【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成18年12月28日(2006.12.28)

【公開番号】特開2005-158040(P2005-158040A)
【公開日】平成17年6月16日(2005.6.16)
【年通号数】公開・登録公報2005-023
【出願番号】特願2004-304748(P2004-304748)
【国際特許分類】
Ｇ０６Ｆ　12/10　(2006.01)
Ｇ０６Ｆ　12/14　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/10　５０１Ｂ
Ｇ０６Ｆ　12/10　５４１
Ｇ０６Ｆ　12/10　５５１Ｂ
Ｇ０６Ｆ　12/14　５１０Ｅ

【手続補正書】
【提出日】平成18年11月10日(2006.11.10)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
複数のマッピング・キャッシュであって、それぞれが、コンピューティング装置の複数の処理装置のうちの対応する１つに関連付けられ、仮想アドレスを物理アドレスに変換するために使用され、アドレス変換マップに基づいてマッピングを記憶する、前記複数のマッピング・キャッシュのうちの第１のマッピング・キャッシュから古くなったエントリをクリアする方法であって、当該方法は、
カウンタを保持すること、
前記複数のマッピング・キャッシュのうちの前記第１のマッピング・キャッシュをフラッシュするたびに前記カウンタを更新すること、
前記アドレス変換マップ中の変更に応答して前記カウンタ値を記録し、記録されたカウンタ値を格納すること、
前記カウンタ値と前記記録済みのカウンタ値との比較に基づいて、前記アドレス変換マップ中の前記変更が行われて以来、前記複数のマッピング・キャッシュのうちの前記第１のマッピング・キャッシュが必ずしも確実にフラッシュされていないことを決定すること、および
前記複数のマッピング・キャッシュのうちの前記第１のマッピング・キャッシュをフラッシュすること
を備え、この方法ではポリシーがメモリに対する許容可能なアクセスを定義し、前記方法は、さらに、
エンティティが前記ポリシーに違反して前記メモリにアクセスできるようにする仮想アドレス・マッピングを、前記アドレス変換マップが前記エンティティに対してさらされないように前記アドレス変換マップのコンテンツを制御することを備え、
前記変更は、
前記ポリシーに一致する前記マップを置くかあるいは保持する、前記アドレス変換マップに対する修正、あるいは

前記マップに対する前記エンティティの書込みアクセスを制限する、前記アドレス変換マップに対する修正
を備えることを特徴とする方法。
【請求項２】
前記アドレス変換マップは、前記メモリの一部分に対するリンクを備え、前記アドレス変換マップのコンテンツを制御することは、前記メモリの前記一部分を前記エンティティからアクセス不可能にすることを備え、前記変更は、前記メモリの前記一部分に対するすべてのリンクを前記アドレス変換マップから取り除くことを備えることを特徴とする請求項１に記載の方法。
【請求項３】
マッピング・キャッシュおよびそれに関連するカウンタを有する複数のプロセッサと、
前記各マッピング・キャッシュがそれに基づいてマッピングを格納するアドレス変換マップを格納するメモリであって、該メモリに対するアクセスを管理するポリシーが存在し、該ポリシーに違反して前記メモリへのアクセスを可能にするマッピングについての露出を防止するように、そのコンテンツが制御される、前記アドレス変換マップ、を記憶するメモリと、
前記マッピング・キャッシュのうちの第１のマッピング・キャッシュをフラッシュし、前記マッピング・キャッシュのうちの前記第１のマッピング・キャッシュがフラッシュされると前記カウンタのうちの第１のカウンタを増分する、第１のロジックと、
前記アドレス変換マップ中または前記アドレス変換マップに関するプロパティ中の変更に応答して前記第１のカウンタの値を記録する第２のロジックであって、前記記録済みのカウンタ値が前記変更に関連して記憶される第２のロジックと、
前記記録済みのカウンタ値を前記第１のカウンタの現在の値と比較し、前記比較により、前記変更以来、前記マッピング・キャッシュのうちの前記第１のマッピング・キャッシュがフラッシュされていないことが示される場合には、前記マッピング・キャッシュのうちの前記第１のマッピング・キャッシュをフラッシュするようにする第３のロジックと
を備えることを特徴とするアドレス・マッピング・キャッシュの使用を管理するシステム。
【請求項４】
前記各プロセッサは、前記カウンタのうちの前記第１のカウンタに関連付けられ、前記第１のロジックは、前記マッピング・キャッシュのうちのどれかがフラッシュされるときに前記カウンタのうちの前記第１のカウンタを増分することを特徴とする請求項３に記載のシステム。
【請求項５】
前記各マッピング・キャッシュは、複数のカウンタのうちの異なるカウンタに関連付けられ、前記第１のロジックは、所与のマッピング・キャッシュがフラッシュされるときに前記所与のマッピング・キャッシュに対応する前記カウンタを増分することを特徴とする請求項３に記載のシステム。
【請求項６】
前記変更は、前記メモリの第１のページに対するすべてのリンクが前記アドレス変換マップから取り除かれる状態に前記アドレス変換マップを置くことを備えることを特徴とする請求項３に記載のシステム。
【請求項７】
前記変更は、前記メモリの第１のページに対する書込み可能リンクがない状態に前記アドレス変換マップを置くことを備えることを特徴とする請求項３に記載のシステム。
【請求項８】
前記第３のロジックは、前記変更の結果を使用すべきことを検出するのに応答して呼び出されることを特徴とする請求項３に記載のシステム。
【請求項９】
前記変更は、前記メモリの第１のページに対するすべてのリンクが前記アドレス変換マ

ップから取り除かれる状態に前記アドレス変換マップを置くことを備え、前記検出は、仮想アドレスが前記第１のページ上のロケーションに変換されていることに基づくものであることを特徴とする請求項８に記載のシステム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】変更
【補正の内容】
【００２５】
このページング・スキームにおいて、ページ・ディレクトリ２０２は、１組のエントリを含んでいる。図３に関して以下でエントリの構造の一例をより詳細に説明するが、本質的には、各エントリは、ページ・テーブル２０４（１）、２０４（２）、２０４（３）など特定のページ・テーブルの物理ロケーション（すなわち、ページ・フレーム番号すなわち「ＰＦＮ」）を識別する。各ページ・テーブルは、やはり１組のエントリを含んでおり、ここで各エントリは、物理ロケーション（この場合にも、ページ・フレーム番号）、すなわちページ２０６（１）、２０６（２）、２０６（３）、２０６（４）などの特定のデータ・ページを識別する。データ・ページは、既定の長さの隣接するＲＡＭ１３２の一部分である。データ・ページは、任意のタイプのデータを記憶することができ、通常のデータを記憶するのに加えてデータ・ページを使用してページ・ディレクトリ２０２およびページ２０４（１）ないし２０４（３）のコンテンツ（contents）を記憶することもあることに留意されたい。したがって、所与のページは、ディレクトリ、テーブル、データ・ページとすることができ、またこれら３つの構造の任意の組合せとしての複合的な役割を果たすことができる。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】変更
【補正の内容】
【００２８】
図２の仮想アドレス・スキームでは、ページ・ディレクトリそれ自体のロケーション（すなわち、ＰＦＮ）は、記憶ロケーション２０１に記憶される。ＭＭＵ２２０は、仮想アドレス２１０を変換し始めると、この記憶ロケーションのコンテンツ（contents）を使用してページ・ディレクトリ２０２を位置決めする。したがって、複数のページ・マップが存在することができ、記憶ロケーション２０１のコンテンツを設定して所与のマップのページ・ディレクトリのＰＦＮを含むようにすることによって現在使用するために特定のマップを選択することができる。ＩＮＴＥＬｘ８６プロセッサの例では、記憶ロケーション２０１は、ＣＲ３と名付けられたレジスタに対応する。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００３４
【補正方法】変更
【補正の内容】
【００３４】
好ましい実施形態では、ハイ・アシュアランス環境は、Ｃｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ、すなわち、非ハイ・アシュアランス環境からはアクセス不可能であるメモリの一部分を含んでいる。したがって、ＲＨＳ３６０は、ＬＨＳ３５０の下で実行されるプロセスが読み取りまたは書き込む危険なしに、Ｃｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ中に機密データ（例えば、暗号キー）を記憶することができる。例えば、仕様３０４は、外部からの改ざん（outside tampering）からＲＨＳ３６０が情報を保護する機能を有し、Ｃｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙによって、ＲＨＳ３６０がこの機能を実施できるようにすること

ができる。さらに、ＲＨＳ３６０がその様々なファンクションを実施するために使用するコードをこのＣｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ中に記憶して、ＬＨＳ３５０の下で実行されるプロセスがこのコードに異なるコード（それによって、ＲＨＳ３６０がその仕様外で振る舞うようになることもある）を上書きしないように防止することができる。図３は、ＲＨＳ３６０が使用する場合には使用可能なＣｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ３１２を示している。物理アドレス空間３１０は、所与のコンピューティング装置上で使用可能な物理メモリ・ロケーションのすべてを含んでいる。Ｃｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ３１２は、これらのロケーションのサブセットである。図３に示すように、ＲＨＳ３６０は、物理アドレス空間３１０のすべてにアクセスできるが、ＬＨＳ３５０は、物理アドレス空間３１０の、Ｃｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ３１２を構成する一部分に対するアクセスができない。（図３は、アドレス空間のＣｕｒｔａｉｎｅｄ部分（他から見えないようにされた部分）およびＮｏｎ－Ｃｕｒｔａｉｎｅｄ部分（他から見えないようにされていない部分）をそれぞれが隣接するものとして示しているが、このように隣接している必要はない。さらに必ずしも、ＲＨＳ３６０が物理アドレス空間全体にアクセスできる必要はなく、またＬＨＳ３５０がＣｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ３１２の外側にある、物理アドレス空間のあらゆる部分にアクセスできる必要もない。）

以上で指摘したように、ほとんどすべてのメモリ・アクセス要求が物理アドレスによって行われるある種のシステムが存在する。かかるシステム上でＣｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ３１２を実装する一方法は、Ｃｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ３１２についての仮想アドレスがＬＨＳ３５０に露出されない（さらされない）ような方法で、アドレス変換マップのコンテンツ（contents）を制御する方法である（あるタイプのアクセス要求が、それらのターゲットを物理アドレスによって識別する可能性がある場合には、ダイレクト・メモリ・アクセス装置または他のソースからの物理的なアクセス要求をフィルタリングする排他ベクトル（exclusion vector）など、何らかの補助的な協働メカニズムによって、Ｃｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙへのアクセスを制限することができる。）。ＬＨＳ３５０が、Ｃｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ３１２へと至るはずのアドレス変換マップを使用できないことを保証するいくつかのアルゴリズムが使用可能であるが、これらのアルゴリズムの背後における中心的なアイデアは、（１）プロセッサがＬＨＳ３５０で動作しているとき、ＣＲ３（図２に示す記憶ロケーション２０１）にロードされたマップはどれも、Ｃｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ３１２に含まれるページには至らないようにする、（２）ＬＨＳ３５０中のアクティブなマップを編集するどのような試みに対しても、提案された編集を評価して、その編集がＣｕｒｔａｉｎｅｄ Ｍｅｍｏｒｙ３１２のページに至るリンクをもたらさないように保証することである。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００４１
【補正方法】変更
【補正の内容】
【００４１】

ＡＴＣシステム中でＴＬＢを使用する際には、ＴＬＢを介して使用可能な変換を考慮に入れるためにこのＡＴＣのインバリアントを修正する。例えば、以前に説明したＡＴＣアルゴリズムの例では、リンクの定義を以下のように修正することができる。すなわち、あるページから別のページへのリンクは、物理メモリ中に存在する場合、または何らかのＴＬＢにキャッシュされている場合、に存在する。ＴＬＢのコンテンツは、たいていのアーキテクチャ（例えばｘ８６プロセッサ）では直接見ることができないが、変換はメモリを介してのみＴＬＢに入力されるので、そのコンテンツをバインドすることができる。このアルゴリズム例においてそのインバリアントを使用すると、Ｄ１またはＤ２からページを取り除いて、ページに対する読取りアクセスまたは読取り書込みアクセスを放棄し、およびＤ２に対して、ページのステイタス（状態）を書込みアクティブから書込み非アクティブに、またはその逆へと変更する書込みまたは追加をし、次いでこのＴＬＢをフラッシュ

する必要がある。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００５５
【補正方法】変更
【補正の内容】
【００５５】
プロセッサＹがＲＨＳ３６０中で実行される場合（６１０）には、ＴＬＢは、そのアクセス・ポリシーに違反することなくページＸに対するマッピングを含むことができ、したがって、ページＸに対するアクセスが許容される（６１４）。しかし、プロセッサＹがＬＨＳ３５０中で実行されている場合（および、ページＸが切り離されて以来、プロセッサＹがそのＴＬＢをフラッシュしていないことが、６０８から知られている場合）、プロセッサＹのＴＬＢのコンテンツ（contents）がＬＨＳ３５０に対してページＸへのマッピングを露出する（さらす）ことになる可能性がある。したがって、プロセッサＹは、ＲＨＳ３６０に入りそのＴＬＢをフラッシュする（６１２）。ＴＬＢがフラッシュされた後、プロセッサＹは、ＬＨＳ３５０へと戻り、そのアクセス要求が再実行される（６１４）（それによってその要求されたアドレスをこの新しい空のＴＬＢを用いて再変換することが必要になる）。