

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号
特表2024-541488
(P2024-541488A)

(43)公表日 令和6年11月8日(2024.11.8)

(51)国際特許分類

F I

G 0 6 F 9/52 (2006.01) G 0 6 F 9/52 1 2 0 Z

G 0 6 F 9/46 (2006.01) G 0 6 F 9/46 4 1 0

審査請求 未請求 予備審査請求 未請求 (全23頁)			
(21)出願番号	特願2024-531100(P2024-531100)	(71)出願人	390009531
(86)(22)出願日	令和4年11月9日(2022.11.9)		インターナショナル・ビジネス・マシー ンズ・コーポレーション
(85)翻訳文提出日	令和6年5月23日(2024.5.23)		INTERNATIONAL BUSI NESS MACHINES CORPO RATION
(86)国際出願番号	PCT/EP2022/081213		アメリカ合衆国10504 ニューヨー ク州 アーモンク ニュー オーチャード ロード
(87)国際公開番号	WO2023/099137		New Orchard Road, A rmonk, New York 105 04, United States of America
(87)国際公開日	令和5年6月8日(2023.6.8)		
(31)優先権主張番号	17/457,446	(74)代理人	100112690
(32)優先日	令和3年12月3日(2021.12.3)		弁理士 太佐 種一
(33)優先権主張国・地域又は機関	米国(US)		
(81)指定国・地域	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,A T,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR ,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC, 最終頁に続く		最終頁に続く

(54)【発明の名称】 処理ユニットのプロセッサ・コア上のセキュア・コード・セグメントの動作

(57)【要約】

コンピュータ実装方法、コンピュータ・システム、およびコンピュータ・プログラム製品が、処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させ、処理ユニットが、少なくとも1つのプロセッサ・コアによって構成される。この方法は、少なくとも1つのプロセッサ・コア上のプログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することを含む。この方法はまた、少なくとも1つのプロセッサ・コアをセキュア・コード・セグメントのための排他的セキュア実行に設定することを含む。この方法は、少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することをさらに含む。追加的に、この方法は、少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することを含む。最後に、この方法は、少なくとも1つのプロセッサ・コアを少なくとも1つのプロセッサ・コア上のプログラム・コードのための第1の実行モードに設定することを含む。

【選択図】 図 1

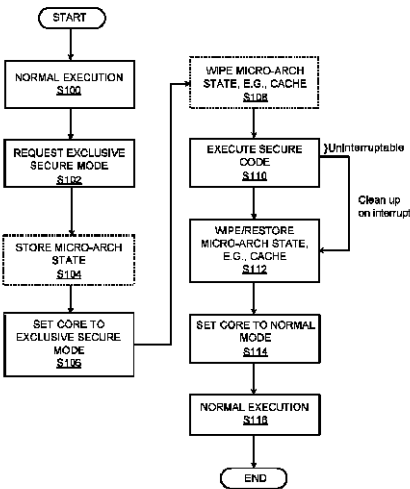


FIG. 1

【特許請求の範囲】

【請求項 1】

処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ実装方法であって、前記処理ユニットが、少なくとも1つのプロセッサ・コアによって、第1の実行モードを走らせて、前記少なくとも1つのプロセッサ・コア上でプログラム・コードを実行し、前記少なくとも1つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成され、前記方法が、

前記少なくとも1つのプロセッサ・コア上の前記プログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、

前記少なくとも1つのプロセッサ・コアを前記セキュア・コード・セグメントのための排他的セキュア実行に設定することと、

前記少なくとも1つのプロセッサ・コア上で前記セキュア・コード・セグメントを中断不能に実行することと、

前記少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、

前記少なくとも1つのプロセッサ・コアを前記少なくとも1つのプロセッサ・コア上でプログラム・コードを実行するための前記第1の実行モードに設定することとを少なくとも含む、コンピュータ実装方法。

【請求項 2】

前記プロセッサ・コアを排他的セキュア・モードに設定する前に、前記物理プロセッサ・コアの少なくとも前記設計状態および前記非設計状態を保存することをさらに含む、請求項 1 に記載のコンピュータ実装方法。

【請求項 3】

前記プロセッサ・コアを前記第1の実行モードに設定する前に、前記物理プロセッサ・コアの少なくとも前記設計状態および前記非設計状態を回復することをさらに含む、請求項 1 または 2 に記載のコンピュータ実装方法。

【請求項 4】

前記セキュア・コード・セグメントを実行する前に、前記物理プロセッサ・コアの少なくとも1つのキャッシュ・ストレージから前記物理プロセッサ・コアの前記非設計状態を一掃することをさらに含む、請求項 1 ないし 3 のいずれか一項に記載のコンピュータ実装方法。

【請求項 5】

前記物理プロセッサ・コアの前記非設計状態を一掃することが、前記処理ユニットのハードウェアによってハードウェア制御式に実行される、請求項 4 に記載のコンピュータ実装方法。

【請求項 6】

前記プロセッサ・コア上でプログラム・コードを実行するための前記第1の実行モードが、同時マルチスレッディング・モードである、請求項 1 ないし 5 のいずれか一項に記載のコンピュータ実装方法。

【請求項 7】

前記少なくとも1つのプロセッサ・コア上で前記セキュア・コード・セグメントを中断不能に実行することが、最小の期間および最小の命令数に対して定義される、請求項 1 ないし 6 のいずれか一項に記載のコンピュータ実装方法。

【請求項 8】

前記少なくとも1つのプロセッサ・コア上で前記セキュア・コード・セグメントを中断不能に実行することが、状態機械によって制御される、請求項 1 ないし 7 のいずれか一項に記載のコンピュータ実装方法。

【請求項 9】

前記セキュア・コード・セグメントの実行中の中断が阻止される、請求項 1 ないし 8 のいずれか一項に記載のコンピュータ実装方法。

10

20

30

40

50

【請求項 10】

前記セキュア・コード・セグメントの実行後に前記少なくとも1つのプロセッサ・コアから前記物理プロセッサ・コアの前記設計状態および前記非設計状態を一掃することが、中断要求によって開始される、請求項1ないし9のいずれか一項に記載のコンピュータ実装方法。

【請求項 11】

仮想機械上またはコンテナ上で動作命令が実装される、請求項1ないし10のいずれか一項に記載のコンピュータ実装方法。

【請求項 12】

処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ・システムであって、前記処理ユニットが、少なくとも1つのプロセッサ・コアによって構成され、前記コンピュータ・システムが、少なくとも1つのプロセッサ・コアを有する少なくとも1つのプロセッサ・ユニットを備え、前記プロセッサ・コアが、第1の実行モードを走らせて、前記少なくとも1つのプロセッサ・コア上でプログラム・コードを実行し、前記少なくとも1つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成され、前記コンピュータ・システムが、

前記少なくとも1つのプロセッサ・コア上の前記プログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、

前記少なくとも1つのプロセッサ・コアを前記セキュア・コード・セグメントのための排他的セキュア実行に設定することと、

前記少なくとも1つのプロセッサ・コア上で前記セキュア・コード・セグメントを中断不能に実行することと、

前記少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、

前記少なくとも1つのプロセッサ・コアを前記少なくとも1つのプロセッサ・コア上でプログラム・コードを実行するための前記第1の実行モードに設定することとを少なくとも含む方法を実行するように構成されている、コンピュータ・システム。

【請求項 13】

前記プロセッサ・コアを排他的セキュア・モードに設定する前に、前記物理プロセッサ・コアの少なくとも前記設計状態および前記非設計状態を保存するように構成されている、請求項12に記載のコンピュータ・システム。

【請求項 14】

前記プロセッサ・コアが前記第1の実行モードに設定される前に、前記物理プロセッサ・コアの少なくとも前記設計状態および前記非設計状態を回復するように構成されている、請求項12または13に記載のコンピュータ・システム。

【請求項 15】

前記セキュア・コード・セグメントが実行される前に、前記物理プロセッサ・コアの少なくとも1つのキャッシュ・ストレージから前記物理プロセッサ・コアの前記非設計状態を一掃するように構成されている、請求項12ないし14のいずれか一項に記載のコンピュータ・システム。

【請求項 16】

前記物理プロセッサ・コアの前記非設計状態を前記処理ユニットのハードウェアによってハードウェア制御式に一掃するように構成されている、請求項15に記載のコンピュータ・システム。

【請求項 17】

前記プロセッサ・コア上でプログラム・コードを実行するための前記第1の実行モードが、同時マルチスレッディング・モードである、請求項12ないし16のいずれか一項に記載のコンピュータ・システム。

【請求項 18】

最小の期間および最小の命令数に対して、前記少なくとも1つのプロセッサ・コア上で

10

20

30

40

50

前記セキュア・コード・セグメントを中断不能に実行するように構成されている、請求項 12 ないし 17 のいずれか一項に記載のコンピュータ・システム。

【請求項 19】

前記少なくとも 1 つのプロセッサ・コア上で前記セキュア・コード・セグメントを中断不能に実行することが、状態機械によって制御される、請求項 12 ないし 18 のいずれか一項に記載のコンピュータ・システム。

【請求項 20】

前記セキュア・コード・セグメントの実行中の中断を阻止するように構成されている、請求項 12 ないし 19 のいずれか一項に記載のコンピュータ・システム。

【請求項 21】

前記セキュア・コード・セグメントの実行後に前記少なくとも 1 つのプロセッサ・コアから前記物理プロセッサ・コアの前記設計状態および前記非設計状態を一掃することが、中断要求によって開始される、請求項 12 ないし 20 のいずれか一項に記載のコンピュータ・システム。

【請求項 22】

仮想機械上またはコンテナ上で動作命令が実装される、請求項 12 ないし 21 のいずれか一項に記載のコンピュータ・システム。

【請求項 23】

処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ・プログラム製品であって、前記処理ユニットが、少なくとも 1 つのプロセッサ・コアによって、第 1 の実行モードを走らせて、前記少なくとも 1 つのプロセッサ・コア上でプログラム・コードを実行し、前記少なくとも 1 つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成され、

前記コンピュータ・プログラム製品が、プログラム命令が実施されたコンピュータ可読記憶媒体を備え、前記プログラム命令が、コンピュータ・システムによって、

前記少なくとも 1 つのプロセッサ・コア上の前記プログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、

前記少なくとも 1 つのプロセッサ・コアを前記セキュア・コード・セグメントのための排他的セキュア実行に設定することと、

前記少なくとも 1 つのプロセッサ・コア上で前記セキュア・コード・セグメントを中断不能に実行することと、

前記少なくとも 1 つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、

前記少なくとも 1 つのプロセッサ・コアを前記少なくとも 1 つのプロセッサ・コア上でプログラム・コードを実行するための前記第 1 の実行モードに設定することを含む方法を前記コンピュータ・システムに実行させるように実行可能である、コンピュータ・プログラム製品。

【請求項 24】

請求項 1 に記載のコンピュータ実装方法を実行するためのコンピュータ可読プログラム命令を含む、データ処理プログラムを実行するためのデータ処理システム。

【請求項 25】

処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるための命令を実行するための集積回路であって、前記処理ユニットが、少なくとも 1 つのプロセッサ・コアによって構成され、前記集積回路が、少なくとも 1 つのプロセッサ・コアを有する少なくとも 1 つのプロセッサ・ユニットを備え、前記プロセッサ・コアが、第 1 の実行モードを走らせて、前記少なくとも 1 つのプロセッサ・コア上でプログラム・コードを実行し、前記少なくとも 1 つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成され、前記集積回路が、

前記少なくとも 1 つのプロセッサ・コア上の前記プログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、

10

20

30

40

50

前記少なくとも1つのプロセッサ・コアを前記セキュア・コード・セグメントのための排他的セキュア実行に設定することと、

前記少なくとも1つのプロセッサ・コア上で前記セキュア・コード・セグメントを中断不能に実行することと、

前記少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、

前記少なくとも1つのプロセッサ・コアを前記少なくとも1つのプロセッサ・コア上でプログラム・コードを実行するための前記第1の実行モードに設定することとを少なくとも含む方法を実行するように構成されている、集積回路。

【発明の詳細な説明】

10

【技術分野】

【0001】

本発明は、一般に、データ処理システムに関し、詳細には、処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ実装方法、コンピュータ・システム、コンピュータ・プログラム製品、およびデータ処理システムに関する。

【背景技術】

【0002】

マルチスレッド・プロセッサは、同時に実行することができる複数のハードウェア・スレッドを含むことができる。マルチスレッド・プロセッサの一例としては、同時マルチスレッド（SMT）プロセッサを挙げることができる。同時マルチスレッディングでは、一度に2つ以上のスレッドからの命令を任意の所与の命令パイプライン段階で実行することができる。したがって、同時マルチスレッディングにより、プロセッサ・アーキテクチャによって提供される資源を複数の独立した実行スレッドがより良好に利用することを可能にすることができる。同時マルチスレッディングにより、仮想機械の各プロセッサを、スレッドと呼ばれるn個のプロセッサとしてアプリケーションに示すことができる。

20

【0003】

クラウド内またはオンプレミスの異なる顧客からのプロセスまたはスレッドを、仮想機械（VM）上またはコンテナ上で仮想化することができ、同じ物理コア上で走らせることができる。スレッドをシングルスレッド・モードで走らせることを要求することが一般的である。

30

【0004】

セキュア・マルチスレッド実行のためのパイプラインの一実装形態は、命令を実行するための集積回路とすることができ、集積回路は、プロセッサ・パイプラインの実行ユニットを使用して2つ以上のスレッドからの命令を並行して実行するように構成されたプロセッサ・パイプラインと、第1のスレッドの命令が感知命令として指定されたことを検出し、感知命令の検出に応答して、感知命令がプロセッサ・パイプラインの実行ユニットによって実行されている間に、プロセッサ・パイプラインの実行ユニットを使用して第1のスレッド以外のスレッドの命令が実行されることを阻止するように構成されたスレッド・ハザード回路とを含む。

40

【0005】

この実装形態では、スレッドの設計状態が分離されたことを検証する単一の命令のみを保護することができ、非設計状態を考慮することはできない。

【0006】

すべてのセキュア作業のためのコアを恒久的に確保することはできるが、常時セキュア作業を行わない場合、これでは全体的なプロセッサ性能を事実上低減させる可能性がある。さらに、コンピュータ・システム上の作業の大部分がセキュア環境の実行を要求した場合でも、これは拡張しない。

【発明の概要】

【0007】

50

処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ実装方法が提案され、処理ユニットは、少なくとも1つのプロセッサ・コアによって、第1の実行モードを走らせて、少なくとも1つのプロセッサ・コア上でプログラム・コードを実行し、少なくとも1つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成される。この方法は、(i) 少なくとも1つのプロセッサ・コア上のプログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、(ii) 少なくとも1つのプロセッサ・コアをセキュア・コード・セグメントのための排他的セキュア実行に設定することと、(iii) 少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することと、(iv) 少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、(v) 少なくとも1つのプロセッサ・コアを少なくとも1つのプロセッサ・コア上でプログラム・コードを実行するための第1の実行モードに設定することとを少なくとも含む。

10

【0008】

提案する方法によれば、セキュア・コード・セグメントは、少なくとも最小の時間および最小の動作命令数に対して、排他的セキュア・コンテキストを要求することができる。これは、ハードウェア制御下で、物理コアを排他的セキュア・モードに少なくとも確実に設定することと、最小の時間または動作命令数あるいはその両方に対して中断なく実行することと、最後に、セキュア・コード・セグメントを終了するとき、あるいは初期期間もしくは動作命令数またはその両方の後に中断を行うとき、キャッシュ・ストレージまたはレジスタまたはメモリから物理コアの少なくとも設計および非設計状態を一掃することを含む。

20

【0009】

有利には、プロセッサ・コア内の異なるコード・セグメント間の干渉を回避することができる。コード・セグメントの実行中の障害の数を低減させることができる。さらに、好ましくは、プロセッサ・コア内のセキュア・コード・セグメントのセキュア動作の提案する方法によって、コンピュータ・システムの性能を向上させることができる。

【0010】

本発明の一実施形態により、追加的または代替的に、プロセッサ・コアを排他的セキュア・モードに設定する前に、物理プロセッサ・コアの少なくとも設計および非設計状態を保存することができる。したがって、セキュア・コード・セグメントの実行を終了した後、物理プロセッサ・コアの設計および非設計状態を回復して、プログラム・コードの正常実行を継続することが可能になる。

30

【0011】

本発明の一実施形態により、追加的または代替的に、プロセッサ・コアを第1の実行モードに設定する前に、物理プロセッサ・コアの少なくとも設計および非設計状態を回復することができる。したがって、セキュア・コード・セグメントの実行を終了した後、物理プロセッサ・コアの設計および非設計状態を回復して、プログラム・コードの正常実行を継続することができる。

【0012】

本発明の一実施形態により、追加的または代替的に、セキュア・コード・セグメントを実行する前に、特に物理プロセッサ・コアの少なくとも1つのキャッシュ・ストレージから、物理プロセッサ・コアの非設計状態を一掃することができる。これによって、セキュア・コード・セグメントが実行された場合に、すでに存在するデータとの干渉が生じなくなる。

40

【0013】

本発明の一実施形態により、追加的または代替的に、物理プロセッサ・コアの非設計状態を一掃することは、処理ユニットのハードウェアによってハードウェア制御式に実行することができる。好ましくは、ソフトウェア障害およびそれに続く不十分な一掃のリスクを低減させることができる。

50

【0014】

本発明の一実施形態により、追加的または代替的に、プロセッサ・コアの第1の実行モードは、同時マルチスレッディング・モードとすることができる。同時マルチスレッディングにより、プロセッサ・アーキテクチャによって提供される資源を複数の独立した実行スレッドがより良好に利用することが可能になり、これが通常のプロセッサ・コアの正常実行モードである。

【0015】

本発明の一実施形態により、追加的または代替的に、セキュア・コード・セグメントの中断不能な実行を、最小の期間または最小の命令数あるいはその両方に対して定義することができる。したがって、効率的な処理のために、セキュア・コード・セグメントの妨げられない実行を保証することができる。

10

【0016】

本発明の一実施形態により、追加的または代替的に、セキュア・コード・セグメントの中断不能な実行は、状態機械によって制御することができる。状態機械は、セキュア・コード・セグメントの中断不能な実行を制御する効率的な方法となることができる。

【0017】

本発明の一実施形態により、追加的または代替的に、セキュア・コード・セグメントの実行中の中断を阻止することができる。好ましくは、セキュア・コード・セグメントは、最小の時間量または動作命令数あるいはその両方に対して、混乱なく実行することができる。

20

【0018】

本発明の一実施形態により、追加的または代替的に、セキュア・コード・セグメントの実行後に少なくとも1つのプロセッサ・コアから設計および非設計状態を一掃することは、中断要求によって開始することができる。したがって、第1の実行状態におけるプログラム・コードのさらなる正常実行を、セキュア・コード・セグメントの実行からの残りのデータとの干渉なく実現することができる。

【0019】

本発明の一実施形態により、追加的または代替的に、仮想機械上またはコンテナ上で動作命令を実装することができる。好ましくは、クラウド内またはオンプレミスの異なる顧客からの同じ物理コア上で走るプロセス／スレッドを、仮想機械上またはコンテナ上で仮想化することができる。

30

【0020】

さらに、処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ・システムが提案され、処理ユニットは、少なくとも1つのプロセッサ・コアによって構成される。コンピュータ・システムは、少なくとも1つのプロセッサ・コアを有する少なくとも1つのプロセッサ・ユニットを備え、プロセッサ・コアは、第1の実行モードを走らせて、少なくとも1つのプロセッサ・コア上でプログラム・コードを実行し、少なくとも1つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成される。コンピュータ・システムは、(i) 少なくとも1つのプロセッサ・コア上のプログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、(ii) 少なくとも1つのプロセッサ・コアをセキュア・コード・セグメントのための排他的セキュア実行に設定することと、(iii) 少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することと、(iv) 少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、(v) 少なくとも1つのプロセッサ・コアを少なくとも1つのプロセッサ・コア上でプログラム・コードを実行するための第1の実行モードに設定することとを少なくとも含む方法を実行するように構成される。

40

【0021】

提案するコンピュータ・システム上を走ることによって、セキュア・コード・セグメントは、少なくとも最小の時間または最小の動作命令数あるいはその両方に対して、排他的

50

セキュア・コンテキストを要求することができる。これは、ハードウェア制御下で、物理コアを排他的セキュア・モードに少なくとも確実に設定することと、最小の時間または動作命令数あるいはその両方に対して中断なく実行することと、最後に、セキュア・コード・セグメントを終了するとき、あるいは初期期間もしくは動作命令数またはその両方の後に中断を行うとき、物理コアのキャッシュ・ストレージまたはレジスタまたはメモリから少なくとも設計および非設計状態を一掃することを含む。

【0022】

有利には、プロセッサ・コア内の異なるコード・セグメント間の干渉を回避することができる。コード・セグメントの実行中の障害の数を低減させることができる。さらに、好ましくは、プロセッサ・コア内のセキュア・コード・セグメントのセキュア動作の提案する方法によって、コンピュータ・システムの性能を向上させることができる。

10

【0023】

本発明の一実施形態により、追加的または代替的に、コンピュータ・システムは、プロセッサ・コアを排他的セキュア・モードに設定する前に、物理プロセッサ・コアの少なくとも設計および非設計状態を保存するように構成することができる。したがって、セキュア・コード・セグメントの実行を終了した後、物理プロセッサ・コアの設計および非設計状態を回復して、プログラム・コードの正常実行を継続することが可能になる。

【0024】

本発明の一実施形態により、追加的または代替的に、コンピュータ・システムは、プロセッサ・コアが第1の実行モードに設定される前に、物理プロセッサ・コアの少なくとも設計および非設計状態を回復するように構成することができる。したがって、セキュア・コード・セグメントの実行を終了した後、物理プロセッサ・コアの設計および非設計状態を回復して、プログラム・コードの正常実行を継続することができる。

20

【0025】

本発明の一実施形態により、追加的または代替的に、コンピュータ・システムは、セキュア・コード・セグメントが実行される前に、特に物理プロセッサ・コアの少なくとも1つのキャッシュ・ストレージから、物理プロセッサ・コアの非設計状態を一掃するように構成することができる。これによって、セキュア・コード・セグメントが実行された場合に、すでに存在するデータとの干渉が生じなくなる。

【0026】

本発明の一実施形態により、追加的または代替的に、コンピュータ・システムは、物理プロセッサ・コアの非設計状態を処理ユニットのハードウェアによってハードウェア制御式に一掃するように構成することができる。好ましくは、ソフトウェア障害およびそれに続く不十分な一掃のリスクを低減させることができる。

30

【0027】

本発明の一実施形態により、追加的または代替的に、プロセッサ・コアの第1の実行モードは、同時マルチスレディング・モードとすることができる。同時マルチスレディングにより、プロセッサ・アーキテクチャによって提供される資源を複数の独立した実行スレッドがより良好に利用することが可能になり、これが通常のプロセッサ・コアの正常実行モードである。

40

【0028】

本発明の一実施形態により、追加的または代替的に、コンピュータ・システムは、最小の期間または最小の命令数あるいはその両方に対して、セキュア・コード・セグメントを中断不能に実行するように構成することができる。したがって、効率的な処理のために、セキュア・コード・セグメントの妨げられない実行を保証することができる。

【0029】

本発明の一実施形態により、追加的または代替的に、セキュア・コード・セグメントの中断不能な実行は、状態機械によって制御することができる。状態機械は、セキュア・コード・セグメントの中断不能な実行を制御する効率的な方法となることができる。

【0030】

50

本発明の一実施形態により、追加的または代替的に、コンピュータ・システムは、セキュア・コード・セグメントの実行中の中断を阻止するように構成することができる。好ましくは、セキュア・コード・セグメントは、最小の時間量または動作命令数あるいはその両方に対して、混乱なく実行することができる。

本発明の一実施形態により、追加的または代替的に、セキュア・コード・セグメントの実行後に少なくとも1つのプロセッサ・コアから設計および非設計状態を一掃することは、中断要求によって開始することができる。したがって、第1の実行状態におけるプログラム・コードのさらなる正常実行を、セキュア・コード・セグメントの実行からの残りのデータとの干渉なく実現することができる。

【0031】

本発明の一実施形態により、追加的または代替的に、仮想機械上またはコンテナ上で動作命令を実装することができる。好ましくは、クラウド内またはオンプレミスの異なる顧客からの同じ物理コア上で走るプロセス／スレッドを、仮想機械上またはコンテナ上で仮想化することができる。

【0032】

さらに、処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるための好ましいコンピュータ・プログラム製品が提案され、処理ユニットは、少なくとも1つのプロセッサ・コアによって構成される。コンピュータ・システムは、少なくとも1つのプロセッサ・コアを有する少なくとも1つのプロセッサ・ユニットを備え、プロセッサ・コアは、第1の実行モードを走らせて、少なくとも1つのプロセッサ・コア上でプログラム・コードを実行し、少なくとも1つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成される。

【0033】

コンピュータ・プログラム製品は、プログラム命令が実施されたコンピュータ可読記憶媒体を備え、プログラム命令は、コンピュータ・システムによって、(i) 少なくとも1つのプロセッサ・コア上のプログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、(ii) 少なくとも1つのプロセッサ・コアをセキュア・コード・セグメントのための排他的セキュア実行に設定することと、(iii) 少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することと、(iv) 少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、(v) 少なくとも1つのプロセッサ・コアを少なくとも1つのプロセッサ・コア上でプログラム・コードを実行するための第1の実行モードに設定することとを含む方法をコンピュータ・システムに実行させるように実行可能である。

【0034】

さらに、上述した方法を実行するためのコンピュータ可読プログラム命令を含む、データ処理プログラムを実行するためのデータ処理システムが提案される。

【0035】

本発明は、上記および他の目的および利点と併せて、実施形態の以下の詳細な説明から最もよく理解することができるが、これらの実施形態に制限されるものではない。

【図面の簡単な説明】

【0036】

【図1】本発明の一実施形態による処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ実装方法の流れ図である。

【図2】本発明による方法を実行するためのデータ処理システムの例示的な実施形態を示す図である。

【発明を実施するための形態】

【0037】

図面では、同様の要素が等しい参照番号で参照される。これらの図面は、単に概略的な表現であり、本発明の特有のパラメータについて説明することを意図したものではない。

10

20

30

40

50

さらに、これらの図面は、本発明の典型的な実施形態のみを示すことが意図されており、したがって本発明の範囲を限定すると見なされるべきではない。

【0038】

本明細書に記載する例示的な実施形態は、処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ・システムを提供し、処理ユニットは、少なくとも1つのプロセッサ・コアによって構成される。コンピュータ・システムは、少なくとも1つのプロセッサ・コアを有する少なくとも1つのプロセッサ・ユニットを備え、プロセッサ・コアは、第1の実行モードを走らせて、少なくとも1つのプロセッサ・コア上でプログラム・コードを実行し、少なくとも1つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成される。

10

【0039】

例示的な実施形態は、(i)少なくとも1つのプロセッサ・コア上のプログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、(ii)少なくとも1つのプロセッサ・コアをセキュア・コード・セグメントのための排他的セキュア実行に設定することと、(iii)少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することと、(iv)少なくとも1つのプロセッサ・コアから設計および非設計状態を一掃することと、(v)少なくとも1つのプロセッサ・コアを少なくとも1つのプロセッサ・コア上のプログラム・コードのための第1の実行モードに設定することとを少なくとも含む方法にさらに使用することができる。

20

【0040】

図1は、本発明の一実施形態による図2に示す処理ユニット216のプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ実装方法の流れ図を示す。

【0041】

処理ユニット216は、少なくとも1つのプロセッサ・コアによって、第1の実行モードを走らせて、少なくとも1つのプロセッサ・コア上でプログラム・コードを正常実行として実行するように構成される。

【0042】

プロセッサ・コアの第1の実行モードは、同時マルチスレッディング・モードとすることができる。同時マルチスレッディングにより、プロセッサ・アーキテクチャによって提供される資源を複数の独立した実行スレッドがより良好に利用することが可能になり、これが通常のプロセッサ・コアの正常実行モードである。

30

【0043】

仮想機械上またはコンテナ上で動作命令を実装することができる。好ましくは、クラウド内またはオンプレミスの異なる顧客からの同じ物理コア上で走るプロセス／スレッドを、仮想機械上またはコンテナ上で仮想化することができる。

【0044】

ステップS100において、第1の実行モードの少なくとも1つのプロセッサ・コア上で、動作命令のプログラム・コードが実行される。

【0045】

ステップS102において、少なくとも1つのプロセッサ・コア上のプログラム・コードのセキュア・コード・セグメントの排他的セキュア実行のために、排他的セキュア・モードが要求される。

40

【0046】

任意選択で、ステップS104において、プロセッサ・コアを排他的セキュア・モードに設定する前に、物理プロセッサ・コアの少なくとも設計および非設計状態を保存することができる。したがって、セキュア・コード・セグメントの実行を終了した後、物理プロセッサ・コアの設計および非設計状態を回復して、プログラム・コードの正常実行を継続することが可能になる。

【0047】

50

次に、ステップ S 1 0 6 において、少なくとも 1 つのプロセッサ・コアは、セキュア・コード・セグメントのための排他的セキュア実行に設定される。

【 0 0 4 8 】

また任意選択で、ステップ S 1 0 8 において、セキュア・コード・セグメントを実行する前に、物理プロセッサ・コアの非設計状態を一掃することができる。特に、物理プロセッサ・コアの少なくとも 1 つのキャッシュ・ストレージまたはレジスタまたはメモリから、非設計状態を一掃することができる。物理プロセッサ・コアの非設計状態を一掃することは、処理ユニット 2 1 6 のハードウェアによってハードウェア制御式に実行することができる。好ましくは、ソフトウェア障害およびそれに続く不十分な一掃のリスクを低減させることができる。これによって、セキュア・コード・セグメントが実行された場合に、すでに存在するデータとの干渉が生じなくなる。

10

【 0 0 4 9 】

次いで、ステップ S 1 1 0 において、少なくとも 1 つのプロセッサ・コア上でセキュア・コード・セグメントが実行される。セキュア・コード・セグメントは、最小の期間または最小の命令数あるいはその両方に対して、中断不能に実行される。セキュア・コード・セグメントの中断不能な実行は、状態機械によって制御することができる。状態機械は、セキュア・コード・セグメントの中断不能な実行を制御する効率的な方法となることができる。

【 0 0 5 0 】

セキュア・コード・セグメントの実行中は、中断を阻止することができる。したがって、効率的な処理のために、セキュア・コード・セグメントの妨げられない実行を保証することができる。好ましくは、セキュア・コード・セグメントは、最小の時間量または動作命令数あるいはその両方に対して、混乱なく実行することができる。

20

【 0 0 5 1 】

セキュア・コード・セグメントの実行を終了した後、ステップ S 1 1 2 において、特に少なくとも 1 つのプロセッサ・コアの少なくとも 1 つのキャッシュ・ストレージまたはレジスタまたはメモリから、設計および非設計状態を一掃することができる。セキュア・コード・セグメントの実行後に少なくとも 1 つのプロセッサ・コアから設計および非設計状態を一掃することは、中断要求によって開始することができる。したがって、第 1 の実行状態におけるプログラム・コードのさらなる正常実行を、セキュア・コード・セグメントの実行からの残りのデータとの干渉なく実現することができる。

30

【 0 0 5 2 】

任意選択で、ステップ S 1 0 4 で設計および非設計状態が保存された場合、ステップ S 1 1 2 において、プロセッサ・コアを第 1 の実行モードに設定する前に、物理プロセッサ・コアの少なくとも設計および非設計状態を回復することができる。したがって、セキュア・コード・セグメントの実行を終了した後、物理プロセッサ・コアの設計および非設計状態を回復して、プログラム・コードの正常実行を継続することができる。

【 0 0 5 3 】

次いで、ステップ S 1 1 4 において、少なくとも 1 つのプロセッサ・コアは、少なくとも 1 つのプロセッサ・コア上のプログラム・コードのための第 1 の実行モードに設定され、ステップ S 1 1 6 において正常実行を継続する。

40

【 0 0 5 4 】

図 2 を次に参照すると、データ処理システム 2 1 0 の一例の概略図が示されている。データ処理システム 2 1 0 は、好適なデータ処理システムの一例にすぎず、本明細書に記載する本発明の実施形態の使用または機能範囲に対する何らかの限定を示唆することを意図したものではない。それにもかかわらず、データ処理システム 2 1 0 は、本明細書に上述した機能のいずれかで実装されること、または本明細書に上述した機能のいずれかを実行すること、あるいはその両方が可能である。

【 0 0 5 5 】

データ処理システム 2 1 0 内にはコンピュータ・システム／サーバ 2 1 2 が設けられ、

50

コンピュータ・システム／サーバ 212 は、多数の他の汎用または特別目的のコンピューティング・システム環境または構成で動作する。コンピュータ・システム／サーバ 212 とともに好適に使用することができるよく知られているコンピューティング・システム、環境、または構成、あるいはその組合せの例には、それだけに限定されるものではないが、パーソナル・コンピュータ・システム、サーバ・コンピュータ・システム、シン・クライアント、シック・クライアント、手持ち式またはラップトップ・デバイス、マルチプロセッサ・システム、マイクロプロセッサ・ベース・システム、セット・トップ・ボックス、プログラム可能な消費者電子機器、ネットワーク PC、ミニコンピュータ・システム、メインフレーム・コンピュータ・システム、および上記のシステムまたはデバイスのいずれかを含む分散型クラウド・コンピューティング環境などが含まれる。

10

【0056】

コンピュータ・システム／サーバ 212 は、プログラム・モジュールなどのコンピュータ・システム実行可能命令が、コンピュータ・システムによって実行されるという概略的な文脈で説明することができる。概して、プログラム・モジュールは、特定のタスクの実行または特定の抽象データ型の実装を行うルーチン、プログラム、オブジェクト、コンポーネント、論理、データ構造などを含むことができる。コンピュータ・システム／サーバ 212 は、通信ネットワークを介してリンクされた遠隔処理デバイスによってタスクが実行される分散型クラウド・コンピューティング環境内で実施することができる。分散型クラウド・コンピューティング環境において、プログラム・モジュールは、メモリ記憶デバイスを含むローカルおよび遠隔の両方のコンピュータ・システム記憶媒体内に位置することができる。

20

【0057】

図 2 に示すように、データ処理システム 210 内のコンピュータ・システム／サーバ 212 は、汎用コンピューティング・デバイスの形態で示されている。コンピュータ・システム／サーバ 212 の構成要素は、それだけに限定されるものではないが、1つまたは複数のプロセッサまたは処理ユニット 216 と、システム・メモリ 228 と、システム・メモリ 228 を含む様々なシステム構成要素を処理ユニット 216 に結合するバス 218 とを含むことができる。

【0058】

バス 218 は、メモリ・バスまたはメモリ・コントローラ、周辺バス、アクセラレータッド・グラフィックス・ポート、および様々なバス・アーキテクチャのうちのいずれかを使用するプロセッサまたはローカル・バスを含む、いくつかのタイプのバス構造のいずれかのうちの1つまたは複数を代表する。限定ではなく例として、そのようなアーキテクチャには、Industry Standard Architecture (ISA) バス、Micro Channel Architecture (MCA) バス、Enhanced ISA (EISA) バス、Video Electronics Standards Association (VESA) ローカル・バス、およびPeripheral Component Interconnect (PCI) バスが含まれる。

30

【0059】

コンピュータ・システム／サーバ 212 は、典型的には、様々なコンピュータ・システム可読媒体を含む。そのような媒体は、コンピュータ・システム／サーバ 212 によってアクセス可能である任意の利用可能な媒体とすることができ、そのような媒体には、揮発性媒体および不揮発性媒体の両方、取り外し可能媒体および取り外し不能媒体の両方が含まれる。

40

【0060】

システム・メモリ 228 は、ランダム・アクセス・メモリ (RAM) 230 またはキャッシュ・メモリ 232 あるいはその両方などの揮発性メモリの形態のコンピュータ・システム可読媒体を含むことができる。コンピュータ・システム／サーバ 212 は、他の取り外し可能／取り外し不能な揮発性／不揮発性コンピュータ・システム記憶媒体をさらに含むことができる。例示のみを目的として、記憶システム 234 は、取り外し不能な不揮発

50

性磁気媒体（示されていないが、典型的には「ハード・ドライブ」と呼ばれる）からの読み取りおよびそこへの書き込みのために設けることができる。示されていないが、取り外し可能な不揮発性磁気ディスク（たとえば、「フロッピー（Ｒ）・ディスク」）からの読み取りおよびそこへの書き込みのための磁気ディスク・ドライブ、ならびにＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、または他の光学媒体などの取り外し可能な不揮発性光学ディスクからの読み取りまたはそこへの書き込みのための光学ディスク・ドライブを設けることができる。そのような事例では、１つまたは複数のデータ媒体インターフェースによって、各々をバス２１８に接続することができる。さらに図示および後述するように、メモリ２２８は、本発明の実施形態の機能を実施するように構成された１組（たとえば、少なくとも１つ）のプログラム・モジュールを有する少なくとも１つのプログラム製品を含むことができる。

10

【００６１】

限定ではなく例として、オペレーティング・システム、１つまたは複数のアプリケーション・プログラム、他のプログラム・モジュール、およびプログラム・データと同様に、１組（少なくとも１つ）のプログラム・モジュール２４２を有するプログラム／ユーティリティ２４０を、メモリ２２８内に記憶することができる。オペレーティング・システム、１つまたは複数のアプリケーション・プログラム、他のプログラム・モジュール、およびプログラム・データの各々、またはこれらの組合せは、ネットワーキング環境の一実装形態を含むことができる。プログラム・モジュール２４２は、概して、本明細書に記載する本発明の実施形態の機能または方法あるいはその両方を実施する。

20

【００６２】

コンピュータ・システム／サーバ２１２はまた、キーボード、ポインティング・デバイス、ディスプレイ２２４などの１つもしくは複数の外部デバイス２１４、ユーザがコンピュータ・システム／サーバ２１２と対話することを可能にする１つもしくは複数のデバイス、またはコンピュータ・システム／サーバ２１２が１つもしくは複数の他のコンピューティング・デバイスと通信することを可能にする任意のデバイス（たとえば、ネットワーク・カード、モデムなど）、あるいはその組合せと通信することができる。そのような通信は、入出力（Ｉ／Ｏ）インターフェース２２２を介して行うことができる。さらに、コンピュータ・システム／サーバ２１２は、ローカル・エリア・ネットワーク（ＬＡＮ）、汎用ワイド・エリア・ネットワーク（ＷＡＮ）、またはパブリック・ネットワーク（たとえば、インターネット）、あるいはその組合せなどの１つまたは複数のネットワークと、ネットワーク・アダプタ２２０を介して通信することができる。示されているように、ネットワーク・アダプタ２２０は、バス２１８を介してコンピュータ・システム／サーバ２１２の他の構成要素と通信する。示されていないが、他のハードウェアまたはソフトウェア構成要素あるいはその両方を、コンピュータ・システム／サーバ２１２とともに使用することもできることを理解されたい。例には、それだけに限定されるものではないが、マイクロコード、デバイス・ドライバ、冗長処理ユニット、外部ディスク・ドライブ・アレイ、ＲＡＩＤシステム、テープ・ドライブ、およびデータ保存記憶システムなどが含まれる。

30

【００６３】

本発明は、システム、方法、またはコンピュータ・プログラム製品、あるいはその組合せとすることができる。コンピュータ・プログラム製品は、本発明の態様をプロセッサに実施させるためのコンピュータ可読プログラム命令を有するコンピュータ可読記憶媒体（または複数の媒体）を含むことができる。

40

【００６４】

コンピュータ可読記憶媒体は、命令実行デバイスが使用するための命令を保持および記憶することができる有形のデバイスとすることができる。コンピュータ可読記憶媒体は、たとえば、それだけに限定されるものではないが、電子記憶デバイス、磁気記憶デバイス、光学記憶デバイス、電磁記憶デバイス、半導体記憶デバイス、または上記の任意の好適な組合せとすることができる。コンピュータ可読記憶媒体のより具体的な例の非網羅的な

50

リストには、携帯型コンピュータ・ディスク、ハード・ディスク、ランダム・アクセス・メモリ（RAM）、リード・オンリー・メモリ（ROM）、消去可能なプログラム可能リード・オンリー・メモリ（EPROMまたはフラッシュ・メモリ）、スタティック・ランダム・アクセス・メモリ（SRAM）、携帯型コンパクト・ディスク・リード・オンリー・メモリ（CD-ROM）、デジタル多用途ディスク（DVD）、メモリ・スティック、フロッピー（R）・ディスク、パンチカードなどの機械的に符号化されたデバイス、または命令が記録された溝の中の凸状構造、および上記の任意の好適な組合せが含まれる。本明細書では、コンピュータ可読記憶媒体は、無線波もしくは他の自由に伝播する電磁波、導波管もしくは他の伝送媒体を通して伝播する電磁波（たとえば、光ファイバ・ケーブルを通過する光パルス）、またはワイアを通して伝送される電気信号などの一時的な信号自体であると解釈されるべきではない。

10

本明細書に記載するコンピュータ可読プログラム命令は、コンピュータ可読記憶媒体からそれぞれのコンピューティング／処理デバイスへ、あるいはネットワーク、たとえばインターネット、ローカル・エリア・ネットワーク、ワイド・エリア・ネットワーク、もしくは無線ネットワークまたはその組合せを介して外部コンピュータまたは外部記憶デバイスへ、ダウンロードすることができる。ネットワークは、銅伝送ケーブル、光伝送ファイバ、無線伝送、ルータ、ファイアウォール、スイッチ、ゲートウェイ・コンピュータ、またはエッジ・サーバ、あるいはその組合せを含むことができる。各コンピューティング／処理デバイス内のネットワーク・アダプタ・カードまたはネットワーク・インターフェースは、ネットワークからコンピュータ可読プログラム命令を受信し、それぞれのコンピューティング／処理デバイス内のコンピュータ可読記憶媒体に記憶するためにコンピュータ可読プログラム命令を転送する。

20

本発明の動作を実施するためのコンピュータ可読プログラム命令は、アセンブラ命令、命令セット・アーキテクチャ（ISA）命令、機械命令、機械依存命令、マイクロコード、ファームウェア命令、状態設定データ、またはSmalltalk、C++などのオブジェクト指向プログラミング言語、および「C」プログラミング言語もしくは類似のプログラミング言語などの従来の手続き型プログラミング言語を含む1つもしくは複数のプログラミング言語の任意の組合せで書かれたソース・コードもしくはオブジェクト・コードとすることができる。コンピュータ可読プログラム命令は、完全にユーザのコンピュータ上で、部分的にユーザのコンピュータ上で、独立型のソフトウェア・パッケージとして、部分的にユーザのコンピュータ上かつ部分的に遠隔コンピュータ上で、または完全に遠隔コンピュータもしくはサーバ上で実行することができる。後者のシナリオでは、遠隔コンピュータは、ローカル・エリア・ネットワーク（LAN）もしくはワイド・エリア・ネットワーク（WAN）を含む任意のタイプのネットワークを介してユーザのコンピュータに接続することができ、または外部コンピュータに（たとえば、インターネット・サービス・プロバイダを使用してインターネットを介して）接続することができる。いくつかの実施形態では、たとえばプログラム可能論理回路、フィールド・プログラム可能ゲート・アレイ（FPGA）、またはプログラム可能論理アレイ（PLA）を含む電子回路が、本発明の態様を実行するために、電子回路をパーソナライズするためのコンピュータ可読プログラム命令の状態情報を利用することによって、コンピュータ可読プログラム命令を実行することができる。

30

40

本発明の態様について、本発明の実施形態による方法、装置（システム）、およびコンピュータ・プログラム製品の流れ図またはブロック図あるいはその両方を参照して本明細書に説明する。流れ図またはブロック図あるいはその両方の各ブロック、および流れ図またはブロック図あるいはその両方のブロックの組合せは、コンピュータ可読プログラム命令によって実装することができることが理解されよう。

【0065】

これらのコンピュータ可読プログラム命令は、コンピュータまたは他のプログラム可能データ処理装置のプロセッサを介して実行される命令が、流れ図またはブロック図あるいはその両方の1つまたは複数のブロックに指定された機能／動作を実装するための手段を

50

もたらしように、汎用コンピュータ、特別目的コンピュータ、または他のプログラム可能データ処理装置のプロセッサに提供されて、機械を作り出すことができる。これらのコンピュータ可読プログラム命令はまた、命令が記憶されたコンピュータ可読記憶媒体が、流れ図またはブロック図あるいはその両方の1つまたは複数のブロックに指定された機能／動作の態様を実装する命令を含む製品を備えるように、コンピュータ可読記憶媒体内に記憶することができ、コンピュータ、プログラム可能データ処理装置、または他のデバイス、あるいはその組合せに特定の方式で機能するように指示することができる。

【0066】

コンピュータ可読プログラム命令はまた、コンピュータ、他のプログラム可能装置、または他のデバイス上で実行される命令が、流れ図またはブロック図あるいはその両方の1つまたは複数のブロックに指定された機能／動作を実装するように、コンピュータ、他のプログラム可能データ処理装置、または他のデバイスへロードされて、コンピュータ、他のプログラム可能装置、または他のデバイス上で一連の動作ステップを実行させ、コンピュータ実装プロセスを作り出すことができる。

【0067】

これらの図の流れ図およびブロック図は、本発明の様々な実施形態によるシステム、方法、およびコンピュータ・プログラム製品の可能な実装形態のアーキテクチャ、機能、および動作を示す。これに関して、流れ図またはブロック図内の各ブロックは、命令のモジュール、セグメント、または部分を表すことができ、命令は、指定された論理機能を実装するための1つまたは複数の実行可能な命令を含む。いくつかの代替実装形態では、ブロック内に記載する機能は、これらの図に示す順序以外で行うことができる。たとえば、関連する機能に応じて、連続して示されている2つのブロックが、実際には実質的に同時に実行されることがあり、またはこれらのブロックが逆の順序で実行されることもある。ブロック図または流れ図あるいはその両方の各ブロック、およびブロック図または流れ図あるいはその両方のブロックの組合せは、指定された機能もしくは動作を実行するまたは特別目的ハードウェアおよびコンピュータ命令の組合せを実施する特別目的ハードウェア・ベース・システムによって実装することができることにも留意されたい。

【0068】

本発明の様々な実施形態の説明は、例示の目的で提示されており、開示する実施形態に対して網羅的または限定的であることを意図したものではない。記載する実施形態の範囲および精神から逸脱することなく、多くの修正形態および変形形態が当業者には明らかである。本明細書で使用する術語は、実施形態の原理、実際の応用例、もしくは市場で見られる技術に対する技術的改善について最もよく説明するために、または当業者であれば本明細書に開示する実施形態を理解することが可能になるように選択されたものである。

【0069】

本開示のさらなる例示的な実施形態について、以下の番号付きの条項に記載する。

【0070】

番号付き条項1：処理ユニット（216）のプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ実装方法であって、処理ユニット（216）が、少なくとも1つのプロセッサ・コアによって、第1の実行モードを走らせて、少なくとも1つのプロセッサ・コア上でプログラム・コードを実行し、少なくとも1つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成され、この方法が、
（i）少なくとも1つのプロセッサ・コア上のプログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、

（ii）少なくとも1つのプロセッサ・コアをセキュア・コード・セグメントのための排他的セキュア実行に設定することと、

（iii）少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することと、

（iv）少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、

10

20

30

40

50

(v) 少なくとも1つのプロセッサ・コアを少なくとも1つのプロセッサ・コア上でプログラム・コードを実行するための第1の実行モードに設定することとを少なくとも含む、方法。

【0071】

番号付き条項2：プロセッサ・コアを排他的セキュア・モードに設定する前に、物理プロセッサ・コアの少なくとも設計状態および非設計状態をさらに保存する、番号付き条項1に記載の方法。

【0072】

番号付き条項3：プロセッサ・コアを第1の実行モードに設定する前に、物理プロセッサ・コアの少なくとも設計状態および非設計状態をさらに回復する、番号付き条項1または2に記載の方法。

【0073】

番号付き条項4：セキュア・コード・セグメントを実行する前に、物理プロセッサ・コアの少なくとも1つのキャッシュ・ストレージから物理プロセッサ・コアの非設計状態をさらに一掃する、番号付き条項1ないし3のいずれか一項に記載の方法。

【0074】

番号付き条項5：物理プロセッサ・コアの非設計状態を一掃することが、処理ユニット(216)のハードウェアによってハードウェア制御式に実行される、番号付き条項4に記載の方法。

【0075】

番号付き条項6：プロセッサ・コア上でプログラム・コードを実行するための第1の実行モードが、同時マルチスレディング・モードである、番号付き条項1ないし5のいずれか一項に記載の方法。

【0076】

番号付き条項7：少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することが、最小の期間または最小の命令数あるいはその両方に対して定義される、番号付き条項1ないし6のいずれか一項に記載の方法。

【0077】

番号付き条項8：少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することが、状態機械によって制御される、番号付き条項1ないし7のいずれか一項に記載の方法。

番号付き条項9：セキュア・コード・セグメントの実行中の中断が阻止される、番号付き条項1ないし8のいずれか一項に記載の方法。

【0078】

番号付き条項10：セキュア・コード・セグメントの実行後に少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することが、中断要求によって開始される、番号付き条項1ないし9のいずれか一項に記載の方法。

【0079】

番号付き条項11：仮想機械上またはコンテナ上で動作命令が実装される、番号付き条項1ないし10のいずれか一項に記載の方法。

【0080】

番号付き条項12：処理ユニット(216)のプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ・システム(212)であって、処理ユニット(216)が、少なくとも1つのプロセッサ・コアによって構成され、コンピュータ・システム(212)が、少なくとも1つのプロセッサ・コアを有する少なくとも1つのプロセッサ・ユニット(216)を備え、プロセッサ・コアが、第1の実行モードを走らせて、少なくとも1つのプロセッサ・コア上でプログラム・コードを実行し、少なくとも1つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成され、コンピュータ・システム(212)が、

(i) 少なくとも1つのプロセッサ・コア上のプログラム・コードのセキュア・コード・

10

20

30

40

50

セグメントの排他的セキュア実行を要求することと、

(i i) 少なくとも1つのプロセッサ・コアをセキュア・コード・セグメントのための排他的セキュア実行に設定することと、

(i i i) 少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することと、

(i v) 少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、

(v) 少なくとも1つのプロセッサ・コアを少なくとも1つのプロセッサ・コア上でプログラム・コードを実行するための第1の実行モードに設定することとを少なくとも含む、番号付き条項1ないし11のいずれか一項に記載の方法を実行するように構成されている、コンピュータ・システム。

10

【0081】

番号付き条項13：プロセッサ・コアを排他的セキュア・モードに設定する前に、物理プロセッサ・コアの少なくとも設計状態および非設計状態を保存するように構成されている、番号付き条項12に記載のコンピュータ・システム。

【0082】

番号付き条項14：プロセッサ・コアが第1の実行モードに設定される前に、物理プロセッサ・コアの少なくとも設計状態および非設計状態を回復するように構成されている、番号付き条項12または13に記載のコンピュータ・システム。

【0083】

番号付き条項15：セキュア・コード・セグメントが実行される前に、物理プロセッサ・コアの少なくとも1つのキャッシュ・ストレージから物理プロセッサ・コアの非設計状態を一掃するように構成されている、番号付き条項12ないし14のいずれか一項に記載のコンピュータ・システム。

20

【0084】

番号付き条項16：物理プロセッサ・コアの非設計状態を処理ユニットのハードウェアによってハードウェア制御式に一掃するように構成されている、番号付き条項12ないし15のいずれか一項に記載のコンピュータ・システム。

【0085】

番号付き条項17：プロセッサ・コア上でプログラム・コードを実行するための第1の実行モードが、同時マルチスレッディング・モードである、番号付き条項12ないし16のいずれか一項に記載のコンピュータ・システム。

30

【0086】

番号付き条項18：最小の期間または最小の命令数あるいはその両方に対して、少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行するように構成されている、番号付き条項12ないし17のいずれか一項に記載のコンピュータ・システム。

【0087】

番号付き条項19：少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することが、状態機械によって制御される、番号付き条項12ないし18のいずれか一項に記載のコンピュータ・システム。

40

【0088】

番号付き条項20：セキュア・コード・セグメントの実行中の中断を阻止するように構成されている、番号付き条項12ないし19のいずれか一項に記載のコンピュータ・システム。

【0089】

番号付き条項21：セキュア・コード・セグメントの実行後に少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することが、中断要求によって開始される、番号付き条項12ないし20のいずれか一項に記載のコンピュータ・システム。

50

【0090】

番号付き条項22：仮想機械上またはコンテナ上で動作命令が実装される、番号付き条項12ないし21のいずれか一項に記載のコンピュータ・システム。

【0091】

番号付き条項23：処理ユニット(216)のプロセッサ・コア上でセキュア・コード・セグメントを動作させるためのコンピュータ・プログラム製品であって、処理ユニット(216)が、少なくとも1つのプロセッサ・コアによって、第1の実行モードを走らせて、少なくとも1つのプロセッサ・コア上でプログラム・コードを実行し、少なくとも1つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成され、コンピュータ・プログラム製品が、プログラム命令が実施されたコンピュータ可読記憶媒体を備え、プログラム命令が、コンピュータ・システム(212)によって、

(i) 少なくとも1つのプロセッサ・コア上のプログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、

(ii) 少なくとも1つのプロセッサ・コアをセキュア・コード・セグメントのための排他的セキュア実行に設定することと、

(iii) 少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することと、

(iv) 少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、

(v) 少なくとも1つのプロセッサ・コアを少なくとも1つのプロセッサ・コア上でプログラム・コードを実行するための第1の実行モードに設定することを含む、番号付き条項1ないし11のいずれか一項に記載の方法をコンピュータ・システム(212)に実行させるように実行可能である、コンピュータ・プログラム製品。

【0092】

番号付き条項24：番号付き条項1ないし11のいずれか一項に記載の方法を実行するためのコンピュータ可読プログラム命令を含む、データ処理プログラム(240)を実行するためのデータ処理システム(210)。

【0093】

番号付き条項25：処理ユニットのプロセッサ・コア上でセキュア・コード・セグメントを動作させるための命令を実行するための集積回路であって、処理ユニットが、少なくとも1つのプロセッサ・コアによって構成され、コンピュータ・システムが、少なくとも1つのプロセッサ・コアを有する少なくとも1つのプロセッサ・ユニットを備え、プロセッサ・コアが、第1の実行モードを走らせて、少なくとも1つのプロセッサ・コア上でプログラム・コードを実行し、少なくとも1つのプロセッサ・コア上で動作命令のプログラム・コードを実行するように構成され、集積回路が、

(i) 少なくとも1つのプロセッサ・コア上のプログラム・コードのセキュア・コード・セグメントの排他的セキュア実行を要求することと、

(ii) 少なくとも1つのプロセッサ・コアをセキュア・コード・セグメントのための排他的セキュア実行に設定することと、

(iii) 少なくとも1つのプロセッサ・コア上でセキュア・コード・セグメントを中断不能に実行することと、

(iv) 少なくとも1つのプロセッサ・コアから物理プロセッサ・コアの設計状態および非設計状態を一掃することと、

(v) 少なくとも1つのプロセッサ・コアを少なくとも1つのプロセッサ・コア上でプログラム・コードを実行するための第1の実行モードに設定することとを少なくとも含む、番号付き条項1ないし11のいずれか一項に記載の方法を実行するように構成されている、集積回路。

10

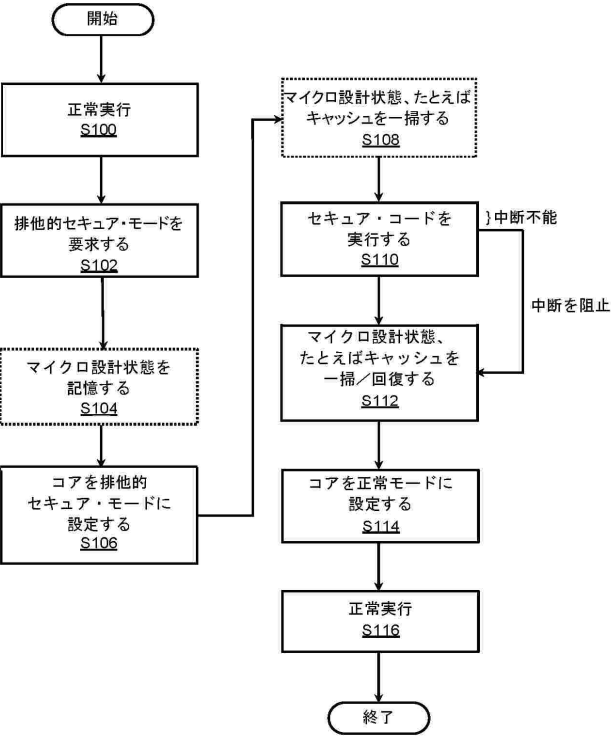
20

30

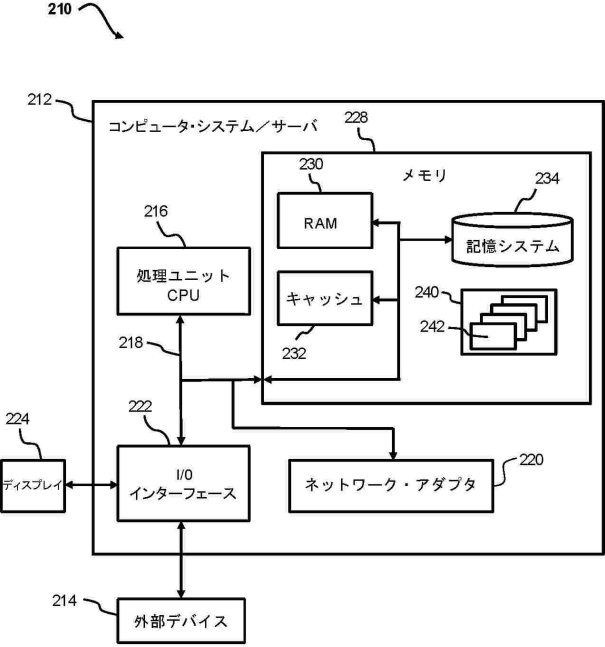
40

【図面】

【図 1】



【図 2】



10

20

30

40

50

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/081213

A. CLASSIFICATION OF SUBJECT MATTER

INV. **G06F9/48** **G06F9/50** **G06F21/74**
ADD. **G06F21/52** **G06F21/53** **G06F21/70** **G06F21/71**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 3 462 362 A1 (ST MICROELECTRONICS INC [US]) 3 April 2019 (2019-04-03) paragraph [0015] paragraph [0018] paragraph [0020] paragraph [0028] paragraph [0030] - paragraph [0032] paragraph [0077] paragraph [0085] - paragraph [0087] paragraph [0113] claim 1 paragraph [0109]	1-25
A	US 2014/230077 A1 (MUFF ADAM J [US] ET AL) 14 August 2014 (2014-08-14) the whole document	1-25

☒ 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

31 January 2023

Date of mailing of the international search report

08/02/2023

Name and mailing address of the ISA/
European Patent Office, P.B. 5618 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Alecu, Mihail

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/081213

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 112 800 431 A (ALIPAY HANGZHOU TECH CO LTD) 14 May 2021 (2021-05-14) the whole document & EP 3 961 446 A1 (ALIPAY HANGZHOU INF TECH CO LTD [CN]) 2 March 2022 (2022-03-02) the whole document -----	1-25
A	US 2019/034357 A1 (NUNEZ MENCIA ANGEL [DE] ET AL) 31 January 2019 (2019-01-31) paragraph [0020] -----	1-25

1

10

20

30

40

50

INTERNATIONAL SEARCH REPORT					International application No PCT/EP2022/081213	
Information on patent family members						
Patent document cited in search report		Publication date	Patent family member(s)		Publication date	
EP 3462362	A1	03-04-2019	CN	109582354 A	05-04-2019	
			EP	3462362 A1	03-04-2019	
			US	2019102538 A1	04-04-2019	
			US	2020380116 A1	03-12-2020	

US 2014230077	A1	14-08-2014	US	2014229690 A1	14-08-2014	
			US	2014230077 A1	14-08-2014	

CN 112800431	A	14-05-2021	CN	111753311 A	09-10-2020	
			CN	112800431 A	14-05-2021	
			EP	3961446 A1	02-03-2022	
			US	2022066809 A1	03-03-2022	

US 2019034357	A1	31-01-2019	CN	110998545 A	10-04-2020	
			DE	112018002947 T5	02-04-2020	
			GB	2578410 A	06-05-2020	
			JP	6955619 B2	27-10-2021	
			JP	2020528608 A	24-09-2020	
			US	2019034356 A1	31-01-2019	
			US	2019034357 A1	31-01-2019	
			US	2020110712 A1	09-04-2020	
			WO	2019021153 A1	31-01-2019	

フロントページの続き

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,N
E,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,
CV,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,I
T,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,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,ST,SV,
SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

(74)代理人 100120710

弁理士 片岡 忠彦

(72)発明者 リヒテナウ、セドリック

ドイツ 7 1 0 3 2 ベー布林ゲン シェーナハイチャー・シュトラーク 2 2 0

(72)発明者 ラング、ヤコブ

ドイツ 7 1 0 3 2 ベー布林ゲン シェーナハイチャー・シュトラーク 2 2 0

(72)発明者 パッシュ、エベルハルト

ドイツ 7 1 0 3 2 ベー布林ゲン シェーナハイチャー・シュトラーク 2 2 0

(72)発明者 ボントレーガー、クリスチャン

ドイツ 7 1 0 3 2 ベー布林ゲン シェーナハイチャー・シュトラーク 2 2 0