(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4775744号
(P4775744)
(45)発行日　平成23年9月21日(2011.9.21)　(24)登録日　平成23年7月8日(2011.7.8)

(51)Int.Cl.　　F I
G06F 21/22 (2006.01)　　G06F 9/06 660Z
G06F 21/24 (2006.01)　　G06F 12/14 560C
G06F 12/14 (2006.01)　　G06F 12/14 510D

請求項の数 29　外国語出願　(全 24 頁)

(21)出願番号　特願2007-273185 (P2007-273185)
(22)出願日　平成19年10月19日 (2007.10.19)
(65)公開番号　特開2009-104258 (P2009-104258A)
(43)公開日　平成21年5月14日 (2009.5.14)
審査請求日　平成19年10月19日 (2007.10.19)

(73)特許権者　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５２　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
(74)代理人　100104156
弁理士　龍華　明裕
(72)発明者　ジマー、ヴィンセント
アメリカ合衆国、９８００３　ワシントン州、フェデラル　ウェイ、サウス　３６９ス　ストリート　１９３７
(72)発明者　クール、ライル
アメリカ合衆国、９７００５　オレゴン州、ビーバートン、エスダブリュー　イーエルエム　アベニュー　５３００
最終頁に続く

(54)【発明の名称】信頼できる共存環境をラウンチする方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
処理システム上に複数のランタイム環境をラウンチする方法であって、
前記処理システムがパーティションマネジャを実行して、所定のインテグリティメトリクスに基づいて第１のランタイム環境の保護コンテンツへのアクセスを管理する前記第１のランタイム環境をプレＯＳ空間に設定する工程と、
前記処理システムの信用検証モジュールが、前記第１のランタイム環境の信頼できるインテグリティメトリクスに対して前記第１のランタイム環境の現在のインテグリティメトリクスを検証する工程と、
前記処理システム上で実行される前記第１のランタイム環境が、前記検証に応答して前記第１のランタイム環境の前記保護コンテンツを復号化する工程と、
前記処理システムが、前記第１のランタイム環境の前記現在のインテグリティメトリクスの前記検証後に、第２のランタイム環境をプレＯＳ空間にラウンチする工程と、
を含み、
前記信用検証モジュールによる前記第２のランタイム環境の現在のインテグリティメトリクスの検証後、前記第２のランタイム環境は前記処理システム上に前記第１のランタイム環境と共存する、方法。
【請求項２】
前記第１のランタイム環境を設定する工程は、
前記第１のランタイム環境にリソースを割り当てる工程と、

前記第１のランタイム環境に割り当てられた前記リソースを隠す工程と、
を含む請求項１に記載の方法。
【請求項３】
前記第１のランタイム環境を設定する工程は、前記第１のランタイム環境への信頼できる通信路を確立する工程を含む請求項１または２に記載の方法。
【請求項４】
前記第１のランタイム環境の信頼できるインテグリティメトリクスに対して前記第１のランタイム環境の現在のインテグリティメトリクスを検証する工程は、
前記第１のランタイム環境の前記現在のインテグリティメトリクスを計測する工程と、
前記信頼できるインテグリティメトリクスに対して前記現在のインテグリティメトリクスを比較するよう信頼できるプラットフォームモジュールのプラットフォーム設定レジスタ７（ＰＣＲ７）内に前記現在のインテグリティメトリクスを与える工程と、
を含む請求項１から３のいずれか１項に記載の方法。
【請求項５】
前記保護コンテンツを復号化する工程は、
鍵を復号化する工程と、
前記鍵を介して前記保護コンテンツを復号化する工程と、
を含む請求項１から４のいずれか１項に記載の方法。
【請求項６】
前記第２のランタイム環境をラウンチする工程は、
前記第２のランタイム環境を設定する工程と、
前記第２のランタイム環境の信頼できるインテグリティメトリクスに対して前記第２のランタイム環境の前記現在のインテグリティメトリクスを検証する工程と、
前記第２のランタイム環境の前記現在のインテグリティメトリクスの前記検証に応答して前記第２のランタイム環境の複数の保護要素を復号化する工程と、
を含む請求項１から５のいずれか１項に記載の方法。
【請求項７】
前記第２のランタイム環境をラウンチする工程は、前記第２のランタイム環境のオペレーティングシステムに前記処理システムのリソースの制御を引き渡す工程を含む請求項１から６のいずれか１項に記載の方法。
【請求項８】
前記第２のランタイム環境をラウンチする工程は、
前記第１のランタイム環境と共存するよう前記第２のランタイム環境を設定する工程と、
前記第２のランタイム環境を計測する工程と、
信頼できるプラットフォームモジュールのＰＣＲ４内に前記第２のランタイム環境のハッシュを与える工程と、
を含む請求項１から７のいずれか１項に記載の方法。
【請求項９】
前記第２のランタイム環境をラウンチする工程は、
前記第１のランタイム環境と共存するよう前記第２のランタイム環境を設定する工程と、
前記第２のランタイム環境を計測する工程と、
ＰＣＲ７内に前記第２のランタイム環境のハッシュを与える工程と、
を含む請求項１から７のいずれか１項に記載の方法。
【請求項１０】
２つ以上のランタイム環境をラウンチするよう処理システムを初期化する方法であって、
前記処理システムが、承認環境のアクティブ化を受ける工程と、
前記処理システムがパーティションマネジャを実行して、第１のランタイム環境の信頼

できるバージョンをプレＯＳ空間にラウンチする工程と、
前記処理システムの信頼できるプラットフォームモジュールが、前記第１のランタイム環境の前記信頼できるバージョンの信頼できるインテグリティメトリクスを計測する工程と、
前記信頼できるプラットフォームモジュールが、信頼できるプラットフォームモジュールの第１のプラットフォーム設定レジスタ内に前記信頼できるインテグリティメトリクスを使用して第１の鍵を封印する工程と、
前記信頼できるプラットフォームモジュールが、前記信頼できるプラットフォームモジュールのもう１つのプラットフォーム設定レジスタ内に第２のランタイム環境のプレＯＳ空間にインテグリティメトリクスを使用して第２の鍵を封印する工程と、
を含み、
前記信頼できるバージョンの信頼性は、前記承認環境のアクティベーションに基づく、方法。
【請求項１１】
前記信頼できるプラットフォームモジュールが、１つ以上の追加のランタイム環境について前記第１のプラットフォーム設定レジスタ内に１つ以上の追加鍵を封印する工程をさらに含み、
前記第１のプラットフォーム設定レジスタのコンテンツに関する制御は、前記処理システムに関連付けられる製造業者用に設計される請求項１０に記載の方法。
【請求項１２】
前記承認環境をアクティブにする工程は、前記処理システムのボード上の複数の接点を接続する工程を含む請求項１０または１１に記載の方法。
【請求項１３】
前記第１の鍵を封印する工程は、前記第１のランタイム環境の前記信頼できるバージョンのハッシュを使用して前記第１の鍵を暗号化する工程を含む請求項１０から１２のいずれか１項に記載の方法。
【請求項１４】
前記第１の鍵を封印する工程は、プラットフォーム設定レジスタ７（ＰＣＲ７）内に前記第１のランタイム環境の前記信頼できるバージョンの前記ハッシュを与える工程を含む請求項１３に記載の方法。
【請求項１５】
前記第２の鍵を封印する工程は、プラットフォーム設定レジスタ４（ＰＣＲ４）内に前記第２のランタイム環境の前記信頼できるバージョンの前記ハッシュを与える工程を含む請求項１３または１４に記載の方法。
【請求項１６】
前記信頼できるバージョンをラウンチする工程は、前記第１のランタイム環境に割り当てられたリソースに対し、ハードウェアにより実行される分離スキームを実施する工程を含む請求項１０から１５のいずれか１項に記載の方法。
【請求項１７】
複数の信頼できる共存環境をラウンチするシステムであって、
少なくとも第１のランタイム環境のプレＯＳ空間と第２のランタイム環境のプレＯＳ空間のための複数のパーティションをサポートし、第１の保護領域および第２の保護領域を有するデータストレージを含むリソースと、
第１のレジスタおよび第２のレジスタを含み、第１のランタイム環境の計測値の検証に応答して第１の鍵を開封し、また、第２のランタイム環境の計測値の検証に応答して第２の鍵を開封する信用検証モジュールと、
前記第１の鍵を使用して前記第１の保護領域におけるデータを復号化するよう前記第１のレジスタ内への前記第１のランタイム環境の前記計測値の付与をリクエストし、前記第２の鍵を使用して前記第２の保護領域におけるデータを復号化するよう前記第２のレジスタ内への前記第２のランタイム環境の前記計測値の付与をリクエストするパーティション

マネジャと、
を含むシステム。
【請求項１８】
前記データストレージは、ハードディスクのホスト保護されたアクセス（ＨＰＡ）領域を含む請求項１７に記載のシステム。
【請求項１９】
前記信用検証モジュールは、複数のプラットフォーム設定レジスタを有する信頼できるプラットフォームモジュールを含み、
前記第１のレジスタは、プラットフォーム設定レジスタ７（ＰＣＲ７）を含む請求項１７または１８に記載のシステム。
【請求項２０】
前記第２のレジスタは、プラットフォーム設定レジスタ４（ＰＣＲ４）を含む請求項１９に記載のシステム。
【請求項２１】
前記パーティションマネジャは、ファームウェアを含む請求項１７から２０のいずれか１項に記載のシステム。
【請求項２２】
前記パーティションマネジャは、前記システムにおけるプロセッサのマイクロコードを含む請求項１７から２１のいずれか１項に記載のシステム。
【請求項２３】
前記パーティションマネジャは、前記第２のランタイム環境内のオペレーティングシステムに残りのリソースの制御を引き渡しする前に、前記第１のランタイム環境および１つ以上の追加の共存環境をラウンチする論理を含む請求項１７から２２のいずれか１項に記載のシステム。
【請求項２４】
複数のオペレーションを含む処理システムを実行させるプログラムであって、
前記処理システムがパーティションマネジャを実行し、前記処理システム上に、第１のランタイム環境の保護コンテンツへのアクセスを管理する前記第１のランタイム環境をプレＯＳ空間に設定することと、
前記処理システムの信用検証モジュールが、前記第１のランタイム環境の現在のインテグリティメトリクスを計測することと、
前記信用検証モジュールが、前記第１のランタイム環境の前記現在のインテグリティメトリクスの検証後、第１の鍵へのアクセスのために、前記第１のランタイム環境の信頼できるインテグリティメトリクスに対して前記第１のランタイム環境の前記現在のインテグリティメトリクスを比較するよう第１のレジスタ内に前記第１のランタイム環境の前記現在のインテグリティメトリクスを与えることと、
前記処理システム上で実行される前記第１のランタイム環境が、前記第１の鍵を介して前記第１のランタイム環境の前記保護コンテンツを復号化することと、
前記処理システムが、前記第１のランタイム環境の前記現在のインテグリティメトリクスの前記検証後に第２のランタイム環境をプレＯＳ空間にラウンチすることと、
を含み、
前記信用検証モジュールによる前記第２のランタイム環境の現在のインテグリティメトリクスの検証後、前記第２のランタイム環境は前記処理システム上に前記第１のランタイム環境と共存する、プログラム。
【請求項２５】
前記複数のオペレーションは、１つ以上の追加のランタイム環境の現在のインテグリティメトリクスを与えた後、１つ以上の追加のランタイム環境の１つ以上の追加の鍵を受信することをさらに含む請求項２４に記載のプログラム。
【請求項２６】
前記第１のランタイム環境を設定することは、前記第１のランタイム環境に割り当てら

れたリソースを隠すことを含む請求項２４または２５に記載のプログラム。
【請求項２７】
前記第１のランタイム環境の前記現在のインテグリティメトリクスを与えることは、信頼できるプラットフォームモジュールのプラットフォーム設定レジスタ７（ＰＣＲ７）内に前記現在のインテグリティマトリクスを与えることを含む請求項２４から２６のいずれか１項に記載のプログラム。
【請求項２８】
前記第２のランタイム環境をラウンチすることは、
前記第１のランタイム環境と共存するよう前記第２のランタイム環境を設定することと、
前記第２のランタイム環境を計測することと、
信頼できるプラットフォームモジュールのＰＣＲ４内に前記第２のランタイム環境のハッシュを与えることと、
を含む請求項２４から２７のいずれか１項に記載のプログラム。
【請求項２９】
前記第２のランタイム環境をラウンチすることは、
前記第１のランタイム環境と共存するよう前記第２のランタイム環境を設定することと、
前記第２のランタイム環境を計測することと、
ＰＣＲ７内に前記第２のランタイム環境のハッシュを与えることと、
を含む請求項２４から２７のいずれか１項に記載のプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータセキュリティの分野に関する。より具体的には、本発明は、２つ以上の信頼できる、別個の共存環境をラウンチする方法および装置に関する。
【背景技術】
【０００２】
コンピュータ上に保存されるデータは、金銭的な意味合いにおいて、および／または競争するまたはビジネスを行う能力に関連して高い価値を有しうる。データは、復号化コードおよび秘密処理といった業務上の秘密、および社会保障番号およびクレジットカード番号といったその他の機密ビジネスデータまたは個人情報を含みうる。本質的に異なる処理システムにおいてこのようなデータのセキュリティを高めることを目的として、非営利の業界規格組織であるトラステッドコンピューティンググループ（ＴＣＧ）は、より安全なコンピューティング環境のための仕様を作成および採用した。ＴＣＧ仕様は、たとえば、ＴＣＧトラステッドプラットフォームモジュール（ＴＰＭ）仕様バージョン１．２リビジョン９４、パートＩデザイン原理（２００６年３月２９日）、およびＴＣＧ主仕様バージョン１．１ｂ（ＴＣＧ主仕様バージョン１．１ｂの日付）を含む。
【０００３】
ＴＣＧ仕様は、信頼できる処理システム、またはプラットフォームを、一般的に、特定目的のために特定の方法で挙動する処理システムとして定義する。信頼できる処理システムは、データ暗号化、復号化、および保存といったデータセキュリティ機能を供給しうる。信頼できる処理システムの重要な構成要素はＴＰＭであり、これは、インテグリティの喪失を検出するための暗号化ハッシング、非認可のデータ開示を防止するための公開および秘密鍵暗号化、および伝送情報を認証するためのデジタル署名を行いうるモジュールである。ハードウェア内にルートされうるＴＣＧ保護ストレージメカニズムは、鍵、秘密、およびハッシュ値を保護しうる。
【０００４】
信頼できる処理システムのインテグリティのメトリクスは、処理システムが、機密データへのアクセスを有する場合に、安全または「信頼できる」ハードウェアおよびソフトウ

ェア設定で動作するか否かに関する判断を容易にする。インテグリティメトリクスは、製造時、および機密データをその設定に封印する時点といった設定が信頼できる時点における処理システムのランタイム設定を計測することによって確立しうる。さらに、信頼性の計測および証明は、認証されたまたは信頼できるコードを使用してハードウェアにおいて実施される。プロセッサ、チップセット、およびＴＰＭといったハードウェアは、特定のトランザクションは認証コードによってのみ開始され、また、インテグリティメトリクスの計測によってそのコードが改ざんされていないまたは侵害されていないことを検証（verify）しうることを保証する機能を含みうる。信頼性は、一般的に、ＯＳをブートする前にデータおよびコードの保護コアを確立することによって処理システムのブートまたはリセット時に確立される。処理システムの電源が落とされるまたはリセットされる度に、保護コアは、処理システムの電源が落とされるまたはリセットされるときにコードを変更することによって保護データを侵害する攻撃者の能力を最小限にするよう再初期化または認証される。ＯＳをブートする前に保護コアを確立することも、セキュリティプロトコルを改ざんする攻撃者の能力を最小限にするセキュリティ手段である。

【０００５】

一般的な処理システムにおいて、ファームウェアは、処理システムの電源オン／リセットと処理システム上のオペレーティングシステム（ＯＳ）のブートとの間のシステムのプレＯＳまたはプレブート、オペレーションを制御する機械命令を供給する。次にＯＳは、処理システムの主な機能を引き継ぐ。たとえば、一部のシステムでは、仮想マシンモニタ（ＶＭＭ）またはハイパーバイザコードは、中央演算処理ユニット（ＣＰＵ）、メモリ、ハードドライブ、および他のコンポーネントといったシステムのリソース全体の制御を行いうる。ＶＭＭは、仮想環境をラウンチおよび管理し、また、各仮想環境においてマイクロソフト（登録商標）Ｗｉｎｄｏｗｓ（登録商標）、Ｌｉｎｕｘ（登録商標）、Ｕｎｉｘ（登録商標）などの高レベルＯＳをラウンチすることができる。

【０００６】

ファームウェアはさらに、ＯＳがロードされた後に、特定のハードウェアイベントおよび／またはシステムインタラプトを処理するオペレーションといったポストブートオペレーションと呼ばれる特定のオペレーションを制御しうる。より具体的には、ファームウェアは、集合的に基本入力／出力システム（ＢＩＯＳ）と呼ばれるルーチンのセットによってプレブートおよびポストブートオペレーションを処理しうる。従って、ＢＩＯＳは、システムのハードウェアコンポーネントと、ＯＳといったソフトウェアコンポーネントとの間のインタフェースを供給する。ＢＩＯＳに代わる幾つかの新しい代替品には、拡張可能ファームウェアインタフェース（ＥＦＩ）仕様のバージョン１．１０（２００２年１２月１日）、および統合ＥＦＩ（ＵＦＥＩ）仕様のバージョン２．０（２００６年1月３１日）が含まれる。

【０００７】

保護コアを確立した後、ＢＩＯＳ、ＥＦＩ、またはＵＥＦＩといったファームウェアは、処理システムの現在のランタイム設定を計測し、現在のランタイム設定をＴＰＭ内にある信頼できる設定のランタイムと比較することができる。現在のランタイム設定のインテグリティが侵害またはそうでなければ変更されている場合、機密データへのアクセスは、拒否または無視されることができる。さらに、信頼できる処理システムは、アクセス時のランタイム設定が信頼できる設定のランタイムに十分に類似して信頼できる場合、機密データへのアクセスを許可しうる。

【０００８】

保護コアは、データおよびコードに対しハードウェアに基づいたセキュリティを提供するが、より強いセキュリティが求められている。ネットワークおよびインターネットを介して提供されるサービスが浸透することによって、不正ユーザやソフトウェアウィルスだけでなく互いからの処理の保護および実行がますます必要となってきている。換言すれば、処理システムにおける単一の保護コアまたはパーティションは不十分である。さらに、現在、処理システムにおけるプロセッサコアの数は多くなる傾向に動いているが、現在の

ＯＳソフトウェアは、８個のプロセッサコア以上に容易に拡張することができない。

【０００９】

現在のソリューションでは、ファームウェアにより管理される保護コアをラウンチし、次に、ＶＭＭを介して追加パーティションをラウンチおよび確保している。ＶＭＭは、論理レベルでのプラットフォームパーティショニングの制御を提供する低レベルＯＳである。ＶＭＭは、幾つかのプロセッサコアにわたっての多くのＯＳランタイムを利用することができ、これは、異なるパーティションでの幾つかのランタイム環境を提供する。しかし、ＶＭＭは、最大で８つのコアだけを処理することができ、追加パーティションのセキュリティは、ファームウェアではなく低レベルＯＳであるＶＭＭに依存する。ＶＭＭは、ファームウェアおよびたとえばＴＰＭではなく追加パーティションに対するソフトウェアロードを制御する。従って、機密データは、攻撃者がハードディスクを奪いＶＭＭにハッキングした場合、侵害されうる。

［先行技術文献］

［特許文献］

［特許文献１］韓国特許　第１００９８９９７７号
［特許文献２］米国特許出願公開　第２００３－００６１４９４号明細書
［特許文献３］米国特許出願公開　第２００５－２１０４６７号明細書
［特許文献４］米国特許出願公開　第２００５－０１３８３７０号明細書
［特許文献５］米国特許出願公開　第２００６－００２６４１８号明細書
［特許文献６］米国特許出願公開　第２００６－０２５６１０６号明細書
［特許文献７］米国特許出願公開　第２００７－００９４７１９号明細書
［特許文献８］米国特許出願公開　第２００７－０１６８９１３号明細書
［特許文献９］米国特許出願公開　第２００８－００７７９９３号明細書
［特許文献１０］米国特許　第７，２６６，８１０号
［特許文献１１］米国特許　第７，５４３，２８３号
［特許文献１２］米国特許　第７，７７４，５８８号

【００１０】

本発明の複数の面は、以下の詳細な説明を読み、同様の参照符号は同様の要素を示しうる添付図面を参照することにより明らかになろう。

【発明を実施するための最良の形態】

【００１１】

以下は、添付図面に示す本発明の実施形態の詳細な説明である。実施形態は、本発明を明白に伝えるよう詳細に示してある。しかし、提供する詳細の度合いは、予想される実施形態の変形を制限することを意図しておらず、むしろ、請求項に定義する本発明の精神および範囲内のすべての変形、等価物、および代替案を対象とすることを意図する。以下の詳細な説明は、当業者にそのような実施形態を明らかにすることを目的とする。

【００１２】

一般的に、２つ以上の信頼できる本質的に異なる共存環境をラウンチする方法および装置を検討している。実施形態は、２つ以上の信頼できる共存環境をプレＯＳ空間に高い確実さでラウンチしうる。各信頼できる環境またはパーティションは、コードおよびデータの保存および実行を容易にするようハードウェアにより実行される分離スキームを介して他の処理システムリソースから分離される指定ハードウェアリソースでありうる。多くの実施形態では、システムは、組み込みおよびメインパーティションを確立するためにパーティションマネジャをラウンチしうる。組み込みまたは隔離されたパーティションは、メインＯＳには可視ではなく、また、ホスト側で重要なオペレーション、Ｉ／Ｏオフローディング、ソフトの周辺装置、プラットフォーム管理容易性、および／またはエラー予測といった様々なアプリケーションに使用されうる。たとえば、組み込みパーティションは、プレミウムコンテンツダウンロードを検査しなければならない個人ビデオレコーダまたはセットトップボックスといった重要なオペレーションをホストするために、たとえば、ＥＦＩ、組み込みＬｉｎｕｘ（登録商標）、マイクロソフト（登録商標）Ｗｉｎｄｏｗｓ（

登録商標）コンパクトエディション（ＷｉｎＣＥ）、他のリアルタイムオペレーティングシステム（ＲＴＯＳ）などのランタイムを含みうる。組み込みパーティションのラウンチにおける信頼性は、ランタイム環境のインテグリティメトリクスを、その組み込みパーティションの信頼できるランタイム環境のインテグリティ計測値と比較することによって確立される。

【００１３】

信頼性の確立後、組み込みパーティションのコンテンツは開封され、追加の組み込みパーティションは、メインパーティションの起動の前にラウンチされうる。メインパーティションは、汎用ＯＳ（たとえば、様々なＷｉｎｄｏｗｓ（登録商標）ベースのＯＳ、Ｌｉｎｕｘ（登録商標）ベースのＯＳなどのうちの１つ）と、１つ以上のユーザアプリケーション（たとえば、ウェブサーバ、ビジネスアプリケーションなど）をホストしうる。信頼性は、たとえば、ファームウェアを介して認証コードを実行し、また、たとえば、トラステッドプラットフォームモジュール（ＴＰＭ）を介してオペレーション時に認証コードおよび信頼できるハードウェアを使用して重要なコマンドの信頼性を計測することによって、メインパーティションのラウンチにおいても確立されうる。

【００１４】

一部の実施形態では、組み込みパーティションおよびメインパーティションは、インタラクとしない場合がある。すなわち、組み込みパーティションにより実行されるオペレーションは、メインパーティションにおけるオペレーションとは無関係でありうる。たとえば、組み込みパーティションは、ネットワーク回路遮断器またはハードウェアファイアウォールといった「ハードウェアデバイス」のように動作しうる。

【００１５】

しかし、他の実施形態では、メインパーティションは、パーティション間ブリッジ（ＩＰＢ）といった通信路を介して組み込みパーティションと通信可能に結合されうる。ＩＰＢは、２つの信頼できるパーティションまたはサブシステムが、暗号化鍵といった期待されるセキュリティポリシーに従って通信することを可能にする信頼できる通信路でありうる。幾つかの実施形態では、ＩＰＢは、共有メモリバッファを含みうる。

【００１６】

幾つかの実施形態は、パーティションを設定するようパーティションマネジャを介してプラットフォームリソースレイヤ（ＰＲＬ）を実施し、プロセッサユニット、ランダムアクセスメモリ（ＲＡＭ）ユニット、周辺デバイス、集積デバイスなどといったリソースを他のパーティションから隠す。一部の実施形態では、パーティションマネジャは、たとえば、ＢＩＯＳ、ＥＦＩ、ＵＥＦＩ、または他のファームウェアにより生成される詳細設定および電源インタフェース（ＡＣＰＩ）表を変更することによってハードウェアにより実行される分離スキームに従ってリソースを隠しうる。更なる実施形態では、パーティションマネジャは、たとえば、デバイスハイドレジスタまたはシステムの入力／出力（Ｉ／Ｏ）コントローラハブ（ＩＣＨ）における他のロケーションを更新することによりＯＳからリソースを隠しうる。他の実施形態では、組み込みパーティションローダ（ＥＰローダ）コードがパーティションマネジャにより実行され、ＥＰローダコードは必要に応じてリソースを隠しうる。また、ＥＰローダコードの認証後、保護データを隠されたリソース内にロードする。

【００１７】

以下の詳細な説明の一部は、バス、ハードウェア、ソフトウェア、および他の論理に関して特定の設定およびプロトコルを参照して実施形態を説明するが、当業者は、実施形態は実質的に同じ機能を達成するために他の設定で、また、他のプロトコルに従って実施されうることを認識しよう。

【００１８】

図面を参照するに、図１は、ランタイム環境を有するソフトウェアレイヤ１１０と、様々なハードウェアリソースを有するハードウェアレイヤ１５０の形の処理システム１００の実施形態を示す。システム１００は、分散型コンピュータシステム、スーパーコンピュ

ータ、高性能コンピュータシステム、コンピュータクラスタ、メインフレームコンピュータ、ミニコンピュータ、クライアントーサーバシステム、パーソナルコンピュータ（ＰＣ）、ワークステーション、サーバ、ポータブルコンピュータ、ラップトップコンピュータ、タブレットコンピュータ、携帯情報端末（ＰＤＡ）といった手持ち式デバイス、または情報を処理または伝送するための他のデバイスといったコンピュータシステムである。同様の実施形態は、たとえば、ポータブル音楽プレイヤまたはポータブルビデオプレイヤといったエンターテインメントデバイス、スマートフォンまたは他のセルラ式電話機、電話機、デジタルビデオカメラ、デジタルスチルカメラ、外部ストレージデバイスなどとして実施されうる。更なる実施形態は、サーバシステムといった大規模のサーバ構成を実施する。

【００１９】

ソフトウェアレイヤ１１０に関して、システム１００は、パーティションマネジャ１８０または１５９を介して、組み込みパーティション１３８、１４０、および１４２といった１つ以上の信頼できる共存組み込みパーティションを確立しうる。パーティションマネジャ１８０または１５９は、システムブートまたはリセットに応答して、メインパーティション１１１内に仮想マシンモニタ（ＶＭＭ）１３６をラウンチする前に組み込みパーティションを確立しうる。

【００２０】

組み込みパーティション１３８、１４０、および１４２といった組み込みパーティションは、組み込みパーティションが使用しなければ使用されないまたはあまり効率よくなくＶＭＭ１３６により使用されうるプロセッサコアを使用しうる。たとえば、プロセッサコアの数が８を超える処理システムでは、ＶＭＭ１３６は、８つのコアがＶＭＭ１３６に対してメインパーティション１１１に割り当てられ、残りのコアは組み込みパーティションに割り当てられうるよう８を超えるコアを効率よく使用することができない場合がある。

【００２１】

多くの実施形態では、パーティションマネジャ１５９または１８０は、メインパーティション１１１から組み込みパーティション１３８、１４０、および１４２を隠しうる、または隔離しうる。特に、パーティションマネジャ１５９または１８０は、組み込みパーティション１３８、１４０、および１４２のハードウェアリソースを隠し、それにより、これらのリソースがＶＭＭ１３６によって発見できないようにしうる。

【００２２】

組み込みパーティション１３８、１４０、および１４２は、メインパーティション１１１から独立して動作しうるが、一部の実施形態は、１つ以上の組み込みパーティションとメインパーティション１１１との間に通信路を提供する。本実施形態では、組み込みパーティション１３８といった組み込みパーティションが、パーティション間ブリッジ（ＩＰＢ）１３９を介してメインパーティション１１１と通信可能に結合されうる。ＩＰＢ１３９は、セキュアされたまたはセキュアされない通信路でありえ、また、入力／出力（Ｉ／Ｏ）およびメモリコントローラハブといったハードウェアを介して実施されるか、または、共有メモリバッファ１７３でありうる。

【００２３】

組み込みパーティション１３８、１４０、および１４２といった組み込みパーティションは、様々な機能を実行しうる。たとえば、一部の実施形態では、組み込みパーティション１４２は隔離され、また、プレミウムコンテンツダウンロードを検査しなければならない個人ビデオレコーダまたはセットトップボックスといった重要なオペレーションをホストしうる。そのような実施形態では、組み込みパーティション１４２内で実行する保護コンテンツ１４４の処理は、そのプレミウムコンテンツを認可しうる。このような処理は、ホスト保護されたアクセス（ＨＰＡ）１８６のコンテンツを介して、または、ネットワークインタフェースカード（ＮＩＣ）１８２を介するリモートシステムとの安全な通信を介して内部でプレミウムコンテンツを認可しうる。

【００２４】

組み込みパーティション１４２は、組み込みパーティションに存在しうるソフトウェアレイヤのタイプの例を示す。具体的には、組み込みパーティション１４２は、保護コンテンツ１４４、組み込みシステム１４５、およびＥＰローダ１４６を含む。保護コンテンツ１４４は、組み込みパーティション１４２のランタイム環境のインテグリティメトリクスの検証後にＨＰＡ１８６から復号化されるコンテンツでありうる。組み込みパーティション１４２のランタイム環境は、組み込みパーティション１４２に関連付けられるハードウェア設定およびソフトウェア設定を含みうる。たとえば、組み込みパーティション１４２のランタイム環境は、ＥＰローダ１４６、および、組み込みパーティション１４２に排他的に割り当てられるプロセッサユニット（ＰＵ）１５７およびＥＰメモリ１７０といったハードウェアリソースを含みうる。一部の実施形態では、パーティションマネジャ１８０またはパーティションマネジャ１５９といったパーティションマネジャは、別個のＥＰローダ１４６が必要でないように組み込みシステム１４５をロードする。

【００２５】

ＥＰローダ１４６は、Ｉ／Ｏデバイス１８４から組み込みシステム１４５をロードし、組み込みシステム１４５に制御を引き渡ししうる。組み込みシステム１４５は、組み込みパーティション１４２内のオペレーションをホストする組み込みＬｉｎｕｘ（登録商標）、マイクロソフト（登録商標）Ｗｉｎｄｏｗｓ（登録商標）コンパクトエディション（ＷｉｎＣＥ）、他のリアルタイムオペレーティングシステム（ＲＴＯＳ）を含みうる。他の実施形態では、組み込みシステム１４５は、特定の機能を実行するよう設計される特殊ソフトウェアを含みうる。たとえば、組み込みシステム１４５は、グラフィクスアクセレレータカードをエミュレートするソフトウェアを含みうる。

【００２６】

組み込みシステム１４５は、組み込みパーティション１４２にロードされ、組み込みパーティション１４２により実行されるすべてのまたは実質的にすべてのサービスまたは機能を供給する命令のモノリシックパッケージから構成されうる。この開示の目的として、組み込みシステムは、従来のＯＳにより一般的に供給される種類のサービス（たとえば、タスクスケジューリング、エラー処理、Ｉ／Ｏサービスなど）、およびシステムファームウェアにより一般的に供給されるサービス（たとえば、ハードウェアコンポーネントの発見および初期化、これらのコンポーネントに対するソフトウェアインタフェースの提供など）を供給するソフトウェアである。組み込みシステムはさらに、ＯＳ上で実行されるプログラムまたはアプリケーションにより一般的に供給されるサービスも供給しうる。

【００２７】

組み込みシステム１４５がロードされると、ＥＰローダ１４６は、ＨＰＡ１８６または他の保護データストレージ内の保存されうる保護コンテンツ１４４へのアクセスをリクエストしうる。トラステッドプラットフォームモジュール（ＴＰＭ）１９０は、ＨＰＡ１８６内に保存される保護コンテンツ１４４にアクセスするための暗号化鍵を保持し、また、暗号化鍵を引き渡す前に組み込みパーティション１４２のランタイム環境のインテグリティメトリクスを検証しうる。ＴＰＭ１９０は、システム１００の各組み込みパーティションに対する暗号化鍵と、メインパーティション１１１内の保護コア１３０の確立に関連付けられる１つ以上の鍵を含みうる。

【００２８】

多くの実施形態では、ＴＰＭ１９０は、組み込みパーティション１４２のランタイム環境のインテグリティメトリクスを計測することによって組み込みパーティション１４２用の鍵のリクエストに対して応答しうる。一部の実施形態では、ＴＰＭ１９０は、システム１００のインテグリティメトリクスの追加の計測も行いうる。インテグリティメトリクスは、たとえば、組み込みパーティション１４２およびより一般的にはシステム１００のランタイム環境のイメージのハッシュを含みうる。組み込みパーティション１４２の計測されたまたは現在のインテグリティメトリクスは、プラットフォーム設定レジスタ７（ＰＣＲ７）内に与えられうる。ＰＣＲ７は、多くの実施形態に使用されうる。なぜならＰＣＲ７は、そのコンテンツは、製造制御または使用に設計されるレジスタだからである。ＴＰ

Ｍ１９０は、ＰＣＲ７のコンテンツを使用してインテグリティメトリクスをハッシングすることによって付与に応答しうる。

【００２９】

ＰＣＲ７は、組み込みパーティション１４２用のランタイム環境の信頼できるイメージのハッシュを含みうる。たとえば、ハードウェアレイヤ１５０は、製造業者により承認された環境（ＭＡＥ）であることを示しうる信号またはショートを識別するようＭＡＥ識別子１６２を含みうる。ＴＰＭ１９０は、製造業者により承認された環境の存在を認識し、また、ＰＣＲ７内への組み込みパーティション１４２のインテグリティメトリクスの付与に応答して鍵を開封するのではなく、ＴＰＭ１９０は、インテグリティメトリクスを使用して組み込みパーティション１４２の鍵を生成および封印しうる。一部の実施形態では、ＥＰローダ１４６は、その鍵または対応する非対称鍵を使用してＨＰＡ１８６内の保護コンテンツ１４４を暗号化しうる。

【００３０】

ＭＡＥ識別子１６２が、システム１００は製造業者により承認された環境であることを示さない場合、組み込みパーティション１４２のインテグリティメトリクスは、組み込みパーティション１４２のランタイム環境が信頼にたるか、または、そうでなければ認証されるべきかを決定するようＰＣＲ７のコンテンツを使用してハッシングされうる。組み込みパーティション１４２のランタイム環境のハッシュが環境のインテグリティを検証すると、ＴＰＭ１９０はＨＰＡ１８６内の保護コンテンツ１４４の鍵をＥＰローダ１４６に供給する。ＥＰローダ１４６は、次に、ＨＰＡ１８６内に保存されるデータおよび処理の一部または全部をＥＰメモリ１７０内にロードしうる。その一方で、ハッシュが、ランタイム環境は侵害されていることを示すと、ＴＰＭ１９０は、鍵を開封しない。さらに、パーティションマネジャ１５９または１８０は、組み込みパーティション１３８および１４０を実質的に同時に同様に、または、所定のシーケンスに従ってラウンチしうる。

【００３１】

メインパーティション１１１は、ＶＭＭ１３６といった信頼できるＯＳカーネルを有する保護されたコア１３０と、ＶＭ１１２および１１４といった１つ以上の仮想マシン（ＶＭ）をホストしうる。他の実施形態では、信頼できるＯＳカーネルは、ＯＳ１１８の信頼できる一部分でありえ、また、メインパーティション１１１内にはＯＳランタイム環境は１つしかない場合もある。

【００３２】

パーティションマネジャ１５９または１８０は、ＴＰＭ１９０を介してＶＭＭ１３６のコードを認証するか、または、ランタイム環境のインテグリティメトリクスを計測して、そのインテグリティメトリクスをＴＰＭ１９０内に保存される信頼できるインテグリティメトリクスと比較することによって、メインパーティション１１１の保護コア１３０のランタイム環境のラウンチにおいて信頼性を確立しうる。たとえば、メインパーティション１１１のハードウェア環境は、組み込みパーティションにリソースを割り当てした後に利用可能な残りのハードウェアリソースでありうる。パーティションマネジャ１５９または１８０は、ＴＰＭ１９０を介してＶＭＭ１３６を認証し、データ１３２および処理１３４を復号化するためにＴＰＭ１９０から鍵を受信しうる。データ１３２および処理１３４は、復号化されＭＰメモリ１７２内にロードされるまでＨＰＡ１８６内に存在しうる。

【００３３】

ＶＭＭ１３６は、論理レベルでのプラットフォームパーティショニングの制御を提供する低レベルＯＳである。具体的には、ＶＭＭ１３６は、ＶＭ１１２および１１４といった多数のＶＭを確立し管理しうる。ＶＭＭ１３６は、追加のパーティションに対するソフトウェアロードを制御する。多くの実施形態では、ＶＭＭ１３６は、仮想ＴＰＭを介してコードおよびランタイム環境を認証することによりＶＭにおけるセキュリティを提供しうる。仮想ＴＰＭは、データ１３２および処理１３４として保護コア１３０内に存在しうる。一部の実施形態では、組み込みパーティション１４０といった１つ以上の組み込みパーティションは、１つ以上のＶＭを有するＶＭＭをホストしうる。そのような実施形態では、

組み込みパーティション１４０は、システム１００内において共存するメインパーティション１１１からは別個の信頼できる処理システムのようにみえうるが、ハードウェアに基づいた分離スキームによってメインパーティション１１１からは分離される。このような実施形態は、ＯＳ１１８といった汎用ＯＳが容易に拡張できる処理コア数より多くの処理コア数を効率よく使用しうる。

【００３４】

ＶＭ１１４を設定後、ＶＭＭ１３６は、基本入力－出力システム（ＢＩＯＳ）１２０をロードしうる。ＶＭＭ１３６は、ＶＭ１１４のインテグリティを検証し、ソフトウェアローディングに関する制御をＢＩＯＳ１２０に渡しうる。ＢＩＯＳ１２０は、ＯＳ１１８をラウンチしうる。各ＶＭは、幾つかのコア１５８にわたってのＯＳランタイムを使用することができ、これは、異なるパーティションにおける幾つかのランタイム環境を提供する。たとえば、ＶＭ１１４は、汎用ＯＳ１１８（たとえば、Ｗｉｎｄｏｗｓ（登録商標）ベースのＯＳ、Ｌｉｎｕｘ（登録商標）ベースのＯＳなどのうちの１つ）と、１つ以上のユーザアプリケーション１１６（たとえば、ウェブサーバ、ビジネスアプリケーションなど）をホストしうる。ＶＭ１１２は、同様のソフトウェアをホストしうる。

【００３５】

ハードウェアレイヤ１５０は、プロセッサ１５２と、ランダムアクセスメモリ（ＲＡＭ）１６４、読み出し専用メモリ（ＲＯＭ）１７４、ネットワークインタフェースカード（ＮＩＣ）１８２、入力／出力（Ｉ／Ｏ）デバイス１８４、およびＴＰＭ１９０に結合されるコントローラハブ１６０を含む。プロセッサ１５２は、インテル（登録商標）のＰｅｎｔｉｕｍ（登録商標）プロセッサ、Ｘｅｏｎ（登録商標）プロセッサ、Ｉｔａｎｉｕｍ（登録商標）プロセッサ、Ｃｅｌｅｒｏｎ（登録商標）プロセッサなどのシステム用の１つ以上のプロセッサを表しうる。本実施形態では、プロセッサ１５２は、処理ユニット（ＰＵ）１５４、処理ユニット１５６、および処理ユニット１５７といった複数の処理ユニットを含む。処理ユニット１５４、１５６、および１５７は、組み込みパーティション１３８、１４０、および１４２への物理的または論理的な処理能力の割り当てである。一部の実施形態では、たとえば、処理ユニット１５４は、組み込みパーティション１３８により使用される専用の１つ以上のコアを表しうる。処理ユニット１５６は、ハイパースレッドといった論理ユニットを表しうる。メインパーティション１１１は一般的に、コアが組み込みパーティション１３８、１４０、および１４２に対して隠されないまたは隔離されない範囲でコア１５８を管理しうる。

【００３６】

コア１５８は、パーティションマネジャ１５９をマイクロコードとして含みうる。なお、多くの実施形態は、パーティションマネジャ１８０といったシステム１００のファームウェア１７６におけるパーティションマネジャか、または、パーティションマネジャ１５９といったプロセッサのマイクロコードにおけるパーティションマネジャのいずれかを含む。一方で、一部の実施形態は両方を含みうる。パーティションマネジャ１８０の使用は、計測の信頼性の静的ルート（Static Root of Trust for Measurement：ＳＲＴＭ）としばしば呼ばれ、パーティションマネジャ１５９の使用は、計測の信頼性の動的ルート（Dynamic Root of Trust for Measurement：ＤＲＴＭ）としばしば呼ばれる。

【００３７】

ＳＲＴＭについて、コンピュータシステムまたはリブートにより開始される信頼の連鎖（a chain of trust）。システムのプロセッサ１５２は既知の状態にある。第１のコードが実行され、パーティションマネジャローダ１７８といった計測の信頼性のコアルート（Core Root of Trust for Measurement：ＣＲＴＭ）は、パーティションマネジャ１８０である実行されるべき次のコードを計測する。侵害されたまたは未知のコードの認識といったことにより信頼が失われた場合、システム１００は、システム１００内の信頼を再び得るためにリブートまたはリセットされうる。

【００３８】

その一方で、ＤＲＴＭは、プロセッサ１５２のコアを既知状態におくために新しいプロ

セッサ命令を使用する。実行されるコードは、特殊プラットフォーム設定レジスタ（ＰＣＲ）に適応されるべきＴＰＭに送信される。このレジスタは、ＤＲＴＭ初期化状態にある場合にだけ、また、プロセッサ１５２の１つ以上のコアだけによってアクセス可能である。最初の計測ＤＲＴＭコードは、ハードウェアにより保護される。さらに、ＤＲＴＭでは、信頼が失われた場合、システム１００は、リブートなしで信頼の連鎖を再スタートすることができる。

【００３９】

プロセッサ１５２は、バスおよびコントローラハブ１６０を介してＲＡＭ１６４、ＲＯＭ１７４、ＮＩＣ１８２、Ｉ／Ｏデバイス１８４、およびＴＰＭ１９０に通信可能に結合する。プロセッサ１５２は、１つ以上のビデオコントローラ、ＳＣＳＩコントローラ、ネットワークコントローラ、汎用シリアルバス（ＵＳＢ）コントローラ、Ｉ／Ｏポート、カメラなどの入力デバイスといったハードウェアレイヤ１５０の追加のコンポーネント（図示せず）とも通信可能に結合されうる。さらに、ハードウェアレイヤ１５０は、複数のシステムコンポーネントを通信可能に結合するための周辺コンポーネントインターコネクト（ＰＣＩ）ルートブリッジなどといった１つ以上のブリッジを含みうる。本願で使用するように「バス」という用語は、２つ以上のデバイスにより共有される径路、およびポイントツーポイント径路を含みうる。

【００４０】

コントローラハブ１６０は、インテル（登録商標）の９７５Ｘ　Ｅｘｐｒｅｓｓチップセット、８６５Ｐチップセット、８４５Ｇチップセット、８５５ＧＭチップセット、Ｅ７５２５チップセット、Ｅ８８７０チップセット、８５２ＧＭＥチップセット、５３７ＥＰチップセット、８５４チップセットなどといったチップセットを表しうる。たとえば、コントローラハブ１６０は、メモリコントローラハブおよびＩ／Ｏコントローラハブを含みうる。

【００４１】

本実施形態では、コントローラハブ１６０は、隠しレジスタ１６１およびＭＡＥ識別子１６２を含む。隠しレジスタ１６１は、組み込みパーティションに対しハードウェアレイヤ１５０のハードウェアリソースを隠すよう使用されるレジスタを含みうる。たとえば、各組み込みパーティション用のランダムアクセスメモリ（ＥＰメモリ１６６、１６８、および１７０）は、隠しレジスタ１６１内に１ビットまたは他の指示子を保存することにより隠されうる。他の機能に使用されるＩＰＢ１７３およびハードウェアも隠されうる。たとえば、ＥＰメモリ１６６を隠すことは、組み込みパーティション１３８以外の任意のパーティションが、ＲＡＭ１６４のその部分の存在を認識することを阻止しうる。

【００４２】

一部の実施形態では、コントローラハブ１６０は、特定のデバイスに対して、これらのデバイスを隠すために設定サイクルを阻止する設定構成を使用しうる。更なる実施形態では、メインパーティション１１１用のＡＣＰＩパラメータが、ＯＳ１１８から処理ユニットおよびＲＡＭ１６４の１つ以上の部分を隠すよう使用されうる一方で、組み込みパーティション１３８、１４０、および１４２といった組み込みパーティション用のＡＣＰＩパラメータは、組み込みシステム１４５といった組み込みシステムから処理ユニットおよびＲＡＭ１６４の他の部分を隠すよう使用されうる。デバイス隠しレジスタおよび関連のトピックについての更なる詳細は、インテル（登録商標）のＩ／Ｏコントローラハブ６（ＩＣＨ６）ファミリーデータシート（２００４年1月（「ＩＣＨ６データシート」））から入手しうる。ＩＣＨ６データシートは、http://www.intel.com/design/chipset/datashts/301473.htmから入手しうる。ＡＣＰＩパラメータおよび関連のトピックについての更なる詳細は、詳細設定および電源インタフェース仕様のリビジョン３．０ａ（２００５年１２月３０日、（「ＡＣＰＩ仕様」））から入手しうる。ＡＣＰＩ仕様は、www.acpi.info/spec.htmから入手しうる。

【００４３】

代替実施形態では、１つ以上のコンポーネント内の他のデータストレージ構成を使用し

て、処理システムにおけるデバイスを無効にするまたは隠しうる。また、他の技術を使用して処理ユニット１５４、１５６、および１５７、およびＲＡＭ１６４の一部を隠しうる。

【００４４】

ＲＡＭ１６４は、アプリケーション、ドライバ、および他のコードといったアプリケーションに関連するデータおよび命令を保存することによってプロセッサ１５２による命令の実行をサポートするシステムメモリでありうる。ＲＡＭ１６４は、１つ以上のメモリモジュールから構成されうる。また、コントローラハブ１６０は、ＲＡＭ１６４の特定の領域にアドレスをマッピングする論理を有するメモリコントローラを含みうる。ＲＡＭ１６４は、ＥＰメモリ１６６、１６８、および１７０、ＭＰメモリ１７２、およびＩＰＢ１７３を含む。ＲＡＭ１６４はさらに、他の機能のために用意されるまたは専用のメモリを含みうる。

【００４５】

ＲＯＭ１７４は、ファームウェア１７６、および一部の実施形態では他の機能用の保護ストレージの１つ以上のメモリモジュールでありうる。ＲＯＭ１７４は、フラッシュメモリ、電気的に消去可能なプログラマブル読み出し専用メモリ（ＥＥＰＲＯＭ）、磁気ＲＡＭ（ＭＲＡＭ）、強誘電体ＲＡＭ（ＦｅＲＡＭ）などといったメモリまたはストレージを含みうる。ファームウェア１７６は、パーティションマネジャローダ１７８およびパーティションマネジャ１８０といったコードを保存しうる。パーティションマネジャローダ１７８は、パーティションマネジャ１８０のインテグリティをロードしおよび検証するようシステム１００のブートまたはリセット時に起動される信頼できるコアローダを含みうる。

【００４６】

ＴＰＭ１９０は、セキュアされた情報を保存できるマイクロコントローラでありうる。ＴＰＭ１９０は、ハードウェアデバイスまたはコードを認証するよう使用できるシステム１００のマザーボード上に組み込みされるチップを含みうる。ＴＰＭ１９０は、暗号化鍵の安全な生成のための設備、鍵の使用を（署名／検証または暗号化／復号化に）制限する能力、およびハードウェアに基づく乱数生成器を提供する。ＴＰＭ１９０の特徴は、リモート認証（remote attestation）、バインディング、および封印を含みうる。リモート認証は、プレミウムコンテンツプロバイダといった第三者がランタイム環境は侵害されていないことを検証することを可能にするよう実質的に偽造不可能なランタイム環境のサマリを作成するためのランタイム環境の計測を含みうる。封印は、ランタイム環境が復号化の時点において実質的に同じでない限りデータは復号化されないような方法でデータを暗号化しうる。バインディングは、製造時にチップ内に入れられる一意のＲＳＡ鍵でありうるＴＰＭエンドースメント鍵、または別の「信頼できる」鍵を使用してデータを暗号化しうる。ＲＳＡは、このアルゴリズムを公開したＲｏｎ　Ｒｉｖｅｓｔ、Ａｄｉ　Ｓｈａｍｉｒ、およびＬｅｎ　Ａｄｌｅｍａｎの姓を表す。

【００４７】

本実施形態では、ＴＰＭ１９０は、幾つかのプラットフォーム設定レジスタ（ＰＣＲ）を含む。説明目的のために２つのレジスタＰＣＲ４およびＰＣＲ７を有するＴＰＭ１９０を示す。他の実施形態では、ＴＰＭ１９０は、２つのレジスタだけを有しうる。更なる実施形態では、ＴＰＭは、ＴＰＭ１９０の外部にあるレジスタにアクセスしうる。

【００４８】

システム１００は、少なくとも部分的に、キーボード、マウスなどのポインティングデバイスといった従来の入力デバイスからの入力により制御されうる。入力デバイスは、たとえば、Ｉ／Ｏデバイス１８４を介してシステム１００と通信しうる。Ｉ／Ｏデバイス１８４は、外部Ｉ／Ｏデバイスとの通信のための１つ以上のポートでありえ、また、モデム、ドライブコントローラ、コンパクトディスクドライブ、ハードディスクドライブ、追加のマスストレージデバイスなどといったＩ／Ｏデバイスを含みうる。ストレージデバイスは、たとえば、集積ドライブ電子部品（ＩＤＥ）、小型コンピュータシステムインタフェ

ース（ＳＣＳＩ）、およびシリアル高度技術アーキテクチャ（ＳＡＴＡ）ハードドライブを含みうる。ストレージデバイスはさらに、フロッピー（登録商標）ディスク、光学ストレージ、テープ、フラッシュメモリ、メモリスティック、コンパクトフラッシュ（登録商標）（ＣＦ）カード、デジタルビデオディスク（ＤＶＤ）といった他のデバイスまたは媒体を含みうる。

【００４９】

システム１００は、他の処理システムまたは他の入力ソースまたは信号から受信したディレクティブまたは他のタイプの情報にも応答しうる。システム１００は、たとえば、ネットワークインタフェースコントローラ（ＮＩＣ）１８２、モデム、または他の通信ポートまたはカップリングを介して１つ以上の遠隔処理システムへの１つ以上の接続を使用しうる。システム１００は、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、イントラネット、インターネットなどといった物理および／または論理ネットワークを介して他のシステムに相互接続しうる。通信には、無線周波数（ＲＦ）、衛星、マイクロ波、電気電子技術者協会（ＩＥＥＥ）８０２．１１、８０２．１６、８０２．２０、ブルートゥース、光学、赤外線、ケーブル、レーザなどを含む様々な有線および／または無線短距離または長距離搬送波およびプロトコルを使用しうる。

【００５０】

たとえば、ＮＩＣ１８２といった一部のコンポーネントは、バスと通信するためのインタフェース（たとえば、ＰＣＩコネクタ）を有するアダプタカードとして実装されうる。或いは、ＮＩＣ１８２および他のデバイスは、プログラマブルまたは非プログラマブル論理デバイスまたはアレイ、特殊用途向け集積回路（ＡＳＩＣ）、組み込みプロセッサ、スマートカードなどといったコンポーネントを使用してオンボードまたは組み込みコントローラとして実装されうる。

【００５１】

本開示の目的として、「コード」という用語は、アプリケーション、ドライバ、処理、ルーチン、メソッド、モジュール、ファームウェア、マイクロコード、およびサブプログラムを含む広い範囲のソフトウェアコンポーネントおよび構成体を対象とする。したがって、「コード」という用語は、処理システムにより実行されると、所望の一のオペレーションまたは複数のオペレーションを実行する命令の任意の集まりを意味するよう使用されうる。たとえば、ＲＡＭ１６４、ＲＯＭ１７４、およびＩ／Ｏデバイス１８４は、実行されると、様々なオペレーションを実行する様々な命令セットを含みうる。このような命令セットは、一般的にソフトウェアまたはコードと称されうる。

【００５２】

図２は、メインランタイム環境においてＯＳをラウンチする前に保護コアを有するメインランタイム環境と共存する１つ以上の信頼できるランタイム環境をラウンチするシステム２００の実施形態を示す。システム２００は、パーティションマネジャ２１０、割り当て可能リソース２３０、および信頼検証モジュール２５０を含みうる。パーティションマネジャ２１０は、システム２００の計測のための信頼のコアルートを供給するよう設計されるコードおよび／またはステートマシーンといった論理を含みうる。具体的には、パーティションマネジャ２１０は、信頼検証モジュール２５０により認証されることのできる信頼にたるコードを含みうる。さらに、パーティションマネジャ２１０は、ランタイム環境および続けてラウンチされるコードのための信頼の連鎖のインテグリティを維持するために信頼することができる。

【００５３】

パーティションマネジャ２１０は、ラウンチ順序論理２１５および環境ランチャ２２０を含みうる。ラウンチ順序論理２１５は、組み込み環境２３２およびメイン環境２３４といったランタイム環境をラウンチするオペレーションの順序を定義するハードウェアおよび／またはソフトウェアといった論理を含みうる。環境ランチャ２２０は、環境にメモリユニットおよび処理ユニットといったハードウェアリソースを割り当てする論理と、ファームウェアまたはＯＳを環境内にロードするコードローダを含みうる。たとえば、ラウン

チ順序論理２１５は、割り当て可能リソース２３０を組み込み環境２３２に割り当てることによって組み込み環境２３２を設定するオペレーションを開始しうる。具体的に、ラウンチ順序論理２１５は、環境ランチャ２２０のリソースアサイナ２２２を起動して、メモリユニット、プロセッサユニット、および他のハードウェアリソースを組み込み環境２３２に割り当てうる。環境ランチャ２２０は、次に、ＯＳを組み込み環境２３２内にロードする、または、ＯＳを組み込み環境２３２内にロードするようファームウェアをロードしうる。多くの実施形態において、リソースハイダ２２４は、組み込み環境のハードウェアリソースを隠しうる。一部の実施形態では、リソースハイダ２２４は、ファームウェアまたはＯＳを組み込み環境２３２内にロードした後にリソースを隠しうる一方で、更なる実施形態では、リソースハイダ２２４は、ローディングと組み込み環境２３２の現在のインテグリティメトリクスを検証する前にリソースを隠しうる。リソースハイダ２２４は、たとえば、ＯＳの初期化の間にリソースを発見するＯＳの能力を阻止することによってなど、ハードウェアにおいて利用可能なスキームを介してリソースを隠しうる。

【００５４】

ファームウェアまたはＯＳを組み込み環境２３２内にロードした後、信頼検証モジュール２５０は、組み込み環境２３２のファームウェアまたはＯＳに保護ストレージ２６０からの鍵２６３を供給する前に、組み込み環境２３２の現在のインテグリティメトリクスをインテグリティメトリクス２６２に対して検証しうる。信頼検証モジュール２５０が、組み込み環境２３２の現在のインテグリティメトリクスを検証すると、組み込み環境２３２のファームウェアまたはＯＳは、鍵２６３を使用して組み込み環境２３２内で使用するための保護コンテンツ２４２を復号化しうる。一部の実施形態では、鍵２６３は、データおよび／または処理を暗号化し、保護コンテンツ２４２内に保存するのにも有用でありうる。他の実施形態では、組み込み環境２３２は、信頼検証モジュール２５０を介して保護コンテンツ２４２内のコンテンツを変更するかまたは保護コンテンツ２４２に対して新しいコンテンツを暗号化しうる。

【００５５】

幾つかの実施形態では、ラウンチ順序論理２１５は、組み込み環境２３２を設定またはラウンチしている間にメイン環境２３４のラウンチを少なくとも開始しうる。たとえば、ラウンチ順序論理２１５は、組み込みパーティション２３２の設定と実質的に同時にメイン環境２３４を設定しうる。更なる実施形態では、ラウンチ順序論理２１５は、組み込み環境２３２の現在のインテグリティメトリクスの検証後にメイン環境２３４の設定を開始しうる。幾つかの実施形態では、組み込み環境２３２といった１つ以上の組み込み環境は、メイン環境２３４におけるＯＳのラウンチの前に設定および／またはラウンチされうる。

【００５６】

ラウンチ順序論理２１５は、組み込み環境２３２のラウンチと同様の方法でメイン環境２３４のランチを開始しうる。たとえば、ラウンチ順序論理２１５は、環境ランチャ２２０に、メイン環境２３４のハードウェアリソースを設定し、次に、メイン環境２３４内で信頼の連鎖を開始できるよう認証されることのできるコードをロードするよう命令しうる。信頼の連鎖は、信頼できるＯＳカーネルおよび保護コンテンツ２４４からの信頼できる処理および／またはデータを含むメイン環境２３４内の保護コアを取り囲みうる。

【００５７】

保護コアを確立および隠した後、ＯＳは、保護コア以外のリソースにおいてメイン環境２３４内にラウンチされうる。たとえば、ＯＳは、汎用ＯＳでありうる。他の実施形態では、ＯＳは、デジタルビデオレコーダ（ＤＶＲ）の機械機能を制御するＯＳといった特殊用途向けＯＳでありうる。たとえば、ＤＶＲは、テレビ番組を記録するハードドライブと、プレミウムビデオコンテンツへのアクセスを容易にする機能を有する保護コアを含みうる。特殊用途向けＯＳは、デジタルビデオコンテンツを再生および記録するようユーザからの命令を受信および解釈する論理を含みうる一方で、保護コアにおけるＯＳカーネルは、プレミウムデジタルビデオコンテンツを購入および再生するよう特殊用途向けＯＳとイ

ンタラクとする機能を含みうる。このような実施形態において、組み込み環境２３２は、たとえば、プレミウムデジタルビデオコンテンツを、保護コアに対してダウンロードし、解釈し、また、ストリーミングする論理を含みうる。

【００５８】

割り当て可能なリソース２３０は、組み込み環境２３２およびメイン環境２３４といったランタイム環境に割り当てられうる論理的および／または物理的ハードウェアリソースを表しうる。割り当て可能なリソース２３０は、プロセッサコア、ＲＡＭ、ＲＯＭ、メモリコントローラハブ、Ｉ／Ｏコントローラハブ、バス、Ｉ／Ｏインタフェースなどを含みうる。

【００５９】

割り当て可能なリソース２３０は、組み込み環境２３２、メイン環境２３４、保護コンテンツ２４２、および保護コンテンツ２４４を含む。組み込み環境２３２は、組み込みランタイム環境を含むハードウェアおよびコードを表しうる。同様に、メイン環境２３４は、システム２００のメインパーティションを構成するハードウェアおよびコードを含みうる。保護コンテンツ２４２は、組み込み環境２３２の現在のインテグリティメトリクスの検証後に組み込み環境２３２により使用されるデータおよび／またはデータを含みうる。保護コンテンツ２４２は暗号化されており、また、鍵２６３を介して復号化されうる。保護コンテンツ２４４は、メイン環境２３４または少なくともメイン環境２３４の保護コアの現在のインテグリティメトリクスの検証後にメイン環境２３４により使用されるデータおよび／または処理を含みうる。保護コンテンツ２４４は暗号化されており、また、鍵２６５を介して復号化されうる。

【００６０】

信頼検証モジュール２５０は、鍵２６３および２６５といった鍵を引き渡す前に環境の現在のインテグリティメトリクスを検証するハードウェアおよび／またはソフトウェアといった論理を含む。鍵２６３および２６５といった鍵は、対応する環境が、たとえば、ハードディスク、ＲＡＭ、フラッシュメモリ、または他の不揮発性および揮発性メモリの保護データストレージ領域内に保存される、保護コンテンツ２４２および保護コンテンツ２４４といったデータおよび／または処理にアクセスすることを可能にする。一部の実施形態では、信頼検証モジュールは、図１に関連して説明したＴＰＭといったＴＰＭを含む。

【００６１】

信頼検証モジュール２５０は、インテグリティメトリクス計測器２５２、保護ストレージアクセサ２５４、保護ストレージ２６０、承認環境識別子２７０、および鍵生成器２７２を含む。インテグリティメトリクス計測器２５２は、組み込み環境２３２といったランタイム環境の現在のインテグリティメトリクスを計測し、そのインテグリティメトリクスを保護ストレージアクセサ２５４に渡しうる。インテグリティメトリクス計測器２５２は、実質的に一意な方法でランタイム環境を識別するランタイム環境のサマリを生成するようランタイム環境に関連付けられるソフトウェアおよびハードウェア割り当てといったインテグリティメトリクスを計測しうる。インテグリティメトリクスの計測処理は、環境へのウィルスまたはハードウェアの導入といったことによってランタイム環境のコードまたはハードウェア設定が変更する場合に、異なる計測値をもたらすよう設計される。一部の実施形態では、計測値は、異なるメモリの物理または論理ブロック、異なる通信路などの割り当てといった環境への重要ではない変更には対応する。

【００６２】

保護ストレージアクセサ２５４は、インテグリティメトリクス計測器２５２からインテグリティメトリクスを受信し、そのメトリクスを保護ストレージ２６０内のメトリクスに対して検証するか、または、そのメトリクスを保護ストレージ２６０内に保存しうる。たとえば、承認環境（ＡＥ）識別子２７０が、組み込み環境２３２といったランタイム環境は、信頼できるインテグリティメトリクス２６２を保存するための承認環境であることを示すと、鍵生成器２７２は、保護コンテンツ２４２を暗号化するための鍵２６３を生成し、保護ストレージアクセサ２５４の暗号化モジュール２５８は、インテグリティメトリク

ス２６２を使用して鍵２６３を暗号化しうる。保護ストレージアクセサ２５４は、次に鍵２６３を保護ストレージ２６０内に保存しうる。

【００６３】

その一方で、ＡＥ識別子２７０が、組み込み環境２３２を、信頼できるインテグリティメトリクス２６２を計測するための承認環境と示さない場合、保護ストレージアクセサ２５４の復号化モジュール２５６は、組み込み環境に鍵２６３を供給するか否かを判断するために、組み込み環境２３２の計測されたインテグリティメトリクスを、インテグリティメトリクス２６２と比較する。現在のインテグリティメトリクスが、インテグリティメトリクス２６２に一致しない場合、鍵２６３は、組み込み環境２３２に戻されない。

【００６４】

保護ストレージ２６０は、インテグリティメトリクスに対して封印される鍵を保存するレジスタまたは他のメモリを含みうる。多くの実施形態では、保護ストレージ２６０は、信頼検証モジュール２５０の外部にあるハードウェアにはアクセスできない。更なる実施形態では、保護ストレージ２６０へのアクセスは、保護ストレージアクセサ２５４を介するアクセスに実質的に制限される。

【００６５】

保護ストレージ２６０は、インテグリティメトリクス２６２および２６４により表されるレジスタを含みうる。多くの実施形態では、少なくとも１つのレジスタは、製造業者によって使用されるよう、および／または、ＯＳまたは他のそのようなソフトウェアによって使用されないよう設計される。

【００６６】

ＡＥ識別子２７０は、図１に関連して説明したＭＡＥといった承認環境を識別する論理を含みうる。承認環境は、ハードウェア、１つ以上の信号などの導入により作成されうる環境でありうる。多くの実施形態では、承認環境は、システム２００の製造時においてのみ実現されうる。他の実施形態では、承認環境は、製造後またはシステム２００のデプロイメント後に実現されうる。

【００６７】

鍵生成器２７２は、暗号化鍵を作成する生成器を含みうる。たとえば、鍵生成器２７２は、保護コンテンツ２４２および２４４のデータおよび処理を暗号化するよう４０ビット鍵、１２８ビット鍵、５１２ビット鍵などを生成しうる。鍵は、多くの現在の暗号化アプリケーションにおいて行われている公開鍵および秘密鍵といったように対称または非対称でありうる。

【００６８】

図３は、１つ以上の信頼できる共存パーティションをラウンチする一実施形態のフローチャート３００を示す。より具体的には、フローチャート３００は、信頼できる方法でパーティションにランタイム環境を設定し、図１に関連して説明したような処理システムといった処理システムのパーティションにおいてオペレーティングシステムをラウンチするためのプロセスを説明する。フローチャート３００は、組み込み環境の設定から開始する（工程３１０）。組み込み環境の設定には、ハードウェアリソースをパーティションに指定するまたは割り当てること、ファームウェアまたはソフトウェアをパーティションにロードすること、および、一部の実施形態では、パーティションに対してハードウェアリソースを隠すことが伴いうる。たとえば、組み込み環境の設定は、ＲＡＭの一部を物理的または論理的なユニットで組み込みシステムに割り当てすること、処理サイクルの一部を物理的または論理的なユニットで組み込みシステムに割り当てすること、通信のために幾つかの物理的および／または論理的ポートを指定すること、および他のリソースを組み込み環境に指定することを含みうる。

【００６９】

組み込み環境の設定後、ＴＰＭといった信頼検証モジュールは、組み込み環境の現在のインテグリティメトリクスを計測する（工程３１５）。組み込み環境の計測は、環境のサマリを作成するよう環境のソフトウェアおよびハードウェアリソースをハッシングするこ

とを含みうる。

【００７０】

現在のインテグリティメトリクスの計測後、信頼検証モジュールは、組み込み環境の現在のインテグリティメトリクスを、信頼検証モジュールのレジスタ内に与えうる（工程３２０）。現在のインテグリティメトリクスのレジスタ内への付与は、レジスタのコンテンツを使用して現在のインテグリティメトリクスをハッシングしうる。現在のインテグリティメトリクスが、組み込み環境の信頼できるインテグリティメトリクスと一致する場合（工程３２５）、信頼検証モジュールは、鍵を引き渡しし、組み込み環境は次に、組み込み環境内での使用のために保護コンテンツを復号化しうる（工程３３０）。

【００７１】

その一方で、現在のインテグリティメトリクスは、組み込み環境の信頼できるインテグリティメトリクスと一致しない場合（工程３２５）、信頼検証モジュールは、鍵を引き渡しせず、組み込み環境は、保護コンテンツを復号化することができない。本実施形態は、鍵へのリクエストは無視され、組み込み環境は、処理システムがリブートまたはリセットされるまで保護コンテンツをアクセスすることができない。他の実施形態では、組み込み環境は、再確立または再設定され、また、信頼できるインテグリティメトリクスに一致させるよう１回または可能ならば複数回の試みを行いうる。

【００７２】

本実施形態では、組み込み環境のインテグリティメトリクスが検証されると、または検証できないと、パーティションマネジャは、複数の組み込み環境がラウンチされる予定がある場合（工程３３５）に、工程３１０から処理を再開しうる。ラウンチが予定される組み込み環境がない場合は、パーティションマネジャは、メイン環境の設定を開始する（工程３４０）。他の実施形態では、複数の組み込み環境は、実質的に同時に設定および／またはラウンチされうる。更なる実施形態では、メインパーティションも実質的に同時に設定されうる。しかし、一部の実施形態では、メイン環境用のＯＳは、組み込み環境がラウンチされるまでラウンチされない場合もある。

【００７３】

メイン環境、または、少なくともメイン環境の保護コアが設定されると、ＴＰＭといった信頼検証モジュールは、メイン環境の現在のインテグリティメトリクスを計測しうる（工程３４５）。メイン環境の計測には、環境のサマリを作成するよう環境のソフトウェアおよびハードウェアリソースをハッシングすることが含まれうる。

【００７４】

現在のインテグリティメトリクスの計測後、信頼検証モジュール（ＴＶＭ）は、現在のインテグリティメトリクスをレジスタ内に与えうる（工程３５０）。現在のインテグリティメトリクスのレジスタ内への付与は、レジスタのコンテンツを使用して現在のインテグリティメトリクスをハッシングしうる。現在のインテグリティメトリクスが、メイン環境の信頼できるインテグリティメトリクスと一致する場合、信頼検証モジュールは、鍵を引き渡しし、メイン環境は次に、メイン環境の保護コア内での使用のために保護コンテンツを復号化し、メイン環境内にＯＳをラウンチしうる（工程３５５）。

【００７５】

図４は、１つ以上の信頼できる同時パーティションのラウンチを容易にする一実施形態のフローチャート４００を示す。フローチャート４００は、処理システム上で共存するために様々な環境に対して信頼できるインテグリティメトリクスを確立するよう処理システム上および／または処理システムによって実行されるオペレーションを説明しうる。フローチャート４００は、製造業者により承認される環境をアクティブにすることで開始する（工程４１０）。たとえば、製造業者承認環境をアクティブにすることは、処理システムのマザーボード上の２つ以上の接点を電気的に相互接続すること、マザーボード上の特定のポイントに特定の信号または信号パターンを導入すること、または他の処理を含みうる。

【００７６】

ＭＡＥをアクティブにした後、または、ＭＡＥの確立と実質的に同時に、処理システムは、第１のランタイム環境の信頼できるバージョンをラウンチしうる（工程４１５）。たとえば、コンパクトディスク（ＣＤ）を処理システムのドライブに挿入して、第１の環境を設定し、第１の環境用のソフトウェアのクリーンな信頼できるバージョンをインストールしうる。処理システムのＴＰＭは次に、第１の環境のインテグリティメトリクスを計測し（工程４２０）、第１の環境用の第１の鍵を生成しうる。第１の鍵の生成後、ＴＰＭは、ＰＣＲ７といったプラットフォーム設定レジスタ（ＰＣＲ）内に第１の環境のインテグリティメトリクスを使用して第１の鍵を封印しうる（工程４２５）。第１の環境のインテグリティメトリクスは、一部の実施形態ではＰＣＲ７内に保存されうる。なぜなら、ＰＣＲ７のコンテンツは、処理システム、または、少なくとも、プロセッサおよびチップセットといった処理システムの重要なコンポーネントの製造者の制御に実質的に任されているからである。

【００７７】

ＭＡＥをアクティブにした後、または、ＭＡＥの確立と実質的に同時に、処理システムは、第２のランタイム環境の信頼できるバージョンもラウンチしうる（工程４３０）。たとえば、コンパクトディスク（ＣＤ）がさらに第２の環境を設定し、第２の環境用のソフトウェアのクリーンな信頼できるバージョンをインストールしうる。処理システムのＴＰＭは次に、第２の環境のインテグリティメトリクスを計測し（工程４３５）、第２の環境用の第２の鍵を生成しうる。第２の鍵の生成後、ＴＰＭは、ＰＣＲ４といったプラットフォーム設定レジスタ（ＰＣＲ）内に第２の環境のインテグリティメトリクスを使用して第２の鍵を封印しうる（工程４４０）。

【００７８】

本発明の別の実施形態は、図１に示すシステム１００、または図２－４に説明する他の実施形態と関連して説明した処理といった処理を実行するようシステムとともに使用するプログラムプロダクトとして実施される。プログラムプロダクトのプログラムは、実施形態の機能（本願に説明する方法を含む）を定義し、しばしば、機械アクセス可能媒体と呼ばれる様々なデータおよび／または信号担持媒体上に含まれることができる。例示的なデータおよび／または信号担持媒体は、以下に限定されないが、（ｉ）書込み不可のストレージ媒体（たとえば、ＣＤ－ＲＯＭドライブにより読出し可能なＣＤ－ＲＯＭディスクといったコンピュータ内の読出し専用メモリデバイス）上に永久的に保存される情報、(ｉｉ)書込み可能なストレージ媒体（たとえば、汎用シリアルバス（ＵＳＢ）フラッシュドライブ、ハードディスクドライブ）上に保存される変更可能な情報、および（ｉｉｉ）ワイヤレス通信を含む、コンピュータまたは電話網を介するといった通信媒体によりコンピュータに伝達された情報を含む。後者の実施形態は特に、インターネットおよび他のネットワークからダウンロードされた情報を含む。このようなデータおよび／または信号担持媒体は、本発明の機能を導くコンピュータ可読命令を担持する場合、本発明の実施形態を表す。

【００７９】

一般的に、本発明の実施形態を実施するよう実行されるルーチンは、オペレーティングシステムの一部、または、特定のアプリケーション、コンポーネント、プログラム、モジュール、オブジェクト、または一連の命令でありうる。本発明のコンピュータプログラムは一般的に、コンピュータによって機械可読な形式、したがって、実行可能な命令に翻訳される複数の命令から構成される。さらにプログラムは、プログラムに対してローカルに存在するか、または、メモリ内またはストレージデバイス上に見つけられる変数およびデータ構造から構成される。また、本願に記載する様々なプログラムは、本発明の特定の実施形態においてそれらが実施されうるアプリケーションに基づいて識別されうる。以下に続く任意の特定のプログラム用語は便宜的に使用されているに過ぎず、したがって、本発明は、そのような用語により識別されるおよび／または示唆される任意の特定のアプリケーションにおける使用だけに限定されるべきではないことを理解すべきである。

【００８０】

この開示内容の利益を得た当業者には、本発明は処理システム上に複数の信頼できる共存ランタイム環境をラウンチするシステムおよび装置を検討することは明らかであろう。詳細な説明および図面に示し且つ説明した本発明の形は、単なる例であると解釈すべきであることを理解するものとする。請求項は、開示した実施形態のすべての変形を包含するよう広く解釈すべきであることを意図する。

【００８１】

本発明の一部の実施形態は、詳細に説明しているが、請求項により定義される本発明の精神および範囲から逸脱することなく様々な変更、代入、および修正できることを理解すべきである。本発明の実施形態は、複数の目的を達成しうるが、請求項の範囲内にある実施形態のすべてが、すべての目標を達成するとは限らない。さらに、本願の範囲は、明細書に説明する処理、機械、製造、合成物、手段、方法、および段階の特定の実施形態に限定されることを意図しない。当業者は本発明の開示内容から容易に理解できるように、本願に説明する対応実施形態と実質的に同じ機能を実行するまたは実質的に同じ結果を実現する現在存在するまたは後に開発される処理、機械、製造、合成物、手段、方法、または段階は、本発明にしたがって使用しうる。したがって、請求項はその範囲内に、そのような処理、機械、製造、合成物、手段、方法、または段階を含むことを意図する。

【図面の簡単な説明】

【００８２】

【図１】信頼できるメイン環境のラウンチの前に１つ以上の信頼できる組み込み環境をラウンチするよう１つ以上のプロセッサ、メモリ、ＴＰＭ、およびファームウェア／マイクロコードを有する他のハードウェアリソースを含むシステムを示す実施形態である。

【００８３】

【図２】保護コアを有するメインパーティション内でＯＳをラウンチする前に１つ以上の信頼できる組み込み環境をラウンチするシステムの一実施形態を示す。

【００８４】

【図３】１つ以上の信頼できる共存パーティションをラウンチするための実施形態のフローチャートを示す。

【００８５】

【図４】１つ以上の信頼できる同時のパーティションのラウンチを容易にする一実施形態のフローチャートを示す。

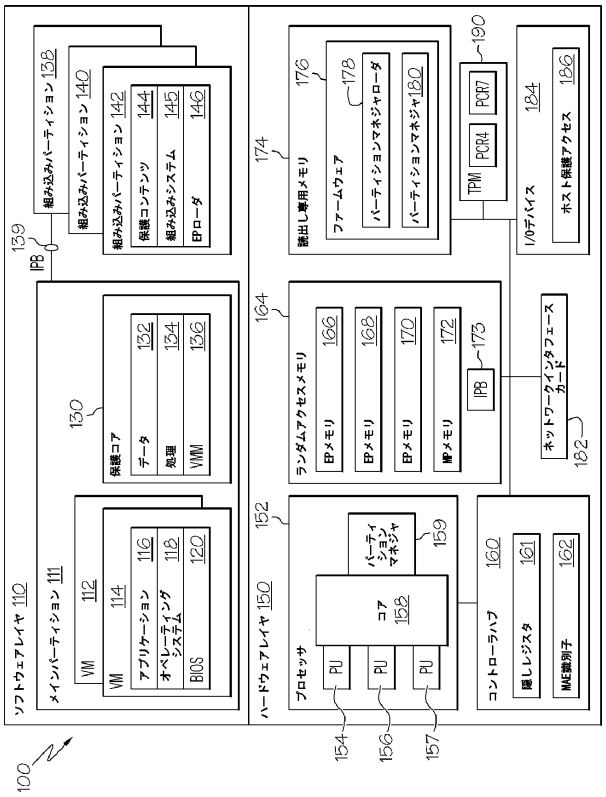
【符号の説明】

【００８６】

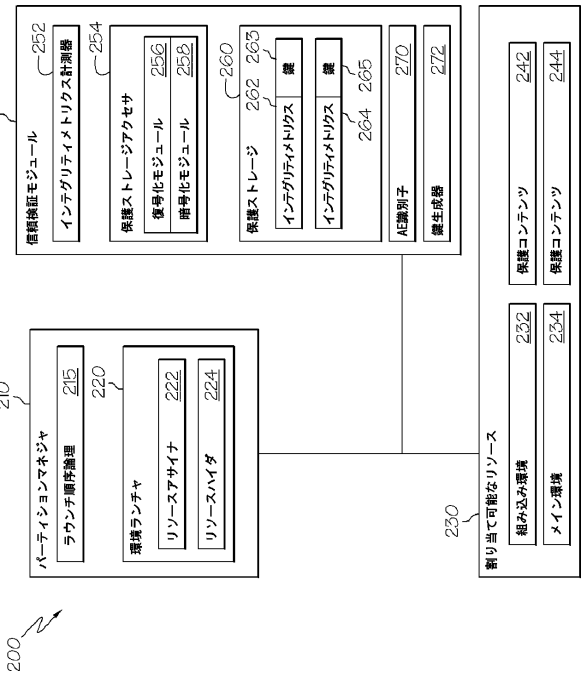
１００　処理システム
１１０　ソフトウェアレイヤ
１１１　メインパーティション
１１２、１１４　ＶＭ
１１６　アプリケーション
１１８　オペレーティングシステム
１２０　ＢＩＯＳ
１３０　保護コア
１３２　データ
１３４　処理
１３６　ＶＭＭ
１３８、１４０、１４２　組み込みパーティション
１３９　ＩＰＢ
１４４　保護コンテンツ
１４５　組み込みシステム
１４６　ＥＰローダ
１５０　ハードウェアレイヤ
１５２　プロセッサ

１５４、１５６、１５７　処理ユニット
１５８　コア
１５９　パーティションマネジャ
１６０　コントローラハブ
１６１　隠しレジスタ
１６２　ＭＡＥ識別子
１６４　ランダムアクセスメモリ
１６６、１６８、１７０　ＥＰメモリ
１７２　ＭＰメモリ
１７３　ＩＰＢ
１７４　読出し専用メモリ
１７６　ファームウェア
１７８　パーティションマネジャローダ
１８０　パーティションマネジャ
１８２　ネットワークインタフェースカード
１８４　Ｉ／Ｏデバイス
１８６　ホスト保護されたアクセス
１９０　ＴＰＭ
２００　システム
２１０　パーティションマネジャ
２１５　ラウンチ順序論理
２２０　環境ランチャ
２２２　リソースアサイナ
２２４　リソースハイダ
２３０　割り当て可能なリソース
２３２　組み込み環境
２３４　メイン環境
２４２、２４４　保護コンテンツ
２５０　信頼検証モジュール
２５２　インテグリティメトリクス計測器
２５４　保護ストレージアクセサ
２５６　復号化モジュール
２５８　暗号化モジュール
２６０　保護ストレージ
２６２、２６４　インテグリティメトリクス
２６３、２６５　鍵
２７０　ＡＥ識別子
２７２　鍵生成器

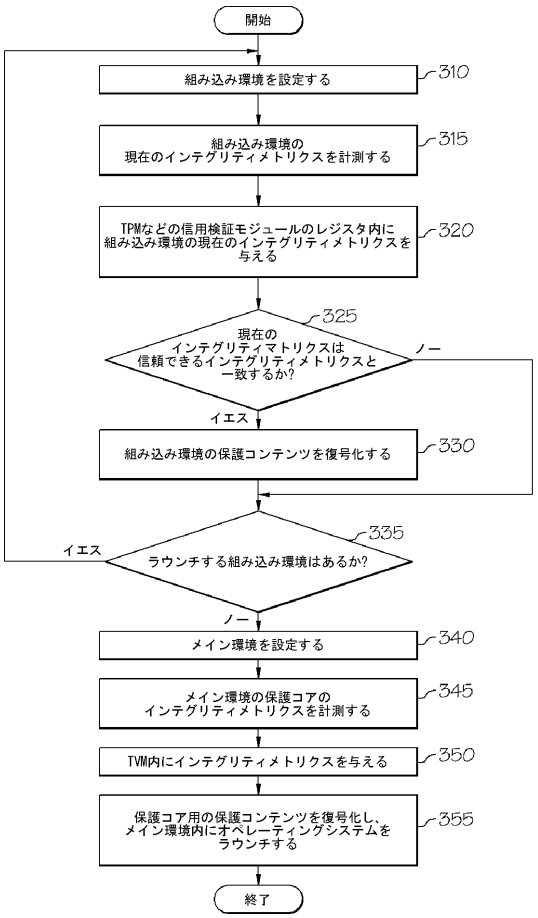
【図１】


ソフトウェアレイヤ 110
メインパーティション 111
VM 112
アプリケーション 116
オペレーティングシステム 118
BIOS 120
保護コア 130
データ 132
処理 134
VMM 136
組み込みパーティション 138
IPB 139
組み込みパーティション 140
組み込みパーティション 142
保護コンテンツ 144
組み込みシステム 145
EPローダ 146
ハードウェアレイヤ 150
プロセッサ 152
PU 154
PU 156
PU 157
コア 158
パーティションマネジャ 159
コントローラハブ 160
隠しレジスタ 161
MAE識別子 162
ランダムアクセスメモリ 164
EPメモリ 166
EPメモリ 168
EPメモリ 170
MPメモリ 172
IPB 173
読出し専用メモリ 174
ファームウェア 176
パーティションマネジャローダ 178
パーティションマネジャ 180
ネットワークインタフェースカード 182
I/Oデバイス 184
ホスト保護アクセス 186
TPM
PCR4
PCR7
190
100

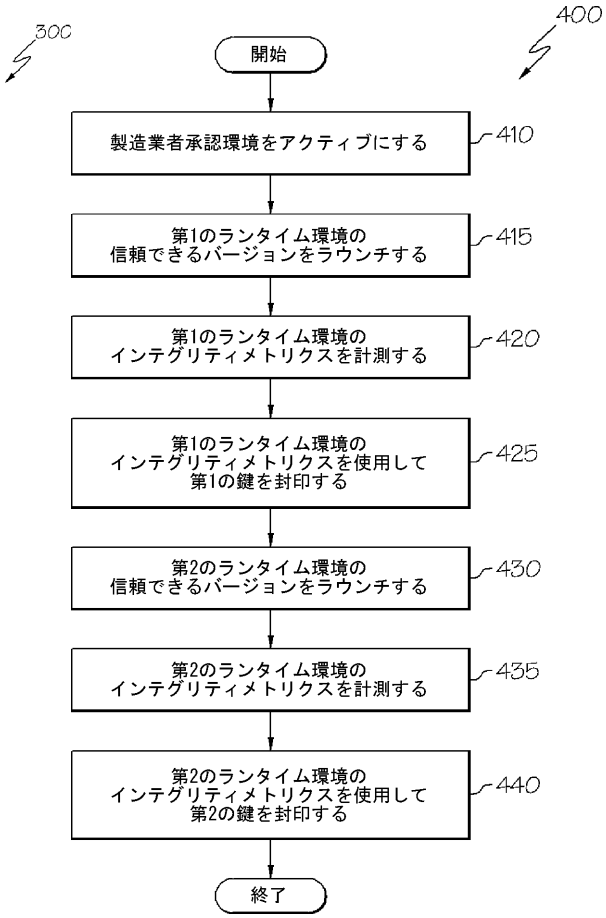
【図２】


信頼検証モジュール 252
インテグリティメトリクス計測器
保護ストレージアクセサ 254
復号化モジュール 256
暗号化モジュール 258
保護ストレージ 260
インテグリティメトリクス 262
鍵 264
鍵 265
AE識別子 270
鍵生成器 272
250
パーティションマネジャ 210
ラウンチ順序論理 215
環境ランチャ 220
リソースアサイナ 222
リソースハイダ 224
割り当て可能なリソース 230
組み込み環境 232
メイン環境 234
保護コンテンツ 242
保護コンテンツ 244
200

【図３】


開始
組み込み環境を設定する 310
組み込み環境の
現在のインテグリティメトリクスを計測する 315
TPMなどの信用検証モジュールのレジスタ内に
組み込み環境の現在のインテグリティメトリクスを
与える 320
現在の
インテグリティマトリクスは
信頼できるインテグリティメトリクスと
一致するか? 325
ノー
イエス
組み込み環境の保護コンテンツを復号化する 330
ラウンチする組み込み環境はあるか? 335
イエス
ノー
メイン環境を設定する 340
メイン環境の保護コアの
インテグリティメトリクスを計測する 345
TVM内にインテグリティメトリクスを与える 350
保護コア用の保護コンテンツを復号化し、
メイン環境内にオペレーティングシステムを
ラウンチする 355
終了

【図４】


300
400
開始
製造業者承認環境をアクティブにする 410
第1のランタイム環境の
信頼できるバージョンをラウンチする 415
第1のランタイム環境の
インテグリティメトリクスを計測する 420
第1のランタイム環境の
インテグリティメトリクスを使用して
第1の鍵を封印する 425
第2のランタイム環境の
信頼できるバージョンをラウンチする 430
第2のランタイム環境の
インテグリティメトリクスを計測する 435
第2のランタイム環境の
インテグリティメトリクスを使用して
第2の鍵を封印する 440
終了

フロントページの続き

審査官　市川　武宜

(56)参考文献　米国特許出願公開第２００７／００９４７１９（ＵＳ，Ａ１）
特開２００６－３２３８１４（ＪＰ，Ａ）
米国特許出願公開第２００５／０１３８３７０（ＵＳ，Ａ１）
米国特許出願公開第２００５／０２１０４６７（ＵＳ，Ａ１）
特開２００７－２５７１９７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２２
Ｇ０６Ｆ　１２／１４
Ｇ０６Ｆ　２１／２４