【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30年9月27日(2018.9.27)

【公表番号】特表2017-530471(P2017-530471A)
【公表日】平成29年10月12日(2017.10.12)
【年通号数】公開・登録公報2017-039
【出願番号】特願2017-516669(P2017-516669)
【国際特許分類】
Ｇ０６Ｆ　21/12　　(2013.01)
Ｇ０６Ｆ　21/62　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/12　　３１０
Ｇ０６Ｆ　21/62　　３１８

【手続補正書】
【提出日】平成30年8月17日(2018.8.17)
【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】
システムであって、
１つ又は複数のプロセッサと、
コンピューター実行可能な命令を記憶する１つ又は複数のコンピューター可読記憶媒体であって、前記コンピューター実行可能な命令が、前記１つ又は複数のプロセッサによる実行に応答して、前記システムに、
オペレーティングシステムコンテキストの表現に対応する認可プリンシパルをトラステッドプラットフォームモジュール内に導出させるステップであって、前記認可プリンシパルは、前記オペレーティングシステムコンテキストが前記トラステッドプラットフォームモジュールに対して表現されることを可能にするルートオブジェクトを表し、前記オペレーティングシステムコンテキストは、オペレーティングシステムに関して発生する１つ又は複数の識別情報ベースの状態条件を表す、ステップと、
前記トラステッドプラットフォームモジュールとインターフェイスをとり、前記認可プリンシパルを、前記トラステッドプラットフォームモジュール内に記憶されたセキュリティ資産に対して前記トラステッドプラットフォームモジュール内でバインドさせるステップと、
前記認可プリンシパルへのアクセスの要求を受信するステップと、
要求コンテキストが前記認可プリンシパルに合致するか否かに基づきアクションを起こすステップであって、前記アクションが、
要求コンテキストが前記認可プリンシパルに合致することに応答して、前記セキュリティ資産へのアクセスが可能となるように、前記認可プリンシパルへのアクセスを可能とするステップ、又は、
前記要求コンテキストが前記認可プリンシパルに合致しないことに応答して、前記セキュリティ資産へのアクセスが可能とならないように、前記認可プリンシパルへのアクセスを拒否するステップ
の内の一方を含む、アクションを起こすステップと
を含む動作を実行させる、１つ又は複数のコンピューター可読記憶媒体と

を含む、システム。
【請求項２】
前記操作が、トラステッドプラットフォームモジュールのドライバーにより実行される、請求項１に記載のシステム。
【請求項３】
前記オペレーティングシステムコンテキストが、ユーザー識別子、アプリケーション識別子、グループ識別子又は特権レベルの１つ又は複数を含む、請求項１に記載のシステム。
【請求項４】
前記セキュリティ資産が、前記トラステッドプラットフォームモジュール内に記憶されたセキュリティキー、セキュリティ証明書又は保護されたデータの１つ又は複数を含む、請求項１に記載のシステム。
【請求項５】
前記認可プリンシパルが、前記セキュリティ資産へのアクセスに対する１つ又は複数の条件を指定する認可ポリシーを介して前記セキュリティ資産にバインドされ、前記１つ又は複数の条件が、前記認可プリンシパルへのアクセス権が前記セキュリティ資産へのアクセスのための条件であることを指定する、請求項１に記載のシステム。
【請求項６】
前記認可プリンシパルへのアクセスの前記要求が、前記トラステッドプラットフォームモジュールの外部のプロセスにより始動され、かつ、前記要求コンテキストが、前記プロセスに関連付けられたユーザー識別子、前記プロセスに関連付けられたアプリケーション識別子、前記プロセスに関連付けられたグループ識別子、又は前記プロセスに関連付けられた特権レベルの内の１つ又は複数を含む、請求項１に記載のシステム。
【請求項７】
コンピューターで実装される方法であって、
トラステッドプラットフォームモジュール内に記憶されたセキュリティ資産に対する認可ポリシーを構成するための要求を受信するステップであって、前記要求が、１つ又は複数のオペレーティングシステムコンテキストの１つ又は複数の表現に個別に対応する１つ又は複数の認可プリンシパルを識別し、前記１つ又は複数の認可プリンシパルのうちの少なくとも１つの認可プリンシパルは、前記１つ又は複数のオペレーティングシステムコンテキストのうちの少なくとも１つのオペレーティングシステムコンテキストが前記トラステッドプラットフォームモジュールに対して表現されることを可能にするルートオブジェクトを表し、前記オペレーティングシステムコンテキストは、オペレーティングシステムに関して発生する識別情報ベースの状態条件を表す、受信するステップと、
前記認可ポリシーを前記トラステッドプラットフォームモジュール内で前記１つ又は複数の認可プリンシパルで構成させるステップと、
前記セキュリティ資産へのアクセスの要求を可能とすることが、要求コンテキストが前記認可ポリシーの前記１つ又は複数の認可プリンシパルに合致することを条件とするように、前記認可ポリシーを前記トラステッドプラットフォームモジュール内に記憶された前記セキュリティ資産に対して前記トラステッドプラットフォームモジュール内でバインドさせるステップと
を含む、コンピューターで実装される方法。
【請求項８】
前記セキュリティ資産が、前記トラステッドプラットフォームモジュール内に記憶されたセキュリティキー、セキュリティ証明書又は保護されたデータの内の１つ又は複数を含む、請求項７に記載のコンピューターで実装される方法。
【請求項９】
前記１つ又は複数のオペレーティングシステムコンテキストが、ユーザー識別子、アプリケーション識別子、グループ識別子又は特権レベルの内の１つ又は複数を含む、請求項７に記載のコンピューターで実装される方法。

【請求項１０】
前記１つ又は複数の認可プリンシパルが、前記１つ又は複数のオペレーティングシステムコンテキストを使用して生成された１つ又は複数のキーを含む、請求項７に記載のコンピューターで実装される方法。
【請求項１１】
前記１つ又は複数の認可プリンシパルが、前記セキュリティ資産へのアクセスのためのアクセス条件を表す複数の異なる認可プリンシパルを含む、請求項７に記載のコンピューターで実装される方法。
【請求項１２】
前記セキュリティ資産へのアクセスの要求を受信するステップと、
前記要求に応答してアクションを実行するステップであって、
前記要求の要求コンテキストが前記認可ポリシーを満足することに応答して前記要求を可能とするステップ、又は、
前記要求の要求コンテキストが前記認可ポリシーを満足しないことに応答して前記要求を拒否するステップ
の少なくとも一方を含む、実行するステップと
をさらに含む、請求項７に記載のコンピューターで実装される方法。
【請求項１３】
前記１つ又は複数の認可プリンシパルへのアクセスの前記要求が、システムプロセスにより始動され、かつ、前記要求コンテキストが、前記システムプロセスに関連付けられたユーザー識別子、前記システムプロセスに関連付けられたアプリケーション識別子、前記システムプロセスに関連付けられたグループ識別子又は前記システムプロセスに関連付けられた特権レベルの内の１つ又は複数を含む、請求項１２に記載のコンピューターで実装される方法。