(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4672281号
(P4672281)
(45)発行日　平成23年4月20日(2011.4.20)　(24)登録日　平成23年1月28日(2011.1.28)

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

請求項の数 28　外国語出願　(全 21 頁)

(21)出願番号	特願2004-134539 (P2004-134539)
(22)出願日	平成16年4月28日 (2004.4.28)
(65)公開番号	特開2004-334870 (P2004-334870A)
(43)公開日	平成16年11月25日 (2004.11.25)
審査請求日	平成19年4月23日 (2007.4.23)
(31)優先権主張番号	60/467,343
(32)優先日	平成15年5月2日 (2003.5.2)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10/610,666
(32)優先日	平成15年6月30日 (2003.6.30)
(33)優先権主張国	米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　マーカス　ペイナード
アメリカ合衆国　９８００８　ワシントン州　ベルビュー　ノースイースト　１６８　アベニュー　７

最終頁に続く

(54)【発明の名称】最適化を用いたメモリアクセス制御の実装

(57)【特許請求の範囲】
【請求項１】
メモリアクセス要求を処理する方法を実施するためのコンピュータ実行可能命令を符号化したコンピュータ読み取り可能な記録媒体であって、前記方法は、
メモリの一部にアクセスするための要求を受け取るステップであって、前記要求は、アドレス変換マップを介して変換可能な識別子によって、アクセスされる前記メモリの一部を識別する、受け取るステップと、
前記アドレス変換マップに関するキャッシュ済み情報に基づいて、前記要求の実行が、前記メモリへのアクセスを制限するポリシーに違反することになるかどうかを判定するステップであって、前記キャッシュ済み情報は、前記アドレス変換マップの、所定のプロパティを有するページの集合を識別するデータを含む、判定するステップと、
前記要求の実行が前記ポリシーに違反しない場合は、前記要求に従って前記メモリへのアクセスを可能にするステップと、
前記要求の実行が前記ポリシーに違反する場合は、
前記要求を阻止すること、または、
前記要求を前記ポリシーに違反しないように修正して、前記修正した要求を実行すること
のどちらかを実施するステップと
を備え、
前記キャッシュ済み情報は、前記アドレス変換マップ中の、前記アドレス変換マップの

ルートから所定距離にあるページの集合を識別するデータを含む
ことを特徴とするコンピュータ読み取り可能な記録媒体。
【請求項２】
前記要求は、前記メモリの前記一部に書き込む要求を含む
ことを特徴とする請求項１に記載のコンピュータ読み取り可能な記録媒体。
【請求項３】
前記アドレス変換マップは前記メモリに記憶され、前記要求は、前記アドレス変換マップが記憶されたメモリの一部に書き込む要求を含む
ことを特徴とする請求項１に記載のコンピュータ読み取り可能な記録媒体。
【請求項４】
前記キャッシュ済み情報は、指定のページへの参照の数を示すデータを含む
ことを特徴とする請求項１に記載のコンピュータ読み取り可能な記録媒体。
【請求項５】
前記キャッシュ済み情報は、指定のページへの参照の数を示すデータを含み、前記参照は指定の属性を有する
ことを特徴とする請求項１に記載のコンピュータ読み取り可能な記録媒体。
【請求項６】
前記キャッシュ済み情報は、前記アドレス変換マップ中の指定のページが参照するページの数を示すデータを含む
ことを特徴とする請求項１に記載のコンピュータ読み取り可能な記録媒体。
【請求項７】
前記キャッシュ済み情報は、前記アドレス変換マップ中の指定のページが参照する、また、前記指定のページが指定の属性を割り当てるページの数を示すデータを含む
ことを特徴とする請求項１に記載のコンピュータ読み取り可能な記録媒体。
【請求項８】
前記ポリシーへの適合は、集合中のページのメンバシップに基づいて判定され、前記キャッシュ済み情報は、前記集合の適切な上位集合を含み、前記要求の実行が前記ポリシーに違反することになるかどうかを判定する前記動作は、前記ページが前記上位集合のメンバかどうかを評価することを含む
ことを特徴とする請求項１に記載のコンピュータ読み取り可能な記録媒体。
【請求項９】
前記ポリシーへの適合は、集合中のページのメンバシップに基づいて判定され、前記キャッシュ済み情報は、前記集合の適切な部分集合を含み、前記要求の実行が前記ポリシーに違反することになるかどうかを判定する前記動作は、前記ページが前記部分集合のメンバかどうかを評価することを含む
ことを特徴とする請求項１に記載のコンピュータ読み取り可能な記録媒体。
【請求項１０】
アドレス変換マップを介してアクセスが提供されるコンピュータメモリを管理する方法であって、
前記アドレス変換マップの状態の少なくとも１つの態様に関する情報を記憶するステップであって、前記記憶済み情報は、前記アドレス変換マップの、所定のプロパティを有するページの集合を識別するデータを含む、記憶するステップと、
前記コンピュータメモリにアクセスするための要求を受け取るステップと、
前記記憶済み情報に少なくとも部分的に基づいて、前記要求の実行が、前記コンピュータメモリへのアクセスを制限するポリシーに違反することにならないと判定するステップと、
前記要求の実行を可能にするステップと、
前記要求の実行から生じる前記アドレス変換マップの状態を反映するように、前記記憶済み情報を更新するステップと
を備え、

前記記憶済み情報は、前記アドレス変換マップ中の、前記アドレス変換マップのルートから所定距離にあるページの集合を識別するデータを含む
ことを特徴とする方法。
【請求項１１】
前記要求は、前記コンピュータメモリの一部に書き込む要求を含む
ことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記アドレス変換マップは前記メモリに記憶され、前記要求は、前記アドレス変換マップが記憶されたメモリの一部に書き込む要求を含む
ことを特徴とする請求項１０に記載の方法。
【請求項１３】
前記記憶済み情報は、指定のページへの参照の数を示すデータを含む
ことを特徴とする請求項１０に記載の方法。
【請求項１４】
前記記憶済み情報は、指定のページへの参照の数を示すデータを含み、前記参照は指定の属性を有する
ことを特徴とする請求項１０に記載の方法。
【請求項１５】
前記記憶済み情報は、前記アドレス変換マップ中の指定のページが参照するページの数を示すデータを含む
ことを特徴とする請求項１０に記載の方法。
【請求項１６】
前記記憶済み情報は、前記アドレス変換マップ中の指定のページが参照する、また、前記指定のページが指定の属性を割り当てるページの数を示すデータを含む
ことを特徴とする請求項１０に記載の方法。
【請求項１７】
前記ポリシーへの適合は、集合中のページのメンバシップに基づいて判定され、前記記憶済み情報は、前記集合の適切な上位集合を含み、前記要求の実行が前記ポリシーに違反することにならないと判定する前記動作は、前記ページが前記上位集合のメンバかどうかを評価することを含む
ことを特徴とする請求項１０に記載の方法。
【請求項１８】
前記ポリシーへの適合は、集合中のページのメンバシップに基づいて判定され、前記記憶済み情報は、前記集合の適切な部分集合を含み、前記要求の実行が前記ポリシーに違反することにならないと判定する前記動作は、前記ページが前記部分集合のメンバかどうかを評価することを含む
ことを特徴とする請求項１０に記載の方法。
【請求項１９】
アドレス変換マップによってアドレス指定されるメモリへのアクセスを制御するためのシステムであって、
前記メモリへのアクセスを制限するポリシーを記憶する１つまたは複数の記憶位置と、
前記アドレス変換マップに関する情報を記憶するキャッシュであって、前記キャッシュに記憶された情報は、前記アドレス変換マップの、所定のプロパティを有するページの集合を識別するデータを含む、キャッシュと、
前記メモリにアクセスするための要求を受け取り、前記キャッシュに記憶された前記情報に少なくとも部分的に基づいて、前記要求が前記ポリシーの下で許可できるかどうかを判定する論理とを備え、
前記論理は、前記要求が前記ポリシーの下で許可できると判定された場合は、前記要求の続行を可能にし、前記要求が前記ポリシーの下で許可できないと判定された場合は、（１）前記要求を阻止すること、または、（２）前記要求を前記ポリシーの下で許可できる

形に修正して、前記修正した要求の続行を可能にすること、のどちらかを実施し、
前記キャッシュに記憶された情報は、前記アドレス変換マップ中の、前記アドレス変換マップのルートから所定距離にあるページの集合を識別するデータを含む
ことを特徴とするシステム。
【請求項２０】
前記要求は、前記メモリの一部に書き込む要求を含む
ことを特徴とする請求項１９に記載のシステム。
【請求項２１】
前記アドレス変換マップは前記メモリに記憶され、前記要求は、前記アドレス変換マップが記憶されたメモリの一部に書き込む要求を含む
ことを特徴とする請求項１９に記載のシステム。
【請求項２２】
前記キャッシュに記憶された情報は、指定のページへの参照の数を示すデータを含む
ことを特徴とする請求項１９に記載のシステム。
【請求項２３】
前記キャッシュに記憶された情報は、指定のページへの参照の数を示すデータを含み、前記参照は指定の属性を有する
ことを特徴とする請求項１９に記載のシステム。
【請求項２４】
前記キャッシュに記憶された情報は、前記アドレス変換マップ中の指定のページが参照するページの数を示すデータを含む
ことを特徴とする請求項１９に記載のシステム。
【請求項２５】
前記キャッシュに記憶された情報は、前記アドレス変換マップ中の指定のページが参照する、また、前記指定のページが指定の属性を割り当てるページの数を示すデータを含む
ことを特徴とする請求項１９に記載のシステム。
【請求項２６】
前記ポリシーへの適合は、集合中のページのメンバシップに基づいて判定され、前記キャッシュに記憶された情報は、前記集合の適切な上位集合を含み、前記論理は、前記ページが前記上位集合のメンバかどうかを評価することによって、前記要求を許可することが前記ポリシーに違反することになるかどうかを判定する
ことを特徴とする請求項１９に記載のシステム。
【請求項２７】
前記ポリシーへの適合は、集合中のページのメンバシップに基づいて判定され、前記キャッシュに記憶された情報は、前記集合の適切な部分集合を含み、前記論理は、前記ページが前記部分集合のメンバかどうかを評価することによって、前記要求を許可することが前記ポリシーに違反することになるかどうかを判定する
ことを特徴とする請求項１９に記載のシステム。
【請求項２８】
前記論理はハードウェアとソフトウェアのうちの少なくとも一方において実現される
ことを特徴とする請求項１９に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に、コンピュータセキュリティの分野に関する。より詳細には、本発明は、アドレス変換制御を用いて隔離（isolated）または「遮蔽（curtained）」メモリを実現するための効率的な技法に関する。
【背景技術】
【０００２】
ある状況では、メモリには、アクセスが制限される部分である隔離されたまたは「遮蔽

」された部分があることが望ましい。例えば、あるコンピュータが２つのオペレーティングシステムを並行して稼動させているが、一方のオペレーティングシステムは安全であり、他方はそうではない場合がある。この場合、安全なオペレーティングシステムは、安全でないオペレーティングシステムからアクセスできない秘密情報を記憶することのできる遮蔽メモリを有することが望ましい。

【０００３】

遮蔽メモリを実現する方法の１つは、アドレス変換制御による方法である。近年の多くのコンピュータは仮想メモリシステムを使用しており、仮想メモリシステムでは、コンピュータ上で稼動するソフトウェアは仮想アドレスを使用してメモリのアドレスを指定し、メモリ管理ユニットが、１組のアドレス変換マップを使用して仮想アドレスを物理アドレスに変換する。通常、各プロセスはそれ自体のアドレス変換マップを有し、したがって、仮想アドレスと物理アドレスとの間のマッピングはプロセスごとに変化する。所与のプロセスのアドレス変換マップは、物理メモリの所与のブロック（例えばページ）用の仮想アドレスをプロセスに露呈しないように構成することが可能である。このように、安全なプロセスだけが物理メモリの所与のブロックについての仮想アドレスを有するようにすることにより、アドレス変換マップの内容を制御して遮蔽メモリを実現することが可能である。

【０００４】

このような機構を使用して遮蔽メモリを実現するときに生じる問題の１つは、アドレス変換マップがメモリに記憶されているので、どんなメモリ書込み動作もマップに影響を与える可能性があり、それにより遮蔽メモリ用の仮想アドレスが、遮蔽メモリにアクセスできるべきでないプロセスに露呈する恐れがあることである。このような仮想アドレスが露呈しないようにする方法の１つは、メモリ書込み動作が実施されるたびに、あらゆるマップのあらゆる要素をチェックして、遮蔽メモリにアクセスできるべきでないプロセスのマップ中に仮想アドレスがあるような遮蔽メモリページがないことを確実にすることである。しかし、書込み動作の頻度を考えると、この技法は非効率的である。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

従来のシステムには上述したような種々の問題があり、従来技術の欠点を克服する機構が必要とされており、さらなる改善が望まれている。

【０００６】

本発明は、このような状況に鑑みてなされたもので、その目的とするところは、アドレス変換マップの変更を効率的に制御するための、最適化を用いたメモリアクセス制御の実装を提供することにある。

【課題を解決するための手段】

【０００７】

本発明は、アドレス変換マップの変更を効率的に制御するための機構を提供する。アドレス変換マップの状態が、遮蔽メモリへのアクセスを許可されないプロセス（またはその他のエンティティ）に対して遮蔽メモリのブロックについての仮想アドレスが露呈する状態に入らないようにすることによって、遮蔽メモリを実現することができる。「ポリシー」が、どんなメモリアクセス動作が許可されるかを定義し、メモリアクセス制御システムが、アドレス変換マップがいずれかのポリシーに違反する状態に入るのを禁じることによって動作する。

【０００８】

このような仮想アドレスが露呈することになる状態は、しばしば、一定のプロパティを満たす複数の集合の共通部分（または非共通部分）に基づいて、あるいは一定のプロパティを満たすページの数に基づいて定義することができる。定義された集合のメンバであるページの識別を記憶またはキャッシュすることができ、したがって、アドレス変換マップの状態を変更する可能性のある書込み動作が実施されるたびに集合のメンバシップを計算

する必要はない。集合中のページの識別は、例えばビットベクトルとして記憶することができ、このようなビットベクトルに対して和や共通部分などの集合演算を効率的に実施することができる。特定のプロパティを満たす正確な集合を計算するのが難しい場合もあり得るが、何らかの明確な部分集合または上位集合を実際の集合の代わりとして使用することによってポリシーへの適合を保証することができることは、数学的に証明可能とすることができる。実際の集合よりも部分集合または上位集合の方が相対的に計算しやすい場合は、実際の集合の代わりに部分集合または上位集合を使用することができる。

【０００９】

さらに、いくつかの書込み動作の許可は、何らかの統計のカウント、例えば一定のプロパティを満たすページの数や所与のページへの参照の数などの点から定義することができる。このような統計は、参照カウンタとして効果的に記憶またはキャッシュすることができ、増分または減分動作によって更新することができる。ビットベクトルまたはカウンタは、マップが状態を変更するたびに更新することができ、次いで、これらを効率的に使用して、ポリシーの下でのメモリアクセス動作を評価することができる。

【００１０】

本発明のその他の特徴については後述する。

【００１１】

前述の概要、ならびに後続の好適実施形態の詳細な説明は、添付の図面と共に読めばよりよく理解される。本発明を例示するために、図面には本発明の例示的な構造を示す。ただし本発明は、開示する特定の方法および手段に限定されるわけではない。

【発明を実施するための最良の形態】

【００１２】

以下、図面を参照して本発明を適用できる実施形態を詳細に説明する。

例示的なコンピューティング構成

図１に、本発明の態様を実施することのできる例示的なコンピューティング環境を示す。コンピューティングシステム環境１００は、適したコンピューティング環境の一例にすぎず、本発明の使用または機能の範囲についてどんな制限も意味しない。またコンピューティング環境１００は、この例示的な動作環境のコンピューティングシステム環境１００に示すコンポーネントのいずれか１つまたは組合せに関してどんな依存も要件も有するものと解釈すべきではない。

【００１３】

本発明は、その他多くの汎用または専用コンピューティングシステム環境または構成でも動作する。本発明で使用するのに適するであろう周知のコンピューティングシステム、環境、および／または構成の例には、限定しないがパーソナルコンピュータ、サーバコンピュータ、ハンドヘルドデバイスまたはラップトップデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、セットトップボックス、プログラム可能な家庭用電化製品、ネットワークＰＣ（personal computer）、ミニコンピュータ、メインフレームコンピュータ、組込みシステムや、これらのシステムまたはデバイスのいずれかを含む分散コンピューティング環境などが含まれる。

【００１４】

本発明は、プログラムモジュールなど、コンピュータによって実行されるコンピュータ実行可能命令の一般的な状況で述べることができる。一般にプログラムモジュールは、特定のタスクを実施するか特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。本発明は分散コンピューティング環境で実施することもでき、その場合、タスクは通信ネットワークまたはその他のデータ伝送媒体を介してリンクされたリモート処理デバイスによって実施される。分散コンピューティング環境では、プログラムモジュールおよびその他のデータは、メモリ記憶デバイスを含めたローカルとリモートの両方のコンピュータ記憶媒体に位置することができる。

【００１５】

図１を参照すると、本発明を実施するための例示的なシステムは、コンピュータ１１０

の形の汎用コンピューティングデバイスを含む。コンピュータ１１０のコンポーネントには、限定しないがプロセッサ１２０と、システムメモリ１３０と、システムメモリを含めた様々なシステムコンポーネントをプロセッサ１２０に結合するシステムバス１２１とを含めることができる。システムバス１２１は、様々なバスアーキテクチャのいずれかを用いた、メモリバスまたはメモリコントローラ、周辺機器バス、ローカルバスを含めて、いくつかのタイプのバス構造のいずれかとすることができる。限定ではなく例として、このようなアーキテクチャには、ＩＳＡ（Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＭＣＡ（Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＥＩＳＡ（Ｅｎｈａｎｃｅｄ ＩＳＡ）バス、ＶＥＳＡ（Ｖｉｄｅｏ Ｅｌｅｃｔｒｏｎｉｃｓ Ｓｔａｎｄａｒｄｓ Ａｓｓｏｃｉａｔｉｏｎ）ローカルバス、およびＰＣＩ（Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔｓ）バス（メザニンバスとも呼ばれる）が含まれる。

【００１６】

コンピュータ１１０は通常、様々なコンピュータ可読媒体を備える。コンピュータ可読媒体は、コンピュータ１１０からアクセスできる任意の利用可能な媒体とすることができ、揮発性と不揮発性媒体、リムーバブルとノンリムーバブル媒体の両方が含まれる。限定ではなく例として、コンピュータ可読媒体には、コンピュータ記憶媒体および通信媒体を含めることができる。コンピュータ記憶媒体には、コンピュータ可読命令、データ構造、プログラムモジュール、その他のデータなどの情報を記憶するための任意の方法または技術で実現された、揮発性と不揮発性、リムーバブルとノンリムーバブルの両方の媒体が含まれる。コンピュータ記憶媒体には、限定しないがＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ（Electronically Erasable and Programmable Read Only Memory）、フラッシュメモリまたは他のメモリ技術、ＣＤ（compact disc）ＲＯＭ、ＤＶＤ（Digital Versatile Disc）または他の光ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置または他の磁気記憶デバイスが含まれ、あるいは、所望の情報を記憶するのに使用できコンピュータ１１０からアクセスできるその他の任意の媒体が含まれる。通信媒体は通常、搬送波や他の移送機構などの変調データ信号中に、コンピュータ可読命令、データ構造、プログラムモジュール、またはその他のデータを組み入れたものであり、任意の情報送達媒体が含まれる。「変調データ信号」という語は、情報が信号中に符号化される形で１つまたは複数の特性が設定または変更された信号を意味する。限定ではなく例として、通信媒体には、有線ネットワークや直接配線接続などの有線媒体と、音響、無線周波、赤外線、その他の無線媒体などの無線媒体とが含まれる。以上の任意の組合せもコンピュータ可読媒体の範囲に含めるべきである。

【００１７】

システムメモリ１３０は、読取り専用メモリ（ＲＯＭ）１３１やランダムアクセスメモリ（ＲＡＭ）１３２など、揮発性および／または不揮発性メモリの形のコンピュータ記憶媒体を含む。ＲＯＭ１３１には通常、起動中などにコンピュータ１１０内の要素間で情報を転送するのを助ける基本ルーチンを含むＢＩＯＳ（ｂａｓｉｃ ｉｎｐｕｔ／ｏｕｔｐｕｔ ｓｙｓｔｅｍ）１３３が記憶されている。ＲＡＭ１３２は通常、プロセッサ１２０がすぐにアクセス可能な、かつ／またはプロセッサ１２０によって現在操作されているデータおよび／またはプログラムモジュールを含む。限定ではなく例として、図１には、オペレーティングシステム１３４、アプリケーションプログラム１３５、その他のプログラムモジュール１３６、およびプログラムデータ１３７を示す。

【００１８】

コンピュータ１１０は、その他のリムーバブル／ノンリムーバブル、揮発性／不揮発性コンピュータ記憶媒体を備えることもできる。例にすぎないが図１には、ノンリムーバブルかつ不揮発性の磁気媒体に対して読み書きするハードディスクドライブ１４１と、リムーバブルかつ不揮発性の磁気ディスク１５２に対して読み書きする磁気ディスクドライブ１５１と、ＣＤＲＯＭや他の光媒体などリムーバブルかつ不揮発性の光ディスク１５６に対して読み書きする光ディスクドライブ１５５を示す。この例示的な動作環境で使用でき

るその他のリムーバブル／ノンリムーバブル、揮発性／不揮発性コンピュータ記憶媒体には、限定しないが磁気テープカセット、フラッシュメモリカード、ＤＶＤ、デジタルビデオテープ、ソリッドステートＲＡＭ、ソリッドステートＲＯＭなどが含まれる。ハードディスクドライブ１４１は通常、インタフェース１４０などの不揮発性メモリインタフェースを介してシステムバス１２１に接続され、磁気ディスクドライブ１５１および光ディスクドライブ１５５は通常、インタフェース１５０などのリムーバブルメモリインタフェースでシステムバス１２１に接続される。

【００１９】

以上に論じ図１に示した各ドライブおよびそれらに関連するコンピュータ記憶媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、およびその他のデータの記憶域をコンピュータ１１０に提供する。例えば図１には、ハードディスクドライブ１４１がオペレーティングシステム１４４、アプリケーションプログラム１４５、その他のプログラムモジュール１４６、およびプログラムデータ１４７を記憶しているのが示されている。これらのコンポーネントは、オペレーティングシステム１３４、アプリケーションプログラム１３５、その他のプログラムモジュール１３６、およびプログラムデータ１３７と同じものとすることもでき、異なるものとすることもできることに留意されたい。ここでは、オペレーティングシステム１４４、アプリケーションプログラム１４５、その他のプログラムモジュール１４６、およびプログラムデータ１４７が少なくとも異なるコピーであることを示すために、異なる番号を付してある。ユーザは、キーボード１６２、マウスやトラックボールやタッチパッドと一般に呼ばれるポインティングデバイス１６１などの入力デバイスを介して、コンピュータ１１０にコマンドおよび情報を入力することができる。その他の入力デバイス（図示せず）には、マイクロホン、ジョイスティック、ゲームパッド、衛星放送受信アンテナ、スキャナなどを含めることができる。これらおよび他の入力デバイスは、システムバスに結合されたユーザ入力インタフェース１６０を介してプロセッサ１２０に接続されることが多いが、パラレルポート、ゲームポート、ユニバーサルシリアルバス（「ＵＳＢ」）など、その他のインタフェースおよびバス構造で接続されてもよい。モニタ１９１または他のタイプの表示デバイスもまた、ビデオインタフェース１９０などのインタフェースを介してシステムバス１２１に接続される。モニタに加えて、コンピュータは通常、スピーカ１９７やプリンタ１９６など他の周辺出力デバイスも備えることができ、これらは出力周辺インタフェース１９５を介して接続することができる。

【００２０】

コンピュータ１１０は、リモートコンピュータ１８０など１つまたは複数のリモートコンピュータへの論理接続を用いて、ネットワーク化された環境で動作することができる。リモートコンピュータ１８０は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイス、またはその他の一般的なネットワークノードとすることができ、図１にはメモリ記憶デバイス１８１しか示していないが、通常はパーソナルコンピュータ１１０に関して上述した要素の多くまたはすべてを備える。図１に示す論理接続は、ローカルエリアネットワーク（ＬＡＮ）１７１およびワイドエリアネットワーク（ＷＡＮ）１７３を含むが、その他のネットワークを含むこともできる。このようなネットワーキング環境は、オフィス、企業全体のコンピュータネットワーク、イントラネット、およびインターネットでよくみられるものである。

【００２１】

コンピュータ１１０は、ＬＡＮネットワーキング環境で使用されるときは、ネットワークインタフェースまたはアダプタ１７０を介してＬＡＮ１７１に接続される。ＷＡＮネットワーキング環境で使用されるときは通常、インターネットなどのＷＡＮ１７３を介した通信を確立するためのモデム１７２または他の手段を備える。モデム１７２は内蔵でも外付けでもよく、ユーザ入力インタフェース１６０または他の適切な機構を介してシステムバス１２１に接続することができる。ネットワーク化された環境では、コンピュータ１１０に関して示したプログラムモジュールまたはその一部をリモートのメモリ記憶デバイス

に記憶することができる。限定ではなく例として、図１には、リモートアプリケーションプログラム１８５がメモリデバイス１８１上にあるものとして示す。図示のネットワーク接続は例示的なものであり、コンピュータ間に通信リンクを確立する他の手段を使用することもできることは理解されるであろう。

【００２２】

アドレス変換を用いたメモリアクセス

コンピュータシステム中のメモリ（例えば図１に示したＲＡＭ１３２）は、各バイトごとに物理アドレスを有する。したがって、メモリを構成するバイトには番号が付いていると見なすことができ、各バイトはその番号で明確に識別することができる。この場合、番号は物理アドレスを構成する。例えば、２５６バイトのメモリでは、バイトは０から2^8－１の範囲の物理アドレスを有することができる。しかし、近年のコンピュータシステムでは、メモリは一般に、その物理アドレスでアクセスされるのではなく仮想アドレスでアクセスされる。アドレス変換マップを使用して、物理アドレスが仮想アドレスに変換される。

【００２３】

図２に、アドレス変換マップの例と、実際のコンピュータシステムにおけるその使用を示す。図２に示す例示的なアドレス変換マップは「ページング」方式であり、メモリは「ページ」と呼ばれるブロック単位で割り当てられる。図２は、ＩＮＴＥＬ（登録商標）ｘ８６プロセッサ上で使用されるページング方式を表す。

【００２４】

図２では、ページディレクトリ２０２が、ページテーブル２０４（１）、２０４（２）、２０４（３）などのページテーブルへの一連のポインタ（すなわちページテーブルの物理ベースアドレス）を含む。各ページテーブルは、ページ（例えばページ２０６（１）、２０６（２）、２０６（３）、２０６（４））のベースアドレスへの一連のポインタを含み、さらに後述するように、読取り専用／読み書き可能属性や存在／非存在ビットなどの情報も含むことができる。ページは、ＲＡＭ１３２の固定長の部分である。さらに、通常はページディレクトリおよびページテーブルもＲＡＭ１３２に記憶される。図２に示すページング方式は２レベルのページング方式である。というのは、特定のページを突き止めるにはページディレクトリ（レベル１）とページテーブル（レベル２）の両方を通る必要があるからである。当業者には理解されるであろうが、任意のレベル数のページング方式を設計することが可能であり、本発明はこのようなすべてのページング方式に適用される。また、ＩＮＴＥＬ（登録商標）ｘ８６プロセッサは通常、図２に示す２レベルのページング方式を使用することが当技術分野で知られているが、１レベルまたは３レベルのページング方式を使用するように構成することもできる。

【００２５】

図２のページング方式では、ページ上のどのバイトも仮想アドレス２１０で識別することができ、仮想アドレス２１０は、ページディレクトリ（ＰＤ）オフセット２１１、ページテーブル（ＰＴ）オフセット２１２、およびページオフセット２１３を含む。したがって、物理アドレスを突き止めるためには、メモリ管理ユニット（ＭＭＵ）２２０が、ページディレクトリオフセット２１１を使用して、ページディレクトリ２０２中の特定のエントリを突き止める。このエントリはページテーブルの物理ベースアドレスであり、したがってＭＭＵ２２０は、このアドレスをデリファレンスして、ページテーブルのうちの１つ（例えばページテーブル２０４（１））を突き止める。次いでＭＭＵ２２０は、識別されたページテーブル中への索引としてページテーブルオフセット２１２を使用し、このオフセットで見つかったエントリを取り出す。このエントリはページ（例えばページ２０６（１））の物理ベースアドレスであり、したがってＭＭＵは、識別されたページのベースアドレスにページオフセット２１３を加えて、物理メモリの特定のバイトを突き止める。図３に関して後述するが、ＭＭＵ２２０はまた、ページが読取り専用としてマークされているか読み書き可能としてマークされているか、ページが存在としてマークされているか非存在としてマークされているかなどの情報を考慮するように構成することもできる。

【００２６】
図２のページング方式は、ページディレクトリへのポインタを含む記憶位置２０１も含む。ＭＭＵ２２０は、仮想アドレス２１０の変換を開始すると、このポインタを使用してページディレクトリ２０２を突き止める。ＩＮＴＥＬ（登録商標）ｘ８６プロセッサの例では、記憶位置２０１は、ＣＲ３という名前のレジスタに対応する。すなわち、ＩＮＴＥＬ（登録商標）ｘ８６プロセッサ上では、レジスタＣＲ３は、現在のコンテキストにおけるページディレクトリの物理アドレスを記憶する。したがって、変換テーブルの代替セット（すなわちページディレクトリとページテーブルの複数のセット）を構築することが可能であり、新しいページディレクトリのベースアドレスを記憶位置２０１に書き込むだけで、変換テーブルのどのセットが適用されるかを変更することが可能である。この技法の一般的な使用法の１つは、コンピュータ上で稼動している各プロセスがそれ自体のページディレクトリおよびページテーブルを有することであり、新しいプロセスのページディレクトリのベースアドレスを記憶位置２０１に書き込むことによって、「コンテキスト切替え」（すなわちとりわけ、仮想メモリシステムが新しいプロセスのアドレス空間をポイントするようにする操作）が実施される。各プロセスがそれ自体のページディレクトリを有する場合、現在稼動しているプロセスの識別が、記憶位置２０１にどの値がロードされるかを決定する。

【００２７】
ページへのポインタを含むことに加えて、ページテーブルおよびページディレクトリはまた、ページについて「属性」を含むこともできる。図３に例示的なページテーブル２０４（１）の詳細を示すが、これはポインタと属性の両方を含んでいる。ページテーブル２０４（１）中の各エントリは、特定のページのアドレス３０２と、エントリによってポイントされるページが「読取り専用」かどうかを示すビット３０４と、エントリによってポイントされるページが「存在」するかどうかを示すビット３０６とを含む。したがって、ページテーブル２０４（１）中の第１のエントリ３０１がページ２０６（１）（図２に示す）をポイントする場合、ビット３０４は、０にセットされているか１にセットされているかに応じて、ＭＭＵ２２０（図２に示す）がページ２０６（１）の読取りと書込みの両方を許容すべきか、読取りだけを許容すべきかを示す。同様に、ビット３０６は、ページ２０６（１）がメモリ中に存在するか否かを示す。（例えばページ２０６（１）の内容がディスクに移動されて、メモリ中に他のページのための空きができた場合、ビット３０６を０にセットして非存在を示すことができる。）その他の属性をページテーブル２０４（１）に記憶することもできる。

【００２８】
アドレス変換マップをメモリアクセス制御に使用する

仮想アドレスでメモリにアクセスするシステムでは、以下の観察に基づいてメモリへのアクセスを制限するシステムを実現することが可能である。すなわち、所与の物理アドレスに変換される仮想アドレスがないようにアドレス変換マップが構成された場合、この物理アドレスで表されるメモリにはアクセス不可能である。例えば、図２に関して上述したページング方式で、メモリの所与のページ（例えばページ２０６（１））は、マップを介してこのページに至るパスがないようにすることによって、アクセス不可能にすることができる。このようなパスがない場合、このページに変換される仮想アドレス２１０はないことになる。すべてのメモリアクセスが仮想アドレスによって行われるシステムでは、アドレス変換マップに対する制御を実施して、メモリの所与のページ（または他の部分）に仮想アドレスを与えないことにより、このメモリ部分は実質的にアクセス不可能になる。メモリに対してある物理アドレス指定が可能なシステムであっても、物理アドレスに基づくアクセス要求に対する制御で、アドレス変換マップに対する制御を補うことにより、メモリをアクセス不可能にすることができる。

【００２９】
アドレス変換マップの内容を制御してメモリへのアクセスを制御する技法は、正式には次のように述べることができる。メモリにアクセスできる可能性のあるソースの集合をＳ

とする。さらに、どのソースがどのメモリ部分にアクセスできるかを定義するポリシーをＰとする。したがって、ｓ∈Ｓがソースである場合、ＭＰ（ｓ）は、アドレス変換マップを介してソースｓからアクセス可能なメモリ部分（例えば仮想アドレスを有するメモリ位置の集合）を表し、ＮＡ（Ｐ，ｓ）は、ポリシーＰの下でソースｓからのアクセスが許可されないメモリ部分を表す。（各プロセスがそれ自体のアドレス変換マップを有する場合、各プロセスは異なる「ソース」と見なすことができる。ただしソースの概念はプロセスの例にとどまらず一般化されることは理解されるであろう。）したがって、ポリシーの施行は、以下の条件が満たされる限り保証することができる。

ＮＡ（Ｐ，ｓ）∩ＭＰ（ｓ）＝φ

【００３０】

この条件を図４に示す。図４には、メモリ位置の集合であるメモリ１３２と、アドレス変換マッピングを介してソースｓから見えるメモリ位置の集合であるＭＰ（ｓ）４０２と、ポリシーＰの下でソースｓからのアクセスが許可されないメモリ位置の集合であるＮＡ（Ｐ，ｓ）４０４が示されている。ソースｓがアドレス変換マッピングを介してアドレス指定できる位置（ＭＰ（ｓ））はどれも、ソースｓがポリシーＰの下でアクセス許可されないメモリ位置の集合には含まれないので、図４に示す条件は、ソースｓに関してポリシーＰを効果的に施行する。

【００３１】

したがって、ソースｓからメモリ１３２の部分へのアクセスを制御する問題は、いくつかの例示的な状況では、図４に示す条件が常に真であるようにすることに還元することができる。この問題に対する解決法の１つは、アドレス変換マッピングを変更する可能性のある任意の動作（例えばメモリ書込みやＣＲ３レジスタのロードなど）、ポリシー、または現在のソースを評価することである。本発明は、このような評価を効率的に実施できるようにする技法を提供する。

【００３２】

図４に示す条件は、メモリアクセス制御を実施するのに使用することのできる条件の例にすぎないことは理解されるであろう。図４の主題に対する他の変形も可能であり、例えば、アドレス変換マップに含まれるメモリ位置の集合や、ソースｓからのアクセスは許可されるが書込み（または読取り）は許可されないメモリ位置の集合などを含む変形が可能である。ただし、メモリアクセス制御に関する条件は一般に、複数のメモリ位置集合が交差しないことの検証を含むことに留意されたい。

【００３３】

さらに、ＭＰ（ｓ）は、ソースｓから見える「マッピングされるページ」と見なすことができるが、メモリアクセス制御の概念は、ページング方式を採用するシステムに限定されないことに留意されたい。典型的な一実装形態では、ポリシーの下でソースがどのメモリ位置に書き込むことができるか、またはどのメモリ位置がソースにマッピングされるかの決定は、ページごとに行われる。ただし本発明は、メモリがページごとに割り振られる場合、またはメモリへのアクセスがページごとに許可または制約される場合に限定されない。

【００３４】

アドレス変換に関する一般化モデル

図２に示すとともに上述したアドレス変換マップは、ラベル付き有向グラフのモデルを使用して一般化することができる。以下、いくつかのタイプのアドレス変換マップに関する一般化モデルについて述べる。

【００３５】

このモデルでは、Ｂはベース集合であり、Ｌは英字である。所与のＢおよびＬについて、Ｇ＝（Ｖ，Ｅ）はエッジラベル付き有向グラフであり、Ｖ⊆Ｂ、およびＥ⊆｛（ｖ，ｗ，ｌ）：ｖ∈Ｖ，ｗ∈Ｖ，ｌ∈Ｌ｝である。Ｅのメンバはどれも、ラベルｌの付いた、頂点ｖから頂点ｗへの有向エッジと解釈することができる。頂点にもラベル付けすることができる。

【００３６】
図５に、前述のモデルに従ったグラフを示す。グラフ５００は、頂点５０２、５０４、５０６、５０８、５１０、５１２を含む。これらの頂点は、図示のようにしてエッジ５２２、５２４、５２６、５２８、５３０、５３２、５３４で接続されている。各エッジは、英字からの記号でラベル付けされている。この例では、英字は記号Ａ、Ｂ、Ｃを含む。したがって、エッジ５２２および５２４は記号Ａでラベル付けされ、エッジ５２６、５２８、５３２は記号Ｂでラベル付けされ、エッジ５３０および５３４は記号Ｃでラベル付けされている。グラフ５００には、頂点ではないベース集合の要素（例えば要素５５０および５５２）がある場合もある。

【００３７】
グラフ５００の構成要素は、図２に示したアドレス変換マップのいくつかの構成要素に対応することを理解されたい。例えば図２で、ページディレクトリ２０２、ページテーブル２０４（１）～２０４（３）、およびページ２０６（１）～２０６（４）は、グラフ中の頂点と見なすことができる。これらの頂点を接続するポインタ（例えばページテーブル２０４（１）中のエントリからページ２０６（１）および２０６（２）へのポインタ）は、グラフ中のエッジと見なすことができる。また図３に関して、エントリの属性３０４および３０６（例えば読取り専用ビットや存在ビット）は、エッジのラベルと見なすことができる。したがって、「英字」は、可能な属性順列の集合である（２つの２進数属性がある図３の例では、４つの可能な組合せがあり、したがって英字には４つの記号がある）。属性が使用されない場合は、英字は「ｎｉｌ」記号からなるものとすることができる。さらに、割り振られないメモリページは、入来エッジを有さないベース集合メンバに対応する。

【００３８】
前述のようなグラフのモデル内では、「状態」を定義することが可能である。所与のＢおよびＬについて、「状態」は（Ｒ，Ｇ）の対であり、ここでＧは、上に定義したラベル付き有向グラフであり、Ｒ⊆Ｖは、Ｇの頂点の集合である。Ｒは、「ルート頂点」の集合を表す。ルート頂点は、グラフのルートとして正当に働くことのできる、ベース集合中の頂点の集合を表す。図２の例では、正当なページディレクトリの集合（すなわち、ＩＮＴＥＬ（登録商標）ｘ８６プロセッサ上のＣＲ３レジスタなどの記憶位置２０１にロードすることが許可されたそれらの値）が、「ルート頂点」の集合である。所与のＢおよびＬについて、すべての状態の集合はＳである。

【００３９】
上に定義したモデルに従って、アドレス変換機構（ＡＴＭ）を以下のようにモデル化することができる。
－頂点のベース集合Ｂ
－英字Ｌ（空の場合もある）
－初期状態$s_0 \in S$（Ｓは状態）
－状態遷移規則のセット（空の場合もある）
－アドレス変換関数
－グローバルフラグ

【００４０】
状態遷移規則は、ＡＴＭをある状態から別の状態に変更する。したがって、状態遷移規則のセット$r_i : S \rightarrow S$（ｉは何らかの指標）を定義することが可能であり、これはＡＴＭの現在状態を変更する。ＡＴＭは、以下のタイプの遷移規則のいずれかを有することができる。
－Ｇのエッジの変更（追加、削除、再ラベル付け）
－Ｇの頂点の追加または削除
－ルート集合Ｒの変更

【００４１】
例えば図２および３の例では、ページへのポインタを削除すること、またはページの属

性を変更することは、グラフのエッジの変更に対応する。新しいページディレクトリ、新しいページテーブル、または新しいデータページを追加することは、頂点の追加または削除に対応する。記憶位置２０１（例えばレジスタＣＲ３）にロードすることのできるベースアドレスを有する新しいページディレクトリを定義することは、ルート集合の変更に対応する。本質的に、現在状態は、アドレス変換によってどのメモリ位置にアクセスできる可能性があるかを定義する。

【００４２】

前述のように、ポリシーの下でソースからのアクセスが許容されないメモリ部分についてのどんな仮想アドレスもソースに露呈しないように、アドレス変換マップに対して制限条件を課すことによって、メモリへのアクセスを制御することができる。さらに、前述のように、条件の真偽に影響を与える可能性のある動作が実施されたとき、これらの条件が継続的に存在することを評価することができる。このメモリアクセス制御技法に対する考え方の１つは、ＡＴＭの正当な状態がＳの何らかの部分集合Ｔに限定されること、または現在状態に関する何らかのプロパティ（または述語）Ｐが常に真でなければならないことである。

【００４３】

何らかのプロパティＰ（前述のポリシーＰとは異なる）がある場合に、状態ｓからr_i（ｓ）に変更する可能性のあるアクション（何らかのｉの場合のr_iの実行）を実施するための要求を評価して、Ｐ（r_i（ｓ））が真であるかどうか、すなわち、r_iを実行することによって生じる新しい（提案）状態がプロパティＰを有することになるかどうかを判定することができる。Ｐが真であることが、メモリアクセスに対する制限に違反しないことを意味する場合、Ｐ（r_i（ｓ））が真であることは、r_iを実行することによって生じる状態変更を続行できるべきであることを意味する。そうでない場合は、この動作は続行できるべきではない。

【００４４】

あらゆるメモリ書込みはＡＴＭの状態を変更する可能性があることがわかるはずである。したがって、以下の２つのことがわかるはずである。

－アルゴリズムは、場合によっては頻繁に、Ｐ（ｓ）を計算しなければならない。

－通常、新しい状態ｓ’は古い状態ｓから派生する。古い状態がプロパティＰを有していた場合は、Ｐ（ｓ）を仮定し、ｓ’を生み出したｓに対する変更（有限数）がＰの違反につながるかどうかを分析するだけで、Ｐ（ｓ’）を決定する複雑さを低減することが可能な場合がある。

【００４５】

本発明は、Ｐの真偽を効率的に計算できるようにする技法を提供する。前述のように、多くの場合、この効率は、ＡＴＭの現在状態を表す何らかの情報を記憶（またはキャッシュ）することによって達成することができ、この情報を後で使用して、状態遷移の下におけるＰの真偽を確認するためにどんなテストを実施する必要があるか、およびどのテストを回避することができるかを決定することができる。

【００４６】

例示的なプロパティの種類

プロパティＰのタイプの１つは、頂点の集合で表すことができるプロパティである。例えば、図４に示すとともに上に論じた条件は、本質的に、集合ＭＰ（ｓ）とＮＡ（Ｐ，ｓ）が相互に交差しないプロパティである。頂点の集合およびこれらの集合間の関係で表すことのできる多くのプロパティは、集合中の頂点の識別を記憶（またはキャッシュ）することによって効率的に実装することができる。

【００４７】

ＡＴＭの状態がメモリアクセス制御条件を満たす状態にあるかどうかを評価する際に有用な集合の例を、以下に挙げる。

【００４８】

１．ルート頂点から距離ｋにある頂点の集合。より正式には、頂点の集合をＳとし、あ

る頂点をｗとした場合、d_k（Ｓ，ｗ）は、Ｓ中の何らかの頂点から頂点ｗまでに距離ｋの（有向）パスがあることのステートメントを表す。$S_d = \{v \in V : d_k(S, v)\}$である。この場合、Ｓがルート頂点である場合、$S_d$は、ルートから距離ｄにあるページの集合を指す。例えば、頂点５０２がグラフ５００のルートである場合、ルート頂点から距離１にある頂点の集合は、頂点５０４および５１０からなる。というのは、これらの頂点はどちらも、１つのエッジを横断することによってルートから到達することができるからである。図２に示したページマップを参照すると、ページディレクトリ２０２は、ルートからの距離１であり、ページテーブル２０４（１）から２０４（３）は、ルートからの距離２である。したがって図２の例では、ページディレクトリおよびページテーブルのアドレスは、ルートからの距離がそれぞれ１および２であるページの識別を記憶することによって、キャッシュすることができる。

【００４９】

２．エッジラベルによって判定される集合。例えば図５を参照すると、ラベル「Ａ」の付いた入エッジを有する頂点の集合は、頂点５０４および５１０からなり、ラベル「Ｂ」の付いた入エッジを有する頂点の集合は、頂点５０４、５０６、５１２からなる。図２のページマップでは、属性がエッジラベルに対応し、所与の属性を有するページとして集合を定義することができる。例えば、読取り専用としてマークされたページの集合を定義（およびキャッシュ）するのが有用なことがあるが、この場合、読取り専用ビット（図３に示した参照番号３０４）が「オン」になっているページの集合を定義することができる。（１つのページがページマップ中で複数回にわたって参照されることもあり得るが、その場合、ページへの異なる参照は、それらの読取り専用属性が個別にセットされているものとすることができる。この場合、集合の定義は競合を解決することができる。例えば、ページへの少なくとも１つの参照が読取り専用属性を有する場合や、ページへのあらゆる参照が読取り専用属性を有する場合などに、ページは集合に含まれる。）

ローカルプロパティと非ローカルプロパティとの間に区別を設けることができる。ローカルプロパティは、所与の頂点に入射するエッジから計算することができる。すなわち、頂点ｖがプロパティＰを有するかどうかを、ｖに入射するエッジだけから決定することが可能な場合、Ｐはローカルであると言う。そうでない場合は、Ｐは非ローカルである。ローカルプロパティの例は、「読み書き可能とラベル付けされた入エッジを頂点が有する」である。非ローカルプロパティの例は、「ページ（ｘ８６マシン上の）が読み書き可能マッピングを有する」である。

【００５０】

３．何らかのプロパティを有するｋ個のエッジのターゲットである頂点の集合。より正式には、Ｐ、Ｑを述語とし、ｗを頂点として、以下のように定められる。

$In\text{-}deg_{P,Q}(w) = |\{v \in V : P(v) \text{ および } (v, w, l) \in E \text{ および } Q(l)\}|$

【００５１】

所与の入次数（in-degree）を有する頂点の集合として集合を定義することができる。

$\{v \in V : In\text{-}deg_{P,Q}(v) = k\}$

【００５２】

同様に、不等式に基づいて集合を定義することもできる。例えば、何らかのプロパティを有するｋ個よりも多い（または少ない）エッジのターゲットである頂点の集合を定義することができる。

【００５３】

例えば図５を参照すると、「Ｃ」のラベルが付いた少なくとも１つの入エッジを有する頂点の集合は、頂点５０８および５１２からなる。図２のページマップを参照すると、このタイプの集合定義を使用して、いくつかのカテゴリのページをキャッシュすることができる。例えば、複数のマッピングを有するページの集合や、ちょうど１つの読出し専用マッピングを有するページの集合などである。

【００５４】

４．同様の集合を、出次数（out-degree）に基づいて定義することもできる。すなわち、何らかのプロパティを備えるｋ個の出エッジ（またはｋ個よりも多い出エッジか、ｋ個よりも少ない出エッジ）を有する頂点の集合である。例えば図５を参照すると、「Ａ」のラベルが付いたちょうど２つの出エッジを有する頂点の集合は、頂点５０２からなる。図２も類似の例を含む。例えば、少なくとも３つの出エッジ（他のページへの参照）を有するページの集合は、ページディレクトリ２０２を含む。

【００５５】

これらの集合を、通常の集合演算（例えば和、共通部分、補集合、集合差）によって結合することができる。例えば、ルートから距離２にあるページの集合をS_2とすると、一定構成のｘ８６ＣＰＵにおける読み書き可能マッピングを有するページの集合は、以下のように表すことができる。

（｛ｘ：ｘはラージページ入エッジを有する｝共通部分｛ｘ：ｘは読み書き可能入エッジを有する｝共通部分S_2）和

（｛ｘ：ｘはスモールページ入エッジを有する｝共通部分｛ｘ：ｘは読み書き可能マッピングを有する｝共通部分S_3）

【００５６】

ナイーブなアルゴリズムで、あらゆる頂点ｖを通ってそれが集合に属するかどうかをテストすることによって、状態変更時ごとにこれらの集合を再計算することもできる。これは高価であろう。述べたタイプの集合で表すことのできる状態プロパティをアルゴリズムで計算する場合、以下に述べるようなキャッシング方式を利用することができる。

【００５７】

キャッシング方式

状態変更を効率的に評価する際に使用するためのデータをキャッシュするために、様々な方式を使用することができる。例示的なキャッシング方式について以下に述べる。

【００５８】

方式１：単純な集合キャッシング

この方式では、集合を明示的に計算して記憶（キャッシュ）する。その後の状態変更のたびに、アルゴリズムはキャッシュを更新する。一例では、以下のアクセス演算を公開するキャッシュを維持することができる。

－Ｉｎｉｔ（）　空集合など、何らかの明確な値にキャッシュを初期化する。

－Ａｄｄ（Ｓ）　Ｓ（単一要素または要素集合）をキャッシュに加える。

－Ｒｅｍｏｖｅ（Ｓ）　Ｓ（単一要素または要素集合）をキャッシュから削除する。

－ＳｈｏｗＣａｃｈｅ（Ｓ）　現在キャッシュされているすべての要素を返す。

キャッシュは追加のアクセス演算を公開することもできる（例えば効率を高めるために）。

【００５９】

このようなキャッシュを表す方法の１つは、ビットベクトルによる方法である。例えば、システムが2^{16}個のメモリ物理ページを有する場合、2^{16}ビット長（すなわち８キロバイト）のベクトルが、各ページごとのブール値を表すことができる。定義された集合中にｎ番目のページがあるかどうかに応じて、ｎ番目のビットはオンとオフのどちらかをとる。したがって、定義されたページ集合について、１ページあたり１ビットのコストで集合中のメンバシップをキャッシュすることができる。このタイプの表現を使用すると、和や共通部分などの集合演算は、ビットごとの「ＯＲ」および「ＡＮＤ」演算子を使用して非常に単純に実施されることが理解されるであろう。

【００６０】

方式２：上位集合化、部分集合化

メモリアクセス制御を実施する基礎のアルゴリズムの詳細によっては、キャッシュが正確なターゲット集合を含む必要がない場合がある。例えば、ターゲット集合の何らかの上位集合または部分集合をキャッシュするだけで十分な場合がある。これにより、キャッシュを維持するコストを削減することができる。図３の例では、メモリアクセス制御条件は

、ＭＰ（ｓ）がＮＡ（Ｐ，ｓ）と交差しないことを要求する。しかし、ＮＡ（Ｐ，ｓ）の正確なメンバを計算するのが不都合であるか実際的でない場合は、ＮＡ（Ｐ，ｓ）の何らかの上位集合を計算してキャッシュし、次いで、ＭＰ（ｓ）が、計算したＮＡ（Ｐ，ｓ）の上位集合と交差しないことを保証することが可能である。この技法では、通常なら許容できる何らかの状態変更を拒否することになる場合があるが、禁じるべき状態変更は許容しないことになる。これにより、メモリアクセス制御のための条件が保存される。

【００６１】

方式３：反転エッジ表現

通常、エッジはソース頂点に記憶されるか、またはソース頂点と共に記憶される。例えば図２では、ページディレクトリおよびページテーブルは、他のページへのポインタ、ならびにそれらの属性を記憶する。所与の頂点について、すべての出エッジのターゲットを見つけるのは、通常は容易である。同時に、すべての入エッジのソースを見つけるのは、通常は高くつく。頂点はその入エッジに関する情報を持たないので、すべての入エッジを見つけるには、すべてのエッジの全数探索が必要である。

【００６２】

アルゴリズムが頂点の入エッジ、または入エッジから得られる情報に素早くアクセスする必要がある場合は、各頂点の入エッジに関する情報を、頂点に何らかの形で関連するデータ構造に明示的に記憶するのが有利であろう。「何らかの形で関連する」という言葉は、所与の頂点についてデータ構造（例えばアレイルックアップ）を容易に見つけられることを意味する。

【００６３】

最も極端な場合では、データ構造はすべての入エッジを記憶する。この場合、データ構造は、上に定義したような、エッジを要素とするキャッシュとすることができる。（また、キャッシュは集合または多重集合を記憶することもできる。）この構造が占める記憶域は、頂点の入エッジの数に比例し、このタイプの構造がすべての頂点について維持される場合、総記憶域はグラフ中のエッジの数に比例する。

【００６４】

派生情報を記憶すれば十分なことが多く、その方が、必要な記憶域は少ない。例えば、アルゴリズムは、各頂点の入エッジの数だけを記憶することができる。この場合、キャッシュは参照カウンタとして実装することができる。参照カウンタは通常、以下のアクセス演算を公開する。

－Ｉｎｉｔ（）　０など、何らかの明確な値にキャッシュを初期化する。
－Ｉｎｃｒｅｍｅｎｔ（）
－Ｄｅｃｒｅｍｅｎｔ（）
－ＧｅｔＶａｌｕｅ（）

【００６５】

参照カウンタ（または同様のデータ構造）の一般的な使用法の１つは、集合を構築することである。例えば、例示的なメモリアクセス制御アルゴリズムは、入エッジのない頂点の集合、すなわち参照カウントが０である頂点の集合を計算しなければならない場合がある。参照カウンタの集まりは、この集合のキャッシュ（方式１）を次のように制御することができる。すなわち、参照カウンタの値が変化したときは常に、アルゴリズムはそれが０になったかどうかをテストする。０になった場合は、頂点をキャッシュに加える。同様に、アルゴリズムは、０であった参照カウンタが別の値をとるイベントがあったかどうかも監視する。このイベントがあった場合、アルゴリズムは頂点をキャッシュから削除する。

【００６６】

以下は、いくつかのキャッシング使用例である。

－　ｄ＝１，２，３について、S_dの上位集合S_d'をキャッシュする。
－　ｄ＝２，３について、キャッシュを（ａ）明示的に記憶するか、（ｂ）参照カウンタによって駆動することができる。

－　ローカルラベルプロパティ「読み書き可能入エッジを有する」および「ラージ／スモールページ入エッジを有する」を計算する。

－　非ローカルプロパティ「読み書き可能マッピングを有する」を計算する。

－　S_2中の頂点の読み書き可能入エッジの数について、参照カウンタを使用する。この情報を使用して、非ローカルプロパティ「読み書き可能マッピングを有する」の計算を加速することができる。

【００６７】

記憶済み情報を使用した例示的なメモリアクセス制御プロセス

図６に、本明細書に述べた技法を使用した、メモリアクセス制御を実施するための例示的なプロセスを示す。

【００６８】

最初に、メモリにアクセスするための要求を受け取る（６０２）。アクセス要求が受け取られると、メモリアクセス制御システムが要求を評価して、メモリアクセスを統制するポリシーに要求の実行が適合するかどうかを判定する（６０４）。メモリアクセスポリシーの例は、上に論じたものである。一例としてポリシーは、ソースの集合に対していくつかのページを立入り禁止と定義することができ、ポリシーは、立入り禁止ページの１つに対して、このページへのアクセスを許可されていないソースの１つから見えるマッピングを生み出すことになるアクセス要求は、どれも禁止することができる。要求の評価は、記憶済みまたはキャッシュ済み情報（６０６）の助けを借りて行うことができる。この記憶済みまたはキャッシュ済み情報は、ページマップに関する情報、例えば正当なページディレクトリを含むことがわかっているページの集合を含むものとすることができる。

【００６９】

要求を実施してもポリシーとの適合が維持されると判定された場合（６０８）は、要求の続行を可能にする（６１２）。そうでない場合は、要求を阻止するか、ポリシーに違反しない形に修正する（６１０）。要求をポリシーに違反しない形に修正することの一例は、次のとおりである。要求が、ページテーブルにエントリを書き込むことを求めており、その結果として立入り禁止ページにマッピングすることになる場合は、この要求を修正して、エントリは書き込まれるが「存在」ビットはオフになるようにすることができる。このため、新たにマッピングされたページに以後アクセスしようとしても、例外が生成されることになり、したがって最終的には例外ハンドラが立入り禁止ページへのアクセスを妨げることができる。このように（または他の何らかのやり方で）要求を修正した場合、修正済み要求の続行を可能にする（６１４）。修正済みまたは未修正の要求が実施された後、要求の実施によってキャッシュ済み情報が変更される場合は、キャッシュを更新することができる（６１６）。

【００７０】

以上の例は単に説明のために提供したものであり、本発明を限定するものと考えるべきでは決してないことに留意されたい。本発明を様々な実施形態に関して述べたが、本明細書で使用した言葉は、限定の言葉ではなく記述および例示の言葉であることを理解されたい。さらに、本発明を特定の手段、材料、および実施形態に関して本明細書に述べたが、本発明は、本明細書に開示した詳細に限定されるものではない。そうではなく本発明は、添付の特許請求の範囲に含まれるものなど、機能的に均等なあらゆる構造、方法、および使用に及ぶ。本明細書の教示があれば、当業者なら、多くの修正を実施することができ、本発明の範囲および趣旨を逸脱することなくその態様に変更を加えることができる。

【図面の簡単な説明】

【００７１】

【図１】本発明を適用できる実施形態のコンピューティング環境のブロック図である。

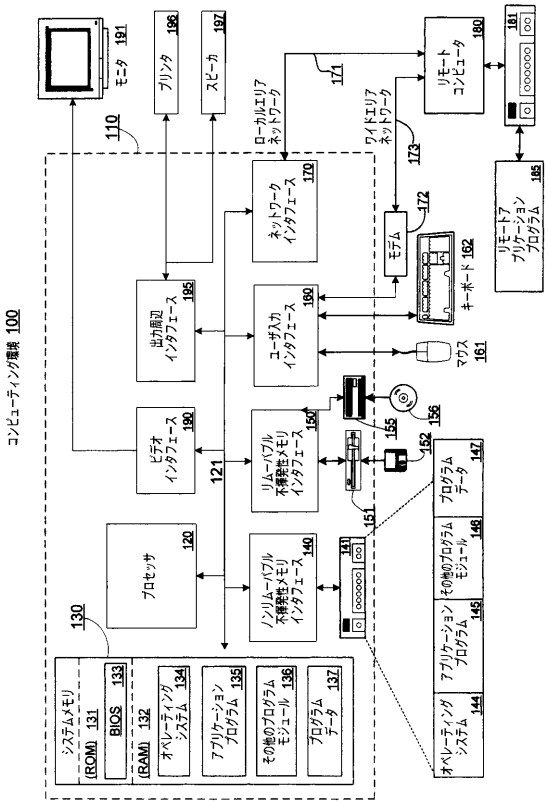
【図２】本発明を適用できる実施形態のアドレス変換マップを介して仮想アドレス指定を実施するメモリシステムのブロック図である。

【図３】本発明を適用できる実施形態の属性を有する例示的なページテーブルのブロック図である。

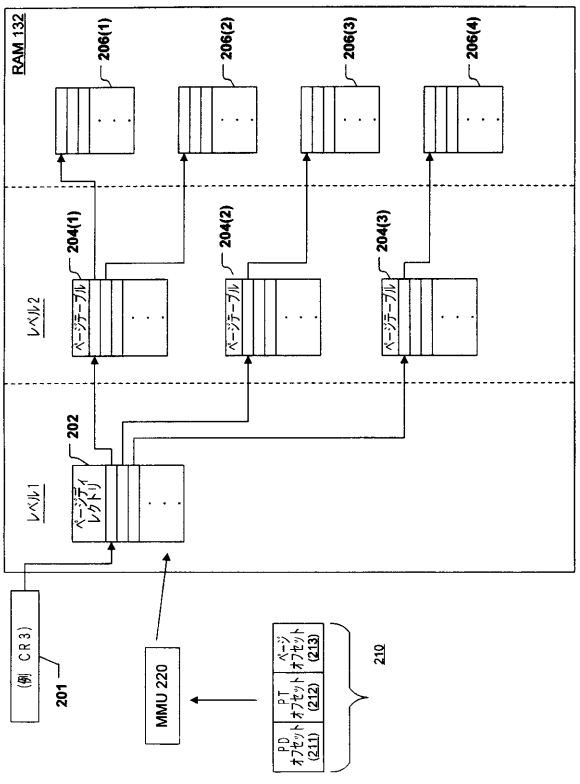
【図４】本発明を適用できる実施形態のメモリアクセス制御を実施するのに使用できる条件を表す、２つの例示的な交差しない集合のブロック図である。
【図５】本発明を適用できる実施形態のアドレス変換マップを表す、ラベル付き有向グラフのブロック図である。
【図６】本発明を適用できる実施形態の例示的なメモリアクセス制御プロセスの流れ図である。
【符号の説明】
【００７２】
１００　コンピューティング環境
１１０　コンピュータ
１２０　プロセッサ
１２１　システムバス
１３０　システムメモリ
１３１　読取り専用メモリ（ＲＯＭ）
１３２　ランダムアクセスメモリ（ＲＡＭ）
１３３　ＢＩＯＳ
１３４　オペレーティングシステム
１３５　アプリケーションプログラム
１３６　その他のプログラムモジュール
１３７　プログラムデータ
１４０　ノンリムーバブル不揮発性メモリインタフェース
１４１　ハードディスクドライブ
１４４　オペレーティングシステム
１４５　アプリケーションプログラム
１４６　その他のプログラムモジュール
１４７　プログラムデータ
１５０　リムーバブル不揮発性メモリインタフェース
１５１　磁気ディスクドライブ
１５２　磁気ディスク
１５５　光ディスクドライブ
１５６　光ディスク
１６０　ユーザ入力インタフェース
１６１　ポインティングデバイス
１６２　キーボード
１７０　ネットワークインタフェース
１７１　ローカルエリアネットワーク（ＬＡＮ）
１７２　モデム
１７３　ワイドエリアネットワーク（ＷＡＮ）
１８０　リモートコンピュータ
１８１　メモリ記憶デバイス
１８５　リモートアプリケーションプログラム
１９０　ビデオインタフェース
１９１　モニタ
１９５　出力周辺インタフェース
１９６　プリンタ
１９７　スピーカ
２０１　記憶位置
２０２　ページディレクトリ
２０４（１）、２０４（２）、２０４（３）　ページテーブル
２０６（１）、２０６（２）、２０６（３）、２０６（４）　ページ

２１０　仮想アドレス
２１１　ページディレクトリオフセット
２１２　ページテーブルオフセット
２１３　ページオフセット
２２０　メモリ管理ユニット（ＭＭＵ）
３０１　第１のエントリ
３０２　アドレス
３０４　ページが「読取り専用」かどうかを示すビット
３０６　ページが「存在」するかどうかを示すビット
４０２　ソースｓから見えるメモリ位置の集合ＭＰ（ｓ）
４０４　ポリシーＰの下でソースｓからのアクセスが許可されないメモリ位置の集合ＮＡ（Ｐ，ｓ）
５００　グラフ
５０２、５０４、５０６、５０８、５１０、５１２　頂点
５２２、５２４、５２６、５２８、５３０、５３２、５３４　エッジ
５５０、５５２　頂点ではない要素

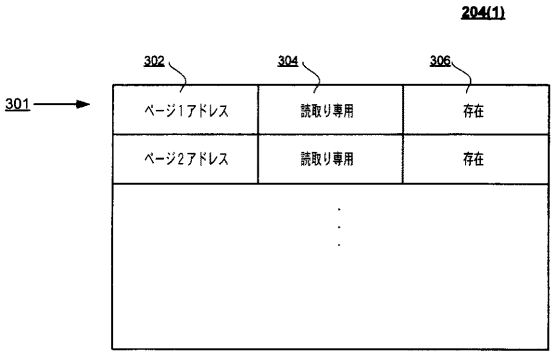
【図１】



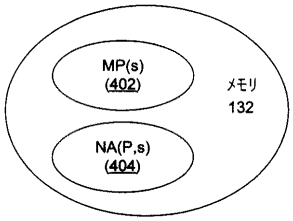
【図２】



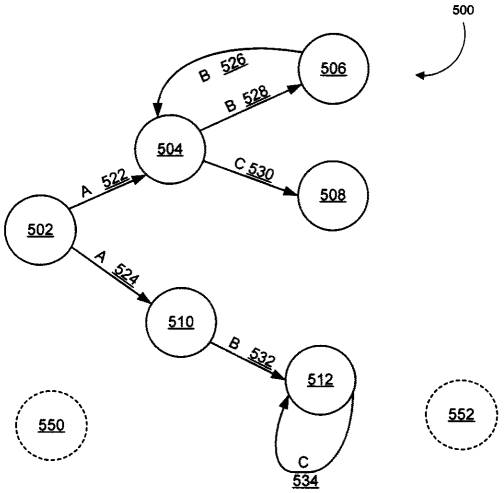
【図３】


204(1)
301
302
304
306
ページ1アドレス
読取り専用
存在
ページ2アドレス
読取り専用
存在

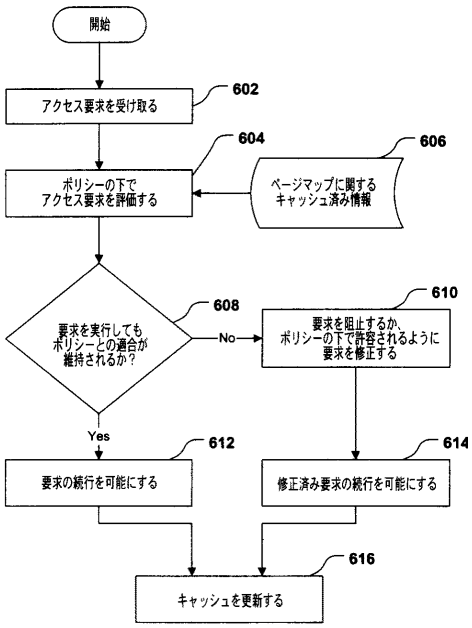
【図４】


MP(s)
(402)
NA(P,s)
(404)
メモリ
132

【図５】


500
502
504
506
508
510
512
550
552
A 522
A 524
B 526
B 528
C 530
B 532
C 534

【図６】


開始
アクセス要求を受け取る
602
ポリシーの下で
アクセス要求を評価する
604
ページマップに関する
キャッシュ済み情報
606
要求を実行しても
ポリシーとの適合が
維持されるか?
608
No
要求を阻止するか、
ポリシーの下で許容されるように
要求を修正する
610
Yes
要求の続行を可能にする
612
修正済み要求の続行を可能にする
614
キャッシュを更新する
616

フロントページの続き

(72)発明者　ポール　イングランド
アメリカ合衆国　９８００８　ワシントン州　ベルビュー　ノーサップ　ウェイ　１６６５９

審査官　前田　浩

(56)参考文献　特開２０００－３５３１２７（ＪＰ，Ａ）
米国特許出願公開第２００２／０１４４０７７（ＵＳ，Ａ１）
米国特許出願公開第２００２／０１１６５９０（ＵＳ，Ａ１）
特開平０７－３１９７３５（ＪＰ，Ａ）
特開平０２－０５６６５３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１２／１４