(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-528665
(P2005-528665A)
(43)公表日　平成17年9月22日(2005.9.22)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 9/46	G06F	9/46	350	5B076
G06F 1/00	G06F	9/06	660G	5B098

審査請求 有　予備審査請求 有　（全 12 頁）

(21)出願番号	特願2003-531310 (P2003-531310)
(86)(22)出願日	平成14年9月27日 (2002.9.27)
(85)翻訳文提出日	平成16年2月24日 (2004.2.24)
(86)国際出願番号	PCT/US2002/031156
(87)国際公開番号	WO2003/027835
(87)国際公開日	平成15年4月3日 (2003.4.3)
(31)優先権主張番号	09/966,015
(32)優先日	平成13年9月27日 (2001.9.27)
(33)優先権主張国	米国 (US)

(71)出願人　593096712
インテル　コーポレイション
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　ブールバード　２２００
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重
(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
最終頁に続く

(54)【発明の名称】システムインテグリティとレガシー環境とを提供するための方法

(57)【要約】
拡張可能なファームウェアアーキテクチャを有する計算システム向けに、プレブートセキュリティとレガシーハードウェア及び環境に対するサポートとを提供する方法及び装置が記載される。仮想マシンモニタ（ＶＭＭ）が利用され、互換性のあるレガシーコードを実行するため、或いはセイフティ及びセキュリティのためにキーデータ及びコード領域をプロテクトするために、システム状態が可視化される。アプリケーションには、システムリソースのサブセットへのアクセス、及び、ＶＭＭに割り出し（プログラム割り込み）する更新用に指定されていないメモリマップの部分へのアクセスを与えることができる。ＶＭＭのプレブートのポリシーエージェントは、状態をプロテクトして、問題のソフトウェアをアンロードする。

【特許請求の範囲】
【請求項１】
物理モードで実行する固有の環境を有する計算システムで仮想マシンモニタを実現するステップと、
該固有の環境が下位の特権モードで実行されるように該物理モードをエミュレートする該仮想マシンモニタを最上位の特権モードで実行するステップと、
を備える方法。
【請求項２】
該固有の環境は、３２ビット環境、６４ビット環境及びＰＣ／ＡＴ環境を含むリストから選択される、
請求項１記載の方法。
【請求項３】
該仮想マシンモニタは、ＰＣ／ＡＴハードウェアのエミュレーション、ＰＣ／ＡＴ環境のエミュレーション、保護されたストレージ及び保護された実行からなるリストから選択された機能を提供するためのコードを含む、
請求項２記載の方法。
【請求項４】
該保護されたストレージは、セキュリティに関連する情報を記憶するために使用される、
請求項３記載の方法。
【請求項５】
該セキュリティに関連する情報は、署名認証、及び暗号化されたハッシュ情報である、
請求項４記載の方法。
【請求項６】
該セキュリティに関連する情報は、認証ログを作成するために使用される、
請求項５記載の方法。
【請求項７】
不信なコードがシステムに障害を与えることを防止するために該コードがサンドボックスモードで実行されるように、拡張可能なファームウェアアーキテクチャを有する計算システムで仮想マシンモニタを実現するステップを備える方法。
【請求項８】
該コードは、レガシーなＢＩＯＳコードである、
請求項７記載の方法。
【請求項９】
プロセッサにより実行されたときに、
物理モードで実行する固有の環境を有する計算システムで仮想マシンモニタを実現するステップと、
該固有の環境が下位の特権モードで実行されるように物理モードをエミュレートする該仮想マシンモニタを最上位の特権モードで実行するステップと、
を備える方法をプロセッサに実行させる実行可能な命令を供給するマシン読み取り可能な媒体。
【請求項１０】
該固有の環境は、３２ビット環境、６４ビット環境及びＰＣ／ＡＴ環境を含むリストから選択される、
請求項９記載の媒体。
【請求項１１】
該仮想マシンモニタは、ＰＣ／ＡＴハードウェアのエミュレーション、ＰＣ／ＡＴ環境のエミュレーション、保護されたストレージ及び保護された実行からなるリストから選択された機能を提供するためのコードを含む、
請求項１０記載のマシン読み取り可能な媒体。
【請求項１２】

該保護されたストレージは、セキュリティに関連する情報を記憶するために使用される、請求項１１記載のマシン読み取り可能な媒体。
【請求項１３】
該セキュリティに関連する情報は、署名認証、及び暗号化されたハッシュ情報である、請求項１２記載のマシン読み取り可能な媒体。
【請求項１４】
該セキュリティに関連する情報は、認証ログを作成するために使用される、請求項１３記載のマシン読み取り可能な媒体。
【請求項１５】
物理モードで実行する固有の実行環境を有する計算システムと、
最上位の特権モードで実行され、該計算システムで実現され、該固有の環境が下位の特権モードで実行されるように物理モードをエミュレートする仮想マシンモニタと、
を備える装置。
【請求項１６】
該固有の環境は、３２ビット環境、６４ビット環境及びＰＣ／ＡＴ環境を含むリストから選択される、
請求項１５記載の装置。
【請求項１７】
該仮想マシンモニタは、ＰＣ／ＡＴハードウェアのエミュレーション、ＰＣ／ＡＴ環境のエミュレーション、保護されたストレージ及び保護された実行からなるリストから選択された機能を提供するためのコードを含む、
請求項１６記載の装置。
【請求項１８】
該保護されたストレージは、セキュリティに関連する情報を記憶するために使用される、請求項１７記載の装置。
【請求項１９】
該セキュリティに関連する情報は、署名認証、及び暗号化されたハッシュ情報である、請求項１８記載の装置。
【請求項２０】
該セキュリティに関連する情報は、認証ログを作成するために使用される、請求項１９記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、拡張可能なファームウェアアーキテクチャを有する計算システムに関し、特に、レガシーハードウェア及び環境（ｌｅｇａｃｙ　ｈａｒｄｗａｒｅ　ａｎｄ　ｅｎｖｉｒｏｎｍｅｎｔ）をエミュレートして、拡張可能なファームウェアアーキテクチャを有する計算システムでのプロテクトされたストレージ及び実行を提供することができる仮想マシンモニタの利用に関する。
【背景技術】
【０００２】
コンピュータシステムのファームウェアにおける最近の進歩は、拡張可能なファームウェアのインタフェース（ＥＦＩ）であり、このＥＦＩにより、ソフトウェアベンダーは、各種の中央処理装置（ＣＰＵ）と共に使用することができるオペレーティングシステムプログラムを開発することができる。スタック上でどのようにデータを渡すかを指定するアプリケーション・バイナリ・インタフェース（ＡＢＩ）が所与のＣＰＵタイプについて含まれる。プラットフォームを抽象化することで、フレームワークは、レガシーアーキテクチャを採用するシステムを通して多くの利点を提供する。このコンポーネントアーキテクチャの進歩の概念として、ＡＢＩと、全体システムの初期化処理を通したソフトウェアの抽象化とを使用したシステムアーキテクチャが登場している。このアーキテクチャは、Ｃ

ＰＵの初期化を含むだけでなく、チップセットとＩ／Ｏ装置の初期化とを含んでいる。チップセット又はＩ／Ｏコンプレックスの一部がどのように動作するかを抽象化する一部のコードを複数パーティーが記述することを可能にするソフトウェアフレームワークが提供されている。かかるフレームワーク内で、様々なベンダーからの製品は、相互使用可能となる。それぞれのベンダーからのコードの一部は、初期化モジュールに含まれる。システム初期化フェーズの間（ＣＰＵリセット後であるが、メモリ初期化前）、コアとなる初期化コードは、基本サービスを提供するために、順序付けされたオーダーで初期化モジュールを送る。初期化フェーズは、フォローオンフェーズを可能にするために十分にシステムを初期化する。たとえば、ドライバ実行フェーズは、初期化処理の責任を果たし、Ｉ／Ｏバスのスキャニング、リソースのエニュメレート及びドライバのインストールのように、アルゴリズム的により複雑である。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

複数パーティーからのドライバ及びアプリケーションの提供を可能にするこの概念は、幾つかの問題点が生じる。１つのベンダーにより提供されるシステムファームウェアのセキュリティは、ベンダーから暗黙的である。サンドボックス又はコードの認可のいずれに対しても手段が存在しないため、様々なソースからのコードモジュールを組み込むことは、システムインテグリティを危険にする。ＥＦＩプラットフォームは、物理モードで実行する。物理モードでの実行は、全てのアドレスが実際のメモリ位置に対応することを意味する。物理モードにおける実行は、全てのプラットフォームリソースへのフルアクセスをＯＳローダに提供するが、また、仮想メモリページテーブルの使用、及びプレブートにおいて提供するプロテクションを不可能にする。ブートファームウェアは、フルマシンアクセスを有するので、高感度のデータ構造及びコアとなるＥＦＩのコードは、ドライバ及びアプリケーションによるアクセスを通して破壊されやすい。ドライバ及びアプリケーションのソースを確認するためのコード署名のような技術は、システム状態が不正なコードにより破壊されたとき、障害隔離を保証することができない。

【０００４】

別の問題は、レガシーコードに対するサポートである。長年の間、ソフトウェアは、ＰＣ／ＡＴプラットフォームと互換性を有するように記述されてきた。多くのレガシーオペレーティングシステム及びオプションＲＯＭ（ｌｅｇａｃｙ　ｏｐｅｒａｔｉｎｇ　ｓｙｓｔｅｍ　ａｎｄ　ｏｐｔｉｏｎ　ＲＯＭ）は、ＰＣ／ＡＴでメモリマップされたハードウェア／ソフトウェアを必要とする。このレガシーコードは、プロセッサを１メガバイトのメモリに制限して、メモリ管理機能又はメモリプロテクション機能を提供しないリアルモードにおいて実行する。

【０００５】

本発明は、例示を経て説明され、同じ参照符号が同じ構成要素を示している添付図面のズにより制限されることが意図されない。

【発明を実施するための最良の形態】

【０００６】

本発明は、第一の実施の形態において、互換性のあるレガシー（古いタイプの）コード（ｌｅｇａｃｙ　ｃｏｍｐａｔｉｂｉｌｉｔｙ　ｃｏｄｅ）を実行すること、或いはセイフティ及びセキュリティのためにキーデータ及びコード領域をプロテクトするために、システム状態を可視化することを提供するための方法及び装置を提供するものである。

【０００７】

ＶＭＭは、全てのＣＰＵ命令及びシステムリソース（たとえば、メモリ及びＩ／Ｏ装置）を含むオリジナルマシンの高性能なレプリカを提供するシミュレータソフトウェアである。第一の実施の形態では、アーキテクチャプラットフォームに基づいた構成要素のためのプレブートセキュリティ（ｐｒｅ－ｂｏｏｔ　ｓｅｃｕｒｉｔｙ）及びインテグリティポリシー（ｉｎｔｅｇｒｉｔｙ　ｐｏｌｉｃｙ）を維持するためにＶＭＭが使用される。

【０００８】
仮想マシンモニタ（ＶＭＭ）が採用され、レガシーハードウェア及び環境をエミュレートし、レガシーコードに対するサポートを提供する。ＶＭＭにより、表面上の特権コード（たとえば、ＢＩＯＳコード）をエミュレートすることができ、そのコードがエミュレートされていることに気づくことなしに実行することができる。

【０００９】
ドライバ実行フェーズでは、ＶＭＭをインストールするドライバがロードされる場合がある。次いで、レガシーアプリケーション（たとえば、レガシーＯＳローダ）は、ＶＭＭ内で実行される場合がある。第一の実施の形態では、レガシーＯＳがブートされたことを示すためにブート変数が設定された場合に、ＶＭＭはロードされるのみである。ＶＭＭを利用することで、メモリ及びシステム構造をプロテクトして、アプリケーションの混乱から助けることができる。アプリケーションには、システムリソースのサブセットへのアクセス、及び、ＶＭＭに割り出し（プログラム割り込み）する更新用に指定されていないメモリマップの一部へのアクセスを与えることができる。ＶＭＭプレブートのポリシーエージェントは、状態をプロテクトし、任意の問題のソフトウェアをアンロードする。ＶＭＭは、物理モードの環境のように見えるが違法な行為に対して予防手段を有する環境をトランスペアレントに広める。また、このポリシーエージェントは、この物理的なアドレスレンジを実際にデコードしないシステムについて、ソフトウェアがレガシーメモリマップを１メガバイト以下で見るようにメモリをマッピングする。このトランスペアレンシーは、レガシーＰＣ／ＡＴ　ＢＩＯＳモジュール、オプションＲＯＭ、ＥＦＩドライバ及びアプリケーションとの互換性を維持する。

【００１０】
第一の実施の形態では、本発明は、全体のＰＣ／ＡＴ環境を可視化して、レガシーＯＳ、及びタイマカウンタ、シリアルポート、及びマスタ／スレーブ割込みコントローラといった８２ｘｘシリーズのようなレガシーハードウェアに対するサポートを提供する。ＶＭにより、拡張可能なファームウェアアーキテクチャを有するシステムは、オプションＲＯＭのプレブート、又はその固有なインタフェースを使用しないランタイム環境のプレブートを容易にする。たとえば、ＶＭは、ＰＣ／ＡＴ環境をエミュレートし、レガシーオプションＲＯＭがそのＩ／Ｏサービスを実行して、作用することを可能にする。次いで、ＶＭＭは、結果を固有のＡＰＩに変換する。すなわち、ＶＭＭは、固有の環境（ｎａｔｉｖｅ　ｅｎｖｉｒｏｎｍｅｎｔ）に等価な意味にＩ／Ｏを割り出す。

【００１１】
代替的な実施の形態では、ＶＭＭは、固有な３２ビット／６４ビット環境をエミュレートするために使用され、物理モードで実行するプラットフォームに、プロテクトされたストレージ及びプロテクトされた実行を提供する。ＥＦＩシステムアーキテクチャは、ページテーブルを考慮せず、指定されたページの読取り専用の指定を考慮しない。これは、ＯＳローダは、ＯＳカーネルをブートストラップするためのページテーブルを使用しているからである。ＶＭＭを使用することで、ドライバ及びアプリケーションコードのバルクがアクセスを有さないセキュリティに関連する情報を生成及び記憶するために、ＯＳローダの下に位置するやり方を提供する。

【００１２】
図１は、本発明のＶＭＭの実現のための典型的な計算システム１００を説明するためのブロック図である。本実施の形態に記載される、互換性のあるレガシーコードを実行するため、又はセイフティとセキュリティのためにキーデータ及びコード領域をプロテクトするためにシステム状態を可視化することが計算システム１００内で実現されて、利用される。計算システム１００は、汎用コンピュータ、携帯用コンピュータ又は他の類似の装置で表すことができる。計算システム１００の構成要素は、典型的なものであって、１つ以上の構成要素を省略又は追加することができる。たとえば、１つ以上のメモリ装置は、計算システム１００のために利用することができる。

【００１３】

図１を参照して、計算システム１００は、表示回路１０５、メインメモリ１０４、スタティックメモリ１０６及び大容量記憶装置１０７にバス１０１を介して接続される中央処理装置１０２及びシグナルプロセッサ１０３を含む。また、計算システム１００は、ディスプレイ１２１、キーパッド入力１２２、カーソルコントロール１２３、ハードコピー装置１２４、入力／出力（Ｉ／Ｏ）装置１２５及びオーディオ／スピーチ装置１２６にもバス１０１を介して接続される。

【００１４】

バス１０１は、情報及び信号を伝達するための標準システムバスである。ＣＰＵ１０２及びシグナルプロセッサ１０３は、計算システム１００のための処理ユニットである。ＣＰＵ１０２又はシグナルプロセッサ１０３、或いはその両者は、計算システム１００のための情報及び／又は信号を処理するために使用することができる。ＣＰＵ１０２は、制御ユニット１３１、算術論理ユニット（ＡＬＵ）１３２、及び複数のレジスタ１３３を含んでおり、これらは、情報及び信号を処理するために使用される。また、シグナルプロセッサ１０３は、ＣＰＵ１０２に類似の構成要素を含むことができる。

【００１５】

メインメモリ１０４は、ＣＰＵ１０２又はシグナルプロセッサ１０３により使用される情報又は命令（プログラムコード）を記憶するために、たとえば、ランダムアクセスメモリ（ＲＡＭ）又は他の動的な記憶装置とすることができる。メインメモリ１０４は、ＣＰＵ１０１又はシグナルプロセッサ１０３による命令の実行の間、一時的な変数又は他の中間的な情報を記憶する。スタティックメモリ１０６は、ＣＰＵ１０２又はシグナルプロセッサ１０３により使用することができる情報又は命令を記憶するために、たとえば、リードオンリメモリ（ＲＯＭ）又は他の静的な記憶装置とすることができる。大容量記憶装置１０７は、計算システム１００の情報又は命令を記憶するために、たとえば、ハードディスクドライブ又はフロプティカルディスクドライブ、或いは光ディスクドライブとすることができる。

【００１６】

ディスプレイ１２１は、たとえば、陰極線管（ＣＲＴ）又は液晶ディスプレイ（ＬＣＤ）とすることができる。ディスプレイ装置１２１は、情報又は図をユーザに表示する。計算システム１００は、表示回路１０５を介してディスプレイ１２１とインタフェースすることができる。キーパッド入力１２２は、アナログ－デジタル変換器による英数字入力装置である。カーソルコントロール１２３は、たとえば、マウス、トラックボール、又はカーソル方向キーとすることができ、ディスプレイ１２１上のオブジェクトの動きを制御する。ハードコピー装置１２４は、たとえば、レーザプリンタとすることができ、紙、フィルム、又は他の類似の媒体に情報をプリントする。多数の入力／出力装置１２５は、計算システム１００に接続することができる。

【００１７】

本発明により、レガシーオペレーティングシステム及びオプションＲＯＭをサポートするために、レガシー環境をエミュレートすること、並びにプロテクトされた実行及びプロテクトされたストレージを提供するために物理モード環境をエミュレートすることは、計算システム１００内に含まれるハードウェア及び／又はソフトウェアにより実現することができる。たとえば、ＣＰＵ１０２又はシグナルプロセッサ１０３は、たとえば、メインメモリ１０４のようなマシン読み取り可能な媒体に記憶されたコード又は命令を実行することができる。

【００１８】

マシン読み取り可能な記憶媒体は、コンピュータ又はデジタル処理装置のようなマシンにより読取り可能な形式で、（すなわち、記憶及び／又は送信）情報を提供するメカニズムを含む。たとえば、マシン読み取り可能な媒体は、リードオンリメモリ（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を含む。コード又は命令は、搬送波信号、赤外線信号、デジタル信号、他の類似の信号により表される。

【００１９】
図２は、本発明の第一の実施の形態によるレガシーエミュレーションを説明する図である。レガシーオプションＲＯＭのみが、レガシー８２５９割込みコントローラの存在を前提としたとしても、パーソナルコンピュータのマザーボードは、レガシー８２５９割込みコントローラに対するサポートを提供する。現代のオペレーティングシステムは、割込みのサポートのためにＡＰＩＣ（ＩＡ３２）又はＳＡＰＩＣ（ＩＰＦ）を使用し、したがって、組になった８２５９のようなマザーボードハードウェアをマシンブートの数秒間に使用可能なままにする。
【００２０】
図２に示されるシステム２００は、ＥＦＩコア２０５、レガシー実行イメージ２１０、ＥＦＩドライバ２１５及びＶＭＭ２２０を含む。レガシー実行イメージ２１０は、プレブートオプションＲＯＭ、又は固有のＥＦＩインタフェースを使用しないランタイム環境である。たとえば、レガシー実行イメージ２１０からのレガシーな８２５９割込み制御ベースへの書込みに応じて、命令がＶＭＭ２２０に割り出される。ＶＭＭ２００は、システム状態（たとえば、割り込みフラグ）に影響を与えるか、或いはプロテクションを変える任意の命令を割り出すことができる。システムがレガシーモードで実行している場合、ＶＭＭ２２０は、レガシー割込み（ＰＩＣ）マスクへのアクセスを、関連する固有の割り込み制御レジスタにマッピングする。たとえば、システムは、含まれていないレガシーなハードウェアへのアクセスを試みる。ＶＭＭは、固有の環境において等価な意味にＩ／Ｏを割り出す。この点で、ＥＦＩドライバ２１５のうちの１つは、関連するチップセットレジスタと通信し、仮想マシンに結果を供給する。これにより、レガシーな環境からの移行パスが供給される。
【００２１】
ＶＭＭは、第三者からのプログラムのサンドボックスによりプレブーストのセキュリティ（ｐｒｅ－ｂｏｏｓｔ　ｓｅｃｕｒｉｔｙ）を提供するために使用される。サンドボックスモードにおいてプログラムを実行することにより、システムの他の部分へのアクセスを有することを防止する。コードは、システムの他の部分を破壊することはないので信頼することができる。アプリケーションには、システムリソースへのサブセットへのアクセス、及び、ＶＭＭに割り出しする更新用に指定されていないメモリマップの一部へのアクセスを与えることができる。ＶＭＭプレブートのポリシーエージェントは、状態を保護し、問題のソフトウェアをアンロードする。
【００２２】
図３は、本発明の第一の実施の形態による、不信なプログラムをサンドボックスするＶＭＭ処理を説明するフローチャートである。図３に示される処理３００は、処理３０５で始まり、ここでは、不信なプログラムは違法な書込みアクセスを試みる。処理３１０で、命令はＶＭＭに割り出される。プログラムがＥＦＩコアコードにより開始された場合、及びプログラムがＥＦＩコアデータ構造へのアクセスを有する場合、アクセスは合法である。これ以外の場合、処理３２０でアクセスは否定され、制御はコアに戻る。
【００２３】
第一の実施の形態では、ＶＭＭは、アダプタカードから導入されたコード及び第三者のドライバを介して導入されたコードが破壊される状態をサンドボックスする。かかるソフトウェア技術のスモールコードの有効域（ｓｍａｌｌ　ｃｏｄｅ　ｆｏｏｔｐｒｉｎｔ）は、コスト依存型のフラッシュメモリベースのシステムにとって有利である。
【００２４】
ＶＭＭは、特権モードで実行し、特権モードをエミュレートして、最高でＯＳロードまでのＥＦＩ環境を実行する。ＶＭＭは、この下位の特権コード（ｌｅｓｓ　ｐｒｉｖｉｌｅｇｅｄ　ｃｏｄｅ）を抽象化するため、ＶＭＭは、アドレス空間の一部を隠すことができる。プロテクトされたモードを可視化するプロテクトされたストレージ及びプロテクトされた実行により、セキュリティ・インフラストラクチャの役割となることができる。
【００２５】

図４は、本発明の第一の実施の形態によるＶＭＭの使用を通したセキュリティアプリケーションの実現を示している。図４に示されるシステム４００は、モジュール４１０を評価するプレブート認証ドライバ４０５を含んでいる。モジュール４１０は、ベンダーからのデジタル認証を含んでいる。署名は、ＭＤ５又はＳＨＡ－１署名である。プレブート認証ドライバ４０５は、署名を確認するためにＶＭＭ４２０の署名ロジック４２１へのエントリポイントを呼出す。ＶＭＭ４２０は、認証ログにおける有効なドライバ及びモジュールの署名を含む保護されたストレージを提供する。認証ログは、システムがロードしたコードの署名を含む場合がある。認証ログが該コードの証明を含んでいる場合、ＶＭＭは該コードを確認する。すなわち、プラットフォームは、コードを実行したことに対して認証する。これにより、制御を行うに先立って、コードを信用することができるという保証がＯＳに対して提供される。

【００２６】

このように、ＶＭＭは、プレブートのセキュリティ（すなわち、ＡＰＩ及びフレームワーク）を提供して、最上位でＯＳロードまでの信頼されたプラットフォームを実現する。この点で、ＯＳローダは、自身のセキュリティを提供することができる。

【００２７】

上記の明細書では、本発明は、特定の典型的な実施の形態を参照して説明された。しかし、様々な変更及び変形は、添付された特許請求の範囲に示されるように、本発明の広い精神及び範囲から逸脱することなしに行われることは明らかである。したがって、明細書及び添付図面は、限定的な意味ではなく、例示的な意味で解釈される。

【図面の簡単な説明】

【００２８】

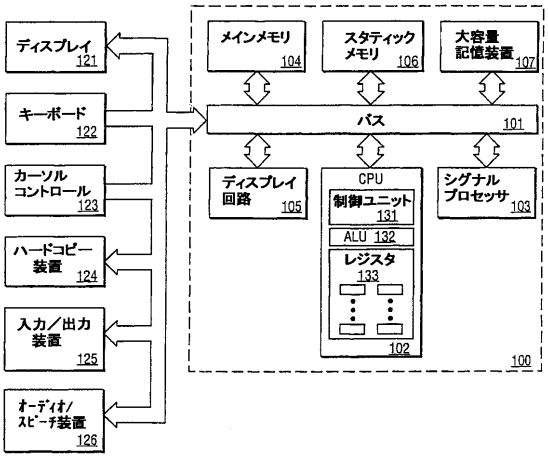
【図１】本発明のＶＭＭを実現するための典型的な計算システムを説明するブロック図である。

【図２】本発明の第一の実施の形態によるレガシーエミュレーションを説明する図である。

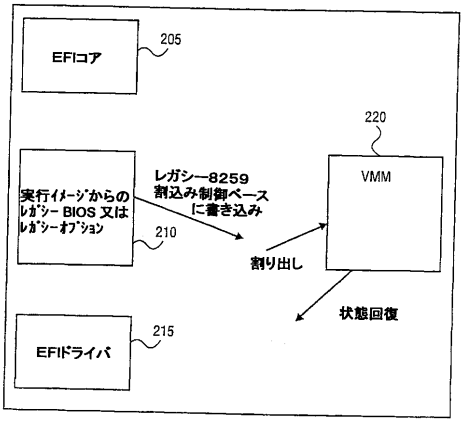
【図３】本発明の第一の実施の形態による不信なプログラムのサンドボックスに対するＶＭＭ動作を説明するフローチャートである。

【図４】本発明の第一の実施の形態によりＶＭＭの使用を通してセキュリティアプリケーションの実現を示す図である。

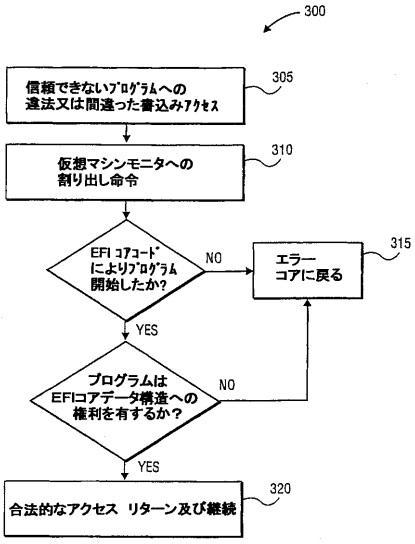
【図１】


ディスプレイ
121
キーボード
122
カーソル
コントロール
123
ハードコピー
装置
124
入力／出力
装置
125
オーディオ/
スピーチ装置
126
メインメモリ
104
スタティック
メモリ
106
大容量
記憶装置
107
バス
101
ディスプレイ
回路
105
CPU
制御ユニット
131
ALU 132
レジスタ
133
102
シグナル
プロセッサ
103
100

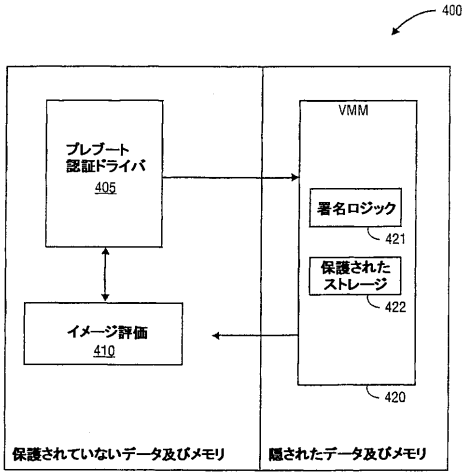
【図２】


EFIコア
205
220
実行イメージからの
レガシー BIOS 又は
レガシーオプション
210
レガシー8259
割込み制御ベース
に書き込み
VMM
割り出し
状態回復
EFIドライバ
215

【図３】


300
信頼できないプログラムへの
違法又は間違った書込みアクセス
305
仮想マシンモニタへの
割り出し命令
310
EFI コアコード
によりプログラム
開始したか?
NO
エラー
コアに戻る
315
YES
プログラムは
EFIコアデータ構造への
権利を有するか?
NO
YES
合法的なアクセス リターン及び継続
320

【図４】


400
プレブート
認証ドライバ
405
VMM
署名ロジック
421
保護された
ストレージ
422
イメージ評価
410
420
保護されていないデータ及びメモリ
隠されたデータ及びメモリ

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 02/31156

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F9/455

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GERALD J. POPEK AND ROBERT P. GOLDBERG: "Formal Requirements for Virtualizable Third Generation Architectures" COMMUNICATIONS OF THE ACM, vol. 16, no. 7, July 1974 (1974-07), pages 412-421, XP002279160 page 413, left-hand column, line 16 - line 25; figure 1 page 414, left-hand column, line 43 - line 53 page 416, right-hand column, line 27 - line 29 page 417, right-hand column, line 9 - line 12 ----- -/--	1-6,9-20

[X] Further documents are listed in the continuation of box C. [ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 May 2004	26/05/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl Fax: (+31-70) 340-3016	Müller, T

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 02/31156

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SOUDER T ET AL: "A tool for securely integrating legacy systems into a distributed environment" REVERSE ENGINEERING, 1999. PROCEEDINGS. SIXTH WORKING CONFERENCE ON ATLANTA, GA, USA 6-8 OCT. 1999, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 6 October 1999 (1999-10-06), pages 47-55, XP010360123 ISBN: 0-7695-0303-9 page 49, left-hand column, line 9 - line 18	7,8
A	DEVANBU P ET AL: "Techniques for trusted software engineering" 19 April 1998 (1998-04-19), SOFTWARE ENGINEERING, 1998. PROCEEDINGS OF THE 1998 INTERNATIONAL CONFERENCE ON KYOTO, JAPAN 19-25 APRIL 1998, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, PAGE(S) 126-135 , XP010276003 ISBN: 0-8186-8368-6 page 135, right-hand column, line 7 - line 15	4-6, 12-14, 18-20
A	BRACKIN S H: "An interface specification language for automatically analyzing cryptographic protocols" NETWORK AND DISTRIBUTED SYSTEM SECURITY, 1997. PROCEEDINGS., 1997 SYMPOSIUM ON SAN DIEGO, CA, USA 10-11 FEB. 1997, LOS ALAMITOS, CA, USA,IEEE COMPUTER. SOC, US, 10 February 1997 (1997-02-10), pages 40-51, XP010216161 ISBN: 0-8186-7767-8 page 45, left-hand column, last paragraph - right-hand column, paragraph 1	4-6, 12-14, 18-20

Form PCT/ISA/210 (continuation of secondsheet) (January 2004)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

Ｆターム(参考) 5B076 FB02
5B098 HH05