(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6463269号
(P6463269)
(45)発行日　平成31年1月30日(2019.1.30)　(24)登録日　平成31年1月11日(2019.1.11)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675B
H04L 9/08	(2006.01)	H04L	9/00	601C
G06F 21/44	(2013.01)	G06F	21/44	

請求項の数 7　(全 13 頁)

(21)出願番号	特願2015-537002(P2015-537002)
(86)(22)出願日	平成25年10月15日(2013.10.15)
(65)公表番号	特表2015-532561(P2015-532561A)
(43)公表日	平成27年11月9日(2015.11.9)
(86)国際出願番号	PCT/US2013/065000
(87)国際公開番号	WO2014/059438
(87)国際公開日	平成26年4月17日(2014.4.17)
審査請求日	平成28年10月4日(2016.10.4)
(31)優先権主張番号	13/651,380
(32)優先日	平成24年10月12日(2012.10.12)
(33)優先権主張国	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　100108501
弁理士　上野　剛史

最終頁に続く

(54)【発明の名称】データ・センター内のデータ・センター・サーバで実行される仮想ディスク・イメージの地理的位置を確認するための方法、システム、およびコンピュータ・プログラム製品

(57)【特許請求の範囲】

【請求項１】

データ・センター内の、仮想ディスク・イメージを実行するデータ・センター・サーバの地理的位置を確認するための方法であって、

前記データ・センターのテナントからの構成証明要求に応答して、前記データ・センター・サーバ内の暗号化プロセッサが構成証明識別鍵を生成するステップと、

前記構成証明識別鍵によって署名された前記仮想ディスク・イメージのディスク・イメージ・ハッシュ値、前記構成証明識別鍵の公開される半分、前記構成証明識別鍵の前記公開される半分を認証するデジタル証明書、および前記暗号化プロセッサに一意の承認鍵の公開される半分をデータ・センターのテナントに送信するステップであって、前記承認鍵の秘密の半分が、前記データ・センター・サーバ内の前記暗号化プロセッサに記憶される、前記送信するステップと、

前記承認鍵の前記公開される半分に合致する前記暗号化プロセッサの地理的位置を、前記データ・センター内の位置プロバイダによって前記データ・センターのテナントに送信するステップとを含む、方法。

【請求項２】

前記暗号化プロセッサの前記地理的位置を送信するステップが、前記位置プロバイダによって無線周波数識別（ＲＦＩＤ）タグを読むステップを含み、前記ＲＦＩＤタグが前記暗号化プロセッサによって保持される、請求項１に記載の方法。

【請求項３】

前記位置プロバイダは、前記データ・センターの所有者が物理的にアクセス不可能である、請求項１に記載の方法。
【請求項４】
前記データ・センターで実行するために前記データ・センターのテナントから前記仮想ディスク・イメージを受信するステップをさらに含む、請求項１に記載の方法。
【請求項５】
前記データ・センター・サーバのコンピュータ・プロセッサによって前記ディスク・イメージ・ハッシュ値を計算するステップをさらに含む、請求項１に記載の方法。
【請求項６】
前記構成証明識別鍵の公開される半分をハイパーバイザを介して認証局に送信するステップと、
前記認証局から前記デジタル証明書を受信するステップと
をさらに含む、請求項１に記載の方法。
【請求項７】
データ・センター内の、仮想ディスク・イメージを実行するデータ・センター・サーバの地理的位置を確認するためのシステムであって、
前記データ・センター・サーバ内の暗号化プロセッサであって、前記暗号化プロセッサに一意の承認鍵を含み、前記データ・センターのテナントからの構成証明要求に応答して構成証明識別鍵を生成する、前記暗号化プロセッサと、
前記構成証明識別鍵によって署名された前記仮想ディスク・イメージのディスク・イメージ・ハッシュ値、前記暗号化プロセッサに発行された前記構成証明識別鍵の公開される半分に関するデジタル証明書、前記構成証明識別鍵の前記公開される半分、および前記承認鍵の公開される半分をデータ・センターのテナントに送信するように構成されたハイパーバイザと、
前記承認鍵に合致する前記暗号化プロセッサの地理的位置を前記データ・センターのテナントに送信するように構成された前記データ・センター内の位置プロバイダとを含む、システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、実行される仮想ディスク・イメージまたはワークロードの地理的位置の確認に関し、より詳細には、クラウド・コンピューティング環境内のサーバの実行されるワークロードの地理的位置の確認に関する。
【背景技術】
【０００２】
いくつかの場合、顧客が、それらの顧客のワークロードが実行される正確な物理的位置を確かめることが望ましい。これは、規制要件のためである可能性があり、例えば、特定のデータは、特定の管轄区域（国、州など）内で実行されるアプリケーションによってのみ処理され得るか、またはこれは、ワークロードが物理的セキュリティに関するコンプライアンスの基準を含むコンプライアンスの基準を満たすデータ・センター内で実行されることを確認する必要性のためである可能性がある。ワークロードがそのような地理的位置または準拠したデータ・センターの外にマイグレーションする場合、脆弱な物理的セキュリティまたはＩＴセキュリティが、セキュリティの侵害またはデータの喪失あるいはその両方につながる可能性がある。
【０００３】
サーバの地理的位置を判定する当技術分野における従来の研究は、以下の４つの手法のうちの１つに基づく。
【０００４】
１．サーバのＩＰアドレスを使用する：世界のそれぞれの地理的地域は、効率を目的として階層的なルーティング・テーブルが使用されることを可能にするためにＩＰアドレス

の一意のブロックを割り振られる。ゆえに、サーバのＩＰアドレスを用いてそのサーバのおよその地理的位置を判定することができる。そのようなサービスは、インターネットでの汎用的な使用のために利用され得る（例えば、http://www.ipaddresslocation.org/で公表されたサービス）。

【０００５】

２．例えばtracerouteまたはpingコマンドによる遅延時間の測定を使用する：地理的位置が知られているインターネット上の複数のホストからそのサーバへのtracerouteまたはpingの時間を測定することによってサーバの地理的位置を判定することができる。

【０００６】

３．サーバに組み込まれた無線受信機を使用する：サーバは、地理的位置が知られている無線ビーコン、またはセル電話の電波塔もしくはＧＰＳ衛星からの信号を受信することができる無線受信機を備えている場合、そのサーバの地理的位置を判定することができる可能性がある。そのとき、サーバは、そのサーバの地理的位置をクライアントに伝達することができる。

【０００７】

４．直接的な人の観察：サーバの物理的位置を特定する要求を受信すると、サーバは、クラウド・プロバイダがサーバの位置を特定することを可能にする人が感知することができる信号を生成する。そのとき、クラウド・プロバイダは、この位置情報をクライアントに与える。

【発明の概要】

【発明が解決しようとする課題】

【０００８】

上述の技術のすべては、位置が判定されるべきサーバのオペレータまたは管理者が、使用されている技術の動作を妨害しないと信じられることを仮定する。

【課題を解決するための手段】

【０００９】

したがって、本発明の１つの例示的な態様は、データ・センター内のデータ・センター・サーバで実行される仮想ディスク・イメージの地理的位置を確認するための方法である。方法は、承認鍵（endorsement key）によって署名された仮想ディスク・イメージのディスク・イメージ・ハッシュ値、承認鍵の公開される半分、および承認鍵の公開される半分を認証するデジタル証明書をデータ・センターのテナントに送信するステップを含む。承認鍵の秘密の半分は、データ・センター・サーバの近くの暗号化プロセッサ（cryptoprocessor）に記憶され、暗号化プロセッサに一意である。さらに、デジタル証明書は、暗号化プロセッサに発行される。次に、位置プロバイダ（location provider）が、承認鍵の公開される半分に合致する暗号化プロセッサの地理的位置をデータ・センターのテナントに送信する。

【００１０】

本発明と考えられる対象は、添付の特許請求の範囲で特に示され、明確に特許請求される。本発明の上述のおよびその他の目的、特徴、および利点は、添付の図面と関連してな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】

【００１１】

【図１】本発明の一実施形態による、データ・センター内のデータ・センター・サーバで実行される仮想ディスク・イメージの地理的位置を確認するための方法を示す図である。

【図２】本発明の一実施形態による、データ・センター内のデータ・センター・サーバで実行される仮想ディスク・イメージの地理的位置を確認するためのシステムを示す図である。

【図３】各サーバがデータセンター内の各データ・センター・サーバのための公開鍵を保有する耐タンパー性のＲＦＩＤチップを備えるシステムとしての本発明の別の実施形態を示す図である。

【発明を実施するための形態】
【００１２】
本発明が、本発明の実施形態を参照して説明される。本発明の説明全体を通じて、図１～３が参照される。図を参照するとき、全体を通じて示される同様の構造および要素は、同様の参照番号で示される。
【００１３】
図１は、本発明の一実施形態による、データ・センター内のデータ・センター・サーバで実行される仮想ディスク・イメージ（本明細書においてはワークロードとも呼ばれる）の地理的位置を確認するための方法を示す。方法は、受信するステップ１０２を含む。受信するステップ１０２の間に、データ・センターは、データ・センターで実行するためにデータ・センターのテナントから仮想ディスク・イメージを受信する。受信するステップ１０２が完了した後、方法は、計算するステップ１０４に続く。
【００１４】
計算するステップ１０４において、ディスク・イメージ・ハッシュ値が、データ・センター・サーバで実行されるハイパーバイザによって計算される。一実施形態において、ディスク・イメージ・ハッシュ値は、ＳＨＡ－１ハッシュであり、割り振られたサーバでのワークロードの展開時に計算される。さらに、ＳＨＡ－１ハッシュは、暗号化プロセッサまたはサーバによって計算される可能性がある。本明細書において使用されるとき、暗号化プロセッサは、暗号化動作を実行するための耐タンパー性の専用のチップ上のコンピュータまたはマイクロプロセッサである。特定の実施形態において、暗号化プロセッサは、中央演算処理装置（ＣＰＵ）およびトラステッド・プラットフォーム・モジュール（ＴＰＭ：trusted platform module）（本明細書においては暗号化プロセッサとも呼ばれる）を含む。加えて、暗号化プロセッサは、データ・センター・サーバの近くに置かれ、暗号化プロセッサに一意の承認鍵（ＥＫ）を含む。
【００１５】
計算されると、ハッシュは、送信され、ＴＰＭのプラットフォーム構成レジスタ（ＰＣＲ：platformconfiguration register）のうちの１つに記憶され得る。ＰＣＲは、ワークロードのハッシュ値のための耐タンパー性の記憶場所を提供する。さらに、テナントは、クラウド・プロバイダから、そのテナントのワークロードが展開されるサーバのＩＰアドレスまたはホスト名を取得する可能性がある。計算するステップ１０４が完了した後、方法は、受信するステップ１０８に続く。
【００１６】
受信するステップ１０８において、構成証明（attestation）要求が、テナントからサーバによって受信される。一実施形態においては、ハイパーバイザが、ＴＰＭがテナントのワークロードのハッシュを返すことを要求するコマンドをＴＰＭに送信する。例えば、ハイパーバイザは、ＴＰＭ_ＱｕｏｔｅコマンドをＴＰＭに送信し、ＴＰＭがテナントのワークロードのハッシュを保有するＰＣＲの内容を返すことを要求する可能性がある。受信するステップ１０８が完了した後、方法は、生成するステップ１１０に続く。
【００１７】
生成するステップ１１０において、ＴＰＭが、構成証明識別鍵（attestationidentity key）ペアを生成する。生成するステップ１１０の後、方法は、送信するステップ１１２に続く。
【００１８】
送信するステップ１１２において、ＴＰＭが、構成証明識別鍵ペアの公開鍵部分をハイパーバイザを介して認証局に送信する。一実施形態において、ＴＰＭは、新しい構成証明識別鍵（ＡＩＫ）ペアを生成し、ＴＰＭのＥＫで署名されたＡＩＫの公開部分をハイパーバイザを介して認証局（プライバシーＣＡ）に送信する。要求は、とりわけ、ＴＰＭのＥＫの公開される半分、新たに生成されたＡＩＫの公開される半分、およびＡＩＫの署名を含む可能性がある。ハイパーバイザは、証明書要求のＴＰＭのＥＫの公開される半分をキャッシュする。送信するステップ１１２の後、方法は、確認するステップ１１４に続く。

【００１９】
確認するステップ１１４において、構成証明識別鍵ペアの公開部分が、認証局により認証される。特定の実施形態においては、プライバシーＣＡが、証明書要求のＥＫが本物のＴＰＭに属することを確認する。例えば、各ＴＰＭが、そのＴＰＭが製造されるときにそのＴＰＭのＥＫペアを生成する可能性があり、製造業者が、各ＴＰＭのＥＫの公開部分をプライバシーＣＡに送信する。プライバシーＣＡは、例えば、有効なＥＫのデータベースを保有し得る。確認するステップ１１４の後、方法は、生成するステップ１１６に続く。
【００２０】
生成するステップ１１６において、認証局が、構成証明識別鍵ペアに関するデジタル証明書を生成する。これは、構成証明識別鍵の公開部分の信憑性が確認されると行われる。一実施形態においては、確認が成功すると、プライバシーＣＡが、ＴＰＭのＡＩＫの公開される半分に署名し、ＡＩＫに関する証明書を生成する。生成するステップ１１６の後、方法は、送信するステップ１１８に続く。
【００２１】
送信するステップ１１８において、仮想ディスク・イメージのディスク・イメージ・ハッシュ値、承認鍵、およびデジタル証明書が、データ・センターのテナントに送信される。一実施形態において、ＴＰＭは、新たに生成されたＡＩＫに関する証明書をプライバシーＣＡから受信する。そのとき、ＴＰＭは、新たに認証されたＡＩＫを用いてテナントのワークロードのハッシュ値に署名する。そして、ＴＰＭは、ＴＰＭ＿Ｑｕｏｔｅコマンドに対する応答として、ハッシュ値を、そのハッシュ値の署名、署名を生成するために使用されたＡＩＫの公開される半分、およびＡＩＫに関するプライバシーＣＡの証明書と一緒にハイパーバイザに送信する。さらに、ハイパーバイザは、受信された構成証明要求に応答して、ＴＰＭ＿Ｑｕｏｔｅコマンドの結果を、ＴＰＭのＥＫと一緒にテナントに送信する。
【００２２】
一実施形態において、ディスク・イメージ・ハッシュ値は、構成証明識別鍵を用いて署名される。加えて、構成証明識別鍵ペアの公開鍵、および識別鍵ペアに関するデジタル証明書が、データ・センターのテナントに送信される可能性がある。ディスク・イメージ・ハッシュ値は、構成証明識別鍵ペアの公開鍵によって署名される可能性がある。さらに、デジタル証明書が、暗号化プロセッサに発行される。送信するステップ１１８の後、方法は、比較するステップ１２０に進む。
【００２３】
比較するステップ１２０において、データ・センターのテナントが、構成証明識別鍵ペアの公開部分をデジタル証明書の内容と比較する。例えば、テナントは、ＡＩＫに関するプライバシーＣＡの証明書を用いて、そのテナントが構成証明応答で受信するＡＩＫの信憑性を確認する可能性がある。比較するステップ１２０の後、方法は、確認するステップ１２２に進む。
【００２４】
確認するステップ１２２において、認証局が、承認鍵、および構成証明識別鍵ペアの公開部分が同じ暗号化プロセッサに属することを確認する。一実施形態において、テナントは、プライバシーＣＡに問い合わせて、そのテナントが受信するＥＫおよびＡＩＫが同じＴＰＭから来るかどうかを調べる。テナントは、ＡＩＫを用いて、そのテナントのワークロードのハッシュ値の信憑性を確認し得る。この段階で、テナントは、そのテナントが受信したＥＫをＴＰＭが有するサーバでそのテナントのワークロードが実行されていることを知る。次に、テナントは、そのＥＫでＴＰＭの地理的位置を確認する必要がある。確認するステップ１２２の後、方法は、送信するステップ１２４に続く。
【００２５】
送信するステップ１２４において、位置プロバイダが、承認鍵に合致する暗号化プロセッサの地理的位置をデータ・センターのテナントに送信する。さらに、暗号化プロセッサの地理的位置を判定することは、位置プロバイダによって無線周波数識別（ＲＦＩＤ：ra

dio-frequency identification）タグを読むことを含む可能性がある。一実施形態において、テナントは、承認鍵を含む要求をクラウド内のすべてのＲＦＩＤリーダに送信し、ＴＰＭの地理的位置を要求する。各ＲＦＩＤリーダは、そのＲＦＩＤリーダの電子的に操作可能なアンテナでそのＲＦＩＤリーダのデータセンターを走査し、データセンター内のすべてのＴＰＭのＥＫを読む。ＲＦＩＤリーダの走査中にテナントの要求でＥＫを受信するＲＦＩＤリーダは、そのＥＫの地理的位置をテナントに送信する。また、ＥＫを含むＲＦＩＤチップは、耐タンパー性であると想定される。一実施形態において、そのＲＦＩＤチップは、暗号化プロセッサによって保持される可能性がある。加えて、ＲＦＩＤリーダは、データ・センターの所有者が物理的にアクセスすることができない可能性がある。

別の実施形態においては、クライアントのワークロードを実行するサーバ内のＴＰＭのＥＫを用いてクラウド内のすべてのＲＦＩＤリーダに問い合わせることによって、クライアントは、ＴＰＭと、ひいてはＴＰＭが属するサーバとの地理的位置を発見し得る。それによって、クライアントは、そのクライアントのワークロードを実行するサーバの地理的位置を知り得る。ソリューションを完全なものにするためには、クラウド内のどのサーバがクライアントのワークロードを実行するか、およびそのサーバのＴＰＭのそのＥＫが何であるかをクライアントが発見し得るプロトコルを規定する必要がある。プロトコルは、ＴＰＭの構成証明メカニズムを用いて構築され得る。サーバで実行されるハイパーバイザは、実行するためにワークロードをロードするとき、ワークロードのＳＨＡ－１ハッシュを計算し、そのハッシュ値をＴＰＭ内のＰＣＲのうちの１つに記憶し得る。どのサーバがクライアントのワークロードを実行するかを判定するために、クライアントは、そのクライアントのワークロードを実行しているとそのクライアントが考えるサーバのＩＰアドレスに構成証明要求を送信し得る。この要求に応答して、サーバのＴＰＭは、新しいＡＩＫペアを生成し、新しいＡＩＫペアの公開される半分に関する証明書を発行するようにプライバシーＣＡに要求し、最後に、クライアントのワークロードのハッシュを含むＰＣＲ内の値を、新たに生成されたＡＩＫを用いて計算されたこの値の署名と一緒にクライアントに送信する。このようにして、クライアントは、そのクライアントのワークロードを実行するサーバ内のＴＰＭのＡＩＫを取得し得る。サーバで実行されるハイパーバイザは、プライバシーＣＡにＴＰＭによって送信された証明書要求をキャッシュする可能性があり、この要求をクライアントに送信する可能性がある。この要求がＴＰＭのＥＫを含むので、クライアントは、そのクライアントのワークロードを実行するサーバのＴＰＭのＥＫを受信する。そして、クライアントは、そのクライアントが知るＥＫを用いてクラウド内のすべてのＲＦＩＤリーダに問い合わせて、そのクライアントのワークロードを実行するサーバのＴＰＭの地理的位置を発見し得る。図２は、本発明の一実施形態による、データ・センター内のデータ・センター・サーバで実行される仮想ディスク・イメージの地理的位置を確認するためのシステムを示す。システムは、暗号化プロセッサ２０８、ハイパーバイザ２０４、および位置プロバイダ２２８を含む。暗号化プロセッサは、データ・センター・サーバ２０６の近くにあり、暗号化プロセッサ２０８に一意の承認鍵２１２を含む。一実施形態において、暗号化プロセッサは、ＴＰＭである。ＴＰＭは、トラステッド・コンピューティング・グループ（ＴＣＧ：Trusted Computing Group）によってリリースされた仕様に基づく耐タンパー性の暗号チップである。今日の多くの商品のコンピュータは、ＴＰＭチップを組み込んでいる。ＴＰＭは、コンピューティング・プラットフォームで２つの主な機能、すなわち、（１）遠隔の確認者にコンピューティング・プラットフォームのソフトウェア構成を証明する能力と、（２）プラットフォームでデータの機密性および完全性を保護するための能力とを提供し、したがって、データは、プラットフォームが特定のソフトウェア構成を有するときにのみアクセスされ得る。ハイパーバイザ２０４は、仮想ディスク・イメージ２１６のディスク・イメージ・ハッシュ値２１８、デジタル証明書２１０、および承認鍵２１２をデータ・センターのテナントに送信するように構成される。位置プロバイダ２２８は、サーバ２０６の近くに置かれる。さらに、位置プロバイダ２２８は、承認鍵２１２に合致する暗号化プロセッサ２０８の地理的位置をデータ・センターのテナント２３０に送信するように構成される。別の実施形態において、暗号化コプロ

セッサ（crypto coprocessor）は、高セキュリティ、高スループットの暗号化サブシステムを提供するＩＢＭ　ＰＣＩ３暗号化コプロセッサ（ＩＢＭ４７６５またはそのより古いバージョン）である。

【００２６】

一実施形態において、ハイパーバイザ２０４は、構成証明識別鍵ペア２２０の公開鍵２２２によって署名された仮想ディスク・イメージ２１６のディスク・イメージ・ハッシュ値２１８を送信するように構成される。別の実施形態において、位置プロバイダ２２８は、無線周波数識別（ＲＦＩＤ）タグ２１４を読むように構成される可能性がある。別の実施形態において、クラウド内の各サーバは、暗号化プロセッサのＥＫの公開部分を保有する耐タンパー性のＲＦＩＤチップを備える可能性がある。このＲＦＩＤチップは、マザーボードに取り付けられる可能性があり、またはその他のチップと統合される可能性がある。さらに、サーバは、ＲＦＩＤチップとの通信を可能にするアンテナを含む可能性がある。ＲＦＩＤチップは、個々のサーバ、または同じ地理的位置を共有する複数のサーバに関連付けられる可能性がある。さらに、位置プロバイダ２２８は、データ・センター２０２の所有者２２６がアクセス不可能である可能性がある。別の実施形態において、位置プロバイダは、錠、または物理的なセキュリティのその他の手段により、データ・センターの所有者によってアクセスされ得ない部屋に置かれたＲＦＩＤリーダである。ＲＦＩＤリーダは、この場合、データ・センター内の各サーバのＲＦＩＤチップと通信するために十分な感度および十分に狭いビーム幅を有する電子的に操作可能なアンテナを有する可能性がある。さらに、ＲＦＩＤリーダは、リーダによって読み取られたすべてのＥＫのデータベースおよびデータ・センターの地理的位置を保有するネットワークに接続されたコンピュータを有する可能性がある。

【００２７】

別の実施形態において、暗号化プロセッサ２０８は、構成証明識別鍵ペア２２０を生成するように構成され得る。さらに、ハイパーバイザ２０４は、構成証明識別鍵ペア２２０の公開鍵２２２を認証局２３２に送信するように構成され得る。

【００２８】

別の実施形態において、認証局２３２は、構成証明識別鍵ペア２２０の公開鍵２２２の信憑性を確認するように構成され得る。さらに、認証局２３２は、公開鍵２２２の信憑性を確認すると、構成証明識別鍵ペア２２０に関するデジタル証明書２１０を生成するように構成され得る。

【００２９】

別の実施形態において、認証局２３２は、承認鍵２１２および公開鍵２２２が同じ暗号化プロセッサ２０８に属することを確認するように構成され得る。

【００３０】

図３は、各サーバがデータセンター内の各データ・センター・サーバのための公開鍵を保有する耐タンパー性のＲＦＩＤチップを備えるシステムとしての本発明の別の実施形態を示す。サーバの公開鍵は、サーバ内に存在するトラステッド・プラットフォーム・モジュール（ＴＰＭ）の承認鍵（ＥＫ）の公開部分である。ＴＰＭチップは、耐タンパー性である可能性があり、したがって、そのＴＰＭチップのＥＫは、修正されない可能性がある。

【００３１】

電子的に操作可能なアンテナを有する長距離ＲＦＩＤリーダが、各データ・センター内で、クラウド・プロバイダがアクセス不可能な物理的位置に置かれる可能性がある。ＲＦＩＤリーダは、そのＲＦＩＤリーダが置かれるデータ・センターの地理的位置を知り、要求に応じてクライアントにこの情報を送信することができる。ＲＦＩＤリーダは、データ・センター内のすべてのサーバのＥＫを読み、ＲＦＩＤリーダの地理的位置でホストされるすべてのサーバのＥＫを含む鍵データベースを構築する。

【００３２】

ワークロードがサーバで展開されるとき、そのワークロードの暗号学的ハッシュの形態

のそのワークロードの識別情報が、サーバのＴＰＭ内に記憶される。サーバで実行されるハイパーバイザは、実行のためにクライアントのワークロードをロードするとき、仮想ディスク・イメージの暗号学的ハッシュを計算し、そのハッシュ値をＴＰＭの内部レジスタのうちの１つに記憶する。

【００３３】

どのサーバがクライアントのワークロードを実行するかを判定するために、クライアントは、そのクライアントのワークロードを実行しているとそのクライアントが考えるサーバのＩＰアドレスに構成証明要求を送信する。この要求に応答して、サーバのＴＰＭは、構成証明識別鍵（ＡＩＫ）と呼ばれる新しいＲＳＡ鍵ペアを生成し、新しいＡＩＫに関する証明書を発行するようにプライバシーＣＡと呼ばれる認証局に要求し、最後に、クライアントのワークロードのハッシュを含むＰＣＲ内の値を、新たに生成されたＡＩＫを用いて計算されたこの値の署名と一緒にクライアントに送信する。このようにして、クライアントは、そのクライアントのワークロードを実行するサーバ内のＴＰＭのＡＩＫを取得する。

【００３４】

サーバで実行されるハイパーバイザは、プライバシーＣＡにＴＰＭによって送信された証明書要求をキャッシュし、この要求をクライアントに送信する。この要求は、ＴＰＭのＥＫを含み、したがって、クライアントは、そのクライアントのワークロードを実行するサーバのＴＰＭのＥＫを受信する。そして、クライアントは、そのクライアントが知るＥＫを用いてクラウド内のすべてのＲＦＩＤリーダに問い合わせて、そのクライアントのワークロードを実行するサーバのＴＰＭの地理的位置を発見し得る。

【００３５】

一実施形態において、ＴＰＭは、コンピューティング・プラットフォームでロードされたソフトウェアの暗号学的ハッシュを記憶することができるプラットフォーム構成レジスタ（ＰＣＲ）と呼ばれるハードウェア・レジスタを有する。ＰＣＲが（耐タンパー性の）ＴＰＭ内に存在するので、それらのＰＣＲに保有されるハッシュ値の完全性が保証される。新しいソフトウェアがコンピューティング・プラットフォームでロードされるとき、ロードする動作を実行するソフトウェアは、ロードされているソフトウェアの暗号学的ハッシュを計算し、このハッシュ値をＰＣＲに記憶する選択肢を有する。例えば、オペレーティング・システムのカーネルは、新しいアプリケーションをロードするとき、アプリケーションのバイナリ・イメージのＳＨＡ－１ハッシュを計算し、そのハッシュ値をＰＣＲのうちの１つに記憶することができる。そのとき、すべてのＰＣＲのハッシュ値の集合は、これらのハッシュがどんなソフトウェアがコンピューティング・プラットフォームで実行するためにロードされたかを示すので、コンピューティング・プラットフォームのソフトウェア構成を反映する。

【００３６】

遠隔の確認者は、コンピューティング・プラットフォームのソフトウェア構成の構成証明を提供するようにコンピューティング・プラットフォームのＴＰＭに要求することができる。そのような要求に応答して、ＴＰＭは、そのＴＰＭのＰＣＲのハッシュのリストを遠隔の確認者に送信する。送信されたハッシュの完全性を保証するために、ＴＰＭは、ＴＰＭにのみ知られているＲＳＡ鍵の秘密部分でハッシュのリストに署名する。遠隔の確認者は、その遠隔の確認者がＴＰＭの署名鍵の公開部分を認証することを可能にする証明書を有する。この証明書を用いて、遠隔の確認者は、その遠隔の確認者が受信するハッシュのリストの署名を確認し、それによって、それらのハッシュの完全性を確認することができる。

【００３７】

すべての構成証明要求に応じてＴＰＭにハッシュ値のリストに署名させることは、完全性の問題に対処するが、プライバシーの問題をもたらす。この問題は、以下の例を考察することによって理解され得る。ウェブサイトが、それらのウェブサイトに接続したいそれぞれのクライアント・コンピュータからの構成証明を要求すると仮定する。ここで、コン

ピュータから来るすべての構成証明応答が同じＲＳＡ鍵で署名された場合、コンピュータのユーザによって訪問された異なるウェブサイトが結託し、同じコンピュータがそれらのウェブサイトとの接続を確立したと判定する可能性がある。明らかに、この種の追跡は望ましくない。

【００３８】

この問題に対処する１つの方法は、ＴＰＭチップが、そのＴＰＭチップが生成するそれぞれの構成証明に一意のＲＳＡ鍵で署名することを可能にすることである。ＴＣＧ仕様は、この手法を採用する。それぞれの構成証明が、ＴＣＧの用語では構成証明識別鍵（ＡＩＫ）と呼ばれる新しいＲＳＡ鍵を用いて署名されるとき、各ＡＩＫ鍵の公開部分に関して新しい証明書が生成されなければならない。ＴＣＧ仕様は、この目的でプライバシーＣＡと呼ばれる認証局（ＣＡ）を導入する。ＴＰＭは、新しいＡＩＫを生成する度に、そのＡＩＫの公開部分を認証のためにプライバシーＣＡに送信する。プライバシーＣＡは、プライバシーＣＡの秘密鍵を用いて署名されたそのＡＩＫに関する証明書を発行する。遠隔の確認者は、プライバシーＣＡの署名鍵の公開部分を有し、その公開部分を用いて、構成証明応答の一部としてその遠隔の確認者が受信するＡＩＫの証明書が本物であることを確認することができる。

【００３９】

しかし、上で説明された手法に問題が存在する。プライバシーＣＡは、そのプライバシーＣＡが証明書を生成しているＡＩＫが本物のＴＰＭから来ることをどのようにして知るのか。結局、攻撃者は、偽のＡＩＫを生成し、偽のＡＩＫに関する証明書をプライバシーＣＡに要求することができる。この問題に対処するために、各ＴＰＭは、そのＴＰＭが製造されるときに、承認鍵（ＥＫ）と呼ばれる一意のＲＳＡ鍵ペアを生成する。そのとき、ＴＰＭのＥＫの公開部分は、そのＴＰＭに関する一意の暗号識別子（cryptographic identifier）である。ＴＰＭの製造業者は、各ＴＰＭのＥＫの公開部分をプライバシーＣＡに送信する。そして、プライバシーＣＡは、すべての本物のＴＰＭのＥＫを含むデータベースを有する。ＴＰＭは、新たに生成されたＡＩＫに関する証明書を要求するとき、そのＴＰＭのＥＫを用いて生成されたＡＩＫの署名を証明書要求でプライバシーＣＡに送信する。プライバシーＣＡは、そのプライバシーＣＡがそのプライバシーＣＡのＥＫデータベースにＴＰＭのＥＫの公開部分を有し、ＡＩＫの署名が確認される場合にのみ、これら２つの条件が満たされるときはＡＩＫが本物のＴＰＭから来ることが保証されるので、ＡＩＫに関する証明書を発行する。したがって、そのとき、ＴＰＭは、新しいＡＩＫと、構成証明応答の対応する証明書とを使用し、それによって、コンピューティング・プラットフォームのプライバシーを保つことができる。

【００４０】

当業者に理解されるであろうように、本発明の態様は、システム、方法、またはコンピュータ・プログラム製品として具現化され得る。したがって、本発明の態様は、すべてハードウェアの実施形態、すべてソフトウェアの実施形態（ファームウェア、常駐ソフトウェア、マイクロコードなどを含む）、またはすべてが概して本明細書において「回路」、「モジュール」、もしくは「システム」と呼ばれることがあるソフトウェアの態様とハードウェアの態様とを組み合わせる実施形態の形態をとる可能性がある。さらに、本発明の態様は、コンピュータ可読プログラム・コードを具現化する１つまたは複数のコンピュータ可読媒体で具現化されたコンピュータ・プログラム製品の形態をとる可能性がある。

【００４１】

１つまたは複数のコンピュータ可読媒体の任意の組み合わせが、利用される可能性がある。コンピュータ可読媒体は、コンピュータ可読信号媒体またはコンピュータ可読ストレージ媒体である可能性がある。コンピュータ可読ストレージ媒体は、例えば、電子、磁気、光、電磁、赤外線、もしくは半導体のシステム、装置、もしくはデバイス、またはこれらの任意の好適な組み合わせである可能性があるがこれらに限定されない。コンピュータ可読ストレージ媒体のより詳細な例（非網羅的なリスト）は、以下、すなわち、１つもしくは複数の配線を有する電気的な接続、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）、読み出し専用メモリ（ＲＯＭ）、消去可能プログラマブル読み出し専用メモリ（ＥＰＲＯＭもしくはフラッシュ・メモリ）、光ファイバ、ポータブル・コンパクト・ディスク読み出し専用メモリ（ＣＤ－ＲＯＭ）、光ストレージ・デバイス、磁気ストレージ・デバイス、またはこれらの任意の好適な組み合わせを含む。本明細書の文脈において、コンピュータ可読ストレージ媒体は、命令実行システム、装置、もしくはデバイスによって、または命令実行システム、装置、もしくはデバイスに関連して使用するためのプログラムを含むまたは記憶することができる任意の有形の媒体である可能性がある。

【００４２】

コンピュータ可読信号媒体は、例えば、ベースバンドで、または搬送波の一部としてコンピュータ可読プログラム・コードを具現化する伝播されるデータ信号を含み得る。そのような伝播される信号は、電磁的、光学的、またはこれらの任意の好適な組み合わせを含むがこれらに限定されないさまざまな形態のうちの任意の形態をとり得る。コンピュータ可読信号媒体は、コンピュータ可読ストレージ媒体ではなく、命令実行システム、装置、もしくはデバイスによって、または命令実行システム、装置、もしくはデバイスに関連して使用するためのプログラムを伝達、伝播、または搬送することができる任意のコンピュータ可読媒体である可能性がある。

【００４３】

コンピュータ可読媒体上に具現化されるプログラム・コードは、無線、有線、光ファイバ・ケーブル、ＲＦなど、またはこれらの任意の好適な組み合わせを含むがこれらに限定されない任意の適切な媒体を用いて送信される可能性がある。

【００４４】

本発明の態様の動作を実行するためのコンピュータ・プログラム・コードは、Ｊａｖａ（Ｒ）、Ｓｍａｌｌｔａｌｋ（Ｒ）、Ｃ＋＋などのオブジェクト指向プログラミング言語と、「Ｃ」プログラミング言語または同様のプログラミング言語などの通常の手続き型プログラミング言語とを含む１つまたは複数のプログラミング言語の任意の組み合わせで記述され得る。プログラム・コードは、すべてユーザのコンピュータ上で、スタンドアロンのソフトウェア・パッケージとしてユーザのコンピュータ上で部分的に、ユーザのコンピュータ上で部分的にかつ遠隔のコンピュータ上で部分的に、またはすべて遠隔のコンピュータもしくはサーバ上で実行され得る。最後の筋書きでは、遠隔のコンピュータが、ローカル・エリア・ネットワーク（ＬＡＮ）もしくは広域ネットワーク（ＷＡＮ）を含む任意の種類のネットワークを介してユーザのコンピュータに接続され得るか、または外部コンピュータへの接続が（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）行われ得る。

【００４５】

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またはブロック図あるいはその両方を参照して以下で説明される。流れ図またはブロック図あるいはその両方の各ブロック、および流れ図またはブロック図あるいはその両方のブロックの組み合わせは、コンピュータ・プログラム命令によって実装され得ることが理解されるであろう。これらのコンピュータ・プログラム命令は、コンピュータまたはその他のプログラム可能なデータ処理装置のプロセッサによって実行される命令が、流れ図またはブロック図あるいはその両方の１つのブロックまたは複数のブロックで規定された機能／動作を実施するための手段をもたらすように、汎用コンピュータ、専用コンピュータ、またはその他のプログラム可能なデータ処理装置のプロセッサに与えられてマシンを作り出すものである可能性がある。

【００４６】

これらのコンピュータ・プログラム命令は、コンピュータ可読媒体に記憶された命令が、流れ図またはブロック図あるいはその両方の１つのブロックまたは複数のブロックで規定された機能／動作を実施する命令を含む製品をもたらすように、コンピュータ可読媒体に記憶され、コンピュータ、他のプログラム可能なデータ処理装置、またはその他のデバ

イスを特定の方法で機能させるように指示するものである可能性がある。

【００４７】

コンピュータ・プログラム命令は、コンピュータまたはその他のプログラム可能な装置で実行される命令が、流れ図またはブロック図あるいはその両方の１つのブロックまたは複数のブロックで規定された機能／動作を実施するためのプロセスを提供するように、コンピュータで実施されるプロセスをもたらすために、コンピュータ、その他のプログラム可能なデータ処理装置、またはその他のデバイスにロードされ、コンピュータ、その他のプログラム可能な装置、またはその他のデバイスで一連の動作のステップが実行されるようにするものである可能性がある。

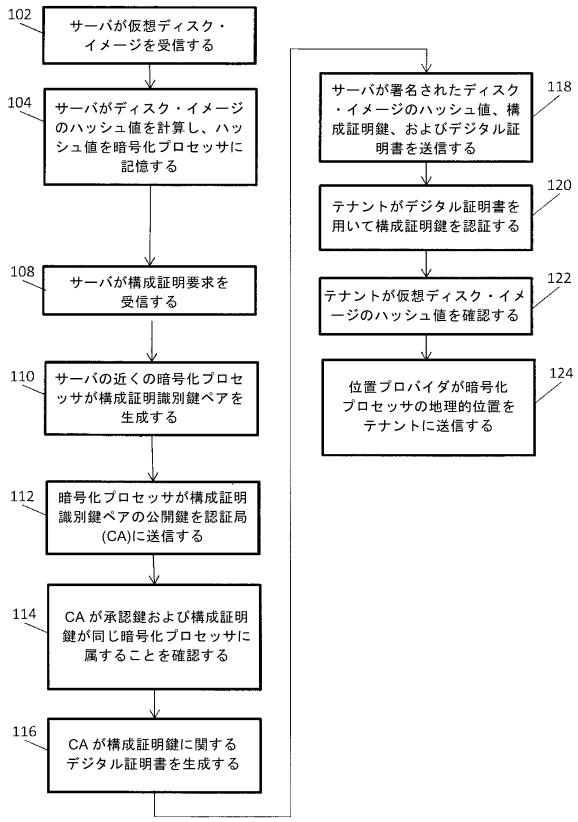
【００４８】

図面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・プログラム製品のあり得る実装のアーキテクチャ、機能、および動作を示す。これに関連して、流れ図またはブロック図の各ブロックは、（１つまたは複数の）規定された論理的な機能を実装するための１つまたは複数の実行可能命令を含むモジュール、セグメント、またはコードの一部を表す可能性がある。一部の代替的な実装においては、ブロックで示された機能が、図面に示された順序とは異なる順序で行われる可能性があることにも留意されたい。例えば、連続で示された２つのブロックが、実際には実質的に同時に実行される可能性があり、またはそれらのブロックが、関連する機能に応じて逆順に実行されることもあり得る。ブロック図または流れ図あるいはその両方の各ブロックと、ブロック図または流れ図あるいはその両方のブロックの組み合わせとは、規定された機能もしくは動作を実行する専用のハードウェアに基づくシステム、または専用のハードウェアとコンピュータ命令との組み合わせによって実装され得ることも認められるであろう。

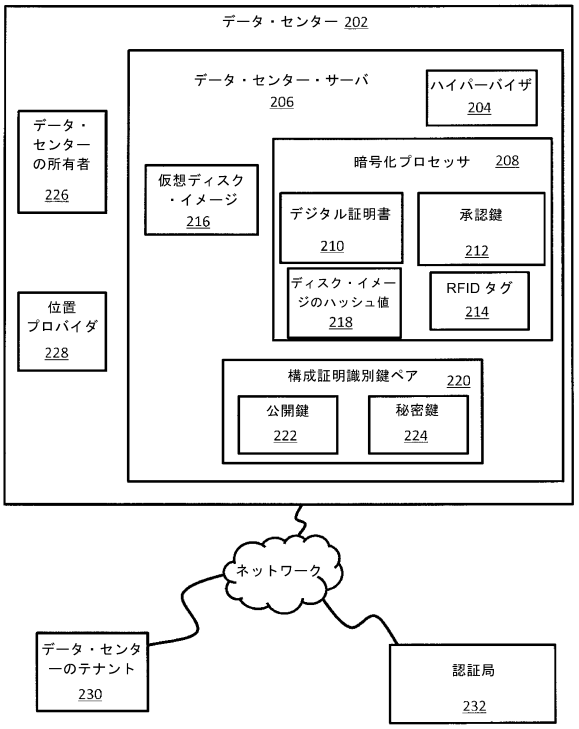
【００４９】

本発明のさまざまな実施形態の説明は、例示を目的として示されたが、網羅的であるように、または開示された実施形態に限定されるように意図されていない。多くの変更および改変が、説明された実施形態の範囲および精神から逸脱することなく当業者に明らかになるであろう。本明細書において使用された用語は、実施形態の原理、実用的な応用、もしくは市場に見られるテクノロジーに勝る技術的な改善を最もよく説明するか、または当業者が本明細書で開示された実施形態を理解することを可能にするように選択された。

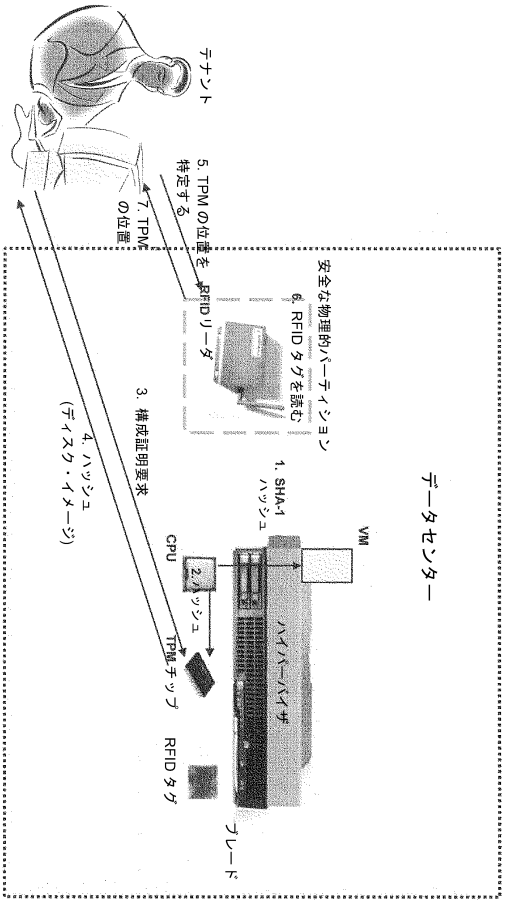
【図１】


102
サーバが仮想ディスク・イメージを受信する
104
サーバがディスク・イメージのハッシュ値を計算し、ハッシュ値を暗号化プロセッサに記憶する
108
サーバが構成証明要求を受信する
110
サーバの近くの暗号化プロセッサが構成証明識別鍵ペアを生成する
112
暗号化プロセッサが構成証明識別鍵ペアの公開鍵を認証局(CA)に送信する
114
CA が承認鍵および構成証明鍵が同じ暗号化プロセッサに属することを確認する
116
CA が構成証明鍵に関するデジタル証明書を生成する
118
サーバが署名されたディスク・イメージのハッシュ値、構成証明鍵、およびデジタル証明書を送信する
120
テナントがデジタル証明書を用いて構成証明鍵を認証する
122
テナントが仮想ディスク・イメージのハッシュ値を確認する
124
位置プロバイダが暗号化プロセッサの地理的位置をテナントに送信する

【図２】


データ・センター 202
データ・センター・サーバ 206
ハイパーバイザ 204
データ・センターの所有者 226
仮想ディスク・イメージ 216
暗号化プロセッサ 208
デジタル証明書 210
承認鍵 212
ディスク・イメージのハッシュ値 218
RFID タグ 214
位置プロバイダ 228
構成証明識別鍵ペア 220
公開鍵 222
秘密鍵 224
ネットワーク
データ・センターのテナント 230
認証局 232

【図３】


テナント
5. TPM の位置を特定する
7. TPM の位置
安全な物理的パーティション
6. RFID リーダ
6. RFID タグを読む
3. 構成証明要求
4. ハッシュ (ディスク・イメージ)
1. SHA-1 ハッシュ
VM
CPU
2. ハッシュ
TPM チップ
RFID タグ
ハイパーバイザ
ブレード
データセンター

フロントページの続き

(74)代理人　100112690
　　弁理士　太佐　種一
(72)発明者　ペンダラキス、ディミトリオス
　　アメリカ合衆国１０５９８　ニューヨーク州ヨークタウン・ハイツ　ルート１３４　キッチャワン・ロード１１０１　ティー・ジェイ・ワトソン・リサーチ・センター
(72)発明者　セシャドリ、アーヴィンド
　　アメリカ合衆国１０５３２　ニューヨーク州ホーソーン　スカイライン・ドライブ１９

審査官　金木　陽一

(56)参考文献　特開２００６－３１１５６２（ＪＰ，Ａ）
　　国際公開第２０１２／０３９７１４（WO，Ａ１）
　　米国特許出願公開第２００６／００９１２０７（ＵＳ，Ａ１）
　　米国特許出願公開第２０１０／０１６１９９８（ＵＳ，Ａ１）
　　KHAN, K.M., et al, Establishing Trust in Cloud Computing, IT Professional, [online], ２０１０年　９月, Vol. 12, No. 5, pp. 20-26, [Retrieved on 2017-10-30.] Retrieved from the Internet, ＵＲＬ, http://doi.org/10.1109/MITP.2010.128

(58)調査した分野(Int.Cl.，ＤＢ名)
　　Ｈ０４Ｌ　　９／３２
　　Ｇ０６Ｆ　２１／４４
　　Ｈ０４Ｌ　　９／０８