(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7393846号
(P7393846)

(45)発行日　令和5年12月7日(2023.12.7)

(24)登録日　令和5年11月29日(2023.11.29)

(51)国際特許分類
Ｇ０６Ｆ　12/14　(2006.01)

ＦＩ
Ｇ０６Ｆ　12/14　５１０Ｄ

請求項の数　13　（全42頁）

(21)出願番号　特願2021-549895(P2021-549895)
(86)(22)出願日　令和2年3月6日(2020.3.6)
(65)公表番号　特表2022-523522(P2022-523522A)
(43)公表日　令和4年4月25日(2022.4.25)
(86)国際出願番号　PCT/EP2020/055966
(87)国際公開番号　WO2020/182638
(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　16/296,457
(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】　セキュア・インターフェイス制御の高レベルのページ管理

(57)【特許請求の範囲】
【請求項１】
コンピュータのメモリ内の位置への許可されていないアクセスを防ぐ前記コンピュータのセキュア・インターフェイス制御によって、ホスト絶対ページの保護に従って、前記ホスト絶対ページが仮想ページに以前にマッピングされていないということを決定することと、
前記セキュア・インターフェイス制御によって、前記ホスト絶対ページの保護に従って、ホスト仮想ページが絶対ページにまだマッピングされていないということを決定することと
を含む方法において、
前記セキュア・インターフェイス制御が、関連する前記ホスト絶対ページと共にホスト仮想アドレスを登録して、セキュアな実体によって使用するためのホスト・アドレス対を作成し、前記セキュアな実体によるアクセス時に、前記ホスト仮想アドレスの一致をチェックする、
前記方法。
【請求項２】
前記セキュア・インターフェイス制御が前記ホスト絶対ページをセキュアとしてマーク付けする、請求項１に記載の方法。
【請求項３】
前記セキュア・インターフェイス制御が、前記セキュア・インターフェイス制御によっ

て使用するための前記ホスト絶対ページを登録し、前記ホスト絶対ページを安全に復号し、その後、前記セキュア・インターフェイス制御によって使用するための前記ホスト絶対ページの登録を解除し、前記ホスト絶対ページをセキュア・ドメインに登録する、請求項１または２に記載の方法。

【請求項４】

前記セキュア・インターフェイス制御が、前記セキュア・インターフェイス制御によって使用するための前記ホスト絶対ページをロックし、前記ホスト絶対ページへの他の呼び出しを防ぐ、請求項１ないし３のいずれか一項に記載の方法。

【請求項５】

前記セキュア・インターフェイス制御が、前記ホスト絶対ページのロックを解除し、前記メモリに読み込まれたセキュア・ゲスト・ドメインを割り当てる、請求項１ないし４のいずれか一項に記載の方法。

【請求項６】

前記セキュアな実体が、前記コンピュータ上で実行されている信頼できない実体によって透過的にページインされた、まだ暗号化されているセキュア・ページにアクセスする、請求項１ないし５のいずれか一項に記載の方法。

【請求項７】

前記セキュア・ページが、非セキュアとしてマーク付けされている、請求項６に記載の方法。

【請求項８】

前記信頼できない実体がハイパーバイザであり、前記セキュアな実体がセキュア・ゲストである、請求項６又は７に記載の方法。

【請求項９】

ハードウェアが、セキュア・ゲスト・ページの復号の必要性を示すプログラム割り込みを前記信頼できない実体に提示する、請求項６ないし８のいずれか一項に記載の方法。

【請求項１０】

前記信頼できない実体が、前記ホスト絶対ページおよび前記ホスト仮想ページを提供するインポート命令を発行する、請求項６ないし９のいずれか一項に記載の方法。

【請求項１１】

コンピュータに、請求項１ないし１０のいずれか一項に記載の方法を実行させるためのプログラム。

【請求項１２】

請求項１１に記載のプログラムを記憶した記憶媒体。

【請求項１３】

システムであって、

メモリと、

前記メモリ内の位置への許可されていないアクセスを防ぐ、前記システムのセキュア・インターフェイス制御とを備え、

コンピュータのメモリ内の位置への許可されていないアクセスを防ぐ前記コンピュータのセキュア・インターフェイス制御によって、ホスト絶対ページの保護に従って、前記ホスト絶対ページが仮想ページに以前にマッピングされていないということを決定することと、

前記セキュア・インターフェイス制御によって、前記ホスト絶対ページの保護に従って、ホスト仮想ページが絶対ページにまだマッピングされていないということを決定することとを含む動作を実行し、

前記セキュア・インターフェイス制御が、関連する前記ホスト絶対ページと共にホスト仮想アドレスを登録して、セキュアな実体によって使用するためのホスト・アドレス対を作成し、前記セキュアな実体によるアクセス時に、前記ホスト仮想アドレスの一致をチェックする、

前記システム。

【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、セキュア・インターフェイス制御の高レベルのページ管理に関する。
【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：ｖｅｒｔｕａｌ　ｍａｃｈｉｎｅ）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】

１つまたは複数の実施形態によれば、方法が提供される。コンピュータのセキュア・インターフェイス制御によって、コンピュータのメモリ内の位置への許可されていないアクセスを防ぐ方法が実施される。セキュア・インターフェイス制御は、ホスト絶対ページの保護に従って、ホスト絶対ページが仮想ページに以前にマッピングされておらず、ホスト絶対ページの保護に従って、ホスト仮想ページが絶対ページにまだマッピングされていないということを決定する。本明細書における本発明の１つまたは複数の実施形態の技術的効果および利点としては、すべての非セキュア・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を禁止することが挙げられる。

【０００７】

１つまたは複数の実施形態または上記の方法の実施形態に従って、セキュア・インターフェイス制御は、ホスト絶対ページをセキュアとしてマーク付けすることができる。

【０００８】

１つまたは複数の実施形態または上記の方法の実施形態のいずれかに従って、セキュア・インターフェイス制御は、セキュア・インターフェイス制御によって使用するためのホスト絶対ページを登録し、ホスト絶対ページを安全に復号し、その後、セキュア・インターフェイス制御によって使用するためのホスト絶対ページの登録を解除し、ホスト絶対ページをセキュア・ドメインに登録することができる。

【０００９】

１つまたは複数の実施形態または上記の方法の実施形態のいずれかに従って、セキュア・インターフェイス制御は、関連するホスト絶対ページと共にホスト仮想アドレスを登録して、セキュアな実体によって使用するためのホスト・アドレス対を作成し、セキュアな実体によるアクセス時に、ホスト仮想アドレスの一致をチェックすることができる。

【００１０】

１つまたは複数の実施形態または上記の方法の実施形態のいずれかに従って、セキュア・インターフェイス制御は、セキュア・インターフェイス制御によって使用するためのホスト絶対ページをロックし、ホスト絶対ページへの他の呼び出しを防ぐことができる。本明細書に記載された本発明の１つまたは複数の実施形態の技術的効果および利点としては、ストレージがセキュア・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ているときに、セキュア・ゲスト間のストレージの共有がないことを保証することが挙げられる。

【００１１】

１つまたは複数の実施形態または上記の方法の実施形態のいずれかに従って、セキュア・インターフェイス制御は、ホスト絶対ページのロックを解除し、メモリに読み込まれたセキュア・ゲスト・ドメインを割り当てることができる。本明細書に記載された本発明の１つまたは複数の実施形態の技術的効果および利点としては、ストレージがセキュア・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ているときに、セキュア・ゲスト間のストレージの共有がないことを保証することが挙げられる。

【００１２】

１つまたは複数の実施形態または上記の方法の実施形態のいずれかに従って、セキュアな実体は、コンピュータ上で実行されている信頼できない実体によって透過的にページインされた、非セキュアであるセキュア・ページにアクセスすることができる。

【００１３】

１つまたは複数の実施形態または上記の方法の実施形態のいずれかに従って、信頼できない実体はハイパーバイザであることができ、セキュアな実体はセキュア・ゲストであることができる。本明細書に記載された本発明の１つまたは複数の実施形態の技術的効果および利点としては、いずれかの特定の常駐するセキュア・ゲスト・ページに関して、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マッピングのみを介してアクセス可能であるということを、ハイパーバイザが保証することが挙げられる。

【００１４】

１つまたは複数の実施形態または上記の方法の実施形態のいずれかに従って、ハードウ

ェアは、セキュア・ゲスト・ページの復号の必要性を示すプログラム割り込みを信頼できない実体に提示する。

【００１５】

１つまたは複数の実施形態または上記の方法の実施形態のいずれかに従って、信頼できない実体は、ホスト絶対ページおよびホスト仮想ページを提供するインポート命令を発行することができる。

【００１６】

１つまたは複数の実施形態または上記の方法の実施形態のいずれかに従って、この方法は、コンピュータ・プログラム製品またはシステムあるいはその両方として実装され得る。

【００１７】

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。

【００１８】

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】

【００１９】

【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５】本発明の１つまたは複数の実施形態に従って、動的アドレス変換（ＤＡＴ）動作のシステム概略図である。

【図６】本発明の１つまたは複数の実施形態に従って、セキュア・インターフェイス制御メモリのシステム概略図である。

【図７】本発明の１つまたは複数の実施形態に従って、インポート動作のプロセス・フローを示す図である。

【図８】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９】本発明の１つまたは複数の実施形態に従って、提供されたメモリの動作のプロセスを示す図である。

【図１０】本発明の１つまたは複数の実施形態に従って、セキュア・インターフェイス制御のセキュア・ページへの非セキュア・ハイパーバイザ・ページの遷移のプロセス・フローを示す図である。

【図１１】本発明の１つまたは複数の実施形態に従って、セキュア・インターフェイス制御によって行われるセキュア・ストレージ・アクセスのプロセス・フローを示す図である。

【図１２】本発明の１つまたは複数の実施形態に従って、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るアクセスのタグ付けのプロセス・フローを示す図である。

【図１３】本発明の１つまたは複数の実施形態に従って、プログラムおよびセキュア・インターフェイス制御によってセキュア・アクセスおよび非セキュア・アクセスを支援するための変換のプロセス・フローを示す図である。

【図１４】本発明の１つまたは複数の実施形態に従って、プログラムおよびセキュア・インターフェイス制御によるセキュア・ストレージの保護を伴うＤＡＴのプロセス・フロー

を示す図である。
【図１５】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の高レベルのページ管理のためのプロセス・フローを示す図である。
【図１６】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の高レベルのページ管理のためのプロセス・フローを示す図である。
【図１７】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１８】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１９】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２０】本発明の１つまたは複数の実施形態に従って、ノードを示す図である。
【発明を実施するための形態】
【００２０】
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。
【００２１】
本発明の１つまたは複数の実施形態は、本明細書ではセキュア・インターフェイス制御と呼ばれるセキュリティの追加レイヤを、信頼できない実体の制御下でホスト・コンピュータ上で実行されている仮想マシン（ＶＭ：virtual machines）に提供する。特に、セキュア・インターフェイス制御は、セキュアな実体（例えば、ゲスト、ＶＭ、またはコンテナ）と信頼できない実体（例えば、信頼できないセキュアでない実体、ホスト、ハイパーバイザ、またはＯＳ）の間で、効率的な軽量の信頼できるファームウェア・インターフェイスを活用して、このセキュリティの向上を行う。セキュア・インターフェイス制御は、いずれかのセキュア・ページのホスト仮想アドレスとホスト絶対アドレスの間の登録されたマッピングを維持および使用して、信頼できない実体が、高レベルのセキュリティを引き続き提供しながら、これらのページに関するページ管理機能を提供し続けることができるようにする。これに関して、セキュア・インターフェイス制御がこれらのページのマッピングにおけるセキュリティを保証しながら、セキュア・インターフェイス制御がシャドウ・テーブル（およびシャドウ・テーブルに関連する高い性能上のコスト）を維持することなく、信頼できない実体がセキュア・ゲスト・ページを管理し続けることができるようにするような方法で、セキュア・インターフェイス制御および信頼できない実体がページ管理を提供できるように、新しいインターフェイスが使用される。
【００２２】
本明細書における本発明の１つまたは複数の実施形態の技術的効果および利点としては、すべての非セキュア・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を禁止することが挙げられる。さらに、本明細書に記載された本発明の１つまたは複数の実施形態の技術的効果および利点としては、ハイパーバイザが、いずれかの特定の常駐するセキュア・ゲスト・ページに関して、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マッピングのみを介してアクセス可能である（すなわち、セキュア・ゲストに割り当てられたいずれかの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）ということと、いずれかの特定のセキュア・ゲスト・ページに関連付けられたハイパーバイザのＤＡＴマッピング（ホスト仮想からホスト絶対へのマッピング）が、このページがページインしている間に変化していないことと、いずれかのセキュア・ゲスト・ページに関連付けられたホスト絶対ページが単一のセキュア・ゲストのみに関してマッピングされるということとを、ハイパーバイザが保証する

ことが挙げられる。さらに、ストレージが、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ているときに、セキュア・ゲスト間のストレージの共有が存在しない。

【００２３】

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）（例えば、信頼できない実体）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）。

【００２４】

セキュア・ゲスト（例えば、セキュアな実体）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、したがって本明細書に記載され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。

【００２５】

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ウルトラバイザという用語は、本明細書では交換可能なように使用され得る。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。

【００２６】

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ｚＡａｒｃｈｉｔｅｃｔｕｒｅ（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。

【００２７】

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、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。

【００２８】

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、ＵＶ呼び出し（ＵＶＣ：UVCall）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。

【００２９】

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、セキュア・ゲスト・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。

【００３０】

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。

【００３１】

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を発行しなければならない。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。

【００３２】

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。

【００３３】

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。

【００３４】

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。

【００３５】

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。

【００３６】

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。

【００３７】

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。

【００３８】

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）Ａ２０８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．Ａ２２０ａ２、およびＡ３．Ａ２２０ａ３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。

【００３９】

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．ＧＶ３２０ｂ２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。

【００４０】

本明細書に記載された本発明の実施形態は、セキュア・ゲストおよびＵＶ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。

【００４１】

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。ＵＶストレージは、セキュア・ストレージであり、セキュア制御インターフェイスによってアクセス可能であるが、ゲスト／ホストによるアクセスは不可能である。ストレージは、ハイパーバイザによってセキュア制御インターフェイスに割り当てられる。本発明の１つまたは複数の実施形態によれば、これらのルールの試みられたすべての違反が、ハードウェアおよびセキュア制御インターフェイスによって禁止される。

【００４２】

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。

【００４３】

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ＵＶ呼び出し（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。

【００４４】

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。

【００４５】

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。

【００４６】

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。

【００４７】

ここで図５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動作のシステム概略図５００が概して示されている。システム概略図５００は、一次ホスト仮想アドレス空間（host primary virtual address space）５１０およびホーム・ホスト仮想アドレス空間（host home virtual address space）５２０を含んでおり、これらの仮想アドレス空間のページが、ハイパーバイザ（ホスト）絶対アドレス空間５３０に変換される（例えば、ホストＤＡＴ変換５２５を参照（点線がＤＡＴ変換５２５によるマッピングを表していることに注意する））。例えば、図５は、２つの異なるホスト仮想アドレ

ス空間によるホスト絶対ストレージの共有を示しており、２つのゲスト間だけでなく、ホスト自体とのそれらのホスト仮想アドレスのうちの１つの共有も示している。これに関して、一次ホスト仮想アドレス空間５１０およびホーム・ホスト仮想アドレス空間５２０は、２つのホスト仮想アドレス空間の例であり、これらのホスト仮想アドレス空間の各々は、別々のＡＳＣＥ（一次ホストＡＳＣＥ（ＨＰＡＳＣＥ：host primary ASCE）５９１およびホーム・ホストＡＳＣＥ（ＨＨＡＳＣＥ：host home ASC）５９２）によってそれぞれアドレス指定される。すべてのセキュア・インターフェイス制御のストレージ（仮想および現実の両方）が、ハイパーバイザによって提供され、セキュアとしてマーク付けされるということに注意する。セキュア・インターフェイス制御のストレージは、提供された後に、関連するセキュアな実体が存在する限り、セキュア・インターフェイス制御のみによってアクセスされ得る。

【００４８】

図に示されているように、一次ホスト仮想アドレス空間５１０は、ゲストＡの絶対ページＡ１．ＨＶ、ゲストＡの絶対ページＡ２．ＨＶ、ゲストＢの絶対ページＢ１．ＨＶ、およびホスト仮想ページＨ３．ＨＶを含んでいる。ホーム・ホスト仮想アドレス空間５２０は、セキュア・インターフェイス制御の仮想ページＵ１．ＨＶ、ホスト仮想ページＨ１．ＨＶ、およびホスト仮想ページＨ２．ＨＶを含んでいる。

【００４９】

本発明の１つまたは複数の実施形態に従って、すべてのセキュア・ゲスト（例えば、セキュア・ゲストＡおよびセキュア・ゲストＢ）ストレージが、本明細書に記載されたゾーン・セキュリティ・テーブルに、セキュア・ゲスト構成に属しているとして登録され、関連するホスト仮想アドレス（例えば、Ａ１．ＨＶ、Ａ２．ＨＶ、Ｂ１．ＨＶ）も、ホスト・アドレス対の一部として登録される。１つまたは複数の実施形態では、すべてのセキュア・ゲスト・ストレージが、一次ホスト仮想空間内でマッピングされる。加えて、すべてのセキュア・インターフェイス制御のストレージが、やはりゾーン・セキュリティ・テーブルに、セキュア・インターフェイス制御に属しているとして登録され、関連するセキュア・ゲスト・ドメインに基づいて、ゾーン・セキュリティ・テーブル内でさら区別されてよい。本発明の１つまたは複数の実施形態に従って、ＵＶ仮想ストレージが、ホーム・ホスト仮想空間（host home virtual space）内でマッピングされ、関連するホスト仮想アドレスがホスト・アドレス対の一部として登録される。１つまたは複数の実施形態に従って、ＵＶ実ストレージが、関連するホスト仮想マッピングを有しておらず、ゾーン・セキュリティ・テーブル内のＤＡビット（仮想アドレスの比較が無効化されることを示す）が、そのことを示すように設定される。ホスト・ストレージが、非セキュアとしてマーク付けされ、非セキュアとしてゾーン・セキュリティ・テーブルにも登録される。

【００５０】

したがって、「ゲスト絶対＝ホスト仮想」である場合、ハイパーバイザ（ホスト）一次ＤＡＴテーブル（ＨＰＡＳＣＥ５９１によって定義される）は、一次ホスト仮想アドレス空間５１０のページを、次のように変換する。ゲストＡの絶対ページＡ１．ＨＶが、セキュア・ゲストＡに属しているホスト絶対Ａ１．ＨＡにマッピングされ、ゲストＡの絶対ページＡ２．ＨＶが、セキュア・ゲストＡに属しているホスト絶対Ａ２．ＨＡにマッピングされ、ゲストＢの絶対ページＢ１．ＨＡが、セキュア・ゲストＢに属しているホスト絶対Ｂ１．ＨＡにマッピングされ、ホスト仮想ページＨ３．ＨＶが、ホスト絶対ページＨ３．ＨＡ　非セキュア・ホストにマッピングされる（非セキュアであるため、ホスト・アドレス対が存在しない）。さらに、ハイパーバイザ（ホスト）ホームＤＡＴテーブル（ＨＨＡＳＣＥ５９２によって定義される）が、ホーム・ホスト仮想アドレス空間５２０のページを、次のように変換する。セキュア・インターフェイス制御の仮想ページＵ１．ＨＶが、セキュアＵＶ仮想として定義されたホスト絶対ページＵ１．ＨＡにマッピングされ、ホスト仮想ページＨ１．ＨＶが、非セキュアとして定義されたホスト絶対ページＨ１．ＨＡにマッピングされ、ホスト仮想ページＨ２．ＨＶが、非セキュアとして定義されたホスト絶対ページＨ２．ＨＡにマッピングされる。Ｈ１．ＨＡおよびＨ２．ＨＡは非セキュアであ

るため、これらのいずれかに関連付けられたホスト・アドレス対は存在しない。

【００５１】

動作中に、セキュア・ゲストが、セキュア・インターフェイス制御に割り当てられたセキュア・ページにアクセスしようとした場合、ハードウェアによってセキュア・ストレージ違反（「３Ｆ」Ｘ）例外がハイパーバイザに提示される。非セキュア・ゲストまたはハイパーバイザが、いずれかのセキュア・ページ（セキュア・インターフェイス制御に割り当てられたセキュア・ページを含む）にアクセスしようとした場合、ハードウェアによってセキュア・ストレージ・アクセス（「３Ｄ」Ｘ）例外がハイパーバイザに提示される。代替として、セキュア・インターフェイス制御の空間に対して試みられたアクセスに関して、エラー状態が提示され得る。ハードウェアが、セキュア・インターフェイス制御のアクセス時に、セキュアな割り当てにおいて不一致を検出した場合（例えば、ストレージが、セキュア・インターフェイス制御ではなくセキュア・ゲストに属しているとしてゾーン・セキュリティ・テーブルに登録されたか、または使用されているホスト・アドレス対に、登録済みの対との不一致が存在する場合）、チェックが提示される。

【００５２】

言い換えると、一次ホスト仮想アドレス空間５１０は、ホスト仮想ページＡ１．ＨＶおよびＡ２．ＨＶ（セキュア・ゲストＡに属している）ならびにＢ１．ＨＶ（セキュア・ゲストＢに属している）を含んでおり、これらのホスト仮想ページは、ホスト絶対Ａ１．ＨＡ、Ａ２．ＨＡ、およびＢ１．ＨＡにそれぞれマッピングされる。加えて、一次ホスト仮想アドレス空間５１０は、ホスト絶対Ｈ３．ＨＡにマッピングされるホスト（ハイパーバイザ）ページＨ３．ＨＶを含んでいる。ホーム・ホスト仮想空間５２０は、ホスト絶対ページＨ１．ＨＡおよびＨ２．ＨＡにマッピングされる２つのホスト仮想ページＨ１．ＨＶおよびＨ２．ＨＶを含んでいる。一次ホスト仮想アドレス空間５１０およびホーム・ホスト仮想アドレス空間５２０の両方は、単一のホスト絶対５３０にマッピングされる。セキュア・ゲストＡおよびセキュア・ゲストＢに属しているストレージ・ページは、セキュアとしてマーク付けされ、それらのセキュア・ドメインおよび関連するホスト仮想アドレスと共に、図１に示されているゾーン・セキュリティ・テーブル１００に登録される。一方、ホスト・ストレージは、非セキュアとしてマーク付けされる。ハイパーバイザは、セキュア・ゲストを定義している場合、これらのセキュア・ゲストの支援において必要なセキュア制御ブロック（secure control blocks）に使用するために、ホスト・ストレージをセキュア・インターフェイス制御に提供しなければならない。このストレージは、ホスト絶対空間またはホスト仮想空間のいずれかにおいて、および１つの例では、特に、ホーム・ホスト仮想空間において定義され得る。図５に戻り、ホスト絶対ページＵ１．ＨＡおよびＵ２．ＨＡ　セキュアＵＶ絶対は、ホスト絶対ストレージとして定義されているセキュア・インターフェイス制御のストレージである。その結果、これらのページは、セキュアとしてマーク付けされ、セキュア・インターフェイス制御に属しているとして、関連するセキュア・ドメインと共に、図１に示されているゾーン・セキュリティ・テーブル１００に登録される。これらのページはホスト絶対アドレスとして定義されるため、関連するホスト仮想アドレスが存在せず、そのためゾーン・セキュリティ・テーブル１００内のＤＡビットが設定される。

【００５３】

変換後のハイパーバイザ（ホスト）絶対アドレス空間５３０の例が、図６で見出すことができる。図６では、本発明の１つまたは複数の実施形態に従って、セキュア・インターフェイス制御メモリに関するシステム概略図６００が示されている。システム概略図６００は、ホスト絶対ページＡ２．ＨＡ　セキュア・ゲストＡ（Ａ２．ＨＶ用）、ホスト絶対ページＢ１．ＨＡ　セキュア・ゲストＢ（Ｂ１．ＨＶ用）、ホスト絶対ページＨ１．ＨＡ　非セキュア（ホスト）、ホスト絶対ページＨ２．ＨＡ　非セキュア（ホスト）、ホスト絶対ページＵ３．ＨＡ　セキュアＵＶ現実（ＨＶマッピングなし）、ホスト絶対ページＵ１．ＨＡ　セキュアＵＶ仮想（Ｕ１．ＨＶ用）、およびホスト絶対ページＡ１．ＨＡ　セキュア・ゲストＡ（Ａ１．ＨＶ用）を含んでいるハイパーバイザ（ホスト）絶対アドレス空間

６３０を示している。
【００５４】
ここで図７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７００が概して示されている。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７００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７００はブロック７０５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７１５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７２０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７２５を参照）。
【００５５】
ブロック７３０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７３５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７４０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７４５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７００は、図８に接続されている「Ａ」に進む。
【００５６】
ここで図８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８００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８０５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。
【００５７】
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８１０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８００がブロック８２０に進む。ブロック８２０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８２５を参照）、インポートＵＶＣを再発行する（プロセス・フロー８００がブロック８０５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８００が判定ブロック８２２に進む。
【００５８】
判定ブロック８２２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８００が判定ブロック８２４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８３０）、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８３５）に進む。

【００５９】

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８００がブロック８４０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８４５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８５０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。

【００６０】

ブロック８５５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。

【００６１】

ここで図９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、提供されたメモリの動作に関するプロセス・フロー９００が概して示されている。プロセス・フロー９００はブロック９０５で開始し、ブロック９０５で、ハイパーバイザが照会ＵＶＣをセキュア・インターフェイス制御に発行する。ブロック９１０で、セキュア・インターフェイス制御がデータ（例えば、照会ＵＶＣ）を返す。このデータは、ゾーン固有のベース・ホスト絶対ストレージの必要な量、セキュア・ゲスト・ドメイン固有のベース・ホスト絶対ストレージの必要な量、ＭＢごとのセキュア・ゲスト・ドメイン固有の可変ホスト仮想ストレージの必要な量、またはセキュア・ゲストＣＰＵ固有のベース・ホスト絶対ストレージの必要な量、あるいはその組み合わせを含むことができる。

【００６２】

ブロック９１５で、ハイパーバイザは、ホスト絶対ゾーン固有のベース・ストレージを（例えば、照会ＵＶＣによって返されたサイズに基づいて）確保する。ブロック９２０で、ハイパーバイザが、初期化をセキュア・インターフェイス制御に発行する。これに関して、ハイパーバイザは、ゾーン全体のセキュア・ゲスト構成間の調整に必要とされるＵＶ制御ブロックのために提供されるストレージを提供する、初期化ＵＶＣを発行することができる。初期化ＵＶＣは、ゾーン固有のベース・ストレージの原点を指定する。

【００６３】

ブロック９２５で、セキュア・インターフェイス制御が、提供されたストレージをＵＶに登録し、セキュアとしてマーク付けすることによって、初期化（例えば、初期化ＵＶＣ）を実施する。初期化ＵＶＣの場合、セキュア・インターフェイス制御は、提供されたストレージをセキュアとしてマーク付けし、その提供されたストレージの一部をゾーン・セキュリティ・テーブルに割り当て、提供されたストレージを、一意のセキュア・ドメインと共に、ただし関連するセキュア・ゲスト・ドメインなしで、関連するホスト仮想アドレス対を有していないとして、ＵＶ使用のためのゾーン・セキュリティ・テーブルに登録することができる。

【００６４】

ブロック９３０で、ハイパーバイザがストレージ（例えば、セキュア・ゲスト・ドメイン固有のベースおよび可変ストレージ）を確保する。例えば、ハイパーバイザは、（例えば、セキュア・ゲスト・ドメインのストレージのサイズに基づいて）セキュア・ゲスト・ドメイン固有のベースおよび可変ストレージ（例えば、照会ＵＶＣによって返されたサイズ）を確保する。ブロック９３５で、ハイパーバイザが、構成作成をセキュア・インター

フェイス制御に発行する。これに関して、ハイパーバイザは、セキュア・ゲスト・ドメイン固有のベースおよび可変ストレージの原点を指定するセキュア・ゲスト構成作成ＵＶＣを発行することができる。さらに、セキュア・ゲスト構成作成ＵＶＣは、このセキュア・ゲスト構成を支援するために必要なＵＶ制御ブロックのために提供されるストレージを提供する。

【００６５】

ブロック９４０で、セキュア・インターフェイス制御が、構成作成（例えば、セキュア・ゲスト構成作成ＵＶＣ）を実施する。セキュア・ゲスト構成作成ＵＶＣの場合、セキュア・インターフェイス制御は、提供されたストレージをセキュアとしてマーク付けし、提供されたストレージをＵＶ使用のためのゾーン・セキュリティ・テーブルに登録し、提供されたストレージを関連するセキュア・ゲスト・ドメインと共に登録することができる。提供されたベース（ホスト絶対）ストレージは、関連するホスト仮想アドレス対を有していないとして登録される。提供された可変（ホスト仮想）ストレージは、関連するホスト仮想アドレス対と共に登録される。

【００６６】

ブロック９４５で、ハイパーバイザは、セキュア・ゲストＣＰＵ固有のベース・ストレージ（例えば、照会ＵＶによって返されたサイズ）を確保する。ブロック９５０で、ハイパーバイザがストレージの原点を指定する。例えば、ハイパーバイザは、セキュア・ゲストＣＰＵ固有のベース・ストレージの原点を指定するセキュア・ゲストＣＰＵ作成をＵＶに発行する。ブロック９５５で、セキュア・インターフェイス制御が、ＣＰＵ作成（例えば、セキュア・ゲストＣＰＵ作成ＵＶＣ）を実施する。セキュア・ゲストＣＰＵ作成ＵＶＣの場合、セキュア・インターフェイス制御は、提供されたストレージをセキュアとしてマーク付けし、提供されたストレージを、関連するセキュア・ゲスト・ドメインなしで、関連するホスト仮想アドレス対を有していないとして、ＵＶ使用のためのゾーン・セキュリティ・テーブルに登録することができる。

【００６７】

ここで図１０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・インターフェイス制御のセキュア・ページへの非セキュア・ハイパーバイザ・ページの遷移に関するプロセス・フロー１０００が概して示されている。プロセス・フロー１０００では、３つのハイパーバイザのページ（例えば、非セキュア・ハイパーバイザのページＡ、非セキュア・ハイパーバイザのページＢ、および非セキュア・ハイパーバイザのページＣ）が示されている。

【００６８】

ハイパーバイザ（非セキュア）のページＡ、Ｂ、およびＣ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。さらに、ハイパーバイザ（非セキュア）のページＡ、Ｂ、およびＣは、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（例えば、図１に示されているゾーン・セキュリティ・テーブル１００）に登録されるのと同時に、非セキュアとして（ＮＳ：non-secure）としてマーク付けされる。矢印１００５で、初期化ＵＶＣが発行され、ゲスト・ページＡを、ゾーン全体（ＵＶ２）に関連付けられたセキュア・インターフェイス制御の実ストレージ・ページ１０１０に遷移させる。セキュア・インターフェイス制御の実ストレージ１０１０は、ＵＶとして、セキュア・ゲスト・ドメインなし、かつ絶対（ＨＶ－＞ＨＡ）マッピングをホストするためのハイパーバイザなしで、ゾーン・セキュリティ・テーブル（例えば、図１に示されているゾーン・セキュリティ・テーブル１００）に登録されるのと同時に、セキュアとしてとしてマーク付けされ得る。代わりに、実ストレージ１０１０は、一意のＵＶ２セキュア・ドメインと共に登録され、ＤＡビットが１に設定される。セキュア・インターフェイス制御の実ストレージ１０１０が、セキュア・インターフェイス制御によって現実としてアクセスされ得るということに注意する。

【００６９】

ハイパーバイザ（非セキュア）のページＢから、矢印１０２５で、ＳＧ構成作成または

ＳＧ－ＣＰＵ作成ＵＶＣが発行され、このページを、セキュア・ゲスト・ドメイン（ＵＶＳ）に関連付けられたセキュア・インターフェイス制御の実ストレージ１０３０に遷移させる。セキュア・インターフェイス制御の実ストレージ１０３０は、ＵＶとして、関連するセキュア・ゲスト・ドメインと共に、絶対（ＨＶ－＞ＨＡ）マッピングをホストするためのハイパーバイザなし（すなわち、ＤＡビット＝１）で、ゾーン・セキュリティ・テーブル（例えば、図１に示されているゾーン・セキュリティ・テーブル１００）に登録されるのと同時に、セキュアとしてとしてマーク付けされ得る。セキュア・インターフェイス制御の実ストレージ１０１０が、セキュア・ゲスト・ドメインの代わりに、セキュア・インターフェイス制御によって現実としてアクセスされ得るということに注意する。

【００７０】

ハイパーバイザ（非セキュア）のページＣから、矢印１０４５で、ＳＧ構成作成ＵＶＣが発行され、このページを、セキュア・ゲスト・ドメイン（ＵＶＶ）に関連付けられたセキュア・インターフェイス制御の仮想ストレージ１０５０に遷移させる。セキュア・インターフェイス制御の仮想ストレージ１０５０は、ＵＶとして、セキュア・ゲスト・ドメイン、および絶対（ＨＶ－＞ＨＡ）マッピングをホストするためのハイパーバイザと共に、ゾーン・セキュリティ・テーブル（例えば、図１に示されているゾーン・セキュリティ・テーブル１００）に登録されるのと同時に、セキュアとしてとしてマーク付けされ得る。セキュア・インターフェイス制御の仮想ストレージ１０５０が、セキュア・ゲスト・ドメインの代わりに、ＵＶ仮想としてアクセスされ得るということに注意する。

【００７１】

ここで図１１を参照すると、１つまたは複数の実施形態に従って、プログラムまたはセキュア・インターフェイス制御によって行われるセキュア・ストレージ・アクセスに関するプロセス・フロー１１００が示されている。この図は、セキュア・インターフェイス制御がゲスト・ストレージまたはセキュア・インターフェイス制御のストレージにアクセスしようとしており、ハードウェアがそのアクセスのセキュリティを検証できるようにするために、そのアクセスに正しくタグ付けしなければならない状況を表している。１１００は、セキュア・インターフェイス制御によるストレージ・アクセスのこのタグ付けを表している。プロセス・フロー１１００はブロック１１１０で開始し、ブロック１１１０で、セキュア・インターフェイス制御が、セキュア・インターフェイス制御のストレージへのアクセスを行っているかどうかを判定する。

【００７２】

このアクセスが、セキュア・インターフェイス制御のストレージへのアクセスでない場合、プロセス・フロー１１００が判定ブロック１１１２に進む（「いいえ」の矢印で示されている）。判定ブロック１１１２で、セキュア・インターフェイス制御が、セキュア・ゲスト・ストレージへのアクセスを行っているかどうかを判定する。このアクセスが、セキュア・ゲスト・ストレージへのアクセスでない場合、プロセス・フロー１１００が、非セキュア・アクセスのデフォルト設定を使用する「Ｂ」（図１２のプロセス・フロー１２００に接続されている）に進む。このアクセスが、セキュア・ゲスト・ストレージへのアクセスである場合、プロセス・フロー１１００が判定ブロック１１１３に進み、判定ブロック１１１３で、セキュア・インターフェイス制御が、デフォルトのセキュア・ゲスト・ドメインが使用されているかどうかを判定する。デフォルトのセキュア・ゲスト・ドメインが使用されている場合、プロセス・フロー１１００が、セキュア・ゲスト・アクセスのデフォルト設定を使用する「Ｂ」（図１２のプロセス・フロー１２００に接続されている）に進む。デフォルトのセキュア・ゲスト・ドメインが使用されていない場合、プロセス・フロー１１００がブロック１１１４に進む。ブロック１１１４で、適切なセキュア・ゲスト・ドメインがＳＧセキュア・ドメイン・レジスタに読み込まれる（図１２のプロセス・フロー１２００に接続されている「Ｂ」に進む）。

【００７３】

このアクセスが、セキュア・インターフェイス制御のストレージへのアクセスである場合、プロセス・フロー１１００がブロック１１２０に進む（「はい」の矢印で示されてい

る）。ブロック１１２０で、アクセスが、セキュアＵＶとしてタグ付けされる（例えば、ＵＶセキュア・ドメイン・レジスタを使用する）。

【００７４】

次に、プロセス・フロー１１００が判定ブロック１１３０に進み、判定ブロック１１３０で、セキュア・インターフェイス制御が、このアクセスがＵＶＶ空間（例えば、ＳＧ構成可変テーブル）へのアクセスであるかどうかを判定する。このアクセスがＵＶＶ空間へのアクセスである場合、プロセス・フロー１１００がブロック１１３４に進む（「はい」の矢印で示されている）。ブロック１１３４で、アクセスが仮想としてタグ付けされる。ブロック１１３６で、適用可能なセキュア・ゲスト・ドメインがＵＶセキュア・ドメイン・レジスタに読み込まれる。ブロック１１３８で、ＤＡＴ変換およびストレージ・アクセスを開始する準備ができる。判定ブロック１１３０に戻り、このアクセスがＵＶＶ空間へのアクセスでない場合、プロセス・フロー１１００がブロック１１４０に進む（「いいえ」の矢印で示されている）。ブロック１１４０で、アクセスが現実としてタグ付けされる。

【００７５】

判定ブロック１１５０で、セキュア・インターフェイス制御が、このアクセスがＵＶＳ空間（例えば、ＳＧ構成またはＣＰＵテーブル）へのアクセスであるかどうかを判定する。このアクセスがＵＶＳ空間へのアクセスである場合、プロセス・フロー１１００がブロック１１３６に進む（「はい」の矢印で示されている）。このアクセスがＵＶＳ空間へのアクセスでない場合、プロセス・フロー１１００がブロック１１７０に進む（「いいえ」の矢印で示されている）。このアクセスは、ＵＶ２空間（例えば、ゾーン・セキュリティ・テーブル）へのアクセスである。ブロック１１７０で、一意のＵＶ２セキュア・ドメインがＵＶセキュア・ドメイン・レジスタに読み込まれる。

【００７６】

図１２は、本発明の１つまたは複数の実施形態に従って、プロセス・フロー１２００を示している。ゲストがディスパッチされるときに、ＳＩＥエントリ・ファームウェア（SIE Entry firmware）が、ゲストが実行中である（例えば、ゲスト・モードが有効である）ことをハードウェアに示すことができ、ゲストがセキュアであるかどうかを示すことができる。ゲストがセキュアである場合、関連するセキュア・ゲスト・ドメインがハードウェア（例えば、ＳＧセキュア・ドメイン・レジスタ）に読み込まれ得る。プログラムがストレージにアクセスしているときに、ハードウェアが、アクセスの時点でのプログラムの現在の状態に基づいてアクセスにタグ付けすることができる。図１２は、このプロセスの例をプロセス・フロー１２００に示している。ブロック１２０５で、ハードウェアが、マシンがゲスト・モードで現在実行中であるかどうかを判定し、ゲスト・モードで実行中でない場合、ブロック１２１０でホストのアクセスであるとして、およびブロック１２１５で非セキュア・アクセスであるとして、アクセスにタグ付けすることができる。ブロック１２０５で、マシンがゲスト・モードで実行中である場合、ブロック１２２０で、ゲストのアクセスとしてアクセスにタグ付けすることができ、ブロック１２２５で、現在のゲストがセキュア・ゲストであるかどうかをさらに判定する。ゲストがセキュアでない場合、ブロック１２１５で、非セキュアとしてアクセスにタグ付けすることができる。ゲストがセキュアである場合、ブロック１２３０で、ハードウェアがセキュアとしてゲストにタグ付けすることができ、セキュア・ゲストがディスパッチされたときに読み込まれたＳＧセキュア・ドメイン・レジスタに、セキュア・ゲストを関連付けることができる。ブロック１２３５で、非セキュア・ゲストおよびセキュア・ゲストの両方に関して、ＤＡＴの状態をチェックすることができる。ＤＡＴがオフである場合、ブロック１２４０で、現実としてアクセスにタグ付けすることができる。ＤＡＴがオンである場合、ブロック１２４５で、仮想としてアクセスにタグ付けすることができる。アクセスが、ＤＡＴがオフの場合に、ブロック１２４０で現実としてタグ付けされるか、またはＤＡＴがオンの場合に、ブロック１２４５で仮想としてタグ付けされた後に、ブロック１２５０で、ハードウェアは、図１３でさら説明されるように、変換およびストレージ・アクセスを開始する準備ができる。

【００７７】

図１３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・アクセスおよび非セキュア・アクセスの両方を支援するためにハードウェアによって実行される変換の例をプロセス・フロー１３００に示している。ブロック１３０５で、ハードウェアは、アクセスがゲスト変換としてタグ付けされているかどうかを判定することができ、アクセスがゲスト変換としてタグ付けされており、ブロック１３１０で、アクセスが仮想である場合、ブロック１３１５で、ゲストＤＡＴが実行され得る。ゲストＤＡＴ変換の間に、ゲストＤＡＴテーブルに対するネストされた中間フェッチが存在することができる。テーブルのフェッチが、ゲスト現実として、および元の変換がセキュアとしてタグ付けされている場合はセキュアとして、タグ付けされ得る。テーブルのフェッチも、プロセス・フロー１３００の変換プロセスに従うことができる。ブロック１３１５で、ゲスト仮想としてタグ付けされたアクセスに対してゲストＤＡＴが実行され、ブロック１３１０で、ゲスト現実（仮想＝いいえ）としてタグ付けされたアクセスに対してゲストＤＡＴが実行された後に、ブロック１３２０で、ゲスト・プレフィックス変換およびゲスト・メモリ・オフセットが適用され得る。ゲスト変換プロセスの完了時に、ブロック１３２５で、得られたアドレスが、ホスト仮想として、および元のゲスト変換がセキュアとしてタグ付けされている場合はセキュアとして、タグ付けされ得る。プロセス１３００は、ホスト仮想としてタグ付けされた任意のアクセスに関して、続行することができる。元のアクセスが、ブロック１３０５でホストのアクセスであり（ゲスト＝いいえ）、ブロック１３３０で仮想である場合、ブロック１３３５でホストＤＡＴが実行され得る。ブロック１３３５で、ホストのテーブルのフェッチが非セキュアとしてマーク付けされ得る。ブロック１３３５でホストＤＡＴが実行された後に、またはブロック１３３０で元のホストのアクセスが現実（仮想＝いいえ）としてタグ付けされた場合に、ブロック１３４０でホスト・プレフィックス変換が適用され得る。ブロック１３４５で、得られたアドレスは、ホスト絶対アドレスであることができる。

【００７８】

図１４は、本発明の１つまたは複数の実施形態に従って、ハードウェアによって実行され得るセキュア・ストレージ保護を伴うＤＡＴ変換の例をプロセス・フロー１４００に示している。図１３のブロック１３４５から続けて、ブロック１４０５で、セキュアＵＶアクセスが識別された場合、ブロック１４１０で、ハードウェアは、ストレージがセキュアＵＶストレージとして登録されているかどうかを検証することができ、ストレージがセキュアＵＶストレージとして登録されていない場合、ブロック１４１５でエラーが提示される。ＵＶストレージにアクセスしている場合、セキュア制御インターフェイスによってセキュアＵＶアクセスが行われ得る。ブロック１４１０で、ストレージがセキュアＵＶストレージとして登録されている場合、任意のセキュア・アクセスに対して実行されるように、保護チェックが継続することができるが、処理が継続する場合、ブロック１４２０で、ＵＶセキュア・ドメイン・レジスタ（セキュアＵＶアクセスを行う前にセキュア制御インターフェイスによって設定される）が、ドメイン・チェックのために指定されたセキュア・ドメインとして使用され得るという点が異なる。加えて、ブロック１４２５でセキュア・ゲスト違反（セキュアＵＶ＝いいえ）に対して実行されるような、ブロック１４３５でのハイパーバイザへの例外ではなく、ブロック１４２５でＵＶアクセスに対して検出された任意の違反（エントリ・ポイントＤ）が、ブロック１４３０でエラーとして提示され得る。

【００７９】

ブロック１４０５でセキュアＵＶアクセスとしてタグ付けされていないアクセスの場合、ブロック１４４０で、ハードウェアは、アクセスがセキュア・ゲストのアクセスであるかどうかを判定し、アクセスがセキュア・ゲストのアクセスでなく、かつブロック１４４５でページがセキュアとしてマーク付けされている場合、ブロック１４３５で、例外がハイパーバイザに提示され得る。しかし、ブロック１４４０でアクセスがセキュア・ゲストのアクセスではなく、ブロック１４４５でページがセキュアとしてマーク付けされていない場合、ブロック１４５０で変換が成功する。

【００８０】
アクセスが、ブロック１４４０で、セキュア・ゲストのアクセスであるか、またはブロック１４１０で、セキュアＵＶストレージとして登録されたストレージへのセキュアＵＶアクセスである場合、ブロック１４２０で、ハードウェアは、ストレージがアクセスに関連付けられたセキュアな実体に登録されていることをチェックして確認することができる。アクセスがセキュアＵＶアクセスである場合、指定されたセキュア・ドメインをＵＶセキュア・ドメイン・レジスタから取得することができ（セキュアＵＶストレージがアクセスされているということに基づいて、セキュア制御インターフェイスによって読み込まれる）、セキュア・ゲストのアクセスの場合、指定されたセキュア・ドメインをＳＧセキュア・ドメイン・レジスタから取得することができる（セキュアな実体がディスパッチされるときに読み込まれる）。ブロック１４２０で、アクセスされているストレージが指定されたセキュア・ドメインに登録されていない場合、ブロック１４２５でセキュアＵＶアクセスである場合は、ブロック１４３０でエラーが選択され、ブロック１４２５でセキュア・ゲストのアクセス（セキュアＵＶ＝いいえ）である場合は、ブロック１４３５で例外がハイパーバイザに提示される。
【００８１】
ブロック１４２０で指定されたセキュア・ドメインに登録された、ブロック１４４０およびブロック１４１０でのストレージへのセキュア・アクセスに関して、ブロック１４５５で仮想アドレス・チェックが無効化されている（すなわち、ＤＡビット＝１）であり、かつブロック１４６０でアクセスが現実である場合、ブロック１４５０で変換が完了する。しかし、ブロック１４５５でＤＡビット＝１であるが、ブロック１４６０でアクセスが仮想（現実＝いいえ）である場合、ブロック１４２５でセキュアＵＶアクセスである場合は、ブロック１４３０でエラーが選択され、ブロック１４２５でセキュア・ゲストのアクセス（セキュアＵＶ＝いいえ）である場合は、ブロック１４３５で例外がハイパーバイザに提示される。ブロック１４５５でＤＡビット＝０であり、かつブロック１４７５でアクセスが仮想アクセスである場合、ブロック１４７０で、ハードウェアは、ホスト仮想からホスト絶対へのアクセスのマッピングが、このホスト絶対アドレスに関して登録されているマッピングに一致するかどうかを判定することができる。一致する場合、ブロック１４５０で変換が正常に完了する。ブロック１４７０で、マッピングが一致しない場合、ブロック１４２５でセキュアＵＶアクセスである場合は、ブロック１４３０でエラーが選択され、ブロック１４２５でセキュア・ゲストのアクセス（セキュアＵＶ＝いいえ）である場合は、ブロック１４３５で例外がハイパーバイザに提示される。ＤＡビット＝０であり、かつブロック１４７５でアクセスが現実のアクセス（仮想＝いいえ）である場合、ブロック１４２５でセキュアＵＶアクセスである場合は、ブロック１４３０でエラーが選択され、ブロック１４２５でセキュア・ゲストのアクセス（セキュアＵＶ＝いいえ）である場合は、ブロック１４３５で例外がハイパーバイザに提示され、代替として、ブロック１４５０で変換が正常に完了してよい。ブロック１４８０でのＩ／Ｏサブシステムによるアクセスは、ブロック１４４５でページがセキュアとしてマーク付けされているかどうかをチェックして確認することができ、ページがセキュアである場合、ブロック１４３５で例外をハイパーバイザに提示することができ、ページがセキュアとしてマーク付けされていない場合、ブロック１４５０で変換が成功する。
【００８２】
ゾーン・セキュリティ・テーブル・インターフェイス１４８５を介して、ストレージの登録およびマッピングのさまざまなチェックが集合的に管理され得る。例えば、ブロック１４１０、１４２０、１４５５、１４７０、および１４７５は、さまざまなアクセスを管理するために同じゾーンに関連付けられているゾーン・セキュリティ・テーブルとインターフェイスをとることができる。
【００８３】
前述したように、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変換を使用してメモリに常駐するページを管理し、ホストは、独立してＤＡＴ変換を使用して、それらのゲスト・ページがメモリに常駐しているときに、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変換を使用して、異なるＶＭ間のストレージの必要な分離または共有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、すべてのゲスト・ストレージにアクセスすることができる。

【００８４】

本明細書において説明されるように、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のインターフェイスを活用して、このセキュリティの向上を行う。これに関して、このインターフェイスは、マシン（セキュア・インターフェイス制御およびハードウェア）がこれらのページのマッピングにおけるセキュリティを保証しながら、ハイパーバイザがセキュア・ゲスト・ページを管理し続けることができるようにする方法で、セキュア・インターフェイス制御およびハイパーバイザがページ管理を提供できるようにするために使用される。

【００８５】

１つまたは複数の実施形態では、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」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。これを行うために、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、セキュア・インターフェイス制御またはセキュア・インターフェイス制御（ＵＶ）と呼ばれる制御構造によってマシンに組み込まれる。セキュア・インターフェイス制御は、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。セキュア・インターフェイス制御は、マシンの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。

【００８６】

セキュア・インターフェイス制御は、遷移の主要ポイントとして仮想マシンのディスパッチを使用して仮想マシン（すなわち、ハイパーバイザとセキュア・ゲストの間）に提供されるか、または変換の主要ポイントとして別の境界（例えば、アドレス空間）の変更を使用して仮想実行ファイルに提供される、保護メカニズムである。

【００８７】

セキュア・インターフェイス制御（例えば、ウルトラバイザ）は、１つの例では、内部のセキュアな信頼できるファームウェアに実装される。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・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、すべて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。この最低レベルは、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などの、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。このアクセスによって、セキュア・インターフェイス制御は、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。また、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。

【００８８】
ソフトウェアは、命令呼び出し（例えば、ＵＶ呼び出し（ＵＶＣ）命令）を使用して、セキュア・インターフェイス制御が特定の動作を実行することを要求する。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。

【００８９】
これらのＵＶＣコマンドは、多くの他の設計された命令と同様に、マシンのファームウェアによって実行される。マシンは、セキュア・インターフェイス制御モードに移行せず、代わりにマシンは、現在実行されているモードでセキュア・インターフェイス制御機能を実行する。これらの動作を処理するためのコンテキストの切り替えはない。この少ないオーバーヘッドによって、必要なレベルのセキュリティを引き続き提供しながら、セキュア・インターフェイス制御における複雑さを最小限に抑えて減らすような方法で、ソフトウェア、信頼できるファームウェア、およびハードウェアの異なるレイヤ間の緊密な連携を可能にする。

【００９０】
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、セキュア・ゲストの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。

【００９１】
軽量のＵＶＣ設計は、セキュア・インターフェイス制御によるハイパーバイザ・テーブルのシャドーイングなしで、したがって、このシャドーイングを提供するための大きいオーバーヘッドなしで、ハイパーバイザのページ管理が進むことを可能にする。これは、暗号化された非セキュア・ページを、単一のセキュア・ゲスト・ドメインのみによるアクセスが許可される復号されたセキュア・ページに遷移させるために、ＵＶ呼び出し命令を使用することによって実現される。このプロセスの一部として、セキュア・インターフェイス制御は、いずれかのセキュア・ゲスト・ページに関して、対応するセキュアなホスト仮想ページが、単一のホスト絶対ページにマッピングされること、単一のホスト仮想アドレスがいずれかの特定のセキュアなホスト絶対アドレスにマッピングされること、およびセキュア・ページが単一のセキュア・ゲスト・ドメインに属することを保証する。加えて、特定のホスト絶対ページへのいずれかのセキュアなホスト仮想アドレスのマッピングに対する変更がハードウェアによって検出され、例外が提示されるように、そのマッピングがセキュア・インターフェイス制御に登録される。

【００９２】
本明細書に記載された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、セキュア・ストレージへの変換（エクスポート）ＵＶＣを発行する必要がある。ＵＶは、このエクスポートＵＶＣに応答して、ページがＵＶによって「遷移中である」か、または「ロックされている」ことを示し、ページを暗号化し、ページを非セキュアに設定し、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。

【００９３】
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、セキュア・ストレージからの変換（インポート）ＵＶＣを発行しなければならない。ＵＶは、このインポートＵＶＣに応答して、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、ページがＵＶによって「遷移中である」か、または「ロックされている」ことを示し、ページを復号し、特定のセキュア・ゲスト・ドメインに対する権限を設定する。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、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。
【００９４】
１つまたは複数の実施形態に従って、新しい追加のステップをハイパーバイザに示すためのマシンからの追加のプログラム割り込みが提供される。この場合、この追加のステップは、ゲスト・ページのインポートであってよい。ハードウェアは、この追加のステップがハイパーバイザによって完了されるまで、セキュア・ゲストによるページのアクセスを防ぐ。これにより、セキュリティ上の理由のため、そのセキュアな環境内で実行されなければならないステップをセキュア・インターフェイス制御が実行することを要求することによって、セキュア・インターフェイス制御におけるハイパーバイザの多くの作業の繰り返しを最小限に抑えるという利点が得られる。この方法は、インポートＵＶＣ中に実行されるチェックと組み合わさって、セキュア・インターフェイス制御がホストＤＡＴテーブルを監視し、場合によってはシャドーイングする必要性、ならびに関連するオーバーヘッドおよび複雑さを取り除く。
【００９５】
上記を考慮して、セキュア・インターフェイス制御の高レベルのページ管理の動作が、図１５～１６に関して説明される。ここで図１５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・インターフェイス制御の高レベルのページ管理のためのプロセス・フロー１５００が示されている。プロセス・フロー１５００は、セキュアな実体（例えば、ＶＭまたはコンテナ）１５０２、ハードウェア１５０４、信頼できない実体（例えば、信頼できない、セキュアでない実体、ハイパーバイザ、またはＯＳ）１５０６、およびセキュア・インターフェイス制御１５０８を重ね合わせて、セキュアな環境のコンポーネントによってどの動作が実行されているかを示している。
【００９６】
ブロック１５１０でプロセス・フロー１５００が開始し、ブロック１５１０で、セキュアな実体１５０２が、信頼できない実体１５０６によって透過的にページインされている、まだ暗号化されている（非セキュアとしてマーク付けされている）セキュア・ページにアクセスする。ブロック１５２０で、ハードウェア１５０４が、セキュア・ゲスト・ページの復号の必要性を示すプログラム割り込みを信頼できない実体１５０６に提示する。ブロック１５３０で、信頼できない実体１５０６がインポートＵＶＣ（例えば、インポート命令）を発行する。インポートＵＶＣは、ホスト絶対ページおよびホスト仮想ページを入力パラメータとして指定する。
【００９７】
ブロック１５３５で、セキュア・インターフェイス制御１５０８が、インポートＵＶＣの実施の一部として、指定されたホスト絶対ページがマッピングされているとしてまだ登録されていないということを決定し、セキュア・インターフェイス制御１５０８によって使用するためにホスト絶対ページをロックする（このホスト絶対ページへの他のＵＶＣま

たはセキュアな実体のアクセスを防ぐ）。インポートされるページがすでにマッピングされている（例えば、ホスト仮想ページが異なるホスト絶対ページにすでにマッピングされているか、またはホスト絶対ページに、異なるホスト仮想ページがすでにマッピングされている）場合、エラーがセキュアでない実体に提示されるということに注意する。ブロック１５４０で、セキュア・インターフェイス制御１５０８が、ページ（例えば、ホスト絶対ページ）をセキュアとしてマーク付けする（セキュアでない実体によるアクセスを防ぐ）。

【００９８】

ブロック１５５０で、セキュア・インターフェイス制御１５０８が、ホスト仮想ページがセキュアな絶対ページにまだマッピングされていないということを決定し、セキュア・インターフェイス制御１５０８によって使用するためにホスト仮想ページを登録する。インポートされるページがすでにマッピングされている（例えば、ホスト仮想ページが異なるホスト絶対ページにすでにマッピングされているか、またはホスト絶対ページに、異なるホスト仮想ページがすでにマッピングされている）場合、エラーがセキュアでない実体に提示されるということに注意する。

【００９９】

ブロック１５６０で、セキュア・インターフェイス制御１５０８が、ゲストによって最終的に使用するためにページを安全に復号する。ブロック１５７０で、セキュア・インターフェイス制御１５０８が、ホスト絶対ページのロックを解除し、ホスト絶対ページを特定のセキュア・ゲスト・ドメインに属しているとして登録し、ホスト仮想からホスト絶対へのマッピングも登録する。

【０１００】

例えば、セキュア・インターフェイス制御１５０８は、セキュア・インターフェイス制御１５０８によって使用するためのホスト絶対ページを登録し、ホスト絶対ページを安全に復号し、その後、セキュア・インターフェイス制御１５０８によって使用するためのホスト絶対ページの登録を解除し、ホスト絶対ページをセキュア・ドメインに登録する。さらに、セキュア・インターフェイス制御１５０８は、関連するホスト絶対ページと共にホスト仮想アドレスを登録して、セキュアな実体によって使用するためのホスト・アドレス対を作成し、セキュアな実体によるアクセス時に、ホスト仮想アドレスの一致をチェックする。

【０１０１】

ブロック１５８０で、信頼できない実体が、セキュアな実体（例えば、ゲストまたはＶＭ）を再ディスパッチする。ブロック１５９０で、セキュアな実体が、例外を発生させずに、現在復号されているページに再アクセスする。

【０１０２】

ここで図１６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・インターフェイス制御の高レベルのページ管理のためのプロセス・フロー１６００が示されている。プロセス・フロー１６００は、セキュアな実体（例えば、ゲスト）１６０２、ハードウェア１６０４、および信頼できない実体１６０６を重ね合わせて、セキュアな環境のコンポーネントによってどの動作が実行されているかを示している。

【０１０３】

プロセス・フロー１６００はブロック１６１０で開始し、ブロック１６１０で、セキュアな実体（例えば、ゲスト、ＶＭ、またはコンテナ）１６０２がセキュアな仮想ページにアクセスする。例えば、セキュアな実体１６０２は、セキュア・ドメインＩＤ　ｎに関連付けられ、セキュア・ゲスト仮想ページＸ．ＧＶにアクセスする。ブロック１６２０で、ハードウェア１６０４がＤＡＴ変換を実行する。例えば、ハードウェア１６０４は、ホスト仮想ページＸ．ＨＶおよびホスト絶対ページＸ．ＨＡへのゲスト仮想ページＸ．ＧＶのＤＡＴ変換を実行する。

【０１０４】

次に、判定ブロック１６３０で、ハードウェア１６０４は、セキュア・ページが、セキ

ュア・アクセスを開始したセキュア・ドメインに属しているとして登録されているかどうかを判定する。例えば、ハードウェア１６０４は、セキュア・ページＸ．ＨＡがセキュア・ドメインｎに登録されているかどうかを判定する。このセキュア・ページがセキュア・ドメインｎに登録されていない場合、プロセス・フロー１６００がブロック１６５０に進む（「いいえ」の矢印で示されている）。ブロック１６５０で、ハードウェア１６０４がプログラム例外を信頼できない実体（例えば、ハイパーバイザ）１６０６に提示する。このセキュア・ページがセキュア・ゲスト・ドメインに割り当てられている場合、プロセス・フロー１６００が判定ブロック１６７０に進む（「はい」の矢印で示されている）。

【０１０５】

判定ブロック１６７０で、ハードウェア１６０４は、登録されたホスト仮想アドレス（登録されたホスト・アドレス対に対応する）がセキュアな仮想アクセスのために実行されたＤＡＴから取得されたホスト・アドレス対に一致するかどうかを判定する。例えば、ハードウェア１６０４は、セキュア・ページＸ．ＨＡと共に登録されたホスト仮想アドレスがＤＡＴによって取得されたＸ．ＨＶに一致するかどうかを判定する。登録されたアドレスがＤＡＴの結果に一致しない場合、プロセス・フロー１６００がブロック１６５０に進む（「いいえ」の矢印で示されている）。ブロック１６５０で、ハードウェア１６０４が例外を信頼できない実体１６０６に提示する。登録されたアドレスがＤＡＴの結果に一致する場合、プロセス・フロー１６００がブロック１６９０に進む（「はい」の矢印で示されている）。ブロック１６９０で、ハードウェア１６０４は、他のすべての保護チェックがセキュアな実体のアクセスを可能にする場合、このアクセスを許可する。

【０１０６】

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。

【０１０７】

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。

【０１０８】

特徴は、次のとおりである。

【０１０９】

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。

【０１１０】

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。

【０１１１】

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。
【０１１２】
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。
【０１１３】
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。
【０１１４】
サービス・モデルは、次のとおりである。
【０１１５】
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。
【０１１６】
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。
【０１１７】
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。
【０１１８】
デプロイメント・モデルは、次のとおりである。
【０１１９】
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。
【０１２０】
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。

【０１２１】

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。

【０１２２】

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。

【０１２３】

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。

【０１２４】

ここで図１７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１７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。

【０１２５】

ここで図１８を参照すると、クラウド・コンピューティング環境５０（図１７）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１８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。

【０１２６】

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。
【０１２７】
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。
【０１２８】
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。
【０１２９】
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、ならびに高レベルのページ管理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。
【０１３０】
ここで図１９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１９００が示されている。システム１９００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。
【０１３１】
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。

【０１３２】

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。

【０１３３】

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１０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のＶＭ Ｓｅｒｖｅｒ、ＣｉｔｒｉｘのＸｅｎＳｅｒｖｅｒ、ＶｍｗａｒｅのＥＳＸ、Ｍｉｃｒｏｓｏｆｔ Ｈｙｐｅｒ－Ｖハイパーバイザ、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。

【０１３４】

ここで図２０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。

【０１３５】

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）２２０１ａ、２００１ｂ、２００１ｃなどを含むことができるプロセッサ２００１を含んでいる。プロセッサ２００１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２００２を介してシステム・メモリ２００３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２００３は、読み取り専用メモリ（ＲＯＭ：read only memory）２００４およびランダム・アクセス・メモリ（ＲＡＭ：random access memory）２００５を含む。ＲＯＭ２００４は、システム・バス２００２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２００１で使用するためにシステム・バス２００２に結合された読み取り書き込みメモリである。

【０１３６】

図２０のノード１０は、プロセッサ２００１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２００７を含んでいる。ハード・ディスク２００７は、ソフトウェア２００８およびデータ２００９を格納する。ソフトウェア２００８は、（図１～１９を参照して説明されたプロセスなどのプロセスを実行するために）プロセッサ２００１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２００９は、ソフトウェア２００８の動作を支援し、ソフトウェア２００８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。

【０１３７】

図２０のノード１０は、ノード１０のプロセッサ２００１、システム・メモリ２００３、ハード・ディスク２００７、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２００２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。

【０１３８】

図に示されているように、ノード１０は、キーボード２０２１、マウス２０２２、スピーカ２０２３、およびマイクロホン２０２４をシステム・バス２００２に相互接続するインターフェイス・アダプタ２０２０を含んでいる。ノード１０は、システム・バス２００２をディスプレイ２０３１に相互接続するディスプレイ・アダプタ２０３０を含んでいる。ディスプレイ・アダプタ２０３０（またはプロセッサ２００１あるいはその両方）は、ＧＵＩ２０３２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２０４１は、システム・バス２００２をネットワーク２０５０と相互接続し、ノード１０が、サーバ２０５１およびデータベース２０５２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２００８およびデータ２００９の動作が、サーバ２０５１およびデータベース２０５２によってネットワーク２０５０上に実装され得る。例えば、ネットワーク２０５０、サーバ２０５１、およびデータベース２０５２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２００８およびデータ２００９の内部の反復を提供することができる。

【０１３９】

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。

【０１４０】

本明細書で開示された本発明の実施形態は、セキュア・インターフェイス制御の高レベルのページ管理を実施するシステム、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。

【０１４１】

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。

【０１４２】

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。

【０１４３】

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。

【０１４４】

「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。

【０１４５】

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。

【０１４６】

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。

【０１４７】

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。

【０１４８】

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。

【０１４９】

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。

【０１５０】

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。

【０１５１】

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。

【０１５２】

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。

【０１５３】

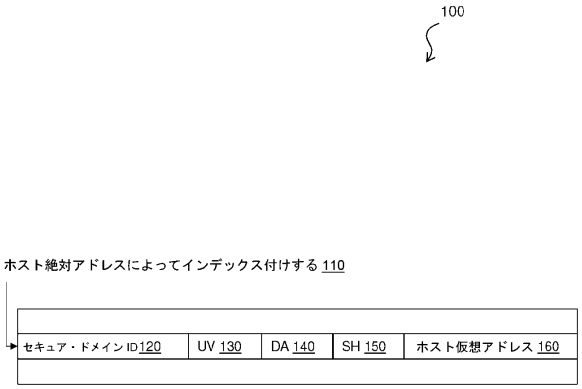
本明細書で使用される用語は、特定の実施形態を説明することのみを目的としており、制限することを意図していない。本明細書において使用されるとき、単数形「ａ」、「ａｎ」、および「ｔｈｅ」は、特に明示的に示されない限り、複数形も含むことが意図されている。「備える」または「備えている」あるいはその両方の用語は、本明細書で使用される場合、記載された機能、整数、ステップ、動作、要素、またはコンポーネント、あるいはその組み合わせの存在を示すが、１つまたは複数のその他の機能、整数、ステップ、動作、要素コンポーネント、またはこれらのグループ、あるいはその組み合わせの存在または追加を除外していないということが、さらに理解されるであろう。

【０１５４】

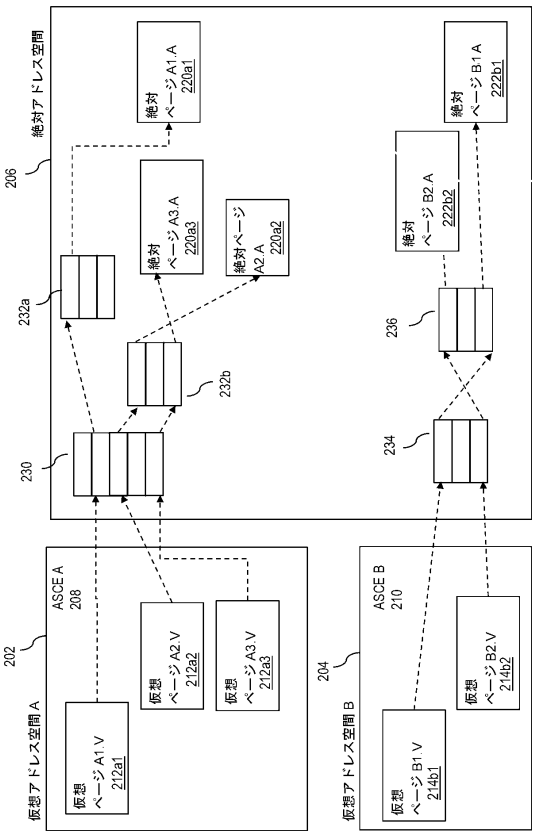
本明細書におけるさまざまな実施形態の説明は、例示の目的で提示されているが、網羅的であることは意図されておらず、開示された実施形態に制限されない。記載された実施形態の範囲および思想を逸脱することなく多くの変更および変形が可能であることは、当業者にとって明らかであろう。本明細書で使用された用語は、実施形態の原理、実際の適用、または市場で見られる技術を超える技術的改良を最も適切に説明するため、あるいは他の当業者が本明細書で開示された実施形態を理解できるようにするために選択されている。

【図面】

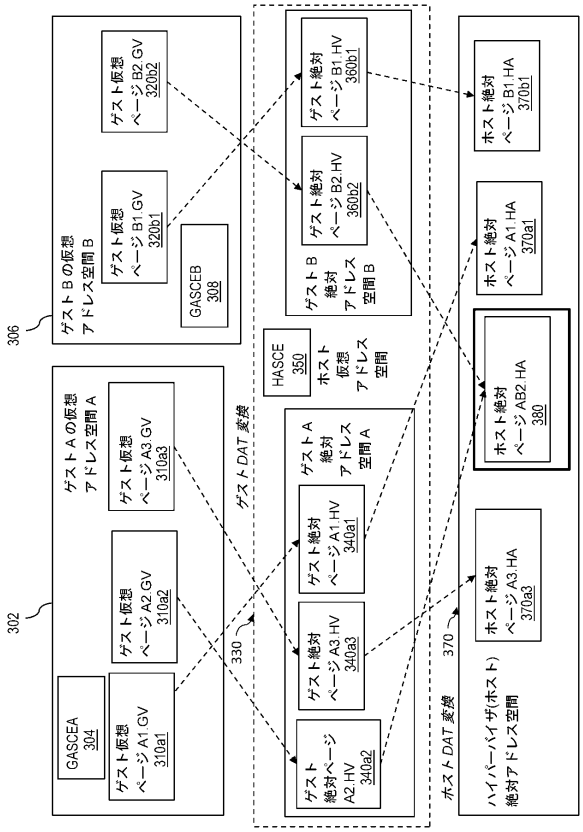
【図１】


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・ドメイン ID120
UV 130
DA 140
SH 150
ホスト仮想アドレス 160

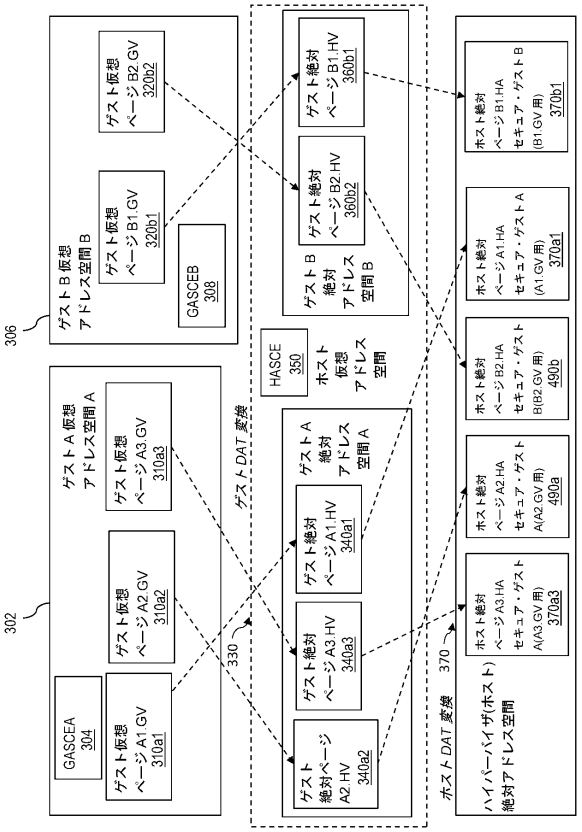
【図２】


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

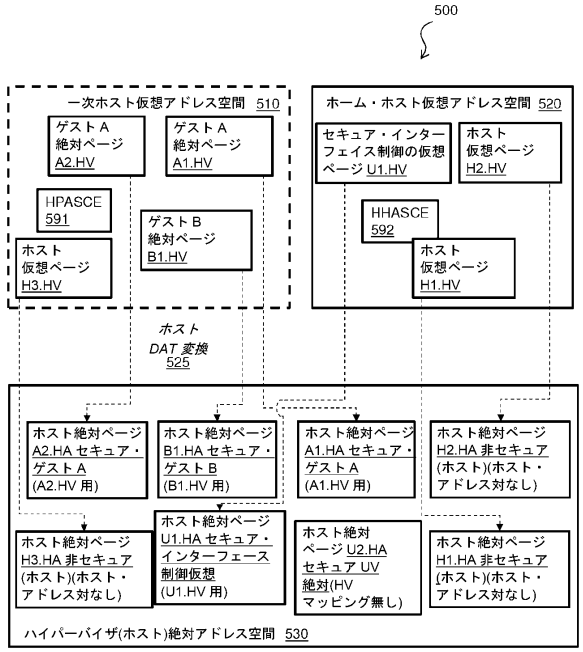
【図３】


306
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
302
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
ゲスト仮想
ページ A1.GV
310a1
GASCEA
304
330
ゲスト DAT 変換
HASCE
350
ホスト
仮想
アドレス
空間
ゲスト B
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
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
370
ホスト DAT 変換
ハイパーバイザ(ホスト)
絶対アドレス空間
ホスト絶対
ページ B1.HA
370b1
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

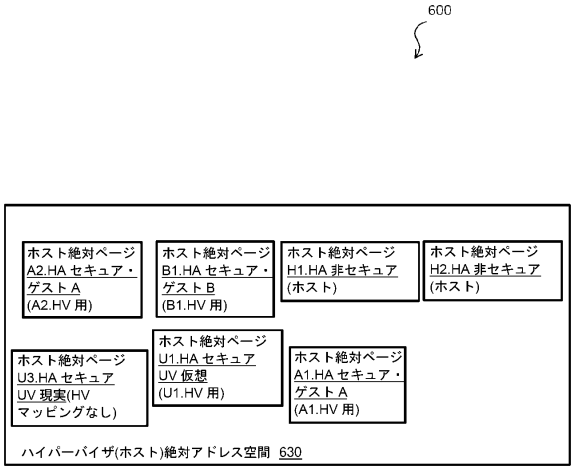
【図４】


306
ゲスト B 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
302
ゲスト A 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
ゲスト仮想
ページ A1.GV
310a1
GASCEA
304
330
ゲスト DAT 変換
HASCE
350
ホスト
仮想
アドレス
空間
ゲスト B
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
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
370
ホスト DAT 変換
ハイパーバイザ(ホスト)
絶対アドレス空間
ホスト絶対
ページ B1.HA
セキュア・ゲスト B
(B1.GV 用)
370b1
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 B2.HA
セキュア・ゲスト
B(B2.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

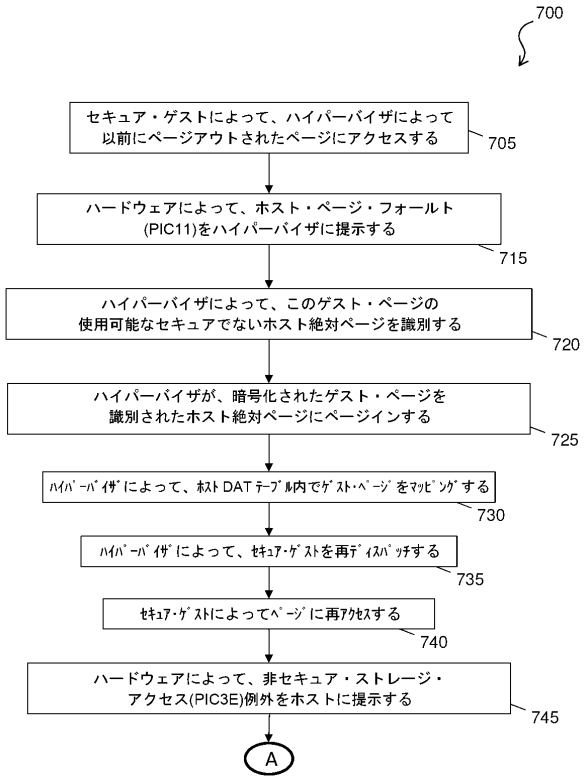
【図５】


500
一次ホスト仮想アドレス空間 510
ゲスト A
絶対ページ
A2.HV
ゲスト A
絶対ページ
A1.HV
HPASCE
591
ゲスト B
絶対ページ
B1.HV
ホスト
仮想ページ
H3.HV
ホーム・ホスト仮想アドレス空間 520
セキュア・インター
フェイス制御の仮想
ページ U1.HV
ホスト
仮想ページ
H2.HV
HHASCE
592
ホスト
仮想ページ
H1.HV
ホスト
DAT 変換
525
ホスト絶対ページ
A2.HA セキュア・
ゲスト A
(A2.HV 用)
ホスト絶対ページ
B1.HA セキュア・
ゲスト B
(B1.HV 用)
ホスト絶対ページ
A1.HA セキュア・
ゲスト A
(A1.HV 用)
ホスト絶対ページ
H2.HA 非セキュア
(ホスト)(ホスト・
アドレス対なし)
ホスト絶対ページ
H3.HA 非セキュア
(ホスト)(ホスト・
アドレス対なし)
ホスト絶対ページ
U1.HA セキュア・
インターフェース
制御仮想
(U1.HV 用)
ホスト絶対
ページ U2.HA
セキュア UV
絶対(HV
マッピング無し)
ホスト絶対ページ
H1.HA 非セキュア
(ホスト)(ホスト・
アドレス対なし)
ハイパーバイザ(ホスト)絶対アドレス空間 530

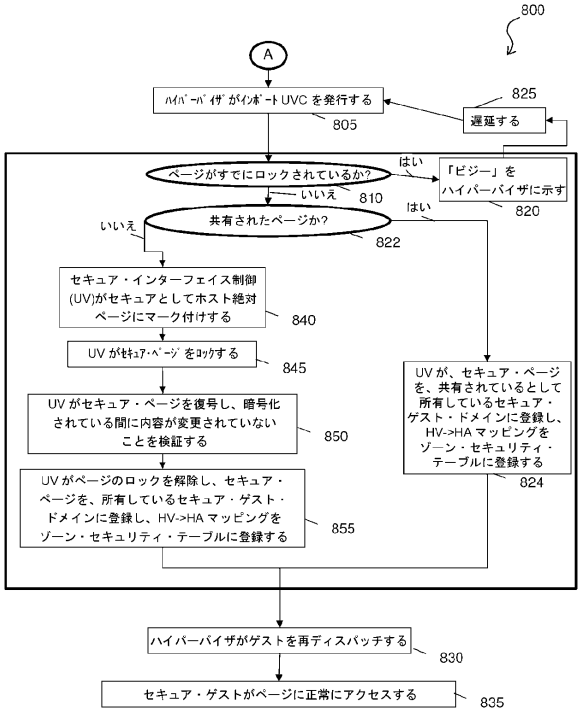
【図６】


600
ホスト絶対ページ
A2.HA セキュア・
ゲスト A
(A2.HV 用)
ホスト絶対ページ
B1.HA セキュア・
ゲスト B
(B1.HV 用)
ホスト絶対ページ
H1.HA 非セキュア
(ホスト)
ホスト絶対ページ
H2.HA 非セキュア
(ホスト)
ホスト絶対ページ
U3.HA セキュア
UV 現実(HV
マッピングなし)
ホスト絶対ページ
U1.HA セキュア
UV 仮想
(U1.HV 用)
ホスト絶対ページ
A1.HA セキュア・
ゲスト A
(A1.HV 用)
ハイパーバイザ(ホスト)絶対アドレス空間 630

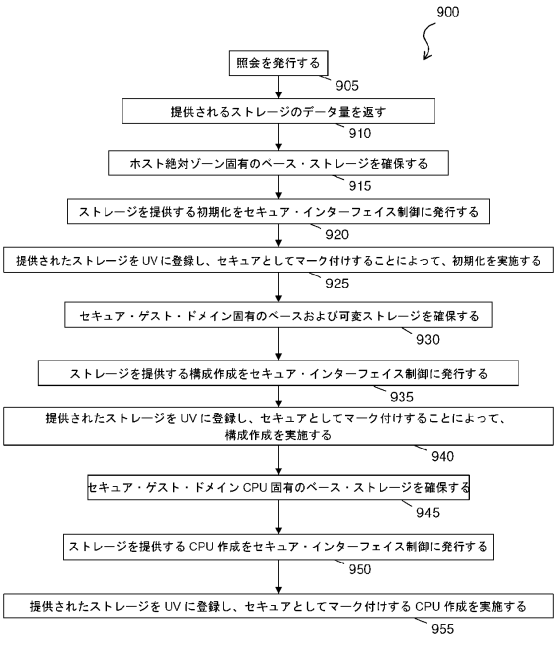
【図７】


700
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
705
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
715
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
720
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
725
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
730
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
735
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
740
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
745
A

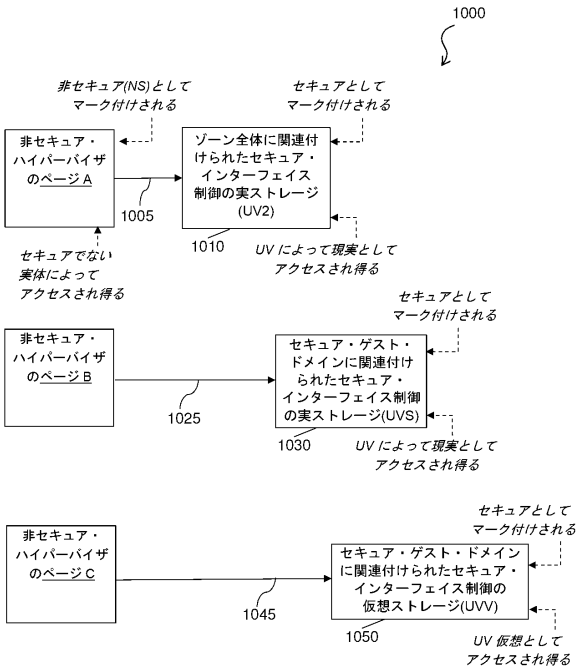
【図８】


800
A
ﾊｲﾊﾟｰﾊﾞｲｻﾞがｲﾝﾎﾞｰﾄUVCを発行する
805
825
遅延する
ページがすでにロックされているか?
はい
いいえ
810
「ビジー」をハイパーバイザに示す
820
共有されたページか?
はい
いいえ
822
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
840
UVがｾｷｭｱ･ﾍﾟｰｼﾞをﾛｯｸする
845
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
850
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
855
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
824
ハイパーバイザがゲストを再ディスパッチする
830
セキュア・ゲストがページに正常にアクセスする
835

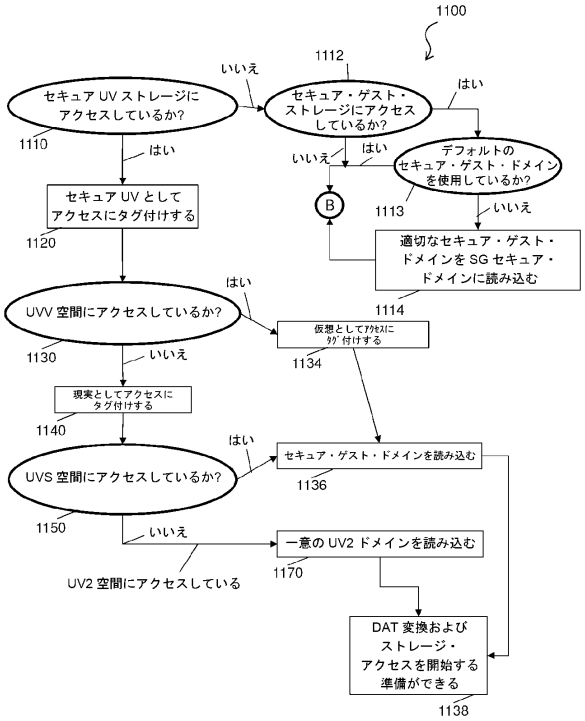
【図９】


900
照会を発行する
905
提供されるストレージのデータ量を返す
910
ホスト絶対ゾーン固有のベース・ストレージを確保する
915
ストレージを提供する初期化をセキュア・インターフェイス制御に発行する
920
提供されたストレージをUVに登録し、セキュアとしてマーク付けすることによって、初期化を実施する
925
セキュア・ゲスト・ドメイン固有のベースおよび可変ストレージを確保する
930
ストレージを提供する構成作成をセキュア・インターフェイス制御に発行する
935
提供されたストレージをUVに登録し、セキュアとしてマーク付けすることによって、構成作成を実施する
940
セキュア・ゲスト・ドメインCPU固有のベース・ストレージを確保する
945
ストレージを提供するCPU作成をセキュア・インターフェイス制御に発行する
950
提供されたストレージをUVに登録し、セキュアとしてマーク付けするCPU作成を実施する
955

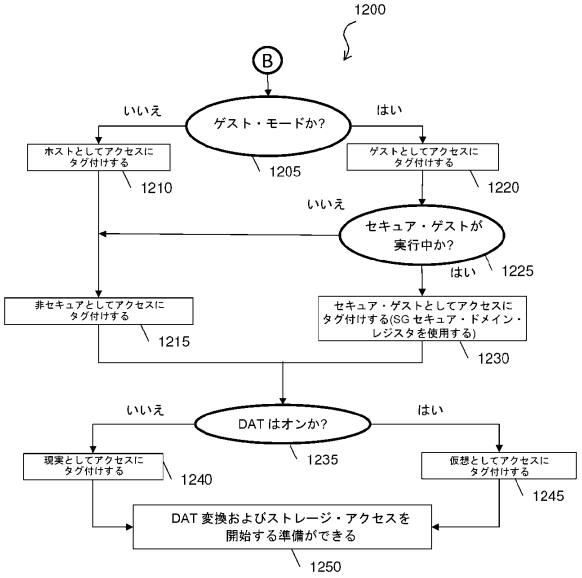
【図１０】


1000
非セキュア(NS)としてマーク付けされる
セキュアとしてマーク付けされる
非セキュア・ハイパーバイザのページA
1005
ゾーン全体に関連付けられたセキュア・インターフェイス制御の実ストレージ(UV2)
1010
セキュアでない実体によってアクセスされ得る
UVによって現実としてアクセスされ得る
セキュアとしてマーク付けされる
非セキュア・ハイパーバイザのページB
1025
セキュア・ゲスト・ドメインに関連付けられたセキュア・インターフェイス制御の実ストレージ(UVS)
1030
UVによって現実としてアクセスされ得る
セキュアとしてマーク付けされる
非セキュア・ハイパーバイザのページC
1045
セキュア・ゲスト・ドメインに関連付けられたセキュア・インターフェイス制御の仮想ストレージ(UVV)
1050
UV仮想としてアクセスされ得る

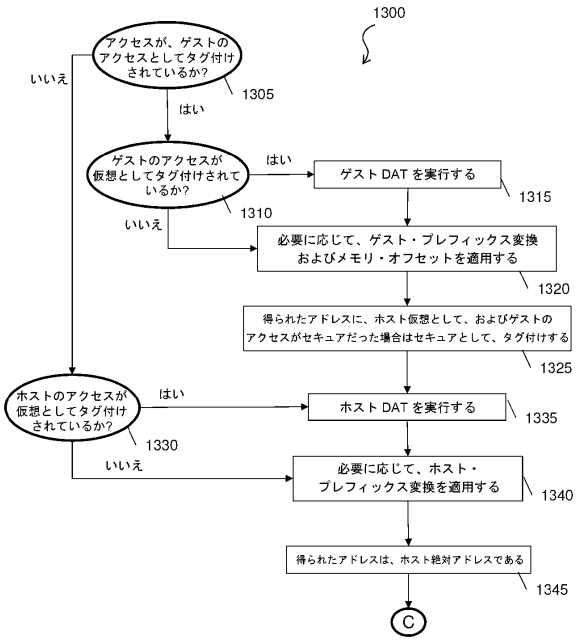
【図１１】



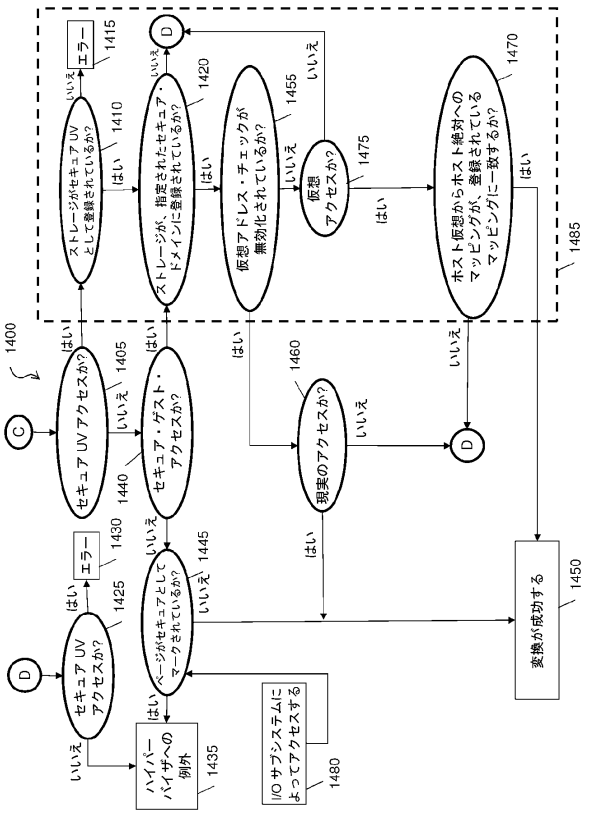
【図１２】



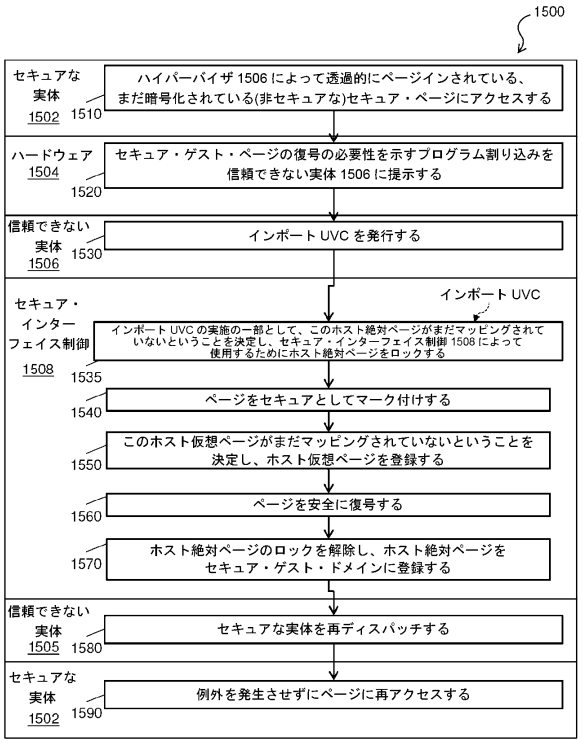
【図１３】



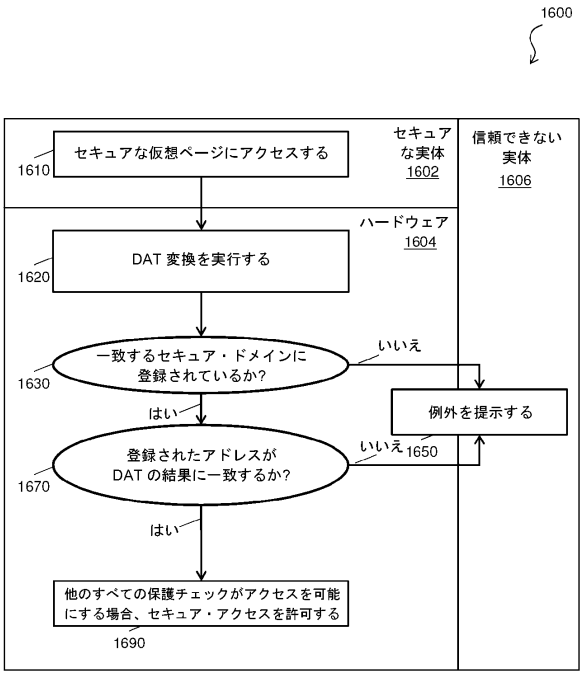
【図１４】



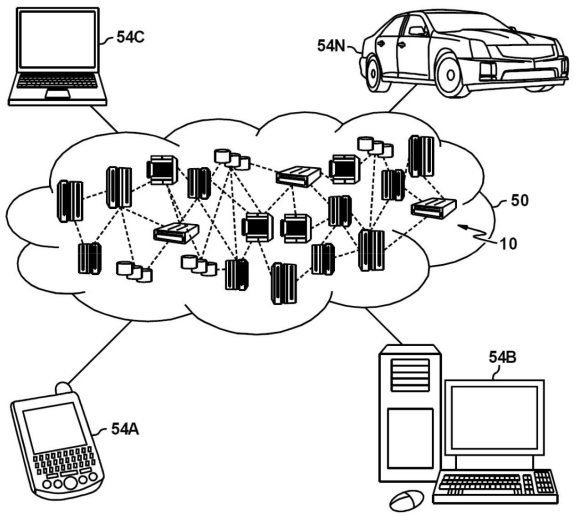
【図１５】



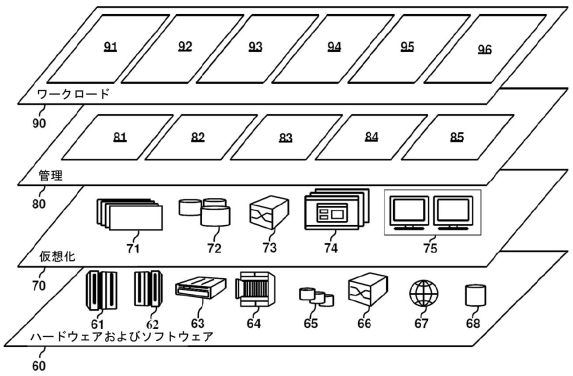
【図１６】



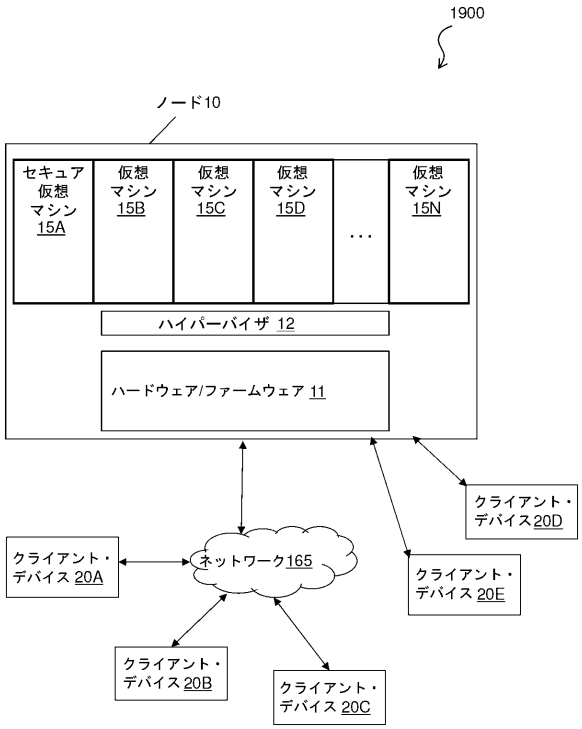
【図１７】



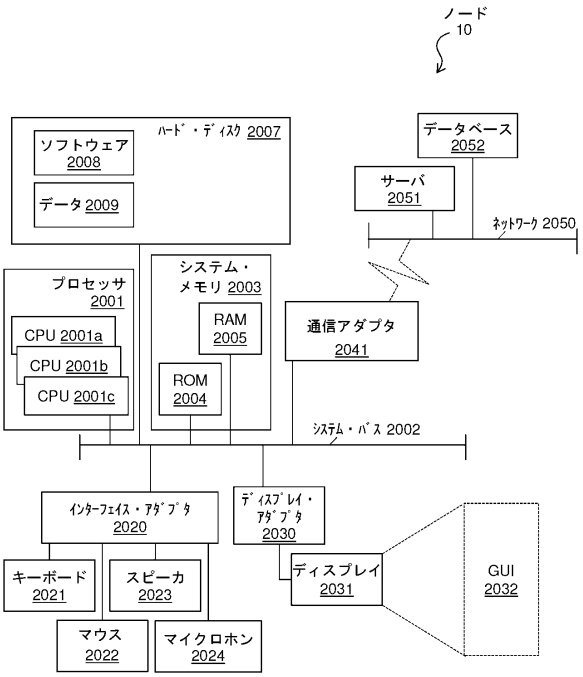
【図１８】



【図１９】


1900
ノード10
セキュア仮想マシン 15A
仮想マシン 15B
仮想マシン 15C
仮想マシン 15D
...
仮想マシン 15N
ハイパーバイザ 12
ハードウェア/ファームウェア 11
クライアント・デバイス20D
クライアント・デバイス 20A
ネットワーク165
クライアント・デバイス 20E
クライアント・デバイス 20B
クライアント・デバイス 20C

【図２０】


ノード 10
ソフトウェア 2008
ﾊｰﾄﾞ・ﾃﾞｨｽｸ 2007
データ 2009
データベース 2052
サーバ 2051
ﾈｯﾄﾜｰｸ 2050
プロセッサ 2001
CPU 2001a
CPU 2001b
CPU 2001c
システム・メモリ 2003
RAM 2005
ROM 2004
通信アダプタ 2041
ｼｽﾃﾑ・ﾊﾞｽ 2002
ｲﾝﾀｰﾌｪｲｽ・ｱﾀﾞﾌﾟﾀ 2020
ﾃﾞｨｽﾌﾟﾚｲ・ｱﾀﾞﾌﾟﾀ 2030
キーボード 2021
スピーカ 2023
ディスプレイ 2031
GUI 2032
マウス 2022
マイクロホン 2024

フロントページの続き

(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　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　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

審査官　平井　誠

(56)参考文献　SEONGWOOK JIN; ET AL，ARCHITECTURAL SUPPORT FOR SECURE VIRTUALIZATION UNDER A VULNERABLE HYPERVISOR，PROCEEDINGS OF THE 44TH ANNUAL IEEE/ACM INTERNATIONAL SYMPOSIUM ON MICROARCHITECTURE，米国，2011年，PAGE(S):272-283，http://dx.doi.org/10.1145/2155620.2155652

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１２／１４
Ｇ０６Ｆ　２１／００－８８