【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成19年2月8日(2007.2.8)

【公開番号】特開2003-233795(P2003-233795A)
【公開日】平成15年8月22日(2003.8.22)
【出願番号】特願2002-346019(P2002-346019)
【国際特許分類】
Ｇ０６Ｋ　19/10　(2006.01)
Ｇ０６Ｆ　12/14　(2006.01)
Ｇ０６Ｋ　17/00　(2006.01)
Ｇ０９Ｃ　 1/00　(2006.01)
Ｈ０４Ｌ　 9/32　(2006.01)
【ＦＩ】
Ｇ０６Ｋ　19/00　　Ｒ
Ｇ０６Ｆ　12/14　３１０Ｈ
Ｇ０６Ｆ　12/14　３２０Ｂ
Ｇ０６Ｆ　12/14　３２０Ｆ
Ｇ０６Ｋ　17/00　　Ｔ
Ｇ０９Ｃ　 1/00　６４０Ｅ
Ｇ０９Ｃ　 1/00　６６０Ａ
Ｈ０４Ｌ　 9/00　６７５Ａ

【手続補正書】
【提出日】平成18年12月15日(2006.12.15)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
電子機器に着脱可能な半導体メモリカードであって、
書き換え可能な不揮発メモリと、
前記不揮発メモリ内の予め定められた２つの記憶領域である認証領域と非認証領域への前記電子機器によるアクセスを制御する制御回路とを備え、
前記制御回路は、
前記非認証領域への前記電子機器によるアクセスを制御する非認証領域アクセス制御部と、
前記電子機器の正当性を検証するために前記電子機器の認証を試みる認証部と、
前記認証部が認証に成功した場合にだけ前記認証領域への前記電子機器によるアクセスを許可する認証領域アクセス制御部とを有し、
前記認証領域と前記非認証領域は、前記不揮発性メモリ内の一定サイズの連続した記憶領域を２分して得られる各領域に割り当てられ、
前記半導体メモリカードはさらに、
前記一定サイズの記憶領域を２分する境界アドレスに関する情報を保持する手段と、
前記認証領域及び前記非認証領域それぞれの領域サイズを変更する領域サイズ変更回路を備え、
前記領域サイズ変更回路は、記憶領域の内容をすべて削除した後に前記境界アドレスに関する情報を変更することによって前記認証領域及び前記非認証領域それぞれの領域サイ

ズを変更し、
前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記境界アドレスに関する情報を参照して、前記認証領域または前記非認証領域へのアクセスを制御する
ことを特徴とする半導体メモリカード。
【請求項２】
前記認証部は、認証の結果を反映した鍵データを生成し、
前記認証領域アクセス制御部は、前記電子機器から送られてくる暗号化された命令を前記認証部が生成した鍵データで復号し、復号された命令に従って前記認証領域へのアクセスを制御する
ことを特徴とする請求項１記載の半導体メモリカード。
【請求項３】
前記認証部は、前記電子機器とチャレンジ・レスポンス型の相互認証を行い、前記電子機器の正当性を検証するために前記電子機器に送信したチャレンジデータと自己の正当性を証明するために生成したレスポンスデータとから前記鍵データを生成する
ことを特徴とする請求項２記載の半導体メモリカード。
【請求項４】
前記電子機器から送られてくる暗号化された命令は、前記認証領域へのアクセスの種別を特定する暗号化されていないタグ部と、アクセスする領域を特定する暗号化されたアドレス部とからなり、
前記認証部は、前記鍵データを用いて、前記命令のアドレス部を復号し、復号されたアドレスによって特定される領域に対して、前記命令のタグ部によって特定される種別のアクセスを実行制御する
ことを特徴とする請求項３記載の半導体メモリカード。
【請求項５】
前記半導体メモリカードはさらに、他の半導体メモリカードと区別して自己を特定することが可能な固有の識別データを予め記憶する識別データ記憶回路を備え、
前記認証部は、前記識別データ記憶回路に格納された識別データを用いて相互認証を行い、前記識別データに依存させて前記鍵データを生成する
ことを特徴とする請求項４記載の半導体メモリカード。
【請求項６】
前記領域サイズ変更回路は、
前記認証領域における論理アドレスと物理アドレスとの対応を示す認証領域変換テーブルと、
前記非認証領域における論理アドレスと物理アドレスとの対応を示す非認証領域変換テーブルと、
前記電子機器からの命令に従って前記認証領域変換テーブル及び前記認証領域変換テーブルを変更する変換テーブル変更部とを有し、
前記認証領域アクセス制御部は、前記認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、
前記非認証領域アクセス制御部は、前記非認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御する
ことを特徴とする請求項１記載の半導体メモリカード。
【請求項７】
前記認証領域及び前記非認証領域は、それぞれ、前記一定サイズの記憶領域を２分して得られる物理アドレスの高い領域及び低い領域に割り当てられ、
前記非認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、
前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられている
ことを特徴とする請求項６記載の半導体メモリカード。

【請求項８】
前記半導体メモリカードはさらに、予めデータが格納された読み出し専用のメモリ回路を備える
ことを特徴とする請求項１記載の半導体メモリカード。
【請求項９】
前記認証領域及び前記非認証領域は、前記電子機器にとって読み書き可能な記憶領域と読み出し専用の記憶領域とからなり、
前記制御回路はさらに、前記電子機器が前記不揮発メモリにデータを書き込むためのアクセスをする度に乱数を発生する乱数発生器を有し、
前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記乱数を用いて前記データを暗号化し、得られた暗号化データを前記読み書き可能な記憶領域に書き込むとともに、前記乱数を前記暗号化データに対応づけられた前記読み出し専用の記憶領域に書き込む
ことを特徴とする請求項１記載の半導体メモリカード。
【請求項１０】
前記制御回路はさらに、
前記認証領域及び前記非認証領域における論理アドレスと物理アドレスとの対応を示す変換テーブルと、
前記電子機器からの命令に従って前記変換テーブルを変更する変換テーブル変更部とを有し、
前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記変換テーブルに基づいて前記電子機器によるアクセスを制御する
ことを特徴とする請求項１記載の半導体メモリカード。
【請求項１１】
前記制御回路はさらに、前記認証領域及び前記非認証領域に書き込むべきデータを暗号化するとともに、前記認証領域及び前記非認証領域から読み出されたデータを復号化する暗号復号部を有する
ことを特徴とする請求項１記載の半導体メモリカード。
【請求項１２】
前記不揮発メモリは、フラッシュメモリであり、
前記制御回路はさらに、前記電子機器からの命令に従って、前記認証領域及び前記認証領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リスト読み出し部を有する
ことを特徴とする請求項１記載の半導体メモリカード。
【請求項１３】
前記認証部は、認証のために電子機器を使用するユーザに対してそのユーザに固有の情報であるユーザキーを要求するものであり、
前記制御回路はさらに、
前記ユーザキーを記憶しておくためのユーザキー記憶部と、
前記認証部による認証に成功した電子機器を特定することができる識別情報を記憶しておくための識別情報記憶部と、
前記認証部による認証が開始されると、その電子機器から識別情報を取得し、その識別情報が前記識別情報記憶部に既に格納されているか否か検査し、既に格納されている場合には、前記認証部によるユーザキーの要求を禁止させるユーザキー要求禁止部とを有する
ことを特徴とする請求項１記載の半導体メモリカード。
【請求項１４】
電子機器に着脱可能な半導体メモリカードを制御する半導体メモリカードの制御方法であって、
前記半導体メモリカードは、
一定サイズの連続した記憶領域を２分して得られる２つの記憶領域である認証領域と非

認証領域を含む書き換え可能な不揮発メモリと、
前記一定サイズの記憶領域を２分する境界アドレスに関する情報を保持する手段と、
前記認証領域と非認証領域への前記電子機器によるアクセスを制御する制御回路とを備え、
前記制御回路における制御方法は、
前記非認証領域への前記電子機器によるアクセスを制御する非認証領域アクセス制御ステップと、
前記電子機器の正当性を検証するために前記電子機器の認証を試み、認証に成功した場合に前記認証領域への前記電子機器によるアクセスを許可する認証領域アクセス制御ステップと、
前記記憶領域の内容をすべて削除した後に前記境界アドレスに関する情報を変更することによって前記認証領域及び前記非認証領域それぞれの領域サイズを変更する領域サイズ変更ステップと、を含み、
前記認証領域アクセス制御ステップ及び前記非認証領域アクセス制御ステップは、それぞれ、前記境界アドレスに関する情報を参照して、前記認証領域または前記非認証領域へのアクセスを制御する
ことを特徴とする半導体メモリカードの制御方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００７
【補正方法】変更
【補正の内容】
【０００７】
【課題を解決するための手段】
上記目的を達成するために、本発明に係る半導体メモリカードは、電子機器に着脱可能な半導体メモリカードであって、書き換え可能な不揮発メモリと、前記不揮発メモリ内の予め定められた２つの記憶領域である認証領域と非認証領域への前記電子機器によるアクセスを制御する制御回路とを備え、前記制御回路は、前記非認証領域への前記電子機器によるアクセスを制御する非認証領域アクセス制御部と、前記電子機器の正当性を検証するために前記電子機器の認証を試みる認証部と、前記認証部が認証に成功した場合にだけ前記認証領域への前記電子機器によるアクセスを許可する認証領域アクセス制御部とを有し、前記認証領域と前記非認証領域は、前記不揮発性メモリ内の一定サイズの連続した記憶領域を２分して得られる各領域に割り当てられ、前記半導体メモリカードはさらに、前記一定サイズの記憶領域を２分する境界アドレスに関する情報を保持する手段と、前記認証領域及び前記非認証領域それぞれの領域サイズを変更する領域サイズ変更回路を備え、前記領域サイズ変更回路は、記憶領域の内容をすべて削除した後に前記境界アドレスに関する情報を変更することによって前記認証領域及び前記非認証領域それぞれの領域サイズを変更し、前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記境界アドレスに関する情報を参照して、前記認証領域または前記非認証領域へのアクセスを制御することを特徴とする。