

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6481900号
(P6481900)

(45) 発行日 平成31年3月13日(2019.3.13)

(24) 登録日 平成31年2月22日(2019.2.22)

(51) Int.Cl.

F I

G 0 6 F 9/44 (2018.01)

G 0 6 F 9/44

請求項の数 29 (全 28 頁)

(21) 出願番号	特願2016-567254 (P2016-567254)	(73) 特許権者	591003943
(86) (22) 出願日	平成26年6月25日 (2014.6.25)		インテル・コーポレーション
(65) 公表番号	特表2017-519281 (P2017-519281A)		アメリカ合衆国 95054 カリフォル
(43) 公表日	平成29年7月13日 (2017.7.13)		ニア州・サンタクララ・ミッション カレ
(86) 国際出願番号	PCT/CN2014/080689		ッジ ブレーバード・2200
(87) 国際公開番号	W02015/196381	(74) 代理人	110000877
(87) 国際公開日	平成27年12月30日 (2015.12.30)		龍華国際特許業務法人
審査請求日	平成29年1月6日 (2017.1.6)	(72) 発明者	ヤオ、ジエウエン
			アメリカ合衆国 95054 カリフォル
			ニア州・サンタクララ・ミッション カレ
			ッジ ブレーバード・2200 インテル
			・コーポレーション内

最終頁に続く

(54) 【発明の名称】 ハードウェア構成レポーティング用の装置、ハードウェア構成アービトレーションの方法、プログラム、機械可読記録媒体、及び、ハードウェア構成アービトレーション用の装置

(57) 【特許請求の範囲】

【請求項1】

T E Eという信頼できる実行環境、および、non-T E Eという信頼できない実行環境を有し、特定のインタラプトに応答して前記non-T E Eから前記T E Eにエントリするプロセッシングデバイスであって、前記T E Eは、前記non-T E Eからアクセス不可能なメモリから実行される、プロセッシングデバイスと、

前記メモリに記憶され、ハードウェア構成レジスタを表わしている要求の指標をアービタ論理から受信するように前記T E E内で動作する要求サービス論理と、

前記メモリに記憶され、前記T E E内で動作し、前記要求によって表わされる前記ハードウェア構成レジスタの値のインジケータを前記アービタ論理にレポートするレポーティング論理であり、前記アービタ論理が、レポートされた前記ハードウェア構成レジスタの値のインジケータを評価して、記憶されたセキュリティ要件が満たされていないと決定される場合にアクションを実行する、レポーティング論理と、

を備える、ハードウェア構成レポーティング用の装置。

【請求項2】

前記アービタ論理からの前記要求の前記指標は、前記non-T E Eにおいて動作している場合に前記プロセッシングデバイスにアクセス可能な予め定められたレジスタに記憶されている値に、少なくとも部分的に基づく、

請求項1に記載の装置。

【請求項3】

10

20

前記アービタ論理からの前記要求の前記指標は、前記プロセッシングデバイスの前記 T E E へのエントリをトリガした前記特定のインタラプトのソースに、少なくとも部分的に基づく、
請求項 1 または 2 に記載の装置。

【請求項 4】

前記アービタ論理は、前記プロセッシングデバイスの前記 n o n - T E E において動作する、
請求項 1 から 3 の何れか一項に記載の装置。

【請求項 5】

前記アービタ論理は、前記プロセッシングデバイスと異なる第 2 のプロセッシングデバ
イス上で動作する、
請求項 1 から 3 の何れか一項に記載の装置。

10

【請求項 6】

前記アービタ論理は、前記プロセッシングデバイスの前記 T E E において動作する、
請求項 1 から 3 の何れか一項に記載の装置。

【請求項 7】

前記要求は前記ハードウェア構成レジスタの値のクエリであり、前記ハードウェア構成
レジスタの前記値の前記インジケータは前記ハードウェア構成レジスタの前記値である、
請求項 1 から 6 の何れか一項に記載の装置。

【請求項 8】

20

前記要求は、前記ハードウェア構成レジスタの値が規定値に等しいことのチェックであ
り、前記ハードウェア構成レジスタの前記値の前記インジケータは、前記ハードウェア構
成レジスタの前記値が前記規定値に等しいか否かのバイナリインジケータである、
請求項 1 から 6 の何れか一項に記載の装置。

【請求項 9】

前記アービタ論理は、前記プロセッシングデバイスの基本入出力オペレーティングシス
テム (B I O S) において動作しているドライバ実行環境 (D X E) スクリプトである、
請求項 8 に記載の装置。

【請求項 10】

前記要求サービス論理は更に、複数のドライバのうちの何れが、前記要求によって表わ
される前記ハードウェア構成レジスタにアクセス可能であることを決定し、決定されたドラ
イバと通信して前記要求をサービスする、
請求項 1 から 9 の何れか一項に記載の装置。

30

【請求項 11】

前記アービタ論理は、起動したときに実行する基本入出力オペレーティングシステム (B I O S) フェーズアービタである、
請求項 1 から 10 の何れか一項に記載の装置。

【請求項 12】

前記 T E E は、システム管理モードである、
請求項 1 から 11 の何れか一項に記載の装置。

40

【請求項 13】

コンピューティング論理が、アプリケーションからの要求の指標を、プロセッシングデ
バイスの T E E という信頼できる実行環境のレポーティング論理に提供する段階であって
、

前記プロセッシングデバイスが、前記 T E E と、 n o n - T E E という信頼できない実
行環境とを有し、

前記プロセッシングデバイスが、特定のインタラプトに応答して前記 n o n - T E E から
前記 T E E にエントリし、

前記 T E E が、前記 n o n - T E E からアクセス不可能なメモリから実行され、
前記レポーティング論理が前記メモリに記憶され、

50

前記要求がハードウェア構成レジスタを表わしている段階と、

前記要求の前記指標を受信したことに応答して前記レポーティング論理によって提供された、前記要求によって表わされる前記ハードウェア構成レジスタの値のインジケータが、記憶されたセキュリティ要件を満たしていないと、前記コンピューティング論理が決定する段階と、

前記コンピューティング論理が、前記記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクションを実行する段階と
を備える、ハードウェア構成アービトレーションの方法。

【請求項 1 4】

前記記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクション
を実行する段階が、前記記憶されたセキュリティ要件が満たされていないとの決定に応答して、前記記憶されたセキュリティ要件が満たされていないことのインジケータの表示をディスプレイデバイス上に引き起こす段階を含む、
請求項 1 3 に記載の方法。

10

【請求項 1 5】

前記記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクション
を実行する段階が、前記記憶されたセキュリティ要件が満たされていないとの決定に応答して、前記ハードウェア構成レジスタと関連付けられたハードウェアにシャットダウンさせる段階を含む、
請求項 1 3 または 1 4 に記載の方法。

20

【請求項 1 6】

前記ハードウェア構成レジスタは、チップセット再マッピングレジスタである、
請求項 1 3 から 1 5 の何れか一項に記載の方法。

【請求項 1 7】

前記ハードウェア構成レジスタは、システム管理モードロックレジスタである、
請求項 1 3 から 1 5 の何れか一項に記載の方法。

【請求項 1 8】

前記ハードウェア構成レジスタは、フラッシュ部分ロックレジスタである、
請求項 1 3 から 1 5 の何れか一項に記載の方法。

【請求項 1 9】

前記コンピューティング論理の少なくとも一部は、前記プロセッシングデバイスの前記
non-TEEにおいて動作する、
請求項 1 3 から 1 8 の何れか一項に記載の方法。

30

【請求項 2 0】

前記コンピューティング論理の少なくとも一部は、前記プロセッシングデバイスと異なる第 2 のプロセッシングデバイス上で動作する、
請求項 1 3 から 1 8 の何れか一項に記載の方法。

【請求項 2 1】

前記コンピューティング論理の少なくとも一部は、前記プロセッシングデバイスの前記
TEEにおいて動作する、
請求項 1 3 から 1 8 の何れか一項に記載の方法。

40

【請求項 2 2】

前記 TEE は、システム管理モードである、
請求項 1 3 から 2 1 の何れか一項に記載の方法。

【請求項 2 3】

装置に請求項 1 3 から 2 2 の何れか一項に記載の方法を実行させるためのプログラム。

【請求項 2 4】

請求項 2 3 に記載のプログラムを格納している、1 つ又は複数の機械可読記録媒体。

【請求項 2 5】

アプリケーションからの要求の指標を、プロセッシングデバイスの TEE という信頼で

50

きる実行環境のレポーティング論理に提供するための手段であって、

前記プロセッシングデバイスが、前記T E Eと、n o n - T E Eという信頼できない実行環境とを有し、

前記プロセッシングデバイスが、特定のインタラプトに応答して前記n o n - T E Eから前記T E Eにエントリし、

前記T E Eが、前記n o n - T E Eからアクセス不可能なメモリから実行され、

前記レポーティング論理が前記メモリに記憶され、

前記要求がハードウェア構成レジスタを表わしている手段と、

前記要求の前記指標を受信したことに応答して前記レポーティング論理によって提供された、前記要求によって表わされる前記ハードウェア構成レジスタの値のインジケータが、記憶されたセキュリティ要件を満たしていないと決定するための手段と、

前記記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクションを実行するための手段と

を備える、ハードウェア構成アービトレーション用の装置。

【請求項26】

前記記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクションを実行するための前記手段が、前記記憶されたセキュリティ要件が満たされていないとの決定に応答して、前記記憶されたセキュリティ要件が満たされていないことのインジケータの表示をディスプレイデバイス上に引き起こすための手段を含む、

請求項25に記載の装置。

【請求項27】

T E Eという信頼できる実行環境、および、n o n - T E Eという信頼できない実行環境を有し、特定のインタラプトに応答して前記n o n - T E Eから前記T E Eにエントリするプロセッシングデバイスであって、前記T E Eは、前記n o n - T E Eからアクセス不可能なメモリから実行される、プロセッシングデバイスと、

前記メモリに記憶され、ハードウェア構成レジスタを表わしている要求の指標をアービタ論理から受信するように前記T E E内で動作する要求サービス論理と、

前記メモリに記憶され、前記T E E内で動作し、前記要求によって表わされる前記ハードウェア構成レジスタの値のインジケータを前記アービタ論理にレポートするレポーティング論理と、

を備え、前記要求は、前記ハードウェア構成レジスタの値が規定値に等しいことのチェックであり、前記ハードウェア構成レジスタの前記値の前記インジケータは、前記ハードウェア構成レジスタの前記値が前記規定値に等しいか否かのバイナリインジケータである、ハードウェア構成レポーティング用の装置。

【請求項28】

T E Eという信頼できる実行環境、および、n o n - T E Eという信頼できない実行環境を有し、特定のインタラプトに応答して前記n o n - T E Eから前記T E Eにエントリするプロセッシングデバイスであって、前記T E Eは、前記n o n - T E Eからアクセス不可能なメモリから実行される、プロセッシングデバイスと、

前記メモリに記憶され、ハードウェア構成レジスタを表わしている要求の指標をアービタ論理から受信するように前記T E E内で動作する要求サービス論理と、

前記メモリに記憶され、前記T E E内で動作し、前記要求によって表わされる前記ハードウェア構成レジスタの値のインジケータを前記アービタ論理にレポートするレポーティング論理と、

を備え、前記要求サービス論理は更に、複数のドライバのうちの何れが、前記要求によって表わされる前記ハードウェア構成レジスタにアクセス可能であるかを決定し、決定されたドライバと通信して前記要求をサービスする、ハードウェア構成レポーティング用の装置。

【請求項29】

T E Eという信頼できる実行環境、および、n o n - T E Eという信頼できない実行環

10

20

30

40

50

境を有し、特定のインタラプトに応答して前記non-TEEから前記TEEにエントリするプロセッシングデバイスであって、前記TEEは、前記non-TEEからアクセス不可能なメモリから実行される、プロセッシングデバイスと、

前記メモリに記憶され、ハードウェア構成レジスタを表わしている要求の指標をアービタ論理から受信するように前記TEE内で動作する要求サービス論理と、

前記メモリに記憶され、前記TEE内で動作し、前記要求によって表わされる前記ハードウェア構成レジスタの値のインジケータを前記アービタ論理にレポートするレポーティング論理と、

を備え、前記アービタ論理は、起動したときに実行する基本入出力オペレーティングシステム（BIOS）フェーズアービタである、ハードウェア構成レポーティング用の装置。

10

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、コンピューティング装置に関する。より具体的には、ハードウェア構成レポーティングに関する。

【背景技術】

【0002】

起動中に利用されるハードウェア構成レジスタの値は通常、ブートエンジニアによって最初に手動で構成される。その結果として、適切な構成はヒューマンエラーを受けやすく、多くの場合、手動構成におけるミスは見逃されることがある。

20

【図面の簡単な説明】

【0003】

複数の実施形態は、添付の図面と共に、以下の詳細な説明によって容易に理解される。この説明を容易にする目的で、同様の構造要素が同様の参照番号によって指定されている。複数の実施形態は、添付の図面の複数の図において、例として図示されるのであって、限定するものとして図示されるのではない。

【図1】様々な実施形態による、ハードウェア構成レポーティングシステムのブロック図である。

【図2】様々な実施形態による、アービタ論理の1つ又は複数のインスタンスエイションを有するハードウェア構成レポーティングシステムのブロック図である。

30

【図3】様々な実施形態による、信頼できる実行環境としてシステム管理モードを有するハードウェア構成レポーティングシステムのブロック図である。

【図4】様々な実施形態による、複数のドライバを含むレポーティング論理のブロック図である。

【図5】様々な実施形態による、ハードウェア構成レポーティングの方法の流れ図である。

【図6】様々な実施形態による、ハードウェア構成アービトレーションの方法の流れ図である。

【図7】様々な実施形態による、ハードウェア構成レポーティングおよびアービトレーションの方法の流れ図である。

40

【図8】幾つかの実施形態による、ハードウェア構成レポーティングシステム100に含まれ得る更新システムのブロック図である。

【図9】様々な実施形態による、開示される複数の実施形態の様々なものを実施するのに適した例示的な装置のブロック図である。

【発明を実施するための形態】

【0004】

ハードウェア構成レポーティングおよびアービトレーションに関連する複数の実施形態が本明細書で開示される。例えば、ハードウェア構成レポーティングの装置は、信頼できる実行環境（TEE）および信頼できない実行環境（non-TEE）を有するプロセッシングデバイスと、メモリに記憶され、ハードウェア構成レジスタを表わす要求の指標を

50

アービタ論理から受信するようにT E E内で動作する要求サービス論理と、メモリに記憶され、T E E内で動作し、その要求によって表わされるハードウェア構成レジスタの値のインジケータをアービタ論理にレポートするレポーティング論理とを含んでもよい。

【0005】

上記で述べたように、コンピューティング装置の複数のスタートアップ操作を担う技術者は、意図しないで又は故意に、(多くの場合に40又はそれより多くの数に達する)特定の複数のハードウェア構成レジスタを適切に設定し損なうことがある。これらのエラーは、極めてコストがかかるかもしれない。もしアクセス許可に対応するレジスタが「オープン」にされたまま(すなわち、改ざんに対してロックされていない)ならば、悪性コードが、そのオープンドアの足元を見て、全ての後続性能に影響する可能性がある複数の変更を行うかもしれない。例えば、もしフラッシュ部分ロックレジスタがアンロックにされたままならば、マザーボード上のリードオンリメモリ(R O M)は、悪性コードによる再書き込みに対してオープンにされたままであるかもしれない。起動中に、チップセットメモリマップは、中央処理装置(C P U)からフラッシュ部分までに対して、複数の第1命令を実行するように指示するかもしれない。これらの命令が悪意をもって変更されている場合、任意の他の保護が適切に行われる前にC P Uがその悪性コードを実行してしまうかもしれない。

10

【0006】

本明細書で開示される複数のハードウェア構成レポーティングシステム及び技術の様々な実施形態は、起動中および／またはランタイム中のそのようなエラーの検出を可能にし得、装置が、そのセキュリティリスクを軽減する、又は、ユーザにそのセキュリティリスクを警告する、といった複数のアクションを取ることを可能にし得る。幾つかの実施形態において、管理者又は権限を与えられた他のエンティティは、本明細書で開示される複数のハードウェア構成レポーティングシステム及び技術を用いて、ハードウェア構成情報を入手及びレビューして、(例えば予め定義されたセキュリティポリシーに従って)次の複数の段階を決定してもよい。

20

【0007】

以下の詳細な説明では、その一部を形成し、全体を通じて同様の部分が同様の番号によって指定されている添付の図面が参照される。その一部は、添付の図面において、実施され得る複数の例示的な実施形態として示されている。複数の他の実施形態が使用され得ること、及び、本開示の範囲から逸脱することなく複数の構造的又は論理的変更が行われ得ることが理解される。従って、以下の詳細な説明は、限定する意味で解釈されるべきではなく、複数の実施形態の範囲は、添付の特許請求の範囲およびその複数の等価物により規定される。

30

【0008】

様々な動作が、特許請求の範囲で主張される主題の理解に最も役立つ態様で、複数の個別のアクション又は動作として順に説明され得る。しかしながら、説明の順序は、これらの動作が必ず順序に左右されるということを暗に示すように解釈されるべきではない。とりわけ、これらの動作は、表示の順序で実行されなくてもよい。説明される複数の動作は、説明される実施形態と異なる順序で実行されてもよい。追加の複数の実施形態では、様々な追加の動作が実行されてもよく、および／または、説明される複数の動作が省略されてもよい。

40

【0009】

本開示の目的のため、「Aおよび／またはB」という文言は、(A)、(B)または(AおよびB)を意味する。本開示の目的のため、「A、Bおよび／またはC」という文言は、(A)、(B)、(C)、(AおよびB)、(AおよびC)、(BおよびC)または(A、BおよびC)を意味する。

【0010】

本明細書では、「ある実施形態において」または「複数の実施形態において」という文言を用いているが、これらは各々、複数の同じ実施形態または異なる実施形態の1つ又は

50

複数を指していてもよい。更に、本開示の複数の実施形態に対して用いられる、「備える (comprising)」、「含む (including)」、「有する (having)」等の用語は類義語である。本明細書で用いられる、「論理」という用語は、ここで説明される機能を提供する、1つ又は複数のソフトウェアまたはファームウェアプログラム、組み合わせ論理回路、および／または、他の複数の適切なコンポーネントを実行する、特定用途向け集積回路 (ASIC)、電子回路、(共有、専用またはグループ) プロセッサ、および／または、(共有、専用またはグループ) メモリを指し、または、その一部であり、または、それらを含んでもよい。

【0011】

図1は、様々な実施形態による、ハードウェア構成レポーティングシステム100のブロック図である。ハードウェア構成レポーティングシステム100は、(図2に示されている) 信頼できる実行環境 (TEE) 116または1つ又は複数の信頼できない実行環境 (non-TEE) 118で動作可能なプロセッシングデバイスを有する装置 (例えば図9を参照して以下で検討される装置900) で実行される。プロセッシングデバイスが TEE 116にある場合に実行されるメモリ記憶論理 (TEEメモリと称される) は、プロセッシングデバイスが non-TEE 118にある場合に実行されるメモリ記憶論理から隔離されてもよい。これにより、プロセッシングデバイスが non-TEE 118にある場合に動作する論理は、TEEメモリにアクセスできない。プロセッシングデバイスは、インタラプトに応答して、TEE 116と non-TEE 118との間で移行するように構成されてもよい。

【0012】

幾つかの実施形態において、TEE 116は、プロセッシングデバイスのシステム管理モード (SMM) であってもよい。SMMは、多くの場合、電力制御および熱調整などの複数の低レベル動作を管理するのに用いられる、プロセッシングデバイスモードである。SMMは、SMMの外部で動作している論理に不可視又はアクセス不可能である、独自の隠しメモリ空間および実行環境を有してもよい。幾つかの実施形態において、SMMは、装置の基本入出力オペレーティングシステム (BIOS) によってインストールされてもよく、プロセッシングデバイスがシステム管理インタラプト (SMI) を受信した場合に入力されてもよい。SMIを検出すると、非SMMのワーキングメモリが後の再インスタンシエーション用に記憶させられ、プロセッシングデバイスがSMMにエントリしてもよい。本明細書でBIOSに関して検討される複数の実施形態は、統一型拡張ファームウェアインタフェース (UEFI) に関して類似的に実行されてもよい。

【0013】

ハードウェア構成レポーティングシステム100は、アービタ論理102とレポーティング論理104とを含んでもよい。レポーティング論理104は、TEEから動作可能であってもよく、プロセッシングデバイスが non-TEE 118にある場合に実行される論理から隔離されてもよい。とりわけ、レポーティング論理104は、TEEメモリに記憶されてもよい。図2を参照して以下で検討されるように、アービタ論理102は、TEE 116内で動作してもよく、または、non-TEE 118内で動作してもよい。アービタ論理102は、レポーティング論理104と通信可能に結合されてもよい。

【0014】

アービタ論理102は、要求論理106と、セキュリティ論理108と、アクション論理110とを含んでもよい。アービタ論理102はまた、メモリ156を含んでもよく、メモリ156は、アービタ論理102の複数のコンポーネントの何れかによって使用され、アービタ論理102の動作に関連するデータを記憶してもよい。

【0015】

要求論理106は、要求の指標をレポーティング論理104に提供するように構成されてもよい。要求は、1つ又は複数のハードウェア構成レジスタを表わしてもよく、アービタ論理102は、これについての情報を受信することを望んでいる。ハードウェア構成レポーティングシステム100は、1つ又は複数の異なるタイプの要求を認識してもよい。

幾つかの実施形態において、要求は、1つ又は複数のハードウェア構成レジスタの値の「クエリ」であってもよい。レポーティング論理104は、これに応じて、複数の値のインジケータを提供してもよい。例えば、要求論理106によってレポーティング論理104に提供される要求は、フラッシュ部分ロックレジスタを表わすクエリであってもよい。これに応じて、レポーティング論理104は、フラッシュ部分ロックレジスタに記憶されているのが「0」の値であるか「1」の値であるかの指標を提供してもよい。一方の値は、フラッシュ部分がロックされ、従って、マザーボードROMを更新できないことを示し、その一方で、他方の値は、フラッシュ部分がアンロックされ、従って、任意のものがマザーボードROMを更新できることを示してもよい。幾つかの実施形態において、要求は、1つ又は複数のハードウェア構成レジスタの値が一組の規定値に等しいという「チェック」であってもよく、これに回答して、レポーティング論理104は、複数のハードウェア構成レジスタの複数の値がその一組の規定値に等しいか否かのバイナリインジケータを提供してもよい。例えば、要求論理106によってレポーティング論理104に提供される要求は、フラッシュ部分ロックレジスタと、「1」の規定値とを表すチェックであってもよく、これに回答して、レポーティング論理104は、フラッシュ部分ロックレジスタに記憶された値が「1」の規定値に等しい、又は、「1」の規定値に等しくないことの指標を提供してもよい。装置がSMMを含んでいる幾つかの実施形態において、要求論理106によってレポーティング論理104に提供される要求は、SMMロックレジスタを表わすクエリまたはチェックであってもよい。一方の値が、SMMメモリを更新できないことを示し、その一方で、他方の値が、SMMメモリがアンロックされ、従って、任意のものがSMMメモリを更新できることを示してもよい。幾つかの実施形態において、アービタ論理102は、クエリと複数のチェック要求とを選択的に提供するように構成されてもよく、その一方で、複数の他の実施形態では、アービタ論理102は、クエリのみを提供すること、又は、複数のチェック要求のみを提供することに制限されてもよい。

【0016】

幾つかの実施形態において、要求論理106によって提供される要求の形態およびコンテンツは、開発者によって構成されてもよい。例えば、開発者は、（例えば、要求によって表わされる複数のハードウェア構成レジスタと要求のタイプといった）要求の形態およびコンテンツを指定する拡張マークアップ言語（XML）スクリプトを書き込んでもよく、そのスクリプトをメモリ156に記憶させてもよい。要求論理106は、メモリ156からXMLスクリプトを取得して、実行用にXMLスクリプトをバイナリスクリプトへと変換するように構成されてもよい。要求論理106は、バイナリスクリプトを記憶させるように構成されてもよい。要求論理106がバイナリスクリプトを実行する場合、要求がレポーティング論理104に提供されてもよい。

【0017】

セキュリティ論理108は、要求論理106と結合されてもよく、要求論理106から要求の指標を受信したことに応じて、レポーティング論理104によって提供されたインジケータを評価するように構成されてもよい。とりわけ、セキュリティ論理108は、（要求論理106によって提供された要求により表わされる）ハードウェア構成レジスタの値のインジケータが、記憶されたセキュリティ要件を満たしていないか満たしているかを決定するように構成されてもよい。記憶されたセキュリティ要件は、管理者又は権限を与えられた他のエンティティによって設定された、予め定義されたセキュリティポリシーの一部であってもよい。1つ又は複数のセキュリティ要件は、メモリ156に記憶されてもよく、（例えば任意の適切なデータベース構造における）様々なハードウェア構成レジスタの、特定の複数の個別の値又は複数の値の複数のパターンと対応してもよい。例えば、メモリ156に記憶されたセキュリティ要件は、チップセット再マッピングレジスタの値が、チップセット再マッピングレジスタがロックされて改ざんされ得ないことを示す「1」でなければならないことを指定してもよい。「0」の値は、任意のものがメモリの複数の部分を再マッピングし得ることを示してもよい（例えば、TEE116に対応する部分のようなメモリの複数の隠し部分を、保護されていない複数のメモリ領域に再マッピン

10

20

30

40

50

グすること)。セキュリティ論理108は、要求論理106の要求に応答して、レポーティング論理104によって提供されたインジケータに基づいて、チップセット再マッピングレジスタの値のインジケータが「1」に等しいか等しくないかを決定するように構成されてもよい。

【0018】

アクション論理110は、セキュリティ論理108と結合されてもよく、セキュリティ論理108による、自己の記憶されたセキュリティ要件が満たされているか満たされていないかの決定に応答して、アクションを実行するように構成されてもよい。様々な記憶されたセキュリティ要件が満たされているときに実行されるアクション、又は、満たされていないときに実行されるアクションは、メモリ156に記憶されてもよく、これによって、セキュリティ論理108による決定のうちの、各々の考え得る結果が、（例えば任意の適切なデータベース構造において）実行される1つ又は複数のアクションと対応して記憶されてもよい。アクション論理110は、セキュリティ論理108による決定の特定の結果をメモリ156に配置して、対応する1つ又は複数のアクションを識別してもよく、対応する1つ又は複数のアクションを実行してもよい。実行される複数のアクションは、ハードウェア構成レポーティングシステム100が危害を受けなくなるように、デバイス設計者によって選択されてもよい。例えば、幾つかの実施形態において、アクション論理110は、ハードウェア構成レポーティングシステム100と結合されたディスプレイデバイス上において、記憶されたセキュリティ要件が満たされているか満たされていないかのインジケータの表示を引き起こすように構成されてもよい。このインジケータは、グラフィカルユーザインタフェースの一部であってもよく、セキュリティ要件のステータスをユーザに通知してもよい。幾つかの実施形態において、アクション論理110は、ハードウェア構成レジスタと関連付けられたハードウェアに対して、記憶されたセキュリティ要件が満たされていないとの（セキュリティ論理108による）決定に応答してシャットダウンさせるように構成されてもよい。例えば、ハードウェア構成レジスタが並列通信ハードウェアと関連付けられている場合、アクション論理110は、並列通信ハードウェア用の記憶されたセキュリティ要件が満たされていないならば、並列通信ハードウェアに、一時的にシャットダウンさせてもよく、又は、複数の動作を中断させてもよい。これらのアクションは単に例示的なものであって、任意の適切なアクションが実行されてもよい。

【0019】

レポーティング論理104は、要求サービス論理112と、プロビジョン論理114とを含んでもよい。レポーティング論理104はまた、レポーティング論理104の複数のコンポーネントの何れかによって使用されてレポーティング論理104の動作に関連するデータを記憶し得るメモリ158を含んでもよい。アービタ論理102に関して上記で検討したように、レポーティング論理104は、アービタ論理102から要求の指標を受信して、それに応答するようにTEE116内で動作するよう、構成されてもよい。とりわけ、（TEEメモリに記憶される）要求サービス論理112は、アービタ論理102から（例えば要求論理106から）要求の指標を受信するようにTEE116内で動作するよう、構成されてもよい。要求は、1つ又は複数のハードウェア構成レジスタを表わしてもよい。

【0020】

（TEEメモリに記憶される）プロビジョン論理114は、要求サービス論理112に結合されてもよく、アービタ論理102に対して（例えばセキュリティ論理108に対して）、要求によって表わされるハードウェア構成レジスタの値のインジケータを提供するようにTEE116内で動作するよう、構成されてもよい。

【0021】

上記で留意されたように、アービタ論理102は、non-TEE118またはTEE116内から動作可能であってもよい。幾つかの実施形態において、アービタ論理102の1つ又は複数のインスタンスエイションは、TEE116内で動作してもよく、アービタ論理102の1つ又は複数のインスタンスエイションは、non-TEE118におい

10

20

30

40

50

て動作してもよい。図2は、そのようなハードウェア構成レポータリングシステム100の実施形態を示している。TEE116におけるアービタ論理102のインスタンスエイションは、例えば、起動したときに、起動中の様々なハードウェア構成レジスタの複数の値を評価することを実行し得る、基本入出力オペレーティングシステム(BIOS)フェーズアービタであってもよい。幾つかの実施形態において、BIOSフェーズアービタは、様々なハードウェア構成レジスタの複数の値が複数の記憶されたセキュリティ要件に従っているかをチェックすべくチェック要求を提供してもよく、もしその要件に従っていないならば、BIOSフェーズアービタは、装置が起動することを防げてよい。non-TEE118におけるアービタ論理102のインスタンスエイションは、例えば、オペレーティングシステム内で動作して、(例えば、周期的に、又は、管理者のコマンドで)動作中の様々なハードウェア構成レジスタの複数の値を評価する、セキュリティコンソールアプリケーションであってもよい。幾つかの実施形態において、non-TEE118は、レポータリング論理104が動作するプロセッシングデバイスとは異なるプロセッシングデバイスで動作してもよく、従って、アービタ論理102は、レポータリング論理104が動作するプロセッシングデバイスと異なるプロセッシングデバイスで動作してもよい。幾つかの実施形態において、non-TEE118は、レポータリング論理104が動作するプロセッシングデバイスと同じプロセッシングデバイスで動作してもよい。

【0022】

アービタ論理102が、レポータリング論理104がインスタンス化されているのと同じプロセッシングデバイスのnon-TEE118内で動作するアプリケーションに含まれる幾つかの実施形態において、ハードウェア構成レポータリングシステム100は、レポータリング論理104とアービタ論理102との間に、信頼できる「帯域内」チャンネルを確立してもよい。上記で留意されたように、アプリケーションは、セキュリティコンソール、ポリシーオーケストレータ、セキュリティドライバ、又は、他のセキュリティ関連ミドルウェアであってもよい。セキュリティコンソールは、アクション論理110からの複数の命令に応答して、任意のハードウェア構成レジスタ要求の複数の結果の視覚的表示をユーザに提供するように構成されてもよい。幾つかの実施形態において、この視覚的インジケータは、「合格／不合格」インジケータの形態を取ってもよい。ユーザが管理者であってより詳細な結果を望んでいる複数の実施形態において、セキュリティコンソールは、アクション論理110からの複数の命令に応答して、要求によって表わされる各ハードウェア構成レジスタの複数の値の視覚的インジケータを提供してもよい。

【0023】

アービタ論理102が、レポータリング論理104がインスタンス化されているプロセッシングデバイスとは異なるプロセッシングデバイスのnon-TEE118内で動作するアプリケーションに含まれる幾つかの実施形態において、ハードウェア構成レポータリングシステム100は、レポータリング論理104とアービタ論理102との間に、信頼できる「帯域外」チャンネルを確立してもよい。幾つかのそのような実施形態において、アービタ論理102は、マネージャビリティエンジン(ME)、コンバインドセキュリティおよびマネージャビリティエンジン(CSME)、又は、アクティブマネジメントテクノロジー(AMT)においてインスタンス化されてもよい。

【0024】

上記で留意されたように、幾つかの実施形態において、TEE116はSMMであってもよく、TEEメモリはSMMメモリ(例えば、システム管理ランダムアクセスメモリまたはSMRAM)であってもよい。図3は、そのようなハードウェア構成レポータリングシステム100の実施形態を示している。図3の実施形態において、SMM160は、TEE116として機能してもよく、レポータリング論理104は、SMM160内で動作してもよい。BIOS120は、SMM160を含んでもよく、また、1つ又は複数のドライバ実行環境(DXE)スクリプト122を含んでもよい。1つ又は複数のDXEスクリプト122は、図2のハードウェア構成レポータリングシステム100の実施形態におけるTEE116に含まれるアービタ論理102として機能してもよい。従って、DXE

スクリプト 1 2 2 は、ハードウェア構成レジスタを表わす要求のインジケータを、（例えば起動中に）レポーティング論理 1 0 4 に提供してもよく、レポーティング論理 1 0 4 はそれに従って応答してもよい。オペレーティングシステム 1 2 4 は、non-TEE 1 1 8 として機能してもよく、（例えば図 2 に示されるように）non-TEE 1 1 8 に含まれるアービタ論理 1 0 2 として機能する 1 つ又は複数のアプリケーション 1 2 6 を含んでもよい。1 つ又は複数のアプリケーション 1 2 6 は、本明細書で開示される複数のハードウェア構成レジスタ要求動作及び応答動作を実行すべく、SMM 1 6 0 のレポーティング論理 1 0 4 と通信可能に結合されてもよい。例えば、アプリケーション 1 2 6 は、ハードウェア構成レジスタを表わす要求のインジケータを、レポーティング論理 1 0 4 に提供してもよく、レポーティング論理 1 0 4 はそれに従って応答してもよい。オペレーティングシステム 1 2 4 が動作するプロセッシングデバイスが、BIOS 1 2 0 が動作するプロセッシングデバイスと同じである複数の実施形態において、要求のインジケータは、プロセッシングデバイスを SMM 1 6 0 にエントリさせるシステム管理インタラプトを伴ってもよく、その場合に、要求のインジケータはレポーティング論理 1 0 4 によって処理されてもよい。

10

【0025】

TEE 1 1 6 用に可能性のある他の候補は、本明細書で説明される機能を有するレポーティング論理と共に構成可能でなくてもよい。例えば、トラステッドプラットフォームモジュール (TPM) は、通常は全てのチップセットレジスタ設定をレコードせず、代わりに、通常は現在のオペレーティングシステム構成情報を前のオペレーティングシステム構成情報と比較して、そのような情報における複数の変更を検出するのみである。しかしながら、TPM は通常、レポーティング論理 1 0 4 に関して上記で説明されたようなハードウェア構成レジスタの実際の値を提供することはできない。仮想マシンモニタ (VMM) といった他の候補は、多数のハードウェア構成レジスタ（例えば SMM 関連ハードウェア構成レジスタ）にアクセスできず、通常は複数の異なるプラットフォームに一般的であり、従って、複数のプラットフォーム特有クエリを実行できない。

20

【0026】

SMM 1 6 0 が TEE 1 1 6 として機能する複数の実施形態は、様々な利点を有し得る。SMM 1 6 0 は、複数のハードウェアレジスタにアクセスするために、他の複数のモード（例えばオペレーティングシステムが動作する複数のモード）に割り当てられるものより高いレベルの特権を有してもよい。幾つかの実施形態において、SMM 1 6 0 における場合には、プロセッシングデバイスは、任意のディスク部分を読み取り可能であってもよく、従って、複数のシステムリソースに完全にアクセス可能であってもよい。上記で検討されたように、SMM 1 6 0 は、別個の実行環境であり、従って、SMM メモリに記憶されるコード及びデータは、オペレーティングシステムカーネルに対して、又は、オペレーティングシステムにおいて動作している複数のアプリケーションに対して、可視ではなくてもよい。SMM 1 6 0 はインタラプトを介して入力されるので、SMM 1 6 0 は、ハードウェアレポーティング用のトリガ応答メカニズムを提供し、複数の外部ソースからの（例えば SMM 1 6 0 の外部のアービタ論理 1 0 2 からの）複数の要求を供給できる。更に、SMM 1 6 0 はまたプラットフォームファームウェアに組み込まれ、プラットフォームハードウェアのコンポーネントとして配送され、これにより、悪意のあるユーザが SMM 1 6 0 を除去する又は改ざんすることを困難にできる。

30

40

【0027】

幾つかの実施形態において、アービタ論理 1 0 2 からの要求のインジケータは、プロセッシングデバイスの TEE 1 1 6 へのエントリをトリガするインタラプトのソースに、少なくとも部分的に基づいてもよい。例えば、non-TEE 1 1 8 におけるアプリケーションが指定の入出力 (I/O) ポートにアクセスするならば、インタラプトがトリガされて、プロセッシングデバイスが TEE 1 1 6 にエントリしてもよい。メモリ 1 5 8 は、様々な I/O ポートの複数の位置を記憶してもよく、それらのポートへのアクセスによってインタラプトがトリガされる場合、そのインタラプトは、アービタ論理 1 0 2 からの要求

50

を示している。幾つかの実施形態において、特定の I / O ポートは、特定のタイプの要求（例えばチェックまたはクエリ）に対応してもよい。

【0028】

幾つかの実施形態において、アービタ論理 102 からの要求のインジケータは、non-TEE 118 において動作している場合にプロセッシングデバイスにアクセス可能な予め定められたレジスタに記憶されている値に、少なくとも部分的に基づいてもよい。例えば、特定のハードウェアレジスタ（例えば I / O ポート）が指定され、アービタ論理 102 によって、要求のインジケータとして特定の値でプログラムされてもよい。インタラプトが検出されてプロセッシングデバイスを TEE 116 にエントリさせた場合、レポーティング論理 104 は、特定のハードウェアレジスタの値を読み取るように構成されてもよい。幾つかの実施形態において、ハードウェアレジスタは、上記で検討されたように、自己のアクセスによって、プロセッシングデバイスを TEE 116 にエントリさせるインタラプトがトリガされたレジスタと同じである。特定のハードウェアレジスタの異なる複数の値は、異なる複数のタイプの要求（例えばチェック又はクエリ）と、要求インジケータによって表わされる異なる複数のハードウェア構成レジスタとに対応してもよい。特定のハードウェアレジスタの複数の値と、要求の複数のタイプおよび／またはハードウェア構成レジスタとの間の対応関係は、メモリ 158 に記憶され、レポーティング論理 104 によってアクセスされてもよい。幾つかの実施形態において、汎用レジスタが指定され、アービタ論理 102 によって特定の値でプログラムされてもよく、その特定の値は、レポーティング論理 104 に渡されるパラメータとして作用し得る。任意の適切なパラメータが、汎用レジスタを介して伝達されてもよい（例えば、レポーティング論理 104 がクエリ又はチェックの結果を提供する宛先の具体的なメモリ位置）。幾つかの実施形態において、この汎用レジスタの位置は、メモリ 158 に記憶されてもよく、レポーティング論理 104 は、要求を受信すると、この汎用レジスタをルックインするように構成されてもよい。

【0029】

図 4 は、レポーティング論理 104 の実施形態を示しており、要求サービス論理 112 と、プロビジョン論理 114 と、メモリ 158 の機能が、複数のドライバ間に配布されている。複数のドライバのうちの異なるものは、異なる複数のハードウェア構成レジスタにアクセス可能であってもよく、従って、異なる複数のハードウェア構成レジスタを表す複数の要求は、異なる複数のドライバによって少なくとも部分的にサービスされてもよい。図 4 は、レポーティング論理 104 が、コアドライバ 128 と、チップセットドライバ 130 と、プラットフォームドライバ 132 とを含む実施形態を示している。

【0030】

コアドライバ 128 は、多数の装置（例えば、単一の製造者によって製造された多数の装置）に共通の、一般的なチップセットであってもよい。レポーティング論理 104 で受信される複数の要求は、コアドライバ 128 で受信されてもよく、コアドライバ 128 は、レポーティング論理 104 の複数のドライバ（例えば、コアドライバ 128、チップセットドライバ 130、又は、プラットフォームドライバ 132）のうち何れが、要求によって表わされるハードウェア構成レジスタにアクセス可能であるかを決定するように構成されてもよい。コアドライバ 128 は次に、決定されたドライバと通信して、要求をサービスしてもよい。例えば、コアドライバ 128 は、（コアドライバ 128 自体が要求をサービスしないならば、）要求を、チップセットドライバ 130 またはプラットフォームドライバ 132 にルーティングしてもよく、チップセットドライバ 130 またはプラットフォームドライバ 132 は、ハードウェア構成レジスタにアクセスして要求に応答してもよく、チップセットドライバ 130 またはプラットフォームドライバ 132 は、アービタ論理 102 への提供用に、コアドライバ 128 に応答を返してもよい。

【0031】

幾つかの実施形態において、コアドライバ 128 は、（どのように SMRAM がキャッシュされるかを決定し得る）システム管理範囲レジスタ、（様々なデバッグおよび性能モ

ニタスク用に用いられる) 複数のモデル特有レジスタ (MSR) 134、複数の周辺コンポーネント相互接続 (PCI) レジスタ140、複数のメモリマップ I/O (MMIO) レジスタ136、及び、複数の I/O レジスタ138などの、基本システムリソースの複数のハードウェア構成レジスタにアクセス可能であってもよい。例えば、コアダライバ128は、システム管理範囲レジスタにアクセスして、(クエリにตอบสนองして、) システム管理範囲レジスタの値と、(例えばシステム管理範囲レジスタが8M整合アドレス (aligned address) として構成されているといった) システム管理範囲レジスタのデータタイプ構成とを含むデータを返すように構成されてもよい。

【0032】

幾つかの実施形態において、チップセットドライバ130は、(チップセット再マッピング用の) 複数のメモリコントローラハブ (MCH) レジスタ142、(VT-d レジスタ146のような) ダイレクトメモリアクセスに関連する複数のレジスタ、及び、(バックアップ起動ブロックを提供するためのRCBA_TOP_SWAP レジスタのような) 複数のルートコンプレックススペースアドレス (RCBA) レジスタ144などの、チップセットリソースの複数のハードウェア構成レジスタにアクセス可能であってもよい。

【0033】

幾つかの実施形態において、プラットフォームドライバ132は、複数のフラッシュ部分ロックレジスタ148、複数の埋め込みコントローラレジスタ、複数のパラレル及びシリアル通信レジスタ150、及び、キーボード、マウスまたは他の周辺機器に関連する複数のレジスタなどの、プラットフォームリソースの複数のハードウェア構成レジスタにアクセス可能であってもよい。

【0034】

図5は、様々な実施形態による、ハードウェア構成レポーティングの方法500の流れ図である。方法500の複数の動作が、レポーティング論理104内に構成されたTEE116を有するプロセッシングデバイスによって実行されるように検討されるかもしれないが、これは単に複数の例示的目的のためであって、これらの動作は、任意の適切なハードウェアによって実行されてもよい。方法500に関して以下で検討される複数の動作の何れも、ハードウェア構成レポーティングシステム100に関して上記で検討された複数の実施形態の何れかに従って実行され得る。

【0035】

段階502では、プロセッシングデバイスは、(例えばnon-TEE118から) TEE116にエントリしてもよい。プロセッシングデバイスは、インタラプトを受信したことにตอบสนองして、TEE116にエントリしてもよい。例えば、TEE116がSMM160である場合、プロセッシングデバイスは、システム管理インタラプトにตอบสนองしてSMM160にエントリしてもよい。

【0036】

段階504では、(TEE116において動作している) プロセッシングデバイスは、ハードウェア構成レジスタを表わしている要求の指標を受信してもよい。幾つかの実施形態において、レポーティング論理104の要求サービス論理112が、要求を受信してもよい。

【0037】

段階506では、(TEE116において動作している) プロセッシングデバイスは、段階504の要求において表わされたハードウェア構成レジスタの値のインジケータを提供してもよい。幾つかの実施形態において、レポーティング論理104のプロビジョン論理114がインジケータを提供してもよい。

【0038】

図6は、様々な実施形態による、ハードウェア構成アービトレーションの方法600の流れ図である。方法600の複数の動作が、アービタ論理102と共に構成されたプロセッシングデバイスによって実行されるように検討されるかもしれないが、これは単に複数の例示的目的のためであって、これらの動作は、任意の適切なハードウェアによって実行

10

20

30

40

50

されてもよい。方法600に関して以下で検討される複数の動作の何れも、ハードウェア構成レポーティングシステム100に関して上記で検討された複数の実施形態の何れかに従って実行され得る。

【0039】

段階602では、プロセッシングデバイスは、ハードウェア構成レジスタを表わしている要求の指標を、プロセッシングデバイスのTEEに位置するレポーティング論理（例えば、TEE116に位置するレポーティング論理104）に提供してもよい。幾つかの実施形態において、要求論理106は、段階602で、要求の指標を提供してもよい。幾つかの実施形態において、要求の指標は、要求を受信するプロセッシングデバイスのTEEと同じTEEにおいて動作しているアービタ論理102によって提供されてもよい。幾つかの実施形態において、要求の指標は、要求を受信するプロセッシングデバイスのnon-TEEにおいて動作しているアービタ論理102によって提供されてもよい。幾つかの実施形態において、要求の指標を提供するプロセッシングデバイスは、要求を受信するプロセッシングデバイスと異なるプロセッシングデバイスであってもよい。幾つかの実施形態において、TEEはSMMであってもよい。

10

【0040】

段階604では、プロセッシングデバイスは、要求に応答してレポーティング論理によって提供されるハードウェア構成レジスタの値がセキュリティ要件を満たしていないと決定してもよい。幾つかの実施形態において、セキュリティ論理108は、段階604の決定を実行してもよい。

20

【0041】

段階606では、プロセッシングデバイスは、セキュリティ要件が満たされていないとの決定に応答して、アクションを実行してもよい。幾つかの実施形態において、アクション論理110は、段階606のアクションを実行してもよい。セキュリティ要件が満たされていないとの決定について段階604および段階606に関して上記で検討されたが、セキュリティ要件が満たされているとの決定が実行されてもよく、それに従って、（例えばアクション論理110に関して上記で検討されたように）複数のアクションが実行されてもよい。

【0042】

図7は、様々な実施形態による、ハードウェア構成レポーティングおよびアービトレーションの方法700の流れ図である。方法700は、方法500（図5）および方法600（図6）の複数の動作のうちの、様々なものの複数の実施形態を含んでもよい。とりわけ、方法700は、複数のレポーティング動作716と、複数のアービトレーション動作730とを含む。複数のレポーティング動作716および複数のアービトレーション動作730は、異なる論理によって実行されてもよい。例えば、幾つかの実施形態において、付k数のレポーティング動作716は、レポーティング論理104によって実行されてもよく、複数のアービトレーション動作730は、アービタ論理102によって実行されてもよい。方法700の複数の動作は図4のレポーティング論理104および図1のアービタ論理102によって様々に実行されるものとして検討されてもよいが、これは単に複数の例示的目的のためであって、これらの動作は、任意の適切なハードウェアによって実行されてもよい。方法700に関して以下で検討される複数の動作の何れも、ハードウェア構成レポーティングシステム100に関して上記で検討された複数の実施形態の何れかに従って実行され得る。

30

40

【0043】

段階702では、レポーティング論理に含まれるコアダライバが起動されてもよい。段階702のコアダライバは、図4を参照して上記で検討されたコアダライバ128であってもよい。幾つかの実施形態において、起動は、ドライバエントリポイントの呼出しを含んでもよい。ドライバ（例えばコアダライバ128）は、メモリにおいて独自のデータ構造を準備してもよく、そのデータ構造におけるデータは、後になって使用されてもよい。幾つかの実施形態において、起動は、後で他の複数のドライバによって呼び出され得る、

50

1つ又は複数のコールバック機能又はプロトコルを登録することを含んでもよい。例えば、（例えば以下で検討されるような）チップセットドライバが、コアダライバによる利用のために、ChipsetCheck()およびChipsetReport()機能を登録してもよい。コアダライバが（例えばB I O SまたはO Sから）対応する機能要求を入手する場合、コアダライバは、その要求を適切なチップセットドライバ機能にディスパッチしてもよい。

【0044】

段階704では、レポーティング論理に含まれるチップセットドライバが起動されてもよい。段階704のチップセットドライバは、図4を参照して上記で検討されたチップセットドライバ130であってもよい。

【0045】

段階706では、レポーティング論理に含まれるプラットフォームドライバが起動されてもよい。段階706のプラットフォームドライバは、図4を参照して上記で検討されたプラットフォームドライバ132であってもよい。

【0046】

段階708では、レポーティング論理が、要求が受信されたかどうかを決定してもよい。上記で検討されたように、要求は、1つ又は複数のハードウェア構成レジスタを表わしてもよく、その要求のプロバイダ（例えばアービタ論理102）は、1つ又は複数のハードウェア構成レジスタについての情報を受信することを望んでいる。幾つかの実施形態において、段階708の決定は、コアダライバ128によって実行されてもよい。

【0047】

レポーティング論理が、要求が受信されていないと決定するならば、レポーティング論理は、段階708へと戻り、要求をモニタし続けてもよい。図7で破線矢印732によって示されているように、要求は、（以下で検討される）段階722の複数の動作を実行したことに応答して、アービタ論理によって提供されてもよい。レポーティング論理が、段階708で要求が受信されたと決定するならば、レポーティング論理は、段階710へと進み、要求がチェックされたかどうかを決定してもよい。要求論理106に関して上記で検討されたように、チェック要求は、1つ又は複数のハードウェア構成レジスタの値が一組の規定値に等しいかどうかを問い合わせてもよい。幾つかの実施形態において、段階710の決定は、コアダライバ128によって実行されてもよい。

【0048】

段階710において、レポーティング論理が、要求がチェックではないと決定するならば、レポーティング論理は、段階712に進み、要求がクエリであるかどうかを決定してもよい。要求論理106に関して上記で検討されたように、クエリは、1つ又は複数のハードウェア構成レジスタの値を求めてもよい。幾つかの実施形態において、段階712の決定は、コアダライバ128によって実行されてもよい。段階712において、レポーティング論理が、要求がクエリではないと決定し、許可されている他の要求タイプが無いならば、レポーティング論理は、段階708へと戻り、有効な要求の受信をモニタし続けてもよい。レポーティング論理が、段階710で要求がチェックであると決定するならば、又は、段階712で要求がクエリであると決定するならば、レポーティング論理は、段階714に進み、要求によって表わされる1つ又は複数のハードウェア構成レジスタの値のインジケータを提供してもよい。幾つかの実施形態において、コアダライバ128は、レポーティング論理104に含まれる複数のドライバのうちの他のドライバ（例えばチップセットドライバ130またはプラットフォームドライバ132）が、要求において表わされるハードウェア構成レジスタにアクセス可能であると決定してもよく、要求を決定されたドライバにルーティングして、決定されたドライバと通信し、適切に、チェック又はクエリへの応答を受信してもよい。幾つかの実施形態において、段階702のコアダライバは、1つ又は複数のハードウェア構成レジスタの値のインジケータを提供してもよい。1つ又は複数のハードウェア構成レジスタの値のインジケータは、例えば、アービタ論理（例えばアービタ論理102）へと提供されてもよい。図7で破線矢印734によって示されるように、その値のインジケータは、アービタ論理へと提供されてもよい。

10

20

30

40

50

【0049】

方法700の複数の動作730へと戻ると、段階718では、XMLスクリプトが生成されてもよい。要求論理106に関して上記で検討されたように、XMLスクリプトは、開発者によって生成されてもよく、（例えば要求論理106によって）自動的に生成されてもよい。XMLは開発者によって容易に理解されるシンタックスを用いているので、XMLスクリプトにより、開発者が、予期されるハードウェア構成を（例えば、1つ又は複数の記憶されたセキュリティ要件の形態で、又は、他のセキュリティポリシーの形態で）容易に定義することが可能になってよい。XMLスクリプトは、特定の要求の形態およびコンテンツを指定してもよく、メモリ156に記憶されてもよい。

【0050】

段階720では、段階718のXMLスクリプトは、バイナリスクリプトへと変換されてもよい。要求論理106に関して上記で検討されたように、バイナリスクリプトは、レポート論理（例えばレポート論理104）に要求の指標を提供すべく、要求論理106によって実行可能であってもよい。幾つかの実施形態において、バイナリスクリプトは、ファームウェアに含まれてもよく、アービタ論理102によって、BIOS起動中にレポート論理104へと送信されてもよい。

【0051】

段階722では、段階720のバイナリスクリプトが実行されて、レポート論理（例えばレポート論理104）に要求の指標を提供してもよい。要求は、情報が求められているハードウェア構成レジスタを表わしてもよい。幾つかの実施形態において、要求は、レポート論理によって認識される特定のタイプの要求であってもよい（例えば、上記で検討されたようなチェック又はクエリ）。図7で破線矢印732によって示されているように、要求はレポート論理に提供されてもよい。

【0052】

段階724において、（例えば矢印734によって示されているように）要求によって表わされるハードウェア構成レジスタの値のインジケータを受信したことに応答して、受信インジケータが評価され、記憶されたセキュリティ要件が満たされているかどうかを決定してもよい。幾つかの実施形態において、セキュリティ論理108は、上記で検討された複数の実施形態の何れかに従って、段階724の複数の動作を実行してもよい。

【0053】

段階724において、何らかの記憶されたセキュリティ要件が満たされていると決定されるならば、アービタ論理は、段階728に進んでもよく、要求によって表わされるハードウェアレジスタと関連付けられたコンピューティングデバイスの通常動作が再開してもよい。幾つかの実施形態において、何らかの記憶されたセキュリティ要件が満たされていると決定したときに、1つ又は複数のアクションが実行されてもよい（例えば、複数の記憶されたセキュリティ要件が満たされていることを、ディスプレイデバイス上でレポートすること）。段階724において、複数の記憶されたセキュリティ要件が何ら満たされていないと決定されるならば、アービタ論理は、段階726に進んでもよく、アクションが実行されてもよい。そのアクションは、アクション論理110に関して上記で検討されたように、任意のセキュリティリスクミティゲーションまたは他の適切なアクションであってもよい。幾つかの実施形態において、アクション論理110が、段階726のアクションを実行してもよい。

【0054】

幾つかの実施形態において、ハードウェア構成レポートシステム100は、自己の複数の動作を更新するための論理を含んでもよい。図8は、幾つかの実施形態による、ハードウェア構成レポートシステム100に含まれ得る更新システム800のブロック図である。更新システム800は、（例えば、図4を参照して上記で検討されたレポート論理104の実施形態に従って）レポート論理104のコアドライバ128においてスクリプト更新エージェント152を含む。スクリプト更新エージェントは、オペレーティングシステム124内で動作しているセキュリティコンソール154と通

10

20

30

40

50

信可能に結合されてもよい。セキュリティコンソール154は、レポーティング論理104に、レポーティング論理104の基礎となるコードのバージョン番号またはデジタル署名を問い合わせる(query)ように構成されてもよく、このコードが最新バージョン(又は許容可能なバージョン)であるかどうかを決定してもよい。TEE116の外部で動作しているコンポーネントがTEE116のメモリを直接見ることができなくてもよいが、セキュリティコンソール154は、TEE116のハンドラに要求を送信して、デジタル署名またはバージョン番号をチェックするように構成されてもよい。幾つかの実施形態において、TEE116は、信頼できるソースから、レポーティング論理104の更新イメージを要求し、それに従ってレポーティング論理104を更新するように構成されてもよい。

10

【0055】

ここで図9を参照すると、様々な実施形態に従って、開示される複数の実施形態を実施するのに適した例示的な装置のブロック図が提供されている。様々な実施形態において、装置900は、サーバ、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、携帯電話、スマートフォン、パーソナルデジタルアシスタント、ゲームコンソール、インターネットアプライアンス、モバイルインターネットデバイスまたは他のコンピューティングデバイスであってもよい。

【0056】

示されるように、装置900は、多数のプロセッシングデバイス902と、システムメモリ904を含む。複数のプロセッシングデバイス902の任意の1つ又は複数のは、ハードウェア構成レポーティングシステム(例えばハードウェア構成レポーティングシステム100)の一部として、(レポーティング論理104のような)レポーティング論理、および/または、(アービタ論理102のような)アービタ論理を含むように構成されてもよい。例えば、複数のプロセッシングデバイス902の1つ又は複数のは、1つのTEEにおいて動作するように構成され、複数のプロセッシングデバイス902の1つ又は複数のは、1つ又は複数のnon-TEEにおいて動作するように構成されてもよい。幾つかの実施形態において、TEEはSMMであってもよい。本明細書で開示される複数のハードウェア構成レポーティングシステムの何れかのコンポーネントの機能を実行している論理は、少なくとも部分的に、(TEEの複数の境界に従ってパーティション化され得る)システムメモリ904に記憶されてもよい。更に、装置900は、(ディスク、ハードドライブ、コンパクトディスクリードオンリーメモリ(CD-ROM)等の)複数の大容量ストレージデバイス906、(ディスプレイ、キーボード、カーソル制御等の)複数の入出力デバイス908、及び、(複数のネットワークインタフェースカード、モデム等の)複数の通信インタフェース910を含んでもよい。複数の要素は、1つ又は複数のバスを表わしているシステムバス912を介して各々他に結合されてもよい。複数のバスの場合、それらは1つ又は複数のバスブリッジ(不図示)によって橋渡しされてもよい。

20

30

【0057】

これらの要素のそれぞれは、この分野で既知である、自己の従来の機能を実行してもよい。とりわけ、システムメモリ904および大容量ストレージ906は、本明細書では計算論理922として集合的に示されている各プロセッシングデバイス902によって実行された場合に、図5-7の何れかの方法を実行する複数のプログラミング命令の作業用コピーおよび永久コピー、又は、それらの複数部分を記憶するのに使用されてもよい。様々なコンポーネントは、複数のプロセッシングデバイス902によってサポートされている複数のアセンブラ命令、又は、例えばそのような命令へとコンパイルされ得るCのような複数の高レベル言語によって実行されてもよい。複数のプロセッシングデバイス902およびシステムメモリ904は、様々な実行速度および電力消費の複数のプロセッシングコアと、(例えば1つ又は複数のレベルのキャッシュを備える)様々なアーキテクチャおよび様々なタイプ(例えばダイナミックランダムアクセス、FLASH等)のメモリとの複数の配置を含む、広範なプロセッシングデバイスおよびメモリ配置を表わしてもよい。例えば、システムメモリ904は、プロセッシングデバイス902がnon-TEEにおい

40

50

て動作している場合にはアクセス不可能である T E E メモリを含んでもよい。

【0058】

複数のプログラミング命令の永久コピーは、ファクトリにおける大容量ストレージ 906 へと置かれてもよく、又は、例えば、コンパクトディスク (C D) のような機械アクセス可能配布媒体 (不図示) を介して、若しくは、(例えば配信サーバ (不図示) から) 通信インタフェース 910 を介して、フィールドに置かれてもよい。すなわち、エージェントプログラムの実装例を有している 1 つ又は複数の配布媒体は、そのエージェントプログラムを様々なコンピューティングデバイスに配布するのに使用されてもよい。幾つかの実施形態において、レポーティングおよび／またはアービタ論理は、更新メカニズム (例えば、図 8 を参照して上記で検討されたレポーティング論理更新メカニズム) に従って、更新されてもよい。複数の要素 902 - 912 の構成は既知であり、従って、更なる説明は行わない。

10

【0059】

上記で説明された複数の技術を実行するための、(機械可読記憶媒体のような非一時的機械可読媒体を含む) 機械可読媒体、複数の方法、システムおよびデバイスは、本明細書で開示される複数の実施形態の複数の用例である。追加して、上記で説明された複数のインタラクションにおける他の複数のデバイスは、開示される様々な技術を実行するように構成されてもよい。

【0060】

本明細書で開示される複数のハードウェア構成レポーティングシステムの様々な実施形態は、任意の数の装置にレポーティングする機能およびハードウェア構成を提供するのに用いられてもよい。例えば、様々な実施形態が、B I O S 整合性試験を提供するのに用いられてもよい。様々な実施形態が、ハードウェアおよびファームウェアセキュリティ状態情報を提供するのに用いられてもよい。

20

【0061】

以下の複数の段落は、本明細書で開示された様々な実施形態の複数の例を記載している。例 1 は、T E E および n o n - T E E を有し、特定のインタラプトに応答して n o n - T E E から T E E にエントリするプロセッシングデバイスであって、T E E は、n o n - T E E からアクセス不可能なメモリから実行される、プロセッシングデバイスと、メモリに記憶され、ハードウェア構成レジスタを表わしている要求の指標をアービタ論理から受信するように T E E 内で動作する要求サービス論理と、メモリに記憶され、T E E 内で動作し、要求によって表わされるハードウェア構成レジスタの値のインジケータをアービタ論理にレポートするレポーティング論理と、を備えるハードウェア構成レポーティング用の装置である。

30

【0062】

例 2 は、例 1 の主題を含んでもよく、更に、アービタ論理からの要求の指標が、n o n - T E E において動作している場合にプロセッシングデバイスにアクセス可能な予め定められたレジスタに記憶されている値に、少なくとも部分的に基づくことを特定してもよい。

【0063】

例 3 は、例 1 - 2 の何れかの主題を含んでもよく、更に、アービタ論理からの要求の指標が、プロセッシングデバイスの T E E へのエントリをトリガした特定のインタラプトのソースに、少なくとも部分的に基づくことを特定してもよい。

40

【0064】

例 4 は、例 1 - 3 の何れかの主題を含んでもよく、更に、アービタ論理がプロセッシングデバイスの n o n - T E E において動作することを特定してもよい。

【0065】

例 5 は、例 1 - 3 の何れかの主題を含んでもよく、更に、アービタ論理が、プロセッシングデバイスと異なる第 2 のプロセッシングデバイス上で動作することを特定してもよい。

50

【0066】

例6は、例1-3の何れかの主題を含んでもよく、更に、アービタ論理が、プロセッシングデバイスのTEEにおいて動作することを特定してもよい。

【0067】

例7は、例1-6の何れかの主題を含んでもよく、更に、要求がハードウェア構成レジスタの値のクエリであり、ハードウェア構成レジスタの値のインジケータがハードウェア構成レジスタの値であることを特定してもよい。

【0068】

例8は、例1-6の何れかの主題を含んでもよく、更に、要求が、ハードウェア構成レジスタの値が規定値に等しいことのチェックであり、ハードウェア構成レジスタの値のインジケータが、ハードウェア構成レジスタの値が規定値に等しいか否かのバイナリインジケータであることを特定してもよい。

10

【0069】

例9は、例8の主題を含んでもよく、更に、アービタ論理が、プロセッシングデバイスの基本入出力オペレーティングシステム（BIOS）において動作しているドライバ実行環境（DXE）スクリプトであることを特定してもよい。

【0070】

例10は、例1-9の何れかの主題を含んでもよく、更に、要求サービス論理が更に、複数のドライバのうちの何れが、要求によって表わされるハードウェア構成レジスタにアクセス可能であるかを決定し、決定されたドライバと通信して要求をサービスすることを特定してもよい。

20

【0071】

例11は、例1-3および6-10の何れかの主題を含んでもよく、更に、アービタ論理が、起動したときに実行する基本入出力オペレーティングシステム（BIOS）フェーズアービタであることを特定してもよい。

【0072】

例12は、例1-11の何れかの主題を含んでもよく、更に、TEEがシステム管理モードであることを特定してもよい。

【0073】

例13は、コンピューティング論理が、アプリケーションからの要求の指標を、プロセッシングデバイスのTEEという信頼できる実行環境のレポート論理に提供する段階であって、プロセッシングデバイスが、TEEと、non-TEEという信頼できない実行環境とを有し、プロセッシングデバイスが、特定のインタラプトに応答してnon-TEEからTEEにエントリし、TEEが、non-TEEからアクセス不可能なメモリから実行され、レポート論理がメモリに記憶され、要求がハードウェア構成レジスタを表わしている、段階と、要求の指標を受信したことに応答してレポート論理によって提供された、要求によって表わされるハードウェア構成レジスタの値のインジケータが、記憶されたセキュリティ要件を満たしていないと、コンピューティング論理が決定する段階と、コンピューティング論理が、記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクションを実行する段階と、を備えるハードウェア構成アービトレーションの方法である。

30

40

【0074】

例14は、例13の主題を含んでもよく、更に、記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクションを実行する段階が、記憶されたセキュリティ要件が満たされていないとの決定に応答して、記憶されたセキュリティ要件が満たされていないことのインジケータの表示をディスプレイデバイス上に引き起こす段階を含むことを特定してもよい。

【0075】

例15は、例13-14の何れかの主題を含んでもよく、更に、記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクションを実行する段階が、記憶され

50

たセキュリティ要件が満たされていないとの決定に応答して、ハードウェア構成レジスタと関連付けられたハードウェアにシャットダウンさせる段階を含むことを特定してもよい。

【0076】

例16は、例13-15の何れかの主題を含んでもよく、更に、ハードウェア構成レジスタがチップセット再マッピングレジスタであることを特定してもよい。

【0077】

例17は、例13-15の何れかの主題を含んでもよく、更に、ハードウェア構成レジスタがシステム管理モードロックレジスタであることを特定してもよい。

【0078】

例18は、例13-15の何れかの主題を含んでもよく、更に、ハードウェア構成レジスタがフラッシュ部分ロックレジスタであることを特定してもよい。

【0079】

例19は、例13-18の何れかの主題を含んでもよく、更に、コンピューティング論理の少なくとも一部がプロセッシングデバイスのnon-TEEにおいて動作することを特定してもよい。

【0080】

例20は、例13-19の何れかの主題を含んでもよく、更に、コンピューティング論理の少なくとも一部が、プロセッシングデバイスと異なる第2のプロセッシングデバイス上で動作することを特定してもよい。

【0081】

例21は、例13-20の何れかの主題を含んでもよく、更に、コンピューティング論理の少なくとも一部がプロセッシングデバイスのTEEにおいて動作することを特定してもよい。

【0082】

例22は、例13-21の何れかの主題を含んでもよく、更に、TEEがシステム管理モードであることを特定してもよい。

【0083】

例23は、装置の1つ又は複数のプロセッシングデバイスによって実行されたことに応答して、装置に例13-22の何れかの方法を実行させる複数の命令を有する1つ又は複数の機械可読媒体である。

【0084】

例24は、アプリケーションからの要求の指標を、プロセッシングデバイスのTEEという信頼できる実行環境のレポート論理に提供するための手段であって、プロセッシングデバイスが、TEEと、non-TEEという信頼できない実行環境とを有し、プロセッシングデバイスが、特定のインタラプトにตอบสนองしてnon-TEEからTEEにエントリし、TEEが、non-TEEからアクセス不可能なメモリから実行され、レポート論理がメモリに記憶され、要求がハードウェア構成レジスタを表わしている、手段と、要求の指標を受信したことにตอบสนองしてレポート論理によって提供された、要求によって表わされるハードウェア構成レジスタの値のインジケータが、記憶されたセキュリティ要件を満たしていないと決定するための手段と、記憶されたセキュリティ要件が満たされていないとの決定にตอบสนองして、アクションを実行するための手段と、を備えるハードウェア構成アービトレーション用の装置である。

【0085】

例25は、例24の主題を含んでもよく、更に、記憶されたセキュリティ要件が満たされていないとの決定にตอบสนองして、アクションを実行するための手段が、記憶されたセキュリティ要件が満たされていないとの決定にตอบสนองして、記憶されたセキュリティ要件が満たされていないことのインジケータの表示をディスプレイデバイス上に引き起こすための手段を含むことを特定してもよい。

【0086】

10

20

30

40

50

例 2 6 は、例 2 4 - 2 5 の何れかの主題を含んでもよく、更に、記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクションを実行するための手段が、記憶されたセキュリティ要件が満たされていないとの決定に応答して、ハードウェア構成レジスタと関連付けられたハードウェアにシャットダウンさせるための手段を含むことを特定してもよい。

【0087】

例 2 7 は、例 2 4 - 2 6 の何れかの主題を含んでもよく、更に、ハードウェア構成レジスタがチップセット再マッピングレジスタであることを特定してもよい。

【0088】

例 2 8 は、例 2 4 - 2 6 の何れかの主題を含んでもよく、更に、ハードウェア構成レジスタがシステム管理モードロックレジスタであることを特定してもよい。

10

【0089】

例 2 9 は、例 2 4 - 2 6 の何れかの主題を含んでもよく、更に、ハードウェア構成レジスタがフラッシュ部分ロックレジスタであることを特定してもよい。

【0090】

例 3 0 は、例 2 4 - 2 9 の何れかの主題を含んでもよく、更に、装置の少なくとも一部がプロセッシングデバイスの `non-TEE` において動作することを特定してもよい。

【0091】

例 3 1 は、例 2 4 - 3 0 の何れかの主題を含んでもよく、更に、装置の少なくとも一部が、プロセッシングデバイスと異なる第 2 のプロセッシングデバイス上で動作することを特定してもよい。

20

【0092】

例 3 2 は、例 2 4 - 3 1 の何れかの主題を含んでもよく、更に、装置の少なくとも一部がプロセッシングデバイスの `TEE` において動作することを特定してもよい。

【0093】

例 3 3 は、例 2 4 - 3 2 の何れかの主題を含んでもよく、更に、`TEE` がシステム管理モードであることを特定してもよい。

【0094】

例 3 4 は、アプリケーションからの要求の指標を、プロセッシングデバイスの `TEE` のレポート論理に提供する要求論理であって、プロセッシングデバイスが、`TEE` および `non-TEE` を有し、プロセッシングデバイスが、特定のインタラプトに応答して `non-TEE` から `TEE` にエントリし、`TEE` が、`non-TEE` からアクセス不可能なメモリから実行され、レポート論理がメモリに記憶され、要求がハードウェア構成レジスタを表わしている、要求論理と、要求の指標を受信したことに応答してレポート論理によって提供された、要求によって表わされるハードウェア構成レジスタの値のインジケータが、記憶されたセキュリティ要件を満たしていないと決定するセキュリティ論理と、記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクションを実行するアクション論理と、を備えるハードウェア構成アービトレーション用の装置である。

30

【0095】

例 3 5 は、例 3 4 の主題を含んでもよく、更に、記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクションを実行することが、記憶されたセキュリティ要件が満たされていないとの決定に応答して、記憶されたセキュリティ要件が満たされていないことのインジケータの表示をディスプレイデバイス上に引き起こすことを含むことを特定してもよい。

40

【0096】

例 3 6 は、例 3 4 - 3 5 の何れかの主題を含んでもよく、更に、記憶されたセキュリティ要件が満たされていないとの決定に応答して、アクションを実行することが、記憶されたセキュリティ要件が満たされていないとの決定に応答して、ハードウェア構成レジスタと関連付けられたハードウェアにシャットダウンさせることを含むことを特定してもよい

50

。

【0097】

例37は、例34-36の何れかの主題を含んでもよく、更に、ハードウェア構成レジスタがチップセット再マッピングレジスタであることを特定してもよい。

【0098】

例38は、例34-36の何れかの主題を含んでもよく、更に、ハードウェア構成レジスタがシステム管理モードロックレジスタであることを特定してもよい。

【0099】

例39は、例34-36の何れかの主題を含んでもよく、更に、ハードウェア構成レジスタがフラッシュ部分ロックレジスタであることを特定してもよい。

10

【0100】

例40は、例34-39の何れかの主題を含んでもよく、更に、装置の少なくとも一部がプロセッシングデバイスのnon-TEEにおいて動作することを特定してもよい。

【0101】

例41は、例34-40の何れかの主題を含んでもよく、更に、装置の少なくとも一部が、プロセッシングデバイスと異なる第2のプロセッシングデバイス上で動作することを特定してもよい。

【0102】

例42は、例34-41の何れかの主題を含んでもよく、更に、装置の少なくとも一部がプロセッシングデバイスのTEEにおいて動作することを特定してもよい。

20

【0103】

例43は、例34-42の何れかの主題を含んでもよく、更に、TEEがシステム管理モードであることを特定してもよい。

【0104】

例44は、コンピューティング論理が、アービタ論理から要求の指標を受信する段階であって、コンピューティング論理はメモリ内に記憶され、プロセッシングデバイスのTEE内で動作し、プロセッシングデバイスは、TEEおよびnon-TEEを有し、プロセッシングデバイスは、特定のインタラプトに応答してnon-TEEからTEEにエントリし、TEEは、メモリから実行され、メモリは、non-TEEからアクセス不可能であり、要求は、ハードウェア構成レジスタを表わしている、段階と、コンピューティング論理が、要求によって表わされるハードウェア構成レジスタの値のインジケータをアービタ論理にレポーティングする段階と、を備えるハードウェア構成レポーティングの方法である。

30

【0105】

例45は、例44の主題を含んでもよく、更に、アービタ論理からの要求の指標が、non-TEEにおいて動作している場合にプロセッシングデバイスにアクセス可能な予め定められたレジスタに記憶されている値に、少なくとも部分的に基づくことを特定してもよい。

【0106】

例46は、例44-45の何れかの主題を含んでもよく、更に、アービタ論理からの要求の指標が、プロセッシングデバイスのTEEへのエントリをトリガした特定のインタラプトのソースに、少なくとも部分的に基づくことを特定してもよい。

40

【0107】

例47は、例44-46の何れかの主題を含んでもよく、更に、アービタ論理がプロセッシングデバイスのnon-TEEにおいて動作することを特定してもよい。

【0108】

例48は、例44-46の何れかの主題を含んでもよく、更に、アービタ論理が、プロセッシングデバイスと異なる第2のプロセッシングデバイス上で動作することを特定してもよい。

【0109】

50

例 4 9 は、例 4 4 - 4 6 の何れかの主題を含んでもよく、更に、アービタ論理がプロセッシングデバイスの T E E において動作することを特定してもよい。

【0 1 1 0】

例 5 0 は、例 4 4 - 4 9 の何れかの主題を含んでもよく、更に、要求がハードウェア構成レジスタの値のクエリであり、ハードウェア構成レジスタの値のインジケータがハードウェア構成レジスタの値であることを特定してもよい。

【0 1 1 1】

例 5 1 は、例 4 4 - 4 9 の何れかの主題を含んでもよく、更に、要求が、ハードウェア構成レジスタの値が規定値に等しいことのチェックであり、ハードウェア構成レジスタの値のインジケータが、ハードウェア構成レジスタの値が規定値に等しいか否かのバイナリインジケータであることを特定してもよい。

10

【0 1 1 2】

例 5 2 は、例 5 1 の主題を含んでもよく、更に、アービタ論理が、プロセッシングデバイスの基本入出力オペレーティングシステム (B I O S) において動作しているドライバ実行環境 (D X E) スクリプトであることを特定してもよい。

【0 1 1 3】

例 5 3 は、例 4 4 - 5 2 の何れかの主題を含んでもよく、更に、コンピューティング論理が、複数のドライバのうちの何れが、要求によって表わされるハードウェア構成レジスタにアクセス可能であるかを決定する段階と、決定されたドライバと通信して要求をサービスする段階と、を更に含んでもよい。

20

【0 1 1 4】

例 5 4 は、例 4 4 - 4 6 および 4 9 - 5 3 の何れかの主題を含んでもよく、更に、アービタ論理が、起動したときに実行する基本入出力オペレーティングシステム (B I O S) フェーズアービタであることを特定してもよい。

【0 1 1 5】

例 5 5 は、例 4 4 - 5 4 の何れかの主題を含んでもよく、更に、T E E がシステム管理モードであることを特定してもよい。

【0 1 1 6】

例 5 6 は、アービタ論理から要求の指標を受信するための手段であって、受信するための手段はメモリ内に記憶され、プロセッシングデバイスの T E E 内で動作し、プロセッシングデバイスは、T E E および n o n - T E E を有し、プロセッシングデバイスは、特定のインタラプトに応答して n o n - T E E から T E E にエントリし、T E E は、メモリから実行され、メモリは、n o n - T E E からアクセス不可能であり、要求は、ハードウェア構成レジスタを表わしている、手段と、要求によって表わされるハードウェア構成レジスタの値のインジケータをアービタ論理にレポートするための手段であって、受信するための手段はメモリ内に記憶され、プロセッシングデバイスの T E E 内で動作する、手段と、を備えるハードウェア構成レポート用の装置である。

30

【0 1 1 7】

例 5 7 は、例 5 6 の主題を含んでもよく、更に、アービタ論理からの要求の指標が、n o n - T E E において動作している場合にプロセッシングデバイスにアクセス可能な予め定められたレジスタに記憶されている値に、少なくとも部分的に基づくことを特定してもよい。

40

【0 1 1 8】

例 5 8 は、例 5 6 - 5 7 の何れかの主題を含んでもよく、更に、アービタ論理からの要求の指標が、プロセッシングデバイスの T E E へのエントリをトリガした特定のインタラプトのソースに、少なくとも部分的に基づくことを特定してもよい。

【0 1 1 9】

例 5 9 は、例 5 6 - 5 8 の何れかの主題を含んでもよく、更に、アービタ論理がプロセッシングデバイスの n o n - T E E において動作することを特定してもよい。

【0 1 2 0】

50

例 60 は、例 56－58 の何れかの主題を含んでもよく、更に、アービタ論理がプロセッシングデバイスと異なる第 2 のプロセッシングデバイス上で動作することを特定してもよい。

【0121】

例 61 は、例 56－58 の何れかの主題を含んでもよく、更に、アービタ論理がプロセッシングデバイスの TEE において動作することを特定してもよい。

【0122】

例 62 は、例 56－61 の何れかの主題を含んでもよく、更に、要求がハードウェア構成レジスタの値のクエリであり、ハードウェア構成レジスタの値のインジケータがハードウェア構成レジスタの値であることを特定してもよい。

10

【0123】

例 63 は、例 56－61 の何れかの主題を含んでもよく、更に、要求が、ハードウェア構成レジスタの値が規定値に等しいことのチェックであり、ハードウェア構成レジスタの値のインジケータが、ハードウェア構成レジスタの値が規定値に等しいか否かのバイナリインジケータであることを特定してもよい。

【0124】

例 64 は、例 63 の主題を含んでもよく、更に、アービタ論理が、プロセッシングデバイスの基本入出力オペレーティングシステム（BIOS）において動作しているドライバ実行環境（DXE）スクリプトであることを特定してもよい。

【0125】

20

例 65 は、例 56－64 の何れかの主題を含んでもよく、更に、複数のドライバのうちの何れが、要求によって表わされるハードウェア構成レジスタにアクセス可能であるかを決定するための手段と、決定されたドライバと通信して要求をサービスするための手段と、を含んでもよく、決定するための手段および通信するための手段は、メモリ内に記憶され、プロセッシングデバイスの TEE 内で動作する。

【0126】

例 66 は、例 56－58 および 61－65 の何れかの主題を含んでもよく、更に、アービタ論理が、起動したときに実行する基本入出力オペレーティングシステム（BIOS）フェーズアービタであることを特定してもよい。

【0127】

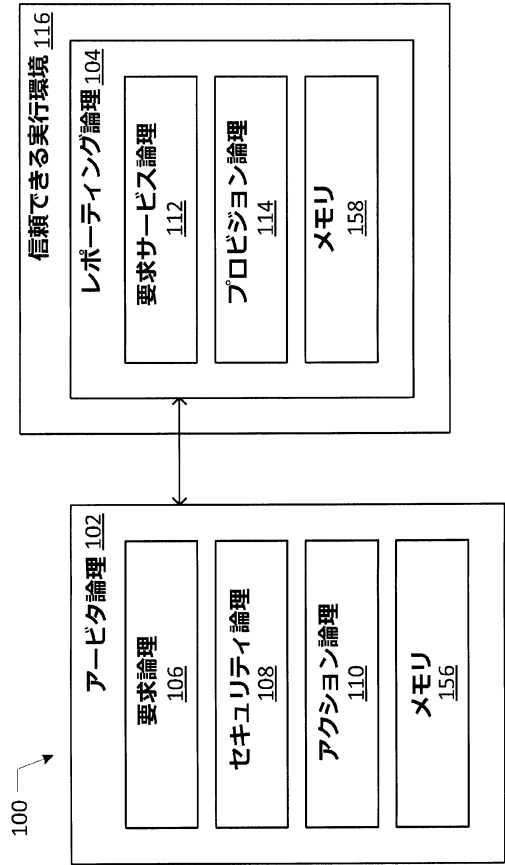
30

例 67 は、例 56－66 の何れかの主題を含んでもよく、更に、TEE がシステム管理モードであることを特定してもよい。

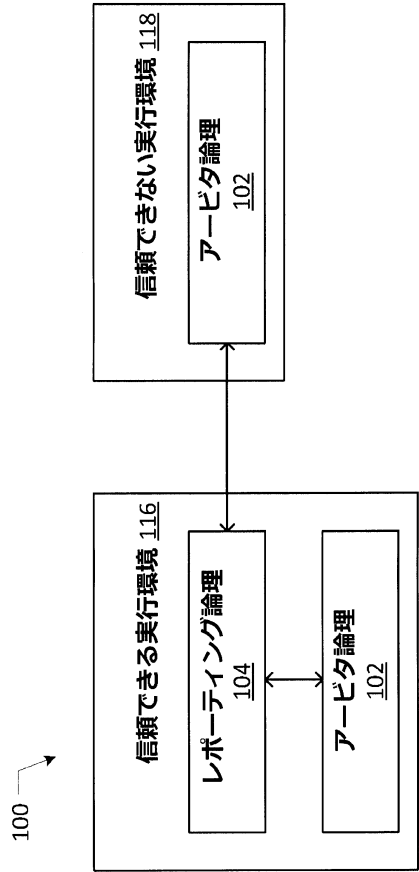
【0128】

例 68 は、装置の 1 つ又は複数のプロセッシングデバイスによって実行されたことに応答して、装置に例 44－55 の何れかの方法を実行させる複数の命令を有する 1 つ又は複数の機械可読媒体である。

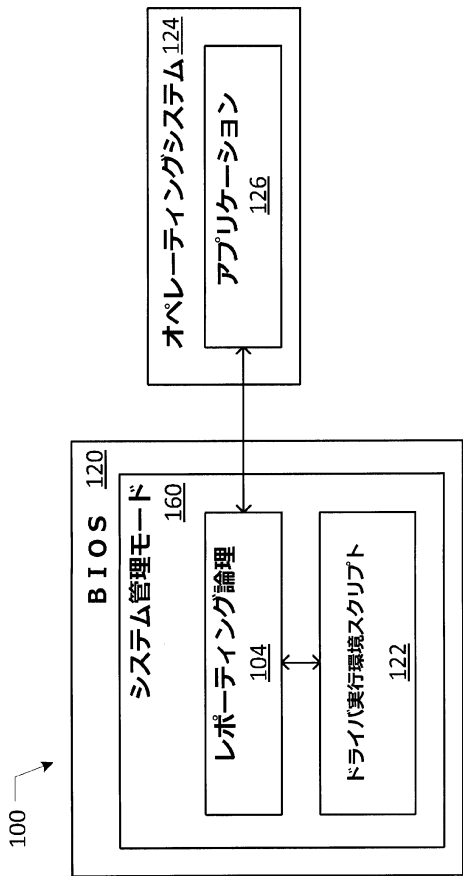
【図 1】



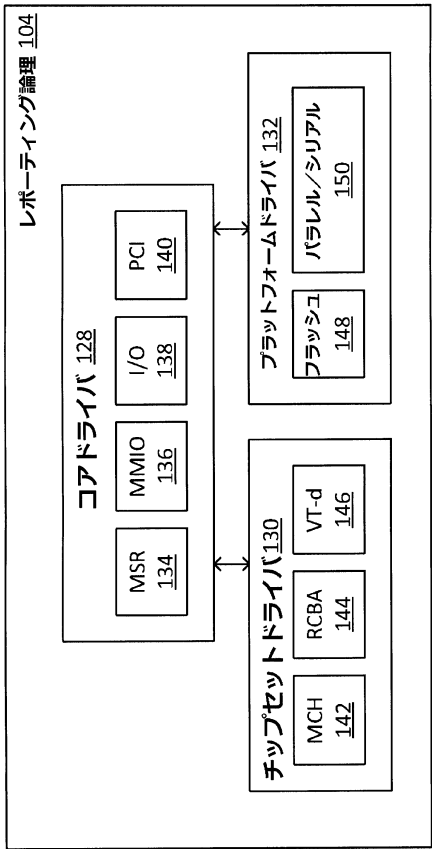
【図 2】



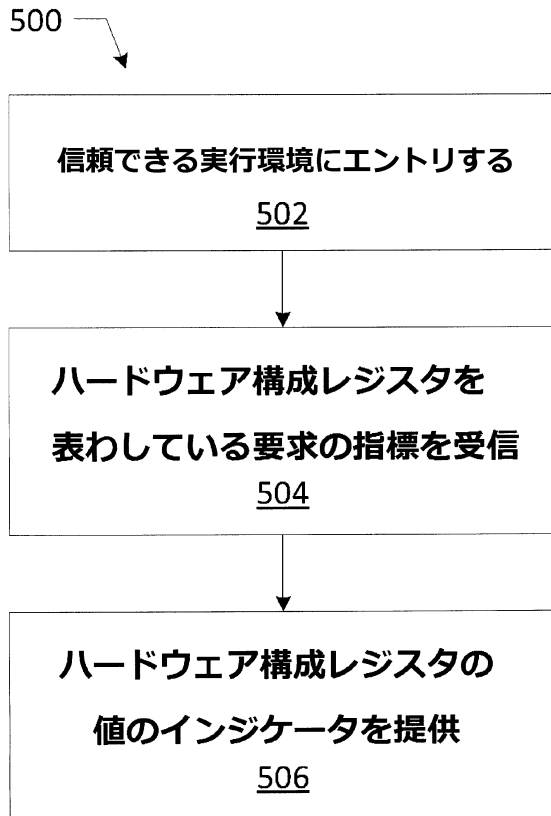
【図 3】



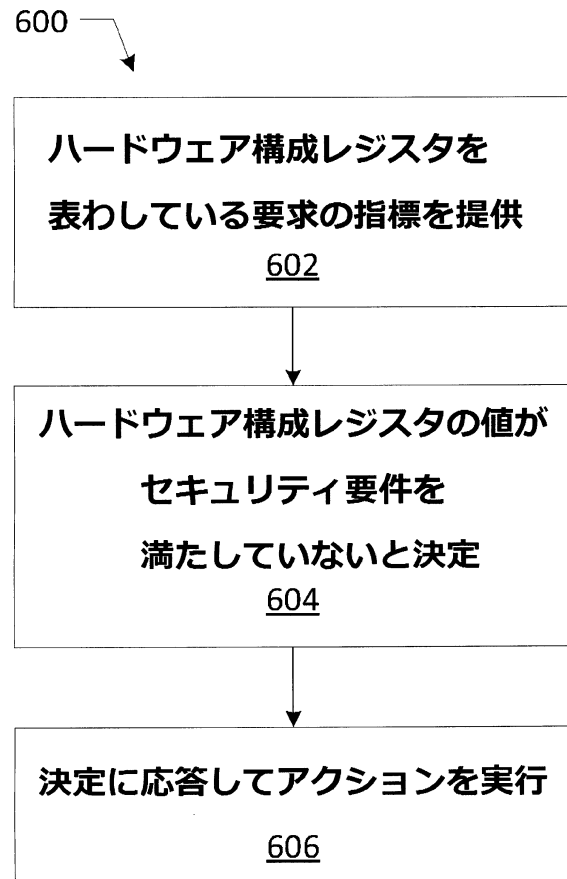
【図 4】



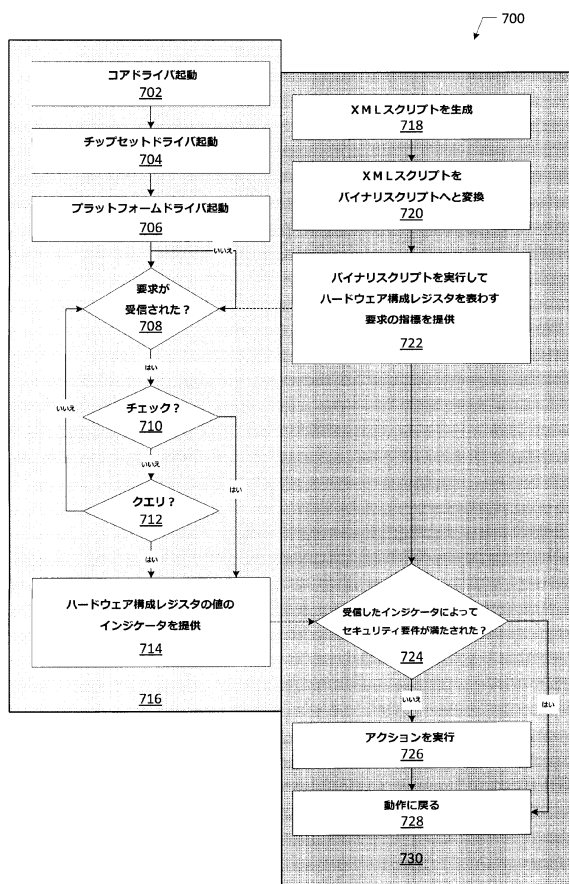
【図 5】



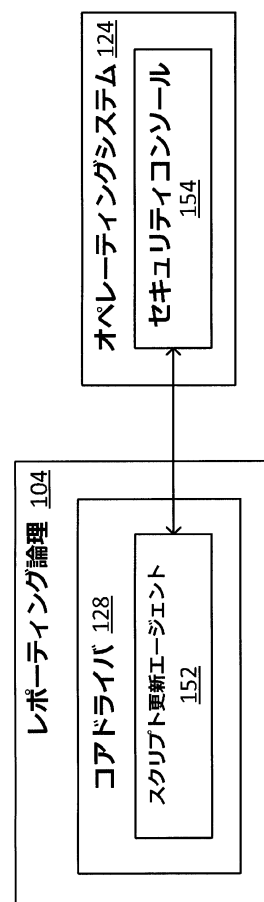
【図 6】



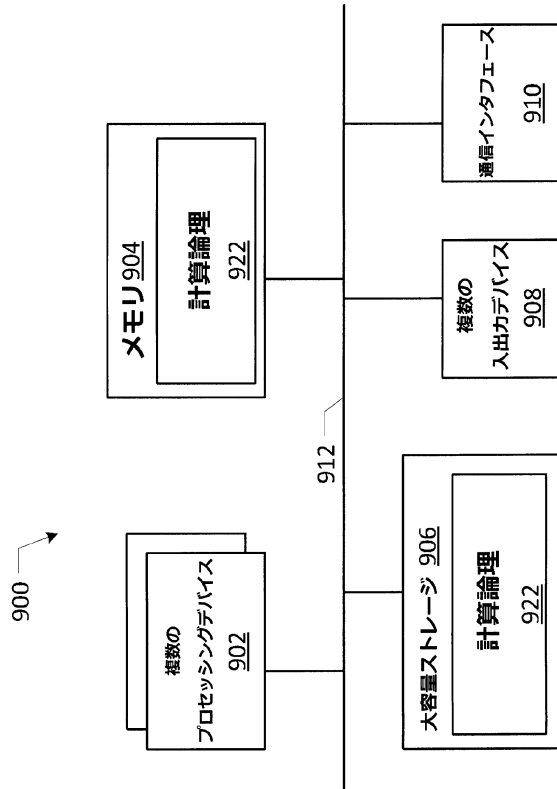
【図 7】



【図 8】



【図 9】



フロントページの続き

- (72)発明者 ジンマー、ヴィンセント ジェイ.
アメリカ合衆国 95054 カリフォルニア州・サンタクララ・ミッション カレッジ ブーレ
バード・2200 インテル・コーポレーション内
- (72)発明者 ペイネ、ブライアン エス.
アメリカ合衆国 95054 カリフォルニア州・サンタクララ・ミッション カレッジ ブーレ
バード・2200 インテル・コーポレーション内
- (72)発明者 アダムス、ニコラス ジェイ.
アメリカ合衆国 95054 カリフォルニア州・サンタクララ・ミッション カレッジ ブーレ
バード・2200 インテル・コーポレーション内

審査官 木村 貴俊

- (56)参考文献 米国特許出願公開第2013/0333005 (US, A1)
特表2011-511383 (JP, A)
特開2006-221633 (JP, A)
特表2014-524091 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
G06F 8/00- 8/38、 8/60- 8/77
9/44- 9/445、 9/451
11/07、11/22-11/36、12/14
21/00-21/88