(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2007-501477
(P2007-501477A)
(43)公表日　平成19年1月25日(2007.1.25)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/24 (2006.01)	G06F 12/14 520A	5B017

審査請求 未請求　予備審査請求 未請求　（全 14 頁）

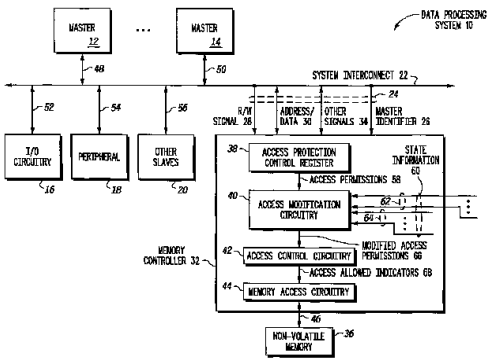
(21)出願番号　特願2006-532516 (P2006-532516)
(86)(22)出願日　平成16年4月30日 (2004.4.30)
(85)翻訳文提出日　平成17年11月28日 (2005.11.28)
(86)国際出願番号　PCT/US2004/013369
(87)国際公開番号　WO2004/107176
(87)国際公開日　平成16年12月9日 (2004.12.9)
(31)優先権主張番号　10/448,031
(32)優先日　平成15年5月29日 (2003.5.29)
(33)優先権主張国　米国 (US)

(71)出願人　504199127
フリースケール　セミコンダクター　インコーポレイテッド
アメリカ合衆国　７８７３５　テキサス州　オースティン　ウィリアム　キャノン　ドライブ　ウエスト　６５０１
(74)代理人　100116322
弁理士　桑垣　衛
(72)発明者　モイヤー、ウィリアム　シー
アメリカ合衆国　７８６２０　テキサス州　ドリッピング　スプリングス　ピア　ブランチ　ロード　１００５

最終頁に続く

(54)【発明の名称】アクセス許可を決定するための方法および装置

(57)【要約】
複数のマスタ（１２，１４）に対応する複数のアクセス要求（８４）を受信するステップと、アクセス許可（８６）を決定するステップと、状態情報（６０）を提供するステップと、アクセス要求（８４）に基づいてアクセス許可（８６）を決定ステップと、状態情報（９０）に基づいてアクセス許可を選択的に修正するステップと、を含むアクセス保護（９６）を決定するための方法および装置。状態情報（６０）は、デバッグ動作、非セキュアまたは検証されていないメモリからの動作、メモリ・プログラミング、ダイレクト・メモリ・アクセス動作、ブート動作、ソフトウェア・セキュリティ検査、セキュリティ・レベル、セキュリティ監視動作、動作モード、障害監視装置、外部バス・インタフェース等（８８）と関連することができる。



【特許請求の範囲】
【請求項１】
アクセス許可回路であって、
第１のバス・マスタに対応する第１のアクセス許可情報を記憶する第１のアクセス保護回路と、
第２のバス・マスタに対応する第２のアクセス許可情報を記憶する第２のアクセス保護回路と、
前記第１および第２のアクセス保護回路と結合しているアクセス修正回路と、
前記アクセス修正回路が提供するアクセス許可インジケータと、を備え、
前記第１のバス・マスタによる第１のアクセスに応じて、前記アクセス修正回路が、第１の状態情報を受信し、また前記第１のアクセス許可情報を受信し、
前記第１の状態情報に基づいて、前記アクセス修正回路が、第１の修正したアクセス許可情報を生成するために、前記第１のアクセス許可情報を選択的に修正し、
前記第１の修正したアクセス許可情報が、前記アクセス許可インジケータが、前記第１のアクセスを許可するかどうかを判断するために使用され、
前記第２のバス・マスタによる第２のアクセスに応じて、前記アクセス修正回路が第２の状態情報を受信し、前記第２のアクセス許可情報を受信し、
前記第２の状態情報に基づいて、前記アクセス修正回路が、第２の修正したアクセス許可情報を生成するために、前記第２のアクセス許可情報を選択的に修正し、
前記第２の修正したアクセス許可情報が、前記アクセス許可インジケータが、前記第２のアクセスを許可するかどうかを判断するために使用される、アクセス許可回路。
【請求項２】
前記第１の状態情報が、前記第１のバス・マスタの信頼性を表示する請求項１に記載のアクセス許可回路。
【請求項３】
前記第１の状態情報が、ブート動作に関連する請求項１に記載のアクセス許可回路。
【請求項４】
前記アクセス許可回路が、データ処理システムの一部を備える請求項１に記載のアクセス許可回路。
【請求項５】
前記第１の状態情報を提供するためのデバッグ回路をさらに備える請求項４に記載のデータ処理システム。
【請求項６】
前記第１の状態情報を提供するためのダイレクト・メモリ・アクセス（ＤＭＡ）をさらに備える請求項４に記載のデータ処理システム。
【請求項７】
前記第１の状態情報を提供するための外部バス・インタフェース回路をさらに備える請求項４に記載のデータ処理システム。
【請求項８】
前記第１のバス・マスタが、命令を実行するマスタ、ダイレクト・メモリ・アクセス（ＤＭＡ）動作を行うマスタ、およびデバッグ動作を行うマスタのうちの少なくとも１つを備える請求項１に記載の方法。
【請求項９】
アクセス保護を決定するための方法であって、
第１のマスタに対応する第１のアクセス要求を受信するステップと、
前記第１のマスタに対応する第１のアクセス許可を決定するステップと、
第１の状態情報を受信するステップと、
前記第１の状態情報に基づいて、前記第１のアクセス許可を選択的に修正するステップと、
第２のマスタから第２のアクセス要求を受信するステップと、

前記第２のマスタに対応する第２のアクセス許可を決定するステップと、
第２の状態情報を受信するステップと、
前記第２の状態情報に基づいて、前記第２のアクセス許可を選択的に修正するステップと、を含み、
前記第１の状態情報が、前記第２の状態情報とは異なるソースから提供される方法。
【請求項１０】
アクセス保護を決定するための方法であって、
第１のマスタに対応する第１のアクセス要求を受信するステップと、
第１の状態情報を提供するステップと、
前記第１のアクセス要求に基づいて、第１のアクセス許可を決定するステップと、
前記第１の状態情報に基づいて、前記第１のアクセス許可を選択的に修正するステップと、
第２のマスタに対応する第２のアクセス要求を受信するステップと、
第２の状態情報を提供するステップと、
前記第２のアクセス要求に基づいて、第２のアクセス許可を決定するステップと、
前記第２の状態情報に基づいて、前記第２のアクセス許可を選択的に修正するステップと、を含む方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アクセス許可に関し、特に、例えば、データ処理システムでアクセス許可を決定するためのアクセス許可回路に関する。
【背景技術】
【０００２】
システム・オン・チップ（ＳｏＣ）法の場合には、通常、例えば、メモリのような共有周辺部品およびスレーブ・デバイスを含む複数のマスタが存在する。共有周辺部品およびスレーブ・デバイスのすべてまたはいくつかのコンテンツは、システムを破壊する恐れがあるいくつかのマスタ上で稼働している、正当でないまたはその他の悪意のあるソフトウェアによる不正な変更、複写または問合せから保護しなければならない場合がある。例えば、システムの周辺デバイスおよびスレーブ・デバイス内のセキュア情報にアクセスするために使用することができる、安全保護されていないマスタ上で稼働しているソフトウェアにより、ウイルスが侵入する場合がある。さらに、システム内のいくつかのバス・マスタには安全保護されていると見なせるものもあるし、見なせないものもある。これらの状態は、システムの状態が変化すると変化する場合がある。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
それ故、システムの統合性およびセキュリティを確保するために、安全保護されていないマスタ上で稼働している正当でないまたは他の悪意のあるソフトウェアからシステムを保護する必要がある。
【課題を解決するための手段】
【０００４】
添付の図面に本発明を示すが、これは例示としてのものであって本発明を制限するものではない。図面中、類似の参照番号は類似の要素を示す。
当業者であれば、図面中の要素は図面を見やすく、分かりやすくするためのものであって、必ずしも正確な縮尺によるものではないことを理解することができるだろう。例えば、本発明の実施形態の理解を助けるために、図の要素のうちのあるものの寸法は他の要素より誇張してある場合がある。
【０００５】
本明細書で使用する場合、「バス」という用語は、データ、アドレス、制御または状態

のような１つ以上の種々のタイプの情報を転送するのに使用することができる複数の信号または導体を指すために使用される。本明細書で使用する導体は、１本の導体、複数の導体、一方向導体、または二方向導体に関連して説明または記述することができる。しかし、他の実施形態の場合には、異なる導体を使用することができる。例えば、二方向導体の代わりに別々の一方向導体を使用することもできるし、その逆を行うこともできる。また、複数の導体の代わりに、直列にまたは時間多重により複数の信号を転送する１本の導体を使用することができる。同様に、複数の信号を運ぶ１本の導体を、これら信号のサブセットを運ぶ種々の異なる導体に分割することもできる。それ故、信号を転送するのに多くの任意の方法を使用することができる。

【０００６】

システムの統合性およびセキュリティを確保するためには、例えば、複数のマスタ・データ処理システムのようなシステムが、安全保護されていないプロセッサまたは他のマスタ上で稼働している正当でないまたは他の悪意のあるソフトウェアにより決して危険にさらされないようにすることが望ましい。例えば、複数のマスタ・システム内の複数のマスタは、例えば、システムの周辺デバイスまたはスレーブ・デバイスのような同じリソースを共有することができる。複数のマスタのうちのいくつかは安全保護されていると見なすことができるが、他のものは安全保護されていないと見なすことができる。本明細書で使用する場合には、セキュア・マスタという用語は、一般的によりアクセスし易く、損傷を受けやすい非セキュア・マスタに比べて、一般的にアクセスしにくく、損傷を受けにくいマスタを意味する。例えば、セキュア・マスタは、アクセスしにくく、またはマスタまたはＳｏＣのメーカーにより完全に制御されている命令を実行することができる（すなわち、セキュア・マスタ上で稼働しているソフトウェアは、信頼性の高いソフトウェアまたはセキュア・ソフトウェアであると見なすことができる）。しかし、非セキュア・マスタは、第三者ソフトウェア（例えば、ユーザが開発したソフトウェア）を受信し、実行することができる一般的な用途向けのプロセッサであってもよいし、または任意の他の信頼できないソフトウェア（一般的に、ソフトウェアの内容および機能が分からない）であってもよい。ソフトウェアが信頼できないので、そのソフトウェアは、システムの他の部分を破壊しようとするかもしれないし、またはセキュア情報にアクセスしようとするかもしれない、正当でないかまたは他の悪意のあるソフトウェアである場合がある。さらに、安全保護されている、または安全保護されていない特定のマスタの状態は、データ処理システムが変化すると変化する場合がある。

【０００７】

それ故、本発明の一実施形態を使用すれば、例えば、不揮発性メモリのようなスレーブ・デバイスまたは周辺デバイスの内容を安全保護されている状態で動作している場合、プログラムの実行を、不揮発性メモリから続行することができるが、もっと安全保護の薄い状態で動作している場合に、不正なアクセスを防止することができる方法で安全保護状態にすることができる。一実施形態は、システム状態が図１～図３を参照しながら以下に説明するように、データ処理システムの予めプログラムしたアクセス保護政策を修正または無視することができる方法を提供する。上記無視は、例えば、システムのリソース（例えば、スレーブ・デバイス、周辺デバイス、メモリ、共有リソース等）へのシステム内の各マスタに対して、一緒にまたは別々に、読出しアクセスおよび書込アクセスを制限するために（または逆にこれらのアクセスに対するアクセス許可を緩やかにするために）使用することができる。さらに、これらの無視は、状態情報が変化すると、動的に変化する場合がある。また、さらに以下に説明するように、状態情報は、例えば、デバッグ・モードを使用できるようにすること、安全保護されていないまたは検証されていないメモリ領域からのプログラムの実行、不揮発性メモリの一部の再プログラミング等に関連する情報のようなデータ処理システムの状態に関する任意のタイプの情報を含むことができる。

【発明を実施するための最良の形態】

【０００８】

図１は、データ処理システム１０の一実施形態である。データ処理システム１０は、マ

スタ１２（相互接続またはバス・マスタ１２とも呼ばれる）と、マスタ１４（相互接続またはバス・マスタ１４とも呼ばれる）と、メモリ・コントローラ３２と、不揮発性メモリ３６と、システム相互接続２２と、１／Ｏ回路１６と、周辺デバイス１８と、他のスレーブ・デバイス２０とを含む。マスタ１２は、導体４８を通してシステム相互接続２２に二方向で結合していて、マスタ１４は、導体５０を通してシステム相互接続２２に二方向で結合していて、Ｉ／Ｏ回路は、導体５２を介してシステム相互接続２２に二方向で結合していて、周辺デバイス１８は、導体５４を通してシステム相互接続２２に二方向で結合していて、他のスレーブ・デバイス２０は、導体５６を通してシステム相互接続２２に二方向で結合していて、メモリ・コントローラ３２は、導体２４を通してシステム相互接続２２に二方向で結合している。導体２４は、マスタ識別子２６、アドレス／データ３０、Ｒ／Ｗ信号２８、および他の信号３４を送るための導体を含む。

【０００９】

メモリ・コントローラ３２は、アクセス保護制御レジスタ３８と、アクセス修正回路４０と、アクセス制御回路４２と、メモリ・アクセス回路４４とを含み、導体４６を通して不揮発性メモリ３６に二方向で結合している。アクセス保護制御レジスタは、アクセス修正回路４０へアクセス許可５８を提供する。アクセス修正回路４０は、データ処理システム１０内の情報から導体６２を通して、またメモリ・コントローラ３２内の情報から導体６４を通して状態情報６０を受信し、修正したアクセス許可６６をアクセス制御回路４２に供給する。他の実施形態の場合には、状態情報６０は、（導体６２を通して）データ処理システム１０が供給した情報だけを含むことができるか、またはメモリ・コントローラ３２内から供給した情報だけを含むことができることに留意されたい。さらに、状態情報６０は、（導体６２の何本かのまたはすべてを介して）データ処理システム１０の外部のソースから供給された情報を含むことができる。それ故、以下にさらに詳細に説明するように、状態情報６０は、アクセス修正回路４０に所望の状態情報を提供する任意のタイプの信号またはインジケータを含むことができる。アクセス制御回路４２は、メモリ・アクセス回路４４にアクセス許可インジケータ６８（１つまたは複数のインジケータを含むことができる）を提供する。

【００１０】

図１には周辺デバイス１８は１つしか図示していないが、データ処理システム１０は、システム相互接続２２と結合している任意の数の周辺デバイスを含むことができる。同様に、任意の数のマスタおよびスレーブをシステム相互接続２２に結合することができ、図１に示すものに限定されない。また、一実施形態の場合には、すべてのデータ処理システム１０を、１つの集積回路上または同じデバイス内に位置させることができることに留意されたい。別の方法としては、データ処理システム１０は、任意の数の個々の集積回路または相互に接続している個々のデバイスを含むことができる。例えば、一実施形態の場合には、メモリおよびメモリ・コントローラ（例えば、不揮発性メモリ３６およびメモリ・コントローラ３２など）をデータ処理システム１０の残りの部分から独立している１つまたは複数の集積回路上に位置させることができる。

【００１１】

一実施形態の場合には、マスタ１２およびマスタ１４は、マイクロプロセッサ、デジタル信号プロセッサ等のような命令を実行することができるプロセッサであってもよいし、またはダイレクト・メモリ・アクセス（ＤＭＡ）回路またはデバッグ回路のような任意の他のタイプの相互接続またはバス・マスタを含むことができる。また、図には２つのマスタしか図示していないが、データ処理システム１０は、必要に応じて任意の数（１つまたは複数）のマスタを含むことができる。また、任意の所与の動作点において、各マスタ１２および１４は、異なるレベルのセキュリティを行うことができることに留意されたい。すなわち、例えば、特定の動作点におけるデータ処理システム１０の状態に従って、各マスタ１２および１４は、安全保護されているマスタであってもよいし、安全保護されていないマスタであってもよい。周辺デバイス１８は、汎用非同期受信送信機（ＵＡＲＴ）、リアルタイム・クロック（ＲＴＣ）、キーボード・コントローラ、任意のタイプのメモリ

等のような任意のタイプの周辺デバイスであってもよい。他のスレーブ２０が、例えば、マスタ１２および１４がアクセスすることができるメモリ、および周辺デバイス１８のような同じタイプの周辺デバイスを含むシステム・バス上に常駐する任意のタイプの周辺デバイスのような任意のタイプの相互接続スレーブを含むことができることに留意されたい。Ｉ／Ｏ回路１６は、データ処理システム１０の内部または外部の情報を受信し、提供する任意のタイプのＩ／Ｏ回路を含むことができる。

【００１２】

図の実施形態の場合には、メモリ・コントローラ３２および不揮発性メモリ３６は、システム相互接続２２と結合している他のスレーブ・デバイスに対応する。一実施形態の場合には、不揮発性メモリ３６を、システム相互接続２２（例えば、マスタ１２および１４など）と結合している少なくとも２つのマスタにより共有することができることに留意されたい。不揮発性メモリ３６は、マスタ１２および１４として同じ集積回路上に、または別々の集積回路上に位置させることができる。さらに、図のメモリ３６は、不揮発性メモリ（フラッシュ・メモリなど）であるが、メモリ３６は、例えば、読出し専用メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、ダイナミックＲＡＭ（ＤＲＡＭ）、スタティックＲＡＭ（ＳＲＡＭ）、不揮発性メモリ（例えば、フラッシュ、ＭＲＡＭ）等のような任意のタイプのメモリであってもよい。また、メモリ３６は、他の周辺デバイスまたはスレーブ・デバイス内に位置するメモリまたは他の記憶装置であってもよい。さらに他の実施形態の場合には、メモリ３６は、メモリ・コントローラ３２を、リソースを保護するためのアクセス保護回路を有する任意のタイプのコントローラと置換できる場合に、保護する必要があるセキュア情報を有する任意の他のタイプのリソースであってもよい。

【００１３】

システム相互接続２２は、マスタ１２、マスタ１４、Ｉ／Ｏ回路１６、周辺デバイス１８、他のスレーブ・デバイス２０、およびメモリ・コントローラ３２を相互に接続する。一実施形態の場合には、図１に示すように、システム相互接続２２は、システム・バス・プロトコルにより動作するシステム・バスとして実施される。別の方法としては、システム相互接続２２を、例えば、種々のデバイス間で情報を経路指定するスイッチング回路のような相互接続回路により実施することができる。

【００１４】

動作中、マスタ１２および１４は、メモリ・コントローラ３２を介して、他のスレーブ・デバイス２０、周辺デバイス１８、または不揮発性メモリ３６へのアクセスを要求するために、システム相互接続２２の使用を要求する。要求を行っているマスタは、システム相互接続２２を介して、メモリ・コントローラ３２にアクセス要求を供給することができる。アクセス要求は、例えば、データまたは命令に対する読出し要求または書込み要求であってもよい。メモリ・コントローラ３２は、読出しアクセス要求に応じて、要求しているマスタが十分なアクセス許可を有しているものと仮定して、システム相互接続２２を介して要求しているマスタに要求された情報（データまたは命令）を返送する。一実施形態の場合には、アクセス要求に対して、マスタ識別子２６がメモリ・コントローラ３２に提供され、メモリ・コントローラはどのマスタが現在のアクセスを要求しているのかを識別する。また、現在のアクセス要求が読出しタイプのアクセスなのか、書込みタイプのアクセスなのかを表示するために、Ｒ／Ｗ信号２８をメモリ・コントローラ３２に提供することもできる。メモリ・コントローラ３２は、また、現在のアクセス要求に対応するアドレス情報を受信し、アドレス／データ３０により要求された情報を提供する。メモリ・コントローラ３２へ／から送らなければならない任意の他の信号（状況、制御、データなど）は、他の信号３４により提供することができる。

【００１５】

マスタ１２および１４のような各マスタは、不揮発性メモリ３６への特定のアクセス要求が許可できるものかどうかを判断するために使用することができる、対応するアクセス許可を有することができる。例えば、特定のマスタは、不揮発性メモリ３６に対する書込みアクセスまたは読出しアクセスに対する異なるアクセス許可を有することができる。一

実施形態の場合には、これらのアクセス許可は、アクセス保護制御レジスタ３８内に記憶される。

【００１６】

図２は、図１のアクセス保護制御レジスタ３８の一例である。一実施形態の場合には、アクセス保護制御レジスタ３８は、データ処理システム１０内の各マスタに対する１つのアクセス保護フィールドを含む。例えば、アクセス保護制御レジスタ３８は、それぞれマスタ１２および１４に対応するマスタ１２アクセス保護フィールド７０およびマスタ１４アクセス保護フィールド７６を含む。アクセス保護フィールドは、特定のマスタにより不揮発性メモリ３６への特定のタイプのアクセスが許可されるかどうかを表示する。例えば、図の実施形態の場合には、各アクセス保護フィールド７０および７６は、各マスタに対する読出しアクセスおよび書込みアクセスに対する許可を表示するために、読出しアクセス保護フィールドおよび書込アクセス保護フィールドを含む。

【００１７】

マスタ１２アクセス保護フィールド７０は、マスタ１２が、不揮発性メモリ３６に読出しアクセスを行うことができるかどうかを表示する、マスタ１２読出しアクセス保護フィールド７２、およびマスタ１２が、不揮発性メモリ３６に書込みアクセスを行うことができるかどうかを表示する、マスタ１２書込みアクセス保護フィールド７４を含む。それ故、マスタ１２は、不揮発性メモリ３６に読出しアクセス、または書込みアクセスの一方だけを行うことを許可することができる。別の方法としては、マスタ１２は、フィールド７２および７４の値に従って、不揮発性メモリ３６への読出しおよび書込みアクセスの両方を行うことを許可することもできるし、読出しアクセスおよび書込みアクセスの両方を行うことを許可しないこともできる。一実施形態の場合には、各フィールド７２および７４は、対応するアクセス・タイプ（読出しまたは書込み）が許可されるかどうかを示すための１ビット・フィールドである。同様に、マスタ１４アクセス保護フィールド７６は、マスタ１４が、不揮発性メモリ３６へ読出しアクセスを行うことができるかどうかを示すマスタ１４読出しアクセス保護フィールド７８、マスタ１４が、不揮発性メモリ３６に対して書込みアクセスを行うことができるかどうかを示すマスタ１４書込みアクセス保護フィールド８０を含む。それ故、マスタ１４は、不揮発性メモリ３６への読出しアクセス、または書込みアクセスの一方だけを行うことを許可することができる。別の方法としては、マスタ１４は、フィールド７８および８０の値に従って、不揮発性メモリ３６への読出しおよび書込みアクセスの両方を行うことを許可することもできるし、読出しアクセスおよび書込みアクセスの両方を行うことを許可しないこともできる。一実施形態の場合には、各フィールド７８および８０は、対応するアクセス・タイプ（読出しまたは書込み）が許可されるかどうかを示すための１ビット・フィールドである。

【００１８】

他の実施形態の場合には、アクセス保護制御レジスタ３８は、フィールド７０および７６のような任意の数のアクセス保護フィールドを含むことができることに留意されたい。例えば、アクセス保護制御レジスタ３８は、データ処理システム１０内の各マスタに対する１つのアクセス保護フィールドを含むこともできるし、データ処理システム１０内にマスタのサブセットだけを含むこともできる。また、各アクセス保護フィールド７０および７６は、読出しおよび書込みアクセス（例えば、バースト・アクセスなど）の代わりにまたはそれに加えて、異なるタイプのアクセスに基づいて、許可を識別するための任意の数のフィールドを含むことができることに留意されたい。さらに、フィールド７０、７２、７４、７６、７８、および８０は、異なるフィールド定義、異なるビット割当て、または異なる数のビットを使用するというような種々の異なる方法で実施することができる。別の方法としては、これらのフィールドは、またはデータ処理システム１０の別々のレジスタまたは他のレジスタまたはメモリ位置のような異なる方法で組織化することができる。通常、アクセス保護制御レジスタ３８は、セキュア・マスタによりプログラムすることができるソフトウェアである。一実施形態の場合には、アクセス保護制御レジスタ３８は、リセットの際にプログラムすることができる。

【００１９】
図１に戻って説明すると、アクセス修正回路４０は、制御レジスタ３８内に記憶しているアクセス許可の１つまたは複数を修正（または無視）するために使用することができる。例えば、状態情報６０に従って、アクセス修正回路４０は、修正したアクセス許可６６を提供するために、アクセス保護制御レジスタ３８からアクセス許可５８を選択的に修正することができる。すなわち、場合によっては、修正したアクセス許可６６を生成するために、すべてのアクセス許可５８を修正することができるし、または別の方法としては、修正したアクセス許可６６が１つだけまたはいくつかの修正した許可を含むように、アクセス許可５８の１つだけまたはいくつかを修正することができる。すなわち、修正したアクセス許可６６は、現在修正されていないアクセス保護制御レジスタ３８からの許可を含むことができる。また、修正したアクセス許可６６は、特定のマスタに対してメモリ３６へのもっと広い（または制限がもっと緩やかな）アクセスを供給することができし、または特定のマスタに対してメモリ３６へのアクセスを制限することもできることに留意されたい。

【００２０】
図１に戻って説明すると、アクセス制御回路４２は、修正したアクセス許可６６に基づいて、現在のアクセス要求が許可されるかどうかを判断することができる。例えば、データ処理システム１０内の各マスタ（マスタ１２および１４など）は、対応するマスタ識別子を有することができる。一実施形態の場合には、各マスタを対応する番号により一意に識別することができるように、マスタ１２をマスタ識別子０に対応させることができるし、マスタ１４をマスタ識別子１に対応させることができる。他の実施形態の場合には、任意のタイプの識別子を使用することができ、任意の方法で割り当てることができ、０からスタートするまたは１桁の番号からスタートするというような番号順に制限されない。また、他の実施形態の場合には、複数のマスタが同じマスタ識別子を共有することができる。それ故、アクセス制御回路４２は、（マスタ識別子２６によりアクセス制御回路４２に表示された）現在のアクセスをどのマスタが要求しているのかに基づいて、また（修正したアクセス許可６６によりアクセス制御回路４２に表示された）アクセス許可に基づいて、不揮発性メモリ３６へのアクセスが許可されるかどうかを判断することができる。アクセスが許可される場合には、アクセス許可インジケータ６８が、メモリ・アクセス回路４４が、要求したアクセスを終了（例えば、要求した読出しまたは書込みを終了）するために必要な信号および情報を不揮発性メモリ３６に供給することができるように、メモリ・アクセス回路４４へのアクセスが許可されることを表示する。しかし、現在要求しているマスタに対する修正したアクセス許可６６に基づいて、アクセス制御回路４２が、アクセスが許可されないと判断した場合には、アクセス許可インジケータ６８は、メモリ・アクセス回路４４が要求したアクセスを終了しないように、アクセスが許可されないことを表示する。図３を参照しながら、メモリ・コントローラ３２の動作についてさらに説明する。

【００２１】
図３は、本発明の一実施形態によるメモリ・コントローラ３２の動作に対応する流れ９６を示す。流れ９６は、スタート８２からスタートし、ブロック８４に進み、ここでアクセス要求が受信される。例えば、マスタ１２または１４は、システム相互接続２２を介して、不揮発性メモリ３６にアクセス要求を供給することができる。アクセス要求は、例えば、Ｒ／Ｗ信号２８で示すように、読出し要求または書込み要求であってもよい。次に、流れはブロック８６に進み、ここでアクセス許可が決定される。例えば、これらのアクセス許可は、アクセス保護制御レジスタ３８内のフィールド（フィールド７０および７６など）により提供することができる。次に、流れはブロック８８に進み、ここで状態情報（状態情報６０など）が受信される。状態情報は、例えば、デバッグ動作、安全保護されていないまたは検証されていないメモリからの動作、メモリ・プログラミング、ダイレクト・メモリ・アクセス（ＤＭＡ）動作、ブート動作、ソフトウェア・セキュリティ検査、セキュリティ・レベル、セキュリティ監視動作、動作モード、障害監視装置、外部バス動作

等と関連することができる。すなわち、情報は、状態情報６０により、上記条件、状態または動作の１つまたは複数を表示することができるアクセス修正回路４０に提供することもできるし、上記条件、状態または動作の１つまたは複数に関連する情報を表示することもできる。それ故、状態情報６０は、メモリ・コントローラ３２内の（マスタ１２、マスタ１４、Ｉ／Ｏ回路１６、周辺デバイス１８または他のスレーブ２０からのような）データ処理システム１０内の種々の場所から、またはデータ処理システム１０の外部の場所から、またはこれらの任意の組合わせから受信することができる。

【００２２】

例えば、デバッグ動作に関連する状態情報の場合には、状態情報６０の信号の１つまたは複数を、別々のユニットとしての、または例えば、マスタ１２または１４の一部としてのシステム相互接続２２と結合しているデバッグ回路（図示せず）から受信することができる。状態情報６０内の信号は、また、アクセス修正回路４０への２つ以上のリソースに基づいて、結合状態情報または状態情報を提供するための種々の異なる方法で結合することができる。この結合回路は、アクセス修正回路４０内、アクセス修正回路４０の外部、またはメモリ・コントローラ３２の外部にも位置することができる。

【００２３】

図３を参照すると、次に、流れはブロック９０に進み、ここで受信した状態情報に基づいて、アクセス許可が選択的に修正される。例えば、一実施形態の場合には、状態情報６０により送られたいくつかの条件または状況が、アクセス保護制御レジスタ３８内に記憶している許可を、ハードウェアにより無視することができるように、アクセス許可を修正するためにハードウェア無視を使用することができる。例えば、一実施形態の場合には、いくつかの条件が満たされた場合に、修正したアクセス許可６６のような修正したアクセス許可を生成するために、ハードウェアによりアクセス保護制御レジスタ３８の値を修正または置換できるように、状態情報６０を必要に応じて結合し、ハードウェア無視回路に入力（または直接入力）することができる。別の方法としては、修正したアクセス許可６６を生成するために、他のハードウェア的方法またはソフトウェア的方法のような他の方法で状態情報６０に基づいて、アクセス許可５８を選択的に修正することができる。

【００２４】

次に、流れは、ブロック９２に進み、ここで修正したアクセス許可に基づいて、要求したアクセスが選択的に実行される。例えば、マスタ１２が不揮発性メモリ３６に読出しアクセスを要求し、マスタ１２の読出しアクセス保護フィールド７２が、マスタ１２による読出しアクセスが許可されることを表示した場合には、（それがアクセス修正回路４０により修正されていないと仮定して）マスタ１２の要求が実行される。しかし、状態情報６０が、マスタ１２の読出しアクセス許可を（許可ではなく拒否するように）修正すべきであると表示している場合には、要求した読出しアクセスが許可ではなく、拒否され、マスタ１２読出しアクセス保護フィールド７２を無視するように、アクセス修正回路４０は、読出しアクセス許可を修正する（およびそれを修正したアクセス許可６６の一部として提供する）ことができる。次に、流れはエンド９４のところで終わる。（図３の流れは、メモリ・コントローラ３２を介して、メモリ３６への各アクセス要求の度に反復することができることに留意されたい。）

それ故、マスタ１２または１４のようなマスタによる不揮発性メモリ３６への各アクセスの場合、アクセス保護制御レジスタ３８は、現在のアクセスを許可すべきかどうかを判断するために使用することができるアクセス許可５８を提供する。しかし、データ処理システム１０の状態情報に従って、これらソフトウェア・プログラマブル・レジスタを無視するのが望ましい（それ故、修正したアクセス許可６６になる）状況がある。例えば、アクセス保護制御レジスタ３８がソフトウェア・プログラマブルである場合には、アクセス保護制御レジスタ３８内に記憶している許可が、非セキュア・ソフトウェアにより、保護しなければならないセキュア情報へのアクセスを間違って許可するように変化している場合がある。それ故、データ処理システム１０のある状態情報または条件に従って、セキュア情報へのアクセスを防止するために、アクセス保護制御レジスタ３８のアクセス許可を

修正するために使用することができる修正（ハードウェア無視など）を行うために、アクセス修正回路４０を使用することができる。

【００２５】

ある例の場合には、デバッグ動作中アクセスを制限しなければならない場合がある。何故なら、デバッグ中は、一般的に、データ処理システム１０にアクセスし易くなるからである。それ故、一実施形態の場合には、状態情報６０は、デバッグを行うことができる時を表示するデバッグ回路（図示せず）からの情報を含む。この場合、アクセス保護制御レジスタ３８内に記憶しているマスタ１２および１４のうちのいくつかまたはすべての許可をアクセス修正回路４０により修正することができる。

【００２６】

他の例の場合には、非セキュアまたは検証されていないメモリからの動作中、データ処理システム１０のセキュリティを確保し、例えば、これらの非セキュアまたは検証されていないメモリ内に記憶している正当でないまたは悪意のあるソフトウェアによるものと思われる破壊を防止するために、アクセスを修正しなければならない場合がある。

【００２７】

他の例の場合には、メモリがプログラムされている場合には、アクセス許可を修正することができる。例えば、図１を参照すると、不揮発性メモリ３６が修正される場合には、不揮発性メモリ３６へのアクセス許可を修正することができる。何故なら、不揮発性メモリ３６の修正した部分のセキュリティを確保することができないからである。例えば、不揮発性メモリ３６が修正されていて、悪いデータ、間違っている情報を含んでいたり、または正当でないまたは悪意のあるソフトウェアを記憶している場合がある。この場合、状態情報６０は、例えば、導体６４を介して、メモリ・コントローラ３２内から提供された情報を含むことができる。

【００２８】

さらに他の例の場合には、アクセス許可を、ダイレクト・メモリ・アクセス（ＤＭＡ）動作のために修正することができる。この例の場合には、状態情報６０は、ＤＭＡ動作（例えば、マスタ１２または１４がＤＭＡであるか、ＤＭＡを含んでいる）の発生を示すために、ＤＭＡからの信号を含むことができる。他の例の場合には、セキュア情報を安全保護されている状態のままに確実に維持するために、ブート動作の際にアクセス許可を修正することができる。何故なら、システムが、正当でないファームウェア、ソフトウェアまたは設定のために未知の状態にブートされる場合があるからである。また、アクセス保護制御レジスタ３８内に記憶しているアクセス許可が、ソフトウェアを検査することができるまでアクセスを制御することができないように（すなわち、無視または修正されるように）、ソフトウェア・セキュリティ検査に基づいてアクセス許可を修正することができる。アクセス許可は、また、データ処理システム１０またはマスタ１２および１４のセキュリティ・レベルに基づいて修正することができる。例えば、各マスタは、（セキュア状態、非セキュア状態をちょうど超えた）変化するセキュリティ・レベルを有することができる。この場合、特定のアクセス要求中のセキュリティ・レベルに基づいて、制御レジスタ３８へのアクセス許可を修正することができる。アクセス許可は、また、セキュリティ監視動作に基づいて修正することもできる。例えば、セキュリティ監視装置（図示せず）を、セキュリティが確実に遵守されるように、データ処理システム１０内の動作を監督するデータ処理システム１０に内蔵させることができる。それ故、セキュリティ監視装置がある状態を検出した場合には、それに従ってアクセスが修正される。それ故、状態情報６０は、アクセス修正回路４０へのこれらの状況、条件および動作に関連する情報を提供するために使用することができる。

【００２９】

また、他の例の場合には、状態情報６０が示すように、データ処理システムまたはメモリ・コントローラ３２の動作モードに基づいて、アクセス許可を修正することができる。例えば、データ処理システム１０が、（動作の基本的セットしかサポートされない最低動作状態のような）低いレベルの動作状態に入った場合には、低いレベルで動作しながらデ

ータ処理システム１０を保護するために、制御レジスタ３８のプログラムしたアクセス許可を修正することができる。他の実施形態の場合には、アクセス許可は、データ処理システム１０の障害監視装置（図示せず）に基づいて修正することができる。例えば、データ処理システム１０の任意の部分の障害を検出する障害監視装置に応じて、制御レジスタ３８のアクセス許可を、障害を検出した場合にアクセスを制限するように修正することができる。この例の場合には、障害監視装置からの信号を、状態情報６０によりアクセス修正回路４０に送ることができる。さらに他の実施形態の場合には、アクセス許可を外部バス動作に基づいて修正することができる。例えば、外部バスの動作中、外部ソースは、セキュア情報にアクセスまたはセキュア情報を修正しようと試みることもできるし、メモリ３６またはデータ処理システム１０を破壊しようと試みることもできる。それ故、データ処理システム１０のセキュリティを確保するために、外部バス動作中、アクセスに対するアクセス許可を制限することができる。

【００３０】

制御レジスタ３８のアクセス許可を選択的に修正するために、状態情報（例えば、状態情報６０により提供された）を使用することができるいくつかの状況に対して多くの例を記述したことに留意されたい。他の実施形態は、上記の例よりももっと多くのまたはもっと少ない情報を使用することができる。さらに、データ処理システム１０のニーズに従って、アクセス許可を修正しなければならない時を決定するために、任意の種々の方法で状態情報６０を組合わせることができる上記状況の組合わせを使用することができる。すなわち、状態情報６０は、アクセス修正回路４０が、アクセス許可を修正するのかしないのかを正しく判断することができるように、アクセス修正回路４０に必要な状態情報を表示するために、メモリ・コントローラ３２内からのものを含む種々の異なるリソースまたはソースから取り出すことができる。さらに、状態情報は、データ処理システム１０またはその構成要素のうちの任意のものの状態および条件を反映する任意のタイプの情報を含むことができる。また、状態情報は、１つまたは複数のマスタ（マスタ１２および１４など）の信頼性を表示することができる。また、上記大部分の例は、アクセス許可の制限についてものであったが、アクセス修正回路４０は、また、データ処理システム１０の設計に従って、アクセス許可を緩和または広くするために状態情報を使用することもできることに留意されたい。

【００３１】

それ故、複数のマスタ・データ処理システムを含むデータ処理システムのセキュリティをどのようにして改善できるのかを理解することができるだろう。アクセス修正回路は、種々の異なるタイプの状態情報に基づいて、アクセス許可を選択的に修正するために使用することができる。それ故、データ処理システム１０の状態が変化した場合、アクセス毎にアクセス許可を制限したり、緩和したりすることにより、必要に応じてセキュリティを維持することができる。さらに、修正は、マスタ毎におよびアクセス・タイプ毎に行うことができる。状態情報は、メモリ・コントローラ３２内の情報を含む、データ処理システム１０の種々の部分から受信した情報を含むこともできるし、データ処理システム１０の外部のソースから受信した情報も含むことができる。また、アクセス修正回路は、ハードウェア無視機構を使用して、アクセス許可を選択的に修正することができることに留意されたい。別の方法としては、修正したアクセス許可６６を生成するために、他のハードウェア、ソフトウェアまたはこれらの組み合わせ、機構を使用することができる。

【００３２】

上記説明においては、特定の実施形態を参照しながら本発明を説明してきた。しかし、通常の当業者であれば、添付の特許請求の範囲に記載する本発明の範囲から逸脱することなしに、種々の修正および変更を行うことができることを理解することができるだろう。例えば、データ処理システム１０およびメモリ・コントローラ３２を、図１の実施形態で説明したのとは別の方法で組織化することができる。さらに、ハードウェア、ソフトウェアおよびファームウェアの任意の組合わせで回路を実施することができる。それ故、明細書および図面は説明のためのものであって、本発明を制限するものではなく、このような

すべての修正は、本発明の範囲内に含まれると解釈すべきである。

【００３３】

特定の実施形態を参照しながら、本発明の利益、他の利点および問題の解決方法について説明してきた。しかし、任意の利益、利点または解決方法をもたらしたり、より優れたものにすることができる上記利益、利点、問題の解決方法および任意の要素は、任意のまたはすべての請求項の重要な、必要なまたは本質的な機能または要素と解釈すべきではない。本明細書で使用する場合、ある（「ａ」または「ａｎ」）という用語は、１つまたは複数と定義される。本明細書で使用する場合、「含む」（ｉｎｃｌｕｄｉｎｇ）および／または「有する」（ｈａｖｉｎｇ）という用語は、「備える」（すなわち、オープン言語）と定義される。本明細書で使用する場合、「備える」（ｃｏｍｐｒｉｓｅ）、「備えている」（ｃｏｍｐｒｉｓｉｎｇ）またはその任意の他の派生語は、要素のリストを備えるプロセス、方法、物品または装置が、これらの要素を含むばかりでなく、リストに明示されていないか、またはこのようなプロセス、方法、物品または装置固有の他の要素を含むことができるように、非排他的な内容を含む。

【図面の簡単な説明】

【００３４】

【図１】本発明の一実施形態によるデータ処理システムのブロック図。

【図２】本発明の一実施形態による、図１のデータ処理システムのアクセス保護制御レジスタのブロック図。

【図３】本発明の一実施形態による、図１のデータ処理システムの動作の流れ図。

【図１】

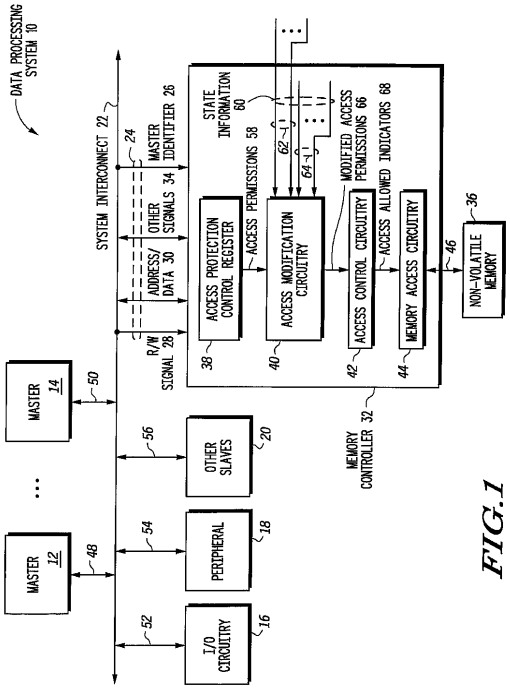


FIG.1

【図２】

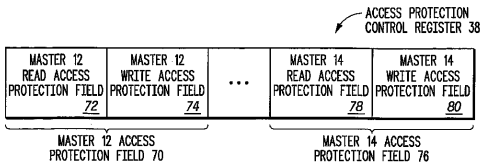


FIG.2

【図３】

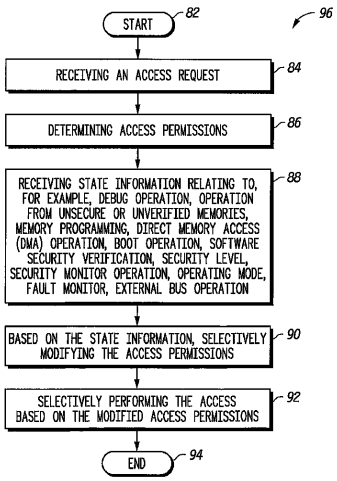


FIG.3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/13369

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 11/30, 13/28, 13/36
US CL : 713/200, 201; 710/241, 113, 22, 28
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/200, 201; 710/241, 113, 22, 28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,021,455 (KONDO et al) 1 February 2000 (01.02.2000), column 3, line 17 - column 4, line 50, column 7, line 1 - column 8, line 27, column 12, lines 6 - 63.	1-10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
20 August 2004 (20.08.2004)

Date of mailing of the international search report
29 OCT 2004

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
Ayaz Sheikh
for Michelle K. Glaser
Telephone No. 703-305-9648

Form PCT/ISA/210 (second sheet) (January 2004)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 マリク、アフザル エム.
アメリカ合衆国 ７８７５９ テキサス州 オースティン グレート ヒルズ トレイル １００５０ アパートメント５１７

Ｆターム(参考) 5B017 AA02 AA03 BA06 CA11