(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7471230号
(P7471230)

(45)発行日　令和6年4月19日(2024.4.19)

(24)登録日　令和6年4月11日(2024.4.11)

(51)国際特許分類

		FI		
Ｇ０６Ｆ	*9/455(2018.01)*	Ｇ０６Ｆ	9/455	１５０
Ｇ０６Ｆ	*9/48 (2006.01)*	Ｇ０６Ｆ	9/48	３００Ｚ

請求項の数　19　（全15頁）

(21)出願番号　特願2020-555025(P2020-555025)
(86)(22)出願日　令和1年5月13日(2019.5.13)
(65)公表番号　特表2021-524077(P2021-524077A)
(43)公表日　令和3年9月9日(2021.9.9)
(86)国際出願番号　PCT/US2019/031930
(87)国際公開番号　WO2019/226380
(87)国際公開日　令和1年11月28日(2019.11.28)
審査請求日　令和4年4月14日(2022.4.14)
(31)優先権主張番号　15/990,310
(32)優先日　平成30年5月25日(2018.5.25)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　314015767
マイクロソフト テクノロジー ライセンシング，エルエルシー
アメリカ合衆国 ワシントン州 ９８０５２ レッドモンド ワン マイクロソフト ウェイ
(74)代理人　100079108
弁理士　稲葉 良幸
(74)代理人　100109346
弁理士　大貫 敏史
(74)代理人　100117189
弁理士　江口 昭彦
(74)代理人　100134120
弁理士　内藤 和彦
(74)代理人　100108213

最終頁に続く

(54)【発明の名称】　仮想化のためのプロセッサ特徴ＩＤ応答

(57)【特許請求の範囲】

【請求項１】

仮想化をサポートするための方法であって、

プロセッサ特徴ＩＤ値についてのゲストパーティションから発信された要求を物理プロセッサによって受信する前に、監視パーティションからのプロセッサ特徴ＩＤ値を前記物理プロセッサによって受信することであって、前記プロセッサ特徴ＩＤ値は、前記ゲストパーティションのポータビリティまたはパフォーマンスの強化のために、前記監視パーティションが取得したプロセッサ特徴ＩＤ値が変更なしで記憶されるべきか、または異なる値が記憶されるべきかどうか判定して決定され、前記プロセッサ特徴ＩＤ値は、仮想マシン制御構造（ＶＭＣＳ）又は仮想マシン制御ブロック（ＶＭＣＢ）について指定され、異なるプロセッサ特徴ＩＤ値が異なるＶＭＣＳ又はＶＭＣＢについて指定される、ことと、

前記物理プロセッサによってアクセス可能なハードウェアレジスタにプロセッサ特徴ＩＤ値を前記物理プロセッサによって記憶することと、

前記プロセッサ特徴ＩＤ値についてのゲストパーティションから発信された要求を前記物理プロセッサによって受信することと、

前記要求に応答して、要求されたプロセッサ特徴ＩＤ値を、前記物理プロセッサによってアクセス可能なハードウェアレジスタから前記ゲストパーティションに前記物理プロセッサによって、前記監視パーティションの介入なしに、提供することと、

を含む、方法。

【請求項２】

前記プロセッサ特徴ＩＤ値は、前記ゲストパーティション、ゲスト仮想プロセッサ、又はゲスト仮想プロセッサ仮想信頼レベルのうちの少なくとも１つのセットアップ動作と併せて前記監視パーティションから受信され、前記受信されたプロセッサ特徴ＩＤ値を前記物理プロセッサによって記憶することを含む、請求項１に記載の方法。

【請求項３】

前記ゲストパーティション、ゲスト仮想プロセッサ、又はゲスト仮想プロセッサ仮想信頼レベルのうちの少なくとも１つのセットアップ動作は、前記ゲストパーティション、ゲスト仮想プロセッサ、又はゲスト仮想プロセッサ仮想信頼レベルのうちの少なくとも１つの生成、インスタンス化、又は起動のうちの少なくとも１つを含む、請求項２に記載の方法。

【請求項４】

前記プロセッサ特徴ＩＤ値は、前記物理プロセッサによってネイティブにサポートされていない第１の特徴のサポート、又は前記物理プロセッサによってネイティブにサポートされている第２の特徴のサポートの欠如を表す、請求項１に記載の方法。

【請求項５】

前記プロセッサ特徴ＩＤ値は、前記物理プロセッサの製造元によって割り当てられた値とは異なる、請求項１に記載の方法。

【請求項６】

前記プロセッサ特徴ＩＤ値は、仮想プロセッサ又は仮想プロセッサの仮想信頼レベルコンテキストについて指定され、異なるプロセッサ特徴ＩＤ値が異なる仮想プロセッサ又は仮想プロセッサの仮想信頼レベルコンテキストについて指定される、請求項１に記載の方法。

【請求項７】

コンピューティングデバイスであって、

コンピューティングデバイスに動作を実行させるための命令を含む、命令を記憶および実行するようにそれぞれ構成されているメモリおよびプロセッサを備え、

前記動作は、

プロセッサ特徴ＩＤ値についてのゲストパーティションで実行するソフトウェアからの要求の前に、前記プロセッサ特徴ＩＤ値についてのゲストパーティションで実行するソフトウェアからの要求に応答して、前記プロセッサによって戻されるべき前記プロセッサ特徴ＩＤ値を監視パーティションにより判定することであって、前記ゲストパーティションのポータビリティまたはパフォーマンスの強化のために、前記監視パーティションが取得したプロセッサ特徴ＩＤ値が変更なしで記憶されるべきか、または異なる値が記憶されるべきかどうか判定することを含み、前記プロセッサ特徴ＩＤ値は、仮想マシン制御構造（ＶＭＣＳ）又は仮想マシン制御ブロック（ＶＭＣＢ）について指定され、異なるプロセッサ特徴ＩＤ値が異なるＶＭＣＳ又はＶＭＣＢについて指定される、ことと、

前記プロセッサがハードウェアレジスタに記憶し、後でハードウェアレジスタからの前記プロセッサ特徴ＩＤ値についての前記ソフトウェアからの要求に応答して、前記監視パーティションの介入なしに前記プロセッサが使用するために、前記監視パーティションにより、前記判定されたプロセッサ特徴ＩＤ値を前記プロセッサに提供することと、

を含むコンピューティングデバイス。

【請求項８】

前記動作は、前記プロセッサ特徴ＩＤ値についての前記ソフトウェアからの要求に応答して、前記プロセッサによる後の使用のために、前記提供されたプロセッサ特徴ＩＤ値を、前記プロセッサにより記憶することを含む、請求項７に記載のコンピューティングデバイス。

【請求項９】

前記提供されたプロセッサ特徴ＩＤ値は、前記プロセッサのプロセッサ特徴ＩＤレジスタに記憶される、請求項７に記載のコンピューティングデバイス。

【請求項１０】

前記動作は、
前記プロセッサ特徴ＩＤ値についての前記ソフトウェアからの要求を前記プロセッサにより受信することと、
前記要求に応答して、前記要求されたプロセッサ特徴ＩＤ値を、前記監視パーティションにより提供されたプロセッサ特徴ＩＤ値に基づいて、前記プロセッサにより提供することと、
を含む、請求項７に記載のコンピューティングデバイス。
【請求項１１】
前記プロセッサ特徴ＩＤ値は、ＣＰＵ　ＩＤ値を含む、請求項７に記載のコンピューティングデバイス。
【請求項１２】
前記プロセッサ特徴ＩＤ値は、前記プロセッサによってネイティブにサポートされていない少なくとも１つの特徴のサポートの表示、又は前記プロセッサによってネイティブにサポートされている少なくとも１つの他の特徴のサポートの欠如の表示を含む、請求項７に記載のコンピューティングデバイス。
【請求項１３】
コンピューティングデバイス上で仮想マシンを動作させるための方法であって、
前記コンピューティングデバイス上で実行される前記仮想マシンによって、前記仮想マシンによる使用のためにプロセッサ特徴ＩＤ値が取得されるべきであると判定することと、
前記仮想マシンによって、プロセッサ特徴ＩＤ値についての要求を前記コンピューティングデバイスのプロセッサに送信することと、
前記要求に応答して、前記要求されたプロセッサ特徴ＩＤ値を前記プロセッサから受信することと、
を含み、
前記受信されたプロセッサ特徴ＩＤ値は、前記プロセッサによりアクセス可能なハードウェアレジスタに記憶されている情報から、監視パーティションの介入なしに、前記プロセッサにより提供されており、
前記プロセッサによりアクセス可能なハードウェアレジスタに記憶されている情報は、前記プロセッサの前に、前記監視パーティションにより、前記仮想マシンのポータビリティまたはパフォーマンスの強化のために、前記監視パーティションが取得したプロセッサ特徴ＩＤ値が変更なしで記憶されるべきか、または異なる値が記憶されるべきかどうか判定して提供され、
前記プロセッサ特徴ＩＤ値は、仮想マシン制御構造（ＶＭＣＳ）又は仮想マシン制御ブロック（ＶＭＣＢ）について指定され、異なるプロセッサ特徴ＩＤ値が異なるＶＭＣＳ又はＶＭＣＢについて指定されている、方法。
【請求項１４】
前記要求されたプロセッサ特徴ＩＤ値は、仮想マシンエグジットなしに、前記プロセッサから受信される、請求項１３に記載の方法。
【請求項１５】
前記プロセッサ特徴ＩＤ値は、前記プロセッサによってネイティブにサポートされていない第１のプロセッサ特徴のサポートを表すか、又は前記プロセッサによってネイティブにサポートされている第２のプロセッサ特徴のサポートの欠如を表す、請求項１３に記載の方法。
【請求項１６】
前記プロセッサ特徴ＩＤ値は、前記仮想マシン、仮想プロセッサ又は仮想プロセッサの信頼レベルのうちの少なくとも１つに固有であり、異なるプロセッサ特徴ＩＤ値は、前記コンピューティングデバイス上の別の仮想マシン、別の仮想プロセッサ、又は別の仮想プロセッサの信頼レベルに固有である、請求項１３に記載の方法。
【請求項１７】
前記プロセッサ特徴ＩＤ値は、前記プロセッサの製造元によって割り当てられた値とは

異なる、請求項１３に記載の方法。
【請求項１８】
前記プロセッサ特徴ＩＤ値は、ＣＰＵ　ＩＤ値を含む、請求項１３に記載の方法。
【請求項１９】
前記プロセッサ特徴ＩＤ値は、前記仮想マシン、仮想プロセッサ、又は仮想プロセッサの信頼レベルのうちの少なくとも１つのセットアップ動作と併せて前記監視パーティションから受信され、前記仮想マシン、仮想プロセッサ、又は仮想プロセッサの信頼レベルのうちの前記少なくとも１つの前記セットアップ動作は、前記仮想マシン、仮想プロセッサ、又は仮想プロセッサの信頼レベルの生成、インスタンス化、又は起動のうちの少なくとも１つを含む、請求項１３に記載の方法。
【発明の詳細な説明】
【背景技術】
【０００１】
仮想化技術が様々な状況において採用されている。例えば、仮想化技術は、ゲストパーティションから物理コンピューティングリソースを抽出し、物理コンピューティングリソースの利用率を高めることを可能にし、物理デバイス間でゲストパーティションのポータビリティを可能にし、ゲストパーティション内で実行される悪意のあるおよび／または誤ったコードから物理コンピューティングリソースを保護し、秘密を保護し、セキュリティ要件またはポリシーを強化するなどのために採用されている。以前の仮想化技術では、特定の動作に応答して、ゲストエグジット（例えば、ゲストパーティションからハイパーバイザなどの監視パーティションへのプロセッサの制御の移行）が発生する場合がある。例えば、ゲストエグジットは、プロセッサ特徴ＩＤ情報についての要求に応答して発生する場合がある。
【発明の概要】
【０００２】
この概要は、以下の発明を実施するための形態でさらに説明される選定された概念を簡略化された形式で紹介するために提供される。この概要は、特許請求される主題の主要な特徴または本質的な特徴を特定することを意図しておらず、特許請求される主題の範囲を制限するために使用されることも意図していない。
【０００３】
簡単に言えば、開示される技術は、概して、仮想化技術を対象としている。開示される技術は、仮想マシン（ＶＭ）、仮想化アプリケーション、仮想化ベースのセキュリティ（ＶＢＳ）ユーザモードプロセス、ＶＢＳカーネルモードプロセス、または他のゲストパーティションによって、またはそれらから要求されたプロセッサ特徴ＩＤ情報をプロセッサによって提供することを含む。そのような情報は、例えば、ハイパーバイザなどの監視パーティションによって、プロセッサに事前に提供される情報に基づいて提供され得る。開示される技術はまた、例えば、そのような情報をプロセッサに提供する監視パーティションを含み、そのような情報を受信するゲストパーティションを含む。
【０００４】
開示される技術の他の態様および用途は、添付の図および説明を読んで理解することで認識されよう。
【図面の簡単な説明】
【０００５】
本開示の非限定的かつ非網羅的な例が、以下の図面を参照しながら説明される。図面では、同様の参照番号は、特に明記しない限り、様々な図全体を通して同様の部分を指す。これらの図面は、必ずしも縮尺どおりに描かれているわけではない。
【０００６】
本開示をよりよく理解するために、添付の図面と併せて読まれるべきである、以下の発明を実施するための形態について言及する。
【図１】開示される技術の態様による好適なコンピューティングデバイスの一例の物理図

を示すブロック図である。
【図２】開示される技術の態様による例示的なコンピューティングデバイスの論理図を示すブロック図である。
【図３】開示される技術の態様による例示的なプロセスを示す。
【図４】開示される技術の追加の態様による別の例示的なプロセスを示す。
【図５】開示される技術の他の態様によるさらに別の例示的なプロセスを示す。
【発明を実施するための形態】
【０００７】
以下の説明は、本技術の様々な例を完全に理解し、説明を可能にするための具体的な詳細を提供する。当業者は、本技術がこれらの多くの詳細なしに実践され得ることを理解されよう。場合によっては、本技術の例の説明を不必要に曖昧にすることを避けるために、公知の構造および機能は、詳細には図示または説明されていない。本開示で使用される用語は、本技術の特定の例の詳細な説明と併せて使用されている場合でも、その最も広い合理的な方法で解釈されるべきであることが意図されている。以下で特定の用語を強調する場合があるが、制限された方法で解釈されることを意図されているいかなる用語も、この発明を実施するための形態の項では、そのように明確かつ具体的に定義される。本明細書および特許請求の範囲を通じて、以下の用語は、文脈が別段の指示をしない限り、少なくとも本明細書に明示的に関連付けられた意味をとる。以下で識別される意味は、必ずしも用語を制限するものではなく、単に用語の説明的な例を提供するものである。例えば、「に基づく（ｂａｓｅｄ　ｏｎ）」および「に基づく（ｂａｓｅｄ　ｕｐｏｎ）」という用語の各々は、それぞれ排他的でなく、「に少なくとも部分的に基づく」という用語と同等であり、本明細書にそのいくつかが記載されていない場合がある追加の要因に基づく選択肢を含む。別の例として、「を介して」という用語は排他的でなく、「を少なくとも部分的に介して」という用語と同等であり、本明細書にそのいくつかが記載されていない可能性がある追加の要因を介する選択肢を含む。「において」の意味は、「において」および「の上で」を含む。本明細書で使用される「一実施形態において」または「一例において」という句は、必ずしも同じ実施形態または例を指すとは限らないが、そうである場合もある。特定のテキスト数値指定子の使用は、より小さい値の数値指定子の存在を示唆するものではない。例えば、「３番目のｆｏｏおよび４番目のｂａｒから構成されるグループから選択されたウィジェット」と具陳すること自体は、少なくとも３つのｆｏｏがあることを示唆せず、また少なくとも４つのｂａｒがあることを示唆しない。単数形での言及は、単に読みやすくするために行われており、複数形の言及が特に除外されていない限り、複数形の言及を含む。「または」という用語は、特に明示されていない限り、包括的「または」演算子である。例えば、「ＡまたはＢ」という句は、「Ａ、Ｂ、またはＡおよびＢ」を意味する。本明細書で使用される場合、「コンポーネント」および「システム」という用語は、ハードウェア、ソフトウェア、またはハードウェアとソフトウェアの様々な組み合わせを包含することを意図している。したがって、例えば、システムまたはコンポーネントは、プロセス、コンピューティングデバイス上で実行されるプロセス、コンピューティングデバイス、またはそれらの一部であり得る。
【０００８】
簡潔に言えば、開示される技術は、概して、仮想化技術を対象としている。開示される技術は、仮想マシン（ＶＭ）、仮想化アプリケーション、仮想化ベースのセキュリティ（ＶＢＳ）ユーザモードプロセス、ＶＢＳカーネルモードプロセス、または他のゲストパーティションによって、またはそれらから要求されたプロセッサ特徴ＩＤ情報をプロセッサによって提供することを含む。例えば、そのような要求は、ゲストパーティション内のゲスト仮想プロセッサ上で実行されるコードによって生成され得る。そのような情報は、例えば、ハイパーバイザなどの監視パーティションによって、プロセッサに事前に提供される情報に基づいて提供され得る。開示される技術はまた、例えば、そのような情報をプロセッサに提供する監視パーティションを含み、そのような情報を受信するゲストパーティションを含む。

【０００９】
いくつかの例では、開示される技術は、仮想化／仮想化されたシステム内で採用され得る。例えば、本技術は、ハイパーバイザ、仮想マシン、仮想化アプリケーション、仮想化ベースのセキュリティ（ＶＢＳ）ユーザモードプロセス、ＶＢＳカーネルモードプロセスなどと併せて採用することができる。例えば、本技術は、ハイパーバイザまたは他の監視パーティションによって、プロセッサ特徴ＩＤ情報の事前計算、またはそれを他の方法で判定することと、例えば、ゲストパーティションからの、プロセッサ特徴ＩＤ情報についての要求に応答する際の後で使用のために、判定されたプロセッサ特徴ＩＤ情報をコンピューティングデバイスのプロセッサに提供することと、を含み得る。例えば、ゲストパーティションからのそのような情報についての要求は、その後、監視パーティションの介入なしにプロセッサによって処理することができる。

【００１０】
開示される技術の使用は、監視パーティションコードを実行するためにシステムがゲストコードの実行で終了するＶＭエグジットまたは他のゲストエグジットの頻度を低減および／または排除するために採用され得る。ゲストエグジットの一例として、プロセッサ特徴ＩＤ情報に対するゲストのクエリに応答して、監視パーティションプロセスは、ゲストパーティションからプロセッサの制御を取得し、プロセッサのプロセッサ特徴ＩＤレジスタをセットアップし、次に、プロセッサの制御をゲストパーティションに戻すことができる。

【００１１】
特定の以前の仮想化システムでは、ゲストパーティションから実行される特定の動作に応答してゲストエグジットが発生する。例えば、ゲストエグジットは、ＣＰＵ　ＩＤまたは他のプロセッサ特徴ＩＤ情報が要求されるゲストパーティションから実行される動作に応答して発生する場合がある。そのようなエグジットは、通常、時間、電力、およびコンピューティングパフォーマンスの点で「高価」である。例えば、ゲストエグジットは、ゲストパーティションコード（例えば、意図されたワークロード）よりも、監視パーティションコード（例えば、オーバーヘッド）のための処理帯域幅の使用に関連付けられ得る。ゲストエグジットはまた、監視パーティションコードなどによるプロセッサデータおよび／または命令キャッシュ位置の上書きによる追加のコンテキスト切り替えオーバーヘッドに関連付けられ得る。

【００１２】
例示的な物理コンピューティングデバイス
図１は、本技術の態様を実践することができるコンピューティングデバイス１００の物理図の一例を示す図である。コンピューティングデバイス１００は、事実上、任意のタイプの汎用または特定目的のコンピューティングデバイスであり得る。例えば、コンピューティングデバイス１００は、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、ディスプレイデバイス、カメラ、プリンタ、またはスマートフォンなどのユーザデバイスであり得る。同様に、コンピューティングデバイス１００はまた、アプリケーションサーバコンピュータ、仮想コンピューティングホストコンピュータ、またはファイルサーバコンピュータなどのサーバデバイスであり得る。コンピューティングデバイス１００はまた、ＩｏＴサービスを受信するためにネットワークに接続するＩｏＴデバイスであり得る。同様に、コンピュータデバイス１００は、以下でより詳細に考察されるように、図２～図５において示されるかまたは言及されるデバイスのいずれかの例であり得る。図１に示すように、コンピューティングデバイス１００は、処理回路１１０、動作メモリ１２０、メモリコントローラ１３０、データ記憶メモリ１５０、入力インターフェース１６０、出力インターフェース１７０、およびネットワークアダプタ１８０を含む。コンピューティングデバイス１００のこれらの前述のコンポーネントの各々は、少なくとも１つのハードウェア要素を含む。

【００１３】
コンピューティングデバイス１００は、本明細書で説明するワークロード、プロセス、

または技術を実装するための命令などの命令を実行するように構成されている少なくとも１つの処理回路１１０を含む。処理回路１１０は、マイクロプロセッサ、マイクロコントローラ、グラフィックスプロセッサ、コプロセッサ、フィールドプログラマブルゲートアレイ、プログラマブルロジックデバイス、信号プロセッサ、またはデータを処理するのに好適な他の任意の回路を含み得る。処理回路１１０は、コアの一例である。前述の命令は、他のデータ（例えば、データセット、メタデータ、オペレーティングシステム命令など）とともに、コンピューティングデバイス１００の実行中に動作メモリ１２０に記憶され得る。動作メモリ１２０はまた、揮発性メモリ、半揮発性メモリ、ランダムアクセスメモリ、スタティックメモリ、キャッシュ、バッファ、または実行時の情報を記憶するために使用される他の媒体などの様々なデータ記憶デバイス／コンポーネントのいずれかを含み得る。一例では、動作メモリ１２０は、コンピューティングデバイス１００の電源がオフにされたときに情報を保持しない。むしろ、コンピューティングデバイス１００は、起動または他のロードプロセスの一部として、不揮発性データ記憶コンポーネント（例えば、データ記憶コンポーネント１５０）から動作メモリ１２０に命令を転送するように構成され得る。

【００１４】

動作メモリ１２０は、第４世代のダブルデータレート（ＤＤＲ４）メモリ、第３世代のダブルデータレート（ＤＤＲ３）メモリ、他のダイナミックランダムアクセスメモリ（ＤＲＡＭ）、高帯域幅メモリ（ＨＢＭ）、ハイブリッドメモリキューブメモリ、３Ｄスタックメモリ、スタティックランダムアクセスメモリ（ＳＲＡＭ）、または他のメモリを含み得、そのようなメモリは、ＤＩＭＭ、ＳＩＭＭ、ＳＯＤＩＭＭ、または他のパッケージに統合された１つ以上のメモリ回路を含み得る。そのような動作メモリモジュールまたはデバイスは、チャネル、ランク、およびバンクに従って編成することができる。例えば、動作メモリデバイスは、チャネル内のメモリコントローラ１３０を介して処理回路１１０に結合され得る。コンピューティングデバイス１００の一例は、チャネルごとに１つまたは２つのＤＩＭＭを含み得、チャネルごとに１つまたは２つのランクを含む。ランク内の動作メモリは、共有クロック、ならびに共有アドレスおよびコマンドバスで動作する場合がある。また、動作メモリデバイスはいくつかのバンクに編成される場合があり、バンクは、行と列によってアドレス指定されるアレイと考えることができる。このような動作メモリの編成に基づいて、動作メモリ内の物理アドレスは、チャネル、ランク、バンク、行、および列のタプルによって参照される場合がある。

【００１５】

上記の考察にもかかわらず、動作メモリ１２０は、具体的には、通信媒体、任意の通信媒体、または任意の信号自体を含まないか、または包含しない。

【００１６】

メモリコントローラ１３０は、処理回路１１０を動作メモリ１２０とインターフェース接続するように構成されている。例えば、メモリコントローラ１３０は、動作メモリ１２０と処理回路１１０との間でコマンド、アドレス、およびデータをインターフェース接続するように構成され得る。メモリコントローラ１３０はまた、処理回路１１０からまたは処理回路１１０のために、メモリ管理の特定の態様を抽出するか、または他の方法で管理するように構成され得る。メモリコントローラ１３０は、処理回路１１０とは別の単一のメモリコントローラとして示されているが、他の例では、複数のメモリコントローラを採用することができ、メモリコントローラ（複数可）を動作メモリ１２０などと統合することができる。さらに、メモリコントローラ（複数可）は、処理回路１１０に統合され得る。これらおよび他の変形態が可能である。

【００１７】

コンピューティングデバイス１００では、データ記憶メモリ１５０、入力インターフェース１６０、出力インターフェース１７０、およびネットワークアダプタ１８０が、バス１４０によって処理回路１１０にインターフェース接続されている。図１は、バス１４０を単一のパッシブバスとして示しているが、バスの集合、ポイントツーポイントリンクの

集合、入出力コントローラ、ブリッジ、他のインターフェース回路、またはそれらの任意の集合などの他の構成もまた、データ記憶メモリ１５０、入力インターフェース１６０、出力インターフェース１７０、またはネットワークアダプタ１８０を処理回路１１０にインターフェース接続するために好適に採用されてもよい。

【００１８】

コンピューティングデバイス１００では、データ記憶メモリ１５０は、長期の不揮発性データ記憶のために採用される。データ記憶メモリ１５０は、不揮発性メモリ、ディスク、ディスクドライブ、ハードドライブ、ソリッドステートドライブ、または情報の不揮発性記憶に使用することができる他の任意の媒体など、様々な不揮発性データ記憶デバイス／コンポーネントのいずれかを含み得る。しかしながら、データ記憶メモリ１５０は、具体的には、通信媒体、任意の通信媒体、または任意の信号自体を含まないか、または包含しない。動作メモリ１２０とは対照的に、データ記憶メモリ１５０は、実行時データ記憶ではなく、不揮発性の長期データ記憶のためにコンピューティングデバイス１００によって採用される。

【００１９】

また、コンピューティングデバイス１００は、プロセッサ可読記憶媒体（例えば、動作メモリ１２０およびデータ記憶メモリ１５０）ならびに通信媒体（例えば、通信信号および電波）などの任意のタイプのプロセッサ可読媒体を含むか、またはそれらに結合され得る。プロセッサ可読記憶媒体という用語は、動作メモリ１２０およびデータ記憶メモリ１５０を含むが、「プロセッサ可読記憶媒体」という用語は、本明細書および特許請求の範囲全体で、単数形で使用されるか複数形で使用されるかにかかわらず、「プロセッサ可読記憶媒体」という用語が、通信媒体、任意の通信媒体、または任意の信号自体を特に除外し、これらを包含しないように、本明細書において定義されている。しかしながら、「プロセッサ可読記憶媒体」という用語は、プロセッサキャッシュ、ランダムアクセスメモリ（ＲＡＭ）、レジスタメモリなどを包含する。

【００２０】

コンピューティングデバイス１００はまた、コンピューティングデバイス１００がユーザまたは他のデバイスからの入力を受信することを可能にするように構成され得る、入力インターフェース１６０を含む。さらに、コンピューティングデバイス１００は、コンピューティングデバイス１００からの出力を提供するように構成され得る、出力インターフェース１７０を含む。一例では、出力インターフェース１７０は、フレームバッファ、グラフィックスプロセッサ、グラフィックスプロセッサまたはアクセラレータを含み（モニタ、プロジェクタ、仮想コンピューティングクライアントコンピュータなどの）、別個の視覚的ディスプレイデバイス上に提示するための表示をレンダリングするように構成されている。別の例では、出力インターフェース１７０は、視覚的ディスプレイデバイスを含み、閲覧のために表示をレンダリングおよび提示するように構成されている。さらに別の例では、入力インターフェース１６０および／または出力インターフェース１７０は、ユニバーサル非同期受信機／送信機（「ＵＡＲＴ」）、シリアルペリフェラルインターフェース（「ＳＰＩ」）、インター集積回路（「Ｉ１Ｃ」）、汎用入出力（ＧＰＩＯ）などを含み得る。さらに、入力インターフェース１６０および／または出力インターフェース１７０は、任意の数もしくはタイプの周辺機器を含むか、またはそれらにインターフェース接続され得る。

【００２１】

図示の例では、コンピューティングデバイス１００は、ネットワークアダプタ１８０を介して、他のコンピューティングデバイスまたはエンティティと通信するように構成されている。ネットワークアダプタ１８０は、有線ネットワークアダプタ、例えば、イーサネットアダプタ、トークンリングアダプタ、またはデジタル加入者線（ＤＳＬ）アダプタを含み得る。ネットワークアダプタ１８０はまた、無線ネットワークアダプタ、例えば、Ｗｉ－Ｆｉアダプタ、Ｂｌｕｅｔｏｏｔｈアダプタ、ＺｉｇＢｅｅアダプタ、Ｌｏｎｇ Ｔｅｒｍ Ｅｖｏｌｕｔｉｏｎ（ＬＴＥ）アダプタ、または５Ｇアダプタを含み得る。

【００２２】
コンピューティングデバイス１００は、特定の配置で構成されている特定のコンポーネントとともに示されているが、これらのコンポーネントおよび配置は、本技術が採用され得るコンピューティングデバイスの一例にすぎない。他の例では、データ記憶メモリ１５０、入力インターフェース１６０、出力インターフェース１７０、またはネットワークアダプタ１８０は、処理回路１１０に直接結合され得るか、または入出力コントローラ、ブリッジ、もしくは他のインターフェース回路を介して処理回路１１０に結合され得る。技術の他の変形態が可能である。
【００２３】
コンピューティングデバイス１００のいくつかの例は、実行時データを記憶するように適合された少なくとも１つのメモリ（例えば、動作メモリ１２０）と、実行に応答してコンピューティングデバイス１００がアクションを実行できるようにする、プロセッサ実行可能コードを実行するように適合された少なくとも１つのプロセッサ（例えば、処理ユニット１１０）とを含む。
【００２４】
例示的な論理コンピューティングデバイス
図２は、本技術の態様を実践することができるコンピューティングデバイス２００の論理図の一例を示す図である。コンピューティングデバイス２００は、図１のコンピューティングデバイス１００の一例であり得る。図２の図では、コンピューティングデバイス２００の論理コンポーネントは、ゲストパーティション２１１～２１３、監視パーティション２３０、物理リソース２４１～２４３、およびプロセッサ特徴ＩＤ２５０を含む。
【００２５】
物理リソース２４１～２４３は、プロセッサコンポーネント、入出力（Ｉ／Ｏ）コンポーネント、および／または他のコンポーネントもしくはデバイスなど、様々な物理コンポーネントを含む場合がある。例えば、物理リソース２４１～２４３は、図１に関連して考察されるものなど、物理コンポーネントの好適な組み合わせを含む場合がある。コンピューティングデバイス２００の一部として示されているが、１つ以上の物理リソース２４１～２４３（例えば、１つ以上のデータ記憶メモリ）は、コンピューティングデバイス２００の外部に実装することができる。監視パーティション２３０を含む、コンピューティングデバイス２００上で実行される様々なコンポーネントまたはモジュールは、物理リソース２４１～２４３を介して提供される機能（複数可）に直接および／または他のコンポーネントもしくはモジュールを介して間接的にアクセスすることができる。
【００２６】
監視パーティション２３０は、任意の数のゲストパーティション、例えば、ゲストパーティション２１１～２１３を生成することができる。ゲストパーティション２１１～２１３の各々は、ＶＭ、仮想化アプリケーション、ＶＢＳ実行環境、ユーザモードプロセスなどであり得る。例えば、ゲストパーティション２１１は、オペレーティングシステム（ＯＳ）２２１とアプリケーション２２２を備えたＶＭとして示され、ゲストパーティション２１２は、仮想化アプリケーション２２３として示され、ゲストパーティション２２４は、プロセス２２４がそこから実行されるものとして示されている。
【００２７】
ゲストパーティション２１１～２１３の各々は、オペレーティングシステムおよび／または他のソフトウェアが実行される分離の論理ユニットである。ゲストパーティション２１１～２１３の各々はまた、ゲスト仮想プロセッサを含み得る。ゲストパーティション２１１～２１３の各々内で実行されるソフトウェアは、他のゲストパーティションの各々内で実行されるソフトウェアから分離されている。例えば、ゲストパーティション２１１～２１３の各々内で実行されるソフトウェアは、他のゲストパーティションの各々内で実行されるソフトウェアにアクセスすることができず、それを認識する必要はない。物理リソース２４１～２４３はゲストパーティション２１１～２１３に仮想化され、物理リソース２４１～２４３へのアクセスは監視パーティション２３０によって管理される。

【００２８】
図示のように、コンピューティングデバイス１００は監視パーティション２３０を含む。監視パーティション２３０は、物理リソース２４１～２４３によって提供される機能へのアクセスを管理する仮想マシンモニタなどのハイパーバイザを含み得る。別の例では、監視パーティション２３０は、ＶＢＳを採用するＯＳなど、ＯＳのカーネルまたはカーネルモードプロセスである。
【００２９】
コンピューティングデバイス２００はまた、１つ以上のプロセッサ特徴ＩＤ２５０を含む。例えば、プロセッサ特徴ＩＤ２５０は、ｘ８６　ＣＰＵ　ＩＤリーフ情報を含むレジスタ（またはレジスタのセット）、高度縮小命令セット計算マシン（ＡＲＭ）プロセッサのＩＤレジスタなど、物理プロセッサの物理ハードウェアＩＤレジスタ（またはレジスタのセット）を表すことができる。プロセッサ特徴ＩＤ２５０はまた、プロセッサによってサポートされている特徴、プロセッサによってサポートされている特徴セット、プロセッサの物理的特性などを表すことができる。例えば、プロセッサ特徴ＩＤ２５０は、プロセッサ周波数、サポートされる物理アドレス幅、クロック乗数、電力設定、命令の可用性、ステッピング番号、シリアル番号などを表すことができる。
【００３０】
例示的なプロセス
明確にするために、本明細書で説明されるプロセスは、システムの特定のデバイスまたはコンポーネントによって特定の順序で実行される動作に関して説明される。しかしながら、他のプロセスは、記載された順序、デバイス、またはコンポーネントに限定されないことが分かる。例えば、特定の行為は、そのような順序、並行性、行為、または特徴が本明細書に記載されているかどうかにかかわらず、異なる順序で実行され、並行して実行され、省略され得るか、または追加の行為もしくは特徴によって補足され得る。同様に、本開示に記載されている技術のいずれも、その技術がプロセスと併せて具体的に説明されているかどうかにかかわらず、説明されているプロセスまたは他のプロセスに組み込むことができる。開示されるプロセスはまた、そのようなデバイス、コンポーネント、またはシステムが本明細書に記載されているかどうかにかかわらず、他のデバイス、コンポーネント、またはシステム上で、またはそれらによって実行され得る。これらのプロセスはまた、様々な方法で具体化することもできる。例えば、それらは、例えば、プロセッサ可読記憶媒体に記憶されたプロセッサ可読命令として製造品に具体化されるか、またはコンピュータ実装プロセスとして実行され得る。代替の例として、これらのプロセスは、プロセッサ実行可能命令としてエンコードされ、通信媒体を介して送信され得る。
【００３１】
図３は、コンピューティングデバイスのプロセッサ、例えば、図１の処理回路１１０または図２の物理リソース２４１、２４２、または２４３の観点から示される例示的なプロセス３００を示す。プロセス３００は、プロセッサ特徴ＩＤについての要求が受信される３８１において開始する。例えば、この要求は物理プロセッサによって受信され得、この要求はゲストパーティションから発信され得る。例えば、この要求は、ゲストパーティション内のゲスト仮想プロセッサ上で実行されるコードによって生成され得る。
【００３２】
３８１から、処理は３８２に流れ、ここで、例えば、プロセッサは、プロセッサ特徴ＩＤを検索する。一例では、プロセッサは、プロセッサ特徴ＩＤレジスタ、プロセッサにアクセス可能なメモリ構造、プロセッサ特徴ＩＤルックアップテーブルなどからプロセッサ特徴ＩＤを検索する。この検索はまた、例えば、図４のプロセス４００と併せてさらに考察されるように、ハイパーバイザまたは他の監視パーティションによってプロセッサに事前に提供された情報に基づくことができる。
【００３３】
次に、処理は３８３に流れ、そこで、例えば、ゲストエグジットなしで、プロセッサ特徴ＩＤが提供される。これは、プロセッサが、ゲストパーティションからの要求プロセス

などに対して、要求されたプロセッサ特徴ＩＤをゲストパーティションに提供することを含む場合がある。提供されるプロセッサ特徴ＩＤは、プロセッサに事前に提供された情報に基づくことができる。３８３に続いて、処理は他の動作に戻る。

【００３４】

図４は、監視パーティション、例えば、ハイパーバイザの観点から示されている例示的なプロセス４００を示す。例えば、プロセス４００は、図２の監視パーティション２３０の観点から示されている。

【００３５】

プロセス４００は、プロセッサ特徴ＩＤの値が取得される４８１において開始する。この値は、ゲストパーティション、ゲスト仮想プロセッサ、またはゲスト仮想プロセッサ仮想信頼レベルのうちの少なくとも１つのセットアップ動作と併せて、またはそれに応答して、監視パーティションによって取得され得る。例えば、そのようなセットアップ動作は、ゲストパーティション、ゲスト仮想プロセッサ、またはゲスト仮想プロセッサ仮想信頼レベルの生成、インスタンス化、または起動のうちの少なくとも１つを含み得る。値は、例えば、コンピューティングデバイスの物理プロセッサの対応するハードウェアレジスタ値を読み取ることによって取得することができる。一例として、取得されたプロセッサ特徴ＩＤ値は、物理プロセッサの製造元によって割り当てられた値（例えば、オンチップ値）であり得、ならびに／またはプロセッサによってサポートされている特徴／特徴セットを表すおよび／もしくは示すことができる。

【００３６】

任意選択的に、処理は、４８２に流れ、そこで、記憶されるプロセッサ特徴ＩＤが計算されるか、または他の方法で判定される。例えば、４８２は、取得されたプロセッサ機能ＩＤ値が変更なしで記憶されるべきかどうか、または異なる値が記憶されるべきかどうかを判定することを含み得る。例えば、監視パーティションが、例えば、ゲストパーティションのポータビリティ、パフォーマンスの強化、および／または他の理由のために、プロセッサによってネイティブにサポートされているものとは異なるプロセッサ特徴のセットをゲストパーティションに「供給」する場合、異なる値が記憶され得る。４８２において、取得されたプロセッサ機能ＩＤ値の複数の値も判定され得、例えば、各々は、異なるゲストパーティションおよび／またはゲスト仮想プロセッサおよび／または信頼レベルコンテキストに関連付けられ、および／またはそれらに対して指定され得る。いくつかの例では、異なるプロセッサ機能ＩＤ値は、仮想プロセッサコンテキストまたは仮想プロセッサの仮想信頼レベルコンテキストごとに採用され得る。仮想プロセッサコンテキストまたは仮想プロセッサの仮想信頼レベルコンテキストごとの例は、仮想マシン制御構造（ＶＭＣＳ）、仮想マシン制御ブロック（ＶＭＣＢ）、ゲストコンテキストを含むシステムレジスタのセット、またはゲストコンテキストの他の仮想化命令セットアーキテクチャ固有コレクションである。

【００３７】

処理は４８３に流れ、そこで、４８２のプロセッサ特徴ＩＤがプロセッサに提供される。例えば、監視パーティションは、プロセッサ特徴ＩＤ情報についてのゲストパーティションソフトウェアからの要求に応答する際のプロセッサによる後の使用のために、４８２で判定されたプロセッサ特徴ＩＤをプロセッサに提供することができる。４８３において、プロセッサはまた、監視パーティションからこのプロセッサ特徴ＩＤ情報を受信することができる。

【００３８】

その後、処理は４８４に流れる。４８４において、提供されたプロセッサ特徴ＩＤが記憶される。例えば、４８４は、プロセッサに、提供されたプロセッサ特徴ＩＤを記憶させる監視プロセスによるアクション、および／または記憶を実行するためにプロセッサによって行われるアクションを含み得る。例えば、この記憶は、プロセッサ特徴ＩＤをプロセッサ特徴ＩＤレジスタ、メモリ内のプロセッサ特徴ＩＤルックアップテーブルなどに記憶することを含み得る。さらに別の例では、監視パーティションコードは、ＩＤ＿ＲＥＧＩ

ＳＴＥＲ＿ＷＲＩＴＥ命令などのプロセッサインターフェース命令を介して、プロセッサ特徴ＩＤを記憶することができる。

【００３９】

さらに別の例では、プロセッサ特徴ＩＤは、プロセッサにアクセス可能なメモリ構造に書き込まれ得、そのメモリ構造の位置は、プロセッサレジスタにプログラムされ得る。この例および他の例では、例えば、異なるゲストパーティション、異なるＶＭＣＳ、仮想プロセッサコンテキスト、信頼レベルコンテキストなどに対して異なるプロセッサ機能ＩＤ値の使用を可能にするために、複数のメモリ構造を採用することができる。使用中、異なるメモリ構造間のコンテキスト切り替えは、例えば、あるゲストパーティション、ゲスト仮想プロセッサ、またはゲスト仮想プロセッサ仮想信頼レベルから別のゲストパーティション、ゲスト仮想プロセッサ、またはゲスト仮想プロセッサ仮想信頼レベルへのプロセッサ切り替えの制御に応答して、プロセッサまたは監視パーティションコード２３０のいずれかによって実行され得る。

【００４０】

任意選択的に、４８４はまた、ゲストパーティションからの所与の要求に対して複数の値／メモリ構造のうちの適切な値／メモリ構造にプロセッサを向ける条件式をプロセッサに記憶することを含み得る。例えば、式は、ＩＤ＿ＲＥＧＩＳＴＥＲ＿ＷＲＩＴＥ（ＶＰ＿ＣＯＮＴＥＸＴ、ＲＥＧＩＳＴＥＲ＿ＮＡＭＥ、ＣＯＮＤＩＴＩＯＮＡＬ、ＶＡＬＵＥ）命令などの命令を介して記憶することができる。

【００４１】

上で考察されるように、この記憶はまた、プロセッサによる、プロセッサ特徴ＩＤのその後の使用を可能にして、ゲストエグジットを引き起こさずにゲストパーティションからの要求に応答することができる。プロセス４００は、追加のプロセッサ機能ＩＤのために繰り返され得るか、または複数のプロセッサ機能ＩＤが、プロセス４００の単一の繰り返しで取得、判定、提供、かつ記憶され得る。４８４に続いて、処理は、他の動作に戻る。

【００４２】

図５は、ゲストパーティション、例えば、図２のゲストパーティション２１１、２１２、または２１３の観点から示されている例示的なプロセス５００を示す。プロセス５００は５８１において開始し、そこで、プロセッサ特徴ＩＤが取得されるべきであるという判定が行われる。例えば、この判定は、ゲストパーティションから実行されるアプリケーションまたは他のプロセスからのプロセッサ特徴ＩＤ情報についての要求に応答して、ゲストパーティションによって、またはゲストパーティション上で行われ得る。別の例として、この判定は、仮想マシンで使用するためにプロセッサ特徴ＩＤを取得するという仮想マシンによる要求を表す場合がある。

【００４３】

次に、処理は５８２に流れ、そこで、プロセッサ特徴ＩＤについての要求がゲストパーティションから送信される。この要求は、プロセッサに送信される場合がある。５８２の要求に応答して、５８３において、プロセッサ特徴ＩＤがプロセッサから受信され得る。上で考察されるように、受信されたプロセッサ特徴ＩＤは、監視パーティションによってプロセッサに事前に提供された情報と一致し得る。５８３から、処理は５８４に流れ得、そこで、受信されたプロセッサ特徴ＩＤがリクエスタ、例えば、ゲストパーティション上のアプリケーションまたは他のプロセスに提供される。５８４に続いて、処理は他の動作に戻る。

結論

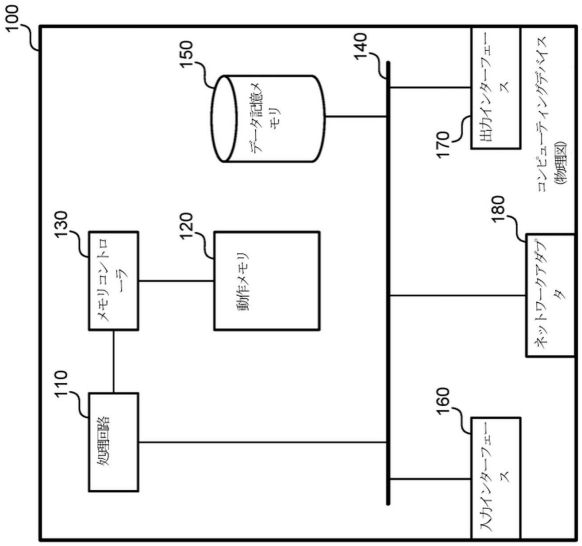
【００４４】

上記の発明を実施するための形態は、本技術の特定の例を説明し、考えられる最良のモードを説明するが、上記のことが本文でどれほど詳細に表わされていても、本技術は多くの方法で実践することができる。詳細は、実装において異なる場合があるが、依然として本明細書に記載の技術に包含されている。上記のように、本技術の特定の特徴または態様を説明するときに使用される特定の用語は、その用語が関連する特定の特性、特徴、また

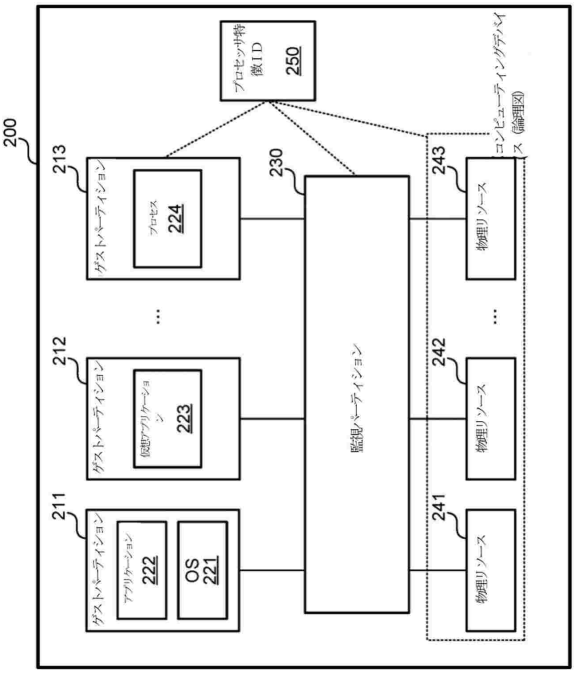
は態様に限定されるように、その用語が本明細書において再定義されていることを示唆するとみなすべきではない。一般に、以下の特許請求の範囲で使用される用語は、発明を実施するための形態がそのような用語を明示的に定義していない限り、本技術を本明細書で開示される特定の例に限定するものと解釈されるべきではない。したがって、本技術の実際の範囲は、開示される例だけでなく、本技術を実践または実装するためのすべての同等な方法も包含する。

【図面】

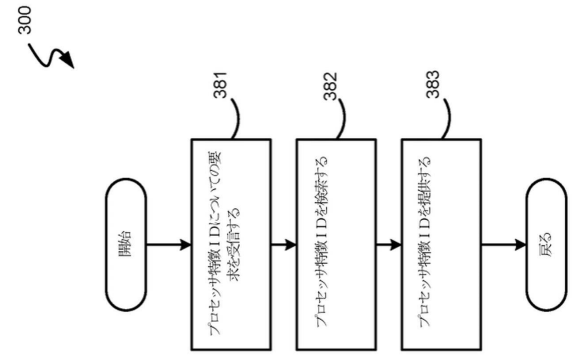
【図１】



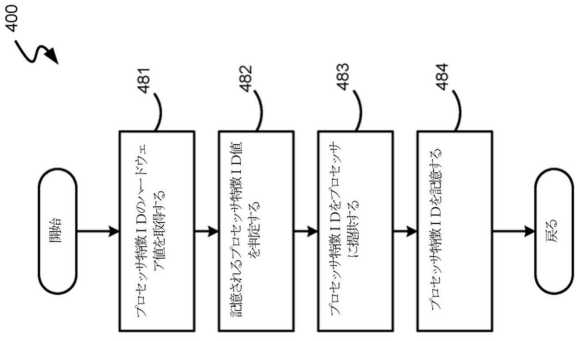
【図２】



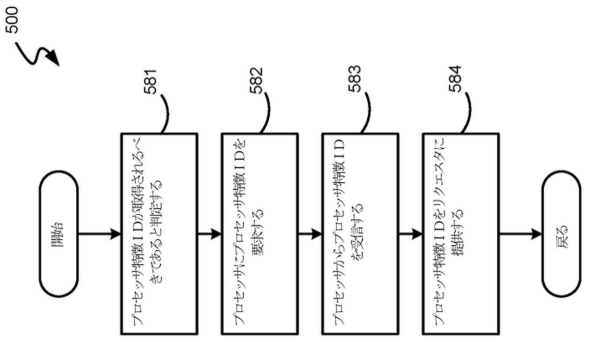
【図３】



【図４】



【図５】


500
581
582
583
584
開始
プロセッサ特徴ＩＤが取得されるべきであると判定する
プロセッサにプロセッサ特徴ＩＤを要求する
プロセッサからプロセッサ特徴ＩＤを受信する
プロセッサ特徴ＩＤをリクエスタに提供する
戻る

フロントページの続き

弁理士　阿部 豊隆
(74)代理人　100134027
弁理士　松田 達也
(72)発明者　シャーウィン，ブルース ジェイ．，ジュニア
アメリカ合衆国，ワシントン州 ９８０５２－６３９９，レッドモンド，ワン マイクロソフト ウェイ，マイクロソフト テクノロジー ライセンシング，エルエルシー
審査官　坂東 博司
(56)参考文献　特開２００６－２５２５６５（ＪＰ，Ａ）
米国特許出願公開第２０１２／００８４７７７（ＵＳ，Ａ１）
特開２０１３－２１８７３８（ＪＰ，Ａ）
特表２０１７－５２０９５９（ＪＰ，Ａ）
米国特許出願公開第２０１５／００８２３０５（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　９／４５５
Ｇ０６Ｆ　９／４８