

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号
特表2025-513583
(P2025-513583A)

(43)公表日 令和7年4月24日(2025.4.24)

(51)国際特許分類
G 0 6 F 21/52 (2013.01)

F I
G 0 6 F 21/52

審査請求 未請求 予備審査請求 未請求 (全66頁)			
(21)出願番号	特願2024-562930(P2024-562930)	(71)出願人	500395107
(86)(22)出願日	令和5年3月17日(2023.3.17)		アーム・リミテッド
(85)翻訳文提出日	令和6年11月13日(2024.11.13)		グレート・ブリテン及び北部アイルラン
(86)国際出願番号	PCT/GB2023/050658		ド連合王国、イングランド、シー・ビー
(87)国際公開番号	WO2023/209324		ー1、9エヌ・ジェイ、ケンブリッジ、
(87)国際公開日	令和5年11月2日(2023.11.2)		フルボーン・ロード 1 1 0
(31)優先権主張番号	2206166.7	(74)代理人	110000855
(32)優先日	令和4年4月28日(2022.4.28)		弁理士法人浅村特許事務所
(33)優先権主張国・地域又は機関		(72)発明者	ヴァングレディ、マドウスダナ レディ
	英国(GB)		インド 5 6 0 0 4 8 バンガロール マ
(81)指定国・地域	AP(BW,CV,GH,GM,KE,LR,LS,MW,MZ ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW), EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES, FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV		ハデバブラ マラタハリ アウター リング
	最終頁に続く		ロード シトリン ブロック フィフス ア
			ンド シックス フロア アーム エンベデ
			ッド テクノロジーズ プライベート リ
			ミテッド
			最終頁に続く

(54)【発明の名称】 メモリ管理

(57)【要約】

ターゲット仮想アドレスは、メモリアクセス要求に対してターゲット物理アドレスに変換される。少なくとも書き込み要求に関して、ターゲット仮想アドレスに対応するターゲットメモリ領域が、リターン状態情報を保護するためのGCSデータ構造を記憶するためのガード制御スタック（GCS）領域であり、メモリアクセス要求が、GCSアクセス命令タイプの制限されたサブセットのうちの1つによってトリガされるGCSメモリアクセス要求ではないことをターゲットステージ1変換テーブルエントリが指定するとき、メモリアクセス要求は拒否される。アンチエイリアシング特性がターゲットメモリ領域に対して指定されている場合、ターゲットステージ1変換テーブルエントリ又はターゲットステージ1変換テーブルエントリを見つけるために使用される別のステージ1変換テーブルエントリが、変換ハードニング機構によって保護されていない非ハードニングエントリである場合、メモリアクセス要求は拒否される。少なくとも1つの動作状態において、アンチエイリアシング特性がターゲットメモリ領域に対して指定されていない場合、G

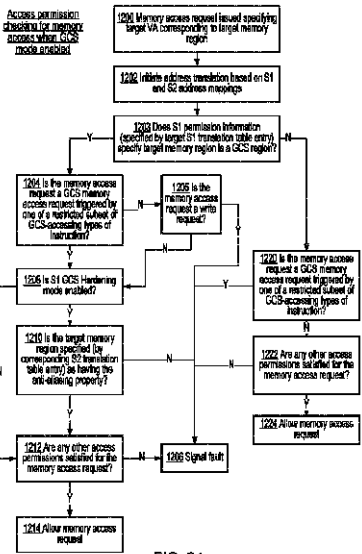


FIG. 24

【特許請求の範囲】

【請求項 1】

装置であって、

複数の実行状態のうちの 1 つにおいて命令を実行する処理回路と、

アクセスされるべきターゲットメモリ領域に対応するターゲット仮想アドレスを指定するメモリアクセス要求に応答して、前記ターゲット仮想アドレスをターゲット物理アドレスに変換するためのアドレス管理回路であって、前記ターゲット仮想アドレスから前記ターゲット物理アドレスへのマッピングは、ステージ 1 変換テーブル構造内のターゲットステージ 1 変換テーブルエントリによって前記ターゲット仮想アドレスに対して指定されたステージ 1 アドレスマッピングに少なくとも依存し、前記ステージ 1 変換テーブル構造は、第 1 の実行状態で前記処理回路によって実行される命令によって設定可能なステージ 1 ベースアドレスを使用してアクセス可能である、メモリ管理回路と、を備え、

10

少なくとも前記メモリアクセス要求が書き込み要求である場合、前記メモリ管理回路は、以下の条件：

前記ターゲットステージ 1 変換テーブルエントリによって指定されるステージ 1 許可情報は、前記ターゲットメモリ領域が、関数呼び出しや例外から戻るためのリターン状態情報を保護するための GCS データ構造を記憶するためのガード制御スタック (GCS) 領域であることを指定する、及び、

前記メモリアクセス要求は、GCS アクセスタイプの命令の制限されたサブセットのうちの 1 つによってトリガされる GCS メモリアccess 要求以外の要求である、

20

の両方が満たされると決定したことに応答して前記メモリアクセス要求を拒否するように構成され、

前記メモリ管理回路は、前記第 1 の実行状態よりも大きな特権を有する第 2 の実行状態で前記処理回路によって実行される命令によって設定可能な変換ハードニング情報に少なくとも基づいて、前記第 1 の実行状態で実行される命令によって改ざんされないように前記変換ハードニング機構によって保護される少なくとも 1 つのハードニングステージ 1 変換テーブルエントリを定義するための変換ハードニング機構をサポートするように構成され、

アンチエイリアシング特性が前記ターゲットメモリ領域に対して指定されている場合、前記メモリ管理回路は、前記ターゲットステージ 1 変換テーブルエントリ又は前記ターゲットステージ 1 変換テーブルエントリを見つけるために使用される別のステージ 1 変換テーブルエントリが、前記変換ハードニング機構によって保護されていない非ハードニング変換テーブルエントリであることを検出したことに応答して、前記メモリアクセス要求を拒否するように構成され、及び、

30

前記処理回路の少なくとも 1 つの動作状態において、前記メモリ管理回路は、前記メモリアクセス要求が前記 GCS メモリアccess 要求であり、前記アンチエイリアシング特性が前記ターゲットメモリ領域に対して指定されていないと決定したことに応答して、前記メモリアクセス要求を拒否するように構成される、

装置。

【請求項 2】

40

前記メモリ管理回路は、前記ステージ 1 アドレスマッピングが前記ターゲット仮想アドレスからターゲット中間アドレスへのマッピングを含む 2 ステージアドレス変換をサポートするように構成され、前記ターゲット仮想アドレスから前記ターゲット物理アドレスへの前記アドレスマッピングは、ステージ 2 変換テーブル構造内のターゲットステージ 2 変換テーブルエントリによって前記ターゲット中間アドレスに対して指定された、前記ターゲット中間アドレスから前記ターゲット物理アドレスへのステージ 2 アドレスマッピングにも依存し、前記ステージ 2 変換テーブル構造は、前記第 2 の実行状態で前記処理回路によって実行される命令によって設定可能なステージ 2 ベースアドレスを使用してアクセス可能である、請求項 1 に記載の装置。

【請求項 3】

50

前記ターゲットステージ 2 変換テーブルエントリは、前記アンチエイリアシング特性が前記ターゲットメモリ領域に対して指定されているかどうかを指定する、請求項 2 に記載の装置。

【請求項 4】

所与の中間アドレスに対応する所与のメモリ領域に記憶された所与のステージ 1 変換テーブルエントリについて、前記所与のステージ 1 変換テーブルエントリがハードニングステージ 1 変換テーブルエントリであるかどうかを指定するための前記変換ハードニング情報には、前記所与の中間アドレスに対応する、対応するステージ 2 変換テーブルエントリによって指定されるステージ 2 許可情報が含まれる、請求項 2 又は 3 に記載の装置。

【請求項 5】

各ハードニングステージ 1 変換テーブルエントリは、そのステージ 1 変換テーブルエントリを記憶する前記所与のメモリ領域が、前記対応するステージ 2 変換テーブルエントリの前記ステージ 2 許可情報によって、

書込み要求が禁止された読取り専用メモリ領域、及び、

書込み要求タイプの制限されたサブセットに対して前記部分読取り専用メモリ領域への書込み要求が許可され、前記制限されたサブセット以外の書込み要求タイプに対して禁止される部分読取り専用メモリ領域であって、書込み要求タイプの前記制限されたサブセットは、変換テーブルエントリ内のアクセス追跡メタデータを更新するために前記メモリ管理回路によって生成されるメタデータ更新書込み要求を少なくとも含む、部分読取り専用メモリ領域、

のうちの 1 つであるとするされるステージ 1 変換テーブルエントリを含む、請求項 4 に記載の装置。

【請求項 6】

前記ステージ 2 許可情報は、前記読取り専用メモリ領域及び前記部分読取り専用メモリ領域の両方を示すための符号化を有する、請求項 5 に記載の装置。

【請求項 7】

前記ステージ 2 許可情報は、前記所与のメモリ領域が、前記部分読取り専用メモリ領域への書込み要求が、書込み要求タイプの制限されたサブセットに対して許可され、前記制限されたサブセット以外の書込み要求タイプに対して禁止される部分読取り専用メモリ領域であるかどうかを指定し、前記書込み要求タイプの制限されたサブセットは、変換テーブルエントリ内のアクセス追跡メタデータを更新するために前記メモリ管理回路によって生成されたメタデータ更新書込み要求を少なくとも含む、及び、

前記メモリ管理回路は、前記第 1 の変換テーブル構造の各ステージ 1 変換テーブルエントリが、保護エントリとして指定されていない非保護ステージ 1 変換テーブルエントリと比較して、更新が制限された保護エントリであるかどうかを指定する符号化を有する前記ステージ 1 変換テーブル構造の各ステージ 1 変換テーブルエントリをサポートするように構成され、前記書込み要求タイプの制限されたサブセットは、非保護ステージ変換テーブルエントリを更新することは許可されるが、保護ステージ 1 変換テーブルエントリのビットの少なくともサブセットを更新することは禁止される書込み要求タイプを含む、請求項 4 に記載の装置。

【請求項 8】

前記処理回路は、所与のメモリシステムロケーションへの更新を要求するための保護エントリチェックタイプの読取りチェック書込み命令を実行する処理回路に応答する保護エントリチェックを含み、

前記所与のメモリシステムロケーションからデータを読取り、

前記所与のメモリシステムロケーションから読取られた前記データが、保護エントリとして指定されたステージ 1 変換テーブルエントリと一致する値を有するかどうかをチェックし、

前記所与のメモリシステムロケーションから読取られた前記データが、保護エントリとして指定されたステージ 1 変換テーブルエントリと一致する値を有すると決定したことに

10

20

30

40

50

応答して、前記ステージ 1 変換テーブルエントリの更新制限されたビットのサブセットが、前記読取りチェック書込み命令に応答して更新されることを防止し、

前記書込み要求タイプの制限されたサブセットは、前記保護エントリチェックタイプの読取りチェック書込み命令に応答して発行される書込み要求を含む、

請求項 7 に記載の装置。

【請求項 9】

前記変換ハードニング情報は、所与のステージ 1 変換テーブルエントリが前記保護エントリとして指定されているかどうかを示す情報を含み、前記メモリ管理回路は、前記対応するステージ 2 変換テーブルエントリによって指定された前記ステージ 2 許可情報が、前記所与のメモリ領域が前記部分読取り専用メモリ領域であることを指定する場合、非保護ステージ 1 変換テーブルエントリを非ハードニングステージ 1 変換テーブルエントリとして扱うように構成される、請求項 7 又は 8 に記載の装置。

10

【請求項 10】

各ハードニングステージ 1 変換テーブルエントリは、

前記所与のメモリ領域が、書込み要求が禁止される読取り専用メモリ領域であるとして前記ステージ 2 許可情報によって示されるステージ 1 変換テーブルエントリ、及び、

前記所与のメモリ領域が、前記部分読取り専用メモリ領域であるとして前記ステージ 2 許可情報によって示される保護エントリとして指定されるステージ 1 変換テーブルエントリ、

のうちの 1 つを含む、請求項 7 ～ 9 のいずれか一項に記載の装置。

20

【請求項 11】

前記処理回路の前記少なくとも 1 つの動作状態は、GCS 変換ハードニングチェックイネーブル制御パラメータが、GCS メモリアクセス要求は前記アンチエイリアシング特性が前記ターゲットメモリ領域に対して指定されているかどうかのチェックを受けるべきである、ことを示すイネーブル状態に設定される動作状態を含む、請求項 1 ～ 10 のいずれか一項に記載の装置。

【請求項 12】

前記メモリ管理回路は、前記メモリアクセス要求が前記 GCS メモリアクセス要求であり、且つ、前記ステージ 1 許可情報が前記ターゲット仮想アドレスに対応する前記メモリ領域が前記 GCS 領域であることを指定しないと決定したことに応答して、前記メモリアクセス要求を拒否するように構成される、請求項 1 ～ 11 のいずれか一項に記載の装置。

30

【請求項 13】

GCS アクセスタイプの命令の前記制限されたサブセットは、前記処理回路の 1 つ以上のレジスタに示される情報に基づいて取得されたリターン状態情報を前記 GCS データ構造にプッシュするように前記処理回路を制御するリターン状態プッシュ命令を含む、請求項 1 ～ 12 のいずれか一項に記載の装置。

【請求項 14】

前記 GCS アクセスタイプの命令の制限されたサブセットは、前記 GCS データ構造からリターン状態情報をポップするように前記処理回路を制御するリターン状態ポップ命令を含む、請求項 1 ～ 13 のいずれか一項に記載の装置。

40

【請求項 15】

前記ガード制御スタックデータ構造のアドレスを示すスタックポインタを記憶するための少なくとも 1 つの GCS ポインタレジスタを備える、請求項 1 ～ 14 のいずれか一項に記載の装置。

【請求項 16】

前記ターゲットメモリ領域が前記 GCS 領域であるかどうかを指定する前記ステージ 1 許可情報は、前記ターゲットステージ 1 変換テーブルエントリによって参照される許可間接レジスタのフィールド内で指定される、請求項 1 ～ 15 のいずれか一項に記載の装置。

【請求項 17】

方法であって、

50

複数の実行状態のうちの1つで命令を実行する工程と、

アクセスされるターゲットメモリ領域に対応するターゲット仮想アドレスを指定するメモリアクセス要求に応答して、前記ターゲット仮想アドレスをターゲット物理アドレスに変換する工程であって、前記ターゲット仮想アドレスから前記ターゲット物理アドレスへのマッピングは、ステージ1変換テーブル構造内のターゲットステージ1変換テーブルエントリによって前記ターゲット仮想アドレスに対して指定されるステージ1アドレスマッピングに少なくとも依存し、前記ステージ1変換テーブル構造は、第1の実行状態で前記処理回路によって実行される命令によって設定可能なステージ1ベースアドレスを使用してアクセス可能である、工程と、を備え、

少なくとも前記メモリアクセス要求が書き込み要求である場合、前記メモリアクセス要求は、以下の条件：

前記ターゲットステージ1変換テーブルエントリによって指定されるステージ1許可情報は、前記ターゲットメモリ領域が、関数呼び出しや例外から戻るためのリターン状態情報を保護するためのGCSデータ構造を記憶するためのガード制御スタック（GCS）領域であることを指定する、及び、

前記メモリアクセス要求は、GCSアクセスタイプの命令の制限されたサブセットのうちの1つによってトリガされるGCSメモリアクセス要求以外の要求である、

の両方が満たされると決定したことに応答して拒否されるように構成され、

前記第1の実行状態よりも大きな特権を有する第2の実行状態で実行される命令によって設定可能な変換ハードニング情報に少なくとも基づいて、前記第1の実行状態で実行される命令によって改ざんされないように前記変換ハードニング機構によって保護される少なくとも1つのハードニングステージ1変換テーブルエントリを定義するために、変換ハードニング機構がサポートされ、

前記方法は、

アンチエイリアシング特性が前記ターゲットメモリ領域に対して指定されている場合、前記ターゲットステージ1変換テーブルエントリ又は前記ターゲットステージ1変換テーブルエントリを見つけるために使用される別のステージ1変換テーブルエントリが、前記変換ハードニング機構によって保護されていない非ハードニング変換テーブルエントリであることを検出したことに応答して、前記メモリアクセス要求を拒否する工程と、

前記処理回路の少なくとも1つの動作状態において、前記メモリアクセス要求が前記GCSメモリアクセス要求であり、前記アンチエイリアシング特性が前記ターゲットメモリ領域に対して指定されていないと決定したことに応答して、前記メモリアクセス要求を拒否する工程と、

を含む、方法。

【請求項18】

ホストデータ処理装置によって実行される場合に、ターゲットコードを実行するための命令実行環境を提供するように前記ホストデータ処理装置を制御するコンピュータプログラムであって、前記コンピュータプログラムは、

複数の実行状態のうちの1つにおいて前記ターゲットコードの命令の実行をシミュレートする処理プログラムロジックと、

アクセスされるターゲットメモリ領域に対応するターゲット仮想アドレスを指定するメモリアクセス要求に応答して、前記ターゲット仮想アドレスをシミュレートされたターゲット物理アドレスに変換するメモリ管理プログラムロジックであって、前記ターゲット仮想アドレスから前記シミュレートされたターゲット物理アドレスへのマッピングは、ステージ1変換テーブル構造内のターゲットステージ1変換テーブルエントリによって前記ターゲット仮想アドレスに対して指定されたステージ1アドレスマッピングに少なくとも依存し、前記ステージ1変換テーブル構造は、第1の実行状態で実行されるようにシミュレートされた命令によって設定可能なステージ1ベースアドレスを使用してアクセス可能である、メモリ管理プログラムロジックと、を含み、

少なくとも前記メモリアクセス要求が書き込み要求である場合、前記メモリ管理プログラ

10

20

30

40

50

ムロジックは、以下の条件：

前記ターゲットステージ1変換テーブルエントリによって指定されるステージ1許可情報は、前記ターゲットメモリ領域が、関数呼び出しや例外から戻るためのリターン状態情報を保護するためのGCSデータ構造を記憶するためのガード制御スタック（GCS）領域であることを指定する、及び、

前記メモリアクセス要求は、GCSアクセスタイプの命令の制限されたサブセットのうちの1つによってトリガされるGCSメモリアクセス要求以外の要求である、

の両方が満たされると決定したことに応答して拒否されるように構成され、

メモリ管理プログラムロジックは、第1の実行状態よりも大きな特権を有する第2の実行状態で実行されるようにシミュレートされた命令によって設定可能な変換ハードニング情報に少なくとも基づいて、第1の実行状態で実行されるようにシミュレートされた命令によって改ざんされないように変換ハードニング機構によって保護される少なくとも1つのハードニングステージ1変換テーブルエントリを定義するための変換ハードニング機構をサポートするように構成され、

アンチエイリアシング特性が前記ターゲットメモリ領域に対して指定されている場合、前記メモリ管理プログラムロジックは、前記ターゲットステージ1変換テーブルエントリ又は前記ターゲットステージ1変換テーブルエントリを見つけるために使用される別のステージ1変換テーブルエントリが、前記変換ハードニング機構によって保護されていない非ハードニング変換テーブルエントリであることを検出したことに応答して、前記メモリアクセス要求を拒否するように構成され、

前記処理回路の少なくとも1つの動作状態において、前記メモリ管理回路は、前記メモリアクセス要求が前記GCSメモリアクセス要求であり、前記アンチエイリアシング特性が前記ターゲットメモリ領域に対して指定されていないと決定したことに応答して、前記メモリアクセス要求を拒否するように構成される、

コンピュータプログラム。

【請求項19】

請求項18に記載のコンピュータプログラムを記憶する記憶媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本技法は、データ処理の分野に関する。

【0002】

データ処理装置では、メモリシステムへのアクセスを制御するためのメモリ管理回路が設けられる。メモリ管理回路は、処理回路によって実行される命令のオペランドに基づいて指定されたターゲット仮想アドレスを、アクセスされるメモリシステムの位置を識別するターゲット物理アドレスに変換するためのアドレス変換を実行する役割を果たす。メモリ管理回路は、例えば、ターゲット仮想アドレスからターゲット物理アドレスへのマッピングを指定するために使用される変換テーブル構造において指定された情報に基づいて、アクセス許可を実施することもある。

【0003】

少なくともいくつかの例は、複数の実行状態のうちの1つで命令を実行する処理回路と、アクセスされるターゲットメモリ領域に対応するターゲット仮想アドレスを指定するメモリアクセス要求に応答して、ターゲット仮想アドレスをターゲット物理アドレスに変換するメモリ管理回路であって、ターゲット仮想アドレスからターゲット物理アドレスへのマッピングは、ステージ1変換テーブル構造内のターゲットステージ1変換テーブルエントリによってターゲット仮想アドレスに対して指定されるステージ1アドレスマッピングに少なくとも依存し、ステージ1変換テーブル構造は、第1の実行状態で処理回路によって実行される命令によって設定可能なステージ1ベースアドレスを使用してアクセス可能である、メモリ管理回路を含む装置を提供し、少なくともメモリアクセス要求が書込み要求である場合、ターゲットステージ1変換テーブルエントリによって指定されるステー

ジ 1 許可情報が、ターゲットメモリ領域が関数呼び出しや例外から戻るためのリターン状態情報を保護するための GCS データ構造を記憶するためのガード制御スタック (GCS) 領域であることを指定すること、及び、メモリアクセス要求が、GCS アクセスタイプの命令の制限されたサブセットのうちの 1 つによってトリガされる GCS メモリアクセス要求以外の要求であること、の両方の条件が満たされると決定したことに応答して、メモリ管理回路は、メモリアクセス要求を拒否するように構成され、メモリ管理回路は、第 1 の実行状態よりも大きな特権を有する第 2 の実行状態で処理回路によって実行される命令によって設定可能な変換ハードニング情報に少なくとも基づいて、第 1 の実行状態で実行される命令によって改ざんされないように変換ハードニング機構によって保護される少なくとも 1 つのハードニングステージ 1 変換テーブルエントリを定義するための変換ハードニング機構をサポートするように構成され、アンチエイリアシング特性がターゲットメモリ領域に対して指定されている場合、メモリ管理回路は、ターゲットステージ 1 変換テーブルエントリ又はターゲットステージ 1 変換テーブルエントリを見つけるために使用される別のステージ 1 変換テーブルエントリが、変換ハードニング機構によって保護されていない非ハードニング変換テーブルエントリであることを検出したことに応答して、メモリアクセス要求を拒否するように構成され、処理回路の少なくとも 1 つの動作状態において、メモリ管理回路は、メモリアクセス要求が GCS メモリアクセス要求であり、アンチエイリアシング特性がターゲットメモリ領域に対して指定されていないと決定したことに応答して、メモリアクセス要求を拒否するように構成される。

10

20

【 0 0 0 4 】

少なくともいくつかの例は、複数の実行状態のうちの 1 つで命令を実行することと、アクセスされるターゲットメモリ領域に対応するターゲット仮想アドレスを指定するメモリアクセス要求に応答して、ターゲット仮想アドレスをターゲット物理アドレスに変換することと、を含む方法を提供し、ターゲット仮想アドレスからターゲット物理アドレスへのマッピングは、ステージ 1 変換テーブル構造内のターゲットステージ 1 変換テーブルエントリによってターゲット仮想アドレスに対して指定されるステージ 1 アドレスマッピングに少なくとも依存し、ステージ 1 変換テーブル構造は、第 1 の実行状態で処理回路によって実行される命令によって設定可能なステージ 1 ベースアドレスを使用してアクセス可能であり、少なくともメモリアクセス要求が書き込み要求である場合、ターゲットステージ 1 変換テーブルエントリによって指定されるステージ 1 許可情報が、ターゲットメモリ領域が関数呼び出しや例外から戻るためのリターン状態情報を保護するための GCS データ構造を記憶するためのガード制御スタック (GCS) 領域であることを指定すること、及び、メモリアクセス要求が、GCS アクセスタイプの命令の制限されたサブセットのうちの 1 つによってトリガされる GCS メモリアクセス要求以外の要求であること、の両方の条件が満たされると決定したことに応答して、メモリアクセス要求は拒否され、第 1 の実行状態よりも大きな特権を有する第 2 の実行状態で実行される命令によって設定可能な変換ハードニング情報に少なくとも基づいて、第 1 の実行状態で実行される命令によって改ざんされないように変換ハードニング機構によって保護される少なくとも 1 つのハードニングステージ 1 変換テーブルエントリを定義するために、変換ハードニング機構がサポートされ、方法は、アンチエイリアシング特性がターゲットメモリ領域に対して指定されている場合に、ターゲットステージ 1 変換テーブルエントリ又はターゲットステージ 1 変換テーブルエントリを見つけるために使用される別のステージ 1 変換テーブルエントリが、変換ハードニング機構によって保護されていない非ハードニング変換テーブルエントリであることを検出したことに応答して、メモリアクセス要求を拒否することと、処理回路の少なくとも 1 つの動作状態において、メモリアクセス要求が GCS メモリアクセス要求であり、アンチエイリアシング特性がターゲットメモリ領域に対して指定されていないと決定したことに応答して、メモリアクセス要求を拒否することと、を含む。

30

40

【 0 0 0 5 】

少なくともいくつかの例は、ホストデータ処理装置によって実行される場合、ターゲットコードを実行するための命令実行環境を提供するようにホストデータ処理装置を制御す

50

る命令を含むコンピュータプログラムを提供し、コンピュータプログラムは、複数の実行状態のうちの1つにおいてターゲットコードの命令の実行をシミュレートする処理プログラムロジックと、アクセスされるターゲットメモリ領域に対応するターゲット仮想アドレスを指定するメモリアクセス要求に応答して、ターゲット仮想アドレスをシミュレートされたターゲット物理アドレスに変換するメモリ管理プログラムロジックとを含み、ターゲット仮想アドレスからシミュレートターゲット物理アドレスへのマッピングは、ステージ1変換テーブル構造内のターゲットステージ1変換テーブルエントリによってターゲット仮想アドレスに対して指定されたステージ1アドレスマッピングに少なくとも依存し、ステージ1変換テーブル構造は、第1の実行状態で実行されるようにシミュレートされた命令によって設定可能なステージ1ベースアドレスを使用してアクセス可能であり、少なくともメモリアクセス要求が書き込み要求である場合、ターゲットステージ1変換テーブルエントリによって指定されるステージ1許可情報が、ターゲットメモリ領域が関数呼び出しや例外から戻るためのリターン状態情報を保護するためのGCSデータ構造を記憶するためのガード制御スタック(GCS)領域であることを指定すること、及び、メモリアクセス要求が、GCSアクセスタイプの命令の制限されたサブセットのうちの1つによってトリガされるGCSメモリアクセス要求以外の要求であること、の両方の条件が満たされると決定したことに応答して、メモリ管理プログラムロジックは、メモリアクセス要求を拒否するように構成され、メモリ管理プログラムロジックは、第1の実行状態よりも大きな特権を有する第2の実行状態で実行されるようにシミュレートされた命令によって設定可能な変換ハードニング情報に少なくとも基づいて、第1の実行状態で実行されるようにシミュレートされた命令によって改ざんされないように変換ハードニング機構によって保護される少なくとも1つのハードニングステージ1変換テーブルエントリを定義するための変換ハードニング機構をサポートするように構成され、アンチエイリアシング特性がターゲットメモリ領域に対して指定されている場合、メモリ管理プログラムロジックは、ターゲットステージ1変換テーブルエントリ又はターゲットステージ1変換テーブルエントリを見つけるために使用される別のステージ1変換テーブルエントリが、変換ハードニング機構によって保護されていない非ハードニング変換テーブルエントリであることを検出したことに応答して、メモリアクセス要求を拒否するように構成され、処理回路の少なくとも1つの動作状態において、メモリ管理回路は、メモリアクセス要求がGCSメモリアクセス要求であり、アンチエイリアシング特性がターゲットメモリ領域に対して指定されていないと決定したことに応答して、メモリアクセス要求を拒否するように構成される。

10

20

30

【0006】

コンピュータプログラムは、コンピュータ可読記憶媒体に記憶されてもよい。記憶媒体は、非一時的記憶媒体であってもよい。

【図面の簡単な説明】

【0007】

本技法の更なる態様、特徴、及び利点は、添付の図面と併せて読まれる以下の例の説明から明らかとなる。

【図1】処理回路及びメモリ管理回路を有するデータ処理装置の一例を示す。

40

【図2】処理回路の実行状態の一例を示す。

【図3】2ステージのアドレス変換を示す。

【図4】それぞれステージ1及びステージ2アドレス変換のための変換テーブルウォークの一例を示す。

【図5】それぞれステージ1及びステージ2アドレス変換のための変換テーブルウォークの一例を示す。

【図6】ステージ1で決定された各テーブルベースアドレス及び最終中間アドレスが、それぞれのステージ2変換を使用して物理アドレスに変換されることを考慮するときの、ステージ1変換及びステージ2変換の両方の完全変換テーブルウォークのために実行されるテーブルルックアップを示す。

50

【図 7】メモリ管理を制御するためのメモリ管理回路及び制御レジスタの一例を示す。

【図 8】ステージ 1 及びステージ 2 アドレス変換のための変換テーブルエントリの一例を示す。

【図 9】ステージ 2 変換テーブルエントリによって定義された部分読取り専用メモリ領域への書き込みを許可された書き込み要求及び禁止された書き込み要求のタイプを示す。

【図 10】アドレス変換及び許可チェックを実行する方法を示す。

【図 11】部分読取り専用許可に基づくチェックを示すフロー図である。

【図 12】保護エントリチェックタイプの読取りチェック書き込み命令の異なるバリエーションの処理を示す。

【図 13-1】保護エントリチェックタイプの読取りチェック書き込み命令の異なるバリエーションの処理を示す。

【図 13-2】保護エントリチェックタイプの読取りチェック書き込み命令の異なるバリエーションの処理を示す。

【図 14-1】保護エントリチェックタイプの読取りチェック書き込み命令の異なるバリエーションの処理を示す。

【図 14-2】保護エントリチェックタイプの読取りチェック書き込み命令の異なるバリエーションの処理を示す。

【図 15】同じ中間アドレス上への仮想アドレスのエイリアシングを示す。

【図 16】アンチエイリアシングチェックを示す。

【図 17】ステージ 1 トップレベルテーブル存在チェック及びステージ 1 トップレベル部分読取り専用チェックを示す。

【図 18】変換テーブルエントリによって間接的に指定された許可情報を示す。

【図 19】関数呼び出し及びリターンの一例を示す。

【図 20】ガード制御スタック (GCS) データ構造へのアクセスを制御するためのレジスタを示す。

【図 21】関数呼び出しや例外から戻るためのリターン状態情報を保護するための GCS データ構造の使用を示す。

【図 22】リターン状態プッシュ命令の処理を示すフロー図である。

【図 23】リターン状態ポップ命令の処理を示すフロー図である。

【図 24】GCS モードがイネーブルにされているときに発行されるメモリアクセス要求に対してメモリ管理回路によって実行されるアクセス許可チェックを示す。

【図 25】使用され得るシミュレータ実装を示す。

【0008】

装置は、多数の実行状態のうちの 1 つで命令を実行する処理回路と、アクセスすべきターゲットメモリ領域に対応するターゲット仮想アドレスを指定するメモリアクセス要求にตอบสนองして、ターゲット仮想アドレスをターゲット物理アドレスに変換するメモリ管理回路とを有する。ターゲット仮想アドレスからターゲット物理アドレスへのマッピングは、ステージ 1 変換テーブル構造内のターゲットステージ 1 変換テーブルエントリによってターゲット仮想アドレスに対して指定されるステージ 1 アドレスマッピングに少なくとも依存する。ステージ 1 変換テーブル構造は、第 1 の実行状態で処理回路によって実行される命令によって設定可能なステージ 1 ベースアドレスを使用してアクセス可能である。

【0009】

リターン指向プログラミング (ROP) に基づく攻撃は、データ処理システムに対する一般的なクラスの攻撃である。ROP 攻撃とは、関数呼び出しや例外から戻るために使用されるリターン状態情報を破損することによって、プログラムを予期せぬ方法で動作させようとする攻撃である。多くの場合、ソフトウェアは、例えば関数呼び出しや例外のネストを容易にするために、リターン状態情報をメモリに保存し、(ネストされた関数呼び出しや例外のセットの) 外部関数呼び出しや例外のリターン状態情報は、内部関数呼び出しや例外のリターン状態情報と共にレジスタに上書きされ得る前にメモリに保存される。ROP 攻撃は、リターン状態情報がレジスタに復元され、関数リターンや例外リターンを制

10

20

30

40

50

御するために使用される前に、リターン状態情報がメモリに記憶されている間にリターン状態情報を改ざんしようと試みることができる。ROP 攻撃が成功すると、関数が呼び出された時点や例外が発生した時点の後の次の命令以外の命令にプログラムフローを戻す関数リターンや例外リターンを引き起こすことができ、これにより、攻撃者は、プログラマが意図した一連の動作以外の任意の処理を実行するように処理回路を制御することができる。

【0010】

ROP ベースの攻撃からガードするために、関数呼び出しや例外から戻るためのリターン状態情報を保護するために使用されるガード制御スタック (GCS) データ構造を提供することが有用であり得る。ステージ1変換テーブルエントリは、所与の仮想アドレスに対応するメモリ領域が、GCS データ構造を記憶するための GCS 領域であるかどうかを指定する。ターゲット仮想アドレスを指定するメモリアクセス要求に応答して、少なくともメモリアクセス要求が書き込み要求であるとき、メモリ管理回路は、以下の条件の両方を満たすと決定したことに応答して、メモリアクセス要求を拒否する。

●ターゲットステージ1変換テーブルエントリによって指定されたステージ1許可情報は、ターゲットメモリ領域が、関数呼び出しや例外から戻るためのリターン状態情報を保護するための GCS データ構造を記憶するためのガード制御スタック (GCS) 領域であることを指定する。

●メモリアクセス要求は、GCS アクセスタイプの命令の制限されたサブセットのうちの1つによってトリガされる GCS メモリアクセス要求以外の要求である。

【0011】

したがって、メモリの領域は、関数呼び出しや例外のリターン状態情報を確保するために使用される GCS 領域として、対応するステージ1変換テーブルエントリによって指定することができる。その領域に記憶された情報は、関数リターンや例外リターンに進む前に、リターン状態情報が適切であるかどうかを検証するために使用できる。GCS 領域として指定された領域への書き込みは、GCS アクセスタイプの命令の制限されたサブセット以外の命令に응答して行われた場合、拒否される。GCS 領域への書き込みアクセスを特定の命令タイプのみによって制限することによって、実行中のプログラムコード内に含まれる他のタイプのメモリアクセス命令によってトリガされた書き込み要求は（それらのアドレスオペランドの修正に続いて GCS 領域にアクセスするようにだまされた場合）、GCS 領域に記憶された情報を正常に更新するために使用することができないため、リターン状態情報を破損しようと試みる攻撃者の利用できる攻撃面を低減することができる。読取り要求は GCS 領域に記憶された保護リターン状態を更新することができないため、読取り要求にこの制限を適用することは必須ではないが、任意選択で、いくつかの実装形態は、読取り要求のターゲットメモリ領域が GCS 領域としてステージ1許可情報によって指定され、読取り要求が GCS アクセスタイプの命令の制限されたサブセットのうちの1つによってトリガされなかった場合に、失敗を通知することを選択することもできる。

【0012】

しかしながら、ステージ1変換テーブルエントリは、GCS 領域を指定するために使用され、ステージ1変換テーブル構造は、第1の実行状態（例えば、これは、オペレーティングシステムが実行される状態であり得る）で実行される命令によって制御可能なベースレジスタを介してアクセスされるので、攻撃者が、第1の実行状態で実行されているオペレーティングシステム又は他のソフトウェアを侵害することができる場合、攻撃者は、GCS 領域を指定するステージ1変換テーブルエントリによって提供される保護を回避しようと、メモリ領域がもはや GCS 領域として指定されないように、GCS 領域に対応するステージ1変換テーブルエントリを修正し、及び／又は対応するメモリ領域を GCS 領域として指定することなく、異なる仮想アドレスを GCS 領域の変換されたアドレスにマッピングするエイリアシングステージ1変換テーブルエントリを作成することができる。

【0013】

以下で説明する例では、メモリ管理回路は、第1の実行状態よりも大きな特権を有する

第2の実行状態で処理回路によって実行される命令によって設定可能な変換ハードニング情報に少なくとも基づいて、第1の実行状態で実行される命令によって改ざんされないように変換ハードニング機構によって保護される少なくとも1つのハードニングステージ1変換テーブルエントリを定義するための変換ハードニング機構をサポートする。アンチエイリアシング特性がターゲットメモリ領域に対して指定されている場合、メモリ管理回路は、ターゲットステージ1変換テーブルエントリ又はターゲットステージ1変換テーブルエントリを見つけるために使用される別のステージ1変換テーブルエントリが、変換ハードニング機構によって保護されていない非ハードニング変換テーブルエントリであることを検出したことに応答して、メモリアクセス要求を拒否する。処理回路の少なくとも1つの動作状態において、メモリ管理回路は、メモリアクセス要求がGCSメモリアクセス要求であり、アンチエイリアシング特性がターゲットメモリ領域に対して指定されていないと決定したことに応答して、メモリアクセス要求を拒否する。

10

【0014】

したがって、以下の手段の組合せが実施される。

ーGCS領域への書込み（ステージ1許可情報を使用して示される）は、特定の指定されたGCSアクセスタイプの命令を使用して実行されるように制限される。

ーステージ1変換テーブルエントリは、ステージ1変換テーブル構造のベースアドレスを制御することができる第1の実行状態よりも特権のある実行状態で実行される命令によって設定可能な情報に基づいて、ハードニングされたものとして指定することができる。

ーアンチエイリアシング特性を有するものとして指定されたメモリ領域は、非ハードニングステージ1変換テーブルエントリに基づいてアクセス不能である。

20

ーGCSメモリアクセス要求は、アンチエイリアシング特性がターゲットメモリ領域に設定されていない場合、拒否される。

【0015】

この手段の組合せにより、アンチエイリアシング特性を任意のGCSメモリ領域に適用する要件が強制される（そうでなければ、GCSメモリアクセス要求は失敗する）ので、GCSデータ構造を改ざんからはるかに安全に保護することができるが、一方アンチエイリアシング特性は、アンチエイリアシング特性がGCS領域に対して定義されるとき、GCS領域へのアクセスを可能にするために、非ハードニング変換テーブルエントリ（攻撃者による修正に対して脆弱であり得るか、又は攻撃者がハードニング変換テーブルエントリを回避するように定義したエイリアシング変換テーブルエントリであり得る）が使用できないことを強制する。したがって、このアプローチは、リターン指向プログラミングに基づく攻撃に対して、はるかに大きな保護を提供する。

30

【0016】

GCSメモリアクセス要求は、読取り要求及び書込み要求を含み得る。GCS読取り要求は、1つ以上のタイプのGCSアクセスロード命令によってトリガされてもよく、GCS書込み要求は、書込み要求をトリガする1つ以上のタイプのGCSアクセスストア命令によってトリガされてもよい。上述したように、GCSメモリアクセス要求は、少なくとも1つの動作状態において、アンチエイリアシング特性がターゲットメモリ領域に対して指定されていない場合に失敗が通知されるという要件に従う。この失敗は、GCSメモリアクセス要求が読取り要求であるか書込み要求であるかに関係なく通知され得る。したがって、GCSアクセスロード命令及びGCSアクセスストア命令の両方は、アンチエイリアシング特性がターゲットメモリ領域に対して指定されていない場合（メモリのGCS領域への読取り要求が、GCSアクセスタイプの命令以外の命令によって引き起こされたときは失敗をトリガしない場合であっても）、アンチエイリアシング特性及び失敗のチェックをトリガし得る。

40

【0017】

メモリ管理回路は、ステージ1アドレスマッピングがターゲット仮想アドレスからターゲット中間アドレスへのマッピングを含み、ターゲット仮想アドレスからターゲット物理アドレスへのアドレスマッピングが、ステージ2変換テーブル構造内のターゲットステ

50

ージ 2 変換テーブルエントリによってターゲット中間アドレスに対して指定されたターゲット中間アドレスからターゲット物理アドレスへのステージ 2 アドレスマッピングにも依存する、2 ステージアドレス変換をサポートしてもよい。ステージ 2 変換テーブル構造は、第 2 の実行状態で処理回路によって実行される命令によって設定可能なステージ 2 ベースアドレスを使用してアクセス可能である。2 ステージアドレス変換は、同じハードウェアプラットフォーム上に多数のゲストオペレーティングシステムが共存するような仮想化をサポートするのに有用であり得る。第 2 の実行状態は、ゲストオペレーティングシステムの仮想化を制御するために使用されるハイパーバイザを実行するための実行状態であってもよい。

【0018】

10

アンチエイリアシング特性は、第 2 の実行状態で実行される命令によって設定可能であってもよい。アンチエイリアシング特性は、ステージ 2 変換テーブル構造とは別に、第 2 の実行状態で実行されるソフトウェアによって維持されるデータ構造内のターゲットメモリ領域に対して指定することができる。

【0019】

しかしながら、ステージ 2 変換テーブル構造は、いずれの場合も、第 2 の実行状態で実行されるソフトウェアによって管理され得るので、アンチエイリアシング特性がターゲットメモリ領域に対して指定されているかどうかを、ターゲットステージ 2 変換テーブルエントリが指定することが最も効率的であり得る。

【0020】

20

同様に、変換ハードニング情報は、ステージ 2 変換テーブル構造とは別個のデータ構造を使用して第 2 の実行状態で実行されるソフトウェアによって定義される情報を含むことができるが、変換ハードニング情報を含む許可情報を定義するためにステージ 2 変換テーブル構造を再利用する方がより効率的であり得る。したがって、所与の中間アドレスに対応する所与のメモリ領域に記憶された所与のステージ 1 変換テーブルエントリについて、所与のステージ 1 変換テーブルエントリがハードニングステージ 1 変換テーブルエントリであるかどうかを指定するための変換ハードニング情報には、所与の中間アドレスに対応する、対応するステージ 2 変換テーブルエントリによって指定されるステージ 2 許可情報が含まれる。

【0021】

30

ソフトウェアが適切なアクセス許可又はアドレスマッピングを設定して、ステージ 2 変換テーブルエントリが、第 1 の実行状態や特権のより低い状態で実行されるソフトウェアによって更新されないように保護されることを保証することを強制するためのアーキテクチャ機構を提供することは必須ではない。ステージ 2 変換テーブル構造を担う第 2 の実行状態で実行されるハイパーバイザソフトウェアは、第 1 の実行状態（又は、第 1 の実行状態よりも特権の低い実行状態）で実行されるオペレーティングシステムソフトウェア又は他のソフトウェアによる修正に対してそれらの構造を保護するための手段を講じることが一般的である。例えば、ハイパーバイザは、ステージ 2 変換テーブル構造のエントリを、第 1 の実行状態（又は、より低い特権状態）で実行されるソフトウェアによって使用されるステージ 2 変換テーブル構造内のどの中間物理アドレスにもマッピングされない物理アドレスに対応するメモリ領域に割り振ることによってこれを行うことができ、したがって、第 1 の実行状態のソフトウェアは、それらの領域にアクセスする方法を有さない（代わりに、ステージ 2 変換テーブル構造を保護するために読取り専用許可を使用することができる）。ステージ 2 変換テーブル構造を記憶するメモリ領域が、第 1 の実行状態で実行されるソフトウェアによるアクセスに対して保護されることを保証するために、適切な変換テーブルマッピング及び／又は許可を定義する責任は、ステージ 2 変換テーブル構造を制御する第 2 の実行状態で実行されるソフトウェアにあり得る。したがって、装置が使用中であるとき、ハイパーバイザ（又は第 2 の実行状態で実行される他のソフトウェア）が、そのソフトウェア自体のニーズに適したアドレスマッピング及びアクセス許可を有するステージ 2 変換テーブル構造を構成して、ステージ 2 変換テーブルエントリを使用して指定

40

50

されるアンチエイリアシング特性及び変換ハードニング情報を、第2の実行状態（又はより特権のある実行状態）で実行される命令によって設定されるように制限することができ、第1の実行状態（又は、より特権のない実行状態）で実行される命令によって設定することができないようにすることが好ましい場合があるが、装置のハードウェアアーキテクチャが、第1の実行状態又はより特権のない実行状態で実行されるソフトウェアによる修正からステージ2変換テーブル構造を保護するために、それらのマッピング／アクセス許可が実際に設定されたことを強制するための特別なアーキテクチャ手段を提供する必要はない。例えば、アンチエイリアシング特性（又は変換ハードニング情報）を定義するために使用されるステージ2変換テーブルエントリ自体が改ざんに対して保護されているかどうかを検証するためのアーキテクチャ的に定義されたチェックは必要ない。ハイパーバイザソフトウェアは、それ自体の動作を保護するために、適切なステージ2アドレスマッピング／許可を設定すると仮定してもよい。

10

【0022】

変換ハードニング機構は、様々な方法で実装することができる。一般に、変換ハードニング機構は、特定のハードニングステージ1変換テーブルエントリが、非保護ステージ1変換テーブルエントリよりも、改ざんに対してより大きな保護を提供されることを可能にする任意のアーキテクチャ機構であり得る。例えば、ステージ1変換テーブルエントリに、エントリをハードニングされたものとしてマークする特定の符号化を提供することができ、処理回路又はメモリ管理回路は、メモリへの書き込みに関して、書き込まれるデータがステージ1変換テーブルエントリのハードニング符号化を有するかどうかをチェックすることができ、その場合、書き込みは抑制され得る。しかしながら、実際には、メモリへの書き込み（変換テーブルエントリを記憶していないメモリ領域への書き込みを含む）ごとにこのようなチェックを強制することは、非常に性能集約的であり、多くの電力を消費する可能性がある。

20

【0023】

変換ハードニング機構のためのより効率的な機構は、ハードニングステージ1変換テーブルエントリを記憶する領域のためのステージ2アドレスマッピングを提供するために使用されるステージ2変換テーブルエントリを使用してステージ2許可情報を指定することであり得、ステージ2許可情報は、対応する領域内のデータが修正される能力を制限する許可タイプを示す少なくとも1つの符号化を有する。例えば、その許可タイプは、書き込み要求が禁止されることを示す読取り専用許可、及び／又は、書き込み要求タイプの制限されたサブセットに対してのみ書き込み要求が許可されることを示す部分読取り専用許可タイプであり得る。

30

【0024】

例えば、各ハードニングステージ1変換テーブルエントリは、そのステージ1変換テーブルエントリを記憶する所与のメモリ領域が、対応するステージ2変換テーブルエントリのステージ2許可情報によって、以下のうちの1つであると示されるステージ1変換テーブルエントリを含んでもよい：

書き込み要求が禁止された読取り専用メモリ領域；

書き込み要求タイプの制限されたサブセットに対して部分読取り専用メモリ領域への書き込み要求が許可され、制限されたサブセット以外の書き込み要求タイプに対して禁止される部分読取り専用メモリ領域であって、書き込み要求タイプの制限されたサブセットは、変換テーブルエントリ内のアクセス追跡メタデータを更新するためにメモリ管理回路によって生成されるメタデータ更新書き込み要求を少なくとも含む、部分読取り専用メモリ領域。

40

【0025】

いくつかの実装形態では、ハードニングステージ1変換テーブルエントリのための読取り専用オプションのみをサポートし得る。これは、読取り専用許可はステージ2ですでにサポートされている可能性があり、読取り専用許可を強制することはそれほど複雑な制御ロジックを必要としないので、実装を簡素化し得る。

【0026】

50

他の実装形態は、部分読取り専用許可をサポートすることを選択することができ、これは、完全読取り専用許可はメモリ管理回路によって更新される変換テーブルエントリ内のアクセス追跡メタデータを妨げる可能性があるため、有用であり得る。このようなメタデータ更新書込み要求は、それぞれのメモリ領域へのアクセス頻度を追跡することを可能にするのに有用であり得て、オペレーティングシステムなどのソフトウェアが、例えば、どのメモリ領域を外部ストレージにページアウトし、どのメモリ領域をより高速アクセスのオンチップメモリ内に保持すべきかを決定するのに有用であり得る。アクセス追跡メタデータは、対応するアドレス領域に対してどのメモリアクセスが許可されるかを定義する許可に影響を与えない場合があるので、書込みアクセスがステージ1変換テーブルエントリの他の部分に対して許可されていない場合であっても、アクセス追跡メタデータを安全に更新することができる。したがって、部分読取り専用許可をサポートすることで、ソフトウェア開発者にとってセキュリティとプログラミングの容易さとのバランスが良くなり得る。

10

【0027】

いくつかの実装形態では、ハードニングステージ1変換テーブルエントリに対して、ステージ2で許可される許可唯一のタイプは、部分読取り専用許可であり得る。

【0028】

しかしながら、他の実装形態では、所与のステージ1変換テーブルエントリを記憶するメモリ領域のステージ2アドレスマッピングを定義する対応するステージ2変換テーブルエントリのステージ2許可情報に、読取り専用許可又は部分読取り専用許可のいずれかが定義される場合、所与のステージ1変換テーブルエントリは、ハードニングステージ1変換テーブルエントリと見なしてもよい。したがって、ステージ2許可情報が、読取り専用メモリ領域と部分読取り専用メモリ領域との両方を示すための符号化を有すること、及び、これらの符号化の両方が、対応するステージ1変換テーブルエントリ（そのステージ2許可情報が適用されるメモリ領域に記憶される）がハードニングされたと見なすことを可能にすることは、有用であり得る。これにより、第2の実行状態で実行するハイパーバイザ又は他のソフトウェアのプログラマは、対応するステージ1変換テーブルエントリの改ざんを防止するために、読取り専用許可又は部分読取り専用許可のどちらが好ましいかを選択するオプションを得る。

20

【0029】

ステージ2許可を読取り専用又は部分読取り専用に設定することは、対応するメモリ領域に記憶されたステージ1変換テーブルエントリをハードニングするのに有用であり得るが、実際には、ステージ2許可はページの粒度で設定され、単一ページに多くのステージ1変換テーブルエントリが記憶され得る。所与のページ内に記憶されたステージ1変換テーブルエントリの全てを、侵害されたオペレーティングシステム又は第1の実行状態で実行される他のソフトウェアによる改ざんから保護する必要はなくてもよい。しかしながら、所与のページに記憶された任意のステージ1変換テーブルエントリがハードニングを要求すると、そのページに対して設定された読取り専用又は部分読取り専用のステージ2許可は、書込み要求（又は、少なくとも部分読取り専用許可の場合は、書込み要求の制限されたサブセット以外の書込み要求）に例外ハンドラを実行させる原因となる失敗を引き起こし得る。対応するメモリ領域が、その領域内の他のエントリを改ざんから保護するために読取り専用許可又は部分読取り専用許可を有するようにステージ2アクセス許可で設定されているにもかかわらず、オペレーティングシステムが非機密情報に関連付けられたステージ1変換テーブルエントリを更新することを許可することが依然として望まれるとしても、1つのアプローチは、更新が許可されるかどうかを決定することができるハイパーバイザに各更新をトラップすることであり得るため、これは問題ではなくてもよい。しかしながら、そのような更新要求は比較的頻繁であり得るので、各正規の変換テーブルエントリ更新をハイパーバイザにトラップすることは、性能の損失を引き起こし得る。

30

40

【0030】

ハイパーバイザへのそのようなトラップは、以下の実装形態において回避することがで

50

きる。

ー 上述したように、ステージ 2 許可情報に定義されている部分読取り専用許可をサポートし、

ー 各ステージ 1 変換テーブルエントリに、そのステージ 1 変換テーブルエントリが、保護エントリとして指定されない非保護ステージ 1 変換テーブルエントリと比較して、更新が制限される保護エントリであるかどうかを指定する符号化を提供し、

ー メモリの部分読取り専用領域への書込みが許可されている書込み要求タイプの制限されたサブセットのうちの 1 つとして含まれる書込み要求タイプをサポートし、これは、非保護ステージ 1 変換テーブルエントリを更新することは許可されるが、保護ステージ 1 変換テーブルエントリのビットの少なくともサブセットを更新することは禁止される。

10

【0031】

このアプローチでは、ステージ 2 許可情報を使用して部分読取り専用許可でマークされたメモリ領域は、保護エントリと非保護エントリとの混合を含むことができるため、メモリ管理回路のハードウェアは、保護ステージ 1 変換テーブルエントリ内で保護されたビットの少なくともサブセットが更新されるのを防ぐことができる一方で、非保護エントリは、部分読取り専用領域に記憶されているにもかかわらず、ソフトウェアによって依然として更新することができる。これにより、非保護エントリの各更新をハイパーバイザにトラップする必要がなくなり、性能が向上する。

【0032】

例えば、書込み要求タイプの制限されたサブセット（メモリの部分読取り専用領域に記憶された非保護ステージ 1 変換テーブルエントリを更新することができる）は、保護エントリチェックタイプの読取りチェック書込み命令に応答して発行された書込み要求を含み得る。装置は、所与のメモリシステムロケーションへの更新を要求するための保護エントリチェックタイプの読取りチェック書込み命令を実行する処理回路に応答する保護エントリチェック回路を有することができ、所与のメモリシステムロケーションからデータを読み取り、所与のメモリシステムロケーションから読取られたデータが、保護エントリとして指定されたステージ 1 変換テーブルエントリと一致する値を有するかどうかをチェックし、所与のメモリシステムロケーションから読取られたデータが、保護エントリとして指定されたステージ 1 変換テーブルエントリと一致する値を有すると決定したことに応答して、ステージ 1 変換テーブルエントリの更新制限されたビットのサブセットが、読取りチェック書込み命令に
30 応答して更新されるのを防止する。更新制限されたビットのサブセットは、ステージ 1 変換テーブルエントリのビットの全てであってもよく、又はステージ 1 変換テーブルエントリのビットの適切なサブセット（全てのビットより少ない）であってもよい。更新制限されたビットのサブセットは、ステージ 1 変換テーブルエントリのビットの固定サブセットとして、又は、保護ステージ 1 変換テーブルエントリのビットのプログラム可能に定義されたサブセットとして（例えば、どのビットがプログラム可能に定義されたビットのサブセットであるかを示す制御レジスタに記憶された制御情報を用いて）、定義され得る。メモリの部分読取り専用領域内の非保護エントリ（及び、任意選択で保護エントリの非保護ビット）を更新することが許可される特定のタイプの読取りチェック書込み命令によってトリガされる特別なタイプの書込み要求を定義することによって（他のロード／ストア動作によってトリガされる他のタイプの書込み要求は、部分読取り専用領域に記憶されたデータを更新することが許可される書込み要求タイプの制限されたサブセットのうちの 1 つと見なされない場合がある）、これは、メモリの部分読取り専用領域への書込みごとに、（所与の書込み要求に対して更新されるデータが保護エントリであるかどうかをチェックするために）ハイパーバイザにトラップする例外をトリガする必要性を回避することができる。

20

30

40

【0033】

ステージ 1 変換テーブルエントリを保護されたものとして定義することをサポートする実装形態では、所与のステージ 1 変換テーブルエントリが保護エントリとして指定されているかどうかを示す情報も、変換ハードニング情報の一部と見なされ得る。メモリ管理回

50

路は、対応するステージ2変換テーブルエントリによって指定されたステージ2許可情報が、所与のメモリ領域が部分読取り専用メモリ領域であることを指定する場合、保護されていないステージ1変換テーブルエントリを、非ハードニングステージ1変換テーブルエントリとして扱ってもよい（読取り専用メモリ領域に記憶された非保護エントリは、依然としてハードニングされていると考えることができる）。したがって、各ハードニングされたステージ1変換テーブルエントリは、所与のメモリ領域が、書込み要求が禁止される読取り専用メモリ領域であるとしてステージ2許可情報によって示されるステージ1変換テーブルエントリ、及び、所与のメモリ領域が、部分読取り専用メモリ領域としてステージ2許可情報によって示される保護エントリとして指定されるステージ1変換テーブルエントリ、のうちの1つを含み得る。保護されていないステージ1変換テーブルエントリは、保護エントリチェックタイプの読取りチェック書込み命令を実行する第1の実行状態で動作するソフトウェアによって任意の方法で修正可能であるため、ステージ2許可情報によって定義された部分読取り専用メモリ領域に記憶されている場合であっても、これらをハードニングされていないものとして扱うことが最も安全である。保護されていないエントリは、読取り専用メモリ領域に記憶された場合は修正可能ではないので、読取り専用メモリ領域に記憶されたエントリに対して保護エントリであるという要件を課す必要はない。

10

【0034】

変換テーブルエントリを保護されたもの又は保護されていないものとして指定することは本質的な特徴ではなく、いくつかの実装形態はこれをサポートしなくてもよいことが理解されよう。例えば、ステージ1変換テーブルエントリをハードニングするためにステージ2読取り専用許可（部分読取り専用許可ではない）を使用するように制限される実装形態は、保護エントリ符号化をサポートする必要がない場合があり、部分読取り専用許可がサポートされている場合であっても、保護／非保護ステージ1変換テーブルエントリ符号化をサポートしない実装形態は、ハードニングされるように意図した変換テーブルエントリのみをステージ2において部分読取り専用許可でマークされた特定のページに割り振ることができるか、又は、対応する領域への全ての書込みをハイパーバイザにトラップすることができ、次いでハイパーバイザは、更新されているデータが改ざんに対してハードニングされるように意図したステージ1変換テーブルエントリであるかどうかに応じて、第1の実行状態にあるオペレーティングシステムによって要求された更新が許可されるかどうかを決定することができる。

20

30

【0035】

上述の変換ハードニング機構及びアンチエイリアシング特性は、GCSデータ構造にアクセスするために使用される変換エントリを保護することに特化したものではないが、侵害されたオペレーティングシステムによる改ざんに対して保護されることが望まれる機密情報を提供する他のデータ構造に使用される他のステージ1変換テーブルエントリの改ざん及びエイリアシングに対して保護するために使用することもできる、一般的なアーキテクチャ機構であってもよい。代替のアプローチとしては、ステージ2許可情報において、対応するメモリ領域を、ガード制御スタック構造を提供するために予約されたGCSメモリ領域として識別する専用符号化を定義することである。この代替アプローチでは、GCSステージ2許可は、GCSデータ構造へのアクセスを与えるために使用されるステージ1変換テーブルエントリを記憶するメモリ領域に対してステージ2で（装置が使用されているときにソフトウェアによって）適用される上述の変換ハードニング情報（例えば、読取り専用又は部分読取り専用許可）とは対照的に、GCSデータ構造を実際に記憶するメモリ領域に適用される。しかしながら、ステージ2において専用GCS許可を定義することの欠点は、所与のステージ2変換テーブルエントリのための許可情報を定義するために利用可能な符号化空間の量が限られている可能性があるため、専用GCS許可を定義することは、他の目的のためにより有用であり得る貴重な符号化空間を浪費する可能性があることである。GCS構造を保護する目的で、一般的な改ざんに対してステージ1アドレス変換をハードニングするために適用可能な汎用アーキテクチャ機構を再利用するが、ア

40

50

ンチエイリアシング特性がターゲットメモリ領域に対して指定されていない場合には G C S メモリアクセス要求を拒否する（変換ハードニング機構が適用されていないリスクがある場合に G C S アクセスを防止する）ことにより、リターン状態情報を保護するために使用されるガード制御スタックデータ構造のための専用保護にステージ 2 変換テーブルエントリ内の符号化空間を費やす必要性を回避することができ、その結果、変換テーブル構造をより効率的に符号化することができる。

【0036】

処理回路の全ての動作状態において発行される G C S メモリアクセス要求に対して、アンチエイリアシング特性をチェックする必要はない。イネーブル状態及びディセーブル状態に設定できる G C S 変換ハードニングチェックイネーブル制御パラメータが（例えば、制御レジスタ内に）提供され得る。処理回路の少なくとも 1 つの動作状態（アンチエイリアシング特性がターゲットメモリ領域に対して設定されていない場合に G C S メモリアクセス要求が拒否される）は、G C S 変換ハードニングチェックイネーブル制御パラメータが、G C S メモリアクセス要求はアンチエイリアシング特性がターゲットメモリ領域に対して指定されているかどうかのチェックを受けるべきである、ことを示すイネーブル状態に設定される動作状態を含み得る。G C S 変換ハードニングチェックイネーブル制御パラメータがディセーブル状態にある場合、G C S メモリアクセス要求が許可されるかどうかは、アンチエイリアシング特性がターゲットメモリ領域に対して設定されているかどうかとは無関係に決定され得る（したがって、G C S 変換ハードニングチェックがディセーブルにされているとき、アンチエイリアシング特性がターゲットメモリ領域に対して設定されていなくても、G C S メモリアクセス要求が許可されることが可能である）。G C S 変換ハードニングチェックのためのイネーブル／ディセーブル制御を提供することは、アンチエイリアシング特性をサポートしないアーキテクチャ用に書かれた可能性があるレガシーソフトウェアを実行するときに後方互換性を可能にするために有用であり得、その場合、G C S アンチエイリアシングチェックはディセーブルにされ得る。

【0037】

上述したように、G C S 領域への書込み要求は、G C S アクセスタイプの命令の制限されたサブセットのうちの 1 つによってトリガされない場合に拒否される（任意選択で、読取り要求も、G C S アクセスタイプの命令によってトリガされない場合に拒否することができるが、これは必須ではない）。メモリ管理回路はまた、メモリアクセス要求が G C S メモリアクセス要求であり、且つ、ステージ 1 許可情報がターゲット仮想アドレスに対応するメモリ領域が G C S 領域であることを指定しないと決定したことに応答して、メモリアクセス要求（書込み要求及び読取り要求の両方を含む）を拒否し得る。これは、G C S メモリアクセス要求が G C S 領域へアクセスするためにのみ使用でき、他のデータを記憶するために使用される通常のメモリ領域へアクセスするためには使用できないことを意味するため、攻撃者の利用できる攻撃面を低減する。つまり、G C S メモリアクセス要求が非 G C S 領域にアクセスするように、G C S アクセスタイプの命令のアドレスオペランドが攻撃者によって修正された（又は、攻撃者がプログラムフローの誤ったシーケンスを強制することによって誤ったものにされた）場合、これはエラーとして検出され、メモリアクセス要求は拒否されることを意味する。

【0038】

多数の異なるタイプの命令が、G C S アクセスタイプの命令の制限されたサブセットの一部としてサポートされ得る。

【0039】

例えば、G C S アクセスタイプの命令の制限されたサブセットは、処理回路の 1 つ以上のレジスタに示される情報に基づいて取得されたリターン状態情報を G C S データ構造にプッシュするように処理回路を制御するリターン状態プッシュ命令を含み得る。いくつかの例では、リターン状態プッシュ命令は、G C S データ構造へのリターン状態情報のプッシュを制御することに特化した専用 G C S 固有命令であり得る。しかしながら、リターン状態プッシュ命令の少なくとも 1 つのバリエーションが、リターン状態情報を G C S データ構

造にプッシュすることに加えて、処理回路が別の動作（例えば、関数を呼び出すときや例外を処理するときにソフトウェアによって実行されることが多い動作）を実行するように制御する命令であることも可能である。例えば、他の動作は、ターゲットアドレスへの分岐をトリガし、レジスタ（例えば、「リンクレジスタ」と呼ばれるレジスタ）に保存される関数リターンアドレスを制御する関数呼び出し分岐動作であり得る。例えば、「リンク付き分岐」命令（そのような関数呼び出し分岐動作を実行するように処理回路を制御するための）は、GCSデータ構造の使用をサポートするために処理回路のGCSモードで実行されるとき、リターン状態プッシュ命令として機能することもできる。GCSモードがディセーブルにされているとき、リンク付き分岐命令は、処理回路に、関数呼び出し分岐動作を実行させてもよいが、リターン状態情報をスタックデータ構造にプッシュする動作を実行させなくてもよい。GCSモードがイネーブルであるとき、リンク付き分岐命令は、処理回路に、関数呼び出し分岐動作とスタックデータ構造へのリターン状態情報のプッシュ（この特定の例では、リターン状態情報は、リンク付き分岐命令に応答してリンクレジスタに保存された関数リターンアドレスを含み得る）との両方を実行させることができる。

10

【0040】

GCSアクセスタイプの命令の制限されたサブセットはまた、GCSデータ構造からリターン状態情報をポップするように処理回路を制御するリターン状態ポップ命令も含み得る。いくつかの例では、リターン状態ポップ命令はまた、GCSデータ構造からポップされたリターン状態情報と、処理回路の1つ以上のレジスタに示された情報に基づいて決定された現在のリターン状態情報との間の不一致を決定することに応答して、失敗状態を通知するように処理回路を制御することができる。他の例では、それ自体はGCSデータ構造からリターン状態情報をポップしないが、以前のリターン状態ポップ命令によってGCSデータ構造からポップされた保護リターン状態が、レジスタ内の情報に基づいて決定された現在のリターン状態情報と一致するかどうかを検証する別個のリターン状態検証命令を定義することができる。リターン状態プッシュ及びポップ命令の多くのバリエーションは、例えば、例外リターン状態情報及び関数（プロシージャ）リターン状態情報をプッシュ／ポップすることにそれぞれ特化したバリエーションを含め、処理回路によってサポートされる命令セットアーキテクチャにおいてサポートされ得る。

20

【0041】

この場合も、リターン状態ポップ命令は、専用GCS固有命令であってもよいし、別の動作も実行する別のタイプの命令を再利用したバリエーションであってもよい。例えば、リターン状態ポップ命令は、例外リターンを実行するように処理回路を制御することもできる。例えば、GCSモードがディセーブルにされているときに実行される場合、例外リターン命令は、レジスタ内で定義された意図した例外リターン状態情報に基づいて例外リターンを実行するように処理回路を制御し得る（ただし、GCSデータ構造からの保護リターン状態情報のポップ及び保護リターン状態情報に対する意図した例外リターン状態情報の検証は行わない）。例外リターン命令がGCSモードで実行される場合、例外リターン命令は、例外リターンと、GCSデータ構造からの保護リターン状態情報のポップ及び保護リターン状態情報に対する意図した例外リターン状態情報の検証との両方を実行するように処理回路を制御し得る。

30

40

【0042】

装置は、ガード制御スタックデータ構造のアドレスを示すスタックポインタを記憶するための少なくとも1つのGCSポインタレジスタを有してもよい。GCSアクセスタイプの命令は、GCSポインタレジスタに記憶されたスタックポインタを参照して、それらのターゲット仮想アドレスを決定し得る。いくつかの例では、1つ以上のGCSポインタレジスタが存在してもよく、各GCSポインタレジスタは、処理回路のそれぞれの実行状態で使用されるスタックポインタを示す。

【0043】

情報が特定の変換テーブルエントリ（ステージ1又はステージ2変換テーブルエントリ

50

のいずれであっても）によって指定されている場合、その情報は、変換テーブルエントリの符号化において直接指定されるか、変換テーブルエントリによって参照されるレジスタ内に記憶された情報を参照して間接的に指定されるかのいずれかである。例えば、間接参照の場合、特定の許可タイプを示すためにソフトウェアによって設定することができる多数のフィールドを含む許可間接レジスタが提供されてもよく、変換テーブルエントリは、許可間接レジスタのどのフィールドが対応するメモリ領域に適用される許可を指定するかを示すフィールド選択情報を指定してもよい。この間接的な許可アプローチは、上述のようにステージ2で提供される読取り専用又は部分読取り専用許可、及び／又はステージ1でのGCS領域としての特定のメモリ領域の定義、及び／又はターゲットメモリ領域に対するアンチエイリアシング特性の定義を含む、多数の異なる許可タイプに使用することができる。例えば、ターゲットメモリ領域がGCS領域であるかどうかを指定するステージ1許可情報は、ターゲットステージ1変換テーブルエントリによって参照される許可間接レジスタのフィールド内で指定され得る。同様に、ステージ2許可情報（ターゲットメモリ領域が読取り専用であるか部分読取り専用であるかを指定する）も、ターゲットステージ2変換テーブルエントリによって参照される許可間接レジスタのフィールド内で指定することができる。許可間接レジスタを使用する間接許可は、多くの理由で有用であり得る。例えば、間接許可指定は、ソフトウェアが、2つ以上の異なるメモリ領域（全てが許可間接レジスタの同じフィールドを参照する）に適用される許可タイプを、それらのメモリ領域に対応する各別個の変換テーブルエントリを更新する必要なく、レジスタへの単一の書込みを使用して更新することを可能にする。また、いくつかの変換テーブルエントリフォーマットでは、符号化されることが望まれる全ての可能な許可タイプを符号化するのに不十分な符号化空間があるかもしれないため、許可間接の使用は、エントリ符号化自体の中の限られた数のビットが、エントリ自体の中で可能であるよりも広い範囲の許可から選択することができる許可間接レジスタのより大きなフィールドを参照することを可能にすることができる。それにもかかわらず、他のアプローチは、変換テーブルエントリの符号化の中で関連する許可を直接指定し得る。したがって、本出願が、情報が変換テーブルエントリ「によって指定されている」ことを示す場合、この情報は、変換テーブルエントリの符号化において直接指定されるか、又は許可間接レジスタ（又は、情報の直接的及び間接的な指定の両方の混合）を介して間接的に指定されるかいずれかの可能性があることが理解されよう。

10

20

30

【0044】

また、いくつかの実装形態では、変換テーブルエントリの特定のビット、又は変換テーブルエントリによって直接的又は間接的に指定された許可情報は、装置の制御レジスタ内で指定された制御状態に応じて異なる方法で解釈され得る。例えば、制御レジスタに記憶された制御パラメータは、許可情報の特定のビット（又はビットフィールド）を第1の方法で解釈するか第2の方法で解釈するかを制御することができる。これは、レガシーソフトウェアがレガシー符号化スキームに従って動作し、より新しいソフトウェアが異なる符号化スキームに従って同じビットを解釈できるようにするのに役立つ。したがって、許可情報が何らかの情報を指定する（又はその情報を識別する符号化を有する）と記載されている場合、場合によっては、その許可情報がその情報を指定すると見なされるかどうかは、少なくとも1つの制御レジスタに記憶された少なくとも1つの制御パラメータの現在の設定に依存し得るので、許可情報は装置の全の動作モードにおいてその情報を指定する必要はない。

40

【0045】

上述の技法は、上述の処理回路及びメモリ管理回路を実装するために設けられたハードウェア回路を有するデータ処理装置内で実装されてもよい。

【0046】

しかしながら、同じ技法はまた、ホストデータ処理装置上で実行されてターゲットコードの実行のための命令実行環境を提供するコンピュータプログラムで実装されてもよい。そのようなコンピュータプログラムは、ホストデータ処理装置自体がそのアーキテクチャ

50

をサポートしていなくても、特定の命令セットアーキテクチャに従ってターゲットコードを実際にサポートするハードウェア装置上に提供されるアーキテクチャ環境をシミュレートするようにホストデータ処理装置を制御することができる。コンピュータプログラムは、上述のように、GCS領域に対するサポート、変換ハードニング機構、アンチエイリアシング特性、及びアンチエイリアシング特性がターゲットメモリ領域に対して指定されているかどうかの（GCSメモリアクセス要求に対する）監視を含む、上述の処理回路及びメモリ管理回路の機能をエミュレートする処理プログラムロジック及びメモリ管理プログラムロジックを有してもよい。そのようなシミュレーションプログラムは、例えば、ある命令セットアーキテクチャに対して書き込まれたレガシーコードが、異なる命令セットアーキテクチャをサポートするホストプロセッサ上で実行されている場合に有用であり得る。また、シミュレーション実行環境上でソフトウェアを実行することにより、新しいアーキテクチャをサポートするハードウェアデバイスの進行中の開発と並行してソフトウェアのテストを可能にすることができるため、シミュレーションは、新しいアーキテクチャバージョンをサポートするハードウェアを処理する前に、命令セットアーキテクチャの新しいバージョンのソフトウェア開発を開始することを可能にすることができる。シミュレーションプログラムは記憶媒体に記憶されてもよく、この記憶媒体は、非一時的記憶媒体であってもよい。

10

【0047】

データ処理装置の具体例

図1は、データ処理装置2の例を概略的に示す。データ処理装置は、いくつかのパイプラインステージを含む処理パイプライン4を有する。この例では、パイプラインステージは、命令キャッシュ8から命令をフェッチするためのフェッチステージ6と、パイプラインの残りのステージによって処理されるマイクロオペレーション（復号命令）を生成するために、フェッチされたプログラム命令を復号するための復号ステージ10と、マイクロオペレーションに必要なオペランドがレジスタファイル14内で利用可能であるかどうかをチェックし、所与のマイクロオペレーションに必要なオペランドが利用可能になると、実行するためのマイクロオペレーションを発行する発行ステージ12と、結果値を生成するためにレジスタファイル14から読取られたオペランドを処理することによって、マイクロオペレーションに対応するデータ処理動作を実行するための実行ステージ16と、処理の結果をレジスタファイル14に書き戻すための書き戻しステージ18と、を含む。これは、可能なパイプラインアーキテクチャの単なる一例にすぎず、他のシステムは追加のステージ又は異なる構成のステージを有してもよいことが理解されるであろう。例えば、アウトオブオーダープロセッサでは、プログラム命令又はマイクロオペレーションによって指定されたアーキテクチャレジスタを、レジスタファイル14内の物理レジスタを識別する物理レジスタ指定子にマッピングするためのレジスタリネームステージが含まれ得る。いくつかの例では、復号ステージ10によって復号されるプログラム命令と、実行ステージによって処理される対応するマイクロ演算との間に1対1の関係が存在し得る。また、プログラム命令とマイクロオペレーションとの間に1対多又は多対1の関係があってもよく、例えば、単一のプログラム命令を2つ以上のマイクロオペレーションに分割してもよいし、2つ以上のプログラム命令を融合して単一のマイクロオペレーションとして処理してもよい。

20

30

40

【0048】

実行ステージ16は、異なるクラスの処理動作を実行するためのいくつかの処理ユニットを含む。例えば、実行ユニットは、レジスタ14から読取られたスカラオペランドに対して算術演算又は論理演算を実施するためのスカラ算術／論理ユニット（arithmetic/logic unit、ALU）20と、浮動小数点値に対して演算を実施するための浮動小数点ユニット22と、分岐動作の結果を評価し、それに応じて現在の実行点を表すプログラムカウンタを調節するための分岐ユニット24と、メモリシステム8、30、32、34内のデータにアクセスするロード／記憶動作を実施するためのロード／ストアユニット26と、を含み得る。データアクセス命令のオペランドに基づいてロード／記憶ユニット26に

50

よって指定される仮想アドレスと、メモリシステム内のデータのストレージロケーションを識別する物理アドレスとの間のアドレス変換を実行するための、メモリ管理回路の一例である、メモリ管理ユニット (memory management unit、MMU) 28 が提供される。MMU は、メモリシステムに記憶されたページテーブルからのアドレス変換データをキャッシュするための変換ルックアサイドバッファ (translation lookaside buffer、TLB) 29 を有し、ページテーブルのページテーブルエントリはアドレス変換マッピングを定義し、また、例えば、パイプライン上で実行している所与のプロセスが所与のメモリ領域から命令を読取り、書込み、又は実行することを可能にするかどうかを支配するアクセスパーミッションを指定し得る。

【0049】

この例では、メモリシステムは、レベル1データキャッシュ30と、レベル1命令キャッシュ8と、共有のレベル2キャッシュ32と、メインシステムメモリ34と、を含む。これは可能なメモリ階層の一例にすぎず、キャッシュの他の配置を提供することができることが理解されるであろう。実行ステージ16に示される特定のタイプの処理ユニット20～26は単なる一例であり、他の実装形態は、処理ユニットの異なるセットを有してもよく、あるいは、同じタイプの複数のマイクロオペレーションを並行して処理できるように同じタイプの処理ユニットの複数のインスタンスを含んでもよい。図1は、可能なプロセッサパイプライン実装形態のいくつかのコンポーネントの簡素化された表現にすぎず、プロセッサは、簡潔にするために図示していない多くの他の要素を含むことができることが理解されるであろう。図1は、メモリ34へのアクセスを有する単一のプロセッサコアを示しているが、装置2は、各コアがそれぞれのキャッシュ8、30、32を有する、メモリ34へのアクセスを共有する1つ以上の更なるプロセッサコアを有することもできる。

【0050】

図2は、命令を実行するときに処理回路4が動作することができる異なる実行状態（例外レベルとも呼ばれる）を示す図である。この例では、4つの例外レベルEL0、EL1、EL2、EL3が存在し、例外レベルEL0は最低特権例外レベルであり、例外レベルEL3は最高特権例外レベルである。一般に、より特権のある例外レベルで実行するときに、処理回路は、より低い特権の低い例外レベルにアクセスできないいくつかのメモリロケーション又はレジスタ14にアクセスすることができる。

【0051】

この例では、例外レベルEL0は、例外レベルEL1で実行される対応するオペレーティングシステム又は仮想マシンによって管理されるアプリケーションを実行するためのものである。複数の仮想マシンが同じ物理プラットフォーム上に共存する場合、それぞれの仮想マシンを管理するために、EL2で動作するハイパーバイザが提供され得る。図2は、ハイパーバイザが仮想マシンを管理し、仮想マシンがアプリケーションを管理する例を示すが、ハイパーバイザがEL0においてアプリケーションを直接管理することも可能である。

【0052】

必須ではないが、いくつかの実装形態は、処理回路のための別個のハードウェア区分されたセキュアな動作ドメイン及び非セキュアな動作ドメインを実装し得る。データ処理システム2は、セキュアドメインで動作するソフトウェアプロセスに関連付けられたデータ及びコードが、非セキュアドメインで動作するプロセスによるアクセスから隔離されることを保証するために、プロセッサ及びメモリシステム内に実装されたハードウェア機能を有してもよい。例えば、英国ケンブリッジのArm（登録商標）Limitedによって提供されるTrustZone（登録商標）アーキテクチャなどのハードウェアアーキテクチャを使用することができる。代替的に、他のハードウェア実施セキュリティ分割アーキテクチャを使用することもできる。セキュアアプリケーション（信頼できるサービス）は、セキュアドメイン内の例外レベルEL0で動作することができ、セキュア（信頼できる）オペレーティングシステム又は仮想マシンは、セキュアドメイン内の例外レベルEL

10

20

30

40

50

1で動作することができる。いくつかの実装形態では、セキュア状態においてEL2に対するサポートはなく、ハイパーバイザは、非セキュアEL2においてのみ実行することができる。他の実装形態では、図2のアスタリスクによって示されるように、セキュアEL2において実行されるセキュアハイパーバイザに対するサポートが存在し得る。いくつかの例では、非セキュアドメインとセキュアドメインとの間の遷移を管理するためのセキュアモニタプログラムが、例外レベルEL3において実行して提供され得る。他の実装形態は、セキュアモニタプログラムが必要とされない場合があるように、ハードウェア内のセキュリティドメイン間の遷移を監視することができる。

【0053】

アドレス変換

MMU 28によって実行される1つのタスクは、仮想アドレス(virtual address、VA)と物理アドレス(physical address、PA)との間のアドレス変換である。処理回路4上で実行されるソフトウェアは、仮想アドレスを使用してメモリロケーションを指定するが、これらの仮想アドレスは、MMU 28によって、アクセスすべきメモリシステムロケーションを識別する物理アドレスに変換され得る。仮想アドレスを使用する利点は、オペレーティングシステム(Operating System、OS)などの管理ソフトウェアが、ソフトウェアに提示されるメモリのビューを制御することを可能にすることである。OSは、どのメモリが可視であるか、そのメモリが可視である仮想アドレス、及びそのメモリにどのアクセスが許可されるかを制御することができる。これは、OSがアプリケーションをサンドボックス化し(1つのアプリケーションのリソースを別のアプリケーションから隠す)、基礎となるハードウェアからの抽象化を提供することを可能にする。仮想アドレスを使用する別の利点は、OSが、メモリの複数の断片化された物理領域を単一の連続仮想アドレス空間としてアプリケーションに提示することができることである。仮想アドレスは、アプリケーションを書くときにシステムの正確なメモリアドレスを知らないソフトウェア開発者にも利益をもたらす。仮想アドレスを用いると、ソフトウェア開発者は、物理メモリに関心を持つ必要がない。アプリケーションは、アドレス変換を実行するために協働するのがOS及びハードウェア次第であることを知っている。

【0054】

実際には、各アプリケーションは、物理システム内の異なるロケーションにマッピングされる、それ自体の仮想アドレスのセットを使用することができる。オペレーティングシステムは、異なるアプリケーション間で切り替えると、マップを再プログラムする。これは、現在のアプリケーションの仮想アドレスがメモリ内の正しい物理ロケーションにマッピングされることを意味する。

【0055】

仮想アドレスはマッピングを介して物理アドレスに変換される。仮想アドレスと物理アドレスとの間のマッピングは、変換テーブル(ページテーブルと呼ばれることもある)に記憶される。変換テーブルはメモリに格納され、ソフトウェア、典型的にはOS又はハイパーバイザによって管理される。変換テーブルは静的ではなく、ソフトウェア変更の必要に応じてテーブルを更新することができる。これは、仮想アドレスと物理アドレスとの間のマッピングを変更する。

【0056】

処理回路4が実行状態の特定のサブセットにあるとき(特に、処理回路4が非セキュアEL0又は非セキュアEL1にあるとき)に実行されるメモリアクセスについては、図3に示されるように2ステージアドレス変換が使用される(他の実行状態については、ステージ1ページテーブルを使用する1つのステージのアドレス変換で十分である)。したがって、非セキュアEL0及び非セキュアEL1からの仮想アドレスは、二組のテーブルを使用して変換される。これらのテーブルは、仮想化をサポートし、ハイパーバイザが、所与の仮想マシン(virtual machine、VM)(ゲストオペレーティングシステム及びそのゲストオペレーティングシステムによって制御されるアプリケーションに対応する仮想マシン)によって見られる物理メモリのビューを仮想化することを可能にする。OSによ

10

20

30

40

50

って制御される変換のセットをステージ 1 と呼ぶ。ステージ 1 テーブルは、仮想アドレスを中間物理アドレス（IPA－前述の中間アドレスの一例）に変換する。ステージ 1 において、OS は、IPA が物理アドレス空間であると考え。しかしながら、ハイパーバイザは、ステージ 2 と呼ばれる変換の第 2 のセットを制御する。この第 2 の変換セットは、IPA を物理アドレスに変換する。

【0057】

ステージ 1 変換テーブル及びステージ 2 変換テーブルは、ステージ 1 及びステージ 2 についてそれぞれ図 4 及び図 5 に示されるような変換テーブルのいくつかのレベルを含む階層テーブル構造として実装される。この例では、ステージ 1 テーブル及びステージ 2 テーブルの両方が、最大 4 レベルのページテーブル、すなわち、レベル 0（level 0、L 0）、レベル 1（level 1、L 1）、レベル 2（level 2、L 2）、及びレベル 3（level 3、L 3）を有することができる。

【0058】

所与のアドレスに対する物理アドレスマッピングを見つけるために、1 つ以上の変換テーブルルックアップを含む変換テーブルウォークが実行される。変換テーブルウォークは、仮想アドレスを物理アドレスに変換するのに必要なルックアップのセットである。非セキュア EL1 & 0 変換レジームの場合、このセットには、ステージ 1 変換及びステージ 2 変換の両方のルックアップが含まれる（以下に示す図 6 を参照）。ステージ 1 及びステージ 2 ルックアップを使用して成功した変換テーブルウォークによって返される情報は、以下の通りである。

●必要な物理アドレス（中間アドレスへのステージ 1 マッピング及び物理アドレスへのステージ 2 マッピングに基づいて変換される）。

●ターゲットメモリ領域に対するアクセス許可及び／又はメモリ属性で、そのメモリ領域へのアクセスをどのように制御するかに関する情報を提供する。これらは、ステージ 1 テーブル構造において定義されたステージ 1 アクセス許可及び／又は属性と、ステージ 2 テーブル構造において定義されたステージ 2 アクセス許可及び／又は属性とを含み得る。

【0059】

ステージ 1 構造及びステージ 2 構造のうちの所与の 1 つをトラバースするために、ウォークは、変換テーブルベースアドレスレジスタ（ステージ 1 については TTBR、ステージ 2 については VTTBR_EL2）において指定されたアドレスに基づいて、初期ルックアップのためのトップレベル（L 0）変換テーブルの読取りから開始する。各変換テーブルルックアップは、以下のうちの 1 つを示す記述子を返す。

●エントリはステージ 1 又はステージ 2 構造のトラバースの最後のエントリであり、求められているアドレスマッピングを提供する。エントリが最後の L 3 にある場合、このエントリはページ記述子（Page descriptor、D_Page）と呼ばれ、一方、ウォークの最後のエントリを提供するエントリがより高いレベルのうちの 1 つにある場合、ブロック記述子（Block descriptor、D_Block）と呼ばれる。トラバースの最終エントリは、出力アドレス（OA、すなわちステージ 1 の IPA 又はステージ 2 の PA）と、アクセスの許可及び属性とを含む。ブロック記述子が変換テーブル構造のより高いレベルで見つかる場合、これは、ブロック記述子が、L 3 における単一エントリによって表される 4 k B メモリページよりも大きいサイズのメモリ領域を表すことを意味する（L 1 及び L 2 におけるブロック記述子によって表される特定のサイズは、L 1 又は L 2 テーブルにインデックスを付けるために使用されるインデックスビットの数に依存し、この例では、L 1 及び L 2 ブロック記述子は、それぞれ 1 G B 及び 2 M B 領域を表す）。

●追加のレベルのルックアップが必要とされる。この場合、エントリは、テーブル記述子（Table descriptor、D_Table）と呼ばれるが、これは、更なるレベルのテーブルにおけるそのルックアップのための変換テーブルベースアドレスを提供するためである。テーブル記述子は、任意選択で、最終変換に適用することができる他の階層属性を提供することもできる。レベル 1 及びレベル 2 での変換テーブルエントリの符号化は、ブロック記述子をテーブル記述子から区別する。

●記述子は無効である。この場合、メモリアクセスは、変換失敗を生成する。

【0060】

図4は、テーブルルックアップのための入力アドレスとして提供される仮想アドレスのそれぞれのビットを使用したステージ1変換テーブルのインデックス付けを示す。トップレベルテーブルL0のベースアドレスはTTBRから読取られ、L1、L2、L3テーブルのベースアドレスは、それぞれL0、L1、L2テーブル内のインデックス付きテーブル記述子に格納されたアドレスによって示される（L1テーブル又はL2テーブル内でブロック記述子が識別されない場合、L1又はL2のインデックス付きエントリ内でブロック記述子が見つかった場合、出力アドレスマッピングがすでに見つかっているので、そのレベルでトラバーサルが停止される）。ステージ1変換テーブルの所与のレベル内で選択すべき特定のエントリは、ルックアップのための入力アドレスとして提供される仮想アドレスのビットのあるサブセットに対応するインデックス値a、b、c、dに基づいて決定される。図4は、1つの特定の例において、各インデックス値a、b、c、dに対して入力アドレスのどのビットが使用されるかを示す。所与のテーブル内の関連エントリのアドレスは、インデックスビットa、b、c、又はdの倍数を、TTBRに基づいて決定されるその所与のテーブルのベースアドレス、又は前のレベルのテーブル記述子内で指定されたアドレスに加算することによって得られる（乗数は、1つの変換テーブルエントリのサイズに対応するインデックス値に適用される）。

10

【0061】

同様に、図5は、ステージ2テーブルルックアップのための入力アドレスとして提供される中間アドレスのそれぞれのビットを使用したステージ2変換テーブルのインデックス付けを示す。インデックス付けは、ステージ1について図4に示されるものと同様であるが、L0テーブルのベースアドレスを提供するために異なるベースアドレスレジスタVTTBR__EL2を使用する。図5の例に示されるように、ステージ2ルックアップの場合、ルックアップがL0又はL1のいずれかから開始すべきであることを指定することができる制御レジスタVTCR__EL2。SL0に記憶された値に基づいて、ステージ2変換テーブルのウォークが開始する開始レベルを変更することが可能である。ステージ2ルックアップがL0から開始する場合、レベル0、1、2、3に対するインデックス付けは、ステージ1に対する図4と同様に、それぞれインデックス値a、b1、c、dを使用する。ステージ2ルックアップがL1から開始する場合、インデックス付けは同様の方法で実行されるが、ここでは、図5に示されるように、ルックアップのトップレベル（L1）でより多くのインデックスビットb2が使用される。可変開始レベルを提供することは本質的な特徴ではなく、所望であれば省略することができる。図4には示されていないが、ステージ1でのルックアップのための可変開始レベルを提供することも可能である。

20

30

【0062】

図6に示すように、実際には、ステージ1変換及びステージ2変換の両方を含む完全な変換テーブルウォークが実行されるとき、TTBRから取得された各ステージ1テーブルベースアドレス、及びステージ1 L0、L1、L2変換テーブルにおいてアクセスされたテーブル記述子は、それ自体がステージ2変換テーブルを使用して変換する必要がある中間アドレスになる。したがって、変換テーブルウォークがブロック記述子に遭遇せず、ページ記述子が見つかるL3までずっと進む場合、完全なページテーブルウォークプロセスは、以下のシーケンスで複数レベルのページテーブルにアクセスすることを含むことができる。

40

●ステージ1 L0ページテーブルのベースアドレスの、物理アドレスへのステージ2変換（ステージ1変換はオペレーティングシステムによって構成されるため、ステージ1 L0ベースアドレスは通常、中間物理アドレスである）。ステージ2変換は、4回のルックアップ（ステージ2 L0；ステージ2 L1；ステージ2 L2；ステージ2 L3）である。

●ステージ1 L1ベースアドレス（中間物理アドレス）を取得するための、ターゲット仮想アドレスのL0インデックス部分「a」及び変換されたステージ1 L0ベースア

50

ドレスに基づいて取得されたアドレスにおけるエントリのステージ1 L0 ルックアップ。

●ステージ1 L1 ベースアドレスの、物理アドレスへのステージ2 変換（ここでも4回のルックアップを含む）。

●ステージ1 L2 ベースアドレス（中間物理アドレス）を取得するための、ターゲット仮想アドレスのL1 インデックス部分「b」及び変換されたステージ1 L1 ベースアドレスに基づいて取得されたアドレスにおけるエントリのステージ1 L1 ルックアップ。

●ステージ1 L2 ベースアドレスの、物理アドレスへのステージ2 変換（ここでも4回のルックアップを含む）。

●ステージ1 L3 ベースアドレス（中間物理アドレス）を取得するための、ターゲット仮想アドレスのL2 インデックス部分「c」及び変換されたステージ1 L2 ベースアドレスに基づいて取得されたアドレスにおけるエントリのステージ1 L2 ルックアップ。

●ステージ1 L3 ベースアドレスの、物理アドレスへのステージ2 変換（ここでも4回のルックアップを含む）。

●ターゲット仮想アドレスに対応するターゲット中間物理アドレスを識別するための、ターゲット仮想アドレスのL3 インデックス部分「d」及び変換されたステージ1 L3 ベースアドレスに基づいて取得されたアドレスにおけるエントリのステージ1 L3 ルックアップ。

●元のターゲット仮想アドレスに対応してアクセスするためにメモリ内のロケーションを表す、ターゲット中間物理アドレスの、ターゲット物理アドレスへのステージ2 変換（ここでも4回のルックアップを含む）。

【0063】

したがって、キャッシングがなく、ステージ2 開始レベルがL0 であると仮定すると、変換は合計24回のルックアップを含むことになる。ステージ2 のための開始レベルがL1 である場合、これは、ルックアップの数を19に低減することができる（実行される5つのステージ2 変換の各々について1回少ないルックアップ）。それにもかかわらず、上記のシーケンスから分かるように、ページテーブルウォークプロセス全体の実行は、アドレス変換のステージの各々のページテーブルのレベルの各々をステップスルーするための、メモリへの多数のアクセスを必要とする可能性があるため、非常に遅くなり得る。これが、変換テーブルウォークから導出された情報をMMU 28のTLB 29にキャッシュすることがしばしば望ましい理由である。キャッシュされた情報は、VAからIPAへの最終ステージ1 アドレスマッピング、IPAからPAへの最終ステージ2 マッピング、又は直接VAからPAへのステージ1 及びステージ2 の組み合わされたマッピング（ステージ1 構造及びステージ2 構造の以前のルックアップから導出される）を含むことができるだけでなく、ステージ1 テーブル及びステージ2 テーブルの上位レベルのページテーブルからのエントリも、MMU 28のTLB 29内にキャッシュすることができる。これにより、所与のターゲットアドレスの最終レベルのアドレスマッピングが現在アドレス変換キャッシュ内にない場合でも、フルページテーブルウォークの少なくともいくつかのステップをバイパスすることができる。

【0064】

図6は、2ステージアドレス変換に含まれる変換テーブルエントリのいくつかについて定義することができる特定の許可又は特性を指定する情報で注釈を付けられている。これらの許可及び特性が以下で説明されるが、後でより詳細に説明されるであろう。

【0065】

メモリ管理ユニットの例

図7は、メモリ管理ユニット28をより詳細に示す。図1及び図7は、簡潔にするために単一のMMU 28を示しているが、フェッチステージ6によって開始される命令フェッチアクセス及びロード／記憶ユニット26によって開始されるデータアクセスのためのメモリ管理動作をそれぞれ処理するために、別個の命令側MMU及びデータ側MMUを設けることも可能であり、この場合、命令側MMU及びデータ側MMUの両方が、図7に示す構成要素を有することができる。TLB 29と同様に、MMU 28は、ルックアップ

ブされた変換テーブルエントリにおいて指定されたアクセス許可をチェックし、それらのアクセス許可に従ってメモリアクセス要求の処理を制御するためのアクセス制御回路50を含む。例えば、アクセス制御回路50は、特定のタイプのメモリアクセス要求（例えば、要求が読取り要求、書込み要求、又は命令フェッチ要求であるかどうかに基づいて、又は要求を発行させた実行された命令のタイプに基づいて）が、アクセスされているメモリの所与の領域に対する対応変換テーブルエントリにおいて指定された許可を満たすかどうかを決定するためのチェックを実装することができる。MMUはまた、変換テーブルウォーク制御回路52を含み、変換テーブルウォーク制御回路52は、変換テーブルからの必要な情報がTLB 29内ですでに利用可能でない場合に、メモリアクセス要求をメモリに発行して、図4～図6に上で示した変換テーブルウォークプロセス中に変換テーブルエントリの読取りを要求する。変換テーブルウォーク制御回路52は、ステージ1又はステージ2変換テーブル構造内の関連する変換テーブルエントリを取得するために読取られるメモリシステムロケーションのアドレスを生成する役割を果たすことができる。更に、変換テーブルウォークを実行している間、変換テーブルウォーク制御回路52は、変換テーブルウォークにおいてトラバースされている特定の変換テーブルエントリ内の追跡メタデータにアクセスするための更新を要求するメタデータ更新書込み要求を生成することができる。これらのメタデータ更新書込み要求は、特定のメモリ領域がアクセスされたことを反映するようにアクセス追跡メタデータを更新することができ、これは、ページングなどの動作を管理するのに有用であり得る。メタデータ更新書込み要求のアドレスは、アクセスされているデータ又は命令のアドレスではなく、変換テーブルウォークにおいてアクセスされる変換テーブルエントリのアドレスであるので、メタデータ更新書込み要求は、命令フェッチアドレスとして直接指定されないアドレス、又は処理回路4によって実行されるロード／記憶命令のオペランドから導出されるロード／記憶ターゲットアドレスを指定するために、ハードウェアにおいて生成される。

10

20

30

40

50

【0066】

MMU 28は、変換テーブルウォーク及びメモリ管理動作の他の態様を制御するための様々な制御レジスタへのアクセスを有する。例えば、制御レジスタは、図4及び図5に関して前述したように、ステージ1ベースアドレスレジスタTTBR__EL1及びステージ2ベースアドレスレジスタVTBR__EL2を含んでもよい。レジスタTTBR__EL1のステージ1ベースアドレスは、例外レベルEL1、EL2、又はEL3で（すなわち、第1の実行状態又は第1の実行状態よりも大きな特権を有する実行状態で）実行される命令に応答して書込み可能である。レジスタTTBR__EL2のステージ2ベースアドレスは、例外レベルEL2又はEL3で（すなわち、第2の実行状態又は第2の実行状態よりも大きな特権を有する実行状態で）実行される命令に応答して書込み可能である。場合によっては、EL1で実行される命令によってトリガされるTTBR__EL1への書込みがEL2にトラップされるべきであることを示すように制御値を設定して、EL2で動作するハイパーバイザが、オペレーティングシステムによって要求されている更新をチェックし、必要であれば更新を防止することができるようにすることが可能である。制御レジスタはまた、レジスタTCR__EL1、VTBR__EL2を含み、これらは、ステージ1及びステージ2変換及びアクセス許可チェックが実行される方法に影響を及ぼす様々な制御ステータス値を指定するために使用される。例えば、ステージ2ウォークのための開始レベルを指定する制御値は、VTBR__EL2において指定され得る。また、TCR__EL1又はVTBR__EL2制御レジスタは、どのタイプのセキュリティチェックがイネーブル／ディセーブルにされるかを指定する制御値を指定することができる。以下でより詳細に説明するように、制御レジスタはまた、有効エントリ及び無効エントリそれぞれについて、保護ステージ1変換テーブルエントリにおいて更新が制限される、更新制限されたビットのサブセットを指定するためのマスクレジスタ(RCWMask__Valid__EL2及びRCWMask__Invalid__EL2とラベル付けされている)を含むことができる。更なる制御レジスタを設けることもでき、制御レジスタに使用されるラベルを変更することができることが理解されよう。例えば、所与の変換テーブルエントリに対

するアクセス許可情報を指定するために所与の変換テーブルエントリによって参照することができる間接アクセス許可情報を指定するために、1つ以上の許可間接レジスタを設けることができる。また、同じ情報を異なるフォーマットで制御レジスタ内に配置することも可能であり、したがって、1つの制御レジスタ又は別の制御レジスタへの情報の特定の割り当ては、本質的な特徴ではない。

【0067】

図7に示すように、装置は、保護エントリとして符号化されたステージ1変換テーブルエントリに対して更新が要求されたときに保護エントリチェックを実行するための保護エントリチェック回路54を有することができる（これについては以下でより詳細に説明する）。図7の点線で示すように、処理システム内の異なるロケーションに保護エントリチェック回路54を実装することが可能である。例えば、保護エントリチェック回路54は、MMU 28のアクセス制御回路50の一部であってもよい。代替的に、保護エントリチェック回路は、保護エントリチェック回路54を使用してチェックされるべき所与のメモリアクセス要求によってアクセスされている物理メモリシステムロケーションにより近いメモリシステム構成要素56内に実装され得る。例えば、メモリシステム構成要素56は、キャッシュ30、32、複数のプロセッサコアによる共有メモリへのアクセスを管理するために使用される相互接続、又は特定のメモリストレージユニットに関連付けられたメモリコントローラであり得る。また、保護エントリチェック回路54は、システム内の複数のロケーション（例えば、MMU 28、ロード／記憶ユニット26、及び／又はメモリシステム構成要素56）に分散ロジックを含むことができる。

【0068】

変換テーブルアクセス許可及び属性

図8は、ステージ1変換テーブル構造及びステージ2変換テーブル構造における変換テーブルエントリの例示的なフォーマットを示す。同じ情報を異なる配置で表すことができ、したがって、記述子内のフィールドの特定の順序付け及びレイアウトは、図8に示されているものとは異なる可能性があることが理解されよう。

【0069】

この例では、有効な変換テーブル記述子は、1に設定された最下位ビットを有し、無効な変換テーブル記述子は、0に設定された最下位ビットを有する。変換テーブル構造のレベル0、1、2のうちの1つで読取られた有効な記述子について、第2の最下位ビットは、記述子がテーブル記述子（第2の最下位ビットが1に設定される）であるか、又はブロック記述子（第2の最下位ビットが0に設定される）であるかを区別する。ステージ1構造又はステージ2構造のL3におけるページ記述子は、ページ記述子がブロック記述子から区別されることを可能にするために、1に設定された第2の最下位ビットを有し得る。もちろん、有効／無効エントリ、及びテーブル／ブロック／ページ記述子は、他の符号化方法によって区別することもできる。

【0070】

ステージ1エントリ及びステージ2エントリの両方に対して、有効なテーブル記述子は、ステージ1変換テーブル構造又はステージ2変換テーブル構造の次のレベルにおける変換テーブルのベースアドレスを示すネクストレベルテーブルアドレス60を提供する。有効なステージ1ブロック又はページ記述子は、ステージ1変換テーブル構造をインデックスするために使用される仮想アドレスに対応する中間アドレスマッピング62を提供する。有効なステージ2ブロック又はページ記述子は、ステージ2変換テーブル構造をインデックスするために使用される中間アドレスに対応する物理アドレスマッピング64を提供する。

【0071】

ステージ1ブロック及びページ記述子はまた、対応メモリ領域へのアクセスを制御するために使用されるステージ1アクセス許可66を提供する。例えば、ステージ1アクセス許可66（通常、EL1においてOSによって設定される）は、領域が実行可能命令の命令フェッチのために読取り、書込み、及び／又は使用されることを許可されるかどうかを

指定することができる。

【0072】

同様に、ステージ2ブロック及びページ記述子は、対応メモリ領域へのアクセスを制御するために使用されるステージ2アクセス許可68を提供する。この場合も、ステージ2アクセス許可68（通常、EL2においてハイパーバイザによって設定される）は、領域が実行可能命令の命令フェッチのために読取り、書込み、及び／又は使用されることを許可されるかどうかを指定することができる。ステージ1アクセス許可66とステージ2アクセス許可68との間に競合が存在する場合、より制限的な属性のセットが優先され得る。

【0073】

ステージ1ブロック／ページ記述子又はステージ2ブロック／ページ記述子は、図8に示されていないメモリ領域に関連付けられた他の属性を指定することもできる。例えば、これらの属性は、対応メモリ領域からのデータをキャッシュすることが許可されるかどうか、デバイスメモリへの異なるメモリアccessの並べ替え又はマージが許可されないように領域がデバイスメモリとして定義されるかどうかなどの特性を指定することができる。

【0074】

ステージ1ブロック／ページ記述子はまた、所与のメモリ領域へのアクセス頻度を追跡するためにオペレーティングシステムによって使用され得るアクセス追跡メタデータを指定することができる。例えば、メタデータは、アクセスフラグ（access flag、AF）70及びダーティビット修飾子（dirty bit modifier、DBM）72を含んでもよい。

【0075】

周期的に、オペレーティングシステムは、監視されるメモリ領域のセットに対応するエントリ内のアクセスフラグをクリアすることができる。読取りアクセスがこれらのメモリ領域のうちの1つに対して行われるとき、アクセスフラグ70は、対応ステージ1ブロック又はページ記述子において設定され得る（以前のアクセスに続いてすでに設定されていない場合）（アクセスフラグ70を設定させるメモリアccess要求は、前述の変換テーブルウォーク制御回路52によって生成されるメタデータ更新書込み要求のうちの1つであり得る）。監視期間の後、オペレーティングシステムは、アクセスフラグ70をチェックして、特定のページがアクセスされる頻度に関する情報から利益を得ることができる動作を支援することができる。例えば、オペレーティングシステムは、メモリ領域が何回アクセスされたかを追跡するメモリ領域ごとのエントリを有する更なる追跡データ構造をメモリ内に維持することができ、したがって、各監視期間の終了時に、アクセスフラグ70セットを有するメモリ領域に対応するその更なる追跡構造のエントリをインクリメントすることができる。したがって、いくつかの監視期間の後、その更なる追跡構造は、対応するメモリ領域へのアクセスの相対頻度の指示を提供する。これは、ページングなどの動作を制御するための有用な情報を提供することができ、対応データが、他のより頻繁にアクセスされるページと比較して外部ストレージにページングアウトするために優先順位付けされ得るメモリの最も頻繁にアクセスされないページを知ることが有用であり得る。

【0076】

同様に、DBM 72は、どのページが書込みを受けたかを追跡することを支援する。オペレーティングシステムが、所与のページが書込まれたかどうかを追跡したい場合、ページがマッピングされるときに、又は監視期間の開始のときに、オペレーティングシステムは、そのページに対するアクセス許可を「読取り専用」として設定し（ページが書込まれることを許可されるように意図されている場合であっても）、DBMビット72を設定することができる。DBMビット72が設定されているときに読取り専用ページへの書込みによってアクセス許可失敗が引き起こされると、オペレーティングシステムは、DBMビット72が設定されていることから、これが読取り専用許可の「真の」違反ではないと決定することができ、その代わりに、オペレーティングシステムに、書込み要求を受けるページを追跡するメモリに記憶されたデータ構造を更新させ、ページに対する書込みアクセス許可を更新させて、失敗をトリガすることなくページに現在書込むことができること

10

20

30

40

50

を示すこともできる。監視期間の後、メモリ内の追跡データ構造をソフトウェアによって使用して、特定の領域をページングアウトする際に、その領域から修正されたデータを外部ストレージに書き戻す必要があるかどうか、又は（書込みが行われていない場合）、外部メモリ内の対応データは、データがクリーンであれば依然として同じであると仮定することができるので、オンチップメモリ内に記憶されたデータを領域をページングアウトする際に単に破棄することができるかどうかを決定することができる。

【0077】

アクセスフラグ70及びダーティビット修正子72は、変換テーブルエントリ内に記憶され得る可能なアクセス追跡データの単なるいくつかの例であり、他の例は、他のタイプのアクセス追跡メタデータを提供し得る。例えば、別の例では、マルチビットアクセスカウンタが、アクセス追跡メタデータとして提供され得る。また、別の例では、書込み要求に対する読取り専用アクセス許可違反の処理を修正し、書込み許可の更新をトリガするためにDBMビット72が使用される代わりに、前述のようにアクセスフラグ70がページへの最初のアクセス時に更新される方法と同様の方法で、DBMフラグ72をクリアした後のページへの最初の書込みに応答して、DBMフラグ72を直接更新することができる。

10

【0078】

図8に示すように、様々な変換テーブル記述子はまた、攻撃者による攻撃下でオペレーティングシステムコードによる破損からステージ1変換テーブルエントリを保護するのに有用であり得るいくつかの他の情報を含むことができる。典型的なオペレーティングシステムコードは、攻撃に対して安全であることを完全に検証することが困難な場合がある多くのコード行を含む場合があり、したがって、攻撃者がオペレーティングシステムコードの挙動を修正して、変換テーブルエントリを記憶するために使用されるメモリ領域への書込みを引き起こすことができ、これらのエントリ内のアドレスマッピング又は許可を修正して、無許可の形でメモリ領域にアクセスする権利を攻撃者に与えることができる可能性から保護するためのアーキテクチャ機構を提供することが望ましい。

20

【0079】

図8に示すように、変換ハードニング機構を提供するために、攻撃に対してステージ1変換テーブルをハードニングするための以下に説明する追加の属性及び許可は、以下を含む。

30

●ステージ2ブロック／ページ記述子は、対応するメモリ領域が部分読取り専用（partially-read-only、PRO）許可を有するかどうかを示す符号化を有するステージ2アクセス許可68を指定する（部分読取り専用許可は、「大部分読取り専用」許可と呼ぶこともできる）。

●ステージ1変換テーブル構造の全てのレベルにおける有効ステージ1記述子（テーブル記述子及びブロック／ページ記述子を含む）は、その変換テーブルエントリが、非保護エントリと比較して無許可の更新に対する追加の保護が提供される「保護」エントリであるかどうかを指定する符号化を有する。例えば、有効なステージ1記述子内のビットフィールド76は、エントリが保護エントリであるか否かを示すことができる。

●ステージ1変換テーブル構造の全てのレベルにおける無効ステージ1記述子はまた、その変換テーブルエントリが「保護」エントリであるかどうかを指定する符号化を有し得る。これは、有効なステージ1変換テーブルエントリのための保護エントリを表すために使用されるビットフィールド76と比較して、変換テーブルエントリ符号化内の異なる位置にあり得るビットフィールド78を使用して示され得る。

40

●ステージ2ブロック／ページ記述子は、対応するメモリ領域がアンチエイリアシング特性を有するかどうかを指定するインジケータ79を有し得る。いくつかの例では、アンチエイリアシング特性の有無は、他のタイプの特性もシグナリングすることができる組み合わせられたビットフィールドにおいて符号化され得るか、又は代替的に、アンチエイリアシングビットフィールドは、他の情報をシグナリングしないスタンドアロンビットフィールドであり得る。指定されている場合、アンチエイリアシング特性は、対応する物理アド

50

レスへのアクセスが許可されるために、そのステージ 2 記述子にアクセスするために使用される中間アドレスを得るために変換テーブルウォークにおいてアクセスされる全てのステージ 1 変換テーブルエントリが、ビットフィールド 7 6 を使用して保護エントリとして指定され、対応するステージ 2 ブロック／ページ記述子が部分読取り専用許可 7 4 を示すメモリの領域に記憶される必要があることを示す。

●ステージ 2 ブロック／ページ記述子はまた、ステージ 2 アクセス許可 6 8 において、対応するメモリ領域がステージ 1 変換のためのトップレベル変換テーブル（すなわち、図 4 及び図 6 の例におけるステージ 1 L 0 テーブル）を保持することを許可されているかどうかを示すステージ 1 トップレベルエントリ存在許可 8 0 を指定し得る。一例では、ステージ 2 アクセス許可 6 8 の符号化は、ステージ 1 トップレベルエントリ存在許可が P R O 許可の更なる属性として符号化されるようなものであってもよく、したがって、ステージ 2 アクセス許可 6 8 のために符号化されることを許される値は、以下を示す値を含んでもよい。

- ステージ 1 トップレベルエントリ存在許可なしの P R O 許可、
- ステージ 1 トップレベルエントリ存在許可を伴う P R O 許可、又は
- P R O 許可又はステージ 1 トップレベルエントリ存在許可のいずれも有さない 1 つ以上の他のタイプの許可（例えば、読取り専用許可、読取り／書込み許可、及び／又は実行許可）である。

【0080】

この場合、ステージ 1 トップレベルエントリの存在許可を P R O 許可とは独立に指定することができない場合がある。しかしながら、他の実装形態は、P R O 許可が提供されない場合であってもステージ 1 トップレベルエントリ存在許可が指定され得るように、ステージ 1 トップレベルエントリ存在許可を P R O 許可とは独立して符号化することができる。

【0081】

これらの属性及び許可の使用については、以下でより詳細に説明する。これらの属性の全てがあらゆる可能性のある実装形態においてサポートされる必要があるわけではないことが理解されるであろう。図 8 は、S 1 及び S 2 アクセス許可が変換テーブルエントリの符号化において直接指定される例を示すが、許可レジスタにおいて指定された許可を使用して同じ情報を間接的に指定することも可能である。例えば、S 1 又は S 2 許可フィールド 6 6、6 8 は、許可レジスタのいくつかの許可フィールドのうちのどれが対応変換テーブルエントリに対するアクセス許可を指定するかを選択するインデックス値を指定することができる。また、変換テーブルエントリのいくつかのフィールドが、制御レジスタに記憶されたコントロール状態に依存した異なる方法で解釈されることも可能である。例えば、ステージ 1 変換テーブルエントリの保護エントリフィールド 7 6 は、制御レジスタに格納された制御値が第 1 の値を有するときにステージ 1 変換テーブルエントリが保護されるかどうかを示すものとして解釈されてもよく、制御値が第 2 の値を有するときに異なる方法で解釈されてもよい。同様に、ステージ 2 変換テーブルエントリのアンチエイリアシング特性フィールド 7 9 は、制御レジスタに記憶された制御値が第 1 の値を有するときに、ステージ 2 変換テーブルエントリがアンチエイリアシング特性を有するかどうかを示すものとして解釈され、制御値が第 2 の値を有するときに、異なる方法で解釈されてもよい。

【0082】

S 1 許可 6 6 及び S 2 許可 6 8 は、対応する S 1 又は S 2 記述子によって直接指定されるものとして示されているが、これらの許可（又は変換テーブルエントリによって指定される他の情報）は、図 1 8 に関して以下に示すように、間接レジスタを使用して間接的に指定されることも可能である。

【0083】

部分読取り専用許可

図 9 は、部分読取り専用（P R O）許可を有するものとしてステージ 2 アクセス許可 6 8 によってマークされたメモリ領域に対する書込みアクセス制御挙動を要約する。P R O

10

20

30

40

50

許可を有するメモリ領域は、少なくとも、現在の実行状態が E L 1（オペレーティングシステムコードが実行されると予想される状態）であるときに発行された書込み要求に対して、書込み要求タイプの制限されたサブセットに対して書込み可能であるが、書込み要求タイプに対して読取り専用として扱われる。いくつかの書込み要求タイプのみがメモリ領域を読取り専用と見なすので、この許可は、したがって、部分読取り専用許可として説明される。

【0084】

図9は、対応ステージ2変換テーブルエントリが領域を P R O 許可を有するものとして定義するメモリ領域への書込みを許可された書込み要求及び禁止された書込み要求のタイプを要約する。書込みが E L 1 で発行されたときに P R O 領域への書込みを許可された書込み要求タイプの制限されたサブセットは、変換テーブルエントリ内のアクセス追跡メタデータを更新するために M M U 28 によって生成されたメタデータ更新書込み要求、例えばアクセスフラグ 70、又は上述のようにダーティビット修正子 72 が設定されている場合の書込み許可を含む。また、制限されたサブセットは、例外状態 E L 1 において実行される少なくとも1つの所定のタイプの変換テーブルエントリ更新命令を含むことができ、この命令は、変換テーブルエントリを更新するためのそのような書込みを、変換テーブルエントリ以外のデータを更新するための書込みから区別するプログラムコードの意図を表現するために、変換テーブルエントリを更新する際に使用するよう意図された専用タイプの命令とすることができる。例えば、所定のタイプの変換テーブルエントリ更新命令は、以下の図12～図14に関して説明される保護エントリチェック読取りチェック書込み（R C W）命令のバリエーションを含むことができる。図9に示されるように、例外状態 E L 0 及び E L 1 のうちの1つにおいて実行される少なくとも1つの他のタイプの記憶命令に応答して発行される書込み要求は、メモリの P R O 領域への書込みを禁止される。例えば、禁止書込み要求タイプは、処理回路4によってサポートされる命令セットアーキテクチャ内の大多数の記憶命令を含み得る。領域が P R O 許可でマークされているときに変換テーブルエントリを更新する能力を命令タイプの限定されたセットに制限することによって、これは、ステージ1変換テーブルエントリを破損しようと試みるときに攻撃者が利用できる攻撃面を低減し、例えば、書込み要求の制限されたサブセットのうちの1つではない汎用記憶のアドレスオペランドを改ざんすると、メモリの P R O 領域へのアクセスが許可されなくなる。

【0085】

任意選択で、実行状態 E L 2 又は実行状態 E L 3 のうちの1つで実行された記憶命令に応答して発行された書込み要求は、実行状態 E L 0 又は実行状態 E L 1 で実行された場合にその領域への書込みが禁止されていた記憶命令のタイプであっても、部分読取り専用領域への書込みが許可され得る。しかしながら、これは前述したように必須ではない。

【0086】

図10は、命令を処理する、及びメモリ管理動作を制御する方法を示すフロー図である。ステップ500において、処理回路4は、異なる特権レベルに関連付けられた複数の実行状態 E L 0 ～ E L 3 のうちの1つにおいて命令を処理する。ステップ502において、メモリアクセス要求に応答して、M M U 28 は、メモリアクセス要求によって指定されたターゲット仮想アドレス（V A）のターゲット物理アドレス（P A）への2ステージアドレス変換を実行し、ターゲット V A のターゲット P A へのマッピングは、ターゲット V A からターゲット中間アドレス（intermediate address、I P A）へのステージ1アドレスマッピング及びターゲット I P A からターゲット P A へのステージ2アドレスマッピングに依存する。ステップ504において、M M U 28 のアクセス制御回路50は、対応ステージ2変換テーブルエントリにおいて指定されたステージ2アクセス許可情報68に少なくとも基づいて、メモリアクセス要求に対する許可チェックを実行する。許可チェックは、ステージ1アクセス許可情報66に基づくこともできる。ステージ2アクセス許可情報66は、ターゲット I P A に対応するメモリ領域が P R O 許可を有するかどうかを指定する符号化を有する。ステップ506において、M M U 28 は、メモリアクセス

要求が所定の実行状態（例えば、E L 1）において発行された書込み要求であり、ステージ2アクセス許可情報がP R O許可を指定し、書込み要求がメモリのP R O領域への書込みを許可された書込み要求タイプの制限されたサブセット以外の書込み要求タイプである場合、メモリアクセス要求を拒絶する。任意選択で、M M U 28はまた、P R O許可がステージ2アクセス許可情報によって指定され、書込み要求タイプが書込み要求タイプの制限されたサブセットのうちの1つでないときに、メモリアクセス要求が所定の実行状態以外の実行状態（例えば、E L 0）で発行された書込み要求であるときに、メモリアクセス要求を拒否することができる。

【0087】

図11は、M M U 28のアクセス制御回路50によって実行される部分読取り専用チェックをより詳細に示す。ステップ600において、処理回路4が所定の実行状態（E L 1）にあるときに、書込みメモリアクセス要求が発行される。書込み要求は、ターゲットV Aを指定する。書込み要求は、処理回路によって実行されるロード／記憶命令に応答して処理回路4のロード／記憶ユニット26によって、又は命令フェッチを要求するときにフェッチステージ6によって発行された可能性がある。書込み要求は、変換テーブルウォークプロセス中に変換テーブルエントリ内のアクセス追跡メタデータを更新するためにM M U 28によって発行されるメタデータ更新書込み要求であってもよい。

【0088】

ステップ602において、ターゲットV Aは、アクセスされるメモリシステムロケーションを識別するターゲットP Aに変換される。変換を実行するために、M M U 28は、T L B 29内のターゲットV Aをルックアップすることができ、ターゲットV AからターゲットP AへのマッピングがT L B 29内ですでに利用可能である場合、変換テーブルウォークは不要である。そうでなければ、図6に示される変換テーブルウォークプロセスの少なくとも一部が必要とされ得るが、変換テーブルウォークのその部分についての対応変換テーブルエントリから導出された情報がすでにT L B 29内にキャッシュされている場合、いくつかの部分スキップすることが可能であり得る。非セキュアE L 1から発行された書込みメモリアクセス要求の場合、変換は、ステージ1変換テーブル及びステージ2変換テーブルの両方で定義されたマッピングに基づいて2ステージアドレス変換として実行されるが、ターゲットI P Aが明示的に決定される必要を回避するために、対応するステージ1許可情報及びステージ2許可情報と共に、ターゲットV AからターゲットP Aへの直接マッピング（ステージ1マッピング及びステージ2マッピングの両方に依存する）をキャッシュする組み合わせされたステージ1／ステージ2 T L Bが提供されることが可能であるので、これは必ずしも2つの別個の変換が実行される必要があることを意味しない。

【0089】

ステップ604において、アクセス制御回路は、対応するステージ2（stage-2、S 2）変換テーブルエントリ（ターゲットI P AからターゲットP Aへのマッピングを指定するステージ2エントリ）がP R O許可を指定するかどうかをチェックする。そうである場合、ステップ606において、アクセス制御回路は、処理されている書込み要求が書込み要求タイプの制限されたサブセットのうちの1つであるかどうかをチェックする。現在の書込み要求が書込み要求タイプの制限されたサブセットのうちの1つでない場合（少なくともメタデータ更新書込み要求を含む）、ステップ608において、メモリアクセス要求は拒否され、失敗が通知される。書込み要求が書込み要求タイプの制限されたサブセットのうちの1つである場合、部分読取り専用チェックにパスし、したがって方法はステップ610に進む。また、ステップ604において、対応ステージ2変換テーブルエントリがP R O許可を指定しなかった場合、ステップ606における部分読取り専用チェックを省略することができ、したがって、方法はステップ604から直接ステップ610に進む。

【0090】

ステップ610において、アクセス制御回路は、書込みメモリアクセス要求が進行する

ことを可能にするために必要とされる任意の他のチェックが満たされるかどうかを決定する。例えば、これらのチェックは、ステージ1アクセス許可66を使用するチェック、PRO許可が指定されていない場合の他のステージ2アクセス許可68を使用するチェック、要求がセキュア状態又は非セキュア状態（セキュア状態をサポートする実装形態において）から発行されたかどうかに基づくセキュリティチェック、並びにターゲットメモリロケーションにおけるデータが保護変換テーブルエントリであるかどうかに関する図12～図14に関して以下で説明するチェックなどの特定の命令タイプに固有の他のチェックを含むことができる。これらの他のチェックのいずれかが満たされない場合、再びステップ608において、メモリアクセス要求は拒絶され、失敗が通知される。失敗シンドローム情報は、失敗の原因を区別するために設定され得る。ステップ610において実行されたチェックが満足される場合、ステップ612において、メモリアクセス要求は続行することを許可され得、したがって、ターゲットPAに関連付けられたメモリシステムロケーションは、書込み要求によって指定された書込みデータで更新され得る。

10

【0091】

したがって、先に説明した図6に示すように、PRO許可は、機密情報を含むメモリ領域の中間アドレスを得るためにステージ1テーブル構造のトラバースにおいて使用される様々なレベルのステージ1変換テーブルを保持するメモリシステムロケーションの物理アドレスを提供するために使用されるステージ2変換テーブルエントリのステージ2アクセス許可68において指定され得る。これは、PRO許可が、対応するメモリ領域に書込む能力を命令タイプの限られたサブセットに制限し、ステージ1変換テーブルの破損に対して脆弱であり得るコードの行の数を大幅に低減するので、悪意のある者による攻撃の下でコード又はオペレーティングシステムコードを誤って機能させることによる破損から、それらのステージ1変換エントリを保護する。それにもかかわらず、変換テーブルエントリ内のアクセス追跡メタデータを更新するためのハードウェア生成書込み要求は、オペレーティングシステムによるページング動作の効率を損なうことを回避するために、そのような領域に対して依然として許可され得る。

20

【0092】

図11は、所定の実行状態EL1にあるときに発行された書込みメモリアクセス要求に対して実行される部分読取り専用チェックを示しているが、他の実行状態に対しても実行することができる。しかしながら、最低特権実行状態EL0において発行された書込み要求に対して、ステージ1変換テーブルを保持するメモリ領域は、いずれの場合もステージ1アクセス許可66によって、EL0において動作するアプリケーションレベルコードにアクセス不可能であるとしてマークされる可能性が高いので、これは必須ではない場合があり、したがって、ステージ1許可チェックは、そのような書込み要求がステージ1変換テーブルを破損することをすでに防止することができる。また、EL2又はEL3で実行されるコードの場合、ハイパーバイザ又はモニタコードが、ステージ1変換テーブルへの更新が許可される制限を制御しているコードである可能性があるので、変換テーブルは、2ステージアドレス変換を使用せず、ステージ1変換テーブルエントリを記憶する領域への書込みを制限する可能性は低い。したがって、いくつかの実装形態は、現在の実行状態がEL1であるときのみ実行されるように部分読取り専用チェックを制限することができる。他の実装形態は、どの実行状態が現在の実行状態であるかにかかわらず、部分読取り専用チェックを適用することができる。

30

40

【0093】

ステージ1変換テーブルエントリのための保護エントリ符号化

書込みタイプの制限されたサブセット以外の書込み要求に対して、あるメモリ領域を読取り専用としてマークするためにPRO許可を使用することは、ステージ1テーブルを破損から保護するのに役立つ。しかしながら、図6に示されるように、典型的には、変換テーブル構造の所与のレベルにおける所与の変換テーブルは、メモリ内のページ全体を占有し、したがって、PRO許可は、ステージ1変換テーブル構造の所与のレベルにおける変換テーブル全体に適用され、これは、不正アクセスに対して保護される必要がある機密情

50

報のために使用されるいくつかのメモリ領域と、この保護を必要としない非機密情報のみを含む他のメモリ領域とを含み得る、様々なメモリ領域のための変換テーブルエントリを含み得る。

【0094】

以下で更に説明されるように、ステージ1変換テーブルエントリに対する保護エントリ符号化の使用をサポートしない実装形態を提供することが可能である。この場合、オペレーティングシステムが、非機密情報を含む非保護領域に関連付けられたあるステージ1変換テーブルエントリを更新することを可能にするために、PRO領域への書込みを許可された書込み要求タイプの1つではないPRO領域への書込みアクセス時に生成された失敗は、EL2で動作するハイパーバイザにトラップを引き起こす可能性があり、ハイパーバイザは、オペレーティングシステムがステージ1変換テーブルエントリを更新したい領域がオペレーティングシステムによって更新されることから保護されるべきかどうかをソフトウェアで決定することができ、その領域が保護される必要がない場合、オペレーティングシステムによって要求された更新を進めることができる。しかしながら、実際には、オペレーティングシステムは、メモリの非保護領域の変換テーブルエントリを比較的頻繁に変更する必要がある場合があり、したがって、更新が必要とされるたびにハイパーバイザにトラップすることは、性能の面で遅い場合がある。

【0095】

ステージ1変換テーブルエントリのための保護エントリ符号化（例えば、ビット76、78を使用する）は、オペレーティングシステムが、ハイパーバイザの介入なしに非保護エントリに更新を行うこと（及び、任意選択で、いくつかの実装形態では、ハイパーバイザの介入なしに保護エントリの非更新制限ビットに更新を行うこと）を可能にするのに役立つ。これは、所与のステージ1変換テーブルがメモリのPRO領域に記憶される場合であっても、保護エントリと非保護エントリとの混合を含むため、ハイパーバイザの関与をより頻繁に回避することができるので、性能を向上させるのに役立つ。処理回路4の命令デコーダ10及び実行ステージ16は、保護エントリチェックタイプの読取りチェック書込み（RCW）命令と呼ばれる少なくとも1つのタイプの命令をサポートし、この命令は、アクセスされたメモリシステムロケーションに記憶されたデータをチェックして、保護ステージ1変換テーブルエントリの符号化と一致する値を有するかどうかをチェックするための保護エントリチェックを条件として更新が行われる所与のメモリシステムロケーションへの更新を要求するために使用することができる。アクセスされたメモリシステムロケーションにおけるデータが、保護ステージ1変換テーブルエントリであるデータと一致する値を有することを判明した場合、所与のメモリシステムロケーションの少なくとも更新制限されたビットのサブセットへの更新が抑制される。RCW命令は、EL1で実行されるオペレーティングシステムによって実行されることが許される。RCW命令は、対応ステージ2変換テーブルエントリによってPRO許可でマークされたメモリ領域中のデータを更新することを許可された命令の制限されたサブセットのうちの1つである。

【0096】

保護エントリチェックは、保護エントリチェック回路54によってハードウェアで実行され、図7に示されるように、保護エントリチェック回路54は、MMU 28内、又はデータを記憶するメモリシステムロケーションのより近く、例えば、キャッシュ、インターコネクト、又はメモリコントローラなどのメモリシステム構成要素56内のいずれかで実装され得る。また、MMU 28（又はパイプラインの実行ステージ16）内に実装された保護エントリチェック回路54のいくつかの部分と、メモリストレージのより近くに実装された他の部分とを有するロジックの分散セットを使用することも可能である。RCW命令を実行するスレッドと同じプロセッサ回路上で実行される別のスレッドによって、又は別のプロセッサコアによって所与のメモリシステムロケーションへのアクセスが要求されるときに、他のアクセスが、RCW命令のいずれかの部分的効果ではなく、RCW命令を処理する前の所与のメモリシステムロケーションの値、又はRCW命令を処理した後の所与のメモリシステムロケーションの値のいずれかを見るように、また、所与のメモリ

10

20

30

40

50

システムロケーションにおけるデータを読み取る保護エントリチェックと、RCW命令に
応答して所与のメモリシステムロケーションにおけるデータに
応答して所与のメモリシステムロケーションにおけるデータの
後続の更新との間の期間に所与のメモリシステムロケー
ションを更新することは不可能であるように、保護エントリ
チェックにおいて実行される読み取り、チェック及び書込
み動作は、アトミック（不可分）動作として実行される。
アトミック性を実施するために、メモリシステムロケーシ
ョンに対してアトミック読み取り／書込み動作を実施する
ための任意の知られている技法を使用することができる
（例えば、読み取りと書込みとの間の期間中に他の動作
によるアクセスに対してメモリロケーションをロックす
る、又はその期間中に競合アクセスを許可するが、競合
アクセスが読み取りと書込みとの間の期間中に検出され
た場合にRCW動作を再開する）。読み取り、チェック、及
び書込みのアトミック性を実施することによって、これは、
不正確な処理結果につながり得る競合状態を回避する。
読み取り、チェック、及び書込み動作がアトミック的に
実行されるので、書込みが進み、書込みデータを記憶す
るメモリシステムロケーションに戻すことができる前に
チェックを実行するために、読み取りデータをMMU 28
又はプロセッサパイプライン4の別の要素までずっと戻
さなければならない場合の持続時間と比較して、読み取
りと書込みとの間の期間の持続時間を短縮するために、
保護エントリチェック回路54を、更新されているストレ
ージロケーションにより近いメモリシステム構成要素56
内に実装することが有用である可能性がある。

10

20

30

40

50

【0097】

図8に示される例では、有効なステージ1変換テーブルエントリ及び無効なステージ1
変換テーブルエントリの両方が、エントリが保護エントリとして指定されることを可能に
する符号化を有する。しかしながら、無効エントリが保護されているとして指定されるこ
とが可能であることは必須ではなく、他の例は、無効エントリフォーマットから保護エン
トリ符号化ビットフィールド78を省略することができる。また、異なる実装形態は、RCW
命令に
応答して保護エントリのいくつかのビットがそれらの更新を抑制されるかについて
異なるオプションを選択することができる。いくつかの実装形態は、RCW命令に
応答して保護エントリへのいかなる更新も防止することができ、所与のメモリシステムロケー
ションにおけるデータが保護エントリとして符号化されない場合、RCW命令に
応答してのみ更新が許可される。他の実装形態は、更新制限されたビットのサブセット及び更新制
限されないビットのサブセットを指定することができ、したがって、更新制限されないビ
ットのサブセットへの更新は、保護エントリに対してさえ許可可能であり得る。例えば、
アクセスフラグ70及びダーティビット修正子72など、セキュリティにとって重要でない
いくつかのフィールドが存在する場合があります、これらは、保護エントリ内であっても更
新することが可能である。どのビットが更新制限されているか又は更新制限されていない
かは、所与のアーキテクチャに対して非プログラマブルな方法で固定されるか、又は制御
レジスタに記憶された選択値を使用してソフトウェアによってプログラマブルであるかの
いずれかであり得る。例えば、選択値は、いくつかの異なるモードのうちの1つから選択
することができ、各モードは、ビットが更新制限される異なる設定に関連付けられる。し
かしながら、図7の例では、選択値は、更新制限されたビットの位置を識別するビットマ
スクとして符号化され、選択値はマスクレジスタに記憶される（例えば、図7に示すRC
WMask__Valid__EL2レジスタ及びRCWMask__Invalid__EL2
レジスタは、それぞれ有効エントリ及び無効エントリの更新制限されたビットを選択する
ためのものであり、RCW__Mask__Invalid__EL2レジスタは、無効エン
トリを保護エントリとして符号化することができない実装形態では省略することができ
る）。選択値への更新は、閾値特権レベル以上で実行するプログラム命令に制限されてもよく、
例えば、EL2又はEL3で実行する命令のみが、選択値を更新することを許可されて
もよい。選択値の状態にかかわらず、強制的に更新制限されるいくつかのビットが存在し
得る。例えば、エントリが保護エントリであるかどうかを符号化するために使用されるビ
ットフィールド76、78は、他のどのビットが更新されることが可能であるにかかわ
らず、更新されることを許可されなくてもよい。一般に、RCW命令は、特定のエントリ

が保護されているか保護されていないかのステータスを変更することを禁止され得る。ビットフィールド 76、78 の設定は、代わりに、EL2 又は EL3 などのより高いレベルの特権で実行されるプログラムコードによって制御され、プログラムコードは、保護エントリを記憶するメモリ領域を部分読取り専用としてマークしないステージ 2 変換テーブルの異なるセットを使用してメモリにアクセスすることができ、したがって、標準的な汎用記憶命令を使用して保護ステージ 1 エントリのビットフィールド 76、78 を設定することができる。

【0098】

プロテクトされたエントリチェックを実装することができる様々な方法がある。一例では、アクセスされたメモリシステムロケーションに記憶されたエントリが有効かつ保護されている場合、それを変更することはできず、無効である場合、それを有効にすることを含めて（エントリも保護されていない限り）、それを変更することができる。代替的に、有効エントリ内に保護ビットフィールド 76 が存在し、無効エントリ内に保護ビットフィールド 78 が存在する可能性があり、保護エントリに対する変更は許可されなくてもよく、そうでなければ、（エントリが保護されているか否かのステータスを変更する）以外の非保護（有効又は無効）エントリに対する更新が許可される。別の例は、有効エントリ内に保護ビットフィールド 76 を提供し、無効エントリ内に保護ビットフィールド 78 を提供することができ、RCW 命令は、保護されていない場合（保護される以外）、エントリに任意の変更を行うことが可能であり、一方、保護されている場合、RCW 命令は、有効エントリについて説明したようにいくつかのビットに変更を行い、無効エントリ内のいくつかのビットに変更を行うことができる。いくつかの例では、どのビットが保護されるかを記述するための機構は、保護フィールド又は有効フィールドを除く任意のフィールドのハードワイヤードアーキテクチャ選択である。代替的に、どのビットが有効エントリ内で保護されるかを記述するための機構は、EL2 によって所有されるマスキレジスタを使用することができ、及び／又はどのビットが無効エントリ内で保護されるかを記述するための機構は、EL2 によって所有されるマスキレジスタである。更新制限されたビットを定義するための異なる選択が、有効エントリ及び無効エントリのそれぞれに対して可能であり、例えば、1つのアプローチは、有効エントリの更新制限されたビットを定義するためのマスキレジスタを定義するが、無効エントリの更新制限されたビットをハードワイヤすることであり得る。

【0099】

また、保護エントリ内のいくつかのフィールドを更新することが許可されるときにチェックを適用する方法にはバリエーションがあり得るが、2つの例示的なオプションは、以下の通りである。

A) 保護エントリチェック回路 54 は、エントリが有効及び／又は保護されているか否かをチェックするために現在のエントリを読取り、次いで、（RCW 命令が、書込むことが許可されていない更新制限されたビットを変更しようとしていたか否かをチェックすることなく）書込むことが許可されているビットのみを記憶する。

B) 保護エントリチェック回路 54 は、現在のエントリを読取り、エントリが有効及び／又は保護されているか否かをチェックする。それが保護されており、RCW 命令が、書込むことが許可されていないビットを変更しようとしていない場合、書込みを行うことができるが、RCW 命令が、更新制限されたビットを更新しようとしている場合、書込みは失敗し、何も書込まれない。

【0100】

A 及び B は両方とも実行可能な選択肢である。

【0101】

RCW 命令に応答して、書込みが成功したか失敗したかの指示を、処理回路 4 の制御レジスタに格納された条件ステータスフラグに書込むことができる。例えば、条件ステータスレジスタは、処理動作の結果に応じて設定することができ、条件ステータスフラグの状態に応じて条件付きで動作（分岐動作又は算術／論理動作など）をトリガすることができ

る条件付き命令によってテストすることができるいくつかの条件フラグ（例えば、負フラグN、0フラグZ、キャリーフラグC、及びオーバーフローフラグV）を含むことができる。したがって、RCW命令によって要求された書込みのいずれかの部分が不成功であったかどうかに基づいて条件ステータスフラグを更新して、書込みが成功したかどうかをチェックするためにメモリスistemロケーションを再読取りする必要なしに、後続の命令が書込みの結果に応じてアクションをとることを可能にすることが有用であり得る。

【0102】

図12、図13、及び図14は、保護エントリチェックRCW命令のいくつかのバリエーションの処理を示す。図12は、命令の記憶バリエーション又はスワップバリエーションのいずれかの処理の例を示す（バリエーションに依存する最終ステップ726又は728以外の処理ステップの大部分は、両方の命令について同じである）。記憶バリエーション及びスワップバリエーションの両方は、更新されるべき所与のメモリスistemロケーションのアドレスを生成するために使用されるアドレスオペランドを提供するレジスタXdと、所与のメモリスistemロケーションに書込まれるべき新しいデータを提供するソースレジスタXsとを指定する。少なくともスワップバリエーションはまた、所与のメモリスistemロケーションから読取られた古いデータが書込まれる宛先レジスタXtを指定する。記憶バリエーションは、古いデータがどの宛先レジスタにも書込まれないという点でスワップバリエーションとは異なるので、記憶バリエーションは、どの宛先レジスタも指定する必要がない。しかしながら、一例では、記憶バリエーション及びスワップバリエーションは、宛先レジスタXtを指定するために使用されるフィールドが所定の値を有する場合に命令が記憶バリエーションとして扱われ得ることを除いて、同一の符号化を使用して符号化され得る。例えば、いくつかの命令セットアーキテクチャは、特定のレジスタ指定子（例えば、レジスタ31）を「0」レジスタに対応するものとして定義することができ、これは、命令のオペランドとして指定されると、オペランドがハードウェア内に設けられたレジスタから実際に読取られる必要なく、オペランドが値0を有するかのように処理されるようにする。したがって、いくつかの例では、宛先レジスタXtが「0」レジスタX31として指定されるとき、命令は記憶バリエーションとして扱われ得る。他の例では、記憶命令は、スワップ命令とは完全に異なる命令タイプとして符号化され得る。

【0103】

図12のステップ700において、書込まれるアドレスオペランド及び新しいデータ（「NewData」）が、それぞれレジスタ指定子Xd及びレジスタ指定子Xsによって識別されるレジスタから読取られる。ステップ702において、メモリアクセスのためのターゲットアドレスが、アドレスオペランドに基づいて決定される。例えば、アドレスオペランドは、ターゲットアドレスを直接指定する絶対アドレスとして扱うことができ、あるいは更なるベースレジスタ内の値又はRCW命令自体のアドレスを識別するプログラムカウンタ値などの基準アドレスに対するオフセットを定義することができる。アドレスオペランドに基づいて計算されたターゲットアドレスは仮想アドレスであり、MMU28によって物理アドレスに変換され得る。ステップ704において、ターゲットアドレスが現在の命令にアクセス可能であるかどうかについての（保護エントリチェック以外の）任意のMMUチェックがパスされると仮定すると、（変換された）ターゲットアドレスに対応するメモリスistemロケーションから読取られたデータ（「ReadData」）を取得するために、メモリスistemに対して読取り要求が発行される。これは、RCW命令の「読取り」に対応する。

【0104】

ステップ706として、保護エントリチェック回路54は、ReadDataが保護ステージ1（stage-1、S1）変換テーブルエントリの符号化と一致する値を有するかどうかを決定する。これは、RCW命令の「チェック」部分に対応する。ReadDataが、保護ステージ1変換テーブルエントリであることと一致する値を有さない場合、ステップ708において、保護エントリチェック回路は、NewDataが保護ステージ1変換テーブルエントリとして符号化されているかどうかをチェックする。もしそうであれば

、ステップ 710 では、RCW 命令によって要求された書込みが拒否されるか、あるいは、RCW 命令によって New Data として指定されたステージ 1 変換テーブルエントリの非更新制限されたビットを、メモリシステムロケーションの対応するビットに書込むことができ、少なくとも、エントリが保護されるかどうかを符号化するために使用されるビットは、書込まれない更新制限されたビットと見なされる。いずれにしても、ステップ 712 で、RCW 命令によって要求された書込みを完全に実行できなかったことを報告するために、条件ステータスフラグがセットされる。

【0105】

ステップ 706 において、Read Data が保護ステージ 1 変換テーブルエントリとして符号化されていると決定された場合、ステップ 716 において、保護エントリチェック回路 54 は、読取られたデータが、有効又は無効なステージ 1 変換テーブルエントリであることと一致する値を有するかどうかを決定する。読取られたデータが無効な保護ステージ 1 変換テーブルエントリであることと一致する値を有する場合、ステップ 718 において、保護エントリチェック回路 54 は、New Data がステージ 1 変換テーブルエントリの任意の無効なエントリ更新制限されたビット（エントリが保護されているかどうかを符号化するために使用される少なくとも任意のビットを含む）を変更しようとするかどうかを決定し、変更しようとする場合、方法は再びステップ 710 及び 712 に進み、少なくとも無効なエントリ更新制限されたビットの更新を抑制し、条件ステータスフラグを設定する（再び、これは、書込みを完全に拒否することによって、又は非更新制限のビットにのみ書込むことによって行うことができる）。

【0106】

一方、ステップ 716 において、Read Data が、保護エントリとして符号化された有効なステージ 1 変換テーブルエントリであることと一致する値を有すると決定された場合、ステップ 720 において、保護エントリチェック回路 54 は、New Data が、ターゲットアドレスに対応するメモリシステムロケーションから読取られたステージ 1 変換テーブルエントリの任意の有効なエントリ更新制限されたビット（エントリが保護されているか否かを符号化するために使用される少なくとも任意のビットを含む）を変更しようとしているか否かを決定する。そうである場合には、再びステップ 710 において、書込みが拒否されるか、又は非更新制限のビットを書込むためだけに許可され、ステップ 712 において、書込みの失敗を報告するために条件ステータスフラグがセットされる。

【0107】

無効な変換テーブルエントリが保護エントリとして符号化されることをサポートしない実装形態では、ステップ 716 及び 718 を省略することができ、方法は、Read Data が保護エントリとして符号化されるときに、ステップ 706 からステップ 720 に直接進むことができる。

【0108】

ステップ 708 で、Read Data が保護エントリでなかった場合に書込まれる New Data、又はステップ 718 若しくは 720 で、New Data（Read Data が保護エントリであった場合に書込まれる）が更新制限されたビットを変更しようとしないう場合、ステップ 714 で、RCW 命令の書込みが許可され、したがって、New Data がターゲットアドレスに対応するメモリシステムロケーションに書込まれる。

【0109】

書込みが成功したか拒否されたか（少なくとも部分的に）にかかわらず、ステップ 724 で、実行されている現在の RCW 命令が記憶バリエーションであるかスワップバリエーションであるかに応じて動作が変化する。命令が記憶バリエーションである場合、ステップ 726 において、更なるアクションは必要とされず、Read Data はどの宛先レジスタにも書込まれない。命令がスワップバリエーションである場合、ステップ 728 で、Read Data が宛先レジスタ X_t に書込まれる。いくつかの実装形態は、記憶バリエーション及びストッパバリエーションの両方をサポートしない場合があり、その場合、ステップ 724 を省略することができ、方法は、ステップ 714 からステップ 726 及び 728 のうちの関連する 1 つ

に直接進むことができる。

【0110】

ステップ704での読取り、ステップ714での書込み、及びステップ704と714との間で実行される様々なチェック動作は、ステップ704での読取りとステップ710又は714での書込みとの間にメモリシステムロケーションへの介入書込みが行われることが不可能な動作の不可分のセットとして、又は実行の別のスレッドが動作のセットを実行する部分的な結果を見ることが不可能な動作の不可分のセットとして、アトミックに実行される。

【0111】

図13は、保護エントリチェックRCW命令の比較及びスワップ（compare-and-swap、CAS）バリエーションの処理を示すフロー図である。図12と同じ参照番号で示された図13のステップは、上述したものと同一である。ReadDataを記憶し、NewDataを提供するために使用されるレジスタに使用される表記は、図12と比較して図13では交換されており、Xtは、NewDataを提供するレジスタであり、Xsは、書込み前にReadDataの古い値が書込まれた宛先レジスタであることに留意されたい。図13は、CASバリエーションが比較データ（「CompareData」）と呼ばれる追加のソースオペランドを指定するので、ステップ700がステップ750で置き換えられるという点で図12と異なる。この例では、命令符号化において必要とされるレジスタフィールドの数を低減するために、CompareDataは、ステップ728においてReadDataを書込むための宛先レジスタとして使用される同じレジスタXsにおいて指定されるが、これは必須ではなく、他の例は、Xsとは別の更なるレジスタにおいて比較データを指定することができる。

【0112】

ステップ702及び704は、図12と同じである。ステップ704の後、追加のステップ752が実行されて、ターゲットアドレスに対応する所与のメモリシステムロケーションから読取られたReadDataと、レジスタXs内のRCW命令によって指定されたCompareDataとが比較される。保護エントリチェック回路54は、比較に基づいて、比較条件が満たされているかどうかを決定する。例えば、比較条件は、CompareDataとReadDataとが等しいかどうかであってもよいし、より小さい、より大きい、等しくないなどの別の比較条件に基づいてもよい。いくつかの実装形態は、比較条件を等しい条件として固定してもよい一方で、他の実装形態は、命令のパラメータがどのタイプの比較を実行するかを選択することを可能にしてもよい。比較条件が満たされていない場合、ステップ754で、RCW命令によって要求された書込みが拒否され、比較条件失敗によって引き起こされた書込みの失敗を報告するために条件ステータスフラグがセットされる（例えば、比較条件失敗時に否定フラグNを設定する）。比較条件が満たされる場合、ステップ706、708、710、714、716、718、720が図12と同様に実行されて、ターゲットアドレスに対応するメモリシステムロケーションから読取られたデータの保護エントリステータスをチェックし、チェックの結果に基づいて書込みが許可されるかどうかを制御する。書込みが許可された場合、ステップ714は、先に説明したものと同一であり、書込みがNewDataをメモリシステムロケーションに書込むことを可能にする。ステップ710において、書込みが拒絶されるか、又は部分的にのみ実行される場合、図12の後続のステップ712は、図13のステップ762で置き換えられ、これは、書込み失敗を報告するために条件ステータスフラグを設定するという点で同一であるが、比較及びスワップバリエーションの場合、失敗が保護エントリチェック失敗によって引き起こされたことを区別し、比較条件失敗の場合にステップ754で使用する値とは異なる値に条件ステータスフラグを設定することができる。

【0113】

比較条件が満たされているか否か、又は保護エントリチェックが成功しているか否かにかかわらず、ステップ724、726、及び728は図12と同じであり、任意選択でReadDataを宛先レジスタXsに書込む（この場合も、宛先レジスタ指定子が所定の

10

20

30

40

50

値、例えば 31 を指定するとき、宛先レジスタ Xs の更新を抑制することが可能である）。

【0114】

図 13 は、比較条件の評価が保護エントリチェックよりも優先される場合を示しており、比較条件が失敗したが、エントリは保護され、ステップ 708, 718, 720 でのチェックが失敗した場合、条件ステータスコードは CAS 失敗を示す。保護エントリチェックが優先されることも可能であり、その結果、エントリが保護され、ステップ 708, 718 又は 720 でのチェックが失敗した場合、たとえ比較条件が失敗したとしても、条件ステータスコードは、保護エントリチェックに起因する書込みの失敗を示す。例えば、図 13 は、ステップ 706 の前の代わりにステップ 714 の後にステップ 752 及び 754 を実装するように修正することができる。

10

【0115】

図 14 は、保護エントリチェック RCW 命令のビット設定／クリアバリエーションの処理を示すフロー図である。図 14 において、ステップ 700～728 は、図 12 と同じであるが、図 14 では、NewData は、ソースレジスタ内で直接指定されるのではなく、アドレス指定されたメモリシステムロケーション内で設定又はクリアされるビットの位置を符号化するソースレジスタ Xs 内に提供されるビットマスク（「BitMask」）に基づいて計算される。したがって、図 12 との唯一の違いは、ステップ 700 において、レジスタ Xs が NewData を直接指定するのではなく BitMask を定義すること、及びステップ 704 とステップ 706 との間に追加のステップ 770、772、774 が実行されることである。ステップ 770 において、方法は、ビット設定命令又はビットクリア命令が実行されているかどうかに応じて異なる（両方のタイプの命令をサポートする必要はなく、したがって、これらの命令のうちの 1 つのみがサポートされる場合、ステップ 770 は省略され、ステップ 772、774 のうちの関連する 1 つがステップ 704 の後に実行され得る）。ビット設定命令が実行されている場合、ステップ 774 において、NewData は、アドレス指定されたメモリシステムロケーションから読取られた ReadData と、RCW 命令によって指定された BitMask とに対してビット単位の OR 演算を実行した結果に設定される（したがって、ビット設定命令について、BitMask において「1」とマークされたビット位置は、アドレス指定されたメモリシステムロケーション内で 1 に設定されるように要求される）。対照的に、ステップ 772 において、ビットクリア命令が実行されている場合、NewData は、ReadData 及び BitMask の逆数に対してビットごとの AND 演算を実行した結果に設定される（したがって、ビットクリア命令について、BitMask において「1」とマークされたビット位置は、アドレス指定されたメモリシステムロケーション内で 0 にクリアされるように要求される）。ビット設定バリエーション及びビットクリアバリエーションの両方について、BitMask の「0」ビットに対応する ReadData のビットは、NewData 内のそれらの元の値を保持し、したがって、RCW 命令によって変更されない。ステップ 772 又は 774 で NewData を計算した後、図 14 の後続のステップは全て図 12 と同じである。

20

30

【0116】

本出願におけるフロー図の全てについて、同じ機能を異なる順序で実装することもでき、したがって、フロー図はステップの順次シーケンスを示すが、互いに依存しない任意のステップについて、ステップを並べ替えるか、又は少なくとも部分的に並列に実行することが可能であることが理解されよう。

40

【0117】

したがって、図 6 に示すように、機密メモリページ（例えば、機密データ又は命令に使用されることが予想されるページ）に対応する中間アドレスマッピングに到達するために変換テーブルツリー構造をトラバースするために使用される様々なステージ 1 変換テーブルエントリは、保護エントリ符号化を有するように設定することができる。これは、これらのエントリのうちの 1 つが、（例えば、ページング動作の結果として）ページへのアク

50

セスを禁止するために一時的に無効として設定される場合であっても当てはまる可能性がある。一方、保護エントリと同じページテーブル内の他のエントリは、更新があまり制限されていない非保護エントリであり得る。保護エントリ符号化をサポートすることによって、これは、メモリのPRO領域に記憶された所与のページテーブルが保護エントリと非保護エントリとの混合を含むことを可能にし、非保護エントリは、上記で説明したバリエーションのいずれかに従ってRCW命令を実行することによって、ハイパーバイザの介入なしにEL1で実行されるオペレーティングシステムコードによって更新されることが可能であり、一方、保護エントリは、より厳しい制限を受けることができる。専用タイプの命令（例えば、上述のRCW命令のバリエーションのうちの1つ以上）が、保護エントリチェックをトリガするために提供され、PRO許可は、他のタイプの命令（記憶命令の大部分など）がメモリのPRO領域を更新することができるのを防止するので、これは、性能の点で非常に高価になるメモリへの書き込みごとに保護エントリチェックを実行する必要性を回避する。

10

20

30

40

50

【0118】

アンチエイリアシングチェック

上述した機構は、特定のステージ1変換エントリを破損（悪意のある者によってハッキングされたコードによって故意に、又は誤って書かれたコードによって）から保護するのに有用である。しかし、図15に示すように、同じ中間アドレスマッピング62を指定するステージ1変換テーブルエントリを定義することによって、いくつかの異なる仮想アドレスが同じ中間アドレスにエイリアスすることが可能である。異なる仮想アドレスVA2を同じ中間アドレスIPAにマッピングするエイリアシングステージ1エントリを定義することによって、攻撃者が、VA1をIPAにマッピングするステージ1変換エントリの第1のセットについて上述したPRO許可及び保護エントリ符号化によって提供される保護を回避することができるのを防止するために、図8に示すように、ステージ2変換テーブルエントリは、対応するメモリ領域がアンチエイリアシング特性を有するかどうかを指定するビットフィールド79を有することができる（あるいは、アンチエイリアシング特性79は、間接レジスタを参照して、ステージ2変換テーブルエントリによって間接的に指定されてもよい）。領域がアンチエイリアシング特性を有すると示される場合、その領域へのアクセスにおいて追加のアンチエイリアシングチェックが実行され、全てのウォークされたステージ1変換テーブルエントリ（その領域の仮想アドレスから物理アドレスへのステージ1アドレスマッピングを指定する対応するステージ1変換テーブルエントリを見つけるために変換テーブルウォークでアクセスされるであろう）が、（a）メモリのPRO又は読取り専用領域に記憶され、保護エントリとして符号化されるか、又は、（b）メモリの読取り専用領域に記憶されるかのいずれかであるかをチェックする。これは、アンチエイリアシング特性を有するステージ2変換テーブルエントリに関連付けられたメモリ領域へのアクセスごとに実際に実行されるために、それらのウォークされたステージ1変換テーブルエントリを通じたページテーブルウォークを必ずしも必要としないことに留意されたい。毎回完全な変換テーブルウォークを実行する必要性を回避するために、アンチエイリアシングチェックに合格したかどうかを示す（又は、あるウォークされたステージ1変換テーブルエントリについて、それらがPRO領域に記憶されている、及び／又は保護エントリであるとすでに決定されているかどうかを示す）ために、情報をTLB 29にキャッシュすることが可能である。

【0119】

図16は、アンチエイリアシングチェックを実行する方法を示すフロー図である。ステップ800において、あるターゲット仮想アドレスVAxを指定するメモリアクセス要求が発行される。ステップ802において、MMU 28は、VAxから中間アドレスIPAyへのステージ1マッピングと、中間アドレスIPAyからターゲット物理アドレスPAzへのステージ2マッピングとに応じて、ターゲット仮想アドレスVAxからターゲット物理アドレスPAzへのアドレス変換を開始する（ステージ1及びステージ2変換のために2つの別個のアクションを実行することは必須ではないが、これは1つのオプション

であり、他の例は、すでにキャッシュされている変換のために V A x から P A z に直接マッピングすることができる組み合わせられたステージ 1 及び 2 T L B を有することができるが、T L B におけるミス時に、図 6 に示すように、ステージ 1 及びステージ 2 ウォークを実行することによって新しい V A から P A へのマッピングが識別される)。

【0120】

ステップ 804 において、M M U 28 は、I P A y に対応するステージ 2 変換テーブルエントリ (ブロック記述子又はページ記述子) がアンチエイリアシング特性を示すかどうかをチェックする。そうである場合、ステップ 806 において、M M U は、全てのウォークされたステージ 1 変換テーブルエントリがアンチエイリアシング条件を満たすかどうかをチェックする。ウォークされたステージ 1 変換テーブルエントリは、仮想アドレス V A x に対応する完全な変換テーブルウォークが実行された場合に、V A x から I P A y への S 1 アドレスマッピングを指定する対応 S 1 変換テーブルエントリを見つけるために変換テーブルウォークにおいてアクセスされるエントリである (このウォークは、T L B 29 にすでにキャッシュされているものに依拠して、現在のメモリアクセスに実際には必要とされない場合がある)。例えば、図 6 では、ウォークされたステージ 1 変換テーブルエントリは、L 0、L 1、及び L 2 ステージ 1 ページテーブル内の D _ T a b l e とマークされたエントリ、並びに L 3 ステージ 1 ページテーブル内の D _ P a g e とマークされたエントリである。アンチエイリアシング条件は、以下の条件のいずれかが満たされるとき、所与のウォークされたステージ 1 変換テーブルエントリに対して満たされる。

a) 所与のウォークされたステージ 1 変換テーブルエントリは保護エントリとして指定され、所与のウォークされたステージ 1 変換テーブルエントリは物理アドレス P A j に記憶され、そのために、P R O 許可又は読取り専用許可は、P A j を導出するために使用されるステージ 2 アドレスマッピングを提供する関連するステージ 2 変換テーブルエントリによって指定される。又は

b) 読取り専用許可は、所与のウォークされたステージ 1 変換テーブルエントリの物理アドレス P A j を導出するために使用されるステージ 2 アドレスマッピングを提供する関連するステージ 2 変換テーブルエントリによって指定される。

【0121】

図 6 の特定の例では、アクセスされたページの P A を導出するために使用される L 1 ステージ 1 エントリに対する関連するステージ 2 変換テーブルエントリは、図 6 において「D _ P a g e」として示されるステージ 2 L 3 エントリである。図 6 に示される他のウォークされたステージ 1 エントリに対して、同様に、アンチエイリアシング条件が満たされるために P R O 又は読取り専用許可でマークされるべき関連するステージ 2 L 3 エントリ (又は、ステージ 2 ブロック記述子が I P A y に対応して発見される場合、ステージ 2 L 1 又は L 2 エントリ) がある (これらは、各ウォークされたステージ 1 変換テーブルの物理アドレスを取得するために示される様々なステージ 2 変換ウォークの最後のエントリである)。

【0122】

図 16 のステップ 806 において、M M U 28 が、ウォークされたステージ 1 変換テーブルエントリのうちのいずれか 1 つ以上がアンチエイリアシング条件を満たさないと決定した場合、ステップ 808 において、メモリアクセスが拒否される。失敗がシグナリングされ得、失敗は、エラー処理アクションを実行するために (例えば、E L 2 において実行する) 例外ハンドラをトリガし得る。

【0123】

全てのウォークされたステージ 1 変換テーブルエントリがアンチエイリアシング条件を満足する場合、ステップ 808 は省略される。この場合、ステップ 810 において、M M U 28 は、任意の他のチェック (メモリ領域へのアクセスに対して設定されている P R O 許可に基づく任意のチェック、メモリアクセス要求が R C W 命令に応答して発行されたかどうかの保護エントリチェック、又はこれをサポートする実装形態におけるセキュア／非セキュア状態に基づくチェックなど、他の不適切なアクセスから保護するための任意の

他の特定のチェックなど)が満たされているかどうかにもチェックする。他のチェックのいずれかが満たされない場合、再びステップ808において、メモリアクセスが拒否される(生成される失敗タイプは、アクセスチェック失敗の原因に依存し得る)。そうであれば、ステップ812においてメモリアクセス要求が続行を許可される。

【0124】

したがって、図6に示すように、アンチエイリアシング特性は、アクセスされているメモリ領域に対する物理アドレスマッピングを提供するステージ2変換テーブルエントリに設定することができる(これは、ページ記述子又はブロック記述子のいずれかであり得る)。アンチエイリアシング特性が、対応するメモリロケーションへの有効なアクセスに対して設定される場合、これは、そのメモリ領域に対する中間アドレスマッピングを提供するエントリへのパス上の全てのウォークされたステージ1変換テーブルエントリが、(a)保護されているとマークされ、PRO許可を指定するためにそれらのウォークされたステージ1変換テーブルエントリを記憶する領域の物理アドレスマッピングを提供するステージ2エントリに対してマークされるか、又は(b)そのPAに対するPAマッピングを提供するステージ2エントリによって読取り専用許可が指定されるPAに記憶されることを必要とする。これは、攻撃者が、メモリの対応する領域にアクセスするために使用されることが予想される信頼できるアドレスマッピングに適用される保護を回避するために、新しいエイリアシングステージ1アドレスマッピングを容易にセットアップすることができないことを意味する。EL1においてオペレーティングシステムコードの挙動に影響を及ぼすことができる攻撃者は、メモリアクセスを制御するために使用されるステージ2エントリに対する制御を有さないが、なぜなら、これは、EL1において実行するコードによって更新することができないVTBR_EL2レジスタ内のベースアドレスに基づくからである(したがって、攻撃者の新たに作成されたエイリアシングステージ1アドレスマッピングを記憶する領域に対してPRO又は読取り専用許可を設定させることができない)。また、ステージ1変換テーブルエントリを更新するためにEL1で実行されるコードの機構は、上述した保護エントリチェックタイプのRCW命令(他の命令はメモリのPRO領域に書込むことを禁止されている)を実行することであり得、その命令は任意の変換テーブルエントリの保護状態を変更することができないので、攻撃者はステージ1エントリを保護されるようにすることができない。また、読取り専用領域は、いかなる書込み命令によっても書込むことができない。したがって、攻撃者が作成することができる任意の新しいエントリは、VA-IPAマッピングを取得するために使用されるステージ1エントリが保護されているかどうか、及び/又はそれらのエントリがメモリのPRO又は読取り専用領域に記憶されているかどうかのアンチエイリアシングチェックのうちの少なくとも1つに失敗するはずである。

【0125】

ステージ1トップレベルベースアドレスへの不適切な更新に対する保護

EL1において実行されるオペレーティングシステムコードの挙動に影響を及ぼすことができる攻撃者によって試みられる可能性がある別の攻撃は、ベースアドレスレジスタVTBR_EL1によって示されるステージ1トップレベルベースアドレス(L0ステージ1ページテーブルのメモリ内のロケーションを識別する)を修正することであり得る。例えば、攻撃者は、攻撃者によって定義されたステージ1テーブルの新しいセットのアドレスを置換して、正しく形成され、ハイパーバイザによって検証されるように正しく挙動する許可されたページテーブル構造のアドレスを置き換えることができる。また、攻撃者は、例えば、正しいL0ベースアドレスを置き換えるためにL1、2、又は3ページテーブルのうちの1つのベースアドレスを置換することによって、MMU 28に既存の許可されたステージ1ページテーブルを予期せぬ方法で使用させようと試みる可能性があり、その結果、アクセスされたテーブルが予測レベルからツリーの誤ったレベルで使用され、仮想アドレスの異なるビットがテーブルから関連するエントリを選択するために使用されることに起因して、異なるメモリ領域に対するネクストレベルテーブルポインタ又はアドレスマッピングが、アクセスされているメモリ領域に対して誤って使用される可能性がある

。

【0126】

図17は、これらのタイプの攻撃から保護するために実行することができるステージ1トップレベルベースアドレスチェックを示す。ステップ1000では、あるターゲット仮想アドレスを指定するメモリアクセス要求に対してページテーブルウォークが必要とされる（必要なアドレスマッピングがTLBからすでに利用可能であるのでページテーブルウォークを必要としないメモリアクセス要求に対しては、前のページテーブルウォークに続いてこれらのアドレスマッピングがキャッシュに割り振られた時点で、必要なステージ1トップレベルベースアドレスチェックがすでに行われているので、別のチェックを実行する必要はない）。ステップ1002において、ステージ1トップレベルベースアドレスは、ステージ1変換テーブルベースアドレスレジスタTTBR_EL1内の値に基づいて決定される。ベースアドレスは、中間アドレスIPA_baseとして指定される。ステップ1004において、MMU_28は、IPA_baseからPA_baseへのマッピングを提供する関連するステージ2変換テーブルエントリによって指定される情報を取得する。例えば、この情報は、すでにTLBにキャッシュされている場合にはTLB_29から取得することができ、又はステージ2変換テーブルベースアドレスレジスタVTBR_EL2において指定されたステージ2ベースアドレスを使用してステージ2変換テーブルウォークを実行することによって取得することができる。

10

【0127】

ステップ1006において、MMU_28は、ステージ1トップレベルテーブル部分読取り専用チェックがイネーブルかどうかを決定する。例えば、これは、制御レジスタ（例えば、更新が例外レベルEL2以上で実行するコードに制限されるステージ2変換制御レジスタVTCR_EL2）に記憶されたステージ1トップレベルテーブル部分読取り専用チェックイネーブル制御値に基づいて決定され得る。代替的に、他の実装形態は、ステージ1トップレベルテーブル部分読取り専用チェックが永続的にイネーブルであると見なし得る。ステージ1トップレベルテーブル部分読取り専用チェックがイネーブルにされている場合、ステップ1008において、MMU_28は、関連するステージ2変換テーブルエントリがPRO許可を指定しているかどうかをチェックし、指定していない場合、ステップ1010において、メモリアクセスが拒絶され、失敗が通知される。これは、攻撃者がステージ1変換テーブルベースアドレスレジスタTTBR_EL1を、攻撃者によって作成された新しいL0ページテーブルを指すように修正しようと試みる場合、攻撃者がメモリのPRO領域を修正することができず、したがって非PRO領域に書込まれているはずなので、修正されたベースアドレスに基づくアクセスが失敗し、したがってステージ1トップレベルテーブルPROチェックが失敗することを意味する。

20

30

【0128】

ステージ1トップレベルテーブルPROチェックが、ステップ1006でディセーブルであるか、又はイネーブルであるがステップ1008でパスする場合、ステップ1012で、MMU_28は、ステージ1トップレベルテーブル存在チェックがイネーブルであるかどうかを決定する。この場合も、これは、制御レジスタ（例えば、ステージ2変換制御レジスタVTCR_EL2）に記憶されたステージ1トップレベルテーブル存在チェックイネーブル制御値に基づいて決定され得る。ステップ1012においてチェックがイネーブルであるかどうかを決定するために使用されるイネーブル制御値は、ステップ1006について上述されたイネーブル制御値と同じであり得る（例えば、いくつかの実装形態では、ステップ1008及び1014におけるチェックは、全体としてイネーブルであるか又は全体としてディセーブルである単一のチェックの2つのステップと見なされ得る）。ステージ1トップレベルテーブル存在チェックがイネーブルである場合、ステップ1014において、MMU_28は、関連するステージ2変換テーブルエントリがステージ1トップレベルエントリ存在許可80を指定しているかどうかを決定する。図8に関して上述したように、ステージ1トップレベルエントリ存在許可は、（ステージ1トップレベルエントリ存在許可を有するメモリ領域もPRO許可を有すると仮定されるように）PRO許可の

40

50

代替的なバリエーションとして符号化されてもよく、あるいは、P R O許可が提供されるか否かの指示とは別個の独立した属性として符号化されてもよい。関連付けられたステージ2変換テーブルエントリがステージ1トップレベルエントリ存在許可を指定しない場合、再びステップ1010において、メモリアクセスが拒否され、失敗がシグナリングされる。これは、L1、L2、又はL3テーブルを保持するために使用されるメモリ領域に対応するステージ2エントリがステージ1トップレベルエントリ存在許可を有さないように定義され得るので、ステージ1トップレベルベースアドレスをL1、L2、又はL3テーブルのアドレスを指すように修正することによって、有効かつ真正なL1、L2、又はL3テーブルがL0テーブルと置換されることから保護するために使用され得る。どのアドレスが有効なメモリアクセスのためのステージ1 L0ベースアドレスとして使用され得るか
10
を制限するために、任意の有効かつ真正なステージ1 L0テーブルを保持するために使用されるメモリ領域のみが、対応するステージ2エントリにおいてステージ1トップレベルエントリ存在許可を有するものとしてマークされ得る。

【0129】

ステージ1トップレベルテーブル存在チェックが、ステップ1012においてディセーブルであるか、又はイネーブルであるがステップ1014においてパスする場合、ステップ1016において、MMUは、P A _ b a s eによって識別されるメモリ領域にアクセスするために必要とされる任意の他のチェックを実行し、これらが失敗する場合、再びステップ1010においてメモリアクセスを拒否する。任意の他のチェックにパスした場合、
20
ステップ1018において、ステージ1トップレベルベースアドレスI P A _ b a s eを有効に使用して、ページテーブルウォークを実行することができる。したがって、ステージ1トップレベル変換テーブルエントリのアドレスは、決定されたP A _ b a s eにインデックスオフセットを適用することによって取得され、インデックスオフセットは、変換されるターゲットV Aのビットのサブセットに基づいて決定される。その後、ページテーブルウォークは前述したように継続する。

【0130】

したがって、図6に示すように、ソフトウェアによって定義される（したがってハードウェアによる要件として実施されない）予想される使用において、追加保護が望まれるメモリ領域のP Aマッピング64を取得するためにページテーブルウォーク上でアクセスされるステージ1エントリの中で、ステージ1 L0ページテーブルの記憶口ケーションを
30
識別するP Aマッピング64を提供するステージ2ページ／ブロック記述子は、P R O及びステージ1トップレベル存在許可の両方を指定し、P Aマッピング64を提供するステージ2ページ／ブロック記述子は、ステージ1 L1、L2、又はL3ページテーブルの記憶口ケーションを識別し、P R O許可を指定するがステージ1トップレベル存在許可を指定しない。これは、上述したベースアドレス置換攻撃から保護する。ベースアドレスチェックを実装する必要性を回避する代替は、E L2において実行するハイパーバイザへのステージ1ベースアドレスレジスタT T B R _ E L1への任意のアクセスをトラップすることであり得、次いで、ハイパーバイザは、E L1において実行するオペレーティングシステムコードによって要求された更新が有効であるかどうかを検査し、必要であれば更新を拒否し得る。しかしながら、実際には、オペレーティングシステムは、コンテキスト切り
40
替え時にベースアドレスレジスタT T B R _ E L1内のアドレスを頻繁に切り替える必要がある場合があり、したがって、全ての更新をトラップすることは、性能の面でコストがかかる場合がある。図17に示されるステージ1トップレベルベースアドレスチェックを実装することによって、これは、T T B R _ E L1へのベースアドレスレジスタ更新に対するそのようなトラップの必要性を回避し、性能を改善することができる。

【0131】

いくつかの例では、ステージ1トップレベルの存在許可の単一のバリエーションがサポートされ得、その場合、図17のステップ1014におけるチェックは、単に、そのステージ1トップレベルの存在許可が指定されているかどうかのチェックであり得る。

【0132】

10

20

30

40

50

他の例は、特定のステージ1変換テーブルベースアドレスレジスタが対応するメモリ領域内のアドレスを指定することができるより細かい制御を可能にするために、ステージ1トップレベル存在許可の2つ以上のバリエーションをサポートすることができる。例えば、いくつかの実装形態は、以下の2つのステージ1ベースアドレスレジスタをサポートし得る。

●変換される仮想アドレスの最上位ビットの構成可能な数 (number、N) が全て0に設定される場合に、EL0又はEL1におけるステージ1変換のために選択される (Nは、制御レジスタにおいて指定される制御値で定義することができる)、TTBR0__EL1、及び

●変換される仮想アドレスのN個の最上位ビットのいずれかが0でないある場合に、EL0又はEL1におけるステージ1変換のために選択される、TTBR1__EL1。

【0133】

次に、ステージ1トップレベルの存在許可のいくつかのバリエーションは、以下を含んで定義されることができる。

●TopLevel0は、TTBR0__EL1を介してアクセスされるトップレベル変換テーブルのためには使用が許可されるが、TTBR1__EL1を介してアクセスされるトップレベル変換テーブルのためには使用が許可されないメモリ領域を示す。

●TopLevel1は、TTBR1__EL1を介してアクセスされるトップレベル変換テーブルのためには使用が許可されるが、TTBR0__EL1を介してアクセスされるトップレベル変換テーブルのためには使用が許可されないメモリ領域を示す。

●TopLevel01は、TTBR0__EL1又はTTBR1__EL1のいずれかを介してアクセスされるトップレベル変換テーブルのために使用が許可されるメモリ領域を示す。

【0134】

この場合、ステップ1014におけるチェックの一実装形態は、以下の条件のいずれかが満たされる場合、図17のステップ1010において失敗がシグナリングされるようにし得る。

●TTBR0__EL1は、対応するメモリ領域がTopLevel0又はTopLevel01許可のいずれも持たないベースアドレスを提供するために使用される。又は

●TTBR1__EL1は、対応するメモリ領域がTopLevel1又はTopLevel01許可のいずれも持たないベースアドレスを提供するために使用される。

【0135】

いくつかの実装形態では、EL2においてソフトウェアによって制御される制御レジスタに設定される更なる制御は、TTBR0__EL1がTopLevel1ページへのアクセスを与えることを禁止されるかどうか、及びTTBR1__EL1がTopLevel0ページへのアクセスを与えることを禁止されるかどうかを制御することができる。この場合、ステップ1014におけるチェックは、以下の条件のいずれかが満たされた場合に、ステップ1010において失敗を通知させることができ、

●TTBR0__EL1は、TTBR0__EL1がTopLevel1ページにアクセスするために使用されたときに、失敗をトリガできるようにTTBR0/TopLevel1失敗イネーブル制御が設定されている場合、対応するメモリ領域がTopLevel01許可を有しないか、又はTopLevel1許可を有するベースアドレスを提供するために使用される。又は

●TTBR1__EL1は、TTBR1__EL1がTopLevel0ページにアクセスするために使用されるときに、失敗をトリガできるようにTTBR1/TopLevel0失敗イネーブル制御が設定されている場合、対応するメモリ領域がTopLevel01許可を有しないか、又はTopLevel0許可を有するベースアドレスを提供するために使用される。

【0136】

これらの特徴は、トップレベルステージ1変換テーブルを提供するためにどのメモリア

ドレス領域に使用され得るかについてのより細かい制御を可能にするが、イネーブル制御は、TTBR0及びTTBR1の両方のベースアドレスを提供するために使用される任意のトップレベルページについて許容可能であると考えられる場合、これらのより細かいチェックがディセーブルされることを可能にする。

【0137】

いくつかの実装形態では、様々なトップレベル存在許可TopLevel0、TopLevel1、TopLevel01の符号化は、これらがTopLevel0 PRO許可、TopLevel1 PRO許可、及びTopLevel01 PRO許可として扱われるように、PRO許可の符号化と組み合わせることができる。そのような実装形態では、TopLevel0、TopLevel1、又はTopLevel01メモリ領域をPRO許可を有さないものとして定義することは不可能である。それにもかかわらず、ステージ1トップレベルテーブル存在許可のいずれかを有するものとして扱われない別個のPRO許可符号化が存在するので、TopLevel0、TopLevel1、又はTopLevel01許可のいずれも有さないものとしてPRO領域を定義することが可能である。

10

【0138】

図8の例では、PRO許可及びS1トップレベルエントリ存在許可は、ステージ2変換テーブルエントリ自体の符号化の一部として直接指定されるS2許可フィールド68で指定されるように示されている。同様に、ステージ1変換テーブルエントリは、エントリ自体のフィールド66でステージ1許可を直接符号化するものとして示されている。

20

【0139】

しかしながら、図18に示すように、許可情報を許可間接レジスタのステージ2変換テーブルエントリによって間接的に指定することも可能である。この場合、ステージ2変換テーブルエントリは、許可間接レジスタのどのフィールドがそのエントリのステージ2許可を指定するかを識別するフィールド識別子を指定することができ、許可間接レジスタの参照されるフィールドは、許可タイプを示すように符号化される。このアプローチは、例えば、PRO許可74、S1トップレベルエントリ存在許可80、上述のアンチエイリアシング特性79、又は後述のGCS属性に使用することができる。レジスタを使用する間接許可指定は、ソフトウェアが、メモリ内の多くの異なる変換テーブルエントリを更新する必要なく、レジスタフィールドに対する単一の更新によって、全てが同じ許可フィールドを参照する多くの変換テーブルエントリに対する許可を迅速に更新することを可能にするために有用である。また、許可間接レジスタの各フィールドが、変換テーブルエントリに対応する許可フィールドよりも多くのビットを有する実装形態では、間接は、エントリ内の許可のための限られた符号化空間で可能であるよりも多くのタイプの許可をサポートするのに役立つことができる。

30

【0140】

リターン指向プログラミング攻撃に対する保護のためのガード制御スタック

図19は、関数（参照を容易にするためにfn1とラベル付けされている）を呼び出し、関数から戻る一例を示す。関数（プロシージャとしても知られる）は、プログラムの別の部分から呼び出すことができ、完了すると、関数が呼び出されたプログラムフローの部分に処理を戻す一連の命令である。同じ関数をプログラム内の多くの異なる位置から呼び出すことができるため、関数を呼び出す際に関数リターンアドレスが記憶され、その結果、関数リターンは、プログラムフローがどのアドレスに戻されるべきかを区別することができる。

40

【0141】

例えば、図19に示すように、関数が呼び出される時点でリンク付き分岐命令BLRを実行し、リンク付き分岐命令のオペランドを使用して指定された分岐ターゲットアドレスの命令にプログラムフローを分岐させることができる。リンク付き分岐命令はまた、処理回路に、リンクレジスタ（関数リターンアドレスを追跡するために使用される指定されたレジスタ）を、リンク付き分岐命令の後の次の命令のアドレスに設定させる。分岐が行わ

50

れた後、多くの命令（例えば、LD、MUL、ADDなど）が関数コード内で実行され、関数が完了すると、リンクレジスタに記憶されたリターンアドレスによって示される命令への分岐を引き起こすリターン分岐命令RETが実行される。

【0142】

f n 1 内から他の関数が呼び出されず、f n 1 の最後のリターン分岐に到達する前に例外が発生しない場合、リンクレジスタのアドレスは、f n 1 が呼び出されたときに設定されたものと依然として同じであるはずである。

【0143】

しかしながら、バックグラウンドコードによって呼び出される第1の関数 f n 1 は、それ自体がネストされた方法で更なる関数（f n 2）を呼び出すことがよくあり、この場合、f n 2 への関数呼び出しは、リンクレジスタに記憶されたリターンアドレスを上書きしてしまうため、その更なる関数を呼び出す前に、第1の関数 f n 1 の関数コードには、リターンアドレスをリンクレジスタからメモリ内のデータ構造（例えば、後入れ先出し（LIFO））方法で動作するスタック構造）に保存する命令を含めるべきであり、f n 2 から戻った後、f n 1 の関数コードは、リターン分岐を実行する前にリターンアドレスをリンクレジスタに復元するべきである。リターンアドレスなどの関数リターン状態を保存及び復元する責任は、通常、ソフトウェアにある（リターンアドレスを保存するためのアーキテクチャ的に強制されたハードウェア機構はなくてもよい）。

【0144】

しかしながら、関数リターンアドレスはメモリに記憶されているが、例えば、別のプロセッサコア上で実行される別のスレッドを使用して、又は、呼び出された関数を中断してその間にメモリに記憶されたリターンアドレスを上書きする他のコードを実行することによって、攻撃者がそのデータを修正することに対して脆弱であり得る。あるいは、攻撃者は、メモリからレジスタにリターンアドレスを復元する命令のアドレスオペランドを修正することを目的とするいくつかの命令を実行することができるため、メモリからロードされたデータは、ネストされた関数を呼び出す前にメモリに最初に保存されたリターンアドレスと同じではなくなる。攻撃者が、関数呼び出し分岐（図19の例では#add1+4）の後の命令以外のプログラムフロー内の時点でリターン分岐を分岐させることができる場合、攻撃者はソフトウェアを誤って動作させることができ、特定のセキュリティ保護を回避したり、望ましくない動作を実行させたりする可能性がある。

【0145】

関数呼び出しは、処理回路が後で復元されることになる状態に関する情報を提供するリターン状態情報を生成する動作の一例である。リターン状態情報が取得され得る別のシナリオは、例外が発生したときであり得、その時点で、ハードウェアに設けられた例外処理回路又はソフトウェア例外ハンドラが、例外処理から戻った後に実行される命令のアドレスを示す例外リターンアドレス、及び／又は例外から戻った後にプロセッサが実行すべきモード又は実行状態を示す保存されたプロセッサ状態情報などの、例外リターン状態情報を取得し得る。例えば、保存されたプロセッサ状態情報は、例外レベルEL0～EL3のうちのどれから例外が発生したかだけでなく、例外が発生した時点のプロセッサの動作状態に関する他の情報を示すことができる。関数呼び出しと同様に、例外はネストされ得るため、1つの例外に対して取得された例外リターン状態は、別の例外が発生したときにメモリに保存される（ハードウェアで自動的に、又はソフトウェア例外ハンドラによってのいずれか）可能性があり、メモリ内に記憶されている間に攻撃者による改ざんに対して脆弱であり得る。これらのタイプの攻撃は、リターン指向プログラミング（ROP）攻撃と呼ばれることがある。そのような攻撃に対するアーキテクチャ上の対策を提供することが望まれる。

【0146】

図20及び図21は、「ガード制御スタック」（GCS）と呼ばれるメモリ内の保護されたデータ構造を使用して、ROP攻撃から保護するためのアプローチを示す。メモリアドレス空間内のGCSデータ構造の位置は、ソフトウェアによって選択され得るが、ハー

ドウェアは、攻撃者によって侵害されたオペレーティングシステム（例外レベル E L 1 で動作する）による改ざんを含む、悪意のある攻撃者による改ざんから G C S データ構造を保護するように設計された多くのアーキテクチャ上の特徴を提供する。

【 0 1 4 7 】

図 2 0 に示されるように、レジスタ 1 4 は、制御レジスタ 1 0 5 0 を含み、これは、G C S モードがイネーブルかディセーブルかを指定するための G C S イネーブルパラメータ 1 0 5 2 と、G C S メモリアクセス要求によってアクセスされるメモリ領域に対して上述のアンチエイリアシング特性 7 9 が設定されているかどうかのチェックを G C S メモリアクセス要求が受けるかどうかを（G C S モードがイネーブルである場合に）制御するステージ 1 G C S ハードニングチェックイネーブル制御パラメータ 1 0 5 4 とを（他のパラメータの中から）指定する 1 つ以上のレジスタを含み得る。レジスタ 1 4 はまた、G C S データ構造上のアドレスを示すスタックポインタを記憶するための 1 つ以上のガード制御スタックポインタ（G C S ポインタ）レジスタ 1 0 5 6 を含む。いくつかの例では、G C S ポインタレジスタ 1 0 5 6 は、実行状態（例外レベル E L 0 ~ E L 3）のうちの少なくとも 2 つに対して別々に提供されるレジスタのバンクセットであってもよく、異なる実行状態で動作するソフトウェアが、各実行状態の変換後に共有スタックポインタレジスタを再プログラムする必要なく、メモリ内の異なる G C S 構造を参照することを可能にする。他の例では、単一の G C S ポインタレジスタを使用することができ、ソフトウェアは、実行状態間の変換時に、G C S ポインタレジスタ 1 0 5 4 に記憶されたスタックポインタを更新することができる。図 2 0 には示されていないが、G C S イネーブルパラメータ 1 0 5 2 及びステージ 1 G C S ハードニングチェックイネーブル制御パラメータ 1 0 5 4 は、2 つ以上の異なる実行状態に対して別々に指定することもできる。

【 0 1 4 8 】

図 2 1 に示すように、G C S データ構造 1 0 5 8 は、（対応するステージ 1 アドレス変換テーブルエントリによって指定されたステージ 1 許可 6 6 によって）メモリの G C S 領域であると指定されたメモリの領域に記憶される。G C S 領域許可は、対応するステージ 1 アドレス変換テーブルエントリの符号化内で直接指定することもできるし、図 1 8 に示すように、許可間接レジスタ内で間接的に参照することもできる。メモリ領域が G C S 領域であると識別されると、その領域への書き込みアクセスは、G C S アクセス命令の特定のサブセットを実行するときに処理回路 4 によってトリガされる書き込み要求に制限される。G C S 構造にアクセスすることを意図しない一般的な記憶命令のためにソフトウェアによって使用される汎用ストア動作は、G C S アクセス命令の制限されたサブセットのうちの 1 つとは見なされない。M M U 2 8 は、G C S メモリアクセス要求ではない読取り要求を発行させる汎用ロード命令を使用して G C S 構造が読取られることを依然として許可し得る。メモリアクセス要求が G C S 領域へのアクセスを要求しており、要求が書き込み要求であり、要求が G C S アクセス命令の制限されたサブセットのうちの 1 つによってトリガされた G C S メモリアクセス要求でない場合、メモリアクセス要求は拒否され、失敗が通知される。

【 0 1 4 9 】

図 2 1 に示すように、G C S アクセス命令のサブセットは、現在の実行状態 E L x に対応する G C S ポインタレジスタ 1 0 5 6 に示されるスタックポインタを使用して決定された G C S 構造上の位置に、リターン状態情報（リンクレジスタからの関数リターンアドレス、又は例外リターンアドレス、もしくは例外発生時に取得された保存されたプロセッサ状態など）をプッシュさせる G C S プッシュ命令を少なくとも含むことができる。G C S アクセス命令はまた、G C S 構造から保護されたリターン情報をポップする少なくとも 1 つの形式の G C S ポップ命令を含む。

【 0 1 5 0 】

G C S 構造は、関数呼び出しや例外のネストを処理するために、ソフトウェアがメモリ内に保存されたリターン状態情報を維持するために使用する任意のデータ構造とは別個である。したがって、G C S 構造は、関数呼び出しや例外がネストされたときに、ソフトウ

エア自体がリターン状態情報の保存及び復元を追跡する必要性を排除することを意図していない（ソフトウェアトリガによるリターン状態の保存は、上述の G C S 保護アーキテクチャ手段をサポートしていないプロセッサと同じ方法で継続し得る）。代わりに、G C S 構造は、例外レベル E L 0 又は E L 1 で動作する侵害されたコードによる改ざんから保護された保護メモリの領域を提供し、これを使用して、関数呼び出しや例外の処理から戻するためにソフトウェアが使用することを意図したリターン状態情報を検証するための情報を提供することができる。

【 0 1 5 1 】

したがって、いくつかの実装形態では、保護リターン状態情報を G C S 構造からポップさせる G C S ポップ命令はまた、処理回路 4 に、ポップされたリターン状態をレジスタ（例えば、関数リターンのためのリンクレジスタ、又は例外リターンのための例外リターンアドレスレジスタ、及び／又は保存されたプロセッサ状態レジスタ）に記憶された現在のリターン状態情報と比較させ、G C S 構造 1 0 5 8 からポップされたリターン状態情報と、ソフトウェアが関数／例外リターンのために使用しようとする意図したリターン状態情報との間に不一致がある場合に失敗を通知させることもできる。したがって、関数呼び出し／リターンや例外エントリ／リターンの周辺で実行されるプログラムコード内に G C S プッシュ命令及び G C S ポップ命令のインスタンスを含めることによって、ソフトウェアを改ざんから保護することができる。

【 0 1 5 2 】

他の実装形態では、G C S 構造 1 0 5 8 からリターン状態情報をポップする命令とは別に、意図したリターン状態情報が有効であるかどうかを検証するための別個の命令を定義し得る。

【 0 1 5 3 】

あるいは、G C S ポップ命令は、保護リターン状態を G C S から、例外リターン又は関数リターンのためのリターン状態を指定するために使用される 1 つ以上のレジスタに直接ポップすることができ（又は、保護リターン状態をポップし、その状態を例外／関数リターンの制御に使用するために、例外／関数リターン命令と組み合わせることができ）、その場合、そのような実装形態においては、G C S 保護リターン状態は例外／関数リターンを制御するために直接使用されるため、ソフトウェアにより提供される意図したリターン状態情報が有効であるかどうかを検証するステップを実行することは必須ではない。

【 0 1 5 4 】

また、他のタイプの G C S アクセス命令もサポートすることができる。G C S イネーブル制御パラメータ 1 0 5 2 を使用して G C S モードがディセーブルにされているときに他の機能を有するいくつかの命令は、G C S モードがイネーブルされているときに実行されると、処理回路 4 に追加の機能（追加の G C S モード固有セキュリティチェックなど）を実行させることができる。

【 0 1 5 5 】

一般に、G C S 構造 1 0 5 8 に使用するための G C S メモリ領域タイプを定義するためのアーキテクチャサポートを提供し、G C S 領域タイプへの書込みアクセスを（G C S 領域タイプ以外のメモリ領域にアクセスすることを許可されていない可能性がある）G C S アクセス命令の限られたサブセットに制限することによって、これは、G C S 構造 1 0 5 8 上に記憶された保護リターン状態情報を改ざんしようとする攻撃者が利用できる攻撃面を低減することができる。

【 0 1 5 6 】

しかしながら、G C S 構造 1 0 5 8 を記憶する領域に対応するステージ 1 変換テーブルエントリに関連付けられたステージ 1 許可は、その領域が G C S 領域であることを示す特性を指定するために使用されるため、侵害されたオペレーティングシステムは、G C S 許可タイプを削除するためにそのステージ 1 変換テーブルエントリを修正しようとするか、又は、G C S 許可タイプを指定しない異なるステージ 1 変換テーブルエントリを使用して物理メモリの同じ領域へのアクセスを可能にするために、図 1 5 に示するようにエイリ

10

20

30

40

50

アッシングステージ1変換テーブルエントリを定義しようと試みる可能性がある。

【0157】

そのような攻撃から保護するために、前述の変換ハードニング機構を使用して、GCSデータ構造1058を記憶するためのGCS領域を指定するために使用されるステージ1変換テーブルエントリを保護することができる。したがって、GCS領域タイプを指定するステージ1変換テーブルエントリは、ステージ1変換テーブルエントリを記憶するメモリ領域の対応するステージ2変換テーブルエントリによって（直接的又は間接的に）指定されるステージ2許可情報によって指定される読取り専用領域又は部分読取り専用領域のいずれかに記憶することによって、改ざんから保護され得る。GCS領域へのリターン状態情報のプッシュはGCS領域へのデータの書き込みを必要とするため、読取り専用又は部分読取り専用領域タイプは、GCS領域自体に対応するステージ2エントリに対するステージ2許可において、指定されるべきではないことに留意されたい。また、上述のように保護エントリ符号化がサポートされている場合、GCS領域に対応するステージ1変換テーブルエントリは、前述のようにEL1において実行される保護エントリチェックタイプのRCW命令による修正から保護するために、保護エントリとして示すこともできる。また、アンチエイリアシング特性79は、GCS領域に対するアドレスマッピングを見つけるために使用される全てのウォークされたステージ1変換テーブルエントリが、メモリの読取り専用又は部分読取り専用領域に記憶されるハードニングステージ1変換テーブルエントリでなければならないことを強制する（また、保護エントリ符号化がステージ1変換テーブルエントリに対してサポートされ、変換テーブルエントリが部分読取り専用領域に記憶される場合、保護エントリとして符号化されることも要求される）ために、GCS領域に対応するステージ2変換テーブルエントリに対して指定することができる。これらの機構は、GCS領域指定を削除するためにステージ1変換テーブルエントリを修正しようとする試み、又はエイリアシングステージ1変換テーブルエントリを使用してそのエントリを回避しようとする試みが失敗することを意味する。

【0158】

上述した変換ハードニング機構がGCS領域に対応するステージ1変換を保護するために使用され、したがって、GCSアクセスが、エイリアシングステージ1変換エントリを提供する攻撃者によって意図されたGCS構造に置換された代替GCS構造には行われていないという信頼性を与えることを保証するために、ステージ1GCS変換ハードニングイネーブルパラメータ1054がイネーブル状態に設定され、GCSイネーブルパラメータ1052によってGCSモードがイネーブルにされているとき、GCSメモリアクセスによってアクセスされようとするターゲットメモリ領域に対応するステージ2変換テーブルエントリがアンチエイリアシング特性79を指定しない場合、GCSメモリアクセス（読取り及び書き込みアクセスの両方を含む）は拒否される（したがって、失敗を引き起こす）。これにより、（a）ステージ2変換テーブルエントリによって指定された領域に読取り専用として記憶されておらず、又は、（b）ステージ2変換テーブルエントリによって指定された領域に部分読取り専用として記憶されておらず、且つ、（保護エントリ符号化をサポートする実装では）非保護エントリとして符号化されている、非ハードニングステージ1変換テーブルエントリを使用してGCS領域へのアクセスが試みられた場合に、失敗が生成されるような保護が適切に行われることが保証される。GCSメモリアクセスに応答してアンチエイリアシング特性79をチェックする必要性は、ステージ1GCS変換ハードニングイネーブルパラメータ1054をディセーブル状態に設定することによってディセーブルすることができる（これは、アンチエイリアシング特性79又は変換ハードニング機構をサポートしなかったシステムのために書かれたレガシーコードに有用であり得る）。

【0159】

GCSモードの動作を制御するためのイネーブル制御値1052、1054は、EL1におけるオペレーティングシステム又はEL0におけるアプリケーションによる更新を防止するために、実行レベルEL2又はEL3で実行する命令によって更新されるように制

限されてもよい。

【0160】

図22は、GCSリターン状態プッシュ命令の処理を示すフロー図であり、GCSリターン状態プッシュ命令は、リターン状態をGCSにプッシュすることに特化したGCS固有命令であってもよいし、又は、GCSモードで実行されたときにGCSリターン状態プッシュ命令としても機能する、再利用された関数呼び出し分岐命令（リンク付き分岐命令）であってもよい。ステップ1100で、命令復号回路10は、GCSモードがGCSイネーブルパラメータ1052によってイネーブルにされていると示されている間に、リターン状態プッシュ命令を復号する。GCSモードがディセーブルにされていると示される場合、このタイプの命令は未定義命令と見なすことができ、したがって失敗を引き起こし得るか、又はアーキテクチャ上の効果はないが失敗を引き起こさないノーオペレーション（NOP）命令として扱われる可能性がある。GCSモードがイネーブルであると仮定すると、GCSリターン状態プッシュ命令に応答して、命令復号回路10は、処理回路4の実行ステージ16を制御して、レジスタ（例えば、関数リターンアドレスを記憶するために使用されるリンクレジスタ、又は例外リターンアドレス及び保存されたプロセッサ状態（例えば、値を示すモード／実行状態）などの例外リターン情報を記憶するために使用される例外リターン状態レジスタ）の情報に基づいてリターン状態情報を取得する。ステップ1104で、処理回路4のロード／ストアユニット26は、ステップ1102で取得されたリターン状態情報を、現在の実行状態（ELx）についてGCSポインタレジスタ1056に記憶されたGCSポインタに基づいて決定されたガード制御スタック上の位置にプッシュするために、1つ以上のGCSメモリアクセス要求を発行し、処理回路4は、スタックポインタをスタック上の次の位置に進めるために、GCSポインタレジスタ1056を更新してスタックポインタを更新する。任意の既知のスタックポインタ更新機構を使用することができる（例えば、スタックは、昇順スタック又は降順スタックとすることができ、スタックポインタは、情報がプッシュされる次の位置、又は情報がプッシュされた最後の位置のいずれかを指すことができる）。

10

20

【0161】

図23は、GCSモードがイネーブルにされている間にステップ1120で復号される、この例ではリターン状態検証命令としても機能する、GCSリターン状態ポップ命令の処理を示すフロー図である。GCSリターン状態ポップ命令は、GCSへのリターン状態のポップに特化したGCS固有命令であってもよく、又はGCSモードで実行されたときにGCSリターン状態ポップ命令としても機能する再利用された例外リターン命令であってもよい。この場合も、GCSモードがディセーブルにされている場合、この命令は未定義又はNOP命令として扱われ得る。GCSリターン状態ポップ命令の復号に応答して、ステップ1122において、命令デコーダ10は、処理回路4の実行ステージ16（ロード／ストアユニット26）を制御して、現在の実行状態ELxについてGCSポインタレジスタ1056に記憶されたスタックポインタに基づいて決定されたガード制御スタック上の位置からのリターン状態情報をポップするために、1つ以上のGCSメモリアクセス要求を発行し、処理回路4は、ポップ動作を考慮してスタックポインタを更新する。

30

【0162】

ステップ1124で、処理回路4は、リターン状態レジスタ（例えば、上述したリンクレジスタ又は例外リターン状態レジスタ）の情報に基づいて現在のリターン状態情報を取得する。ステップ1126で、処理回路4は、現在のリターン状態情報と、ステップ1122でGCSデータ構造1058から取得されたポップされたリターン状態情報とを比較し、比較された状態が一致するかどうかを決定する。現在のリターン状態情報とポップされた（GCS保護された）リターン状態情報との間に不一致が検出された場合、ステップ1128で、不一致のリターン状態はROP攻撃が試みられた兆候である可能性があるため、失敗状態が通知される。現在のリターン状態が、GCS構造1058から取得されたポップされたリターン状態と一致する場合、ステップ1130において、ソフトウェアは、関数／例外からのリターンに進むことが許可される。関数リターンや例外リターンは、

40

50

図 19 に示すリターン分岐又は例外リターン命令のような別個の命令の実行によってトリガされ得るため、GCSポップ／リターン状態検証命令によって直接トリガされる必要はないことに留意されたい。

【0163】

図 23 は、GCS からのリターン状態情報をポップすること、及びポップされたリターン状態に対して現在のリターン状態を検証することの両方を組み合わせた命令を示すが、これらの動作を別個の命令（GCS からのリターン状態をポップするための 1 つの命令、及び、現在のリターン状態に対してポップされたリターン状態を検証するための第 2 の命令）に分離することも可能である。また、対応する関数／例外リターンがもはや必要とされないシナリオにおいて、リターン状態情報を GCS 構造 1058 から削除できるようにするために、スタンドアロン GCS ポップ命令が提供され得る。また、GCS リターン状態ポップ命令が、関数／例外リターンに使用される関数／例外リターン状態を直接制御する場合（GCS リターン状態ポップ命令が、上述のように例外リターン命令と組み合わせられるため、又は、GCS リターン状態ポップ命令が、関数／例外リターンを制御するためのリターン状態を提供するために使用されるレジスタに直接 GCS 保護リターン状態をポップするためのいずれか）、検証ステップ 1126、1128 を実行する必要はなくてもよい。

【0164】

図 24 は、GCS イネーブルパラメータ 1052 によって GCS モードがイネーブルにされているときに発行されるメモリアクセスに対して MMU 28 によって実行されるアクセス許可チェックを示すフロー図である。ステップ 1200 で、ターゲットメモリ領域に対応するターゲット仮想アドレスを指定するメモリアクセス要求が発行される。メモリアクセス要求は、図 22 及び図 23 に示す GCS プッシュ／ポップ命令のうちの 1 つによって（又は別のタイプの GCS アクセス命令によって）トリガされる GCS メモリアクセス要求である可能性もあるし、GCS アクセスタイプの命令によってトリガされない別のタイプのメモリアクセス要求である可能性もある。ステップ 1202 で、MMU 28 は、ステージ 1 アドレス変換構造及びステージ 2 アドレス変換構造において定義された関連するステージ 1 アドレスマッピング及びステージ 2 アドレスマッピングに基づいてアドレス変換を開始する。ステップ 1203 で、MMU 28 は、ターゲット仮想アドレスに対するアドレスマッピングを提供するターゲットステージ 1 変換テーブルエントリによって直接的又は間接的に指定されたステージ 1 許可情報が、ターゲットメモリ領域が GCS 領域であることを指定するかどうかを決定する。

【0165】

ターゲットメモリ領域が GCS 領域である場合、ステップ 1204 において、MMU 28 は、メモリアクセス要求が、GCS アクセスタイプの命令の制限されたサブセットのうちの 1 つによってトリガされた GCS メモリアクセス要求であるかどうかを決定する。そうでない場合、ステップ 1205 において、MMU 28 は、メモリアクセス要求が書込み要求であるかどうかを決定する。メモリアクセス要求が書込み要求である場合、ステップ 1206 において、他の一般的なストア命令タイプが GCS 領域に記憶された GCS 構造 1058 に書き込むことができないようにするために、失敗が通知される。

【0166】

メモリアクセス要求が GCS メモリアクセス要求又は読取り要求である場合、ステップ 1208 において、MMU 28 は、ステージ 1 GCS ハードニングチェックイネーブルパラメータ 1054 が、ステージ 1 GCS ハードニングモードがイネーブルにされていることを示すかどうかを決定する。ステージ 1 GCS ハードニングモードがイネーブルにされているとき、ステップ 1210 において、GCS メモリアクセス要求に対して追加のチェックが実行され、アンチエイリアシング特性 79 がターゲットメモリ領域に対応するステージ 2 変換テーブルエントリによってターゲットメモリ領域に対して指定されているかどうかチェックされる。アンチエイリアシング特性 79 がターゲットメモリ領域に対して指定されていない場合には、再びステップ 1206 で失敗が通知される。

【0167】

ステップ1208で、ステージ1 GCSハードニングモードがディセーブルであると決定された場合、又は、ステップ1210で、ターゲットメモリ領域が、対応するステージ2変換テーブルエントリにおいて定義されたアンチエイリアシング特性79を有する場合、ステップ1212において、MMU28は、メモリアクセス要求に対して他のアクセス許可が満たされているかどうかを決定する。例えば、これは、ターゲット領域に対応するステージ1やステージ2変換テーブルエントリにおいて指定された他のパラメータ、又は、セキュリティ状態、例外レベル、もしくは処理回路4の他の動作モードに基づくような他のセキュリティ条件に基づいてもよい。他のアクセス許可が満たされない場合には、ステップ1206で失敗が再び通知される。他の全てのアクセス許可が満たされる場合、ステップ1214でメモリアクセス要求を許可することができる。

10

【0168】

ステップ1203で、ターゲットメモリ領域がGCS領域ではなかったとMMU28が決定した場合、ステップ1220で、MMU28は、メモリアクセス要求が、GCSアクセスタイプの命令の制限されたサブセットのうちの1つによってトリガされたGCSメモリアクセス要求であるかどうかを決定する。これはステップ1204と同じチェックであるが、ステップ1204と比較すると結果が異なる。ステップ1220で、メモリアクセス要求がGCSメモリアクセス要求である場合、ステップ1206で失敗が通知される（この失敗は、読取り及び書込み要求の両方に対してトリガされ得る）。これは、GCSメモリアクセス要求がメモリの非GCS領域にアクセスするために使用され得ないことを保証し、これにより、ソフトウェア開発者が、攻撃者の利用できる攻撃面を増加させる非GCSアクセス用のGCSアクセスタイプの命令を使用しようとするのが回避され、GCS以外の領域を指すように攻撃者によって修正されているGCSアクセスタイプの命令のアドレスオペランドに基づく攻撃の検出を可能になる。GCSアクセスタイプの命令をGCS領域にアクセスするものに制限し、非GCSアクセスタイプの命令を非GCS領域にアクセスするものに制限することによって、セキュリティを向上させることができる。

20

【0169】

ステップ1220で、メモリアクセス要求がGCSメモリアクセス要求でないと決定された場合、ステップ1222で、MMU28は、メモリアクセス要求に対して他のアクセス許可が満たされているかどうかを決定する。例えば、これは、上述のセキュリティ状態、例外レベル、又は動作モードに基づくチェックを含むことができ、前述した部分読取り専用領域タイプ又はアンチエイリアシング特性79に基づくチェックも含むことができる。また、メモリアクセス要求が前述の保護エントリチェックタイプのRCW命令によってトリガされた場合、アクセスが許可されるかどうかは、ターゲットVAに対応するターゲット位置から読取られた古いデータのチェックにも依存し得る。全ての必要なアクセス条件が満たされる場合、ステップ1224でメモリアクセス要求が許可される。いずれかのアクセス許可が破られた場合、ステップ1206で失敗が通知される。

30

【0170】

図24は、多くの異なるチェックが失敗したことに応答して、失敗を通知する単一のステップ1206を示すが、いくつかの実装形態は、失敗の原因に応じて異なる失敗タイプを通知し得ることが理解されよう。

40

【0171】

また、図24は、非GCS読取り要求がGCS領域をターゲットとする場合に失敗が必要でない一例を示すが、他の例では、ステップ1205を省略し、ステップ1204からステップ1206に進むことができ、メモリアクセス要求が読取り要求であるか書込み要求であるかにかかわらず、メモリのGCS領域をターゲットとするメモリアクセス要求がGCSメモリアクセス要求でない場合に失敗を通知する。

【0172】

GCSモードがGCSイネーブルパラメータ1052を使用して現在ディセーブルにされている場合、GCSアクセス命令は、失敗（例えば、未定義命令失敗）をトリガしても

50

よいし、ノーオペレーション（NOP）命令として扱われてもよい。また、GCSアクセス要求以外のメモリアクセス要求では、図24のステップ1212又は1222に示すチェックが行われ得るが、GCSモードがディセーブルにされている場合には、ステップ1203、1204、1208、1210、及び1220でのチェックは省略され得る。

【0173】

図25は、使用され得るシミュレータ実装を例示する。上記の実施形態は、当該技法をサポートする特定の処理ハードウェアを動作させる装置及び方法の点において本発明を実装しているが、コンピュータプログラムの使用によって実装される本明細書に記載の実施形態による命令実行環境を提供することも可能である。このようなコンピュータプログラムは、コンピュータプログラムがハードウェアアーキテクチャのソフトウェアベースの実装を提供する限り、シミュレータと称されることがよくある。様々なシミュレータコンピュータプログラムは、エミュレータ、仮想マシン、モデル、及び動的バイナリトランスレータを含むバイナリトランスレータを含む。典型的に、シミュレータ実装は、ホストプロセッサ1330上で実行されてもよく、任意選択でホストオペレーティングシステム1320を実行し、シミュレータプログラム1310をサポートする。いくつかの配置では、ハードウェアと提供されている命令実行環境との間に複数のレイヤのシミュレーションがあってもよく、及び／又は、同じホストプロセッサ上に提供されている複数の異なる命令実行環境があってもよい。歴史的に、強力なプロセッサが、合理的な速度で実行されるシミュレータ実装を提供するのに必要とされてきたが、このような手法は、互換性又は再使用の理由から別のプロセッサにネイティブなコードを実行することが望まれるようなときなど一定の状況では、正当化され得る。例えば、シミュレータ実装は、ホストプロセッサハードウェアによってサポートされていない追加の機能性を有する命令実行環境を提供し得るか、又は典型的には異なるハードウェアアーキテクチャに関連付けられた命令実行環境を提供し得る。シミュレーションの概要は、「Some Efficient Architecture Simulation Techniques」、Robert Bedichek、1990年冬 USENIX Conference、53～63頁に記載されている。

【0174】

これまで、特定のハードウェア構成物又は特徴を参照して実施形態を説明してきたが、シミュレーションされた実施形態では、好適なソフトウェア構成物又は特徴によって同等の機能性を提供することができる。例えば、特定の回路は、シミュレーションされた実施形態で、コンピュータプログラムロジックとして実装されてもよい。同様に、レジスタ又はキャッシュなどのメモリハードウェアは、シミュレーションされた実施形態で、ソフトウェアのデータ構造として実装されてもよい。前述の実施形態で参照されたハードウェア要素のうちの1つ以上がホストハードウェア（例えば、ホストプロセッサ1330）上に存在する配置では、いくつかのシミュレーションされた実施形態は、好適な場合、ホストハードウェアを利用することができる。

【0175】

シミュレータプログラム1310は、コンピュータ可読記憶媒体（非一時的媒体であってもよい）に記憶されてもよく、シミュレータプログラム1310によってモデル化されているハードウェアアーキテクチャのインターフェースと同じであるターゲットコード1300（アプリケーション、オペレーティングシステム、及びハイパーバイザを含みんでもよい）にプログラムインターフェース（命令実行環境）を提供する。したがって、上述した保護エントリチェックRCW命令及びGCSアクセス命令を含むターゲットコード1300のプログラム命令は、シミュレータプログラム1310を使用して命令実行環境内から実行することができ、その結果、上述した装置2のハードウェア機能を実際には有していないホストコンピュータ1330は、これらの機能をエミュレートすることができる。同様に、PRO領域タイプ、アンチエイリアシング特性、及びGCSメモリ領域タイプのサポートを含む、上述したような様々なメモリ管理チェック機能は、シミュレータプログラム1310のメモリ管理プログラムロジック1318を使用してエミュレートするこ

とができる。

【0176】

したがって、シミュレータプログラム1310は、上述した処理回路4の状態をシミュレートする処理プログラムロジック1312を有しし得る。例えば、処理プログラムロジック1312は、ターゲットコード1300のシミュレートされた実行中に発生するイベントに応答して、実行状態EL0～EL3の変換を制御することができる。命令復号プログラムロジック1314は、ターゲットコード1300の命令を復号し、これらをホスト装置1330のネイティブ命令セット内の対応する命令セットにマッピングする。レジスタエミュレーションプログラムロジック1316は、ターゲットコードによって要求されたレジスタアクセスを、ホスト装置1330のレジスタ又はメモリ1332内のデータにアクセスすることなどによって、ホスト装置1330のホストハードウェア上に維持された対応するデータ構造へのアクセスにマッピングする。メモリ管理プログラムロジック1318は、アドレス変換、ページテーブルウォーク、及びアクセス制御チェックを、上記のハードウェア実装の実施形態で説明したMMU28に対応する方法で実装するが、ターゲットコード1300に対して定義されたページテーブルに基づくアドレス変換におけるステージ2マッピングによって得られるシミュレートされた物理アドレスを、ホストメモリ1332にアクセスするために使用されるホスト仮想アドレスにマッピングする追加機能も有する。これらのホスト仮想アドレスは、それ自体、ホストによってサポートされる標準アドレス変換機構を使用して、ホスト物理アドレスに変換され得る（ホスト仮想アドレスのホスト物理アドレスへの変換は、シミュレータプログラム1310によって制御されるものの範囲外である）。

【0177】

本出願において、「～ように構成された（configured to...）」という用語は、装置の要素が、定義された動作を行うことが可能である構成を有することを意味するために使用される。この文脈において、「構成」とは、ハードウェア又はソフトウェアの配置又は相互接続の方法を意味する。例えば、装置は、定義された動作を提供する専用ハードウェアを有し得るか、又はプロセッサ若しくは他の処理デバイスが、機能を実施するようにプログラムされ得る。「ように構成された」は、装置要素が、定義された動作を提供するために何らかの変更がなされる必要があることを意味しない。

【0178】

本発明の例解的な実施形態が添付の図面を参照して本明細書で詳細に説明されているが、本発明はこれらの正確な実施形態に限定されないこと、及び様々な変更及び修正が、当業者によって、添付の特許請求の範囲によって定義されている本発明の範囲から逸脱することなく、実施形態に行われ得ることが理解されよう。

10

20

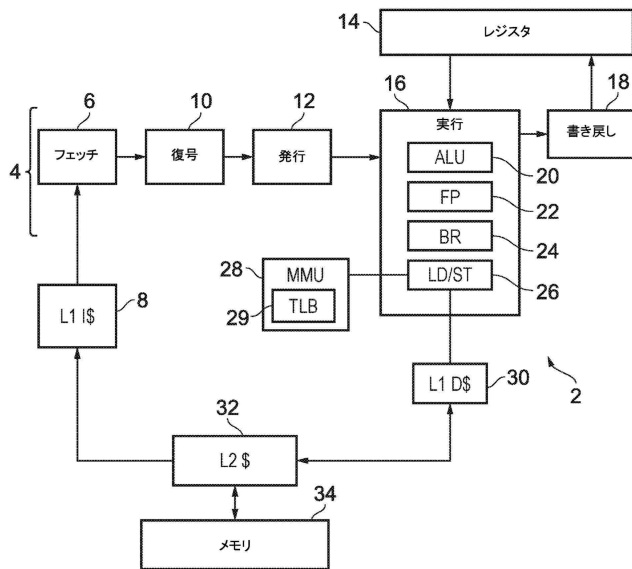
30

40

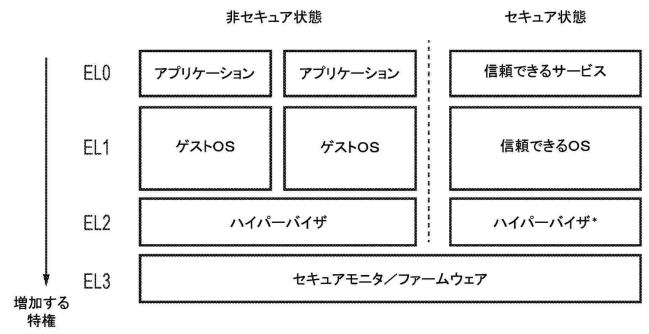
50

【図面】

【図 1】



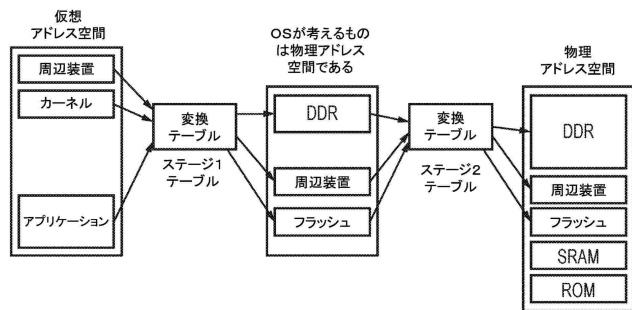
【図 2】



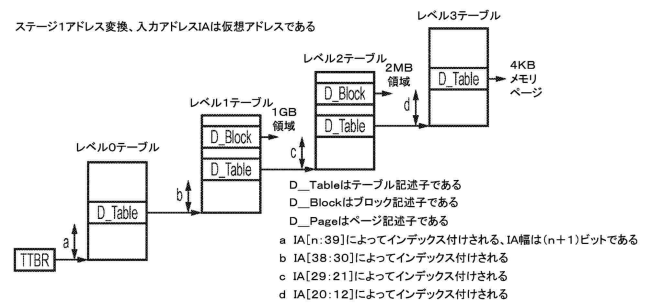
10

20

【図 3】



【図 4】

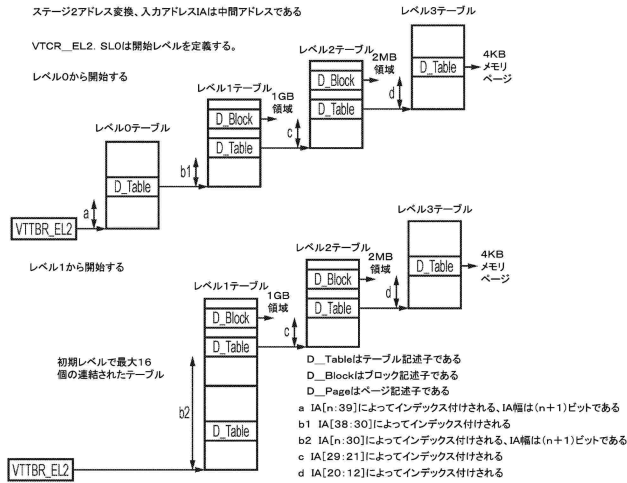


30

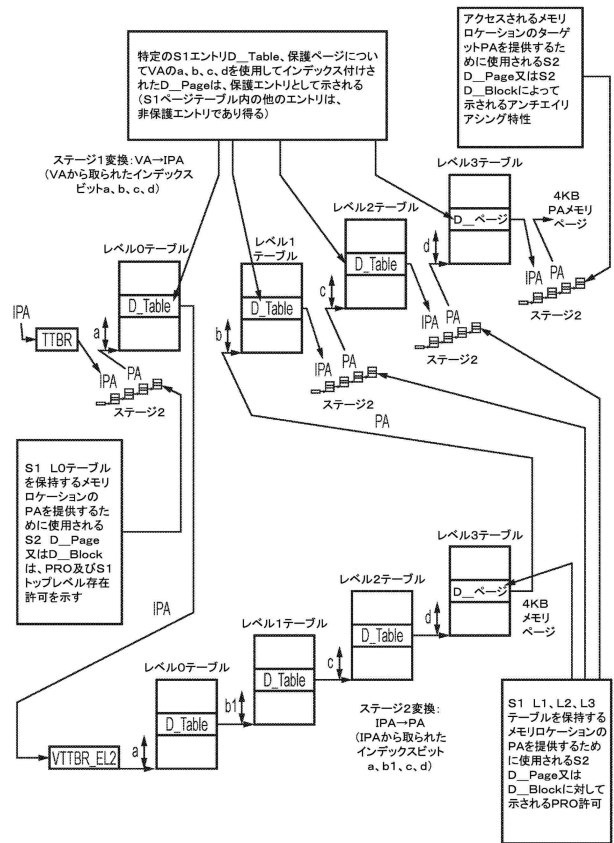
40

50

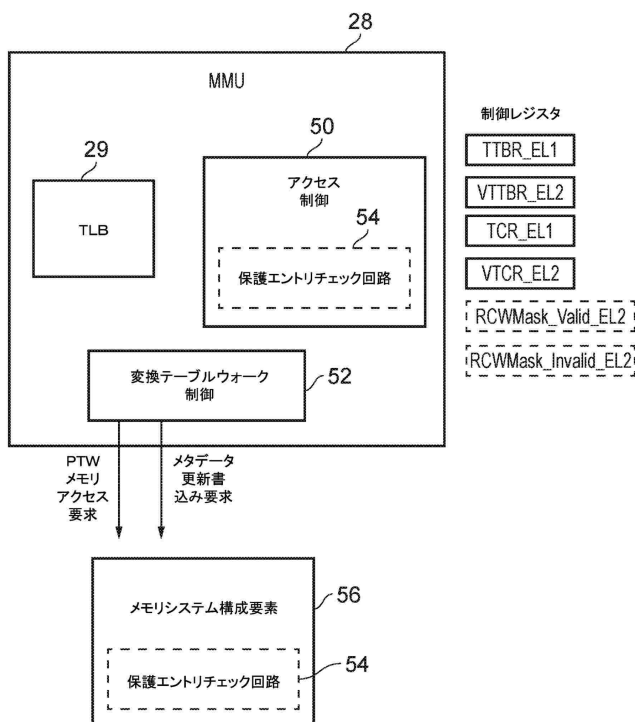
【図 5】



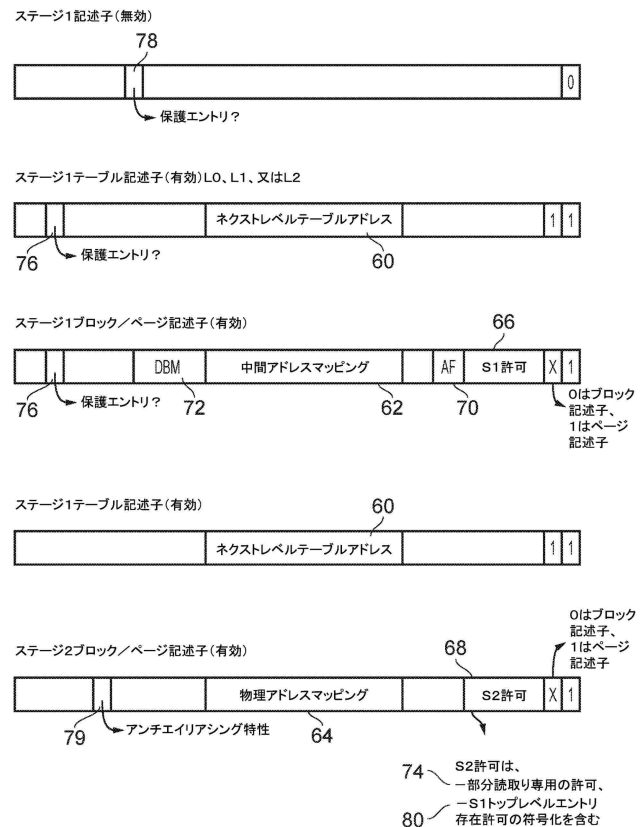
【図 6】



【図 7】



【図 8】



10

20

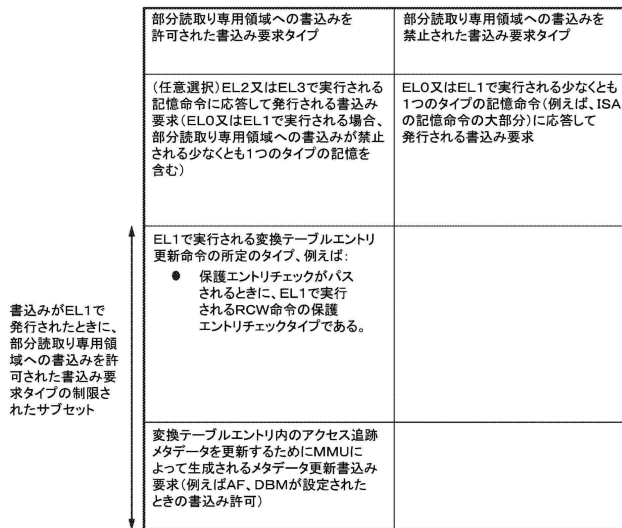
30

40

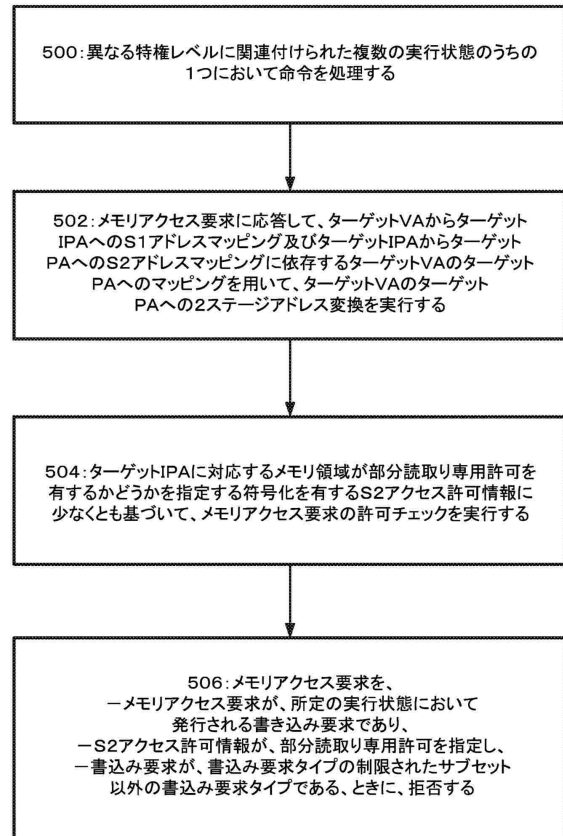
50

【図 9】

異なる書込み要求タイプにตอบสนองして、部分読取り専用としてS2許可によってマークされたメモリ領域に対する書込みアクセス制御:



【図 10】

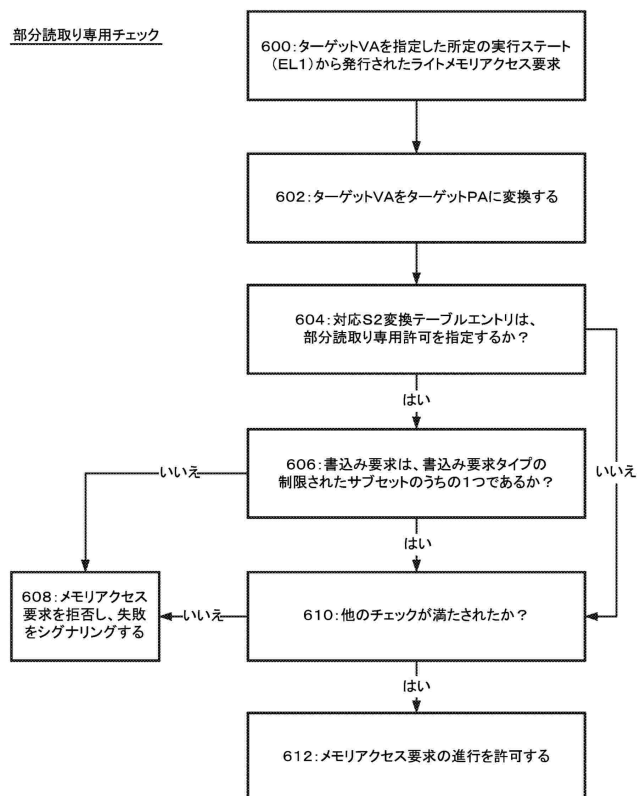


10

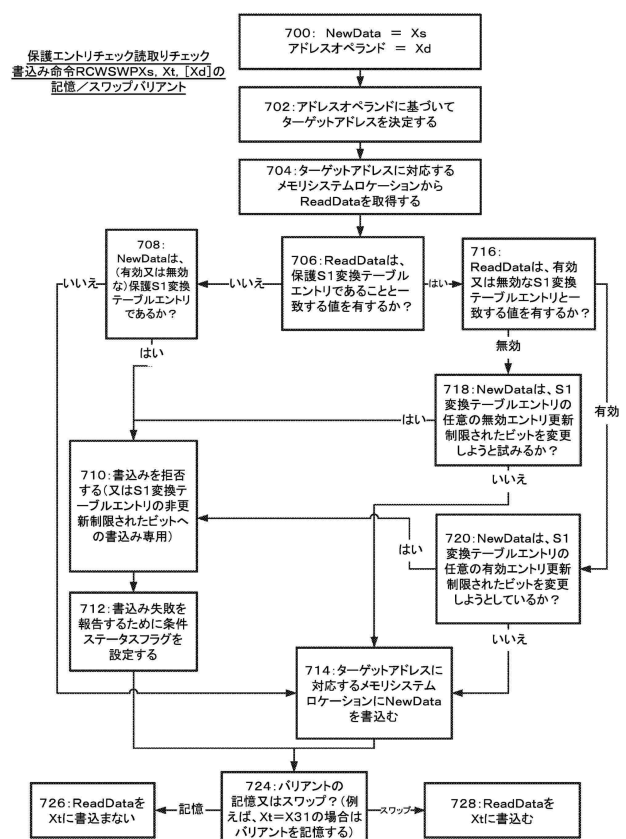
20

【図 11】

部分読取り専用チェック



【図 12】

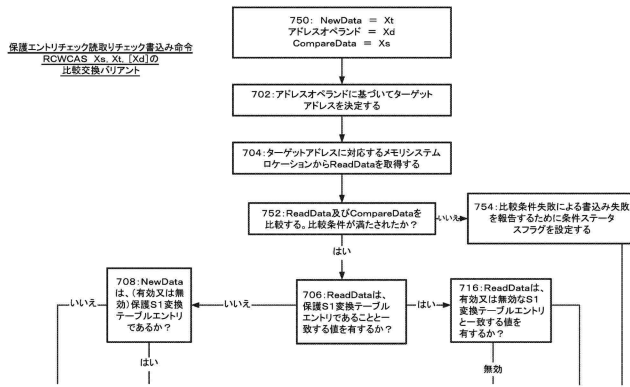


30

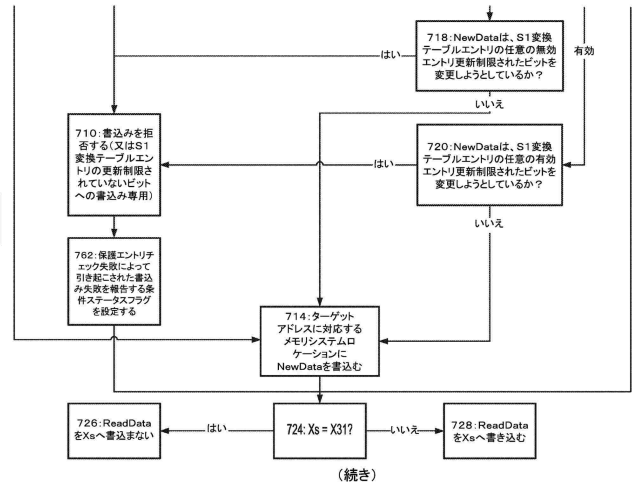
40

50

【図 13-1】

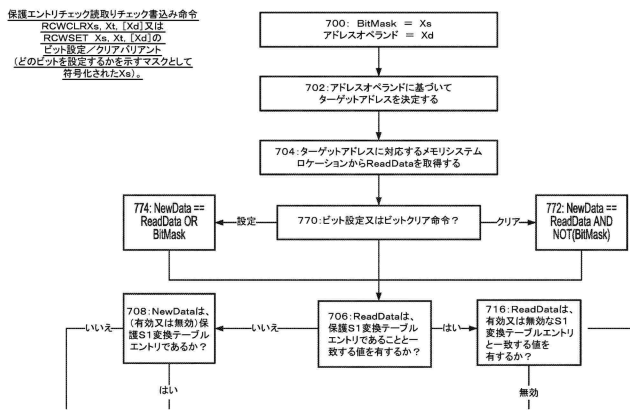


【図 13-2】

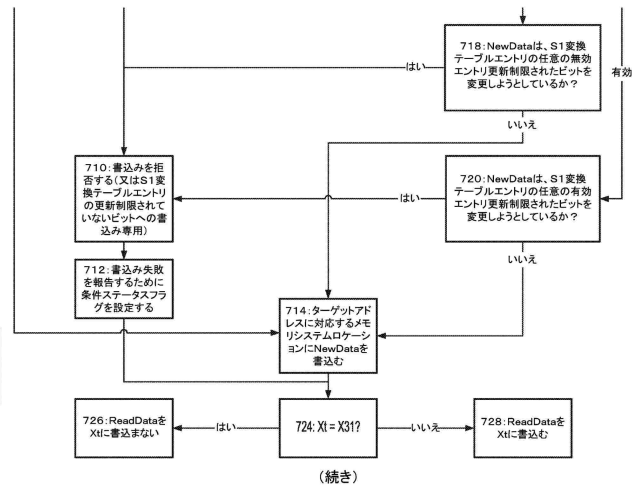


10

【図 14-1】



【図 14-2】



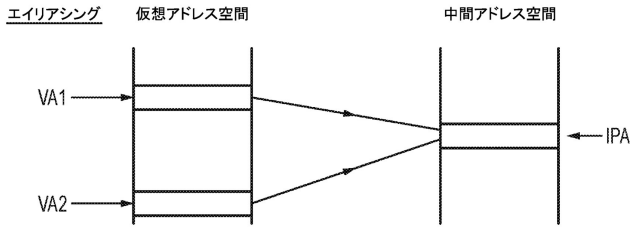
20

30

40

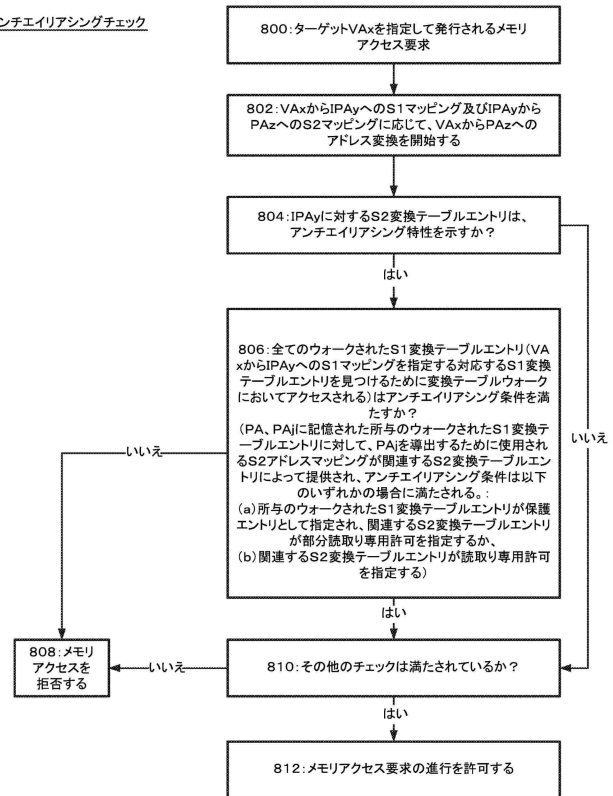
50

【図 15】



【図 16】

アンチエイリアシングチェック

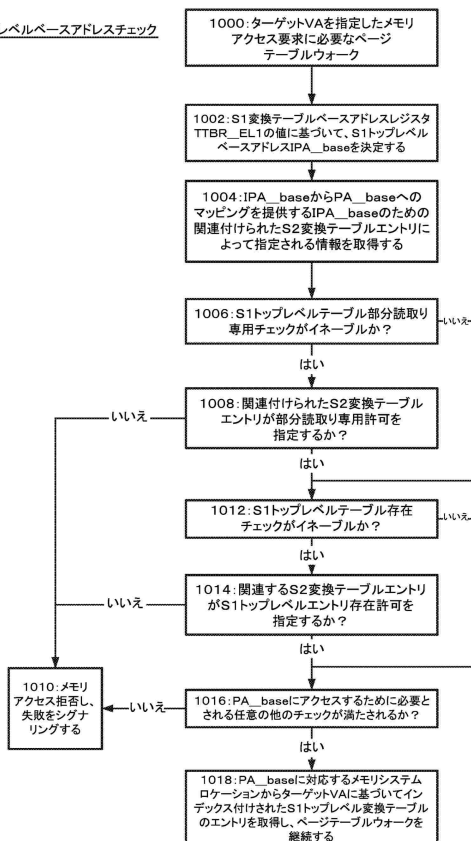


10

20

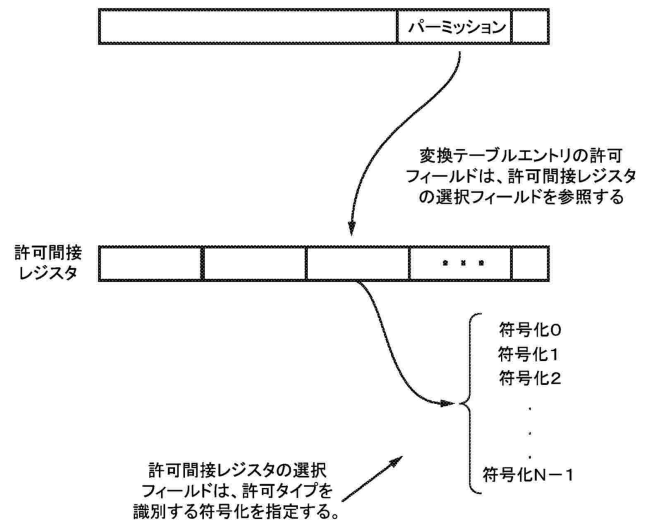
【図 17】

S1トップレベルベースアドレスチェック



【図 18】

S1/S2変換テーブルエントリ

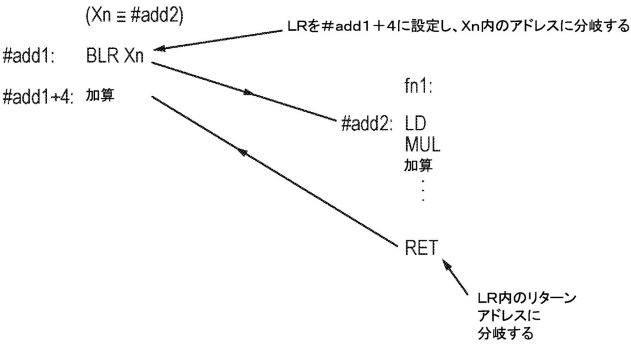


30

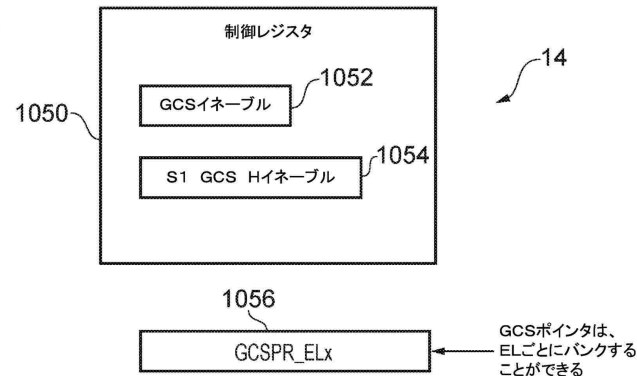
40

50

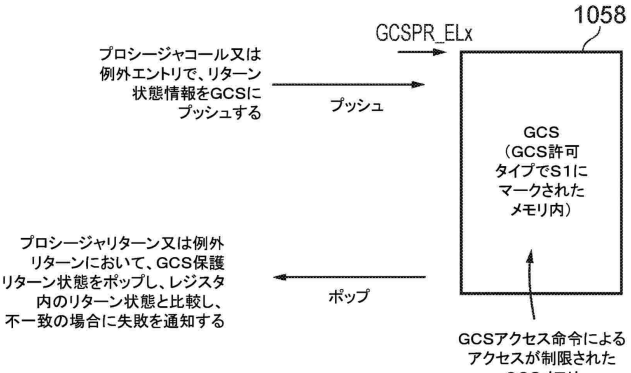
【図 19】



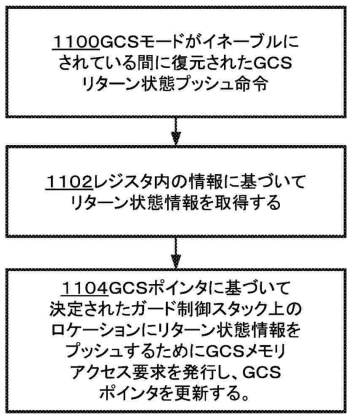
【図 20】



【図 21】



【図 22】



10

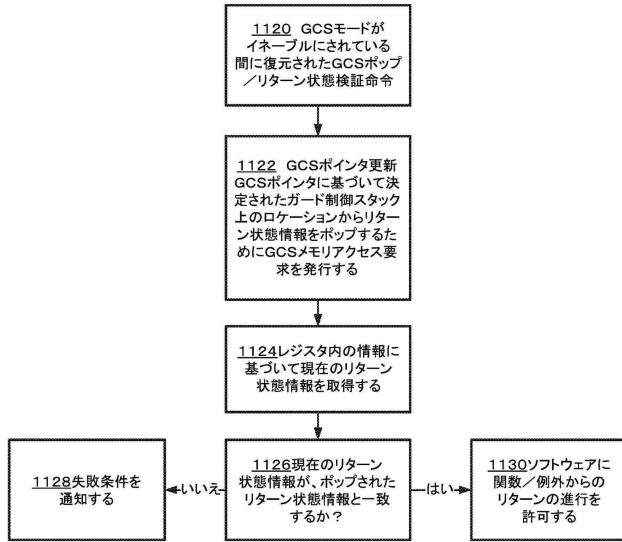
20

30

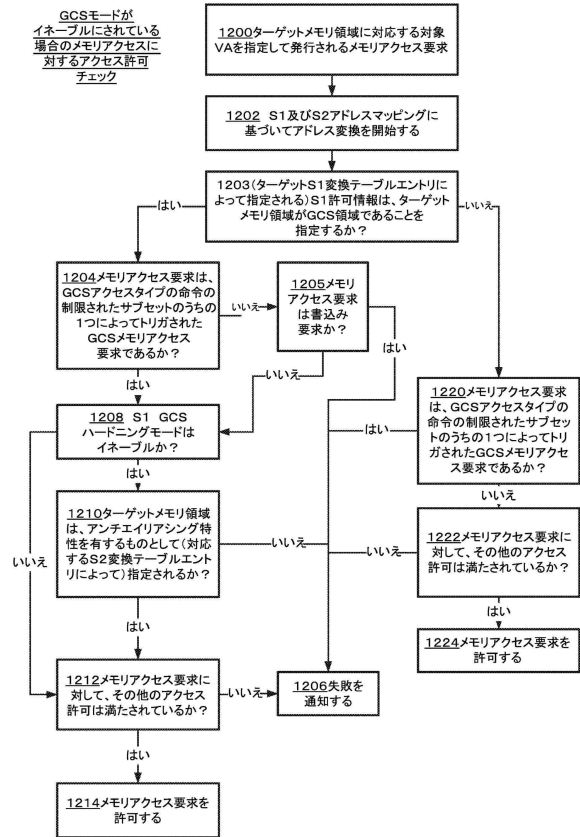
40

50

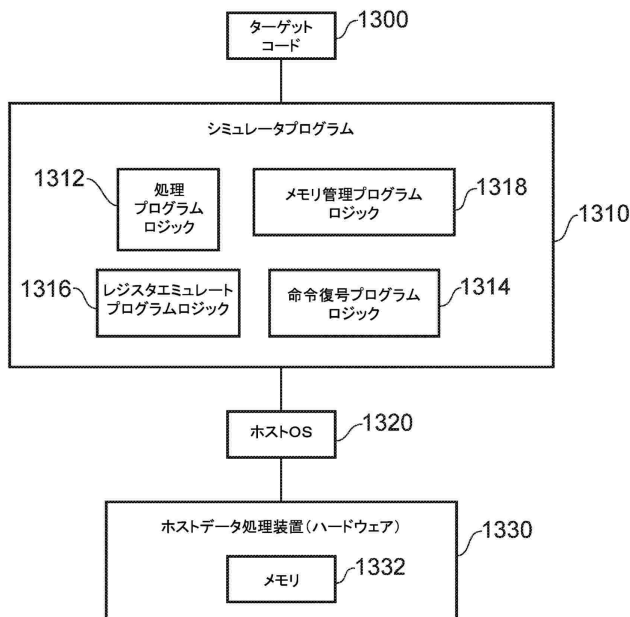
【図 2 3】



【図 2 4】



【図 2 5】



10

20

30

40

50

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2023/050658

A. CLASSIFICATION OF SUBJECT MATTER INV. G06F12/1009 G06F12/14 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017/344492 A1 (BOLBENES GUILLAUME [FR] ET AL) 30 November 2017 (2017-11-30) paragraph [0021] - paragraph [0033] -----	1-19
A	US 2010/088705 A1 (ATTINELLA JOHN E [US] ET AL) 8 April 2010 (2010-04-08) paragraph [0024] - paragraph [0031] -----	1-19
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 14 June 2023		Date of mailing of the international search report 22/06/2023
Name and mailing address of the ISA/ European Patent Office, P.B. 5618 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Toader, Elena Lidia

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT				International application No PCT/GB2023/050658	
Information on patent family members					
Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 2017344492 A1		30-11-2017	GB 2550859 A US 2017344492 A1		06-12-2017 30-11-2017
US 2010088705 A1		08-04-2010	NONE		

10

20

30

40

50

フロントページの続き

,MC,ME,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,
ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,C
O,CR,CU,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,I
R,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,MG,MK,MN,MU,MW
,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL
,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

(72)発明者 ホーリー、ジョン マイケル
グレート・ブリテン及び北部アイルランド連合王国 シービー１ ９エヌジェイ ケンブリッジシャ
ー ケンブリッジ フルボーン ロード １１０ アーム リミテッド宛

【要約の続き】

C S メモリアクセス要求は拒否される。