

【特許請求の範囲】**【請求項 1】**

オペレーティングシステムと、
プロセッサを含むプラットフォームであり、前記プロセッサはエラーレジスタを含む、
プラットフォームと、を備え、

前記オペレーティングシステムは、前記プラットフォームを介して前記エラーレジスタにセキュアな方式でのみ書き込むことができ、前記エラーレジスタは、前記プラットフォームを介して有効にされる及び／又は無効にされる、装置。

【請求項 2】

前記プラットフォームはさらに、システム管理モード機能を含み、前記オペレーティングシステムは、前記システム管理モード機能を介して前記エラーレジスタにセキュアな方式でのみ書き込むことができる、請求項 1 に記載の装置。

【請求項 3】

前記システム管理モード機能は、基本入出力システムに含まれる、請求項 2 に記載の装置。

【請求項 4】

前記オペレーティングシステムは、プラットフォームファームウェアを介して前記エラーレジスタにセキュアな方式でのみ書き込むことができる、請求項 1 に記載の装置。

【請求項 5】

前記エラーレジスタは、マシンチェックアーキテクチャレジスタ及びエラーシグナル送信レジスタのうち少なくとも 1 つを含む、請求項 1 に記載の装置。

【請求項 6】

前記エラーレジスタは、前記プラットフォームによってのみ有効にされる及び／又は無効にされるマシンチェックアーキテクチャレジスタである、請求項 1 に記載の装置。

【請求項 7】

前記プラットフォームは、前記オペレーティングシステムと前記プロセッサとの間のエラーシグナル送信を制御する、請求項 1 に記載の装置。

【請求項 8】

前記プラットフォームは、前記オペレーティングシステムと前記プロセッサとの間のエラーシグナル送信を有効にする及び／又は無効にする、請求項 1 に記載の装置。

【請求項 9】

前記エラーレジスタは、前記プラットフォームにより制御されるマシンチェックアーキテクチャレジスタであり、前記プロセッサはさらに、前記プラットフォームにより制御されるエラーシグナル送信レジスタを含む、請求項 1 に記載の装置。

【請求項 10】

前記オペレーティングシステムは、前記プラットフォームを介して前記エラーレジスタに書き込む、請求項 1 に記載の装置。

【請求項 11】

エラー注入が、前記プラットフォームを介して実施される、請求項 1 に記載の装置。

【請求項 12】

オペレーティングシステムから、プロセッサに含まれるエラーレジスタに、プラットフォームを介してセキュアな方式で書き込むステップと、

前記プラットフォームを介して前記エラーレジスタを有効にする及び／又は無効にするステップと、
を含む方法。

【請求項 13】

前記オペレーティングシステムから、前記プロセッサに含まれる前記エラーレジスタに、前記プラットフォームに含まれるシステム管理モード機能を介してセキュアな方式で書き込むステップ、をさらに含む請求項 12 に記載の方法。

【請求項 14】

10

20

30

40

50

前記システム管理モード機能は、前記プラットフォームの基本入出力システムに含まれる、請求項 13 に記載の方法。

【請求項 15】

前記オペレーティングシステムから、前記エラーレジスタに、プラットフォームファームウェアを介してセキュアな方式で書き込むステップ、をさらに含む請求項 12 に記載の方法。

【請求項 16】

前記エラーレジスタは、マシンチェックアーキテクチャレジスタ及びエラーシグナル送信レジスタのうち少なくとも 1 つを含む、請求項 12 に記載の方法。

【請求項 17】

前記エラーレジスタはマシンチェックアーキテクチャレジスタであり、前記プラットフォームのみが前記マシンチェックアーキテクチャレジスタを有効にする及び / 又は無効にするステップ、をさらに含む請求項 12 に記載の方法。

【請求項 18】

前記プラットフォームを介して、前記オペレーティングシステムと前記プロセッサとの間のエラーシグナル送信を制御するステップ、をさらに含む請求項 12 に記載の方法。

【請求項 19】

前記プラットフォームを介して、前記オペレーティングシステムと前記プロセッサとの間のエラーシグナル送信を有効にする及び / 又は無効にするステップ、をさらに含む請求項 12 に記載の方法。

【請求項 20】

前記エラーレジスタはマシンチェックアーキテクチャレジスタであり、前記プラットフォームが前記マシンチェックアーキテクチャレジスタと前記プロセッサ内のエラーシグナル送信レジスタとを制御するステップ、をさらに含む請求項 12 に記載の方法。

【請求項 21】

前記オペレーティングシステムから、前記エラーレジスタに、前記プラットフォームを介して書き込むステップ、をさらに含む請求項 12 に記載の方法。

【請求項 22】

前記プラットフォームを介して 1 又は複数のエラーを注入するステップ、をさらに含む請求項 12 に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は概してセキュアなエラーハンドリングに関する。

【背景技術】

【0002】

サーバシステム（特に、拡張可能な、スケーラブルな、ミッションクリティカルなシステム）は、より良好な信頼性（Reliability）、可用性（Availability）及び保守性（Serviceability）（RAS）のエクスペリエンスのためのエラー検出、エラー訂正、エラーリカバリ及びエラーロギングの能力を備えている。

【0003】

マシンチェックアーキテクチャ（MCA）が、インテル Xeon（登録商標）プロセッサにおいて用いられて、プロセッサ関連のエラーを上位レイヤソフトウェアにレポートする。マシンチェックアーキテクチャは、典型的には、コア、キャッシュなどのプロセッサコンポーネント関連のエラーに限定される。しかしながら、メモリコントローラ、PCIe ルートコンプレックスの、Xeon（登録商標）プロセッサソケットへの統合とともに、マシンチェックアーキテクチャのスコープは、すべてのこれらのコンポーネントからのエラーハンドリング及びRAS イベントを包含するようにレポートされている。マシンチェックアーキテクチャにおける別の進化が、エラーリカバリであり、これにおいて、プロセッサ / プラットフォームの観点から訂正できないエラーが、リカバリのため、オペレー

10

20

30

40

50

ティングシステム（OS）又は仮想マシンモニタ（VMM）に提供される。

【0004】

上記のイノベーションを考慮すると、プラットフォーム上のエラーハンドリング、エラーレポーティング及びエラーリカバリがオペレーティングシステム（OS）及び／又は仮想マシンモニタ（VMM）によって預期されるとおりに動作することを、オペレーティングシステムベンダ（OSV）及び／又は仮想マシンベンダ（VMV）において包括的に検証することが重要である。これは、RAS／エラーハンドリングコードカバレッジと呼ばれる。上記コードカバレッジにより、OS及び／又はVMMは、エラーハンドリング、リカバリ及びRAS機構がエンドツーエンドで実際に動作していることを保証することが可能となる。これには、種々のプロセッサコア、プロセッサキャッシュ、メモリ、入出力装置、システム相互接続などにおけるエラーなどの、種々のタイプのエラーを生成することを含む。エラーハンドリング能力を検証するために、エラー注入能力を、製造プラットフォーム上での実行時にOS及び／又はVMMが利用可能であることが必要となる。ハードウェアにおいて、種々のエラーサブシステム上にすべてのエラーケースについての実際のエラー注入メカニズムを実装することは、非常に複雑となり、非常に高価となる。さらに、エラー注入メカニズム自体は、システムのセキュリティに対するリスクをもたらすべきではない。

10

【0005】

エラーハンドリングコードは、現状、限定されたセットの実際のエラー注入を用いて検証されている。実施のエラー注入メカニズムは、1回に1つだけのエラーを注入することを可能にする。したがって、エラーハンドリングコードは、限定されたエラーコード実行カバレッジしか得られない。ひいては、多くの手作業のコードレビューを行ってさらなるコードカバレッジパスを決定することが必要となる。

20

【発明の概要】

【発明が解決しようとする課題】

【0006】

いくつかの従前の実装は、リング0コードからMCAバンクに書き込むことを、別のリング0コードアクセス可能レジスタに書き込むことによって、可能にしている。これは、セキュリティホールである。MCAバンク書き込み有効化レジスタがリング0ドメイン内にあるため、任意のリング0コードが、MCAバンク書き込み能力を有効にしに行き、MCAバンクに書き込み、無用のエラーケースを引き起こす可能性がある。さらに、従前の実装は、マシンチェックアーキテクチャ（MCA）及び訂正マシンチェックエラー割り込み（Corrected Machine Check Error Interrupt）（CMCEI）などのエラーのシグナル送信を提供せず、上記実装の機構の有用性を限定している。

30

【0007】

本願発明者らはさらに、現在の解決法がMCAバンク書き込み有効化／無効化能力の保護又はエラーシグナル送信（MCA／CMCEI）生成有効化／無効化の保護を提供しないことを、識別している。

【課題を解決するための手段】

【0008】

いくつかの実施形態が、オペレーティングシステムと、プロセッサを含むプラットフォームとを含む。プロセッサは、エラーレジスタを含む。オペレーティングシステムは、プラットフォームを介してセキュアな方式でのみエラーレジスタに書き込むことができる。

40

【図面の簡単な説明】

【0009】

本発明は、以下に与えられる詳細説明と本発明のいくつかの実施形態の添付図面とからさらに十分に理解されるものである。しかしながら、上記詳細説明及び添付図面は、説明される特定の実施形態に本発明を限定するものと解されるべきではなく、単に説明及び理解のためのものである。

【図1】本発明のいくつかの実施形態に従うシステムを示す。

50

【図 2】本発明のいくつかの実施形態に従うフローを示す。

【図 3】本発明のいくつかの実施形態に従うフローを示す。

【図 4】本発明のいくつかの実施形態に従うフローを示す。

【発明を実施するための形態】

【0010】

本発明のいくつかの実施形態は、セキュアなエラーハンドリングに関する。

【0011】

いくつかの実施形態において、マシンチェックエラーコードカバレッジのためのエラー注入が、実施するのにセキュアかつ効率的である（例えば、インテルサーバプロセッサ及び／又はインテル X e o n（登録商標）プロセッサのためのいくつかの実施形態において）。

10

【0012】

いくつかの実施形態は、オペレーティングシステムと、システム管理モード（System Management Mode）（SMM）制御（例えば、及び／又は SMM 機能及び／又は SMM ファームウェア）を含む基本入出力システムと、エラーレジスタを含むプロセッサとを含む。オペレーティングシステムは、システム管理モード制御、機能、ファームウェアなどを介してのみエラーレジスタに書き込むことができる。

【0013】

いくつかの実施形態は、オペレーティングシステムと、プロセッサを含むプラットフォームとを含む。プロセッサは、エラーレジスタを含む。オペレーティングシステムは、プラットフォームを介してセキュアな方式でのみエラーレジスタに書き込むことができる。いくつかの実施形態において、オペレーティングシステムは、プラットフォームファームウェアを介してセキュアな方式でのみエラーレジスタに書き込むことができる。

20

【0014】

図 1 は、いくつかの実施形態に従うシステム 100 を示す。いくつかの実施形態において、システム 100 は、プラットフォーム 102 と、オペレーティングシステム／仮想マシンモニタ（又はリング 0 コード）104 と、エラーハンドラ 106 と、アプリケーション／ゲストオペレーティングシステム 108 と、アプリケーション／ゲストオペレーティングシステム 110 とを含む。いくつかの実施形態において、プラットフォーム 102 は、プロセッサ（及び／又はプロセッサハードウェア）122 と、システム基本入出力システム（BIOS）124 と、エラー注入ソフトウェア抽象化 126 とを含む。いくつかの実施形態において、システム BIOS 124 は、システム管理モード（SMM）コード／データ 128（及び／又は SMM 制御、SMM 機能、SMM コントローラなど）を含む。いくつかの実施形態において、SMM コード／データは、ファームウェアで実装される。いくつかの実施形態において、プロセッサ 122 は、マシンチェックアーキテクチャ（MCA）バンク書き込み能力有効／無効レジスタ 132 と、エラーシグナル送信（error signaling）マシンチェックアーキテクチャ（MCA）／訂正マシンチェックエラー割り込み（CMCI）有効／無効レジスタ 134 とを含む。

30

【0015】

いくつかの実施形態において、プロセッサ 122 は、MCA メモリバンクへの書き込みを有効にする又は無効にすることができる。いくつかの実施形態において、プロセッサ 122 は、モデル固有レジスタ（Model Specific Register）（MSR）又はコンフィギュレーション空間レジスタ（Configuration Space Register）（CSR）としてエラーをシグナル送信することができる。いくつかの実施形態に従い、プロセッサ 122 内の有効／無効レジスタ 132 及び 134 は、システム管理モード（SMM）からのみアクセス可能である。このことは、オペレーティングシステム（OS）コードが、信頼された SMM コードを直接経由することなしに、上記機構を有効にすることは決してできないことを、確かにする。

40

【0016】

いくつかの実施形態において、MCA バンクへの書き込みは、リング 0 コード 104 か

50

ら実施される。いくつかの実施形態において、リング0コード104は、MCA/CMCIをシグナル送信することができる。いくつかの実施形態において、MCAバンク書き込み能力は、システム管理モード(SMM)からのみ有効にされ及び/又は無効にされ、上記機構の利用についてのセキュリティを提供する。いくつかの実施形態において、エラーシグナル送信(MCA/CMCI)は、SMMからのみ有効にされ及び/又は無効にされ、上記機構の利用についてのセキュリティを提供する。いくつかの実施形態において、オペレーティングシステム(OS)は、コードカバレッジのためのセキュアなエラー注入の可用性を検出する。いくつかの実施形態において、BIOS/OSインタフェースとして、OSに対するエラー注入機能のソフトウェア抽象化が実装される。

【0017】

10

図2は、いくつかの実施形態に従うフロー200を示す。いくつかの実施形態において、フロー200は、BIOS/OSインタフェースを公開するBIOSフローを示す。いくつかの実施形態において、フロー200は、ブート処理中のBIOSフローコードを示し、ここでは、プラットフォーム及び/又はプロセッサ内で利用可能な機構が識別され、BIOS/OSインタフェース(ACPIテーブル/メソッド、すなわち、アドバンスト・コンフィグレーション・アンド・パワー・インターフェイス・テーブル/メソッド)が公開される。いくつかの実施形態において、フローは、202において始まり、ここでは、BIOSセットアップオプションがエラー注入について有効にされているかどうかに関して、決定が行われる。BIOSセットアップオプションがエラー注入について有効にされていないことが202において決定された場合、204において、エラー注入のためのBIOS/OSインタフェースは公開されず、フローは206に移動してOSブート処理を継続する。BIOSセットアップオプションがエラー注入について有効にされていることが202において決定された場合、208において、プロセッサがコードカバレッジエラー注入能力をサポートするかどうかに関して、決定が行われる。プロセッサがコードカバレッジエラー注入能力をサポートしないことが208において決定された場合、フローは206に移動してOSブート処理を継続する。プロセッサがコードカバレッジエラー注入能力をサポートすることが208において決定された場合、210において、SMMインフラストラクチャが、エラーハンドリングコードカバレッジエラー注入インタフェース(Error Handling Code Coverage Error Injection Interface)を処理するようにセットアップされる。次いで212において、エラー注入のためのBIOS/OSインタフェースが公開され、次いで、フローは206に移動してOSブート処理を継続する。

20

30

【0018】

図3は、いくつかの実施形態に従うフロー300を示す。いくつかの実施形態において、フロー300は、エラーログ/エラーシグナル送信ハードウェアの書き込みを有効化/無効化するシステム管理モード(SMM)コードフローを示す。いくつかの実施形態において、フロー300は、OSがBIOS/OSインタフェースを呼び出してMCAバンク書き込み能力及びエラーシグナル送信能力を有効/無効にするとときに、SMMコードにより行われる動作を示す。

【0019】

いくつかの実施形態において、フロー300は、302においてシステム管理割り込み(System Management Interrupt)(SMI)モジュールにおいて始まる。304において、上記SMIがエラーハンドリングコードカバレッジをもたらすSMIであるかどうかに関して、決定が行われる。上記SMIがエラーハンドリングコードカバレッジをもたらすSMIではないことが304において決定された場合、306において、通常のSMIフローが継続される。上記SMIがエラーハンドリングコードカバレッジをもたらすSMIであることが304において決定された場合、308において、エラーログハードウェア有効化及び/又は無効化が所望されるかどうかに関して、決定が行われる。エラーログハードウェア有効化及び/又は無効化が308において所望されない場合、フローは310に移動し、ここでは、エラーシグナル送信有効化/無効化を決定するように、決定がなされる。エラーログハードウェア有効化/無効化が308において所望される場合、3

40

50

12において、エラーログハードウェア（MCAバンク）書き込み能力の有効化／無効化が行われ、フローが、要求された動作を310に移動する前に設定することができない場合、エラーで応答する。エラーシグナル送信有効化／無効化が310においてまったく決定されない場合、306において通常のSMIフローが継続される。エラーシグナル送信有効化／無効化が310において決定された場合、314において、エラーシグナル送信能力の有効化／無効化が行われ、306において通常のSMIフローが継続される。

【0020】

図4は、いくつかの実施形態に従うフロー400を示す。いくつかの実施形態において、フロー400は、エラーを注入するためのOSフローを示す。いくつかの実施形態において、フロー400は、OSがどのようにBIOS／OSインタフェースを実行し（cons
umes）、いくつかの実施形態に従うシステムにエラーを注入するのかわを示す。

10

【0021】

フロー400は、402において始まり、ここでは、BIOS／OSインタフェースがエラーハンドリングコードカバレッジエラー注入に利用可能であるのかどうかに関して、決定が行われる。402においてBIOS／OSインタフェースがエラーハンドリングコードカバレッジエラー注入に利用可能でない場合、404において、プラットフォームがエラー注入能力をサポートしない（例えば、MCAバンクエラー注入能力をサポートしない）という決定が行われる。402においてBIOS／OSインタフェースがエラーハンドリングコードカバレッジエラー注入に利用可能である場合、406において、注入すべきエラーが決定される（例えば、エラーログリストを構築することによる）。次いで40
8において、MCAバンク書き込み能力が、BIOSインタフェース（及び／又はACPI
インタフェース）を呼び出すことによって有効にされる。410において、MCAバンク書き込み能力が成功したかどうかに関して、決定が行われる。成功しなかった場合、4
12においてエラー注入は失敗する。成功した場合、414において、エラーがリストから選択される。416において、エラーを設定すべきスレッドが選択され、エラーを設定すべきMCAバンクが選択される。418において、エラーログデータが書き込まれる。420において、現在のMCAバンクが読み出され、読み出されたものが書き込まれた値に一致するかどうかに関して、決定が行われる。一致しなかった場合、フローが418に
戻される前に、422において、現在のMCAバンクがクリアされ、別のMCAバンクが
選択され、すべてのバンクが使い尽くされている場合はエラーが生じる。420において
読み出されたものが書き込まれた値に一致する場合、424において、エラーリスト内の
すべてのエラーが設定されたかどうかに関して、決定が行われる。設定されていない場合、
フローは414に戻される。設定されている場合、426において、MCAバンクの非
ゼロの書き込み能力が、BIOSインタフェース（及び／又はACPIインタフェース）
を呼び出すことによって無効にされる。これは、成功したエラー登録セットアップを示し、
428において、エラーがシグナル送信される。次いで430において、MCA／CM
CIシグナル送信能力が、BIOSインタフェース（及び／又はACPIインタフェース）
を呼び出すことによって有効にされる。次いで432において、CMCIがシグナル送
信されるべきである場合、要求されたスレッドが選択される。次いで434において、M
CA又はCMCIがシグナル送信される（例えば、BIOSインタフェース動作シーケ
ンスを呼び出すことによる）。次いで436において、MCA／CMCIシグナル送信能力
が無効にされる。

20

30

40

【0022】

基本入出力システム（BIOS）の実行時コンテキストが、システム管理割り込み（S
MI）であり、この実行コンテキストの下で、BIOSはMCAをシグナル送信することが
できない場合がある。この実装は、MCAバンク書き込み（エラーレジスタ書き込み）
及びMCA／CMCIシグナル送信制御レジスタがSMI制御下にあることを可能にする
ことを備える。上記実装はさらに、いったんMCA／CMCIシグナル送信が有効にされ
ると、OS／VMMが書き込みをしてMCA又はCMCIのシグナル送信を引き起こすこ
とを可能にする。これらの詳細はBIOSインタフェースによって抽象化され、したがっ

50

てOS/VMMは実装詳細を知る必要がなくなる。

【0023】

いくつかの実施形態において、信頼されたプラットフォーム実行(TXT)が有効にされる場合、SMI自体が信頼された計算境界(trusted compute boundary)(TCB)の範囲内に入るまで、MCAバンクレジスタに書き込むための制御レジスタとMCA/CMCIシグナル送信を有効にするための制御レジスタとが無効にされる。これは、上記のような信頼された環境で実施される他の実施形態を可能にする。

【0024】

いくつかの実施形態において、OS/ドライバが、コードカバレッジのためのエラー注入を行う準備ができていることを決定する。次いで、OS/ドライバは、BIOSインタフェースを呼び出してMCAバンク書き込み能力を有効にする。この時点で、OS/ドライバ(リング0コード)は、MCAバンクに書き込む。エラーハンドリングコードカバレッジ検証ドライバが、検証において関心のあるエラーを決定し、種々のMCAバンク及びスレッドのためのエラーログ値を構築する。検証ドライバは、選択されたMCAバンク及びスレッドにエラーログを書き込む。次いで、エラータイプに基づいて、検証ドライバは、例えば、CMCI又はMCAをシグナル送信する。いったんエラーがシグナル送信されると、割り込みがエラーハンドラを起動させ、エラーハンドラは、実際のエラーを受信したのかを考え、標準的にエラーを処理する。エラーハンドリングコードパスを検証するためにエラーハンドラコードを変更する必要はない。いくつかの実施形態に従うエラー注入が、1のエラーをシグナル送信する前に複数のMCAバンク及びスレッド上のエラーが作成される方式で、実施される。この方式において、同時的なエラーシナリオを作成することができる。

【0025】

いくつかの実施形態に従い、MCAバンク有効化及び/又は無効化とエラーシグナル送信制御とはシステム管理モード(SMM)の範囲内にあり、エラー注入中にデータがまったく公開されないため、セキュリティホールはまったく公開されない。

【0026】

いくつかの実施形態において、種々のタイプのエラーが、エラーをシグナル送信する前に、種々のMCAバンク、種々の中央処理ユニット(CPU)若しくはプロセッサスレッド、及び/又は種々のCPU若しくはプロセッサソケット上に設定される。このことは、種々のエラーハンドラコードフローの実行を可能にし、従前には可能ではなかった種々のエラーシナリオを作成する。これらのタイプのシナリオの作成は、エラーハンドリングフローにおける様々なコーナーケースの検証を可能にする。

【0027】

いくつかの実施形態において、MCAバンク書き込み及びエラーシグナル送信の機構は、システム管理モード(SMM)からのみ許容される。SMMアーキテクチャは、SMMコード又はデータにSMMの外部からアクセスすることができなくなるため、プラットフォームに対してセキュリティを提供する。このことは、マルウェア又は信頼されていないコードがSMMに入り込み、上記の機構を有効にすることが、決してないことを確かにする。

【0028】

いくつかの従前の実装は、リング0コードからMCAバンクを書き込むことを、別のリング0コードアクセス可能レジスタに書き込むことによって、許容する。これは、セキュリティホールである。MCAバンク書き込み有効化レジスタがリング0ドメイン内にあるため、任意のリング0コードが、MCAバンク書き込み能力を有効にしに行き、MCAバンクに書き込み、無用のエラーケースを引き起こす可能性がある。さらに、従前の実装は、MCA及びCMCIなどのエラーのシグナル送信を提供せず、上記実装の機構の有用性を限定している。

【0029】

現在の解決法は、MCAバンク書き込み有効化/無効化能力の保護又はエラーシグナル

10

20

30

40

50

送信 (MCA / CMC I) 生成有効化 / 無効化の保護を提供していない。いくつかの実施形態に従い、保護が、MCA バンク書き込み能力及びエラーシグナル送信能力の有効化について提供される。いくつかの実施形態において、MCA バンク書き込み能力及びエラーシグナル送信能力の有効化 / 無効化についてのソフトウェア抽象化が実装される。いくつかの実施形態において、ハードウェアが変化した場合、エラーハンドリングコードカバレージエラー注入は変更する必要がない。

【0030】

いくつかの実施形態において、MCA バンク書き込みの有効化及び / 又は無効化が実装される (エラーロギングハードウェア書き込み)。いくつかの実施形態において、エラーシグナル送信ハードウェアの利用が保護される。いくつかの実施形態において、ソフトウェアに対するハードウェア実装の抽象化が実装され、したがってハードウェア実装レジスタ又は配置が変化した場合にソフトウェアの変更は必要なくなる。

10

【0031】

いくつかの実施形態において、オペレーティングシステムベンダ (OSV) がエラーハンドリングフローを検証することができ、プロセッサ上のRASのOS実装 (例えば、サーバプロセッサ及び / 又はインテルXeon (登録商標) プロセッサ) がより良好な品質を有することになる。このことは、RAS / エラーハンドリングを有効化するコストを削減する。いくつかの実施形態に従い、任意のエラーの組み合わせを、MCA バンクに投入する (populated) ことができ、OSは、シリコンが利用可能となる前でさえ、セキュアな方式で将来の機構のエラーハンドリングを検証することが可能となる。

20

【0032】

本明細書において、いくつかの実施形態を、特定の方式で実装されるものとして説明してきたが、いくつかの実施形態では、上記の特定の実装は、必要とされるものではない。例えば、本明細書において、いくつかの実施形態を、システム管理モード (SMM) コード / データ、SMM機能、SMM制御、SMMコントローラなどを含むものとして説明してきた。しかしながら、他の実施形態は、SMMを実装することを必要としない。さらに、いくつかの実施形態において、SMM、BIOSなどのいくつかの機能を、ファームウェア、ソフトウェア及び / 又はハードウェアで実装することができる。いくつかの実施形態において、エラーレジスタを有効化 / 無効化するため、及び / 又はエラーを検出、訂正、リカバリ、ロギングなどするためのプラットフォーム制御が、例えばオペレーティングシステム (OS) 及び / 又は仮想マシンモニタ (VMM) を用いて上記の機能を制御するよりはセキュアな方式で実施される。

30

【0033】

いくつかの実施形態が特定の実装を参照して説明されたが、他の実装がいくつかの実施形態に従って可能である。さらに、図面に示された及び / 又は本明細書に記載された回路素子又は他の機構の配置及び / 又は順序は、図示及び記載された特定の 방법으로配置される必要はない。多くの他の配置がいくつかの実施形態に従って可能である。

【0034】

図に示される各システムにおいて、いくつかの場合の要素が、同一の参照番号又は異なる参照番号を各々有して、表された要素が異なる及び / 又は類似するであろうことを示唆し得る。しかしながら、要素は、種々の実装を有し、本明細書に図示又は記載されたシステムのうち一部又はすべてと共に動作するほど十分な適応性を有し得る。図面に示される種々の要素は、同一である又は異なる可能性がある。どの要素が第1の要素として参照され、どれが第2の要素と呼ばれるのかは、任意である。

40

【0035】

本願説明と特許請求の範囲とにおいて、用語「結合される」及び「接続される」とその派生語とが用いられる場合がある。上記の用語は互いに対して同義語である意図はないことを、理解されたい。むしろ、特定の実施形態において、「接続される」を用いて複数の要素が直接的な物理的又は電氣的接触を有することを示す場合がある。「結合される」は、複数の要素が直接的な物理的又は電氣的接触を有することを、意味する場合がある。し

50

かしながら、「結合される」はさらに、複数の要素が互いに直接的な接触を有さず、しかしながらなお互いに協働又は相互作用することを意味する場合がある。

【0036】

本説明において、また一般的に、アルゴリズムは、所望の結果につながる動作又は操作についての自己矛盾のないシーケンスと見なされる。上記には、物理量の物理的な操作を含む。一般に、必ずしも必要ないが、上記の量は、保存され、転送され、組み合わせられ、比較され、及びその他の操作をされることが可能な、電氣的又は磁氣的な信号の形式をとる。主に一般的な用法の理由で、こうした信号をビット、値、要素、シンボル、文字、用語、数字又は類似のものと呼ぶことは、時に便利であることが証明されている。しかしながら、上記及び類似の用語のすべてが、適切な物理量に関連付けられるべきであり、単に上記の量に適用される便利なラベルであることを、理解されたい。

10

【0037】

いくつかの実施形態は、ハードウェア、ファームウェア及びソフトウェアのうちの1つ又はそれらの組み合わせで実装することができる。いくつかの実施形態は、さらに、機械読み取り可能媒体に記憶された命令として実装することができ、上記機械読み取り可能媒体は、コンピューティングプラットフォームによって読み出され、実行されて、本明細書に記載の動作を実行することができる。機械読み取り可能媒体には、機械（例えば、コンピュータ）により読取可能な形式の情報を記憶する又は送信する任意のメカニズムを含むことができる。例えば、機械読み取り可能媒体には、読取専用メモリ（ROM）、ランダムアクセスメモリ（RAM）、磁気ディスク記憶媒体、光記憶媒体、フラッシュメモリ装置、電氣的、光学的、音響的又は他の形式の伝播信号（例えば、搬送波、赤外線信号、デジタル信号、信号を送受信するインタフェースなど）及びその他を含むことができる。

20

【0038】

実施形態は、本発明の実装又は例示である。本明細書における「ある実施形態」「1つの実施形態」「いくつかの実施形態」又は「他の実施形態」という言葉は、その実施形態と関連して説明された特定の機構、構造又は特徴が、本発明の少なくともいくつかの実施形態に含まれ、しかしながら必ずしもすべての実施形態には含まれないことを、意味する。「ある実施形態」「1つの実施形態」又は「いくつかの実施形態」の種々の出現は、必ずしもすべて同一の実施形態を参照するものではない。

【0039】

30

本願において記載及び図示されたすべてのコンポーネント、機構、構造、特徴などが、特定の1又は複数の実施形態に含まれる必要はない。例えば、あるコンポーネント、機構、構造又は特徴が含まれる「場合がある」「可能性がある」「ことができる」又は「であろう」ことを本明細書が述べる場合、上記の特定のコンポーネント、機構、構造又は特徴が含まれることは必要とはされない。本明細書又は請求項が「1の（“a”又は“an”）」要素に言及する場合、上記は、要素が1つしか存在しないことを意味するものではない。本明細書又は請求項が「1のさらなる（“an additional”）」要素に言及する場合、上記は、1より多くのさらなる要素が存在することを除外しない。

【0040】

本願においてフロー図及び／又は状態図を用いて実施形態を説明している場合があるが、本発明は、本願におけるこうした図、又は対応する記載に限定されない。例えば、フローは、本願において図示及び記載されたとおりの、各々の図示されたボックス若しくは状態を通して、又は正確に同一の順序で、移動する必要はない。

40

【0041】

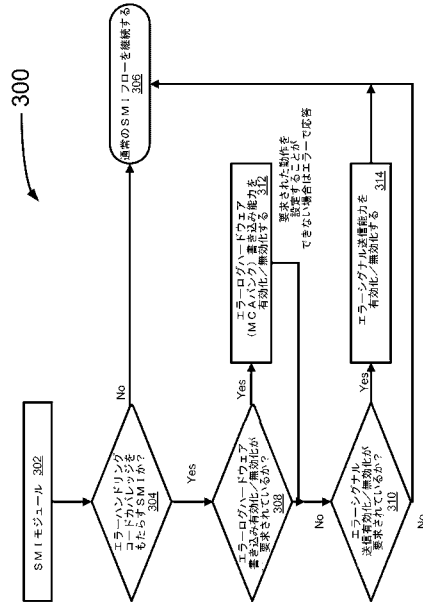
本発明は、本明細書に列挙された特定の詳細に限定されない。実際に、本開示の便益を有する当業者は、前述の説明及び図面から多くの他の変形を本発明の範囲内で行うことができることを、十分理解するであろう。したがって、本発明の範囲を定義するものは、いかなる補正をも含む別記の特許請求の範囲である。

【0042】

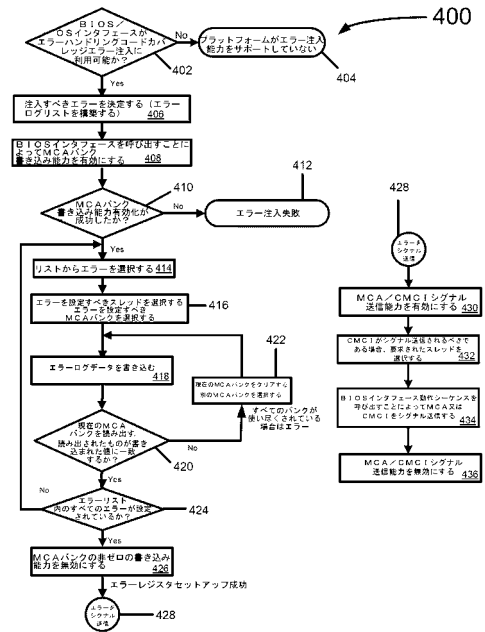
[関連出願]

50

【図 3】



【図 4】



フロントページの続き

(72)発明者 クマール, モハン ジェイ .
アメリカ合衆国 9 7 0 0 7 オレゴン州 アロハ サウスウエスト マルコ レーン 1 8 6 8
0

(72)発明者 イグゾー, セオドロス
アメリカ合衆国 9 7 1 4 0 オレゴン州 シャーウッド サウスウエスト チャップマン ロー
ド 2 1 5 0 5

(72)発明者 ヴァルガス, アンドリュー
アメリカ合衆国 9 5 6 7 2 カリフォルニア州 レスキュー フォックスモア レーン 3 4 3
9

(72)発明者 クラムコテ, ラジェンドラ
アメリカ合衆国 9 8 0 5 6 ワシントン ニューキャッスル 1 2 9 ス コート サウスイース
ト 8 6 1 3

F ターム(参考) 5B017 AA02 CA04
5B042 GA22 JJ15 JJ29
5B048 DD18

【外国語明細書】
2015195065000001.pdf