

【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 6 部門第 3 区分

【発行日】令和 2 年 10 月 22 日 (2020.10.22)

【公表番号】特表 2019-533253 (P2019-533253A)

【公表日】令和 1 年 11 月 14 日 (2019.11.14)

【年通号数】公開・登録公報 2019-046

【出願番号】特願 2019-521371 (P2019-521371)

【国際特許分類】

G 0 6 F 21/53 (2013.01)

G 0 6 F 9/455 (2006.01)

【 F I 】

G 0 6 F 21/53

G 0 6 F 9/455 1 5 0

【手続補正書】

【提出日】令和 2 年 9 月 10 日 (2020.9.10)

【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】

少なくとも一つのプロセッサと、前記少なくとも一つのプロセッサによって実行可能な命令を記憶するメモリとを備えるコンピューティング・システムであって、

前記命令は、実行されると、

ポリシ・エンジンであって、実行環境によって実行されるべきサービスを表す役割を識別する役割識別子を受け取り、前記実行環境内で展開される仮想マシンイメージを示す仮想マシン ( V M ) イメージ測定値を受け取り、測定値 - 役割マッピングに基づいて、前記 V M イメージ測定値が前記役割にマッピングされるかどうかを判定し、前記判定を示す評価信号を生成するように構成されたポリシ・エンジンと、

鍵ラッピング暗号エンジンであって、前記 V M イメージ測定値が前記役割にマッピングされることを示す前記評価信号に基づいて、役割に対応する役割鍵の集合をラップし、前記実行環境が前記サービスを実行することを可能にするように構成された鍵ラッピング暗号エンジンと、

ラップされた役割鍵の前記集合を前記実行環境に提供する鍵サービスと、

を提供する、コンピューティング・システム。

【請求項 2】

前記ポリシ・エンジンは、前記役割識別子、前記 V M イメージ測定値、および実行環境識別子を、要求する実行環境から受け取るように構成され、前記実行環境識別子は、前記要求する実行環境を識別する、請求項 1 に記載のコンピューティング・システム。

【請求項 3】

前記ポリシ・エンジンは、前記要求する実行環境が前記 V M イメージ測定値にマッピングされるかどうかを前記実行環境識別子に基づいて判定し、前記判定に基づいて前記評価信号を生成するように構成される、請求項 2 に記載のコンピューティング・システム。

【請求項 4】

前記ポリシ・エンジンは、複数の異なる役割のそれぞれを異なる V M イメージ測定値にマッピングする測定値 - 役割マッピングの集合にアクセスし、前記 V M イメージ測定値が前記役割にマッピングされるかどうかを前記測定値 - 役割マッピングの集合に基づいて判

定するように構成されている、請求項 2 に記載のコンピューティング・システム。

【請求項 5】

前記命令は、

役割鍵の前記集合を前記鍵ラッピング暗号エンジンに提供するように構成された役割鍵ストア/ジェネレータと、

鍵ラッパー鍵の集合であって、各鍵ラッパー鍵は、所与の役割にマッピングされ、前記鍵ラッピング暗号エンジンは、前記役割にマッピングされた 1 つまたは複数の鍵ラッパー鍵を識別し、前記識別された 1 つまたは複数の鍵ラッパー鍵を用いて前記役割鍵を暗号化する、鍵ラッパー鍵の集合と、

を提供する、請求項 4 に記載のコンピューティング・システム。

【請求項 6】

前記命令は、

展開エンジンであって、前記役割識別子を受け取り、前記役割識別子に基づいて前記 VM イメージを入手し、前記 VM イメージを前記実行環境に展開するように構成された展開エンジンを提供する、請求項 1 に記載のコンピューティング・システム。

【請求項 7】

前記命令は、

役割を VM イメージにマッピングする役割 - イメージ・マッピングの集合を提供し、

前記展開エンジンは、前記 VM イメージを識別するために役割 - イメージ・マッピングの前記集合にアクセスするように構成されている、請求項 6 に記載のコンピューティング・システム。

【請求項 8】

前記命令は、

前記 VM イメージを記憶するように構成された VM イメージ・リポジトリを提供し、

前記展開エンジンは、前記 VM イメージ・リポジトリから展開のために前記 VM イメージを入手するように構成されている、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】

前記実行環境は、前記 VM イメージ測定値を生成し、前記 VM イメージ測定値を前記鍵サービスに提供するように構成された測定システムを含む、請求項 6 に記載のコンピューティング・システム。

【請求項 10】

前記測定システムは、前記 VM イメージ測定値を含むハッシュ値を入手するために前記 VM イメージに対してハッシュ関数を実行する、請求項 9 に記載のコンピューティング・システム。

【請求項 11】

コンピューティング・システムによって実行される方法であって、

サービスを実行するように構成された実行環境に関連付けられるサービスを識別することと、

前記実行環境内で展開される仮想マシンイメージを示す仮想マシン (VM) イメージ測定値を識別することと、

測定値 - 役割マッピングに基づいて、前記 VM イメージ測定値が前記サービスにマッピングされるかどうかを判定することと、

前記判定を示す評価信号を生成することと、

前記 VM イメージ測定値が前記サービスにマッピングされることを示す前記評価信号に応答して、前記サービスに対応する役割鍵の集合を入手することと、

前記実行環境が前記サービスを実行することを可能にすることと、

役割鍵の前記集合内の前記役割鍵を暗号化することと、

前記実行環境に暗号化された役割鍵の前記集合を提供することと、

を含む方法。

【請求項 12】

前記サービスを識別する役割識別子を受け取ることと、

前記VMイメージ測定値を受け取ることと、

要求する実行環境から実行環境識別子を受け取ることであって、前記実行環境識別子は、前記要求する実行環境を識別し、前記VMイメージ測定値が前記実行環境サービスにマッピングされるかどうかを判定することは、前記要求する実行環境が前記VMイメージ測定値にマッピングされるかどうかを前記実行環境識別子に基づいて判定することを含み、前記評価信号を生成することは、前記判定に基づいて前記評価信号を生成することを含む、実行環境識別子を受け取ることと、  
をさらに含む、請求項11に記載の方法。

【請求項13】

前記VMイメージ測定値が前記サービスにマッピングされるかどうかを判定することは、

役割の複数の異なる集合を異なるVMイメージ測定値にマッピングする測定値 - 役割マッピングの資産にアクセスすることによって、前記VMイメージ測定値が前記役割にマッピングされるかどうかを判定すること  
を含む、請求項12に記載の方法。

【請求項14】

前記役割鍵を暗号化することは、

前記役割にマッピングされた1つまたは複数の鍵ラッパー鍵を識別することと、

前記識別された1つまたは複数の鍵ラッパー鍵を用いて前記役割鍵を暗号化することと、

を含む、請求項13に記載の方法。

【請求項15】

展開システムで、役割を受け取ることと、

前記展開システムで、役割をVMイメージにマッピングする役割 - イメージ・マッピングの集合にアクセスすることによって、役割に基づいてVMイメージを入手することと、  
前記VMイメージを前記実行環境に展開することと、  
を更に含む、請求項11に記載の方法。

【請求項16】

前記実行環境内の測定システムを用いて前記VMイメージ測定値を生成することと、

前記VMイメージ測定値を鍵サービスに提供することと、

を更に含む、請求項15に記載の方法。

【請求項17】

前記VMイメージ測定値を生成することが、測定システムを用いて、VMイメージ測定値を含むハッシュ値を入手するためにVMイメージに対してハッシュ関数を実行することを含む、請求項16に記載の方法。

【請求項18】

少なくとも一つのプロセッサと、前記少なくとも一つのプロセッサによって実行可能な命令を記憶するメモリとを備えるコンピューティング・システムであって、

前記命令は、実行されると、

展開された仮想マシン（VM）イメージによって表され、役割によって識別されるサービスを実行し、

VMイメージ測定値を生成するために前記VMイメージにハッシュ関数を適用し、

前記役割及び前記VMイメージ測定値を鍵サービスに提供し、役割鍵の集合を要求し、

前記鍵サービスからラップされた役割鍵の集合を受け取り、

ラップされた役割鍵の前記集合を暗号化解除し、要求された役割鍵の集合を入手し、

前記要求された役割鍵を使用して前記サービスを実行するように、

前記コンピューティング・システムを構成する、コンピューティング・システム。

【請求項19】

前記命令は、

前記サービスを識別する役割と、前記実行環境内で展開される仮想マシンイメージを示す仮想マシンイメージ測定値とを前記実行環境から受け取り、

前記VMイメージ測定値が前記役割にマッピングされることを判定し、

前記判定を示す評価信号を生成し、

前記VMイメージ測定値が前記役割にマッピングされることを示す前記評価信号に基づいて、役割鍵の集合をラップし、

前記実行環境にラップされた役割鍵の前記集合を提供するように、

前記コンピューティング・システムを構成する、請求項18に記載のコンピューティング・システム。

**【請求項20】**

前記命令は、

役割をVMイメージにマッピングする役割 - イメージ・マッピングの集合にアクセスし、

前記役割に基づいて前記役割 - イメージ・マッピングにアクセスすることにより、VMイメージ・リポジトリから展開のためのVMイメージを入手し、

前記VMイメージを前記実行環境に展開するように、

前記コンピューティング・システムを構成する、コンピューティング・システム。