

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7398472号
(P7398472)

(45)発行日 令和5年12月14日(2023.12.14)

(24)登録日 令和5年12月6日(2023.12.6)

(51)国際特許分類

F I

G 0 6 F 21/62 (2013.01)

G 0 6 F 21/62

G 0 6 F 9/455(2018.01)

G 0 6 F 9/455 1 5 0

請求項の数 12 (全39頁)

(21)出願番号 特願2021-552193(P2021-552193)
(86)(22)出願日 令和2年2月28日(2020.2.28)
(65)公表番号 特表2022-522374(P2022-522374
A)
(43)公表日 令和4年4月18日(2022.4.18)
(86)国際出願番号 PCT/EP2020/055317
(87)国際公開番号 WO2020/182498
(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7月25日(2022.7.25)
(31)優先権主張番号 16/296,452
(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 BUSI
NESS MACHINES CORPO
RATION
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, A
rmonk, New York 105
04, 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】 割り込みイネーブルのためのセキュア・インターフェース制御ハイレベル命令インターセ
プト

(57)【特許請求の範囲】

【請求項1】

割り込みをイネーブルする命令に対する部分的な命令解釈を提供するコンピュータのセキュア・インターフェース制御によって、セキュア・ゲスト・ストレージからプログラム状況ワードまたは制御レジスタ値をフェッチすることと、

前記セキュア・インターフェース制御によって、信頼されないエンティティにゲスト割り込みマスク更新を通知することであって、前記信頼されないエンティティは、前記信頼されないエンティティにおいて実行されるセキュア・エンティティの動作をサポートするために、前記セキュア・インターフェース制御を介して前記コンピュータのハードウェアにおいて実行され、それと通信する、前記通知することと、

前記セキュア・インターフェース制御によって、前記ゲスト割り込みマスク更新を前記通知することに応答して、最高優先順位のイネーブルされたゲスト割り込みを提供する要求を前記信頼されないエンティティから受信することと、

前記セキュア・インターフェース制御によって、ゲスト・プレフィックス・ページに割り込み情報を移動し、前記割り込みの挿入が有効と判定されたときに前記セキュア・エンティティに前記割り込みを挿入することと

を含む、方法。

【請求項2】

前記セキュア・エンティティによって、前記信頼されないエンティティによってモニタされるロード・プログラム状況ワードまたはロード制御を発行することをさらに含む、請

求項 1 に記載の方法。

【請求項 3】

前記フェッチすることに応答して、前記セキュア・インターフェース制御によって、前記プログラム状況ワードまたは制御レジスタをロードすることをさらに含む、請求項 1 または 2 に記載の方法。

【請求項 4】

前記信頼されないエンティティによって、保留およびイネーブルされた割り込みの優先順位付けをして、前記最高優先順位のイネーブルされたゲスト割り込みを決定することをさらに含む、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】

前記信頼されないエンティティによって、前記最高優先順位のイネーブルされたゲスト割り込みに対する割り込み情報を非セキュア・ストレージに記憶することをさらに含む、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】

前記信頼されないエンティティは、状態記述に前記割り込み情報を提供する、請求項 5 に記載の方法。

【請求項 7】

前記信頼されないエンティティは前記セキュア・インターフェース制御に前記割り込み情報を提供するための命令を発行し、前記割り込み情報は前記命令に対するパラメータとして渡される、請求項 5 に記載の方法。

【請求項 8】

前記割り込みの前記挿入が無効と判定されたときに、前記セキュア・インターフェース制御によって、前記信頼されないエンティティに例外を発行することをさらに含む、請求項 1 ないし 7 のいずれか一項に記載の方法。

【請求項 9】

前記挿入された割り込みを受信したことに応答して、前記セキュア・エンティティによって割り込みハンドラを実行することをさらに含む、請求項 1 ないし 8 のいずれか一項に記載の方法。

【請求項 10】

前記セキュア・エンティティはセキュア・ゲストを含み、前記信頼されないエンティティはハイパーバイザを含む、請求項 9 に記載の方法。

【請求項 11】

コンピュータのセキュア・インターフェース制御を含むシステムであって、前記システムは、割り込みをイネーブルする命令に対する部分的な命令解釈を提供するよう、請求項 1 ないし 10 のいずれか 1 項に記載の方法を行うように構成される、システム。

【請求項 12】

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

【発明の詳細な説明】

【技術分野】

【0001】

本発明は一般的にコンピュータ技術に関し、より具体的には割り込みイネーブルのためのセキュア・インターフェース制御ハイレベル命令インターセプトに関する。

【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、ユーザに自身のデータをサード・パーティ・データ・センタで記憶および処理するためのケイパビリティを提供する。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したり物理サーバのためにフロア空間を提供したりする必要なしに、顧客に対する仮想マシン（VM: v i r

10

20

30

40

50

t u a l m a c h i n e) を迅速かつ容易にプロビジョニングする能力を促進する。顧客は、顧客のプリファレンスまたは要求の変更に従ってVMを容易に拡張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VMをプロビジョニングし、そのVMはプロバイダのデータ・センタのサーバに物理的に存在する。特に、コンピューティング・プロバイダはしばしば同じサーバに複数の顧客のデータを記憶するため、顧客はしばしばVM内のデータのセキュリティについて懸念する。顧客は、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／データとの間のセキュリティに加えて、顧客自身のコード／データとそのプロバイダのサイトで動作する他のVMのコード／データとの間のセキュリティも望むことがある。加えて顧客は、プロバイダの管理者からのセキュリティに加えて、マシンで動作する他のコードからのセキュリティ侵害の可能性に対するセキュリティも望むことがある。

10

【0003】

こうしたセンシティブな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確実にするためのセキュリティ制御を実施してもよい。クラウド・インフラストラクチャの実現に仮想化を広く用いることによって、クラウド・サービスの顧客に独自のセキュリティの懸念がもたらされる。なぜなら、基礎的なハードウェアがコンピューティング、ストレージ、またはたとえネットワーク形成ハードウェアであっても、仮想化はそのハードウェアとオペレーティング・システム(OS: operating system)との関係を変えてしまうためである。このため、仮想化はそれ自身が適切な構成、管理、および保護を受ける必要がある付加的なレイヤとして導入される。

20

【0004】

一般的に、ホスト・ハイパーバイザの制御下でゲストとして動作するVMは、そのゲストに対する仮想化サービスを透過的に提供するためにそのハイパーバイザに頼っている。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は自身のデータをディスクからメモリに存在するように移動(ページイン)でき、かつVMは自身のデータを出してディスクに戻すこと(ページアウト)もできる。ページがメモリに存在する間、VM(ゲスト)はダイナミック・アドレス変換(DAT: dynamic address translation)を用い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プする。加えて、ホスト・ハイパーバイザはメモリ内のゲスト・ページに対して独自のDATマッピング(ホスト仮想アドレスからホスト絶対アドレスへ)を有し、ゲストとは独立に透過的にゲスト・ページをメモリの中および外にページできる。ハイパーバイザは、ホストDATテーブルを通じて、2つの別個のゲストVM間のゲスト・メモリのメモリ分離または共有を提供する。ホストは、ゲストの代わりに必要なときにゲスト動作をシミュレートするためにゲスト・メモリにアクセスすることもできる。

30

【0006】

命令エミュレーションおよび割り込み処理の場合、ゲストが特定の命令を実行するとき、ハイパーバイザが設定した制御に基づいて、マシンはハイパーバイザに制御を戻すことで、ハイパーバイザがゲストの代わりにその特定の命令をエミュレートできるようにする。たとえば、ロード・プログラム状況ワード(LPSW: Load program status word)またはロード制御(LCTL: load control)命令などがハイパーバイザによってエミュレートされることによって、ハイパーバイザは割り込みイネーブルをモニタして、ハイパーバイザによって維持されている保留割り込みを適切な優先順位のゲストに提供できるようにしてもよい。

40

【発明の概要】

【課題を解決するための手段】

【0007】

1つ以上の実施形態によると、割り込みをイネーブルする命令に対する部分的な命令解

50

釈を提供するコンピュータのセキュア・インターフェース制御による方法が提供される。セキュア・インターフェース制御は、セキュア・ゲスト・ストレージからプログラム状況ワードまたは制御レジスタ値をフェッチする。セキュア・インターフェース制御は、信頼されないエンティティにゲスト割り込みマスク更新を通知する。信頼されないエンティティにおいて実行されるセキュア・エンティティの動作をサポートするために、信頼されないエンティティはセキュア・インターフェース制御を通じてコンピュータのハードウェアにおいてそれと通信しながら実行される。セキュア・インターフェース制御は、信頼されないエンティティから、ゲスト割り込みマスク更新の通知に応答して最高優先順位のイネーブルされたゲスト割り込みを提供する要求を受信する。セキュア・インターフェース制御はゲスト・プレフィックス・ページに割り込み情報を移動させて、その割り込みの挿入が有効と判定されたときにはセキュア・エンティティに割り込みを挿入する。本明細書における1つ以上の実施形態の技術効果および利益は、セキュア・ゲスト状態またはメモリへの信頼されないエンティティによるアクセスを許可することなく、単一の場所にこの複雑なコードを常駐させることによって、複雑性およびリスクを低減することを含む。

10

【0008】

1つ以上の実施形態または上記の方法実施形態によると、この方法はさらに、セキュア・エンティティによって、信頼されないエンティティによってモニタされるロード・プログラム状況ワードまたはロード制御を発行することを含み得る。

【0009】

1つ以上の実施形態または上記の方法実施形態のいずれかによると、この方法はさらに、セキュア・インターフェース制御によって、フェッチすることに応答して、プログラム状況ワードまたは制御レジスタをロードすることを含み得る。

20

【0010】

1つ以上の実施形態または上記の方法実施形態のいずれかによると、この方法はさらに、信頼されないエンティティによって、保留およびイネーブルされた割り込みの優先順位付けをして、最高優先順位のイネーブルされたゲスト割り込みを定めることを含み得る。

【0011】

1つ以上の実施形態または上記の方法実施形態のいずれかによると、この方法はさらに、信頼されないエンティティによって、最高優先順位のイネーブルされたゲスト割り込みに対する割り込み情報を非セキュア・ストレージに記憶することを含み得る。

30

【0012】

1つ以上の実施形態または上記の方法実施形態のいずれかによると、信頼されないエンティティは、状態記述の割り込み情報を提供できる。

【0013】

1つ以上の実施形態または上記の方法実施形態のいずれかによると、信頼されないエンティティはセキュア・インターフェース制御に割り込み情報を提供するための命令を発行でき、割り込み情報はその命令に対するパラメータとして渡される。

【0014】

1つ以上の実施形態または上記の方法実施形態のいずれかによると、この方法はさらに、セキュア・インターフェース制御によって、割り込みの挿入が無効と判定されたときには信頼されないエンティティに例外を発行することを含み得る。本明細書における1つ以上の実施形態の技術効果および利益は、セキュア・ゲスト状態またはメモリへの信頼されないエンティティのアクセスを許可することなく、単一の場所にこの複雑なコードを存在させることによって、複雑性およびリスクを低減することを含む。

40

【0015】

1つ以上の実施形態または上記の方法実施形態のいずれかによると、この方法はさらに、セキュア・エンティティによって、挿入された割り込みを受信したことに応答して割り込みハンドラを実行することを含み得る。

【0016】

1つ以上の実施形態または上記の方法実施形態のいずれかによると、セキュア・エンテ

50

ィティはセキュア・ゲストを含むことができ、信頼されないエンティティはハイパーバイザを含む。

【0017】

1つ以上の実施形態によると、上記の方法実施形態のいずれかは、コンピュータ・プログラム製品またはシステムとして実現され得る。

【0018】

本開示の技術によって、付加的な特徴および利点の実現される。本明細書において本発明の他の実施形態および態様が詳細に説明されており、本発明の一部とみなされる。利点および特徴とともに本発明をより良好に理解するために、説明および図面を参照されたい。

【0019】

本明細書に記載される独占権の明細は、本明細書の末尾の請求項において特定の指摘され、明確に請求されている。本発明の実施形態の前述およびその他の特徴および利点は、添付の図面とともに得られる以下の詳細な説明から明らかである。

【図面の簡単な説明】

【0020】

【図1】本発明の1つ以上の実施形態によるゾーン・セキュリティに対するテーブルを示す図である。

【図2】本発明の1つ以上の実施形態によるDATを行うための仮想および絶対アドレス・スペースを示す図である。

【図3】本発明の1つ以上の実施形態によるハイパーバイザの下で動作する仮想マシン（VM）をサポートするためのネストされたマルチパートDATを示す図である。

【図4】本発明の1つ以上の実施形態によるセキュア・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つ以上の実施形態によるダイナミック・アドレス変換（DAT）動作のシステム概要を示す図である。

【図6】本発明の1つ以上の実施形態によるセキュア・インターフェース制御メモリのシステム概要を示す図である。

【図7】本発明の1つ以上の実施形態によるインポート動作のプロセスの流れを示す図である。

【図8】本発明の1つ以上の実施形態によるインポート動作のプロセスの流れを示す図である。

【図9】本発明の1つ以上の実施形態による供与メモリ動作のプロセスを示す図である。

【図10】本発明の1つ以上の実施形態によるセキュア・インターフェース制御のセキュア・ページへの非セキュア・ハイパーバイザ・ページの移行のプロセスの流れを示す図である。

【図11】本発明の1つ以上の実施形態によるセキュア・インターフェー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の流れを示す図である。

【図12】本発明の1つ以上の実施形態によるセキュア・インターフェース制御およびハードウェアによって行われるアクセス・タグ付けのプロセスの流れを示す図である。

【図13】本発明の1つ以上の実施形態によるプログラムおよびセキュア・インターフェース制御によるセキュアおよび非セキュア・アクセスをサポートするための変換のプロセスの流れを示す図である。

【図14】本発明の1つ以上の実施形態によるプログラムおよびセキュア・インターフェース制御によるセキュア・ストレージ保護を伴うDATのプロセスの流れを示す図である。

【図15】本発明の1つ以上の実施形態による割り込みイネーブルのためのセキュア・インターフェース制御ハイレベル命令インターセプトに対するプロセスの流れを示す図である。

【図16】本発明の1つ以上の実施形態による割り込みイネーブルのためのセキュア・インターフェース制御ハイレベル命令インターセプトに対するプロセスの流れを示す図である。

10

20

30

40

50

【図 17】本発明の 1 つ以上の実施形態によるクラウド・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 つ以上の実施形態による抽象化モデル・レイヤを示す図である。

【図 19】本発明の 1 つ以上の実施形態によるシステムを示す図である。

【図 20】本発明の 1 つ以上の実施形態によるノードを示す図である。

【発明を実施するための形態】

【0021】

本明細書に示される図面は例示である。本発明の思想から逸脱することなく、図面またはそこに記載される動作には多くの変形が存在し得る。たとえば、動作は異なる順序で行われ得るし、動作は追加、削除、または変更され得る。加えて、「結合される (coupled)」という用語およびその変形は、2 つの構成要素間に通信経路を有することを説明するものであって、それらの間に介在する構成要素／接続を伴わない構成要素間の直接の接続を意図するものではない。これらの変形はすべて、本明細書の一部とみなされる。

【0022】

本明細書における 1 つ以上の実施形態は、付加的なセキュリティを提供するためにソフトウェアとマシンとの間の効率的な軽量のインターフェースを利用している。この場合、このインターフェースは、セキュア・インターフェース制御が大多数の割り込みイネーブル命令 (例、ロード・プログラム状況ワードまたはロード制御) をエミュレートすることを可能にする一方で、信頼されないエンティティがセキュア・エンティティの代わりに保留割り込みを維持することをなおも可能にするために使用される。この保留割り込み構造は、ハードウェアにおいてディスパッチされていないセキュア・エンティティに基づく割り込みの優先順位付けに対処するために、信頼されないエンティティによって必要とされる。本明細書における 1 つ以上の実施形態の技術効果および利益は、セキュア・ゲスト状態またはメモリへの信頼されないエンティティのアクセスを許可することなく、単一の場所にこの複雑なコードを存在させることによって、複雑性およびリスクを低減することを含む。

【0023】

ホスト・ハイパーバイザ (例、信頼されないエンティティ) の制御下でゲストとして動作する仮想マシン (VM) は、そのゲストに対する仮想化サービスを透過的に提供するためにそのハイパーバイザに頼っている。これらのサービスは、セキュア・エンティティと別の信頼されないエンティティとの間の任意のインターフェースに適用でき、そのインターフェースはこの他方のエンティティによるセキュア・リソースへのアクセスを従来可能にするものである。前述のとおり、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み得るが、これに限定されない。たとえば、割り込みおよび例外挿入のために、ハイパーバイザは通常ゲストのプレフィックス・エリア (低コア) への読取りもしくは書込みまたはその両方を行う。本明細書において用いられる「仮想マシン」または「VM」という用語は、物理マシン (コンピュータ・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) の論理的表現を示す。VM は、基礎的なホスト・マシン (物理プロセッサまたはプロセッサのセット) において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・リソースの観点からは、VM は自身の独立した物理マシンであるように見える。本明細書において用いられる「ハイパーバイザ」および「VM モニタ (VMM: VM Monitor)」という用語は、同じホスト・マシンにおいて複数の (かつ異なることもある) OS を用いて複数の VM が実行され得るように管理を行う処理環境またはプラットフォーム・サービスを示す。当然のことながら、VM の配置は VM のインストール・プロセスと、VM のアクティベーション (または始動) プロセスとを含む。別の例において、VM の配置は VM のアクティベーション (または始動) プロセスを含む (例、VM が予めインストールされているか、または既に存在している場合)。

【0024】

現在利用可能な技術的解決策において、ハイパーバイザ (例、IBM (IBM 社の登録

10

20

30

40

50

商標)のz/VM(IBM社の登録商標)、またはオープン・ソース・ソフトウェアのカーネル・ベース仮想マシン(KVM:Kernel Based Virtual machine))は、解釈実行開始(SIE:Start-Interpretive-Execution)命令を発行してSIEエントリ・ミリコードを呼び出すことによって、物理処理ユニットまたはホスト・サーバにおける新たなVM仮想CPU(vCPU:virtual CPU)をディスパッチする。ミリコードは、プロセッサ・ハードウェアに対する拡張機能として動作する信頼されるファームウェアである。SIE命令のオペランドは状態記述と呼ばれる制御ブロックであり、それはゲスト状態を含む。SIEエントリの際に、このゲスト状態(汎用目的および制御レジスタ、ゲスト命令アドレスおよびゲスト・プログラム状況ワード(PSW:program-status-word)を含む)がミリコードによってハードウェアにロードされる。これによって、ゲストvCPUが物理プロセッサで動作できるようになる。vCPUがハードウェアで動作している間、ゲスト状態はハードウェア内に維持される。どこかの時点で、ハードウェア/ミリコードは制御をハイパーバイザに戻す必要がある。このことはしばしばSIEエグジットと呼ばれる。これが必要になるのはたとえば、このvCPUがハイパーバイザによるエミュレーションを必要とする命令を実行するとき、またはvCPUのタイムスライス(すなわち、このvCPUが物理プロセッサで動作するために割り当てられた時間)が経過したときなどであってもよい。既存のハイパーバイザは、vCPUをディスパッチするためにSIE命令を通じてこうしたインターフェースを使用することに頼っている。

【0025】

セキュア・ゲスト(例、セキュア・エンティティ)を促進およびサポートするために、ハイパーバイザに頼らないハイパーバイザとセキュア・ゲストとの間の付加的なセキュリティが必要とされることで、ハイパーバイザはVMからのデータにアクセスできないために上述のやり方でサービスを提供できなくなるところに、技術的課題が存在する。

【0026】

本明細書に記載されるセキュア実行は、セキュア・ストレージおよび非セキュア・ストレージの間、ならびに異なるセキュア・ユーザに属するセキュア・ストレージの間の分離を保証するためのハードウェア機構を提供する。セキュア・ゲストに対して、「信頼されない」非セキュア・ハイパーバイザとセキュア・ゲストとの間に付加的なセキュリティが提供される。これを行うためには、通常ハイパーバイザがゲストの代わりに行う機能の多くをマシンに組み込む必要がある。ハイパーバイザとセキュア・ゲストとのセキュア・インターフェースを提供するための、本明細書において「UV」とも呼ばれる新たなセキュア・インターフェース制御についてここに説明する。本明細書において、セキュア・インターフェース制御およびUVという用語は交換可能に用いられる。セキュア・インターフェース制御は、この付加的なセキュリティを提供するためにハードウェアと連携して働く。

【0027】

一例において、セキュア・インターフェース制御は、内部のセキュアかつ信頼されるハードウェアもしくはファームウェアまたはその両方において実現される。セキュア・ゲストまたはエンティティに対して、セキュア・インターフェース制御は、セキュア環境の初期化および維持と、ハードウェアにおけるこれらのセキュア・エンティティのディスパッチの調整とを提供する。セキュア・ゲストがデータをアクティブに使用しており、かつそのデータがホスト・ストレージに存在するとき、それはセキュア・ストレージ内で「暗号化されずに」保たれる。セキュア・ゲスト・ストレージはその単一のセキュア・ゲストによるアクセスが可能であり、これはハードウェアによって厳密に実施される。つまり、ハードウェアは、任意の非セキュア・エンティティ(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ことを防ぐ。この例において、セキュア・インターフェース制御は、ファームウェアの最低レベルの信頼される部分として実行される。最低レベルすなわちミリコードは、実際にはハードウェアの拡張機能であり、たとえばIBM(IBM社の登録商標)のzArchitecture(IBM社の登録商標)などにおいて定義される複雑な命令および機能を実

10

20

30

40

50

現するために用いられる。ミリコードはストレージのすべての部分にアクセスでき、セキュア実行の状況において、ストレージには自身のセキュア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が含まれる。このため、ミリコードは、セキュア・ゲストまたはそのゲストのサポートを行うハイパーバイザが必要とする任意の機能を提供できる。セキュア・インターフェース制御はハードウェアへの直接アクセスも有し、それによってハードウェアは、セキュア・インターフェース制御が確立した条件の制御下でセキュリティ・チェックを効率的に提供できる。

【0028】

本発明の1つ以上の実施形態によると、セキュア・ページをマーク付けするためにハードウェア内にセキュア・ストレージ・ビットが提供される。このビットがセットされるとき、ハードウェアは任意の非セキュア・ゲストまたはハイパーバイザがこのページにアクセスすることを防ぐ。加えて、各セキュア・ページまたは共有ページは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（ID: *i d e n t i f i c a t i o n*）によってタグ付けされる。そのページが非セキュアであるときは、ゾーンセキュリティ・テーブルにおいてそのようにマーク付けされる。このゾーンセキュリティ・テーブルは、パーティションまたはゾーン毎にセキュア・インターフェース制御によって維持される。そのページがセキュア・ゲストまたはそれを所有するエンティティのみにアクセスされることを検証するためにセキュア・エンティティによって行われる任意のDAT変換においてハードウェアによって用いられるホスト絶対ページ毎に1つのエン

【0029】

本発明の1つ以上の実施形態によると、ソフトウェアはUVコール（UV C: *U V C a l l*）命令を用いて、セキュア・インターフェース制御が特定の動作を行うことを要求する。たとえばUV C命令は、セキュア・インターフェース制御を初期化し、セキュア・ゲスト・ドメイン（例、セキュア・ゲスト構成）を作成し、そのセキュア構成内に仮想CPUを作成するために、ハイパーバイザによって使用され得る。加えて、ハイパーバイザのページイン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（復号してセキュア・ゲスト・ドメインに割り当てる）およびエクスポート（暗号化してホストのアクセスを許可する）するためにUV C命令が用いられ得る。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の定義、セキュア・ストレージの共有化、および共有ストレージのセキュア化を行う能力を有する。

【0030】

ハイパーバイザがセキュア・ゲスト・データを透過的にページインおよびページアウトするときにセキュリティを提供するために、セキュア・インターフェース制御はハードウェアとともに働いて、データの復号および暗号化を提供および保証する。このことを達成するために、ハイパーバイザは、ゲスト・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たなUV Cを発行することが要求される。これらの新たなUV Cの際にセキュア・インターフェース制御によってセットアップされた制御に基づいて、ハードウェアはこれらのUV Cが確かにハイパーバイザによって発行されたことを保証することとなる。

【0031】

この新たなセキュア環境において、ハイパーバイザがセキュア・ページをページアウトするときは常に、セキュア・ストレージからの新たな変換（エクスポート）UV Cを発行することが要求される。このエクスポートUV Cに応答して、UVまたはセキュア・インターフェース制御は、1) そのページがUVによって「ロック」されたことを示し、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ロックをリセットすることとなる。エクスポートUV Cが完了したとき、ハイパーバイザはここで暗号化ゲスト・ページをページアウトすることができる。

【0032】

10

20

30

40

50

加えて、ハイパーバイザがセキュア・ページをページインするときは常に、ハイパーバイザはセキュア・ストレージへの新たな変換（インポート）UVCを発行する必要がある。このインポートUVCに応答して、UVまたはセキュア・インターフェース制御は、1）ハードウェアにおいてそのページをセキュアとマーク付けし、2）ページがUVによって「ロック」されたことを示し、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ロックをリセットすることとなる。セキュア・エンティティによるアクセスが行われるときは常に、ハードウェアは変換の際にそのページに対する認可チェックを行う。これらのチェックは、1）そのページがアクセスを試みているセキュア・ゲスト・ドメインに確か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・メモリに存在していた間にハイパーバイザがこのページのホスト・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。ページがセキュアであるとマーク付けされたとき、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のいずれかによる任意のセキュア・ページへのアクセスを防ぐ。付加的な変換ステップは、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リマッピングを防ぐ。

【0033】

ハイパーバイザが非セキュア・ゲストの代わりに命令をエミュレートする場合がある。しかし、セキュア・ゲストに対しては、セキュア・インターフェース制御が介在して、「信頼されない」ハイパーバイザがセキュア・ゲスト状態を損なうおそれがある任意の機能を提供する必要がある。この介在はいくつかの理由のために必要なことがある。たとえば、この命令のエミュレーションは、セキュア・ゲスト・メモリまたはセキュア・ゲスト設備へのアクセスを必要とすることがある。いくつかの場合には、UVが命令を完全にエミュレートすることとなる。他の場合には、セキュア・インターフェース制御が命令のエミュレーションを完了するが、ゲスト状態に対する何らかの更新をハイパーバイザに通知することとなる。さらに他の場合には、ゲスト状態を損なわずにセキュア・インターフェース制御とハイパーバイザとの間で限定された情報を受け渡しするために、インターフェースが用いられる。このアプローチはセキュア・インターフェース制御とハイパーバイザとの間で軽量のインターフェースを利用して、この場合にはセキュア・インターフェース制御における保留割り込み構造の複製の最小化を可能にする。ここで図1を参照すると、本発明の1つ以上の実施形態によるゾーン・セキュリティに対するテーブル100が一般的に示されている。図1に示されるゾーン・セキュリティ・テーブル100は、セキュア・インターフェース制御によって維持され、セキュア・エンティティにアクセスされる任意のページに対するセキュア・アクセスを保証するために、セキュア・インターフェー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によってインデックス付けされる110。つまり、ホスト絶対ストレージの各ページに対して1つのエントリが存在する。各エントリは、そのエントリがアクセスを行うセキュア・エンティティに属することを検証するために用いられる情報を含む。

【0034】

さらに、図1に示されるとおり、ゾーン・セキュリティ・テーブル100は、セキュア・ドメインID120（このページに関連するセキュア・ドメインを識別する）と、UVビット130（このページはセキュア・インターフェース制御に供与されたものであり、セキュア・インターフェース制御が所有することを示す）と、ディスエーブル・アドレス比較（DA:disable address compare）ビット140（たとえばホスト絶対として定められたセキュア・インターフェース制御ページに関連するホスト仮想アドレスを有さないときなど、特定の状況においてホスト・アドレス対比較をディスエーブルするために用いられる）と、共有（SH:shared）ビット150（この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に対して登録されたホスト仮想アドレスを示し、これはホスト・アドレス対と呼ばれる）とを含む。なお、ホスト・アドレス対は、ホスト絶対および関連する登録されたホスト仮想アドレスを示す。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ときのこのページのマッピングを表し、その比較は、ゲストに使用されている間にホストがそのページをリマップしないことを保証する。

【0035】

ダイナミック・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プするために用いられる。ゲストVMがハイパーバイザの制御下でページ可能ゲストとして動作するとき、ゲストは自身のメモリに存在するページを管理するためにDATを用いる。加えてホストは独立して、それらのゲスト・ページが自身のメモリに存在するときにそれらのページ（および自身のページ）を管理するためにDATを用いる。ハイパーバイザは、異なるVM間のストレージの分離もしくは共有またはその両方を提供するため、およびハイパーバイザ・ストレージへのゲストのアクセスを防ぐためにDATを用いる。ゲストが非セキュア・モードで動作しているとき、ハイパーバイザはゲストのストレージのすべてにアクセスできる。

【0036】

DATは、1つのアプリケーションと別のアプリケーションとの分離を可能にする一方で、それらが共通のリソースを共有することをなおも可能にする。加えてDATはVMの実現を可能にし、それはアプリケーション・プログラムの同時処理とともに新たなバージョンのOSの設計およびテストに用いられてもよい。仮想アドレスは、仮想ストレージ内の場所を識別する。アドレス・スペースは仮想アドレスの連続配列であり、特定の変換パラメータ（DATテーブルを含む）が伴うことによって、各仮想アドレスは、ストレージ内のバイト位置によってそのアドレスを識別する関連絶対アドレスに変換され得る。

【0037】

DATは、仮想アドレスを関連絶対アドレスに変換するためにマルチテーブル・ルックアップを用いる。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および維持される。このストレージ・マネージャは、たとえば1つのページをページアウトして別のページを取り入れることなどによって、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、たとえばストレージ・マネージャは関連するページ・テーブルにおいて無効ビットをセットすることとなる。プログラムがページアウトされたページへのアクセスを試みるとき、ハードウェアはストレージ・マネージャに、しばしばページ・フォールトと呼ばれるプログラム割り込みを提供することとなる。応答において、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て、無効ビットをリセットすることとなる。これはすべてプログラムに対して透過的に行われ、ストレージ・マネージャがストレージを仮想化してそれをさまざまな異なるユーザに共有させることを可能にする。

【0038】

CPUがメイン・ストレージにアクセスするために仮想アドレスを用いるとき、仮想アドレスは最初にDATによって実アドレスに変換され、次いでプレフィックス変換によって絶対アドレスにされる。特定のアドレス・スペースに対する最高レベルのテーブルの指定（オリジンおよび長さ）はアドレス・スペース制御エレメント（ASCE: address-space-control element）と呼ばれ、関連するアドレス・スペースを定義する。

【0039】

ここで図2を参照すると、本発明の1つ以上の実施形態によるDATを行うための仮想アドレス・スペース202および204ならびに絶対アドレス・スペース206の例が一般的に示されている。図2に示される例においては、2つの仮想アドレス・スペース、すなわち仮想アドレス・スペース202（アドレス・スペース制御エレメント（ASCE）A 208によって定められる）および仮想アドレス・スペース204（ASCE B 210によって定められる）が存在する。仮想ページA1. V 212 a1、A2. V 212 a2、およびA3. V 212 a3は、マルチテーブル（セグメント230およびページ・テーブル232 a、232 b）ルックアップにおいてストレージ・マネージャによって、ASCE A 208を用いて絶対ページA1. A 220 a1、A2. A 220 a

2、およびA3．A 220a3にマップされる。同様に、仮想ページB1．V 214b1およびB2．V 214b2は2テーブル234および236ルックアップにおいて、ASCE B 210を用いて絶対ページB1．A 222b1およびB2．A 222b2にそれぞれマップされる。

【0040】

ここで図3を参照すると、本発明の1つ以上の実施形態によるハイパーバイザの下で動作するVMをサポートするために用いられるネストされたマルチパートDAT変換の例が一般的に示されている。図3に示される例においては、ゲストA仮想アドレス・スペースA 302（ゲストASCE（GASCE: guest ASCE）A 304によって定められる）およびゲストB仮想アドレス・スペースB 306（GASCE B 308によって定められる）の両方が、共有ホスト（ハイパーバイザ）仮想アドレス・スペース325に存在する。示されるとおり、ゲストAに属する仮想ページA1．GV 310a1、A2．GV 310a2、およびA3．GV 310a3は、ゲストAストレージ・マネージャによってGASCE A 304を用いてゲスト絶対ページA1．HV 340a1、A2．HV 340a2、およびA3．HV 340a3にそれぞれマップされ、ゲストBに属する仮想ページB1．GV 320b1およびB2．GV 320b2は、独立的にゲストBストレージ・マネージャによって、GASCE B 308を用いてゲスト絶対ページB1．HV 360b1およびB2．HV 360b2にそれぞれマップされる。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・スペース325に直接マップされた後に、ホスト絶対アドレス・スペース330に対する付加的なホストDAT変換を受ける。示されるとおり、ホスト仮想アドレスA1．HV 340a1、A3．HV 340a3、およびB1．HV 360b1は、ホスト・ストレージ・マネージャによってホストASCE（HASCE: host ASCE）350を用いてA1．HA 370a1、A3．HA 370a3、およびB1．HA 370b1にマップされる。ゲストAに属するホスト仮想アドレスA2．HV 340a2およびゲストBに属するB2．HV 360b2は、どちらも同じホスト絶対ページAB2．HA 380にマップされる。これによって、これら2つのゲスト間でデータを共有することが可能になる。ゲストDAT変換の際に、各々のゲスト・テーブル・アドレスはゲスト絶対として処理され、付加的なネストされたホストDAT変換を受ける。

【0041】

本明細書に記載される本発明の実施形態は、セキュア・ゲストおよびUVストレージ保護を提供する。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、所与の存在するセキュア・ゲスト・ページに対して、以下が起こることを提供する。関連ホスト絶対アドレスは、単一のハイパーバイザ（ホスト）DATマッピングのみを通じ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任意の所与のホスト絶対アドレスにマップされる単一のホスト仮想アドレスが存在する。所与のセキュア・ゲスト・ページに関連するハイパーバイザDATマッピング（ホスト仮想対ホスト絶対）は、ページインされている間は変わらない。セキュア・ゲスト・ページに関連するホスト絶対ページは、単一のセキュア・ゲストに対してマップされる。

【0042】

本発明の1つ以上の実施形態によると、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との間で共有される。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ースによってアクセス可能であるが、ゲスト／ホストはアクセスできない。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ースに割り当てられる。本発明の1つ以上の実施形態によると、これらの規則に違反しようとする任意の試みは、ハードウェアおよびセキュア制御インターフェースによって禁止される。

【0043】

ここで図4を参照すると、本発明の1つ以上の実施形態によるセキュア・ゲスト・スト

レージのマッピングの例が一般的に示されている。図4は図3と類似しているが、図4の例はセキュア・ゲストAとセキュア・ゲストBとのストレージの共有を許可しないところが異なっている。図3の非セキュアの例においては、ゲストAに属するホスト仮想アドレスA2.HV 340a2およびゲストBに属するB2.HV 360b2は、どちらも同じホスト絶対ページAB2.HA 380にマップされる。図4のセキュア・ゲスト・ストレージの例においては、ゲストAに属するホスト仮想アドレスA2.HV 340a2はホスト絶対アドレスA2.HA 490aにマップされ、一方でゲストBに属するB2.HV 360b2は自身のB2.HA 490bにマップされる。この例では、セキュア・ゲスト間の共有は存在しない。

【0044】

セキュア・ゲスト・ページがディスク上に存在する間、それは暗号化される。ハイパーバイザがセキュア・ゲスト・ページをページインするとき、ハイパーバイザはUVコール(UVC)を発行し、それによってセキュア制御インターフェースはそのページをセキュアとマーク付けし(共有されない限り)、そのページを復号し(共有されない限り)、かつそのページを適切なセキュア・ゲスト(たとえばゲストA)に属するものとして(ゾーン・セキュリティ・テーブルに)登録する。加えて、セキュア制御インターフェースは、関連するホスト仮想アドレス(たとえばA3.HV 340a3)をそのホスト絶対ページに対して登録する(ホスト・アドレス対と呼ばれる)。ハイパーバイザが正しいUVCを発行できないとき、ハイパーバイザはセキュア・ゲスト・ページへのアクセスを試み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、同様のUVCが発行され、それによって、ゲスト・ページが非セキュアとマーク付けされて非セキュアとしてゾーン・セキュリティ・テーブルに登録される前に、ゲスト・ページが暗号化される(共有されない限り)。

【0045】

5つの所与のホスト絶対ページK、P、L、M、およびNを有する例において、ハイパーバイザがそれらをページインするときに、セキュア制御インターフェースによって各々のホスト絶対ページはセキュアとマーク付けされる。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それらのホスト絶対ページにアクセスすることが防がれる。ホスト絶対ページK、P、およびMは、ハイパーバイザがそれらをページインするときにゲストAに属するものとして登録され、ホスト絶対ページLおよびNは、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に対して登録される。単一のセキュア・ゲストとハイパーバイザとに共有されるページである共有ページは、ページングの際に符号化も復号もされない。それらの共有ページはセキュアと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、ゾーン・セキュリティ・テーブルにおいて単一のセキュア・ゲスト・ドメインとともに登録される。

【0046】

本発明の1つ以上の実施形態によると、非セキュア・ゲストまたはハイパーバイザがセキュア・ゲストの所有するページへのアクセスを試みるとき、ハイパーバイザはセキュア・ストレージ・アクセス(PIC3D)例外を受信する。これを定めるために付加的な変換ステップは必要とされない。

【0047】

1つ以上の実施形態によると、セキュア・エンティティがページへのアクセスを試みるとき、ハードウェアは、ストレージがその特定のセキュア・ゲストに確かに属することを検証する付加的な変換チェックを行う。もしそうでなければ、非セキュア・アクセス(PIC3E)例外がハイパーバイザに提供される。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・テーブルに登録されたホスト・アドレス対からのホスト仮想アドレスと一致しないときは、セキュア・ストレージ侵害('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可する限り、セキュアとマーク付けされていないストレージにアクセスしてもよい。

10

20

30

40

50

【0048】

ここで図5を参照すると、本発明の1つ以上の実施形態によるDAT動作のシステム概要500が一般的に示されている。システム概要500はホスト一次仮想アドレス・スペース510と、ホスト・ホーム仮想アドレス・スペース520とを含み、ここからページがハイパーバイザ（ホスト）絶対アドレス・スペース530に変換される（例、ホストDAT変換525を参照、なお点線はDAT変換525を通じたマッピングを表す）。たとえば図5は、2つの異なるホスト仮想アドレス・スペースによるホスト絶対ストレージの共有に加えて、それらのホスト仮想アドレスの1つを2つのゲストだけでなくホスト自体とも共有することを示している。これに関して、ホスト一次仮想アドレス・スペース510およびホスト・ホーム仮想アドレス・スペース520は、2つのホスト仮想アドレス・スペースの例であり、その各々はホスト一次ASCE（HPASCE：host primary ASCE）591およびホスト・ホームASCE（HHASCE：host home ASCE）592という別個のASCEによってそれぞれアドレス指定される。なお、すべてのセキュア・インターフェース制御ストレージ（仮想および実の両方）はハイパーバイザによって供与され、セキュアとマーク付けされる。いったん供与されると、セキュア・インターフェース制御ストレージは、関連するセキュア・エンティティが存在する限り、セキュア・インターフェース制御のみによってアクセスされ得る。

10

【0049】

図示されるとおり、ホスト一次仮想アドレス・スペース510はゲストA絶対ページA1．HVと、ゲストA絶対ページA2．HVと、ゲストB絶対ページB1．HVと、ホスト仮想ページH3．HVとを含む。ホスト・ホーム仮想アドレス・スペース520はセキュア・インターフェース制御仮想ページU1．HVと、ホスト仮想ページH1．HVと、ホスト仮想ページH2．HVとを含む。

20

【0050】

本発明の1つ以上の実施形態によると、すべてのセキュア・ゲスト（例、セキュア・ゲストAおよびセキュア・ゲストB）ストレージは、セキュア・ゲスト構成に属するものとして本明細書に記載されるゾーンセキュリティ・テーブルに登録され、関連するホスト仮想アドレス（例、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つ以上の実施形態において、すべてのセキュア・ゲスト・ストレージは、ホスト一次仮想スペースにマップされる。加えて、すべてのセキュア・インターフェース制御ストレージもセキュア・インターフェース制御に属するものとしてゾーンセキュリティ・テーブルに登録され、ゾーンセキュリティ・テーブルにおいて関連するセキュア・ゲスト・ドメインに基づいてさらに区別されてもよい。本発明の1つ以上の実施形態によると、UV仮想ストレージはホスト・ホーム仮想スペースにマップされ、関連するホスト仮想アドレスはホスト・アドレス対の一部として登録される。1つ以上の実施形態によると、UV実ストレージは関連するホスト仮想マッピングを有さず、このことを示すためにゾーンセキュリティ・テーブルのDAビット（仮想アドレス比較がディスエーブルされたことを示す）がセットされる。ホスト・ストレージは非セキュアとマーク付けされ、ゾーンセキュリティ・テーブルにも非セキュアとして登録される。

30

【0051】

よって、「ゲスト絶対＝ホスト仮想」である場合は、ハイパーバイザ（ホスト）一次DATテーブル（HPASCE591によって定められる）はホスト一次仮想アドレス・スペース510のページを次のとおりに変換する。ゲストA絶対ページA1．HVはセキュア・ゲストAに属するホスト絶対A1．HAにマップされ、ゲストA絶対ページA2．HVはセキュア・ゲストAに属するホスト絶対A2．HAにマップされ、ゲストB絶対ページB1．HVはセキュア・ゲストBに属するホスト絶対B1．HAにマップされ、ホスト仮想ページH3．HVはホスト絶対ページH3．HA非セキュア・ホストにマップされる（非セキュアであるためホスト・アドレス対は存在しない）。さらに、ハイパーバイザ（ホスト）ホームDATテーブル（HHASCE592によって定められる）は、ホスト・ホーム仮想アドレス・スペース520のページを次のとおりに変換する。セキュア・イン

40

50

ターフェース制御仮想ページU1。HVはセキュアUV仮想として定められたホスト絶対ページU1。HAにマップされ、ホスト仮想ページH1。HVは非セキュアとして定められたホスト絶対ページH1。HAにマップされ、ホスト仮想ページH2。HVは非セキュアとして定められたホスト絶対ページH2。HAにマップされる。H1。HAまたはH2。HAのいずれかに関連するホスト・アドレス対は、それらが非セキュアであるために存在しない。

【0052】

動作中に、セキュア・ゲストがセキュア・インターフェース制御に割り当てられたセキュア・ページへのアクセスを試みると、セキュア・ストレージ侵害（‘3F’X）例外がハードウェアによってハイパーバイザに提供される。非セキュア・ゲストまたはハイパーバイザが任意のセキュア・ページ（セキュア・インターフェース制御に割り当てられたものを含む）へのアクセスを試みると、セキュア・ストレージ・アクセス（‘3D’X）例外がハードウェアによってハイパーバイザに提供される。代替的に、セキュア・インターフェース制御スペースに対して行われたアクセスの試みに対して、エラー条件が提供され得る。ハードウェアがセキュア・インターフェース制御アクセスにおけるセキュア割り当てにおけるミスマッチを検出したとき（例、ストレージがセキュア・インターフェース制御ではなくセキュア・ゲストに属するものとしてゾーン・セキュリティ・テーブルに登録されているか、または用いられているホスト・アドレス対と登録された対とのミスマッチが存在するとき）、チェックが提供される。

【0053】

言い換えると、ホスト一次仮想アドレス・スペース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に属する）ならびにB1。HV（セキュア・ゲストBに属する）を含み、これらはホスト絶対A1。HA、A2。HA、およびB1。HAにそれぞれマップされる。加えて、ホスト一次仮想アドレス・スペース510はホスト（ハイパーバイザ）ページH3。HVを含み、これはホスト絶対H3。HAにマップされる。ホスト・ホーム仮想スペース520は2つのホスト仮想ページH1。HVおよびH2。HVを含み、これらはホスト絶対ページH1。HAおよびH2。HAにマップされる。ホスト一次仮想アドレス・スペース510およびホスト・ホーム仮想アドレス・スペース520は、両方とも単一のホスト絶対530にマップされる。セキュア・ゲストAおよびセキュア・ゲストBに属するストレージ・ページはセキュアとマーク付けされ、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ともに図1に示されるゾーン・セキュリティ・テーブル100に登録される。他方でホスト・ストレージは、非セキュアとマーク付けされる。ハイパーバイザがセキュア・ゲストを定めているとき、ハイパーバイザは、これらのセキュア・ゲストのサポートに必要なセキュア制御ブロックに用いるためにホスト・ストレージをセキュア・インターフェース制御に供与する必要がある。このストレージはホスト絶対またはホスト仮想スペースのいずれかで定められてもよく、一例において具体的には、ホスト・ホーム仮想スペースで定められる。図5に戻ると、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められるセキュア・インターフェース制御ストレージである。結果として、これらのページはセキュアとマーク付けされ、図1に示されるゾーン・セキュリティ・テーブル100に、セキュア・インターフェース制御に属するものとして関連するセキュア・ドメインとともに登録される。これらのページはホスト絶対アドレスとして定められるために関連するホスト仮想アドレスは存在しないため、ゾーン・セキュリティ・テーブル100にはDAビットがセットされる。

【0054】

変換後のハイパーバイザ（ホスト）絶対アドレス・スペース530の例が図6に見出され得る。図6には、本発明の1つ以上の実施形態によるセキュア・インターフェース制御メモリに関するシステム概要600が示されている。システム概要600はハイパーバイザ（ホスト）絶対アドレス・スペース630を示しており、これはホスト絶対ページA2。HAセキュア・ゲストA（A2。HVに対するもの）と、ホスト絶対ページB1。HA

セキュア・ゲストB（B1．HVに対するもの）と、ホスト絶対ページH1．HA非セキュア（ホスト）と、ホスト絶対ページH2．HA非セキュア（ホスト）と、ホスト絶対ページU3．HAセキュアUV実（HVマッピングなし）と、ホスト絶対ページU1．HAセキュアUV仮想（U1．HVに対するもの）と、ホスト絶対ページA1．HAセキュア・ゲストA（A1．HVに対するもの）とを含む。

【0055】

ここで図7を参照すると、本発明の1つ以上の実施形態によるインポート動作に対するプロセスの流れ700が一般的に示されている。ハイパーバイザによってページアウトされたページにセキュア・ゲストがアクセスするとき、そのページをセキュアに中に戻すために、たとえばプロセスの流れ700に示されるような一連のイベントが生じる。プロセスの流れ700はブロック705にて開始され、ここでセキュア・ゲストはゲスト仮想ページにアクセスする。たとえばそのページが無効であるために、ハードウェアは、プログラム割り込みコード11（PIC11：program-interruption-code11）によって示されるホスト・ページ・フォールトをハイパーバイザに提供する（ブロック715を参照）。次にハイパーバイザは、このゲスト・ページに対して利用可能な非セキュア・ホスト絶対ページを特定し（ブロック720を参照）、特定されたホスト絶対ページに暗号化されたゲスト・ページをページインする（ブロック725を参照）。

【0056】

ブロック730において、次いでホスト絶対ページは適切な（ホスト仮想アドレスに基づく）ホストDATテーブルにマップされる。ブロック735において、次いでハイパーバイザ・ホストはセキュア・ゲストを再ディスパッチする。ブロック740において、セキュア・ゲストはゲスト・セキュア・ページに再アクセスする。ページ・フォールトはもはや存在しないが、このセキュア・ゲスト・アクセスおよびページは図1のゾーンーセキュリティ・テーブル100においてセキュアとマーク付けされていないため、ブロック745において、ハードウェアは非セキュア・ストレージ例外（PIC3E）をハイパーバイザに提供する。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、プロセスの流れ700は「A」に進み、これは図8に接続する。

【0057】

ここで図8を参照すると、本発明の1つ以上の実施形態によるインポート動作を行うためのプロセスの流れ800が一般的に示されている。挙動の良好なハイパーバイザ（例、エラーなしに予期される方式で動作している）は、PIC3Eに応答してインポートUVCを発行することとなる（ブロック805を参照）。なお、この時点でインポートされるべきページは非セキュアとマーク付けされており、ハイパーバイザと、その他の非セキュア・エンティティと、セキュア・インターフェース制御とのみによるアクセスが可能である。セキュア・ゲストはそのページにアクセスできない。

【0058】

インポートUVCの一部として、セキュア・インターフェース制御として動作する信頼されるファームウェアは、このページがすでにセキュア・インターフェース制御によってロックされているかどうかをチェックする（判定ブロック810を参照）。もしそうであれば、プロセスの流れ800はブロック820に進む。ブロック820において、「ビジー」戻りコードがハイパーバイザに戻され、ハイパーバイザはそれに応答してインポートUVCを遅延させ（ブロック825を参照）、再発行する（プロセスの流れ800はブロック805に戻る）。もしそのページがまだロックされていなければ、次いでプロセスの流れ800は判定ブロック822に進む。

【0059】

判定ブロック822において、セキュア・インターフェース制御は、そのページが非セキュア・ハイパーバイザと共有されるページかどうかをチェックする。もしそのページが共有されていれば（プロセスの流れ800は判定ブロック824に進む）、セキュア・インターフェース制御はゾーンーセキュリティ・テーブルにホスト絶対アドレスとともに、

関連するセキュア・ゲスト・ドメイン、ホスト仮想アドレス、および共有されていることを登録する。このページは非セキュアとマーク付けされたままである。これによってインポートUVCは完了し、このページはゲストによるアクセスのために利用可能となる。ハイパーバイザがゲストを再ディスパッチすることによって処理が続き（ブロック830）、セキュア・ゲストはページに正常にアクセスする（ブロック835）。

【0060】

インポートされるべき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とき（プロセスの流れ800はブロック840に進む）、セキュア・インターフェース制御はそのページをセキュアとマーク付けすることとなるため、ハイパーバイザはそのページにアクセスできなくなる。ブロック845において、セキュア・インターフェース制御はページをロックして、他のUVCがページ状態を変更できないようにする。ロックが設定されたとき（ブロック850）、セキュア・インターフェース制御は、ゲスト・ページが暗号化されている間にその内容が変わらなかったことを検証することとなる。もしその内容が変わっていれば、ハイパーバイザにエラー戻りコードが戻され、そうでなければセキュア・インターフェース制御はセキュア・ページを復号することとなる。

【0061】

ブロック855において、セキュア・インターフェース制御はページのロックを解除し、他のUVCによるアクセスを可能にし、そのページをゾーン・セキュリティ・テーブルに、セキュアでありかつ適切なゲスト・ドメインおよびホスト仮想アドレスと関連するものとして登録して、ホスト・アドレスHV→HA対を完了させる。これによってゲストによるアクセスが可能になり、UVCが完了する。

【0062】

ここで図9を参照すると、本発明の1つ以上の実施形態による供与メモリ動作に関するプロセスの流れ900が一般的に示されている。プロセスの流れ900はブロック905で開始され、ここでハイパーバイザはクエリUVCをセキュア・インターフェース制御に発行する。ブロック910において、セキュア・インターフェース制御はデータを戻す（例、クエリUVC）。このデータは、必要とされるベース・ゾーン・特定のホスト絶対ストレージの量、必要とされるベース・セキュア・ゲスト・ドメイン・特定のホスト絶対ストレージの量、MB毎に必要とされる可変セキュア・ゲスト・ドメイン・特定のホスト仮想ストレージの量、もしくは必要とされるベース・セキュア・ゲスト・CPU・特定のホスト絶対ストレージの量、またはその組み合わせを含み得る。

【0063】

ブロック915において、ハイパーバイザはベース・ホスト・絶対ゾーン・特定のストレージ（例、クエリUVCから戻されたサイズに基づく）を予約する。ブロック920において、ハイパーバイザはセキュア・インターフェース制御に初期化を発行する。これに関して、ハイパーバイザは、ゾーン全体に対するセキュア・ゲスト構成の間で調整する必要があるUV制御ブロックに対する供与ストレージを提供する初期化UVCを発行できる。初期化UVCは、ベース・ゾーン・特定のストレージ・オリジンを特定する。

【0064】

ブロック925において、セキュア・インターフェース制御は、UVに対して供与ストレージを登録してセキュアとマーク付けすることによって、初期化（例、初期化UVC）を実現する。初期化UVCに対して、セキュア・インターフェース制御は供与ストレージをセキュアとマーク付けし、ゾーン・セキュリティ・テーブルに対してその供与ストレージのいくらかを割り当て、UV使用のためにゾーン・セキュリティ・テーブルに供与ストレージを独自のセキュア・ドメインとともに登録できるが、関連するセキュア・ゲスト・ドメインは伴わず、関連するホスト・仮想アドレス対は有さないものとして登録する。

【0065】

ブロック930において、ハイパーバイザはストレージ（例、ベースおよび可変セキュア・ゲスト・ドメイン・特定のストレージ）を予約する。たとえば、ハイパーバイザはベースおよび可変（例、セキュア・ゲスト・ドメイン・ストレージのサイズに基づく）セキ

10

20

30

40

50

セキュア・ゲスト・ドメイン・特定のストレージ（例、クエリUVCによって戻されたサイズ）を予約する。ブロック935において、ハイパーバイザはセキュア・インターフェース制御に作成構成を発行する。これに関して、ハイパーバイザは、ベースおよび可変セキュア・ゲスト・ドメイン・特定のストレージ・オリジンを特定する作成ーセキュア・ゲスト・構成UVCを発行できる。さらに、この作成ーセキュア・ゲスト・構成UVCは、このセキュア・ゲスト構成をサポートするために必要とされるUV制御ブロックに対する供与ストレージを提供する。

【0066】

ブロック940において、セキュア・インターフェース制御は作成構成（例、作成ーセキュア・ゲスト・構成UVC）を実施する。作成ーセキュア・ゲスト・構成UVCに対して、セキュア・インターフェース制御は供与ストレージをセキュアとマーク付けし、供与ストレージをUV使用のためにゾーン・セキュリティ・テーブルに登録し、かつ供与ストレージに関連するセキュア・ゲスト・ドメインとともに登録できる。供与ベース（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さないものとして登録される。供与可変（ホスト・仮想）ストレージは、関連するホスト・仮想アドレス対とともに登録される。

【0067】

ブロック945において、ハイパーバイザはベース・セキュア・ゲスト・CPU・特定のストレージ（例、クエリUVから戻されたサイズ）を予約する。ブロック950において、ハイパーバイザはストレージ・オリジンを特定する。たとえば、ハイパーバイザはUVに、ベース・セキュア・ゲスト・CPU・特定のストレージ・オリジンを特定する作成ーセキュア・ゲスト・CPUを発行する。ブロック955において、セキュア・インターフェース制御は作成ーCPU（例、作成ーセキュア・ゲスト・CPU UVC）を実施する。作成ーセキュア・ゲスト・CPU UVCに対して、セキュア・インターフェース制御は供与ストレージをセキュアとマーク付けし、かつ供与ストレージをUV使用のためにゾーン・セキュリティ・テーブルに登録できるが、関連するセキュア・ゲスト・ドメインは伴わず、関連するホスト・仮想アドレス対は有さないものとして登録する。

【0068】

ここで図10を参照すると、本発明の1つ以上の実施形態によるセキュア・インターフェース制御のセキュア・ページへの非セキュア・ハイパーバイザ・ページの移行に関するプロセスの流れ1000が一般的に示されている。このプロセスの流れ1000には、3つのハイパーバイザ・ページが示されている（例、非セキュア・ハイパーバイザ・ページA、非セキュア・ハイパーバイザ・ページB、および非セキュア・ハイパーバイザ・ページC）。

【0069】

ハイパーバイザ（非セキュア）ページA、B、およびCは、非セキュア・エンティティ（ハイパーバイザを含む）によってアクセス可能である。さらに、ハイパーバイザ（非セキュア）ページA、B、およびCは非セキュア（NS: non-secure）とマーク付けされるとともに、ゾーン・セキュリティ・テーブル（例、図1に示されるゾーン・セキュリティ・テーブル100）に非セキュアおよび非共有と登録される。矢印1005において、初期化UVCが発行され、それによってゲスト・ページAはゾーン全体（UV2）に関連するセキュア・インターフェース制御実ストレージ・ページ1010に移行される。セキュア・インターフェース制御実ストレージ1010はセキュアとマーク付けされるとともに、ゾーン・セキュリティ・テーブル（例、図1に示されるゾーン・セキュリティ・テーブル100）にUVとして登録されてもよく、セキュア・ゲスト・ドメインおよびハイパーバイザ対ホスト絶対（HV→HA）マッピングは伴わない。代わりに、セキュア・インターフェース制御実ストレージ1010は独自のUV2セキュア・ドメインとともに登録され、DAビットは1にセットされる。なお、セキュア・インターフェース制御実ストレージ1010は、実のものとしてセキュア・インターフェース制御にアクセスされ得る。

10

20

30

40

50

【0070】

ハイパーバイザ（非セキュア）ページBから矢印1025において、作成－SG－構成または作成－SG－CPU UV Cが発行され、それによってこのページはセキュア・ゲスト・ドメイン（UV S）に関連するセキュア・インターフェース制御実ストレージ1030に移行される。セキュア・インターフェース制御実ストレージ1030はセキュアとマーク付けされるとともに、ゾーン－セキュリティ・テーブル（例、図1に示されるゾーン－セキュリティ・テーブル100）にUVとして関連するセキュア・ゲスト・ドメインとともに登録されてもよく、ハイパーバイザ対ホスト絶対（HV→HA）マッピングは伴わない（すなわち、DAビット＝1）。なお、セキュア・インターフェース制御実ストレージ1010は、セキュア・ゲスト・ドメインの代わりに実のものとしてセキュア・インターフェース制御にアクセスされ得る。

10

【0071】

ハイパーバイザ（非セキュア）ページCから矢印1045において、作成－SG－構成UV Cが発行され、それによってこのページはセキュア・ゲスト・ドメイン（UV V）に関連するセキュア・インターフェース制御仮想ストレージ1050に移行される。セキュア・インターフェース制御仮想ストレージ1050はセキュアとマーク付けされるとともに、ゾーン－セキュリティ・テーブル（例、図1に示されるゾーン－セキュリティ・テーブル100）にUVとして、セキュア・ゲスト・ドメインおよびハイパーバイザ対ホスト絶対（HV→HA）マッピングとともに登録され得る。なお、セキュア・インターフェース制御仮想ストレージ1050は、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。

20

【0072】

ここで図11を参照すると、1つ以上の実施形態によるプログラムまたはセキュア・インターフェー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の流れ1100が示されている。この図面は、セキュア・インターフェース制御がゲスト・ストレージまたはセキュア・インターフェース制御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そのアクセスを正しくタグ付けする必要があるという状況を表している。1100は、このセキュア・インターフェース制御によるストレージ・アクセスのタグ付けを説明するものである。プロセスの流れ1100はブロック1110で開始され、ここでセキュア・インターフェース制御は、自身がセキュア・インターフェース制御ストレージにアクセスしているのかどうかを判定する。

30

【0073】

もしこれがセキュア・インターフェース制御ストレージへのアクセスでなければ、次いでプロセスの流れ1100は判定ブロック1112に進む（NO矢印で示されるとおり）。判定ブロック1112において、セキュア・インターフェース制御は、自身がセキュア・ゲスト・ストレージにアクセスしているのかどうかを判定する。もしこれがセキュア・ゲスト・ストレージへのアクセスでなければ、次いでプロセスの流れ1100は「B」（図12のプロセスの流れ1200に接続する）に進み、非セキュア・アクセスに対するデフォルト設定を用いることとなる。もしこれがセキュア・ゲスト・ストレージへのアクセスであれば、次いでプロセスの流れ1100は判定ブロック1113に進み、ここでセキュア・インターフェース制御は、デフォルト・セキュア・ゲスト・ドメインが用いられているのかどうかを判定する。もしyesであれば、次いでプロセスの流れ1100は「B」（図12のプロセスの流れ1200に接続する）に進み、セキュア・ゲスト・アクセスに対するデフォルト設定を用いることとなる。もしnoであれば、次いでプロセスの流れ1100はブロック1114に進む。ブロック1114において、適切なセキュア・ゲスト・ドメインがSG－セキュアドメイン・レジスタにロードされる（それから「B」に進み、これは図12のプロセスの流れ1200に接続する）。

40

【0074】

もしこれがセキュア・インターフェース制御ストレージへのアクセスであれば、次にプ

50

プロセスの流れ1100はブロック1120に進む（YES矢印で示されるとおり）。ブロック1120において、アクセスはセキュアUV（例、UV-セキュアードメイン・レジスタを用いる）とタグ付けされる。

【0075】

次いでプロセスの流れ1100は判定ブロック1130に進み、ここでセキュア・インターフェース制御は、これがUVVスペース（例、SG-構成変数テーブル）へのアクセスであるかどうかを判定する。もしこれがUVVスペースへのアクセスであれば、次いでプロセスの流れ1100はブロック1134に進む（YES矢印で示されるとおり）。ブロック1134において、アクセスは仮想とタグ付けされる。ブロック1136において、適用可能なセキュア・ゲスト・ドメインがUV-セキュアードメイン・レジスタにロードされる。ブロック1138において、DAT変換およびアクセス・ストレージの開始準備が整う。判定ブロック1130に戻って、もしこれがUVVスペースへのアクセスでなければ、次いでプロセスの流れ1100はブロック1140に進む（NO矢印で示されるとおり）。ブロック1140において、アクセスは実とタグ付けされる。

【0076】

判定ブロック1150において、セキュア・インターフェース制御は、これがUVSスペース（例、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。もしこれがUVSスペースへのアクセスであれば、次いでプロセスの流れ1100はブロック1136に進む（YES矢印で示されるとおり）。もしこれがUVSスペースへのアクセスでなければ、次いでプロセスの流れ1100はブロック1170に進む（NO矢印で示されるとおり）。よってこのアクセスはUV2スペース（例、ゾーン・セキュリティ・テーブル）へのアクセスと考えられる。ブロック1170において、独自のUV2セキュア・ドメインがUV-セキュアードメイン・レジスタにロードされる。

【0077】

図12は、本発明の1つ以上の実施形態によるプロセスの流れ1200を示している。ゲストがディスパッチされる時、SIEエントリ・ファームウェアはハードウェアに対して、ゲストが動作中である（例、ゲスト・モードがアクティブである）ことを示してもよく、かつそのゲストがセキュアかどうかを示し得る。もしゲストがセキュアであれば、関連するセキュア・ゲスト・ドメインがハードウェア（例、SG-セキュアードメイン・レジスタ）にロードされ得る。プログラムがストレージにアクセスするとき、ハードウェアはアクセスの時点のプログラムの現行状態に基づいてアクセスをタグ付けできる。図12は、プロセスの流れ1200においてこのプロセスの例を示している。ブロック1205において、ハードウェアはマシンが現在ゲスト・モードで動作しているかどうかを判定でき、もしそうでなければ、ブロック1210においてそのアクセスがホスト・アクセスであるとタグ付けでき、かつブロック1215において非セキュア・アクセスとタグ付けできる。ブロック1205において、もしマシンがゲスト・モードで動作していれば、ブロック1220においてそのアクセスはゲスト・アクセスとタグ付けされてもよく、さらにブロック1225において、現在のゲストがセキュア・ゲストであるかどうか判定される。もしゲストがセキュアでなければ、ブロック1215においてそのアクセスは非セキュアとタグ付けされ得る。もしゲストがセキュアであれば、ブロック1230においてハードウェアはゲストをセキュアとタグ付けでき、それによってセキュア・ゲストは、そのセキュア・ゲストがディスパッチされたときにロードされたSG-セキュアードメイン・レジスタと関連付けられ得る。非セキュアおよびセキュア・ゲストの両方に対して、ブロック1235においてDAT状態がチェックされ得る。もしDATがオフであれば、ブロック1240においてアクセスが実とタグ付けされ得る。もしDATがオンであれば、ブロック1245においてアクセスが仮想とタグ付けされ得る。DATがオフであることによってブロック1240においてアクセスが実とタグ付けされるか、またはDATがオンであることによってブロック1245において仮想とタグ付けされたとき、ブロック1250においてハードウェアは変換およびアクセス・ストレージを開始する準備が整い、これについては図13でさらに説明する。

10

20

30

40

50

【0078】

図13は、本発明の1つ以上の実施形態によるプロセスの流れ1300においてセキュアおよび非セキュア・アクセスの両方をサポートするためにハードウェアによって行われる変換の例を示している。ブロック1305において、ハードウェアはアクセスがゲスト変換とタグ付けされているかどうかを判定でき、もしそうであり、かつブロック1310においてアクセスが仮想であれば、次いでブロック1315においてゲストDATが行われ得る。ゲストDAT変換の際に、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起こり得る。このテーブル・フェッチはゲスト実とタグ付けされてもよく、かつ元の変換がセキュアとタグ付けされているときはセキュアとタグ付けされ得る。このテーブル・フェッチも、プロセスの流れ1300の変換プロセスに従い得る。ブロック1315においてゲスト仮想とタグ付けされたアクセスに対するゲストDATが行われた後、およびブロック1310においてゲスト実（仮想＝No）とタグ付けされた任意のアクセスに対して、ブロック1320においてゲスト・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が完了すると、ブロック1325において、結果として得られたアドレスはホスト仮想とタグ付けされてもよく、かつ元のゲスト変換がセキュアとタグ付けされているときはセキュアとタグ付けされ得る。ホスト仮想とタグ付けされた任意のアクセスに関してプロセス1300が続き得る。ブロック1305において元のアクセスがホスト・アクセス（ゲスト＝No）であり、かつブロック1330において仮想であるとき、次いでブロック1335においてホストDATが行われ得る。ブロック1335において、ホスト・テーブル・フェッチは非セキュアとマーク付けされ得る。ブロック1335においてホストDATが行われた後、またはブロック1330において元のホスト・アクセスが実（仮想＝No）とタグ付けされたときに、次いでブロック1340においてホスト・プレフィックス変換が適用され得る。ブロック1345において、結果として得られたアドレスはホスト絶対アドレスであり得る。

【0079】

図14は、本発明の1つ以上の実施形態によるプロセスの流れ1400においてハードウェアによって行われ得るセキュア・ストレージ保護を伴うDAT変換の例を示している。図13のブロック1345からの続きで、ブロック1405においてセキュアUVアクセスが識別されたとき、次いでブロック1410において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でき、もしそうでなければ、ブロック1415においてエラーが提供される。セキュアUVアクセスは、UVストレージにアクセスするときにセキュア制御インターフェースによって行われ得る。ブロック1410において、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とき、処理の続きのブロック1420におけるドメイン・チェックに対する特定のセキュア・ドメインとして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ースによってセットアップされる）が用いられ得る場合を除いて、任意のセキュア・アクセスに対して行われ得るとおりの保護チェックが続き得る。加えて、ブロック1425においてUVアクセスに対して検出される侵害（エントリ・ポイントD）は、ブロック1425におけるセキュア・ゲストの侵害（セキュアUV＝No）に対して行われるようなブロック1435におけるハイパーバイザに対する例外ではなく、ブロック1430におけるエラーとして提供され得る。

【0080】

ブロック1405においてセキュアUVアクセスとタグ付けされていなかったアクセスに対して、ブロック1440においてハードウェアはアクセスがセキュア・ゲスト・アクセスかどうかを判定し、もしそうではなく、かつブロック1445においてそのページがセキュアとマーク付けされていれば、ブロック1435においてハイパーバイザに例外が提供され得る。そうではなくて、ブロック1440においてアクセスがセキュア・ゲスト・アクセスではなく、かつブロック1445においてページがセキュアとマーク付けされていないとき、次いでブロック1450において変換が成功する。

【0081】

アクセスがブロック1440においてセキュア・ゲスト・アクセスであるか、またはブロック1410においてセキュアUVストレージとして登録されているストレージに対するセキュアUVアクセスであるとき、ブロック1420においてハードウェアは、ストレージがそのアクセスに関連するセキュア・エンティティに登録されていることを確認するためのチェックを行い得る。もしこれがセキュアUVアクセスであれば、UV-セキュアードメイン・レジスタ（アクセスされるセキュアUVストレージに基づいてセキュア制御インターフェースによってロードされる）から特定のセキュア・ドメインを得ることができ、セキュア・ゲスト・アクセスに対しては、SG-セキュアードメイン・レジスタ（セキュア・エンティティがディスパッチされるときにロードされる）から特定のセキュア・ドメインが得られる。ブロック1420において、アクセスされているストレージが特定のセキュア・ドメインに登録されていないとき、ブロック1425におけるセキュアUVアクセスに対してはブロック1430においてエラーが得られ、ブロック1425におけるセキュア・ゲスト・アクセス（セキュアUV=N o）に対してはブロック1435においてハイパーバイザに例外が提供される。

【0082】

ブロック1420において特定のセキュア・ドメインに登録されている、ブロック1440およびブロック1410におけるストレージへのセキュア・アクセスに対して、仮想アドレス・チェックがディスエーブルされるとき、すなわちブロック1455においてDAビット=1であり、かつブロック1460においてアクセスが実であるとき、次いでブロック1450において変換が完了する。しかし、ブロック1455においてDAビット=1であるがブロック1460においてアクセスが仮想（実=N o）であるとき、ブロック1425におけるセキュアUVアクセスに対してはブロック1430においてエラーが得られ、ブロック1425におけるセキュア・ゲスト・アクセス（セキュアUV=N o）に対してはブロック1435においてハイパーバイザに例外が提供される。ブロック1455においてDAビット=0であり、かつブロック1475においてアクセスが仮想アクセスであるとき、次いでブロック1470において、ハードウェアはアクセスのホスト仮想対ホスト絶対マッピングがこのホスト絶対アドレスに対して登録されたものと一致するかどうかを判定し得る。もしそうであれば、次いでブロック1450において変換は正常に完了する。もしブロック1470においてマッピングが一致しなければ、ブロック1425におけるセキュアUVアクセスに対してはブロック1430においてエラーが得られ、ブロック1425におけるセキュア・ゲスト・アクセス（セキュアUV=N o）に対してはブロック1435においてハイパーバイザに例外が提供される。もしDAビット=0であり、かつブロック1475においてアクセスが実アクセス（仮想=N o）であれば、ブロック1425におけるセキュアUVアクセスに対してはブロック1430においてエラーが得られ、ブロック1425におけるセキュア・ゲスト・アクセス（セキュアUV=N o）に対してはブロック1435においてハイパーバイザに例外が提供され、代替的にはブロック1450において変換が正常に完了してもよい。ブロック1480におけるI/Oサブシステムによる任意のアクセスは、ブロック1445においてページがセキュアとマーク付けされているかどうかをチェックされてもよく、もしそのページがセキュアであれば、ブロック1435においてハイパーバイザに例外が提供されてもよく、もしそのページがセキュアとマーク付けされていないならば、ブロック1450において変換が成功する。

【0083】

ストレージ登録およびマッピングのさまざまなチェックは、ゾーン・セキュリティ・テーブル・インターフェース1485を通じて集合的に管理され得る。たとえば、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たゾーン・セキュリティ・テーブルとインターフェースし得る。

【0084】

本明細書において考察されるとおり、本明細書における1つ以上の実施形態は、この付

10

20

30

40

50

加的なセキュリティを提供するためにソフトウェアとマシンとの間の効率的な軽量のウルトラバイザ・インターフェースを利用している。この場合、このインターフェースは、ウルトラバイザが大多数の割り込みイネーブル命令（例、ロード・プログラム状況ワードまたはロード制御）をエミュレートすることを可能にする一方で、ハイパーバイザがゲストの代わりに保留割り込みを維持することをなおも可能にするために使用される。この保留割り込み構造は、ハードウェアにおいてセキュア・ゲストがディスパッチされていないときの割り込みの優先順位付けに対処するために、ハイパーバイザによって必要とされる。本明細書における1つ以上の実施形態の技術効果および利益は、セキュア・ゲスト状態またはメモリへのハイパーバイザのアクセスを許可することなく、単一の場所にこの複雑なコードを存在させることによって、複雑性およびリスクを低減することを含む。

10

【0085】

上記に鑑みて、割り込みイネーブルのためのセキュア・インターフェース制御ハイレベル命令インターセプトのための動作を、図15～16に関して考察する。ここで図15を参照すると、本発明の1つ以上の実施形態による割り込みイネーブルのためのセキュア・インターフェース制御ハイレベル命令インターセプトに対するプロセスの流れ1500が示されている。セキュア環境のコンポーネントによってどの動作が行われているのかを示すために、プロセスの流れ1500にセキュア・エンティティ1502（例、セキュア・ゲストまたはコンテナ）、セキュア・インターフェース制御1504、および信頼されないエンティティ1506（例、ハイパーバイザまたはOS）が重ね合わせられている。

20

【0086】

プロセスの流れ1500はブロック1510で開始され、ここでセキュア・エンティティ1502は割り込み（例、LP SWおよびLC TL）をイネーブルし得る命令を発行し、その命令は信頼されないエンティティ1506によってモニタされる。ブロック1520において、セキュア・インターフェース制御1504はセキュア・ゲスト・ストレージから新たなPSW（例、LP SWに対して）または制御レジスタ値（例、LC TLに対して）をフェッチする。ブロック1530において、セキュア・インターフェース制御1504は新たなPSWまたは制御レジスタをセキュア・エンティティ状態にロードし、これはフェッチに応答したものであり得る。

【0087】

ブロック1540において、セキュア・インターフェース制御1504は、信頼されないエンティティ1506にゲスト割り込みイネーブル更新を通知する。ブロック1550において、信頼されないエンティティ1506は、保留およびイネーブルされた割り込みの優先順位付けをして、最高優先順位のイネーブルされたゲスト割り込みを定める。ブロック1560において、信頼されないエンティティ1506は、最高優先順位の割り込み（例、最高優先順位のイネーブルされたゲスト割り込み）に対する割り込み情報を非セキュア・ストレージに記憶する。一例において、この非セキュア・ストレージは、このゲスト割り込みに関連する状態記述であり得る。別の例において、この非セキュア・ストレージは、挿入割り込みUVC命令への入力として用いられることとなるパラメータ・ブロックである。プロセスの流れ1500は丸Zに進み、これは図16およびプロセスの流れ1600に接続する。

30

【0088】

ここで図16を参照すると、本発明の1つ以上の実施形態による割り込みイネーブルのためのセキュア・インターフェース制御ハイレベル命令インターセプトに対するプロセスの流れ1600が示されている。セキュア環境のコンポーネントによってどの動作が行われているのかを示すために、プロセスの流れ1600にセキュア・エンティティ1602、セキュア・インターフェース制御1604、および信頼されないエンティティ1606が重ね合わせられている。なお、図16のセキュア・エンティティ1602、セキュア・インターフェース制御1604、および信頼されないエンティティ1606は、図15のセキュア・エンティティ1502、セキュア・インターフェース制御1504、および信頼されないエンティティ1506と類似のものである。

40

50

【0089】

プロセスの流れ1600はブロック1610で開始され、ここで信頼されないエンティティ1606はセキュア・インターフェース制御1604に対して、最高優先順位のイネーブルされたゲスト割り込みを提供するよう要求する。この要求は通知に応答して行われ得る。一例において、この要求は、割り込みを挿入すべきだという表示およびその割り込みに関する情報によるSIEディスパッチであり得る。別の例において、この要求は、割り込み情報およびUVCに関連するパラメータ・ブロックにおける関連ゲストの表示による挿入割り込みUVC命令であり得る。判定ブロック1620において、セキュア・インターフェース制御1604は、割り込み挿入が有効かどうかを判定する。たとえば、セキュア・インターフェース制御1604は、関連ゲストが挿入される割り込みに対してイネーブルされているかどうかを判定する。もし割り込み挿入が有効でなければ、プロセスの流れ1600はブロック1640に進む（NO矢印で示されるとおり）。ブロック1640において、セキュア・インターフェース制御1604は信頼されないエンティティ1606に例外を発行する。

10

【0090】

もし割り込み挿入が有効であれば、プロセスの流れ1600はブロック1660に進む（YES矢印で示されるとおり）。ブロック1660において、セキュア・インターフェース制御1604はゲスト・プレフィックス・ページに割り込み情報を移動させて、セキュア・エンティティ1602に割り込みを挿入する（例、ゲスト状態を更新する）。ブロック1670において、セキュア・エンティティ1602は挿入された割り込みを受信したことに応答して、割り込みハンドラを実行する。

20

【0091】

この開示はクラウド・コンピューティングに対する詳細な説明を含むが、本明細書に記述される教示の実現はクラウド・コンピューティング環境に限定されないことが理解されるべきである。むしろ本発明の実施形態は、現在公知であるか、または後に開発される任意のその他のタイプのコンピューティング環境とともに実現され得る。

【0092】

クラウド・コンピューティングは、最小限の管理努力またはサービスのプロバイダとのインタラクションによって迅速にプロビジョニングおよびリリースされ得る構成可能なコンピューティング・リソース（例、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・ネットワーク・アクセスを可能にするためのサービス配信のモデルである。このクラウド・モデルは少なくとも5つの特性と、少なくとも3つのサービス・モデルと、少なくとも4つの配置モデルとを含んでいる。

30

【0093】

特性は次のとおりである。

【0094】

オンデマンド・セルフサービス。クラウド消費者は、たとえばサーバ時間およびネットワーク・ストレージなどのコンピューティング・ケイパビリティを、必要に応じて自動的に、サービスのプロバイダとの人的インタラクションを必要とせずに一方的にプロビジョニングできる。

40

【0095】

広範なネットワーク・アクセス。ケイパビリティはネットワークを通じて利用可能であり、様々なシンまたはシック・クライアント・プラットフォーム（例、携帯電話、ラップトップ、およびPDA）による使用を容易にする標準的な機構を通じてアクセスされる。

【0096】

リソース・プール。マルチテナント・モデルを用いて複数の消費者にサービスするために、プロバイダのコンピューティング・リソースはプールされ、要求に従って異なる物理および仮想リソースが動的に割り当ておよび再割り当てされる。消費者は一般的に、提供されるリソースの正確な場所に対する制御も知識も有さないが、より高い抽象化レベルに

50

おける場所（例、国、州、またはデータセンタ）を特定できてもよいという点で、場所独立性の意味が存在する。

【0097】

迅速な順応性。ケイパビリティは、素早くスケール・アウトするために場合によっては自動的に、迅速かつ順応的にプロビジョニングされ、かつ素早くスケール・インするために迅速にリリースされ得る。消費者にとって、プロビジョニングのために利用可能なケイパビリティはしばしば無制限にみえ、任意のときに任意の量を購入できる。

【0098】

従量制サービス。クラウド・システムは、サービスのタイプ（例、ストレージ、処理、帯域幅、およびアクティブ・ユーザ・アカウント）に対して適切な何らかの抽象化レベルにおいて計測ケイパビリティを利用することによって、リソースの使用を自動的に制御および最適化する。リソースの使用をモニタ、制御、および報告して、使用されるサービスのプロバイダおよび消費者の両方に対する透明性を提供できる。

【0099】

サービス・モデルは次のとおりである。

【0100】

サービスとしてのソフトウェア（SaaS：Software as a Service）。消費者に提供されるケイパビリティは、クラウド・インフラストラクチャにおいて動作するプロバイダのアプリケーションの使用である。アプリケーションは、さまざまなクライアント・デバイスからたとえばウェブ・ブラウザ（例、ウェブ・ベースのeメール）などのシン・クライアント・インターフェースを通じてアクセス可能である。消費者はネットワーク、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・ケイパビリティさえも含む基盤となるクラウド・インフラストラクチャを管理または制御することはなく、例外となり得るのは限られたユーザー特有のアプリケーション構成設定である。

【0101】

サービスとしてのプラットフォーム（PaaS：Platform as a Service）。消費者に提供されるケイパビリティは、プロバイダによってサポートされるプログラミング言語およびツールを用いて作成された、消費者が作成または取得したアプリケーションのクラウド・インフラストラクチャへの配置である。消費者はネットワーク、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となるクラウド・インフラストラクチャを管理または制御することはないが、配置されたアプリケーションおよびおそらくはアプリケーション・ホスティング環境構成に対する制御を有する。

【0102】

サービスとしてのインフラストラクチャ（IaaS：Infrastructure as a Service）。消費者に提供されるケイパビリティは、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、消費者が任意のソフトウェアを配置および実行することが可能な処理、ストレージ、ネットワーク、およびその他の基本的なコンピューティング・リソースのプロビジョニングである。消費者は基盤となるクラウド・インフラストラクチャを管理または制御することはないが、オペレーティング・システム、ストレージ、配置されたアプリケーションに対する制御、およびおそらくはネットワーク形成コンポーネント（例、ホスト・ファイアウォール）の選択に対する限られた制御を有する。

【0103】

配置モデルは次のとおりである。

【0104】

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、ある組織に対してのみ操作される。これはその組織またはサード・パーティによって管理されてもよく、オンプレミスまたはオフプレミスに存在してもよい。

【0105】

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

10

20

30

40

50

共有され、共通する関心事項（例、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の検討）を有する特定のコミュニティをサポートする。これはそれらの組織またはサード・パーティによって管理されてもよく、オンプレミスまたはオフプレミスに存在してもよい。

【0106】

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、一般人または大規模な産業グループに対して利用可能にされ、クラウド・サービスを販売する組織が所有している。

【0107】

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）の複合体であり、それらのクラウドは独自のエンティティに留まるが、データおよびアプリケーション・ポータビリティを可能にする標準または独自の技術（例、クラウド間のロード・バランシングのためのクラウド・バースティング）によってともに結合される。

【0108】

クラウド・コンピューティング環境はサービス指向型であり、ステートレス性、低結合性、モジュラリティ、およびセマンティックな相互運用性に焦点を合わせている。クラウド・コンピューティングの中心には、相互接続されたノードのネットワークを含むインフラストラクチャがある。

【0109】

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。示されるとおり、クラウド・コンピューティング環境50は1つ以上のクラウド・コンピューティング・ノード10を含み、たとえばパーソナル・デジタル・アシスタント（PDA: personal digital assistant）もしくは携帯電話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、または自動車のコンピュータ・システム54N、あるいはその組み合わせなどの、クラウド消費者によって用いられるローカル・コンピュータ・デバイスが、このクラウド・コンピューティング・ノード10によって通信してもよい。ノード10は互いに通信してもよい。これらのノードは、たとえば上述したプライベート、コミュニティ、パブリック、もしくはハイブリッド・クラウド、またはその組み合わせなどの1つ以上のネットワークにおいて、物理的または仮想的にグループ化（図示せず）されてもよい。このことは、クラウド・コンピューティング環境50がインフラストラクチャ、プラットフォーム、もしくはソフトウェア、またはその組み合わせを、クラウド消費者がそれに対するリソースをローカル・コンピュータ・デバイスにおいて維持する必要のないサービスとして提供することを可能にする。図17に示されるコンピュータ・デバイス54A～Nのタイプは単なる例示であることが意図されており、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、任意のタイプのネットワークもしくはネットワーク・アドレス可能接続（例、ウェブ・ブラウザを使用するもの）またはその両方を通じて、任意のタイプのコンピュータ・デバイスと通信できることが理解される。

【0110】

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化レイヤのセットが示されている。図18に示されるコンポーネント、レイヤ、および機能は単なる例示であることが意図されており、本発明の実施形態はそれらに限定されないことが予め理解されるべきである。示されるとおり、以下のレイヤおよび対応する機能が提供される。

【0111】

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は、メインフレーム61、RISC（縮小命令セット・コンピュータ（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

10

20

30

40

50

・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形成コンポーネント 66 を含む。いくつかの実施形態において、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。

【0112】

仮想化レイヤ 70 は抽象化レイヤを提供し、この抽象化レイヤから仮想エンティティの以下の例が提供されてもよい。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。

【0113】

一例において、管理レイヤ 80 は以下に記載される機能を提供してもよい。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行うために使用されるコンピューティング・リソースおよびその他のリソースの動的調達を提供する。計測および価格決定 82 は、クラウド・コンピューティング環境内でリソースが使用される際のコスト追跡と、これらのリソースの消費に対する請求書またはインボイスの送付とを提供する。一例において、こ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もよい。セキュリティは、クラウド消費者およびタスクに対するアイデンティティ検証、ならびにデータおよびその他のリソースの保護を提供する。ユーザ・ポータル 83 は、消費者およびシステム管理者に対するクラウド・コンピューティング環境へのアクセスを提供する。サービス・レベル管理 84 は、要求されるサービス・レベルが満たされるようにクラウド・コンピューティング・リソースの割り当ておよび管理を提供する。サービス・レベル・アグリーメント (SLA: Service Level Agreement) 計画および実現 85 は、SLA によって将来の要求が予測されるクラウド・コンピューティング・リソースに対する事前の取り決めおよびその調達を提供する。

【0114】

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が使用され得る機能の例を提供する。このレイヤから提供され得るワークロードおよび機能の例は、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、仮想教室の教育配信 93、データ分析処理 94、トランザクション処理 95、および割り込みイネーブルのためのハイレベル命令インターセプト 96 を含む。これらは単なるいくつかの例であり、他の実施形態におけるレイヤは異なるサービスを含み得ることが理解される。

【0115】

ここで図 19 を参照すると、本発明の 1 つ以上の実施形態によるシステム 1900 が示されている。システム 1900 はノード 10 の一例 (例、ホスティング・ノード) を含み、このノード 10 はたとえばネットワーク 165 などを通じて、1 つ以上のクライアント・デバイス 20A ~ 20E と直接的または間接的に通信している。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またはホスト・サーバであり得る。ノード 10 は、1 つ以上の VM 15 (15A ~ 15N) の配置を促進するハイパーバイザ 12 を実行する。ノード 10 はさらにハードウェア／ファームウェア・レイヤ 11 を含み、このハードウェア／ファームウェア・レイヤ 11 は、VM 15A ~ N およびハイパーバイザ 12 が必要とする機能に対する直接的サポートを提供し、かつハイパーバイザ 12 が VM 15 に 1 つ以上のサービスを提供することを促進する。現在の実施においては、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 との間、ハードウェア／ファームウェア・レイヤ 11 と VM 15 との間、ハイパーバイザ 12 と VM 15 との間、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 VM 15 との間の通信が提供される。本発明の 1 つ以上の実施形態によると、ハードウェア／ファームウェア・レイヤ 11 にセキュア・インターフェース制御が提供され、ハイパーバイザ 12 と VM 15 との間の直接的通信が排除される。

【0116】

たとえば、ノード 10 はクライアント・デバイス 20A が VM 15A ~ 15N の 1 つ以

10

20

30

40

50

上を配置することを促進できる。VM 15 A～15 Nは、別個のクライアント・デバイス 20 A～20 Eからのそれぞれの要求に応答して配置されてもよい。たとえば、VM 15 Aはクライアント・デバイス 20 Aによって配置されてもよく、VM 15 Bはクライアント・デバイス 20 Bによって配置されてもよく、VM 15 Cはクライアント・デバイス 20 Cによって配置されてもよい。加えてノード 10は、(VMとして動作することなく)クライアントが物理サーバをプロビジョニングすることを促進してもよい。本明細書に記載される例は、VMの一部としてのノード 10のリソースのプロビジョニングを具現化するが、記載される技術的解決策は、リソースを物理サーバの一部としてプロビジョニングすることにも適用され得る。

【0117】

一例において、クライアント・デバイス 20 A～20 Eは、たとえば人、ビジネス、政府機関、会社の部署、または任意のその他のエンティティなどの同じエンティティに属していてもよく、ノード 10はそのエンティティのプライベート・クラウドとして動作されてもよい。この場合、ノード 10は、そのエンティティに属するクライアント・デバイス 20 A～20 Eによって配置されたVM 15 A～15 Nのみをホストする。別の例において、クライアント・デバイス 20 A～20 Eは別個のエンティティに属していてもよい。たとえば、第1のエンティティはクライアント・デバイス 20 Aを所有してもよく、一方で第2のエンティティはクライアント・デバイス 20 Bを所有してもよい。この場合、ノード 10は、異なるエンティティからのVMをホストするパブリック・クラウドとして動作されてもよい。たとえば、VM 15 A～15 Nは、VM 15 AがVM 15 Bへのアクセスを促進しないような覆い隠された方式で配置されてもよい。たとえば、ノード 10はIBM z Systems (IBM社の登録商標) プロセッサ・リソース／システム・マネージャ (PR／SM: Processor Resource／Systems Manager) ロジカル・パーティション (LPAR: Logical Partition) 機構を用いて、VM 15 A～15 Nを覆い隠してもよい。たとえばPR／SM LPARなどのこれらの機構は、パーティション間の分離を提供することによって、ノード 10が異なるエンティティに対する2つ以上のVM 15 A～15 Nを同じ物理ノード 10の異なるロジカル・パーティションに配置することを促進する。

【0118】

クライアント・デバイス 20 A～20 Eのうちのクライアント・デバイス 20 Aは、たとえばコンピュータ、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の配置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 20 Aは、ネットワーク 165を介してハイパーバイザが受信するための要求を送信してもよい。VM 15 A～15 NのうちのVM 15 Aは、クライアント・デバイス 20 A～20 Eのうちのクライアント・デバイス 20 Aからの要求に応答してハイパーバイザ 12が配置するVMイメージである。ハイパーバイザ 12はVM モニタ (VMM: VM monitor) であり、これはVMを作成および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もよい。ハイパーバイザ 12は、VM 15 Aがノード 10のハードウェア・コンポーネントを用いてプログラムの実行もしくはデータの記憶またはその両方を行うことを促進する。適切な特徴および修正を伴うハイパーバイザ 12は、IBM z Systems (IBM社の登録商標)、オラクル (Oracle) のVM Server (TM)、シトリックス (Citrix) のXen Server (TM)、ブイエムウェア (Vmware) のESX (TM)、マイクロソフト (Microsoft) (R) Hyper-V (TM) 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もよい。ハイパーバイザ 12は、ノード 10において直接実行されるネイティブ・ハイパーバイザであってもよいし、別のハイパーバイザにおいて実行されるホステッド・ハイパーバイザであってもよい。

【0119】

ここで図 20を参照すると、本発明の1つ以上の実施形態による本明細書の教示を実現

10

20

30

40

50

するためのノード10が示されている。本明細書に記載されるとおり、ノード10は、さまざまな通信技術を使用した任意の数および組み合わせのコンピュータ・デバイスおよびネットワークを含むか、もしくは使用するか、またはその両方である電子コンピュータ・フレームワークであり得る。ノード10は、容易にスケラブルであり、拡張可能であり、かつモジュール式であってもよく、他のものとは独立に異なるサービスに変化したり、いくつかの特徴を再構成したりする能力を有する。

【0120】

この実施形態において、ノード10はプロセッサ2001を有し、このプロセッサ2001は1つ以上の中央処理ユニット(CPU: central processing units) 2001a、2001b、2001cなどを含み得る。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およびさまざまなその他のコンポーネントに結合される。システム・メモリ2003は、リード・オンリ・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。ROM 2004はシステム・バス2002に結合され、かつノード10の特定の基本機能を制御する基本入力/出力システム(BIOS: basic input/output system)を含んでもよい。RAMは、プロセッサ2001による使用のためにシステム・バス2002に結合された読取り書き込みメモリである。

【0121】

図20のノード10はハード・ディスク2007を含み、このハード・ディスク2007はプロセッサ2001によって読取り可能で実行可能な有形ストレージ媒体の一例である。ハード・ディスク2007は、ソフトウェア2008およびデータ2009を記憶する。ソフトウェア2008は、たとえば図1~19を参照して説明したプロセスなどのプロセスを行うために、プロセッサ2001によってノード10において実行されるための命令として記憶される。データ2009は、ソフトウェア2008の動作をサポートし、かつそれによって用いられるためのさまざまなデータ構造に組織化された質的変数または定量的変数の値のセットを含む。

【0122】

図20のノード10は、プロセッサ2001、システム・メモリ2003、ハード・ディスク2007、およびノード10の他のコンポーネント(例、周辺デバイスおよび外部デバイス)を相互接続してそれらの間の通信をサポートする1つ以上のアダプタ(例、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つ以上の実施形態において、1つ以上のアダプタは、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つ以上のI/Oバスに接続されてもよく、この1つ以上のI/Oバスは、たとえばペリフェラル・コンポーネント・インターコネクト(PCI: Peripheral Component Interconnect)などの共通プロトコルを使用し得る。

【0123】

示されるとおり、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ース・アダプタ2020を含む。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を含む。ディスプレイ・アダプタ2030(もしくはプロセッサ2001またはその両方)は、たとえばディスプレイおよびGUI 2032の管理などのグラフィックス性能を提供するためのグラフィックス・コントローラを含み得る。通信アダプタ2041はシステム・バス2002とネットワーク2050とを相互接続して、ノード10がたとえばサーバ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することを可能にする。本発明の1つ以上の実施形態において、ソフトウェア2008およびデータ2009の動作は、サーバ2051およびデータベース2052によってネットワーク2

050上で実施され得る。たとえばネットワーク2050と、サーバ2051と、データベース2052とが組み合わさって、サービスとしてのプラットフォーム、サービスとしてのソフトウェア、もしくはサービスとしてのインフラストラクチャ、またはその組み合わせとして（例、分散型システムにおけるウェブ・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の内部反復を提供し得る。

【0124】

本明細書に記載される実施形態は、必然的にコンピュータ技術、特にVMをホストするコンピュータ・サーバに根差したものである。さらに、本発明の1つ以上の実施形態は、VMをホストするコンピュータ・サーバがセキュアVMをホストすることを促進することによって、コンピューティング技術自体の動作、特にVMをホストするコンピュータ・サーバの動作に対する改善を促進するものであり、ここではハイパーバイザさえもがセキュアVMに関連するメモリ、レジスタ、およびその他のこうしたデータにアクセスすることを禁止される。加えて、本発明の1つ以上の実施形態は、ハードウェア、ファームウェア（例、ミリコード）、またはその組み合わせを含むセキュア・インターフェース制御（本明細書においては「ウルトラバイザ（ultravisor）」または「UV」とも呼ばれる）を用いてセキュアVMとハイパーバイザとの分離を促進することによって、コンピュータ・サーバにホストされるVMのセキュリティを維持することによって、VMホスティング・コンピュータ・サーバの改善に向けた顕著なステップを提供する。本明細書に記載されるとおり、セキュア・インターフェース制御は、VMの初期化／エグジットの際にセキュア化VM状態に対して実質的なオーバーヘッドを加えることなくセキュリティを促進するための軽量の間接動作を提供する。

【0125】

本明細書において開示される本発明の実施形態は、割り込みイネーブルのためのセキュア・インターフェース制御ハイレベル命令インターセプトを実現するシステム、方法、もしくはコンピュータ・プログラム製品（本明細書においてはシステム）、またはその組み合わせを含んでもよい。なお、各々の説明に対して、異なる図面の他の類似の構成要素に対して構成要素の識別子が再使用されている。

【0126】

本明細書において、関連する図面を参照して本発明のさまざまな実施形態を説明している。本発明の範囲から逸脱することなく、本発明の代替的实施形態が考案され得る。以下の説明および図面において、構成要素間のさまざまな接続および位置関係（例、上、下、隣など）が示されている。これらの接続もしくは位置関係またはその両方は、別様に指定されない限り直接的または間接的であってもよく、本発明はこれに関して限定することは意図されていない。したがって、エンティティの結合は直接的または間接的な結合を示すことができ、エンティティ間の位置関係は直接的または間接的な位置関係であり得る。さらに、本明細書に記載されるさまざまなタスクおよびプロセス・ステップは、本明細書に詳細に記載されていない付加的なステップまたは機能を有するより包括的な手順またはプロセスに組み込まれ得る。

【0127】

以下の定義および略語は、請求項および明細書の解釈に用いられるべきものである。本明細書において用いられる「含む（comprises）」、「含む（comprising）」、「含む（includes）」、「含む（including）」、「有する（has）」、「有する（having）」、「含有する（contains）」、もしくは「含有する（containing）」という用語、またはその任意のその他の変形は、非排他的包含をカバーすることが意図される。たとえば、構成要素のリストを含む組成物、混合物、プロセス、方法、物品、または装置は、それらの構成要素のみに限定される必要はなく、明確にリストに挙げられていないその他の構成要素、あるいはこうした組成物、混合物、プロセス、方法、物品、または装置に固有のその他の構成要素を含み得る。

【0128】

加えて、本明細書において「例示的」という用語は、「一例、実例、または例示の役割

をする」ことを意味するために用いられる。本明細書において「例示的」なものとして記載される任意の実施形態または設計は、他の実施形態また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必要はない。「少なくとも1つ」および「1つ以上」という用語は、1以上の任意の整数、すなわち1、2、3、4などを含むものと理解されてもよい。「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などを含むものと理解されてもよい。「接続」という用語は、間接的「接続」および直接的「接続」の両方を含んでもよい。

【0129】

「約 (about)」、「実質的に」、「約 (approximately)」という用語およびそれらの変形は、本出願の提出の時点で利用可能な機器に基づく特定量の測定に関連する誤差の程度を含むことが意図される。たとえば、「約」は所与の値の±8%もしくは5%、または2%の範囲を含み得る。

【0130】

本発明は、任意の可能な技術的詳細レベルの統合におけるシステム、方法、もしくはコンピュータ・プログラム製品、またはその組み合わせであってもよい。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行わせるためのコンピュータ可読プログラム命令を有するコンピュータ可読ストレージ媒体（または複数の媒体）を含んでもよい。

【0131】

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記憶できる有形デバイスであり得る。コンピュータ可読ストレージ媒体は、たと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、電磁気ストレージ・デバイス、半導体ストレージ・デバイス、または前述の任意の好適な組み合わせなどであってもよいが、それに限定されない。コンピュータ可読ストレージ媒体のより具体的な例の非網羅的リストは以下を含む。ポータブル・コンピュータ・ディスクレット、ハード・ディスク、ランダム・アクセス・メモリ (RAM)、リード・オンリ・メモリ (ROM: read-only memory)、消去可能プログラマブル・リード・オンリ・メモリ (erasable programmable read-only memory) (EPROM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・リード・オンリ・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、フレキシブル・ディスク、機械的にコード化されたデバイス、たとえばパンチ・カードまたは記録された命令を有する溝の中の隆起構造など、および前述の任意の好適な組み合わせ。本明細書において用いられるコンピュータ可読ストレージ媒体は、たとえば電波もしくはその他の自由に伝播する電磁波、導波路もしくはその他の伝送媒体を通じて伝播する電磁波（例、光ファイバ・ケーブルを通過する光パルス）、またはワイヤを通じて伝送される電気信号など、それ自体が一時的信号のものであると解釈されるべきではない。

【0132】

本明細書に記載される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それぞれのコンピューティング／処理デバイスにダウンロードされ得るか、またはたと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、もしくは無線ネットワーク、またはその組み合わせなどのネットワークを介して外部コンピュータまたは外部ストレージ・デバイスにダウンロードされ得る。ネットワークは銅伝送ケーブル、光伝送ファイバ、無線伝送、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、もしくはエッジ・サーバ、またはその組み合わせを含んでもよい。各コンピューティング／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・インターフェースは、ネットワークからコンピュータ可読プログラム命令を受信して、そのコンピュータ可読プログラム命令をそれぞれのコンピューティング／処理デバイス内のコンピュータ可読ストレージ媒体に記憶するために転送する。

【0133】

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、集積回路に対する構成データ、または1つ以上のプログラミング言語の任意の組み合わせで書かれたソース・コードもしくはオブジェクト・コードであってもよく、このプログラミング言語はオブジェクト指向プログラミング言語、たとえばSmalltalk、またはC++など、および手続き型プログラミング言語、たとえば「C」プログラミング言語または類似のプログラミング言語などを含む。コンピュータ可読プログラム命令は、すべてがユーザのコンピュータで実行されてもよいし、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ユーザのコンピュータで実行されてもよいし、一部がユーザのコンピュータで、一部がリモート・コンピュータで実行されてもよいし、すべてがリモート・コンピュータまたはサーバで実行されてもよい。後者のシナリオにおいて、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）を含む任意のタイプのネットワークを通じてユーザのコンピュータに接続されてもよいし、（たとえば、インターネット・サービス・プロバイダを用いてインターネットを通じて）外部コンピュータへの接続が行われてもよい。いくつかの実施形態において、たとえばプログラマブル・ロジック回路、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）などを含む電子回路は、本発明の態様を行うために電子回路をパーソナライズするためのコンピュータ可読プログラム命令の状態情報を使用することによって、コンピュータ可読プログラム命令を実行してもよい。

【0134】

本明細書においては、本発明の実施形態による方法、装置（システム）、およびコンピュータ・プログラム製品の流れ図もしくはブロック図またはその両方を参照して、本発明の態様を説明している。流れ図もしくはブロック図またはその両方の各ブロック、および流れ図もしくはブロック図またはその両方におけるブロックの組み合わせは、コンピュータ可読プログラム命令によって実現され得ることが理解されるだろう。

【0135】

これらのコンピュータ可読プログラム命令は、汎用目的コンピュータ、特定目的コンピュータ、またはマシンを生成するためのその他のプログラマブル・データ処理装置のプロセッサに提供されることによって、そのコンピュータまたはその他のプログラマブル・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、流れ図もしくはブロック図またはその両方の単数または複数のブロックにおいて指定される機能／動作を実現するための手段を生じてもよい。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、プログラマブル・データ処理装置、もしくはその他のデバイスまた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コンピュータ可読ストレージ媒体にも記憶されることによって、命令が記憶されたコンピュータ可読ストレージ媒体が、流れ図もしくはブロック図またはその両方の単数または複数のブロックにおいて指定される機能／動作の態様を実現する命令を含む製造物を含んでもよい。

【0136】

コンピュータ可読プログラム命令は、コンピュータ、他のプログラマブル・データ処理装置、または他のデバイスにもロードされて、コンピュータに実現されるプロセスを生成するためにコンピュータ、他のプログラマブル装置、または他のデバイスにおいて一連の動作ステップを行わせることによって、そのコンピュータ、他のプログラマブル装置、または他のデバイスにおいて実行される命令が、流れ図もしくはブロック図またはその両方の単数または複数のブロックにおいて指定される機能／動作を実現してもよい。

【0137】

図面における流れ図およびブロック図は、本発明のさまざまな実施形態によるシステム、方法、およびコンピュータ・プログラム製品の可能な実施のアーキテクチャ、機能、および動作を示すものである。これに関して、流れ図またはブロック図の各ブロックは、指定される論理機能（単数または複数）を実現するための1つ以上の実行可能命令を含むモジュール、セグメント、または命令の一部を表してもよい。いくつかの代替的实施において、ブロック内に示される機能は、図面に示されるものとは異なる順序で起こってもよい。たとえば、連続して示される2つのブロックは、実際には実質的に同時に実行されてもよいし、関与する機能によってはこれらのブロックがときに逆の順序で実行されてもよい。加えて、ブロック図もしくは流れ図またはその両方の各ブロック、およびブロック図もしくは流れ図またはその両方のブロックの組み合わせは、指定された機能または動作を行うか、特定目的のハードウェアおよびコンピュータ命令の組み合わせを実施または実行する特定目的のハードウェア・ベースのシステムによって実現され得ることが注目されるだろう。

【0138】

本明細書において用いられる用語は、単に特定の実施形態を説明する目的のためのものであり、限定することは意図されていない。本明細書において用いられる単数形「a」、「an」、および「the」は、状況が別様を明確に示さない限り複数形も含むことが意図される。この明細書において用いられるときの「含む（comprises）」もしくは「含む（comprising）」またはその両方の用語は、記述される特徴、整数、ステップ、動作、エレメント、もしくは構成要素、またはその組み合わせの存在を特定するが、1つ以上の他の特徴、整数、ステップ、動作、エレメント、構成要素、もしくはそのグループ、またはその組み合わせの存在または付加を除外しないことがさらに理解されるだろう。

【0139】

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のために提供されたものであるが、開示される実施形態に対して網羅的または限定的になることは意図されていない。記載される実施形態の範囲および思想から逸脱することなく、当業者には多くの修正および変更が明らかになるだろう。本明細書において用いられる用語は、実施形態の原理、市場に見出される技術に対する実際の適用または技術的改善点を最もよく説明するか、または他の当業者が本明細書に開示される実施形態を理解できるようにするために選択されたものである。

10

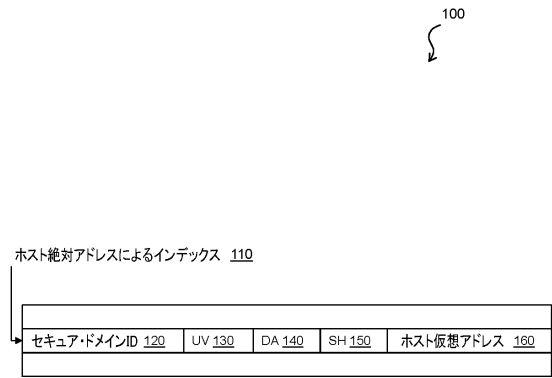
20

30

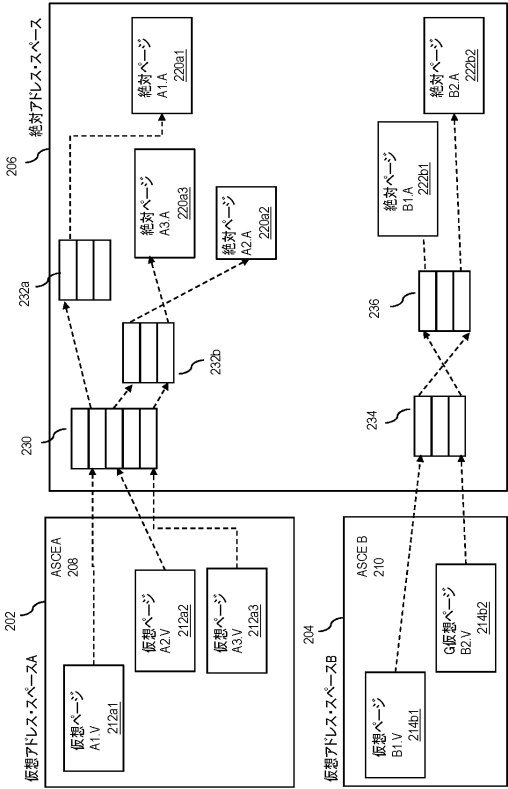
40

50

【図面】
【図 1】



【図 2】



10

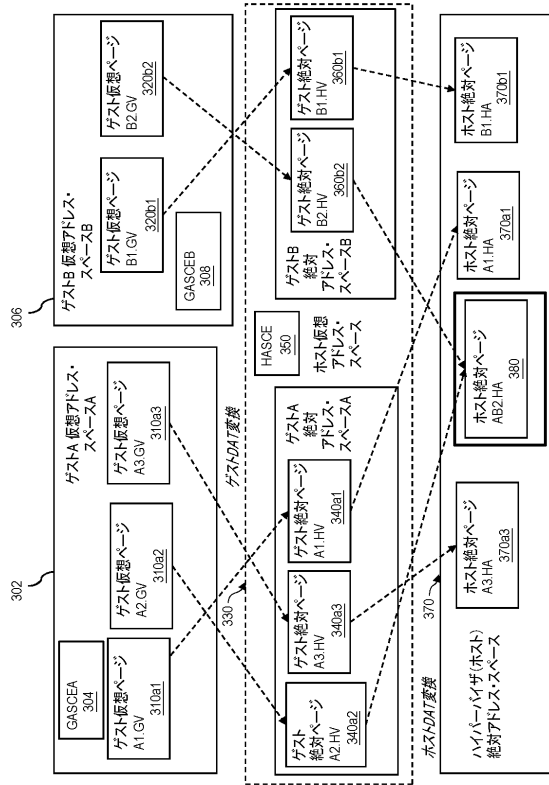
20

30

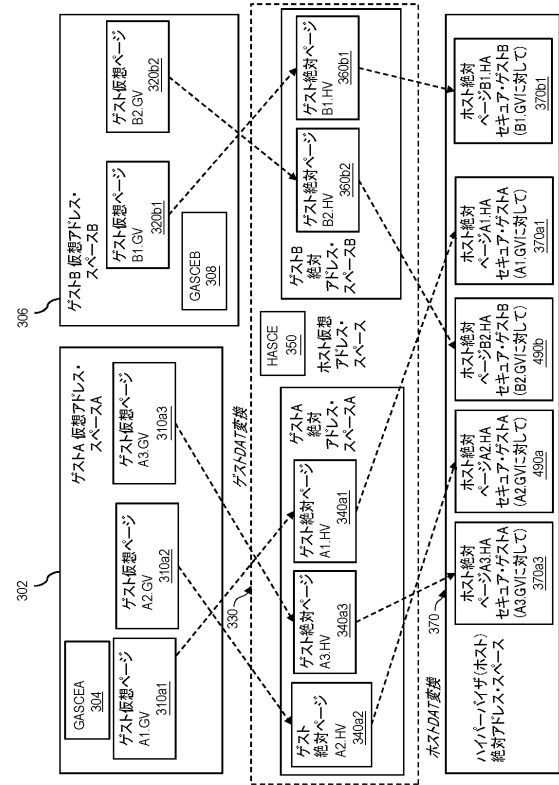
40

50

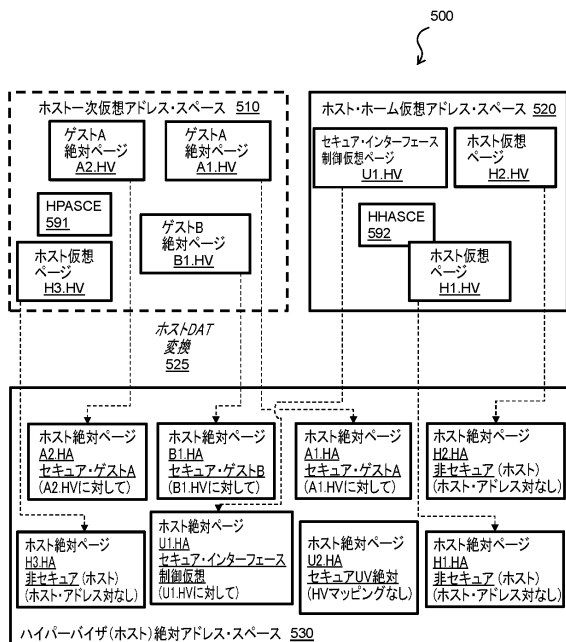
【図 3】



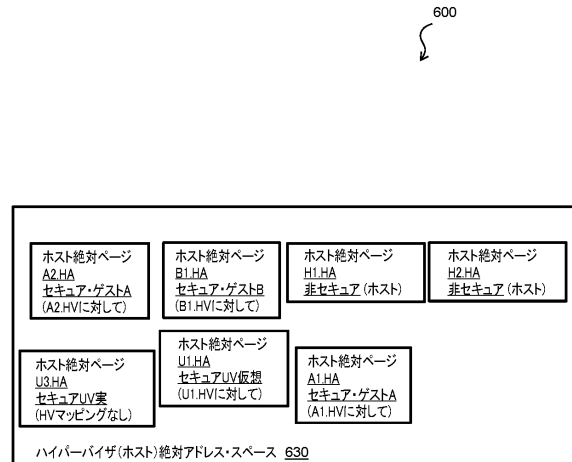
【図 4】



【図 5】



【図 6】



10

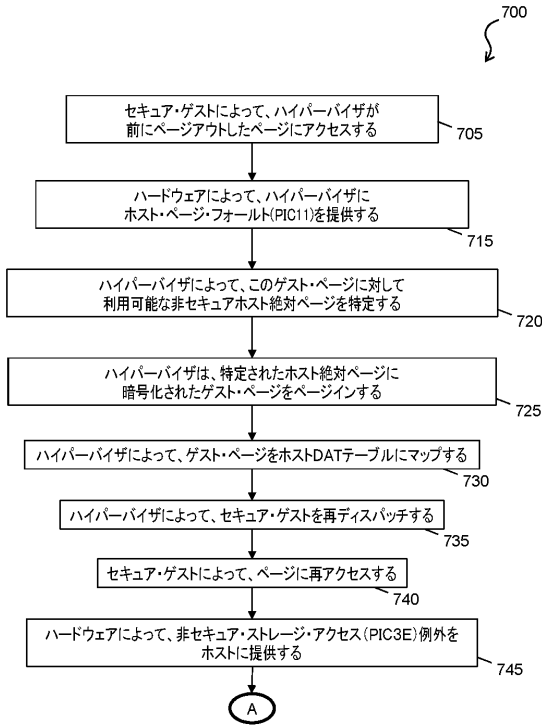
20

30

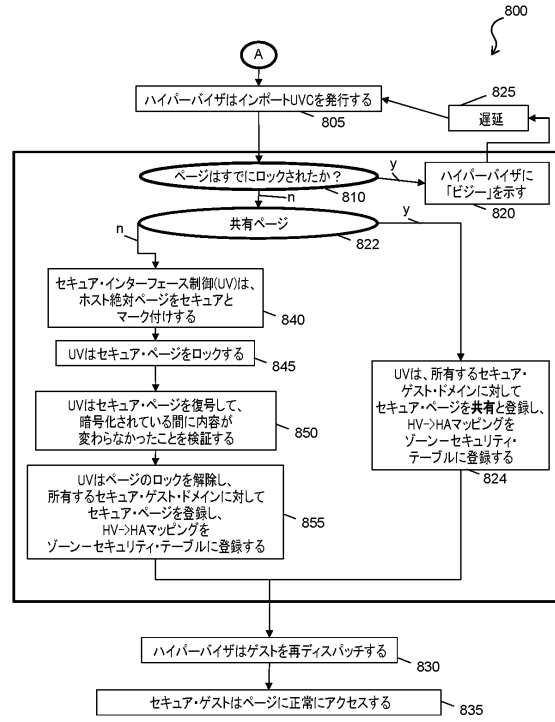
40

50

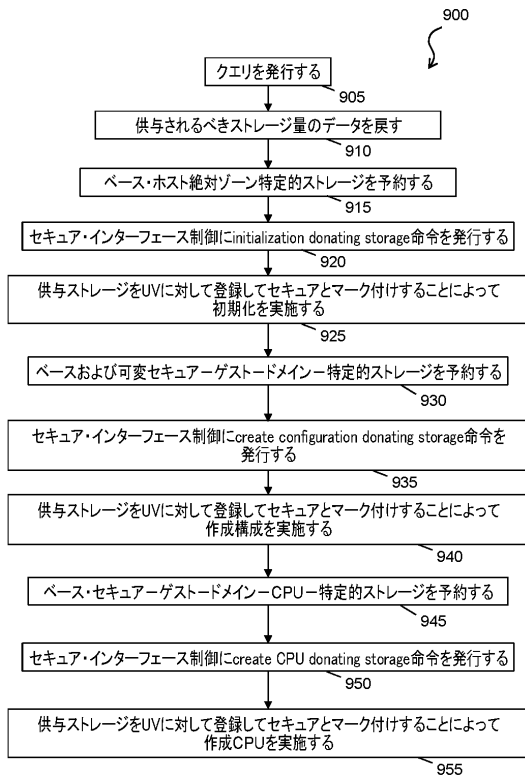
【図 7】



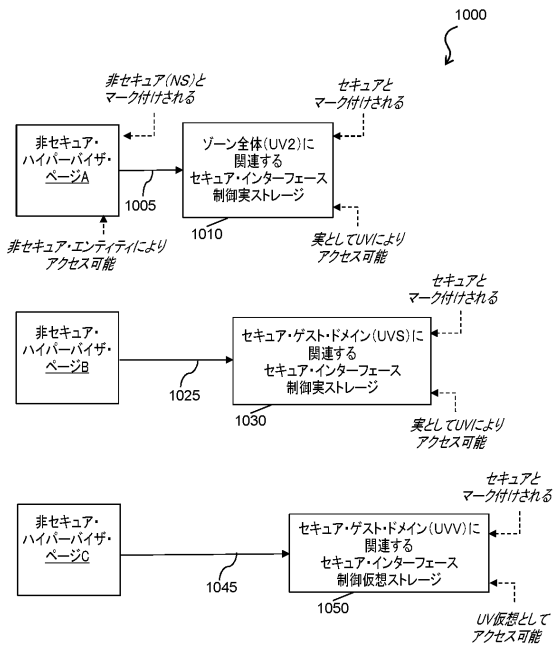
【図 8】



【図 9】



【図 10】



10

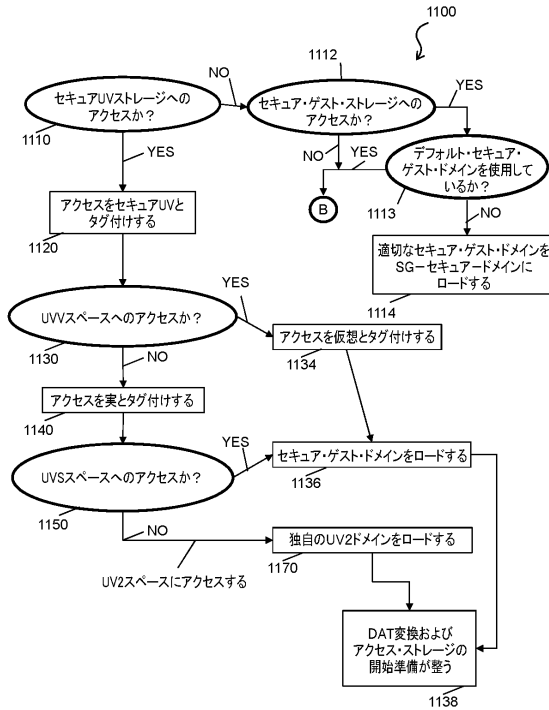
20

30

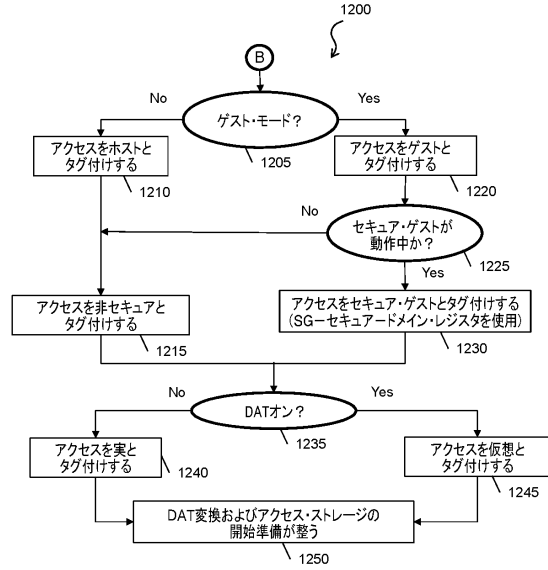
40

50

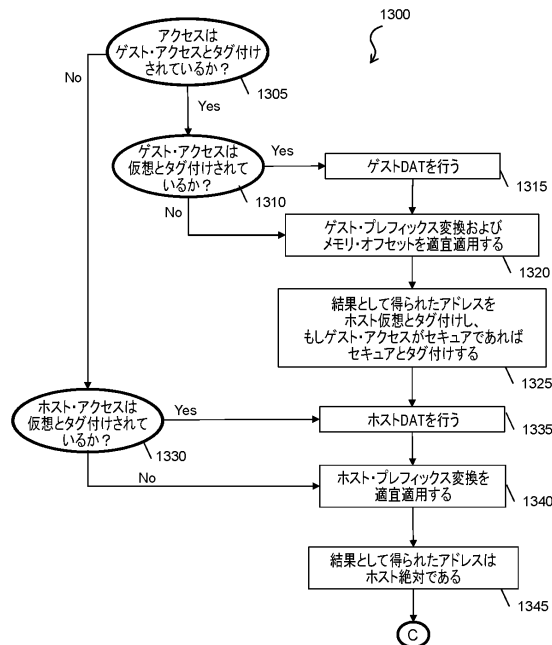
【図 1 1】



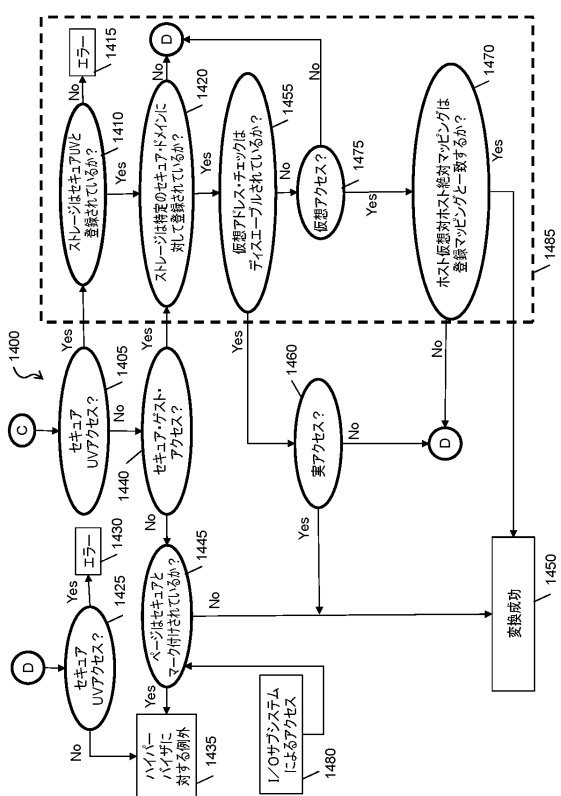
【図 1 2】



【図 1 3】



【図 1 4】



10

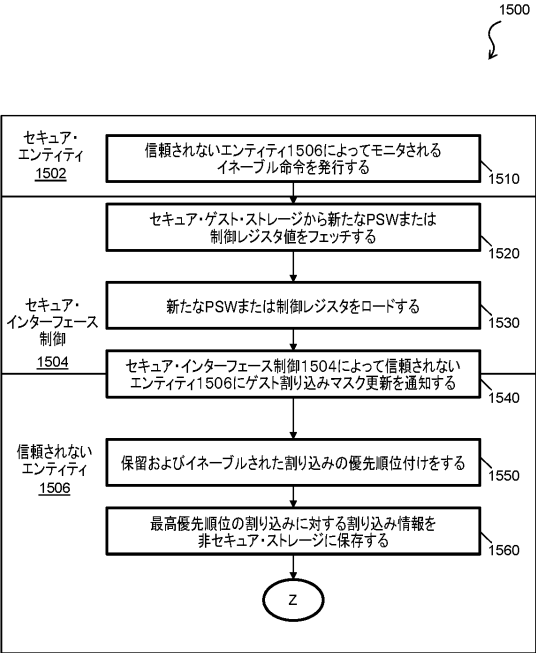
20

30

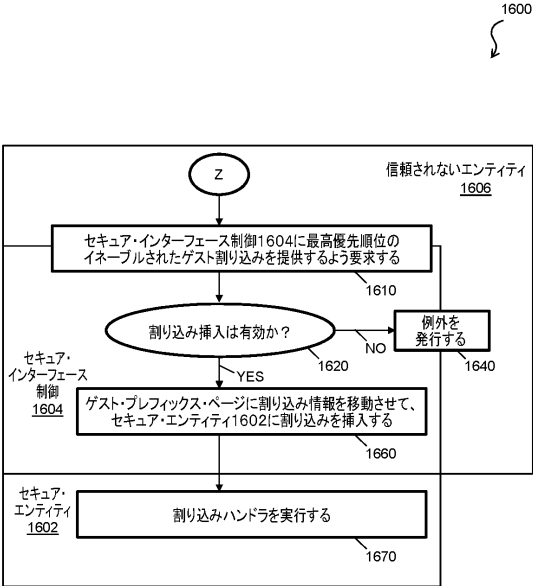
40

50

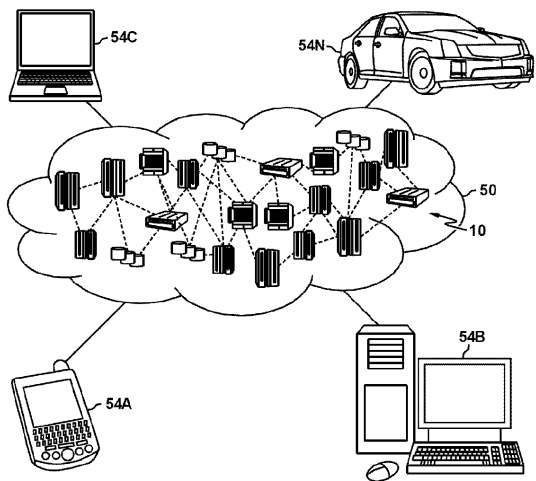
【図 1 5】



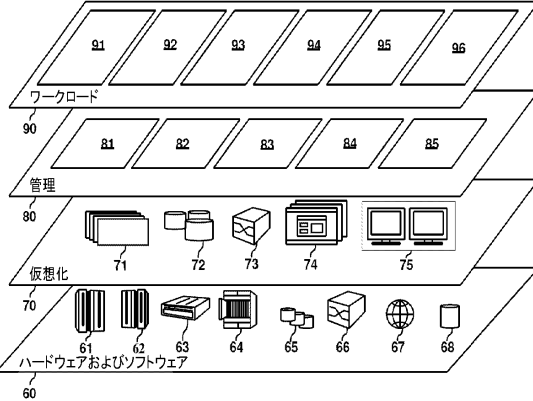
【図 1 6】



【図 1 7】



【図 1 8】



10

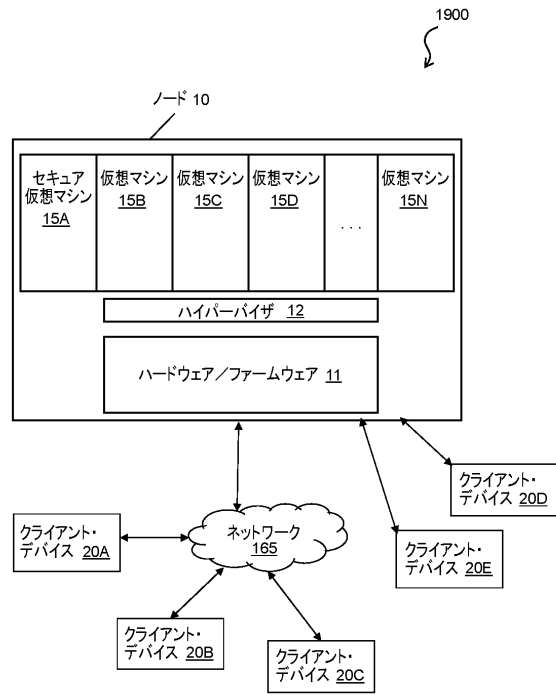
20

30

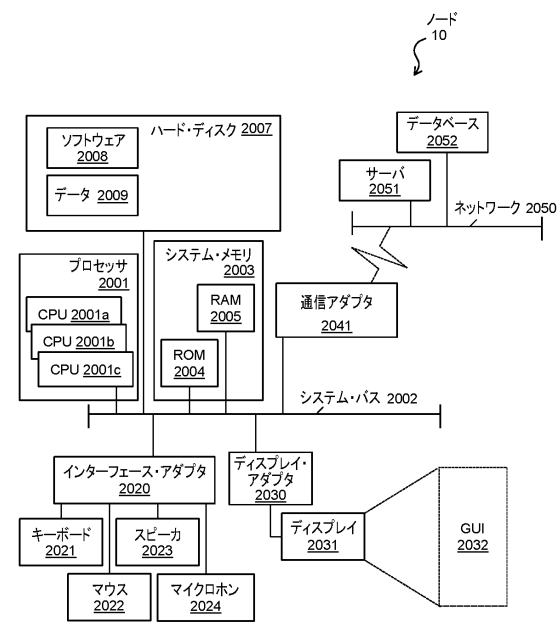
40

50

【図 19】



【図 20】



10

20

30

40

50

フロントページの続き

- (72)発明者 ボルントレガー、クリスチャン
 ドイツ連邦共和国 7 1 0 3 2 ベーブリンゲン シェーナイヒャー・シュトラッセ 2 2 0
- (72)発明者 インブレンダ、クラウディオ
 ドイツ連邦共和国 7 1 0 3 2 ベーブリンゲン シェーナイヒャー・シュトラッセ 2 2 0
- (72)発明者 ブサバ、ファディ
 アメリカ合衆国 1 2 6 0 1 ニューヨーク州 ポーキプシー サウス・ロード 2 4 5 5
- (72)発明者 ブラッドベリー、ジョナサン
 アメリカ合衆国 1 2 6 0 1 ニューヨーク州 ポーキプシー サウス・ロード 2 4 5 5
- (72)発明者 ヘラー、リサ
 アメリカ合衆国 1 2 6 0 1 ニューヨーク州 ポーキプシー サウス・ロード 2 4 5 5
- 審査官 宮司 卓佳
- (56)参考文献 米国特許出願公開第 2 0 1 6 / 0 1 3 2 3 4 5 (U S , A 1)
 特表 2 0 1 6 - 5 2 3 4 2 1 (J P , A)
 特表 2 0 1 7 - 5 1 5 2 0 2 (J P , A)
 特表 2 0 1 1 - 5 2 9 2 4 0 (J P , A)
 特表 2 0 1 1 - 5 1 7 7 9 7 (J P , A)
- (58)調査した分野 (Int.Cl., D B 名)
 G 0 6 F 2 1 / 6 2
 G 0 6 F 9 / 4 5 5