(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7461694号
(P7461694)

(45)発行日　令和6年4月4日(2024.4.4)

(24)登録日　令和6年3月27日(2024.3.27)

(51)国際特許分類

		FI		
G06F 12/14 (2006.01)		G06F	12/14	510D
G06F 21/60 (2013.01)		G06F	21/60	320

請求項の数　17　（全31頁）

(21)出願番号　特願2021-549802(P2021-549802)
(86)(22)出願日　令和2年3月6日(2020.3.6)
(65)公表番号　特表2022-522339(P2022-522339A)
(43)公表日　令和4年4月18日(2022.4.18)
(86)国際出願番号　PCT/IB2020/051943
(87)国際公開番号　WO2020/183310
(87)国際公開日　令和2年9月17日(2020.9.17)
審査請求日　令和4年8月24日(2022.8.24)
(31)優先権主張番号　16/296,352
(32)優先日　平成31年3月8日(2019.3.8)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MACHINES CORPORATION
アメリカ合衆国１０５０４ ニューヨーク州 アーモンク ニュー オーチャード ロード
New Orchard Road, Armonk, New York 10504, United States of America
(74)代理人　100112690
弁理士　太佐 種一

最終頁に続く

(54)【発明の名称】　ページのインポート／エクスポートのためのプログラム割り込み

(57)【特許請求の範囲】
【請求項１】
コンピューティング・システムのハードウェア制御によって、信頼できない実体が、前記コンピューティング・システムのメモリに格納されたセキュア・ページをページアウトするために前記セキュア・ページにアクセスするときに、例外を前記信頼できない実体に提示することであって、前記例外が、前記信頼できない実体が前記セキュア・ページにアクセスするのを防ぐ、前記提示することと、
前記例外に応答して、前記信頼できない実体によってエクスポート呼び出しルーチンを発行することと、
前記セキュア・ページおよびホスト仮想アドレスを関連付けるゾーン・セキュリティ・テーブルを用いる、前記コンピューティング・システムのセキュア・インターフェイス制御によって、前記エクスポート呼び出しルーチンを実行することと
を含む、コンピュータ実装方法。
【請求項２】
前記エクスポート呼び出しルーチンが、
前記セキュア・インターフェイス制御によって、前記セキュア・ページを暗号化することを含む、請求項１に記載のコンピュータ実装方法。
【請求項３】
前記エクスポート呼び出しルーチンが、
前記暗号化の前に、前記セキュア・インターフェイス制御によって、前記セキュア・ペ

ージをロックすることと、
前記暗号化の後に、前記セキュア・インターフェイス制御によって、前記セキュア・ページのロックを解除することとを含む、請求項２に記載のコンピュータ実装方法。
【請求項４】
前記エクスポート呼び出しルーチンが、
前記暗号化の前に、前記セキュア・インターフェイス制御によって、前記セキュア・インターフェイス制御への前記セキュア・ページを前記ゾーン・セキュリティ・テーブルに登録することを含む、請求項２または３のいずれか一項に記載のコンピュータ実装方法。
【請求項５】
前記エクスポート呼び出しルーチンが、
前記セキュア・インターフェイス制御によって、前記セキュア・ページの暗号化された内容のハッシュを捕捉することを含む、請求項２ないし４のいずれか一項に記載のコンピュータ実装方法。
【請求項６】
前記エクスポート呼び出しルーチンが、
前記暗号化の後に、前記セキュア・インターフェイス制御によって、ホスト絶対ページを非セキュアとしてマーク付けすることを含む、請求項２ないし５のいずれか一項に記載のコンピュータ実装方法。
【請求項７】
前記エクスポート呼び出しルーチンが、
前記暗号化の後に、前記セキュア・インターフェイス制御によって、ホスト絶対ページを非セキュアとして前記ゾーン・セキュリティ・テーブルに登録することを含む、請求項２ないし６のいずれか一項に記載のコンピュータ実装方法。
【請求項８】
前記セキュア・ページをロックする前に、前記セキュア・ページがロックされているかどうかを判定することと、
前記セキュア・ページがロックされているということの決定に応答して、前記信頼できない実体へのビジー・インジケータを生成することと、
遅延期間の間待つこととをさらに含む、請求項３に記載のコンピュータ実装方法。
【請求項９】
前記ゾーン・セキュリティ・テーブルは、ページに関連付けられたセキュア・ドメインを識別する識別情報と、前記ページが前期セキュア・インターフェイス制御によって所有されているかを示すセキュア・インターフェイス制御ビットと、前記ページのホスト・アドレス対の比較を無効化するためのアドレス比較無効化ビットと、前記ページが信頼できない実体と共有されているかを示す共有ビットとを含む、請求項１ないし８のいずれか一項に記載のコンピュータ実装方法。
【請求項１０】
請求項１ないし９のいずれか一項に記載のコンピュータ実装方法を実行するプロセッサを備えたシステム。
【請求項１１】
請求項１ないし９のいずれか一項に記載のコンピュータ実装方法をプロセッサに実行させるためのプログラム。
【請求項１２】
セキュアな実体が、コンピューティング・システムの信頼できない実体によってページインされたがまだセキュアでないページにアクセスすることに応答して、前記コンピューティング・システムのハードウェア制御によって、例外を前記コンピューティング・システムの前記信頼できない実体に提示することであって、前記例外が、前記信頼できない実体が前記ページにアクセスするのを防ぐ、前記提示することと、
前記例外に応答して、前記信頼できない実体によってインポート呼び出しルーチンを発行することと、

前記コンピューティング・システムのセキュア・インターフェイス制御によって、前記ページをセキュア・ページとし、前記セキュア・ページおよびホスト仮想アドレスを関連付けるようにゾーン・セキュリティ・テーブルに登録する前記インポート呼び出しルーチンを実行することとを含む、コンピュータ実装方法。

【請求項１３】

セキュアな実体が、コンピューティング・システムの信頼できない実体によってページインされたがまだセキュアでないページにアクセスすることに応答して、前記コンピューティング・システムのハードウェア制御によって、例外を前記コンピューティング・システムの前記信頼できない実体に提示することであって、前記例外が、前記信頼できない実体が前記ページにアクセスするのを防ぐ、前記提示することと、

前記例外に応答して、前記信頼できない実体によってインポート呼び出しルーチンを発行することと、

前記コンピューティング・システムのセキュア・インターフェイス制御によって、前記インポート呼び出しルーチンを実行することと

を含み、前記インポート呼び出しルーチンが、

前記コンピューティング・システムのセキュア・インターフェイス制御によって、前記ページが共有されたページであるかどうかを判定することを含む、コンピュータ実装方法。

【請求項１４】

前記インポート呼び出しルーチンが、

前記ページが共有されたセキュア・ページでないということの決定に応答して、前記セキュア・インターフェイス制御によって、前記ページをセキュアとしてマーク付けすることをさらに含む、請求項１３に記載のコンピュータ実装方法。

【請求項１５】

前記インポート呼び出しルーチンが、

前記セキュア・インターフェイス制御によって、前記セキュア・インターフェイス制御への前記ページをゾーン・セキュリティ・テーブルに登録することをさらに含む、請求項１３または１４のいずれか一項に記載のコンピュータ実装方法。

【請求項１６】

前記インポート呼び出しルーチンが、

前記セキュア・インターフェイス制御によって、前記ページを復号すること

をさらに含む、請求項１３ないし１５のいずれか一項に記載のコンピュータ実装方法。

【請求項１７】

請求項１２ないし１６のいずれか一項に記載のコンピュータ実装方法をプロセッサに実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、一般に、コンピュータ技術に関し、より詳細には、ページのインポート／エクスポートのためのプログラム割り込みに関する。

【背景技術】

【０００２】

クラウド・コンピューティングおよびクラウド・ストレージは、それらのデータをサードパーティのデータ・センターに格納して処理する能力をユーザに提供する。クラウド・コンピューティングは、顧客がハードウェアを購入することも、物理的サーバのための床スペースを提供することも必要とせずに、仮想マシン（ＶＭ）を顧客のために迅速かつ簡単にプロビジョニングする能力を促進する。顧客は、顧客の嗜好または要件の変化に従って、ＶＭを簡単に拡大または縮小することができる。通常、クラウド・コンピューティング・プロバイダは、プロバイダのデータ・センターで、サーバ上に物理的に存在するＶＭをプロビジョニングする。特に、コンピューティング・プロバイダが、多くの場合、通常は２人以上の顧客のデータを同じサーバ上に格納するため、顧客は、多くの場合、ＶＭ内

のデータのセキュリティについて心配する。顧客は、顧客自身のコード／データとプロバイダのサイトで実行されている他のＶＭのコード／データの間のセキュリティだけでなく、顧客自身のコード／データとクラウド・コンピューティング・プロバイダのコード／データの間のセキュリティを要求することがある。加えて、顧客は、マシン上で実行されている他のコードからの可能性のあるセキュリティ違反に対するセキュリティだけでなく、プロバイダの管理者からのセキュリティを要求することがある。

【０００３】

そのような注意を要する状況に対処するために、クラウド・サービス・プロバイダは、適切なデータ分離および論理的ストレージ分離を保証するようにセキュリティ制御を実施することがある。クラウド・インフラストラクチャの実装における仮想化の広範囲に及ぶ使用の結果、仮想化が、オペレーティング・システム（ＯＳ：operating system）と基礎になるハードウェアの間の関係を（ハードウェアがコンピューティング、ストレージ、またはネットワークのいずれであっても）変更するため、クラウド・サービスの顧客に固有のセキュリティに関する懸念が生じる。このため仮想化は、それ自体が適切に構成され、管理され、保護されなければならない追加のレイヤとして導入される。

【０００４】

一般に、ホスト・ハイパーバイザの制御下でゲストとして実行されるＶＭは、そのハイパーバイザが仮想化サービスをそのゲストに透過的に提供することに依存する。これらのサービスは、メモリ管理、命令エミュレーション、および割り込み処理を含む。

【０００５】

メモリ管理の場合、ＶＭは、そのデータをメモリに常駐させるためにディスクから移動する（ページインする）ことができ、ＶＭは、そのデータをディスクに戻す（ページアウトする）こともできる。ページがメモリに常駐している間、ＶＭ（ゲスト）は、動的アドレス変換（ＤＡＴ：dynamic address translation）を使用してメモリ内のページをゲスト仮想アドレスからゲスト絶対アドレスにマッピングする。加えて、ホスト・ハイパーバイザは、メモリ内のゲスト・ページに関して、それ自身の（ホスト仮想アドレスからホスト絶対アドレスへの）ＤＡＴマッピングを有しており、ゲスト・ページを、ゲストから独立して透過的にメモリにページインし、メモリからページアウトすることができる。ホストＤＡＴテーブルによって、ハイパーバイザは、メモリ分離、または２つの分離したゲストＶＭ間のゲスト・メモリの共有を実現する。ホストは、必要な場合に、ゲスト・メモリにアクセスし、ゲストの代わりにゲストの動作をシミュレートすることもできる。

【発明の概要】

【０００６】

本明細書に記載された１つまたは複数の例によれば、コンピュータ実装方法は、コンピューティング・システムのハードウェア制御によって、信頼できない実体がコンピューティング・システムのメモリに格納されたセキュア・ページにアクセスするときに、例外を信頼できない実体に提示することを含み、この例外が、信頼できない実体がこのセキュア・ページにアクセスするのを防ぐ。この方法は、例外に応答して、信頼できない実体によってエクスポート呼び出しルーチンを発行することをさらに含む。この方法は、コンピューティング・システムのセキュア・インターフェイス制御によって、エクスポート呼び出しルーチンを実行することをさらに含む。

【０００７】

本明細書に記載された１つまたは複数の例によれば、エクスポート呼び出しルーチンは、セキュア・インターフェイス制御によって、セキュア・ページを暗号化することを含む。本明細書に記載された１つまたは複数の例によれば、エクスポート呼び出しルーチンは、暗号化の前に、セキュア・インターフェイス制御によってセキュア・ページをロックすることと、暗号化の後に、セキュア・インターフェイス制御によってセキュア・ページのロックを解除することとを含む。本明細書に記載された１つまたは複数の例によれば、エクスポート呼び出しルーチンは、暗号化の前に、セキュア・インターフェイス制御によって、セキュア・インターフェイス制御へのセキュア・ページをゾーン・セキュリティ・テ

ーブルに登録することを含む。本明細書に記載された１つまたは複数の例によれば、エクスポート呼び出しルーチンは、セキュア・インターフェイス制御によって、セキュア・ページの暗号化された内容のハッシュを捕捉することを含む。本明細書に記載された１つまたは複数の例によれば、エクスポート呼び出しルーチンは、暗号化の後に、セキュア・インターフェイス制御によって、ホスト絶対ページを非セキュアとしてマーク付けすることを含む。本明細書に記載された１つまたは複数の例によれば、エクスポート呼び出しルーチンは、暗号化の後に、セキュア・インターフェイス制御によって、ホスト絶対ページを非セキュアとしてゾーン・セキュリティ・テーブルに登録することを含む。本明細書に記載された１つまたは複数の例によれば、エクスポート呼び出しルーチンは、セキュア・ページをロックする前に、セキュア・ページがロックされているかどうかを判定することと、セキュア・ページがロックされているということの決定に応答して、信頼できない実体へのビジー・インジケータを生成することと、遅延期間の間待つこととを含む。本明細書に記載された１つまたは複数の例によれば、セキュア・インターフェイス制御は、ファームウェア、ハードウェア、またはファームウェアとハードウェアの組み合わせを備え、信頼できない実体はハイパーバイザを備える。

【０００８】

本明細書に記載された１つまたは複数の例によれば、コンピュータ実装方法は、セキュアな実体が、コンピューティング・システムの信頼できない実体によってページインされたがまだセキュアでないページにアクセスすることに応答して、コンピューティング・システムのハードウェア制御によって、例外をコンピューティング・システムの信頼できない実体に提示することを含み、この例外が、信頼できない実体がこのページにアクセスするのを防ぐ。この方法は、例外に応答して、信頼できない実体によってインポート呼び出しルーチンを発行することをさらに含む。この方法は、コンピューティング・システムのセキュア・インターフェイス制御によって、インポート呼び出しルーチンを実行することをさらに含む。

【０００９】

本明細書に記載された１つまたは複数の例によれば、インポート呼び出しルーチンは、コンピューティング・システムのセキュア・インターフェイス制御によって、セキュア・ページが共有されたページであるかどうかを判定することを含む。本明細書に記載された１つまたは複数の例によれば、インポート呼び出しルーチンは、セキュア・ページが共有されたセキュア・ページでないということの決定に応答して、セキュア・インターフェイス制御によって、セキュア・ページをセキュアとしてマーク付けすることを含む。本明細書に記載された１つまたは複数の例によれば、インポート呼び出しルーチンは、セキュア・インターフェイス制御によって、セキュア・インターフェイス制御へのセキュア・ページをゾーン・セキュリティ・テーブルに登録することを含む。本発明の追加または代替の実施形態に従って、インポート呼び出しルーチンは、セキュア・インターフェイス制御によってセキュア・ページを復号することを含む。

【００１０】

本明細書に記載された他の例では、開示された手法の利点は、コンピュータ・システムおよびコンピュータ・プログラム製品において、前述した方法の特徴を実装することを含む。

【００１１】

開示された手法の利点は、信頼できない実体からの悪意のある挙動を防ぐことを含む。例えば、本手法は、ホスト・プログラム割り込みを使用して、悪意をもって行動していない実体に、セキュア・インターフェイス制御への呼び出しが必要であることを通知できるようにしながら、悪意のある信頼できない実体がセキュア・ストレージにアクセスするのを防ぐ。これによって、ハイパーバイザとゲストの間でメモリ内のページを共有する既存のシステムを超える技術的改良を実現する。このようにして、悪意のある信頼できない実体がセキュア・ゲスト・ストレージにアクセスするのを防ぐことによって、ハイパーバイザ環境内のセキュリティを改善する。

【００１２】
追加の特徴および利点が、本開示の手法によって実現される。本発明のその他の実施形態および態様は、本明細書において詳細に説明され、本発明の一部と見なされる。本発明を利点および特徴と共によく理解するために、説明および図面を参照されたい。
【００１３】
本明細書に記載された専有権の詳細は、本明細書の最後にある特許請求の範囲において具体的に指摘され、明確に請求される。本発明の各実施形態の前述およびその他の特徴と利点は、添付の図面と併せて行われる以下の詳細な説明から明らかになる。
【図面の簡単な説明】
【００１４】
【図１】本発明の１つまたは複数の実施形態に従って、ゾーン・セキュリティのためのテーブルを示す図である。
【図２】本発明の１つまたは複数の実施形態に従って、ＤＡＴを実行するための仮想アドレス空間および絶対アドレス空間を示す図である。
【図３】本発明の１つまたは複数の実施形態に従って、ハイパーバイザの下で実行されている仮想マシン（ＶＭ：virtual machine）を支援するためのネストされたマルチパートＤＡＴ（multi-part DAT）を示す図である。
【図４】本発明の１つまたは複数の実施形態に従って、セキュア・ゲスト・ストレージのマッピングを示す図である。
【図５Ａ】本発明の１つまたは複数の実施形態に従って、インポート動作のプロセス・フローを示す図である。
【図５Ｂ】本発明の１つまたは複数の実施形態に従って、インポート動作のプロセス・フローを示す図である。
【図６】本発明の１つまたは複数の実施形態に従って、インポート動作のプロセス・フローを示す図である。
【図７】本発明の１つまたは複数の実施形態に従って、セキュア・ゲスト・ページへの遷移のプロセス・フローを示す図である。
【図８Ａ】本発明の１つまたは複数の実施形態に従って、ゲストの（復号された）セキュア・ページをページアウトするプロセス・フローを示す図である。
【図８Ｂ】本発明の１つまたは複数の実施形態に従って、エクスポート動作のプロセス・フローを示す図である。
【図８Ｃ】本発明の１つまたは複数の実施形態に従って、エクスポート動作のプロセス・フローを示す図である。
【図９】本発明の１つまたは複数の実施形態に従って、クラウド・コンピューティング環境を示す図である。
【図１０】本発明の１つまたは複数の実施形態に従って、抽象モデル・レイヤを示す図である。
【図１１】本発明の１つまたは複数の実施形態に従って、システムを示す図である。
【図１２】本発明の１つまたは複数の実施形態に従って、処理システムを示す図である。
【発明を実施するための形態】
【００１５】
本明細書において示される図は、実例である。本発明の思想から逸脱することなく、本明細書に記載された図または動作の多くの変形が存在することが可能である。例えば、動作は異なる順序で実行されることが可能であり、あるいは動作は追加、削除、または変更されることが可能である。また、「結合される」という用語およびその変形は、２つの要素間に通信経路が存在することを表しており、それらの要素間に要素／接続が介在しない要素間の直接的接続を意味していない。これらのすべての変形は、本明細書の一部であると見なされる。
【００１６】
本明細書に記載された手法は、ページングのためのマシンの介入が必要であることをハ

イパーバイザに知らせるため、および悪意のあるハイパーバイザの挙動を防ぐために、セキュア・ゲスト環境におけるホスト・プログラム割り込みの使用を提供にする。本手法は、ホスト・プログラム割り込みを使用して、「正常に動作している」ハイパーバイザ（すなわち、悪意をもって行動していないハイパーバイザ）に、セキュア・インターフェイス制御（「ＵＶ」とも呼ばれる）への呼び出しが必要であることを通知できるようにしながら、悪意のあるハイパーバイザがセキュア・ゲスト・ストレージにアクセスするのを防ぐ。

【００１７】

本発明の１つまたは複数の実施形態は、単一のセキュア・ゲスト構成によって（暗号化されていない）疑いが晴れた状態でアクセス可能であることから、暗号化され、ページアウトするためにハイパーバイザによってアクセス可能であることに、ページを遷移させるために、セキュア・ストレージからの変換（エクスポート）ＵＶ呼び出し（ＵＶＣ：UV call）命令を提供する。ページイン後にストレージを復号してセキュア・ゲスト構成に割り当てるために、セキュア・ストレージへの変換（インポート）ＵＶＣ命令も提供される。

【００１８】

本発明の１つまたは複数の実施形態は、ソフトウェアとマシンの間の効率的な軽量のセキュア・インターフェイス制御を活用して、セキュリティを強化する。

【００１９】

ホスト・ハイパーバイザの制御下でゲストとして実行される仮想マシン（ＶＭ）は、そのハイパーバイザが仮想化サービスをそのゲストに透過的に提供することに依存する。これらのサービスは、セキュアな実体と別の信頼できない実体の間の、この他の実体によるセキュア・リソースへのアクセスを従来は許可していた任意のインターフェイスに適用され得る。前述したように、これらのサービスは、メモリ管理、命令エミュレーション、および割り込み処理を含むことができるが、これらに限定されない。例えば、割り込みおよび例外の投入の場合、ハイパーバイザは、通常、ゲストのプレフィックス領域（ロー・コア）に対して、読み取りまたは書き込みあるいはその両方を行う。「仮想マシン」または「ＶＭ」という用語は、本明細書において使用されるとき、物理マシン（コンピューティング・デバイス、プロセッサなど）およびその処理環境（オペレーティング・システム（ＯＳ）、ソフトウェア・リソースなど）の論理的表現のことを指す。ＶＭは、基礎になるホスト・マシン（物理プロセッサまたはプロセッサのセット）上で実行されるソフトウェアとして維持される。ユーザまたはソフトウェア・リソースの視点からは、ＶＭは、それ自身が独立した物理マシンであるように見える。「ハイパーバイザ」および「ＶＭモニタ（ＶＭＭ：VM Monitor）」という用語は、本明細書において使用されるとき、同じホスト・マシン上で複数の（しばしば異なる）ＯＳを使用して実行するように、複数のＶＭを管理および許可する処理環境またはプラットフォーム・サービスのことを指す。ＶＭをデプロイすることが、ＶＭのインストール・プロセスおよびＶＭの有効化（または起動）プロセスを含むということが、理解されるべきである。別の例では、ＶＭをデプロイすることは、ＶＭの有効化（または起動）プロセスを含む（例えば、ＶＭがすでにインストールされているか、またはすでに存在する場合）。

【００２０】

セキュア・ゲストを促進し、支援するためには、ハイパーバイザがＶＭのデータにアクセスできず、したがって前述した方法でサービスを提供できないように、ハイパーバイザに依存しない、ハイパーバイザとセキュア・ゲストの間のセキュリティの向上が必要になるという技術的課題が存在する。

【００２１】

本明細書に記載されたセキュアな実行は、セキュア・ストレージと非セキュア・ストレージの間の分離、および異なるセキュアなユーザに属するセキュア・ストレージ間の分離を保証するためのハードウェア・メカニズムを提供する。セキュア・ゲストの場合、「信頼できない」非セキュア・ハイパーバイザとセキュア・ゲストの間のセキュリティが強化される。これを行うには、通常はゲストの代わりにハイパーバイザが実行する機能の多くがマシンに組み込まれる必要がある。ハイパーバイザとセキュア・ゲストの間のセキュア

・インターフェイスを提供するための新しいセキュア・インターフェイス制御（本明細書では、「ＵＶ」とも呼ばれる）が、本明細書において説明される。セキュア・インターフェイス制御およびＵＶという用語は、本明細書では交換可能なように使用される。セキュア・インターフェイス制御は、ハードウェアと連携して機能し、このセキュリティの向上を実現する。加えて、下位レベルのハイパーバイザが、この信頼できないハイパーバイザに仮想化を提供していることがあり、この下位レベルのハイパーバイザは、信頼できるコードで実装されている場合、セキュア・インターフェイス制御の一部になることもできる。

【００２２】

このメカニズムは、サービス呼び出し元のデータおよび状態にもアクセスできる別の許可されたプログラムによってさまざまなサービスが提供される場合にも、適用されてよい。１つの事例では、この別のプログラムは、別の事例のスーパーバイザ呼び出しインターフェイスの使用によってスーパーバイザ機能を提供するスーパーバイザ・プログラムであってよい。

【００２３】

セキュア・インターフェイス制御は、１つの例では、内部のセキュアな信頼できるハードウェアまたはファームウェアあるいはその両方に実装される。セキュア・ゲストまたはセキュアな実体に関して、セキュア・インターフェイス制御は、セキュアな環境の初期化および維持に加えて、ハードウェア上でこれらのセキュアな実体のディスパッチの調整を行う。セキュア・ゲストがデータを活発に使用しており、ホスト・ストレージに常駐している間、このセキュア・ゲストは、セキュア・ストレージ内で「疑いが晴れた状態」に保たれる。その単一のセキュア・ゲストによって、セキュア・ゲスト・ストレージにアクセスすることができ、このアクセスは、ハードウェアによって厳密に実施される。すなわち、ハードウェアは、任意のセキュアでない実体（ハイパーバイザまたはその他の非セキュア・ゲストを含む）または異なるセキュア・ゲストがそのデータにアクセスするのを防ぐ。この例では、セキュア・インターフェイス制御は、最低レベルのファームウェアの信頼できる部分として実行される。この最低レベル、またはミリコードは、実際にはハードウェアの拡張であり、例えばＩＢＭのｚＡｒｃｈｉｔｅｃｔｕｒｅ（Ｒ）において定義されている複雑な命令および機能を実装するために使用される。ミリコードは、セキュアな実行との関連において、それ自身のセキュアＵＶストレージ、非セキュア・ハイパーバイザ・ストレージ、セキュア・ゲスト・ストレージ、および共有ストレージを含む、ストレージのすべての部分にアクセスすることができる。これによって、ミリコードは、セキュア・ゲストによって、またはそのゲストの支援においてハイパーバイザによって必要とされるすべての機能を提供することができる。セキュア・インターフェイス制御は、ハードウェアに直接アクセスすることもでき、セキュア・インターフェイス制御によって確立された条件の制御下で、ハードウェアが効率的にセキュリティ・チェックを実行できるようにする。

【００２４】

本発明の１つまたは複数の実施形態に従って、セキュア・ページをマーク付けするためのセキュア・ストレージ・ビットがハードウェアにおいて提供される。このビットが設定された場合、ハードウェアは、任意の非セキュア・ゲストまたは非セキュア・ハイパーバイザがこのページにアクセスするのを防ぐ。加えて、各セキュア・ページまたは共有されたページが、ゾーン・セキュリティ・テーブルに登録され、セキュア・ゲスト・ドメイン識別情報（ＩＤ）でタグ付けされる。ページは、非セキュアである場合、非セキュアであるとしてゾーン・セキュリティ・テーブル内でマーク付けされる。このゾーン・セキュリティ・テーブルは、セキュア・インターフェイス制御によって、パーティションまたはゾーンごとに維持される。ページが、このページを所有しているセキュア・ゲストまたはセキュアな実体のみによってアクセスされることを検証するために、セキュアな実体によって行われるいずれかのＤＡＴ変換時にハードウェアによって使用される、ホスト絶対ページごとに１つのエントリが存在する。

【００２５】

本発明の１つまたは複数の実施形態に従って、ソフトウェアは、ＵＶＣ命令を使用して、セキュア・インターフェイス制御に対して特定の動作を実行するよう要求する。例えば、ＵＶＣ命令は、ハイパーバイザによって、セキュア・インターフェイス制御を初期化し、セキュア・ゲスト・ドメイン（例えば、セキュア・ゲスト構成）を作成し、そのセキュアな構成内で仮想ＣＰＵを作成するために使用され得る。ＵＶＣ命令は、ハイパーバイザのページイン動作またはページアウト動作の一部として、セキュア・ゲスト・ページをインポートすること（復号してセキュア・ゲスト・ドメインに割り当てること）、およびエクスポートすること（暗号化してホストがアクセスできるようにすること）にも使用され得る。加えて、セキュア・ゲストは、ハイパーバイザと共有されるストレージを定義し、セキュア・ストレージを共有にし、共有ストレージをセキュアにする能力を有する。

【００２６】

セキュリティを提供するために、ハイパーバイザがセキュア・ゲストのデータを透過的にページインおよびページアウトしているときに、ハードウェアと連携しているセキュア・インターフェイス制御は、データの復号および暗号化を提供し、保証する。これを実現するために、ハイパーバイザは、ゲストのセキュア・データをページインおよびページアウトするときに、新しいＵＶＣを発行する必要がある。ハードウェアは、これらの新しいＵＶＣの間にセキュア・インターフェイス制御によって設定された制御に基づいて、これらのＵＶＣがハイパーバイザによって実際に発行されることを保証する。

【００２７】

この新しいセキュアな環境では、ハイパーバイザは、セキュア・ページをページアウトしているときに常に、新しいセキュア・ストレージからの変換（エクスポート）ＵＶＣを発行する必要がある。セキュア・インターフェイス制御は、このエクスポートＵＶＣに応答して、（１）ページがＵＶによって「ロックされている」ことを示し、（２）ページを暗号化し、（３）ページを非セキュアに設定し、（４）ＵＶのロックをリセットする。エクスポートＵＶＣが完了した後に、ハイパーバイザは、次に暗号化されたゲスト・ページをページアウトできるようになる。

【００２８】

加えて、ハイパーバイザは、セキュア・ページにページインしているときに常に、新しいセキュア・ストレージへの変換（インポート）ＵＶＣを発行する。セキュア・ゲストが、正常に動作するハイパーバイザによってページアウトされており、したがってホスト・メモリに常駐しておらず、ホスト変換（例えば、ページ）テーブル内で無効であるページにアクセスしようとした場合、ページ変換例外（ＰＩＣ１１）がホストに提示される。次に、ハイパーバイザが、ゲスト・ページを、セキュアでないホスト絶対ページにページインし、そのゲスト絶対ページのホストのマッピングを確立し、セキュア・ゲストを再ディスパッチする。この時点で、ページは暗号化されたままであり、非セキュアとしてまだマーク付けされている。そのゲストがそのページに再アクセスしようとするときに、ハードウェアが非セキュア・ストレージ・アクセス（ＰＩＣ３Ｅ）例外を提示する。この例外は、ページが復号されていないときに、セキュア・ゲストがそのページにアクセスするのを防ぐため、およびインポートＵＶＣが必要であることを正常に動作するハイパーバイザに示すために、選択される。ＵＶまたはセキュア・インターフェイス制御は、このインポートＵＶＣに応答して、（１）ページをハードウェア内でセキュアとしてマーク付けし、（２）ページがＵＶによって「ロックされている」ことを示し、（３）ページを復号し、（４）特定のセキュア・ゲスト・ドメインに対する権限を設定し、（５）ＵＶのロックをリセットする。アクセスがセキュアな実体によって行われるときに常に、変換中にハードウェアは、そのページに対して許可チェックを実行する。これらのチェックは、（１）ページが、このページにアクセスしようとしているセキュア・ゲスト・ドメインに実際に属していることを検証するためのチェック、および（２）このページがゲスト・メモリに常駐している間にハイパーバイザがこのページのホストのマッピングを変更していないことを確認するためのチェックを含む。ページがセキュアとしてマーク付けされた後に、ハードウェアは、ハイパーバイザまたは非セキュア・ゲストＶＭのいずれかによるすべてのセキ

ュア・ページへのアクセスを防ぐ。追加の変換ステップが、別のセキュアＶＭによるアクセスを防ぎ、ハイパーバイザによる再マッピングを防ぐ。

【００２９】

本発明の１つまたは複数の実施形態は、ハイパーバイザとゲストの間でメモリ内のページを共有する既存のシステムを超える技術的改良を実現する。そのような既存のシステムは、ページの完全性およびアクセスを損なう可能性がある不完全な挙動の（または悪意のある）ハイパーバイザによる影響を受けやすい。本発明の１つまたは複数の実施形態は、正常に動作する（悪意のない）ハイパーバイザに、セキュア・インターフェイス制御への呼び出しが必要であることを通知できるようにしながら、悪意のあるハイパーバイザがセキュア・ゲスト・ストレージにアクセスするのを防ぐために、セキュア・インターフェイス制御を提供する。このようにして、悪意のあるハイパーバイザがセキュア・ゲスト・ストレージにアクセスするのを防ぐことによって、ハイパーバイザ環境内のセキュリティを改善する。

【００３０】

標準的な／現在のハイパーバイザに基づく環境に関する技術的課題は、ハイパーバイザが悪意をもって行動し、セキュア・ゲスト・ストレージにアクセスできることである。本発明の１つまたは複数の実施形態は、単一のセキュア・ゲスト構成によってアクセス可能であることから、暗号化され、ページアウトするためにハイパーバイザによってアクセス可能であることに、ページを遷移させるために、セキュア・ストレージからの変換（エクスポート）ＵＶＣ命令を使用することによって、そのような技術的課題に対処する。本発明の１つまたは複数の実施形態は、ページイン後にストレージを復号し、セキュア・ゲスト構成に割り当てるために、セキュア・ストレージへの変換（インポート）ＵＶＣ命令を使用することによって、そのような技術的課題に対処する。したがって、本明細書において提供される手法は、悪意のあるハイパーバイザがセキュア・ゲスト・ストレージにアクセスするのを防ぐ。

【００３１】

ここで図１を参照すると、本発明の１つまたは複数の実施形態に従って、ゾーン・セキュリティのためのテーブル１００が概して示されている。図１に示されているゾーン・セキュリティ・テーブル１００は、セキュアな実体によってアクセスされるすべてのページへのセキュアなアクセスを保証するために、セキュア・インターフェイス制御によって維持され、セキュア・インターフェイス制御およびハードウェアによって使用される。ゾーン・セキュリティ・テーブル１００は、ホスト絶対アドレス１１０によってインデックス付けされる。すなわち、ホスト絶対ストレージのページごとに１つのエントリが存在する。各エントリは、アクセスを行っているセキュアな実体に属しているとしてエントリを検証するために使用される情報を含んでいる。

【００３２】

さらに、図１に示されているように、ゾーン・セキュリティ・テーブル１００は、セキュア・ドメインＩＤ１２０（ページに関連付けられたセキュア・ドメインを識別する）と、ＵＶビット１３０（このページがセキュア・インターフェイス制御に提供されており、セキュア・インターフェイス制御によって所有されていることを示す）と、アドレス比較無効化（ＤＡ）ビット１４０（ホスト絶対として定義されたセキュア・インターフェイス制御のページが関連するホスト仮想アドレスを有していないなどの場合に、特定の環境内でホスト・アドレス対の比較を無効化するために使用される）と、共有（ＳＨ）ビット１５０（ページが非セキュア・ハイパーバイザと共有されていることを示す）と、ホスト仮想アドレス１６０（このホスト絶対アドレスの登録されたホスト仮想アドレスを示し、これらのアドレスはホスト・アドレス対と呼ばれる）とを含んでいる。ホスト・アドレス対が、ホスト絶対アドレスと、関連する登録されたホスト仮想アドレスとを示すということに注意する。ホスト・アドレス対は、ハイパーバイザによってインポートされた後の、このページのマッピングを表し、比較は、このページがゲストによって使用されている間に、ホストがこのページを再マッピングしていないことを保証する。

【００３３】
動的アドレス変換（ＤＡＴ）は、仮想ストレージを実ストレージにマッピングするために使用される。ゲストＶＭがハイパーバイザの制御下でページング可能なゲストとして実行されている場合、ゲストは、ＤＡＴを使用してメモリに常駐するページを管理する。加えて、ホストは、ゲスト・ページがメモリに常駐しているときに、独立してＤＡＴを使用して、それらのゲスト・ページを（ホスト自身のページと共に）管理する。ハイパーバイザは、ＤＡＴを使用して、異なるＶＭ間のストレージの分離または共有あるいはその両方を提供するだけでなく、ハイパーバイザ・ストレージへのゲストのアクセスを防ぐ。ハイパーバイザは、ゲストが非セキュア・モードで実行されているときに、すべてのゲストのストレージにアクセスすることができる。

【００３４】
ＤＡＴは、アプリケーションが共有リソースを共有することを引き続き許可しながら、アプリケーション間の分離を可能にする。また、ＤＡＴはＶＭの実装を許可し、ＶＭは、アプリケーション・プログラムの同時処理と共に、ＯＳの新しいバージョンの設計およびテストにおいて使用することができる。仮想アドレスは、仮想ストレージ内の位置を識別する。アドレス空間は、連続する一連の仮想アドレスであり、各仮想アドレスを関連する絶対アドレスに変換できるようにする特定の変換パラメータ（ＤＡＴテーブルを含む）を伴っており、絶対アドレスは、ストレージ内のバイト位置でそのアドレスを識別する。

【００３５】
ＤＡＴは、複数の検索テーブルを使用して、仮想アドレスを関連する絶対アドレスに変換する。このテーブル構造は、通常、ストレージ・マネージャによって定義され、維持される。このストレージ・マネージャは、例えば、あるページをページアウトし、別のページを取り込むことによって、複数のプログラム間で絶対ストレージを透過的に共有する。ページがページアウトされるときに、ストレージ・マネージャは、例えば、関連するページ・テーブル内で無効ビットを設定する。プログラムが、ページアウトされたページにアクセスしようとするときに、ハードウェアがプログラム割り込み（多くの場合、ページ・フォールトと呼ばれる）をストレージ・マネージャに提示する。それに応じて、ストレージ・マネージャは、要求されたページをページインし、無効ビットをリセットする。これは、プログラムにとってすべて透過的に実行され、ストレージ・マネージャがストレージを仮想化し、さまざまな異なるユーザ間で共有することを可能にする。

【００３６】
ＣＰＵによって仮想アドレスが使用されて主記憶装置にアクセスする場合、仮想アドレスは、まずＤＡＴを用いて実アドレスに変換され、次にプレフィックス変換を用いて絶対アドレスに変換される。特定のアドレス空間に対する最高レベルのテーブルの指定（原点および長さ）は、アドレス空間制御要素（ＡＳＣＥ：address-space-control element）と呼ばれ、関連するアドレス空間を定義する。

【００３７】
ここで図２を参照すると、本発明の１つまたは複数の実施形態に従って、ＤＡＴを実行するための例示的な仮想アドレス空間２０２および２０４ならびに絶対アドレス空間２０６が概して示されている。図２に示されている例では、仮想アドレス空間２０２（アドレス空間制御要素（ＡＳＣＥ）Ａ２８によって定義される）および仮想アドレス空間２０４（ＡＳＣＥ　Ｂ２１０によって定義される）という２つの仮想アドレス空間が存在する。ストレージ・マネージャによって、ＡＳＣＥ　Ａ２０８を使用して、仮想ページＡ１．Ｖ２１２ａ１、Ａ２．Ｖ２１２ａ２、およびＡ３．Ｖ２１２ａ３が、複数の検索テーブル（セグメント２３０およびページ・テーブル２３２ａ、２３２ｂ）内で、絶対ページＡ１．Ａ２２０ａ１、Ａ２．Ａ２２０ａ１、およびＡ３．Ａ２２０ａ１にマッピングされる。同様に、ＡＳＣＥ　Ｂ２１０を使用して、仮想ページＢ１．Ｖ２１４ｂ１およびＢ２．Ｖ２１４ｂ２が、２つの検索テーブル２３４および２３６内で、絶対ページＢ１．Ａ２２２ｂ１およびＢ２．Ａ２２２ｂ２にそれぞれマッピングされる。

【００３８】

ここで図３を参照すると、本発明の１つまたは複数の実施形態に従って、ハイパーバイザの下で実行されているＶＭを支援するために使用されるネストされたマルチパートＤＡＴ変換の例が、概して示されている。図３に示されている例では、ゲストＡの仮想アドレス空間Ａ３０２（ゲストＡＳＣＥ（ＧＡＳＣＥ）Ａ３０４によって定義される）およびゲストＢの仮想アドレス空間Ｂ３０６（ＧＡＳＣＥＢ３０８によって定義される）の両方が、共有ホスト（ハイパーバイザ）仮想アドレス空間３２５に存在する。図に示されているように、ゲストＡのストレージ・マネージャによって、ＧＡＳＣＥＡ３０４を使用して、ゲストＡに属している仮想ページＡ１．ＧＶ３１０ａ１、Ａ２．ＧＶ３１０ａ２、およびＡ３．ＧＶ３１０ａ３が、ゲスト絶対ページ（guest absolute pages）Ａ１．ＨＶ３４０ａ１、Ａ２．ＨＶ３４０ａ２、およびＡ３．ＨＶ３４０ａ３にそれぞれマッピングされ、ゲストＢのストレージ・マネージャによって、独立してＧＡＳＣＥＢ３０８を使用して、ゲストＢに属している仮想ページＢ１．ＧＶ３２０ｂ１およびＢ２．ＧＶ３２０ｂ１が、ゲスト絶対ページＢ１．ＨＶ３６０ｂ１およびＢ２．ＨＶ３６０ｂ２にそれぞれマッピングされる。この例では、これらのゲスト絶対ページは、共有ホスト仮想アドレス空間３２５に直接マッピングされ、その後、ホスト絶対アドレス空間３３０への追加のホストＤＡＴ変換を受ける。図に示されているように、ホストのストレージ・マネージャによって、ホストＡＳＣＥ（ＨＡＳＣＥ）３５０を使用して、ホスト仮想アドレスＡ１．ＨＶ３４０ａ１、Ａ３．ＨＶ３４０ａ３、およびＢ１．ＨＶ３６０ｂ１が、Ａ１．ＨＡ３７０ａ１、Ａ３．ＨＡ３７０ａ３、およびＢ１．ＨＡ３７０ｂ１にマッピングされる。ゲストＡに属しているホスト仮想アドレスＡ２．ＨＶ３４０ａ２、およびゲストＢに属しているＢ２．ＨＶ３６０ｂ２の両方が、同じホスト絶対ページ（host absolute page）ＡＢ２．ＨＡ３８０にマッピングされる。これによって、これら２つのゲスト間でデータを共有できるようにする。ゲストＤＡＴ変換中に、ゲストのテーブル・アドレスの各々が、ゲスト絶対として扱われ、追加のネストされたホストＤＡＴ変換を受ける。

【００３９】

本明細書に記載された本発明の実施形態は、セキュア・ゲスト・ストレージの保護を実現する。非セキュア・ゲストおよびハイパーバイザによるセキュア・ストレージへのアクセスが禁止される。ハイパーバイザは、特定の常駐するセキュア・ゲスト・ページに関して、次のことを発生させる。関連するホスト絶対アドレスが、単一のハイパーバイザ（ホスト）ＤＡＴマッピングのみによってアクセス可能になる。すなわち、セキュア・ゲストに割り当てられた特定のホスト絶対アドレスにマッピングされる単一のホスト仮想アドレスが存在する。特定のセキュア・ゲスト・ページに関連付けられたハイパーバイザの（ホスト仮想からホスト絶対への）ＤＡＴマッピングは、このページがページインされている間に変化しない。セキュア・ゲスト・ページに関連付けられたホスト絶対ページは、単一のセキュア・ゲストに関してマッピングされる。

【００４０】

本発明の１つまたは複数の実施形態に従って、セキュア・ゲスト間のストレージの共有も禁止される。ストレージは、セキュア・ゲストの制御下で、単一のセキュア・ゲストとハイパーバイザの間で共有される。

【００４１】

ここで図４を参照すると、本発明の１つまたは複数の実施形態に従って、セキュア・ゲスト・ストレージのマッピングの例が概して示されている。図４は図３に似ているが、図４の例が、セキュア・ゲストＡとセキュア・ゲストＢの間のストレージの共有を可能にしない点が異なっている。図３のセキュアでない例では、ゲストＡに属しているホスト仮想アドレスＡ２．ＨＶ３４０ａ２、およびゲストＢに属しているＢ２．ＨＶ３６０ｂ２の両方が、同じホスト絶対ページＡＢ２．ＨＡ３８０にマッピングされる。図４のセキュア・ゲスト・ストレージの例では、ゲストＡに属しているホスト仮想アドレスＡ２．ＨＶ３４０ａ２がホスト絶対アドレスＡ２．ＨＡ４９０ａにマッピングされ、一方、ゲストＢに属しているＢ２．ＨＶ３６０ｂ２が、それ自身のＢ２．ＨＡ４９０ｂにマッピングされる。この例では、セキュア・ゲスト間に共有が存在しない。

【００４２】
セキュア・ゲスト・ページは、ディスク上に存在する間、暗号化されている。ハイパーバイザは、セキュア・ゲスト・ページをページインするときにＵＶＣを発行し、このＵＶＣは、セキュア制御インターフェイスに、（共有されていない限り）ページをセキュアとしてマーク付けし、（共有されていない限り）復号し、適切なセキュア・ゲスト（例えば、ゲストＡ）に属しているとして（ゾーン・セキュリティ・テーブルに）登録することを実行させる。加えて、ハイパーバイザは、関連するホスト仮想アドレス（例えば、Ａ３．ＨＶ３４０ａ３）を、そのホスト絶対ページ（ホスト・アドレス対と呼ばれる）に登録する。ハイパーバイザは、正しいＵＶＣを発行できない場合、セキュア・ゲスト・ページにアクセスしようとするときに、例外を受信する。ハイパーバイザがゲスト・ページをページアウトするときに同様のＵＶＣが発行され、このＵＶＣは、ゲスト・ページを非セキュアとしてマーク付けして、非セキュアとしてゾーン・セキュリティ・テーブルに登録する前に、（共有されていない限り）ゲスト・ページを暗号化する。

【００４３】
５つの特定のホスト絶対ページＫ、Ｐ、Ｌ、Ｍ、およびＮを含んでいる例では、ハイパーバイザがこれらのホスト絶対ページをページインするときに、セキュア制御インターフェイスによってホスト絶対ページの各々がセキュアとしてマーク付けされる。これによって、非セキュア・ゲストおよびハイパーバイザがこれらのホスト絶対ページにアクセスするのを防ぐ。ハイパーバイザがホスト絶対ページＫ、Ｐ、およびＭをページインするときに、これらのホスト絶対ページが、ゲストＡに属しているとして登録され、ホスト絶対ページＬおよびＮが、ハイパーバイザによってページインされるときに、ゲストＢに登録される。共有ページ（単一のセキュア・ゲストとハイパーバイザの間で共有されたページ）は、ページング中に暗号化も復号も実行されない。これらの共有ページは、セキュアとしてマーク付けされない（ハイパーバイザによるアクセスを許可する）が、単一のセキュア・ゲスト・ドメインと共にゾーン・セキュリティ・テーブルに登録される。

【００４４】
本発明の１つまたは複数の実施形態に従って、非セキュア・ゲストまたはハイパーバイザが、セキュア・ゲストによって所有されているページにアクセスしようとするときに、ハイパーバイザがセキュア・ストレージ・アクセス（ＰＩＣ３Ｄ）例外を受信する。これを決定するための追加の変換ステップは不要である。

【００４５】
１つまたは複数の実施形態に従って、セキュアな実体がページにアクセスしようとするときに、ハードウェアが追加の変換チェックを実行し、ストレージがその特定のセキュア・ゲストに実際に属していることを検証する。ストレージがその特定のセキュア・ゲストに属していない場合、非セキュア・アクセス（ＰＣＩ３Ｅ）例外がハイパーバイザに提示される。加えて、変換されているホスト仮想アドレスが、ゾーン・セキュリティ・テーブル内の登録済みのホスト・アドレス対のホスト仮想アドレスに一致しない場合、セキュア・ストレージ違反（「３Ｆ」ｘ）例外が認識される。ハイパーバイザとの共有を可能にするために、セキュア・ゲストは、変換チェックがアクセスを許す限り、セキュアとしてマーク付けされていないストレージにアクセスすることができる。

【００４６】
ここで図５Ａを参照すると、本発明の１つまたは複数の実施形態に従って、インポート動作のプロセス・フロー５５０が概して示されている。ブロック５５２で、セキュアな実体が、コンピューティング・システムの信頼できない実体によってページインされているセキュア・ページにアクセスすることに応答して、コンピューティング・システムのハードウェア・インターフェイスが、例外をコンピューティング・システムの信頼できない実体に提示する。この例外は、信頼できない実体がセキュア・ページにアクセスするのを防ぐ。ブロック５５４で、信頼できない実体がインポート呼び出しルーチンを発行し、このインポート呼び出しルーチンは、本明細書においてさらに説明される。ブロック５５６で、コンピューティング・システムのセキュア・インターフェイス制御がインポート呼び出

しルーチンを実行する。

【００４７】

図５Ｂは、本発明の１つまたは複数の実施形態に従って、インポート動作のプロセス・フロー５００をさらに示している。セキュア・ゲストが、ハイパーバイザによってページアウトされたページにアクセスするときに、そのページを安全に取り戻すために、プロセス・フロー５００に示されているイベントなどの一連のイベントが発生する。プロセス・フロー５００はブロック５０５で開始し、ブロック７０５で、セキュア・ゲストがゲスト仮想ページにアクセスする。例えばこのページが無効であるため、ハードウェアが、プログラム割り込みコード１１（ＰＩＣ１１）によって示されたホスト・ページ・フォールトをハイパーバイザに提示する（ブロック５１５を参照）。次に、ハイパーバイザは、このゲスト・ページの使用可能なセキュアでないホスト絶対ページを識別し（ブロック５２０を参照）、暗号化されたゲスト・ページを識別されたホスト絶対ページにページインする（ブロック５２５を参照）。

【００４８】

ブロック５３０で、次にホスト絶対ページが、（ホスト仮想アドレスに基づいて）適切なホストＤＡＴテーブル内でマッピングされる。ブロック５３５で、次にハイパーバイザ（ホスト）が、セキュア・ゲストを再ディスパッチする。ブロック５４０で、セキュア・ゲストがセキュア・ゲスト・ページに再アクセスする。ページ・フォールトはすでに存在しないが、このセキュア・ゲストのアクセスおよびページが、図１のゾーン・セキュリティ・テーブル１００内でセキュアとしてマーク付けされていないため、ブロック５４５で、ハードウェアが非セキュア・ストレージ例外（ＰＩＣ３Ｅ）をハイパーバイザに提示する。このＰＩＣ３Ｅは、必要なインポートが発行されるまで、ゲストによるこのセキュア・ページへのアクセスを防ぐ。次に、プロセス・フロー５００は、図６に接続されている「Ａ」に進む。

【００４９】

ここで図６を参照すると、本発明の１つまたは複数の実施形態に従って、インポート動作を実行するためのプロセス・フロー６００が概して示されている。正常に動作する（例えば、エラーのない期待される方法で動作している）ハイパーバイザが、ＰＩＣ３Ｅに応答して、インポートＵＶＣを発行する（ブロック６０５を参照）。この時点で、インポートされるページが、非セキュアとしてマーク付けされ、ハイパーバイザ、他のセキュアでない実体、およびセキュア・インターフェイス制御のみによってアクセス可能であるということに注意する。セキュア・ゲストによって、このページにアクセスすることはできない。

【００５０】

インポートＵＶＣの一部として、セキュア・インターフェイス制御として機能する信頼できるファームウェアが、セキュア・インターフェイス制御によってこのページがすでにロックされているかどうかをチェックして確認する（判定ブロック６１０を参照）。このページがロックされている場合、プロセス・フロー６００がブロック６２０に進む。ブロック６２０で、「ビジー」復帰コードがハイパーバイザに返され、それに応じてハイパーバイザは、遅延し（ブロック６２５を参照）、インポートＵＶＣを再発行する（プロセス・フロー６００がブロック６０５に戻る）。このページがまだロックされていない場合、プロセス・フロー６００が判定ブロック６２２に進む。

【００５１】

判定ブロック６２２で、セキュア・インターフェイス制御が、このページが、非セキュア・ハイパーバイザと共有されたページであるかどうかをチェックして確認する。このページが共有されている場合（プロセス・フロー６００が判定ブロック６２４に進む）、セキュア・インターフェイス制御が、ホスト絶対アドレスを、関連するセキュア・ゲスト・ドメイン、ホスト仮想アドレスと共に、共有されているとしてゾーン・セキュリティ・テーブルに登録する。このページは、非セキュアとしてマーク付けされたままである。これでインポートＵＶＣが完了し、ゲストによってこのページにアクセスできるようになった

。処理は、ハイパーバイザがゲストを再ディスパッチすること（ブロック６３０）、およびセキュア・ゲストがこのページに正常にアクセスすること（ブロック６３５）に進む。

【００５２】

インポートされるホスト仮想ページがハイパーバイザと共有されていない場合（プロセス・フロー６００がブロック６４０に進む）、セキュア・インターフェイス制御は、ハイパーバイザがこのページにアクセスできなくなるように、このページをセキュアとしてマーク付けする。ブロック６４５で、セキュア・インターフェイス制御は、他のＵＶＣがページの状態を変更できないように、ページをロックする。（ブロック６５０で）ロックが設定された後に、セキュア・インターフェイス制御は、ゲスト・ページの内容が、暗号化されている間に変化しなかったことを検証する。ゲスト・ページの内容が変化していた場合、エラー復帰コードがハイパーバイザに返され、そうでない場合、セキュア・インターフェイス制御がセキュア・ページを復号する。

【００５３】

ブロック６５５で、セキュア・インターフェイス制御がページのロックを解除して、他のＵＶＣによるアクセスを許可し、ページを、セキュアとして、ＨＶ－＞ＨＡホスト・アドレス対を完成させるための適切なゲスト・ドメインおよびホスト仮想アドレスに関連付けて、ゾーン・セキュリティ・テーブルに登録する。これによって、ゲストによるアクセスを許可し、ＵＶＣを完了する。

【００５４】

図７は、本発明の１つまたは複数の実施形態に従って、セキュア・ゲスト・ページへの遷移のプロセス・フロー７００を示している。暗号化されたセキュア・ゲスト・ページまたは共有されたセキュア・ゲスト・ページが、ハイパーバイザによってページインされる（７０２）。このページは現在、非セキュア（ＮＳ：non-secure）としてマーク付けされており、非セキュアおよび非共有としてゾーン・セキュリティ・テーブルに登録されている。このページは、セキュアでない実体（ハイパーバイザを含む）によってアクセスされ得る。このページがセキュアな実体によってアクセスされた場合、ホスト例外が提示される。このページは、インポートＵＶＣを使用して（インポートされた）セキュア・ストレージに変換される（７０４）。インポートＵＶＣの一部として、セキュア・インターフェイス制御によって、ページが共有されているかどうかが判定される（７０６）。ページが共有されていない場合、ページが復号され、セキュア・ゲスト・ページ（すなわち、ページが現在「疑いが晴れた状態」である）としてマーク付けされる（ブロック７０８）。特に、疑いが晴れた状態である間にこのページを保護するために、このページは、セキュア・インターフェイス制御によってセキュアとしてマーク付けされ、ゾーン・セキュリティ・テーブルに、セキュアであり、関連するセキュア・ゲスト・ドメインおよびＨＶ－＞ＨＡマッピングと共有されていないとして登録される。しかし、ページが共有されている（すなわち、ハイパーバイザと単一のセキュア・ゲストの間で共有されている）場合、このページは、ハイパーバイザを含む任意のセキュアでない実体によってアクセスされ得る（７１０）。このページは、ハイパーバイザによるアクセスを許可するために非セキュアとしてマーク付けされたままであり、ゾーン・セキュリティ・テーブルに、関連するセキュア・ゲスト・ドメインおよびＨＶ－＞ＨＡマッピングと共有されているとして登録される。

【００５５】

図８Ａは、本発明の１つまたは複数の実施形態に従って、ゲストの（復号された）セキュア・ページをページアウトするプロセス・フロー８３０を示している。本明細書に記載された新しいセキュアな環境では、ハイパーバイザは、セキュア・ページをページアウトしているときに常に、新しいセキュア・ストレージからの変換（エクスポート）ＵＶＣを発行する必要がある。これを実行するために、プロセス・フロー８００が実施される。ブロック８３１で、コンピューティング・システムのハードウェア制御は、信頼できない実体がコンピューティング・システムのメモリに格納されたセキュア・ページにアクセスするときに、例外を信頼できない実体に提示し、この例外が、信頼できない実体がこのセキ

ュア・ページにアクセスするのを防ぐ。ブロック８３２で、信頼できない実体がエクスポート呼び出しルーチンを発行する。ブロック８３３で、コンピューティング・システムのセキュア・インターフェイス制御が、エクスポート呼び出しルーチン（すなわち、セキュア・ストレージからの変換（エクスポート）ＵＶＣ）を実行する。

【００５６】

図８Ｂおよび８Ｃは、本発明の１つまたは複数の実施形態に従って、ページをページアウトするために使用されるエクスポートＵＶＣルーチン８１０のプロセス・フロー８００を示している。ハイパーバイザは、ページアウトするためのセキュア・ゲスト・ページを識別し（８０２）、ハイパーバイザは、ホストＤＡＴテーブル内のセキュア・ゲスト・ページを無効化する（８０４）。ハードウェアは、ホストがページアウトするために共有されていないセキュア・ゲスト・ページにアクセスするときに、セキュア・ストレージ・アクセス（ＰＩＣ３Ｄ）例外をホストに提示し（８０６）、それに応じて、ハイパーバイザがエクスポートＵＶＣを発行する（８０８）。次に、セキュア・インターフェイス制御によって実行されるエクスポートＵＶＣルーチン８１０が開始する。

【００５７】

特に、エクスポートＵＶＣルーチン８１０は、ページがセキュア・インターフェイス制御によってすでにロックされているかどうかを判定することによって、開始する。ページがロックされている場合、「ビジー」インジケータがハイパーバイザに示され（８１４）、ハイパーバイザが遅延を待ち（８１６）、その後、エクスポートＵＶＣの再発行を試みる（８０８）。ページがロックされていない場合、ＵＶがセキュア・ページをロックし、ＵＶに属しているとしてゾーン・セキュリティ・テーブルに登録する（８１８）。セキュア・ゲストは、ページにアクセスできなくなり、他のＵＶＣはホスト絶対ページを操作できない。ＵＶはページを暗号化し、ページの暗号化された内容のハッシュを捕捉する（８２０）。次にＵＶは、ホスト絶対ページを非セキュアとしてマーク付けする（８２２）。これでハイパーバイザは、ページにアクセスできる。次に、ＵＶがページのロックを解除し、非セキュアとしてゾーン・セキュリティ・テーブルに登録する（８２４）。セキュア・ゲストは、ページにまだアクセスできないが、セキュア・インターフェイス制御はページにアクセスできる。ページは、インポートを要求された場合、ゲストのためにインポートされ得る。エクスポートＵＶＣルーチン８１０が終了し、ハイパーバイザがゲスト・ページをページアウトする（８２６）。

【００５８】

本開示にはクラウド・コンピューティングに関する詳細な説明が含まれているが、本明細書において示された教示の実装は、クラウド・コンピューティング環境に限定されないと理解されるべきである。むしろ、本発明の実施形態は、現在既知であるか、または今後開発される任意のその他の種類のコンピューティング環境と組み合わせて実装できる。

【００５９】

クラウド・コンピューティングは、構成可能な計算リソース（例えば、ネットワーク、ネットワーク帯域幅、サーバ、処理、メモリ、ストレージ、アプリケーション、ＶＭ、およびサービス）の共有プールへの便利なオンデマンドのネットワーク・アクセスを可能にするためのサービス提供モデルであり、管理上の手間またはサービス・プロバイダとのやりとりを最小限に抑えて、これらのリソースを迅速にプロビジョニングおよび解放することができる。このクラウド・モデルは、少なくとも５つの特徴、少なくとも３つのサービス・モデル、および少なくとも４つのデプロイメント・モデルを含むことができる。

【００６０】

特徴は、次のとおりである。

【００６１】

オンデマンドのセルフ・サービス：クラウドの利用者は、サーバの時間およびネットワーク・ストレージなどの計算能力を一方的に、サービス・プロバイダとの人間的なやりとりを必要とせず、必要に応じて自動的にプロビジョニングすることができる。

【００６２】

幅広いネットワーク・アクセス：能力は、ネットワークを経由して利用可能であり、標準的なメカニズムを使用してアクセスできるため、異種のシン・クライアントまたはシック・クライアント・プラットフォーム（例えば、携帯電話、ラップトップ、およびＰＤＡ）による利用を促進する。

【００６３】

リソース・プール：プロバイダの計算リソースは、プールされ、マルチテナント・モデルを使用して複数の利用者に提供される。さまざまな物理的および仮想的リソースが、要求に従って動的に割り当ておよび再割り当てされる。場所に依存しないという感覚があり、利用者は通常、提供されるリソースの正確な場所に関して管理することも知ることもないが、さらに高い抽象レベルでは、場所（例えば、国、州、またはデータセンター）を指定できる場合がある。

【００６４】

迅速な順応性：能力は、迅速かつ柔軟に、場合によっては自動的にプロビジョニングされ、素早くスケールアウトし、迅速に解放されて素早くスケールインすることができる。プロビジョニングに使用できる能力は、利用者には、多くの場合、任意の量をいつでも無制限に購入できるように見える。

【００６５】

測定されるサービス：クラウド・システムは、計測機能を活用することによって、サービスの種類（例えば、ストレージ、処理、帯域幅、およびアクティブなユーザのアカウント）に適した、ある抽象レベルで、リソースの使用を自動的に制御および最適化する。リソースの使用量は監視、制御、および報告することができ、利用されるサービスのプロバイダと利用者の両方に透明性が提供される。

【００６６】

サービス・モデルは、次のとおりである。

【００６７】

ＳａａＳ（Software as a Service）：利用者に提供される能力は、クラウド・インフラストラクチャ上で稼働しているプロバイダのアプリケーションの利用である。それらのアプリケーションは、Ｗｅｂブラウザ（例えば、Ｗｅｂベースの電子メール）などのシン・クライアント・インターフェイスを介して、さまざまなクライアント・デバイスからアクセスできる。利用者は、ネットワーク、サーバ、オペレーティング・システム、ストレージ、または個々のアプリケーション機能でさえも含む基盤になるクラウド・インフラストラクチャを、限定的なユーザ固有のアプリケーション構成設定を行う可能性を除き、管理することも制御することもない。

【００６８】

ＰａａＳ（Platform as a Service）：利用者に提供される能力は、プロバイダによって支援されるプログラミング言語およびツールを使用して作成された、利用者が作成または取得したアプリケーションをクラウド・インフラストラクチャにデプロイすることである。利用者は、ネットワーク、サーバ、オペレーティング・システム、またはストレージを含む基盤になるクラウド・インフラストラクチャを管理することも制御することもないが、デプロイされたアプリケーション、および場合によってはアプリケーション・ホスティング環境の構成を制御することができる。

【００６９】

ＩａａＳ（Infrastructure as a Service）：利用者に提供される能力は、処理、ストレージ、ネットワーク、およびその他の基本的な計算リソースのプロビジョニングであり、利用者は、オペレーティング・システムおよびアプリケーションを含むことができる任意のソフトウェアをデプロイして実行できる。利用者は、基盤になるクラウド・インフラストラクチャを管理することも制御することもないが、オペレーティング・システム、ストレージ、デプロイされたアプリケーションを制御することができ、場合によっては、選択されたネットワーク・コンポーネント（例えば、ホスト・ファイアウォール）を限定的に制御できる。

【００７０】
デプロイメント・モデルは、次のとおりである。
【００７１】
プライベート・クラウド：このクラウド・インフラストラクチャは、組織のためにのみ運用される。この組織またはサード・パーティによって管理することができ、オンプレミスまたはオフプレミスに存在することができる。
【００７２】
コミュニティ・クラウド：このクラウド・インフラストラクチャは、複数の組織によって共有され、関心事（例えば、任務、セキュリティ要件、ポリシー、およびコンプライアンスに関する考慮事項）を共有している特定のコミュニティを支援する。これらの組織またはサード・パーティによって管理することができ、オンプレミスまたはオフプレミスに存在することができる。
【００７３】
パブリック・クラウド：このクラウド・インフラストラクチャは、一般ユーザまたは大規模な業界団体が使用できるようになっており、クラウド・サービスを販売する組織によって所有される。
【００７４】
ハイブリッド・クラウド：このクラウド・インフラストラクチャは、データとアプリケーションの移植を可能にする標準化された技術または独自の技術（例えば、クラウド間の負荷バランスを調整するためのクラウド・バースト）によって固有の実体を残したまま互いに結合された２つ以上のクラウド（プライベート、コミュニティ、またはパブリック）の複合である。
【００７５】
クラウド・コンピューティング環境は、ステートレス、疎結合、モジュール性、および意味的相互運用性に重点を置いたサービス指向の環境である。クラウド・コンピューティングの中心になるのは、相互接続されたノードのネットワークを含んでいるインフラストラクチャである。
【００７６】
ここで図９を参照すると、例示的なクラウド・コンピューティング環境５０が示されている。図示されているように、クラウド・コンピューティング環境５０は、クラウドの利用者によって使用されるローカル・コンピューティング・デバイス（例えば、パーソナル・デジタル・アシスタント（ＰＤＡ：personal digital assistant）または携帯電話５４Ａ、デスクトップ・コンピュータ５４Ｂ、ラップトップ・コンピュータ５４Ｃ、または自動車コンピュータ・システム５４Ｎ、あるいはその組み合わせなど）が通信できる１つまたは複数のクラウド・コンピューティング・ノード１０を含んでいる。ノード１０は、互いに通信してよい。ノード１０は、１つまたは複数のネットワーク内で、本明細書において前述されたプライベート・クラウド、コミュニティ・クラウド、パブリック・クラウド、またはハイブリッド・クラウド、あるいはこれらの組み合わせなどに、物理的または仮想的にグループ化されてよい（図示されていない）。これによって、クラウド・コンピューティング環境５０は、クラウドの利用者がローカル・コンピューティング・デバイス上でリソースを維持する必要のないインフラストラクチャ、プラットフォーム、またはＳａａＳ、あるいはその組み合わせを提供できる。図９に示されたコンピューティング・デバイス５４Ａ～Ｎの種類は、例示のみが意図されており、コンピューティング・ノード１０およびクラウド・コンピューティング環境５０は、任意の種類のネットワークまたはネットワーク・アドレス可能な接続（例えば、Ｗｅｂブラウザを使用した接続）あるいはその両方を経由して任意の種類のコンピュータ制御デバイスと通信することができると理解される。
【００７７】
ここで図１０を参照すると、クラウド・コンピューティング環境５０（図９）によって提供される機能的抽象レイヤのセットが示されている。図１０に示されたコンポーネント

、レイヤ、および機能は、例示のみが意図されており、本発明の実施形態がこれらに限定されないということが、あらかじめ理解されるべきである。図示されているように、次のレイヤおよび対応する機能が提供される。

【００７８】

ハードウェアおよびソフトウェア・レイヤ６０は、ハードウェア・コンポーネントおよびソフトウェア・コンポーネントを含む。ハードウェア・コンポーネントの例としては、メインフレーム６１、ＲＩＳＣ（Reduced Instruction Set Computer）アーキテクチャベースのサーバ６２、サーバ６３、ブレード・サーバ６４、ストレージ・デバイス６５、ならびにネットワークおよびネットワーク・コンポーネント６６が挙げられる。一部の実施形態では、ソフトウェア・コンポーネントは、ネットワーク・アプリケーション・サーバ・ソフトウェア６７およびデータベース・ソフトウェア６８を含む。

【００７９】

仮想化レイヤ７０は、仮想サーバ７１、仮想ストレージ７２、仮想プライベート・ネットワークを含む仮想ネットワーク７３、仮想アプリケーションおよびオペレーティング・システム７４、ならびに仮想クライアント７５などの仮想的実体の例を提供できる抽象レイヤを備える。

【００８０】

一例を挙げると、管理レイヤ８０は、以下で説明される機能を提供することができる。リソース・プロビジョニング８１は、クラウド・コンピューティング環境内でタスクを実行するために利用される計算リソースおよびその他のリソースの動的調達を行う。計測および価格設定８２は、クラウド・コンピューティング環境内でリソースが利用される際のコスト追跡、およびそれらのリソースの利用に対する請求書の作成と送付を行う。一例を挙げると、それらのリソースは、アプリケーション・ソフトウェア・ライセンスを含んでよい。セキュリティは、クラウドの利用者およびタスクのＩＤ検証を行うとともに、データおよびその他のリソースの保護を行う。ユーザ・ポータル８３は、クラウド・コンピューティング環境へのアクセスを利用者およびシステム管理者に提供する。サービス・レベル管理８４は、必要なサービス・レベルを満たすように、クラウドの計算リソースの割り当てと管理を行う。サービス水準合意（ＳＬＡ：Service Level Agreement）計画および実行８５は、今後の要求が予想されるクラウドの計算リソースの事前準備および調達を、ＳＬＡに従って行う。

【００８１】

ワークロード・レイヤ９０は、クラウド・コンピューティング環境で利用できる機能の例を示している。このレイヤから提供されてよいワークロードおよび機能の例としては、マッピングおよびナビゲーション９１、ソフトウェア開発およびライフサイクル管理９２、仮想クラスルーム教育の配信９３、データ解析処理９４、トランザクション処理９５、ならびにページのインポート／エクスポートのためのプログラム割り込み９６が挙げられる。これらが単なる例であり、他の実施形態では、各レイヤが異なるサービスを含むことができるということが理解される。

【００８２】

ここで図１１を参照すると、本発明の１つまたは複数の実施形態に従って、システム１１００が示されている。システム１１００は、ネットワーク１６５などを介して１つまたは複数のクライアント・デバイス２０Ａ～２０Ｅと直接的または間接的に通信する例示的なノード１０（例えば、ホスティング・ノード）を含んでいる。ノード１０は、クラウド・コンピューティング・プロバイダのデータセンターまたはホスト・サーバであることができる。ノード１０は、１つまたは複数のＶＭ１５（１５Ａ～１５Ｎ）のデプロイを容易にするハイパーバイザ１２を実行する。ノード１０は、ＶＭ１５Ａ～Ｎおよびハイパーバイザ１２によって必要とされる機能を直接支援し、ハイパーバイザ１２が１つまたは複数のサービスをＶＭ１５に提供することを容易にする、ハードウェア／ファームウェア・レイヤ１１をさらに含んでいる。現在の実装では、ハードウェア／ファームウェア・レイヤ１１とハイパーバイザ１２の間、ハードウェア／ファームウェア・レイヤ１１とＶＭ１５

の間、ハイパーバイザ１２とＶＭ１５の間、およびハードウェア／ファームウェア・レイヤ１１を介したハイパーバイザ１２とＶＭ１５の間で、通信が提供される。本発明の１つまたは複数の実施形態に従って、セキュア・インターフェイス制御がハードウェア／ファームウェア・レイヤ１１において提供され、ハイパーバイザ１２とＶＭ１５の間の直接通信が除外される。

【００８３】

例えば、ノード１０は、クライアント・デバイス２０ＡがＶＭ１５Ａ～１５Ｎのうちの１つまたは複数をデプロイするのを容易にすることができる。個別のクライアント・デバイス２０Ａ～２０Ｅからの各要求に応答して、ＶＭ１５Ａ～１５Ｎがデプロイされてよい。例えば、クライアント・デバイス２０AによってＶＭ１５Ａがデプロイされてよく、クライアント・デバイス２０ＢによってＶＭ１５Ｂがデプロイされてよく、クライアント・デバイス２０ＣによってＶＭ１５Ｃがデプロイされてよい。ノード１０は、クライアントが（ＶＭとして実行するのではなく）物理的サーバをプロビジョニングするのを容易にすることもできる。本明細書に記載された例は、ＶＭの一部としてノード１０内のリソースのプロビジョニングを具現化するが、説明された技術的解決策は、物理的サーバの一部としてリソースをプロビジョニングするように適用されてもよい。

【００８４】

１つの例では、クライアント・デバイス２０Ａ～２０Ｅは、人、企業、政府機関、会社内の部門、または任意のその他の実体などの、同じ実体に属してよく、ノード１０は、実体のプライベート・クラウドとして運用されてよい。この場合、ノード１０は、実体に属しているクライアント・デバイス２０Ａ～２０ＥによってデプロイされているＶＭ１５Ａ～１５Ｎのみをホストする。別の例では、クライアント・デバイス２０Ａ～２０Ｅは、個別の実体に属してよい。例えば、第１の実体はクライアント・デバイス２０Ａを所有してよく、第２の実体はクライアント・デバイス２０Ｂを所有してよい。この場合、ノード１０は、異なる実体のＶＭをホストするパブリック・クラウドとして運用されてよい。例えば、ＶＭ１５Ａ～１５Ｎは、ＶＭ１５ＡがＶＭ１５Ｂへのアクセスを容易にしないような、覆い隠される方法でデプロイされてよい。例えば、ノード１０は、ＩＢＭ　ｚ　Ｓｙｓｔｅｍ（Ｒ）プロセッサ・リソース／システム・マネージャ（ＰＲ／ＳＭ：Processor Resource/System Manager）論理パーティション（ＬＰＡＲ：Logical Partition）機能を使用してＶＭ１５Ａ～１５Ｎを覆い隠してよい。ＰＲ／ＳＭ　ＬＰＡＲなどのこれらの機能は、パーティション間を分離することによって、ノード１０が、同じ物理ノード１０上の異なる実体のために、異なる論理パーティション内で、２つ以上のＶＭ１５Ａ～１５Ｎをデプロイするのを容易にする。

【００８５】

クライアント・デバイス２０Ａ～２０Ｅからのクライアント・デバイス２０Ａは、コンピュータ、スマートフォン、タブレット・コンピュータ、デスクトップ・コンピュータ、ラップトップ・コンピュータ、サーバ・コンピュータ、またはノード１０のハイパーバイザ１２によるＶＭのデプロイメントを要求する任意のその他の通信装置などの、通信装置である。クライアント・デバイス２０Ａは、ネットワーク１６５を介してハイパーバイザによって受信するための要求を送信してよい。ＶＭ１５Ａ～１５ＮからのＶＭ１５Ａは、クライアント・デバイス２０Ａ～２０Ｅからのクライアント・デバイス２０Ａからの要求に応答してハイパーバイザ１２がデプロイするＶＭイメージである。ハイパーバイザ１２は、ＶＭモニタ（ＶＭＭ）であり、ＶＭを作成して実行するソフトウェア、ファームウェア、またはハードウェアであってよい。ハイパーバイザ１２は、ＶＭ１５ＡがノードＡ１０のハードウェア・コンポーネントを使用してプログラムを実行すること、またはデータを格納すること、あるいはその両方を容易にする。ハイパーバイザ１２は、適切な機能および変更を伴って、ＩＢＭ　ｚ　Ｓｙｓｔｅｍ（Ｒ）、ＯＲＡＣＬＥ　ＶＭ　ＳＥＲＶＥＲ（ＴＭ）、ＣＩＴＲＩＸ　ＸＥＮＳＥＲＶＥＲ（ＴＭ）、ＶＭＷＡＲＥ　ＥＳＸ（ＴＭ）、ＭＩＣＲＯＳＯＦＴ　ＨＹＰＥＲ－Ｖ（ＴＭ）、または任意のその他のハイパーバイザであってよい。ハイパーバイザ１２は、ノード１０上で直接実行されるネイティブ・ハイパー

バイザであるか、または別のハイパーバイザ上で実行されるホストされたハイパーバイザであってよい。

【００８６】

ここで図１２を参照すると、本発明の１つまたは複数の実施形態に従って、本明細書の教示を実装するためのノード１０が示されている。ノード１０は、本明細書において説明されているように、さまざまな通信技術を利用するコンピューティング・デバイスおよびネットワークの任意の数および組み合わせを備えるか、または採用するか、あるいはその両方である、電子的コンピュータ・フレームワークであることができる。ノード１０は、容易にスケーリング可能であり、拡張可能であり、モジュール式であり、異なるサービスに変化する能力、または他の機能とは無関係に、一部の機能を再構成する能力を有することができる。

【００８７】

この実施形態では、ノード１０が、１つまたは複数の中央処理装置（ＣＰＵ：central processing units）１２０１ａ、１２０１ｂ、１２０１ｃなどを含むことができるプロセッサ１２０１を含んでいる。プロセッサ１２０１は、処理回路、マイクロプロセッサ、コンピューティング・ユニットとも呼ばれ、システム・バス１２０２を介してシステム・メモリ１２０３およびさまざまな他のコンポーネントに結合される。システム・メモリ１２０３は、読み取り専用メモリ（ＲＯＭ：read only memory）１２０４およびランダム・アクセス・メモリ（ＲＡＭ：random access memory）１２０５を含む。ＲＯＭ１２０４は、システム・バス１２０２に結合され、ノード１０の特定の基本機能を制御する基本入出力システム（ＢＩＯＳ：basic input/output system）を含んでよい。ＲＡＭは、プロセッサ１２０１で使用するためにシステム・バス１２０２に結合された読み取り書き込みメモリである。

【００８８】

図１２のノード１０は、プロセッサ１２０１による読み取りおよび実行が可能な有形のストレージ媒体の例であるハード・ディスク１２０７を含んでいる。ハード・ディスク１２０７は、ソフトウェア１２０８およびデータ１２０９を格納する。ソフトウェア１２０８は、（図５、８Ａ、８Ｂ、および８Ｃのプロセス・フローなどのプロセスを実行するために）プロセッサ１２０１によってノード１０上で実行される命令として格納される。データ１２０９は、ソフトウェア１２０８の動作を支援し、ソフトウェア１２０８の動作によって使用されるさまざまなデータ構造に構造化された定性的変数または定量的変数の値のセットを含む。

【００８９】

図１２のノード１０は、ノード１０のプロセッサ１２０１、システム・メモリ１２０３、ハード・ディスク１２０７、およびその他のコンポーネント（例えば、周辺機器および外部デバイス）の間を相互接続し、これらの間の通信を支援する１つまたは複数のアダプタ（例えば、ハード・ディスク・コントローラ、ネットワーク・アダプタ、グラフィックス・アダプタなど）を含む。本発明の１つまたは複数の実施形態では、１つまたは複数のアダプタを、中間バス・ブリッジを介してシステム・バス１２０２に接続された１つまたは複数のＩ／Ｏバスに接続することができ、１つまたは複数のＩ／Ｏバスが、ＰＣＩ（Peripheral Component Interconnect）などの一般的なプロトコルを利用することができる。

【００９０】

図に示されているように、ノード１０は、キーボード１２２１、マウス１２２２、スピーカ１２２３、およびマイクロホン１２２４をシステム・バス１２０２に相互接続するインターフェイス・アダプタ１２２０を含んでいる。ノード１０は、システム・バス１２０２をディスプレイ１２３１に相互接続するディスプレイ・アダプタ１２３０を含んでいる。ディスプレイ・アダプタ１２３０（またはプロセッサ１２０１あるいはその両方）は、ＧＵＩ１２３２の表示および管理などのグラフィックス性能を提供するために、グラフィックス・コントローラを含むことができる。通信アダプタ１２４１は、システム・バス１

２０２をネットワーク１２５０と相互接続し、ノード１０が、サーバ１２５１およびデータベース１２５２などの他のシステム、デバイス、データ、およびソフトウェアと通信できるようにする。本発明の１つまたは複数の実施形態では、ソフトウェア１２０８およびデータ１２０９の動作が、サーバ１２５１およびデータベース１２５２によってネットワーク１２５０上に実装され得る。例えば、ネットワーク１２５０、サーバ１２５１、およびデータベース１２５２は、組み合わさって、ＰａａＳ（Platform as a Service）、ＳａａＳ（Software as a Service）、またはＩａａＳ（Infrastructure as a Service）、あるいはその組み合わせとして（例えば、分散システム内のＷｅｂアプリケーションとして）、ソフトウェア１２０８およびデータ１２０９の内部の反復を提供することができる。

【００９１】

したがって、図１２で構成されているように、ソフトウェア１２０８およびデータ１２０９（例えば、ノード１０）の動作は、必然的に、従来のハイパーバイザ環境の本明細書に記載された欠点を克服し、対処するためのプロセッサ１２０１またはサーバ１２５１あるいはその両方の計算能力に根差している。これに関して、ソフトウェア１２０８およびデータ１２０９は、悪意のあるハイパーバイザが追加の処理サイクルを引き起こすのを防ぐことによって、ノード１０のプロセッサ１２０１またはサーバ１２５１あるいはその両方の計算動作を改善する（それによって、ノード１０の効率を向上させる）。

【００９２】

本明細書に記載された実施形態は、必然的にコンピュータ技術に根差しており、特に、ＶＭをホストするコンピュータ・サーバに根差している。さらに、本発明の１つまたは複数の実施形態は、コンピューティング技術自体の動作に対する改良を促進し、特に、ハイパーバイザがセキュアＶＭに関連付けられたメモリ、レジスタ、およびその他のそのようなデータにアクセスすることを禁止されていても、ＶＭをホストするコンピュータ・サーバがセキュアＶＭをホストするのを容易にすることによって、ＶＭをホストするコンピュータ・サーバの動作に対する改良を促進する。加えて、本発明の１つまたは複数の実施形態は、ハードウェア、ファームウェア（例えば、ミリコード）、またはこれらの組み合わせを含むセキュア・インターフェイス制御（本明細書では「ＵＶ」とも呼ばれる）を使用して、セキュアＶＭとハイパーバイザの分離を促進し、このようにして、コンピューティング・サーバによってホストされるＶＭのセキュリティを維持することによって、コンピューティング・サーバをホストするＶＭの改善に向かう重要な手順を提供する。セキュア・インターフェイス制御は、本明細書において説明されているように、ＶＭの初期化／終了時に、ＶＭの状態を保護することに大きなオーバーヘッドを追加せずに、セキュリティを促進するための軽量の中間動作を提供する。

【００９３】

本明細書で開示された本発明の実施形態は、ページのインポート／エクスポートのためのプログラム割り込みを使用するシステム、方法、またはコンピュータ・プログラム製品（本明細書ではシステム）、あるいはその組み合わせを含んでよい。説明ごとに、要素の識別子が、異なる図の他の類似する要素に再使用されるということに注意する。

【００９４】

本明細書では、関連する図面を参照して、本発明のさまざまな実施形態が説明される。本発明の範囲を逸脱することなく、本発明の代替の実施形態が考案され得る。以下の説明および図面において、要素間のさまざまな接続および位置関係（例えば、上、下、隣接など）が示される。それらの接続または位置関係あるいはその両方は、特に規定されない限り、直接的または間接的であることができ、本発明はこの点において限定するよう意図されていない。したがって、実体の結合は、直接的結合または間接的結合を指すことができ、実体間の位置関係は、直接的位置関係または間接的位置関係であることができる。さらに、本明細書に記載されたさまざまな作業および工程段階は、本明細書に詳細に記載されない追加の段階または機能を含んでいるさらに包括的な手順または工程に組み込まれ得る。

【００９５】

以下の定義および略称が、特許請求の範囲および本明細書の解釈に使用される。本明細書において使用されているように、「備える」、「備えている」、「含む」、「含んでいる」、「有する」、「有している」、「含有する」、もしくは「含有している」という用語、またはこれらの任意のその他の変形は、非排他的包含をカバーするよう意図されている。例えば、要素のリストを含んでいる組成、混合、工程、方法、製品、または装置は、それらの要素のみに必ずしも限定されず、明示的に列記されていないか、またはそのような組成、混合、工程、方法、製品、もしくは装置に固有の、その他の要素を含むことができる。

【００９６】

さらに、「例示的」という用語は、本明細書では「例、事例、または実例としての役割を果たす」ことを意味するために使用される。「例示的」として本明細書に記載された任意の実施形態または設計は、必ずしも他の実施形態もしくは設計よりも好ましいか、または有利であると解釈されるべきではない。「少なくとも１つ」および「１つまたは複数」という用語は、１以上の任意の整数（すなわち、１、２、３、４など）を含んでいると理解されてよい。「複数」という用語は、２以上の任意の整数（すなわち、２、３、４、５など）を含んでいると理解されてよい。「接続」という用語は、間接的「接続」および直接的「接続」の両方を含んでよい。

【００９７】

「約」、「実質的に」、「近似的に」、およびこれらの変形の用語は、本願書の出願時に使用できる機器に基づいて、特定の量の測定に関連付けられた誤差の程度を含むよう意図されている。例えば、「約」は、特定の値の±８％または５％、あるいは２％の範囲を含むことができる。

【００９８】

本発明は、任意の可能な統合の技術的詳細レベルで、システム、方法、またはコンピュータ・プログラム製品、あるいはその組み合わせであってよい。コンピュータ・プログラム製品は、プロセッサに本発明の態様を実行させるためのコンピュータ可読プログラム命令を含んでいる１つ（または複数）のコンピュータ可読ストレージ媒体を含んでよい。

【００９９】

コンピュータ可読ストレージ媒体は、命令実行デバイスによって使用するための命令を保持および格納できる有形のデバイスであることができる。コンピュータ可読ストレージ媒体は、例えば、電子ストレージ・デバイス、磁気ストレージ・デバイス、光ストレージ・デバイス、電磁ストレージ・デバイス、半導体ストレージ・デバイス、またはこれらの任意の適切な組み合わせであってよいが、これらに限定されない。コンピュータ可読ストレージ媒体のさらに具体的な例の非網羅的リストは、ポータブル・フロッピー（Ｒ）・ディスク、ハード・ディスク、ランダム・アクセス・メモリ（ＲＡＭ：random access memory）、読み取り専用メモリ（ＲＯＭ：read-only memory）、消去可能プログラマブル読み取り専用メモリ（ＥＰＲＯＭ：erasable programmable read-only memoryまたはフラッシュ・メモリ）、スタティック・ランダム・アクセス・メモリ（ＳＲＡＭ：static random access memory）、ポータブル・コンパクト・ディスク読み取り専用メモリ（ＣＤ－ＲＯＭ：compact disc read-only memory）、デジタル多用途ディスク（ＤＶＤ：digital versatile disk）、メモリ・スティック、フロッピー（Ｒ）・ディスク、パンチカードまたは命令が記録されている溝の中の隆起構造などの機械的にエンコードされるデバイス、およびこれらの任意の適切な組み合わせを含む。本明細書において使用されるとき、コンピュータ可読ストレージ媒体は、それ自体が、電波またはその他の自由に伝搬する電磁波、導波管またはその他の送信媒体を伝搬する電磁波（例えば、光ファイバ・ケーブルを通過する光パルス）、あるいはワイヤを介して送信される電気信号などの一過性の信号であると解釈されるべきではない。

【０１００】

本明細書に記載されたコンピュータ可読プログラム命令は、コンピュータ可読ストレージ媒体から各コンピューティング・デバイス／処理デバイスへ、またはネットワーク（例

えば、インターネット、ローカル・エリア・ネットワーク、広域ネットワーク、または無線ネットワーク、あるいはその組み合わせ）を介して外部コンピュータもしくは外部ストレージ・デバイスへダウンロードされ得る。このネットワークは、銅伝送ケーブル、光伝送ファイバ、無線送信、ルータ、ファイアウォール、スイッチ、ゲートウェイ・コンピュータ、またはエッジ・サーバ、あるいはその組み合わせを備えてよい。各コンピューティング・デバイス／処理デバイス内のネットワーク・アダプタ・カードまたはネットワーク・インターフェイスは、コンピュータ可読プログラム命令をネットワークから受信し、それらのコンピュータ可読プログラム命令を各コンピューティング・デバイス／処理デバイス内のコンピュータ可読ストレージ媒体に格納するために転送する。

【０１０１】

本発明の動作を実行するためのコンピュータ可読プログラム命令は、アセンブラ命令、命令セット・アーキテクチャ（ＩＳＡ：instruction-set-architecture）命令、マシン命令、マシン依存命令、マイクロコード、ファームウェア命令、状態設定データ、集積回路のための構成データ、あるいは、Ｓｍａｌｌｔａｌｋ（Ｒ）、Ｃ＋＋などのオブジェクト指向プログラミング言語、および「Ｃ」プログラミング言語または同様のプログラミング言語などの手続き型プログラミング言語を含む、１つもしくは複数のプログラミング言語の任意の組み合わせで記述されたソース・コードまたはオブジェクト・コードのいずれかであってよい。コンピュータ可読プログラム命令は、ユーザのコンピュータ上で全体的に実行すること、ユーザのコンピュータ上でスタンドアロン・ソフトウェア・パッケージとして部分的に実行すること、ユーザのコンピュータ上およびリモート・コンピュータ上でそれぞれ部分的に実行すること、あるいはリモート・コンピュータ上またはサーバ上で全体的に実行することができる。後者のシナリオでは、リモート・コンピュータは、ローカル・エリア・ネットワーク（ＬＡＮ：local area network）または広域ネットワーク（ＷＡＮ：wide area network）を含む任意の種類のネットワークを介してユーザのコンピュータに接続されてよく、または接続は、（例えば、インターネット・サービス・プロバイダを使用してインターネットを介して）外部コンピュータに対して行われてよい。一部の実施形態では、本発明の態様を実行するために、例えばプログラマブル論理回路、フィールドプログラマブル・ゲート・アレイ（ＦＰＧＡ：field-programmable gate arrays）、またはプログラマブル・ロジック・アレイ（ＰＬＡ：programmable logic arrays）を含む電子回路は、コンピュータ可読プログラム命令の状態情報を利用することによって、電子回路をカスタマイズするためのコンピュータ可読プログラム命令を実行してよい。

【０１０２】

本発明の態様は、本明細書において、本発明の実施形態に従って、方法、装置（システム）、およびコンピュータ・プログラム製品のフローチャート図またはブロック図あるいはその両方を参照して説明される。フローチャート図またはブロック図あるいはその両方の各ブロック、ならびにフローチャート図またはブロック図あるいはその両方に含まれるブロックの組み合わせが、コンピュータ可読プログラム命令によって実装され得るということが理解されるであろう。

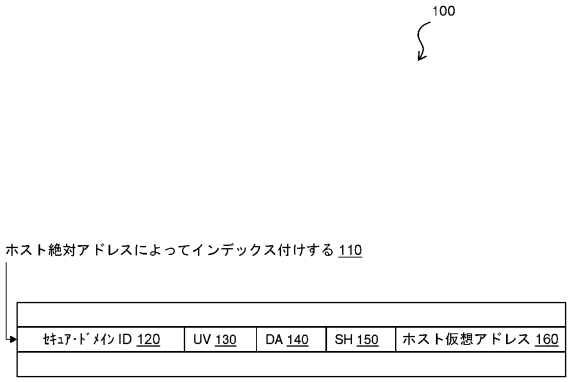
【０１０３】

これらのコンピュータ可読プログラム命令は、コンピュータまたはその他のプログラム可能なデータ処理装置のプロセッサを介して実行される命令が、フローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックに指定される機能／動作を実施する手段を作り出すべく、汎用コンピュータ、専用コンピュータ、または他のプログラム可能なデータ処理装置のプロセッサに提供されてマシンを生成するものであってよい。これらのコンピュータ可読プログラム命令は、命令が格納されたコンピュータ可読ストレージ媒体がフローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックに指定される機能／動作の態様を実施する命令を含んでいる製品を備えるように、コンピュータ可読ストレージ媒体に格納され、コンピュータ、プログラム可能なデータ処理装置、または他のデバイス、あるいはその組み合わせに特定の方式で機能するように指示できるものであってもよい。

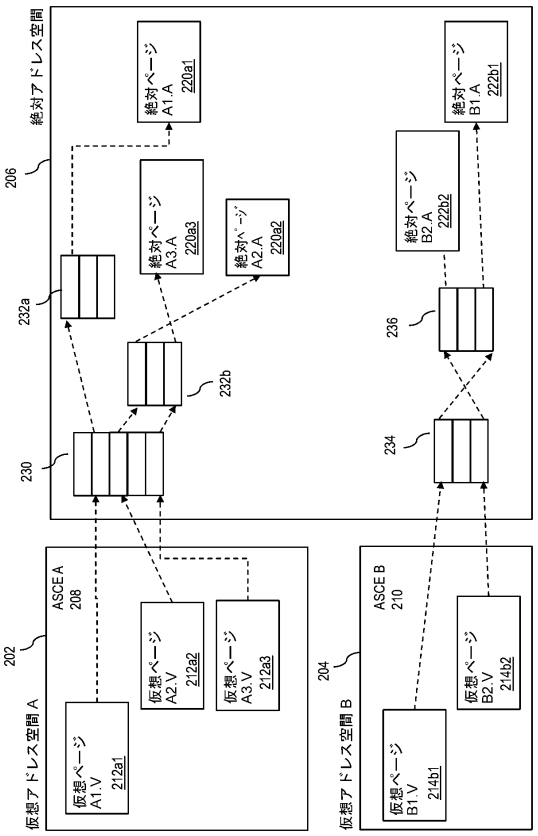
【０１０４】
コンピュータ可読プログラム命令は、コンピュータ上、その他のプログラム可能な装置上、またはその他のデバイス上で実行される命令が、フローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックに指定される機能／動作を実施するように、コンピュータ、その他のプログラム可能なデータ処理装置、またはその他のデバイスに読み込まれてもよく、それによって、一連の動作可能なステップを、コンピュータ上、その他のプログラム可能な装置上、またはコンピュータ実装プロセスを生成するその他のデバイス上で実行させる。
【０１０５】
図内のフローチャートおよびブロック図は、本発明のさまざまな実施形態に従って、システム、方法、およびコンピュータ・プログラム製品の可能な実装のアーキテクチャ、機能、および動作を示す。これに関連して、フローチャートまたはブロック図内の各ブロックは、規定された論理機能を実装するための１つまたは複数の実行可能な命令を備える、命令のモジュール、セグメント、または部分を表してよい。一部の代替の実装では、ブロックに示された機能は、図に示された順序とは異なる順序で発生してよい。例えば、連続して示された２つのブロックは、実際には、含まれている機能に応じて、実質的に同時に実行されるか、または場合によっては逆の順序で実行されてよい。ブロック図またはフローチャート図あるいはその両方の各ブロック、ならびにブロック図またはフローチャート図あるいはその両方に含まれるブロックの組み合わせは、規定された機能または動作を実行するか、あるいは専用ハードウェアとコンピュータ命令の組み合わせを実行する専用ハードウェアベースのシステムによって実装され得るということにも注意する。
【０１０６】
本明細書で使用される用語は、特定の実施形態を説明することのみを目的としており、制限することを意図していない。本明細書において使用されるとき、単数形「ａ」、「ａｎ」、および「ｔｈｅ」は、特に明示的に示されない限り、複数形も含むことが意図されている。「備える」または「備えている」あるいはその両方の用語は、本明細書で使用される場合、記載された機能、整数、ステップ、動作、要素、またはコンポーネント、あるいはその組み合わせの存在を示すが、１つまたは複数のその他の機能、整数、ステップ、動作、要素コンポーネント、またはこれらのグループ、あるいはその組み合わせの存在または追加を除外していないということが、さらに理解されるであろう。
【０１０７】
本明細書におけるさまざまな実施形態の説明は、例示の目的で提示されているが、網羅的であることは意図されておらず、開示された実施形態に制限されない。記載された実施形態の範囲および思想を逸脱することなく多くの変更および変形が可能であることは、当業者にとって明らかであろう。本明細書で使用された用語は、実施形態の原理、実際の適用、または市場で見られる技術を超える技術的改良を最も適切に説明するため、あるいは他の当業者が本明細書で開示された実施形態を理解できるようにするために選択されている。

【図面】

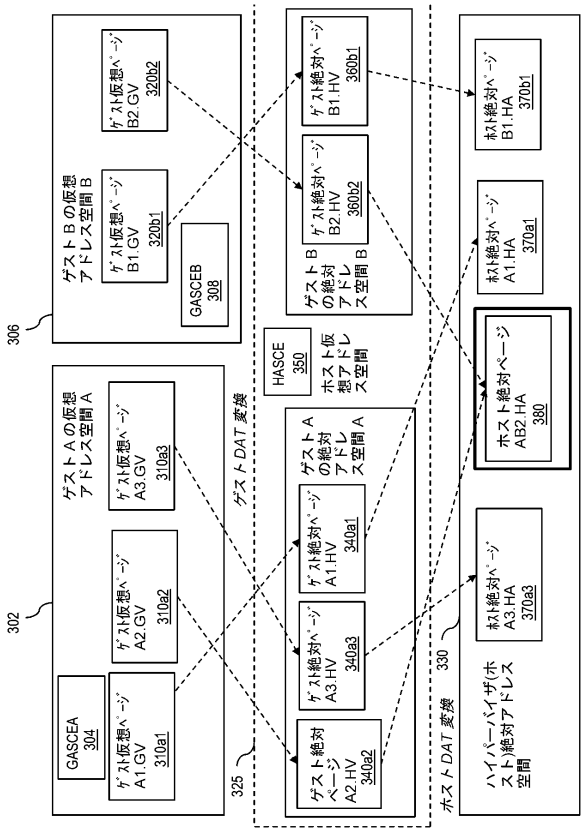
【図１】


100
ホスト絶対アドレスによってインデックス付けする 110
ｾｷｭｱ･ﾄﾞﾒｲﾝ ID 120
UV 130
DA 140
SH 150
ホスト仮想アドレス 160

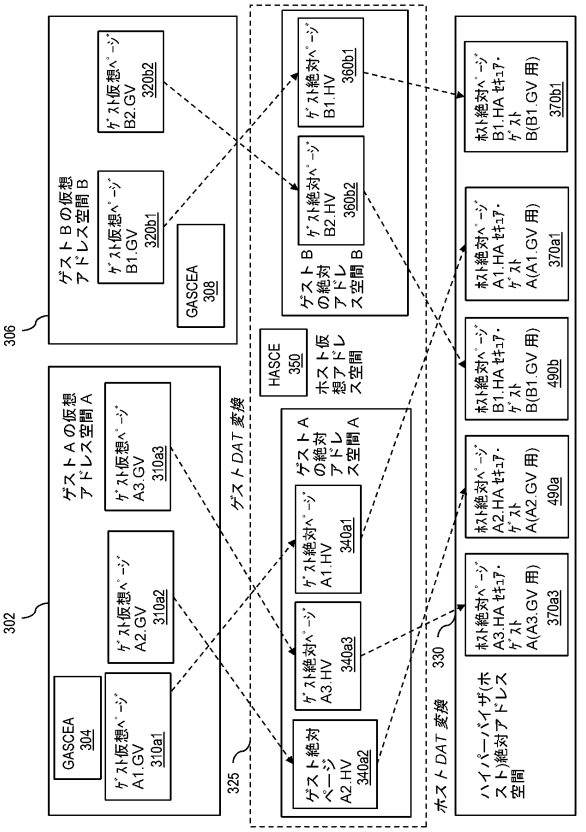
【図２】


絶対アドレス空間
206
絶対ページ A1.A 220a1
絶対ページ A3.A 220a3
絶対ページ A2.A 220a2
絶対ページ B2.A 222b2
絶対ページ B1.A 222b1
232a
232b
236
230
234
ASCE A 208
ASCE B 210
202
204
仮想アドレス空間 A
仮想アドレス空間 B
仮想ページ A1.V 212a1
仮想ページ A2.V 212a2
仮想ページ A3.V 212a3
仮想ページ B1.V 214b1
仮想ページ B2.V 214b2

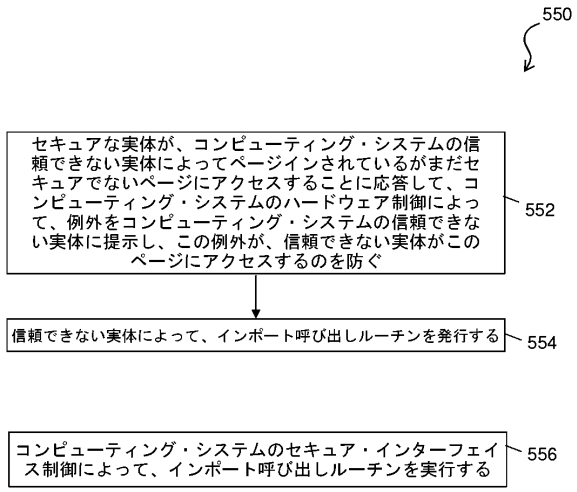
【図３】


ゲストBの仮想アドレス空間B
ゲスト仮想ページ B2.GV 320b2
ゲスト仮想ページ B1.GV 320b1
GASCEB 308
306
ゲストAの仮想アドレス空間A
ゲスト仮想ページ A3.GV 310a3
ゲスト仮想ページ A2.GV 310a2
GASCEA 304
ゲスト仮想ページ A1.GV 310a1
302
325
ゲストDAT変換
HASCE 350
ホスト仮想アドレス空間
ゲストBの絶対アドレス空間B
ゲスト絶対ページ B1.HV 360b1
ゲスト絶対ページ B2.HV 360b2
ゲストAの絶対アドレス空間A
ゲスト絶対ページ A1.HV 340a1
ゲスト絶対ページ A3.HV 340a3
ゲスト絶対ページ A2.HV 340a2
ホストDAT変換
330
ホスト絶対ページ A1.HA 370a1
ホスト絶対ページ AB2.HA 380
ホスト絶対ページ A3.HA 370a3
ホスト絶対ページ B1.HA 370b1
ハイパーバイザ(ホスト)絶対アドレス空間

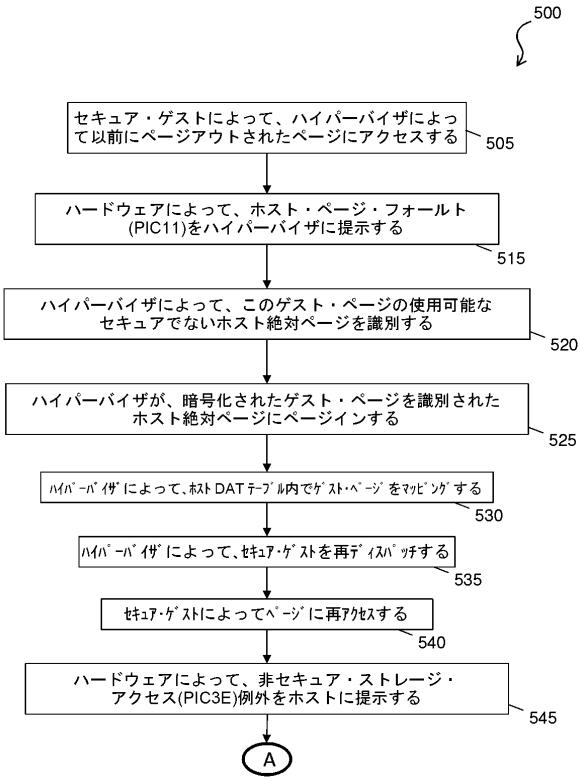
【図４】


ゲストBの仮想アドレス空間B
ゲスト仮想ページ B2.GV 320b2
ゲスト仮想ページ B1.GV 320b1
GASCEA 308
306
ゲストAの仮想アドレス空間A
ゲスト仮想ページ A3.GV 310a3
ゲスト仮想ページ A2.GV 310a2
GASCEA 304
ゲスト仮想ページ A1.GV 310a1
302
325
ゲストDAT変換
HASCE 350
ホスト仮想アドレス空間
ゲストBの絶対アドレス空間B
ゲスト絶対ページ B1.HV 360b1
ゲスト絶対ページ B2.HV 360b2
ゲストAの絶対アドレス空間A
ゲスト絶対ページ A1.HV 340a1
ゲスト絶対ページ A3.HV 340a3
ゲスト絶対ページ A2.HV 340a2
ホストDAT変換
330
ホスト絶対ページ A1.HA セキュア・ゲスト A(A1.GV 用) 370a1
ホスト絶対ページ B1.HA セキュア・ゲスト B(B1.GV 用) 490b
ホスト絶対ページ A2.HA セキュア・ゲスト A(A2.GV 用) 490a
ホスト絶対ページ A3.HA セキュア・ゲスト A(A3.GV 用) 370a3
ホスト絶対ページ B1.HA セキュア・ゲスト B(B1.GV 用) 370b1
ハイパーバイザ(ホスト)絶対アドレス空間

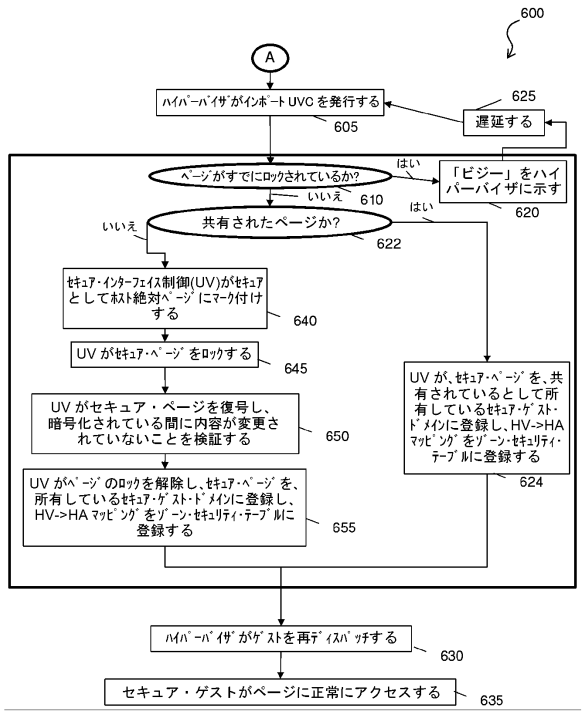
【図５Ａ】


550
セキュアな実体が、コンピューティング・システムの信頼できない実体によってページインされているがまだセキュアでないページにアクセスすることに応答して、コンピューティング・システムのハードウェア制御によって、例外をコンピューティング・システムの信頼できない実体に提示し、この例外が、信頼できない実体がこのページにアクセスするのを防ぐ
552
信頼できない実体によって、インポート呼び出しルーチンを発行する
554
コンピューティング・システムのセキュア・インターフェイス制御によって、インポート呼び出しルーチンを実行する
556

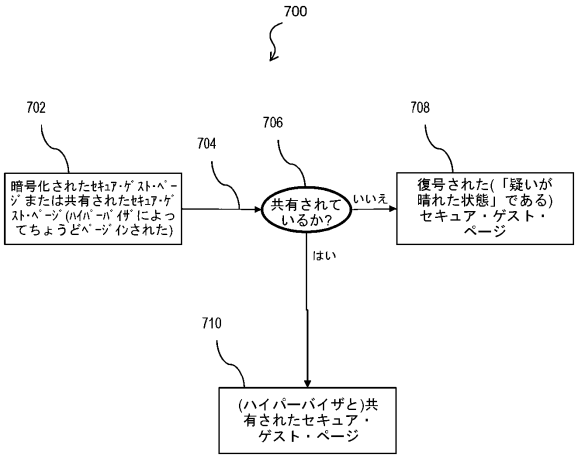
【図５Ｂ】


500
セキュア・ゲストによって、ハイパーバイザによって以前にページアウトされたページにアクセスする
505
ハードウェアによって、ホスト・ページ・フォールト(PIC11)をハイパーバイザに提示する
515
ハイパーバイザによって、このゲスト・ページの使用可能なセキュアでないホスト絶対ページを識別する
520
ハイパーバイザが、暗号化されたゲスト・ページを識別されたホスト絶対ページにページインする
525
ﾊｲﾊﾟｰﾊﾞｲｻﾞによって、ﾎｽﾄDATﾃｰﾌﾞﾙ内でｹﾞｽﾄ・ﾍﾟｰｼﾞをﾏｯﾋﾟﾝｸﾞする
530
ﾊｲﾊﾟｰﾊﾞｲｻﾞによって、ｾｷｭｱ・ｹﾞｽﾄを再ﾃﾞｨｽﾊﾟｯﾁする
535
ｾｷｭｱ・ｹﾞｽﾄによってﾍﾟｰｼﾞに再ｱｸｾｽする
540
ハードウェアによって、非セキュア・ストレージ・アクセス(PIC3E)例外をホストに提示する
545
A

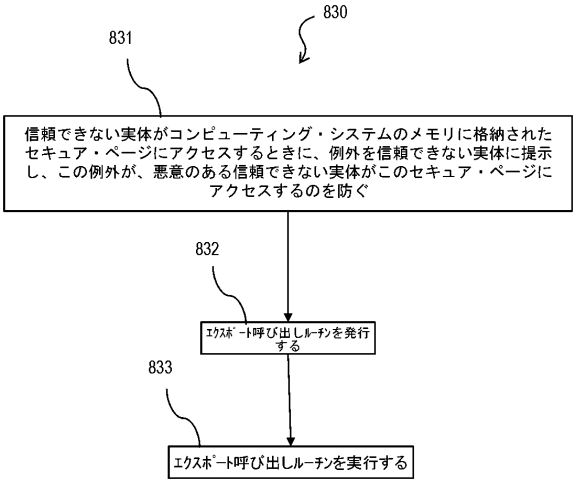
【図６】


600
A
ハイパーバイザがインポートUVCを発行する
605
625
遅延する
ページがすでにロックされているか?
はい
「ビジー」をハイパーバイザに示す
620
いいえ
610
共有されたページか?
はい
いいえ
622
セキュア・インターフェイス制御(UV)がセキュアとしてホスト絶対ページにマーク付けする
640
UVがセキュア・ページをロックする
645
UVがセキュア・ページを復号し、暗号化されている間に内容が変更されていないことを検証する
650
UVが、セキュア・ページを、共有されているとして所有しているセキュア・ゲスト・ドメインに登録し、HV->HAマッピングをゾーン・セキュリティ・テーブルに登録する
624
UVがページのロックを解除し、セキュア・ページを、所有しているセキュア・ゲスト・ドメインに登録し、HV->HAマッピングをゾーン・セキュリティ・テーブルに登録する
655
ハイパーバイザがゲストを再ディスパッチする
630
セキュア・ゲストがページに正常にアクセスする
635

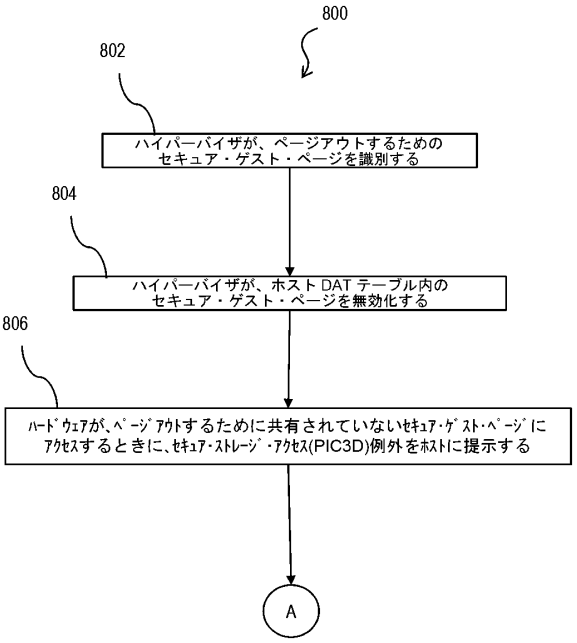
【図７】


700
702
暗号化されたセキュア・ゲスト・ページまたは共有されたセキュア・ゲスト・ページ(ハイパーバイザによってちょうどページインされた)
704
706
共有されているか?
いいえ
はい
708
復号された(「疑いが晴れた状態」である)セキュア・ゲスト・ページ
710
(ハイパーバイザと)共有されたセキュア・ゲスト・ページ

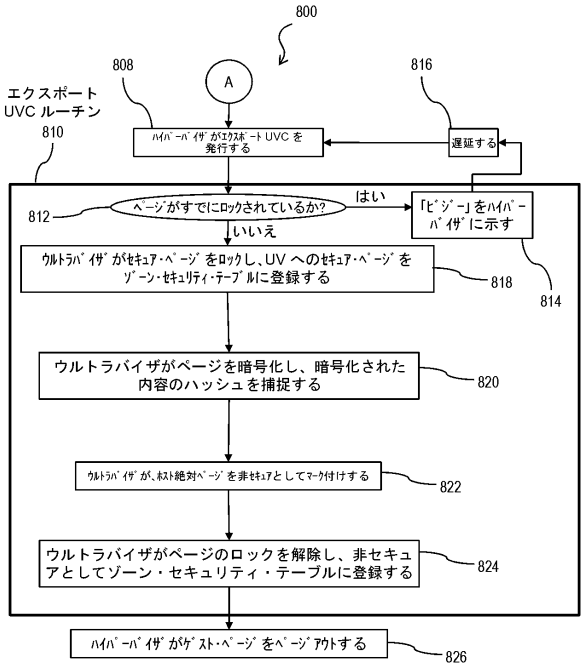
【図８Ａ】


830
831
信頼できない実体がコンピューティング・システムのメモリに格納されたセキュア・ページにアクセスするときに、例外を信頼できない実体に提示し、この例外が、悪意のある信頼できない実体がこのセキュア・ページにアクセスするのを防ぐ
832
エクスポート呼び出しルーチンを発行する
833
エクスポート呼び出しルーチンを実行する

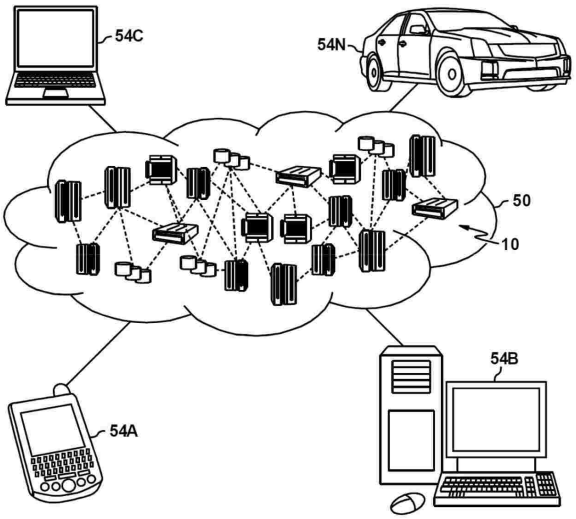
【図８Ｂ】


800
802
ハイパーバイザが、ページアウトするためのセキュア・ゲスト・ページを識別する
804
ハイパーバイザが、ホストDATテーブル内のセキュア・ゲスト・ページを無効化する
806
ハードウェアが、ページアウトするために共有されていないセキュア・ゲスト・ページにアクセスするときに、セキュア・ストレージ・アクセス(PIC3D)例外をホストに提示する
A

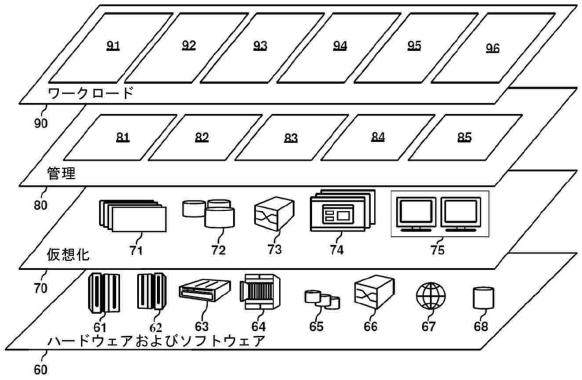
【図８Ｃ】



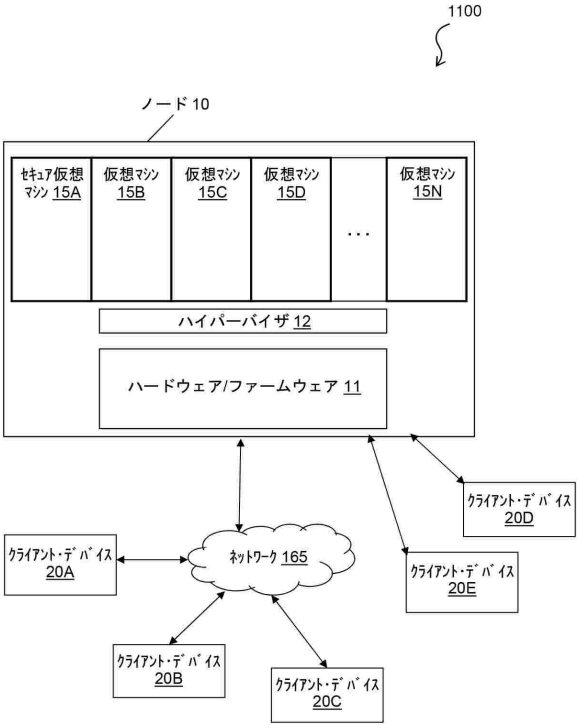
【図９】



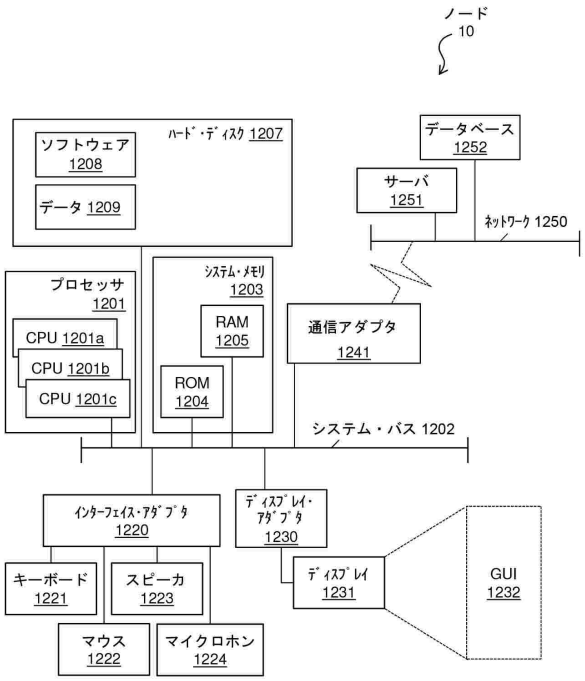
【図１０】



【図１１】



【図１２】


ノード
10
ソフトウェア
1208
ﾊｰﾄﾞ･ﾃﾞｨｽｸ 1207
データ 1209
データベース
1252
サーバ
1251
ﾈｯﾄﾜｰｸ 1250
プロセッサ
1201
CPU 1201a
CPU 1201b
CPU 1201c
ｼｽﾃﾑ･ﾒﾓﾘ
1203
RAM
1205
ROM
1204
通信アダプタ
1241
システム・バス 1202
ｲﾝﾀｰﾌｪｲｽ･ｱﾀﾞﾌﾟﾀ
1220
ﾃﾞｨｽﾌﾟﾚｲ･
ｱﾀﾞﾌﾟﾀ
1230
ｷｰﾎﾞｰﾄﾞ
1221
ｽﾋﾟｰｶ
1223
ﾃﾞｨｽﾌﾟﾚｲ
1231
GUI
1232
ﾏｳｽ
1222
ﾏｲｸﾛﾎﾝ
1224

フロントページの続き

(72)発明者　ブラッドベリー、ジョナサン
アメリカ合衆国１２６０１　ニューヨーク州ポキプシー　サウス・ロード２４５５
(72)発明者　シュヴィデフスキー、マーティン
ドイツ　７１０３２　ベーブリンゲン　シェーナイヒャー・シュトラーセ　２２０
(72)発明者　ボーントレーガー、クリスチャン
ドイツ　７１０３２　ベーブリンゲン　シェーナイヒャー・シュトラーセ　２２０
(72)発明者　ヘラー、リサ
アメリカ合衆国１２６０１　ニューヨーク州ポキプシー　サウス・ロード２４５５
(72)発明者　カーステンス、ハイコ
ドイツ　７１０３２　ベーブリンゲン　シェーナイヒャー・シュトラーセ　２２０
(72)発明者　ブサバ、ファディ
アメリカ合衆国１２６０１　ニューヨーク州ポキプシー　サウス・ロード２４５５

審査官　岸野　徹
(56)参考文献　米国特許出願公開第２０１６／０１３２３４５（ＵＳ，Ａ１）
国際公開第２０１９／００２８１０（WO，Ａ１）
特開２０１０－１７０２１０（ＪＰ，Ａ）
特表２０１６－５２３４２１（ＪＰ，Ａ）
特表２０１８－５０２３７１（ＪＰ，Ａ）
特表２０２０－５２７７７７（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１２／１４
Ｇ０６Ｆ　２１／６０