(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7350868号
(P7350868)

(45)発行日　令和5年9月26日(2023.9.26)

(24)登録日　令和5年9月15日(2023.9.15)

(51)国際特許分類
*G06F 12/14 (2006.01)*

FI
G06F 12/14 510E

請求項の数 14 （全44頁）

(21)出願番号　特願2021-550114(P2021-550114)
(86)(22)出願日　令和2年3月2日(2020.3.2)
(65)公表番号　特表2022-522702(P2022-522702A)
(43)公表日　令和4年4月20日(2022.4.20)
(86)国際出願番号　PCT/EP2020/055469
(87)国際公開番号　WO2020/182528
(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　16/296,306
(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】　複数のセキュリティ・ドメインにわたるセキュア・メモリの共用

(57)【特許請求の範囲】
【請求項１】
メモリのセキュア・ページに対するセキュア・アクセス・リクエストを、コンピュータ・システムのセキュア・インタフェース制御において受け取ること、
前記セキュア・インタフェース制御によって、前記セキュア・ページに関連づけられた仮想アドレス比較無効化状態をチェックすること、および
複数の仮想アドレスから同じ絶対アドレスへのマッピングをサポートするために、前記セキュア・インタフェース制御によって、前記仮想アドレス比較無効化状態がセットされていることに基づいて、前記セキュア・ページにアクセスする際の仮想アドレス・チェックを、前記セキュア・ページに対して無効化すること
を含む、方法。
【請求項２】
前記セキュア・インタフェース制御によって、複数のセキュア・ドメインのうちのセキュア・ドメインが共用ページにアクセスすることが許可されていることを、ドメイン識別子に基づいて確認すること
をさらに含む、請求項１に記載の方法。
【請求項３】
前記共用ページにアクセスする許可を確かめるために、前記セキュア・ドメインの前記ドメイン識別子が、共用を許すと識別された前記セキュア・ドメインの複数のドメイン識別子と比較される、請求項２に記載の方法。

【請求項４】
仮想アドレスを絶対アドレスにマップする動的アドレス変換テーブルの複数のグループがセキュアでないホストによって変更されていないことを確かめることであって、前記セキュアでないホストは前記セキュア・ページにアクセスすることができる複数のセキュア・ドメインのうちのいずれかについて前記動的アドレス変換テーブルの前記グループのうちの１つまたは複数のグループを管理するように構成されており、仮想アドレスに対してマップするそれぞれのテーブルが前記動的アドレス変換テーブルの前記１つまたは複数のグループの中の複数の関連テーブルを含む、確かめること、および
前記動的アドレス変換テーブルの前記１つまたは複数のグループの中で変化を検出したことに基づいて、前記セキュア・アクセス・リクエストを終了すること
を含む、請求項２または請求項３に記載の方法。
【請求項５】
前記仮想アドレス比較無効化状態が、前記セキュア・ページに関連づけられたセキュア・ドメイン識別子、前記セキュア・ページに関連づけられた仮想アドレス・マッピング・データおよび前記仮想アドレス比較無効化状態を含むゾーン・セキュリティ・テーブルを通して記憶および更新される、請求項１から請求項４のいずれか一項に記載の方法。
【請求項６】
前記セキュア・インタフェース制御がファームウェア、ハードウェアもしくは信頼できるソフトウェア、またはファームウェア、ハードウェアおよび信頼できるソフトウェアの組合せを含み、前記セキュア・ページがハイパーバイザまたはオペレーティング・システムによって管理されたセキュア仮想機械またはセキュア・コンテナに割り当てられる、請求項１から請求項５のいずれか一項に記載の方法。
【請求項７】
システムであって、
処理ユニットと、
セキュア・インタフェース制御と、
を備え、前記セキュア・インタフェース制御が、請求項１から請求項６のいずれか一項に記載の方法を前記処理ユニットに実行させるように構成されている、システム。
【請求項８】
処理ユニットに請求項１から請求項６のいずれか一項に記載の方法を実行させるように構成されている、コンピュータ・プログラム。
【請求項９】
請求項８に記載のコンピュータ・プログラムを記録した、コンピュータ可読ストレージ媒体。
【請求項１０】
メモリのセキュア・ページに対するセキュア・アクセス・リクエストを、コンピュータ・システムのセキュア・インタフェース制御において受け取ること、
前記セキュア・インタフェース制御によって、前記セキュア・ページに関連づけられた仮想アドレス比較無効化状態をチェックすること、および
前記セキュア・アクセス・リクエストを出したエンティティの許可ステータス、および前記仮想アドレス比較無効化状態がセットされていることに基づいて、仮想アドレスが指定されていない前記セキュア・ページへの絶対アドレス・アクセスを有効化すること
を含む、方法。
【請求項１１】
前記セキュア・インタフェース制御によって、複数のセキュア・ドメインのうちのセキュア・ドメインが共用ページにアクセスすることが許可されていることを、ドメイン識別子に基づいて確認すること
をさらに含む、請求項１０に記載の方法。
【請求項１２】
前記共用ページにアクセスする許可を確かめるために、前記セキュア・ドメインの前記

ドメイン識別子が、共用を許すと識別された前記セキュア・ドメインの複数のドメイン識別子と比較される、請求項１１に記載の方法。
【請求項１３】
前記セキュア・インタフェース制御がファームウェアもしくはハードウェア、またはファームウェアとハードウェアの組合せを含み、前記セキュア・ページがハイパーバイザまたはオペレーティング・システムによって管理されたセキュア・コンテナまたはセキュア仮想機械に割り当てられる、請求項１０から請求項１２のいずれか一項に記載の方法。
【請求項１４】
システムであって、
処理ユニットと、
セキュア・インタフェース制御と、
を備え、前記セキュア・インタフェース制御が、請求項１０から請求項１３のいずれか一項に記載の方法を前記処理ユニットに実行させるように構成されている、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、複数のセキュリティ・ドメイン（security domain）にわたってセキュアな（secure）（以後、セキュア）メモリを共用することに関する。
【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、ユーザが所有するデータを第三者のデータ・センタに記憶し、それらのデータをそのデータ・センタで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、ハードウェアを購入することまたは物理サーバのための床面積を提供することを顧客に要求することなしに、ＶＭを迅速かつ簡単に顧客に提供する能力を容易にする。顧客は、顧客の嗜好または要件の変化に応じてＶＭを簡単に拡張または縮小することができる。クラウド・コンピューティングのプロバイダは通常、プロバイダのデータ・センタのサーバ上に物理的に存在するＶＭを提供する。顧客はしばしば、ＶＭ内のデータのセキュリティについて心配する。これは特に、コンピューティング・プロバイダがしばしば、同じサーバ上に２以上の顧客のデータを記憶しているためである。顧客は、顧客が所有するコード／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、および顧客が所有するコード／データとプロバイダのサイトで動作している他のＶＭのコード／データとの間のセキュリティを要望することがある。さらに、顧客が、プロバイダの管理者からのセキュリティ、および機械上で動作している他のコードによる潜在的なセキュリティ侵害に対するセキュリティを要望することもある。
【０００３】
このような機密に関わる状況を取り扱うために、クラウド・サービス・プロバイダは、適正なデータ分離および論理ストレージ隔離を保証するためのセキュリティ制御を実装することがある。クラウド・インフラストラクチャを実装する際に仮想化が広範に使用されている結果、クラウド・サービスの顧客に対するセキュリティ上の特有の心配が生じている。これは、仮想化が、オペレーティング・システム（ＯＳ）と基礎をなすハードウェアとの間の関係を変化させるためである。このハードウェアは、コンピューティングもしくはストレージ・ハードウェアであることがあり、またはネットワーキング・ハードウェアであることさえある。これにより、仮想化は、それ自体が適正に構成、管理および防護されなければならない追加の層として導入される。
【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動作しているＶＭは、ゲストに対する仮想化サービスをトランスペアレントに（transparently）提供することを、このハイパーバイザに頼っている。これらのサービスには、メモリ管理、命令エミュレーシ

ョンおよび割込み処理が含まれる。

【０００５】

メモリ管理の場合、ＶＭは、そのＶＭのデータを、メモリに存在するようにディスクから移動させ（ページイン）、さらに、そのＶＭのデータをディスクに戻す（ページアウト）ことができる。そのページがメモリに存在する間、ＶＭ（ゲスト）は、動的アドレス変換（dynamic address translation）（ＤＡＴ）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プする。さらに、ホスト・ハイパーバイザも、メモリ内のゲスト・ページに対するそれ自体の（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、ホスト・ハイパーバイザは、ゲストとは独立に、またゲストに対してトランスペアレントに、ゲスト・ページをメモリにページインすることおよびメモリからページアウトすることができる。ハイパーバイザは、２つの別個のゲストＶＭ間でのゲスト・メモリのメモリ分離またはメモリ共用を、ホストＤＡＴテーブルによって提供する。ホストはさらに、必要に応じて、ゲストに代わって、ゲスト・メモリにアクセスして、ゲスト・オペレーションをシミュレートすることができる。

【発明の概要】

【０００６】

本発明の１つまたは複数の実施形態によれば、コンピュータ実施方法（computerimplemented method）は、メモリのセキュア・ページに対するセキュア・アクセス・リクエストを、コンピュータ・システムのセキュア・インタフェース制御（secure interface control）において受け取ることを含む。セキュア・インタフェース制御は、そのセキュア・ページに関連づけられた仮想アドレス比較無効化状態（disable virtual address compare state）をチェックすることができる。セキュア・インタフェース制御は、複数の仮想アドレスから同じ絶対アドレスへのマッピングをサポートするために、仮想アドレス比較無効化状態がセットされていることに基づいて、セキュア・ページにアクセスする際の仮想アドレス・チェックを、セキュア・ページに対して無効化することができる。利点は、複数のセキュリティ・ドメインにわたってセキュア・メモリを共用することを含みうる。

【０００７】

本発明の追加の実施形態または代替実施形態によれば、セキュア・インタフェース制御は、複数のセキュア・ドメインのうちのセキュア・ドメインが共用ページにアクセスすることが許可されていることを、ドメイン識別子に基づいて確認することができる。利点は、ドメイン識別子に基づいて共用を拘束することを含みうる。

【０００８】

本発明の追加の実施形態または代替実施形態によれば、共用ページにアクセスする許可を確かめるために、セキュア・ドメインのドメイン識別子を、共用を許すと識別されたセキュア・ドメインの複数のドメイン識別子と比較することができる。利点は、ドメイン識別子のリストのメンバーに共用を限定することを含みうる。

【０００９】

本発明の追加の実施形態または代替実施形態によれば、セキュア・インタフェース制御は、仮想アドレスを絶対アドレスにマップする動的アドレス変換テーブルの複数のグループがセキュアでないホストによって変更されていないことを確かめることができ、セキュアでないホストは、セキュア・ページにアクセスすることができる複数のセキュア・ドメインのうちのいずれかについて動的アドレス変換テーブルのグループのうちの１つまたは複数のグループを管理するように構成されている。仮想アドレスに対してマップするそれぞれのテーブルは、動的アドレス変換テーブルの１つまたは複数のグループの中の複数の関連テーブルを含む。動的アドレス変換テーブルの１つまたは複数のグループの中で変化を検出したことに基づいて、セキュア・アクセス・リクエストを終了することができる。利点は、セキュアでないホストが、セキュア・ページにアクセスするために使用されるアドレス・マッピングを変更しないことを確かめることを含みうる。

【００１０】

本発明の追加の実施形態または代替実施形態によれば、セキュア・ページに関連づけら

れたセキュア・ドメイン識別子、セキュア・ページに関連づけられた仮想アドレス・マッピング・データおよび仮想アドレス比較無効化状態を含むゾーン・セキュリティ・テーブルを通して、仮想アドレス比較無効化状態を記憶および更新することができる。利点は、メモリのセキュア・ドメインもしくはページまたはその両方ごとにオプションを追跡および構成することを含みうる。

【００１１】

本発明の追加の実施形態または代替実施形態によれば、セキュア・インタフェース制御を、ファームウェア、ハードウェアもしくは信頼できるソフトウェア、またはファームウェア、ハードウェアおよび信頼できるソフトウェアの組合せとすることができる。セキュア・ページを、ハイパーバイザまたはオペレーティング・システムによって管理されたセキュア仮想機械またはセキュア・コンテナ（secure container）に割り当てることができる。利点は、システム全体の性能に対する関連オペレーション影響が小さいセキュア・インタフェース制御を実現することを含みうる。

【００１２】

本発明の１つまたは複数の実施形態によれば、コンピュータ実施方法は、メモリのセキュア・ページに対するセキュア・アクセス・リクエストを、コンピュータ・システムのセキュア・インタフェース制御において受け取ることを含む。セキュア・インタフェース制御は、そのセキュア・ページに関連づけられた仮想アドレス比較無効化状態をチェックすることができる。セキュア・インタフェース制御は、セキュア・アクセス・リクエストを出したエンティティの許可ステータス、および仮想アドレス比較無効化状態がセットされていることに基づいて、仮想アドレスが指定されていないセキュア・ページへの絶対アドレス・アクセスを有効化することができる。利点は、セキュア・ページを共用するために絶対アドレス・アクセスをサポートすることを含みうる。

【００１３】

本発明の他の実施形態は、上述の方法の特徴を、コンピュータ・システムおよびコンピュータ・プログラム製品に実装する。

【００１４】

本開示の技法によって、追加の特徴および利益が実現される。本明細書には、本発明の他の実施形態および態様が詳細に記載されており、それらは、本発明の部分とみなされる。本発明ならびに本発明の利点および特徴をより十分に理解するためには、以下説明および図面を参照されたい。

【００１５】

本明細書に記載された独占権の詳細は、本明細書の末尾の特許請求の範囲に具体的に示されており、明確に主張されている。本発明の実施形態の上記の特徴および利点ならびにその他の特徴および利点は、添付図面とともに解釈さ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】

【００１６】

【図１】本発明の１つまたは複数の実施形態による、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よる、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よる、ハイパーバイザの下で動作している仮想機械（virtual machine）（ＶＭ）をサポートするネストされた（nested）マルチパート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つまたは複数の実施形態による、動的アドレス変換（ＤＡＴ）オペレーションのシステム概略図を示す図である。

【図６】本発明の１つまたは複数の実施形態による、セキュア・インタフェース制御メモ

リのシステム概略図を示す図である。
【図７】本発明の１つまたは複数の実施形態による、インポート・オペレーションのプロセス・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よる、インポート・オペレーションのプロセス・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よる、供与メモリ・オペレーション（donated memory operation）のプロセス・フローを示す図である。
【図１０】本発明の１つまたは複数の実施形態による、非セキュア（non-secure）ハイパーバイザ・ページからセキュア・インタフェース制御のセキュア・ページへの移行（transition）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よる、セキュア・インタフェース制御によってなされたセキュア・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よる、セキュア・インタフェース制御およびハードウェアによるアクセス・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よる、プログラムおよびセキュア・インタフェース制御によるセキュア・アクセスおよび非セキュア・アクセスをサポートする変換のプロセス・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よる、プログラムおよびセキュア・インタフェース制御によるセキュア・ストレージ保護付きの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よる、仮想アドレス・モード・チェッキングのためのプロセス・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よる、アドレス変換によるページ共用のブロック図である。
【図１７】本発明の１つまたは複数の実施形態による、アドレス変換およびページ複製によるページ共用のブロック図である。
【図１８】本発明の１つまたは複数の実施形態による、複数のセキュリティ・ドメインにわたってセキュア・メモリを共用するためのプロセス・フローを示す図である。
【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２０】本発明の１つまたは複数の実施形態による抽象化モデル層を示す図である。
【図２１】本発明の１つまたは複数の実施形態によるシステムを示す図である。
【図２２】本発明の１つまたは複数の実施形態による処理システムを示す図である。
【発明を実施するための形態】
【００１７】
本明細書に示された図は例示を目的としている。本発明の思想を逸脱しない、図および図に記載されたオペレーションに対する多くの変形態様が存在しうる。例えば、動作を異なる順序で実行することができ、または動作を追加、削除もしくは変更することができる。さらに、用語「結合された（coupled）」およびその変異語は、２つの要素間に通信経路を有することを示し、要素間に介在要素／接続がない要素間の直接接続を含意しない。これらの変形態様は全て本明細書の一部とみなされる。
【００１８】
本発明の１つまたは複数の実施形態は、追加のセキュリティを提供するために、ソフトウェアと機械との間の効率的で軽量のセキュア・インタフェース制御を強化する。
【００１９】
ホスト・ハイパーバイザの制御下でゲストとして動作している仮想機械（ＶＭ）は、ゲストに対する仮想化サービスをトランスペアレントに提供することを、こ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・エンティティと信頼できない別のエンティティとの間のインタフェースに適用することができる。このインタフェースは従来、この別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許している。前述のとお

り、これらのサービスには、限定はされないが、メモリ管理、命令エミュレーションおよび割込み処理が含まれうる。例えば、割込みおよび例外インジェクション（exception injection）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領域（ロー・コア（low core））に対する読出しもしくは書込みまたはその両方を実行する。本明細書で使用される用語「仮想機械」ないし「ＶＭ」は、物理機械（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）の論理表現のことを指している。ＶＭは、基礎をなすホスト機械（物理プロセッサまたは一組のプロセッサ）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・リソースから見ると、ＶＭは、それ自体の独立した物理機械であるように見える。本明細書で使用される用語「ハイパーバイザ」および「ＶＭモニタ（ＶＭＭ）」は、複数のＶＭを管理する処理環境またはプラットフォーム・サービスであって、それらのＶＭが、同じホスト機械上で複数の（時に異なる）ＯＳを使用して実行されることを可能に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している。ＶＭをデプロイすることは、ＶＭのインストール・プロセスおよびＶＭの起動（または始動）プロセスを含むことを理解すべきである。別の例では、ＶＭをデプロイすることが、ＶＭの起動（または始動）プロセスを含む（例えばＶＭが以前にインストールされた場合またはＶＭが既に存在する場合）。

【００２０】

セキュア・ゲストを容易にし、サポートするため、ハイパーバイザとセキュア・ゲストとの間の、ハイパーバイザに依存しない追加のセキュリティであって、ハイパーバイザが、ＶＭからのデータにアクセスすることができず、したがって上で説明したやり方でサービスを提供することができないような態様の追加のセキュリティが求められているという、技術上の課題が存在している。

【００２１】

本明細書に記載されたセキュア実行（secure execution）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・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ハードウェア機構を提供する。セキュア・ゲストに関しては、「信頼できない」非セキュア・ハイパーバイザとセキュア・ゲストの間に追加のセキュリティが提供される。これを達成するためには、通常はゲストに代わってハイパーバイザが実行する機能の多くを機械に組み込む必要がある。ハイパーバイザとセキュア・ゲストの間にセキュア・インタフェースを提供するために、本明細書では「ＵＶ」とも呼ぶ新規のセキュア・インタフェース制御を説明する。本明細書では、用語セキュア・インタフェース制御とＵＶとが相互に交換可能に使用される。この追加のセキュリティを提供するために、セキュア・インタフェース制御はハードウェアと協力して働く。さらに、より低水準の（lower level）ハイパーバイザが、この信頼できないハイパーバイザに対して仮想化を提供していることがあり、このより低水準のハイパーバイザが、信頼できるコード（例えば信頼できるソフトウェア）の中に実装されている場合には、このハイパーバイザを、セキュア・インタフェース制御の部分とすることもできる。

【００２２】

一例では、セキュア・インタフェース制御が、内部の信頼できるセキュア・ハードウェアもしくはファームウェアまたはその両方の中に実装される。この信頼できるファームウェアは、例えばプロセッサ・ミリコードまたはＰＲ／ＳＭ論理分割コード（logical partitioning code）を含むことができる。セキュア・ゲストまたはエンティティに関して、セキュア・インタフェース制御は、セキュア環境の初期化および維持、ならびにハードウェア上でのこれらのセキュア・エンティティのディスパッチの調整を提供する。セキュア・ゲストがデータを能動的に使用しており、セキュア・ゲストがホスト・ストレージに存在する間、セキュア・ゲストは、セキュア・ストレージ内で「妨げるものなしに（in the clear）」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・ゲストによってアクセスされ得る。このことは、ハードウェアによって厳しく実行される。すなわち、ハードウェアは、（ハイパーバイザまたは他の非セキュア・ゲストを含む）非セキュア

・エンティティ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。この例では、セキュア・インタフェース制御が、最も低水準のファームウェアの信頼できる部分として動作する。最も低水準のファームウェアまたはミリコードは、実際にハードウェアの拡張であり、複雑な命令および機能、例えばＩＢＭのｚＡｒｃｈｉｔｅｃｔｕｒｅ（Ｒ）に定義された複雑な命令および機能を実施するために使用される。ミリコードは、ストレージの全ての部分にアクセスすることができ、セキュア実行の文脈では、この部分が、それ自体のセキュア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用ストレージを含む。このことは、このミリコードが、セキュア・ゲストまたはそのゲストをサポートするハイパーバイザが必要とする機能を提供することを可能にする。セキュア・インタフェース制御はさらに、ハードウェアに直接にアクセスすることができ、このことは、ハードウェアが、セキュア・インタフェース制御によって確立された条件の制御の下で、セキュリティ・チェックを効率的に提供することを可能にする。

【００２３】

本発明の１つまたは複数の実施形態によれば、このソフトウェアは、ＵＶ呼出し（ＵＶＣ）命令を使用して、特定の動作を実行するようセキュア・インタフェース制御に要求する。例えば、ハイパーバイザはこのＵＶＣ命令を使用して、セキュア・インタフェース制御を初期化すること、セキュア・ゲスト・ドメイン（例えばセキュア・ゲスト構成）を生成すること、およびそのセキュア構成内に仮想ＣＰＵを生成することができる。さらに、このＵＶＣ命令を使用して、ハイパーバイザ・ページイン・オペレーションまたはハイパーバイザ・ページアウト・オペレーションの部分として、セキュア・ゲスト・ページをインポートすること（復号し、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、セキュア・ゲスト・ページへのホスト・アクセスを許すこと）もできる。さらに、セキュア・ゲストは、ハイパーバイザと共用するストレージを定義し、セキュア・ストレージを共用し、共用ストレージをセキュアにする能力を有する。

【００２４】

多くの他のアーキテクテッド命令（architected instruction）と同様に、これらのＵＶＣコマンドを機械ファームウェアによって実行することができる。この機械はセキュア・インタフェース制御モードには入らず、その代わりに、この機械が現在動作しているモードでセキュア・インタフェース制御の機能を実行する。ハードウェアは、ファームウェア状態とソフトウェア状態の両方を維持し、そのため、これらのオペレーションを取り扱うための文脈の切換え（switch of contexts）は起こらない。この低いオーバヘッドは、ソフトウェア、セキュア・インタフェース制御の複雑さを最小化し低減させ、それにもかかわらず必要なセキュリティ・レベルを提供するような形での、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層間の緊密な協働を可能にする。

【００２５】

本発明の１つまたは複数の実施形態によれば、セキュア・ゲスト環境およびサポート・ハイパーバイザ環境を適正に維持するためにセキュア・インタフェース制御およびハードウェアが必要とする制御ブロック構造のサポートにおいて、ハイパーバイザは、セキュア・ゲスト環境を初期化する間に、セキュア・インタフェース制御にストレージを供与する。その結果として、ハイパーバイザは、１）セキュア・ゲストを動作するゾーンを初期化するため、２）セキュア・ゲスト・ドメインを生成するため、および３）それぞれのドメインで動作するセキュアＣＰＵを生成するための準備において、とりわけ供与に必要なストレージの量を決定するために、照会ＵＶＣ（query UVC）命令を発する。ストレージが供与された後、そのストレージにはセキュア・ストレージのマークが付けられ、そのストレージは、セキュア・インタフェース制御に属するものとして登録され、非セキュアまたはセキュア・ゲスト・エンティティによるアクセスが禁じられる。このことは、関連エンティティ（例えばセキュア・ゲストＣＰＵ、セキュア・ゲスト・ドメインまたはゾーン）が破壊されるときまで事実であり続ける。

【００２６】

一例では、ゾーン特定ＵＶ制御ブロックをサポートするＵＶストレージの第１のセクションが、初期化ＵＶＣの一部としてセキュア・インタフェース制御に供与され、このセクションは、本明細書ではＵＶ２ストレージと呼ぶものの中に存在する。（それぞれのセキュア・ゲスト・ドメインに対する）ベース（base）セキュア・ゲスト構成制御ブロックおよび可変(variable)セキュア・ゲスト構成制御ブロックをサポートするＵＶストレージの第２および第３のセクションは、セキュア・ゲスト構成生成（create-secure-guest-configuration）ＵＶＣの一部として供与され、それらのセクションはそれぞれ、ＵＶＳおよびＵＶＶストレージの中に存在する。セキュアＣＰＵ制御ブロックをサポートするＵＶストレージの第４のセクションおよび最終セクションもＵＶＳ空間に存在し、それらのセクションは、セキュア・ゲストＣＰＵ生成（create-secure-guest-CPU）ＵＶＣの一部として供与される。これらのそれぞれのエリアが供与されると、セキュア制御インタフェースは、（非セキュア・エンティティがそれらエリアにアクセスすることを防ぐために）それらのエリアにセキュアのマークを付け、さらに、（セキュア・ゲスト・エンティティがそれらのエリアにアクセスすることを防ぐために）それらのエリアを、ゾーン・セキュリティ・テーブルに、セキュア・インタフェース制御に属するものとして登録する。ＵＶ空間内のさらなる分離を提供するため、（特定のどのセキュア・ゲスト・ドメインにも関連づけられていない）ＵＶ２空間にさらに、固有のＵＶ２セキュア・ドメインのタグが付けられ、その一方で、ＵＶＳ空間とＵＶＶ空間の両方に、関連する特定のセキュア・ゲスト・ドメインのタグが付けられる。この例では、ＵＶＶ空間がホスト仮想空間に存在し、したがって、ホスト仮想－ホスト絶対マッピングによってＵＶＶ空間をさらに識別することができる。

【００２７】

セキュア・インタフェース制御は、全てのストレージ（非セキュア・ストレージ、セキュア・ゲスト・ストレージおよびＵＶストレージ）にアクセスすることができるが、本発明の１つまたは複数の実施形態は、セキュア・インタフェース制御がＵＶストレージに非常に特異的にアクセスすることを可能にする機構を提供する。セキュア・ゲスト・ドメイン間の分離を提供する同じハードウェア機構を使用して、本発明の実施形態は、ＵＶストレージ内の同様の分離を提供することができる。このことは、セキュア・インタフェース制御が、意図および指定されたときにＵＶストレージだけにアクセスすること、セキュア・インタフェース制御が、所望の指定されたセキュア・ゲストに対するセキュア・ゲスト・ストレージだけにアクセスすること、および、セキュア・インタフェース制御が、指定されたときに、非セキュア・ストレージだけにアクセスすることを保証する。すなわち、セキュア・インタフェース制御は、セキュア・インタフェース制御がアクセスしようと意図するストレージを非常に明確に指定することができ、そのため、ハードウェアは、セキュア・インタフェース制御がそのストレージに実際にアクセスすることを保証することができる。さらに、セキュア・インタフェース制御は、セキュア・インタフェース制御が、指定されたセキュア・ゲスト・ドメインに関連づけられたＵＶストレージだけにアクセスすることを意図していることをさらに指定することができる。

【００２８】

セキュリティを提供するため、ハイパーバイザが、セキュア・ゲスト・データをトランスペアレントにページインおよびページアウトしているときには、ハードウェアとともに働いているセキュア・インタフェース制御が、データの復号および暗号化を提供および保証する。これを達成するため、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ＵＶＣを発行する必要がある。これらの新たなＵＶＣ中にセキュア・インタ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ＵＶＣが実際にハイパーバイザによって発行されることを保証する。

【００２９】

この新規のセキュア環境では、ハイパーバイザがセキュア・ページをページアウトしているときにはいつでも、ハイパーバイザは、新たなセキュア・ストレージからの変換（co

nvert from secure storage）（エクスポート）ＵＶＣを発行する必要がある。このエクスポートＵＶＣに応答して、セキュア・インタフェース制御は、１）そのページがＵＶによって「ロックされている」ことを示し、２）そのページを暗号化し、３）そのページを非セキュアにセットし、４）ＵＶロックをリセットする。このエクスポートＵＶＣが完了した後、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することができる。

【００３０】

さらに、ハイパーバイザがセキュア・ページをページインしているときにはいつでも、ハイパーバイザは、新たなセキュア・ストレージへの変換（convert to secure storage）（インポート）ＵＶＣを発行しなければならない。このインポートＵＶＣに応答して、ＵＶないしセキュア・インタフェース制御は、１）ハードウェア内で、そのページにセキュア・ページのマークを付け、２）そのページがＵＶによって「ロックされている」ことを示し、３）そのページを復号し、４）特定のセキュア・ゲスト・ドメインに権限（authority）をセットし、５）ＵＶロックをリセットする。セキュア・エンティティによってアクセスがなされているときにはいつでも、ハードウェアは、変換中にそのページに対する許可チェックを実行する。これらのチェックは、１）このページが実際に、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・ドメインに属していることを確認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る間、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なかったことを確かめるためのチェックを含む。ページにセキュア・ページのマークが付けられた後、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によるセキュア・ページへのアクセスを防ぐ。これらの追加の変換ステップは、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再マッピングを防ぐ。

【００３１】

セキュアＶＭまたはセキュア・コンテナなどのセキュア・エンティティに関して、メモリのそれぞれの絶対ページは通常、１つのセキュアＶＭ（またはコンテナ）に割り当てられ、それらのページが、他のＶＭ／コンテナないしハイパーバイザ／ＯＳによってアクセスされること、または他のＶＭ／コンテナないしハイパーバイザ／ＯＳによって共用されることは許されない。ある種の動作環境では、さまざまなセキュアＶＭ／コンテナ間で論理的に共用された共通のセキュア・メモリ（例えばセキュア・データベースまたはＯＳカーネル内のセキュア共用エリア）が存在しうる。異なるＶＭ（またはコンテナ）を管理しているハイパーバイザ（またはＯＳ）は、必要なメモリ分離を達成するために、動作しているそれぞれのＶＭ（またはコンテナ）に対して異なるメモリ・アドレス空間を割り当てることができる。動作しているそれぞれのＶＭ（またはコンテナ）は、動作している他のＶＭ（または、コンテナ）から独立したそれ自体のアドレス空間を有するように見えることがある。これらのＶＭ間で共通のストレージを共用するため、ハイパーバイザは、アドレス変換によって、動作しているさまざまなＶＭからの仮想アドレスを、同じ物理メモリにマップすることができる。セキュアＶＭ／コンテナに関して、ハイパーバイザ／ＯＳは信頼できないことがあり、さまざまなＶＭからの異なる仮想アドレスを単一の絶対アドレスにマップすることが普通は禁じられていることがある。仮想アドレスから物理アドレスへのマッピングが非セキュア・ハイパーバイザ／ＯＳによって改竄されていないことを確認することに、セキュア・インタフェース制御が責任を負うようにすることができる。重複マッピングのないページ共用の可能な回避法は、複製コピーを使用し、動作しているそれぞれのＶＭまたはコンテナに１つのコピーを割り当てる方法である。複製イメージを管理する複雑さに共通のセキュア・データベースを共用する複雑さが加わるときには、数千ものＶＭまたはコンテナ・イメージを動作しているシステムに対してこの手法が実行可能でないことがある。

【００３２】

上述のとおり、セキュア・インタフェース制御が、とりわけアドレス変換完全性を保証することに責任を負うようにすることができる。セキュア・ゲスト・ストレージの他に、

ハイパーバイザ・ストレージから供与され、セキュア・インタフェース制御に与えられたメモリ・エリアが存在しうる。これらのエリアには、セキュア・インタフェース制御だけがアクセス可能であることがある。これらのエリアを絶対メモリとして維持および参照することができ、これらのエリアは通常、動的アドレス変換を受けない。これらのセキュア絶対ページは、それらのページに関連づけられた仮想アドレス・マッピングを持たないことがある。本発明の実施形態は、動作しているセキュア・コンテナまたはセキュアＶＭに適用することができ、セキュアＯＳとセキュア・コンテナとの間またはハイパーバイザとセキュアＶＭとの間での共通のセキュア・エリアの共用を可能にする。動作している複数のセキュア・コンテナ／ＶＭ間で共用をサポートすることもできる。これについては本明細書でさらに説明される。

【００３３】

次に図１を参照すると、本発明の１つまたは複数の実施形態による、ゾーン・セキュリティのためのテーブル１００が概括的に示されている。図１に示されたゾーン・セキュリティ・テーブル１００は、セキュア・エンティティによってアクセスされたページへのセキュア・アクセスを保証するために、セキュア・インタフェース制御によって維持され、セキュア・インタ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１１０によって索引付けされている。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。それぞれのエントリは、アクセスしているセキュア・エンティティにそのエントリが属していることを確認するために使用される情報を含む。

【００３４】

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、（このページに関連づけられたセキュア・ドメインを識別する）セキュア・ドメインＩＤ１２０、（このページが、セキュア・インタフェース制御に供与されたものであること、およびこのページが、セキュア・インタフェース制御によって所有されていることを示す）ＵＶビット１３０、（ホスト絶対ページと定義されたセキュア・インタフェース制御ページが関連ホスト仮想アドレスを有していないときなどのある種の状況においてホスト・アドレス対比較を無効(ディスエーブル)にするために使用される）アドレス比較無効化（disable address compare）（ＤＡ）ビット１４０、（このページが非セキュア・ハイパーバイザによって共用されていることを示す）共用（shared）（ＳＨ）ビット１５０、および（ホスト・アドレス対と呼ばれる、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す）ホスト仮想アドレス１６０を含む。ホスト・アドレス対は、ホスト絶対アドレスおよび登録された関連ホスト仮想アドレスを示すことに留意されたい。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、この比較は、このページがゲストによって使用されている間、ホストがこのページをリマップしないことを保証する。

【００３５】

動的アドレス変換（ＤＡＴ）は、仮想記憶を実ストレージにマップするために使用される。ハイパーバイザの制御下で、ゲストＶＭが、ページング可能なゲストとして動作しているとき、ゲストは、ＤＡＴを使用して、ゲストのメモリに存在するページを管理する。さらに、ホストは、独立してＤＡＴを使用して、それらのページがホストのメモリに存在するときに、（ホスト自体のページとともに）それらのゲスト・ページを管理する。ハイパーバイザは、ＤＡＴを使用して、異なるＶＭ間でのストレージの分離もしくは共用またはその両方を提供し、ハイパーバイザ・ストレージへのゲスト・アクセスを防ぐ。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、それらのゲストの全てのストレージにアクセスすることができる。

【００３６】

ＤＡＴは、１つのアプリケーションを別のアプリケーションから分離することを可能にし、その一方で、それでも、それらのアプリケーションが共通のリソースを共用することを許す。さらに、ＤＡＴは、ＶＭの実装を可能にする。ＶＭは、ＯＳの新しいバージョン

の設計および試験、ならびにアプリケーション・プログラムの並行処理に使用されることがある。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、それらの仮想アドレスは、（ＤＡＴテーブルを含む）特定の変換パラメータとともに、それぞれの仮想アドレスを関連絶対アドレスに変換することを可能にする。この関連絶対アドレスは、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。

【００３７】

ＤＡＴは、マルチテーブル・ルックアップ（例えば変換ごとの一群のＤＡＴテーブル）を使用して、仮想アドレスを関連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および維持される。このストレージ・マネージャは、１つのページをページアウトして例えば別のページを持ち込むことによって、複数のプログラム間で絶対ストレージをトランスペアレントに共用する。そのページがページアウトされたとき、ストレージ・マネージャは、例えば、関連ページ・テーブル内の無効ビットをセットする。１つのプログラムが、ページアウトされたページにアクセスしようとすると、ハードウェアは、しばしばページ・フォールト（page fault）と呼ばれるプログラム割込みをストレージ・マネージャに提示する。これに応答して、ストレージ・マネージャは、リクエスト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。これは全て、そのプログラムに対してトランスペアレントに実行され、これによって、ストレージ・マネージャは、そのストレージを仮想化し、さまざまな異なるユーザ間でそのストレージを共用することができる。

【００３８】

主ストレージにアクセスするためにＣＰＵによって仮想アドレスが使用されるとき、その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（prefixing）によっ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も高水準のテーブルの指示（designation）（起点および長さ）は、アドレス空間制御要素（address-space-controlelement）（ＡＳＣＥ）と呼ばれ、この指示が関連アドレス空間を定義する。

【００３９】

本発明の１つまたは複数の実施形態によれば、セキュア・ページにアクセスするためにセキュア・インタフェース制御によってなされる仮想アドレス・チェックを無効化するために、図１のゾーン・セキュリティ・テーブル１００内のＤＡビット１４０をそれぞれのセキュア・ページに関連づけることができる。ＤＡビット１４０は、セキュア・インタフェース制御の制御下にあるフィールドとすることができる。ＤＡビット１４０は、ゾーン・セキュリティ・テーブルにセキュア・ページを登録し、そのセキュア・ページをセキュア・ドメインに割り当てるときに、適切にセットすることができる。セキュア・インタフェース制御がセキュア・ページにアクセスしているときにそのアクセスが許されているかどうかを判定するためにセキュア・インタフェース制御によって実行されるセキュリティ・チェッキングの部分として、ＤＡビットを使用することができる。ＤＡビットが０のとき、セキュア・ページへのアクセスがなれているときにセキュア・インタフェース制御によって実行されるセキュリティ・チェックのこの部分は、そのセキュア・ページに対するＤＡＴ変換テーブルが、セキュア・インタフェース制御が知らないうちに変更されていることがないことを保証することである。セキュア・ドメインにページが与えられた後、（ホスト絶対アドレスと結合してホスト・アドレス対を生成する）ホスト仮想アドレス１６０が、関連セキュア・ドメインＩＤ１２０およびそのセキュア・ページに関連した図１に示された他の属性とともに、そのページに対する図１のゾーン・セキュリティ・テーブル１００に登録される。そのページにアクセスするたびに、セキュア・インタフェース制御は、アクセスしている仮想／絶対ホスト・アドレス対とアクセスしているセキュア・ドメインＩＤの両方を、以前に登録されたアドレス対およびドメインＩＤと比較することによって、そのアクセスを確認することができる。不一致が存在する場合、セキュア・インタフェース制御は、例外を報告することができる。したがって、ＤＡ＝０のとき、所与のホ

スト絶対アドレスには１つのホスト仮想アドレスだけがマップすることができる。

【００４０】

本発明の１つまたは複数の実施形態において説明されているとおり、ＤＡビットのマーク付け（marking）は、それがセットされているときに、多くのホスト仮想アドレスを同じ１つのホスト絶対アドレスにマップすることを可能にすることができる。このＤＡビット・マーク付けは、セキュア・インタフェース制御の制御下に置くことができ、このＤＡビット・マーク付けは、他のドメインとページを共用することが許可されたドメイン、およびセキュア共通ページとしてマーク付けされたホスト仮想ページに対してのみセットすることができる。したがって、ＤＡ＝１のときには、さまざまなセキュア・ドメインにわたって、固有の１対１の仮想アドレス－絶対アドレス・マッピングまたは同じ１対１の仮想アドレス－絶対アドレス・マッピングが存在することができ、それぞれの１対１マッピングは、１つのセキュア・ドメインによって所有されうる。ハイパーバイザによってセキュア・インタフェース制御に供与され、絶対アドレスとして定義された（例えば仮想アドレスが指定されていない）ホスト絶対ページに対してＤＡビットをセットすることもできる。この両方の使用をサポートして、セキュア・インタフェース制御もしくは他のシステム構成要素またはその両方は、ＤＡ＝１とマーク付けされたページに対する仮想アドレス・チェックを無視することができる。特定のページにこのマーク付けを関連づけることができ、このマーク付けは、必ずしもセキュア・ドメイン全体に適用されない。さらに、そのページがセキュア・ページであるとき、システムは、許可されたコンテナ／ＶＭだけがその共用セキュア・ページにアクセスすることができることを確認することができる。

【００４１】

次に図２を参照すると、本発明の１つまたは複数の実施形態による、ＤＡＴを実行するための例示的な仮想アドレス空間２０２、２０４および絶対アドレス空間２０６が概括的に示されている。図２に示された例には、２つの仮想アドレス空間、すなわち（アドレス空間制御要素（ＡＳＣＥ）Ａ　２０８によって定義された）仮想アドレス空間２０２、および（ＡＳＣＥ　Ｂ　２１０によって定義された）仮想アドレス空間２０４が存在する。仮想ページＡ１．Ｖ　２１２ａ１、Ａ２．Ｖ　２１２ａ２およびＡ３．Ｖ　２１２ａ３は、ストレージ・マネージャによって、マルチテーブル（セグメント２３０およびページ・テーブル２３２ａ、２３２ｂ）ルックアップにおいて、ＡＳＣＥ　Ａ　２０８を使用して、絶対ページＡ１．Ａ　２２０ａ１、Ａ２．Ａ　２２０ａ２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を使用して、それぞれ絶対ページＢ１．Ａ　２２２ｂ１およびＢ２．Ａ　２２２ｂ２にマップされる。

【００４２】

次に図３を参照すると、本発明の１つまたは複数の実施形態による、ハイパーバイザの下で動作しているＶＭをサポートするために使用されるネストされたマルチパートＤＡＴ変換の一例が概括的に示されている。図３に示された例では、（ゲストＡＳＣＥ（ＧＡＳＣＥ）Ａ　３０４によって定義された）ゲストＡ仮想アドレス空間Ａ　３０２と（ＧＡＳＣＥＢ　３０８によって定義された）ゲストＢ仮想アドレス空間Ｂ　３０６がともに、共用ホスト（ハイパーバイザ）仮想アドレス空間３２５内に存在する。示されているように、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はそれぞれ、ゲストＡストレージ・マネージャによって、ＧＡＳＣＥＡ　３０４を使用して、ゲスト絶対ページＡ１．ＨＶ　３４０ａ１、Ａ２．ＨＶ　３４０ａ２およびＡ３．ＨＶ　３４０ａ３にマップされている。ゲストＢに属する仮想ページＢ１．ＧＶ　３２０ｂ１およびＢ２．ＧＶ　３２０ｂ２はそれぞれ、独立して、ゲストＢストレージ・マネージャによって、ＧＡＳＣＥＢ　３０８を使用して、ゲスト絶対ページＢ１．ＨＶ　３６０ｂ１およびＢ２．ＨＶ　３６０ｂ２にマップされている。この例では、これらのゲスト絶対ページが、共用ホスト仮想アドレス空間３２５内に直接にマップし、続いて、追加のホストＤＡＴ変換を経て、ホスト絶対アドレス空間３３０にマップする。示されているように、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）３５０を使用して、Ａ１．ＨＡ　３７０ａ１、Ａ３．ＨＡ　３７０ａ３およびＢ１．ＨＡ　３７０ｂ１にマップされている。ゲストＡに属するホスト仮想アドレスＡ２．ＨＶ　３４０ａ２とゲストＢに属するＢ２．ＨＶ　３６０ｂ２はともに、同じホスト絶対ページＡＢ２．ＨＡ　３８０にマップされている。これによって、これらの２つのゲスト間でデータを共用することができる。ゲストＤＡＴ変換の間、それぞれのゲスト・テーブル・アドレスはゲスト絶対アドレスとして取り扱われ、追加のネストされたホストＤＡＴ変換を受ける。

【００４３】

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は禁じられる。ハイパーバイザは、存在する所与のセキュア・ゲスト・ページに関して以下のことが起こることを規定している。関連するホスト絶対アドレスには、単一のハイパーバイザ（ホスト）ＤＡＴマッピングによってのみ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所与のホスト絶対アドレスにマップす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・ページに関連した（ホスト仮想アドレスからホスト絶対アドレスへの）ハイパーバイザＤＡＴマッピングは、そのページがページインされている間、変化しない。セキュア・ゲスト・ページに関連した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。

【００４４】

本発明の１つまたは複数の実施形態によれば、セキュア・ゲスト間のストレージの共用も禁じられる。ストレージは、単一のセキュア・ゲストとハイパーバイザとの間で、そのセキュア・ゲストの制御下で共用される。ＵＶストレージはセキュア・ストレージであり、セキュア・インタフェース制御によるアクセスは可能だが、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・インタフェース制御に割り振られる。本発明の１つまたは複数の実施形態によれば、これらの規則の違反の企ては、ハードウェアおよびセキュア・インタフェース制御によって禁じられる。

【００４５】

次に図４を参照すると、本発明の１つまたは複数の実施形態による、セキュア・ゲスト・ストレージのマッピングの一例が概括的に示されている。図４は図３に似ているが、図４の例は、セキュア・ゲストＡとセキュア・ゲストＢとの間のストレージの共用を許さない点が異なる。図３の非セキュア例では、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がともに、同じホスト絶対ページＡＢ２．ＨＡ　３８０にマップされている。図４のセキュア・ゲスト・ストレージ例では、ゲストＡに属するホスト仮想アドレスＡ２．ＨＶ　３４０ａ２がホスト絶対アドレスＡ２．ＨＡ　４９０ａにマップしており、ゲストＢに属するＢ２．ＨＶ　３６０ｂ２がそれ自体のＢ２．ＨＡ　４９０ｂにマップしている。この例では、セキュア・ゲスト間の共用がない。

【００４６】

ディスク上にある間、セキュア・ゲスト・ページは暗号化されている。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呼出し（ＵＶＣ）を発行する。このＵＶＣは、（共用されていない場合に）そのページにセキュア・ページのマークを付けること、（共用されていない場合に）そのページを復号すること、およびそのページを、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、セキュア・インタフェース制御に実行させる。さらに、セキュア・インタフェース制御は、関連するホスト仮想アドレス（例えばＡ３．ＨＶ　３４０ａ３）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。正しいＵＶＣを発行することにハイパーバイザが失敗した場合、ハイパーバイザは、そのセキュア・ゲスト・ページにアクセスしようとしたときに例外を受け取る。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も、同様のＵＶＣが発

行される。このＵＶＣは、（共用されていない場合に）ゲスト・ページを暗号化し、その後、そのゲスト・ページに非セキュア・ページのマークを付け、そのゲスト・ページを、ゾーン・セキュリティ・テーブルに非セキュア・ページとして登録する。

【００４７】

５つの所与のホスト絶対ページＫ、Ｐ、Ｌ、ＭおよびＮを有する一例では、ハイパーバイザがそれらのページをページインするときに、セキュア・インタフェース制御によって、それぞれのホスト絶対ページにセキュア・ページのマークが付けられる。このことは、非セキュア・ゲストおよびハイパーバイザがそれらのページにアクセスすることを防ぐ。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のページ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に登録される。共用ページ、すなわち単一のセキュア・ゲストとハイパーバイザとの間で共用されたページは、ページング中に暗号化もまたは復号もされない。それらのページにはセキュア・ページのマークが付けられていない（それらのページはハイパーバイザによるアクセスを許す）が、それらのページは、単一のセキュア・ゲスト・ドメインとともに、ゾーン・セキュリティ・テーブルに登録される。

【００４８】

本発明の１つまたは複数の実施形態によれば、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たページにアクセスしようとすると、ハイパーバイザが、セキュア・ストレージ・アクセス（ＰＩＣ３Ｄ）例外を受け取る。これを決定するのに追加の変換ステップは必要ない。

【００４９】

１つまたは複数の実施形態によれば、セキュア・エンティティがページにアクセスしようとすると、ハードウェアが、ストレージが実際にその特定のセキュア・ゲストに属していることを確認する追加の変換チェックを実行する。その特定のセキュア・ゲストに属していない場合には、ハイパーバイザに、非セキュア・アクセス（ＰＩＣ３Ｅ）例外が提示される。さらに、変換中のホスト仮想アドレスが、ゾーン・セキュリティ・テーブル内の登録されたホスト・アドレス対のホスト仮想アドレスと一致しない場合には、セキュア・ストレージ違反（‘３Ｆ’ｘ）例外が認識される。ハイパーバイザによる共用を可能にするため、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・ストレージのマークが付けられていないストレージにアクセスすることができる。

【００５０】

次に図５を参照すると、本発明の１つまたは複数の実施形態による、ＤＡＴオペレーションのシステム概略図５００が概括的に示されている。システム概略図５００は、ホスト・プライマリ（primary）仮想アドレス空間５１０およびホスト・ホーム（home）仮想アドレス空間５２０を含み、これらの空間のページが、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５２５参照。点線は、ＤＡＴ変換５２５によるマッピングを表していることに留意されたい）。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用、２つのゲスト間での、それらのホスト仮想アドレスのうちの１つのホスト仮想アドレスの共用、および、ホスト自体による、それらのホスト仮想アドレスのうちの１つのホスト仮想アドレスの共用を示している。この点に関して、ホスト・プライマリ仮想アドレス空間５１０およびホスト・ホーム仮想アドレス空間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２つのホスト仮想アドレス空間はそれぞれ、別個のＡＳＣＥ、すなわちホスト・プライマリＡＳＣＥ（ＨＰＡＳＣＥ）５９１およびホスト・ホームＡＳＣＥ（ＨＨＡＳＣＥ）５９２によってアドレスされる。セキュア・インタフェース制御ストレージ（仮想ストレージと実ストレージの両方）は全てハイパーバイザによって供与されたものであり、それらのストレージにはセキュア・ストレージのマークが付けられていることに留意されたい。供与された後、セキュア・インタフェース制御ストレージには、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・インタフェース制御だけがアクセスすることができ

る。
【００５１】
示されているとおり、ホスト・プライマリ仮想アドレス空間５１０は、ゲストＡ絶対ページＡ１．ＨＶ、ゲストＡ絶対ページＡ２．ＨＶ、ゲストＢ絶対ページＢ１．ＨＶおよびホスト仮想ページＨ３．ＨＶを含む。ホスト・ホーム仮想アドレス空間５２０は、セキュア・インタフェース制御仮想ページ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を含む。
【００５２】
本発明の１つまたは複数の実施形態によれば、全てのセキュア・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・ゲスト構成に属するものとして登録され、さらに、関連するホスト仮想アドレス（例えばＡ１．ＨＶ、Ａ２．ＨＶ、Ｂ１．ＨＶ）が、ホスト・アドレス対の部分として登録される。１つまたは複数の実施形態では、全てのセキュア・ゲスト・ストレージが、ホスト・プライマリ仮想空間でマップされる。さらに、全てのセキュア・インタフェース制御ストレージが、やはりゾーン・セキュリティ・テーブルに、セキュア・インタフェース制御に属するものとして登録され、さらに、全てのセキュア・インタフェース制御ストレージを、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・テーブル内で区別することができる。本発明の１つまたは複数の実施形態によれば、ＵＶ仮想ストレージがホスト・ホーム仮想空間でマップされ、関連するホスト仮想アドレスが、ホスト・アドレス対の部分として登録される。１つまたは複数の実施形態によれば、ＵＶ実ストレージは、関連するホスト仮想マッピングを有しておらず、このことを示すために、（仮想アドレス比較が無効化されていることを示す）ゾーン・セキュリティ・テーブル内のＤＡビットがセットされる。ホスト・ストレージには非セキュア・ストレージのマークが付けられ、さらに、ホスト・ストレージは、ゾーン・セキュリティ・テーブルに、非セキュア・ストレージとして登録される。
【００５３】
したがって、「ゲスト絶対＝ホスト仮想」である場合には、（ＨＰＡＳＣＥ　５９１によって定義された）ハイパーバイザ（ホスト）プライマリＤＡＴテーブルが、ホスト・プライマリ仮想アドレス空間５１０のページを以下のように変換する。ゲストＡ絶対ページＡ１．ＨＶが、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が、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が、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が、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（このページは非セキュア・ページであるためホスト・アドレス対は存在しない）。さらに、（ＨＨＡＳＣＥ　５９２によって定義された）ハイパーバイザ（ホスト）ホームＤＡＴテーブルが、ホスト・ホーム仮想アドレス空間５２０のページを以下のように変換する。セキュア・インタフェース制御仮想ページＵ１．ＨＶが、セキュアＵＶ仮想ページとして定義さ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が、非セキュア・ページとして定義さ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が、非セキュア・ページとして定義さ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は非セキュア・ページであるため、それらのページに関連づけられたホスト・アドレス対は存在しない。
【００５４】
オペレーションの際、セキュア・ゲストが、セキュア・インタフェー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には、ハードウェアによって、ハイパーバイザに、セキュア・ストレージ違反（‘３Ｆ’Ｘ）例外が提示される。非セキュア・ゲストまたはハイパーバイザが、セキュア・ページ（セキュア・インタフェー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には、ハードウェアによって、ハイパーバイザに、セキュア・ストレージ・アクセス（‘３Ｄ’Ｘ）例外が提示

される。あるいは、セキュア・インタフェース制御空間に対して試みられたアクセスに対して、エラー条件を提示することもできる。セキュア・インタフェース制御アクセスに関して、ハードウェアが、セキュア割当ての不整合を検出した場合（例えば、ストレージが、セキュア・インタフェース制御に属するものとしてではなく、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場合、または使用されているホスト・アドレス対と登録された対との間に不整合がある場合）には、チェックが提示される。

【００５５】

言い換えると、ホスト・プライマリ仮想アドレス空間５１０は、（セキュア・ゲストＡに属する）ホスト仮想ページＡ１．ＨＶおよびＡ２．ＨＶ、ならびに（セキュア・ゲストＢに属する）Ｂ１．ＨＶを含み、それらのページはそれぞれ、ホスト絶対Ａ１．ＨＡ、Ａ２．ＨＡおよびＢ１．ＨＡにマップする。さらに、ホスト・プライマリ仮想アドレス空間５１０はホスト（ハイパーバイザ）ページＨ３．ＨＶを含み、このページは、ホスト絶対Ｈ３．ＨＡにマップする。ホスト・ホーム仮想空間５２０は、２つのホスト仮想ページＨ１．ＨＶおよびＨ２．ＨＶを含み、それらのページは、ホスト絶対ページＨ１．ＨＡおよびＨ２．ＨＡにマップする。ホスト・プライマリ仮想アドレス空間５１０とホスト・ホーム仮想アドレス空間５２０はともに単一のホスト絶対アドレス空間５３０にマップする。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・ページにはセキュア・ページのマークが付けられ、図１に示されたゾーン・セキュリティ・テーブル１００に、それらのセキュア・ドメインおよび関連ホスト仮想アドレスとともに登録される。他方、ホスト・ストレージには非セキュアのマークが付けられる。ハイパーバイザがセキュア・ゲストを定義しているとき、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おいて必要とされるセキュア制御ブロックに対して使用するために、セキュア・インタフェース制御にホスト・ストレージを供与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に定義することができ、一例では、特に、ホスト・ホーム仮想空間に定義することができる。図５に戻る。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たセキュア・インタフェース制御ストレージである。その結果として、これらのページにはセキュア・ページのマークが付けられ、これらのページは、図１に示されたゾーン・セキュリティ・テーブル１００に、セキュア・インタ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。それらのページはホスト絶対アドレスとして定義されているため、関連するホスト仮想アドレスは存在せず、そのため、ゾーン・セキュリティ・テーブル１００内のＤＡビットがセットされる。

【００５６】

この変換後のハイパーバイザ（ホスト）絶対アドレス空間５３０の一例が図６に示されている。図６には、本発明の１つまたは複数の実施形態による、セキュア・インタフェー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、ハイパーバイザ（ホスト）絶対アドレス空間６３０を示しており、ハイパーバイザ（ホスト）絶対アドレス空間６３０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）、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）、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に対するもの）、およびホスト絶対ページＡ１．ＨＡセキュア・ゲストＡ（Ａ１．ＨＶに対するもの）を含む。

【００５７】

次に図７を参照すると、本発明の１つまたは複数の実施形態による、インポート・オペレーションのためのプロセス・フロー７００が概括的に示されている。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、そのページを再びセキュアにページインするために、プロセス・フロー７００に示されたイベントなど

の一連のイベントが実行される。プロセス・フロー７００はブロック７０５から始まり、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。このページは例えば無効であるため、ハードウェアは、プログラム割込みコード（program-interruption-code）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７１５参照）。これを受けて、ハイパーバイザは、このゲスト・ページに対する使用可能な非セキュア・ホスト絶対ページを識別し（ブロック７２０参照）、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７２５参照）。

【００５８】

次いで、ブロック７３０で、このホスト絶対ページを、（ホスト仮想アドレスに基づいて）適切なホストＤＡＴテーブルにマップする。次いで、ブロック７３５で、ハイパーバイザ・ホストが、セキュア・ゲストを再びディスパッチする。ブロック７４０で、セキュア・ゲストが、ゲスト・セキュア・ページに再びアクセスする。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・セキュリティ・テーブル１００内でセキュアのマークが付けられていないため、ブロック７４５で、ハードウェアは、ハイパーバイザに、非セキュア・ストレージ例外（ＰＩＣ３Ｅ）を提示する。このＰＩＣ３Ｅは、必要なインポートが発行されるまで、ゲストがこのセキュア・ページにアクセスすることを防ぐ。次に、プロセス・フロー７００は、図８に接続された「Ａ」に進む。

【００５９】

次に図８を参照すると、本発明の１つまたは複数の実施形態による、インポート・オペレーションを実行するためのプロセス・フロー８００が概括的に示されている。行儀のよい（well-behaved）ハイパーバイザ（例えば期待されるやり方でエラーなく実行するハイパーバイザ）は、このＰＩＣ３Ｅに応答して、インポートＵＶＣを発行する（ブロック８０５参照）。この時点で、インポートするページには、非セキュアのマークが付けられており、このページには、ハイパーバイザ、他の非セキュア・エンティティおよびセキュア・インタフェース制御だけがアクセスできることに留意されたい。セキュア・ゲストはこのページにアクセスできない。

【００６０】

このインポートＵＶＣの一部として、セキュア・インタフェース制御の役目を果たす信頼できるファームウェアが、このページがセキュア・インタフェース制御によって既にロックされているかどうかを知るためのチェックを実行する（判断ブロック８１０参照）。ロックされている場合、プロセス・フロー８００はブロック８２０に進む。ブロック８２０で、ハイパーバイザに「使用中（busy）」リターン・コードが返され、ハイパーバイザは、それに応答して遅延し（ブロック８２５参照）、インポートＵＶＣを再発行する（プロセス・フロー８００はブロック８０５に戻る）。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は判断ブロック８２２に進む。

【００６１】

判断ブロック８２２で、セキュア・インタフェース制御は、そのページが、非セキュア・ハイパーバイザによって共用されているページであるかどうかを知るためのチェックを実行する。そのページが共用されている場合には（プロセス・フロー８００は判断ブロック８２４に進み）、セキュア・インタフェース制御が、ホスト絶対アドレスを、関連セキュア・ゲスト・ドメイン、ホスト仮想アドレスとともに、ゾーン・セキュリティ・テーブルに、共用されているとして、登録する。このページは、非セキュアのマークが付けられたままである。これによってインポートＵＶＣは完了し、このページは、この時点で、ゲストによるアクセスに対して使用可能である。処理は進んで、ハイパーバイザがゲストを再びディスパッチし（ブロック８３０）、セキュア・ゲストは、成功のうちにこのページにアクセスする（ブロック８３５）。

【００６２】

インポートするホスト仮想ページがハイパーバイザによって共用されていない場合、（

プロセス・フロー８００はブロック８４０に進み、）セキュア・インタフェース制御が、そのページにセキュアのマークを付け、もはやハイパーバイザがそのページにアクセスできないようにする。ブロック８４５で、セキュア・インタフェース制御はそのページをロックし、他のＵＶＣがページ・ステータスを変更できないようにする。ロックをセットした後、（ブロック８５０で、）セキュア・インタフェース制御は、ゲスト・ページが暗号化される間にゲスト・ページの内容が変化しなかったことを確認する。ゲスト・ページの内容が変化した場合には、ハイパーバイザにエラー・リターン・コードが返され、変化しなかった場合には、セキュア・インタフェース制御がセキュア・ページを復号する。

【００６３】

ブロック８５５で、セキュア・インタフェース制御は、ページのロックを解除して、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、セキュアとして登録し、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づけて、ホスト・アドレスＨＶ→ＨＡ対を完成させる。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。

【００６４】

次に図９を参照すると、本発明の１つまたは複数の実施形態による、供与メモリ・オペレーションに関するプロセス・フロー９００が概括的に示されている。プロセス・フロー９００はブロック９０５から始まり、ブロック９０５で、ハイパーバイザが、セキュア・インタフェース制御に照会ＵＶＣを発行する。ブロック９１０で、セキュア・インタフェース制御は、データ（例えば照会ＵＶＣ）を返す。このデータは、必要なベース・ゾーン特定（zone-specific）ホスト絶対ストレージの量、必要なベース・セキュア・ゲスト・ドメイン特定（secure-guest-domain-specific）ホスト絶対ストレージの量、ＭＢごとに必要な可変セキュア・ゲスト・ドメイン特定（secure-guest-domain-specific）ホスト仮想ストレージの量、もしくは必要なベース・セキュア・ゲストＣＰＵ特定（secure-guest-CPU-specific）ホスト絶対ストレージの量、またはこれらの組合せを含むことができる。

【００６５】

ブロック９１５で、ハイパーバイザが、ベース・ホスト絶対ゾーン特定ストレージを（例えば照会ＵＶＣによって返されたサイズに基づいて）予約する。ブロック９２０で、ハイパーバイザは、セキュア・インタフェース制御に初期化を発行する。この点に関して、ハイパーバイザは、ゾーン全体に対するセキュア・ゲスト構成間の調整に必要なＵＶ制御ブロックのための供与されたストレージ（以後、供与ストレージ）を提供する初期化ＵＶＣを発行することができる。この初期化ＵＶＣは、ベース・ゾーン特定ストレージ起点を指定する。

【００６６】

ブロック９２５で、セキュア・インタフェース制御は、供与ストレージをＵＶに登録し、供与ストレージにセキュアのマークを付けることにより、初期化（例えば初期化ＵＶＣ）を実施する。この初期化ＵＶＣに関して、セキュア・インタフェース制御は、供与ストレージにセキュアのマークを付け、その供与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、その供与ストレージを、ＵＶが使用するために、ゾーン・セキュリティ・テーブルに、固有のセキュア・ドメインとともに、関連セキュア・ゲスト・ドメインは含めずに、関連ホスト仮想アドレス対を持たないものとして、登録することができる。

【００６７】

ブロック９３０で、ハイパーバイザは、ストレージ（例えばベースおよび可変セキュア・ゲスト・ドメイン特定ストレージ）を予約する。例えば、ハイパーバイザは、ベースおよび（例えばセキュア・ゲスト・ドメイン・ストレージのサイズに基づく）可変セキュア・ゲスト・ドメイン特定ストレージ（例えば照会ＵＶＣによって返されたサイズ）を予約する。ブロック９３５で、ハイパーバイザは、構成生成（create configuration）をセキュア・インタフェース制御に発行する。この点に関して、ハイパーバイザは、ベースおよび可変セキュア・ゲスト・ドメイン特定ストレージ起点を指定するセキュア・ゲスト構成

生成ＵＶＣを発行することができる。さらに、このセキュア・ゲスト構成生成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なＵＶ制御ブロックのための供与ストレージを提供する。

【００６８】

ブロック９４０で、セキュア・インタフェース制御は、構成生成（例えばセキュア・ゲスト構成生成ＵＶＣ）を実施する。このセキュア・ゲスト構成生成ＵＶＣに関して、セキュア・インタフェース制御は、供与ストレージにセキュアのマークを付け、この供与ストレージを、ＵＶが使用するために、ゾーン・セキュリティ・テーブルに登録し、この供与ストレージを、関連セキュア・ゲスト・ドメインとともに登録することができる。ベース（ホスト絶対）供与ストレージは、関連ホスト仮想アドレス対を持たないものとして登録される。可変（ホスト仮想）供与ストレージは、関連ホスト仮想アドレス対とともに登録される。

【００６９】

ブロック９４５で、ハイパーバイザが、ベース・セキュア・ゲストＣＰＵ特定ストレージ（例えば照会ＵＶによって返されたサイズ）を予約する。ブロック９５０で、ハイパーバイザはストレージ起点を指定する。例えば、ハイパーバイザは、ベース・セキュア・ゲストＣＰＵ特定ストレージ起点を指定するセキュア・ゲストＣＰＵ生成を、ＵＶに発行する。ブロック９５５で、セキュア・インタフェース制御が、ＣＰＵ生成（例えばセキュア・ゲストＣＰＵ生成ＵＶＣ）を実施する。このセキュア・ゲストＣＰＵ生成ＵＶＣに関して、セキュア・インタフェース制御は、供与ストレージにセキュアのマークを付け、その供与ストレージを、ＵＶが使用するために、ゾーン・セキュリティ・テーブルに、関連セキュア・ゲスト・ドメインなしで、関連ホスト仮想アドレス対を持たないものとして、登録することができる。

【００７０】

次に図１０を参照すると、本発明の１つまたは複数の実施形態による、非セキュア・ハイパーバイザ・ページからセキュア・インタフェース制御のセキュア・ページへの移行に関するプロセス・フロー１０００が概括的に示されている。プロセス・フロー１０００には、３つのハイパーバイザ・ページ（例えば非セキュア・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）が示されている。

【００７１】

ハイパーバイザ（非セキュア）ページＡ、ＢおよびＣには、（ハイパーバイザを含む）非セキュア・エンティティがアクセスすることができる。さらに、ハイパーバイザ（非セキュア）ページＡ、ＢおよびＣには、非セキュア（ＮＳ）のマークが付けられており、ハイパーバイザ（非セキュア）ページＡ、ＢおよびＣは、ゾーン・セキュリティ・テーブル（例えば図１に示されたゾーン・セキュリティ・テーブル１００）に、非セキュアおよび非共用として登録されている。矢印１００５において、初期化ＵＶＣが発行される。この初期化ＵＶＣは、ゲスト・ページＡを、ゾーン全体に関連したセキュア・インタフェース制御実ストレージ・ページ（ＵＶ２）１０１０に移行させる。セキュア・インタフェース制御実ストレージ１０１０にセキュアのマークを付けることができ、セキュア・インタフェース制御実ストレージ１０１０を、ゾーン・セキュリティ・テーブル（例えば図１に示されたゾーン・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－ホスト絶対（ＨＶ→ＨＡ）マッピングなしで登録することができる。その代わりに、セキュア・インタフェース制御実ストレージ１０１０は、固有のＵＶ２セキュア・ドメインとともに登録され、ＤＡビットが１にセットされる。セキュア・インタフェース制御実ストレージ１０１０には、セキュア・インタフェース制御が実ストレージとしてアクセスすることができることに留意されたい。

【００７２】

矢印１０２５において、ハイパーバイザ（非セキュア）ページＢから、ＳＧ構成生成ＵＶＣまたはＳＧ　ＣＰＵ生成ＵＶＣが発行される。このＵＶＣは、このページを、セキュ

ア・ゲスト・ドメインに関連したセキュア・インタフェース制御実ストレージ（ＵＶＳ）１０３０に移行させる。セキュア・インタフェース制御実ストレージ１０３０にセキュアのマークを付けることができ、セキュア・インタフェース制御実ストレージ１０３０を、ゾーン・セキュリティ・テーブル（例えば図１に示されたゾーン・セキュリティ・テーブル１００）に、ＵＶとして、関連セキュア・ゲスト・ドメインとともに、ハイパーバイザ－ホスト絶対（ＨＶ→ＨＡ）マッピングなし（すなわちＤＡビット＝１）で登録することができる。セキュア・インタフェース制御実ストレージ１０３０には、セキュア・ゲスト・ドメインに代わって、セキュア・インタフェース制御が実ストレージとしてアクセスすることができることに留意されたい。

【００７３】

矢印１０４５において、ハイパーバイザ（非セキュア）ページＣから、ＳＧ構成生成ＵＶＣが発行される。このＵＶＣは、このページを、セキュア・ゲスト・ドメインに関連したセキュア・インタフェース制御仮想ストレージ（ＵＶＶ）１０５０に移行させる。セキュア・インタフェース制御仮想ストレージ１０５０にセキュアのマークを付けることができ、セキュア・インタフェース制御仮想ストレージ１０５０を、ゾーン・セキュリティ・テーブル（例えば図１に示されたゾーン・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－ホスト絶対（ＨＶ→ＨＡ）マッピングとともに登録することができる。セキュア・インタフェース制御仮想ストレージ１０５０には、セキュア・ゲスト・ドメインに代わって、ＵＶ仮想ストレージとしてアクセスすることができることに留意されたい。

【００７４】

次に図１１を参照すると、１つまたは複数の実施形態による、プログラムまたはセキュア・インタフェース制御によってなされたセキュア・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・インタフェース制御ストレージにアクセスしようとしており、そのアクセスのセキュリティをハードウェアが確認することを可能にするために、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。プロセス・フロー１１００は、セキュア・インタフェース制御によるストレージ・アクセスのこのタグ付けを示している。プロセス・フロー１１００はブロック１１１０から始まり、ブロック１１１０で、セキュア・インタフェース制御は、セキュア・インタフェース制御がセキュア・インタフェース制御ストレージにアクセスしているかどうかを判定する。

【００７５】

このアクセスが、セキュア・インタフェース制御ストレージへのアクセスでない場合、プロセス・フロー１１００は、（いいえの矢印によって示されているように）判断ブロック１１１２に進む。判断ブロック１１１２で、セキュア・インタフェース制御は、セキュア・インタフェース制御がセキュア・ゲスト・ストレージにアクセスし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は、非セキュア・アクセスのためのデフォルト設定を使用する（図１２のプロセス・フロー１２００に接続された）「Ｂ」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は判断ブロック１１１３に進み、判断ブロック１１１３で、セキュア・インタフェース制御は、デフォルト・セキュア・ゲスト・ドメインが使用されているどうかを判定する。はいの場合、プロセス・フロー１１００は、セキュア・ゲスト・アクセスのためのデフォルト設定を使用する（図１２のプロセス・フロー１２００に接続された）「Ｂ」に進む。いいえの場合、プロセス・フロー１１００はブロック１１１４に進む。ブロック１１１４で、適切なセキュア・ゲスト・ドメインをＳＧセキュア・ドメイン・レジスタにロードする（プロセス・フロー１１００は、図１２のプロセス・フロー１２００に接続された「Ｂ」に進む）。

【００７６】

このアクセスが、セキュア・インタフェース制御ストレージへのアクセスである場合、プロセス・フロー１１００は、（はいの矢印によって示されているように）ブロック１１

２０に進む。ブロック１１２０で、そのアクセスにセキュアＵＶのタグを付ける（例えば、そのアクセスはＵＶセキュア・ドメイン・レジスタを使用する）。

【００７７】

プロセス・フロー１１００は次いで判断ブロック１１３０に進み、判断ブロック１１３０で、セキュア・インタフェース制御は、このアクセスが、ＵＶＶ空間（例えばＳＧ構成可変テーブル（SG-Config Variable Table））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は、（はいの矢印によって示されているように）ブロック１１３４に進む。ブロック１１３４で、そのアクセスに仮想アクセスのタグを付ける。ブロック１１３６で、適用可能なセキュア・ゲスト・ドメインをＵＶセキュア・ドメイン・レジスタにロードする。ブロック１１３８では、ＤＡＴ変換およびストレージ・アクセスが始まる準備ができている。判断ブロック１１３０に戻る。このアクセスが、ＵＶＶ空間へのアクセスではない場合、プロセス・フロー１１００は、（いいえの矢印によって示されているように）ブロック１１４０に進む。ブロック１１４０で、そのアクセスに実アクセスのタグを付ける。

【００７８】

判断ブロック１１５０で、セキュア・インタフェース制御は、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は、（はいの矢印によって示されているように）ブロック１１３６に進む。このアクセスがＵＶＳ空間へのアクセスではない場合、プロセス・フロー１１００は、（いいえの矢印によって示されているように）ブロック１１７０に進む。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ということになる。ブロック１１７０で、固有のＵＶ２セキュア・ドメインをＵＶセキュア・ドメイン・レジスタにロードする。

【００７９】

図１２は、本発明の１つまたは複数の実施形態によるプロセス・フロー１２００を示している。ゲストがディスパッチされると、ＳＩＥ　Ｅｎｔｒｙファームウェアは、ゲストが動作していること（例えばゲスト・モードがアクティブであること）をハードウェアに示すことができ、その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、関連セキュア・ゲスト・ドメインをハードウェアに（例えばＳＧセキュア・ドメイン・レジスタに）ロードすることができる。プログラムがストレージにアクセスしているとき、ハードウェアは、そのアクセスの時点におけるプログラムの現在の状態に基づいて、そのアクセスにタグを付けることができる。図１２は、プロセス・フロー１２００の中のこのプロセスの一例を示している。ブロック１２０５で、ハードウェアは、機械が現在、ゲスト・モードで動作しているかどうかを判定することができ、ゲスト・モードで動作していない場合には、ブロック１２１０で、そのアクセスに、ホスト・アクセスであるとのタグを付けることができ、ブロック１２１５で、そのアクセスに、非セキュア・アクセスであるとのタグを付けることができる。ブロック１２０５で、機械がゲスト・モードで動作している場合、ブロック１２２０で、そのアクセスに、ゲスト・アクセスのタグを付けることができ、さらに、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判定することができる。ゲストがセキュアでない場合、ブロック１２１５で、そのアクセスに、非セキュアのタグを付けることができる。ゲストがセキュアである場合、ブロック１２３０で、ハードウェアは、そのゲストに、セキュアのタグを付けることができ、それによって、そのセキュア・ゲストを、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・ドメイン・レジスタに関連づけることができる。非セキュア・ゲストとセキュア・ゲストの両方に関して、ブロック１２３５で、ＤＡＴステータスをチェックすることができる。ＤＡＴがオフの場合、ブロック１２４０で、そのアクセスに、実アクセスのタグを付けることができる。ＤＡＴがオンの場合、ブロック１２４５で、そのアクセスに、仮想アクセスのタグを付けることができる。ＤＡＴがオフの場合に、ブロック１２４０で、そのアクセスに、実アクセスのタグを付けた後、またはＤＡＴがオンの場合に、ブロック１２４５で、そのアクセスに、仮想アクセス

のタグを付けた後に、ブロック１２５０において、ハードウェアは、変換を開始し、ストレージにアクセスする準備ができている。これについては図１３でさらに説明する。

【００８０】

図１３は、本発明の１つまたは複数の実施形態による、セキュア・アクセスと非セキュア・アクセスの両方をサポートするためにプロセス・フロー１３００においてハードウェアによって実行される変換の一例を示している。ブロック１３０５で、ハードウェアは、そのアクセスにゲスト変換のタグが付けられているかどうかを判定することができ、ゲスト変換のタグが付けられており、ブロック１３１０で、そのアクセスが仮想アクセスである場合、ブロック１３１５で、ゲストＤＡＴを実行することができる。ゲストＤＡＴ変換の間、ゲストＤＡＴテーブルのためのネストされた介在フェッチが存在しうる。それらのテーブル・フェッチに、ゲスト実フェッチのタグを付けることができ、元の変換にセキュアのタグが付けられた場合には、それらのテーブル・フェッチにセキュア・フェッチのタグを付けることができる。それらのテーブル・フェッチはさらに、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でゲスト仮想アクセスのタグが付けられたアクセスに対して、ゲストＤＡＴが実行された後、およびブロック１３１０でゲスト実アクセスのタグが付けられたアクセス（仮想＝いいえ）に対して、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・オフセットを適用することができる。このゲスト変換プロセスが完了したら、ブロック１３２５で、結果として生じたアドレスに、ホスト仮想アドレスのタグを付けることができ、元のゲスト変換にセキュアのタグが付けられた場合には、結果として生じたアドレスに、セキュア・アドレスのタグを付けることができる。ホスト仮想アクセスのタグが付けられた任意のアクセスに対して、プロセス１３００を続けることができる。ブロック１３０５で、元のアクセスがホスト・アクセスであり（ゲスト＝いいえ）、ブロック１３３０で、元のアクセスが仮想アクセスである場合、ブロック１３３５で、ホストＤＡＴを実行することができる。ブロック１３３５で、ホスト・テーブル・フェッチに、非セキュア・フェッチのマークを付けることができる。ブロック１３３５でホストＤＡＴを実行した後、またはブロック１３３０で、元のホスト・アクセスに実アクセスのタグが付けられた場合（仮想＝いいえ）、ブロック１３４０で、ホスト・プレフィックス変換を適用することができる。ブロック１３４５で、結果として生じたアドレスはホスト絶対アドレスでありうる。

【００８１】

図１４は、本発明の１つまたは複数の実施形態による、プロセス・フロー１４００においてハードウェアによって実行することができるセキュア・ストレージ保護付きのＤＡＴ変換の一例を示している。図１３のブロック１３４５から続いて、ブロック１４０５で、セキュアＵＶアクセスが識別された場合、ハードウェアは、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かどうかを確認することができ、セキュアＵＶストレージとして登録されていない場合には、ブロック１４１５で、エラーを提示する。ＵＶストレージにアクセスするときには、セキュア・インタフェース制御によってセキュアＵＶアクセスを実行することができる。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、保護チェックを続けることができ、（セキュアＵＶアクセスを実行する前にセキュア・インタフェース制御によってセットアップされた）ＵＶセキュア・ドメイン・レジスタを、処理が続く場合にブロック１４２０で実行されるドメイン・チェックのための指定されたセキュア・ドメインとして使用することができることを除いて、この保護チェックは、任意のセキュア・アクセスに対して実行することができる。さらに、ブロック１４２５でＵＶアクセスに対して検出された違反（入口点Ｄ）を、ブロック１４３０で、エラーとして提示することができ、ブロック１４２５でのセキュア・ゲスト違反（セキュアＵＶ＝いいえ）に対しては、ブロック１４３５で、ハイパーバイザに例外を提示することができる。

【００８２】

ブロック１４０５でセキュアＵＶアクセスのタグが付けられていなかったアクセスについて、ハードウェアは、ブロック１４４０で、そのアクセスがセキュア・ゲスト・アクセ

スであるかどうかを判定し、そのアクセスがセキュア・ゲスト・アクセスではなく、ブロック１４４５で、そのページにセキュアのマークが付けられている場合、ブロック１４３５で、ハイパーバイザに例外を提示することができる。一方、ブロック１４４０で、そのアクセスがセキュア・ゲスト・アクセスでなく、ブロック１４４５で、そのページにセキュアのマークが付けられていない場合、ブロック１４５０で、変換は成功となる。

【００８３】

ブロック１４４０で、そのアクセスがセキュア・ゲスト・アクセスである場合、または、そのアクセスが、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、ハードウェアは、ブロック１４２０で、そのストレージが、そのアクセスに関連したセキュア・エンティティに登録されていることを確かめるためのチェックを実行することができる。このアクセスがセキュアＵＶアクセスである場合、（アクセスされているセキュアＵＶストレージに基づいてセキュア・インタフェース制御によってロードされた）ＵＶセキュア・ドメイン・レジスタから、指定されたセキュア・ドメインを取得することができ、セキュア・ゲスト・アクセスに関して、指定されたセキュア・ドメインは、（セキュア・エンティティがディスパッチされたときにロードされた）ＳＧセキュア・ドメイン・レジスタから取得される。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、ゾーン・セキュリティ・テーブル・インタフェース１４８５に関する図１５に示された副プロセス１５００が実行される。

【００８４】

副プロセス１５００では、ブロック１５１０で、複数のセキュア・ドメインにわたる仮想アドレス共用が許されているかどうかを判定するためのチェックを実行する。このチェックは、ゾーンまたはパーティションに関連したレジスタ値に基づいて実行することができる。ブロック１５２０で、複数のセキュア・ドメインにわたる共用が許されており、現在のセキュア・ドメインによる共用が許されている場合、ブロック１５３０で、仮想アドレス・チェッキングが無効化されているかどうかのチェックを実行することができる。現在のセキュア・ドメインによって共用が許されているかどうかのチェックは、ゾーン・セキュリティ・テーブル内でのセキュア・ドメインに対するレジスタ・アクセスまたはテーブル・ルックアップによって実行することができ、これは、このホスト絶対ページに対して特定とすることができる。仮想アドレス・チェッキングが無効化されているかどうかのチェックは、仮想アドレス比較無効化状態（ＤＡ）を調べることによって実行することができ、マークが付けられたページ（例えばＤＡ＝１）は、仮想アドレス・チェッキングの無効化に帰着する。ブロック１５１０で、複数のセキュア・ドメインにわたる仮想アドレス共用が許されていない場合、またはブロック１５２０で、現在のセキュア・ドメインによる共用が許されていない場合、またはブロック１５３０で、仮想アドレス・チェッキングが無効化されていない（例えばＤＡ＝０）場合、ブロック１４３５で、ハイパーバイザに例外を提示することができる。あるいは、ブロック１５２０で、仮想アドレス・チェッキングが無効化されていない（ＤＡ＝０）場合、セキュア・インタフェース制御は、このホスト絶対ページおよびセキュア・ゲスト・ドメインについて、登録されたホスト仮想アドレスをチェックすることができ、アクセス・ホスト・アドレス対が、登録されたホスト・アドレス対と一致した場合、ブロック１４５０で、変換は成功のうちに完了となり、これらの対が一致しなかった場合、ブロック１４３５で、ハイパーバイザに例外が提示されることになる。一方、ブロック１５３０で、仮想アドレス・チェッキングが無効化されている場合、ブロック１４５０で、変換は成功し、副プロセス１５００は終了することができる。

【００８５】

図１４のプロセス１４００に戻る。ブロック１４４０およびブロック１４１０におけるストレージに対するセキュア・アクセスであって、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セキュア・アクセス関して、ブロック１４５５で、仮想アドレス・チェックが無効化されており、すなわちＤＡビット＝１であり、かつ、ブロック１

４６０でそのアクセスが実アクセスである場合、ブロック１４５０で、変換は完了となる。しかしながら、ブロック１４５５ではＤＡビット＝１だが、ブロック１４６０で、そのアクセスが仮想アクセスであり（実アクセス＝いいえ）、ブロック１４６５で、仮想アドレス（ＶＡ）共用が許されている場合には、ブロック１４５０で、変換は完了となる。しかしながら、ブロック１４５５でＤＡビット＝１、ブロック１４６０で、そのアクセスが仮想アクセスであり（実アクセス＝いいえ）、ブロック１４６５で、ＶＡ共用が許されていない場合には、２つのオプションのうちの一方のオプションを実行することができる。オプション１では、続いて、ブロック１４７０で、ホスト仮想－ホスト絶対の一致が判定され、オプション２では、ブロック１４２５でのセキュアＵＶアクセスに関して、ブロック１４３０でエラーが提示され、ブロック１４２５でのセキュア・ゲスト・アクセス（セキュアＵＶアクセス＝いいえ）に関して、ブロック１４３５で、ハイパーバイザに例外が提示される。ブロック１４５５でＤＡビット＝０、ブロック１４７５で、そのアクセスが仮想アクセスである場合、ハードウェアは、ブロック１４７０で、そのアクセスのホスト仮想－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ているマッピングと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、変換は成功のうちに完了となる。ブロック１４７０で、このマッピングが一致しない場合、ブロック１４２５でのセキュアＵＶがアクセスに関しては、ブロック１４３０でエラーが提示され、ブロック１４２５でのセキュア・ゲスト・アクセス（セキュアＵＶアクセス＝いいえ）に関しては、ブロック１４３５で、ハイパーバイザに例外が提示される。ブロック１４７５で、ＤＡビット＝０であり、そのアクセスが実アクセスである（仮想アクセス＝いいえ）場合、ブロック１４２５でのセキュアＵＶがアクセスに関しては、ブロック１４３０でエラーが提示され、ブロック１４２５でのセキュア・ゲスト・アクセス（セキュアＵＶアクセス＝いいえ）に関しては、ブロック１４３５で、ハイパーバイザに例外が提示され（オプション２）、あるいは、ブロック１４５０で、変換は成功のうちに完了となる（オプション１）。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でそのページにセキュア・ページのマークが付けられているかどうかを知るためのチェックを実行することができる。そのページがセキュア・ページである場合、ブロック１４３５で、ハイパーバイザに例外を提示することができ、そのページにセキュア・ページのマークが付けられていない場合、ブロック１４５０で、変換は成功となる。

【００８６】

ゾーン・セキュリティ・テーブル・インタフェースによって、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を集合的に管理することができる１４８５。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、同じゾーンに関連づけられたゾーン・セキュリティ・テーブルとインタフェースすることができる。同様に、図１５のブロック１５１０、１５２０および１５３０は、さまざまなアクセスを管理するために、同じゾーンに関連づけられたゾーン・セキュリティ・テーブルとインタフェースすることができる。

【００８７】

さらなる例として、図１６および１７は、マッピング・プロセスのオプションを示している。前述のとおり、セキュア・ドメインまたはセキュア・インタフェース制御からのそれぞれのメモリ・アクセスに、セキュア・ドメイン、ホスト・アドレス対およびＤＡマーク付けのタグを付けることができる。ホスト・アドレス対は、仮想アドレスおよび関連絶対アドレスを含むことができる。それぞれのエンティティ、例えばセキュア・コンテナまたはＶＭは、それ自体のセキュア・ドメインＩＤを有することができる。以下の例では、いくつかの用語が定義される。すなわち、Ｖ＝メモリ・アクセスの仮想アドレス。Ａ＝メモリ・アクセスの絶対アドレス。Ｄ＝セキュア・ドメインＩＤ。ＤＡ＝仮想アドレス比較無効化ビット。通常のオペレーティング・セキュア・ドメインについては、アクセス時にページインされ確認されたときに全てのメモリ・アクセスを登録することができる。一例として、セキュア・ドメインＸが、メモリ内に３つのページを所有しているとする。それらのページは、以下の登録されたホスト・アドレス対および関連情報を有する。すなわち

、１つのページについては（Ｖ１ｘ，Ａ１ｘ）、ＤＡ＝０（共用なし）、Ｄ＝Ｘ、別のページについては（Ｖ２ｘ，Ａ２ｘ）、ＤＡ＝０（共用なし）、Ｄ＝Ｘ、第３のページについては（Ｖ３ｘ，Ａ３ｘ）、ＤＡ＝０（共用なし）、Ｄ＝Ｘである。これらのホスト・アドレス対およびセキュア・ゲスト・ドメインが、例えば図１のゾーン・セキュリティ・テーブル１００の中で一致していない場合には、これらのページへのアクセスが許されないことがある。別のセキュア・ドメインＹが動作することもでき、このセキュア・ドメインは、以下の２つのホスト・アドレス対および関連情報とともに登録された２つのページをメモリ内に所有することができる。すなわち、１つのページについては（Ｖ１ｙ，Ａ１ｙ）、ＤＡ＝０（共用なし）、Ｄ＝Ｙ、別のページについては（Ｖ２ｙ，Ａ２ｙ）、ＤＡ＝０（共用なし）、Ｄ＝Ｙである。このアクセスに関するホスト・アドレス対およびセキュア・ゲスト・ドメインが、このページに関して登録されたホスト・アドレス対およびセキュア・ゲスト・ドメインと一致していない場合には、これらのページへのアクセスが許されないことがある。セキュア・ドメインＸおよびＹはともに、対応する絶対アドレスが固有である限り、同じ仮想アドレス値によってマップされたページを有することができる。例えば、これらの全てのページでＤＡ＝０であるため、Ｖ１ｘとＶ２ｙは等しくてもよいが、Ａ１ｘは、Ａ２ｘ、Ａ３ｘ、Ａ１ｙまたはＡ２ｙのいずれとも異なっていなければならない。仮想アドレスとともに登録された絶対ページの共用を可能にするため、または（仮想アクセスではなく）絶対アクセスを可能にするために、図１のＤＡビット１４０がセットされる。

【００８８】

以下の例は、２つのセキュア・ドメイン間のページの共用を示している。上記のものと同じ２つのセキュア・ドメインＸおよびＹに関して、Ａ１ｘとＡ１ｙとを共用することができ、そのためＡ１ｘ＝Ａ１ｙ＝Ａ１である。セキュア・エンティティＸおよびＹに対する登録されたホスト・アドレス対および関連情報は、（Ｖ１ｘ，Ａ１）、ＤＡ＝１（共用ページ）、Ｄ＝Ｘ、（Ｖ２ｘ，Ａ２ｘ）、ＤＡ＝０（共用なし）、Ｄ＝Ｘ、（Ｖ３ｘ，Ａ３ｘ）、ＤＡ＝０（共用なし）、Ｄ＝Ｘ、（Ｖ１ｙ，Ａ１）、ＤＡ＝１（共用ページ）、Ｄ＝Ｙ、および（Ｖ２ｙ，Ａ２ｙ）、ＤＡ＝０（共用なし）、Ｄ＝Ｙとなりうる。共用絶対ページＡ１へのアクセスは、ドメインＸおよびＹに対してのみ許されていることがあり、一例では、ＤＡ＝１であるため、仮想アドレスに対する一致チェックが飛ばされる。別のケースでは、それぞれのドメインＸおよびＹが、それぞれの共用ページに対して別個の（固有のまたは一致した）仮想アドレスを登録することができる。複数のセキュア・ドメイン間のページ・リクエストの共用は、１つまたは複数のセキュア・ドメインによって開始し、残りのドメインによって確認することができる。

【００８９】

別の例として、セキュア・インタフェース制御は、セキュアＵＶページが、仮想アドレス・チェックが実行されないことを示すＤＡ＝１とともに登録されている場合、絶対アドレスを使用してそのページにアクセスすることができる。このケースでは、このページが、ホスト仮想アドレスを問題としないホスト・アドレス対（－，Ａ１ａｓ）、ＤＡ＝１およびＤ＝ＡＳ（aux-secure。これは、そのページが、セキュア・インタフェース制御に属していることを示す）とともに登録されている。セキュア・インタフェース制御は、このページへのアクセスがセキュア・インタフェース制御だけに許されていることを保証するために、セキュア・ドメインを比較することができる。ＤＡ＝１であるため、仮想アドレス・チェックは実行されない。

【００９０】

図１６は、２つのセキュア・ドメイン間のページの共用の実施態様の一例を、ＤＡ＝１（共用）を有する一例として示している。この例では、仮想アドレス空間１６０２から絶対アドレス空間１６０４へのホスト・アドレス対が（Ｖ１，Ａ２）、（Ｖ２，Ａ１）、（Ｖ３，Ａ２）、（Ｖ４，Ａ３）、（Ｖ５，Ａ２）である。３つの異なる仮想アドレス間で絶対アドレスＡ２を共用することができる１６０６。Ｖ１およびＶ５は、同じセキュア・ゲスト・ドメイン１６０８からのものであり、Ｖ３は、別のセキュア・ドメイン１６１０

からのものである。仮想アドレス空間１６０２から絶対アドレス空間１６０４へのこの変換は、信頼できないハイパーバイザまたはＯＳによって所有されうる。このような共用は、ある種の状況下では有益となりうる。しかしながら、ドメイン１６０８、１６１０間の同じ絶対アドレスＡ２の共用は、ドメイン１６０８、１６１０がともに、共用されている１６０６同じ絶対アドレスＡ２にアクセスすることができる場合に、セキュリティ上の問題を引き起こしうる。

【００９１】

本発明の１つまたは複数の実施形態によれば、図１７は、図１６の例を変更したものを、ＤＡ＝１（共用）を有する別の例として示しており、ホスト・アドレス対は、（Ｖ１，Ａ２）、（Ｖ２，Ａ１）、（Ｖ４，Ａ３）、（Ｖ５，Ａ２）である。注目すべきは、アドレス変換対（Ｖ３，Ａ２）が、仮想アドレス空間１６０２から絶対アドレス空間１７０４へのマッピングにおいて直接には使用可能でないことである。セキュア・コンテナ／ＶＭに対してページの共用が許されないことがある。（Ｖ３，Ａ２）は（Ｖ３，Ａ２’）に変更されており、このことは、それぞれのコンテナ／ＶＭに対して１つの固有のコピーを有するために物理Ａ２ページを複製することを含みうる。したがって、ドメイン１６０８、１６１０によるアクセスはともに、Ａ２の別個のコピーを見ることができるが、Ａ２の内容を変更しようとする試みはいずれも、異なる絶対ページＡ２、Ａ２’上で実行される。図１のＤＡビット１４０を使用して、２つの異なる仮想アドレス（例えばドメイン１６０８のＶ１およびドメイン１６１０のＶ３）を使用している２つの異なるセキュア・ドメイン１６０８、１６１０間での１つの絶対ページの共用を可能にすることができる。

【００９２】

次に図１８を参照すると、本発明の１つまたは複数の実施形態による、複数のセキュリティ・ドメインにわたってセキュア・メモリを共用するためのプロセス・フロー１８００が概括的に示されている。ブロック１８０５で、コンピュータ・システムのセキュア・インタフェース制御は、メモリのセキュア・ページに対するセキュア・アクセス・リクエストを受け取ることができる。ブロック１８１０で、セキュア・インタフェース制御は、そのセキュア・ページに関連づけられた仮想アドレス（例えばＤＡビット１４０）比較無効化状態をチェックすることができる。ブロック１８１５で、セキュア・インタフェース制御は、複数の仮想アドレスから同じ絶対アドレスへのマッピングをサポートするために、仮想アドレス比較無効化状態がセットされていること（例えばＤＡ＝１であること）に基づいて、セキュア・ページにアクセスする際の仮想アドレス・チェックを、セキュア・ページに対して無効化することができる。セキュア・アクセス・リクエストを出したエンティティの許可ステータス、および仮想アドレス比較無効化状態がセットされていること（例えばＤＡ＝１であること）に基づいて、仮想アドレスが指定されていないセキュア・ページへの絶対アドレス・アクセスを有効化することができる。セキュア・インタフェース制御は、複数のセキュア・ドメインのうちのセキュア・ドメインが共用ページにアクセスすることが許可されていることを、ドメイン識別子に基づいて確認することができる。共用ページにアクセスする許可を確かめるために、セキュア・ドメインのドメイン識別子を、共用を許すと識別されたセキュア・ドメインの複数のドメイン識別子と比較することができる。

【００９３】

セキュア・インタフェース制御は、セキュア・ドメインに関して、セキュア・ページの登録ステータスをチェックすることができる。セキュア・インタフェース制御は、そのセキュア・ページが、セキュア・ドメインとともに登録されていないと判定したことに基づいて、そのセキュア・ドメインによる共用が許されているかどうかを判定することができる。セキュア・ドメインによる共用が許されていると判定したことに基づいて、仮想アドレス比較無効化状態をチェックすることができる。セキュア・インタフェース制御は、複数のセキュリティ・ドメインにわたって仮想アドレス共用が許されていることを確かめることができる。例えば、セキュア・インタフェース制御は、仮想アドレスを絶対アドレスにマップするＤＡＴテーブルの複数のグループがセキュアでないホストによって変更され

ていないことを確かめることができ、セキュアでないホストは、セキュア・ページにアクセスすることができる複数のセキュア・ドメインのうちのいずれかに対して１つまたは複数のＤＡＴテーブルのグループを管理するように構成されている。仮想アドレスに対してマップするそれぞれのテーブルは、ＤＡＴテーブルの１つまたは複数のグループの中の複数の関連テーブルを含むことができる。ＤＡＴテーブルの１つまたは複数のグループの中で変化を検出したことに基づいて、セキュア・アクセス・リクエストを終了することができる。

【００９４】

セキュア・ページの仮想－絶対アドレス対を、セキュア・ドメイン識別子とともに、例えば図１のゾーン・セキュリティ・テーブル１００に登録することができる。セキュア・アクセス・リクエストに関連づけられたアドレスを確認することができ、セキュア・アクセス・リクエストに応答して、仮想－絶対アドレス対およびセキュア・ドメイン識別子を有するアクセスしているセキュア・ドメインを確認することができる。仮想アドレス比較無効化状態は、セキュア・ページに関連づけられたセキュア・ドメイン識別子、セキュア・ページに関連づけられた仮想アドレス・マッピング・データおよび仮想アドレス比較無効化状態を含むゾーン・セキュリティ・テーブル１００を通して記憶および更新することができる。セキュア・ページは、ハイパーバイザまたはオペレーティング・システムによって管理されたセキュア仮想機械またはセキュア・コンテナに割り当てることができる。

【００９５】

本開示はクラウド・コンピューティングに関する詳細な説明を含むが、本明細書に記載された教示の実施態様はクラウド・コンピューティング環境だけに限定されないことを理解されたい。本発明の実施形態は、現在知られているまたは後に開発される他の任意のタイプのコンピューティング環境において実施することができる。

【００９６】

クラウド・コンピューティングは、最小限の管理労力またはサービスのプロバイダとの最小限のインタラクションで迅速に供給およびリリースすることができる構成可能なコンピューティング・リソース（例えばネットワーク、ネットワーク帯域、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）の共用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サービス配信モデルである。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（deployment）モデルを含むことができる。

【００９７】

特徴は以下のとおりである。

オンデマンド・セルフサービス：クラウド・コンシューマは、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機能を、このサービスのプロバイダとのヒューマン・インタラクションを必要とすることなく必要に応じて自動的に一方的に供給することができる。

ブロード・ネットワーク・アクセス：機能は、ネットワーク上で利用可能であり、異種のシンまたはシック・クライアント・プラットフォーム（例えば移動電話、ラップトップおよびＰＤＡ）による使用を促進する標準的機構を通してアクセスされる。

リソース・プーリング（resource pooling）：マルチテナント・モデルを使用して複数のコンシューマにサービスを提供するために、プロバイダのコンピューティング・リソースがプールされており、要求に応じて、異なる物理的および仮想リソースが動的に割当ておよび再割当てされる。コンシューマは一般に、提供されたリソースの正確な位置を制御できずまたは正確な位置を知らないが、より高次の抽象化レベル（例えば国、州またはデータセンタ）で位置を指定することができるという意味で、位置独立の感覚がある。

ラピッド・エラスティシティ（rapid elasticity）：機能は、素早くスケールアウトするために迅速かつ弾力的に、場合によっては自動的に供給することができ、素早くスケールインするために迅速にリリースすることができる。コンシューマにとって、供給に利用可能な機能はしばしば無限であるように見え、いつでも好きな量だけ購入することができ

る。
メジャード・サービス（measured service）：クラウド・システムは、サービスのタイプ（例えば、ストレージ、処理、帯域および使用中ユーザ・アカウント）に対して適切なある抽象化レベルで計測機能に介入することによって、リソースの使用状況を自動的に制御および最適化する。リソースの使用状況を監視、制御および報告して、利用されているサービスのプロバイダとコンシューマの両方に透明性を提供することができる。
【００９８】
サービス・モデルは以下のとおりである。
ソフトウェア・アズ・ア・サービス（ＳａａＳ）：コンシューマに提供されるこの機能は、クラウド・インフラストラクチャ上で動作しているプロバイダのアプリケーションを使用する機能である。ウェブ・ブラウザなどのシン・クライアント・インタフェース（例えばウェブ・ベースの電子メール）を通してさまざまなクライアント・デバイスからアプリケーションにアクセス可能である。場合によっては可能な限られたユーザ固有のアプリケーション構成の設定を除けば、コンシューマは、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を含む基礎をなすクラウド・インフラストラクチャを管理もまたは制御もしない。
プラットフォーム・アズ・ア・サービス（ＰａａＳ）：コンシューマに提供されるこの機能は、クラウド・インフラストラクチャ上で、プロバイダがサポートするプログラム言語およびツールを使用して作成されたコンシューマ作成または取得のアプリケーションをデプロイする機能である。コンシューマは、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礎をなすクラウド・インフラストラクチャを管理もまたは制御もしないが、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・ホスティング環境構成は制御することができる。
インフラストラクチャ・アズ・ア・サービス（ＩａａＳ）：コンシューマに提供されるこの機能は、処理、ストレージ、ネットワークおよび他の基本的なコンピューティング・リソースを供給する機能であり、コンシューマは任意のソフトウェアをデプロイおよび動作することができ、これらのソフトウェアは、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。コンシューマは、基礎をなすクラウド・インフラストラクチャを管理もまたは制御もしないが、オペレーティング・システム、ストレージおよびデプロイされたアプリケーションは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構成要素（例えばホスト・ファイアウォール）を限定的に制御することができる。
【００９９】
デプロイメント・モデルは以下のとおりである。
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、組織体のためだけに運営される。インフラストラクチャは、その組織体または第三者が管理することができ、オンプレミス（on-premises）またはオフプレミス（off-premises）で存在することができる。
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、いくつかの組織体によって共有され、利害（例えばミッション、セキュリティ要件、ポリシーおよびコンプライアンス上の問題）を共有する特定のコミュニティをサポートする。インフラストラクチャは、その組織体または第三者が管理することができ、オンプレミスまたはオフプレミスで存在することができる。
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、一般大衆または大きな産業グループが利用可能であり、クラウド・サービスを販売している組織体によって所有される。
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、固有のエンティティを維持しているが、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化された技術または独占技術（例えば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（cloud bursting））によって１つに結合された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）の合成体である。

【０１００】

クラウド・コンピューティング環境は、ステートレス性、低結合、モジュール性および意味論的相互運用性（semantic interoperability）に重きを置く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。

【０１０１】

次に図１９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。示されているとおり、クラウド・コンピューティング環境５０は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を含み、クラウド・コンシューマ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・ディジタル・アシスタント（ＰＤＡ）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または自動車コンピュータ・システム５４Ｎあるいはこれらの組合せは、これらのノードと通信することができる。ノード１０は互いに通信することができる。それらのノードは、上で説明したプライベート、コミュニティ、パブリックまたはハイブリッド・クラウドまたはこれらの組合せなどの１つまたは複数のネットワークに、物理的にまたは仮想的にグループ分けされていることがある（図示せず）。これによって、クラウド・コンピューティング環境５０は、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これらの組合せをサービスとして提供することができ、そのため、クラウド・コンシューマは、ローカル・コンピューティング・デバイス上にリソースを維持する必要がない。図１９に示されたタイプのコンピューティング・デバイス５４Ａ～Ｎは単なる例であることが意図されていること、ならびに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上もしくはアドレス指定可能なネットワーク接続上またはその両方で（例えばウェブ・ブラウザを使用して）、コンピュータ化された任意のタイプのデバイスと通信することができることが理解される。

【０１０２】

次に図２０を参照すると、クラウド・コンピューティング環境５０（図１９）によって提供される一組の機能抽象化層が示されている。図２０に示された構成要素、層および機能は単なる例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を予め理解しておくべきである。図示のとおり、以下の層および対応する機能が提供される。

【０１０３】

ハードウェアおよびソフトウェア層６０は、ハードウェア構成要素およびソフトウェア構成要素を含む。ハードウェア構成要素の例は、メインフレーム６１、ＲＩＳＣ（縮小命令セット・コンピュータ）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（blade server）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キング構成要素６６を含む。いくつかの実施形態では、ソフトウェア構成要素が、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。

【０１０４】

仮想化層７０は抽象化層を提供し、この層から、仮想エンティティの以下の例を提供することができる：仮想サーバ７１、仮想ストレージ７２、仮想専用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。

【０１０５】

一例では、管理層８０が以下の機能を提供することができる。リソース供給（Resource provisioning）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目的に利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。計量および価格決定（Metering and Pricing）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たときの費用追跡、およびこれらのリソースの消費に対する課金または請求を提供する。一例では、これらのリソースがアプリケーション・ソフトウェア・ライセンスを含むことがある。セキュリティは、クラウド・コンシューマおよびタスクの識別確認ならびにデータおよび他のリソースの保護を提供する。ユーザ・ポータル８３は、コンシューマおよびシステム管理者に、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。サービス水準管理８４は、必要なサービス水準が達成されるようなクラウド・コンピューティング・リソースの割振りおよび管理を提供する。サービス水準合意（Service Level Agreement）（ＳＬＡ）計画および履行８５は、ＳＬＡによって将来必要になると予想されるクラウド・コンピューティング・リソースの事前調整および調達を提供する。

【０１０６】

ワークロード層９０は、クラウド・コンピューティング環境を利用することができる機能の例を提供する。この層から提供することができ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、仮想教室教育配信９３、データ解析処理９４、トランザクション処理９５、および仮想機械に関連づけられたセキュア・ストレージへのアクセスの制御９６を含む。これらは一部の例でしかないこと、および他の実施形態ではこれらの層が異なるサービスを含みうることが理解される。

【０１０７】

次に図２１を参照すると、本発明の１つまたは複数の実施形態によるシステム２１００が示されている。システム２１００は、１つまたは複数のクライアント・デバイス２０Ａ～２０Ｅと直接にまたは間接的に、例えばネットワーク１６５を介して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）を含む。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・サーバとすることができる。ノード１０は、ハイパーバイザ１２を実行する。ハイパーバイザ１２は、１つまたは複数のＶＭ１５（１５Ａ～１５Ｎ）のデプロイを容易にする。ノード１０はさらに、セキュア・インタフェース制御１１を含むハードウェア／ファームウェア層１３を含む。セキュア・インタフェース制御１１は、ハイパーバイザ１２が１つまたは複数のサービスを仮想機械１５に提供するのを容易にする１つまたは複数のハードウェア・モジュールおよびファームウェアを含む。既存の技術的ソリューションでは、ハイパーバイザ１２とセキュア・インタフェース制御１１の間、セキュア・インタフェース制御１１と１つまたは複数のＶＭ１５の間、およびハイパーバイザ１２と１つまたは複数のＶＭ１５の間の通信、ならびにセキュア・インタフェース制御１１を通したハイパーバイザ１２からＶＭ１５への通信が存在する。セキュアＶＭ環境を容易にするため、本発明の１つまたは複数の実施形態によるホスティング・ノード１０は、ハイパーバイザ１２と１つまたは複数のＶＭ１５との間の直接通信を一切含まない。

【０１０８】

例えば、ホスティング・ノード１０は、ＶＭ１５Ａ～１５Ｎのうちの１つまたは複数のＶＭをクライアント・デバイス２０Ａがデプロイするのを容易にすることができる。ＶＭ１５Ａ～１５Ｎは、異なるクライアント・デバイス２０Ａ～２０Ｅからのそれぞれのリクエストに応答してデプロイすることができる。例えば、ＶＭ１５Ａは、クライアント・デバイス２０Ａによってデプロイすることができ、ＶＭ１５Ｂは、クライアント・デバイス２０Ｂによってデプロイすることができ、ＶＭ１５Ｃは、クライアント・デバイス２０Ｃによってデプロイすることができる。ノード１０はさらに、クライアントが、（ＶＭとして動作しない）物理サーバを供給するのを容易にすることができる。本明細書に記載された例は、ノード１０内のリソースをＶＭの一部として供給することを実施するが、記載された技術的ソリューションを適用して、それらのリソースを物理サーバの一部として供給することもできる。

【０１０９】

一例では、クライアント・デバイス２０Ａ～２０Ｅが、同じエンティティ、例えば同じ

人間、ビジネス、政府機関、企業内の部門または他のエンティティに属していてもよく、そのエンティティのプライベート・クラウドとしてノード１０を動作させることができる。その場合、ノード１０は単に、そのエンティティに属するクライアント・デバイス２０Ａ～２０Ｅによってデプロイされた１５Ａ～１５Ｎのホストの役目を果たす。別の例では、クライアント・デバイス２０Ａ～２０Ｅが異なるエンティティに属していてもよい。例えば、第１のエンティティは、クライアント・デバイス２０Ａを所有することができ、その一方で、第２のエンティティは、クライアント・デバイス２０Ｂを所有することができる。その場合には、異なるエンティティからのＶＭのホストの役目を果たすパブリック・クラウドとしてノード１０を動作させることができる。例えば、ＶＭ１５ＡがＶＭ１５Ｂへのアクセスを容易にしないシュラウドされた（shrouded）方式で、ＶＭ１５Ａ～１５Ｎをデプロイすることができる。例えば、ノード１０は、ＩＢＭ ｚ Ｓｙｓｔｅｍｓ（Ｒ） Ｐｒｏｃｅｓｓｏｒ Ｒｅｓｏｕｒｃｅ／Ｓｙｓｔｅｍｓ Ｍａｎａｇｅｒ（ＰＲ／ＳＭ）Ｌｏｇｉｃａｌ Ｐａｒｔｉｔｉｏｎ（ＬＰＡＲ）フィーチャを使用して、ＶＭ１５Ａ～１５をシュラウドすることができる。ＰＲ／ＳＭ ＬＰＡＲなどのこれらのフィーチャは、パーティション間の分離を提供し、したがって、ノード１０が、異なる論理パーティション内の同じ物理ノード１０上の異なるエンティティに対して２つ以上のＶＭ１５Ａ～１５Ｎをデプロイすることを容易にする。ＰＲ／ＳＭ ＬＰＡＲハイパーバイザは、この分離を提供するための特定のハードウェアを有する信頼できる内部ファームウェア内に実装される。

【０１１０】

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、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リクエストする、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が受け取るリクエストを送ることができる。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からのリクエスト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、そのＶＭＭは、ＶＭを生成および動作するソフトウェア、ファームウェアまたはハードウェアとすることができる。ハイパーバイザ１２は、ＶＭ１５Ａが、ノード１０のハードウェア構成要素を使用して、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実施することを容易にする。適切なフィーチャおよび変更がある場合、ハイパーバイザ１２は、ＩＢＭ ｚ Ｓｙｓｔｅｍｓ（Ｒ）、オラクル（Oracle）のＶＭ Ｓｅｒｖｅｒ、シトリックス（Citrix）のＸｅｎＳｅｒｖｅｒ、ＶｍｗａｒｅのＥＳＸ、Ｍｉｃｒｏｓｏｆｔ Ｈｙｐｅｒ－Ｖハイパーバイザ、または他の任意のハイパーバイザとすることができる。ハイパーバイザ１２は、ノード１０上で直接に実行されるネイティブのハイパーバイザ、または別のハイパーバイザ上で実行されるホステッド（hosted）・ハイパーバイザとすることができる。

【０１１１】

次に図２２を参照すると、本発明の１つまたは複数の実施形態による、本明細書の教示を実施するためのノード１０が示されている。ノード１０は、本明細書に記載されたさまざまな通信技術を利用する任意の数および組合せのコンピューティング・デバイスおよびネットワークを含み、もしくはそのようなコンピューティング・デバイスおよびネットワークを使用し、またはそのようなコンピューティング・デバイスおよびネットワークを含み、使用する、電子コンピュータ・フレームワークとすることができる。ノード１０は、異なるサービスに変化する能力または他から独立していくつかのフィーチャを再構成する能力を有したまま、簡単にスケーリング、拡張、およびモジュール化することができる。

【０１１２】

この実施形態では、ノード１０がプロセッサ２２０１を有し、プロセッサ２２０１は、１つまたは複数の中央処理ユニット（ＣＰＵ）２２０１ａ、２２０１ｂ、２２０１ｃなど

を含むことができる。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るプロセッサ２２０１は、システム・バス２２０２を介してシステム・メモリ２２０３および他のさまざまな構成要素に結合されている。システム・メモリ２２０３は、リード・オンリー・メモリ（ＲＯＭ）２２０４およびランダム・アクセス・メモリ（ＲＡＭ）２２０５を含む。ＲＯＭ２２０４は、システム・バス２２０２に結合されており、基本入出力システム（ＢＩＯＳ）を含むことができ、ＢＩＯＳは、ノード１０のある種の基本機能を制御する。ＲＡＭは、プロセッサ２２０１によって使用されるためにシステム・バス２２０２に結合された読出し－書込みメモリである。

【０１１３】

図２２のノード１０はハードディスク２２０７を含む。ハードディスク２２０７は、プロセッサ２２０１が読み、実行することができる有形のストレージ媒体の例である。ハードディスク２２０７は、ソフトウェア２２０８およびデータ２２０９を記憶している。ソフトウェア２２０８は、（図１～２１を参照して説明し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２２０１によってノード１０上で実行される命令として記憶されている。データ２２０９は、ソフトウェア２２０８のオペレーションをサポートするように、およびソフトウェア２２０８のオペレーションによって使用されるようにさまざまなデータ構造で編成された定性的または定量的変量の一組の値を含む。

【０１１４】

図２２のノード１０は、プロセッサ２２０１、システム・メモリ２２０３、ハードディスク２２０７およびノード１０の他の構成要素（例えば周辺および外部デバイス）を相互接続し、それらの構成要素間の通信をサポートする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、この１つまたは複数のアダプタを、介在するバス・ブリッジを介してシステム・バス２２０２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、この１つまたは複数のＩ／Ｏバスは、ペリフェラル・コンポーネント・インターコネクト（Peripheral Component Interconnect）（ＰＣＩ）などの一般的なプロトコルを利用することができる。

【０１１５】

示されているとおり、ノード１０は、キーボード２２２１、マウス２２２２、スピーカ２２２３およびマイクロフォン２２２４をシステム・バス２２０２に相互接続するインタフェース・アダプタ２２２０を含む。ノード１０は、システム・バス２２０２をディスプレイ２２３１に相互接続するディスプレイ・アダプタ２２３０を含む。ディスプレイ・アダプタ２２３０（もしくはプロセッサ２２０１またはその両方）は、ＧＵＩ２２３２の表示および管理などのグラフィクス性能を提供するグラフィクス・コントローラを含むことができる。通信アダプタ２２４１が、システム・バス２２０２をネットワーク２２５０に相互接続し、ノード１０が、サーバ２２５１やデータベース２２５２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つまたは複数の実施形態では、ソフトウェア２２０８およびデータ２２０９のオペレーションを、ネットワーク２２５０上で、サーバ２２５１およびデータベース２２５２によって実施することができる。例えば、ソフトウェア２２０８およびデータ２２０９の内部反復を、プラットフォーム・アズ・ア・サービス、ソフトウェア・アズ・ア・サービスもしくはインフラストラクチャ・アズ・ア・サービスまたはこれらの組合せとして（例えば分散システム内のウェブ・アプリケーションとして）提供するために、ネットワーク２２５０、サーバ２２５１およびデータベース２２５２を結合することができる。

【０１１６】

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、特にＶＭのホストの役目を果たすコンピュータ・サーバに根差したものである。さらに、本発明の１つまたは複数の実施形態は、ＶＭのホストの役目を果たすコンピュータ・サーバが、ハイパーバイザでさえもセキュアＶＭに関連づけられたメモリ、レジスタおよび他のデータにアクセスすることが禁じられているセキュアＶＭのホストの役目を果たすことを容易にすることによ

って、コンピューティング技術のオペレーション自体の改良、特にＶＭのホストの役目を果たすコンピュータ・サーバのオペレーションの改良を容易にする。さらに、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）またはこれらの組合せを含むセキュア・インタフェース制御（本明細書では「ＵＶ」とも呼ばれる）を使用して、セキュアＶＭとハイパーバイザとの分離を容易にすることによって、したがって、コンピューティング・サーバがホストの役目を果たしている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・コンピューティング・サーバの改良に向けてのかなりのステップを提供する。セキュア・インタフェース制御は、本明細書に記載されたとおり、ＶＭの初期化／終了時のセキュアＶＭ状態に重大なオーバヘッドを追加することなく、セキュリティを容易にするための軽量の介在オペレーションを提供する。

【０１１７】

本明細書に開示された本発明の実施形態は、ＶＭのセキュア・ストレージへのアクセスを制御するシステム、方法もしくはコンピュータ・プログラム製品（本明細書ではシステム）またはこれらの組合せを含むことがある。それぞれの説明に関して、要素の識別子は、異なる図の他の類似の要素に対して再使用されていることに留意されたい。

【０１１８】

本明細書では、本発明のさまざまな実施形態が関連図を参照して説明される。本発明の範囲を逸脱することなく本発明の代替実施形態を考案することができる。以下の説明および図面には、要素間のさまざまな接続および位置関係（例えば上、下、隣りなど）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、特に指定されていない限り、直接的なものであることまたは間接的なものであることができ、本発明は、この点に関して限定を意図したものではない。したがって、実体の結合は、直接結合または間接結合であることができ、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、本明細書には詳細に記載されていない追加の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、本明細書に記載されたさまざまなタスクおよびプロセス・ステップを組み込むことができる。

【０１１９】

特許請求の範囲および本明細書の解釈のために、以下の定義および略語が使用される。本明細書で使用されるとき、用語「備える（comprises）」、「備える（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）」、またはこれらの用語の他の変異語は、非排他的包含（non-exclusive inclusion）をカバーすることが意図されている。例えば、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、必ずしもそれらの要素だけに限定されるわけではなく、明示的にはリストに入れられていない他の要素、あるいはこのような組成物、混合物、プロセス、方法、物品または装置に固有の他の要素を含みうる。

【０１２０】

さらに、本明細書では、用語「例示的な」が、「例、事例または実例として役立つ」ことを意味するものとして使用されている。本明細書に「例示的」として記載された実施形態または設計は必ずしも、他の実施形態または設計よりも好ましいまたは有利であるとは解釈されない。用語「少なくとも１つの」および「１つまたは複数の」は、１以上の任意の整数、すなわち１、２、３、４などを含むと理解してもよい。用語「複数の」は、２以上の任意の整数、すなわち２、３、４、５などを含むと理解してもよい。用語「接続」は、間接「接続」と直接「接続」の両方を含むことがある。

【０１２１】

用語「約」、「実質的に」、「およそ」およびこれらの用語の変異語は、特定の数量の大きさに関連した、本出願の提出時に利用可能な機器に基づく誤差の程度を含むことが意図されている。例えば、「約」は、所与の値の±８％、５％または２％の範囲を含みうる。

【０１２２】

本発明は、インテグレーションの可能な技術的詳細レベルにおいて、システム、方法も

しくはコンピュータ・プログラム製品、またはこれらの組合せであることができる。コンピュータ・プログラム製品は、本発明の態様をプロセッサに実行させるためのコンピュータ可読プログラム命令をその上に有するコンピュータ可読ストレージ媒体を含むことができる。

【０１２３】

このコンピュータ可読ストレージ媒体は、命令実行デバイスが使用するための命令を保持および記憶することができる有形のデバイスとすることができる。このコンピュータ可読ストレージ媒体は例えば、限定はされないが、電子ストレージ・デバイス、磁気ストレージ・デバイス、光学ストレージ・デバイス、電磁気ストレージ・デバイス、半導体ストレージ・デバイスまたはこれらの適当な組合せとすることができる。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なリストは、ポータブル・コンピュータ・ディスケット、ハードディスク、ランダム・アクセス・メモリ（ＲＡＭ）、リード・オンリー・メモリ（ＲＯＭ）、消去可能なプログラマブル・リード・オンリー・メモリ（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）、ポータブル・コンパクト・ディスク・リード・オンリー・メモリ（ＣＤ－ＲＯＭ）、ディジタル・バーサタイル・ディスク（ＤＶＤ）、メモリ・スティック、フロッピー（Ｒ）・ディスク、機械的にコード化されたデバイス、例えばパンチカードまたはその上に命令が記録された溝の中の一段高くなった構造体、およびこれらの適当な組合せを含む。本明細書で使用されるとき、コンピュータ可読ストレージ媒体は、それ自体が一過性の信号、例えば電波もしくは他の自由に伝搬する電磁波、ウェーブガイドもしくは他の伝送体内を伝搬する電磁波（例えば光ファイバ・ケーブル内を通る光パルス）、または電線を通して伝送される電気信号であると解釈されるべきではない。

【０１２４】

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対応する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することができ、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、ワイド・エリア・ネットワークもしくは無線ネットワークまたはそれらの組合せを介して外部コンピュータもしくは外部ストレージ・デバイスにダウンロードすることができる。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、またはこれらの組合せを含むことができる。それぞれの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・インタフェースは、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け取り、それらのコンピュータ可読プログラム命令を、対応する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。

【０１２５】

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）命令、機械命令、機械依存命令、マイクロコード、ファームウェア命令、状態設定データ、もしくは集積回路用の構成データであってもよく、または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種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つまたは複数のプログラミング言語の任意の組合せで書かれた、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い。このコンピュータ可読プログラム命令は、全体がユーザのコンピュータ上で実行されてもよく、一部がユーザのコンピュータ上で実行されてもよく、独立型ソフトウェア・パッケージとして実行されてもよく、一部がユーザのコンピュータ上で、一部が遠隔コンピュータ上で実行されてもよく、または全体が遠隔コンピュータもしくは遠隔サーバ上で実行されてもよい。上記の最後のシナリオでは、遠隔コンピュータが、ローカル・エリア・ネットワーク（ＬＡＮ）もしくはワイド・エリア・ネットワーク（ＷＡＮ）を含む任意のタイプ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もよく、またはこの接続が、外部コンピュータ

に対して（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）実施されてもよい。いくつかの実施形態では、本発明の態様を実施するために、例えばプログラム可能論理回路、フィールドプログラマブル・ゲート・アレイ（ＦＰＧＡ）またはプログラム可能論理アレイ（ＰＬＡ）を含む電子回路が、このコンピュータ可読プログラム命令の状態情報を利用してその電子回路をパーソナライズすることにより、このコンピュータ可読プログラム命令を実行してもよい。

【０１２６】

本明細書では、本発明の態様が、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の図を参照して説明される。それらの流れ図もしくはブロック図またはその両方の図のそれぞれのブロック、およびそれらの流れ図もしくはブロック図またはその両方の図のブロックの組合せは、コンピュータ可読プログラム命令によって実施することができることが理解される。

【０１２７】

これらのコンピュータ可読プログラム命令は、機械を形成する汎用コンピュータ、専用コンピュータまたは他のプログラム可能データ処理装置のプロセッサに、それらのコンピュータまたは他のプログラム可能データ処理装置のプロセッサによって実行されるこれらの命令が、これらの流れ図もしくはブロック図またはその両方の図のブロックに指定された機能／動作を実施する手段を生成するような態様で、提供することができる。これらのコンピュータ可読プログラム命令はさらに、特定の方式で機能するようにコンピュータ、プログラム可能データ処理装置もしくは他のデバイスまたはこれらの組合せに指図することができるコンピュータ可読ストレージ媒体に、その中に命令が記憶されたコンピュータ可読ストレージ媒体が、これらの流れ図もしくはブロック図またはその両方の図のブロックに指定された機能／動作の態様を実施する命令を含む製品を含むような態様で、記憶することができる。

【０１２８】

これらのコンピュータ可読プログラム命令はさらに、コンピュータ、他のプログラム可能装置または他のデバイス上で一連の動作ステップを実行させて、コンピュータによって実施されるプロセスを生み出すために、このコンピュータ、他のプログラム可能データ処理装置または他のデバイス上に、このコンピュータ、他のプログラム可能装置または他のデバイス上で実施されるこれらの命令が、これらの流れ図もしくはブロック図またはその両方の図のブロックに指定された機能／動作を実施するような態様で、ロードすることができる。

【０１２９】

添付図中の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態様のアーキテクチャ、機能および動作を示す。この点に関して、それらの流れ図またはブロック図のそれぞれのブロックは、指定された論理機能を実施する１つまたは複数の実行可能命令を含む、命令のモジュール、セグメントまたは部分を表すことがある。いくつかの代替実施態様では、ブロックに示された機能を、図に示された順序とは異なる順序で実行することができる。例えば、連続して示された２つのブロックが、実際は、実質的に同時に実行されることがあり、または、含まれる機能によってはそれらのブロックが逆の順序で実行されることもある。それらのブロック図もしくは流れ図またはその両方の図のそれぞれのブロック、ならびにそれらのブロック図もしくは流れ図またはその両方の図のブロックの組合せを、指定された機能もしくは動作を実行しまたは専用ハードウェアとコンピュータ命令の組合せを実施するハードウェアベースの専用システムによって実施することができることにも留意すべきである。

【０１３０】

本明細書で使用される用語の目的は特定の実施形態を説明することだけであり、それらの用語が限定を目的とすることは意図されていない。文脈からそうでないことが明らかである場合を除き、本明細書で使用されるとき、単数形の「ａ」、「ａｎ」および「ｔｈｅ

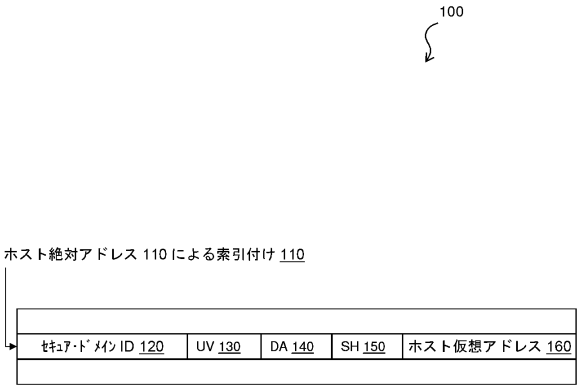
」は複数形も含むことが意図されている。本明細書で使用されるとき、用語「備える（comprises）」もしくは「備える（comprising）」またはその両方は、明示された特徴、完全体（integer）、ステップ、動作、要素もしくは構成要素またはこれらの組合せの存在を指定するが、他の１つもしくは複数の特徴、完全体、ステップ、動作、要素、構成要素もしくはこれらのグループ、またはこれらの組合せの存在または追加を排除しないことも理解される。

【０１３１】

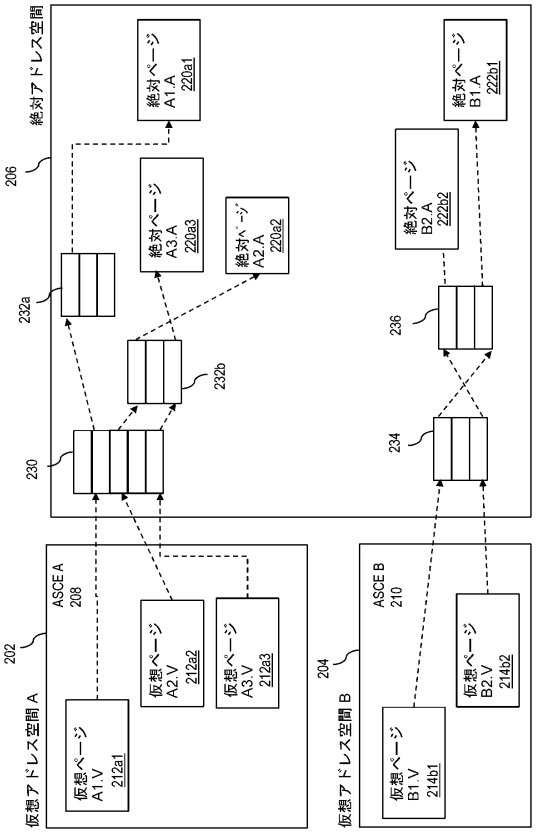
本明細書のさまざまな実施形態の説明は例示のために提示されたものであり、それらの説明が網羅的であること、または開示された実施形態に限定されることは意図されていない。当業者には、記載された実施形態の範囲および思想を逸脱しない多くの変更および変形が明白になるであろう。本明細書で使用されている用語は、実施形態の原理、実際的用途、もしくは市場に出ている技術には見られない技術的改良を最もうまく説明するように、または本明細書に開示された実施形態を他の当業者が理解することができるように選択した。

【図面】

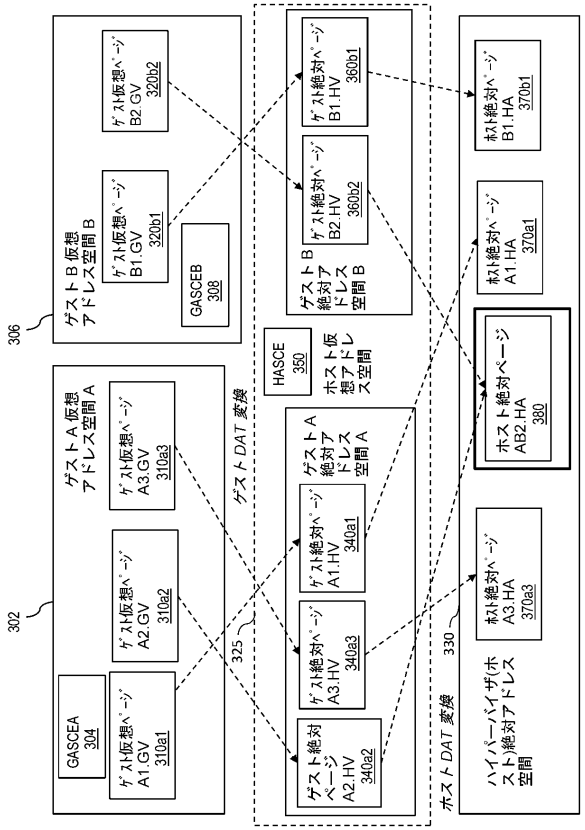
【図１】


100
ホスト絶対アドレス 110 による索引付け 110
ｾｷｭｱ･ﾄﾞﾒｲﾝ ID 120
UV 130
DA 140
SH 150
ホスト仮想アドレス 160

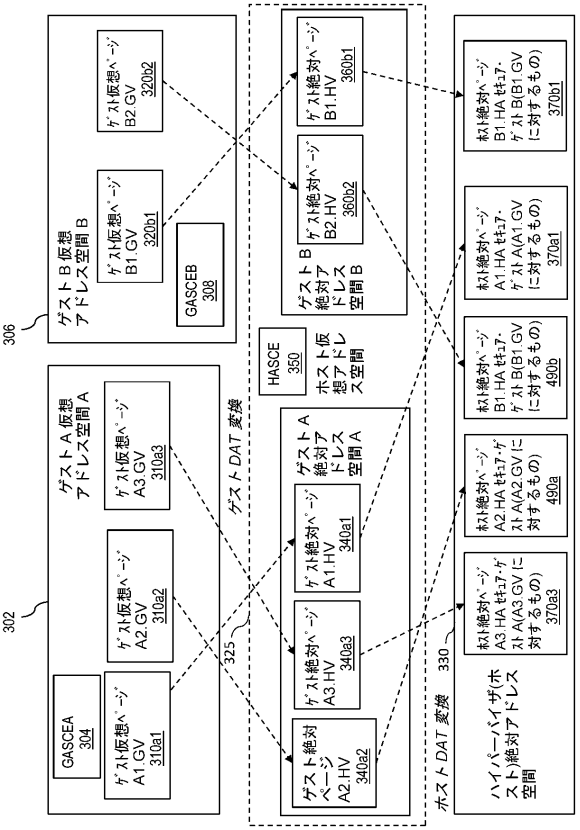
【図２】


絶対アドレス空間
206
絶対ページ A1.A 220a1
絶対ページ A3.A 220a3
絶対ページ A2.A 220a2
232a
232b
230
絶対ページ B1.A 222b1
絶対ページ B2.A 222b2
236
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

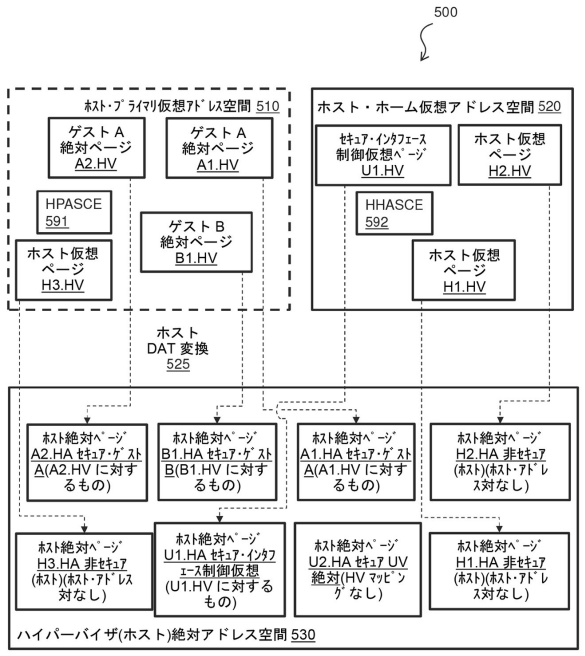
【図３】


306
ゲスト B 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
GASCEA
304
ゲスト仮想ページ
A1.GV
310a1
325
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
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
330
ホスト DAT 変換
ハイパーバイザ(ホスト)絶対アドレス
空間

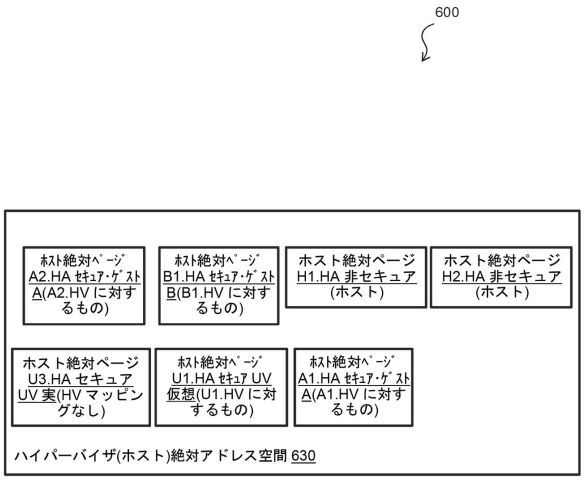
【図４】


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
GASCEA
304
ゲスト仮想ページ
A1.GV
310a1
325
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
ホスト絶対ページ
B1.HA セキュア・ゲスト B(B1.GV に対するもの)
370b1
ホスト絶対ページ
A1.HA セキュア・ゲスト A(A1.GV に対するもの)
370a1
ホスト絶対ページ
B1.HA セキュア・ゲスト B(B1.GV に対するもの)
490b
ホスト絶対ページ
A2.HA セキュア・ゲスト A(A2.GV に対するもの)
490a
ホスト絶対ページ
A3.HA セキュア・ゲスト A(A3.GV に対するもの)
370a3
330
ホスト DAT 変換
ハイパーバイザ(ホスト)絶対アドレス
空間

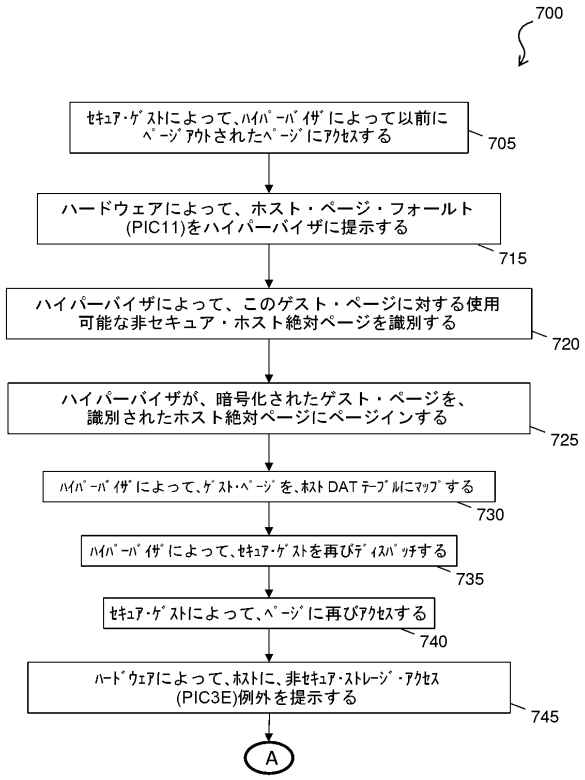
【図５】


500
ホスト・プライマリ仮想アドレス空間 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
ホスト・ホーム仮想アドレス空間 520
セキュア・インタフェース
制御仮想ページ
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 に対するもの)
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)
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)
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・インタフェース制御仮想
(U1.HV に対するもの)
ホスト絶対ページ
U2.HA セキュア UV
絶対(HV マッピングなし)
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

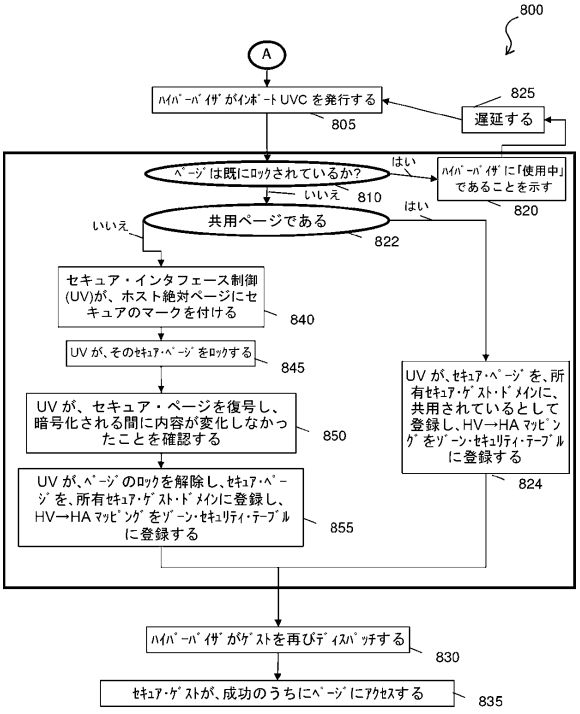
【図６】


600
ホスト絶対ページ
A2.HA セキュア・ゲスト
A(A2.HV に対するもの)
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)
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 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 に対するもの)
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)
ハイパーバイザ(ホスト)絶対アドレス空間 630

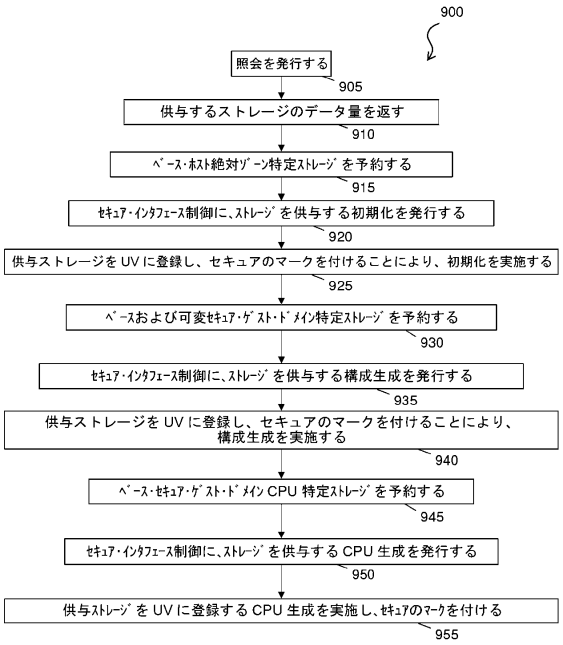
【図７】


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・ページに対する使用可能な非セキュア・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
ハイパーバイザによって、ゲスト・ページを、ホスト DAT テーブルにマップする
730
ハイパーバイザによって、セキュア・ゲストを再びディスパッチする
735
セキュア・ゲストによって、ページに再びアクセスする
740
ハードウェアによって、ホストに、非セキュア・ストレージ・アクセス(PIC3E)例外を提示する
745
A

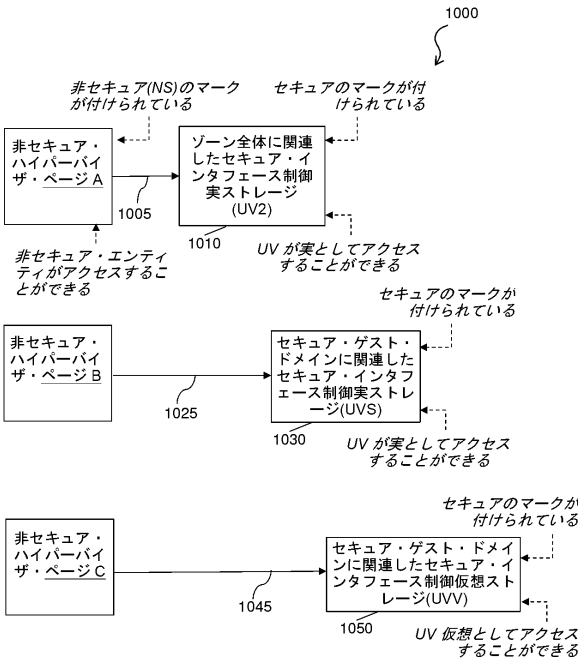
【図８】


800
A
ハイパーバイザがインボート UVC を発行する
805
825
遅延する
ページは既にロックされているか?
810
はい
ハイパーバイザに「使用中」であることを示す
820
いいえ
共用ページである
822
はい
いいえ
セキュア・インタフェース制御(UV)が、ホスト絶対ページにセキュアのマークを付ける
840
UV が、そのセキュア・ページをロックする
845
UV が、セキュア・ページを復号し、暗号化される間に内容が変化しなかったことを確認する
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、所有セキュア・ゲスト・ドメインに、共用されているとして登録し、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びディスパッチする
830
セキュア・ゲストが、成功のうちにページにアクセスする
835

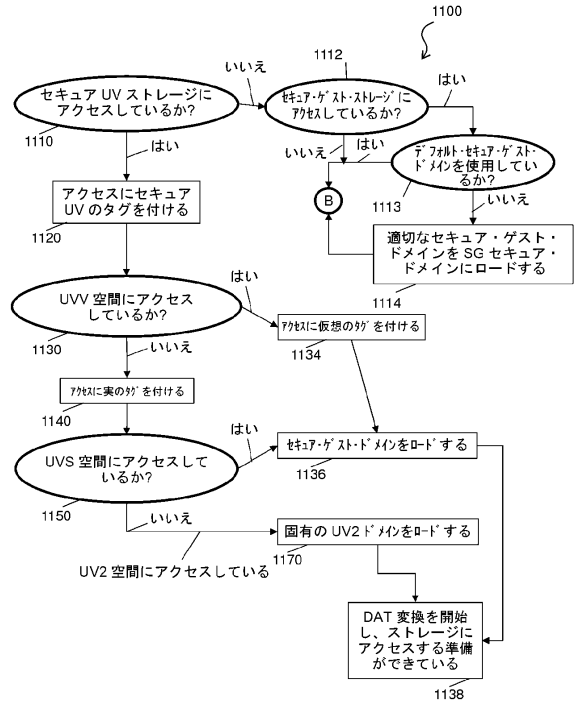
【図９】


900
照会を発行する
905
供与するストレージのデータ量を返す
910
ベース・ホスト絶対ゾーン特定ストレージを予約する
915
セキュア・インタフェース制御に、ストレージを供与する初期化を発行する
920
供与ストレージを UV に登録し、セキュアのマークを付けることにより、初期化を実施する
925
ベースおよび可変セキュア・ゲスト・ドメイン特定ストレージを予約する
930
セキュア・インタフェース制御に、ストレージを供与する構成生成を発行する
935
供与ストレージを UV に登録し、セキュアのマークを付けることにより、構成生成を実施する
940
ベース・セキュア・ゲスト・ドメイン CPU 特定ストレージを予約する
945
セキュア・インタフェース制御に、ストレージを供与する CPU 生成を発行する
950
供与ストレージを UV に登録する CPU 生成を実施し、セキュアのマークを付ける
955

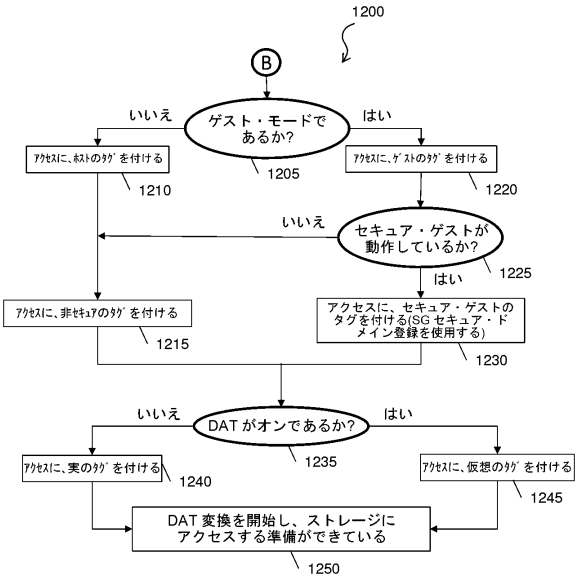
【図１０】


1000
非セキュア(NS)のマークが付けられている
セキュアのマークが付けられている
非セキュア・ハイパーバイザ・ページ A
1005
ゾーン全体に関連したセキュア・インタフェース制御実ストレージ(UV2)
1010
非セキュア・エンティティがアクセスすることができる
UV が実としてアクセスすることができる
セキュアのマークが付けられている
非セキュア・ハイパーバイザ・ページ B
1025
セキュア・ゲスト・ドメインに関連したセキュア・インタフェース制御実ストレージ(UVS)
1030
UV が実としてアクセスすることができる
セキュアのマークが付けられている
非セキュア・ハイパーバイザ・ページ C
1045
セキュア・ゲスト・ドメインに関連したセキュア・インタフェース制御仮想ストレージ(UVV)
1050
UV 仮想としてアクセスすることができる

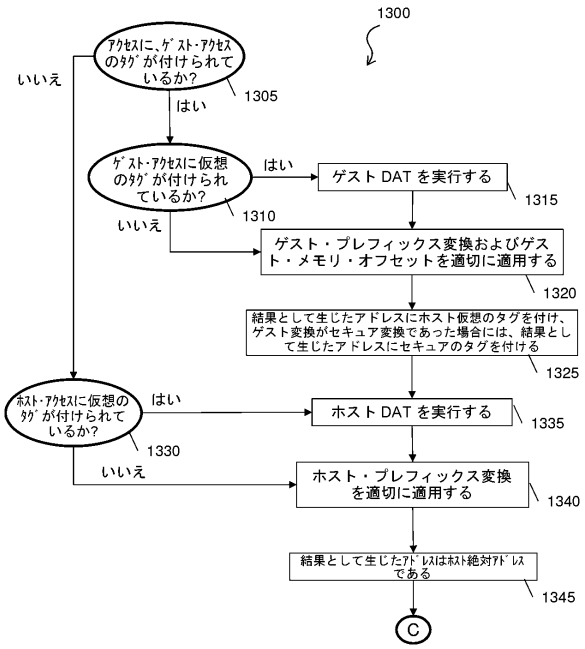
【図１１】



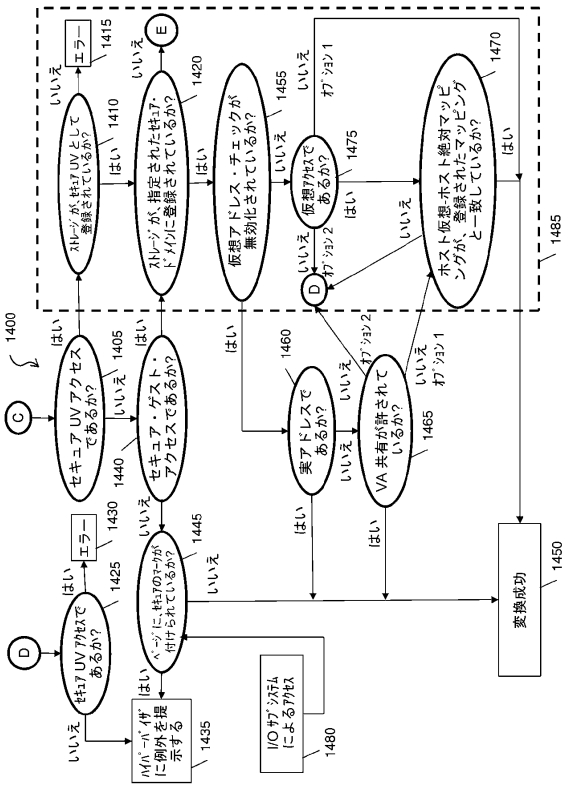

【図１２】



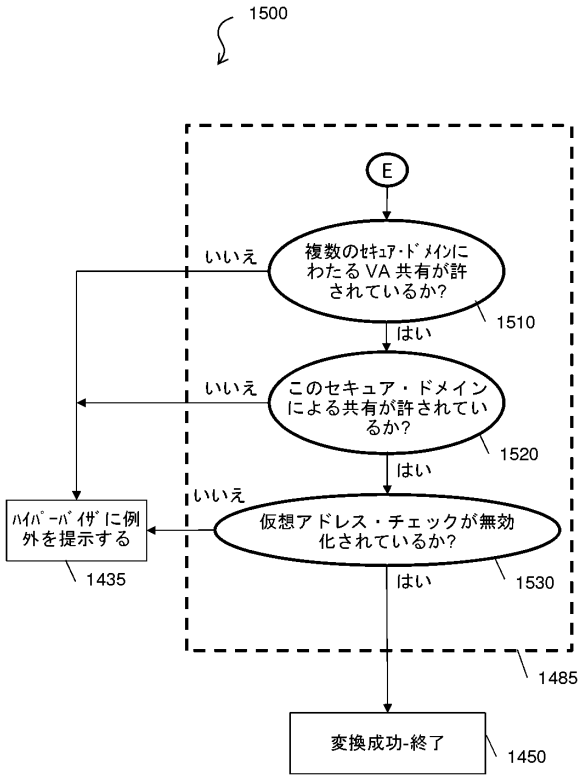

【図１３】



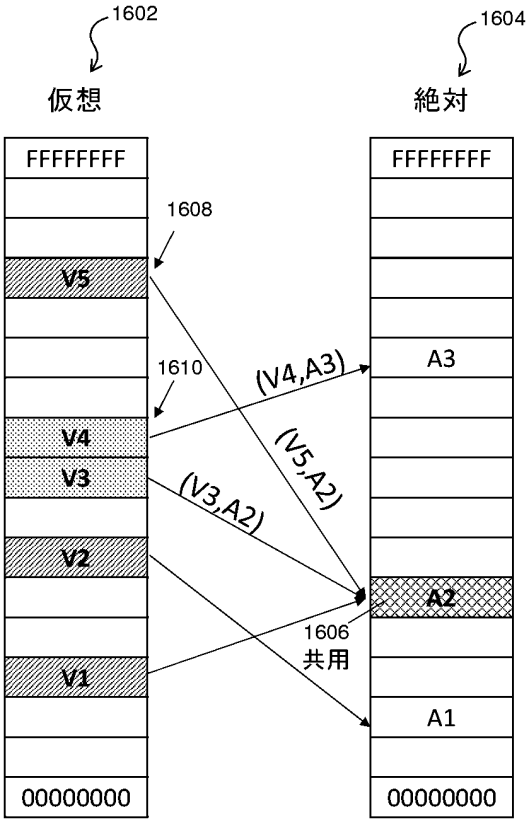

【図１４】



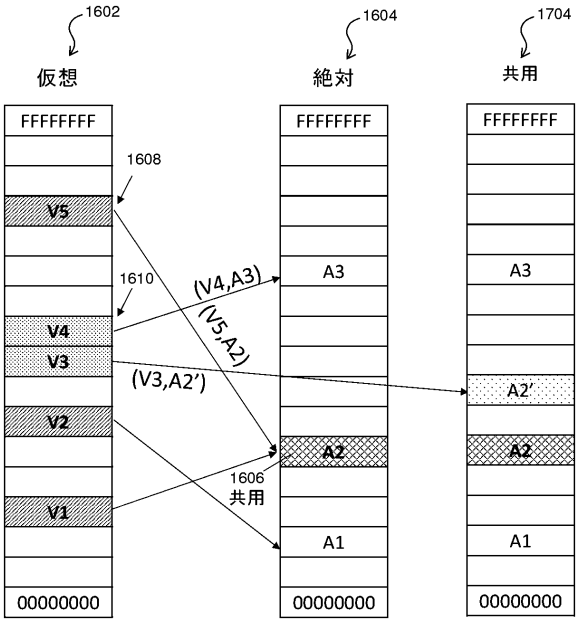
【図１５】



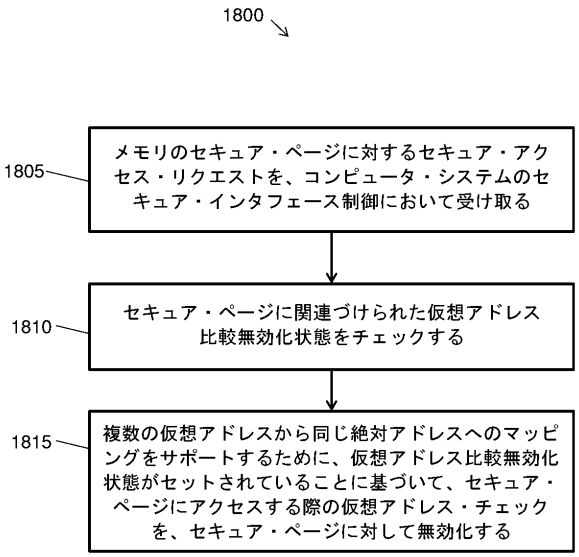

【図１６】



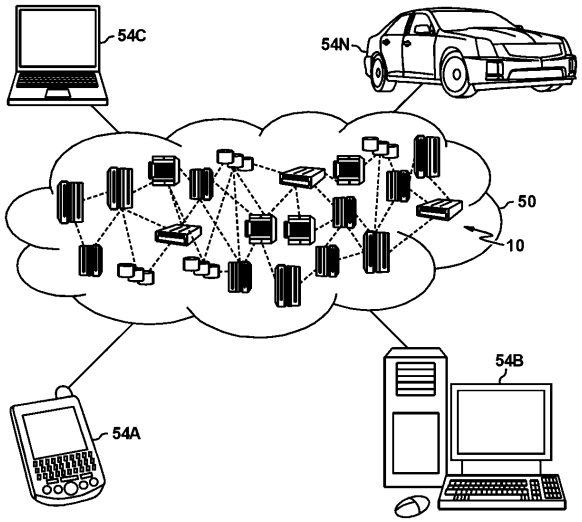

【図１７】



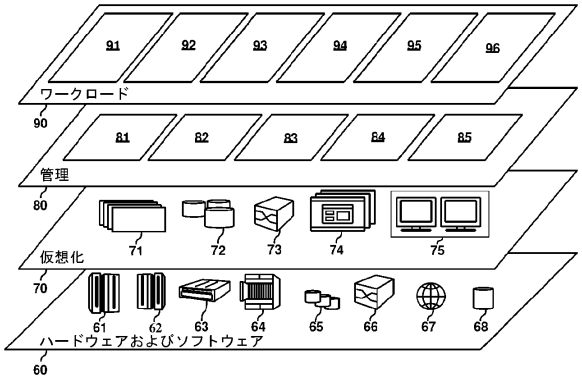

【図１８】



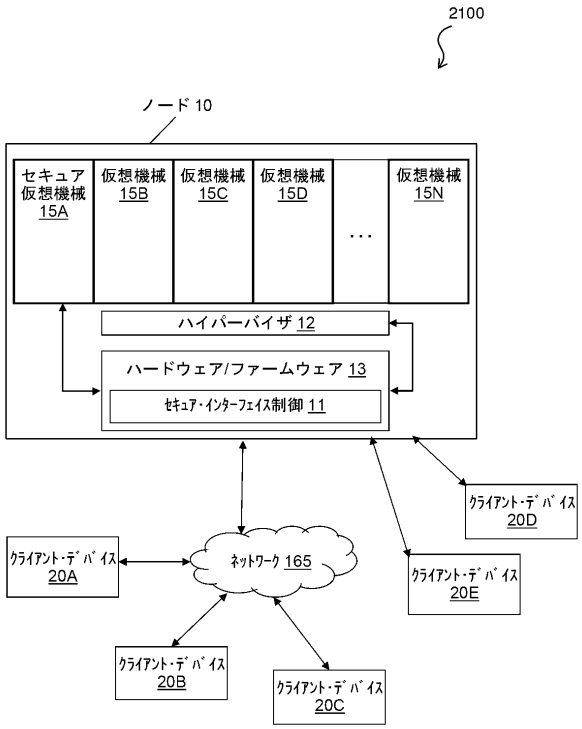
【図１９】



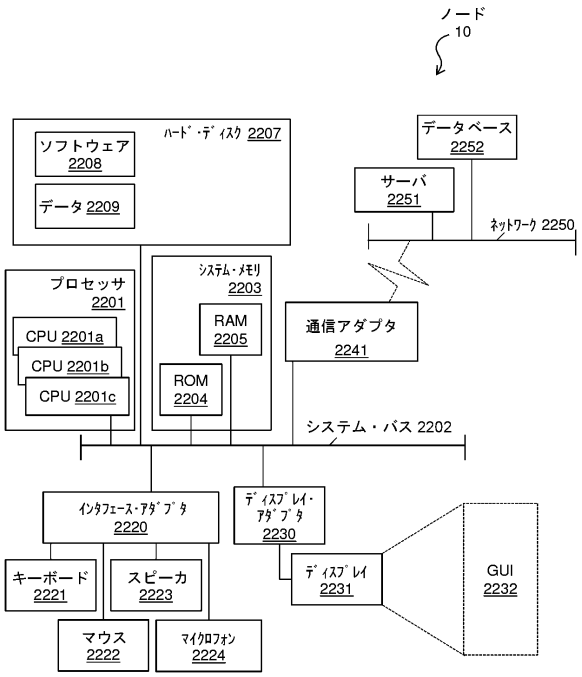

【図２０】




【図２１】




【図２２】



フロントページの続き

(72)発明者　ブサバ、ファディ
アメリカ合衆国１２６０１－５４００ 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、クラントン
アメリカ合衆国１２６０１－５４００ ニューヨーク州ポキプシー サウス・ロード２４５５
(72)発明者　ブラッドベリー、ジョナサン
アメリカ合衆国１２６０１－５４００ 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　米国特許出願公開第２０１９／００４２４６３（ＵＳ，Ａ１）
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　２１／００－８８
Ｇ０６Ｆ　１２／１４