(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6301378号
(P6301378)

(45)発行日　平成30年3月28日(2018.3.28)　(24)登録日　平成30年3月9日(2018.3.9)

(51)Int.Cl.　F I

G06F 12/10 (2016.01)	G06F	12/10	509B
G06F 12/14 (2006.01)	G06F	12/10	553Z
	G06F	12/10	505B
	G06F	12/10	501F
	G06F	12/14	510E

請求項の数 15　(全 18 頁)

(21)出願番号　特願2015-561522(P2015-561522)
(86)(22)出願日　平成26年3月4日(2014.3.4)
(65)公表番号　特表2016-513836(P2016-513836A)
(43)公表日　平成28年5月16日(2016.5.16)
(86)国際出願番号　PCT/US2014/020185
(87)国際公開番号　WO2014/138005
(87)国際公開日　平成26年9月12日(2014.9.12)
審査請求日　平成29年2月9日(2017.2.9)
(31)優先権主張番号　13/785,979
(32)優先日　平成25年3月5日(2013.3.5)
(33)優先権主張国　米国(US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　トーマス・ゼン
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】ハードウェアテーブルウォーク（HWTW）を実行する際にいくつかの条件下でレジスタの内容に対する許可のないアクセスを防止するための方法および装置

(57)【特許請求の範囲】

【請求項１】

ハードウェアテーブルウォーク(HWTW)の実行中にコンピュータシステムの記憶要素にロードされている物理アドレス(PA)の内容に対する許可のないアクセスを防止するための前記コンピュータシステムの装置であって、

前記PAの前記内容がないか変換ルックアサイドバッファ(TLB)を調べている際にミスが生じた場合、中間物理アドレス(IPA)および一意の仮想マシン識別子のオフセット関数の関数としてPAを決定する決定アルゴリズムが現在、イネーブルにされているか否かを判定するように構成されたセキュリティ論理手段を備え、前記セキュリティ論理手段は、前記セキュリティ論理手段が、前記決定アルゴリズムが現在、イネーブルにされていると判定した場合、前記記憶要素の前記内容に、特権のないエンティティによってアクセスが行われることを防止するように構成される装置。

【請求項２】

前記記憶要素は、前記決定アルゴリズムが現在、イネーブルにされている場合、前記決定されるPAの前記内容がロードされている前記TLBのレジスタであり、前記セキュリティ論理手段は、

前記決定アルゴリズムが現在、イネーブルにされているか否かの前記判定を行う第1の判定論理手段であって、特権のあるエンティティが前記レジスタの前記内容にアクセスしようと試みているか、特権のないエンティティが前記レジスタの前記内容にアクセスしようと試みているかも判定し、前記第1の判定論理手段が、前記決定アルゴリズムが現在、

イネーブルにされており、かつ特権のあるエンティティが前記レジスタの内容にアクセスを得ようと試みていると判定した場合、第1の判定を出力し、前記決定アルゴリズムが現在、イネーブルにされていない、または特権のないエンティティが前記レジスタの内容にアクセスを得ようと試みていると判定した場合、第2の判定を出力する第1の判定論理手段と、

前記第1の判定論理手段が、前記第2の判定を出力した場合、前記レジスタの前記内容にマスク値が上書きされるようにするように構成された選択論理手段であって、前記第1の判定論理手段が前記第1の判定を出力した場合、前記レジスタの前記内容を保存するように構成される選択論理手段とを備える請求項1に記載の装置。

【請求項３】

前記セキュリティ論理手段は、

前記PAが、メインメモリのセキュリティ保護された部分に対応するか否か、もしくはセキュリティで保護されていない部分に対応するか否か、または前記第1の判定論理手段が、前記第1の判定を出力したか否か、もしくは前記第2の判定を出力したか否かを判定するように構成された第2の判定論理手段をさらに備え、前記第2の判定論理手段が、前記PAがメインメモリのセキュリティ保護された部分に対応すると判定した場合、前記第2の判定論理手段は、第1の判定を出力し、前記第2の判定論理手段が、前記PAがメインメモリのセキュリティ保護されていない部分に対応する、または前記第1の判定論理手段が前記第2の判定を出力したと判定した場合、前記第2の判定論理手段は、第2の判定を出力し、

前記選択論理手段は、前記第2の判定論理手段が前記第1の判定を出力した場合、前記レジスタの前記内容がマスクされるようにするように構成され、前記選択論理手段は、前記第2の判定論理手段が前記第2の判定を出力した場合、前記レジスタの前記内容を保存するように構成される請求項2に記載の装置。

【請求項４】

前記セキュリティ論理手段は、前記コンピュータシステムのメモリ管理ユニット(MMU)の一部である請求項1に記載の装置。

【請求項５】

前記MMUは、前記コンピュータシステムの中央処理装置(CPU)の一部である請求項4に記載の装置。

【請求項６】

前記CPUは、前記コンピュータシステムのCPUクラスタの一部である請求項5に記載の装置。

【請求項７】

前記コンピュータシステムは、モバイル電話機の一部である請求項1に記載の装置。

【請求項８】

ハードウェアテーブルウォーク(HWTW)の実行中にコンピュータシステムの記憶要素にロードされている物理アドレス(PA)の内容に対する許可のないアクセスを防止するために前記コンピュータシステムにおいて実行される方法であって、

セキュリティ論理手段を提供するステップと、

前記セキュリティ論理手段を用いて、前記PAの前記内容がないか変換ルックアサイドバッファ(TLB)を調べている際にミスが生じた場合、中間物理アドレス(IPA)および一意の仮想マシン識別子のオフセット関数の関数としてPAを決定する決定アルゴリズムが現在、イネーブルにされているか否かを判定するステップとを備え、

前記セキュリティ論理手段が、前記決定アルゴリズムが現在、イネーブルにされていると判定した場合、前記セキュリティ論理手段は、前記記憶要素の前記内容に、特権のないエンティティによってアクセスが行われることを防止する方法。

【請求項９】

前記記憶要素は、前記決定アルゴリズムが現在、イネーブルにされている場合、前記決定されるPAの前記内容がロードされている前記TLBのレジスタである方法であって、

前記セキュリティ論理手段の第1の判定論理手段を用いて、前記決定アルゴリズムが現

在、イネーブルにされているか否かの前記判定を行うステップであって、前記第1の判定論理手段は、特権のあるエンティティが前記レジスタの前記内容にアクセスしようと試みているか、特権のないエンティティが前記レジスタの前記内容にアクセスしようと試みているかも判定するステップと、

前記第1の判定論理手段を用いて、前記第1の判定論理手段が、前記決定アルゴリズムが現在、イネーブルにされており、かつ特権のあるエンティティが前記レジスタの内容にアクセスを得ようと試みていると判定した場合、第1の判定を出力するステップと、

前記第1の判定論理手段を用いて、前記決定アルゴリズムが現在、イネーブルにされていない、または特権のないエンティティが前記レジスタの内容にアクセスを得ようと試みていると判定した場合、第2の判定を出力するステップと、

前記セキュリティ論理手段の選択論理手段を用いて、前記第1の判定論理手段が、前記第2の判定を出力した場合、前記レジスタの前記内容にマスク値が上書きされるようにすることによって、前記レジスタの前記内容にアクセスが行われるのを防止するステップと、

前記選択論理手段を用いて、前記第1の判定論理手段が前記第1の判定を出力した場合、前記レジスタの前記内容を保存するステップとをさらに備える請求項8に記載の方法。

【請求項１０】

前記セキュリティ論理手段の第2の判定論理手段を用いて、前記PAが、メインメモリのセキュリティ保護された部分に対応するか否か、もしくはセキュリティで保護されていない部分に対応するか否か、または前記第1の判定論理手段が、前記第1の判定を出力したか否か、もしくは前記第2の判定を出力したか否かを判定するステップと、

前記第2の判定論理手段を用いて、前記第2の判定論理手段が、前記PAがメインメモリのセキュリティ保護された部分に対応すると判定した場合、前記第2の判定論理手段から第1の判定を出力するステップと、

前記第2の判定論理手段を用いて、前記第2の判定論理手段が、前記PAがメインメモリのセキュリティ保護されていない部分に対応する、または前記第1の判定論理手段が前記第2の判定を出力したと判定した場合、前記第2の判定論理手段から第2の判定を出力するステップと、

前記選択論理手段を用いて、前記第2の判定論理手段が前記第1の判定を出力した場合、前記レジスタの前記内容がマスクされるようにするステップと、

前記選択論理手段を用いて、前記第2の判定論理手段が前記第2の判定を出力した場合、前記レジスタの前記内容が保存されるようにするステップとをさらに備える請求項9に記載の方法。

【請求項１１】

前記セキュリティ論理手段は、前記コンピュータシステムのメモリ管理ユニット(MMU)の一部である請求項8に記載の方法。

【請求項１２】

前記MMUは、前記コンピュータシステムの中央処理装置(CPU)の一部である請求項11に記載の方法。

【請求項１３】

前記CPUは、前記コンピュータシステムのCPUクラスタの一部である請求項12に記載の方法。

【請求項１４】

前記コンピュータシステムは、モバイル電話機の一部である請求項8に記載の方法。

【請求項１５】

請求項８～１４のいずれか一項に記載の方法を実行するための命令を含むコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コンピュータシステムに関し、より詳細には、ハードウェアテーブルウォーク(HWTW)中に、レジスタにロードされている物理メモリアドレスの内容に対する許可のないアクセスを、いくつかの条件下で防止するための方法および装置に関する。

【背景技術】

【０００２】

最新のコンピュータシステムは、メモリ管理ユニット(MMU)を使用して、たとえば、ソリッドステートメモリデバイスなどの1つまたは複数の物理メモリデバイスにデータを書き込むこと、およびそのような物理メモリデバイスからデータを読み取ることを管理する。コンピュータシステムのMMUは、コンピュータシステムの中央処理装置(CPU)に、CPUが、アプリケーションプログラムのすべてに、しばしば、断片化したまたは不連続である物理メモリアドレス空間を共有させるのではなく、CPU自らの専用の連続的な仮想メモリアドレス空間内で各アプリケーションプログラムを実行することを許す仮想メモリを提供する。MMUの目的は、仮想メモリアドレス(VA)を、CPUのための物理メモリアドレス(PA)に変換することである。CPUは、MMUに対してVAを直接に読み取ること、および書き込むことを行うことによってPAを間接的に読み取ること、および書き込むことを行い、MMUが、それらのVAをPAに変換し、次に、PAを書き込む、または読み取る。

【０００３】

これらの変換を実行するために、MMUは、システムメインメモリの中に記憶されたページテーブルにアクセスする。ページテーブルは、ページテーブルエントリから構成される。ページテーブルエントリは、VAをPAにマップするのにMMUによって使用される情報である。MMUは、最近使用されたマッピングをキャッシュするのに使用されるキャッシュメモリ要素である、変換ルックアサイドバッファ(TLB:Translation lookaside buffer)を、通常含む。MMUが、VAをPAに変換する必要がある場合、MMUはまず、TLBを調べて、そのVAに対するマッチが存在するかどうかを判定する。存在する場合、MMUはTLBの中で見出されたマッピングを使用してPAを計算し、次にそのPAにアクセスする(すなわち、そのPAを読み取る、または書き込む)。このことは、TLB「ヒット」として知られている。MMUが、TLBの中でマッチを見出さない場合、このことはTLB「ミス」として知られている。

【０００４】

TLBミスが生じた場合、MMUは、ハードウェアテーブルウォーク(HWTW)として知られていることを実行する。HWTWは、MMUの中で対応するページテーブルを見出す「テーブルウォーク」を実行し、次に、そのページテーブルの中の複数のロケーションを読み取って、対応するVA-PAアドレスマッピングを見出すことを含む、時間のかかる、計算コストの高いプロセスである。MMUは、次に、そのマッピングを使用して、対応するPAを計算し、そのマッピングをTLBに返すように書き込む。

【０００５】

オペレーティングシステム(OS)仮想化を実施するコンピュータシステムにおいて、一般にハイパーバイザとも呼ばれる仮想メモリモニタ(VMM)が、コンピュータシステムのハードウェアとコンピュータシステムのシステムOSの間に介在させられる。ハイパーバイザは、特権モードで実行され、1つまたは複数のゲスト高レベルOSをホストすることができる。そのようなシステムにおいて、OS上で実行されるアプリケーションプログラムは、仮想メモリの第1の層のVAを使用してメモリをアドレス指定し、ハイパーバイザ上で実行されるOSは、仮想メモリの第2の層の中間物理アドレス(IPA)を使用してメモリをアドレス指定する。MMUにおいて、ステージ1(S1)変換が、各VAをIPAに変換するのに実行され、ステージ2(S2)変換が、各IPAをPAに変換するのに実行される。

【０００６】

そのような変換を実行している際にTLBミスが生じた場合、マルチレベルの2次元(2D)HWTWが、対応するIPAおよびPAを計算するのに必要とされるテーブルエントリを取得するように実行される。これらのマルチレベルの2D HWTWを実行することは、パフォーマンス上のペナルティを通常もたらす、MMUに関する相当な量の計算オーバーヘッドをもたらし得る。

【０００７】
図1は、読取り変換を実行している間にTLBミスが生じた場合に実行される、既知の3レベルの2D HWTWの絵画的例示である。図1に示されるHWTWは、データが物理メモリの中に記憶されているPAを取得するのに15回のテーブルルックアップの実行を要求する3レベルの2D HWTWに関する最悪シナリオを表す。この例に関して、コンピュータシステムのMMUは、少なくとも1つのゲスト高レベルOS(HLOS)をホストしているハイパーバイザを実行しており、このHLOSは、少なくとも1つのアプリケーションプログラムを実行している。そのような構成において、ゲストHLOSによって割り当てられているメモリは、システムの実際の物理メモリではなく、代わりに前述した中間物理メモリである。ハイパーバイザが、実際の物理メモリを割り当てる。したがって、各VAはIPAに変換され、このIPAが次に、読み取られるデータが実際に記憶される実際の物理メモリのPAに変換される。
【０００８】
このプロセスは、MMUが、S1ページグローバルディレクトリ(PGD)IPA2を受け取ることから始まる。この最悪シナリオ例に関して、MMUが、マッチがないかTLBを調べる際にTLBミスが生じるものと想定される。このミスのため、MMUはHWTWを実行しなければならない。このHWTWは、IPA2をPAにコンバートするのに必要とされるマッピングを取得する3回のS2テーブルルックアップ3、4、および5、ならびにそのPAを読み取る1回のさらなるルックアップ6を実行することを含む。テーブルルックアップ3、4、および5は、それぞれ、S2 PGD、S2 ページミドルディレクトリ(PMD)、およびS2 ページテーブルエントリ(PTE)を読み取ることを含む。ルックアップ6でPAを読み取ることは、MMUにS1 PMD IPA7をもたらす。この最悪シナリオ例に関して、MMUが、S1 PMD IPA7とのマッチがないかTLBを調べる際にTLBミスが生じるものと想定される。このミスのため、MMUは別のHWTWを実行しなければならない。このHWTWは、S1 PMD IPA7をPAにコンバートするのに必要とされるマッピングを取得する3回のS2テーブルルックアップ8、9、および11、ならびにそのPAを読み取る1回のさらなるルックアップ12を実行することを含む。テーブルルックアップ8、9、および11は、それぞれ、S2 PGD、S2 PMD、およびS2 PTEを読み取ることを含む。ルックアップ12でPAを読み取ることは、MMUにS1 PTE IPA13をもたらす。
【０００９】
この最悪シナリオ例に関して、MMUが、S1 PTE IPA13とのマッチがないかTLBを調べる際にTLBミスが生じるものと想定される。このミスのため、MMUは別のHWTWを実行しなければならない。このHWTWは、S1 PTE IPA13をPAにコンバートするのに必要とされるマッピングを取得する3回のS2テーブルルックアップ14、15、および16、ならびにそのPAを読み取る1回のさらなるルックアップ17を実行することを含む。テーブルルックアップ14、15、および16は、それぞれ、S2 PGD、S2 PMD、およびS2 PTEを読み取ることを含む。ルックアップ17でPAを読み取ることは、MMUに実際のIPA18をもたらす。この最悪シナリオ例に関して、MMUが、実際のIPA18とのマッチがないかTLBを調べる際にTLBミスが生じるものと想定される。このミスのため、MMUは別のHWTWを実行しなければならない。このHWTWは、実際のIPA18をPAにコンバートするのに必要とされるマッピングを取得する3回のS2テーブルルックアップ19、21、および22を実行することを含む。テーブルルックアップ19、21、および22は、それぞれ、S2 PGD、S2 PMD、およびS2 PTEを読み取ることを含む。次に、そのPAが読み取られて、対応する読取りデータが取得される。ルックアップ18でPAを読み取ることは、MMUにS1 PTE IPA13をもたらす。
【００１０】
このため、3レベルの2D HWTWに関する最悪シナリオにおいて、大量の時間を消費し、パフォーマンス上のペナルティをもたらす大量の計算オーバーヘッドである、12回のS2テーブルルックアップ、および3回のS1テーブルルックアップが実行されることが分かる。たとえば、TLBのサイズを大きくすること、複数のTLBを使用すること、フラットなネストされたページテーブルを使用すること、シャドウページングもしくは投機的シャドウページングを使用すること、およびページウォークキャッシュを使用することを含め、様々な技法およびアーキテクチャが、HWTWを実行することに関与する時間および処理オーバーヘッ

ドの量を低減するのに使用されてきた。これらの技法およびアーキテクチャのすべては、HWTWを実行することに関連する処理オーバーヘッドを低減することができる一方で、しばしば、コンピュータシステムのどこか別の所で処理オーバーヘッドの増加をもたらす。

【発明の概要】

【発明が解決しようとする課題】

【００１１】

したがって、HWTWを実行するのに要求される時間およびコンピューティングリソースの量を低減するコンピュータシステムおよび方法の必要性が存在する。また、HWTW中にTLBレジスタにロードされているPAの内容に対する許可のないアクセスを防止するための方法および装置の必要性も存在する。

【課題を解決するための手段】

【００１２】

本発明は、HWTWの実行中にコンピュータシステムの記憶要素にロードされているPAの内容に対する許可のないアクセスを防止するためのセキュリティ装置およびセキュリティ方法を対象とする。このセキュリティ装置およびセキュリティ方法は、PAに基づいてVAを予測するのに予測アルゴリズムが使用されているかどうかを検出することを含め、いくつかの条件を検出して、それらの内容に対するアクセスが防止されるべきかどうかを判定する。

【００１３】

この装置は、PAの内容に関してTLBを調べている際にミスが生じた場合、IPAの関数としてPAを予測する予測アルゴリズムが現在、イネーブルにされているか否かを判定するように構成されたセキュリティロジックを備える。このセキュリティロジックは、予測アルゴリズムが現在、イネーブルにされている間、記憶要素の内容に、特権のないエンティティによってアクセスが行われることを防止するように構成される。

【００１４】

この方法は、

セキュリティロジックを提供すること、

セキュリティロジックを用いて、PAの内容に関してTLBを調べている際にミスが生じた場合、IPAの関数としてPAを予測する予測アルゴリズムが現在、イネーブルにされているか否かを判定すること、および

セキュリティロジックが、予測アルゴリズムが現在、イネーブルにされていると判定した場合、セキュリティロジックは、記憶要素の内容に、特権のないエンティティによってアクセスが行われることを防止することを備える。

【００１５】

また、本発明は、HWTWの実行中にコンピュータシステムの記憶要素にロードされているPAの内容に対する許可のないアクセスを防止するためにコンピュータシステムの1つまたは複数のプロセッサによって実行されるようにコンピュータコードが記憶されている非一時的コンピュータ可読媒体(CRM)も対象とする。このコンピュータコードは、第1のコンピュータコード部分と、第2のコンピュータコード部分とを備える。第1のコンピュータコード部分は、PAの内容に関してTLBを調べている際にミスが生じた場合、IPAの関数としてPAを予測する予測アルゴリズムが現在、イネーブルにされているか否かを判定する。第2のコンピュータコード部分は、第1のコンピュータコード部分が、予測アルゴリズムが現在、イネーブルにされていると判定した場合、記憶要素の内容に、特権のないエンティティによってアクセスが行われることを防止する。

【００１６】

これら、および他の特徴および利点は、後段の説明、図面、および特許請求の範囲から明白となろう。

【図面の簡単な説明】

【００１７】

【図１】本発明の例示的な実施形態によるコンピュータシステムを示すブロック図である

。
【図２】HWTWを実行するのに要求される時間およびコンピューティングリソースの量を低減するための方法を実行するように構成された例示的な、または例としての実施形態によるコンピュータシステムを示すブロック図である。
【図３】HWTW読取りトランザクションを実行するのに要求される時間および処理オーバーヘッドの量を低減するように図2に示されるハイパーバイザによって実行される、例示的な実施形態による方法を表す流れ図である。
【図４】例示的な実施形態による図3に示される流れ図によって表される方法を使用してHWTW読取りトランザクションが実行される様態を示す絵画的図である。
【図５】図3に示される流れ図によって表される方法を実行する例示的な実施形態によるハードウェアプレディクタを示すブロック図である。
【図６】図2に示されるコンピュータシステムが組み込まれたモバイルスマートフォンを示すブロック図である。
【図７】図5に示されるプレディクタがイネーブルにされている間、TLBの中のレジスタにロードされているPAの内容に対する許可のないアクセスを防止するセキュリティアルゴリズムを実行するための例示的な実施形態によるセキュリティロジックを示すブロック図である。
【図８】例示的な実施形態による図7に示されるセキュリティロジックによって実行されるプロセスを示す流れ図である。
【発明を実施するための形態】
【００１８】
本明細書で説明される例示的な実施形態によれば、HWTWを実行するのに要求される時間およびコンピューティングリソースの量を低減するためのコンピュータシステム、およびコンピュータシステムにおいて使用するための方法が提供される。S1ページテーブルが記憶されているPAを見出すためにS2 HWTWを実行している際にTLBミスが生じた場合、MMUが、IPAを使用して対応するPAを予測する予測アルゴリズムを実行し、これにより、S2テーブルルックアップのいずれを実行する必要性も回避する。このことは、これらのタイプのHWTW読取りトランザクションを実行している際に実行される必要があるルックアップの回数を大幅に減らし、このことが、これらのタイプのトランザクションを実行することに関連する処理オーバーヘッドおよびパフォーマンス上のペナルティを大幅に低減する。
【００１９】
さらに、予測アルゴリズムがイネーブルにされた結果として、記憶要素(たとえば、TLBのレジスタ)にロードされているPAの内容に対する許可のないアクセスを防止するセキュリティアルゴリズムを実行するためのセキュリティ装置およびセキュリティ方法の例示的な実施形態が提供される。予測アルゴリズムがイネーブルにされると、システムの知識を有する個人が、メインメモリのセキュリティ保護された部分のPAに記憶されている内容がTLBの中のレジスタにロードされるようにするように予測アルゴリズムを構成することが可能であり得る。このようにして、メインメモリのセキュリティ保護された部分の中に記憶された内容にアクセスを有するべきでない個人が、それらの内容に対する許可のないアクセスを間接的に得る可能性がある。このセキュリティ装置およびセキュリティ方法は、いくつかの状況下でそれらの内容をマスクすることによって、そのような許可のないアクセスが行われることを防止する。セキュリティ装置およびセキュリティ方法の例示的な実施形態を説明するのに先立って、予測アルゴリズムを実行するためのコンピュータシステムおよび方法の例示的な実施形態が、図2～図6を参照して説明される。次に、セキュリティ装置およびセキュリティ方法の例示的な実施形態が、図7および図8を参照して説明される。
【００２０】
図2は、S1ページテーブルが記憶されているPAを見出すためにS2 HWTWを実行するのに要求される時間およびコンピューティングリソースの量を低減するための方法を実行するように構成された例示的な、または例としての実施形態によるコンピュータシステム100の

ブロック図を示す。図2に示されるコンピュータシステム100の例は、CPUクラスタ110、メインメモリ120、ビデオカメラディスプレイ130、グラフィックス処理装置(GPU)140、ペリフェラルコネクトインターフェースエクスプレス(PCIe:peripheral connect interface express)入出力(IO)デバイス150、複数のIO TLB(IOTLB)160、およびシステムバス170を含む。CPUクラスタ110は、MMU110bを各々が有する複数のCPUコア110aを有する。各CPUコア110aは、マイクロプロセッサまたは他の任意の適切なプロセッサであり得る。ビデオカメラディスプレイ130は、システムMMU(SMMU)130aを有する。GPU140は、GPU140自らのSMMU140aを有する。同様に、PCIe IOデバイス150は、PCIe IOデバイス150自らのSMMU150aを有する。

【００２１】

プロセッサコア110aのMMU110bは、VAをIPAに変換するタスク、およびIPAをPAに変換するタスクを実行するように構成される。ページテーブルは、メインメモリ120の中に記憶される。MMU110b、ならびにSMMU130a、140a、および150aの各々は、メインメモリ120の中に記憶されるページテーブルのサブセットを記憶する各々の自らのTLB(簡明のため図示せず)を有する。この例示的な実施形態によれば、TLBミスが生じた後、MMU110bが、IPAを処理してPAを予測する予測アルゴリズムを実行する。この予測アルゴリズムは、次のように数学的に表される。

PA=f(IPA) (式1)

ただし、fは、数学的な関数である。この目的で使用され得る関数fは、図5を参照して詳細に説明される。「予測する」という句は、本明細書でその句が使用される際、「決定する」を意味して、確率的決定も確率論的決定も暗示しないが、確率的決定または確率論的決定が、本発明の範囲から必ずしも除外されるわけではない。予測アルゴリズムによって行われる予測は通常、ただし必然的にではなく、決定論的である。

【００２２】

CPUクラスタ110は、システムOS200および仮想マシンモニタ(VMM)、つまり、ハイパーバイザ210を実行する。ハイパーバイザ210は、変換を実行することに加えて、MMU110b、ならびにSMMU130a、140a、および150aの中に記憶されたページテーブルを更新することを含む変換タスクを管理する。また、ハイパーバイザ210はゲストHLOS220および/またはゲストデジタル権利マネージャ(DRM)230も実行する。HLOS220はビデオカメラディスプレイ130に関連付けられてもよく、DRM230はGPU140に関連付けられてもよい。ハイパーバイザ210は、HLOS220およびDRM230を管理する。

【００２３】

TLBミスが生じた後、ハイパーバイザ210が、予測アルゴリズムを実行してIPAをPAにコンバートするようにMMU110b、ならびにSMMU130a、140a、および150aを構成する。そのような事例において、TLBミスに関連するVAに対する開始IPAは、S1変換が正常に始まる通常の様態で、CPUクラスタ110のハードウェアベースレジスタ(簡明のため図示せず)から取得される。次に、予測アルゴリズムが、後段でより詳細に説明されるように式1によりPAを予測する。SMMU130a、140a、および150aを管理し、更新するのに、CPU MMU110bが、バス170を介してSMMU130a、140a、および150aに分散仮想メモリ(DVM)メッセージを送信する。MMU110b、ならびにSMMU130a、140a、および150aは、メインメモリ120にアクセスしてHWTWを実行する。

【００２４】

例示的な実施形態によれば、CPU MMU110bが、MMUトラフィックを3つのトランザクションクラス、すなわち、(1)S1ページテーブルが記憶されているPAを見出すS2 HWTW読取りトランザクション、(2)クライアントトランザクション、および(3)アドレス障害(AF)/ダーティフラグ書込みトランザクションに分類する。この例示的な実施形態によれば、予測アルゴリズムは、クラス1トランザクション、すなわち、HWTW読取りトランザクションに関してIPAをPAにコンバートするにすぎない。他のすべてのクラスのトランザクションに関しては、この例示的な実施形態によれば、MMU110b、ならびにSMMU130a、140a、および150aが、通常の様態で他のすべての変換(たとえば、S1変換およびクライアントトランザクシ

ョンS2変換)を実行する。

【００２５】

図3は、HWTW読取りトランザクションを実行するのに要求される時間および処理オーバーヘッドの量を低減するようにCPU MMU110bによって実行される、例示的な実施形態による方法を表す流れ図である。ブロック301は、方法の開始を表し、通常CPUクラスタ110が起動し、システムOS200およびハイパーバイザ210を実行することを開始する。MMU110bは、ブロック302によって示されるように、トラフィックを前述したトランザクションクラス(1)、(2)、および(3)に分類する。この分類プロセスは、トランザクションを、これら3つよりも多くのクラス、または少ないクラスに分類してもよいが、分類のうちの少なくとも1つは、クラス(1)トランザクション、すなわち、S1ページテーブルが記憶されているPAを見出すS2 HWTW読取りトランザクションである。ブロック303によって表されるステップで、クラス(1)トランザクションを実行している際にTLBミスが生じたかどうかの判定が行われる。生じていない場合、方法はブロック306に進み、ブロック306で、MMU110b、またはSMMU130a、140a、もしくは150aが、通常の様態でHWTWを実行する。

【００２６】

ブロック303によって表されるステップで、CPU MMU110bが、クラス(1)トランザクションを実行している際にミスが生じたと判定した場合、方法はブロック305によって表されるステップに進む。ブロック305によって表されるステップで、前述した予測アルゴリズムが実行されてIPAをPAにコンバートまたは変換する。

【００２７】

図4は、例示的な実施形態によりHWTW読取りトランザクションが実行される様態を示す絵画的図である。この例示的な実施形態に関して、例として、ページテーブルは3レベルページテーブルであり、HWTWは、2D HWTWであるものと想定される。また、この例は、TLBミス最悪シナリオも想定する。このプロセスは、MMUがVAを受け取り、次に、制御レジスタ(簡明のために図示せず)からS1 PGD IPA401を取り出すことから始まる。次に、MMUが、S1 PGD IPA401とのマッチがないかTLBを調べる。この最悪シナリオ例に関して、MMUが、マッチがないかTLBを調べる際にTLBミスが生じるものと想定される。このミスのため、MMUは予測アルゴリズムを実行して、S1 PGD IPA401を、S1 PMD IPA403が記憶されているPA402にコンバートする。このため、S1 PGD IPA401をPA402にコンバートするのに単一のルックアップが使用される。

【００２８】

この最悪シナリオ例に関して、MMUが、S1 PMD IPA403とのマッチがないかTLBを調べる際にTLBミスが生じるものと想定される。このミスのため、MMUは予測アルゴリズムを実行して、S1 PMD IPA403を、S1 PTE IPA405が記憶されているPA404にコンバートする。このため、S1 PMD IPA403をPA404にコンバートするのに単一のルックアップが使用される。この最悪シナリオ例に関して、MMUが、S1 PTE IPA405とのマッチがないかTLBを調べる際にTLBミスが生じるものと想定される。このミスのため、MMUは予測アルゴリズムを実行して、S1 PTE IPA405を、IPA1 407が記憶されているPA406にコンバートする。IPA1 407が取得されると、3回のルックアップ408、409、および411が実行されて、読み取られるべきデータが記憶されている最終的なPA412が取得される。

【００２９】

このため、この実施形態によれば、ルックアップの合計回数が、15回(図1)から6回に減らされており、このことは、処理オーバーヘッドの60%低減であることが分かる。もちろん、本発明は、特定の数のレベル、または特定の数のHWTW次元を有するMMU構成に限定されない。本発明の概念および原理は、ページテーブルの構成にかかわらず適用されることが、当業者には理解されよう。また、この方法およびシステムは、IPA-PAコンバートに関して本明細書で説明されているものの、IPAを使用しないシステムにおける直接のVA-PAコンバートにも同様に適用可能である。

【００３０】

図5は、予測アルゴリズムを実行するプレディクタ500の例示的な実施形態のブロック図

である。プレディクタ500は通常、MMU110b、ならびにSMMU130a、140a、および150aにおいて実装される。前述したように、例示的な実施形態によれば、予測アルゴリズムは、クラス1読取りトランザクションを実行する際に限って実行される。図5に示されるプレディクタ500の構成は、プレディクタ500が、クラス1トランザクションに関してイネーブルにされ、クラス2トランザクションおよびクラス3トランザクションを含む他のすべてのクラスのトランザクションに関してディセーブルにされることを許す1つの構成の例である。

【００３１】

また、図5に示されるプレディクタ500の構成は、プレディクタ500が、IPAに基づいてPAを計算するのに前述の式1において使用される関数fを選択することも許す。各仮想マシン(VM)は、関数fの異なるセットを使用していてもよく、したがって、使用される関数のセットが、IPAの範囲にわたってIPAとPAの間で1対1マッピングが存在することを確実にすることが重要である。ハイパーバイザ210は、ハイパーバイザ210において実行されている対応するVMを各々が有することになる複数のHLOSまたはDRMを管理していてよい。使用される関数のセットは、予測されるPAが、別のVMに割り当てられた予測されるPAと重なり合わないことを確実にする。

【００３２】

関数fの例は、次のとおりである、すなわち、

PA=IPA、

PA=IPA+Offset_function(VMID)、ただし、VMIDは、HWTW読取りトランザクションに関連付けられたVMを識別するすべてのVMにわたる一意識別子であり、Offset_functionは、VMIDに関連付けられた特定のオフセット値に基づいて選択された出力を有する関数である、

PA=IPA XOR Extended_VMID、ただし、XORは、排他的OR演算を表し、Extended_VMIDは、拡張されたVMIDである。ハイパーバイザ210は、VM間の衝突が回避されるように関数fを選択する。

【００３３】

図5で、関数fは、多項式であり、かつハイパーバイザ210は、複数の多項式から関数fとして使用されるべき多項式を選択するものと想定される。選択される多項式は、たとえば、HWTW読取りトランザクションが実行されているVMのVMIDに基づいてもよい。プレディクタ500の構成レジスタ510が、1つまたは複数の予測イネーブルビット510aと、1つまたは複数の多項式選択ビット510bとを保持する。プレディクタ500の多項式計算ハードウェア520が、レジスタ510から受け取られた多項式選択ビット510bの値に基づいて多項式関数を選択するハードウェアを備える。また、多項式計算ハードウェア520は、IPA-PA変換要求を受け取り、選択された多項式関数によりその要求を処理して、予測されるPAをもたらすこともする。

【００３４】

予測イネーブルビット510aおよびクラス1イネーブルビットは、ANDゲート530の入力で受け取られる。クラス1イネーブルビットは、クラス1読取りトランザクションを実行している際にミスが生じると、アサートされる。プレディクタ500のマルチプレクサ(MUX)540が、MUX540のセレクタポートでANDゲート530の出力を受け取り、予測されるPA、および通常の様態で取得されたIPA-PA変換結果を受け取る。予測イネーブルビット510aとクラス1イネーブルビットがともにアサートされた場合、S2ウォーク制御ロジックおよび状態マシン550が、ディセーブルにされ、MUX540は、予測されるPAがMUX540から出力されるように選択する。

【００３５】

予測イネーブルビット510aおよび/またはクラス1イネーブルビットがデアサートされた場合、S2ウォーク制御ロジックおよび状態マシン550が、イネーブルにされる。S2ウォーク制御ロジックおよび状態マシン550がイネーブルにされた場合、他のタイプのS2ウォーク(たとえば、クラス2およびクラス3)は、S2ウォーク制御ロジックおよび状態マシン550によってメインメモリ120の中で実行され得る。このため、S2ウォーク制御ロジックおよび状態マシン550がイネーブルにされた場合、MUX540は、S2ウォーク制御ロジックおよび

状態マシン550から出力されたIPA-PA変換結果を出力する。

【００３６】

プレディクタ500は、多くの異なる構成を有し得ることに留意されたい。図5に示されるプレディクタ500の構成は、予測アルゴリズムを実行するための多くの適切な構成のうちの1つにすぎない。図5に示される以外の多くの構成が、予測アルゴリズムを実行するのに使用されてもよいことが、当業者には理解されよう。

【００３７】

図2に示されるコンピュータシステム100は、たとえば、デスクトップコンピュータ、サーバ、およびモバイルスマートフォンを含め、メモリ仮想化が実行される任意のタイプのシステムにおいて実施され得る。図6は、コンピュータシステム100が組み込まれたモバイルスマートフォン600のブロック図を示す。スマートフォン600は、本明細書で説明される方法を実行することができなければならないことを除いて、いずれの特定のタイプのスマートフォンであることにも、いずれの特定の構成を有することにも限定されない。また、図6に示されるスマートフォン600は、本明細書で説明される方法を実行するためのコンテキスト認識および処理能力を有するセルラー電話機の簡略化された例であることを意図している。スマートフォンの動作および構造は、当業者には理解され、このため、実装の詳細は、省略されている。

【００３８】

例示的な実施形態によれば、スマートフォン600は、システムバス612を介して一緒に接続されたベースバンドサブシステム610および無線周波数(RF)サブシステム620を含む。システムバス612は、前述した要素を一緒に結合し、それらの要素の相互運用性を可能にする物理接続および論理接続を、通常備える。RFサブシステム620は、ワイヤレストランシーバであり得る。詳細は、簡明のため示していないものの、RFサブシステム620は、当業者に知られているように、一般に、送信のためにベースバンド情報信号を準備するための変調回路、アップコンバージョン回路、および増幅回路を有する送信(Tx)モジュール630を含み、RF信号を受信し、ベースバンド情報信号にダウンコンバートしてデータを回復するための増幅回路、フィルタリング回路、およびダウンコンバージョン回路を有する受信(Rx)モジュール640を含み、ダイプレクサ回路、デュプレクサ回路、もしくは受信信号から送信信号を分離することができる他の任意の回路を含むフロントエンドモジュール(FEM)650を含む。アンテナ660が、FEM650に接続される。

【００３９】

ベースバンドサブシステム610は、一般に、システムバス612を介して一緒に電気的に結合されたコンピュータシステム100、アナログ回路要素616、およびデジタル回路要素618を含む。システムバス612は、前述した要素を一緒に結合し、それらの要素の相互運用性を可能にする物理接続および論理接続を、通常備える。

【００４０】

入出力(I/0)要素621が、接続624を介してベースバンドサブシステム610に接続される。I/0要素621は、たとえば、マイクロフォン、キーパッド、スピーカ、ポインティングデバイス、ユーザインターフェース制御要素、ならびにユーザが、スマートフォン600に入力コマンドを与え、スマートフォン600から出力を受け取ることを可能にする他の任意のデバイスもしくはシステムを、通常含む。メモリ628が、接続629を介してベースバンドサブシステム610に接続される。メモリ628は、任意のタイプの揮発性メモリまたは不揮発性メモリであり得る。メモリ628は、スマートフォン600に永久に組み込まれてもよく、またはリムーバブルメモリカードなどのリムーバブルメモリ要素であってもよい。

【００４１】

アナログ回路616およびデジタル回路618は、I/0要素621によって与えられた入力信号を、送信されるべき情報信号に変換する信号処理、信号コンバート、およびロジックを含む。同様に、アナログ回路616およびデジタル回路618は、受信された信号から、回復された情報を包含する情報信号を生成するのに使用される信号処理要素を含む。デジタル回路618は、たとえば、デジタル信号プロセッサ(DSP)、フィールドプログラマブルゲートアレイ

(FPGA)、または他の任意の処理デバイスを含み得る。ベースバンドサブシステム610は、アナログ要素とデジタル要素をともに含むため、混合信号デバイス(MSD)と呼ばれ得る。

【００４２】

スマートフォン600は、たとえば、カメラ661、マイクロフォン662、全地球測位システム(GPS)センサ663、加速度計665、ジャイロスコープ667、およびデジタルコンパス668などの様々なセンサのうちの1つまたは複数を含み得る。これらのセンサは、バス612を介してベースバンドサブシステム610と通信する。

【００４３】

スマートフォン600に組み込まれたコンピュータシステム100を有することは、複数のOS、およびそれぞれの複数のVMがスマートフォン600上で実行されることを可能にする。この環境において、コンピュータシステム100のハイパーバイザ210(図2)が、スマートフォン600のハードウェアとVMによって実行されているアプリケーションソフトウェアの間のセキュリティ保護された分離をもたらす。

【００４４】

例示的な実施形態によれば、図5を参照して前述した予測アルゴリズムが実行されているかどうかを検出し、実行されている場合、いくつかのレジスタおよび/またはバッファの内容が、特権のない、または許可のないエンティティによってアクセス可能であることを防止するセキュリティ上の予防策をとるセキュリティ方法およびセキュリティ装置が提供される。このセキュリティ方法およびセキュリティ装置が必要とされる理由は、予測アルゴリズムがイネーブルにされると、システムの知識を有する個人が、物理メインメモリ120(図2)のセキュリティ保護された部分のPAに記憶されている内容がTLBの中のレジスタにロードされるようにするように予測アルゴリズムを構成することが可能であり得るためである。このようにして、物理メインメモリ120のセキュリティ保護された部分の中に記憶された内容にアクセスを有するべきでない個人が、それらのPAに対する許可のないアクセスを間接的に得る可能性がある。この方法および装置は、そのような許可のない、または特権のないアクセスを防止する。

【００４５】

図7は、予測アルゴリズムがイネーブルにされている間にTLBの中のレジスタにロードされているPAの内容に対する許可のないアクセスを防止するセキュリティアルゴリズムを実行するための例示的な実施形態による装置700のブロック図である。このブロック図は、概念的な性質のものであり、もっぱらハードウェアとして実施されても、ハードウェアとソフトウェアの組合せとして実施されても、ファームウェアとして実施されてもよい。装置700は、セキュリティアルゴリズムを実行するように構成されたセキュリティロジックである。セキュリティロジック700は通常、CPUコア110aの一部であり、MMU110b、ならびにSMMU130a、140a、および150a(図2)の一部であり得る。本発明は、コンピュータシステム100のどこにセキュリティロジック700が配置されるかに関して限定されない。

【００４６】

図5に示される予測イネーブルビット510aは、セキュリティロジック700のANDゲート710の入力に接続される。特権アクセスビットが、ANDゲート710の他方の入力に印加される。特権アクセスビットは、複数のレジスタ720のうちの1つにアクセスしようと試みるエンティティが、特定のレジスタ720にアクセスする特権を与えられている場合にアサートされる。例示の目的で、レジスタ720は、TLBの中にあるものと想定される。ANDゲート710の出力が、ORゲート730の入力のうちの1つに印加される。レジスタアクセステーブル740から出力されたアクセス識別子ビットが、ORゲート730の他方の入力に印加される。アクセス識別子ビットは、アクセスされているレジスタ720が、メインメモリ120(図5)のセキュリティ保護された、または特権のある部分の中にあるPAからの内容を包含する場合、アサートされる。レジスタアクセステーブル740は、いずれのPAが、メインメモリ120のセキュリティ保護された部分の中にあるかを把握し続けており、それに相応してアクセス識別子ビットをアサートする、またはデアサートする。レジスタ720のうちの1つを選択するのに使用されるレジスタ選択アドレス750が、レジスタアドレステーブル740の中で対応するエン

トリを選択するのにも使用される。このため、レジスタ選択アドレス750によって選択されたレジスタ720に特権がある場合、ORゲート730に入力される対応するアクセス識別子ビットが、アサートされる。

【００４７】

ORゲート730の出力は、MUX760のセレクタ端子に印加される。レジスタ選択アドレス750によってアドレス指定されたレジスタ720の内容が、MUX760の第1のセットの入力端子に印加される。MUX760の第2のセットの入力端子が、オール論理0を受け取る。予測アルゴリズムがイネーブルにされ、かつ特権アクセスビットがアサートされた場合、MUX760は、MUX760から出力されて、結果レジスタ770にロードされるべき、レジスタ選択アドレス750によってアドレス指定されたレジスタ720の内容を選択する。予測アルゴリズムがディセーブルにされ、または特権アクセスビットがデアサートされ、かつアクセス識別子ビットがデアサートされた(アクセスされている内容が、メインメモリ120のセキュリティ保護されていない部分からであることを示して)場合、MUX760は、MUX760から出力されて、結果レジスタ770にロードされるべき、レジスタ選択アドレス750によってアドレス指定されたレジスタ720の内容を選択する。アクセス識別子ビットがアサートされた(アクセスされている内容が、メインメモリ120のセキュリティ保護された部分からであることを示して)場合、MUX760は、MUX760から出力されて、結果レジスタ770にロードされるようオール論理0を選択する。

【００４８】

このため、レジスタ選択アドレス750によってアドレス指定されたレジスタ720の実際の内容は、2つの事例、すなわち、(1)予測アルゴリズムがイネーブルにされ、かつ特権アクセスビットがアサートされる事例、または(2)アクセス識別子ビットがアサートされる事例のいずれかの場合を除いて、MUX760から出力されて、結果レジスタ770にロードされる。これら2つの事例のいずれにおいても、オール論理0が、結果レジスタ770にロードされて、レジスタ720の実際の内容が結果レジスタ770の中でアクセス可能であることを防止する。

【００４９】

図8は、図7を参照して前述したセキュリティロジック700によって実行される判定プロセスを示す流れ図である。ブロック801で、予測アルゴリズムがイネーブルにされているか否かの判定が行われる。イネーブルにされていない場合、ブロック802によって示されるとおり、レジスタ720の実際の内容が戻される。イネーブルにされている場合、ブロック803で、それらの内容にアクセスしようと試みているエンティティに特権があるか否かの判定が行われる。特権がある場合、ブロック802で、レジスタ720の実際の内容が戻される。特権がない場合、ブロック804で、レジスタ720が、特権データを公開するか否かの判定が行われる。公開しない場合、ブロック802で、レジスタ720の実際の内容が戻される。公開する場合、ブロック805によって示されるように、ロジック0が戻される。

【００５０】

セキュリティロジック700の説明から、特権のないエンティティ(たとえば、ハイパーバイザ以外のエンティティ)が、図5に示されるプレディクタ500を使用して、メインメモリ120の許可のないPAの中に記憶された内容に対する許可のないアクセスを得ようと試みた場合、実際の内容には、0が上書きされて、許可のない、または特権のないエンティティが実際の内容にアクセスすることが防止されることが分かる。本発明の範囲内で、図7に示されるセキュリティロジック700、および図8に示されるプロセスに多くの変形が行われ得る。たとえば、図8を参照すると、プロセスは、ブロック803を取り除き、ブロック801、802、804、および805を残すことによって変形されることが可能である。代替として、ブロック804が取り除かれて、ブロック801、802、803、および805を残すことも可能である。図7に示されるセキュリティロジック700は、当業者には理解されるように、変形されたプロセスを実現するように容易に変形され得る。

【００５１】

図5、図7、および図8を参照して前述したもの、またはそれらに加えたセキュリティ関

数が、許可のないアクセス試行が検出されると、実施されることも可能であることに留意されたい。レジスタの内容に論理0を上書きすることは、セキュリティをもたらす1つの方法の例にすぎない。代替形態の例は、内容に論理1、または真の内容を不明瞭にする他の何らかのバイナリ値を上書きすること、内容と、等しい長さの他の何らかのバイナリ値とのXORをとること、実際の内容の代わりにエラーメッセージを戻すこと、割込みを発行すること、プロセッサ110a、MMU110、またはSMMU130a、140aもしくは150aをリセットすることなどを含む。本明細書で与えられている説明に鑑みて、本明細書で説明される例示的な実施形態に対するこれら、および他の適切な代替形態が実施され得る様態は、当業者には理解されよう。

【００５２】

図3および図8を参照して前述したプロセスは、もっぱらハードウェアとして実施されても、ハードウェアとソフトウェアの組合せとして、またはハードウェアとファームウェアの組合せとして実施されてもよい。同様に、図2に示されるコンピュータシステム100の構成要素の多くも、もっぱらハードウェアとして実施されても、ハードウェアとソフトウェアの組合せとして実施されても、ファームウェアとして実施されてもよい。たとえば、ハイパーバイザ210は、もっぱらハードウェアとして実施されても、ハードウェアとソフトウェアの組合せとして実施されても、ファームウェアとして実施されてもよい。図3および図8に示されるプロセス、または図2に示されるコンピュータシステム100の構成要素が、ソフトウェアまたはファームウェアとして実施される事例において、対応するコードは、コンピュータ可読媒体であるメインメモリ120(図2)の中に記憶される。メインメモリ120は通常、不揮発性ランダムアクセスメモリ(RAM)、ダイナミックRAM(DRAM)、読取り専用メモリ(ROM)デバイス、プログラマブルROM(PROM)、消去可能なPROM(EPROM)などのソリッドステートコンピュータ可読媒体である。しかし、たとえば、磁気記憶デバイスおよび光記憶デバイスなどの他のタイプのコンピュータ可読媒体が、コードを記憶するために使用されてもよい。

【００５３】

本明細書で説明される例示的な実施形態は、本発明の原理および概念を示すことを意図していることに留意されたい。本発明は、本明細書で与えられる説明に鑑みて、当業者によって理解されるように、これらの実施形態に限定されない。また、本発明の範囲を逸脱することなく、図2～図8を参照して前述した方法およびシステムに多くの変更が行われ得ることにも留意されたい。たとえば、図7に示されるセキュリティロジック700の構成は、本明細書で与えられている説明に鑑みて当業者によって理解されるように、前述した目標を依然として実現しながら、多くの様態で変形され得る。また、図6に示されるスマートフォン600は、この方法を実行するための適切な構成および機能を有するモバイルデバイスの一例にすぎない。本明細書で与えられる説明に鑑みて、本発明の範囲を逸脱することなく、図6に示されるスマートフォン600に多くの変更が行われ得ることが当業者には理解されよう。これら、および他の変更は、本発明の範囲に含まれる。

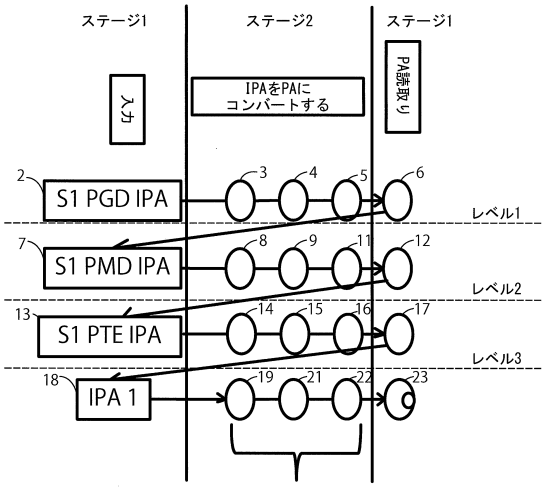
【符号の説明】

【００５４】

100　コンピュータシステム
110　CPUクラスタ
110a　CPUコア
110b、130a、140a、150a　メモリ管理ユニット(MMU)
120、628　メモリ
130　ビデオカメラディスプレイ
140　グラフィックス処理装置(GPU)
150　PCIe入出力(IO)デバイス
160　IO変換ルックアサイドバッファ(IOTLB)
170、612　システムバス
200　システムオペレーティングシステム(OS)

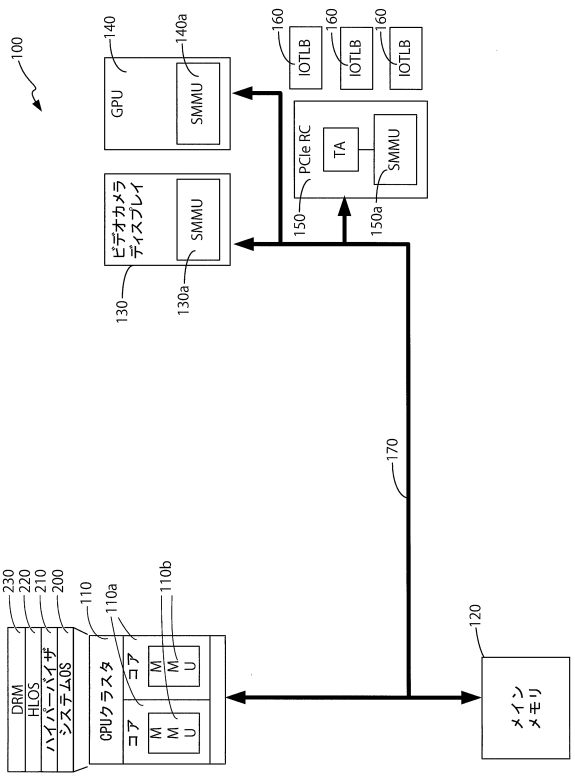
210　ハイパーバイザ
220　高レベルOS(HLOS)
230　デジタル権利マネージャ(DRM)
500　プレディクタ
510　構成レジスタ
520　多項式計算ハードウェア
530、710、730　ゲート
540、760　マルチプレクサ(MUX)
550　S2ウォーク制御ロジックおよび状態マシン
600　スマートフォン
610　ベースバンドサブシステム
616　アナログ回路要素
618　デジタル回路要素
620　無線周波数(RF)サブシステム
621　入出力(I/O)要素
624、629　接続
630　送信(Tx)モジュール
640　受信(Rx)モジュール
650　フロントエンドモジュール(FEM)
660　アンテナ
661、662、663、665、667、668　センサ
700　セキュリティロジック
720、770　レジスタ
740　レジスタアクセステーブル

【図１】

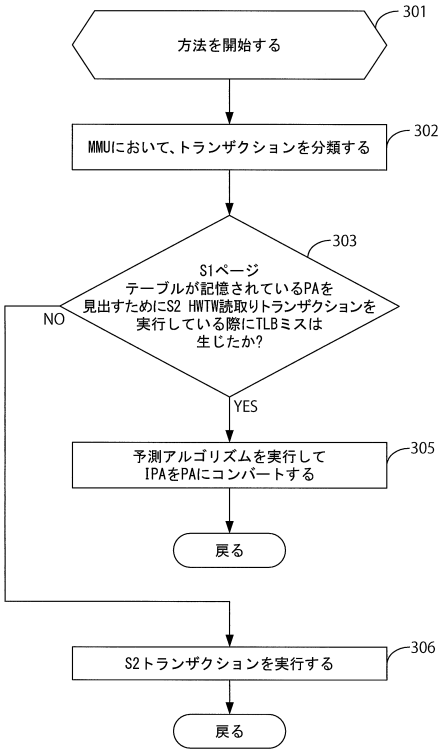


（従来技術）

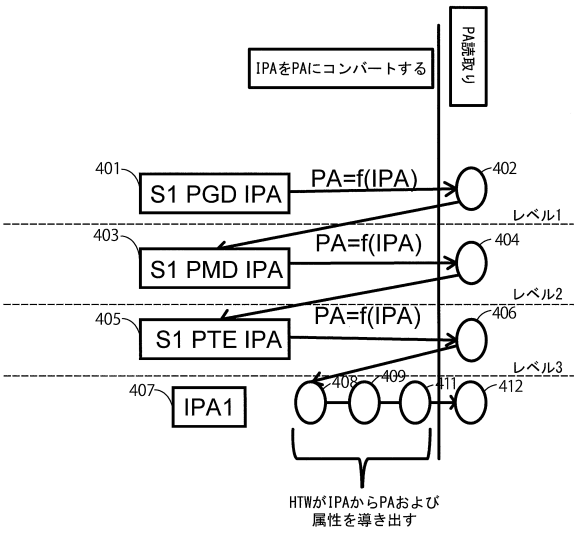
【図２】



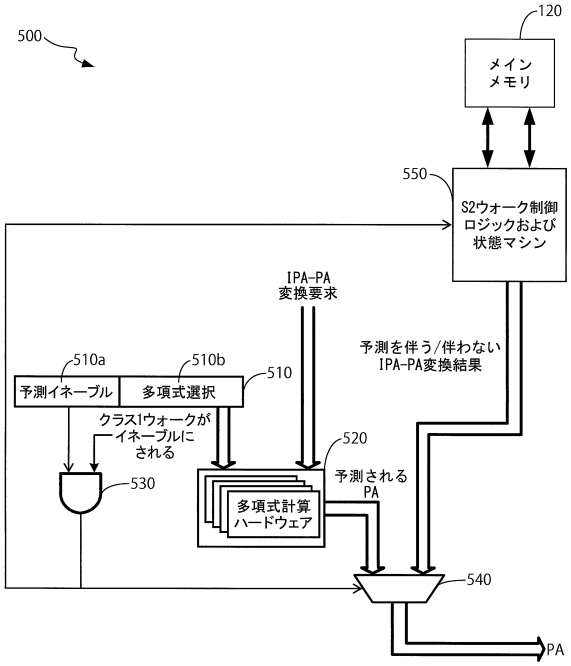
【図３】


301
方法を開始する
302
MMUにおいて、トランザクションを分類する
303
S1ページ
テーブルが記憶されているPAを
見出すためにS2 HWTW読取りトランザクションを
実行している際にTLBミスは
生じたか?
NO
YES
305
予測アルゴリズムを実行して
IPAをPAにコンバートする
戻る
306
S2トランザクションを実行する
戻る

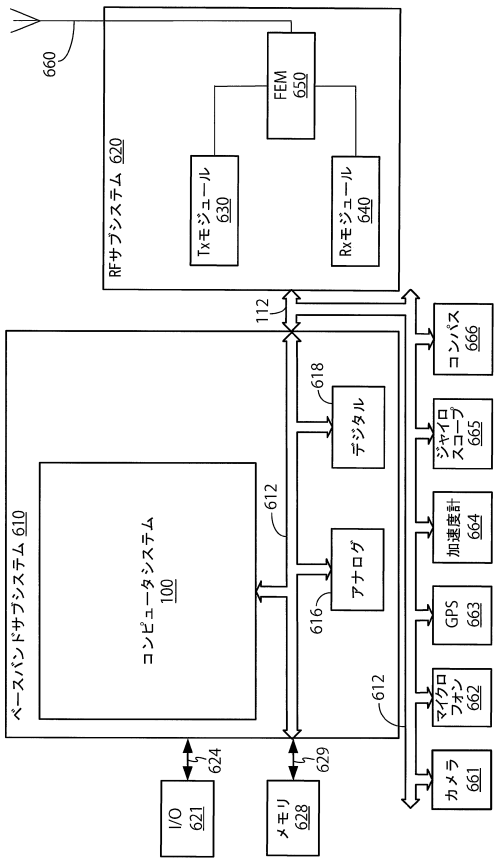
【図４】


PA読取り
IPAをPAにコンバートする
401
S1 PGD IPA
PA=f(IPA)
402
レベル1
403
S1 PMD IPA
PA=f(IPA)
404
レベル2
405
S1 PTE IPA
PA=f(IPA)
406
レベル3
407
IPA1
408
409
411
412
HTWがIPAからPAおよび
属性を導き出す

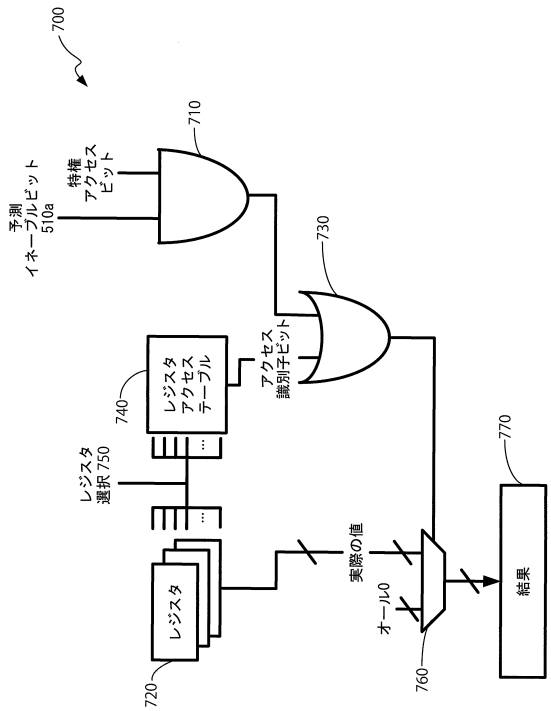
【図５】


500
120
メイン
メモリ
550
S2ウォーク制御
ロジックおよび
状態マシン
IPA-PA
変換要求
予測を伴う/伴わない
IPA-PA変換結果
510a
予測イネーブル
510b
多項式選択
510
クラス1ウォークが
イネーブルにされる
520
予測される
PA
530
多項式計算
ハードウェア
540
PA

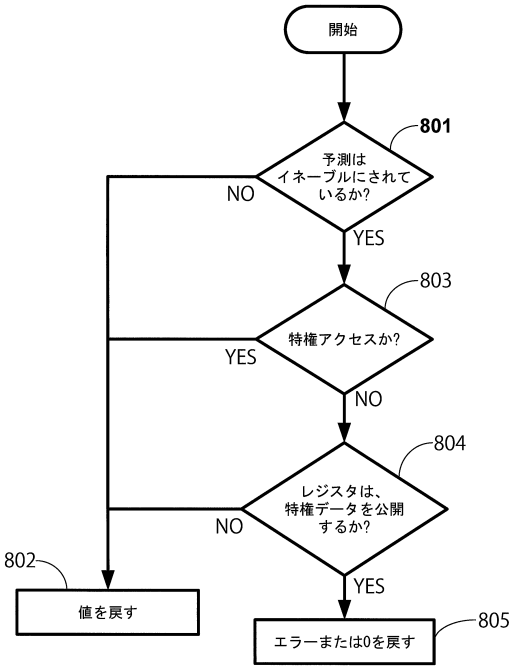
【図６】


660
RFサブシステム 620
FEM
650
Txモジュール
630
Rxモジュール
640
112
ベースバンドサブシステム 610
コンピュータシステム
100
612
618
デジタル
アナログ
616
612
624
629
I/O
621
メモリ
628
コンパス
666
ジャイロ
スコープ
665
加速度計
664
GPS
663
マイクロ
フォン
662
カメラ
661

【図７】


700
710
予測
イネーブルビット
510a
特権
アクセス
ビット
730
アクセス
識別子ビット
740
レジスタ
アクセス
テーブル
レジスタ
選択 750
770
実際の値
オール0
結果
レジスタ
720
760

【図８】


開始
801
予測は
イネーブルにされて
いるか?
NO
YES
803
特権アクセスか?
YES
NO
804
レジスタは、
特権データを公開
するか?
NO
YES
802
値を戻す
エラーまたは0を戻す
805

フロントページの続き

(72)発明者 アゼディン・トウズニ
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者 ズン・レン・ツェン
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者 フィル・ジェイ・ボストリー
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官 後藤 彰

(56)参考文献 特開２００６－１９６００５（ＪＰ，Ａ）
米国特許出願公開第２００６／０２０６６８７（ＵＳ，Ａ１）
特開平５－２５７８１１（ＪＰ，Ａ）
特開平２－ ３３６３９（ＪＰ，Ａ）
米国特許出願公開第２００７／０２８３１２３（ＵＳ，Ａ１）
特表２００５－５０９９４６（ＪＰ，Ａ）
THOMAS W. BARR, "SpecTLB: A Mechanism for Speculative Address Translation", 2011 38TH ANNUAL INTERNATIONAL SYMPOSIUM ON COMPUTER ARCHITECTURE (ISCA), 米国, IEEE, ２０１１年６月 ４日, P307-317

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ １２／１０
Ｇ０６Ｆ １２／１４