(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2016-524257
(P2016-524257A)
(43)公表日　平成28年8月12日(2016.8.12)

(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 23 頁）

(21)出願番号	特願2016-524277 (P2016-524277)
(86)(22)出願日	平成26年6月30日 (2014.6.30)
(85)翻訳文提出日	平成27年12月18日 (2015.12.18)
(86)国際出願番号	PCT/US2014/044776
(87)国際公開番号	WO2015/002851
(87)国際公開日	平成27年1月8日 (2015.1.8)
(31)優先権主張番号	61/841,881
(32)優先日	平成25年7月1日 (2013.7.1)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	14/014,032
(32)優先日	平成25年8月29日 (2013.8.29)
(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　トーマス・ツェン
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】グラフィックス処理装置への安全なアクセス制御を提供するためのシステムおよび方法

(57)【要約】
グラフィックス処理装置(GPU)へのセキュアなアクセス制御を提供するためのシステム、方法、およびコンピュータプログラムが、開示される。1つのシステムは、GPU、複数のGPUプログラミングインタフェース、およびコマンドプロセッサを含む。各GPUプログラミングインタフェースは、複数のセキュリティゾーンのうちの相異なる1つに動的に割り当てられる。各GPUプログラミングインタフェースは、対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を受け取るように構成される。作業命令は、GPUによって実行されるべき命令を備える。コマンドプロセッサは、複数のGPUプログラミングインタフェースと通信する。コマンドプロセッサは、複数のGPUプログラミングインタフェースによって受け取られる作業命令の実行を、別個のセキュアなメモリ領域を使用して制御するように構成される。各セキュアなメモリ領域は、複数のセキュリティゾーンのうちの1つに割り振られる。

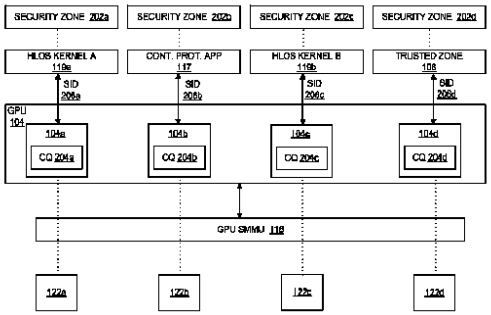


FIG. 2

【特許請求の範囲】
【請求項１】
グラフィックス処理装置へのセキュアなアクセス制御を提供するための方法であって、
グラフィックス処理装置へのアクセスを制御するための複数のセキュリティゾーンを定義するステップと、
前記セキュリティゾーンの各々を、前記GPUによって提供される複数のGPUプログラミングインタフェースのうちの対応する1つに割り当てるステップであって、前記GPUプログラミングインタフェースの各々は、前記対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を受け取るためのものであり、前記作業命令は、前記GPUによって実行されるべき命令を備える、ステップと、
前記複数のGPUプログラミングインタフェースによって受け取られた前記作業命令の実行を、別個のセキュアなメモリ領域を使用して制御するステップであって、各セキュアなメモリ領域は、前記複数のセキュリティゾーンのうちの1つに割り振られる、ステップとを備える方法。
【請求項２】
前記GPUプログラミングインタフェースは、前記対応するGPUプログラミングインタフェースによって受け取られた作業命令を記憶するための、それぞれのコマンド待ち行列を備える、請求項1に記載の方法。
【請求項３】
前記作業命令は、前記セキュリティゾーンに従って、前記対応するGPUプログラミングインタフェース内へ中央処理装置(CPU)によって注入される、請求項1に記載の方法。
【請求項４】
前記作業命令は、前記対応するGPUプログラミングインタフェースを識別するストリーム識別子を使用して注入される、請求項3に記載の方法。
【請求項５】
前記別個のメモリ領域は、セキュアなメモリ管理装置によって割り振られる、請求項1に記載の方法。
【請求項６】
前記別個のメモリ領域のうちの1つまたは複数は、前記セキュアなメモリ管理装置内の関連付けられたコンテキストバンクを使用してハードウェアで実現される保護を伴う、隔離されたアドレス空間を備える、請求項5に記載の方法。
【請求項７】
前記隔離されたアドレス空間は、2つ以上のオペレーティングシステムを管理するためのハイパーバイザソフトウェアレイヤ、および信頼されるハードウェアと信頼されないハードウェアとの間の分離のうちの、1つまたは複数によって実装される、請求項6に記載の方法。
【請求項８】
前記セキュリティゾーンのうちの2つ以上は、並行に管理される、請求項1に記載の方法。
【請求項９】
前記セキュリティゾーンのうちの1つまたは複数は、非セキュアなゾーンまたはセキュアなゾーンを備える、請求項1に記載の方法。
【請求項１０】
前記作業命令を発行する前記1つまたは複数のアプリケーションは、コンテンツ保護ゾーンアプリケーション、オペレーティングシステムと関連したコンテンツ保護ゾーンカーネル、ハイレベルオペレーティングシステムカーネル、および信頼されるゾーンセキュリティモニタのうちの1つまたは複数を備える、請求項1に記載の方法。
【請求項１１】
グラフィックス処理装置へのセキュアなアクセス制御を提供するためのシステムであって、

グラフィックス処理装置(GPU)へのアクセスを制御するための複数のセキュリティゾーンを定義するための手段と、
前記セキュリティゾーンの各々を、前記GPUによって提供される複数のGPUプログラミングインタフェースのうちの対応する1つに割り当てるための手段であって、前記GPUプログラミングインタフェースの各々は、前記対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を受け取るためのものであり、前記作業命令は、前記GPUによって実行されるべき命令を備える、手段と、
前記複数のGPUプログラミングインタフェースによって受け取られた前記作業命令の実行を、別個のセキュアなメモリ領域を使用して制御するための手段であって、各セキュアなメモリ領域は、前記複数のセキュリティゾーンのうちの1つに割り振られる、手段と
を備えるシステム。
【請求項１２】
前記GPUプログラミングインタフェースは、前記対応するGPUプログラミングインタフェースによって受け取られた作業命令を記憶するための、それぞれの手段を備える、請求項11に記載のシステム。
【請求項１３】
前記作業命令は、前記セキュリティゾーンに従って、前記対応するGPUプログラミングインタフェース内へ中央処理装置(CPU)によって注入される、請求項11に記載のシステム。
【請求項１４】
前記作業命令は、前記対応するGPUプログラミングインタフェースを識別するストリーム識別子を使用して注入される、請求項13に記載のシステム。
【請求項１５】
前記別個のメモリ領域は、セキュアなメモリ管理装置によって割り振られる、請求項11に記載のシステム。
【請求項１６】
前記別個のメモリ領域のうちの1つまたは複数は、前記セキュアなメモリ管理装置内の関連付けられたコンテキストバンクを使用してハードウェアで実現される保護を伴う、隔離されたアドレス空間を備える、請求項15に記載のシステム。
【請求項１７】
前記隔離されたアドレス空間は、2つ以上のオペレーティングシステムを管理するためのハイパーバイザソフトウェアレイヤ、および信頼されるハードウェアと信頼されないハードウェアとの間の分離のうちの、1つまたは複数によって実装される、請求項16に記載のシステム。
【請求項１８】
前記セキュリティゾーンのうちの2つ以上は、並行に管理される、請求項11に記載のシステム。
【請求項１９】
前記セキュリティゾーンのうちの1つまたは複数は、非セキュアなゾーンまたはセキュアなゾーンを備える、請求項11に記載のシステム。
【請求項２０】
前記作業命令を発行する前記1つまたは複数のアプリケーションは、コンテンツ保護ゾーンアプリケーション、オペレーティングシステムと関連したコンテンツ保護ゾーンカーネル、ハイレベルオペレーティングシステムカーネル、および信頼されるゾーンセキュリティモニタのうちの1つまたは複数を備える、請求項11に記載のシステム。
【請求項２１】
グラフィックス処理装置へのセキュアなアクセス制御を提供するための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、プロセッサによる実行のためにコンピュータ可読媒体において実施され、
グラフィックス処理装置(GPU)へのアクセスを制御するための複数のセキュリティゾー

ンを定義することと、
前記セキュリティゾーンの各々を、前記GPUによって提供される複数のGPUプログラミングインタフェースのうちの対応する1つに割り当てることであって、前記GPUプログラミングインタフェースの各々は、前記対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を受け取るためのものであり、前記作業命令は、前記GPUによって実行されるべき命令を備えることと、
前記複数のGPUプログラミングインタフェースによって受け取られた前記作業命令の実行を、別個のセキュアなメモリ領域を使用して制御することであって、各セキュアなメモリ領域は、前記複数のセキュリティゾーンのうちの1つに割り振られることと
をするように構成されたロジックを備えるコンピュータプログラム。
【請求項２２】
前記GPUプログラミングインタフェースは、前記対応するGPUプログラミングインタフェースによって受け取られた作業命令を記憶するための、それぞれのコマンド待ち行列を備える、請求項21に記載のコンピュータプログラム。
【請求項２３】
前記作業命令は、前記セキュリティゾーンに従って、前記対応するGPUプログラミングインタフェース内へ中央処理装置(CPU)によって注入される、請求項21に記載のコンピュータプログラム。
【請求項２４】
前記作業命令は、前記対応するGPUプログラミングインタフェースを識別するストリーム識別子を使用して注入される、請求項23に記載のコンピュータプログラム。
【請求項２５】
前記別個のメモリ領域は、セキュアなメモリ管理装置によって割り振られる、請求項21に記載のコンピュータプログラム。
【請求項２６】
前記別個のメモリ領域のうちの1つまたは複数は、前記セキュアなメモリ管理装置内の関連付けられたコンテキストバンクを使用してハードウェアで実現される保護を伴う、隔離されたアドレス空間を備える、請求項25に記載のコンピュータプログラム。
【請求項２７】
前記隔離されたアドレス空間は、2つ以上のオペレーティングシステムを管理するためのハイパーバイザソフトウェアレイヤ、および信頼されるハードウェアと信頼されないハードウェアとの間の分離のうちの、1つまたは複数によって実装される、請求項26に記載のコンピュータプログラム。
【請求項２８】
前記セキュリティゾーンのうちの2つ以上は、並行に管理される、請求項21に記載のコンピュータプログラム。
【請求項２９】
前記セキュリティゾーンのうちの1つまたは複数は、非セキュアなゾーンまたはセキュアなゾーンを備える、請求項21に記載のコンピュータプログラム。
【請求項３０】
前記作業命令を発行する前記1つまたは複数のアプリケーションは、コンテンツ保護ゾーンアプリケーション、オペレーティングシステムと関連したコンテンツ保護ゾーンカーネル、ハイレベルオペレーティングシステムカーネル、および信頼されるゾーンセキュリティモニタのうちの1つまたは複数を備える、請求項21に記載のコンピュータプログラム。
【請求項３１】
グラフィックス処理装置へのセキュアなアクセス制御を提供するためのシステムであって、
グラフィックス処理装置(GPU)と、
前記GPUによって提供される複数のGPUプログラミングインタフェースであって、各GPU

プログラミングインタフェースは、複数のセキュリティゾーンのうちの相異なる1つに動的に割り当てられ、対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を受け取るように構成され、前記作業命令は、前記GPUによって実行されるべき命令を備える、複数のGPUプログラミングインタフェースと、

前記複数のGPUプログラミングインタフェースと通信するコマンドプロセッサであって、前記コマンドプロセッサは、前記複数のGPUプログラミングインタフェースによって受け取られた前記作業命令の実行を、別個のセキュアなメモリ領域を使用して制御するように構成され、各セキュアなメモリ領域は、前記複数のセキュリティゾーンのうちの1つに割り振られる、コマンドプロセッサと

を備えるシステム。

【請求項３２】

前記GPUプログラミングインタフェースは、前記対応するGPUプログラミングインタフェースによって受け取られた作業命令を記憶するための、それぞれのコマンド待ち行列を備える、請求項31に記載のシステム。

【請求項３３】

前記作業命令は、前記セキュリティゾーンに従って、前記対応するGPUプログラミングインタフェース内へ中央処理装置(CPU)によって注入される、請求項31に記載のシステム。

【請求項３４】

前記作業命令は、前記対応するGPUプログラミングインタフェースを識別するストリーム識別子を使用して注入される、請求項33に記載のシステム。

【請求項３５】

前記別個のメモリ領域は、セキュアなメモリ管理装置によって割り振られる、請求項31に記載のシステム。

【請求項３６】

前記別個のメモリ領域のうちの1つまたは複数は、前記セキュアなメモリ管理装置内の関連付けられたコンテキストバンクを使用してハードウェアで実現される保護を伴う、隔離されたアドレス空間を備える、請求項35に記載のシステム。

【請求項３７】

前記隔離されたアドレス空間は、2つ以上のオペレーティングシステムを管理するためのハイパーバイザソフトウェアレイヤ、および信頼されるハードウェアと信頼されないハードウェアとの間の分離のうちの、1つまたは複数によって実装される、請求項36に記載のシステム。

【請求項３８】

前記セキュリティゾーンのうちの2つ以上は、並行に管理される、請求項31に記載のシステム。

【請求項３９】

前記セキュリティゾーンのうちの1つまたは複数は、非セキュアなゾーンまたはセキュアなゾーンを備える、請求項31に記載のシステム。

【請求項４０】

前記作業命令を発行する前記1つまたは複数のアプリケーションは、コンテンツ保護ゾーンアプリケーション、オペレーティングシステムと関連したコンテンツ保護ゾーンカーネル、ハイレベルオペレーティングシステムカーネル、および信頼されるゾーンセキュリティモニタのうちの1つまたは複数を備える、請求項31に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

優先権および関連出願に関する陳述

本出願は、2013年7月1日に出願された米国特許仮出願、「System and Method for Prov

iding Secure Access Control to a Graphics Processing Unit」という表題の、譲渡された仮出願第61/841,881号の米国特許法第119条(e)に基づく優先権を主張するものであり、上記出願の内容全体が参照により本明細書に組み込まれる。

【背景技術】

【０００２】

モバイルフォンなどのポータブルコンピューティングデバイス(「PCD」)は、より複雑になりつつある。既存のPCDは、しばしば、相異なる機能性を実行するとともに、そのようなデバイスに対して増加する需要を満たすための、いくつかのプロセッサ(たとえば、中央処理装置(CPU)、グラフィックス処理装置(GPU)、デジタルシグナルプロセッサ(DSP)など)を有する。既存のPCDは、また、コンテンツ保護アーキテクチャをサポートすることができ、コンテンツ保護アーキテクチャは、一般に、バンキング、診療記録、指紋などを含むアプリケーションのための秘密のデータへのアクセスを制御する、デジタル著作権管理(DRM)などのユースケースのためのアクセス制御要件をサポートする。コンテンツ保護アーキテクチャは、通常、機密を扱うコンテンツへの、アプリケーションによるアクセスを制御するために、メモリ領域を相異なるセキュリティゾーンへ分離する。しかしながら、既存のPCDおよびコンテンツ保護アーキテクチャは、CPUレベルのアクセス制御に限られる。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

したがって、当技術分野において、GPUへのセキュアなアクセス制御を提供するための、改善されたメカニズムに対する必要性がある。

【課題を解決するための手段】

【０００４】

グラフィックス処理装置(GPU)へのセキュアなアクセス制御を提供するためのシステム、方法、およびコンピュータプログラムが、開示される。1つの方法は、グラフィックス処理装置(GPU)へのアクセスを制御するための複数のセキュリティゾーンを定義するステップと、セキュリティゾーンの各々を、GPUによって提供される複数のGPUプログラミングインタフェースのうちの対応する1つに割り当てるステップであって、GPUプログラミングインタフェースの各々は、対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を受け取るためのものであり、作業命令は、GPUによって実行されるべき命令を備える、ステップと、複数のGPUプログラミングインタフェースによって受け取られた作業命令の実行を、別個のセキュアなメモリ領域を使用して制御するステップであって、各セキュアなメモリ領域は、複数のセキュリティゾーンのうちの1つに割り振られる、ステップと、を備える。

【０００５】

別の実施形態は、グラフィックス処理装置へのセキュアなアクセス制御を提供するためのコンピュータプログラムである。コンピュータプログラムは、プロセッサによる実行のために、コンピュータ可読媒体で実施される。コンピュータプログラムは、グラフィックス処理装置(GPU)へのアクセスを制御するための複数のセキュリティゾーンを定義することと、セキュリティゾーンの各々を、GPUによって提供される複数のGPUプログラミングインタフェースのうちの対応する1つに割り当てることであって、GPUプログラミングインタフェースの各々は、対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を受け取るためのものであり、作業命令は、GPUによって実行されるべき命令を備えることと、複数のGPUプログラミングインタフェースによって受け取られた作業命令の実行を、別個のセキュアなメモリ領域を使用して制御することであって、各セキュアなメモリ領域は、複数のセキュリティゾーンのうちの1つに割り振られることとをするように構成されるロジックを備える。

【０００６】

別の実施形態は、グラフィックス処理装置(GPU)へのセキュアなアクセス制御を提供す

るためのシステムである。システムは、複数のGPUプログラミングインタフェースおよびコマンドプロセッサを有するGPUを備える。各GPUプログラミングインタフェースは、複数のセキュリティゾーンのうちの相異なる1つに動的に割り当てられ、対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を受け取るように構成される。作業命令は、GPUによって実行されるべき命令を備える。コマンドプロセッサは、複数のGPUプログラミングインタフェースと通信し、複数のGPUプログラミングインタフェースによって受け取られた作業命令の実行を、別個のセキュアなメモリ領域を使用して制御するように構成される。各セキュアなメモリ領域は、複数のセキュリティゾーンのうちの1つに割り振られる。

【０００７】

図面では、別段に規定されていない限り、様々な図の全体を通して、同様の参照番号は同様の部分を指す。「102A」または「102B」などの文字指定を伴う参照番号の場合、文字指定は、同じ図に存在する2つの同様の部分または要素を区別することができる。参照番号がすべての図において同じ参照番号を有するすべての部分を包含することが意図されるとき、参照番号に対する文字指定は省略される場合がある。

【図面の簡単な説明】

【０００８】

【図１】グラフィックス処理装置(GPU)へのセキュアなアクセス制御を提供するためのシステムの一実施形態を示すブロック図である。

【図２】4つのセキュリティゾーンならびに対応するGPUプログラミングインタフェースおよび割り振られたメモリ領域を用いて構成される、図1のシステムの一実施形態を示すブロック図である。

【図３】GPUへのセキュアなアクセス制御を提供するための、図1のシステムで実施される方法の一実施形態を示すフローチャートである。

【図４】図1のシステムを組み込むための例示的なポータブルコンピューティングデバイスを示すブロック図である。

【発明を実施するための形態】

【０００９】

「例示的」という言葉は、「例、事例、または例示としての役割を果たすこと」を意味するように本明細書で使用される。「例示的な」ものとして本明細書で説明するいずれの態様も、必ずしも他の態様よりも好ましいか、または有利であると解釈されるわけではない。

【００１０】

本明細書では、「アプリケーション」という用語は、オブジェクトコード、スクリプト、バイトコード、マークアップ言語ファイル、およびパッチなどの実行可能なコンテンツを有するファイルも含み得る。加えて、本明細書で言及する「アプリケーション」は、開封される必要があり得るドキュメント、またはアクセスされる必要がある他のデータファイルなどの本質的に実行可能ではないファイルも含み得る。

【００１１】

「コンテンツ」という用語は、オブジェクトコード、スクリプト、バイトコード、マークアップ言語ファイル、およびパッチなどの実行可能なコンテンツを有するファイルを含む場合もある。加えて、本明細書で言及される「コンテンツ」は、開封される必要があり得るドキュメント、またはアクセスされる必要がある他のデータファイルなどの、本質的に実行可能ではないファイルを含む場合もある。

【００１２】

本明細書で使用されるように、「構成要素」、「データベース」、「モジュール」、「システム」などの用語は、ハードウェア、ファームウェア、ハードウェアとソフトウェアの組合せ、ソフトウェア、または実行中のソフトウェアのいずれかである、コンピュータ関連のエンティティを指すものとする。たとえば、構成要素は、プロセッサ上で動作するプロセス、プロセッサ、オブジェクト、実行ファイル、実行スレッド、プログラム、およ

び/またはコンピュータであり得るが、これらに限定されない。例として、コンピューティングデバイス上で動作しているアプリケーションもしくはモジュールとコンピューティングデバイスの両方が、構成要素であり得る。1つもしくは複数の構成要素は、プロセスおよび/または実行スレッド内に存在してよく、1つの構成要素を1つのコンピュータに局在化すること、および/または2つ以上のコンピュータ間に分散することが可能である。加えて、これらの構成要素は、様々なデータ構造が記憶されている様々なコンピュータ可読媒体から実行することができる。構成要素は、1つまたは複数のデータパケット(たとえば、信号によって、ローカルシステム、分散システム中の別の構成要素と、かつ/または、インターネットなどのネットワークにわたって他のシステムと対話する、1つの構成要素からのデータ)を有する信号に従うなどして、ローカルプロセスおよび/またはリモートプロセスによって通信することができる。

【００１３】

「ポータブルコンピューティングデバイス」(「PCD」)は、たとえば、セルラー電話、衛星電話、ページャ、携帯情報端末、スマートフォン、ナビゲーションデバイス、スマートブックすなわち電子リーダー、メディアプレーヤ、タブレットコンピュータ、ラップトップコンピュータ、または他のそのようなデバイスを備え得る。

【００１４】

図1は、グラフィックス処理装置(GPU)102へのセキュアなアクセス制御を提供するために、たとえば、PCD(図4)に組み込まれ得るシステム100である。システム100は、1つもしくは複数のアプリケーション118および/または1つもしくは複数のオペレーティングシステム120と関連した、グラフィックス命令および/または計算命令を実行するための、1つもしくは複数の中央処理装置(CPU)402および1つもしくは複数のGPU102を備える。CPU402およびGPU102は、ハードウェアバス、接続、または他のインタフェースによって接続され得る。システム100は、GPUアクセス制御に、複数のセキュリティおよび/またはコンテンツ保護ゾーン(「セキュリティゾーン」)を提供する。

【００１５】

GPUのハードウェアおよび/またはソフトウェアは、複数のGPUプログラミングインタフェース104をCPU402に提供する。GPUプログラミングインタフェース104の各々は、相異なるセキュリティゾーンの中に常駐する1つまたは複数のアプリケーション118およびオペレーティングシステム120によって発行された作業命令を受け取るための、相異なるセキュリティゾーンに関連付けられている。セキュリティゾーンは、セキュリティポリシーマネージャ106によって、任意の望ましいセキュリティユースケースに基づいて定義され得る。各セキュリティゾーンは、別個のGPUプログラミングインタフェース104に割り当てられ、別個のメモリ領域に割り振られる。図1の実施形態では、システム100は、対応するセキュアなメモリ領域を伴う4つのGPUプログラミングインタフェース104a、104b、104c、および104dを備える。コンテキストバンク122a、122b、122c、および122dは、対応するセキュリティゾーン内の作業命令を実行するためのメモリリソースとして割り振られ得る。この点について、セキュアなメモリ領域は、システムメモリ管理装置(SMMU)116内に、コンテキストバンク122a、122b、122c、および122dを使用してハードウェアで実現される保護を伴う、隔離されたアドレス空間を備え得る。各コンテキストバンク122は、固有の、セキュアかつ隔離されたアドレス空間を実現するための、ハードウェアリソースを備え得る。

【００１６】

作業命令は、GPU102によって実行されるべきグラフィックス命令を備える。アプリケーション118が、GPU102にリソースを要求する任意の適当なアプリケーションを備え得ることを諒解されたい。オペレーティングシステム120は、たとえば、ハイレベルオペレーティングシステム(HLOS)などの、1つまたは複数のオペレーティングシステムを備え得る。一実施形態では、GPU102は、特殊構成のコンテンツ保護アプリケーション(たとえば、オペレーティングシステム120と関連したコンテンツ保護アプリケーション117またはコンテンツ保護カーネル119)から作業命令を受け取ることができる。

【００１７】

当業者には、GPUプログラミングインタフェース104が制御リソースを備えることが諒解されよう。一実施形態では、制御リソースは、対応するセキュリティゾーン内のアプリケーションからの作業命令を受領するためのレジスタリソース、および作業命令の実行の完了または失敗のステータスを示すための1つまたは複数の割込みリソースを、備え得る。GPUプログラミングインタフェース104は、たとえば、仮想マシンのサイズ決定、およびセキュリティポリシーマネージャ106または信頼されるゾーン構成要素108(すなわち、システム100内の「信頼のルート」)がGPU102へのアクセスを必要とするかどうかに基づいて、仮想マシンマネージャ(VMM)110によって構成可能であり得る。システム100内の「信頼のルート」は、セキュリティポリシーマネージャ106のシステムセキュリティポリシーに基づいて、GPUプログラミングインタフェース104を指定のセキュリティゾーンに動的に割り当て、これは、セキュアなユースケースの開始時において起こり得る。

【００１８】

先に述べたように、各GPUプログラミングインタフェース104は、特有の使用シナリオに応じて、対応するコンテキストバンク122にメモリマップされ得、その場合、それらは、メモリマップされた入力/出力(MIMO)レジスタを備え得る。GPUプログラミングインタフェース104は、1つまたは複数の仮想マシンすなわちVMM110に直接割当て可能であり得る。各GPUプログラミングインタフェース104が、システムメモリ管理装置(SMMU)116を使用してハードウェアで実現されるアクセス制御によって保護され得ることを、さらに諒解されたい。このようにして、各セキュリティゾーンは、特有のユースケースが開始した後、GPUプログラミングインタフェース104に関連付けられたレジスタリソースおよび割込みリソースを介した完全な制御を有し得る。

【００１９】

さらに図1に示すように、GPU102は、複数のGPUプログラミングインタフェース104と通信するコマンドプロセッサ114を含み得る。コマンドプロセッサ114は、GPUプログラミングインタフェース104に関連付けられたコンテンツ待ち行列204(図2)の中から、作業命令を選択するように構成され得る。この点について、コマンドプロセッサ114は、たとえば、GPUスケジューリングポリシーに基づいて、どの作業命令を処理するかを決定し得、次いで、セキュリティゾーンに割り振られた適切なコンテキストバンク122を使用して、作業命令の実行を制御し得る。

【００２０】

一実施形態では、多数のセキュリティゾーンが、CPU402上で同時に動作しているアプリケーション118によって、並行に管理され得ることを諒解されたい。各アプリケーション118は、関連付けられたコマンド待ち行列を直接管理し得る。セキュリティゾーンのうちの1つまたは複数は、また、セキュアおよび/または非セキュアであり得る。アプリケーション118(および、その関連付けられたメモリ)がそれに基づいてセキュアおよび/または非セキュアとなるセキュリティポリシーは、GPU102を制御しているプロセッサ(たとえば、CPU402)によって決定され得る。CPU402によって実行および/または管理されるセグメント化は、たとえば、以下の例示的な方法、すなわち、(1)ハイパーバイザレイヤ(たとえば、多数のゲストオペレーティングシステム120を管理するためのソフトウェアレイヤ)による隔離、および/または(2)メモリアクセスおよびGPUコマンドを追跡するとともに要求のソースを隔離するための、命令のさらなるハードウェアタグ付けを介して、信頼されるハードウェアと信頼されないハードウェアとの間の分離を制御し得る、ハードウェアのセキュアなドメインを定義するハードウェアプロセス構築(たとえば、ARMアーキテクチャで使用される「トラストゾーン」セキュリティ拡張)を含む、様々な方法で実施され得ることをさらに諒解されたい。ハイパーバイザレイヤは、制御ユニットのメモリアクセスの隔離に限られ得る、ハードウェア上でのソフトウェアの抽象化を備えることができる。

【００２１】

システム101は、GPUアクセス制御に関係する任意の望ましいセキュリティユースケースをサポートし得る。たとえば、システム101は、デジタル著作権管理(DRM)などのユースケース、および、いくつかの例を挙げれば、バンキング、診療記録、指紋などを含むアプリ

ケーションのための秘密のデータへのアクセスを制御することをサポートし得る。一実施形態では、システム101は、それぞれのセキュリティゾーンに関連付けられた4つの例外レベルを提供し得、各レベルは、相異なるまたは格付けされたセキュリティ特権を有する。第1の例外レベル(EL0)は、ユーザモードにゆるく対応し得る。第2の例外レベル(EL1)は、カーネルモードに対応し得る。第3の例外レベル(EL2)は、ハイパーバイザに対応し得る。第4の例外レベル(EL3)は、最高の特権のあるセキュリティゾーンを備える信頼されるゾーン構成要素108に対応し得る。

【００２２】

図2は、4つのセキュリティゾーン202a、202b、202c、および202dを伴う例示的なユースケースを示す。セキュリティゾーン202aは、第1のHLOSカーネル119aに対して構成されコンテンツ待ち行列204aを有する、GPUプログラミングインタフェース104aに割り当てられる。コンテキストバンク122aは、セキュリティゾーン202aに割り振られる。セキュリティゾーン202bは、コンテンツ保護アプリケーション117に対して構成されコンテンツ待ち行列204bを有する、GPUプログラミングインタフェース104bに割り当てられる。コンテキストバンク122bは、セキュリティゾーン202bに割り振られる。セキュリティゾーン202cは、第2のHLOSカーネル119bに対して構成されコンテンツ待ち行列204cを有する、GPUプログラミングインタフェース104cに割り当てられる。コンテキストバンク122cは、セキュリティゾーン202cに割り振られる。セキュリティゾーン202dは、信頼されるゾーン構成要素108に関連付けられコンテンツ待ち行列204dを有する、GPUプログラミングインタフェース104dに割り当てられる。信頼されるゾーン構成要素108は、信頼されるコンテキストバンク122dを所有し、信頼されるコンテキストバンク122dは、信頼されるゾーン構成要素108だけに認識できる隔離されたアドレス空間を備える。

【００２３】

セキュリティゾーン202が、適切なアプリケーション118を伴う任意の望ましいユースケースをサポートし得ることを諒解されたい。たとえば、一実施形態では、セキュリティゾーン202aは、ゲーミングアプリケーションおよび関連した仮想メモリ空間に関連付けられ得る。セキュリティゾーン202bは、ビデオアプリケーションおよび関連した高価なビデオ仮想メモリ空間に関連付けられ得る。セキュリティゾーン202cは、ブラウザアプリケーションおよび関連した仮想メモリ空間に関連付けられ得る。セキュリティゾーン202dは、バンキングアプリケーションおよび関連した仮想メモリ空間に関連付けられ得る。

【００２４】

図2にさらに示すように、各GPUプログラミングインタフェース104a、104b、104c、および104dは、別個のデータストリーム識別子(それぞれ、SID206a、SID206b、SID206c、およびSID206d)によって識別され得る。作業命令を適切なGPUプログラミングインタフェースへ注入するために、ストリーム識別子が、たとえば、CPU402によって使用され得ることを諒解されたい。コマンドプロセッサ114は、ストリーム識別子に従って作業命令を選択し得、SMMU116は、ストリーム識別子に従ってメモリリソースを管理し得る。

【００２５】

図3は、システム100内のGPUアクセス制御を提供するための方法300の一実施形態を示す。ブロック301において、複数のセキュリティゾーン202が、GPU104によって実行されるべき命令に対して定義される。セキュリティゾーン202は、セキュリティポリシーマネージャ106、信頼されるゾーン構成要素108、またはシステム101と関連した他のソフトウェアおよび/もしくはハードウェアによって定義され得る。一実施形態では、セキュリティゾーン202のうちの2つ以上は、並行に管理され得る。さらに、いくつかの実施形態では、セキュアなゾーンと非セキュアなゾーンの両方が実装され得ることを諒解されたい。ブロック303において、各セキュリティゾーン202は、別個のGPUプログラミングインタフェース104に割り当てられ、別個のメモリ領域(たとえば、コンテキストバンク122a、122b、122c、および122d)に割り振られる。先に述べたように、GPUプログラミングインタフェース104は、たとえば、仮想マシンのサイズ決定、およびセキュリティポリシーマネージャ106または信頼されるゾーン構成要素108がGPU104へのアクセスを必要とするかどうかに基づい

て、VMM110によって構成可能であり得る。一実施形態では、システム100内の「信頼のルート」は、セキュリティポリシーマネージャ106のシステムセキュリティポリシーに基づいて、GPUプログラミングインタフェース104を指定のセキュリティゾーンに動的に割り当て、これは、セキュアなユースケースの開始時において起こり得る。ブロック305において、セキュリティゾーン202のうちの1つの中に常駐しているアプリケーション118は、作業命令を適切なGPUプログラミングインタフェース104に発行し得る。CPU402は、ストリーム識別子206を使用して作業命令を注入し得る。ブロック307において、作業命令は、対応するセキュリティゾーン202に基づいて、適切なGPUプログラミングインタフェース104に提供され得る。ブロック309において、コマンドプロセッサ114および/またはSMMU116は、対応するセキュリティゾーン202およびGPUプログラミングインタフェース104に割り振られた別個のメモリ領域(たとえば、コンテキストバンク122a、122b、122c、および122d)を使用して、作業命令の実行を制御し得る。

【００２６】

当業者には、代替のユースケースが実施され得ることが諒解されよう。信頼されるゾーン構成要素108を伴う例示的な「信頼されるゾーン」のユースケースが、GPUアクセス制御の機能性のいくつかの態様をさらに示すために記載される。信頼されるゾーン構成要素108は、信頼されるコンテキストバンク122d(図2)の所有権を主張し得る。SMMUコンテキストバンクに関連付けられたページテーブルが、構成され得る。ページテーブルは、信頼されるゾーン(すなわち、セキュリティゾーン202d)によって所有され、別のセキュリティゾーン202a、202b、または202cと共有されるバッファを除いて、いかなる他の構成要素にも認識できないバッファが実装され(populated with)得る。セキュリティポリシーは、信頼されるゾーン構成要素108が、GPUプログラミングインタフェース104dの所有権を主張することを特定し得る。SID206dは、信頼されるコンテキストバンク122dにマップするセキュアなSIDとして、構成され得る。動作において、信頼されるゾーン構成要素108は、要求をコマンド待ち行列204dに注入することによって、GPU作業命令を発行する。

【００２７】

作業命令がコマンド待ち行列204d内に注入されると、コマンドプロセッサ114は、処理を開始するように(たとえば、「ドアベル」レジスタによって)促され得る。コマンドプロセッサ114は、どの作業命令にとりかかるべきかを選択するために、GPUプログラミングインタフェース104dをスキャンする。作業命令が処理され得、一方、SID206dがGPUプログラミングインタフェース104dに従って設定される。SID206dは、適切なメモリ保護をセットアップする特定のコンテキストバンクを選択する。作業が首尾よく完了されると、またはエラーの場合に、コマンドプロセッサ114がCPU402に割込みをかけ、および/または信頼されるゾーン構成要素108が割込みを受け取る。作業命令の完了の後、信頼されるゾーン構成要素108は、さらなる作業命令を発行し得る。割込みがエラーを示す場合、信頼されるゾーン構成要素108は、さらなる処理をやめてもよく、エラー処理ポリシーに従ってエラーを処理し得る。

【００２８】

図4は、例示的なポータブルコンピューティングデバイス(PCD)400に組み込まれた、上述のシステム100を示す。システム100のいくつかの構成要素はSoC322上に含まれるが、他はオフチップに存在し得ることを諒解されたい。SoC322は、個別に製造されるとともにポータブルコンピューティングデバイス400用の設計物の中に組み込まれ得る、任意の組込みシステムを備え得る。

【００２９】

図示のように、PCD400は、マルチコアCPU402Aを含むSoC322を含む。マルチコアCPU402Aは、第0のコア410、第1のコア412、および第Nのコア414を含み得る。ディスプレイコントローラ328およびタッチスクリーンコントローラ330は、CPU402上に存在し得る、またはCPU402に接続され得る、GPU104に結合され得る。一方、SoC322の外部にあるタッチスクリーンディスプレイ108は、ディスプレイコントローラ328およびタッチスクリーンコントローラ330に結合され得る。

【００３０】
図4はさらに、ビデオエンコーダ334、たとえば位相反転線(PAL)エンコーダ、順次式カラーメモリ(SECAM)エンコーダ、または全米テレビジョン方式委員会(NTSC)エンコーダが、マルチコアCPU402Aに結合されること示す。さらに、ビデオ増幅器336は、ビデオエンコーダ334およびタッチスクリーンディスプレイ108に結合される。また、ビデオポート338はビデオ増幅器336に結合される。図4に示すように、ユニバーサルシリアルバス(USB)コントローラ340ならびに他のトレースシンク109およびトレースダンプ110は、マルチコアCPU402Aに結合され得る。また、USBポート342がUSBコントローラ340に結合される。メモリ404Aおよび加入者識別モジュール(SIM)カード346も、マルチコアCPU402Aに結合され得る。

【００３１】
さらに、図4に示されるように、デジタルカメラ348が、マルチコアCPU402Aに結合され得る。例示的な態様では、デジタルカメラ348は、電荷結合デバイス(CCD)カメラまたは相補型金属酸化物半導体(CMOS)カメラである。

【００３２】
図4にさらに示されたように、ステレオオーディオコーダ-デコーダ(コーデック)350は、マルチコアCPU402Aに結合され得る。その上、オーディオ増幅器352が、ステレオオーディオコーデック350に結合され得る。例示的な態様では、第1のステレオスピーカ354および第2のステレオスピーカ356が、オーディオ増幅器352に結合される。図4は、マイクロフォン増幅器358もステレオオーディオコーデック350に結合され得ることを示す。加えて、マイクロフォン360は、マイクロフォン増幅器358に結合され得る。特定の態様では、周波数変調(FM)ラジオチューナ362が、ステレオオーディオコーデック350に結合され得る。また、FMアンテナ364が、FMラジオチューナ362に結合される。さらに、ステレオヘッドフォン366が、ステレオオーディオコーデック350に結合され得る。

【００３３】
図4はさらに、無線周波(RF)トランシーバ368がマルチコアCPU402Aに結合される場合があることを示す。RFスイッチ370は、RFトランシーバ368およびRFアンテナ372に結合され得る。図4に示されるように、キーパッド204が、マルチコアCPU402Aに結合され得る。また、マイクロフォン付きモノヘッドセット376が、マルチコアCPU402Aに結合され得る。さらに、バイブレータデバイス378が、マルチコアCPU402Aに結合され得る。

【００３４】
図4はまた、電源380がSoC322に結合され得ることを示す。特定の態様では、電源380は、電力を必要とするPCD400の様々な構成要素に電力を供給する直流(DC)電源である。さらに、特定の態様では、電源は、充電式DCバッテリー、または交流(AC)電源に接続されたAC-DC変換器から得られるDC電源である。

【００３５】
図4は、PCD400がデータネットワーク、たとえばローカルエリアネットワーク、パーソナルエリアネットワーク、または任意の他のネットワークにアクセスするために使用され得るネットワークカード388も含み得ることをさらに示す。ネットワークカード388は、Bluetooth(登録商標)ネットワークカード、WiFiネットワークカード、パーソナルエリアネットワーク(PAN)カード、パーソナルエリアネットワーク超低電力技術(PeANUT)ネットワークカード、または当技術分野でよく知られている任意の他のネットワークカードであり得る。さらに、ネットワークカード388は、チップに組み込まれる場合があり、すなわち、ネットワークカード388は、チップ内のフルソリューションであり得るし、個別のネットワークカード388ではない場合がある。

【００３６】
図4に描写されたように、タッチスクリーンディスプレイ108、ビデオポート338、USBポート342、カメラ348、第1のステレオスピーカ354、第2のステレオスピーカ356、マイクロフォン360、FMアンテナ364、ステレオヘッドフォン366、RFスイッチ370、RFアンテナ372、キーパッド374、モノヘッドセット376、バイブレータ378、および電源380は、オンチッ

プシステム322の外部にある場合がある。

【００３７】

特定の態様では、本明細書で説明する方法ステップの1つまたは複数は、図1に示すシステム100に関して上記で説明したモジュールなど、コンピュータプログラム命令としてメモリ404Aに記憶され得る。

【００３８】

これらの命令は、本明細書で説明される方法を実行するためにマルチコアCPU402Aおよび/またはGPU102によって実行され得る。さらに、マルチコアCPU402A、GPU102、PCD400のメモリ404A、またはそれらの組合せが、本明細書で説明する方法ステップのうちの1つまたは複数を実行するための手段として働き得る。

【００３９】

本発明が記載されたように機能するために、本明細書に記載されたプロセスまたはプロセスフロー内のあるステップが他のステップよりも先行するのは当然である。しかしながら、そのような順序またはシーケンスが本発明の機能を変えない場合、本発明は記載されたステップの順序に限定されない。すなわち、本発明の範囲および趣旨から逸脱することなく、あるステップは、他のステップの前に実施されるか、後に実施されるか、または他のステップと並行して(実質的に同時に)実施される場合があることを認識されたい。いくつかの例では、ある特定のステップは、本発明から逸脱することなく、省略されるか、または実施されない場合がある。さらに、「その後」、「次いで」、「次に」などの言葉は、ステップの順番を限定することを意図していない。これらの言葉は、単に例示的な方法の説明を通じて読者を導くために使用されている。

【００４０】

加えて、プログラミングの当業者は、たとえば本明細書内のフローチャートおよび関連する説明に基づいて、コンピュータコードを書くか、または適切なハードウェアおよび/もしくは回路を識別して、開示された発明を容易に実施することができる。

【００４１】

したがって、特定の1組のプログラムコード命令または詳細なハードウェアデバイスの開示が、本発明をどのように製作し使用すべきかについて適切に理解するために必要であるとは見なされない。特許請求されるコンピュータ実施プロセスの発明性のある機能は、上記の説明において、かつ様々なプロセスフローを示すことができる図面とともに、より詳細に説明される。

【００４２】

1つまたは複数の例示的な態様では、記載した機能は、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施され得る。ソフトウェアで実施される場合、機能は、1つまたは複数の命令もしくはコードとして、コンピュータ可読媒体上に記憶されるか、またはコンピュータ可読媒体上で送信され得る。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む、コンピュータ記憶媒体と通信媒体の両方を含む。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。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、または、命令もしくはデータ構造の形態で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され得、コンピュータによってアクセスされ得る任意の他の媒体を備えることができる。

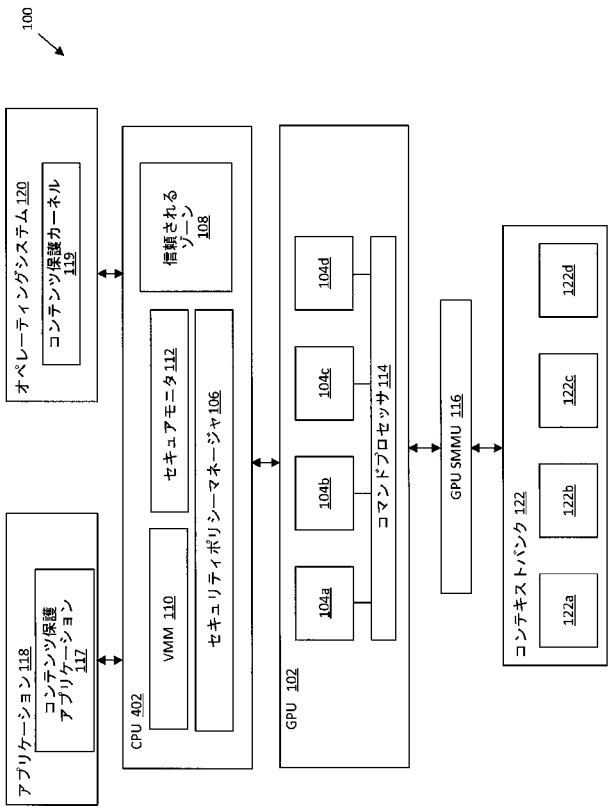
【００４３】

また、任意の接続部が適切にコンピュータ可読媒体と呼ばれる。たとえば、ソフトウェアが、ウェブサイト、サーバ、または他の遠隔ソースから、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用して伝送される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、マイクロ波などのワイヤレス技術は、媒体の定義に含まれる。

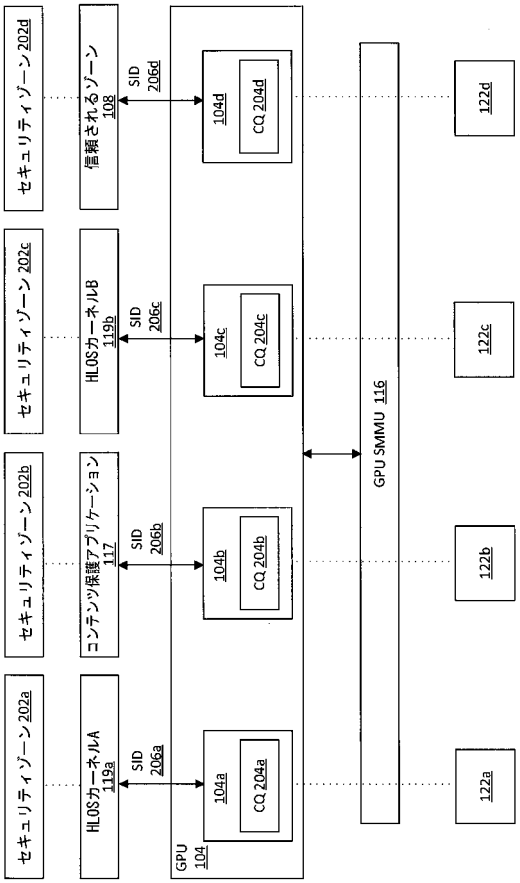
【００４４】
ディスク(disk)およびディスク(disc)は、本明細書で使用されるときに、コンパクトディスク(disc)(「CD」)、レーザディスク(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(「DVD」)、フロッピディスク(disk)、およびブルーレイディスク(disc)を含み、ディスク(disk)は、通常はデータを磁気的に再生し、ディスク(disc)は、レーザを用いてデータを光学的に再生する。前述の組合せも、コンピュータ可読媒体の範囲内に含まれるべきである。
【符号の説明】
【００４５】
100 システム
101 システム
102 グラフィックス処理装置
104 GPUプログラミングインタフェース
104 GPU
106 セキュリティポリシーマネージャ
108 タッチスクリーンディスプレイ
108 信頼されるゾーン構成要素
109 トレースシンク
110 仮想マシンマネージャ
110 トレースダンプ
114 コマンドプロセッサ
116 システムメモリ管理装置
117 コンテンツ保護アプリケーション
118 アプリケーション
119 コンテンツ保護カーネル
120 オペレーティングシステム
122 コンテキストバンク
202 セキュリティゾーン
204 コンテンツ待ち行列
204 キーパッド
206 ストリーム識別子
322 SoC
328 ディスプレイコントローラ
330 タッチスクリーンコントローラ
334 ビデオエンコーダ
336 ビデオ増幅器
338 ビデオポート
340 ユニバーサルシリアルバスコントローラ
342 USBポート
346 加入者識別モジュールカード
348 デジタルカメラ
350 ステレオオーディオコーデック
352 オーディオ増幅器
354 第1のステレオスピーカ
356 第2のステレオスピーカ
358 マイクロフォン増幅器
360 マイクロフォン
362 周波数変調ラジオチューナ
364 FMアンテナ
366 ステレオヘッドフォン

368　無線周波トランシーバ
370　RFスイッチ
372　RFアンテナ
374　キーパッド
376　マイクロフォン付きモノヘッドセット
378　バイブレータデバイス
380　電源
388　ネットワークカード
400　ポータブルコンピューティングデバイス
402　中央処理装置
402A　マルチコアCPU
404A　メモリ
410　第0のコア
412　第1のコア
414　第Nのコア

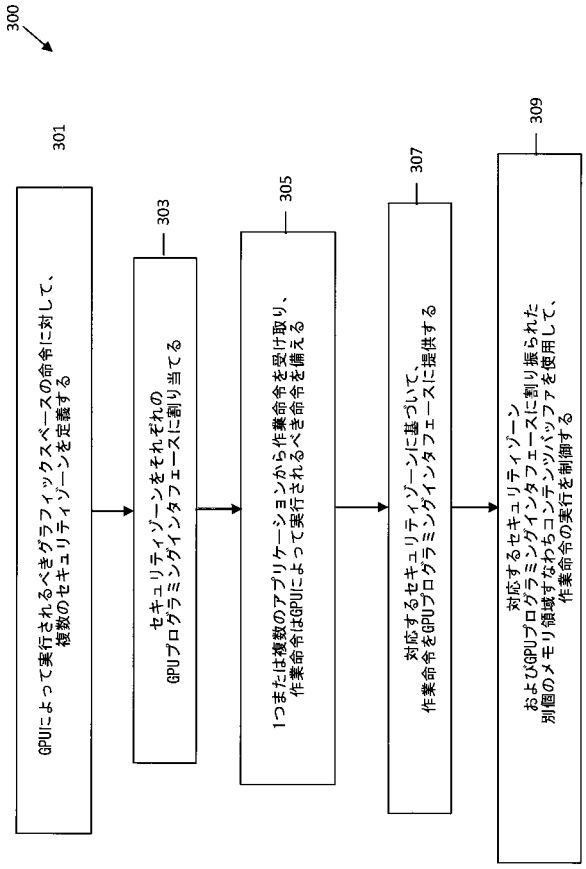
【図１】



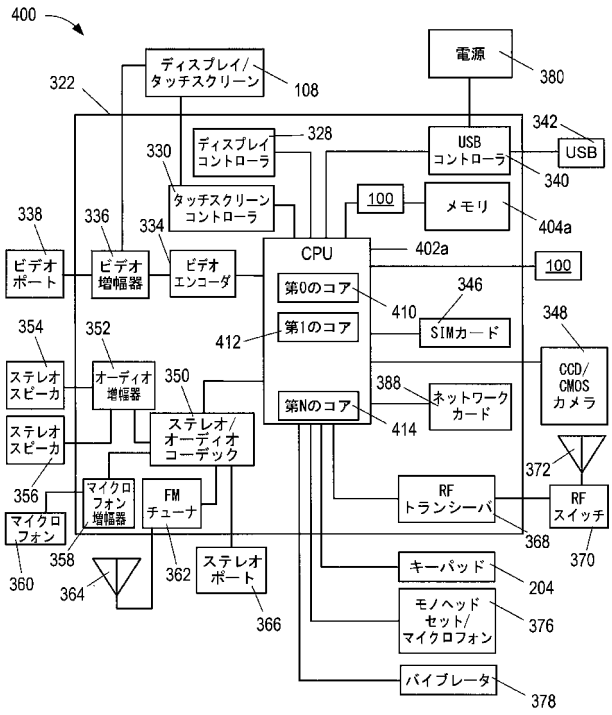
【図２】



【図３】



【図４】



【手続補正書】
【提出日】平成27年4月29日(2015.4.29)
【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装置へのセキュアなアクセス制御を提供するための方法であって、
グラフィックス処理装置(GPU)への共通の通信チャネルを介するアクセスを制御するための複数のセキュリティゾーンを定義するステップと、
前記セキュリティゾーンの各々を、前記GPUによって提供される複数のGPUプログラミングインターフェースのうちの対応する1つに割り当てるステップであって、前記GPUプログラミングインターフェースの各々は、前記対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を前記共通の通信チャネルを介して受け取るためのものであり、前記作業命令は、前記GPUによって実行されるべき命令を備える、ステップと、
前記複数のGPUプログラミングインターフェースによって受け取られた前記作業命令の実行を、別個のセキュアなメモリ領域を使用して制御するステップであって、各セキュアなメモリ領域は、前記複数のGPUプログラミングインターフェースのうちの1つに割り振られる、ステップと
を備える方法。
【請求項２】
前記GPUプログラミングインターフェースは、前記対応するGPUプログラミングインター

フェースによって受け取られた作業命令を記憶するための、それぞれのコマンド待ち行列を備える、請求項1に記載の方法。
【請求項３】
前記作業命令は、前記セキュリティゾーンに従って、前記対応するGPUプログラミングインターフェース内へ中央処理装置(CPU)によって注入される、請求項1に記載の方法。
【請求項４】
前記作業命令は、前記対応するGPUプログラミングインターフェースを識別するストリーム識別子を使用して注入される、請求項3に記載の方法。
【請求項５】
前記別個のメモリ領域は、セキュアなメモリ管理装置によって割り振られる、請求項1に記載の方法。
【請求項６】
前記別個のメモリ領域のうちの1つまたは複数は、前記セキュアなメモリ管理装置内の関連付けられたコンテキストバンクを使用してハードウェアで実現される保護を伴う、隔離されたアドレス空間を備える、請求項5に記載の方法。
【請求項７】
前記隔離されたアドレス空間は、2つ以上のオペレーティングシステムを管理するためのハイパーバイザソフトウェアレイヤ、および信頼されるハードウェアと信頼されないハードウェアとの間の分離のうちの、1つまたは複数によって実装される、請求項6に記載の方法。
【請求項８】
前記セキュリティゾーンのうちの2つ以上は、並行に管理される、請求項1に記載の方法。
【請求項９】
前記セキュリティゾーンのうちの1つまたは複数は、非セキュアなゾーンまたはセキュアなゾーンを備える、請求項1に記載の方法。
【請求項１０】
前記作業命令を発行する前記1つまたは複数のアプリケーションは、コンテンツ保護ゾーンアプリケーション、オペレーティングシステムと関連したコンテンツ保護ゾーンカーネル、ハイレベルオペレーティングシステムカーネル、および信頼されるゾーンセキュリティモニタのうちの1つまたは複数を備える、請求項1に記載の方法。
【請求項１１】
グラフィックス処理装置へのセキュアなアクセス制御を提供するためのシステムであって、
グラフィックス処理装置(GPU)への共通の通信チャネルを介するアクセスを制御するための複数のセキュリティゾーンを定義するための手段と、
前記セキュリティゾーンの各々を、前記GPUによって提供される複数のGPUプログラミングインターフェースのうちの対応する1つに割り当てるための手段であって、前記GPUプログラミングインターフェースの各々は、前記対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を前記共通の通信チャネルを介して受け取るためのものであり、前記作業命令は、前記GPUによって実行されるべき命令を備える、手段と、
前記複数のGPUプログラミングインターフェースによって受け取られた前記作業命令の実行を、別個のセキュアなメモリ領域を使用して制御するための手段であって、各セキュアなメモリ領域は、前記複数のGPUプログラミングインターフェースのうちの1つに割り振られる、手段と
を備えるシステム。
【請求項１２】
前記GPUプログラミングインターフェースは、前記対応するGPUプログラミングインターフェースによって受け取られた作業命令を記憶するための、それぞれの手段を備える、請

求項11に記載のシステム。
【請求項１３】
前記作業命令は、前記セキュリティゾーンに従って、前記対応するGPUプログラミングインターフェース内へ中央処理装置(CPU)によって注入される、請求項11に記載のシステム。
【請求項１４】
前記作業命令は、前記対応するGPUプログラミングインターフェースを識別するストリーム識別子を使用して注入される、請求項13に記載のシステム。
【請求項１５】
前記別個のメモリ領域は、セキュアなメモリ管理装置によって割り振られる、請求項11に記載のシステム。
【請求項１６】
前記別個のメモリ領域のうちの1つまたは複数は、前記セキュアなメモリ管理装置内の関連付けられたコンテキストバンクを使用してハードウェアで実現される保護を伴う、隔離されたアドレス空間を備える、請求項15に記載のシステム。
【請求項１７】
前記隔離されたアドレス空間は、2つ以上のオペレーティングシステムを管理するためのハイパーバイザソフトウェアレイヤ、および信頼されるハードウェアと信頼されないハードウェアとの間の分離のうちの、1つまたは複数によって実装される、請求項16に記載のシステム。
【請求項１８】
前記セキュリティゾーンのうちの2つ以上は、並行に管理される、請求項11に記載のシステム。
【請求項１９】
前記セキュリティゾーンのうちの1つまたは複数は、非セキュアなゾーンまたはセキュアなゾーンを備える、請求項11に記載のシステム。
【請求項２０】
前記作業命令を発行する前記1つまたは複数のアプリケーションは、コンテンツ保護ゾーンアプリケーション、オペレーティングシステムと関連したコンテンツ保護ゾーンカーネル、ハイレベルオペレーティングシステムカーネル、および信頼されるゾーンセキュリティモニタのうちの1つまたは複数を備える、請求項11に記載のシステム。
【請求項２１】
グラフィックス処理装置へのセキュアなアクセス制御を提供するための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、プロセッサによる実行のためにコンピュータ可読媒体において実施され、
グラフィックス処理装置(GPU)への共通の通信チャネルを介するアクセスを制御するための複数のセキュリティゾーンを定義することと、
前記セキュリティゾーンの各々を、前記GPUによって提供される複数のGPUプログラミングインターフェースのうちの対応する1つに割り当てることであって、前記GPUプログラミングインターフェースの各々は、前記対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を前記共通の通信チャネルを介して受け取るためのものであり、前記作業命令は、前記GPUによって実行されるべき命令を備えることと、
前記複数のGPUプログラミングインターフェースによって受け取られた前記作業命令の実行を、別個のセキュアなメモリ領域を使用して制御することであって、各セキュアなメモリ領域は、前記複数のGPUプログラミングインターフェースのうちの1つに割り振られることと
をするように構成されたロジックを備えるコンピュータプログラム。
【請求項２２】
前記GPUプログラミングインターフェースは、前記対応するGPUプログラミングインター

フェースによって受け取られた作業命令を記憶するための、それぞれのコマンド待ち行列を備える、請求項21に記載のコンピュータプログラム。
【請求項２３】
前記作業命令は、前記セキュリティゾーンに従って、前記対応するGPUプログラミングインターフェース内へ中央処理装置(CPU)によって注入される、請求項21に記載のコンピュータプログラム。
【請求項２４】
前記作業命令は、前記対応するGPUプログラミングインターフェースを識別するストリーム識別子を使用して注入される、請求項23に記載のコンピュータプログラム。
【請求項２５】
前記別個のメモリ領域は、セキュアなメモリ管理装置によって割り振られる、請求項21に記載のコンピュータプログラム。
【請求項２６】
前記別個のメモリ領域のうちの1つまたは複数は、前記セキュアなメモリ管理装置内の関連付けられたコンテキストバンクを使用してハードウェアで実現される保護を伴う、隔離されたアドレス空間を備える、請求項25に記載のコンピュータプログラム。
【請求項２７】
前記隔離されたアドレス空間は、2つ以上のオペレーティングシステムを管理するためのハイパーバイザソフトウェアレイヤ、および信頼されるハードウェアと信頼されないハードウェアとの間の分離のうちの、1つまたは複数によって実装される、請求項26に記載のコンピュータプログラム。
【請求項２８】
前記セキュリティゾーンのうちの2つ以上は、並行に管理される、請求項21に記載のコンピュータプログラム。
【請求項２９】
前記セキュリティゾーンのうちの1つまたは複数は、非セキュアなゾーンまたはセキュアなゾーンを備える、請求項21に記載のコンピュータプログラム。
【請求項３０】
前記作業命令を発行する前記1つまたは複数のアプリケーションは、コンテンツ保護ゾーンアプリケーション、オペレーティングシステムと関連したコンテンツ保護ゾーンカーネル、ハイレベルオペレーティングシステムカーネル、および信頼されるゾーンセキュリティモニタのうちの1つまたは複数を備える、請求項21に記載のコンピュータプログラム。
【請求項３１】
グラフィックス処理装置へのセキュアなアクセス制御を提供するためのシステムであって、
共通の通信チャネルを介するグラフィックス処理装置(GPU)と、
前記GPUによって提供される複数のGPUプログラミングインターフェースであって、各GPUプログラミングインターフェースは、複数のセキュリティゾーンのうちの相異なる1つに動的に割り当てられ、対応するセキュリティゾーンに関連付けられた1つまたは複数のアプリケーションによって発行された作業命令を前記共通の通信チャネルを介して受け取るように構成され、前記作業命令は、前記GPUによって実行されるべき命令を備える、複数のGPUプログラミングインターフェースと、
前記複数のGPUプログラミングインターフェースと通信するコマンドプロセッサであって、前記コマンドプロセッサは、前記複数のGPUプログラミングインターフェースによって受け取られた前記作業命令の実行を、別個のセキュアなメモリ領域を使用して制御するように構成され、各セキュアなメモリ領域は、前記複数のGPUプログラミングインターフェースのうちの1つに割り振られる、コマンドプロセッサと
を備えるシステム。
【請求項３２】

前記GPUプログラミングインターフェースは、前記対応するGPUプログラミングインターフェースによって受け取られた作業命令を記憶するための、それぞれのコマンド待ち行列を備える、請求項31に記載のシステム。

【請求項３３】

前記作業命令は、前記セキュリティゾーンに従って、前記対応するGPUプログラミングインターフェース内へ中央処理装置(CPU)によって注入される、請求項31に記載のシステム。

【請求項３４】

前記作業命令は、前記対応するGPUプログラミングインターフェースを識別するストリーム識別子を使用して注入される、請求項33に記載のシステム。

【請求項３５】

前記別個のメモリ領域は、セキュアなメモリ管理装置によって割り振られる、請求項31に記載のシステム。

【請求項３６】

前記別個のメモリ領域のうちの1つまたは複数は、前記セキュアなメモリ管理装置内の関連付けられたコンテキストバンクを使用してハードウェアで実現される保護を伴う、隔離されたアドレス空間を備える、請求項35に記載のシステム。

【請求項３７】

前記隔離されたアドレス空間は、2つ以上のオペレーティングシステムを管理するためのハイパーバイザソフトウェアレイヤ、および信頼されるハードウェアと信頼されないハードウェアとの間の分離のうちの、1つまたは複数によって実装される、請求項36に記載のシステム。

【請求項３８】

前記セキュリティゾーンのうちの2つ以上は、並行に管理される、請求項31に記載のシステム。

【請求項３９】

前記セキュリティゾーンのうちの1つまたは複数は、非セキュアなゾーンまたはセキュアなゾーンを備える、請求項31に記載のシステム。

【請求項４０】

前記作業命令を発行する前記1つまたは複数のアプリケーションは、コンテンツ保護ゾーンアプリケーション、オペレーティングシステムと関連したコンテンツ保護ゾーンカーネル、ハイレベルオペレーティングシステムカーネル、および信頼されるゾーンセキュリティモニタのうちの1つまたは複数を備える、請求項31に記載のシステム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/044776

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/71 G06F21/74
ADD. G06T1/20 G06T1/60

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 G06T

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.
X	US 2010/031342 A1 (VOGSLAND ROBIN O [US]) 4 February 2010 (2010-02-04) paragraphs [0002], [0003], [0005] - [0010], [0022], [0030] - [0038], [0045], [0051] - [0052], [0060] - [0062] figures 1, 2, 4	1-40
A	US 2011/265183 A1 (WU ZHIXUE [GB] ET AL) 27 October 2011 (2011-10-27) paragraphs [0101] - [0105,] figure 3B	1-40

☐ 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
24 September 2014	01/10/2014

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	Volpato, Gian Luca

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/044776

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010031342 A1	04-02-2010	NONE	
US 2011265183 A1	27-10-2011	CN 102754077 A	24-10-2012
		EP 2513789 A2	24-10-2012
		US 2011265183 A1	27-10-2011
		US 2014032893 A1	30-01-2014
		WO 2011075484 A2	23-06-2011

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,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,LT,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 アゼディン・トウズニ
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者 ウィリアム・トーッツースキー
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

Ｆターム(参考) 5B017 AA01 BA01 BB02 CA01