(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4584044号
(P4584044)
(45)発行日　平成22年11月17日(2010.11.17)　(24)登録日　平成22年9月10日(2010.9.10)

(51)Int.Cl.　　F I
G06F 21/02 (2006.01)　　G06F 12/14 510C
G06F 21/24 (2006.01)　　G06F 12/14 560D

請求項の数 14　(全 29 頁)

(21)出願番号　特願2005-178829 (P2005-178829)
(22)出願日　平成17年6月20日 (2005.6.20)
(65)公開番号　特開2006-350885 (P2006-350885A)
(43)公開日　平成18年12月28日 (2006.12.28)
審査請求日　平成20年4月14日 (2008.4.14)

(73)特許権者　302062931
ルネサスエレクトロニクス株式会社
神奈川県川崎市中原区下沼部１７５３番地
(74)代理人　100064746
弁理士　深見　久郎
(74)代理人　100085132
弁理士　森田　俊雄
(74)代理人　100083703
弁理士　仲村　義平
(74)代理人　100096781
弁理士　堀井　豊
(74)代理人　100109162
弁理士　酒井　將行
(74)代理人　100111246
弁理士　荒川　伸夫

最終頁に続く

(54)【発明の名称】半導体装置

(57)【特許請求の範囲】
【請求項１】
複数のブロックに分割されたデータ領域と、ブロック毎にアクセスを禁止するための保護情報が格納される保護情報領域とを含む不揮発性記憶部と、
前記保護情報領域に格納された前記保護情報を読出す読出部と、
いずれかのブロックに対するアクセスの禁止を解除する前に、当該ブロックに格納されているデータを消去する制御部とを備え、
前記制御部は、前記読出部から前記保護情報を受け、前記保護情報によりアクセスを禁止され得るいずれかのブロックにおいてアクセスが禁止されていれば、前記保護情報によりアクセスを禁止され得るすべてのブロックへのアクセスを禁止する、半導体装置。
【請求項２】
演算部をさらに備え、
前記制御部は、起動時における前記演算部からのアクセスであれば、前記保護情報にかかわらず、アクセスを許可する、請求項１に記載の半導体装置。
【請求項３】
前記保護情報は、ブロック毎にそれぞれ複数のフラグを含み、
前記複数のフラグに含まれる各々のフラグは、対応のブロックに対するアクセスを禁止するため互いに同値に設定され、
前記制御部は、いずれかのブロックに対する前記保護情報を前記読出部から受け、前記保護情報に含まれる前記複数のフラグのうちいずれか１つでもアクセスを禁止する値に設

定されていれば、前記保護情報により当該ブロックに対するアクセスが禁止されていると判断する、請求項１または２に記載の半導体装置。

【請求項４】

前記保護情報は、前記データ領域に含まれる複数のブロックのうち、少なくとも１以上のブロックに対してアクセスを禁止する、請求項１～３のいずれか１項に記載の半導体装置。

【請求項５】

前記データ領域は、前記保護情報領域を含む、請求項１～４のいずれか１項に記載の半導体装置。

【請求項６】

複数のブロックに分割されたデータ領域と、ブロック毎にそれぞれアクセスを禁止するための第１および第２の保護情報が格納される保護情報領域とを含む不揮発性記憶部と、

前記保護情報領域に格納された前記第１および第２の保護情報を読出す読出部と、

いずれかのブロックに対するアクセスの禁止を解除する前に、当該ブロックに格納されているデータを消去する制御部と、

前記データ領域に格納された命令コードを読出して処理を実行する演算部とを備え、

前記制御部は、

前記読出部から前記第１の保護情報を受け、前記第１の保護情報によりアクセスを禁止され得るいずれかのブロックにおいてアクセスが禁止されていれば、前記第１の保護情報によりアクセスを禁止され得るすべてのブロックへのアクセスを禁止し、かつ、

前記読出部から受けた前記第２の保護情報に基づいて、前記第２の保護情報によりアクセスを禁止され得るブロックへのアクセスを許可するか否かを決定し、かつ、

前記演算部から前記命令コードの読出しを行なうためのアクセス要求を受けると、前記第２の保護情報にかかわらず当該アクセスを許可する、半導体装置。

【請求項７】

前記制御部は、起動時における前記演算部からのアクセスであれば、前記第１の保護情報にかかわらず、アクセスを許可する、請求項６に記載の半導体装置。

【請求項８】

前記第１の保護情報は、ブロック毎にそれぞれ複数のフラグを含み、

前記複数のフラグに含まれる各々のフラグは、対応のブロックに対するアクセスを禁止するため互いに同値に設定され、

前記制御部は、いずれかのブロックに対する前記第１の保護情報を前記読出部から受け、前記第１の保護情報に含まれる前記複数のフラグのうちいずれか１つでもアクセスを禁止する値に設定されていれば、前記第１の保護情報により当該ブロックに対するアクセスが禁止されていると判断する、請求項６または７に記載の半導体装置。

【請求項９】

前記第２の保護情報は、ブロック毎にそれぞれ複数のフラグを含み、

前記複数のフラグに含まれる各々のフラグは、対応のブロックに対するアクセスを禁止するため互いに同値に設定され、

前記制御部は、いずれかのブロックに対する前記第２の保護情報を前記読出部から受け、前記第２の保護情報に含まれる前記複数のフラグのうちいずれか１つでもアクセスを禁止する値に設定されていれば、前記第２の保護情報により当該ブロックに対するアクセスが禁止されていると判断する、請求項６～８のいずれか１項に記載の半導体装置。

【請求項１０】

前記制御部は、前記第１および第２の保護情報により同一のブロックに対するアクセスが禁止されている場合には、前記第１の保護情報を無視する、請求項６～９のいずれか１項に記載の半導体装置。

【請求項１１】

前記制御部は、さらに、前記読出部から前記第２の保護情報を受け、前記第２の保護情報によりアクセスを禁止され得るいずれかのブロックにおいてアクセスが禁止されていれ

ば、前記第２の保護情報によりアクセスを禁止され得るすべてのブロックに対するアクセスが禁止されていると判断する、請求項６～１０のいずれか１項に記載の半導体装置。
【請求項１２】
前記第２の保護情報は、少なくとも２以上のブロックに対するアクセスを禁止し、
前記制御部は、前記第２の保護情報がアクセスを禁止し得るブロックのそれぞれに対して、互いに独立にアクセスを許可するか否かを決定する、請求項６～１０のいずれか１項に記載の半導体装置。
【請求項１３】
前記第１の保護情報は、前記データ領域に含まれる複数のブロックのうち、少なくとも１以上のブロックに対してアクセスを禁止する、請求項６～１２のいずれか１項に記載の半導体装置。
【請求項１４】
前記データ領域は、前記保護情報領域を含む、請求項６～１３のいずれか１項に記載の半導体装置。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、不揮発性記憶部を備える半導体装置に関し、特にデータ機密保護機能を有する半導体装置に関するものである。
【背景技術】
【０００２】
従来から、さまざまな用途に用いられるマイクロコンピュータ（以下、マイコンと称す）では、フラッシュメモリやＥＥＰＲＯＭ（Electrical Erasable and Programmable Read Only Memory）などの不揮発性記憶部（以下、不揮発性メモリと称す）を備えたものが一般的となっている。不揮発性メモリは、一旦データが書込まれると電源が遮断されてもそのデータを保持し、かつ、データの書換えも自由に行なうことができる。そのため、プログラムを不揮発性メモリに格納して製品に組込んだマイコンに対して、プログラムの修正や新たな機能の追加といったいわゆるアップデートを容易に行なうことができるという利点がある。
【０００３】
一方、上述のような不揮発性メモリを備えたマイコンでは、当該マイコンが組込まれた製品の使用者（以下、エンドユーザと称す）などにより、その格納しているプログラムが書換えられると、動作不具合や人的被害などの発生が懸念される。また、競業者などにより、プログラムの内容を不正に読出されることも懸念される。そこで、エンドユーザによるデータの読出しや書換え（以下、アクセスと称す）を防止するため、マイコンには、機密保護（以下、プロテクトと称す）機能を付加することが一般的となっている。
【０００４】
このようなプロテクト機能は、たとえば、不揮発性メモリ内において、データが格納されるデータ領域に加え、そのデータ領域に対するプロテクトを設定するためのプロテクト情報領域を配置し、そのプロテクト情報領域に格納されるプロテクト設定に応じて、ハードウェア回路によりアクセスを禁止する構成で実現される。
【０００５】
特許文献１には、メモリアレイのブロックグループ単位で、ライトプロテクトの状態を柔軟に設定できる半導体記憶装置が開示されている。
【０００６】
一方、プロテクトが設定されたプログラムのアップデートを行なうためには、プロテクト設定を解除した上で、プログラムの書換えを行なう必要がある。したがって、プロテクト機能を付加する場合には、付随的にプロテクトの解除機能を備えておく必要がある。
【０００７】
プロテクトの解除機能は、たとえば、マイコンと接続される外部装置から特定の信号を

与えてプロテクトを解除する構成や、入力されたＩＤ（パスワード）が特定のＩＤと一致した場合にのみプロテクトが解除される構成で実現される場合もある。しかしながら、このような構成においては、構成の存在自体がセキュリティーホールとなる。すなわち、悪意の第三者が当該マイコンを詳細に調査するなどして、特定の信号や特定のＩＤを知ると、プロテクト機能は無効化されてしまう。

【０００８】

そこで、プロテクトが解除される前に、そのプロテクトされているデータを消去する構成が提案されている。

【０００９】

特許文献２には、プロテクト設定の解除が指示されると、プロテクトの設定を無視して、格納されているすべてのデータを消去する不揮発性半導体記憶装置が開示されている。また、特許文献３には、不揮発性メモリのデータを消去した後にのみ、不揮発性メモリに対するアクセスを許可するマイクロコンピュータ装置が開示されている。

【００１０】

さらに、一般的に不揮発性メモリは、複数のブロックに分割されており、データの読出しおよび書込みはブロック単位で行なわれる。そのため、特許文献３には、ブロック単位でプロテクトの設定を行なう構成が開示されている。

【００１１】

ところで、近年のマイコンの高性能化に伴い、マイコンを動作させるためのプログラムも複雑化・大規模化している。そのため、プログラム製作者は、一からプログラムを製作するより、予め機能別に用意されたライブラリソフトウェアをプログラム中で読出す（サブルーチンコールする）ことでプログラム製作の効率化を図っている。このようなライブラリソフトウェアの提供者は、マイコンの製造者以外であることも多く、ＩＰ（Intellectual Property）ベンダと呼ばれる。

【特許文献１】特開平１１－１２０７８１号公報
【特許文献２】特開２００１－０１４８７１号公報
【特許文献３】特開２００３－２０３０１２号公報

【発明の開示】

【発明が解決しようとする課題】

【００１２】

しかしながら、特許文献２に開示される構成では、プロテクトを解除しようとすると、その都度すべてのメモリが消去されるので、データ領域の容量に比較して格納されているプログラムの容量が小さい場合などには、その消去に要する時間が相対的に大きくなり、マイコンの処理速度の低下をもたらすという問題点があった。一方、特許文献３に開示されている構成では、ブロック単位でプロテクト設定が行なわれるので、プロテクト対象となるプログラムなどが複数のブロックに格納される場合などには、その格納される複数のブロックのすべてに対してプロテクト設定を行なう必要があるが、その処理は複雑となるため、プロテクト設定のミスによりデータの漏洩が生じるという問題点があった。

【００１３】

また、ＩＰベンダにとって、ライブラリソフトウェアをプログラム中で読出して実行されることは通常の使用であり問題はないが、ライブラリソフトウェア自体（命令コード）の内容が読出されてしまうと、第三者に不当にコピーされ、開発費が回収できない事態やノウハウの流出が生じるという問題があった。そのため、プログラム製作者およびエンドユーザに対して、ライブラリソフトウェア自体の内容が読出されないように、プロテクトを設定する必要が生じている。

【００１４】

しかしながら、従来のプロテクト機能においては、プログラム中の読出し（サブルーチンコール）であるか否かにかかわらず、プロテクトされているデータは、一律にアクセスが禁止されるため、プロテクトを設定してしまうと、ライブラリソフトウェアを利用することができずジレンマに陥るという問題点があった。

【００１５】
そこで、この発明は、かかる問題を解決するためになされたものであり、その第１の目的は、処理速度を低下させることなく、かつ、容易な処理により高いデータ機密保護機能を実現する半導体装置を提供することである。
【００１６】
また、この発明の第２の目的は、格納される命令コード自体の機密保護を実現すると同時に、命令コードに基づく処理を実行できる半導体装置を提供することである。
【００１７】
また、この発明の第３の目的は、上記の第１および第２の目的を同時に実現する半導体装置を提供することである。
【課題を解決するための手段】
【００１８】
第１の発明によれば、複数のブロックに分割されたデータ領域と、ブロック毎にアクセスを禁止するための保護情報が格納される保護情報領域とを含む不揮発性記憶部と、保護情報領域に格納された保護情報を読出す読出部と、いずれかのブロックに対するアクセスの禁止を解除する前に、当該ブロックに格納されているデータを消去する制御部とを備える半導体装置である。そして、制御部は、読出部から保護情報を受け、保護情報によりアクセスを禁止され得るいずれかのブロックにおいてアクセスが禁止されていれば、保護情報によりアクセスを禁止され得るすべてのブロックへのアクセスを禁止する。
【００１９】
また、第２の発明によれば、複数のブロックに分割されたデータ領域と、ブロック毎にアクセスを禁止するための保護情報が格納される保護情報領域とを含む不揮発性記憶部と、保護情報領域に格納された保護情報を読出す読出部と、いずれかのブロックに対するアクセスの禁止を解除する前に、当該ブロックに格納されているデータを消去する制御部と、データ領域に格納された命令コードを読出して処理を実行する演算部とを備える半導体装置である。そして、制御部は、読出部から受けた保護情報に基づいて、保護情報によりアクセスを禁止され得るブロックへのアクセスを許可するか否かを決定し、かつ、演算部から命令コードの読出しを行なうためのアクセス要求を受けると、保護情報にかかわらず当該アクセスを許可する。
【００２０】
また、第３の発明によれば、複数のブロックに分割されたデータ領域と、ブロック毎にそれぞれアクセスを禁止するための第１および第２の保護情報が格納される保護情報領域とを含む不揮発性記憶部と、保護情報領域に格納された第１および第２の保護情報を読出す読出部と、いずれかのブロックに対するアクセスの禁止を解除する前に、当該ブロックに格納されているデータを消去する制御部と、データ領域に格納された命令コードを読出して処理を実行する演算部とを備える半導体装置である。そして、制御部は、読出部から第１の保護情報を受け、第１の保護情報によりアクセスを禁止され得るいずれかのブロックにおいてアクセスが禁止されていれば、第１の保護情報によりアクセスを禁止され得るすべてのブロックへのアクセスを禁止し、かつ、読出部から受けた第２の保護情報に基づいて、第２の保護情報によりアクセスを禁止され得るブロックへのアクセスを許可するか否かを決定し、かつ、演算部から命令コードの読出しを行なうためのアクセス要求を受けると、第２の保護情報にかかわらず当該アクセスを許可する。
【発明の効果】
【００２１】
第１の発明によれば、アクセスの禁止が解除される場合において、ブロック単位でデータが消去される一方、アクセスを禁止され得るすべてのブロックに対するアクセスの禁止が解除されない限り、いずれのブロックに対するアクセスも許可されない。よって、すべてのブロックに格納されているデータを一括で消去する場合に比較して、効率的にデータ消去ができるので、処理速度の低下を抑制でき、かつ、すべてのブロックに対するアクセスの禁止を一体的に行なうことができるので、高いデータ機密保護機能を実現できる。

【００２２】
また、第２の発明によれば、アクセスの禁止が設定されているブロックに対しては、アクセスが許可されず、かつ、アクセスの禁止を解除する場合には、必ず当該ブロックに格納されているデータは消去される。例外的に、演算部がデータ領域に格納されている処理コードを読出して処理を実行する場合に限り、アクセス先のブロックにおける保護情報にかかわらずアクセスが許可される。よって、命令コード自体の機密保護が確保されると同時に、演算部は命令コードに基づく処理の実行を実現できる。
【００２３】
また、第３の発明によれば、第１の保護情報によるアクセスの禁止が解除される場合において、ブロック単位でデータが消去される一方、アクセスを禁止され得るすべてのブロックに対するアクセスの禁止が解除されない限り、いずれのブロックに対するアクセスも許可されない。よって、すべてのブロックに格納されているデータを一括で消去する場合に比較して、効率的にデータ消去ができるので、処理速度の低下を抑制でき、かつ、すべてのブロックに対するアクセスの禁止を一体的に行なうことができるので、高いデータ機密保護機能を実現できる。また、第２の保護情報によりアクセスの禁止が設定されているブロックに対しては、アクセスが許可されず、かつ、アクセスの禁止を解除する場合には、必ず当該ブロックに格納されているデータは消去される。例外的に、演算部がデータ領域に格納されている処理コードを読出して処理を実行する場合に限り、アクセス先のブロックにおける保護情報にかかわらずアクセスが許可される。よって、命令コード自体の機密保護が確保されると同時に、演算部は命令コードに基づく処理の実行を実現できる。
【発明を実施するための最良の形態】
【００２４】
この発明の実施の形態について、図面を参照しながら詳細に説明する。なお、図中の同一または相当部分については、同一符号を付してその説明は繰返さない。
【００２５】
［実施の形態１］
実施の形態１では、ＩＰベンダまたはプログラム製作者がエンドユーザに対するプロテクトを目的とするプロテクト機能について説明する。
【００２６】
図１は、実施の形態１に従う半導体装置１０１の概略構成図である。
図１を参照して、半導体装置１０１は、データバス９８と、演算部（ＣＰＵ：Central Processing Unit；以下、ＣＰＵと称す）９０と、不揮発性メモリ１と、読出部１２と、制御部１０と、電源部９７とからなる。
【００２７】
データバス９８は、ＣＰＵ９０、制御部１０、外部メモリ（図示しない）および外部装置（図示しない）などを互いに接続し、データの授受を仲介する。
【００２８】
ＣＰＵ９０は、データバス９８を介して不揮発性メモリ１との間でデータの授受を行なう。そして、ＣＰＵ９０は、外部からリセット信号を受けると、後述する動作モードに応じて、不揮発性メモリ１または外部メモリ（図示しない）に格納されているプログラムを読出して起動する。さらに、ＣＰＵ９０は、不揮発性メモリ１からプログラムを読出して起動する場合には、そのモード信号を制御部１０へ出力する。
【００２９】
不揮発性メモリ１は、フラッシュメモリやＥＥＰＲＯＭなどの半導体からなり、複数のブロックに分割されたデータ領域１．１とプロテクト情報領域１．２とを含む。
【００３０】
データ領域１．１は、ブロック１，２，・・・，Ｎに分割されており、それぞれデータ１，２，・・・，Ｎが格納される。
【００３１】
プロテクト情報領域１．２は、データ領域１．１におけるブロックに対応するように分

割されており、データ領域のそれぞれのブロックに対するプロテクト設定が格納される。実施の形態１におけるプロテクト情報領域１．２には、それぞれ１ビットからなる全体保護フラグ１ａ，２ａ，・・・，Ｎａが格納され、このフラグ値（「０」または「１」）に応じて、データ領域１．１のそれぞれのブロックに対するプロテクト設定の有無が判断される。

【００３２】

読出部１２は、不揮発性メモリ１のプロテクト情報領域１．２に格納されている全体保護フラグ１ａ，２ａ，・・・，Ｎａを読出し、制御部１０へ出力する。そして、読出部１２は、読出回路１６と、読出レジスタ１８とからなる。

【００３３】

読出回路１６は、外部からのリセット信号や電源部９７からの投入信号を受けて、プロテクト情報領域１．２に格納されている全体保護フラグ１ａ，２ａ，・・・，Ｎａを読出し、読出レジスタ１８へ出力する。

【００３４】

読出レジスタ１８は、全体保護フラグ１ａ，２ａ，・・・，Ｎａのそれぞれを一旦格納し、その値を制御部１０へ出力する。読出レジスタ１８は、読出回路１６から新たに全体保護フラグを受けるまで、その値を保持する。そのため、読出レジスタ１８から出力される値は、外部からのリセット信号や電源部９７からの投入信号を受けるタイミングでのみ更新される。

【００３５】

制御部１０は、ＯＲ回路１５と、起動モード判断部（判断部ａ）１４と、制御回路１１とからなる。

【００３６】

ＯＲ回路１５は、読出レジスタ１８から全体保護フラグ１ａ，２ａ，・・・，Ｎａを受けて論理和（ＯＲ）演算を行ない、全体保護フラグ１ａ，２ａ，・・・，Ｎａのうちいずれか１つでもプロテクト設定がなされていれば、起動モード判断部１４へ「ＯＮ」を出力する。

【００３７】

起動モード判断部１４は、ＯＲ回路１５から「ＯＮ」を受けている場合には、データ領域１．１のすべてのブロックに対する読出しおよび書込み（以下、アクセスとも称す）を禁止させるプロテクト制御信号を制御回路１１へ出力する。そして、起動モード判断部１４は、例外的にＣＰＵ９０からモード信号を受けている場合においては、そのアクセスを禁止させるプロテクト制御信号をマスクする。これは、ＣＰＵ９０は、不揮発性メモリ１に格納されているプログラムを読出して起動するため、アクセスの禁止が解除されていないと、ＣＰＵ９０が起動できないという問題が生じるからである。

【００３８】

制御回路１１は、データバスを介して、データ領域１．１のいずれかのブロックに対するプロテクトの設定解除の要求を受けると、当該ブロックに格納されているデータを消去し、そのデータが消去されたことを確認した後に、プロテクト情報領域１．２に格納されている当該ブロックに対応する保護フラグの値を変更し、プロテクトの設定を解除する。また、制御回路１１は、データバスを介して、データ領域１．１のいずれかのブロックに対するアクセスの要求を受けると、起動モード判断部１４からアクセスを禁止するプロテクト制御信号を受けているか否かを判断する。そして、制御回路１１は、アクセスを禁止するプロテクト制御信号を受けていなければ、そのアクセスを許可し、その要求先のブロックに格納されているデータを読出し、またはその要求先のブロックへデータを書込む。さらに、制御回路１１は、データバスを介して、データ領域１．１のいずれかのブロックに対するプロテクトの設定要求を受けると、プロテクト情報領域１．２に格納されている当該ブロックに対応する全体保護フラグの値を変更し、プロテクトを設定する。

【００３９】

電源部９７は、外部からの指令を受けて、半導体装置１０１の各部への電源供給を開始

し、かつ、その電源供給の開始と同時に投入信号を読出回路１６へ出力する。

【００４０】

上述したように、半導体装置１０１は、複数の動作モードを有し、その動作モードに応じて、プロテクト設定の有効および無効を判断する必要がある。

【００４１】

図２は、半導体装置１０１の動作モードを説明するための図である。

図２（ａ）は、マイコン内蔵メモリプログラム起動モードである。

【００４２】

図２（ｂ）は、マイコン外部メモリプログラム起動モードである。

図２（ｃ）は、ＣＰＵ非動作起動モードである。

【００４３】

図２（ａ）を参照して、「マイコン内蔵メモリプログラム起動モード」では、ＣＰＵ９０は、不揮発性メモリ１からデータバス９８を介してプログラムを読出し、起動する。そのため、ＣＰＵ９０が起動できるように、不揮発性メモリ１のプロテクト設定を一時的に無効にする必要がある。

【００４４】

図２（ｂ）を参照して、「マイコン外部メモリプログラム起動モード」では、半導体装置１０１にデータバス９８を介して、外部メモリ２００が接続される。そして、ＣＰＵ９０は、外部メモリ２００からデータバス９８を介してプログラムを読出し、起動する。ここで、ＩＰベンダおよびプログラム製作者以外の何人でも外部メモリ２００にプログラムを書込むことが可能であるので、プロテクト設定されたブロックに格納されているデータを読出すような悪意のあるプログラムが実行されるおそれがある。そのため、「マイコン外部メモリプログラム起動モード」では、ＣＰＵ９０の処理状態にかかわらず不揮発性メモリ１のプロテクト設定を常時有効とする。

【００４５】

図２（ｃ）を参照して、「ＣＰＵ非動作起動モード」では、半導体装置１０１のデータバス９８に外部装置２０２が接続される。そして、外部装置２０２は、ＣＰＵ９０の処理にかかわらず、不揮発性メモリ１に対して直接アクセスを行なう。ここで、ＩＰベンダおよびプログラム製作者以外の何人でも半導体装置１０１に外部装置２０２を接続できるので、悪意のある第三者が不揮発性メモリ１に格納されているデータを直接読出すおそれがある。そのため、「ＣＰＵ非動作起動モード」では、ＣＰＵ９０の処理状態にかかわらず不揮発性メモリ１のプロテクト設定を常時有効とする。

【００４６】

（プロテクト設定）

データ領域１．１のいずれのブロックに対してもプロテクトが設定されていない状態において、ＣＰＵ９０または外部からプロテクト対象のデータが転送されると、制御回路１１は、転送されたデータを所定のブロックに書込む。さらに、ＣＰＵ９０または外部から当該データに対するプロテクトの設定が要求されると、制御回路１１は、データを格納したブロックに対応するプロテクト情報領域１．２の全体保護フラグの値を変更し、プロテクト設定を行なう。以下、同様の処理により、不揮発性メモリ１に格納されるすべてのデータをプロテクトすることができる。

【００４７】

なお、制御回路１１は、プロテクトされているブロックに対するデータの読出し要求を受けると、格納されているデータと異なるデータを応答する。また、制御回路１１は、プロテクトされているブロックに対するデータの書込み要求を受けると、何らの動作も行なわない（無視）、または、その要求を違反動作として扱う。

【００４８】

（プロテクト解除）

ＣＰＵ９０または外部からデータ領域１．１のいずれかのブロックに対するプロテクトの設定解除が要求されると、制御回路１１は、指定されたブロックに格納されているデー

タを消去する。そして、制御回路１１は、消去ベリファイ動作などにより、格納されているデータの消去が完了したことを確認した後、そのブロックに対応するプロテクト情報領域１．２の全体保護フラグの値を変更し、当該ブロックのプロテクト設定を解除する。

【００４９】

一方、制御回路１１は、データ領域１．１のいずれかのブロックに対するプロテクト設定がされていれば、起動モード判断部１４からアクセスを禁止するプロテクト制御信号を受けるため、すべてのブロックに対するアクセスを禁止する。そのため、１つのブロックに対するプロテクト設定が解除されたとしても、プロテクト設定がされている他のブロックが存在すれば、データ領域１．１のすべてのブロックに対してプロテクトが設定されていることになる。すなわち、制御回路１１は、データ領域１．１のすべてのブロックに対してプロテクトの設定を解除しなければ、データ領域１．１のいずれのブロックに対してもアクセスを許可しない。

【００５０】

そこで、ＣＰＵ９０または外部から、データ領域１．１のすべてのブロックに対して、プロテクトの設定解除が要求され、すべてのブロックに格納されているデータが消去されて、初めてデータ領域１．１へのアクセスが可能となる。

【００５１】

なお、読出部１２は、外部からのリセット信号や電源部９７からの投入信号を受けるまで、保護フラグの値を更新しないので、プロテクト設定または設定解除は、半導体装置１０１がリセットされた場合または、電源が再投入された場合に有効となる。

【００５２】

以上のように、少なくともデータ領域１．１のいずれか１つのブロックに対してプロテクト設定が行なわれれば、すべてのブロックに対してプロテクトが有効となる。一方、データ領域１．１のすべてのブロックに対してプロテクト設定が解除されなければ、すべてのブロックに対してプロテクト設定が解除されない。

【００５３】

すなわち、データ領域１．１のプロテクトを設定する場合には、ブロック単位で容易に行なうことができるが、データ領域１．１のプロテクト設定を解除する場合には、すべてのブロックのそれぞれに対して複雑な処理が必要となる。

【００５４】

この発明の実施の形態１によれば、データ領域のプロテクト設定を解除する場合には、ブロック単位でデータ消去および保護フラグ値の変更が行なわれる。そのため、すべてのブロックを一括で消去する場合に比較して、効率的にデータ消去が行なえるので、処理速度の低下を抑制できる。一方、データ領域のプロテクト設定を解除するためには、すべてのブロックに対するプロテクト設定を解除しなければならない。よって、プロテクト設定を解除するためには、すべてのブロックに格納されているデータを消去する必要があり、高いデータ機密保護機能を実現できる。

【００５５】

また、この発明の実施の形態１によれば、制御部は、ＣＰＵが「マイコン内蔵メモリプログラム起動モード」であれば、ＣＰＵからのアクセスを許可する一方、他のモードであればアクセスを許可しない。よって、半導体装置と接続された外部装置からの要求によるデータ漏洩を防止できる。

【００５６】

［実施の形態２］

実施の形態１においては、ＩＰベンダまたはプログラム製作者がエンドユーザに対するプロテクトを目的としたプロテクト機能を備える半導体装置について説明した。

【００５７】

一方、実施の形態２では、ＩＰベンダがプログラム製作者およびエンドユーザに対するプロテクトを目的としたプロテクト機能を備える半導体装置について説明する。

【００５８】

図３は、実施の形態２に従う半導体装置１０２の概略構成図である。
図３を参照して、半導体装置１０２は、データバス９８と、ＣＰＵ９２と、不揮発性メモリ２と、読出部２２と、制御部２０と、電源部９７とからなる。
【００５９】
データバス９８は、ＣＰＵ９２、制御部２０、外部メモリ（図示しない）および外部装置（図示しない）などを互いに接続し、データの授受を仲介する。
【００６０】
ＣＰＵ９２は、データバス９８を介して不揮発性メモリ２との間でデータの授受を行なう。そして、ＣＰＵ９２は、実施の形態１におけるＣＰＵ９０と同様に、不揮発性メモリ２からプログラムを読出して起動する（「マイコン内蔵メモリプログラム起動モード」の）場合には、そのモード信号を制御部２０へ出力する。
【００６１】
また、ＣＰＵ９２は、プログラムカウンタ（ＰＣ）９５を含み、プログラムカウンタ９５に格納されるプログラムカウンタ値に従い、不揮発性メモリ２から命令コードを読出して処理を実行する。このようなＣＰＵ９２による命令コードの読出しは、命令フェッチと称される。なお、プログラムカウンタ値は、ＣＰＵ９２の処理実行に伴い、順次カウントアップされる。
【００６２】
さらに、ＣＰＵ９２は、不揮発性メモリ２に対するアクセスを実行する際に、その不揮発性メモリ２のアクセス先のアドレス（以下、アクセスアドレスと称す）を制御部２０へ出力する。同時に、ＣＰＵ９２は、そのアクセスが命令フェッチによるものであるか、命令フェッチ以外のデータへのアクセス（以下、データアクセスと称す）によるものであるかを示すステータス信号（以下、アクセスステータスと称す）を制御部２０へ出力する。
【００６３】
不揮発性メモリ２は、フラッシュメモリやＥＥＰＲＯＭなどの半導体からなり、複数のブロックに分割されたデータ領域２．１とプロテクト情報領域２．２とを含む。
【００６４】
データ領域２．１は、ブロック１，２，・・・，Ｍ，・・・，Ｎに分割されており、それぞれデータ１，２，・・・，Ｍ，・・・，Ｎが格納される。
【００６５】
プロテクト情報領域２．２は、データ領域２．１に含まれるブロックのうち所定のブロックに対応するように配置されており、その所定のブロックに対するプロテクト設定が格納される。実施の形態２におけるプロテクト情報領域２．２には、データ領域２．１に含まれるブロック１，２，・・・，Ｍ，・・・，Ｎのうち、ブロックＭに対する１ビットの部分保護フラグＭｂが格納され、このフラグ値（「０」または「１」）に応じて、ブロックＭに対するプロテクト設定の有無が判断される。
【００６６】
読出部２２は、不揮発性メモリ２のプロテクト情報領域２．２に格納されている部分保護フラグＭｂを読出し、制御部２０へ出力する。そして、読出部２２は、読出回路２６と、読出レジスタ２８とからなる。
【００６７】
読出回路２６は、外部からのリセット信号や電源部９７からの投入信号を受けて、プロテクト情報領域２．２に格納されている部分保護フラグＭｂを読出し、読出レジスタ２８へ出力する。
【００６８】
読出レジスタ２８は、部分保護フラグＭｂを一旦格納し、その値を制御部２０へ出力する。読出レジスタ２８は、読出回路２６から新たに部分保護フラグＭｂを受けるまで、その値を保持する。そのため、読出レジスタ２８から出力される値は、外部からのリセット信号や電源部９７からの投入信号を受けるタイミングでのみ更新される。
【００６９】

制御部２０は、アクセスモード判断部（判断部ｂ）２４と、制御回路２１とからなる。
アクセスモード判断部２４は、読出レジスタ２８に格納される部分保護フラグＭｂに基づいて、ブロックMに対するプロテクトの設定がされている場合には、データ領域２．１のブロックMに対するアクセスを禁止させるプロテクト制御信号を制御回路２１へ出力する。そして、アクセスモード判断部２４は、例外的に、ＣＰＵ９２からモード信号を受けている場合で、かつ、ＣＰＵ９２からブロックMに対する命令フェッチによる命令コードの読出しである場合に限り、そのアクセスを禁止させるプロテクト制御信号をマスクする。これは、ＣＰＵ９２においてプログラム製作者により製作されたプログラムが実行される際に、サブルーチンコールだけを許可するためである。

【００７０】

制御回路２１は、データバスを介して、データ領域２．１のブロックMに対するプロテクトの設定解除の要求を受けると、ブロックMに格納されているデータを消去し、そのデータが消去されたことを確認した後に、プロテクト情報領域２．２に格納されているブロックMに対応する部分保護フラグＭｂの値を変更し、プロテクトの設定を解除する。また、制御回路２１は、データバスを介して、データ領域２．１のブロックMに対するアクセスの要求を受けると、起動モード判断部１４からアクセスを禁止するプロテクト制御信号を受けているか否かを判断する。そして、制御回路２１は、アクセスを禁止するプロテクト制御信号を受けていなければ、そのアクセスを許可し、その要求先のブロックMに格納されているデータを読出し、またはその要求先のブロックMへデータを書込む。さらに、制御回路２１は、データバスを介して、データ領域２．１のブロックMに対するプロテクトの設定要求を受けると、プロテクト情報領域２．１に格納されている部分保護フラグＭｂの値を変更し、プロテクトを設定する。

【００７１】

電源部９７については、実施の形態１と同様であるので、詳細な説明は繰返さない。
（プロテクト設定）
データ領域２．１のブロックMに対してプロテクト設定がなされていない状態において、ＣＰＵ９２または外部からプロテクト対象のデータが転送されると、制御回路２１は、転送されたデータをブロックMに書込む。さらに、ＣＰＵ９２または外部から当該データに対するプロテクトの設定が要求されると、制御回路２１は、データを格納したブロックMに対応する部分保護フラグＭｂの値を変更し、プロテクトを設定する。

【００７２】

上述のように、ブロックMに対してプロテクトが設定された場合には、制御回路２１は、ＣＰＵ９２がマイコン内蔵メモリプログラム起動モードであり、かつ、命令フェッチにより命令コードを読出すためのアクセスであれば、ブロックMに対するアクセスを許可する。そのため、ＣＰＵ９２がブロックM以外のブロックに格納されている命令コードを命令フェッチして実行し、その実行処理中においてブロックMに対してデータアクセスがなされたとしても、制御回路２１はそのアクセスを禁止する。

【００７３】

なお、制御回路２１は、プロテクトされているブロックに対するデータの読出し要求を受けると、格納されているデータと異なるデータを応答する。また、制御回路２１は、プロテクトされているブロックに対するデータの書込み要求を受けると、何らの動作も行なわない（無視）、または、その要求を違反動作として扱う。

【００７４】

（プロテクト解除）
ＣＰＵ９２または外部からデータ領域２．１のブロックMに対するプロテクトの設定解除が要求されると、制御回路２１は、ブロックMに格納されているデータを消去する。そして、制御回路２１は、消去ベリファイ動作などにより、格納されているデータの消去が完了したことを確認した後、プロテクト情報領域２．２の部分保護フラグＭｂの値を変更し、ブロックMのプロテクト設定を解除する。

【００７５】

以上のように、制御回路２１は、データ領域２．１に格納されるライブラリソフトウェアに対して、命令フェッチによる命令コードの読出しに限定して、プロテクトを無効にするので、ＣＰＵ９２で実行されるプログラム中のサブルーチンコールを実現しながら、命令コード自体の漏洩を防止することができる。

【００７６】

この発明の実施の形態２によれば、プロテクトが設定されているブロックに対してのアクセスは許可されず、かつ、プロテクト設定を解除する場合には、当該ブロックに格納されているデータは必ず消去される。例外的に、ＣＰＵがデータ領域に格納されているライブラリソフトウェアなどの処理コードを読出して処理する場合に限り、保護情報にかかわらずアクセスが許可される。よって、命令コード自体の漏洩を防止し、かつ、ＣＰＵによるサブルーチンコールを制限なく実行させることができる。

【００７７】

［実施の形態３］

実施の形態１および２においては、それぞれ目的とする対象が異なるプロテクト機能について説明した。

【００７８】

一方、実施の形態３では、実施の形態１および２の機能を同時に実現する半導体装置について説明する。なお、以下の説明では、明確化のため、実施の形態１におけるプロテクトを「全体プロテクト」とも称し、実施の形態２におけるプロテクトを「部分プロテクト」とも称す。

【００７９】

図４は、実施の形態３に従う半導体装置１０３の概略構成図である。

図４を参照して、半導体装置１０３は、データバス９８と、ＣＰＵ９２と、不揮発性メモリ３と、読出部３２と、制御部３０と、電源部９７とからなる。

【００８０】

データバス９８は、ＣＰＵ９２、制御部３０、外部メモリ（図示しない）および外部装置（図示しない）などを互いに接続し、データの授受を仲介する。

【００８１】

ＣＰＵ９２は、データバス９８を介して不揮発性メモリ３との間でデータの授受を行なう。そして、ＣＰＵ９２は、実施の形態１におけるＣＰＵ９０と同様に、不揮発性メモリ２からプログラムを読出して起動する（「マイコン内蔵メモリプログラム起動モード」の）場合には、そのモード信号を制御部１０へ出力する。

【００８２】

また、ＣＰＵ９２は、実施の形態２におけるＣＰＵ９２と同様に、プログラムカウンタ（ＰＣ）９５を含み、プログラムカウンタ９５に格納されるプログラムカウンタ値に従い、不揮発性メモリ３から命令コードを読出して処理を実行する。そして、ＣＰＵ９２は、不揮発性メモリ３に対するアクセスを実行する際に、アクセスアドレスおよびアクセスステータスを制御部３０へ出力する。

【００８３】

不揮発性メモリ３は、フラッシュメモリやＥＥＰＲＯＭなどの半導体からなり、複数のブロックに分割されたデータ領域３．１とプロテクト情報領域３．２および３．３とを含む。

【００８４】

データ領域３．１は、ブロック１，２，・・・，Ｍ，・・・，Ｎに分割されており、それぞれデータ１，２，・・・，Ｍ，・・・，Ｎが格納される。

【００８５】

プロテクト情報領域３．２は、データ領域３．１におけるブロックに対応するように分割されており、データ領域のそれぞれのブロックに対する全体プロテクト設定が格納される。実施の形態３におけるプロテクト情報領域３．２には、それぞれ１ビットからなる全体保護フラグ１ａ，２ａ，・・・，Ｍａ，・・・，Ｎａが格納され、このフラグ値（「０

」または「１」）に応じて、データ領域３．１のそれぞれのブロックに対する全体プロテクト設定の有無が判断される。

【００８６】

プロテクト情報領域３．３は、データ領域３．１に含まれるブロックのうち所定のブロックに対応するように配置されており、その所定のブロックに対する部分プロテクト設定が格納される。実施の形態３におけるプロテクト情報領域３．３には、データ領域３．１に含まれるブロック１，２，・・・，Ｍ，・・・，Ｎのうち、ブロックＭに対する部分保護フラグＭｂが格納され、このフラグ値（「０」または「１」）に応じて、ブロックＭに対する部分プロテクト設定の有無が判断される。

【００８７】

読出部３２は、不揮発性メモリ３のプロテクト情報領域３．２および３．３に格納されている全体保護フラグ１ａ，２ａ，・・・，Ｍａ，・・・，Ｎａおよび部分保護フラグＭｂを読出し、制御部３０へ出力する。そして、読出部３２は、読出回路３６と、読出レジスタ１８および２８とからなる。

【００８８】

読出回路３６は、外部からのリセット信号や電源部９７からの投入信号を受けて、プロテクト情報領域３．２に格納されている全体保護フラグ１ａ，２ａ，・・・，Ｎａを読出して読出レジスタ１８へ出力し、プロテクト情報領域３．３に格納されている部分保護フラグＭｂを読出して読出レジスタ２８へ出力する。

【００８９】

読出レジスタ１８は、実施の形態１と同様であるので詳細な説明は省略する。また、読出レジスタ２８は、実施の形態２と同様であるので詳細な説明は省略する。

【００９０】

制御部３０は、優先回路（優先回路Ｍ）３４と、ＯＲ回路３５および３８と、起動モード判断部（判断部ａ）１４と、アクセスモード判断部（判断部ｂ）２４と、制御回路３１とからなる。

【００９１】

優先回路３４は、後述するように、ブロックＭに対して全体プロテクトおよび部分プロテクトが同時に設定された場合に生じる問題を回避するため、部分プロテクトを全体プロテクトに優先させるための回路である。そして、優先回路３４は、データ領域３．１のブロックＭに対して設定される全体保護フラグＭａおよび部分保護フラグＭｂを受けて、部分保護フラグＭｂによる設定を優先する。すなわち、優先回路３４は、読出レジスタ１８から受けた全体保護フラグＭａと読出レジスタ２８から受けた部分保護フラグＭｂとの論理演算を行ない、部分保護フラグＭｂにより部分プロテクトが設定されていれば、全体保護フラグＭａのプロテクト設定を無視して、全体プロテクト設定の解除を示す値をＯＲ回路３５へ出力する。

【００９２】

ＯＲ回路３５は、読出レジスタ１８から受けた全体保護フラグ１ａ，２ａ，・・・，Ｎａ（Ｍａを除く）および優先回路３４から受けた値で論理和（ＯＲ）演算を行ない、全体保護フラグ１ａ，２ａ，・・・，Ｎａ（Ｍａを除く）および優先回路３４から受けた値のうちいずれか１つでも全体プロテクトの設定を示す値であれば、起動モード判断部１４へ「ＯＮ」を出力する。

【００９３】

起動モード判断部１４は、実施の形態１と同様であるので、詳細な説明は繰返さない。また、アクセスモード判断部２４は、実施の形態２と同様であるので、詳細な説明は繰返さない。

【００９４】

ＯＲ回路３８は、起動モード判断部１４およびアクセスモード判断部２４から出力されるプロテクト制御信号を結合し、制御回路３１へ出力する。

【００９５】

制御回路３１は、データバスを介して、データ領域３．１のいずれかのブロックに対する全体プロテクトの設定解除の要求を受けると、当該ブロックに格納されているデータを消去し、そのデータが消去されたことを確認した後に、プロテクト情報領域３．２に格納されている当該ブロックに対応する全体保護フラグの値を変更し、全体プロテクトの設定を解除する。また、制御回路３１は、データバスを介して、データ領域３．１のブロックＭに対する部分プロテクトの設定解除の要求を受けると、ブロックＭに格納されているデータを消去し、そのデータが消去されたことを確認した後に、プロテクト情報領域３．３に格納されている部分保護フラグＭｂの値を変更し、部分プロテクトの設定を解除する。なお、制御回路３１は、全体プロテクトおよび部分プロテクトを互いに独立に扱うので、たとえば、ブロックＭに対する全体プロテクトの設定解除の要求を受けると、格納されているデータを消去した後にブロックＭに対する全体保護フラグＭａの値を変更するが、部分保護フラグＭｂの値を変更することはない。そのため、全体プロテクトおよび部分プロテクトのいずれもが設定されている場合には、それぞれに対してプロテクト設定を解除する必要がある。

【００９６】

また、制御回路３１は、データバスを介して、データ領域３．１のいずれかのブロックに対するアクセスの要求を受けると、ＯＲ回路３８からアクセスを禁止するプロテクト制御信号を受けているか否かを判断する。そして、制御回路３１は、アクセスを禁止するプロテクト制御信号を受けていなければ、そのアクセスを許可し、その要求先のブロックに格納されているデータを読出し、またはその要求先のブロックへデータを書込む。

【００９７】

さらに、制御回路３１は、データバスを介して、データ領域３．１のいずれかのブロックに対する全体プロテクトの設定要求を受けると、プロテクト情報領域３．２に格納されている当該ブロックに対応する全体保護フラグの値を変更し、全体プロテクトを設定する。また、制御回路３１は、データバスを介して、データ領域３．１のブロックＭに対する部分プロテクトの設定要求を受けると、プロテクト情報領域３．３に格納されている部分保護フラグＭｂの値を変更し、部分プロテクトを設定する。

【００９８】

電源部９７については、実施の形態１と同様であるので、詳細な説明は繰返さない。

（プロテクト設定）

データ領域３．１に対して全体プロテクトおよび部分プロテクトのいずれも設定されていない状態において、ＣＰＵ９２または外部からプロテクト対象のデータが転送されると、制御回路３１は、転送されたデータを所定のブロックに書込む。さらに、ＣＰＵ９２または外部から当該データに対する全体プロテクトまたは部分プロテクトの設定が要求されると、制御回路３１は、データを格納したブロックに対応する全体保護フラグ１ａ，２ａ，・・・，Ｍａ，・・・，Ｎａまたは部分保護フラグＭｂの値を変更し、プロテクト設定を行なう。なお、制御回路３１は、全体プロテクト要求または部分プロテクト要求を受けて、互いに独立にプロテクトを設定する。

【００９９】

したがって、制御回路３１は、全体保護フラグ１ａ，２ａ，・・・，Ｍａ，・・・，Ｎａのうちいずれかのフラグにおいて全体プロテクトが設定されていれば、ＣＰＵ９２がマイコン内蔵メモリプログラム起動モードである場合を除いて、すべてのブロックへのアクセスを禁止する。

【０１００】

さらに、制御回路３１は、部分保護フラグＭｂにおいて部分プロテクトが設定されていれば、ＣＰＵ９２がマイコン内蔵メモリプログラム起動モードであっても、ブロックＭへのアクセスを禁止する。そして、制御回路３１は、ＣＰＵ９２がマイコン内蔵メモリプログラム起動モードであり、かつ、命令フェッチにより命令コードを読出すためのアクセスである場合に限りブロックＭへのアクセスを許可する。

【０１０１】

（プロテクト解除）
ＣＰＵ９２または外部からデータ領域３．１のいずれかのブロックに対する全体プロテクトまたは部分プロテクトの設定解除が要求されると、制御回路３１は、指定されたブロックに格納されているデータを消去する。そして、制御回路３１は、消去ベリファイ動作などにより、格納されているデータの消去が完了したことを確認した後、そのブロックに対応する全体保護フラグまたは部分保護フラグの値を変更し、当該ブロックのプロテクト設定を解除する。なお、制御回路３１は、全体プロテクトの解除要求または部分プロテクトの解除要求を受けて、互いに独立にプロテクト設定を解除する。
【０１０２】
したがって、ブロックMに対して全体プロテクトおよび部分プロテクトが設定されていれば、これらのプロテクトを解除するためには、それぞれのプロテクトに対する解除要求を制御回路３１へ与える必要がある。
【０１０３】
（優先回路）
上述したように、全体プロテクトは、ＩＰベンダまたはプログラム製作者がエンドユーザに対するプロテクトを設定するための機能である。一方、部分プロテクトは、ＩＰベンダがプログラム製作者およびエンドユーザに対するプロテクトを設定するための機能である。すなわち、通常の流通過程においては、ＩＰベンダが、自身のライブラリソフトウェアに対して部分プロテクトを設定し、その後、プログラム製作者が、自身の製作したプログラムに対して全体プロテクトを設定する。そして、エンドユーザへ提供されることになる。
【０１０４】
ところで、プログラム製作者が、自己の製作したプログラムをブロックM以外のブロックに格納した後、ブロックMに対して全体プロテクトを設定してしまった場合を考えると、不揮発性メモリ３のデータ領域３．１に格納されているプログラムを更新するためには、ブロックMに対する全体プロテクト設定を解除する必要がある。上述したように、プロテクト設定を解除するためには、そのブロックに格納されているデータを消去する必要があるため、ブロックMに対する全体プロテクト設定の解除は、ブロックMに格納されているソフトウェアライブラリの消去を意味する。すなわち、プログラム製作者は、自己の製作したプログラムを更新するために、ＩＰベンダに対してライブラリソフトウェアの再提供を求めるという不合理な状況が生じる。
【０１０５】
そこで、優先回路３４は、ライブラリソフトウェアが格納されるブロックMに対して、全体プロテクト設定を無効にする。すなわち、優先回路３４は、ブロックMに対して部分プロテクトが設定されていれば、同時に全体プロテクトが設定されていても、全体プロテクトが設定されていないとみなす。
【０１０６】
よって、プログラム製作者が、誤って、ライブラリソフトウェアが格納されているブロックに対して全体プロテクトを設定したとしても、ライブラリソフトウェアを消去することなく、プログラムの更新が可能となる。
【０１０７】
なお、優先回路３４は、あくまでも、プログラム製作者などのミスを補うものであり、必須の構成要件ではないが、どのような状況においても不合理な状況を生じさせないために、配置することが望ましい。
【０１０８】
この発明の実施の形態３によれば、データ領域の全体プロテクト設定を解除する場合には、ブロック単位でデータ消去および全体保護フラグ値の変更が行なわれる。そのため、すべてのブロックを一括で消去する場合に比較して、効率的にデータ消去が行なえるので、処理速度の低下を抑制できる。一方、データ領域の全体プロテクト設定を解除するためには、すべてのブロックに対する全体プロテクト設定を解除しなければならない。よって

、全体プロテクト設定を解除するためには、すべてのブロックに格納されているデータを消去する必要があり、高いデータ機密保護機能を実現できる。また、部分プロテクトが設定されているブロックに対してのアクセスは許可されず、かつ、部分プロテクト設定を解除する場合には、当該ブロックに格納されているデータは必ず消去される。例外的に、ＣＰＵがデータ領域に格納されているライブラリソフトウェアなどの処理コードを読出して処理する場合に限り、部分保護フラグにかかわらずアクセスが許可される。よって、命令コード自体の漏洩を防止し、かつ、ＣＰＵによるサブルーチンコールを制限なく実行させることができる。

【０１０９】

また、この発明の実施の形態３によれば、同一のブロックに対して、全体プロテクトおよび部分プロテクトが設定されている場合には、部分プロテクトが優先し、全体プロテクトは無視される。そのため、既に、部分プロテクトが設定されているブロックに対して、誤って全体プロテクトを設定してしまった場合においても、当該ブロックに格納されているデータを消去することなく、全体プロテクトの設定を解除してデータの更新を行なうことができる。

【０１１０】

［実施の形態４］

実施の形態１～３においては、それぞれ１ビットからなる全体保護フラグまたは部分保護フラグによりプロテクトを設定する場合について説明した。

【０１１１】

一方、実施の形態４では、複数のビットからなる全体保護フラグまたは部分保護フラグを用いる場合について説明する。なお、実施の形態４においては、実施の形態３に示す半導体装置１０３に適用した例について説明する。

【０１１２】

図５は、実施の形態４に従う半導体装置１０４の概略構成図である。

図５を参照して、半導体装置１０４は、データバス９８と、ＣＰＵ９２と、不揮発性メモリ４と、読出部４２と、制御部４０と、電源部９７とからなる。

【０１１３】

データバス９８は、ＣＰＵ９２、制御部４０、外部メモリ（図示しない）および外部装置（図示しない）などを互いに接続し、データの授受を仲介する。

【０１１４】

ＣＰＵ９２については、実施の形態３と同様であるので、詳細な説明は繰返さない。

不揮発性メモリ４は、複数のブロックに分割されたデータ領域４．１とプロテクト情報領域４．２および４．３とを含む。

【０１１５】

データ領域４．１は、ブロック１，２，・・・，Ｍ，・・・，Ｎに分割されており、それぞれデータ１，２，・・・，Ｍ，・・・，Ｎが格納される。

【０１１６】

プロテクト情報領域４．２は、データ領域４．１におけるブロックに対応するように分割されており、データ領域のそれぞれのブロックに対する全体プロテクト設定が格納される。実施の形態４におけるプロテクト情報領域４．２には、たとえば、それぞれ２ビットからなる全体保護フラグ１ａ’，２ａ’，・・・，Ｍａ’，・・・，Ｎａ’が格納され、このフラグ値（「００」または「１１」）に応じて、データ領域４．１のそれぞれのブロックに対する全体プロテクト設定の有無が判断される。

【０１１７】

プロテクト情報領域４．３は、データ領域４．１に含まれるブロックのうちブロックＭに対する部分プロテクト設定が格納される。実施の形態４におけるプロテクト情報領域４．３には、２ビットからなる部分保護フラグＭｂ’が格納され、このフラグ値（「００」または「１１」）に応じて、ブロックＭに対する部分プロテクト設定の有無が判断される。

【０１１８】
読出部４２は、不揮発性メモリ４のプロテクト情報領域４．２および４．３に格納されている全体保護フラグ１ａ’，２ａ’，・・・，Ｎａ’および部分保護フラグＭｂ’を読出し、制御部４０へ出力する。そして、読出部４２は、読出回路４６と、読出レジスタ４８および４７とからなる。
【０１１９】
読出回路４６は、外部からのリセット信号や電源部９７からの投入信号を受けて、プロテクト情報領域４．２に格納されている全体保護フラグ１ａ’，２ａ’，・・・，Ｍａ’，・・・，Ｎａ’を読出し、ビット単位で読出レジスタ４８へ出力する。同時に、読出回路４６は、プロテクト情報領域４．３に格納されている部分保護フラグＭｂ’を読出し、ビット単位で読出レジスタ４７へ出力する。
【０１２０】
読出レジスタ４８は、全体保護フラグ１ａ’，２ａ’，・・・，Ｍａ’，・・・，Ｎａ’のそれぞれをビット単位で一旦格納し、それぞれのビットの値を制御部４０へ出力する。
【０１２１】
読出レジスタ４７は、部分保護フラグＭｂ’をビット単位で一旦格納し、各ビットの値を制御部４０へ出力する。
【０１２２】
制御部４０は、実施の形態３における制御部３０にＯＲ回路４３．１，４３．２，・・・，４３．Ｍ，・・・，４３．Ｎおよび４４を追加したものと同様である。
【０１２３】
ＯＲ回路４３．１は、読出レジスタ４８に格納されている全体保護フラグ１ａ’の０ビット目の値１ａ’（０）および１ビット目の値１ａ’（１）を読出し、論理和（ＯＲ）演算を行なう。そして、ＯＲ回路４３．１は、その論理和演算の結果をＯＲ回路３５へ出力する。すなわち、ＯＲ回路４３．１は、全体保護フラグ１ａ’の０ビット目の値１ａ’（０）または１ビット目の値１ａ’（１）のうち、どちらかのビットがプロテクトを設定する値となっていれば、プロテクトが設定されていると判断する。
【０１２４】
以下同様に、ＯＲ回路４３．２，・・・，４３．Ｍ，・・・，４３．Ｎは、それぞれ全体保護フラグ２ａ’，・・・，Ｍａ’，・・・，Ｎａ’の０ビット目の値２ａ’（０），・・・，Ｍａ’（０），・・・，Ｎａ’（０）および１ビット目の値２ａ’（１），・・・，Ｍａ’（１），・・・，Ｎａ’（１）を読出し、論理和（ＯＲ）演算を行なう。そして、ＯＲ回路４３．２，・・・，４３．Ｍ，・・・，４３．Ｎは、それぞれ論理和演算の結果をＯＲ回路３５へ出力する。
【０１２５】
制御回路４１は、データバスを介して、データ領域４．１のいずれかのブロックに対する全体プロテクトの設定要求を受けると、プロテクト情報領域４．２に格納されている当該ブロックに対応する全体保護フラグを構成するすべてのビットを同値に変更し、プロテクトを設定する。また、制御回路４１は、データバスを介して、データ領域４．１のブロックＭに対するプロテクトの設定要求を受けると、プロテクト情報領域４．３に格納されている部分保護フラグＭｂを構成するすべてのビットを同値に変更し、プロテクトを設定する。また、制御回路４１は、プロテクトの設定解除の要求を受けると、プロテクトを設定する場合と同様に、プロテクト情報領域４．２に格納されている全体保護フラグまたはプロテクト情報領域４．３に格納されている部分保護フラグＭｂを構成するすべてのビットを同値に変更し、プロテクトを解除する。すなわち、制御回路４１は、プロテクトの設定または解除に応じて、「００」または「１１」を書込む。
【０１２６】
なお、制御回路４１の他の処理については、実施の形態３における制御回路３１と同様であるので、詳細な説明は繰返さない。

【０１２７】
以下、優先回路３４、ＯＲ回路３５および３８、起動モード判断部（判断部ａ）１４ならびにアクセスモード判断部（判断部ｂ）２４については、実施の形態３と同様であるので、詳細な説明は繰返さない。
【０１２８】
電源部９７については、実施の形態３と同様であるので、詳細な説明は繰返さない。
上述のように、制御回路４１は、フラグを構成する複数のビットを同値に変更して、プロテクトを設定する。そのため、フラグを構成するビットが何らかの原因で揮発した場合にも、プロテクト設定を維持できる。
【０１２９】
たとえば、プロテクトの設定を示すフラグ値を「１」とした場合において、制御回路４１は、ブロック１に対する全体プロテクトの設定要求を受けると、全体保護フラグ１ａ’の０ビット目の値１ａ’（０）および１ビット目の値１ａ’（１）をいずれも「１」に変更する。同様に、制御回路４１は、ブロック１に対する全体プロテクトの設定解除の要求を受けると、ブロック１に格納されているデータを消去した後、全体保護フラグ１ａ’の０ビット目の値１ａ’（０）および１ビット目の値１ａ’（１）をいずれも「０」に変更する。すなわち、制御回路４１は、プロテクトの設定要求を受けると、保護フラグの値を「１１」に変更し、プロテクトの設定解除の要求を受けると、保護フラグの値を「００」に変更する。
【０１３０】
さらに、ブロック１に対する全体プロテクトが設定された状態、すなわち全体保護フラグ１ａ’の値が「１１」に変更された場合において、何らかの原因により１ビット分のデータが揮発して「１０」に変化したとすると、ＯＲ回路４３．１に与えられる値は、「１」，「１」から「１」，「０」に変化する。しかしながら、ＯＲ回路４３．１から出力される値は「１」のまま維持されるので、全体プロテクト設定が解除されることはない。
【０１３１】
よって、保護フラグを構成するビットが何らかの原因で揮発したとしても、誤ってプロテクトの設定が解除されることを回避できる。なお、上述の説明から明らかなように、保護フラグをより多くのビットで構成することで、プロテクト機能をより強化することができる。
【０１３２】
なお、実施の形態４においては、実施の形態１における全体プロテクト機能および実施の形態２における部分プロテクト機能を同時に実現する実施の形態３に従う半導体装置に適応した場合について説明したが、実施の形態１に従う半導体装置および実施の形態２に従う半導体装置のいずれに対しても同様に適応できることは言うまでもない。
【０１３３】
実施の形態４によれば、実施の形態３における効果に加えて、全体プロテクト設定または部分プロテクト設定を行なうための全体保護フラグまたは部分フラグが何らかの原因で揮発したとしても、それらを構成するすべてのビットの値が変化しなければ、その保護フラグにより設定されるプロテクトが解除されることはない。よって、１つのビットからなる保護フラグを用いる場合に比較して、プロテクト機能をより強化した半導体装置を実現できる。
【０１３４】
［実施の形態５］
実施の形態２～４においては、データ領域を構成する複数ブロックのうち１つのブロックに対して部分プロテクトを設定する場合について説明した。
【０１３５】
一方、実施の形態５では、複数のブロックに対して一体的に部分プロテクトを設定する場合について説明する。なお、実施の形態５においては、実施の形態４に示す半導体装置１０４に適用した例について説明する。

【０１３６】
不揮発性メモリに格納されるライブラリソフトウェアの容量が大きく、１つのブロックに収まらない場合には、複数のブロックにまたがって格納される。このような場合において、ライブラリソフトウェアは、単一的に取り扱われることが望ましい。そこで、複数のブロックを１つのブロックとみなして一体的に部分プロテクトを設定できる機能が必要となる。
【０１３７】
図６は、実施の形態５に従う半導体装置１０５の概略構成図である。
図６を参照して、半導体装置１０５は、データバス９８と、ＣＰＵ９２と、不揮発性メモリ５と、読出部５２と、制御部５０と、電源部９７とからなる。
【０１３８】
データバス９８は、ＣＰＵ９２、制御部５０、外部メモリ（図示しない）および外部装置（図示しない）などを互いに接続し、データの授受を仲介する。
【０１３９】
ＣＰＵ９２については、実施の形態４と同様であるので、詳細な説明は繰返さない。
不揮発性メモリ５は、複数のブロックに分割されたデータ領域５．１とプロテクト情報領域５．２および５．３とを含む。
【０１４０】
データ領域５．１は、ブロック１，２，・・・，Ｌ，Ｍ，・・・，Ｎに分割されており、それぞれデータ１，２，・・・，Ｌ，Ｍ，・・・，Ｎが格納される。
【０１４１】
プロテクト情報領域５．２は、データ領域５．１におけるブロックに対応するように分割されており、それぞれ全体保護フラグ１ａ’，２ａ’，・・・，Ｌａ’，Ｍａ’，・・・，Ｎａ’が格納される。
【０１４２】
プロテクト情報領域５．３は、データ領域５．１を構成するブロックのうち複数のブロックに対する部分プロテクトを設定するための部分保護フラグを格納する。実施の形態５においては、たとえば、ブロックＬおよびＭに対して部分プロテクトを設定するための部分保護フラグＬｂ’およびＭｂ’が格納される。
【０１４３】
なお、実施の形態４と同様に、全体保護フラグ１ａ’，２ａ’，・・・，Ｌａ’，Ｍａ’，・・・，Ｎａ’および部分保護フラグＬｂ’，Ｍｂ’は、それぞれ２ビットで構成される。
【０１４４】
読出部５２は、不揮発性メモリ５のプロテクト情報領域５．２および５．３に格納されている全体保護フラグ１ａ’，２ａ’，・・・，Ｌａ’，Ｍａ’，・・・，Ｎａ’およびに部分保護フラグＬｂ’，Ｍｂ’を読出し、制御部５０へ出力する。そして、読出部５２は、読出回路５６と、読出レジスタ５８および５７とからなる。
【０１４５】
読出回路５６は、外部からのリセット信号や電源部９７からの投入信号を受けて、全体保護フラグ１ａ’，２ａ’，・・・，Ｌａ’，Ｍａ’，・・・，Ｎａ’を読出し、読出レジスタ５８へ出力する。同時に、読出回路５６は、部分保護フラグＬｂ’，Ｍｂ’を読出し、読出レジスタ５７へ出力する。
【０１４６】
読出レジスタ５８は、全体保護フラグ１ａ’，２ａ’，・・・，Ｌａ’，Ｍａ’，・・・，Ｎａ’のそれぞれをビット単位で一旦格納し、各ビットの値を制御部５０へ出力する。
【０１４７】
読出レジスタ５７は、部分保護フラグＬｂ’，Ｍｂ’をビット単位で一旦格納し、各ビットの値を制御部５０へ出力する。

【０１４８】
制御部５０は、実施の形態４における制御部４０において、ＯＲ回路４３．Ｌおよび４３．ＭをＯＲ回路５３．ＬＭに代え、かつ、ＯＲ回路４４をＯＲ回路５４に代えたものである。
【０１４９】
ＯＲ回路５３．ＬＭは、読出レジスタ５８に格納されている全体保護フラグＬａ’の０ビット目の値Ｌａ’（０）および１ビット目の値Ｌａ’（１）ならびに、全体保護フラグＭａ’の０ビット目の値Ｍａ’（０）および１ビット目の値Ｍａ’（１）を読出し、論理和（ＯＲ）演算を行なう。そして、ＯＲ回路５３．ＬＭは、その論理和演算の結果を優先回路３４へ出力する。
【０１５０】
同様に、ＯＲ回路５４は、読出レジスタ５７に格納されている部分保護フラグＬｂ’の０ビット目の値Ｌｂ’（０）および１ビット目の値Ｌｂ’（１）ならびに、部分保護フラグＭｂ’の０ビット目の値Ｍｂ’（０）および１ビット目の値Ｍｂ’（１）を読出し、論理和（ＯＲ）演算を行なう。そして、ＯＲ回路５４は、その論理和演算の結果を優先回路３４へ出力する。
【０１５１】
すなわち、ＯＲ回路５３．ＬＭおよび５４は、ブロックＬまたはブロックＭのいずれかに全体プロテクトまたは部分プロテクトが設定されていれば、ブロックＬおよびＭに対して全体プロテクトまたは部分プロテクトが設定されていると判断する。
【０１５２】
以下、優先回路３４、ＯＲ回路３５および３８、起動モード判断部（判断部ａ）１４ならびにアクセスモード判断部（判断部ｂ）２４については、実施の形態４と同様であるので、詳細な説明は繰返さない。
【０１５３】
電源部９７については、実施の形態４と同様であるので、詳細な説明は繰返さない。
上述のように、ＯＲ回路５４は、部分保護フラグＬｂ’またはＭｂ’のいずれかが設定されていれば、ブロックＬおよびＭに対する部分プロテクトが設定されていると出力する。そのため、制御回路４１は、ブロックＬまたはＭに対して部分プロテクトが設定されている場合には、ＣＰＵ９２からの命令フェッチによるアクセスを除き、ブロックＬおよびブロックＭに対するアクセスを禁止する。さらに、ブロックＬまたはＭに対する部分プロテクトを解除するためには、ブロックＬおよびＭに格納されているデータをすべて消去する必要がある。
【０１５４】
よって、ブロックＬおよびＭに格納されるデータに対して一体的なプロテクトを行なうことができる。
【０１５５】
なお、実施の形態５においては、データ領域に含まれる複数ブロックのうち２ブロックに対して部分プロテクトを設定する構成について説明したが、２ブロックに限定されることはなく、ブロックの数は、格納されるライブラリソフトウェアの容量などに応じて適宜設計すればよい。
【０１５６】
また、実施の形態５においては、実施の形態４に従う半導体装置に適応した場合について説明したが、部分プロテクト機能を備える実施の形態２に従う半導体装置および実施の形態３に従う半導体装置のいずれに対しても同様に適応できることは言うまでもない。
【０１５７】
実施の形態５によれば、実施の形態４における効果に加えて、複数のブロックに対して部分プロテクトを設定でき、かつ、それらのブロックに対する部分プロテクトの設定および解除は、一体的に行なわれる。よって、ライブラリソフトウェアの容量が増加し、複数のブロックにわたって格納される場合であっても、１つのブロックに格納される場合と同

様に、処理コードの漏洩を防止することができる。

【０１５８】

［実施の形態６］

実施の形態５においては、複数のブロックに対して、一体的に部分プロテクトを設定する場合について説明した。

【０１５９】

一方、実施の形態６では、複数の部分プロテクトを互いに独立に設定できる場合について説明する。なお、実施の形態６においては、実施の形態４に示す半導体装置１０４に適用した例について説明する。

【０１６０】

複数のＩＰベンダによりライブラリソフトウェアが供給される場合などにおいては、複数のブロックに対して、互いに独立に部分プロテクトを設定できる機能が必要となる。

【０１６１】

図７は、実施の形態６に従う半導体装置１０６の概略構成図である。

図７を参照して、半導体装置１０６は、データバス９８と、ＣＰＵ９２と、不揮発性メモリ５と、読出部５２と、制御部６０と、電源部９７とからなる。

【０１６２】

データバス９８は、ＣＰＵ９２、制御部５０、外部メモリ（図示しない）および外部装置（図示しない）などを互いに接続し、データの授受を仲介する。

【０１６３】

ＣＰＵ９２については、実施の形態４と同様であるので、詳細な説明は繰返さない。

不揮発性メモリ５および読出部５２は、実施の形態５と同様であるので、詳細な説明は繰返さない。

【０１６４】

制御部６０は、実施の形態４における制御部４０において、ＯＲ回路６４、優先回路（優先回路Ｌ）６２およびアクセスモード判断部（判断部ｂ）６５を付加し、ＯＲ回路３８をＯＲ回路６８に代えたものである。

【０１６５】

ＯＲ回路６４は、読出レジスタ５７に格納されている部分保護フラグＬｂ’の０ビット目の値Ｌｂ’（０）および１ビット目の値Ｌｂ’（１）を読出し、論理和（ＯＲ）演算を行なう。そして、ＯＲ回路６４は、その論理和演算の結果を優先回路６２へ出力する。

【０１６６】

優先回路６２は、ＯＲ回路４３．Ｌから受けた全体保護フラグＬａ’の値とＯＲ回路６４から受けた部分保護フラグＬｂ’の値との論理演算を行ない、部分保護フラグＬｂ’により部分プロテクトが設定されていれば、全体保護フラグＬａ’による全体プロテクト設定を無視して、全体プロテクトの設定解除を示す値をＯＲ回路３５へ出力する。

【０１６７】

アクセスモード判断部６５は、実施の形態４におけるアクセスモード判断部２４と同様に、ＯＲ回路６４から出力される部分保護フラグＬｂ’の値に基づいて、ブロックＬに対する部分プロテクトの設定がされている場合には、データ領域５．１のブロックＬに対するアクセスを禁止させるプロテクト制御信号をＯＲ回路６８へ出力する。そして、アクセスモード判断部６５は、例外的に、ＣＰＵ９２からモード信号を受けている場合で、かつ、ＣＰＵ９２からブロックＬに対する命令フェッチによる命令コードの読出しである場合に限り、そのアクセスを禁止させるプロテクト制御信号をマスクする。

【０１６８】

ＯＲ回路６８は、起動モード判断部１４、アクセスモード判断部６５および２４から出力されるプロテクト制御信号を結合し、制御回路４１へ出力する。

【０１６９】

以下、優先回路３４、ＯＲ回路３５、起動モード判断部１４ならびにアクセスモード判断部２４については、実施の形態４と同様であるので、詳細な説明は繰返さない。

【０１７０】
電源部９７については、実施の形態４と同様であるので、詳細な説明は繰返さない。
上述のように、アクセスモード判断部６５および２４は、それぞれ部分保護フラグＬｂ’およびＭｂ’の値に応じて、ブロックＬおよびＭに対する部分プロテクトが設定されているか否かを判断する。また、優先回路６２および３４は、それぞれ部分保護フラグＬｂ’およびＭｂ’の値に応じて、全体保護フラグＬａ’およびＭａ’の設定が有効であるか否かを判断する。
【０１７１】
よって、ブロックＬおよびＭに格納されているデータに対して、互いに独立に全体プロテクトまたは部分プロテクトが設定される。
【０１７２】
なお、実施の形態６においては、データ領域に含まれる複数ブロックのうち２ブロックに対して互いに独立に部分プロテクトを設定する構成について説明したが、２ブロックに限定されることはなく、ブロックの数は、ＩＰベンダの数などに応じて適宜設計すればよい。
【０１７３】
また、実施の形態６においては、実施の形態４に従う半導体装置に適応した場合について説明したが、部分プロテクト機能を備える実施の形態２に従う半導体装置および実施の形態３に従う半導体装置のいずれに対しても同様に適応できることは言うまでもない。
【０１７４】
実施の形態６によれば、実施の形態４における効果に加えて、複数のブロックに対してそれぞれ独立に部分プロテクトを設定できる。そのため、複数のＩＰベンダなどがライブラリソフトウェアを提供する場合などには、それぞれ独立して部分プロテクトを設定でき、かつ、その部分プロテクトを設定したデータは、他のＩＰベンダを含めたいずれの者に対しても有効である。よって、同一の半導体装置に対して、複数のＩＰベンダがライブラリソフトウェアを提供する場合においても、その処理コードの漏洩を防止することができる。
【０１７５】
［実施の形態７］
実施の形態１においては、不揮発性メモリを構成するすべてのブロックに対して、全体プロテクトを設定する場合について説明した。
【０１７６】
一方、実施の形態７では、不揮発性メモリを構成するブロックのうち限られたブロックに対してのみ全体プロテクトを設定できる場合について説明する。なお、実施の形態７においては、実施の形態１に示す半導体装置１０１に適用した例について説明する。
【０１７７】
不揮発性メモリのデータ領域に対して、格納されるプログラムが小さい場合などには、プログラムに加えてユーザデータなどを格納することも考えられる。その際、不揮発性メモリを構成するすべてのブロックを全体プロテクトの対象とすると、エンドユーザは、ユーザデータに対してアクセスできない。そこで、不揮発性メモリを構成するブロックのうち、プログラムが格納されるブロックに対してのみ、全体プロテクトを設定できる構成とする。
【０１７８】
図８は、実施の形態７に従う半導体装置１０７の概略構成図である。
図８を参照して、半導体装置１０７は、データバス９８と、ＣＰＵ９０と、不揮発性メモリ７と、読出部７２と、制御部１０と、電源部９７とからなる。
【０１７９】
データバス９８は、ＣＰＵ９０、制御部１０、外部メモリ（図示しない）および外部装置（図示しない）などを互いに接続し、データの授受を仲介する。
【０１８０】

ＣＰＵ９０については、実施の形態１と同様であるので、詳細な説明は繰返さない。
不揮発性メモリ７は、複数のブロックに分割されたデータ領域７．１とプロテクト情報領域７．２とを含む。
【０１８１】
データ領域７．１は、ブロック１，２，・・・，Ｌ，Ｍ，・・・，Ｎに分割されており、それぞれデータ１，２，・・・，Ｌ，Ｍ，・・・，Ｎが格納される。
【０１８２】
プロテクト情報領域７．２は、データ領域７．１に含まれるブロックのうち所定のブロックに対応するように配置されており、その所定のブロックに対する全体プロテクト設定が格納される。実施の形態７におけるプロテクト情報領域７．２には、データ領域７．１に含まれるブロックＬおよびＭに対する全体保護フラグＬａおよびＭａが格納される。
【０１８３】
読出部７２は、不揮発性メモリ７のプロテクト情報領域７．２に格納されている全体保護フラグＬａおよびＭａを読出し、制御部１０へ出力する。そして、読出部７２は、読出回路７６と、読出レジスタ７８とからなる。
【０１８４】
読出回路７６は、外部からのリセット信号や電源部９７からの投入信号を受けて、プロテクト情報領域７．２に格納されている全体保護フラグＬａおよびＭａを読出し、読出レジスタ７８へ出力する。
【０１８５】
読出レジスタ７８は、全体保護フラグＬａおよびＭａを一旦格納し、その値を制御部１０へ出力する。
【０１８６】
制御部１０および電源部９７については、実施の形態１と同様であるので、詳細な説明は繰返さない。
【０１８７】
上述のように、制御部１０は、全体プロテクトフラグＬａおよびＭａの値に応じて、ブロックＬおよびＭに対して全体プロテクトが設定されているか否かを判断する。また、制御部１０は、ブロックＬおよびＭのいずれに対しても全体プロテクトが設定されていなければ、ブロックＬおよびＭに対するアクセスを許可する。
【０１８８】
すなわち、不揮発性メモリ７に含まれるブロックＬおよびＭ以外のブロックに対しては、全体プロテクトの設定を行なうことができない。そのため、ブロックＬおよびＭにプロテクト対象のプログラムなどを格納し、その他のブロックに対しては、エンドユーザへ開放するような使用形態が可能となる。
【０１８９】
なお、実施の形態７においては、データ領域に含まれる複数ブロックのうち２ブロックに対して全体プロテクトを設定する構成について説明したが、２ブロックに限定されることはなく、全体プロテクトを設定可能なブロックの数は、プログラムの容量などに応じて適宜設計すればよい。
【０１９０】
また、実施の形態７においては、実施の形態１に従う半導体装置に適応した場合について説明したが、全体プロテクト機能を備える実施の形態３～６に従う半導体装置のいずれに対しても同様に適応できることは言うまでもない。
【０１９１】
実施の形態７によれば、実施の形態１における効果に加えて、不揮発性メモリを構成するブロックのうち、一部のブロックに対してのみ全体プロテクトの対象とする。そのため、全体プロテクトの対象となるプログラムの容量が、不揮発性メモリの容量より十分小さい場合などにおいて、プログラムが格納されるブロック以外のブロックをエンドユーザに開放し、不揮発性メモリをより有効に使用することができる。よって、不揮発性メモリを

複数の用途に用いることができるので、半導体装置に内蔵される不揮発性メモリの容量などを合理的に決定できる。

【０１９２】

［実施の形態８］

実施の形態１～７においては、不揮発性メモリ内にデータ領域とプロテクト情報領域とを配置する場合について説明した。

【０１９３】

一方、実施の形態８では、不揮発性メモリ内にデータ領域のみを配置し、そのデータ領域にデータとプロテクト情報フラグとを格納する構成について説明する。なお、実施の形態８においては、実施の形態３に示す半導体装置１０３に適用した例について説明する。

【０１９４】

図９は、実施の形態８に従う半導体装置１０８の概略構成図である。

図９を参照して、半導体装置１０８は、データバス９８と、ＣＰＵ９２と、不揮発性メモリ８と、読出部８２と、制御部８０と、電源部９７とからなる。

【０１９５】

データバス９８は、ＣＰＵ９２、制御部８０、外部メモリ（図示しない）および外部装置（図示しない）などを互いに接続し、データの授受を仲介する。

【０１９６】

ＣＰＵ９２については、実施の形態３と同様であるので、詳細な説明は繰返さない。

不揮発性メモリ８は、複数のブロックに分割されたデータ領域からなる。そして、不揮発性メモリ８は、ブロック１，２，・・・，Ｍ，・・・，Ｎに分割されており、それぞれデータ１，２，・・・，Ｍ，・・・，Ｎおよび各ブロックに対する全体保護フラグ１ａ，２ａ，・・・，Ｍａ，・・・，Ｎａが格納される。さらに、ブロックＭには、ブロックＭに対する部分保護フラグＭｂが格納される。

【０１９７】

読出部８２は、不揮発性メモリ８に格納されているデータの中から、全体保護フラグ１ａ，２ａ，・・・，Ｍａ，・・・，Ｎａおよび部分保護フラグＭｂを抽出し、制御部８０へ出力する。そして、読出部８２は、読出回路８６と、読出レジスタ１８および３７とからなる。

【０１９８】

読出回路８６は、外部からのリセット信号や電源部９７からの投入信号を受けて、不揮発性メモリ８のそれぞれのブロックに格納されているデータを読出し、その読出したデータに含まれる全体保護フラグ１ａ，２ａ，・・・，Ｍａ，・・・，Ｎａおよび部分保護フラグＭｂを抽出し、読出レジスタ１８および３７へ出力する。

【０１９９】

読出レジスタ１８および３７は、実施の形態３と同様であるので、詳細な説明は繰返さない。

【０２００】

制御部８０は、実施の形態３における制御部３０において、制御回路３１を制御回路８１に代えたものである。

【０２０１】

制御回路８１は、データバスを介して、いずれかのブロックに対するプロテクトの設定解除の要求を受けると、当該ブロックに格納されているデータを消去するとともに、全体保護フラグまたは部分保護フラグの値を変更し、プロテクトの設定を解除する。また、制御回路８１は、データバスを介して、いずれかのブロックに対するプロテクトの設定要求を受けると、当該ブロックに格納されている全体保護フラグまたは部分保護フラグの値を変更し、プロテクトを設定する。制御回路８１の他の処理については、実施の形態３における制御回路３１と同様であるので、詳細な説明は繰返さない。

【０２０２】

以下、優先回路３４、ＯＲ回路３５および３８、起動モード判断部１４ならびにアクセ

スモード判断部２４については、実施の形態３と同様であるので、詳細な説明は繰返さない。

【０２０３】

電源部９７については、実施の形態３と同様であるので、詳細な説明は繰返さない。

上述のように、不揮発性メモリ８のそれぞれのブロックには、通常のデータに加えて、各ブロックのプロテクトを設定するための全体保護フラグおよび部分保護フラグが格納される。そのため、全体プロテクトおよび部分プロテクトを設定する対象のブロックを比較的自由に設定することができる。

【０２０４】

なお、実施の形態８においては、全体保護フラグおよび部分保護フラグの両方をデータと共に格納する場合について説明したが、全体保護フラグまたは部分保護フラグのいずれか一方をデータと共に格納し、他方のフラグは、実施の形態１～７と同様にプロテクト情報領域に格納する構成としてもよい。

【０２０５】

また、実施の形態８においては、実施の形態３に従う半導体装置に適応した場合について説明したが、実施の形態１、２および４～７に従う半導体装置のいずれに対しても同様に適応できることは言うまでもない。

【０２０６】

実施の形態８によれば、実施の形態３における効果に加えて、全体プロテクトおよび部分プロテクトを格納するためのプロテクト情報領域を必要としないので、プロテクトの対象となるブロックに応じて、プロテクト情報領域を配置する必要がない。そのため、全体プロテクトおよび部分プロテクトの対象となるブロックを自由に選択することができ、かつ、変更も容易である。よって、不揮発性メモリに格納されるプログラムやサブルーチンプログラムに応じて、プロテクトの対象となるブロック数を自由に変更できる半導体装置を実現できる。

【０２０７】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した説明ではなく、特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【０２０８】

【図１】実施の形態１に従う半導体装置の概略構成図である。

【図２】半導体装置の動作モードを説明するための図である。

【図３】実施の形態２に従う半導体装置の概略構成図である。

【図４】実施の形態３に従う半導体装置の概略構成図である。

【図５】実施の形態４に従う半導体装置の概略構成図である。

【図６】実施の形態５に従う半導体装置の概略構成図である。

【図７】実施の形態６に従う半導体装置の概略構成図である。

【図８】実施の形態７に従う半導体装置の概略構成図である。

【図９】実施の形態８に従う半導体装置の概略構成図である。

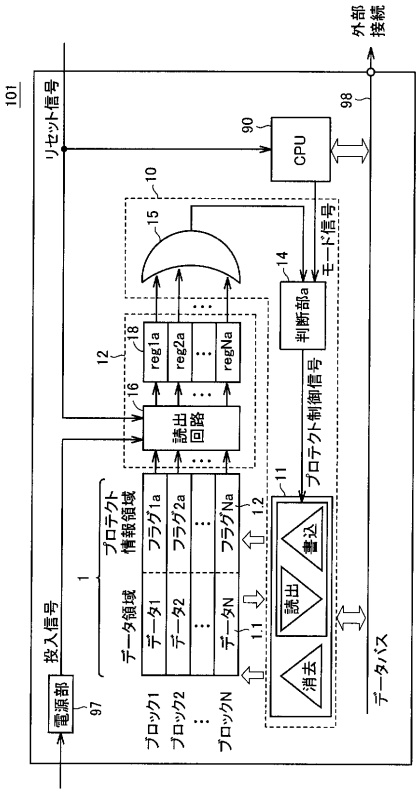
【符号の説明】

【０２０９】

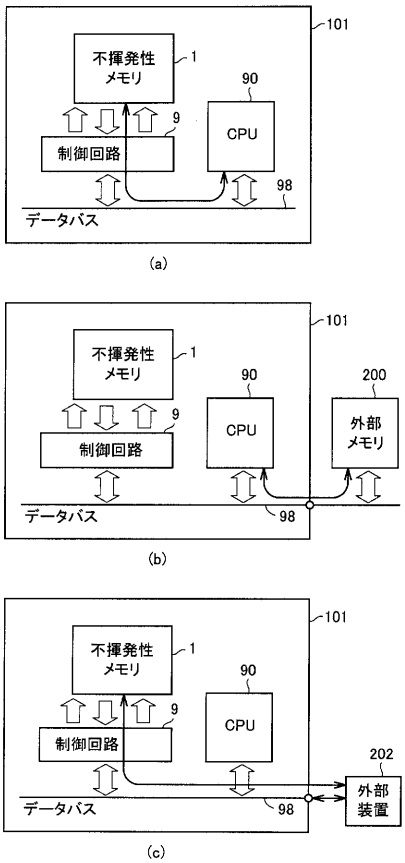
１，２，３，４，５，７，８　不揮発性メモリ、１．１，２．１，３．１，４．１，５．１，７．１　データ領域、１．２，２．２，３．２，３．３，４．２，４．３，５．２，５．３，７．２　プロテクト情報領域、１ａ，２ａ，・・・，Ｌａ，Ｍａ，・・・，Ｎａ，１ａ’，２ａ’，・・・，Ｌａ’，Ｍａ’，・・・，Ｎａ’　全体保護フラグ、Ｍｂ，Ｌｂ’，Ｍｂ’　部分保護フラグ、１０，２０，３０，４０，５０，６０，８０　制御部、１１，２１，３１，４１，８１　制御回路、１２，２２，３２，４２，５２，７２，８２　読出部、１４　起動モード判断部（判断部ａ）、１５，３５，３８，４３．１，４

３．２，・・・，４３．Ｍ，・・・，４３．Ｎ，４６，５３．ＬＭ，４４，５３．ＬＭ，５４，６４，６８　ＯＲ回路、１６，２６，３６，５４，５６，７６，８６　読出回路、１８，２８，４７，４８，５７，５８，７８　読出レジスタ、２４，６５　アクセスモード判断部（判断部ｂ）、３４　優先回路（優先回路Ｍ）、６２　優先回路（優先回路Ｌ）、９０，９２　演算部（ＣＰＵ）、９５　プログラムカウンタ（ＰＣ）、９７　電源部、９８　データバス、１０１，１０２，１０３，１０４，１０５，１０６，１０７，１０８　半導体装置、２００　外部メモリ、２０２　外部装置。

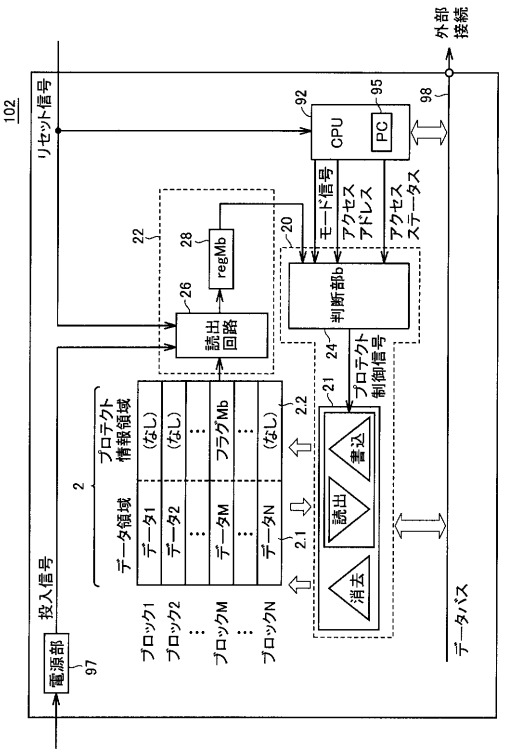
【図１】



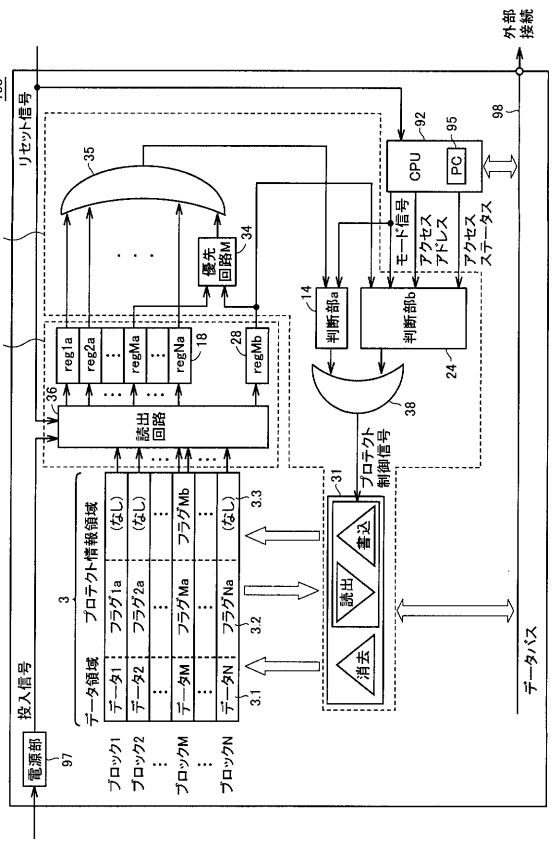
【図２】



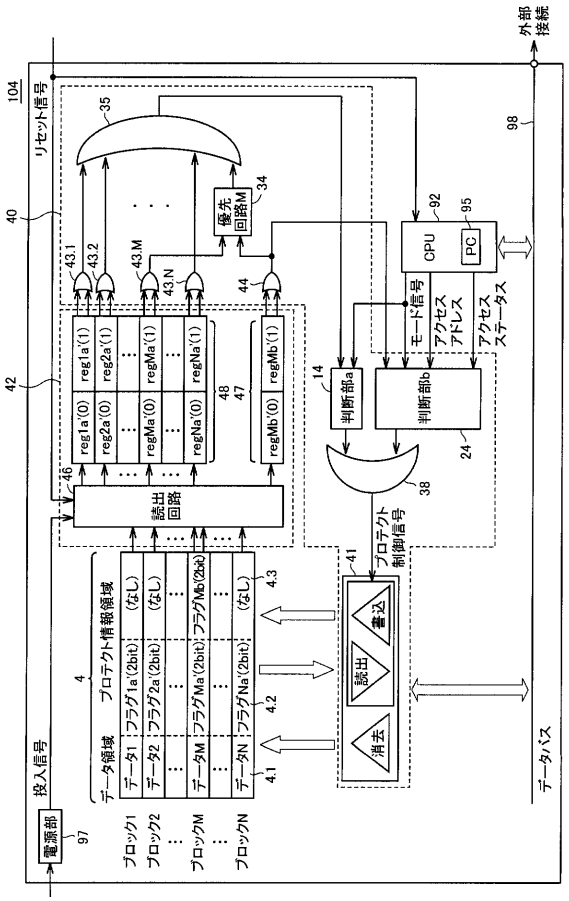
【図３】


102
リセット信号
外部接続
CPU
PC
92
95
98
モード信号
アクセスアドレス
アクセスステータス
判断部b
20
22
28
regMb
読出回路
26
プロテクト制御信号
24
21
書込
読出
消去
2.2
2.1
2
プロテクト情報領域
データ領域
データ1
データ2
データM
データN
(なし)
フラグMb
データバス
投入信号
電源部
97
ブロック1
ブロック2
ブロックM
ブロックN

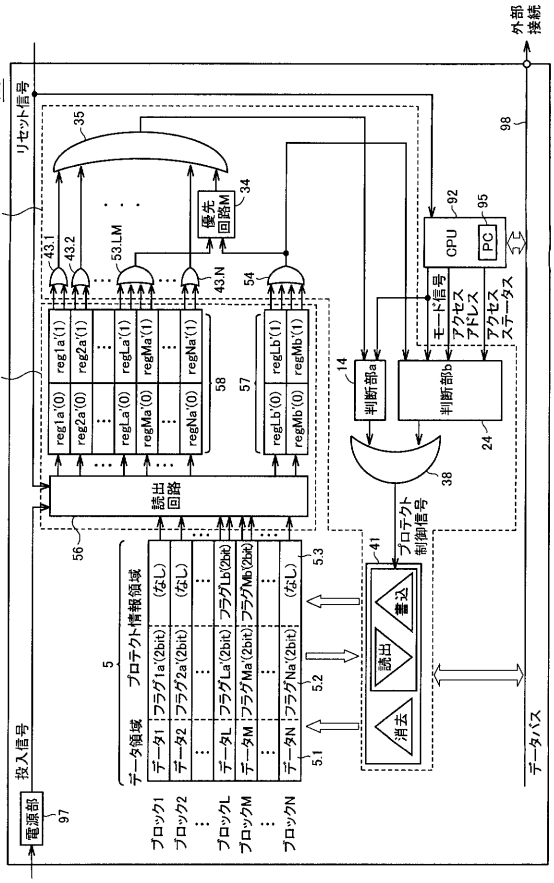
【図４】


103
リセット信号
外部接続
CPU
PC
92
95
98
モード信号
アクセスアドレス
アクセスステータス
判断部a
判断部b
14
24
35
30
32
優先回路M
34
reg1a
reg2a
regMa
regNa
18
regMb
28
読出回路
36
38
プロテクト制御信号
31
書込
読出
消去
3
プロテクト情報領域
データ領域
データ1
データ2
データM
データN
フラグ1a
フラグ2a
フラグMa
フラグNa
フラグMb
(なし)
3.1
3.2
3.3
データバス
投入信号
電源部
97
ブロック1
ブロック2
ブロックM
ブロックN

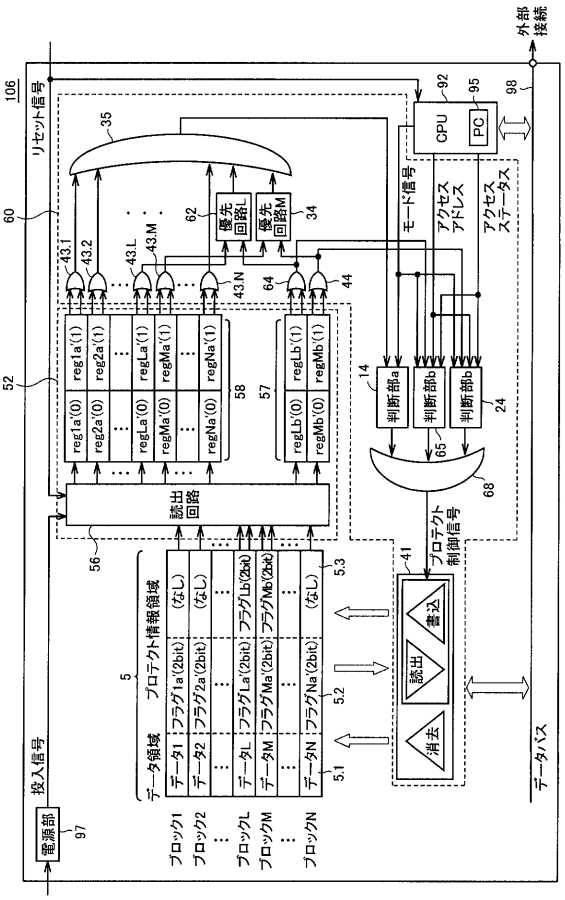
【図５】


104
リセット信号
外部接続
CPU
PC
92
95
98
モード信号
アクセスアドレス
アクセスステータス
判断部a
判断部b
14
24
35
40
42
優先回路M
34
43.1
43.2
43.M
43.N
44
reg1a'(0)
reg2a'(0)
regMa'(0)
regNa'(0)
reg1a'(1)
reg2a'(1)
regMa'(1)
regNa'(1)
regMb'(0)
regMb'(1)
48
47
読出回路
46
38
プロテクト制御信号
41
書込
読出
消去
4
プロテクト情報領域
データ領域
データ1
データ2
データM
データN
フラグ1a'(2bit)
フラグ2a'(2bit)
フラグMa'(2bit)
フラグNa'(2bit)
フラグMb'(2bit)
(なし)
4.1
4.2
4.3
データバス
投入信号
電源部
97
ブロック1
ブロック2
ブロックM
ブロックN

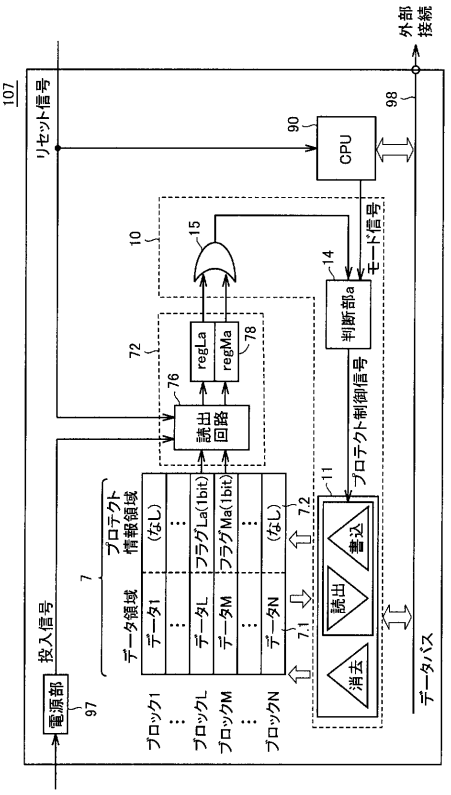
【図６】


105
リセット信号
外部接続
CPU
PC
92
95
98
モード信号
アクセスアドレス
アクセスステータス
判断部a
判断部b
14
24
35
50
52
優先回路M
34
43.1
43.2
53.LM
43.N
54
reg1a'(0)
reg2a'(0)
regLa'(0)
regMa'(0)
regNa'(0)
reg1a'(1)
reg2a'(1)
regLa'(1)
regMa'(1)
regNa'(1)
regLb'(0)
regMb'(0)
regLb'(1)
regMb'(1)
58
57
読出回路
56
38
プロテクト制御信号
41
書込
読出
消去
5
プロテクト情報領域
データ領域
データ1
データ2
データL
データM
データN
フラグ1a'(2bit)
フラグ2a'(2bit)
フラグLa'(2bit)
フラグMa'(2bit)
フラグNa'(2bit)
フラグLb'(2bit)
フラグMb'(2bit)
(なし)
5.1
5.2
5.3
データバス
投入信号
電源部
97
ブロック1
ブロック2
ブロックL
ブロックM
ブロックN

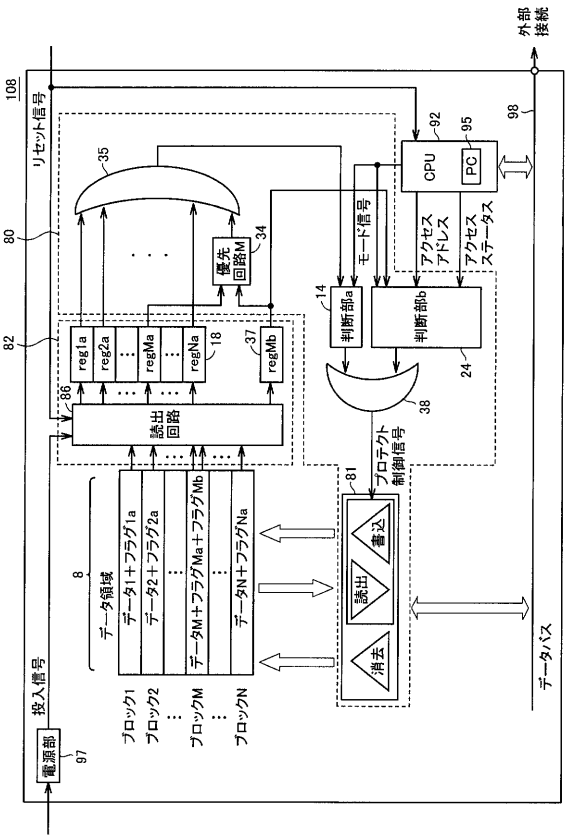
【図７】


106
リセット信号
投入信号
電源部
97
外部接続
98
CPU
92
PC
95
モード信号
アクセスアドレス
アクセスステータス
データバス
60
52
35
43.1
43.2
43.L
43.M
43.N
62
優先回路L
優先回路M
34
64
44
reg1a'(1)
reg2a'(1)
regLa'(1)
regMa'(1)
regNa'(1)
regLb'(1)
regMb'(1)
58
57
14
判断部a
判断部b
24
65
68
読出回路
56
5
データ領域
プロテクト情報領域
データ1
データ2
データL
データM
データN
フラグ1a'(2bit)
フラグ2a'(2bit)
フラグLa'(2bit)
フラグMa'(2bit)
フラグNa'(2bit)
フラグLb'(2bit)
フラグMb'(2bit)
(なし)
5.1
5.2
5.3
41
プロテクト制御信号
書込
読出
消去
ブロック1
ブロック2
ブロックL
ブロックM
ブロックN

【図８】


107
リセット信号
投入信号
電源部
97
外部接続
98
CPU
90
データバス
10
15
14
判断部a
モード信号
72
76
78
regLa
regMa
読出回路
プロテクト制御信号
11
7
プロテクト情報領域
データ領域
データ1
データL
データM
データN
(なし)
フラグLa(1bit)
フラグMa(1bit)
7.1
7.2
書込
読出
消去
ブロック1
ブロックL
ブロックM
ブロックN

【図９】


108
リセット信号
投入信号
電源部
97
外部接続
98
CPU
92
PC
95
モード信号
アクセスアドレス
アクセスステータス
データバス
80
82
35
34
優先回路M
14
判断部a
判断部b
24
38
reg1a
reg2a
regMa
regNa
regMb
18
37
86
読出回路
81
プロテクト制御信号
8
データ領域
データ1+フラグ1a
データ2+フラグ2a
データM+フラグMa+フラグMb
データN+フラグNa
書込
読出
消去
ブロック1
ブロック2
ブロックM
ブロックN

フロントページの続き

(74)代理人 100124523
弁理士 佐々木 眞人
(74)代理人 100098316
弁理士 野田 久登
(72)発明者 黒澤 飛斗矢
東京都千代田区丸の内二丁目４番１号 株式会社ルネサステクノロジ内

審査官 滝谷 亮一

(56)参考文献 特開平１１－１２０７８１（ＪＰ，Ａ）
特開平０８－２９２９１５（ＪＰ，Ａ）
特開平０７－２４４６１１（ＪＰ，Ａ）
特開平０９－１１４７４３（ＪＰ，Ａ）
特開平１０－３０１８５５（ＪＰ，Ａ）
特開昭６２－１９４５６５（ＪＰ，Ａ）
特開２００１－０１４８７１（ＪＰ，Ａ）
特開２００３－２０３０１２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／０２
Ｇ０６Ｆ ２１／２４