【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成30年6月14日(2018.6.14)

【公表番号】特表2017-520959(P2017-520959A)
【公表日】平成29年7月27日(2017.7.27)
【年通号数】公開・登録公報2017-028
【出願番号】特願2016-566758(P2016-566758)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/57　(2013.01)
Ｇ０６Ｆ　9/46　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｄ
Ｇ０６Ｆ　21/57　３５０
Ｇ０６Ｆ　9/46　３５０

【手続補正書】
【提出日】平成30年4月23日(2018.4.23)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コンピューティング環境において、ホストに対する信頼を確立するための方法であって、
ホストアテステーションサービスが、物理マシン上に展開されたホストから、前記ホストが満たすある特徴の検証可能な指標を受けるステップと、
前記ある特徴の前記指標から、前記ホストがある要件を満たすことの判定を試みるステップと、
前記ホストが信頼実行環境（ＴＥＥ）を含むという要件を少なくとも満たすことを含む前記ある要件を前記ホストが満たす場合に、前記ホストアテステーションサービスが、前記ホストアテステーションサービスと信頼関係を有する１つまたは複数のエンティティに対する認証を行うために前記ホストが使用できる証明書を前記ホストに発行するステップと
を含み、前記証明書は、鍵を、前記ホストアテステーションサービスと信頼関係を有するキー分配サービスから、前記証明書が前記キー分配サービスに提供されることに応答して取得するために前記ホストが使用するように構成され、前記鍵は、遮蔽型ゲスト仮想マシンを復号化するために前記ホストが使用するように構成され、前記遮蔽型ゲスト仮想マシンは、仮想マシンマネージャーによって、ゲスト仮想マシンが前記ホスト上で実行可能となるように前記ホストに対するテナントの要求時に展開される、方法。
【請求項２】
請求項１に記載の方法であって、前記ある要件がさらに、前記ホストを実施する物理マシン上のＴＰＭ（信頼プラットフォームモジュール）に関連する要件を含む、方法。
【請求項３】
請求項１に記載の方法であって、前記ホストを実施する前記物理マシンが前記ある要件を検証可能な形で満たすことの判定に失敗した結果として、前記ホストが前記ある要件を満たさない旨を、前記仮想マシンマネージャーへ通知するステップをさらに含む方法。

【請求項４】
請求項１に記載の方法であって、前記ホストが前記ある要件を検証可能な形で満たすことの判定に失敗した結果として、前記ホストが遮蔽型ゲスト仮想マシンの展開に利用可能でない旨を、前記仮想マシンマネージャーへ通知するステップをさらに含む方法。
【請求項５】
請求項１に記載の方法であって、前記ある要件がさらに、前記ホストを実施する物理ホストマシンに、侵害されずに起動が発生したことを検証するための、適正かつ信頼に値するＵＥＦＩ（統一拡張ファームウェアインターフェース）報告が提供されるという要件を含む、方法。
【請求項６】
請求項１に記載の方法であって、前記ある要件がさらに、前記ホストが適正なＨＶＣＩ（ハイパーバイザー強制型コード整合性）ポリシー妥当性確認を含むという検証可能な指標が提供されるという要件を含む、方法。
【請求項７】
請求項１に記載の方法であって、前記ある要件がさらに、前記ホストが特定の地理的位置に所在するという要件を含む、方法。
【請求項８】
請求項１に記載の方法であって、前記ある要件がさらに、前記ホストがセキュアなネットワークに連結されるという要件を含む、方法。
【請求項９】
請求項１に記載の方法であって、前記ホストアテステーションサービスと、前記ホストが前記証明書の提示によってキーを取得できる前記キー分配サービスとの間で、信頼関係をつくるステップをさらに含む、方法。
【請求項１０】
請求項１に記載の方法であって、ファブリック管理システムを有する環境において前記ホストアテステーションサービスが実施される環境で実行され、前記ファブリック管理システムは、ホストオペレーティングシステム、ホスト構成、ＨＶＣＩホワイトリスト、ＨＶＣＩ取消リスト、ＵＥＦＩホワイトリストまたはＵＥＦＩ取消リストのうち少なくとも１つを管理するよう構成され、前記ファブリック管理システムの管理者の認証に使用されるものとは異なる認証および認可の一方または双方のサービスが、前記ホストアテステーションサービスの管理者の認証に使用される、方法。
【請求項１１】
請求項１に記載の方法であって、前記仮想マシンマネージャーを有する環境において前記ホストアテステーションサービスが実施される環境で実行され、前記仮想マシンマネージャーは、遮蔽型ゲスト仮想マシンを前記ホストに展開するように構成されるが、前記仮想マシンマネージャーは、前記遮蔽型ゲスト仮想マシンを復号化できない、方法。
【請求項１２】
請求項１１に記載の方法であって、前記仮想マシンマネージャーの管理者の認証に使用されるものとは異なる認証サービスが、前記ホストアテステーションサービスの管理者の認証に使用される環境で実行される方法。
【請求項１３】
コンピューティング環境において、ホストに対する信頼を確立するための方法であって、
物理マシンを用いて実施されたホストが、前記ホストのある特徴の検証可能な指標をホストアテステーションサービスに送るステップと、
ある特徴の前記指標を評価する前記ホストアテステーションサービスが判定した、前記ホストが信頼実行環境（ＴＥＥ）を含むという要件を少なくとも満たすことを含むある要件を前記ホストが満たすことの結果として、前記ホストが、前記ホストアテステーションサービスから、前記ホストアテステーションサービスと信頼関係を有する１つまたは複数のエンティティに対する認証を行うために前記ホストが使用できる証明書を受けるステッ

プと、
前記ホストが、鍵を、キー分配サービスから、前記証明書を前記キー分配サービスに提供することに応答して取得するステップであって、前記キー分配サービスは、前記ホストアテステーションサービスを、前記キー分配サービスが前記ホストアテステーションサービスによって署名された証明書を受け入れるという点で信頼する、ステップと、
前記ホストが、前記鍵を使用して、仮想マシンマネージャーによって展開される遮蔽型ゲスト仮想マシンを、ゲスト仮想マシンが前記ホスト上で実行可能となるように前記ホストに対するテナントの要求時に復号化するステップと
を含む方法。
【請求項１４】
請求項１３に記載の方法であって、前記ある要件がさらに、
（ａ）前記ホストを実施する前記物理マシン上のＴＰＭ（信頼プラットフォームモジュール）に関連する要件、
（ｂ）前記ホストが実施される前記物理マシンに、適正かつ信頼に値するＵＥＦＩ（統一拡張ファームウェアインターフェース）報告が提供されるという要件、
（ｃ）前記ホストが適正なＨＶＣＩ（ハイパーバイザー強制型コード整合性）ポリシー妥当性確認を含むという検証可能な指標が提供されるという要件、
（ｄ）前記ホストが特定の地理的位置に所在するという要件、および
（ｅ）前記ホストがセキュアなネットワークに連結されるという要件
を含む群から選択される要件を含む、方法。
【請求項１５】
請求項１３に記載の方法であって、
前記ホストが、前記ゲスト仮想マシンの前記展開のセキュリティ上の詳細に関する暗号化メッセージを作成するステップであって、前記暗号化メッセージは、前記仮想マシンマネージャーによる復号化が不可能であるが、前記テナントによる復号化が可能である、ステップと、
前記ホストが、前記暗号化メッセージを前記仮想マシンマネージャーに送るステップであって、前記暗号化メッセージは、前記仮想マシンマネージャーによる前記暗号化メッセージの読み取りを可能とすることなく前記テナントに転送可能である、ステップと
を含む方法。
【請求項１６】
ホストが実施される物理マシンを含むコンピューティングシステムであって、前記ホストは、前記ホストに対する信頼を確立するための方法を実行し、前記方法は、
前記ホストが、前記ホストのある特徴の検証可能な指標をホストアテステーションサービスに送るステップと、
ある特徴の前記指標を評価する前記ホストアテステーションサービスが判定した、前記ホストが信頼実行環境（ＴＥＥ）を含むという要件を少なくとも満たすことを含むある要件を前記ホストが満たすことの結果として、前記ホストが、前記ホストアテステーションサービスから、前記ホストアテステーションサービスと信頼関係を有する１つまたは複数のエンティティに対する認証を行うために前記ホストが使用できる証明書を受けるステップと、
前記ホストが、鍵を、キー分配サービスから、前記証明書を前記キー分配サービスに提供することに応答して取得するステップであって、前記キー分配サービスは、前記ホストアテステーションサービスを、前記キー分配サービスが前記ホストアテステーションサービスによって署名された証明書を受け入れるという点で信頼する、ステップと、
前記ホストが、前記鍵を使用して、仮想マシンマネージャーによって展開される遮蔽型ゲスト仮想マシンを、ゲスト仮想マシンが前記ホスト上で実行可能となるように前記ホストに対するテナントの要求時に復号化するステップと
を含む、コンピューティングシステム。
【請求項１７】

請求項１６に記載のコンピューティングシステムであって、前記方法は、
前記ホストが、前記ゲスト仮想マシンの前記展開のセキュリティ上の詳細に関する暗号化メッセージを作成するステップであって、前記暗号化メッセージは、前記仮想マシンマネージャーによる復号化が不可能であるが、前記テナントによる復号化が可能である、ステップと、
前記ホストが、前記暗号化メッセージを前記仮想マシンマネージャーに送るステップであって、前記暗号化メッセージは、前記仮想マシンマネージャーによる前記暗号化メッセージの読み取りを可能とすることなく前記テナントに転送可能である、ステップと
を含む、コンピューティングシステム。
【請求項１８】
請求項１６に記載のコンピューティングシステムであって、前記ある要件が、前記ホストを実施する前記物理マシン上のＴＰＭ（信頼プラットフォームモジュール）に関連する要件を含む、コンピューティングシステム。
【請求項１９】
請求項１６に記載のコンピューティングシステムであって、前記ある要件が、前記ホストが実施される前記物理マシンに、適正かつ信頼に値するＵＥＦＩ（統一拡張ファームウェアインターフェース）報告が提供されるという要件を含む、コンピューティングシステム。
【請求項２０】
請求項１６に記載のコンピューティングシステムであって、前記ある要件が、前記ホストが適正なＨＶＣＩ（ハイパーバイザー強制型コード整合性）ポリシー妥当性確認を含むという検証可能な指標が提供されるという要件を含む、コンピューティングシステム。
【請求項２１】
請求項１６に記載のコンピューティングシステムであって、前記ある要件が、前記ホストが特定の地理的位置に所在するという要件を含む、コンピューティングシステム。
【請求項２２】
請求項１６に記載のコンピューティングシステムであって、前記ある要件が、前記ホストがセキュアなネットワークに連結されるという要件を含む、コンピューティングシステム。