【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】平成27年8月6日(2015.8.6)

【公表番号】特表2014-525105(P2014-525105A)
【公表日】平成26年9月25日(2014.9.25)
【年通号数】公開・登録公報2014-052
【出願番号】特願2014-522856(P2014-522856)
【国際特許分類】
Ｇ０６Ｆ　21/57　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/00　　１５７Ａ

【手続補正書】
【提出日】平成27年6月15日(2015.6.15)
【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】
ハードウェアのトラステッドプラットフォームモジュール（ＴＰＭ）コンポーネントを必要としないで、コンピューターデバイスにおいて信頼された実行環境（ＴｒＥＥ）を可能にする方法であって：
コンピューターデバイスのファームウェアコンポーネントからｆＴＰＭモジュールを取得するステップであり、前記ｆＴＰＭは、前記コンピューターデバイスにおける一つまたはそれ以上のプロセッサに不可欠なセキュリティ拡張機能に対するソフトウェア基盤のインターフェイスを提供するステップと；
前記コンピューターデバイスの前記ファームウェアコンポーネントからソフトウェア基盤のモニターモジュールを取得するステップと；
前記コンピューターデバイス上にＯＳをブートする以前に、前記コンピューターデバイスの保護されたメモリーの中のセキュアワールド環境の中に前記ｆＴＰＭモジュールと前記モニターモジュールをインスタンス化するステップと；
一つまたはそれ以上の前記プロセッサは、ＡＲＭ（アドバンストＲＩＳＣマシン）基盤アーキテクチャを使用し、ＡＲＭ基盤プロセッサに不可欠な前記セキュリティ拡張機能は、トラストゾーンタイプのセキュリティ拡張、および、ｆＴＰＭのインスタンス化に続いてｆＴＰＭによって使用されるセキュリティプリミティブを含み；
前記モニターモジュールに対するセキュアモニターコールを介して、通常ワールド環境におけるコーラーが前記一つまたはそれ以上のプロセッサのセキュリティ機能にアクセスできるようにすることによって、前記コンピューターデバイス上でＴｒＥＥを可能にするステップであり、前記モニターモジュールは、次に、前記セキュアモニターコールに関するインストラクションを前記セキュアワールドにおける前記ｆＴＰＭに対してパスするステップと、を含む、
ことを特徴とする方法。
【請求項２】
前記ｆＴＰＭは、前記コンピューターデバイス上で実行されている一つまたはそれ以上の仮想マシンによってアクセス可能である、
請求項１に記載の方法。
【請求項３】

前記コンピューターデバイスにおける一つまたはそれ以上のプロセッサはＡＲＭプロセッサであり、かつ、前記ＡＲＭプロセッサに不可欠な前記セキュリティ拡張機能はトラストゾーン及びセキュリティプリミティブを含んでいる、
請求項１に記載の方法。
【請求項４】
ＯＳブートの以前に、前記コーラーは、一つまたはそれ以上のプリブートアプリケーションに対して前記ＴｒＥＥを明らかにするためのプリブートアプリケーションモジュールを含んでおり、それによって前記アプリケーションが前記ＴｒＥＥを使用してタスクを実行できるようにしている、
請求項１に記載の方法。
【請求項５】
ＯＳブートに続いて、前記コーラーは、前記ＯＳ上で実行されている一つまたはそれ以上のアプリケーションに対して前記ＴｒＥＥを明らかにするためのＴＰＭドライバーモジュールを含んでおり、それによって前記アプリケーションが前記ＴｒＥＥを使用してタスクを実行できるようにしている、
請求項１に記載の方法。
【請求項６】
前記コンピューターデバイスの前記ファームウェアコンポーネントは、前記ｆＴＰＭモジュールを含むソフトウェアを用いて前記ファームウェアを更新することによって、前記ｆＴＰＭモジュールを受取る、
請求項１に記載の方法。
【請求項７】
ハードウェアのトラステッドプラットフォームモジュール（ＴＰＭ）コンポーネントを必要としないで、コンピューターデバイス上に信頼されたコンピューター環境を実施するためのシステムであって：
ｆＴＰＭモジュールが保管されているコンピューターデバイスの不揮発性メモリーコンポーネントであり、前記ｆＴＰＭは、前記コンピューターデバイスにおける一つまたはそれ以上のプロセッサに不可欠なセキュリティ拡張機能に対するソフトウェア基盤のインターフェイスを提供するコンポーネントと；
前記不揮発性メモリーコンポーネントは、さらに、ソフトウェア基盤のモニターモジュールを含んでおり、
前記不揮発性メモリーコンポーネントから前記ｆＴＰＭモジュールと前記モニターモジュールを読み出し、前記コンピューターデバイスの保護されたメモリーの中のセキュアワールド環境の中に前記ｆＴＰＭモジュールと前記モニターモジュールをインスタンス化するためのデバイスと；を含み、
一つまたはそれ以上の前記プロセッサは、ＡＲＭ（アドバンストＲＩＳＣマシン）基盤アーキテクチャを使用し、ＡＲＭ基盤プロセッサに不可欠な前記セキュリティ拡張機能は、トラストゾーンタイプのセキュリティ拡張、および、ｆＴＰＭのインスタンス化に続いてｆＴＰＭによって使用されるセキュリティプリミティブを含み；かつ、
前記モニターモジュールに対するセキュアモニターコールを介して、通常ワールド環境におけるコーラーが前記一つまたはそれ以上のプロセッサのセキュリティ機能にアクセスできるようにすることによって、前記コンピューターデバイス上で信頼されたコンピューター環境を可能にし、前記モニターモジュールは、次に、前記セキュアモニターコールに関するインストラクションを前記セキュアワールドにおける前記ｆＴＰＭに対してパスする、
ことを特徴とするシステム。
【請求項８】
ＯＳブートの以前に、前記コーラーは、一つまたはそれ以上のプリブートアプリケーションに対して前記信頼されたコンピューター環境を表すためのプリブートアプリケーションモジュールを含んでおり、それによって前記アプリケーションが前記信頼されたコンピ

ューター環境を使用してタスクを実行できるようにしている、
請求項７に記載のシステム。
【請求項９】
ＯＳブートに続いて、前記コーラーは、前記ＯＳ上で実行されている一つまたはそれ以上のアプリケーションに対して前記信頼されたコンピューター環境を表すためのＴＰＭドライバーモジュールを含んでおり、それによって前記アプリケーションが前記信頼されたコンピューター環境を使用してタスクを実行できるようにしている、
請求項７に記載のシステム。
【請求項１０】
ハードウェアのトラステッドプラットフォームモジュール（ＴＰＭ）コンポーネントを必要としないで、コンピューターデバイスを用いて信頼されたコンピューター環境を実施するための方法をコンピューターで実行可能なインストラクションが保管されたコンピューターで読取り可能な媒体であって、前記インストラクションは：
前記コンピューターデバイスにおける一つまたはそれ以上のプロセッサに不可欠なセキュリティ拡張機能に対するソフトウェア基盤のインターフェイスを提供するためのｆＴＰＭモジュールと；
ソフトウェア基盤のモニターモジュールと；を有し、
前記方法は、
前記コンピューターデバイスの不揮発性メモリーコンポーネントの中に前記ｆＴＰＭモジュールと前記モニターモジュールをロードするステップと；
不揮発性メモリーから前記ｆＴＰＭモジュールと前記モニターモジュールを取得するステップと；
前記コンピューターデバイスの保護されたメモリーの中のセキュアワールド環境の中に前記ｆＴＰＭモジュールと前記モニターモジュールをインスタンス化するステップと；
前記モニターモジュールに対するセキュアモニターコールを介して、通常ワールド環境におけるコーラーが前記一つまたはそれ以上のプロセッサのセキュリティ機能にアクセスできるようにすることによって、前記コンピューターデバイス上で信頼されたコンピューター環境を可能にするステップであり、前記モニターモジュールは、次に、前記セキュアモニターコールに関するインストラクションを前記セキュアワールドにおける前記ｆＴＰＭに対してパスするステップと、を含む、
ことを特徴とする媒体。