(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6556710号
(P6556710)

(45)発行日　令和1年8月7日(2019.8.7)　(24)登録日　令和1年7月19日(2019.7.19)

(51)Int.Cl.		F I		
G06F 9/50	(2006.01)	G06F	9/50	150A
G06F 9/455	(2006.01)	G06F	9/50	120A
G06F 21/57	(2013.01)	G06F	9/455	150
		G06F	21/57	

請求項の数 9　(全 28 頁)

(21)出願番号　特願2016-524325 (P2016-524325)
(86)(22)出願日　平成26年7月1日(2014.7.1)
(65)公表番号　特表2016-526734 (P2016-526734A)
(43)公表日　平成28年9月5日(2016.9.5)
(86)国際出願番号　PCT/US2014/045125
(87)国際公開番号　WO2015/002992
(87)国際公開日　平成27年1月8日(2015.1.8)
審査請求日　平成28年2月26日(2016.2.26)
審判番号　不服2018-7271 (P2018-7271/J1)
審判請求日　平成30年5月29日(2018.5.29)
(31)優先権主張番号　13/932,828
(32)優先日　平成25年7月1日(2013.7.1)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　506223509
アマゾン・テクノロジーズ、インコーポレイテッド
アメリカ合衆国、９８１０８－１２２６
ワシントン州　シアトル　ピーオー　ボックス　８１２２６
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100103034
弁理士　野河　信久
(72)発明者　ポトラパリー、ナチケス・ラオ
アメリカ合衆国、ワシントン州　９８１０９－５２１０、シアトル、テリー・アベニュー・ノース　４１０

最終頁に続く

(54)【発明の名称】仮想マシンをホスティングする暗号的に保証されたリソース

(57)【特許請求の範囲】
【請求項１】
コンピュータ実施方法であって、
ユーザの仮想マシンをプロビジョニングする要求を受信すること、
前記要求の受信に応答して、前記仮想マシンを実行する１つまたは複数のリソースを含む、前記仮想マシンをホスティングするホスト・コンピューティング・デバイスを選択すること、
前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの暗号測定を得ること、ここにおいて、前記暗号測定は、前記ホスト・コンピューティング・デバイス上のソフトウエア及び／またはハードウェアのリソースのハッシュ測定を含み、
前記ユーザから前記ホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの特別な構成の選択を受信すること、
前記ホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの前記特別な構成に関連する既知の承認された暗号測定を決定すること、
前記暗号測定が、前記ホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの前記特別な構成に関連する前記承認された暗号測定と一致することを確認すること、及び
前記ユーザに、前記一致することの確認に基づいて、前記ホスト・コンピューティング・デバイス上の前記仮想マシンへのアクセスを提供すること、

を含む、コンピュータ実施方法。
【請求項２】
前記承認された暗号測定は、信頼ある第三者により作成され、前記信頼ある第三者により保証される、請求項１に記載のコンピュータ実施方法。
【請求項３】
ホスト・コンピューティング・デバイスの複数の構成に対する承認された暗号測定のリストを作成すること、及び
信頼ある第三者により保証してもらうために、承認された暗号測定の前記リストを前記信頼ある第三者に提供すること、
をさらに含む、請求項１に記載のコンピュータ実施方法。
【請求項４】
複数のユーザがネットワークでアクセス可能になるように、承認された暗号測定の前記リストが、前記信頼ある第三者によって公表される、請求項３に記載のコンピュータ実施方法。
【請求項５】
承認された暗号測定の前記リストが、前記仮想マシンをプロビジョニングする要求と同時に前記ユーザによって提供される、請求項３に記載のコンピュータ実施方法。
【請求項６】
前記暗号測定が、
前記ホスト・コンピューティング・デバイスの基本入出力システム（ＢＩＯＳ）に関連付けられた値、
前記ホスト・コンピューティング・デバイスのハイパーバイザの構成、
前記仮想マシンの起動オペレーティング・システムの構成、
１つまたは複数のハードウェア構成レジスタの値、または
周辺コンポーネント相互接続（ＰＣＩ）カードのファームウェア、
のうちの１つまたは複数に少なくとも一部基づく、請求項１に記載のコンピュータ実施方法。
【請求項７】
コンピューティング・システムであって、
少なくとも１つのプロセッサ、及び
前記プロセッサによって実行されたときに前記コンピューティング・システムに
ユーザの仮想マシンをプロビジョニングする要求を受信すること、
前記要求の受信に応答して、前記仮想マシンを実行する１つまたは複数のリソースを含む、前記仮想マシンをホスティングするホスト・コンピューティング・デバイスを選択すること、
前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの暗号測定を得ること、ここにおいて、前記暗号測定は、前記ホスト・コンピューティング・デバイス上のソフトウエア及び／またはハードウェアのリソースのハッシュ測定を含み、
前記ユーザから前記ホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの特別な構成の選択を受信すること、
前記ホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの前記特別な構成に関連する既知の承認された暗号測定を決定すること、
前記暗号測定が、前記ホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの前記特別な構成に関連する前記承認された暗号測定と一致することを確認すること、及び
前記ユーザに、前記一致することの確認に基づいて、前記ホスト・コンピューティング・デバイス上の前記仮想マシンへのアクセスを提供すること、
をさせる命令、
を含むメモリを含む、コンピューティング・システム。

【請求項８】
前記メモリが、前記コンピューティング・システムに
ホスト・コンピューティング・デバイスの複数の構成に対する承認された暗号測定のリストを作成すること、及び
信頼ある第三者により保証してもらうために、承認された暗号測定の前記リストを前記信頼ある第三者に提供すること、
をさせる、前記少なくとも１つのプロセッサによって実行される命令をさらに含む、請求項７に記載のコンピューティング・システム。
【請求項９】
前記メモリが、前記コンピューティング・システムに
複数のホスト・コンピューティング・デバイスのうちの少なくとも１つがパッチ付けされたかまたは更新されたことを判断すること、及び
承認された暗号測定の前記リストを新たな暗号測定で更新して前記ホスト・コンピューティング・デバイスに対するパッチまたは更新を構成すること、
をさせる、前記少なくとも１つのプロセッサによって実行される命令をさらに含む、請求項８に記載のコンピューティング・システム。
【発明の詳細な説明】
【背景技術】
【０００１】
本出願は、『仮想マシンをホスティングする暗号的に保証されたリソース』と題して２０１３年７月１日に出願されたＵ．Ｓ．１３／９３２８２８の優先権を主張するものであり、その全体がその全ての目的のために、ここに参照により援用される。
【０００２】
ますます多くのアプリケーション及びサービスがインターネットなどのネットワークを通して利用できるようになるにつれて、ますます多くのコンテンツ、アプリケーション及び／またはサービス・プロバイダが、クラウド・コンピューティングなどの技術に変わってきている。クラウド・コンピューティングは、一般に、ウェブ・サービスのようなサービスを通して電子リソースへのアクセスを提供することへのアプローチであり、そこでは、これらのサービスを支援するために使用されるハードウェア及び／またはソフトウェアが動的にスケーラブルであってどんなときでもサービスの必要性を満たす。典型的には、ユーザまたは顧客は、クラウドを通してリソースを借り、リソースをリースし、またはその反対にリソースへのアクセス料を支払い、したがって、必要なハードウェア及び／またはソフトウェアを購入し維持する必要がない。
【０００３】
この状況で、多くのクラウド・コンピューティングのプロバイダは仮想化を利用して多数のユーザが基礎となるハードウェア及び／またはソフトウェアのリソースを共有できるようにする。仮想化は、コンピューティング・サーバ、記憶装置または他のリソースが、特定のユーザ（例えば、顧客）に関係している（例えば、所有された）多数の分離されたインスタンス（すなわち、仮想マシン）に分割され得るようにすることができる。各仮想マシンは、従来、ユーザの代わりに１つまたは複数のアプリケーションを実行することができるそれ自身のオペレーティング・システムを含む。仮想化は、したがって、様々なユーザが、クラウド・コンピューティングのプロバイダまたはオペレータのリソース（例えば、ホスト・サーバなど）上で使用して、遠隔からアプリケーションを動作させることができるようにする。しかし、従来の仮想コンピューティング環境の提供をすることにはいくつかの制限がある。例えば、ある顧客は、遠隔のリソース上で仮想マシンを実行する結果発生するかもしれないセキュリティ問題に特に敏感である場合がある。顧客がこれらのリソースに物理的にアクセスしないので、多くの顧客がリソースが悪意のあるユーザによって不正に変更されたり、危険にさらされたりしていない、ある種の暗号の保証を得たいと思う。
【図面の簡単な説明】

【０００４】
本開示による様々な実施形態が以下の図面を参照して記述される。
【図１】様々な実施形態により使用することができる電子リソース環境の例を示す。
【図２】様々な実施形態による、仮想マシンがプロビジョニングされるホスト・コンピューティング・デバイス上でリソースの暗号測定を得る例を示す。
【図３】様々な実施形態による、信頼ある機関によって保証されている承認された測定のリストと暗号測定を比較する例を示す。
【図４】様々な実施形態による、ハイパーバイザを使用する１つの仮想化技術を利用する例を示す。
【図５】様々な実施形態による、仮想化コンピューティング環境を可能にするために使用することができる物理的リソースを提供するサービス・プロバイダのリソース・センタの例を示す。
【図６】様々な実施形態による、仮想化コンピューティング環境でユーザに提供することができる多数の仮想マシンの仮想ネットワークの例を示す。
【図７】様々な実施形態による、仮想マシンをホスティングするように構成されたコンピューティング・リソースを証明する方法の例を示す。
【図８】様々な実施形態による、承認された暗号測定のリストをコンパイルし、信頼ある第三者にリストを提供する方法の例を示す。
【図９】様々な実施形態により利用することができるコンピューティング・デバイスの１組の一般的なコンポーネントの論理的な配置を示す。
【図１０】様々な実施形態による態様を実行するための環境の例を示す。
【発明の詳細な説明】
【０００５】
以下の説明では、様々な実施形態が、添付図面の図に限定するためではなく例として示されるであろう。本開示での様々な実施形態への言及は、必ずしも同じ実施形態を指さず、かかる言及は少なくとも１つへの言及を意味する。特定の実装形態及び他の詳細が論じられているが、これが説明する目的のためだけになされたことを理解すべきである。当該技術の当業者なら、請求された主題の範囲及び趣旨から逸脱することなく、他のコンポーネント及び構成を使用できることを理解するであろう。
【０００６】
本開示の様々な実施形態によるシステム及び方法は、暗号的にコンピューティング・リソースを保証する従来の手法で経験した１つまたは複数の以前のまたは他の不備を克服することができる。特に、様々な実施形態は、仮想化マルチテナント・コンピューティング環境のオペレータが、ユーザ（例えば顧客、クライアントなど）の代わりに１つまたは複数の仮想マシンを実行するのに使用したコンピューティング・リソースに対して暗号的に証明し、かつ／または確認することができるようにする。ユーザが、仮想マシンをプロビジョニングしてもらうように要求するとき、仮想化コンピューティング環境のオペレータ（例えば、クラウド・コンピューティングのサービス・プロバイダ）は仮想マシンの２段階立ち上げを開始することができる。第１段階では、オペレータは、ホスト・コンピューティング・デバイス上に仮想マシンをプロビジョニングし、ホスト・コンピューティング・デバイス上でソフトウェア及び／またはハードウェアのリソースの暗号測定を得る。暗号測定は、信頼あるプラットフォーム・モジュール（ＴＰＭ）を用いて得ることができ、ＴＰＭの機器構成レジスタ（ＰＣＲ）に格納することができる。その後、オペレータは、仮想マシンを要求したユーザにこれらの暗号測定を提供することができる。ユーザが暗号測定を承認すれば、オペレータは第２段階を始めて、実際に、ホスト・コンピューティング・デバイス上で仮想マシンを立ち上げる（すなわち、実行を開始する）ことができる。いくつかの実施形態では、ユーザに暗号測定を供給する代わりに（または、加えて）、オペレータは、暗号測定を既知の測定または承認された測定（例えば「ホワイトリスト」）または他の基準値と比較してホスト・コンピューティング・デバイスが仮想マシンのホスティングに受け入れ可能かどうかを判断する。承認された暗号測定のリストは仮想マシン

をプロビジョニングする要求の一部としてユーザが提供することができるし、または、信頼ある機関（例えば、信頼ある第三者）が提供することもできる。

【０００７】

実施形態により、ユーザは、仮想化マルチテナント・コンピューティング環境のオペレータによって提供されるウェブ・サービスＡＰＩなどの１つまたは複数のアプリケーション・プログラミング・インターフェース（ＡＰＩ）を使用して仮想マシンに対する要求を提出する。いくつかの実施形態では、要求を提出する側として、ユーザは、ホスト・コンピューティング・デバイスの特別な機器構成を指定するか、または仮想マシンをプロビジョニングするときに使用される承認された暗号測定のリストを提供することができる。ユーザからのかかる要求を受け取って、オペレータ（例えばサーバ上で動作するサービス）は、ユーザの仮想マシンのプロビジョニングを開始することができる。特に、仮想マシンのプロビジョニングは、ホスト・コンピューティング・デバイスを選択することと、仮想マシンの機器構成を含むマシン・イメージを解凍し、ユーザのために仮想マシンをプロビジョニングするその他の必要なステップを行うことを含むことができる。一旦、仮想マシンがプロビジョニングされて、ホスト・コンピューティング・デバイス上で立ち上げられる（すなわち、実行される）準備ができれば、プロセスは休止され得、ホスト・コンピューティング・デバイス上の様々なソフトウェア及び／またはハードウェアのリソースの１つまたは複数の暗号測定を得ることができる。例えば、信頼のあるプラットフォーム・モジュール（ＴＰＭ）またはホスト・コンピューティング・デバイス上の他の暗号のモジュールが使用されてホスト・コンピューティング・デバイスのソフトウェア構成のハッシュ測定を行うことができる。ハッシュ測定はあるメモリ位置の値を読み取りこれらの値にハッシュ関数を適用してハッシュ測定をすることにより行うことができる。メモリ位置は、ホスト・コンピューティング・デバイスの基礎的入出力システム（ＢＩＯＳ）、ホスト・コンピューティング・デバイス上のハイパーバイザ（すなわち、仮想マシン・マネージャ）、仮想マシンのゲスト・オペレーティング・システムの構成、ハードウェア構成レジスタ、周辺機器相互接続（ＰＣＩ）カード上のファームウェアなどと関連付けられることができる。一実施形態では、ハッシュ測定は、ＴＰＭのＰＣＲに格納されるセキュア・ハッシュ・アルゴリズム１（ＳＨＡ－１）測定である。

【０００８】

一旦、暗号測定が得られたならば、それらはホスト・コンピューティング・デバイス上のリソースが仮想マシンを立ち上げるのに受け入れ可能な状態かどうかを判断するために使用することができる。一実施形態では、仮想化マルチテナント・コンピューティング環境のオペレータは、仮想マシンを要求したユーザに暗号測定（例えば、ＳＨＡ－１）を提供することができ、ユーザは仮想マシンを立ち上げる前に暗号測定を承認するかまたは拒否することができる。別の実施形態では、ユーザがホスト・コンピューティング・デバイスの特別な構成を、要求の一部として指定した場合、オペレータは、このホストの暗号測定と、指定された構成に対応した既知の承認された暗号測定（例えば、公知のＳＨＡ－１）とを比較することができる。別の実施形態では、ユーザが承認された暗号測定のリストをオペレータに提供すると（例えば、仮想マシンに対する要求の一部として、または異なる時間に）、オペレータは、この暗号測定を承認された測定のリストと比較して仮想マシンの立ち上げを承認するかまたは拒否するかを決定することができる。いくつかの実施形態では、承認された測定のリストは、多数のユーザ（例えば、インターネット上の）によるアクセスのリストを公表するなどの信頼ある第三者により保証され得る。

【０００９】

様々な実施形態で、オペレータがホスト・コンピューティング・デバイスの構成の暗号測定がいかなる基準値とも一致しないと判断すれば、オペレータはホスト・コンピューティング・デバイス上の仮想マシンをプロビジョニングするプロセスをロールバック、または取消すことができる。あるいは、オペレータは、仮想マシンがユーザの仮想ネットワークに加わるのを防ぐことなどの他の方法でユーザに仮想マシンを供給しなくてもよい。

【００１０】

図１は、様々な実施形態により使用することができる電子リソース環境１００の例を示す。この例において、エンド・ユーザのコンピューティング・デバイス１０２が、少なくとも１つのネットワーク１０６（例えば、インターネット、セルラー・ネットワーク、ワイヤレス・ネットワーク、ローカル・エリア・ネットワーク（ＬＡＮ）など）を介してコントロール・プレーン１０８内に呼び出しを行って、データ・プレーン１１０内でデータ・リポジトリをプロビジョニングするか、または仮想マシンを立ち上げるなどのタスクを行なうことができることが示される。ユーザまたはアプリケーション１０４は、例えば、データ・プレーン１１０インターフェースを介してリポジトリ及び／または仮想マシンに直接アクセスすることができる。エンド・ユーザのコンピューティング・デバイス及びアプリケーションは説明の目的で使用されているが、様々な実施形態において必要に応じて、いかなる適切なユーザ、アプリケーション、サービス、デバイス、コンポーネントまたはリソースもコントロール・プレーン及び／またはデータ・プレーンのインターフェースにアクセスすることができることを理解すべきである。さらに、コンポーネントがコントロール及びデータ「プレーン」に分けられると、少なくともいくつかのリソース（例えば、ハードウェア及び／またはソフトウェア）を論理的にまたは地理的に、実際のまたは仮想的分離と称し、それぞれ機能的に提供するよう使用されることに留意する。

【００１１】

この例におけるコントロール・プレーン１０８は、本質的に、プロビジョニング、インスタンス作成、立ち上げ、スケーリング、複製などの、制御活動及び管理活動を扱うハードウェア・コンポーネント及びソフトウェア・コンポーネントの仮想レイヤである。この実施形態でのコントロール・プレーンは、コンピュータ実行可能なソフトウェア、アプリケーション・サーバ、または他のかかるコンポーネントに併せて、例えば、少なくとも１つのウェブ・サーバを含むことができるウェブ・サービス・レイヤ１１２（すなわち、層）を含む。ウェブ・サービス・レイヤも、少なくとも１つのネットワーク１０６からのサービス、呼び出しまたは要求を受信する一組のＡＰＩ１３２（または、他のかかるインターフェース）を含むことができる。各ＡＰＩは、少なくとも１つの特殊なアクションがデータ環境に対して行われる要求を受け取るために設けてよい。ＡＰＩのうちの１つに対する要求を受け取る際、ウェブ・サービス・レイヤは、要求を解析または別の方法で分析して呼び出しに従って行動または処理するのに必要なステップまたはアクションを決定することができる。例えば、仮想マシンを立ち上げる要求を含むウェブ・サービス呼び出しが受け取られるかもしれない。この例では、ウェブ・サービス・レイヤは、要求を解析して、生成すべき仮想マシンのタイプ、要求されたハードウェアのタイプ（もしあれば）、または他のかかる態様を決定することができる。要求の情報は、後の処理のために、管理データ保管所、または他の適切な格納場所、またはジョブ・キューに書き込むことができる。

【００１２】

一実施形態でのウェブ・サービス・レイヤは、様々なコントロール・プレーンＡＰＩを提供することができ、ＡＰＩ仕様に基づいて適切な応答を返すことができる、顧客に対応するサーバのスケーラブルなセットを含む。ウェブ・サービス・レイヤは、一実施形態で外向きの顧客ＡＰＩを処理するステートレスな複製サーバからなる少なくとも１つのＡＰＩサービス・レイヤを含むこともできる。ウェブ・サービス・レイヤは、認証証明書に基づく顧客の証明、顧客の認可、ＡＰＩサーバに対する顧客の要求の絞り込み、ユーザ入力の妥当性検査、及び、要求と応答の秩序化または無秩序化などのウェブ・サービスのフロント・エンド・フィーチャに責任を負うことができる。ＡＰＩレイヤはまた、ＡＰＩ呼び出しに応答して管理データ・ストアから構成データを読み出しかつ管理データ・ストアに構成データを書き込むこともできる。多くの実施形態では、ウェブ・サービス・レイヤ及び／またはＡＰＩサービス・レイヤは、外部から見ることができる唯一のコンポーネント、すなわち、コントロール・サービスの顧客が見ることができアクセスすることができる唯一のコンポーネントになるであろう。ウェブ・サービス・レイヤのサーバは、当技術分野で知られるようにステートレスで垂直にスケーリングされ得る。ＡＰＩサーバならびに

永続データ・ストアは、例えば、サーバが単一のデータ・センタの故障に回復力があるように地域の多数のデータ・センタに散在することができる。ＡＰＩまたは他のかかるコンポーネントの機能または構成は、少なくとも１つのシステム・マネジメント・コンポーネント１１４あるいは他のかかるシステムまたはサービスによって管理することができる。

【００１３】

この実施形態でのコントロール・プレーン１０８は少なくとも１つのホスト・モニタリング・コンポーネント１１６を含む。ホスト・モニタリング・コンポーネントは、データ・プレーンの態様をモニタリングするための指示を含むハードウェア及び／またはソフトウェアのいかなる適切な組合せも含むことができる。例えば、ホスト・モニタリング・コンポーネントは、他のかかるオプションの間で、専用のホスト・マシン、いくつかのマシンにわたって分散されたプロセス、または、ウェブ・サービスを含むことができる。仮想マシン（ＶＭ）がデータ・プレーンに作成されるとき、ＶＭの情報は、モニタリング・データ・ストア１２０などのコントロール・プレーン内のデータ・ストアに書き込まれることができる。モニタリング・データ・ストアは、別個のデータ・ストアであり得、または管理データ・ストア１２２などの離散的なテーブルのセット、または適切なリポジトリなどの別のデータ・ストアの一部であり得る。ホスト・モニタリング・コンポーネント１１６は、モニタリング・データ・ストアにアクセスして、データ・プレーン１１０内のアクティブなＶＭ、リソース・インスタンス、あるいは他のかかるリソースまたはコンポーネント１３４を決定することができる。ホスト・モニタリング・コンポーネントはまた、ウェブ・サービス・レイヤ及び／または様々なホスト・マネージャ１２８などの、コントロール・プレーン及び／またはデータ・プレーンの複数のコンポーネントからログ及び／またはイベントの情報を集めることなどの他のタスクを行うこともできる。モニタリング・コンポーネントは、かかるイベント情報を用いて、顧客対応ＡＰＩを実施することなどの目的のために顧客が見ることができるイベントを露にすることができる。モニタリング・コンポーネントは、コントロール・プレーンのすべての動作中のリポジトリ及び／またはインスタンスの健全性を常にモニタリングし、これらのインスタンスのうちのいずれかの故障を検知し、適切な回復プロセスを開始することができる。

【００１４】

データ・プレーン内の仮想マシン・インスタンス１３４はそれぞれ、少なくとも１つのデータ・ストア１２６、及びデータ・ストアへのアクセスを提供するマシンのホスト・マネージャ・コンポーネント１２８を含むことができる。一実施形態でのホスト・マネージャは、データ・ストア及び／またはそれぞれのインスタンスの状態をモニタリングすることだけではなくソフトウェア配信及びデータ・ストア・オペレーションなどのタスクを管理するようにプログラムされた、インスタンス及び／またはトムキャットまたはジャバのアプリケーション・サーバなどのアプリケーション・サーバ上で実行するアプリケーションまたはソフトウェア・エージェントである。一実施形態でのホスト・マネージャは、内部システム・コンポーネントからのみ到達することができ顧客または他の外部機関が利用できないポートを聞く。いくつかの実施形態では、ホスト・マネージャはコントロール・プレーン・レイヤ内への呼び出しを開始できない。ホスト・マネージャは、データベース・バイナリ及びシーズをインストールすること、ならびにリポジトリを開始または停止することを含む、論理ボリューム及びファイル・システムの設定を含む新たなリポジトリのインスタンスを設定することなどのタスクを管理し且つ／または実施する責任を負うことができる。ホスト・マネージャは、Ｉ／Ｏエラーまたはデータ格納エラーなどのエラー条件のデータ・ストアをモニタリングするだけではなく、データ・ストアの健全性をモニタリングすることができ、必要なら、データ・ストアを再開することができる。ホスト・マネージャはまた、構成（例えば、特定の仮想マシン・イメージ）またはファームウェアなどに対する更新だけでなくソフトウェア・パッチ及びアップグレードのインストールを行い且つ／または管理することもできる。ホスト・マネージャはまた、ＣＰＵ、メモリ、及び／またはＩ／Ｏなどの使用に関連し得る指標を集めることもできる。

【００１５】

コントロール・プレーン１０８内のホスト・モニタリング・コンポーネント１１６は、例えば、特殊な要求を送るか、またはホスト・マネージャからのハートビートをモニタリングすることによって、モニタリングされた仮想マシン・インスタンス１３４の各ホスト・マネージャ１２８と定期的に通信して各ホストの状況を判断することができる。一実施形態では、モニタリング・コンポーネントは、例えば、特別なホスト及び／または仮想マシン・インスタンスの状況を得るために、各ホスト・マネージャにコマンドを出すように構成されたイベント・プロセッサ（または、モニタリング・サーバ）のセットを含む。少なくともいくつかの実施形態では、展開モニタ・コンポーネント１１８がまた、ホスト、インスタンス、及び他のかかるコンポーネントと通信して、いつバーションまたは構成が展開または更新されたか、いつ通信が送られたか、及び他のかかる情報を判断しようと試みることもできる。展開モニタは、コトロール・プレーンのモニタリング・サービスの一部として提供され得るため、ホスト・モニタの一部でもよく、またはホスト・モニタとは別個であってもよい。

【００１６】

論じてきたように、一旦仮想マシン・インスタンスがプロビジョニングされ、ユーザにＤＮＳアドレスあるいは他のアドレスまたは位置が提供されていれば、ユーザは、ジャバ・データベース接続性（ＪＤＢＣ）にネットワークを通してデータ・プレーン１１０に要求を「直接」送信するか、または他のかかるクライアントを用いて、インスタンス１３４と直接対話することができる。一実施形態では、データ・プレーンは、ハードウェア及び／またはソフトウェアのコンポーネントの「クラウド」または動的なネットワークを横切ってデータ保存及びデータ・アクセスを提供するコンピューティング・クラウド環境（あるいは、少なくとも含んでいるか、または一部分である）またはウェブ・サービス及びリソースのセットの形式をとる。インスタンスまたは可用性の障害が、例えば、プログラムによって覆われる場合があるので使用のための任意の適切な置換インスタンスにＤＮＳアドレスをプログラムで再マッピングすることによって覆い隠され得るため、ＤＮＳアドレスはかかるダイナミックなクラウド環境において有益である。ユーザ１０２またはアプリケーション１０４から受け取られた要求は、例えば、要求のＤＮＳに対応する実際のインスタンス１３４またはホストに要求を向けることができるネットワーク・アドレス変換（ＮＡＴ）ルータ１２４または他の適切なコンポーネントに向けることができる。論じたように、かかる手法は、ユーザまたはアプリケーションがインスタンスにアクセスするのに使用されたＤＮＳアドレスまたは他のアドレスの変更を要求することなく、インスタンスがダイナミックに移動され、更新され、複製されることなどを可能にする。論じたように、各インスタンス１３４は、例えば、ホスト・マネージャ１２８及びデータ・ストア１２６を含むことができ、永続的記憶装置１３０内に少なくとも１つのバックアップ・インスタンスまたはコピーを有することができる。かかる手法を用いて、インスタンスがコントロール・プレーンよって一旦構成されたならば、ユーザ、アプリケーション、サービスまたはコンポーネントは、コントロール・プレーン１０８にアクセスすることなく、データ・プレーンへの要求によってインスタンスと直接対話することができる。例えば、ユーザは、ＤＮＳアドレスを通してインスタンス内のデータに関係のあるＳＱＬまたは他のかかるコマンドを直接発行することができる。ユーザは、インスタンスの記憶装置の容量を拡大することなどのタスクを行いたければ、単にコントロール・プレーンにアクセスするだけでよいはずである。少なくとも１つの実施形態では、コントロール・プレーン１０８の機能性は、データ・プレーン１１０のプロバイダと関係していてもしていなくともよいプロバイダによる少なくとも１つのサービスとして提供することができるが、単に、データ・プレーン内の仮想マシン・インスタンスをプロビジョニングし管理するのに用いることができ、かつ、別個のデータ・プレーン１１０内のこれらのインスタンスの可用性をモニタリングし保証することもできる第三者のサービスであってもよい。

【００１７】

図２は、様々な実施形態による、仮想マシンがプロビジョニングされるホスト・コンピューティング・デバイス上のリソースの暗号測定を得る例２００を示す。ユーザ２０１な

どのあるユーザは、マルチテナント環境（例えば、クラウド・コンピューティング環境）でのプロビジョニングを仮想マシンに要求するときにセキュリティ問題に特に敏感であり得る。例えば、これらのユーザにとって仮想マシンが立ち上がる前に仮想マシン（すなわち、ハイパーバイザ・ハードウェアなど）を動作させるリソース・スタックを彼らが測定することができることは重要であり得る。これは、感染されていないマシン・イメージから起動された完全に妥当性のある仮想マシンであっても感染され易いホスト・コンピューティング・デバイス上で実行されるものは依然として問題があり、依然としてユーザのインフラストラクチャを感染させるおそれがあるからである。

【００１８】

これらのタイプのユーザに対しては、マルチテナント環境のオペレータは、ＢＩＯＳ、ハイパーバイザ３０８、ホスト・ドメイン２０７、ゲスト仮想マシン３０８、起動オペレーティング・システム（ＯＳ）、ハードウェア・コンフィギュレーション・レジスタ、周辺コンポーネント相互接続（ＰＣＩ）カード、及び／または、ホスト・コンピューティング・デバイス２０４上の他のリソースが特別な構成にあることの暗号保証を提供することができる。これが承認された構成または他の基準値と組み合わされると、ユーザ３０１は、ホスト・コンピューティング・デバイス上のリソース・インフラストラクチャが感染されておらず仮想マシンのホスティングに受け入れ可能であることを確認することができる。

【００１９】

一実施形態では、２段階の立上げプロセスが仮想マシンのプロビジョニングのために実行され得る。第１段階では、ユーザ２０１は、ウェブ・サービスＡＰＩ２０２などのＡＰＩを使用する仮想マシンを要求する。この要求は、対応するそれに関連する既知の承認された測定値を有したホスト・コンピューティング・デバイス上のリソースの特別な構成を指定することができる。要求に応じて、オペレータ（例えば、サーバ上で動作するプロビジョニング・サービス２０３）は、仮想マシンを載置するホスト・コンピューティング・デバイス２０４の選択、マシン・イメージのアンパッキングなどによって仮想マシンをプロビジョニングするプロセスを開始することができる。仮想マシンが一旦プロビジョニングされ、立ち上げられる準備ができていれば、ホスト・コンピューティング・デバイス２０４上のリソースの構成の１つまたは複数の暗号測定を得ることができる。例えば、ＴＰＭ２０５を用いて、ハイパーバイザ２０６、ホスト・ドメイン２０７及び／またはゲスト仮想マシン２０８の構成のハッシュ測定を行うことができる。これらの暗号測定は、ユーザの要求に応じてユーザに提供することができる。ユーザが暗号測定を承認すれば、それらは仮想マシンの立上げ（例えば、「継続する」のクリック）を受け入れることができ、インスタンスの立上げが完了する。あるいは、ユーザは測定を拒否（例えば、「中断」をクリック）することもでき、仮想マシンをプロビジョニングするプロセスが完了せず、そうでなければ仮想マシンがユーザに提供されない。

【００２０】

ユーザがそれらの仮想マシンがホスティングされるべき特別な構成を指定した実施形態では、マルチテナント環境のオペレータは、指定された構成に関連した既知の承認された暗号測定を検索することができる。この承認された測定はまた、測定が正しいことの保証をユーザに提供するために信頼ある第三者により保証してもらうこともできる。これらの実施形態では、オペレータは、暗号測定を承認するかまたは拒絶することをユーザに要求するよりはむしろ、既知のまたは承認された測定を検索し、それをホスト・コンピューティング・デバイスの暗号測定と比較することができる。次いで、比較に関する情報はユーザに提供することができる。あるいは、ユーザには、得られた暗号測定が既知の測定／承認された測定と一致したかどうかの指示とともに、要求を承認するか否定するかの選択が依然として提供することができる。

【００２１】

図３は、様々な実施形態による、暗号測定を信頼ある機関によって保証された承認済み測定のリストと比較する例３００を示す。図２を参照して以前に説明したように、ユーザ

３０１は、ＡＰＩ３０２を用いて仮想マシンをプロビジョニングしてもらう要求を提出することができる。プロビジョニング・サービス３０３は、ホスト・コンピューティング・デバイス３０４を選択し、ホスト・コンピューティング・デバイス上に仮想マシン３０８をプロビジョニングすることができる。仮想マシンを立ち上げる前に、プロセスが一時停止され、ホスト・コンピューティング・デバイス３０４上のＴＰＭ３０５の利用などによってリソース（例えば、ハードウェア及び／またはソフトウェアのソース）の暗号測定が得られる。例えば、ＴＰＭ３０５は、限定はされないがハイパーバイザ３０６及びホスト・ドメイン３０７を含む仮想マシン３０８をホスティングするソフトウェア・スタックのハッシュ測定３０９を得るのに用いることができる。

【００２２】

一旦、暗号測定３０９が得られれば、それがネットワーク・マネージャ３１２に提供される。ネットワーク・マネージャ３１２は、承認された暗号測定３１５のリストを検索し、暗号測定３０９を承認された測定３１５のリストと比較することができる。いくつかの実施形態では、信頼ある第三者機関３１１によって承認された測定３１５のリストが保証することができる。例えば、マルチテナント環境のオペレータは、ホスト・コンピューティング・デバイスのそれぞれの可能な構成のすべての承認された暗号測定のリストをコンパイルすることができる。このリストは、各暗号測定を検査しその精度を証明する、信頼のある第三者３１１に提供することができる。あるいは、信頼のある第三者３１１は、オペレータのリソースへのアクセスを得ることに基づいて承認された測定のリストを作成することができる。信頼のある第三者３１１はさらに、ユーザ３０１などの様々なユーザによるアクセスに対する承認された測定３１５のこのリストを公表することができる。これにより、ユーザがどの暗号測定がそれらの仮想マシンの立ち上げに受け入れ可能でどれがそうでないのかを判断する必要がないという意味でユーザ３０１にとってより容易となる。ユーザ３０１は、測定を検証し、それらが妥当で正しいことを確認したのは独立した第三者であるという仮定のもとで信頼ある第三者３１１を信用することができる。

【００２３】

以前に述べたように、仮想マシンは、仮想化コンピューティング環境のサービス・プロバイダまたは他のオペレータのリソース・センタに存在するホスト・コンピューティング・デバイス上で動作することができる。ホスト・コンピューティング・デバイス上では、いくつかの仮想化技術を用いて、複数のゲスト仮想マシンまたはゲスト・オペレーティング・システムを同時に動作させることができる。図４は、様々な実施形態による、ハイパーバイザを用いる一仮想化技術を利用する例４００を示す。ホスト・コンピューティング・デバイス４０１のハードウェア４０２は、そのハードウェア４０２（例えば、「ベア・メタル」またはナイーブ・ハイパーバイザ）上で直接動作するハイパーバイザ４０３と連動する。かかるハイパーバイザの例には、ゼン、ハイパーＶ（商標）などが含まれる。ハイパーバイザは、典型的には、マシン上の他のいかなるソフトウェアよりも速く、より権限が付与されたプロセッサ状態で動作し、従属するレイヤ及び／またはドメインのメモリ管理及びプロセッサ・スケジューリングなどのサービスを提供する。権限を付与されたかかるレイヤ及び／またはドメインは、サービス・ドメイン・レイヤ内に存在し、このレイヤは、ハイパーバイザ４０３のオペレーション及び機能性を構成する管理上のオペレーティング・システムを含み得るホスト・ドメイン４０４、ならびに、異機種環境（すなわち、互いに異なるオペレーティング・システムを動作させる）であり得るゲスト仮想マシンのドメイン（４０５、４０６、４０７）または他のオペレーティング・システムのドメインなどのより権限の低いドメインの管理上のオペレーティング・システムを含むことができる。ホスト・ドメイン４０４（例えば、ＤＯＭ－０）は、ハイパーバイザ４０３経由でホスト・コンピューティング・デバイス４０１のハードウェア・リソース４０２への直接のアクセスを有することができるが、他方、ゲスト仮想マシンのドメイン（４０５、４０６、４０７）はできない。

【００２４】

図５は、様々な実施形態による、仮想化コンピューティング環境を可能にするために使

用することができる物理的なリソースを提供するサービス・プロバイダのリソース・センタの例５００を示す。示した実施形態では、サービス・プロバイダ（または仮想化コンピューティング環境の他のオペレータ）は、サービス・プロバイダの物理的なリソース（例えば、ホスト・コンピューティング・デバイスなど）を格納する１つまたは複数のリソース・センタ５２３（例えばデータ・センタ、サーバ・ファームなど）を維持することができる。リソース・センタは、様々な地理的位置に位置してリソースへのより局所的なアクセスだけでなく改善された冗長性及びフェイルオーバーを提供することができる。物理的なリソースはインターネットなどのネットワーク５０２上のユーザ５０１に提供することができるいくつかの仮想マシンまたは仮想サーバをホスティングするために使用することができる。例えば、ユーザが、サービス・プロバイダの物理的なリソースを使用してアプリケーションを実行したいときは、ユーザは、アプリケーションを展開させて実行するのに使用されることになるユーザの仮想マシンのプロビジョニングをサービス・プロバイダに要求することができる。ユーザのアプリケーションに対する需要が増大するにつれて、ユーザは、負荷の平衡を保つためにより多くの仮想マシンがプロビジョニングされること、１つまたは複数の仮想ネットワークの生成などを要求することができる。

【００２５】

図示した例では、サービス・プロバイダのリソース・センタ５２３は、特定のラック上の各ホスト・コンピューティング・デバイスが単一のトップ・オブ・ラック（ＴＯＲ）スイッチ（５０４、５０５）に結合されている、ホスト・コンピューティング・デバイス（５０６、５０７、５０８、５０９、５１０）の１つまたは複数のラック５２１、５２２を含むことができる。これらのＴＯＲスイッチはさらに、ホスト・コンピューティング・デバイスをネットワークに接続することができるようにする１つまたは複数の他のスイッチ（５２４、５２５）に接続することができる。本開示の全体にわたって使用されるように、ネットワークは、限定はされないがインターネットあるいは他のワイド・エリア・ネットワーク（ＷＡＮ）、セルラー・ネットワーク、ローカル・エリア・ネットワーク（ＬＡＮ）、ストレージ・エリア・ネットワーク（ＳＡＮ）、イントラネット、エクトラネットなどを含む、互いに通信することができるデバイスの任意の有線または無線のネットワークであり得る。リソース・センタは、データ・センタ、サーバ・ファーム、コンテンツ・デリバリー・ネットワーク（ＣＤＮ）ポイント－オブ－プレゼンス（ＰＯＰ）などのリソースの任意の物理的または論理的なグルーピングを含むことができる。

【００２６】

一実施形態によれば、各ホスト・コンピューティング・デバイスは、サービス・プロバイダの顧客の代わりに様々なアプリケーション及びサービスを実行するためにこれらの顧客に対してプロビジョニングされた１つまたは複数の仮想マシン・インスタンス（５１３、５１４、５１５、５１６、５１７、５１８、５１９）をホスティングすることができる。各仮想マシンは、カーネル、ドライバ、プロセス管理などを含む、それ自身のオペレーティング・システム（ＯＳ）がプロビジョニングされ得る。

【００２７】

ある顧客が仮想マシン・インスタンスを得たいときは、この顧客は先ず、使用したいＶＭのタイプを示した要求をサービス・プロバイダに提出することができる。サービス・プロバイダ（または、他のオペレータ）は、諸プロセスを実行してサービス・プロバイダの物理的なリソース（例えば、ホスト・コンピューティング・デバイス）をホスティングすることになる仮想マシン・インスタンスをプロビジョニングすることができる。先に述べたように、ＶＭを要求するときに、ユーザは、ＶＭで使用される構成情報を指定することができる。

【００２８】

先に述べたように、仮想マシンがユーザに対してプロビジョニングされるとき、この仮想マシンはそのユーザに対してプロビジョニングされた仮想ネットワークに関連付けられることができる。図６は、様々な実施形態による、仮想化コンピューティング環境内のユーザに提供することができる複数の仮想マシンの仮想ネットワークの例６００を示す。先

に述べたように、サービス・プロバイダ（または仮想化コンピューティング環境の他のオペレータ）は、物理的なリソース（例えば、ホスト・コンピューティング・デバイスなど）を維持して、１つまたは複数のサービス・プロバイダの顧客に対して、様々な仮想マシン及び仮想ネットワーク６５１などの仮想ネットワークをホスティングするリソース・センタを提供することができる。いくつかの実施形態では、サービス・プロバイダは、サービス・プロバイダの様々な顧客が仮想ネットワークを作成し構成するために使用することができるネットワーク・サービスを提供することができる。

【００２９】

図示した例において、仮想ネットワーク６５１は、顧客の遠隔プライベート・コンピュータ・ネットワークに対するプライベート・ネットワークの拡張である。仮想ネットワーク６５１は、（例えば、地理的位置１に位置する第一のデータ・センタにおける）第一の地理的位置１（６６０）に位置する様々な仮想マシンを含む。仮想マシンは論理グループ６５７、６５８、６５９に（例えば、異なるサブネット及び図示していない関連するネットワーキング・デバイスに対応するために）構成することができる。この例では、起こり得る様々なタイプの通信を説明するために、これらの仮想マシンと他のコンピューティング・システムとの間の通信をコントロールするための単一の概念的仮想ルータ６５５が地理的位置１（６６０）に示されている。しかし、代替実施形態では、地理的位置１に複数のネットワーキング・デバイスがある場合もあり、まったくない場合もある。仮想ネットワークは、下層の物理的基板ネットワーク及び下層のネットワークにわたる通信をコントロールする関連モジュールなどを使用することによって、複数の物理的な相互接続ルータまたは他のネットワーキング・デバイスを介するなどの様々な方法で地理的位置１（６６０）に実装することができる。この例では、仮想ルータ６５５は、仮想ネットワーク６５１用の構成された情報であって、サービス・プロバイダによって提供されるネットワーク・サービスを用いて顧客が構成できるように構成されたネットワーク・トポロジ情報を含む情報に従って作動する。

【００３０】

この例では、仮想ネットワーク６５１は、例えば、顧客１に提供される、また顧客１のリモート・コンピュータ・ネットワークに対するネットワーク拡張である。顧客１のリモート・コンピュータ・ネットワークは、プライベート・ネットワーク・サイトＡ６５２などの第一の遠隔地で複数のコンピューティング・システム（図示せず）を含み、仮想ルータ６５５は、仮想通信リンク６５８を介してこれらの複数のコンピューティング・システムと通信するように構成される。例えば、仮想ネットワークは、サイトＡ６５２での複数のコンピューティング・システムへの１つまたは複数の構成された仮想プライベート・ネットワーク（ＶＰＮ）接続を含むことができ、通信リンク６５８は１つまたは複数のかかるＶＰＮ接続に対応することができる。加えて、顧客１のリモート・コンピュータ・ネットワークは、任意選択で、図示した任意選択のプライベート・ネットワーク・サイトＢ６５３などの他の１つまたは複数の位置にコンピューティング・システムを含むことができる。そして、もしそうであれば、仮想ルータ６５５は、さらに、サイトＢ６５３に対する任意選択の仮想通信リンク６５８などを介して（例えば、サイトＢに１つまたは複数の他の構成されたＶＰＮ接続を直接介して）それらの他の位置でこれらの他のコンピューティング・システムと通信するように構成することができる。複数のＶＰＮ接続または他の安全な接続がリモート・コンピュータ・ネットワークのリモート・コンピューティング・システムに使用されるときは、各接続は、通信が適切な接続に経路指定されるようにリモート・コンピューティング・システムのサブセットに（例えば、これらのコンピューティング・システムに対応するリモート・コンピュータ・ネットワークのネットワーク・アドレスのサブセットに関連付けられることによって）対応することができる。他の実施形態では、多数のＶＰＮ接続または他の安全な接続は１つまたは複数の位置でリモート・コンピューティング・システムに使用することができるが、複数の接続が冗長化の選択肢（例えば、負荷分散に使用される）であるなどの場合であれば、それぞれは、任意のリモート・コンピューティング・システムへの通信を支援することができる。さらに、いくつかの実

施形態では、クライアントのリモート・コンピュータ・ネットワークは複数のサイトに複数のコンピューティング・システムを含むことができるが、リモート・コンピューティング・システムに対する単一のＶＰＮ接続または他のセキュアな接続のみが、リモート・コンピュータ・ネットワークが適切なサイト及びコンピューティング・システムに対する通信のルーティンに責任を負った状態で、使用され得る。

【００３１】

加えて、仮想ネットワーク６５１は、仮想ネットワークの仮想マシンとインターネット６５４または他の公衆ネットワーク上で一般にアクセス可能な他の外部コンピューティング・システムとの間の通信のすべてまたはいくらかが許可されるかまたはすべてが許可されなくなるように構成することができる。かかる外部通信のうちの少なくともいくつかが許可される場合、仮想ルータ６５５はさらに、任意選択の仮想通信リンク６５９を介してこれらの複数の外部コンピューティング・システムと通信するように構成することができる。

【００３２】

図示した実施形態では、地理的位置１　６６０の仮想マシン（６５６、６５７、６５８）に加えて、仮想ネットワークはさらに、第二の地理的位置２　６６１（例えば、第二の地理的位置２の異なるリソース・センタ）に位置する仮想マシン６６５を含むことができる。したがって、仮想ルータ６５５は、地理的位置２　６６１の仮想ネットワークの部分との仮想通信リンク６６２を含むように構成することができる。この例では、地理的位置２　６６１の仮想ネットワークの部分が、同様に、仮想通信リンク６６３を介して地理的位置１　６６０の仮想ネットワークの部分と通信することを含む、仮想マシン６６５への通信及び仮想マシンからの通信を管理する概念的な仮想ルータ６６４と共に図示されている。異なる地理的位置の仮想ネットワークの仮想マシン間のかかる通信は、様々な実施形態で、インターネットまたは他の公衆ネットワーク（例えば、暗号を用いたセキュア・トンネルの部分としての）を横切って通信を送ること、個人的で安全な方法で（例えば、地理的位置間の専用線を介して）通信を送ること、などの様々な方法で扱うことができる。加えて、ここでは図示していないが、地理的位置２の仮想ネットワークの部分は、同様に、リモート・クライアント・プライベート・ネットワーク（例えば、地理的位置１への任意のＶＰＮ接続とは異なる１つまたは複数のＶＰＮ接続を介して）、インターネットなどへの他の仮想通信リンクを含むことができる。

【００３３】

以前に説明したように、仮想マシンがユーザ（例えば、顧客１）に対してプロビジョニングされるとき、この仮想マシンはそのユーザのネットワークに加えることができる。いくつかの実施形態では、ユーザは、承認された暗号測定のリストを提供し、彼らの仮想ネットワークに属するすべての仮想マシンが彼らの暗号測定の少なくとも１つと一致する必要があると指定することができる。これらの実施形態では、ユーザが追加の仮想マシンが彼らの仮想ネットワークに対してプロビジョニングされることを要求するとき、オペレータはホスト・コンピューティング・デバイスを選択し、このホストのリソースの暗号測定を行い、次に、これらの暗号測定をユーザにより最初に提供されていた承認された測定のリストと比較することができる。ホスト・コンピューティング・デバイス承認された測定の１つと一致しない場合、仮想マシンはユーザの仮想ネットワークに加えられない。

【００３４】

図７は、様々な実施形態による、仮想マシンをホスティングするように構成されたコンピューティング・リソースを保証するプロセス７００の例を示す。この図は機能的なオペレーションの特別なシーケンスを描くことができるが、これらのプロセスは必ずしもこの特別な順番または図示したオペレーションに限定されない。当業者なら、本図または他の図に描かれた様々なオペレーションは、変更し、再編成し、並行して行なうことができ、または、様々な方法で適用できることを理解するであろう。さらに、あるオペレーションまたはオペレーションのシーケンスが、様々な実施形態の範囲から逸脱することなくプロセスに追加するまたはプロセスから省くことができることを理解すべきである。加えて、

本明細書に含まれる絵は、異なるフローまたはシーケンスで実行されたり、性能のために最適化されたり、または、その他様々な方法で修正されたりすることができるコード実行の実際のシーケンスを特定するものではなく、プロセス・フローの考え方を当業者に明示することが意図されている。

【００３５】

オペレーション７０１では、ユーザに仮想マシンをプロビジョニングする要求が受信される。先に説明したように、この要求は１つまたは複数のＡＰＩにアクセスすることによってユーザが提出することができる。いくつかの実施形態では、ユーザは、要求を提出する一環として、ユーザの仮想マシンをホスティングするためにホスト・コンピューティング・デバイスが順守する必要がある特別な構成を指定することができる。要求の受信に応答して、マルチテナント環境のオペレータは、オペレーション７０２に示すように仮想マシンをホスティングするホスト・コンピューティング・デバイスを選択することができる。様々な実施形態では、選択されたホスト・コンピューティング・デバイスは、仮想マシンを実行するソフトウェア及びハードウェアのリソースを含む。例えば、これらのリソースは、デバイス上の複数の仮想マシンをホスティングするハイパーバイザ及びホスト・ドメイン（または、仮想マシン・モニタ）を含むことができる。

【００３６】

オペレーション７０３では、オペレータは、選択されたホスト・コンピューティング・デバイス上に仮想マシンをプロビジョニングする。一旦、仮想マシンがプロビジョニングされており、立ち上げの準備ができていれば、オペレーション７０４に示すように、オペレータはホスト・コンピューティング・デバイス上のソフトウェア及び／またはハードウェアのリソース構成の暗号測定（例えば、ハッシュ測定）を行う。いくつかの実施形態では、ホスト・コンピューティング・デバイスに埋め込まれたＴＰＭは、暗号測定を行う際に利用することができる。

【００３７】

オペレーション７０５では、オペレータは、承認された暗号測定のリストを検索する。様々な実施形態では、この承認されたハッシュ測定のリストは、ユーザが提供することができるか、またはオペレータがコンパイルすることができ、信頼ある第三者によって保証することができる。さらに他の実施形態では、信頼ある第三者が、承認された暗号測定のリストにユーザがインターネットでアクセスすることができるようにすることなどでこのリストを公表することができる。一旦、このリストが得られると、選択されたホスト・デバイス上で行われたハッシュ測定を承認されたハッシュ測定のリストと比較して、選択されたホスト・コンピューティング・デバイス上のリソースが仮想マシンをホスティングするのに受け入れ可能かどうかを判断することができる。もし、暗号測定が承認された測定リストの測定の１つと一致する場合、仮想マシンは、オペレーション７０６に示すように、ホスト・コンピューティング・デバイス上で立ち上げられる。ユーザが、元の要求の一環として、ホスト・コンピューティング・デバイスの特別な構成を指定している実施形態では、承認された測定のいかなるリストも必要としなくてもよい。より正確に言えば、ＴＰＭによって得られた暗号測定を、ホストの構成が受け入れ可能かどうか判断するためにユーザが指定した特別な構成に対応する既知の承認された測定と単に比較することができる。いくつかの実施形態では、測定が一致するかどうかに関する情報は、この情報を提供するＡＰＩにユーザをアクセス可能にすることなどによってユーザに提供し直すことができる。

【００３８】

図８は、様々な実施形態による、承認された暗号測定のリストをコンパイルし、このリストを信頼のある第三者に提供するプロセス８００の例を示す。オペレーション８０１では、マルチテナント環境のオペレータは、承認された暗号測定のリストならびにこれらの測定に対応するソフトウェア及び／またはハードウェアの構成をコンパイルする。オペレーション８０２では、承認された測定のリストが信頼ある第三者に提供される。信頼ある第三者は承認された測定を分析し、それらの精度を保証することができる。一旦、信頼の

ある第三者が測定のリストの精度を保証すると、先に説明したように、様々なユーザが彼らの仮想マシンを要求するときにリスト内の測定に頼ることができる。

【００３９】

オペレーション８０３では、マルチテナント環境のオペレータは時々、仮想マシンをホスティングするのに使用される様々なリソース（例えば、ハイパーバイザなど）を更新するか、またはそれらにパッチを当てることができる。例えば、マルチテナント環境のサービス・プロバイダまたはオペレータはマルチテナント環境にインフラストラクチャ及び新しいコンポーネント（例えば、異なるＢＩＯＳなどを備えた新しいハードウェア）を導入することができる。多くの場合、かかる更新、パッチまたは新コンポーネントは、それらのリソースに対して新しい暗号測定が行われることを要求することができる。オペレーション８０４では、オペレータは、更新されたリソースに対応する新しい暗号測定を行い、オペレーション８０５では、オペレータは、これらの測定を信頼ある第三者に提供する。その後、信頼のある第三者がこれらの新たな暗号測定を保証し、ユーザはそれらの測定に頼り続けることができる。

【００４０】

本開示の実施形態は、以下の条項を考慮して説明することができる。

１．非一時的なコンピュータ可読媒体であって、１つまたは複数のプロセッサよって実行されたときにコンピューティング・システムに、

マルチテナント・コンピューティング環境をホスティングするサービス・プロバイダの顧客から受けた顧客の仮想マシンをプロビジョニングする要求を受けること、

複数のホスト・コンピューティング・デバイスから前記仮想マシンを実行する１つまたは複数のリソースを含むある１つのホスト・コンピューティング・デバイスを選択して前記仮想マシンをホスティングすること、

前記選択されたホスト・コンピューティング・デバイス上に前記仮想マシンをプロビジョニングすること、

前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの構成のハッシュ測定を行うこと、

前記１つまたは複数のリソースの前記構成が前記仮想マシンをホスティングするのに許容できるかどうかの指示であって、前記ハッシュ測定と承認されたハッシュ測定のリストとの比較に少なくとも部分的に基づいた指示を前記顧客から得ること、及び

前記１つまたは複数のリソースの前記構成が受け入れ可能である前記指示に応答して前記選択されたホスト・コンピューティング・デバイス上に前記仮想マシンを立ち上げること、

をさせる非一時的なコンピュータ可読媒体。

２．承認されたハッシュ測定の前記リストは信頼ある第三者により保証された信頼あるリストである、項１に記載の非一時的なコンピュータ可読媒体。

３．前記ハッシュ測定が、

前記ホスト・コンピューティング・デバイスの基本入出力システム（ＢＩＯＳ）に関連付けられた値、

前記ホスト・コンピューティング・デバイスのハイパーバイザの構成、

前記仮想マシンの起動オペレーティング・システムの構成、

１つまたは複数のハードウェア構成レジスタ内の値、または

周辺コンポーネント相互接続（ＰＣＩ）カード内のファームウェア

のうちの１つまたは複数に少なくとも部分的に基づいている、項１に記載の非一時的なコンピュータ可読媒体。

４．１つまたは複数のプロセッサによって実行されるコンピューティング・システムに

前記仮想マシンをプロビジョニングする前記要求に応答して前記顧客に前記ハッシュ測定を提供すること、

をさせる命令をさらに含む、項１に記載の非一時的なコンピュータ可読媒体。

５．コンピュータ実施方法であって、実行可能な命令から構成される１つまたは複数の

コンピュータ・デバイスのコントロール下で、
ユーザの仮想マシンをプロビジョニングする要求を受信すること、
前記仮想マシンを実行する１つまたは複数のリソースを含む、前記仮想マシンをホスティングするホスト・コンピューティング・デバイスを選択すること、
前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの暗号測定を得ること、及び
前記ユーザに、前記暗号測定と１つまたは複数の基準値との比較に少なくとも一部基づいて、前記ホスト・コンピューティング・デバイス上の前記仮想マシンへのアクセスを提供するかどうかを判断すること、
を含む、コンピュータ実施方法。
６．前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
前記ユーザから前記ホスト・コンピューティング・デバイスの構成の選択を受信すること、
前記ホスト・コンピューティング・デバイスの選択された構成に関連する承認された暗号測定を決定すること、及び
前記暗号測定が前記ホスト・コンピューティング・デバイスの選択された構成に関連する承認された前記暗号測定と一致することを確認すること、
をさらに含む、項５に記載のコンピュータ実施方法。
７．前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
前記仮想マシンをプロビジョニングする前記要求に応答して前記ユーザに前記暗号測定を提供すること、
前記暗号測定が前記ユーザに承認されたかどうかを示した指示を前記ユーザから受信すること、及び、
前記暗号測定が承認されたことの指示を受信することに応答して前記ホスト・コンピューティング・デバイス上に前記仮想マシンを立ち上げること、
をさらに含む、項５に記載のコンピュータ実施方法。
８．前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
承認された暗号測定のリストを検索すること、
前記暗号測定を承認された暗号測定の前記リストと比較して前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースが前記仮想マシンをホスティングするのに許容できるかを判断すること、及び、
前記１つまたは複数のリソースが受け入れ可能との判断に応答して前記選択されたホスト・コンピューティング・デバイス上に前記仮想マシンを立ち上げること、
をさらに含む、項５に記載のコンピュータ実施方法。
９．前記１つまたは複数の参照値が、
信頼ある第三者により作成され前記信頼ある第三者により保証された、承認済み暗号測定を、
さらに含む、項５に記載のコンピュータ実施方法。
１０．ホスト・コンピューティング・デバイスの複数の構成に対する承認された暗号測定のリストをコンパイルすること、及び
承認された暗号測定の前記リストを信頼ある第三者に提供して前記信頼ある第三者により保証してもらうこと、
をさらに含む、項５に記載のコンピュータ実施方法。
１１．複数のホスト・コンピューティング・デバイスのうちの１つがパッチ付けされたかまたは更新されたことを判断すること、及び
承認された暗号測定の前記リストを新たな暗号測定で更新して前記ホスト・コンピューティング・デバイスに対するパッチまたは更新を構成すること、
をさらに含む、１０項に記載されたコンピュータ実施方法。
１２．承認された暗号測定の前記リストが、信頼ある第三者によって公表されて複数のユーザがネットワークでアクセス可能になる、１０項に記載のコンピュータ実施方法。

１３．承認された暗号測定の前記リストが、前記仮想マシンをプロビジョニングする要求と同時に前記ユーザによって提供される、項８に記載のコンピュータ実施方法。
１４．前記ハッシュ測定が、
前記ホスト・コンピューティング・デバイスの基本入出力システム（ＢＩＯＳ）に関連付けられた値、
前記ホスト・コンピューティング・デバイスのハイパーバイザの構成、
前記仮想マシンの起動オペレーティング・システムの構成、
１つまたは複数のハードウェア・レジスタの値、または
周辺コンポーネント相互接続（ＰＣＩ）カードのファームウェア、
のうちの１つまたは複数に少なくとも一部基づく、項５に記載のコンピュータ実施方法。
１５．コンピューティング・システムであって、
少なくとも１つのプロセッサ、及び
前記プロセッサによって実行されたときに前記コンピューティング・システムに
ユーザの仮想マシンをプロビジョニングする要求を受信すること、
前記仮想マシンを実行する１つまたは複数のリソースを含む、前記仮想マシンをホスティングするホスト・コンピューティング・デバイスを選択すること、
前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの暗号測定を得ること、及び
前記ユーザに、前記暗号測定と１つまたは複数の基準値との比較に少なくとも一部基づいて、前記ホスト・コンピューティング・デバイス上の前記仮想マシンへのアクセスを提供するかどうかを判断すること、
をさせる命令、
を含む、コンピューティング・システム。
１６．前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
前記ユーザから前記ホスト・コンピューティング・デバイスの構成の選択を受信すること、
前記ホスト・コンピューティング・デバイスの選択された構成に関連する承認された暗号測定を決定すること、及び
前記暗号測定が前記ホスト・コンピューティング・デバイスの選択された構成に関連する承認された前記暗号測定と一致することを確認すること、
をさらに含む、項１５に記載のコンピューティング・システム。
１７．前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
前記仮想マシンをプロビジョニングする前記要求に応答して前記ユーザに前記暗号測定を提供すること、
前記暗号測定が前記ユーザに承認されたかどうかを示した指示を前記ユーザから受信すること、及び、
前記暗号測定が承認されたことの指示を受信することに応答して前記ホスト・コンピューティング・デバイス上に前記仮想マシンを立ち上げること、
をさらに含む、項１５に記載のコンピューティング・システム。
１８．前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
承認された暗号測定のリストを検索すること、
前記暗号測定と承認された暗号測定の前記リストとを比較して前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースが前記仮想マシンをホスティングするのに受け入れ可能かを判断すること、及び、
前記１つまたは複数のリソースが受け入れ可能との判断に応答して前記選択されたホスト・コンピューティング・デバイス上に前記仮想マシンを立ち上げること、

をさらに含む、項１５に記載のコンピューティング・システム。
１９．前記メモリが、前記コンピューティング・システムに
ホスト・コンピューティング・デバイスの複数の構成に対する承認された暗号測定のリストをコンパイルすること、及び
承認された暗号測定の前記リストを信頼ある第三者に提供して前記信頼ある第三者により保証してもらうこと、
をさせる、少なくとも１つのプロセッサによって実行される命令をさらに含む、項１５に記載のコンピューティング・システム。
２０．前記メモリが、前記コンピューティング・システムに
複数のホスト・コンピューティング・デバイスのうちの１つがパッチ付けされたかまたは更新されたことを判断すること、及び
承認された暗号測定の前記リストを新たな暗号測定で更新して前記ホスト・コンピューティング・デバイスに対するパッチ
または更新を構成すること、
をさせる、少なくとも１つのプロセッサによって実行される命令をさらに含む、項１９に記載のコンピューティング・システム。
２１．承認された暗号測定の前記リストが、信頼ある第三者によって公表されて複数のユーザがネットワークでアクセス可能になる、項１９に記載のコンピューティング・システム。
２２．承認された暗号測定の前記リストが、前記仮想マシンをプロビジョニングする要求と同時に前記ユーザによって提供される、項１８に記載のコンピューティング・システム。

【００４１】

図９は、一例のコンピューティング・デバイス９００の一般的なコンポーネント・セットの論理的な配置を示す。この例では、デバイスは、メモリ・デバイスまたはメモリ素子９０４に格納することができる命令を実行するプロセッサ９０２を含む。当業者には明らかであるはずであるが、デバイスは、多くのタイプのメモリ、データ・ストレージ、または、プロセッサ９０２が実行するプログラム命令用の第一のデータ・ストレージ、画像またはデータ用の別個のストレージ、他のデバイスと情報を共有するための着脱式メモリなどの非一時的コンピュータ可読記憶媒体を含むことができる。このデバイスは典型的には、タッチ・スクリーンや液晶ディスプレイ（ＬＣＤ）などのいくつかのタイプの表示素子９０６を含むであろうが、ポータブルメディア・プレイヤーなどのデバイスは、オーディオ・スピーカなどの他の手段を介して情報伝達することができるはずである。論じたように、多くの実施形態でのデバイスは、ユーザから従来の入力を受信することができる少なくとも１つの入力素子９０８を含むであろう。従来の入力素子は、例えば、押しボタン、タッチ・パッド、タッチ・スクリーン、ホイール、ジョイスティック、キーボード、マウス、キーパッド、またはそれによってユーザがデバイスにコマンドを入力できる任意のかかるデバイスまたは素子を含むことができる。しかし、いくつかの実施形態では、かかるデバイスは、ボタンを全く含まないで、ユーザがデバイスに接する必要なしにデバイスをコントロールできるように視覚的及び聴覚的なコマンドの組合せを介してのみコントロールできるはずである。いくつかの実施形態では、図９のコンピューティング・デバイス９００は、Ｗｉ－Ｆｉ、ブルートゥース（登録商標）、ＲＦ、有線または無線の通信システムなどの様々なネットワークで通信するための１つまたは複数のネットワーク・インターフェース素子９０８を含むことができる。多くの実施形態におけるデバイスは、インターネットなどのネットワークと通信することができ、他のかかるデバイスと通信することができる場合がある。

【００４２】

論じたように、説明した実施形態により異なる手法を様々な環境で実装することができる。例えば、図１０は、様々な実施形態による態様を実装する環境１０００の例を示す。これから分かるように、ウェブ・ベースの環境が説明の目的で使用されているが、必要に

応じて、様々な実施形態を実装するために異なる環境を使用してもよい。このシステムは、電子的なクライアント・デバイス１００２であって、適切なネットワーク１００４で要求、メッセージまたは情報を送受信し、かつデバイスのユーザに情報を伝え戻す働きをするものを含む。かかるクライアント・デバイスの例には、パーソナル．コンピュータ、携帯電話、携帯型通信デバイス、ラップトップ・コンピュータ、セット－トップ・ボックス、パーソナル・データ・アシスタント、電子ブック・リーダ、などが含まれる。ネットワークには、イントラネット、インターネット、セルラー・ネットワーク、ローカル・エリア・ネットワークまたは他の任意のかかるネットワークまたはそれらの組み合わせを含む任意の適切なネットワークを含むことができる。かかるシステムに使用されるコンポーネントは、ネットワークのタイプ及び／または選択された環境に少なくとも一部左右され得る。かかるネットワークを介して通信するプロトコル及びコンポーネントは周知であり、本明細書では詳細を論じない。ネットワークでの通信を、有線接続または無線接続及びそれらの組み合わせを介して可能にすることができる。この環境が要求を受信しそれに応答してコンテンツを提供するウェブ・サーバ１００６を含むため、この例ではネットワークはインターネットを含む。しかし、当業者には明らであるように、他のネットワークに対して同様の目的に役立つ代替デバイスを用いることができるはずである。

【００４３】

例示の環境には、少なくとも１つのアプリケーション・サーバ１００８及びデータ・ストア１０１０が含まれる。鎖状に繋がるかまたは他の方法で構成された、いくつかのアプリケーション・サーバ、レイヤまたは他の要素、プロセスまたはコンポーネントが存在できることを理解すべきであり、これらは相互に作用して、適切なデータ・ストアからデータを得ることなどのタスクを果たすことができる。本明細書で使用されるとき、用語「データ・ストア」は、データを格納し、データにアクセスし、データを検索することができる任意のデバイスまたはデバイスの組み合わせを指し、任意の標準的な、分散化またはクラスタ化した環境における、データ・サーバ、データベース、データ格納デバイス及びデータ格納媒体の任意の組み合わせと任意の数を含むことができる。アプリケーション・サーバは、必要ならデータ・ストアと一体化されてクライアント・デバイスの１つまたは複数のアプリケーションの態様を実施し、アプリケーションに対するデータ・アクセス及びビジネス・ロジックの大部分を扱う任意の適切なハードウェア及びソフトウェアを含むことができる。アプリケーション・サーバは、データ・ストアと協力してアクセス制御サービスを提供し、この例ではＨＴＭＬ、ＸＭＬまたは他の適切な構造化言語の形態のウェブ・サーバによってユーザに提供され得る、テキスト、グラフィックス、オーディオ及び／またはビデオなどのユーザに転送すべきコンテンツを作ることができる。すべての要求及び応答の扱い、ならびにクライアント・デバイス１００２とアプリケーション・サーバ１００８の間でのコンテンツの送達の扱いは、ウェブ・サーバ１００６によって扱うことができる。本明細書で論じた構造化コードは、本明細書の別のところで論じたような任意の適切なデバイスまたはホスト・マシン上で実行することができるので、ウェブ・サーバ及びアプリケーション・サーバは必要なものではなく、単なる例示的なコンポーネントであることを理解すべきである。

【００４４】

データ・ストア１０１０は特別な態様に関係したデータを格納するいくつかの別個のデータ・テーブル、データベースまたは他のデータ記録機構及び媒体を含むことができる。例えば、例示したデータ・ストアは、生産側にコンテンツを提供するのに使用することができる生産データ１０１２及びユーザ情報７１６を格納する機構を含む。データ・ストアは、また、ログまたはセッションのデータ１０１４を格納する機構も含むことが示されている。ページ画像情報、アクセス権情報などのデータ・ストアに格納される必要のある多くの他の態様が存在し得ることを理解すべきである。これらは、必要に応じて、上記に挙げた機構のうちの任意のものまたはデータ・ストア１０１０内の追加的な機構に格納することができる。データ・ストア１０１０は、それに関連付けられた論理によってアプリケーション・サーバ１００８から命令を受信することができ、それに応答してデータを得、

更新し、またはデータにそれ以外の処理をすることができる。一例では、ユーザはあるタイプの品目を検索する要求を提出することができるはずである。この場合、データ・ストアは、ユーザ情報にアクセスしてユーザの身元を確認できるはずであり、カタログ詳細情報にアクセスしてそのタイプの品目の情報を得ることができる。次いで、この情報は、ユーザがユーザ・デバイス１００２上のブラウザを介して見ることができるウェブページ上の結果一覧表などの形でユーザに戻すことができる。興味のある特別な品目の情報はブラウザの専用ページまたは専用ウィンドウで見ることができる。

【００４５】

各サーバは、典型的にはそのサーバの一般管理及びオペレーションのために実行可能なプログラム命令を提供するオペレーティング・システムを含むであろう、また、典型的には、サーバのプロセッサによって実行されたときにサーバの意図した機能をサーバが行なうことができるようにする命令を格納したコンピュータ可読媒体を含むであろう。サーバのオペレーティング・システム及び一般的な機能に適した実装形態は、公知であるか、または市販されている。また、特に、本明細書の開示に照らせば、当業者によって容易に実施される。

【００４６】

一実施形態での環境は、１つまたは複数のコンピューター・ネットワークまたは直接接続を使用し通信リンクを介して相互接続された、いくつかのコンピュータ・システム及びコンポーネントを利用する分散型コンピューティング環境である。しかし、かかるシステムが図１０に例示されたコンポーネントよりも数が少ないかまたは多いコンポーネントを有するシステムにおいて同様にうまく動作できるはずであることは当業者には明らかであろう。したがって、図１０のシステム１０００の描写は、本来、例示的なものであるとみなされるべきであり本開示の範囲を限定するものとみなされるべきではない。

【００４７】

本明細書で議論または示唆された様々な実施形態は、ある場合にはいくつかのアプリケーションのうちの任意のものを操作するのに使用することができる１つまたは複数のユーザ・コンピュータ、コンピューティング・デバイス、または処理デバイスを含むことができる、多種多様な操作環境で実施することができる。ユーザ・デバイスまたはクライアント・デバイスは、標準オペレーティング・システムを動作させるデスクトップ・コンピュータまたはラップトップ・コンピュータなどのいくつかの汎用のパーソナル・コンピュータのうちの任意のものと、モーバイル・ソフトウェアを動作させ、ネットワーキング・プロトコル及びメッセージング・プロトコルのいくつかを支援することができるセルラー・デバイス、無線デバイス及び携帯デバイスを含むことができる。かかるシステムはまた、開発及びデータベース管理などの目的で様々な市販のオペレーティング・システムならびに他の公知のアプリケーションのうちの任意のものを実行するいくつかのワークステーションを含むこともできる。これらのデバイスはまた、ダミー端子、シン・クライアント、ゲーミング・システム、及びネットワークを介して通信することができる他のデバイスなどの他の電子デバイスを含むこともできる。

【００４８】

ほとんどの実施形態は、ＴＣＰ／ＩＰ、ＦＴＰ、ＵＰｎＰ、ＮＦＳ及びＣＩＦＳなどの様々な市販のプロトコルのうちの任意のものを使用して通信を支援する当業者によく知られた少なくとも１つのネットワークを利用する。このネットワークは、例えば、ローカル・エリア・ネットワーク、広域ネットワーク、仮想プライベート・ネットワーク、インターネット、イントラネット、エクストラネット、公衆交換電話網、赤外線ネットワーク、ワイヤレス・ネットワーク及びそれらの任意の組合せであり得る。

【００４９】

ウェブ・サーバを利用する実施形態では、ウェブ・サーバは、ＨＴＴＰサーバ、ＦＴＰサーバ、ＣＧＩサーバ、データ・サーバ、ジャバ・サーバ及びビジネス・アプリケーション・サーバを含む様々なサーバまたは中間層のアプリケーションのうちのいずれかを動作させることができる。サーバはまた、例えば、ジャバ（登録商標）、Ｃ、Ｃ＃またはＣ＋

＋などの任意のプログラミング言語、あるいはパール、パイソンまたはＴＣＬなどの任意のスクリプト言語、ならびにそれらの組み合わせで書かれた１つまたは複数のスクリプトまたはプログラムを実行することによって、ユーザ・デバイスからの要求に応じてプログラムまたはスクリプトを実行することができる場合もある。サーバはまた、限定はされないが、オラクル（商標）、マイクロソフト（商標）、サイベース（商標）、及びＩＢＭ（商標）を含むデータベース・サーバを含むこともできる。

【００５０】

環境は、上記で論じたような様々なデータ・ストア及び他の記録・記憶媒体を含むことができる。これらは、１つまたは複数のコンピュータに局在した（及び／または存在する）記憶媒体上、またはネットワーク全域の任意のまたはすべてのコンピュータから遠く離れた記憶媒体上などの様々な場所に存在し得る。特定の実施形態では、情報は、当業者によく知られているストレージ・エリア・ネットワーク（「ＳＡＮ」）に存在する場合がある。同様に、コンピュータ、サーバまたは他のネットワーク・デバイスに起因する機能を果たすいかなる必要なファイルも、必要なら、ローカルに及び／または遠隔で格納される場合がある。システムがコンピュータ化されたデバイスを含む場合は、かかるデバイスはそれぞれ、バスを介して電気結合できるハードウェア素子であって、例えば、少なくとも１つの中央処理装置（ＣＰＵ）、少なくとも１つの入力装置（例えば、マウス、キーボード、コントローラ、タッチ・スクリーン、またはキーパッド）及び少なくとも１つの出力装置（例えば、ディスプレイ装置、プリンタ、またはスピーカ）を含む素子を、含むことができる。かかるシステムはまた、リムーバブル・メディア装置、メモリーカード、フラッシュカードなどと同様に、ディスク・ドライブ、光記憶装置、及び、ランダム・アクセス・メモリ（「ＲＡＭ」）または読み取り専用メモリ（「ＲＯＭ」）などの固体記憶装置などの１つまたは複数の記憶装置も含み得る。

【００５１】

かかるデバイスはまた、コンピュータ可読記憶媒体リーダ、通信装置（例えば、モデム、ネットワーク・カード（無線または有線の）、赤外線通信装置など）及び上述したような作業メモリを含むことができる。コンピュータ可読記憶媒体リーダは、遠隔の、ローカルな、固定の、及び／または取り外し可能な記憶装置、並びに、コンピュータ可読情報を一時的及び／またはより永久的に含み、格納し、送信し、検索する記憶媒体を表すコンピュータ可読記憶媒体と接続することができるかまたはそれを受け入れるように構成することができる。システム及び様々なデバイスはまた、典型的には、クライアント・アプリケーションまたはウェブ・ブラウザなどのオペレーティング・システム及びアプリケーション・プログラムを含む、いくつかの、ソフトウェア・アプリケーション、モジュール、サービスまたは少なくとも１つの作業メモリ・デバイス内に位置する他の要素を含むであろう。代替実施形態が、上記で説明した実施形態の多くの変形を有し得ることは理解されるべきである。例えば、カスタマイズされたハードウェアも使用され得るはずであり、かつ／または、特定の要素がハードウェア、ソフトウェア（アプレットなどの高移植性ソフトウェアを含む）または両方で実装され得るはずである。さらに、ネットワーク入出力装置などの他のコンピューティング・デバイスへの接続が採用され得る。

【００５２】

コードまたはコードの部分を含むための記憶媒体及びコンピュータ可読媒体は、当技術分野で知られているかまたは使用されている任意の適切な媒体であって、限定はされないが、コンピュータ可読命令、データ構造、プログラム・モジュールまたは他のデータなどの情報の格納及び／または送信のための任意の方法または技術において実装された、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ（登録商標）、フラッシュ・メモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、ディジタル多用途ディスク（ＤＶＤ）または他の光記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置また他の磁気記憶装置、あるいは所望の情報を格納するのに使用することができシステム機器によってアクセスされ得る他の媒体を含む、揮発性及び不揮発性で、取り外し可能及び取り外し不可能な媒体などの記憶媒体及び通信媒体を含む、媒体を含むことができる。当業者なら、本明細書に提供された開示及び教示に

基づいて、様々な実施形態を実行する他のやり方及び／または方法を理解するであろう。
【００５３】
したがって、明細書と図面は、限定的な意味ではなく例示的なものとみなすべきである。しかし、特許請求の範囲に記述されたような発明のより広い趣旨と範囲から逸脱することなく、それに様々な修正と変更を加え得ることは明らかであろう。
以下に、本願出願の当初の特許請求の範囲に記載された発明を付記する。
〔１〕
コンピュータ実施方法であって、実行可能な命令から構成される１つまたは複数のコンピュータ・システムの制御下で、
ユーザの仮想マシンをプロビジョニングする要求を受信すること、
前記仮想マシンを実行する１つまたは複数のリソースを含む、前記仮想マシンをホスティングするホスト・コンピューティング・デバイスを選択すること、
前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの暗号測定を得ること、及び
前記ユーザに、前記暗号測定と１つまたは複数の基準値との比較に少なくとも一部基づいて、前記ホスト・コンピューティング・デバイス上の前記仮想マシンへのアクセスを提供するかどうかを判断すること、
を含む、コンピュータ実施方法。
〔２〕
前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
前記ユーザから前記ホスト・コンピューティング・デバイスの構成の選択を受信すること、
前記ホスト・コンピューティング・デバイスの選択された構成に関連する承認された暗号測定を決定すること、及び
前記暗号測定が前記ホスト・コンピューティング・デバイスの選択された構成に関連する承認された前記暗号測定と一致することを確認すること、
をさらに含む、〔１〕に記載のコンピュータ実施方法。
〔３〕
前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
前記仮想マシンをプロビジョニングする前記要求に応答して前記ユーザに前記暗号測定を提供すること、
前記暗号測定が前記ユーザに承認されたかどうかを示した指示を前記ユーザから受信すること、及び、
前記暗号測定が承認されたことの指示を受信することに応答して前記ホスト・コンピューティング・デバイス上に前記仮想マシンを立ち上げること、
をさらに含む、〔１〕に記載のコンピュータ実施方法。
〔４〕
前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
承認された暗号測定のリストを検索すること、
前記暗号測定と承認された暗号測定の前記リストとを比較して、前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースが前記仮想マシンをホスティングするのに許容できるかを判断すること、及び、
前記１つまたは複数のリソースが許容できるとの判断に応答して、前記選択されたホスト・コンピューティング・デバイス上に前記仮想マシンを立ち上げること、
をさらに含む、〔１〕に記載のコンピュータ実施方法。
〔５〕
前記１つまたは複数の基準値が、
信頼ある第三者により作成され前記信頼ある第三者により保証された、承認済み暗号測定のリストを、
さらに含む、〔１〕に記載のコンピュータ実施方法。

〔６〕
ホスト・コンピューティング・デバイスの複数の構成に対する承認された暗号測定のリストをコンパイルすること、及び
承認された暗号測定の前記リストを信頼ある第三者に提供して前記信頼ある第三者により保証してもらうこと、
をさらに含む、〔１〕に記載のコンピュータ実施方法。
〔７〕
承認された暗号測定の前記リストが、前記信頼ある第三者によって公表されて複数のユーザがネットワークでアクセス可能になる、〔６〕に記載のコンピュータ実施方法。
〔８〕
承認された暗号測定の前記リストが、前記仮想マシンをプロビジョニングする要求と同時に前記ユーザによって提供される、〔４〕に記載のコンピュータ実施方法。
〔９〕
前記ハッシュ測定が、
前記ホスト・コンピューティング・デバイスの基本入出力システム（ＢＩＯＳ）に関連付けられた値、
前記ホスト・コンピューティング・デバイスのハイパーバイザの構成、
前記仮想マシンの起動オペレーティング・システムの構成、
１つまたは複数のハードウェア・レジスタの値、または
周辺コンポーネント相互接続（ＰＣＩ）カードのファームウェア、
のうちの１つまたは複数に少なくとも一部基づく、〔１〕に記載のコンピュータ実施方法。
〔１０〕
コンピューティング・システムであって、
少なくとも１つのプロセッサ、及び
前記プロセッサによって実行されたときに前記コンピューティング・システムに
ユーザの仮想マシンをプロビジョニングする要求を受信すること、
前記仮想マシンを実行する１つまたは複数のリソースを含む、前記仮想マシンをホスティングするホスト・コンピューティング・デバイスを選択すること、
前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースの暗号測定を得ること、及び
前記ユーザに、前記暗号測定と１つまたは複数の基準値との比較に少なくとも一部基づいて、前記ホスト・コンピューティング・デバイス上の前記仮想マシンへのアクセスを提供するかどうかを判断すること、
をさせる命令、
を含むメモリを含む、コンピューティング・システム。
〔１１〕
前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
前記ユーザから前記ホスト・コンピューティング・デバイスの構成の選択を受信すること、
前記ホスト・コンピューティング・デバイスの選択された構成に関連する承認された暗号測定を決定すること、及び
前記暗号測定が前記ホスト・コンピューティング・デバイスの選択された構成に関連する承認された前記暗号測定と一致することを確認すること、
をさらに含む、〔１０〕に記載のコンピューティング・システム。
〔１２〕
前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
前記仮想マシンをプロビジョニングする前記要求に応答して前記ユーザに前記暗号測定を提供すること、
前記暗号測定が前記ユーザに承認されたかどうかを示した指示を前記ユーザから受信す

ること、及び、
前記暗号測定が承認されたことの指示を受信することに応答して前記ホスト・コンピューティング・デバイス上に前記仮想マシンを立ち上げること、
をさらに含む、〔１０〕に記載のコンピューティング・システム。
〔１３〕
前記ユーザに前記仮想マシンへのアクセスを提供するかどうかを判断することが、
承認された暗号測定のリストを検索すること、
前記暗号測定と承認された暗号測定の前記リストとを比較して、前記選択されたホスト・コンピューティング・デバイス上の前記１つまたは複数のリソースが前記仮想マシンをホスティングするのに許容できるかを判断すること、及び、
前記１つまたは複数のリソースが許容できるとの判断に応答して、前記選択されたホスト・コンピューティング・デバイス上に前記仮想マシンを立ち上げること、
をさらに含む、〔１０〕に記載のコンピューティング・システム。
〔１４〕
前記メモリが、前記コンピューティング・システムに
ホスト・コンピューティング・デバイスの複数の構成に対する承認された暗号測定のリストをコンパイルすること、及び
承認された暗号測定の前記リストを信頼ある第三者に提供して前記信頼ある第三者により保証してもらうこと、
をさせる、少なくとも１つのプロセッサによって実行される命令をさらに含む、〔１０〕に記載のコンピューティング・システム。
〔１５〕
前記メモリが、前記コンピューティング・システムに
複数のホスト・コンピューティング・デバイスのうちの１つがパッチ付けされたかまたは更新されたことを判断すること、及び
承認された暗号測定の前記リストを新たな暗号測定で更新して前記ホスト・コンピューティング・デバイスに対するパッチまたは更新を構成すること、
をさせる、少なくとも１つのプロセッサによって実行される命令をさらに含む、〔１４〕に記載のコンピューティング・システム。

【図１】

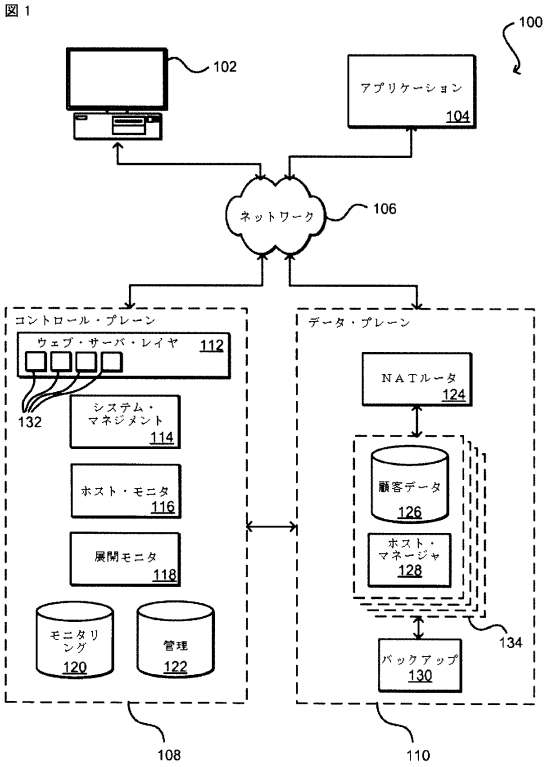
図１
100
102
アプリケーション
104
ネットワーク
106
コントロール・プレーン
ウェブ・サーバ・レイヤ
112
132
システム・
マネジメント
114
ホスト・モニタ
116
展開モニタ
118
モニタリ
ング
120
管理
122
データ・プレーン
NATルータ
124
顧客データ
126
ホスト・
マネージャ
128
134
バックアップ
130
108
110

【図２】

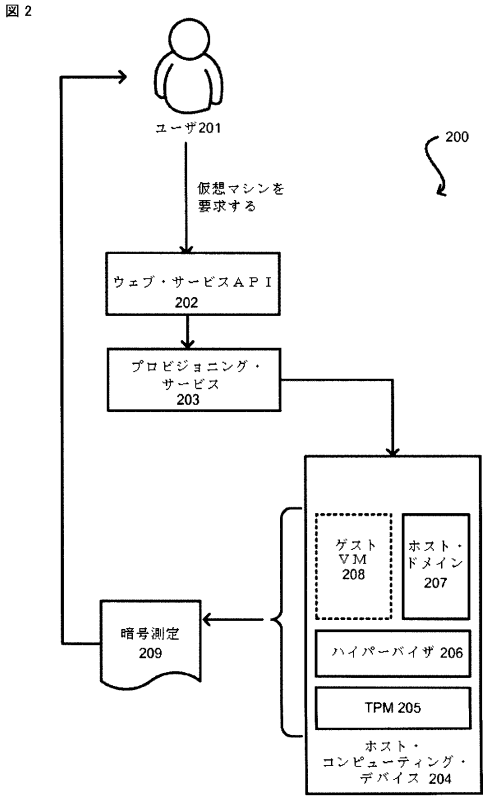
図２
ユーザ201
200
仮想マシンを
要求する
ウェブ・サービスＡＰＩ
202
プロビジョニング・
サービス
203
ゲスト
ＶＭ
208
ホスト・
ドメイン
207
暗号測定
209
ハイパーバイザ 206
TPM 205
ホスト・
コンピューティング・
デバイス 204

【図３】

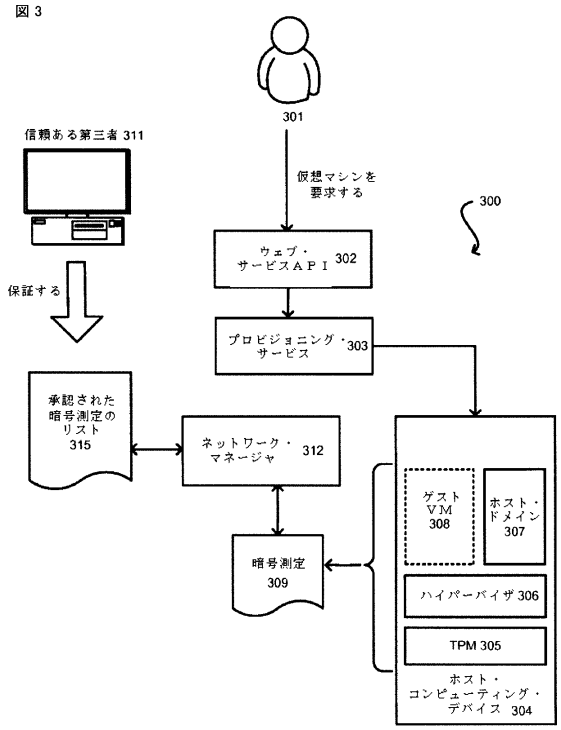
図３
301
信頼ある第三者 311
仮想マシンを
要求する
300
ウェブ・
サービスＡＰＩ 302
保証する
プロビジョニング・
サービス 303
承認された
暗号測定の
リスト
315
ネットワーク・
マネージャ 312
ゲスト
ＶＭ
308
ホスト・
ドメイン
307
暗号測定
309
ハイパーバイザ 306
TPM 305
ホスト・
コンピューティング・
デバイス 304

【図４】

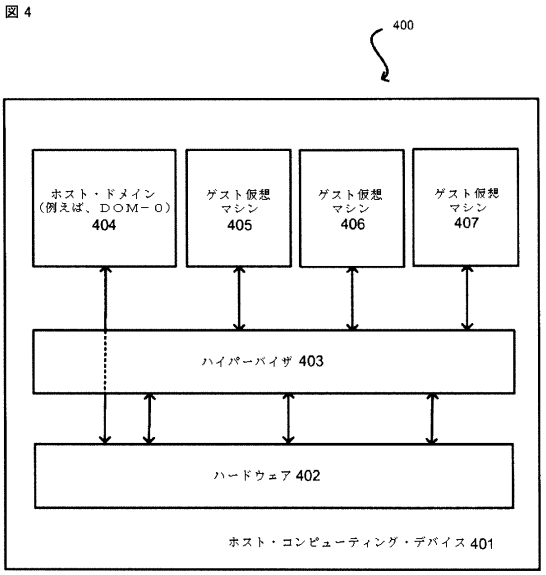
図４
400
ホスト・ドメイン
（例えば、ＤＯＭ－０）
404
ゲスト仮想
マシン
405
ゲスト仮想
マシン
406
ゲスト仮想
マシン
407
ハイパーバイザ 403
ハードウェア 402
ホスト・コンピューティング・デバイス 401

【図５】

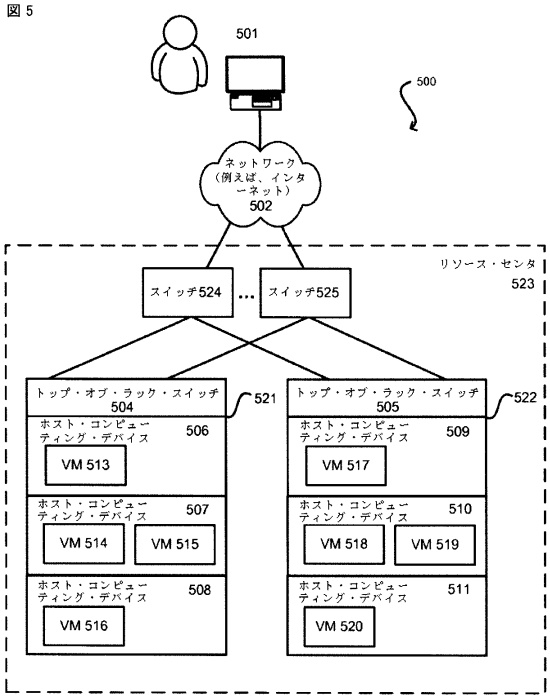
図５
501
500
ネットワーク（例えば、インターネット）
502
リソース・センタ
523
スイッチ524
スイッチ525
トップ・オブ・ラック・スイッチ
504
521
トップ・オブ・ラック・スイッチ
505
522
ホスト・コンピューティング・デバイス
506
VM 513
ホスト・コンピューティング・デバイス
507
VM 514
VM 515
ホスト・コンピューティング・デバイス
508
VM 516
ホスト・コンピューティング・デバイス
509
VM 517
ホスト・コンピューティング・デバイス
510
VM 518
VM 519
ホスト・コンピューティング・デバイス
511
VM 520

【図６】

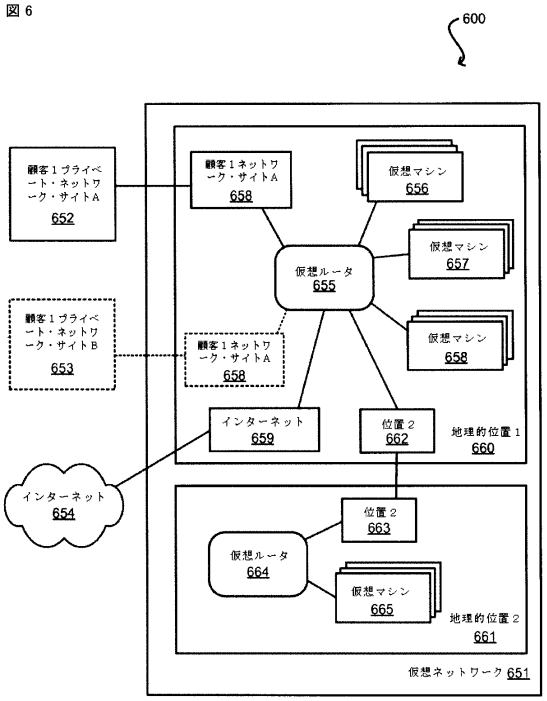
図６
600
顧客１プライベート・ネットワーク・サイトA
652
顧客１ネットワーク・サイトA
658
仮想マシン
656
仮想マシン
657
仮想ルータ
655
顧客１プライベート・ネットワーク・サイトB
653
顧客１ネットワーク・サイトA
658
仮想マシン
658
インターネット
659
位置２
662
地理的位置１
660
インターネット
654
位置２
663
仮想ルータ
664
仮想マシン
665
地理的位置２
661
仮想ネットワーク 651

【図７】

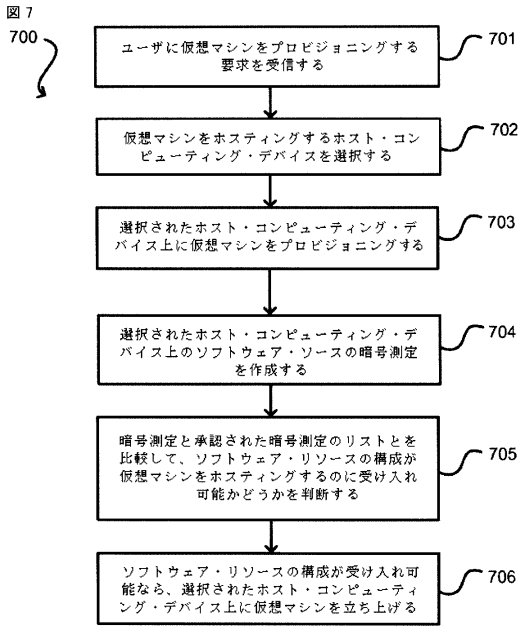
図７
700
ユーザに仮想マシンをプロビジョニングする要求を受信する
701
仮想マシンをホスティングするホスト・コンピューティング・デバイスを選択する
702
選択されたホスト・コンピューティング・デバイス上に仮想マシンをプロビジョニングする
703
選択されたホスト・コンピューティング・デバイス上のソフトウェア・ソースの暗号測定を作成する
704
暗号測定と承認された暗号測定のリストとを比較して、ソフトウェア・リソースの構成が仮想マシンをホスティングするのに受け入れ可能かどうかを判断する
705
ソフトウェア・リソースの構成が受け入れ可能なら、選択されたホスト・コンピューティング・デバイス上に仮想マシンを立ち上げる
706

【図８】

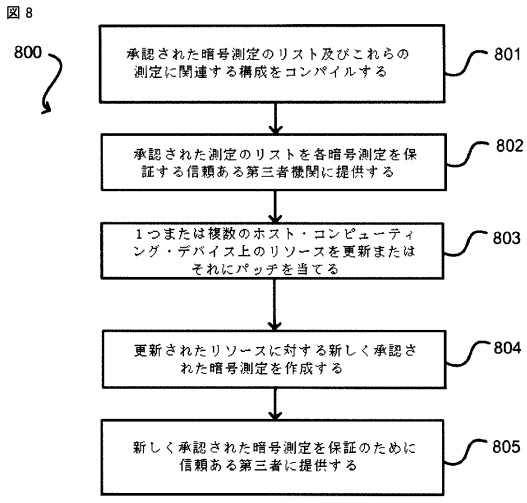
図８
800
承認された暗号測定のリスト及びこれらの測定に関連する構成をコンパイルする
801
承認された測定のリストを各暗号測定を保証する信頼ある第三者機関に提供する
802
１つまたは複数のホスト・コンピューティング・デバイス上のリソースを更新またはそれにパッチを当てる
803
更新されたリソースに対する新しく承認された暗号測定を作成する
804
新しく承認された暗号測定を保証のために信頼ある第三者に提供する
805

【図９】

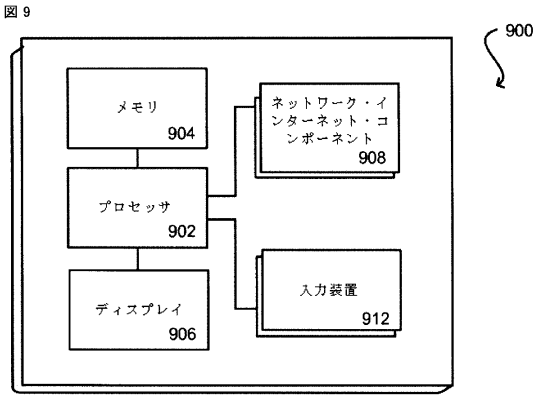
図 9
900
メモリ
904
ネットワーク・インターネット・コンポーネント
908
プロセッサ
902
入力装置
912
ディスプレイ
906

【図１０】

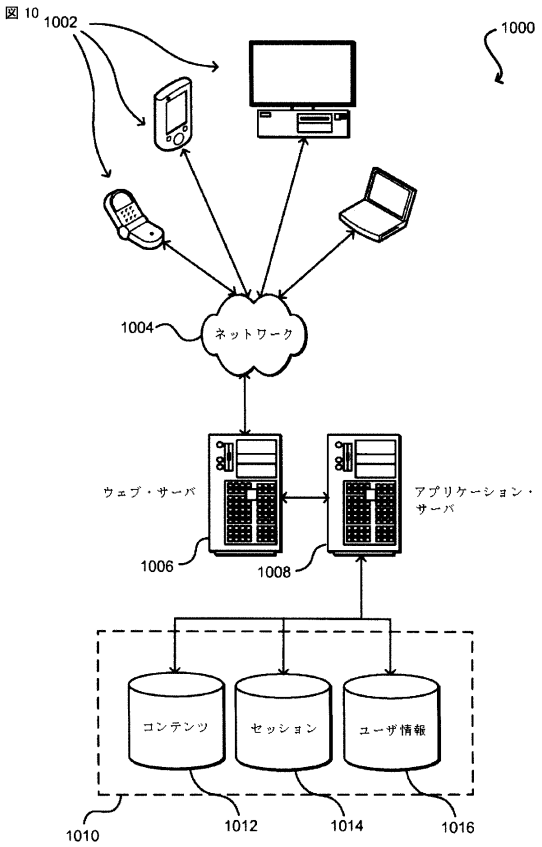
図 10
1002
1000
1004
ネットワーク
ウェブ・サーバ
アプリケーション・サーバ
1006
1008
コンテンツ
セッション
ユーザ情報
1010
1012
1014
1016

フロントページの続き

(72)発明者　ブランドワイン、エリック・ジェイソン
アメリカ合衆国、ワシントン州　９８１０９－５２１０、シアトル、テリー・アベニュー・ノース　４１０
(72)発明者　ウィルソン、マシュー・シャウン
アメリカ合衆国、ワシントン州　９８１０９－５２１０、シアトル、テリー・アベニュー・ノース　４１０

合議体
審判長　辻本　泰隆
審判官　須田　勝巳
審判官　山崎　慎一

(56)参考文献　特開２０１２－１９０４４１（ＪＰ，Ａ）
米国特許出願公開第２００８／００８３０３９（ＵＳ，Ａ１）
特開２０１２－１９８６３１（ＪＰ，Ａ）
特開２０１２－２０８５８０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 9/46
G06F 9/48
G06F 9/50- 9/52
G06F 9/54
G06F21/12-21/16
G06F21/50-21/57