(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-292959
(P2005-292959A)
(43)公開日　平成17年10月20日(2005.10.20)

| (51)Int.Cl.[7] | F I | | テーマコード（参考） |
|---|---|---|---|
| G06F 12/14 | G06F | 12/14　560D | 5B017 |

審査請求 未請求　請求項の数 5　OL　（全 9 頁）

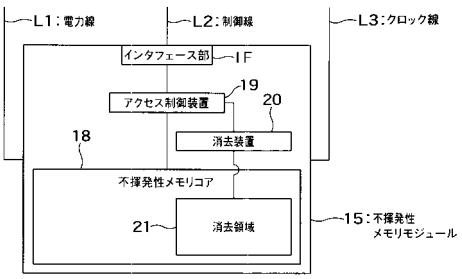
(21)出願番号　特願2004-103871 (P2004-103871)
(22)出願日　平成16年3月31日 (2004.3.31)

(71)出願人　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　100075812
弁理士　吉武　賢次
(74)代理人　100088889
弁理士　橘谷　英俊
(74)代理人　100082991
弁理士　佐藤　泰和
(74)代理人　100096921
弁理士　吉元　弘
(74)代理人　100103263
弁理士　川崎　康
(74)代理人　100118876
弁理士　岡澤　順生

最終頁に続く

(54)【発明の名称】不揮発性メモリモジュール及び不揮発性メモリシステム

(57)【要約】
【課題】　不揮発性メモリに格納されるデータを第３者から有効に保護する。
【解決手段】　不揮発性メモリは、電力供給装置供給された電力、クロック供給装置から供給されたクロックを用いて動作する。この不揮発性メモリに対する電力及びクロックの供給が停止状態から供給状態に遷移した場合は、消去部は、不揮発性メモリ内のデータを消去する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
供給された電力及び供給されたクロックを用いて動作する不揮発性メモリと、
前記不揮発性メモリに対する前記電力及び前記クロックの供給が停止状態から供給状態に遷移した場合は、前記不揮発性メモリ内のデータを消去する消去部と、
を備えた不揮発性メモリモジュール。
【請求項２】
前記消去部は、前記停止状態から前記供給状態への遷移が所定回数生じたら、前記不揮発性メモリ内のデータを消去することを特徴とする請求項１に記載の不揮発性メモリモジュール。
【請求項３】
前記消去部による前記データの消去が行われている間は、前記不揮発性メモリへのアクセスを阻止するアクセス制御部をさらに備えたことを特徴とする請求項１又は２に記載の不揮発性メモリモジュール。
【請求項４】
供給された電力及び供給されたクロックを用いて動作する不揮発性メモリと、
前記不揮発性メモリ内のデータに誤りがあるか否かを検査するための誤り検出コードを格納したコード格納部と、
前記不揮発性メモリに対する前記電力及び前記クロックの供給が停止状態から供給状態に遷移した場合は、前記誤り検出コードを用いて、前記不揮発性メモリ内のデータに誤りがあるか否かを検査する検査部と、
検査の結果、前記不揮発性メモリ内のデータに誤りがある場合は、誤りのある前記データを消去する消去部と、
を備えた不揮発性メモリモジュール。
【請求項５】
不揮発性メモリと、
前記不揮発性メモリに電力を供給する電力供給部と、
前記不揮発性メモリにクロックを供給するクロック供給部と、
前記不揮発性メモリに対する前記電力及び前記クロックの供給が停止状態から供給状態に遷移した場合は、前記不揮発性メモリ内のデータを消去する消去部と、
前記消去部による前記データの消去が行われている間は、前記不揮発性メモリへのアクセスを阻止するアクセス制御部と、
を備えた不揮発性メモリシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、不揮発性メモリモジュール及び不揮発性メモリシステムに関する。
【背景技術】
【０００２】
電子化された社会では、個人情報やパスワードなどの機密情報、及びコンテンツやプログラムなどの著作権データに対する漏洩、不正使用、改ざん及び破壊が問題となり、それらを防止する技術が求められている。
【０００３】
通常、これらの機密情報及び著作権データは、暗号化技術や認証技術を用いたアクセス制限などの対策により保護される。
【０００４】
機密情報や著作権データ等の保護されるべきデータをソフトウェアで処理する場合、処理の間は、そのデータは、主記憶装置に一時的に保存される。処理が終了した後は、一時的に保存されたデータは、揮発メモリの電源切断等により消去される。
【０００５】

ところで、機器の主記憶装置にFeRAMやMRAMなどの不揮発性メモリを用いた場合、保護されるべきデータは、電源切断後も不揮発性メモリに保持される。そのため、機器の故障や不正行為などによりメモリモジュールが取り出されると、不揮発性メモリ内のデータが漏洩したり不正使用されたりする危険性が存在する。

【０００６】

以上の問題を解決する従来の手段として、特開平第９－２０４５０３号公報のように、メモリに対して暗号化されたデータを書き込むことにより、データの漏洩を防止する装置が存在する。

【０００７】

しかし、この装置では、書き込み時の暗号化と、読み出し時の復号化に多くの処理時間を要するため、高速動作するメモリモジュールには適用できないという問題があった。

【０００８】

また、特開平第５－２５０５２６号公報のように、メモリモジュールにアクセス制限装置を内蔵させ、認証が行われるまではアクセス制限装置によってメモリへのアクセスを制限し、これによりデータの漏洩を防止する装置がある。

【０００９】

しかし、この装置では、メモリへのアクセスのために外部から入力する認証用の鍵が漏洩した場合への対応が困難である問題があった。

【特許文献１】特開平第９－２０４５０３号公報

【特許文献２】特開平第５－２５０５２６号公報

【特許文献３】特開２００３－５８４３２公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

本発明の目的は、不揮発性メモリ内のデータを第３者から有効に保護する不揮発性メモリモジュール及び不揮発性メモリシステムを提供することにある。

【課題を解決するための手段】

【００１１】

本発明の不揮発性メモリモジュールは、供給された電力及び供給されたクロックを用いて動作する不揮発性メモリと、前記不揮発性メモリに対する前記電力及び前記クロックの供給が停止状態から供給状態に遷移した場合は、前記不揮発性メモリ内のデータを消去する消去部と、を備える。

【００１２】

本発明の別の不揮発性メモリモジュールは、供給された電力及び供給されたクロックを用いて動作する不揮発性メモリと、前記不揮発性メモリ内のデータに誤りがあるか否かを検査するための誤り検出コードを格納したコード格納部と、前記不揮発性メモリに対する前記電力及び前記クロックの供給が停止状態から供給状態に遷移した場合は、前記誤り検出コードを用いて、前記不揮発性メモリ内のデータに誤りがあるか否かを検査する検査部と、検査の結果、前記不揮発性メモリ内のデータに誤りがある場合は、少なくとも前記データを消去する消去部と、を備える。

【００１３】

本発明の不揮発性メモリシステムは、不揮発性メモリと、前記不揮発性メモリに電力を供給する電力供給部と、前記不揮発性メモリにクロックを供給するクロック供給部と、前記不揮発性メモリに対する前記電力及び前記クロックの供給が停止状態から供給状態に遷移した場合は、前記不揮発性メモリ内のデータを消去する消去部と、前記消去部による前記データの消去が行われている間は、前記不揮発性メモリへのアクセスを阻止するアクセス制御部と、を備える。

【発明の効果】

【００１４】

本発明により、不揮発性メモリ内のデータを第３者から有効に保護できる。

【発明を実施するための最良の形態】
【００１５】
図１は、本発明の第１の実施の形態に従った不揮発性メモリモジュールの構成を概略的に示す図である。
【００１６】
図２は、図１の不揮発性メモリモジュールを適用した不揮発性メモリシステムの構成を示す図である。
【００１７】
図２に示すように、第１の電力供給装置１１は、電源１２から供給される電力を用いて、ＣＰＵ１３、メモリ制御装置１４及び不揮発性メモリモジュール１５に供給する動作電圧（電力）を生成する。生成された電力は、電力線Ｌ１を介して、ＣＰＵ１３、メモリ制御装置１４及び不揮発性メモリモジュール１５に供給される。
【００１８】
第２の電力供給装置１６は、電源１２から供給される電力を用いて、クロック供給装置１７への動作電圧（電力）を生成する。クロック供給装置１７は、第２の電力供給装置１６から供給された電力を用いて所定の周波数によるクロックを生成し、生成したクロックを、クロック線Ｌ３を介して、不揮発性メモリモジュール１５に供給する。ＣＰＵ１３、メモリ制御装置１４へのクロックは、クロック供給装置１７から供給されるか、あるいは、図示しない別のクロック供給装置から供給される。
【００１９】
ＣＰＵ１３は、与えられた各種命令を実行し、メモリ制御装置１４は、ＣＰＵ１３による指示を受けて、制御線Ｌ２を介して、不揮発性メモリモジュール１５における不揮発性メモリコア１８にアクセスする。不揮発性メモリコア１８は、例えばFeRAM、MRAM等の不揮発性ＲＡＭの他、種々の不揮発性のメモリを含み得る。メモリ制御装置１４と不揮発性メモリモジュール１５とはインターフェース部ＩＦを介して接続される。
【００２０】
通常動作時においては、不揮発性メモリモジュール１５におけるアクセス制御装置１９は、メモリ制御装置１４による不揮発性メモリコア１８へのアクセスを許容する。即ち、データ書き込み時は、メモリ制御装置１４は、ＣＰＵ１３によって指定されたアドレスに、指定のデータを書き込む。データ読み出し時は、メモリ制御装置１４は、ＣＰＵ１３によって指定されたアドレスからデータを読み出してＣＰＵ１３に渡す。
【００２１】
ここで、通常動作時は、不揮発性メモリモジュール１５、ＣＰＵ１３及びメモリ制御装置１４に電力及びクロックが供給された状態の時を示す。
【００２２】
これに対し、不揮発性メモリモジュール１５に電力及びクロックが供給されていない状態から、電力及びクロックが供給された状態に遷移する時を、即ち、不揮発性メモリモジュール１５が起動した時を、動作開始時（起動時）と称する。例えば、ユーザによる電源投入時がこの起動時に該当する。
【００２３】
この起動時における動作について以下詳細に説明する。
【００２４】
起動時においては、不揮発性メモリモジュール１５における消去装置２０が、不揮発性メモリコア１８における所定の消去領域２１内のデータを消去する。即ち、消去装置２０は、不揮発性メモリコア１８に対する電力及びクロックの供給が停止状態から供給状態に遷移したことを検知した場合は、消去領域２１内のデータを消去する。消去領域を特定する情報は、あらかじめアクセス制御装置１９あるいは消去装置２０内に格納されている。消去領域には、例えば個人情報、パスワード、著作権データ等が格納される。不揮発性メモリアコアの全領域を消去領域としても良い。消去領域を特定する情報は、上述の通常動作時において、例えばＣＰＵ１３により変更可能であることが好ましい。

【００２５】
消去装置２０によるデータ消去の間、アクセス制御装置１９は、メモリ制御装置１４から不揮発性メモリコア１８へのアクセスを阻止する。例えば、データ消去の間に、メモリ制御装置１４から不揮発性メモリコア１８へのアクセス（書き込み、読み出し等）が発生した場合は、そのアクセス内容を、アクセス制御装置１９が一時的に記憶する。
【００２６】
消去装置２０によるデータの消去が終了すると、消去装置２０は、完了信号をアクセス制御装置１９に出力し、アクセス制御装置１９は、メモリ制御装置１４から不揮発性メモリコア１８へのアクセスを許容する（有効にする）。アクセス制御装置１９が、消去装置２０によるデータ消去の間に、メモリ制御装置１４からのアクセス内容を記憶した場合は、そのアクセス内容を不揮発性メモリコア１８に出力する。不揮発性メモリコア１８は、そのアクセス内容に応じた処理を実行する。
【００２７】
上述した不揮発性モジュール１５は、アクセス制御装置１９、消去装置２０及び不揮発性メモリコア１８が同一の半導体基板上に形成されることにより構成されてもよいし、それぞれあるいは任意の組み合わせが別個の半導体基板上に形成されてこれらが同一のパッケージに含まれる場合も含む。
【００２８】
また、不揮発性メモリシステムは、例えば、不揮発性メモリモジュール１５、第１の電力供給装置１１及びクロック供給装置１７がそれぞれ別個のチップとして構成される場合や、アクセス制御装置１９、消去装置２０、不揮発性メモリコア１８、第１の電力供給装置及びクロック供給装置１７の任意の組み合わせがそれぞれ別個のチップとして構成される場合、これらが同一のチップ上に形成される場合も含む。
【００２９】
以上のように、本実施の形態によれば、不揮発性メモリモジュールの起動時、即ち、不揮発性メモリコアの起動時に、不揮発性メモリコアへのアクセスを不可としつつ、不揮発性メモリコア内のデータを消去するようにしたので、不揮発性メモリコア内のデータを第３者から有効に保護できる。例えば、不揮発性メモリモジュールが第３者によって不正にシステムから取り出された場合でも、電源投入時に、不揮発性メモリコア内のデータが自動的に消去されるので、第３者によって機密情報や著作権データ等が読み出されることを有効に防止できる。
【００３０】
図３は、本発明の第２の実施の形態に従った不揮発性メモリモジュールの構成を示す図である。
【００３１】
上述した第１の実施の形態では、不揮発性メモリモジュール１５が起動する度に、消去装置２０によるデータの消去が実行されたが、本実施の形態では、不揮発性メモリモジュール１５の起動が所定回数生じた時点で、データの消去が実行される。以下、本実施の形態について詳しく説明する。
【００３２】
図３に示すように、不揮発性メモリコア１８内には、「残り起動回数」を示す数値を格納する回数記録領域２２が配置される。不揮発性メモリモジュール１５が起動する度に、消去装置２０によってこの値が「１」減算される。そして、この値が「０」になると、消去装置２０は、データの消去を実行する。
【００３３】
消去装置２０は、データの消去を実行すると、回数記録領域２２内に、所定の数値（使用回数制限値）を格納する。従って、例えば、データの消去の後、所定の数値として、「１０」が格納された場合、この後、さらに起動が１０回発生した時点で、再びデータの消去が実行される。
【００３４】

回数記録領域２２内への数値の格納は、消去装置２０が、通常動作時にＣＰＵ１３から設定指示を受け、この設定指示に基づいて行うことも可能である。消去装置２０は、ＣＰＵ１３からの設定指示を受けると、回数記録領域２２内の数値を確認し、「０」であれば、設定指示に基づいて回数記録領域２２内に数値を入力し、「０」でなければ、前回の設定を優先し、設定指示を実行しない。

【００３５】

以上のように、本実施の形態によれば、不揮発性メモリモジュールが所定の回数だけ起動したら、不揮発性メモリコア内のデータを消去するようにしたので、種々の事情を考慮したデータ消去機能の使用が可能になる。例えば、本不揮発性メモリモジュールを搭載した端末をあるサーバに接続する際にパスワードの入力を必要とする場合に、通常はメモリコアに記憶されたパスワードを用いて自動接続すると共に、定期的にメモリコア内のパスワードを消去することで、ユーザに定期的にパスワードの入力を求めることが可能となる。また、この端末をあるサーバに接続する回数を制限する場合では、その実装として、接続に必要な情報を消去対象とすることで、所定の回数起動後に接続できなくすることも考えられる。

【００３６】

図４は、本発明の第３の実施の形態に従った不揮発性メモリモジュールの構成を示すブロック図である。

【００３７】

図４に示すように、メモリ制御装置１４（図２参照）は、不揮発性メモリコア１８にデータを書き込む際、誤り検出コード領域２３に誤り検出コードを格納する。この誤り検出コードは、後に不揮発性メモリコア１８からデータを読み出した際、このデータに誤りが無いかどうか、即ち、書き込んだデータと読み出したデータとが一致しているか否かを検査するために用いるものである。誤り検出コードとしては、例えば書き込みデータから算出されるチェックサム等がある。このような誤り検出の手法は周知であるので、ここでは詳細な説明は省略する。

【００３８】

誤り検査装置２４は、不揮発性メモリモジュール１５の起動時に、不揮発性メモリコア１８内のデータに誤りが無いかを、誤り検出コード領域２３内の誤り検出コードを用いて検査する。検査対象となるメモリ領域は、不揮発性メモリコア１８内の全領域でもよいし、あらかじめ指定された領域でもよい。誤り検査装置２４がこの検出処理を行っている間は、アクセス制御装置１９は、メモリ制御回路１４（図２参照）による不揮発性メモリコア１８へのアクセスを阻止する。

【００３９】

誤り検査装置２４は、データに誤りが無い場合は、その旨をアクセス制御装置１９に送出し、アクセス制御装置１９は、メモリ制御回路１４（図２参照）から不揮発性メモリコア１８へのアクセスを有効にする。

【００４０】

一方、誤り検査装置２４は、データ誤りが存在した場合は、誤りデータの格納されたメモリ領域を消去装置２０に通知し、消去装置２０は、そのメモリ領域内のデータを消去する。誤り検査装置２４は、検査を終えると、その旨を消去装置２０に通知し、消去装置２０は、誤り検査装置２４によって指定された全てのメモリ領域内のデータを消去したら、終了通知をアクセス制御装置１９に送出する。アクセス制御装置１９は、メモリ制御装置１４（図２参照）による不揮発性メモリコア１８へのアクセスを有効にする。

【００４１】

以上のように、本実施の形態によれば、不揮発性メモリモジュールの起動時に不揮発性メモリコア内のデータに誤りがあるか否かを検査し、データに誤りがある場合は、少なくともそのデータを消去するようにしたので、不揮発性メモリコア内に誤ったデータを保持することによる問題を未然に防止できる。

【００４２】

例えば、ユーザを識別するコードが不揮発性メモリコアに格納されおり、ハードエラー等で、そのコードが、例えば他人の識別コードに変わったとする。もし、ユーザが、その状態で、そのコードに基づいて、認証を要するサーバにアクセスすると、そのユーザは不正アクセスであると判断される恐れがある。しかし、本実施の形態では、このようにデータが変わってしまった場合は、自動時にデータが消去されるので、このような問題を未然に防止できる。

【図面の簡単な説明】

【００４３】

【図１】本発明の第１の実施の形態に従った不揮発性メモリモジュールの構成を示す図である。

【図２】図１の不揮発性メモリモジュールを適用した不揮発性メモリシステムの構成を示す図である。

【図３】本発明の第２の実施の形態に従った不揮発性メモリモジュールの構成を示す図である。

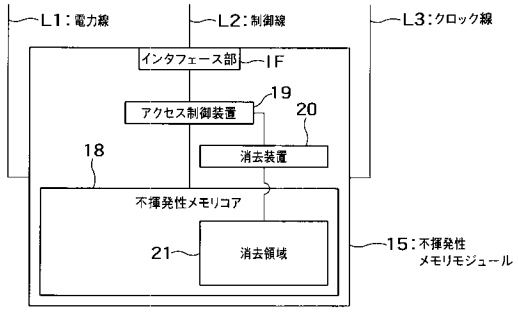
【図４】本発明の第３の実施の形態に従った不揮発性メモリモジュールの構成を示す図である。

【符号の説明】

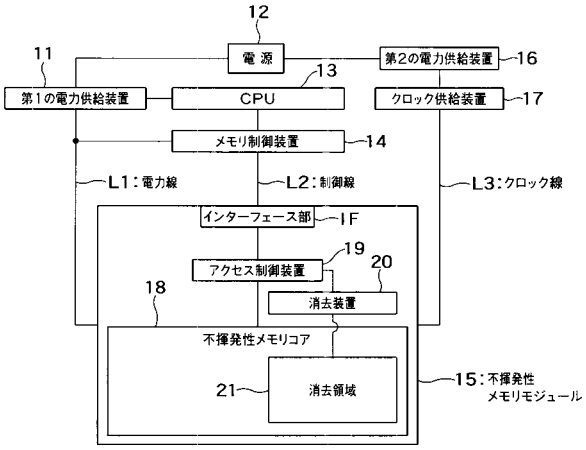
【００４４】

１１　第１の電力供給装置
１２　電源
１３　ＣＰＵ
１４　メモリ制御装置
１５　不揮発性メモリモジュール
１６　第２の電力供給装置
１７　クロック供給装置
１８　不揮発性メモリコア
１９　アクセス制御装置
２０　消去装置
２１　消去領域
２２　回数記録領域
２３　誤り検出コード領域
２４　誤り検査装置
Ｌ１　電力線
Ｌ２　制御線
Ｌ３　クロック線
ＩＦ　インターフェース部

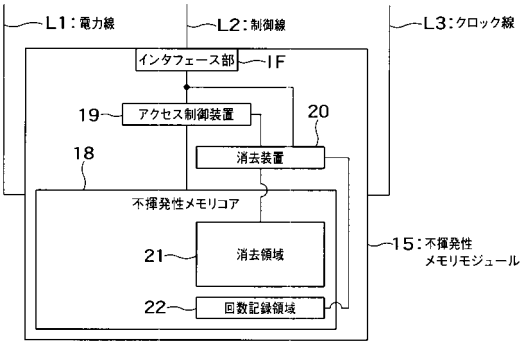
【図１】


L1：電力線
L2：制御線
L3：クロック線
インタフェース部
IF
アクセス制御装置
19
20
消去装置
18
不揮発性メモリコア
21
消去領域
15：不揮発性
メモリモジュール

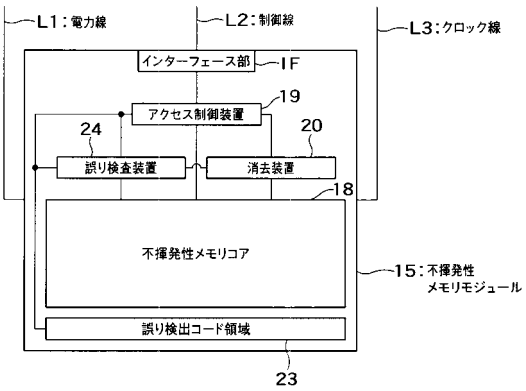
【図２】


12
電 源
11
第2の電力供給装置
16
第1の電力供給装置
CPU
13
クロック供給装置
17
メモリ制御装置
14
L1：電力線
L2：制御線
L3：クロック線
インターフェース部
IF
19
アクセス制御装置
20
18
消去装置
不揮発性メモリコア
21
消去領域
15：不揮発性
メモリモジュール

【図３】


L1：電力線
L2：制御線
L3：クロック線
インタフェース部
IF
19
アクセス制御装置
20
18
消去装置
不揮発性メモリコア
21
消去領域
22
回数記録領域
15：不揮発性
メモリモジュール

【図４】


L1：電力線
L2：制御線
L3：クロック線
インターフェース部
IF
19
アクセス制御装置
24
20
誤り検査装置
消去装置
18
不揮発性メモリコア
15：不揮発性
メモリモジュール
誤り検出コード領域
23

フロントページの続き

(72)発明者　江　野　聡　史
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝マイクロエレクトロニクスセンター内

Ｆターム(参考) 5B017 AA07　BA08　CA12