(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3982687号
(P3982687)
(45)発行日　平成19年9月26日(2007.9.26)　(24)登録日　平成19年7月13日(2007.7.13)

(51)Int.Cl.　F I
G06F 12/14 (2006.01)　G06F 12/14 510E

請求項の数 12　(全 24 頁)

(21)出願番号	特願2002-512776(P2002-512776)
(86)(22)出願日	平成13年7月13日(2001.7.13)
(65)公表番号	特表2004-504663(P2004-504663A)
(43)公表日	平成16年2月12日(2004.2.12)
(86)国際出願番号	PCT/US2001/022027
(87)国際公開番号	WO2002/006929
(87)国際公開日	平成14年1月24日(2002.1.24)
審査請求日	平成16年9月2日(2004.9.2)
(31)優先権主張番号	09/618,738
(32)優先日	平成12年7月18日(2000.7.18)
(33)優先権主張国	米国(US)

(73)特許権者　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５２　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　ゴリバー，ロジャー
アメリカ合衆国・９７００７・オレゴン州・ビーバートン・サウスウェスト　ナイトホーク　ドライブ・１６１８５
(72)発明者　サットン，ジェイムズ・ザ　セカンド
アメリカ合衆国・９７２２９・オレゴン州・ポートランド・ノースウェスト　パウリナ　ドライブ・２０２０５
最終頁に続く

(54)【発明の名称】分離実行環境での複数の分離メモリへのアクセスの制御

(57)【特許請求の範囲】
【請求項１】
相互に接続されるプロセッサとメモリとを有する装置であって、
複数のページを非分離区域と分離区域とに分割される前記メモリの複数の異なる区域にそれぞれ分配し、前記メモリの分離区域に配置され、前記プロセッサの制御の下で実行されるページ・マネージャと、
前記メモリの分離区域に配置され、前記メモリの各ページを記述するメモリ所有権ページ・テーブルと、
を含む装置。
【請求項２】
相互に接続されるプロセッサとメモリとを有する装置の動作方法であって、
複数のページを非分離区域と分離区域とに分割される前記メモリの複数の異なる区域に、前記メモリの分離区域に配置され、前記プロセッサの制御の下で実行されるページ・マネージャを使用して、それぞれ分配するステップと、
前記メモリの分離区域に配置されるメモリ所有権ページ・テーブルに前記メモリの各ページを記述するステップと、
を含む方法。
【請求項３】
相互に接続されるプロセッサとメモリとを有するコンピュータに、
複数のページを非分離区域と分離区域とに分割される前記メモリの複数の異なる区域に

、前記メモリの分離区域に配置され、前記プロセッサの制御の下で実行されるページ・マネージャを使用して、それぞれ分配するステップと、
前記メモリの分離区域に配置されるメモリ所有権ページ・テーブルに前記メモリの各ページを記述するステップと、
を有する処理を実行させるコンピュータプログラム。
【請求項４】
チップセットと、
前記チップセットに結合されたメモリと、
前記チップセット及び前記メモリに結合され、通常実行モード及び分離実行モードを有するプロセッサと、
複数のページを非分離区域と分離区域とに分割される前記メモリの複数の異なる区域にそれぞれ分配し、前記メモリの分離区域に配置され、前記プロセッサの制御の下で実行されるページ・マネージャと、
前記メモリの分離区域に配置され、前記メモリの各ページを記述するメモリ所有権ページ・テーブルと、
を含むシステム。
【請求項５】
前記ページ・マネージャは、ページが前記メモリの分離区域に分配されている場合、前記ページに分離属性を割り当てる、請求項１記載の装置。
【請求項６】
前記ページ・マネージャは、前記ページが前記メモリの非分離区域に分配されている場合、前記ページに非分離属性を割り当て、
前記メモリ所有権ページ・テーブルは、各ページに対して前記属性を記録する、請求項５記載の装置。
【請求項７】
通常実行モード及び分離実行モードを有する前記プロセッサによって生成され、アクセス情報を有するアクセス・トランザクションを構成するための構成設定を有する構成ストレージと、
前記構成ストレージに接続され、前記構成設定と前記アクセス情報の少なくとも１つを使用して前記アクセス変換をチェックするアクセス検査回路と、
をさらに有する、請求項６記載の装置。
【請求項８】
前記構成設定は、ページの属性と実行モードワードとを有する、請求項７記載の装置。
【請求項９】
前記メモリの各ページを記述するステップは、ページが前記メモリの分離区域に分配されている場合、前記ページに分離区域を割り当てるステップを有する、請求項２記載の方法。
【請求項１０】
前記メモリの各ページを記述するステップはさらに、
前記ページが前記メモリの非分離区域に分配されている場合、前記ページに非分離属性を割り当てるステップと、
各ページの属性をメモリ所有権ページ・テーブルに記録するステップと、
を有する、請求項９記載の方法。
【請求項１１】
通常実行モード及び分離実行モードを有し、構成設定を有する構成ストレージを有する前記プロセッサによって生成され、アクセス情報を有するアクセス・トランザクションを構成するステップと、
前記構成設定と前記アクセス情報との少なくとも１つを使用して、アクセス検査回路により前記アクセス・トランザクションをチェックするステップと、
を有する、請求項１０記載の方法。

【請求項１２】
前記構成設定は、ページの属性と実行モードワードとを有する、請求項１１記載の方法。

【発明の詳細な説明】
【０００１】
（背景）
（発明の分野）
本発明は、マイクロプロセッサに関する。具体的には、本発明は、プロセッサ・セキュリティに関する。
【０００２】
（関連技術の説明）
マイクロプロセッサ技術および通信技術の進歩によって、従来の取引の形を超えた応用分野の機会が開かれた。電子商取引（Ｅ－ｃｏｍｍｅｒｃｅ）および産業間（Ｂ２Ｂ）トランザクションが、現在、普及しつつあり、常に増加する速度でグローバル・マーケット全体で行われている。残念ながら、現代のマイクロプロセッサ・システムは、ユーザに取引、通信、および取引実行の便利で効率的な方法を提供するが、悪辣な攻撃に対して脆弱でもある。これらの攻撃の例に、たとえば、ウィルス、侵入、セキュリティ・ブリーチ、およびタンパリングが含まれる。したがって、コンピュータ・システムの完全性を保護し、ユーザの信頼を高めるために、コンピュータ・セキュリティがますます重要になりつつある。
【０００３】
悪辣な攻撃によって引き起こされる脅威は、複数の形態である可能性がある。ハッカーによる遠隔起動の侵入的攻撃は、数千または数百万のユーザに接続されたシステムの正常な動作を中断させる可能性がある。ウィルス・プログラムが、単一ユーザ・プラットフォームのコードおよび／またはデータを破壊する可能性がある。
【０００４】
攻撃に対して保護する既存の技法は、多数の短所を有する。アンチウィルス・プログラムは、既知のウィルスだけをスキャンし、検出することができる。暗号または他のセキュリティ技法を使用するセキュリティ・コプロセッサまたはスマート・カードは、速度性能、メモリ容量、および柔軟性に制限を有する。さらに、オペレーティング・システムの再設計によって、ソフトウェア互換性の問題が生じ、開発労力への莫大な投資が必要になる。
【０００５】
本発明の特徴および長所は、本発明の以下の詳細な説明から明らかになる。
【０００６】
（説明）
本発明は、分離実行環境で複数の分離メモリへのメモリ・アクセスを制御する方法、装置、およびシステムである。ページ・マネージャを使用して、複数のページを、それぞれメモリの複数の異なる区域に分配する。メモリは、非分離区域と分離区域に分割される。ページ・マネージャが、メモリの分離区域に配置される。さらに、メモリ所有権ページ・テーブルによって、メモリの各ページが記述され、そのメモリ所有権ページ・テーブルもメモリの分離区域に配置される。ページ・マネージャは、ページがメモリの分離区域に分配される場合に、分離属性をページに割り当てる。その一方で、ページ・マネージャは、ページがメモリの非分離区域に分配される場合に、非分離属性をページに割り当てる。メモリ所有権ページ・テーブルに、各ページの属性が記録される。
【０００７】
一実施形態では、通常実行モードおよび分離実行モードを有するプロセッサが、アクセス・トランザクションを生成する。アクセス・トランザクションは、構成設定を含む構成ストレージを使用して構成される。アクセス・トランザクションには、アクセスされるメモリの物理アドレスなどのアクセス情報が含まれる。構成設定によって、アクセス・トラン

ザクションにかかわるメモリのページに関する情報が提供される。構成設定には、ページを分離または非分離として定義するページに関する属性と、プロセッサが分離実行モードに構成される時にアサートされる実行モード・ワードが含まれる。一実施形態では、実行モード・ワードが、プロセッサが分離実行モードであるかどうかを示す単一のビットである。構成ストレージに結合されたアクセス検査回路が、構成設定およびアクセス情報の少なくとも１つを使用して、アクセス・トランザクションを検査する。

【０００８】

一実施形態では、アクセス検査回路に、ＴＬＢアクセス検査回路が含まれる。ＴＬＢアクセス検査回路は、アクセス・トランザクションが有効である場合に、アクセス許可信号を生成する。具体的に言うと、ページの属性に分離が設定され、実行モード・ワード信号がアサートされる場合に、ＴＬＢアクセス検査回路が、メモリの分離区域へのアクセス許可信号を生成する。したがって、プロセッサがメモリの分離区域の物理アドレスを要求する時に、そのプロセッサが分離実行モードで動作しており、物理アドレスに関連するページの属性に分離がセットされている場合に限って、アクセス・トランザクションが許可される。

【０００９】

以下の説明では、説明のために、本発明の完全な理解を提供するために多数の詳細を示す。しかし、これらの詳細が、本発明を実践するのに必要ではないことを、当業者は諒解するであろう。他の場合には、本発明を不明瞭にしないために、周知の電気構造および電気回路を、ブロック図形式で示す。

【００１０】

アーキテクチャの概要

コンピュータ・システムまたはコンピュータ・プラットフォームでセキュリティを提供するための原理の１つが、分離実行アーキテクチャという概念である。分離実行アーキテクチャには、直接にまたは間接にコンピュータ・システムまたはコンピュータ・プラットフォームのオペレーティング・システムと相互作用するハードウェア構成要素およびソフトウェア構成要素の論理定義および物理定義が含まれる。オペレーティング・システムおよびプロセッサは、さまざまな動作モードに対応する、リングと称する複数レベルの階層を有する場合がある。リングは、オペレーティング・システム内の専用のタスクを実行するように設計された、ハードウェア構成要素およびソフトウェア構成要素の論理的分割である。この分割は、通常は、特権の度合またはレベルすなわち、プラットフォームに対する変更を行う能力に基づく。たとえば、リング０は、最も内側のリングであり、階層の最上位である。リング０には、最もクリティカルな、特権を与えられた構成要素が含まれる。さらに、リング０のモジュールは、より低い特権を与えられたデータにもアクセスすることができるが、逆は成り立たない。リング３は、最も外側のリングであり、階層の最下位である。リング３には、通常は、ユーザまたはアプリケーションのレベルが含まれ、最低の特権を有する。リング１およびリング２は、セキュリティおよび／または保護のレベルが減少する、中間のリングである。

【００１１】

図１Ａは、本発明の一実施形態による論理オペレーティング・アーキテクチャ５０を示す図である。論理オペレーティング・アーキテクチャ５０は、オペレーティング・システムの構成要素およびプロセッサの抽象化である。論理オペレーティング・アーキテクチャ５０には、リング０　１０、リング１　２０、リング２　３０、リング３　４０、およびプロセッサ・ナブ・ローダ５２が含まれる。プロセッサ・ナブ・ローダ５２は、プロセッサ・エグゼクティブ（ＰＥ）ハンドラのインスタンスである。ＰＥハンドラは、後で説明するように、プロセッサ・エグゼクティブ（ＰＥ）の処理および／または管理に使用される。論理オペレーティング・アーキテクチャ５０は、２つの動作モードすなわち、通常実行モードおよび分離実行モードを有する。論理オペレーティング・アーキテクチャ５０内の各リングが、両方のモードで動作することができる。プロセッサ・ナブ・ローダ５２は、分離実行モードのみで動作する。

【００１２】
リング０　１０には、２つの部分すなわち、通常実行リング０　１１および分離実行リング０　１５が含まれる。通常実行リング０　１１には、通常はカーネルと称する、オペレーティング・システムにとってクリティカルなソフトウェア・モジュールが含まれる。このソフトウェア・モジュールには、主オペレーティング・システム（たとえばカーネル）１２、ソフトウェア・ドライバ１３、およびハードウェア・ドライバ１４が含まれる。分離実行リング０　１５には、オペレーティング・システム（ＯＳ）ナブ１６およびプロセッサ・ナブ１８が含まれる。ＯＳナブ１６は、ＯＳエグゼクティブ（ＯＳＥ）のインスタンスであり、プロセッサ・ナブ１８は、プロセッサ・エグゼクティブ（ＰＥ）のインスタンスである。ＯＳＥおよびＰＥは、分離区域および分離実行モードに関連する保護された環境で動作するエグゼクティブ・エンティティの一部である。プロセッサ・ナブ・ローダ５２は、システムのチップセット内に保持される保護されたブートストラップ・ローダ・コードであり、後で説明するように、プロセッサまたはチップセットから分離区域にプロセッサ・ナブ１８をロードする責任を負う。

【００１３】
同様に、リング１　２０、リング２　３０、およびリング３　４０に、それぞれ、通常実行リング１　２１、通常実行リング２　３１、および通常実行リング３　４１と、分離実行リング１　２５、分離実行リング２　３５、および分離実行リング３　４５が含まれる。具体的に言うと、通常実行リング３に、Ｎ個のアプリケーション42_1から42_Nが含まれ、分離実行リング３に、Ｋ個のアプレット46_1から46_Kが含まれる。

【００１４】
分離実行アーキテクチャの概念の１つが、コンピュータ・システム内のプロセッサおよびチップセットの両方によって保護される、分離区域と称するシステム・メモリ内の分離された領域の作成である。分離領域は、アドレス変換バッファ（ＴＬＢ）アクセス検査によって保護される、キャッシュ・メモリ内に置くこともできる。また、下で説明するように、分離領域を複数の分離メモリ区域に副分割することができる。この分離領域へのアクセスは、分離読取サイクルおよび分離書込サイクルと称する特殊なバス（たとえばメモリ読み書き）サイクルを使用して、プロセッサのフロント・サイド・バス（ＦＳＢ）からのみ許可される。特殊なバス・サイクルを、スヌープに使用することもできる。分離読取サイクルおよび分離書込サイクルは、分離実行モードで動作するプロセッサによって発行される。分離実行モードは、プロセッサ・ナブ・ローダ５２と組み合わされた、プロセッサの特権命令を使用して初期化される。プロセッサ・ナブ・ローダ５２は、リング０ナブ・ソフトウェア・モジュール（たとえばプロセッサ・ナブ１８）を検証し、分離区域にロードする。プロセッサ・ナブ１８は、分離実行に関するハードウェア関連のサービスを提供する。

【００１５】
プロセッサ・ナブ１８の作業の１つが、リング０のＯＳナブ１６を検証し、分離区域にロードし、プラットフォーム、プロセッサ・ナブ１８、およびオペレーティング・システム・ナブ１６の組合せに一意の鍵階層のルートを生成することである。プロセッサ・ナブ１８は、オペレーティング・システム・ナブ１６の検証、ロード、およびログ記録を含む分離区域の初期セットアップおよび低水準管理と、オペレーティング・システム・ナブの秘密を保護するのに使用される対称鍵の管理を行う。プロセッサ・ナブ１８は、他のハードウェアによって提供される低水準セキュリティ・サービスへのアプリケーション・プログラミング・インターフェース（ＡＰＩ）抽象化も提供することができる。

【００１６】
オペレーティング・システム・ナブ１６は、主ＯＳ１２（たとえば、オペレーティング・システムの保護されないセグメント）内のサービスへのリンクを提供し、分離区域内のページ管理を提供し、アプレット46_1から46_Kを含むリング３アプリケーション・モジュール４５を、分離区域に割り振られた保護されたページにロードする責任を有する。オペレーティング・システム・ナブ１６は、リング０サポート・モジュールもロードする。

下で説明するように、主ＯＳ１２は、分離区域の外のページを管理する。

【００１７】

オペレーティング・システム・ナブ１６は、分離区域と普通の（たとえば非分離）区域との間のデータのページングをサポートすることを選択することができる。そうである場合には、オペレーティング・システム・ナブ１６は、ページを普通のメモリに追い出す前に分離区域ページを暗号化し、ハッシュし、ページの復元の際にページ内容を検査する責任も負う。分離モードのアプレット46_1から46_Kおよびこれらのデータは、他のアプレットならびに、非分離空間アプリケーション（たとえば42_1から42_N）、ダイナミック・リンク・ライブラリ（ＤＬＬ）、ドライバ、および主オペレーティング・システム１２だけからのすべてのソフトウェア攻撃に対して抗タンパであり、抗モニタである。プロセッサ・ナブ１８またはオペレーティング・システム・ナブ１６だけは、アプレットの実行に干渉するかアプレットの実行を監視することができる。

【００１８】

図１Ｂは、本発明の一実施形態による、オペレーティング・システム内のさまざまな要素１０およびプロセッサのアクセス可能性を示す図である。例示のために、リング０　１０およびリング３　４０の要素だけを図示する。論理オペレーティング・アーキテクチャ５０のさまざまな要素が、そのリング階層および実行モードに従って、アクセス可能物理メモリ６０にアクセスする。

【００１９】

アクセス可能物理メモリ６０には、分離区域７０と非分離区域８０が含まれる。分離区域７０には、アプレット・ページ７２とナブ・ページ７４が含まれる。非分離区域８０には、アプリケーション・ページ８２とオペレーティング・システム・ページ８４が含まれる。分離区域７０は、分離実行モードで動作する、オペレーティング・システムの要素およびプロセッサだけからアクセス可能である。非分離区域８０は、リング０オペレーティング・システムのすべての要素およびプロセッサからアクセス可能である。

【００２０】

主ＯＳ１２、ソフトウェア・ドライバ１３、およびハードウェア・ドライバ１４を含む通常実行リング０　１１は、ＯＳページ８４およびアプリケーション・ページ８２の両方にアクセスすることができる。アプリケーション42_1から42_Nを含む通常実行リング３は、アプリケーション・ページ８２だけにアクセスすることができる。しかし、通常実行リング０　１１と通常実行リング３　４１の両方が、分離区域７０にアクセスできない。

【００２１】

ＯＳナブ１６およびプロセッサ・ナブ１８を含む分離実行リング０　１５は、アプレット・ページ７２およびナブ・ページ７４を含む分離区域７０と、アプリケーション・ページ８２およびＯＳページ８４を含む非分離区域８０の両方にアクセスすることができる。アプレット46_1から46_Kを含む分離実行リング３　４５は、アプリケーション・ページ８２およびアプレット・ページ７２だけにアクセスすることができる。アプレット46_1から46_Kは、分離区域７０に常駐する。

【００２２】

図１Ｃは、本発明の一実施形態による、分離メモリ区域７０が複数の分離メモリ区域７１に分割され、非分離メモリ区域８０が複数の非分離メモリ区域８３に分割される、オペレーティング・システム内のさまざまな要素およびプロセッサを示す、図１Ｂに類似する図である。例示のために、リング０　１０およびリング３　４０の要素だけを図示する。論理オペレーティング・アーキテクチャ５０のさまざまな要素が、そのリング階層および実行モードに従ってアクセス可能物理メモリ６０にアクセスする。アクセス可能物理メモリ６０には、複数の分離区域７１と複数の非分離区域８３が含まれる。

【００２３】

複数の分離区域７１には、アプレット・ページ７２およびオペレーティング・システム（ＯＳ）ナブ・ページ７４が含まれる。複数の分離区域７１の１つに、プロセッサ・ナブ・ページ７３に埋め込まれるプロセッサ・ナブ１８（すなわちプロセッサ・エグゼクティブ

（ＰＥ））も含まれる。複数の非分離区域８３には、アプリケーション・ページ８２とオペレーティング・システム（ＯＳ）ページ８４が含まれる。複数の分離区域７１は、分離実行モードで動作する、オペレーティング・システムの要素およびプロセッサだけからアクセス可能である。非分離区域８３は、リング０のオペレーティング・システムの要素のすべておよびプロセッサからアクセス可能である。

【００２４】

図１Ｃに示されたこの実施形態では、図１Ｂに示された単一ブロックの分離メモリ区域７０とは異なって、分離メモリ区域７０が、複数の分離メモリ区域７１に分割され、分離メモリを使用する際の高められたプラットフォーム機能性が可能になる。複数の分離メモリ区域７１をサポートするために、ＯＳナブ・ページ７４に埋め込まれるＯＳナブ１６（すなわちＯＳエグゼクティブ（ＯＳＥ））に、ページ・マネージャ７５とメモリ所有権ページ・テーブル７７が含まれる。ＯＳナブは、ページ・マネージャ７５を制御する。ページ・マネージャ７５は、ＯＳナブ・ページ７４およびアプレット・ページ７２などの複数の分離メモリ区域７１と、ＯＳページ８４およびアプリケーション・ページ８２などの非分離メモリ区域８３にページを分配する責任を負う。ページ・マネージャ７５は、メモリ所有権ページ・テーブル７７も管理し、維持する。後で説明するように、メモリ所有権ページ・テーブル７７によって、各ページが記述され、メモリ所有権ページ・テーブル７７は、プロセッサによるアクセス・トランザクションの構成を助け、さらに、アクセス・トランザクションが有効であることを検証するのに使用される。ページ・マネージャ７５が、複数の分離メモリ区域７１および複数の非分離メモリ区域８３を作成できるようにすることによって、アクセス可能物理メモリ６０が、システム・メモリ要件の変更に容易に対処できるようになる。

【００２５】

主ＯＳ１２、ソフトウェア・ドライバ１３、およびハードウェア・ドライバ１４を含む通常実行リング０　１１は、ＯＳページ８４とアプリケーション・ページ８２の両方にアクセスすることができる。アプリケーション４２_{1}から４２_{N}を含む通常実行リング３は、アプリケーション・ページ８２だけにアクセスすることができる。しかし、通常実行リング０　１１および通常実行リング３　４１の両方が、複数の分離メモリ区域７１にアクセスすることができない。

【００２６】

ＯＳナブ１６およびプロセッサ・ナブ１８を含む分離実行リング０　１５は、アプレット・ページ７２およびＯＳナブ・ページ７４を含む複数の分離メモリ区域７１と、アプリケーション・ページ８２およびＯＳページ８４を含む複数の非分離メモリ区域８３の両方にアクセスすることができる。アプレット４６_{1}から４６_{K}を含む分離実行リング３　４５は、アプリケーション・ページ８２およびアプレット・ページ７２だけにアクセスすることができる。アプレット４６_{1}から４６_{K}は、複数の分離メモリ区域７１に常駐する。

【００２７】

図１Ｄは、本発明の一実施形態による、分離実行のためにメモリのページを分配する処理８６を示す流れ図である。

【００２８】

開始時に、処理８６では、メモリのページを、それぞれアクセス可能物理メモリ６０の異なる区域に分配する（ブロック８７）。ページは、分離区域７１と非分離区域８３の両方に分配される。好ましい実施形態では、ページのサイズが固定される。たとえば、各ページを、４ＭＢまたは４ＫＢとすることができる。次に、処理８６では、各ページに属性を割り当てる（ブロック８８）。処理８６では、ページがメモリの分離区域に分配される場合に分離属性をページに割り当て、ページがメモリの非分離区域に分配される場合に非分離属性をページに割り当てる。その後、処理８６が終了する。

【００２９】

図１Ｅは、本発明の一実施形態による、メモリ所有権ページ・テーブル７７と、仮想アドレスを物理アドレスに変換する処理を示す図である。前に述べたように、ページ・マネー

ジャ７５が、メモリ所有権ページ・テーブル７７を管理する。メモリ所有権ページ・テーブル７７には、複数のページ・テーブル・エントリ９３が含まれる。各ページ・テーブル・エントリ９３に、下記の構成要素が含まれる：ページのベース９５およびページの属性９６（分離または非分離）。ページ・マネージャ７５だけが、ページに割り当てられる属性９６を変更することができる。各ページ９８に、複数の物理アドレス９９が含まれる。ページ・マネージャ７５は、分離メモリ区域および非分離メモリ区域が変更される時に、メモリ所有権ページ・テーブル７７をフラッシュするか、ページ・テーブル・エントリ９３を無効化する。その後、ページ・マネージャ７５が、分離メモリ区域および非分離メモリ区域を再割り当てし、初期化する。

【００３０】

仮想アドレス２１２に、ページ・テーブル・コンポーネント９１とオフセット９２が含まれる。仮想アドレス２１２を物理アドレス９９に変換する処理を、下で説明する。

【００３１】

図１Ｆは、本発明の一実施形態を実践することができるコンピュータ・システム１００を示す図である。コンピュータ・システム１００には、プロセッサ１１０、ホスト・バス１２０、メモリ・コントローラ・ハブ（ＭＣＨ）１３０、システム・メモリ１４０、入出力コントローラ・ハブ（ＩＣＨ）１５０、不揮発性メモリまたはシステム・フラッシュ１６０、大容量記憶デバイス１７０、入出力デバイス１７５、トークン・バス１８０、マザーボード（ＭＢ）トークン１８２、リーダ１８４、およびトークン１８６が含まれる。ＭＣＨ１３０は、分離実行モード、ホスト－周辺バス・インターフェース、メモリ制御などの複数の機能性を統合したチップセットに統合することができる。同様に、ＩＣＨ１５０も、入出力機能を実行するために、ＭＣＨ１３０と一緒にまたは別々にチップセットに統合することができる。説明を明瞭にするために、周辺バスのすべてが図示されているわけではない。システム１００に、Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ（ＰＣＩ）、ａｃｃｅｌｅｒａｔｅｄ ｇｒａｐｈｉｃｓ ｐｏｒｔ（ＡＧＰ）、Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ（ＩＳＡ）バス、およびＵｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ（ＵＳＢ）などの周辺バスも含めることができることが企図されている。

【００３２】

プロセッサ１１０は、複合命令セット・コンピュータ（ＣＩＳＣ）、縮小命令セット・コンピュータ（ＲＩＳＣ）、ｖｅｒｙ ｌｏｎｇ ｉｎｓｔｒｕｃｔｉｏｎ ｗｏｒｄ（ＶＬＩＷ）、またはハイブリッド・アーキテクチャなど、すべてのタイプのアーキテクチャの中央処理装置を表す。一実施形態では、プロセッサ１１０が、Ｐｅｎｔｉｕｍ（登録商標）シリーズ、ＩＡ－３２（商標）、およびＩＡ－６４（商標）などのインテル・アーキテクチャ（ＩＡ）プロセッサとの互換性を有する。プロセッサ１１０には、通常実行モード１１２および分離実行回路１１５が含まれる。通常実行モード１１２は、プロセッサ１１０が非保護環境または分離実行モジュールによって提供されるセキュリティ機能がない普通の環境で動作するモードである。分離実行回路１１５は、プロセッサ１１０が分離実行モードで動作できるようにする機構を提供する。分離実行回路１１５は、分離実行モード用のハードウェア・サポートおよびソフトウェア・サポートを提供する。このサポートには、分離実行の構成、１つまたは複数の分離区域の定義、分離命令の定義（たとえばデコードおよび実行）、分離アクセス・バス・サイクルの生成、および分離モード割込みの生成が含まれる。

【００３３】

一実施形態では、コンピュータ・システム１００を、たとえばプロセッサ１１０などの１つの主中央制御装置だけを有する、デスクトップ・コンピュータなどの単一の処理システムとすることができる。他の実施形態では、コンピュータ・システム１００に、図１Ｆに示されたものなど、たとえばプロセッサ１１０、１１０ａ、１１０ｂなどの複数のプロセッサを含めることができる。したがって、コンピュータ・システム１００は、任意の数のプロセッサを有するマルチプロセッサ・コンピュータ・システムとすることができる。た

とえば、マルチプロセッサのコンピュータ・システム１００は、サーバまたはワークステーション環境の一部として動作することができる。プロセッサ１１０の基本的な説明およびオペレーションを、下で詳細に説明する。プロセッサ１１０の基本的な説明およびオペレーションが、図１Ｆに示された他のプロセッサ１１０ａおよび１１０ｂ、ならびに、本発明の一実施形態に従ってマルチプロセッサ・コンピュータ・システム１００内で使用することができる任意の数の他のプロセッサに適用されることを、当業者は諒解するであろう。

【００３４】

プロセッサ１１０は、複数の論理プロセッサを有することもできる。時々スレッドとも称する論理プロセッサは、ある区分ポリシに従って割り振られるアーキテクチャ的状態および物理リソースを有する、物理プロセッサ内の機能単位である。本発明の文脈では、用語「スレッド」および「論理プロセッサ」が、同一のことを意味するのに使用される。マルチスレッド・プロセッサは、複数のスレッドまたは複数の論理プロセッサを有するプロセッサである。マルチプロセッサ・システム（たとえばプロセッサ１１０、１１０ａ、１１０ｂを含むシステム）は、複数のマルチスレッド・プロセッサを有することができる。

【００３５】

ホスト・バス１２０は、プロセッサ１１０またはプロセッサ１１０、１１０ａ、および１１０ｂが、他のプロセッサまたはデバイス、たとえばＭＣＨ１３０と通信できるようにするインターフェース信号を提供する。通常モードの外に、ホスト・バス１２０は、プロセッサ１１０が分離実行モードで構成される時にメモリ読取サイクルおよびメモリ書込サイクルに関する対応するインターフェース信号を有する分離アクセス・バス・モードを提供する。分離アクセス・バス・モードは、プロセッサ１１０が分離実行モードである間に開始されるメモリ・アクセスの際にアサートされる。分離アクセス・バス・モードは、命令プリフェッチ・サイクルおよびキャッシュ・ライトバック・サイクルに、アドレスが分離区域アドレス範囲内であり、プロセッサ１１０が分離実行モードで初期化される場合にもアサートされる。プロセッサ１１０は、分離アクセス・バス・サイクルがアサートされ、プロセッサ１１０が分離実行モードに初期化される場合に、分離区域アドレス範囲内のキャッシングされるアドレスへのスヌープ・サイクルに応答する。

【００３６】

ＭＣＨ１３０は、システム・メモリ１４０およびＩＣＨ１５０などのメモリおよび入出力デバイスの制御および構成を提供する。ＭＣＨ１３０は、分離メモリ読取サイクルおよび分離メモリ書込サイクルを含む、メモリ参照バス・サイクルでの分離アクセス・アサートを認識し、サービスするインターフェース回路を提供する。さらに、ＭＣＨ１３０は、システム・メモリ１４０内の１つまたは複数の分離区域を表すメモリ範囲レジスタ（たとえばベース・レジスタおよび長さレジスタ）を有する。構成された後に、ＭＣＨ１３０は、分離アクセス・バス・モードをアサートされていない、分離区域へのアクセスのすべてを打ち切る。

【００３７】

システム・メモリ１４０には、システム・コードおよびデータが格納される。システム・メモリ１４０は、通常は、ダイナミック・ランダム・アクセス・メモリ（ＤＲＡＭ）またはスタティック・ランダム・アクセス・メモリ（ＳＲＡＭ）を用いて実装される。システム・メモリ１４０には、アクセス可能物理メモリ６０（図１Ｂおよび１Ｃに図示）が含まれる。アクセス可能物理メモリには、ロードされたオペレーティング・システム１４２、分離区域７０（図１Ｂ）または分離区域７１（図１Ｃ）、および分離制御および状況空間１４８が含まれる。ロードされたオペレーティング・システム１４２は、オペレーティング・システムのうちでシステム・メモリ１４０にロードされた部分である。ロードされたＯＳ１４２は、通常は、ブート読取専用メモリ（ＲＯＭ）などのブート・ストレージ内のブート・コードを介して大容量記憶デバイスからロードされる。分離区域７０（図１Ｂ）または分離区域７１（図１Ｃ）は、分離実行モードで動作する時のプロセッサ１１０によって定義されるメモリ区域である。分離区域へのアクセスは、プロセッサ１１０および／

またはＭＣＨ１３０もしくは分離区域機能性を統合する他のチップセットによって、制限され、実施される。分離制御および状況空間１４８は、プロセッサ１１０および／またはＭＣＨ１３０によって定義される、入出力風の、独立のアドレス空間である。分離制御および状況空間１４８には、主に、分離実行制御および状況レジスタが含まれる。分離制御および状況空間１４８は、既存のアドレス空間とオーバーラップせず、分離バス・サイクルを使用してアクセスされる。システム・メモリ１４０に、図示されていない他のプログラムまたはデータを含めることもできる。

【００３８】

ＩＣＨ１５０は、分離実行モード機能性を有するシステム内の既知の単一の点を表す。説明を明瞭にするために、１つのＩＣＨ１５０だけを図示する。システム１００は、ＩＣＨ１５０に類似する多数のＩＣＨを有することができる。複数のＩＣＨがある時に、指定されたＩＣＨが、分離区域の構成および状況を制御するために選択される。一実施形態では、この選択が、外部ストラッピング・ピンによって実行される。当業者に既知のように、プログラマブル構成レジスタの使用を含む、他の選択方法を使用することができる。ＩＣＨ１５０は、従来の入出力機能に加えて、分離実行モードをサポートするために設計された複数の機能性を有する。具体的に言うと、ＩＣＨ１５０には、分離バス・サイクル・インターフェース１５２、プロセッサ・ナブ・ローダ５２（図１Ａに図示）、ダイジェスト・メモリ１５４、暗号鍵ストレージ１５５、分離実行論理処理マネージャ１５６、およびトークン・バス・インターフェース１５９が含まれる。

【００３９】

分離バス・サイクル・インターフェース１５２には、分離読取バス・サイクルおよび分離書込バス・サイクルなどの分離バス・サイクルを認識し、サービスするために分離バス・サイクル信号にインターフェースする回路が含まれる。図１Ａに示されたプロセッサ・ナブ・ローダ５２には、プロセッサ・ナブ・ローダ・コードとそのダイジェスト（たとえばハッシュ）値が含まれる。プロセッサ・ナブ・ローダ５２は、割り当てられた分離命令（たとえばＩｓｏ－Ｉｎｉｔ）の実行によって呼び出され、分離区域７０または分離区域７１の１つに転送される。分離区域から、プロセッサ・ナブ・ローダ５２が、プロセッサ・ナブ１８をシステム・フラッシュ（たとえば不揮発性メモリ１６０内のプロセッサ・ナブ１８）から分離区域７０にコピーし、その保全性を検証し、ログ記録し、プロセッサ・ナブの秘密を保護するのに使用される対称鍵を管理する。一実施形態では、プロセッサ・ナブ・ローダ５２が、読取専用メモリ（ＲＯＭ）内に実装される。セキュリティのために、プロセッサ・ナブ・ローダ５２は、変更されず、抗タンパであり、置換不能である。通常はＲＡＭ内に実装されるダイジェスト・メモリ１５４には、プロセッサ・ナブ１８の、オペレーティング・システム・ナブ１６の、および分離実行空間にロードされた他のクリティカル・モジュール（たとえばリング０モジュール）の、ダイジェスト（たとえばハッシュ）値が格納される。

【００４０】

暗号鍵ストレージ１５５には、システム１００のプラットフォームについて一意の対象暗号化／復号鍵が保持される。一実施形態では、暗号鍵ストレージ１５５に、製造時にプログラムされる内部ヒューズが含まれる。代替案では、暗号鍵ストレージ１５５を、乱数ジェネレータおよびピンのストラップを用いて作成することもできる。分離実行論理処理マネージャ１５６は、分離実行モードで動作する論理プロセッサのオペレーションを管理する。一実施形態では、分離実行論理処理マネージャ１５６に、分離実行モードに参加する論理プロセッサの数を追跡する論理プロセッサ・カウント・レジスタが含まれる。トークン・バス・インターフェース１５９は、トークン・バス１８０にインターフェースする。プロセッサ・ナブ・ローダ・ダイジェスト、プロセッサ・ナブ・ダイジェスト、オペレーティング・システム・ナブ・ダイジェスト、および任意選択の追加のダイジェストの組合せによって、分離ダイジェストと称する、包括的な分離実行ダイジェストが表される。分離ダイジェストは、分離実行の構成およびオペレーションを制御するリング０コードを識別する指紋である。分離ダイジェストは、現在の分離実行の状態を証明または立証するの

に使用される。

【００４１】

不揮発性メモリ１６０には不揮発性情報が格納される。通常、不揮発性メモリ１６０は、フラッシュ・メモリで実装される。不揮発性メモリ１６０には、プロセッサ・ナブ１８が含まれる。

【００４２】

プロセッサ・ナブ１８は、オペレーティング・システム・ナブ１６の検証、ロード、およびログ記録を含む分離区域（システム・メモリ１４０内）の初期セットアップおよび低水準管理と、オペレーティング・システム・ナブの秘密を保護するのに使用される対称鍵の管理を行う。プロセッサ・ナブ１８は、他のハードウェアによって提供される低水準セキュリティ・サービスへのアプリケーション・プログラミング・インターフェース（ＡＰＩ）抽象化を提供することもできる。プロセッサ・ナブ１８は、相手先商標製造会社（ＯＥＭ）またはオペレーティング・システム・ベンダ（ＯＳＶ）によって、ブート・ディスクを介して配布することもできる。

【００４３】

大容量記憶デバイス１７０には、コード（たとえばプロセッサ・ナブ１８）、プログラム、ファイル、データ、アプリケーション（たとえばアプリケーション42_1から42_N）、アプレット（たとえばアプレット46_1から46_K）、およびオペレーティング・システムなどのアーカイブ情報が格納される。大容量記憶デバイス１７０に、コンパクト・ディスク（ＣＤ）ＲＯＭ１７２、フロッピ・ディスケット１７４、ハード・ドライブ１７６、および他の磁気記憶デバイスまたは光学記憶デバイスを含めることができる。大容量記憶デバイス１７０は、機械可読媒体を読み取る機構を備えている。

【００４４】

入出力デバイス１７５には、入出力機能を実行するすべての入出力デバイスを含めることができる。入出力デバイス１７５の例には、入力デバイス（たとえば、キーボード、マウス、トラックボール、ポインティング・デバイス）のコントローラ、メディア・カード（たとえば、オーディオ、ビデオ、グラフィックス）、ネットワーク・カード、および他の周辺コントローラが含まれる。

【００４５】

トークン・バス１８０は、ＩＣＨ１５０とシステム内のさまざまなトークンの間のインターフェースを提供する。トークンとは、セキュリティ機能性を伴う専用の入出力機能を実行するデバイスである。トークンは、少なくとも１つの目的を予約された秘密鍵／公開鍵対と秘密鍵を用いてデータに署名する能力を含むスマート・カードに類似する特性を有する。トークン・バス１８０に接続されるトークンの例には、マザーボード・トークン１８２、トークン・リーダ１８４、および他のポータブル・トークン１８６（たとえばスマート・カード）が含まれる。ＩＣＨ１５０内のトークン・バス・インターフェース１５９は、トークン・バス１８０を介してＩＣＨ１５０に接続され、分離実行の状態を証明するように指令された時に、対応するトークン（たとえばマザーボード・トークン１８２、トークン１８６）が、有効な分離ダイジェスト情報だけに署名するようにする。セキュリティのために、トークンは、ダイジェスト・メモリに接続されなければならない。

【００４６】

ソフトウェアで実施される時に、本発明の要素は、必要な作業を実行するコード・セグメントである。プログラム・セグメントまたはコード・セグメントは、プロセッサ可読媒体などの機械可読媒体に格納されるか、伝送媒体を介して、搬送波に組み込まれたコンピュータ・データ信号または搬送波によって変調される信号によって伝送される。「プロセッサ可読媒体」には、情報を格納するか転送することができるすべての媒体を含めることができる。プロセッサ可読媒体の例には、電子回路、半導体メモリ・デバイス、ＲＯＭ、フラッシュ・メモリ、消去可能プログラマブルＲＯＭ（ＥＰＲＯＭ）、フロッピ・ディスケット、コンパクト・ディスクＲＯＭ（ＣＤ－ＲＯＭ）、光ディスク、ハード・ディスク、光ファイバ媒体、無線（ＲＦ）リンク、などが含まれる。コンピュータ・データ信号には

、電子ネットワーク・チャネル、光ファイバ、空気、電磁気、ＲＦリンクなどの伝送媒体を介して伝播することができるすべての信号を含めることができる。コード・セグメントを、インターネット、イントラネットなどのコンピュータ・ネットワークを介してダウンロードすることができる。

【００４７】

分離実行環境での複数の分離メモリへのアクセスの制御

本発明は、分離実行環境で、図１Ｃに示された複数の分離メモリ７１へのメモリ・アクセスを制御する方法、装置、およびシステムである。図２Ａは、本発明の一実施形態による、図１Ｆに示された分離実行回路１１５を示す図である。分離実行回路１１５には、コア実行回路２０５、アクセス・マネージャ２２０、およびキャッシュ・メモリ・マネージャ２３０が含まれる。

【００４８】

コア実行ユニット２０５には、命令デコーダおよび実行ユニット２１０とアドレス変換バッファ（ＴＬＢ）２１８が含まれる。命令デコーダおよび実行ユニット２１０は、命令フェッチ・ユニットから命令ストリーム２１５を受け取る。命令ストリーム２１５には、複数の命令が含まれる。命令デコーダおよび実行ユニット２１０は、命令をデコードし、デコードされた命令を実行する。これらの命令は、マイクロレベルまたはマクロレベルとすることができる。命令デコーダおよび実行ユニット２１０は、物理回路とするか、命令のデコードおよび実行の処理の抽象化とすることができる。さらに、命令に、分離命令と非分離命令を含めることができる。命令デコーダおよび実行ユニット２１０は、アクセス・トランザクションがある時に、仮想アドレス２１２を生成する。

【００４９】

ＴＬＢ２１８によって、仮想アドレス２１２が物理アドレス９９に変換される。ＴＬＢ２１８には、メモリ所有権ページ・テーブル（ＭＯＰＴ）７７のキャッシュ２１９が含まれる。ＴＬＢ２１８では、まず、キャッシュ２１９を調べて、仮想アドレス２１２と一致する物理アドレスおよび関連するページ・テーブル・エントリを見つける。物理アドレスがキャッシュ２１９内にない場合には、ＴＬＢ２１８では、ＭＯＰＴ７７自体を検索する。ＴＬＢ２１８では、ＭＯＰＴのベース２２１を使用して、物理アドレスを検索する。図１Ｅを参照すると、ＭＯＰＴのベース２２１および仮想アドレス２１２のページ・テーブル・コンポーネント９１から開始して、ＴＬＢ２１８では、仮想アドレス２１２のページ・テーブル・エントリ９３を見つける。前に述べたように、各ページ・テーブル・エントリ９３に、ページのベース９５およびページの属性９６（分離または非分離）が含まれる。仮想アドレスのページのベース９５およびオフセット構成要素９２を使用して、ＴＬＢ２１８で、仮想アドレスに対応する物理アドレス９９を見つけることができる。ＴＬＢを使用する物理アドレスへの仮想アドレスの変換が、当技術分野で周知であることを諒解されたい。後で説明するように、ページの属性９６（分離または非分離）は、分離実行のためにアクセス・トランザクションを構成する際に重要である。

【００５０】

図２Ａを参照すると、コア実行ユニット２０５は、制御／状況情報２２２、オペランド２２４、およびアクセス情報２２６を介して、アクセス・マネージャ２２０とインターフェースする。制御／状況情報２２２には、分離バス・サイクル・ジェネレータ２２０のさまざまな要素を操作する制御ビットおよびアクセス・マネージャ２２０からの状況データが含まれる。オペランド２２４には、アクセス・マネージャ２２０との間で読み書きされるデータが含まれる。アクセス情報２２６には、アドレス情報（たとえば、ＴＬＢ２１８によって供給される物理アドレス）、読取／書込、およびアクセス・タイプの情報が含まれる。

【００５１】

アクセス・マネージャ２２０は、命令実行の結果としてコア実行ユニット２０５から、制御／状況情報２２２を受け取り、供給し、オペランド２２４情報を受け取り、供給し、アクセス情報２２６を受け取り、キャッシュ・メモリ・マネージャ２３０からキャッシュ・

アクセス信号２３５（たとえばキャッシュ・ヒット）および属性９６（分離または非分離）を受け取る。アクセス・マネージャ２２０は、システム内の別のプロセッサから、外部分離アクセス信号２７８およびフロント・サイド・バス（ＦＳＢ）アドレス情報信号２２８も受け取る。外部分離アクセス信号２７８は、システム内の別のプロセッサが分離メモリ区域の１つへのアクセスを試みる時にアサートされる。アクセス・マネージャ２２０は、分離アクセス信号２７２、アクセス許可信号２７４、およびプロセッサ・スヌープ・アクセス信号２７６を生成する。分離アクセス信号２７２は、プロセッサ１１０が分離モード命令を実行していることを示すためにプロセッサ１１０の外部のデバイス（たとえばチップセット）に送られる分離バス・サイクル２３０を生成するのに使用することができる。プロセッサ・スヌープ・アクセス信号２７６は、スヌープ・アクセスがヒットまたはミスのどちらであるかを判定するために、他のデバイスまたはチップセットが使用することができる。分離アクセス信号２７２、アクセス許可信号２７４、およびプロセッサ・スヌープ・アクセス信号２７６は、他の分離アクティビティまたは非分離アクティビティを制御し、監視するために、プロセッサ１１０によって内部的にも使用することができる。

【００５２】

キャッシュ・メモリ・マネージャ２３０は、コア実行ユニット２０５からアクセス情報２２６を受け取り、アクセス・マネージャ２２０へのキャッシュ・アクセス信号２３５を生成する。キャッシュ・メモリ・マネージャ２３０には、当業者に既知のように、キャッシュ情報を格納するキャッシュ・メモリ２３２およびキャッシュ・トランザクションを管理する他の回路が含まれる。キャッシュ・アクセス信号２３５によって、キャッシュ・アクセスの結果が示される。一実施形態では、キャッシュ・アクセス信号２３５が、キャッシュ・アクセスからのキャッシュ・ヒットがある時にアサートされるキャッシュ・ヒット信号である。

【００５３】

図２Ｂは、本発明の一実施形態による、図２Ａに示されたアクセス・マネージャを示す図である。アクセス・マネージャ２２０には、構成ストレージ２５０およびアクセス検査回路２７０が含まれる。アクセス・マネージャ２２０は、図２Ａに示されたコア実行ユニット２０５とオペランド２２４情報を交換し、コア実行ユニット２０５からアクセス情報２２６を受け取る。オペランド２２４情報には、物理アドレス９９に関連するページの属性９６（分離または非分離）が含まれる。アクセス・マネージャ２２０は、図２Ａに示されているように、キャッシュ・マネージャ２３０からキャッシュ・アクセス信号２３５を受け取り、別のプロセッサから外部分離アクセス信号２７８およびＦＳＢアドレス情報２２８を受け取る。アクセス・マネージャ２２０は、さらに、キャッシュ・マネージャ２３０から属性９６（分離または非分離）を受け取る。属性は、キャッシュ・ラインごとである。アクセス情報２２６には、物理アドレス９９、読取／書込（ＲＤ／ＷＲ＃）信号２８４、およびアクセス・タイプ２８６が含まれる。アクセス情報２２６は、プロセッサ１１０によるアクセス・トランザクション中に生成される。アクセス・タイプ２８６によって、メモリ参照、入出力参照、および論理プロセッサ・アクセスを含むアクセスのタイプが示される。論理プロセッサ・アクセスには、分離されたイネーブルされた状態への論理プロセッサ進入(entry)と、分離されたイネーブルされた状態からの論理プロセッサ離脱(withdrawal)が含まれる。

【００５４】

構成ストレージ２５０には、プロセッサ１１０によって生成されるアクセス・トランザクションを構成するための構成パラメータが含まれる。プロセッサ１１０は、通常実行モードと分離実行モードを有する。アクセス・トランザクションは、アクセス情報を有する。構成ストレージ２５０は、命令デコーダおよび実行ユニット２１０（図２Ａ）からオペランド２２４情報を受け取る。構成ストレージ２５０には、ページの属性レジスタ２５１およびプロセッサ制御レジスタ２５２が含まれる。属性レジスタ２５１には、分離または非分離のいずれかがセットされる、物理アドレスに関連するページの属性９６が含まれる。プロセッサ制御レジスタ２５２には、実行モード・ワード２５３が含まれる。実行モード

・ワード２５３は、プロセッサ１１０が分離実行モードに構成される時にアサートされる。一実施形態では、実行モード・ワード２５３は、プロセッサ１１０が分離実行モードであるかどうかを示す単一のビットである。

【００５５】

アクセス検査回路２７０は、構成パラメータ（たとえば実行モード・ワード２５３および属性９６）およびアクセス情報２２６の少なくとも１つを使用して、アクセス・トランザクションを検査する。アクセス検査回路２７０は、構成ストレージ２５０内のパラメータ、プロセッサ１１０によって生成されるトランザクション内のアクセス情報２２６、およびＦＳＢアドレス情報２２８の少なくとも１つを使用して、プロセッサ分離アクセス信号２７２、アクセス許可信号２７４、およびプロセッサ・スヌープ・アクセス信号２７６を生成する。ＦＳＢアドレス情報２２８は、通常は、別のプロセッサによって供給され、ＦＳＢ上でスヌープされる。分離アクセス信号２７２は、プロセッサ１１０が分離実行モードに構成される時にアサートされる。アクセス許可信号２７４は、アクセスが許可されたことを示すのに使用される。プロセッサ・スヌープ・アクセス信号２７６は、別のプロセッサからのアクセスがヒットまたはミスのどちらをもたらしたかを判定するのに使用される。

【００５６】

図３Ａは、本発明の一実施形態による、アクセス検査回路２７０を示す図である。アクセス検査回路２７０には、ＴＬＢアクセス検査回路３１０と、ＦＳＢスヌープ検査回路３３０が含まれる。

【００５７】

ＴＬＢアクセス検査回路３１０は、属性９６および実行モード・ワード２５３を受け取って、アクセス許可信号２７４を生成する。分離区域へのアクセス許可信号２７４は、属性９６に分離がセットされ、実行モード・ワード２５３がアサートされ、分離アクセスが有効であるか構成に従って許可されることが示される時にアサートされる。一実施形態では、ＴＬＢアクセス検査回路３１０が、論理「排他ＮＯＲ」オペレーションを実行する。したがって、プロセッサが、分離区域の物理アドレスを要求する時に、そのプロセッサが分離実行モードで動作しており、物理アドレスに関連するページの属性に分離がセットされている場合に限って、アクセス・トランザクションが許可される。

【００５８】

ＦＳＢスヌープ検査回路３３０は、ＴＬＢアクセス検査回路３１０に似た機能を実行する。ＦＳＢスヌープ検査回路３３０は、キャッシュ・アクセス信号２３５、外部分離アクセス信号２７８、および属性９６を組み合わせることによって、プロセッサ・スヌープ・アクセス信号２７６を生成する。ＦＳＢスヌープ検査回路３３０には、第１コンバイナ３４２および第２コンバイナ３４４が含まれる。第１コンバイナ３４２は、スヌープされるラインの属性９６（分離または非分離）をキャッシュ・マネージャ２３０から受け取り、スヌープを行う別のプロセッサから外部分離アクセス信号２７８を受け取る。属性は、キャッシュ・ラインごとである。一実施形態では、第１コンバイナ３４２が、論理「排他ＮＯＲ」オペレーションを実行する。第２コンバイナ３４４は、第１コンバイナ３４２の結果をキャッシュ・アクセス信号２３５（たとえばキャッシュ・ヒット）と組み合わせる。一実施形態では、第２コンバイナ３４４が、論理ＡＮＤオペレーションを実行する。したがって、プロセッサは、スヌープするプロセッサが分離実行モードで動作しており、ページの属性に分離がセットされ、キャッシュ・ヒットがある時に限って、分離区域について別のプロセッサからのラインをスヌープすることができる。これらの条件が満たされる時に限って、アクセス・トランザクションが許可され、プロセッサ・スヌープ・アクセス信号２７６が、分離区域について生成される。

【００５９】

ＦＳＢスヌープ検査回路３３０によって、すべてのプロセッサが分離メモリ区域アクセスのために初期化されているのではない時に、マルチプロセッサ・システムの正しい機能性が保証される。Ｘ－ＮＯＲ要素３４２によって、スヌープ・ヒットが、分離アクセスのた

めに割り振られたプロセッサからのみ発生することが保証される。あるプロセッサが、分離メモリ区域アクセスにまだ参加していない場合に、そのプロセッサは、分離メモリ区域アクセスに参加している別のプロセッサからラインをスヌープすることができない。同様に、分離アクセスについてイネーブルされているプロセッサは、まだイネーブルされていない別のプロセッサからのラインを偶然にスヌープはしない。

【００６０】

キャッシュ・アクセス信号２３５がアサートされてキャッシュ・ヒットがあることが示され、外部分離アクセス信号２７８がアサートされ、属性９６に分離がセットされている時に、分離区域に関するプロセッサ・スヌープ・アクセス信号２７６がアサートされ、アクセス・ヒットがあることが示される。

【００６１】

図３Ｂは、本発明のもう１つの実施形態による、プロセス論理プロセッサ・オペレーションを管理するアクセス検査回路２７０を示す図である。アクセス検査回路２７０には、論理プロセッサ・マネージャ３６０が含まれる。

【００６２】

１つの物理プロセッサが、複数の論理プロセッサを有することができる。各論理プロセッサは、論理プロセッサ・アクセスと称する、分離プロセッサ状態に入り、出ることができる。論理プロセッサ・アクセスは、通常は、対応する論理プロセッサが、分離進入（ｉｓｏ＿ｅｎｔｅｒ）および分離エグジット（ｉｓｏ＿ｅｘｉｔ）などの分離命令を実行する時に生成される。論理プロセッサ・マネージャ３６０は、論理プロセッサ・アクセスによって引き起こされる論理プロセッサ・オペレーションを管理する。本質的に、論理プロセッサ・マネージャ３６０は、プロセッサ内でイネーブルされた論理プロセッサの数を追跡する。論理プロセッサ・マネージャ３６０には、論理プロセッサ・レジスタ３７０、論理プロセッサ状態イネーブラ３８２、論理プロセッサ・アップデータ３８０、最小ディテクタ３７４、および最大ディテクタ３７６が含まれる。論理プロセッサ・レジスタ３７０には、現在イネーブルされている論理プロセッサの数を示すために、論理プロセッサ・カウント３７２が格納される。論理プロセッサ状態イネーブラ３８２は、論理プロセッサ・アクセスが有効である時に、論理プロセッサ状態をイネーブルする。論理プロセッサ・アップデータ３８０は、論理プロセッサ・アクセスに従って論理プロセッサ・カウント３７２を更新する。論理プロセッサ・アップデータ３８０は、イネーブルされた論理プロセッサ状態によってイネーブルされる。一実施形態では、論理プロセッサ・レジスタ３７０および論理プロセッサ・アップデータ３８０が、イネーブルを有するアップ／ダウン・カウンタとして実装される。最小ディテクタ３７４は、論理プロセッサ・カウント３７２が、最小論理プロセッサ値（たとえば０）と等しいかどうかを判定する。最大ディテクタ３７６は、論理プロセッサ・カウント３７２が、最大論理プロセッサ値を超えるかどうかを判定する。最大論理プロセッサ値は、プロセッサ１１０内で分離実行モードによってサポートすることができる論理プロセッサの最大個数を示す数である。

【００６３】

論理プロセッサ・アップデータ３８０は、システム・リセット時に論理プロセッサ・レジスタ３７０を初期化する。論理プロセッサ・アップデータ３８０は、アクセス・トランザクションが論理プロセッサ進入に対応する時に、第１の（たとえば増分する）方向に論理プロセッサ・カウント３７２を更新する。論理プロセッサ・アップデータ３８０は、アクセス・トランザクションが論理プロセッサ・エグジット(exit)または論理プロセッサ離脱(withdrawal)に対応する時に、第１の方向と反対の第２の（たとえば減分する）方向に論理プロセッサ・カウント３７２を更新する。論理プロセッサ・カウント３７２が、最小論理プロセッサ値と等しい時に、論理プロセッサ・マネージャ３６０が、プロセッサ１１０に、キャッシュ・メモリ２３２（図２Ａ）をメイン・メモリに書き込み、すべての分離情報から分離設定レジスタ（図２Ａ）を書き込むことによってキャッシュ・メモリ２３２をクリアさせて、これらのストレージ要素の初期状態を復元させる。論理プロセッサ・カウント３７２が、最大論理プロセッサ値を超える時には、論理プロセッサの総数がプロセッ

サ内でサポートできる論理プロセッサの最大個数を超えたので、論理プロセッサ・マネージャ３６０が、プロセッサ１１０に、障害またはフォールト状態を生成させる。

【００６４】

図４は、本発明の一実施形態による、分離実行に関するアクセス許可信号を生成する処理４００を示す流れ図である。

【００６５】

開始時に、処理４００では、ページを複数の分離メモリ区域に分配する（ブロック４１０）。その後、処理４００では、プロセッサを分離実行モードで構成するために、プロセッサ制御レジスタ内の実行モード・ワードをアサートする（ブロック４２０）。次に、処理４００では、プロセッサからのアクセス・トランザクションからアクセス情報を受け取る（ブロック４２５）。アクセス情報には、物理アドレス（ＴＬＢによって供給される）、ページの属性（分離／非分離）、およびアクセス・タイプが含まれる。次に、処理４００では、属性に分離がセットされ、実行モード・ワードがアサートされている（分離に設定されていることを示す）かどうかを判定する（ブロック４３０）。そうでない場合には、処理４００では、障害またはフォールト状態を生成し（ブロック４３５）、終了する。アサートされている場合には、処理４００では、アクセス許可信号をアサートする（ブロック４４０）。その後、処理４００が終了する。

【００６６】

図５は、本発明の一実施形態による、分離実行に関するプロセス論理プロセッサ・オペレーションを管理する処理５００を示す流れ図である。

【００６７】

開始時に、処理５００では、イネーブルされた論理プロセッサがない時に、論理プロセッサ・レジスタを初期化する（ブロック５１０）。その後、処理５００では、論理プロセッサ・アクセス命令（たとえばｉｓｏ＿ｅｎｔｅｒ、ｉｓｏ＿ｅｘｉｔ）を実行する。論理プロセッサ・アクセス命令によって、実行モード・ワードがアサートされる。次に、処理５００では、論理プロセッサ状態をイネーブルする（ブロック５２５）。次に、処理５００では、論理プロセッサ・アクセス・タイプを判定する（ブロック５３０）。

【００６８】

論理プロセッサ・アクセス・タイプが、論理プロセッサ進入である場合には、処理５００では、第１の（たとえば増分する）方向に論理プロセッサ・カウントを更新する（ブロック５４０）。その後、処理５００では、論理プロセッサ・カウントが最大論理プロセッサ値を超えたかどうかを判定する（ブロック５５０）。そうでない場合には、処理５００はブロック５７０に進む。超えた場合には、処理５００では、障害またはフォールト状態を生成し（ブロック５６０）、その後、終了する。

【００６９】

論理プロセッサ・アクセス・タイプが、論理プロセッサ・エグジットまたは論理プロセッサ離脱である場合には、処理５００では、論理プロセッサ・カウントを第１の方向と反対の第２の（たとえば減分する）方向に更新する（ブロック５４５）。その後、処理５００では、論理プロセッサ・カウントが最小値（たとえば０）と等しいかどうかを判定する（ブロック５５５）。そうでない場合には、処理５００はブロック５７０に進む。等しい場合には、処理５００では、分離情報のすべてから、キャッシュ・メモリおよび分離設定レジスタを初期化する（ブロック５６５）。

【００７０】

次に、処理５００では、次の論理プロセッサ・アクセスがあるかどうかを判定する（ブロック５７０）。次の論理プロセッサ・アクセスがある場合には、処理５００は、ブロック５２０に戻って、論理プロセッサ・アクセス命令を実行する。論理プロセッサ・アクセスがない場合には、処理５５０が終了する。

【００７１】

分離実行環境でのメモリ・コントローラを使用する複数の分離メモリへのアクセスの制御上の説明では、プロセッサ１１０内の分離実行処理に言及した。図１Ｃに示された、複数

の分離メモリ区域７１へのアクセスは、さらに、ＭＣＨ１３０（図１Ｆ）によって制御される。図１Ｆを参照すると、プロセッサ１１０は、ＭＣＨ１３０を、アドレス・ロケーションにマッピングされた入出力デバイスとみなす。分離メモリ区域７０、特に複数の分離メモリ区域７１（図１Ｃ）へのアクセスを有するために、プロセッサ１１０は、適宜ＭＣＨ１３０内のメモリ構成ストレージを構成する必要がある。ＭＣＨ１３０には、プロセッサ１１０が複数の非分離メモリ区域８３（図１Ｃ）内のメモリ１４０にもアクセスできるようにする制御機能も含まれる。ＭＣＨ１３０は、分離アクセス信号またはバス・サイクル情報など、ホスト・バス１２０を介してプロセッサ１１０から信号を受け取る。

【００７２】

図１Ｆでは、ＭＣＨ１３０が、プロセッサ１１０の外部に図示されている。しかし、ＭＣＨ１３０をプロセッサ１１０の内部に含めることが可能である。この場合には、ＭＣＨ１３０内のレジスタへの書込アクセスを外部化して、外部キャッシュがキャッシュ・コヒーレンシに関して参加できるようにする。

【００７３】

本質的に、ＭＣＨ１３０内のアクセス・コントローラは、図３Ａに示されたアクセス検査回路２７０に類似する機能を実行する。プロセッサ１１０とＭＣＨ１３０の両方でアクセス一貫性を維持することによって、メモリへのアクセスをきちんと制御することができる。ＭＣＨ１３０内のアクセス・コントローラは、プロセッサ１１０からのアクセス・トランザクションが有効であるかどうかを判定する。そうである場合には、アクセス・コントローラは、アクセス許可信号を返して、そのアクセス・トランザクションを完了させる。そうでない場合には、障害またはフォールト状態を生成する。さらに、ＭＣＨ１３０内のアクセス・コントローラは、それ自体の構成および制御ストレージへの意図的なまたは偶発的な書込のすべてを保護する。ＭＣＨ１３０は、メモリ１４０に直接にインターフェースするので、アクセス・コントローラは、リセット時に、分離メモリ区域の内容およびそれ自体の内部ストレージの初期化も提供する。

【００７４】

図６は、本発明の一実施形態による、図１Ｆに示されたメモリ・コントローラ・ハブ（ＭＣＨ）の分離区域アクセス・コントローラ１３５を示す図である。アクセス・コントローラ１３５には、構成ストレージ６１０、構成コントローラ６４０、およびＭＣＨアクセス検査回路８１０が含まれる。

【００７５】

構成ストレージ６１０によって、図１Ｆに示されたプロセッサ１１０によって生成されるアクセス・トランザクションが構成される。プロセッサ１１０は、通常実行モードと分離実行モードを有する。アクセス・トランザクションは、アクセス情報６６０を有する。アクセス情報６６０は、ホスト・バス１２０（図１Ｆ）を介して搬送され、アクセス情報６６０には、アドレス情報と分離アクセス状態が含まれる。アドレス情報は、物理アドレス６６２によって表される。分離アクセス状態は、分離アクセス信号６６４によって表される。分離アクセス信号６６４は、本質的に図２Ａに示されたプロセッサ分離アクセス信号２７２と同等である。分離アクセス信号６６４は、プロセッサ１１０が複数の分離メモリ区域７１（図１Ｃに図示）の１つへの有効な参照を生成する時にアサートされる。

【００７６】

構成ストレージ６１０には、メモリ所有権ページ・テーブル（ＭＯＰＴ）７７のキャッシュ６６０が含まれる。構成ストレージ６１０では、キャッシュ６６０内の物理アドレス６６２の検索を実行して、物理アドレスおよび関連するページ・テーブル・エントリを見つける。物理アドレスがキャッシュ２１９内にない場合には、構成ストレージ６１０で、ＭＯＰＴ７７（図１Ｅ）自体で物理アドレス６６２の検索を実行する。構成ストレージ６１０では、ＭＯＰＴのベース２２１を使用して、ＭＯＰＴ７７内の物理アドレス６６２を検索する。図１Ｅも参照すると、ＭＯＰＴのベース２２１から開始して、構成ストレージ６１０で、ＭＯＰＴ７７への検索を実行し、物理アドレス６６２に関連するページ・テーブル・エントリ９３を見つける。構成ストレージでは、ページ９８の物理アドレスを検索し

て、その物理アドレスに関連するページ・テーブル・エントリ９３を見つけることができる。各ページ・テーブル・エントリ９３に、ＭＣＨ１３０に関するアクセス・トランザクションを構成するのに重要な物理アドレスに関連するページの属性９６（分離または非分離）が含まれる。物理アドレスおよび関連するページ・テーブル・エントリを突き止めるためのページ・テーブル内の検索の実行が、当技術分野で周知であることと、検索を実行する他の方法が、当業者の知識に含まれることを諒解されたい。

【００７７】

構成ストレージ２５０には、ＭＣＨ１３０によって生成されるアクセス・トランザクションを構成するための構成パラメータも含まれる。構成ストレージには、属性レジスタ６１１が含まれ、この属性レジスタ６１１に、検索によって見つけられる、分離または非分離のいずれかがセットされる、物理アドレスに関連する属性９６が含まれる。前に説明したように、分離メモリ区域７１は、分離実行モードのプロセッサ１１０だけからアクセス可能である。

【００７８】

構成コントローラ６４０は、構成ストレージ６１０へのアクセスを制御し、メモリ１４０へのいくつかの制御機能を提供する。

【００７９】

ＭＣＨアクセス検査回路８１０は、アクセス情報６６０、属性９６、分離アクセス信号６６４、および分離メモリ優先順位７３６を使用してアクセス許可信号６５２を生成する。アクセス許可信号６５２は、アクセス・トランザクションが有効であるかどうかを示す。アクセス許可信号６５２を、プロセッサ１１０または他のチップセットまたは周辺デバイスが使用して、分離メモリ区域７１へのアクセスの試みが許可されるかどうかを判定することができる。

【００８０】

図７は、本発明の一実施形態による、図６に示されたＭＣＨアクセス検査回路８１０を示す図である。

【００８１】

ＭＣＨアクセス検査回路８１０は、属性９６および分離アクセス信号６６４に基づいてアクセス許可信号６５２を生成する。アクセス許可信号６５２によって、アクセス・トランザクションが有効であるかどうかが示される。ＭＣＨアクセス検査回路８１０は、属性９６および分離アクセス信号６６４を受け取って、アクセス許可信号６５２を生成する。分離区域へのアクセス許可信号６５２は、属性９６に分離がセットされ、分離アクセス信号６６４がアサートされ、構成に従って分離アクセスが有効または許可されることが示される時に、アサートされる。一実施形態では、ＭＣＨアクセス検査回路８１０が、論理「排他ＮＯＲ」オペレーションを実行する。したがって、プロセッサが分離区域の物理アドレスを要求する時に、そのプロセッサが分離実行モードで動作しており、物理アドレスに関連するページの属性に分離がセットされている場合に限って、アクセス・トランザクションが許可される。

【００８２】

図８は、本発明の一実施形態による、ＭＣＨに関する分離実行のためにアクセス許可信号を生成する処理８００を示す流れ図である。

【００８３】

開始時に、処理８００では、ＭＣＨに関するアクセス・トランザクションを構成する（ブロック８１０）。その後、処理８００では、アクセス・トランザクションからアクセス情報を受け取る（ブロック８２０）。アクセス情報には、ページの物理アドレス、分離アクセス信号、および属性（分離／非分離）が含まれる。次に、処理８００では、属性に分離がセットされているかどうか、および分離アクセス信号がアサートされているかどうかを判定する（ブロック８３０）。そうでない場合には、処理８００では、障害またはフォールト状態を生成し（ブロック８３５）、その後、終了する。そうである場合には、処理８００では、アクセス許可信号をアサートする（ブロック８４０）。その後、処理８００が

終了する。

【００８４】

本発明を、例示的実施形態に関して説明してきたが、この説明は、制限的な意味で解釈されることを意図されていない。例示的実施形態のさまざまな修正形態ならびに本発明が関係する技術の当業者に明白な本発明の他の実施形態は、本発明の趣旨および範囲に含まれるとみなされる。

【図面の簡単な説明】

【図１Ａ】　本発明の一実施形態によるオペレーティング・システムを示す図である。

【図１Ｂ】　本発明の一実施形態による、オペレーティング・システム内のさまざまな要素、プロセッサ、および単一の連続する分離メモリ区域のアクセス可能性を示す図である。

【図１Ｃ】　本発明の一実施形態による、オペレーティング・システム内のさまざまな要素およびプロセッサ、特に複数の分離メモリ区域および複数の非分離メモリ区域のアクセス可能性を示す、図１Ｂに類似する図である。

【図１Ｄ】　本発明の一実施形態による、分離実行のためにメモリのページを分配する処理を示す流れ図である。

【図１Ｅ】　本発明の一実施形態による、メモリ所有権ページ・テーブルと、仮想アドレスを物理アドレスに変換する処理を示す図である。

【図１Ｆ】　本発明の一実施形態を実践することができるコンピュータ・システムを示す図である。

【図２Ａ】　本発明の一実施形態による、図１Ｆに示された分離実行回路を示す図である。

【図２Ｂ】　本発明の一実施形態による、図２Ａに示されたアクセス・マネージャを示す図である。

【図３Ａ】　本発明の一実施形態による、アクセス検査回路を示す図である。

【図３Ｂ】　本発明のもう１つの実施形態による、論理プロセッサ・オペレーションを管理するアクセス検査回路を示す図である。

【図４】　本発明の一実施形態による、分離実行に関するアクセス許可信号を生成する処理を示す流れ図である。

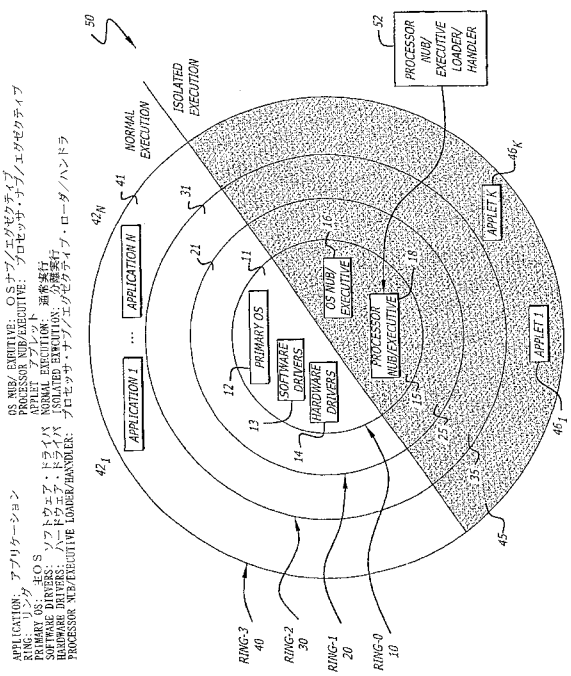
【図５】　本発明の一実施形態による、分離実行に関するプロセス・スレッド・オペレーションを管理する処理を示す流れ図である。

【図６】　本発明の一実施形態による、図１Ｆに示されたメモリ・コントローラ・ハブ（ＭＣＨ）の分離区域アクセス制御を示す図である。

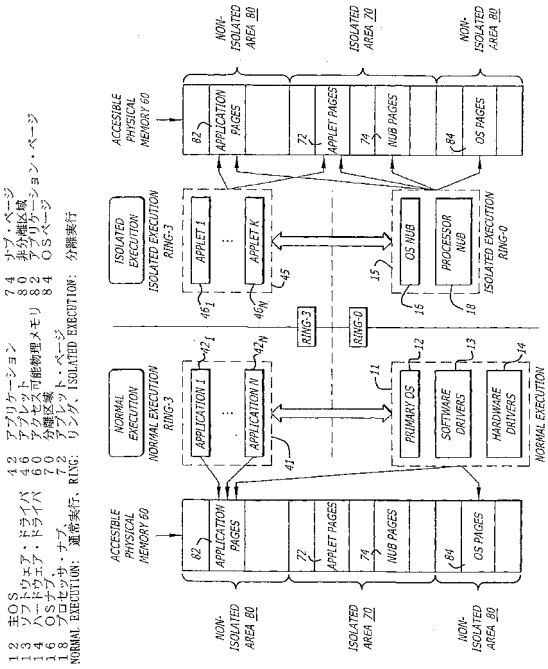
【図７】　本発明の一実施形態による、図６に示されたＭＣＨアクセス検査回路を示す図である。

【図８】　本発明の一実施形態による、ＭＣＨに関する分離実行のためにアクセス許可信号を生成する処理を示す流れ図である。

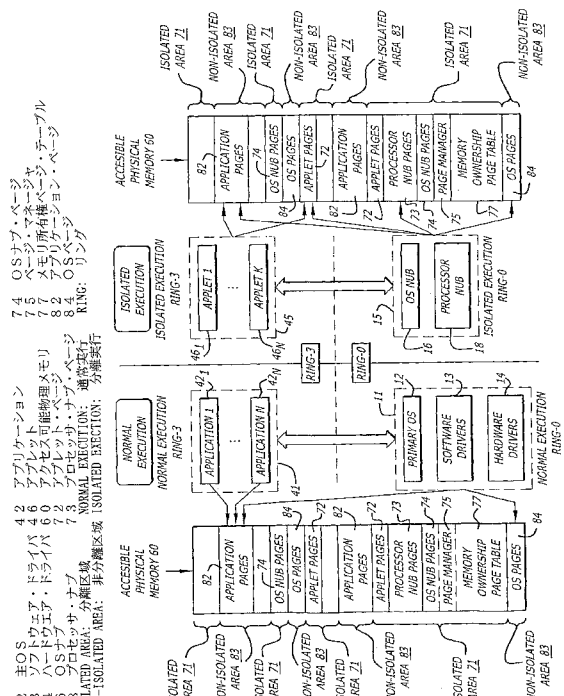
【図１Ａ】



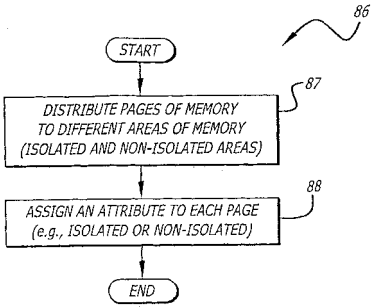
【図１Ｂ】



【図１Ｃ】

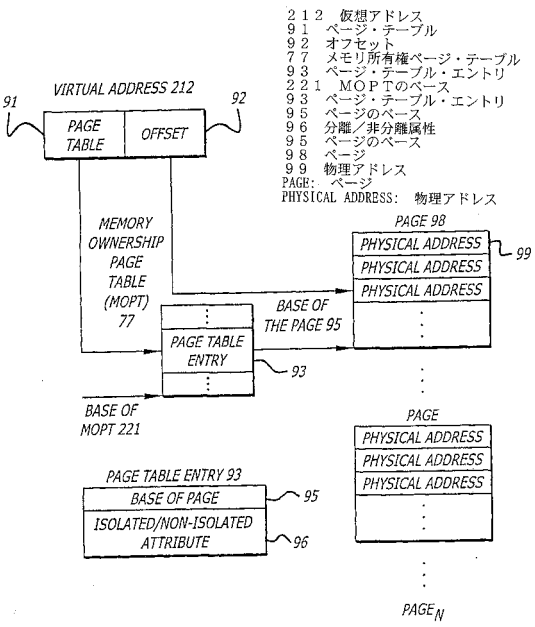


【図１Ｄ】

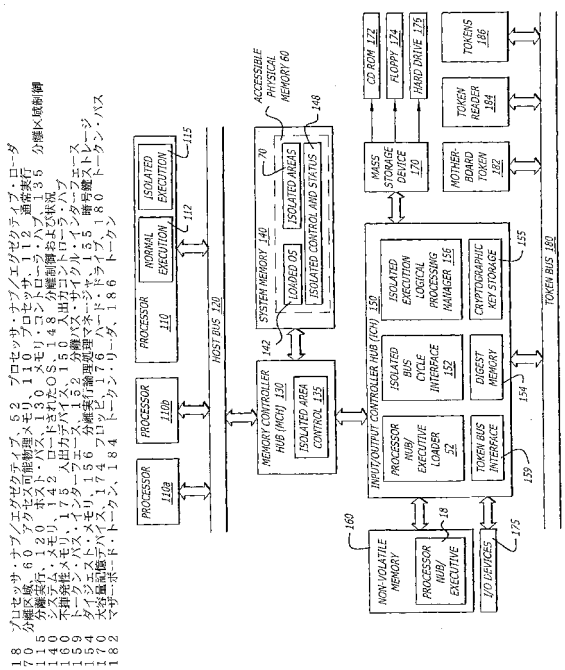


87 メモリのページをメモリの異なる区域
（分離区域および非分離区域）に分配する
88 各ページに属性（たとえば分離または非分離）を割り当てる

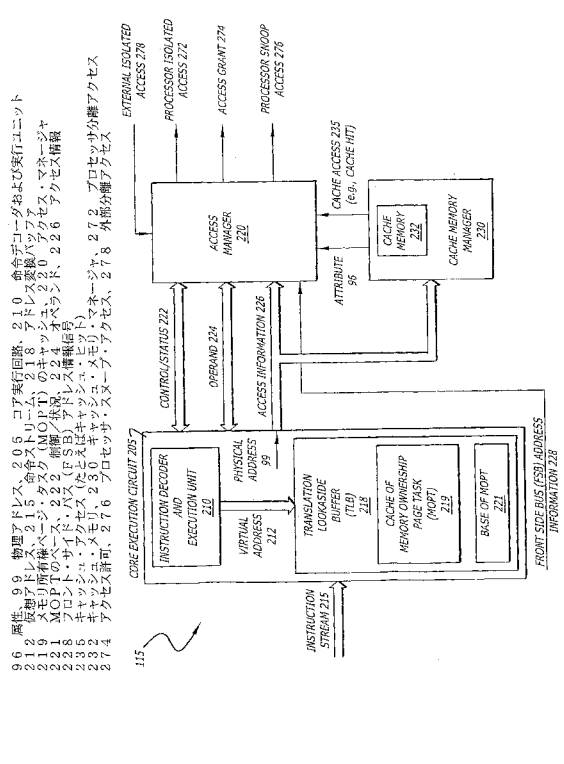
【図１Ｅ】



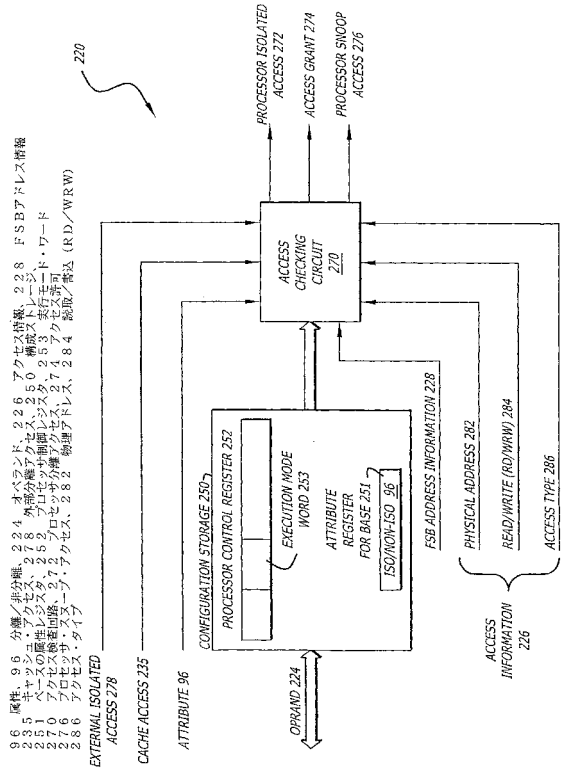
【図１Ｆ】



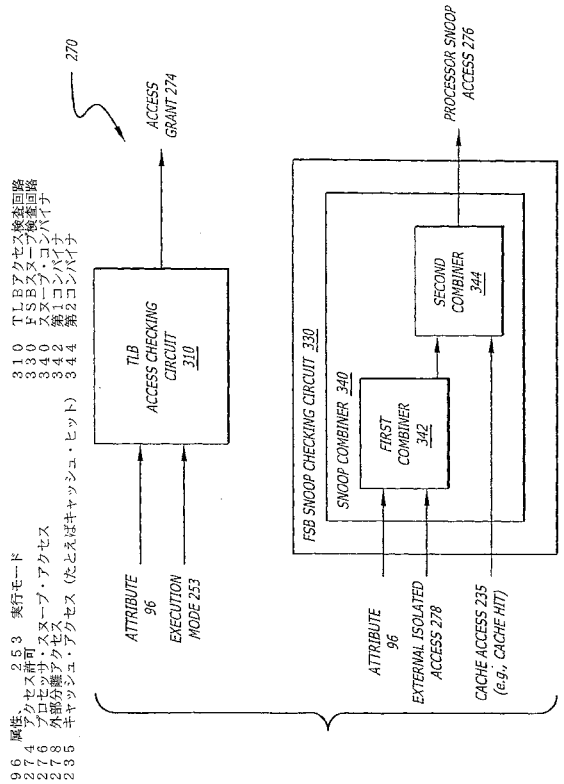
【図２Ａ】



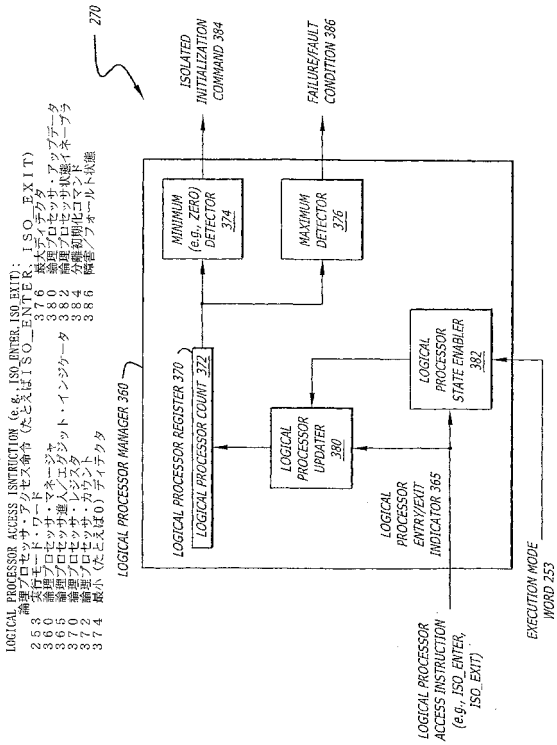
【図２Ｂ】



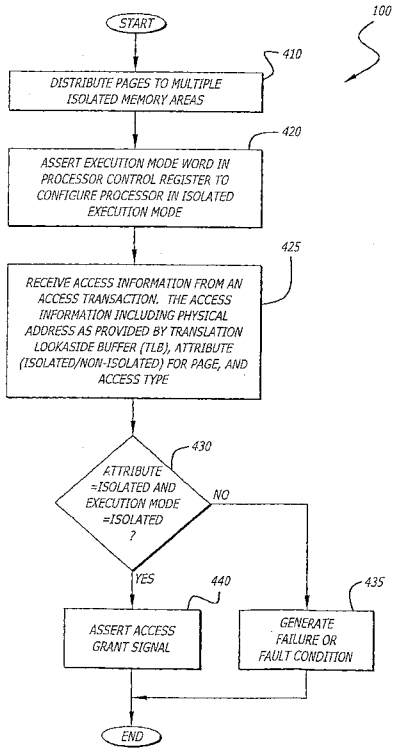
【図３Ａ】



【図３Ｂ】

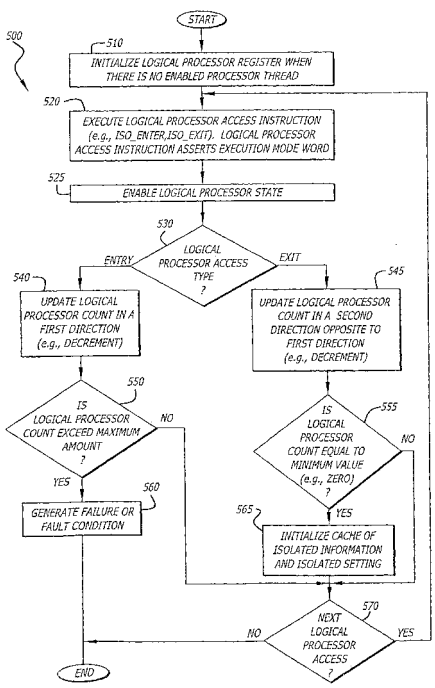


【図４】



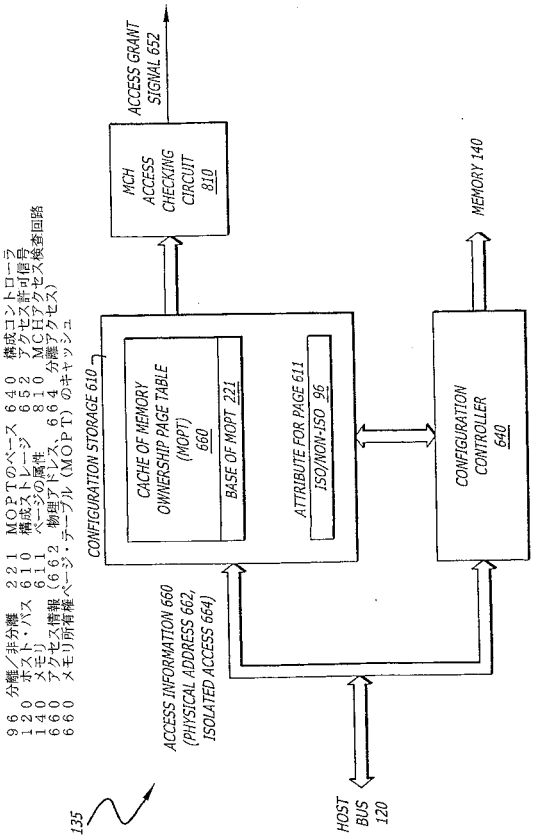
410 ページを複数の分離メモリ区域に分配する
420 プロセッサを分離実行モードで構成するために、プロセッサ制御レジスタ内の実行モード・ワードをアサートする
425 アクセス・トランザクションからアクセス情報を受け取る。アクセス情報には、アドレス変換バッファによって供給される物理アドレス、ページの属性（分離／非分離）、およびアクセス・タイプが含まれる
430 属性＝分離かつ実行モード＝分離か
435 障害またはフォールト状態を生成する
440 アクセス許可信号をアサートする

【図５】

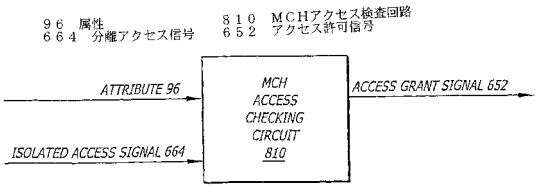


510 イネーブルされたプロセッサ・スレッドがない時に、論理プロセッサ・レジスタを初期化する
520 論理プロセッサ・アクセス命令（たとえばiso_enter、iso_exit）を実行する。論理プロセッサ・アクセス命令によって、実行モード・ワードがアサートされる
525 論理プロセッサ状態をイネーブルする
530 論理プロセッサ・アクセス・タイプは何か
540 第１の（たとえば減分する）方向に論理プロセッサ・カウントを更新する
550 論理プロセッサ・カウントが最大値を超えたか
560 障害またはフォールト状態を生成する
545 論理プロセッサ・カウントを第１の方向と反対の第２の（たとえば減分する）方向に更新する
555 論理プロセッサ・カウントが最小値（たとえば０）と等しいか
565 分離情報のキャッシュおよび分離設定を初期化する
570 次の論理プロセッサ・アクセスがあるか
EXIT: エグジット、ENTRY: 進入

【図６】

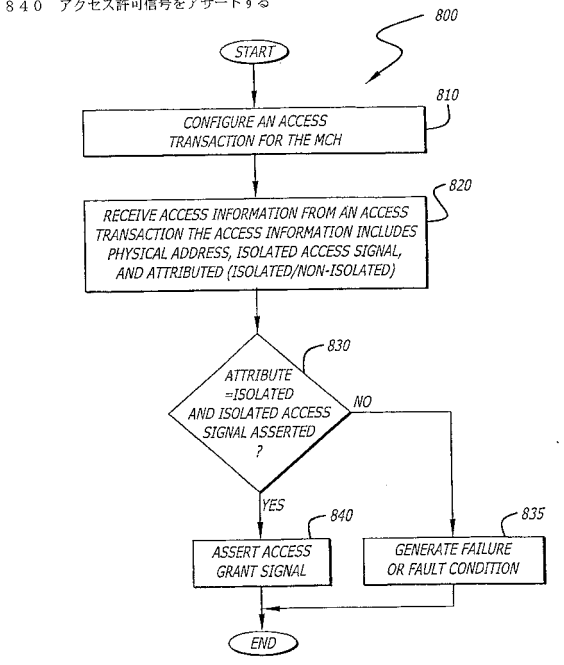


【図７】



【図８】

810 MCHに関するアクセス・トランザクションを構成する
820 アクセス・トランザクションからアクセス情報を受け取る。アクセス情報には、物理アドレス、分離アクセス信号、および属性（分離／非分離）が含まれる
830 属性＝分離かつ分離アクセス信号がアサートされているか
835 障害またはフォールト状態を生成する
840 アクセス許可信号をアサートする



フロントページの続き

(72)発明者 リン，デリック
アメリカ合衆国・９４０４４・カリフォルニア州・フォスター シティ・バーケンタイン ストリート・１１３
(72)発明者 サッカー，シュリーカント
アメリカ合衆国・９７２２５・オレゴン州・ポートランド・サウスウェスト ムーンリッジ プレイス・１５０
(72)発明者 ネイジャー，ギルバート
アメリカ合衆国・９７２１２・オレゴン州・ポートランド・ノースイースト １１ティエイチ アベニュ・２４２４
(72)発明者 マッキーン，フランシス
アメリカ合衆国・９７２２９・オレゴン州・ポートランド・ノースウェスト レーマンズ コート・１０６１２
(72)発明者 ハーバート，ハワード
アメリカ合衆国・８５０４５・アリゾナ州・フィーニックス・サウス ファースト ドライブ・１６８１７
(72)発明者 レネリス，ケネス
アメリカ合衆国・９８０７２・ワシントン州・ウッドインヴィル・ノースイースト １４１エスティ ストリート・２１８１６
(72)発明者 エリソン，カール
アメリカ合衆国・９７２１０・オレゴン州・ポートランド・ノースウェスト ２８ティエイチ アベニュ・１８１８

審査官 高橋 克

(56)参考文献 特開昭６１－１１４３５４（ＪＰ，Ａ）
特開平０７－１５２６５３（ＪＰ，Ａ）
特開平１１－２４２６３３（ＪＰ，Ａ）
特表２００１－５１６０８１（ＪＰ，Ａ）
実開平０３－２２５４５５（ＪＰ，Ｕ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 12/14