【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29年9月21日(2017.9.21)

【公表番号】特表2015-524128(P2015-524128A)
【公表日】平成27年8月20日(2015.8.20)
【年通号数】公開・登録公報2015-052
【出願番号】特願2015-518461(P2015-518461)
【国際特許分類】
Ｇ０６Ｆ　12/14　(2006.01)
Ｇ０６Ｆ　21/62　(2013.01)
Ｇ０６Ｆ　21/57　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　５１０Ｄ
Ｇ０６Ｆ　21/62
Ｇ０６Ｆ　21/57

【誤訳訂正書】
【提出日】平成29年8月10日(2017.8.10)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
システムであって、
複数のエンティティによって出された信頼実行環境コマンドをネットワークを介して受信することができる受信モジュールであって、各信頼実行環境コマンドが、前記コマンドを出したエンティティに対応するセキュリティ・コンテキストに対して動作するコマンドである、受信モジュールと、
前記受信モジュールによって受信された前記信頼実行環境コマンドに応答して、鍵および被保護データー集合に対して複数の暗号プロセスおよびセキュリティ・プロセスを実行するように構成されたセキュリティ・プロセッサー・インスタンスであって、該セキュリティ・プロセッサー・インスタンスが、特定のエンティティと該特定のエンティティの対応する被保護データー集合とに結び付けられ、該セキュリティ・プロセッサー・インスタンスが、他のエンティティからの実行環境コマンドを処理するのを阻止される、セキュリティ・プロセッサー・インスタンスと、
複数の被保護アカウントを維持するように構成されたアカウント管理モジュールであって、前記複数のアカウントの内特定の被保護アカウントが、前記特定のアカウントに割り当てられた前記特定のエンティティに対応し、前記特定のエンティティに対応する複数の鍵を含む被保護データー集合を含み、前記被保護データー集合が、前記システムの外部では読み取り可能ではなく、前記セキュリティ・プロセッサー・インスタンスが、前記複数の鍵の内少なくとも一部を使用して、前記特定のエンティティから受信した１つ以上の信頼実行環境コマンドに応答して、暗号プロセスを実行する、アカウント管理モジュールと、
を含み、
前記特定のアカウントが、各々前記特定のアカウントに関連するエンティティに対応する複数のデーター集合を含み、前記特定のデーター集合が第１データー集合であり、前記特定のエンティティが第１エンティティであり、前記複数の鍵が第１複数の鍵であり、前

記特定のアカウントが、更に、
前記特定のアカウントに割り当てられた第２エンティティに対応し、前記第２エンティティに対応する第２複数の鍵を含む第２被保護データー集合を含み、前記第２被保護データー集合が、前記システムの外部では読み取り可能でなく、前記セキュリティ・プロセッサー・インスタンスが、前記第２エンティティから受信した１つ以上の信頼実行環境コマンドに応答して、前記第２複数の鍵の内少なくとも一部を使用して暗号プロセスを実行する、システム。
【請求項２】
請求項１記載のシステムにおいて、前記信頼実行環境コマンドが、トラステッド・プラットフォーム・モジュール（ＴＰＭ）通信プロトコルに準拠する、システム。
【請求項３】
請求項１記載のシステムにおいて、前記被保護データー集合が、前記セキュリティ・プロセッサー・インスタンスによる場合を除いて、読み取り不可である少なくとも一部を含む、システム。
【請求項４】
請求項１記載のシステムにおいて、前記アカウント管理モジュールが、更に、新たなエンティティが前記アカウントに追加されたとき、新たな被保護データー集合を前記複数のデーター集合に追加するように構成される、システム。
【請求項５】
請求項１記載のシステムにおいて、前記アカウント管理モジュールが、更に、対応するエンティティがもはや動作しなくなった後に、被保護データー集合を前記複数のデーター集合から除去するように構成される、システム。
【請求項６】
請求項１記載のシステムにおいて、前記特定のエンティティが特定のデバイスまたはシステムであり、前記アカウント管理モジュールが、更に、前記被保護データー集合の一部をリセットしたことに応答して、前記特定のデバイスまたはシステムがリブートされたことを検出するように構成される、システム。
【請求項７】
請求項１記載のシステムであって、更に、
前記データー集合に関してポリシーが満たされるか否かに依存して、前記特定のエンティティによるアクションを許可するように構成されたポリシー・モジュールを含む、システム。
【請求項８】
コンピューター・プログラムであって、計算システムに、複数の被保護アカウントを維持するように構成されたアカウント管理モジュールを、インスタンス化させ、前記複数のアカウントの内特定の被保護アカウントが、前記特定のアカウントに割り当てられた特定のエンティティに対応し、前記特定のエンティティに対応する複数の鍵を含む被保護データー集合を含み、前記被保護データー集合が、前記特定のアカウントの外部では読み取り可能ではなく、セキュリティ・プロセッサー・インスタンスが、前記特定のエンティティから受信した１つ以上の信頼実行環境コマンドに応答して、前記複数の鍵の内少なくとも一部および被保護データー集合を使用して暗号プロセスおよびセキュリティ・プロセスを実行し、前記セキュリティ・プロセッサー・インスタンスが、前記特定のエンティティと該特定のエンティティの対応する被保護データー集合とに結び付けられ、前記セキュリティ・プロセッサー・インスタンスが、他のエンティティからの実行環境コマンドを処理するのを阻止され、
前記特定のアカウントが、各々前記特定のアカウントに関連するエンティティに対応する複数のデーター集合を含み、前記特定のデーター集合が第１データー集合であり、前記特定のエンティティが第１エンティティであり、前記複数の鍵が第１複数の鍵であり、前記特定のアカウントが、更に、
前記特定のアカウントに割り当てられた第２エンティティに対応し、前記第２エンティ

ティに対応する第２複数の鍵を含む第２被保護データー集合を含み、前記第２被保護データー集合が、前記システムの外部では読み取り可能でなく、前記セキュリティ・プロセッサー・インスタンスが、前記第２エンティティから受信した１つ以上の信頼実行環境コマンドに応答して、前記第２複数の鍵の内少なくとも一部を使用して暗号プロセスを実行する、
コンピューター・プログラム。
【請求項９】
請求項８記載のコンピューター・プログラムであって、更に、前記計算システムに、ネットワークを介して複数のエンティティによって出された前記信頼実行環境コマンドに応答して複数の暗号プロセスおよびセキュリティ・プロセスを鍵に対して実行するように構成された前記セキュリティ・プロセッサー・インスタンスをインスタンス化させ、各信頼実行環境コマンドが、前記コマンドを出したエンティティに対応するセキュリティ・コンテキストに対して動作するコマンドである、コンピューター・プログラム。

【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】０００３
【訂正方法】変更
【訂正の内容】
【０００３】
[0003] このように、ＴＰＭは動作を実行する動作コンポーネントと、ＴＰＭの外部に読み出すことができない被保護データーを保持するメモリー・コンポーネントとを有する。ＴＰＭの動作速度は、ＴＰＭ内部のハードウェアの能力に限定される。また、被保護データーのサイズもＴＰＭ内部の空間に限定される。

【誤訳訂正３】
【訂正対象書類名】明細書
【訂正対象項目名】００２７
【訂正方法】変更
【訂正の内容】
【００２７】
[0031] 更に、セキュリティ・プロセッサー２１３は、ローカルＴＰＭが通常信頼実行環境コマンドに応答するのと同様に、このような信頼実行環境コマンドに応答することができる。例えば、セキュリティ・プロセッサー２１３は、鍵および／または被保護データー集合に対して暗号処理および／またはセキュリティ処理を実行することもできる。これによって、ＴＰＭの機能の多くをエミュレートすることができる。クライアントが破壊されても、ＴＰＭは引き続きシステム２１０において利用可能であり、したがって、ＴＰＭから生成された鍵および他のデーター（ＴＰＭに関連する単調カウンター、不揮発性ＲＡＭのコンテンツ等）を引き続き使用することができる。

【誤訳訂正４】
【訂正対象書類名】明細書
【訂正対象項目名】００３２
【訂正方法】変更
【訂正の内容】
【００３２】
[0036] クライアント２０１の一部はＴＰＭを含んでもよく、一部は含まなくてもよい。例えば、図２の場合、クライアント２０１ＡはＴＰＭ２０２Ａを有し、クライアント２０１ＢはＴＰＭ２０２Ｂを有し、クライアント２０１ＥはＴＰＭ２０２Ｅを有する。クライアントの内、クライアント２０１Ｃ、２０１Ｄ、または２０１Ｆを含む他のものは、Ｔ

ＰＭを有さない。ローカル・クライアントＴＰＭが完全にＴＰＭとして実行していなくても、ＴＰＭの存在は、以下で説明するように、そのＴＰＭの一部のマシン特定機能をオフロードすることを可能にする（マシンに関連する信頼イベント履歴を供給する能力というような）。しかしながら、ＴＰＭがなくても、以下で説明するようにＴＰＭ機能の一部をなおもオフロードすることができる。