(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2018-523876
(P2018-523876A)
(43)公表日　平成30年8月23日(2018.8.23)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 12/14	(2006.01)	G06F	12/14	510D	5B017

審査請求 未請求　予備審査請求 有　（全 43 頁）

(21)出願番号	特願2018-505701 (P2018-505701)
(86)(22)出願日	平成28年7月25日 (2016.7.25)
(85)翻訳文提出日	平成30年2月2日 (2018.2.2)
(86)国際出願番号	PCT/US2016/043903
(87)国際公開番号	WO2017/027196
(87)国際公開日	平成29年2月16日 (2017.2.16)
(31)優先権主張番号	14/821,174
(32)優先日	平成27年8月7日 (2015.8.7)
(33)優先権主張国	米国 (US)

(71)出願人　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　コリン・クリストファー・シャープ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】グラフィックス処理ユニットのためのハードウェア強制コンテンツ保護

(57)【要約】
本開示は、グラフィックス処理のための技法を提案する。一例では、グラフィックス処理ユニット(GPU)が、非セキュアモードおよびセキュアモードのうちの1つに従って、メモリにアクセスするように構成される。GPUは、非セキュアモードまたはセキュアモードと、メモリリソースに関連付けられたリソース記述子とに基づいて、GPUの少なくとも1つのハードウェアユニットからのメモリトランザクションを非セキュアメモリユニットまたはセキュアメモリユニットに向けるように構成されるメモリアクセスコントローラを含んでもよい。

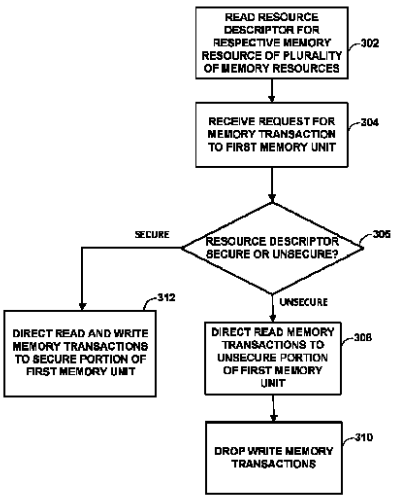


FIG. 11

【特許請求の範囲】
【請求項１】
グラフィックス処理のための装置であって、
非セキュアモードおよびセキュアモードのうちの1つと、複数のメモリリソースの各々に関連付けられたそれぞれのリソース記述子とに従って、第1のメモリユニットにアクセスするように構成されるグラフィックス処理ユニット(GPU)を備え、前記GPUは、
前記複数のメモリリソースの各々に関連付けられた前記それぞれのリソース記述子を読み取るように構成されるメモリアクセスコントローラを備え、
前記メモリアクセスコントローラは、前記第1のメモリユニットへのメモリトランザクションについての要求を受信するように構成され、
前記メモリアクセスコントローラは、前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子がセキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するすべてのメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットのセキュア部分に向けるように構成され、
前記メモリアクセスコントローラは、前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するすべてのメモリ読取りトランザクションを前記第1のメモリユニットの非セキュア部分に向けるように構成され、
前記メモリアクセスコントローラは、前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するすべてのメモリ書込みトランザクションを取り下げるように構成される、
装置。
【請求項２】
前記メモリアクセスコントローラは、前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットの非セキュア部分に向けるようにさらに構成され、
前記メモリアクセスコントローラは、前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを取り下げるようにさらに構成される、
請求項1に記載の装置。
【請求項３】
前記メモリアクセスコントローラは、セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記セキュア部分にデータを書き込むように構成され、前記セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記セキュア部分についてのアドレス範囲を含むセキュアページテーブルを使用し、
前記メモリアクセスコントローラは、非セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記非セキュア部分からデータを読み取るように構成され、前記非セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記非セキュア部分についてのアドレス範囲を含む非セキュアページテーブルを使用する、
請求項1に記載の装置。
【請求項４】
前記メモリアクセスコントローラは、仮想メモリアドレスの範囲からの仮想メモリアドレスに従ってデータを読み取りかつ書き込み、前記仮想メモリアドレスの範囲は、前記セキュアメモリ管理ユニットによって使用される前記セキュアページテーブル中のエントリ

に関する仮想メモリアドレスの第1の範囲、および前記非セキュアメモリ管理ユニットによって使用される前記非セキュアページテーブル中のエントリに関する仮想メモリアドレスの第2の範囲を含む、請求項3に記載の装置。

【請求項５】

グラフィックスドライバを記憶する第2のメモリユニットであって、前記グラフィックスドライバは、前記GPUをセキュアモードまたは非セキュアモードに置くように構成される第2のメモリユニットをさらに備える、請求項4に記載の装置。

【請求項６】

前記セキュアメモリ管理ユニットと、

前記非セキュアメモリ管理ユニットと、

セキュアオペレーティングシステムおよび前記グラフィックスドライバを実行する中央処理ユニット(CPU)であって、前記セキュアオペレーティングシステムは、前記セキュアページテーブルを前記セキュアメモリ管理ユニットに、かつ前記非セキュアページテーブルを前記非セキュアメモリ管理ユニットに供給するように構成される中央処理ユニットと

をさらに備える、請求項5に記載の装置。

【請求項７】

前記GPUはクリアレジスタおよび1つまたは複数の内部メモリをさらに備え、前記セキュアオペレーティングシステムは、前記GPUが前記セキュアモードから前記非セキュアモードに遷移されると、前記GPUに少なくとも何らかのコンテンツを前記1つまたは複数の内部メモリからクリアかつ無効にさせる命令を前記クリアレジスタに送信するように構成される、請求項6に記載の装置。

【請求項８】

前記GPUはコマンドストリームレジスタおよび1つまたは複数の内部メモリをさらに備え、前記グラフィックスドライバは、前記GPUが前記セキュアモードから前記非セキュアモードに遷移されると、前記GPUに少なくとも何らかのコンテンツを前記1つまたは複数の内部メモリからクリアかつ無効にさせる命令を前記コマンドストリームレジスタに送信するように構成される、請求項6に記載の装置。

【請求項９】

前記GPUは、

前記GPUが前記非セキュアモードにあるか、または前記セキュアモードにあるかにかかわらず、前記第1のメモリの前記非セキュア部分にデータを書き込むように構成される1つまたは複数のハードウェアブロックであって、前記1つまたは複数のハードウェアブロックは、前記第1のメモリユニットの前記セキュア部分への読取りアクセスを有さない、ハードウェアブロック

をさらに備える、請求項1に記載の装置。

【請求項１０】

前記1つまたは複数のハードウェアブロックはフロントエンドコマンドプロセッサを含む、請求項9に記載の装置。

【請求項１１】

複数のメモリリソースのそれぞれのメモリリソースについてのそれぞれのリソース記述子を読み取るステップと、

第1のメモリユニットへのメモリトランザクションについての要求を受信するステップと、

前記要求に応答して、グラフィックス処理ユニット(GPU)がセキュアモードに従って動作しているとき、前記それぞれのリソース記述子がセキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットのセキュア部分に向けるステップと、

前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを前記第1のメモリユニ

ットの非セキュア部分に向けるステップと、
前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げるステップと
を含む、方法。
【請求項１２】
前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットの非セキュア部分に向けるステップと、
前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを取り下げるステップと
をさらに含む、請求項11に記載の方法。
【請求項１３】
セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記セキュア部分にデータを書き込むステップであって、前記セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記セキュア部分についてのアドレス範囲を含むセキュアページテーブルを使用する、ステップと、
非セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記非セキュア部分からデータを読み取るステップであって、前記非セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記非セキュア部分についてのアドレス範囲を含む非セキュアページテーブルを使用する、ステップと
をさらに含む、請求項11に記載の方法。
【請求項１４】
仮想メモリアドレスの範囲からの仮想メモリアドレスに従ってデータを読み取りかつ書き込むステップであって、前記仮想メモリアドレスの範囲は、前記セキュアメモリ管理ユニットによって使用される前記セキュアページテーブル中のエントリに関する仮想メモリアドレスの第1の範囲、および前記非セキュアメモリ管理ユニットによって使用される前記非セキュアページテーブル中のエントリに関する仮想メモリアドレスの第2の範囲を含む、ステップ
をさらに含む、請求項13に記載の方法。
【請求項１５】
前記GPUをセキュアモードまたは非セキュアモードに置くステップをさらに含む、請求項14に記載の方法。
【請求項１６】
前記セキュアページテーブルを前記セキュアメモリ管理ユニットに、および前記非セキュアページテーブルを前記非セキュアメモリ管理ユニットに供給するステップ
をさらに含む、請求項15に記載の方法。
【請求項１７】
前記GPUのクリアレジスタに命令を送信するステップと、
前記命令に応答して、前記GPUが前記セキュアモードから前記非セキュアモードに遷移されると、少なくとも何らかのコンテンツを前記1つまたは複数の内部メモリからクリアかつ無効にするステップと
をさらに含む、請求項16に記載の方法。
【請求項１８】
前記GPUのコマンドストリームレジスタに命令を送信するステップと、
前記命令に応答して、前記GPUが前記セキュアモードから前記非セキュアモードに遷移

されると、少なくとも何らかのコンテンツを前記1つまたは複数の内部メモリからクリアかつ無効にするステップと
をさらに含む、請求項16に記載の方法。
【請求項１９】
前記GPUが前記非セキュアモードにあるか、または前記セキュアモードにあるかにかかわらず、前記GPUの1つまたは複数のハードウェアブロックから、前記第1のメモリの前記非セキュア部分にデータを書き込むステップであって、前記1つまたは複数のハードウェアブロックは、前記第1のメモリユニットの前記セキュア部分への読取りアクセスを有さない、ステップ
をさらに含む、請求項11に記載の方法。
【請求項２０】
前記1つまたは複数のハードウェアブロックはフロントエンドコマンドプロセッサを含む、請求項19に記載の方法。
【請求項２１】
グラフィックス処理のための装置であって、
複数のメモリリソースのそれぞれのメモリリソースについてのそれぞれのリソース記述子を読み取るための手段と、
第1のメモリユニットへのメモリトランザクションについての要求を受信するための手段と、
前記要求に応答して、グラフィックス処理ユニット(GPU)がセキュアモードに従って動作しているとき、前記それぞれのリソース記述子がセキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットのセキュア部分に向けるための手段と、
前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを前記第1のメモリユニットの非セキュア部分に向けるための手段と、
前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げるための手段と
を備える、装置。
【請求項２２】
前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットの非セキュア部分に向けるための手段と、
前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを取り下げるための手段と
をさらに備える、請求項21に記載の装置。
【請求項２３】
セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記セキュア部分にデータを書き込むための手段であって、前記セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記セキュア部分についてのアドレス範囲を含むセキュアページテーブルを使用する、手段と、
非セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記非セキュア部分からデータを読み取るための手段であって、前記非セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記非セキュア部分についてのアドレス範囲を含む非セキュ

アページテーブルを使用する、手段と
をさらに備える、請求項21に記載の装置。
【請求項２４】
仮想メモリアドレスの範囲からの仮想メモリアドレスに従ってデータを読み取りかつ書き込むための手段であって、前記仮想メモリアドレスの範囲は、前記セキュアメモリ管理ユニットによって使用される前記セキュアページテーブル中のエントリに関する仮想メモリアドレスの第1の範囲、および前記非セキュアメモリ管理ユニットによって使用される前記非セキュアページテーブル中のエントリに関する仮想メモリアドレスの第2の範囲を含む、手段
をさらに含む、請求項23に記載の装置。
【請求項２５】
前記GPUをセキュアモードまたは非セキュアモードに置くための手段
をさらに備える、請求項24に記載の装置。
【請求項２６】
命令を記憶するコンピュータ可読記憶媒体であって、前記命令は、実行されると、1つまたは複数のプロセッサに、
複数のメモリリソースのそれぞれのメモリリソースについてのそれぞれのリソース記述子を読み取ることと、
第1のメモリユニットへのメモリトランザクションについての要求を受信することと、
前記要求に応答して、グラフィックス処理ユニット(GPU)がセキュアモードに従って動作しているとき、前記それぞれのリソース記述子がセキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットのセキュア部分に向けることと、
前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを前記第1のメモリユニットの非セキュア部分に向けることと、
前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げることと
を行わせる、コンピュータ可読記憶媒体。
【請求項２７】
前記命令は、前記1つまたは複数のプロセッサに、
前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを、前記第1のメモリユニットの非セキュア部分に向けることと、
前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを取り下げることと
をさらに行わせる、請求項26に記載のコンピュータ可読記憶媒体。
【請求項２８】
前記命令は、前記1つまたは複数のプロセッサに、
セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記セキュア部分にデータを書き込むことであって、前記セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記セキュア部分についてのアドレス範囲を含むセキュアページテーブルを使用する、書き込むことと、
非セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記非セキュア部分からデータを読み取ることであって、前記非セキュアメモリ管理ユニットは、前記第

1のメモリユニットの前記非セキュア部分についてのアドレス範囲を含む非セキュアページテーブルを使用する、読み取ることと
をさらに行わせる、請求項26に記載のコンピュータ可読記憶媒体。
【請求項２９】
前記命令は、前記1つまたは複数のプロセッサに、
仮想メモリアドレスの範囲からの仮想メモリアドレスに従ってデータを読み取りかつ書き込むことであって、前記仮想メモリアドレスの範囲は、前記セキュアメモリ管理ユニットによって使用される前記セキュアページテーブル中のエントリに関する仮想メモリアドレスの第1の範囲、および前記非セキュアメモリ管理ユニットによって使用される前記非セキュアページテーブル中のエントリに関する仮想メモリアドレスの第2の範囲を含む、読み取りかつ書き込むこと
をさらに行わせる、請求項28に記載のコンピュータ可読記憶媒体。
【請求項３０】
前記命令は、前記1つまたは複数のプロセッサに、
前記GPUをセキュアモードまたは非セキュアモードにさらに置かせる、請求項29に記載のコンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、グラフィックス処理のための技法に関し、より詳細には、コンテンツ保護のための技法に関する。
【背景技術】
【０００２】
オープンプラットフォーム(たとえば、Androidまたは他のオープンソースプラットフォーム)およびクローズドプラットフォーム(たとえば、Microsoft Windows(登録商標))を含む現代のオペレーティングシステムは通常、そのようなオープンプラットフォームへストリーミングされるか、またはそのようなオープンプラットフォームによって処理されるセキュアコンテンツの保護に関して信頼されない。現代のオペレーティングシステムは、ユーザとカーネルモードの分離により一定のレベルのセキュリティを提供するが、最終的には、カーネルモードの構成要素が、クローズドプラットフォームと、特にオープンプラットフォームの両方において、強力な信頼レベルを提供しない。カーネルモードドライバは容易にインストールすることができ、悪意のあるカーネルモードドライバは当然ながら、セキュリティ境界をバイパスする。そのようなオープンプラットフォームにおけるカーネルモードハードウェアドライバは、セキュアコンテンツを処理する場合があるハードウェア(たとえば、グラフィックス処理ユニット(GPU))の動作を制御するのに使用される。ただし、そのようなドライバはしばしば、オープンソースであり、かつ/または保護コンテンツに関して「セキュア」であるとはみなされないので、サードパーティによる変更を比較的受けやすい。そのような変更により、そのようなドライバによって制御されるハードウェアを通してストリーミングされるか、またはハードウェアによって処理される保護コンテンツ(たとえば、デジタル著作権が管理された(DRM)コンテンツ)が、非セキュアメモリに記憶され、かつコピーされる場合がある。したがって、オープンプラットフォーム上でのセキュアコンテンツの制御はしばしば困難である。
【発明の概要】
【課題を解決するための手段】
【０００３】
概して、本開示はグラフィックス処理ユニット(GPU)のためのハードウェア強制コンテンツ保護のための技法について記載する。ハードウェアプラットフォーム上でセキュアコンテンツを制御するために、セキュアメモリへのアクセスは、GPUなどのハードウェアによって制御される場合がある。
【０００４】

本開示の一例では、グラフィックス処理のための装置が、非セキュアモードおよびセキュアモードのうちの1つに従ってメモリにアクセスするように構成されるGPUを備え、GPUは、GPUがセキュアモードで動作しているとき、GPUの少なくとも1つのハードウェアユニットからのメモリトランザクションをメモリコントローラ中のセキュアコンテキストバンクに向けるように構成され、GPUが非セキュアモードで動作しているとき、GPUの少なくとも1つのハードウェアユニットからのメモリトランザクションをメモリコントローラ中の非セキュアコンテキストバンクに向けるように構成されるメモリアクセスコントローラを備える。

【０００５】

本開示の別の例では、GPUが、非セキュアモードおよびセキュアモードのうちの1つに従って、GPUのメモリにアクセスするように構成される1つまたは複数のハードウェアユニットと、GPUがセキュアモードで動作しているとき、GPUの1つまたは複数のハードウェアユニットのうちの少なくとも1つからのメモリトランザクションをメモリコントローラ中のセキュアコンテキストバンクに向けるように構成され、GPUが非セキュアモードで動作しているとき、GPUの1つまたは複数のハードウェアユニットのうちの少なくとも1つからのメモリトランザクションをメモリコントローラ中の非セキュアコンテキストバンクに向けるように構成されるメモリアクセスコントローラとを備える。

【０００６】

本開示の別の例では、グラフィックス処理のための方法が、GPUの少なくとも1つのハードウェアユニットからのメモリトランザクションをメモリコントローラ中の非セキュアコンテキストバンクに向けることによって、非セキュアモードに従って、GPUを用いてメモリの非セキュア部分にアクセスするステップと、GPUの少なくとも1つのハードウェアユニットからのメモリトランザクションをメモリコントローラ中のセキュアコンテキストバンクに向けることによって、セキュアモードに従って、GPUを用いて、メモリのセキュア部分にアクセスするステップとを備える。

【０００７】

本開示の別の例では、グラフィックス処理のための装置が、GPUの少なくとも1つのハードウェアユニットからのメモリトランザクションをメモリコントローラ中の非セキュアコンテキストバンクに向けることによって、非セキュアモードに従って、メモリの非セキュア部分にアクセスするための手段と、GPUの少なくとも1つのハードウェアユニットからのメモリトランザクションをメモリコントローラ中のセキュアコンテキストバンクに向けることによって、セキュアモードに従ってメモリのセキュア部分にアクセスするための手段とを備える。

【０００８】

本開示の別の例では、グラフィックス処理のための装置が、非セキュアモードおよびセキュアモードのうちの1つと、複数のメモリリソースの各々に関連付けられたそれぞれのリソース記述子とに従って、第1のメモリユニットにアクセスするように構成されるGPUを備え、GPUは、複数のメモリリソースの各々に関連付けられたそれぞれのリソース記述子を読み取るように構成されるメモリアクセスコントローラと、第1のメモリユニットへのメモリトランザクションについての要求を受信するように構成されるメモリアクセスコントローラと、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子がセキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するすべてのメモリ読取りおよび書込みトランザクションを第1のメモリユニットのセキュア部分に向けるように構成されるメモリアクセスコントローラと、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するすべてのメモリ読取りトランザクションを、第1のメモリユニットの非セキュア部分に向けるように構成されるメモリアクセスコントローラと、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するすべてのメモリ書込

みトランザクションを取り下げるように構成されるメモリアクセスコントローラとを備える。

【０００９】

本開示の別の例では、本方法は、複数のメモリリソースのそれぞれのメモリリソースについてのそれぞれのリソース記述子を読み取るステップと、第1のメモリユニットへのメモリトランザクションについての要求を受信するステップと、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子がセキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを第1のメモリユニットのセキュア部分に向けるステップと、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを第1のメモリユニットの非セキュア部分に向けるステップと、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げるステップとを含む。

【００１０】

本開示の別の例では、グラフィックス処理のための装置が、複数のメモリリソースのそれぞれのメモリリソースについてのそれぞれのリソース記述子を読み取るための手段と、第1のメモリユニットへのメモリトランザクションについての要求を受信するための手段と、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子がセキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを第1のメモリユニットのセキュア部分に向けるための手段と、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを第1のメモリユニットの非セキュア部分に向けるための手段と、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げるための手段とを備える。

【００１１】

別の例では、本開示は、命令を記憶するコンピュータ可読記憶媒体について記載し、命令は、実行されると、1つまたは複数のプロセッサに、複数のメモリリソースのそれぞれのメモリリソースについてのそれぞれのリソース記述子を読み取らせ、第1のメモリユニットへのメモリトランザクションについての要求を受信させ、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子がセキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを第1のメモリユニットのセキュア部分に向けさせ、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを第1のメモリユニットの非セキュア部分に向けさせ、要求に応答して、GPUがセキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げさせる。

【００１２】

1つまたは複数の例の詳細が、添付図面および以下の説明に記載される。他の特徴、目的、および利点は、説明および図面から、ならびに特許請求の範囲から明らかになろう。

【図面の簡単な説明】

【００１３】

【図１】本開示の技法を使用するように構成される例示的なコンピューティングデバイスを示すブロック図である。

【図２】図1のシステムメモリの例示的物理ページを示す概念図である。
【図３】本開示の技法を使用するように構成される例示的な処理ユニットを示すブロック図である。
【図４】本開示のハードウェア強制コンテンツ保護技法を実施するように構成される例示的な構造を示すブロック図である。
【図５】本開示のハードウェア強制コンテンツ保護技法を実施するように構成される別の例示的な構造を示すブロック図である。
【図６】本開示のハードウェア強制コンテンツ保護技法を実施するように構成される別の例示的な構造を示すブロック図である。
【図７Ａ】本開示のハードウェア強制コンテンツ保護技法を実施するように構成される別の例示的な構造を示すブロック図である。
【図７Ｂ】本開示のハードウェア強制コンテンツ保護技法を実施するように構成される別の例示的な構造を示すブロック図である。
【図８】本開示の一例によるキャッシュクリアリング技法を示すブロック図である。
【図９】本開示の別の例によるキャッシュクリアリング技法を示すブロック図である。
【図１０】本開示の一例による方法を示すフローチャートである。
【図１１】本開示の別の例による別の例示的方法を示すフローチャートである。
【発明を実施するための形態】
【００１４】
本開示は、グラフィックス処理のための技法に関し、より詳細には、グラフィックス処理ユニット(GPU)向けのハードウェア強制コンテンツ保護のための技法に関する。
【００１５】
オープンプラットフォーム(たとえば、Androidまたは他のオープンソースプラットフォーム)およびクローズドプラットフォーム(たとえば、Microsoft Windows(登録商標))を含む現代のオペレーティングシステムは通常、そのようなオープンプラットフォームへストリーミングされるか、またはそのようなオープンプラットフォームによって処理されるセキュアコンテンツの保護に関して信頼されない。現代のオペレーティングシステムは、ユーザとカーネルモードの分離により、一定のレベルのセキュリティを提供するが、最終的には、カーネルモードの構成要素が、クローズドプラットフォームと、特にオープンプラットフォームの両方において、強力な信頼レベルを提供しない。カーネルモードドライバは容易にインストールすることができ、悪意のあるカーネルモードドライバは当然ながら、セキュリティ境界をバイパスする。そのようなオープンプラットフォームにおけるカーネルモードハードウェアドライバは、セキュアコンテンツを処理する場合があるハードウェア(たとえば、グラフィックス処理ユニット(GPU))の動作を制御するのに使用される。ただし、そのようなドライバはしばしば、オープンソースであり、かつ/または保護コンテンツに関して「セキュア」であるとはみなされないので、サードパーティによる変更を比較的受けやすい。そのような変更により、そのようなドライバによって制御されるハードウェアを通してストリーミングされるか、またはハードウェアによって処理される保護コンテンツ(たとえば、デジタル著作権が管理された(DRM)コンテンツ)が、非セキュアメモリに記憶され、かつコピーされる場合がある。したがって、オープンプラットフォーム上でのセキュアコンテンツの制御はしばしば困難である。この問題に対処するために、本開示は、セキュアメモリへのアクセスがハードウェア自体によって(たとえば、GPUによって)制御される方法および装置を提案する。
【００１６】
セキュアまたは非セキュアメモリへのハードウェアアクセスをドライバコードを通して直接制御するのではなく、本開示は、一例では、GPUをセキュアモードまたは非セキュアモードのいずれかに置くためだけに、グラフィックスドライバ(たとえば、オープンソース非セキュアドライバ)を使用することを提案する。セキュアモードに置かれると、GPU構成要素は、GPUによるセキュアおよび非セキュアメモリへの読取りおよび/または書込みアクセスが、GPUのモード(すなわち、セキュアまたは非セキュアモード)に基づいて制限さ

れる場合があるように構成されてもよい。たとえば、セキュアモードでは、いくつかのGPU構成要素が、セキュアメモリ領域中への書込みを行うことにのみ制限されるように構成されてもよい。これは、信頼できないドライバが、セキュアメモリ領域から非セキュアメモリ領域へメモリコンテンツをコピーするのにGPUを使用することを防止する。セキュアモードにおいてセキュアメモリへのGPUアクセスを制限し、非セキュアモードまたはセキュアモードのうちの1つにGPUを置き、特定のデータリソースをセキュアメモリまたは非セキュアメモリに関連付けるための他の技法について、以下でより詳しく論じる。

【００１７】

本開示の一例では、このセキュアモードにおいて、GPUは、セキュア(たとえば、コピー保護(CP))コンテンツならびに非セキュアコンテンツ(たとえば、セキュアにされていないメモリに記憶されたコンテンツ)の両方を読み取るように構成されてもよい。非セキュアモードにおいて、GPUは、GPU構成要素がセキュアメモリへのあらゆるアクセスを拒否されるように構成されてもよい。このようにして、非セキュアドライバが、GPUを非セキュアモードに置くように変更された場合であっても、GPU自体は、セキュアメモリからどのデータを読み取るのも防止されることになる。したがって、セキュアメモリ中のセキュアコンテンツへのアクセスが防止される。

【００１８】

図1は、GPU向けのハードウェア強制コンテンツ保護のための本開示の技法を実装するために使用されてもよい例示的なコンピューティングデバイス2を示すブロック図である。コンピューティングデバイス2は、たとえば、パーソナルコンピュータ、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピュータ、コンピュータワークステーション、ビデオゲームプラットフォームもしくはコンソール、たとえば、セルラー電話もしくは衛星電話などの携帯電話、固定電話、インターネット電話、いわゆるスマートフォン、ポータブルビデオゲームデバイスもしくは携帯情報端末(PDA)などのハンドヘルドデバイス、パーソナル音楽プレーヤ、ビデオプレーヤ、ディスプレイデバイス、テレビジョン、テレビジョンセットトップボックス、サーバ、中間ネットワークデバイス、メインフレームコンピュータ、任意のモバイルデバイス、またはグラフィカルデータを処理および/もしくは表示する任意の他のタイプのデバイスを含んでもよい。

【００１９】

図1の例に示すように、コンピューティングデバイス2は、ユーザ入力インターフェース4、中央処理ユニット(CPU)6、1つまたは複数のメモリコントローラ8、システムメモリ10、グラフィックス処理ユニット(GPU)12、グラフィックスメモリ14、ディスプレイインターフェース16、ディスプレイ18、ならびにバス20および22を含んでもよい。いくつかの例では、グラフィックスメモリ14はGPU12に「オンチップ」であってもよいことに留意されたい。場合によっては、図1に示すすべてのハードウェア要素は、たとえば、システムオンチップ(SoC)設計において、オンチップであってもよい。ユーザ入力インターフェース4、CPU6、メモリコントローラ8、GPU12およびディスプレイインターフェース16は、バス20を使用して互いと通信してもよい。メモリコントローラ8およびシステムメモリ10はまた、バス22を使用して互いと通信してもよい。バス20、22は、第3世代バス(たとえば、HyperTransportバスまたはInfiniBandバス)、第2世代バス(たとえば、アドバンストグラフィックスポートバス、ペリフェラルコンポーネントインターコネクト(PCI)エクスプレスバス、もしくはアドバンストエクステンシブルインターフェース(AXI)バス)または別のタイプのバスもしくはデバイスインターコネクトなどの様々なバス構造のいずれかであってもよい。図1に示す異なる構成要素間のバスおよび通信インターフェースの特定の構成は例にすぎず、同じまたは異なる構成要素を有するコンピューティングデバイスおよび/または他のグラフィックス処理システムの他の構成が本開示の技法を実装するために使用されてもよいことに留意されたい。

【００２０】

CPU6は、コンピューティングデバイス2の動作を制御する汎用または専用プロセッサを備えてもよい。ユーザは、CPU6に1つまたは複数のソフトウェアアプリケーションを実行

させるために、コンピューティングデバイス2に入力を与えてもよい。CPU6上で実行するソフトウェアアプリケーションは、たとえば、オペレーティングシステム、ワードプロセッサアプリケーション、電子メールアプリケーション、スプレッドシートアプリケーション、メディアプレーヤアプリケーション、ビデオゲームアプリケーション、グラフィカルユーザインターフェースアプリケーションまたは別のプログラムを含んでもよい。加えて、CPU6は、GPU12の動作を制御するためのGPUドライバ7を実行してもよい。ユーザは、ユーザ入力インターフェース4を介してコンピューティングデバイス2に結合されるキーボード、マウス、マイクロフォン、タッチパッド、タッチスクリーン、または別の入力デバイスなどの1つまたは複数の入力デバイス(図示せず)を介して、入力をコンピューティングデバイス2に与えてもよい。

【００２１】

CPU6上で実行するソフトウェアアプリケーションは、ディスプレイ18へのグラフィックスデータのレンダリングを引き起こすようCPU6に命令する1つまたは複数のグラフィックスレンダリング命令を含んでもよい。いくつかの例では、ソフトウェア命令は、たとえば、オープングラフィックスライブラリ(OpenGL(登録商標))API、オープングラフィックスライブラリ組込みシステム(OpenGL ES)API、オープンコンピューティング言語(OpenCL(登録商標))、Direct3D API、X3D API、RenderMan API、WebGL API、または任意の他の公的もしくはプロプライエタリ規格グラフィックスAPIなどのグラフィックスアプリケーションプログラミングインターフェース(API)に準拠してもよい。グラフィックスレンダリング命令を処理するために、CPU6は、GPU12にグラフィックスデータのレンダリングの一部または全部を実施させるために、1つまたは複数のグラフィックスレンダリングコマンドをGPU12に(たとえば、GPUドライバ7を通して)発行してもよい。いくつかの例では、レンダリングされるべきグラフィックスデータは、グラフィックスプリミティブ、たとえば、点、線、三角形、四角形、三角形ストリップなどのリストを含んでもよい。

【００２２】

メモリコントローラ8は、システムメモリ10を出入りするデータの転送を容易にする。たとえば、メモリコントローラ8は、メモリ読取りコマンドおよびメモリ書込みコマンドを受け取り、メモリサービスをコンピューティングデバイス2内の構成要素に提供するためにシステムメモリ10に対してそのようなコマンドをサービスしてもよい。メモリコントローラ8は、メモリバス22を介してシステムメモリ10に通信可能に結合される。メモリコントローラ8は、CPU6とシステムメモリ10の両方とは別の処理モジュールであるものとして図1に示されているが、他の例では、メモリコントローラ8の機能性の一部または全部は、CPU6、GPU12およびシステムメモリ10のうちの1つまたはいずれかの上で実装されてもよい。システムメモリ10は、1つまたは複数のメモリユニットを備えてもよい。メモリユニットは、物理的に分割されてもよく(たとえば、別個の物理ディスクもしくはソリッドステートメモリユニット)、またはメモリアドレス範囲によって分割されてもよい。具体的には、システムメモリ10は、「セキュア」メモリユニットおよび「非セキュア」メモリユニットからなる2つ以上のメモリユニットに分割されてもよい。いくつかの例では、セキュアメモリユニットは、そこに記憶されたデータのアクセス、コピー、または解読を防止するのに、暗号化および/または他のデジタル著作権管理(DRM)技法を使用してもよい。

【００２３】

メモリコントローラ8はまた、システムメモリ10へのIOデバイスアクセス(たとえば、GPU)を制御するためのIOMMU(すなわち、入出力MMU)を含む、1つまたは複数のメモリ管理ユニット(MMU)を含んでもよい。メモリ管理ユニットは、仮想メモリシステムを実装してもよい。仮想メモリ空間は、複数の仮想ページに分割されてもよい。これらの仮想ページは連続してもよいが、これらの仮想ページが対応するシステムメモリ10内の物理ページはシステムメモリ10内で連続しなくてもよい。ページは、MMUが管理することが可能であってもよい最小単位と考えられてもよい。

【００２４】

中央処理ユニット(CPU)上で稼動する現代のオペレーティングシステム(OS)は通常、CPU

上で動作する複数のプログラムにメモリを割り振るための仮想メモリ方式を使用する。仮想メモリは、アプリケーションがメモリ(すなわち、仮想メモリ)の1つのセットを参照する必要だけがあるように、コンピュータシステムの物理メモリ(たとえば、RAM、ディスクストレージなど)を仮想化するメモリ管理技法である。仮想メモリは、物理メモリ中のロケーションにマッピングされる、連続するアドレス空間からなる。このようにして、物理メモリのフラグメント化はアプリケーションから「隠され」、アプリケーションは代わりに、仮想メモリの連続するブロックと対話してもよい。仮想メモリ中の連続するブロックは通常、「ページ」に配列される。各ページは、仮想メモリアドレスのある程度の固定長の連続するブロックである。仮想メモリから物理メモリへのマッピングはしばしば、メモリ管理ユニット(MMU)によって扱われる。物理メモリ中のロケーションに現在マッピングされている仮想メモリ空間は、物理メモリに「戻される」とみなされる。

【００２５】

仮想メモリ空間中のロケーションの物理メモリへのマッピングは、トランスレーションルックアサイドバッファ(TLB)を用いて記憶される。TLBは、MMUによって仮想アドレスを物理アドレスに素早く翻訳するのに使用される。TLBは、仮想メモリアドレスを入力として使用し、物理メモリアドレスを出力するコンテンツアドレス可能メモリ(CAM)として実装されてもよい。MMUは次いで、要求されたデータを出力物理メモリアドレスを使って素早く取り出してもよい。

【００２６】

図2は、システムメモリ10の例示的物理ページを示す概念図である。たとえば、図2は、4つのセクション(セクション0～3)を含む仮想ページ42を含むIOMMU40を示す。仮想ページ42は、理解しやすいように図2に示されている仮想構成物であることを理解されたい。図2において、システムメモリ10は、仮想ページ42に対応する物理ペーhジ44を含んでもよい。

【００２７】

物理ページ44は、システムメモリ10の複数のメモリユニットにわたって記憶されてもよい。たとえば、物理ページ44は、メモリユニット11Aとメモリユニット11Nの両方を包含してもよい。一例では、メモリユニット11Aは「セキュア」メモリユニットであり、メモリユニット11Nは「非セキュア」メモリユニットである。メモリユニット11Aは、部分44Aとして示される物理ページ44の一部分を記憶してもよく、メモリユニット11Nは、部分44Bとして示される物理ページ44の一部分を記憶してもよい。図示されているように、メモリユニット11Aは、物理ページ44のセクション0およびセクション2を記憶し、メモリユニット11Nは、物理ページ44のセクション1およびセクション3を記憶する。

【００２８】

図2の例は、説明のために2つのメモリユニットのみを含むが、任意の数のメモリユニットが使用されてもよい。たとえば、再び図1を参照すると、GPUドライバ7は、GPU12にピクセル値またはどの他の計算された値も記憶させる命令を伝送してもよく、ピクセル値が記憶されるところについての仮想アドレスを伝送してもよい。GPU12は、仮想アドレスに従ってピクセル値を記憶するようにIOMMU40に要求してもよい。IOMMU40は、仮想アドレスを物理アドレスにマッピングし、その物理アドレスに基づいて、インターリービング様式でシステムメモリ10のページ中にピクセル値を記憶してもよい。

【００２９】

図1に戻ると、システムメモリ10は、CPU6による実行のためにアクセス可能なプログラムモジュールおよび/もしくは命令ならびに/またはCPU6上で実行するプログラムが使用するためのデータを記憶してもよい。たとえば、システムメモリ10は、ディスプレイ18上にグラフィカルユーザインターフェース(GUI)を提示するためにCPU6によって使用されるウィンドウマネージャアプリケーションを記憶してもよい。加えて、システムメモリ10は、ユーザアプリケーションと、アプリケーションに関連付けられたアプリケーションサーフェスデータとを記憶してもよい。システムメモリ10は加えて、コンピューティングデバイス2の他の構成要素が使用するための、および/またはそれらの構成要素によって生成され

る情報を記憶してもよい。たとえば、システムメモリ10は、GPU12用のデバイスメモリとして働いてもよく、GPU12による操作を受けるべきデータならびにGPU12によって実施された動作から生じたデータを記憶してもよい。たとえば、システムメモリ10は、DRM保護ゲームコンテンツまたはGPU12によって生じた復号ビデオを記憶してもよい。この状況において、そのようなDRM保護コンテンツは好ましくは、システムメモリ10のセキュアメモリユニット中に記憶される。他の例として、システムメモリ10は、テクスチャバッファ、デプスバッファ、ステンシルバッファ、頂点バッファ、フレームバッファなどの任意の組合せなど、他のグラフィックスデータを記憶してもよい。システムメモリ10は、たとえば、ランダムアクセスメモリ(RAM)、スタティックRAM(SRAM)、ダイナミックRAM(DRAM)、読取り専用メモリ(ROM)、消去可能プログラマブルROM(EPROM)、電気的消去可能プログラマブルROM(EEPROM)、フラッシュメモリ、磁気データ媒体または光学記憶媒体など、1つまたは複数の揮発性または不揮発性メモリまたはストレージデバイスを含んでもよい。

【００３０】

GPU12は、1つまたは複数のグラフィックスプリミティブをディスプレイ18にレンダリングするためのグラフィックス演算を実施するように構成されてもよい。したがって、CPU6上で実行するソフトウェアアプリケーションのうちの1つがグラフィックス処理を必要とするとき、CPU6はディスプレイ18にレンダリングするためにグラフィックスコマンドおよびグラフィックスデータをGPU12に与えてもよい。グラフィックスデータは、たとえば、描画コマンド、状態情報、プリミティブ情報、テクスチャ情報などを含んでもよい。GPU12は、いくつかの事例では、CPU6よりも効率的な、複雑なグラフィック関連動作の処理を実現する高度並列構造で構築されてもよい。たとえば、GPU12は、複数の頂点またはピクセル上で並行して動作するように構成される複数の処理要素を含んでもよい。GPU12の高度並列の性質は、いくつかの事例では、CPU6を使用してシーンを直接ディスプレイ18に描画するよりも速く、GPU12がグラフィックス画像(たとえば、GUIならびに2次元(2D)および/または3次元(3D)グラフィックスシーン)をディスプレイ18上で描画することを可能にする場合がある。

【００３１】

GPU12は、いくつかの事例では、コンピューティングデバイス2のマザーボードに統合される場合がある。他の事例では、GPU12は、コンピューティングデバイス2のマザーボード内のポートにインストールされたグラフィックスカード上に存在してもよく、またはそうでなければコンピューティングデバイス2と相互動作するように構成される周辺デバイス内に組み込まれてもよい。GPU12は、1つもしくは複数のマイクロプロセッサ、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)、デジタル信号プロセッサ(DSP)、または他の等価な集積論理回路もしくはディスクリート論理回路などの1つまたは複数のプロセッサを含んでもよい。

【００３２】

GPU12は、グラフィックスメモリ14に直接結合されてもよい。したがって、GPU12は、バス20を使用することなしに、グラフィックスメモリ14からデータを読み取り、グラフィックスメモリ14にデータを書き込んでもよい。言い換えれば、GPU12は、他の、より遅いシステムメモリを使用する代わりに、ローカルストレージを使ってデータをローカルに処理してもよい。このことは、GPU12が重いバストラフィックを経る場合がある、システムバス20を介してGPU12がデータを読み書きする必要をなくすことによって、より効率的に動作することを可能にする。しかしながら、いくつかの事例では、GPU12は別個のメモリを含まないが、代わりにバス20を介してシステムメモリ10を利用する場合がある。グラフィックスメモリ14は、たとえば、ランダムアクセスメモリ(RAM)、スタティックRAM(SRAM)、ダイナミックRAM(DRAM)、消去可能プログラマブルROM(EPROM)、電気的消去可能プログラマブルROM(EEPROM)、フラッシュメモリ、磁気データ媒体または光学記憶媒体など、1つまたは複数の揮発性または不揮発性メモリまたはストレージデバイスを含んでもよい。

【００３３】

CPU6および/またはGPU12は、レンダリングされた画像データをフレームバッファ15に記

憶してもよい。通常、フレームバッファ15は、システムメモリ10内で割り振られることになるが、いくつかの状況では独立メモリであってもよい。ディスプレイインターフェース16は、フレームバッファ15からデータを取り出し、レンダリングされた画像データによって表される画像を表示するようにディスプレイ18を構成してもよい。いくつかの例では、ディスプレイインターフェース16は、フレームバッファから取り出されたデジタル値をディスプレイ18が消費できるアナログ信号にコンバートするように構成されるデジタルアナログコンバータ(DAC)を含んでもよい。他の例では、ディスプレイインターフェース16は、処理のためにデジタル値を直接ディスプレイ18に渡してもよい。ディスプレイ18は、モニタ、テレビジョン、投影デバイス、液晶ディスプレイ(LCD)、プラズマディスプレイパネル、有機LED(OLED)ディスプレイなどの発光ダイオード(LED)アレイ、陰極線管(CRT)ディスプレイ、電子ペーパー、表面伝導電子放出ディスプレイ(SED)、レーザーテレビジョンディスプレイ、ナノ結晶ディスプレイまたは別のタイプのディスプレイユニットを含んでもよい。ディスプレイ18は、コンピューティングデバイス2内に統合されてもよい。たとえば、ディスプレイ18は、携帯電話またはタブレットコンピュータのスクリーンであってもよい。代替的に、ディスプレイ18は、ワイヤードまたはワイヤレス通信リンクを介してコンピューティングデバイス2に結合されるスタンドアロンデバイスであってもよい。たとえば、ディスプレイ18は、ケーブルまたはワイヤレスリンクを介してパーソナルコンピュータに接続されるコンピュータモニタまたはフラットパネルディスプレイであってもよい。

【００３４】

図3は、図1のCPU6、GPU12、およびシステムメモリ10の例示的な実装形態をさらに詳細に示すブロック図である。CPU6は、少なくとも1つのソフトウェアアプリケーション24、グラフィックスAPI26、およびGPUドライバ7を含んでもよく、これらの各々は、CPU6上で実行する1つまたは複数のソフトウェアアプリケーションまたはサービスであってもよい。GPU12は、グラフィックス処理コマンドを実行するために一緒に動作する複数のグラフィックス処理ステージを含む3Dグラフィックス処理パイプライン30を含んでもよい。GPU12は、ビニングレンダリングモードおよび直接レンダリングモード(タイルベースまたは遅延レンダリングモードとも呼ばれる)を含む様々なレンダリングモードでグラフィックス処理パイプライン30を実行するように構成されてもよい。GPU12はまた、GPUハードウェアの高度並列の性質によって実行されるように適用可能なより一般的な計算を実施するための汎用シェーダ39を実行するように動作可能であってもよい。そのような汎用アプリケーションは、いわゆる汎用グラフィックス処理ユニット(GPGPU)であってもよく、OpenCLなどの汎用APIに準拠する場合がある。

【００３５】

図3に示すように、グラフィックス処理パイプライン30は、コマンドエンジン32、ジオメトリ処理ステージ34、ラスタ化ステージ36、およびピクセル処理パイプライン38を含んでもよい。グラフィックス処理パイプライン30中の構成要素の各々は、固定機能構成要素、(たとえば、プログラマブルシェーダユニット上で実行するシェーダプログラムの一部としての)プログラマブル構成要素として、または固定機能構成要素とプログラマブル構成要素の組合せとして実装されてもよい。CPU6およびGPU12が利用可能なメモリは、それ自体がフレームバッファ15を含む場合があるシステムメモリ10を含んでもよい。フレームバッファ15は、レンダリングされた画像データを記憶してもよい。

【００３６】

ソフトウェアアプリケーション24は、GPU12の機能性を利用する任意のアプリケーションであってもよい。たとえば、ソフトウェアアプリケーション24は、GUIアプリケーション、オペレーティングシステム、ポータブルマッピングアプリケーション、エンジニアリングもしくは美術アプリケーション用のコンピュータ支援設計プログラム、ビデオゲームアプリケーション、または2Dもしくは3Dグラフィックスを使用する別のタイプのソフトウェアアプリケーションであってもよい。ソフトウェアアプリケーション24はまた、たとえばGPGPUアプリケーションにおいて、より全般的な計算を実施するのにGPUを使用するアプ

リケーションであってもよい。

【００３７】

ソフトウェアアプリケーション24は、グラフィカルユーザインターフェース(GUI)および/またはグラフィックスシーンをレンダリングするようGPU12に命令する1つまたは複数の描画命令を含んでもよい。たとえば、描画命令は、GPU12によってレンダリングされるべき1つまたは複数のグラフィックスプリミティブのセットを定義する命令を含んでもよい。いくつかの例では、描画命令は、GUIで使用される複数のウィンドウ処理サーフェスの全部または一部をまとめて定義してもよい。追加の例では、描画命令は、アプリケーションによって定義されたモデル空間またはワールド空間内に1つまたは複数のグラフィックスオブジェクトを含むグラフィックスシーンの全部または一部をまとめて定義してもよい。

【００３８】

ソフトウェアアプリケーション24は、1つまたは複数のグラフィックスプリミティブを表示可能なグラフィックス画像にレンダリングするための1つまたは複数のコマンドをGPU12に発行するために、グラフィックスAPI26を介してGPUドライバ7を呼び出す場合がある。たとえば、ソフトウェアアプリケーション24は、プリミティブ定義をGPU12に与えるために、グラフィックスAPI26を介してGPUドライバ7を呼び出す場合がある。いくつかの事例では、プリミティブ定義は、描画プリミティブ、たとえば、三角形、矩形、三角形ファン、三角形ストリップなどのリストの形でGPU12に与えられる場合がある。プリミティブ定義は、レンダリングされるべきプリミティブに関連付けられた1つまたは複数の頂点を指定する頂点仕様を含んでもよい。頂点仕様は、頂点ごとの位置座標と、いくつかの事例では、たとえば、色座標、法線ベクトル、およびテクスチャ座標など、頂点に関連付けられた他の属性とを含んでもよい。プリミティブ定義はまた、プリミティブタイプ情報(たとえば、三角形、矩形、三角形ファン、三角形ストリップなど)、スケーリング情報、回転情報などを含んでもよい。ソフトウェアアプリケーション24によってGPUドライバ7に発行された命令に基づいて、GPUドライバ7は、プリミティブをレンダリングするためにGPU12が実施する1つまたは複数の動作を指定する1つまたは複数のコマンドを公式化する場合がある。GPU12がCPU6からコマンドを受け取ると、グラフィックス処理パイプライン30は、コマンドを復号し、コマンドにおいて指定された動作を実施するようにグラフィックス処理パイプライン30内の1つまたは複数の処理要素を構成する。指定された動作を実施した後、グラフィックス処理パイプライン30は、レンダリングされたデータをディスプレイデバイスに関連付けられたフレームバッファ15に出力する。グラフィックス処理パイプライン30は、ビニングレンダリングモードおよび直接レンダリングモードを含む複数の異なるレンダリングモードのうちの1つで実行するように構成されてもよい。

【００３９】

GPUドライバ7は、1つまたは複数のシェーダプログラムをコンパイルし、コンパイルされたシェーダプログラムをGPU12内に含まれる1つまたは複数のプログラマブルシェーダユニットにダウンロードするようにさらに構成されてもよい。シェーダプログラムは、たとえば、OpenGL Shading Language(GLSL)、High Level Shading Language(HLSL)、C for Graphics(Cg) shading languageなどの高レベルシェーディング言語で書かれる場合がある。コンパイルされたシェーダプログラムは、GPU12内のプログラマブルシェーダユニットの動作を制御する1つまたは複数の命令を含んでもよい。たとえば、シェーダプログラムは、頂点シェーダプログラムおよび/またはピクセルシェーダプログラムを含んでもよい。頂点シェーダプログラムは、プログラマブル頂点シェーダユニットまたはユニファイドシェーダユニットの実行を制御し、1つまたは複数の頂点ごとの動作を指定する命令を含んでもよい。ピクセルシェーダプログラムは、プログラマブルピクセルシェーダユニットまたはユニファイドシェーダユニットの実行を制御するピクセルシェーダプログラムを含み、1つまたは複数のピクセルごとの動作を指定する命令を含んでもよい。本開示のいくつかの例によれば、ピクセルシェーダプログラムはまた、ソースピクセルについてのテクスチャ値を、それらのソースピクセルについての対応する宛先アルファ値に基づいて選択

的に取り出させる命令を含んでもよい。

【００４０】

グラフィックス処理パイプライン30は、グラフィックスドライバ7を介してCPU6から1つまたは複数のグラフィックス処理コマンドを受け取り、表示可能なグラフィックス画像を生成するためのグラフィックス処理コマンドを実行するように構成されてもよい。上記で説明したように、グラフィックス処理パイプライン30は、グラフィックス処理コマンドを実行するために一緒に動作する複数のステージを含む。しかしながら、そのようなステージは必ずしも別個のハードウェアブロックにおいて実装される必要はないことに留意されたい。たとえば、ジオメトリ処理ステージ34およびピクセル処理パイプライン38の部分は、ユニファイドシェーダユニットの一部として実装されてもよい。やはり、グラフィックス処理パイプライン30は、ビニングレンダリングモードおよび直接レンダリングモードを含む複数の異なるレンダリングモードのうちの1つで実行するように構成されてもよい。

【００４１】

コマンドエンジン32は、グラフィックス処理コマンドを受信し、グラフィックス処理コマンドを実践するための様々な動作を実施するようにグラフィックス処理パイプライン30内の残りの処理ステージを構成してもよい。グラフィックス処理コマンドは、たとえば、描画コマンドおよびグラフィックス状態コマンドを含んでもよい。描画コマンドは、1つまたは複数の頂点の位置座標と、いくつかの事例では、たとえば、色座標、法線ベクトル、テクスチャ座標およびかぶり座標など、頂点の各々に関連付けられた他の属性値とを指定する頂点仕様コマンドを含んでもよい。グラフィックス状態コマンドは、プリミティブタイプコマンド、変換コマンド、照明コマンドなどを含んでもよい。プリミティブタイプコマンドは、レンダリングされるべきプリミティブのタイプおよび/またはプリミティブを形成するために頂点がどのように組み合わされるかを指定してもよい。変換コマンドは、頂点に対して実施すべき変換のタイプを指定してもよい。照明コマンドは、グラフィックスシーン内の異なる照明のタイプ、方向および/または配置を指定してもよい。コマンドエンジン32は、ジオメトリ処理ステージ34に、1つまたは複数の受信されたコマンドに関連付けられた頂点および/またはプリミティブに対してジオメトリ処理を実施させる場合がある。

【００４２】

ジオメトリ処理ステージ34は、ラスタ化ステージ36のためのプリミティブデータを生成するために、1つまたは複数の頂点に対して頂点ごとの動作および/またはプリミティブセットアップ動作を実施してもよい。各頂点は、たとえば、位置座標、色値、法線ベクトル、およびテクスチャ座標などの属性のセットに関連付けられてもよい。ジオメトリ処理ステージ34は、様々な頂点ごとの動作に従って、これらの属性のうちの1つまたは複数を修正する。たとえば、ジオメトリ処理ステージ34は、修正された頂点位置座標を生成するために、頂点位置座標に対して1つまたは複数の変換を実施してもよい。ジオメトリ処理ステージ34は、修正された頂点位置座標を生成するために、たとえば、モデリング変換、ビューイング変換、投影変換、モデルビュー(ModelView)変換、モデルビュー投影(ModelViewProjection)変換、ビューポート変換およびデプス範囲スケーリング変換のうちの1つまたは複数を頂点位置座標に適用してもよい。いくつかの事例では、頂点位置座標はモデル空間座標であってもよく、修正された頂点位置座標はスクリーン空間座標であってもよい。スクリーン空間座標は、モデリング変換、ビューイング変換、投影変換およびビューポート変換の適用の後で取得されてもよい。いくつかの事例では、ジオメトリ処理ステージ34はまた、頂点の修正された色座標を生成するために、頂点に対して頂点ごとの照明動作を実施してもよい。ジオメトリ処理ステージ34はまた、たとえば、正規変換、ノーマル正規化動作(normal normalization operations)、ビューボリュームクリッピング、同次除算動作および/またはバックフェースカリング動作を含む他の動作を実施してもよい。

【００４３】

ジオメトリ処理ステージ34は、ラスタ化されるべきプリミティブを定義する1つまたは複数の修正された頂点のセットを含むプリミティブデータ、ならびにプリミティブを形成

するために頂点がどのように組み合わされるかを指定するデータを生成してもよい。修正された頂点の各々は、たとえば、修正された頂点位置座標と、頂点に関連付けられた処理された頂点属性値とを含んでもよい。プリミティブデータはまとめて、グラフィックス処理パイプライン30のさらなるステージによってラスタ化されるべきプリミティブに対応する場合がある。概念的には、各頂点は、プリミティブの2つの辺がぶつかるプリミティブの角に対応する場合がある。ジオメトリ処理ステージ34は、さらなる処理のためにプリミティブデータをラスタ化ステージ36に与えてもよい。

【００４４】

いくつかの例では、ジオメトリ処理ステージ34の全部または一部が、1つまたは複数のシェーダユニット上で実行する1つまたは複数のシェーダプログラムによって実装される場合がある。たとえば、ジオメトリ処理ステージ34は、そのような例では、頂点シェーダ、ジオメトリシェーダまたはそれらの任意の組合せによって実装される場合がある。他の例では、ジオメトリ処理ステージ34は、固定機能ハードウェア処理パイプラインとして、または固定機能ハードウェアと1つもしくは複数のシェーダユニット上で実行する1つもしくは複数のシェーダプログラムの組合せとして実装される場合がある。

【００４５】

ラスタ化ステージ36は、ジオメトリ処理ステージ34から、ラスタ化されるべきプリミティブを表すプリミティブデータを受信し、プリミティブをラスタ化して、ラスタ化されたプリミティブに対応する複数のソースピクセルを生成するように構成される。いくつかの例では、ラスタ化ステージ36は、どのスクリーンピクセルロケーションがラスタ化されるべきプリミティブによってカバーされるかを決定し、プリミティブによってカバーされると決定されたスクリーンピクセルロケーションごとのソースピクセルを生成してもよい。ラスタ化ステージ36は、たとえば、エッジウォーキング(edge-walking)技法、エッジ方程式評価(evaluating edge equations)などの、当業者に知られている技法を使用することによって、どのスクリーンピクセルロケーションがプリミティブによってカバーされるかを決定してもよい。ラスタ化ステージ36は、さらなる処理のために、得られたソースピクセルをピクセル処理パイプライン38に与えてもよい。

【００４６】

ラスタ化ステージ36によって生成されたソースピクセルは、スクリーンピクセルロケーション、たとえば、宛先ピクセルに対応し、1つまたは複数の色属性に関連付けられる場合がある。特定のラスタ化されたプリミティブのために生成されたソースピクセルのすべては、ラスタ化されたプリミティブに関連付けられていると言える。プリミティブによってカバーされるべき、ラスタ化ステージ36によって決定されたピクセルは、概念的には、プリミティブの頂点を表すピクセル、プリミティブの辺を表すピクセル、およびプリミティブの内部を表すピクセルを含んでもよい。

【００４７】

ピクセル処理パイプライン38は、ラスタ化されたプリミティブに関連付けられたソースピクセルを受信し、ソースピクセルに対して1つまたは複数のピクセルごとの動作を実施するように構成される。ピクセル処理パイプライン38によって実施される場合があるピクセルごとの動作は、たとえば、アルファテスト、テクスチャマッピング、色計算、ピクセルシェーディング、ピクセルごとの照明、かぶり処理、ブレンディング、ピクセルオーナーシップテキスト、ソースアルファテスト、ステンシルテスト、デプステスト、シザーテストおよび/またはスティップリング動作を含む。加えて、ピクセル処理パイプライン38は、1つまたは複数のピクセルごとの動作を実施するための1つまたは複数のピクセルシェーダプログラムを実行してもよい。ピクセル処理パイプライン38によって生成された得られたデータは、本明細書では宛先ピクセルデータと呼ばれ、フレームバッファ15に記憶される場合がある。宛先ピクセルデータは、処理されたソースピクセルと同じ表示ロケーションを有する、フレームバッファ15内の宛先ピクセルに関連付けられる場合がある。宛先ピクセルデータは、たとえば、色値、宛先アルファ値、デプス値などのデータを含んでもよい。

【００４８】
フレームバッファ15は、GPU12のための宛先ピクセルを記憶する。各宛先ピクセルは、一意のスクリーンピクセルロケーションに関連付けられる場合がある。いくつかの例では、フレームバッファ15は、宛先ピクセルごとの色成分および宛先アルファ値を記憶してもよい。たとえば、フレームバッファ15はピクセルごとの赤(Red)、緑(Green)、青(Blue)、アルファ(Alpha)(RGBA)成分を記憶してもよく、"RGB"成分は色値に対応し、"A"成分は宛先アルファ値に対応する。ピクセル値はまた、ルーマ成分(Y)ならびに1つまたは複数のクロマ成分(たとえば、UおよびV)で表されてもよい。フレームバッファ15およびシステムメモリ10は別個のメモリユニットであるものとして示されているが、他の例では、フレームバッファ15はシステムメモリ10の一部であってもよい。

【００４９】
汎用シェーダ39は、計算を実施するようにGPU12上で実行可能な、どのアプリケーションであってもよい。通常、そのような計算は、算術論理ユニット(ALU)を含む、GPU処理コアの高度並列構造を利用するタイプである。例示的汎用シェーダ39は、OpenCL APIに準拠してもよい。OpenCLは、アプリケーションが、異種システム(たとえば、CPU、GPU、DSPなど)を含むシステムにおいて複数のプロセッサにわたってアクセスを有することができるようにするAPIである。通常、OpenCLに準拠するアプリケーションにおいて、GPU12は、非グラフィカルコンピューティングを実施するのに使用されることになる。非グラフィカルコンピューティングアプリケーションの例は、特に、物理ベースのシミュレーション、高速フーリエ変換、オーディオ信号処理、デジタル画像処理、ビデオ処理、画像ポストフィルタリング、コンピュテーショナルカメラ、気候研究、天気予報、ニューラルネットワーク、暗号技術、および超並列データクランチングを含み得る。

【００５０】
図4は、本開示のハードウェア強制コンテンツ保護技法を実装するように構成される例示的なデバイスを示すブロック図である。図4の例では、GPU12は、セキュアモードまたは非セキュアモードに従って動作するように構成されてもよい。本開示の一例では、セキュアモードでは、GPU12は、出力データ(たとえば、ゲームデータ、ビデオなど)を非セキュアメモリ56に書き込むことを制限される。そうではなく、セキュアモードでは、GPU12は、セキュアメモリ57に出力データを書き込むことしかできない。セキュアモードにある間、GPU12は、セキュアメモリ57または非セキュアメモリ56のいずれかからデータを読み取ってもよい。非セキュアモードにおいて、この例では、GPU12は、セキュアメモリ57からどのデータを読み取ることも制限される。むしろ、非セキュアモードでは、GPU12は、非セキュアメモリ56からデータを読み取ることしかできない。同様に、非セキュアモードにある間、GPU12は、非セキュアメモリ56にデータを書き込むことしかできない。

【００５１】
非セキュアメモリ56およびセキュアメモリ57は、1つまたは複数の揮発性または不揮発性メモリまたは記憶デバイスを含む、どのタイプのメモリであってもよい。例示的メモリおよび記憶デバイスは、RAM、SRAM、DRAM、ROM、EPROM、EEPROM、フラッシュメモリ、磁気データ媒体または光学記憶媒体を含む。セキュアメモリ57は、非セキュアメモリ56には見られない追加特徴を含む。たとえば、セキュアメモリ57は、そこに記憶されたデータへのアクセス、コピー、または解読を防止するのに、暗号化、認証および/または他のデジタル著作権管理技法を使用してもよい。概して、セキュアメモリ57は、システムメモリ10の一部分であるとみなされてもよく、非セキュアメモリ56は、システムメモリ10の別の部分であるとみなされてもよい。

【００５２】
以下で説明する本開示の1つまたは複数の例によると、GPU12は、メモリアクセスコントローラ53を使って、データがどこから読み取られ、どこに書き込まれるかを制御し、またはそうでなければ影響を与えるように構成されてもよい。メモリアクセスコントローラ53は、GPU12が動作しているモード(すなわち、セキュアモードまたは非セキュアモード)に応答し、モードに基づいて読取り/書込み決定を行う。概して、メモリアクセスコントロ

ーラ53は、GPU12とメモリコントローラ50との間のトランザクションの性質に制約を課すように構成されてもよい。メモリアクセスコントローラ53は、GPU12が現在動作しているモード(すなわち、セキュアモードまたは非セキュアモード)に応答するように構成されてもよく、以下の本開示の例に従って、メモリトランザクションに制約を課してもよい。

【００５３】

本開示の一例では、GPUメモリモード(たとえば、セキュアモードまたは非セキュアモード)は、CPU6上で動作するGPUドライバ7によってセットされる。GPUドライバ7は、GPU12におけるメモリモードを、いくつかの異なるやり方で変えてもよい。一例では、GPUドライバ7は、どのメモリモードを使用するべきか(たとえば、セキュアモードまたは非セキュアモード)をGPU12に対して示す値を、GPU12中のレジスタに直接書き込んでもよい。別の例では、GPU12は、どのメモリモードを使用するべきかを示す特定の値をレジスタに書き込むようGPU12自体に命令する、GPU12によって実行可能な1つまたは複数の命令をコマンドストリーム中に含んでもよい。このようにして、GPUドライバ7は、GPUが動作するメモリモードを選択するだけでもよく、どのデータがどのメモリに書き込まれるべきかを指定する、いかなる直接命令も行わない。したがって、GPUドライバ7が、GPU12を非セキュアモードに置くように変更された場合であっても、メモリアクセスコントローラ53の機能を通して、GPU12は、セキュアメモリ57からのどの読取りアクセスも防止することになり、それは、メモリアクセスコントローラ53は、非セキュアモードでは非セキュアメモリ56から読み取ることだけが可能だからである。同様に、GPUドライバ7が、GPU12をセキュアモードに置くように変更された場合であっても、メモリアクセスコントローラ53の機能を通して、GPU12は、非セキュアメモリ56へのどの書込みアクセスも防止することになり、それは、メモリアクセスコントローラ53は、セキュアモードではセキュアメモリ57に書き込むことだけが可能だからである。したがって、本開示の技法は依然として、GPUドライバ7がGPU12をセキュアモードに置くように変更された場合であっても、非セキュアメモリ56へのデータのコピーを防止する場合がある。

【００５４】

本開示の一例では、メモリアクセスコントローラ53は、それぞれ、セキュアおよび非セキュアメモリ管理ユニット(MMU)ページテーブルを介してセキュアメモリ57および非セキュアメモリ56にアクセスするように構成される。この例では、GPUドライバ7によって、GPU12に仮想アドレス範囲が与えられる。仮想アドレス範囲は、セキュアメモリ用の仮想アドレスの範囲および非セキュアメモリ用の仮想アドレスの範囲を含む。GPUドライバ7によってセキュアモードに置かれているとき、GPU12は、読取りおよび書込みを実施するのに、セキュアメモリ用の仮想アドレスの範囲を使用する。GPU12はまた、セキュアモードにおいて読取りを実施するのに、ただし書込みは実施しないように、非セキュアメモリ用の仮想アドレスの範囲を使用することが可能であり、そうすることによって、セキュアメモリからの、保護データの無許可コピーを防止する。GPUドライバ7によって非セキュアモードに置かれているとき、GPU12は、読取りおよび書込みを実施するのに、非セキュアメモリ用の仮想アドレスの範囲を使用することになる。

【００５５】

一例では、メモリアクセスコントローラ53は、読取りまたは書込み要求中で使用される仮想アドレスが仮想メモリアドレスの非セキュア範囲内にあるか、または仮想アドレスのセキュア範囲内にあるか判断することによって、読取りおよび書込みを適切なメモリユニット(たとえば、セキュアメモリ57または非セキュアメモリ56)にルーティングする。範囲判断に基づいて、メモリアクセスコントローラは、メモリコントローラ50中の非セキュアIOMMU51またはセキュアIOMMU52のうちの1つを使用する。メモリコントローラ50は、システムメモリ10を出入りするデータの転送を容易にするように構成される。いかなるそのようなトランザクションも効果的に扱うために、メモリコントローラ50は、システムメモリ10への、GPU12などのデバイスアクセスを制御するための1つまたは複数のMMUを含んでもよい。非セキュアIOMMU51およびセキュアIOMMU52は、そのクライアントにページの連続閲覧を提供する、仮想化メモリアドレスのためのマッピングを含む。この例では、クライア

ントは、1つまたは複数のリソースをバインドし、またはGPU12に提供する、どのエンティティ(たとえば、GPU12によって実行されるアプリケーションまたはCPU6上で実行するアプリケーション)であってもよい。リソースとは、GPU12が何らかのやり方で使用するための情報のコンテナ(たとえば、メモリまたはバッファ)である。いくつかの例では、リソースは、メモリがどのように使用されるべきかについての情報を提供する記述子を有してもよい。

【００５６】

本開示の一例では、非セキュアIOMMU51は、非セキュアメモリ56中で仮想メモリアドレスを物理メモリアドレスにマッピングするように構成されているIOMMUである。セキュアIOMMU52は、セキュアメモリ57中で仮想メモリアドレスを物理メモリアドレスにマッピングするように構成されているIOMMUである。非セキュアIOMMU51は、非セキュアページテーブルを使って、非セキュアメモリ56へのマッピングを実施する。非セキュアページテーブルは、仮想メモリアドレスの範囲(たとえば、GPUドライバ7によって与えられる範囲)を非セキュアメモリ56中のロケーションにマッピングするページテーブルである。同様に、セキュアIOMMU52は、セキュアページテーブルを使って、セキュアメモリ57へのマッピングを実施する。セキュアページテーブルは、仮想メモリアドレスの範囲(たとえば、GPUドライバ7によって与えられる範囲)をセキュアメモリ57中のロケーションにマッピングするページテーブルである。図4に示すように、非セキュアIOMMU51およびセキュアIOMMU52は、単一のメモリコントローラ50の一部である。メモリコントローラ50は、図1に示すメモリコントローラ8のうちの1つであってもよい。実際、メモリコントローラ50は、セキュアページテーブルを用いて動作しているときはセキュアIOMMUになり、非セキュアページテーブルを用いて動作しているときは非セキュアIOMMUになる。他の例では、非セキュアIOMMU51およびセキュアIOMMU52は、物理的に別個のMMUであってもよい。

【００５７】

本開示の一例では、セキュアおよび非セキュアページテーブルの両方が、CPU6上で実行するセキュアオペレーティングシステム(OS)54によって、セキュアIOMMU52および非セキュアIOMMU51に与えられる。セキュアOSとは、通常の「リッチ」OS(たとえば、Apple iOS、Google Android、Microsoft Windowsなど)とともに動作するOSである。セキュアOSは、セキュアカーネルおよびどのセキュア周辺装置(たとえば、セキュアIOMMU52)も保護し、リッチOS上で稼動するどのコード(たとえば、GPUドライバ7)からも分離するためのセキュリティアプリケーションを提供する。セキュアOSの例が、ARM Holdings製のTrustZoneソフトウェアである。概して、セキュアOSは、グラフィックスドライバなどのソフトウェアを含む、リッチOS上で稼動するソフトウェアよりも変更および攻撃をはるかに受けにくいとみなされる。本開示の技法によると、セキュアOSのみが、仮想メモリアドレス範囲を物理メモリアドレスにマッピングするためのページテーブルを更新することを許可される。したがって、ドライバによって与えられる仮想アドレス範囲を含むグラフィックスドライバを変更するためのどの試みも、セキュアコンテンツが非セキュアメモリに記憶される結果とはならず、それは、セキュアOSのみが、セキュアおよび非セキュアメモリへの最終的マッピングを提供するからである。

【００５８】

セキュアおよび非セキュアページテーブルの両方がメモリコントローラ50において利用可能である(たとえば、メモリコントローラ50が、非セキュアIOMMU51とセキュアIOMMU52の両方を含む)例では、GPU12は、セキュアモードにおいて、非セキュアメモリ56とセキュアメモリ57の両方からデータを読み取ることが可能である。他の読取り/書込み制約が、依然としてあてはまる。つまり、セキュアモードでは、書込みは、GPU12によってセキュアメモリ57に対して行われるだけであり、非セキュアモードでは、GPU12による読取りと書込みの両方が、非セキュアメモリ56に限られる。

【００５９】

本開示の別の例では、データトラフィックが、メモリアクセスコントローラ53を介してセキュアまたは非セキュアIOMMUのいずれかに向けられる場合、セキュアおよび非セキュ

アIOMMUの両方をGPUにとって利用可能にするのではなく、ただ1つのIOMMU(すなわち、非セキュアIOMMU51またはセキュアIOMMU52のいずれか)が、選択されたメモリモードに依存して、GPU12にとって利用可能にされることになる。つまり、メモリモードが非セキュアモードである場合、セキュアOS54は、非セキュアIOMMU51にページテーブルマッピングを提供するだけである。この状況において、セキュアIOMMU52は利用不可能になる。メモリモードがセキュアモードである場合、セキュアOS54は、セキュアIOMMU52にページテーブルマッピングを提供するだけである。この状況において、非セキュアIOMMU51は利用不可能になる。メモリモードごとに1つのIOMMUのみを利用可能にするこの例は、メモリモードごとに読取りと書込みの両方が制限されたより単純な実装形態を提供する。つまり、セキュアモードでは、GPU12による、セキュアメモリ57に対する読取りおよび書込みのみが許可され、非セキュアモードでは、GPU12による、非セキュアメモリ56に対する読取りおよび書込みのみが許可される。これは、セキュアモードが非セキュアメモリ56向けの読取りをそれ以上許可しないという点で、両方のIOMMUが利用可能であってもよい、上述した手法とはわずかに異なる。

【００６０】

セキュアモードにあるときであっても、GPU12の最終出力産物以外の、いくつかの書込みがあり、これらは、GPUが非セキュアメモリに書き込むためにより優れている。これらの書込みは、GPU12とグラフィックスドライバ7との間の通信トークンを含む。そのようなデータは、タイムスタンプと、カウンタデータおよび照会データなど、他の補助データおよび制御データとを含む。GPU12は、そのようなタイムスタンプおよびデータをドライバに通信するのに、メモリ(たとえば、非セキュアメモリ56)を使用する。グラフィックスドライバ7は信頼できないので、通信経路に関わるメモリは、非セキュアである必要がある(たとえば、非セキュアメモリ56)。一例として、GPU12が、処理におけるある特定の地点に達すると、GPU12は、タイムスタンプ/順序マーカをメモリに書き込む。グラフィックスドライバ7は、この情報を、GPUが特定のコマンドストリーム中でどれだけ進んだかを判断するのに使用する。この判断は、たとえば、GPU12が終了すると、グラフィックスドライバ7が、GPU12がその上で動作しているメモリオブジェクトを解放できるようにする。グラフィックスドライバ7に情報を提供するためにGPU12が使ってもよい多くの他のタイプのシグナリングおよび通信経路がある。別の例として、グラフィックスドライバ7は、GPU12に、描画コールの後で実施カウンタを報告するよう要求することができる。GPU12は次いで、これらの実施カウンタを、グラフィックスドライバ7によって指定された(たとえば、非セキュアメモリ56中の)記憶ロケーションに書き込む。

【００６１】

GPU12が、セキュアモードでは非セキュアメモリに書き込まないという、上記の一般規則に対するこの例外を解消するために、GPU12ハードウェアは、いくつかのハードウェアブロックが、GPUがセキュアモードで稼動しているときにセキュアコンテンツに接続するか、またはセキュアコンテンツを含むデータ経路およびキャッシュへのアクセスをやはり有さないまま、非セキュアメモリアクセスを有するように構成されるように修正されてもよい。

【００６２】

図5は、GPU12のいくつかのハードウェアブロックが、GPU12がセキュアモードにあるときであっても、GPU12のメモリインターフェースブロック(VBIF60)を通して、次いで、非セキュアIOMMU51を通して、非セキュアメモリへの直接アクセスのみを有する例示的実装形態を示す。そのようなハードウェアブロックの一例が、GPUのフロントエンドにあるコマンドプロセッサ(CP)62ブロックである。CP62は、図3に示すコマンドエンジン32などのコマンドエンジンを実行してもよい。CP62は、メッセージを(非セキュアメモリを介して)GPUドライバ7に送信することを担当する。図5に示すように、CP62は、非セキュアIOMMU51を通る、メモリ(この場合、非セキュアメモリ)へのただ1つの物理経路を有するように構成される。したがって、GPU12の他の任意のハードウェアブロックがセキュアコンテンツ上で動作しているかどうかにかかわらず、CP62は、そのようなセキュアコンテンツへのア

クセスを得ることはない。CP62がセキュアコンテンツへのアクセスを有さないことをさらに確実にするために、CP62はまた、デバッグバスを含む、セキュアコンテンツを記憶するのに使用される場合があるどのレジスタからも物理的に隔離されてもよい(たとえば、どのレジスタへの接続も有さない)。図5に示すように、CP62は、L2キャッシュ61およびグラフィックスメモリ(GMEM)70への直接アクセスを有さない。GMEM70は、GPU12がGPU12のいくつかの動作モードにおいて表示するためにコンテンツをレンダリングするときにレンダターゲットまたはフレームバッファとして使用する高速メモリ(しばしば、SRAM)である。L2キャッシュ61は、メインメモリ(たとえば、セキュアメモリ)へのアクセスの数が削減されてもよいように、最近アドレス指定されたデータまたは頻繁に使用されるデータを記憶するのに使用される2次キャッシュである。L2キャッシュ61はまた、プログラム命令をバッファリングするのに使用されてもよい。通常、L2キャッシュ61はGMEM70よりも大きい。

【００６３】

GPU12の他のハードウェアブロックはまた、非セキュアメモリへのアクセスのみを有するように構成されてもよい。たとえば、プリミティブ制御(PC)ユニットおよび可視性ストリーム圧縮器(VSC)が、非セキュアメモリへのアクセスのみを有するように構成されてもよい。PCユニットが、プリミティブ(たとえば、三角形)がグラフィックスパイプライン(たとえば、図3のグラフィックス3D処理パイプライン30)を通ってどのように進行し、または「歩く」かを制御する。VSCは、タイルベースまたは遅延レンダリング方式において、可視性ストリームを圧縮し、管理するのに使用される。概して、いくつかの状況では、いくつかのハードウェアブロックに対して、セキュアメモリに書き込むよう求めるのを避けることが有益な場合がある。そのような状況は、ハードウェアブロックがセキュアコンテンツを書き込んでいない状況、およびハードウェアブロックが、グラフィックスドライバによって必要とされる制御データを書き込んでいるときを含む。

【００６４】

図5の他のハードウェアブロックは、上述した技法に基づいて、非セキュアメモリまたはセキュアメモリにコンテンツを記憶する。つまり、非セキュアモードでは、データは、非セキュアメモリから読み取られるか、またはそこに書き込まれるだけであってもよい。どのデータも、非セキュアモードではセキュアメモリから読み取られなくてもよい。セキュアモードでは、データは、セキュアメモリに書き込まれるだけであってもよい。どのデータも、セキュアモードでは非セキュアメモリに書き込まれなくてもよい。ただし、いくつかの例におけるセキュアモードでは、データは、セキュアメモリと非セキュアメモリの両方から読み取られる場合がある。メモリモードに従ってメモリにアクセスしてもよいGPU12のこれらの追加ハードウェアブロックは、頂点フェッチ復号(VFD)ユニット65、高レベルシーケンサ(HLSQ)66、頂点シェーダ(VS)67、ピクセルシェーダ(PS)68、およびレンダバックエンド(RB)69を含む。VFD65は、CP62の要求により、頂点データをフェッチすることを担当する。HLSQ66は、シェーダプロセッサ(すなわち、シェーダコードを実行する、GPU上のプログラム可能プロセッサ)を制御して、実行されるジョブおよび起動ジョブについての正しい状態をシェーダプロセッサに投入する。VS67は、シェーダプロセッサ上で実行する頂点シェーダである。たとえば、VS67は、図3のグラフィックス3D処理パイプライン30のジオメトリ処理ステージ34を実行する頂点シェーダコードを含んでもよい。PS68は、シェーダプロセッサ上で実行するピクセルシェーダである。たとえば、PS68は、図3のグラフィックス3D処理パイプライン30のピクセル処理パイプライン38を実行するピクセルシェーダコードを含んでもよい。レンダバックエンド(RB)69は、デプスバッファおよびステンシルバッファ用のピクセルを書き込み、読み取ることを担当する。

【００６５】

図6は、本開示のハードウェア強制コンテンツ保護技法を実施するように構成される別の例示的な構造を示すブロック図である。図6の例では、GPU12およびメモリコントローラ50は、メモリアクセスコントローラ53の動作を除いて、図5において上述したものと同じである。さらに、簡略化のために、GPU12中に存在する様々なハードウェアユニットが概して、GPUハードウェアブロック71などとして標示されている。GPUハードウェアブロック

71は、VFDユニット65、HLSQ66、VS67、PS68、およびRB69のうちの1つまたは複数を含んでもよい。

【００６６】

図6の例では、メモリアクセスコントローラ53は、GPU12のメモリモード(すなわち、非セキュアモードまたはセキュアモード)と、メモリリソース(たとえば、図6のクライアント73に示すように、データを記憶するバッファまたはキャッシュライン)に関連付けられたリソース記述子とに基づいて、メモリユニット(たとえば、非セキュアメモリ56またはセキュアメモリ57)中にデータを向けるように構成されてもよい。たとえば、「セキュアタグ」と呼ばれるリソース記述子は、リソース向けのデータが、セキュアモードに従って(たとえば、セキュアIOMMU52を通して)ルーティングされるべきであるか、または非セキュアモードに従って(たとえば、非セキュアIOMMU51を通して)ルーティングされるべきであるかを示すように、各リソースに関連付けられてもよい。図6に示すように、リソース記述子は、セキュアIOMMU52を使用する、信頼される"T"リソース、および非セキュアIOMMU51を使用する、信頼できない"U"リソースを示してもよい。

【００６７】

リソース記述子と、GPU12のメモリモードとを使って、メモリアクセスコントローラ53は、リソース記述子に基づいて、GPUハードウェアブロック71からのメモリ読取りおよび書込みを、L2キャッシュ61を通して向けるように構成されてもよい。L2キャッシュ61中の各キャッシュラインは、リソース記述子情報を含んでもよい。一例では、メモリアクセスコントローラ53は、特定のメモリトランザクション(たとえば、読取りまたは書込み)についての、リソース中に存在するセキュアタグ情報を調べ、非セキュアIOMMU51またはセキュアIOMMU52のうちのどちらを、トランザクションをルーティングするのに使用するか判断するように構成されてもよい。

【００６８】

たとえば、GPU12が、セキュアモードで動作するようにセットされると、メモリアクセスコントローラ53は、メモリトランザクションにおけるリソース用のリソース記述子中のセキュアタグ情報を調べてもよい。セキュアタグが、信頼されるリソース"T"を示す場合、メモリアクセスコントローラ53は、そのようなセキュアリソースの読取りと書込みの両方を、セキュアIOMMU52に向ける。いくつかの例では、メモリアクセスコントローラは、Tリソース記述子を有するリソースのすべての読取りおよび書込みを、セキュアIOMMU52に向ける。セキュアタグ情報が、信頼できないリソース"U"を示す場合、メモリアクセスコントローラ53は、そのような非セキュアリソースの(たとえば、一部または全部の)読取りを非セキュアIOMMU51に向けるが、非セキュアリソースの書込みについての要求(たとえば、一部または全部)を取り下げるか、または許可しない。

【００６９】

上記例によると、GPU12は、非セキュアモードおよびセキュアモードのうちの1つと、複数のメモリリソースの各々に関連付けられたそれぞれのリソース記述子とに従って、第1のメモリユニット(たとえば、システムメモリ10)にアクセスするように構成されてもよい。メモリアクセスコントローラ53は、複数のメモリリソースのリソース記述子を読み取り、第1のメモリユニットへのメモリトランザクションについての要求を受信するように構成されてもよい。

【００７０】

メモリアクセスコントローラ53は、要求に応答して、GPU12がセキュアモードに従って動作しているとき、セキュアリソース記述子を有する、複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを、第1のメモリユニットのセキュア部分へ向けるようにさらに構成されてもよい。メモリアクセスコントローラ53は、要求に応答して、GPU12がセキュアモードに従って動作しているとき、非セキュアリソース記述子を有する、複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを、第1のメモリユニットの非セキュア部分へ向けるようにさらに構成されてもよい。メモリアクセスコントローラ53は、要求に応答して、GPUがセキ

ュアモードに従って動作しているとき、非セキュアリソース記述子を有する、複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げるようにさらに構成されてもよい。

【００７１】

本開示の別の例では、メモリアクセスコントローラ53は、要求に応答して、GPUが非セキュアモードに従って動作しているとき、非セキュアリソース記述子を有する、複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを、第1のメモリユニットの非セキュア部分へ向けるようにさらに構成されてもよい。メモリアクセスコントローラ53は、要求に応答して、GPUが非セキュアモードに従って動作しているとき、セキュアリソース記述子を有する、複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを取り下げるようにさらに構成されてもよい。

【００７２】

図7Aおよび図7Bは、本開示のハードウェア強制コンテンツ保護技法を実施するように構成される他の例示的な構造を示すブロック図である。図7Aおよび図7Bの例において、メモリコントローラ100は1つまたは複数のMMUを含んでもよい。上述したように、MMUが、そのクライアントに、ページの連続閲覧を提供する仮想化メモリ方式を実装する。仮想メモリ空間は、仮想ページに分割されてもよい。MMUは、これらの仮想ページテーブルを維持するために、1つまたは複数のコンテキストバンクを実装してもよい。コンテキストバンクは、仮想メモリアドレスを物理メモリアドレスにマッピングするページテーブル(PT)エントリ、ならびに各コンテキストバンク中の特定のPTエントリについて、読取り、書込み、または読取りと書込みの両方が許可されるかを示す規則の両方を含んでもよい。

【００７３】

図7Aおよび図7Bの例において、メモリコントローラ100のMMUは、非セキュアコンテキストバンク102およびセキュアコンテキストバンク105を含んでもよい。非セキュアコンテキストバンク102は、読取り専用アクセスのためにマッピングされた非セキュアPTエントリ104を含んでもよい。非セキュアPTエントリ104は、非セキュアメモリ56における仮想メモリアドレスから物理メモリアドレスへのマッピングを含んでもよい。非セキュアPTエントリ104は読取り専用アクセスのためにマッピングされるので、メモリコントローラ100は、非セキュアコンテキストバンク102を使って、非セキュアメモリ56から読み取ることだけが可能である。セキュアコンテキストバンク105は、読取り専用アクセスのためにマッピングされた非セキュアPTエントリ106と、読取りおよび書込みアクセス(R/W)の両方のためにマッピングされたセキュアPTエントリ108とを含んでもよい。非セキュアPTエントリ106は、非セキュアメモリ56における仮想メモリアドレスから物理メモリアドレスへのマッピングを含んでもよい。セキュアPTエントリ106は、セキュアメモリ57における仮想メモリアドレスから物理メモリアドレスへのマッピングを含んでもよい。

【００７４】

GPU12が、上で論じた技法のうちの1つを使ってセキュアモードに置かれているとき、メモリアクセスコントローラ53は、GPUハードウェアブロック71用のメモリトランザクションをメモリコントローラ100のセキュアコンテキストバンク105に向けるように構成されてもよい。GPU12、またはGPU12を使用するクライアントからの命令が、非セキュアリソース(たとえば、非セキュアメモリ56)中への書込みを実施することを試みる場合、メモリコントローラ100は、ページフォールトを発行するように構成され、それは、非セキュアコンテキストバンク102中のPTエントリは、セキュアコンテキストバンク105において読取り専用としてマッピングされるからである。ページフォールトは、そのようなメモリトランザクションが許可されないことをクライアントに対して示す。

【００７５】

本開示の一例では、CP62は、GPU12のメモリモードにかかわらず、常に非セキュアモードで動作するように構成されてもよい。つまり、CP62は、非セキュアコンテキストバンク102を常に使用するように構成されてもよい。図7Aは、GPU12がセキュアモードにあるとき

の、GPU12から非セキュアコンテキストバンク102およびセキュアコンテキストバンク105へのメモリトランザクションの流れを示す。図7Bは、GPU12が非セキュアモードにあるときの、GPU12から非セキュアコンテキストバンク102およびセキュアコンテキストバンク105へのメモリトランザクションの流れを示す。

【００７６】

繰り返すと、GPU12は、非セキュアモードおよびセキュアモードのうちの1つに従って、メモリ(たとえば、非セキュアメモリ56またはセキュアメモリ57)にアクセスするように構成されてもよい。GPU12は、GPU12がセキュアモードで動作しているとき、GPU12の少なくとも1つのハードウェアユニット(たとえば、GPUハードウェアブロック71のうちの1つまたは複数)から、メモリコントローラ100中のセキュアコンテキストバンク105にメモリトランザクションを向けるように構成されるメモリアクセスコントローラ53を含んでもよい。メモリアクセスコントローラ53はまた、GPU12が非セキュアモードで動作しているとき、GPU12の少なくとも1つのハードウェアユニットからのメモリトランザクションをメモリコントローラ100中の非セキュアコンテキストバンク102に向けるように構成されてもよい。

【００７７】

上述したように、セキュアコンテキストバンク105は、メモリ(たとえば、非セキュアメモリ56)の非セキュア部分への読取り専用ページテーブルエントリ、およびメモリ(たとえば、セキュアメモリ57)のセキュア部分への読取り/書込みページテーブルエントリを含んでもよい。非セキュアコンテキストバンク102は、メモリ(たとえば、非セキュアメモリ56)の非セキュア部分への読取り専用ページテーブルエントリを含んでもよい。一例では、メモリコントローラ100は、セキュアコンテキストバンク105の読取り専用ページテーブルエントリ内に含まれるアドレスにデータを書き込むための要求が受信されたとき、ページフォールトを発行するように構成されてもよい。

【００７８】

上述した例のうちのいずれにおいても、GPU12がセキュアモードから非セキュアモードに遷移したとき、GPU12の様々なキャッシュ、メモリおよびレジスタ内にセキュアコンテンツが残っている場合がある。本開示の一例では、非セキュアメモリモードを使用する非セキュアジョブをGPU12上で起動させる前に、セキュアコンテンツを保持してもよい、GPU12の様々な記憶ユニットをクリアし、かつ/または無効にするための機構が提供される。

【００７９】

このコンテキストにおいて、メモリをクリアすることは、メモリ中に記憶されたデータが消去され、かつ/または上書きされることが許可されることを意味する。実際、クリアリングは、メモリユニット中のすべてのデータが上書きされてもよいように、メモリユニット向けのすべてのメモリアドレスを割振り解除することを伴う場合がある。他の例では、クリアリングは、どの以前記憶されたデータもそれ以上利用可能でないように、メモリユニット中のすべてのデータを(たとえば、すべて1またはすべて0で)上書きすることを伴う場合がある。メモリユニットがクリアされない場合、非セキュアジョブは、セキュアデータの末尾の残りを非セキュアメモリにコピーすることができる。この問題は、セキュアソフトウェア技法、ハードウェア技法、または両方の技法の組合せにより解決することができる。それにもかかわらず、クリアリングおよび非セキュアへの遷移は、この動作が非セキュアドライバによってトリガされるので、アトミック動作である場合がある。このコンテキストにおいて、アトミック動作は、非セキュアモードへの遷移と一緒に(すなわち、自動的に)内部GPU12メモリをクリアリングすることを含む。たとえば、両方を行う(モードを変え、内部メモリをクリアする)単一の「コマンド」がなければならず、そうでない場合、悪意のあるソフトウェアが、非セキュアモードへの遷移だけを実施し、クリアリング動作を実行しない可能性がある。

【００８０】

いくつかの例では、セキュアモードから非セキュアモードに遷移するとき、GPU12のすべての記憶ユニットをクリアする必要がない場合がある。そうではなく、セキュアコンテンツへの無許可アクセスを効果的に防止するために、記憶ユニットの一部分のみがクリア

される必要がある。一例として、記憶されたコンテンツの半分だけがクリアされてもよい。別の例として、1つおきのデータチャンク(たとえば、1つおきの32バイトのデータ)がクリアされてもよい。

【００８１】

図8は、本開示の一例によるキャッシュクリアリング技法を示すブロック図である。図8の例では、セキュアソフトウェアソリューションは、GPUをセキュアおよび非セキュアモードの間で遷移させるのに使用される。一例では、GPUレジスタ(たとえば、クリアレジスタ74)は、ホストCPU6上で稼動するセキュアソフトウェア(たとえば、セキュアOS54)の制御下にある。GPUドライバ7がGPU12のメモリモードを非セキュアモードからセキュアモードに切り替えた場合、GPUドライバ7は、L2キャッシュ61、GMEM70、および他のレジスタ72を含む、GPU12のキャッシュ、メモリまたはレジスタ上に残っているどのセキュアコンテンツもクリアするために、セキュアOS54中のセキュアソフトウェアも呼び出す。その時点で、セキュアOS54は、メモリクリアおよび/または無効化命令をクリアレジスタ74に書き込むことによって、GPU12上のジョブを最初に起動することもできる。そのような命令の結果、GPU12中の残っているセキュアデータすべてがクリアされることになる。そのような命令は、シェーダプログラム、メモリ書込みおよび/またはレジスタプログラミング(たとえば、GPU L2キャッシュ無効化)の組合せであってもよい。

【００８２】

図9は、本開示の別の例によるキャッシュクリアリング技法を示すブロック図である。図9の例では、ハードウェアソリューションは、GPU12をセキュアおよび非セキュアモードの間で遷移させるのに使用される。この例では、外部的に可視的な(たとえば、メモリマップト入出力(MMIO))または内部(たとえば、コマンドストリーム)レジスタ76は、グラフィックスドライバ7によって直接書き込まれるように構成されてもよい。GPU12のハードウェアは、レジスタ76が書き込まれたとき(たとえば、セキュアモードから非セキュアモードに進んだとき)、GPU12のハードウェアが現在のセキュアジョブを完了し、パイプラインを流し(すなわち、処理されるどの残っているセキュアコンテンツも削除し)、クリアし、かつ/またはL2キャッシュ61、GMEM70、および他のレジスタ72を含むセキュアコンテンツを含むことができるすべてのレジスタ、メモリ、およびキャッシュを無効にするように構成されてもよい。このクリアリングプロセスは、GPU12上に常駐する、配線接続されるか、またはセキュアにロードされ、保護されたシェーダコードを使用することを含んでもよい。

【００８３】

図10は、本開示の一例による方法を示すフローチャートである。メモリアクセスコントローラ53を含むGPU12、およびメモリコントローラ100は、図10の技法を実施するように構成されてもよい。

【００８４】

本開示の一例では、メモリアクセスコントローラ53は、GPU12の少なくとも1つのハードウェアユニットからのメモリトランザクションをメモリコントローラ100中の非セキュアコンテキストバンクに向けることによって、非セキュアモードに従って、メモリ(たとえば、システムメモリ10)の非セキュア部分にアクセスするように構成されてもよい(202)。メモリアクセスコントローラ53は、GPU12の少なくとも1つのハードウェアユニットからのメモリトランザクションをメモリコントローラ100中のセキュアコンテキストバンクに向けることによって、セキュアモードに従って、メモリのセキュア部分にアクセスするようにさらに構成されてもよい(204)。本開示の一例では、セキュアコンテキストバンクは、メモリの非セキュア部分への読取り専用ページテーブルエントリおよびメモリのセキュア部分への読取り/書込みページテーブルエントリを含み、非セキュアコンテキストバンクは、メモリの非セキュア部分への読取り専用ページテーブルエントリを含む。本開示の別の例では、メモリコントローラ100は、セキュアコンテキストバンクの読取り専用ページテーブルエントリ内に含まれるアドレスにデータを書き込むための要求が受信されると(206)、ページフォールトを発行する(208)ように構成されてもよい。

【００８５】
本開示の別の例では、GPUの少なくとも1つのハードウェアユニットは、頂点フェッチ復号ユニット、高レベルシーケンサ、頂点シェーダ、ピクセルシェーダ、およびレンダバックエンドユニットのうちの1つまたは複数を含む。
【００８６】
本開示の別の例では、GPU12は、GPU12が非セキュアモードで動作しているか、またはセキュアモードで動作しているかにかかわらず、非セキュアコンテキストバンクを通して、フロントエンドコマンドプロセッサを用いて、メモリの非セキュア部分にアクセスするように構成されてもよい。
【００８７】
本開示の別の例では、GPUドライバ7は、GPU12をセキュアモードまたは非セキュアモードに置くように構成されてもよい。本開示のさらに別の例では、GPU12は、GPUドライバ7から、GPU12の1つまたは複数の内部メモリをクリアしかつ無効にするための、GPU12のコマンドストリームレジスタへの命令を受信するように構成されてもよい。GPU12は、GPU12がコマンドストリームレジスタ中の命令に基づいて、セキュアモードから非セキュアモードに遷移されると、少なくとも何らかのコンテンツを、GPU12の1つまたは複数の内部メモリからクリアしかつ無効にするようにさらに構成されてもよい。
【００８８】
本開示の別の例では、GPU12は、クリアレジスタにおいて、GPUの1つまたは複数の内部メモリをクリアしかつ無効にするための指示を受信し、GPU12がクリアレジスタ中の指示に基づいて、セキュアモードから非セキュアモードに遷移されると、少なくとも何らかのコンテンツを、GPU12の1つまたは複数の内部メモリからクリアしかつ無効にするように構成されてもよい。
【００８９】
図11は、本開示の一例による方法を示すフローチャートである。メモリアクセスコントローラ53を含むGPU12は、図11の技法を実施するように構成されてもよい。
【００９０】
本開示の一例では、GPU12は、非セキュアモードおよびセキュアモードのうちの1つと、複数のメモリリソースの各々に関連付けられたそれぞれのリソース記述子とに従って、第1のメモリユニット(たとえば、システムメモリ10)にアクセスするように構成されてもよい。メモリアクセスコントローラ53は、複数のメモリリソースの各々に関連付けられたそれぞれのリソース記述子を読み取り(302)、第1のメモリユニットへのメモリトランザクションについての要求を受信する(304)ように構成されてもよい。
【００９１】
メモリアクセスコントローラ53は、メモリトランザクションについての要求に関連したメモリリソースに関連付けられたリソース記述子が、セキュア記述子であるか、または非セキュアリソース記述子であるか判断する(306)ようにさらに構成されてもよい。メモリアクセスコントローラ53は、要求に応答して、GPU12がセキュアモードに従って動作しているとき、それぞれのリソース記述子がセキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを第1のメモリユニットのセキュア部分に向ける(312)ようにさらに構成されてもよい。メモリアクセスコントローラ53は、要求に応答して、GPU12がセキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを第1のメモリユニットの非セキュア部分に向ける(308)ようにさらに構成されてもよい。メモリアクセスコントローラ53はまた、要求に応答して、GPU12がセキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げる(310)ように構成されてもよい。
【００９２】

本開示の別の例では、メモリアクセスコントローラ53は、要求に応答して、GPU12が非セキュアモードに従って動作しているとき、それぞれのリソース記述子が非セキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを第1のメモリユニットの非セキュア部分に向け、要求に応答して、GPU12が非セキュアモードに従って動作しているとき、それぞれのリソース記述子がセキュアリソース記述子である複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを取り下げるようにさらに構成される。

【００９３】

本開示の別の例では、メモリアクセスコントローラ53は、セキュアメモリ管理ユニットを使用することによって、第1のメモリユニットのセキュア部分にデータを書き込むように構成され、セキュアメモリ管理ユニットは、第1のメモリユニットのセキュア部分についてのアドレス範囲を含むセキュアページテーブルを使用する。本開示の別の例では、メモリアクセスコントローラ53は、非セキュアメモリ管理ユニットを使用することによって、第1のメモリユニットの非セキュア部分からデータを読み取るように構成され、非セキュアメモリ管理ユニットは、第1のメモリユニットの非セキュア部分についてのアドレス範囲を含む非セキュアページテーブルを使用する。

【００９４】

本開示の別の例では、メモリアクセスコントローラ53は、仮想メモリアドレスの範囲からの仮想メモリアドレスに従って、データを読み取り、書き込むように構成され、仮想メモリアドレスの範囲は、セキュアメモリ管理ユニットによって使用されるセキュアページテーブル中のエントリに関する仮想メモリアドレスの第1の範囲、および非セキュアメモリ管理ユニットによって使用される非セキュアページテーブル中のエントリに関する仮想メモリアドレスの第2の範囲を含む。

【００９５】

1つまたは複数の例では、上記で説明した機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せで実装されてもよい。ソフトウェアで実装される場合、機能は、非一時的コンピュータ可読媒体を備える製造品上の1つまたは複数の命令またはコードとして記憶されてもよい。コンピュータ可読媒体は、コンピュータデータ記憶媒体を含んでもよい。データ記憶媒体は、本開示で説明した技法を実装するための命令、コード、および/またはデータ構造を取り出すために1つまたは複数のコンピュータまたは1つまたは複数のプロセッサによってアクセスすることのできる任意の利用可能な媒体であってもよい。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスクストレージ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、フラッシュメモリ、または、命令もしくはデータ構造の形態の所望のプログラムコードを搬送もしくは記憶するために使用することができ、コンピュータによってアクセスすることができる、任意の他の媒体を備えることができる。本明細書で使用するディスク(disk)およびディスク(disc)は、コンパクトディスク(disc)(CD)、レーザーディスク(登録商標)(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピーディスク(disk)、およびブルーレイディスク(disc)を含み、ディスク(disk)は、通常、データを磁気的に再生し、ディスク(disc)は、レーザーを用いてデータを光学的に再生する。上記の組合せもコンピュータ可読媒体の範囲に含まれるべきである。

【００９６】

コードは、1つまたは複数のDSP、汎用マイクロプロセッサ、ASIC、FPGA、または他の等価の集積論理回路もしくはディスクリート論理回路などの、1つまたは複数のプロセッサによって実行されてもよい。加えて、いくつかの態様では、本明細書で説明する機能性は、専用のハードウェアモジュールおよび/またはソフトウェアモジュール内で提供されてもよい。また、本技法は、1つまたは複数の回路または論理要素において完全に実装することができる。

【００９７】

本開示の技法は、ワイヤレスハンドセット、集積回路(IC)、またICのセット(たとえば、チップセット)を含む、様々なデバイスまたは装置において実装されてもよい。本開示では、開示される技法を実行するように構成されるデバイスの機能的側面を強調するために、様々な構成要素、モジュール、またはユニットが説明されているが、それらは、必ずしも異なるハードウェアユニットによる実現を必要とするとは限らない。むしろ、上記で説明したように、様々なユニットは、コーデックハードウェアユニットにおいて結合されてよく、または好適なソフトウェアおよび/もしくはファームウェアとともに、上記で説明したような1つもしくは複数のプロセッサを含む相互動作可能なハードウェアユニットの集合によって設けられてもよい。

【００９８】

様々な例について述べた。これらおよび他の例は、以下の特許請求の範囲内に入る。

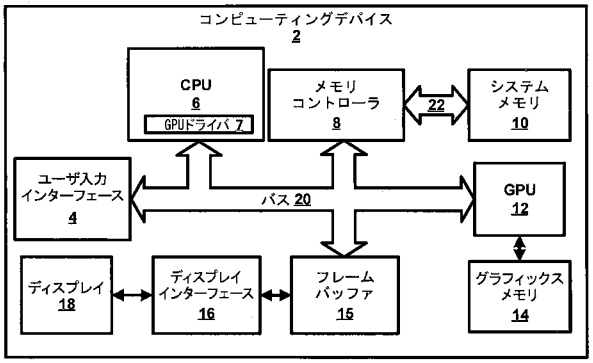
【符号の説明】

【００９９】

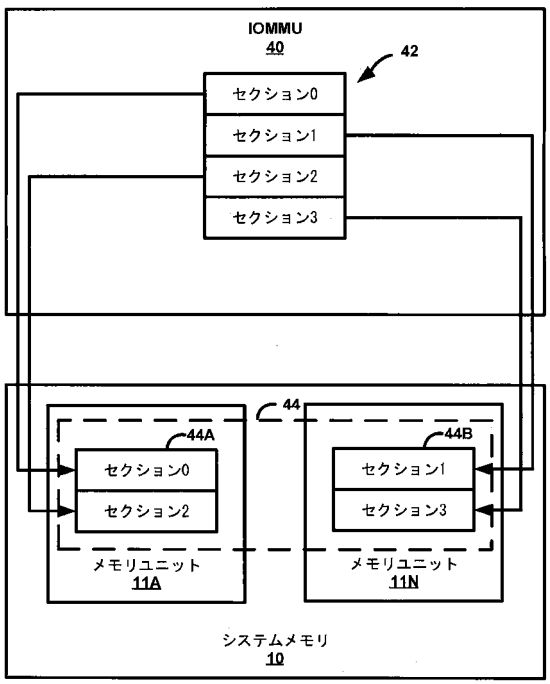
2 コンピューティングデバイス
4 ユーザ入力インターフェース
6 中央処理ユニット(CPU)
7 GPUドライバ、グラフィックスドライバ
8 メモリコントローラ
10 システムメモリ
11A メモリユニット
11N メモリユニット
12 グラフィックス処理ユニット(GPU)
14 グラフィックスメモリ
15 フレームバッファ
16 ディスプレイインターフェース
18 ディスプレイ
20 バス、システムバス
22 バス、メモリバス
24 ソフトウェアアプリケーション
26 グラフィックスAPI
30 グラフィックス処理パイプライン、グラフィックス3D処理パイプライン
32 コマンドエンジン
34 ジオメトリ処理ステージ
36 ラスタ化ステージ
38 ピクセル処理パイプライン
39 汎用シェーダ
40 IOMMU
42 仮想ページ
44 物理ページ
44A 部分
44B 部分
50 メモリコントローラ
51 非セキュアIOMMU
52 セキュアIOMMU
53 メモリアクセスコントローラ
54 セキュアオペレーティングシステム(OS)
56 非セキュアメモリ
57 セキュアメモリ
60 VBIF
61 L2キャッシュ

62　コマンドプロセッサ(CP)
65　頂点フェッチ復号(VFD)ユニット
66　高レベルシーケンサ(HLSQ)
67　頂点シェーダ(VS)
68　ピクセルシェーダ(PS)
69　レンダバックエンド(RB)
70　グラフィックスメモリ(GMEM)
71　GPUハードウェアブロック
72　他のレジスタ
73　クライアント
74　クリアレジスタ
76　レジスタ
100　メモリコントローラ
102　非セキュアコンテキストバンク
104　非セキュアPTエントリ
105　セキュアコンテキストバンク
106　非セキュアPTエントリ
108　セキュアPTエントリ

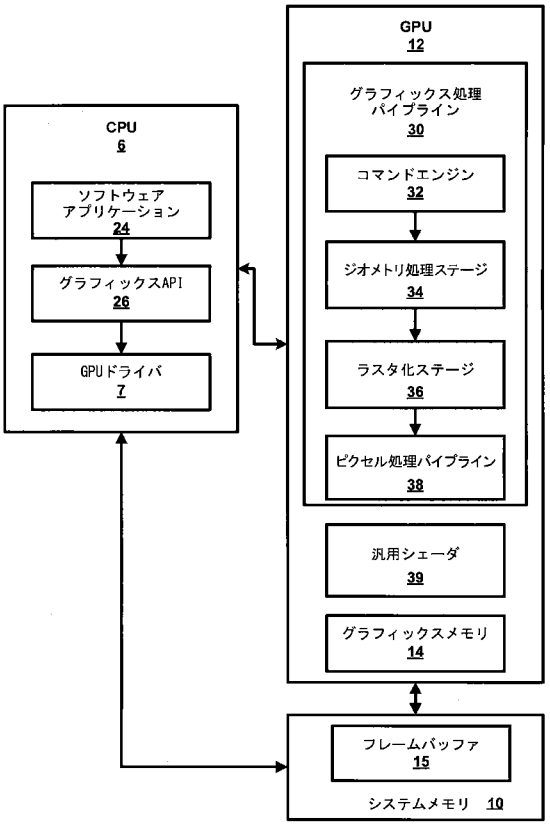
【図１】



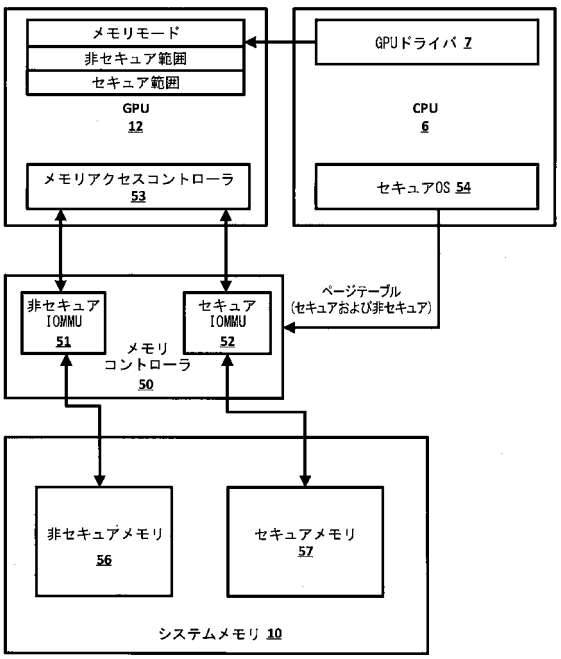
【図２】



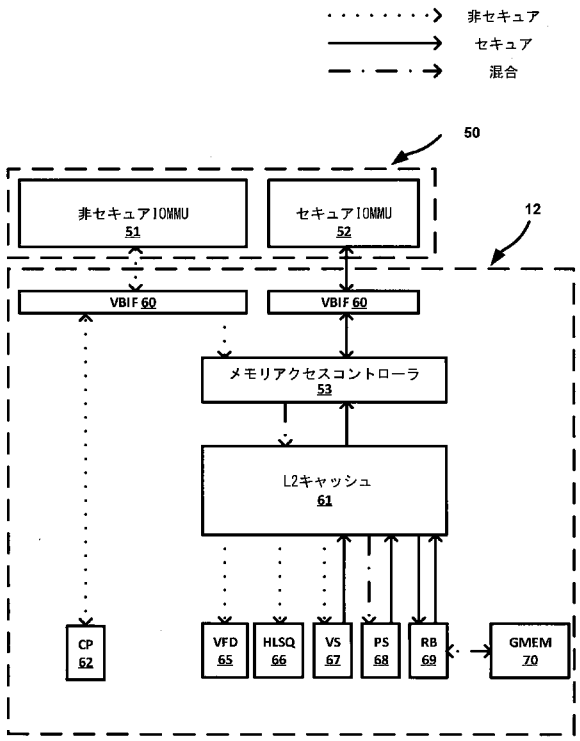
【図３】


GPU
12
グラフィックス処理
パイプライン
30
コマンドエンジン
32
ジオメトリ処理ステージ
34
ラスタ化ステージ
36
ピクセル処理パイプライン
38
汎用シェーダ
39
グラフィックスメモリ
14
CPU
6
ソフトウェア
アプリケーション
24
グラフィックスAPI
26
GPUドライバ
7
フレームバッファ
15
システムメモリ 10

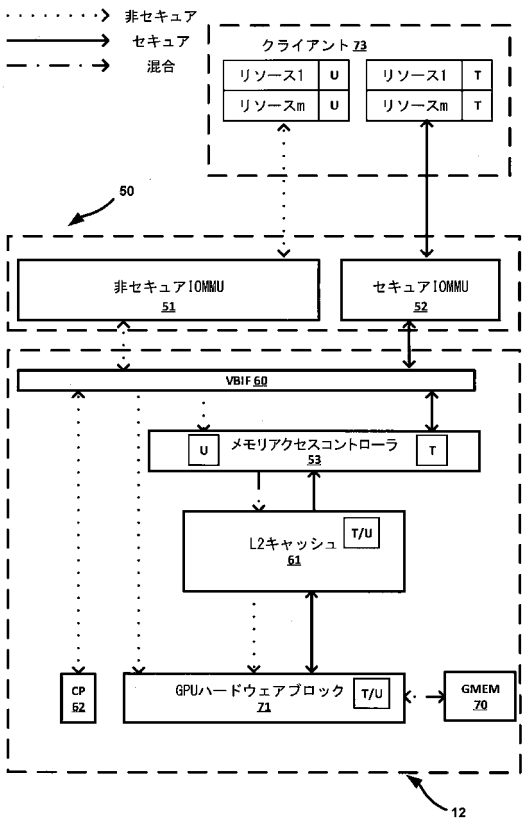
【図４】


メモリモード
非セキュア範囲
セキュア範囲
GPU
12
メモリアクセスコントローラ
53
GPUドライバ 7
CPU
6
セキュアOS 54
非セキュア
IOMMU
51
セキュア
IOMMU
52
ページテーブル
(セキュアおよび非セキュア)
メモリ
コントローラ
50
非セキュアメモリ
56
セキュアメモリ
57
システムメモリ 10

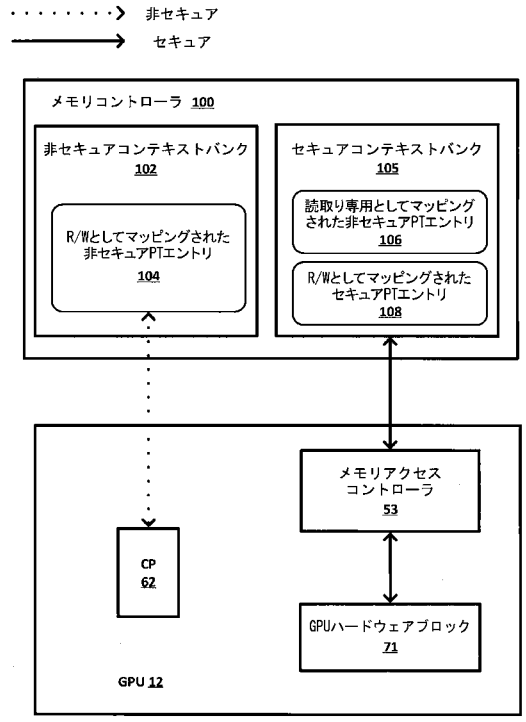
【図５】


非セキュア
セキュア
混合
50
非セキュアIOMMU
51
セキュアIOMMU
52
12
VBIF 60
VBIF 60
メモリアクセスコントローラ
53
L2キャッシュ
61
CP
62
VFD
65
HLSQ
66
VS
67
PS
68
RB
69
GMEM
70

【図６】

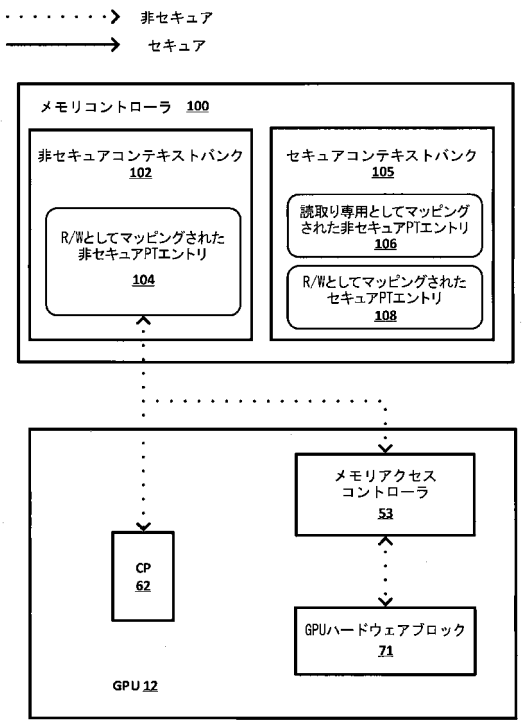

非セキュア
セキュア
混合
クライアント 73
リソース1
U
リソースm
U
リソース1
T
リソースm
T
50
非セキュアIOMMU
51
セキュアIOMMU
52
VBIF 60
U
メモリアクセスコントローラ
53
T
L2キャッシュ
61
T/U
CP
62
GPUハードウェアブロック
71
T/U
GMEM
70
12

【図７Ａ】



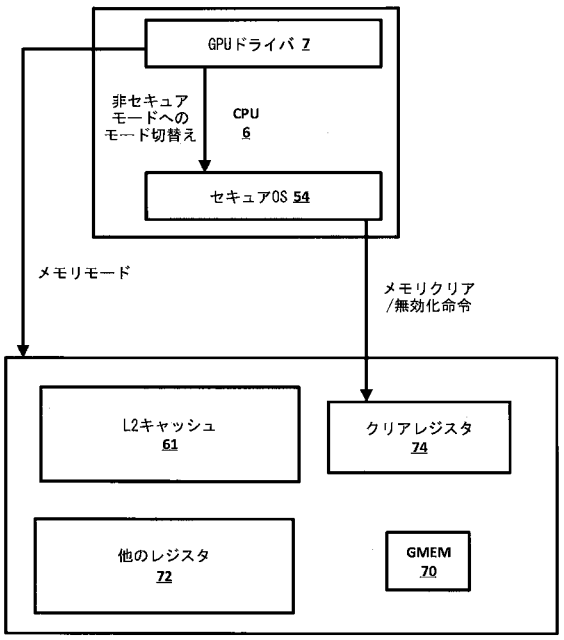
セキュアモード

【図７Ｂ】

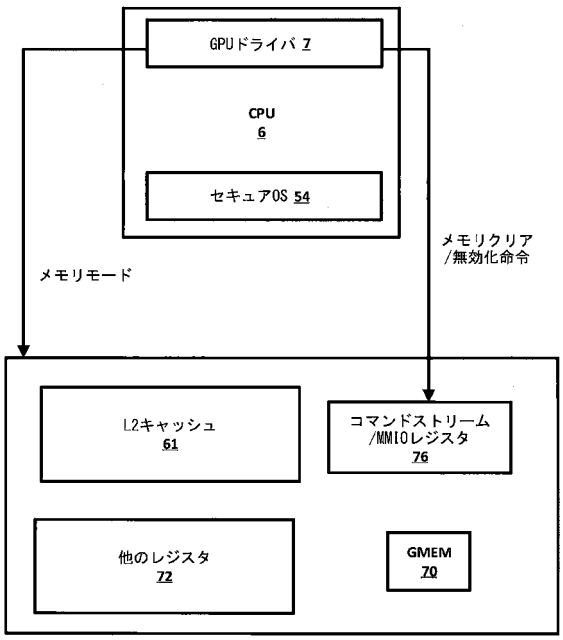


非セキュアモード

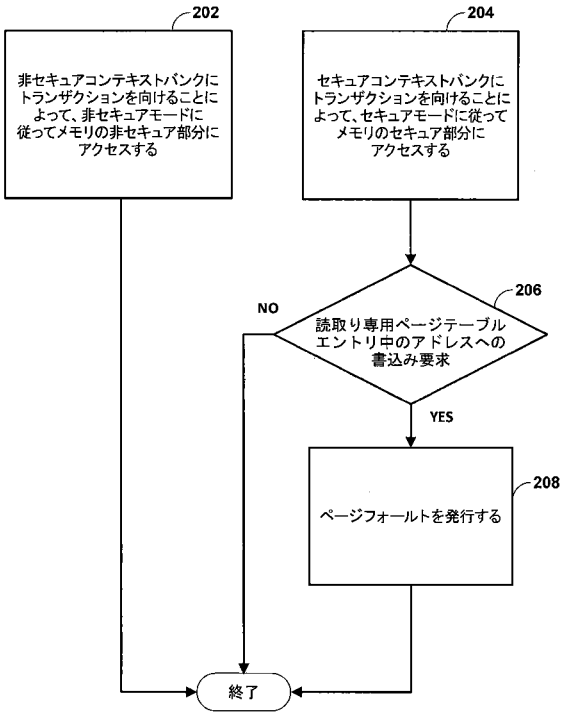
【図８】



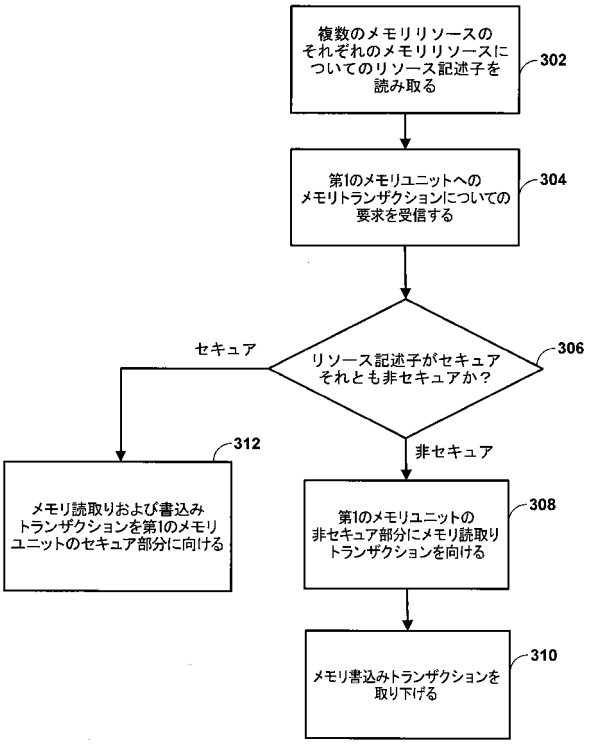
【図９】



【図１０】



【図１１】



【手続補正書】
【提出日】平成30年2月8日(2018.2.8)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
グラフィックス処理のための装置であって、
非セキュアモードおよびセキュアモードのうちの1つと、複数のメモリリソースの各々に関連付けられたそれぞれのリソース記述子とに従って、第1のメモリユニットにアクセスするように構成されるグラフィックス処理ユニット(GPU)を備え、各それぞれのリソース記述子は、前記複数のリソースの各それぞれのメモリリソースがどのように使われるべきかを示すタグ情報であり、前記GPUは、
前記複数のメモリリソースの各々に関連付けられた前記それぞれのリソース記述子を読み取るように構成されるメモリアクセスコントローラを備え、
前記メモリアクセスコントローラは、前記第1のメモリユニットへのメモリトランザクションについての要求を受信するように構成され、
前記メモリアクセスコントローラは、前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子がセキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するすべてのメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットのセキュア部分に向けるように構成され、
前記メモリアクセスコントローラは、前記要求に応答して、前記GPUが前記セキュアモ

ードに従って動作しているとき、前記それぞれのリソース記述子が非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するすべてのメモリ読取りトランザクションを前記第1のメモリユニットの非セキュア部分に向けるように構成され、

前記メモリアクセスコントローラは、前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するすべてのメモリ書込みトランザクションを取り下げるように構成される、

装置。

【請求項２】

前記メモリアクセスコントローラは、前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットの非セキュア部分に向けるようにさらに構成され、

前記メモリアクセスコントローラは、前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを取り下げるようにさらに構成される、請求項1に記載の装置。

【請求項３】

前記メモリアクセスコントローラは、セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記セキュア部分にデータを書き込むように構成され、前記セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記セキュア部分についてのアドレス範囲を含むセキュアページテーブルを使用し、

前記メモリアクセスコントローラは、非セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記非セキュア部分からデータを読み取るように構成され、前記非セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記非セキュア部分についてのアドレス範囲を含む非セキュアページテーブルを使用する、

請求項1に記載の装置。

【請求項４】

前記メモリアクセスコントローラは、仮想メモリアドレスの範囲からの仮想メモリアドレスに従ってデータを読み取りかつ書き込み、前記仮想メモリアドレスの範囲は、前記セキュアメモリ管理ユニットによって使用される前記セキュアページテーブル中のエントリに関する仮想メモリアドレスの第1の範囲、および前記非セキュアメモリ管理ユニットによって使用される前記非セキュアページテーブル中のエントリに関する仮想メモリアドレスの第2の範囲を含む、請求項3に記載の装置。

【請求項５】

グラフィックスドライバを記憶する第2のメモリユニットであって、前記グラフィックスドライバは、前記GPUをセキュアモードまたは非セキュアモードに置くように構成される第2のメモリユニットをさらに備える、請求項4に記載の装置。

【請求項６】

前記セキュアメモリ管理ユニットと、

前記非セキュアメモリ管理ユニットと、

セキュアオペレーティングシステムおよび前記グラフィックスドライバを実行する中央処理ユニット(CPU)であって、前記セキュアオペレーティングシステムは、前記セキュアページテーブルを前記セキュアメモリ管理ユニットに、かつ前記非セキュアページテーブルを前記非セキュアメモリ管理ユニットに供給するように構成される中央処理ユニットと

をさらに備える、請求項5に記載の装置。

【請求項７】

前記GPUはクリアレジスタおよび1つまたは複数の内部メモリをさらに備え、前記セキュアオペレーティングシステムは、前記GPUが前記セキュアモードから前記非セキュアモードに遷移されると、前記GPUに少なくとも何らかのコンテンツを前記1つまたは複数の内部メモリからクリアかつ無効にさせる命令を前記クリアレジスタに送信するように構成される、請求項6に記載の装置。

【請求項８】

前記GPUはコマンドストリームレジスタおよび1つまたは複数の内部メモリをさらに備え、前記グラフィックスドライバは、前記GPUが前記セキュアモードから前記非セキュアモードに遷移されると、前記GPUに少なくとも何らかのコンテンツを前記1つまたは複数の内部メモリからクリアかつ無効にさせる命令を前記コマンドストリームレジスタに送信するように構成される、請求項6に記載の装置。

【請求項９】

前記GPUは、

前記GPUが前記非セキュアモードにあるか、または前記セキュアモードにあるかにかかわらず、前記第1のメモリの前記非セキュア部分にデータを書き込むように構成される1つまたは複数のハードウェアブロックをさらに備え、前記1つまたは複数のハードウェアブロックは、前記第1のメモリユニットの前記セキュア部分への読取りアクセスを有さない、請求項1に記載の装置。

【請求項１０】

前記1つまたは複数のハードウェアブロックはフロントエンドコマンドプロセッサを含む、請求項9に記載の装置。

【請求項１１】

複数のメモリリソースのそれぞれのメモリリソースについてのそれぞれのリソース記述子を読み取るステップであって、各それぞれのリソース記述子は、前記複数のリソースの各それぞれのメモリリソースがどのように使われるべきかを示すタグ情報である、ステップと、

第1のメモリユニットへのメモリトランザクションについての要求を受信するステップと、

前記要求に応答して、グラフィックス処理ユニット(GPU)がセキュアモードに従って動作しているとき、前記それぞれのリソース記述子がセキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットのセキュア部分に向けるステップと、

前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを前記第1のメモリユニットの非セキュア部分に向けるステップと、

前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げるステップと

を含む、方法。

【請求項１２】

前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットの非セキュア部分に向けるステップと、

前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを取り下げるステップと

をさらに含む、請求項11に記載の方法。
【請求項１３】
セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記セキュア部分にデータを書き込むステップであって、前記セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記セキュア部分についてのアドレス範囲を含むセキュアページテーブルを使用する、ステップと、
非セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記非セキュア部分からデータを読み取るステップであって、前記非セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記非セキュア部分についてのアドレス範囲を含む非セキュアページテーブルを使用する、ステップと
をさらに含む、請求項11に記載の方法。
【請求項１４】
仮想メモリアドレスの範囲からの仮想メモリアドレスに従ってデータを読み取りかつ書き込むステップであって、前記仮想メモリアドレスの範囲は、前記セキュアメモリ管理ユニットによって使用される前記セキュアページテーブル中のエントリに関する仮想メモリアドレスの第1の範囲、および前記非セキュアメモリ管理ユニットによって使用される前記非セキュアページテーブル中のエントリに関する仮想メモリアドレスの第2の範囲を含む、ステップ
をさらに含む、請求項13に記載の方法。
【請求項１５】
前記GPUをセキュアモードまたは非セキュアモードに置くステップをさらに含む、請求項14に記載の方法。
【請求項１６】
前記セキュアページテーブルを前記セキュアメモリ管理ユニットに、および前記非セキュアページテーブルを前記非セキュアメモリ管理ユニットに供給するステップ
をさらに含む、請求項15に記載の方法。
【請求項１７】
前記GPUのクリアレジスタに命令を送信するステップと、
前記命令に応答して、前記GPUが前記セキュアモードから前記非セキュアモードに遷移されると、少なくとも何らかのコンテンツを1つまたは複数の内部メモリからクリアかつ無効にするステップと
をさらに含む、請求項16に記載の方法。
【請求項１８】
前記GPUのコマンドストリームレジスタに命令を送信するステップと、
前記命令に応答して、前記GPUが前記セキュアモードから前記非セキュアモードに遷移されると、少なくとも何らかのコンテンツを1つまたは複数の内部メモリからクリアかつ無効にするステップと
をさらに含む、請求項16に記載の方法。
【請求項１９】
前記GPUが前記非セキュアモードにあるか、または前記セキュアモードにあるかにかかわらず、前記GPUの1つまたは複数のハードウェアブロックから、前記第1のメモリの前記非セキュア部分にデータを書き込むステップであって、前記1つまたは複数のハードウェアブロックは、前記第1のメモリユニットの前記セキュア部分への読取りアクセスを有さない、ステップ
をさらに含む、請求項11に記載の方法。
【請求項２０】
前記1つまたは複数のハードウェアブロックはフロントエンドコマンドプロセッサを含む、請求項19に記載の方法。
【請求項２１】
グラフィックス処理のための装置であって、

複数のメモリリソースのそれぞれのメモリリソースについてのそれぞれのリソース記述子を読み取るための手段であって、各それぞれのリソース記述子は、前記複数のリソースの各それぞれのメモリリソースがどのように使われるべきかを示すタグ情報である、手段と、

第1のメモリユニットへのメモリトランザクションについての要求を受信するための手段と、

前記要求に応答して、グラフィックス処理ユニット(GPU)がセキュアモードに従って動作しているとき、前記それぞれのリソース記述子がセキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットのセキュア部分に向けるための手段と、

前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを前記第1のメモリユニットの非セキュア部分に向けるための手段と、

前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げるための手段と

を備える、装置。

【請求項２２】

前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットの非セキュア部分に向けるための手段と、

前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを取り下げるための手段と

をさらに備える、請求項21に記載の装置。

【請求項２３】

セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記セキュア部分にデータを書き込むための手段であって、前記セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記セキュア部分についてのアドレス範囲を含むセキュアページテーブルを使用する、手段と、

非セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記非セキュア部分からデータを読み取るための手段であって、前記非セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記非セキュア部分についてのアドレス範囲を含む非セキュアページテーブルを使用する、手段と

をさらに備える、請求項21に記載の装置。

【請求項２４】

仮想メモリアドレスの範囲からの仮想メモリアドレスに従ってデータを読み取りかつ書き込むための手段であって、前記仮想メモリアドレスの範囲は、前記セキュアメモリ管理ユニットによって使用される前記セキュアページテーブル中のエントリに関する仮想メモリアドレスの第1の範囲、および前記非セキュアメモリ管理ユニットによって使用される前記非セキュアページテーブル中のエントリに関する仮想メモリアドレスの第2の範囲を含む、手段

をさらに含む、請求項23に記載の装置。

【請求項２５】

前記GPUをセキュアモードまたは非セキュアモードに置くための手段

をさらに備える、請求項24に記載の装置。

【請求項２６】
命令を記憶するコンピュータ可読記憶媒体であって、前記命令は、実行されると、1つまたは複数のプロセッサに、
複数のメモリリソースのそれぞれのメモリリソースについてのそれぞれのリソース記述子を読み取ることであって、各それぞれのリソース記述子は、前記複数のリソースの各それぞれのメモリリソースがどのように使われるべきかを示すタグ情報である、読み取ることと、
第1のメモリユニットへのメモリトランザクションについての要求を受信することと、
前記要求に応答して、グラフィックス処理ユニット(GPU)がセキュアモードに従って動作しているとき、前記それぞれのリソース記述子がセキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを前記第1のメモリユニットのセキュア部分に向けることと、
前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りトランザクションを前記第1のメモリユニットの非セキュア部分に向けることと、
前記要求に応答して、前記GPUが前記セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ書込みトランザクションを取り下げることと
を行わせる、コンピュータ可読記憶媒体。
【請求項２７】
前記命令は、前記1つまたは複数のプロセッサに、
前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記非セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを、前記第1のメモリユニットの非セキュア部分に向けることと、
前記要求に応答して、前記GPUが前記非セキュアモードに従って動作しているとき、前記それぞれのリソース記述子が前記セキュアリソース記述子である前記複数のメモリリソースのうちのメモリリソースに関するメモリ読取りおよび書込みトランザクションを取り下げることと
をさらに行わせる、請求項26に記載のコンピュータ可読記憶媒体。
【請求項２８】
前記命令は、前記1つまたは複数のプロセッサに、
セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記セキュア部分にデータを書き込むことであって、前記セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記セキュア部分についてのアドレス範囲を含むセキュアページテーブルを使用する、書き込むことと、
非セキュアメモリ管理ユニットを使用して前記第1のメモリユニットの前記非セキュア部分からデータを読み取ることであって、前記非セキュアメモリ管理ユニットは、前記第1のメモリユニットの前記非セキュア部分についてのアドレス範囲を含む非セキュアページテーブルを使用する、読み取ることと
をさらに行わせる、請求項26に記載のコンピュータ可読記憶媒体。
【請求項２９】
前記命令は、前記1つまたは複数のプロセッサに、
仮想メモリアドレスの範囲からの仮想メモリアドレスに従ってデータを読み取り書き込むことであって、前記仮想メモリアドレスの範囲は、前記セキュアメモリ管理ユニットによって使用される前記セキュアページテーブル中のエントリに関する仮想メモリアドレスの第1の範囲、および前記非セキュアメモリ管理ユニットによって使用される前記非セキュアページテーブル中のエントリに関する仮想メモリアドレスの第2の範囲を含む、読み取りかつ書き込むこと

をさらに行わせる、請求項28に記載のコンピュータ可読記憶媒体。
【請求項３０】
前記命令は、前記1つまたは複数のプロセッサに、
前記GPUをセキュアモードまたは非セキュアモードにさらに置かせる、請求項29に記載のコンピュータ可読記憶媒体。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/043903

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/10
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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/305388 A1 (KOTTILINGAL SUDEEP RAVI [US] ET AL) 14 November 2013 (2013-11-14) paragraphs [0034], [0055] - [0058]; figure 4	1-30
Y	US 2015/002523 A1 (ZENG THOMAS [US] ET AL) 1 January 2015 (2015-01-01) paragraphs [0018] - [0025]; figures 1,2	1-30
Y	EP 1 801 725 A2 (NVIDIA CORP [US]) 27 June 2007 (2007-06-27) abstract; figures 1,7	1-30

☐ 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	Date of mailing of the international search report
13 October 2016	26/10/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kerschbaumer, J

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/043903

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013305388 A1	14-11-2013	US 2013305388 A1	14-11-2013
		WO 2013169434 A1	14-11-2013
US 2015002523 A1	01-01-2015	CA 2912929 A1	08-01-2015
		CN 105393258 A	09-03-2016
		EP 3017396 A1	11-05-2016
		JP 2016524257 A	12-08-2016
		KR 20160025554 A	08-03-2016
		US 2015002523 A1	01-01-2015
		WO 2015002851 A1	08-01-2015
EP 1801725 A2	27-06-2007	CN 1984298 A	20-06-2007
		EP 1801725 A2	27-06-2007
		JP 4740830 B2	03-08-2011
		JP 2007215159 A	23-08-2007
		KR 20070063465 A	19-06-2007

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,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,MC,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,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,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,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(72)発明者 ラメシュ・ヴィスワナタン
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

Ｆターム(参考) 5B017 AA01 BA01 BB02 CA01