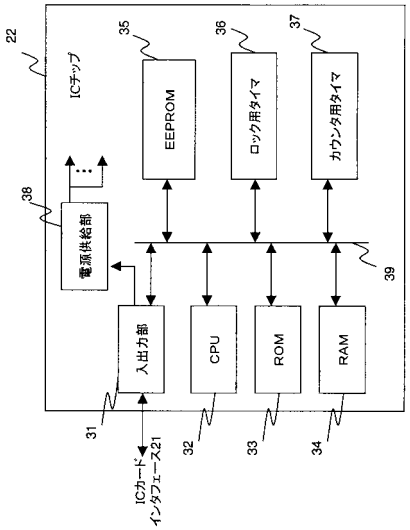
【図５】　タイマ３６／３７が時間経過に伴った状態変化を示した図。

【図６】　タイマ３６／３７の時間と出力信号との関係を示した図。
【図７】　タイマ３６／３７の基本概念を実現する第二の具体例。
【図８】　タイマ３６／３７の基本概念を実現する第三の具体例。
【図９】　タイマ３６／３７とＣＰＵ３２との接続例。
【図１０】　本チップ２２のＣＰＵ３２上で動作する全体の概略フローチャート。
【図１１】　ＰＩＮ認証に関する動作についてのフローチャート。
【図１２】　ＰＩＮ認証に関する動作についてのフローに従う具体例のタイムチャート。
【図１３】　ＰＩＮ認証に関する動作についての別の変形例のフローチャート。
【図１４】　ＰＩＮ認証に関する動作についてのフローに従う具体例のタイムチャート。
【符号の説明】
１０・・・ＩＣカード端末
１１・・・挿入部
１２・・・入力部
１３・・・ＩＣカードインタフェース
１４・・・制御部
２０・・・ＩＣカード
２１・・・ＩＣカードインタフェース
２２・・・ＩＣチップ
２３・・・封止材
２４・・・ＩＣモジュール
２５・・・プラスチック部材
３１・・・入出力部
３２・・・ＣＰＵ
３３・・・ＲＯＭ
３４・・・ＲＡＭ
３５・・・ＥＥＰＲＯＭ
３６・・・ロック用タイマ
３７・・・カウンタ用タイマ
３８・・・電源供給部
３９・・・内部バス
４１・・・経時変化部
４２・・・入力部
４３・・・出力部
５１、６１、７１・・・ソース領域
５２、６２、７２・・・ドレイン領域
５３、６３、７３・・・チャネル領域
５４、６４、７４・・・トンネル絶縁膜
５５・・・フローティングゲート
５６・・・絶縁膜
５７・・・制御ゲート
５８、６８、７８・・・ソース電極
５９、６９、７９・・・ドレイン電極
６５、７５・・・ゲート
６６・・・ＰＮ接合
７６・・・ショットキー接合
８１・・・電源端
８２・・・ＧＮＤ端
８３・・・スイッチ素子
８４・・・電流計
８５・・・平均化回路

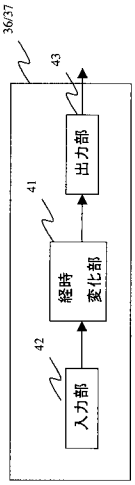
【図１】


ICカード
ICカード端末
挿入部
入力部
制御部
10
11
12
13
14
20
21
22
23
24
25
V

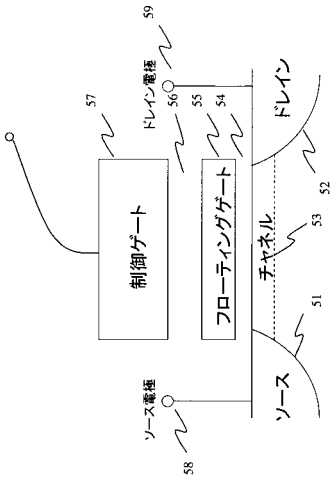
【図２】


ICチップ
EEPROM
ロック用タイマ
カウンタ用タイマ
電源供給部
入出力部
CPU
ROM
RAM
ICカードインタフェース21
22
31
32
33
34
35
36
37
38
39

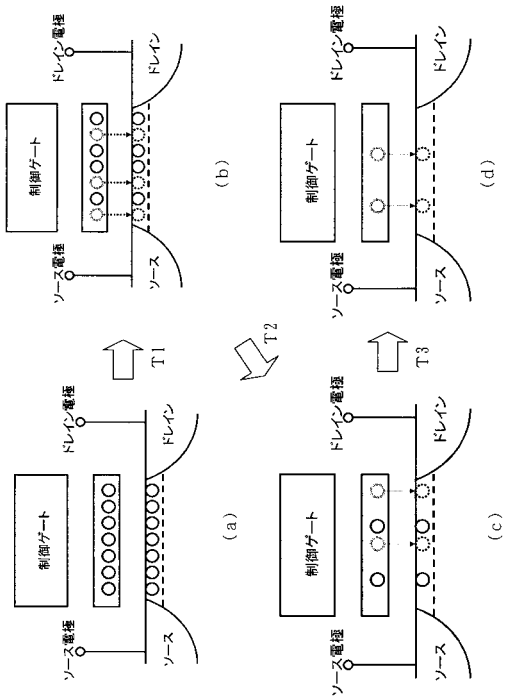
【図３】


出力部
経時変化部
入力部
36/37
41
42
43

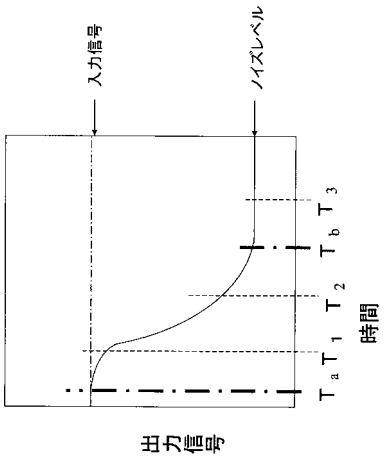
【図４】


制御ゲート
フローティングゲート
チャネル
ドレイン
ソース
ドレイン電極
ソース電極
51
52
53
54
55
56
57
58
59

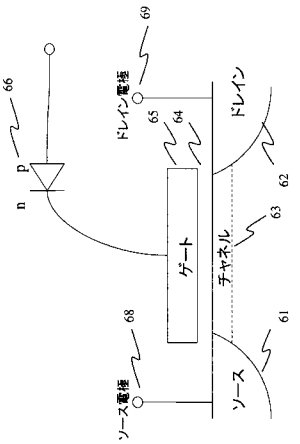
【図５】


ドレイン電極
ドレイン
制御ゲート
ソース電極
ソース
(a)
(b)
(c)
(d)
T1
T2
T3

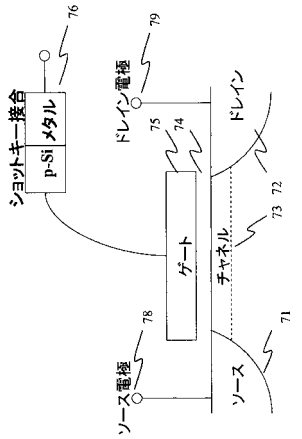
【図６】


入力信号
ノイズレベル
出力信号
時間
Ta T1 T2 Tb T3

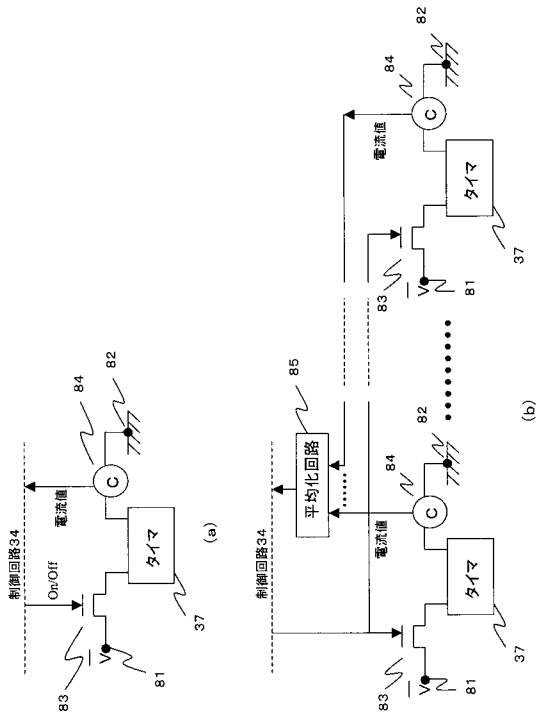
【図７】


n
p
66
69
ドレイン電極
65
64
ドレイン
62
63
ゲート
チャネル
68
61
ソース電極
ソース

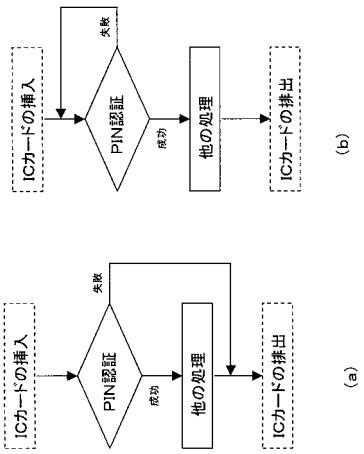
【図８】


76
ショットキー接合
p-Si
メタル
79
ドレイン電極
75
74
ドレイン
72
73
ゲート
チャネル
78
71
ソース電極
ソース

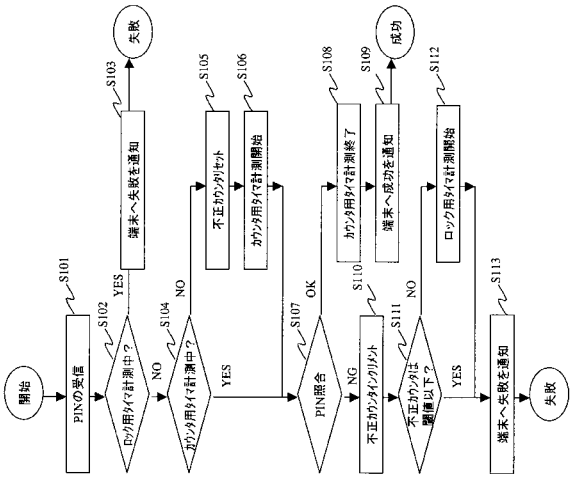
【図９】



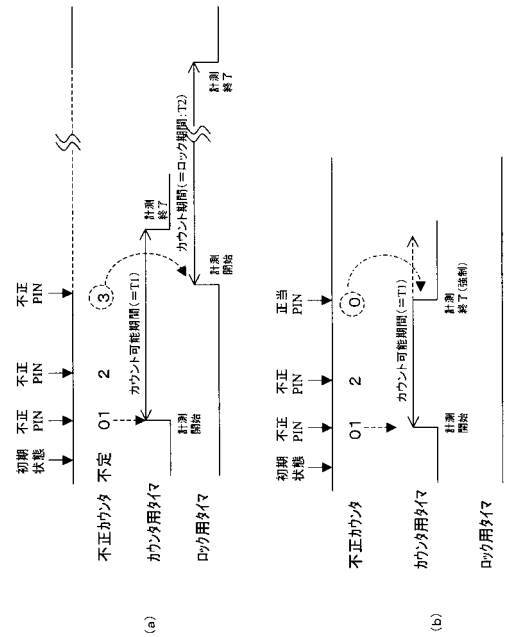
【図１０】



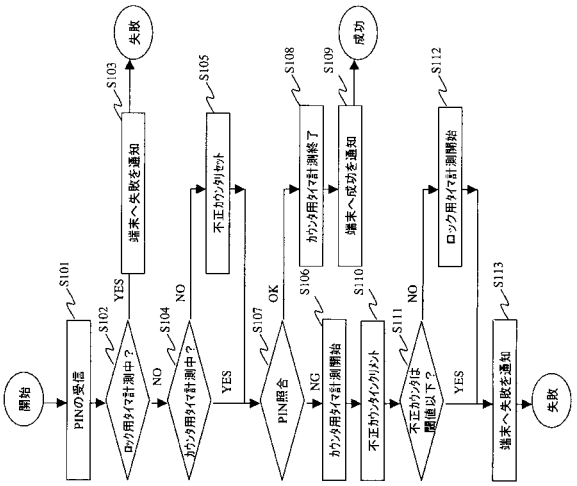
【図１１】



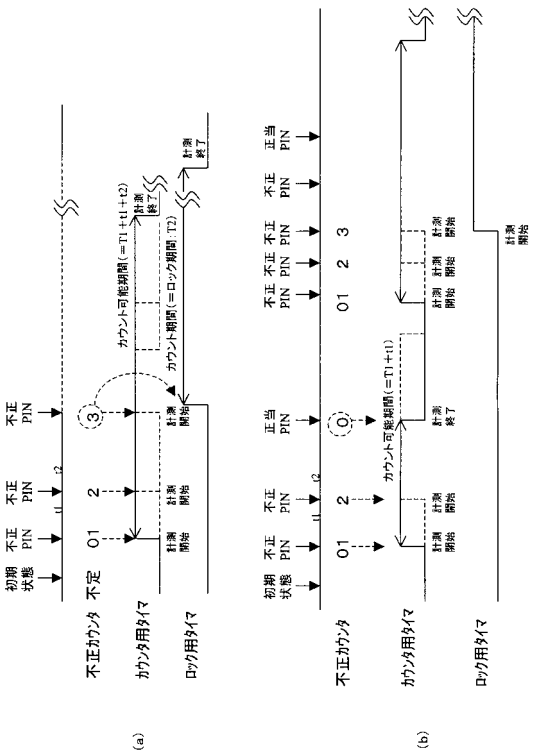
【図１２】



【図１３】


開始
S101
PINの受信
S102
ロック用タイマ計測中？
YES
S103
端末へ失敗を通知
失敗
NO
S104
カウンタ用タイマ計測中？
NO
S105
不正カウンタリセット
YES
S107
PIN照合
OK
S108
カウンタ用タイマ計測終了
S109
端末へ成功を通知
成功
NG
S106
カウンタ用タイマ計測開始
S110
不正カウンタインクリメント
S111
不正カウンタは閾値以下？
NO
S112
ロック用タイマ計測開始
YES
S113
端末へ失敗を通知
失敗

【図１４】


初期状態
不正PIN
不正PIN
不正PIN
正当PIN
不正カウンタ
カウンタ用タイマ
ロック用タイマ
計測開始
計測終了
カウント可能期間(＝T1＋t1＋t2)
カウント期間(＝ロック期間(T2))
(a)
(b)

フロントページの続き

(72)発明者　松下　達之
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内
(72)発明者　友枝　裕樹
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内
(72)発明者　清水　秀夫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内
(72)発明者　渡辺　浩志
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝　横浜事業所内

審査官　前田　浩

(56)参考文献　特開昭５７－１２０１８３（ＪＰ，Ａ）
特開平０８－０４４９３５（ＪＰ，Ａ）
特開平０２－２８８９９３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06K 17/00-19/18